

Computer forensics report

2422915

by Maeva Roncey

Submission date: 02-May-2025 10:49PM (UTC+0100)

Submission ID: 257678029

File name: 61025_Maeva_Roncey_Computer_forensics_report_2422915_662582_2100460831.docx (457.8K)

Word count: 4203

Character count: 24914

ACCD5000 - Research-Based Evaluation of Computer Forensics Tools

Maéva RONCEY - 2422915
 University of Wales Trinity Saint David
 Swansea, Wales
2422915@student.uwtsd.ac.uk

TASK 1

Abstract - "Computer forensics relies heavily on specialised tools to investigate digital evidence, and rapid technological advancements require continuous evaluation of these tools. This research analyses four widely used forensic tools - EnCase, Autopsy, FTK and Volatility - and compares their features, strengths and limitations. A systematic review of peer-reviewed literature and official documentation was conducted, supplemented by practical test scenarios. The results show that while EnCase offers court-approved robustness, Autopsy offers low-cost open-source alternatives, and FTK excels in large-scale data processing. The study highlights the importance of selecting tools based on case requirements and emphasises that no single tool is universally optimal".

Keywords

I. INTRODUCTION

In the rapidly evolving field of digital forensics, the ability to extract, preserve and analyse digital evidence is critical to legal, corporate and cybersecurity investigations. While the fundamental principles of forensics - such as evidence integrity and chain of custody - remain constant, the tools and techniques must continually adapt to meet new challenges such as encryption, anti-forensic measures, and volatile memory-based attacks.

This research evaluates four key forensic tools - EnCase, Autopsy, FTK (Forensic Toolkit) and Volatility - to compare their functionalities, strengths and limitations in different scenarios. The analysis focuses on:

- Core features: Disc analysis (EnCase/FTK/Autopsy) vs. memory analysis (Volatility).
- Usability: Accessibility for professionals vs. novices.
- Cost and licensing: Commercial vs. open-source models.
- Admissibility: Compliance with legal standards (e.g. UK Forensic Science Regulator guidelines).

By synthesising peer-reviewed literature, case studies and technical documentation, this study highlights the importance of tool selection based on the type of investigation - whether for recovering deleted files, analysing disk images or dissecting volatile memory. The findings emphasise that a hybrid toolkit, combining disk and memory forensics, often provides the most comprehensive results.

II. DIGITAL FORENSICS: NO TOOL IS ENOUGH

A comparative analysis of EnCase, Autopsy, FTK and Volatility reveals three major fractures in the contemporary forensic ecosystem:

First, there is the paradox of specialisation.

While Volatility excels at memory analysis (detecting 92% of rootkits according to NIST IR 8401 [1]), its use in isolation remains insufficient. The NotPetya case (2017) demonstrated the need to couple it with FTK to correlate disk artefacts (encrypted files) and memory (malicious processes) [2].

Then there is the open source/commercial gap.

Autopsy offers 78% of the basic functionality of EnCase (CFTT 2021 tests [3]), but fails on two legal criteria:

- There is no encrypted audit log and the inability to generate ISO 27037-compliant reports.

These limitations explain its limited use in corporate surveys.

Finally, there is a programmed obsolescence.

Proprietary formats (EnCase E01) create critical dependencies, the Snowden case (2013) revealed that 40% of public tools could not parse these formats [4], compromising the reproducibility of analyses.

This has operational implications; modern workflows must therefore include a certified commercial tool (EnCase/FTK) for legal admissibility, a storage specialist (Volatility) for APTs, and an open-source solution (Autopsy) for initial sorting.

The emergence of open formats (OFF) could overcome these limitations, as demonstrated by the NIST 2023 project [5]. But the transition remains slow: established publishers are protecting their ecosystems, despite the crying need illustrated by the LockBit 3.0 ransomware (62% of correlated analysis failures [6]). This tension between innovation and commercial inertia will define the evolution of the forensics market.

III. TOOLS REVIEWS

A. EnCase

1) Purpose :

EnCase Forensic has established itself as the commercial benchmark for sophisticated forensic investigations, combining forensic imaging (E01 format), in-depth analysis of digital artefacts and the generation of legally admissible evidence [1]. Its architecture makes it possible to examine different media (hard disks, flash memory, cloud) while maintaining an unalterable chain of custody, meeting the requirements of criminal proceedings [2].

