Advanced PC Troubleshooting – Techniques, Tips, Tools, and Tricks

Introduction

This booklet is a spinoff of the workbook used in the Virus Remediation Training workshops, offered by The Virus Doctor™. While most of the items presented here may play a role in cleaning malware from an infected computer, they more generally fall into the category of "random troubleshooting techniques."

This information is intended to be used by experienced and knowledgeable computer technicians. The author assumes no responsibility for any unintended consequences of following the procedures contained herein.

As always, you should make sure that you have a way to Undo anything you might Do with these techniques, tips, tools, and tricks. If you discover any inaccuracies in this booklet, please report them to kdwight@thevirusdoc.com.

If you have suggestions for additional items you believe would be appropriate to include in future editions of this publication, you are invited to submit them to kdwight@thevirusdoc.com. Your suggestions are welcome, and all submissions will be acknowledged.

If you are interested in attending a Virus Remediation Training workshop, you can find more details here: http://www.thevirusdoc.com/virus-remediation-training. These workshops are presented on a regular basis, both in a public format and on-site for those organizations with at least 5 techs who need the training.

The public workshops are presented in-person at various locations, or online for your convenience. You will find the current schedule on the web site shown above. If you would like to discuss or schedule an on-site workshop at your location, please contact kdwight@thevirusdoc.com.

Table of Contents

1. **F8 doesn't take you to Boot Menu on a Windows XP computer**

   If you are unable to access the Boot Menu by hitting F8 at startup time, the most likely cause is a new keyboard that is different from the one that originally came with that computer. If the computer has a PS/2 keyboard connector but is using a USB keyboard, the BIOS may not recognize that keyboard at bootup time.

   The easiest solution is to connect a PS/2 keyboard and reboot; a more convenient option would be to always have a USB-to-PS/2 adapter with you for this purpose. Failing either of these options, you may find a selection in the BIOS to recognize a USB keyboard. But with only a USB keyboard available, you may not be able to access the BIOS settings.

   This situation applies mostly to computers that originally came with Windows XP installed. Most computers produced since Windows 7 became the standard should fully support USB keyboards, even at bootup time.

2. **How to recover a Windows 8 Key**

   Personal Computers that come with Microsoft Windows preinstalled have always come with a sticker on the outside of the computer case with the Product Key for that specific installation of Windows. If you ever needed to reinstall Windows on that computer, you would use that Key to verify that this is a "legal" installation of the Operating System.

   Major changes to the hardware environment have led to a significant change in this policy by Microsoft. Computers that come with Windows 8 or 8.1 preinstalled no longer carry an external sticker with the Product Key; instead, that Key is now stored internally in the BIOS of the computer. While this approach offers some benefits, it also causes a problem if you need to reinstall the Operating System on that computer.

   Once you understand how the system works and have the appropriate tools, you can recover the Key when necessary. This excellent article in Technibble.com, written by Micah Lahren, gives you a step-by-step procedure to do exactly that: http://www.technibble.com/recover-windows-8-key/.

3. Windows 8 – Enable Advanced Boot Options

In Windows 8, Microsoft removed the option to boot into Safe Mode or other Advanced Boot Options that have always been accessed by pressing the F8 key at bootup time. You can restore that functionality by taking the following steps, as described by Bleeping Computer at http://www.bleepingcomputer.com/tutorials/enable-the-f8-key-in-windows-8/:

- Open an elevated command prompt. If you don't know how to do this, this article from Bleeping Computer describes two methods you may use to open an elevated command prompt: http://www.bleepingcomputer.com/tutorials/open-an-elevated-command-prompt-in-windows-8/.
- Type the following in the command prompt and then press the Enter key:

  Bcdedit /set {default} bootmenupolicy legacy

- After you have entered this command, Windows will report that "The operation completed successfully." You now need to restart the computer for the change to go into effect. With this setting configured, you can now press F8 while Windows 8 starts in order to access Safe Mode and other Advanced Boot Options.
- If you would like to reset this computer to the default Windows 8 setting with the F8 key disabled, you can open an elevated command prompt and enter the following command:

  Bcdedit /set {default} bootmenupolicy standard

- After you have entered this command, Windows will report that "The operation completed successfully." When you restart the computer, the F8 key will now be disabled in Windows 8.

