A Windows Registry Quick Reference:
For the Everyday Examiner

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

Abstract
This quick reference was created for examiners in the field of computer and digital forensics. It can often be time consuming and inconvenient to drop everything you're doing to thumb through a 200 page book or scroll through a 200 page PDF for a quick reference during a Windows Registry analysis. This reference is by no means comprehensive, and an in-depth discussion of each topic is beyond the scope of this guide. All research was conducted in a Windows XP environment.

In addition, you should practice other established methods when conducting a forensic analysis. If you choose to explore the Windows Registry you do so at your own risk.

Quick Reference

Registry Hive Locations

As seen in regedt32.exe, the left-hand pane (also referred to 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.

The system files that correspond to each Registry hive.

Registry Hive	**Location**
HKEY_USERS	\Documents and Settings\User Profile\NTUSER.DAT
HKEY_USERS/.DEFAULT	\WINDOWS\system32\config\default
HKEY_LOCAL_MACHINE/SAM	\WINDOWS\system32\config\SAM
HKEY_LOCAL_MACHINE/SECURITY	\WINDOWS\system32\config\SECURITY
HKEY_LOCAL_MACHINE/SOFTWARE	\WINDOWS\system32\config\software
HKEY_LOCAL_MACHINE/SYSTEM	\WINDOWS\system32\config\system

Registry hives and their supporting files.

Registry Hive	**Supporting files**
HKEY_USERS	ntuser.dat, ntuser.dat.log
HKEY_USERS/.DEFAULT	default, default.log, default.sav
HKEY_LOCAL_MACHINE/SAM	sam, sam.log, sam.sav
HKEY_LOCAL_MACHINE/SECURITY	security, security.log, security.sav
HKEY_LOCAL_MACHINE/SOFTWARE	software, software.log, software.sav
HKEY_LOCAL_MACHINE/SYSTEM	system, system.alt, system.log, system.sav

System file extensions associated with Registry files.

Registry Hive	**Description**
No extension	A complete copy of the hive data
.alt	A backup copy of the SYSTEM hive, the only hive that associates a .alt extension.
.log	A log file that records the changes to key and value entries in the hive.
.sav	A copy of the hive file as it appeared during the initial installation of the OS.

Registry files and their typical content.

Registry File	**Content**
NTUSER.DAT	Protected storage for user, MRU lists, User's preference settings.
DEFAULT	System settings set during initial install of operating system.
SAM	Security settings and user account management.
SECURITY	Security settings.
SOFTWARE	All installed programs on the system and their settings associated with them.
SYSTEM	System settings.

Note: On Windows 98/ME machines the registry data is contained in two files, system.dat and user.dat, located in \Windows. There is also a user.dat file specific to every user profile in \Windows\profiles\user profile.

For more information on Registry structure in general:
http://msdn2.microsoft.com/en-us/library/ms724182.aspx

Time Zone Information
The TZI key is a critical reference for supporting a consistent timeline of evidence. There are certain values contained within this key that can help determine time zone and daylight savings time (DST) information, which may be necessary in converting UTC timestamps to local time. DST does not affect UTC time, but it can play a significant roll in determining local time.

HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Values of Interest:
ActiveTimeBias Bias DaylightBias StandardBias

Formulas of Interest:
UTC = Local Time + ActiveTimeBias Local Time = UTC – ActiveTimeBias Standard Time = Bias + StandardBias Daylight Time = Bias + DaylightBias

Note: Decimal values in the data field represents time in minutes. For more information on time zone information structure: http://msdn2.microsoft.com/en-us/library/ms725481.aspx

Time Stamp Structure
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.

Knowing the LastWrite time of a key could allow a forensic analyst to obtain 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. A comprehensive discussion of that process is beyond the scope of this reference, but I've compiled a couple tables to assist in this correlation:

File Properties

	Modified timestamp same	Created timestamp changes to current timestamp	Created timestamp same
Copy C:\FAT to C:\FAT\sub	X	X	
Move C:\FAT to C:\FAT\sub	X		X
Copy C:\FAT to D:\NTFS	X	X	
Move C:\FAT to D:\NTFS	X		X
Copy D:\NTFS to D:\NTFS\sub	X	X	
Move D:\NTFS to D:\NTFS\sub	X		X

Note: Modified timestamp does not change if the file is being moved or copied. It only changes when the properties of the file is changed.

