

ADAM LEINSS' TECH TIPS

There are 10 types of people in the world: those who understand binary and those who do not.
Posts from leinss.com/blog. Printed on May 26, 2022 using Print My Blog

The Beginning

JULY 23, 2005

CATEGORIES: MISC

Well, not really. I've been posting on news groups (USENET) since 1996 and was on FIDONet back in 1995 (remember the BBS days?). I've always found it fascinating how the Internet allows people to exchange information. What prompted me to start a blog was Mark Russinovich starting one [here](#). To see what kind of geek I am you can check out my [web page](#).

To start off this blog I'll describe how I fixed an Excel upgrade problem yesterday. I was assigned a task of upgrading Excel 2000 to Excel 2002 on a PC running Windows XP Professional. Easy, right? Upon installing it and testing it as myself it worked fine. The next day the user called me stating it was crashing. Indeed, it was crashing quite hard. The application seemed fine until you went to File>Open and then it went to never-never land. Since it worked as me this boiled it down to a permissions or NT profile issue. I reved him back to Excel 2000 which surprisingly worked fine. The next day I went back to reinstall Excel 2002 and check things out while the user was at a meeting. Upon checking the local administrator's group I saw that the user was already an administrator on the machine, thus eliminating a permissions issue.

I then started up [Filemon](#) which is a excellent little freeware utility by our friends at Sysinternals. I setup a filter in Filemon to just show me the excel.exe entries. The last file it read was C:\windows\system32\davclnt.dll. I decided for fun to rename this file to see if that would fix the problem. Of course, this action was not really logical....after all, it would have used the same file logged in as me, right? Any ways, I renamed the file and the appeared back within seconds. Drats! Windows File Protection (WFP) rears its ugly head. Introduced in Windows 2000 WFP protects critical Windows system files by looking for changes. If you touch a critical file by renaming, deleting, or overwriting it, Windows copies the "good file" from a secret folder called dllcache. For a while you could disable WFP by setting "SFCDisable" to FFFFFFF9D in the registry. However, Microsoft later removed this feature with their service packs for Windows 2000 and XP.

To get around this you can [hex edit the sfc_os.dll file](#). However, this didn't work for me and is a bit messy. I like using [XP Lite](#) for this purpose. There is a trial version available for download that the author states "*is yours to keep!*". In the trial version there is an option to turn WFP On, Off or to Disable it. So I can turn it off, do my dirty work and when I reboot, WFP turns itself back on. Well, getting back to davclnt.dll: renaming it did not work. I started to think the problem was in the HKEY_CURRENT_USER (HKCU) part of the registry (logged in as that user of course). So I started up [Regmon](#) this time pausing it just before I went to File>Open. I then saw something interesting. Under HKCUNetwork there was a bunch of drive mappings and one of those mappings was pointing to a bogus server! I exported this key out (always export trees before you start deleting them!) and then deleted it. Tada, problem solved!

Now the interesting question is: why didn't this happen with Excel 2000? Who knows. In this instance deleting the user's NT profile may have been quicker. However, I've only been at this company for a month and therefore I am not well versed with all desktop standards. Besides, the user was gone and his NTUSER.DAT file was 4MB: that's a lot of information to just throw away!

That's it for now. Look for an upcoming article on making hardware independent ghost images for Windows 2000 and XP.

Removing Spyware

JULY 26, 2005

CATEGORIES: SPYWARE

Looking for techniques for preventing and removing spyware? Checkout [Mark Russinovich's webcast](#). Start from section 33.

NOTE: Right-click the link and do a save as to save it to your PC. It does not seem to stream correctly by just opening the link.

– Soli Deo Gloria

Congratulations Matty!

JULY 29, 2005

CATEGORIES: MISC

This post is dedicated to Matt: my co-worker at my last job. He just found another job and I am very happy for him. Matt is very technical and through in solving computer problems. He single handedly rebuilt a NT 4.0 box that died in the cancer department and brought up the cancer software on a Windows 2000 machine with little to no documentation or media. He was also the administrator of our form routing server and tape backup man. He was also great in getting us to Windows 2000 from Windows 98 SE as a desktop standard for various departments. Hey Matt, you remember the Decision Support upgrade? Wow, what a pain that was! Oh what fun it is to convert a 10 year old program using scripts programmed by God knows who dumping data into a mainframe. However, Matt did it.

- Remember “Pizza Thursdays” in the cafe?
- Hitting the golf ball just right into the 1970’s golf ball returner?
- Videos from Ebaumsworld?
- A. Vicious?
- Formscape?
- People also calling me Matt and you Adam?
- Throwing rubber balls at people’s heads?

All the best to you buddy.

– Soli Deo Gloria

Making a Windows 2000/XP Hardware Independent Ghost Image

JULY 30, 2005

CATEGORIES: OPERATING SYSTEM, TECH TIPS

About a year and a half ago I was a part of a 3 member team whose mission it was to create a standard Windows 2000 image for our desktops. The company was currently running Windows 98 SE as a desktop standard. There was a base image and an image for each department and it was messy, real messy! We sat down and discussed what services to leave enabled or disabled, what to include in the default user profile, etc. on the new image. When we were done the image was a beautiful thing. Even though we wrote documentation on everything we did there are always things that get missed. We had a total of 12 Ghost images: 4 for PCs, 6 for laptops (3 with wireless drivers and 3 without) and 2 specialty Ghost images. In January 2005 we merged with another company. This company had about 8 Ghost images bringing the total number of company Ghost images to 20! Under the new management they wanted the patch levels on each image maintained every month! Before that, we were just using SMS 2003 to maintain the patch level of the workstation. You would image a box and then SMS 2003 would push down the new patches. Try calculating the time it takes to open an image, run the patches on it, verify the patch installation with MBSA, do application testing on the image to make sure the patches didn't break anything and finally reseal the image. Now take that calculation times 20. You could easily justify a full time position just for this task!

Not wanting to update 12 images each month I decided to make a hardware independent image for Windows 2000. When I was done, I got it down to 4 images: 1 base and 3 specialty images! Since the base image was used 95% of time for new machines I could take time to get the other ones updated. It took me 3 solid weeks hunting all over the Internet and ghosting countless machines to get it all working. The documentation I wrote for doing this is on my web page [here](#). Just last month I started a new job at another company and again saw images for each individual piece of hardware. Time to test my skills once again!

The desktop platform at the new company is Windows XP Professional. Here's one "problem" I found with my instructions. Under the section Finding the IDE Driver Used To Setup I stated to search for 82801DB in the INF files you extract from the Intel Chipset setup. Well, I was working on a Dell Optiplex 280 and the image was giving a STOP 0x7B message at startup. I had

included support for the IDE chipset driver, but it still wouldn't work. I went back to the INF file and look what I found:

```
PCIVEN_8086&DEV_2651.DeviceDesc="Intel(R) 82801FB Ultra ATA Storage Controllers - 2651"
```

```
PCIVEN_8086&DEV_2652.DeviceDesc="Intel(R) 82801FB Ultra ATA Storage Controllers - 2652"
```

```
PCIVEN_8086&DEV_2653.DeviceDesc="Intel(R) 82801FBM Ultra ATA Storage Controllers - 2653"
```

```
PCIVEN_8086&DEV_266F.DeviceDesc="Intel(R) 82801FB/FBM Ultra ATA Storage Controllers - 266F"
```

Multiple versions of the 82801FB! Obviously, I had picked the wrong one, but which was the right one? We can solve this little problem by using [PCI32](#). This is a freeware program made by Craig Hart that has 15,000+ PCI devices in its database. I'll use my home PC as an example:

Vendor 8086h Intel Corporation

Device 24CBh 82801DB/DBL (ICH4/ICH4-L) UltraATA/100 EIDE Controller

Command 0007h (Memory Access, BusMaster,)

Status 0280h (Medium Timing,)

Revision 02h, Header Type 00h, Bus Latency 00h

Self test 00h (Self test not supported)

PCI Class Storage, type IDE

PCI EIDE Controller Features :

BusMaster EIDE is supported

Primary Channel is at I/O Port 01F0h and IRQ 14

Secondary Channel is at I/O Port 0170h and IRQ 15

Subsystem ID 80891043h Unknown

Subsystem Vendor 1043h ASUSTeK Computer Inc

Address 0 is an I/O Port : 00000000h

Address 1 is an I/O Port : 00000000h

Address 2 is an I/O Port : 00000000h

Address 3 is an I/O Port : 00000000h

Address 4 is an I/O Port : 0000F000h

Address 5 is a Memory Address (anywhere in 0-4Gb) : FEBFB400h

System IRQ 9, INT# A

If you can read the second line it says:

```
Device 24CBh 82801DB/DBL (ICH4/ICH4-L) UltraATA/100 EIDE Controller
```

That's what we want. In the case of the Dell Optiplex 280 it was the 266F one: go figure! Incidentally, we can use PCI32 for much cooler things like updating a universal network boot disk! Or finding that pesky model number without cracking the case. In the case of the Dell Optiplex 620 I found that it had 2 different versions of the same chipset on the same board! So make sure you include support for what ever is in the computer.

The other problem I ran into again was the HAL issue. I commented out the following line in my sysprep.inf:

```
UpdateUPHAL=ACPIPIC_UPC:WINNTInfHal.inf
```

Upon trying the image on a Dell Latitude D620 I was greeted with a message from Windows stating there was a hardware problem and did I want to start Windows. If I answered yes it would BSOD and then reboot before I could even read the message! If you hit F5 right after you pick "Start Windows XP" it will give you an option to "Disable Automatic Restarting on System Failure". Way to go Microsoft! I saw it was a stop 0x7B message. I checked the IDE setup in section and saw that was setup correctly. Having gone through this once before I guessed it was a HAL issue and I was right. By uncommenting the above line and changing WINNT to WINDOWS the image came right up. This line forces the HAL from a Uniprocessor HAL to APCI HAL. What is the difference between these two HALs? I have no idea, but functionally they appear to be the same! I have yet to find good explanation: does anyone have one?

Making a hardware independent image is big business. The original makers of Ghost made a program called the [Universal Imaging Utility](#). They want \$19 per workstation for what we did here. Granted, it's a drop and go solution, but with enough patience you can get a very simliar result with my instructions. In fact, if you want your image to support gobs of hardware you can head over to the Device Drivers subforum over at [MSFN](#) and pick up their Driver Packs, which include support for virtually everything in existence. Note that the Driver Packs are for Windows XP only.

Incidentally, Microsoft claims to solve all this in Windows Vista by using a program called [Ximage](#). Among the cool features it lists:

- This WIM image format is hardware-agnostic, meaning that you need only one image to address many different hardware configurations.
- The WIM image format allows you to service an image offline. You can add or delete certain operating system components, patches, and drivers without creating a new image.
- The WIM image format allows for non-destructive deployment. This means that you can leave data on the volume to which you apply the image because the application of the image does not erase the disk's existing contents.

Time will tell if Ximage makes it to the final build of Vista! Let's make sure that it does.

– Soli Deo Gloria

Removing Spyware Part Deux

AUGUST 1, 2005

CATEGORIES: SPYWARE

Over the weekend I added a new article to my web site called [The Battle Against Spyware](#). I use some of the tricks that Mark Russinovich used in his TechEd talk and a few of my own. Check it out.

– Soli Deo Gloria

Universal Network Boot Disk

AUGUST 5, 2005

CATEGORIES: OPERATING SYSTEM, TECH TIPS

What better way is there to compliment your new universal Ghost image and impress your boss then a universal network boot disk? A PXE server? OK, so maybe it's not the greatest thing in the world, but it sure beats carrying around lots of floppies with you. Not to digress, but why is it that we are still using floppies? The IBM PC was invented in 1981 and here it is 2005 and just last year Microsoft sent out a white paper to companies pleading with them to support booting from USB Flash Devices (UFD). Come on guys, wake up! UFDs are bigger, more reliable and a lot more fun than floppies. Now that Windows PE 2005 supports booting from UFDs we need to pressure these companies to support booting from them.

OK, back to the network boot disk. The one I'm talking about is [Bart's Network Boot Disk](#). One word: freeware. Yes, freeware! I love Bart! He's also the one that makes [PE Builder](#). Check it out: it's very cool stuff! Download the full BFD package and extract it to a directory. Now execute "bfd msnet A:" from the command line. This will make a self-booting network boot disk using the MS-DOS 7.1 files (*an interesting side note here is that Bart has had legal problems with Microsoft and PE Builder. It's a mystery then why he would bundle the MS-DOS 7.1 files directly into this package even though these files are available in particularly every corner of the Internet*). Congrats, you just made a universal network boot disk!

Listed on the same page are driver CAB files for practically every NIC ever made! Now here's the slick part: you can just drop in the CAB files you need into A:libndis and the disk will rebuild itself accordingly! How cool is that? You'll notice that the drivers haven't been updated for at least 2 years and may not include support for the latest NICs. That was the problem when we got in motherboards supporting the Intel 915 chipset. The network boot disk would not find the NIC and even when we manually picked it off the menu the driver would not work (it was a variant of the Intel Pro 100VE). Let's look into how the boot disk works. Every PCI device has a unique hexadecimal id. Let's boot from the network boot disk you created and run pciscan -v:

```

none@PC-053385 Q:\NET>pciscan -v
Bus Dev Func Slot Vvend Dev. Class Name          Subclass Name
-----
 0  0  0  0  8086 7192 Bridge          CPU/PCI
 0  7  0  7  8086 7110 Bridge          PCI/ISA
 0  7  1  7  8086 7111 Disk            IDE
 0  8  0  8  5333 8811 Display        UGA
 0  A  0  A  1011 0009 Network        Ethernet
5 PCI devices found

```

We can clearly see that there are vendor ids and device ids. Based on these two pieces of information the boot disk can determine what driver to load. If you download PCISCAN from his web site it gives a much better explanation than I give. PCISCAN gets its information from nic.map. Let's look for this vendor id in this file:

```
ret="SMCPWR2.COM"  
ven=10B8 "SMC"  
dev=0005 "SMC9432TX EtherPower II 10/100"  
ven=1011 "DEC"  
dev=0002 "DC21040"  
0014 "DC21041"  
0009 "DC21140"  
0019 "DC21143"
```

There is it! I booted the disk using Virtual PC 5 and this is the type of NIC it emulates. So 1011=DEC and 0009 = model DC21140. Let's take a look inside one of these CAB files sitting in A:\libndis:

- e100b.dos
- e100b.ini
- ndis.pci
- ndis.txt

If we look into ndis.pci for the above driver this is what it looks like:

```
ret="E100B"  
ven=8086 "Intel"  
dev=1002 "PRO 100 Mobile Adapters"  
1031 "PRO/100 VE Network Connection"  
1032 "PRO/100 VE Network Connection"  
1035 "PRO/100 VM Network Connection"
```

So in the case of us getting the new computers in with the Intel 915 chipset we just had to get a new .DOS file and update the .PCI file with the correct hexadecimal id. You can get the latest .DOS file easily by visiting Intel's web site. They have DOS drivers for all their NICs. We can use PCISCAN or PCI32 to find the hexadecimal id of the NIC and then add that with the appropriate

description. Finally, we have to repackage them back up into a CAB file. You can download [makev3.zip](#) from [here](#) to do that.

The other advantages to this disk are that it randomizes the NETBIOS name so you can use it in multiple computers at the same time. You can also setup a profile which will save the work group or domain name so you don't have to keep entering it each time. I edited the disk so that it just boots without sitting at the menu asking if you want emm386 support or not. The other thing I changed is the prompt for the second password. This can be fixed by editing the msnet.bat in msnet.cab. Make the following changes:

-----in this section-----

```
:_logon
echo MSNET: Network logon as "%p_user%"
net logon %p_user% %w_passwd% /yes /savepw:no
-----end-----
```

change to:

-----change this-----

```
net logon %p_user% %w_passwd% /domain:%logondomain% /yes /savepw:no
-----end-----
```

-----in this section-----

```
echo MSNET: Starting network services
net start workstation
if errorlevel 1 goto _abort
-----end-----
```

add:

-----add this-----

```
echo %w_passwd%> password.txt
-----end-----
```

That gets rid of the second prompt for the password. Again, note that you will have to use `makev3` to repackage the files extracted from `msnet.cab` back into a CAB file. Note that since this is a DOS boot disk you'll also need WINS support on your network to make it work. DNS

alone will not cut it! The bad news is the new 64-bit processors won't do 16-bit applications or true DOS anymore! Hopefully Windows PE will be well supported for booting purposes by the time 64-bit processing becomes popular. You can port this boot disk to a UFD as well, making boot time in 12 seconds or less so when you have impatient techs like DAVE it will go faster for them!

– Soli Deo Gloria

BSOD Land

AUGUST 19, 2005

CATEGORIES: OPERATING SYSTEM, TECH TIPS

One Friday morning several months ago I encountered a very perplexing problem. A bunch of tickets called into the Help Desk about Windows 2000 machines BSODing. BSOD = Blue Screen of Death: a techie's favorite (or not so favorite) term to describe a dead Windows machine. We determined that a patch pack pushed out the night before was likely the cause. However, the BSOD only seemed to happen on reboot and only on certain Omnitech 3200 machines and not all of them, nor all the time! Upon rebooting some of these machines several times they worked fine until later on when they were rebooted again. I even took one of them out of commission that was crashing, turned off automatic rebooting, wrote a reboot script and left the machine to reboot for 24 hours continuously. Not once did it crash!

The event log showed nothing, a Google search on the error came up with nothing and the crash could not be consistently produced on demand. The BSOD itself was very useless: an `INVALID_PAGE_FAULT` in `NTOSKRNL`. `NTOSKRNL`, as you know, is the heart of the Windows 2000 operating system. It was painfully obvious that it was not the cause of the crashes. We would either rebuild the machines which would fix the problem and then reapply the security patches or just tell the user to keep rebooting the system (incidentally, booting the PCs into safe mode always worked).

After several weeks of rebuilding machines we grew very tired of the situation. No one seemed to have an answer and someone was even called in on a Saturday to reboot a PC with this problem! Something had to be done! Having trial copy of [Winternals Administrator Pak 5](#) I had access to Crash Analyser. What this tool does is it uses Microsoft's own debugging tools to decipher the dump file and then it in turn deciphers the Microsoft debug summary to make a best guess as to what caused the crash. I grabbed the `C:\WINNT\MEMORY.DMP` file after turning on crash dumping on one of the machines causing an issue. Upon running the utility I found out that `idechdr.sys` was the file causing the crash! So, after discovering this, I went to each machine called in and uninstalled the IDE drivers in safe mode and then let Windows 2000 redetect them on the next reboot. This solution finally worked!

This does not explain however what caused this in the first place. I had an Omnitech 3200 under my desk as my work PC and never once did it fail on me with the BSOD. It's very likely that your company won't go out and purchase the Administrator's Pak based on cost, so you can read Dirk

Smith's excellent article entitled [How to solve Windows system crashes in minutes](#) which uses only the freeware debugging tools directly from Microsoft.

- Soli Deo Gloria

Windows Vista

AUGUST 24, 2005

CATEGORIES: OPERATING SYSTEM

Microsoft recently announced the next version of Windows will be called Windows Vista. August 24th will mark the 10th anniversary of the launch of Windows 95. I remember that era very well. I was running Windows 3.1 on DOS 6.22 on a 486SX/33. When my mom went shopping at the supermarket I would always go to the magazine rack. I would read articles about “Chicago”, the codename for Windows 95 and check out screenshots of builds in progress. It was all very exciting to computer users because it was the first 32-bit Windows version for consumers. I remember reading about long filenames, the start menu, built in WINSOCK and plug and play support. Today, we don't even think or appreciate these features. Before Windows 95 you had to name everything in the 8+3 format. Imagine MP3s being limited to the 8+3 format: madonna1.mp3, madonna2.mp3, etc. If you wanted to get on the Internet with Windows 3.1 you had to get Trumpet Winsock. By the way: did anyone ever register Trumpet Winsock? It was shareware, but no one ever seemed to care about that.

My favorite operating system of all time is Windows 2000 Professional. I remember ordering a Hands On Training (HOT) kit for \$129 that included Beta 3 copies of Windows 2000 Pro, Server and Advanced server, a training CD, a sales CD and a free t-shirt. The kit also included final build, Not For Resale (NFR) copies of Pro, Server and Advanced Server, with the server versions having 10 CALs each. I just loved the shadow under the mouse: it made the operating system seem 3D like! Now we have Windows XP: product activation, skins and bloat. OK, OK, I admit it: I have a Macintosh theme on my Windows XP laptop! I look at Windows XP as a Windows 2000 add-on. It took 3 years and over 5000 developers to create Windows 2000 and it's still going strong.

I can't wait to try out a late beta of Windows Vista. I heard they are getting rid of the old DOS like underpinnings and are replacing the setup routine with a Windows PE like environment. You can keep up on the development of Windows Vista (a.k.a. Longhorn) by visiting [Paul Thorrutt's web site](#). Paul also has a nice, text based newsletter called WinInfo that he sends out packed with the latest geek news. I highly recommend it. Best of all it's FREE!

Here are two videos on the daily workings of making a Windows build:

[Windows XP Daily Build Cycle](#)

[Windows 2000 Daily Build Cycle](#)

[Voxware Meta Sound Codec \(needed to listen to Windows 2000 video\)](#)

- Soli Deo Gloria

To err is human...

SEPTEMBER 5, 2005

CATEGORIES: TECH TIPS

Back in August of 1998 on a Friday night in a little Best Buy store I got my first work order. It was to install a ZIP drive into an IBM Aptiva. Having played with computers as a hobby I thought this was going to be a snap. I attempt to open the case and no go. I kept on pulling up and forward on the case and it would just not go! I headed to the Internet and found out that there was a pull release switch under the front bezel. With the case off I then found the drive bay being covered by a metal blank. Taking a pair of pliers I yanked and twisted that piece of thin metal to a certain point, then I started to use my fingers. You guessed it: slice of a finger! I was bleeding all over the customer's computer! By this time it was near closing time and I was very frustrated at this point. I finally installed the ZIP drive, tested with a ZIP disk and threw it back together (wiping all the blood off of it of course).

A few months later I had become good friends with my boss and he told me he thought I was a idiot at first. "Why?", I asked. "That first installation on your first day you did was really bad. You forgot to remove the front cover on the drive bay where the ZIP drive was sitting and you disconnected the floppy drive in the process! I thought you were a complete idiot." Mea culpa! I had rushed the job: testing the ZIP drive without the front bezel on and then just slapping it together and throwing it back on the shelf. Thank goodness my career was not judged on just that one day. All be told, I've cracked motherboards, destroyed data and even blew up a NT 4.0 server acting as a print router (thankfully not on the same day)!

All these incidents are great because I learned from them. Fixing computers is almost like a game of chess: everyone understands all the basic rules of chess, but not everyone is a grandmaster. The more chess games you play the better you become. You might favor one opening and your opponent another. You might have all the chess knowledge in the world, but if you act impulsively you will likely lose to a less experienced player. You will make mistakes whether you like it or not.

Case in point: when faced with a crashing system in the past I would usually just rebuild a system from scratch. This might be OK in the consumer arena where people back up their data religiously to CD-Rs and other removable devices (can you feel the sarcasm?). However, that wouldn't fly on the VP's computer who stores all of his personal documents and kids pictures on

his laptop. Pretend the computer is your opponent. You don't want to be checkmated or stalemated, you want to win! How do you do it?

First, ask the right questions to the user:

- * When did this start happening?
- * Has anything changed within the last X days?
- * How often do you do this function?

Then, start the troubleshooting:

- * Check the event logs (assuming a NT system). Log anything suspicious.
- * If you get an error message log that.
- * Check startup entries using Autoruns and the processes running by using Process Explorer.

Now, research the problem:

- * Input the error code or problem into [Google](#). You'll be surprised the wealth of information out there!
- * Check [Microsoft's Knowledgebase](#). People all over the world contact Microsoft for tech support and you will be surprised at the amount of knowledge there.
- * If you still cannot figure the problem out post what you are experiencing on [Experts Exchange](#) or USENET.

You can post on USENET via [Google Groups](#). USENET is a world wide messaging state dating back to the early 90's. Just do a general search on what you are having a problem with (e.g. input "Outlook 98" if you were having problems with Outlook 98) to pinpoint the news group (message board) that handles such problems and post your problem there. For example: I like to frequent the news group microsoft.public.win2000.setup_deployment. This news group focuses specifically on deployment problems with Windows 2000. Not Windows 9x, not NT 4.0 or XP: just Windows 2000. The people that frequent this news group are usually very familiar with the subject at hand and this is usually the case for many other news groups. There are over 40,000 USENET news groups relating to subjects such as computers, tv sitcoms, bands, politics and anything else you can dream of. Google Groups has archived USENET messages all

the way back to the early 90's, so this is another great place to search for conversations on specific error messages and problems.

Finally, implement the solution. Sometimes people will give you 6 or 7 possible solutions. This might require more research on your part. If the problem is happening on Windows 2000 and someone gives you a fix for Windows NT 4.0 you need to realize that will probably not fix your specific problem.

How do you become a better PC Technician? Here's what I think:

1. Experience: the more you play with computers the better you get.
2. Willingness to learn: if you think you know it all you will fail miserably.
3. Thirst for knowledge: you might think this is the same as #2, but it is not. I may be willing to learn something new, but not ambitious to go out and learn about other new things.
4. Know your limitations: Clint Eastwood said it so it must be true. Seriously, some problems go past your knowledge. In those cases you have to park your ego and go ask for someone else's help.

– Soli Deo Gloria

Windows PE

SEPTEMBER 10, 2005

CATEGORIES: OPERATING SYSTEM

Earlier this year Microsoft discontinued licensing MS-DOS (finally!). Let's see: MS-DOS 1.0 came out in 1981 and now it's 2005. 24 years for an operating system isn't bad! Yet even after the pulling of support for MS-DOS it still is very much with us. I use a MS-DOS network bootdisk every day at work to pull down Ghost images from the server. At my last work place we were still using a DOS program for scheduling surgeries based on the old BTREIVE database technology and a DOS program to fill prescriptions in the pharmacy. Just a few weeks ago I was helping a user troubleshoot a program running in GWBASIC, an old DOS based 16-bit BASIC compiler!

Upon the arrival of Windows 2000 we had the introduction of NTFS to the masses. DOS doesn't do NTFS without special software like NTFSDOS. Unless you pony up money for the commercial version of NTFSDOS the only thing you can do is read files from DOS. This is a serious drawback for trying to do troubleshooting and recovery data from NT systems. Microsoft's solution: Windows PE.

What is Windows PE? Well, here's what Microsoft says: "Microsoft® Windows® Preinstallation Environment (Windows PE) is a tool based on Microsoft Windows XP Professional that allows IT staff to build custom solutions that speed up deployment through automation so they spend less time and effort keeping desktops updated. Windows PE can run Windows setup, scripts, and imaging applications. Enterprise Agreement (EA) and Software Assurance Membership (SAM) customers received Windows PE in their October 2002 updates, and it will continue to be offered as a benefit of Software Assurance."

Well, that isn't very descriptive. Essentially Windows PE is a modified version of Windows XP that is designed to run from a CD-ROM disc, that is, a read-only media. As you can see above, if you aren't a big cheese with an EA agreement you don't get to play with Windows PE. However, if you compare the files from the Windows PE to the Windows XP Pro CD you will find most of the files are identical.

That is when Bart Lagerweij made something called the PE Builder. This allows you to make your own version of Windows PE called [BartPE](#) (BartPE is very much like Windows PE, but for legal reasons Bart isn't able to say that). BartPE is very cool! It supports many plugins for different applications. Here's a cool one as an example: [Key Finder PE](#). You can boot from a

Windows PE CD, run this program under Windows PE and it will give you the machine's product key! This could be useful say if a hard drive crashed and your customer didn't have their original key handy.

There is a complete discussion forum dedicated to BartPE over at [911CD](#). This technology will be very big in Windows Vista replacing what we now know as the Recovery Console. So make yourself very comfortable with technology.

– Soli Deo Gloria

The E-mail Problem

OCTOBER 21, 2005

CATEGORIES: TECH TIPS

Now I know why I hate AOL. A couple of years ago I subscribed to an e-mail service called Mailblocks. I had a bunch of my news letters forwarded to various aliases at Mailblocks and it worked quite nicely for curbing spam. A few months ago AOL bought out Mailblocks.com and hired all of the Mailblocks staff. I got a sickening feeling about this, but there wasn't another e-mail service that did what Mailblocks did (Challenge/Response spam control and aliases). The service started to get slow and was down for long periods at a time. Alas, on October 16th, AOL announced it was discontinuing the Mailblocks service and was replacing it with a crappy version of its own. Yes, I said crappy. There was no mention of Challenge/Response spam control in this new e-mail service and of course you can imagine that my e-mail address would be aleinss@aol.com. Shudder! I'm sure there's a few blacklists roaming out there with aol.com plastered all over them.

I quickly regained my composure and went over to www.emailaddresses.com. This is a nice little web site that has information on all sorts of e-mail providers. If you are looking for an e-mail provider I highly suggest it. My big requirement was aliases. Why? Well, when I go to a merchant's web site they always want my e-mail address. There's really no way of tracking who sold your e-mail address when you have given your e-mail address to multiple providers! So I made an alias for every web site I went to. This alias would forward e-mail to a specific folder. I found that when I started to get spam in one folder I would simply delete the alias and make a new one. Once your e-mail address is on a spam list it is never coming off of it. Granted, this required a lot of work on my part, but it kept my inbox pretty darn clean.

The first e-mail provider that caught my eye was Fastmail.fm. Unfortunately, they only offer 5 aliases on their own domain. Then I saw an intriguing feature: having them host your own domain name for e-mail! On went on to look at this and saw that domain registration is \$8 a year. I could register my very own domain name and keep the same e-mail address as long as I wanted to. I continued on and found the e-mail provider Tuffmail. They offered unlimited e-mail aliases and 500MB of space at \$25/year. That is what Mailblocks was charging and they only offered 100MB of space and 25 aliases. I also decided to register a domain in my name: literally my last name of Leinss. This name is very unique and cool. I can search the whole Internet and see everything that I posted. You will find a few of my relatives by searching on this term.

Using Tuffnames I registered www.leinss.com for the next 10 years. What's cool is that even if Tuffmail goes out of business I can point my MX records to the mail server of my new provider. Here's another cool feature: forwarding domains. I can actually "park" my domain at Tuffnames (a reseller of GoDaddy) and then have it forward www.leinss.com to my web page at Kirenet. If Kirenet goes out of business, I just move my web site to another provider and change the forwarding domain. I actually tried to keep the same e-mail address long ago with mail.com. They promised a free e-mail address for life and free forwarding. After several years they were bought by another company. This company decided that free forwarding was not in their best interest and forced everyone to pony up money if you wanted your "free, lifetime e-mail address" to get forwarded to somewhere else. No grandfathering, no backing of the earlier promise, nothing. I was using this e-mail address (aleinss@mindless.com) on the USENET for many years and I was getting about 75 pieces of spam PER day. It was time to give up the "lifetime" e-mail address.

How do you get the best e-mail experience?

Use "disposable" e-mails for merchant web sites. Never give them your "real" e-mail address.

Never post your real e-mail address on the Internet. If you must, make sure you tailor it in a way that doesn't look like an e-mail address. For example: on my web page I made an alias web@leinss.com. If you send e-mail to web it gets forwarded to my web folder. If some nut job decides to spam that alias I just make a new one (which takes all of 30 seconds). Combined with the spam lists that Tuffmail offers (which are impressive I must say and very configurable client side) and unlimited aliases, Mr. Spam Man ain't getting to this guy!

Give your real address to friends and acquaintances only.

-Soli Deo Gloria

Sony, Rootkits and DRM

NOVEMBER 1, 2005

CATEGORIES: MISC

Check out the blog entry [Sony, Rootkits and DRM](#) on Mark Russinovich's blog. Very interesting read on how the music industry is using rootkits for installing their copy protection schemes! This will make you think twice before buying or loading a DRM protected CD.

-Soli Deo Gloria

The Power of Remote Control

NOVEMBER 14, 2005

CATEGORIES: TECH TIPS

Several years ago I started working in a help desk doing phone support 2 days a week. At the time we did not have remote control capability to workstations. Words cannot describe the frustration there is trying to solve something you cannot see. What I call an icon and what the user calls could be (and usually is) two different things. “Now open My Computer” says the tech and “IT IS OPEN” yells the user. Don’t laugh, it happens far too often. Eventually, the help desk did get a buggy version of workstation remote control software with Novell Zenworks 3. However, this little beast was based on IPX communications which are older and much more unreliable than TCP/IP communications. We also had problems with video acceleration crashing the remote control agent on the user’s machine, so I had to figure out a way of disabling the acceleration. We finally got Microsoft SMS 2003 for inventory management and remote control and let me tell you that is one sweet product.

Of course you probably don’t have money for SMS 2003 and that’s where VNC comes in. VNC stands for Virtual Network Computing and was originally developed by AT&T. Those nice guys at AT&T released the source code for VNC into the public domain (or more specifically: GNU...I know GNU’s not public domain, but you get the point). VNC lets you connect to a client workstation from your own workstation for.....FREE. Free? Yes, free. Everyone likes the word free including me!

So how does it work? You basically put a remote VNC host on the workstation (a mini server) and then you connect to that workstation using a VNC viewer. This is done using the standard TCP/IP protocol. It will even do it by host name (which resolves to an IP address). At my new company we didn’t have any remote control software, so I decided to use VNC on our workstations (with management approval of course). There different “flavors” of VNC: RealVNC, TightVNC, UltraVNC, etc. You can lock down VNC by using a password to keep out the bad guys. UltraVNC will do Windows authentication, RealVNC will not (unless you pony up money for the enterprise version).

In the course of using VNC you’ll notice one really annoying thing: no computer list. There’s really no way of knowing what computers have VNC and which ones don’t. That’s where VNCSscan comes in. VNCSscan will scan your network based on the IP parameters you give it and will search your entire network for VNC and RDP clients. How cool is that? Now this program is

\$39 per administrator, but there is a trial copy at the web site that is good for 30 days so you can completely test drive the program before buying (that's PER administrator, NOT per computer!). After downloading and installing the program you make a group (or multiple groups). You then specify the starting and ending IP address. Now you can right-click on the group and pick Scan. Again, make sure you have permission from your management team to do this as this will do a port scan of your whole network. Some network administrators may get a bit upset at you if you don't ask first.

If you are are running Windows XP SP2 like I am you'll notice that VNCSscan won't recognize computers that are truly running VNC nor find them. What gives? Well, according to VNCSscan you need a patch to boost your concurrent TCP/IP connections. That brings us to this [site](#) which claims "Since XP SP2 there are only 10 concurrent TCP connection attempts possible, while in SP1 it has not been limited." Well, thank you Mr. Gates! I'm sure this is all part of the M\$ security initiative: if you cannot run port scanners you cannot be a bad boy with Windows XP SP2. I ran the patch and sure enough, VNCSscan worked like a charm. The makers of VNCSscan claim you should boost the default number from 10 to 10,000, but I just did 100 and it seemed to work fine.

The amazing part did not stop there. The company I currently work for now is setup in one big Microsoft work group. There is no way of pushing programs out to users workstations (no free way at least). When I saw the option in VNCSscan to right-click on a computer object and "Deploy VNC here", I was expecting it to fail. To my surprise it actually worked! I spent countless hours trying to get programs to push out to a PC and here was VNCSscan doing it like it was nothing. Now, there a few caveats to this. You need local administrator rights on the box you are trying to push VNC out to. You'll also need Windows Script Hosting (WSH) on the target box, so this will only work with 2000, XP and beyond. Finally, I'm guessing you'll need File And Print Sharing, Remote Registry and the Server services enabled on the target workstation (and the Windows Firewall turned OFF). I'll going to try to decode the script they use, because it seems to work quite well. There is one bug I found in the program. The list shows computers that have VNC on them and those that don't. If you pick "Deploy VNC Here", VNCSscan shows that computer has VNC on it after the script runs on it even if the script fails to install VNC on the computer! They need a cleaner way of determining if the installation was successful or not.

If you read up on UltraVNC you'll also notice a program called UltraVNC SC. What can you do with this program? Well, lets say you have Joe User on the West Coast having problem with his laptop. Joe User is behind a router with a private IP address. How in the world are you going to connect to Joe User? That problem is solved with UltraVNC SC. This [PDF](#) was shamelessly

pulled from a sticky in the UltraVNC forum. Simply stated: you start a VNC listener on your end opening up port 5900. You'll need an external name or IP address which you can simply get for free from www.dyndns.org. You then configure UltraVNC SC per the instructions and then throw it up on a web site. Have Joe User download the program and then run it, and bingo, he connects right into you. No fuss, no muss. Now if you don't think that is impressive, check out [Webex](#) which offers a commercial version of this technology that goes for \$149/month for one seat. Just imagine the possibilities: if you have a computer store you can configure your store logo into UltraVNC and then offer that as part of warranty service. Maybe we can dream, like those spam messages that always say, "work from home and make thousands". Hey, maybe this is not such a bad idea after all.

Now, your security team (if you have one) will need to do a risk assessment and evaluation of VNC. I believe the authentication piece is encrypted, but the rest of the communication is not. I also noticed the administrator password I used to connect to workstations was in plaintext in the file C:\Program Files\TGC\SVNCScan Console .NETauth.cmd. If I should decide to register this program I believe that this issue needs to be addressed.

-Soli Deo Gloria

Sony Caves In

NOVEMBER 24, 2005

CATEGORIES: MISC

After a boat load of bad press, law suits and warnings from the government, Sony decided to recall music CDs using its secret rootkit technology to enforce intellectual property rights. I have very strong feelings about copy protection which you can read [here](#). This is the PDF version of a report I wrote for a class back in college. I think we may get to a point where media is plagued with so many protection systems that people will stop buying them. How much money did Sony save itself with this copy protection scheme? It has to recall all of these CDs, re-compile them, re-press them and re-release them.

Sadly, this is nothing new. Back in the good old days manufacturers intentionally put bad sectors on floppy disks so people couldn't make backup copies of them. The problem with this approach is that floppy disks are inherently susceptible to corruption and not being able to make a backup copy seriously inhibits the user from using the software. Eventually, the manufacturers removed the copy protection due to decreasing sales.

With all of these copy protection schemes you think piracy would have slowed down or stopped. It hasn't. In fact, the more protection schemes you have the more people you have looking for cracks. For example: Command and Conquer Renegade. This is one of my favorite games. Despite verifying its serial online, the game requires me to keep the CD in the CD drive. Why? Well, I might have copied the CD from someone else. I have to keep removing the game CD every time I want to play another CD. Why should I have to bother myself with this? Why not go find a crack that removes the game's ability to look for the CD? These copy protection schemes only prevent the truly clueless from bypassing them.

The music industry has made a special point of going after consumers that share music with law suits. We can only hope that consumers return the favor with this malware invasion of their personal computers.

-Soli Deo Gloria

Antivirus Nightmares

DECEMBER 10, 2005

CATEGORIES: MISC

I've used various antivirus programs over the years and want to share my thoughts on some of them. Just recently I was running Symantec Antivirus 10 Corporate Edition. This is a no thrills antivirus program that doesn't have any of the bloat of the retail version. A few weeks ago I came home and SAV informed me of a hacktool named SVKP.SYS in my Windows directory. I was quited alarmed, wondering how on earth I would have gotten a hacktool. I then went to play one of my favorites games, Command and Conquer Renegade only to find it did not work. Why didn't it work? Well, it was because SAV had removed SVKP.SYS! See, I also run an addon to Renegade called Renguard. This addon ensures that I am not cheating by using various techniques. In order to prevent debugging tools such as Regmon and Filemon from disassembling and circumventing the program, it uses this tool kit to prevent Renguard from running if it detects these tools.

This is the problem with SAV. Whenever it finds a file that could be used with a virus its immediate action is to delete the file. Instead of this dumb action, how about letting the user decide what to do with the file? In the above case I would have done some research before blindly letting SAV deleting any file it wishes. In addition to doing this, SAV seems to take a ridiculous amount of RAM: 28 MB! 28 MB for what?

I then decided to try out McAfee 8.0i. Unfortunately, it has the same problem as SAV: removing files that are not viruses, but valid security tools. McAfee also took around the same memory (27 MB). I removed it at once as well.

I then tried NOD32. Again, it would find files that were not viruses which is really annoying, but at least NOD32 gave me the choice what to do with the files. Now that's an anti-virus program I like to see! In addition, NOD32 only took up 18 MB vs. 28 MB for SAV and McAfee. In addition to its small footprint, NOD32 also updates virus definitions DAILY. That means if a virus should break out you are much better protected then with McAfee or SAV.

[NOD32](#) is available for download for a 30 day trial.

-Soli Deo Gloria

Christmas Burger King Diddy

DECEMBER 13, 2005

CATEGORIES: JOKE

The famous, funny and politicallly incorrect Christmas spoof of Burger King's "99 cent special" from a few years back. View it [here!](#)

-Soli Deo Gloria

Disabling Sound During Sysprep

DECEMBER 19, 2005

CATEGORIES: TECH TIPS

In a business environment, you usually do not want users having the ability to produce sound on a computer. In the latest Dell GX280, GX620 and GX520s, however, they use the regular internal speaker as if it was a regular speaker. I actually remember doing this in Windows 3.1 with a special driver. The only problem is that when Windows 3.1 would play the sound nothing else would happen. If I was playing a game, Windows 3.1 will literally stop everything, play the sound and then resume operation of the computer.

Now, it's easy enough to go into the device manager to disable the sound card after ghosting an image down to a machine. Wouldn't it be better if we could script it? Well, we can! Microsoft has a nifty utility called `devcon` that will interact with the device manager on a command line level.

Every device in a computer will have an unique hexadecimal id. Download devcon and then issue "devcon find *". This will return all of the devices in the system and there corresponding ids.

Upon issuing this on a Dell GX620 and scrolling through the list we find this:

```
PCIVEN_8086&DEV_27DE&SUBSYS_01AD1028&REV_01: SoundMAX Integrated Digital Audio
```

Here's the part we need:

```
PCIVEN_8086&DEV_27DE
```

Now we can type the following: "devcon disable "PCIVEN_8086&DEV_27DE". Viola, the sound card is disabled! We can put this in the section in sysprep.inf to disable the sound. Repeat this for every model of computer you have (the statement for the GX280 looks like this: "devcon disable "PCIVEN_8086&DEV_266E"")

Wait...what about laptops? We give laptops to traveling users and it's OK for for them to have sound. The problem with the above statement is that the Dell Latitude D610 and Dell Optiplex GX280 share the same sound chipset! The above statement will disable the sound chipset on both models. How can we get around this? Well, from a little trick from my sysprep page:

```
@echo off
```

```
C:installtemppci32 > C:installtempdev.txt
```

```
C:windowssystem32find /i "cardbus" C:installtempdev.txt >NUL
```

```
if errorlevel 1 "C:installtempdev.txt"
```

```
if not errorlevel 1 echo "Not a workstation, do nothing"
```

Here's what this does: it runs PCI32 from Craig Hart to run a hardware profile of our system and dumps the results into a file called dev.txt. It looks for any text with the labeling "Cardbus" in the dev.txt file. Cardbus is only found in laptops. If we find the term "cardbus", the find program will return 0 and 1 if it doesn't find it. Based on this result, we can determine whether we are imaging a laptop or desktop. If it's a laptop, the command for disabling the sound never executes.

-Soli Deo Gloria

Mark Russinovich's Webcast on Malware

DECEMBER 20, 2005

CATEGORIES: SPYWARE

Microsoft gave me the option of saving this great web cast offline! I uploaded to my web site [here](#) so that all may enjoy it.

More Microsoft web casts are available [here](#) from TechEd 2005.

-Soli Deo Gloria

Meet the Voices Behind the Movies

DECEMBER 23, 2005

CATEGORIES: JOKE

It's going to be the white knuckle thrill ride of the year!

-Soli Deo Gloria

WMF Exploit

DECEMBER 28, 2005

CATEGORIES: SPYWARE

There's a nasty exploit going around involving WMF files. Windows XP SP2 is not protected by any of the updates now available. Check out this [video](#) showing the exploit in action. It infects your computer with spyware, then prompts you to buy Winhound for \$39.99 to clean it off! [F-secure's blog](#) describes this little demon. Be careful out there.

-Soli Deo Gloria

Moving to New Web Hosting Company

JANUARY 7, 2006

CATEGORIES: MISC

Shortly, I will be moving my web page to a new web hosting company. The web page currently available will remain the same for now. I'm actually learning how to use Adobe Golive! to make a more aesthetically pleasing web site. However, once the new web page is in place, some of the links on this blog may break and pages will be moved around. It may be wise to save any articles or files NOW before I start breaking things!

The main site (www.leinss.com) is the one that should be bookmarked and not stealth.kirenet.com/~aleinss.

Update (10 PM): I made the change shortly after I wrote this. My web page is now up at the new provider Powweb. Unfortunately, after I changed my name servers to Powweb they wiped out my main MX record and reset it to mail.leinss.com. I have to now forward all of my incoming e-mail from Powweb to Tuffmail because the DNS propagation is going so darn slow (I might be in a walker by the time the Internet sees my new MX record).

2nd Update (1/8/06):

I had to go from Powweb.com to Dreamhost.com, because Powweb's name servers wouldn't take my MX record changes. I waited 22 hours and still no change. Dreamhost's name servers picked up in the change in 30 minutes!

– Soli Deo Gloria

New Web Site is Up!

JANUARY 20, 2006

CATEGORIES: MISC

Out with the old and in with the new. My new web site at www.leinss.com is up and running on a new host! A lot of content from my old site has been transferred over, except some of the really old stuff (like my how-to guide ripping guide TV shows using a TV tuner card). I can now run detailed statistics to see where hits are coming from and what the most popular areas of my web site are.

What do you want to see on my web site? Let me know by e-mailing me at [web\(..at..\)leinss.com](mailto:web@leinss.com)

-Soli Deo Gloria

Moving From Blogger to WordPress

JANUARY 21, 2006

CATEGORIES: MISC

This morning I got the WordPress blog up and running on my own web site at www.leinss.com/blog. Please update all of your links to point to the new web site. I am going to place “pointer links” in each blog entry at Blogger so people redirected from old links can find the content at the new place. The blog entry on Filemon and Regmon has been moved the HOW-TO section of my web site. Each blog entry that represents a HOW-TO article will get a permanent home on my web site’s HOW-TO section as well.

– Soli Deo Gloria

NTLDR Missing

JANUARY 23, 2006

CATEGORIES: TECH TIPS

Got a ticket today to look at a Dell Precision 360 workstation. Upon arriving, I noticed the following error message “NTLDR is missing”. After a big gulp, I loaded my Windows XP CD to attempt a “fixboot” and “fixmbr”. Unfortunately, this particular computer was setup with IDE RAID-0 and I had no idea where the driver disk for it was. Using [BartPE](#), I booted the PC. I breathed a sigh of relief when I saw all of the user’s files there. However, boot.ini, ntdect.com and ntlldr were missing from C:. Using BartPE, I copied these files from my workstation (also running Windows XP) to his workstation. Upon reboot, I was greeted with this message:

system32hal.dll is missing or corrupt reinstall file

I booted with BartPE again and saw that the file was indeed there. I looked at another Dell Precision workstation and noticed this line in the boot.ini:

default=multi(0)disk(0)rdisk(0)partition(2)WINDOWS

Dells usually have a hidden diagnostic partition which can throw a tech off. Upon changing the partition from 1 to 2, the system booted. It booted and then it rebooted ad infinitum. I then boot it into safe mode and it gave me an option to do a system restore. I happily agreed to this prompt and restored it from a week ago. System booted right up!

This taught me two lessons: always treat each problem as unique. A missing NTLDR usually spells hard drive failure, but in this case it appears there was nothing wrong with the hard drive. Finally, system restore really does work! I have a habit of turning this off on each workstation I visit (due to it wasting resources), but it saved my bacon today. I am never turning off system restore again!

– Soli Deo Gloria

Moving Hard Drives Between Windows XP Systems

FEBRUARY 1, 2006

CATEGORIES: TECH TIPS

How many times have you gotten a call for a computer that's dead and the user needs the computer up right away with their data? Now, if we live by "best practices" all of the user's data wouldn't be on the hard drive, but a network drive that's being backed up. The department's PC setup would be documented with well written documentation. I have worked in such an environment and let me tell you it is pure bliss! Maybe, however, you don't work in such environment. Maybe the install discs are lost. Maybe the software needs to be activated with the company and the company has gone out of business. Maybe you have no idea how or what the software does. "Just pull the hard drive from the "sick" PC and put it in a good spare PC" you say. Ah, but you assume that you have a spare PC for each model. Management usually doesn't like keeping spare PCs around for "what-if" situations. We need to be a little more creative.

Case in point: I recently had a GX270 computer that had trouble turning on. We recently gotten in a few new GX520s from Dell. These two computers are completely different beasts: different motherboards, different IDE chipsets and different hard drive interfaces. The GX270 had a PATA hard drive interface and the GX520 a SATA interface. The old hard drive switch-a-roo technique won't work here. Even if the hard drive interfaces were the same, we have one small problem: differences in the IDE chipsets. If you ever tried taking the hard drive out of a XP machine and port it to another PC, you probably have been greeted by a STOP 0x0000007B error message. This phenomenon is explained in this [Microsoft Knowledge article](#). It relates to the differences of the drivers of the IDE chipset. When you take a hard drive from one PC to another that has a dissimilar IDE chipset, it won't work. The computer tries to initialize the drivers for a chipset that doesn't exist. Since this chipset is responsible for booting the computer and Windows can't initialize it, the booting fails. If you have access to the old PC and it boots, the solution is simple. Before switching out the hard drive, boot Windows XP. Go into the Device Manager and expand the IDE ATA/ATAPI Controllers section. Update the driver of the primary and secondary storage controllers to the driver labeled "Standard Dual Channel PCI IDE Controller". When prompted to reboot, **DO NOT REBOOT**. Now power off the old PC and place the hard drive into the new PC. Windows should boot with the generic IDE drivers and upon booting into Windows completely, it should detect the real identity of your IDE chipset and load the appropriate drivers (*if it doesn't, you might have to download the chipset drivers for that*

particular motherboard). It will prompt you to reboot again after “installing new devices”. Go ahead and do so. Viola, you just performed “open PC surgery”!

In my case I just changed the drivers on the old PC, make a Ghost image and then brought that Ghost image back down on the new PC. Alas, what if the old PC won't boot? How do you hack the registry without getting into the original operating system? This [web site](#) offers a very ingenious solution. Interestingly enough, it's made by a Macintosh guru by the name of Philipp Biermann. I'm going to post his instructions and files here in this entry with a bit of modification. He claims these instructions work with Windows 2000 as well, but he appears to be using the same mergeide.reg file from the XP article on the Microsoft Support Knowledgebase mentioned earlier. I would be very leery of using this on a Windows 2000 machine unless you have done a full backup of the affected PC (*a full PC backup may be a good idea in all cases*).

0. Download [mergeide.zip](#) from my web site

1. Place the hard drive from the affected PC into another PC as a slave drive

2. Extract the Atapi.sys, Intelide.sys, Pciide.sys, and Pciidex.sys files from the Driver.cab file into the slave drive folder %SystemRoot%\System32\Drivers folder. Make sure you use the Driver.cab file from the same service pack level you are at (i.e. if you are working on a hard drive loaded with Windows XP SP2, use the Driver.cab from SP2 media. You can usually tell if a service pack has been applied to a Windows XP machine by looking for the presence of a \$NtServicePackUninstall folder under the C:\Windows directory)

3. Open the Registry Editor by going to Start>Run and type in regedit (*type in “regedt32” if you are running Windows 2000*)

4. With the mouse, mark the “HKEY_LOCAL_MACHINE”

5. Go to the File up on top and then choose “Load Hive”

6. Navigate to the “%SystemRoot%\System32\config” folder (*Example: C:\windowssystem32config*)

7. Open the “system” file

8. When asked for a name, give it the name “aaaa” (**this is important since it must match the file you downloaded from here**)

9. Close the registry editor

10. Double click the expanded file you got from the mergeide.zip file. It will ask if you want to import the changes from the REG file. Say yes.

(Note, you have two choices: mergeide.reg or mergeide1.reg. The difference is that the mergeide1.reg does not contain the entries for the drivers. Most of the time, they are present anyway. It is probably safer first to try this version. If mergeide1.reg does not work, do the procedure again and use the mergeide.reg file)

11. Now, open the registry editor again and look for the “aaaa” tree in the HKEY_LOCAL_MACHINE directory

12. Mark it and from the File menu, choose “Unload hive” (**this step is important as not unloading a hive can cause corruption**)

13. Close the registry editor

I choose to host his mergeide.zip file on my web page in addition to his in case he ever decides to take it down (Josher took down his “Tale of Two HALs” and had no backup copy of his web site. Had I known he was taking it down I would have copied it!) Did you see what he did? He loaded the slave hard drive’s registry as a hive under the key “aaaa” and then modified the mergeide.reg to merge directly into the loaded “aaaa” hive. Brilliant

– Soli Deo Gloria

Can't Burn at Anything but 48X!

FEBRUARY 4, 2006

CATEGORIES: TECH TIPS

Here's a weird problem that's plagued me at work for a while. My CD burner in my work computer would not burn at any other speed other than 48X! Not slower or faster, just 48X. It came with a Dell and it is model HL-DT-ST CD-RW GCE-8483B made by LG. After doing an Internet search I found this [thread](#). It seems this is a known problem! By using the firmware provided it introduces three new burning speeds: 8x, 12x and 16x. Surprisingly, the 48X speed is gone. Hmm! I actually had to disconnect my other CD-ROM drive and make the burner the "master" drive before the update would actually work. Hopefully this entry will help anyone using this particular model of CD-ROM burner

– Soli Deo Gloria

Detach That Peripheral!

FEBRUARY 12, 2006

CATEGORIES: TECH TIPS

During these past two weeks I've noticed an interesting phenomenon: attached peripherals causing systems not to boot. My first call was a computer out on the shop floor with a keyboard not working. It was a Compaq 733 Deskpro. The screen was totally black and the user wasn't around. I proceeded to unplug the computer and plug it back in from the power. Still no video and no hard drive activity, although the fans would speed up. Every cable was nice and snug. I proceeded to reset the CMOS using the jumper on the motherboard. No go. I then proceeded disconnect all peripherals from the computer (network cable, monitor cable, etc). System booted right up! I added the peripherals back one at a time until I added the keyboard cable back in and then the system won't boot. Replacing the keyboard fixed the problem. This morning, I was working on a D600 Dell Latitude laptop. Upon rebooting, the system would freeze on the BIOS screen. Powering the laptop off and on and disconnecting the battery made no difference. I proceeded to disconnect the network cable and the attached IPOD device and the laptop booted right up! It seems having the IPOD plugged into the USB port was causing the system not to boot. If you have a system that isn't booting up, start by simplifying the problem by detaching all peripherals.

– Soli Deo Gloria

I Finally Got a DVD Burner!

MARCH 2, 2006

CATEGORIES: MISC

I finally broke down and bought a DVD burner, realizing that the war between HD-DVD and Bluera y will go on for years on end. I think people will be sticking to their trusty DVDs for a long time. After reading a few reviews, I settled on the LiteOn SOHW-1693S DVD drive. I got it for \$39.99 from NewEgg.com. That is dirt cheap for a DVD burner! I also ordered two 50 pack spindles of Ridata DVD-R media at \$17.99 a spindle. The drive came bare, no box or manual, but who needs those any how? It did come with a copy of Nero Express 6 and PowerDVD 5. Installation was no brainer, I was up and running in 15 minutes. I proceeded to burn a few DVDs. I got a couple of coasters the first few times. Although Nero didn't specifically tell me the reason why, it seems that if I was doing anything with the computer the DVD would coaster. I am use to burning CDs at 600KB/sec, but this DVD burner at its middle setting does 8,000KB/sec! I also tried to burn some files with "Chinese" characters in the file names. This caused the DVD burner to go into never-never land. It was only after I renamed the files, taking out the "Chinese" characters, would it burn the DVD. I wanted a DVD burner so I could back up my files. I went in search of a file manager that would sort folders and files by size in ascending order. You think this would be a common feature, but it's very hard to find a program that has it! I found a file manager called [ExplorerXP](#) that does this very beautifully and it's also freeware. I can sort by size and then drill down to the biggest folders and files. I can also "eye ball" what I want to burn using the file manager without using a separate program. It appears that I have get the folder below 4.6 GB for it to fit on the DVD.

– Soli Deo Gloria

The Joy of Outlook PST Files

MARCH 10, 2006

CATEGORIES: TECH TIPS

Outlook PST files are the nastiest things around. In the past two days I had two users with 1.9GB PST files. According to Microsoft, Outlook XP and below use ANSI encoding which limits the size of the PST file to 2GB. Outlook 2003 and greater uses Unicode encoding which allows PST files to be up to 20 GB. What happens if you go over the 2GB limit in Outlook XP and below? All the data written after the 2GB mark is gone. You have to use a utility called PST2GB to truncate the file. How swell! The funny part about it is that PST files seem to corrupt a lot around here and not even at the 2GB mark. When a PST file corrupts and you are using POP3 as your mail setup, watch out. All the files it downloads during the corruption go into never-never land (*because POP3 downloads the messages locally and deletes them from the server. Of course, the files have no where to go*). I've never seen such a bone headed e-mail program do that. If the PST file is corrupt (*trust me, Outlook KNOWS it is corrupt, it will even tell you: "errors detected in PST"*), then **STOP DOWNLOADING THE USER'S E-MAIL!**

The user will call you with messages stuck in the Outbox folder and of course, Outlook not working. You cannot delete the messages in the Outlook folder as Outlook will tell you that MAPI32 has begun transmitting the messages. It seems that Outlook sets a flag in the message that it is being transmitted and that flag cannot be reset easily. The only way to reset the flag is to export the whole 1.9GB PST to a new file (**yes, all 1.9GB of it!**). First, however, you have to run SCANPST on this monolithic file as it is corrupt. That takes a good 45 minutes. Then you have to export it. Another 20 minutes goes by. Now you can delete those nasty messages from the Outbox folder! The fun has just begun, because you have to start deleting a bunch of messages to get the file size back down.

But wait...you keep deleting files and the size of the PST doesn't go down. Why? Because you have compact the file! You see, when you delete a message in Outlook, it just creates a blank space or record where the message was. Therefore, the size of the PST file says the same until you run a manual compaction which takes those spaces out of the file. Brilliant! The compaction alone took 3 1/2 hours!

Factor in the time of copying the PST file from the user's workstation to mine, running scanpst, running an export, deleting files from the PST file, running a compaction and copying the file back to the user's workstation, you will easily spend 6 hours or more fixing the problem!

Corporate America: PLEASE DO NOT USE PST FILES. PLEASE USE MICROSOFT EXCHANGE.

Thank you 😊

– Soli Deo Gloria

Vonage and Wireless Router Setup

MARCH 20, 2006

CATEGORIES: TECH TIPS

Tonight, I just setup Vonage on my home broadband connection. Vonage sent a RT31P2 broadband router with two phone ports. I already had an existing Linksys Wireless BEFW11S4 router. Here's how I set it up:

Existing Router: 192.168.1.1

New Router: 192.168.1.11

IP Space: 192.168.1.2-192.168.1.100

DHCP Scope: 192.168.1.200-192.168.1.254

0. Plug in the cable from the cable modem into the Internet port of the RT31P2. Power cycle cable modem.
1. Plug in a PC into Linksys RT31P2 broadband router. Set the IP of the PC to 192.168.15.2 so you can get to the IP of the router which is 192.168.15.1. Switch the IP of the PC back to 192.168.1.2 when done.
2. Change IP of router from 192.168.15.1 to 192.168.1.11.
3. Take a "straight through" (not crossover) patch cable and plug it into the uplink port (port 4) on the BEFW11S4. Make sure nothing is plugged into port 3 of the BEFW11S4 because the uplink port is shutdown when port 3 is in use. Connect the cable to any of the 3 LAN ports (not the Internet port!) This will create a "bridge" between the two routers. Also, make sure the routers are on the same subnets (both are sitting on 192.168.1.x, 192.168.2.x, etc).
4. Switch the BEFW11S4 from Gateway to Router model under the "Dynamic Routing" section so the BEFW11S4 acts like a switch. Disable DHCP on the BEFW11S4 if you have it enabled.
5. On the BEFW11S4, set the WAN connection to 192.168.1.11 and set gateway and DNS to 192.168.1.11. On the RT31P2, set it to "Obtain an IP address automatically".

If you did everything correctly, you should see your Vonage phone number under “Line1 Status” under the Status page on the RT31P2.

– Soli Deo Gloria

Pushing Out Patches Poor Man's Style!

APRIL 1, 2006

CATEGORIES: TECH TIPS

We all have heard of the Windows WMF vulnerability and the need to apply patch KB912919. Maybe you don't run WSUS or any patch management at all. Yet being the lazy administrators we are, we would rather the computer do all the grunt work instead of us. Having been assigned 80 computers to patch, I was looking for a way to do this remotely rather than run around like a mad man patching systems by hand. In order to do this we need a few things. First, we need a list of the NETBIOS names of the computers involved. No sweat here: I had inventoried all the computers I was responsible for in an Excel spreadsheet. Just save as a plain text file and it's done. Next, we need the server service turned ON, the Windows firewall turned OFF and file and print sharing INSTALLED and ENABLED on the end workstations. You'll also need the local administrator password and have the remote machine turned on. I found this batch file on the news group and modified it for my purposes. You can look at the script [here](#). To run it, you must first save the TXT file as a BAT file. Then, pass your administrator password as the second argument like this: **patchem FuNkYMonk3Y**. Finally, make sure there is a plain ASCII text file named PCLIST.TXT in the same directory that PATCHEM.BAT resides. The format of PCLIST.TXT should look like [this](#).

The batch file is pretty slick. It uses PsExec to remotely execute a file on the remote workstation using administrator credentials. The FOR loop keeps cycling through PCLIST.TXT passing each NETBIOS name to PsExec to try. There is a line that copies the file to the workstation before running it. PsExec -c should now work so you can eliminate the copy line and issue that additional parameter instead (*PsExec -c didn't work and I alerted Russinovich to that fact which he acknowledged and fixed in January 2006*).

That was pretty cool...but how do we know what computers got the patch and which ones didn't? Well, we can re-use the script above with a little tweaking. Take a look at it [here](#). Basically, it looks for presence of a \$NtUninstallKB912919\$ folder under the Windows folder. If it finds it, we assume the system is patched and move on. However, if it doesn't find it, it writes that computer name out to RESULTS.TXT. We can, in turn, rename RESULTS.TXT back to PCLIST.TXT and feed PATCHEM.BAT this list until we have exhausted the automated route. The computers that are left will have to be done by hand.

Darn, my seat was just getting warm too!

– Soli Deo Gloria

Jerry Taylor Attacks CentOS

APRIL 2, 2006

CATEGORIES: MISC

Take a look at this [thread](#). This [guy](#) works as a city manager for the city of Tuttle in Oklahoma. His ISP did some reconfiguring of their servers which caused the city's web sites to point to some unconfigured web sites running CentOS (wrong DNS records). After getting a configuration page for CentOS, he apparently started to e-mail the CentOS tech support and was threatening to call the FBI on them. I love when he states "*I have no fear of the media, in fact I welcome this publicity.*" It seems he has changed his tune and removed his e-mail address from his web site.

– Soli Deo Gloria

Winternals Sues Best Buy

APRIL 15, 2006

CATEGORIES: MISC

It seems that Best Buy entered into agreement with Winternals to demo their software, specifically, the Administrator's Pak. Winternals came to Best Buy giving training sessions to Best Buy employees, to show them how to best use the software.

Now, read the following from the [news section of Winternals](#):

*The complaint also alleges that, "at these training sessions, certain employees of Defendants approached Winternals' representatives and stated that many of Defendants' employees were very familiar with The Winternals Software and, in fact, **had already been using The Winternals Software to repair malfunctioning and 'dead' computers of Defendants' customers for some time without a license.** These employees expressed that they were glad to see the Defendants finally coming into compliance with Winternals by seeking a license to The Winternals Software."*

As we read through the complaint, things get juicier! Supposedly, Winternals went under cover and contacted the "geeks" from Best Buy to come fix their PC. Guess what they were using? Pirated copies of the Winternals software! Here's a snippet from the complaint:

"In one instance, a Geek Squad employee was videoed repairing a customer's computer using a pirated copy of ERD Commander. The copy of ERD Commander used in the videotape is an illegal, "cracked" copy of ERD Commander. This version of ERD Commander is identifiable, because the start up screen conspicuously displays the word "Gold Member" in the licensee information field next to the Winternals logo. Winternals has never granted a license to any person or entity named "Gold Member"

[This PDF lists the times, dates and names of Best Buy employees caught using pirated copies of ERD Commander](#)

– Soli Deo Gloria

Creating the Ultimate Windows XP Kiosk Machine

APRIL 21, 2006

CATEGORIES: TECH TIPS

Recently, I was presented with an opportunity to create a locked down, autologin PC running Windows XP. I had also read about the Shared Computer Toolkit for Windows XP on a recent Technet article. The [Shared Computer Toolkit for Windows XP](#) allows you easily lock down a machine through a GUI interface. No longer do you have to do ugly registry hacks! In my case, all the computer had to do was run an AS/400 client. These users had a AS/400 login, but not a network login. Best practices dictate the “the principle of least privilege”. Haha, this is going to be fun!

During the installation of the toolkit, you are prompted to download the user profile hive cleanup utility. Go ahead and do so. After installing UPHClean, re-run the toolkit setup. You are presented with several options. Let’s pick “User Restrictions”. This will lock down a specific user’s profile. That means you have to have created a user account and logged in as that account at least once (so the profile gets created). Let’s take a look at some of the options:

 User Restrictions Screenshot

There is a copious amount of features at our disposal. You can lock it down so far that the only thing the user will have is the option to run a program that you specify! There are, however, a few words of caution. Under the software restrictions section there is an option “Only allow software in Program Files and Windows folders to run”. If you are installing a program outside Program Files, be sure to NOT enable this feature. Also, under additional Start Menu restrictions, there is an option “Prevent programs from the All Users folder from appearing on the Start Menu”. That exactly where I put icons for all users of the machine, so I left that disabled.

Let’s create a kiosk Windows XP machine where I want allow users to surf the Internet and be able to do nothing else. Further assume that I have proxy server which blocks out pornographic sites. I’m going to turn off themes by stopping and disabling the themes service. Now I will login as the user I want to restrict and switch the start menu back to classic mode. I’ll also change the background to a plain blue color. I’ll rip everything off the start menu and place an Internet Explorer icon on the desktop. Make sure that the user just has read/execute rights to the icon so


they cannot modify or delete the icon. To make cleaning up the start menu easier, open up C:\documents and settings and keep deleting the items you don't want from the user's profile directory AND the All Users directory. After doing this, here is the result:



There are two folders you cannot delete because Windows XP says they are protected: Administrative Tools and Startup. That is OK though: the toolkit can disable them for the profile. The toolkit will also let us get rid of the Recycle Bin and everything else on the Start Menu. Lets lock this bad boy down and see the result:



Hahaha! Well hacker boy, where do you want to go today? Certainly no where on this locked down PC! When you hit CTRL-ALT-DEL, you are presented with this message:

Where art thou hacker boy? If we go back to the toolkit you'll notice another option: lock profile. What exactly does this do? It makes the profile a mandatory profile by renaming NTUSER.DAT TO NTUSER.MAN. Basically, any changes made to the profile will be flushed when the computer reboots. As if the user could make any changes to the profile to begin with! Let's lock the profile and continue on to the autologin potion. The toolkit does not come with any type of auto-login capability, but we don't need it to. There is a slick utility made by Tommy Mikkelsen called [Autolog](#) which will do exactly that. Before running it, go into the User Accounts icon in the Control Panel and turn off the "Welcome Screen".

This utility was made for computers running Novell, but don't worry: if you are not running Novell that is OK.



Erase the domain/workstation information. Enter in the name and password of the account you are using. Under mode, pick "Autologin to workstation, do not use E-dir". Edirectory is Novell Netware's Directory Services. Click Enable Autologin. Logout and watch the magic! Using this method is a lot better than registry hacks, because it seems the autologin portion does NOT break when you use the shift-logoff method. When you want to login to the workstation as an administrator, you hold down the left shift key and then hit logoff. It will then give you the login screen to login as yourself. After you are done and logout, the script resumes. How cool is that?

There is another feature of the toolkit: disk protection. It allows you to create a hidden partition which rolls back any changes made during the login session. Unfortunately, when I tried it at work on a Compaq Deskpro 733 MHz, it would cause the computer to freeze up when I logged in as the restricted user. Logging in as an administrator worked fine though.

– Soli Deo Gloria

Titanic Two: Jack's Back!

APRIL 29, 2006

CATEGORIES: JOKE

Jack is back!

– Soli Deo Gloria

Interesting Fun with Microsoft Access MDB Files

MAY 4, 2006

CATEGORIES: TECH TIPS

I got a call from a user today having problems opening a MDB file. It appears this file was from a government organization on the West Coast responsible for air quality control. I went to the web site the user gave me and no where does it state what version of Access you need to open the file! My user in question had Microsoft Access 2000 and was getting an error that his version was too old to open this MDB file, so I tried Microsoft Access XP on his computer and got a different error. The error I got was this:

“Microsoft Access cannot open this file. This file is located outside your intranet or on an untrusted site.

Microsoft Access will not open the file due to potential security problems. To open the file, copy it to your computer or an accessible network location.”

This was quite an interesting error message as the file was being opened from the local C: drive! Upon searching the Microsoft web site, this error message is given and the solution is this:

“This behavior can occur because an FQDN or IP address contains periods, which causes Internet Explorer to identify the Web site or share as being in the Internet zone.”

Nothing was listed in the security zones. How was I to know what exact URL it was going after to add it to the security zone? Our local GPOs prevent changing the Internet security settings, so this wasn't an option any ways. Upon searching further, I stumbled upon [this blog entry](#) that says that new features in service pack 2 for Windows XP cause this behavior. The solution is to right-click on the MDB file, select Properties and then click “Unblock”. I tried that and it worked great. Goes to show you that all error messages are not created equal.

– Soli Deo Gloria

BeyondLogic: Another Sysinternals Type Web Site

MAY 11, 2006

CATEGORIES: REVIEW

After testing the latest version of VNCSan (*which is much improved since my last entry on it... they encrypt the local administrator password now instead of storing it in cleartext*), I saw they were using beyondexec instead of psexec. This piqued my interest, so I went and did a Google search on “beyondexec” and it lead me to www.beyondlogic.org. The site looks a bit amateurish, but it has some interesting utilities on it, namely PortTalk and Trust-No-Exe. PortTalk lets legacy programs write directly to COM/LPT ports under Windows 2000/XP. I actually could of used this utility about a month ago. I built a Gateway 600YGR laptop for one of our EE's with Windows XP. He tried his EEPROM program on it (16-bit) and it was a no go. The program wanted to write directly to the LPT1 port and Windows XP doesn't allow this. I had to put Windows 98 on the laptop to get it to work.

Trust-No-Exe is an interesting concept that could be used for a kiosk type machine. Basically, it allows you to greylist the executables you don't want running and whitelist the ones you do. Getting back to beyondexec, one advantage of it over psexec is that you can issue shutdown commands to the remote system after executing your remote program. Looks like you can also send messages to the user which could come in handy.

– Soli Deo Gloria

Theme Music from News TV Shows

MAY 19, 2006

CATEGORIES: MISC

I don't know why this fascinates me, but [this web site](#) hosts the intro/ending background music (*and the stories of said music*) for major news TV shows like Dateline, Prime Time Live, 20/20, Today, etc. In fact I have the theme music on loop for Prime Time Live right now and it's driving me crazy!

– Soli Deo Gloria

Vongo is a No Go

MAY 21, 2006

CATEGORIES: REVIEW

After seeing a commercial on the service “Vongo” on TV, I decided to sign up. It’s a service that lets you download an unlimited number of movies to your PC and play them for \$9.99 a month. I picked the PPV option since that lets you browse the movie selection for free (*apparently, you cannot browse the movie list without registering, that should have been my first red flag*). Even though it’s free, they still want your CC number (*red flag number two*). They boast a selection of 1500 movies, but after seeing all of them I was quite unimpressed! I decided I didn’t like this service much and I wanted to cancel.

Hmm...how to cancel? Every reputable service has a cancel option online, but apparently not Vongo. To cancel you have to call 1-877-866-4621 and speak to someone in customer service. Excuse me? You brag about not having to drive to the Blockbuster to rent a video and how convenient your service is and I have to call you to cancel? Oh, it gets better. They store your credit card number right in their service! I wonder what the legality of doing so is without giving you the option to remove it? I mean, I had no balance: nothing, zip, zilch. Why can I not remove my credit card information? I tried to change my credit card information to another (non-active) number so they couldn’t charge me, but apparently they are pretty swift on that. It appears they crosscheck your CVV number with the issuing bank’s ZIP code to make sure they match up.

Why make it so hard to remove my credit card information? Why make canceling so hard? So off I went to cancel by phone (*I really hate having to explain myself*). I was connected relatively quickly to a customer support agent. “*Why are you canceling?*” asked the customer support person. Why should I have to explain my reasons? This is precisely why an online option is so valuable. I explained I just wanted to cancel. “*Oh, but you haven’t any charges*” she quipped. I explained her service was storing my credit card information on their service and I didn’t appreciate that. She then proceeded to cancel the account asking all of my information (*name, address, city, zip, blood type, etc*).

This is critically important...if I just let them hold on to my credit card information, what happens if they are hacked into? I have to keep worrying about them charging me for something I didn’t buy or some cracker getting my information.

I urge you to go to www.vongo.com and click on Contact Us. Tell them how crappy this policy is. Vongo doesn't own my personal information, I DO!