4. "The User Profile Service failed the logon" message at Windows startup

This is a relatively common error, with several possible causes. It is usually fairly easy to correct, using any of three methods described in Microsoft KnowledgeBase Article ID 947215, here: http://support.microsoft.com/kb/947215/en-us. In most cases Method 1 will work just fine, with a minimal amount of effort and disruption to the existing User Profile. Total time to apply should be less than 10 minutes.

5. "Windows is shutting down in 60 seconds"

If you see the message "Windows is shutting down in 60 seconds" or some other indication that the shutdown sequence has been initiated, you can abort the shutdown by entering "shutdown /a" from the Run command in Windows XP; in Vista, Windows 7, or Windows 8, enter the command in the Start Menu search box and use Ctrl + Shift + Enter to Run as Administrator.

6. Malware keeps reinstalling, same name and same place

In some cases a piece of malware may reinstall itself after you have deleted it. This will frequently be done using the same file name every time. You can prevent this reinstallation by creating a folder by that same name in the normal location of the malware. Windows will not allow a file to be created with the same name as a folder at the same level on the hard drive.

One easy way to create such a folder is through the creative use of the standard functions and keyboard shortcuts in Windows Explorer, like so:

- Before deleting the malware, right-click on the file and select Rename. This will highlight the file name
- Use the keyboard shortcut Ctrl-C to Copy that file name (including the extension)
- Delete the malicious file
- In the same location, select File | New | Folder, then use Ctrl-V to Paste the file name
- Hit "Enter" to complete the process

7. Desktop icons gone

Following removal of some malware the desktop icons may disappear. This behavior should be easy to fix, using the following procedure (in Windows XP): Right-click on the desktop, then go to Properties | Arrange Icons By | Show Desktop Icons.

In Vista, Windows 7, and Windows 8, the procedure is slightly different. After right-clicking on the Desktop, go to View and check the box for Show desktop icons.

8. Missing thumbnail view in Taskbar

Most of us have become accustomed to seeing a thumbnail view of each open window as we hover over the icons in the Taskbar. But your computer may have lost

that feature, and now you're seeing only the text representation of what each window contains.

That change may have occurred in an effort by the Operating System to improve the computer's performance. If that's the case, it was usually the result of a temporary condition that no longer exists. But you will have to manually change this option back to the desired value.

You can find this setting in Control Panel | System | Advanced System Settings. On the Advanced tab, go to Performance Settings, then the Visual Effects tab. Several of the options shown on this page affect the thumbnail view, but the easiest way to reset it is to choose "Adjust for best appearance," then click Apply.

Note that all of these options may appear to be selected, but the thumbnail views are not showing as you want. In that case, click "Adjust for best performance," then "Adjust for best appearance," click Apply, then click OK, and you will have the desired behavior back.

9. Rebuild missing Windows Services

There are two Windows Services that are sometimes deleted or corrupted as a result of malware infection, or possible other causes. These are the BITS and Windows Update Services. The procedure for rebuilding these services is described in Microsoft KnowledgeBase Article ID 971058, "How do I reset Windows Update components?" here: http://support.microsoft.com/kb/971058/en-us.

This article provides a link to a FixIt routine that may resolve the issue for you; it's definitely worth a try. If that doesn't work, there is a lengthy manual procedure that will help you rebuild these services manually. It works, but is probably unlike anything you have done in Windows previously. Be sure and follow the instructions precisely.

10. Windows Update fails, with Error 0x80070424

Malware will frequently disable the Windows Update functionality, since a Windows Update could protect the user from the malware in question. In many cases, a Microsoft-provided Fix-It Solution will resolve this problem. If Windows Update fails with an Error number 0x80070424, the following article in the Microsoft KnowledgeBase gives detailed instructions to resolve the issue:

968002 – "Error 0x80070424 occurs when you use Windows Update, Microsoft Update, or Windows Firewall," at http://support.microsoft.com/kb/968002/en-us.

