

Computer Forensics

ACCD5000

SYNTHESIZE A SOLUTION TO A POTENTIAL REAL-LIFE
SCENARIO

Daniel Mark Jones
0300760

Contents

Task 1: Comparative Evaluation of Modern Digital Forensic Tools for CHFI Investigations (2026).....	3
Task 2 – Case study: Sabotage	7
Executive Summary	7
Section 1 – Methodology & Investigation Plan	7
1.1 Legal and ethical framework	7
1.2 Acquisition strategy — encrypted drive	8
1.3 Anti-forensic detection strategy	9
1.4 File carving and recovery strategy	9
1.5 Cloud synchronisation evidence strategy	9
Section 2 – Forensic Investigation Process	10
2.1 First Response and Scene Preservation	10
2.2 Forensic Acquisition	10
2.3 Examination – Anti-Forensic Activity	11
2.4 Examination – File Recovery	11
2.5 Examination – Cloud Synchronisation Evidence	12
Section 3 – Findings	14
3.1 Anti-Forensic Activity (Eraser Execution)	14
3.2 File Recovery and Residual Artefacts	14
3.3 Cloud Synchronisation and Data Exfiltration Evidence.....	14
3.4 Timeline Correlation of Events.....	15
Section 4 – Conclusion	15
Appendix A – Simulated Hash log	18
Appendix B – Professional Invoice	19

Task 1: Comparative Evaluation of Modern Digital Forensic Tools for CHFI Investigations (2026)

Daniel Jones
Computing Portfolio – ACCD5000
University of Wales Trinity St David

Abstract—The rapid growth of cybercrime and the increasing reliance on digital evidence have intensified the need for reliable, legally defensible forensic tools. As shown in this analysis, no single platform fully covers all phases of the CHFI process, and tool selection carries legal as well as technical implications. This paper evaluates four widely used tools – FTK Imager, Autopsy, Magnet AXIOM, and Cellebrite UFED – assessing technical capabilities and legal admissibility through the Daubert Standard. In this study, the difference between open-source and commercial tools appears to be influenced more by legal infrastructure than purely technical performance, with commercial tools benefiting from institutional validation while open-source tools offer transparency without equivalent formal recognition. It also demonstrates that no single tool provides complete CHFI coverage, making a multi-tool strategy essential. The paper recommends a hybrid approach combining commercial tools for primary analysis with open-source tools for transparent verification, applied directly to the CMMC investigation in Task 2.

INTRODUCTION

The rapid growth of cybercrime and the increasing reliance on digital evidence in legal proceedings have made effective forensic investigation a critical component of modern justice systems. Recent studies highlight a significant rise in cyber-enabled offences between 2023 and 2025, underscoring the need for reliable, defensible forensic tools capable of supporting complex investigations. As digital evidence becomes central to both criminal and civil litigation, the tools used to acquire, analyse, and present that evidence carry substantial technical and legal implications.

Digital forensics operates across multiple phases of the CHFI process, and investigators must navigate a landscape divided broadly between commercial and open-source tools. While the underlying investigative concepts remain stable, the tools themselves evolve rapidly, creating a persistent challenge in selecting appropriate, legally defensible solutions. Despite the wide range of tools available, research consistently shows that no single platform provides complete coverage of all investigative phases — a limitation identified consistently across the literature, from early comparative studies[1] to recent evaluations[2].

This paper addresses that problem by critically evaluating four widely used forensic tools — FTK Imager, Autopsy, Magnet AXIOM, and Cellebrite UFED — across both technical capability and legal admissibility dimensions. It examines not only what these tools can do, but how their design, validation status, and evidential track records shape their suitability for high-value investigations. In doing so, the paper extends beyond technical comparison to incorporate the Daubert Standard and broader legal infrastructure, offering a

more holistic assessment of forensic tool suitability for legal proceedings.

The paper is structured as follows: Section II presents individual tool overviews; Section III provides a comparative analysis; Section IV develops three critical arguments concerning legal credibility, cost, and Daubert compliance; and Section V concludes with a multi-tool recommendation applied directly to the CMMC case study.

DIGITAL FORENSIC TOOLS

FTK Imager

FTK Imager is a free forensic acquisition tool developed by Exterro, used to create bit-for-bit forensic images of storage media while preserving evidential integrity. When used with a hardware write blocker, it supports ACPO Principle 1 by ensuring no data on the source device is altered during acquisition. The tool generates MD5, SHA-1, and SHA-256 hash values for both the original media and acquired image, providing verification that the copy is identical to the source. This cryptographic validation is essential for demonstrating evidential integrity in legal proceedings [3].

FTK Imager can also capture live RAM, which is particularly important in BitLocker-protected systems where decryption keys may reside in memory while the system is running [2]. This capability is directly relevant to the CMMC investigation.

However, FTK Imager is limited to acquisition and does not support analysis, cloud evidence, or mobile forensics. As a result, images must be transferred to other tools for examination, requiring careful documentation to maintain chain of custody.

Within the CHFI framework, FTK Imager operates solely in the acquisition phase, providing a legally defensible foundation for further forensic analysis.

Autopsy

Autopsy is an open-source digital forensics platform developed by Basis Technology and built on The Sleuth Kit, providing a graphical interface for analysing forensic images. It is primarily used in the examination and analysis phases of the CHFI process.

Key features include timeline analysis, which correlates file system, log, and browser activity to reconstruct user

behaviour; indexed keyword search for efficient data retrieval; and web artefact extraction, which identifies browser history, cookies, and cached data. These capabilities are particularly relevant for investigating cloud-based activity [4].

Autopsy also supports file carving, allowing recovery of deleted files from unallocated disk space by identifying file signatures. This is useful in cases involving deliberate data deletion or wiping attempts [3].

However, Autopsy has limitations in professional contexts. Comparative studies show it is slower than commercial tools, which can impact time-sensitive investigations [5]. In addition, although technically reliable, open-source tools may face challenges in legal proceedings due to the lack of standardised validation frameworks, which can affect how evidence is perceived in court [5].

For this reason, Autopsy is most effective when used alongside commercial tools, providing independent verification of findings rather than acting as a standalone solution.

Within the CHFI methodology, Autopsy is best positioned in the examination and analysis phase as part of a multi-tool investigative approach.

Magnet AXIOM

Magnet AXIOM is a commercial digital forensics platform developed by Magnet Forensics that provides an end-to-end workflow across acquisition, examination, analysis, and reporting phases of the CHFI process.