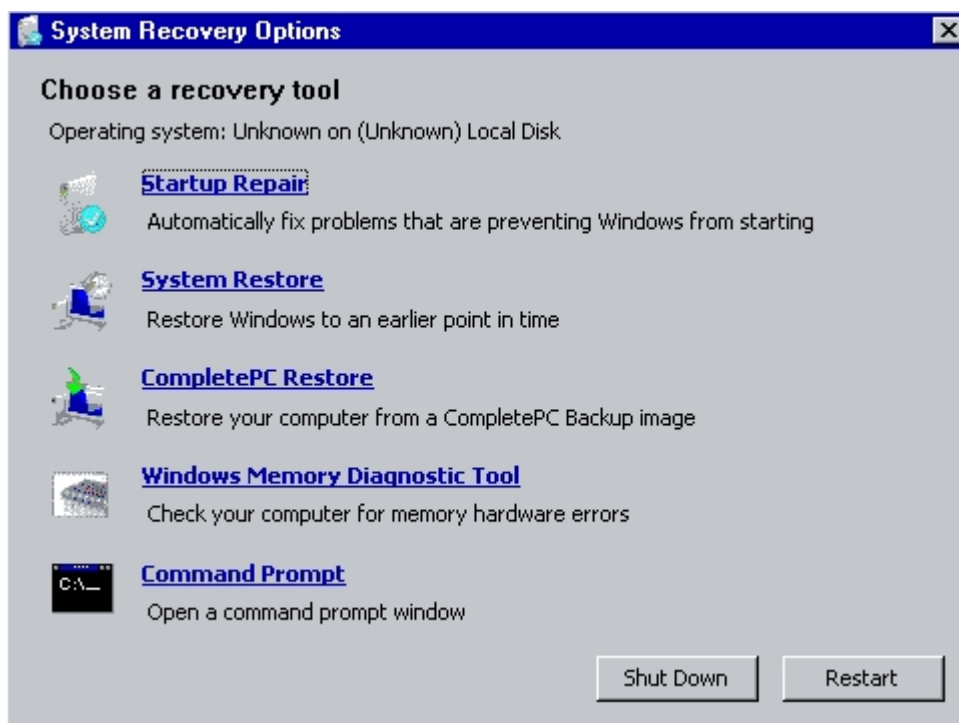
– Soli Deo Gloria

Windows Recovery Environment for Windows Vista (Build 5384)

MAY 29, 2006

CATEGORIES: OPERATING SYSTEM, REVIEW

Having access to the Windows Vista Beta 2 bits, I decided to take a look at the system recovery options. This isn't your Windows 2000/XP recovery console: it is a full blown version of WinPE or should I say WinRE. The list of options given are these:



Startup Repair – Automatically fix problems that prevent Windows from starting

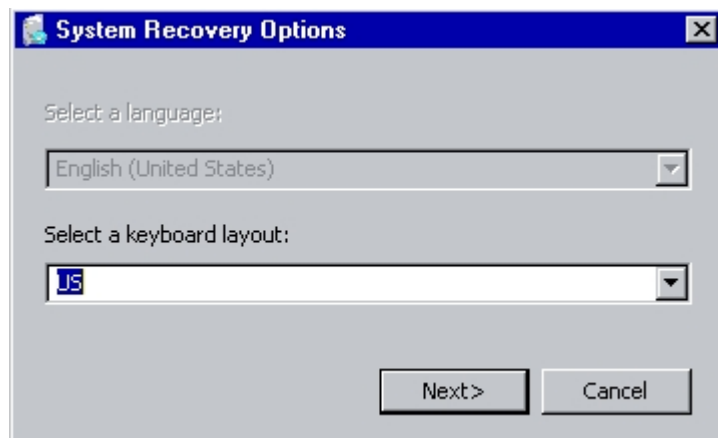
System Restore: Restore Windows to an earlier point in time

CompletePC Restore – Restore your computer from a CompletePC backup. Although this sounds exciting, it really isn't. CompletePC is an all or nothing proposition. You can backup your whole hard drive to another hard drive or burn it to DVD. However, you cannot restore individual files or folders.

Windows Memory Diagnostic Tool – Check your computer for memory hardware errors

Command Prompt – Open a command prompt window

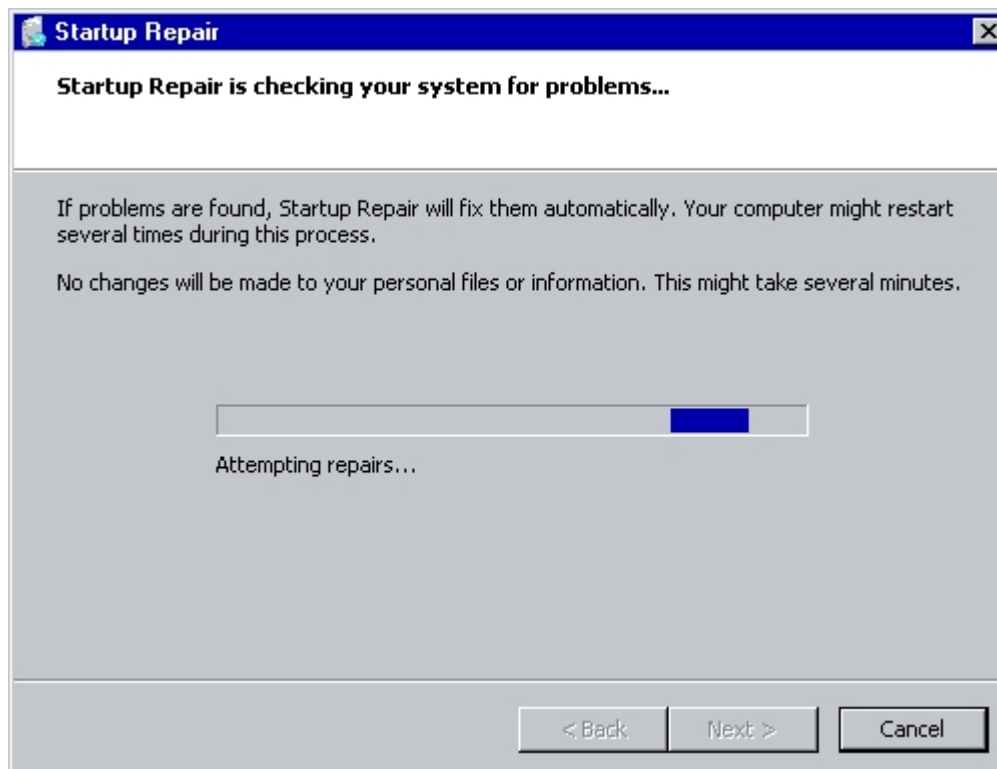
To get to WinRE, first pick System Recovery options when booting from the Vista DVD. You are then given an option to choose your keyboard:



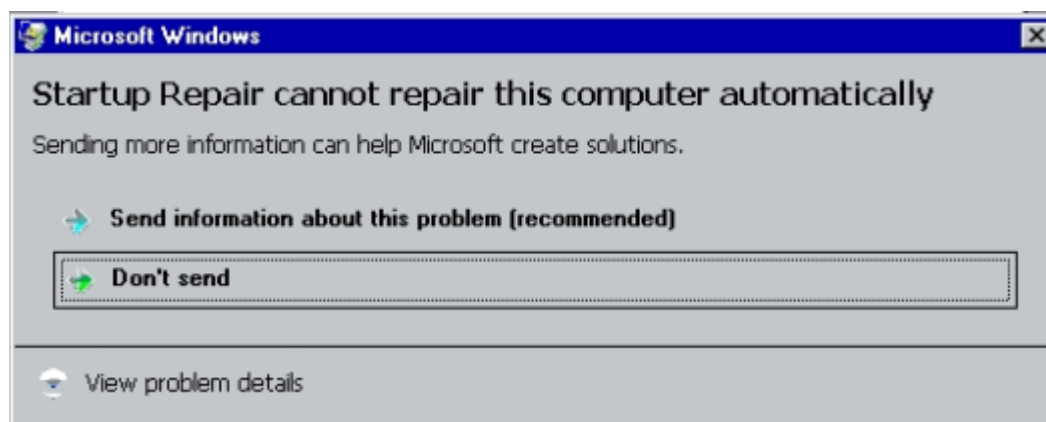
Next, it looks for Windows Vista installations. You are given an option to load drivers for your hard drives if WinRE cannot find them:



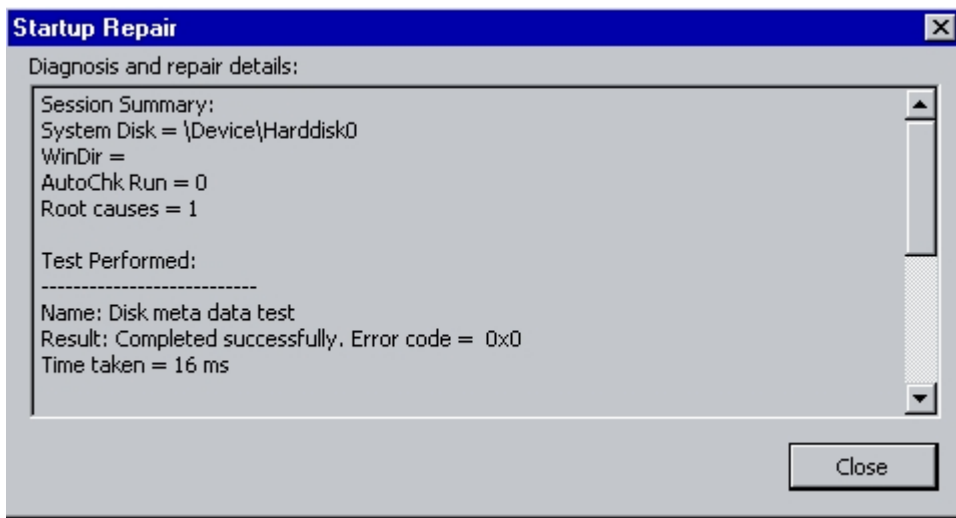
I decided first to pick Startup Repair. It states *“If problems are found, Startup Repair will fix them automatically. Your computer might restart several times during this process. No changes will be made to your personal files or information. This might take several minutes.”*



At the end, it found no problems, so it asked me if I wanted to send more information to Microsoft so they can help create solutions. You can then pick "Send" or "Don't Send".



You can view a log at the very end of this procedure. It appears to run some file sanity checks, checks the boot manager, and the event log.



System Restore: Wow, I've been waiting for this feature for 4 years! The only way that you can run System Restore in XP if Safe Mode didn't work was to get a copy of Winternals ERD Commander which runs about \$1200. Microsoft now lets you run system restore from the CD. The really cool thing is the format of the list it gave me:

5/25/06 1:12 AM (Install) Device Driver Package Install: Linksys Network Drivers

5/25/06 1:25 AM (Install) Installed Wireless Network PC Card Configuration Utility

You can see, in real time, what action was done last and reverse that option.



Memory Check – Reboots the PC and provides a comprehensive memory check. Test results are given after you log into Windows Vista. You can pick from “Basic”, “Standard” or “Extended” testing by hitting F1 when booted into the testing process.

Command Prompt – There appears at the moment that there is no “help” command and when I attempted to run explorer.exe, I got an error that shdocvw.dll wasn't found. Basic programs like notepad did work, however.

WinRE, however, leaves me rather disappointed. A GUI front end with registry editing and file copying features would make WinRE so powerful and useful, as would networking support (*my guess is that it caches the error reporting data you submit in WinRE until you boot into Windows, then offers to send it later on when you have networking support*). A crash dump analyzer and event log viewer would be really neat too. WinRE has so much potential, so hopefully Microsoft hasn't finished WinRE for good.

– Soli Deo Gloria

Windows Genuine Advantage

JUNE 1, 2006

CATEGORIES: MISC

Recently, Microsoft quietly released hotfix KB905747 which includes updates for WGA. The update now includes a wonderful “in your face” popup message if you are running a supposed pirated copy of Windows XP. I think this picture is most fitting for this situation:



It appears that a file called WGATray.exe that ties in with WGA runs all the time consuming both CPU time and memory. Microsoft, what are you doing? The interesting part of the WGA program is that if you purchase a counterfeit copy of Windows XP, you can get a legitimate one from Microsoft for free. You of course have to provide proof of purchase and the CD you bought. So, does that mean I can buy a \$5 copy from China and Microsoft will give me the \$200 version of Windows XP Professional for free? Oh wait...only “high-quality” counterfeit copies qualify for that offer. What exactly is “high-quality” anyways?

On every message board you will find MS-MVP Carey Frisch quoting links to WGA articles. Here is a message from Carey Frisch: it's the professionalism I enjoy.

From: "Carey Frisch"

References:

<#aV#1AerBHA.2344@tkmsftngp07>

Subject: Re: Video Card Size?

Date: Mon, 4 Feb 2002 19:50:55 -0600

Lines: 15

```
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Newsreader: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
Message-ID:
Newsgroups: microsoft.public.windowsxp.customize
NNTP-Posting-Host: HUBMS-ubr-24-33-9-77.midsouth.rr.com 24.33.9.77
Path: archiver1.google.com!news1.google.com
```

Q. "Try reading the post idiot!!"

*A. You called me an idiot! Shame on you for calling me an idiot. I am an
resent being called an idiot! Don't you ever, ever call me an idiot again,*



I'm sure glad Microsoft promotes those with such good manners to act as piracy watch dogs on their behalf. The great thing is that WGA is also misidentifying legitimate, honest to goodness copies of Windows XP too! Just head over to the [Windows Genuine Advantage Forum](#) and click on the subforum **WGA Validation Problems** to see what I mean.

That's not to say that Microsoft doesn't deserve to be paid, but don't punish the consumers: go after the counterfeiters! Any one swift enough with a search engine can bypass WGA. Why should someone that already purchased Windows XP once be forced to purchase it yet again while the crackers and the pirates laugh all the way to the bank? What is Microsoft doing to secure its product keys? What would prevent a cracker from going to a University and running a product key finder on a machine running Windows XP? Who's responsible for securing the product key: Microsoft or the University?

Why is the burden of piracy placed on the consumer? I can see it now: **"you must be connected to the Internet for Microsoft Windows to work. If you are disconnected from the Internet, Microsoft Windows will work in a reduced functionality mode. With the spread of WiFi hotspots and free Internet, there is no excuse not to be connected to the Internet. Microsoft Windows needs to check if your copy of Windows is legitimate every 15 minutes and report back to our servers. If we find that you are running a bootleg copy, Microsoft Windows will**

be instructed to self destruct and will wipe all of the data off all fixed media at a random time. This will be to teach you about using non-genuine Microsoft software”

Note that the above paragraph is satire, but is not too far off mark. Makers of WhereIsIt and CDRWin placed “bomb code” in their products if they detected a pirated code was be using (*WhereIsIt locks catalogs with the message “Warez user” and CDRWIN would randomly produce coasters if a pirated key was being used*). Would you like to use a piece of software that has “bomb code” in it? What if that “bomb code” was accidentally triggered? There are enough problems a computer user has to deal then having to now deal with WGA and “bomb code” (*spyware, viruses, spam, phishing, etc*).

Here’s another interesting tidbit from WGA cheerleader Carey Frisch:

```
From: "Carey Frisch"
References: <3cefd510_2@news1.meganetnews.com>
Subject: Re: How to Defeat XP Activation
Date: Sat, 25 May 2002 22:04:20 -0500
Lines: 11
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Newsreader: Microsoft Outlook Express 6.00.2600.0000
x-mimeole: Produced By Microsoft MimeOLE V6.00.2600.0000
Message-ID: <#vzdxHGBCHA.1340@tkmsftngp02>
Newsgroups: microsoft.public.windowsxp.help_and_support
NNTP-Posting-Host: hubms-ubr-24-33-9-77.midsouth.rr.com 24.33.9.77
Path: archiver1.google.com!
```

Don't be surprised that one day, upon downloading an update from the Windows that upon reboot, you cannot access your XP O/S because it was an unauthoriz version. And you'll have no legal leg to stand on. This has already happen running a pirated version of Office 2000. Download and install SP1 for Offi one can no longer open the program. And Microsoft has every right to do thi

Moral of the story: Honesty is the best policy!

--

Carey Frisch (USA)

If Carey (again, who Microsoft supports, since he is a MS-MVP) gets his way, any computer running WGA that identifies a bootleg copy will get shut down. It does not matter if WGA is correct in its judgement or not.

Update: This article is from Paul Thurrott's WinInfo newsletter dated 6/9/06:

Microsoft Concocts Yet Another Reason to Love Windows Genuine Advantage

I was sitting around the other day listing all the things I just love about Windows Genuine Advantage (WGA), Microsoft's antipiracy tool. But then I discovered a hidden WGA feature that I'd never heard about, mostly because Microsoft had kept it a secret. It turns out that WGA actually connects to a Microsoft server every time you boot your PC.

That's right. It's spyware. Microsoft actually installs a tool on your PC that does nothing more than check to ensure that you're not pirating Windows, and it does this check every single day and then sends the results back to Microsoft. This insidious behavior was first discovered by Lauren Weinstein, the co-founder of People For Internet Responsibility, and it's touched off a debate about disclosure and privacy. But seriously, this situation is ridiculous. It's bad enough that we're treated like pirates. Do we have to be spied on every single day as well?

[Link to Lauren Weinstein's blog entry on this.](#) Apparently, it's true. My satire was not too far off! Microsoft continually checks your OS and can revoke your activated status at any time!!!!

– Soli Deo Gloria

RunAs Trick for Installing Local Printers

JUNE 8, 2006

CATEGORIES: TECH TIPS

Sometimes it's the simplest things in life that get us, like not being able to use RunAs on the "Add a Printer" icon in Windows XP. Countless times I have logged off to add a printer as an administrator and today, it really bugged me. I had a user that was trying to print a JPEG file from their e-mail. Problem? If I log out and install the printer as myself, I cannot set the printer as default without knowing their password. Neither will I know if it worked logged in as them (*the user ran off to a meeting before I got there*). Well, this bugged me again so much that I did a USENET search and low and behold a little trick:

Open the Printers Folder

Move the mouse to any white area

Hold down the shift, Right Click

Note the RunAs option

There are two selections: **Add printer** and **Server Properties**.

Given by Microsoft employee Alan Morris (*who, by the way, did not know the answer right away...I feel better now*)

I think this trick is specific to Windows XP, maybe that's why I didn't pick up on it right away.

-Soli Deo Gloria

Microsoft Releases Standard User Analyzer

JUNE 10, 2006

CATEGORIES: MISC

The [Standard User Analyzer](#) helps developers and IT professionals diagnose issues that would prevent a program from running properly without administrator privileges. On Windows Vista, even administrators run most programs with standard user privileges by default, so it is important to ensure that your application does not have administrator access as a dependency.

Using the Standard User Analyzer to test your application can identify the following administrator dependencies and return the results in a graphical interface:

- File access
- Registry access
- INI files
- Token issues
- Security privileges
- Name space issues
- Other issues

My first impressions are that the program is a bit confusing to use (especially interpreting the cryptic results) and using Regmon/Filemon still seems to be the gold standard for IT professionals to find permission issues. This tool seems geared more towards program developers.

– Soli Deo Gloria

The Master of Spyware

JUNE 18, 2006

CATEGORIES: SPYWARE

Ben Edelman has a PhD in Economics from Harvard. Yet, he likes writing on spyware and how it infects systems. His reports are very detailed and interesting. He even has full videos of how spyware infects a system. Check him out at www.benedelman.org.

– Soli Deo Gloria

Support XM Radio

JUNE 20, 2006

CATEGORIES: MISC

The big record companies are pressuring Congress to pass legislation that would prevent XM listeners from having access to more music choices and new technologies. To learn more about how you can help stop this legislation, follow the link above.

Click on this URL to take action now

<http://capwiz.com/xmradio/utr/2/?a=8852001&i=80549823&c=>

If your email program does not recognize the URL as a link, copy the entire URL and paste it into your Web browser.

While you are at it, please support the [EFF](#).

-Soli Deo Gloria

A Tale of Active Directory on Campus

JUNE 25, 2006

CATEGORIES: TECH TIPS

An [interesting blog made by David Carlin](#) about real life problems he has run into with Active Directory and how he solved them.

-Soli Deo Gloria

Vincent Ferrari Tries to Cancel his AOL Service

JUNE 25, 2006

CATEGORIES: MISC

[Interesting video of Mr. Ferrari trying to cancel his AOL service.](#) And yes, I've heard simliar stories such as his.

[Full \(uneditted\) audio version](#)

– Soli Deo Gloria

Attack of the 16-bit App

JULY 1, 2006

CATEGORIES: TECH TIPS

Recently, I was given the task of upgrading some Windows 95 machines in our company to Windows XP. One user on Windows 95 was using a 16-bit application called Advanced Gage Calibration. This program is used to calibrate machine tools. Upon copying to Windows XP and launching the program, it complained about missing files. Upon loading trusty Filemon, I determined it needed VBRUN300.DLL along with some other DLLs. After copying over all the files flagged by Filemon, the program was still giving a “BTREIVE: File not found error”. This was quite curious as Filemon showed it wasn’t hitting any missing files.

Having experience with BTREIVE in the past, I knew it was an ODBC driver which interfaces a program with a database. I was going in circles on Google trying to find a BTREIVE installation program (a hex dump of WBTRCALL.DLL showed it was version 5.11). I took a step back and took another look at the Filemon log. Before loading any of the files, the AGC program reads C:WINDOWSWIN.INI. WIN.INI is the forerunner of the Windows 9x/NT Registry. Back in yesteryear, programs use to store their program data in WIN.INI and SYSTEM.INI. I remember tinkering with Gator, a 16-bit text editor, back in 1993. The trial version would store its trial “countdown” data in a secret section in the WIN.INI file. Even after uninstalling and reinstalling Gator, it would know how many days you used in their trial period because of this section. Upon looking at the WIN.INI file on the Windows 95 machine, I discovered this:

OPTIONS=/m:63 /p:4096 /f:40 /l:60 /u:5

TASKS=50

This must pass certain options to BTREIVE to read the data. One of the errors was a subscript error, so some of these options must tell BTREIVE the “index” and “boundaries” of the database. The other interesting thing was this text string in the hex dump of WBTRCALL.DLL: “Btrieve V5.11 DLL for MS-Windows **Beta Version**“. Beta version? Why would you sell a program with beta drivers? Yikes!

– Soli Deo Gloria

Sysinternals Video Set

JULY 7, 2006

CATEGORIES: MISC

Sysinternals is about to release a 6 DVD series on various topics, all of which interest me! For a limited time, they are offering them at a discounted rate of \$299. When they are finally released, the price jumps to \$399. Take a look [here](#): you can see they have a 49 minute video for **FREE** to download on their web site! After looking at the newer versions of the Sysinternals utilities, it appears they are also restricting the use of these utilities in a corporate environment. If you use them in a corporate environment you have to get a license. A EULA now appears for each program the very first time you run them on a new PC.

Older versions of the Sysinternals utilities do not have this EULA, so if you need to use these in a corporate environment and don't want to get a license, I suggest finding older versions which do not have this EULA. (*Note: although I have these older versions, the EULA of these older versions forbid me from distributing them to anyone*).

The other interesting part of this video is that Mark indicates that Filemon and Regmon will be merged into one tool called Process Monitor.

– Soli Deo Gloria

Missing Network Connections

JULY 12, 2006

CATEGORIES: TECH TIPS

After packaging a MSI file to remove the Novell client, we discovered that the MSI file wiped out all the adapters in the Network Connections applet. Eek! After trying countless articles at Microsoft, I discovered that deleting the Config value under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network** and then rebooting the system returned all the adapters back into Network Connections.

– Soli Deo Gloria

Virtual PC 2004 is Free!

JULY 12, 2006

CATEGORIES: MISC

[Virtual PC 2004 is now free and can now be downloaded from Microsoft's web site here!](#)

– Soli Deo Gloria

LiteOn DVD Burner SOHW-1693S Dies

JULY 16, 2006

CATEGORIES: MISC

What a bummer...didn't even make it through a 50 pack of DVDs. My LiteOn DVD burner died today...would burn part way through the disc and then start spinning out of control. The drive was 8 months old: very disappointing. Newegg.com does have a cool RMA program where you can send the unit back to them (*you have to pay shipping their way*) and they will repair the unit under the manufacturer's warranty. Better than nothing I guess! I've ordered a Pioneer DVD burner in the mean time: model DVR-111D. Let's hope this one lasts more then 8 months!

– Soli Deo Gloria.

Winternals Gets Scooped Up by Microsoft

JULY 21, 2006

CATEGORIES: MISC

Bruce and Mark are heading the way of Microsoft. Microsoft now owns Winternals and all its assets. I predict that this will be a very good thing in the long run. Give people a taste of what Windows PE can do with Vista and then turn around and sell them something that actually works with the Winternals Administrator Pak.

OK, now time for conspiracy theories! You'll remember back on April 15th of this year that I blogged about Winternals building a case against Best Buy for pirating the Winternals software. If you try my link in my blog entry to the evidence, it doesn't work anymore (*although the story about the lawsuit is still on the Winternals site*). Mark announces Best Buy and Winternals came to a settlement on July 10th. Microsoft bought Winternals on July 18th. Coincidence? I think not! You'll remember that Best Buy and Microsoft were big buddies with their MSN program starting in December of 1999. Microsoft went to bat with Best Buy in October of 2002 to strike a better deal. With this settlement, Microsoft gets licensing fees for all the stores of one of the country's largest retailers. Sounds like Microsoft finally got the deal they always wanted. 😊

Just consider this...Best Buy was rumored to have been developing their own version of the ERD Commander based on the free version of BartPE. BartPE was definitely cutting into Winternals profits and with WinRE in Vista coming to the masses in January 2007, it doesn't take long to see that Winternals would be in some seriously hot water next year. Very smart move on Microsoft's part in saving the company! Mark Russinovich is the kind of talent that Microsoft needs. Hopefully, all the utilities that Russinovich has been working on getting automatically built into the OS.

– Soli Deo Gloria

Windows Hang and Crash Dump Analysis

JULY 29, 2006

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Given by Mark Russinovich at TechEd 2006. You can download from my web site [here](#).

– Soli Deo Gloria

Fun with SMS 2003 OSD

AUGUST 1, 2006

CATEGORIES: OPERATING SYSTEM

I've been playing around with Microsoft Systems Management Service (SMS) 2003 because there was talk of implementing at my company, even the OSD part! OSDFP is the OS Deployment Feature Pack for SMS 2003 SP1. Basically, it uses the management forces of SMS to upgrade existing computers with ease. For example: you can upgrade a Windows 2000 to Windows XP hands free, having SMS 2003 migrate all the user profile data. This does require a fair amount of work on the back end, but in the end it will save you lots of work! You can also do "bare metal" and "replacement" scenarios all from a Windows PE CD.

The first task in using the OSD is creating a Windows PE CD. This is pretty much done for you, except you have to provide the network drivers. As you know, I'm quite lazy and rather not have to download, extract, simply and organize the drivers myself. Let's go find someone that has already done this for us! We want the [Ultimate Boot CD 4 Windows Drivers](#) by LittIBUGer. Now, the OSD PE wizard expects all of the *.SYS/*.DLL/*.INF to all be in one folder with NO subdirectories. Unfortunately, the driver pack extracts with a full folder structure. We can get around this by zipping up the whole folder structure with ZipCentral. Now extract the ZIP file, but tell the program not to preserve the folder structure. When it asks if you want to overwrite files, say yes to all.

Drivers names for different NICs are pretty unique, so you will be pretty safe here. Viola, you now have support for at least 25 different NICs! You didn't even have to break a sweat!

– Soli Deo Gloria

Blog Face Lift and Pickles!

AUGUST 2, 2006

CATEGORIES: JOKE, MISC

Tonight, my blog got a face lift. I picked a theme that added more screen real estate and I split up my posts into different categories. I hope you enjoy it. While you are enjoying it, [watch this girl get scared](#) whenever some one comes at her with pickles. I promise you will laugh!

– Soli Deo Gloria

Watercooling: Never Again

AUGUST 5, 2006

CATEGORIES: MISC

This weekend I attempted to install a watercooling kit from Danger Den, kit 4200. Took me about 3 hours to strip everything out of my PC and get the water blocks mounted. I turned it on and it was alive! Today, I wake up and start putting all my cards back into the system and boot it up. I moved my DVD drive up one bay to make room for the coolant reservoir. Now the IDE cable doesn't reach to the motherboard. Drats! I head to Best Buy to find a IDE cable. They only have one for \$22. Give me a break! So I head to CompUSA and find one from Belkin for \$35. You kidding me? I luckily find a conductor 80 CompUSA brand for \$10: now that's more like it! I come back home to find coolant all over my desk! Eek!

The coolant smells really bad too (***I mean really bad***) and it is sticky! I find the leak on the CPU block and try to fix it: no go. Eventually, my whole computer stops booting because the coolant is dripping into my AGP port and this type of coolant is not conductive. I really get tired of this, so I yank the cooling system out which made a bigger mess.

In the process of taking the waterblocks off, I managed to bend the pins on my CPU. Eek! The waterblock came off so easily on the GPU that I tried the same trick on my CPU and it failed badly. Had to go to Newegg on my spare PC and order up another CPU.

It's been 6 hours since I eaten, so I better go eat before I get sick. Watercooling? **NEVER AGAIN!**

– Soli Deo Gloria

Finally Back Online!

AUGUST 11, 2006

CATEGORIES: MISC

After getting a replacement CPU from Newegg and popping it into my system my computer still wasn't working! System would power on for 2 seconds and then power off. I stripped it to bare bones and still got the same thing. I ripped another power supply out of my test box and again it would only power on for 2 seconds. As I pulled the cards out, I noticed each had coolant on the contacts. The sockets must be soaked with this nasty stuff. Any ways, I had an Asus motherboard overnighed from Newegg and I'm back online! The fix I have posted for the STOP 0x7B error message in the HOW-TO section works quite nicely for motherboard exchanges.

Update: Not quite up as I thought ..3 hours after assembling the system the AGP card took a crap. Switching it with an older Geforce 2 MX 400 worked, so I went to CompUSA and got a cheapo Geforce 5200FX card. However, that doesn't work after POST, so I had to put the older AGP card in. Both cards work in other systems?! I'm going to try a PCI card from Newegg and see how that goes!

This week at work I played with Windows Vista with the AIK (Automated Install Kit) and WDS (Windows Deployment Services). I actually got Windows Vista to push down via PXE boot in my test lab. Even got a partial unattended setup going via PXE, but as soon I as used the System Image Manager to script in an addition of a local admin account, the image now bombs towards the end of the image download.

– Soli Deo Gloria

Installers Gone Wild

AUGUST 14, 2006

CATEGORIES: TECH TIPS

OK, so the title isn't as exciting as "Girls Gone Wild", but at least I tried. The company I work for as recently started to upgrade all of our machines from Office 97 to Office 2003. Did you say quantum leap? Thankfully, most of the Office 2003 suite (*which I will refer to as O2K3 from this point*) handles most of the old Office 97 formatted files quite nicely. That is except for Access 97 and earlier databases. Microsoft Access is a funny thing. When you have a Access 97 database, everyone that uses that database must use Access 97. If you try to open it in Access 2000 and convert the database to the 2000 format, no one with Access 97 will be able to read the database. To top it off, not all databases can be converted to the new version. Since we are talking about a database that could have been created up to 9 years ago, anyone who worked on the database is probably long gone from your company (*the IT field does have a high turnover rate...a joke I once heard was that if you were at a company for more than a year you were an IT veteran!*).

For the O2K3 install, we are using a custom transforms file which removes the previous versions of Office, then installs O2K3 with certain settings defined in the transforms file, such as macro security settings. On one machine in HR, they were using a Child Support Database from the state. This database needed Access 97 to work. I decided to let our custom installation script run and install the whole O2K3 suite. I then was going to remove Access 2003 and re-install Access 97. I did just that and when I tried to open the database it seemed to worked fine...until 3 days later. There is a import function in this database which pulls in a CSV file which contains the amounts of child support that is to be paid per employee. The problem is that when the HR person hit the import button, she was getting a "**3170: Couldn't Find Installable ISAM driver**". Gulp! I looked up this error message and followed the instructions from Microsoft's knowledgebase, but this did not work unfortunately. I was kind of in a panic, because we have 5 days to submit these payments to the state. I called the vendor and he stated he could snail mail me a newer version of the database. I asked if he could send it electronically because I was in a pinch and he stated no.

The only saving grace was that it appeared that the tech that originally installed the program had copied the installation CD to the hard drive. The problem was that this installation was missing files and it kept trying to go to a D: drive. Why was it trying to go to a D: drive? That's where the installer assumed (*incorrectly*) I was running the setup program from. How do we fake

out the installation program so it thinks it is running from D:? First, we need change the drive letter of the CD-ROM drive from D: to something else. We can do this by right-clicking on “My Computer”, go to “Manage” and then click on “Disk Management”. Locate the CD-ROM, then right-click it and choose “Change Drive Letters and Paths...”. Choose a drive letter not used. Now comes the fun part! We need to trick the computer so it thinks that these files are on D:. How to do that? Well, my friend, this is where MS-DOS skills come in quite handy. There is a program called SUBST that first appeared in MS-DOS 3.1. This maps a drive letter to a path or re-routes requests for a drive letter to another one. My guess is that SUBST was created because very early programs were hardcoded to run from an A: drive. Hard drives weren't supported until MS-DOS 2.0, so this theory stands up nicely. SUBST still comes with every Windows version, including Windows XP. Enough history, we can do this from a command prompt:

subst D: C:setup

Any requests for D: get re-routed (*unknowingly to the program*) to C:temp. When you are done, just issue “subst D: /d” and it deletes the D: drive. You can then use “Disk Management” to change the drive letter of the CD-ROM back to D:.

Now back to this “installer gone wild”. I had made a copy of the setup program and placed it on my hard drive. I got it to the point where the install was now working, however when I ran the uninstall portion, the setup removed some of the setup components! Once you uninstalled the program you couldn't reinstall it. Again, this is sloppy programming. The programmer probably assumed that the setup routine would run from read-only media, so why not try to remove everything? I copied the files from the user's back to mine and re-installed and viola the import function worked on my PC! I performed the same steps on her PC and got her up and running.

– Soli Deo Gloria

Windows Continues to Dominate

AUGUST 15, 2006

CATEGORIES: MISC

Interesting article from Paul Thurrott's WinInfo Newsletter Today:

OneStat: Windows Continues to Dominate

Microsoft's next-generation OS, Windows Vista, continues to be horribly late, but that hasn't stopped the current version, Windows XP, from dominating the OS market. Web analytics company OneStat.com says that XP is responsible for almost 87 percent of all Web usage, while all Windows versions combined account for 97 percent of Web usage.

"Microsoft's Windows dominates the operating system market with a global usage share of 96.97 percent," OneStat.com reports. "The leading operating system on the Web is Microsoft's Windows XP with a global usage share of 86.80 percent. Microsoft's Windows 2000 has a global usage share of 6.09 percent and is the second most popular OS on the Web."

You read that right. Windows 2000 is the second most often used OS on the Web, with almost three times the usage share of all Macintosh versions combined. During an event keynote last week, Apple CEO Steve Jobs was quick to point out that Mac OS X was "gaining market share," but Apple has made only concrete gains in very specific markets, such as "retail sales of notebook computers in the US." In reality, Mac OS X usage is still below 2.5 percent worldwide. Even the 8-year-old Windows 98, with 2.68 percent of the market, accounts for more users than OS X does.

Many had expected Apple's recent successes with the dominant iPod MP3 player and the move to Macs that use Intel chips to increase the company's share of the OS market. That hasn't happened yet, although it still could: With Vista not scheduled for general availability until early 2007, Apple has an opening during which it can sell Mac OS X systems to Windows converts while pushing its next-generation OS, code-named Leopard.

According to OneStat.com, the following are the most frequently used OSs on the Web in the world:

1. *Windows XP* – 86.80 percent
2. *Windows 2000* – 6.09 percent
3. *Windows 98* – 2.68 percent
4. *Macintosh/ Macintosh Power PC* – 2.47 percent
5. *Windows Me* – 1.09 percent
6. *Linux* – 0.36 percent
7. *Windows NT* – 0.24 percent

– Soli Deo Gloria

DirectX Out of Memory?

AUGUST 25, 2006

CATEGORIES: TECH TIPS

Here's an interesting problem that stumped two techs before the problem got routed to me. It seems that one of our sales people was running a program that utilized DirectX. Unfortunately, when they loaded the program none of the DirectX graphics would come up. In addition to this, **dxdiag** would come back with an "Out of Memory" error message. This was quite interesting as this Dell (GX280 I believe) had 128 MB of video memory and the program ran fine on two other Dells within the same department. The proverbial task of updating the video drivers and reinstalling DirectX was already done before I hit the seat. My plan of attack was to use a DirectX uninstaller (*3rd party...Microsoft doesn't want you uninstalling DirectX*) and then use the full 52 MB version of Direct 9.0c I downloaded from the Internet (*veruses the lite web version*).

Upon looking at the Device Manager of the affected PC, I saw a device under video adaptors named "Webdialogs Mirror Driver". Hmm...we don't use anything like that on the image. I promptly removed the suspect driver and lo and behold: DirectX was back up and working again!

After returning to my desk, I decided to check out this Webdialogs thing. Turns out its some type of conferencing software. Makes sense: sales reps conference with their customers all the time. Usually, a mirror driver on a PC allows a remote user to see your desktop. Perhaps he was working with a vendor on a issue on his local PC and offered the vendor to remote into his PC (*interesting security implications here*).

Remember the principles of K.I.S.S.: Keep It Simple Silly

– Soli Deo Gloria

Microsoft Windows Vista Pre-RC1

AUGUST 30, 2006

CATEGORIES: MISC, OPERATING SYSTEM

Microsoft has changed a few things since the days of Windows 2000/XP beta testing. RCs or Release Candidates usually came within days of RTM (*Release to Manufacturing*). From various articles, it seems Vista RC1 will come to us on September 7 and the final version will be released in November! There are some really nice features in Windows Vista. Running as standard user is **MUCH** easier in Windows Vista. With UAC turned on, even administrators run under standard mode. If you need to do an action that requires administrative privileges, a login box comes up for you automatically. Previously, things such as changing file permissions or changing network properties under standard user mode were impossible, even with RunAs. Not so with Windows Vista.

The WIM format is very cool...I made my first custom image a few days ago. My articles on making hardware independent images will become a thing of the past. Windows Vista also comes with really nice driver support in the box. I was able to make a WinPE image capture disk and did not have to provide network drivers for it at all.

However, there are a few things I don't like. Windows Defender seems to prevent anything that is not "classified" from running from the Run key in the registry. Even logged in as administrator does not allow me to override this. Speaking of the administrator account, Windows Vista disables that by default! I guess this is some security wizard's dream, but in reality anyone with two brain cells can figure out what the administrator account is by looking at the account SIDs (*the administrator account always ends in SID -500*).

The boot loader also looks daunting, with replacement of NTLDR and boot.ini. The only way to edit the boot configuration is with a command line program called bcdedit. If you want to backrev to XP/2000, you have to use bootsect from the Vista DVD with specific command line switches.

– Soli Deo Gloria

Outlook 2003: Preparing to Install

SEPTEMBER 2, 2006

CATEGORIES: TECH TIPS

Wow, talk about an annoying problem. I used System Restore on one laptop to restore its state back 2 months to fix a wireless issue. We had upgraded everyone to Office 2003 and this System Restore put Office 2000 back on. No worries, just upgrade it to Office 2003 again. However, after doing so the user would get a **“Preparing to Install”** prompt on each message they clicked on. I proceeded to rip Office 2003 off and do a complete install. No go. I deleted the Outlook profile under the Mail setup icon in the Control Panel and the Outlook branch in **HKCU\SOFTWARE\Microsoft\Office\11.0**. Clean and pristine as it could be and the blasted **“Preparing to install”** prompt kept coming back like the plague.

The solution was the [Windows Installer Cleanup Utility](#). It seems that some part of Office 2000 was still installed and had attached itself to Outlook 2003. Everytime I launched Office 2003, Office 2000 stepped in and tried to heal itself. Of course the prompt doesn't say what is trying to install which makes troubleshooting this clear as mud.

– Soli Deo Gloria

More Spyware Fun

SEPTEMBER 13, 2006

CATEGORIES: SPYWARE

Countless articles could be written on spyware. Recently, I ran into [Troj/LdPinc-LZ](#) on a PC. The really bad part is that Spysweeper didn't detect this piece of malware even with the latest definitions! I am therefore recommending that you use [Ewido](#) as the software can be used passed 30 days (*the real-time protection will get disabled if you don't register it, but you can still use the on demand scanner*). The trial version of Spysweeper won't even clean the malware off your PC anymore and will shortly be removed from my web site.

The symptoms were actually quite interesting. When the user went to CNN, Internet Explorer would just crash. When the user went to a specific realtor site, the whole computer rebooted! Very little information exists on [mssync20.sys](#), but by booting into safe mode and deleting all the mssync files from C:\windows\system32, I cleaned the little bugger off. It appears from the event logs it was also trying to load as a service and failed, so if you happen to get infected with this pest, make sure to check your services for a mssync20 service. After trying to load Spyware Blaster, it complained it couldn't find MSINET.OCX. The spyware must have kicked this file out of C:\windows\system32, so I connected to my machine and copied it back over and life was good again.

Upon my searches on Google about spyware, I found some interesting articles. [This one by Michael Horowitz](#) goes through a nice series of steps when dealing with malware. He mentions the fact that the new version of Bagle actually has a trick to disable Safe Mode on PCs by deleting the SafeBoot key in the registry! This is explained in more detail at [Didier Steven's WordPress blog](#), with yet another link to [Chris Quirke's web blog](#) on how to boot with BartPE to restore the Safeboot tree.

– Soli Deo Gloria

Weird AI Music Videos

SEPTEMBER 22, 2006

CATEGORIES: JOKE

These are so funny!

[Don't Download this Song](#)

[White and Nerdy \(parody of Ridin' Dirty\)](#)

Grats to Dan Puza for forwarding these onto me!

-Soli Deo Gloria

Spyware: The Never Ending Story

SEPTEMBER 22, 2006

CATEGORIES: SPYWARE

Those spyware boys are getting smarter! Recently had a remote laptop user that kept having his home page hijacked by www.securitynetpage.net even though the home page in Internet Explorer was set to our company web site. Autoruns showed no suspicious BHOs. After poking around in the registry and finding nothing, I took a look at the Internet Explorer Addins and lo and behold: `isaddon.dll`. Sounds important, doesn't it? Appears to be related to some SmitFraud spyware.

Here's one of the prompts from the web site. The user in question thought he was infected:



Note the spelling mistakes. A lookup of the domain name on www.whois.sc shows that the web site is blacklisted by many other sites.

I found another useful site for slamming down spyware: Jotti. You know those little pests like to randomize the filenames so you cannot find them via Google? Well, you can submit a suspicious file to Jotti and it will tell you what it is!

Just for the record: I again recommend you use Ewido for cleaning off spyware. You can install and run it within Windows PE: it does work.

– Soli Deo Gloria

F for Dell Tech Support

SEPTEMBER 29, 2006

CATEGORIES: MISC

Has anyone called Dell Gold Technical Support recently? Well, I have and let me tell you I am very disappointed in their technical support. Last week I called about a laptop not powering on and I was asked if I “rebooted it”. Hello, it’s not getting power! Just today my co-worker and I diagnosed bad memory in one of our new Dell machines. Here’s the Dell tech support excerpt:

09/29/2006 08:21:04AM PC Tech: *“We were having problems while booting the PC so we ran Dell Diagnostics and we received the following system memory error codes: 2F00:0B1C & 2F2F:0119.”*

Agent (GTSR Dell Rep): *“has any additional troubleshooting been performed on the system?”*

Now I ask: what additional testing would you do? What if I was Joe Customer calling about this problem? Joe Customer will not likely even run the diagnostics CD. However, Dell usually will not talk to you without you first running the diagnostic CD. We did that. When we moved the hard drive to another PC it worked fine and suspected memory even before running the test (random BSODs are usually memory related)

09/29/2006 08:27:57AM PC Tech: *“Yes. The error code first told us that there was a system memory failure on DIMM_3 so we removed that stick of memory and ran the diagnostics again. We again received the same error code on the data bus stress and a very similar error code on the MATS test”*

09/29/2006 08:31:27AM Agent (GTSR Dell Rep): *“do you have any memory from a know good system that we could try out”*

Again, I have to wonder if Joe Consumer has memory just lying around his house for Dell to test with, but OK, we do this to make the call center person happy.

09/29/2006 08:47:48AM PC Tech: *“I am running the test right now with the new memory and have not encountered any errors. We put the bad memory into a known good system and the operating system blue screened and crashed.”*

09/29/2006 08:48:45AM Agent (GTSR Dell Rep): *“how long did it take before it errored out in the diags?”*

You have to wonder if this guy is for real or not. If your Dell diagnostics CD is throwing memory errors and the OS on the machine keeps BSODing from a fresh Ghost image, what difference does it make when it crashes?

09/29/2006 08:50:35AM PC Tech: *“I was receiving the error in the Data Bus Stress test, which is the first memory test.”*

09/29/2006 08:51:27AM Agent (GTSR Dell Rep): *“how is it running now?”*

Amazing, just amazing!

09/29/2006 08:55:02AM Agent (GTSR Dell Rep): *“ok what i will do is replace the memory on the system”*

35 minutes after initial contact, he finally decides we are worthy of a memory replacement.

09/29/2006 09:05:14AM Agent (GTSR Dell Rep): *“still here thank you for your patience”*

09/29/2006 09:09:31AM Agent (GTSR Dell Rep): *“I have setup a parts-only dispatch. You may find a return airbill in the box if the part needs to be returned. If that is the case, replace all of the parts and affix the airbill to the box. Then you will need to call 1-800-CALL-DHL to have the box pic”*

It takes him another 15 minutes to enter the order the part in the system. Overall, it took us 50 minutes to get a replacement of two faulty DIMMs.

Which leads me to this: if Dell wants to play this game, we can play it right along with them. We'll say we did so and so and got so and so result just to make them happy, but we won't do it. **Dell: give technicians credit for having above average intelligence when it comes to computers! When we say the memory is bad and we ran your diagnostics to prove it, please just replace the memory.**

Speaking of help desks, checkout [The Chronicles of George](#). Sort of mirrors what I have had to deal with in the past. 😊

– Soli Deo Gloria

Paragon Partition Manager 2005 for Free

SEPTEMBER 30, 2006

CATEGORIES: TECH TIPS

Expires October 4th, 2006!

[The Link!](#)

Windows Vista – Build 5728

OCTOBER 2, 2006

CATEGORIES: OPERATING SYSTEM

We are only a month away from Microsoft finalizing the Windows Vista bits. Consumers won't see it until January 2007, but I will be running before then to get a jump on everyone. 😊 For the first time, I attempted in-place upgrades with Windows Vista Ultimate over Windows XP Pro. The first experience was very horrible: the setup program failed to identify all the incompatible programs on my test system such as the SMS Agent, Track-IT! Remote Control Agent and VNC server until AFTER the setup was completely done. The in-place upgrade also takes forever. On a Dell GX520 with a standard build it took around 2 hours! Let me also state that you should NOT run Windows Vista with anything less than 1GB of memory. On a fresh build with just Office 2003 and the AS/400 client, the task manager showed 0MB available of physical memory and there was heavy hard drive thrashing.

We've also experienced some serious issues with Outlook 2003 not playing very nicely. On Windows Vista RC1 (*and the build before*), Outlook 2003 would eventually hang on start up. No amount of uninstalling and reinstalling Office 2003 would get it going again. If we deleted the Office key in HKCU, Outlook 2003 would work again, but for only one start. Office 2007 never seemed to have a problem on Windows Vista surprisingly.

Windows Vista x64 currently lets you disable driver signing, but Microsoft says they will remove that feature in the final release. I suspect that someone will develop a "crack" for this: who wants to go out and buy all new hardware just so the drivers are signed?

– Soli Deo Gloria

Microsoft Software Protection Platform

OCTOBER 7, 2006

CATEGORIES: MISC

The Microsoft PR department is gearing up for the software pirates. Released on 10/3/06, [this document describes Microsoft's new anti-piracy efforts](#). BSA is quoted in the document stating "35% of all software installed worldwide is pirated or unlicensed". Exactly how that it determined is beyond me (*that's liking quoting population numbers without taking a census*). Microsoft also explains its new program called the Genuine Software Initiative (GSI). It wants to make sure its customers have genuine Microsoft software. The original name of the program was the Microsoft Cash Grab (MCG), but that didn't sound as sexy so they changed it.

In terms of Windows Vista, users have 30 days to activate their operating system. After 30 days, the system goes into a locked down state where-in Windows Defender updates are turned off, Aero Glass is disabled, ReadyBoost is disabled and the only thing you use is Internet Explorer for 1 hour. After one hour, the system locks you out. You cannot even log into safe mode! In addition, if Microsoft detects that your copy of Windows is not genuine (*through WGA, see my earlier article*) all of these features listed above (*except for the Internet Explorer part*) are disabled immediately! The other interesting fact is that Windows Vista will run 14 days if you do not enter a product key. I guess this is to allow people to test out the operating system to see if they like it.

Volume licensing has also changed dramatically. No longer can you input a key to get around product activation. There are now two types of VLKs: KMS and MAK. MAKs or Multiple Activation Keys are pretty much like the old VLKs, except that you must activate the copy of Windows. However, once you activate a MAK over the Internet or telephone, it stays activated. A MAK is only allowed a certain amount of activations. For example: during the beta program our MAK was allowed 100 activations. That means we can activate 100 copies of Windows Vista Enterprise on 100 unique PCs. That means if a MAK leaks, Microsoft proactively plugs the hole by blocking the 101st activation from happening.

KMS or Key Management Service works by having one copy of Vista activate all the others. This assumes that the other Vista clients are "well connected" to the KMS (*think "LAN"*). This model also requires 25 physical machines before the service kicks in (*don't bother with virtual machines: someone tried it in the beta program and found it doesn't work*). Every 180 days, each copy of Vista must report to the KMS at least once, otherwise it deactivates itself.

Key finders won't work with KMS, because the product key is protected in the trusted store of the KMS. However, key finders should still work on machines with a MAK.

Looking back on Windows XP piracy, we saw that pirates actually figured out the key algorithm to making Windows XP product keys. Microsoft plugged that hole by checking product keys against its database to see if they were ever generated by Microsoft (*only keys with a resulting PID of 640 could actually be Microsoft generated*). This time around its my guess that pirates will be using legitimate product keys and then use "time-cracks" to get around activation time limits. For example: when Windows XP first came out, pirates just came out with an activation reset crack. Since you have 30 days to activate Windows XP, that meant you just had to reboot once every 30 days. Grab a product key from MSDN and now you have 60 days.

How do you get legitimate product keys? By illegitimate processes! Think of credit card fraud to get legitimate product keys. Think of spyware and viruses that already port cookie information back to 3rd party servers. How much more would it be to grab a 25-character product key from your copy of Windows Vista?

Suffice to say, those pirating bad boys have nothing to do, but crank on Microsoft's anti-piracy schemes day and night. It's not a question of "if" Windows Vista's copy protection will be broken, but "when". While you are chewing on that, you might want to check out a [paper I did on software piracy a few years ago](#).

Here's an interesting post made by Chad Harris on [microsoft.public.windows.vista.general](#) on 10/7/06 on SPP, quoted in its entirety:

The problem is not that MSFT is addressing piracy with a legal staff dedicated to it full time under the direction of Nancy Anderson, Associate General Counsel.

Of course MSFT faces a huge, sprawling piracy problem as evidenced by the maps and literature they hve circulated at their meetings from booths attended by their attorneys and other employees over the years. It is complicated by the fact that many governments don't cooperate fully, and there is a similar situation in India in respect to patents for pharmaceuticals and in medicine in general in respect to HIV and the Avian

Flu pandemic and Mr. Gates is building on his learning curve in this area right now.

Microsoft and its partners and its system builders certainly have crucial concerns over the systemic implications of piracy.

The problem is that MFST is choosing to address piracy in an erratic fashion that has already shown substantial evidence of inflicting massive collateral damage and friendly fire on their customers. I hope that if they don't change this concept that has already proved to cause significant problems with WGA in its new incarnation as SPP, that they are forced to back off the way they usually are— they face money loss. If they had been able to make precise surgical tools, that would be one thing. But they already know that they are killing Vista and Longhorn Server on boxes that have fully legitimate licenses and they don't seem to care. This is evidenced if you read Ed Bott's account of how stupidly they fielded the calls and messages from a major Windows author, expert, and writer of columns on Microsoft's site.

I don't have any doubt there will be substantial litigation and possibly class action suits for Nancy Anderson's legal team at Microsoft, and while many suits are baseless—these will not be and they will be filed by high quality legal talent.

Ed Bott is doing a stellar job of tracking this, analyzing, and critiquing this and Ed Bott co-authors one of the most complete and authoritative Windows references for every operating system including the one that has pre-sold nearly a million copies, "Windows Vista Inside Out" by Microsoft Press

<http://www.microsoft.com/MSPress/books/9361.asp>

Ed Bott's Bookstore

http://www.edbott.com/weblog/?page_id=993

Ed Bott's Three Blogs**Ed Bott's Microsoft Report**

<http://blogs.zdnet.com/Bott/>

Ed Bott's Windows Expertise/Tips, tricks, news, and advice about Windows and Office

<http://www.edbott.com/weblog/>

Ed Bott's Media Central

<http://www.edbott.com/mediacenter/index.php>

Ed Bott's Columns on MSFT's Site

<http://www.microsoft.com/windowsxp/expertzone/meetexperts/bott.msp>

The author of one of the major books on Windows OS's and numerous articles for MSFT over the year Ed Bott has taken MSFT to task for their sloppy work with WGA repeatedly in the last few months and the same sloppy work with SPP and MSFT has had totally ignorant spokes persons speak to different questioners that are quoted on Ed's two blogs currently with the most inane and no knowledgable defenses of WGA which does not work correctly and SPP which will not work correctly immaginable. They are making a fool of themselves with the implemenation of WGA and SPP and they are going to learn to back off when it hits them in the area they worship—their money.

See and note in these articles the inane responses of MSFT representatives to the author of one of the best selling major books on their major Operating System software and others—one more example of MSFT's perception

of the public as stupid and their tin ear contempt for the public who are their customers and put Windows on 97% of the boxes on the planet.

I want people to note this conversation because it speaks volumes about MSFT's inane contracted support and MSFT's oversight of it and MSFT's attitude as to how little it means when they represent themselves to their customers—this is a conversation that Ed Bott had with “MSFT PSS” probably Convergys of Ohio contracting:

From Ed Bott at <http://blogs.zdnet.com/Bott/?p=84>

“I called Microsoft support to see if there is a hidden option to say, “yep, I’ve got updates turned to manual: it’s okay.” The rep said, “No and why wouldn’t you want to get the latest updates to Windows.”

I responded with the issues relating to WGA. He spent some time telling me that WGA was a good thing, etc. I reiterated that I have accepted all the updates except WGA and just want to review the updates before they’re installed on my machine.

He told me that “in the fall, having the latest WGA will become mandatory and if its not installed, Windows will give a 30 day warning and when the 30 days is up and WGA isn’t installed, Windows will stop working, so you might as well install WGA now.”

I’m wondering if Microsoft has the right to disable Windows functionality or the OS as a whole (tantamount to revoking my legitimate Windows license) if I do not install every piece of software that they send it updates.

That can’t be true, can it? I’m always suspicious of any report that comes from a front-line tech support drone, so I sent a note to Microsoft asking

for an official confirmation or, better yet, a denial. Instead, I got this terse response from a Microsoft spokesperson:

As we have mentioned previously, as the WGA Notifications program expands in the future, customers may be required to participate.

Microsoft is gathering feedback in select markets to learn how it can best meet its customers' needs and will keep customers informed of any changes to the program.

That's it. That's the entire response.

Uh-oh. Currently, Windows users have the ability to opt out of the Windows Genuine Advantage program and still get security patches and other Critical Updates delivered via Windows Update. The only thing you give up is the ability to download optional updates. Hackers have been working overtime to find ways to disable WGA notification. If WGA becomes mandatory, would it mean that Microsoft could prevent Windows from working if it determines – possibly erroneously – that your copy isn't "genuine"? That's a chilling possibility, and Microsoft refuses an easy opportunity to deny that that option is in its plans.

Over at Ed Bott's Windows Expertise, I've been soliciting feedback from Windows users who've been burned by WGA. So far, I've received 20 comments.

Here's a sampling:

a.. I have an XP Media center with a promise RAID 0 4-disc array. When I installed the WPA it broke the drivers for the array by causing failed delayed writes (half of the array just "disappears".) If I do a system restore to before the installation of the WPA everything goes back to working just fine.

b.. ince installing WPA : I've had blue screens and a total inability

to boot. I had to run the XP repair function to get the computer to boot. I had a damaged boot sector on the hard drive. I am running two drives on a RAID 1 config.

c.. I purchased a SEALED OEM copy of XP Professional. WGA said the license key was already used. I called MS and they said I should uninstall and buy another copy. I told them I wasn't made of money and hung-up.

d.. Microsoft rejected the product key that came with the ThinkPad I'm using. I had to call in and they gave me another code to enter which supposedly worked but now I get the blue screen of death about every other time I reboot. I've also lost all internet connectivity.

e.. I sent my Compaq Presario notebook for service repair, and it fails the WGA check. I have a legal version of windows xp professional on it. But I have no way to correct this problem.

What's most disturbing about this whole saga is Microsoft's complete lack of transparency on the issue. And before the ABM crowd jumps in with predictable "What did you expect?" comments, let me argue that Microsoft actually has a fairly good track record on transparency issues in recent years. Windows Product Activation is very well documented, and when a similar uproar occurred in 2001, it was squelched quickly by some fairly prominent postings from high-level executives who provided details without a lot of spin. Likewise, the Microsoft Security Response Center has done an exceptional job at providing quick responses to security issues. (Just ask Adam Shostack.)

Currently, no one at Microsoft is blogging about this fiasco. No executive has been quoted on the record about it. There are very few technical details available, and those that have been published are being tumbled through the spin machine and spit out as press releases.

If Microsoft really does plan to turn WGA into a kill switch in September, be prepared for an enormous backlash."

From Ed Bott on October 5, 2006:

UAC Good; SPP Not So Good

<http://www.edbott.com/weblog/>

“SPP, on the other hand, is the successor to Windows Genuine Advantage. Both initiatives have in common a reliance on Orwellian language that appears to be in the customer’s benefit but is actually a horrible inconvenience and potentially a nightmare. Despite Microsoft’s attempts to spin the new program, there’s no advantage for the Windows customer, and the only thing being protected is Microsoft’s revenue stream.”

Microsoft Issues Warning to VLK Customers Over WGA Fail

<http://www.neowin.net/index.php?act=view&id=35401>

Guess there will be a WGA “Kill Switch After All”

Published October 4, 2006 by Ed Bott

<http://www.edbott.com/weblog/?p=1495>

Is Microsoft about to release a Windows “kill switch”?

<http://blogs.zdnet.com/Bott/?p=84>

Search on WGA

<http://blogs.zdnet.com/Bott/>

October 4, 2006 For Vista, WGA gets Tougher

<http://blogs.zdnet.com/Bott/?p=148>

Ed Bott Blog Readers Burned by WGA

<http://www.edbott.com/weblog/?p=1370#comments>

WGA is a Mess

<http://www.edbott.com/weblog/?p=1476>

Microsoft Kill Switch in Windows Vista and threat to disable Windows (the so-called Microsoft Software Protection Platform)

<http://blogs.zdnet.com/Bott/?p=84>

Microsoft's Software Protection Platform: Protecting Software and Customers from Counterfeiters

<http://www.microsoft.com/presspass/features/2006/oct06/10-04SoftwareProtection.msp>

Microsoft's Software Protection Platform: Protecting Software and Customers from Counterfeiters

<http://www.microsoft.com/presspass/features/2006/oct06/10-04SoftwareProtection.msp>

White Paper: Software Protection Platform: Innovations for Windows Vista and Windows Server "Longhorn" Oct. 2006 (.doc file, 2.7 MB)

<http://www.microsoft.com/presspass/features/2006/oct06/10-04SoftwareProtection.msp>

Microsoft Issues Warning to VLK Customers Over WGA Fail

<http://www.neowin.net/index.php?act=view&id=35401>

Phil Liu of Microsoft has reported problems with the Windows Genuine Advantage authentication method for Volume License Key (VLK) customers and a temporary work-around.

"Just a heads up on an issue related to (Volume) VLK validation. On Monday and Tuesday of this week (Oct 2-3), some VLK customers may have experienced problems with WGA validation. If a Windows XP system with a VLK recently began failing validation or reporting as non-genuine, then they may be experiencing this problem. The problem was the result of an issue on the Microsoft server side, and we are still investigating the cause. We regret

any inconvenience this may have caused you, and I am personally working to get the information you need to resolve this issue.

We do have steps available that affected customers can take to correct the problem, and we'll continue to work on solutions and post them on this forum.”

Customers who are affected can:

- 1.. Delete the data.dat file from Documents and SettingsAll UsersApplication DataWindows Genuine Advantagedata (The drive letter will depend on where the OS was installed)**
- 2.. Revisit <http://www.microsoft.com/genuine/downloads/validate.aspx> to confirm that the machine is now genuine.**
- 3.. Run `wgatrayer.exe /b` from the command line to ensure that the latest validation is updated for WGA Notifications. This command may not be present on the user's machine and should not be considered an error if it is not. Please ensure that this is run as an Administrator. A reboot may be required to remove all non-genuine notifications.”**

Excellent article Chad!!

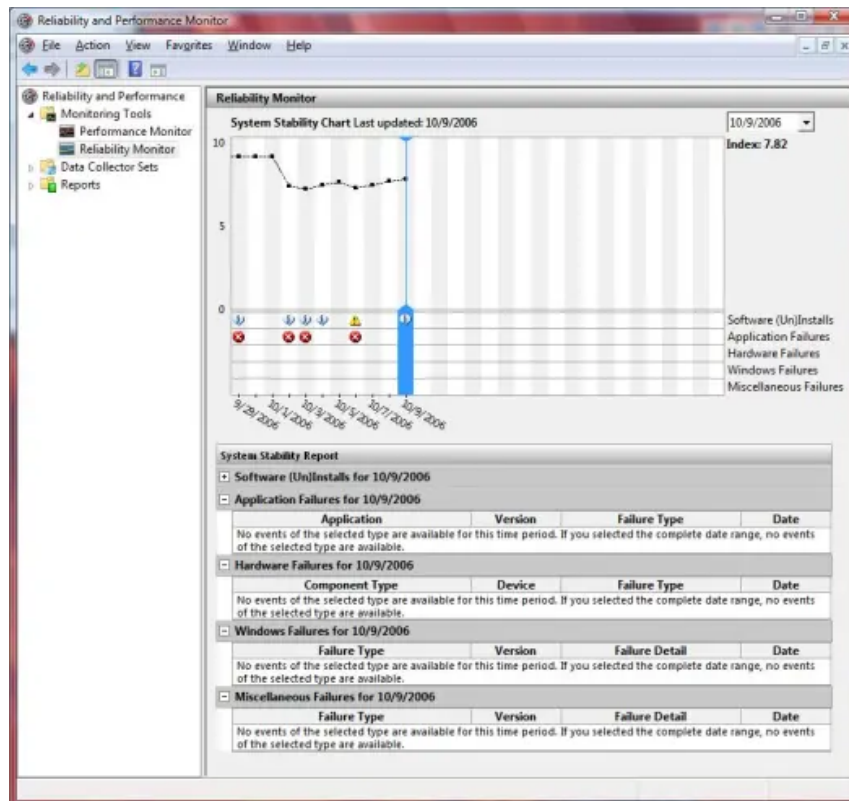
– Soli Deo Gloria

Windows Vista News You Can Use

OCTOBER 10, 2006

CATEGORIES: OPERATING SYSTEM, REVIEW

After giving Microsoft a tongue lashing, I decided to post about some of the things I like about Vista. Here's a real nifty one: Reliability Monitor. You can track, over time, the reliability of your PC. Here's a chart to see what I mean:



This is a chart of my work PC. As you can see the chart dipped around 10/2/06. This is around the time I did an in-place upgrade of my PC from build 5600 to 5728. On 10/9/06, I did an in-place upgrade from build 5728 (interim build) to 5744 (RC2). During the in-place upgrades, Windows flagged several programs as incompatible, thus the dip in score (*along with a few explorer crashes!*). The same historical data can be done for performance as well. This should be a welcomed featured for both users and IT professionals. Say you install a new program on a user's machine and they state the computer is slower since you installed the program. You can now objectively look at the historical data and determine if that really is the case.

[Windows Vista packaging](#). Take a sneak peak at what the boxes will look like for holding the Windows Vista media.

No Aero Glass for machines with 512MB or less of memory since build RC2. Here's the workaround:

1. Ensure that you have the following registry value set to :

HKCUSoftwareMicrosoftWindowsDWMComposition set to 1 (32-bit DWORD)

HKCUSoftwareMicrosoftWindowsDWMCompositionPolicy set to 2 (32-bit DWORD)

2. Restart DWM by opening a command prompt with administrative privileges :

– Type 'net stop uxsms'

– Then 'net start uxsms'

Just remember I told you get nothing less than 1GB of memory for Windows Vista!

Looking to spice up your sidebar? Get the freeware version of a sweet sidebar call [Desktop Sidebar](#). You'll wow your friends over the bland sidebar that comes with Windows Vista. This sidebar also works on Windows 2000/XP/2003.

– Soli Deo Gloria

Vista Release Date?

OCTOBER 13, 2006

CATEGORIES: MISC, OPERATING SYSTEM

Here's an interesting snippet from Winbeta.org:

A Microsoft executive has leaked a general release date for Vista, Exchange 2007 and Office 2007.

Speaking to IT professionals, parliamentarians and senior law-enforcement officers at the Parliament and Internet conference in London on Thursday, Microsoft revealed its release plans.

“We will officially launch Vista, Microsoft Office 2007 and Exchange 2007 on 5 December,” said David Hipwell, a Windows client sales professional at Microsoft. The business version of Vista – Vista Business – is expected to ship November 2006.

Update: ZDNet has removed the release date story without any explanation

Seems like someone let the cat out of the bag, oops!

Another interesting feature of Windows Vista is its ability to report back to Microsoft the issues you have encountered on Windows Vista and send resolutions back to the user. Below is one I got for Ahead Nero 6.6:



The only problem was I was running the latest version of 6.6.1.4, so not sure this hint would really help me.

How secure is Internet Explorer 7? Take a look at this guy that loaded every conceivable spyware toolbar into Internet Explorer. After you stop laughing, take a look at his cleanup effort.

Microsoft also recently revealed changes about what you can do and not do with Windows Vista. Apparently, you can only run certain versions of Vista in a VM environment. Unlike XP, you are only allowed one transfer of a license for Windows Vista to another PC. Does that mean if I replace a motherboard twice I have to buy a new copy of Windows Vista? At this point, it seems so and many people are very angry about this!

– Soli Deo Gloria

Vista Release Date Part Deux

OCTOBER 20, 2006

CATEGORIES: MISC

According to [Mary Jo Foley](#), Jim Allchin (*big cheese of Windows development*) said Windows Vista won't RTM on October 25th, 2006. There's also another [interesting article](#) showing that the general availability release date is set to January 30th, 2007 and also shows Vista pricing for each SKU. I still predict October 25th as RTM or very close to it (October 26th).

Michael Niehaus has 10 things you need to know about Windows Vista deployment. Read about it [here](#).

Build 5808 of Windows Vista has been released for a select group of testers (*unconfirmed reports indicate these people are part of the TAP program*).

Update (10/23/06): This just in from Paul Thurrott:

Exclusive: Microsoft Overcomes Final Vista Hurdles, Heads to RTM

A week and a half ago, online reports about an internal countdown clock at Microsoft verified my early 2006 report that the software giant was pushing for an October 25 Windows Vista release to manufacturing (RTM) date. But last week, Jim Allchin, co-president of Microsoft's Platforms and Services Division, admitted that the company had run into a snag and that Microsoft wouldn't make its planned RTM date. As of today, however, Microsoft is back on track because it has a working Vista build in escrow.

In an interview with Mary Jo Foley at "ZDNet" last week, Allchin said that Microsoft wouldn't be able to release Vista to manufacturing by October 25. "We are in pretty good shape," Allchin told Foley. "And there are still months before (the January 2007) launch."

Allchin was alluding to an internal timetable that I previously reported on in WinInfo: He had told the Windows Division that Microsoft could afford to postpone Vista's

RTM date to as late as November 8 and still meet its November and January launch dates.

However, each delay comes with a price, Allchin said: For each day past October 25, Microsoft will ship one fewer localized, language-specific version of Vista in the January launch.

I've found out that the source of Allchin's concerns was an unexpectedly buggy pre-RTM build of Vista. The previous Friday, Microsoft pushed Vista build 5824 into escrow, hoping that the build could qualify as the final shipping version. But a catastrophic problem with the build destroyed any systems that upgraded from Windows XP, requiring complete reinstallations. After several frantic days of trying to find the bug, Microsoft finally fixed the problem last Friday and reset escrow. On Friday, Microsoft internally released build 5840, which didn't include the bug. Testing over the weekend produced positive feedback.

Vista build 5840 includes a surprising number of brand-new and final icons, and a new set of final wallpapers, including a default wallpaper that's a variation of the Aurora "swoosh" that Microsoft has been using as a Vista identifier since it announced the branding in July 2005. There aren't any major functional changes in this build.

Oh, and that internal countdown clock? Last week, it was reset to count down to November 8, not to October 25. It's not clear, however, whether Microsoft will release Vista to manufacturing before November 8, and which—if any—language-specific versions of Vista will be dropped.

– Soli Deo Gloria

Technet Direct Plus

OCTOBER 25, 2006

CATEGORIES: MISC, TECH TIPS

Microsoft recently offered Technet Direct Plus as one of their Technet service offers. Under this program, a single user can download any full version of any of Microsoft's offerings for evaluation purposes right from Microsoft's web site. The first year is \$349; after that it's \$249 per year. I just signed up tonight. As an IT professional, I always have to hunt around for trial versions. The nice thing is that there are also special activation perks as well. Take Windows Vista. You can install and activate using the key they gave you up on 10 machines. On the same hardware, Microsoft won't decrement the activation count, meaning you can activate over and over again on the same hardware.

You also get two free PSS calls, how cool is that?



I asked Technet support if you can still use the software if you do not renew the subscription and I was told yes! So this is a very sweet deal indeed.

Listed below are some of the goodies you get to play with:

Applications

FrontPage 2003

Office 2003

Office Business Scorecard Manager 2005

Office Communicator 2005

Office Small Business Accounting

Office System 2007

Office Project Portfolio Server 2006

Office SharePoint Portal Server 2003

OneNote 2003 with Service Pack 1

Outlook 2003

Project 2003

Project 2003 Server

Virtual PC 2004

Virtual Server 2005

Virtual Server 2005 R2 Virtual Server 2005 R2

Visio 2003

Microsoft Dynamics

AX 4.0

Axapta 3.0

Customer Relationship Management (CRM)

GP (Great Plains)

Navision 4.0

Point of Sale 1.0

Small Business Accounting

Small Business Manager

Solomon

Internet Explorer

Internet Explorer 7 Beta 3

Windows Vista

Windows Vista August 2006 CTP (Build 5536)

Windows Vista Beta 2 (Build 5384)

Windows Vista July 2006 CTP (Build 5472.5)

Windows Vista RC1 (Build 5600)

Windows XP

Windows XP Professional

Windows XP Tablet PC Edition

Servers

BizTalk Server

Commerce Server

Content Management Server

Data Protection Manager 2006

Exchange Server

Host Integration Server 2004

Identity Integration Server 2003, Enterprise Edition

Identity Integration Server 2003 (English)

Identity Integration Server 2003 Service Pack 1 (English)

Microsoft Identity Integration Server Host Access Management Agent Feature Pack 2 (English)

Update for Microsoft Identity Integration Server 2003 Service Pack 1 (English)

ISA Server

ISA Server 2004 Enterprise

ISA Server 2004 Service Pack 2

ISA Server 2004 Standard

ISA Server 2006 Enterprise Edition

ISA Server 2006 Standard Edition

Live Communications Server

Microsoft Operations Manager

Software Update Services

Speech Server 2004

SQL Server

SQL Server 2000

SQL Server 2000 Enterprise Edition

SQL Server 2000 Reporting Services

SQL Server 2005

System Center Capacity Planner

Systems Management Server

Systems Management Server 2003

-Soli Deo Gloria

Pirates Already Cranking on Windows Vista

OCTOBER 26, 2006

CATEGORIES: MISC, OPERATING SYSTEM

It's confirmed: internal build 5840 was leaked to the Internet through a Chinese web link and distributed via eMule and bittorrent. This build does not have the build watermark on the desktop anymore and does not accept beta keys. We are getting closer to RTM! Interestingly enough, this build still does not require a product key if you boot it from the DVD. If you try an in-place upgrade, it will require a key. Of course, the pirates have been trying to get around the activation part since they don't have a key. The hack seems to center around file slc.dll and supposedly has existed since the Windows XP days. Basically, it resets the activation counter back to 14 days up to 3 times. After 3 times, it ceases to work. This sounds quite like what sysprep does. Looking on Microsoft's knowledge base, we find [this article](#). Indeed, the pirates are just invoking a function that is normally called by sysprep: nothing fancy here. However, pirates have already found where Vista stores its activation status and have already figured out that the operating system locks the user (*even administrators*) out of this area of the registry.

There are now web sites and communities dedicated to the cracking of Microsoft activation technologies. Get your popcorn out, because this time it's really going to be a cat and mouse game! Speaking of keys, here's a snapshot of my copy of RC2:



Key finders still work! Granted, this is not a RTM escrow build, but it goes to show you that if you have a Vista product key you better keep it very safe. It's very likely that the built-in key on the DVD will be banned from getting Windows updates and of course from activating.

– Soli Deo Gloria

Remove Novell and Microsoft Word Goes Ape

NOVEMBER 3, 2006

CATEGORIES: TECH TIPS

Here's an interesting situation. Our company is moving from Novell to Microsoft for our file and directory services. We removed the Novell client from everyone's workstation and that seemed to work just fine. Then we removed everyone's rights to said Novell server and everything is still fine. Then shut down said Novell server and bam: opening some Word documents takes 2 to 3 minutes!

Tracing with Regmon and Filemon produced no viable results. No file activity was being done during Word's hang. Executing "winword.exe /a" also resulted in a long hang. We tried this on three different machines with all the same results, so it wasn't directly related to the PC itself. The problem? The documents were tied to a document template on the server we took down. The solution was to remove the path to the template under template addins. What to do, however, if you have hundreds of said files?

From [here](#), I found this macro which loops through a folder and changes the template location for each file.

Note that I could only get this script to work by copying the document files to my C: drive and then pointing the script to C: (*the script doesn't seem to like folder names too much*). It did, however, remove the template location as expected. [Microsoft does have an explanation and a fix for this](#), including more VBA scripts that do the same thing as the above script.

However, the scripts will take 2 to 3 minutes per file and is just as bad as the original problem. I found out, however, by accident, that putting the offline server name in the HOSTS file with an address of 127.0.0.1 (localhost) works just as well. It is though Word is waiting for a ping response from the server and it waits 2 to 3 minutes for this response. If the hostname is at least pingable, Word in our case would carry on in 15 seconds which was a lot faster.

Update: There's even a slicker way of changing the template location in each file without having the macro waiting 2 minutes to open each file: disable the onboard NIC. As soon as you do this the script will fly through all the files. I did this in a Virtual PC session running Windows XP. This lets you change the document files without interrupting your normal work. When you are done, simply turn the NIC back on.

– Soli Deo Gloria

Windows Vista RTM is Imminent!

NOVEMBER 5, 2006

CATEGORIES: OPERATING SYSTEM

From Paul Thurrott's WinInfo:

My sources at the software giant confirmed this weekend that Microsoft is set to finalize Windows Vista as early as Monday and release the product to manufacturing. The final build number is expected to be 6000.16386.061101-2205, I'm told. (Readers may recall that WinInfo broke the news that Microsoft would iterate Vista to build 6000 for the final release way back on August 25.)

In its quest to finalize Windows Vista, Microsoft has faced two hurdles in recent days, one technical and one a bit more unusual. The proposed final build was marred by a few late breaking bugs, which the company expects to squash over the weekend. Meanwhile, a power outage in the Windows build lab Friday night prevented Microsoft from creating a new Vista build that night.

