Bite the ***Big*** Bullet...

072409 - 2000

Laptop got Trojan Horse and Packed It In...

Sooner or later, all PC computer users can face a harsh reality; they get a virus or their hard drive packs it in. I've had both happen; this time it was called a Trojan horse. The suggested solution - reformat the hard drive, reinstall Windows XP, and all your software.

The wary computer user will usually employ a virus checker and a firewall. The virus checker should be up to date and look for any form of virus when you're working on the Internet. The firewall should stop any ardent hacker from accessing your machine. In this case, the firewall was a router on a high-speed commercial Comcast line. And the free AVG virus checker was up to date.

Nevertheless, one day, somehow, in trotted a Trojan horse, taking huge chunks out of the registry (area which knows where everything is located on the computer). Yes, I did try to remove the Trojan horse ~ that's what eventually chewed up the registry. And my laptop bit the dust... out of commission from Sunday through Thursday.

To set the stage, here's the computer information:

Microsoft	Windows XP Professional
Version	5.1.2600 Service Pack 3 Build 2600
OS Manufacturer	Microsoft Corporation
System Manufacturer	Dell Inc.
System Model	Inspiron 1501
Processor	x86 Family 15 Model 104 Stepping 1 AuthenticAMD ~1795 Mhz

BIOS Version/Date	Dell Inc. 2.6.3, 12/7/2007
SMBIOS Version	2.4
Hardware Abstraction Layer	Version = "5.1.2600.5512 (xpsp.080413-2111)"
Total Physical Memory	2,048.00 MB

After serious cogitation, it was decided that we needed to reformat the hard drive, reinstall Windows, then reinstall all software which were tailored for the laptop.

Fortunately, the reinstall preserved some important data on the hard drive; we were able to choose (NAME THAT OPTION) an option which did not require reformatting. Unfortunately, the reinstall forgot to put any drivers between Windows XP and video, audio, ethernet, network connectors, or wireless connector.

Oops ~ What DO I Do Now?

First Option - your computer's under warranty, you call Dell support, and India (***inja***…) answers. They take control of your computer, reinstall Windows, supply all drivers, and, hopefully, things work out rather smoothly.

Second Option - you ditch the old machine, buy a new, current computer, install your software, and live happily ever after (yes, I agree - this last remark is a little tongue-in-cheek!).

Last Option - you know just enough to get in trouble, you decide to do it yourself, and many, many hours if not days later, you get a running machine. I took the road less traveled; with Larry Stroup's remarkable help, I looked up all the CDs and DVDs containing original software, serial numbers, and began this laborious process.

Day 1 – 17 July – Get a 'New' Windows Running, Then Upgrade

Last Thursday morning, reconstruction began. Reinstall Windows XP – Install the latest Firefox browser to do other simple processes. Reinstall AVG Free (which let in the original Trojan horse) to protect from virus corruption. Reinstall PDFCreator 0.9.8 and Adobe Reader 9.

Backup important data recovered by reinstall.

Use MS Update through Internet Explorer 6 to download all upgrades since 2006 (try this little number on dial-up). Always run MS Update several times to assure you've completed all downloads.

Larry showed me suppor.dell.com – then downloaded some 15 drivers.

I tried to use Dell's CD Resource Disk for drivers…

*It was never **any** help!*

Day 2 - 18 July – Get Office and Dragon Talking Together

Reinstall Microsoft Office (I use Word and Excel a lot).

Reinstall Dragon NaturallySpeaking 9 so I can continue blogging with ease. Activate both. And there lay the tip of an *enormous* iceberg; DNS 9 promptly wanted to begin listening for dictation. Unfortunately, there was no audio driver; DNS 9 doesn't work without audio.

Something's wrong here...

Activate network and synchronize workgroups for studio and laptop LAN.

Ahh - now the laptop and audio talk again!

Check out Word and Excel, pursuing normal business of the day put aside by this prodigious outlay of energy, to get the laptop working; oops, each time you try to use either, it goes through a short, unnecessary Windows Install phase, then finally loads the software. *Something's also wrong here…*

Day 3 - 19 July – Update Office Upgrade

Microsoft Windows Update now works both for Windows and for Office.

