**Text

Description automatically generated**

**Case Project 01**

**CY5210 Information System Forensics**

**Instructor: Elton Booker**

**Jonathan Metzger**

# Table of Contents

[Table of Contents 2](#_Toc116592001)

[EXECUTIVE SUMMARY 4](#_Toc116592002)

[INTRODUCTION 5](#_Toc116592003)

[ANALYSIS 6](#_Toc116592004)

[REGISTRY 6](#_Toc116592005)

[USER 7](#_Toc116592006)

[USB DEVICE 8](#_Toc116592007)

[APPLICATION 9](#_Toc116592008)

[PREFETCH 10](#_Toc116592009)

[SHELLBAG ITEMS 11](#_Toc116592010)

[LINKED FILES 12](#_Toc116592011)

[JUMP FILES 13](#_Toc116592012)

[MALWARE APPLICATIONS 14](#_Toc116592013)

[CONCLUSION 15](#_Toc116592014)

[TOOLS 16](#_Toc116592015)

[APPENDIX 17](#_Toc116592016)

[APPENDIX I: Registry Paths 17](#_Toc116592017)

[APPENDIX II: Artifacts List 17](#_Toc116592018)

[APPENDIX III: Prefetch Analysis 17](#_Toc116592019)

[APPENDIX IV: Link Analysis 18](#_Toc116592020)

[APPENDIX V: Jump List Analysis 19](#_Toc116592021)

[APPENDIX VI: Shellbag Analysis 22](#_Toc116592022)

# EXECUTIVE SUMMARY

[This section should be written last. This section should be one page, or less, or explain the case at a high level. I will often copy the first paragraph of the introduction, remove any technical jargon, and make sure it’s straightforward for non-technical folks. This will include the initial problem, the date you were notified, and how the detection was made (could be 1-2 paragraphs in the end).

I will include any relevant findings of the analysis section, but minimal detail. For example, I may summarize the USB and Shell Items sections to say – J. Smith connected two USB devices to his system. One device, a 32GB Kingston Data Traveler, was connected and four company proprietary documents were moved to the USB drive. I might also include the installation of malware and any attempt to perform anti-forensics using specific software or deleting outside of normal operation.

I will conclude this section with some items noted in the Conclusion section. For example – Analysis of J. Smith’s system identified indicators of data exfiltration via USB devices and personal e-mail. Evidence was clear that J. Smith was disgruntled and intended to leave the company with proprietary data to improve his reputation when he began employment with a competitor. J. Smith performed anti-forensic techniques in attempt to hide his activity. The personal USB devices should be requested and remediated so that proprietary data is not removed from the company, otherwise legal action may need to be initiated against J. Smith.]

**[Note:** This section needs to be less than one page.]

**[Report Notes:** Spell everyone’s name out the first time, but subsequent times their name should be abbreviated to F. LASTNAME. This includes your name as the Forensic Analyst/Investigator. Make sure you use the same tense throughout a paragraph. I attempt to use an active voice and past tense. I also use the “Justify” paragraph formatting, except bulleted points and section headings. If a new section begins at the end of a page, enter “Returns” so the section begins at the top of the next page. Finally, delete all template notes and sections with [] used as a guide before submitting the report.]

[The Executive Summary should be page 2, but the Intro needs to begin on page 3 even if the Executive Summary is only ½ page.]

# INTRODUCTION

There was an alert that was received by Shield SOC that an illegal download for BitTorrent and Privacy Cleaner utilities. Both applications violated the company’s Acceptable Use Policy (AUP) and possibly be Potentially Unwanted Programs (PUPs). The incident response team identified the violated-on Monday, January 21st, 2019, at 3:17:18 PM EST. The Forensics Team was requested to perform an analysis on the system that notified the alert for a Case Study.

The image and devices were acquired and imaged by the Forensics Team on Monday, September 19th, 2022. The Chain of Custody document required for the Case Study was completed on Sunday, October 16th, 2022, EST, and is in Appendix 1. Figure 1 below verified the hash verification of the system. It is calculated in both MD5 and SHA1 hash values. It is checked that the hash computed and reported match. This is essential because the tool checks to see if the image's content was modified, with its integrity in tacked, between computing and reporting on the case. Once the Forensics Team starts their analysis, they have the authority to use the tools FTK Imager Lite, Arsenal Image Mounter, Registry Ripper, AccessData Registry Viewer, LECmd (LNK file parser), JLECmd (Jump List parser), Shellbags Explorer, PECmd (Prefetch file parser) and USB Detective. They can utilize a Windows 11 machine provided to run these tools with administrator privileges.

