

Cyber Law and Forensics (CS402)

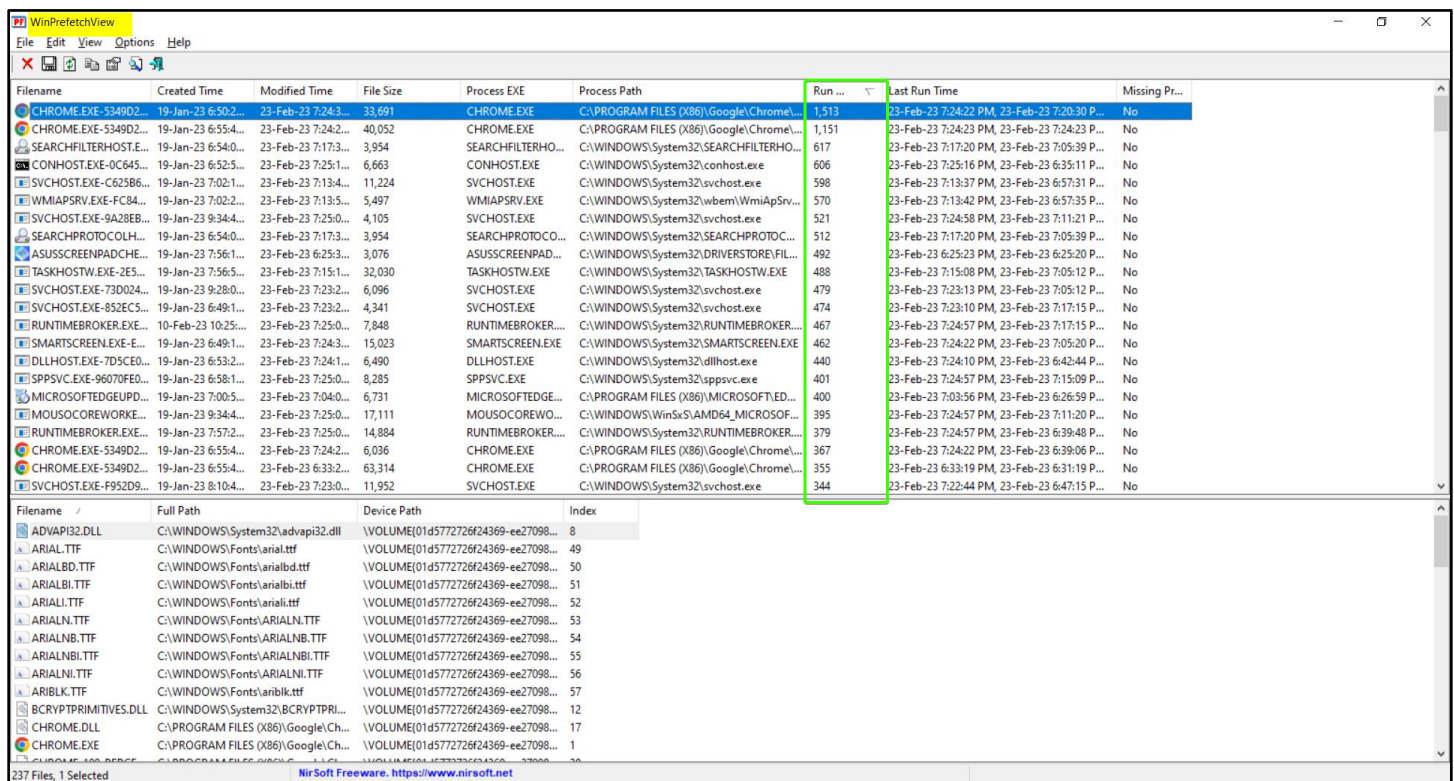
Lab Assignment 3

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



The screenshot shows the WinPrefetchView application window. The main table lists prefetch files with columns: Filename, Created Time, Modified Time, File Size, Process EXE, Process Path, Run count, Last Run Time, and Missing Pr... The 'Run' column is highlighted with a green box. Below the main table, there is a section for 'Full Path', 'Device Path', and 'Index' for the selected file, ADVAPI32.DLL.