The article indicates that it only applies to Vista and Windows 7, but it also works with Windows XP.

In some cases you may be able to restore automatic updates by re-registering a single file, entering the following command from a Command Prompt:

regsvr32 wuaueng.dll

11. Windows Update fails on .Net updates, with Error 0x80070643

Within the overall category of Windows Update problems, a significant number of them involve the .NET Framework in its multiple versions. This article in the Microsoft KnowledgeBase contains detailed instructions for resolving these problems:

976982 – Error codes "0x80070643" or "0x643" occur when you install the .NET Framework updates, here: http://support.microsoft.com/kb/976982/en-us.

12. Windows Update repeatedly offers the same update

Sometimes a Windows Update will install successfully, but for whatever reason that installation doesn't register properly with Microsoft; as a result, the next check for Windows Updates will show that one as not having been installed. The same update will continue to be installed successfully until this problem is resolved.

If this problem is happening on a Windows XP computer, the following procedure may fix it with minimal effort (provided by Gary Campbell, of Nearly New Buy & Sell):

- Turn off Automatic Updates
- Download and install KB2879017 from this link: http://www.microsoft.com/en-us/download/details.aspx?id=40612
- Download and install KB2898785 from this link: http://www.microsoft.com/en-us/download/details.aspx?id=41404
- Turn on Automatic Updates
- Reboot the computer and all should be good

If this procedure doesn't resolve the issue, or for later versions of Windows, the subject is addressed in the following article in the Microsoft KnowledgeBase:

910339 – Windows Update or Microsoft Update repeatedly offers the same update, here: http://support.microsoft.com/kb/910339/en-us.

When you first pull up this article, a Pop-Up gives you a link to fix this problem (and other Windows Update problems) automatically. It is not clear whether this is the same general "FixIt" for Windows Update issues described in the following tip, but it is effective in resolving this specific problem.

There are two issues you can anticipate with this fix, though: It will take a while to run (may be well over one hour), and it will wipe out all history of Windows Updates. It may be necessary to reinstall some Windows Updates that had been successfully installed in the past, but Service Packs seem to survive this procedure.

13. General "FixIt" for Windows Update issues

In response to numerous problems with the Windows Update procedure, Microsoft has developed a "Fix It" that will automatically resolve most Windows Update issues. This link goes to an article titled "Fix Microsoft Windows Update Issues:"

http://support.microsoft.com/gp/windows-update-issues/en-us#find_topsupport

The article includes different procedures for the four most recent desktop versions of Windows – Windows 8, Windows 7, Windows Vista, and Windows XP. For each version, a list of specific problems is included, along with steps to resolve each one.

The article also includes a link to let Microsoft automatically fix the problem for you. Before spending a lot of time on a manual repair, you may want to try the Automated Troubleshooter instead. If that doesn't fix the problem, you can still come back and follow the indicated procedures to resolve the issue manually.

14. Translating BSOD error codes

Blue Screen of Death (BSOD) errors can be some of the most cryptic and most difficult to troubleshoot. Microsoft actually provides some help in diagnosing and recovering from those errors, in this article from the Microsoft Developer Network: http://msdn.microsoft.com/en-us/library/hh994433(v=vs.85).

The article lists more than 300 error codes and provides additional information on possible recovery actions for each one. The article also contains links to more generic information for troubleshooting BSOD errors in different versions of Windows.

