File downloaded:

Open/Save MRU

Description:
In simplest terms, this key tracks files that have been opened or saved. It not only including web browsers such as Internet Explorer and Firefox, but also a majority of commonly used applications.

Location is registry:
Command: -
reg query
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU

In place of HKEY_CURRENT_USER search for NTSUER.DAT

Email Attachments

Description:
The email industry estimates that 80% of email data is stored via attachments. Email standards allow only text. Attachments must be encoded with MIME/base64 format

Check Path:
Command: -
Cd %USERPROFILE%\AppData\Local\Microsoft\Outlook

MS Outlook data files found in these locations include OST and PST files.
OST (Offline Storage Table) and PST (Personal Storage Table) files are commonly used by Microsoft Outlook to store email, calendar, contacts, and other data. OST files are used in cached mode to allow offline access to mailbox data, while PST files are used to store mailbox data locally.

Command: -
copy "OriginalFilename.ost" "DestinationPath"

Analysis Tools:
To perform forensic analysis on OST and PST files,
FTK, ENCASE, MailXaminer, Kernal for OST viewer

Skype History

Description:

Skype history keeps a log of chat sessions and files transferred from one machine to another.
Location of Path:
Command: -
C:\Users\<usemame>\AppData\Roaming\Skype\<skype-name>

Downloads. SQLite (or SQLite Database for Browsers)

Firefox

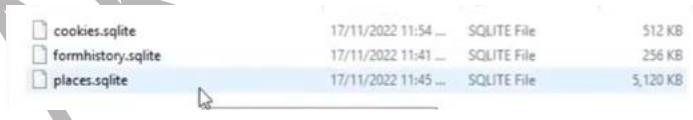
Description:
Firefox has a built-in download manager application that keeps a history of every file downloaded by the user. This browser artifact can provide excellent information about the sites users have been visiting and the kinds of files they have been downloading from them.

Location: Firefox:
Command: -
cd %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles

after that of you do
DIR: you get \<random text>.default
DIR: you get SQL Database

Analysis Tool:
One such tool is "DB Browser for SQLite" (previously known as "SQLite Database Browser"). You can download and install it from the official website.
https://sqlitebrowser.org/dl/
Understanding you can use YouTube.
https://www.youtube.com/watch?v=RKgGa6Rc2N8&ab_channel=Moss%C3%A9CyberSecurityInstitute

https://www.epochconverter.com/
Convert SQL data base time stamp into human readable.



Downloads. SQLite: if you find analyse that it contains.
Filename, size, and type
• Download from and referring page
• File save location
• Application used to open folder
• Download start and end times

Index.dat/ Places. SQLite: Details stored for each local user account. Records number of times visited (frequency).

Location: Internet Explorer
Command: -
cd %userprofile%\AppData\Local\Microsoft\Windows\History\Low\History.IE5

Location: Chrome
Command: -
cd %userprofile%\AppData\Local\Google\Chrome\User Data\Default

gather artifacts like

- Browsing history (`History` file)
- Cache (`Cache` directory)
- Cookies (`Cookies` file)
- Bookmarks (`Bookmarks` and `Bookmarks.bak` files)
- Downloads (`History` file)
- Extensions (`Extensions` directory)
- Autofill data (`Web Data` file)

(the thing is collecting artifact from FTK is little issue because it generate image in .ad1 form and autopsy don't allow to use that image for analyses so Still finding way to capture memory and analyse as soon as I find tool I will write but these artifacts must be captured for analysis)

Note: - you can use SQL database for analyses you have to just copy file to another location

*******Tools for collection these artifacts:***

1. ***Unleashing Kape: A Forensic Powerhouse***

For a comprehensive approach to artifact gathering, Kape emerges as a potent tool. With its versatility, Kape can efficiently collect browser artifacts, providing investigators with a unified dataset for analysis.

