

ACCD5000 Synthesize a solution to a potential real-life scenario

2421062

Hasan Sivas

Task 1 - Research	2
Introduction	2
1. Main:	2
1.1 Acquisition & Evidence Integrity	4
1.2 Examination & Analysis	4
1.4 Cost	6
1.5 Conclusion	6
Task 2 - Case study: sabotage	7
Introduction	7
2.1 Forensic Methodology and Investigation Plan	7
2.2 Professional Forensic Report	10
2.2.1 Investigative Steps	11
2.2.3 Findings	12
2.2.4 Conclusion	14
Appendix: Simulated Hash Log	14
Invoice	14
Sources:	15

Task 1 - Research

Introduction

As computer-based crimes become more and more common, the need for proper adherence to established computer forensic investigation procedures and the use of appropriate forensics tools grows more and more important. This report will aim to present an evaluation focusing mostly on four major modern forensic tools: FTK Imager, Magnet AXIOM, Autopsy and Cellebrite UFED. The aim of the report is not to put down one tool as ultimately better than or worse than the other, as in the modern-day landscape, the usage of multiple tools is required. The aim of the report will be to elucidate which tool is most suitable for what scenario and obstacle during the Computer Hacking Computer Hacking Forensic Investigator (CHFI) stages by covering: their strengths and weaknesses, the obstacles they are suited to, their cost, key features, supported file systems, types of evidence analysed, and their reporting capabilities.

1. Main:

The field of digital forensics has undergone significant growth, specialisation and evolution over the past decades, necessitated by the ever-evolving threat landscape and available technologies. Early investigations were conducted using

command-line tools and manual analysis, but with the proliferation of digital devices and the increasing complexity of data, sophisticated software tools have become indispensable. These tools automate tedious tasks, enhance analytical capabilities, and ensure the integrity of evidence. An important aspect of digital forensics is that it involves not just the acquisition, preservation and analysis of digital evidence of crimes, but must also be done with reproducibility and admissibility for legal proceedings[1]. A foundational principle underpinning digital forensics is also that the tools selected must be reliable, verifiable, and appropriate for the specific category of evidence under examination, as courts will not accept evidence from just any tool.

An important defining feature is the distinction between open source and commercial use tools. Open-source tools, such as Autopsy and CAINE, are free, modifiable, and benefit from community-driven development, allowing them to rapidly update to new and emerging threats. Their transparency can enhance trust in their methodologies, as their code can be scrutinised. However, they may lack the polished user interfaces, extensive support, and advanced features often found in commercial tools. Commercial tools, such as Magnet AXIOM, Exterro FTK, and Cellebrite UFED, typically offer comprehensive functionalities, professional support, and regular updates, but can often be very expensive and require ongoing

subscriptions [2]. Prices can also change year to year.

	FTK Imager	Exterro FTK	Autopsy	Cellebrite	Magnet AXIOM
Purpose	Imaging	All-in-One-Suite	All-in-One-Suite	Mobile Forensics	Multi-source evidence analysis and correlation
Commerciality	Commercial	Commercial	Open Source	Commercial	Commercial
Cost	Free	High ~£4,000 a year	Free	Very high, Many packages at different prices. E.g. 10k for 30 unlocks.	High, Various subscription levels ~£4,000 for a one-year license
Key Features	Disk Imaging, hashing, evidence preview, and memory capture	Fast Indexing, keyword search, data carving, decryption, case management, reporting	Timeline analysis, keyword search, hash filtering, and deleted file recovery	Extraction, Password bypassing, deleted data recovery, case management	Artefact parsing, timeline correlation, reporting
Platforms	Windows	Windows	Windows, Linux, macOS	Windows	Windows
Media	HDD, SDD, USB, disk images, RAM dumps	NTFS, FAT, exFAT, EXT, HFS+, APFS, disk images, email, mobile backup, cloud artefacts	NTFS, FAT, exFAT, EXT, HFS+, Disk images, mobile images, system logs	IOS, Android, Windows Phone, BlackBerry file systems	NTFS, FAT, exFAT, APFS, EXT4, SMS messages, call logs, app data, documents
CHFI Stage	Aquisition	Examination & Analysis + Reporting	Examination & Analysis	Aquisition	Examination, Analysis, Reporting

Figure 1: Comparison table showing the various features of four key tools: FTK, Autopsy, Magnet AXIOM and Cellebrite.

1.1 Acquisition & Evidence Integrity

The acquisition stage is fundamental to computer forensics investigations; if evidence is any way tampered with without being properly documented in the chain of custody, the evidence may not be admissible in court (for this reason, analysis is done on extracted images of the suspect device, not on the actual device. Imaging is done in read-only mode to prevent alteration). Likewise, the data that is available to be analysed depends entirely on the data can be collected. This makes the acquisition stage the fundamental foundation on which the whole CHFI investigation process depends on.

