Northeastern University
College of Computer and Information Science

Case Project

CY5210 Information System Forensics

Instructor: Elton Booker

Samyukta Kurikala

EXECUTIVE SUMMARY

On 3 February 2025, the Shield SOC team alerted me to a network event involving the download of BitTorrent and Privacy Cleaner on the AVENGERS01 system. These applications violate the company's Acceptable Use Policy (AUP) and raised concerns about potential data exfiltration or unauthorized activity. Upon notification, I acquired a forensic image of the system on 4 February 2025 and began a comprehensive analysis to determine the extent of any policy violations or security breaches.

The investigation revealed that the user "srogers" had connected a USB device, "Shield_USB - Kingston DataTraveler 2.0," and transferred sensitive files, including "Presentation with Sensitive IP.pptx." Additionally, Dropbox was used to upload and download corporate files, further increasing the risk of data exfiltration. Analysis of prefetch, registry, and shell item artifacts confirmed attempts to obfuscate actions, including the use of Privacy Eraser and the uninstallation of BitTorrent and OneDrive before the forensic analysis. A presence of Tor Browser was also found in the system

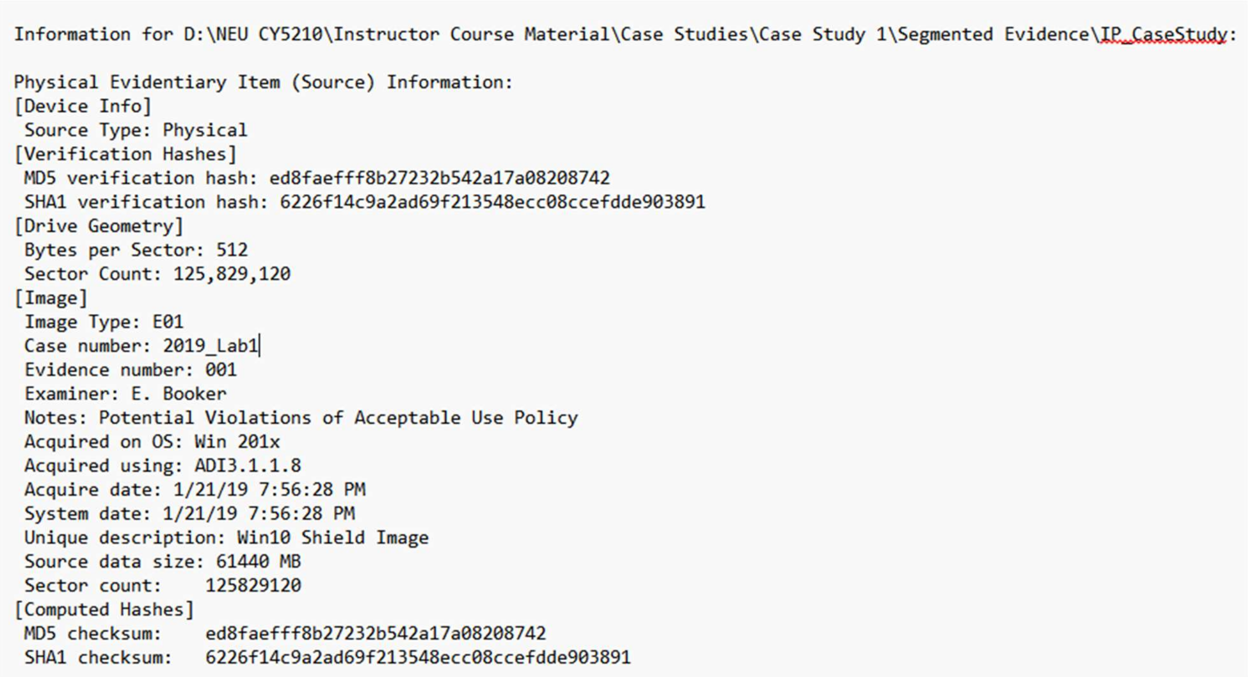
Key findings indicate that unauthorized data transfer occurred through both physical and cloud-based storage, constituting a significant security policy violation. The presence of anti-forensic activity suggests intentional concealment. As a result, I recommend immediate mitigation actions, including a full security review of corporate email and network logs, recovery of the suspect’s USB device, and further questioning by corporate investigators or law enforcement. Based on these findings, disciplinary action against the user is advised, potentially leading to civil or criminal charges if deemed necessary by legal counsel.

INTRODUCTION

On 3 February 2025, I was notified of the incident when the Shield SOC team alerted me to a network event indicating the download of BitTorrent and a Privacy Cleaner utility on one of the systems over the weekend. Both tools are in violation of the company's Acceptable Use Policy (AUP) and are flagged as potentially unwanted programs (PUPs). The download of these programs raised concerns due to the possibility of malicious activity, such as malware installation, data exfiltration, or unauthorized actions.