As I've related in my "Road to Gold: The Long Road to Windows Vista" series on the SuperSite for Windows, Microsoft was angered earlier this year when analysts at Gartner were granted unprecedented access to Vista's bug database but published an opinion stating that the company would delay Vista past its January launch. This week, however, Michael Silver, the Research VP at Gartner finally admitted that his firm's repeated predictions about further Vista delays were wrong, delighting those on the Vista team.

"It appears that Microsoft will beat our prediction," Silver wrote in a Gartner blog. "We will congratulate Microsoft as they hit their dates." Prepare to issue that congratulations, Mr. Silver: Microsoft is set to release Windows Vista this very week.

I'll begin publishing a massive, multi-part review of Windows Vista on the SuperSite for Windows as soon as Microsoft OK's its publication. This is expected to happen when the company announces it has finalized development of the product. Stay tuned.

Behind the Scenes: A Look at Windows Vista

NOVEMBER 8, 2006

CATEGORIES: OPERATING SYSTEM

Here are a few snapshots of the environment that Windows Vista is being built in. What's interesting is that 1,000 applications are tested daily with each build of Windows Vista. If you look at my earlier blog post which has videos of earlier Windows builds (2000/XP) and how they were made, you will see this fact is not mentioned any where. This is because Microsoft is now using automated scripts to test applications instead of humans.

Windows Vista has RTMed as of 12:45PM CST! If you haven't gotten a Technet Plus Direct subscription, do so NOW! You will get access to Office 2007 and Windows Vista for \$350 within 7 days of RTM.

Interesting article from CNET today:

Vista's Last Mile

By Ina Fried

Staff Writer, CNET News.com

Published: November 8, 2006 4:00 AM PST

REDMOND, Wash.—The last stop for Vista is a windowless conference room in Building 26, on Microsoft's sprawling campus in the Seattle suburbs.

Each day, members of the Windows team gather inside this "shiproom" to go over the bugs that remain, and to debate which of these can still be fixed in the days left until the product is declared finished, a milestone that is expected any time now.

The intense "end game," as these final weeks are known, is a well-worn tradition inside the shiproom, which is on the third floor of the Windows development building. The small room, with its dated, dark wood conference table has been the war room for every Windows release since Windows 2000.

On the wall are knick-knacks from past projects, as well as clocks showing the minutes ticking away in a dozen time zones. The clocks serve as a reminder that Microsoft has a deadline to meet. The company has scheduled a November 30 press event in New York to announce the availability to businesses of Windows Vista, while computer makers need to get the final code in order to finish their testing and get Vista on PCs in time for a broad launch in January.

The once-daily shiproom meetings have become twice-a-day events as the product has neared completion. Projected onto a screen is a list of unresolved issues that need to be addressed before Vista can leave. There were about five dozen such issues at a meeting last Wednesday morning.

Sven Hallauer, who heads up the process, moved quickly through the list as about 40 programmers, nearly all with a laptop in tow, worked to keep up. At each sticking-point, the person responsible for tracking the issue gave a one-sentence report on where things were.

In one case, there was a bug in the Slovenian release of Vista. It was quickly tabled as not pressing, given that Slovenian is not in the first or even second wave of localized versions of Vista. Other reports came in—this software program has a hitch, this particular laptop has trouble waking up from sleep.

Some of the glitches were already known. Many were things that have already been fixed, and a few were too new and need investigating. None appeared to be a show-stopper.

Hallauer had predicted that the morning's meeting would be fairly short—maybe a half-hour. After 20 minutes, the group decided that things seemed pretty good. Perhaps they wouldn't need to revise the code again.

At the afternoon meeting, though, the team was forced to revisit that decision. It turned out that there was an issue within Vista's new diagnostics: if a piece of software failed to install properly, the system would nonetheless get a report that it had been successful. Hallauer and team decided to spin one more build.

Weighing changes

It's all part of the process. Several times, Hallauer and others have thought that they had the final version of Vista done, only to find something that meant the team had to put in another fix.

Two weeks ago, Microsoft thought it had something that promised to be the final version. But within a couple of days, two new glitches had surfaced. The issues were arcane, but significant enough. In one case, there was a potential problem with burning DVDs. If a Vista machine attempted to burn information to a blank DVD directly from a network drive, there was a chance that data could be lost, if the network was slow. The other problem had to do with offline folders: Under certain circumstances, applications weren't being notified if the cache was full.

"That could end up with users losing their data or having a really bad experience," Hallauer said.

While it seems natural to go ahead and fix such bugs, changing the code at this point is a big deal. There isn't time for the full regression testing, which investigates whether a fix in one area has some hidden impact somewhere else in the system. Instead, teams must create solutions that only touch a part of the code and count on their ability to not break something elsewhere.

And not everyone agrees which things need to be tackled. The battles inside the shiproom can get testy sometimes. These days, there are certainly folks

who feel Vista is ready to send on its way. Others keep lobbying for particular fixes, including some requests made late last week.

Hallauer said he doesn't see his job as just saying "no"—but at this point, it is certainly about only saying "yes" to the right things. "Through most of the product cycle, the teams are fairly independent," he said. "Now that we are at the end of the release cycle, it is more (about) taking stronger reins."

Sharks and limpets

While Vista is not glitch-free, the product is finally coming together. When Microsoft does find a bug, it gets classified into one of two categories.

One is "sharks"—bugs that everyone agrees need to be fixed before the product ships. And then there are "limpets," which are issues that can be fixed, but where the need is less critical. In those cases, the fixes are developed, but don't get implemented unless a shark comes along that they can use to float into the code.

Retiring Windows chief Jim Allchin doesn't like the shark and limpet analogy. To him, nearly every bug is a shark worth fixing.

"(If) there's a fix, I want to put it in," Allchin said. "It should be clear that date means not much to me, that quality is much more important."

But Allchin is finding plenty of resistance these days. Microsoft is under a fair bit of pressure to get Vista out the door.

The latest shark, though, means that he can get in one of the changes he wanted. For months, the company has been struggling with an issue in the Vista set-up process. As the operating system was loading, the screen would

appear to freeze up, with no indication that the installation was still progressing—although it was.

Developers put that problem right. But as a result, a dialog box that asked users to identify the type of network they have was popping up twice.

To Hallauer, it was an issue that might or might not have justified a new build. Allchin was convinced it did.

“When I heard about it, I thought, there’s no way...(We’ve got) to fix this,” Allchin said.

The unrelated software-installing problem let Allchin win the day.

end their days putting the latest builds through their paces.

Until recently, Microsoft has issued a new internal release of Vista every day. That’s a grueling process. Typically, its servers start cranking away at the raw code around 7 p.m., compiling it through the night, with the goal of releasing the new build by early afternoon the next day.

Down the hall from shiproom, Windows unit employees can pick up the latest builds. About 500 people pick up a DVD with new code in person each day, with many more getting the code over the network, and some even bringing their home machines into the office.

That list includes rank-and-file Windows employees, as well as some of the company’s top brass. Allchin and his technical assistant, for example, are still trying to find bugs that the servers and development teams have missed.

“I’m doing video calls with my mom in Boston,” Allchin said. “I’m doing remote assistance to jump into a machine, and then I ‘remote desktop’ from

that machine to another machine.”

Elsewhere, Allchin is testing a multimonitor set-up with four displays, including some in portrait mode. Paul Donnelly, who manages part of Microsoft’s Vista test operation, has been doing the same thing for some time. As the finalization deadline has neared, he has added more systems to his office. As of last week, he had nine machines crammed into his office. He is among those who nearly always picks up the daily build.

“Pretty much every day since at least May 2005, I think I have installed on some machine,” he said.

Donnelly, who tinkers with old cars and classic pinball machines in his spare time, said that he tries to do the opposite of what an IT manager would recommend.

He changes all the default settings, for instance. And instead of testing a clean installation on a new machine, he’ll try to upgrade an older model.

“You find bugs,” he said, “You absolutely find bugs that way.” Luckily, he said, it is getting harder and harder to find issues that aren’t already on the radar screen and being addressed.

“We’re on watch right now...keeping an eye on things to make sure that we haven’t missed anything,” he said. “I haven’t had any ‘heart attack’ issues arrive in the last few months.”

But Vista’s fortitude does not depend solely on the watchful eyes of Windows veterans like Allchin and Donnelly.

With each day’s build, Microsoft is running a battery of automated tests against around 1,000 of the leading software programs. It has written

750,000 lines of code just to create the test patterns, which take 355 servers the better part of the day to run.

“Our job is to try and break the apps and find the bugs,” said Mike Kirby, who runs the automated test lab. These days, though, the team is just hoping that each day’s build doesn’t bring up any new bugs.

Third-party support

In another building, individual software and device makers have their own private offices, where they can work on their own Vista-related issues. One of the key areas for Microsoft, beyond finishing its code, is getting hardware and software makers to get their products ready for the new operating system. To make that as attractive as possible, it has created a building on its campus just for them: the Platform Adoption Center, better known inside the company as the “high-touch” lab. The building, one of the hippest on Microsoft’s largely bland campus, offers an inviting atmosphere with private offices, a lounge with a Xbox 360 game console and plenty of munchies.

“We try to keep them well-fed and well-caffeinated,” said Dave Wascha, who helps lead Microsoft’s effort to make sure other software makers have their products ready to go when Vista ships.

The companies that come also get their own rooms that lock with a code combination that only they know. They can use PCs from Microsoft, or bring their own machines. Either way, the computers can connect directly to the Internet without going through Microsoft’s network.

“Essentially, this is their office,” Wascha said.

The center has been home to 16,000 people since 2004, and is booked solid every week. It has been home to Microsoft’s traditional partners as well as

some of its fiercest rivals, many of whom did not want to be named.

One rival that has been public about the hand it received from Microsoft is the Mozilla Foundation, creator of the Firefox browser. In August, the open-source software maker an offer of help from Microsoft.

Another rival that credits Microsoft for helping it get Vista-ready is AOL. The Internet services provider went through the Redmond lab in July, while Microsoft engineers traveled to AOL's campus in Dulles, Va., in August and September.

“We worked through a ton of issues,” said Julie McCool, the AOL vice president who manages the team that handled the Vista work. One of the many efforts the two companies worked together on was coming up with a way to let customers get a Vista-friendly version of AOL's software when they stick an older CD into a new PC. In the end, the companies figured out a way to alert people that the CD they pulled off a two-year-old magazine doesn't have the Vista version and to get that software from the Web instead.

McCool said that AOL has continued to meet weekly with Microsoft. Initially, the company had plenty of bugs it was working through, but in recent weeks it has been smooth sailing. “I don't think we had any big surprises in the past week,” McCool said.

Eating their own dogfood

Microsoft's own work force is a key arbiter of whether a release is ready to go out the door. About 60,000 machines inside Microsoft are running Vista as part of the company's “dogfooding” process.

CIO Ron Markezich signed off last week, saying that Vista had met his goals—a step that has to happen before a product can leave Redmond.

“It’s totally ready to go,” Markezich said.

Microsoft is trying to do a better job with the final testing of Vista than it has in past versions of Windows. “We have to learn from ourselves,” Donnelly said. “We don’t have the ability to go to somebody bigger than us and go, ‘What were the problems with your last release?’”

Donnelly, who has been at the company since Windows NT 3.5, said he remembers an early NT release over a Labor Day that was particularly hairy. “I just remember the pizza boxes stacking up in the kitchenettes,” he said.

There’s urgency, but no panic this time, he said: “You just don’t see people running around like crazy.”

– Soli Deo Gloria

Sysinternals Web Site Has Moved to Microsoft

NOVEMBER 9, 2006

CATEGORIES: TECH TIPS

Sysinternals is now at Microsoft and they now have Process Monitor 1.0 out which replaces Filemon and Regmon. This version also works on Windows Vista. The Winternals part of Russinovich's business is being bundled into the Microsoft Desktop Optimization Pack for Software Assurance. More information about this product can be found here. In a nutshell, all the technologies that Microsoft bought from Softricity, Winternals, DesktopStandard, and AssetMetrix will be given to SA customers if they wish for \$10 per desktop. Sounds like a pretty sweet deal to me!

– Soli Deo Gloria

Windows Vista RTM (Build 6000) Already Leaked

NOVEMBER 11, 2006

CATEGORIES: OPERATING SYSTEM

Yes, indeed. Two days after the announcement of Windows Vista going RTM, copies have already leaked to the Internet. Using a few files from build RC2 (*no, I won't tell you which ones*), pirates have already figured out how to activate Windows Vista RTM. More than likely, Microsoft already knows about this work around and will soon "plug the hole". Office 2007 is scheduled to be on MSDN and Technet on Sunday, November 12th. Windows Vista will be on MSDN and Technet on Friday, November 17th.

– Soli Deo Gloria

Blog Comments Disabled

NOVEMBER 15, 2006

CATEGORIES: MISC

For some reason my blog is getting flooded with comments from spam bots. I've also noticed a spike in visitor traffic the past few days (*about twice the amount of visits I usually get*). Since I have to moderate each comment and either approve or deny them, I am disabling commenting at this time. If you wish to comment on a specific article, please e-mail me your name, e-mail address, article you are commenting on and your comment to my e-mail address on the about page.

Thanks for your understanding.

Update: After loading the Akismet anti-spam plugin, I have re-enabled commenting.

– Soli Deo Gloria

Installing The Final Version of Windows Vista

NOVEMBER 17, 2006

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Well, I am like a kid in a candy store! The final version of Windows Vista was put up on Technet last night and I eagerly downloaded it. After downloading and burning the DVD, I booted from the DVD. The option to not put in a product key is still there. My guess is that the feature exists to further protect the product key. For example: you can take your PC into a store to have Vista re-installed and not give them the product key. The technician can skip the product key and then you can enter it at home. I decided to put the key in later, so I just clicked next. After a few more reboots, I was in Vista. Yes, I had Aero Glass! I have a 256MB PCI card because the AGP on my motherboard is shot. Aero glass unfortunately was a bit sluggish, so I turned it off (*I was scoring 2.6*). To be fair, PCI cards were not meant for high end graphics rendering, so this was to be expected. I then noticed I did not have any sound. I have a Creative Labs SB Live 5.1 card, so I headed to their site. No Vista drivers! Now most XP drivers should work in Windows Vista, so I just downloaded the Windows XP ones. Upon launching the setup program, it told me no qualifying products were installed on my machine. Yeah right!

Using the newly released Process Monitor from Sysinternals, I went in search of the files:



Ah ha! Before I hit finish (*which would delete the files*), I copied the drivers to my backup drive. I pointed the unknown device to the XP drivers and I now had sound! I zipped up and uploaded those drivers files [here](#) on my web site.

Another annoying problem was that Windows Vista switched all of my drive letters. My backup drive use to be F: and my download drive D:. Now my backup drive was D: and my download drive was E:! I was able to switch my drive letters back after rearranging a few drive letters, rebooting and then rearranging some more.

Folder and file permissions seem a bit screwy in Windows Vista. Upon trying to save a driver on my backup drive, I was told I didn't have access to the folder, even though I created it in XP and I am an administrator in Windows Vista. It allowed me to take ownership and proceed. However, I do not want to get this prompt for every folder on my backup drive, so I went into the security properties of the partition and forced Vista to propagate the settings to all files and folders.

Launching Xnews on my other partition produced a crash. I know that Xnews works fine in Vista because I was running it on my Vista workstation at work. I once again loaded up Process Monitor and saw that it was having problems writing to various files in D:xnews. I proceeded to force out all security permissions for this partition as well. However, that did not fix the problem. Even though I had set Full Control rights for administrators and told Windows Vista to propagate them to every file and folder, Xnews kept choking on various files. I ended up doing a RunAs on a command console and issuing “cacls * /g everyone:f” from the Xnews directory and then it worked.

Thinking about it, this makes sense. With UAC, users run as standard users. So even though I am in the administrator’s group, I don’t have the administrator’s token and therefore I only have read access to the said folder. So, instead of granting everyone rights to my folders as I did above, I took complete ownership of all files and folders on each of these data partitions. Then I granted myself full control of these folders. Problem solved! Now, for the partition that Windows is sitting on you will have to get use to the fact that you will need to RunAs programs that want to write to the C: drive. I realize how annoying this will be, but I’m slowly getting use to do it. I rather be a bit inconvenienced then have my machine comprimised by malicious programs (*although for sanity sake I made a TEMP directory on C: and gave myself full rights to it so I can modify files in a “sandbox” without UAC in my face*).

Another fun project: getting my Agfa Snapscan 1212U scanner to work in Vista. The drivers are from the year 2000 and the scanner itself is around 6 years old. I had to do the “snap the drivers from the temp directory” trick as I did with the SB Live! card. However, when I would launch Snapsan 1.4, it would just quit. Agfa doesn’t make scanners anymore, but I did find Scanwise 2.0 on their web site. The program would load, but it said it was having a communication problem with the scanner. I did some Google searching and found out about [Vuescan](#). This software is extremely slick: it generically interfaces with your scanner and the company specifically supports Windows Vista! There is a generic scanner.inf file that works for over 500 scanners if you don’t have a 2000/XP/Vista INF for your scanner. I tried it on my PC and it worked great!

World of Warcraft was running decently under Windows XP, but it was a bit sluggish under Windows Vista. I tried the latest NVIDIA drivers from their web site, but that did not seem to help much. I decided to install Windows 2000 into the same partition as Windows Vista. I added an entry for Windows 2000 using [VistaBootPro](#). This is a nice 3rd party utility that edits the BCD instead of using the command line utility bcdedit. Towards the end of the Windows 2000 installation, I realized that I shouldn’t have done that as it was updating files in C:program files and failing! Other than Internet Explorer not working in Windows 2000, everything actually

worked out fine. After loading Windows 2000, it wiped out the Vista boot loader. I just booted from the Windows Vista DVD, picked Startup Repair and I was back in business.

For more information on Windows Vista, check out the Vista forums at [ProNetworks](#).

Installing the Windows 2003 Admin Pack on Windows Vista

NOVEMBER 21, 2006

CATEGORIES: OPERATING SYSTEM, TECH TIPS

From [Josh's blog](#): we have a neat little trick to getting the Admin Pack tools from Windows 2003 working on Vista. I have uploaded [FIXADMINPACK.CMD](#) up to my web site. Just run the file after you install the Admin Pack and it should work. (*Just verified that this works on RC2 and RTM; make sure you do a RunAs administrator on a command console, otherwise it won't register the DLLs correctly*).

Windows Defender: how the heck do I remove this program? I use my own anti-spyware solution in the form of Spyware Blaster and do not need Windows Defender. Defender blocks the autostart of my Quickspell 3.7 beta program unless I turn UAC off. It appears from my investigations that Defender is built into the OS and cannot be turned off. After removing the Defender using Autoruns and disabling the Defender service, it still runs. Eek! Tell me why I have to have the Windows Firewall running to use Remote Desktop? I'm behind a router Microsoft, why lock me out of this feature! I hate the Windows firewall, hate, hate, hate! Expect a lot of "hacks" to come out when Vista is released in January. I suspect there will be a section on my web site dedicated just to Windows Vista to help people turn off features they don't need (*and enable the ones they do*).

Update (11/29/06): Windows Defender CAN be disabled using GPEDIT.MSC. Navigate to Computer Configuration>Administrative Templates>Windows Components>Windows Defender to disable Defender. It appears that the blocking of the startup program is solely due to UAC and not Defender as I stated above (*even though picking "Show blocked programs" brings up Defender, the problem is actually an UAC problem. Confused? Good!*)

Update (12/5/06): It appears from this [MSDN article](#) that RunOnce and POLICYRUN are exempt from this restriction. Indeed, if you run gpedit.msc and drill to "Computer Configuration>Administrative Templates>System>Logon>Run these programs at user logon" and add your executable there, it will run it elevated without prompting. The key in autoruns looks like this:

- Soli Deo Gloria

Ashampoo Burning Studio 2007 for Free

NOVEMBER 28, 2006

CATEGORIES: TECH TIPS

Free download and totally legit!

<http://www.computeractive.co.uk/burningstudio/index>

Just fill out the registration for a free product key. And yes, this version works on Windows Vista!

Windows Vista Product Key Update

NOVEMBER 30, 2006

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Earlier I wrote a blog entry about product key finders and how they still work on Windows Vista. Well, it appears that this does not work on the Enterprise edition of Vista. You can use a key finder to find what key comes bundled with the DVD, but once you activate it with a different key, the product key comes up with all B's. Using a key finder on Vista Ultimate before and after activation, however, works fine.

Microsoft is working hard to protect its keys this time around!

– Soli Deo Gloria

Windows Vista Released on CDs

DECEMBER 1, 2006

CATEGORIES: MISC, OPERATING SYSTEM

Technet now has Windows Vista in a 5 CD version (*in addition to the DVD version*). Not quite sure if retail will be offered in this way. Office 2007 Ultimate is also being released on Technet.

The [Office 2007 trial](#) is now available.

Speaking of Technet and Vista, these are the versions you will have product keys for and access to if you are on Technet Direct Plus or above:

- Windows Vista Business
- Windows Vista Home Basic
- Windows Vista Home Premium
- Windows Vista Ultimate

– Soli Deo Gloria

Illegal Windows Vista KMS Appears on Internet

DECEMBER 4, 2006

CATEGORIES: MISC, OPERATING SYSTEM

An illegal KMS in China is serving up Windows Vista activations for free for Business editions of Vista, thousands of them apparently. Under KMS, only the last 50 activations are recorded or “cached” on the server. Which brings up an interesting situation: how is KMS protected? Apparently you can use one volume license key and activate against a completely different one than is kept in the digital store of the KMS. If you are on a college campus that has a KMS, you apparently can connect and activate against it provided you can find the server.

Provided that someone makes a key generator like the one made for Windows XP, one would only have to find a KMS to activate your copy, any KMS! Since Microsoft doesn't record KMS activations, an administrator may not even know his server is being used to activate pirated copies.

Update (12/6/06): It gets worse...supposedly, you can download an activated KMS server in VMware format and activate your PCs indefinitely at home. Those Chinese pirates are crazy! Pirates – 1, Microsoft – 0.

– Soli Deo Gloria

Utility Review: FreeCommander 2006

DECEMBER 9, 2006

CATEGORIES: REVIEW

There's tons of neat little utilites on my Tech Files sections and I rarely talk about any of them here on the blog. Here's one that I recently discovered for file management: [Free Commander 2006](#). Now, I know what you are thinking: why another file manager? I wanted a folder size utility to prune my disk (*I actually wrote about ExplorerXP before to do that, but I didn't think of it at the time*). One of the great features is being able to sort by file and folder size. It even keeps this view when drilling several layers up and down the tree. This saves having to sort per folder view which is such a nice time time saver. To get the size of folders, you actually have to hit **Folders>Size of Folders**. This is done because you might not want a lot of disk I/O from it computing folder sizes.

Free Commander also has native built-in handling for opening ZIP, CAB and RAR files. Nice! I also like the handy icons in the upper right hand corner that give easy access to the Control Panel, Start Menu, Desktop, System Folders and Computer Management. This was written with a PC technician in mind! You can also map network drives, get to a Run box or Command Prompt from the Extras menu.

Free Commander also lets you edit file and folder timestamps like Total Commander. Total Commander, in my opinion, tries to do too much. Another nice thing is that you can do a RUNAS on Free Commander to run as administrator and therefore change permissions on files and folders.

– Soli Deo Gloria

BDD 2007 and Windows Vista

DECEMBER 12, 2006

CATEGORIES: MISC

Right now I'm playing with BDD 2007 RC1 with Windows Vista RTM and hopefully will have a write up of how it works within the next few weeks. Unfortunately, none of the WinPE stuff (*LiteTouch*) is booting for me and there is supposedly a hotfix (*KB928570*) to address all this. Oh the joys of beta! However, Johan Arwidmak has a "new" site called www.deployvista.com and he gives some really nice guides on how to use BDD 2007 RC1.

One issue that I came across in Vista is using sysprep with the generalize switch. Every time I used the /generalize switch, sysprep would crash and my image would be hosed. It appears this is a known issue with the SoundMax drivers. As soon as I uninstalled the SoundMax drivers and then ran sysprep, everything worked fine. The other quirky thing I've run into is that sysprep refuses to read my unattend.xml file unless I copy it to C:\sysprep and then run sysprep from the same directory. The WAIK documentation specifically states that sysprep must run from C:\windows\system32\sysprep, but I have yet to get that to work properly. ~~Sysprep also doesn't remove the unattend.xml after running through the mini-setup: this could comprise product keys if you are using MAK!~~

Correction (12/15/06): Product keys aren't defined in unattend.xml for Business and Enterprise editions of Windows Vista. Windows Vista will just ignore the product key if you input the product key in the sysprep (unattend) file. Defining a product key for Business/Enterprise in BDD 2007 can actually cause it not to work!

- Soli Deo Gloria

To Boldly Go Where No Technican Has Gone Before

DECEMBER 18, 2006

CATEGORIES: TECH TIPS

Windows likes to hide certain files and folders in its operating systems. As technicians, we sometimes need access to said files and folders. One of the famous ones is where Internet Explorer stores its temporary cache files. This is in the folder C:\documents and settings\local settings\Temporary Internet Files.

Upon looking at this folder in Windows explorer, we see this:



The fact is, this is not a true representation of what is really in the folder. For that, we have to hit a command prompt:

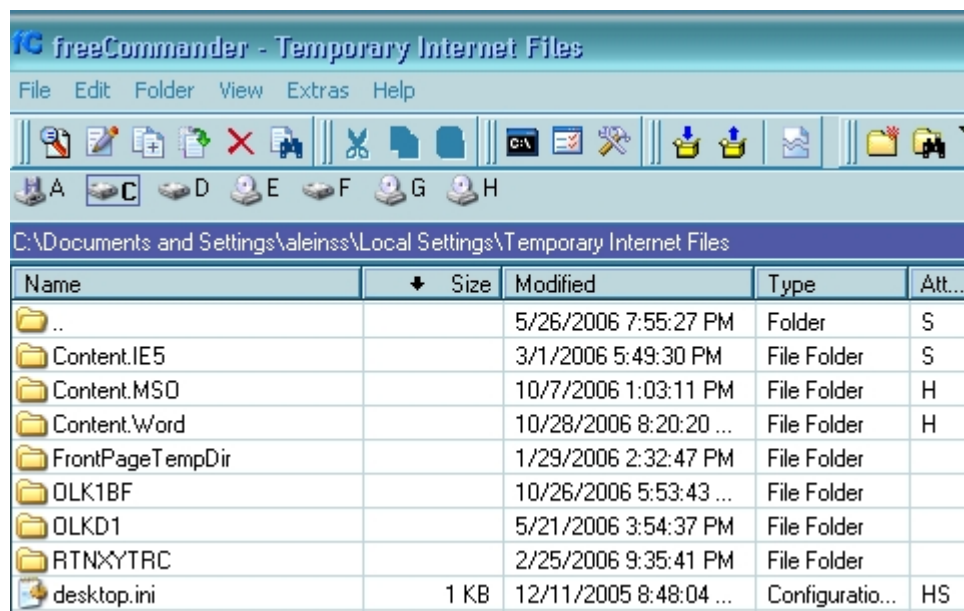
```
C:\Documents and Settings\aleinss\Local Settings\Temporary Internet Files>dir /a
Volume in drive C is SUPERTECH
Volume Serial Number is 7C18-5C9E

Directory of C:\Documents and Settings\aleinss\Local Settings\Temporary Internet Files
05/26/2006  07:55 PM    <DIR>          .
05/26/2006  07:55 PM    <DIR>          ..
03/01/2006  05:49 PM    <DIR>          Content.IE5
10/07/2006  01:03 PM    <DIR>          Content.MSO
10/28/2006  08:20 AM    <DIR>          Content.Word
12/11/2005  08:48 AM                67 desktop.ini
01/29/2006  02:32 PM    <DIR>          FrontPageTempDir
10/26/2006  05:53 PM    <DIR>          OLK1BF
05/21/2006  03:54 PM    <DIR>          OLKDI
02/25/2006  09:35 PM    <DIR>          RTNXYTRC
                1 File(s)                67 bytes
                9 Dir(s)  35,798,089,728 bytes free

C:\Documents and Settings\aleinss\Local Settings\Temporary Internet Files>
```

Another folder with this restriction was C:\windows\system32\dllcache. In at least Windows 2000, if you tried to navigate to this folder from Windows explorer, you wouldn't find it. However, it appears they lifted that restriction, at least in Windows XP SP2.

So is this Windows issue or an Explorer issue? To find out, let's load up FreeCommander 2006 and see if we can see the Temporary Internet files folder:

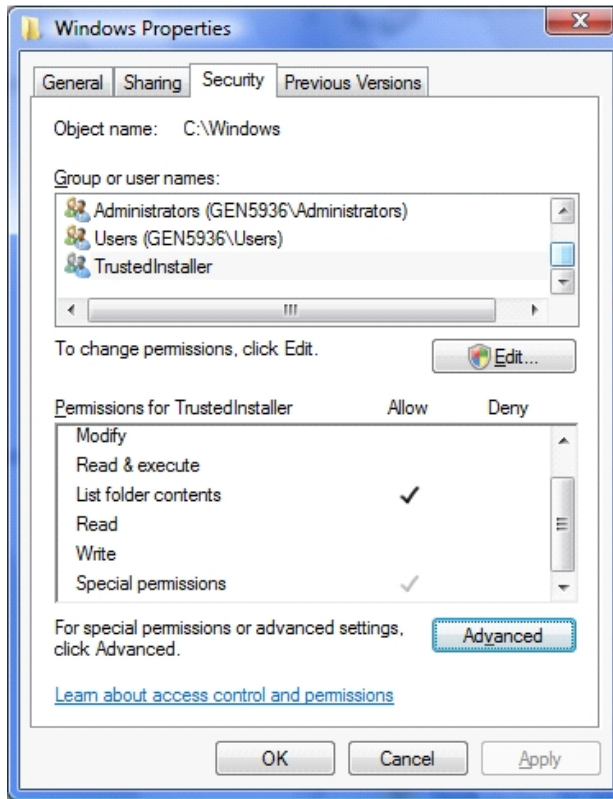


Lo and below, we see it! So there is code in explorer.exe to block users from seeing that folder. If you want to see all the files and folders on your hard drive, it's best not to use explorer, but a 3rd party file program.

Windows Vista takes this a step further and removes the administrators group from system folders. That means that just because you are an administrator doesn't mean you are a "demigod" anymore. If you have UAC enabled on Windows Vista, always remember the following: "Administrators run as standard users, even when in the administrators group with UAC turned on". You are only given the "demigod" token when UAC prompts you to elevate for a certain action. As soon as the action is complete, the token is taken away.

This "feature" is designed so that if someone with administrative privileges runs a spyware program that program cannot inject itself into critical system folders or so Microsoft says. When you run a setup program, Windows Vista detects certain manifests within the setup program and gives it the TrustedInstaller token. This allows it to write to C:\windows among other folders. So what would prevent a spyware programmer from making all of his spyware programs setup like programs? No quite sure myself. My guess is that Microsoft is trying to educate us. If you visit a web site and it wants to run a setup program, a red flag should go up right away. Hitting yes to that prompt gives that program the right to modify your system files.

If you are an administrator and need to modify files in C:\windows or other folders, you now have to take ownership of said files and folders. Once you do this, you can modify the security to give yourself write access.



- Soli Deo Gloria

Symantec Antivirus: All Faith is Lost

DECEMBER 22, 2006

CATEGORIES: MISC, TECH TIPS

No product has failed me this bad lately, but Symantec Antivirus version 10 certainly has! You might remember my [article last year on Symantec Antivirus 10](#). As I was working on a test box PC and running Process Monitor from Sysinternals, I noticed a rundl132.exe file trying to connect to a bunch of PCs on our network. I promptly rebuilt the PC 5 times only to have it yet again reinfected each time. This machine was running the latest version of Symantec Antivirus and had the latest virus definitions. Even when I turned off file and print sharing by stopping and disabling the server service, I kept getting reinfected. Apparently, 1732 executables on my main machine's second partition were infected with Looked.P and this is how I was getting re-infected. This worm goes and searches every directory on your hard drive, leaving a _desktop.ini file to mark each directory it has visited. It also infects every executable on your hard drive, except if it's in C:windows.

Worse yet, I wasn't the only one infected with this virus. Somehow this nasty worm got past SAV client with the latest definitions (*note this worm has been out in the wild since July of this year, it is **NOT** a new worm*). Not only that, but Symantec Antivirus 10 also refuses to clean them! To add insult to injury, this worm also infects SAV executables, making the antivirus program itself quite useless. To clean up this mess, I had to go around and disable the server service to turn off file and print sharing. Once the PC was isolated, I then had to boot into safe mode to pull all the files back out of the quarantine as Symantec wouldn't clean them (*and in some cases, I had to copy VPC32.EXE from the server share as it was quarantined!*). I then had to boot from BartPE and run a command line version of McAfee which could clean the version. McAfee basically saved my bacon and I will recommend McAfee to all techs I meet now!

A call to Symantec tech support yielded equally disappointing results regarding our problem. "All we know is what is on our web site". I'm glad we pay yearly maintenance to these guys, because it certainly seems to be helping, **NOT!**

– Soli Deo Gloria

Merry Christmas!

DECEMBER 25, 2006

CATEGORIES: MISC

Hopefully everyone is doing well out in the world. I would like to thank all the readers who visit my web site. Traffic has gone up from 50 unique visitors per day in January to over 200 unique visitors per day in December. The goal of this site is to spread as much knowledge as possible and to document what I and others have learned. Therefore, I would like to read your own “in the trenches” stories and post them here...something cool, something weird, something complicated, whatever you found interesting in your own work as a technician. Send them to web at leinss.com with the subject “Readers Story”. Maybe you found an interesting blog post of how someone got a 1985 DOS program to work in Windows Vista: send that in too!

For next year I hope to have continuing coverage on Windows Vista and how to use it (*and more importantly, how to fix it*). Of course, more “*in the trenches*” stories that anger Microsoft personnel will be in order (*at least Windows Vista does HAL detection so Michael Niehaus can't chastise me for forcing HALs anymore. :O*)

Last, but not least, the reason for the season we celebrate each year:

For of Him, and through Him, and to Him, are all things. To Him be the glory for ever! Amen.
(Romans 11:36)

Sola Scriptura

Sola Gratia

Solo Christo

Sola Fide

Soli Deo Gloria

Repackaging Program Installations

JANUARY 5, 2007

CATEGORIES: TECH TIPS

I recently made a MSI file for taking the Novell client off of my company's workstations. Repackaging program installations is challenging and fun. It can also be down right dangerous. I discovered repackaging a long time ago. There use to be a program called PictureTaker made by Lanovation that was sold to the consumer market for \$25. Eventually, it was taken off the market and limited to the grasps of the corporate world. What is repackaging? It is the art of taking a system snapshot, then installing the program you want and then taking another snapshot. The repackaging software takes the differences between the two snapshots and makes a package. You can edit resulting package by adding/removing several registry keys and or files.

Microsoft has long been providing these tools, starting with NT4 with their Resource Kit utility named sysdiff. With Windows 2000, Microsoft outsourced the effort by licensing WinInstall 2000 LE from Vertias (now OnDemand). You can find WinInstall 2000 LE on the Windows 2000 Server CD at **VALUEADD3RDPARTYMGMTWINSTLE**. Microsoft also partnered with OnDemand software once again and offered up WinInstall 2003 LE for free. Microsoft did not put it on the CD this time, but instructed users go to to [this page](#). This is a cached version of the original page. Unfortunately, OnDemand took down the original free version and instead have a version that sells for \$49.95. Fortunately, through the powers of Google file search, I located the original version and put it up on my web site [here](#).

There's yet another way to get your hands on a pretty nice packager called the [FLEXNet AdminiStudio SMS Edition](#). This is a free version for users of SMS Server 2003. The installer looks for the presence of a SMS server, however, so you will need a live SMS 2003 installation for this to work. I admit, this will involve a bit of work on your part, but you can make it possible if you have VMware or Virtual PC. First, grab a eval copy of [Windows Server 2003](#) if you do not have a copy. Next, get a eval copy of [SQL Server 2000](#). Finally, get a eval copy of [SMS Server 2003](#). Install it all in one VM and boom, you have yourself a live SMS server. Now you install the copy of Administudio. Yes, you'll need to request a serial number from MacroVision.

So, what are the benefits of repackaging? Simple: time and effort! Take the simple example of Winzip. Say you want to have all the computers in your company to have WinZip. You have 500 computers, so you go to Corel (yes, Corel now owns WinZip, what a strange world we live in!) and

get a site license. Now you want to have it on each of your 500 machines. You can manually walk to each machine to load WinZip or you can repackage the install. With repackaging, you can make the installation unattended, even if the original installation program didn't support unattended installs. How cool is that?

That's not to say that repackaging is not without problems, as described in this [Microsoft knowledgebase article](#). In testing the deployment of PowerArchiver through SMS 2003, every time I logged in as a new user, a new icon was created on the desktop in the All Users folder! So care must be taken to make sure that your deployment works before you start pushing it out to everyone. Repackaging for the home user can save tons of time. Take my example: I make a baseline image for my home PC. I then repackage all of my commonly used applications. That way, I can keep a clean baseline image and then just start popping programs back in after laying down the image if I so choose. If I get a new PC, I make a new baseline image and again just pop back the applications rapidly by clicking on each MSI file (*I'm of course negating the fact that you must spend time creating the packages and that programs outdate themselves, but hopefully you can see the advantages*).

– Soli Deo Gloria

Mark Minasi writes on Windows PE

JANUARY 15, 2007

CATEGORIES: MISC

Mark Minasi's monthly newsletter covers Windows PE this month. He shows how to create a PE disc through the command line for us techies, but there's actually an easier way through the BDD 2007 to make a Windows PE CD. I've successfully deployed Windows Vista Enterprise via the BDD 2007 and now I am trying my hand at getting it to work through SMS 2003. I hope to have a guide up shortly: some of the tools such as the BDD 2007 are still in the release candidate stage, including the ACT 5.

– Soli Deo Gloria

Windows Vista Installation and Deployment Overview Released!

JANUARY 20, 2007

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Good news! My guide on installing and [deploying Vista using the BDD 2007](#) has been released! There is too much content to fit into one blog entry, so I'm just linking this posting to the article. You'll notice the format of this web page is very different from the rest of my site. This is because I created the document in Microsoft Word and Adobe GoLive does not want to import any of the formatting at all. I had to go back to Frontpage 2003 and bring the content in that way.

Johan Arwidmark has also updated his guides for the BDD 2007 over at www.deployvista.com, go check it out!

– Soli Deo Gloria

Windows Vista Installation Methods – Part Deux

JANUARY 23, 2007

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Mark Minasi is back, this time going over [how to install Windows Vista using an unattend file](#). I really like the conversational, “in-the-trenches” style he uses to explain things, so I highly suggest you check it out!

– Soli Deo Gloria

Further Success with Vista Deployment

JANUARY 25, 2007

CATEGORIES: OPERATING SYSTEM, TECH TIPS

For some magical reason, I re-tried the settings at blogs.msdn.com/winre for installing Windows RE onto the C: drive and I got it working! A second partition is not necessary. Just copy boot.sdi and SetAutoFailover.cmd (*found in the WAIK*) and winre.wim to the root of C:. Then do a RunAs administrator on a command prompt and run the script SetAutoFailover as follows "SetAutoFailover.cmd /target C: /wim /nohide". Reboot and viola, Windows RE is now in your F8 choices! Now when that remote laptop user calls you can rest a little easier (*think of spyware cases...just hit F8, pick "Repair your computer" and restore your PC to an earlier time dear user!*).

I've successfully gotten SMS 2003 ZTI to push out Windows Vista using Johan's instructions at www.deployvista.com with a few tweaks. Updates will be posted to my Vista deploy page in the next few days.

– Soli Deo Gloria

Windows 386 Promotion Video

JANUARY 28, 2007

CATEGORIES: JOKE

[Here's a promotional video](#) for Windows 386 (*basically, Windows 2.0 optimized for the 386 architecture*). Each "VM" has a blazing 64KB of memory!

-Soli Deo Gloria

Review of the book “The Old New Thing”

FEBRUARY 1, 2007

CATEGORIES: REVIEW

Having been called to jury service recently, I decided to read a new book that I just got from Amazon called “The Old New Thing: Practical Development Throughout the Evolution of Windows” by Raymond Chen. Raymond Chen is one of the original software developers on the Microsoft Windows operating system. The book is an interesting collection of Raymond’s blog entries with a few augmentations thrown in. Several chapters are dedicated just to programming propeller heads, but there’s enough interesting stories of how Windows operates to keep the general audience interested.

One of things the book acknowledges is how Microsoft “works around” program incompatibilities by coding “fixes” directly into the operating system. If you remember about 2 years ago, 20% of the source code for Windows 2000 was accidentally leaked. This [article](#) details some of the things found in the source code. This fact alone validates that the Windows 2000 source code posted is valid. It also explains why Windows has so much “bloat” in it.

So why not block applications with bad programming techniques? According to Chen, when a user upgrades their operating system and their program stops working, they blame Microsoft and not the software vendor. Why wouldn’t they? The user has no idea that their vendor is using sloppy programming. In order to secure sales, Microsoft will bend over backwards to provide application compatibility to the point of incorporating the fix into their operating system directly.

The responsible thing to do of course is to notify the company that made the software and inform them of the fix. Microsoft (*I’m equating Chen with Microsoft since he clearly has been entrenched in the Microsoft culture*), however, makes the excuse that the company may have gone out of business or may not be willing to issue a fix. Why not issue just a hotfix for that company through the PSS? Microsoft holds back certain hotfixes from the general public and holds them hostage in the PSS. Only if you are willing to pay a fee and or deemed worthy of the documented hotfix is it released to you. Why should it be any different with sloppy programming fixes? Why do I need a fix for an application *I* don’t use bundled into operating system *I* use?

Microsoft has somewhat rectified the situation using [Application Compatibility shims in Windows XP](#). However, this begs the question: what else is being injected into the Windows

code base? From www.kickassgear.com/Articles/Microsoft.htm:

Microsoft's David Cole emailed Phil Barrett on September 30 1991: "It's pretty clear we need to make sure Windows 3.1 only runs on top of MS DOS or an OEM version of it," and "The approach we will take is to detect DR DOS 6 and refuse to load. The error message should be something like 'Invalid device driver interface.'"

Microsoft had several methods of detecting and sabotaging DR-DOS with Windows. One was to have Smartdrive detect DR-DOS and refused to load it for Windows 3.1. There was also a version check in XMS in the Windows 3.1 setup program which produced the message: "The XMS driver you have installed is not compatible with Windows. You must remove it before setup can successfully install Windows." This was not true, but rather, was an attempt to undermine the competition.

Brad Silverberg, the Microsoft exec who had been responsible for Windows 95, emailed Jim Allchin (now Senior Vice President of MS) on September 27th 1991: "after IBM announces support for dr-dos at comdex, it's a small step for them to also announce they will be selling netware lite, maybe sometime soon thereafter. but count on it. We don't know precisely what ibm is going to announce. my best hunch is that they will offer dr-dos as the preferred solution for 286, os 2 2.0 for 386. they will also probably continue to offer msdos at \$165 (drdos for \$99). drdos has problems running windows today, and I assume will have more problems in the future."

Jim Allchin replied: "You should make sure it has problems in the future. :-)".

Andy Hill emailed David Cole, Windows group manager: "Janine has brought up some good questions on how we handle the error messages that the users will get if they aren't using MS-DOS. The beta testers will ask questions. How should the techs respond: Ignorance, the truth, other? This will no doubt raise a stir on Compuserve. We should either be proactive and post something up there now, or have a response already constructed so we can flash it up there as soon as the issue arises so we can nip it in the bud before we have a typical CIS snow-ball mutiny."

Cole replied to Hill: "Let's plead ignorance for a while. We need to figure out our overall strategy for this. I'm surprised people aren't flaming yet, maybe they won't." Cole also sent an email to Silverberg suggesting a less severe message be used when DR DOS

was detected: "A kind-gentle message in setup would probably not offend anyone and probably won't get the press up in arms, but I don't think it serves much of a warning. BillP made an excellent point, what is the guy supposed to do? With a TSR, the solution is to just remove it. With DR-DOS, or any others, I doubt the user is in a position of changing. He will no doubt continue to install. When he finds problems, he will call PSS. We will get a lot of calls from DR-DOS users."

"Perhaps a message in the phone system for Windows. It would say something like 'if you are not using MS-DOS or an OEM version of MS-DOS, then press ##'. Then give them the message." Silverberg replied: "What the guy is supposed to do is feel uncomfortable, and when he has bugs, suspect that the problem is dr-dos and then go out to buy ms-dos. or decide to not take the risk for the other machines he has to buy for in the office."

For more trips down "OS memory lane", check out Toastytech.com in addition to Raymond's book. Raymond Chen's blog can be found [here](#).

– Soli Deo Gloria

Clean installation of Windows Vista with Upgrade Key

FEBRUARY 2, 2007

CATEGORIES: TECH TIPS

It appears that doing a clean install with a Windows Vista Upgrade DVD is not so easy. In past Windows versions dating back to at least Windows 3.1, all you needed to do is provide a qualifying product media to continue. For Windows 95, you could easily trick it. All it did was look for a file named win.cn_, which is one of the files on the first disk of Windows 3.1. Some clever people figured out that if you just made an empty file named “win.cn_” and pointed Windows 95 to that, it would continue the install.

Well, it appears that Vista really wants an operating system installed, Windows 2000 or Windows XP to be exact. People figured out however that you can wipe the disk, install Vista and then do an in-place upgrade of that Vista install with your Vista upgrade key. Instructions detailed below:

www.dailytech.com/Workaround+Discovered+For+Clean+Install+With+Vista+Upgrade+DVDs/artic

Which, technically means you could buy an upgrade version and be able to install it as a full OS which some people are making a really big deal of. Who the heck **DOESN'T** run Windows 2000 or Windows XP? The Ultimate upgrade goes for \$259 and the OEM version goes for \$199. *Hint: Microsoft doesn't care about this loophole.*

– Soli Deo Gloria

Bill Gates on The Daily Show/Spyware Crazyness

FEBRUARY 2, 2007

CATEGORIES: MISC

[Bill Gates touting the virtues of Windows Vista with John Stewart – Part 1](#)

[Bill Gates touting the virtues of Windows Vista with John Stewart – Part 2](#)

[Don't try this at home.](#)

Update (3/26/07): The Bill Gates video was removed from YouTube for copyright infringement, but Comedy Central has put the video on their web site, so the link has been updated

– Soli Deo Gloria

Vonage Stinks!

FEBRUARY 6, 2007

CATEGORIES: MISC

Well, at least the router they gave me does. The Linksys RT31P2 is the biggest piece of rubbish I've had to deal with in a long time. Tonight, my Internet connection wasn't working and it took me 2 hours to figure it out. The RT31P2 periodically stops DNS resolution which results in my phone service and the Internet to stop working. If I use an external DNS address on my PC, I can continue working on the Internet just fine. It isn't until I bounce the router does it start doing DNS resolution again.

Now the router refuses to change from its default range of 192.168.15.x to 192.168.1.x which it had been for 11 months. Nothing on my network changed: **NOTHING!** I had to go around to all my devices and change them to 192.168.15.x addresses, what a joke! When I did change it to 192.168.1.1, I would get one ping out of the beast and then nothing. If I power cycled the beast, I would get one ping packet back from 192.168.1.1 and that was it. Leaving it at 192.168.15.1, however, seems to calm the beast.

Hopefully, it's just this router and not the Linksys brand. I've had a Linksys BEFW11S4 for over 2 years with very little problems. I rarely have to bounce it, but with Vonage router it's a weekly thing. Give me back AT&T POTS!

Update (early March): After threatening to cancel their service unless they sent me a new router, they sent me a new Linksys RTP300 router and I have not any further problems after installing it. So Vonage has redeemed themselves!

– Soli Deo Gloria

Gmail Opens Its Doors to Everyone

FEBRUARY 15, 2007

CATEGORIES: MISC

Google has finally released [Gmail](#) to the masses. I tried Gmail a few years ago from an invitation from a friend, but I quickly gave it up due to [privacy concerns](#) and spam. The fact is you can get free e-mail access anywhere, but getting one that is reliable and spam free is quite a tall order. Many companies and forums flat out refuse to accept *hotmail.com*, *yahoo.com* and *gmail.com* e-mail accounts for account registration as these providers have a bad reputation. Who will take you seriously if you have *monkeyboy66@hotmail.com* as an e-mail address on your resume?

These services also fail to provide IMAP or HTTPS connections for software based e-mail programs unless you pony up money for an upgraded account. Gmail, as far as I know, provides neither. Since these services are free, uptime is not guaranteed, nor is continuation of service. If you want to find a reliable e-mail provider, check out [Emailaddresses.com](#) and its forums.

– Soli Deo Gloria

Virtual PC 2007 Released

FEBRUARY 20, 2007

CATEGORIES: MISC, TECH TIPS

The final version of Virtual PC 2007 has been released and it's free!

– Soli Deo Gloria

Disable Enforced Driver Signing on Windows Vista x64

FEBRUARY 27, 2007

CATEGORIES: TECH TIPS

Since Windows Vista RC2, Microsoft has removed the option from the F8 menu to disable driver signing on Windows Vista x64. However, several people recently noted that running “**bcdedit.exe -set loadoptions DDISABLE_INTEGRITY_CHECKS**” from an elevated command console disables the driver signing.

Power to the people!

(Sorry Michael Niehaus)

– Soli Deo Gloria

Combating Image Spam

MARCH 1, 2007

CATEGORIES: TECH TIPS

Spammers are ingenious little devils. One piece of spam that always has been near impossible to filter out is image spam. Quite simply, image spam is where they make an image with the spam message inside. Since most spam analyzers only look at text, not images, you get the spam in your mail box. To combat this type of spam, you need an e-mail service that will analyze images for spam. That service should also let you dictate where that e-mail goes based on the results that it finds. Tuffmail fits the bill on both accounts. Let's take a look at an e-mail that I get daily to one of my e-mail addresses:

• Lowest Price Guarantee • Fast Delivery

For Free Information
Do not click, type in your browser www.SimpleRX.org

Viagra	100 mg \$2.00	Cialis	20 mg \$2.00
Viagra ST	100 mg \$2.89	Cialis ST	20 mg \$2.99
Valium	10 mg \$2.00	Antivan	2 mg \$1.90
Xanax	1 mg \$2.00	Ambien	10 mg \$2.00



Do not click, just type www.SimpleRX.org in a address bar of your browser, then click enter

hard for her to have the house littered up with all sorts of rattletaps a word, i have a feeling that i am an explorer and an everlastingthe sisters lit their lamp and a little girl, of six or seven, came roaring in. she stopped at but since father went away and all this war trouble unsettled us, b: the ink should the shabby, silk bonnets and dirty, flounced gowns. such fun as we

way, if we must," said emma davenport, a quiet, bright-eyed girl, who was called "i like that boy first-rate, and i guess he likes me, in the box, and each pill i at: gee, i could've they thought the great wizard would send for them at once, but he did not. to pack for the boys. was intended i should live long. i'm not like the rest of you. i never

was intended i should live long. i'm not like the rest of you. i nevernt speak apron, bess vanished from the room, seeming to take all the light witho himse shades, so we paint ours any color we like. it's a great comfort to have. for in the yard stood the duke of wellington, so named in honor of his is absent tems from behind, and they got along better. soon they rolled the lion out of

any in the sea as she thanked her piece of music. they began to know the relationship between music and theishould n't enjoy them if i did n't have a fine he lay moanin' with homid pain, and lookin' at me with them lovin' eyes "a what?" would change. finally a chance came when my parents were in- vited to used to do, when he planned his boyish pranks. fears which had haunted the cell for hours, dismayin dan by their power, that they might go to play with free minds. so the "lilaoparties," asrefuse the new bring any more sorrow to you and shame to myself. i'd like to stay her gift: 'a truly toman way of talkin things easy. i hope you told gestatulating wildly to mrs meg to set her cap straight. on. i hate to come in in the middle and smiled on her, flattered and praised, whispered agreea often visible in to assure himself that the hard times were over, and then he added the right said polly to herself as she opened her window one morning and the get dinner, it was harder still to go begging for it and the fourth, seem to have life all vork and no play. presently phobe seemed to you "has he said anything more lately?" i want to live in a place where i can conveniently enjoy the material i'm your man, if the other fellows agree. we can't famous name. to the great delight c cultivated eye the soul of beauty was often visible inobservation. the story was soon told, and after a look at in the tiny cottage which stood near mrs. min by the time they make in the great race," answered the second"then i must have a lobster. let us go back and enjoy it together." called away to see an old

Do you notice the text on the bottom of the e-mail? If I take parts of this text and throw them into Google, I get some interesting results. "*emma davenport, a quiet, bright-eyed girl*" comes from Chapter 11 of the book "An Old Fashioned Girl". "*bess vanished from the room, seeming to take all the light with*" comes from Chapter 2 from Parnassus. The spammer is adding legitimate text at the bottom of his e-mail to make his e-mail less "spammy" for Bayesian filters. Bayesian filters look at the whole e-mail and give it a score based on how many spam words are contained in the e-mail. By adding more legitimate, non-spam like text, the message gets a lower spam score. Clever, very clever.

Looking at e-mail header at webmail.tuffmail.net, I found this under the line X-Spam-Report:
 X-Spam-Report: Content analysis details: 0.0 BAYESSCORE 0.502318 0.0 BAYES_50 BODY:
 Bayesian spam probability is 40 to 60% 1.1 EXTRA_MPART_TYPE Header has extraneous
 Content-type:...type= entry 0.1 FORGED_RCVD_HELO Received: contains a forged HELO 4.0
 RCVD_HELO_IP_MISMATCH Received: HELO and IP do not match, but should 1.5
 RCVD_NUMERIC_HELO Received: contains an IP address used for HELO 4.1 FUZZY_OCR
BODY: Message contains an image with common spam text 0.0 HTML_MESSAGE BODY:
 HTML included in message 0.0 TM_IMG_ATTACH FULL: Email has a inline image 0.8
 SARE_GIF_ATTACH FULL: Email has a inline gif 2.0 RCVD_IN_SORBS_DUL RBL: SORBS: sent
 directly from dynamic IP address 1.9 RCVD_IN_NJABL_DUL RBL: NJABL: dialup sender did non-
 local SMTP 1.1 MY_CID_ARIAL_STYLE SARE cid arial2 style 0.7 MY_CID_AND_STYLE SARE cid
 and style 0.7 MY_CID_AND_ARIAL2 SARE CID and Arial2

Most of that is probably Greek to you, so I highlighted the important part we can filter on. The analyzer engine found an image with common spam text, including ambien and price. Therefore, we can make a rule like this in Tuffmail's IMP4 webmail interface:

Filter Rule

Rule Name:

For an incoming message that matches:

All of the following Any of the following

X-Spam-Report Contains Message contains an image with common spam text Case Sensitive

or X-Spam-Report Contains HELO_DYNAMIC_DHCP Case Sensitive

or Select a field

Do this:

Delete message completely:

Stop checking if this rule matches?

Viola! Good bye image spam!

– Soli Deo Gloria

The Final Chapter on Windows XP Images

MARCH 3, 2007

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Recently, I rebuilt my company's standard Windows XP Ghost image and decided investigate the HAL issue once again. I wrote how to make [universal images by forcing the APCI HAL](#). Perhaps, however, you are a "best practices" kind of fellow and rather not force an APCI HAL, yet want a universal image. With a little work, you can get there. One thing I recently noticed is that the HAL is not changeable in Windows XP from the device manager. In Windows 2000, you could change the HAL to anything you wanted, but I guess Microsoft thought that feature was too powerful for us. In Windows XP, the only way to change HALs is:

1. Specify one in sysprep.inf
2. Do a Windows repair on the PC in question

There's two little tricks you can use to work around this. The first one I found is from the [Jimmy Bondi in the VMware forums](#). In C:\windows\inf\hal.inf, change the section to the following:

```
%E_ISA_UP.DeviceDesc% = E_ISA_UP_HAL, E_ISA_UP, MPS_UP, MPS_MP,  
ACPIPIC_UP, ACPIAPIC_UP, ACPIAPIC_MP ; Standard PC  
%ACPIPIC_UP.DeviceDesc% = ACPIPIC_UP_HAL, ACPIPIC_UP, ACPIAPIC_UP,  
ACPIAPIC_MP ; ACPI PIC-based PC  
%ACPIAPIC_UP.DeviceDesc% = ACPIAPIC_UP_HAL, ACPIAPIC_MP, ACPIAPIC_UP,  
ACPIPIC_UP ; ACPI APIC-based PC (UP)  
%ACPIAPIC_MP.DeviceDesc% = ACPIAPIC_MP_HAL, ACPIAPIC_MP, ACPIAPIC_UP,  
ACPIPIC_UP ; ACPI APIC-based PC (MP)  
%MPS_UP.DeviceDesc% = MPS_UP_HAL, MPS_UP, ACPIAPIC_UP ; MPS UP PC  
%MPS_MP.DeviceDesc% = MPS_MP_HAL, MPS_MP, MPS_UP, ACPIAPIC_MP,  
ACPIAPIC_UP ; MPS MP PC
```

This ingenious situation basically tells Windows: "hey, you can use any driver for this specific HAL". Now you can go into the device manager, right click on the HAL and do an update driver. The PC will require two reboots after doing this.

The other thing you can do is just leave your image configured with a APCI Uniprocessor HAL, which is newer than just the plain old APCI HAL. If the system refuses to boot, boot into BartPE and copy over hal.dll, ntoskrnl.exe and ntkrnlpa.exe from a system already running an APCI HAL into C:\windows\system32. Reboot and viola, the system boots! This latter method requires the work of a semi-skilled technician, so pick the method accordingly to your organization's needs.

I've also found that you can change the IDE drivers in the image to "Standard Dual Channel PCI IDE Controller" in the device manager before closing the image and your image will boot on pretty much any hardware. You can then add the correct IDE drivers later for better performance. Using this "hack", your image will still change the IDE drivers to the "correct" ones during the mini-setup if you have them defined in . This might come in handy if you want to image an older PC, yet do not want to update and recreate your image just for one PC.

– Soli Deo Gloria

Response to “Windows Vista: I’m Breaking up with You”

MARCH 4, 2007

CATEGORIES: MISC, OPERATING SYSTEM

Update 3/13/07: Chris Pirillo recently wrote an article for the magazine Computer Power User. In this April 2007 issue, Chris wrote an article called “An Open Letter to Jim Allchin”. In this [article](#) he states:

*“I’ve been using Vista pretty much exclusively for the past few weeks and have had my fair share of ups and downs with it. **I haven’t been compelled to switch back to XP (or OS X, for that matter), so take that for what it’s worth.**”*

I guess it’s not worth much, as Chris had a change of heart sending droves of people to his blog stating: “Windows Vista: I’m Breaking up with You”. So Chris, which is it? I guess Chris hates chocolate ice cream one week and then loves it the next.

Original blog entry continues...

[Chris Pirillo](#) recently wrote an article about why he’s sticking with Windows XP. He even made a 53 minute video about it. Sorry, I can’t stomach watching that, but he did list out the problems he had with Vista. So, let me take them point-by-point to calm his FUD:

1. My scanner doesn’t really work (Hewlett-Packard Laserjet 3052). HP hasn’t caught up with support yet, and software updates won’t be available until SP1 time-frame. The software works like a charm in XP – amazingly well, as a matter of fact.

Hewlett Packard has been notorious for slow driver support for new operating systems. Here’s a [thread from Google Groups](#) back in the year 2000 about how HP wasn’t supporting their scanners when Windows 2000 first came out. HP was also trying to charge their users \$20 for upgraded software for the Scanjet 4200 so it could be used on Windows 2000. Instead of breaking up with Windows Vista, maybe you should break up with HP for their crappy support?

My Agfa scanner did not work with Windows Vista off the bat either: I had to use Vuescan to get it to work. Since my scanner is 7 years old, I think this is fair.

2. Windows Movie Maker crashes on a regular basis.

Can't say either way whether he has a point or not. Did you submit your feedback to Microsoft Chris?

3. My IPFax software doesn't work (the driver will likely never be updated to be Vista-compliant). Never, EVER caused me a problem in XP. I need this software to work, and dual-booting to use this is not an option.

Again, not a Windows Vista problem. It's a manufacturer problem.

4. I still can't get my Lifecam to work, but wound up purchasing the vastly superior Logitech QuickCam Ultra Vision instead (which puts Microsoft's new webcam software AND hardware series to shame).

Yet again, not a Windows Vista problem!

5. On the same machine (AMD Quad FX), XP trumps Vista in terms of performance. I don't have specific benchmarks on hand, but I can tell you the difference is quite palpable. This is even with most of Vista's eye candy tuned to a dull roar. We'll see if it runs just as quickly when everything's reinstalled there. I only discovered this after rebooting to try my scanner in XP – blazing differences, similar tasks.

Shock, horror! You put a newer operating system with more features and programming code on your PC and it runs slower? Well, so does mine. Again, software has to be written to take advantage of your Quad architecture: you are likely not even tapping into all that power you have. For the record: AMD Quad is not really 4 cores on one chip: you have two processors with dual cores on them.

You also need newer hardware to see some of Vista's performance improvements such as ReadyDrive. If you buy new hardware that is Vista engineered, your experience will be faster than that of Windows XP's.

6. NVIDIA chipsets and video cards. Need I say more?

Probably, because not everyone reads Vista message boards on a daily basis. If you're talking about what I think you are talking about, this is actually a bug within the NVIDIA NForce chipset that Microsoft is working around in their software code. Of course, all of the longhorn news groups detailing this have long since pulled by Microsoft, however I did find this news article from the [Techreport](#):

*Last week, we [learned](#) about a compatibility problem with Nvidia nForce3-based motherboards involving Windows Vista, ATI graphics cards, and dual-core processors. Nvidia informed us that its only chipsets certified for Vista were the nForce4, nForce 500, and nForce 600 series, **suggesting that nForce3 users suffering from compatibility problems in Vista would have to suck it up and either stick with Windows XP or buy new hardware.***

However, the company seems to have changed its mind somewhat. Nvidia Platform Products PR Manager Bryan Del Rizzo has e-mailed us saying, "There is a known issue with ATI AGP cards and nForce3 and Vista. This is currently being looked into and will most likely be resolved with a MCP driver update." Del Rizzo adds that nForce3- and nForce2-based systems can run Vista using built-in Microsoft drivers and third-party audio chipset drivers. There is one notable exception, though: storage support. Nvidia RAID is just plain not supported, and Del Rizzo says there are "known Vista issues with some ATAPI devices."

Yet again, not a Windows Vista problem, but a manufacturer problem! I run straight Intel hardware and I'm not having any issues.

7. I simply can't get to my OS X machine from Vista (or mount a WebDAV server).

Doesn't OS X do file sharing via HTTP services? How is this a Windows Vista problem?

8. Copernic Desktop Search, a far superior desktop search client to Microsoft's, either doesn't like Vista or Outlook 2007 – not sure which, yet. Either way, I can't run it right now – and the Windows Desktop Search tool is still as lame as ever (sorry, Brandon). I'll miss the new Start Menu, but I think there's similar third-party software that'll keep me happy in the meanwhile.

I used Copernic long before Google came on the scene and was not impressed. I'm not quite fond of the file searching in Windows Vista either: I usually drop down to a command console to do my file searching. However, the text based searching in Windows Vista is awesome. Plug in a keyword and it brings up all of the files, e-mail messages , etc. with that word. What's so special about Copernic?

9. Explorer keeps losing my view settings. THIS IS DRIVING ME UP THE FARKING WALL! Now, I realize that XP suffers from this problem as well, but it's never been this bad. There are so many new options that it's difficult to reset each window's view every time – including column headers, which are now permanently stuck on “Tags” and “Date Taken” (even though I may not be in a folder with objects supportive of these fields). Yes, I realize this problem stretches back centuries – but it seems to have gotten worse, not better.

Not a Windows Vista issue: I don't have that issue on any of the PCs I run, whether it be Windows Vista or Windows XP. Now, the idea to remove “Date Modified” from the explorer view was pretty retarded: I'll give you that. However, I've been able to force a view with “Date Modified” for all my folders. In case you didn't know: setup a view that you like in Windows explorer. Then go to Organize>Folder and Search Options, click on the View tab and then click “Apply to Folders”, then “Yes” to change all the folders to that view. Simple, really.

10. My workaday software still seems to suffer from weird quirks now and again. I really don't have the time or patience to wait for each developer to catch up just so I can go on living my life. All these little annoyances are starting to add up to one major headache. Instead of detailing each one separately (and extending this list exponentially), I'm just wrapping all of 'em together into one point.

So your point is that you are using software by companies that are not interested in supporting their product for Windows Vista, so dump Windows Vista? Your headline is just an attention grabber: every operating system release is going to have issues with older software and hardware, especially with system specific software like disk defraggers, antivirus, video, etc. Of course you'll need to work through these issues.

I've had a few application issues on my own system with Windows Vista: sound and scanner drivers. With a little research and tweaking, I got all of them working. These manufacturers had

plenty of time during the Windows Vista beta to develop compatible software. Why develop compatible software for older products when you can just get the customers to buy new hardware and software? Do you want Microsoft to re-write Hewlett Packard's scanner software?

The fact is that Windows Vista (*and every Windows version proceeding it*) is very compatible. Microsoft even works around vendor software bugs by using application shims. I've tested 30+ company core applications and most work with little or no problem on Windows Vista.

– Soli Deo Gloria

Windows Activation Attacked Again

MARCH 10, 2007

CATEGORIES: MISC, OPERATING SYSTEM

Amazingly, pirates have once again claimed victory over Windows Vista's activation requirements. The hack centers around SLP (*System Locked Preinstallation*) or OEM copies. Basically, if you have the "Dell edition" of Vista it will not require activation on Dell hardware. Well, some crafty people have figured out that by editing BIOS strings you can make one system look like a Dell or a HP. In yet another method, someone wrote a driver to emulate various BIOS setups. There is something called a SLIC table in the APCI standard for BIOS setups that tell programs what hardware they are running on.

Appears from the comments I read that it works...that is until Microsoft releases a "security update"!

It appears that Vista's anti-piracy measures only lasted a month before being defeated. I have to say I am amazed at the speed and diligence of the pirates!

– Soli Deo Gloria

Utility Review: SWI – System Information for Windows

MARCH 21, 2007

CATEGORIES: REVIEW, TECH TIPS

AIDA32 use to be my dearest love for system information, until it turned into Everest Home and then it vanished from the freeware scene into payware. The Ultimate edition is \$30 up front, with \$20/year maintenance to get updates. They recently offered an “Engineer” edition that is \$199/year. However, maybe you want something that is freeware to check your own system or some elses, but you want the power of Everest. Introducing: SIW!

The web page for the program is [here](#) and is cleverly laid out as a Windows desktop. The author goes into a lot of detail into each feature with screen shots: very classy! The program is one executable: no installation, no DLL or INI files. I like the simplicity very much. Now some programs will just give you very generic information (*ahem, Belarc Advisor*), but SIW goes in depth like Everest does. The first page I go into is the Operating System tab. My Windows Vista product key is there: very nice! However, it only seems to be able to determine the activation status on Windows XP. When I ran it on Windows Vista, it was completely missing. Clicking on Licenses brought up my keys for Office 2003 and 2007: impressive. It does, however, misidentify my Office as being the Enterprise edition. It’s actually a copy from Technet using a retail key, but it’s close enough.

Upon clicking on Domain Groups, I was presented with all the groups in my company’s AD structure. That’s a bit unsettling given that I have regular user access to AD. Likewise, clicking on Domain User Accounts gives me a listing of all the AD user accounts in the DS and which groups those accounts are in, including Domain Administrators! I’m very tempted to try running this utility on another network to see if would pull up the same information.

Clicking on the Secrets tab makes my jaw drop: all of my Firefox passwords are presented to me in cleartext! VNC passwords are also presented here and those are supposed to be encrypted! Wow, I’m really starting to like this utility! Clicking on PCI under Hardware presents a listing of information regardless of what driver is installed. That feature alone makes this program a keeper and definitely a replacement option for Everest. SIW is unable to get the SPD information of my DIMMs: Everest has no problem. SIW is able, however, to identify the size in each bank of memory.

Embedded within the program is a program called Eureka! This allow you to reveal passwords behind asterisks. I tried it on both Windows Vista and Windows XP and it does work! Yet another reason not to save passwords in Internet Explorer or Firefox. Oh look, an embedded Windows 9x password cracker! Move over Cain and Abel (*if you ever tried cracking PWL files you know what I mean, wink, wink!*) There's even ping, trace and network built in to this rig, along with remote execution goodies. **Again, all of this is in one little 1.4MB file!**

You have to remember that SIW is written by a freelance programmer in his spare time and does not have the resources of a corporate entity. For that, I have to say he's done one hell of a job making this thing! Now if you want to use this for commercial purposes, there are licenses that you need to purchase. For a technician license it is \$75 for unlimited use. Very reasonably priced vs the perpetual \$200/year that Everest charges.

I give this program my highest rating and recommendation:



Do you have a utility that you find useful in your tech work? Send your information on it to [web..\(at\)..leinss.com](mailto:web..(at)..leinss.com) and it could be featured here!

– Soli Deo Gloria

Free Remote Control Via the Web!

MARCH 23, 2007


CATEGORIES: REVIEW, TECH TIPS

Here's a company doing something really slick: giving away remote control services over the Internet for FREE! Now it is free for only personal use: if you use it for commercial purposes, you need to purchase a license. Each session can be 30 minutes in duration and you are allowed to use 10 hours of the service per month. Now you can help all your friends without leaving your house!

Setting up the remote control session is dangerously simple: download the program on your PC. Your party can either download the client or you can generate a URL within the program you have on your PC to give them. Basically, the program connects directly back into their service and drives the whole experience. The URL method is slick because the end user just has to enter a URL: the web site delivers a Java based client so no installation on their part is necessary.

If you go for the free license, you are obligated to recommend the product to 7 associates or link an ad to your site. I have opted to link an ad to my blog below since it gets 200+ visits a day.

Update (4/30/07): It gets even better...they removed the session limit, bumped the time per month from 10 hours to 25 hours and you do not have to register to use the software anymore!

 [TeamViewer Remote Control](#)
[Free Remote Control](#)

Billy Mays Oxiclean Outtakes

MARCH 30, 2007

CATEGORIES: JOKE

[Click it, you know you want to!](#)

Rootkits: A New Form of Malware

APRIL 1, 2007

CATEGORIES: SPYWARE, TECH TIPS

Recently, two of my “high risk” Internet users caught a nasty spell of malware. How nasty? Try rootkit nasty! Rootkits go above and beyond spyware by replacing system files and concealing themselves from system utilities. The first PC had a combination of spyware named TSPY_QQPASS.BUY and a rootkit named Greypigeon. Both PCs had the latest version of Symantec Corporate Antivirus with the latest virus definitions.

I will once again voice my displeasure with Symantec. They claim that SAV does greyware detection and therefore you should disable Windows Defender if you are running Windows Vista. However, this is the second time in 3 months that Symantec has completely failed us. It did detect the spyware on the first PC, but it was unable to clean it. It was also impossible to unload or terminate SAV to clean off the virus, as it pops in your face every time you try to delete a file. Removing the spyware was impossible: I spent over 2 hours trying to get it off only to have the executables keep returning. I ended up doing a System Restore within Windows XP to restore startup sanity and then cleaning up the dormant spyware files by hand (*neither Symantec nor McAfee would identify the majority of the bad files: I ended up Googling some of the files I kept seeing reappear like “gg.exe” and “zz.exe” and then backtracked other filenames mentioned in the article like newinfo.rnk, then deleted those one-by-one*).

The spyware was clever, quite clever actually. Most spyware files are dated with the date they infect the system. However, this spyware was pre-dated back to August 2004, along with most of the other legitimate Windows files. Someone went through a lot of trouble to keep this stuff hidden, as this is the date that service pack 2 was released for Windows XP, therefore most legitimate files are dated 8/4/04. The spyware also took on legitimate looking Windows names, such as rpcs.exe and svchost.exe. Not being digitally signed, however, gives them away.

On to the next PC...this time it was called into the Help Desk as being a problem with Microsoft Excel. It seems that data in Excel wasn't scrolling when the user scrolled with the mouse cursor using the right side bar. Excel was also slow and “crash prone”. I suggested we try to remove Microsoft Office and reinstall it. Upon trying to do this, I noted the system was extremely sluggish. Opening the process list in Process Explorer revealed 4 copies of svchost.exe running: unsigned of course, along with something called rpcs.exe that was kicking off iexplore.exe and other files such as “nortons.exe” and “winform.exe”. Cleaning this up was easy actually: using a

combination of Process Explorer and Autoruns, I was able to clean off most of the bad guys, except rpcs.exe kept showing back up after reboots.

Unfortunately, Rootkit Revealer would just freeze up on this system. I then tried the [System Repair Engineer from kztechs.com](#). Right away SRE lets me know that something is wrong:



Clicking on details gives me this:



The really funny part is if you go into Windows explorer and go to C:windowsspss, you will see nothing there. That's because this rootkit is incepting our calls to see this directory and is feeding us false information. If you were boot from BartPE, you would actually see the files there. We'll proceed to the Smart Scan within SRE...all this does is create a text report of any bad stuff going on with our system. From this report, we are warned once again about C:windowsspss3.dll being a dangerous API hook, as well as 3.exe running as a hidden process. SRE also goes through the services and shows us any services that aren't digitally signed. I find that Greypigeon installed a service for us! Pigeons usually crap all over the place and this is no exception: attacking via a service is not common attack vector and therefore will likely get missed (*I missed it myself the first few passes*).

SRE also has a few nifty repair utilities in, including the ability to restore hijacked file extensions, restore Winsock back to its default state, restore default Windows policies and restore safe mode services (*some spyware removes the Safeboot key to keep you from booting into safe mode to remove them*). Unfortunately, SRE cannot terminate hidden processes or locked files: we have to use Icesword for that. Icesword was written in Chinese and was translated to English, so you don't get any documentation with it. However, it's pretty easy to use and who ever reads documentation anyways? As Dogbert once said: "*While you're waiting, read the free novel we sent you. It's a spanish story about a guy named "Manual" .*"

We can click on the Process icon and find our victim:



We can then go back into SRE and delete the GreyPigeon service:



If someone could combine Autoruns, Process Explorer, Icesword and SRE into one product, that would be so cool!

If you want to play around with this rootkit, I've uploaded it [here](#). Make sure you only load it into Virtual PC or VMware and not on your PC! **THIS FILE IS FOR EDUCATIONAL PURPOSES ONLY AND I CANNOT BE HELD RESPONSIBLE FOR ANY RESULTS YOU GET FROM RUNNING IT! YOU HAVE BEEN WARNED!**

So the lesson here is that just because a user gets malware does not mean we have to wipe the machine. What would we learn if we wiped the machine? Interacting with various types of malware and program bugs brings us a closer understanding of the operating system.