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run	Last Run Time	Missing Pr...
CHROME.EXE-5349D2...	19-Jan-23 6:50:2...	23-Feb-23 7:24:3...	33,691	CHROME.EXE	C:\PROGRAM FILES (X86)\Google\Chrome\...	1,513	23-Feb-23 7:24:22 PM, 23-Feb-23 7:20:30 P...	No
CHROME.EXE-5349D2...	19-Jan-23 6:55:4...	23-Feb-23 7:24:2...	40,052	CHROME.EXE	C:\PROGRAM FILES (X86)\Google\Chrome\...	1,151	23-Feb-23 7:24:23 PM, 23-Feb-23 7:24:23 P...	No
SEARCHFILTERHOST.E...	19-Jan-23 6:54:0...	23-Feb-23 7:17:3...	3,954	SEARCHFILTERHO...	C:\WINDOWS\System32\SEARCHFILTERHO...	617	23-Feb-23 7:17:20 PM, 23-Feb-23 7:05:39 P...	No
CONHOST.EXE-0C645...	19-Jan-23 6:52:5...	23-Feb-23 7:25:1...	6,663	CONHOST.EXE	C:\WINDOWS\System32\conhost.exe	606	23-Feb-23 7:25:16 PM, 23-Feb-23 6:35:11 P...	No
SVCHOST.EXE-C625B6...	19-Jan-23 7:02:1...	23-Feb-23 7:13:4...	11,224	SVCHOST.EXE	C:\WINDOWS\System32\svchost.exe	598	23-Feb-23 7:13:37 PM, 23-Feb-23 6:57:31 P...	No
WMIAPSRV.EXE-FC84...	19-Jan-23 7:02:2...	23-Feb-23 7:13:5...	5,497	WMIAPSRV.EXE	C:\WINDOWS\System32\wbem\WmiApSrv...	570	23-Feb-23 7:13:42 PM, 23-Feb-23 6:57:35 P...	No
SVCHOST.EXE-9A28E...	19-Jan-23 9:34:4...	23-Feb-23 7:25:0...	4,105	SVCHOST.EXE	C:\WINDOWS\System32\svchost.exe	521	23-Feb-23 7:24:58 PM, 23-Feb-23 7:11:21 P...	No
SEARCHPROTOCOLH...	19-Jan-23 6:54:0...	23-Feb-23 7:17:3...	3,954	SEARCHPROTOCOL...	C:\WINDOWS\System32\SEARCHPROTOC...	512	23-Feb-23 7:17:20 PM, 23-Feb-23 7:05:39 P...	No
ASUSSCREENPADCHE...	19-Jan-23 7:56:1...	23-Feb-23 6:25:3...	3,076	ASUSSCREENPAD...	C:\WINDOWS\System32\DRIVERSTORE\FIL...	492	23-Feb-23 6:25:23 PM, 23-Feb-23 6:25:20 P...	No
TASKHOSTW.EXE-2E5...	19-Jan-23 7:56:5...	23-Feb-23 7:15:1...	32,030	TASKHOSTW.EXE	C:\WINDOWS\System32\TASKHOSTW.EXE	488	23-Feb-23 7:15:08 PM, 23-Feb-23 7:05:12 P...	No
SVCHOST.EXE-73D024...	19-Jan-23 9:28:0...	23-Feb-23 7:23:2...	6,096	SVCHOST.EXE	C:\WINDOWS\System32\svchost.exe	479	23-Feb-23 7:23:13 PM, 23-Feb-23 7:05:12 P...	No
SVCHOST.EXE-852EC...	19-Jan-23 6:49:1...	23-Feb-23 7:23:2...	4,341	SVCHOST.EXE	C:\WINDOWS\System32\svchost.exe	474	23-Feb-23 7:23:10 PM, 23-Feb-23 7:17:15 P...	No
RUNTIMEBROKER.EXE...	10-Feb-23 10:25...	23-Feb-23 7:25:0...	7,848	RUNTIMEBROKER...	C:\WINDOWS\System32\RUNTIMEBROKER...	467	23-Feb-23 7:24:57 PM, 23-Feb-23 7:17:15 P...	No
SMARTSCREEN.EXE-E...	19-Jan-23 6:49:1...	23-Feb-23 7:24:3...	15,023	SMARTSCREEN.EXE	C:\WINDOWS\System32\SMARTSCREEN.EXE	462	23-Feb-23 7:24:22 PM, 23-Feb-23 7:05:20 P...	No
DLLHOST.EXE-7D5CE...	19-Jan-23 6:53:2...	23-Feb-23 7:24:1...	6,490	DLLHOST.EXE	C:\WINDOWS\System32\dllhost.exe	440	23-Feb-23 7:24:10 PM, 23-Feb-23 6:42:44 P...	No
SPPSVC.EXE-96070FE...	19-Jan-23 6:58:1...	23-Feb-23 7:25:0...	8,285	SPPSVC.EXE	C:\WINDOWS\System32\sppsvc.exe	401	23-Feb-23 7:24:57 PM, 23-Feb-23 7:15:09 P...	No
MICROSOFTEDGEUPD...	19-Jan-23 7:00:5...	23-Feb-23 7:04:0...	6,731	MICROSOFTEDGE...	C:\PROGRAM FILES (X86)\MICROSOFT\ED...	400	23-Feb-23 7:03:56 PM, 23-Feb-23 6:26:59 P...	No
MOUSOCOREWORKE...	19-Jan-23 9:34:4...	23-Feb-23 7:25:0...	17,111	MOUSOCOREWO...	C:\WINDOWS\WinSxS\AMD64_MICROSO...	395	23-Feb-23 7:24:57 PM, 23-Feb-23 7:11:20 P...	No
RUNTIMEBROKER.EXE...	19-Jan-23 7:57:2...	23-Feb-23 7:25:0...	14,884	RUNTIMEBROKER...	C:\WINDOWS\System32\RUNTIMEBROKER...	379	23-Feb-23 7:24:57 PM, 23-Feb-23 6:39:48 P...	No
CHROME.EXE-5349D2...	19-Jan-23 6:55:4...	23-Feb-23 7:24:2...	6,036	CHROME.EXE	C:\PROGRAM FILES (X86)\Google\Chrome\...	367	23-Feb-23 7:24:22 PM, 23-Feb-23 6:39:06 P...	No
CHROME.EXE-5349D2...	19-Jan-23 6:55:4...	23-Feb-23 6:33:2...	63,314	CHROME.EXE	C:\PROGRAM FILES (X86)\Google\Chrome\...	355	23-Feb-23 6:33:19 PM, 23-Feb-23 6:31:19 P...	No
SVCHOST.EXE-F952D9...	19-Jan-23 8:10:4...	23-Feb-23 7:23:0...	11,952	SVCHOST.EXE	C:\WINDOWS\System32\svchost.exe	344	23-Feb-23 7:22:44 PM, 23-Feb-23 6:47:15 P...	No