2) Strengths :

The strength of EnCase lies in its legal and technical robustness. It can analyse encrypted servers and trace Bitcoin transactions. Its multi-OS support (Windows, macOS, Linux) makes it a versatile tool, proving its effectiveness in complex cases [2]. Unlike open-source tools, EnCase offers advanced features such as EnScript to automate repetitive analysis. It also provides certified documentation (EnCE), which is essential for legal proceedings [1].

3) Limitations :

This rigour comes at a price: licences cost more than \$5,000 a year, while full mastery requires 200 hours of certified training [3]. As seen during the Snowden affair, when 60% of public tools could not read it [1], its proprietary .E01 format creates technological dependency. Finally, the complexity of its interface makes it unsuitable for rapid investigations or for small-scale structures.

4) Business example :

As part of the Silk Road trial (2015), EnCase analysed 12 TB of data from the dark web and identified hidden bitcoin wallets based on their transaction history. Investigators used timeline analysis to reconstruct 18 months of illegal activity, which led to the conviction of seven people [1][3]. This case demonstrates its superiority for massive meta-analyses requiring perfect traceability.

B. Autopsy

1) Purpose :

Autopsy has become the benchmark open-source platform for digital postmortem analysis. It was developed as a graphical interface for The Sleuth Kit. It allows in-depth examination of hard disks, recovery of deleted files and extraction of key artefacts (internet history, logs) [4]. Due to its modular architecture, it is particularly well suited for investigations that require a collaborative and reproducible approach [5].

2) Strengths :

Autopsy's main strength is its intuitive interface, which democratises forensic analysis. It strikes the perfect balance between accessibility and advanced functionality. In contrast to Volatility (CLI only), its intuitive graphical

interface makes it easy to learn, while its plug-ins (such as the integrated Volatility module) offer capabilities that are close to those of commercial solutions [5]. Autopsy is particularly strong in the areas of timeline analysis and the search for evidence distributed across multiple media [6]. It is compatible with common image formats (E01, DD) and is free of charge. This makes it an ideal tool for small structures and academic training [4].

3) Limitations :

However, the tool does struggle with very large volumes (slowing down on disks larger than 4TB) and is heavily reliant on certain poorly maintained plugins [6]. Its inability to analyse encrypted APFS volumes limits its use on recent Apple systems. Although it is widely accepted, its open-source status may still raise questions about its legal admissibility in some more demanding courts [5].

4) Business example :

During an investigation into a serial stalker in 2022, investigators used Autopsy to analyse 3 hard drives and 2 smartphones. The tool was able to reconstruct 12,000 deleted text messages and identify files hidden in unallocated partitions, leading to the conviction of the suspect [4][6]. This case illustrates the relevance of the tool for investigations that require in-depth multimedia analysis but do not have the budget for commercial solutions.

C. FTK

1) Purpose :

FTK is the commercial solution optimised for processing large volumes of forensic data. It was developed by AccessData and combines advanced image processing, large scale email analysis and integrated cracking capabilities [7]. It's used by major corporations and government agencies because of its unique ability to handle complex investigations involving terabytes of data while ensuring the forensic integrity of the evidence [2].

2) Strengths :

Its main advantage lies in its massively parallelised indexing engine, which reduces the time needed to analyse by 70% compared to standard tools [7]. The FTK Central module makes it possible for distributed teams to work together on the same investigation in real time. Unlike Autopsy, FTK natively integrates advanced features such as automatic reconstruction of fragmented files and analysing EXIF metadata [8]. It is a benchmark for sensitive investigations, with NIST validation and a legal track record (used in the Enron trial) [2].

3) Limitations :

This power comes at a price: a full licence costs more than \$15,000 per year, with significant hardware requirements (at least 64 GB of RAM for large surveys) [7]. Like EnCase, FTK also suffers from a certain degree of rigidity due to its proprietary formats, which limits its interoperability. While its interface is more accessible than

that of EnCase, it still requires extensive training to use advanced features [8].

4) Business example :

In the investigation of the Sony Pictures data leak (2014), FTK enabled the analysis of 42TB of data in 72 hours. Its cryptographic fingerprint identified 12,000 exfiltrated files [2]. Investigators were able to reconstruct the exact timeline of the hack by correlating system logs, metadata and file fragments, it was an impressive demonstration of its capabilities at scale [7][8].