2. ***Taking Artifacts Home: A Command of Copy(Manually copying artifacts)***
Whether using Kape or opting for a manual approach, the command

Command :- copy "C:\Users\<YourUsername>\AppData\Local\Google\Chrome\User Data\Default\History" "C:\Path\To\New\Location\HistoryCopy"

*allows forensic analysts to copy artifacts for further analysis. The subsequent use of SQLite3 facilitates in-depth examination******

Program execution:

Last Visited MRU

Description:
Tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key. In addition, each value also tracks the directory location for the last file that was accessed by that application.

Location: Path
Command: -
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

You can use registry as well.
Reg Query
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU
Can use HKLM as well.

From command prompt:
Reg Save
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU C:\Users\User\Downloads\output.hiv

(To Save hive details into hive file for further analysis)

Analysis Tool:
One such tool is reg-ripper/Registory explorere which will tell hive is dirty or not // other you can use REcmd/Kape.

Application Compatibility Cache (Shimcache)

Description:
Tracks the executable's filename, file size, last modified time, and in Windows XP the last update time.
*****Forensic analysts should note that the most recent events are listed at the top, and new entries are written only on system shutdown. Entries are committed to the registry during shutdown or, in Windows 10, during a reboot*****

Location: Registry
Command: -
reg query "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\AppCompatCache"

Analysis Tool:
Such tool is you can use AppcompatcacheParser.exe. you can also use registry editor/Registry explorer.
Amcompatcacheparser give you output in excel file you can learn if you want from your inventory.
https://www.cyberengage.org/post/shimcache-amcache-analysis-tool-appcompactcacheparser-exe-amcacheparser-exe

https://www.cyberengage.org/post/amcache-hiv-analysis-tool-registry-explorer

Any executable ran on the Windows system can be found in this key. You can use this key to identify systems that specific malware was executed on. In addition, based on the interpretation of the time-based data, you might be able to determine the last time of execution or activity on the System.

Prefetch

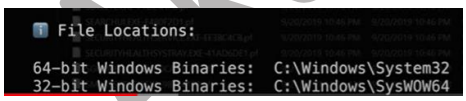
Description:
Increases performance of a system by preloading code pages of commonly used applications. Cache Manager monitors all files and directories referenced for each application or process and maps them into a .pf file. Utilized to know an application was executed on a system.

The Prefetch directory maintains a collection of .pf files, each generated after the first execution of an application.

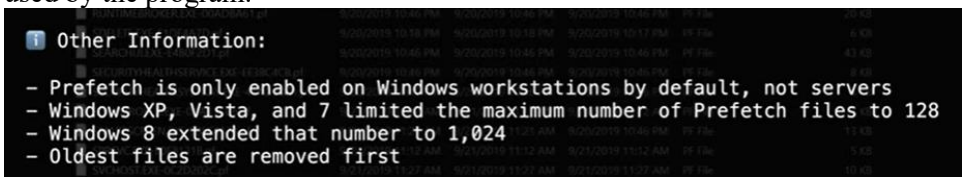
https://www.cyberengage.org/post/prefetch-analysis-tool-pecmd-exe

Example:
(exename)-(hash).pf

Location: Path
Command:
cd C:\Windows\Prefetch



Each .pf will include the last time of execution, number of times run, and device and file handles used by the program.



Note: Any Valid Svchost.exe process should have -k parameter followed by 1 or more value:

Analysis Tool:

Such tool like PECmd can be used to parse .pf files.
https://www.cyberengage.org/post/prefetch-analysis-tool-pecmd-exe

Each .pf will include the last time of execution, number of times run, and device and file handles used by the program.
Date/Time file by that name and path was first executed.
Date/Time file by that name and path was last executed.