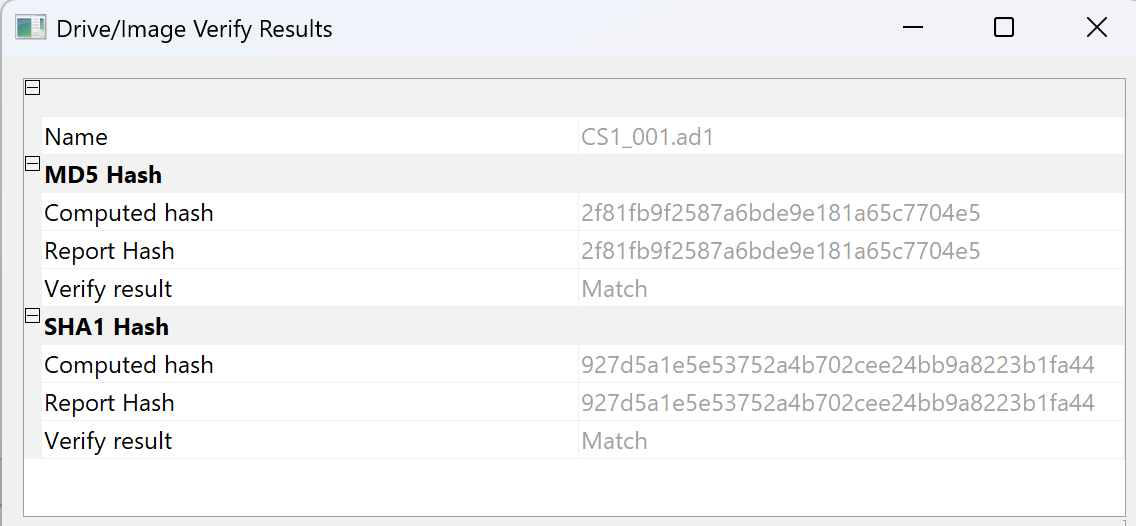


Figure 1 Verification of the system investigated named “CS1\_001”

# ANALYSIS

## REGISTRY

|  |  |
| --- | --- |
| Key | Value |
| Microsoft OS Version | Windows 10 Pro (10.0.16299.15) |
| Build Version | 16299 |
| Current Control Set | 001 |
| Computer Name | AVENGERS01 |
| Time Zone | Eastern Standard Time |
| OS Install Date | 2019-01-19 03:06:56Z |
| Network Interfaces |  |
| Autostart Programs | LastWrite Time 2019-01-20 21:12:14Z - SecurityHealth - %ProgramFiles%\Windows Defender\MSASCuiL.exe - VMware User Process - "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr |
| LastWrite Time 2019-01-20 21:17:39Z - Dropbox - "C:\Program Files (x86)\Dropbox\Client\Dropbox.exe" /systemstartup |
| LastWrite Time 2019-01-20 21:17:37Z  - GrpConv - grpconv -o |
| Last Shutdown Time | 2019-01-20 21:11:38Z |

Table 1 System Information

The hostname “avengers01” was analyzed by the Forensics team to inspect the malicious activity that was reported. On the Windows 10 system, we found that the operating installation time was 2019-01-19 03:06:56Z and set in Eastern Standard time. We used Registry Ripper to analyze the SAM, SYSTEM, SOFTWARE, and User (NTUSER.DAT and USRCLASS.DAT) hives. Our goal was to collect the system’s configurations, settings, user data, and activity to scope a full picture of the activity that went on around the time of the alert.

## USER

Users have the Domain UID of S-1-5-21-263698462-3103634936-1936700066. With “S” indicating the type is a SID, “1” as the revision level, “5” as the authority value, “21” indicating that it is a domain ID and 263698462-3103634936-1936700066 and the “unique identified”. Next are each username “RID” of the system specified below in Table 1. Together make the “Security IDentified” or SID.

No user was under the group Remote Desktop Users, so no user was able to ssh into the system. However, both the Administrator and srogers users are under the group Administrator. All but the Administrator account has their password not required and not expired. This says that the srogers account was given full privileges and not properly secured. User account srogers is a focus of this analysis since that account is given administrative privileges, 10 logins, a password reset time of 2019-01-19 03:11:57Z, password not required and does not expire, and the last login is around the time of the security alert.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Username** | **RID** | **Status** | **Last Login** | **Group** | **Password** |
| **srogers** | 1001 | Enabled, 10 logins | 2019-01-21 18:56:51Z | Administrator | Not Required/Not Expired |
| **Administrator** | 500 | Disabled | Never | Administrator | Not Expire |
| **Guest** | 501 | Disabled | Never | Guest | Not Required/Not Expired |
| **DefaultAccount** | 503 | Disabled | Never | System Managed Accounts Group | Not Required/Not Expired |
| **WDAGUtilityAccount** | 504 | Disabled | Never | n/a | n/a |

Table 2 User Information

The forensics team went through the user activity of the user srogers. They went through the user’s Windows Search History, Typed Paths, RecentDocs, Last Executed Commands and UserAssist findings. These registry locations can be found in APPENDIX 1. After the investigation, the team identified that the user srogers did not search for specific files or applications of interest. The user did not search for specific paths on the systems that related to the investigation. However, RecentDocs revealed that various sensitive files were accessed by the user at the time of the alert. They include the following in order of file creation and modified timestamps.