FTK Imager is a well-known and widely accepted as a reliable and standard tool for disk imaging and memory capture. It allows investigators to make forensic images which can be run as virtual machines to conduct investigations on a copy of the system, all whilst leaving the actual device untouched. Images are generated in the E01 format. FTK also incorporates hash values (e.g. MD5, SHA-1) that allow the investigator to compare if the files have been in any way changed and reduce the risk of accidental evidence tampering. This helps ensure that the final report will be admissible in court[1]. It's ease of use also marks it suitable for beginners and students.

Cellebrite UFED(Universal Forensics Extraction Device) is another well-known extraction tool. Unlike FTK, Cellebrite is designed for acquiring evidence from mobile devices. Cellebrite's ability to perform physical, logical, and file system extractions,

including from locked and secured devices makes it a significantly more suitable solution for mobile forensics. Padmanabhan et al. [2] highlight that commercial mobile forensic tools like Cellebrite can outperform many alternative mobile forensics tools (TSK, SIFT, MOBIL) in terms of data extraction depth and device compatibility. This is particularly important given the increasing reliance on smartphones as primary sources of digital evidence.

However, both of these tools have their flaws and cannot support the CHFI process on their own. FTK Image lacks advanced analysis capabilities as it is only intended for images and Cellebrite's prices may make it prohibitive for some investigations. Additionally, their proprietary nature limits transparency compared to more open-source solutions leading to less community documentation.

1.2 Examination & Analysis

The examination and analysis stage involves processing acquired data to extract evidence that can be used to make deductions or form conclusions. This is where tools such as Exterro FTK, Autopsy, and Magnet AXIOM may be employed.

Exterro FTK is a well-established commercial forensic suite that is known for its powerful indexing and search capabilities. FTK enables investigators to rapidly process large volumes of data and perform keyword searches, email analysis, and data carving, keeping things well organised using its case-manager feature.

Its ability to handle complex datasets efficiently makes it suitable for enterprise-level investigations. However, its cost and steep learning curve may limit accessibility for smaller organisations.

Autopsy can be considered an open-source alternative to versatile commercial all-in-one tools like Exterro FTK and Magnet AXIOM. Autopsy provides a comprehensive set of analysis features, including timeline reconstruction, keyword searching, hash filtering, and file recovery. Delija et al. [3] emphasise the effectiveness of Autopsy in educational environments, particularly when integrated with artificial intelligence techniques to enhance forensic analysis. Its modular architecture allows for extensibility, enabling investigators to add plugins for specific tasks. Thanks to its open source nature, autopsy's usage is also very well documented.

However, despite its advantages, Autopsy has some limitations compared to commercial tools. It may lack the advanced automation and artefact parsing capabilities found in solutions like Magnet AXIOM. Additionally, performance issues can arise when handling very large datasets or operating on weaker devices.

Magnet AXIOM is a potentially very useful analysis tool, particularly in its ability to correlate data across multiple sources. It supports analysis of computer systems, mobile devices, and cloud platforms within a single interface. AXIOM excels in artefact recovery and user activity reconstruction[4], making it highly effective for modern investigations involving diverse data sources. Its timeline feature allows investigators to visualise events across devices, providing a holistic view of user behaviour.

Mehta et al. [4]'s study compared Autopsy, Belkasoft X, and Magnet AXIOM against forensic image files from Android 10, iOS 13, and iOS 14 platforms. They found that no single tool dominated across all artefact categories. Magnet AXIOM recovered the highest number of picture and document artefacts on iOS devices, while Belkasoft X uniquely identified encrypted files and led in installed-application enumeration. Autopsy, despite being open-source, performed competitively on browser history extraction but lagged on call records and SMS recovery for Android. These show that multi-tool approaches are still the most suitable practise.

1.3 Mobile and Cloud Forensics

With the increasing use of mobile devices and cloud services, forensic investigations no longer centre solely on investigating desktop or laptop computers seized from suspects. Mobile forensics has received growing attention as smartphones increasingly store the most forensically significant evidence[2]. When it comes to mobile analysis, Cellebrite UFED and Magnet AXIOM are particularly relevant.

Cellebrite UFED is primarily focused on mobile acquisition, but it also offers analysis capabilities through its associated software (e.g., Physical Analyser). It supports a wide range of devices and operating systems, making it a versatile tool for mobile investigations.

