

Evaluation of Computer Forensics Tools

- ACCD5000 -

Sarah LEVY - 2422988
 University of Wales Trinity Saint David
 Swansea, Wales
 2422988@student.uwtsd.ac.uk

Abstract - This research examines and compares three of the most widely used computer forensic tools: EnCase Forensic, Forensic Toolkit (FTK), and Autopsy. The study compares their features, strengths, and weaknesses to understand how they help investigators collect and analyze digital evidence. The results show that each tool has different advantages. This comparison helps forensics investigators choose the right tool for different types of digital investigations. While forensics tools continue to change and evolve, the basic concepts and methods of digital forensics stay constant.

Keywords – Computer Forensics, EnCase, FTK, Autopsy, evidence acquisition, data recovery, forensic analysis, disk imaging, chain of custody.

I. INTRODUCTION

Digital forensics uses special software to collect, analyze, and protect digital evidence in a reliable way. Among the different tools available, some are widely known and often used by professional investigators. As digital data grows and cybercrime increases, it is important to have strong forensic software to examine computers, networks, and mobile devices. There are many tools available to meet this need, some are paid, and others are free. **EnCase Forensics**, **Forensic Toolkit (FTK)**, and **Autopsy** are three of the most popular tools in this field. They are known for following legal standards and being trusted by professionals, including certifications like CHFI (Computer Hacking Forensic Investigator) and CEH (Certified Ethical Hacker). The next sections will describe these tools and provide a comparison table showing their main features.

II. ENCASE FORENSIC

A. History and use :

EnCase is a digital forensic software originally developed by Shawn McCreight, CEO of *Guidance Software* in 1998 and later bought by *OpenText* in 2017. Since it was made, it has become one of the most important tools for computer forensics [1].

EnCase only works on Windows computers but it can still look at files from other systems (like macOS or Linux) by examining them through Windows. The program makes special copies of evidence (called E01 or Expert Witness format) that preserve everything exactly as it was [1]. It has a complete set of tools

including file browsers, search tools, and ways to create reports. Users need to plug in a special security device (called a hardware dongle) to use the software, which helps control who can use it.

B. Strengths :

EnCase is considered one of the best tools in digital forensics. It can work with many different types of file systems (like FAT, NTFS, Ext2/3/4, HFS+) and can even examine files from iPhones and iPads. One of its best features is how well it can search through files. It supports advanced search functionalities including Boolean operators, fuzzy logic, and contextual keyword analysis [2, p. 55], allowing investigators to conduct targeted and nuanced queries even in large datasets.

The software has its own programming language called EnScript (like Java or C++) that lets users create custom tools and automate repetitive tasks. EnCase also has special versions (EnCase Enterprise, eDiscovery) that can do things like collect evidence from computers over a network or process large amounts of data using multiple computers at once [2, p.61]

EnCase has been used in many famous court cases, and court have accepted its evidence format (E01 files) for over 20 years. Evidence found using EnCase has helped solve major cases (like the BTK killer case and Casey Anthony case). Because it's so well-respected, evidence from EnCase is rarely questioned in court, which gives investigators more confidence.

C. Weaknesses :

EnCase has few problems. First, it costs a lot of money (e.g., "version 3 cost approximately \$1,995 for government and educational agencies and \$2,495 for private-sector companies") [1], which makes it hard for smaller companies to afford. Also, it's not easy to learn as the software has many features and buttons that can be confusing at first. The program doesn't automatically prepare files for searching, which can make some searches slower. Finally EnCase only works on Windows computers, so you can't use it directly on Mac or Linux systems.

III. FORENSIC TOOLKIT

A. History and use:

Forensics Toolkit (FTK) is a digital forensics software approved for use in courts, created by AccessData in 2000. Over the years, it has grown to become one of the most complete tools for digital investigations available today. FTK was made specifically to help investigators examine electronic evidence thoroughly and in a way that can stand up in court. With FTK, investigators can look at, extract, analyze and create reports about digital evidence while making sure the original data stays unchanged throughout the investigation [4].

B. Strengths:

FTK has several important advantages. First, it is very good at recovering data, helping investigators find deleted files, hidden data, and information in unused parts of storage devices. It has powerful filtering tools that make it easy to find specific types of files or patterns in large collections of data [3].