Jump Lists

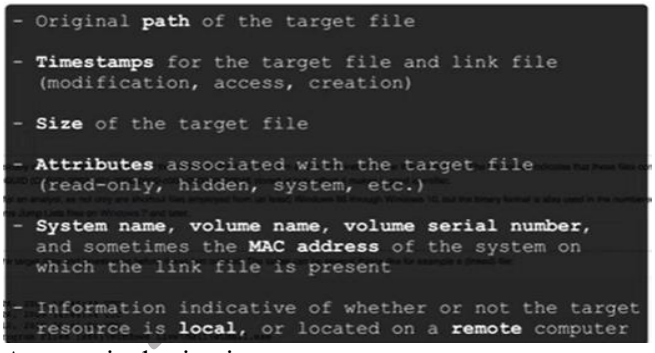
Description:
Jump Lists represent a dynamic feature engineered to empower users by granting them swift access to frequently or recently used items. This functionality extends beyond mere media files, encompassing recent tasks as well. Whether it's opening a favorite document or resuming a recent project, Jump Lists facilitate seamless navigation and productivity.

https://www.cyberengage.org/post/unveiling-the-significance-of-jump-list-files-in-digital-forensics

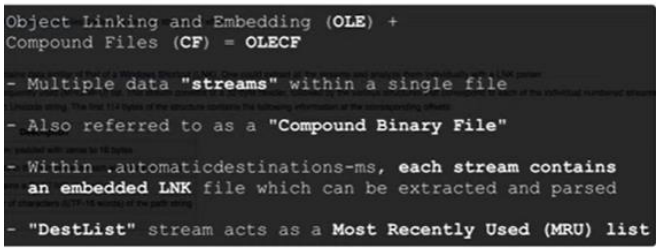
Location: Jump List
Command:
cd C:\Users\<User>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
cd C:\Users\<User>\AppData\Roaming\Microsoft\Windows\Recent\ CustomDestinations

Copy Artifacts: *(Manually copying artifact and taking home to analyze)(from live system) copy*

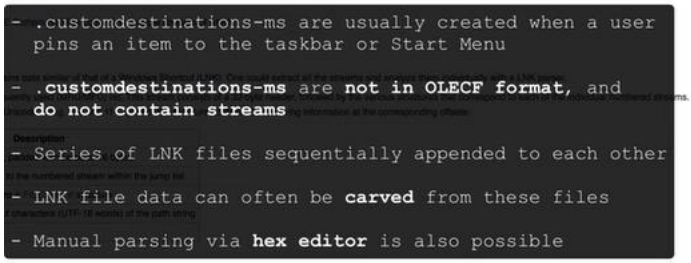
*"C:\Users\User\AppData\Ro*aming\Microsoft\Windows\Recent\AutomaticDestinations*"
"C:\Users\User\Downloads\artifact"



Automatic destinations



Custom



Jump list naming is like
de48a32edcbe79e4.automaticDestinations-ms
de48a32edcbe79e4. (This part is App ID) this ID is for application you can check the id here. That which app it belongs to
https://github.com/EricZimmerman/JumpList/blob/master/JumpList/Resources/AppIDs.txt

Analysis Tool:
we have multiple tool to analyse For Jumplist we can use JLECmd or JumpList explorer GUI version.

https://www.cyberengage.org/post/jump-list-analysis-tool-jlecmd-exe

RunMRU Start->Run

Description:
Whenever someone does a Start -> Run command, it will log the entry for the command the person executed.

Location: NTUSER.DAT HIVE
Command:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Reg Save HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU C:\Users\User\Downloads\output1.hiv

Analysis Tool:
Registry explorer can used as a tool to explore.

Commands are executed is listed in the RunMRU list value. The letters represent the order in which the commands were executed.

UserAssist

Description:
GUI-based programs launched from the desktop are tracked in the launcher on a Windows system.
https://www.cyberengage.org/post/artifacts-for-program-execution-part-2-jump-lists-runmru-start-userassist

Location: NTUSER.DAT HIVE
Command:
NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count

All values are ROT-13 encoded.
Understanding UserAssist involves deciphering the GUIDs associated with different functionalities.