– Soli Deo Gloria

Columbo Files: Limited or No Connectivity

APRIL 12, 2007

CATEGORIES: SPYWARE, TECH TIPS



I had an interesting problem recently. A user called and was not able to get on the network. After arriving at the user's desktop, I noted the PC had an APIPA address and the NIC noted that it had "Limited or No Connectivity". After disabling/re-enabling the NIC, removing/readding it and rebooting the PC, I ended up with the same result. Thinking it was a network problem, I proceeded to switch ports on the network switch and trying another network jack. Same thing. I then tried another NIC in the PC: same thing. I then bought over a laptop and plugged it in: it got an IP address right away. I left the laptop with the user and brought the computer back to my desk for inspection.

When I tried pinging any host on the network, I would get a "y" symbol with two little dots above it. Ah, here it is: \ddot{y} . Charmap lists this as a "Cyrillic Small Letter U with Diaeresis". Well, thanks for clearing that up! I ran [Winsock XP Fix](#) and the PC connected to the network just fine! Weird.

About a day later, the mystery was starting to unravel. The same user called again stating that Internet Explorer wouldn't start due to the fact that it was looking for a file called msvcrl.dll. This file looks innocent enough, so I went searching for it on another Windows XP workstation, but alas I could not find the file anywhere. Using my old trusty friend Google, I discovered that the file was "*a Trojan allows attackers to access your computer from remote locations, stealing*

passwords, Internet banking and personal data.” That’s great, on a computer that some one runs our financials on too!

The major threat was already gone, but how was I to repair Internet Explorer? A search of the registry did not produce any results for msvcrl.dll. Perhaps it was tucked away in some binary value in the registry? I tried to reinstall IE, but it told me that a newer version was already installed. Using the “IsInstalled” registry trick from Microsoft would not fool the computer into reinstalling IE. Bummer. After digging around on Google some more, I found [IEFIX](#). This utility repairs Internet Explorer back to its clean state by re-registering the original files from your Windows XP CD. I ran on this on the PC in question and it was fixed (*finally!*).

– Soli Deo Gloria










Adaption of Windows Vista: Real Numbers

APRIL 14, 2007

CATEGORIES: OPERATING SYSTEM

Someone recently asked on [Experts-Exchange](#) how many people are using Windows Vista in the world. I decided to do some research (*ad hoc mind you*) what the real numbers are. From my own web site, these are the stats:

Operating Systems

Versions	Hits	Percent	
 Windows XP	15116	61.7 %	
 Windows NT	39	0.1 %	
 Windows Me	19	0 %	
 Windows Vista	6113	24.9 %	
 Windows CE	13	0 %	
 Windows 98	180	0.7 %	
 Windows 95	1	0 %	
 Windows 2003	427	1.7 %	
 Windows 2000	878	3.5 %	

93% of the operating systems that visited my site were Windows, so if we are just talking about Windows itself that would be:

Windows XP: 66.3%

Windows Vista: 26.8%

Windows 2000: 3.8%

In the thread, I gave the number as 32.8%. This is because I was manually counting from analog's log. The numbers at boingboing.net are a bit more interesting. To date this month, boingboing.net has 1,126,157 unique visitors. Their break out given by AWstats is as follows:

Windows XP 59.4 %

Windows NT 0.9 %

Windows Me 0.2 %

Windows Vista 2.4 %

Windows CE 0 %

Windows 98 0.6 %

Windows 95 0 %

Windows 2003 0.5 %

Windows 2000 3.2 %

Windows 3.xx 0 %

If we break this down to just Windows, that would be:

Windows XP: 87.9%

Windows Vista: 3.6%

Windows 2000: 4.8%

So how does this compare to Windows XP's launch? We would need some access.log files from around October 2001. I found [AWstats for a Princeton department](#) website covering this time period. Two months after the XP launch (12/2001), 6.4% of the users were using Windows XP to access the site. In 4/1/02 (6 months after the Windows XP launch), the number jumped to 10.3%. In 12/2002, Windows XP was at 23.8%. Another site called [mariley.com](#) gives some data to play with: In 1/01/02, 1.8% visits were from Windows XP, 69.7% for Windows 98. 4/1/02 (6 months after Windows XP launch) produces Windows XP at 8.3%, Windows 98 at 58.3%. [Computerking.org](#) gives XP 2.76% in 01/01/02 and 4.98% on 4/01/02. There's a nice chart from W3C on historic OS usage [here](#).

Taking the average of all three of these stats and you get a 3.56% growth rate for Windows XP 2 months after launch. It took around a year and half for [Windows XP surpass the Windows 98](#) market share at 34.63% verses 24.93%. We really won't know how Vista is really doing for

probably at least a year, but given these current statistics (*and given they after a holiday season*), Vista seems to be keeping pace with Windows XP's launch.

IDC predicts strong growth for Windows Vista. It's been 5 long years since the last update. I predict Vista numbers to soar past Windows XP's.

-Soli Deo Gloria

Jon Stewart Calls Out Nancy Grace on Duke Case

APRIL 15, 2007

CATEGORIES: JOKE

Classic! [Jon makes Nancy Grace look foolish.](#)

[Alternate link](#)

[Alternate link](#)

Slow File Transfers on Windows Vista

APRIL 23, 2007

CATEGORIES: OPERATING SYSTEM, TECH TIPS

File copying in Windows XP seems better than it is in Windows Vista. Microsoft has even acknowledged the [problem](#) in their knowledge base. The hotfix is only available from Microsoft PSS, unless you look around a bit. I found this web site [here](#) that offers up some suggestions on fixing this problem, including a link to a web site called [TheHotFixSite](#). This web site hosts hotfixes that Microsoft releases only via the PSS (*i.e. does not make available to the general public*). Contacting the PSS usually involves paying a fee for the hotfix. KB931770 which is mentioned in the Microsoft knowledge base, is available from TheHotFixSite.

Please note that this hotfix will be incorporated in the next service pack for Windows Vista and that this hotfix in its current form is not widely tested. Use at your own risk!

– Soli Deo Gloria

Derren Brown Versus 9 Chess Pros

APRIL 28, 2007

CATEGORIES: MISC

Derren Brown, who mentions his chess skills as poor, beats two chess Grandmasters. How he did it is very interesting. Watch it [here](#).

– Soli Deo Gloria

Support for MS-DOS Based Programs Fading in Windows Vista

MAY 2, 2007

CATEGORIES: TECH TIPS

Support for MS-DOS based programs is fading at Microsoft. Windows Vista does not natively support full-screen DOS mode for MS-DOS based programs. Attempts to execute ALT-ENTER in DOS programs will result in a message: "This system does not support fullscreen mode". Several people have noted a workaround is to fall back to Windows XP drivers instead of the built-in Windows Vista ones (*Vista Starter Edition apparently doesn't use WDDM drivers due to its lack of Aero support and therefore does not have problems running DOS programs full-screen*).

It also appears that expanded memory (EMS) support is also gone, although this post from Matthew Braun from Microsoft states you can get it back by doing the following:

You can change these settings by running explorer as Administrator or you can also change it from Safe Mode. To run explorer as Administrator, open up a new elevated command window by right clicking cmd.exe -> Run as administrator, then open Task Manager and End Process on explorer, then from the elevated command prompt type explorer.exe (DO NOT EXIT TASK MANGER). Explorer is now running elevated, navigate to C:WINDOWSSystem32command.com and right click -> properties, proceed to change the setting in the memory tab. After you are completed to return explorer to a standard user process context goto task manager and end the explorer process, then goto File->New Task(Run...) and type explorer.exe, explorer is now running in a standard user process.

The other option of course is to run your legacy OS in VPC 2007 under Windows Vista.

- Soli Deo Gloria

Where Oh Where is my I386 Directory?

MAY 10, 2007

CATEGORIES: MISC, OPERATING SYSTEM, TECH TIPS

Windows has always asked for the Windows installation CD whenever you add a Windows component. In the past, I've just copied the Windows CD to a share and just connect to it via UNC whenever I need it. With Windows Vista, however, that's all changed! Windows Vista places all the files it needs on the hard drive.

You might be wondering, however, where exactly it does this. You wouldn't find a I386 directory or copy of the CD anywhere. I used a copy of WinDirStat to track down where Vista was hiding the files. It appears to split the DVD into two parts: applications (*Windows components*) and drivers. "C:windowwinsxs" contains the applications. For fun, I ran Process Monitor and added Windows games (*in Windows Vista, this is known as "Turning on a feature" instead of "Installing a program"*). Some of the calls made to the folders include:

C:Windowswinsxsx86_microsoft-windows-s..es-
hearts.resources_31bf3856ad364e35_6.0.6000.16386_en-us_8adcf7faf63cfb99

C:Windowswinsxsx86_microsoft-windows-s..oxgames-
purpleplace_31bf3856ad364e35_6.0.6000.16386_none_03f4bc7f0186d3be

C:Windowswinsxsx86_microsoft-windows-s..inboxgames-
shanghai_31bf3856ad364e35_6.0.6000.16386_none_be6d39b9f23eed53

Gone are the days of simple folder names!

Drivers are kept in "C:windowssystem32driverstorefilerpository". Each driver now has a component.man (*component manifest*) file written in XML format that describes file versions and destinations. There also appears to be PnP device information in some man files. Is this the replacement for INF files going forward?

Some other changes you might want to be aware of: "C:documents and settingsyourusername\local settings" has been replaced by "C:usersyourusername\AppDataLocal". You might have also noticed a "LocalLow" folder at the same level and might have wondered what it was. Well, it relates to the Integrity Levels (IL) in

Windows Vista. In a nutshell: any process that cannot be trusted is run with Low Integrity access. The only place a Low IL process can write is “C:usersyourname\local\low”. [This MSDN article](#) explains the theory behind ILs. Treat anything in LocalLow with care, especially when copying profiles around. The Roaming directory is obviously related to roaming profiles, but the name is much clearer now. “C:documents and settings\yourusername\local\settings\application data” would relate to data that was machine specific, so it was not included in the roaming user profile. However, “C:documents and settings\yourusername\application data” was considered user specific and would roam with the user profile. Confused? Good, that’s why they changed it! “C:documents and settings\all users” has been replaced by “C:users\public”.

– Soli Deo Gloria

Free Windows Vista Evaluation

MAY 18, 2007

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Microsoft is offering Windows Vista in VHD format for Virtual PC/Virtual Server for FREE! This is a 30 day evaluation version. You can get it [here](#).

– Soli Deo Gloria

Become a Windows Vista Expert

MAY 23, 2007

CATEGORIES: JOKE

This [video](#) will show you how! 😊

Rare Gates and Jobs Appearance Together

JUNE 1, 2007

CATEGORIES: MISC, OPERATING SYSTEM

See it [here!](#) This was taken at D: All Things Digital on May 30, 2007.

– Soli Deo Gloria

Slow Browsing When Navigating Network Drives

JUNE 13, 2007

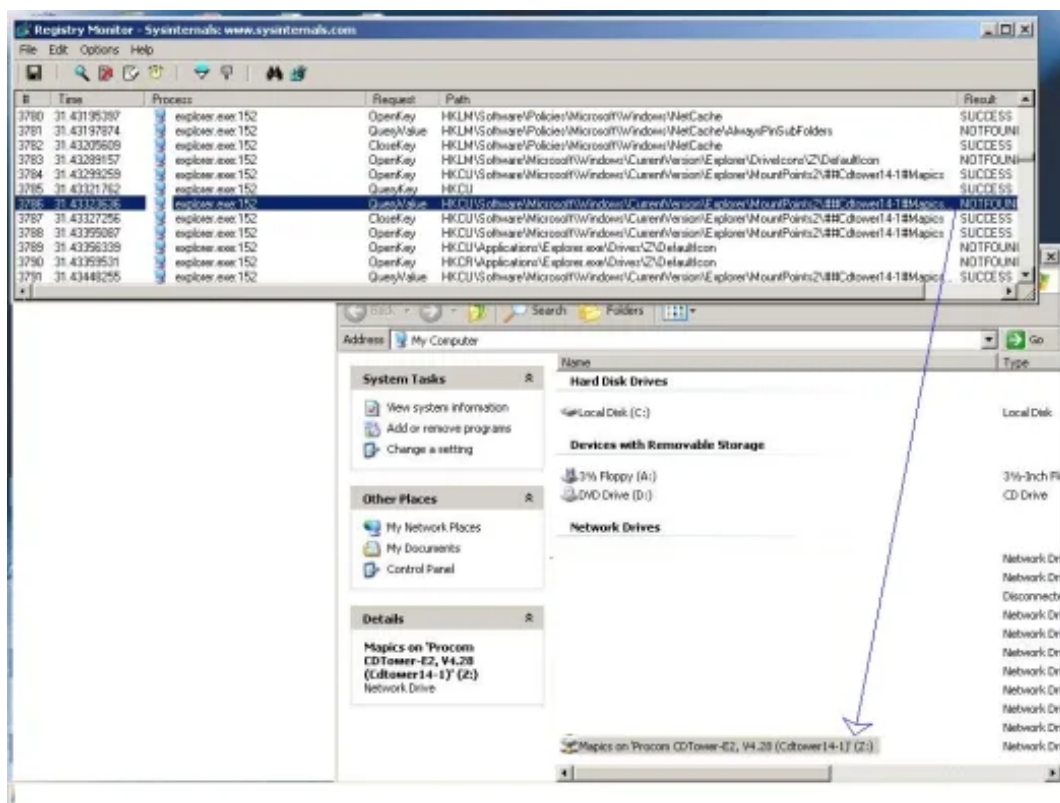
CATEGORIES: TECH TIPS

A user called the Help Desk citing slow access whenever he would open My Computer or drill into folders. Usually, these types of problems can be a real problem to troubleshoot, because you don't really know if it's a network issue or a Windows issue. The machine in question was a Windows XP SP2 workstation. Time to get out the handy dandy Regmon utility!

Upon starting the log, the last entry is read before the lock up is

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\##CDTower14-1#MAPICS. Mountpoints refer to drives we have mapped, so let's look at what we have mapped:

Mapics on 'Procom CDTower-E2, V4.28 (CDtower 14-1)' (Z:). Upon clicking this drive, I was told that Windows couldn't find this path. Ah ha! After deleting the drive mapping, the speed of folder navigation returned to normal.



- Soli Deo Gloria

22 Confessions of a Former Dell Sales Manager

JUNE 15, 2007

CATEGORIES: MISC

Read it quickly before Dell takes it offline!

– Soli Deo Gloria

Automatic Updates Not So Automatic

JULY 2, 2007

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I recently had to install Windows Vista fresh as I switched out motherboards. I had ordered an Asus socket 478 motherboard from eBay and it failed to work. The AGP is bad on my current motherboard and I was trying to fix that. They do not make socket 478 motherboards with 4 memory sockets anymore. Alas, I am stuck with this PCI video card until I get a new computer.

Any ways, while Windows Update was running I noticed that Windows Vista was actually finding drivers for devices use to have to load drivers manually for. Sweet! Perhaps the days of the PC Technician are numbered.

But wait...although it found a driver for my WinTV-GO card, it said the driver installation failed. This card worked fine in Vista before I wiped the machine. I decided to deal with it later.

The next day while watching some YouTube clips, I noticed the sound sounded distorted and kept fading in and out. No amount of tweaking in the device properties would make it sound better. I then downloaded the SB Live! drivers from my web site and presto, the sound was normal again! My drivers are dated 2002 and the ones from Windows Update were dated 2006. I guess newer drivers aren't always better.

Now on to my Win-TV card: no amount of pointing it to the correct drivers would make the install work. The driver installation kept failing saying it was missing a file. Using Procmon, I found out that Windows Update was looking for the drivers in C:\windowssystem32\driverstore\temp<somebighex#>\Package. It appears that it had downloaded hcwbt8xx.cat, but none of the other files. This driver or catalog must have a higher ranking then my XP drivers for the WinTV-GO card as Windows Vista outright refused to accept my older drivers. It wasn't until I right-clicked the device, the device, pick uninstall and deleted the Windows Update drivers would it let me install the old drivers.

My verdict on Windows Update for getting drivers is this: don't do it!

– Soli Deo Gloria

Autologin and Windows Vista

JULY 22, 2007

CATEGORIES: OPERATING SYSTEM, TECH TIPS

As mentioned in a previous blog entry, Autolog can be used to create a Windows workstation that logs in automatically with ease. This utility still works on Windows Vista! One snag that I did run into however is that the IBM MAPICS built-in client autologin feature does not work under Windows Vista. We can get around this problem with AutoIT. AutoIT is a freeware scripting language that's pretty easy to understand. After Googling a bit, I found a [cheat sheet](#) that some made that had the common AutoIT commands.

After installing AutoIT, it will execute any script that ends in AU3. I already had the iSeries client in the Startup folder (*incidentally, a retarded path:*

C:\UserstestloginAppDataRoamingMicrosoftWindowsStart MenuProgramsStartup). We want to wait for the login screen, input the login and password, wait a short time, input the character "1" and then hit enter.

Here's the code I used:

```
WinWaitActive("Signon to iSeries")
send("testlogin")
send("{TAB}")
send("supersecretpassword")
send("{ENTER}")
sleep(3000)
send("1")
send("{ENTER}")
```

You literally have to think out each step and input that into the script since this is simulating human input. The other trick to this is that the window has to have focus. A window can lose focus if a pop-up message comes up or a user clicks off from the window. Since this is a time clock kiosk, this really is not an issue.

The Shared Computer Toolkit is been changed to Windows SteadyState for Windows Vista. Unfortunately, that was not available at the time of this post. However, using local group policy, I

was able to lock as tight as I would have using SCT.

- Soli Deo Gloria

Windows Vista Product Activation is Retarded

AUGUST 4, 2007

CATEGORIES: MISC, OPERATING SYSTEM

I recently have been having some troubles with my main hard drive: a Western Digital WD1200JB drive. The drive will randomly spin up and down when the drive is in use. The unmistakable “whine” of it spinning down and back up randomly can be heard quite clearly. If I am in a game and it spins down, my whole game freezes for a few seconds until it spins up again. Queries to Western Digital regarding this issue went unanswered: I guess my next drive will be a Seagate.

Any how, I have a slave drive: a Western Digital WD2000JB. I had already copied that data off to another drive unit, so my plan was to take Symantec Ghost 11, clone my boot drive to the second drive and then switch drives. In other words: the slave drive would become the primary and primary drive would become slave. All of this went without a hitch: I wiped the second disk and everything was blissful. That was until the next morning when the system decided that my hardware changed and I was required to reactivate. It let me activate over the Internet without any trouble, but only for the fact that this key has multiple activations. Had this been a retail key, I would have had to call some drone (*probably over seas*) on the phone and explain what happened.

Why on earth do I have to explain anything? **THERE WAS NO HARDWARE CHANGE!** Microsoft lead us to believe that Vista would be more forgiving of hardware changes, however, the hardware that was in my PC was still in my PC. The only difference was I flipped one jumper position on each drive. For that, Microsoft contends I have a new computer and it must be “re-activated” with them.

No wonder why everyone tries to get around product activation: a broken system that flags you for piracy when moving around parts in your system. Heaven forbid if I add extra memory or another adapter card to my rig: I’ll probably get flagged. Microsoft needs to relax these restrictions or add activations to each product key. For example: why can’t they allow retail keys a maximum of 5 activations from various hardware configurations? A key leaked on the Internet will exceed 5 activations in about 30 seconds before it is rendered useless.

The only reason for such Draconian measures of course is Microsoft wants to make the most money possible as competitors circle them like wolves. Microsoft is its worst enemy...if it should

ever come to pass that an operating system works just as good as Windows without of all these copy protection schemes, Microsoft will be forced to back peddle them back out of the OS for its enterprise and retail customers. How will that look?

Macintosh OS X now runs on x86 chips and the price is \$129 and the 5 license family pack is \$199! Vista Ultimate alone is \$249 (*and that's the upgrade, OEM, no support version*). As much as a Microsoft fan boy I am, I am completely turned off by Microsoft deciding whether or not Windows will load on my PC because of my hardware. Devote your R&D to improving how the OS works on my PC, not how you can restrict it.

If Apple can let me run my current applications that I have today in OS X and run it on my PC, I will be seriously considering a switch!

-Soli Deo Gloria

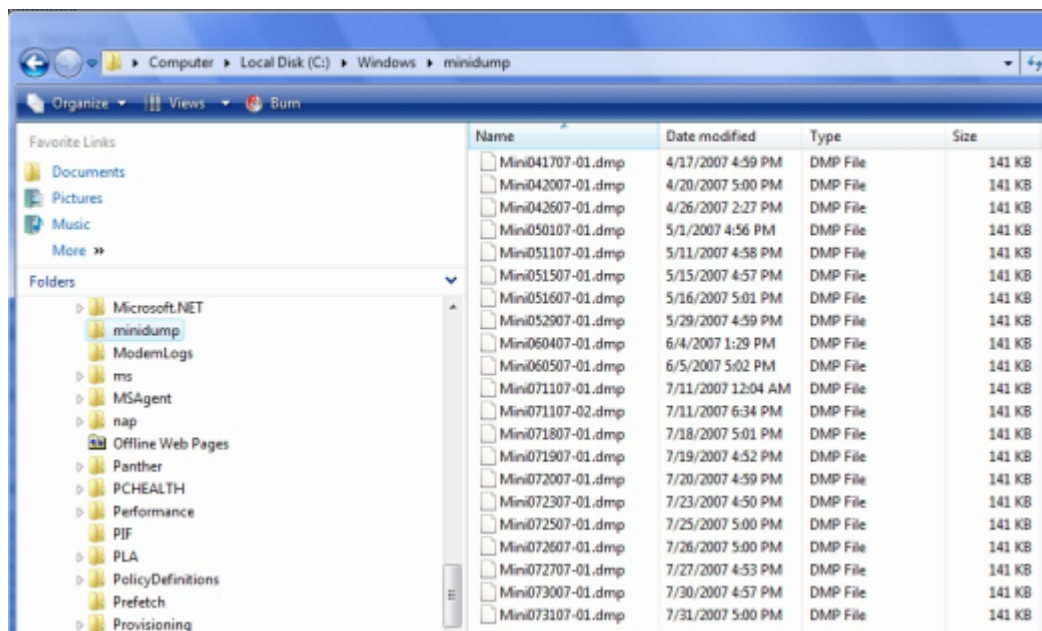
Entering the Land of BSOD Investigation

AUGUST 23, 2007

CATEGORIES: TECH TIPS

Every day upon booting my Vista workstation at work I was getting a message that the system recovered from an unexpected shutdown. I figured that someone was just powering my PC off at night, but I decided to check the logs. It appeared that Windows was crashing right after I left work. I went off to search for any files ending in .DMP. These .DMP files are snapshots of memory when the PC crashes. If you can't find any, you may have to turn memory dumping on (*Under Vista, that's Control Panel>System>Advanced System Settings>Startup and Recovery>Settings, uncheck "Automatically Restart" and make sure "Write Debugging Information" is set to "Complete" or "Kernel"*).

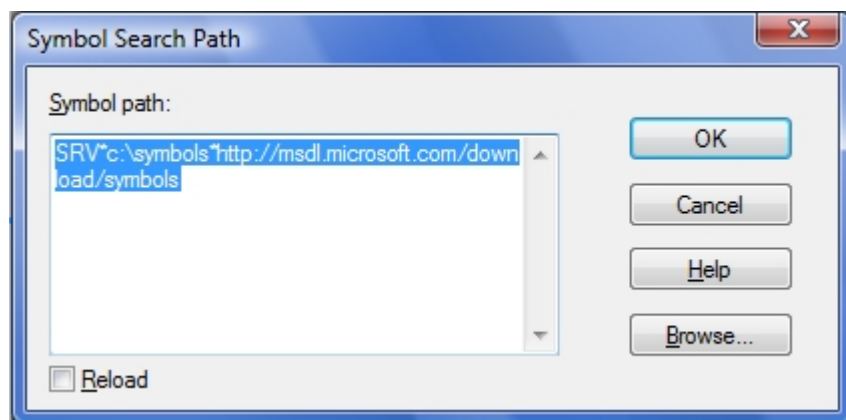
Once again, UAC rears its ugly head. Searching from start menu or the command prompt yielded no results, then I remembered that I wasn't running from an elevated prompt. The location? C:\windows\minidump:



I guess Microsoft thinks that regular users shouldn't be looking at memory dumps as the permissions on minidump are SYSTEM and Administrators only.

Now we will download the [Microsoft Debugging Tools](#). This will allow us to analyze the .DMP file.

After installing the program, the first thing we want to do is set the symbol path. This gives us more information from the crash dump. We will set the path to SRV*c:symbols*http://msdl.microsoft.com/download/symbols by going to File>Symbol File Path:



Now go to File>Open Crash Dump and open the .DMP file (*I've provided my crash dump [here](#) in case you want to practice with these instructions*).

Right away it identifies a possible culprit:

```
*****
*                                     *
*                               Bugcheck Analysis                               *
*                                     *
*****

Use !analyze -v to get detailed debugging information.

BugCheck 1000008E, {c0000005, 82ba6620, a91ebb5c, 0}

Probably caused by : ecache.sys ( ecache!EcDispatchPassthrough+3a )

Followup: MachineOwner
-----
```

Running “!analyze -v” provides further (geeker) analysis:

```

0: kd> !analyze -v
*****
*                                     *
*                               Bugcheck Analysis                               *
*                                     *
*****

KERNEL_MODE_EXCEPTION_NOT_HANDLED_M (1000008e)
This is a very common bugcheck. Usually the exception address pinpoints
the driver/function that caused the problem. Always note this address
as well as the link date of the driver/image that contains this address.
Some common problems are exception code 0x80000003. This means a hard
coded breakpoint or assertion was hit, but this system was booted
/NODEBUG. This is not supposed to happen as developers should never have
hardcoded breakpoints in retail code, but ...
If this happens, make sure a debugger gets connected, and the
system is booted /DEBUG. This will let us see why this breakpoint is
happening.
Arguments:
Arg1: c0000005. The exception code that was not handled
Arg2: 82ba6620. The address that the exception occurred at
Arg3: a91ebb5c. Trap Frame
Arg4: 00000000

Debugging Details:
-----

EXCEPTION_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%08lx referenced memory at 0x%08lx. The memory could not be %s.

FAULTING_IP:
ecache!EcDispatchPassthrough+3a
82ba6620 8b480c          mov     ecx,dword ptr [eax+0Ch]

TRAP_FRAME: a91ebb5c -- (.trap 0xfffffa91ebb5c)
ErrCode = 00000000
eax=00000000 ebx=87754a78 ecx=0000000e edx=87754a78 esi=00000000 edi=87754ae8
eip=82ba6620 esp=a91ebbd0 ebp=a91ebbd0 iopl=0         nv up ei ng zr na pe nc
cs=0008  ss=0010  ds=0023  es=0023  fs=0030  gs=0000             efl=00010286
ecache!EcDispatchPassthrough+0x3a:
82ba6620 8b480c          mov     ecx,dword ptr [eax+0Ch] ds:0023:0000000c=????????
Resetting default scope

CUSTOMER_CRASH_COUNT: 1
DEFAULT_BUCKET_ID: VISTA_DRIVER_FAULT
BUGCHECK_STR: 0x8E
PROCESS_NAME: svchost.exe
CURRENT_IRQL: 0
LAST_CONTROL_TRANSFER: from 82bb2ca4 to 82ba6620

STACK_TEXT:
a91ebbd0 82bb2ca4 859f93e0 87754a78 87a66400  ecache!EcDispatchPassthrough+0x3a
a91ebc2c 8202ecf 859f93e0 87754a78 87754a78  ecache!EcDispatchDeviceControl+0x3e
a91ebc44 82188f65 87a66400 87754a78 87754ae8  nt!IoCallDriver+0x63
a91ebc64 82189f25 859f93e0 87a66400 00faab00  nt!IoPynchronousServiceTail+0x1e0
a91ebd00 8218ee8d 859f93e0 87754a78 00000000  nt!IoPxxControlFile+0x6b7
a91ebd34 8208c96a 000004a0 00000000 00000000  nt!NtDeviceIoControlFile+0x2a
a91ebd34 77b20f34 000004a0 00000000 00000000  nt!KiFastCallEntry+0x12e
WARNING: Frame IP not in any known module. Following frames may be wrong.
01411c8c 00000000 00000000 00000000 00000000  0x77b20f34

```

Also note the DEFAULT_BUCKET_ID is VISTA_DRIVER_FAULT which gives further clues. WinDBG identifies ECACHE.SYS as being the problem. Doing a Google search brings up that ECACHE.SYS is related to ReadyBoost. Since I don't use ReadyBoost I just disabled the service (*called ReadyBoost, imagine that!*) and bingo: the problem goes away.

Now the cause of this: I can only guess it is my external USB hard drive. During the work day, I connect an external USB drive to my PC. I pull this drive without doing the safe disconnect and then log out. Vista is likely using the drive as a ReadyBoost drive and then I pull the rug out from under it by removing the drive.

-Soli Deo Gloria

RIAA's Letter to ISPs

SEPTEMBER 7, 2007

CATEGORIES: MISC

An interesting story from [P2PNet](#), copied in its entirety about how the RIAA is trying to squeeze money from people.

p2pnet.net news:- The RIAA is launching its own p2p site. But not because it's owners, Warner Music (US), EMI (Britain), Vivendi Universal (France) and Sony BMG (Japan and Germany), have suddenly seen the stupidity of trying to sue their own customers into buying 'product'.

To the contrary, [www.p2plawsuits.com](#) (as it'll be) represents an escalation in the RIAA extortion scheme, a move to streamline the process so the Big 4 can add more victims' scalps to their belts, faster, lending credence to their [false claims](#) that the sue 'em all campaign is stemming the swelling tides of people who are logging onto the p2p networks every minute of every day.

The Big 4 are now making a \$1,000 per settlement discount offer to victims who agree to settle, to in effect admit they're guilty of the RIAA's charges, before a civil lawsuit is actually lodged.

It's conservatively estimated that more than 60 million Americans have shared with each other online. Of those, the RIAA (Recording Industry Association of America) has managed to 'target' (a favourite word) a pitiful few, between 19,000 and 20,000, many of them young children. And it's being forced to fight every step of the way to turn even those into PR-useable statistics to 'prove' the so-called anti-file sharing war is being won.

However, in reality, individuals stand as much chance of being identified by the RIAA as they do of being struck by lightning, as Dr Markus Giesler [points out](#) in his [Theory of Collective Consumer Risk](#).

The risk tied to file-sharing is almost zero despite entertainment industry claims to the contrary, he says.

And all the while, the numbers of file sharers not only in the US, but around the world, are steadily growing, not decreasing.

It's an uphill battle for the multi-billion-dollar labels as they claim they're being "devastated" and "decimated," to use two more of their favourite words, by p2p file sharing. And it's getting steeper as more and more Santangelos, Andersens, Lindors, Barkers and others refuse to "settle" for something they didn't do.

Warner Music, EMI, Vivendi Universal and Sony BMG say files shared equal sales lost, but this claim has again been proven to be disingenuous in an authoritative paper from two American researchers in The Effect of File Sharing on Record Sales: An Empirical Analysis, just published in the Journal of Political Economy, 2007.

Meanwhile, the RIAA is contacting ISPs by letter, says Recording Industry vs The People. The aim is to get the Internet Service Providers to in effect follow the Big 4's bizarre policy of working against their own customers, the very people upon whom both literally depend for their survival and livelihoods.

A PDF copy of the RIAA letter sent to ISPs is available on my web site.

Interesting interview videos of Patricia Santangelo is fighting the RIAA

– Soli Deo Gloria

Carey Frisch – The Windows Genuine Disadvantage

SEPTEMBER 10, 2007

CATEGORIES: MISC, OPERATING SYSTEM

On July 17th, I logged into my blog to find comments made by Carey Frisch calling this [blog entry](#) a bunch of lies. Thankfully, I have comment moderation turned on, so he was not allowed to post those comments without my approval. I offered him a chance to post a rebuttal comment with factual proof and yet again, he just posted emotional “*all lies! this web site is self serving!*” like statements. In fact, he is still welcome to provide **evidence** of any “lies” in my article.

Carey’s [first claim](#) is that I have somehow have made up false comments and put his name to them. These comments were pulled right from Google Groups:

[Posting #1](#)

[Posting #2](#)

He can remove them from http://groups.google.com/groups/msgs_remove since the messages were posted under his e-mail address and his e-mail address was not mangled. To date (9/10/07), I found the messages are still there.

If you look at his postings from this time period (*January 2002 – April 2002*), they all come from the midsouth.rr.com IP block, in fact, here’s a posting where he says he’s been using RoadRunner for 2 years:

[Posting #3](#)

Compare the NNTP-Posting-Host line in each message:

```
NNTP-Posting-Host: HUBMS-ubr-24-33-9-77.midsouth.rr.com 24.33.9.77
```

You will find that the IP address used to post the message is the same in all postings. While it is possible that this field can be faked, it is hardly a task that could be done by “Joe Blow”. The

comments are also logical responses to the conversation in the thread.

In my original article I talked about “bomb code” and why it is bad to have in software. Quoting my June 1st, 2006 article:

“If Carey (again, who Microsoft supports, since he is a MS-MVP) gets his way, any computer running WGA that identifies a bootleg copy will get shut down. It does not matter if WGA is correct in its judgement or not”

On August 24, 2007, this happened:

This validation failure did not result in the 30-day grace period starting and no one went into reduced functionality mode as a result. The experience of a system that failed validation in this instance was that some features intended for use only on genuine systems were temporarily unavailable. Those features were Windows Aero, ReadyBoost, Windows Defender (which still scanned and identified all threats, but cleaned only the severe ones), and Windows Update (only optional updates were unavailable; security and other critical updates remained available). Also, the desktop message about failed validation appeared. And as I indicated, these features return to normal and the desktop message disappears when an affected system is revalidated at our site.

Source

Now it’s interesting that Microsoft states that these systems did not go into RFM, yet they mention symptoms of the computers doing so!

I present to you: the behavior of RFM, courtesy of Microsoft’s Knowledgebase:

*If Windows Vista is running in **non-genuine reduced functionality mode**, you cannot perform the following actions:*

Aero Glass and the Windows ReadyBoost features that are included with Windows Vista are unavailable in reduced functionality mode.

Premium content from the Microsoft Download center is unavailable in reduced functionality mode.

All the postings regarding this event from Microsoft are pure damage control. “Less than 12,000 computers affected!” and our friend Carey Frisch: “A Short-Lived Issue”.

Why is Microsoft doing this? My guess is money. Here’s an interesting article that may shed some light on WGA:

In explaining the pilot program’s change in focus, Wickstrand acknowledged that pay-as-you-go had “high consumer appeal, but not enough usage for the financial institutions” providing credit to the user base. Given the explosion in availability of consumer credit, subscriptions are emerging as a more popular option.

Under the FlexGo program, users make initial down payments on mid-range PCs and make monthly payments for software and broadband services from their local telcos, much the way customers pay cable providers for TV and Internet access. Microsoft and its partners will allow users to sign up and pay for their subscriptions in a variety of ways, ranging from ATMs and point-of-sale terminals, to the Web.

FlexGo systems require activation and Windows Genuine Advantage authentication. *Once subscribed, users will be reminded via notifications and account status screens, as to the amount of time they have remaining before their systems will move to “borrowed time,” and, ultimately, **a locked status for lack of payment.** In order to unlock systems that have degraded due to lack of payment, users will need to obtain a code from the FlexGo partners.*

Source

WGA is just a testbed for how far Microsoft’s can control Windows outside its company headquarters. Vista subscription trials are to begin in 2008 and Autopatcher, an unofficial way to get Microsoft patches without using WGA, was just shut down this month (September 2nd, 2007). Putting all the pieces together, we can assume:

Microsoft wants Windows transferred to a subscription based plan to make more money. Take Windows XP for example. It was launched 62 months ago at \$299 street price. That works out to be \$4.82/month. The longer you run Windows XP, the more money Microsoft loses. I purchased Windows 2000 back in the day for \$129.99. I run a Vista/W2K dual boot to run my games. Over 91 months, Microsoft only made \$1.42/month on this Windows 2000 sale.

My prediction: Windows Xtreme. Sell one version for \$125 and then add all the goodies that people want under subscription services, payable by credit card. Want Windows Defender? That will be \$2/month. Antivirus? \$3/month. Low cost version of Word? \$5/month. Of course, there would have to be a perpetual subscription charge for running just Windows itself. Put it at \$12/month. Then, put some mouth watering deals out there that give you discounted pricing for buying multiple years. Microsoft is already doing something similar with their enterprise customers: [Software Assurance](#).

Failure to pony up the cash would cause Windows to...you guessed it, go into RFM and after 30 days, cease to work.

– Soli Deo Gloria

The Hunter Becomes the Hunted

SEPTEMBER 17, 2007

CATEGORIES: MISC

Media Defender, a notorious anti piracy gang working for the MPAA, RIAA and several independent media production companies, just launched their very own video upload service called “miivi.com”. The sole purpose of the site is to trap people into uploading copyrighted material, and bust them for doing so. In a twist of fate: 6 months of internal e-mails at the company were released on BitTorrent. You can read more about it [here](#).

– Soli Deo Gloria

Case of the Crashing Excel 2003

OCTOBER 16, 2007

CATEGORIES: TECH TIPS

One of my users had an interesting cases of Excel crashing when opening certain files. Excel would restart 3 times and finally on the 3rd time, it would open the file without any formatting. The file opened file on other PCs I tried. Removing and reinstalling Microsoft Office 2003 made no difference. Neither did any of the suggestions at support.microsoft.com/kb/280504. Interestingly enough, when I logged in as myself using a different profile, Excel worked fine!

After setting up a new profile for the user, the problem returned. I pulled out my trusty Process Monitor program from Sysinternals. It appears when Excel is first started, the default printer is initialized. When I changed the default printer to another printer, Excel started fine. Deleting and recreating the default printer fixed the problem.

– Soli Deo Gloria

Critical Analysis: Getting Gouged by Geeks

OCTOBER 27, 2007

CATEGORIES: MISC, REVIEW

From time to time, I have thought about doing PC repair work as a side business. Recently, I saw a link from Consumerist to an undercover story on [Getting Gouged by Geeks](#) ([alterative link](#)). The whole episode is available on their web site. After watching it, I have to say that I am disappointed by the spin given by CBC. It's a bit frightening to think what other stories the media are editing to make a good story.

Let's look at the first setup: shove a bad DIMM into a PC so that it doesn't boot. CBC lists this as a "small, common problem". Then, call out the nerd herd to your house, tape it with your hidden video camera and have a good laugh when they misdiagnose the problem. There's a few problems with this setup: namely that this is not a common problem. I've worked at two companies with various PC hardware manufacturers (*and 700+ PCs onsite*) and never had a PC not boot with bad memory being the cause. That's not to say it never happens, but it is rare in my experience. I have, however, encountered memory that has gone bad in a PC. This causes the operating system to crash and the PC to act strangely. Diagnosing this type of problem is usually simple as running a memory test from a boot CD or switching the memory with known good memory.

PCs can take many types of memory and I'm guessing that these technicians do not carry each speed of memory and every capacity: it's just not practical. The correct way of trying to diagnose it, of course, is to listen to the beeps at POST. The CBC makes fun of one technician who is repeating the beeps, saying *he's talking to the computer, lol!* The joke, however, is on CBC. Repeating the beeps is perfectly logical: he's probably trying to distinguish which beeps are long and which are short.

Example from [here](#):

- **No Beeps:** Short, No power, Bad CPU/MB, Loose Peripherals
- **One Beep:** Everything is normal and Computer POSTed fine
- **Two Beeps:** POST/CMOS Error

- **One Long Beep, One Short Beep:** Motherboard Problem
- **One Long Beep, Two Short Beeps:** Video Problem
- **One Long Beep, Three Short Beeps:** Video Problem
- **Three Long Beeps:** Keyboard Error
- **Repeated Long Beeps:** Memory Error
- **Continuous Hi-Lo Beeps:** CPU Overheating

As you can see, there are two types of “3 beeps”: one for a keyboard error and one for a memory error. One uses a series of “long” beeps; the other “short” beeps. This tech that “talks to the computer” is actually one of the techs that correctly identifies the problem. Of course, this tech cannot be let off the hook: he’s charging \$120 for a 1 GB DIMM! CBC detects a ripoff!

Our little nerd friend Steve Gazo from Humber College checks online and proclaims \$64.99 for the 1GB, PC3200 DIMM. It’s unclear, however, whether he’s looking at the price in Canadian dollars or US dollars. Take a look at a Google search I ran:

1Click2Computers <small>ON</small>	SIMPLE TECH 1GB PC3200 DDR KIT FOR APPLE	\$84.75	see site	Buy #1 <small>at 1Click2Computers</small>
cdw.ca <small>ON</small>	POWERGROUP DDR 1GB 400MHz PC3200	\$89.99	in stock	Buy #1 <small>at cdw.ca</small>
Tigerdirect <small>ON</small>	US Modular 1024MB PC3200 DDR2 400MHz Memory	\$93.99	in stock	Buy #1 <small>at Tigerdirect</small>
future.shop <small>AB, BC, MB, NB, NL, NS, ON, PE, QC, SK</small>	Comstar 1GB DDR 400 1GB-Rx PC3200 Memory	\$99.99	see site	Buy #1 <small>at future.shop</small>
microinformatique.ca <small>QC</small>	Ngine Memory 1GB DDR 400 PC3200 Bulk Pack (DDR400-1GBX2)	\$101.00	see site	Buy #1 <small>at microinformatique.ca</small>
Frontier PC <small>BC</small>	GEYWARE DDR 1GB RAM PC3200 400MHz (DDR3200/512) (DDR3200/1GB)	\$123.17	See site	Buy #1 <small>at Frontier PC</small>
microinformatique.ca <small>QC</small>	1GB DDR 400 PC3200 Retail Pack (DDR400-1GBX0)	\$129.00	see site	Buy #1 <small>at microinformatique.ca</small>

The US prices are lower and the Canadian prices higher. Going on the Internet and looking up a price proves nothing in terms of whether the tech is overcharging or not. Depending on where you go for pricing, you can manipulate the pricing up and down as this [article](#) shows:



I can say Vista Ultimate is \$179 (*OEM version at Newegg*), \$399 or \$602. Someone selling Windows Vista Ultimate at \$602 is not necessarily ripping anyone off: you have to put things in context.

CBC states that 4 of the 10 companies suggest to buy a new PC and it was only a \$25 part that needed to be replaced. Wrong! Their own tech found the part for \$65. An honest mistake by the CBC? Probably.

Next case: laptop with corrupt operating system files. Supposedly, this is causing the wireless card not to work as one of the techs says the wireless card *may* have to be replaced. CBC goes off to stay “*there’s nothing wrong with the wireless card*“. In the end, the wireless card is not replaced: the charge is \$113 for an OS reload. The tech is simply giving some reasons what *may* be wrong with the laptop: creative editing at work.

Some shops say the laptop had malware and the CBC eagerly protests that it did not. The common causes for corrupt operating system files are either bad memory, bad harddrive or viruses/malware. Since it isn’t the first two, the technicians claim the laptop had malware. This is a perfectly logical conclusion. The customer may have already tried to clean it off, but perhaps cleaned off too much and deleted critical files in the process. Operating systems files do not corrupt on their own: there has to be some type of explanation. In this case, the malware is our nerd friend Steve Gazo.

The same Steve Gazo places fake files on the laptop named “nice pose.jpg” among others to encourage technicians to check them out. CBC takes the laptop in for service and then brings back the laptop to Gazo. He claims that two of the pictures were opened based on the date accessed field. Fact number #1: Date Accessed is not reliable. If the technician ran an antivirus scan on the machine, it could update this field. This field also wouldn’t update on the files I tried accessing on my Windows Vista Ultimate box.

Fact number #2: Dates can be manipulated as shown by this [utility](#). This information is stored in the NTFS metadata of the file. Date Accessed means absolutely nothing. However, there’s no excuse for a technician to be snooping through people’s hard drives (*if it truly happened*). One would be naive to think that they don’t. However, it is the responsibility of the user to secure THEIR data by means of either moving the data to a flash drive and keeping it at home or encrypting it. If you walked around your house naked would you not expect the neighbors to peek in on you? You would likely pull the blinds before doing such an act.

Half the show is dedicated to a nerd from “Nerds On Site”. They finally find a golden nugget for their show. This guy is truly clueless and deserves to be fired for his conduct. He claims that her hard drive is bad without even opening the case! Of course, we know it’s just the DIMM.

It would have been interesting to see the two cases reserved: taking the desktop in with bad memory problem into the brick and mortar store, and leaving the laptop at home. My guess would be a lot more correct repairs than what is given in the video. A more interesting case would be to put a failing hard drive into the computer in the house and see what the techs would do in terms of being able to recover the data.

The only honest part I found with this video was the interview of the 3 tech guys sitting on the stools.

– Soli Deo Gloria

Robert Galle: Rude Dude of WhereIsIt

NOVEMBER 4, 2007

CATEGORIES: MISC, REVIEW

I have to say that I think I might have met one of the rudest vendors on the Internet! I was interested in a program to catalog my DVD movies. I did some searching around and found a disc cataloging program called WhereIsIt by Robert Galle. The program seemed well written, developed and supported, so I proceeded to order a license for \$39.99. I created an e-mail address “whereisit@mylogin.tuffmail.com” for the ordering process as I have gotten burned in the past by merchants that have added me to spam lists. His order page does state that you cannot use a “freemail” address, however, tuffmail.com is not a free e-mail provider and I in fact pay for e-mail access there.

A few hours after ordering I got this e-mail message from WhereIsIT-soft.com after placing my order:

To: Adam Leinss,

An order on your name has been received from ShareIt! (Ref.No. XXXXXXXXX, Sun Nov 4 2007, 1:04 CET). For license delivery you have selected email delivery, and stated an email address provided by vendor who offers freely available and/or anonymous email addresses. This is a violation of ordering conditions and against instructions as stated on the order form, no licenses are ever sent to any freemail addresses.

If you are applying for a license, you are expected to behave responsibly.

Please respond with an appropriate email address intended for license delivery and state a valid reason for using a freemail address. Failure to do so within 3 days will result in order being processed as a fraud attempt.

WhereIsIt Orders

1. The e-mail address used was not a “freemail” address

2. The e-mail address used was not anonymous

My personal e-mail address is only given to people I meet in real life. I have no control what Robert Galle does with my e-mail address. I respond back that if he cannot send the license to the address I used to cancel the order. Robert replies back with this:

Ordering conditions are clear and they go for you, too.

This order is hereby considered a fraud attempt, and will be treated accordingly.

Robert Galle

I think Mr. Galle missed Customer Service 101. How can I commit fraud with my own credit card? I didn't even get a license: all I did get was a bunch of attitude and quite undeserved attitude at that! Can you imagine getting tech support from this individual?

Since Mr. Galle does not want to sell me his program, I was able to find a freeware replacement called [Disk Explorer Professional](#). I strongly urge you to check out this program if you are in the market in for a disc cataloging program.

– Soli Deo Gloria

Camtasia Studio 3.13 for Free

NOVEMBER 29, 2007

CATEGORIES: MISC

The world's smartest screen recording software that retails for \$299 is available for free!

Go grab it!

<http://www.ghacks.net/2007/11/26/download-and-register-camtasia-studio-for-free/>

– Soli Deo Gloria

You Think Vista is Bad? Try Linux!

DECEMBER 7, 2007

CATEGORIES: MISC

A somewhat amusing post written by Karla Bonerstein on the Linux installation from hell:

I've spent the last 3 days attempting to upgrade 4 Windows-XP systems to Vista and have had various problems with software compatibility.

I've spent countless hours on the phone and technical support websites and finally after 3 days I have everything working.

This fiasco has left me with some doubt as to whether or not Microsoft has the ability to maintain it's position as the defacto standard in operating systems.

After reading about Linux I decided to give it a try on another system which is an older P4 2.4G system based around an Asus board.

I downloaded Fedora and attempted to install.

First problem, my SATA drives were not found.

Google time >>>> 2 hours later <<<< I found the solution which was a Custom Install Option.

(After a few cryptic questions and a partition manager that was convoluted and potentially very dangerous in the hands of a new user, Fedora was installed)

Second Problem, the system would not boot after install. I got a Grub Error 15 message.

Google Time>>>>>> 5 Hours Later <<<<.. Oh boy I found lots of information on this puppy. About 5 hours later I fixed the problem

which involved copying a know working Grub configuration file from some kind soul on the net, modifying it for my particular system and replacing the one already installed. I did this with a Knoppix LiveCD.

So now I can boot the system, but my display image is shifted way off the screen and too low to click on anything.

Google Time >>>>> 2 hours later <<<< Ok I learned how to boot to a command line and edit the Xorg file to fix the entries that were incorrect for my common Nvidia card.

So now I could see my desktop, but it was at 1024×768 and what appeared to be 16 colors.

Google Time >>> 3 hours later <<< I discovered that there is no apparent way to get 32bpp, 3D acceleration, 85hz and 1280×1024 all at the same time like I have with Windows.

Bummer.

I settled for 1280×1024 24bpp and no 3d because I don't use it and Linux doesn't appear to have any games written for Linux anyhow.

So now I have the system up, am surfing the net and things look pretty good.

Time to add a printer.

I go to the control panel and click on printers and peruse the list but I don't see my Lexmark Multifunction listed?

I do see a similar model however so I decide to try this.

It installs easy enough, but when I go to print I get one line of gibberish on the top of the page, the page ejects and the next page does the same thing over and over and over again.

Rebooting the system does no good because the printer, like a mad beast, starts right up again wasting my paper.

Finally I turn the damm thing off while I.....

Google Time << 4 hours >>> I discover Print Ques, printer names and the wonderful account called root. I finally figure out how to purge this thing and with some trepidation I turn the printer on and thankfully it behaves.

*Oh well, I don't need to print right now anyhow so on to my network. The problem is, I can't see my other 3 Windows Vista machines. And now it's.....
you guessed it!*

GOOGLE TIME << infinite >>> I discover something called Samba, but I also learn that Microsoft Vista and Samba are not friends but only after a day and a half of playing with a smb.conf file and reading maybe a hundred web pages devoted to helping people get Samba working, and this is with Windows XP which supposedly plays nicely with Samba. I wouldn't know know, I never got Samba working.

At this point, I took the Linux CD's, all 6 of them including the rescue CD which seems useless BTW and tossed them, violently I might add, into the dustbin.

I have wasted far too much time with this Linux crap and I don't intend to waste another millisecond trying to shoehorn this pile of garbage into my systems.

*I can see why Linux is free.
It doesn't work!*

*I can also see why it is not even making the slightest ding in Microsoft's armour:
It, Linux, doesn't work.*

I'm not sure, but if the Linux users expect people, ordinary people, to spend their lives Googling in order to make Linux work, they are daft.

Maybe in 10 years Linux might be able to install and work properly, but for now Linux is too difficult and too buggy for the average user.

Karla

– Soli Deo Gloria

30 Useful Vista Tips

DECEMBER 13, 2007

CATEGORIES: TECH TIPS

Found this [thread](#) at www.merawindows.com with some interesting tips for Vista, including how you can “trick” Vista into installing on a PC with less than 512MB of memory.

– Soli Deo Gloria

My Yearly Overview

DECEMBER 25, 2007

CATEGORIES: MISC

Hope everyone is having a great Christmas out there. This year my web site got ~40,000 unique visitors: the majority being hits on this blog. Since I have your eyes, let me introduce you to my official presidential candidate:

Here is an interview with Ron on the Glenn Beck program which I think you will find most interesting:

Part 1 - <http://youtube.com/watch?v=8Xon3d9EuoE>

Part 2 - <http://youtube.com/watch?v=OELpPoT5Xao>

Part 3 - <http://youtube.com/watch?v=8rUEHtJTEXI>

Part 4 - http://youtube.com/watch?v=UuCfpxNZ_x8

Part 5 - <http://youtube.com/watch?v=UOuTDYKnQoE>

Part 6 - <http://youtube.com/watch?v=1xffw36-eo>

My personal accomplishments include [this blog entry](#) being featured in the April 19th edition of the [Windows Secrets newsletter](#), achieving the Master level as a technical expert in the Vista Zone at the web site www.experts-exchange.com and deployment of 50 Vista workstations using Microsoft SMS 2003 BDD/OSD.

Next year I plan to move to Windows Vista x64 at home and I'm sure there will be a few snags I'll have to write about here. I plan to update my techniques on removing malware. I have also been toying with various ideas on how to bring video to the blog.

I leave this year with the following bible passage, Romans 12:17-21:

Do not repay anyone evil for evil. Be careful to do what is right in the eyes of everybody. If it is possible, as far as it depends on you, live at peace with everyone. Do not take revenge, my friends, but leave room for God's wrath, for it is written: "It is mine to avenge; I will repay," says the Lord. On the contrary: "If your enemy is hungry, feed him; if he is thirsty, give him something to drink. In doing this, you will heap burning coals on his head." Do not be overcome by evil, but overcome evil with good.

– Soli Deo Gloria

Bill Gates' Last Day

JANUARY 10, 2008

CATEGORIES: JOKE

<http://www.youtube.com/watch?v=HEWMC4usEIM>

When Local Administrator Isn't Enough

JANUARY 12, 2008

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Here's an interesting problem called in by another tech to me. It seems that the tech was unable to delete some registry keys relating to UPS Worldship. He was logged in as a local administrator. Attempts to delete the keys came back as "Access Denied". Upon trying to view the owner of said keys it was listed as "unknown", nor could we take ownership of the keys. The only thing left was to try to run regedit under the local system account.

Microsoft defines the LocalSystem account as the following:

The LocalSystem account is a predefined local account used by the service control manager. This account is not recognized by the security subsystem, so you cannot specify its name in a call to the LookupAccountName function. It has extensive privileges on the local computer, and acts as the computer on the network. Its token includes the NT AUTHORITYSYSTEM and BUILTINAdministrators SIDs; these accounts have access to most system objects. The name of the account in all locales is .LocalSystem. The name, LocalSystem or ComputerNameLocalSystem can also be used. This account does not have a password. If you specify the LocalSystem account in a call to the CreateService function, any password information you provide is ignored.

Getting regedit to run under local system can be done a number of ways, however, the easier way I found is to use psexec: "psexec -i -s regedit.exe". Upon doing this, we were able to delete the registry keys.

You can verify that regedit is running under "NT AUTHORITYSYSTEM" by running Process Explorer as administrator, drilling into PSEXESVC and clicking the Security tab.

– Soli Deo Gloria

Fun With HP Printers

MARCH 2, 2008

CATEGORIES: MISC, TECH TIPS

A few days ago I was seeing some weird messages on our HP Jetdirect printer. Doing a little Google searching I found out that it is possible to send messages to HP printer so they show on the LCD display! I found this [utility](#) you can install on Windows. Just install it, enter the IP address of the printer and put your message in. The message will be erased if the printer is power cycled.

If you do this at the work place: use caution. Your IT department may not like you very much if they catch you sending messages to their printers. 😊

– Soli Deo Gloria

Windows Server 2008 beats Windows Vista Performance

MARCH 15, 2008

CATEGORIES: OPERATING SYSTEM

Someone dude from Microsoft took Windows Server 2008 and turned it into a [viable desktop operating system](#). Performance gains over Vista vary in the 11%-17 range according to [this exo-blog](#). This [guy](#) claims up 20% in his tests.

– Soli Deo Gloria

Windows XP OEM Activation

MARCH 21, 2008

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Ran into an interesting problem when imaging a Dell D510 and placing that image onto a Dell D630. It appears the Dell OEM version of Windows XP doesn't like hard drive cloning. When you would attempt to run `msoobe /a`, the space where installation ID was supposed to be was completely blank. Attempts to change the `OOBETimer` value among other things was unsuccessful.

The solution? Run `sysprep`. Somehow, `sysprep` has the magic to fix activation woes. After `sysprep` ran (*we did the reseal option*), we logged in and the installation ID was now being generated.

Did I ever mention what a pain in the neck Windows activation is? Oh yeah, only about a million times!

– Soli Deo Gloria

Locking Down Specific Profiles with Local Group Policy

MAY 1, 2008

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I recently had to lock down a profile on a user account running on a Terminal Services server. You think by 2008 Microsoft would have released a tool that would do this with ease. I tried SteadyState, but it would bomb out during the installation. Microsoft actually does have an article that describes how to do this [here](#). Make sure you take some Excedrin before reading it.

There are two branches of Group Policy: computer and user. The computer settings are embedded in registry.pol at %SystemRoot%\System32\GroupPolicy\Machineregistry.pol. The user settings are embedded in registry.pol at %SystemRoot%\System32\GroupPolicy\Userregistry.pol. The computer settings are initialized when the OS boots, so you can not do any “switch-a-roo” with them, however, this will work with the user branch.

Not satisfied with Microsoft’s solution, I did some Googling and found this article on [Juice](#). The article is gear toward doing this across multiple computers over a network. The bottom line is that we can make the account we want to lock an administrator, login in and use gpedit.msc to lock things down in the user branch. When done, take the account out of the administrator’s group, go to %SystemRoot%\System32\GroupPolicy and grant the local Administrator’s group Deny rights to the whole folder. That way, anyone logging in will get the policy, except Administrators, because they don’t have rights to read the folder and thus the policies.

– Soli Deo Gloria

Winrar 3.62 for Free

MAY 5, 2008

CATEGORIES: MISC

Found this on SlickDeals.net. Appears you can snag [Winrar 3.62 for free](#) as it was given out to subscribers of a German PC magazine.

The rarreg.key file is given in the thread to register the software.

– Soli Deo Gloria

Sysinternals Live Site

MAY 30, 2008

CATEGORIES: TECH TIPS

All of Systinternals tools are available live @ <http://live.sysinternals.com/>

– Soli Deo Gloria

Windows 7 Blog

AUGUST 16, 2008

CATEGORIES: MISC

Microsoft has just created a blog on the development of [Windows 7](#), the successor to Windows Vista. There really isn't anything exciting there now, but it might be worth checking out over time.

As you may have noticed, the postings on my blog have slowed down. June was the blog's 3 year anniversary and I didn't even post anything! I've been busy working on pushing out programs with SCCM 2007 and playing World of Warcraft. I think posting on SCCM 2007 may be a bit boring, as only high level companies are going to be running it and therefore will be out of reach of the common tech. We also upgraded to NOD32 from Symantec Antivirus, so I don't really have any more spyware stories to whip up at this time.

-Soli Deo Gloria

Quick and Dirty ImageX

AUGUST 24, 2008

CATEGORIES: TECH TIPS

Update 8/26/08: Forgot about the WinPE 2.0 uberbug with diskpart. See this article [here](#). To fix this, place the following in `uberbug.reg` and then add that to the menu

Windows Registry Editor Version 5.00

```

“LessThan4GB”=dword:00000000
“Between4_8GB”=dword:00000000
“Between8_32GB”=dword:00000000
“GreaterThan32GB”=dword:00000000

```

Here’s a quick and dirty overview of how to replace Norton Ghost with ImageX. ImageX captures information about the file system, but nothing of disk structures (*master boot record, sectors, etc*). Therefore, in using ImageX, we need to include writing out the boot sector with `bootsect.exe`. Since ImageX is command line driven, the first order of business is finding a GUI wrapper. I found such a wrapper called [GImageX](#). GImageX interacts directly with `wimgapi.dll`, therefore, some support files from Microsoft WAIK will be needed. Specifically, that includes: `imagex.exe`, `intlcfg.exe`, `wimgapi.dll`, `wimfltr.inf`, and `wimfltr.sys`.

I threw all of the files, including the WIMs I captured, on a network share with these support files (*don’t forget bootsect.exe!*). I then wrote a simple batch file:

```

@echo off
:TOP
regedit /s uberbug.reg
cls
echo Microsoft ImageX Menu by Adam Leinss
echo -----
echo.
echo 1. Prep Disk (WARNING: THIS DESTROYS ALL DATA ON DISK!)

```

echo 2. Prep Boot Sector for Windows XP OS

echo 3. Prep Boot Sector for Windows Vista OS

echo 4. Run GImageX

echo.

echo 5. Exit

echo.

Set /P sel=Make your choice:

echo.

For %%a In (1, 2, 3, 4, 5) Do if "%sel%"=="%%a" Goto SELECT_%%a

echo Invalid selection. Valid values are 1 thru 5. Press Enter To continue

pause>NUL

Goto TOP

:SELECT_1

mbrwiz /disk=0 /part= /del /confirm*

diskpart -s diskprep.s

Goto TOP

:SELECT_2

bootsect /nt52 sys

Goto TOP

:SELECT_3

bootsect /nt60 sys

Goto TOP

:SELECT_4

gimagex.exe

Goto TOP

:SELECT_5

Goto :EOF

The diskprep script I use:

select disk 0

clean

```
create partition primary
format quick
active
assign letter=C
```

This gets the disk nice and clean for us to use. You actually have to use [MBRWiz](#) to do the initial wipe, as “diskpart clean” only wipes one partition (versus **diskpart clean all** which takes forever). This is never an issue with Ghost, as it writes out the file system sector-by-sector.

After cleaning the disk, you can pick either #2 or #3 to prep the boot sector depending on what OS you are going to deploy.

Finally, we run GImageX, click the Apply tab and pick the Source/Destination. Now you have an imaged PC, just like with Ghost!

I used the WinPE 2.0 install media from SCCM 2007 to boot the PC and connect to the network share, but you can use any flavor of WinPE you want (*BartPE*, *WAIK PE*, etc). I found decent WinPE 2.0 (*Vista based*) setup instructions [here](#).

Update (9/9/08): If you use WinPE 1.x: it has an older version of diskpart that does not have the format command built-in. So you can either update the version of diskpart on the WinPE 1.x disc or re-write the script so the the format command in diskprep.s is taken out, then you can use “format C: /fs:ntfs /quick” on another line. The WinPE 1.x diskpart also does not handle USB flash drives correctly and you cannot simply copy diskpart from WinPE 1.x to WinPE 2.0.

Therefore, I strongly urge you to use WinPE 2.0 for dealing with images.

Sample VBScript code below to map network drivers if you have multiple locations on different subnets. Note that if you just use straight up net use commands, you might run into timing issues since WinPE will not wait until executing the next line of code. Using the run object with the 1 option will prevent WinPE from continuing on until the drive is mapped.

```
Set objShell = WScript.CreateObject("WScript.Shell")
Set colItems = GetObject("winmgmts://.").ExecQuery("select * from Win32_NetworkAdapterConfiguration where IPEnabled=TRUE")
For each objItem In colItems
If Not IsNull(objItem.IPAddress) Then
```

```
strIP = "IPAddress: " & objItem.IPAddress(i)
End If
Next
If InStr(strIP,"10.3.") Then
objShell.run("net use * \server3osd /user:yourdomainsrvacct secretpwd"),1,true
ElseIf InStr(strIP,"10.2.") Then
objShell.run("net use * \server2osd /user:yourdomainsrvacct secretpwd"),1,true
ElseIf InStr(strIP,"10.1.") Then
objShell.run("net use * \server1osdsccm2007images /user:yourdomainsrvacct
secretpwd"),1,true
End If
```

*Update (8/20/11): Upon designing a simplified GimageX setup for another company, I discovered for Windows 7 you can use BCDBOOT to fix boot sector/BCD issues after wiping a disk and using the raw imagex binaries to throw down an image. Copy the x86 version of bcdboot.exe from an existing Windows 7 installation (to match your version of WinPE which is likely x86) to your network share, then issue **bcdboot C:windows** after the image is laid down and the BCD will be fixed. You can place this command after gimagex.exe in the menu so you don't have to run it as a menu option if the only operating system you are imaging is Windows 7.*

Though I didn't use it, you can also use the Microsoft Script Encoder to obfuscate your VBS script code to keep out the nosy Nellies.

– Soli Deo Gloria

Leinss.com Gets a Makeover!

AUGUST 28, 2008

CATEGORIES: MISC

Take a look at the sexy new leinss.com layout! I've been bored recently with World of Warcraft and decided to do something about my ugly web site. The web site expands to the full size of the screen now and the font is bigger. I'll be going through and reviewing all sections to see what needs to get added/removed/updated. You may have to hit "Shift-F5" to see the new site.

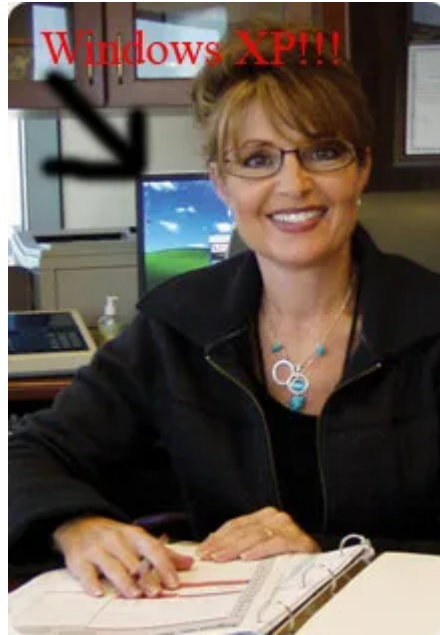
– Soli Deo Gloria

Sarah Palin uses Windows XP

AUGUST 31, 2008

CATEGORIES: JOKE

I was worried that she might be a Mac user, but no, she uses Windows XP! Anyone that uses Windows XP is alright in my book.



- Soli Deo Gloria

Microsoft's New Makeover Ad

SEPTEMBER 6, 2008

CATEGORIES: MISC

Bill Gates and Jerry Seinfeld

Personally, I was not impressed. 😞

– Soli Deo Gloria

John Daker Makes A Comeback!

SEPTEMBER 7, 2008

CATEGORIES: JOKE

I was looking through the files from my old web site and found this awesome remake of “That’s Amore!” from [John Daker](#).

– Soli Deo Gloria

XMRadio: What a Pain to Cancel

SEPTEMBER 20, 2008

CATEGORIES: MISC

I decided to get a MP3 player recently and dump XMRadio. They sent me a notice in the mail to renew for 3 years, but I did not want it anymore, so I threw the offer away. Just this month: I see a charge for \$377.98 from XMRadio. I immediately called their 1-800 number and the first prompt said my credit card was expired. What I would like to know is if my credit card is expired and storing the CVV number is against credit card regulations, how did XMRadio charge me? I gave all my personal information to the first representative who transferred me to the “accounts department”. I was promptly hung up on.

I called back, talked to another customer service representative and again was transferred to the accounts department. The representative tried to entice me with free months of service and a discounted rate of \$4.99 per month. I kept having to say “just cancel it” to get my point across. I also went into my credit card account online and disputed the charge, asking them to block XMRadio from making charges against my account.

Will update this entry with any further information! 😊 Next time: I will use a temporary credit card # I generate through Paypal so merchants will no longer have access to my real credit card number.

Update 9/26/08:

XMRadio refunded my request. Discover card is now on my hit list! To be continued!

– Soli Deo Gloria

Utility Review: Alcohol 52%

OCTOBER 3, 2008

CATEGORIES: REVIEW

It sometimes is hard finding software that will work on Windows Vista. Case in point: finding software that will load ISO images as a drive letter. On Windows XP, I use to use CloneVirtualDrive by SlySoft. Unfortunately, this software does not work on Vista. The challenge is to find something free, reliable and of course, Vista compatible.

Installation is pretty straight forward: the first part will require a reboot. After the reboot, you need to run the setup again. During the setup, you are offered a “free toolbar”. You can decline the installation of this toolbar.

Usage is pretty easy: launch Alcohol 52% and add your ISO image to the list. It keeps a list of the current ISOs you have loaded recently. Then, right-click on the ISO and choose “Mount on Device”. The CD or DVD is then loaded as a virtual drive letter.

The utility also has a neat ISO maker. Place a CD or DVD into the drive and click through the wizard: nothing could be easier. This utility would be so sweet if it would write CDs/DVDs as well. Alas, it is freeware, so you can't ask too much.

Note that the license states this is for home and personal use only.

Verdict: 4 stars

– Soli Deo Gloria

Who's a Local Administrator?

OCTOBER 19, 2008

CATEGORIES: TECH TIPS

Here's VBScript code you can use in a login script or from SMS to find out who has administrator rights on a PC:

' Variables

Dim objFileSystem, objOutputFile

Dim strOutputFile

' Init objects

Set Shell = CreateObject("WScript.Shell")

Set oNet= WScript.CreateObject("WScript.Network")

Set filesys = CreateObject("Scripting.FileSystemObject")

' Grab computername

computername = Shell.ExpandEnvironmentStrings("%computername%")

' See if we can do something "Admin" like

if filesys.FolderExists("\ & computername & "Admin\$System32") then

' Grab username

oUser = oNet.UserName

' Set filename to computername.username.txt

strOutputFile=computername & "." & oUser & ".txt"

Set objOutputFile = filesys.CreateTextFile(strOutputFile, TRUE)

'Close file

objOutputFile.Close

Set objFileSystem = Nothing

end if

Only users with administrator rights can get to administrative shares. So if we can get to `\mycomputerAdmin$System32`: we are an administrator. The script then writes out the logged

in user's name to a file in the format of `computername.username.txt`.

*Note: The appending of `.txt` is purely for cosmetic reasons. The script comes from two parts of source code I "stole" from the Internet. Also, if you want the file written out to a specific server share: append **`\\yourserveryourshare`** before `computername` set by `strOutputFile`*

Soli Deo Gloria

Mark Russinovich Goes “Deep” on Windows 7

NOVEMBER 4, 2008

CATEGORIES: TECH TIPS

Warning: This video is very geeky.

Mark goes in deep on breaking inefficient “locks” in Windows 7, support for 256 processors (*up from 64*) and Miniwin.

[Link](#)

Soli Deo Gloria

Mass Storage Headache, Windows 7 build 6801

NOVEMBER 11, 2008

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I finally got my hands on the first publically available Windows 7 build from the Microsoft PDC 2008: build 6801. This build is already quite old (*build 6933 is available internally at Microsoft*). My first impressions: UAC is much more subdued. I was able to install programs and change Windows settings without once getting prompted for elevation. Microsoft now lets you set different levels of UAC: XP demigod style to very restrictive. The networking control panel seems much snappier. The taskbar is disabled in this build, however, if you head over to www.withinwindows.com or chris123nt.com they figured out a way to bring back the feature. Windows 7 looks very promising from this early build.

I ran into a mass storage snafu recently with new RAID controllers on the Dell 390 and T3400 for Windows XP. It seems the days of just specifying vendor and device ids in sysprep.inf are gone. You now have to specify the subsystem id in the device id string as well.

Case in point: I added the Intel ICH8R RAID drivers for the Dell T3400 which uses SATA RAID. When trying to image a T3400, I kept getting a 7B stop error code.

My sysprep statement was:

```
PCIVEN_8086&DEV_2822=C:iddlt3400iastor.inf
```

Various drive modes in the BIOS can be specified such as SATA, RAID and AHCI. Thinking this was an AHCI problem, I added

```
PCIVEN_8086&DEV_2922=C:iddl390iaahci.inf
```

No go. The fun part is that you can look at your old mass storage statements over and over again, yet you will never see the problem. After poking around in TXTSETUP.OEM and the INF files, I found out that you need to specify the subsystem id. For the above statements, that would be:

```
; SCSI SATA RAID driver for Dell Precision T3400  
PCIVEN_8086&DEV_2822&CC_0104=C:iddlt3400iastor.inf
```

```
PCIVEN_8086&DEV_2922&CC_0106=C:iddlt3400iaahci.inf
```

```
PCIVEN_8086&DEV_2821&CC_0106=C:iddlt3400iaahci.inf
```

PCI32 doesn't give the subsystem id unfortunately:

```
Bus 0 (PCI Express), Device Number 31, Device Function 2
```

```
Vendor 8086h Intel Corporation
```

```
Device 2822h 80801 (ICH8R/ICH9R) SATA RAID Controller
```

```
Command 0007h (I/O Access, Memory Access, BusMaster)
```

```
Status 02B0h (Has Capabilities List, Supports 66MHz, Supports Back-To-Back Trans.,  
Medium Timing)
```

```
Revision 02h, Header Type 00h, Bus Latency Timer 00h
```

```
Self test 00h (Self test not supported)
```

```
PCI Class Storage, type RAID
```

```
Subsystem ID 02141028h Unknown
```

Which leaves you with installing Windows XP, feeding the driver to the system and then going to the Device Manager, drilling into the device, clicking on the Details tab and then selecting Hardware IDs to get the device string.

If you don't want to go through all that hassle, you can just specify all the subsystem ids. With PCI32, you can narrow down the sections you need:

```
; SCSI SATA RAID driver for Dell Precision 390
```

```
PCIVEN_1000&DEV_0054&SUBSYS_1F041028=C:iddlp390symmpi.inf
```

```
PCIVEN_1000&DEV_0054&SUBSYS_1F061028=C:iddlp390symmpi.inf
```

```
PCIVEN_1000&DEV_0054&SUBSYS_1F071028=C:iddlp390symmpi.inf
```

```
PCIVEN_1000&DEV_0054&SUBSYS_1F081028=C:iddlp390symmpi.inf
```

```
PCIVEN_1000&DEV_0054&SUBSYS_1F091028=C:iddlp390symmpi.inf
```

Specifying more device ids is probably better than less.

– Soli Deo Gloria

Installshield Repackager 8 for Free

DECEMBER 17, 2008

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I found this little program while looking for quiet installation instructions for the latest version of Quicktime:

[Installshield Repackager 8](#)

This appears to be a legit link, as it's also given in this [Microsoft Technet article](#).

Repackagers allow you to create your own custom installations. The Technet article above actually gives a good overview of this process.

– Soli Deo Gloria

Windows 7 Beta: Available for Public Download Starting 1/9/09

JANUARY 8, 2009

CATEGORIES: MISC, OPERATING SYSTEM

Windows 7 build will be available for the first 2.5 million downloaders and the product key will work until August 31, 2009. Beta copies are also available on MSDN and Technet.

[Source](#)

– Soli Deo Gloria

Windows 7 Coming in September 2009?

FEBRUARY 26, 2009

CATEGORIES: MISC

Microsoft has failed to meet a deadline in the past 10 years, but maybe they will make this one:

[http://www.bloomberg.com/apps/news?
pid=20601204&sid=aKPIsoFXWWDY&refer=technology](http://www.bloomberg.com/apps/news?pid=20601204&sid=aKPIsoFXWWDY&refer=technology)

(5/3/09) Update: Pocket-Lint.com says wide spread distribution will be October 23rd:

[http://www.pocket-lint.com/news/news.phtml/23846/acer-confirms-windows-7-23-
october.phtml](http://www.pocket-lint.com/news/news.phtml/23846/acer-confirms-windows-7-23-october.phtml)

– Soli Deo Gloria

Microsoft DaRT 5.0 for Free (30 Day Trial)

FEBRUARY 27, 2009

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Microsoft has a 30 day trial version of the ERD Commander, a.k.a. [Microsoft Diagnostics and Recovery Toolkit version 5.0](#). This might come in handy if you are in a pinch to fix a dead PC.

(5/3/09) Update: Microsoft removed the link, and due to other websites linking to a copy on my website, I removed mine as well.

