A Review of Forensic Artifacts in a Windows 8 Environment

Mohit Soni
ASAS,
Amity University
Haryana

Seema R. Pathak
ASAS
Amity University
Haryana

ABSTRACT
Forensic artifacts refer to bits of information that an operating system records, when a user is using his computer system. These bits of data are user/session specific and provide all information regarding the use of a particular application or program along with the necessary time stamps. A digital forensic investigator needs to be aware of such artifacts in order to perform a legally acceptable, accurate and tool-independent analysis of a questioned system. This paper provides a comprehensive review guide for all forensic artifacts available in a Windows 8 environment. These artifacts supply both conclusive and probative evidence to an investigator and form vital preliminaries of incident response in a digital crime scenario.

General Terms
Digital Forensics

Keywords
Artifacts, Digital Forensics Analysis, Incident Response, Log Files, MAC, Pathway, Probative Evidence, Registry, Timestamps, Windows 8

1. INTRODUCTION
Windows 8 is built for personal computers (touch & otherwise), tablets & smartphones. The Metrostyle interface is the brand new development windows is planning to base further operating systems on. It is a key feature which suits both touch and traditional mouse and keyboard inputs. Windows 8 has a tile based screen in which each tile represents an application and its relevant information. The user is unaware that the operating system registers traces of their activity, specific to their usage. This stored information contains probative information known as "Artifacts". By knowing where these artifacts are stored can assist crime scene reconstruction in forensic analysis[19]. These artifacts find great use in forensics analysis. Digital forensic scientists can employ these in incident response scenarios or lab analysis. This paper is a compilation of several reviews and proceedings of such artifact based studies. Each artifact, along with the relevant forensic information it supplies, is stated individually in Section 2.

2. ARTIFACTS

2.1 Metro Apps
Metro apps connects to the internet with a windows live(Microsoft) account. It has new immersive concepts. One application can access other app& the following app becomes an operating system [16]. Windows 8 forensic artifacts of Metro app can be found in App data folder.

2.1.1 Forensics Relevance
Metro app's cache, cookies and history are very useful to a forensics investigator as it provides information about the used app.This forensically relevant data can be accessed by an investigator through the below mentioned paths. Figure 1 shows the screen shot of the relevant location for Metro Apps [19].

Metro App Cache

%Root%\Users\%User%\AppData\Local\Packages\%MetroAppName%\AC\INetCache

These contain Web cache of Metro Apps. Fig 1 shows Metro app Bing's cache files

Metro App Cookies

%Root%\Users\%User%\AppData\Local\Packages\%MetroAppName%\AC\INetCookies Contains cookie files of Metro App. It is in a text file.

Metro App History

%Root%\Users\%User%\AppData\Local\Packages\%MetroAppName%\AC\INetHistory

It contains history files of each metro app.

Figure 1: Cache files of Microsoft's Metro app Bing

2.2 Internet Explorer 10
IE 10 is a latest version of Internet Explorer. It has two states-immersive and desktop [19]. Both leaves the traces about the URL's accessed in different locations.

2.2.1 Forensics Relevance
Information from both (immersive and desktop),along with date & time stamps can be found in the below mentioned locations [19].

ImmersiveIE 10 Web sites Visited %Root%\Users\%User%\AppData\Local\Microsoft\InternetExplorer\Recovery\Immersive\Active Desktop IE 10 Web sites Visited%Root%\Users\%User%\AppData\Local\Microsoft\InternetExplorer\ Recovery\Active

2.3 Communication Apps

Communication App contains application in which a user can communicate with others. It includes Twitter, Facebook, chats, e-mails and other social networking websites.

2.3.1 Forensics Relevance

For applications like Facebook a web cache contains information like profile pictures and other pictures which were visited by the user[19]. It leaves traces of user's chats and e-mail conversations. Such snippets could supply probative evidences. These can be found at the below mentioned locations:

Communication App Web Cache
%Root%\Users\%User%\AppData\Local\Packages\microsoft.windowscommunicatisapps_8wekyb3d8bbwe\AC\INetCache
Communication App Cookies
%Root%\Users\%User%\AppData\Local\Packages\microsoft.windowscommunicatisapps_8wekyb3d8bbwe\AC\INetCookies
User contacts are synchronized with all other social media accounts like Facebook, e-mail, and Twitter. All synchronized addresses linked to a contact that can be found under this location [19]. Contacts are generated and user tile is assigned to a particular contact. Fig. 2 shows a screenshot of the user tiles linked to each contact. Fig 3 shows user tile associated with contact. The path way to access the same is below:

User's Contacts from Communications Apps%Root%\Users\%User%\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\LiveComm\%User'sWindowsLiveEmailAddress%\%AppCurrentVersion%\DBStore\LogFiles\edb####.log.