---GUID for XP
• 75048700 Active Desktop
---GUID for Win7-10
• CEBFF5CD Executable File Execution
• F4E57C4B Shortcut File Execution
---Program Locations for Win7-10 UserAssist
• ProgramFilesX64 6D809377-...
• ProgramFilesX86 7C5A40EF-...
• System 1AC14E77-...
• SystemX86 D65231BO-...
• Desktop B4BFCC3A-...
• Documents FDD39ADO-...
• Downloads 374DE290-...
• UserProfiles 0762D272-.

File opening and creation:

Open/Save MRU

Description:
This key tracks files that have been opened or saved within a Windows shell dialog box. This happens to be a big dataset, not only including web browsers such as Internet Explorer and Firefox, but also a majority of commonly used applications.

Location:

Command:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU

You can use registry as well.
Reg Query
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU

From command prompt:
Reg Save
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU C:\Users\User\Downloads\output.hiv

(To Save hive details into hive file for further analysis)

Analysis Tool:
Registry explorer

Recent Files

Description:
Registry Key that will track the last files and folders opened and is used to populate data in "Recent" menus of the Start menu.

Location: NTUSER.DAT
Command:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

You can use registry as well.
Reg Query
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

From command prompt:
Reg Save
HKCU\ Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
C:\Users\User\Downloads\output.hiv

(To Save hive details into hive file for further analysis)

Analysis Tool:
Registry explorer

RecentDocs: Overall key will track the overall order of the last 150 files or folders opened. The MRU list will keep track of the temporal order in which each file/folder was opened

Shell bags (Very important artifact)

Description:
stores information about which folders were most recently browsed by the user.

https://www.cyberengage.org/post/understanding-shell-bags-in-windows-forensics

For Windows 7-10:

- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
- NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
- NTU**SER.DA**T\Software\Microsoft\Windows\Shell\Bags

For XP

NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags
NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\Bags
NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\BagMRU

Location:
Command:
Win7-10 *USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags*
reg query "HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags"

(Will suggest if you copying hive copy data from Shell instead of shell/bags.)
Win7-10 *USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU*
reg query "HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU"
Win7-10 *NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU*
Win7-10 *NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags*

```
UsrClass.dat Location:
C:\Users\[username]\AppData\Local\Microsoft\Windows
```

```
HKEY_CURRENT_USER\Software\Classes == UsrClass.dat
```

```
Shellbag Locations (Windows XP):

Local Folders:
NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam

Network Folders:
NTUSER.DAT\Software\Microsoft\Windows\Shell

Removable Device Folders:
NTUSER.DAT\Software\Microsoft\Windows\StreamMRU
```

Bag MRU: -Stores actual directory structure of folders accesses

```
BagMRU Subkey:

- MRUListEx: 4-Byte value indicating the order in which folders were accessed,
  with the most recent access listed first

- NodeSlot: Points to the Bags key, which stores the customization data

- NodeSlots: Found in the root BagMRU subkey, updated upon new Shellbag creation
```

Bags: - Stores actual folder customization data(WINDOW SIZE, WINDOW LAYOUT)

The NTUSER.DAT file is the Registry hive for the currently logged-in user on a Windows system.

Location of Both .Dat Files:

1. NTUSER.DAT File Location:

- *The NTUSER.DAT file is typically located within each user's profile folder on the system.*
- *For example, if the username is "User," the NTUSER.DAT file for that user will be found in:*
  C:\Users\User

- *It's important to note that the NTUSER.DAT file is hidden by default, so you may need to enable "Show hidden files and folders" in Windows Explorer to view it.*

2. USRCLASS.DAT File Location:

- *The USRCLASS.DAT file is also a part of the user's registry hive and contains information related to user-specific COM (Component Object Model) classes.*
- *Unlike the NTUSER.DAT file, the USRCLASS.DAT file is typically not found directly in the user's profile folder.*
- *Instead, it is located within the "AppData" directory under the user's profile folder:*

  C:\Users\User\AppData\Local\Microsoft\Windows

- *Within this directory, you may find the USRCLASS.DAT file alongside other system and application data specific to the user.*

