

Assignment 3 – Shell Item Analysis

Background

Students will continue to analyze Windows systems and artifacts extracted from Lab Assignment 1A in order to profile account activity, files accessed, opened, and moved across systems. This is the final lab that will comprise the bulk of Case Study 1 analysis.

Scenario(Recap): The Shield SOC received a network alert for a download for BitTorrent and a Privacy Cleaner utility over the weekend. Both tools are against the company's acceptable use policy and may be potentially unwanted programs (PUPs). The incident response team identified the system of interest and requested that the forensic team image the system and perform an analysis.

Objectives

- Parse LNK files, Jump Lists and Shellbags to profile user and system actions
- Conduct USB device analysis to identify other evidence sources and possible data exfiltration
- Parse Windows prefetch files to identify applications that executed and their parameters

Exercise Preparation

Preparation

Load the image from Lab Assignments 1A and 2A (IP_CaseStudy.E01) into FTK Imager and/or Autopsy. You may have exported the required artifacts during Lab Assignment 1A, which allows you to choose mounting the image locally, or running the tools against the exported artifacts (in some cases and is what we do in this assignment).

Note: I typically create a directory named "Tools" on my Desktop or the root of my "C:\\" drive. Download Eric Zimmerman's tools (<https://ericzimmerman.github.io/#!index.md>) (recently updated to the same version) and USB tools as follows:

1. LECmd 1.5.0.0 – LNK file parser
2. JLECmd 1.5.0.0 – Jump List parser AND/OR Jump List Explorer 1.4.0.0 GUI-based Jump List Viewer
3. SBECmd – Shellbag parser AND/OR Shellbags Explorer 2.0.0.0 – GUI tool for browsing shellbag data
4. PECmd 1.5.0.0 Prefetch file parser
5. USB Detective (<https://usbdetective.com/>) or Download from OneDrive.¹

LNK File Analysis

1. Extract or unzip the LECmd archive.
2. Open a command prompt and navigate to the extracted LECmd folder.
3. Simply run **LECmd.exe** to see the available options and review them.

¹ [USB Detective](https://usbdetective.com/)

- Run the tool from the command line as follows: **LECcmd -d "Directory of exported LNK Files" --csv "Directory Output\lnk.csv"**

```
$ ./LECcmd.exe -d ../../Labs/CaseFolder/Recent/ --csv ../../Labs/CaseFolder/LinkAnalysis
```

- Open the new .CSV and **SAVE AS** an Excel spreadsheet before editing (example: LNK_Files.xls or .xlsx), which allows editing while preserving original data and formatting.
- Delete (or hide) all columns except: **SourceCreated, SourceModified, SourceAccessed, FileSize, DriveType, VolumeSerialNumber, VolumeLabel, and LocalPath.**
- Delete or hide any rows without timestamps or actual LocalPath information (three should be removed).
- Review the **SourceCreated, SourceModified, VolumeSerialNumber, VolumeLabel, and LocalPath** fields and answer the questions below (for a forensic report similar to Lab 2 and Lab 4, I typically include Creation and Modified dates, the Local Path, and file size). You will find the remaining fields are great for analysis and research. For instance, identifying volume serial numbers, machine IDs, and full paths allow you to draw conclusions based on where files existed (shares and removable media) and how the files have change (file size).
- Also note, during an actual lab or forensic report, the table should be formatted, any ambiguous data removed, and pasted within a report. If more than 10 rows exist, include the pertinent info inline and the full output in an appendix.

20221007051326_LECcmd_Output								
SourceFile (NONAME [NTFS][root][Users\srogers\AppData\Roaming\Microsoft\Windows\Recent])	Source Created	Source Modified	Source Accessed	File Size	DriveType	Volume Serial Number	Volume Label	LocalPath
Presentation with Sensitive IP.lnk	2019-01-21 05:07:00	2019-01-21 05:07:00	2022-10-07 05:06:43	31590	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Shield Documents\Presentation with Sensitive IP.pptx
The Internet.lnk	2019-01-19 03:13:02	2019-01-20 21:09:55	2022-10-07 05:06:43	0	(None)			
Alloys (2).lnk	2019-01-21 05:04:43	2019-01-21 05:04:43	2022-10-07 05:06:43	697230	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Desktop\Alloys.pptx
Alloys.lnk	2019-01-21 05:00:45	2019-01-21 05:04:07	2022-10-07 05:06:43	946688	Removable storage media (Floppy, USB)	6A018124	Shield_USB	E:\Alloys.ppt
Documents.lnk	2019-01-21 05:06:50	2019-01-21 05:06:50	2022-10-07 05:06:43	4096	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents
Random Accounting Spreadsheet.lnk	2019-01-21 19:16:10	2019-01-21 19:16:10	2022-10-07 05:06:43	10144	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Personal\Random Accounting Spreadsheet.xlsx
USB Backup.lnk	2019-01-21 05:06:50	2019-01-21 19:15:47	2022-10-07 05:06:43	4096	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup
Selection_of_materials.lnk	2019-01-21 19:15:47	2019-01-21 19:15:47	2022-10-07 05:06:43	4237312	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Selection_of_materials.ppt