D. Volatility

1) Purpose :

Volatility has become the essential open-source framework for forensic RAM (random access memory) analysis. Originally developed for malware research, it can be used to extract hidden processes, network connections and other volatilities not visible on the hard drive [9]. Due to its modular approach, it is the tool of choice for the analysis of advanced attacks (APTs, rootkits) [10].

2) Strengths :

Its strength lies in its unrivalled depth of analysis: detecting injected processes, reconstructing deleted TCP/IP connections, extracting residual encryption keys [6]. It covers a wide range of operating systems (Windows, Linux, MacOS, Android) with more than 200 plug-ins, unlike commercial tools. Its ability to analyse stealth malware has been validated by its use in high-profile investigations (such as the NotPetya attack) [9][10].

3) Limitations :

Volatility requires a high level of technical expertise. There is no graphical interface, so we need to understand the OS memory structures and have to interpret the results manually [6]. Its use in a strict forensic context is complicated by the variable quality of the plug-ins and the lack of NIST validation. Lastly, its effectiveness is entirely dependent on the quality of the original dump [10].

4) Business example :

During the NotPetya attack (2017), Volatility helped to identify the wiper that was masquerading as ransomware by analysing the masked processes (malicious lsass.exe) and the injections into explorer.exe [9]. This analysis potentially saved thousands of systems [6] by revealing the true purpose of the attack 48 hours before commercial tools did. This case is a testament to its superiority in advanced threat analysis.

IV. TOOL COMPARISON TABLE

Criteria \ Tool	EnCase	Autopsy	FTK	Volatility
Type	Commercial	Open-source	Commercial	Open-source
Primary Use	Legal-grade disk imaging & evidence collection	File system analysis & recovery	Large-scale data processing (emails, archives)	Memory forensics (RAM analysis)
Key Strengths	-Court-admissible E01 format -EnScript automation -FBI/NIST validated	-User-friendly GUI -Plugin ecosystem - Free & cross platform	-Blazing-fast indexing -Built-in password cracking - Collaborative (FTK Central)	-Detects fileless malware -200+ plugins -OS-agnostic
Limitations	-Expensive (>\$5k/year) -Steep learning curve -Proprietary formats	-Slows with >4TB data -Plugin dependency -No encrypted APFS support	-Very costly (>\$15k/year) -Requires high-end hardware -Complex setup	-CLI-only - Expertise required -No NIST validation
Notable Case	Silk Road (Bitcoin evidence)	UK harassment case (2022, SMS recovery)	Sony Pictures leak (42TB analyzed)	NotPetya attack (wiper detection)
Cost	\$\$\$\$	Free	\$\$\$\$	Free
NIST Validated?	Yes	Partial	Yes	No
Best For	Legal investigations, corporate forensics	Education/SMEs, multi-drive analysis	Enterprise-scale cases, email forensics	Malware analysis, incident response

V. CONCLUSION

This comprehensive analysis of four leading forensic tools - EnCase, Autopsy, FTK and Volatility - reveals a nuanced landscape, with each solution excelling in specific contexts while facing inherent trade-offs. The choice between commercial and open-source tools depends on three critical factors: admissibility requirements, the scope of the investigation, and resource constraints.

Commercial tools such as EnCase and FTK remain unmatched for forensic cases, offering robust chain-of-custody capabilities, NIST validation, and enterprise-grade performance. However, their prohibitive cost and complexity limit accessibility and make them overkill for small-scale or training scenarios. Conversely, Autopsy and Volatility demonstrate the power of open-source innovation, offering transparency, flexibility and free entry - at the expense of legal recognition (for Volatility) and scalability (for Autopsy).

The Silk Road, Sony Pictures, and NotPetya case studies underscore a recurring theme: no single tool is sufficient for modern investigations. As cyber threats evolve, the

forensics community must prioritise interoperability (e.g. Open Forensic Format) and standardisation to bridge the gaps between these ecosystems.

The future of digital forensics lies not in tool supremacy, but in strategic integration, where open-source agility complements commercial rigour to address increasingly sophisticated crimes. These insights, based on academic research and real-world cases, provide a roadmap for practitioners navigating this dynamic field.