Analysis Tool:

SBECmd and Shellbag explorer

https://www.cyberengage.org/post/shell-bags-analysis-tool-sbecmd-exe-or-shellbagsexplorer-gui-version-very-important-artifact

It will show information that is not present there like cache for example like you connected flash drive later you remove it but even after removing the flash drive shell bag contain information about

Last Visited MRU

Description:

Tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key. In addition, each value also tracks the directory location for the last file that was accessed by that application.
Example: Notepad.exe was last run using the C:\Users\Rob\Desktop folder.

Location:

Command:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisited PidlMRU

You can use registry as well.
Reg Query
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU
Can use HKLM as well.

From command prompt:
Reg Save
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU C:\Users\User\Downloads\output.hiv

(To Save hive details into hive file for further analysis)

Analysis Tool:
Registry explorer

Office Recent Files

Description:
MS Office programs will track their own Recent Files list to make it easier for users to remember the last file they were editing.

Location:
*Forensic investigators can locate information about Office versions within the Windows registry, specifically in the **NTUSER.DAT hive**.*

NTUSER.DAT\Software\Microsoft\Office\VERSION

This key stores information about the Office version, where VERSION can be either 16.0 or 14.0.

NTUSER.DAT\Software\Microsoft\Office\VERSION\User MRU\LiveID_####\File MRU

This key contains information about recently accessed files and documents within specific Office applications.

***"PlaceMRU,"** which shows the path of the location of the previously opened file in that directory.*

LNK Files

Description:

The ".lnk" file is a shortcut file used in Microsoft Windows operating systems. It stands for "Link." When you create a shortcut to a file, folder, program, or website, Windows creates an .lnk file that points to the target item. This allows users to access the target item quickly without having to navigate through the file system.

***** During a forensic examination of a hard drive, LNK files can determine what programs and files a user were accessing on their computer."*****

https://www.cyberengage.org/post/unveiling-the-significance-of-lnk-files-in-digital-forensics

Location: link

Command:

cd C:\Users\<User>\AppData\Roaming\Microsoft\Windows\Recent

cd C:\Users\User\AppData\Roaming\Microsoft\Office\Recent

Analysis Tool:

we have tool to analyse for lnk file analyse we can use LECmd parser.

https://www.cyberengage.org/post/lnk-files-analysis-tool-lecmd-exe

4. Prefetch

5. JumpLists

Same as previously told:

Deleted File and file knowledge:

XP: ACMRU

Description:

You can search for multiple things through the search assistant on a Windows XP machine. The search assistant will remember a user's search terms for filenames, computers, or words that are inside a file. This is an example of where you can find the "Search History" on the Windows system.

Location:

The search history is stored in the Windows registry within the NTUSER.DAT hive:

NTUSER.DAT\Software\Microsoft\SearchAssistant\ACMru\####

Interpretation: The "ACMru" key contains different subkeys identified by numeric values ("####"), each representing a specific type of search history:

- Search the internet: #### = 5001
- Search for all or part of a document name: #### = 5603
- Search for a word or phrase within a file: #### = 5604
- Search for printers, computers, and people: #### = 5647

2. **Last Visited MRU**
   Same as previously told

Vista/Win7-10 Thumbnails

Description:
On Vista/Win7-10 versions of Windows, thumbs.db does not exist. The data now sits under a single directory for the users of the machine, located in their application data directory under their home directory.