FTK is also excellent at indexing (organizing) data, which makes searching for text very fast and efficient across entire hard drives. Another big advantage is its built-in password cracking tool (called PRTK) that can break passwords from more than 280 different programs and file types [3].

The software keeps detailed records of everything done during an investigation, which maintains a complete chain of custody that is important for court cases. Finally, FTK can use multiple computers at the same time to analyze evidence faster, which is very helpful when working with large amounts of data.

C. Weaknesses:

Despite its strengths, FTK does have some limitations. The software needs a lot of computer power, especially for processing large amounts of data, which can make it hardware-intensive and potentially expensive for smaller companies that might need to buy better computers. Some users find that the interface, while full of features, is harder to learn compared to other forensic tools.

Also, FTK licenses can be expensive, especially if you want all the features. Finally, while powerful, the software can sometimes be slow when handling very large collections of data, particularly during the first phase when it's processing everything.

B. Strengths:

Autopsy has several advantages, especially that it's completely free to use. Despite costing nothing, it offers many of the same features as paid tools, including ways to analyze file systems, search for specific words, examine Windows registry data, and create timelines of computer activity.

Autopsy is built with modules that can be added or changed, allowing users to customize it and add new features through plugins created by the community. The program also allows multiple investigators to work on the same case at the same time [5].

Another big advantage is that Autopsy works on different computer types: Windows, Linux and Mac, giving investigators more flexibility in their work environment. Its user-friendly design makes it easy for both beginners and experienced forensic analysts to learn and use, with a shorter learning time compared to many paid alternatives.

C. Weaknesses:

Autopsy does have some limitations compared to commercial tools. When users have technical problems, they can't call a support hotline like with paid software, instead, they must rely on community forums and online help. Some specialized features found in expensive tools might be missing entirely or not as well-developed in Autopsy.

Autopsy can be slower than commercial tools when processing very large amounts of data. Finally, while it's becoming more accepted, Autopsy isn't as widely used in courts as EnCase. Judges and lawyers might be less familiar with it and more likely to trust results from well-known commercial tools they've seen before. This sometimes means investigators must do extra work to show that Autopsy's findings are just as reliable as those from more expensive programs.

Recent evaluations have acknowledged Autopsy's progress in enterprise-level forensics. According to J. Maras and Easttom (2022), "Autopsy has matured significantly through community-driven enhancements, enabling reliable evidence analysis in both civil and criminal contexts." However, legal acceptance still lags behind commercial tools, and court familiarity remains a barrier to widespread adoption [1].

V. COMPARISON OF TOOLS

TABLE I. COMPARISON TABLE

Feature / Aspects	EnCase Forensic	Forensic Toolkit (FTK)	Autopsy
Status / License	Commercial	Commercial	Open source
Cost	High (commercial)	High (commercial)	Free (Open source)
Operating system support	Windows only	Windows only	Windows, Linux, macOS
Evidence Format	E01 (Expert Witness)	AD1	Multiple formats
User Interface	Complex	Comprehensive	intuitive

IV. AUTOPSY

A. History and use:

Autopsy is a free, open-source digital forensics program created by Brian Carrier in 2000 as the visual interface for The Sleuth Kit. Unlike paid alternatives, Autopsy cost nothing and is improved by a community of volunteer developers. It was designed to be easy to use while still offering complete digital forensics capabilities for police, military, and business investigators. Autopsy stands out because it's one of the few comprehensive free options in a field where most good tools cost a lot of money [5, p. 59].

Processing speed	Good	Excellent	Moderate
Memory Requirements	Moderate	High	Low to moderate
Court acceptance	Extensive (industry standard)	Well-established	Growing but less precedent
Technical Support	Commercial support available	Commercial support available	Community forums
Best suited for	Legal/court investigations	Corporate incident response	Education/quick triage

VI. CONCLUSION

The comparative evaluation of EnCase Forensic, Forensic Toolkit and Autopsy demonstrates that while the tools in computer forensics evolve continuously, the fundamental concepts and methodologies remain consistent. Each tool offers unique advantages and has specific limitations that make it more suitable for investigation scenarios.

For important court cases where evidence must be easily accepted by judges, paid tools like Encase and FTK are better choices because courts are familiar with them. For smaller companies, teaching purposes, or first looks at evidence, Autopsy works well and saves money while still providing basic features.

