

# Assignment Report

*by* Lewis James

---

**Submission date:** 29-Apr-2026 09:42PM (UTC+0100)

**Submission ID:** 281573176

**File name:** 61043\_Lewis\_James\_Assignment\_Report\_737277\_760805909.docx (1.36M)

**Word count:** 3782

**Character count:** 22434



# SYNTHESIZE A SOLUTION TO A POTENTIAL REAL-LIFE SCENARIO

ACCD5000

Lewis James

2427497@student.uwtsd.ac.uk

## Table of Contents

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Abstract.....                                                            | 3  |
| Task 1 – Research and Critical Evaluation of Modern Forensic Tools ..... | 4  |
| 1. Introduction .....                                                    | 4  |
| 2. Comparative Analysis of Forensic Tools.....                           | 5  |
| 3. Critical Evaluation of Forensic Tools.....                            | 6  |
| 3.1. FTK (Forensic Toolkit) .....                                        | 6  |
| 3.2. Magnet AXIOM.....                                                   | 6  |
| 3.3. Autopsy .....                                                       | 6  |
| 3.4. CAINE Linux.....                                                    | 7  |
| 4. Comparative Discussion.....                                           | 7  |
| 5. Suitability Across Forensic Phases .....                              | 8  |
| Task 2 – Case Study.....                                                 | 9  |
| 1. Introduction .....                                                    | 9  |
| 2. Forensic Methodology .....                                            | 9  |
| 3. Investigation Plan .....                                              | 10 |
| 3.1 Evidence Acquisition .....                                           | 10 |
| 3.2 Disk Imaging and Preservation.....                                   | 10 |
| 3.3 Detection of Anti-Forensic Activity.....                             | 11 |
| 3.4 File Recovery .....                                                  | 11 |
| 3.5 Cloud Evidence Extraction .....                                      | 11 |
| 4. Forensic Report.....                                                  | 12 |
| 4.1 Executive Summary .....                                              | 12 |
| 4.2 Investigation Steps.....                                             | 12 |
| 4.3 Findings.....                                                        | 13 |
| 4.4 Conclusion.....                                                      | 14 |
| 5. Simulated Hash Log Table.....                                         | 15 |
| 6. Appendix (Example FTK screenshots from a lab environment) .....       | 16 |
| 7. Professional Invoice .....                                            | 21 |
| References .....                                                         | 22 |

## Abstract

This report evaluates modern computer forensic tools and applies forensic methodology to a simulated intellectual property theft and sabotage investigation. Task 1 compares commercial and open-source tools, including FTK, Magnet AXIOM, Autopsy and Caine Linux, with references to cost, supported evidence types, file systems and suitability across CHFI investigation phases. Task 2 applies CHFI and ACPO principles to a case involving BitLocker encryption, file wiping, deleted Autodesk Maya design files, and suspected Google Drive exfiltration. The report proposes a forensic acquisition strategy, evidence preservation process, anti-forensic analysis, file recovery approach, and cloud artefact examination. It concludes that a combination of disk, registry, browser, and recovered file evidence could support legal action against the suspect, while recognising limitations caused by encryption and secure deletion.

# Task 1 – Research and Critical Evaluation of Modern Forensic Tools

## 1. Introduction

Computer forensics involves the identification and presentation of digital evidence. While the fundamental principles of digital forensics remain consistent, the tools used in investigations continuously evolve in order to address new challenges such as encryption, cloud storage, or mobile devices [1].

Modern forensic tools vary significantly in terms of cost, usability, and capability. Some tools are comprehensive suites designed for enterprise-level investigations, while others are open-source alternatives that provide flexibility and accessibility [2]. Selecting the correct tool depends on the type of investigation and evidence, and the availability of resources.

This section evaluates four widely used forensic tools:

- FTK (Forensic Toolkit)
- Magnet AXIOM
- Autopsy
- CAINE Linux

## 2. Comparative Analysis of Forensic Tools

| Tool         | Type        | Cost | Key Features                             | Supported File Systems                           | Evidence Types        | Strengths                       | Weaknesses                    | Reporting Capabilities                                                                    | Best Phase                         |
|--------------|-------------|------|------------------------------------------|--------------------------------------------------|-----------------------|---------------------------------|-------------------------------|-------------------------------------------------------------------------------------------|------------------------------------|
| FTK          | Commercial  | High | Disk Imaging, indexing, email analysis   | NTFS, FAT, exFAT, EXT                            | Disk, email, registry | Fast search, powerful indexing  | Expensive, resource intensive | Integrated legal-style case reports, bookmarks, hash reports, exported artefact summaries | Analysis                           |
| Magnet AXIOM | Commercial  | High | Cloud, mobile, and disk analysis         | NTFS, APFS, EXT                                  | Mobile, cloud, disk   | Strong cloud/mobile support     | High cost                     | Automated with timelines, artefact summaries, cloud/mobile evidence reports               | Acquisition / Processing, analysis |
| Autopsy      | Open source | Free | GUI, keyword search, timeline analysis   | NTFS, FAT, EXT                                   | Disk images           | Easy to use, cost effective     | Limited advanced features     | Basic reports in formats such as HTML, CSV, and Excel reports                             | Analysis                           |
| CAINE Linux  | Open source | Free | Live forensic environment, imaging tools | NTFS, FAT, exFAT, EXT, HFS, UFS, ISO 9660, BTRFS | Disk, memory          | Portable, comprehensive toolkit | Steep learning curve          | Limited built in reporting                                                                | Imaging                            |

### 3. Critical Evaluation of Forensic Tools

#### 3.1. FTK (Forensic Toolkit)

FTK is a widely recognised forensic suite used in law enforcement and corporate investigations [3]. The primary strength of FTK is its advanced indexing and search capabilities, allowing investigators to process large volumes of data efficiently.