## USB DEVICE

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device Name** | **Serial Number** | **User Account** | **First Time** | **Last Time** |
| **Kingston Data Traveler 2.0** | 200706200000000059187F6F | sroger | 2019-01-21 05:00:14Z | 2019-01-21 18:41:06Z |

Table 3 USB Device Connected to AVENGERS01

We found that a USB with the labeled name “Kingston Data Traveler 2.0” was connected to the system at the time of the alert. The USB was being accessed by the user srogers through the E: drive. Table 5 above reveals that the first time and last time of the device was between 5:00AM and 6:45PM, more than 13 hours.

## APPLICATION

[Note what applications were downloaded, installed, and executed if they are relevant to a malware investigation or the policy violation being investigated. Were any applications uninstalled from the system in attempt to remove evidence?]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Path** | **Filename** | **LastUsed** | **Download** | **Installed** | **Executed** | **Uninstalled** |
| **2019-01-20 21:10:08Z**  **{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}** | cmd.exe | 2019-01-20 21:10:08Z |  |  | X |  |
| **C:\Users\srogers\Downloads** | DropboxInstaller.exe | 2019-01-20 21:13:26Z | X | X | X |  |
| **C:\Users\srogers\Downloads** | BitTorrent.exe | 2019-01-20 21:26:03Z | X | X | X | X |
| **C:\Users\srogers\Downloads** | torbrowser-install-win64-8.0.4\_en-US.exe | 2019-01-21 05:10:14Z | X | X | X |  |
| **C:\Users\srogers\Documents\USB Backup** | privacy-eraser-setup.exe | 2019-01-21 16:57:41Z |  |  | X |  |
| **N/A** | Microsoft OneDrive v.18.240.1202.0004 | 2019-01-20 02:46:39Z |  |  |  | X |

Table 4 Applications

## PREFETCH

[Here you may also include the userassist and shimcache analysis results in a table or a figure. Explain any important findings in the narrative and these sections should have their own heading, similar to the PREFETCH heading.]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Executable**  **Name** | **Source**  **Created** | **Source**  **Modified** | **Size** | **Run**  **Count** | **LastRun** | **FirstRun** | **Volume0**  **Serial** |
| FTK IMAGER.EXE | 2019-01-21 19:50:48 | 2019-01-21 19:50:48 | 112198 | 1 | 2019-01-21 19:50:38 | N/A | CEFB0E37 |
| TOR.EXE | 2019-01-21 05:10:59 | 2019-01-21 05:10:59 | 45416 | 1 | 2019-01-21 05:10:49 | N/A | EA174897 |
| BITTORRENT.EXE | 2019-01-20 21:27:28 | 2019-01-20 21:27:28 | 108952 | 1 | 2019-01-20 21:27:18 | N/A | EA174897 |
| DROPBOX.EXE | 2019-01-20 21:18:01 | 2019-01-20 21:18:07 | 155234 | 4 | 2019-01-20 21:17:55 | 2019-01-20 21:17:55 | EA174897 |
| DROPBOXINSTALLER.EXE | 2019-01-20 21:13:36 | 2019-01-20 21:13:36 | 39974 | 1 | 2019-01-20 21:13:26 | N/A | EA174897 |

Table 5 Prefix Analysis for "AVENGERS01"

The Prefetch data that was found included executables ran by the srogers user.

## SHELLBAG ITEMS

[Here you want a table to shellbags, LNK files, and jump lists that are relevant to your case. If there are items unrelated to the policy violation or crime, remove them entirely or add the full list as an Appendix if there are more than 10. Identify for each files that were accessed, the first and last access or open dates, the filenames of interest and where these files are located.]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **File**  **Path** | **Shell**  **Type** | **Value** | **Created**  **On** | **Modified**  **On** |
| Desktop\E:\\Shield Documents | Directory | Shield Documents | 1/21/19 04:59 | 1/21/19 04:57 |
| Desktop\MyComputer\Documents\USB Backup\Shield Documents | Directory | Shield Documents | 1/21/19 05:06 | 1/21/19 05:06 |
| Desktop\Shared Documents Folder (Users Files)\Dropbox\Shield Documents | Directory | Shield Documents | 1/21/19 05:06 | 1/21/19 05:07 |
| Desktop\My Computer\Downloads\shielddocuments | Directory | shielddocuments | 1/21/19 16:57 | 1/21/19 16:57 |

Table 6 ShellBags

## LINKED FILES

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **File**  **Path** | **Source Created** | **Source Modified** | **Source Accessed** | **File Size** | **Drive Type** | **Volume Serial/Label** |
| **C:\Users\srogers\Documents\USB Backup\Shield Documents\Presentation with Sensitive IP.pptx** | 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\Desktop\Alloys.pptx** | 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 |
| **E:\Alloys.ppt** | 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 |
| **C:\Users\srogers\Documents\USB Backup\Personal\Random Accounting Spreadsheet.xlsx** | 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\Shield Documents** | 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 |
| **E:\Shield Documents\Confidential Alloy Expense Accounts.xlsx** | 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 |

Table 7 Linked Files

The Link File Analysis shows which files were connected between drives. The two types showed in the table above are Removable Storage Media (USB) and Fixed Storage Media (Hard Drive). The user srogers linked two documents titled “Confidential Alloy Expense Accounts.xlsx” and “Alloys.ppt” from the Hard Drive to the USB Drive named “Shield\_USB”.