Shield Documents.lnk	2019-01-21 05:05:04	2019-01-21 05:07:00	2022-10-07 05:06:43	4096	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Shield Documents
Cap-1.lnk	2019-01-21 05:22:40	2019-01-21 05:22:40	2022-10-07 05:06:43	0	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\Cap-1.jpg
Personal.lnk	2019-01-21 05:06:25	2019-01-21 19:16:10	2022-10-07 05:06:43	4096	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Personal
Cap-2.lnk	2019-01-21 05:23:13	2019-01-21 05:23:13	2022-10-07 05:06:43	0	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\Cap-2.jpg
This PC.lnk	2019-01-21 05:06:50	2019-01-21 05:06:50	2022-10-07 05:06:43	0	(None)			
Confidential Alloy Expense Accounts.lnk	2019-01-21 05:05:04	2019-01-21 05:06:18	2022-10-07 05:06:43	10147	Removable storage media (Floppy, USB)	6A018124	Shield USB	E:\Shield Documents\Confidential Alloy Expense Accounts.xlsx
ms-settingsnetwork.lnk	2019-01-20 21:09:55	2019-01-20 21:09:55	2022-10-07 05:06:43	0	(None)			
Shield_USB (E).lnk	2019-01-21 05:00:45	2019-01-21 05:04:46	2022-10-07 05:06:43	0	Removable storage media (Floppy, USB)	6A018124	Shield USB	E:\
Chapter 4.lnk	2019-01-21 05:04:46	2019-01-21 19:14:41	2022-10-07 05:06:43	1008692	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Chapter 4.pdf
S. Rogers Resume.lnk	2019-01-21 05:06:24	2019-01-21 05:06:25	2022-10-07 05:06:43	17597	Removable storage media (Floppy, USB)	6A018124	Shield USB	E:\Personal\S. Rogers Resume.docx

Jump List Analysis

1. Extract or unzip the JLECmd archive.
2. Open a command prompt and navigate to the extracted JLECmd folder.
3. Simply run **JLECmd.exe** to see the available options and review them.
4. Run the tool from the command line as follows: **JLECmd -d "Directory of exported Automatic Jump Lists" --csv "Directory Output\jump.csv"**

```
$. /JLECmd.exe -d ../../Labs/CaseFolder/Recent/ --csv ../../Labs/CaseFolder/JumpAnalysis
```

5. Open the two new .CSVs and **SAVE AS** an Excel spreadsheet before editing (example: Automatic_jump.xls or .xlsx), which allows editing while preserving original data and formatting.
6. Delete (or hide) all columns except: **TargetCreated, TargetModified, FileSize, DriveType, VolumeSerialNumber, VolumeLabel, LocalPath, and Machine ID.**
7. Delete or hide any rows without timestamps or actual LocalPath information (two should be removed).

8. Review the **SourceCreated**, **SourceModified**, **VolumeSerialNumber**, **VolumeLabel**, and **LocalPath** fields and answer the questions below.

