A FORENSIC ANALYSIS OF THE WINDOWS REGISTRY

Derrick J. Farmer
Champlain College
Burlington, Vermont
dfarmer03@gmail.com

Abstract

This paper will introduce the Microsoft Windows Registry database and explain how critically important a registry examination is to computer forensics experts. In essence, the paper will discuss various types of Registry "footprints" and delve into examples of what crucial information can be obtained by performing an efficient and effective forensic examination. Many of the Registry keys that are imperative and relevant to an examination will also be discussed.

Acknowledgements

This paper is primarily a product of research, but may also serve as a reference to a Windows registry examination. For the sake of simplicity, there will only be reference to the Windows XP operating system – Even though earlier versions of Windows utilize the Registry, contain similar characteristics, and even apply many of the same concepts. The reasons XP was chosen to be discussed over other versions of Windows is because it remains popular and very widely used among average computer users, thus the chance of encountering it in a forensic examination is higher. Windows XP is still very current and much of the same information can still be applied to previous versions of Windows.

The illustrations throughout this paper are intended to provide a better understanding of the subject being discussed. All of the screenshot images contained in this paper were captured from the Windows XP system in which the research was conducted on.

The P2P client programs that were downloaded, installed, used, and examined were for the purpose of research use only. Searches were conducted and files were downloaded from these networks, not to engage in illegal or malicious activity, but to help provide a better understanding of the software's architecture and how it utilizes the Windows Registry from a forensics standpoint.

Introduction

The Importance of a Registry Examination

Today's society relies heavily on computers and the internet to accomplish everyday tasks, which includes practically everything from communicating and shopping online to banking and investing. It is much more common to send or receive an email than a physical letter. Along with the increasing use of computers and the internet, comes a *little* problem called computer crime-- facetiously speaking. Computer crimes present exorbitant issues in today's society. Including, but certainly not limited to – fraud, identity theft, phishing, network infiltration, DoS attacks, piracy of copyrighted material,

and child pornography. With computer crimes on the rise, it is becoming extremely crucial for law enforcement officers and digital forensic examiners to understand computer systems and be able to examine them efficiently and effectively. In order to do this a study of how operating systems work must be explored from the inside out. The Registry is the heart and soul of the Microsoft Windows XP operating system and an exponential amount of information can be derived from it.

History

First, it is important to understand what the Registry is, why it exists, and the types of information it contains. Virtually everything done in Windows refers to or is recorded into the Registry. A program called RegMon by Sysinternals can be used to display registry activity in real time. After running this program it is apparent that registry access barely remains idle. The Registry is referenced in one way or another with every action taken by the user.

The Microsoft knowledge database and also the *Microsoft Computer Dictionary*, Fifth Edition, define the registry as:

A central hierarchical database used in Microsoft Windows 9x, Windows CE, Windows NT, and Windows 2000 used to store information necessary to configure the system for one or more users, applications and hardware devices.

The Registry was first introduced with Windows 95 and has been incorporated into many Microsoft operating systems since. Although some versions slightly differ, they all are essentially composed of the same structure and serve the main purpose as a configuration database. The Registry replaces configuration files that were used in MS-DOS, such as config.sys and autoexec.bat. The primary purpose of config.sys was to load device drivers and the primary purposes of autoexec.bat was to run startup programs and set environment variables – the Registry now handles these functions. In addition to replacing DOS configuration files, the Registry also replaces text-based initialization (.ini) files that were introduced in Windows 3.0. The .ini files – specifically win.ini and system.ini – store user settings and operating system parameters.

This very basic history of the Windows Registry, why it was implemented, and some of its functions are the core fundaments of understanding the structure and what each part of the Registry pertains to.

Structure of the Windows Registry

By opening the Registry Editor (by typing "regedit" in the run window), the Registry can be seen as one unified "file system". The left-hand pane, also known as the key pane contains an organized listing of what appear to be folders. The five most hierarchal folders are called "hives" and begin with "HKEY" (an abbreviation for Handle to a Key). Although five hives can be seen, only two of these are actually "real", HKEY_USERS (HKU) and HKEY_LOCAL_MACHINE (HKLM). The other three are shortcuts or aliases to branches within one of the two hives. Each of these five hives is composed of keys, which contain values and subkeys. Values are the names of certain items within a key, which uniquely identify specific values pertaining to the operating system, or to applications that depend upon that value.

A common analogy that is often used to help understand the structure of the Windows Registry is a comparison between it and the Windows Explorer file system, both are very similar in their structures. The key pane of the Registry is much like the hierarchical structure of the left-hand pane in the Windows Explorer file system. The keys and subkeys located within the five main hives are similar to folders and subfolders of Windows Explorer, and a key's value is similar to a file within a folder. In the right-hand pane of the Windows Registry – a value's *name* is similar to a file's name, its *type* is similar to a file's extension, and its *data* is similar to the actual contents of a file.

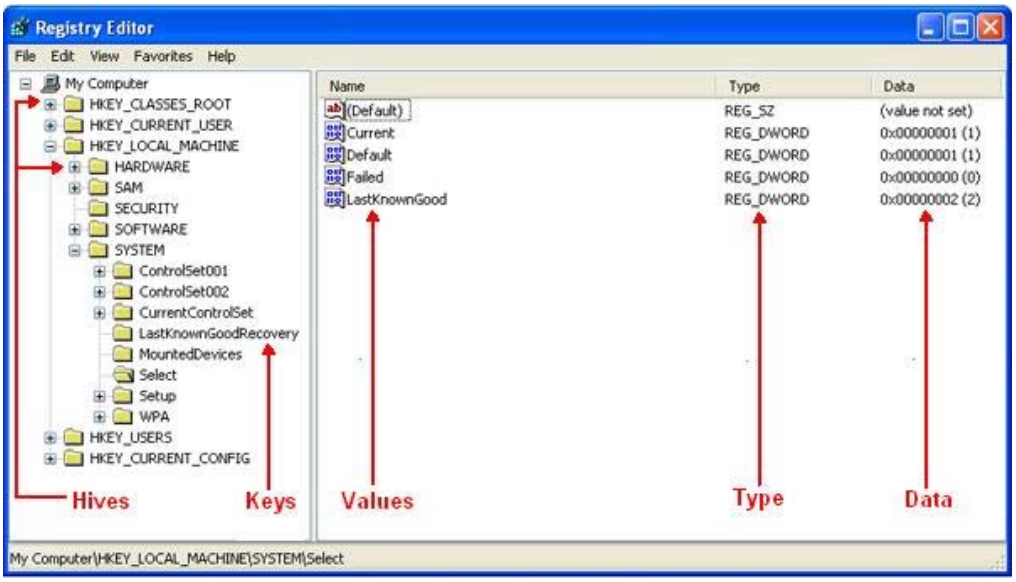

Figure 1 – Structure of the Windows Registry

Root Key Functions:

Below are listed the five hierarchical hives seen in Figure 1, with a very basic description of each. Beside the root key is their commonly referred to abbreviation in parenthesis, which will frequently be referred to as throughout the paper.

