

ACCD5000 - Research-Based Evaluation of Computer Forensics Tools (Task 1)

Armand OCTEAU - 2422790
University of Wales Trinity Saint David
Swansea, Wales

Academic year 2024-2025
2422790@student.uwtsd.ac.uk

Abstract— In modern cybersecurity investigations, digital forensics plays a critical role in the processing of digital evidence. With the rise of IoT and the digital world, threats have evolved to new boundaries that require appropriate forensic tools to conduct effective investigations. In this research, four widely used open-source computer forensic tools are evaluated based on their characteristics—namely Autopsy, Hashcat, Volatility, and Wireshark. Each of these tools covers a different area of forensics: file system analysis, password recovery, memory forensics, and network traffic analysis. Their functionalities, strengths, limitations, and level of legal recognition are explored to better understand how and when to use each of them in a forensic context.

Keywords—Computer Forensics Tools, Cybercrime Investigation, Cybersecurity, Data Recovery, Digital Forensics, Evidence Acquisition, Forensic Imaging, Incident Response, Autopsy, Hashcat, Volatility, Wireshark.

I. INTRODUCTION

In computer forensics, open-source software plays a crucial role in processing digital evidence. Unlike proprietary software, the source code of such software is fully accessible to anyone: everything an open-source app does, we know how. During investigations, reliability and transparency above all are mandatory. That's why the use of open-source software has become highly recognized in this field. The capability to prove how data has been extracted is essential in defending findings in legal contexts such as in court.

Volatility, Hashcat, Autopsy, and Wireshark were chosen for this research because of their open-source code base. Furthermore, each of these tools is used for four main different purposes in forensics: memory extraction for Volatility; password cracking or brute-force attacks for Hashcat; analyzing file systems, recovering files on external disks, and more for Autopsy; and network analysis for Wireshark.

Even though other tools like FTK Imager or DumpIt are widely used and often combined with those discussed here, this study focuses on open-source tools due to their accessibility, transparency, and frequent use in academic and training contexts. These choices allow for a diversified exploration across the three major areas commonly studied in digital forensics: disk forensics, password analysis, and memory forensics. Many commercial alternatives such as EnCase or FTK Imager are also widely used in the field, but were not the focus of this research.

II. OPEN-SOURCE TOOLS IN DIGITAL FORENSICS

Like said in the introduction, an open-source software is characterized by its publicly accessible source code, allowing users to inspect, modify, and redistribute it freely. The term “open-source” is formally defined by the Open Source Initiative (OSI), which shows what's necessary in terms of conditions for a license to be considered open. According to Altheide and Carvey, these conditions include free redistribution, access to source code, and the right to modify and use the software without any restrictions [1, ch. 1].

A. Open Source licenses types

Open-source software is distributed under licenses that define how it can be used, modified, and shared. Actually, there are currently dozens of licenses approved by the Open Source Initiative (OSI), each with its own conditions related to the redistribution and modification [1, p. 4].

Among the most common licenses is the GNU Public License (GPL), which follows a copyleft model. This means that any software using GPL code must also remain open-source if it is redistributed. The GPL thus prioritizes the rights of the original author so that all new versions of the code remain open and transparent [1, p. 5].

In contrast, the BSD license is more permissive. It allows developers to use, modify, and redistribute code without the obligation to make their changes public. This license favors the user's freedom, even if it means the code may be incorporated into proprietary software [1, p. 5].

Another widely used license is the Apache License, which also allows flexible use of the code while requiring proper attribution and including a clear limitation of liability.

B. Limitations and Risks

However, while open-source software may be a blessing for some, it's also a nightmare for others. Designed after the type of licenses they were given, a tool can be discontinued: there's a lack of guaranteed long-term support. Many projects are initiated by individuals or small teams and may be abandoned over time. In some cases, restrictive licenses (e.g., GPLv3) may sometimes prevent others from legally continuing the development after a project is discontinued, and so even if the source code is publicly available.

This issue creates a dependency risk for investigators who build workflows around those tools that may suddenly stop evolving or becoming insecure.

An other risk is that some of those tools aren't recognized by the National Institute of Standards and Technology (NIST). This United States government agency is world widely known and plays a pivotal role in the evaluation and standardization of digital forensic tools. Without such recognition or validation, any evidences obtained through unrecognized tools may be challenged in court or even deemed inadmissible, especially if the methodology cannot be demonstrated or legally reliable.

Therefore, when choosing open-source tools, investigators should carefully evaluate the community activity, updates frequencies, licensing terms and validation from the NIST.

C. Importance of Open Source in Computer Forensics

In computer forensics, tools must be reliable and transparent, as the evidence collected may be used in legal proceedings. In this case, open-source tools are particularly valuable because their code is publicly accessible, allowing both investigators and courts to verify how evidence was acquired and analysed. This transparency builds trust and supports the principle of reproducibility, which is a necessity in both scientific and legal contexts.

During the last few years, open-source forensic tools have become more widely adopted than proprietary alternatives software... This shift is due mainly to the rising costs of commercial licenses, the flexibility of open-source development, and the rapid evolution of cyber threats that require customizable solutions [2]. Open-source tools are often updated by active online communities on websites like Github, and those communities eliminate the "black box" problem of closed-source software, where the internal workings of the tool cannot be reviewed or audited by the users. For forensic investigators, this makes open-source solutions not only more accessible, but often more trustworthy and adaptable than proprietary ones.

III. INDIVIDUAL TOOL ANALYSIS

In Computer Forensics, tools constantly evolve. Depending on the case and the type of evidence that's been collected, different tools will be used. The four previously chosen tools will be evaluated based on the five followings criteria: Functionality and purpose of the tool. What's it means to be used for; Is it easy of use? (does it have a user interface or is it shell based?); The compatibility with every operating system (Windows, Macintosh, Linux...); And finally, its strengths and weaknesses.