A key advantage of FTK is its ability to perform in-depth analysis of file systems like NTFS and FAT, as well as email databases and registry artefacts. This capability makes FTK particularly effective during the analysis phase of an investigation [4]. The tool is, however, quite resource-intensive and requires high-performance hardware to operate efficiently.

FTK's high licensing cost may limit accessibility for smaller organisations. Additionally, while it offers powerful features, it can be difficult to learn for beginners.

#### 3.2. Magnet AXIOM

Magnet AXIOM is a modern forensic tool designed to address the increasing importance of mobile and cloud-based evidence [5]. It supports artefact recovery from smartphones, cloud platforms, and internet applications, which makes it highly relevant to modern investigations.

One of AXIOM's strongest features is its ability to extract and analyse data from cloud services such as Google Drive and social media platforms. This capability aligns with modern forensic challenges where data is no longer confined to local storage and must be acquired in accordance with forensic best practices and evidential integrity requirements [6].

Similarly to FTK, this tool is associated with high licensing costs, which can restrict its use. Furthermore, reliance on APIs and third-party integration can create limitations if access to services is restricted.

#### 3.3. Autopsy

Autopsy is an open-source digital forensic platform that provides a graphical interface for The Sleuth Kit [7]. Autopsy is widely used in academic environments and by smaller organisations due to its accessibility and ease of use.

This tool offers essential forensic capabilities, including keyword searching, timeline analysis, and file recovery. Autopsy's modular design allows for the addition of plugins, enhancing its functionality.

Despite its advantages, Autopsy does lack some advanced features commonly found in commercial tools, particularly in areas such as cloud and mobile forensics. The performance of the tool may also be slower when handling large datasets, limiting its effectiveness in complex investigations.

### 3.4. CAINE Linux

CAINE (or Computer Aided Investigative Environment) is a specialised Linux distribution designed for digital forensics [8]. CAINE provides a complete forensic environment, including tools for disk imaging, memory analysis, and data recovery.

A key strength of CAINE is its ability to operate as a live system, allowing investigators to perform forensic acquisition without modifying the target system. This aligns with forensic best practices and the ACPO principles, which require that digital evidence is handled in a way that preserves its integrity and admissibility in court [6].

CAINE, however, requires a high level of technical expertise compared to GUI-based tools such as Autopsy. The complexity of CAINE makes it far less suitable for inexperienced users. Additionally, it lacks the integrated reporting capabilities found in commercial solutions.

## 4. Comparative Discussion

A significant distinction between commercial and open-source forensic tools lies in their scalability and feature integration. Commercial tools such as FTK and Magnet AXIOM offer comprehensive, enterprise-level capabilities, such as advanced automation, reporting, and support for a wide range of evidence types [3], [5]. These tools are particularly effective in complex investigations involving large datasets or multiple sources of evidence.

In contrast, open-source tools like Autopsy and CAINE provide cost effective alternatives which are more suitable for smaller scale investigations or for academic use [7], [8]. While these tools do offer essential forensic functionality, they often lack more advanced features and integration capabilities that are standard in commercial tools.

Another key difference between these tools is the type of evidence supported. Magnet AXIOM excels in cloud and mobile forensics, reflecting the growing importance of these areas in modern investigations and the need to handle distributed data sources in line with established forensic guidelines [6]. Comparatively, FTK is stronger in disk and email analysis. Open-source tools are usually more focused on disk-based evidence and may require additional tools to handle mobile or cloud data.

## 5. Suitability Across Forensic Phases

Different tools are better suited to specific phases of the forensic process:

- Imaging Phase:
  - CAINE Linux is highly effective due to its live boot capability and built-in imaging tools.
- Analysis Phase:
  - FTK and Autopsy are suited for analysing disk images, with FTK offering more advanced capabilities.
- Mobile Forensics:
  - Magnet AXIOM provides comprehensive support for mobile device data extraction and analysis.
- Cloud Forensics:
  - Magnet AXIOM is also strong in extracting and analysing cloud-based artefacts.

There is no single tool that is sufficient for all aspects of a forensic investigation. Instead of using one single tool, investigators must select tools based on the specific requirements of each case.

## Task 2 – Case Study

### 1. Introduction

This investigation centres around a suspected intellectual property theft and sabotage by an employee named Rich Daley at Cyfusion Mobile Manufacturing Company (CMMC). The objective is to forensically examine the suspect's encrypted Windows 11 system to recover deleted design files, identify evidence of anti-forensic activity, and determine whether data was exfiltrated to a cloud service.

The investigation will follow recognised UK forensic principles, such as those set out by ACPO, while also considering current quality requirements set out by the Forensic Science regulator's statutory code of practice for forensic science activities in England and Wales. [9]

### 2. Forensic Methodology

The forensic investigation will follow the four ACPO principles. These principles are:

- 1. Integrity of evidence
  - No action should change the data that may be relied on in court. Write blockers can be used to prevent this, as well as the creation of clean forensic images rather than working on the original device.
- 2. Competence
  - Only trained personnel should have access to the original data. In this case, the investigation should be conducted by the certified examiner, Troy Simpson.
- 3. Audit Trail
  - All actions must be recorded and repeatable. Logs should be maintained of imaging process, hash values, and tool usage.
- 4. Responsibility
  - The lead investigator is accountable for compliance. Full documentation should be included in the final report.