Folder Properties

	Created and Modified timestamp same	Created and Modified timestamp changes to current	Created timestamp same, Modified timestamp changes	Created timestamp changes, Modified timestamp same	No Change
Create two new folders on NTFS	D:\NTFS D:\NTFS2				
Move D:\NTFS2 into D:\NTFS			D:\NTFS	D:\NTFS\NTFS2	
Copy D:\NTFS2 into D:\NTFS		D:\NTFS\NTFS2	D:\NTFS		D:\NTFS2
Copy D:\FAT2 into D:\FAT					D:\FAT2 D:\FAT

Note: On a FAT file system, the modified date doesn't change on a folder when the content of the folder is changed.

Autorun Locations

Autorun Locations are common locations where programs or applications are launched during the boot process.

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

A "Most Recently Used List" contains entries made due to specific actions performed by the user. There are numerous MRU list locations throughout various Registry keys. These lists are maintained in case the user returns to them in the future. Essentially, their function is similar to how the history and cookies act in a web browser.

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

Note: This list provides many common locations, but isn't comprehensive.
For additional MRU lists: http://windowsxp.mvps.org/RegistryMRU.htm.

UserAssist

This key contains two or more subkeys, which have long hexadecimal names or globally unique identifiers (GUIDs) and beneath each GUID is a subkey called Count. The Count subkey contains recorded values that pertain to objects the user has accessed on the system, such as Control Panel applets, shortcut files, programs, documents, media, etc.

HCU\Software\Microsoft\Windows\CurrentVersion \Explorer\UserAssist

These values, however, are encoded with the ROT-13 encryption algorithm. This 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 a ROT-13 decoder, such as http://www.edoceo.com/utilis/rot13.php.

Each encrypted name has a 16 byte hexadecimal value associated with it. The fifth byte (from left to right) is a counter that represents how many times the application has been launched. It is important to note that the counter starts at 5. Therefore, if the counter displays a 6, then the application has only been run one time. If the UserAssist key gets cleared, then the hex counter value will start over at 5. The last 8 bytes is the timestamp in UTC format. With this information one can see what program was launched, when it was launched and how many times it was launched.

Example:
As the key appears in UserAssist: HRZR_EHACNGU:P:\\Cebtenz Svyrf\\Nqbor\\Npebong 7.0\\Npebong\\Npebong.rkr Hex value: 24 00 00 00 15 00 00 00 40 0f 7b fa 8d 15 c8 01 (Hex value is not encrypted)
After the encrypted name has been decoded, such as with the tool mentioned above. UEME_RUNPATH:C:\\Program Files\\Adobe\\Acrobat 7.0\\Acrobat\\Acrobat.exe
Analyzing the hexadecimal address The **15** of the hex value shows that the application has been launched 10 times (15-5). The **40 0f 7b fa 8d 15 c8 01** is the timestamp information, which can be converted a number of ways. There is a great utility used for converting time stamps and can be found at: http://www.digital-detective.co.uk/freetools/decode.asp
Timestamp Conversion – UserAssist timestamps are 64bit hex values Tue, 23 October 2007 15:54:22 UTC
Conclusion Adobe acrobat has been launched 10 times and was last launched at 15:54:22 UTC

Note: FTK Registry Viewer and EnCase will decode ROT-13 automatically. Also note, the timestamp of the UserAssist key does not reflect the last time an object was run or created. The UserAssist key timestamp reflects the most recent GUID subkey that was created within it.

Wireless Networks

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.

HKLM\SOFTWARE\ Microsoft\WZCSVC\Parameters\Interfaces

When opening this Registry key there may be subkeys beneath it, like UserAssist, that look like GUIDs. The contents of these GUID subkeys 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."

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 server, domain, subnet mask, etc.

