

Forensics Assignment

by Drew McClennon

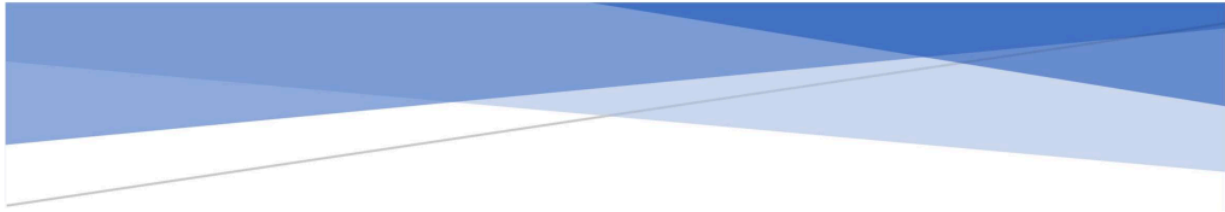
Submission date: 30-Apr-2026 12:13PM (UTC+0100)

Submission ID: 281657043

File name: 51169_Drew_McClennon_Forensics_Assignment_737277_2001234728.docx (128.19K)

Word count: 4049

Character count: 22777



SYNTHESIZE A SOLUTION TO A POTENTIAL REAL- LIFE SCENARIO

Computer Forensics – ACCD5000

Drew McClennon (2312801)
2312801@student.uwtsd.ac.uk

Table of Contents

TASK 1 : RESEARCH ASPECT ON VARIOUS TOOLS	1
INTRODUCTION.....	1
COMPARATIVE TABLE OF DIGITAL FORENSIC TOOLS	2
FTK IMAGER (IMAGING TOOL)	2
MAGNET AXIOM (COMMERCIAL FORENSIC SUITE).....	3
AUTOPSY (OPEN-SOURCE FORENSIC SUITE)	4
CELLEBRITE UFED (MOBILE FORENSICS TOOL)	5
DISCUSSION AND CRITICAL COMPARISON	5
CONCLUSION	6
TASK 2 : CASE STUDY: SABOTAGE INVESTIGATION.....	6
FORENSIC METHODOLOGY (CHFI AND ACPO)	6
METHODOLOGY & INVESTIGATION PLAN	7
<i>Identification and Initial Response</i>	7
<i>Preservation of Evidence</i>	8
<i>Acquisition from BitLocker Encrypted Drive</i>	8
<i>Examination of File System and Metadata</i>	9
<i>Deletion of Anti Forensic Activity</i>	9
<i>File Carving and Data Recovery</i>	10
<i>Browser and Cloud Synchronisation Analysis</i>	10
<i>Timeline Reconstruction</i>	11
<i>Tool Justification</i>	11
PROFESSIONAL FORENSIC REPORT	12
<i>Executive Summary</i>	12
<i>Investigation Steps</i>	12
<i>Findings</i>	12
<i>Conclusion</i>	13
<i>Simulated Hash Log</i>	13
EVALUATION OF INVESTIGATION EFFECTIVENESS	13
PROFESSIONAL INVOICE.....	14
WORKS CITED	15

Task 1 : Research Aspect on Various Tools

Introduction

Digital forensics is an important area within cybersecurity that focuses on identifying, collecting, and analysing digital evidence. Even though the core concept of digital forensics has stayed mostly the same, the methods and especially the tools used are constantly changing. This is mainly because technology is always evolving, with new operating systems, file systems, cloud platforms and mobile devices being introduced regularly.

Because of this, there is no single forensic tool that can be used for every investigation. Different tools are designed for different purposes, and investigators need to choose the correct tool depending on the type of case and

the type of evidence that they are dealing with. For example, some tools are mainly used for imaging storage devices, while others focus on analysing artifacts or extracting data from mobile phones.

EC Councils CHFI (Computer Hacking Forensic Investigator) process is typically split into several phases, including identification, preservation, collection (imaging), examination, analysis and reporting. Each phase has different requirements, and as a result, different tools are more suitable at different stages. Using the wrong tool at the wrong stage could result in missed evidence or contamination of data.