20221007053701_AutomaticDestinations								
SourceFile	TargetCreated	TargetModified	File Size	DriveType	VolumeSerialNumber	VolumeLabel	LocalPath	MachinelID
83dd64e7fa560bd5.a utomaticDestinations- ms	2019-01-21 05:06:54	2019-01-21 03:50:58	101 44	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Personal\Random Accounting Spreadsheet.xlsx	avegers01
83dd64e7fa560bd5.a utomaticDestinations- ms	2019-01-21 04:59:17	2019-01-21 04:11:14	101 47	Removable storage media (Floppy, USB)	6A018124	Shield _USB	E:\Shield Documents\Confidential Alloy Expense Accounts.xlsx	
9d1f905ce5044aee.au tomaticDestinations- ms	2019-01-21 05:06:54	2019-01-21 04:55:58	100 869 2	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Chapter 4.pdf	avegers01
9d1f905ce5044aee.au tomaticDestinations- ms	2019-01-21 04:59:58	2019-01-21 04:55:58	100 869 2	Removable storage media (Floppy, USB)	6A018124	Shield _USB	E:\Chapter 4.pdf	
d38a3ea7ec79fbed.au tomaticDestinations- ms	2019-01-21 04:59:17	2019-01-21 03:58:34	175 97	Removable storage media (Floppy, USB)	6A018124	Shield _USB	E:\Personal\S. Rogers Resume.docx	
ecd1a5e2c3af9c46.au tomaticDestinations- ms	2019-01-21 05:06:54	2019-01-21 04:58:06	423 731 2	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Selection_of_materials.ppt	avegers01
ecd1a5e2c3af9c46.au tomaticDestinations- ms	2019-01-21 05:06:54	2019-01-21 03:48:38	315 90	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Shield Documents\Presentation with Sensitive IP.pptx	avegers01
ecd1a5e2c3af9c46.au tomaticDestinations- ms	2019-01-21 05:04:38	2019-01-21 05:04:42	697 230	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Desktop\Alloys.pptx	avegers01
ecd1a5e2c3af9c46.au tomaticDestinations- ms	2019-01-21 04:59:57	2019-01-21 04:56:56	946 688	Removable storage media (Floppy, USB)	6A018124	Shield _USB	E:\Alloys.ppt	
f01b4d95cf55d32a.au tomaticDestinations- ms	2019-01-21 05:06:54	2019-01-21 19:16:11	409 6	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Personal	avegers01
f01b4d95cf55d32a.au tomaticDestinations- ms	2019-01-21 05:06:45	2019-01-21 19:15:49	409 6	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup	avegers01
f01b4d95cf55d32a.au tomaticDestinations- ms	2019-01-21 16:57:05	2019-01-21 16:57:05	409 6	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Downloads\shielddocument s	avegers01
f01b4d95cf55d32a.au tomaticDestinations- ms	2019-01-19 03:11:57	2019-01-21 05:23:12	409 6	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents	avegers01
f01b4d95cf55d32a.au tomaticDestinations- ms	2019-01-21 05:21:26	2019-01-21 05:21:26	409 6	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Shield Documents	avegers01
f01b4d95cf55d32a.au tomaticDestinations- ms	2019-01-21 05:06:54	2019-01-21 05:07:41	409 6	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Dropbox\Shield Documents	avegers01
f01b4d95cf55d32a.au tomaticDestinations- ms	2019-01-21 05:09:39	2019-01-21 05:21:16	409 6	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Dropbox	avegers01
f01b4d95cf55d32a.au tomaticDestinations- ms	2019-01-21 04:59:17	2019-01-21 04:54:20	0	Removable storage media (Floppy, USB)	6A018124	Shield _USB	E:\Personal	
f01b4d95cf55d32a.au tomaticDestinations- ms	2019-01-21 04:59:17	2019-01-21 04:57:06	0	Removable storage media (Floppy, USB)	6A018124	Shield _USB	E:\Shield Documents	
f01b4d95cf55d32a.au tomaticDestinations- ms	2019-01-19 03:11:57	2019-01-21 05:04:43	409 6	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Desktop	avegers01
f01b4d95cf55d32a.au tomaticDestinations- ms	2019-01-19 03:11:57	2019-01-19 03:12:57	0	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Downloads	desktop- 16pttv2
f01b4d95cf55d32a.au tomaticDestinations- ms	2019-01-19 03:11:57	2019-01-19 03:12:57	0	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Videos	desktop- 16pttv2

<u>f01b4d95cf55d32a.automaticDestinations-ms</u>	2019-01-19 03:11:57	2019-01-19 03:12:57	0	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Music	desktop-16pttv2
<u>f01b4d95cf55d32a.automaticDestinations-ms</u>	2019-01-19 03:11:57	2019-01-19 03:12:57	0	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Pictures	desktop-16pttv2
<u>5f7b5f1e01b83767.automaticDestinations-ms</u>	2019-01-21 05:06:54	2019-01-21 03:50:58	10144	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Personal\Random Accounting Spreadsheet.xlsx	avengers01
<u>5f7b5f1e01b83767.automaticDestinations-ms</u>	2019-01-21 05:06:54	2019-01-21 04:58:06	4237312	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Selection_of_materials.ppt	avengers01
<u>5f7b5f1e01b83767.automaticDestinations-ms</u>	2019-01-21 05:06:54	2019-01-21 04:55:58	1008692	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\USB Backup\Chapter 4.pdf	avengers01
<u>5f7b5f1e01b83767.automaticDestinations-ms</u>	2019-01-21 05:23:12	2019-01-21 05:23:13	0	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\Cap-2.jpg	avengers01
<u>5f7b5f1e01b83767.automaticDestinations-ms</u>	2019-01-21 05:22:40	2019-01-21 05:22:40	0	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Documents\Cap-1.jpg	avengers01
<u>5f7b5f1e01b83767.automaticDestinations-ms</u>	2019-01-21 05:06:54	2019-01-21 03:48:38	31590	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Dropbox\Shield Documents\Presentation with Sensitive IP.pptx	avengers01
<u>5f7b5f1e01b83767.automaticDestinations-ms</u>	2019-01-21 04:59:17	2019-01-21 03:58:34	17597	Removable storage media (Floppy, USB)	6A018124	Shield_USB	E:\Personal\S. Rogers Resume.docx	
<u>5f7b5f1e01b83767.automaticDestinations-ms</u>	2019-01-21 04:59:17	2019-01-21 04:11:14	10147	Removable storage media (Floppy, USB)	6A018124	Shield_USB	E:\Shield Documents\Confidential Alloy Expense Accounts.xlsx	
<u>5f7b5f1e01b83767.automaticDestinations-ms</u>	2019-01-21 04:59:58	2019-01-21 04:55:58	1008692	Removable storage media (Floppy, USB)	6A018124	Shield_USB	E:\Chapter 4.pdf	
<u>5f7b5f1e01b83767.automaticDestinations-ms</u>	2019-01-21 05:04:38	2019-01-21 05:04:42	697230	Fixed storage media (Hard drive)	EA174897		C:\Users\srogers\Desktop\Alloys.pptx	avengers01
<u>5f7b5f1e01b83767.automaticDestinations-ms</u>	2019-01-21 04:59:57	2019-01-21 04:56:56	946688	Removable storage media (Floppy, USB)	6A018124	Shield_USB	E:\Alloys.ppt	