## JUMP FILES

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Local Path** | **Target Created** | **Target Modified** | **File Size** | **Drive Type** | **Volume Serial/Label** | **Machine ID** |
| **C:\Users\srogers\Documents\USB Backup\Shield Documents\Presentation with Sensitive IP.pptx** | 2019-01-21 05:06:54 | 2019-01-21 03:48:38 | 31590 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Dropbox\Shield Documents\Presentation with Sensitive IP.pptx** | 2019-01-21 05:06:54 | 2019-01-21 03:48:38 | 31590 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Desktop\Alloys.pptx** | 2019-01-21 05:04:38 | 2019-01-21 05:04:42 | 697230 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **E:\Alloys.ppt** | 2019-01-21 04:59:57 | 2019-01-21 04:56:56 | 946688 | Removable storage media (Floppy, USB) | 6A018124/ Shield\_USB |  |
| **C:\Users\srogers\Documents\USB Backup\Shield Documents** | 2019-01-21 05:21:26 | 2019-01-21 05:21:26 | 4096 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **E:\Shield Documents\Confidential Alloy Expense Accounts.xlsx** | 2019-01-21 04:59:17 | 2019-01-21 04:11:14 | 10147 | Removable storage media (Floppy, USB) | 6A018124/ Shield\_USB |  |
| **C:\Users\srogers\Downloads\shielddocuments** | 2019-01-21 16:57:05 | 2019-01-21 16:57:05 | 4096 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Program Files\Cybertron\Privacy Eraser\PrivacyEraser64.exe** | 2019-01-21 16:58:30 | 2018-07-17 16:25:08 | 7081696 | Fixed storage media (Hard drive) | EA174897 | avengers01 |

Table 8 Jump Files

## MALWARE APPLICATIONS

[This section is used to identify any malicious applications identified on the system and may have some data similar to the prefetch section above. This is where you follow the basic malware triage steps and is not required for the case project, but can be extra credit. If you run anti-virus against a mounted drive, or your local antivirus engine identifies malware, make sure you identify the source file as well as the virus name identified by the antivirus vendor.]

[Also note any hashes, screenshots, or tables of the malicious program. This program could be adware, spyware, or malware in general. Identify any open source information about the malware and its capabilities. Review the section headers using tools similar to PEiD. Perform any static analysis to quickly triage the malware and recommend that the system be wiped. You may perform dynamic analysis or reverse engineer the malware if you think this is appropriate for the case to create IOCs. This is not done for general crimeware or spyware often.]

[INCLUDE OTHER SECTIONS AS NECESSARY OR DESIRED]

[Examples include deleted files,

items in the Recycle.Bin,

items that were downloaded to the system

and if they were executed or malicious, they may be listed above.

A list of specific documents or share access may also be highlighted.

Somewhere in the report, e-mail addresses should be identified that could be avenues of misuse.]

# CONCLUSION

[Here you will wrap up the case and draw conclusions. Did you verify there was a policy violation or law broken? Was there an infection or compromise caused by user action/interaction? Where is the largest risk of data loss or exfiltration?

Summarize the evidence you found. Where are the files of interest? What conclusions can you make about the evidence? Answer the initial questions asked of you by your manager, chief security officer, or legal counsel.

Finally, make recommendations. Note how the case be handled as a result of what was discovered during the exam? Should the user receive additional security training, a reprimand, or some form of administrative hearing? Should the suspect be charged civilly or criminally? Also, make sure you note any additional questions you believe the suspect should be asked by law enforcement or corporate investigators. Should we ask about the whereabouts for a specific device? Should we identify other systems or mobile devices, should we review corporate e-mail? This can be a bulleted list where you recommend actions be taken that may further your case and investigation.]

# TOOLS

# APPENDIX

## APPENDIX I: Forensic Tools

|  |  |  |
| --- | --- | --- |
| **Tool** | **Version** | **Command** |
| **Access Data Forensic Toolkit (FTK)** | v6.4 | GUI |
| **Access Data FTK Imager** | v3.4.2.6 | GUI |
| **Registry Ripper** | v3.0 | GUI |
| **Autopsy** | v4.6.0 | GUI |
| **USBDeviceForensics** | v1.5.2 | GUI |
| **AccessData Registry Viewer** | v2.0 | GUI |
| **ShellBags Explorer\*** | V1.0 | GUI |
| **DCode Date** | V4.02 | GUI |
| **Prefetch\*** | v1.5 | PECmd –d “Directory for Prefetch Files” --csv “Directory Output\pf.csv” |
| **Link File\*** | v1.5 | LECmd –d “Directory for Link Files” --csv “Directory Output\lnk.csv” |
| **Jump List\*** | v1.5 | JLECmd –d “Directory for Jump Files” --csv “Directory Output\jmp.csv” |
| **Shellbags Cmd** | v2.0 | SBECmd –d “Directory for ShellBag Items” --csv “Directory Output\sb.csv” |