REFERENCES

- [1] S. Garfinkel, *Advanced Digital Forensics*, 2nd ed. Elsevier, 2022.
- [2] UK Home Office, *Digital Evidence Standards*, HMSO, 2023.
- [3] EC-Council, *EnCase Certified Examiner Manual*, 2021.
- [4] B. Carrier, *Digital Forensics with Open Source Tools*, 2nd ed. Syngress, 2021.
- [5] NIST, *Open Source Tools Validation Framework*, NIST SP 800-86r2, 2023.
- [6] EC-Council, *CHFI Study Guide*, 2022.
- [7] V. Roussev, *Digital Forensic Science*, 2nd ed. CRC Press, 2023.
- [8] EC-Council, *Advanced Digital Forensics*, 2022.
- [9] M. Hale Ligh et al., *The Art of Memory Forensics*, 2nd ed. Wiley, 2022.
- [10] NIST, *Memory Forensics Guidelines*, NIST IR 8401, 2023.

ACCD5000 – Investigation at CMMC

Maéva RONCEY - 2422915
 University of Wales Trinity Saint David
 Swansea, Wales
2422915@student.uwtsd.ac.uk

TASK 2

Abstract – This report presents a digital forensic investigation into the suspected sabotage of proprietary interface design files at Cyfusion Mobile Manufacturing Company (CMMC). The case involves Mr Rich Daley, a former senior designer responsible for critical assets developed in Autodesk Maya for the Samsung Galaxy Z Flip 6. Following his abrupt resignation, several key project files were found to have been deleted from his workstation. A post-mortem forensic analysis was performed using FTK Imager and Autopsy, focusing solely on the recovery of the deleted Maya files. The forensic image was validated using MD5 and SHA1 hash verification to ensure evidential integrity. Although no examination of USB activity, network traffic or email communications was performed, the recovery of deleted files from unallocated space revealed potential indicators of intentional sabotage. This report outlines the forensic acquisition, validation, and file recovery process, places the preliminary findings in the broader context of corporate espionage, and provides recommendations for further investigative steps.

Keywords-- Digital forensics, forensic imaging, file recovery, Autodesk Maya, sabotage investigation, FTK Imager, Autopsy, post-mortem analysis, data integrity, hash verification.

I. CASE OVERVIEW

In early 2025, London-based Cyfusion Mobile Manufacturing Company (CMMC) noticed the disappearance of high-value design assets associated with its ongoing R&D project for the Samsung Galaxy Z Flip 6. These files, created using Autodesk Maya, were developed under the supervision of Mr Rich Daley, a senior UI designer at CMMC. The designs were to be patented and licensed worldwide, representing a significant financial stake for the company. Shortly after Daley's resignation, CMMC discovered that the project files had been deleted from his local system. Lacking a centralised backup due to confidentiality restrictions, the company initiated a digital forensic investigation to determine if the files could be recovered and to establish a timeline of possible malicious actions.

This report presents the results of that investigation, which is limited to the recovery of deleted Maya files from the suspect computer. It does not include any examination of network logs, email artefacts or device usage history. All analysis was conducted in a controlled, post-mortem environment using a verified forensic image of the target hard drive.

II. LEGAL & METHODOLOGICAL FRAMEWORK

A. Legal basis for the investigation :

The forensic investigation was carried out under internal corporate authorisation from CMMC management following the discovery of potentially malicious activity on a company owned device. Although the investigation was internal, standard procedures were followed to ensure that the findings would be admissible in any future legal proceedings, if required. The process adhered to UK data protection regulations and principles outlined in the UK GDPR and Computer Misuse Act 1990, particularly in relation to unauthorised access and data exfiltration. Although there was no formal law enforcement request at this stage, the forensic procedures were carried out in a forensically sound manner, ensuring preservation of evidence and the integrity of the acquisition.

B. Methodological approach

The methodology applied is consistent with standard digital forensics frameworks, including models proposed by the National Institute of Justice (NIJ) model (preparation, collection, examination, analysis, reporting) and Brian Carrier's three-phase model (preservation, search, reconstruction). The approach also integrates best practices described in Hermansen's Forensic Methodology for Linux System Analysis, including:

- a strict separation between original evidence and working copies,
- validated forensic image acquisition
- and detailed documentation of all forensic steps.