15. Command Prompt – Commands to know and use

Haven't used a Command Prompt lately? It may be time to review what was once known as the MS-DOS commands. Here are some commands you may need to use when removing malware from an infected computer. All of these will run from a Command Prompt in Windows (Normal or Safe Mode), from Safe Mode Command Prompt, or from a non-Windows bootup such as The Ultimate Boot CD:

- Attrib
- Cd or Chdir
- Copy
- Delete or Erase
- Dir
- FC
- Find
- Md or Mkdir
- More
- Rd or Rmdir
- Ren or Rename
- Set
- Tree
- Xcopy

16. Terminate processes by using the Taskkill command

Another method you may use to terminate a malicious process is the Taskkill command, from a Command Prompt. Here is an example of that process:

- Open a Command Prompt window, using Start | Run | Cmd (in Windows XP or older), typing Cmd in the Search box (Vista or later), or selecting Start | All Programs | Accessories | Command Prompt.
- Enter the command "tasklist" (without the quotes).
- Search through the list of Image Name entries to find the malicious process or processes.
- Note the PID for any such processes.
- Enter the command "taskkill /f /pid nnnn /t" (without the quotes), where nnnn is the PID of the process to be terminated. If there are multiple processes to be terminated, they may all be included in a single entry by using multiple "/pid nnnn" operands.
- Enter the command "exit" to close the Command Prompt window.

17. Additional commands from Command Prompt – Driverquery and Edit

The Driverquery command lets you enumerate and display the list of installed device drivers as well as their properties. You can find details of its use by entering, from a Command Prompt, "driverquery /?" (without the quotes).

The Edit command lets you open text files, which include .txt, .ini, .log, .reg, .adm, and .pol, among others. You may use this command to view these files and to safely edit them if necessary.

18. System File Checker tool (SFC), from Microsoft

If a Windows system component is missing or corrupted, you may be able to resolve that issue by the use of the SFC (System File Checker) tool. From a Command Prompt, type the following command: sfc /scannow.

For more details of this tool and its options, see one of the following articles in the Microsoft KnowledgeBase:

310747 – Description of Windows XP and Windows Server 2003 System File Checker (sfc.exe), http://support.microsoft.com/default.aspx?scid=kb;en-us;310747

-- or --

929833 – How to use the System File Checker tool to troubleshoot missing or corrupted system files on Windows Vista, Windows 7, or Windows 8, http://support.microsoft.com/kb/929833

19. Expand a Windows component from installation media

If you only need a known-good copy of a few Windows system components, and you have an installation CD or DVD for that Operating System (must be the very same version, Service Pack level, and language version), the Expand command provides that functionality. This command may be entered from a regular Command Prompt or from the Recovery Console.

The compressed files will normally be found in the \i386 folder of the installation CD or DVD. The file name for each file in that folder will normally end in an underscore (_).

The Expand command is fairly straightforward, normally composed of two parameters – the source and the destination. The following example would create a fresh copy of atapi.sys from the installation media:

expand d:\i386\atapi.sy_ c:\windows\system32\drivers\atapi.sys

You can find more details of the options in the Expand command by using the standard Help query, e.g. **expand /?** from a Command Prompt.

Another option to expand a compressed file from the installation media is available to you in Windows XP. In Msconfig, on the General tab, you will notice a button labeled "Expand File…" Clicking on that button gives you the same options through the GUI that you have from the Expand command as shown above.

20. System Restore from Safe Mode, Command Prompt

Some malware will start automatically, even in Safe Mode or Safe Mode with Networking. If your objective is to try a System Restore to a time before the malware was active, you may be able to accomplish that objective by booting into Safe Mode with Command Prompt.

From the Command Prompt in Safe Mode, type the following command: **%systemroot%\system32\restore\rstrui.exe**, and then press Enter. At that point you may choose a restore point prior to the time of the infection. Note that the infection will still be present on the computer following a successful System Restore, but it will not be active. In that environment you should be able to use most of the normal tools for malware cleanup.

21. Using Task Manager to kill a program or a process

If you want to terminate a program or a process by using Task Manager, there is a "best way" to do it. Here is the recommended sequence:

- If the program appears on the Applications tab, click on it and End Task from there
- If it's not there, find it on the Processes tab; note that there may be multiple Processes associated with an application
- Right-click on each process to be terminated and choose "End Process Tree." This is a more effective choice than the usual "End Process."