A key strength of AXIOM is its cloud acquisition capability, enabling recovery of artefacts from services such as Google Drive and OneDrive. This is particularly relevant to the CMMC investigation, where browser-based cloud activity forms a central evidential source. Comparative studies indicate AXIOM can recover significantly more artefacts than open-source tools in data-intensive investigations [6].

AXIOM also includes advanced analysis features such as Connections, which maps relationships between users, devices, and accounts. This supports identification of links between a suspect device and external services, strengthening evidential interpretation [2].

Its commercial status contributes to stronger perceived legal credibility, as proprietary tools are often supported by established validation processes and documentation [5]. However, this introduces limitations, including high licensing costs, vendor dependency, and reduced transparency due to closed-source design.

Within the CHFI methodology, AXIOM spans multiple investigative phases and is most effective as the primary analysis platform, supported by additional tools for acquisition and independent verification.

Cellebrite UFED

Cellebrite UFED is a commercial mobile forensics platform used for extracting and analysing data from smartphones and

tablets. It supports logical, file system, and physical extraction, with physical extraction providing the deepest access, including recovery of deleted data [2].

UFED can also perform cloud extraction using authentication tokens obtained from devices, enabling access to associated accounts. It supports analysis of application data, including messaging apps, location artefacts, and user activity, and produces court-ready reports with hash verification.

Although the CMMC investigation focuses on a workstation, a suspect's mobile device would represent a valuable secondary evidence source. UFED would therefore be appropriate if additional exhibits were available.

However, UFED is highly specialised and limited to mobile forensics, making it less suitable for broader system or cloud investigations. Its closed-source design has also faced scrutiny in legal contexts, particularly regarding transparency and validation under standards such as Daubert [5]. Additionally, the tool is expensive and requires frequent updates to remain compatible with evolving mobile operating systems [6].

Within the CHFI framework, UFED is positioned in the mobile forensics phase, reflecting its role as a specialist tool within a multi-tool investigation strategy.

COMPARATIVE ANALYSIS

COMPARATIVE ANALYSIS OF DIGITAL FORENSIC TOOLS

Feature	Tools			
	<i>FTK Imager</i>	<i>Autopsy</i>	<i>Magnet AXIOM</i>	<i>Cellebrite UFED</i>
Cost	Free	Free	Commercial (£££)	Commercial (££££)
Type	Imaging only	Analysis suite	All-in-one	Mobile specialist
File Systems	NTFS, FAT, ext, HFS+	NTFS, FAT, ext, HFS+	Wide range	Mobile platforms
Cloud Support	None	Limited	Excellent	Token extraction
Mobile Support	None	Limited	Good	Excellent
Reporting	Basic	Moderate	Comprehensive	Comprehensive
CHFI Phase	Acquisition	Analysis	All phases	Mobile phase
Open Source	No (freeware)	Yes	No	No
Legal Track Record	Strong	Moderate	Strong	Strong (contested)
Key Limitation	Imaging only	Processing speed	Cost, closed source	Mobile only, version dependent

Table I summarises the key characteristics of the four forensic tools across cost, capability, and CHFI phase coverage. Several clear patterns emerge from this comparison.

First, a capability gap exists between open-source and commercial tools. FTK Imager and Autopsy provide strong functionality in acquisition and analysis respectively but lack

integrated cloud and mobile support. In contrast, commercial tools such as Magnet AXIOM and Cellebrite UFED offer broader capabilities, particularly in cloud artefact recovery and mobile data extraction [4]. However, this distinction is not solely technical. Studies suggest that commercial tools are often favoured in legal contexts due to established validation processes and documented use in investigations, whereas open-source tools may lack equivalent institutional recognition despite producing comparable results [5].

Second, the comparison shows that no single tool covers all phases of the CHFI process. Each tool addresses a specific aspect: FTK Imager supports acquisition, Autopsy provides analysis, AXIOM offers multi-phase capability including cloud analysis, and UFED focuses on mobile forensics. This reinforces the need for a multi-tool approach, where tools are combined based on their strengths rather than used in isolation.

In the context of the CMMC investigation, this approach is reflected using FTK Imager for acquisition, AXIOM for primary analysis and cloud artefact recovery, and Autopsy for independent verification. This combination ensures both technical effectiveness and stronger evidential support.

Overall, the comparison demonstrates that effective digital forensic investigation depends on selecting complementary tools that collectively support all phases of the CHFI process.

CRITICAL EVALUATION

The comparative findings in Section III reveal that the open source versus commercial debate in digital forensics is fundamentally mis-framed when treated as a question of technical capability. Open-source tools such as Autopsy and The Sleuth Kit offer a transparency advantage: their codebases are publicly inspectable, allowing independent scrutiny that theoretically aligns with the Daubert Standard's peer-review requirement. Yet this transparency has not translated into stronger legal acceptance. The problem is not technical performance – Ismail and Ariffin [5] demonstrated 0% error rates for Autopsy across repeated testing, and Manson et al.[1] showed as early as 2007 that open-source tools can produce forensically equivalent results in controlled testing environments. Instead, the barrier is institutional: no authoritative body has formalised validation procedures for open-source tools, leaving them without the standardised certification frameworks that courts rely on. Ismail and Ariffin's three-phase validation model[5] represents a meaningful attempt to close this gap, but it has not yet been widely adopted. The implication for practice, including the CMMC investigation, is that open-source tools should be used primarily for verification, not as the sole basis for high-value evidential claims – not because they are inferior, but because the legal infrastructure has not caught up with their proven technical reliability[4].

This legal credibility gap has direct financial implications for investigative practice, raising questions about cost proportionality and access to forensically sound evidence.

Commercial tools such as Magnet AXIOM and Cellebrite UFED are not inherently more accurate than open-source alternatives, but they carry established courtroom track records, vendor-supported validation documentation, and recognised testing procedures – all of which strengthen admissibility under scrutiny [5]. In high-value cases such as CMMC, where millions of pounds of intellectual property are at risk, the cost of commercial licensing is easily justified when weighed against the consequences of evidence being excluded or challenged. Yet this creates an uncomfortable systemic implication: organisations with limited budgets may be unable to access the tools that carry the greatest legal weight, effectively producing a two-tier forensic justice system. Agboola et al. [4] highlight this tension directly, noting that open-source tools can be highly productive in resource-constrained environments, but the trade-off in legal credibility remains significant. The critical question, therefore, is not which tool is technically superior, but which combination of tools provides the most legally defensible evidential pathway for the specific investigative context [5], [2].