When choosing which forensic tool to use, you should think about what your case needs, what kind of digital evidence you're looking at, what your team knows how to use, how much money you can spend, and how closely your evidence might be questioned in court.

As hackers create new threats and new devices appear in the markets, forensic tools will keep changing and getting better. However as noted in the introduction, while tools may change, the basic ideas of digital forensics will stay the same: keeping evidence safe, following the correct steps, and making sure your results can be trusted.

REFERENCES

- [1] C. Hoyland, "EnCase software preserves evidence on seized computer hard drives," *Business First*, vol. 18, (19), 2001.
- [2] B. E. Hermansen, "An Evaluation of Forensic Tools for Linux : Emphasizing EnCase and PyFlag," 2010.
- [3] Anonymous "Access Data: Forensic Tool Kit (FTK)," *SC Magazine*, vol. 28, (5), pp. 32, 2017.
- [4] "AccessData group forensic toolkit (FTK) v4," *SC magazine*, vol. 23, no. 5. Haymarket Media, Inc, New York, pp. 61-, 2012.
- [5] 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.
- [6] J. Maras and R. Easttom, *Digital Forensics: Threatscape and Best Practices* Pearson, 2022.

Digital Forensic Investigation at CMMC by Troy Simpson

- ACCD5000 -

Sarah LEVY - 2422988
University of Wales Trinity Saint David
 Swansea, Wales
 2422988@student.uwtsd.ac.uk

Abstract - This report documents a digital forensic investigation conducted at Cyfusion Mobile Manufacturing Company (CMMC) following the suspicious departure of a key employee. Using standard forensic tools and procedures, the analysis focused on recovering deleted files, tracing potential data exfiltration methods, and assessing compliance with UK legal standards. The report outlines the investigative process, key findings, and recommendations to improve organizational data security.

Keywords – *Digital forensic, data exfiltration, FTK Imager, Autopsy, forensic imaging, intellectual property theft, chain of custody, USB artifacts, encrypted archives, UK Computer Misuse Act.*

I. INVESTIGATION AT CMMC HEADQUARTERS

A. Case Preparation

1) Context

Following the sudden resignation of Rich Daley, a senior interface designer at Cyfusion Mobile Manufacturing Company (CMMC), several key design files related to the upcoming Samsung Galaxy Z Flip 6 project were reported missing or deleted from the company's internal systems. The incident raised internal suspicion of deliberate sabotage or intellectual property theft.

Upon discovery of the anomaly by the CMMC engineering team, the case was escalated to senior management. An initial internal audit indicated possible unauthorized data exfiltration. In response, the CEO of CMMC authorized the initiation of a formal forensic investigation to establish the facts, identify any malicious activity and recover critical assets. The CEO officially referred the case to Mr Troy Simpson, a certified digital forensics investigator. Mr. Simpson was tasked with conducting a formal investigation to determine whether data had been maliciously exfiltrated or destroyed, and to recover any potential digital evidence.

As part of this process, the workstation previously used by Rich Daley was secured and assigned as primary evidence. Access to the device was restricted, and the internal IT department transferred custody to the digital forensics team. A chain-of-custody document was initiated at the point of collection detailing the device's serial

number, collection date, storage location and individuals involved in the evidence handover [1].

2) Authorizations and Legal

The investigation was carried out under internal authorization in accordance with CMMC's information security and employee conduct policies. All procedures followed the UK's legal requirement, particularly the *Computer Misuse Act 1990* and the *Data Protection Act 2018*, ensuring that digital evidence collection respected both criminal law standards and privacy obligations. The forensic investigator followed the ACPO guidelines (now under NPCC) for handling digital evidence, ensuring that all evidence remained intact, traceable, and valid for court proceedings.

3) Documenting the crimescene

Before the start of the technical investigation, Mr. Simpson was briefed by the CMMC's IT and engineering leads regarding the nature of the incident.

When he arrived, Mr. Simpson performed a preliminary visual inspection to verify that no physical tampering had occurred. At the time of recovery, the workstation was already powered off. While a live acquisition would have allowed recovery of volatile data such as running processes, network connections, and in-memory artifacts, the opportunity had passed. In accordance with forensics best practices, the device was left unpowered to avoid any alteration of persistent data on the disk. The investigation proceeded in post-mortem mode, focusing on non-volatile artifacts such as deleted files, system logs, internet history and metadata.