I downloaded the image of a system – AVENGERS01 released by Elton Booker on 4 February 2025 and started my analysis. My primary goal was to assess whether any malicious activity had occurred, including the installation of malware or the exfiltration of data. I examined the system for signs of unauthorized access, any malicious payloads associated with the downloaded programs, and any evidence of data transfers that could indicate exfiltration or other unauthorized actions.

The chain of custody documents was completed on 06 February 2025.



```
Information for D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 1\Segmented Evidence\IP_CaseStudy:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Verification Hashes]
 MD5 verification hash: ed8faefff8b27232b542a17a08208742
 SHA1 verification hash: 6226f14c9a2ad69f213548ecc08ccefdde903891
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 125,829,120
[Image]
 Image Type: E01
 Case number: 2019_Lab1
 Evidence number: 001
 Examiner: E. Booker
 Notes: Potential Violations of Acceptable Use Policy
 Acquired on OS: Win 201x
 Acquired using: ADI3.1.1.8
 Acquire date: 1/21/19 7:56:28 PM
 System date: 1/21/19 7:56:28 PM
 Unique description: Win10 Shield Image
 Source data size: 61440 MB
 Sector count:    125829120
[Computed Hashes]
 MD5 checksum:    ed8faefff8b27232b542a17a08208742
 SHA1 checksum:   6226f14c9a2ad69f213548ecc08ccefdde903891
```

Figure 1: Verified Hashes

ANALYSIS

I focused my analysis on the key registry hives (SAM, SECURITY, SOFTWARE, SYSTEM) and user hives (NTUSER.DAT and USERCLASS.DAT). These hives played a critical role in identifying user-specific activities, system configurations and security settings that provided insight into unauthorized or malicious activities.

During my analysis, I identified a USB device that had being plugged into the system. A detailed examination of the device determined a potential involvement in the incident.

Further, an application analysis was carried out using artifacts line Prefetch files, LNK files, Jump Lists and Shellbags. These were essential in identifying recently executed applications and potentially malicious programs running on the system.

The subsections below explain the findings in detail, providing a comprehensive view of the analysis process and the obtained evidence.

REGISTRY ANALYSIS

- The Windows registry for AVENGERS01 was analyzed for specific system configurations and settings, user specific settings, and user activity using Windows Registry Ripper v3.0. The SAM, SYSTEM, SOFTWARE and user hives (NTUSER.DAT and USRCLASS.DAT) were reviewed for relevant information pertinent to this investigation. The Windows registry identifies current system configuration and settings that may be useful to show the current state of the system and the actions performed by all users on a system.

USER/GROUP INFORMATION

- **Users:**

Table 1 – User Information in AVENGERS01

Usernames	SIDs	Last Login Date
Administrator	S-1-5-21-263698462-3103634936-1936700066-500	Never
Guest	S-1-5-21-263698462-3103634936-1936700066-501	Never
Default Account	S-1-5-21-263698462-3103634936-1936700066-503	Never
WDAGUtilityAccount	S-1-5-21-263698462-3103634936-1936700066-504	Never
srogers	S-1-5-21-263698462-3103634936-1936700066-1001	2019-01-21

After the analysis of the SAM registry hive, 5 users were identified out of which 4 of them were never logged into. This makes the srogers user with the SID S-1-5-21-263698462-3103634936-1936700066-1001 the only user account of interest. This account was last logged into on 21 January 2019.

- **Groups:**
  Under the Administrators group 2 accounts exist Admistrator and srogers
  SIDs:
  S-1-5-21-263698462-3103634936-1936700066-500
  S-1-5-21-263698462-3103634936-1936700066-1001
  No users are granted the right to logon remotely
  Password Policy : No Password required

SYSTEM INFORMATION

- **Microsoft OS Version:** Windows 10 Pro
- **Build Version:** 16299.rs3_release_svc.180808-1748
- **Current Control Set:** ControlSet001
- **OS Install Date:** 2019-01-19
- **Computer Name:** AVENGERS01
- **Time Zone:** Eastern Standard Time
- **Network Interfaces with Last Connection Time:**
- **Autostart Programs:** Dropbox, SecurityHealth, VMware User Process, GrpConv
- **Last Shutdown Time:** 2019-01-20 21:11:38Z

USB DEVICE ANALYSIS

The USB device was analyzed using USB Detective v1.3.6. The SYSTEM, SOFTWARE, NTUSER.DAT and setupapi.log files were given to the tool for analysis. FTK Imager v4.7.1 was used to extract these files from the image.