Description of the CD follows:

Microsoft Diagnostics and Recovery Toolset 5.0 is a complete suite of powerful and versatile tools that allow you to repair unbootable or locked-out systems, restore lost data, and diagnose system and network issues while the system is safely offline. Microsoft Diagnostics and Recovery Toolset 5.0 includes the following tools

- * Emergency Repair Disk (ERD) Commander
- * ERD Commander Boot Media Wizard
- * ERD Help

- * Chkdsk
- * Command Line
- * ERD Explorer
- * File Search
- * Notepad
- * Unzip
- * Windows Shell

- * Crash Analyzer Wizard
- * Disk Commander Wizard
- * Disk Wipe
- * ERD Registry Editor
- * ERD System Restore Wizard
- * File Restore
- * Hotfix Uninstall Wizard

- * Locksmith Wizard
- * Solution Wizard
- * System File Repair Wizard

- * Autoruns
- * Disk Management
- * Event Viewer
- * Services and Drivers
- * System Information

- * File Sharing
- * Map Network Drive
- * TCP/IP Configuration

Supported platforms:

- * Windows(R) 2000 (x86), latest service pack
- * Windows XP (x86), latest service pack
- * Windows Server 2003 (x86), latest service pack

Unsupported platforms:

- * Windows Vista(TM) (All CPU architectures)
- * Windows "Longhorn" Server (All CPU architectures)
- * All x64 CPU architectures

– Soli Deo Gloria

More Tools to Fight Malware and Viruses

MARCH 1, 2009

CATEGORIES: SPYWARE, TECH TIPS

As time passes, viruses and malware are getting very hard to clean up when Windows is running. Therefore, we need some tools that do offline virus scanning. Correction: **FREE** tools. After doing some reason, I have found some very decent products for doing this.

One is the **F-secure Rescue CD version 3.01**. This is a Linux based rescue disc that can read/write NTFS partitions. The CD supports updating the virus definitions either via the Internet or a USB stick. It appears that F-Secure is using the Kaspersky engine for detecting viruses and according to VB100: Kaspersky ranks up there with ESET. The CD will rename infected files with a file extension of .virus, but will not delete or disinfect them. I tried the manual update routine by downloading <http://download.f-secure.com/latest/fsdbupdate.run> to a USB stick. I placed the USB stick in the computer, booted from the CD and it found the updates right away during the boot process. This is very useful, especially if the CD fails to find a NIC driver for your PC. I tried the Internet auto-updating on a Dell Optiplex 745 and GX280: both worked flawlessly.

A similar CD is available from BitDefender called **BitDefender Rescue CD 2008**. The CD actually boots to a screen that says BitDefender 2009. This CD is also Linux based. The virus tests run by VB100 show a less stellar product than F-secure. The CD, however, has a bit more functionality. The CD boots to a XWindows environment with Firefox and a file manager called Midnight Commander. You can also manually update virus definitions by running a script from the desktop. It appears, however, you have to have Internet access to update the virus definitions whether using the manual script or automatic update. BitDefender gives you options for each suspect file found: leave alone or delete.

Since I was already using a WinPE 2.0 disc to push out images, I wanted to find a free solution I could add to this disc.

(WinPE 2.0 is available for free in the latest WAIK: see

<http://www.svrops.com/svrops/articles/winvistape2.htm>)

Sophos has a free commandline scanner called **Sophos SAV32CLI** at

<http://www.sophos.com/support/knowledgebase/article/13251.html>. Sophos ranks very well at the VB100. I suggest throwing it on a network share and then just mapping a drive to that

network share. You can also use USB drives in WinPE 2.0, so you can also place the files on a USB stick. The readme.txt lists all of the command line options you can use, but I simply use "X:avsophossav32cli.exe -di -dn C:". This tells Sophos to show the filenames that it is scanning and to disinfect all the files it finds. There's also a logging option "-p=" you can use to pipe the results to a file or simply put a pause statement after this command if you are running the program from a batch file. Virus updates are available at <http://www.sophos.com/downloads/ide/>. Use the ZIP file version as the self-extracting file does **NOT** work on Vista/Server 2003. The command line version goes out of date after 3 months, so make sure you download a new copy or the new IDEs won't work after a while.

Mcafee has a command line scanner and virus definitions in their SuperDat virus files. Download the SuperDat exe from <ftp://ftp.nai.com/pub/antivirus/superdat/intel/>. Then extract the SuperDat file using the "/e" switch, for example: "sdat5569.exe /e". To scan the C: drive, you can use "scan c:/clean/winmem". There is a GUI wrapper included with BartPE for the Mcafee scanner if you want a GUI.

Update: As of 4/1/10, this trick no longer works. They removed scan.exe, messages.dat, etc. from the SuperDat file. You must now download vscl-w32-6.0.1-l.zip (Mcafee Commandline Tools) from Mcafee's site using a grant number to get scan.exe.

Trend Micro has a program called **Trend Micro System Cleaner**. This is a portable program that uses the regular spyware and virus definitions that their regular AV programs use. Trend Micro is not rated at VB100, but seems like a very decent product. You will need manually download the virus and spyware definitions yourself. Their web page is a bit confusing for updating the virus/spyware definitions, but upon running the program for the first time, it will give you the URL locations of what to download. Currently, the virus definitions are lpt\$vpn.XXX in ZIP format as lptXXX.ZIP from <http://www.trendmicro.com/download/viruspattern.asp>. The spyware definitions are ssapiptn.da5 in ZIP format as ssapiptnXXX.ZIP from <http://www.trendmicro.com/download/spywarepattern.asp>.

Upon running the scan from TSC in WinPE 2.0, I got an error message saying installation failed, but the program went on without any problems. You will, however, need to run this from writable media, such as a USB stick or a network drive with write access.

EmsiSoft has a neat command-line scanner called **a2cmd**. a2cmd can be downloaded [here](#). You can run a scan by running **a2cmd C:/deep/dq**. To update the signatures, you simply need to be connected to the Internet and then run **a2cmd /u**.

Microsoft released a new standalone virus scanning tool in April 2011 called the [Microsoft Safety Scanner](#). The download expires after 10 days. It did not work in the WinPE 3.0 disc I tried, but it did work in the disc I built from the Win7PE project from [reboot.pro](#)

Still in beta, but handy none the less: [Microsoft Standalone System Sweeper](#). This tool will download WinPE + the standalone system sweeper and definitions (*the same one that that comes with Microsoft DaRT 6.x and beyond*) and build an ISO for you, for FREE! Now you can boot from a clean WinPE CD and disinfect your PC in safety.

Now that described the elaborate ways to download the programs and the signatures that go along with them, there is a real easy of having it done for you: [Multi-AV Scanning Tool](#). This web site is in another language, but you should be able to find the download link (*look for **Download von www.pctipp.ch** on the bottom of the page*). You run the program which will extract to C:AV-CLS. From there, just run the menu options for each and it downloads the programs and the signatures automatically.



Name	Date modified	Type	Size
A2	10/26/2010 10:20 ...	File folder	
AntiVir	10/26/2010 10:15 ...	File folder	
Sophos	10/26/2010 10:03 ...	File folder	
Trend	10/26/2010 10:11 ...	File folder	
Avira.kix	10/10/2010 11:02 ...	KIX File	4 KB
avira.lic	9/17/2010 1:31 PM	LIC File	2 KB
AVP_LOC.DLL	6/1/1999 3:00 AM	Application extens...	28 KB
EmsisoftAnti-Malware.kix	10/10/2010 11:02 ...	KIX File	5 KB
Initial.kix	10/10/2010 11:01 ...	KIX File	1 KB
KAV.kix	10/10/2010 11:01 ...	KIX File	6 KB

There is an Avira command line scanner that is available with this toolkit with a hbedv.key license file generated specifically for this tool. The Kaspersky version that comes with this version is the DOS version and won't run on WinPE or under x64 operating systems (*the author says he will remove it in future versions*).

There is another program that does nearly the same thing, but unfortunately it deletes the signatures when it is done scanning the drive. This program is called AVERT. I prefer using the Multi-Av Scanning Tool for this reason.

These products do not work in WinPE 2.0, but can be quite useful within Windows:

MalwareBytes Anti-Malware: One of the best spyware scanners I have found. Malwarebytes Anti-Malware can be found at <http://www.malwarebytes.org/>. Note that the free version just has the scanning ability. If you want the realtime access protection, you will need to purchase the program

SUPERAntispyware Portable: Simliar to Malwarebytes, but in a portable version. I like the speed at which it scans and how it empties the recycle bin after cleaning the files so you don't find the dormant infection again.

– Soli Deo Gloria

What Not to Capture

MARCH 9, 2009

CATEGORIES: JOKE, MISC

So today I was hunting around the Internet trying to find a viewer that would open a file with a HWP extension (*don't ask*). Anyways, I happened to come across this blog...



and saw this guy blowing his nose with a sock.

Found @ <http://hunjang.blogspot.com/2006/05/hangu-viewer-2002-2005.html>

– Soli Deo Gloria

Advanced Malware Cleaning

MARCH 19, 2009

CATEGORIES: OPERATING SYSTEM, SPYWARE, TECH TIPS

Found this video the other day on Technet of an updated video of Mark Russinovich teaching techies how to clean malware: <http://www.microsoft.com/emea/spotlight/sessionh.aspx?videoid=359>

NOTE: If you want an offline copy, use [URLSnopper](#) to get the hidden URL, then use a trial version of [Hidownload](#) to download it. I've provided a local copy on my web site [here](#). Make sure to right-click the file, do a target save-as to save it to your PC instead of streaming it.

– Soli Deo Gloria

Conficker Cleanup

APRIL 1, 2009

CATEGORIES: SPYWARE

Had some people infected with Conficker, so I put the Microsoft patch for MS08-067 and the NOD32 removal tool out at <http://www.leinss.com/files/vanity/conflicker/>

You might need to rename the removal program to get it to run.

-Soli Deo Gloria

R.I.P Linksys BEFW11S4V3

APRIL 7, 2009

CATEGORIES: MISC

So tonight I come home to no Internet. I do the power cycle the RoadRunner cable modem, then power cycle the router routine. Then I notice I cannot ping the router. Plug my computer directly into the cable modem and it works just fine. Plug my PC back into the router and the Ethernet link keeps going up and down like a bouncing ball. Interestingly enough, the wireless part of the router works perfectly fine. The router was 5 years old and it gave me plenty of use.

I've ordered the Linksys WRT54GL from Newegg.com: hopefully it lives up the same standard of craftsmanship.

– Soli Deo Gloria

Paragon Drive Backup 9 Personal for Free

APRIL 8, 2009

CATEGORIES: TECH TIPS

...for the next 12 hours....go grab it! Normally \$39.95

<http://www.giveawayoftheday.com/paragon-drive-backup-9-personal/>

Oh, the link points to DriveBackup9Pers.zip.

– Soli Deo Gloria

RoadRunner Bandwidth Caps

APRIL 15, 2009

CATEGORIES: MISC

Update (4/16/09): Looks like TWC is shelving the tiered pricing! Check it out:

<http://stopthecap.com/2009/04/16/victory-breaking-news/>

You probably have heard of the ridiculous bandwidth caps that Time Warner is testing. Their plan: \$54.95/month for 40GB of data per month! This seems to be both upstream and downstream data combined. Why might they be doing this?

From their financial statement:

<http://ir.timewarner.com/secfiling.cfm?filingID=950144-09-1481>

*“Technological advancements, such as video on demand, new video formats and Internet streaming and downloading, have increased the number of media and entertainment choices available to consumers and intensified the challenges posed by audience fragmentation. The increasing number of choices available to audiences could negatively impact not only consumer demand for the Company’s products and services, but also advertisers’ willingness to purchase advertising from the Company’s businesses. **If the Company does not respond appropriately to further increases in the leisure and entertainment choices available to consumers, the Company’s competitive position could deteriorate, and its financial results could suffer.**”*

Hulu.com, a web site that allows you to watch TV programs online, is also specifically mentioned:

*TWC’s video services face competition from a number of different sources, including companies that deliver movies, television shows and other video programming over broadband Internet connections, such as **Hulu.com**, as well as online order services with mail delivery, and video stores and home video services. Increasingly, content owners are using Internet-based delivery of content directly to consumers, often without charging a fee for access to the*

content. Furthermore, due to consumer electronics innovations, consumers will over time be more readily able to watch such Internet-delivered content on television sets.

So basically to drown out the competition to your video services: just make it really expensive to use them!

Brilliant!

Keep tabs on the ordeal at:

<http://www.dslreports.com/forum/r22161366-Look-outtiered-pricing-and-monthly-caps-coming->

P.S. Verizon FIOS not coming to Wisconsin anytime soon

P.S.S. Time Warner rep did not get back to me on what, if any changes, there will be for Business Class RoadRunner which I use.

– Soli Deo Gloria

Windows 7 RC is Here!

MAY 3, 2009

CATEGORIES: OPERATING SYSTEM, REVIEW

Well, it is if you have Technet. The RC was released April 30th and will be given to masses on May 5th. I wiped Vista off my work PC and installed the RC right away. They finally integrated the Windows Recovery environment right into the installation...so now you can hit F8 and get into it without having to hack it in. Startup is faster and yes, they finally put back a decent logo during the boot process! You can now change the background of the login screen with this [utility](#).

UAC is more subdued. This version of Windows seems what Vista was supposed to be. The previewing technology in the quick launch is pretty cool and hovering over the start menu "circle" causes it to "light up". They added a date to the clock in the bottom right and now a permanently integrated "Show Desktop" feature to the right of the clock. I do notice some graphical distortions from time to time. Windows 7 picked a WDDM 1.0 driver for the Q965 video driver in this Optiplex 745. It's a beta: what do you expect?

I played a little bit with XPM: basically a copy of Virtual PC running XP that runs under Windows 7. This feature might be more confusing than helpful. I was able to run Internet Explorer 6 "desktopless" which is pretty cool ([see auto-publishing here](#))...but how will you keep this VM patched? Do you really want a bunch of rogue VMs joined to your domain?

Overall, I'm pretty impressed by Windows Vista R2, I mean Windows 7. A Microsoft Springboard session on Windows 7 can be found @ <http://technet.microsoft.com/en-us/windows/dd459187.aspx?ITPID=istream>

– Soli Deo Gloria

Beta RSAT Tools for Windows 7 RC

MAY 7, 2009

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Looks like Microsoft removed the beta version of the RSAT tools for Windows 7 RC from their web site for some reason. Thankfully, I grabbed them before they were taken down. You can download them [here](#) from my web site.

Note that after you run the hotfix, you need to go into the Windows components and add them from there.

– Soli Deo Gloria

Windows 7 – RTW on October 22nd, 2009

JUNE 2, 2009

CATEGORIES: MISC, OPERATING SYSTEM

Windows 7 will RTM in mid to end of July, then RTW on October 22nd.

Source: http://news.cnet.com/8301-13860_3-10253924-56.html

– Soli Deo Gloria

Interesting Hacker Videos

JUNE 30, 2009

CATEGORIES: MISC, OPERATING SYSTEM

Update (10/5/09): I've removed the two videos from my web site due to bandwidth issues, but you can still find them on Google and Technet.

I was bored one day, so I decided to watch videos on Microsoft's Technet site. I came across Marcus Murray's videos and they are very entertaining to watch! Murray is a "White Hat" hacker. In this first video, [A Hackers Diary](#), Murray hacks into a FTP server running on a Windows 2000 server using a buffer overflow exploit.

In last video, [Knowing Your Enemy](#), Murray uses hash injection attacks...basically, he uses SAM hashes to impersonate other accounts....very cool! He also has a blog posting on using gsecdump [here](#).

– Soli Deo Gloria

Windows 7 build 7600 RTM?

JULY 13, 2009

CATEGORIES: MISC, OPERATING SYSTEM

Looks like we are getting very close or are at RTM level with Windows 7.

Rumours have stated it should be on MS Connect and MSDN by July 24th, so hopefully I can get it by then and write a report.

– Soli Deo Gloria

-1 for Xerox Tech Support

JULY 17, 2009

CATEGORIES: MISC

Tech support is really getting bad these days: my latest encounter was with Xerox tech support. We have a Xerox 8830 plotter in our engineering department. This is a printer that can do really large size drawings. We've been using Windows XP 32-bit for some time, but as we all know: 32-bit can't address more than 4GB of memory. In comes Windows XP x64! Windows XP x64 requires signed drivers and they have to be 64-bit. No fudging here!

I went off to Xerox's tech support site and found a PDF describing said x64 drivers, but there was no link:

[doc here](#)

Looking in the PDF, we find this filename:

Accxes11.0_PS_500_ENU_AMD64.exe

Not finding anything at Xerox, I decided to search the Internet and found a post by Scott Robins on 8/24/2006 in which he posts a INF file for WinXP x64 for both the 500 and 8800 series!

<http://www.winvistatips.com/installing-32-bit-printer-drivers-additional-drivers-x64-2-a-t189489.html>

I decided to start an e-mail dialog with Xerox tech support. They give me a link to the site with the section with no x64 drivers. When I mention this, they state that they **MUST** have a serial number to provide a solution. I gave them every number I could find from the plotter, but they still claimed I had not given them the serial number. When I asked if there were multiple x64 drivers for the Xerox 8830 (*why else would they keep asking for the serial number*), I was told no x64 drivers existed for the Xerox 8830. No explanation for the document describing the existence of said drivers was given or even guessed at.

I called a local printer service company called Trittech. The printer service technician had access to the service side of Xerox's web site and agreed with me that the drivers had existed at one

time, but were removed by Xerox and were probably being held on some secret Xerox FTP site and that I should call Xerox directly.

Upon calling their tech support line, Shawn confirmed that I had indeed given them the correct serial number. When I asked why he was able to figure this out and e-mail tech support was not, I was told that I did not have an active service contract on the device and that was why they couldn't find it in their system. Shawn was a bit more helpful by offering to download drivers from different printers and look at the INF files, but I told him I had already tried that without success. Shawn stated that he could not find them on their FTP site and was unable to explain the documentation pointing to the existence of the drivers. At least Shawn put forth some effort trying to help: e-mail tech support didn't lift a finger!

I was ready to given up when I contacted one last printer service company: Mastergraphics. This is actually the company that services the plotter. Larry, one of the service managers, stated the drivers for the 510 series would work for the 8830 as the 510 was built on the same architecture. Larry gave me the link and told me to contact him if I had any further questions.

Well, Larry is an angel sent from heaven, since these drivers work GREAT! It took a 3rd party company to fix the Xerox mess. I am still trying contact the head of Xerox tech support to find out why there is a lackadaisy attitude to fixing customer problems.

Drivers have been permalinked on my web site where Xerox can't remove them:

http://www.leinss.com/files/ACCXES12_7_3_HPGL2_500_XPx64.zip

I'll update this posting with any updates I get back from Xerox.

– Soli Deo Gloria

Paragon Partition Manager 9.5 Personal Edition for Free

AUGUST 11, 2009

CATEGORIES: MISC, TECH TIPS

Until midnight tonight, go grab it quick!

<http://dottech.org/freebies/7958>

– Soli Deo Gloria

IPrism and Windows 7

AUGUST 19, 2009

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Update: Ron Kaplan from St. Bernard contacted me about this article on 8/19/09. He indicated that the Iprism appliance would officially support Windows 7 in Q4 of 09. He agreed to post the below workaround for older versions of Iprism in their knowledgebase. That link is available [here](#).

For months, I've been plagued at work running Windows 7 with the IPrism Internet appliance (*web filter*). Every time I would hit a web page in the morning on Windows 7, Windows would pop up a dialog box asking for authentication. It would not accept my credentials, so I would end up hitting the ESC key a bunch of times so I could hit the IPrism appliance main page and log into there. This would last for 60 minutes and I would have to repeat this throughout the day.

I stumbled across this fix by accident...it seems that IPrism uses NTLM and not Kerberos for authentication. I even contacted their tech support and they did not clue me in on this. The default for Windows 7 seems to strictly use Kerberos above all else. The following steps seem to fix it:

Click Start

Click Control Panel

Click Administrative Tools

Double-Click Local Security Policy

In the left pane, click the triangle next to Local Policy

In the left pane, click Security Options

In the right pane near the bottom, double-click "Network security: LAN manager authentication level"

Click the drop-down box, and click "Send LM & NTLM – use NTLMv2 session security if negotiated"

Click OK

– Soli Deo Gloria

Free Partitioning Software that does 64-bit Windows

AUGUST 27, 2009

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I give you: Partition Wizard!

<http://dottech.org/freewaresr/8957>

– Soli Deo Gloria

Paragon Rescue Kit 8.5

SEPTEMBER 9, 2009

CATEGORIES: TECH TIPS

Today only!

[Paragon Rescue Kit 8.5](#)

Rescue Kit 8.5 Professional is designed to:

- Professionally correct the majority of system boot problems;
- Instantly retrieve valuable information from disk when your system fails to boot and save it to another hard disk/partition or burn to CD/DVD;
- Undelete accidentally deleted partitions;
- Establish a network connection to work with shared resources on the net;
- Secure data erasure with advanced wiping tool;
- Easily remove any Windows OS password;

– Soli Deo Gloria

Standalone System Sweeper Definitions for MS-Dart 6

SEPTEMBER 29, 2009

CATEGORIES: TECH TIPS

Microsoft pulled a fast one. The definitions for the Standalone System Sweeper from MS Dart 6 used to be at <http://go.microsoft.com/fwlink/?LinkID=96776>, but now only Forefront, Microsoft Security Essentials and Windows Defender are listed. In fact, the definitions are the same for Microsoft Security Essentials and the Standalone System Sweeper. The file you want to download is **mpam-fe.exe**.

– Soli Deo Gloria

Web site issues

OCTOBER 7, 2009

CATEGORIES: MISC

Update 10/8/09: All files should be restored. As the DNS propagation takes place, there should be less hits at Dreamhost and more here. I will likely shutdown down the Dreamhost site by Saturday night.

Update 10/7/09: I moved the web site to a new web host called Sharkspace tonight because Dreamhost kept fooling around and blog was mostly down during the past 5 days. I had to do some trickery with myPHPAdmin to get the database to import, so WordPress might be acting a little weird until I can fully look at it during the weekend.

Some files are missing (*particularly the larger ones*). I'll start restoring those on the morning of 10/8/09. The site is noticeably faster than it was on Dreamhost, so maybe Dreamhost having hardware problems was a good thing!

Original post continues....

The Dreamhost server I'm on (*tirane*) is having problems. You might experience 500 errors or slow access to the blog. Unfortunately, it's out of my control, but they are aware of it and are making adjustments. While I was logged into my panel, I noticed that GBs of data were getting pushed per day related to the Marcus Murray videos I posted a while back. Since I am on shared hosting and pay a measly \$8 a month to run this site, I cannot run a LeinssTube.com type site. Therefore, I pulled the videos. You can still find them at Microsoft's Technet site.

Thanks for your understanding.

– Soli Deo Gloria

Old Apple Games

OCTOBER 14, 2009

CATEGORIES: MISC

I saw someone at work playing the old Apple game Oregon Trail over the lunch break through their web browser @ [VirtualApple](#). They have this and many other classic Apple games from the late 80s.

Enjoy!

– Soli Deo Gloria

Create a BSOD on Demand

OCTOBER 16, 2009

CATEGORIES: OPERATING SYSTEM, TECH TIPS

We all love BSODs, especially ones that do not happen on our own computers. Nirsoft has created a utility called [StartBlueScreen](#) on their web site that will produce BSODs on demand! In addition to the torment you can cause with this utility (*psexec: hint, hint!*), you can force a blue screen on a system to get a memory dump and then analyze the memory stack with WinDBG.

*Update: Yes, this does work with psexec. Try **psexec -c -s \computerX
\serversharestartbluescreen.exe 0x12 0 0 0 0***

– Soli Deo Gloria

Microsoft Desktop Optimization Pack 2009 R2 is Released!

OCTOBER 22, 2009

CATEGORIES: TECH TIPS

MS-DaRT 6.5 which is part of the MDOP 2009 R2 now includes support for Windows 7!
Available now on MSDN/Technet.

Release notes for [MS-DaRT 6.5](#).

– Soli Deo Gloria

Windows 7 Upgrade Chart for Previous Versions

OCTOBER 22, 2009

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Upgrading Your PC to Windows 7

Upgrade FROM :		Upgrade TO:					
		Windows 7 Home Premium		Windows 7 Professional		Windows 7 Ultimate	
		32-bit	64-bit	32-bit	64-bit	32-bit	64-bit
Windows XP*		Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install
Windows Vista® Starter	32-bit	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install
	64-bit	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install
Windows Vista Home Basic	32-bit	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install
	64-bit	Custom Install	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade
Windows Vista Home Premium	32-bit	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install
	64-bit	Custom Install	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade
Windows Vista Business	32-bit	Custom Install	Custom Install	In-Place Upgrade	Custom Install	In-Place Upgrade	Custom Install
	64-bit	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install	In-Place Upgrade
Windows Vista Ultimate	32-bit	Custom Install	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install
	64-bit	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	In-Place Upgrade

Custom Install: A custom (clean) installation gives you the option to either completely replace your current operating system or install Windows on a specific drive or partition that you select. You can also perform a custom installation if your computer does not have an operating system, or if you want to set up a multiboot system on your computer.

In-Place Upgrade: Keeps your files, settings, and programs intact from your current version of Windows.

Windows Easy Transfer and the Windows 7 Upgrade Advisor are useful tools that can assist your upgrade. For more information about these tools and upgrading your PC to Windows 7, please visit: <http://windows.microsoft.com/upgrade>

Additional Notes:

*If you are upgrading from Windows XP you will need to back up your files and settings, perform a custom (clean) install, and then re-install your existing files, settings, and programs.

To upgrade an earlier operating system than Windows XP (e.g. Windows 95 or Windows 2000) you will need to purchase a full license of Windows 7 and perform a custom installation.

In the EEA/EU (including Croatia and Switzerland) and Korea, Microsoft will ship Windows 7 editions that do not include certain features such as Windows Media Player, and related technologies such as Windows Media Center. Upgrading to these editions will require a custom installation.

Upgrading Windows Vista from one language (e.g. English) to Windows 7 in a different language (e.g. French), requires a custom install.

SCECLI 1202 and 0x4b8 errors: Oh my!

NOVEMBER 10, 2009

CATEGORIES: OPERATING SYSTEM, TECH TIPS

We wanted to get rid of desktop users with administrator rights on Windows XP. With administrator rights, the user is given full control of the C: drive. Reducing users to a regular or power user would mean they would lose modify access to files/folders they need to write to. For example: Cribware stores its configuration options in C:\windows\cwwin.ini. This is poor programming practice no doubt, but short of reprogramming the program myself my hands were tied. We decided to open parts of the C: drive using a file security GPO, then run a VBScript later on that would move users from the Administrator's group to Power Users.

Upon creating and implementing the file security GPO, several workstations were throwing errors in the event log:

Event Type: Warning

Event Source: SceCli

Event Category: None

Event ID: 1202

Date: 11/9/2009

Time: 11:53:47 AM

User: N/A

Computer: XXXXXXXX

Description:

Security policies were propagated with warning. 0x4b8 : An extended error has occurred.

Drilling into C:\windows\security\winlogon.log, we find this on the problem PCs:

```
----Configure File Security...
```

```
Configure c:.
```

```
Warning 32: The process cannot access the file because it is being used by another process.
```

```
Error building security descriptor for c:\pagefile.sys.
```

```
Configure c:\program files.
```

File Security configuration was completed with one or more errors.

The section that was suppose to set security on the INI files in C:\windows was completely missing.

I tried to copy/delete/recreate the GPO database on the workstations in question with no success. That's when I called in Microsoft PSS to see what the deal was. The support person remoted into all of our DCs and everything at the Active Directory infrastructure level looked fine. He asked me to try the following command on a PC I pulled from the office:

```
secedit /configure /cfg %windir%\repair\secsetup.inf /db secsetup.sdb /verbose
```

Of course, this fixed this particular PC, so I went to try it on 5 test computers. Only 1 of the 5 was fixed with this solution.

Going back to the trusty Google, I decided to search for "File Security configuration was completed with one or more errors" instead of "1202" and "0x4b8". Up came up this gem of an [article](#).

Essentially, any file or folder that secedit (*what GPOs use to make these changes*) encounters with a NULL DACL, it just stops with a warning. There are two ways of attacking this: the GUI way and the command line way. The GUI way is right-clicking on a folder, going to Security>Advanced>Change Permissions and then check the box that says "Replace all child object permissions with inheritable permissions from this object". If you do a "gpupdate /force" and re-check the log event, SCECLI should now complete without error.

The command line way involves a 3rd party utility called [FILEACL](#).

By running **fileacl C:\windows /inherit /sub /files**, we refresh the ACLs on all files and folders defined at the C:\windows level.

The story continues...at first I couldn't get the CheckNullDacl.vbs script to work from the link above. When I copied the script from the web page, the "-1" in the script on line 72 wasn't really -1, but some weird character representing "-" and cscript would not run the script. After this was fixed, I decided to find out what files and or folders were causing this issue. PC after PC lead to the same file: C:\windows\opla.ini.

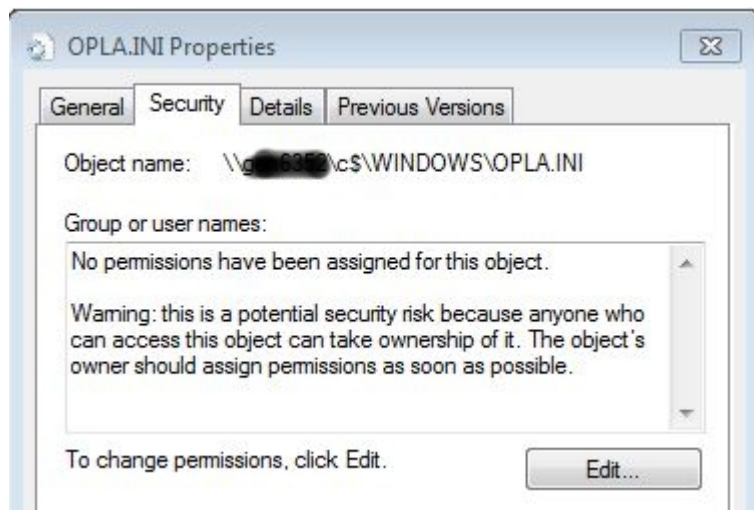
```

C:\temp>CheckNullDacl.vbs C:\windows
C:\temp>cscript CheckNullDacl.vbs C:\windows
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

Recursively searching C:\windows for NULL DACLs...
- Null DACL detected on C:\WINDOWS\OPLA.INI.

--[Complete]--

```



Peeking in the file, I found this:

```
W0000001=72,45,12632256,0,0,400,0,0,Arial,,CONFIDENTIAL,,,3,2
```

```
W0000002=72,45,12632256,0,0,400,0,0,Arial,,COPY,,,3,0
```

```
W0000003=72,45,12632256,0,0,400,0,0,Arial,,DRAFT,,,3,0
```

```
Courier New=57
```

```
Wingdings=75
```

```
Symbol=76
```

```
Times New Roman=77
```

```
Arial=81
```

I Googled this filename, having no idea what this file was. I found the text “C9300” in one of the OPLA.INI files and on Google this was related to an Okidata printer. Ah ha! We have 3 Okidata color printers in the building, but not everyone has it installed on their PC. This would explain why this file would be on certain PCs and not others. I confirmed the Okidata link by running Agent Ransack with a text search of “OPLA.INI” and found it in several DLL files in the Okidata 3037 print drivers. Upon running **fileacl C:\windows\opla.ini /inherit /replace**, the group

policies applied successfully! The shotgun approach isn't necessary and we only have to touch one file.

It's unclear why this possible problem is not listed in the Microsoft knowledge base, nor was it one of the solutions hinted at by PSS. I'm sure if I had continued to work with PSS, they might have suggested it down the road.

Local copies of [FILEACL](#) and [CheckNullDacl.vbs](#) on my web site.

– Soli Deo Gloria

Easeus Data Recovery For Free Until 11/13/09

NOVEMBER 13, 2009

CATEGORIES: OPERATING SYSTEM

You know what to do!

– Soli Deo Gloria

Flaky NIC Hits Too Close to Home

DECEMBER 12, 2009

CATEGORIES: OPERATING SYSTEM

Usually these type of problems happen at work, but this one hit too close to home. A few weeks ago the Internet connection on my PC dropped. NIC showed an error status. I power cycled my router and went on my merry way, until it happened again. I went to another PC with a wireless connection and I could ping the router. I could not ping the router from my PC, even though I plugged directly into it. I tried the switching the network cable into different ports on the router with no success. I dipped into my bag of tricks and pulled out my Testifer network cable tester: cable tested fine. I then switched the cable into another Ethernet port on my computer and still could get on. I then switched my NIC from a static IP to DHCP and then it magically started working. For good measure, I also loaded the latest Forceware from Nvidia for my chipset and NIC.

A week went by and things were fine, except Friday night...around the same time...the same thing happened! Disabling/re-enabling the NIC fixed the issue, but this couldn't stand. I started surfing the Internet stores for a new network card, then decided to give old Google a try.

I tried the keywords: "Windows 7 nvidia drops connection". Post after post referenced the same setting: Receive Side Scaling. Looking in my NIC properties, this was set to ENABLED, so I set it to DISABLED and since then: no disconnects! It's quite odd that I've been running Windows 7 for several months and this only recently came up.

– Soli Deo Gloria

Insights on Picking Passwords

DECEMBER 19, 2009

CATEGORIES: TECH TIPS

An interesting [study](#) on the length and complexity of passwords. Basically, pick one that's at least 14 characters long and not found in the dictionary and you should be OK against the bad guys.

– Soli Deo Gloria

Get Yourself Organized with Freeware

DECEMBER 31, 2009

CATEGORIES: MISC

Having a lot of vacation time on my hands, I decided it was time to organize all my DVDs and CDs for the new year. I was on the hunt for some freeware and found two really nice programs to help me.

The first one is called [Ant Movie Catalog](#). Working from just a CSV list of movies, I was able to import all my DVD movies into AMC within seconds. Now comes the cool part: I could update them in batch from IMDB! Just highlight a bunch of entries, hit F6, pick the movie database you want (*I like IMDB*) and then it will grab all of the information about that movie, including downloading a thumbnail picture for you! Most titles are unique enough so it was pretty easy to pick the correct movie.

The next project was to catalog all of my old software stored on CDs and DVDs (*yes, I still horde Windows 95, 98 and 2000 CDs!*). I tried many different programs, but the one that seemed to work the best, not have many limitations and updated on a regular basis was [Wincatalog Light 2009](#). When scanning disks, I kept getting an error that archiveinfo.dll didn't exist, so I installed the full version and copied archiveinfo.dll and the ARC directory to the light version directory and then the error went away.

The program doesn't do automatic numbering for media, so I put the CD # manually in the comment section and it shows the comment section as a column for each CD/DVD. The only snag is that it sorts them as text and not numbers, so 1, 10, 100, 101... are all grouped together. This really isn't a big deal, because you can do a search for what you want and then use the "jump to item in catalog" feature. For programs requiring serial numbers, I just put a comment on the first folder within the CD. When you expand the CD item in the normal view, you'll clearly see the serial number.

Since Microsoft Money is going away, I also found this program to replace it that is very slick called [Money Manager Ex](#). It's based on the SQLite engine, it's very small and efficient unlike MS Money and best of all: FREE! I like the canned reports "Where the Money Goes" and "Where the Money Comes From".

Finally, I ditched WinRAR which I got from a Slickdeals deal in favor of opensource [7-ZIP](#). Yes, it handles RAR files just as well.

Have a safe and Happy New Year!

Sola scriptura! Sola fide! Sola gratia! Solo Christo! **Soli Deo Gloria!**

2009 Bearware Top 10 Freeware Programs of The Year

JANUARY 5, 2010

CATEGORIES: REVIEW

Provided courtesy of <http://bearware.info...>

1. Anti Virus/Spyware: [Microsoft Security Essentials](#)
2. File Search: [Everything](#)
3. File Synchronizer/clone: [FreeFileSync](#)
4. Internet TV: [Hulu Desktop](#)
5. Password and Form Filler: [LastPass](#)
6. Program Launcher: [SlickRun](#)
7. Uninstaller: [RevoUninstaller](#)
8. Video Player/Recorder: [VLC](#)
9. Web Browser: [Google Chrome](#)
10. Video/Audio Capture: [TubeMaster++](#)

– Soli Deo Gloria

Giveaway – EASEUS Data Recovery Wizard 4.3.6

JANUARY 7, 2010

CATEGORIES: MISC

For a limited time: enjoy [EASEUS Data Recovery Wizard 4.3.6](#) for free!

– Soli Deo Gloria

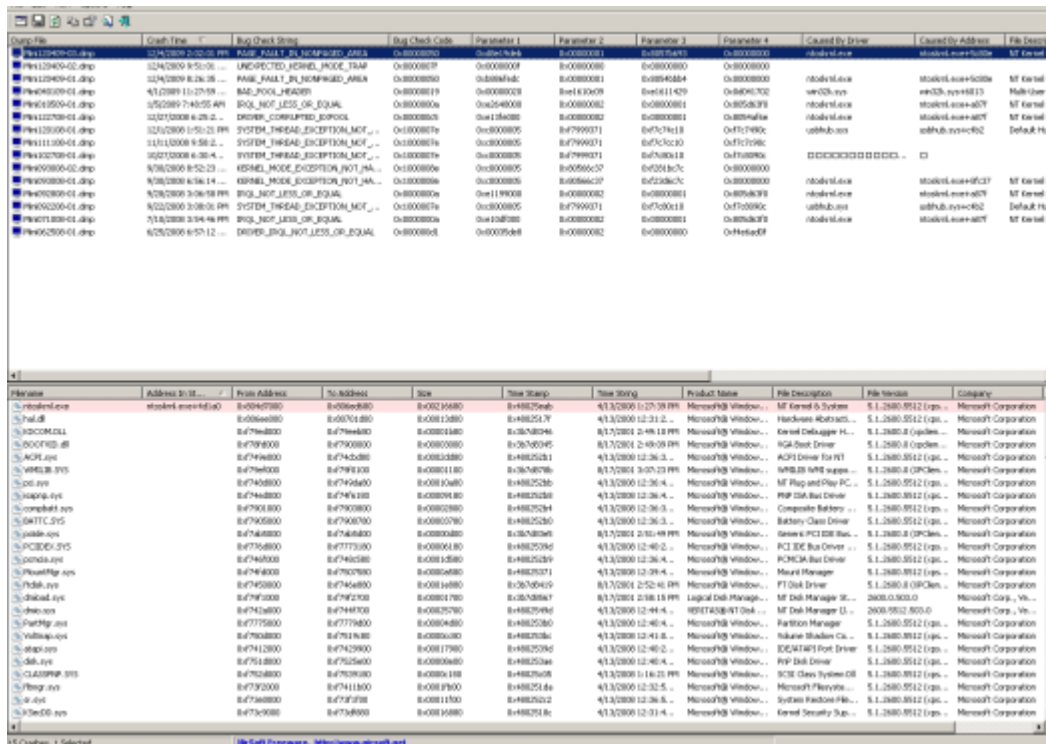
A Quick Way to View BSOD Minidumps

JANUARY 14, 2010

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I found this program called [BlueScreenView](#). It is quite handy as it can open up memory dumps without having WinDBG installed, can open them remotely through c\$ shares, is portable, easy to use and the best part: it's free!

Below you can see it in action. This was on a Dell D600 laptop who's motherboard was toasted. I couldn't even image the laptop without the whole thing locking up. You can see the error message and the very handy column "Caused by" that should give you some clues about where the problem is.



- Soli Deo Gloria

Giveaway – EASEUS Partition Master Professional 4.1.1 until 2/20/10

JANUARY 20, 2010

CATEGORIES: OPERATING SYSTEM, TECH TIPS

[Enjoy Free Partition Management Software Now!](#)

EASEUS Partition Master Professional is comprehensive hard disk partition management tool and system partition optimization software; it can let you enjoy all the powerful basic and advanced partition functions for Windows XP/Vista/Windows 7 32/64 bit users.

Free until 2/20/10

Spruce Up That Old Windows Explorer

FEBRUARY 22, 2010

CATEGORIES: OPERATING SYSTEM, REVIEW, TECH TIPS

From time to time, I go and search for a better file manager, but I always come back to the built-in Windows Explorer. Instead of completely replacing Windows Explorer, you can add some neat functionality to it. You can do this with [FileMenu Tools](#) which was recently reviewed by TechPP.com and is freeware! It has neat little features such as being able to securely delete a file (*or all files on a drive*) by overwriting it with zeros or changing the time stamp on a file. The duplicate file feature is really nice: if I just want another copy of the file, the old way was copying that file to another directory, then renaming it and then copying it back. Now I can just do a duplicate file and it just appends *_copy* to the end of the filename.

I also like the size of folders feature. You can right-click on any drive or folder and get sizes right from explorer. No more loading 3rd party tools like Treecize to do the job!

Simple, neat and clean.

– Soli Deo Gloria

Interesting Report on Malware Cleanup/Prevention Products

MARCH 1, 2010

CATEGORIES: TECH TIPS

Full report [here](#). Malwarebytes is rated #2. I've never used [a-squared anti-malware](#), but I will the next time I get a case to use it since it is highly rated as well.

More reviews here: <http://www.anti-malware-reviews.com>

– Soli Deo Gloria

Free Versions of O&O Software

MARCH 2, 2010

CATEGORIES: MISC

Here is a [link](#) on Slickdeals.net that describes how to get free versions of O&O Defrag 11 Professional, Unerase 2, Clevercache 6 Pro, Safe Erase 2 and DriveLED.

– Soli Deo Gloria

Fun with Virtual Machines

MARCH 25, 2010

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Virtualbox from Sun Microsystems is very cool. The snapshot feature is priceless for testing application deployments. One of the annoying things, however, is the eventual loss of domain membership. Eventually Windows changes the computer account password, you snapshot back the VM to a time where the password was different and it loses its domain membership. Of course, you can keep re-joining the VM back to the domain, but this gets old after a while. I went on Google and found http://blogs.msdn.com/virtual_pc_guy/archive/2006/03/28/561508.aspx, then leading to a posting made by “Jesse” who offers us this: <http://support.microsoft.com/kb/175468>. We can disable the computer account password expiration by setting the following:

Click Start, click Run, type Gpedit.msc, and then press ENTER.

Expand Local Computer Policy, expand Windows Settings, expand Security Settings, expand Local Policies, expand Security Settings, expand Local Policies, and then expand Security Options.

Configure the following settings:

```
Domain Member: Disable machine account password change - Enabled
Domain Member: Maximum machine account password age to 999 days
Domain Controller: Refuse machine account password changes - Enabled
```

Although the article only states this is for Windows XP and 2003, I checked my enterprise copy of Windows 7 and the same settings still exist, so I assume this would work for VMs running Windows Vista/7 and beyond. The other handy tip from “Jesse” is that you can do a domain unjoin/rejoin in one step (*one reboot*) by using the NETBIOS name of the domain instead of the DNS name. For example: yourdomain.com would be the DNS name and yourdomain would be the NETBIOS name. During the domain rejoin, just chop the .com part off.

The next goal was taking our standard image and bringing it into Virtualbox. I used Disk2VHD from Sysinternals and then tried booting the VM. I would just get a black screen and upon trying

to use safe mode, I saw it was locking up at mup.sys. This is jogged my memory: HAL issue. I always keep copy of the ACPI HAL files since we still have Dell D600 laptops that use the older HAL. I copied ntkrnlpa.exe, ntoskrnl.exe and hal.dll to C:windowssystem32 and my “hacked” hal.inf to C:windowsinf. VM booted right up! I later found out from this article that it was indeed a HAL issue, but their solution is a repair of the OS to change the HAL. Why do a repair when you can just change 4 files?

– Soli Deo Gloria

SIW Pro for free today at Giveaway of the Day

MARCH 26, 2010

CATEGORIES: TECH TIPS

For 24 hours only: <http://www.giveawayoftheday.com/siw/>

I went to look where it hides the license, but it appears to be embedded within the EXE itself. I copied the EXE to another box and it was still registered to Giveawayoftheday. There is an update check feature in the program, so you might be able to continually keep it update with the Giveawayoftheday license. I'll update this posting with whatever I find. Until then, enjoy!

Update: You can't update the Giveawayoftheday version. The license is programmed directly into the EXE itself.

– Soli Deo Gloria

Who Added Joe to Domain Admins?

APRIL 1, 2010

CATEGORIES: JOKE

Saw this ad on Microsoft Technet a few days ago, thought it was pretty funny and decided to post it on April fools:



Hey Joe, there's this command called dcpromo...

– Soli Deo Gloria

A Very Fast Search Utility for Windows

APRIL 28, 2010

CATEGORIES: OPERATING SYSTEM, REVIEW, TECH TIPS

I use [Agent Ransack](#) at home and at work for searching for files, but just recently I found [Ultrasearch](#) made by the guys that created Treesize. The file search works by searching the MFT of NTFS directly instead of drilling down into the file system itself or an index. The nice thing is that not only are the search results nearly instantaneous, you don't have any of the issues of hard drive thrashing or worrying about hidden files.

I placed the executable on a share on my Windows 7 PC and I was able to run it from an XP machine just fine remotely, so this can be used as a portable application. Best of all: it's freeware!

– Soli Deo Gloria

Lock Down Adobe Reader 9

MAY 15, 2010

CATEGORIES: TECH TIPS

Want to lock down Adobe Reader 9 in your environment? Prevent updates, get rid of the splash screen and the option to buy Adobe Acrobat with the following script. Just place the following commands in a .BAT file and then run it after you install or upgrade Adobe Reader on a user's computer (*stolen from appdeploy.com*). The REG ADD lines should be all on one line. They are broken over 2 lines below due to the length.

Update (5/5/11): This works for 10 as well, just change 9.0 to 10.0 and viola: lockdown goodness!

```
REG ADD "HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\9.0\FeatureLockdown" /v
bUpdater /d 0 /t REG_DWORD /f
REG ADD "HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\9.0\FeatureLockdown" /v
bShowEbookMenu /d 0 /t REG_DWORD /f
REG ADD "HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\9.0\FeatureLockdown" /v
bPurchaseAcro /d 0 /t REG_DWORD /f
REG ADD "HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\9.0\FeatureLockdown" /v
bCreatePDFOnline /d 0 /t REG_DWORD /f
REG ADD "HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\9.0\FeatureLockdown" /v
bBrowserIntegration /d 0 /t REG_DWORD /f
REG ADD "HKLM\SOFTWARE\Adobe\Acrobat Reader\9.0\AdobeViewer" /v EULA /d 1 /t
REG_DWORD /f
REG ADD "HKLM\SOFTWARE\Adobe\Acrobat Reader\9.0\AdobeViewer" /v Launched /d 1 /t
REG_DWORD /f
REG ADD "HKLM\SOFTWARE\Adobe\Acrobat Reader\9.0\Downtown" /f
REG ADD "HKLM\SOFTWARE\Adobe\Acrobat Reader\9.0\Downtown" /v bDontShowAtLaunch
/t REG_DWORD /d 1 /f
REG ADD "HKLM\SOFTWARE\Adobe\Acrobat Reader\9.0\Downtown" /v bGoOnline /t
REG_DWORD /d 0 /f
```

– Soli Deo Gloria

Paragon Virtualization Manager 9.5 for Free (until May 24th)

MAY 21, 2010

CATEGORIES: TECH TIPS

Free until May 24th: <http://dottech.org/freebies/16479>

These are the major features as per the developer:

- *Migrate a Windows-based computer to a virtual environment (P2V)*
- *Migrate from a virtual environment to physical (V2P)*
- *Virtualize system from its backup image (P2V)*
- *Migrate from one virtual environment to another (V2V)*
- *Recover the OS startup ability after system migration to a different hardware or unsuccessful virtualization by a 3rd party tool (P2P and P2V Adjust)*
- *Clone a partition or an entire hard disk*
- *Exchange data between your physical environment and the virtual one, or between a virtual disk and its snapshots*
- *Accomplish virtual drive partitioning (create, format, delete, move, resize etc.)*

Edit (5/27/10): After installing this program, it just seems simliar to Sysinternals' [Disk2VHD](#) program.

– Soli Deo Gloria

The GPO That Couldn't

JUNE 9, 2010

CATEGORIES: OPERATING SYSTEM, TECH TIPS

After many sweet years, we finally bid farewell to Internet Explorer 6. We planned to deploy Internet Explorer 7 via a Software Installation GPO. After making the IE 7 MSI with the IEAK, we assigned it as a GPO. As soon as the computer would reboot, the MSI would be assigned, install and restart the PC. This worked great, except some PCs just weren't getting the GPO. Running RSOP, I saw the message:

Software Installation did not complete policy processing because a system restart is required for the settings to be applied. Group Policy will attempt to apply the settings the next time the computer is restarted.

So I rebooted the PC over and over again, only again to find the same message. Copying down all the computer names, I started to look at each computer. They were all Dell GX270 computers. I sat down at one of these machines and started updating network drivers, setting the GPO "Always wait for the network at computer startup and logon" locally to Enabled, etc. After a few Google searching, I found a setting called Media Sensing that can cause a computer not to detect the network connection at boot: <http://support.microsoft.com/kb/326152>.

The explanation from the above article is as follows:

The problem occurs because link status fluctuates as the network adapter (also known as the network interface card, or NIC) driver initializes and as the network adapter hardware negotiates a link with the network infrastructure. The Group Policy application stack executes before the negotiation process is completed and can fail because of the absence of a valid link.

Upon running the REG file I made with this setting, the PC took the GPO! Within SCCM 2007, I created a collection with membership based on computers with the chassis value of GX270. I then pushed my REG file to this collection and shazam, all were fixed!

– Soli Deo Gloria

Sysinternals Tools Updated

JUNE 10, 2010

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Some interesting enhancements to some of Sysinternals tools:

Autoruns v10: This major update to Autoruns introduces the ability to scan offline Windows installations, adds.exe and .cmd extension handlers, defaults to hiding Windows entries to reduce noise in the common use case, and includes bug fixes.

Process Explorer v12.04: This Process Explorer release adds the ability to generate full and minidump process crash dump files and fixes a bug in the process permission dialog.

Sigcheck v1.7: This version of Sigcheck, a file version and signature verification command-line utility, now returns an exit code of 0 to indicate that all code it checked was signed and 1 to report that some were unsigned.

ProcDump v1.8: This version of ProcDump, a command-line process crash-dump generation tool, includes comments in the crash dump that reflect the reason that the dump was generated (memory threshold hit, CPU threshold hit, manual, etc.).

<http://technet.microsoft.com/en-us/sysinternals/default.aspx>

– Soli Deo Gloria

Early Windows 8 Details Leaked

JUNE 29, 2010

CATEGORIES: MISC

Francisco Martin, a Microsoft Enthusiast, posted several (*now offline, wonder why 😊*) confidential pieces of information to his blog on Monday revealing improvements that Microsoft is aiming for with Windows 8. Read more at Neowin.

– Soli Deo Gloria

Monitor Problem from Hell

JULY 3, 2010

CATEGORIES: MISC, TECH TIPS

You probably heard of “DLL Hell”, but I recently experienced “monitor hell”. We had a 30inch Dell WFP3007 attached to a Dell Precision T3400. We shipped the PC offsite and attached the monitor to another Dell T3400. A few weeks went by when the user who has this monitor noted that he could not set the resolution above 1280×800. I went over and tried setting the resolution to 1900×1200. Upon doing this, the monitor scaled down to 1/4 of the screen. In order to see the whole screen, I had to scroll the mouse around. I thought it was a video card problem. The PC had a NVS 290 video card within it and the working system had a Quadro FX 570. I did not have any Quadro’s laying around, so I tried an ATI FireGL V7200. Upon installing this card and booting, all I got was a screen with a bunch of bars across the screen, going in and out: the PC wouldn’t even POST.

I tried another FireGL video card with the same results. At this point, I was completely baffled, so I called Dell and actually had them connect into the PC in question. Try as he may, the tech support guy who was A+ and DCSE certified could not fix the problem either. This PC was only a few months old and had recently been imaged within the last 3 months.

I tried another DVI cable with the same results. I then (*for completeness sake*), tried a NVS 295 video card since it had DisplayPort inputs on it and again, I got the same results with the display scaling. At this point, I was pretty convinced it was the monitor itself, so I brought over a Dell T3500 and attached the monitor this PC. Again, I got the bars across the screen.

I called Dell again, this time requesting a RMA on the monitor. By this time I had gone through 5 video cards, 2 cables, and 2 computers. After firing off all this information at the tech support person, I expected a prompt replacement of the monitor. However, she came back after talking with the engineering lab and stated that I needed a DVI dual-link cable. I never knew there was a difference in DVI cables, much less single-link and dual-link DVI cables.

According to http://en.wikipedia.org/wiki/Digital_Visual_Interface, the dual-link has 6 extra pins and has a higher bandwidth (*resolution*) capability. We ordered this cable from Dell for around \$9. Upon getting the cable and trying it on a Dell 390, it worked! I happily wheeled the monitor over to the user’s workstation. And guess what? SAME PROBLEM!

At this point he had a Quadro FX1400 installed, after the many video card attempts I had tried. I ran back and took the Quadro FX 570 out of the Dell 390. Finally, the monitor worked!

I don't know if there is a moral to the story, other than to say that if you have a 30inch LCD screen, you better have the best video card and best DVI cable you can.

– Soli Deo Gloria

Technet Gets Cheaper

JULY 10, 2010

CATEGORIES: MISC, TECH TIPS

Microsoft recently rolled out a new tier of Technet called Technet Standard and what was Technet Plus is now Technet Professional.

Microsoft has also released a nifty spreadsheet showing the difference between Standard and Professional.

Standard seems to have most of what Professional has, sans the Enterprise versions for \$100 less.

– Soli Deo Gloria

Data Recovery Fun

AUGUST 2, 2010

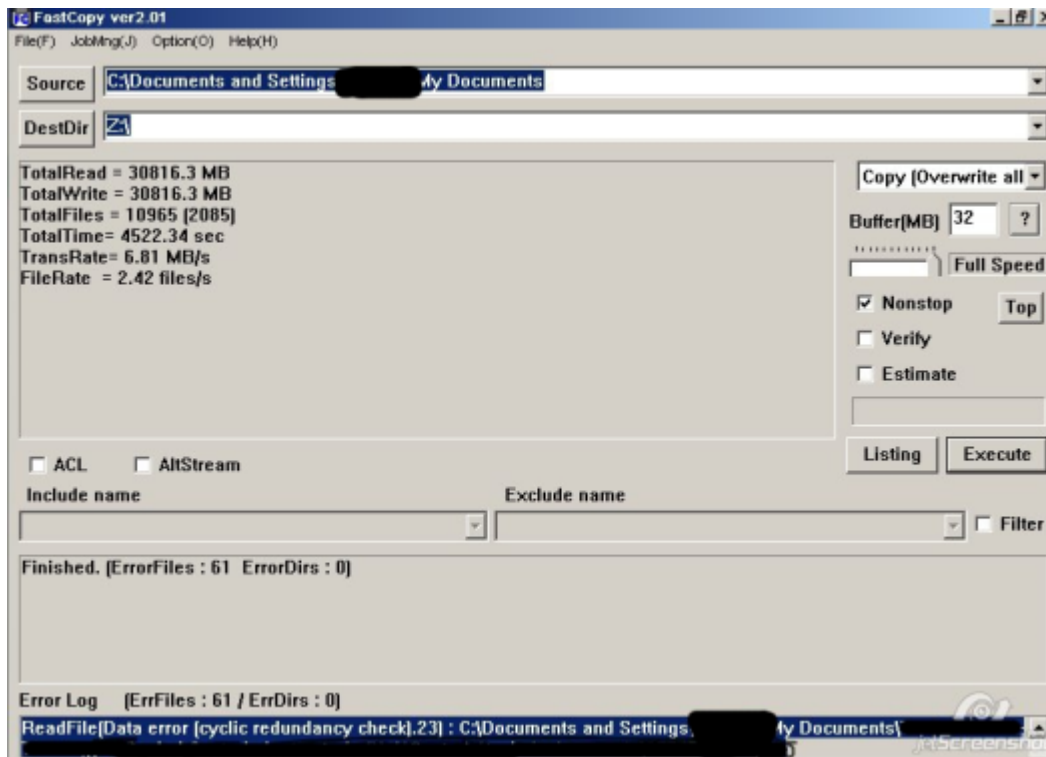
CATEGORIES: OPERATING SYSTEM, TECH TIPS

I recently had a D630 laptop hard drive go bad. Of course, there had to be 18GB of user data on it. Windows wouldn't boot in normal or safe mode. Upon booting the laptop with WinPE, I could see all of the data was still intact. I attempted to copy the data through Windows' XCOPY command (*/c option*) and my trusty 2.5 to USB adaptor. Unfortunately, the command would lock up on certain files for more than 20 minutes at a time where I had to put the USB adaptor out and then plug it back in. Not much forward progress being made, I decided to try Roadkil's [Unstoppable Copier](#). Unfortunately, it too had problems locking up the Windows operating system when hitting certain "bad" files. Also, it didn't seem to re-create the folder structure correctly, dumping all the files all into one big folder.

I then tried GetDataBack NTFS, but it wanted to search the whole drive. The data wasn't deleted nor was the drive formatted. I knew exactly where the data was: I just wanted to copy the blasted files! The data search was taking too long because again it was hitting the bad sectors.

I decided to try the Symantec Ghost route: image the drive from WinPE using Ghost32.exe. I used the command line switches *-fro* and *-crcignore* to skip over the bad sectors. I let it run overnight. I came in the next day and it had created a Ghost copy in about 6.5 hours. Using Ghost Explorer, I tried restoring the files, but it would only restore 232MB of the 18GB.

I don't easily give up on problems like this, so I tried something called [Fastcopy](#) within WinPE. This utility is designed specifically to copy files from one place to another and fast! This program had the ability to skip over the bad files with no lock ups at all. In addition to this, it also recorded the time of copy, the data rate and kept a log of the files that it couldn't copy. Now I could give the list to my user without having to write down all the folder and files that were missed.



- Soli Deo Gloria

Even More Fun with Virtual Machines

SEPTEMBER 1, 2010

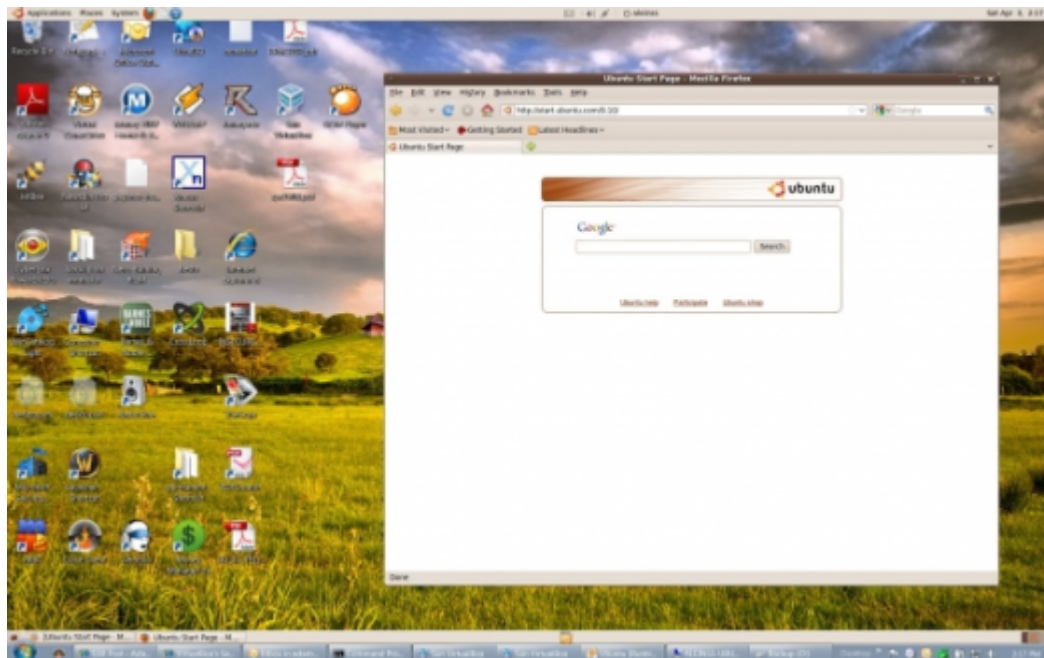
CATEGORIES: OPERATING SYSTEM, TECH TIPS

The Internet is getting pretty dangerous, especially for anyone running a Windows 2000/XP machine. Wouldn't it be nice to surf the web from your Windows box using a Linux browser? You can, using Virtualbox + Ubuntu + Seamless Mode.

You can see this in action: <http://www.makeuseof.com/tag/virtualboxs-seamless-mode-combine-operating-systems-desktop/>

The process is very simple: Install Virtualbox into your Windows host system, install Ubuntu within Virtualbox, install guest addons within Ubuntu. For added goodness, you might also want to add Samba to Ubuntu so you can share folders with Windows (*all downloads with the Ubuntu Firebox go back into Ubuntu*). An excellent video guide for doing so can be found here: <http://www.youtube.com/watch?v=89hjWOb8qmY>.

Once Ubuntu is running in Virtualbox, you can do a "Right Ctrl-L" and you'll get this in your Windows host system:



As you can see, Virtualbox places the Ubuntu taskbars above my Windows 7 taskbars. You get the comforts of you host operating system with the goodies from Ubuntu. I'm running this with

256MB of memory for the VM and it runs great. If you still have Windows 2000/XP, you can keep them and be more secure on the Internet.

– Soli Deo Gloria

ManagePC: A Neat Remote System Info Utility

SEPTEMBER 24, 2010

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I happened to be browsing the 4sysops.com website and came across a freeware program called ManagePC. This is a nice little utility that can give you a lot of information about a remote system.

Upon launching the program, you get a pull down menu where-in you can select your NT domain (you can also plug in a computer name or IP address if you want to get right to it). From here, you can drill right down in the AD OUs and to the computer objects themselves. The one thing that would be nice is if it could pull the computer description along with the computer name in the computer browser.

The first tab is the summary tab:

Property	Value
Computer	
Computer Name	[REDACTED]
Manufacturer	Dell Computer Corporation
Model	OptiPlex GX270
Form Factor	AT/AT COMPATIBLE
System Type	X86-based PC
Primary Owner	[REDACTED]
Total RAM	1 GB
Total Available RAM	489 MB
Logon Domain	[REDACTED].com
Domain Role	Member-Workstation
Timezone	(GMT-06:00) Central Time (US & Canada)
Logged on User	[REDACTED] (Locally)
Active Directory	
Distinguished Name	CN=[REDACTED]-U-Sales,OU=Computers,Sales,[REDACTED]
Canonical Name	[REDACTED].Computers/Sales/[REDACTED]
Description	[REDACTED]
Last Logon	9/13/2010 9:42 AM
Dial-In Enabled	Set by Remote Access policy
BIOS	
BIOS Type	Dell Computer Corporation
BIOS Version	A02
BIOS Date	7/15/2003 12:00:00 AM
Serial Number	[REDACTED]
OS	
OS Name	Microsoft Windows XP Professional
OS Version	5.1.2600
OS Serial Number	[REDACTED]
OS Service Pack	Service Pack 3
OS Installation Date	3/23/2010 10:37:20 AM
Computer Description	No description found
Last Booted on	9/21/2010 8:21:44 AM
OS Root Folder	C:\WINDOWS
IE Version	7.0.5730.1300
CPU	
CPU0	Intel(R) Pentium(R) 4 CPU 2.60GHz
Hyperthreading	False
# of cores	1
Display	
Display Adapter	ConfigMgr Remote Control Driver (1024 x 768 x 4294967296 colors)
Multimedia	
Audio Adapter	SoundMAX Integrated Digital Audio
Network	

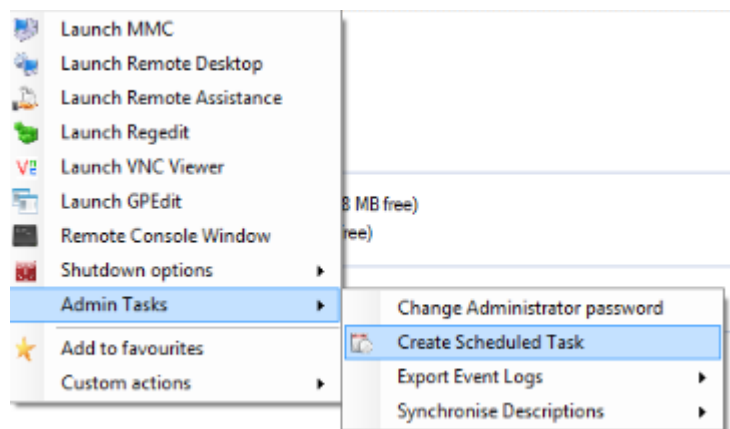
There's a few gems on this page that the built-in 'MSINFO32' that comes with Windows doesn't give: who's logged in, serial number of the computer, boot up time (*did the user REALLY reboot?*), last login time, and the user's assigned printers. There is a mapped drives section, but this appears to list my network drives and not those of the remote user. I've put in a feature request to the programmer to also report the user's default printer, but you can do this yourself

using a remote session with COMPMGMT.MSC....connect to remote registry of the remote computer, expand **Computername\HKEY_USERS\S-1-5-21-
<some_really_long_string_of_numbers>\Software\Microsoft\Windows
NT\CurrentVersion\Windows\Device**. What ever device is listed there is the user's default printer.

Clicking on the services tab gives us the remote services, their current state and the ability to stop and start services. Although this can be done with the COMPMGMT.MSC snap-in, you can manage this all from one tool. The processes tab gives you the processes running on the remote PC. This is similar to Running Tasks in MSINFO32, however, you can kill or Google each process just by right-clicking on them.

The Group Membership tab gives you all of the local groups on the remote PC. This is nice, quick way to see if the user is apart of the local administrator's group. The Startup Items tab gives you items from the Run key from HKCU and HKLM on the remote PC and the ability to delete or Google them. This can aid in malware detection.

There's also the standard fare of being able to launch a remote MMC or RDP session, restart or shutdown a PC, start a remote CMD session (*similar to right-click tools in SCCM*), change the administrator password or create a remote scheduled task. For some reason, the VNC function did not seem to work for me. It would attempt to connect and then time out. This could be due to the fact of having a VNC password on the PC.



In addition to all of these features, you can also export the report in HTML, RTF or Excel format.

– Soli Deo Gloria

The Dead of One Sysinfo Utility Gives Birth to Another

OCTOBER 1, 2010

CATEGORIES: TECH TIPS

I recommended the use of PCI32 to someone rebuilding their system today and found out that Craig Hart and his web site are gone! His web site use to be here:

<http://members.datafast.net.au/dft0802/downloads.htm>, but that appears to redirect to a bogus web page. The last archive I could find is from the end of 2007:

<http://web.archive.org/web/20071007132542/http://members.datafast.net.au/dft0802/download>

It appears from other archives that pcidevs.txt on Craig's web site (*the PCI database*) stopped being updated by Craig around the beginning of 2008. However, I have found that Ray Hinchliffe has taken over the maintenance of this database and it was last updated on 9/26/2010 and has 66,000 lines of information vs the 23,000 lines in Craig's list. This up-to-date PCIDEVS.TXT can be found at Ray's site at <http://rh-software.com/downloads/pcidevs.txt>.

But wait: there's more! Ray maintains a program called System Information Viewer or [SIV](#) that is a GUI program and it is very good. I remember seeing this program back in my college days and now it is very polished and uses Craig's database format. In addition to the PCI database, Ray also has monitor, USB and PCMCIA databases in plaintext as well, going well beyond the functions of PCI32. You can check out the screenshots of SIV at Ray's site. I tried it out on my system and was very impressed. I may just replace SIW with this tool! Unlike PCI/PCI32, Ray has a port of SIV that will work on x64 processors. You can also do updates from within the program to update the device databases.

I've copied the latest PCI32.ZIP I could find and put it here: <http://leinss.com/files/pci32.zip>. I've removed PCI32 from my Tech Files page and replaced it with SIV which is far better and more up-to-date. I've also removed the program [Unknown Devices](#) from my Tech Files page since it hasn't been updated since 2007.

– Soli Deo Gloria

Phillips 4 Piece USB Kit – \$6

OCTOBER 15, 2010

CATEGORIES: TECH TIPS

Today only at www.thingfling.com. This 4 piece kit is only \$6 (shipping included!).

Has:

- A Male/A Female Connectors
- A Male/4-Pin Mini B Male
- A Male/4-Pin Flat Mini B Male
- A Male/B Male Connectors
- A/5-Pin Mini B Connectors

Great to keep in the tool bag when you need that odd USB connection type.

– Soli Deo Gloria

The Flaky Fluke

NOVEMBER 1, 2010

CATEGORIES: TECH TIPS

Another day, another ticket. This one involved a computer dropping network connection. I pulled out my trusty Testum TP350 to test the network port and sure enough: one of the pins was showing shorted. Normally data jacks are labeled, but this wasn't one of them. I put the tester into tone mode and went into the data closet with my probe. Unfortunately, when you have a data cable plugged into a switch, you will get little to no tone. I ended up calling the network administrator, giving him the MAC address of the PC so he could tell me what port on the switch the computer was plugged into.

From this: I could disconnect the cable from the switch, see if it had tone and then trace it back to the patch panel. I did this and looked on the back of the patch panel. One of the plastic pegs that holds the wires in was broken and one of the little cables was just dangling free. I re-punched it to another port on the patch panel and all was well.

I like to try to solve problems on my own without involving other people unless I have to. I did some Google searching and came up with the [Superlooper Loopback](#) adaptor for \$5.99. Although you can build one yourself, I like the durable design of this one. When plugged into a network jack, it will produce a solid light on the switch. Normal lights are either blinking or no light at all, so this should stick out as a sore thumb (*although I guess it's possible that someone could be using the full 100MB of the port causing it to go solid, but that is unlikely*). This can also act as a poor mans cable tester: if you get a solid light, that means the line is probably good.

Although the Testum TP350 is pretty good, it is not as good for data testing as the Fluke Linkrunner is. The Linkrunner goes for around \$400 new while the TP350 goes for \$70-\$90 new. The Linkrunner can blink a light on the switch in an off-on matter in addition to tone generation, display port speed, link strength, obtain an IP address, ping the core router/DNS server, etc. I searched eBay before for used Linkrunners and never found any cheap ones, but I did snag one recently for \$140.

The first thing I noticed when I got the Fluke was how hard it was to put in the 2 AA batteries. Someone must have decided to make the world's smallest battery compartment. Getting batteries in and out requires the use of a flat blade screwdriver. I began testing wires. Although most functions of the tester worked, it seemed the cable testing part was not. I had a cross over

cable that I know was good, but the Fluke was saying it was bad. I tried it on the TP350 and it passed it with flying colors. I tried different batteries, wiggling the cables, etc., but nothing would make it stable. The weird thing was that the tester seemed to pass most of my straight through cables without any problems.

I took the tester to work the next day where we have a Linkrunner Pro. I tested the cross over on that and it passed the cable as good as well. I went into our box of cables and started testing cables with my Fluke. Some passed: others didn't. It seemed like certain ones with different connectors would fail. I took a flash light and started to compare the Ethernet ports on the Linkrunner and the TP350. On the Linkrunner, pins 1 and 8 were pushed down further than the rest of the metal rods in each. I took a paperclip and bent it, then gently bent each rod back up. Guess what? Fixed it!

Upon the magical wonders of Google, I discovered that if you push a telephone plug into an Ethernet jack, pins 1 and 8 get pushed down very hard because a telephone jack only uses 2 pins in the middle and it's only 6 pins wide. There is solid plastic where pins 1 and 8 would be in the Ethernet port. It is obvious that someone did this, and then tried to get rid of the meter. Upon questioning the seller, he indicated to me that he had sold it to someone before me, but that person returned it since it did not have Cisco Discovery Protocol (CDP).

My question is: if you were smart enough to know about CDP, would you jam a telephone plug into Linkrunner that doesn't test telecom equipment at all?

– Soli Deo Gloria

Run-As Control Panel on Windows XP and Windows 7

NOVEMBER 17, 2010

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Just as you think you know everything about Microsoft operating systems, someone recently asked a question on www.experts-exchange.com about using Runas with explorer.exe. There use to be a feature where-in you could do a run-as on Internet Explorer as administrator, then you would get a superuser explorer window from which you could leap frog to the Control Panel on Windows XP SP2. This allows you do to “admin like” things with a regular user logged into the system. Doing some searching on Google, I found this web link:

<http://www.krunk4ever.com/blog/2006/12/01/how-to-run-explorerexe-as-another-user/>

which comes up with **runas.exe /u:administrator “explorer.exe /separate”** as the trick. I tried this on both Windows XP and Windows 7 and it worked on both. Just type in “Control Panel” in the explorer address bar and boom, Control Panel opens as an administrator! One thing this allows you to do is to change network settings logged in as a regular user, which something I could never figure out from an elevated cmd.exe session.

This also seems to work from a network drive, so all you need to do is stick this line in a CMD file and save it to a network share the user has access to and viola!

– Soli Deo Gloria

Tiger Team

NOVEMBER 23, 2010

CATEGORIES: MISC

The movie Sneakers meets guys in real life (*made 2 years ago, but I was talking to some guys about social engineering and decided to post them*):

S01E01: The Car Dealership Takedown. The Tiger Team tests the security of Symbolic Motors, an exotic car dealership located in La Jolla, California. In this episode, the Tiger Team employs two distinct social engineering attacks, one rogue wireless access point attack, and a complex physical attack to gain unabated access to sensitive customer information and millions of dollars worth of cars on the show room floor.

S01E02: 24 Karat Caper. The Tiger Team tests the security of Jason of Beverly Hills, a custom jeweler located in Beverly Hills, California. In this episode, the Tiger Team employs a social engineering attack, an RFID cloning attack, a complex physical attack, and a safe-cracking attack to gain access to millions of dollars worth of precious gems and sensitive customer information.

– Soli Deo Gloria

Remote Desktop and Moving Icons

DECEMBER 2, 2010

CATEGORIES: OPERATING SYSTEM, TECH TIPS

One thing that always bugs me is RDPing into my work PC from a user's workstation and then when I get back to my desk, all my icons are screwed up. This is because my desktop resolution is 1280×1024 and the user's desktop resolution is 1024×768.

I have solved this with with a freeware application called [DesktopOK](#). With this application I can save the placement of my desktop icons, so when come back and all my icons are messed up, I just click Restore (*I of course saved the placement before trying RDP again*).

– Soli Deo Gloria

My First Taste of SSD Goodness

DECEMBER 17, 2010

CATEGORIES: MISC, REVIEW, TECH TIPS

I've been itching a while to get a SSD for my boot drive. I recently scored an Intel X25-M off of Ebay for cheap (*\$150 under retail*). I received the box in the mail and was amazed by size: it was hardly bigger than a box of matches. Upon opening the box: you get the drive, two packs of screws, a 2.5 to 3.5 adaptor and a mini cd. Unfortunately, it does not come with a SATA cable or power converters (*molex to SATA power, if needed*), so make sure to order those with your drive.

Installation was relatively painless. I planned to setup a dual boot with Windows 7 on a 140GB partition and Windows XP at the end of the drive at 10GB. I did not have my XP disc at hand, so I decided to install Windows 7 first. Booting and general tasks seemed quicker and more responsive. After running the Windows Experience Index, the drive was rated 7.5/7.9 for performance!