When I ran Windows update, 150 mb of Office updates occurred.

Yet, individually, Word and Excel still wanted Windows Install.

For many years now, I've enjoyed the privilege of putting a picture in Word, donning a microphone headset, and as I talk, watching words flow around the picture to describe the remarkable poetry of enchanting landscapes.

Unfortunately, at this stage of rebuild, each time I opened Word it would ask for a Windows install. The computer would go away briefly. When it came back, Windows was on screen.

The same thing was true for Excel; something must be done so Office would quickly come on screen as my main work horse.

Although the software reinstall was from an old CD, usually, software is dated. That's to say, since software is continually improving, when you have a CD of a release, it's only up through that release date.

So, although I had run Windows update and 150 MB of Office upgrades occurred, it was time to run update again and again until no more updates could be found. After another 14 MB, when I tried Word, it instantly sprang to life!

One big hurdle overcome...

Yet, let's recall *'Something's Wrong Here...'*

DNS 9 couldn't find a sound card.

A PC is put together in layers; there's the hardware and there's the software. Between the two, drivers connect hardware and software.

Somehow, in the reinstall, drivers were simply ignored.

How do you decide what drivers are needed?

1. Usually, for Dell computers, you insert a CD called Resources. The drivers are own that CD.
2. If you're under warranty, you call India, and a technician helps you through the process (maybe…).
3. If you know what the hardware is, say a sound card, you put the computer name and the sound card name in Google and look it up.
4. Or, if you're familiar with Dell, you log on to support.dell.com, supply a service tag ID attached to the base of the laptop, then begin to ask just which Dell drivers are relevant. This is far the easier…

When I got the virus, the warranty had expired, it would turn out that the resources CD wasn't helpful, Google searches make you wade through a lot of shit, and for the poorly informed, support.dell.com has most of the drivers.

Right click on My Computer> Manage> Device Manager and examine the list to see if you have yellow question marks, yellow exclamation points, or any other colored indication that your software and hardware have missing driver links.

At this point, our Device Manager shows 6 Other Problems.

Notebook System Software
Chipset
SMBus
Audio
Video
Network Controller

So, we make a careful Excel list of what we think are potential drivers to fix each of these problems.

		Function	*Version*	*Driver#*	*OEM*
Network					
Sys	1	SysUtil	4.8.0, A24	r134838	Notebook sys software
Chipset	2	chipset	5.10.1000.7, A00	r134875	SMBus/ChipsetDriver
Video	3	Video	8.31 XP WHQL…	r168684	ATI Driver IGP Xpress 1150
NIC	4	Network	v4.60, A02	r149798	driver
Audio	5	Audio	5.10.0.5515…	r171789	Sigmatel STAC 92XX C-MAJOR HD AUDIO
Modem	6	Comm	Drv7.38.0xp, A05	r114200	Conexant D110 HAD MDC v92 modem
Wireless					
NIC	7	Network	4.100.15.5	*r151517*	wireless LAN
Touchpad	8	Input Device	8.2.4.6, A17	r120179	Synoptics yada yada

r151517 – Oops, it doesn't work

Day 4 - 20 July – Get Software Drivers for Audio, Video, Ethernet, etc

Unfortunately, Microsoft and Dell use different terminology for a separate function. This requires the user to put together complex matrices, download the drivers, then through a deductive process of elimination, see which driver solves which problem!

The Device Manager indicated audio, video, ethernet, and wireless were also missing... we could remember an ATI video card, Sigmatel audio, but didn't know a lot about other hardware providers.

Dell has a list of OEM drivers for each service tag at support.dell.com. Each dell laptop as a service tag pasted to its base. The list initially shows 15 drivers but can be expanded to 41. In addition, Dell has a white paper suggesting the preferred order in which you install drivers.

In the case of an audio driver, Dell described it as Optional. They had categories of optional, recommended, and urgent.