22. Task Manager – additional details

There are several features of Task Manager that are not generally known, but that can provide useful functionality for the technician. Here are some of those features:

- On the Processes tab, the View menu includes the option to Select Columns. There are several columns that are not displayed by default, that can provide useful information for troubleshooting various issues – including malware.
- On the Performance tab, the View menu includes the option to Show Kernel Times. This option produces a separate performance graph in red, showing CPU time being used by the Operating System (as opposed to applications).
- If your view of Task Manager doesn't show any of the tabs, the Menu bar, or the frame around the window, it has (possibly inadvertently) been switched to Tiny Footprint mode. To return to the normal view of Task Manager, double-click in the top border area of the window.

23. Access all system settings in one place, using God Mode

God Mode is a feature of Windows 7 that Microsoft has never documented. It was revealed by CNet's Microsoft correspondent, Ina Fried. It is a special folder that brings all of the Windows customization settings together in one place.

To install this feature on a computer, it only requires a few steps:

- Create a New folder (on the Desktop or the location of your choice)
- Give it the following name: GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}
- That name will cause the icon to change to look like Control Panel
- Double-click on that icon, and explore all of the settings on that computer

24. Windows Installer Cleanup Utility (Msicuu2.exe)

This program was formerly available from Microsoft, to uninstall programs that could not be uninstalled through the Add/Remove Programs applet in Control Panel. These programs may not have followed the standard installation and removal protocol, or the uninstall procedure may have been corrupted.

Microsoft no longer supports this program, and it is not on their web site to be downloaded; however, it can be found on many sites that distribute shareware and

trialware. While it was reliable and useful in Windows XP and previous versions of Windows, it evidently had some problems with the newer Operating Systems.

Microsoft now offers a FixIt to resolve some problems of this type. It is described in this KnowledgeBase article: 290301 – "What happened to the Windows Installer Cleanup Utility (MSICUU2.exe)?" at http://support.microsoft.com/kb/290301/en-us.

Another program that is useful in this situation is Revo Uninstaller. They offer a free version and a paid version with many additional features. More information and download links here: http://www.revouninstaller.com/revo_uninstaller_free_download.html.

25. Enable Hidden Secret Control Panel Items in Windows Vista, 7, and 8

There are some potentially useful Control Panel items that are hidden by default in the latest versions of Windows. This topic is covered in detail on the AskVG web site. Here is a link to the article: http://www.askvg.com/enable-hidden-secret-control-panel-items-in-windows-vista-and-7/.

26. Force NumLock On at Startup

Regardless of the BIOS setting for "Bootup NumLock Status," or words to that effect, all NT-based versions of Windows force NumLock Off at bootup time. It's easy to change this behavior, with a simple Registry edit.

Go to HKEY_USERS\.DEFAULT\Control Panel\Keyboard and find the entry for InitialKeyboardIndicators. In Windows XP and earlier versions, this entry contained a numeric value between 0 and 7, to set the initial status of CapsLock, NumLock, and ScrollLock. By default all were turned Off, with a value of 0 in this entry. Changing that value to 2 turns NumLock On when Windows starts.

The usage of this entry changed in Vista and later versions of Windows. Although it appears to be a major change, it is actually trivial. That entry now contains a 10-digit number, starting with 214. In reality, this is simply a different representation of the same number combinations.

The heart of the entry is still a value of 0-7, but with a one-bit difference. The value that is shown is derived from the decimal equivalent of a binary value contained in a Doubleword in memory. In hexadecimal notation the value ranges from 80000000

through 80000007. In other words, the high-order bit is turned on, but the remainder of that Doubleword is the same 0-7 as always.

To summarize, the default value of InitialKeyboardIndicators in these later versions of Windows is 2147483648; this forces NumLock Off. Changing that value to 2147483650 forces NumLock On at startup. Actually, changing that value to 2 still works as well.