Evaluating these tools against the Daubert Standard provides the most rigorous framework for resolving this tension and offers a principled basis for tool selection in legal proceedings. The four Daubert criteria — testability, peer review, known error rates, and general acceptance — map unevenly across the tool landscape. Commercial tools score highly on general acceptance and established courtroom use, but their closed-source nature limits independent verification and obscures error-rate transparency. Open-source tools, conversely, excel in transparency and peer-review potential but have historically lacked formalised validation and documented error-rate metrics. Ismail and Ariffin's framework[5] directly addresses this gap by providing repeatability testing and error-rate calculation for open-source tools, representing a significant step toward Daubert compliance. The implication for investigators — including in the CMMC case — is that neither tool category fully satisfies Daubert alone. In this investigation, a stronger evidential position is achieved by combining commercial tools for primary analysis with open-source tools for verification[6]. This conclusion reinforces the multi-tool strategy established in Section III and forms the foundation for the investigative approach applied in Task 2.

CONCLUSION

The comparative analysis demonstrates that digital forensic tool selection is shaped less by technical capability than by the structural realities of legal infrastructure. No single tool provides full CHFI coverage, and the long-standing open-source versus commercial divide is revealed not as a question of performance but of institutional trust, validation, and courtroom authority. FTK Imager, Autopsy, AXIOM, and Cellebrite each occupy distinct evidential roles: FTK Imager provides the acquisition foundation; Autopsy offers transparent, verifiable analysis; AXIOM delivers cloud-aware, multi-phase capability; and Cellebrite specialises in deep mobile extraction. Within this investigation, these tools operate together as complementary components rather than direct alternatives.

The Daubert Standard reinforces this conclusion. Its emphasis on testability, peer review, error rates, and general acceptance exposes the limitations of both tool categories: commercial tools excel in acceptance but lack transparency, while open-source tools excel in transparency but lack formalised validation[4]. Ismail and Ariffin's framework[5] provides the clearest path toward resolving this imbalance, but until such validation becomes standard, the strongest evidential position is achieved through a hybrid approach.

The evidence therefore supports a clear recommendation: investigators should combine commercial tools for primary acquisition and analysis with open-source tools for independent verification. This multi-tool strategy directly informs the methodology applied in Task 2, where the CMMC investigation relies on the same balanced, defensible approach.

Task 2 – Case study: Sabotage

Executive Summary

This report presents the findings of a digital forensic investigation commissioned by Cy-fusion Mobile Manufacturing Company (CMMC) into suspected intellectual property theft and deliberate data sabotage by former employee Richard Daley. The investigation was conducted by Troy Simpson, a Certified Hacking Forensic Investigator (CHFI) and Certified Ethical Hacker (CEH), in accordance with ACPO principles and the CHFI forensic methodology. The primary evidence source was Daley's assigned Windows 11 workstation, protected with BitLocker full-disk encryption, which was addressed through forensically sound decryption procedures prior to examination.

Forensic examination identified three key findings. First, artefacts consistent with the use of a file-wiping utility were recovered, demonstrating deliberate anti-forensic activity intended to destroy Autodesk Maya project files. Second, browser artefacts revealed access to and synchronisation with a personal Google Drive account, indicating off-network exfiltration of company design assets. Third, file-system metadata, Windows thumbnail cache entries, and partial file fragments consistent with Autodesk Maya GUI design files were identified within unallocated disk space, surviving despite deliberate wiping attempts.

Collectively, the evidence demonstrates intentional data destruction and unauthorised transfer of confidential intellectual property by Daley prior to his resignation. All evidence was acquired, preserved, and analysed under strict chain-of-custody procedures to ensure forensic integrity and legal admissibility, consistent with established best practice in digital evidence handling[7], [8]. The artefacts, timestamps, and findings presented in this report are simulated exemplar results consistent with what would be expected in a real-world investigation of this nature. They are provided to demonstrate forensic methodology, reporting format, and evidential reasoning, rather than to represent analysis of a supplied evidential image.

Section 1 – Methodology & Investigation Plan

1.1 Legal and ethical framework

The investigation was conducted in accordance with ACPO principles and established digital evidence handling practices [7]. ACPO Principle 1 (no alteration of data) was maintained by minimising interaction with the live system and conducting analysis on forensic images. Where live response actions were required due to full-disk encryption, they were necessary, proportionate, and fully documented.

ACPO Principle 2 (competent access) was satisfied through the use of a qualified investigator, with all actions recorded. Principle 3 (audit trail) was maintained through detailed

logging of tools, processes, and results, enabling reproducibility. Principle 4 (overall responsibility) was upheld through full accountability for evidence handling and chain of custody [7].

1.2 Acquisition strategy — encrypted drive

The workstation was identified as BitLocker-encrypted and powered on, which is significant as decryption keys may reside in memory [8]. A live RAM acquisition was performed using FTK Imager to capture volatile data before shutdown.

A full forensic image of the drive was then created using FTK Imager with a hardware write blocker and stored in E01 format. Memory artefacts were analysed using Volatility to recover cryptographic material for decryption [2], [8]. Decryption was applied to a forensic copy, while the original image was preserved.

MD5 and SHA-256 hash values were generated to verify integrity and recorded in the evidence log [3]. The following figures contained within this assignment are illustrative examples demonstrating the use of forensic tools and techniques described in this investigation. They are included to support the methodology and do not represent analysis of actual evidential material from the case.