Function		*Date*	*Version*	*Driver#*	*OEM*
Audio	o	12/4/2007	5.10.0.5515…	r171789	Sigmatel STAC 92XX C-MAJOR HD AUDIO

In English, the audio driver was created on 4 December, 2007, it's version 5.10.0.5515, it's made by Sigmatel, and Sigmatel's driver is r171789. r171789.exe is really an executable file which will install the driver so software can talk to Windows and make the sound card function. Simply click the executable then restart the machine when the install is done. Check the Sound and Video Controller in the Device Manager to see if Windows tells you the install was okay.

Yep, SigmaTel High Definition Audio CODEC showed up...

With that vital step done, we started DNS 9 and calibrated the sound by reading Kennedy's Inaugural address aloud.

Nothings wrong here...

But, this step sent us off on a wild goose chase for 5 missing drivers

Here's the deductive algorithm you use to clean up the driver problems…

1. Guess which downloads might be the answer
2. Download
3. Place in specific order
    a. Dell has paper on what order to install drivers
4. Click executables
5. Restart after each install
6. See which Problem is solved
7. REPEAT UNTIL ALL DONE

When done, we had installed the following drivers:

Network
Bios

video	ATI
network	Broadcom 10/100 ethernet
modem	Conexant v. 92
wireless	Dell Wireless WLAN
FN+F2	Quickset - BATTERY METER
audio	Sigmatel
touchpad	Synaptics Touchpad

Unfortunately, we have YET to find the right driver for Network Controller – which we think has to do with wireless LAN.

Options:

1. Call Dell India (if you have a warranty)
2. Exhaust meager support.dell.com and Dell.Community resources
    a. Fixed 5 of 6
3. Begin extended Google search
    a. Mostly crap
        i. People tell you of drivers for their PC, not yours!
        ii. Or, they just don't know what they're talking about.

iii. Or, nobody gives them a clean answer.

b. Be careful to use communities where experienced MSCEs (Microsoft Certified System Engineers) talk

When the dust cleared, we'd repaired five problems and the computer was running efficiently. Alas, the Network Controllers problem is still around...

We went into the control panel, click the power button, and made sure that when you shut the laptop lid, the laptop would hibernate.

But, beside the pesky network controllers problem, AVG had been warning us that we had a problem; we still had a virus!

So, we ran a full virus scan, located several Trojan horses, and put them in AVG's virus vault. AVG found virus Downloader.DELF.CVG

We then ran another virus scan which suggested that our Windows reinstall, Office and Dragon upgrade, and various settings had this computer back in a semi-normal state.

When this scan showed no errors, we *thought* we were home free...

*Day 5 - 21 July – Clean PC of Trojan Horse Virus ~ **AGAIN***

We don't normally scan a computer daily. When we reinstalled AVG, we forgot to turn off the scan daily default. While we were running an errand, AVG came up and began another scan... *in short English, it found another damn virus!*

So here we are, we have a running computer but it still has a virus on it. Not only that, we've not had to deal with viruses before this. Or, we're just too damn old to remember most of that stuff!

Back to the salt mines to collect AVG problems, look at their forum, and decide what to do next...

At day's end, we'd run 2 consecutive clean virus checks... *maybe, just maybe this catastrophe is close to an end!*

Update 072209

We have run 3 additional virus scans with AVG with the following results:

	Date	*Time*	*Result*
1.	072109	1436	0 infected files 5 warnings

2. 072109 2144 0 infected files 0 warnings
3. 072209 1216 0 infected files 0 warnings

Warnings were from cookies attained the last time the laptop was connected to the Internet. No virus was found. All scans performed with Virus DB 270.13.22/2253.

AVG Free

When I told some friends about my dilemma, one of whom has had trouble with AVG, the suggestion was that I switch to another free virus checker.

In Microsoft's litany, Windows XP, Windows Vista, and Windows 7 have considered AVG a prime OEM supplier of virus software.

My own practice - upgrade for *latest* virus database ***before*** downloading anything from the Internet.