A. Volatility

Volatility is a powerful python written open-source memory forensics framework that was originally created by Aaron Walters as part of an academic research. It later became one of the most trusted tools in malware analysis, live response, and advanced digital forensics. First released in 2007, it has since been widely adopted in law enforcement, military and cybersecurity operations. Combined to other tools like DumpIt to get memory dumps from the working machine, Volatility focuses on the memory (RAM) and the information that disappear when a

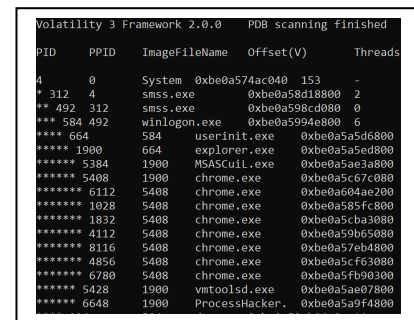
machine is shut down (unlike disk forensics) (e.g., an hidden process).

1) Strengths

Volatility has a modular design that allows it to analyse memory dumps from different operating systems, and even more recent ones since version 3 came out. Its flexibility and architecture allows it to be extended in numerous ways: analysis plugins, volshell commands, profiles and over 200 others extensions. [4, 2.3.]

This framework is ideal for detecting stealthy malware as it can reveal rootkits, process injection, hidden drivers and other forms of fileless malware that don't appear on disk.

Furthermore, this framework is command-line based, it can be easily scriptable for large-scale investigations and automation within any forensic workflows.



PID	PPID	ImageFileName	Offset(V)	Threads
4	0	System	0xbe0a574ac040	153
* 312	4	smss.exe	0xbe0a58d18800	2
** 492	312	smss.exe	0xbe0a598cd080	0
*** 584	492	winlogon.exe	0xbe0a5994e800	6
**** 664	584	userinit.exe	0xbe0a5a5d6800	
***** 1900	664	explorer.exe	0xbe0a5a5ed800	
***** 5384	1900	MSASCUIL.exe	0xbe0a5a63a800	
***** 5408	1900	chrome.exe	0xbe0a5c67c080	
***** 6112	5408	chrome.exe	0xbe0a604ae200	
***** 1028	5408	chrome.exe	0xbe0a585fc800	
***** 1832	5408	chrome.exe	0xbe0a5c3a3080	
***** 4112	5408	chrome.exe	0xbe0a59b65080	
***** 8116	5408	chrome.exe	0xbe0a57eb4800	
***** 4856	5408	chrome.exe	0xbe0a5cf33080	
***** 6780	5408	chrome.exe	0xbe0a5fb90300	
***** 5428	1900	vmtoolsd.exe	0xbe0a5ae07800	
***** 6648	1900	ProcessHacker.	0xbe0a5a9f4800	

Fig. 1. Screenshot showing the CLI interface of a memory scan from Volatility

With its efficiently written code, Volatility is fast and reliable. For example, it can list kernel modules from an 80 GB system in just a few seconds [3, p. 60]. Additionally, Volatility can be run directly from anywhere (e.g., a USB stick), without any installation required on the host system.

2) Limitations

Yet, Volatility also has its limitations. First of all, it's a CLI based framework, thus being, there's no user-interface for this program. And if that wasn't enough, Volatility has a steep learning curve, since there's no interpretation of the outputs and results given. The usage of Volatility therefore require knowledge of OS internals and memory structure.

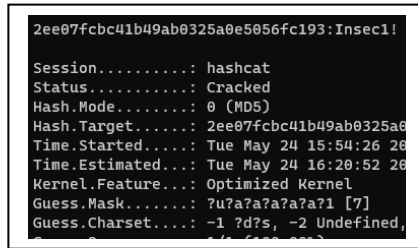
Since it's an open-source framework, as well as its extensions, some are actually outdated and not well-documented. And in addition, a memory dump is required to use Volatility. Unlike other tools (e.g., Wireshark), Volatility can't analyse systems in real-time.

Additionally, Volatility still isn't recognized as a validated tool by the NIST. Even though it is largely used and recognized widely, its usage can be disputed in court, even if most likely accepted due to its wide reputation and utilisation.

B. Hashcat

Hashcat is a powerful and widely used open-source CLI based password recovery tool. Created by a German security researcher known under the pseudonym Jens 'atom' Steube in 2009, it has then became the industry standard for password auditing.

For example, Hashcat can be used to recover a password-protected .zip file on a suspect's machine. The hash is extracted and processed to recover access.



```

2ee07fcbc41b49ab0325a0e5056fc193:Insec1!
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: 2ee07fcbc41b49ab0325a0e5056fc193:Insec1!
Time.Started....: Tue May 24 15:54:26 2016
Time.Estimated...: Tue May 24 16:20:52 2016
Kernel.Feature...: Optimized Kernel
Guess.Mask.....: ?u?a?a?a?a?1 [7]
Guess.Charset....: -1 ?d?s, -2 Undefined

```

Fig. 2. Screenshot showing the command-line interface of Hashcat processing a hash

1) Strengths

Hashcat actively supports a wide variety of hashing algorithms, including MD5, SHA1, SHA256, bcrypt, NTLM, WPA2 (e.g., used for WI-FI passwords), and many more.

A recent implementation being the GPU acceleration (supporting CUDA/OpenCL) made Hashcat extremely fast regarding its algorithms. This implementation came at a time when bitcoin mining became a thing worldwide (cryptocurrency mining being a hashing algorithm running on the hardware of the computer) [6].

Hashcat possess a lot of different attack modes to decrypt passwords: being brute-force, dictionary, hybrid, and rule-based attacks. Those are what makes Hashcat very efficient to crack-open any password protected system.

This software is also cross-platform, actively maintained by its strong community, given frequent updates, and highly efficient for password auditing and testing hash strength.

2) Limitations

By default, Hashcat is a command-line tool, making it challenging to use for beginners in forensics. It also requires in some cases an high-performance hardware (e.g., mainly the Graphic Processing Unit) for optimal and fast results.

Hashcat is also limited and cannot crack strong passwords without any hints, patterns, or dictionaries. Furthermore, Hashcat is not recognized by the NIST and has limited legal precedent. While the hash algorithms it targets are standardized, the tool itself is not formally validated. Therefore, its use should be carefully justified.

C. Autopsy

Autopsy is an open-source software that was created by Brian Carrier in March 2001, a well-known researcher and author in the field of digital forensics at his time. This software was developed as a graphical interface for The Sleuth Kit, a set of command-line forensics tools that was already existent, enabling investigators without CLI expertise to use this kit [3 and 4, 2.4].