This report will critically evaluate four modern digital forensic tools:

- FTK Imager (imaging tool)
- Magnet AXIOM (commercial forensic suite)
- Autopsy (open-source forensic suite)
- Cellebrite UFED (mobile forensic tool)

These tools will be compared on cost, features, supported file systems, types of evidence analysed and reporting capabilities. The report will also discuss which tools are most suitable for different phases of the CHFI process.

Comparative Table of Digital Forensic Tools

Tool	Type	Cost	Key Features	File Systems	Evidence Types	Reporting	CHFI Phase
FTK Imager	Imaging	Free	Disk imaging, Hashing, Memory capture.	NTFS, FAT, exFAT	Disk, RAM, USB	Basic	Acquisition
Magnet AXIOM	Commercial Suite	High	Artifact parsing, Cloud Analysis, Automation	NTFS, FAT, APFS, EXT	PC, Mobile cloud	Advanced	Analysis
Autopsy	Open-Source	Free	File carving, Keyword search, Timeline	NTFS, FAT, EXT, HFS+	Disk Images	Moderate	Examination
Cellebrite UFED	Mobile	Very High	Mobile extraction, Lock bypass, Recovery	IOS, Android	Mobile Data	Advanced	Collection

FTK Imager (Imaging Tool)

FTK Imager is a digital forensic tool that is mainly used for creating forensic images of storage devices. It allows investigators to capture data from hard drives, USB devices and even system memory without modifying the original data. This is important because maintaining the integrity of evidence is a key requirement in any forensic investigation.

One of the main features of FTK Imager is its support for multiple image formats such as E01, SMART and raw (dd). It also generates hash values such as MD5 and SHA1, which are used to verify that the data has not been changed during acquisition [1]. This ensures that the evidence remains reliable and can be used in legal situations.

Another useful feature is the ability to preview files before imaging. This allows investigators to quickly check if a device contains relevant data before committing to a full acquisition [2]. It also supports memory capture, which is important when analysing volatile data such as running processes, active network connections, or malware that only exists in RAM.

FTK Imager supports common file systems such as NTFS, FAT, and exFAT, which covers most Windows-based systems. However, support for other file systems is more limited compared to full forensic suites. This can be a disadvantage when dealing with Linux or macOS systems.

There are also some limitations. FTK Imager does not provide advanced analysis tools, meaning it cannot perform tasks such as timeline reconstruction or artifact parsing. It also has very limited reporting capabilities, so it is not suitable for presenting findings.

Overall, FTK Imager is best suited for the collection and acquisition phase of the CHFI process. It is reliable, easy to use and ensures that evidence is captured correctly, but it must be used alongside other tools for full investigations.

Magnet AXIOM (Commercial Forensic Suite)

Magnet AXIOM is a commercial digital forensic tool that is designed to analyse data from multiple sources, including computers, mobile devices, and cloud services. It is widely used in professional environments because of its advanced features and ability to handle complex investigations.

One of the key strengths of Magnet AXIOM is its artifact-based analysis. Instead of manually searching through files, the tool automatically identifies and categorises relevant data such as emails, chat messages, browser history and social media activity [3]. This saves a significant amount of time and reduces the chances of missing important evidence.

It supports a wide range of file systems including NTFS, FAT, EXT, and APFS, which makes it suitable for analysing data from different operating systems. It also has strong support for cloud-based evidence, including data from services such as

Google Drive and social media platforms [4]. This is important because a large amount of modern data is stored in the cloud rather than on local devices.

Magnet AXIOM also includes advanced features such as timeline analysis, keyword searching and data visualisation. These features help investigators understand how events occurred and identify patterns within the data. The tool can also link evidence from multiple sources, which is useful in cases involving multiple devices.

Another major advantage is its reporting capabilities. Magnet AXIOM can generate detailed, structured reports that include timelines, categories and visual representations of the evidence. These reports are useful for presenting findings in court or to clients.

However, there are some disadvantages. The tool is quite expensive, which can make it inaccessible for smaller organisations or students. It also requires high performance hardware, as analysing large datasets can be resource intensive. In addition, because the tool automates many processes, there is a risk that investigators may rely too heavily on it without fully understanding the underlying data.