1. `HKEY_CLASSES_ROOT` (HKCR)
   Information stored here ensures that the correct program opens when it is executed in Windows Explorer. It also contains further details on drag-and-drop rules, shortcuts, and information on the user interface. Alias for: `HKLM\Software\Classes`

2. `HKEY_CURRENT_USER` (HKCU)
   Contains configuration information for the user who is currently logged into the system, including user's folders, screen colors, and Control Panel settings. Alias for a user specific branch in `HKEY_USERS`. The generic information usually applies to all users and is `HKU\.DEFAULT`.

3. `HKEY_LOCAL_MACHINE` (HKLM)
   Contains machine hardware-specific information that the operating system runs on. It includes a list of drives mounted on the system and generic configurations of installed hardware and applications.

4. `HKEY_USERS` (HKU)
   Contains configuration information of all user profiles on the system, which concerns application configurations, and visual settings.

5. `HKEY_CURRENT_CONFIG` (HCU)
   Stores information about the systems current configuration. Alias for: `HKLM\Config\profile`

Examination Tools

Currently, there are many tools available to forensic examiners for extracting evidentiary information from the Registry. The tool used in this paper to analyze and navigate the registry is Registry Editor (regedit.exe). Registry Editor is free and available on any installation of Microsoft Windows XP with administrator privileges.

Registry Examination

The Registry as a Log

All Registry keys contain a value associated with them called the "LastWrite" time, which is very similar to the last modification time of a file. This value is stored as a FILETIME structure and indicates when the Registry Key was last modified. In reference to the Microsoft Knowledge Base, A FILETIME structure represents the number of 100 nanosecond intervals since January 1, 1601. The LastWrite time is updated when a registry key has been created, modified, accessed, or deleted. Unfortunately, only the LastWrite time of a registry key can be obtained, where as a LastWrite time for the registry value cannot.

Harlan Carvey, author of *Windows Forensics and Incident Recovery*, refers to a tool called Keytime.exe, which allows an examiner to retrieve the LastWrite time of any specific key. Keytime.exe can be downloaded from http://www.windows-ir.com/tools.html.

Knowing the LastWrite time of a key can allow a forensic analyst to infer the approximate date or time an event occurred. And although one may know the last time a Registry key was modified, it still remains difficult to determine what value was actually changed. Using the Registry as a log is most helpful in the correlation between the LastWrite time of a Registry key and other sources of information, such as MAC (modified, accessed, or created) times found within the file system. However, a comprehensive discussion of that process is outside the scope of this paper.

Autorun Locations

Autorun locations are Registry keys that launch programs or applications during the boot process. It is generally a good practice to look here depending on the case of examination. For instance, if a computer is suspected to have been involved in a system intrusion case, autorun locations should be looked at. If the user denies their involvement then it's possible their own system was compromised and used to initiate the attack. In a case such as this, the autorun locations could prove that the system had a trojan backdoor installed leaving it vulnerable for an attacker to use at their discretion.

List of common autorun locations:

HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
HKLM\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
(ProfilePath)\Start Menu\Programs\Startup

MRU lists

MRU, or "most recently used" lists contain entries made due to specific actions performed by the user. There are numerous MRU lists located throughout various Registry keys. The Registry maintains these lists of items incase the user returns to them in the future. It is basically similar to how the history and cookies act to a web browser.

One example of an MRU list located in the Windows Registry is the RunMRU key. When a user types a command into the "Run" box via the Start menu, the entry is added to this Registry key. The location of this key is **`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU`** and its contents can be seen in Figure 2. The chronological order of applications executed via "Run" can be determined by looking at the *Data* column of the "MRUList" value. The first letter of this is "g", which tells us that the last command typed in the "Run" window was to execute notepad. Also, the LastWrite time of the RunMRU key will correlate with the last application executed in "Run", or in this case application "g".

With the information provided from the RunMRU key, an examiner can gain a better understanding of the user they are investigating and the applications that are being used. In reference to Figure 2, it is apparent the user has sufficient knowledge of the Windows operating system – based on applications that have been executed, such as msconfig, cmd, sysedit, and regedit.

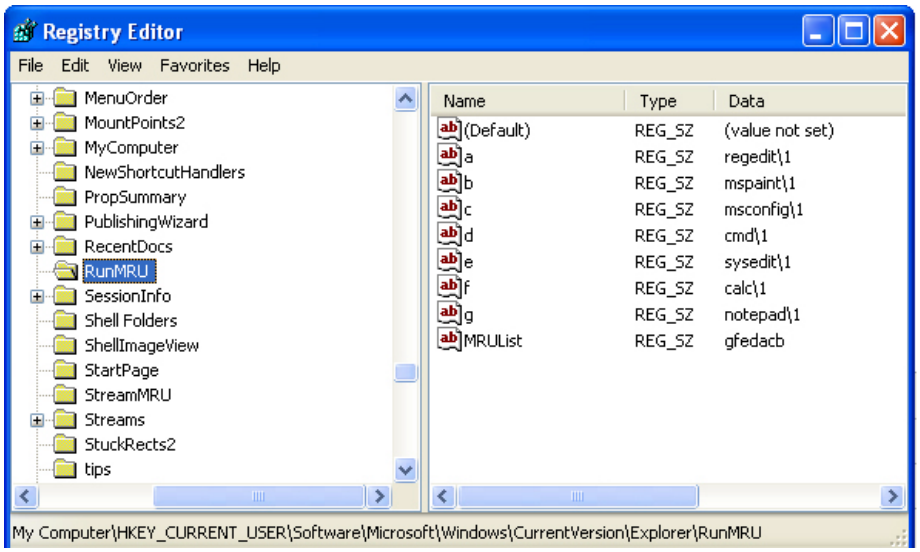

Figure 2 – RunMRU key

Locations of other MRU lists that may be useful in a forensic analysis. This list is by no means conclusive.