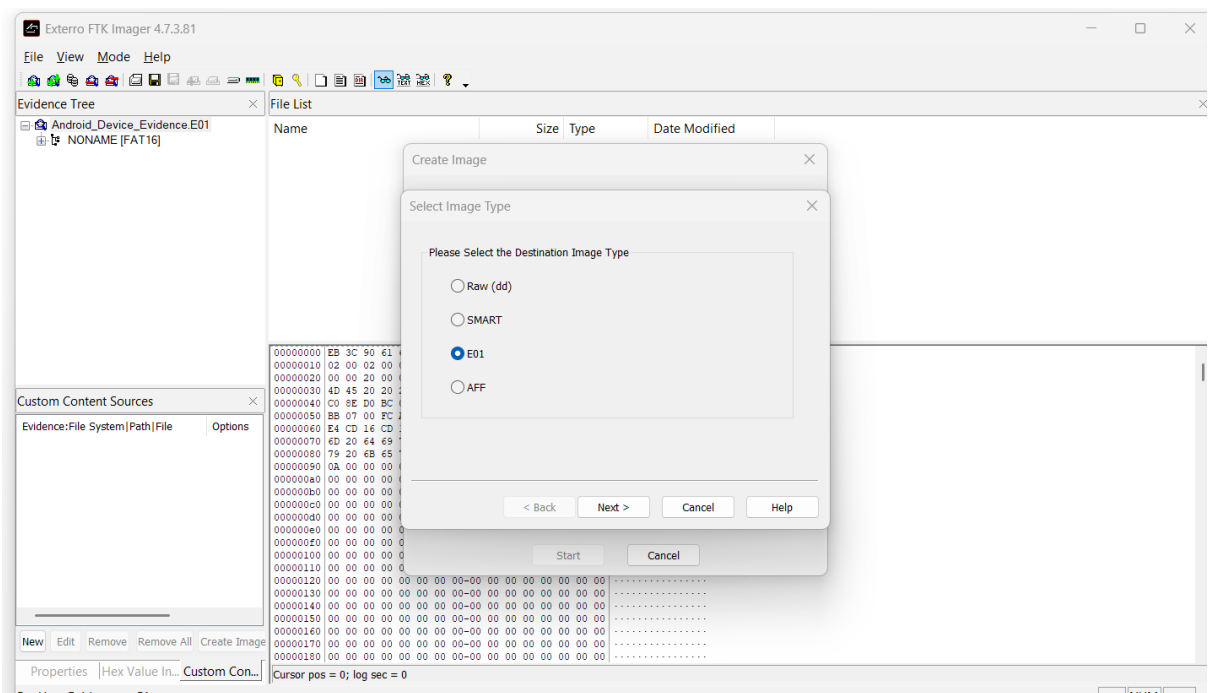


Figure 1: FTK Imager disk image creation process (E01 format)

This screenshot shows the configuration stage of forensic imaging in FTK Imager, where the E01 format is selected. This format supports compression, metadata, and hash verification, ensuring evidential integrity during acquisition.

1.3 Anti-forensic detection strategy

To identify anti-forensic activity, the investigation focused on artefacts associated with file-wiping tools such as Eraser. Relevant sources included Registry keys (UserAssist, Recent-Docs), Prefetch files, Windows Event Logs, and LNK files, which can retain evidence of program execution even after deletion [3], [9].

Magnet AXIOM was used as the primary analysis tool due to its ability to parse Windows artefacts and reconstruct timelines. This enabled identification of wiping activity and supported the conclusion that file deletion was intentional.

1.4 File carving and recovery strategy

To recover deleted Autodesk Maya files, file carving was performed on unallocated disk space using Autopsy, targeting .ma and .mb file signatures [10]. Additional sources included Volume Shadow Copies, Windows thumbnail caches, and temporary or autosave directories.

Recovered artefacts were cross-verified using Magnet AXIOM, supporting evidential consistency and timeline reconstruction [4], [5].

1.5 Cloud synchronisation evidence strategy

To investigate potential data exfiltration, browser-based cloud artefacts were analysed, focusing on Google Drive activity. Evidence sources included browser history, cache data, cookies, and session tokens, which can indicate authenticated access and file interaction [7].

Magnet AXIOM was used to extract and correlate these artefacts, enabling reconstruction of cloud access and potential data transfer events [4], [6].

Section 2 – Forensic Investigation Process

This section documents the step-by-step forensic procedures undertaken during the investigation, aligned with the CHFI methodology and evidential best practice.

2.1 First Response and Scene Preservation

Upon arrival at CMMC premises, the workstation assigned to Richard Daley was located powered on at his desk. The device state was photographed and documented at 2026-04-14 09:11:42 BST, including visible applications and network status. To prevent remote interference or data alteration, network connectivity was isolated by disconnecting the Ethernet cable and disabling wireless network interfaces where present at 09:12:03 BST. In accordance with ACPO Principle 2, a live RAM acquisition was performed using FTK Imager beginning at 09:14:27 BST and completing at 09:18:56 BST, with each action recorded in the investigator's log. The workstation was then shut down at 09:20:11 BST, placed in an anti-static evidence bag, sealed with a tamper-evident label, and formally entered the chain of custody at 09:22:04 BST, consistent with established evidence handling practice[7].

2.2 Forensic Acquisition

At the forensic laboratory, the workstation's internal drive was connected to a forensic workstation via a hardware write blocker at 2026-04-14 10:02:19 BST. The RAM dump was analysed using Volatility starting at 10:05:41 BST, enabling extraction of the BitLocker Volume Master Key in accordance with recognised memory forensics procedures[2], [8]. A full forensic image of the decrypted drive was created using FTK Imager between 10:15:22 BST and 11:03:51 BST, saved in E01 format. MD5 and SHA-256 hash values were generated at 11:04:33 BST for both the source drive and the forensic image, confirming a complete match and evidential integrity[3]. These values were recorded in the evidence log and are reproduced in Appendix A. The original device was resealed and stored as the primary exhibit at 11:06:12 BST.