\*Eric Zimmerman’s Tools (Source: https://ericzimmerman.github.io/#!index.md)

## APPENDIX I: Registry Paths

|  |  |  |  |
| --- | --- | --- | --- |
| Hive | Directory | Name | Description |
| NTUSER.DAT | SYSTEM\CurrentControlSet\Control\Windows |  |  |
| NTUSER.DAT | Software\Microsoft\Windows\CurrentVersion\Explorer | TypedPaths |  |
| NTUSER.DAT | Software\Microsoft\Windows\CurrentVersion\Explorer | WordWheelQuery | Windows Search History |
| NTUSER.DAT | Software\Microsoft\Windows\CurrentVersion\Explorer | RecentDocs |  |
| **NTUSER.DAT** | | Software\Microsoft\Windows\CurrentVersion\Explorer | UserAssist |  |
| **NTUSER.DAT** | | Software\Microsoft\Windows\CurrentVersion | Run |  |
| **NTUSER.DAT** | | Software\Microsoft\Windows\CurrentVersion | RunOnce |  |
| **NTUSER.DAT** | | Software\Microsoft\Windows\Shell | Bags (Desktop) |  |
| **NTUSER.DAT** | | Software\Microsoft\Windows\Shell | BagMRU (Desktop) |  |
| **USRCLASS.DAT** | | Local Settings\Software\Microsoft\Windows\Shell | Bags (Explorer) |  |
| **USRCLASS.DAT** | | Local Settings\Software\Microsoft\Windows\Shell | BagMRU (Explorer) |  |

## APPENDIX II: Artifacts List

1. NTFS Files
   * NONAME [NTFS]/[root]/$MFT
   * NONAME [NTFS]/[root]/$LogFile
2. Registry Hives
   * NONAME [NTFS]/[root]/Windows/System32/config/SYSTEM
   * NONAME [NTFS]/[root]/Windows/System32/config/SECURITY
   * NONAME [NTFS]/[root]/Windows/System32/config/SAM
   * NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
   * NONAME [NTFS]/[root]//Users/srogers/NTUSER.DAT
   * NONAME [NTFS]/[root]//Users/srogers/AppData/Local/Microsoft /Windows/UsrClass.dat
3. Logs
   * NONAME [NTFS]/[root]/Windows/System32/winevt/Logs
4. Additional Shellbag Folders
   * NONAME [NTFS]/[root]/Windows/Prefetch
   * NONAME [NTFS]/[root]/Users/srogers/AppData
   * NONAME [NTFS]/[root]/Users/srogers/AppData/Roaming/Microsoft/Windows/Recent
5. User’s Profile Folders
   * NONAME [NTFS]/[root]/Users/srogers/Desktop
   * NONAME [NTFS]/[root]/Users/srogers/Documents
   * NONAME [NTFS]/[root]/Users/srogers/Downloads
   * NONAME [NTFS]/[root]/Users/srogers/Dropbox
6. Additional Artifacts
   * NONAME [NTFS]/[root]/$Recycle.Bin (folder)
   * NONAME [NTFS]/[root]/Windows/INF/setupapi.dev.log

## APPENDIX III: Prefetch Analysis

Sort by LastRun Descending

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Executable Name** | **Source Created** | **Source Modified** | **File Size** | **Run Count** | **LastRun** | **FirstRun** | **Volume**  **Serial** |
| SEARCHFILTERHOST.EXE | 2019-01-19 03:15:18 | 2019-01-21 19:51:29 | 16574 | 59 | 2019-01-21 19:51:19 | 2019-01-21 18:57:21 | EA174897 |
| FTK IMAGER.EXE | 2019-01-21 19:50:48 | 2019-01-21 19:50:48 | 112198 | 1 | 2019-01-21 19:50:38 |  | CEFB0E37 |
| CONHOST.EXE | 2019-01-19 03:22:06 | 2019-01-21 19:49:57 | 28406 | 42 | 2019-01-21 19:49:47 | 2019-01-21 17:56:08 | CEFB0E37 |
| EDD.EXE | 2019-01-21 19:49:57 | 2019-01-21 19:49:57 | 29050 | 1 | 2019-01-21 19:49:47 |  | CEFB0E37 |
| CONSENT.EXE | 2019-01-19 03:21:45 | 2019-01-21 19:49:47 | 130694 | 10 | 2019-01-21 19:49:46 | 2019-01-20 02:44:09 | CEFB0E37 |
| TOR.EXE | 2019-01-21 05:10:59 | 2019-01-21 05:10:59 | 45416 | 1 | 2019-01-21 05:10:49 |  | EA174897 |
| BITTORRENT.EXE | 2019-01-20 21:27:28 | 2019-01-20 21:27:28 | 108952 | 1 | 2019-01-20 21:27:18 |  | EA174897 |
| BITTORRENT.EXE | 2019-01-20 21:26:13 | 2019-01-20 21:26:13 | 48388 | 1 | 2019-01-20 21:26:03 |  | EA174897 |
| DROPBOX.EXE | 2019-01-20 21:18:01 | 2019-01-20 21:18:07 | 155234 | 4 | 2019-01-20 21:17:55 | 2019-01-20 21:17:55 | EA174897 |
| DROPBOX.EXE | 2019-01-20 21:17:24 | 2019-01-20 21:17:24 | 151882 | 1 | 2019-01-20 21:17:18 |  | EA174897 |
| DROPBOXINSTALLER.EXE | 2019-01-20 21:13:36 | 2019-01-20 21:13:36 | 39974 | 1 | 2019-01-20 21:13:26 |  | EA174897 |