Mr. Simpson conducted the forensic acquisition on-site at CMMC's headquarters using a validated write blocker and FTK imager. He created a bit for bit forensic image of the suspect's hard drive onto a forensically wiped external drive. This ensured that the original device remained untouched and available for future reference if required.

B. Preservation of Digital Evidences

For this report, the same steps taken by Mr. Simpson were replicated on the class computer in the University of Wales Saint David (UWTSD). A new virtual disk image was created using a pre-existent one from the class's OneDrive folder, and using the OSFMount software, the disk image was mounted and edited to contain the files related to this case scenario. A folder structure was created mimicking a real file tree structure of a Windows computer alongside folders containing files from Maya Desktop and other applications such as emails leftovers or web browser history.

1) Copy to a Forensically Wiped Hard Drive

Using the FTK Imager software, Mr. Simpson performed a bit-for-bit (sector level) acquisition of the entire suspect drive. The acquisition was configured to generate both E01 format (for long term archival) and a raw DD format (for tool compatibility).

This step was done on the school computer like shown below.

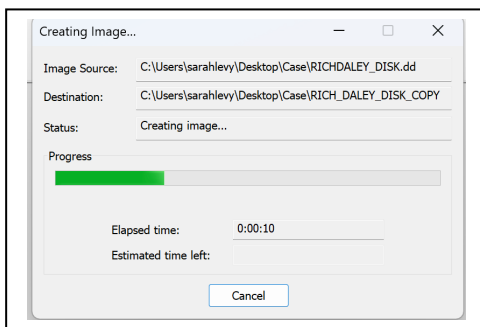


Fig. 1. Screenshot showing the disk imaging process by FTK Imager

2) Verifying hashes and CRC

To ensure the bit-by-bit copy was properly made and without any loss, it's necessary to validate the hashes (such as MD5 or SHA-1) using protocols like CRC. This step was automatically done by the software, instead of doing it manually.

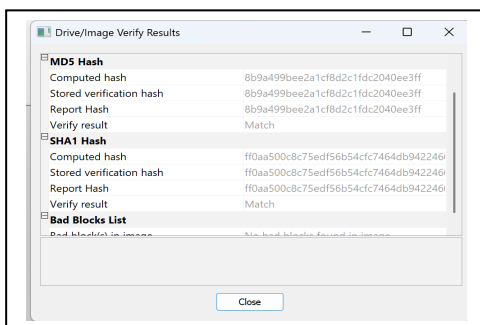


Fig. 2. Screenshot showing the hash verification by FTK Imager

Once the acquisition process was complete and the hash values were verified to confirm the integrity of the copy, Mr. Simpson transported the forensic image to his private laboratory for further analysis. The original

workstation remained secured on site under CMMC's custody.

All imaging steps were documented, including tools version, hash calculation and chain of custody updates. The operation complied with UK forensic standards and followed the ACPO/NPCC guidelines for evidence preservation and met the standards defined in BS ISO/IEC 27037:2012.

II. EXAMINATION OF GATHERED EVIDENCES

A. Creating the Working Environment

After the forensic image was acquired and confirmed to be authentic through MD5 and SHA-1 verification, Mr. Troy Simpson prepared a secure and isolated analysis environment. Once the image was imported into Autopsy, a recognized forensic investigation suite the key ingestion modules were activated to enable the recovery of deleted files, analysis of browser history, extraction of e-mail caches, and generation of user activity timelines.

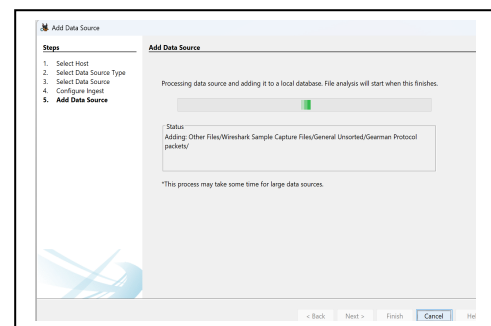


Fig. 3. Screenshot showing the case creation in Autopsy

B. Hard Drive Analysis

Afterwards, the first stage of analysis consisted in examining the file system of Rich Daley's workstation. By the use of Autopsy's keyword search, it was possible to easily identify the wanted files in the system. Therefor, Mr. Simpson navigated to the "C:\Users\RichDaley\Documents\PROJECTS\" directory, where he identified a deleted folder titled Flip6_Designs. Although no longer visible to the operating system, the folder and its internal structure were recovered through metadata still present on the disk. The contents of the folder included several .ma files associated with Autodesk Maya, which matching the naming conventions of the confidential interface design files for the Galaxy Z Flip 6 prototype.

