

Case Project 01

CY5210 Information System Forensics

Instructor: Elton Booker

Jonathan Metzger

October 16th, 2022

Table of Contents

TABLE OF CONTENTS.....	2
EXECUTIVE SUMMARY	3
INTRODUCTION.....	4
ANALYSIS	5
WINDOWS REGISTRY.....	5
SYSTEM INFORMATION	5
USER ACTIVITY	6
USB DEVICE ACTIVITY	7
APPLICATIONS AND MALWARE	8
PREFETCH	8
SHELL ITEMS.....	9
CONCLUSION	11
APPENDIX	12
APPENDIX I: FORENSIC TOOLS	12
APPENDIX II: REGISTRY PATHS.....	12
APPENDIX III: ARTIFACTS LIST.....	13
APPENDIX IV: PREFETCH ANALYSIS	14
APPENDIX V: SHELLBAG ANALYSIS	14
APPENDIX VI: LINK ANALYSIS	16
APPENDIX VII: JUMP LIST ANALYSIS	16

EXECUTIVE SUMMARY

On January 21st, 2019, the company “The Shield SOC” was notified of the unusual activity of downloading multiple Potentially Unwanted Programs (PUPs) onto one of their systems. The Incident Response Team collected and provided the system in question to the Forensics Teams to perform an investigation. After budgeting constraints and the COVID, pandemic delayed the investigation, the Case Study for this report was finalized on October 16th, 2022.

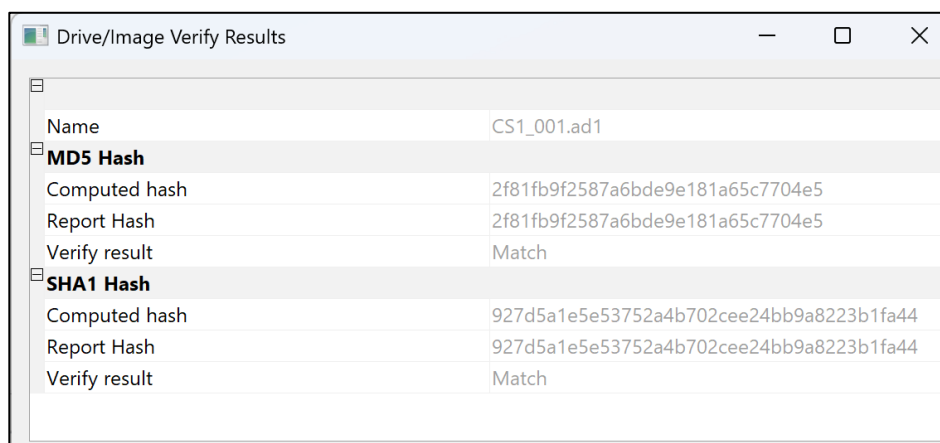
The Forensics Team appointed Jon Metzger as the Forensic Analyst and Investigator for the case. His investigation found that a company employee named Steven Rogers copied confidential documents from their company-owned system onto a USB external media and a cloud storage Dropbox. S. Rogers knew where sensitive information was located on the file system. The user was able to use their administrative privileges to download malicious applications onto the system illegally. These applications enabled him to move confidential documents from the company’s hard drive system to his external media. From there, he attempted to cover his tracks from security and log out before the workday started. The analysis section will detail the user’s actions to violate the organization's enforced Acceptable Use Policy (AUP).

INTRODUCTION

There was an alert that was received by Shield SOC that an illegal download for BitTorrent and Privacy Cleaner utilities. These applications are of concern because they can be used with confidential data to expose sensitive data outside the company. Both applications violated the company's Acceptable Use Policy (AUP) and can be Potentially Unwanted Programs (PUPs). The incident response team member Bucky Barnes identified the violation 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 delivered with this report. Figure 1 below verified the hash of the system. It is calculated in both MD5 and SHA1 hash values. The verification checked that the hash computed and reported a match. This is essential because the tool checks to see if the image's content was modified, with its integrity intact, between computing and reporting on the case.