Initially used by U.S. law enforcement agencies, Autopsy helps investigators analyse disk images in cybercrime cases. Its name “Autopsy” reflects the idea of a digital post-mortem, to examine a system after an incident (e.g., a cybercrime). This software is open-source and regularly updated by the community and Sleuth Kit Labs, preventing discontinuation problems.

1) Strengths

Autopsy has a great numbers of strengths as a computer forensic tool. For start, it has a user-friendly graphical interface that is suitable for beginners as shown below with three main windows: a tree viewer, a result viewer and a content viewer.

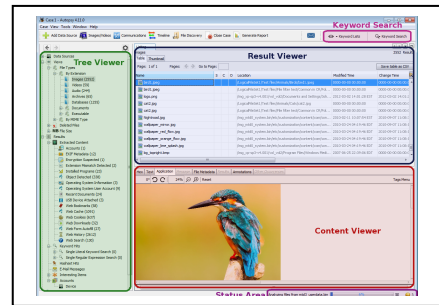


Fig. 3. Screenshot showing the user-interface of Autopsy v4

Additionally, Autopsy also supports a lot of different file-system format such as NTFS (e.g., Windows), APFS (e.g., MacOS), EXT (e.g., Linux), and others for the extraction of contents as-well as Encase images (e.g., E01) and virtual machine images (e.g., vmdk and vhd).

In the app, there's also a lot of different integrated modules that were added in addition to the Sleuth Kit. Those modules are what make Autopsy such a unique platform. We can find in those a module for example an Hash database lookup (e.g., to search for known hash extracted from Hashcat), an EXIF parser, an email and virtual machine extractor and most importantly a case management module [3, p.60].

The case management module is very useful for forensic investigators, as it provides a centralized case repository to store all case-related data, including disk images, reports, and findings. It also enables collaboration, allowing multiple investigators to work on the same case simultaneously in Autopsy. It supports automatic report generation directly within the interface.

The Keyword Search ingester from Autopsy is also a powerful tool capable to analyse from an entire disk image to a simple log file. The standard keyword list from Autopsy includes IP addresses, phone numbers, email addresses, credit card numbers, and URLs [4]. Thus giving the opportunity to search the entire disk for anything easily.

Furthermore and most of all, Autopsy enable the use of external python written plugins in its software. A plugin being a small component that adds specific features to an existing application, this means that investigators can add external features to Autopsy. Such being, since the Volatility framework is python based, a Volatility plugin can be added to Autopsy to also analyse memory dumps and basically do memory forensics, the whole while benefiting of the user-friendly interface of Autopsy [4].

Even though the Volatility plugin is not as complete as the original framework, this feature alongside the other provided plugins and the active development of this software is what makes Autopsy a great deal for forensic investigators.

2) Limitations

Despite all those cited, Autopsy is still less flexible than CLI tools for advanced or customized tasks. It is primarily focused on disk and file system analysis and is not intended

for network forensics. Autopsy also relies heavily on plugins for many advanced features (e.g., registry parsing and email analysis), some of which may not be actively maintained.

This software is also really plugin dependant for some powerful functionalities (e.g., registry parsing, email analysis, etc.), the problem being that those plugins may not be officially maintained.

And furthermore, performance issues may arise with large datasets (e.g., very heavy disks) and Autopsy does not have support for APFS encrypted volumes (thus being why Macintosh are labelled as having more privacy and security).

D. Wireshark

Wireshark is a network protocol analyser initially released in 1998 by Gerald Combs under the name Ethereal, before being renamed in 2006. Today, it is the most widely used tool for network troubleshooting, traffic inspection, and network forensics [5, p. 3].

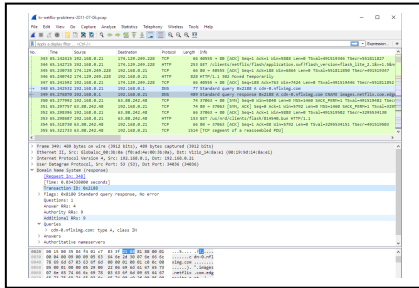


Fig. 4. Screenshot of the interface of Wireshark

1) Strengths

Wireshark possesses several strengths, the most notable being real-time packet capture from live networks or pre-recorded .pcap files. It features a user-friendly GUI with robust capabilities such as filtering, protocol breakdowns, and color-coded packet analysis. It supports hundreds of protocols and can interpret complex traffic. Wireshark is also regularly updated and maintained by a large community.

This software also supports hundreds of network protocols as well as can decode complex network communications.

Being open-source, Wireshark is also regularly updated and supported by a very large community.

2) Limitations

To use, Wireshark requires a strong understanding of network protocols to analyze captured traffic effectively. It can be resource-intensive on busy networks or when working with large .pcap files. Although it is not formally validated by NIST, its results can be used in court if clearly documented and supported by expert testimony.

IV. TOOL CATEGORISATION TABLE

Table 1 below categorizes the selected open-source forensic tools based on their category, if they are CLI or GUI based, if they are receiving active updates and if they are recognized by the NIST institute.

TABLE I. CATEGORISATION OF SELECTED FORENSIC TOOLS

Tool	Category	Interface	Updated	Cost	NIST?
Volatility	Memory Forensics	CLI	Yes	Free	Partially
Hashcat	Password Cracking	CLI	Yes	Free	No
Autopsy	File Analysis	GUI	Yes	Free	Yes
Wireshark	Network Forensics	GUI/CLI	Yes	Free	Partially

To summarize, Volatility focuses on memory analysis, operates through a command-line interface, and receives active updates. However, it is only partially recognized in legal contexts. The same applies to Wireshark, although it is GUI-based. Hashcat, on the other hand, is not formally recognized in court cases but is actively maintained and widely used. Autopsy, by contrast, is well recognized by NIST, actively updated, GUI-based, and versatile, offering a wide range of forensic utilities and extensible modules.

V. CONCLUSION

In this report, four open-source forensic tools were analysed. Tools like Autopsy, Volatility, Hashcat, and Wireshark each serve different but complementary roles in digital forensics: from file system analysis to memory inspection, password recovery, and network traffic monitoring.