27. Quit waiting for menus to pop up, by changing the MenuShowDelay setting

Any time a menu flies out or pops up in any version of Windows, there is a built-in delay. That delay was most noticeable in Windows XP and earlier versions, but it is present in the newer Operating Systems as well.

The default value of this delay is 400 milliseconds, or .4 seconds. While this doesn't sound like a long time, reducing it to 100 milliseconds gives any computer the appearance of being significantly faster than it was with the default value. The average time it takes a human to blink their eyes is 400 milliseconds, so it has been speculated that Microsoft chose that delay accordingly.

To change the delay setting, in the Registry you will need to navigate to HKEY_CURRENT_USER\Control Panel\Desktop and find the entry MenuShowDelay. Change the value of this entry from 400 to 100 and speed up the computer.

Note: This setting is only examined at Windows startup time. So, your change will not take effect until the computer is re-booted. Also, the delay is there for a good reason; changing it to 0 or any value less than 100 is not recommended.

28. Uninstall a program that is not shown in the Add/Remove Programs applet

There may be times when you want to uninstall a program, but it doesn't appear in the Add/Remove Programs listing in Control Panel. That omission may be because the developer of the program didn't follow the standards set by Microsoft for installation and removal; if that's the case, this tip may not work for you.

It's also possible that the Uninstall procedure has become corrupted; in that case, you can probably reproduce it with minimal effort. The first step in this process is to run Regedit and navigate to the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

subkey. Expand that subkey and you will see a listing of all Windows applications installed on that computer.

As you look through that list of subkeys, you will notice that the first group (and it may be a large group) does not contain a program name; instead, these subkeys are made up of a string of alphanumeric characters enclosed in brackets, such as {04B83666-3A62…}.

For your first step in this process, skip over the bracketed entries and see if the program you want to uninstall is listed under its actual name. If you find it, click on that subkey and look in the right-hand pane of Regedit for an entry named UninstallString. That is the actual command that is used to uninstall the program.

Double-click on UninstallString, and then use Ctrl+C to copy that value to the Windows Clipboard. Go to a Run command or the search box and use Ctrl+V to paste this command into that location. Click OK to initiate the uninstall process.

You may also find an entry named QuietUninstallString; if so, you may use that command in lieu of UninstallString. This option performs the Uninstall without showing its progress on the monitor as it runs.

If you didn't find the desired program as a subkey with its own name, your next step is to go to the top of the list under the Uninstall subkey and start looking for it among the bracketed entries. Click on the first such entry and look in the right-hand pane of Regedit for an entry named DisplayName.

Using the down-arrow key on your keyboard, go through all of the bracketed subkeys and look for the desired DisplayName in each one. If you find it, you will follow the same procedure outlined above to run the UninstallString or QuietUninstallString.

As an alternative, you may use the Find command in Regedit. With the first bracketed entry selected, use Ctrl + F to open the Find command. In the "Find what:" box, enter the name of the program you want to uninstall. Uncheck the boxes for Keys and Values, so that you are only searching in the Data field, then click on Find next.

If you don't find it, that tells you the program probably did not follow the Microsoft conventions for installing and uninstalling. In that case, you may be able to remove it with Revo Uninstaller, as described in #20, above.

If that fails, about the only option you have left is to manually delete the program files from the hard drive and remove any references to it from the Registry. Be sure to make a backup of those Registry keys before you delete them; you may need to get them back.

29. Taking ownership (Permission) of a Registry key

There may be times when you need to take ownership and assign full permission on a particular Registry key. This can be a fairly involved process, but AskVG has posted a detailed tutorial on the subject. This article gives you a step-by-step guide, with screenshots: http://www.askvg.com/guide-how-to-take-ownership-permission-of-a-registry-key-in-windows/.

30. Install and update programs automatically with Ninite

Ninite is a program that can be used to automatically install selected programs on computers you designate. The free version lets you choose from 90 programs in 13 categories, and the Ninite Pro increases that to 110 programs.