Once the Forensics Team started their analysis, they had 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. These tools and their commands are found in APPENDIX I. The team was also provided a Windows 11 machine to run these tools with administrator privileges.



Drive/Image Verify Results	
Name	CS1_001.ad1
MD5 Hash	
Computed hash	2f81fb9f2587a6bde9e181a65c7704e5
Report Hash	2f81fb9f2587a6bde9e181a65c7704e5
Verify result	Match
SHA1 Hash	
Computed hash	927d5a1e5e53752a4b702cee24bb9a8223b1fa44
Report Hash	927d5a1e5e53752a4b702cee24bb9a8223b1fa44
Verify result	Match

Figure 1 Verification of the system investigated named "CS1_001"

ANALYSIS

The analysis will cover Windows Registry, System Information, User activity, USB Device activity, Application and Malware use, Prefetch, Shellbags, Linkfiles, and JumpLists. By the forensics team obtaining this information from the incident response team, we will be able to justify if the user S. Rogers violated company policy.

WINDOWS REGISTRY

The Windows Registry identifies current system configurations and settings used during the investigation. They can show the current state of the system and actions performed by all users on the system. The following Hives were analyzed for the analysis using the tool Access Data FTK Imager, which can be found in APPENDIX III:

- **NONAME [NTFS]/[root]/Windows/System32/config/SAM**
- **NONAME [NTFS]/[root]/Windows/System32/config/SYSTEM**
- **NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE**
- **NONAME [NTFS]/[root]/Users/srogers/NTUSER.DAT**

The SAM Registry Hive focused on profiling users and groups. The SYSTEM Registry Hive identified system information and configuration settings. The SOFTWARE Registry Hive revealed applications downloaded, installed, executed, and uninstalled onto the system. The NTUSER.DAT Registry Hive focused on specific user activity.

SYSTEM INFORMATION

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	10.0.0.81, hsd1.ma.comcast.net, configured for DHCP
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

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. The hostname "AVENGERS01" was analyzed by the Forensics team to inspect the malicious activity that was reported. On the Windows 10 Pro system, we found that the operating installation time was 2019-01-19 at 03:06:56Z and set in Eastern Standard time. We used Registry Ripper to analyze the hives of SAM, SYSTEM, SOFTWARE, and User (NTUSER.DAT and USRCLASS.DAT). The system's network configurations are set to IP Address 10.0.0.81 and configured for DHCP. The system's last shutdown occurred before the incident, meaning the system has been running since the incident occurred.

Interestingly, the application "Dropbox" is one of the system's AutoStart Programs. This application is on the company-restricted list and should not have been installed onto the system. This finding will need to be further investigated when analyzing the user activity around the time of the incident.

USER ACTIVITY

Users for this system 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" meaning that it is a domain ID, and 263698462-3103634936-1936700066 as the "unique identifier." Next are each username "RID" of the system specified below in Table 2. Together make the "Security IDentified" or SID. Using the template:

"<id_type>-<revision_level>-<authority_value>-<specification_id>-<unique_identifier>-<RID>"

The srogers' SID is **S-1-5-21-263698462-3103634936-1936700066-1001**.

As shown in the table below, 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. This indicates that the srogers user had administrator privileges and caused harm to the system and company. All but the Administrator account has their password not required and not expired. This analysis states that the srogers account was not adequately secured and given full privileges. It was also the only account on the system that was enabled with the last login time of 2019-01-21 at 18:56:51Z.