Overall, Magnet AXIOM is best suited for the analysis and reporting phases of the CHFI process. It provides powerful features that make it easier to analyse large amounts of data, but it comes at a high cost.

Autopsy (Open-Source Forensic Suite)

Autopsy is an open-source digital forensic tool that provides a graphical interface for analysing digital evidence. It is built on The Sleuth Kit and is commonly used in both educational and professional environments.

One of the main advantages of Autopsy is that it is completely free, which makes it accessible for students and organisations with limited budgets. Despite being free, it still provides a range of useful features such as file carving, keyword searching, hash filtering and timeline analysis [5]. These features allow investigators to examine disk images and recover deleted files.

Autopsy supports multiple file systems including NTFS, FAT, EXT, and HFS+, which makes it suitable for analysing data from different platforms. It also supports plugins, which allow users to extend its functionality depending on their needs.

The tool can generate reports in formats such as HTML and PDF, which can be used to document findings, however, these reports are not as advanced nor customisable as those produced by commercial tools.

There are also some limitations. Autopsy can struggle with performance when dealing with large datasets, which can slow down investigations. It also lacks official support, meaning that users must rely on community resources. Compared to commercial tools, it has fewer automation features, and a less intuitive interface [6], which means more manual work is required.

Another limitation is that while Autopsy is good for disk analysis, it has limited capabilities when it comes to cloud and mobile data. This means it is not suitable as a complete solution for modern investigations.

Overall, Autopsy is best suited for the examination and analysis phases of the CHFI process. It provides a strong set of features for a free tool, but it may need to be combined with other tools for more complex cases.

Cellebrite UFED (Mobile Forensics Tool)

Cellebrite UFED (Universal Forensic Extraction Device) is a specialised forensic tool used for extracting and analysing data from mobile devices. It is widely used by law enforcement and forensic professionals because of its ability to handle a wide range of devices and data types.

One of the key features of UFED is its ability to perform both logical and physical data extraction. This means that it can recover data such as messages, call logs, contacts, photos and even deleted files [7]. It can also bypass security features on some devices, which makes it very useful in investigations.

UFED supports both iOS and Android devices, as well as some older mobile systems. It can extract data from apps such as messaging services, social media platforms, and GPS systems. This is important because a large amount of personal data is stored on mobile devices.

The tool also provides strong reporting capabilities, generating detailed reports that can be used in legal proceedings. These reports are designed to be clear and easy to understand, which is important when presenting evidence.

However, UFED is very expensive and requires specialised training to use effectively. It is also limited to mobile devices, meaning it cannot be used for analysing computer systems or networks. Another issue is that mobile security is constantly evolving, which means the tool may not always be able to access the latest devices.

Overall, Cellebrite UFED is best suited for the collection and mobile analysis phases of the CHFI process. It is one of the most effective tools for mobile forensics, but it must be used alongside other tools for a full investigation.

Discussion and Critical Comparison

When comparing these tools, it is clear that each one has a specific role within the forensic process. FTK Imager focuses on acquisition, Autopsy and Magnet AXIOM focus on analysis, and UFED focuses on mobile data.

One key point is that open source and commercial tools both have their advantages. Autopsy is free and accessible, but it lacks some of the advanced

features and performance of tools like Magnet AXIOM. On the other hand, commercial tools provide more automation and support but come at a high cost.

Another important factor is the type of evidence being analysed. Traditional disk based tools like Autopsy and FTK Imager are effective for analysing hard drives, but they are less effective when dealing with cloud or mobile data. This is where tools like Magnet AXIOM and UFED become more important.

There is also a trade off between automation and control. Tools like Magnet AXIOM automate many processes, which can save time, but may reduce the investigator's understanding of how the data is processed. In contrast, tools like Autopsy require more manual work but give the investigator greater control.

In modern investigations, it is becoming more common to use multiple tools together. For example, an investigator might use FTK Imager to create a disk image, analyse it using Autopsy, and then use Magnet AXIOM for deeper analysis and reporting. This approach helps ensure that evidence is thoroughly examined and verified.

Conclusion

In conclusion, digital forensics tools are essential for investigating and analysing digital evidence, but no single tool can handle every situation. Each tool has its own strengths and weaknesses and must be used at the appropriate stage of the CHFI process.