While open-source tools offer strong advantages, they also present risks. These include inconsistent legal recognition, lack of official validation from institutions like NIST (in some cases), and maintenance or licensing concerns. Therefore, selecting a forensic tool requires not only technical evaluation but also legal and procedural considerations.

Ultimately, combining multiple tools tailored to the type of investigation remains the most effective strategy. Each tool reviewed in this report brings a unique capability, and when used together in a well-documented and professional workflow, they significantly strengthen the reliability and depth of a forensic analysis.

REFERENCES

- [1] C. Altheide and H. Carvey, *Digital Forensics with Open Source Tools*. Burlington, MA: Syngress, 2011.
- [2] S. Garfinkel, "Digital forensics research: The next 10 years", *Digital Investigation*, vol. 7, pp. S64–S73, 2010.
- [3] A. A. Ayetiran and I. O. Oladimeji, "Evaluation of Autopsy and Volatility for Cybercrime Investigation", *Int. J. Comput. Appl.*, vol. 183, no. 45, pp. 1–6, 2021.
- [4] M. D. Firoozjaei, A. H. Lashkari, and A. A. Ghorbani, "Memory forensics tools: a comparative analysis", *Journal of Cyber Security Technology*, vol. 6, no. 3, pp. 149–173, 2022, doi: 10.1080/23742917.2022.2100036.
- [5] G. Jain and Anubha, "Application of SNORT and Wireshark in Network Traffic Analysis," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 1119, p. 012007, 2021.
- [6] Z. Huang, D. Wang, and Y. Zou, "Prob-Hashcat: Accelerating Probabilistic Password Guessing with Hashcat by Hundreds of Times", in *Proc. of the 27th Int. Symposium on Research in Attacks, Intrusions and Defenses (RAID 2024)*, Padua, Italy, Sept. 2024, pp. 1–19, doi: 10.1145/3678890.3678919.

ACCD5000 – Digital Forensic Investigation of Internal Sabotage at CMMC (Task 2)

Armand OCTEAU - 2422790
University of Wales Trinity Saint David
Swansea, Wales

Academic year 2024-2025
2422790@student.uwtsd.ac.uk

Abstract— This report details a comprehensive digital forensic investigation into a suspected case of internal sabotage at Cyfusion Mobile Manufacturing Company (CMMC) in early 2025. Rich Daley, a former senior designer involved in the confidential development of the Samsung Galaxy Z Flip 6 interface, is believed to have exfiltrated sensitive design files and deleted critical data before resigning. Appointed by CMMC, forensic expert Mr. Troy Simpson conducted a legally compliant investigation that involved imaging the suspect's hard drive with FTK Imager and analyzing the data using Autopsy. For academic replication, the same procedures were performed using a simulated disk environment at the University of Wales Trinity Saint David. The investigation revealed deliberate file deletions, encrypted archiving, USB and web-based data transfers, and incriminating email exchanges, all of which support the hypothesis of corporate data theft. The report concludes with a timeline reconstruction, legal implications, and actionable recommendations to enhance CMMC's data security posture.

Keywords— *Digital forensics, sabotage, FTK Imager, Autopsy, forensic imaging, data exfiltration, chain of custody, Maya files, corporate espionage, WeTransfer, metadata analysis.*

I. PRE-INVESTIGATION ACTIVITIES AT CMMC HEADQUARTERS

A. Preliminary Investigation

In early 2025, Cyfusion Mobile Manufacturing Company (CMMC), based in London, discovered a severe case of internal sabotage. Rich Daley, a senior GUI designer involved in the development of a highly confidential interface for the upcoming Samsung Galaxy Z Flip 6, unexpectedly resigned from the company. Shortly after his departure, CMMC engineers found that several crucial design files were missing from his workstation. These files, created using Autodesk Maya, represented a substantial portion of the company's R&D investments and were planned for global patent registration and licensing.

CMMC suspects that Daley, suspected to be motivated by personal gain, intentionally deleted or transferred these sensitive assets and struck a deal with a rival company, 360tech.

1) Appointment of a Forensic Expert

Concerned about the financial and strategic impact of the data loss, CMMC's CEO, Ms. Ker Walters, decided to initiate a digital forensic investigation. She appointed Mr. Troy Simpson, a certified CHFI (Computer Hacking Forensic Investigator) and CEH (Certified Ethical Hacker),

to lead the investigation. His role was to retrieve any deleted files, determine whether any data was transferred externally, and gather evidence that could be used in legal proceedings if necessary.

2) Authorization and Legal Basis

A formal internal authorization was issued to Mr. Simpson by the CEO of CMMC. This document granted him full access to the suspect's workstation, network logs, and any other digital assets necessary for the investigation. All actions were conducted under the framework of UK data protection laws and corporate confidentiality policies [1].

3) Objectives of the Investigation

The main objectives of the investigation were defined as follows:

- To identify the method used to sabotage or exfiltrate the design files.
- To recover the deleted or hidden files, especially the Samsung Galaxy Z Flip 6 interface.
- To establish a digital trail linking Rich Daley to the sabotage.
- To preserve all findings in a legally admissible format suitable for court use.
- To assess weaknesses in CMMC's data security infrastructure.

B. Identification and Preservation of Digital Evidence

Upon his arrival at CMMC headquarters, Mr. Simpson began by identifying and preserving all relevant digital evidence related to the suspected sabotage. Rich Daley's workstation had been automatically powered down and physically secured by the IT department immediately after his resignation, which unfortunately prevented the capture of any volatile data from the system's RAM, active network sessions, or temporary logs.

Since no live response was possible, Troy Simpson proceeded directly with the standard post-mortem forensic procedures. The workstation was opened, and the internal hard-drive was carefully unscrewed and removed under anti-static conditions. Mr. Simpson then proceeded to create a forensically sound bit-by-bit image of the entire drive using FTK Imager. This image included all files, deleted data, unallocated space, and system metadata.

For the purpose of this report, the same procedure was replicated using the class computer from the University of Wales Trinity Saint David (UWTSd).

