Cyber Law and Forensics (CS402)

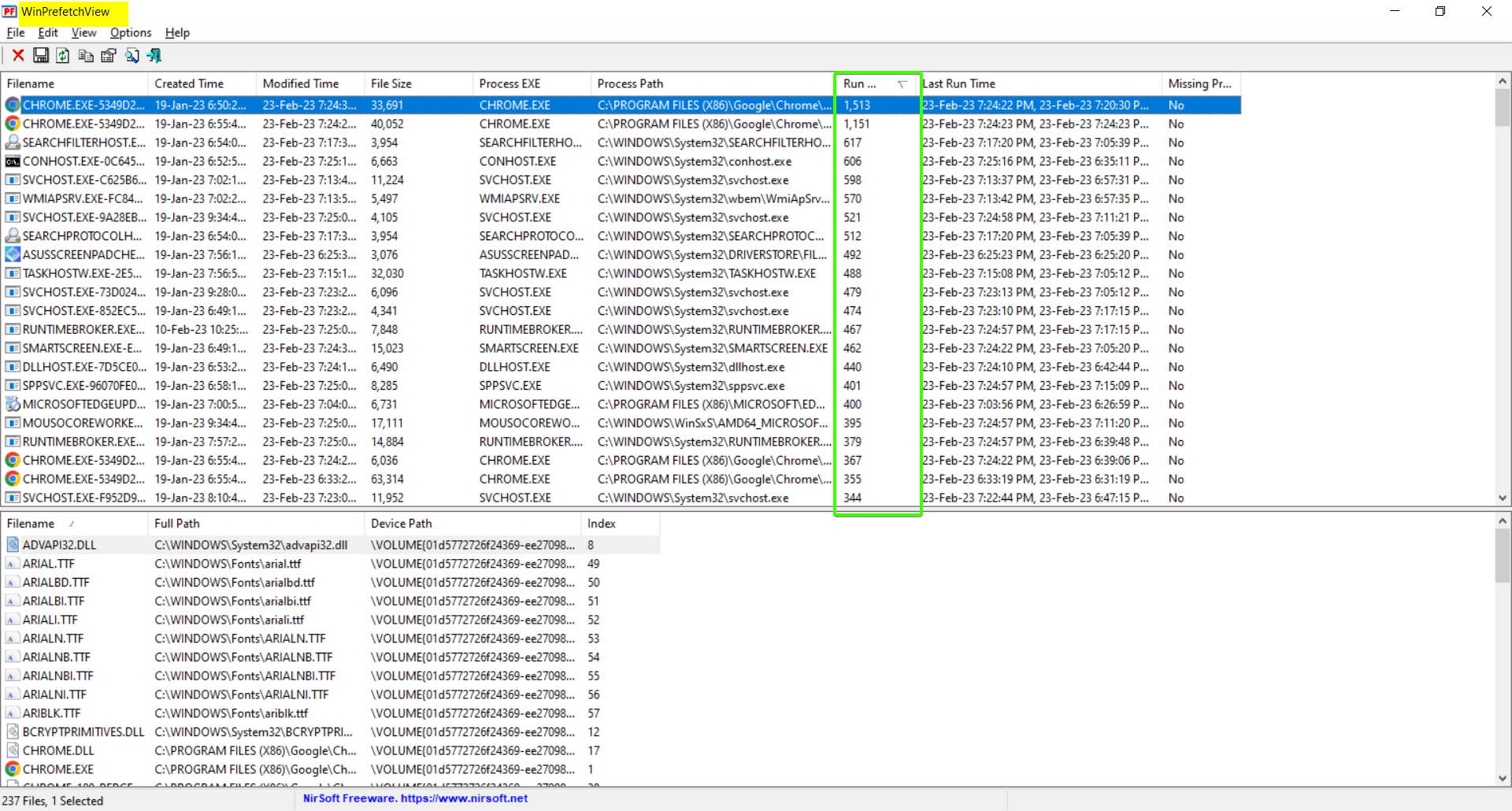
Lab Assignment 3

**U19CS012**

A.) Learn the Following Windows Forensics Artifacts:-

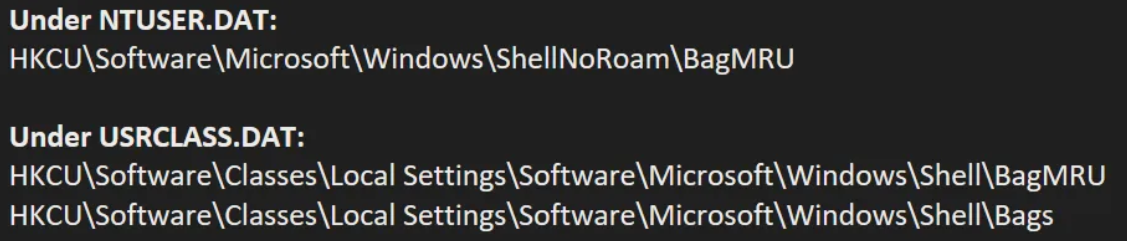
(1) prefetch

* Introduced in Windows XP.
* Used to **Speed up** Application Startup.
* When an Application is started up for the first time, then Windows will record the first 10 seconds of the startup. Windows will **store which DLL** (Dynamic Link Library) are loaded, and will save the names of them into the Prefetch file. So Windows can load this DLLs **faster next time**.
* The Prefetch files contain the following metadata:
* Executables name
* Run count