These principles are also consistent with wider digital evidence handling standards, including ISO/IEC 27037, which identifies the core stages of digital evidence handling as identification, collection, acquisition, and preservation. [10]

### 3. Investigation Plan

#### 3.1 Evidence Acquisition

The first stage of the investigation focuses on acquiring evidence from the suspect's Windows 11 system, which is protected using BitLocker full-disk encryption. This will pose as a challenge, as encrypted drives can't be accessed without the appropriate decryption keys.

If the system is powered on at the time of seizure, a live acquisition will be carried out in order to capture volatile memory, which may contain the BitLocker encryption keys. This will ensure investigators are able to bypass encryption without altering stored data. In the scenario that the device is powered off, alternative methods such as obtaining the BitLocker recovery key or retrieving it from the domain controller will be considered.

This approach is supported by forensic acquisition guidance which recognises that where encryption is present, investigators may need to capture memory before disk imaging in order to preserve encryption keys. Recovery keys may also be available through enterprise management systems, cloud accounts, or other authorised routes [11]. This is relevant on Windows 11 systems as TPM-protected BitLocker can prevent access to the drive unless the volume master key or recovery key can be obtained [12].

Tools such as CAINE Linux will be used to perform live forensic acquisition in a controlled environment, while FTK imager will be used to access and prepare the system for imaging once decryption is achieved. This approach will ensure compliance with forensic best practices by minimising changes to the original evidence.

#### 3.2 Disk Imaging and Preservation

Following successful access to the encrypted drive, a forensic image of the system will be created. This involves generating a bit-by-bit copy of the entire storage device, ensuring that all data is preserved. The imaging process will be conducted using FTK imager, which is widely recognised for its reliability and ability to maintain evidential integrity.

During this process, cryptographic hash values, such as MD5 and SHA-256 will be generated for both the original device and the forensic image. These hash values serve as digital fingerprints and are used to verify that the image is an exact replica of the original data.

Once the image is created and verified, the original device will be securely stored to prevent any modification, and all analysis will be performed on the forensic copy. This procedure adheres to forensic principles and maintains the admissibility of evidence in legal proceedings.

### 3.3 Detection of Anti-Forensic Activity

One of the primary goals of this investigation is to determine whether any anti-forensic techniques were used to conceal evidence, specifically the use of file wiping software. The analysis will focus on identifying traces of any anti-forensic activity on the system. This includes examining installed applications, registry entries, prefetch files, and system event logs to identify evidence of file wiping software like Eraser.

Tools such as FTK will be used to conduct analysis of registry artefacts and system logs, while Autopsy will be used to create a timeline of system activity. This timeline will help correlate the execution of wiping tools with the deletion of critical files. Indicators such as repeated overwrite patterns, abnormal file deletion behaviour, and execution traces of wiping utilities will be used to demonstrate intentional anti-forensic activity. Establishing the use of these tools is crucial in proving deliberate attempts to destroy evidence.

### 3.4 File Recovery

Due to critical design files being deleted prior to the suspect's departure, file recovery techniques will be used to retrieve as much data as possible. File carving will be conducted on unallocated disk space to recover fragments of deleted Autodesk Maya project files. This technique relies on identifying file signatures rather than file system metadata, making it useful when files have been partially overwritten or removed.

Autopsy will be used to perform signature-based recovery and to analyse recovered file fragments, while additional recovery tools available with CAINE Linux may be used to enhance the recovery process. Although complete recovery may not be possible, partial file fragments can serve as valuable evidence by demonstrating the prior existence of the files and supporting claims of data deletion and sabotage.

### 3.5 Cloud Evidence Extraction

To investigate potential data exfiltration, the analysis will extend to cloud-related artefacts, specifically focusing on the suspected use of Google Drive. As the suspect is believed to have uploaded files via a web browser, browser artefacts will be examined in order to identify evidence of cloud activity. This includes analysing browsing history, cookies, cached files, and session data to identify access to Google Drive and associated user accounts.

Magnet AXIOM will be used as the primary tool for this stage due to its capabilities in extracting and analysing cloud and browser artefacts. FTK may also be used to support browser analysis and to validate findings. Evidence such as login timestamps, file upload records, and account identifiers will be used to demonstrate that data was transferred to an external cloud storage device. This is critical in establishing intent and confirming the unauthorised removal of company data.

## 4. Forensic Report

### 4.1 Executive Summary

This investigation examined a company issued Windows 11 device belonging to former employee Rich Daley. The objective of the investigation was to determine whether intellectual property theft and sabotage had occurred. Using industry standard forensic tools and methodologies, evidence was recovered indicating the use of file wiping software, deletion of critical design files, and access to a cloud storage platform consistent with data exfiltration.

### 4.2 Investigation Steps

The investigation started with the secure seizure of the suspect's company issued device, ensuring that the proper chain of custody procedures were followed. The device was documented, labelled, and stored in a controlled environment to prevent unauthorised access or alteration. All handling procedures were conducted in accordance with the principles defined by the ACPO to ensure the integrity and admissibility of evidence.

Once the device was preserved, forensic acquisition took place. Due to the presence of BitLocker encryption, appropriate measures were taken to gain access to the data in a forensically sound manner. Once access was established, FTK Imager was used to create a forensic image of the device. During this process, cryptographic hash values (MD5 and SHA-256) were generated and recorded for both the original device and the acquired image. These hash values were then verified to confirm that the forensic image was an exact copy of the original data.

Following this, all analysis was conducted on the verified forensic image in order to preserve the original evidence. The image was loaded into forensic tools, such as FTK and Autopsy, to examine the file system, system artefacts, and user activity. A detailed examination of registry entries, installed applications, and system logs was performed to identify any evidence of anti-forensic activity. Artefacts such as execution traces in prefetch files, and installation records in the system registry were also checked, as they can be associated with file wiping utilities.