User Tile Associated with Contact
%Root%\Users\%User%\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\LiveComm\%User'sWindowsLiveEmailAddress%\%AppCurrentVersion%\UserTiles

Figure2: User contacts

2.4 Registry

It is a central database of windows system. It stores values in binary. Registry is a set of discrete files called hives. Each hive contains a Registry tree, which has a key that serves as the root (i.e., starting point) of the tree. *Subkeys* and their values reside beneath the root [2]. These fragments can be used to rebuild a damaged Registry file or to reconstruct the previous state of a Registry file. They can also stand on their own as items of evidence [19]. Timeline of typed URL'skey is added and updated in a windows registry when types directly or copy paste into address bar. But it does not update when user clicks on a link. It shows intentionally work is done by user. It will save maximum 25 entries, when 26th entry is made, the first entry is deleted to make space for newly added data [3][13]. User Assist key has values in subkeys that relate to each item executed on the system. Registry name are encoded using ROT13 algorithm also known as Caeser cipher. The registry value of windows 8 are 72bytes values. This key contains two GUID subkeys. Each subkey maintains a list of system objects such as program, shortcut, and control panel applets that a user has accessed. The GUID subkey beginning with "5E6" corresponds to IE toolbar, while subkey starting with "750" pertains to Active Desktop .The Typed URL Time is stored in binary and represents the number of 100-nanosecond intervals [2]. The new feature in Windows8 is Volume Shadow copy Service (VSS) also called File History. It is a set of COM APIs that implements a framework to allow volume backups to be performed while applications on a system continue to write to the volumes [12].

Figure 3: A user tile associated with user's contact

2.4.1 Forensic Relevance

Registries are the most relevant of all artifacts. These provide a wide range of information. Registry can supply information about all user timeline activity such as applications installed and open, windows position andsize, MACtimes and values (Modified,Accessed Created). They can also supply the configuration of the system. Several location in a Windows 8 environment supply different information fromthe system's registry [9].

2.4.1.1 NTUSER.dat

NTUSER.dat is a private system file of user. If there are multiple users there will be multiple registry entries [19][7].

%SystemRoot%\Users\%User%\NTUSER.DAT\Software\Microsoft\

Recent Docs

Windows\CurrentVersion\Explorer\Recent Docs

Recently Opened/Saved Folders

Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Last Visited Folder

Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRULegacy

Recently Used Apps (Non-Metro Apps)

Windows\CurrentVersion\Explorer\ComDlg32\CIDSizeMRU

Recently Used Apps with Saved Files

Windows\CurrentVersion\Explorer\ComDlg32\FirstFolder

Recently Run Items

Windows\CurrentVersion\Explorer\Policies\RunMRU

Computer Name & Volume S/N

Windows Media\WMSDK\General

File Extension Associations

Windows\CurrentVersion\Explorer\FileExts

2.4.1.2 Typed URL's

Microsoft\Internet Explorer\TypedURLs
Typed URL Time
Microsoft\Internet Explorer\TypedURLsTime

2.4.1.3 Windows Explorer

Windows Explorer is the default GUI shell.Activities performed in this shell can also be used as an artifact. Different information is available at several location. These are specified below [15].

Recently opened files from Windows Explorer
C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent.
Network Shortcuts
C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Network Shortcuts
Items recently ran from the "Run" bar
KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU.

ComDlg32 recently opened/saved files
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU.
ComDlg32 recently opened/saved folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU.
Recent Docs
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
EXE to main window title cache
HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache

User Assist
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

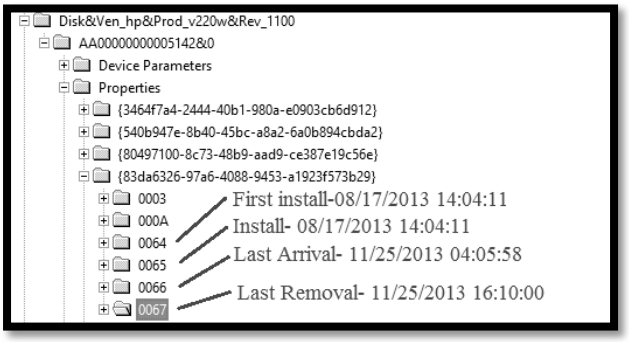

Figure 4: Device Timestamp

2.4.1.4 SAM

Security Accounts Manager contain local user names and their encoded passwords hives.Security identifiers(SIDs) and Relative Identifiers (RIDs) are used in SAM file [19].

