

Computer forensics: Assignment

Table of Contents

Task 1	2
Abstract	2
FTK Imager	2
Autopsy	3
X-Ways Forensics	3
Magnet AXIOM	3
CHFI process	3
References:.....	17
Task 2	6
Methodology	6
Acquisition	7
Anti-Forensic Activity	8
File carving	8
Cloud synchronization	9
Professional forensic report	10
Investigating steps	10
Findings.....	11
Conclusion.....	12
Appendix	12
Invoice	13

Task 1

Abstract

This paper examines four widely used digital forensic tools: FTK Imager, Autopsy, X-Ways Forensics, and Magnet AXIOM. Along with their analysis, it will demonstrate their roles within the CHFI process. FTK Imager is primarily utilized during the acquisition phase, enabling investigators to create exact disk images while preserving the integrity of original evidence. Autopsy, an open-source platform, supports multiple file systems and provides efficient data organization, analysis, and reporting capabilities, making it suitable for general forensic examination. X-Ways Forensics offers advanced disk analysis features, including data recovery, slack space examination, and detailed file system support, though it requires a paid license. Magnet AXIOM stands out as a comprehensive solution with capabilities spanning disk, mobile, cloud, and IoT forensics, enhanced by AI-driven analysis and robust reporting tools. Overall, each tool serves a distinct purpose within the CHFI framework, with FTK Imager focusing on acquisition, Autopsy and X-Ways on analysis, and Magnet AXIOM providing an all-in-one solution for complex, multi-source investigations.

FTK Imager

FTK Imager is a program used to save images of hard disks into a file, making exact copies of digital devices and allowing you to collect evidence while keeping the original drive untouched, as stated in the official website [1]. The site also shows that the software is completely free, having garnered over 1 million downloads and it used by thousands of investigators worldwide. The image file

can take different formats, like DD/raw, AD1, and E01 according to a comparative analysis of acquisitions methods in digital forensics [2].

Himanshu et al. [2] state that FTK Imager can be used to search disks for deleted files or passwords, as well as computing the MD5 and SHA1 checksums. It can also be used to check if a USB key was recently used, in what ways

it was modified while attached to the drive, and at what time [2].

Autopsy

Autopsy is a free open-source platform used to investigate hard disks, disk images, mobile images, and smartphone recovery files, as stated in [4]. Its management system allows for an organized view of a case and the different users who have access to it [3]. According to M. Farnan et al. [3], it can support file systems like FAT, exFAT, HFS+, and NTFS.

Autopsy can analyze and organize all the different components of a device's data, while also exporting said components into an Excel document [3]. According to J. Mehta et al. [4], Autopsy has a good capability of generating reports based on evidence collected, making it useful for investigations.

X-Ways Forensics

X-Ways Forensics is a software with various forensic features, hence Seth Adjei Gyimah calling it “a powerful disk analysis tool” [5]. It supports numerous file systems such as FAT, NTFS, Ext2/3, Reiser, CDFS, and UDF [5]. The software is not free, costing at least £1,109 for a yearly license, as shown in the official page to place orders [6].

It can examine and extract hidden data such as slack space, create listings of both existing and deleted content, and create exact disk images, although low quality, that preserve all data. The

software also organizes files, clones drives, and recovers volatile data. [5]

Magnet AXIOM

Magnet AXIOM is a digital forensics platform with subscription pricing, often varying by edition (e.g., standard vs. enterprise “Cyber” as shown on the official site [8]) and user scale. It offers features like an artifact-first approach, AI-driven analysis, timeline reconstruction, and cross-source correlation of evidence [8]. Morgan Siamukulule [9] confirms the tool supports multiple file systems and environments, including Windows, macOS, Linux, and mobile file systems, with capabilities for disk decryption and full file system analysis.

AXIOM analyzes diverse evidence types: disk images, mobile data, cloud artifacts and IoT data [9]. Its reporting capabilities are strong, enabling export in formats like PDF, HTML, and Excel, plus portable case sharing for collaboration. Overall, it is a comprehensive, all-in-one forensic solution.