Filename	Full Path	Device Path	Index
ADVAPI32.DLL	C:\WINDOWS\System32\advapi32.dll	VOLUME{01d5772726f24369-ee27098...	8
ARIAL.TTF	C:\WINDOWS\Fonts\arial.ttf	VOLUME{01d5772726f24369-ee27098...	49
ARIALBD.TTF	C:\WINDOWS\Fonts\arialbd.ttf	VOLUME{01d5772726f24369-ee27098...	50
ARIALBI.TTF	C:\WINDOWS\Fonts\arialbi.ttf	VOLUME{01d5772726f24369-ee27098...	51
ARIALI.TTF	C:\WINDOWS\Fonts\ariali.ttf	VOLUME{01d5772726f24369-ee27098...	52
ARIALN.TTF	C:\WINDOWS\Fonts\arialn.ttf	VOLUME{01d5772726f24369-ee27098...	53
ARIALNB.TTF	C:\WINDOWS\Fonts\ARIALNB.TTF	VOLUME{01d5772726f24369-ee27098...	54
ARIALNBI.TTF	C:\WINDOWS\Fonts\ARIALNBI.TTF	VOLUME{01d5772726f24369-ee27098...	55
ARIALNI.TTF	C:\WINDOWS\Fonts\ARIALNI.TTF	VOLUME{01d5772726f24369-ee27098...	56
ARIBLK.TTF	C:\WINDOWS\Fonts\ariblk.ttf	VOLUME{01d5772726f24369-ee27098...	57
BCRYPTPRIMITIVES.DLL	C:\WINDOWS\System32\BCRYPTPRIL...	VOLUME{01d5772726f24369-ee27098...	12
CHROME.DLL	C:\PROGRAM FILES (X86)\Google\Ch...	VOLUME{01d5772726f24369-ee27098...	17
CHROME.EXE	C:\PROGRAM FILES (X86)\Google\Ch...	VOLUME{01d5772726f24369-ee27098...	1

237 Files, 1 Selected

NirSoft Freeware. <https://www.nirsoft.net>

(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

Under NTUSER.DAT:

HKCU\Software\Microsoft\Windows\ShellNoRoam\BagMRU

Under USRCLASS.DAT:

HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags

Shellbag Locations

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

The screenshot displays the ShellBags Explorer v1.4.0.0 application. The left pane shows a file tree with the following structure:

- Desktop
- E:\
- Office
- Shared Documents Folder (Users Files)
- AppData
- Local
- Temp
- MicrosoftEdgeDownloads
- eeb4a03c-dfc2-4251-b56c-b486...
- 46bf03c-e02b-4a5a-ba2c-5d33db6cd
- 20a3ae0b-d187-4f2d-a872-9d547c561
- 4ca6fc1f-8872-4c7f-92af-a933c0ae2c0
- a802e401-df5a-4bb1-b8f3-19f8d7d36
- Discord
- Roaming
- OneDrive
- Search Folder
- My Computer
- Documents
- Downloads
- Desktop
- Videos
- D:
- C:
- Users
- Windows
- System32
- Program Files (x86)
- ASUS
- Microsoft
- Program Files
- ProgramData
- Pictures
- Wallpapers
- Saved Pictures
- E:

The right pane shows a table of shellbags with the following columns: Value, Icon, Shell Type, MRU Position, Created On, Modified On, Accessed On, First Interacted, and Last Interacted. The table contains one entry:

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted	Last Interacted
ShellBagsExplorer.zip	No im...	File	0	2020-11-17 17:29:16	2020-11-17 17:29:30	2020-11-17 17:29:30		

Below the table, the 'Summary' tab is selected, showing the following details:

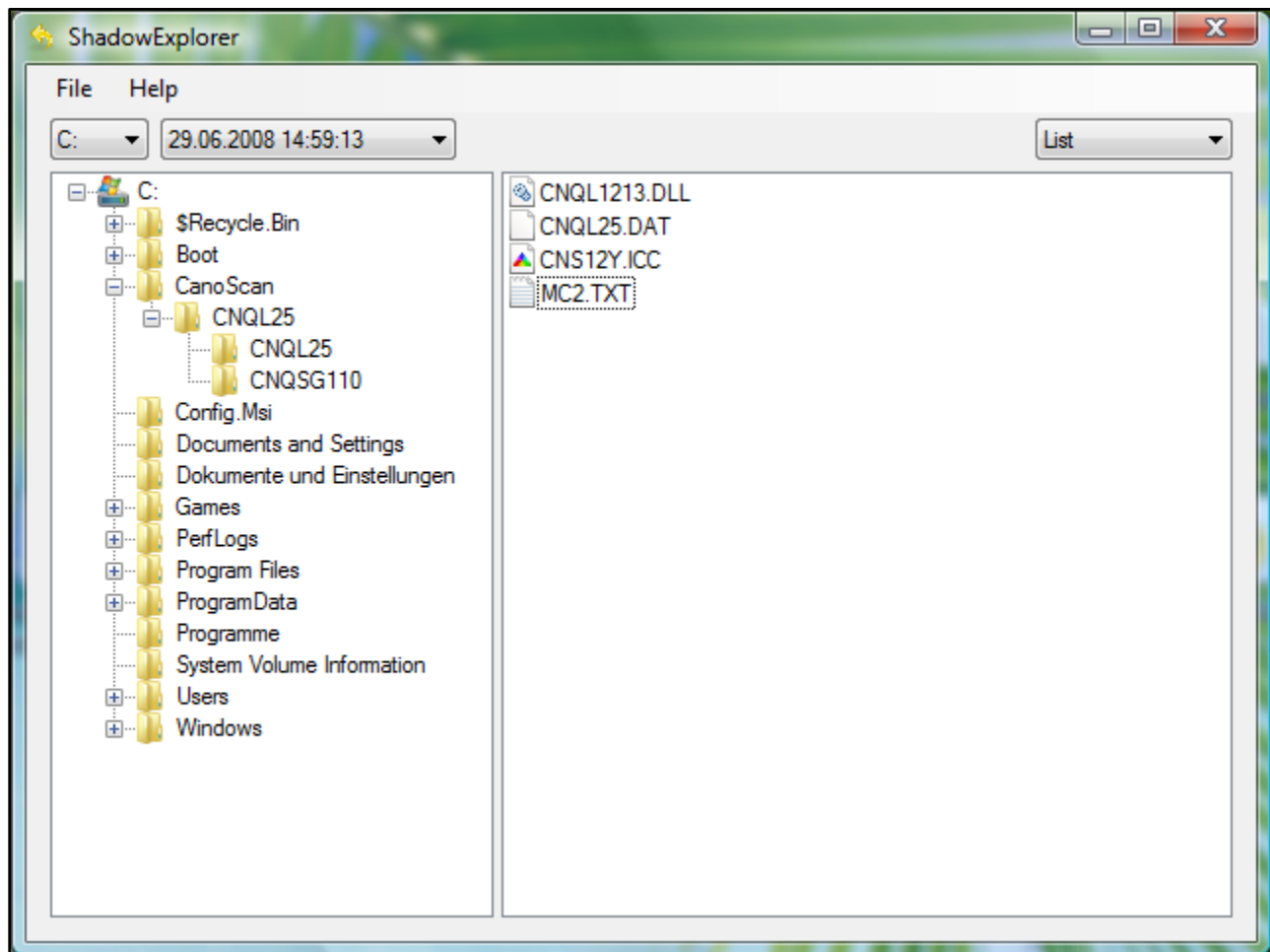
- Name:** ShellBagsExplorer.zip
- Absolute path:** Desktop\Shared Documents Folder (Users Files)\AppData\Local\Temp\MicrosoftEdgeDownloads\eeb4a03c-dfc2-4251-b56c-b486330bf82e\ShellBagsExplorer.zip
- Key-Value name path:** BagMRU\4\0\1\1\0\4-0
- Target timestamps:**
 - Created on: 2020-11-17 17:29:16.000
 - Modified on: 2020-11-17 17:29:30.000
 - Last accessed on: 2020-11-17 17:29:30.000
- Miscellaneous:**
 - Shell type: File
 - Node slot: 343
 - MRU position: 0