Padmanabhan et al. [2] performed a cross-device comparative study of four tools: Cellebrite UFED Physical Analyser, MOBILedit! Forensic, The Sleuth Kit with Autopsy, and SANS SIFT finding that commercial tools held a strong advantage

over open source tools weight comes to physical extraction and recovery of deleted data from mobile devices.

Magnet AXIOM is in addition to mobile forensics, also suitable for acquiring and analysing data from cloud services such as Google Drive, icloud and various social media platforms. This sort of distributed evidence gathering can often be useful when a case requires a wider breadth of evidence.

Autopsy by itself cannot directly acquire images or evidence from mobile devices or cloud-based evidence, however it is able to work with provided mobile data and disk images in order to construct effective timelines.

1.4 Cost

Price is an important factor when selecting forensics tools. Open source or free tools like Autopsy and FTK Imager can be cost-effective solutions to basic forensics tasks and at times may be suitable to provide a large amount of usable evidence. These tools are especially useful in education settings or to investigators with limited budgets e.g. an in-house investigation for a small company.

Commercial tools such as Exterro FTK, Cellebrite and Magnet AXIOM come with advanced capabilities and up to date functionality but with tend to be considerably expensive. E.g. it is, at the time of writing, £3,897 GBP to acquire a virtual license for FTK that lasts for one year. These prices are suitable and competitive for forensics tools as they are often used occupationally and paid for by companies and

organisations, not individuals. The cost of these tools is reasonable thanks to their performance, reliability and compatibility with a wide range of data types for investigation.

Many different tools may be needed in the forensic process, however, some smaller organisations may need to carefully evaluate their needs and budget accordingly as forensics tools can be very costly. Many forensic investigators use combinations of tools to balance cost and functionality. e.g. using FTK Imager to acquire a device image and then using Autopsy or Magnet AXIOM is for analysing the data. This approach allows investigators to reap the benefits of each tool whilst helping keep costs more reasonable.

1.5 Conclusion

To conclude, no single forensic tool is sufficient on its own. Each tool ultimately has its own strengths and weaknesses that make them more or less suitable for different stages of the investigation and different scenarios. As a result, real-world digital forensics typically involves using multiple tools in combination throughout different stages of the CHFI investigation process.

During the Acquisition and Preservation stages, FTK imager and Cellebrite UFED are very suitable due to their ability to create forensic images and extract data whilst maintaining integrity, thanks to their validation and hashing features.

During the examination and analysis stages, wherein the goal is to comb through the data for evidence, Exterro FTK, Magnet AXIOM and Autopsy provide robust capabilities for organising data and identifying patterns.

Both Magnet AXIOM and Exterro FTK act as all-in-one suites and have features that support the investigation at every stage. They also support case management and reporting, helping investigators produce structured, court-admissible reports that clearly present their findings.

Task 2 - Case study: sabotage

Introduction

This section of the report will focus on the hypothetical sabotage case study wherein Cyfusion Mobile Manufacturing Company (CMMC) has had its designs leaked to a rival company by former employee Rich Daley. The report will detail the methodology & investigation plan and forensic report produced by Troy Simpson, a CHFI certified professional who has been hired by CMMC to investigate the incident.

2.1 Forensic Methodology and Investigation Plan

In order to make sure that the produced evidence is admissible in court, it is important to ensure that procedures adhere strictly to digital forensics principles, such as those outlined by the Association of Chief Police Officers (ACPO). The key aspect that Troy Simpson would have to keep in mind is that all evidence must be preserved and any actions taken to obtain evidence must be documented such that a 3rd party can easily replicate them and obtain the same result [11]. The ACPO guidelines emphasise that no action to change the data held on a device and that access to the original data must be controlled and documented with a clear audit trail. For this reason CHFI investigators maintain a chain of custody during the investigation.

CHAIN OF CUSTODY FORM

Your Logo Here

Your Address Here

[Agency Name] Case #: _____

Item #	Date/Time Removed	Reason for Removal of Evidence	Signature

Example image of a Chain of Custody Form, from [Researchgate](#).

Throughout the investigation, strict adherence to the chain of custody procedures must be followed. Other things to document include date and time of access, the identity of the investigator, and the reason for each action. Without proper adherence to these rules, there is a possibility of claims of tampering or contamination derailing any possibility of legal action[7].

Acquisition Phase:

As outlined in the previous part, the investigation must begin the securing of the evidence as the acquisition of data forms the foundation of the investigation. In this case study, the only device that is seized will be Rich Daley's Window's 11 desktop protected with BitLocker full-disk encryption.