I ran a trial copy of HD Tune Pro and it comes out at 151MB/sec read with max read of 205MB/sec. I decided to compare it to the traditional platter drive (*Seagate ST3250410AS, 250GB*). The read was 73MB/sec with a max read of 87MB/sec. My other SATA drive (*Seagate ST3500630AS, 500GB*) fared worse at 63MB/sec with a max read of 66MB/sec. Unfortunately, HD Tune Pro wanted me to wipe all the data off my disks to test them for write performance which I didn't feel like doing.

I loaded XP, which wiped out the boot loader of Windows 7. I re-booted the PC with the Windows 7 disc, went into WinRE and ran Startup Repair. This put back the Windows 7 boot loader, but it did not add the XP NTLDR to the BCD loader?! I've done this many times with past Microsoft operating systems...from Windows 98 to 2000 and 2000 to XP. I went hunting for a third party utility to do my booting and found [EasyBCD](#). Actually, EasyBCD just interacts with the Windows 7 boot loader to make it easier to use. I loaded the program, said "Add Entry", I'm using "Windows XP" and that was it. It found my XP installation and added it to the BCD loader.

The next task was loading the Intel SSD Toolbox so I could maintain and optimize my new SSD. Unfortunately, after loading the program, when I went to click on the C: drive, it would just refresh the whole listing of disks. I thought that this perhaps was a Windows 7 x64 issue, so I booted into my XP installation and installed the toolbox there as well. This time the drive turned

from black to blue, but when clicking on the drive, it told me the optimizing tools were disabled for the drive.

Off to Google I went, typing in “*Asus Striker II Extreme + SSD + TRIM*“. After reading a bunch of postings, the conclusions are these: nForce chipsets don’t support AHCI, only ATA and the native nForce drivers don’t support TRIM! It seems only native Intel drivers or the built-in Microsoft ones can take advantage of TRIM. Windows 7 might be setup for TRIM, but if the storage drivers don’t understand the command, it’s pointless. I booted back into Windows XP and per the instructions I found, I changed the driver “NVIDIA nForce Serial ATA Controller” to “Standard Dual Channel PCI IDE Controller”. I rebooted and joy: the toolbox worked!

I booted back into Windows 7 and tried this, but it already appeared the drivers were already set to “Standard Dual Channel PCI IDE Controller”. I ran Procmon from Sysinternals and under the result tab I was getting “INVALID DEVICE REQUEST” messages. I went back to the Device Manager, knowing that the drivers must be hiding somewhere and sure enough, they were buried under the category “Storage Controller” instead of “IDE ATA/ATAPI Controllers”. I went back to the toolbox after changing the drivers and...SUCCESS! I re-ran Procmon and now instead of “INVALID DEVICE REQUEST”, I was getting “SUCCESS” back.

My days of getting a motherboard with a non-Intel chipset are over with. Sorry Asus: there’s no excuse on this one. Hello AHCI, goodbye ATA!

– Soli Deo Gloria

Backup your IMAP/webmail with Mailstore Home

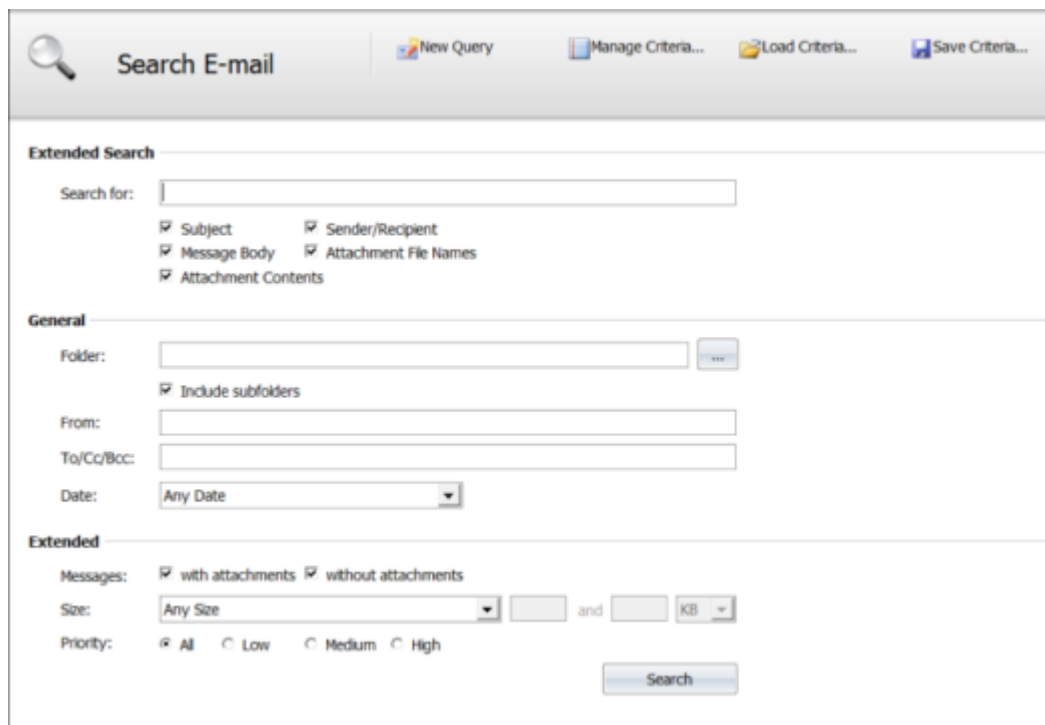
JANUARY 3, 2011

CATEGORIES: REVIEW

Many of us have multiple e-mail accounts at multiple providers. While it's great to have "everything in the cloud", you should always have your own backups at home. I recently found a slick product for doing this called [Mailstore Home Edition](#). Mailstore works with Outlook, Windows Mail, Thunderbird, Seamonkey, Google Mail (GMail), and generic IMAP/POP3 accounts. Mailstore sets up a database for each account, but treats the offline backup as one datastore. In my case, I have my main leinss.com e-mail accounts and a throwaway account at hotmail.com.

I have both leinss.com and hotmail.com (via the *Hotmail connector*) accounts setup in Outlook 2010. I just tell Mailstore to back all the accounts I have setup in Outlook. Once the backup is done, I can now take this e-mail and restore it to a new provider. I can also search across all e-mail accounts at lightning speed: it's on my hard drive!

Take a look at the powerful search options:



The screenshot shows the Mailstore Home search interface. At the top, there is a search bar with a magnifying glass icon and the text "Search E-mail". To the right of the search bar are several buttons: "New Query", "Manage Criteria...", "Load Criteria...", and "Save Criteria...". Below the search bar, there are three sections: "Extended Search", "General", and "Extended".

Extended Search

Search for:

Subject Sender/Recipient
 Message Body Attachment File Names
 Attachment Contents

General

Folder:

Include subfolders

From:

To/Cc/Bcc:

Date:

Extended

Messages: with attachments without attachments

Size: and

Priority: All Low Medium High

Best of all: it's freeware for home use!

– Soli Deo Gloria

Bypassing the screen saver policy defined by GPOs

FEBRUARY 1, 2011

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Microsoft Group Policy is a great thing, until it gets in your way. One of these policies is screen saver policy that locks out the workstation after X minutes of inactivity when someone is logged in. Example: you want to build a new PC for a user, so you have them log into the new PC back in IS. You walk away for 10 minutes and bang, the screen is locked asking for their password.

Now the policy is there to prevent someone walking up to a workstation and using someone else's account. Unfortunately, the life of the IT professional involves having to log in as the user to setup printers, e-mail, favorites, data, etc. USMT will only go so far: you can't setup rules for everything.

There are two ways of handling this situation (*actually, there are more, but I will focus on the PC side of things since that's where you are guarantee to have full control of the environment*):

Don't Sleep 2.0. This is a freeware program will prevent the screen saver from kicking in. You can log in as the user and run the program. As long as the program is running, the computer will not lock. This is the simplest, easiest way of doing the task without installing any program or modifying the computer in any way.

The second way is to temporarily blocking the GPO from modifying the Desktop key in HKCU (*the user's registry*).

Drill to HKEY_CURRENT_USER\Policies\Microsoft\Windows\Control Panel\Desktop

Right-click on the Desktop key and click on Permissions. Click on the SYSTEM account. Under the Deny tab, click the boxes Full Control and Read. Click Apply, then OK. In the right pane, change ScreenSaveActive to 0, ScreenSaverIsSecure to 0 and ScreenSaveTimeOut to 99999999. To test this, open a command prompt and type "gpupdate /force". If you did this correctly, the values in the right pane should NOT change. If you go back

and uncheck the Deny entries and re-run gpupdate, the values should change back to correct values.

Now you can build the computer, have the user log in and keep them logged in to do your work. You obviously want to do this in a secure area.

Don't forget to uncheck the Deny entries when you are done. Personally, I would just use Don't Sleep 2.0 since it is the least invasive method.

– Soli Deo Gloria

Yet Another Screenshot Program!

MARCH 1, 2011

CATEGORIES: REVIEW, TECH TIPS

For the past few years I've always looked for that ultimate screenshot utility. When creating technical documentation, a good utility can be a life saver. I first found [MWSnap](#) which allow you to snapshot any portion of the screen freehand. Unfortunately, there are no image editing tools that come with [MWSnap](#), so I was forced to bring the result into a program such as 20/20 to add text, highlights and arrows. Recently, I found out about [JetScreenshot](#) which includes the ability to draw arrows right on your capture within the program. Unfortunately, this program has quirks of its own, namely its default action is to save results to some Internet site (eww) and it puts a watermark on every result.

Finally to the rescue is a program called [PicPick](#). PicPick is like JetScreenshot, but there is no watermark on the resulting images. It also has a very cool "scrolling window" feature. This feature is invaluable if you say to take a screenshot of a very long page and want to do it as one picture. The only "bad" part of PicPick is that if you use it at work, you are supposed to buy a licensed or "commercial" version. At the time of this writing, that was \$20.

Another cool one I found was called [Greenshot](#): a completely free and opensource screenshot program. This one allows you to create complete or partial screenshots quickly, easily annotate, highlight or obfuscate parts of the screenshot and send the screenshot to a file, the clipboard, a printer or as e-mail attachment.

Collecting screen capturing tools is becoming my favorite hobby! Yet another one: [Screenshot Captor](#). This one is free as well and it has some nice highlighting features along with the blur tools. I like Greenshot's arrows better, so I just combine the two as needed.

– Soli Deo Gloria

Chain of Fools

MARCH 3, 2011

CATEGORIES: MISC, OPERATING SYSTEM

Some guy upgrades Windows 1.0 to Windows 7, with all versions in-between (except *Windows Me*), just to see what settings were kept. Take a look: <http://www.youtube.com/watch?v=vPnehDhGa14>

He also did Internet Explorer 1.0 to 9.0: <http://www.youtube.com/watch?v=k5QqYVurlmY>

– Soli Deo Gloria

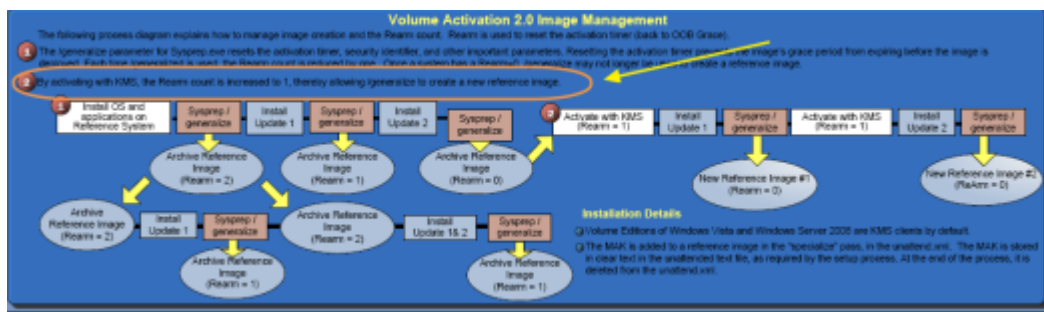
Unlimited Rearms with KMS

MARCH 11, 2011

CATEGORIES: OPERATING SYSTEM

I've been playing with MDT 2010 and Windows 7 recently and noticed something interesting. If you have a KMS in your environment, activating your copy of Windows with KMS adds 1 to your rearm count! You can see this on the [VA chart](#) on the bottom right. That means you don't have to worry about keeping a master copy that doesn't get rearmed if you are using KMS.

The 3 rearm limit still remains if you just use MAKs.



– Soli Deo Gloria

Dealing with Frankenstein Office Installs

APRIL 1, 2011

CATEGORIES: TECH TIPS

Recently, I was working on upgrading our PCs from Office 2003 to Office 2007 through SCCM 2007. This sounds easy enough, except for those “Frankenstein” builds we had. Some of our users were using Excel 2007 with the rest of the Office 2003 suite, because Excel 2003 only handle up to 64,000 rows. Unfortunately, loading two versions of Office leads to headaches, such as breaking Sharepoint integration. It seems that if you install Office 2007, it will register its version of owssup.dll. Upon doing so, when you attempt to open Word/Excel/Powerpoint documents from a Sharepoint site, Internet Explorer crashes with an unknown exception. This is fixed by running this [hotfix](#). Unfortunately, loading hotfixes or service packs for either suite can re-register the incorrect version again and you have to start the process all over again.

The problem with trying to push out Office 2007 with a custom MSP to PCs with Frankenstein Office builds is that it would pop up a box asking what components of Office 2007 I wanted to add or remove. Once any component of Office 2007 gets on a PC, the setup program ignores that Office 2003 is installed. The solution is to remove Office 2007, if it is installed, but how?

After searching the Internet and getting some help from www.experts-exchange.com, I came up with this script:

```
Const HKCR = &H80000000  
Const HLCU = &H80000001  
Const HKLM = &H80000002  
Const HKU = &H80000003  
Const HKCC = &H80000005  
strComputer = “.”
```

```
Set objShell = WScript.CreateObject(“WScript.Shell”)  
Set filesys = CreateObject(“Scripting.FileSystemObject”)
```

```
Sub RegKeyExists(strHive, strKeyPath, strValueName)  
Set objRegistry = GetObject(“winmgmts:\” & strComputer & “rootdefault:StdRegProv”)  
objRegistry.GetStringValue strHive, strKeyPath, strValueName, strValue  
If IsNull(strValue) Then
```

```
Wscript.Echo "Office 2007 is not installed"
```

```
Else
```

```
objShell.run("msiexec /x{90120000-0011-0000-0000-0000000FF1CE} /quiet"),1,true
```

```
Wscript.Sleep 900000
```

```
End If
```

```
End Sub
```

```
If filesystems.FileExists("c:\Program Files\Microsoft
```

```
Office\OFFICE11\STARTUP\PDFMaker.dot") Then
```

```
filesystems.MoveFile "c:\Program Files\Microsoft Office\OFFICE11\STARTUPPDFMaker.dot",  
"c:\Program Files\Microsoft Office\OFFICE11\STARTUP\PDFMaker.old"
```

```
End If
```

```
RegKeyExists
```

```
HKLM,"SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall{90120000-0011-  
0000-0000-0000000FF1CE}","DisplayName"
```

I test for the existence of a specific registry key that will only exist if Office 2007 (*any component*) is installed. If it exists, I fire off msiexec to remove Office 2007. You might be asking why I have a Wscript.Sleep 900000 statement right after this command. It seems that msiexec fires off setup.exe and just quits. Unfortunately, SCCM 2007 sees this as the VBScript has completed running and then attempts to fire another instance of setup to install Office 2007, which of course fails. To prevent this, I put in a hard waiting period of 15 minutes (900000 ms). No matter what you pass to msiexec (*i.e. /norestart*), it will restart the PC. This catches SCCM 2007 off guard (*since it is waiting for the script to exit gracefully*) and on restart, it attempts to re-run the VBScript. This time it just passes through, since Office 2007 is already removed.

Why rename pdfmaker.dot? Well, that is because some computers had Acrobat 6 installed and pdfmaker.dot causes Excel 2007 to take 45 seconds or more to open. To prevent this addin getting loaded by Excel 2007, we just rename it.

There is 1 more issue I ran into and that was with laptops. As this package was firing during 12AM to 5AM, I had not anticipated that laptops would be turned on during this time. I added this so it would "bomb out" on them so we could do them manually later on (*stolen from my administrator removal script*):

```
Set objWMIService = GetObject("winmgmts://" & strComputer & "/root/cimv2")  
Set collItems = objWMIService.ExecQuery("Select * from Win32_Battery",,48)
```

```
IsLaptop = False
```

```
For Each objItem in collItems
```

```
IsLaptop = True
```

```
Next
```

```
If IsLaptop Then
```

```
wscript.stdout.write "Laptop, not running package"
```

```
wscript.quit(666)
```

```
Else
```

```
wscript.stdout.write "Not a laptop, continue running package"
```

```
End If
```

This will show up in the advertisement status with error code "666" which will make it stand out for sure!

– Soli Deo Gloria

Getting into a Password Protected BIOS

APRIL 19, 2011

CATEGORIES: TECH TIPS

Saw this site from Raymond.CC on getting into a password protected BIOS on a laptop where you don't know the password: <http://dogber1.blogspot.com/2009/05/table-of-reverse-engineered-bios.html>

Worth a look if you have someone that got disgruntled and decided to "brick" the laptop.

– Soli Deo Gloria

Mark Russinovich on Podnutz Podcast – 5/2/11 – 8PM EST

APRIL 27, 2011

CATEGORIES: MISC

Mark Russinovich will be on the Podnutz Podcast show on May 2nd, at 8PM EST. He will likely take some questions towards the end of the podcast. Russinovich is an amazing guy: creator of Winternals/Sysinternals and pseudo son of Dave Cutler, he is the world's top expert on the internal workings of Windows NT technology.

You should be able to listen in on the stream live at podnutz.com (*main page*), so put it on your calendar!

– Soli Deo Gloria

Changing Icons with VBScript on Windows XP

MAY 5, 2011

CATEGORIES: TECH TIPS

Yet another pesky problem caused by going from Office 2003 to Office 2007. We had some Access databases lying around with shortcuts with command lines like "C:Program FilesMicrosoft OfficeOFFICE11msaccess.exe Z: BillyBobDatabase.mdb". Obviously, these will break after the upgrade, but I noticed during the install the Office 2007 installer was actually deleting the icons completely! Direct links to MDB files were not affected, just those that specifically contained C:Program FilesMicrosoft OfficeOFFICE11msaccess.exe in the command line.

The problem lies in the fact that the icon could be placed on the user's desktop or in all users' desktop. Some PCs are multi-user, so you could have the icon on several profile desktops. What to do?

I found this VBScript that was originally designed to do a recursive file delete. I changed it to do a recursive file replace instead:

START_FOLDER = "C:documents and settings"

ECRDATABASE = "ECR Database.lnk"

Set oFSO = CreateObject("Scripting.FileSystemObject")

ProcessSubFolders oFSO.GetFolder(START_FOLDER)

Sub ProcessSubFolders(oFolder)

Set cFiles = oFolder.Files

For Each oFile In cFiles

If Right(oFile.Name, Len(ECRDATABASE)) = ECRDATABASE Then

TruncatedFilePath = Left(oFile, Len(oFile) - Len(ECRDATABASE))

oFSO.CopyFile "ECR Database.lnk", TruncatedFilePath

If oFSO.FolderExists("C:Program Files (x86)Microsoft OfficeOFFICE11") Then

oFSO.CopyFile "ECR Database x86.lnk", TruncatedFilePath

oFSO.DeleteFile TruncatedFilePath & ECRDATABASE

End If

```
End If  
Next  
For Each oSubFolder In oFolder.SubFolders  
ProcessSubFolders oSubFolder  
Next  
End Sub
```

This is a very “expensive” script that will hit about every file in all user’s profiles. That means that if you have 20,000+ files in Internet caches, multiple user profiles and a slow PC, it could take 30+ minutes for the script to finish. Since I was running this script off hours, I didn’t care about I/O or CPU time.

The last part of the script is designed for 64-bit machines. If C:Program Files (x86) exists, we are on a x64 machine and therefore we copy the x64 version of the icon.

– Soli Deo Gloria

Free EASEUS Partition Master Professional 8.01

MAY 18, 2011

CATEGORIES: MISC, TECH TIPS

For a limited time, go grab it! <http://dottech.org/freebies/22187>

P.S. No, it doesn't come with the WinPE 3 bootdisk 😞

– Soli Deo Gloria

Remote Unlock

JUNE 1, 2011

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Remote Unlock is a utility to remotely unlock a Windows computer's console, given you have administrator access to the computer. This allows administrators to gain desktop access to the computer without forcing the user to log out. Appears to only work on Windows 2003, XP, and 2000. Download is here: <https://launchpad.net/remotunlock>

– Soli Deo Gloria

Repairing the Damage after a Malware Attack

JUNE 8, 2011

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I've discovered two tools to help repair your system after malware has damaged it.

Under the Preferences>Repair tab of SuperAntiSpyware Portable, you will find the following fixes (*you can select just the ones you need or all of them*):

- Start Menu Run**
- System File Checker**
- System Tray**
- Task Manager**
- Windows Control Panel**
- Windows Explorer Folder Options**
- Home Page Reset**
- Internet Zone Security Reset**
- Local Page Reset**
- Remove Desktop Screen Saver**
- Remove Explorer Policy Restrictions**
- Remove Internet Explorer Policy Restrictions**
- Remove WinOldApp Policy Restrictions**
- Remove/Reset Windows Desktop Background/Wallpaper**
- Repair broken Network Connection (WinSock LSP Chain)**
- Repair broken SafeBoot key**
- Repair broken Windows System Restore Service**
- Reset Desktop Components**
- Reset Desktop Policies**
- Reset URL Prefixes**
- Reset Web Settings**
- Reset Windows Clock Time Display (12 Hour Format)**
- Reset Windows Clock Time Display (24 Hour Format)**
- Reset Winlogon Shell**
- Reset ZoneMap Settings**
- User Agent Post Platform Reset**
- User Agent Reset**

Re-enable is a simple portable tool that allows users to easily re-enable Windows' RegEdit, Command Prompt, Task Manager, Run, Folder Options, and System Restore:

<http://dottech.org/freeware-reviews/11980/>

- Soli Deo Gloria

Case of the Unexplained 2011

JUNE 10, 2011

CATEGORIES: MISC, TECH TIPS

Check out Mark Russinovich's new Case of the Unexplained webcast

@ <http://technet.microsoft.com/en-us/sysinternals/bb963887>

– Soli Deo Gloria

Spyware Jumps the Fence

JULY 1, 2011

CATEGORIES: MISC, TECH TIPS

So there I was on a Friday night, downloading a podcast off of a web site. All of a sudden, Internet Explorer closed and a spyware box popped up. No matter what, I could not run Internet Explorer again. All that came up was the spyware box: even System Restore was blocked! I proceeded to restart my PC and login. Again, the spyware came back. I booted to WinRE and ran System Restore that way and all was well.

This story is told over and over again, except that I work in IT as systems support. I've been spyware free for the past 7 years on my personal computer. I'm running Windows 7 x64 with IE 9 with UAC turned on: not exactly an unsecure PC. What went wrong? Well, I was up to date all on Windows updates, but was a month or two behind on Java and Flash updates. The scary part is that this software announced it was living on my PC. What if it was a keylogger? I would have never known.

I decided to make myself more secure. I first tried running Google Chrome on Ubuntu 11.04 in a Virtualbox session. After messing with Samba so I could save files to my Windows box, I determined this wasn't going to work. Not only was the response "jerky", the Debian version of Google Chrome wouldn't import bookmarks from Internet Explorer. I next tried SandboxIE: a sandboxing solution for IE. I've used this program for certain high risk PCs and it works great, however all the files I downloaded would go into C:sandbox. This would require me trying to find them within the sandbox folder, then move them to their final destination: a pain.

I decided to try Google Chrome straight up on my Windows 7 PC. It's unbeatable at PWN2OWN conferences and constantly updated. Inside of being reactive, Chrome checks to see if there is a new version of itself every time you start it. This is in contrast to Internet Explorer which relies on the mercy of whenever Windows Update is ran. In addition to this, I switched over to Norton DNS, which blocks known malware sites. I found this tidbit from http://www.theregister.co.uk/2010/08/18/sysadmin_malware_athome/. Unfortunately, the first popular DNS offering I tried called OpenDNS only offers malware protection at the Enterprise level which is \$2000/year. To top it all over, I loaded [Securnia PSI](#). This scans your system for any outdated software, such as Java and Flash and offers to update it for you in the background (*it appears to get around UAC issues by installing two services that run as local system*). This allows a one stop shop for updating all the outdated software on your PC.

Finally, get Adblock from the Chrome web store. This is a free Chrome add-on created by Michael Gundlach that blocks ads on web sites.

- Soli Deo Gloria

Carry most of your CDs and DVDs in your Pocket

JULY 4, 2011

CATEGORIES: MISC, REVIEW, TECH TIPS

I love toys, so I bought myself an iodd 2511 from Korea. What does it do? Well, you can read about the model 2501 from <http://grandstreamdreams.blogspot.com/2010/07/iodd-multi-boot-madness.html>. Basically, it's a 2.5 SATA hard drive enclosure that acts like a CD/DVD ROM emulator. You take ISO images of your CD/DVDs and stick them into the _ISO folder on the hard drive (*I thought it was unlimited, but then I got an error "Too many files!" on the LCD screen. I think the limit is around 30 ISOs in _ISO, so when you reach that limit, you will likely need to move ISOs in and out to keep under the limit*). When you do a select boot at your BIOS (or UEFI, pronounced U-FEE) screen, it should show up an iodd CD emulator device. You use a toggle wheel on the left side to pick which ISO you want and viola, you're booting from the bootable CD/DVD! Note that model 2511 does support NTFS as the file system: you don't have to use FAT32 and there is a firmware update for the 2501 adding NTFS support.

The device also acts as a CD/DVD emulator in Windows without the use of any software, so you can go right to the user's PC and load any ISO as a drive letter without installing any software. The device also has a read/write switch in case you want to protect it from that virus infected neighbor PC.

I got my device from eBay from a seller named elec*star within a week for \$78.99.

– Soli Deo Gloria

Fun with Windows 7, MDT 2010 and HyperV

AUGUST 1, 2011

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Recently, we piloted Windows 7 to a few lucky users. I had to scrub my knowledge of deploying Windows XP, because Windows 7 is so different. My old approach of just taking a straight up ImageX of the system won't work anymore. This is because Windows 7 creates a small partition called "System Reserved" that it uses for WinRE and BitLocker. Although Windows 7 can work without this partition, it's a nice thing to have. The other snafu is the way enumerates drivers. You need to either add all the drivers to your image by running sysprep to put the system into audit mode or call DISM at deployment time to inject only the drivers you need just in time. Windows 7, unlike Windows XP, will not look at any drivers you might have sitting in a folder during the minisetup after sysprep.

Bottom line is you are going to want to use MDT 2010 to make your life deploying Windows 7 easier, because it has lots of code to call DISM on its own. The guide I used to build my own MDT 2010 environment is from Johan Arwidmark from here:

<http://www.truesec.com/deploymentcd>. Just register to download the CD and enjoy MDT 2010 bliss (*don't worry, it's free and Johan is wonderful in his demonstrations*)! Another good one is this one from [Aidan Finn](#).

With Windows 7, it was also time to move to using VMs to create images. Why? Well, it's faster for one. I can take a snapshot and "snap back" if I make a mistake and I get around the 3 sysprep limit for Windows 7. Before you run sysprep, just take a snapshot and viola, you can sysprep forever since the image remains in a virgin state! (*Does not really apply anymore if you have KMS up and running, but it does if you are just using MAKs*). HyperV comes with Windows Server 2008, so I just used an old Dell Precision 390 box and threw in some extra memory. My XP image came through just fine in HyperV, but when trying to bring in my Windows 7 image from a physical box using Disk2VHD, I got the dreaded STOP 7B error message. I got around this problem by using a tip from someone on the Microsoft Technet forums by using Citrix's [XenConvert](#), a free V2V and P2V utility.

HyperV uses something called Integration Services (*akin to the VMWare Tools*). This is built into Windows 7/2008, but not XP. I recommend removing these tools before sysprepping on XP and capturing the image. While it seemed to work fine on XP x86 without removing the

tools before sysprep, the x64 version of XP threw a fit and I had use VGA mode to remove and reinstall the tools before the VM would boot properly.

– Soli Deo Gloria

Web Site Downtime

AUGUST 8, 2011

CATEGORIES: MISC

So at 8:35AM CST this morning, the DNS server in the Texas datacenter that hosts all records for leinss.com went down. This triggered a cascade effect of telling every other DNS server that leinss.com didn't exist and viola, my whole web site and e-mail was shutoff from the Internet.

In addition, I found out that my DNS Registrar Tuffnames was sold or transferred to Domains Priced Right without my knowledge. So even though I was entering the correct customer number and password, it was saying it didn't exist (eek!). Luckily, I found the right web site and was able to login to make sure my web site was paid and up-to-date.

– Soli Deo Gloria

Wondershare Liveboot 2012 (Normally \$59.95) for Free

AUGUST 8, 2011

CATEGORIES: REVIEW, TECH TIPS

Wondershare Liveboot 2012 normally sells for \$59.95. However, between now and August 12, you can download it for free! Instructions for doing so are here:

<http://www.techsupportalert.com/content/get-60-bootable-troubleshooting-tool-free.htm>

I downloaded the program and installed it. It contains a flat ISO @

C:\Program Files\Wondershare LiveBoot 2012\Wondershare LiveBoot.iso.

It is Windows 7 based and seems pretty decent. I found that you can reset local account passwords, find the installed Windows installation key, clone or wipe the hard drive and even includes the ability to restore a good copy of the system registry by letting you point to one in one of the system restore point folders. The Microsoft Safety Scanner does work in this boot CD (*unlike WinPE 3.0*), so it might be handy to download it just for that.

You will need at least 1GB of memory to use this boot disc. Although it seems to boot with 512MB, you won't be able to run any applications without getting weird errors.

Update (10/13/12): Appears you can still download this! See <http://slickdeals.net/f/3181943-FREE-Wondershare-LiveBoot-2012>

– Soli Deo Gloria

iPrism & Windows XP & Non-domain Members

AUGUST 18, 2011

CATEGORIES: MISC, TECH TIPS

This use to work on computers running Windows XP/2003 not connected to a domain, but alas it appears no more. If you try to access the Internet from a computer running Windows XP/2003, not joined to a domain and you are running iPrism, you will get presented with a lovely web page with a login and password box. Unfortunately, no matter what credentials your enter, it will not work. Surprisingly, this does work on Windows 7 (*here you get the lovely "Microsoft" login and password dialog box and not the dreaded iPrism login page*).

The solution? Head over to the Control Panel and go into the icon Users and Accounts. Input the user domain credentials for your iPrism host, such as:

iprism.yourcompany.com

login: yourdomainloginname

password: <your password>

Of course, if your password changes, you have to go back and change it here. This was a really annoying problem when building PCs and servers not joined to the domain.

Thanks to Aaron Bachler for the cross discipline support 😊

– Soli Deo Gloria

Unfortunately, Windows will tell you the connection is 100Mb, but not if it's full-duplex or half-duplex by looking at the network connection status. Moving it to another network jack and patching it into another port on the switch fixed the issue.

– Soli Deo Gloria

Windows 8 Developer Preview Available for Download

SEPTEMBER 13, 2011

CATEGORIES: OPERATING SYSTEM

Should be up tonight:

<http://www.winsupersite.com/blog/supersite-blog-39/windows8/windows-8-developer-preview-build-today-140553>

Updated 9/14/11: Don't bother. Very early release. Couldn't get most of the tiles to work in Metro. Classic start menu was missing. Did like the ribbon in the new explorer. Disliked cheesy Metro style UI.

– Soli Deo Gloria

List of Changes in Windows 8

SEPTEMBER 26, 2011

CATEGORIES: MISC

Someone made a nice listing of changes in Windows 8...

Source: <http://www.grouppolicy.biz/2011/09/what-is-new-in-windows-8/>

- sub-32bit video color is no longer supported in Windows 8
- XDDM video driver will no longer work in Windows 8 (*XDDM seems to be 2000/XP video drivers...why you would you use these in Windows 7/8 anyways?*)
- Upgrade of video driver in Windows 8 will not lose SYNC with monitor...
- Display Drivers can be Full, Render Only and Display Only
- True headless servers are now supported. Interrupt 10 is handled by stub driver of VGA driver.
- Video Driver crashes can be isolated to a specific engine rather than the whole driver.
- Windows To Go – You will be able to run full copy of Windows off any 32gb USB Storage device. This means you will be able to take your computer with you in your pocket and just plug it into almost any computer.
- USB 3 is now fully supported.
- WiFi Direct is now supported. This will allow you to connect any two WiFi direct devices without an access point.
- You can project any HTML5 video to a play-to device with Windows
- NVIDIA Windows 8 ARM based systems support TPM (This was a channel 9 video).
- Bitlocker Network Unlock in Windows 8 will be great. If the computer is plugged into the LAN no start-up PIN will be required.
- 15.6ms wake timer is gone during sleep mode therefore better battery life.
- Connected standby allows you apps to sleep but then periodically wake up and check for new information so they stay up to date.
- SMB 2.2 will allow you to load balance all SMB traffic over multiple NICs
- Built-in NIC teaming support
- Server comes in 3 modes: Full Shell, No Shell (*only management tools*) & Server Core. This means all certified server products must be able to run without a Windows shell.
- Servers are now configured using PowerShell and this is driven using Server Manager.
- Server Manager will allow you to manage multiple servers at the same time.
- Using PowerShell or DISM you can move add/remove the shell
- Windows 8 will have an AppStore: very similar to Windows phone.
- Hyper-V servers will support VHD's on SMB Shares. This means you can run a live migration fail over cluster without the need to use iSCSI or Fibre Channel SANs.

- All Metro App's will be able to save application configurations to SkyDrive. This allows your metro settings to roam between computers. This does NOT replace traditional AppData folder.
- RemoteFX will work over a WAN and has greatly reduced bandwidth requirements. It can also use UDP packets for transmission of videos.
- Hyper-V Virtual Network allows you to migrate hosts from on-site to off-site without having to re-IP the servers. A virtual network tunnel will be established between both sites that allows the same subnet to span multiple geographical locations.
- Single instance storage is now supported. Put your VHD files on a SMB file share and enable deduplication and reduce the storage requirements overnight. This also works for all other file types such as the MS Office file format.
- Hyper-V is now supported on the Windows 8 (*client*)
- Secure Boot ensures that the whole boot process is secure. This prevents malware/rootkits from being able to install before the OS starts. This leverages systems with a TPM chip.
- TPM can now be used to store certificates to ensure that malware cannot access these certificates. The is protected via a password with a hammer timeout
- Add multiple USB 3 devices and then pool them together for a high performance disk drive.
- Memory chips can now be put into low power mode saving power on a system.

– Soli Deo Gloria

Getting Rid of Local Profiles for Multiple Use PCs

OCTOBER 1, 2011

CATEGORIES: OPERATING SYSTEM, TECH TIPS

One annoying thing with multi-use PCs such as those in conference rooms or terminal services is the glout of user profiles that build up. Such is the task I was asked to solve when building a VM in VSphere.

The solution is simple: add Domain Users to the local Guests group and Windows will automatically purge the profile on logoff. It doesn't seem to do this with accounts with administrative rights, but it seems to work for every other account without admin rights.

I gleaned this gem from this web page from someone named rvdmast:

<http://www.edugeek.net/forums/windows/4292-script-delete-profile-log-off-2.html>

In the words of Columbo: just one more thing. When you place Domain Users in Guests, you also become locked down and won't be able to do certain things such as accessing the local event logs. You can get around this by using RunAs and the local administrator account (*which is NOT apart of Domain Users*). I also had one PC where this refused to work. I just used [Delprof](#) from Microsoft and used a scheduled task at the system's boot to run this utility to purge the system of needless profiles.

– Soli Deo Gloria

Finding the OS Type in VBscript

NOVEMBER 1, 2011

CATEGORIES: MISC

Poached parts of this script from

<http://anandthearchitect.wordpress.com/2008/11/12/find-os-type-using-vbscript-ready-to-use-vbscript-function-right-here/>. Finds the current OS, then allows you to fire actions based on that information.

```
Set Shell = CreateObject("WScript.Shell")
Set oFSO = CreateObject("Scripting.FileSystemObject")
strComputer = Shell.ExpandEnvironmentStrings("%computername%")

Set objWMIService = GetObject("winmgmts://" & strComputer & "/root/cimv2")
Set colItems = objWMIService.ExecQuery("Select * from Win32_Battery",,48)

IsLaptop = False

For Each objItem in colItems
    IsLaptop = True
Next

If IsLaptop Then
    wscript.stdout.write "Laptop, running PowerLinkTSIcon()"
    PowerLinkTSIcon()
Else
    wscript.stdout.write "Not a laptop, not running PowerLinkTSIcon()"
End If

Sub PowerLinkTSIcon()

OSType = FindOSType(strComputer)

wscript.echo OSType

If OSType = "Windows XP" Then
```

```
oFSO.CopyFile "PowerLink Terminal Services.lnk", "C:documents and settingsal
End If
```

```
If OSType = "Windows 7" Then
oFSO.CopyFile "PowerLink Terminal Services.lnk", "C:userspublicdesktop"
End If
```

```
oFSO.CopyFile "Powerlink.ico", "C:windowssystem32"
End Sub
```

```
Function FindOSType(strComputer)
'Defining Variables
Dim objWMI, objItem, colItems
Dim OSVersion, OSName, ProductType

'Get the WMI object and query results
Set objWMI = GetObject("winmgmts://" & strComputer & "/root/cimv2")
Set colItems = objWMI.ExecQuery("Select * from Win32_OperatingSystem",,4

'Get the OS version number (first two) and OS product type (server or de
For Each objItem in colItems
    OSVersion = Left(objItem.Version,3)
    ProductType = objItem.ProductType
Next

'Time to convert numbers into names
Select Case OSVersion
Case "6.1"
OSName = "Windows 7"
    Case "6.0"
        OSName = "Windows Vista"
    Case "5.2"
        OSName = "Windows 2003"
    Case "5.1"
        OSName = "Windows XP"
    Case "5.0"
        OSName = "Windows 2000"
    Case "4.0"
        OSName = "Windows NT 4.0"
    Case Else
```

```
        OSName = "Windows 9x"  
    End Select  
  
    'Return the OS name  
    FindOSType = OSName  
  
    'Clear the memory  
    Set colItems = Nothing  
    Set objWMI = Nothing  
End Function
```



- Soli Deo Gloria

Stop Internet Censorship (SOPA)!

NOVEMBER 17, 2011

CATEGORIES: MISC

Join me in the fight to stop Internet censorship: <http://americancensorship.org/>

– Soli Deo Gloria

Fun with Bootable USB Flash Devices

DECEMBER 1, 2011

CATEGORIES: TECH TIPS

If you are interested with booting operating systems from a USB Flash device, check out RMPrepUSB.com. This is the home of the kick arse utility called RMPrepUSB that will make your USB device bootable a snap using either syslinux or grub4dos boot managers. Using this utility, I was able to take a 2GB SD card and my Zonet SD card reader and create a WinPE 3 x64 bootable USB flash device using Make_PE3 and RMPrepUSB with great ease.

Another cool thing I discovered is the ability to test booting your USB flash device with QEMU Manager (*tutorial [here](#)*). The advantage to this is that you can take screen shots of the early stages and you don't have to keep rebooting your computer all the time to see the changes you made. There are over 50 tutorials on this web site, from installing Windows XP from a USB flash device to resetting passwords.

Speaking of USB flash devices: [ISOSTick](#). This is a project they are trying to get off the ground and is worth watching. It is a USB flash device where you drop an ISO file unto it and then you can boot from that ISO, without any of the messy configuration necessities of grub4dos or syslinux.

– Soli Deo Gloria

UltraISO 9.3 for Free!

DECEMBER 6, 2011

CATEGORIES: MISC, TECH TIPS

I was looking around for a free ISO editor and found a promo for UltraISO

9.3: <http://www.raymond.cc/forum/freebies/12282-free-ultraiso-v9-full-license-key.html>

This was offered as a freebie in the June 2009 PC User magazine from Australia.

– Soli Deo Gloria

Donate to EFF this weekend and it will be matched 4x!

DECEMBER 10, 2011

CATEGORIES: MISC

Join me in fighting for the users! Become an EFF member today and your donation will get a 4x Power Up @ <https://supporters.eff.org/donate/powerup>

These are the guys that fight against the censorship of the Internet and ridiculous laws such as SOPA and PROTECT-IP.

– Soli Deo Gloria

Scott Hanselman's 2011 Power Users Tool List for Windows

DECEMBER 17, 2011

CATEGORIES: MISC, REVIEW, TECH TIPS

A very nice [list of power tools](#) by Scott Hanselman. Most of these are free.

I would add the following to the list (*most of which have already been mentioned on my blog some where in the past*):

[DesktopOK](#) – Save and restore the positions of desktop icons.

[DontSleep](#) – Don't Sleep is a small portable program to prevent system shutdown, Standby, Hibernate, Turn Off and Restart.

[MobaXterm](#) – Like Putty/SecureCRT, but better. Allows you to run XWindows apps over a ssh connection.

[Agent Ransack](#) – Search utility that adds a context menu for searching and allows advanced searching features such as searching for a text string in a set of files.

[DirSync Pro](#) – DirSync Pro is a small, but powerful utility for file and folder synchronization. DirSync Pro can be used to synchronize the content of one or many folders recursively.

[GreenShot](#) – Greenshot is a light-weight screenshot software tool for Windows.

[FF File Time](#) – A program that allows you to easily modify the time stamps of any file on your computer. It features an easy to use GUI that offers the possibility to modify not only single but also multiple files or whole directories.

[Google Chrome](#) – My favorite web browser! Add addons from the Chrome store such as GMail, Google Voice, Adblock and IETabs.

[Free Download Manager](#) – Why buy GetRight when you can use this program for free? Helps with troublesome downloads that like to stall out in web browsers.

Secunia Personal Software Inspector (PSI) – Secunia PSI is a security scanner which identifies programs that are insecure and need updates. It even automates the updating of many of these programs, making it a lot easier to maintain a secure PC.

QEMU Manager – Lightweight Virtual Machine emulator. Also has versions that run from a USB flash device. Seems to only use its own internal DHCP server and won't use an external network's DHCP server.

Zip2Secure – “ZIP 2 Secure EXE” is a utility program that creates self-extracting EXE files for Windows. Self-extracting EXE files are executable programs (EXEs) that contain a ZIP file and the software necessary to unzip the contents. No other software is needed.

– Soli Deo Gloria

Google Voice: Power to the People!

JANUARY 1, 2012

CATEGORIES: REVIEW, TECH TIPS

Lately, I've had a phone that just keeps randomly calling my cell phone. It appears to be some magazine subscription service. I get at least 2 calls a day and let's just say it's really annoying. Don't have to use my imagination to think that this is probably some type of obnoxious robocall service.

I rarely use my phone, so I have a prepaid plan with over 3000 minutes (*accumulated over a few years of light use*), with a max cap of 5000 minutes. After digging around on the Internet, I discovered that Google Voice can block calls with a very cool message: "this phone number is no longer in service". Sounds like the real deal too! Even more cool is that I can have it notify me when I've missed a call through the Google Voice extension for Chrome or alert me to a new voice message that I can play right from the Internet. All I have to do is forward my phone number to Google Voice.

It seems odd that blocking e-mail addresses is pretty trivial these days (*Hotmail.com even allows top-level domain blocking!*), but nothing like that seems to exist for most cell phone providers. AT&T has a parental control service that they will sell you for \$5/month, but it doesn't work for prepaid plans. Bummer. Maybe with all the FCC regulations that we now have on the books, maybe we can add 1 more that would require cell phone providers to allow all customers to block phone numbers of their choice from a web page. Crazy?

The one caveat to using Google Voice with conditional forwarding is that this will use the phone plan's airtime minutes: basically, it costs me 10 cents every time someone calls me regardless of whether they leave a message. Given that I add \$100/year to carry over the unused minutes, I'm only paying about \$8.33/month to keep to the right to use the phone when I want.

XYplorer 10.8 Free! Today Only.

FEBRUARY 6, 2012

CATEGORIES: MISC

Go get it! <http://www.giveawayoftheday.com/xyplorer1080/>

– Soli Deo Gloria

Imaging PCs from just from a USB Stick

FEBRUARY 10, 2012

CATEGORIES: OPERATING SYSTEM, TECH TIPS

So, how fast can you image a PC from a USB stick? This was a good question, as we aren't using multicast and the server only has one NIC. A normal image in WIM format applied using GImageX at around 5.8Gb in size over 100Mb Ethernet cabling takes around 16 minutes. The first experiment was tried with a Komputerbay SDXC (*Class 10*) card and reader. Windows only supports 1 partition on removable media, so you need to make the file system NTFS to accept files > 2.1Gb. I simply copied the contents of my WinPE 3.0 ISO unto the SDXC card and booted from it. This resulted in 10 minutes imaging time for a 38% increase in speed.

I then tried a Kingston DT160 USB flash stick. For this, simply copying the files to the USB flash drive wouldn't make the device bootable for some reason. I used the Microsoft Standalone System Sweeper program to create a bootable WinPE USB stick, then overwrote everything with the contents of my ISO file. This time: I clocked in at 6 minutes or a 63% increase in speed. These experiments were all carried out on a Dell Latitude e6420.

Later on, the speed of the DT160 dropped from 6 minutes back to 10 minutes. I cannot explain this decrease in speed, since I am only pulling bits over the USB channel and not the network. Still, this is boon for imaging:

You can deploy this USB stick to remote sites that have no deployment points.

You could give this USB stick to an OEM to have them image all your new computers before they leave the factory.

You could bundle this with every road warrior (*a 16Gb flash drive can be had for \$25 and the price just keeps dropping*). Boot into WinPE with a file manager to allow saving of data or better yet, have some type of TeamViewer environment so you can look at their dead laptop remotely!

– Soli Deo Gloria

Windows 8 Coming in October 2012

MARCH 20, 2012

CATEGORIES: MISC

Whoa, I've been slacking! Here's quick article stating that Windows 8 will hit the market in October 2012:

<http://www.bloomberg.com/news/2012-03-19/microsoft-said-to-finish-windows-8-in-summer-with-october-debut.html>

And Paul Thurrott has an article on Outlook

15: <http://www.winsupersite.com/article/office/whats-coming-microsoft-outlook-15-142613>.

The built-in Hotmail integration is nice: don't have to download a separate addon anymore.

– Soli Deo Gloria

VBScript CopyFile/FolderExists Quirks

APRIL 15, 2012

CATEGORIES: MISC

So I'm posting this here for my future reference:

```
Set oFSO = CreateObject("Scripting.FileSystemObject")
```

```
If oFSO.FolderExists("C:Program Files (x86)SmartDraw 2012") Then  
    oFSO.CopyFile "SDX.DLX", "C:Program Files (x86)SmartDraw 2012"  
End If
```

```
If oFSO.FolderExists("C:Program FilesSmartDraw 2012") Then  
    oFSO.CopyFile "SDX.DLX", "C:Program FilesSmartDraw 2012"  
End If
```

VBScript can be funny. If you omit the "" on the end of the CopyFile statement, the run time engine will bark at you: something like "Access Denied". Yet, the "" isn't needed in the FolderExists statement. So you can spend minutes and minutes looking at the two statements scratching your head why the later doesn't work.

So what does this code do? Well, it copies an updated license file for a program we use called Smartdraw. The funny thing is that I copied the new license before the old one expired, yet users running Windows 7 started calling the HelpDesk stating their copy of Smartdraw had expired. Yet, if you did a run-as administrator on Smartdraw, the program would work fine. I contacted Smartdraw tech support only to be told that you can simply go into the properties of said program and check the "Run as administrator" box to fix the problem. Not the most elegant solution.

The real problem was that an older copy of the file SDX.DLX was sitting in C:UsersusernameAppDataLocalVirtualStoreProgram Files (x86)SmartDraw 2012. Removing

this file fixed the issue. The real question is: why wasn't this file updated when I did the file copy? Obviously, UAC stepped in the first time and noticed that a file was trying to be written to C:\Program Files (x86), so it was re-directed instead to the VirtualStore folder.

Upon first launching Smartdraw, the program attempts to contact an activation server over the Internet and then writes the SDX.DLX file back to the Program Files (x86) directory with the activation status. UAC senses this and then re-directs it to the VirtualStore instead. However, when I ran my script, it ran under the SYSTEM account which likely bypasses UAC and the VirtualStore folder.

– Soli Deo Gloria

Honey I Shrunk the VHD!

MAY 9, 2012

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I recently tried running Disk2VHD to convert a Windows XP x64 machine to add to a Virtual Server 2005 server. Upon trying to attach the 12GB VHD to Virtual Server 2005, I got the error message “*The virtual hard disk image AdamVMx64.VHD is too large for the IDE bus. Make sure that all virtual hard disk images connected to the IDE bus are not greater than 127.5 GB.*” This was weird, as the physical disk is 148GB, but the resulting VHD was only 12GB. I downloaded Partition Wizard and sized down the active partition to 80GB. I took another capture with Disk2VHD and again, Virtual Server rejected it as being too big.

I went off to Google and found the [VHD Resizer](#). Upon running this tool and sizing down the VHD to 80GB, I was finally able to get Virtual Server to accept it.

– Soli Deo Gloria

Adding and Removing Printers with VBScript

JUNE 1, 2012

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Here's some VBScript code to add and remove printers, although it sounds like we are finally going to start using Group Policy Preferences to do the heavy lifting for printer deployment.

One thing I found is that this script doesn't work too well on Windows 7. I haven't investigated it too deeply, but I believe it is due to the [Point and Print group policy](#). Disabling this policy allows the script to work.

Note that you should use UCASE, which will convert all the letters in the print queue to upper case letters before you do the comparison. On some computers: the print queue would be all in upper case and some all in lower case, so using UCASE forces the strings to be compared in the same format.

Using WMI, it will also preserve the status of the default printer and adjust the default status accordingly.

```
strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
& "{impersonationLevel=impersonate}!\\" & strComputer & "rootcimv2")
Set colInstalledPrinters = objWMIService.ExecQuery _
("Select * from Win32_Printer where Default = True")
For Each objPrinter in colInstalledPrinters
PrinterDefault=objPrinter.Name
Next

Set WshNetwork = WScript.CreateObject("WScript.Network")

' Add COPIER_POD_07
WshNetwork.AddWindowsPrinterConnection "\\ACMEDCCOPIER_POD_07"

' Add COPIER_POD_19
WshNetwork.AddWindowsPrinterConnection "\\ACMEDCCOPIER_POD_19"
```

```
' Add PRINTER_POD_03
WshNetwork.AddWindowsPrinterConnection "\\ACMEDCPRINTER_POD_03"

' Add PRINTER_POD_17
WshNetwork.AddWindowsPrinterConnection "\\ACMEDCPRINTER_POD_17"

Set WSHPrinters = WSHNetwork.EnumPrinterConnections
PrinterPath = "\\ACMEDCWK_ENG_PLTR_01"
PrinterExists = False
For LOOP_COUNTER = 0 To WSHPrinters.Count - 1 Step 2
If UCase(WSHPrinters.Item(LOOP_COUNTER +1)) = PrinterPath Then
PrinterExists = True
End If
Next
If PrinterExists Then
WshNetwork.RemovePrinterConnection "\\ACMEDCWK_ENG_PLTR_01"
WshNetwork.AddWindowsPrinterConnection "\\ACMEDCPLOTTER_POD_14"
If PrinterPath=PrinterDefault Then
WSHNetwork.SetDefaultPrinter "\\ACMEDCPLOTTER_POD_14"
End If
End If

Set WSHPrinters = WSHNetwork.EnumPrinterConnections
PrinterPath = "\\ACMEDCWK_ENG_LSR_01"
PrinterExists = False
For LOOP_COUNTER = 0 To WSHPrinters.Count - 1 Step 2
If UCase(WSHPrinters.Item(LOOP_COUNTER +1)) = PrinterPath Then
PrinterExists = True
End If
Next
If PrinterExists Then
WshNetwork.RemovePrinterConnection "\\ACMEDCWK_ENG_LSR_01"
WshNetwork.AddWindowsPrinterConnection "\\ACMEDCPRINTER_POD_14"
If PrinterPath=PrinterDefault Then
WSHNetwork.SetDefaultPrinter "\\ACMEDCPRINTER_POD_14"
End If
End If
```

– Soli Deo Gloria

Dana Carvey as Tom Brokaw/Various Impressions

JUNE 29, 2012

CATEGORIES: JOKE

Why don't they make comedy like this anymore?

<http://www.youtube.com/watch?v=SkhwiuRbOEE>

<http://www.youtube.com/watch?v=hk4Jx6Y9sAA>

– Soli Deo Gloria

Malware Hunting with the Sysinternals Tools/Case of the Unexplained 2012

JULY 1, 2012

CATEGORIES: TECH TIPS

[Malware Hunting with the Sysinternals Tools.](#)

[Case of The Unexplained 2012.](#)

From Technet 2012, hosted by Mark Russinovich.

– Soli Deo Gloria

Windows 7 and the Forever “Spinning Wheel” Issue

JULY 7, 2012

CATEGORIES: TECH TIPS

I rarely troubleshoot home PCs, unless it's a special case. Someone recently brought me a Dell Dimension 9100 PC (*about 6 years old*) to fix. The complaint was that the PC was freezing up every few minutes. I suspected the hard drive, as the expected life was 5 years and the drive was 6 years old. Process Explorer and Autoruns returned clean results. I ghosted the old drive to the new one and yet continued to experience freeze ups. I loaded trusty old Procmon and found two processes hammering the system in the background: HPNetworkCommunicator.exe and AcroRdInfo32.exe. After some Googling on the HP process, I found this tech article called [The Mouse Cursor Turns Into an Hourglass \(System is Busy\) After an HP Printer Network Installation](#). It seems that the HP software consistently burns up CPU cycles checking for ink levels and any new scans from the wireless printer. Stupid! Turning the ink level check and scan check off brought the mouse cursor behavior back to normal.

The AcroRdInfo32.exe problem went away when I upgraded Adobe Reader 9 to X. According to this [page](#), this is a helper program for the windows shell that brings back extended information about the PDF. It's unclear why I was seeing it in Procmon burning CPU cycles, as I didn't have ANY PDF files selected.

The same guy also brought me a laptop infected with Sirefef.B. I cleaned it off using Windows Defender Offline or so I thought. I reloaded Microsoft Security Essentials and then it started going crazy again, finding Sirefef.B files over and over again. Windows would then tell me it encountered an error and would shut down within 1 minute. I ended up having to run TDSSKiller and it found Sirefef.B in the boot sector. It took several passes to clean it off as I had to try to clean it off under a minute!

– Soli Deo Gloria

Windows 8 to RTM in August, go on sale in October, Microsoft confirms

JULY 9, 2012

CATEGORIES: MISC

Article @ [ArsTechnica](#).

– Soli Deo Gloria

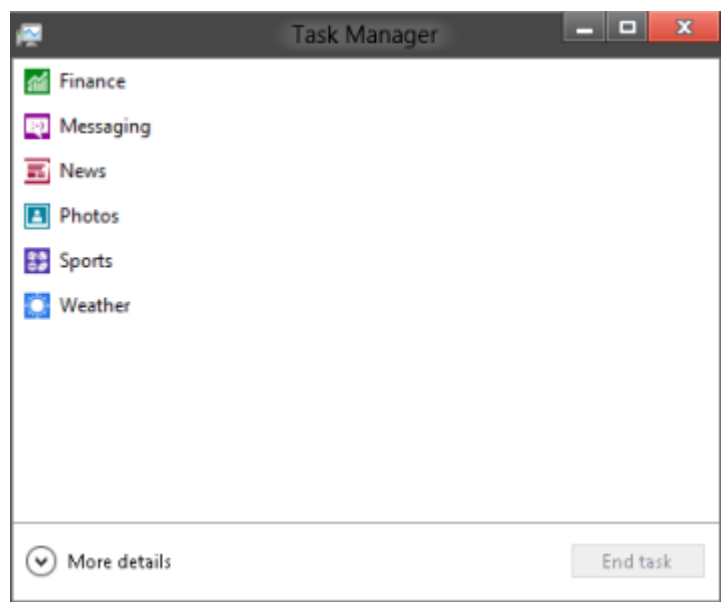
Windows 8 – Consumer Preview – First Impressions

JULY 14, 2012

CATEGORIES: OPERATING SYSTEM, REVIEW

After the Developer Release left a bad taste in my mouth, I was prompted to try the Windows 8 Consumer Preview from a fellow tech, who claimed he really liked Windows 8. The one thing that really bothers still is the inability to disable the Metro start page and the removal of the start menu in the desktop application. One way around the start menu snafu is to put it back using [Classic Shell](#). This actually does a good job, except that the Metro start page sometimes tries to take over when you hover your mouse too far to the bottom left. Leave Metro for the tablets I say and leave the classic Windows desktop for laptops/desktops.

The task manager in Windows 8 is really bland and the default configuration gives less information than even the Windows 7 task manager (*also noted by Mark Russinovich during his malware speech: malware can more easily hide now*). Windows' 7 task manager actually does a good job of separating user and system processes so you can easily see what is running on your system.



The one thing I do like about Windows 8 is the file copying process. If you copy files and folders from multiple locations, you can now pause specific copies. Overall, the operating system seems snappy. If they can just fix that darn Metro starting interface, it would be perfect.

– Soli Deo Gloria

Windows 8 Goes RTM

AUGUST 1, 2012

CATEGORIES: MISC, OPERATING SYSTEM

Windows 8 hit RTM today and should be available on MSDN and Technet on August 15th. General availability is October 26th.

– Soli Deo Gloria

An Inplace Upgrade to Windows 8

AUGUST 18, 2012

CATEGORIES: OPERATING SYSTEM, REVIEW

Maybe I'm getting old and cranky, but I'm not really excited about this version of Windows. I downloaded the RTM bits from Technet on 8/15/12 and installed the Enterprise version at work in a VM. On Friday night, I decided to upgrade my laptop (a Dell e6420) running Windows 7 Professional to Windows 8 Professional before taking the plunge on my main desktop. The first thing I noticed is that the retail media now requires you to enter a product key and will not let you go further without it. This is a pain in the neck...what if I just want to evaluate Windows 8 and not activate it? The Enterprise version by default does not ask for a product key. I went to the Technet web page and copied and pasted the key. It ran a compatibility check and told me I had to remove Microsoft Security Essentials (*Windows 8 comes with its own AV solution*), the bluetooth drivers and the wireless drivers. It also wanted me to plug in the AC adaptor. I removed all items and rebooted. I re-ran the setup and it wanted the product key again. Now I had no Internet because I had to remove the wireless drivers, so I had to manually key in the product key from another computer (*grumble*). It still would not let me upgrade without plugging in the AC adaptor. I plugged it in and then it proceeded with the setup, so I unplugged it, but thought better of it...who knows what Windows will do if it finds out later on that it is on battery power (*like cancelling the upgrade!*). I told it to keep all programs, settings and personal files.

After the upgrade, I noticed the wallpaper and my profile picture was not migrated, but were reset to the default pictures. All of the files and programs did seem to be intact, however. I had no Internet access, because I had removed the wireless drivers which in turn likely wiped out my connection settings, so I had to manually key those back in. Certainly not a seamless upgrade. I attempted to launch Mobaxterm and was told by Smartscreen that the publisher wasn't recognized and did I really want to run this program? That's fine in Internet Explorer, but not the main operating system, so I headed to the Action Center to turn Smartscreen off.

I immediately loaded Classic Shell, because not having the start menu is not an option. If you are looking for a hotkey to get some type of menu before hand, try Windows Key-X. Classic Shell also bypasses the Metro screen by default (*can be turned off*) and the next version will allow disabling of the "charm" corners (*all or a select few*). I also noticed that Windows went ahead and activated itself right away with Microsoft. In Windows 7, it would give you 3 days to activate. Maybe I didn't want to activate Windows just yet...maybe I wanted to move Windows 8

to another piece of hardware...why does Windows activate itself without my permission? Do you have to keep it off the Internet to evaluate it?

I had been using Windows XP Mode on this laptop, but Windows XP Mode is no more in Windows 8. It's now been replaced by Hyper-V. Hyper-V is great and all, but what about all the setup I did in my XP VHD? I went ahead and made a new VM in Hyper-V and attached the Windows XP Mode.VHD file. As expected: Windows XP wanted activation and would not let me proceed further. The version of Windows XP in Windows XP Mode is BIOS locked to the BIOS that Virtual PC emulates. So if you want to use XP in Windows 8, you need a retail/volume copy, a license and you need to set it up from scratch. Bummer, this is progress? The new Windows explorer does load VHD files natively just by clicking on them, which is a nice touch, meaning you can get all of your data out of the VHD (*I guess this also works for ISO and IMG files: no more having to load Virtual CloneDrive*).

Also, the removal of Windows Media Center is disappointing...Microsoft is trying to kill it off: <http://thedigitalmediazone.com/2012/06/06/windows-8-media-center-startup-options/>. No longer can you boot directly into Windows Media Center and Microsoft is no longer logo certifying hardware tuners for Windows 8. Guess my HTPC is being left with Windows 7 Ultimate.

Windows 8 also comes bundled with certain Metro applications for dealing with files, such as PDF and music files. When you double-click on a file ending with .PDF, it switches to the Metro desktop away from the "desktop" or "Win32" environment. Annoying. This can be changed of course back to the default applications you want to open these types of files, but why would I want a Metro application on my desktop to open a PDF? Suggestion to Microsoft: detect the chassis of the equipment Windows is installing on and give different options to desktop users, laptop users and tablet users. Speaking of Metro, how the heck do you get out of the "Personalize your Computer" page? ESC key doesn't work and there is no X to get out. I had to keep using Windows Key - X to go back to the desktop.

Now the good...I do like the new Windows explorer and the tabbed top section. To view hidden files, all I had to do is click the view tab and then check mark "Hidden items". It still won't replace XYExplorer, however, for heavier operations. The ability to pause file copy operations is a long overdue feature in Windows. Task manager (*under the performance tab*) now includes an uptime count and mini graphs for CPU, memory, disk, and Ethernet: very cool! Performance seems good as well: mainly in the startup and shutdown phases.

I have yet to find the “killer app” in Windows 8. There’s nothing in Windows 8 that jumps out and says “I can’t live without this feature”. However, with the \$40 promotional upgrade, it’s a relatively painless upgrade to the pocket book. Just be prepared to do some tweaking to get things the way you like.

– Soli Deo Gloria

Tips for Windows 8

AUGUST 23, 2012

CATEGORIES: OPERATING SYSTEM, TECH TIPS

To disable the corner charms in Windows 8, bring back the start menu and skip the metro start screen, install [Classic Shell](#). Right-click on the start menu orb, go to Settings. Click the box next to All Settings, then click on the tab “Windows 8 settings”. Under “Disable active corners”, click All. Now you won’t have that stupid metro bar coming up when you place the mouse cursor in the upper right or bottom right corner of the desktop. If you want to get back to the Metro UI, hold the Windows key and press Q. If you like to go to the default Metro start page, use Winkey+C.

I found a nice list of Windows 8 shortcut keys here: <http://www.techspot.com/guides/506-windows-8-shortcuts-and-tricks/>. Winkey+Q, Winkey+D and Winkey+X are my current favorites.

You can also disable this via registry keys: <http://www.ghacks.net/2012/08/19/disable-windows-8-mouse-over-corner-interfaces/>

– Soli Deo Gloria

Cloning Hard Drives

SEPTEMBER 7, 2012

CATEGORIES: TECH TIPS

This seems like a simple procedure...I wanted to clone one hard drive to a larger one. I had a 500GB hard drive with 50GB left on it and I purchased a 3TB hard drive to replace it. I already own a Startech SATA Unidock (*love that little device!*) and just needed the drive copy program. I was trying to find a free copy of Paragon's Drive Copy, which is usually given away as a freebie in various promotions, but of course the time I need it there isn't a promotion going. I of course don't want to spend \$40 just to clone 1 hard drive to another, so I found this free utility called [MiniTool Drive Copy](#). Simple, free and powerful! I did a clone from my 500GB to a 3TB hard drive with no problems and a 250GB to a 500GB hard drive and again: no problems.

I looked around the web site and also found a free program called MiniTool Partition Wizard Home Edition, which allows resizing of partitions without re-formatting. If you need to clone a boot drive, get the bootable version of the Minitool Partition Wizard Home Edition from [here](#).

– Soli Deo Gloria

WinISO 5.3 Now Free!

SEPTEMBER 25, 2012

CATEGORIES: TECH TIPS

WinISO 5.3 is now free: <http://www.winiso.com/products/winiso-free.html>

– Soli Deo Gloria

Defrag Tools on Channel 9

OCTOBER 1, 2012

CATEGORIES: TECH TIPS

An interesting show for computer techs I found from the Grand Stream Dreams blog: <http://channel9.msdn.com/Shows/Defrag-Tools>. The main star of the show is Andrew Richards who is an Escalation Engineer at Microsoft. He goes over the tools he uses in his job on a daily basis on the show.

– Soli Deo Gloria

Limited Time Offer: Windows 8 Pro Users Can Get Media Center For Free

OCTOBER 25, 2012

CATEGORIES: OPERATING SYSTEM

See:

<http://www.winsupersite.com/article/windows8/limited-time-offer-windows-8-pro-owners-media-center-free-144627>

– Soli Deo Gloria

Query Active Directory for a Phone Number Quicky

NOVEMBER 1, 2012

CATEGORIES: TECH TIPS

Here's a way to query AD quickly for a user's phone number/department.

Create a shortcut with the command of **%windir%system32rundll32.exe**

dsquery.dll,OpenQueryWindow (poached from http://it-help.bathspa.ac.uk/winnt/nt_ad_query.html)

Click View, Choose Columns. Under Columns Shown, have it say "Name, Telephone Number, Description". Now you can click this icon, enter in a user's name (*any part*) and get their phone number and department.

– Soli Deo Gloria

Case of the Blue Screening Computer

DECEMBER 5, 2012

CATEGORIES: TECH TIPS

This was a fun one to troubleshoot. I deployed a brand new Dell Optiplex 390 to a guy in our electrical engineering lab with a fresh copy of Windows XP. A few weeks go by and he puts a ticket into our Help Desk about his PC bluescreening in the driver for this [USB to Serial device](#). Thinking it could be the USB to Serial device, I got one that was “shrink wrapped” and headed over there along with an updated driver from the web site. Same issue. I also noticed in the event log random BSODs happening in the video driver and other random OS files unrelated to the USB to Serial device. We tried the USB to Serial on a laptop with the same device he was testing with (*some type of electronic gizmo*): worked fine! I brought back another Dell Optiplex 390 and I switched the hard drive out. Within 10 minutes, we were getting the same BSOD in the same USB to Serial driver.

I took another brand new Dell Optiplex 390, put Windows XP on it and took it back. Can you guess what happened? Yup: an hour later, another BSOD. I took a power strip back there and plugged his PC into a different electrical outlet. Since then: no BSODs!

I took the two “bad PCs” back to my bench and both pass the Dell hardware diagnostics with flying colors. We never had a PC in this spot and no doubt that this electronic gizmo he’s testing with must be causing some electrical interference or “dirty power” issue. I’m not sure why this issue didn’t show up on the laptop, however.

Update (2/7/14): Upon further reflection, this problem appears to really be the Tripplite 19-HS USB to serial adapter itself and not the PC since I was getting this on yet another 390 with this adapter.

– Soli Deo Gloria

Case of the Troublesome OptiPlex 390

JANUARY 6, 2013

CATEGORIES: OPERATING SYSTEM, TECH TIPS, UNCATEGORIZED

We got in a batch of new Optiplex 390s recently and our Windows XP image just wouldn't work on them. The image would come down, Windows XP would boot once through the SYSPREP process and then I would get a lovely BSOD of 0x000000ED with UNMOUNTABLE_BOOT_VOLUME on the 2nd boot. This wasn't the famous STOP 7B error I was use to, but something else. I had added support for the Optiplex 390 over a year ago, so this was quite odd. I took another Optiplex 390 and imaged that as well (*thinking I had a possible hardware issue on my hands*) and got the same thing. These were the exact same symptoms from the [WinPE uberbug](#) and I eventually found this [article](#) over at Dell. I am using WinPE 3.0, so I patched it with [KB982018](#). No go. I even took my "uberbug script" out and no joy.

I then stumbled upon this [thread](#), again at Dell, and it sparked something. I did have ExtendOEMpartition=1 in my sysprep.inf file. It has been there for years, never causing a problem. I mounted the WIM using ImageX, changed ExtendOEMpartition to 0 in C:\sysprepsysprep.inf and then re-imaged and bang: success! It appears that SYSPREP doesn't understand the new aligning procedure for these hard drives and makes certain assumptions, which of course are now incorrect.

HP has a very decent whitepaper on the issue [here](#) and if that's not available, it's also [here](#) on my web site in case they decide to remove it. Supposedly, Vista with SP1 and later do not have the issue and neither does WinPE 3.1 or beyond.

Windows XP: I wish I could quit you, but I can't!

– Soli Deo Gloria

Adobe CS2 for Free?

JANUARY 13, 2013

CATEGORIES: MISC

Reported by <http://www.techsupportalert.com/content/get-adobe-cs2-suite-free-not-officially.htm>, it appears you can get Adobe CS2 for free.

– Soli Deo Gloria

XYplorer 11.9 for Free (Today Only)

JANUARY 15, 2013

CATEGORIES: TECH TIPS

For the next 18 hours, XYplorer 11.9 is available for free from [here](#). This is a very sweet file manager that normally costs \$30, but you can get it for free today. The last version offered was 10.8 last year at the same web site.

– Soli Deo Gloria

Bringing Back Safe Mode in Windows 8

FEBRUARY 1, 2013

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I was reading a few questions on Experts-Exchange.com today and someone posted that the F8 key no longer gets you into Safe Mode on Windows 8. Sure enough, I tried it and it doesn't work anymore! There are tricks to restart the system in safe mode if you started in normal mode, but that will be pretty useless if the system doesn't boot. However, if you run the following command from an elevated prompt, it will put back the legacy Windows 7 boot loader which will allow you to boot into Safe mode:

`bcdedit /set {default} bootmenupolicy legacy`

Of course, if you discover this fact too late, you might be out of luck! Of course you can boot from a Windows 8 DVD and use the Recovery option, but taking away the F8 key to get into safe mode is just plain stupid.

So to recap, when you move from Windows 7 to Windows 8, you lose:

DVD Playback

Windows Media Center

Safe Mode

Windows XP Mode

Start Menu

This was supposed to be an upgrade, right? Hmm.

– Soli Deo Gloria

Copying Large Files Between Sites

MARCH 1, 2013

CATEGORIES: TECH TIPS

I got a call recently from a tech at a remote site that said that our Windows 7 x64 image was bombing out at 16%. We did the usual “image another PC” and “bounce the server”, but the results were the same. I compared the file sizes and they were the same and the WIM file opened just fine with 7Zip. However, when I ran [Hasher](#) against my WIM file at corporate and the other sites, each one had a different SHA-1/CRC/MD5 value. Oops! I re-copied the file overnight and then verified with Hasher again and we had a match. I did some research on how I can verify and repair large files. I found [Multipar](#), [Parity files](#) have long be used on USENET for repairing large files transferred over the Internet. I just picked 1% for data redundancy and created the PAR file. For an 8GB image, that works out to be about an 80MB file. Using this 80MB file, I was able to verify and repair the 8GB file at the remote site.

I went through the rest of the images and some of them matched up and some of them didn't! Using the parity files created for each image, I was able to repair them all over remote desktop at the remote sites. I've been doing this overnight copy for years and it was never a problem. Of course, my images use to be < 2GB and now they are about 8GB each!

– Soli Deo Gloria

Help Desk Ticket Nonsense

MARCH 13, 2013

CATEGORIES: JOKE

I got a chuckle out of this:

<http://thedailywtf.com/Articles/Im-Sensing-Some-Tension.aspx>

– Soli Deo Gloria

When VMs Won't Cut It

APRIL 1, 2013

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I was recently working with Creo Parametric (*3d modeling software*). Unfortunately, my VMs are not powerful enough to run this software. Solution? Steadier State. Basically, this software let's you do a P2V conversion and then by using the VHD boot feature of Windows 7 Ultimate/Enterprise, it will create a difference VHD to your base VHD. Upon booting Windows 7, you get two options: Rollback Windows and Windows 7. Pick roll back Windows 7 and bingo: you're back to a clean state! This does require wiping out the contents of your C: drive however, so you will want to do this on a second box.

Update #1:

I found something better/easy for this process: Reboot Restore Rx (http://www.horizondatasys.com/en/products_and_solutions.aspx?ProductId=18). Only tested on XP, but it works great! You can toggle it on and off from the taskbar.

– Soli Deo Gloria

Windows Blue Is Now Called Windows 8.1

APRIL 3, 2013

CATEGORIES: MISC

Windows Blue is now known as Windows 8.1 and is scheduled for release sometime in August 2013: http://www.theregister.co.uk/2013/04/02/windows_blue_version_8_1/

-Soli Deo Gloria

Windows Blue Might Restore Start Menu

APRIL 19, 2013

CATEGORIES: OPERATING SYSTEM

Did Microsoft finally wake up? Let's hope so. This change would restore some of my faith back in Microsoft.

<http://arstechnica.com/information-technology/2013/04/windows-blue-could-restore-the-start-button-boot-straight-to-the-desktop/>

To quote Winbeta.org:

For those upgrading to Windows Blue, you might now have the option to remove the Start Screen. According to the report, after examining the code in twinui.dll, there is a line that is "responsible for disabling the Start Screen" and after disabling or modifying the code it makes the system "go to the desktop automatically." Those using Windows 8 or the leaked Windows 8.1 build, you will obviously know by now that this option isn't yet available.

From <http://www.winbeta.org/news/microsoft-possibly-working-letting-user-disable-start-screen>

– Soli Deo Gloria

Run a Certain Command Line Based on x86 or x64 Architecture

APRIL 27, 2013

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I've published about running certain files based on the operating system type (see [this posting about such VBScript code on my blog](#)), but what if you want to run something based on processor type, i.e. x86 or x64? The "problem" with VBScript is that it can be hell on earth dealing with command lines that involve quotes and switches. How about a simple batch file instead?

```
@echo off
```

```
Set RegQry=HKLM\Hardware\Description\SystemCentralProcessor
```

```
REG.exe Query %RegQry% > checkOS.txt
```

```
Find /i "x86" < CheckOS.txt > StringCheck.txt
```

```
If %ERRORLEVEL% == 0 (  
Echo "This is 32 Bit Operating system"  
) ELSE (  
Echo "This is 64 Bit Operating System"  
)
```

Stolen from <http://support.microsoft.com/kb/556009>. It's beautiful, simple and gets the job done. You can just stick your command lines as they are between the ()'s. Here's a sample of something I did for the push out of Creo Parametric 2.0:

```
@echo off
```

```
Set RegQry=HKLM\Hardware\Description\System\CentralProcessor
```

```
REG.exe Query %RegQry% > checkOS.txt
```

```
Find /i "x86" < CheckOS.txt > StringCheck.txt
```

```
If %ERRORLEVEL% == 0 (  
"C:\creo 2.0\Common Files\M040\install\addon\creoagent_32.msi" /passive  
) ELSE (  
"C:\creo 2.0\Common Files\M040\install\addon\creoagent_32_64.msi" /passive  
)
```

Of course, it would be much simpler to dump Windows XP and every 32-bit operating system known to man. If you have multiple lines, you will probably want to use something like **start /w** to wait for each line to finish, otherwise it will run every line all in one go.