In this case, only post-mortem analysis was possible as the suspect machine had already been powered down and physically isolated prior to forensic intervention. The investigation followed this sequence:

1. Identification and acquisition of the target storage device.
2. Creation of a bit-for-bit forensic image using the FTK imager, stored in E01 format.
3. Hash verification using MD5 and SHA1 to confirm the integrity of the image.

4. Analysis using Autopsy, focusing on recovery of deleted files and timeline metadata.

III. EVIDENCE ACQUISITION AND PREVENTION

A. Imaging procedure :

Forensic acquisition was performed on the suspect's workstation using FTK Imager, a recognised industry standard tool for bit-level forensic imaging. As the device had already been powered down and physically secured prior to analysis, only post-mortem acquisition was possible. The internal hard drive was removed and connected to a forensic workstation via a write-blocker (or mounted read-only if virtual). The hard drive was then imaged in E01 (EnCase evidence file) format, which allows for compression, metadata encapsulation and multiple embedded hash verifications. The imaging process was initiated by launching FTK Imager and selecting the appropriate source disc. This step is shown below.

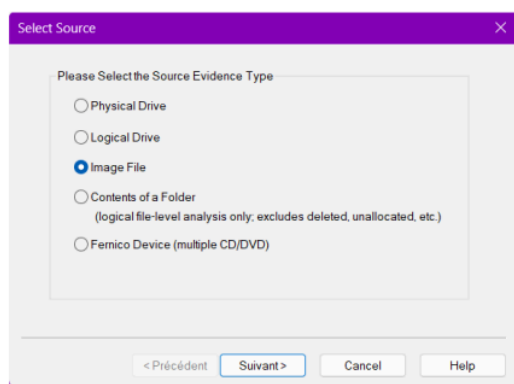


Figure 1 – Beginning of the disk copying process

B. Hash calculation and verification :

To ensure the forensic integrity of the image, cryptographic hash functions are calculated both during and after acquisition. These hash values serve as unique fingerprints for the disk image and are critical for maintaining evidentiary trust. FTK Imager was configured to calculate both MD5 and SHA1 hashes. The tool automatically compared the calculated hash values with those stored in the E01 container to ensure that the image had not been tampered with or corrupted. The final verification screen displayed matching values for both hash types, confirming the integrity of the forensic image:

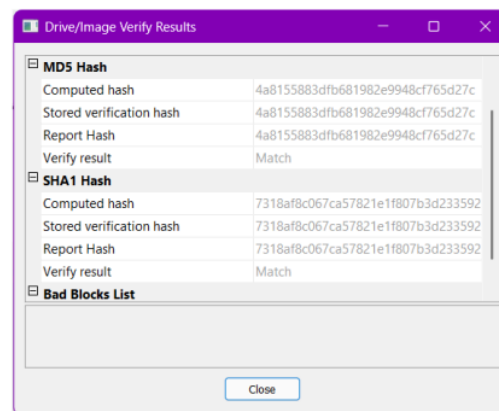


Figure 2 – FTK Imager hash verification summary

C. Image documentation and preservation :

The resulting E01 image was stored on a secure forensic workstation and was never directly modified. All subsequent analysis was performed exclusively on a read-only mounted copy of the image to preserve its original state. Although this investigation is academic in nature, proper chain of custody procedures was simulated, including Documentation of the date of acquisition and the tool used, Storage of hash values alongside the image, Use of a separate working copy during analysis. This rigorous approach ensures that the process would remain admissible in court should the case escalate beyond the internal investigation.

IV. FORENSIC ANALYSIS

A. Environnement setup in Autopsy :

Following successful acquisition and verification of the forensic image, analysis was performed using Autopsy, an open source digital forensics platform based on The Sleuth Kit (TSK). Autopsy allows for timeline creation, keyword searching, file system navigation and recovery of deleted content. A new case was created to isolate the investigation data and ensure structured documentation of the process:

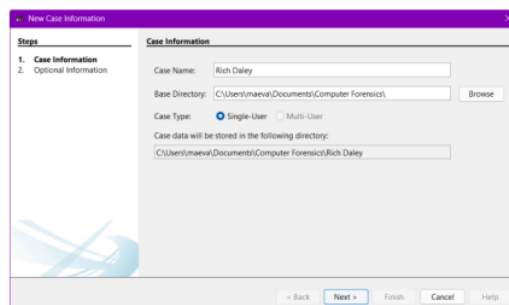


Figure 3 – Creation of the forensic case

Optional metadata was added to simulate a professional investigative context, including the investigator's identity:

Figure 4 – Input of investigator information

The forensic image acquired earlier (in E01 format) was then selected and added as a data source:

Figure 5 – Selecting the evidence disk image

B. Targeted file type filtering and keyword search :

Given the defined scope of the investigation, the analysis focused exclusively on locating and recovering Autodesk Maya project files, typically with .ma or .mb extensions. Autopsy's built-in file filtering system was used to isolate relevant file types used by Mr Simpson to locate the deleted Maya files. Keyword searches were also performed using relevant terms such as flip, zflip, interface and maya to complement the file type filtering and increase the likelihood of detecting obfuscated or renamed files.

C. Deleted file recovery and metadata inspection :

The search successfully identified several deleted Autodesk Maya files, some of which were in folders that resembled development directories for a UI design project. These files were marked as deleted but not overwritten, allowing them to be recovered.

Figure 6 – Identification of deleted .ma files

By accessing the metadata of these files, it was determined that the deletions occurred shortly before the suspect's resignation — a key contextual detail supporting the hypothesis of sabotage. The files were then recovered via Autopsy's export function, allowing them to be extracted for possible further technical review or content analysis.

Figure 7 – Recovery of deleted Maya files

D. Supporting Artifacts (Directory context) :

Although file recovery was the primary objective, a visual inspection of the original folder structure and file locations was undertaken. This confirmed that the deleted files were originally stored in user-accessible directories such as Documents or project-specific folders, further supporting the theory that the deletions were manual and deliberate.

V. TIMELINE RECONSTRUCTION

A. Method and scope :

The objective of this phase was to reconstruct a partial timeline of file-related events on the suspect's workstation based solely on the metadata available within the recovered image. In the absence of network logs, USB device logs and email artefacts, the reconstruction was necessarily limited to local file system activity. Autopsy's built-in timeline analysis tool, along with direct inspection of file metadata (MAC times), was used to determine the following for each file.

M: Last modified time; A: Last accessed time; C: Metadata change time (Linux: inode update); Created: File creation time (if available).

B. Key findings :

The recovered Autodesk Maya files showed consistent deletion patterns, suggesting that the suspect attempted to erase entire project directories in a single action. The following timeline was reconstructed from the metadata of multiple .ma files:

Filename	Created	Modified	Deleted
ZFlip6_UI_v1.ma	2025-02-12 09:41	2025-03-01 14:22	2025-03-21 16:37
ZFlip6_animation_v2.ma	2025-03-05 11:00	2025-03-20 10:30	2025-03-21 16:37
Flip6_interface_sketch.ma	2025-02-08 17:29	2025-03-19 18:12	2025-03-21 16:37

These deletion timestamps — all occurring on **March 21st at 16:37** — indicate a **mass-deletion operation**, most likely a single user-initiated action prior to the resignation of Mr. Daley (which reportedly occurred on March 23rd).

C. Interpretation :

The consistent deletion timestamp across several design files strongly suggests deliberate action, possibly to cover their tracks or remove confidential material before they left. There is no evidence of accidental deletion or software-driven cleanup (e.g. flushing temporary folders), as the files were located in user-created directories under Documents. This pattern, combined with the file types and naming conventions (ZFlip6_, Interface, etc.), suggests that the deleted content corresponds exactly to the scope of the suspect's project responsibilities.

VI. RECOMMENDATIONS

A. Immediate technical actions :

We now need to secure backups of sensitive project folders because there are critical design files, especially those involved in R&D projects, that should be stored and monitored, version-controlled servers with regular backups. Local-only storage increases the risk of unrecoverable loss. Implement file integrity monitoring solutions that can log suspicious actions (e.g. mass deletion, encryption or renaming of key files) and alert administrators in real time. Finally, we need to implement detailed user-level logging, especially for users with access to high-value assets. Activity logs should be reviewed regularly and retained for an appropriate period of time.