The device was named **Shield_USB** and it is a **Kingston DataTraveler 2.0 USB Device**. The serial number was **200706200000000059187F6F**. The user account was **srogers** and the volume letter assigned to the device was **E**: . The first time the device was connected to the system is recorded as **21 January 2019 at 12:00:14 AM** and the last time was on **21 January 2019 at 12:17:03 PM**.

Table 2 – USB Devices Connected to AVENGERS01

Device Name	Serial Number	User Account	First Time	Last Time
Shield_USB - Kingston DataTraveler 2.0 USB Device	200706200000000059187F6F	srogers	1/21/2019 12:00:14 AM	1/21/2019 12:17:03 PM

APPLICATION ANALYSIS

During the application analysis I found that **Privacy Eraser** and **BitTorrent** were installed on the system. Along with that I also found that **Tor Browser** and **DropBox** applications were installed on the system too. These also indicate potential malicious behavior and must be investigated further. The user srogers uninstalled the applications **BitTorrent** and **Microsoft OneDrive** prior to the investigation, suggesting an attempt to remove evidence.

PREFETCH ANALYSIS

A prefetch analysis was conducted to identify the frequently used applications. The prefetch files were exported using **FTK Imager**. I used **PECmd.exe v1.5.1** for prefetch analysis. Out of all the applications the below table shows the applications of interest. Tor Browser was run once, DropBox and DropBox Update were run 18 times, Privacy Eraser was run thrice and BitTorrent was run twice.

Table 3 – Prefetch Analysis for AVENGERS01

Application Name	Times Ran	First Time	Last Time
TOR.EXE	1	1/21/2019 5:10	1/21/2019 5:10
DROPBOX.EXE	1	1/20/2019 21:13	1/20/2019 21:17
PRIVACYERASER64.EXE	3	1/21/2019 16:57	1/21/2019 16:57
BITTORRENT.EXE	2	1/20/2019 21:26	1/20/2019 21:27
DROPBOXUPDATE.EXE	17	1/20/2019 21:19	1/21/2019 19:18

SHELL ITEM ANALYSIS

Shell item analysis was done. I analysed Shellbags, Jump Lists and LNK Files. Shellbags provide evidence of accessed or deleted directories, even if the files themselves no longer exist. Jumplists identify frequently used programs and LNK files contain metadata about files and applications that were opened.

Table 4 – Shellbag Analysis for AVENGERS01

Filename	Location	User Account	Created Time	Modified Time
Dropbox	Desktop\Shared Documents Folder (Users Files)\Dropbox	srogers	1/21/2019 5:09	1/21/2019 5:09

Shield Documents	Desktop\Shared Documents Folder (Users Files)\Dropbox\Shield Documents	srogers	1/21/2019 5:06	1/21/2019 5:07
USB Backup	Desktop\My Computer\Documents\USB Backup	srogers	1/21/2019 5:06	1/21/2019 5:06
shielddocuments	Desktop\MyComputer\Downloads\shielddocuments	srogers	1/21/2019 16:57	1/21/2019 16:57

After a shellbag analysis using SBECmd v2.1.0 was done, I found these files and applications of interest. The user appears to be using Dropbox to transfer files over the internet. He uploaded sensitive files to Dropbox at 5:07 AM named Shield Documents and downloaded a file named shielddocuments at 16:57. He also appears to be maintaining these a USB Backup for these files.

Table 5– Jump List Analysis for AVENGERS01

Filename	MRU	AppId	User Account	Source Created (First)	Source Modified (Last)
Dropbox	6	20614-f01b4d95cf55d32a	srogers	1/20/2019 9:12:02 PM	1/21/2019 5:21:16 AM
Presentation with Sensitive IP.pptx	5	20603-5f7b5f1e01b83767	srogers	1/20/2019 9:12:02 PM	1/21/2019 5:07:00 AM
Shield Documents	5	20614-f01b4d95cf55d32a	srogers	1/20/2019 9:12:02 PM	1/21/2019 5:21:16 AM
USB Backup\Shield Documents	4	20614-f01b4d95cf55d32a	srogers	1/20/2019 9:12:02 PM	1/21/2019 5:21:26 AM
USB Backup	1	20614-f01b4d95cf55d32a	srogers	1/20/2019 9:12:02 PM	1/21/2019 7:15:47 PM

The jumplist data extracted from JLECmd v1.5.1, reveals user srogers accessed and transferred multiple files across different storage locations. A file named "Presentation with Sensitive IP.pptx" was accessed from Dropbox and later modified. Additionally, a folder labeled "Shield Documents" appeared in Dropbox and was also backed up to a USB device. The USB backup contained the "Shield Documents" folder, indicating a potential transfer of sensitive information. The presence of the same folder across multiple locations suggests an intentional effort to store or duplicate the data on different mediums.