A pre-existing disk image file, named “Windows Evidence 001.dd”, was downloaded from the class OneDrive repository and mounted using OSFMount. A custom file tree was created within the virtual environment to simulate Rich Daley’s workstation, including specific file types such as Autodesk Maya project files and other relevant assets intended to be located during the forensic investigation. The customized disk was then saved and unmounted, representing the emulated version of Rich Daley’s physical hard drive.

Following this setup, the FTK Imager software was launched to begin the analysis, just as Mr. Simpson would have done on his computer during the actual investigation.

A bit-by-bit copy of the disk was created, and the output format was chosen as E01 (the EnCase forensic image format) to ensure data integrity, compression efficiency, and compatibility with industry-standard forensic tools as shown in Figure 1.

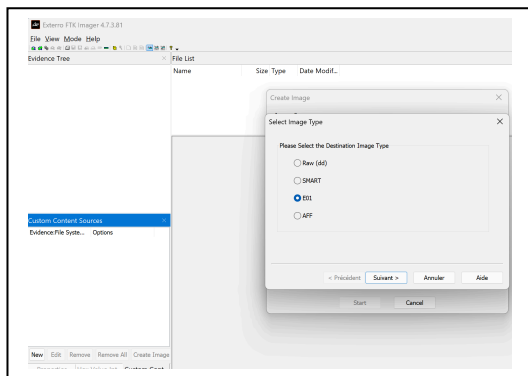


Fig. 1. Screenshot showing the FTK Imager interface and the output format option for the bit-by-bit image of the hard-drive (E01 selected).

After the creation process, its hash value was verified to ensure the data had not been altered during the acquisition process. Hash verification confirms the forensic integrity of the image, as any modification would result in a different hash value, as shown in Figures 2 and 3.

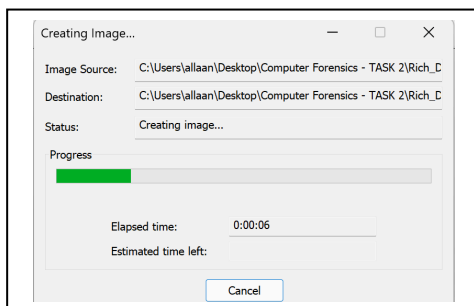


Fig. 2. Screenshot showing the creation of the bit-by-bit copy of the hard-drive.

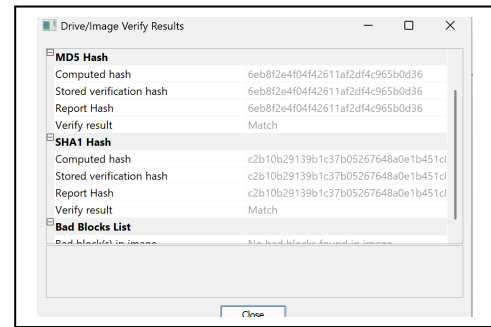


Fig. 3. Screenshot showing the hash verification proceeded by FTK Imager after the disk image was created.

Afterwards, Mr. Simpson proceeded to seal in a static-safe evidence bag the original hard-drive, which was then labelled and documented in the chain of custody log (also attached to this report as an appendix). The workstation itself was also sealed to maintain its original state. All subsequent analysis was performed solely on the forensic image, ensuring the evidential integrity of the original media.

In addition, Mr. Simpson preserved other potential sources of digital evidences, including access logs from shared servers and design repositories, and any email communications along internal chat logs CMMC had regarding Rich Daley.

II. FORENSIC EXAMINATION AND DATA ANALYSIS

Following the successful acquisition of the suspect’s hard drive image, Mr. Simpson left CMMC headquarters and returned to his forensic laboratory with the copy of the original drive. The investigation continued with an in-depth analysis using the Autopsy software, with all procedures performed exclusively on the forensic image to preserve the integrity of the original evidence.

The same steps were replicated in the university environment using the custom disk image previously created for this case study. This emulated scenario was designed to reflect the findings and methodology of Mr. Simpson’s real-world investigation.

A. Setting Up the Analysis Environment

Autopsy was launched and a new case was created, mirroring Mr. Simpson’s process. The disk image file previously created using FTK Imager was loaded into the software via the “Add Data Source” option. The image was mounted in read-only mode to ensure that no data would be altered during the analysis. The case was configured to perform full indexing and keyword pre-processing, as shown in Figure 4 and 5.

All actions undertaken by Mr. Simpson were documented in a forensic journal to maintain the chain of custody and ensure the legal admissibility of the evidence.

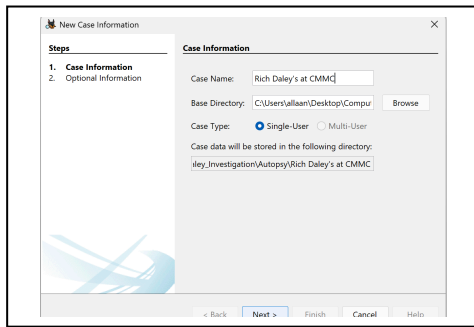


Fig. 4. Screenshot showing the creation of the case in Autopsy.

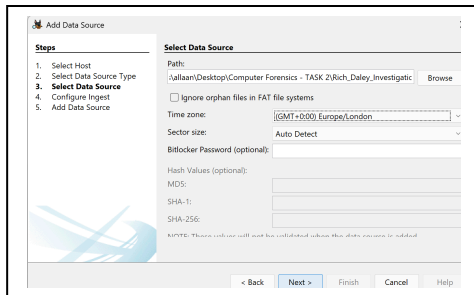


Fig. 5. Screenshot showing the copy of the disk image being added to the case in Autopsy.

B. File System and Directory Structure review in Autopsy

After successfully imaging Rich Daley's workstation, Mr. Simpson began his examination by analysing the overall file system structure. This preliminary examination allowed Mr. Simpson to map out the system architecture and pinpoint critical directories that might contain evidence.

Our replication of this process in the university environment revealed the same findings as we navigated through the directory structure using Autopsy's file browser interface.

Using Autopsy's powerful keyword search functionality, Mr. Simpson efficiently located the relevant Maya files across the disk image. By searching for specific terms like '.ma', (Maya's file extension), 'GalaxyZFlip6', and 'Samsung', he quickly identified all design files related to the project, even those that had been deleted or moved from their original locations.