XP Search Files	Software\Microsoft\Search Assistant\ACMru\5603
Internet Search Assistant	Software\Microsoft\Search Assistant\ACMru\5001
Printers, Computers and People	Software\Microsoft\Search Assistant\ACMru\5647
Pictures, music, and videos	Software\Microsoft\Search Assistant\ACMru\5604
XP Start Menu - Recent	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
R. Desktop - Connect	Software\Microsoft\Terminal Server Client\Default [MRUnumber]
Run dialog box	Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
Regedit - Last accessed key	Software\Microsoft\Windows\CurrentVersion\Applets\Regedit
Regedit - Favorites	Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\Favorites
MSPaint - Recent Files	Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List
Mapped Network Drives -	Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
Computer searched via Windows Explorer	Software\Microsoft\Windows\CurrentVersion\Explorer\FindComputerMRU
WordPad - Recent Files	Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List
Common Dialog - Open	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Common Dialog - Save As	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
WMP XP - Recent Files	Software\Microsoft\MediaPlayer\Player\RecentFileList
WMP XP - Recent URLs	Software\Microsoft\MediaPlayer\Player\RecentURLList
OE6 Stationery list 1 - New Mail	Identities\{C19958F2-22F3-4C6A-9AE0-12049CE0706F}\Software\Microsoft\Outlook Express\5.0\Recent Stationery List *the CLSID varies, just an example given
OE 6 Stationery list 2 - New Mail	Identities\{C19958F2-22F3-4C6A-9AE0-12049CE0706F}\Software\Microsoft\Outlook Express\5.0\Recent Stationery Wide List *the CLSID varies
PowerPoint - Recent Files	Software\Microsoft\Office\10.0\PowerPoint\Recent File List
Access - Filename MRU	Software\Microsoft\Office\10.0\Common\Open Find\Microsoft Access\Settings\File New Database\File Name MRU
FrontPage - Recent lists	Software\Microsoft\FrontPage\Explorer\FrontPage Explorer\Recent File List
Excel - Recent Files	Software\Microsoft\Office\10.0\Excel\Recent Files
Word - Recent Files	Software\Microsoft\Office\10.0\Word\Data

Reference to additional MRU lists: **http://windowsxp.mvps.org/RegistryMRU.htm.**

UserAssist

The UserAssist key, **`HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist`**, contains two or more subkeys which have long hexadecimal names that appear as globally unique identifiers (GUIDs). Each subkey records values that pertain to specific objects the user has accessed on the system, such as Control Panel applets, shortcut files, programs, etc. These values however, are encoded using a ROT-13 encryption algorithm, sometimes known as a Caesar cipher. This particular encryption technique is quite easy to decipher, as each character is substituted with the character 13 spaces away from it in the ASCII table. A much faster and easier method to decipher this code is with the use of an online ROT-13 decoder, such as http://www.edoceo.com/utilis/rot13.php.