Forensically, it contains System user's group account information like logon and their passwords.
%SystemRoot%\Windows\System32\Config\SAM\Domains\Account\Users

2.4.1.5 SYSTEM

The SYSTEM key control set contains device driver and service configurations.
Forensically an investigator can identify the System Name , Last Shutdown Time, Time zone and Hardware information(floppy present, drives present, human interface devices, LPT ports, Storage Devices, USB storage, Mounted Device, Clear page file, Memory on shut down, network connection, process id) [6] [17].

%SystemRoot%\Windows\System32\config\SYSTEM\
MountedDevices
%CurrentControlSet%\Enum\SWD\SensorsAndLocationEnum\HardwareID.
USB Storage Devices
%CurrentControlSet%\Enum\USBSTOR
%CurrentControlSet%\services\Tcpip\parameters\interface\GUID%CurrentControlSet%\control\session manager\MemoryManagement

Timestamps for Devices
Last Insertion Date, Device **Last Removal** Date and Install Date. This information is located under SYSTEM hive. Figure 4 shows the screenshot of Device's Timestamp information. The path are specified below.
CurrentControlSet\Enum\DeviceType\DeviceID\InstanceID\{GUID}\Properties\xxxx

2.4.1.6 SOFTWARE

The SOFTWARE key contains information about the operating system, such as the version, when it was installed, who is the registered owner, who was the last user to log on, and who are the members of a group (if there is one).

Forensic Relevance

It contain information about Class Identifiers (CLSIDs) and user profiles. Software set too Run On startup and evidence of uninstalled software can be trace out from here. The various settings key like Recycle Bin Settings, Wireless Connection,Autologonsettings, Application Restrictions (winlogon restriction) are also found in this. The interesting key of Cached Password Enabled also seen otherwise normally user not be able to see anywhere in the system [6] [14].

%SystemRoot%\Windows\System32\config\SOFTWARE\

Metro Apps Installed on System

Microsoft\Windows\CurrentVersion\Appx\AppxAllUserStore\Applications

User Account Installed Metro Apps

Microsoft\Windows\CurrentVersion\Appx\AppxAllUserStore\%SID%

Applications that Run at Startup

Microsoft\Windows\CurrentVersion\Run

Lists command to be run each time cmd.exe is run

HKLM\SOFTWARE\Microsoft\Command Processor

This key has a registry value named Shell with default data Explorer.exe.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

This key contain information about wireless network

HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interface\GUID

Services used by Microsoft Products to Provide secure private information. HKLM\SOFTWARE\Microsoft\Protected storage system Provider

2.4.1.7 UserAssist

It stores last executed time in 8 Bytes File time values and executed counts. Some malicious tool changes system date and time information can be identified by the analysis. These also let us know how long user has interacted with a given program and from whence items were being launched most often [3].

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Userassist
{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
{CAA59E3C-4792-41A5-9909-6A6A8D32490E}
{B267E3AD-A825-4A09-82B9-EEC22AA3B847}
{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}
{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}

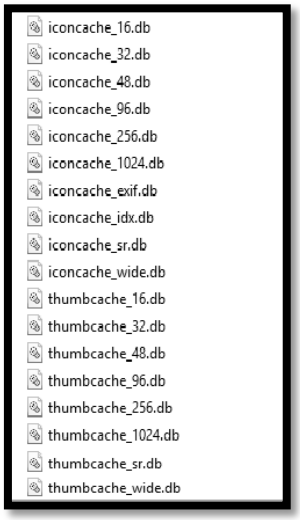

Figure 5: Thumb-Cache and Icon-Cache in Windows 8

2.5 Shadow copy volume (shadow copy forensics)

Forensically, system refresh and restore points can be utilized to obtain all information carried to the systems at a previous point in time [3] [10] [4]. The path way to reach the same is:

HKLM\software\MS\WindowsNT\Currentversion\systemrestore%root%\windows\system32\VSSadminlistshadows

2.6 User pinned Application

User can pin any application to Desktop. It contains link files [19]. These link files can be found following the below path:

%Root%\Users\%User%\AppData\Roaming\Internet Explorer\Quick Launch\UserPinned\TaskBar

2.7 Jump Lists

Jump lists are list of recently and frequently accessed files, folder and applications.

Forensics Relevance
It gives artifacts of user's recently accessed files,folder and applications. If any application opens a file and if that application is deleted from the system then still jump lists contains information after the application was removed [1] [18].Jump lists information can be found under the below folder.

%Root%\Users\%User%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\
%Root%\Users\%User%\AppData\Roaming\Microsoft\Windows\Recent\CutomaticDestinations\

2.8 Thumbnail cache and Icon cache

Thumbnail cache is used to store thumbnails of an images. It saves the time and speed up the display of images [19] [8]. File name is like *Thumbnailcache_xxxx.db*. Number shows the size of thumbnail. The *Thumbnailcache_32.db* files stores the thumbnail of 32*32 pixel's size.