Day 7a – 23 July – Virus Free

Downloaded latest AVG virus database 270.13.22/2256 to perform final Trojan horse check

4. 072309 1415 0 infected files 2 warnings

This computer is declared Virus Free – Thanks to AVG…

Day 7b – 23 July – Backup & Compacting HD Files

One reason to reinstall rather than reformat was to recover the laptop's Active Desktop. Some 5 GB of video, 8 GB of individual Photoshop workups, and 3 GB of general files were on the laptop at the time of the crash.

After carefully comparing files with the backup hard drive across the network, many files have been removed from the laptop. Although it's my pattern to regularly back up, I was checking to see that the latest file in each category and folder were indeed on the backup hard drive.

When that job's done, you're left with gaping holes across the hard drive between safe segments. You also have fragments of individual files.

To defragment the hard drive, I used Windows Disk Defragmenter.

1. First, it puts fragmentary files together.
2. Second, it compacts the file structure on the hard drive.

All this is in preparation to reinstalling all Photoshop software to get this machine back to being a professional photographer's delight - an enthusiastic wilderness traveling companion.

Day 8 – 24 July ~ Re-Install Photoshop

Installing Photoshop represents a different set of requirements than hooking up drivers. Adobe has been working on Photoshop for 20 years. When you buy the first full copy of Photoshop, then try to economize by buying subsequent upgrades, reinstalls can become an interesting and lengthy problem.

Photoshop	Adobe Camera Raw	Format
CS2	3.7	Full-CD
CS3	4.6	Upgrade-downloaded executable
CS4	5.4	Upgrade-DVD
Lightroom 2.4	5.4	Upgrade-downloaded executable

My first Photoshop was CS2. With serial number prominently displayed, I put the CD in the laptop's DVD reader and began the install. In some 30 minutes, CS2 was installed and activated on the Internet. At this point, it's a matter of clicking the help menu and asking if there are updates. The CS3 upgrade was an executable I downloaded two years ago; clicking on this executable installed a folder on the desktop which contained necessary files for the installation. When I opened that folder, it was a simple matter of clicking on setup.exe to install CS3. Updates were downloaded and installed.

The CS4 upgrade was a DVD bought this year. The laptop's reader promptly began the install. Thinking I was smart, I tried to only do a partial install; CS4 promptly gave me the bird - they install *everything*. I used the control panels add and remove software to clean the machine. The next install I let CS4 do its own thing. Once again updates from the Help folder installed remaining software.

For several releases now, Photoshop has been working around a kernel called Adobe Camera Raw. ACR is a facility which includes both new cameras and updates to new software or software improvements between major upgrades. The CS4 on the upgrade had 5.0 for its ACR. The latest ACR is 5.4. 5.4 can be downloaded from Adobe as a separate file. It's installed at:

After ACR was installed in CS4, it was time to install Lightroom. While ACR is separate from CS4, at Lightroom 2.3, ACR 5.3 was incorporated. From the experience of the CS3 installation, I wondered,

"Can I simply click on the executable, install Lightroom 2.4 and Adobe Camera Raw 5.4, supply the serial number for Lightroom 2, and be done with it?"

The answer... yes! And Lightroom was quickly installed...

Please don't presume that this is all there is to it... Photoshop CS4 and Lightroom 2.4 are very complex pieces of software. Presets, camera profiles, preferences, actions... just a few of the buzzwords for tailoring this photography environment to both suit your learning curve and speed up your workflow.

Closure

At completion of this process, it was time to *curry* the hard drive one last time.

1. De fragment the hard drive once more.
2. Install and run Registry Booster.
    a. 271 errors corrected in the registry
    b. Registry defragmented
3. Setup Windows Restore
    a. With Windows Restore turned on, maybe we would have never had this mess in the first place...

"By the seventh day, God had finished the work he'd been doing; so on the seventh day he rested from all his work." Genesis 2:2

What was God doing? Creating our universe...

Well, re-creating this universe took me 8 days so I guess it's pretty obvious ~ I'm not God!

But, I *have* re-created my own much smaller universe...

If there is no further virus contamination, we are in a position to focus on the final driver need – hooking up WiFi.