CHFI process

In the CHFI process, different tools are best suited to specific phases of an investigation. FTK Imager is best used during the imaging and acquisition phase, as it reliably creates disk and memory images. For the analysis phase, Autopsy is

Madeleine Vuillemin

useful for general examination, timeline creation, and report creation, while X-Ways Forensics is better for deeper, expert-level analysis and data carving. Magnet AXIOM stands out as a sources within a single case.

comprehensive tool, excelling in analysis, and is the strongest option for mobile and cloud forensics, as it can extract data from smartphones, computers, and online

Tool name	Cost	Key features	Supported file systems	Types of evidence	Reporting capabilities
FTK Imager	Free	- Creates forensic disk images - File preview without altering evidence - Hashing to ensure integrity - Memory capture - Basic file carving	DD/raw, AD1, and E01	Disk images, USB drives	- Generates basic reports - Limited reporting: mainly acquisition-focused - Can document evidence integrity for court use
Autopsy	Free	- File recovery & data carving - Timeline analysis of user activity - Keyword search across disk + unallocated space - Artifact extraction - Plugin support via The Sleuth Kit	FAT, exFAT, HFS+, and NTFS	Disk images, mobile data	- Generates detailed forensic reports - Includes findings like timelines, artifacts, keyword hits - Supports case documentation for investigations
X-Ways Forensics	≥£1,109 for 1 year	- Advanced disk and memory analysis - Fast searching and indexing of large datasets - Integrated hex editor - Disk imaging, cloning, and file system analysis - Efficient handling of large evidence sets	FAT, NTFS, Ext2/3, Reiser, CDFS, and UDF	Hard disks, memory card, flash disks, floppy disks, ZIP, JAZ, CDs, DVDs, and more [5]	- Produces customizable reports - Allows fine-grained control over included evidence - Suitable for technical/legal reporting with detailed artifacts
Magnet AXIOM	≥£4,000 for 1 year	- All-in-one platform: computer, mobile, and cloud forensics - Automated evidence collection & processing - Advanced analytics - Memory analysis + artifact parsing - Centralized case management	-	Mobile, computer, cloud, IoT, and vehicle sources	- Generates comprehensive, multi-format reports - Includes artifacts like chats, timelines, media, etc. - Supports custom filtering and case-focused reporting - Designed for court-ready, detailed investigation reports

Task 2

Introduction

Cyfusion Mobile Manufacturing Company (CMMC), a London-based firm specializing in mobile phone interface and GUI design, has quickly become a leader in its industry. However, the company recently experienced a serious internal security breach involving a former employee, Rich Daley, who had exclusive access to highly confidential design files.

Before resigning, Rich deleted critical Autodesk Maya project files using file-wiping software and transferred sensitive data to a personal cloud account, with suspected intent to share it with a competitor. As these designs represent significant financial investment and were intended for patenting, their loss poses a major risk to the company.

To address the incident, CMMC has appointed a digital forensics expert, Troy Simpson, to investigate the breach, recover lost data, and provide evidence of any malicious activity. This report outlines the investigation and its findings.

Methodology

The investigation adhered to the principles established by the ACPO. Integrity preservation was maintained throughout, ensuring that no action taken altered the original evidence, as stated by the first principle [10]. All evidence handling was carried out by qualified personnel, demonstrating adherence to the principle of competence, as demanded by the second principle [10]. A clear audit trail was established, with all actions thoroughly documented and capable of being reproduced if necessary, as asked of the third principle [10]. Furthermore, as the fourth and last principle states [10], the investigator maintained full responsibility and accountability for all aspects of the investigation. In addition, the investigation followed the phases of the CHFI methodology, which included preparation, seizure, acquisition, analysis, reporting, and testimony.

Acquisition

The acquisition phase faced a significant challenge due to BitLocker full-disk encryption. To address this, a live acquisition approach was employed in order to capture the system in its decrypted state while it was still powered on. Additionally, RAM capture was conducted to extract the BitLocker encryption keys necessary for accessing the protected data.

A range of forensic tools was utilized during this process. FTK Imager was used for live disk imaging due to its ability to maintain forensic integrity and generate hash values for verification. Magnet RAM Capture [11] and Belkasoft Live RAM Capturer [12] were employed to extract encryption keys from the system memory, providing alternative methods for reliable RAM acquisition.

This approach was justified as FTK Imager supports the creation of forensically sound images with integrated hashing capabilities [2], ensuring data integrity throughout the process. Meanwhile, the RAM capture tools enabled the recovery of encryption keys required to mount the BitLocker volume without altering the original evidence.

The acquisition process followed a structured sequence of steps. First, the system was powered on and isolated from the network to prevent external interference. Next, RAM was captured to obtain the BitLocker encryption keys. Following this, a forensic image of the system was acquired in E01 format. Finally, hash values (MD5 and SHA256) were generated and verified to ensure the integrity and authenticity of the acquired data.

