**Text

Description automatically generated**

Case Project 01

CY5210 Information System Forensics

Instructor: Elton Booker

Jonathan Metzger

# Table of Contents

[Table of Contents 2](#_Toc116405317)

[EXECUTIVE SUMMARY 3](#_Toc116405318)

[INTRODUCTION 4](#_Toc116405319)

[ANALYSIS 4](#_Toc116405320)

[REGISTRY ANALYSIS 4](#_Toc116405321)

[USER/GROUP INFORMATION 4](#_Toc116405322)

[SYSTEM INFORMATION 5](#_Toc116405323)

[USER ACTIVITY 5](#_Toc116405324)

[USB DEVICE ANALYSIS 5](#_Toc116405325)

[APPLICATION 6](#_Toc116405326)

[SHELL ITEM ANALYSIS 6](#_Toc116405327)

[MALWARE ANALYSIS 6](#_Toc116405328)

[CONCLUSION 7](#_Toc116405329)

[TOOLS 7](#_Toc116405330)

# 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.

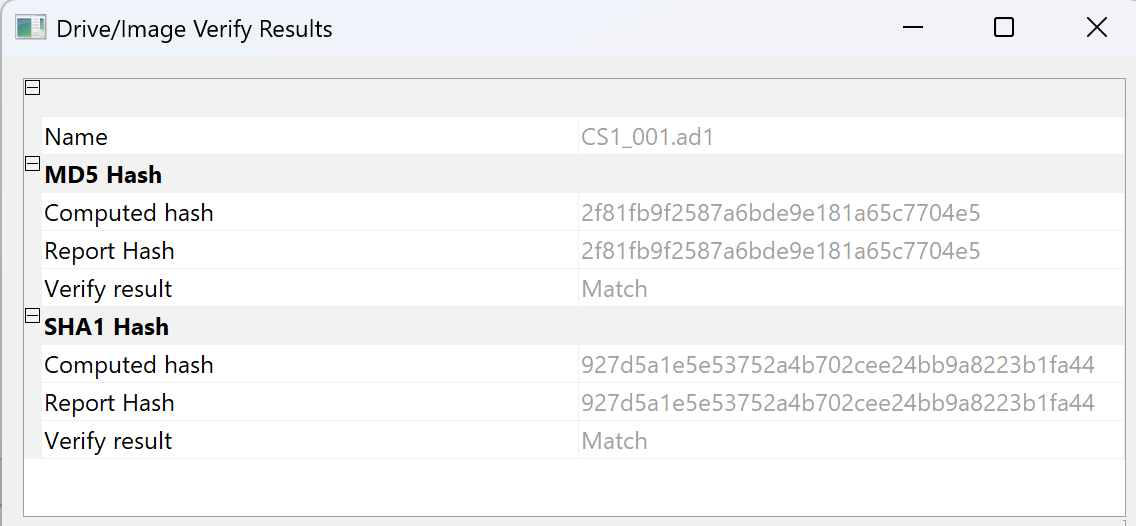


Figure 1 Verification of the system investigated named “CS1\_001”

# ANALYSIS

## REGISTRY ANALYSIS

|  |  |
| --- | --- |
| Key | Value |
| Microsoft OS Version | Windows 10 Pro (10.0.16299.15) |
| Build Version | 16299 |
| Current Control Set |  |
| 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. We used the tool 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.

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.

Users have the Domain UID of S-1-5-21-263698462-3103634936-1936700066. With “S” indicating the type is an 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 require 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 priviledges, 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

### USER ACTIVITY

[This may be easier in paragraph form, but this is up to your own discretion. You could also explain the findings of each item in 2-3 sentences in a bullet point.]

* **Windows Search History:** Analysis identified that J. Smith searched for specific files or applications in the Windows Explorer bar which included, “CCleaner, proprietary document, stolen password file.”

**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersionExplorer\WordWheelQuery**

* **Typed Paths:** User srogers have not searched for specific paths on the systems based on the lack of findings under the registry key NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths.
* **RecentDocs:** Identify recent documents opened by the user or note this will be covered in a separate section if this list is long.
* **Last Executed Commands:** This may not be populated if commands were not run from the START -> RUN box.
* **UserAssist:** Identify any programs executed by the user. If this is explained under application analysis – skip this.

**2019-01-21 05:10:14Z C:\Users\srogers\Downloads\torbrowser-install-win64-8.0.4\_en-US.exe (1)**   
**...  
2019-01-20 21:26:03Z**   
**C:\Users\srogers\Downloads\BitTorrent.exe (1)   
...**  
**Mon Jan 21 16:57:41 2019 UTC**   
**C:\Users\srogers\Documents\USB Backup\privacy-eraser-setup.exe (1)**

## USB DEVICE ANALYSIS

[Detail any relevant findings and note any devices connected by users of interest in a specific timeframe. Include the Friendly Name or type of device, the user that connected the device, serial number, first time connected, and last time connected. In the narrative, explain why devices are of interest. You can omit devices unrelated to your investigation or suspect, or leave them in, but explain why they’re unrelated. Identify any volume letters that may have been assigned to the device by the operating system.]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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

[Note: I typically remove timestamps for policy violations, but for legal and malware cases these are may be important. The idea is to keep the tables clean and report the relevant information for sanctions or appropriate action. This table can be used for shell items and prefetch as well. The amount of columns and their titles will clearly change.]

## APPLICATION ANALYSIS

[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?]

## PREFETCH ANALYSIS

[Identify any programs executed, the number of times, the first time and last time of execution. Include a table that shows ONLY the rows that are important to your investigation. If there are more than 10 rows, this table must be moved to an appendix. Make sure the table is labeled and formatted, similar to the USB device table above.

Table X – Prefetch Analysis for [System Name]

[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.]

## SHELL ITEM ANALYSIS

[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.]

[These tables can be made yourself or be formatted after being output from a tool, which is easier.]

## MALWARE ANALYSIS

[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

[Here I list the tools and version numbers used throughout the report. This allows other examiners to verify my work and determine what conclusions may have been drawn incorrectly due to the tool itself. This is a best practice to ensure the tool versions are at least in the body of the report.]

Access Data Forensic Toolkit (FTK) v6.4

Access Data FTK Imager v3.4.2.6

Registry Ripper v2.8

Autopsy v4.6.0

Eric Zimmerman’s tools and version numbers

USBDeviceForensics v.X.X.X