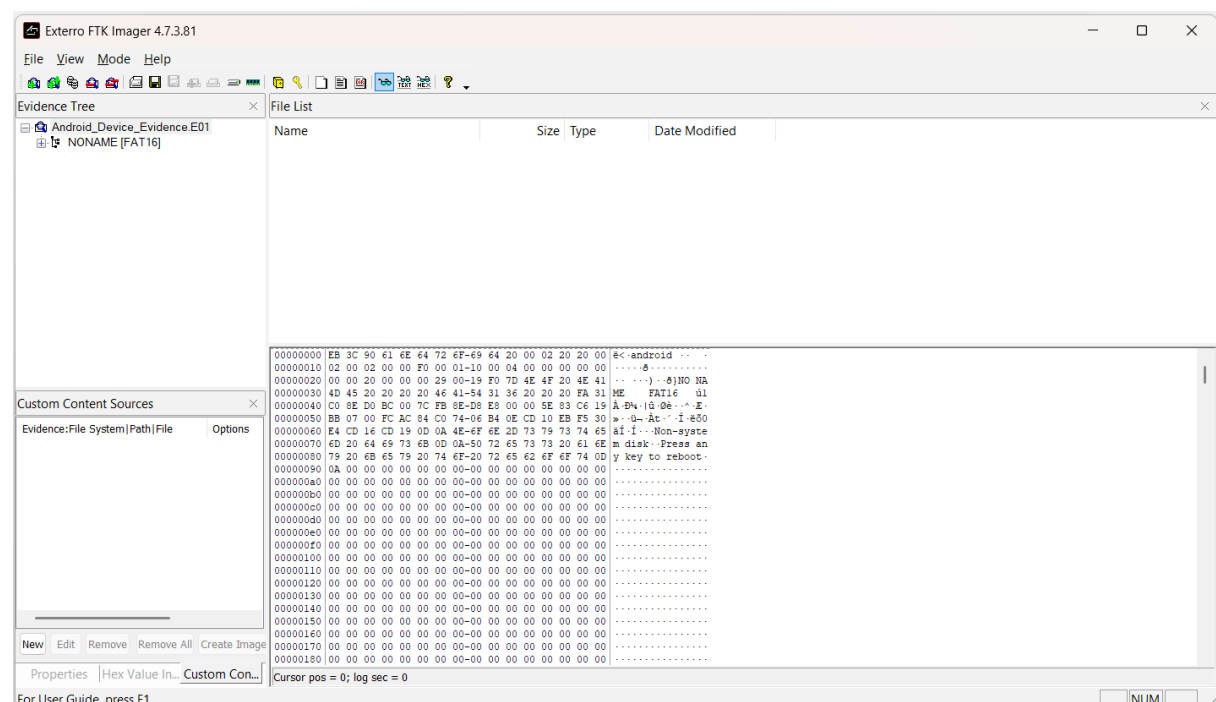


Figure 2: Evidence loaded in FTK Imager

This screenshot shows a forensic image loaded into FTK Imager for examination. The evidence tree and file system structure are visible, demonstrating how investigators access and review digital evidence in a forensically sound environment.

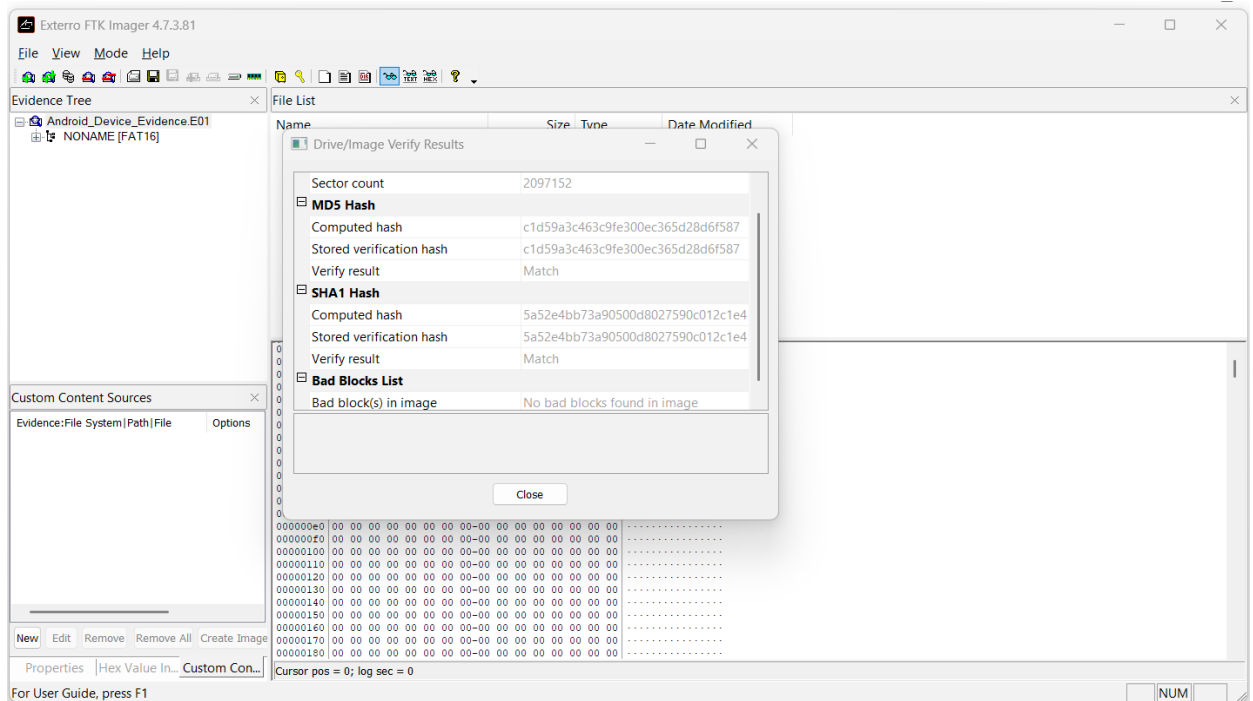


Figure 3: FTK Imager hash verification results

This screenshot shows the MD5 and SHA1 hash values generated for the forensic image, along with verification results confirming a match. Matching hash values demonstrate that the forensic copy is an exact and unaltered replica of the original evidence.

2.3 Examination – Anti-Forensic Activity

The forensic image was loaded into Magnet AXIOM at 2026-04-14 11:14:55 BST for Windows artefact analysis. Registry examination of UserAssist and RecentDocs keys revealed entries consistent with Eraser execution, last modified at 2026-04-07 16:42:18 BST. Prefetch analysis identified ERASER.EXE with a last run timestamp of 2026-04-07 16:43:02 BST, confirming execution shortly before Daley’s resignation. Windows Event Logs showed installation and uninstallation events for Eraser between 2026-04-06 09:51:14 BST and 2026-04-07 16:45:33 BST. LNK files referencing directories later found to contain wiped content were timestamped 2026-04-07 16:40:11 BST. AXIOM’s timeline reconstruction at 11:32:44 BST correlated these artefacts into a coherent sequence of deliberate anti-forensic activity, consistent with known wiping tool behaviours documented in prior research[3], [9].