The automatic installation installs apps in their default locations, says no to toolbars or extra junk, and does all its work in the background. It downloads the apps from each publisher's official site and installs 64-bit apps on machines that are running 64-bit Operating Systems.

Ninite Pro adds the functionality to manage apps on your whole network and multiple clients. It's licensed for business use, faster because of its download cache, can uninstall apps, has options to disable built-in updaters, notifications, and desktop shortcuts, and many more features.

Pricing for Ninite Pro is based on the number of computers under your control that are touched in a given month. It ranges from $20 per month for up to 100 computers to $185 per month for up to 1,000 computers.

More details on Ninite and Ninite Pro are here: https://ninite.com/.

31. Registry tools from Nirsoft

A collection of small and useful freeware utilities were developed by Nir Sofer and can be found and downloaded here: http://www.nirsoft.net/. His Registry Tools are

of particular interest, and you can find them here: http://www.nirsoft.net/windows_registry_tools.html.

There are five utilities in this category, the most generally useful of which would be the first one listed, RegScanner. This program complements Regedit in several useful ways, especially with regard to searches in the Registry.

32. Alternate DNS Servers

By default most home and small-business users use the DNS Server provided by their Internet Service Provider. It may be more desirable to use an alternate DNS Server, for any of several reasons – reliability, performance, or security.

In some cases malware may have reset the DNS Server address on an infected computer to a malicious address. In any event, there may be times when you want to know a given computer is using a legitimate, safe DNS Server.

This article on About.com includes a list of free and public DNS Servers, updated on a regular basis: http://pcsupport.about.com/od/tipstricks/a/free-public-dns-servers.htm.

You can find the current DNS Server address(es) on a given computer by using the Ipconfig /all command from a Command Prompt. You can find those addresses in the Registry by opening Regedit and navigating to the following subkey: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{adapter}. In the right-hand pane, the entry NameServer will have a value that contains the address of the Primary DNS Server, followed by the address of the Secondary DNS Server, if specified.

33. Using Sandboxie for additional protection

Today's more sophisticated malware may avoid detection by most anti-virus and Internet Security programs. For an additional layer of protection, you may wish to do your Internet surfing in an isolated, protected environment that is sometimes referred to as a sandbox.

One of the most popular sandbox programs is Sandboxie. Here is a very useful and readable one-page summary of using Sandboxie to safely browse the Internet: http://gegeek.com/documents/tech_docs/Using%20Sanboxie%20to%20Safely%20Browse.pdf.

Sandboxie is offered in a Home version and a Commercial version. Pricing is stated in Euros, as follows: Home version, 15 Euros (~$19 US) per year; Commercial version, one user, 41 Euros (~$52 US) per year; 2-49 users, 38 Euros (~$48 US) per computer per year. Here is their home page: http://www.sandboxie.com/.

Sandboxie was acquired by Invincea in 2013 for two reasons, according to their web site: Provide more resources to enhance the Sandboxie consumer product and offer advanced security protection for organizations considering Sandboxie Commercial by using the Invincea security platform instead.

The web site indicates that the additional protection and features of Invincea of Invincea Small Business costs less than Sandboxie Commercial, although the site does not show specific pricing. More details here: http://www.sandboxie.com/index.php?CommercialLicensing.

34. Lots of useful tools and references from Gegeek.com

This one site includes links to more than 200 other web sites, tools, and reference materials that can be useful for IT Support techs: http://www.gegeek.com/. At last count there were 228 such links, as well as a few paid advertisements.

35. Windows 8 – replace Start Menu

One of the major complaints about Windows 8 and even 8.1 is its elimination of the traditional Start Menu. There are at least four programs that will restore this functionality, at little or no cost. Here they are, listed in alphabetical order:

- Classic Shell, free (donations accepted), from http://www.classicshell.net/
- Classic Start by Ninite, free, from http://ninite.com/classicstart/
- Start Menu Reviver 2.0 by ReviverSoft, free, from http://www.reviversoft.com/start-menu-reviver/
- Start8 by Stardock, $4.99, from http://www.stardock.com/products/start8/