File recovery techniques were used to locate and reconstruct deleted files. File carving was performed on unallocated disk space to recover fragments of Autodesk Maya project files. Recovered data was analysed and categorised to determine its relevance to the investigation. Although some files were found to be partially overwritten, identifiable fragments provided evidence of their prior existence and deletion.

The investigation also included analysis of internet and cloud related activity. Browser artefacts were extracted and examined using Magnet AXIOM to identify evidence of access to cloud storage services. Analysis of browser history, cookies, and cached data revealed user interactions with Google Drive, including timestamps and session data which indicated file uploads. These findings were linked to system activity timelines to establish a sequence of events leading to the suspect's resignation.

Finally, all findings were documented in a structured and repeatable manner, which ensured that every step of the investigation could be independently verified. This included maintaining detailed logs of all tools used, processes undertaken, and evidence identified, ensuring full compliance with forensic standards and supporting the credibility of the investigation.

### 4.3 Findings

The forensic analysis of the suspect's system revealed multiple pieces of evidence supporting the claim that deliberate sabotage and data exfiltration had taken place. One of the most significant findings was the presence of artefacts indicating the installation and execution of file wiping software. Analysis of system registry entries and prefetch files confirmed that a wiping tool had been executed on the system shortly before the suspect left the company. The timing of this suggests a deliberate effort to remove critical data and hinder forensic recovery.

Further examination of the file system showed that a significant number of files associated with Autodesk Maya projects had been deleted. Although many of these had been overwritten, file carving techniques enabled the recovery of partial file fragments from unallocated disk space. These fragments included components of design files, which confirmed their former existence on the system. The condition of the recovered data implies the use of secure deletion methods, which reinforces the claim that anti-forensic techniques were used.

In addition, analysis of browser artefacts provided clear indications of unauthorised data transfer. Examination of web browsing history, cookies, and cached files showed repeated access to Google Drive through a web browser. Timestamp analysis showed that this activity occurred near the same time as file deletion events, which suggests a planned series of actions. Session artefacts and account identifiers linked this activity to the suspect, providing further evidence of data exfiltration.

Correlation of all evidence sources allowed for the construction of a timeline of events. This timeline indicates that the suspect accessed and potentially transferred sensitive design files to a personal cloud storage account before using a file wiping tool to delete local copies. The combination of file recovery results, anti-forensic artefacts, and cloud access records provides a strong evidential basis for concluding that the suspect engaged in deliberate sabotage and unauthorised removal of company intellectual property.

#### 4.4 Conclusion

The forensic investigation of the suspect's device has produced consistent and corroborated evidence of deliberate sabotage and unauthorised data exfiltration. All procedures were conducted in accordance with the principles established by the ACPO, to ensure that the integrity and admissibility of the evidence were maintained through the investigation. Artefacts identified within registry entries and prefetch files confirm the installation and execution of file wiping software, which indicates a clear attempt to destroy data and obstruct forensic recovery.

Additionally, analysis of browser artefacts revealed access to Google Drive, with activity occurring in close proximity to the deletion of critical files. The combination of this and the recovery of partial Autodesk Maya file fragments through file carving, supports the conclusion that sensitive company data existed on the system prior to deletion and was likely transferred to an external cloud account. A coherent sequence of events linking data access, exfiltration, and subsequent deletion, was established by the alignment of these findings.

Overall, the evidence recovered indicates that Rich Daley intentionally removed proprietary data and used anti-forensic techniques in order to hide his actions before his resignation. While some limitations exist due to encryption and secure deletion methods, the available evidence is sufficiently robust and reliable to support further legal action by Cyfusion Manufacturing Company.

### 5. Simulated Hash Log Table

**Evidence ID:** CMMC-RD-001

**Source Device:** Rich Daley Windows 11 laptop SSD

**Image File:** CMMC-RD-001.E01

**Tool Used:** FTK Imager

| Hash Algorithm | Original Hash                                                                | Image hash                                                                   | Result         |
|----------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------|----------------|
| SHA-256        | b7f4c9e1a03d6b82<br>5e14f9a7c2d85e0f<br>6a31b9c44d2e708f<br>95a6c1d3b8e24790 | b7f4c9e1a03d6b82<br>5e14f9a7c2d85e0f<br>6a31b9c44d2e708f<br>95a6c1d3b8e24790 | Verified match |
| MD5            | 9f3a7c2d4e8b1a65<br>c0d94f7e2b6a113c                                         | 9f3a7c2d4e8b1a<br>65c0d94f7e2b6a113c                                         | Verified match |