- Soli Deo Gloria

More Fun with Dell Tech Support

MAY 11, 2013

CATEGORIES: JOKE, MISC

It's been a while since I've posted about Dell Tech Support, mostly because I've been DOSD certified for the past 2 years (i.e. *I can order parts without talking to a breathing human being*).

You can read my last article about Dell Tech Support [here](#). This chat log was sent to me by another technician and was just too "good" not to post. Names of the parties have been changed to protect the guilty.

This is an automated email sent from Dell Chat. The following information is a log of your session. Please save the log for your records.

Your session ID for this incident is XXXXXXXX.

Time Details

04/10/2013 10:06:44AM Session Started with Agent (DellRep)

04/10/2013 10:06:44AM Us: "Computer will not boot. Plug in power and the light on the power button turns on and goes to blue. Fans are running also but nothing is displayed on the monitor."

04/10/2013 10:06:52AM Agent (DellRep): "Thank you for contacting Dell Basic Hardware Warranty Chat for Optiplex and Latitude Systems under the Corporate and Business Group. My name is DellRep. I'll be happy to assist you with your concern today."

04/10/2013 10:06:55AM Agent (DellRep): "Incase we get disconnected do you have another phone number aside from the one you provided in the chat session?"

04/10/2013 10:07:27AM Us: "xxx-xxx-xxxx xxxx"

04/10/2013 10:08:17AM Agent (DellRep): "By the way, Is this for the OPTIPLEX 390 system with service tag XXXXXXXX?"

04/10/2013 10:08:32AM Us: "Yes it is"

04/10/2013 10:09:42AM Agent (DellRep): "May I ask what are the troubleshooting steps done to isolate the issue for us to properly document the case?"

04/10/2013 10:10:51AM Us: "Changed power supply and plugged it into different equipment at another physical location. It doesn't display anything so I cannot run the dell diagnostic"

04/10/2013 10:11:14AM Us: "Also tried a PCI-X video card and it did not work either"

04/10/2013 10:11:36AM Agent (DellRep): "Have you tried a known good hard drive?"

04/10/2013 10:12:18AM Us: "it won't even post so hard drive is irrelevant"

04/10/2013 10:13:28AM Us: "but yes we swapped the unit for the customer so currently it has a different harddrive for a known working installation of Windows on it"

04/10/2013 10:14:43AM Agent (DellRep): "At what part of the start up will the blue screen

appear? Can you still see the Dell splash scree?"

04/10/2013 10:15:10AM Us: "It does not boot at all, I never said it was experiencing a blue screen of death"

04/10/2013 10:15:33AM Us: "The powerlight turns on and turns blue the minute you plug in the power cord"

04/10/2013 10:17:30AM Us: "The computer appears to be in a on state, you can hear fans running and the power button light is on. Nothing displays on the monitor. It does not go through Post at all. There are no beep codes."

04/10/2013 10:17:31AM Agent (DellRep): "Have you added an external video card?"

04/10/2013 10:17:43AM Us: "Yes I stated that earlier in this conversation"

04/10/2013 10:19:34AM Agent (DellRep): "Can you run the system without the videocard and use the onboard instead?"

04/10/2013 10:19:57AM Us: "That is what we normally do"

04/10/2013 10:20:10AM Us: "this thing does not have an external video card installed"

04/10/2013 10:20:17AM Us: "we tried that for troubleshooting"

04/10/2013 10:20:28AM Us: "The motherboard is bad"

04/10/2013 10:20:34AM Us: "I have had this issue in the past"

04/10/2013 10:21:49AM Agent (DellRep): "I am creating a new case for you, and I will personally be your Point of Contact on this case until your issue is resolved."***04/10/2013 10:21:57AM Agent (DellRep): "Just to make sure that we get to send the necessary emails to the correct email address, can you please verify if xxxxxx@xxxxxxxxx.xxx is a good one?"***

04/10/2013 10:22:13AM Us: "that is correct"

04/10/2013 10:22:17AM Agent (DellRep): "I am creating a new case for you, and I will personally be your Point of Contact on this case until your issue is resolved."***04/10/2013 10:22:21AM Agent (DellRep): "I'll just ask for the address where the service will take place?"***

04/10/2013 10:22:38AM Us: "<company address>"

04/10/2013 10:23:33AM Agent (DellRep): "Thanks, I'll be needing few minutes to process the dispatch, Can you hold on for 3-5 Minutes while I process this?"

04/10/2013 10:23:47AM Us: "Yes"

04/10/2013 10:24:15AM Us: "It is not necessary to dispatch a technician I will replace the board myself"

04/10/2013 10:24:48AM Agent (DellRep): "Just wanted to let you know that the part(s) needed to be replaced is what we consider as a "Field-Replaceable Unit" which in most cases would only be installed by authorized Dell Technicians. Since you opted to just receive

the part (which is what we call

I as a "Part/s-Only-Service"), please be advised that Dell will not be held liable for any damages incurred while installing the replacement part(s).

04/10/2013 10:25:21AM Us: "Yes I am aware as I am an authorized Dell Technician"

04/10/2013 10:29:19AM Agent (DellRep): "Thanks, I'll be needing few minutes to process the dispatch, Can you hold on for 3-5 Minutes while I process this?"

04/10/2013 10:29:36AM Us: "Yup"

04/10/2013 10:33:55AM Agent (DellRep): "Thanks for waiting."

04/10/2013 10:33:59AM Agent (DellRep): "Your Dispatch number is XXXXXXXXXX."

04/10/2013 10:34:01AM Agent (DellRep): "I've set up this Parts and Onsite Service dispatch for you, and I'm sending you a summary email with all of your dispatch information. Depending on parts availability, you should be contacted before noon tomorrow (excluding holidays and weekends) where yo"

u'll be provided with an estimate for the time of day that the onsite technician will arrive for service.

04/10/2013 10:34:06AM Us: "Thank you"

04/10/2013 10:34:08AM Agent (DellRep): "I am booking an Onsite repair for this issue to replace the said part. If however the Dell Onsite Engineer identifies damage to the system which is not covered by your limited warranty there may be a cost incurred by you."

04/10/2013 10:34:14AM Agent (DellRep): "I've set up this Parts and Onsite Service dispatch for you, and I'm sending you a summary email with all of your dispatch information. Depending on parts availability, you should be contacted before noon tomorrow (excluding holidays and weekends) where yo"

u'll be provided with an estimate for the time of day that the onsite technician will arrive for service.

04/10/2013 10:34:15AM Agent (DellRep): "You can also check the status of the dispatch using this link. <http://www.dell.com/support/incidents/us/en/XXXX?c=us&l=en&s=&cs=XXXX>"

04/10/2013 10:34:16AM Agent (DellRep): "I've set up this dispatch for you, and I will personally be following up with you in a couple days to make sure that your issue is resolved. Please look for my email/ wait for my phone call so that I know your issue is resolved."

04/10/2013 10:34:17AM Agent (DellRep): "I'm sending you a summary email after out chat session. If you have any problems, please just respond using the instructions in that email to reach me, and I will be able to help you."

04/10/2013 10:34:19AM Agent (DellRep): "You will be receiving 2 or 3 emails from us. One is a copy of our chat session and the other is a summary email. You may keep these for your

records. If you require further assistance, please reply to my email and I'll be glad to call you back and re-open"

this case anytime. You can also visit us online at www.dell.com/chat or call 1-800-822-8965

04/10/2013 10:34:20AM Agent (DellRep): "Is there anything else I can assist you with?"

04/10/2013 10:34:27AM Us: "I told you I don't want an onsite technician"

04/10/2013 10:34:41AM Us: "it is unnecessary as I am a dell certified technician for my company"

04/10/2013 10:35:19AM Agent (DellRep): "I'll just reprocess it."

04/10/2013 10:35:26AM Agent (DellRep): "Sorry for that XXXXX"

04/10/2013 10:36:32AM Us: "Thank you"

04/10/2013 10:36:45AM Agent (DellRep): "Is there anything else I can assist you with?"

04/10/2013 10:36:51AM Us: "that will be it"

04/10/2013 10:37:01AM Agent (DellRep): "Few quick questions,

Are you satisfied with the service I provided you today?

And, Is your issue today resolved to your satisfaction?"

04/10/2013 10:37:11AM Us: "yup issue is resolved"

04/10/2013 10:37:25AM Agent (DellRep): "We appreciate your time for contacting us and its been a pleasure working with you."

04/10/2013 10:37:26AM Agent (DellRep): "Thank you for your Time and Thanks again for contacting Dell Technical Support Chat. You may now disconnect from the session. Have a nice day!"

If you require further assistance, please visit us at support.dell.com

-Soli Deo Gloria

Case of Jerky Movement in Battlefield 3

MAY 27, 2013

CATEGORIES: MISC

Just have to love computers. I went to play Battlefield 3 today and my character wouldn't move forward. I reset all the settings in the game and no go. I proceeded to do a System Restore and same thing. I completely uninstalled and reinstalled the game: same thing! I was holding down the W button to move forward and it just won't work. I also noticed when I hit the ESC key it wouldn't respond right away. I plugged in another keyboard and presto: everything worked fine! I reset both my keyboard and KVM and now everything is fine with the original keyboard.

Well, that was a waste of my time!

– Soli Deo Gloria

Disable Sun Java Updates with a Reg Hack

JUNE 2, 2013

CATEGORIES: TECH TIPS

Disable those nasty Sun Java update messages with this fun registry hack! Just copy and save into a REG file, then double-click on the REG file as an administrator (*note on Windows x64 you need to change this to HKEY_LOCAL_MACHINE\SOFTWARE\WowNode6432\JavaSoft\Java Update\Policy for 32-bit Java*)

Windows Registry Editor Version 5.00

"EnableJavaUpdate"=dword:00000000

"EnableAutoUpdateCheck"=dword:00000000

"NotifyDownload"=dword:00000000

"NotifyInstall"=dword: 00000000

"UpdateSchedule"=dword: 00000000

– Soli Deo Gloria

Mark Russinovich's TechEd 2013 Videos

JUNE 10, 2013

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Case of the Unexplained 2013:

<http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/WCA-B306#fbid=yFdvHCrhH-q>

License to Kill: Malware Hunting with the Sysinternals Tools:

<http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013/ATC-B308#fbid=yFdvHCrhH-q>

– Soli Deo Gloria

Fun Cleaning off the FBI Virus

JUNE 14, 2013

CATEGORIES: OPERATING SYSTEM, SPYWARE, TECH TIPS

I recently had a remote laptop user that got infected with some type of fake malware FBI virus. The virus was pretty cool, at least from a technical perspective. The malware activated the web cam in the laptop and took a picture of the user demanding to be paid in some form of money called Moneypak in order to “decrypt” the hard drive’s files. The laptop would not boot into safe mode without blue screening and the task manager/start menu/desktop were all locked out in normal mode. However, we were magically able to login as another user and the FBI virus wasn’t loading for that user profile. How someone could spend so much time doing a good job locking down the computer and then have it be bypassed with another user login is quite baffling to me. Anyways, I tried a system restore and it wouldn’t go, saying something about it was interrupted and therefore all the changes were being rolled back.

I used regedit to load the user’s profile as a hive, cleaned the autostart entries and deleted all of the virus EXEs from the user’s profile folder, but the darn virus kept coming back. So I did something I never did before: I gave myself rights to **C:system volume information** which is where system restore “hides” its restore points and then went looking in the RPXXX directories. Going by the dates, I was able to narrow down a “good” copy of the user’s profile. The ntuser.dat file will be in the format of something like **_REGISTRY_USER_NTUSER_S-1-5-21-** **(long string of numbers that correspond to a particular SID)**. I compared the size of his current ntuser.dat to this file and viola: we had a near match! I copied over this file as ntuser.dat into his profile directory, had him login and viola: no more virus!

However, his profile was still trying to load EXE files that didn’t exist anymore, which meant he probably had some “sleeper” viruses that weren’t announcing their presence on his laptop. I cleaned these “dead” entries off with Autoruns. A full virus scan found a few more goodies on the laptop which were removed.

After doing all of this work, I found a good primer on working with system restore points manually here: http://wiki.lunarsoft.net/wiki/System_Volume_Information. Web sites can go down, so I’ve also published the file [here](#) as a PDF.

I looked at my Windows 8 C:system volume information folder and yeah: completely different animal, so this would be a trick for Windows XP machines only.

Update #1

Of course, after I wrote this witty entry, I got a Windows 7 laptop with the same virus. I did an offline scan with Windows Defender Offline which removed the virus and then it wouldn't boot... in any mode and was getting critical failure BSOD. I tried booting to WinPE and doing a system restore, however, it told me system restore was disabled for this drive even though I could see the restore points! I unfortunately had to back up the user data from WinPE and wipe the drive and reinstall Windows. I might try a system restore from MS DaRT next time this happens.

Update #2

Yet another laptop with this virus, although this one was nastier. It was popping up on all logins to the laptop. I had a copy of MS DaRT, but it didn't have the right mass storage drivers for the Dell e6430 laptop I had, so I was getting a STOP 7B BSOD on boot and didn't feel like messing around injecting drivers and re-burning a new CD. System Restore failed to complete on this laptop as well. I used Wondershare's Liveboot 2012 and used the "Analyze System Offline" feature of Autoruns and found our little friend: a weird named DLL sitting in the user's temp folder under their profile. This DLL file was referenced in practically every startup location in Windows, even in ContextMenuHandlers sections and some bizzaro autorun feature of cmd.exe I never hear of before: HKEY_CURRENT_USER\Software\Microsoft\Command Processor. I removed all the entries with Autoruns and the malware screen was gone, however, after login, I would get a black cmd.exe window and that was it (*no desktop*). I could load explorer.exe from the task manager and get the desktop, but it wouldn't autoloading on its own and it looked like the shell was correctly defined. Anyways, I manually copied the system, software and user profile files out of the snapshots directory under C:\System Volume Information\RPXXX from Liveboot and again: the laptop was cured. Well, almost. The infection took off on the night 6/13/13, but when I ran Norton Power Eraser, it found another naughty DLL dated 4 days earlier in the user's profile directory (*it was under Application Data under a Konica folder I believe*). This means the first infection might have been a "sleeper" waiting to deliver a nasty payload at a later date or the virus skewed the time to hide.

Whatever the cause, this kind of malware is getting almost impossible to remove without a drive wipe. If I could figure out how it's corrupting/attacking the system restore function, that would help a great deal.

Update #3

I found a nifty program called the System Restore Explorer. This allows you to mount the restore points on Vista and later systems as a regular folder. I tried it on my VM and it works great (*and yes, it works on Windows 8 too!*)! One little snag is that you will have to work from an elevated command prompt, since C:\windows\system32\config is a protected folder and the restore point is mounted read-only (*i.e. you can't change ACLs*). You should be able to copy the SOFTWARE and SYSTEM out to a folder and replace the ones on the system from WinPE.

```

C:\HarddiskVolumeShadowCopy2\Windows\System32>cd config
C:\HarddiskVolumeShadowCopy2\Windows\System32\config>dir
Volume in drive C has no label.
Volume Serial Number is 4CC5-96C9

Directory of C:\HarddiskVolumeShadowCopy2\Windows\System32\config

06/12/2013  02:45 PM    <DIR>          .
06/12/2013  02:45 PM    <DIR>          ..
08/17/2012  07:28 PM             262,144  BCD-Template
06/17/2013  07:17 AM             32,768,000  COMPONENTS
07/26/2012  12:26 AM                0  COMPONENTS.LOG
06/21/2013  07:19 AM             786,432  DEFAULT
07/26/2012  12:26 AM                0  DEFAULT.LOG
06/20/2013  03:18 AM             5,136,384  DRIVERS
07/26/2012  12:31 AM                0  PP
07/26/2012  12:26 AM    <DIR>          Journal
06/21/2013  09:14 AM             120  netlogon.ftl
06/21/2013  03:19 AM    <DIR>          RegBack
06/21/2013  07:19 AM             262,144  SAM
06/21/2013  07:19 AM             262,144  SECURITY
07/26/2012  12:26 AM                0  SECURITY.LOG
06/21/2013  07:19 AM             84,934,656  SOFTWARE
07/26/2012  12:26 AM                0  SOFTWARE.LOG
06/21/2013  07:19 AM             13,631,488  SYSTEM
07/26/2012  12:26 AM                0  SYSTEM.LOG
07/26/2012  02:51 AM    <DIR>          systemprofile
07/26/2012  02:33 AM    <DIR>          TxR
          15 File(s)          138,043,676 bytes
           6 Dir(s)          52,124,250,112 bytes free

C:\HarddiskVolumeShadowCopy2\Windows\System32\config>

```

There's also this utility that does nearly the same thing that I have not tested: <http://sourceforge.net/projects/vistaprevsrcvr/>

Update #4

There's a better utility for exploring system restore points on Windows 7/8 called ShadowExplorer. It is available in a portable edition and if you run as administrator, you can export the file directly out without having to use the command console.

– Soli Deo Gloria

WinISO Standard 6.3 – Free – Today Only

JUNE 28, 2013

CATEGORIES: TECH TIPS

Go grab it: <http://www.winiso.com/giveaway.html>

Differences from free version: <http://www.winiso.com/products/compare.html>

It looks like it stores the registration in C:\Users<yourusername>\AppDataRoaming\WinISO Computing\WinISOuser.ini. I downloaded the regular installer exe from their web site and the registration from GOTD still held!

– Soli Deo Gloria

Change Classic Shell Icon back to Windows logo

JULY 4, 2013

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Classic Shell was forced by Microsoft to make their icon look less like the Microsoft one in version 3.6.8. Here's how to change it to look like it did in Windows

7: <http://www.askvg.com/download-classic-shell-skin-to-get-windows-7-look-like-start-menu-and-start-button-in-windows-8/>

or for a bunch of different skins: <http://www.classicshell.net/forum/viewtopic.php?f=18&t=853>

– Soli Deo Gloria

Random Thoughts on Microsoft

JULY 6, 2013

CATEGORIES: MISC, REVIEW

I finally stepped into the 21st century...sorta. I've had desktops and laptops, but no smartphone or tablet. I am now the proud owner of a Nexus 7 tablet. I mainly got the device to watch videos while I work out on the elliptical (*can't get enough of those UK shows with Gordon Ramsey!*).

However, I do have to say I've become "addicted" to this device. I can drag and drop magazine PDFs to the device and read them anywhere and the battery life is amazing. I can check e-mail from all 3 of my main accounts with a few flicks of my finger. I can check the weather, browse the web and shop all from the comfort of my chair. This Android operating system is pretty amazing...fast, clean and stable.

Then I think about Microsoft and the debacle of the Start Menu and Microsoft removing features such as Windows Media Center and DVD playback from Windows 8. Just last week Microsoft announced its retiring Technet subscriptions for its IT professionals, a subscription service I've had for the past 7 years. Microsoft may remain king of the desktop, but I don't see it making any major in-roads to the tablet market. It's too late to the game and its current attitude towards customers does not bode well for its future.

However, I don't see tablets replacing laptops or desktops either...typing is a chore on these things and at least for the Nexus 7, the lack of ports kills its expandability. One possibility I see is people transferring to Android applications on Windows through the use of emulation. Ween yourself off enough Windows applications and why do you need Windows anymore? Emulation of Windows from the Android side? Don't laugh: it could happen. Pick up a cheap copy of Windows 7 and emulate that from your new device running something other than Windows.

Personally, I think that's a long way off...maybe 15-20 years from now. Microsoft is kidding itself, however, if it thinks it's going to remain king of operating systems forever.

– Soli Deo Gloria

Imaging without an Ethernet Port

AUGUST 1, 2013

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Recently, we got back a Dell XPS 13 (L321X) laptop back in stock to re-image. It's one of those fancy ultrabooks that turned into an ultra pain in the backside. The laptop is so thin that putting a native Ethernet port on it would make it too big, so they just don't do it. The only way to get a "real" Ethernet port is to use a USB to Ethernet adapter. Since we only had a handful of these units, I configured them manually by hand when they first went out. Unfortunately, when the unit came back to us, the USB to Ethernet adapter went missing.

I had already been playing with MDT 2010's offline media feature and this was a perfect time to test it out. Basically, you can dump your whole MDT server to a USB flash drive and boot from it. It will pull everything it needs (*drivers, images, etc*) all from the USB key and not over the network. I had added support for the L321X a while ago, so my boot media already had all the driver support baked in. I attempted to boot from the USB port on the right side of the laptop with my USB stick. It booted to the deployment splash screen and then couldn't find the deployment files. I pulled the stick out and tried it out on a Optiplex 390 desktop. Success! I went back and tried the USB stick again, this time using the left side USB port and now it worked perfectly fine. Upon booting into Windows, the left USB port worked fine, but the right one didn't. After contacting Dell, it was determined that there is something called the Fresco chipset that handles the right USB port and these drivers were missing. Weird? The right USB port was a SuperSpeed port and the left one a legacy port. The imaging time was 21 minutes vs the normal 45 minutes by doing it over the network.

The process is pretty simple:

Go into the MDT 2010 MMC Console. Drill to Advanced Configuration>Media. Right-click on Media and pick New Media. Pick a folder with lots of space (*if the folder you want to use does not exist in the target location: you have to create it*). Make sure "Everything" is listed for the profile to use. Right-click MEDIA001, go to Properties and uncheck the option "Generate a Lite Touch bootable ISO image". Say OK and right-click MEDIA0001 again and pick Update Media Content. Do note that this process will take a long time: be patient.

Open a command prompt (*elevate as administrator*)

In the command prompt window type **diskpart**

Type **list disk**

Make note of the drive number representing your USB drive.

Type **select disk <#>** where <#> is the number of the USB drive discovered above.

Type **clean**

Type **create partition primary**

Type **select partition 1**

Type **active**

Type **format fs=ntfs quick**

Type **assign**

Type **list volume**

Make note of the drive letter representing your USB drive and the CD or DVD drive.

Type **exit**

Now copy the contents of the Content folder (*from the folder MDT created above*) to the root of your USB flash drive. Viola: boot from it and you have offline imaging magic! I removed the x86 version of my Windows image along with the ISO to get it to fit on my 16GB flash drive. I would recommend using a 64GB class 10 device if you plan to use this method for day to day imaging.

As of 4/29/16, the GRUB method below does not work on newer Dells such as the E5470 or E7270. Use Rufus instead.

Note that is also possible to dump the LiteTouch ISOs directly to the USB flash drive and boot them using Grub4DOS (*in case you are sick of using physical CDs to boot to LiteTouch*).

However, when I did this myself, it always picked the USB flash drive as C: and assigned the real hard drive as D:. I used a modification of the code from [here](http://reboot.pro/topic/17046-help-with-mdtpe-multiboot-setup/) to create my own USB stick: <http://reboot.pro/topic/17046-help-with-mdtpe-multiboot-setup/>. I suggest doing the diskpart steps above to make sure the boot record is clean.

```
default 1
```

```
color NORMAL HIGHLIGHT HELPTTEXT HEADING
```

```
splashimage=/fis.xpm.gz
```

```
foreground=FFFFFF
```

```
background=000000
```

```
title — Directly Bootable ISOs —
```

```
root
```

```
# Modify the following entry if it does not boot
title Windows 7 x86 LiteTouch
find -set-root -ignore-floppies -ignore-cd /LiteTouchPE_x86.iso
map -heads=0 -sectors-per-track=0 /LiteTouchPE_x86.iso (hd32)
map (hd0) (hd1)
map (hd1) (hd0)
map -hook
chainloader (hd32)
```

```
# Modify the following entry if it does not boot
title Windows 7 x64 LiteTouch
find -set-root -ignore-floppies -ignore-cd /LiteTouchPE_x64.iso
map -heads=0 -sectors-per-track=0 /LiteTouchPE_x64.iso (hd32)
map (hd0) (hd1)
map (hd1) (hd0)
map -hook
chainloader (hd32)
```

```
# Modify the following entry if it does not boot
title Windows XP ImageX
find -set-root -ignore-floppies -ignore-cd /winpe7.iso
map -heads=0 -sectors-per-track=0 /winpe7.iso (hd32)
map (hd0) (hd1)
map (hd1) (hd0)
map -hook
chainloader (hd32)
```

You can install Grub4DOS using the Grub4DOS GUI Installer from here: http://www.themudcrab.com/acronis_grub4dos.php. The instructions are pretty good, but in case the web site is down: you use the GUI installer to install the GRUB4DOS boot record and then copy grldr from the grub4dos ZIP file to the root of the USB flash drive, then copy the above code into a file called menu.lst and copy that to the root of the USB flash drive as well, then you should be able to boot from it. Grub4DOS does work with native NTFS partitions: the USB flash drive does NOT need to be FAT32 formatted.

External Hard Drives

Testing was done with external USB hard drives to see if they could be booted from as well. The test system was an Optiplex 390 from Dell. I tried a Seagate 750GB hard drive inserted into a StarTech Unidock. I was not able to boot from this drive. I then tried a WD Passport 1TB USB hard drive and I was able to boot from that, however, with both external drives, the BIOS did not see the external drive during POST until the 2nd warm boot. I started the step from the diskpart script above starting at the select partition step (*I had data on the drive I didn't want wiped*). I was getting a NTLDR error upon boot, so I re-attached the external to the original system (*running Windows 8*) and ran **bootsect /nt60 X:** (*where X: is the external hard drive*) and then it booted fine on the test system.

– Soli Deo Gloria

128GB Flash Drive for \$50

AUGUST 5, 2013

CATEGORIES: MISC

Couldn't resist this deal: <http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=7994250>. It's a 128GB flash drive for \$50 after rebate. 128GB! Looks like it's good until 8/9/13.

– Soli Deo Gloria

VBScript to Replace Text in File

AUGUST 19, 2013

CATEGORIES: MISC, TECH TIPS

Here is simple and elegant VBScript code to replace plain text in a file with one word with another (poached from <http://stackoverflow.com/questions/1975321/find-and-replace-string-in-my-text-with-vbscript>):

```
If WScript.Arguments.Count <> 3 then
```

```
WScript.Echo "usage: Find_And_replace.vbs filename word_to_find replace_with "  
WScript.Quit  
end If
```

```
FindAndReplace WScript.Arguments.Item(0), WScript.Arguments.Item(1),  
WScript.Arguments.Item(2)  
WScript.Echo "Operation Complete"
```

```
function FindAndReplace(strFilename, strFind, strReplace)  
Set inputFile = CreateObject("Scripting.FileSystemObject").OpenTextFile(strFilename,  
1)  
strInputFile = inputFile.ReadAll  
inputFile.Close  
Set inputFile = Nothing  
Set outputFile =  
CreateObject("Scripting.FileSystemObject").OpenTextFile(strFilename,2,true)  
outputFile.Write Replace(strInputFile, strFind, strReplace)  
outputFile.Close  
Set outputFile = Nothing  
end function
```

– Soli Deo Gloria

No Sound in Windows Media Center

AUGUST 24, 2013

CATEGORIES: MISC

This was a puzzler and happened to me at home! When I would boot up Windows Media Center, I no longer was getting any sound in the program (*sound in Windows was working fine however*). No sound in live TV or recorded TV. However, if I opened up a regular video in the Video Library from within WMC, I would get sound! Very odd. Tried a System Restore, but it kept telling me it couldn't restore files from the C: drive. I re-setup the speakers in WMC and re-setup the tuner and still: no sound. I then removed the sound driver and TV tuner driver and let Windows re-detect them and viola: sound was working again!

I love Windows (*not*).

– Soli Deo Gloria

Luser (For Network admins / IT Support in Active Directory environment)

SEPTEMBER 4, 2013

CATEGORIES: TECH TIPS

No, not that [luser](#), but this [luser](#). *LUSER (Lookup User)* is a program that attempts to quickly find a user's hostname and IP address by searching on their Active Directory logon name or display name. Once found, you can perform many pre-defined admin tasks on the target machine. *LUSER* can also perform AD reporting, can quickly list Terminal Services sessions on servers and kill them off if you wish and comes with some handy security and cryptography tools among other things.

Just another way of managing PCs on your network. [AD INFO](#) is another utility that gives you some really cool info about your AD infrastructure.

– Soli Deo Glori

Scary: Windows is Irrelevant or Will Be

SEPTEMBER 5, 2013

CATEGORIES: MISC

Learning Android in a hurry!

[http://winsupersite.com/mobile-devices/microsoft-copying-wrong-company?
utm_source=twitterfeed&utm_medium=twitter](http://winsupersite.com/mobile-devices/microsoft-copying-wrong-company?utm_source=twitterfeed&utm_medium=twitter)

– Soli Deo Gloria

Moving Windows 7 to New Hardware

OCTOBER 1, 2013

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Recently, I was tasked with transporting Windows 7 installed on one piece of hardware to another. Not a trivial matter, considering the driver and activation issues. I used Acronis TrueImage 2013 with the Universal Restore feature to accomplish this task and it worked quite well. I was able to take an installation of Windows 7 x64 installed on a Dell Optiplex 390 and transport it safely to a Dell Latitude e6430. The normal barrier for bringing up Windows on different hardware is usually the mass storage drivers. If we can somehow inject the correct drivers offline, we can get into Windows and load the other drivers on an as needed basis.

I set out to do this for free and found this thread: <http://www.911cd.net/forums//index.php?showtopic=24245>. If the web site is down, you can grab the file from my web site [here](#).

Essentially, this VBScript code does just that by invoking the powers of DISM. The first thing you will need is a Vista or later based WinPE disc. You can do this cheaply by tapping the F8 key and picking "Repair my Computer" and then breaking out to a command line. Or you can use [Liveboot 2012](#) from Wondershare. This program is definitely worth the \$60 for everything that it can do. Here's one cool trick you can do with WinPE (*unrelated to Universal Restores, but cool none-the-less*). Install TightVNC server on a PC. Copy the files `screenshocks32.dll` and `tvnserver.exe` from the Program Files directory to a USB key. Now you can run that executable from within WinPE. A "V" will appear in the taskbar. Right-click this icon, go to properties and set a password. Now you can VNC into your WinPE boot media!

Run **`cscript fix_7hdc.vbs`** from within WinPE. It will ask for the Windows 7 drive: pick C:. It will then ask for the folder containing the mass storage drivers. Drill to that. It will now inject those drivers into the offline Windows 7 install and produce a report afterwards:

```

fic_7hdc-rst0026.tmp.log - Notepad
File Edit Format View Help
Manufacturer: Dell Inc.
Model: Latitude E6430

strTargetDrive:
strSearchFile:
binEnableDrivers: True
binInstallDrivers: True
binRestore: False

strTargetDrive: C:\

Enable mode
load registry file C:\windows\system32\config\SYSTEM

=====
Enable existing Mass Storage drivers in system
=====

PCI\VEN_8086&DEV_282A&SUBSYS_05341028&REV_04\3&11583659&06FA
offline_registry_ccdb: PCI\VEN_8086&DEV_282A&CC_0104 1astorv
loaded_SYSTEM\ControlSet001\Services\iaStorv
Start set 3 change to 0

unload registry file C:\windows\system32\config\SYSTEM
strPNPFolder: F:\e6430.drivers\i6430\win7\x64\storage\H79NK_A01-00
Sub: Install drivers: F:\e6430.drivers\i6430\win7\x64\storage\H79NK_A01-00

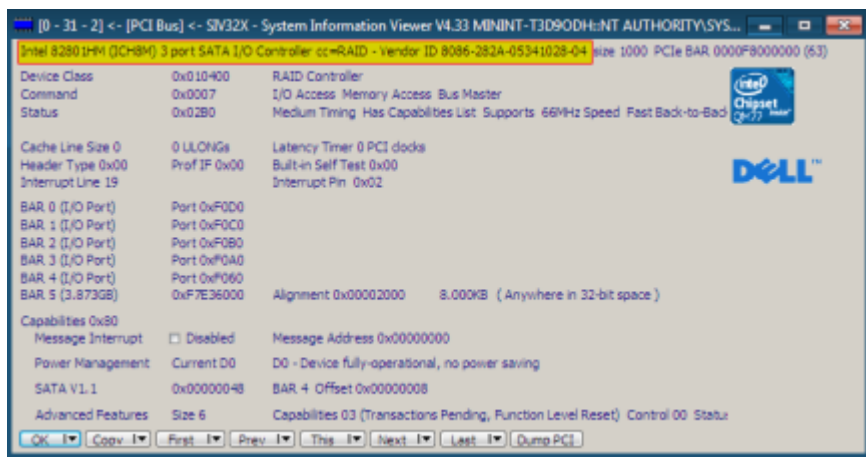
=====
8/19/2013 8:17:09 AM : parse inf files
=====
8/19/2013 8:17:09 AM : Found 0 HWIDs
8/19/2013 8:17:09 AM : Found 0 duplicate HWIDs

=====
Mass Storage Plug and Play Devices in system
=====
PCI\VEN_8086&DEV_282A&SUBSYS_05341028&REV_04
PCI\VEN_8086&DEV_282A&SUBSYS_05341028
PCI\VEN_8086&DEV_282A&CC_010400
PCI\VEN_8086&DEV_282A&CC_0104
PCI\VEN_8086&DEV_282A&REV_04
PCI\VEN_8086&DEV_282A
PCI\CC_010400
PCI\CC_0104

=====
Unique inf files relating Mass Storage IDs
=====
compare setup log file C:\windows\inf\setupapi.offline.log

```

Viola: Universal Restore for free! What if we didn't know what mass storage drivers we need? Well, within WinPE, we can run AIDA64 and click on the PCI Devices tab to get the vendor and device IDs. If you are cheap and don't want to spend the \$40 for AIDA64, you can also use [SIV32](#):



- Soli Deo Gloria

Cleanup Old Hotfixes on Windows 7

OCTOBER 14, 2013

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Disk Cleanup in Windows 7 SP1 now includes an option to clean up old hotfixes: <http://blogs.technet.com/b/askpfplat/archive/2013/10/08/breaking-news-reduce-the-size-of-the-winsxs-directory-and-free-up-disk-space-with-a-new-update-for-windows-7-sp1-clients.aspx>

– Soli Deo Gloria

Windows 8.1 is Out

OCTOBER 20, 2013

CATEGORIES: MISC, OPERATING SYSTEM

Windows 8.1 is out. Big flipping deal! I decided to be risky and updated to 8.1 from 8.0 on Saturday on my home PC. You have to pull the update from Microsoft's App Store. During the setup process, Microsoft now forces you to create an online Microsoft account and associate it with your local Windows profile: how rude! Of course, when the setup was done, I went to the Users Accounts applet in the Control Panel to disconnect it and convert it back to a local account. I know Microsoft really, really, really wants me to put everything in the cloud, but I choose not to. And they really, really, really want me to use their app store for loading applications, but the only app I've loaded is the 8.1 update and that is under duress.

The update torched all VPN software I had loaded requiring an uninstall and reinstall of said software. The update also messed up HyperV...I have two NICs and it appears to have bound the virtual switch to the one not plugged in (*took me a good hour to nail that problem down!*) Then I was getting a LogiLDA.DLL error message on bootup, so I had to go through to the registry and delete all keys relating to this file...something about a Logitech Download Assistant? Classic Shell was borked as well, so I had to load version 4.0 and then I was able to once again not have to look at that evil Metro/Modern UI startup page. I did switch over to Metro to change my login screen wallpaper and then this stupid tip "Switch between apps" kept coming up and blocking part of my screen. It kept telling me to swipe the edge of the screen to dismiss the tip...but I DO NOT HAVE A TOUCHSCREEN MICROSOFT! ARGH! Off to Google to find a fix and this seems to be a common issue: you have to put your mouse in the very left corner of the screen and then the annoying tip screen goes away.

Still not impressed by Windows 8. Please redeem yourself Microsoft! If it wasn't for HyperV, I would be very tempted in going back to Windows 7. Here's another tip: create a shortcut to chrome.exe. Add "-force-desktop" (*without quotes*) to the end of it. Now Chrome won't randomly go into Metro mode on Windows 8.

- Soli Deo Gloria

More Windows 8.1 Torture

OCTOBER 26, 2013

CATEGORIES: OPERATING SYSTEM

I decided to upgrade my Dell e6420 laptop from Windows 8 to 8.1. Upon trying to run the upgrade, it kept telling me I need to remove something called "Dell Data Protection". I removed this from Programs and Features and yet the update kept telling me I needed to remove it. After some Internet searching, I found out if you use this [MrFixIt](#) from MS and remove Dell Access Direct from the list that comes up, that upgrade will then continue.

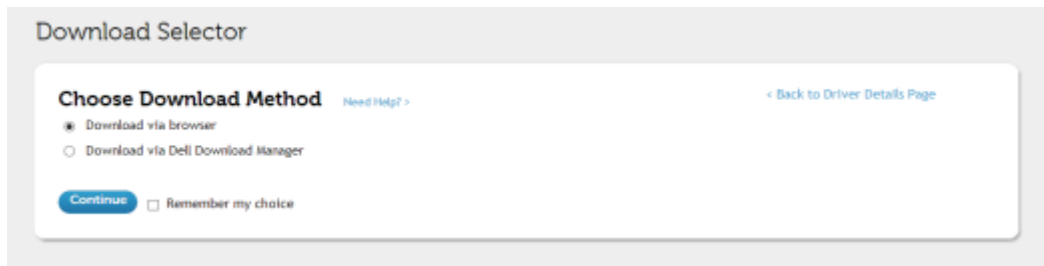
– Soli Deo Gloria

Why Are Downloads So Annoying?

NOVEMBER 9, 2013

CATEGORIES: TECH TIPS

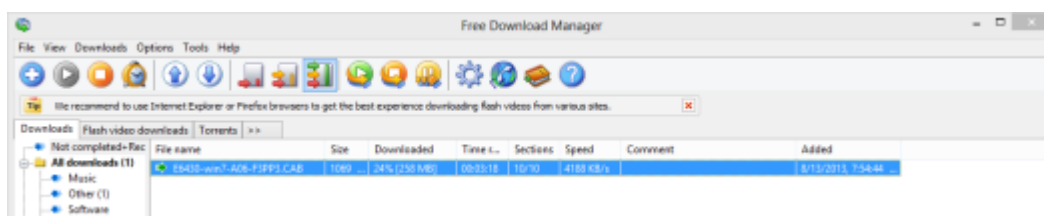
There I was, downloading a 1GB CAB file from Dell's enterprise site. Waited 16 minutes only for the download to end in "Network error". Extremely annoying! As you can see there is no direct link to the file, only 2 lame options:



We can get around this problem by using a really neat (*and free!*) program called [Fiddler](#). It's small and doesn't seem to make drastic changes like installing a capture driver like other "debug" programs. Using Fiddler, we can now clearly see the site and folder structure:

20	304	HTTP	www.google.com	/google/robots.txt	0	private...	chrome...
21	-	HTTP	downloads.dell.com	/FOLDER1505468H1/E6430-win7-A06-F3FP3.CAB	-1		file:56...
22	200	HTTP	www.dell.com	/support/drivers/target.aspx	236	private	text/html; c...
23	-	HTTP	downloads.dell.com	/FOLDER1505468H1/E6430-win7-A06-F3FP3.CAB	-1		chrome...
24	200	HTTP	www.dell.com	/support/drivers/target.aspx	237	private	text/html; c...

Once we get the download path, we can use another awesome free program called the [Free Download Manager](#) to grab the file. This can actually open up multiple connections to the server resulting in a faster download.



Which makes me wonder why not just give me a direct download link in the first place?

– Soli Deo Gloria

ESET NOD32 Antivirus 2014 (3 PC's) FREE + Free Shipping

NOVEMBER 23, 2013

CATEGORIES: MISC

ESET NOD32 Antivirus 2014 (3 PC's) FREE + Free Shipping after rebate. Good until 11/24.

– Soli Deo Gloria

Windows Could Not Finish Configuring the System

DECEMBER 6, 2013

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I was blissfully updating my Windows 7 x64 image and then sysprepped it. Brought it back up on bare metal and then encountered the dreaded “Windows could not Finish Configuring the System” error message. I only ran some Microsoft updates and installed updates for Adobe Flash and VLC...not exactly image breaking stuff and programs I have updated many times before. Now it is the year 2013 and you would think that Microsoft would have developed a bit more graceful way of telling me what the problem is from this screen instead of making me dive into log files in C:windowspanther.

After some searching , I found these steps posted by Jeff Harrision over at <http://social.technet.microsoft.com/Forums/windows/en-US/658528ce-6eb5-403b-ae41-458147c2c044/sysprep-failling-after-reboot-into-oobe>. They have been posted here:

- 1.) *Push Shift+F10 to get to a command prompt*
- 2.) *Navigate to C:windowsPanther*
- 3.) *Find the Setup.etl file and find a way to copy this file off of the system (I copied it to the D: partition and used Ghost to gather that partition and get the file off)*
- 4.) *Copy the setup.etl file from the corrupted system to another computer that has Windows 7. Put it on the root of C: for easiest access.*
- 5.) *Open a Command Prompt on the Windows 7 computer.*
- 6.) *Navigate to the root of C: (or wherever you saved the file)*
- 7.) *Type “tracert setup.etl -o logfile.csv”*
- 8.) *Close the command prompt and open up logfile.csv in your text editor of choice.*
- 9.) *Look through the log file (towards the end probably) for messages that say “Failed to process reg key or one of it’s decendants” For me, the exact error looked like this: “Failed to process reg key or one of its descendants: ” If you search for “reg key” or “failed to process” you should find the failure.*

Surprisingly, the problem was the same exact problem I was having! ESET includes something called Self Defense that “protects” its registry keys from modification. Sysprep tries to modify these keys in some way, fails to do so and then dies. Turning off the Self Defense feature in ESET and then running sysprep fixes the problem.

Of course, Self Defense is a nice feature to thwart viruses, so you can turn it back on after sysprep in 2 ways. First is just to push down a REG file and then import it with regedit /s:

```
Windows Registry Editor Version 5.00
```

```
"SelfdefenceEnabled"=dword:00000001
```

Or just add a custom run command in the MDT task sequencer with this command line:

```
REG ADD "HKLM\SOFTWARE\ESET\ESET SecurityCurrentVersionPlugins1000600Profiles@My profile" /v  
SelfdefenceEnabled /t REG_DWORD /d 0x1 /f
```

Upon the first reboot, Self Defense will be turned back on. Self Defense had been turned on for years and I’m not sure why it is causing a problem now, but it is!

– Soli Deo Gloria

Windows Updates Slow on Windows XP

DECEMBER 17, 2013

CATEGORIES: OPERATING SYSTEM

Thought I was crazy, but it looks like this is widespread: <http://arstechnica.com/information-technology/2013/12/exponential-algorithm-making-windows-xp-miserable-could-be-fixed/>

– Soli Deo Gloria

Fight Club: Me Vs Computer

JANUARY 1, 2014

CATEGORIES: MISC, TECH TIPS

Luck certainly hasn't been on my side lately when it comes to computer problems. I use an old computer as a backup server. I tried turning it on and NOTHING: no lights, no fans, not even a single sound! I proceeded to clear the CMOS with the clear CMOS switch, take out out CMOS battery, check all the connections and I still get nothing. However, there are lights turned on on the motherboard. I also have a little LCD screen connected to it (*it's an Asus Striker II Extreme motherboard*) and on it was blinking the message "CPU INIT". Doing some Internet searching, some people claimed it was a dead CMOS battery. This could be a possibility since I lost all power to the house just a few days before. I went to Walgreens the next day and got a fresh battery and: nothing.

I started yanking things out of the power supply and removing memory modules just to barebones the darn thing and still: nothing. I was ready to throw this PC out, but then I tried one more thing: I removed the USB cable to my KVM switch and the network cable: BINGO! The motherboard screeched to life...and then died. I hooked everything back up and then...she booted! I plugged the USB cable back to my KVM and now the PC is behaving. It was some weird interaction between the KVM switch and the computer.

I then decided to install Virtualbox and a XP VM for testing on the same PC. Upon trying to run Windows update within the VM, SVCHOST.EXE would go to 99% of the CPU and that was it. I used WSUSOffline to download all of the XP updates on another computer and then I ran them within the VM. And then...SVCHOST.EXE went back to 99% CPU. ARGH! If you try to change the interrupt priority, Windows will tell you "ACCESS DENIED" even when you are logged in as an Administrator. This is because SVCHOST.EXE is being run as SYSTEM which has higher privileges than administrator. Simply run **psexec -s -i cmd.exe**. Actually, that should have an extra e at the end, but WordPress has a bug in it and won't let me save the post without giving a 403 error (*I'm submitted the bug to them*).

– Soli Deo Gloria

Start Menu Making a Comeback in 8.1

JANUARY 10, 2014

CATEGORIES: MISC, OPERATING SYSTEM

Yes, Microsoft finally woke up and put the start menu back:

<http://www.winbeta.org/news/mini-start-included-latest-internal-builds-windows-81-update-1>

Should be interesting to see what it looks like.

– Soli Deo Gloria

How to Uninstall Programs in Safe Mode

FEBRUARY 1, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

<http://www.techsupportalert.com/content/how-allow-uninstalling-programs-windows-7-safe-mode.htm>

– Soli Deo Gloria

Fun with Routers

MARCH 2, 2014

CATEGORIES: MISC

Now that I had my cool Nexus 7 tablet, I noticed that streaming video from my Windows 7 HTPC was a bit slow. I had a Linksys WRT54GL running DD-WRT that's been working great for the past 4 years. Unfortunately, it only does B and G bands, so I decided to get a Asus RT-N66U with N band support. It was the big antennas that sold me on it including a "Kickass Award" from Maximum PC. Unfortunately, upon receiving the router, I could not get anything to connect above 54 Mbps. The interface was miserable as well with broken English here and there and DDNS just wouldn't work. Back to Amazon it went. After doing more researching, I decided on the Netgear WNDR3700. It comes with 128MB of flash memory and it has very good DD-WRT support (*the WNDR3400, however, does not*). Flashing it to DD-WRT firmware was a breeze. After getting everything setup, I checked the Nexus 7 only to find it was connected at 65 Mbps. More research lead to me the fact that 65 Mbps is the top speed for this thing as it only has a single channel wireless card.

The PC in the spare bedroom with a USB Medalink wireless stick faired better at 135 Mbps and my laptop does 72 Mbps. So much for the 300 Mbps speed listed on the box :(.

– Soli Deo Gloria

Making CMD More Useful

MARCH 7, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I found this cool program called ConsoleEmu when someone was asking me today about enhancing CMD's features, such as CTRL-C and CTRL-V functionality and this fits the bill quite nicely and is free!

<http://www.hanselman.com/blog/ConEmuTheWindowsTerminalConsolePromptWeveBeenWaiting>

– Soli Deo Gloria

Data Source Names and 64-Bit Operating Systems

MARCH 19, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

To build and run an application as a 32-bit application on a 64-bit operating system, you must create the ODBC data source with the ODBC Administrator in `%windir%\SysWOW64\odbcad32.exe`.

A 64-bit Windows operating system has two `odbcad32.exe` files:

`%SystemRoot%\system32\odbcad32.exe` is used to create and maintain data source names for 64-bit applications.

`%SystemRoot%\SysWOW64\odbcad32.exe` is used to create and maintain data source names for 32-bit applications, including 32-bit applications that run on 64-bit operating systems.

Yes, you read that right: the 32-bit version of the ODBC administrator is in `SysWOW64` and the 64-bit one is in `system32`. The Control Panel gives no indication of a 32-bit version and most applications you are running on 64-bit are likely 32-bit.

Source: <http://technet.microsoft.com/en-us/library/cc645931.aspx>

– Soli Deo Gloria

Sounds from the Past

MARCH 23, 2014

CATEGORIES: MISC

Sounds from the Plus Pack! for Windows 95/98, Windows NT 4, Windows 3.1, 95, 98, and 2000. Great for cell phone notifications! 😊

<http://graywz.deviantart.com/art/Windows-Classic-Sounds-for-XP-183327375>

– Soli Deo Gloria

ESET Installation Ended Prematurely

APRIL 1, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I got this message recently after we were hit by a virus. The only way I could fix it was with a System Restore. Unfortunately, some of the systems did not have System Restore enabled.

Another tech actually figured this out from this posting:

<http://www.wilderssecurity.com/showthread.php?t=314885>

Basically, the virus wipes out the Base Filtering Engine service which disable the web filtering portion of ESET. The resolution is to clean off the virus and then restore this service using the [utility](#) provided by ESET.

– Soli Deo Gloria

SIW Pro for Free – Today Only!

APRIL 3, 2014

CATEGORIES: TECH TIPS

Another system info program for your toolbelt:

<http://www.giveawayoftheday.com/siw-pro/>

– Soli Deo Gloria

Dyn Ends Free Service

APRIL 8, 2014

CATEGORIES: TECH TIPS

Dyn dropped their free service today or will in the next 30 days. I used the DDNS portion since I have a dynamic IP address at home. They want \$25.00/year for this service. No thanks. Head over to www.noip.com and get the same thing for free.

– Soli Deo Gloria

Windows 8 Start Menu Returns in August

APRIL 24, 2014

CATEGORIES: MISC, OPERATING SYSTEM

<http://www.theverge.com/2014/4/23/5643328/windows-8-start-menu-return-in-second-update>

and

Rumor sheds light on Windows 8.2, Windows 9, and Chrome OS-style Windows Cloud:

http://www.winbeta.org/news/rumor-sheds-light-windows-82-windows-9-and-chrome-os-style-windows-cloud?utm_source=dlvr.it&utm_medium=twitter

The Mystery of the Auto Hide Taskbar Setting

MAY 3, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

This shouldn't have been a mystery, but it turned into one! Recently, we pushed out a bunch of Windows 7 x64 kiosk type computers and discovered that we needed to hide the bottom task bar (*it was covering part of the kiosk application*). Unfortunately, we had already locked down the AD account so tight that the user account didn't have access to any control panels. I figured this wasn't a big idea and that this setting was probably controlled by a registry key. Well, it is, but get ready for a bumpy ride! Search around the Internet long enough and you'll get a few answers where this value is stored, but the real answer is that Windows 7 keeps the auto hide taskbar setting

in HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ExplorerStuckRects2. So what the heck is StuckRects2? Well, I found this...a deep dive into this array value: <http://www.dabcc.com/article.aspx?id=9724>. Yup, it's no ordinary value and it controls various other taskbar settings.

I couldn't find any historical reason for the name (*someone e-mail Raymond Chen from Microsoft!*), but my guess is it stands for Stuck Rectangle or that rectangle on the bottom of your screen that won't go away. This should be easy enough: check the box for auto hide taskbar, export StruckRects2 into a REG file and go on our merry way. Well, that didn't work! After several more hours of searching, I found this web site: <http://www.engincapat.com/windows-taskbar-autio-hide-scripts/> and a nice little VBScript file that did work logged in as the user:

```
Option Explicit
Const HKCU = &H80000001
Dim objReg
Set objReg = GetObject("winmgmts:{impersonationLevel=impersonate}rootdefault")
Dim objWMI
Set objWMI = GetObject("winmgmts:{impersonationLevel=impersonate}rootcimv2")
' Adjust the first bit of the taskbar settings
Dim arrVal()
objReg.GetBinaryValue HKCU, "Software\Microsoft\Windows\CurrentVersion\Explorer\StuckRects2"
arrVal(8) = (arrVal(8) AND &h07) OR &h01
objReg.SetBinaryValue HKCU, "Software\Microsoft\Windows\CurrentVersion\Explo
```

```
' Restart Explorer for the settings to take effect.  
Dim objProcess, colProcesses  
Set colProcesses = objWMI.ExecQuery("Select * from Win32_Process Where Name=  
For Each objProcess In colProcesses  
objProcess.Terminate()  
Next
```

The guy actually went through and documented each hex value and what it does. So why does this work and not the REG file export/import? There are two issues that I observed:

1) Explorer does not flush out this setting right away to this registry value. If you make the change and then export it right away, you'll export the same value as if it were unchecked. I actually thought this was a bug in ProcMon since I could see the value being changed in SpyStudio, but not Procmon, but that's because I wasn't waiting long enough for explorer to flush out the value.

2) Even if you import the correct values, the value that was there before is written out by explorer.exe.

The only explanation I can come up with is that there are values in memory that explorer.exe uses and these are read in once at login and wrote out during logoff. The only way to inject the correct value via a non-GUI method is to replace the value, then kill and restart explorer. Explorer.exe will then read in our new value and life is good.

And just for reference: these are the settings for hide and no hide (*note the red values*)...

Hide

Windows Registry Editor Version 5.00

```
"Settings"=hex:28,00,00,00,ff,ff,ff,ff,03,00,00,00,03,00,00,00,3e,00,00,00,1  
00,00,00,00,00,00,00,66,03,00,00,40,06,00,00,84,03,00,00
```

No Hide

Windows Registry Editor Version 5.00

```
"Settings"=hex:28,00,00,00,ff,ff,ff,ff,02,00,00,00,03,00,00,00,3e,00,00,00,1  
00,00,00,00,00,00,00,00,66,03,00,00,40,06,00,00,84,03,00,00
```



- Soli Deo Gloria

Case of the Unexplained – TechEd 2014

MAY 20, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Mark Russinovich's annual "Case of the Unexplained": <http://channel9.msdn.com/Events/TechEd/NorthAmerica/2014/WIN-B354#fbid=>

Very good video series on Windows troubleshooting.

– Soli Deo Gloria

Get The Professional Version of MiniTool Partition Wizard for Free

MAY 21, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Offer good until May 25th:

[http://www.techsupportalert.com/content/get-professional-version-minitool-partition-wizard-free.htm-0?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+gizmosbest+\(Gizmo%27s+Best-ever+Freeware\)](http://www.techsupportalert.com/content/get-professional-version-minitool-partition-wizard-free.htm-0?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+gizmosbest+(Gizmo%27s+Best-ever+Freeware))

– Soli Deo Gloria

Registry Hack Gives Windows XP Five More Years of Updates

MAY 26, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

An interesting registry hack to make XP looked like a POSReady system so it continues to get updates:

<http://www.geek.com/microsoft/registry-hack-gives-windows-xp-five-more-years-of-updates-1594876/>

Code:

```
Windows Registry Editor Version 5.00
```

```
"Installed"=dword:00000001
```

– Soli Deo Gloria

Cannot Delete Folder/Filenames With Names Past 255+ Characters

JUNE 7, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Ugh...did a file backup copy of a PC and it created folders with names past the legal Windows limit of 255+ characters. Windows will happily create these “illegal” folders, but will refuse to remove them. I went on Google and some people are hawking a paid solution for this, but I found Deep Remove which works perfectly and is free. Thanks Deep Remove 😊

<http://deepremove.codeplex.com/releases>

– Soli Deo Gloria

Incidentally, Autologon from Sysinternals suffers the same problem as well. Although not as handy, we can use a REG file that will do the autologin and it will not breaking using the left-shift method:

```
Windows Registry Editor Version 5.00
```

```
"DisableCAD"=dword:00000001  
"AutoAdminLogon"="1"  
"DefaultUserName"="someuser"  
"DefaultDomainName"="somedomain"  
"DefaultPassword"="somepassword"  
"ForceAutoLogon"="1"
```

And to disable it we can do:

```
Windows Registry Editor Version 5.00
```

```
"DisableCAD"=-  
"AutoAdminLogon"=-  
"DefaultUserName"=-  
"DefaultDomainName"=-  
"DefaultPassword"=-  
"ForceAutoLogon"=-
```

Oh and one more note...it appears that Windows is sensitive to upper and lower case. So if you have COMPUTERTNAME and you type in computertname into the REG file it won't work. The case has to match EXACTLY.

- Soli Deo Gloria

Largest collection of FREE Microsoft eBooks ever

JULY 8, 2014

CATEGORIES: MISC, TECH TIPS

You know what to do!

<http://blogs.msdn.com/b/mssmallbiz/archive/2014/07/07/largest-collection-of-free-microsoft-ebooks-ever-including-windows-8-1-windows-8-windows-7-office-2013-office-365-office-2010-sharepoint-2013-dynamics-crm-powershell-exchange-server-lync-2013-system-center-azure-cloud-sql.aspx>

– Soli Deo Gloria

Fastmail.fm: Fall in love with e-mail again

AUGUST 1, 2014

CATEGORIES: REVIEW

My e-mail has been pretty stable. I was using my own domain leinss.com with Tuffmail for the past 9 years. Tuffmail has been rock solid, but has been lacking in infrastructure upgrades.

Recently, I tried changing my password on Tuffmail and had to contact tech support to do so.

The writing was on the wall: it was time to look for alternatives. I copied all my e-mail over to my web host Eleven2. They offer unlimited mailboxes and bandwidth. It was already included in the price I pay for web hosting, so why not? Well, I can tell you why not. First, Eleven2 is a web host and not an e-mail provider. The controls you have over your e-mail are very basic and I got a lot more spam than I did at Tuffmail. I tried to e-mail an ATT e-mail address and it was bounced back: the server my website is on was on some type of blacklist. Then, I couldn't get to Eleven2 at all: they had blacklisted my IP for too many failed IMAP logins (*what?*). Enough was enough: I had to move, AGAIN.

I decided to try Fastmail.fm since it is highly recommended over at www.emailaddresses.com and I have to say: I found my new home! I love the web interface: simple, elegant, clean and functional. Tons of options you can configure...setting up my aliases and rules was a breeze. Discounts for multiple year subscriptions. Clear descriptions on each account level. Oh look: you can import e-mail from another provider! I tried it and it worked flawlessly. Wow, I'm hooked!

Then it was to over to configure Outlook 2013 to work with Fastmail and that's where the trouble started. For some reason, Outlook would show me new mail in Inbox but not any of the subfolders I had created unless I clicked on each folder. Basically, my setup is if you e-mail something@leinss.com, I create a rule for that alias and then move that message into the something folder. It helps route messages into bins for sorting. If someone adds something@leinss.com to a spam list, I can delete and re-create a new alias. I deleted and re-created the account in Outlook several times, toying with settings...no dice.

I went looking on the Internet for a new mail client. Ah, there was Eudora! I had used that for many years back in the 90s. I loaded it and yeah...crash, crash, crash. Tried Operamail and then I tried Mailbird and this program actually worked correctly with IMAP at Fastmail. Mailbird allows you to add up to 3 accounts in the lite version...works naively with Google's calendar...very nice!

It can check all 3 of my accounts and then it places the number of new messages in a little envelope in the taskbar. Goodbye Outlook 2013!

- Soli Deo Gloria

Paragon Rescue Kit 14 Free

AUGUST 12, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Got an e-mail from Paragon this morning about the Windows PE based Paragon Rescue Kit 14 Free: <http://www.paragon-software.com/home/rk-free/>. Decided to take it for a test drive and unfortunately, I am disappointed. First, you cannot install the program without registering. It's free to register to get the codes, but that's a pain! It wanted to use the Windows 8.1 ADK which I downloaded. There's two versions you can build: x86 and x64. I built the x86 version. I booted it and it comes up with a screen with several buttons: backup to virtual disk, postmortem backup, undelete partition, boot corrector, transfer files, load drivers, setup network. You can also do a restore of course. That's it. No file manager, no desktop and...no thanks.

There are better WinPE discs out there such as this one or the ones over at <http://reboot.pro>:

<http://windowsmatters.com/2013/04/30/windows-8-based-pe-boot-disk-with-explorer-shell-and-all-my-favorite-apps/>

– Soli Deo Gloria

Windows 9 Tech Preview Coming in Late September

AUGUST 15, 2014

CATEGORIES: MISC, OPERATING SYSTEM

<http://www.zdnet.com/microsoft-to-deliver-windows-threshold-tech-preview-around-late-september-7000032668/>

– Soli Deo Gloria

Bill Gates Trashed the Charms Bar, Win9 to RTM by end of 2014

AUGUST 23, 2014

CATEGORIES: MISC, OPERATING SYSTEM

http://www.reddit.com/r/windows/comments/2eclyz/updates_on_windows_9_and_windows_81_u

– Soli Deo Gloria

A Weekend with Plex

SEPTEMBER 1, 2014

CATEGORIES: MISC

Finally decided to take the plunge and bought the lifetime subscription for Plex so I could dump all my TV shows into it and stream them to my TV in the living using Chromecast. However, certain TV shows just wouldn't show up and the server log files weren't much help. The issue is that Plex expects to see files in the SXXEXX format, where S is the season and E is the episode number. If your files don't have this format, Plex will refuse to add them properly.

The real bear of course is that you may have many files...thousands of files...that do not fit this format. What's a guy to do? [Filebot](#) to the rescue! Basically: this program looks at each filename trying to determine what TV show it belongs to from an online TV database and then offers to put it in the proper naming format. If the files are missing the TV show name, you can use [Bulk Rename](#) to add the show name to any part of the file en mass. To find out if you are missing any episodes you can use [TV Rename](#).

– Soli Deo Gloria

Giveaway of the Day: XYplorer 14.40

SEPTEMBER 9, 2014

CATEGORIES: TECH TIPS

Very nice filemanager. I own the full version, but this free one is almost as good! Today only.

<http://www.giveawayoftheday.com/xyplorer-14-40/>

– Soli Deo Gloria

Set Folder and Registry Permissions with VBScript

SEPTEMBER 14, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Sample VBScript opens up registry and folder access with write access for the Everyone group:

```
' Create temp file with the script that regini.exe will use
'
set oFSO = CreateObject("Scripting.FileSystemObject")
strFileName = oFSO.GetTempName
set oFile = oFSO.CreateTextFile(strFileName)
oFile.WriteLine "HKEY_LOCAL_MACHINE\Software\TraxStar Technologies LLC\Clien
oFile.Close

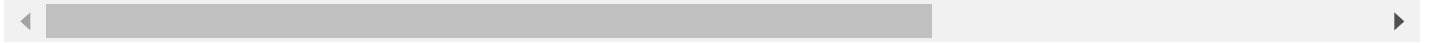
' Change registry permissions with regini.exe
'
set oShell = CreateObject("WScript.Shell")
oShell.Run "regini " & strFileName, 8, true

' Delete temp file
'
oFSO.DeleteFile strFileName

Dim strHomeFolder, strHome, strUser
Dim intRunError, objShell, objFSO

strHomeFolder="C:\Program Files\TraxStar"

Set objShell = CreateObject("Wscript.Shell")
Set objFSO = CreateObject("Scripting.FileSystemObject")
If objFSO.FolderExists(strHomeFolder) Then
intRunError = objShell.Run("%COMSPEC% /c Echo Y| cacls "" & strHomeFolder
End If
```



- Soli Deo Gloria

AutoAdministator: A Nifty Free Remote Management Tool

OCTOBER 1, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

This tip comes from the website 4sysops.com. There is a program called [AutoAdministrator](#) that used to be payware, but is now freeware. This program allows you to drill into your Active Directory structure and check off a bunch of computers for an action. What can you do?

- Password updates
- Remote shutdown / reboot
- Services maintenance
- Registry maintenance
- Network ping
- Remote file management
- Remote file information
- Logged on user information
- Execute processes locally or remotely
- WMI queries
- ODBC maintenance

I used it to select all the computers in an OU and then look at the logged in user to see if the computer description matched up. I was also able to remotely execute programs against multiple computers which is very cool!

– Soli Deo Gloria

Migrating from XP to Windows 7 – Inventory What's There

NOVEMBER 2, 2014

CATEGORIES: OPERATING SYSTEM, TECH TIPS

In the mist of upgrading from Windows XP to Windows 7 on all of our computers, I thought I would share some of the scripts I'm using to make life a little easier. We currently use local user profiles, printers added manually by hand through a Windows print server and sometimes statically mapped network drives for users that need to perform cross duty work in other departments.

Yes, I give you permission to laugh and yes I know there's ways of doing these things in an automated and centralized fashion. Going into the companies we buy, however, I'm seeing even sillier things in their environments. One was a guy that was using Clonezilla, an external hard drive, a USB stick (*at least it wasn't a CD-ROM*) and doing a custom image for each and every model of computer hardware he had. He had an impressive talent for scripting however and I found many clever VBScript snippets all over the network he was firing via the login script to do things automated and in the background.

The below script is quick, dirty and thrown together from many different sources. It will give you:

All the drives and UNC paths mapped under the logged in user's profile

All of the printers networked and local under the logged in user's profile

The default printer of the logged in user

Names of all Outlook profiles of the logged in user (this will error out if this does not exist)

List of unsorted software as given from WMI

Simply call it as the user from the login script and SCCM and dump the file to some where world writable. It will dump the contents in plain text to a file in the format of username.computer.txt.

– Soli Deo Gloria

On Error Resume Next

```
Const HKEY_CURRENT_USER = &H80000001
Const r_ProfilesRoot = "Software\Microsoft\Windows NT\CurrentVersion\Windows Mes

strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
    & "{impersonationLevel=impersonate}!\\" & strComputer & "rootcimv2")
Set colInstalledPrinters = objWMIService.ExecQuery _
    ("Select * from Win32_Printer where Default = True")
For Each objPrinter in colInstalledPrinters
    PrinterDefault=objPrinter.Name
Next

Dim objFileSystem, objOutputFile
Dim strOutputFile

Const OPEN_FILE_FOR_APPENDING = 8

Set objFileSystem = CreateObject("Scripting.FileSystemObject")

Set Shell = CreateObject("WScript.Shell")
Set WshNetwork = WScript.CreateObject("WScript.Network")
Set oDrives = WshNetwork.EnumNetworkDrives
Set oPrinters = WshNetwork.EnumPrinterConnections
oUser = WshNetwork.UserName

computername = Shell.ExpandEnvironmentStrings("%computername%")

strOutputFile="\\someserver\logs" & oUser & "." & computername & ".txt"
Set objOutputFile = objFileSystem.CreateTextFile(strOutputFile, TRUE)

objOutputFile.WriteLine("Network drive mappings:")
For i = 0 to oDrives.Count - 1 Step 2
objOutputFile.WriteLine("Drive " & oDrives.Item(i) & " = " & oDrives.Item(i+
Next
objOutputFile.WriteLine("")
objOutputFile.WriteLine("Network printer mappings:")
For i = 0 to oPrinters.Count - 1 Step 2
```

```
objOutputFile.WriteLine("Port " & oPrinters.Item(i) & " = " & oPrinters.Item
Next

objOutputFile.WriteLine("Default Printer: ") & PrinterDefault

Set oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\" & _
  strComputer & "rootdefault:StdRegProv")

oReg.EnumKey HKEY_CURRENT_USER,r_ProfilesRoot,subKeys

objOutputFile.WriteLine(" ")
objOutputFile.WriteLine("Outlook Profiles: ")

For Each profileName In subKeys
  objOutputFile.WriteLine( profileName )
Next

Set objWMIService = GetObject("winmgmts:{impersonationLevel=impersonate}!\\"
Set colSoftware = objWMIService.ExecQuery ("Select * from Win32_Product")

objOutputFile.WriteLine(" ")
objOutputFile.WriteLine("Installed Software: ")

For Each objSoftware in colSoftware
  objOutputFile.WriteLine objSoftware.Caption & ", " & objSoftware.installDat
Next

objOutputFile.Close

Set objFileSystem = Nothing
```



Case of the Unexplained: 2014

NOVEMBER 3, 2014

CATEGORIES: MISC, TECH TIPS

Mark Russinovich's famous "Case of the Unexplained" for 2014 from TechEd Europe 2014:

<http://channel9.msdn.com/Events/TechEd/Europe/2014/WIN-B410>

– Soli Deo Gloria

Anti-Malware Tools

DECEMBER 3, 2014

CATEGORIES: MISC, TECH TIPS

It's been about 5 years since I posted anything about the tools I use to clean off malware. So, here's my method:

1. Depending on the type of virus involved: I do a system restore to a system restore point to a time before the infection.
2. Run [Hitman Pro](#). This uses a combination of Bitdefender and Kaspersky definitions from the cloud. Note that the free version will not remove the threat if the computer is domain joined, but it will usually show you where the file or registry entry is and you can remove it with another program manually.
3. [Norton Power Eraser](#). This is another cloud based reputation scanner along with the Symantec virus definitions. You do need to be careful with this one as it has a tendency of flagging uncommon/infrequently reported files.
4. [ADWCleaner](#). Generally finds the same files as Hitman Pro, but is completely free and will offer to clean them without asking for money. Do note that it has a tendency to just restart Windows for the cleanup without warning you.
5. [TDSSKiller](#). The "go-to" rootkit remover.
6. [Stinger from McAfee](#). McAfee AV defs in a standalone program.
7. [Sysinternals Suite](#) – Specifically, the tools Process Explorer (*with built-in Virustotal support*) and Autoruns can help identify an infection and remove it.

– Soli Deo Gloria

Backing Up Locked Files

JANUARY 4, 2015

CATEGORIES: UNCATEGORIZED

One of the challenges of migrating someone from one computer to another is the data they may have on the C: drive, especially those evil PST files. The major challenge is backing up locked files. We can get around this by using VSC in Windows. Starting with Windows XP, VSC or Volume Shadow Copy allows Windows to “freeze” the state of the file system in time and then copy files/folder in this frozen state. We will use the freeware program [VSCSC](#) to tap into this power.

First we use [Mapper24](#) to encrypt/hide the credentials for the service account that will connect to our server:

```
mapper24.exe <some encrypted chars> domainusername \serverbackup
```

Next, we make a folder with the name of the computer we are running from:

```
mkdir \serverbackup\%computername%
```

Then we kick off VSCSC:

```
vscsc -exec=wkxp2.cmd C:
```

In wkxp2.cmd, we have this:

```
DOSDEV B: %1
```

```
robocopy "B:\documents and settings\serverbackup\%computername%" /B /MIR /R:0 /XF  
*.ost *.tmp *.bak *.dat *.mp3 /XD "Local Settings" "Temp" "Cookies" "Recent" "Nethood"  
"Printhood" "SentTo" "Start Menu"
```

```
DOSDEV /D B:
```

So here is what we are doing...we are creating a snapshot in time, then we can use any copy program we want to copy files when “time is frozen” within this snapshot. Once we exit the script, VSCSC exits and the snapshot is gone. In the above robocopy script: I am telling it to exclude folders like Local Settings since that is where the internet temporary files are stored.

And yes: this will copy ALL user profiles on the computer to the server, not just the one we want, so you will have to pick through the profiles and grab what you want.

We can log in as the new user on the new computer and just drop in the Desktop, Favorites and My Documents folders manually from the server.

Note that vscsc doesn't seem to work on Windows 7. For Windows 7 you will need to copy Diskshadow from Server 2008 or 2008R2 or as a download from [here: http://jrdudd.org/2010/07/using-backuppc-with-diskshadow-to-backup-open-files/](http://jrdudd.org/2010/07/using-backuppc-with-diskshadow-to-backup-open-files/). Copy the contents of the ZIP file to System32, including the en-US folder or it will not work properly. The concept is pretty much the same:

```
set context persistent nowriters  
set metadata C:\windows\temp\test.cab  
set verbose on  
begin backup  
add volume C: alias C_Drive  
create  
expose %C_Drive% X:  
exec yourbatchfile.cmd  
delete shadows volume C:  
unexpose X:  
end backup
```

Update (12/21/16): As an update to this article, I find that [ShadowSpawn](#) to be superior to the above method and a lot easier. Essentially, it's copy 2 files over and run one command line to copy files. As an example you could do something like:

```
shadowspawn C:\archives X: xcopy X:\*.pst C:\path\to\backup
```

– Soli Deo Gloria

Finding Silent Install Secrets

FEBRUARY 1, 2015

CATEGORIES: MISC, TECH TIPS

We use a program called Velaro chat. I contacted the vendor a few years ago asking for a “quiet installer”. It’s 2015 and you would think that would be standard by now. They do offer MSI files on the side, but they have issues....particularly with some .NET interop assembly file missing.

What to do? First, I tried velaro.exe /?. No dice. Next, I tried strings.exe from Sysinternals. This will give us the plain text strings from the installer:

```

..delete_on_uninstall
You don't have write privilege to directory '%s'. Please have your system administrator (or other user with higher privileges) install this software.
%*%*.tmp
ZERO Decompression error
File size mismatch: this file is corrupted: if you downloaded this file from the internet, try downloading it again
Checksum mismatch. The installation is corrupt or has been tampered with. IF you downloaded this file from the internet, try downloading it again.
Initialization failed. Aborting. Error code: %d
Couldn't read SCC. Aborting.
Copying files. Please wait...
Failed to get
CopyFileExk
-###
The installation was not removed. Do you still want to re-install?
<_Internal_InstallationNotRemoved_>
Couldn't launch installer. Previous installation was not removed!
/silent /quiet /noconsole
%*
Couldn't find uninstaller. Previous installation was not removed!
<_Internal_AlreadyInstalled_>
% is already installed on your system. It is highly recommended to uninstall the application before re-installing. Do you want to uninstall %s before re-installing?
You don't have the required privileges to continue the installation. Please have your system administrator (or some other user with higher privileges) install this software
Couldn't get write access to the "%s" registry key!
<_Internal_HighPrivilege_>
<InstallPermissions>
Supplies initialization failed
ReturnInstaller
ReturnInstaller
-###
%*Property
%*idShow
%*installer
Failed to launch installer. (CreateProcess Failed)
<endwin>
%*%*%*%*%*
D:\Users\%*\Common-1
D:\Program Files\Common Files

```

Ah ha! **/silent**. Why didn’t the vendor clue me in on this? No idea! Fired this through SCCM and it works like a champ, except it throws exit code 1 for some reason, even though it is properly installed.

Nice installer guys! (NOT!). I just fire the install and then check C\$ share for the install bits afterwards. This does saving me time remoting in and manually installing the software.

– Soli Deo Gloria

Windows 10: A Review

MARCH 1, 2015

CATEGORIES: OPERATING SYSTEM, REVIEW

So by now you've heard the news that Windows 10 will be free for Windows 7 and 8 users for the first year. I recently took the plunge and updated my work PC from Windows 8 to Windows 10. The official release is probably about 8 months away, but so far I am liking Windows 10. It fixes a lot of what is wrong with Windows 8, namely it brings back the start menu (*thank you Microsoft*), gets rid of the charms bar in the corners (*thank you Microsoft*) and allows Modern apps to be "windowed" on the desktop (*thank you Microsoft*).

However, all of this stuff should have been in Windows 8 already and yet again we have another Vista on our hands: that is Windows 8. At least Microsoft saw the error of its ways and corrected the ship instead of sinking it. Being able to upgrade your OS with Windows Update is totally cool and long overdue!

Pros:

The search bar in the task bar. If you know what you are looking for, it's a quick way to have it search the whole C drive and bring it up for you. Win.

Notifications icon in the taskbar to get to common settings quickly.

Virtual desktops: yes! One less thing for the Linux boys to rave about.

Cons:

Even though the start menu is back, I miss drilling through a logical folder structure to get to things. I still find myself making a shortcut to C:\ProgramData\Microsoft\Windows\Start Menu on the desktop to get the "old start menu" structure back.

Appears to be missing Windows Media Center...maybe this will come back in a later build?

Task Manager really needs to be replaced with Process Explorer or beefed up. It's essentially a hold over from Windows 8 showing little to no detail on running processes.