## APPENDIX IV: Link Analysis

**Sort by Source Modified Descending**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Local FilePath** | **Source Created** | **Source Modified** | **Source Accessed** | **File Size** | **Drive Type** | **Volume Serial/Label** |
| **C:\Users\srogers\Documents\USB Backup\Personal\Random Accounting Spreadsheet.xlsx** | 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\Selection\_of\_materials.ppt** | 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\Cap-2.jpg** | 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-1.jpg** | 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\USB Backup\Shield Documents\Presentation with Sensitive IP.pptx** | 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** | 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\USB Backup** | 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 |
| [**This PC.lnk**](smb://Mac/Home/Documents/_Education/Northeastern/PhD_Cybersecurity/CY5210_Information_System_Forensics/Module_4/Lab_3/CaseFolder/Recent/Recent/This) | 2019-01-21 05:06:50 | 2019-01-21 05:06:50 | 2022-10-07 05:06:43 | 0 | (None) |  |
| **C:\Users\srogers\Documents\USB Backup\Personal** | 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 |
| **E:\Personal\S. Rogers Resume.docx** | 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 |
| **C:\Users\srogers\Documents\USB Backup\Shield Documents** | 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 |
| **E:\Shield Documents\Confidential Alloy Expense Accounts.xlsx** | 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 |
| **C:\Users\srogers\Documents\USB Backup\Chapter 4.pdf** | 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\Desktop\Alloys.pptx** | 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 |
| **E:\Alloys.ppt** | 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:\** [**Shield\_USB (E).lnk**](smb://Mac/Home/Documents/_Education/Northeastern/PhD_Cybersecurity/CY5210_Information_System_Forensics/Module_4/Lab_3/CaseFolder/Recent/Recent/Shield_USB) | 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 |
| [**ms-settingsnetwork.lnk**](smb://Mac/Home/Documents/_Education/Northeastern/PhD_Cybersecurity/CY5210_Information_System_Forensics/Module_4/Lab_3/CaseFolder/Recent/Recent/ms-settingsnetwork.lnk) | 2019-01-20 21:09:55 | 2019-01-20 21:09:55 | 2022-10-07 05:06:43 | 0 | (None) |  |
| [**The Internet.lnk**](smb://Mac/Home/Documents/_Education/Northeastern/PhD_Cybersecurity/CY5210_Information_System_Forensics/Module_4/Lab_3/CaseFolder/Recent/Recent/The) | 2019-01-19 03:13:02 | 2019-01-20 21:09:55 | 2022-10-07 05:06:43 | 0 | (None) |  |