## 6. Appendix (Example FTK screenshots from a lab environment)

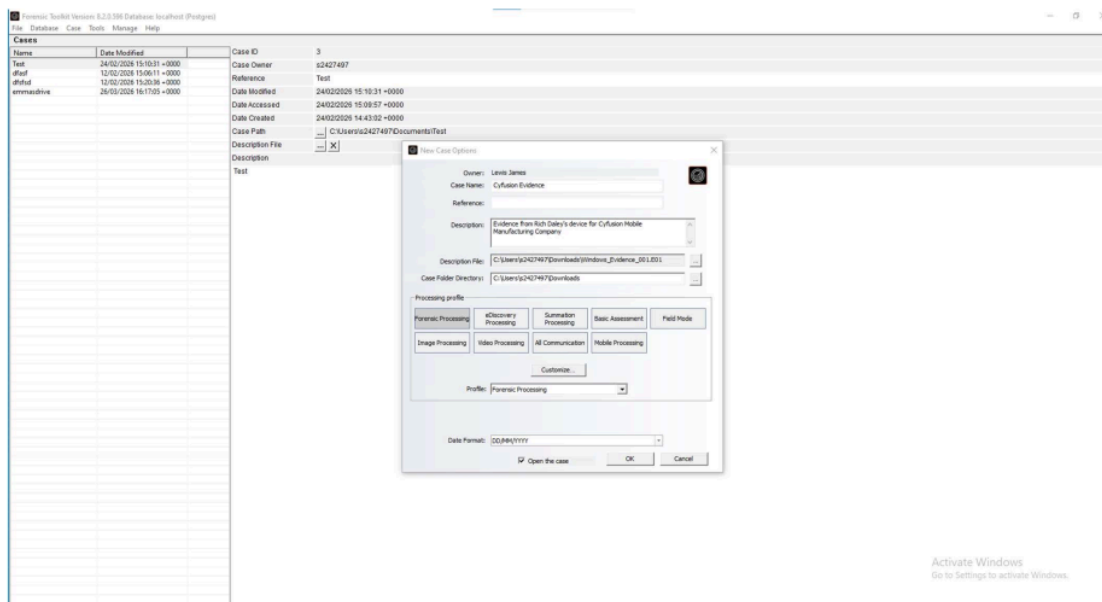


FIGURE 1. FTK IMAGER CASE CREATION SCREEN

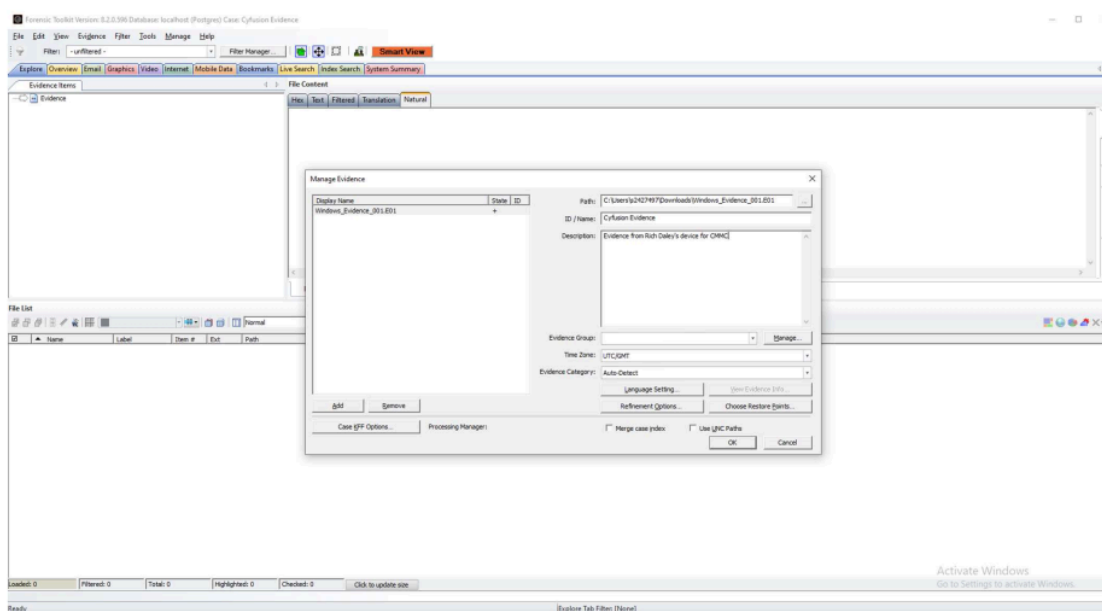


FIGURE 2. ADDING THE WINDOWS FORENSIC IMAGE IN FTK IMAGER

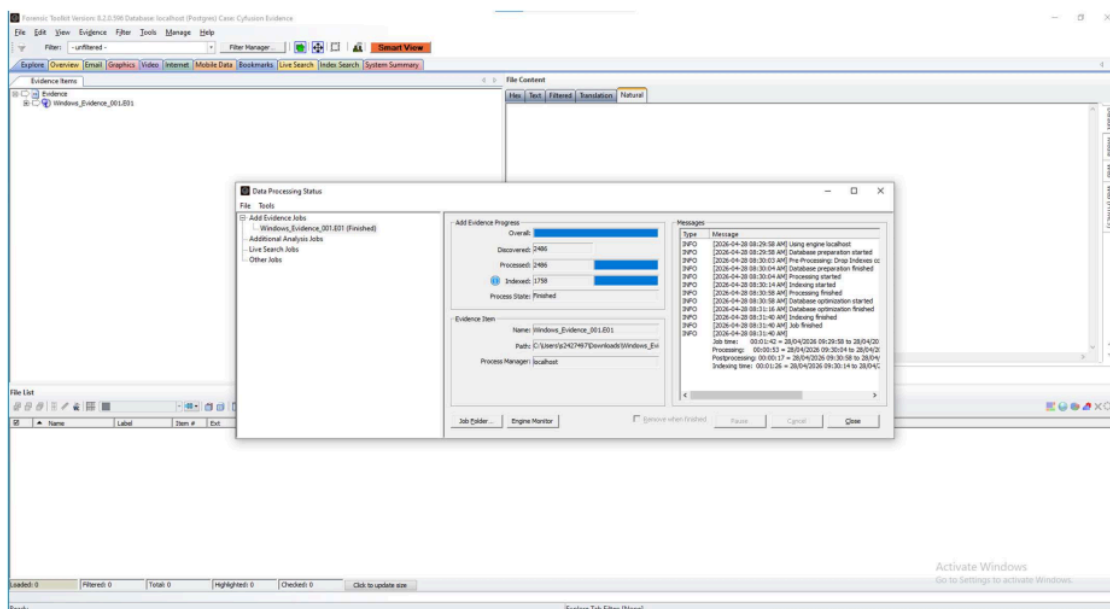


FIGURE 3. FTK IMAGER DATA PROCESSING STATUS

### Image Verification Results

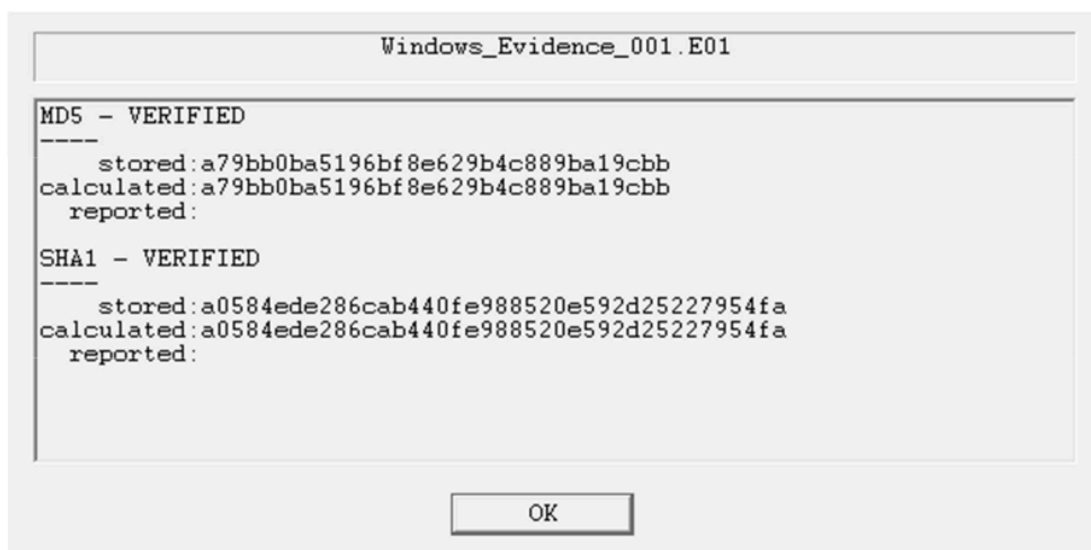