Table 6 – LNK File Analysis for AVENGERS01

Filename	Location	User Account	Source Created (First)	Source Modified (Last)
Presentation with Sensitive IP.pptx	C:\Users\srogers\Documents\USB Backup\Shield Documents\Presentation with Sensitive IP.pptx	srogers	1/21/2019 5:06:54 AM	1/21/2019 3:48:38 AM
USB Backup	C:\Users\srogers\Documents\USB Backup	srogers	1/21/2019 5:06:45 AM	1/21/2019 5:21:26 AM
Shield Documents	C:\Users\srogers\Documents\USB Backup\Shield Documents	srogers	1/21/2019 5:06:54 AM	1/21/2019 5:06:54 AM

The LNK file analysis done using LECmd v1.5.1 also indicates that the user, srogers, maintained a USB backup of sensitive files. The folder "Shield Documents" was stored within "USB Backup", and it contained a file named "Presentation with Sensitive IP.pptx. The creation time of "Presentation with Sensitive IP.pptx" occurs after its last modified time. This suggests that the file was originally created or modified on another system or location before being copied to the USB Backup directory.

ACTIVITY TIMELINE

- The user installed DropBox on 1/20/2019 at 21:13
- The user installed BitTorrent on 1/20/2019 at 21:26
- The USB device Shield_USB was connected to the system for the first time on 1/21/2019 at 12:00 AM
- The user accessed or copied the folder Shield Documents onto the USB on 1/21/2019 at 4:57
- The user modified the folder Shield Documents in USB Backup on 1/21/2019 at 5:06
- The folder Shield Documents was accessed on Dropbox on 1/21/2019 at 5:07
- The user installed Tor Browser on 1/21/2019 at 5:10
- The user installed Privacy Eraser on 1/21/2019 at 16:57

- The user downloaded a folder named “shielddocuments” on 1/21/2019 at 16:57
- The user uninstalled BitTorrent and Privacy Eraser.

USER ACTIVITY

- **Windows Search History:** The user srogers has not appeared to have searched for specific files or applications in the Windows Explorer bar according to the lack of evidence identified under the registry key NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery.
- **Typed Paths:** The user srogers has not appeared to have searched for specific paths on the system according to the lack of evidence identified under the registry key NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths.
- **RecentDocs:** The recent documents opened by the user include -Personal, Random Accounting Spreadsheet.xlsx, USB Backup, Selection_of_materials.ppt, Chapter 4.pdf, Cap-2.jpg, Cap-1.jpg, Shield Documents, Presentation with Sensitive IP.pptx, This PC, Documents, S. Rogers Resume.docx, Confidential Alloy Expense Accounts.xlsx, Shield_USB (E:), Alloys.pptx, Alloys.ppt, network, The Internet.
- **Last Executed Commands:** The user has not appeared to typed commands START -> RUN box according to the lack of evidence under the registry key NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU.

CONCLUSION

The forensic examination of AVENGERS01 confirmed a clear violation of company policy, specifically unauthorized data transfer and the use of prohibited applications. The evidence suggests that user "srogers" engaged in potentially malicious activity, including the exfiltration of sensitive corporate documents through USB and cloud-based storage services.

Findings:

- **USB Device Usage:** The "Shield_USB" Kingston DataTraveler 2.0 was used to store sensitive company files.

- **Cloud Storage:** The user uploaded proprietary files to Dropbox, including "Shield Documents" and "Presentation with Sensitive IP.pptx."

- **Application Activity:** BitTorrent, Tor Browser, and Privacy Eraser were installed, with Privacy Eraser used to delete traces of activity.

- **Anti-Forensics:** The user uninstalled BitTorrent and OneDrive before analysis, indicating an attempt to hide evidence.

Recommendations:

- **Security Measures:** Restrict USB access and enforce stricter monitoring of cloud storage usage.
- **Disciplinary Actions:** Consider administrative or legal proceedings against the user of the account "srogers," depending on company policy and legal review.
- **Further Investigation:**
    - Retrieve and analyze "Shield_USB" for additional evidence.
    - Identify any additional devices used by "srogers" to access corporate data.
    - Conduct an interview with "srogers" to clarify intent and additional actions.

Based on the findings, this case requires immediate remediation efforts to prevent future data exfiltration attempts and reinforce the organization's cybersecurity policies.

TOOLS

- Access Data FTK Imager v4.7.1
- Arsenal Image Mounter v3.4.141
- Registry Ripper v3.0
- Access Data Registry Viewer v2.0.0
- Autopsy v4.6.0
- Eric Zimmerman's tools and version numbers
    - LECmd v1.5.1
    - JLECmd v1.5.1
    - SBECmd v2.1.0
    - PECmd v1.5.1
- USB Detective v1.3.6