20221007053701_CustomDestinations								
SourceFile	TargetCreated	TargetModified	File Size	DriveType	VolumeSerialNumber	VolumeLabel	LocalPath	MachineID
<u>5d696d521de238c3.customDestinations-ms</u>	2019-01-20 02:44:31	2018-12-12 05:11:41	1587680	Fixed storage media (Hard drive)	EA174897		C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	desktop-16pttv2
<u>5d696d521de238c3.cust omDestinations-ms</u>	2019-01-20 02:44:31	2018-12-12 05:11:41	1587680	Fixed storage media (Hard drive)	EA174897		C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	desktop-16pttv2
<u>5d696d521de238c3.cust omDestinations-ms</u>	2019-01-20 02:44:31	2018-12-12 05:11:41	1587680	Fixed storage media (Hard drive)	EA174897		C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	desktop-16pttv2
<u>5d696d521de238c3.cust omDestinations-ms</u>	2019-01-20 02:44:31	2018-12-12 05:11:41	1587680	Fixed storage media (Hard drive)	EA174897		C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	desktop-16pttv2
<u>d73913f45fe28db3.cust omDestinations-ms</u>	2019-01-21 16:58:30	2018-07-17 16:25:08	7081696	Fixed storage media (Hard drive)	EA174897		C:\Program Files\Cybertron\Privacy Eraser\PrivacyEraser64.exe	avengers01
<u>d73913f45fe28db3.cust omDestinations-ms</u>	2019-01-21 16:58:30	2018-07-17 16:25:08	7081696	Fixed storage media (Hard drive)	EA174897		C:\Program Files\Cybertron\Privacy Eraser\PrivacyEraser64.exe	avengers01
<u>d73913f45fe28db3.cust omDestinations-ms</u>	2019-01-21 16:58:30	2018-07-17 16:25:08	7081696	Fixed storage media (Hard drive)	EA174897		C:\Program Files\Cybertron\Privacy Eraser\PrivacyEraser64.exe	avengers01

Shellbag Analysis

1. Extract or unzip the ShellbagsExplorer archive (included is a CLI and GUI tool to parse shellbag information).
2. Open a command prompt and navigate to the extracted SBECmd folder.
3. Simply run **SBECmd.exe** to see the available options and review them.
4. Run the tool from the command line as follows: **SBECmd -d "Directory of exported Registry Files" --csv "Directory Output\sbags.csv"** **NOTE: You may receive an error that the transaction logs must be included. Export all NTUSER.DAT and USRCLASS.DAT logs from the evidence image as well as the two hives.**
5. Open the new .CSV and **SAVE AS** an Excel spreadsheet before editing (example: Automatic_jump.xls or .xlsx), which allows editing while preserving original data and formatting.
6. Delete (or hide) all columns except: **AbsolutePath, ShellType, Value, CreatedOn, and Modified on columns.**
7. Answer the questions below.

ShellBags Explorer

ShellBags Explorer v1.4.0.0

File Tools Help

Value

Desktop

E:\

- Imaging and Triage Lab
- SANS To Sort
- Forensic Tools
- Imager_Lite_3.1.1
- Personal
- Shield Documents
- Shared Documents Folder (Users Files)
- Dropbox
- Shield Documents
- My Computer
- Documents
- USB Backup
- Personal
- Shield Documents
- Downloads
- shielddocuments
- Pictures
- Desktop
- C:\
- Users
- srogers
- AppData
- Roaming
- Microsoft
- Windows
- Recent
- Local
- Microsoft
- Windows
- Search Folder
- Search Folder
- D:\
- Home Folder

Drag a column header here to group by that column

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted
c:	No im...	#c:	=	=	=	=	=
My Computer		Root folder: GUID	2				
Home Folder		Root folder: GUID	7				2019-01-20 19:18:
C:\		Users property view: Drive letter	3				
D:\		Users property view: Drive letter	6				2019-01-20 19:18:
E:\		Users property view: Drive letter	0				
Shared Documents Folder (Users Files)		Root folder: GUID	1				
Search Folder		Users property view	5				2019-01-21 19:13:
Search Folder		Users property view	4				2019-01-21 19:13:

Summary Details Hex

ShellBag items: 8

'UsrClass.dat' Registry hive loaded in 0.5676 seconds! 8 shellbags loaded in 0.0229 seconds Time zone: UTC 8 of 8 rows visible (100.00%)

```
$. /SBECmd.exe -d ../../Labs/CaseFolder/ --csv ../../Labs/CaseFolder/ShellbagAnalysis
```

Blank NTUSER.csv

UsrClass					
BagPath	AbsolutePath	ShellType	Value	CreatedOn	ModifiedOn
BagMRU	Desktop\My Computer	Root folder: GUID	My Computer		
BagMRU	Desktop\Home Folder	Root folder: GUID	Home Folder		
BagMRU	Desktop\C:\	Users property view: Drive letter	C:\		
BagMRU	Desktop\D:\	Users property view: Drive letter	D:\		
BagMRU	Desktop\E:\	Users property view: Drive letter	E:\		
BagMRU	Desktop\Shared Documents Folder (Users Files)	Root folder: GUID	Shared Documents Folder (Users Files)		
BagMRU	Desktop\Search Folder	Users property view	Search Folder		
BagMRU	Desktop\Search Folder	Users property view	Search Folder		
BagMRU\0	Desktop\My Computer\Downloads	Root folder: GUID	Downloads		
BagMRU\0	Desktop\My Computer\Documents	Root folder: GUID	Documents		
BagMRU\0	Desktop\My Computer\Desktop	Root folder: GUID	Desktop		
BagMRU\0	Desktop\My Computer\Pictures	Root folder: GUID	Pictures		
BagMRU\0\0	Desktop\My Computer\Downloads\shielddocuments	Directory	shielddocuments	1/21/19 16:57	1/21/19 16:57
BagMRU\0\1	Desktop\My Computer\Documents\USB Backup	Directory	USB Backup	1/21/19 05:06	1/21/19 05:06
BagMRU\0\1\0	Desktop\My Computer\Documents\USB Backup\Shield Documents	Directory	Shield Documents	1/21/19 05:06	1/21/19 05:06
BagMRU\0\1\0	Desktop\My Computer\Documents\USB Backup\Personal	Directory	Personal	1/21/19 05:06	1/21/19 05:06
BagMRU\2	Desktop\C:\Users	Directory	Users	9/29/17 08:45	1/20/19 02:44
BagMRU\2\0	Desktop\C:\Users\srogers	Directory	srogers	1/19/19 03:11	1/21/19 05:09
BagMRU\2\0\0	Desktop\C:\Users\srogers\AppData	Directory	AppData	1/19/19 03:11	1/19/19 03:12
BagMRU\2\0\0\0	Desktop\C:\Users\srogers\AppData\Local	Directory	Local	1/19/19 03:11	1/21/19 16:58
BagMRU\2\0\0\0	Desktop\C:\Users\srogers\AppData\Roaming	Directory	Roaming	1/19/19 03:11	1/21/19 18:22
BagMRU\2\0\0\0\0	Desktop\C:\Users\srogers\AppData\Local\Microsoft	Directory	Microsoft	1/19/19 03:11	1/20/19 21:17
BagMRU\2\0\0\0\0\0	Desktop\C:\Users\srogers\AppData\Local\Microsoft\Windows	Directory	Windows	1/19/19 03:11	1/21/19 05:09
BagMRU\2\0\0\0\1	Desktop\C:\Users\srogers\AppData\Roaming\Microsoft	Directory	Microsoft	1/19/19 03:11	1/20/19 21:27
BagMRU\2\0\0\0\1\0	Desktop\C:\Users\srogers\AppData\Roaming\Microsoft\Windows	Directory	Windows	1/19/19 03:11	1/19/19 03:13
BagMRU\2\0\0\0\1\0\0	Desktop\C:\Users\srogers\AppData\Roaming\Microsoft\Windows\Recent	Directory	Recent	1/19/19 03:11	1/21/19 05:23
BagMRU\4	Desktop\E:\Personal	Directory	Personal	1/21/19 04:59	1/21/19 04:54
BagMRU\4	Desktop\E:\Shield Documents	Directory	Shield Documents	1/21/19 04:59	1/21/19 04:57
BagMRU\4	Desktop\E:\Forensic Tools	Directory	Forensic Tools	1/21/19 18:34	1/21/19 18:34
BagMRU\4	Desktop\E:\SANS To Sort	Directory	SANS To Sort	1/21/19 18:33	1/21/19 18:33
BagMRU\4	Desktop\E:\Imaging and Triage Lab	Directory	Imaging and Triage Lab	1/21/19 19:54	1/21/19 19:54
BagMRU\4\2	Desktop\E:\Forensic Tools\Imager Lite 3.1.1	Directory	Imager_Lite_3.1.1	1/21/19 18:37	1/21/19 18:37
BagMRU\5	Desktop\Shared Documents Folder (Users Files)\Dropbox	Users Files Folder	Dropbox	1/21/19 05:09	1/21/19 05:09
BagMRU\5\0	Desktop\Shared Documents Folder (Users Files)\Dropbox\Shield Documents	Directory	Shield Documents	1/21/19 05:06	1/21/19 05:07