Anti-Forensic Activity

The objective of this stage was to determine whether file-wiping tools, such as Eraser, had been used on the system. The approach focused on analyzing installed programs and execution artefacts in order to identify traces of wiping activity, including file overwrite signatures and patterns consistent with secure deletion.

A combination of forensic tools was used to support this analysis. Autopsy was employed for file system examination and artefact analysis [3], while EnCase Forensic provided deeper disk-level investigation and cross-correlation of evidence.

Evidence was gathered from multiple system sources like installed program information, execution history, event logs for system activity, and unallocated disk space for residual data patterns. This approach allowed for a more comprehensive assessment of potential wiping activity.

Indicators of file wiping were identified through several artefacts. The presence of Eraser software within the system suggested potential use of a file-wiping tool. In addition, Prefetch files referencing ERASER.EXE provided evidence of execution. Analysis of unallocated space revealed overwritten file clusters exhibiting random data patterns consistent with secure deletion processes, and inconsistencies in file metadata further supported the likelihood of file wiping activity.

File carving

The objective of this stage was to recover deleted Autodesk Maya project files from the system. The approach focused on examining unallocated disk space for residual file fragments and performing signature-based carving to reconstruct deleted data where possible.

Several forensic tools were used to support this recovery process. FTK Imager was employed due to its effectiveness in recovering deleted files and previewing data from disk images. X-Ways Forensics was used for advanced file carving, allowing more precise recovery based on defined file type headers and footers. Autopsy was also utilized, providing integrated artifact recovery and analysis capabilities within a comprehensive forensic environment.

This approach was justified on the basis that deleted files are not immediately removed from disk storage; instead, their data often remains in unallocated space until it is overwritten. As a result, file fragments can still be recovered if they have not been fully replaced by new data.

The recovery process followed a structured sequence. First, unallocated disk space was scanned for residual data. Next, Autodesk Maya file signatures, specifically .mb and .ma formats, were identified to locate relevant fragments. These fragments were then reconstructed into partial or complete files where possible. Finally, the integrity of the recovered data was validated to ensure the files were usable and accurately restored.

Cloud synchronization

The objective of this stage was to determine whether data exfiltration had occurred via a web browser. The approach focused on analyzing browser artefacts to identify any interaction with cloud storage services, specifically Google Drive, and to assess whether files may have been uploaded or transferred externally.

A combination of forensic tools was used to support this analysis. Autopsy was utilized to review web activity, including visited URLs and associated timestamps and Magnet AXIOM was employed to correlate artefacts and reconstruct a detailed activity timeline across multiple sources of evidence.

Key indicators of potential data exfiltration were identified through this analysis. Visits to drive.google.com suggested interaction with Google Drive services, while evidence of file upload activity further supported the possibility of data transfer. The presence of login credentials or active session tokens indicated authenticated access to cloud storage, and correlation of timestamps with file deletion events strengthened the likelihood that data may have been exfiltrated shortly before or during those deletions.

Professional forensic report

Investigating steps

The investigation began by securing the suspect machine and documenting the chain of custody to ensure evidence integrity and maintain a clear record of handling. A live RAM acquisition was then performed in order to preserve volatile data, including the extraction of BitLocker encryption keys required for accessing encrypted volumes.

Following this, a forensic disk image was created using FTK Imager, ensuring a bit-for-bit copy of the storage media. Hash values were generated and verified to confirm the integrity of the acquired evidence and to ensure that no alterations had occurred during the imaging process.

A full forensic analysis was then conducted using Autopsy and EnCase, allowing for comprehensive examination of the file system, system artefacts, and recovered data. During this phase, the installation and execution of file-wiping software were identified, indicating potential attempts to remove or obscure evidence.

Further analysis included file carving techniques to recover deleted data from unallocated disk space, enabling the reconstruction of partially or fully deleted files. Browser artefacts were also examined to identify cloud storage activity, particularly interactions with online services and potential data transfers.

Finally, all findings were correlated into a unified timeline, allowing for a structured reconstruction of events and supporting the overall interpretation of user activity and potential data exfiltration.

Findings

The forensic analysis identified multiple indicators of anti-forensic activity. The installation of the Eraser application was confirmed through registry entries, while Prefetch artefacts (ERASER.EXE) provided evidence of program execution. In addition, overwritten disk sectors were detected, showing patterns consistent with secure deletion techniques designed to prevent data recovery.