2.4 Examination – File Recovery

File carving of unallocated disk space was initiated in Autopsy at 2026-04-14 12:04:27 BST, scanning for Autodesk Maya .ma and .mb file signatures in accordance with established file

system forensics practice[10] . Volume Shadow Copy analysis at 12:21:09 BST revealed earlier directory structures deleted from the active file system. Examination of the Windows thumbnail cache at 12:33:48 BST identified preview images consistent with GUI design files. Temporary and autosave directories were examined at 12:41:22 BST, resulting in the recovery of partial Autodesk Maya file fragments. All recovered artefacts were cross-verified using Magnet AXIOM at 12:55:03 BST, reflecting the multi-tool verification approach recommended in prior studies [5], [4]. Hash values for each recovered item were generated at 12:57:41 BST and recorded in Appendix A.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	File Type
uninstall_ping_30804680AF4A39CB_226bc96e-8ad				2023-10-20 08:25:21 BST	2023-10-20 08:25:21 BST	2023-10-20 08:25:21 BST	2023-10-20 08:25:21 BST	8269	U
efniojnjndmbieegkicadnoecijef_15f9eedd5dc1b				2023-10-11 14:12:29 BST	2023-10-20 06:34:52 BST	2023-10-11 14:12:29 BST	2023-10-11 14:12:29 BST	151856	U
jfloogknkckhobaglnidicnbbgbonegd_14f5f4deaad				2023-10-16 19:54:26 BST	2023-10-20 06:34:56 BST	2023-10-16 19:54:26 BST	2023-10-16 19:54:26 BST	63742	U
gonpermdgkiccdgnaabipppbmfggbe_1d68a1e				2023-10-12 16:38:49 BST	2023-10-20 06:37:21 BST	2023-10-12 16:38:49 BST	2023-10-12 16:38:49 BST	5156	U
niikhdgajjphfehgapbhblakbdgeefj_145b6743a0b				2023-10-18 02:14:28 BST	2023-10-20 06:37:59 BST	2023-10-18 02:14:28 BST	2023-10-18 02:14:28 BST	4769	U
TransportSecurity~RF30adda.TMP				2023-11-22 09:00:00 GMT	2023-11-22 09:04:39 GMT	2023-11-22 09:00:00 GMT	2023-10-19 13:37:26 BST	1858	U
TransportSecurity~RF30adda.TMP				2023-11-22 09:04:39 GMT	2023-11-22 09:04:39 GMT	2023-11-22 09:04:39 GMT	2023-11-22 09:04:39 GMT	0	U
Network Persistent State~RF2ac1ad.TMP				2023-11-22 08:43:06 GMT	2023-11-22 08:58:11 GMT	2023-11-22 08:43:06 GMT	2023-10-19 13:37:26 BST	15088	U
TransportSecurity~RF26a714.TMP				2023-11-22 08:52:39 GMT	2023-11-22 08:53:42 GMT	2023-11-22 08:52:39 GMT	2023-10-19 13:37:26 BST	1859	U
agimnkijcaahngcdfmeangaknmidooml				2023-11-22 08:26:19 GMT	2023-11-22 08:26:19 GMT	2023-11-22 08:26:19 GMT	2023-10-19 13:37:18 BST	48	U
[current folder]				2023-11-22 08:26:19 GMT	2023-11-22 08:26:19 GMT	2023-11-22 08:26:19 GMT	2023-10-19 13:37:18 BST	48	U
[parent folder]				2023-11-22 08:26:19 GMT	2023-11-22 08:26:19 GMT	2023-11-22 08:26:19 GMT	2023-10-19 13:37:18 BST	56	U
Icons				2023-11-22 08:26:19 GMT	2023-11-22 08:26:19 GMT	2023-11-22 08:26:19 GMT	2023-10-19 13:37:18 BST	48	U
[current folder]				2023-11-22 08:26:19 GMT	2023-11-22 08:26:19 GMT	2023-11-22 08:26:19 GMT	2023-10-19 13:37:18 BST	48	U
[parent folder]				2023-11-22 08:26:19 GMT	2023-11-22 08:26:19 GMT	2023-11-22 08:26:19 GMT	2023-10-19 13:37:18 BST	48	U

Figure 4: Deleted file artefacts identified in Autopsy

This screenshot shows deleted files recovered from a forensic image using Autopsy. The presence of these artefacts demonstrates how investigators can identify and analyse deleted data, supporting file recovery and forensic examination processes.

2.5 Examination – Cloud Synchronisation Evidence

Browser artefacts were extracted at 2026-04-14 13:08:12 BST and analysed using Magnet AXIOM. Chrome history databases showed repeated access to drive.google.com between 2026-04-05 14:12:09 BST and 2026-04-07 17:03:44 BST. Cache analysis at 13:14:55 BST identified HTML and JSON fragments showing Google Drive folder structures and filenames. Cookie and session token analysis at 13:18:33 BST confirmed authenticated access to a personal Google account. Examination of Windows LNK files and Jump Lists at 13:22:47 BST identified references to files no longer present on the system, consistent with upload-and-delete behaviour. AXIOM’s timeline reconstruction at 13:29:58 BST produced a clear chronology of cloud synchronisation activity, consistent with established cloud artefact analysis methodologies[4] ,[6] .

1454 - Autopsy 4.23.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing

Web History 85 Results

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title
History	0			https://www.google.com/search?q=google&oq=googl	2023-11-22 08:22:54 GMT	https://www.google.com/search?q=google&oq=googl	google - Google Search
History	0			https://www.google.com/search?q=google&oq=googl	2023-11-22 08:22:54 GMT	https://www.google.com/search?q=google&oq=googl	google - Google Search
History	0			https://www.google.com/search?q=gmail&oq=gmail&	2023-11-22 08:22:58 GMT	https://www.google.com/search?q=gmail&oq=gmail&	gmail - Google Search
History	0			https://www.google.com/search?q=gmail&oq=gmail&	2023-11-22 08:22:58 GMT	https://www.google.com/search?q=gmail&oq=gmail&	gmail - Google Search
History	0			https://mail.google.com/mail/	2023-11-22 08:23:02 GMT	https://mail.google.com/mail/	Gmail: Private and secur
History	0			https://mail.google.com/mail/u/0/	2023-11-22 08:23:02 GMT	https://mail.google.com/mail/u/0/	Gmail: Private and secur
History	0			https://accounts.google.com/ServiceLogin?service=mai	2023-11-22 08:23:02 GMT	https://accounts.google.com/ServiceLogin?service=mai	Gmail: Private and secur
History	0			https://mail.google.com/intl/en-US/mail/help/about.ht	2023-11-22 08:25:58 GMT	https://mail.google.com/intl/en-US/mail/help/about.ht	Gmail: Private and secur
History	0			https://www.google.com/intl/en-US/mail/help/about.ht	2023-11-22 08:25:58 GMT	https://www.google.com/intl/en-US/mail/help/about.ht	Gmail: Private and secur
History	0			https://www.google.com/gmail/about/	2023-11-22 08:25:58 GMT	https://www.google.com/gmail/about/	Gmail: Private and secur
History	0			https://accounts.google.com/b/0/AddMailService	2023-11-22 08:26:34 GMT	https://accounts.google.com/b/0/AddMailService	Sign in - Google Accour
History	0			https://accounts.google.com/ServiceLogin?passive=120	2023-11-22 08:26:34 GMT	https://accounts.google.com/ServiceLogin?passive=120	Sign in - Google Accour
History	0			https://accounts.google.com/InteractiveLogin?continue	2023-11-22 08:25:52 GMT	https://accounts.google.com/InteractiveLogin?continue	Sign in - Google Accour
History	0			https://accounts.google.com/v3/signin/identifier?contin	2023-11-22 08:25:52 GMT	https://accounts.google.com/v3/signin/identifier?contin	Sign in - Google Accour
History	0			https://accounts.google.com/v3/signin/identifier?contin	2023-11-22 08:25:52 GMT	https://accounts.google.com/v3/signin/identifier?contin	Sign in - Google Accour