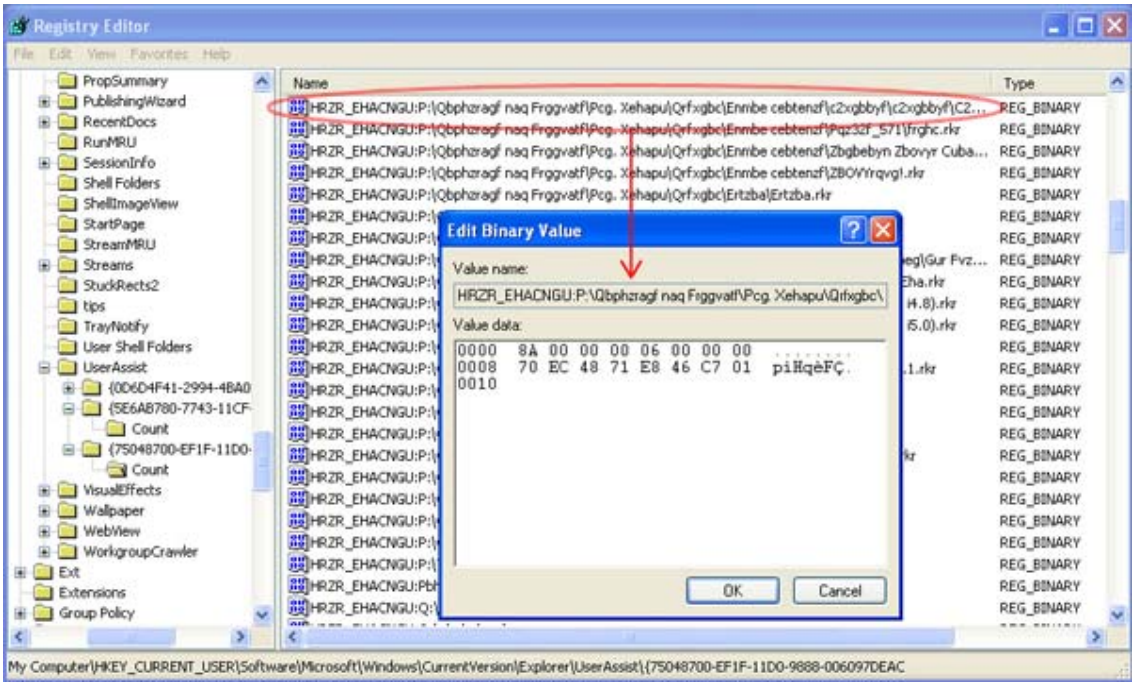

Figure 3 – UserAssist Key

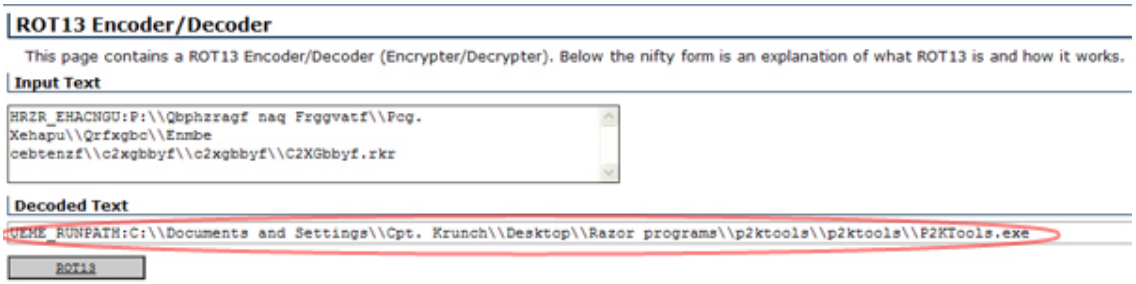

Figure 3a – ROT-13 cipher decoded

With the UserAssist key, a forensic examiner can gain a better understanding of what types of files or applications have been accessed on a particular system. Even though these entries are not definitive, for they cannot be associated with a specific date and time, it may still indicate a specific action by the user.

For instance, in the example of Figures 3 and 3a the decoded value can show a potential amount of information. First, it tells the name of the user profile – "Cpt. Krunch" – from which the .exe was executed from. Cpt. Krunch could also indicate a handle or an alias of some sort. Second, by researching "p2ktools.exe", it tells that it is a program used for editing and managing Motorola cell phones. Finally, it shows the user has the p2ktools folder in a parent directory called "Razor programs", which is located on their desktop. Not only does this give the location of where similar programs may reside, but the name of this directory is a good indicator that the suspect has a Motorola Razor cell phone. If so, that too should be seized for further analysis.

Wireless Networks

Wireless networks today are popular and are only becoming more popular. A wireless ethernet card picks up wireless access points within its range, which are identified by their SSID or service set identifier. When an individual connects to a

network or hotspot the SSID is logged within Windows XP as a preferred network connection. Unsurprisingly, this can be found in the Registry in the **HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces** key. When opening this Registry key there may be subkeys beneath it, like UserAssist, that look like GUIDs. The contents of these should contain the values "ActiveSettings" and "Static#0000". There may be additional values that begin with "Static#" and are sequentially numbered. In the binary data of these "Static#" values are the network SSIDs of all the wireless access points that system has connected to. This can be seen by right clicking the value and selecting "modify", as shown in Figure 4.

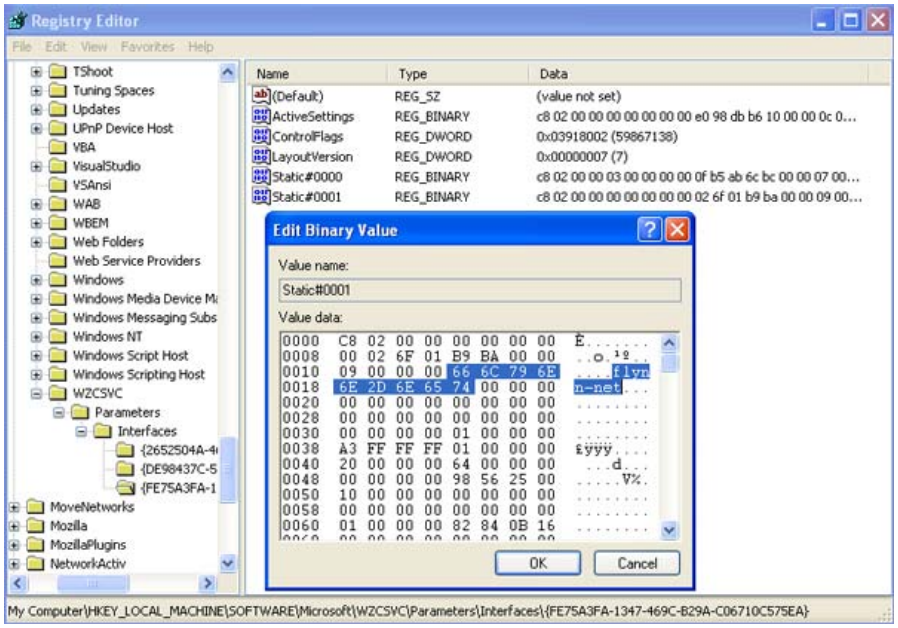

Figure 4 – SSID "flynn-net"

In addition to logging the name of the SSID, Windows also logs the network settings of that particular connection – such as the IP address, DHCP domain, subnet mask, etc. The Registry key in which this can be found is **HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces**, which is illustrated in Figure 4a.

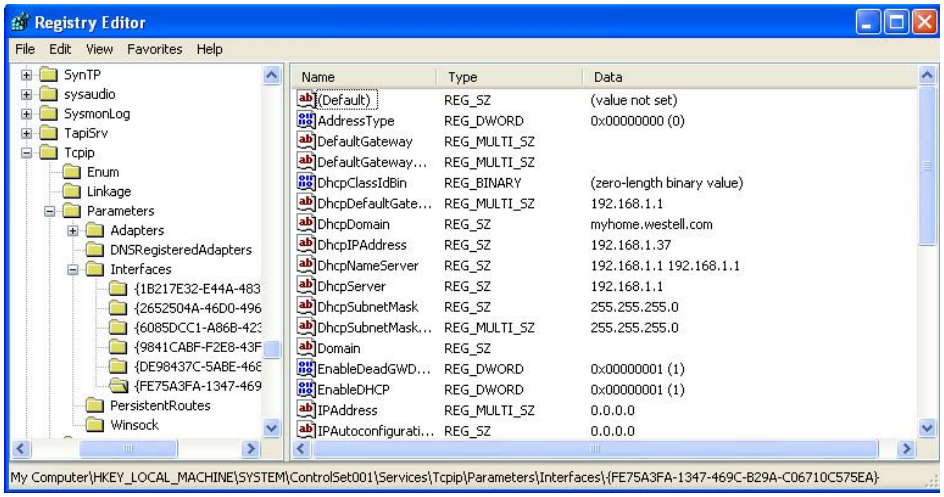

Figure 4a – Network settings of SSID "flynn-net"

Based on this wireless network information, a Forensic examiner can determine if a user connected to specific wireless access point, the timeframe, and their IP address they were assigned by the DHCP server. For instance, if it were a case about a child pornography suspect that was war-driving to various network connections and using them illegally, these methods would be very useful. Given the suspect's computer to run an analysis on would make it possible to see what network connections they were using and the IP address that was assigned to further support a subpoena of the ISP.