Timestamp recovered from these files indicated they had been created, modified, and deleted within a short timeframe prior to Rich Daley's departure of CMMC. In particular, the final deletion occurred less than 48 hours before resignation.

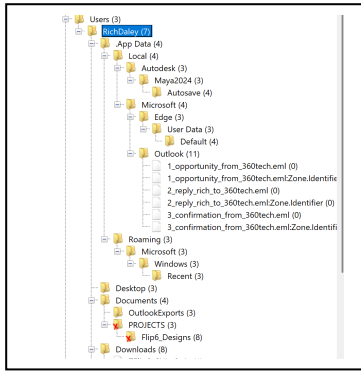


Fig. 4. Screenshot showing the tree structure of the disk image

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	File
[current folder]				2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	48	Un
[parent folder]				2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	48	Un
Galaxy2Flip6_experimental_20250310_R0.ma				2025-03-27 14:16:38 CEST	2025-03-27 14:16:38 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	155386	Un
Galaxy2Flip6_experimental_20250310_R0.ma.z0r				2025-03-27 14:16:38 CEST	2025-03-27 14:16:38 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	88	Un
Galaxy2Flip6_kidanim_v3_final_R0.ma				2025-03-27 14:16:38 CEST	2025-03-27 14:16:38 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	155386	Un
Galaxy2Flip6_kidanim_v3_final_R0.ma.z0r				2025-03-27 14:16:38 CEST	2025-03-27 14:16:38 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	88	Un
Galaxy2Flip6_GUI_v1_20250202_R0.ma				2025-03-27 14:16:38 CEST	2025-03-27 14:16:38 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	155386	Un
Galaxy2Flip6_GUI_v1_20250202_R0.ma.z0r				2025-03-27 14:16:38 CEST	2025-03-27 14:16:38 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	88	Un

Fig. 5. Screenshot showing the PROJECTS folder with the deleted .ma files

Additional files were identified in the Download folder of the suspect machine, containing text files, ZIP archive, compression utility software... They will be examined in the following sections of this report.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	File
[current folder]				2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	160	Allocated
[parent folder]				2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	2025-04-07 13:37:10 CEST	160	Allocated
7z2020-64.exe				2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	40	Allocated
7z2020-64.exe.Zone.Identifier				2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	40	Allocated
passwords.txt				2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	14	Unallocated
passwords.txt.Zone.Identifier				2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	95	Unallocated
ZFlip6_GUI_v2.zip				2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	2025-04-01 16:54:49 CEST	182	Unallocated

Fig. 6. Screenshot showing the Download folder with the deleted files

C. File Recovery

Using the recovery modules in Autopsy, Mr. Troy Simpson identified and restored several deleted items from the unallocated space of the drive. Among these were earlier versions of .ma files as well as a compressed archive named Zflip6_GUI_v2.zip. This ZIP archive appeared in a directory related to recent downloads, accompanied by a plaintext file named passwords.txt and an executable installer for 7-Zip.

Upon further inspection, the archive was confirmed to be encrypted with AES-256. Analysis of the passwords.txt file showed that one of the stored passwords matched the archive's decryption pattern, allowing access to its contents. This archive appeared to contain copies of the lost .ma files that were also discovered and recovered from the Document folder.