User account srogers is a focus of this analysis since that account is given administrative privileges, ten logins, a password reset time of 2019-01-19 at 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	Password Reset	Group	Password
srogers	1001	Enabled, 10 logins	2019-01-21 18:56:51Z	2019-01-19 03:11:57Z	Administrator	Not Required/Not Expired
Administrator	500	Disabled	Never	Never	Administrator	Not Expire
Guest	501	Disabled	Never	Never	Guest	Not Required/Not Expired
DefaultAccount	503	Disabled	Never	Never	System Managed Accounts Group	Not Required/Not Expired
WDAGUtilityAccount	504	Disabled	Never	2019-01-19 06:04:22Z	n/a	n/a

Table 2 User Information

The forensics team went through the user activity of the user srogers. They reviewed the user's Windows Search History, Typed Paths, RecentDocs, Last Executed Commands, and UserAssist findings. These registry locations can be found in APPENDIX II.

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 paths on the systems related to the investigation. However, RecentDocs revealed that the user accessed various sensitive files at the time of the alert. These documents are addressed in the LinkedFiles and JumpList portion of the analysis.

USB DEVICE ACTIVITY

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 60 GB-sized USB labeled "Kingston Data Traveler 2.0" was connected to the system at the time of the alert. The user srogers were accessing the USB through the E: drive. The table above reveals that the first and last time of the device's first and last time was between 5:00 AM and 6:45 PM, more than 13 hours. Later, it was revealed that the USB connected and used by user "srogers" was labeled "Shield_USB," with multiple confidential and sensitive documents copied onto this volume. This information is covered in the Chain of Custody form attached to the report.

APPLICATIONS AND MALWARE

Path	Filename	LastUsed	Download	Installed	Executed	Uninstalled
N/A	Microsoft OneDrive v.18.240.1202.0004	2019-01-20 02:46:39Z				X
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	

Table 4 Applications by LastUsed

The applications, including possible malware highlighted in **RED**, used by the user "srogers" are shown in the table above, sorted by LastUsed. The user executed the command line prompt and privacy eraser. The user downloaded and installed multiple applications, including DropboxInstaller (highlighted in **BLUE**), BitTorrent, and Torbrowser Installer. Lastly, the user uninstalled the BitTorrent application to attempt to hide their tracks. In addition, the user moved DropboxInstaller and ChromeSetup to the RecycleBin.

These items were recovered and analyzed. Microsoft OneDrive was not used during these events but was uninstalled. This action raises questions on the purpose of uninstalling the application after the chain of events of downloading, installing, and executing these applications.

PREFETCH

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 were found included executables run by the srogers user. More of the findings can be found in APPENDIX IV. This information overlaps with the previous section but goes into more detail about each application. The malicious applications are again highlighted in RED, and applications of interest that export information to the cloud is highlighted in BLUE. It includes the source created and modified.

It is verified that these applications were not modified since their installation and that their integrity was intact. These applications were only used once, with Dropbox running four times, but their timestamps match. With the inclusion of FTK Imager and the exclusion of Privacy Erased, it seemed that the tool was used at the time of the event.

SHELL ITEMS

The following documents from the below table show that the “Shield Documents” directory was taken from the hard drive and copied onto the E: drive where the external “Shield_USB” was located. More information on the ShellBags collected can be found in APPENDIX V. Also, it seemed that the user later copied the shielddocuments onto the desktop. These file names indicate that the user was handling sensitive information about the organization, especially outside regular work hours.

The Link File Analysis shows which files were connected between drives. The two types shown in the table above are Removable Storage Media (USB) and Fixed Storage Media (Hard Drive). More information on the linked files obtained in this investigation can be found in APPENDIX VI. The user srogers linked two documents titled “Confidential Alloy Expense Accounts.xlsx” and “Alloys.pptx” from the Hard Drive to the USB Drive named “Shield_USB.” It was interesting to see that the Alloys.pptx file had a file size great than that on the hard drive.

We tracked the system’s JumpList, which followed that sensitive documents were copied from the hard drive named “AVENGERS01” to the removable storage media “Shield_USB” These documents contain “Confidential Alloy Expense Accounts” and “Allows.” Additionally, a copy labeled “Presentation with Sensitive IP.pptx” More information on jump lists can be found in APPENDIX VII.