LAN Computers

Windows XP implements a network mapping tool called *My Network Place*, which allows users to easily find other users within a LAN or Local Area Network. A computer on a properly configured LAN should be able to display all the users on that network through *My Network Place*. This list of users or computers, like many other things, is stored in the Registry. Therefore, even after the user is no longer connected to the LAN, the list of devices still remain, including desktop computers, laptops, and printers. The Registry key where this information is stored is **`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions.`**

The `ComputerDescriptions` key is useful in determining whether or not a user was connected to certain computers or belonged to a specific LAN. Figure 5 displays the output of this key.

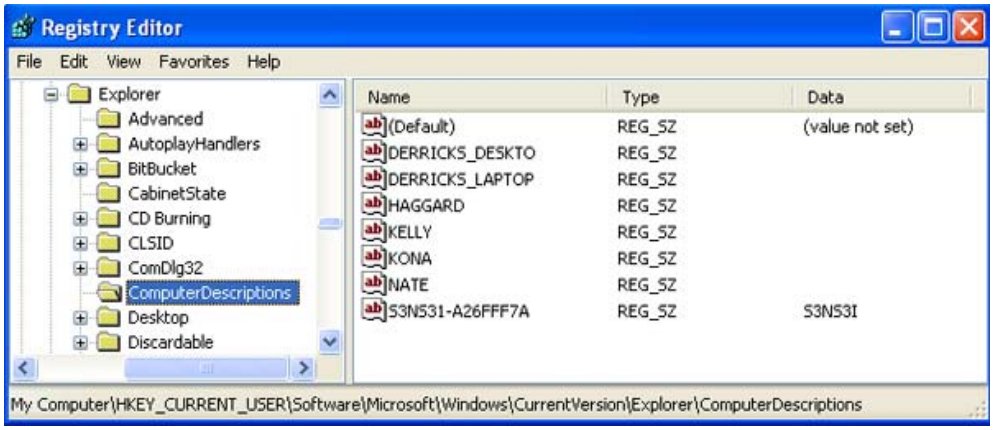

Figure 5 – List of computers associated with on a LAN

USB Devices

There is sufficient information on this topic to write an entire research paper on, however, for the scope of this paper only the basics will be discussed to show the most relevant Registry keys.

Anytime a device is connected to the Universal Serial Bus (USB), drivers are queried and the device's information is stored into the Registry (i.e., thumb drives). The first important key is **`HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR`**. This key stores the contents of the product and device ID values of any USB device that has ever been connected to the system. Figure 6 reveals the contents of this key. All of which can be interpreted – there lists an ipod, two external hard drives, a digital video camcorder, and several different thumb drives.

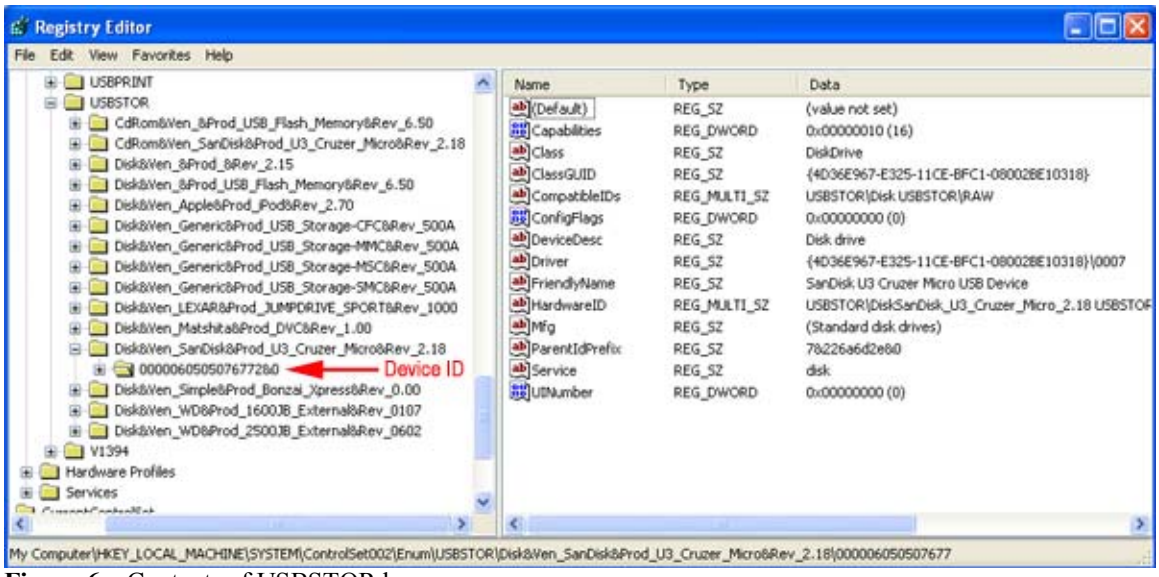

Figure 6 – Contents of USBSTOR key

Beneath each device is the Device ID, which is also a serial number. The serial numbers of these devices are a unique value assigned by the manufacturer, much like the MAC address of a network interface card. Therefore, a particular USB device can be identified to determine whether or not it has been connected to other Windows systems.

Carvey mentions in his article *The Windows Registry as a Forensic* Resource, an important consideration to keep in mind regarding USB device IDs. Not every thumb drive will have a serial number. Particularly, those that have an "&" symbol for the second character of the device ID. In reference to Figure 6, the Device ID that is pointed out has a serial number. However, if the "0" was an "&" that would indicate to an examiner that the device doesn't have a designative serial number. An example of a device that doesn't have an assigned serial number can be seen in Figure 6a, a Western Digital 250GB external hard drive.