Name	Modified Time	Size	Type	File
Galaxy2Flip6_experimental_20250310_R0...	2025-03-27 14:16:38	155,386	File	MA
Galaxy2Flip6_experimental_20250310_R0...	2025-03-27 14:16:38	88	File	MA
Galaxy2Flip6_kidanim_v3_final_R0.ma	2025-03-27 14:16:38	155,386	File	MA
Galaxy2Flip6_kidanim_v3_final_R0.ma.z0r	2025-03-27 14:16:38	88	File	MA
Galaxy2Flip6_GUI_v1_20250202_R0.ma	2025-03-27 14:16:38	155,386	File	MA
Galaxy2Flip6_GUI_v1_20250202_R0.ma.z0r	2025-03-27 14:16:38	88	File	MA

Fig. 7. Screenshot showing the recovered .ma files

D. USB Activity

The forensic analysis of system logs revealed a notable USB storage event that occurred on March 4th, 2025 at 13:04. The Windows *setupapi.dev.log* file documented the installation of a generic flash drive under the path: `USB\TORDisk&Ven_Generic&Prod_Flash_Disk&Rev_8.07\000000000020&0`.

This indicates that an external storage device was connected on Rich Daley's workstation. The presence of this USB device installation was logged along with relevant driver and catalog information, indicating that this was a newly connected and configured device.

```
[Device Install (Hardware initiated)] - USBSTOR\Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07\000000000020&0
Section start 2025/03/04 13:04:35.952
cmd: "C:\Windows\System32\services.exe"
inf: Driver Store = C:\Windows\System32\DriverStore\FileRepository\usbstor.inf
inf: Provider: Microsoft
inf: Class GUID: {4D36E967-E325-11CE-BFC1-08002BE10318}
inf: Driver Version = 06/21/2006.6.1.7600.16385
inf: CatalogFile = usbstor.cat
<<< Section end 2025/03/04 13:04:39.201
```

Fig. 8. Screenshot showing USB storage device installation log on 04/03/2025

E. Web Activity

Mr. Simpson extended his analysis to browser history and cached web sessions stored in the Edge browser profile directory. The investigation revealed a sequence of visits to *wetransfer.com* around the same period as the file deletions. Cached upload metadata confirmed that the file *ZFlip6_GUI_v2.zip* had been uploaded through the *WeTransfer* platform shortly before the resignation.

The date and time of the upload aligned precisely with the file deletion discovered earlier. No browsing activity suggested research or data retrieval.

Page	Time	URL	Size	File
1	03/01/2025 - 11:12	Visited https://www.7-zip.org/download.html	11,118	HTML
2	03/01/2025 - 11:18	Downloaded 7z2021-64.exe	40	EXE
3	03/02/2025 - 14:21	Visited https://www.passwordgenerator.net/	1,821	HTML
4	03/02/2025 - 14:32	Downloaded ZFlip6_GUI_v2.zip	182	ZIP
5	03/02/2025 - 14:34	Visited https://wetransfer.com/upload	1,821	HTML

Fig. 9. Screenshot showing browser history entries related to WeTransfer.

F. Email Cache

Finally, Mr. Simpson examined the Outlook *.ost* file retrieved from suspect's user profile. This file contained local copies of email communications, some of which were not yet synchronised with the server. Among them were messages exchanged between the suspect and a contact from a competing company named 360tech.

In one message, the suspect responded to a request from "Sébastien Martel" by indicating he would prefer to "keep things discreet for now". He even sent shortly afterwards of

a ZIP with some of his sketches and *.ma* builds via WeTransfer as indicated in the email.

