**Methods of Collection – Artifacts-**

Different data collection methods in forensics:

Collection techniques include picking, lifting, scraping, vacuum sweeping, combing and clipping. Several tools can be used for the collection of trace evidence (eg tweezers, tape lifts, spatulas).

**There are two types of data, that can be collected in a computer forensics investigation:**

**Persistent data: It is the data that is stored on a non-volatile memory type storage device such as a local hard drive, external storage devices like SSDs, HDDs, pen drives, CDs, etc. the data on these devices is preserved even when the computer is turned off.**

**Volatile data: It is the data that is stored on a volatile memory type storage such as memory, registers, cache, RAM, or it exists in transit, that will be lost once the computer is turned off or it loses power. Since volatile data is evanescent, it is crucial that an investigator knows how to reliably capture it.**

Forensic artifacts are the forensic objects that have some forensic value. Any object that contains some data or evidence of something that has occurred like logs, register, hives, and many more.

forensic investigator look for while performing a Forensic analysis in Windows.

1. **Recycle Bin**: The windows recycle bin contains some great artifacts like:

$1 file containing the metadata. You can find this file under the path C:\$Recycle.Bin\SID\*\$Ixxxxxx

$R file containing the contents of the deleted files. This file can be located under the path C:\$Recycle.Bin\SID\*\$Rxxxxxx

$1 file can be parsed using a tool $1 Parse.

2. **Browsers**: Web browsers contain a lot of information like:

Cookies.

Cached website data.

Downloaded files.

3**. Windows Error Reporting**: This features enables user to inform Microsoft about application faults, kernel faults, unresponsive application, and other application specific problems. This feature provides us with various artifacts like:

Program Execution, if a malicious program crashes during program execution.

You can locate these artifacts at the following locations:

C:\ProgramData\Microsoft\Windows\WER\ReportArchive

C:\Users\XXX\AppData\Local\Microsoft\Windows\WER\ReportArchive

C:\ProgramData\Microsoft\Windows\WER\ReportQueue

C:\Users\XXX\AppData\Local\Microsoft\Windows\WER\ReportQueue

4. **Remote Desktop Protocol Cache**: When using the “mstc” client that is provided by the Windows, RDP can be used to move laterally through the network. Cache files are created containing the sections of the screen of the machine to which we are connected to and that is rarely changing. These cache files can be located in the directory:

C:\Users\XXX\AppData\Local\Microsoft\Terminal Server Client\Cache

Tools like BMC-Tools can be used to extract images stored in these cache files.

5. **LNK Files**: .lnk files are the windows shortcut files. LNK files link or point to other files or executables for ease of access. You can find following information in these files:

The original path of the target file.

Timestamp of both the target files and the .lnk files.

File Attributes like System, Hidden, etc.

Details about the disk.

Remote or local execution.

MAC address of the machines.

You can use tools like Windows LNK Parsing Library or LECmd to parse the contents of these files.

6. **Jump Lists**: They contain information about the recently accessed applications and files. This feature was introduced with Windows 7. Two types of Jump Lists can be created in Windows:

AUTOMATICDESTINATIONS-MS: These jump lists are created automatically when a user opens a file or an application. They are located under the path:

C:\Users\xxx\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

CUSTOMDESTINATIONS-MS: These jump lists are custom made and are created when a user pins a file or an application. They are located under the directory C:\Users\xxx\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

You can use tools like JumpList Explorer, JLECmd, or Windows JumpList Parser to parse Jump lists.

7. **Prefetch Files**: These files contain a wealth of information like:

Application Name.

Application path.

Last execution timestamp.

Creation timestamp.