Forensics Relevance
One can retrieve deleted images.
Iconcache stores the copy of Icons. So windows can used that database to retrieve icon faster [5]. Figure 5 shows the list of thumbcache and iconcache.

Forensics Relevance
When USB connected to any system, if executable file is invoked or not it will create artifacts in iconcache.db files [11].

%userprofile%\AppData\Local\Microsoft\Windows\Explorer\thumbcache_xxxx.db (numbered by size)

%userprofile%\AppData\iconcache.db
%userprofile%\AppData\Local\Microsoft\Windows\Explorer\Iconcache_xxxx.db (numbered by size).

3. CONCLUSION

All window artifacts provide differentially usable information. Some are conclusive while others can be of probative value. It is vital for a digital forensic investigator to be acquainted of all of them in order to carry out an accurate investigation. In our opinion, windows registry is an excellent source for potential evidential data. Knowing the type of information that could possible exist in registry and its location can give a forensic examiner the necessary edge in a forensic analysis process.

4. REFERENCES

[1] Carvey H. Jumplistsanalysis, Windows Incident Response Blog, August 172011 http://windowsir.blogspot.in/2011/08/jump-list-analysis.html

[2] Carvey H. Registry analysis, SANS Forensics summit 2009, Accessed on 2014 October 15http://computer-forensics.sans.org/summit-archives/2009/8-harlan-carvey-registry-analysis.pdf

[3] Farmer D. A forensics analysis of the windows Registry.-Accessedon2013October22http://eptuners.com/forensics/contents/examination.htm

[4] Harrell C. Volume Shadow Copy Timeline, Journey into incident response Blog, Sunday, March 25, 2012

http://journeyintoir.blogspot.in/2012/03/volume-shadow-copy-timeline.html

[5] How to repair Windows desktop icons with AB Commander,Wednesday,May4th,2011http://www.winability.com/info/icon-cache/

[6] Farmer D., "A Forensic Analysis of Windows Registry", Forensic Focus 2014http://www.forensicfocus.com/a-forensic-analysis-of-the-windows-registry

[7] Lee R., "Digital Forensics and Incident Response Poster"22nd Edition' 2012 http://computer-forensics.sans.org

[8] Mueller L., "Windows 7 Forensics Thumbcache_*.db". PostedJanuary10th,2010http://www.forensickb.com/2010/01/windows-7-forensics-part-iv.html

[9] Wong WernL., "Forensic Analysis of Windows Registry", Accessed 23rd December' 2014, http://www.forensicfocus.com

[10] Johnson K.' "Windows 8 recovery forensics", SANS DFIASUMMIT2012.https://computerforensics.sans.org/summit-archives/2012/windows-8-recovery-forensics-understanding-the-three-rs.pdf

[11] Collie J., "The windows IconCache.db: A Resource of Forensic Artifacts from USB connectable devices", Vol.9, Issue 3-4, Digital Investigation, Elsevier 2013, Pg. 200-210.

[12] Johnson K.W., "Windows 8: Recovery Forensics", : In Proceedings of SANS DFIR Summit 2012https://digital-forensics.sans.org/summit-archives/2012

[13] Koepi D., "Taking One Byte at a Time", Posted September29,2013https://davidkoepi.wordpress.com/category/windows-artifacts/

[14] Lee R., "Windows 7 Computer Forensics", SANS Digital Forensics and Incident Response Blog, Posted October 27th 2009http://digitalforensics.sans.org/blog/2009/10/27/windows-7-computer-forensics

[15] "Managing Roaming User Data Deployment Guide ", accessed December 25th2014https://technet.microsoft.com/en-us/library/cc766489%28v=ws.10%29.aspx

[16] Miller J.M., "Build: More Details On Building Windows 8 Metro Apps", Forward Thinking, PC Magazine September 2014 http://forwardthinking.pcmag.com/show-reports/287736-build-more-details-on-building-windows-8-metro-apps

[17] "Windows Sensor and Location Platforms":accessed on October 10th 2014http://archive.msdn.microsoft.com/

[18] Lynes R., " Forensic Analysis of Windows 7 Jump Lists", Forensic Focus , created October 30th, 2012.http://articles.forensicfocus.com/2012/10/30/forensic-analysis-of-windows-7-jump-lists/

[19] Thomson A.C.F, "Windows 8: Forensic Guide", Windows8ConsumerGuide2012https://propellerheadforensics.files.wordpress.com/2012/05/thomson_windows-8-forensic-guide2.pdf