## APPENDIX V: Jump List Analysis

Sort by Target Created Descending

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Local Path** | **Target Created** | **Target Modified** | **File Size** | **Drive Type** | **Volume Serial/Label** | **Machine ID** |
| **C:\Program Files\Cybertron\Privacy Eraser\PrivacyEraser64.exe** | 2019-01-21 16:58:30 | 2018-07-17 16:25:08 | 7081696 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Program Files\Cybertron\Privacy Eraser\PrivacyEraser64.exe** | 2019-01-21 16:58:30 | 2018-07-17 16:25:08 | 7081696 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Program Files\Cybertron\Privacy Eraser\PrivacyEraser64.exe** | 2019-01-21 16:58:30 | 2018-07-17 16:25:08 | 7081696 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Downloads\shielddocuments** | 2019-01-21 16:57:05 | 2019-01-21 16:57:05 | 4096 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Documents\Cap-2.jpg** | 2019-01-21 05:23:12 | 2019-01-21 05:23:13 | 0 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Documents\Cap-1.jpg** | 2019-01-21 05:22:40 | 2019-01-21 05:22:40 | 0 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Documents\USB Backup\Shield Documents** | 2019-01-21 05:21:26 | 2019-01-21 05:21:26 | 4096 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Dropbox** | 2019-01-21 05:09:39 | 2019-01-21 05:21:16 | 4096 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Documents\USB Backup\Chapter 4.pdf** | 2019-01-21 05:06:54 | 2019-01-21 04:55:58 | 1008692 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Documents\USB Backup\Selection\_of\_materials.ppt** | 2019-01-21 05:06:54 | 2019-01-21 04:58:06 | 4237312 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Documents\USB Backup\Shield Documents\Presentation with Sensitive IP.pptx** | 2019-01-21 05:06:54 | 2019-01-21 03:48:38 | 31590 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Documents\USB Backup\Personal** | 2019-01-21 05:06:54 | 2019-01-21 19:16:11 | 4096 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Dropbox\Shield Documents** | 2019-01-21 05:06:54 | 2019-01-21 05:07:41 | 4096 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Documents\USB Backup\Personal\Random Accounting Spreadsheet.xlsx** | 2019-01-21 05:06:54 | 2019-01-21 03:50:58 | 10144 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Documents\USB Backup\Selection\_of\_materials.ppt** | 2019-01-21 05:06:54 | 2019-01-21 04:58:06 | 4237312 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Documents\USB Backup\Chapter 4.pdf** | 2019-01-21 05:06:54 | 2019-01-21 04:55:58 | 1008692 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Dropbox\Shield Documents\Presentation with Sensitive IP.pptx** | 2019-01-21 05:06:54 | 2019-01-21 03:48:38 | 31590 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Documents\USB Backup** | 2019-01-21 05:06:45 | 2019-01-21 19:15:49 | 4096 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Desktop\Alloys.pptx** | 2019-01-21 05:04:38 | 2019-01-21 05:04:42 | 697230 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Desktop\Alloys.pptx** | 2019-01-21 05:04:38 | 2019-01-21 05:04:42 | 697230 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **E:\Chapter 4.pdf** | 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** | 2019-01-21 04:59:58 | 2019-01-21 04:55:58 | 1008692 | Removable storage media (Floppy, USB) | 6A018124/ Shield\_USB |  |
| **E:\Alloys.ppt** | 2019-01-21 04:59:57 | 2019-01-21 04:56:56 | 946688 | Removable storage media (Floppy, USB) | 6A018124/ Shield\_USB |  |
| **E:\Alloys.ppt** | 2019-01-21 04:59:57 | 2019-01-21 04:56:56 | 946688 | Removable storage media (Floppy, USB) | 6A018124/ Shield\_USB |  |
| **E:\Shield Documents\Confidential Alloy Expense Accounts.xlsx** | 2019-01-21 04:59:17 | 2019-01-21 04:11:14 | 10147 | Removable storage media (Floppy, USB) | 6A018124/ Shield\_USB |  |
| **E:\Personal\S. Rogers Resume.docx** | 2019-01-21 04:59:17 | 2019-01-21 03:58:34 | 17597 | Removable storage media (Floppy, USB) | 6A018124/ Shield\_USB |  |
| **E:\Personal** | 2019-01-21 04:59:17 | 2019-01-21 04:54:20 | 0 | Removable storage media (Floppy, USB) | 6A018124/ Shield\_USB |  |
| **E:\Shield Documents** | 2019-01-21 04:59:17 | 2019-01-21 04:57:06 | 0 | Removable storage media (Floppy, USB) | 6A018124/ Shield\_USB |  |
| **E:\Personal\S. Rogers Resume.docx** | 2019-01-21 04:59:17 | 2019-01-21 03:58:34 | 17597 | Removable storage media (Floppy, USB) | 6A018124/ Shield\_USB |  |
| **E:\Shield Documents\Confidential Alloy Expense Accounts.xlsx** | 2019-01-21 04:59:17 | 2019-01-21 04:11:14 | 10147 | Removable storage media (Floppy, USB) | 6A018124/ Shield\_USB |  |
| **C:\Program Files (x86)\Google\Chrome\Application\chrome.exe** | 2019-01-20 02:44:31 | 2018-12-12 05:11:41 | 1587680 | Fixed storage media (Hard drive) | EA174897 | desktop-16pttv2 |
| **C:\Program Files (x86)\Google\Chrome\Application\chrome.exe** | 2019-01-20 02:44:31 | 2018-12-12 05:11:41 | 1587680 | Fixed storage media (Hard drive) | EA174897 | desktop-16pttv2 |
| **C:\Program Files (x86)\Google\Chrome\Application\chrome.exe** | 2019-01-20 02:44:31 | 2018-12-12 05:11:41 | 1587680 | Fixed storage media (Hard drive) | EA174897 | desktop-16pttv2 |
| **C:\Program Files (x86)\Google\Chrome\Application\chrome.exe** | 2019-01-20 02:44:31 | 2018-12-12 05:11:41 | 1587680 | Fixed storage media (Hard drive) | EA174897 | desktop-16pttv2 |
| **C:\Users\srogers\Documents** | 2019-01-19 03:11:57 | 2019-01-21 05:23:12 | 4096 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Desktop** | 2019-01-19 03:11:57 | 2019-01-21 05:04:43 | 4096 | Fixed storage media (Hard drive) | EA174897 | avengers01 |
| **C:\Users\srogers\Downloads** | 2019-01-19 03:11:57 | 2019-01-19 03:12:57 | 0 | Fixed storage media (Hard drive) | EA174897 | desktop-16pttv2 |
| **C:\Users\srogers\Videos** | 2019-01-19 03:11:57 | 2019-01-19 03:12:57 | 0 | Fixed storage media (Hard drive) | EA174897 | desktop-16pttv2 |
| **C:\Users\srogers\Music** | 2019-01-19 03:11:57 | 2019-01-19 03:12:57 | 0 | Fixed storage media (Hard drive) | EA174897 | desktop-16pttv2 |
| **C:\Users\srogers\Pictures** | 2019-01-19 03:11:57 | 2019-01-19 03:12:57 | 0 | Fixed storage media (Hard drive) | EA174897 | desktop-16pttv2 |