* Files and directories used during application startup



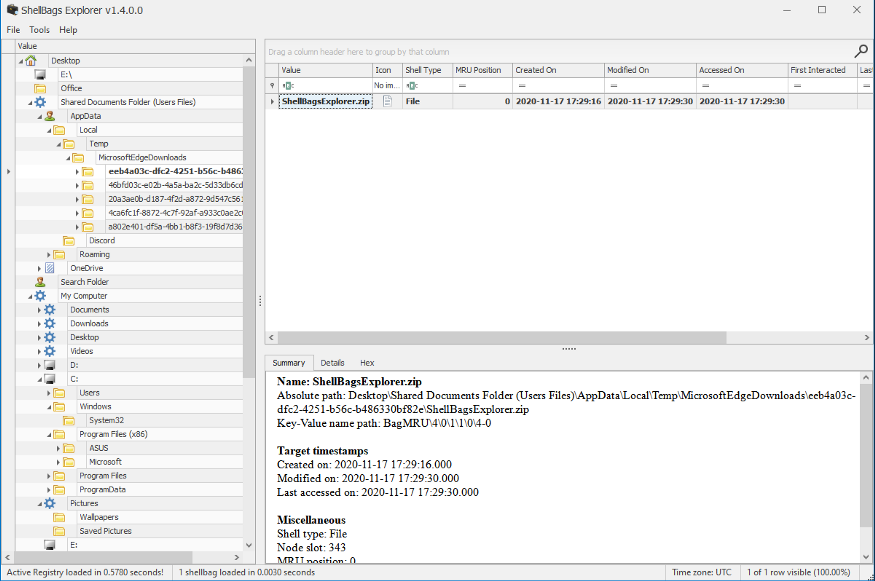
(2) Shellbags

* Store the **view preferences** of the user
* Used to determine **which folder** were accessed by a particular user
* To identify some directories which is not available anywhere in computer



Shellbag Locations

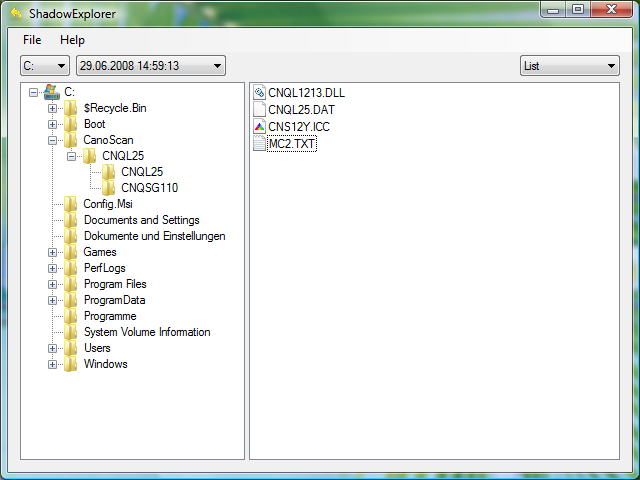
**Tool**: ShellBags Explorer - GUI for browsing shellbags data. Handles locked files



(3) Volume Shadow Copy [Windows XP]

* Technology that can create volume or file snapshots, even if they are in use
* Used to recover corrupted files.
* Used to restore deleted files or examine registry hives. [Only for NTFS]