HKLM\SYSTEM\ControlSet001\ Services\Tcpip\Parameters\Interfaces\

Below this key there also may be GUID subkeys, as mentioned above. It's also important to note that there are timestamps associated with some of the values in this key. One, for example, is LeaseObtainedTime. This is the time in which the IP address was obtained from the DHCP server.

Example:
If there is a timestamp for LeaseObtainedTime of 471d1e69, a Unix 32 bit hex value, then it would translate to a Date & Time of Mon, 22 October 2007 17:04:25 UTC.

Note: If the computer is using vendor software to manage wireless connections then there may be additional locations where this information is stored, depending on the vendor.

LAN Computers

Windows XP implements a network mapping tool called My Network Place, which allows computers to easily find other computers within a LAN or Local Area Network. A computer on a properly configured LAN will record the Computer Name of all the computers on that network. Even after the computer is no longer connected to the LAN, the list of devices that have ever connected to that system still remains, including desktop computers, laptops, and printers.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions

USB Devices

Anytime a device is connected to the Universal Serial Bus (USB), drivers are queried and the device's information is stored in the Registry (i.e., thumb drives, cameras, etc.).

The following key contains subkeys that represent the device descriptor (Vendor ID, Product ID and Revision) of any USB device that has been connected to the system.

HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR

Beneath each of these device descriptors 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 as to whether or not it has been connected to other Windows systems.

Example:
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_I-Stick2&Prod_IntelligentStick&Rev_2.00\106C1141A2DC690F&0
The Vendor ID. Ven_I-Stick2
The Product ID. Prod_IntelligentStick
Revision. Rev_2.00
Device ID or serial number. 106C1141A2DC690F&0

Note: Harlan 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. For example: 6&1543608a&0

Mounted Devices

This key makes it possible to view each drive associated with the system. 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 that has been connected to that system.

HKLM\SYSTEM\MountedDevices

Internet Explorer

Internet Explorer stores its data in one key and has three subkeys within it that holds the majority of useful information.

HKCU\Software\Microsoft\Internet Explorer

The first subkey, Main, stores the user's settings in Internet Explorer. It contains information like search bars, start page, form settings, etc.

There is a form within this key that is interesting and pertains to the next section on Windows passwords. The form is called "FormSuggest PW Ask." If this value is "yes," then it is a good indicator that they have the Windows AutoComplete password feature enabled. If the user has unchecked the box to not ever remember passwords, then this value would be "no" and would not save the user's passwords. These passwords are saved in the SPW (SavedPassWords) key, which is discussed in the next section.

HKCU\Software\Microsoft\ Internet Explorer\Main

This next location stores all URLs that a user has typed into the address field of the web browser.

HKCU\Software\Microsoft\ Internet Explorer\TypedURLs

Note: If the user clears the history within the Internet Options window, it will delete the TypedURLs key entirely and it will not be recreated until a URL is typed into the address field again.

The next key displays the last directory used to store a downloadable file from Internet Explorer, which could give a fairly good idea as to where the user stores his/her files.

HKCU\Software\Microsoft\ Internet Explorer\Download Directory

Note regarding other web browsers: Opera, Netscape, and Firefox do not 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 in the default location C:\Documents and Settings\User Profile\Application Data\Opera\Opera\profile\. Like Opera, Netscape and Firefox leave limited registry footprints as well. 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\User Profile\Application Data\Netscape\NSB\Profiles \x.default\.

Windows Passwords

As stated above, if "FormSuggest PW Ask" within the Internet Explorer\Main key contains a "yes" value and the user tells the system to remember the password when they are prompted, then these Internet Explorer AutoComplete passwords are stored in the following key:

HKCU\Software\Microsoft\Internet Explorer\IntelliForms\SPW

If "FormSuggest PW Ask" contains a "yes" value and the user selects the AutoComplete option to NOT remember the password, the password is still logged in the Registry because the OS needs to refer to it in order to know not to ask the user to remember it again. These passwords consist of Internet Explorer protected sites, MSN Explorer, AutoComplete, and Outlook passwords. They are stored in the following key:

HKCU\Software\Microsoft\Protected Storage System Provider

Note: Passwords stored in either of these keys are encrypted by the Operating System. However, there are tools available that can decrypt these values, such as Protected Storage PassView by NirSoft or Helix's incident response tools.

