Windows Forensics and Security

By: Adrian Leon Mare

Expert in Digital Forensic Investigation

8/27/2013

NVPI Lic 1498
www.ExpertDataForensics.com
702.435.8885 | 888.355.3888
The world we live in today is a technologically advanced world. While on one hand, commercialization of IT (Information technology) revolutionized our modern day lifestyle, it has raised a big question mark about the confidentiality and privacy of the information shared and managed using advanced means of communication.

As computer technology continues to evolve, the task of managing and handling private and sensitive information is becoming more and more challenging with each passing day. Increased rates of cyber crimes leading to unsolicited invasions of privacy have resulted in the emergence of a new field of computer science known as cyber forensics.

With the increasing demand of computer security in recent times, it has become more important than ever to understand the digital forensic technology.

**What is Digital Forensics/Cyber Forensics?**
Also known as cyber forensics, computer forensics involve the application of acquiring and analyzing digital information (as a part of structured investigation) to be used as evidence in the court of law.

**Digital Forensics-Primary Goals**
The primary goal of Digital Forensics is to carry out an organized and structured investigation in order to preserve, identify, extract, document and interpret digital information that is then utilized to prevent, detect and solve cyber incidents.

A typical forensic investigation consists of the following main steps:

1. Preserving the data.
2. Acquiring the data.
3. Authenticating the data.
4. Analyzing the data.
Figure 1: Steps involved in a Forensic Investigation Process

1. **Preserving and acquiring the data** - The first and foremost step of a digital forensic investigation is to preserve and acquire the data from a computer. The step involves creating a bit by bit copy of the hard drive data.

2. **Authenticating the data** - The next process involves verifying the data seized. To ensure that the acquired data is an exact copy of the contents of the hard drive, the md5/sha1 of the original and copied data are checked and matched.

3. **Analyzing the data** - This is perhaps the most important part of the investigation process which involves careful examination and analysis of the data using forensic tools.

   The process mainly involves:
   - Recovering deleted files /Data Recovery
   - Tracking or identifying hacking activities

**Digital Forensics and Windows**

21st century is the century of revolution and change. The transformation of the analog world into a digital world has raised new challenges and opportunities for technology lovers.

New forensic challenges arise with the introduction of newly released and latest operating systems. While on one hand, these newly released versions of Windows are aimed at making things easier for users, many of the functions (such as auto play, file indexing) performed by your operating system for your convenience can actually be used against you.

If you look at the current cyber crime statistics, you will notice that the highest percentage of cyber crimes is committed in the United States of America. 23% of the total cyber crimes take place in U.S. This calls for increased security measures to protect your confidential information from being misused.
The average user is mostly unaware of the fact that their newly upgraded operating system is leaving tracks of their activity. It is essential for users to know that valuable pieces of sensitive and confidential information is stored in Windows Artifacts. These artifacts can be used to recreate and restore the account history of a particular user.

**Digital Forensics and Windows-The Windows Artifacts**

Some of the artifacts of Windows 7 operating system include:

- Root user Folder
- Desktop
- Pinned files
- Recycle Bin Artifacts
- Registry Artifacts
- App Data Artifacts
- Favorites Artifacts
- Send to Artifacts
- Swap Files Artifacts
- Thumb Cache artifacts
• HKey Class Root Artifacts
• Cookies Artifacts
• Program files Artifacts
• Meta Data Artifacts
• My Documents Artifacts
• Recent Folder Artifacts
• Restore Points Artifacts
• Print Spooler Artifacts
• Logo Artifacts
• Start menu Artifacts
• Jump lists

Information collected from any of these artifacts can be used to recreate the account history of a user. To gain a better understanding of how these artifacts can be used to access or retrieve valuable information, it is essential to briefly discuss some of the most important Artifacts of Windows 7.

1. Root User Folder artifacts
The Root User Folder gives access to the complete operating system. The Root User reserves the right to delete and modify files on the operating system besides having the rights to generate new users and award them some rights. Nonetheless, these rights cannot exceed the rights of a root user.

The Windows Folder is specified by %SYSTEMROOT%. The Folder can be accessed through Start\Run\%SYSTEMROOT%\System32.

2. Desktop Artifacts
All the files present on the desktop of a user are stored in the desktop folder of the operating system. Typically, the desktop is populated either,

• By the user, or
• By programs that automatically create files and place them on the desktop.

The Desktop can be accessed using the following link;
C:\\USERS\username\desktop

3. Pinned Files/Jump Lists Artifacts
Pinned Files or Jump lists is a relatively new feature introduced in Windows 7 released by Microsoft. Using the Jump lists all the pinned files can be accessed. Additionally, these lists also maintain a record of recently or last visited files relative to a particular software. Pinned files can be accessed from the jump list using the following link,
C:\Users\username\AppData\Roaming\Microsoft\InternetExplorer\QuickLaunch\UserPinned\TaskBar.
4. Recycle Bin Artifacts
The Recycle Bin stores the recently deleted files temporarily. These files can be restored easily. You can only view the Recycle Folder after un-checking the hide\protect system files option using the following link;
C:\$recycle.bin

5. Registry Artifacts
Registry is the location where the configuration information of Windows is kept and stored. It can be used to obtain information related to historical and current use of applications in addition to obtaining valuable pieces of information about option preferences and system settings. It can be accessed using the following link;
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

6. App Data Artifacts
Application data or App data is a junction designed to provide backward compatibility. A junction can roughly be defined as a shortcut that serves to redirect programs and files to different locations. All the information related to settings configuration (of various apps) is stored in this folder. Furthermore, information related to the Windows address book and recently accessed files are also stored in this folder. The junction can be accessed through:
C: User\ (username)\AppData\Roamingfolder

7. Favorite Artifacts
The folder contains valuable bits of information related to Windows Explorer and Internet Explorer favorites. The folder can be accessed using the following link;
C:\ USERS\username\favorites.