Tool to extract snapshots: Shadow Explorer



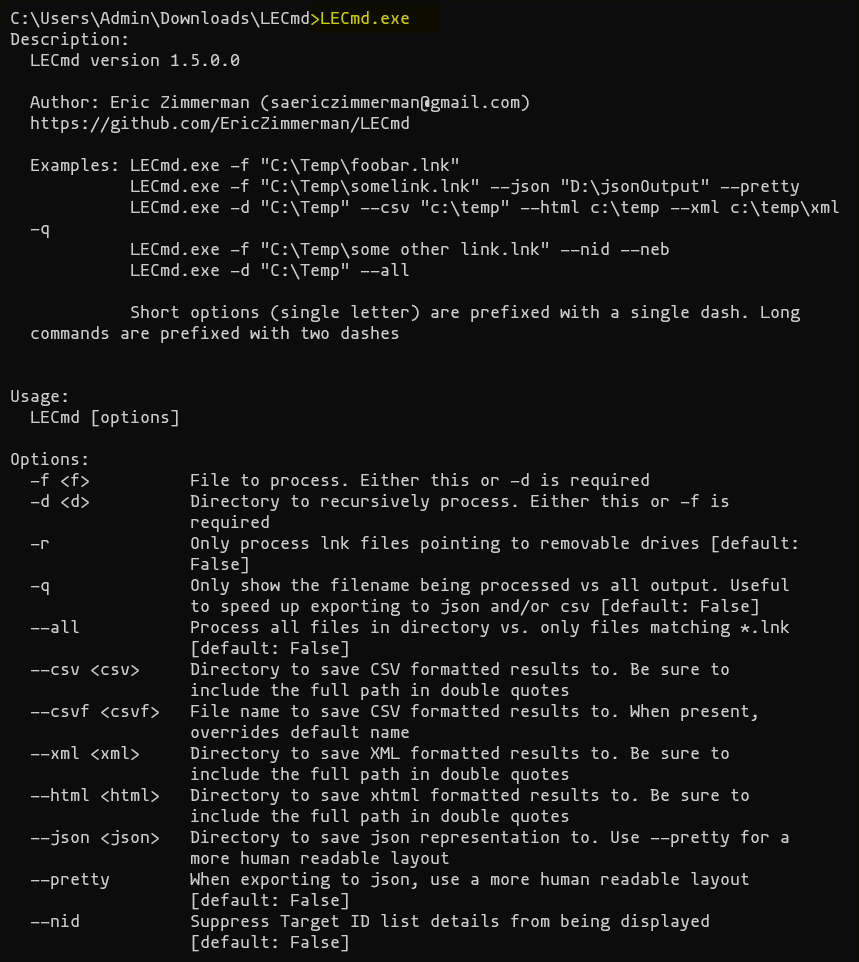
(4) LNK files

“LNK” files are **shortcut files** that can be auto generated by Windows or can be generated by the user.

“LNK” files point to another application or file.

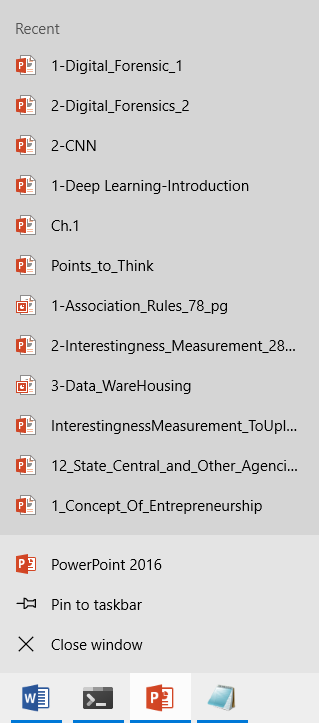
LNK files can contains the following information’s:

* MAC time attributes (Creation, Modification, Access Time) for LNK file and linked file
* User’s previous activities on Computer and Linked file size
* Original path of the linked file
* Extension: .lnk



(5) Jump lists

* Jump Lists are a new Windows 7 Taskbar feature that gives the user quick access to recently accessed application files and actions.
* Whenever you right click on icon of program shows in taskbar you will find jump lists.



They contain information about recently accessed applications and files.

**SUBMITTED BY**:

U19CS012

BHAGYA VINOD RANA