USB Device Analysis

1. Extract or unzip the “USB Detective” archive.
2. Execute the GUI application (v1.3.6) and accept the User Account Control prompt.
3. Select the “**Select Files/Folders...**” when prompted for the Input Data source.
4. Complete the **Case Information** section and choose the appropriate evidence artifacts from your triage collection (**SYSTEM, SOFTWARE, NTUSER.DAT, and the Setupapi Log** options).
5. Choose **Process Artifacts**.

- Ignore transaction log error.
- Review the output and answer the questions below.

Serial/UID	Description	First Connected (UTC)	Last Connected (UTC)	Last Disconnected (UTC)	Volume Name/Label	Drive Letter(s)	VSN	Last User
20070620000000059187F6F	Kingston DataTraveler 2.0 USB Device	1/21/2019 5:00:14 AM	1/21/2019 5:17:03 PM	1/21/2019 6:41:06 PM	Shield_USB	E:		NTUSER_sroger

NOTE: Typically students are walked through pulling removable media information manually first. This is because some tools may not pull all data, or do so correctly. In this case, use the slides or SANS USB cheat sheet to manually pull the information from the hives or setupapi.dev.log.

Prefetch Analysis

- Extract or unzip the PECmd archive.
- Open a command prompt and navigate to the extracted PECmd folder.
- Simply run **PECmd.exe** to see the available options and review them.
- Run the tool from the command line as follows: **PECmd -d "Directory of exported Prefetch Files" --csv "Directory Output\prefetch.csv"**

```
$. /PECmd.exe -d {$PWD}/../Labs/CaseFolder/Prefetch --csv {$PWD}/../Labs/CaseFolder/PrefetchAnalysis
```

- Open the new .CSV and **SAVE AS** an Excel spreadsheet before editing (example: Automatic_jump.xls or .xlsx), which allows editing while preserving original data and formatting.
- Delete (or hide) all columns except: **SourceCreated and SourceModified timestamps, ExecutableName, Size, RunCount, LastRun, PreviousRun# (7 columns max), and Volume0Serial.**
- Delete or hide any rows with long, miscellaneous data including directory paths (there should be 6).
- Review the **SourceCreated, SourceModified, ExecutableName, RunCount, PreviousRun#, and Volume0Serial** fields and answer the questions below.

20221007211959_PECmd_Output														
SourceFilename	Source Create d	Source Modified	Executable Name	Size	RunCount	LastRun	PreviousRun0	PreviousRun1	PreviousRun2	PreviousRun3	PreviousRun4	PreviousRun5	PreviousRun6	Volume0 Serial
CONHOST.EXE-F98A1078.pf	2019-01-19 03:22:06	2019-01-21 19:49:57	CONHOST.EXE	28406	42	2019-01-21 19:49:47	2019-01-21 19:37:43	2019-01-21 19:23:05	2019-01-21 19:07:26	2019-01-21 18:51:32	2019-01-21 18:41:07	2019-01-21 18:12:50	2019-01-21 17:56:08	CEFB0E37
CONSENT.EXE-2D674CE4.pf	2019-01-19 03:21:45	2019-01-21 19:49:47	CONSENT.EXE	130694	10	2019-01-21 19:49:46	2019-01-21 16:57:42	2019-01-20 21:26:05	2019-01-20 21:13:27	2019-01-20 21:11:19	2019-01-20 21:09:46	2019-01-20 02:47:16	2019-01-20 02:44:09	CEFB0E37
EDD.EXE-F38EB619.pf	2019-01-21 19:49:57	2019-01-21 19:49:57	EDD.EXE	29050	1	2019-01-21 19:49:47								CEFB0E37
FTK IMAGER.EXE-57AE1478.pf	2019-01-21 19:50:48	2019-01-21 19:50:48	FTK IMAGER.EXE	112198	1	2019-01-21 19:50:38								CEFB0E37

