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]](#footnote-1)

**Files Needed:**

NONAME [NTFS]|[root]|Users|srogers|AppData|Roaming|Microsoft|Windows|Recent

**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.
4. Run the tool from the command line as follows: **LECmd –d “Directory of exported LNK Files” --csv “Directory Output\lnk.csv”**

$ ./LECmd.exe -d ../../Module\_4/Lab\_3/CaseFolder/Recent/ --csv ../../Module\_4/Lab\_3/CaseFolder/LinkAnalysis.csv

1. 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.
2. Delete (or hide) all columns except: **SourceCreated, SourceModified, SourceAccessed, FileSize, DriveType, VolumeSerialNumber, VolumeLabel, and LocalPath.**
3. Delete or hide any rows without timestamps or actual LocalPath information (three should be removed).
4. 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).
5. 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.

**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”**
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.

**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.

**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**.
6. Ignore transaction log error.
7. Review the output and answer the questions below.

**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**

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

$ ./PECmd.exe -d ../../Module\_4/Lab\_3/CaseFolder/Prefetch/ --csv ../../Module\_4/Lab\_3/CaseFolder/PrefetchAnalysis.csv

1. 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.
2. Delete (or hide) all columns except: **SourceCreated and SourceModified timestamps, ExecutableName, Size, RunCount, LastRun, PreviousRun# (7 columns max), and Volume0Serial.**
3. Delete or hide any rows with long, miscellaneous data including directory paths (there should be 6).
4. Review the **SourceCreated, SourceModified, ExecutableName, RunCount, PreviousRun#, and Volume0Serial** fields and answer the questions below.

# Exercise – Questions

**LNK File Analysis**

1. What was the machine ID of the system these files were collected from?
2. Was any removable media connected to the system? If so, what was the Volume Label of the device where files were opened from?
3. What is the Volume Serial Number of any removable device connected, if any?
4. What was the volume letter assigned to any removable media connected to the system?
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.

**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?
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?
3. What is the largest file documented from Jump List analysis?
4. When might have the E: volume first been accessed by the user? Include the date and time.
5. What is the volume serial number of the primary hard drive?

**Shellbag Analysis**

1. Are there any shellbags in the NTUSER.DAT .csv? Why or why not?
2. Can you identify any directories that might exist on external media?
3. What connects shellbag information with potential removable media, if anything?
4. Are they any shellbags that identify potential IP being exfiltrated from the corporate defenses? If so, can you identify any descriptors of that IP data?
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 it’s what on to the system, where it was first stored, and the ways the folder may have been removed from the system?

**USB Device Analysis**

1. What is the serial number of any connected devices?
2. What is the description of this device?
3. When was the device first and last connected?
4. Can you identify the volume name/label?
5. What was the drive letter assigned by the operating system at the time of last connection?

**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.
2. When was the Dropbox installer run?
3. What file was run the most amount of times? What is the function of this file according to open source information?
4. When was FTK Imager and EDD run? Why should these applications be whitelisted?
5. Given the files executed from the volume, what type of device or media would you believe the Volume Serial CEFB0E37 identifies?

# 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.

1. [USB Detective](https://northeastern-my.sharepoint.com/:u:/g/personal/e_booker_northeastern_edu/EQA-exp496pJpXDbSEH-8WgBP7_ZJmGtB5V2CpXX_eGnLg?e=DvkYqZ) [↑](#footnote-ref-1)