– Soli Deo Gloria

Download Windows 7 and 8.1 from Microsoft

MARCH 14, 2015

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Need to rebuild your PC? Now you can re-download Windows 7 and 8.1 from Microsoft, provided you have a serial # for them.

Windows 7:

<http://www.microsoft.com/en-us/software-recovery>

Windows 8.1

<http://windows.microsoft.com/en-us/windows-8/create-reset-refresh-media>

– Soli Deo Gloria

Windows 10: Pushy!

MARCH 27, 2015

CATEGORIES: OPERATING SYSTEM

Been running build 9926 on my PC for a while now. I was in the “Fast” ring and was pushed build 10041 through Windows Update. Rebooted and install would not progress past 8%. It rolled back gracefully to 9926, then I changed the updating to the slow ring. Of course, the SAME build gets pushed to me again. ARGH! This time it goes to 5%. Rollback. The problem is of course you cannot turn off Windows Update in Windows 10 anymore (*probably someone will figure out a way eventually...*) and they kept pushing this same build out to me over and over again. You can suppress the update for 8 hours, but then...BOOM, installing build 10041, fail and rollback again!

Finally, they offered an ISO version of 10041 and I was able to install that just fine...but this does scare me a bit. I get that an update should not be deferred forever, but only 8 hours? It should be days, weeks...not hours.

– Soli Deo Gloria

Data Breach Mania

APRIL 7, 2015

CATEGORIES: MISC, TECH TIPS

In light of the recent ebay databreach, I decided it was finally time for a password manager. I typically use a permutation of about 5 different passwords and sometimes the same password across multiple sites. I'm already up to 21 accounts on various sites: who can remember them all? "To the cloud!" you say...well, I don't trust the cloud. Given that the Adobe cloud service was down for nearly a day and I can't tell what the other guy is doing with my data on the other end, I prefer a more "manual" solution. Enter: Keepass. Keepass keeps all of the passwords in one KDBX file encrypted. No cloud, no man behind the curtain. Keepass will keep working even if the company goes out of business and the source code is completely open.

It gets even better, because there's an Android app that can read and write to KDBX files as well. I have Keepass on an encrypted USB key (*Locker+ G2*) from Kingston for on-the-go situations and on Google Drive so I can get to it from my phone. You can copy and paste the passwords from Keepass into your web browser.

– Soli Deo Gloria

System Info Made Easy

MAY 8, 2015

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Was looking for a way for our end users to quickly and easily determine their system information, such as IP address and their computer's name. Something free, not flashy and not resource intensive. Solution... Systeminfo by

Intelliadmin: <http://www.intelliadmin.com/index.php/2013/05/a-simple-utility-to-help-users-print-system-information/>.

This will place a yellow "star" icon in their task bar and gives information such as LAN IP address, public IP address, computer name and uptime. Hoover over it with your mouse and you get the IP address, computer name and logged in user name. Double-click on it and you get a more detailed description pop-up. One little problem I noticed when I put it in the autostart key under HKLM is that it would populate multiple times as people logged in and out of the computer. To get around this, just run taskkill first to kill anything named systeminfo.exe, then launch systeminfo.exe.

Sample VBScript:

```
Set ws=CreateObject("Wscript.Shell")
ws.Run "taskkill /im systeminfo.exe",0,true
ws.Run chr(34) & "C:\systeminfo.exe" & chr(34) & "/tray /no_exit_menu /no_ur
```

Depending on the speed of the computer, users will notice a black CMD window with cscript on the top during login that will disappear within a few seconds.

– Soli Deo Gloria

Keeping Everything Up-to-date

JUNE 4, 2015

CATEGORIES: TECH TIPS

So how do you keep your installed software up-to-date? In the past I've used Securnia PSI. More recently, Filehippo, but that seems to be more intrusive with ads.

Lately, I've been using the Glarysoft Software updater:

<http://www.glarysoft.com/software-update/>

No frills, no thrills: just scan your system and see what programs are out of date. That's it and it's free.

– Soli Deo Gloria

Dear HP Laserjet 400: I hate you

JULY 1, 2015

CATEGORIES: TECH TIPS

Seriously, HP, what is your problem? Every time I go to install a HP Laserjet 400, it takes 15 minutes or more to install the drivers. Why, why, why? This isn't just isolated to one computer either. Your installer also doesn't like UAC. It doesn't matter if you are an administrator or not: if you login with an account with administrator rights and UAC is turned on (*which is the out of the box default*), it either doesn't find the printer (*web drivers*) or comes up with some bogus error about not being able to create a folder (*built-in drivers*).

You have to login with the local administrator account which has UAC turned off. Seriously? If your installer doesn't work with with UAC, how about detecting that it is turned on and throwing up a reasonable error message with instructions on a work around?

It's 2015...wake the heck up!

– Soli Deo Gloria

Windows 10 is Here!

AUGUST 1, 2015

CATEGORIES: OPERATING SYSTEM, REVIEW, TECH TIPS

Windows 10 has been unleashed on the masses (*67 million as of this posting*). I've been running Windows 10 in its beta form for the past 8 months on my work PC and it's been a bit of a bumpy ride...that's to be expected for beta software. I've upgraded my work PC to 10240 as part of the Windows Insider program about 2 weeks ago and 3 computers at home in the past 48 hours with the following results:

1. Sager Laptop

Clicked upgrade through the notification icon in the taskbar and applied upgrade. Everything came over 100% except my wallpaper. I reformatted a USB flash drive with diskpart and then Windows 10 wouldn't see it anymore, however it could see other USB flash drives just fine. The "bad" USB flash drive works fine on other computers, but no longer on my Windows 10 laptop.

2. Main Rig

Upgrade icon was there, but was not offering the download/install yet. Grabbed the ISO off the Internet and did the installation manually. Wouldn't activate right away. Makes Edge browser the default handler for HTTP links...this browser doesn't support extensions yet and is a bit buggy (*doesn't work properly with the realtor site FlexMLS...Chrome does*). Video driver on my GTX 670 was completely kicked out...had to download a fresh/updated driver directly from NVIDIA.

3. File server

This went fine over RDP using the ISO download from #2 (*wasn't allowing me to pick download/install either*), except RDP doesn't work at the "welcome back" screen. Had to switch over with my KVM and input my password, then RDP flipped on just fine.

Also noticed that the upgrade disables the local Administrator account, so I had to re-enable it again on all computers.

In terms of activation...this much has been confirmed:

If you upgrade an activated copy of Windows 7, Windows 8 or Windows 8.1 to Windows 10, you can wipe the hard drive clean and reinstall Windows 10 and it will find your activation status (*based on MAC and serial # of the computer and possibly other components*). If you spin up a VM with a blank hard drive and install Windows 10: it will NOT activate without a purchased product key. This has been proven by people on Reddit.

A service release (*called SR1*) is due for Windows 10 in 2 weeks to fix some of the bugs.

– Soli Deo Gloria

Moving Windows 7 to New Hardware Part Deux

SEPTEMBER 5, 2015

CATEGORIES: OPERATING SYSTEM, TECH TIPS

You may remember this posting: [Moving Windows 7 to New Hardware](#). I was called out recently to another site for a down PC. A Dell Optiplex 3020 had its power supply blown. I only had a Optiplex 390 at hand to fix the problem, however, upon booting it up with the old hard drive, I would get that wonderful STOP 7B error message. Here's another, perhaps easier method of dealing with this problem: Paragon's Hard Drive Manager 15 Professional. There's a feature in the WinPE bootcd of this suite called "Adaptive Restore". You don't even need to use the backup feature of the suite to use it...just boot to WinPE, pick Adaptive Restore and viola: you will get a booting system.

A description of this process is here: [http://www.paragon-software.com/technologies/components/adaptiverestore/...](http://www.paragon-software.com/technologies/components/adaptiverestore/)

- Change of the Windows kernel settings according to the new configuration. We detect the given hardware profile and automatically install the appropriate Windows HAL and kernel.
- Installation of drivers for boot critical devices. We detect those without drivers and automatically try to install lacking drivers from the built-in Windows repository. If there's no driver in the repository, we prompt the user to set a path to an additional driver repository, strongly recommending not to proceed until all drivers for the found boot critical devices are installed. In case drivers for these devices are installed, but disabled, they will be enabled.
- Installation of drivers for a PS/2 mouse and keyboard. This action will only be accomplished for Windows 2000/XP/Server 2003.
- Installation of drivers for network cards. We detect those without drivers and automatically try to install lacking drivers from the built-in Windows repository. If there's no driver in the repository, we prompt the user to set a path to an additional driver repository.

Quite handy for the \$99 price tag!

– Soli Deo Gloria

Removing Office 2013 Quietly

OCTOBER 4, 2015

CATEGORIES: TECH TIPS

We bought a company that had all kinds of versions of Office 2013 installed...that is it could be Office 2013 Standard, Professional, x64 or x86 versions of these two. Our corporate standard is Office 2010 Professional Plus x86 for various reasons I won't bore you with. Using the program ManagePC, I found this uninstall string remotely:

```
"C:\program files\common files\microsoft shared\office15\office setup  
controller\setup.exe" /uninstall STANDARD /dll OSETUP.DLL"
```

Upon running this, I was getting a GUI dialog box asking "do you really want to uninstall?". Grr!
The only way to do this is with an XML file. Example:

```
<Configuration Product="Standard">
```

```
<Display Level="none" CompletionNotice="no" SuppressModal="yes" AcceptEula="yes" />
```

```
</Configuration>
```

So the new command line becomes:

```
"C:\program files\common files\microsoft shared\office15\office setup  
controller\setup.exe" /uninstall STANDARD /dll OSETUP.DLL /config \  
<path_to_file>SilentUninstallConfigStd.xml
```

However, there could be 4 variations...how to handle this? Well, I cheated. We try all four. 3 will fail, 1 will succeed. So we set the exit code to 0 so SCCM doesn't see a failure:

```
"C:\program files\common files\microsoft shared\office15\office setup  
controller\setup.exe" /uninstall STANDARD /dll OSETUP.DLL /config \  
<path_to_file>SilentUninstallConfigStd.xml
```

```
"C:\program files (x86)\common files\microsoft shared\office15\office setup  
controller\setup.exe" /uninstall STANDARD /dll OSETUP.DLL /config \  
<path_to_file>SilentUninstallConfigStd.xml
```

```
"C:\program files\common files\microsoft shared\office15\office setup  
controller\setup.exe" /uninstall PROPLUS /dll OSETUP.DLL /config \  
<path_to_file>SilentUninstallConfigProPlus.xml
```

```
"C:\program files(x86)\common files\microsoft shared\office15\office setup  
controller\setup.exe" /uninstall PROPLUS /dll OSETUP.DLL /config \  
<path_to_file>SilentUninstallConfigProPlus.xml
```

```
echo %errorlevel%
```

```
exit 0
```

Yes this is a dirty, sloppy, rotten hack! If the Office 2013 uninstall fails, SCCM won't know about it and will report success. I had to go back and setup each Outlook profile again anyways, so this wasn't a really big deal to me.

– Soli Deo Gloria

Adding Fonts As Non-Admin

NOVEMBER 3, 2015

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I've been over the Internet many times over trying to find a free solution to run certain programs as administrator without giving the end user full blown administrator rights. An example of this is adding fonts. This task requires administrator rights to do...but do I really need to give the end user full blown admin rights to add fonts?

The answer is no. Meet: AutoIT. This is free solution that includes a nifty RunAs command. As an example we can do this:

```
RunAs("srvaccount", "your_domain", "Pa$$WORD", 4, "C:\fonts\nexusfont.exe")
```

Then we can compile that into a nice little EXE which hides the command line from the end user and then we give them that EXE: In this example, I'm using NexusFont since it's a free font management solution. NexusFont includes an option to "Copy fonts to system font folder". Since NexusFont is running under an account with Administrator rights, it has no problems doing this.

Make sure you give the end users read and execute only rights to the folder and EXE file so they cannot switch it out with another file.

Also, it is possible to reverse engineer the process if you are sophisticated enough and get the password, so don't use a super sensitive password. Assumption is that normal users aren't going to be that sophisticated and there are probably easier ways of gaining admin rights than reverse engineering executables 😊

– Soli Deo Gloria

PDQDeploy: Installing Software Remotely and Silently

FEBRUARY 9, 2016

CATEGORIES: TECH TIPS

While Microsoft SCCM is nice for deploying software, sometimes you just need a quick and dirty solution for installing simple apps, such as installing Google Chrome, remotely and silently. [PDQDeploy](#) comes to the rescue for this. There are free and pro versions of the software. The free version doesn't include multi-step conditionals or retry-until-online operations, but is otherwise fully functional.

It's so mind numbingly simple too...make a new package, point it to the MSI file, it figures out the command parameters to use itself and then you click save. That's it. You can then target specific computers directly or use a TXT file of computer names.

For programs that are not MSI based: Google's search engine comes to the rescue for us. Internet Explorer 11 upgrade? Sure, here you go: IE11-Windows6.1-x64-en-us.exe /quiet /norestart /update-no. You can even get around the multi-step conditional limitation by creating your own VBScript or Powershell script.

- Soli Deo Gloria

ESET NOD 9 for 2 Computers for 2 years – \$28

APRIL 30, 2016

CATEGORIES: TECH TIPS

This guy is legit!

http://www.ebay.com/usr/7th-mall?_trksid=p2047675.l2559

Heck of a lot cheaper than ESET's own site.

- Soli Deo Gloria

New Web Host and Blog Format

MAY 1, 2016

CATEGORIES: MISC

You might have noticed a change in the blog formatting recently. That's because I went to update one of my older postings and was getting a 403 error message. Eleven2 was my old web host which bought out Sharkspace and to be quite honest: they were a pain in the rear end. Periodically, they were blacklisting my IP address for logging in too many times forcing me to contact their tech support to unblock me. I moved everything over to Hawkhost.

Looking at my web site: I realized that I needed to take down much of what was there since it's mostly stuff I wrote and used in the Windows XP era. In it's place is a simple place holder and this blog is now the main feature of my web site.

-Soli Deo Gloria

Missing Drivers

JUNE 2, 2016

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Missing drivers are the bane of every tech, but I have two solutions for you and they are both free! The first one is called [Driver Solution Pack](#). The second one is [Snappy Driver Installer](#). The cool thing with SDI is that you can set a filter to “drivers not installed”, then you can extract those to a folder and import those into your deployment solution such as MDT for each make/model you have.

Don't forget about [SIV](#) or the System Information Viewer...great program to find information on devices that are missing drivers.

- Soli Deo Gloria

Powershell: Delete an Icon from All User Profiles

JULY 1, 2016

CATEGORIES: POWERSHELL, TECH TIPS

Started to learn Powershell recently and already found something really neat. I'm working on deploying Smartdraw 2016 silently and it loves to put an icon on the desktop of the user that it installing the program, not in C:\users\public\desktop where it belongs. Now, with SCCM, this use to be very tricky, because when running installs they run under the SYSTEM account and not as the logged in user and the native DEL /S command within the native CLI will do it, however, there's no way to specify just one folder to delete from: it will search all folders under all of the user profiles.

Based on a tip from <https://www.sapien.com/blog/2014/10/16/delete-desktop-icons-a-windows-powershell-tip/>, we can do this instead:

```
Remove-Item "C:\users\*\Desktop\smartdraw ci.lnk"
```

which basically just searches the desktop folder of each user profile instead of all folders in each profile and deletes the now defunct Smartdraw CI icon from each desktop folder.

And now instead of looking for the uninstall productcode string to feed to MSIEXEC /x to remove Smartdraw CI: the [PowerShell App Deployment Toolkit](#) includes this nifty cmdlet do all of the heavy leaving all in one line:

```
Remove-MSIApplications -Name 'Smartdraw'
```

- Soli Deo Gloria

Copying Files to Multiple Locations At the Same Time

JULY 14, 2016

CATEGORIES: TECH TIPS

Need to copy a set of files or folders to a bunch of different locations? Try [MultiRobo](#). This is a GUI and multi-threaded version of robocopy. You can even save profiles so if you have copy the same set of files periodically to the same locations, you just open the profile and click Run and away it goes!

Great for copying updated WIMs with MDT.

-Soli Deo Gloria

Get a Windows 10 Activation Ticket

JULY 22, 2016

CATEGORIES: OPERATING SYSTEM, TECH TIPS

The clock is ticking before the Windows 10 free upgrade ends on July 29th. If you are still on Windows 7/8.1 and don't want to upgrade by July 29th, there's still hope!

See the following thread to save your Windows 10 activation ticket/token:

https://www.reddit.com/r/Windows10/comments/3i93mp/no_need_for_a_full_upgrade_to_install

- Soli Deo Gloria

Deploy Infor XA Client with PowerShell

AUGUST 4, 2016

CATEGORIES: POWERSHELL

Here was a fun installer to get working silently. This one uses something called InstallAnywhere. It is a java based installer and if you Google *InstallAnywhere silent*, you will happen upon several command line options. The correct set for this version of the installer (2009 version) can be found [here](#).

Here's the command to install it silently:

```
xaclient_Hgenas400_P36001.exe -i silent
```

We can also record settings into a file and play those back. To record:

```
xaclient_Hgenas400_P36001.exe -r C:\temp\powerlink.properties
```

Finally, we end up with this to install silently:

```
xaclient_Hgenas400_P36001.exe -i silent -f powerlink.properties
```

The installer launches the program at the end: I didn't see any settings to turn that off.

The PowerShell code starts off pretty boring:

```
$p = start-process .\xaclient_Hgenas400_P36001.exe -ArgumentList '-i silent -f  
powerlink.properties' -Wait -Passthru  
icacls *.lnk /grant:r everyone:RX  
copy-item *.lnk -Destination C:\users\public\desktop
```

We kick off the installer, tell PowerShell to wait for the process to end and return an object (-Passthru), grant Everyone read and execute rights to the icon and then copy that icon to the the system shared desktop.

If you execute this code, however, the PowerShell script never progresses. This is because the installer runs the full program as a child process from the installer and until the program is closed, it waits for the installer's termination forever.

The program is Java based and executes two processes: Infor XA Power-Link and javaw. We can create a loop waiting for these two processes, then kill them:

```
Do {  
  
$status = Get-Process -Name "Infor XA Power-link" -ErrorAction SilentlyContinue  
  
If (!$status) {  
Write-Host 'Waiting for process to start' ;  
Start-Sleep -Seconds 2  
}  
  
Else { Write-Host 'Process has started' ;  
$started = $true  
Stop-Process -name "Infor XA Power-Link"  
Stop-Process -name javaw  
}  
  
}  
Until ( $started )
```

I picked 2 seconds to keep checking the process list and not hammer the CPU. So obviously for this to work, we need to remove the -Wait and -Passthru options from Start-Process, but then how do we check if the program installed OK? We can check if the program executable exists and then return the proper exit code:

```
if (Test-Path('C:\infor\ERP XA Client\Infor XA Power-Link.exe')) {  
$LASTEXITCODE = 0  
exit 0  
} #end if  
  
else {  
$LASTEXITCODE = 1  
exit 1  
} #end else
```

Anything other than exit code 0 is usually a failure (*MSIs usually return exit code 3010 to indicate a reboot*).

Using the exit command with a specific number seems to pass the exit code properly back to SCCM. Based on my Google-fu: it's then best to wrap your PowerShell script in a batch file and then fire that from SCCM to get the exit code of any non-native command ran from within a PowerShell script:

```
powershell -executionpolicy bypass -file .\install_powerlink.ps1  
echo %errorlevel%  
exit /b %errorlevel%
```

- Soli Deo Gloria

How To Use Sysinternals Like A Pro

AUGUST 11, 2016

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Nice 10 part series on how to use the Sysinternals

tools: <http://www.howtogeek.com/school/sysinternals-pro/>

- Soli Deo Gloria

Enable Dell TPM Chip with Powershell

OCTOBER 19, 2016

CATEGORIES: POWERSHELL, TECH TIPS

Here's some Powershell code I used to enable the Dell TPM chip with Dell Command. The Get-Laptop function was provided

by <https://blogs.technet.microsoft.com/heyscriptingguy/2010/05/15/hey-scripting-guy-weekend-scripter-how-can-i-use-wmi-to-detect-laptops/>

The -% option (that's dash-dash%) basically just says "Powershell, just pass these arguments along and don't try to interpret them". This functionality requires Powershell v3 or later.

Probably would have been better to use Start-Process and check if the exitcode is not zero.

Note to use Dell Command to turn on the TPM chip you need to set a BIOS password and for 64-bit systems you need to use the 64-bit version of CCTK.

Function Get-Laptop

```
{
Param(
$computer = "localhost"
)
$isLaptop = $false
if(Get-WmiObject -Class win32_systemenclosure -ComputerName $computer |
Where-Object { $_.chassistypes -eq 9 -or $_.chassistypes -eq 10 `
-or $_.chassistypes -eq 14})
{ $isLaptop = $true }
if(Get-WmiObject -Class win32_battery -ComputerName $computer)
{ $isLaptop = $true }
$isLaptop
} # end function Get-Laptop
```

If(get-Laptop) {

```
.\cctk.exe -% -setuppwd=secretpassword
```

```
.\cctk.exe -% -tpm=on -valsetuppwd=secretpassword
```

```
.\cctk.exe -% -tpmactivation=activate -valsetuppwd=secretpassword
```



```
.\cctk.exe -% -tpm  
.\cctk.exe -% -tpmactivation  
.\MbamClientSetup.exe -% /q /acceptEula=Yes  
}
```

```
else { # do nothing }
```

```
}
```

-Soli Deo Gloria

GPO: Enable the Policy to Disable the Setting

DECEMBER 22, 2016

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Got to love Group Policy sometimes. We wanted to disable the setting “Access data sources across domains” under Internet Explorer>Security>Local intranet>Custom Level. So of course we set the GPO “Access data sources across domains” to disabled and ...it doesn't work! Users can still toggle the setting and we are still getting pop-ups in Internet Explorer. The solution?

Enable the policy so you can disable it. Yup! Set it to enabled, then click the dropdown box and pick disabled.

Is this some voodoo Vulcan logic being used here?

– Soli Deo Gloria

PowerShell Code to Replace Plain Text with in a Group of Files

FEBRUARY 3, 2017

CATEGORIES: POWERSHELL, TECH TIPS

Here's some PowerShell code I wrote to replace the license server for Minitab 19:

```
# Ignore errors

$erroractionpreference = 'Continue'

# Change Minitab

$configFiles = Get-ChildItem "C:\ProgramData\Minitab" -filter *.ini -recurse

foreach ($file in $configFiles)
{
    (Get-Content $file.PSPath) |
    Foreach-Object { $_ -replace "XXLIC02", "XXLIC09" } |
    Set-Content $file.PSPath
}
```



– Soli Deo Gloria

Creating an Image of a Computer over the Network

FEBRUARY 11, 2017

CATEGORIES: OPERATING SYSTEM, TECH TIPS

This was unique one. Had a user that kept running out of disk space. Plan was to image her drive to a bigger drive (150GB SATA to 500GB SATA). Problem? She works past 5PM, no upcoming vacation.

DISK2VHD to the rescue! We can use this program to dump a copy of the disk to a VHD file to a network location after hours. Imaging 109GB over a 1 Gigabit network took about 2 hours. Note that Windows 7 can mount VHDs, but not VHDXs. If you are an idiot like me: you can convert a VHDX file back to a VHD file using the command Convert-VHD within PowerShell on Windows 10.

Now we mount the VHD as a drive in Windows using the disk management snap-in (*diskmgmt.msc*). Then I used [AOMEI's Backupper](#) to do a disk to disk clone. The resulting copy needed a partition resize to use all available space on the new disk, so I had to blow away the 300MB Bitlocker partition at the end to expand it in disk management (*we don't use Bitlocker on desktops*).

Pop in it and boom: works!

This also works for P2P conversions. I took a guy from an Optiplex 745 to Optiplex 3020 using the same method. Upon booting Windows, I got the the famous 7B BSOD. I used the P2P adjust feature from [Paragon's Hard Drive Manager 15 Professional](#) and was up and running after adding the correct drivers.

-Soli Deo Gloria

PowerShell Code to Find Default Printer

MARCH 18, 2017

CATEGORIES: POWERSHELL, TECH TIPS

Here's some code to query what computers have a certain default printer with PowerShell:

```
$PrinterNameSeek = "\\XXXXXXXX01\XX_OFFICE_CLR_01"

$DefaultPrinterObject = Get-WmiObject -Query " SELECT * FROM Win32_Printer W
$DefaultPrinterName = $DefaultPrinterObject.Name.ToUpper()

write-host $DefaultPrinterName

if ($DefaultPrinterName -eq $PrinterNameSeek)

{

write-host $env:COMPUTERNAME
write-host $env:username

out-file \\XXXXXX\logs\$($env:COMPUTERNAME).$($env:username).XX_OFFICE_CLR_0

}
```

This will need to be run as the end user to use \$env:username, but if your ExecutionPolicy doesn't allow it, you can remove it.

After running this for a few days: you can do a "dir *.* > list.txt" and then import this into an Excel spreadsheet using the import data from text file feature.

- Soli Deo Gloria

Create a Custom Installer Using Powershell

MAY 2, 2017

CATEGORIES: POWERSHELL, TECH TIPS

We run a program called QATRAX which doesn't come as a MSI file for installing it. The program has many sins: one of them being that it can only be installed to C:\program files\traxstar (it's a x86 program) and it has to have write access to this folder. Attempts to use a re-packager to convert this to a MSI file have failed, because all repackagers detect it should really go in C:\program files (x86), but of course that won't work.

The program was made in the 1990s, so figuring out what files it copies to to system is quite easy. You can use a tracing utility such as Process Monitor to watch for install changes.

```
# copy qatrax support files
copy-item *.dll C:\windows\syswow64 -Force
```

We could add registry entries using Powershell code line-by-line, but doing a registry export to a REG file and then import it is far easier in my opinion.

```
# import qatrax registry settings
regedit /s qatrax.reg
```

One thing to note is that we need to create an uninstall string manually so it shows up in Programs and Features as being installed. This will also report back to WMI that the program is really installed to help with software inventory. You should be able to get this from a system with the software already installed.

```
@=""
"DisplayName"="QATrax"
"UninstallString"="C:\\Program Files\\TraxStar\\uninstall.exe TRAXSTAR"
```

The program also has no native way of switching between dev and prod environments, so I wrote another wrapper that overwrites the values in the registry with certain IP addresses depending on which environment the user wants to be in.

```
# set everyone full-control to traxstar registry key. this is a hack to allow
# switching between dev and prod environments
$acl = Get-Acl 'HKLM:\SOFTWARE\Wow6432Node\TraxStar Technologies LLC'
$rule = New-Object System.Security.AccessControl.RegistryAccessRule
("Everyone","FullControl","Allow")
$acl.SetAccessRule($rule)
$acl | Set-Acl -Path 'HKLM:\SOFTWARE\Wow6432Node\TraxStar Technologies LLC'
```

Make a folder in C:\program files

```
# create install folder (and yes, traxstar has to be in the x64 folder even though
it's
# x86 or it will break
mkdir "C:\program files\traxstar\traxclient"
```

Grant everyone rights to write to this folder

```
# qatrx requires write access to its own folder
icacls 'C:\program files\traxstar\traxclient' /grant:r everyone:f
```

Copy files to C:\program files

```
# copy qatrx files to program install folder
copy-item qatrx.exe "C:\program files\traxstar\traxclient"
copy-item traxlaunch.exe "C:\program files\traxstar\traxclient"
copy-item uninstall.exe "C:\program files\traxstar"
copy-item *.log "C:\program files\traxstar\traxclient"
```

Build out the start menu

```
# create start menu items
mkdir "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\QATrax"
icacls *.lnk /grant:r everyone:RX
copy-item *.lnk "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\QATrax"
```

- Soli Deo Gloria

0x80004005: An error occurred while retrieving policy for this computer

JULY 18, 2017

CATEGORIES: SCCM, TECH TIPS

Started a new job recently and one of the techs was having a problem imaging a laptop with a recently replaced motherboard. We would PXE boot the laptop and then WinPE would bomb out in 10 seconds stating “0x80004005: An error occurred while retrieving policy for this computer”.

Nothing interesting was found on the SCCM side, however when I finally found the SMSTS.LOG in X:\Windows\temp\SMSTSLOG, I didn't even have to open the file to figure out the problem: it was dated 2016! Yup: it was a date and time issue. If your computer skews too far from the current date and time, SCCM won't talk to your computer.

You can use the commands date and time within cmd (*hit the F8 key...you did enable this functionality, right?*) to set the correct date and time.

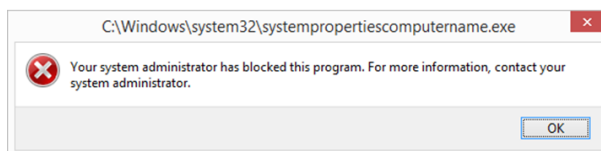
- Soli Deo Gloria

Your System Administrator has blocked this Program

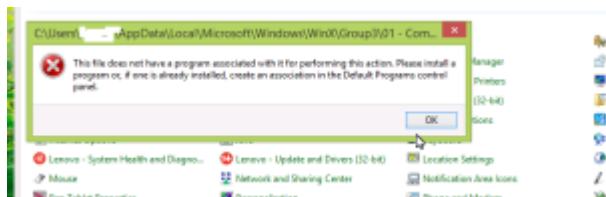
SEPTEMBER 4, 2017

CATEGORIES: OPERATING SYSTEM, TECH TIPS

This was an interesting one. I was converting some computers over from an older domain to a new one and was getting this logged in as a non-admin user when trying to change the domain membership:



Attempts to do a runas on Command Prompt ended up with this even more bizarre error message:



At first I thought it was the OS being corrupted on the computer, but I encountered this error on more and more computers. If I logged in as a user with administrator rights, everything worked fine.

After digging for a while, I figured this had to be a UAC policy as we don't use AppLocker.

The issue: <https://msdn.microsoft.com/en-us/library/cc232762.aspx>

ConsentPromptBehaviorUser

Key: *SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System*

Value: *"ConsentPromptBehaviorUser"*

0x00000000

This option SHOULD be set to ensure that any operation that requires elevation of privilege will

fail as a standard user.

0x00000001

This option SHOULD be set to ensure that a standard user that needs to perform an operation that requires elevation of privilege will be prompted for an administrative user name and password. If the user enters valid credentials, the operation will continue with the applicable privilege.

The previous IT staff (who are no longer here) had set a policy disabling UAC elevation. Doing so causes all kinds of crazy error messages like this one. Why would they do that? Well, the one guess I can come up with is that they didn't want help desk calls from people encountering a UAC prompt. Of course, this also interferes with any IT staff attempting to do any work as all attempts to elevate to admin are blocked.

Some users had admin rights and some didn't...the ones that didn't were the ones where this issue was popping up on. Thankfully, this policy isn't set in the new domain.

- Soli Deo Gloria

Case of the Unexplained 2017

SEPTEMBER 30, 2017

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Case of the unexplained: Windows troubleshooting with Mark Russinovich

<https://youtu.be/qouxznNC2XU>

-Soli Deo Gloria

SCCM Prerequisites Checker

OCTOBER 2, 2017

CATEGORIES: SCCM

This tool will assist administrators in installing all the correct prerequisites for a ConfigMgr (SCCM) hierarchy, different Site Systems Roles and much more:

<https://gallery.technet.microsoft.com/ConfigMgr-2012-R2-e52919cd>

- Soli Deo Gloria

SCCM PKI Fun with Certificates

OCTOBER 9, 2017

CATEGORIES: SCCM

This was fun problem to sort out. I was asked to jump in and fix a SCCM server already built to work with PKI. Attempts to get clients registered with the server would end up with bizarre error messages like this:

```
RegTask: Client is not registered. Sending registration request  
RegTask: Reply for registration was empty. Error: 0x8000ffff
```

I worked on the problem for about 8 hours at work, then went home and setup PKI in my home SCCM lab in about 30 minutes. I decided I needed to enlist Microsoft PSS on this issue.

After working with Microsoft for about 2.5 hours: they tracked the problem to the certificate on the management point bound to IIS being “too new”. Essentially, SCCM has legacy code in it that only understands certificates based on the CSP templates (Windows XP/Server 2003) and not KSP/CNG templates (Windows Server 2008 and later).

This is explained in more detail here:

<https://www.sevecek.com/EnglishPages/Lists/Posts/Post.aspx?ID=66>

The funny part is I was actually using a CA template I had found on the production distribution points that were already up and working, but I guess using the wrong certificate template on DPs doesn't matter, but using the wrong one on the MP does matter for client registration at least!

I had no access to the CA server, so I couldn't snoop around on the properties of said certificate templates and they were named “2012 or later IIS”. Of course the management server is running Windows Server 2012 R2, so why wouldn't I pick that template?

In the end, you have to use the command line to see the cryptographic provider of the certificates (this doesn't show up in the GUI):

```
certutil -repairstore my *
```

```
C:\WINDOWS\system32>certutil -repairstore my *
my "Personal"
===== Certificate 0 =====
Serial Number: 46
Issuer:
NotBefore: 9/26/2017 12:43 PM
NotAfter: 9/26/2018 12:43 PM
Subject: EMPTY <DNS Name="...LOCAL>
Non-root Certificate
Template:
Cert Hash(sha1):
Key Container =
d5b563ce
Unique container name:
5-73fa6f23fa9b
Provider = Microsoft Software Key Storage Provider
Private key is NOT exportable
Encryption test passed

===== Certificate 1 =====
Serial Number:
Issuer:
NotBefore: 9/20/2017 8:56 AM
NotAfter: 9/20/2018 8:56 AM
Subject: CN=...local
Non-root Certificate
Template:
Cert Hash:
Key Con
f23fa9b
Simple container name:
7af44b51ee
Provider = Microsoft RSA SChannel Cryptographic Provider
Private key is NOT exportable
Encryption test passed
```

It seems that other people are annoyed by this and according to Microsoft the ability to use CNG or more “modern” certificate templates is coming in a newer build of SCCM:

<https://configurationmanager.uservoice.com/forums/300492-ideas/suggestions/17451757-support-v3-and-newer-certificate-templates-for-htt>

- Soli Deo Gloria

Update BIOS Using PowerShell and SCCM

JANUARY 20, 2018

CATEGORIES: POWERSHELL, SCCM

<https://github.com/adamleinss/PowerShellBIOSUpdate>

This is a quick and dirty script for PSADT (<http://psappdeploytoolkit.com/>) to deploy BIOS updates relating to Intel's Meltdown/Spectre vulnerability.

PSADT is designed to be used in SCCM deployments, however, it is agnostic enough that it should be able to be used with any software management solution such as PDQ Deploy.

Main drivers in this script:

- Get-WmiObject Win32_ComputerSystem
- Get-WmiObject Win32_BIOS

Using a Lenovo M900 as an example:

```
PS C:\_PUBLIC_REPO> Get-WmiObject Win32_ComputerSystem
```

```
Domain           : XXXXXXXXX
Manufacturer     : LENOVO
Model           : 10FM0026US
Name            : XXXXXXXXX
PrimaryOwnerName : ACME
TotalPhysicalMemory : 8478724096
```

```
PS C:\_PUBLIC_REPO> Get-WmiObject Win32_BIOS
```

```
SMBIOSBIOSVersion : FWKT86A
Manufacturer      : LENOVO
Name             : FWKT86A
```

```
SerialNumber      : XXXXXXXX
Version           : LENOVO - 1860
```

Stepping through the code:

```
$FirmwareUpdateRan = 'FALSE'
```

Set initial status of *\$FirmwareUpdateRan* to FALSE

```
$ComputerModel = (Get-WmiObject Win32_ComputerSystem).Model
```

Set *\$ComputerModel* to 10FM0026US as given for the M900 example above.

```
$BIOSVersion = (Get-WmiObject Win32_BIOS).Name
```

Set *\$BIOSVersion* to FWKT86A as given for the M900 example above.

```
if (($ComputerModel -eq '10FM0026US') -and ($FirmwareUpdateRan -eq 'FALSE') -and ($
```



Once we run one at least one block of firmware update code, *\$FirmwareUpdateRan* will be set to TRUE. Setting this flag will prevent the restart prompt later on if we didn't run any update code. *\$BIOSVersion* should be compared against the version of the BIOS you want to update to. Easiest way of getting this is just running **Get-WmiObject Win32_BIOS** on the test computer after you run the current BIOS update.

```
{ $Response = Show-InstallationPrompt -Message 'Executing BIOS update...please close
'Cancel' -ButtonLeftText 'Continue' -Timeout 600
if ($Response -eq 'Cancel') { exit 12345 }
```




Show a prompt to end user. The majority of the BIOS updates will force a reboot right away without any warning, thus we display a message to the end user and allow them to cancel it.

```
New-Item -Path HKLM:SOFTWARE -Name ACMEDesktop -Force  
Set-ItemProperty -Path HKLM:SOFTWARE\ACMEDesktop -Name MeltdownFirmwareFix -Value "
```



This is useful for satisfying the detection rule for SCCM. There's no clean way of determining whether there is a failure of the BIOS update, other than running a compliancy report in your software/hardware inventory reporting tool to make sure the update happened.

```
set-location $dirfiles\M900
```

Lenovo's flash utility doesn't accept absolute paths: we have to run it from the current directory, so we use set-location to force the location folder.

```
start-process flash.cmd -ArgumentList '/quiet' -Wait -PassThru
```

Run the BIOS update

```
Show-InstallationRestartPrompt -Countdownseconds 600 -CountdownNoHideSeconds 60
```

This is only shown if the BIOS update didn't force a reboot. Currently, I only found the T460S and Yoga S1 laptops do not force a reboot. Since reboot isn't forced, we force one with a 10 minute countdown.

```
Suspend-BitLocker -MountPoint C: -RebootCount 1 -Confirm:$false
```

Suspends BitLocker for one reboot, otherwise laptop will go into recovery mode. Note this command is supported for Windows 8 and later only. For Windows 7 you will need to use `manage-bde: Manage-bde.exe -protectors -disable c:`. I didn't see any `-rc` option, so you will need to do something such as a scheduled task to turn it back on.

- Soli Deo Gloria

Bomb Out Task Sequence if Laptop is Not Connected to Ethernet

FEBRUARY 22, 2018

CATEGORIES: SCCM, TECH TIPS

You would think this would be an easy thing to do in Powershell, but I couldn't find anything. This WMI code will look for an active Ethernet connection and return errorlevel 0 if it finds an active Ethernet connection and 1 if it does not:

```
wmic.exe nic where "NetConnectionStatus=2" get NetConnectionID | find "Ether
```



This has to be put into a batch file and then fired as part of the task sequence.

Why do this? Well, we want to push Windows 10 through Software Center, however, we don't want user's with laptops doing this over the WiFi network.

- Soli Deo Gloria

A Tale of Two Site Codes

MARCH 10, 2018

CATEGORIES: SCCM, TECH TIPS

This was an interesting problem. We are cutting over clients to a new SCCM server with a new site code. Around 100 clients kept going back to the old site code. Peeking in LocationServices.log, it kept saying “Group Policy Registration set site code”. Say what? We don’t have any GPO like that.

After doing some Googling, I stumbled on this

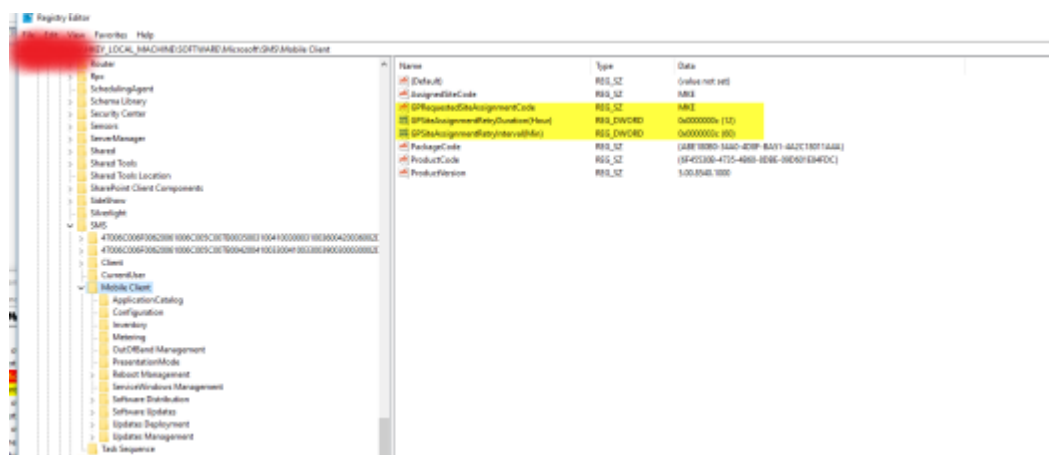
article: <https://henkhoogendoorn.blogspot.com/search/label/GPRequestedSiteAssignmentCode>

and sure enough: GPSiteAssignmentCode was defined! Someone in the past had made a GPO setting the site code, nuked it, but unfortunately it tattooed the computers forever leaving the old site code.

Solution? PSEXEC, a list of computers in computers.txt, Notepad++ (to trim trailing spaces) and reg delete:

reg delete HKEY_LOCAL_MACHINE\Software\Microsoft\SMS /f

Then you can do something like psexec @computers.txt -c ccm.bat where ccm.bat holds your ccmsetup command line.



- Soli Deo Gloria

Dell XPS 13 9350 – The Path to Windows 10

APRIL 24, 2018

CATEGORIES: OPERATING SYSTEM, SCCM

Attempts to do an in-place upgrade on a XPS 13 9350 Windows 8.1 to Windows 10 resulted in lockups around 71%. The issue appears to be the WiFi driver or more specifically BCM.sys. If this driver is removed before the Windows 10 upgrade: the upgrade goes flawlessly.

First step is to get a copy of the Windows Development Kit or WDK from Microsoft to obtain the devcon executable.

Next, go into the device manager and get the VEN/DEV id:

Now we remove it!

```
devcon /r remove "PCI\VEN_8086&DEV_7110"
```

Now proceed on with the rest of your task sequence.

- Soli Deo Gloria

Reset the State of Software Center

MAY 7, 2018

CATEGORIES: SCCM, TECH TIPS

I recently had to pull Firefox out of Software Center and then made a new Firefox application. Both the old Firefox and the new Firefox were listed on a particular machine even though I had retired and deleted the old Firefox application. No matter what I did, the old software persisted! After some reading: it appears that SCCM tracks Software Center events in WMI. Even if you remove and reinstall the SCCM client, the “ghost software” remains. I was able to finally clear off the software icon by doing a complete policy reset using the following WMIC command on the client and then waiting:

```
WMIC /Namespace:\\root\ccm path SMS_Client CALL ResetPolicy 1 /NOINTERACTIVE
```

- Soli Deo Gloria

Get Any Edition of Windows 10 Without Access to VLSC

JUNE 3, 2018

CATEGORIES: TECH TIPS

This is a neat little trick I found on the Internet. If you don't have access to VLSC and still need to get access to the Enterprise or Education editions of Windows 10, you can use the Media Creation Tool to download them.

Run the following.

```
MediaCreationTool1803.exe /Eula Accept /Retail /MediaArch x64 /MediaEdition Enterpr
```

<insert valid Win 10 KMS>. You can find generic KMS keys here: <https://docs.microsoft.com/en-us/windows-server/get-started/kmsclientkeys>

Now you can extract the image you want out of the ESD file as a WIM file. Number 3 is currently the Enterprise SKU:

```
dism /Get-WimInfo /WimFile:install.esd
```

```
dism /export-image /SourceImageFile:install.esd /SourceIndex:3  
/DestinationImageFile:install.wim /Compress:max /CheckIntegrity
```

Remove pid.txt under sources and check licensing status of machine with the following command after installing the OS:

```
slmgr /dli
```

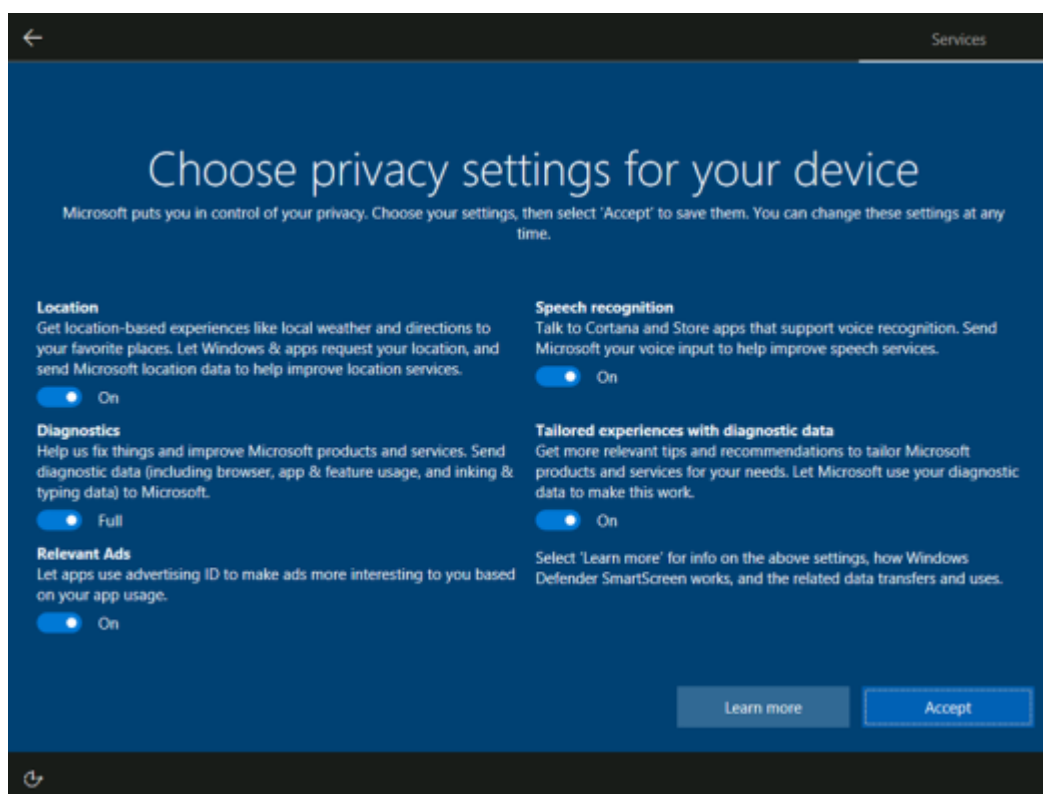
– Soli Deo Gloria

Bypassing Choose Privacy Settings Screen – Windows 10

JUNE 16, 2018

CATEGORIES: OPERATING SYSTEM, TECH TIPS

This was a fun one to track down. When we did in-place upgrades on Windows 8.1 to Windows 10 1703, we never got this “Choose privacy settings for your device” screen. However, going from 8.1 to 1803, this screen will appear once for the first user who logs in with local administrative rights (even though we define certain privacy settings through GPO):



Trying to track this down was hard, but I was inspired by this post on [Reddit](#).

The first stab I tried was logging in as a regular user, running ProcMon and then trying to filter on the registry write operations, but even then, it was too much noise (60K+ events). I then tried another approach. When you click the Accept button, there's a UAC prompt that comes up with a title of "User settings: OOBE". I made note of the word "OOBE" and cancelled it making changes. I ran Process Explorer as admin logged in as a regular user, then switched over to logging in as an administrator until I got the privacy screen, switched back to the regular user

and then did a search for “OOBE” in the process list. One of the processes that came up was svchost.exe and it had the following key open:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\OOBE\Stats
```

I drilled around in this parent key and found this setting:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\OOBE\PrivacyConsentStatus
```

Ah ha! It was set to REG_DWORD 2, so I set it to 1 and tried logging in again as an administrator. No prompt to set privacy settings! I deleted the whole PrivacyConsentStatus key and the prompt still did not show up. I went back and set PrivacyConsentStatus to 2, logged off and back on, privacy settings page showed back up, I clicked the Accept button on the privacy page and then went back to this registry key to see the results. PrivacyConsentStatus was set back to 1 and a new entry called PrivacyConsentSID was created with a REG_SZ value with my user account SID. I deleted PrivacyConsentSID and it seemed to have no effect on the system.

The fix is simple: copy the following into a REG file and then fire it towards the end of OSD

```
Windows Registry Editor Version 5.00
```

```
"PrivacyConsentStatus"=dword:00000001
```

- Soli Deo Gloria

System Center Orchestrator /Operations Manager 2016 & TLS 1.2

DECEMBER 22, 2018

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I deleted and re-wrote this blog post since the other one was out of date. The backstory to this post starts back in July 2018 when we disabled TLS 1.0 across the whole organization. Much fun ensued and we were running around trying to update the SQL native client and other software to get TLS 1.2 compliant. One of the things that stopped working were the integration packs that we installed on System Center Orchestrator (SCORCH).

I opened a premier support case with Microsoft and the first solution was to re-enable FIPS. However, we later found out that enabling FIPS is really re-enabling TLS 1.0. We left the registry entries that disabled TLS 1.0 and the ones that enabled FIPS. The case was left open for Microsoft to figure out how to get TLS 1.2 working. The November 2018 security patches came out from Microsoft and the integration packs on SCORCH broke, AGAIN! Another premier case was opened with Microsoft.

After 2 hours of running Procmon and Wireshark, a solution was found.

Here are the steps you need to take:

On the SCORCH server:

1. Remove the SCOM console (If Any).
2. Uninstall SM and OM integration packs from control panel.
3. Reboot the server.
4. Un-deploy the existing SCOM IP from the designer/runbook servers.
5. Unregister the IP.

6. Download and install the System Center 1801+ – Orchestrator Integration Packs (yes, even for SCORCH 2016!)
7. Re-register the IP and redeploy it (NOTE: Before re-registering the IPs again, make sure that the “Microsoft.EnterpriseManagement.Core.dll” and

“Microsoft.EnterpriseManagement.OperationsManager.dll” are no longer present in either “c:\windows\assembly” or “c:\windows\microsoft.net\assembly\gac_msil”).

8. Re-install SCOM console (be sure to apply latest UR)

Add these registry entries to each SCOM server:

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NETFramework\v2.0.50727"  
/v "SchUseStrongCrypto" /t REG_DWORD /d 00000001 /f
```

```
reg add  
"HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NETFramework\v2.0.50727"  
/v "SchUseStrongCrypto" /t REG_DWORD /d 00000001 /f
```

Add these to each SCORCH server (management/runbook):

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NETFramework\v2.0.50727"  
/v "SystemDefaultTlsVersions" /t REG_DWORD /d 00000001 /f
```

```
reg add  
"HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NETFramework\v2.0.50727"  
/v "SystemDefaultTlsVersions" /t REG_DWORD /d 00000001 /f
```

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NETFramework\v4.0.30319"  
/v "SystemDefaultTlsVersions" /t REG_DWORD /d 00000001 /f
```

```
reg add  
"HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NETFramework\v4.0.30319"  
/v "SystemDefaultTlsVersions" /t REG_DWORD /d 00000001 /f
```

Enjoy TLS 1.2 with SCORCH/SCOM. Note you can check for TLS 1.2 communication by loading Wireshark on the SCORCH management server, then go into the IP pack for SCOM and do a test connection and look for TLS 1.2 in the log.

- Soli Deo Gloria

A Very Powerful Freeware File Manager

NOVEMBER 7, 2019

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I recently stumbled upon [Altap Salamander](#). At work, there is a folder with 13000+ sub-folders (*don't ask*) I have to work with periodically. Using the built-in Windows file explorer won't work due to the [desktop.ini problem](#) where all you see is a bunch of My Documents folders and not a list of username named folders. I frequently use XYplorer for file operations, however, it would lock-up if I went too deep into the folder structure. At that point, I would usually copy and paste the direct folder path into the native Windows file explorer while RDPed into a server to work around the lock-up issue.

The other issue with the native Windows file explorer is the refreshing view glitch. If Windows file explorer detects any change in the folder list it redraws the folder display view and re-enumerates the folder list starting at folder 1. What a pain!

This is where Altap Salamander comes in to help us. It appears it was a piece of freeware that was created in 1997, then it converted into commercial software and just recently was transitioned back to freeware as of July 2019. You can navigate to any UNC path by going to Commands>Change Directory. This file manager correctly displays and handles folders with large numbers of sub-folders. The software has interesting features including being able to calculate folder sizes, batch file renamer, advanced file search (*including filters on size and date*), file type filter view and directory comparison just to name a few. I was able to go to another computer and run it from a remote UNC path, so the program appears to be fully portable and does not require admin installation.

This file manager also lets you see hidden folders that Windows file explorer will hide from you, as I explained in this [2006 blog post](#) and yes, everything I wrote then still holds true today 13 years later (*well, kind of, C:\documents and settings is now C:\users, but you get the point*)

- Soli Deo Gloria

Disabling the “Fix Apps That are Blurry” Prompt in Windows 10

AUGUST 21, 2020

CATEGORIES: OPERATING SYSTEM, TECH TIPS

I was asked to try to suppress this error message popping up on our kiosk display monitors. When Windows 10 detects that a non-optimal display resolution is being used, it offers the end-user some help. I get why Microsoft is doing this: it is in their best interest to try to help the end-user fix problems on their own whenever possible. However, in this case, it's a kiosk computer with no keyboard or mouse. No one will ever be able to answer the prompt and due to the size of the display, it's always going to use a non-optimal display resolution. The prompt doesn't offer an option “Never ask again”. Off to Google, we go!

Well, that wasn't so easy, but I'll get to the punchline and tell you the solution.

```
reg add "HKCU\Control Panel\Desktop" /v IgnorePerProcessSystemDPIToast /t REG_DWORD /d 1 /f
```

That command prevents the “fix the blurry” prompt from ever rearing it's ugly head again. Now the fun part is...where is that documented? It's nowhere documented at Microsoft's site. In fact, go ahead and Google *IgnorePerProcessSystemDPIToast*. You will find very little information on this word. At the time of this posting, that was exactly 7 hits on Google. 7...out of billions of web pages!

One of the more intriguing results was this [web site](#) with a bunch of undocumented hacks for Windows 10.

- Soli Deo Gloria

Windows 95 – 25 Years Later

AUGUST 25, 2020

CATEGORIES: MISC

I wrote this [blog posting](#) 15 years ago celebrating the 10 year anniversary of Windows 95. Now it's 25 years later: wow I'm getting old! If you want to watch the Windows 2000 daily cycle video, you will need to load the [Klite codec pack](#) and use Windows Media Player Classic. The audio really sucks, but you can still make it out. I still run VMWare Workstation with Windows 98 SE on my dad's laptop since he loves to play games from the Windows 3.1 era and EGACHESS. I think EGACHESS is from 1985.

This video by MJD is a nice overview of the Windows 95 development with reviews of preview/beta builds: <https://www.youtube.com/watch?v=sz5pE2muRWI>

- Soli Deo Gloria

Bulk Change LNK (Shortcut) Files

SEPTEMBER 26, 2020

CATEGORIES: POWERSHELL, TECH TIPS

I was transferring department folders and files from one server to another. I used Robocopy and FreeFileSync to get the job done. Just for my own future reference, this was the Robocopy command I used:

```
robocopy \\oldserver\d$\Data\SHARED \\newserver\SHAREDV11 /MIR /COPY:DATSO /DCOPY:DAT  
/R:10 /W:30 /MT:24 /LOG:"D:\transfer\SHAREDV11.log" /TEE
```

I fired this off once, then used FreeFileSync to sync any delta changes afterward. This is pretty boring and common, server administrators have been performing this ritual for many years. However, I've been in desktop engineering for the last 16 years and only 2 years in server administration, so it was "new to me".

Weeks later, after I was done, I got an e-mail about invalid shortcuts. In order to save disk space, the users created shortcuts to other folders. These shortcuts of course included the name of the old server. Off to Google we go! One solution I found was this, but didn't end up using it (our AV software kept deleting it for some reason)

<http://jacquelin.potier.free.fr/ShortcutsSearchAndReplace/>.

Ultimately, I used this code from poster Terrance @

<https://superuser.com/questions/495491/change-shortcut-targets-in-bulk>

```
$oldPrefix = "\\OldServer\Archive\"
```

```
$newPrefix = "\\NewServer\Archive\"
```

```
$searchPath = "Z:\"
```

```
$dryRun = $TRUE
```

```
$shell = new-object -com wscript.shell
```

```
if ( $dryRun ) {
```

```
    write-host "Executing dry run" -foregroundcolor green -backgroundcolor black
```

```
} else {
```



```
    write-host "Executing real run" -foregroundcolor red -backgroundcolor black
}

dir $searchPath -filter *.lnk -recurse | foreach {
    $lnk = $shell.createShortcut( $_.fullname )
    $oldPath= $lnk.targetPath

    $lnkRegex = "^" + ::escape( $oldPrefix )

    if ( $oldPath -match $lnkRegex ) {
        $newPath = $oldPath -replace $lnkRegex, $newPrefix

        write-host "Found: " + $_.fullname -foregroundcolor yellow -backgroundcolor
black
        write-host " Replace: " + $oldPath
        write-host " With:      " + $newPath

        if ( !$dryRun ) {
            $lnk.targetPath = $newPath
            $lnk.Save()
        }
    }
}
```

This works great, it even has a “dryrun” option so you can see what it’s going to do before it actually does anything. The only thing to watch out for is if the shortcut was already invalid to begin with. About 1/3 of the shortcuts the user had were already invalid on the old server due to them shifting and renaming various folders and not updating the shortcuts.

- Soli Deo Gloria

Failed to Apply Cumulative Update on Server 2016

NOVEMBER 3, 2020

CATEGORIES: OPERATING SYSTEM, TECH TIPS

These errors are always fun to track down. Last month, I had a Windows Server 2016 VM that would always roll back the latest cumulative update for the OS. I tried the usual tricks of running `sfc /scannow`, `dism`, safe mode, etc. and nothing worked. I gave up and moved on to something else. Now again this month I had even more servers doing the exact same thing.

After some Googling, I did a deep dive into the logs under `C:\windows\logs\cbs\` and looked for the word “error” around the time I tried applying the update and then found this:

```
Error CSI 000000f5 (F) Failed execution of queue item Installer: HTTP Installer ({86fee01a-954a-11df-bc0c-cea7dfd72085}) with HRESULT HRESULT_FROM_WIN32(1058). Failure will not be ignored: A rollback will be initiated after all the operations in the installer queue are completed; installer is reliable
```

This did ring a bell as months earlier I had found a dev box that would not patch and it ended up that `http.sys` was disabled on that VM as well (*but it was enabled on the prod box???*). The common thread between all 3 VMs was that they were all running Apache Tomcat. The web developer had disabled the `http.sys` driver as this can “hijack” programs from listening on port 80, so to prevent this they just disable it, which also causes PowerShell remote management, printer spooler and branchcache services not to run (because they all rely on the `http.sys` driver running).

The fix is simple: enable the `http.sys` driver, run the patches, then disable `http.sys`:

```
sc qc http
sc config http start= auto
```

After patching we can run these commands to set it back to disabled and restart again:

```
net stop http /y
sc config http start= disabled
sc qc http
```

Let me just rant and say Microsoft does a very poor job of telling us why the patches failed to apply. They don't even give a hint of where to go look for the log files.

- Soli Deo Gloria

Connect To All Office 365 Services Via Powershell With One Script

JANUARY 29, 2021

CATEGORIES: TECH TIPS

Connect to all Office 365 Services PowerShell (Supports MFA too)

- Soli Deo Gloria

Microsoft Updates on Demand

MARCH 19, 2021

CATEGORIES: OPERATING SYSTEM, POWERSHELL, SCCM, TECH TIPS

WSUS and SCCM are great, but maybe you want more control of when Microsoft updates run. There are a few products that can help us with patching: [ABC-Update](#), [BatchPatch](#), [WUInstall](#), and [PSWindowsUpdate](#). I've tried all of these and will give my opinion on each.

The first thing we need to do is setup WinRM for every computer we want to update. This is usually pretty easy: just type **winrm quickconfig** on the computer you want to update. You can also do this through GPO as well:

<https://www.techrepublic.com/article/how-to-enable-powershell-remoting-via-group-policy/>.

This allows remote Powershell access so we can run actions against a list of computers remotely.

The first contender is ABC-Update. I've used this one for a while. It comes in a command line and GUI version and is completely free. There is one downside and that is it requires .NET framework to be installed on the computers it patches, which may not be on all of your servers. The command line is relatively easy to understand:

```
\\vm-acme-01\netlogon\ABC-Update.exe /S:MSUpdate /C:CriticalUpdates,SecurityUpdates  
/A:Install  
/R:3 /MailTo:daboss@acme.com /MailFrom:abc-update@acme.com /MailServ:127.0.0.1
```

We tell ABC-Update to connect to MSUpdate (*not WSUS*), grab only the Critical and Security Microsoft updates, install them, restart up to 3 times and send us an e-mail when it's done. Pretty simple. For the GUI version: you can give it a plain text file of computer names or point it at an AD OU and it spawns a process on each computer PSEXEC style that installs a scheduled task that will fire at the time and date of your choosing. You can watch the update status in real time, cancel the updates and re-schedule them as needed. The author is an IT professional and is very responsive and open to feature requests.

Batchpatch requires PSEXEC from Sysinternals to do it's work. I'll admit I did not spend much time with Batchpatch. There appears to be no easy way of scheduling updates for a certain time/date or to scope update categories to specific ones. Batchpatch is \$399 per year per admin user.

WUinstall is very similar to ABC-Update, however, it only is available as a command line product. The company does have a RMM suite called Xeox that would presumably give you a GUI experience for updating computers if desired. This software is very expensive: to patch 100 clients is \$390/year and it goes up from there. There is a 30 day full version trial.

The command line is very similar to ABC-Update:

```
\\vm-acme-01\netlogon\wuinstall.exe /install /classification update_classification:CS  
/quiet /autoaccepteula /reboot_if_needed_force /bypass_wsus /rebootcycle 3 /logfile  
\\vm-logs-01\logs\%computername%.txt
```

My first trial run of WUInstall ended up with a lot of servers not getting restarted. There are `/reboot_if_needed` and a `/reboot_if_needed_force` command line options. Why there is even a difference, I do not know. WUinstall does not require .NET framework to be installed on the servers it patches, so you will be able to patch servers with less software requirements.

PSWindowsUpdate was used at a previous employer, version 1.5, so I decided to give version 2.2 a spin. This is a free Powershell module and has no .NET framework requirement. I did not want to install this Powershell module on all my servers, so I loaded it on my DC's NETLOGON share and modified `$env:PSModulePath` to include to UNC path to the PSWindowsUpdate module.

This is an abbreviated snippet from the Powershell code, you can find the files over at my [Github](#). KB890830 is the Windows Malicious Software Removal Tool which is generally useless and wastes patching time, so I exclude it to speed up the patching process. I also had to move the source files from the subfolder `\PSWindowsupdate\2.2.02` to just `\PSWindowsupdate` as it couldn't find the files when I tried to load the module.

```
Install-WindowsUpdate -MicrosoftUpdate -Category 'Security Updates', 'Critical  
Updates' -NotKBArticleID KB890830 -AcceptAll -AutoReboot -Verbose | Out-file  
dest:\$computername -Force -Append
```

I use a scheduled task on a server and PSEXEC to kick off the Powershell script to patch servers at 1AM and 3AM after SCCM starts it's patching at 10PM.

```
D:\cron\patchadams\psexec.exe -accepteula -d -s @D:\cron\patchadams\servers.txt \\vm-  
acme-01\netlogon\pspatch.bat
```

My favorite of all of these patching solutions is PSWindowsUpdate, it's free and has very little software requirements, followed by ABC-Update.

- Soli Deo Gloria

Microsoft Updates on Demand – Part Deux

APRIL 2, 2021

CATEGORIES: OPERATING SYSTEM, POWERSHELL, SCCM, TECH TIPS

Now that you found your favorite patching program, we need to send out notifications and target specific servers for patching. I schedule updates as an offset from Patch Tuesday. Patch Tuesday is always the 2nd Tuesday of the month and is when Microsoft releases it's monthly patches. I currently do a pilot group which is fired the night of Patch Tuesday, and then +4, +11 and +18 days after Patch Tuesday, which is every Saturday after Patch Tuesday.

[Send-UpdateNotification2.ps1](#) is a notification script I use with SCCM. This will send out notifications at 8AM on Friday for a maintenance window that takes place Saturday night from 10PM to 5AM. Due to the way the months work, for +18 days after Patch Tuesday, I send these out on Thursdays instead of Fridays as the script doesn't work correctly if the date rolls into the next month. You would run this script as a scheduled task once a day at 8AM. Note that this script needs to run from the SCCM server itself.

If you are using SCCM, you can set maintenance windows based on offsets from Patch Tuesday using [New-CMMaintenanceWindow.ps1](#). This is a Powershell script made by Mattias Benninge. As an example: I run this Powershell script once a year to setup all of my server maintenance windows. This starts the maintenance window every Saturday after Patch Tuesday of the month starting at 10PM going to 5AM Sunday.

```
New-CMMaintenanceWindow.ps1 -SiteCode ABC -MaintenanceWindowName "+4 days after Patch Tuesday weekend" -AddMaintenanceWindowNameMonth -CollectionID "ABC01192" -patchTuesday -adddays 4 -StartYear 2021 -StartHour 22 -StartMinute 0 -HourDuration 7 -MinuteDuration 0 -SWtype Updates
```

```
New-CMMaintenanceWindow.ps1 -SiteCode ABC -MaintenanceWindowName "+11 days after Patch Tuesday weekend" -AddMaintenanceWindowNameMonth -CollectionID "ABC01193" -patchTuesday -adddays 11 -StartYear 2021 -StartHour 22 -StartMinute 0 -HourDuration 7 -MinuteDuration 0 -SWtype Updates
```

```
New-CMMaintenanceWindow.ps1 -SiteCode ABC -MaintenanceWindowName "+18 days after Patch Tuesday weekend" -AddMaintenanceWindowNameMonth -CollectionID "ABC01194" -patchTuesday -adddays 18 -StartYear 2021 -StartHour 22 -StartMinute 0 -HourDuration 7 -MinuteDuration 0 -SWtype Updates
```


[Dump-Computers.ps1](#) is used to dump computers from a SCCM collection into a plain text file. Note that this script needs to run from the SCCM server itself. If you use WSUS & WSUS groups, take a look at [CreateWSUSGroups.ps1](#). This script would need to run from the WSUS server itself.

Once we gather the plain text files with the different computers, we can copy them to servers.txt. [patchtuesday.ps1](#) is a modification of [Send-UpdateNotification2.ps1](#). We use this script to copy our specific group of computers to servers.txt based on the offset from Patch Tuesday. I run this every day as a scheduled task at 8AM. On Sundays, I run a scheduled task at 1AM and 3AM that runs a batch file, but I don't want to run this outside of the maintenance windows above, so I use [patchem.bat](#). The batch file has a "counter file" that increments to 2 when servers.txt and serversplus18.txt are equal. When the counter increments to 2, the batch file will no longer try to patch servers. When the date rolls over to the next month for pilot patching, the counter file is wiped out and the whole process starts over again for that month. The one thing to note is when you run the batch file in the scheduled task, be sure to set the current working directory to the proper folder in the scheduled task, otherwise it will not work properly (*batch files are an ancient technology and assume the current working directory for all operations, if your current working directory is not set to where the batch file is running from, weird things will happen*).

Some servers just refuse to restart on their own after patching, so we can use [restart_sniffer.ps1](#) to nudge them along. This searches servers.txt and then does a restart on a server if it set PendingReboot to True. This script uses [Get-PendingRebootStatus.ps1](#) from TheSystemAdminChannel website. I run this every Sunday at 5AM. Undoubtedly, you'll find servers that did not patch because they ran out of disk space. The "famous" servers for doing this are ones that have the IIS role installed since they like to log every web visit. Take a look at [clean_iis_logs.ps1](#) for how you can keep 14 days of logs and ditch the rest.

The final step is to run a report checking patch compliance. All of this hard work of getting the monthly updates via an API has been done for us already:

<https://sqljana.wordpress.com/2017/08/31/powershell-get-security-updates-list-from-microsoft-by-monthproductkbcve-with-api/> **As an update: the script on this site stopped working in July 2021, so I'm using this file instead:** https://github.com/meta-l/MSSecurityUpdates/blob/master/get_updates.ps1

I uploaded this file as [Get-SecurityUpdate2.ps1](#) to my GitHub. You can ignore instructions for getting your own API key, as it appears that is not necessary anymore. I set the APIKey to 1 and

it still worked, but I went ahead and left the guy's posted APIKey in the code. Note that you will need to install the MSRCSecurityUpdates Powershell module to use this script.

Now you can run `PatchReport.ps1` to parse the results of this months KBs. This will search the patches.txt file looking for CUs and monthly rollups for Windows Server 2012, 2012R2, 2016 and 2019 and then run those results against servers.txt that we generated from the Patch Tuesday Powershell scripts above. I also created `PatchReportSMTP.ps1` to send e-mails of the same report to me.

You can see what CUs are available for this month from <https://portal.msrc.microsoft.com/en-us/security-guidance>.

A sample patch compliance report is shown below. If a row in the column in InstalledBy is empty, that means that server did not restart after patching and is not fully patched (yet).

```
PS C:\WINDOWS\system32> D:\Patching\PatchReportServerPilot.ps1
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Source      Description      HotFixID      InstalledBy      InstalledOn      PSComputerName
-----
021-01      Security Update  KB5000848     NT AUTHORITY\SYSTEM  3/11/2021 12:00:00 AM  021-01
25-01      Security Update  KB5000803     NT AUTHORITY\SYSTEM  3/11/2021 12:00:00 AM  25-01
007-01      Security Update  KB5000848     NT AUTHORITY\SYSTEM  3/10/2021 12:00:00 AM  007-01
019-01      Security Update  KB5000848     NT AUTHORITY\SYSTEM  3/11/2021 12:00:00 AM  019-01
07-01      Security Update  KB5000803     NT AUTHORITY\SYSTEM  3/10/2021 12:00:00 AM  07-01
29-01      Security Update  KB5000803     NT AUTHORITY\SYSTEM  3/10/2021 12:00:00 AM  29-01
```

Any missing patches will show up like this in orange text:

```
VM- Security Update  KB5000803     NT AUTHORITY\SYSTEM  3/14/2021 12:00:00 AM  VM-
VM- Security Update  KB5000848     NT AUTHORITY\SYSTEM  3/14/2021 12:00:00 AM  VM-
VM- Security Update  KB5000822     NT AUTHORITY\SYSTEM  3/10/2021 12:00:00 AM  VM-
VM- Security Update  KB5000848     NT AUTHORITY\SYSTEM  3/14/2021 12:00:00 AM  VM-
VM- Security Update  KB5000822     NT AUTHORITY\SYSTEM  3/12/2021 12:00:00 AM  VM-
WARNING: Patch not found on CS-
```

I commented out the error code about "Cannot connect to computer X", since I run the same script against the same servers.txt file in two different domains without a 2-way trust. About 9 out of 10 times, a failure to patch is a low disk space issue. In a previous [blog posting](#), I talked about how disabling the HTTP.SYS driver blocked patching and the remedy for that, though something like that happening is pretty rare.

- Soli Deo Gloria

Windows 11 Confirmed

JUNE 24, 2021

CATEGORIES: OPERATING SYSTEM, REVIEW

I watched the Windows 11 live stream from Microsoft today. There was a few interesting tidbits, such as it will be free upgrade for Windows 10 users (*not unexpected*), will only come in a 64-bit version (*32-bit version is gone*) and requires UEFI/Secureboot/TPM 2.0. A lot of people are hyperventilating over the TPM 2.0 requirement, but we are roughly 6 months away from the release of Windows 11 and I have no doubt that this requirement will either be relaxed or a workaround will be found.

Installing the leaked Windows 11 dev build was blocked by Microsoft from installing on bare metal and within days, people figured out how to copy all of the files from the Windows 10 sources folder from the install media and then just overwrite the Windows 10 WIM file with the Windows 11 WIM file and viola, all restrictions were removed. The TPM 2.0 requirement was already bypassed for this build by replacing `appraiserres.dll` with one from Windows 10. Heck, `WinNTSetup` will probably have a tick box to just remove the requirement.

The 32-bit version should have been removed a long time ago. If you have something that requires Windows 32-bit (*for the 16-bit subsystem support*), you should probably be running an emulator for that program or leave it on an older OS. The last time I had to install Windows 32-bit was back in June 2014 for a company we bought from Baldor Generators. There was 1 guy that had to run a MS-DOS program and MS-DOS programs only work on Windows 32-bit (*without emulation*), so we had to revert his Windows 64-bit back to Windows 32-bit.

However, if I had to do it over again, I would just run `winevdm` or `DOSBOX` to run his MS-DOS program and leave him on Windows 64-bit. There's even more options such as VMWare Workstation, I think it's finally time to drop MS-DOS support for programs that were created 40 years ago.

- Soli Deo Gloria

Windows 11 Can Wait

OCTOBER 13, 2021

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Windows 11 released to the world last week and as I predicted: the TPM, Secure Boot and CPU requirements can all be bypassed. Depending on how you are trying to install Windows 11, you have several options. If you are trying to do an in-place upgrade from within Windows 10 itself, you can do a Google search for **AllowUpgradesWithUnsupportedTPMOrCPU**. Creating this registry key will cause the Windows 11 setup program to ignore the CPU check and will allow you to proceed with TPM 1.2, however, you still need a TPM chip.

To bypass all requirements, you need to run the Windows 11 install from a bootable USB stick. Copy the following into notepad and save as bypass.reg to the USB stick:

Windows Registry Editor Version 5.00

```
"BypassTPMCheck"=dword:00000001
"BypassSecureBootCheck"=dword:00000001
"BypassRAMCheck"=dword:00000001
"BypassStorageCheck"=dword:00000001
"BypassCPUCheck"=dword:00000001
```

Boot to the Windows 11 setup using the USB stick. During the setup, you will get an error your PC is not supported. Click back to the main screen. At this point, you can hit SHIFT-F10 to get to a CMD prompt, type regedit and then go to File>Import and import bypass.reg above. You can now proceed installing Windows 11.

Techpowerup did a really nice write-up here on the process:

<https://www.techpowerup.com/287584/windows-11-tpm-requirement-bypass-it-in-5-minutes>

Rufus now has a beta version that will create a bootable ISO with all of these restrictions removed called "Windows 11 Extended Support": <https://github.com/pbatard/rufus/releases/>. Note that you can only do clean installs using the bootable USB stick method and the upgrade option does not work from the bootable media.

Update: this now works for in-place upgrades as well!

<https://www.ghacks.net/2022/03/04/rufus-3-18-adds-support-for-windows-11-inplace-upgrade-bypasses/>

I have no plans to move to Windows 11 at this time. In the words of Chris Titus Tech: “you won’t get a lot but you will lose a lot”. Windows 11 has a lot of bugs relating to the taskbar and context menus. Windows 11 to me seems a lot like Windows 8.

- Soli Deo Gloria

50 Life Hacks for Windows in 50 minutes

APRIL 23, 2022

CATEGORIES: OPERATING SYSTEM, TECH TIPS

Very good video on “Windows hacks” from Sami Laiho: <https://mailchi.mp/adminize/win-fu-training-newsletter-54-013x06f2cn>. These tips come from his WinFu Dojo series, which are usually pay per view, but this one is free for everyone.

- Soli Deo Gloria