The presence of full-disk encryption presents a significant roadblock in the acquisition phase, as encrypted drives cannot be meaningfully analysed without decrypting them first. Modern forensic research shows that traditional dead acquisition techniques are insufficient in many scenarios, and investigators must attempt to use live acquisition strategies before dead acquisition wherever possible [5] or they risk missing vital context that can be found in more transient data from running processes and cache.

In the best case scenario wherein the system is still powered on at the time of seizure, more data is available in the form of volatile memory which has not yet been lost. It is essential that a live acquisition response approach is used and any volatile data (RAM) is captured whilst it is still available with respect to the order of volatility. Volatile evidence, such as RAM contents, running processes, network connections and logged-in user sessions, can be lost as soon as the device is powered down. In contrast, non-volatile evidence, such as disk contents, file metadata and registry entries, is more persistent. By doing this, it may be possible to obtain the encryption key through RAM, circumventing the need to find Rich Daley's credentials. Ghode et al. demonstrate that RAM capture can be used effectively to extract BitLocker encryption keys, enabling access to otherwise inaccessible data [8].

In a scenario where the device is already powered off at the time of acquisition, the situation is more difficult and alternative means need to be considered in order to acquire usable data. Recent advancements in forensic techniques, such as those described by Assumpção et al.[6], demonstrate that BitLocker volumes protected by Trusted Platform Module (TPM) can be decrypted using hardware debugging interfaces such as Intel Direct Connect Interface (DCI) [6]. Though this method requires specialised hardware and expertise, making it undoubtedly expensive, it is worth the investment in cases such as what CMMC has experienced where there is a possibility of significant financial loss and loss of market viability. Once access to the encrypted portion of data is obtained, a forensic image of the drive must be created using a trusted acquisition tool such as FTK Imager. During the imaging process, the generation of cryptographic hash values (e.g. MD5 and SHA-256) should be used to verify that the integrity of the acquired data remains, ensuring compliance with forensic best practices [5][11].

Examination phase:

Following acquisition, the next stage of investigation is examination: In this stage, the forensic image produced during the first stage is analysed using tools such as Exterro FTK, Autopsy or Magnet AXIOM. Either of these would be suitable due to their ability to process large datasets efficiently and extract notable artefacts from the Windows 11 file system [4].

The examination process involves reconstructing the file system, identifying any deleted files and analysing file metadata to construct an image of the user's activity at the time.

In particular, attention should be paid to the usage of anti-forensics tools, such as the file-wiping software used by Rich Daley. Anti-forensics techniques are behaviours used by cybercriminals to obscure evidence and erase their tracks, as Rich Daley carried out this attack with intention, it is likely a critical component of this investigation. Anti-forensics techniques, especially when done by laymen are not perfect and usually leave traces such as application logs, registry entries and patterns of disk activity[9] which can then be used to infer their use.

To prove the use of wiping tools, the investigation should focus on identifying installed applications and any evidence of their recent usage: Windows registry artefacts, prefetch files and event logs can be used to provide evidence of program execution. Prefetch files are used by Windows OS to speed up application launching by caching data prior to launch. E.g. The presence of a prefetch file associated with the Eraser application could indicate that the program was executed on the system. Further analysis of file system structures could potentially reveal anomalies consistent with secure deletion or patterns indicative of known data wiping algorithms. File deletion tools may leave behind residual fragments (artefacts) such as file headers, if a file header associated with Autodesk Maya project files (.ma or .mb) were to be discovered, it may allow Simpson to identify residual fragments of the project that could be recoverable.

File carving is a key strategy in recovering deleted Autodesk Maya project files and can be handled using FTK. The use of tools such as Autopsy or Magnet AXIOM can also facilitate this process, as they incorporate automated carving algorithms and support a wide range of file formats. File carving involves scanning the raw disk image for file signatures and then reconstructing the files with an interpretation based on known header and footer patterns. Unlike traditional recovery methods, this does not rely on file system metadata such as file allocation tables, but instead analyses the underlying data structures and content within unallocated disk space to identify and rebuild files[12]. This makes file carving particularly effective in situations where metadata has been deleted, corrupted, or intentionally destroyed which is likely the case with the incident at CMMC.

However, its usefulness may be weakened based on the extent of overwriting performed by the wiping tool. If the files have been securely overwritten multiple times, filecarving may not be able to identify many intact fragments and recovery may be limited. Even if they cannot be used, however, partial recovery of file fragments may still provide valuable evidence, particularly if they contain identifiable elements of the missing design work.