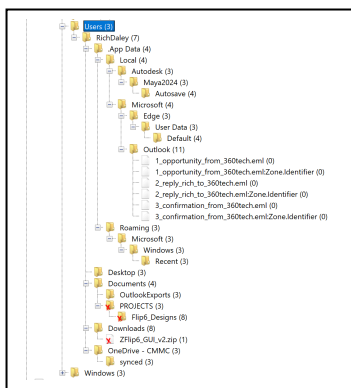


Fig. 6. Screenshot showing Autopsy's navigation tree with the recovered directory structure

The analysis immediately revealed suspicious activity as entire directories had been deliberately deleted from the system. Most notably, the "C:\Users\RichDaley\Documents\PROJECTS\Flip6_Designs\" folder showed evidence of mass deletion, with all Maya project files related to the Samsung Galaxy Z Flip 6 interface removed from their original location. The examination of file system metadata indicated these deletions occurred approximately 47 hours before Rich Daley submitted his resignation.

ns\" folder showed evidence of mass deletion, with all Maya project files related to the Samsung Galaxy Z Flip 6 interface removed from their original location. The examination of file system metadata indicated these deletions occurred approximately 47 hours before Rich Daley submitted his resignation.

/img_Rich_Daley_DISK_COPY.E01/Users/RichDaley/Documents/PROJECTS/Flip6_Designs				
Table	Thumbnail	Summary		
Name	S	C	O	Modified Time
[current folder]				2025-04-07 13:37:10 CEST
[parent folder]				2025-04-07 13:37:10 CEST
GalaxyZFlip6_experimentalUI_20250310_RD.ma				2025-03-27 14:16:38 CET
GalaxyZFlip6_experimentalUI_20250310_RD.ma.Zone.Identifier				2025-03-27 14:16:38 CET
GalaxyZFlip6_foldanim_v3_final_RD.ma				2025-03-27 14:16:38 CET
GalaxyZFlip6_foldanim_v3_final_RD.ma.Zone.Identifier				2025-03-27 14:16:38 CET
GalaxyZFlip6_GUI_v1_20250222_RD.ma				2025-03-27 14:16:38 CET
GalaxyZFlip6_GUI_v1_20250222_RD.ma.Zone.Identifier				2025-03-27 14:16:38 CET

Fig. 7. Screenshot showing deleted Maya project files in Documents folder

Further inspection of the Downloads folder showed equally suspicious activity: recently deleted files including compression utility software (7-Zip), password text files, and a ZIP archive named **ZFlip6_GUI_v2.zip**. These deletions appeared to be part of a systematic attempt to conceal evidence of file exfiltration.

/img_Rich_Daley_DISK_COPY.E01/Users/RichDaley/Downloads				
Table	Thumbnail	Summary		
Name	S	C	O	Modified Time
[current folder]				2025-04-20 12:33:02 CEST
[parent folder]				2025-04-07 13:37:10 CEST
7z2301-x64.exe				2025-04-01 16:54:49 CEST
7z2301-x64.exe.Zone.Identifier				2025-04-01 16:54:49 CEST
passwords.txt				2025-04-01 16:54:49 CEST
passwords.txt.Zone.Identifier				2025-04-01 16:54:49 CEST
ZFlip6_GUI_v2.zip				2025-04-01 16:54:49 CEST
ZFlip6_GUI_v2.zip.Zone.Identifier				2025-04-01 16:54:49 CEST

Fig. 8. Screenshot showing deleted Maya project files in the Download folder

The initial file system examination also uncovered numerous additional artifacts requiring further analysis, including residual email fragments in the Outlook cache, Maya autosave files containing unsaved project versions, system event logs, and web browser history. The subsequent sections of this report will detail how these artifacts were examined to reconstruct a complete timeline of Rich Daley's activities leading up to his resignation.

C. Recovery of Deleted Files and Archives

Following the directory structure analysis, Mr. Simpson focused on recovering the deleted files and analysing archive-related activities on the workstation. Using Autopsy's File Recovery functionality, he was able to reconstruct several deleted Maya project files from unallocated disk space.

The recovered files included initial interface design dated February 22, 2025, experimental interfaces from March 10, and a final animation sequence for the folding mechanism. File metadata confirmed the timeline previously established, showing these items were deleted in the same timeframe as the directory removals.

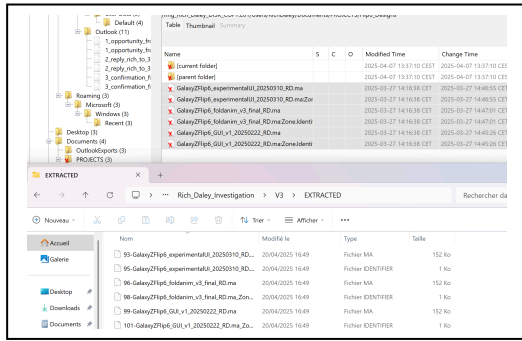


Fig. 9. Screenshot showing recovered Maya files in Autopsy

Further investigation also revealed that Rich Daley had downloaded the 7-Zip compression utility (**7z2301-x64.exe**) one day before the mass deletion occurred. File fragments in slack space indicated he had used this software to create an encrypted archive named **ZFlip6_GUI_v2.zip**. The archive employed AES-256 encryption, as confirmed by its header signature, suggesting a deliberate attempt to secure the files before exfiltration.

A text file named **passwords.txt** found in the Downloads folder contained several complex password strings. Analysis confirmed one of these matched the encryption pattern used for the ZIP archive. This discovery provided strong evidence that Rich Daley had planned the file extraction in advance, creating secure containers for the proprietary data before removing it from CMMC systems. Those files were also recovered afterwards as shown in Figure 10.

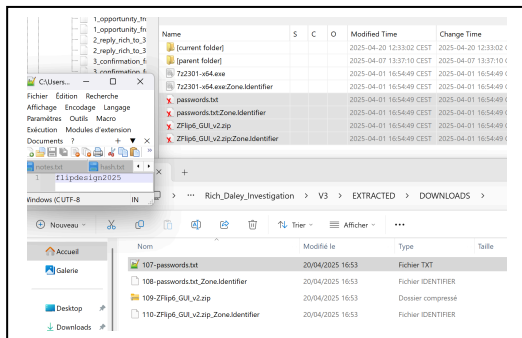


Fig. 10. Screenshot showing recovered files from the Download folder

D. Web Activity and Cloud Transfer Logs

The investigation next examined web browsing history to identify potential external transfer methods. Analysis of Microsoft Edge history logs located at *'C:\Users\RichDaley\AppData\Local\Microsoft\Edge\User Data\Default\Edge History.log'* provided significant evidence of data exfiltration activities.