FIGURE 4. IMAGE VERIFICATION SHOWING MD5 AND SHA1 HASH VALUES

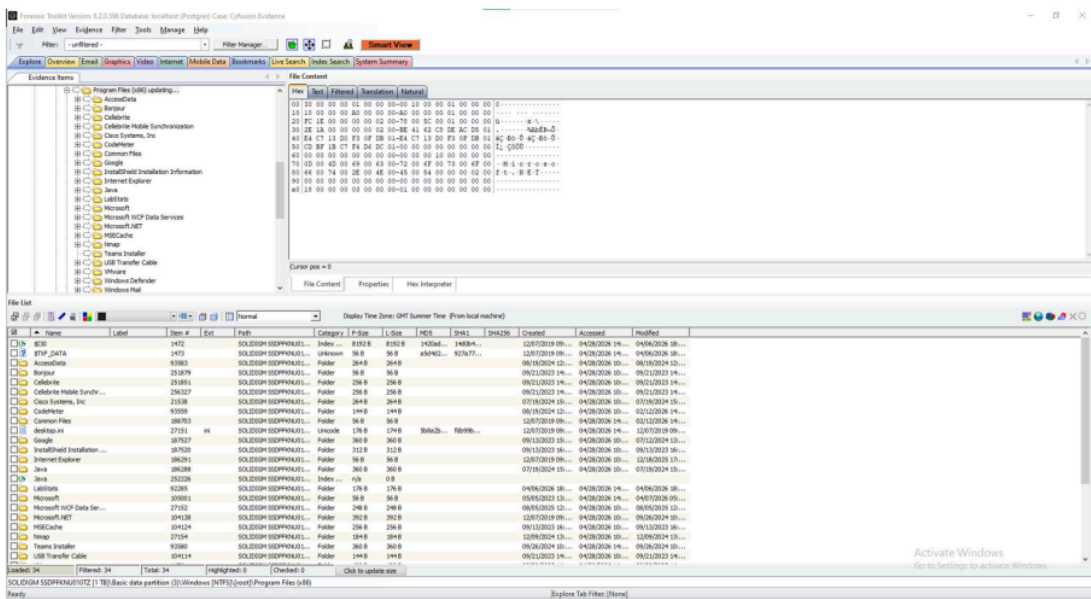


FIGURE 5. PROGRAM FILE LOCATION USED TO IDENTIFY INSTALLED WIPING TOOLS

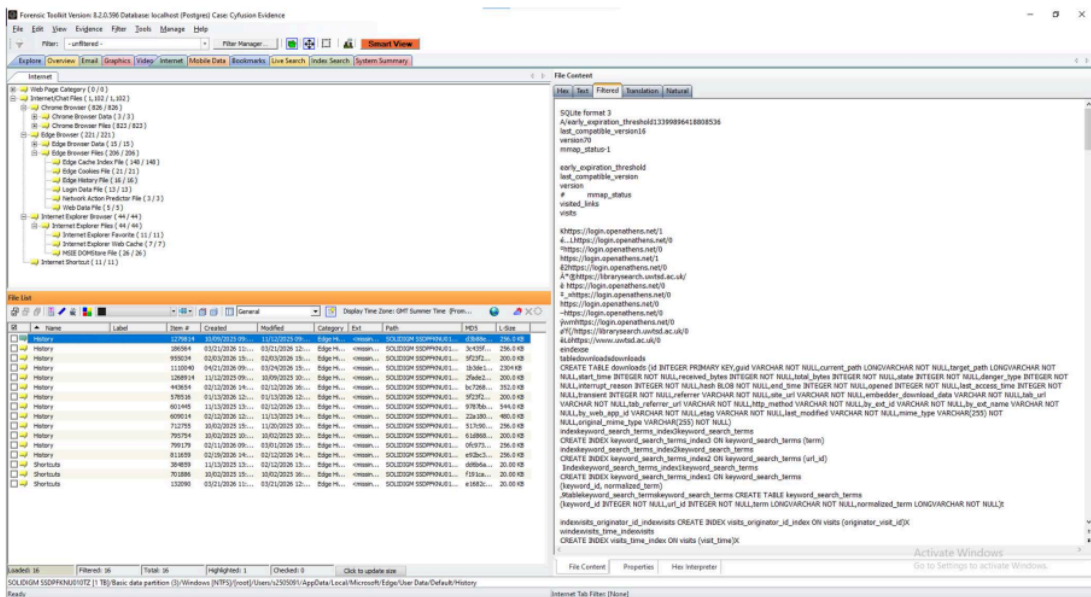


FIGURE 6. BROWSER HISTORY ARTEFACTS RELEVANT TO GOOGLE DRIVE ACCESS

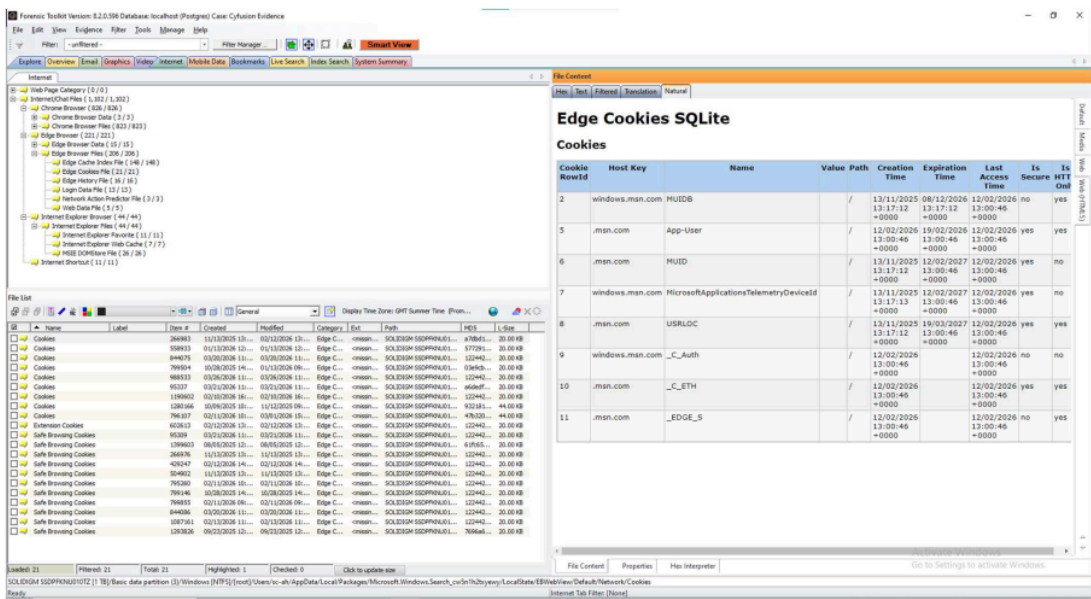


FIGURE 7. BROWSER COOKIES RELEVANT TO GOOGLE DRIVE SESSION ACTIVITY

