Northeastern University
College of Computer and Information Science

Case Project

CY5210 Information System Forensics

Instructor: Elton Booker

Samyukta Kurikala

EXECUTIVE SUMMARY

On 18 February 2025, the Director of Cybersecurity requested a full investigation into a potential data exfiltration incident involving Ethan Thomas, following concerns raised by his supervisor, Daniel Smith. Mr. Thomas was reported to be drafting a resignation letter while planning to join a competitor, Next Generation Computing. Additionally, his primary Windows system had been wiped and re-imaged due to reported performance issues and multiple antivirus alerts. Given the sensitive nature of Capital Computing's proprietary projects, an investigation was launched to determine whether corporate data had been improperly accessed, transferred, or exposed.

A forensic analysis of ETHOMAS_DESKTOP revealed strong evidence of data exfiltration and potential corporate espionage. Key findings indicate that USB devices were used to store sensitive company data, proprietary files were uploaded to Dropbox, and PuTTY may have facilitated unauthorized transfers between user accounts. Additionally, forensic traces show that CCleaner was used and later uninstalled, a known anti-forensics tactic to erase activity logs. Malware was also detected on the system, possibly from unauthorized downloads. These findings suggest deliberate attempts to conceal digital activity and move company data outside of secure corporate channels.

Based on these discoveries, immediate remediation is required to prevent further security risks. It is recommended that USB access restrictions and enhanced cloud storage monitoring be implemented. Legal and administrative actions should be considered against Mr. Thomas, depending on company policy and legal review. Further investigation is necessary, including retrieving USB devices, identifying additional devices involved, and conducting an interview with Mr. Thomas to clarify intent. These steps will help strengthen the organization's cybersecurity posture and mitigate future risks of data breaches.

INTRODUCTION

On 18 February 2025 I was notified of the situation when the Director of Cybersecurity asked for a full report on any potential data loss, exposure or leak of company proprietary data. The incident was initially reported by Mr. Thomas's supervisor, Daniel Smith, who informed Human Resources that Thomas was drafting his resignation and planning to join a competitor, Next Generation Computing. Mr. Thomas had reported performance issues and multiple anti-virus alerts on his primary Windows system, which was subsequently wiped and re-imaged by the Service Desk. Due to the sensitive nature of Capital Computing's proprietary projects, this activity raised concerns regarding potential data exfiltration and corporate espionage.

I downloaded the image of a system, ETHOMAS_DESKTOP, released by Elton Booker on 18 February 2025 and started my analysis. My primary goal is to assess any probable data exfiltration and espionage. I examined the system for signs of unauthorized downloading or transfer of information.

The chain of custody document was completed on 02/18/2025.

```
Information for D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 2\Segmented\InsiderThreat_CaseStudy:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Verification Hashes]
 MD5 verification hash: 4346fde8ca6e6b5feed3dd2c566e3abd
 SHA1 verification hash: 342a4c51c508aa21d77de0a7710838785ff470a2
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 125,829,120
[Image]
 Image Type: E01
 Case number: IA5210_InTP
 Evidence number: 2018_001
 Examiner: Forensic Analyst XXXXXX
 Notes:
 Acquired on OS: Win 201x
 Acquired using: ADI3.4.2.6
 Acquire date: 4/3/18 4:59:25 PM
 System date: 4/3/18 4:59:25 PM
 Unique description: InsiderThreat Case
 Source data size: 61440 MB
 Sector count:    125829120
[Computed Hashes]
 MD5 checksum:    4346fde8ca6e6b5feed3dd2c566e3abd
 SHA1 checksum:   342a4c51c508aa21d77de0a7710838785ff470a2

Image Information:
 Acquisition started:   Wed Oct 13 08:39:14 2021
 Acquisition finished:  Wed Oct 13 08:55:19 2021
 Segment list:
  D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 2\Segmented\InsiderThreat_CaseStudy.E01
  D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 2\Segmented\InsiderThreat_CaseStudy.E02
  D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 2\Segmented\InsiderThreat_CaseStudy.E03
  D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 2\Segmented\InsiderThreat_CaseStudy.E04
  D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 2\Segmented\InsiderThreat_CaseStudy.E05
  D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 2\Segmented\InsiderThreat_CaseStudy.E06
  D:\NEU CY5210\Instructor Course Material\Case Studies\Case Study 2\Segmented\InsiderThreat_CaseStudy.E07

Image Verification Results:
 Verification started:  Wed Oct 13 08:55:20 2021
 Verification finished: Wed Oct 13 09:03:23 2021
 MD5 checksum:    4346fde8ca6e6b5feed3dd2c566e3abd : verified
 SHA1 checksum:   342a4c51c508aa21d77de0a7710838785ff470a2 : verified
```

Figure 1: Hash Verification

Both the hashes MD5 and SHA1 are verified.