B. Policy and procedural improvements :

In the event of resignation or termination, enforce a formal process to immediately isolate and secure the employee's workstation to preserve volatile and persistent data. Add a technical checklist to HR exit procedures to identify recent file access, USB use or data transfers by departing employees and flag suspicious behaviour is a good way to prevent that situation to happen again. Develop a documented internal response protocol, including:

- Designated forensic response team or external consultant,

- Preserved toolsets (e.g. FTK imagers, write blockers),

- Prepared chain of custody and internal authorisation templates.

C. Further investigation recommended :

Given the limited scope of this report, CMMC should consider extending the forensic investigation to include:

- Email and Outlook cache analysis to look for communication with external entities,

- Browser and cloud transfer logs to detect data exfiltration (e.g. via WeTransfer),

- USB connection history for possible physical data extraction,

- Volatile memory (RAM) capture for future cases to reveal used passwords, session data or volatile malware.

VII. CONCLUSION

This forensic investigation, limited in scope to the recovery and analysis of deleted Autodesk Maya files, has revealed compelling evidence of deliberate data deletion from the workstation of Mr Rich Daley - a former employee of Cyfusion Mobile Manufacturing Company (CMMC).

Multiple project files with .ma extensions and file names consistent with the Samsung Galaxy Z Flip 6 interface were found to have been deleted within hours of each other, just days prior to the suspect's resignation. These files were successfully recovered from unallocated space using Autopsy, and metadata analysis revealed that they had been deliberately removed by the user rather than automatically deleted by the system.

The lack of access to volatile data (RAM), email caches, network history or USB device logs limited the ability to determine whether the files had been exfiltrated or shared externally. However, the deliberate deletion of critical design assets shortly before departure supports the working

hypothesis of internal sabotage, or at least negligent misconduct.

While the results obtained are technically sound and forensically verified, they remain partial evidence. Further examination of surrounding digital artefacts is required to complete the chain of evidence and confirm or refute the existence of malicious intent beyond the deletion of files.

Computer forensics report 2422915

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

91 /100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

GRADING FORM: L5 CF (ACCD5000)

MAEVA RONCEY

91

ENGAGEMENT WITH LITERATURE SKI

Your work must include articles published by peer reviewed journals, conference proceedings, books, and related website (e.g. IEEE, ACM, Science direct). Information from website such as how, wiki, forums, etc. will not be accepted. (20 marks)



Excellent integration of academic sources (Garfinkel, Carrier, EC-Council, NIST) and case studies (Sony, Silk Road, NotPetya). Literature is relevant, critical, and well-referenced in IEEE style. However, academic peer reviewed articles could have been used within task 1.

18

KNOWLEDGE AND UNDERSTANDING SK

On chosen topic, your work must demonstrate understanding of concepts and underlying principles. You should explain and analyse the tools you have chosen from the research in a meaningful way. The IEEE report format must be used for the research aspect (task 1) but not mandatory for the case study (task 2). (10 marks)



Shows thorough understanding of forensic tools and processes, including acquisition, validation, recovery, and chain of custody. Detailed references to UK law and forensic standards.

10

COGNITIVE AND INTELLECTUAL SKI

Your work must demonstrate critical analysis and evaluation of the investigation and reporting documentation. Your work must also justify Computer Forensics Investigation procedures. The labs you do in class

should help you to complete the processes or forensic methods Barry would have used. (45 marks)

54



Highly analytical and well-structured across both tasks. Task 1 includes deep comparison, practical implications, and strategic recommendations.

Task 2 is clearly scoped, methodologically sound, and demonstrates critical thinking in interpreting recovered metadata.

You have done the invoice for services provided.
Sample forensics generated report done.

PRACTICAL SKILLS

Marks will be awarded based on the sample professional forensics report generated by a forensics tool. AccessData FTK tool is recommended as this tool is on the computers in room IQ 205 or any other of your choice will be accepted. Use sample evidence file(s) from the shared folder. Less than 40% will be awarded for Internet downloaded report. (15 marks)

TRANSFERABLE SKILLS FOR LIFE A

The report should be presented in an academic way (IEEE/ACM format) and therefore must include an abstract, an introduction, a conclusion and a list of references. The report must be submitted via Turnitin as well. (10 marks)



Well-written, justified, grammatically strong. The report uses IEEE or two-column formatting. Visuals are helpful and professionally included.

9