Location:
Command:
C:\Users\<usemame>\AppData\Local\Microsoft\Windows\Explorer

Manually extraction of files: So later can be
copy "C:\Users\User\AppData\Local\Microsoft\Windows\Explorer"*
"C:\Users\User\Downloads\Shell"

Tool used:
thumbcache_viewer_64'

https://thumbcacheviewer.github.io/

Recycle Bin

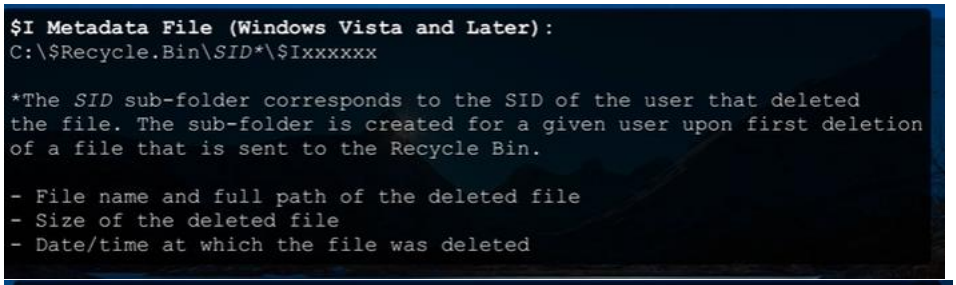
Description:
The recycle bin is an important location on a Windows filesystem to understand. It can help you when accomplishing a forensic investigation, as every file that is deleted from a Windows recycle bin aware program is generally first put in the recycle bin.

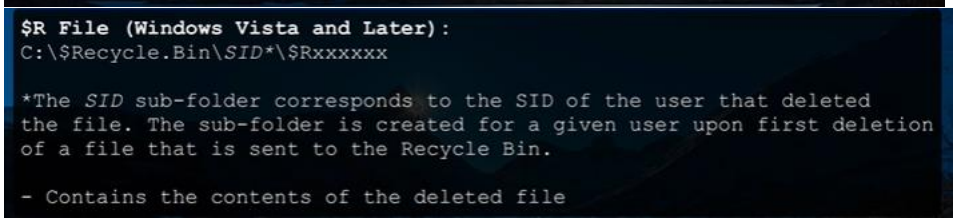
https://www.cyberengage.org/post/recycle-bin-forensic

Location:
Command: Windows XP
C:\RECYCLER"

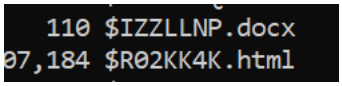
Location:
Command

C:\$Recycle.bin





Commands:
C:\$Recycle.bin

1. *DIR /ah (you will see hidden files)*
2. *wmic useraccount get name,sid (get information about all account and there sid IDs)*
3. *cd SID (move to particular sid value) example C:\$Recycle.Bin\S-1-5-21-166528716-2058207302-1224197115-1001>*
4. 

5. *As expected, you will see $R, $I files.*

   As $R IS recoverable files so no need for parsing but $I files need parsing tool use for that is $I Parse

SID can be mapped to users via Registry Analysis.
Files preceded by $I###### files contain original PATH and name.
Files preceded by $R###### files contain recovery data.

Analysis Tool:
$I Parse

https://www.cyberengage.org/post/recycle-bin-i-analyses-tool-i_parse_v1-1

Search -WordWheelQuery

Description:
It stores information about keywords searched for from the START menu bar, providing insights into user search behavior and interests.

Location: Win7-10 NTUSER.DAT Hive
Command:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

You can use registry as well.

Reg Query
HKCU\ Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

From command prompt:
Reg Save
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
C:\Users\User\Downloads\output.hiv

(To Save hive details into hive file for further analysis)

Analysis Tool:
Registry explorer

2.Index.dat file://
https://www.cyberengage.org/post/artifacts-for-deleted-file-or-file-knowledge-part-2-search-wordwheelquery-index-dat-file

Physical location:

Timezone

Description:
Identifies the current system time zone.

Location: SYSTEM Hive
Command:
SYSTEM\CurrentControlSet\Control\TimeZoneInformation

You can use registry as well.
Reg Query
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Can use HKCU as well.