P2P Clients
Two very popular P2P networks – Kazaa and Morpheus – record useful information in the Registry. Limewire is also a popular P2P network, but doesn't utilize the registry like Kazaa and Morpheus do.

Kazaa
There are two keys of interest. The first contains about 13 subkeys that show user specific settings:

```
HKCU\Software\Kazaa
```

Note: One of these subkeys is 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.

The second key that pertains to Kazaa that is worth mentioning holds connection information and the destination directory of downloaded files.

```
HKLM\Software\Kazaa
```

Morpheus
The Morpheus installation creates a Registry key that logs recently searched for keywords or phrases. A very useful key in seeing exactly the type of material the user was querying.

```
HKCU\Software\Morpheus\GUI\SearchRecent
```

Note: There is one key that all P2P applications should have 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, which was implicated in Service Pack 2. If the P2P programs weren't included in this list then they wouldn't be assigned a TCP or UDP port to access the P2P client's server, and they would consequently be blocked. Therefore, any type of program in use for file sharing purposes *should* appear on this list.

Instant Messaging Applications
Instant messaging applications can provide strong evidence in certain cases. A few of the most popular ones are AIM, MSN Messenger, Yahoo instant messenger, and ICQ.

AIM (AOL Instant Messenger)
The following Registry locations depend on the version of AIM in use. Here we will be looking into versions 5.9 and AIM6.

Version 5.9 - HKCU\Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\
AIM6 - HKCU\Software\America Online\AIM6\

Note: AIM6 does not seem to rely on storing information in the Registry as much as AIM 5.9 does. However, if a user checks the "save password" box when they login, the password will be stored in the Password key: AIM6\Passwords. The password is encrypted, but can be decrypted using Helix's incident response tool *Messenger Password*.

MSN Messenger or Windows Live Messenger
Windows Messenger, MSN Messenger, and Windows Live Messenger (which is the new MSN) generally utilize any of the three following keys:

HKEY_CURRENT_USER\Software\Microsoft\MessengerService
HKEY_CURRENT_USER\Software\Microsoft\MSNMessenger
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MessengerService

Yahoo! Messenger
The Yahoo! Instant messaging applications relies on the Windows Registry quite extensively as a configuration database. The following key is the basic root key where this information is stored. Below this key, the \Pager and \Profiles subkeys are probably the most relevant to an examination.

HKEY_CURRENT_USER\Software\Yahoo

ICQ
This is the basic root key where ICQ information is stored.

HKEY_LOCAL_MACHINE\SOFTWARE\Mirabilis\ICQ

Note: Even though Trillian and Pidgin (formally GAIM) are popular instant messaging clients, they act much like Firefox and Opera do in the browser world, where registry artifacts barely exist.

Final Note

Given the popularity of the Windows operating system œ in homes and businesses œ 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 fundamentals of the Registry from a forensics standpoint, an examiner can develop a more accurate account of what actions occurred on the given machine. As long as operating systems are dependent upon the Registry as a configuration database, there will always be other locations to discover that provide evidential support to an investigation. This Registry Quick Reference may not provide conclusive evidence in a Registry analysis, but it does present some examples and explanations of what types of data can be found, how they can be found, and why they may be relevant to an examination.

Resources

Books

Carvey, Harlan. Windows Forensic Analysis. Rockland, MA: Syngress, 2007.

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, "About the Registry (Windows)." Microsoft Developer Network. 01 Oct 2007. Microsoft Corp. 20 Oct 2007 < http://msdn2.microsoft.com/en-us/library/ms724182.aspx>.

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, "Description of NTFS date and time stamps for files and folders." Help and Support. 28 Feb 2007. Microsoft Corp. 27 Oct 2007 <http://support.microsoft.com/default.aspx?scid=kb;en-us;299648>.

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

Microsoft, "TIME_ZONE_INFORMATION Structure (Windows)." Microsoft

Developer Network. 01 Oct 2007. Microsoft Corp. 22 Oct 2007 <http://msdn2.microsoft.com/en-us/library/ms725481.aspx>.

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>.