In addition to analysis of just the seized device, the investigation should also consider the possibility of data transfer via cloud services such as iCloud, Google Drive, OneDrive or Dropbox. If Rich Daley has synced files to a cloud storage account using a web browser, this activity may be revealed by analysing browser artefacts such as browsing history, cached files, cookies and download records. The analysis tool Autopsy can also be used to easily browse and view uploads and downloads to and from web addresses. Magnet AXIOM also provides detailed analysis of web activity, including access to cloud storage services. Evidence of Google Drive access could be used to support the hypothesis that patent data was transferred to the cloud before it was deleted locally.

The investigation also needs to consider the broader context of Rich Daley's behaviour in the time leading up to his resignation. By looking at the overall activity and taking into account sources such as file timestamps, application logs and network activity, a timeline of events can be constructed. E.g. It may be possible that for certain Daley transferred an item before deleting the pattern. This approach is a key feature of modern digital forensics frameworks, which seek to emphasise the integration of data from multiple sources to construct a detailed understanding of incidents[10], rather than just tying one piece of evidence to a single occurrence.

2.2 Professional Forensic Report

This report presents the findings of the digital forensic investigation into the incident occurring at CMMC wherein a former employee, Rich Daley, is suspected of leaking designs to rival companies before deleting the design from the local device and resigning. The investigation focused on analysing Rich Daley's Windows 11 workstation, which was protected by BitLocker

encryption, to determine whether the designs were intentionally exfiltrated and deleted. Using industry-standard forensic methodology and tools, evidence was recovered indicating the use of file-wiping tools and illegal access to cloud storage services from the company device. Overall the evidence suggests that it was likely that Rich Daley intentionally deleted CMMC's proprietary design files and transferred them to a cloud service prior to resigning.

2.2.1 Investigative Steps

The investigation began with the seizure of the Windows 11 desktop. The device was immediately documented, photographed and assigned a unique identifier. A chain of custody form was initiated to record all subsequent handling of the device. As the computer had not been turned off, and was instead only logged off, a live acquisition approach was used: Volatile memory was captured using a forensic RAM acquisition tool, and a forensic image of the device was immediately obtained.

The forensic image of the system drive was then created using FTK Imager. The imaging process was conducted in a controlled environment, and cryptographic hash values were generated to verify the integrity of the acquired image. The original device was then secured and stored to prevent the possibility of any further modification. Analysis of the memory image revealed the presence of encryption keys making access to the rest of the data possible.

The forensic image was analysed using Extor FTK and the open source forensics tool Autopsy. The analysis focused on identifying deleted files, application usage and evidence of data transfer via the cloud. File system analysis revealed a significant number of deleted files, likely corresponding to Autodesk Maya project files after Rich Daley's resignation based on the header. Although many of these files had been overwritten by the eraser tool, artefacts were recovered using file carving techniques.

Further analysis showed evidence of the usage of the Eraser file-wiping tool on the system, due to the presence of prefetch files that suggested the application was executed in the hours leading up to Daley's resignation. The close timing to the resignation very strongly suggests that the project files were intentionally wiped with possible intention to sabotage CMMC's business.

Browser artefact analysis using autopsy provided evidence of access to Google Drive with the desktop's cached files showing multiple instances of file upload activity. The timestamps of the upload activity date to both several days before and in the morning before the usage of the Eraser file-wiping tool. This suggests that that Rich Daley uploaded the files to Google Drive before deleting them on the desktop.

2.2.3 Findings

The investigation has narrowed down several key pieces of evidence: Analysis of the desktop's installed applications confirmed the installation of a file-wiping tool at some point in time, and prefetch files indicating recent use immediately preceding resignation. Recovered file fragments include portions of Autodesk Maya project files, suggesting that the designs may have been present on the system prior to deletion. Browser artefacts show that Daley accessed and uploaded files to Google Drive multiple times leading up to file deletion.

From these findings, a very clear timeline can be constructed: Rich Daley accessed Google Drive several days prior to the incident and transferred files, then did so again the morning before the incident. After transferring the last files, Daley deleted the designs from the Windows 11 desktop and then several hours later, tendered his resignation. Combined, these activities all strongly hint towards an intentional act of sabotage of company assets.

Timeline correlation is central to the investigation because individual artefacts may be considered ambiguous when viewed in isolation. Google Drive access, deleted Autodesk Maya file fragments and Eraser execution each provide useful evidence, but their evidential value increases when placed in chronological order. If the timeline shows that Rich Daley accessed Google Drive, uploaded or staged files, executed a wiping tool, and then resigned shortly afterwards, the combined pattern be excellent in helping CMMC plead its case.

It is, however, important to recognise the limitations of the investigation. The presence of wiping-tool artefacts and Google Drive browser activity strongly supports the hypothesis of intentional deletion and exfiltration, but these artefacts do not automatically prove the exact contents of every uploaded file unless filenames, cached metadata, recovered fragments or cloud-side records can be correlated.