From command prompt:
Reg Save
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
C:\Users\User\Downloads\output.hiv

(To Save hive details into hive file for further analysis)

Analysis Tool:
Registry explorer

Browser Search Terms
https://www.cyberengage.org/post/artifacts-for-physical-location-timezone-browser-search-terms-network-history-cookies

VISTA/Win7-10 Network History

Description:
• Identify networks that the computer has been connected to.
• Networks could be wireless or wired.
• Identify domain name/intranet name.
• Identify SSID.
• Identify Gateway MAC address.

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Signatures\Managed
SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Nla\Cache

Location: SOFTWARE HIVE
Commands:
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged"
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed"
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache\"

Cookies (See above where started collecting browser artifact)

Description:
Cookies give insight into what websites have been visited and what activities may have taken place there.

https://www.cyberengage.org/post/artifacts-for-file-download-part-2-firefox-internet-explorer-chrome

Location: Internet Explorer
XP *%userprofile%\Cookies*
Win7-10 *%userprofile%\AppData\Roaming\Microsoft\Windows\Cookies*
Win7-10 *%userprofile%\AppData\Roaming\Microsoft\Windows\Cookies\Low*

Location: Firefox
XP *%userprofile%\Application Data\Mozilla\Firefox\Profiles\<random text>.default\cookies.sqlite*
Win7-10 *%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default\cookies.sqlite*

When I capture other thing at start on Firefox I will include these as well

USB and Drive Usage:

https://www.cyberengage.org/post/artifacts-for-usb-or-drive-usage-part-1-key-identification-first-last-times-user

Key Identification

Description:

Track USB devices plugged into a machine.

Location:

Command:
Reg Query HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
Reg Query HKLM\SYSTEM\CurrentControlSet\Enum\USB

Query using CMD:

1. *Reg Query HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR*
2. *Reg Query HKLM\SYSTEM\CurrentControlSet\Enum\USB*

Manually collect artifact using CMD: or can use Kape

1. *Reg Save HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR C:\Users\User\Downloads\output.hiv*

2. .Reg Save HKLM\SYSTEM\CurrentControlSet\Enum\USB C:\Users\User\Downloads\output.hiv

First/Last Times

Description:

Determine temporal usage of specific USB devices connected to a Windows machine.

Location: First Time
Command:
Plug and Play Log Files
XP *C:\Windows\setupapi.log*

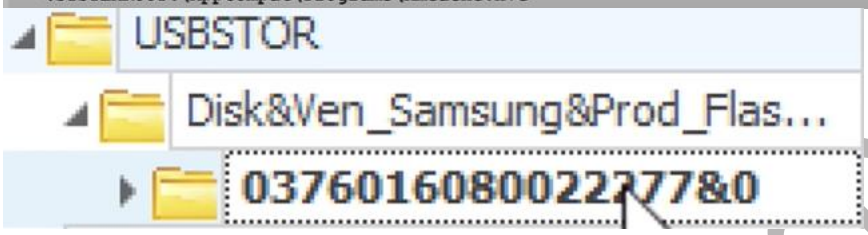
C:\Windows\INF>setupapi.dev.log (it is file so if you enter it will open with notepad)

Interpretation:

• Search for Device Serial Number
• Log File times are set to local time zone

Location: Last Time
Command:
NTUSER//Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2/{GUID}
reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2"

```
                    Common Artifact Locations

HKLM\SYSTEM\CurrentControlSet\Enum\USB      < VID / PID
HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR  < Class ID / Serial #

HKLM\SYSTEM\MountedDevices
     • Find Serial # to obtain the Drive Letter of the USB device
     • Find Serial # to obtain the Volume GUID of the USB device

HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices
     • Find Serial # and then look for FriendlyName to obtain the
       Volume Name of the USB device

*NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Mountpoints2
     *HKCU on a live system

XP:              %SYSTEMROOT%\setupapi.log
Vista and later: %SYSTEMROOT%\inf\setupapi.dev.log

%SYSTEMROOT%\AppCompat\Programs\Amcache.hve
```



(Serial Number)

Manually collect artifact using CMD: or can use Kape

1. ***Reg Save***
   "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2" C:\Users\User\Downloads\output.hiv

You can use DFIR Cheat sheet from My folder.