BITTORRENT .EXE- 17035B82.pf	2019-01-20 21:27:28	2019-01-20 21:27:28	BITTORRENT.EXE	108952	1	2019-01-20 21:27:18								EA174897
BITTORRENT .EXE- 1749C890.pf	2019-01-20 21:26:13	2019-01-20 21:26:13	BITTORRENT.EXE	48388	1	2019-01-20 21:26:03								EA174897
DROPBOX.EX E-41A1197E.pf	2019-01-20 21:18:01	2019-01-20 21:18:07	DROPBOX.EXE	155234	4	2019-01-20 21:17:55	2019-01-20 21:17:55	2019-01-20 21:17:59	2019-01-20 21:17:55					EA174897
DROPBOX.EX E-B349B609.pf	2019-01-20 21:17:24	2019-01-20 21:17:24	DROPBOX.EXE	151882	1	2019-01-20 21:17:18								EA174897
DROPBOXINSTALLED.EXE- 89207B53.pf	2019-01-20 21:13:36	2019-01-20 21:13:36	DROPBOXINSTALLER.EXE	39974	1	2019-01-20 21:13:26								EA174897
SEARCHFILTERHOST.EXE- 10E4267C.pf	2019-01-19 03:15:18	2019-01-21 19:51:29	SEARCHFILTERHOST.EXE	16574	59	2019-01-21 19:51:19	2019-01-21 19:41:07	2019-01-21 19:21:19	2019-01-21 19:17:26	2019-01-21 19:14:43	2019-01-21 19:07:21	2019-01-21 19:02:23	2019-01-21 18:57:21	EA174897
TOR.EXE- 37D54E52.pf	2019-01-21 05:10:59	2019-01-21 05:10:59	TOR.EXE	45416	1	2019-01-21 05:10:49								EA174897

Exercise – Questions

LNK File Analysis

1. What was the machine ID of the system these files were collected from?

avengers01

2. Was any removable media connected to the system? If so, what was the Volume Label of the device where files were opened from?

Yes, four instances had “Shield_USB” as the removable media connected to the system

3. What is the Volume Serial Number of any removable device connected, if any?

For the above Volume Label, the corresponding VolumeSerialNumber is “6A018124”

4. What was the volume letter assigned to any removable media connected to the system?

The volume letter assigned to the removable media is “E”

5. Were there any files of interest that were opened? If so, please list any files that should be investigated and the first and last times these files were opened.

Yes, there was a file opened from the removable media titled “Confidential Alloy Expense Accounts.xlsx”. Other interesting files were “Presentation with Sensitive IP.pptx” , “Random Accounting Spreadsheet.xlsx” and “Shield Documents”

Jump List Analysis

1. How many files were identified as being on a USB? Were there any differences from those identified during the LNK file analysis?

There are 10 files with the VolumeLabel "Shield_USB". There are 7 additional files than the LNK file analysis (4 were duplicates), 3 Files matched what was found in the LNK file analysis, 3 were in the C: drive under USB Backups.

2. There are two Machine IDs that appear to have similar information as the primary disk. What hypothesis can we make about the difference between the two IDs?

The two MachineIDs are "avengers01" and "desktop-16pttv2". The latter MID are the folders under the user "srogers" of Downloads, Videos, Music and Pictures. These seem like the default directory structure of a Windows machine. However, they are of size 0, where Desktop and Documents have data. That can mean that these 4 areas owned by desktop-16pttv2 haven't been touched and can be ignored from the investigation.

3. What is the largest file documented from Jump List analysis?

Selection_of_materials.ppt

4. When might have the E: volume first been accessed by the user? Include the date and time.

The first time a user might have accessed the E: drive was at "2019-01-21 04:59:16"

5. What is the volume serial number of the primary hard drive?

The primary hard drive's volume serial number (Fixed storage media) is "EA174897"

Shellbag Analysis

1. Are there any shellbags in the NTUSER.DAT .csv? Why or why not?

There are no shellbags in NTUSER.csv. On modern OSs there are more items in USRClass than NTUSER. USRClass is used for registry purposes for the system and NTUser is used for keys for the user. The user may have the privileges to wipe the NTUser information, but unable to remove actions tracked in USRClass.

2. Can you identify any directories that might exist on external media?

Anything in the E: drive is external media. These files were moves from or to the local system from the external media. Also under Misc. column, it stats that the E: drive data is under exFAT file system. Most local system states NTFS file system or blank.

Desktop\E:\

Desktop\E:\\Forensic Tools
Desktop\E:\\Forensic Tools\\Imager_Lite_3.1.1
Desktop\E:\\Imaging and Triage Lab
Desktop\E:\\Personal
Desktop\E:\\SANS To Sort
Desktop\E:\\Shield Documents

3. What connects shellbag information with potential removable media, if anything?

I believe that the "Value" column connects shellbag information with potential removable media. Since the value for "Shield Documents" and ignoring Upper/Lower case and Whitespaces, I can track the four locations that Shield Documents traveled (Number 5).

4. Are there any shellbags that identify potential IP being exfiltrated from the corporate defenses? If so, can you identify any descriptors of that IP data?

Shield Documents seems like a shellbag of interest to track where the IP is sourced and its destination. This is evidence that sensitive information is because taken from a corporate system.