Evidence ID	Artefact Found	Location / Source	Forensic Meaning
E01	Eraser prefetch file	Windows Prefetch folder	Indicates the wiping tool was executed.
E02	Deleted Autodesk Maya fragments	Unallocated disk space	Suggests Maya design files were present before deletion.
E03	Google Drive browser history	Browser history/cache	Indicates access to personal cloud storage.
E04	Upload-related cached artefacts	Browser cache/session data	Supports possible exfiltration before deletion.
E05	Matching timestamps	Timeline analysis	Shows cloud activity occurred before

			wiping and resignation.
--	--	--	----------------------------

Simple table summarising the main points of evidence

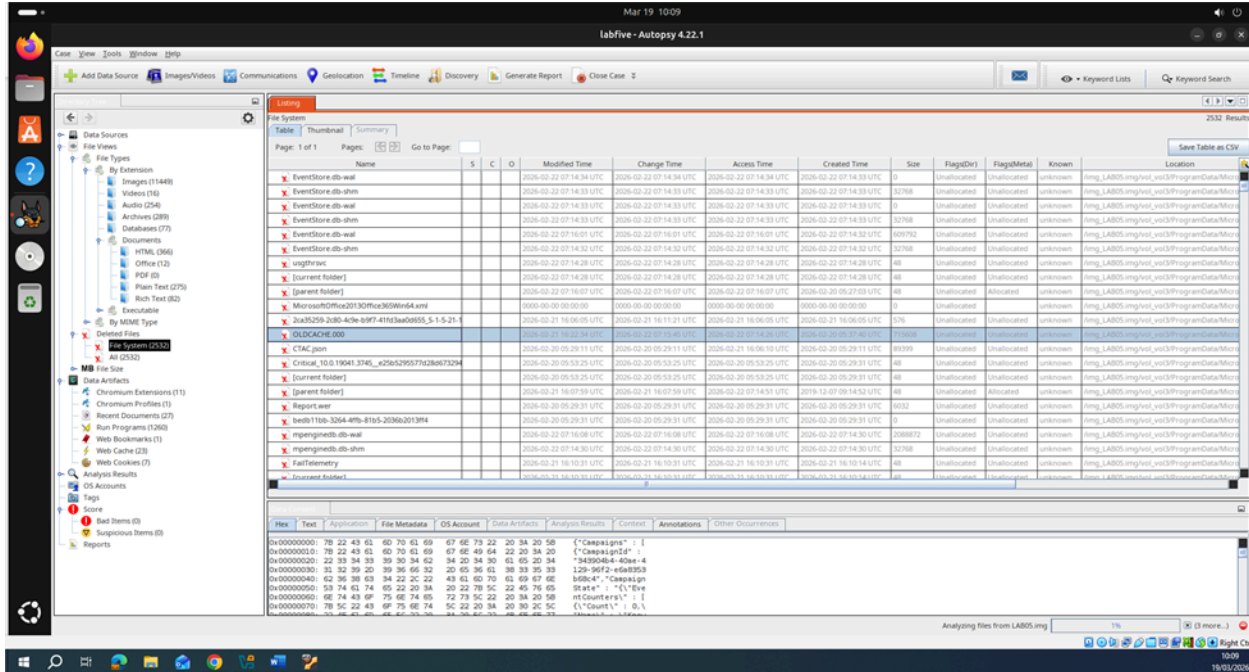
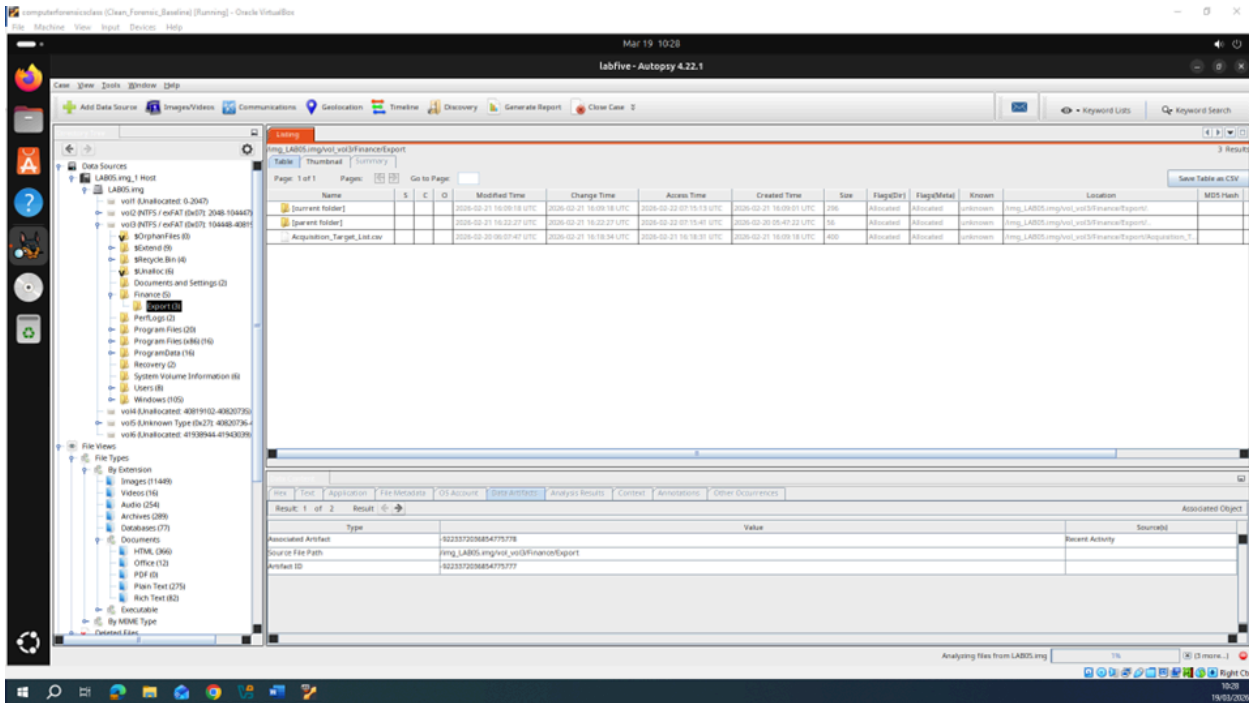