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 USB devicse that were plugged into the system. A detailed examination of the devices 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 ETHOMAS_DESKTOP was analyzed for specific system configurations and settings, user specific settings, and user activity using Windows Registry Ripper v2.8. 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 ETHOMAS_DESKTOP

Username	SID	Last Login
Administrator	S-1-5-21-82160412-4011698849-1881082856-500	Never
Guest	S-1-5-21-82160412-4011698849-1881082856-501	Never
DefaultAccount	S-1-5-21-82160412-4011698849-1881082856-503	Never
WDAGUtilityAccount	S-1-5-21-82160412-4011698849-1881082856-504	Never
ethomas	S-1-5-21-82160412-4011698849-1881082856-1001	2018-04-03 16:30:23
ethan_local	S-1-5-21-82160412-4011698849-1881082856-1002	2018-04-03 16:14:23

- **Groups:**
  Administrators
    SIDs:
      - S-1-5-21-82160412-4011698849-1881082856-500 (Administrator)
      - S-1-5-21-82160412-4011698849-1881082856-1001 (ethomas)
      - S-1-5-21-82160412-4011698849-1881082856-1002 (ethan_local)

Password Policies: No password needed

The Administrator group has 3 users Administrator, ethomas, ethan_local
There do not seem to be any other groups of interest.
No user is given access to login remotely.

SYSTEM INFORMATION

- **Microsoft OS Version:** Windows 10 Pro
- **Build Version:** 16299.rs3_release.170928-1534
- **Current Control Set:** ControlSet001
- **OS Install Date:** 2018-03-27 00:01:29
- **Computer Name**: ETHOMAS_DESKTOP
- **Time Zone:** Eastern Standard Time
- **Network Interfaces with Last Connection Time:** Ethernet0 - Intel(R) 82574L Gigabit Network Connection (wired) - 2018-04-03 16:29:08
- **Autostart Programs:** SecurityHealth, VMWare User Process, Dropbox
- **Last Shutdown Time:** 2018-04-03 00:56:01

USER ACTIVITY

- **Windows Search History:** Analysis identified that Ethan Thomas searched for specific files or applications in the Windows Explorer bar which included, “ccsetup, cc, sensitive, intellectual, proprietary”
- **Typed Paths:** E.Thomas 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.
- **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.

RECENT DOCS

ethan_local:

1. Ethan Thomas Resignation Letter.docx
2. EthanThomas_Notes.docx

3. Intellectual Property Document.docx
4. Downloads
5. Personal USB (E:)
6. Sensitive Potential Client List.xlsx
7. Cat with Tongue Out.jpg
8. Cat in cute pose.jpg
9. Adorable Cats.jpg
10. The Internet

ethomas:

1. EthanThomas_Notes.docx
2. Company Sensitive Document.docx
3. Dropbox
4. Intellectual Property Document.docx
5. IronKey Secure Files (F:)
6. Proprietary Corporate Data.pptx
7. SFIR Lab Lesson 5.pptx
8. 9781111310646_PPT_ch07.pptx
9. Sensitive Potential Client List.xlsx
10. Downloads
11. ::{E2E7934B-DCE5-43C4-9576-7FE4F75E7480}

According to the analyzed user activity, E.Thomas seems to be searching for and working on files that appear to be confidential and proprietary. He also appears to be transferring these files into USB drives. There is also a Resignation letter which confirms that he wanted to resign.