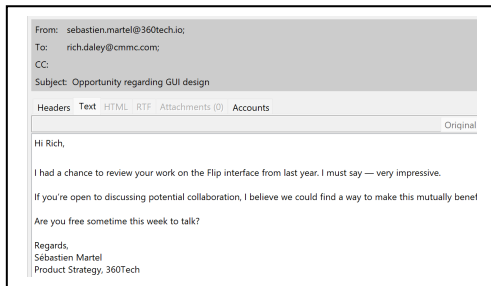


Fig. 10. Screenshot of the first message sent by Sébastien Martel

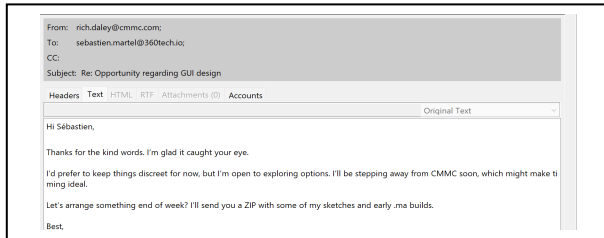


Fig. 11. Screenshot of the response by Rich to Sébastien

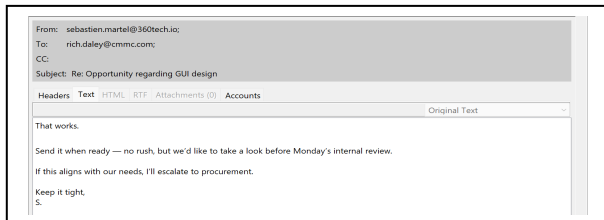


Fig. 12. Screenshot of the last message sent by Sébastien Martel

III. EVENT RECONSTRUCTION

A. Summary of all the Findings

Troy Simpson's investigation found strong evidence that Richard Daley took confidential design files before leaving CMMC. Mr. Simpson discovered deleted Flip 6 project files, an encrypted ZIP archive, and records showing file transfers through WeTransfer. He also found password files, download logs, and email to someone at competitor 360tech.

The evidence collected includes:

- Deleted Maya (.ma) files related to the Galaxy Z Flip 6 Project.
- An encrypted ZIP archive named "Zflip6_GUI_v2.zip" containing copies of the deleted files.
- A text file containing passwords, one of which matched the encryption for the ZIP archive.
- Evidence of 7-Zip compression software installation.
- System logs showing USB storage device connection on March 4th, 2025.
- Browser history showing visits to wetransfer.com and file uploads.

- Email communications between Rich Daley and Sébastien Martel from 360tech discussing file transfers.

B. Timeline of Events

Looking at everything we found during our investigation, here's how things unfolded:

TABLE II. TIMELINE OF EVENT

Date	Time	Event
01/03/2025	11:12	Suspect visited 7-zip.org : preparing to install compression tools
01/03/2025	11:18	Downloaded 7z2301-x64.exe installer for 7-Zip.
02/03/2025	14:21	Visited passwordsgenerator.net : likely used to generate encryption credential
02/03/2025	14:32	Created Zflip6_GUI_v2.zip : encrypted archive created
02/03/2025	14:34	Accessed wetransfer.com/upload : Zip file transmitted externally
04/03/2025	13:04	USB device connected : possible attempt to exfiltrate or store evidence offline
27/03/2025	14:16	Last known modification of GalaxyZFlip6_foldanim_backupD.ma
01/04/2025	16:43	Final file deletion and last recorded system interaction

The forensic analysis finally reveals a calculated sequence of actions by Rich Daley that demonstrates deliberate misappropriation of CMMC's intellectual property. The recovered email evidence shows that the entire operation was initiated when Sébastien Martel from 360tech reached out to Daley on his work email with a seemingly innocent subject line "Opportunity regarding GUI design.". In this initial contact, Martel strategically complimented Daley's previous work on the Flip interface, writing "I had a chance to review your work on the Flip interface from last year. I must say — very impressive," before suggesting a "mutually beneficial" collaboration.

Daley's response reveals both his receptiveness to the approach and his awareness of wrongdoing, stating he would "prefer to keep things discreet for now" and explicitly mentioning his imminent departure from CMMC. Most significantly, he volunteered to send confidential materials, writing "I'll send you a ZIP with some of my sketched and early .ma builds," clearly indicating intent to transfer proprietary files. Martel's final response demonstrates 360tech's eagerness to obtain CMMC's design files before their own design review, suggesting corporate espionage rather than legitimate recruitment.

Following this email exchange, Daley methodically executed his plan between March 1-4, 2025. He first acquired the necessary tools by downloading 7-Zip compression software, then visited a password generator website to create secure credentials for encrypting the files. Within 24 hours, he had packaged the confidential Maya files into an encrypted archive (ZFlip6_GUI_v2.zip) and

uploaded it to WeTransfer, precisely as promised in his email. As a contingency measure, he also connected a USB device to create a physical backup of the stolen files. In the final stage of his operation, Daley systematically deleted all evidence from his workstation before submitting his resignation.

This comprehensive forensic timeline reveals not merely opportunistic data theft, but a calculated conspiracy between an employee and a competitor to misappropriate valuable intellectual property. The explicit language in the emails, combined with the precise technical steps taken to secure and transfer the files, demonstrates clear intent and awareness of wrongdoing by both parties.