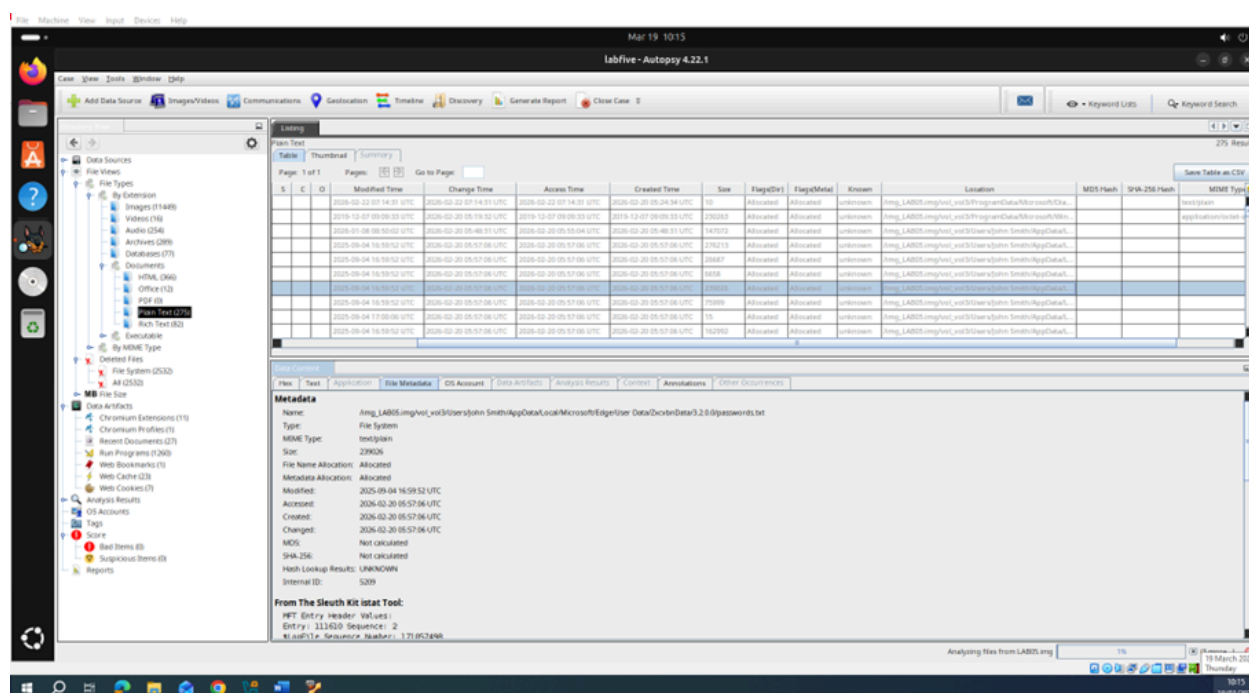


Image1 - View of Autopsy showing deleted files and the time of deletion





Images 2 & 3 - View of Autopsy showing evidence of stanging files for transfer online

2.2.4 Conclusion

The forensic analysis provides strong evidence that Rich Daley may potentially have engaged in deliberate sabotage of CMMC's intellectual property. The use of a file-wiping tool indicates an attempt to permanently destroy evidence, while the presence of cloud storage activity demonstrates the possibility of intentional data exfiltration. These actions could potentially constitute a breach of company policy and may have legal implications, including potential charges of intellectual property theft and corporate espionage.