Mr. Simpson discovered multiple visits to WeTransfer.com in the days preceding Rich Daley's resignation. The browser cache contained partial fragments of the WeTransfer interface showing an upload of a file named **Zflip6_GUI_v2.zip** with a size of approximately 245MB, consistent with compressed Maya project files.

These web activity discoveries provided crucial evidence of external data transfer. When integrated into the developing timeline of events, these activities formed a link between the file deletion and Rich Daley's communication with external parties.

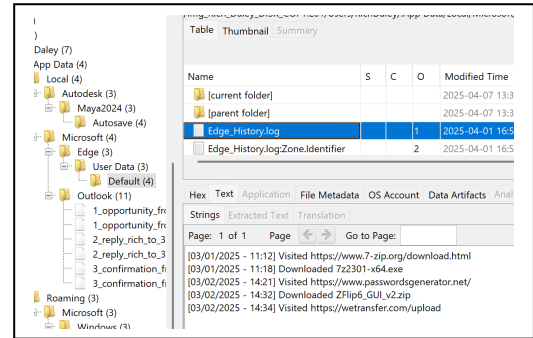


Fig. 11. Screenshot showing the web browsing history with WeTransfer access

E. Email Cache and Communication Review

Afterwards, one of the most compelling pieces of evidence came from the analysis of email communications recovered from the Outlook cache directory. Mr. Simpson extracted several emails from *'C:\Users\RichDaley\AppData\Local\Microsoft\Outlook\'* that established direct communication between Rich Daley and Sébastien Martel from 260tech, CMMC's competitor.

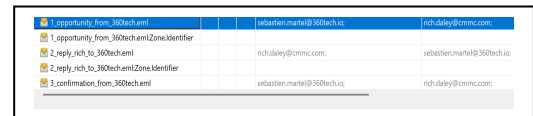


Fig. 12. Screenshot showing the recovered email files in Autopsy

Three key emails were recovered that told most of the story of the conspiracy:

- An initial contact from Sébastien Martel expressing interest in Rich Daley's design work.
- Rich Daley's response confirming his imminent departure from CMMC and offering to send design samples.
- Martel's confirmation accepting the offer and requesting the files before an internal design review.

The timeline of these communications perfectly matched the pattern of file archiving and web transfer activities identified elsewhere on the system.

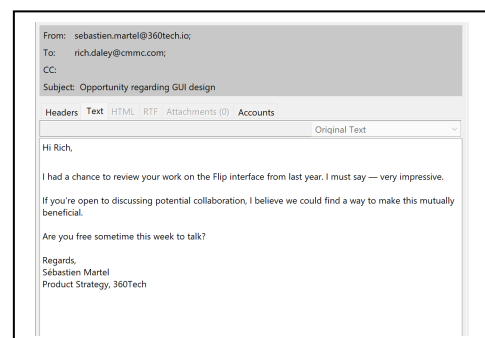


Fig. 13. Screenshot showing the first recovered email

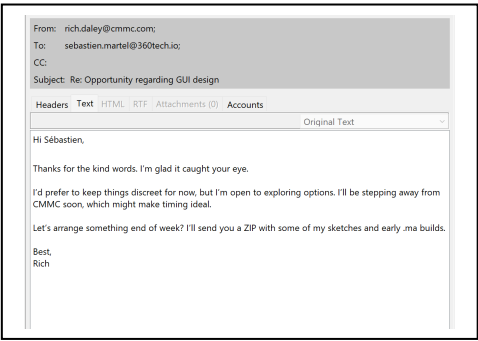


Fig. 14. Screenshot showing the second recovered email

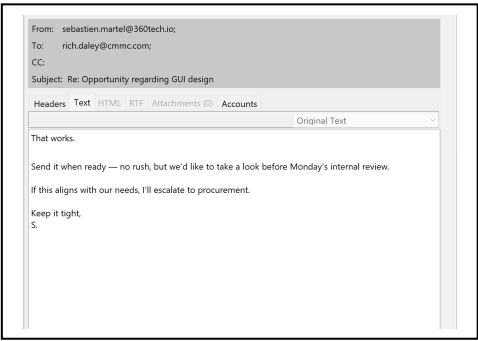


Fig. 15. Screenshot showing the third recovered email

The language used in these communications showed awareness of impropriety, with explicit requests to maintain discretion and references to proprietary design concepts.

F. USB Device Usage Analysis

The final component of Mr. Simpson’s technical analysis focused on external device usage. System logs, particularly the **setupapi.dev.log** file, contained detailed records of USB device connections that provided additional evidence of data exfiltration.

Analysis revealed that an 8GB SanDisk USB flash drive had been connected to Rich Daley’s workstation three days before his resignation. The connection timestamp aligned precisely with the creation time of the **Zflip6_GUI_v2.zip** archive, suggesting that the USB drive was used as a physical backup method for the stolen files.

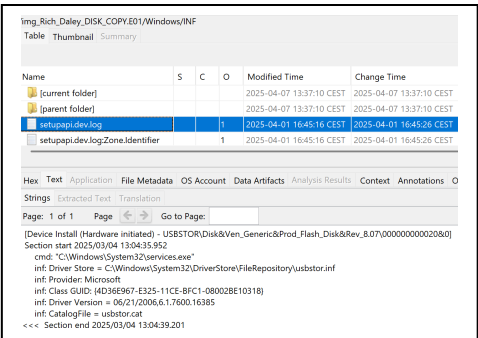


Fig. 16. Screenshot showing the USB device connection logs

III. FINDINGS AND CONCLUSIONS

A. Summary of Key Findings

The forensic investigation revealed clear evidence of intentional data exfiltration and sabotage by Rich Daley prior to his resignation at CMMC. The main findings are summarised as follows:

- Multiple Autodesk Maya project files related to the Samsung Galaxy Z Flip 6 were recovered from the suspect's workstation despite being deliberately deleted.
- Evidence of 7-Zip compression software usage and password-protected archives was discovered.
- Web browsing artifacts confirmed file transfers via WeTransfer.com.
- Email correspondence with a competitor (360tech) was recovered from Outlook cache.
- System logs documented USB storage device connections and file transfers.
- A clear timeline of activities was established spanning the week before Rich Daley's resignation.