In relation to file deletion and recovery, several Autodesk Maya project files were found to be missing from the system. However, partial fragments of these files were successfully recovered from unallocated disk space, indicating that deletion had occurred but was not fully completed or overwritten. The nature of the deletions and associated artefacts suggests deliberate removal of data rather than accidental loss.

Analysis of cloud storage activity revealed significant browser-based interaction with Google Drive. Browser history indicated repeated access to the service, and the timing of these events aligned closely with the observed file deletion activity. Cached data further suggested that file upload operations had taken place, supporting the possibility of external data transfer.

When all artefacts were correlated into a unified timeline, a clear sequence of events emerged: file access, followed by cloud upload activity, then secure deletion of local files, and finally the subject's resignation. This chronological pattern strongly supports the conclusion of intentional data exfiltration followed by deliberate attempts to destroy forensic evidence.

Conclusion

The forensic investigation provides strong evidence indicating that Rich Daley accessed and removed proprietary design files without authorization. Analysis suggests that sensitive data was transferred to a personal Google Drive account, supported by browser artefacts and cloud storage activity. In addition, the presence of a file-wiping tool and associated execution evidence indicates that deliberate steps were taken to permanently remove traces of the activity from the system.

These actions appear to have taken place shortly before the subject's resignation, with the timeline showing a consistent sequence of file access, external transfer, and subsequent evidence destruction. The use of secure deletion tools, combined with recovered artefacts from unallocated space and browser history, supports the conclusion that the activity was intentional rather than accidental or routine system behavior.

Based on the findings, the actions observed are consistent with intellectual property theft, deliberate sabotage of digital evidence, and a breach of confidentiality agreements. The evidence collected has been preserved using standard forensic procedures, including chain of custody documentation, hashing, and verified imaging, and is therefore considered forensically sound and suitable for presentation in legal proceedings.

Appendix

Evidence Item	Hash Type	Hash Value
Disk Image (E01)	MD5	9f86d081884c7d659a2feaa0c55ad015
Disk Image (E01)	SHA256	5e884898da28047151d0e56f8dc6292773603d0d6aabbdd
RAM Dump	MD5	3c59dc048e8850243be8079a5c74d079
RAM Dump	SHA256	2c26b46b68ffc68ff99b453c1d30413413422f1640

Invoice

TROY SIMPSON FORENSICS

Digital Forensics & Incident Response Specialists

London, United Kingdom

Email: info@troysimpsonforensics.co.uk

Phone: +44 20 7946 0000

INVOICE

Invoice Number: TSF-2026-041

Invoice Date: 30/04/2026

Bill To:

Cyfusion Mobile Manufacturing Company (CMMC)

London, United Kingdom

Case Reference:

Investigation into Data Sabotage and Intellectual Property Theft – Rich Daley

Billing Summary

Description	Hours	Rate (GBP/day)	Pro-rated Rate (GBP/hour)	Amount (GBP)
Initial Case Review & Planning	6	£1,200	£150	£900
Evidence Acquisition & Imaging	8	£1,200	£150	£1,200
Decryption & Data Access (BitLocker)	6	£1,200	£150	£900
Forensic Analysis (Disk & Artifacts)	16	£1,200	£150	£2,400
File Recovery & Carving	10	£1,200	£150	£1,500
Anti-Forensic Activity Analysis	8	£1,200	£150	£1,200
Cloud Artifact Examination	6	£1,200	£150	£900
Report Writing & Documentation	12	£1,200	£150	£1,800
Expert Testimony Preparation	6	£1,200	£150	£900

Total Hours: 78 Hours

Madeleine Vuillemin

Subtotal: £11,700

VAT (20%): £2,340

Total Amount Due: £14,040

Payment Terms:

- Payment due within 14 days of invoice date
 - Bank Transfer (Preferred)
 - Late payments may incur a 5% surcharge
-

Notes:

- Daily rate of £1,200 reflects industry-standard pricing for CHFI and CEH certified digital forensic experts in the UK.
 - Hours are recorded in accordance with forensic audit standards and are fully traceable to case activity logs.
 - Additional charges may apply for court attendance or extended expert testimony.
-

Authorised by:

Troy Simpson
Lead Digital Forensic Investigator
Troy Simpson Forensics

End of Invoice

Acronym	Stands For	Definition & Context
ACPO	Association of Chief Police Officers	A UK body that established the core principles for digital evidence handling. The ACPO Principles are a fundamental guideline for ensuring the integrity and admissibility of evidence in a UK context.
AI	Artificial Intelligence	Artificial intelligence refers to computer systems that can perform complex tasks normally done by human-reasoning, decision making, creating, etc. Magnet AXIOM utilizes an AI tool in order to help with investigations.
CD	Compact Disc	A digital optical data storage format used for audio and computer data, developed by Sony and Philips in the early 1980s.
CHFI	Computer Hacking Forensic Investigator	A professional certification offered by EC-Council that teaches modern forensic investigation techniques. The assignment aligns with its methodologies.
DVD	Digital Video Disc or Digital Versatile Disc	A digital optical disc data storage format. It was invented and developed in 1995 and first released on November 1, 1996, in Japan.
FTK	Forensic Toolkit	A powerful, all-in-one commercial computer forensics suite developed by Exterro. It is an industry standard for disk imaging, analysis, and reporting.
HTML	Hypertext Markup Language	HTML is the language used to create Web pages for display in Web Browsers. In short, it is the code for creating web pages, using tags and other commands that a browser reads and converts into the normal web pages that people see.
MD	Message-Digest Algorithm	A widely used cryptographic hash function that converts input data of any size into a fixed-length 128-bit (32-character hexadecimal) string. It is used primarily for data integrity verification and non-critical checksums.
PDF	Portable Document Format	A file format developed by Adobe in 1993 used to present documents, including text formatting and images, in a manner independent of application software, hardware, and operating systems.
RAM	Random Access Memory	A computer's short-term memory where running programs and active data are stored. Can be acquired for "live" forensic analysis of encrypted volumes or running processes.



SHA	Secure Hash Algorithm	A hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest.
USB	Universal Serial Bus	An industry standard for connection, communication, and power supply between computers and devices. A common vector for data exfiltration.

References:

- [1] Exterro, “FTK Imager - Forensic Data Imaging and Preview Solution,” *Exterro*.
<https://www.exterro.com/digital-forensics-software/ftk-imager>
- [2] 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>
- [3] M. Farnan, J. Pratt, A. David, and Masoud Shakiba, “Digital Forensic Tools: Comparison of Autopsy TSK and Forensic Explorer,” pp. 1–5, Jun. 2024, doi:
<https://doi.org/10.1109/iciteics61368.2024.10625076>.
- [4] J. Mehta, Yash Bhadania, P. Shah, and P. Prajapati, “Comparative Study of Mobile Forensics Tools: Autopsy, Belkasoft X and Magnet Axion,” pp. 1257–1263, Aug. 2024, doi: <https://doi.org/10.1109/icesc60852.2024.10689971>.
- [5] S. A. Gyimah, “X-Ways Forensics Platform For Digital Forensics Examiners,” *Advances in Multidisciplinary and scientific Research Journal Publication*, vol. 1, no. 1, pp. 353–356, Jul. 2022, doi: <https://doi.org/10.22624/aims/crp-bk3-p56>.
- [6] “Place Orders / Request Quotes for New Licenses,” *www.x-ways.net*. <https://www.x-ways.net/order.html>
- [7] “Why Magnet Forensics? - Magnet Forensics,” *Magnet Forensics*, Oct. 02, 2025.
<https://www.magnetforensics.com/why-magnet-forensics/>
- [8] “Why Magnet Forensics? - Magnet Forensics,” *Magnet Forensics*, Oct. 02, 2025.
<https://www.magnetforensics.com/why-magnet-forensics/>
- [9] M. Siamukulule, “A Deep Dive into Magnet AXIOM’s Workflow: Exploring the Roles of AXIOM Process and AXIOM Examine in Digital Evidence Acquisition and Analysis.” Available: <https://www.ijfmr.com/papers/2024/6/30679.pdf>
- [10] G. Horsman, “ACPO principles for digital evidence: Time for an update?,” *Forensic Science International: Reports*, vol. 2, p. 100076, Feb. 2020, doi:
<https://doi.org/10.1016/j.fsir.2020.100076>.
- [11] Magnet Forensics, “MAGNET RAM Capture,” *Magnet Forensics*, 2019.
<https://www.magnetforensics.com/resources/magnet-ram-capture/>
- [12] belkasoft, “Belkasoft RAM Capturer: Volatile Memory Acquisition Tool,” *belkasoft.com*. <https://belkasoft.com/ram-capturer>