USB DEVICE ANALYSIS

Table 1 – USB Devices Connected to ETHOMAS_DESKTOP

Device Name	Serial Number	User Account	First Connected	Last Connected
IronKey Secure Drive USB Device	00787613	ethomas	3/31/2018 10:03:01 AM	4/3/2018 12:15:35 PM
Kingston DataTraveler G3 USB Device	0019E000B499EBB166A2018F	ethan_local	3/31/2018 11:36:49 AM	4/3/2018 9:36:29 AM
Kingston DT Rubber 3.0 USB Device	0018F30C9FEABD80610D1AAC	ethomas	4/3/2018 12:20:19 PM	4/3/2018 12:20:20 PM
WD My Passport 2599	575854314541354441545352		4/3/2018 12:22:43 PM	4/3/2018 12:23:23 PM

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.

4 devices have been identified out of which 2 seem to be relevant to the case. Both users have accessed these drives and data has been transferred from the computer into the drives.

APPLICATION ANALYSIS

An application 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 table below shows the applications of interest.

PREFETCH ANALYSIS

During my analysis, I discovered several applications that could indicate potential data exfiltration and evidence tampering. Dropbox was installed on the device, suggesting it may have been used to transfer confidential company data externally. Additionally, CCleaner was found and had been used on the same day the device was seized for analysis, indicating a possible attempt to erase forensic evidence and cover tracks. Further investigation revealed the presence of IRONKEY, which suggests the use of an encrypted USB device, potentially requiring decryption to access stored data. FSQUIRT, a Bluetooth file transfer application, was also identified, which could have been used for legitimate purposes or for unauthorized data transfers. The presence of PuTTY indicates possible SSH connections to external servers, raising concerns about remote data access. Finally, 7-Zip was installed, likely to compress large files for easier transfer. These findings collectively point to potential data exfiltration.

Table 2 – Prefetch Analysis for ETHOMAS_DESKTOP

Application Name	Times Ran	First Time	Last Time
CCLEANER	5	4/3/2018 13:37	4/3/2018 14:01
DROPBOX	12	3/31/2018 14:44	4/3/2018 0:59
IRONKEY	4	3/31/2018 14:03	4/3/2018 16:15
FSQUIRT	2	3/27/2018 0:12	3/31/2018 14:48
PUTTY	1	3/31/2018 16:08	3/31/2018 17:14
7Z1801-X64.EXE-5C12C475	1	3/31/2018 13:22	3/31/2018 13:22

USERASSIST

Table 3 – UserAssist Analysis for ETHOMAS_DESKTOP

User Account	Application File	Times Ran	Last Time
ethan_local	IronKey.exe	2	2018-04-03 14:01:43
ethan_local	CCleaner64.exe	1	2018-04-03 13:59:16
ethomas	Dropbox.Desktop.Client	2	2018-03-31 14:45:48Z

SHELL ITEM ANALYSIS

Shell item analysis was done. I analyzed 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 ETHOMAS_DESKTOP

Filename	Location	User Account	Created Time	Modified Time
Dropbox	Desktop\Shared Documents Folder (Users Files)\Dropbox	ethomas	3/31/2018 13:21	3/31/2018 13:21

After a shellbag analysis using SBECmd v2.1.0 was done, I found that the user had Dropbox installed on the device. He probably used it to upload sensitive files onto the internet.

Table 5 – Jump List Analysis for ETHOMAS_DESKTOP

Filename	MRU	AppId	User Account	Source Created (First)	Source Modified (Last)
Ethan Thomas Resignation Letter.docx	0	5f7b5f1e01b83767	ethan_local	3/31/2018 14:48	3/31/2018 23:10
Intellectual Property Document.docx	3	d38a3ea7ec79fbed	ethan_local	3/31/2018 15:39	3/31/2018 15:39
Sensitive Potential Client List.xlsx	8	d38a3ea7ec79fbed	ethan_local	3/30/2018 18:18	3/30/2018 18:17

EthanThomas_Notes.docx	2	5f7b5f1e01b83767	ethan_local, ethomas	3/27/2018 0:11	3/31/2018 14:45
Company Sensitive Document.docx	5	5f7b5f1e01b83767	ethomas	3/31/2018 14:21	3/31/2018 14:45
Proprietary Corporate Data.pptx	9	ecd1a5e2c3af9c46	ethomas	3/27/2018 0:11	3/31/2018 14:45
9781111310646_PPT_ch07.pptx	7	ecd1a5e2c3af9c46	ethomas	3/27/2018 0:11	3/31/2018 14:45
SFIR Lab Lesson 5.pptx	6	ecd1a5e2c3af9c46	ethomas	3/27/2018 0:11	3/31/2018 14:45
Dropbox	0	f01b4d95cf55d32a	ethomas	3/27/2018 0:11	3/31/2018 14:45

The Jump List file analysis was done using JLECmd v1.5.1. It provides insight into the recent activities of users ethomas and ethan_local. The timestamps indicate that sensitive files, such as "Ethan Thomas Resignation Letter.docx", "Intellectual Property Document.docx", and "Sensitive Potential Client List.xlsx", were accessed and modified between March 27 and March 31, 2018.