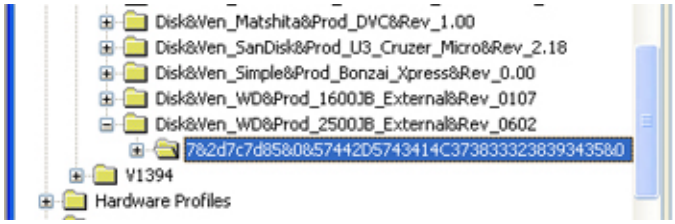

Figure 6a –USB device without a designated Device ID

Knowing what USB devices have been connected to a system can assist an examiner in collecting additional evidence that may be crucial to the investigation.

Mounted Devices

There is a key in the Registry that makes it possible to view each drive associated with the system. The key is **`HKLM\SYSTEM\MountedDevices`** and it stores a database of mounted volumes that is used by the NTFS file system. The binary data for each \DosDevices\x: value contains information for identifying each volume. This is demonstrated in Figure 7, where \DosDevice\F: is a mounted volume and listed as "STORAGE Removable Media".

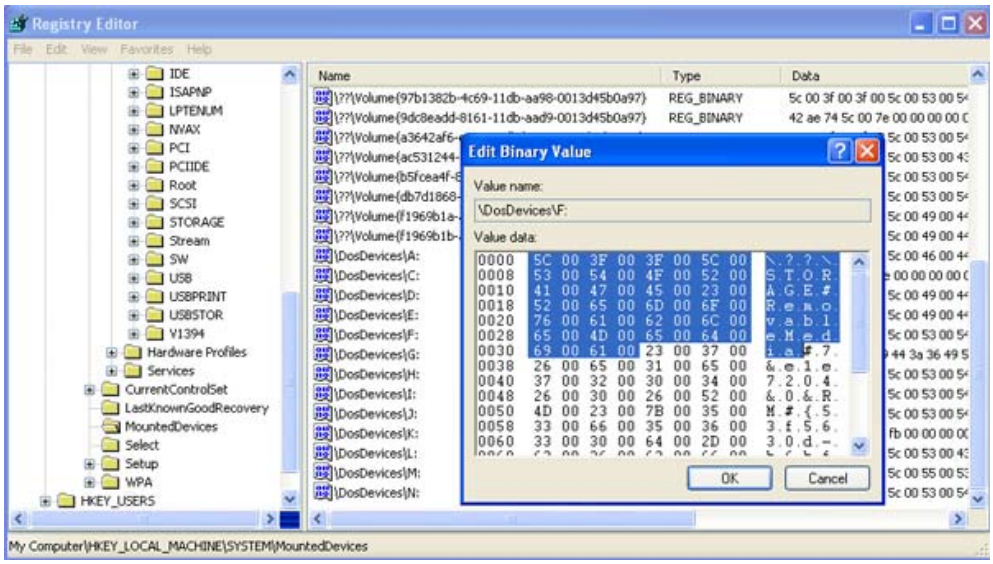

Figure 7 –Identification of volume \DosDevice\F:

This information can be useful to a digital forensics examiner as it shows the hardware devices that should be connected to the system. Therefore, if a device is shown in the list of MountedDevices and that device isn't physically in the system, it may indicate that the user removed the drive in attempt to conceal the evidence. In this case, the examiner would know they have additional evidence that needs to be seized.

Internet Explorer

Internet Explorer is the native web browser in Windows operating systems. It utilizes the Registry extensively in storage of data, like many applications discussed thus far. Internet Explorer stores its data in the **`HKCU\Software\Microsoft\Internet Explorer`** key. There are three subkeys within the `Internet Explorer` key that are most important to the forensic examiner. The first is **`HKCU\Software\Microsoft\Internet Explorer\Main.`** This key stores the user's settings in Internet Explorer. It contains information like search bars, start page, form settings, etc. The second and most important key to a forensic examiner is **`HKCU\Software\Microsoft\Internet Explorer\TypedURLs.`** Figure 8 demonstrates the content of what the `TypedURLs` key displays.

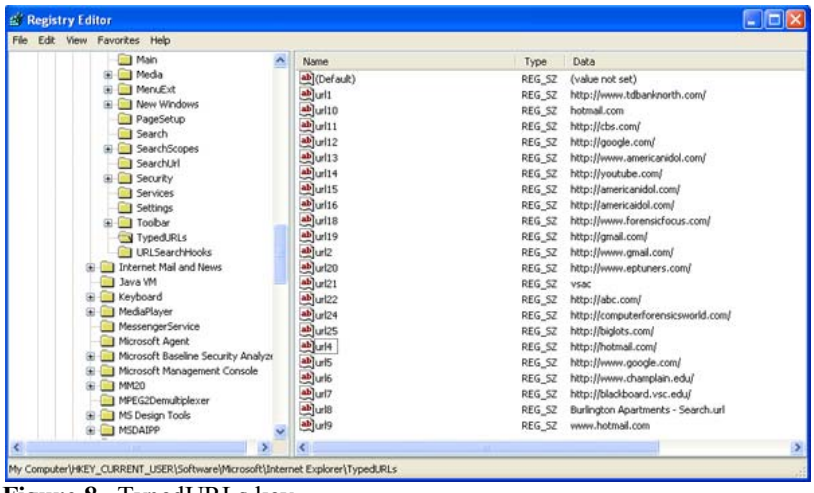

Figure 8 –TypedURLs key

From this data an examiner could conclude that the user possibly has a gmail and hotmail email address, they engage in online banking at tdbanknorth, is interested in digital forensic websites, and that they perhaps go to college at Champlain and have been researching apartments in the area.

The third subkey that may interest an examiner is **`HKCU\Software\Microsoft\Internet Explorer\Download Directory.`** This key reveals the last directory used to store a downloaded file from Internet Explorer, giving the examiner an idea as to the location of where the user stores their files.

Opera, Netscape, and Firefox

It is the best to my knowledge that none of these browsers utilize the Registry in the way that Internet Explorer does. Internet Explorer stores web history in a file called Index.dat, which is referenced in the Windows Registry database – hence the reason we can see the history contents in the `TypedURLs` key.