IV. DOCUMENTATION

A. Attribution and Intent

The forensic analysis establishes Rich Daley's culpability through multiple converging evidence streams. His actions show technical sophistication in selecting valuable intellectual property, implementing secure transfer methods, and attempting to conceal digital traces. The timing of preparations, nearly a month before resignation, also demonstrates calculated premeditation rather than impulsive behavior. The evidence confirms Daley targeted specifically valuable Samsung Z Flip 6 designs rather than collecting random data, and his communications with 360tech revealed awareness of impropriety through explicit requests for discretion. These elements collectively establish knowing and deliberate misappropriation of CMMC's protected intellectual assets for potential competitive advantage.

B. Legal Impact

From a UK legal standpoint, these actions constitute a clear violation of *the Computer Misuse Act 1990*, the data Protection Act 2018, and the UK General Data Protection Regulation (UK GDPR).

Daley's unauthorized access, deletion, and potential transmission of confidential files align with offences outlined in *the Computer Misuse Act 1990*:

- **Section 1:** Unauthorised access to computer material. This offence is committed when an individual knowingly accesses data without permission.
- **Section 3:** Unauthorised acts with intent to impair the operation of a computer. This includes actions that intentionally or recklessly impair the operation of any computer or the reliability of data.

The **Copyright, Design and Patents Act 1988** is most directly relevant, as Daley's actions constitute intellectual property theft. The proprietary Maya design files represent CMMC's protected creative work and trade secrets. Unauthorized copying and transmission to a competitor could lead to civil litigation for damages and potential criminal charges, depending on the nature and extent of the infringement.

The **Trade Secrets Regulations 2018** specifically protect confidential business information that has commercial value. Daley's transfer of unreleased product designs to a competitor represents a textbook violation that could subject both him and potentially 360tech to legal action.

Although the **Data Protection Act 2018** and **UK GDPR** primarily concern personal data rather than intellectual property, breaches involving that information can lead to serious consequences. The Information Commissioner's (ICO), which is responsible for enforcing these laws in the UK, can issue fines of up to £17.5 million or 4% of a company's global annual turnover.

The legal consequences for these violations include potential criminal prosecution, civil liability for damages, and injunctive relief to prevent use of stolen intellectual property.

C. Recommendations

The forensic investigation into Richard Daley's activities has revealed several security weaknesses at CMMC's. The following recommendations address these vulnerabilities:

When design team members resign, immediately revoke their system access and conduct supervised handovers of work files. This measure would have prevented Rich Daley from accessing sensitive files during his notice period.

Install monitoring software that detects suspicious file operations like mass encryption, compression, or deletion. Such a system would have flagged Daley's activities when he began preparing files for removal.

Block external file sharing services like WeTransfer. Implement a company-approved transfer solution that maintains logs and require manager approval for sensitive data transfers.

Conduct regular training on intellectual property protection. Ensure employees understand their legal obligations and the consequences of data theft. Reinforce this information during exit interviews. Perform quarterly security checks on design workstations and add controls that prevent unauthorized copying of proprietary files to external storage.

These improvements will help safeguard valuable designs while maintaining an effective collaborative environment for design teams.

V. CONCLUSION

The forensic investigation has demonstrated, through systematic analysis and evidence recovery, that the disappearance of proprietary design files at CMMC was not accidental but involved deliberate data exfiltration. By following standard forensic procedures, including evidence preservation, imaging, hash verification, and artifact analysis, the investigation provided clear indicators of unauthorised deletion and transmission of confidential files to a competing firm.

The tools used (FTK Imager and Autopsy) proved reliable for the acquisition and analysis phases, enabling recovery of deleted files, deletion of USB activity, and retrieval of

relevant browser and email artifacts. These findings, along with the reconstituted timeline, present, a compelling case of intellectual property theft.

From a legal standpoint, the incident potentially violates multiple UK laws, including the Computer Misuse Act 1990, the Copyright, Designs and Patents Act 1988, and the Trade Secrets Regulations 2018.

CMMC should now consider legal action, while urgently reviewing its internal security policies. Key recommendations include enforcing device activity logging, employee access control during notice periods, and implementing a robust Data Loss Prevention (DLP) strategy to protect future intellectual property.

REFERENCES

- [1] B. E. Hermansen, "An Evaluation of Forensic Tools for Linux : Emphasizing EnCase and PyFlag," 2010.

APPENDIX

- [2] Invoice from Troy Simpson to CMMC
- [3] Complete Autopsy Forensic Report