Appendix: Simulated Hash Log

Evidence Item	Description	MD5 Hash	SHA-256 Hash
EVI1.E01	Disk Image (CMMC Workstation)	d41d8cd98f00b204e9800998ecf8427e	e3b0c44298fc1c149afb4c8996fb924...
EVI2.E01	RAM Dump	0cc175b9c0f1b6a831c399e269772661	2e7d2c03a9507ae265ecf5b5356885a...

Invoice

Troy Simpson Forensics Ltd
London, UK

Invoice Number: 8301238EE

Client: Cyfusion Mobile Manufacturing Company (CMMC)

Service	Hours	Rate (£/hr)	Total (£)
Evidence Acquisition & Imaging	10	150	1500
Forensic Analysis	25	150	3750
Reporting	12	150	1800
Expert Testimony Preparation	8	150	1200

Total Amount Due: £8,250

Sources:

[1] Himanshu, S. Bhatt, and G. Garg, "Comparative analysis of acquisition methods in digital forensics," *IEEE Xplore*, Jul. 01, 2021.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9514970>

[2] R. Padmanabhan, K. Lobo, M. Ghelani, D. Sujan, and M. Shirole, "Comparative analysis of commercial and open source mobile device forensic tools," *IEEE Xplore*, Aug. 01, 2016.

<https://ieeexplore.ieee.org/abstract/document/7880238>

[3] Damir Delija, G. Sirovatka, and Marinko Žagar, "Forensic Analysis of the NIST Hacking Case: Integrating Autopsy Tools and Artificial Intelligence in Teaching Digital Forensics," pp. 1514–1519, May 2024, doi: <https://doi.org/10.1109/mipro60963.2024.10569327>.

[4] J. Mehta, Yash Bhadania, P. Shah, and P. Prajapati, "Comparative Study of Mobile Forensics Tools: Autopsy, Belkasoft X and Magnet Axiom," pp. 1257–1263, Aug. 2024, doi:

<https://doi.org/10.1109/icesc60852.2024.10689971>.

[5] Himanshu, S. Bhatt, and G. Garg, "Comparative analysis of acquisition methods in digital forensics," *IEEE Xplore*, Jul. 01, 2021.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9514970>

[6] M. Bichara de Assumpção, M. A. dos Reis, M. R. Marcondes, P. M. da S. Eleutério, and V. H. Vieira, "Forensic method for decrypting TPM-protected BitLocker volumes using Intel DCI," *Forensic Science International: Digital Investigation*, vol. 44, p. 301514, Mar. 2023, doi:

<https://doi.org/10.1016/j.fsidi.2023.301514>.

[7] Computerforensicslab, "Complete Guide to Digital Forensics Chain of Custody," *Computer Forensics Lab | Digital Forensics Services | Digital Detectives*, Nov. 05, 2025.

<https://computerforensicslab.co.uk/digital-forensics-chain-of-custody-guide/>

[8] Bhushan D. Ghode, Akhlesh Kumar, and S. K. Jain, "Forensic investigation utilizing RAM capture to decrypt BitLocker volumes: A case study," *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 9, no. 8, pp. c65–c72, Aug. 2022.

[9] H. Majed, H. N. Noura, and A. Chehab, "Overview of Digital Forensics and Anti-Forensics Techniques," *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, Jun. 2020, doi: <https://doi.org/10.1109/isdfs49300.2020.9116399>.

[10] Dhruv Suvarna, Mahesh KM, M. Gupta, Sonal Gabburi, Prasad Honnavalli, and Sapna VM, "The Development of a Digital Forensic Framework for Ease of Forensic Analysis," vol. 6, pp. 1–5, Apr. 2024, doi: <https://doi.org/10.1109/isdfs60797.2024.10527263>.

[11] ACPO, "ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evidence for Digital Evidence," Mar. 2012. Available: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[12] Geovanni Ninahualpa, S. Yoo, T. Guarda, J. Díaz, and D. Piccirilli, "Protocol of Information Recovery in Solid Hard Drives - SSD Using File Carving Techniques," Jun. 2019, doi: <https://doi.org/10.23919/cisti.2019.8760783>.