Opera on the other hand, stores its history in a file called opera.dir. The default location of this file is `C:\Documents and Settings\User Profile\Application Data\Opera\Opera\profile\.` Upon installing and using this browser, the only remnants of Opera located in the Registry were install paths. In fact, according to the features of Opera (http://operawiki.info/WhyOpera), two of the many reasons people choose to use this browser is because it doesn't use the registry to store data and the size of it is very small. It is only a 1.8mb executable and according to the "Add or Remove Programs" applet in Control Panel; the total installation is only 5.33mb.

Like Opera, Netscape and Firefox leave limited footprints (other then install paths) regarding Registry activity. Netscape and Firefox both store web history in a history.dat file, which is in ASCII format and plainly visible when opened. The location for the history.dat file in Firefox is `C:\Documents and Settings\User Profile\Application Data\Mozilla\Firefox\Profiles\x.default\` and Netscape is `C:\Documents and Settings\derrick.farmer\ Application Data\Netscape\NSB\Profiles\x.default\`. An in-depth analysis of these browsers is out of the scope of this particular paper as they are not relevant in a Windows Registry examination.

P2P Clients

Peer-to-Peer (P2P) networks are notorious of providing users with the ability to distribute illegal and sometimes unethical materials. Three popular P2P clients were downloaded, installed, used, and examined for the purpose of this research. The clients that were used are Limewire, Kazaa, and Morpheus.

Limewire

The research conducted on Limewire was somewhat inconclusive in regards to a Registry examination. There were very minimal footprints of user activity and no logs of searches or downloaded files could be found. The most helpful thing discovered in the Registry was install paths of the program. Knowing this information would give the exact location of where to look in the file system. In a default installation of Limewire

the location of the install directory is `C:\Program Files\Limewire` and the share directory is `C:\Documents and Settings\User Profile\Shared.`

Kazaa

Kazaa, however, was a bit more successful. Two Registry keys of interest were discovered. The first was **`HKCU\Software\Kazaa`**, and contained many user settings that could be useful to an investigator. For instance, beneath the `Kazaa` key there is a subkey called `ResultsFilter`, which shows the value for the `"adult_filter_level"`. This setting will filter adult content from search results. If the value of the `adult_filter_level` is `(1)` it is enabled and if it is `(0)` it is disabled. By default Kazaa enables the adult filter, so if this setting is disabled then it's a good indication the user has taken the initiative to do so within the Kazaa options menu. Figure 9 shows the location of this key and the information in which it contains.

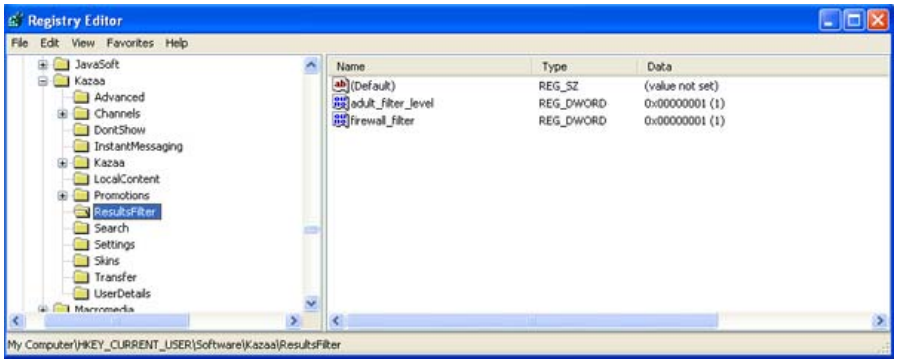

Figure 9 –Kazaa key

The other Kazaa Registry key that is worth pointing out is **`HKLM\Software\Kazaa`**. This key contains subkeys that hold connection information and the destination directory of the downloaded files, which show that a default installation of Kazaa stores downloaded files to `C:\Program Files\Kazaa\My Shared Folder`.

Morpheus

Of the three P2P clients that were researched, Morpheus was the only one that kept a log in the Registry of recently searched for keywords or phrases. The location of this key is **`HKCU\Software\Morpheus\GUI\SearchRecent`** and can be seen in Figure 10.

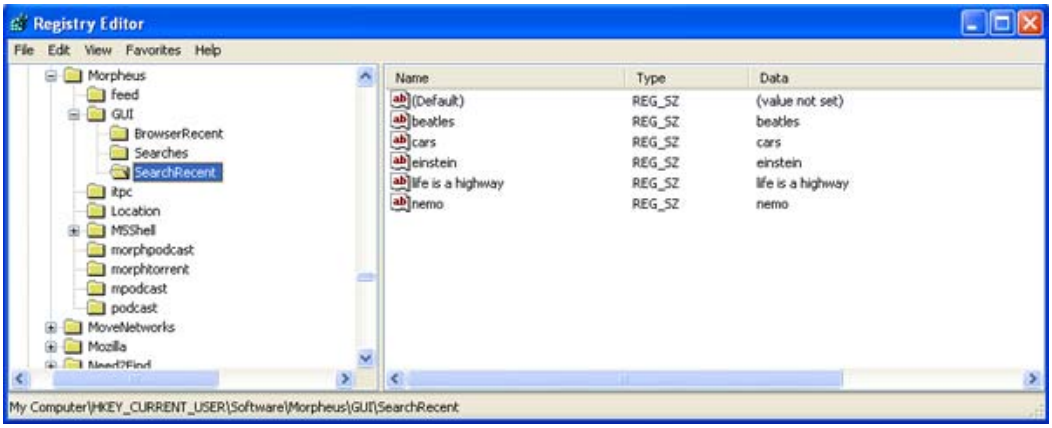

Figure 9a –Morpheus recent search list

If an examiner is investigating a case where the user is suspected to have used Morpheus to download illegal content, this key could be very useful in seeing exactly the type of material the user was querying.

One Thing in Common

Research of these three P2P clients revealed one Registry key that they all had in common:

HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List

This is a list of applications that are allowed "outside access" by the Windows Firewall that was implicated in SP2. If the P2P programs are not included in this list then they wouldn't be assigned a TCP or UDP port to access the P2P client's server and would consequently be blocked. Therefore, any type of program in use for file sharing purposes *should* appear on this list. This would be a great place for a forensic examiner to look in determining if the system has other potential file sharing applications that have been overlooked.