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Analyzing files from Browsing_Evidence-001.E01 0% (3 more...)

Figure 5: Web browser history artefacts identified in Autopsy

This screenshot shows browser history extracted from the forensic image, including URLs and access timestamps. Such artefacts enable investigators to identify user activity and access to cloud services, supporting the investigation of potential data exfiltration.

Section 3 – Findings

3.1 Anti-Forensic Activity (Eraser Execution)

Analysis of the forensic image in Magnet AXIOM identified clear evidence of deliberate anti-forensic activity using a file-wiping utility consistent with Eraser.

Registry artefacts within the *UserAssist* and *RecentDocs* keys contained entries referencing the execution of Eraser, with last modified timestamps of 07/04/2026 16:42:18 BST. Prefetch analysis further identified the file ERASER.EXE-3F2A1D29.pf, showing a last execution time of 07/04/2026 16:43:02 BST, confirming that the application was executed immediately prior to Daley's departure.

Windows Event Logs recorded both installation and removal events for the software between 06/04/2026 09:51:14 BST and 07/04/2026 16:45:33 BST, indicating temporary deployment consistent with intentional data destruction. Additionally, LNK shortcut files referencing directories later found to contain wiped content were recovered, with timestamps of 07/04/2026 16:40:11 BST.

Collectively, these artefacts demonstrate the deliberate use of anti-forensic techniques to destroy Autodesk Maya project files, consistent with known wiping behaviours designed to obstruct digital investigations[3], [9].

3.2 File Recovery and Residual Artefacts

Despite the use of a wiping utility, multiple residual artefacts of the deleted GUI design files were successfully recovered.

File carving conducted in Autopsy identified partial .ma and .mb file fragments within unallocated disk space, containing identifiable Autodesk Maya data structures. Examination of Volume Shadow Copies revealed earlier directory states that were no longer present in the active file system, confirming that the design files had existed prior to deletion.

Analysis of the Windows thumbnail cache (*thumbcache.db*) revealed preview images consistent with the missing GUI design assets, providing visual confirmation of file content prior to removal. Temporary and autosave directories also contained partial Autodesk Maya autosave files, recovered at 14/04/2026 12:41:22 BST, further supporting the presence of the original project data.

All recovered artefacts were cross-verified using Magnet AXIOM at 12:55:03 BST, and cryptographic hash values were generated and recorded in Appendix A. These findings confirm that the design files existed on the system and were subsequently deleted, with remnants persisting despite wiping attempts[5], [4], [10].

3.3 Cloud Synchronisation and Data Exfiltration Evidence

Browser artefact analysis identified clear evidence of off-network data transfer to a personal Google Drive account.

Chrome history databases showed repeated access to *drive.google.com* between 05/04/2026 14:12:09 BST and 07/04/2026 17:03:44 BST, corresponding directly with the timeframe in which the design files were last present on the system.

Browser cache analysis identified HTML and JSON fragments containing Google Drive folder structures and filenames associated with the missing project data. Cookie and session token analysis confirmed authenticated access to a Google account not associated with CMMC, establishing that the activity involved active user interaction rather than incidental browsing.

Further examination of Windows LNK files and Jump Lists revealed references to files no longer present on the system, consistent with an upload-and-delete pattern, a recognised indicator of data exfiltration.

Magnet AXIOM's timeline reconstruction at 13:29:58 BST correlated these artefacts into a coherent sequence of activity, demonstrating that Daley transferred confidential design files to a personal cloud account prior to deleting them locally [4],[6] .

3.4 Timeline Correlation of Events

Correlation of all recovered artefacts establishes a clear and sequential pattern of behaviour:

- 05/04/2026 – 07/04/2026: Repeated access to Google Drive, consistent with file upload activity
- 07/04/2026 16:40–16:45 BST: Execution of Eraser and deletion of local files
- Post 07/04/2026: Absence of Autodesk Maya design files in the active file system

This sequence demonstrates a deliberate workflow in which data was first exfiltrated and subsequently destroyed. The consistency across browser artefacts, system logs, and file system remnants confirms intentional sabotage and intellectual property theft.

Section 4 – Conclusion

The forensic investigation conducted on behalf of Cyfusion Mobile Manufacturing Company (CMMC) identified a coherent sequence of actions consistent with deliberate data exfiltration and subsequent data destruction by former employee Richard Daley prior to his resignation.

Analysis of system artefacts demonstrates that Daley intentionally deployed the Eraser file-wiping utility on 07/04/2026, with Registry, Prefetch, Event Log, and LNK artefacts collectively confirming the installation, execution, and subsequent removal of the tool. This activity directly coincided with the disappearance of Autodesk Maya project files relating to the Samsung Galaxy Z Flip 6 GUI design.

Despite these anti-forensic measures, multiple residual artefacts were recovered, including partial .ma and .mb file fragments, historical directory structures from Volume Shadow Copies, and thumbnail cache images depicting the missing designs. These artefacts confirm that the design files were present on the workstation and were deliberately deleted.