The status bar at the bottom indicates: Active Registry loaded in 0.5780 seconds! 1 shellbag loaded in 0.0030 seconds. Time zone: UTC. 1 of 1 row visible (100.00%).

(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

```
C:\Users\Admin\Downloads\LECmd>LECmd.exe
Description:
  LECmd version 1.5.0.0

  Author: Eric Zimmerman (saericzimmerman@gmail.com)
  https://github.com/EricZimmerman/LECmd

  Examples: LECmd.exe -f "C:\Temp\foobar.lnk"
             LECmd.exe -f "C:\Temp\somelink.lnk" --json "D:\jsonOutput" --pretty
             LECmd.exe -d "C:\Temp" --csv "c:\temp" --html c:\temp --xml c:\temp\xml

  -q
             LECmd.exe -f "C:\Temp\some other link.lnk" --nid --neb
             LECmd.exe -d "C:\Temp" --all

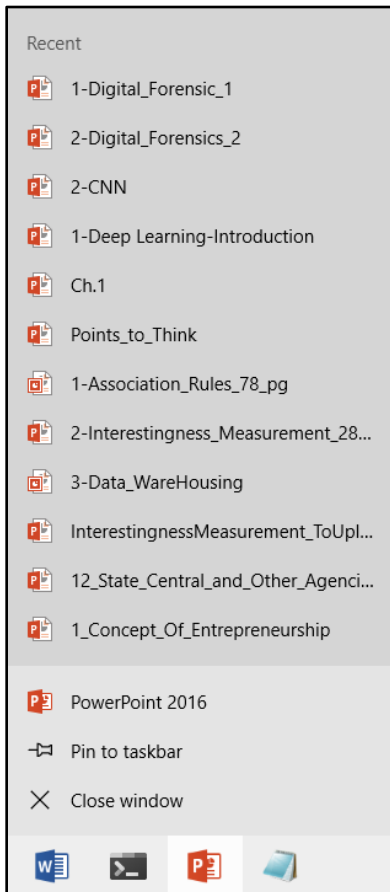
  Short options (single letter) are prefixed with a single dash. Long
  commands are prefixed with two dashes

Usage:
  LECmd [options]

Options:
  -f <f>      File to process. Either this or -d is required
  -d <d>      Directory to recursively process. Either this or -f is
              required
  -r          Only process lnk files pointing to removable drives [default:
              False]
  -q          Only show the filename being processed vs all output. Useful
              to speed up exporting to json and/or csv [default: False]
  --all       Process all files in directory vs. only files matching *.lnk
              [default: False]
  --csv <csv> Directory to save CSV formatted results to. Be sure to
              include the full path in double quotes
  --csvf <csvf> File name to save CSV formatted results to. When present,
                overrides default name
  --xml <xml>  Directory to save XML formatted results to. Be sure to
              include the full path in double quotes
  --html <html> Directory to save xhtml formatted results to. Be sure to
                include the full path in double quotes
  --json <json> Directory to save json representation to. Use --pretty for a
                more human readable layout
  --pretty    When exporting to json, use a more human readable layout
              [default: False]
  --nid       Suppress Target ID list details from being displayed
              [default: False]
```

(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