5. If you filter the shellbag data by "Value," and review the order of the timestamps (in standard and military time), what conclusions can be drawn about how the folder "Shield Documents" made its way onto the system, where it was first stored, and the ways the folder may have been removed from the system?

BagPath	AbsolutePath	ShellType	Value	CreatedOn	ModifiedOn
BagMRU\4	Desktop\E:\\Shield Documents	Directory	Shield Documents	1/21/19 04:59	1/21/19 04:57
BagMRU\0\1\0	Desktop\My Computer\Documents\USB Backup\Shield Documents	Directory	Shield Documents	1/21/19 05:06	1/21/19 05:06
BagMRU\5\0	Desktop\Shared Documents Folder (Users Files)\Dropbox\Shield Documents	Directory	Shield Documents	1/21/19 05:06	1/21/19 05:07
BagMRU\0\0	Desktop\My Computer\Downloads\shielddocuments	Directory	shielddocuments	1/21/19 16:57	1/21/19 16:57

Based on the location of Shield Documents and timestamp of its actions. It seems that Shield Documents was copied onto the E: drive. Moved to the local Desktop via a USB Backup directory. Moved into Dropbox and then finally to the local downloads area. I also found that the MFTEntry (matching "Short name: SHIELD~1") value from Dropbox to USB Backup match. However when it goes from E: drive and onto the local system it changes (Short Name stays the same on the local system). Signature: 0xbeef0004 is constant throughout all four locations.

USB Device Analysis

1. What is the serial number of any connected devices?

200706200000000059187F6F

2. What is the description of this device?

Kingstone Data Traveler 2.0 USB Device

3. When was the device first and last connected?

First: 1/21/2019 5:00:14 AM

Last: 1/21/2019 5:17:03 PM

4. Can you identify the volume name/label?

Shield_USB (as explored in other analyses)

5. What was the drive letter assigned by the operating system at the time of last connection?

E:

Prefetch Analysis

1. List at least three unique applications that might cause concern and should be investigated. Include the number of times run and the last run time for each application.

Executable Name	Hash	Number of Times Ran	Last Time Ran
BITTORRENT.EXE	1749C890	1	2019-01-20 21:26:03
	17035B82	1	2019-01-20 21:27:18
DROPBOX.EXE	41A1197E	4	2019-01-20 21:17:55
	B349B609	1	2019-01-20 21:17:18
TOR.EXE	37D54E52	1	2019-01-21 05:10:49

2. When was the Dropbox installer run?

2019-01-20 21:13:26

3. What file was run the most amount of times?

Executable Name	Hash	Number of Times Ran	Last Time Ran
SEARCHFILTERHOST.EXE	10E4267C	59	2019-01-21 19:51:19

What is the function of this file according to open source information?

The function of this file sounds to be searching and filtering hostnames based on user input

4. When was FTK Imager and EDD run? Why should these applications be whitelisted?

Executable Name	Hash	Number of Times Ran	Last Time Ran
FTK IMAGER.EXE	57AE1478	1	2019-01-21 19:50:38
EDD.EXE	F38EB619	1	2019-01-21 19:49:47

These applications should be whitelisted (or deemed safe and allowed to run on the system). FTK Imager should be permitted because it paints a bigger picture of what was run on the system by security. EDD.exe should be allowed because non-system processes track these processes and paint a bigger picture of what is going on in the system by security.

5. Given the files executed from the volume, what type of device or media would you believe the Volume Serial CEFB0E37 identifies?

Executable Name	Hash	Number of Times Ran	Last Time Ran
< Includes Chart from Number 4 Above >			
CONHOST.EXE	F98A1078	42	2019-01-21 19:49:47
CONSENT.EXE	2D674CE4	10	2019-01-21 19:49:46

CONHOST.EXE (Console Windows Host) allows the Command Prompt to interact with File Explorer. One function it allows is drag and drop files and directories into the command prompt.

CONSENT.EXE (Consent UI for administrative applications) is called when a user executes system-wide actions. This checks the authentication of the user to perform this action.

These applications (extended from Number 4) located on the Volume Serial CEFB0E37 are necessary to be run to keep the system secure and available to security investigators. Without these applications, malicious users can secretly perform root-level actions while hiding their tracks. This volume, seen in this analysis, is a list of applications that should be whitelisted and required for all Windows systems.

Source:

<https://www.lifewire.com/conhost-exe-4158039>

<https://www.file.net/process/consent.exe.html>

Exercise—Key Takeaways

- Shell item analysis can identify files and applications that no longer exist on a system
- Shell item analysis can provide insight into insider threats and attacker activity
- USB device analysis allows us to identify potential infection vectors and data exfiltration
- USB device analysis can provide an investigator with additional sources of evidence for forensics

***Please submit the final assignment as a single .PDF and any applicable reports as a .ZIP file.**

****Screenshots may also be added to this document when appropriate.**