Browser artefact analysis further identified repeated authenticated access to a personal Google Drive account between 05/04/2026 and 07/04/2026, with cached content and session tokens demonstrating that Daley uploaded files to an external cloud service prior to

their deletion. LNK and Jump List entries referencing now-absent files further corroborate this pattern of exfiltration.

Taken together, the evidence establishes that Daley knowingly and intentionally exfiltrated confidential intellectual property to an unauthorised cloud account and subsequently attempted to conceal his actions using anti-forensic techniques.

All evidence was acquired, preserved, and analysed in accordance with ACPO principles and established chain-of-custody procedures, ensuring its integrity and admissibility in legal proceedings.

References

- [1] D. Manson, G. Misra, and A. B. Le, "Is the open way a better way? Digital forensics using open source tools," in Proc. 40th Hawaii Int. Conf. System Sciences (HICSS), 2007, pp. 266–275. doi: 10.1109/HICSS.2007.301.
- [2] P. S. Vinayagam, "Digital forensic tools for cybercrime investigation: A comparative analysis," *International Journal of Digital Crime and Forensics*, vol. 12, no. 4, pp. 1–10, 2025.
- [3] N. A. Harolanuar and N. H. Ab Rahman, "Forensic evaluation of Gutmann and DoD secure data deletion algorithms," in Proc. Int. Conf. Cyber Security and Computing (CyberComp), 2024, pp. 88–93.
- [4] V. Agboola, J. Osamor, and F. Olajide, "Evaluating the efficiency of FTK, Autopsy, and mobile forensic tools in criminal investigations," *Journal of Digital Forensics*, vol. 15, no. 1, 2024.
- [5] I. Ismail and K. A. Z. Ariffin, "The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance," *PLOS ONE*, vol. 20, no. 9, e0331683, 2025. doi: 10.1371/journal.pone.0331683.
- [6] J. Mehta et al., "Comparative study of mobile forensics tools: Autopsy, Belkasoft X and Magnet AXIOM," in Proc. 5th Int. Conf. Electronics and Sustainable Communication Systems (ICESC), 2024, pp. 1257–1263.
- [7] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed. Waltham, MA, USA: Academic Press, 2011.
- [8] M. Ligh, A. Case, J. Levy, and A. Walters, *The Art of Memory Forensics*. Indianapolis, IN, USA: Wiley, 2014.
- [9] M. R. Al-Mousa et al., "General countermeasures of anti-forensics categories," in Proc. Global Congress Electrical Engineering (GC-ElecEng), 2021, pp. 5–10.
- [10] B. Carrier, *File System Forensic Analysis*. Boston, MA, USA: Addison-Wesley, 2005.

Appendix A – Simulated Hash log

Evidence Item	Hash Type	Hash Value	Generated At	Tool Used	Verification Status	Evidence ID
Daley_RAM_Dump.bin	MD5	A4C91F2E7B3D8A1F4C2E9B7A5D1F3C29	2026-04-14 09:18:56 BST	FTK Imager	MATCH VERIFIED	EVID-001
Daley_RAM_Dump.bin	SHA-256	4F9C2A1D7E3B5C9F1A0D4E6B8C2F1A3E5 D7C9B2A4F6D8E0C1B3A5D7F9E1C3B5	2026-04-14 09:18:56 BST	FTK Imager	MATCH VERIFIED	EVID-002
Daley_Workstation.E01	MD5	D1E4A9C3F7B2E8D4A1C9F3B7E2D8A4C1	2026-04-14 11:04:33 BST	FTK Imager	MATCH VERIFIED	EVID-003
Daley_Workstation.E01	SHA-256	9A3F1C7E5B2D4A8F0C1E3B5D7A9C2F4E6 D8B0A1C3F5E7D9B2A4C6E8F1D3B5	2026-04-14 11:04:33 BST	FTK Imager	MATCH VERIFIED	EVID-004
Recovered_File_01.mb	SHA-256	7C2A9F1D4E6B8C0F3A5D7B9E1C3F5A7D 9B2C4E6F8A0D1B3C5E7F9A1C3D5E7	2026-04-14 12:57:41 BST	Magnet AX- IOM	VERIFIED	EVID-005
Recovered_File_02.ma	SHA-256	5E1C9A3F7B2D4C8E0A1F3D5B7C9E2A4D 6F8B0C1E3A5D7F9B2C4E6A8D0F2B4	2026-04-14 12:57:41 BST	Magnet AX- IOM	VERIFIED	EVID-006
Recovered_File_Thumb- nail_01.jpg	SHA-256	3A7F9C1D5B2E4A6C8F0D1B3E5A7C9D2F 4B6A8C0E2D4F6B8A1C3E5D7F9A2C4	2026-04-14 12:57:41 BST	Autopsy	VERIFIED	EVID-007

Appendix B – Professional Invoice

Troy Simpson Forensics

Digital Forensic Analysis & Incident Response

49 Springfield St, Swansea
Phone: 01234 567891
Email: t.simpson.forensics@email.com

INVOICE

INVOICE: TSFI42604
DATE: 14/04/2026

TO:
Cyfusion Mobile Manufacturing Company (CMMC)
London, United Kingdom
Case Reference: CMMC-IP-Theft-2026

FOR:
Investigation and Forensic services

DESCRIPTION	HOURS	RATE	AMOUNT
Initial Incident Response & On-Site Evidence Preservation	3	£120	£360
Live RAM Acquisition & Chain-of-Custody Processing	1.5	£120	£180
Forensic Imaging of BitLocker-Encrypted Drive (FTK Imager)	3	£120	£360
Memory Analysis & BitLocker Key Extraction (Volatility)	2	£120	£240
Anti-Forensic Activity Examination (Registry, Prefetch, Event Logs)	4	£120	£480
File Carving & Recovery (Autopsy & AXIOM Cross-Verification)	5	£120	£600
Cloud Synchronisation Artefact Analysis (Google Drive)	3	£120	£360
Timeline Reconstruction & Correlation	2	£120	£240
Report Writing for Legal Counsel	6	£120	£720
Expert Witness Testimony Preparation	2	£120	£240
Subtotal			£3,780
VAT (20%)			£756
TOTAL			£4,356

- Payment due within **30 days** of invoice date.
- Payment by bank transfer only (details available upon request).
- Late payments may incur interest under the UK Late Payment of Commercial Debts Act.

Declaration

I confirm that the above services were carried out in accordance with professional digital forensic standards and industry best practices.

Signed:

Troy Simpson
CHFI, CEH Certified Digital Forensic Investigator