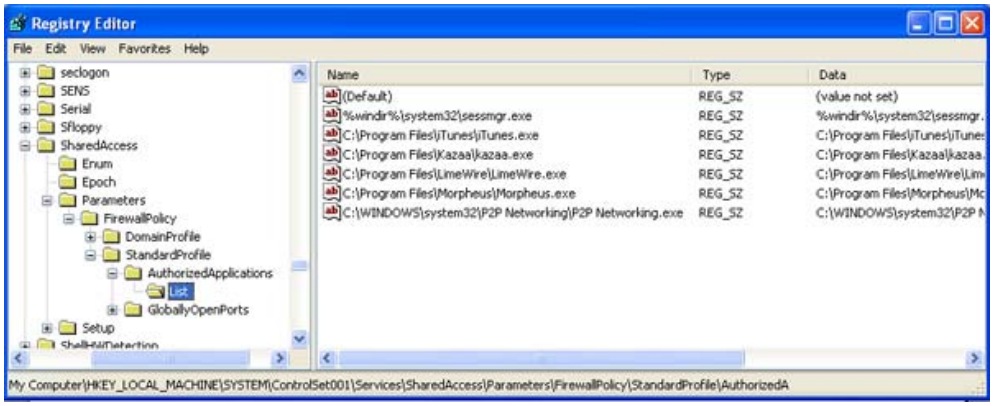

Figure 9b –Firewall Authorized Applications key

Overview

The following list includes a brief recap of the Registry keys discussed in this paper.

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
- HKLM\SOFTWARE\ Microsoft\WZCSVC\Parameters\Interfaces
- HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ ComputerDescriptions
- HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR
- HKLM\SYSTEM\MountedDevices
- HKCU\Software\Microsoft\Internet Explorer\Main
- HKCU\Software\Microsoft\Internet Explorer\TypedURLs
- HKCU\Software\Microsoft\Internet Explorer\Download Directory
- HKCU\Software\Kazaa
- HKCU\Software\Morpheus\GUI\SearchRecent
- HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\ FirewallPolicy\StandardProfile\AuthorizedApplications\List

For a comprehensive list of Registry keys that directly relate to a computer forensic examination, many of which were not discussed in this paper, refer to AccessData's PDF document *Registry Quick Find Chart*.

http://www.accessdata.com/media/en_US/print/papers/wp.Registry_Quick_Find_Chart.en_us.pdf

Conclusion

Given the popularity of the Windows operating system – in homes and businesses – it is important for computer forensic experts to understand the complexity of the Windows Registry. The information and potential evidence that reside in the Registry make it a significant forensic resource; uncovering this data can be crucial to any computer related investigation. By understanding the fundaments of the Registry from a forensics standpoint, an examiner can develop a more precise account on what actions occurred on the given machine. This report is by no means conclusive in terms of a Registry Examination. It presents some explanations and examples of what types of data can be found, how it can be found, and why it may be relevant to an examination. For as long as operating systems are dependent upon the Registry as a configuration database, and for as long as applications continue to use that database for storage, there will always be different locations to discover that provide evidential support in an investigation.

References

Books

Honeycutt, Jerry. Microsoft Windows Registry Guide. 2nd. Redmond, WA: Microsoft Press, 2005.

Kruse, Warren G., and Jay G. Heiser. Computer Forensics: Incident Response Essentials. New York: Addison-Wesley, 2004.

Nelson, Bill, Amelia Phillips, Frank Enfinger, and Christopher Steuart. Guide to Computer Forensics and Investigations. 2nd. Canada: Course Technology, 2006.

Journals

Carvey, Harlan. "The Windows Registry as a forensic resource." Digital Investigation: The International Journal of Digital Forensics & Incident Response 2(2005): 201-05.

Carvey, Harlan, and Cory Altheide. "Tracking USB storage: Analysis of windows artifacts generated by USB storage devices." Digital Investigation: The International Journal of Digital Forensics & Incident Response 2(2005): 94-100.

Online

Carvey, Harlan. "Windows Incident Response." [Weblog Mounted Devices] 21 Dec 2004. 8 Apr 2007 <http://windowsir.blogspot.com/2004_12_01_archive.html>.

Davies, Peter. "Forensic Analysis of the Windows Registry." Peter Davies. 2006. 3 Feb 2007 <http://www.pkdavies.co.uk/documents/computer_forensics/registry_examination.pdf>.

Jones, Kieth J., and Rohyt Belani. "Web Browser Forensics, Part 1." Security Focus. 30 Mar 2005. 13 Apr 2007 <http://www.securityfocus.com/infocus/1827>.

Microsoft, "Description of the Microsoft Windows Registry." Help and Support. 27 Jan 2007. Microsoft Corp. 8 Apr 2007 <http://support.microsoft.com/kb/256986/>.

Microsoft, "INFO: Working with the FILETIME Structure." Help and Support. 23 Jan 2007. Microsoft Corp. 8 Apr 2007 <http://support.microsoft.com/kb/188768>.

Opera, "Why Choose the Opera Internet Suite?." Operawiki. 2007. 13 Apr 2007 <http://operawiki.info/WhyOpera>.

“Registry Quick Find Chart." AccessData. 2005. AccessData Corp. 1 Apr 2007 <http://www.accessdata.com/media/en_US/print/papers/wp.Registry_Quick_Find_Chart.en_us.pdf>.

"ROT 13 Encoder/Decoder." Consulting, Development, Research, and Support. 2007. Edoceo, inc.. 14 Apr 2007 <http://www.edoceo.com/utilis/rot13.php>.

Srinivasan, Ramesh. "Registry MRU Locations." Ramesh's Site: Troubleshooting Windows. 2006. 14 Apr 2007 <http://windowsxp.mvps.org/RegistryMRU.htm>.

Websense, "Emerging Threats: Peer-to-Peer File Sharing." Advanced Systems Group. Websense, Inc. 13 Apr 2007 <http://www.virtual.com/whitepapers/Websense_ Emerging_Threats_Peer-to-Peer_wp.pdf>.

Wong, Lih Wern. "Forensic Analysis of the Windows Registry." Forensic Focus. 1 Feb 2007 <http://www.forensicfocus.com/index.php?name=Content&pid=73&page=1>.