User

Description:
Find user that used the unique USB device.

Location:
Command
• Look for GUID from SYSTEM\MountedDevices
reg query HKLM\SYSTEM\MountedDevices

GUID

```
\??\Volume{84c22bf1-5901-11ec-9ab0-f594c1f627d6}
```

• NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2"

Interpretation: (Important)

- **The first step is to locate the GUID associated with** the USB device of interest from the SYSTEM\MountedDevices registry key. Locate User's Personal MountPoints Key:

- **Once the GUID is identified, it is used** to locate the user's personal mountpoints key in the NTUSER.DAT hive, specifically in the Explorer\MountPoints2 subkey. Determine Last Write Time:
- **The last write time of the user**'s mountpoints key corresponds to the last time the USB device was plugged into the machine by that user. User Attribution:
- By examining the user's mountpoints key, forensic investigators can attribute the usage of the USB device to a specific user account.

Drive Letter and Volume Name

Description:
USB devices play a significant role in forensic investigations, and understanding the drive letter and volume name associated with a USB device can provide valuable insights into user activity and data access.

Location: XP
Command
• Find *ParentldPrefix.*
Reg Query HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
• Use *ParentldPrefix* Discover Last Mount Point.
reg query HKLM\SYSTEM\MountedDevices

Location: Win7-10
Command
reg query "HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices
reg query HKLM\SYSTEM\MountedDevices

Examine drive letters looking at value data looking for serial number.

Interpretation: Identify the USB device that was last mapped to a specific drive letter

Volume Serial Number

Description:
Discover the Volume Serial Number of the filesystem partition on the USB. (Note: This is not the USB Unique Serial Number; this is created when a filesystem is initially formatted.)

Location:
Command:
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt "
(Key will ONLY be present if system drive is NOT SSD)

• Use Volume Name and USB Unique Serial Number to find.
• Last integer number in line.
• Convert Decimal Serial Number into Hex Serial Number.

Interpretation:

1. Identify Registry Key:

- **Locate the EMDMgmt registr**y key under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ to access information about the filesystem partition. 2. Volume Serial Number:
- Use the Volume Name and USB Unique Serial Number to find the Volume Serial Number.
- **The Volume Serial Number is typically the** last integer number in the line of information retrieved from the registry key. 3. Convert Decimal to Hex Serial Number:
- Once the Volume Serial Number is identified in decimal format, it can be converted to hexadecimal format for further analysis if needed.

3.Shortcut (LNK) Files

4.P&P Event Log

The Plug and Play (P&P) Event Log is a crucial source of information for forensic investigators, providing insights into driver installations and device connections on a Windows system.

Location:

- System Log File (Windows 7-10):
- *%systemroot%\System32\winevt\logs\System.evtx*

Event ID:

- **20001:** Plug and Play driver install attempted

Interpretation:
Event Identification:

- The P&P Event Log records events triggered when a Plug and Play driver installation is attempted on the system.
- **Each event is assign**ed a unique identifier, with Event ID 20001 specifically indicating a Plug and Play driver install attempt.

Account Usage:

You must gather information like

https://www.cyberengage.org/post/artifacts-for-account-usage-last-login-success-fail-logons-last-password-change-logon-typ

Last logon
Successful/failed logons
Last password change
Logon types

RDP Usage

Description:
Track Remote Desktop Protocol logons to target machines.

This you can do by checking Security Logs and with events IDs like
• Event ID 682/4778-Session Connected/Reconnected
• Event ID 683/4779-Session Disconnected

I am focusing on RDP cache.
Every time when somebody use mstsc.exe for RDP there is cache memory got create which got store in location.
You can use below tool.
https://github.com/ANSSI-FR/bmc-tools

```
RDP Cache Location:
C:\Users\[username]\AppData\Local\Microsoft\Terminal Server Client\Cache
```