Several documents, including "Company Sensitive Document.docx" and "Proprietary Corporate Data.pptx", were accessed frequently used files. The presence of Dropbox in the Jump List further suggests that files may have been uploaded or synchronized with a cloud storage service. The activity patterns indicate potential data transfers or preparations for document movement.

Table 6 – LNK File Analysis for ETHOMAS_DESKTOP

Filename	Location	User Account	Source Created (First)	Source Modified (Last)
9781111310646_PPT_ch07 .pptx	F:\9781111310646_PPT_ch07.pptx	ethomas	3/31/2018 14:41	3/31/2018 14:41
Dropbox	C:\Users\ethomas\Dropbox	ethomas	3/31/2018 14:45	3/31/2018 14:45
Intellectual Property Document.docx	C:\Users\ethomas\Dropbox\ Intellectual Property Document.docx	ethomas	3/31/2018 14:43	3/31/2018 14:45
Sensitive Potential Client List.xlsx	F:\Sensitive Potential Client List.xlsx	ethomas	3/31/2018 14:22	3/31/2018 14:22

SFIR Lab Lesson 5.pptx	F:\SFIR Lab Lesson 5.pptx	ethomas	3/31/2018 14:42	3/31/2018 14:42
Ethan Thomas Resignation Letter.docx	C:\Users\ethan_local\Desktop\ Ethan Thomas Resignation Letter.docx	ethan_local	3/31/2018 15:54	3/31/2018 23:10

The LNK file analysis done using LECmd v1.5.1 reveals a series of files accessed and user activity by **ethomas** and **ethan_local** on **March 31, 2018**. The presence of LNK files referencing documents on both **F:** (USB device) and **C:** suggests that files were accessed, possibly transferred, or modified. Notably, the **"Sensitive Potential Client List.xlsx"** and **"Intellectual Property Document.docx"** indicate the sensitive company data, with the latter being stored in **Dropbox**, hinting at cloud synchronization or data transfer. The **"Ethan Thomas Resignation Letter.docx"** on the desktop of **ethan_local** was last accessed at **23:10**, hours after its creation, potentially signaling revision or review. The timestamps across these LNK files provide insight into the sequence of user activity, data movement between storage devices, and possible exfiltration concerns.

ACTIVITY TIMELINE

- Mr. Thomas was given a new updated Windows 10 system on 27 March 2018
- He installed Dropbox
- He copied sensitive files onto the USB devices on 31st March 2018 at around 14:42
- He wrote his resignation letter on 31st March 2018 at 14:48
- He installed PuTTY and 7Zip applications on 31st March 2018 between 16:00 to 17:30
- He accessed the encrypted USB on 3rd April 2018
- He used CCleaner on 3rd April 2018
- A remote acquisition of the device was carried out on 3rd April 2018

MALWARE ANALYSIS

Cat_And_Dog Screensaver.exe

slitherio.exe

CONCLUSION

The forensic examination of ETHOMAS_DESKTOP indicates probable data exfiltration and espionage. The user has shared sensitive files on Dropbox and copied them to USB devices. Data has been transferred between both the user accounts ethan_local and ethomas possibly using PuTTY. Apart from that there is also evidence of malware present on the system from some downloads.

Findings:

- **USB Device Usage**: USB devices were used to store sensitive company data.

- **Resignation Letter**: Mr. Thomas did have plans to resign.
- **Cloud Storage**: The user uploaded proprietary files to Dropbox
- **Application Activity**: CCleaner was used to erase traces of activities.
- **Anti-Forensics**: The user uninstalled CCleaner 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 ETHAN_DESKTOP depending on company policy and legal review.
- **Further Investigation:**

  o Retrieve and analyze the USB devices for additional evidence.

  o Identify any additional devices used by the user to access corporate data.

  o Conduct an interview with Mr.Thomas 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