With these findings, the Forensics Team could track which files were copied from the hard drive onto the external media and the Dropbox directory to export into the cloud. The following table explains the evidence required to be presented to the legal team against S. Rogers.

File Path	Src/Dst Created	Src/Dst Modified	Source Accessed	File Size	Shell/Drive Type	Volume Serial/Label	MachineID
Desktop\E:\Shield Documents	1/21/19 04:59	1/21/19 04:57	n/a	n/a	Directory	n/a	n/a
Desktop\MyComputer\Documents\USB Backup\Shield Documents	1/21/19 05:06:00	1/21/19 05:06:00	n/a	n/a	Directory	n/a	n/a
Desktop\Shared Documents Folder (Users Files)\Dropbox\Shield Documents	1/21/19 05:06:00	1/21/19 05:07:00	n/a	n/a	Directory	n/a	n/a
Desktop\My Computer\Downloads\shielddocuments	1/21/19 16:57:00	1/21/19 16:57:00	n/a	n/a	Directory	n/a	n/a
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	n/a
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	n/a
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	n/a
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	n/a
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	n/a
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	n/a
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	n/a	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	n/a	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	n/a	697230	Fixed storage media (Hard drive)	EA174897	avengers01
E:\Alloys.ppt	2019-01-21 04:59:57	2019-01-21 04:56:56	n/a	946688	Removable storage media (Floppy, USB)	6A018124/ Shield_USB	n/a
C:\Users\srogers\Documents\USB Backup\Shield Documents	2019-01-21 05:21:26	2019-01-21 05:21:26	n/a	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	n/a	10147	Removable storage media (Floppy, USB)	6A018124/ Shield_USB	n/a

Table 6 Shellbags, Linked Files, JumpList

CONCLUSION

To conclude, after observing the evidence on the hard drive labeled “avengers01” on Monday, January 21st, 2019, at 3:17:18 PM EST, an alert of applications that violate the company’s Acceptable Use Policy (AUP) and possibly be Potentially Unwanted Programs (PUPs) were installed onto the system.

After thoroughly investigating the system, the Forensics Team found instances where the user labeled “srogers” connected an external media device labeled “Shield_USB” on the approach to extract sensitive documents. S. Rogers installed Dropbox, BitTorrent, and TORBROWSER to bypass any company safeguards to extract data. They copied papers under the “Shield Documents” directory from the hard drive to the external media, violating company policy. Installing those applications also violated company policy since those programs were installed outside of the company-approved method. Utilizing these documents was during off hours around 5 AM that morning.

The user tried to cover their tracks by uninstalling the Dropbox application and moving the installer to the Recycling Bin. These actions were recovered by forensics and tied back to the original user. This user had Administrator privileges and could have harmed the system and organization. Luckily, no harm was done, and the user tried to use stealth techniques to infiltrate the organization’s strategy, extract sensitive documents, and hide their tracks.

Recommendations following the investigation are as follows. Legal actions should be taken by the organization that owns the sensitive documents against the individual. The organization’s IT department will need to restrict USB access to their system for this does not occur again. They additionally will need to lock down elevated privileges, require administrative rights to download applications not already authorized by the ISSO, and secure these sensitive and confidential documents in a secure location and not on the user's Documents and Desktop directories. Overall, it is a good idea to notify the organization of this breach, to provide reminders on the consequences, and require additional security/human error training. This event may have occurred in a public setting with other employees on the premises. They should be reminded to report any unusual behavior to security.