## APPENDIX VI: Shellbag Analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Absolute**  **Path** | **Shell**  **Type** | **Value** | **Created**  **On** | **Modified**  **On** |
| **Desktop\My Computer** | Root folder: GUID | My Computer |  |  |
| **Desktop\Home Folder** | Root folder: GUID | Home Folder |  |  |
| **Desktop\C:\** | Users property view: Drive letter | C:\ |  |  |
| **Desktop\D:\** | Users property view: Drive letter | D:\ |  |  |
| **Desktop\E:\** | Users property view: Drive letter | E:\ |  |  |
| **Desktop\Shared Documents Folder (Users Files)** | Root folder: GUID | Shared Documents Folder (Users Files) |  |  |
| **Desktop\Search Folder** | Users property view | Search Folder |  |  |
| **Desktop\Search Folder** | Users property view | Search Folder |  |  |
| **Desktop\My Computer\Downloads** | Root folder: GUID | Downloads |  |  |
| **Desktop\My Computer\Documents** | Root folder: GUID | Documents |  |  |
| **Desktop\My Computer\Desktop** | Root folder: GUID | Desktop |  |  |
| **Desktop\My Computer\Pictures** | Root folder: GUID | Pictures |  |  |
| **Desktop\My Computer\Downloads\shielddocuments** | Directory | shielddocuments | 1/21/19 16:57 | 1/21/19 16:57 |
| **Desktop\My Computer\Documents\USB Backup** | Directory | USB Backup | 1/21/19 05:06 | 1/21/19 05:06 |
| **Desktop\My Computer\Documents\USB Backup\Shield Documents** | Directory | Shield Documents | 1/21/19 05:06 | 1/21/19 05:06 |
| **Desktop\My Computer\Documents\USB Backup\Personal** | Directory | Personal | 1/21/19 05:06 | 1/21/19 05:06 |
| **Desktop\C:\\Users** | Directory | Users | 9/29/17 08:45 | 1/20/19 02:44 |
| **Desktop\C:\\Users\srogers** | Directory | srogers | 1/19/19 03:11 | 1/21/19 05:09 |
| **Desktop\C:\\Users\srogers\AppData** | Directory | AppData | 1/19/19 03:11 | 1/19/19 03:12 |
| **Desktop\C:\\Users\srogers\AppData\Local** | Directory | Local | 1/19/19 03:11 | 1/21/19 16:58 |
| **Desktop\C:\\Users\srogers\AppData\Roaming** | Directory | Roaming | 1/19/19 03:11 | 1/21/19 18:22 |
| **Desktop\C:\\Users\srogers\AppData\Local\Microsoft** | Directory | Microsoft | 1/19/19 03:11 | 1/20/19 21:17 |
| **Desktop\C:\\Users\srogers\AppData\Local\Microsoft\Windows** | Directory | Windows | 1/19/19 03:11 | 1/21/19 05:09 |
| **Desktop\C:\\Users\srogers\AppData\Roaming\Microsoft** | Directory | Microsoft | 1/19/19 03:11 | 1/20/19 21:27 |
| **Desktop\C:\\Users\srogers\AppData\Roaming\Microsoft\Windows** | Directory | Windows | 1/19/19 03:11 | 1/19/19 03:13 |
| **Desktop\C:\\Users\srogers\AppData\Roaming\Microsoft\Windows\Recent** | Directory | Recent | 1/19/19 03:11 | 1/21/19 05:23 |
| **Desktop\E:\\Personal** | Directory | Personal | 1/21/19 04:59 | 1/21/19 04:54 |
| **Desktop\E:\\Shield Documents** | Directory | Shield Documents | 1/21/19 04:59 | 1/21/19 04:57 |
| **Desktop\E:\\Forensic Tools** | Directory | Forensic Tools | 1/21/19 18:34 | 1/21/19 18:34 |
| **Desktop\E:\\SANS To Sort** | Directory | SANS To Sort | 1/21/19 18:33 | 1/21/19 18:33 |
| **Desktop\E:\\Imaging and Triage Lab** | Directory | Imaging and Triage Lab | 1/21/19 19:54 | 1/21/19 19:54 |
| **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 |
| **Desktop\Shared Documents Folder (Users Files)\Dropbox** | Users Files Folder | Dropbox | 1/21/19 05:09 | 1/21/19 05:09 |
| **Desktop\Shared Documents Folder (Users Files)\Dropbox\Shield Documents** | Directory | Shield Documents | 1/21/19 05:06 | 1/21/19 05:07 |