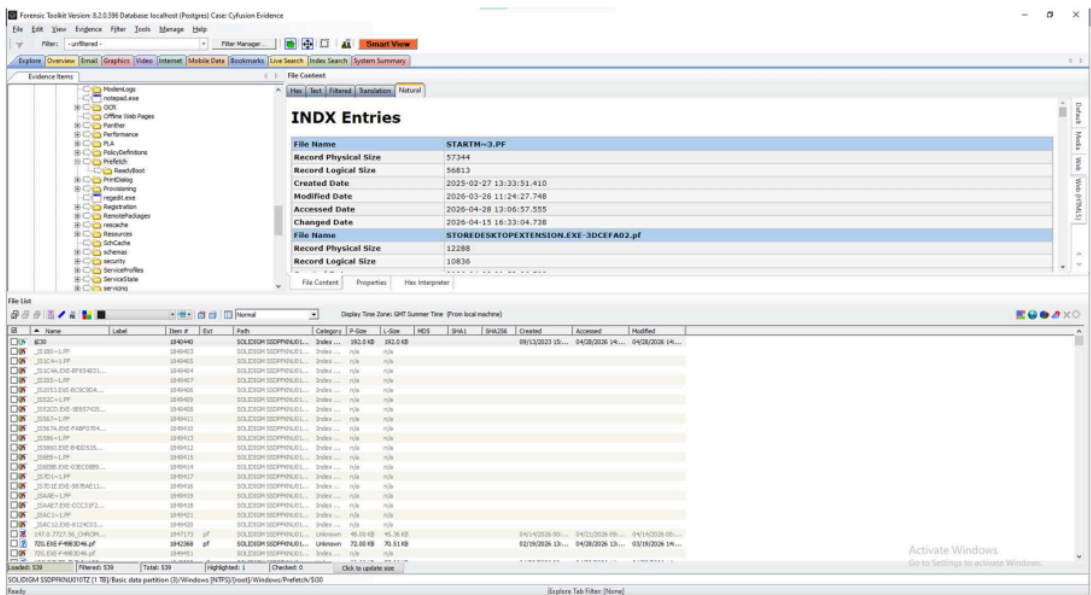


FIGURE 8. PREFETCH ARTEFACTS SHOWING EVIDENCE OF PROGRAM EXECUTION



## 7. Professional Invoice

### INVOICE

**Troy Simpson**

T.Simpson@TSForensics.com

**To:**

Ms Ker Walters  
Cyfusion Mobile Manufacturing Company  
K.Walters@CMMC.com

**Invoice #:** INV-001  
**Customer #:** CUS-001  
**Issue Date:** 21/05/2026  
**Due Date:** 21/06/2026  
**Currency:** GBP (£)  
**Amount Due:** £