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 II: Registry Paths

Hive	Directory	Name	Description
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer	TypedPaths	Paths Typed by User
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer	WordWheelQuery	Windows Search History
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer	RecentDocs	Recent Documents
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer	UserAssist	User Program execution
NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Explorer\	<Policies>\RunMRU	User Command execution
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion	Run	Applications Ran
NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion	RunOnce	Applications Ran Once
NTUSER.DAT	Software\Microsoft\Windows\Shell	Bags (Desktop)	ShellBags
NTUSER.DAT	Software\Microsoft\Windows\Shell	BagMRU (Desktop)	ShellBags List
NTUSER.DAT	System\CurrentControlSet\Services\Tcpip\Parameters	Interfaces	Network Interfaces
USRCLASS.DAT	Local Settings\Software\Microsoft\Windows\Shell	Bags (Explorer)	ShellBags
USRCLASS.DAT	Local Settings\Software\Microsoft\Windows\Shell	BagMRU (Explorer)	ShellBags List

APPENDIX III: Artifacts List

- I. NTFS Files
 - NONAME [NTFS]/[root]/\$MFT
 - NONAME [NTFS]/[root]/\$LogFile
- II. 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
- III. Logs
 - NONAME [NTFS]/[root]/Windows/System32/winevt/Logs
- IV. Additional Shellbag Folders
 - NONAME [NTFS]/[root]/Windows/Prefetch
 - NONAME [NTFS]/[root]/Users/srogers/AppData
 - NONAME [NTFS]/[root]/Users/srogers/AppData/Roaming/Microsoft/Windows/Recent
- V. 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
- VI. Additional Artifacts
 - NONAME [NTFS]/[root]/\$Recycle.Bin (folder)
 - NONAME [NTFS]/[root]/Windows/INF/setupapi.dev.log

APPENDIX IV: Prefetch Analysis

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 V: Shellbag Analysis

Absolute Path	Shell Type	Value	Created On	Modified On
Desktop\My Computer	Root folder: GUID	My Computer	n/a	n/a
Desktop\Home Folder	Root folder: GUID	Home Folder	n/a	n/a
Desktop\C:\	Users property view: Drive letter	C:\	n/a	n/a
Desktop\D:\	Users property view: Drive letter	D:\	n/a	n/a
Desktop\E:\	Users property view: Drive letter	E:\	n/a	n/a
Desktop\Shared Documents Folder (Users Files)	Root folder: GUID	Shared Documents Folder (Users Files)	n/a	n/a
Desktop\Search Folder	Users property view	Search Folder	n/a	n/a
Desktop\Search Folder	Users property view	Search Folder	n/a	n/a
Desktop\My Computer\Downloads	Root folder: GUID	Downloads	n/a	n/a
Desktop\My Computer\Documents	Root folder: GUID	Documents	n/a	n/a
Desktop\My Computer\Desktop	Root folder: GUID	Desktop	n/a	n/a
Desktop\My Computer\Pictures	Root folder: GUID	Pictures	n/a	n/a
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

APPENDIX VI: Link Analysis

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.Ink	2019-01-21 05:06:50	2019-01-21 05:06:50	2022-10-07 05:06:43	0	(None)	n/a
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).Ink	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.Ink	2019-01-20 21:09:55	2019-01-20 21:09:55	2022-10-07 05:06:43	0	(None)	n/a
The Internet.Ink	2019-01-19 03:13:02	2019-01-20 21:09:55	2022-10-07 05:06:43	0	(None)	n/a

APPENDIX VII: Jump List Analysis

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	n/a
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	n/a
E:\Alloys.ppt	2019-01-21 04:59:57	2019-01-21 04:56:56	946688	Removable storage media (Floppy, USB)	6A018124/ Shield_USB	n/a
E:\Alloys.ppt	2019-01-21 04:59:57	2019-01-21 04:56:56	946688	Removable storage media (Floppy, USB)	6A018124/ Shield_USB	n/a
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	n/a
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	n/a
E:\Personal	2019-01-21 04:59:17	2019-01-21 04:54:20	0	Removable storage media (Floppy, USB)	6A018124/ Shield_USB	n/a
E:\Shield Documents	2019-01-21 04:59:17	2019-01-21 04:57:06	0	Removable storage media (Floppy, USB)	6A018124/ Shield_USB	n/a
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	n/a
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	n/a
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