8. Send To Artifacts
The Send to folder stores information pertaining to shortcuts to different locations, and other software apps on the operating system of your computer. These shortcuts serve as destination points. Using these destination points a file can be sent or activated. Furthermore, these points can also be modified as per your convenience. The Send to folder can be accessed using the following link;
C:\Users\username\AppData\Roaming\Microsoft\Windows\SendTo

9. Swap Files Artifacts
Page Files or Swap files are the memory files of your computer that aid in expanding the memory of your computer. These files are not visible and are hidden by default settings. To view these files, following link can be used;
10. **Thumbs Cache Artifacts**
Thumbs.db files are files that are stored in every directory on the Windows systems that includes thumbnails. These are default files (created by default) and store valuable information that is not available elsewhere. The file is created locally amongst the images. The location where cache is stored is as follows;

C:\Users\Username\AppData\Local\Microsoft\Windows\Explorer

The display can be stopped by a user by checking on the ‘Always show icon, not thumbnails’ from the list of Folder options.

11. **HKEY Class Root Artifacts**
The HKEY Class Root or simply HKCR key contains sensitive information about different file name extensions in addition to containing information related to COM class registration. Furthermore, it is designed to be compatible with the 16-bit Window registry.

HKEY _LOCAL_MACHINE and HKEY_CURRENT_USER key both store valuables information related to file name extensions and class registration.

HKEY_LOCAL_MACHINE\Software\Classes: This key stores all the information pertaining to different users using the system.

The HKEY_CURRENT_USER\Software\Classes: On the other hand, this key stores information pertaining to the interactive user.

12. **Cookies Artifacts**
A number of websites store information on your computer in the form of cookies. Cookies can roughly be defined as small text files containing information related to preferences and configuration of a particular user.

These files can be accessed using the following link;

C: User\{username}\AppData\Roaming folder\ Microsoft\Windows\Cookies.

13. **Program Files Artifacts**
Windows 7 consists of two Program files folders including;

1. C:\program files
2. C:\Program files (x86)

These folders are designed to be compatible for 32 bits and 64 bits version of Windows 7. The first one is compatible with the 64 bit version of Windows 7, whereas, the second one is compatible with 32 bit version of Windows 7.
14. **Meta Data Artifacts**
Meta Data simply refers to information related to data itself. Using the metadata artifacts, valuable strings of file information can be obtained that can be used as evidence in digital forensic investigation.

15. **Restore Points Artifacts**
Windows & gives its users the option of restoring points thereby creating the image of your system. This essentially helps in providing users with an option to revert back to the point when the system was working perfectly in case of fatal system errors. This system image also contains the drives that are required by your operating system to run in addition to including program settings, system settings and file settings.

16. **My Documents Artifacts**
My Documents contains all the information related to files that have been created by users themselves. Usually when a program is installed on a system, the information is stored in this folder. It is also known as the primary storage space meant for storing all the key information. The folder can be accessed through;

C:\Users\username\MyDocuments.

17. **Start Menu Artifacts**
The traditional Start menu has been replaced by Start in Windows 7. Using software like classic shell, it is absolutely possible to get the menu back. In Windows 7, the right column of the start (new version of start menu), links to respective libraries are shown instead of folders.

18. **Logo Artifacts**
The Logos included in the Windows 7 Operating System include valuable information pertaining to application events information, security related events information, setup event information, forwarded event information, and application events information.

19. **Print Spooler Artifacts**
Print Spooler is a software program responsible for organizing all the print jobs that have been sent to the print server or the computer printer. In essence all the print related information is stored in this folder.

The folder can be accessed by using the following link;

C:\Window\System32\Spool\Printers.

20. **Recent Folder Artifacts**
The Recent Folder stores links of the recently accessed or opened files by a specific user. The folder can be accessed by using the following link;

C:\Users\username\AppData\Roaming\Microsoft\Windows\Recent.
Windows Forensics - Analysis of Windows Artifacts

Analysis of Windows artifacts is the perhaps the most crucial and important step of the investigation process that requires attention to detail.

The following flowchart depicts a typical windows artifact analysis for the collection of evidence.

Fig: 3 File Downloads

Fig: 4 Program Execution
FILE OPEN/CREATE

- Save/Open MRU
- Most Recently Visited (MRU) files
- Recently Opened Files/MS Office files
- Shell bags
- LNK Shortcut Files/Jump lists
- Prefetch, Index.dat file://

Fig: 5 Program Execution

PHYSICAL LOCATION

- Time Zone
- Network History
- Cookies
- Search Terms Used On Browser

Fig: 6 Physical Location Information

USB USAGE

- Key Identification
- First and Last Time Usage
- User History
- Volume Serial Number of the USB
- LNK Shortcut Files

Fig: 7 USB Usage Details
ACCOUNT USAGE

- Last Login Details
- Recent Passwords Change
- Successful/Failed Attempts
- RDP Usage (Remote Desktop Protocol)

Fig: 8 Account Usage Details

DELETED FILES

- ACMRU-Search Assistant
- Recently Visited MRU
- Thumbs.db
- Recycle Bin
- Index.dat files://

Fig: 9 Deleted Files

End