| Description           | Hours | Price (£) | Amount (£) |
|-----------------------|-------|-----------|------------|
| Initial Consultation  | 1     | 20.00     | 20.00      |
| Evidence Acquisition  | 6     | 120.00    | 720.00     |
| Forensic Analysis     | 12    | 120.00    | 1440.00    |
| File Recovery         | 5     | 120.00    | 600.00     |
| Report Writing        | 6     | 120.00    | 720.00     |
| Expert Testimony Prep | 4     | 120.00    | 480.00     |
| Subtotal              |       |           | 3,970.00   |
| Tax (5%)              |       |           | 198.50     |
| Total                 |       |           | 4,168.50   |

#### Terms and Conditions

Payment is due within 1 month of issue

Make all checks payable to Troy Simpson Forensics

Please include invoice number on your check

## References

- [1] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd ed., Academic Press, 2011.
- [2] J. Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, Syngress, 2012.
- [3] Exterro, "Forensic Toolkit (FTK) Product Overview," Exterro, 2026. [Online]. Available: <https://www.exterro.com/digital-forensics-software/ftk-forensic-toolkit>.
- [4] B. Carrier, File System Forensic Analysis, Addison-Wesley, 2005.
- [5] Magnet Forensics, "Magnet Axiom | Digital Forensic Software," Magnet Forensics, 2026. [Online]. Available: <https://www.magnetforensics.com/products/magnet-axiom/>.
- [6] Association of Chief Police Officers (ACPO), Good Practice Guide for Digital Evidence, 5th ed., 2012.
- [7] Sleuth Kit Labs, "Autopsy," Sleuth Kit Labs, 2026. [Online]. Available: <https://www.sleuthkit.org/autopsy/>.
- [8] CAINE Live, "CAINE Live USB/DVD - computer forensics digital forensics," CAINE Live, 2026. [Online]. Available: <https://www.caine-live.net>.
- [9] Forensic Science Regulator and Home Office, "Forensic science activities: statutory code of practice - version 2," 5 June 2025. [Online]. Available: <https://www.gov.uk/government/publications/forensic-science-activities-statutory-code-of-practice-version-2>.
- [10] ISO, "ISO/IEC 27037:2012: Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence," International Organization for Standardization, 2012.
- [11] Scientific Working Group on Digital Evidence, "Best Practices for Computer Forensic Acquisitions, Version 2.0," 2023.
- [12] M. B. de Assumpcao, M. A. dos Reis, M. R. Marcondes, P. M. d. S. Eleuterio and V. H. Vieira, "Forensic method for decrypting TPM-protected BitLocker volumes using Intel DCI," Forensic Science International: Digital Investigation, 2023.

# Assignment Report

## GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

66/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

GRADING FORM: L5 CF (ACCD5000)

LEWIS JAMES

65.50

### ENGAGEMENT WITH LITERATURE SKI

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



The report demonstrates good engagement with relevant forensic literature, standards, and technical guidance. Appropriate references are integrated throughout the discussion, particularly regarding ACPO principles, NIST frameworks, cloud forensics, encryption, and forensic acquisition methodologies. The work reflects a clear understanding of current forensic challenges and investigative practices.

The literature review is reasonably detailed and demonstrates independent research. However,

13

some sections remain descriptive rather than critically synthesising contrasting viewpoints or evaluating the reliability and limitations of sources in greater depth.

## KNOWLEDGE AND UNDERSTANDING SK

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



The submission demonstrates shows understanding of forensic acquisition procedures, BitLocker encryption challenges, anti-forensic techniques, cloud investigations, and file carving methodologies. The explanation of forensic standards and evidential handling procedures is accurate and appropriately contextualised within the case study. Some explanations could be expanded further at a deeper technical level and critically discuss.

**6.5**

## COGNITIVE AND INTELLECTUAL SKI

*Your work must demonstrate critical analysis and evaluation of the investigation and reporting documentation. Your work must also justify Computer Forensics Investigation procedures. The labs you do in class should help you to complete the processes or forensic methods Barry would have used. (45 marks)*



The report demonstrates good analytical reasoning and effective application of forensic methodologies throughout both tasks.

**25**

The investigation methodology is logically structured and demonstrates awareness of evidential integrity, encryption barriers, cloud artefact analysis, and anti-forensic behaviour. The report also shows good understanding of how different tools align to CHFI phases.

However, some sections remain descriptive and would benefit from deeper critical evaluation of evidential reliability, operational limitations, and alternative investigative interpretations. More detailed analytical discussion of practical investigative challenges would further strengthen the intellectual depth.

## PRACTICAL SKILLS

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



The appendix provided relevant practical screenshots; numbered and named. However these figures are not use to interconnect and discuss the case scenario. This would have been a strong report if you had incorporate them into task 2 report.

**15**

## TRANSFERABLE SKILLS FOR LIFE A

*The report should be presented in an academic way (IEEE/ACM format) and therefore must include an abstract, an introduction, a conclusion*

*and a list of references. The report must be submitted via Turnitin as well. (10 marks)*



The report is structured, logically organised, and generally written in a clear academic style. You have not use the IEEE report format for task 1./ Minor grammatical inconsistencies and formatting irregularities remain throughout some sections. Greater consistency in paragraph formatting and presentation would improve the professional standard further.

**6**