B. Attribution and Intent

The evidence found on Rich Daley's workstation clearly shows that his actions were intentional and not due to negligence. All traces point to a deliberate attempt to steal CMMC's confidential design files and share them with a competitor, 360tech.

The timeline is consistent: a few days before his resignation, Rich Daley connected a USB device to save the files for himself just in case, he used the software 7-Zip to compress the files and to create a password-protected archive. He then uploaded the encrypted archive to WeTransfer, sending the files to an external recipient. Right after completing these transfers, he deleted the contents of his "Documents" and "Downloads" folders in an attempt to cover his tracks. The files involved were Autodesk Maya projects linked to the Samsung Galaxy Z Flip 6 interface.

Even more revealing were the emails recovered from the Outlook cache. The conversation with Sébastien Martel from 360tech confirmed a clear agreement between them. Martel offered to discuss a collaboration and complimented Daley's past work. Daley responded that he was about to leave CMMC and offered to send a ZIP file containing his sketches and early .ma builds. He even asked to "keep things discreet," which shows that he knew he was not acting within legal or ethical limits. Martel then replied to confirm and encouraged him to send the files before their internal review.

When putting the email discussion and system activity together, the pattern is visible: Rich Daley copied CMMC’s internal files, archived them securely, sent them using WeTransfer, and erased the traces. The tone of the emails and the steps taken support the conclusion that Rich Daley acted with full awareness of what he was doing, and why.

C. Legal and Operational Impact

To ensure the evidence could be used in legal proceedings, the entire forensic process followed standard procedures and respected legal best practices as shown earlier in this report. A full bit-by-bit image of the original hard drive was created using FTK Imager, and its integrity was verified using both MD5 and SHA-1 hash values. All analysis was performed exclusively on the forensic image to avoid any modification of the original evidence. Additionally, a chain of custody was maintained and documented from the moment the hard drive was extracted to the end of the investigation.

From a legal point of view, the actions of Rich Daley may fall under several UK laws:

- **The Data Protection Act 2018 (DPA 2018):** By copying and sending confidential design files outside of CMMC without consent, Rich Daley may have unlawfully processed personal or sensitive data. Under this law, organisations can be fined up to £17.5 million or 4% of global turnover. While this case targets an individual, the misuse still constitutes a serious offence under UK data protection principles.
- **The Computer Misuse Act 1990:** This law prohibits unauthorized access to computer systems and data. Daley's actions, by accessing, copying and deleting sensitive files without authorization are potentially punishable under:
 - *Section 1*, which covers basic unauthorized access (up to 2 years in prison)
 - *And Section 2*, which addresses unauthorized access with intent to commit further offences (up to 5 years in prison).
- **The Copyright, Designs and Patents Act 1988:** The Maya projects files and related assets may be considered intellectual property owned by CMMC. Distributing or disclosing these assets without permission can be considered copyright infringement. The maximum penalty can reach 10 years of imprisonment and/or an unlimited fine.

In addition, Rich Daley likely violated internal confidentiality agreements outlined in his employment contract. The combination of emails, file activity, and system logs forms a strong and legally admissible body of evidence supporting both civil and criminal liability.

Furthermore, the email exchange with 360tech raises concerns that the competitor knowingly received confidential materials. **Under the Trade Secrets (Enforcement, etc.) Regulations 2018**, this could be grounds for legal action. If proven, CMMC could request an injunction to stop 360tech from using the data and claim financial compensation.

However, for such action to be pursued, a separate investigation would need to be initiated by CMMC. At this stage, Mr. Troy Simpson is not authorised to conduct any analysis involving external systems or third-party

infrastructure unless a new cyber investigation is officially opened with proper legal support and cooperation.

IV. SECURITY RECOMMENDATIONS FOR CMMC

Based on the findings of this investigation, Mr. Simpson provided CMMC with comprehensive security recommendations to prevent similar incidents in the future:

A. Technical Recommendations

Implementation of a Data Loss Prevention (DLP) system would enable monitoring and blocking unauthorized file transfers. Role-based access control should restrict access to design files to only authorized personnel. USB port restrictions and monitoring software would prevent physical data exfiltration. Network monitoring would help detect transfers to external platforms like WeTransfer, while regular automated backups would safeguard critical files from deliberate deletion.

B. Organizational Measures

CMMC should establish a security awareness program focused on intellectual property protection. A formal incident response plan for data theft scenarios would improve reaction time. Strengthened employee offboarding procedures should include immediate access revocation and device inspection. Regular security audits and penetration testing should target data exfiltration vectors to identify vulnerabilities proactively.

C. Policy-Level Suggestions

A comprehensive intellectual property policy should classify design files and establish handling procedures. Employee agreements (non-disclosure, non-compete) should explicitly address digital assets with clear violation consequences. Vendor security requirements should be formalized for any external entities accessing CMMC designs. Finally, strict policies should govern remote work and personal device usage when handling proprietary information.

These measures, implemented together, would significantly improve CMMC's defence against insider threats and intellectual property theft.

V. CONCLUSION

In conclusion, the forensic investigation conducted by Mr. Troy Simpson successfully recovered the deleted design files and established clear evidence of intentional data exfiltration by Rich Daley. The recovered Maya project files can now be restored to CMMC's design repository, while the detailed forensic findings provide legally admissible evidence should the company decide to pursue legal action. This case highlights the critical importance of implementing robust security measures to protect valuable intellectual property in today's competitive business environment.

REFERENCES

- [1] EC-Council, “CHFI Computer Hacking Forensiv Investigator”, Official Courseware, 2021.

APPENDIX

- [1] Invoice from Troy Simpson to CMMC
- [2] Complete Autopsy Forensic Report
- [3] Chain of Custody Documentation Log