FTK Imager is ideal for acquiring data while maintaining integrity, Autopsy provides a strong source solution for analysis, magnet AXIOM offers advanced features for complex investigations, and Cellebrite UFED is highly effective for mobile forensics.

Overall, investigators should use a combination of tools to ensure accurate and reliable results, as technology continues to evolve, forensic tools will also continue to change making it important for investigators to stay up to date and adapt to new challenges.

Task 2 : Case Study: Sabotage Investigation

Forensic Methodology (CHFI and ACPO)

Digital forensic investigations much follow a structured methodology to ensure that any evidence collected is reliable, repeatable and legally admissible. In the UK, investigations commonly follow the ACPO (Association of Chief Police Officers)

principles alongside structured forensic processes such as the CHFI model. Both of these frameworks are important in this case because there is only a single device available as evidence, and there are risks such as encryption and anti forensic activity that could result in data loss if not handled properly.

The ACPO principles are designed to protect the integrity of evidence:

1. No action should change data that may be relied upon in court.
2. If it is necessary to access original data, it must be done by a competent person.
3. A full audit trail must be maintained so another examiner could follow the same process.
4. The person in charge of the investigation is responsible for ensuring compliance with the law.

These principles are especially important here because the suspect used a file-wiping tool and full disk encryption, this means that improper handling of the device could destroy potential evidence permanently.

The investigation will follow the CHFI phases, which include:

- Identification: Recognising the incident and available evidence.
- Preservation: Securing the evidence to prevent alteration.
- Collection (Acquisition): Creating forensic copies.
- Examination: Identifying relevant data.
- Analysis: Interpreting the evidence.
- Reporting: Presenting findings clearly.

Each stage is important and must be completed carefully. For example, if acquisition is not performed correctly, the data may not be trusted in court. Similarly, if the analysis is not thorough, evidence such as cloud activity or deletion traces could be missed.

Methodology & Investigation Plan

Identification and Initial Response

The first stage is identifying the incident and the available evidence. In this case, the incident involves suspected sabotage and data theft by Rich Daley. The only available evidence is his company issued Windows 11 workstation.

At this stage, the investigator must assess the risks. The system uses BitLocker full disk encryption which means that the data is protected using encryption keys. If the system is powered off before capturing those keys, it may prove difficult or impossible to access the data. There is also evidence that a file wiping tool was used, which suggests that the suspect attempted to destroy evidence.

The system should be immediately isolated from the network to prevent any further activity. If the system is still powered on, a live forensic response should be considered. This is important because live systems contain volatile data which is lost when the device is powered off.

During live acquisition, the following should be captured:

- RAM (Memory dump)
- Running processes
- Network connections
- Logged in user sessions

RAM is particularly important because BitLocker encryption keys are often stored in memory while the system is running. Capturing RAM increases the chances of accessing the encrypted disk.

Preservation of Evidence

Preservation ensures that evidence is not modified during the investigation. The system should be handled in a secure environment, and access should be restricted.

If the system is live, volatile data should be captured first. After this, the system can be powered down in a controlled way. Write blockers should be used when accessing storage devices to prevent accidental modification.

A chain of custody must be maintained throughout the investigation. This includes documenting:

- Who collected the evidence
- When it was collected
- How it was stored
- What actions were performed

Maintaining this documentation ensures that the evidence is admissible in court and can be trusted.

Acquisition from BitLocker Encrypted Drive

The acquisition phase is more complex in this case because the system uses BitLocker encryption. BitLocker encrypts the entire disk using AES (Advanced Encryption Standard) encryption, meaning that without the correct key, the data appears unreadable.

If the system is still unlocked, FTK Imager can be used to create a forensic image of the disk in its decrypted state. This is the preferred approach because it allows access to all files.

If the system is locked, investigators may need to:

- Extract the encryption keys from the RAM
- Analyse the hibernation file (hiberfil.sys)
- Check for the recovery keys stored on the system

Once access is gained, a full forensic image should be created. This includes:

- System partitions
- User files
- Unallocated space
- Slack space

FTK Imager is suitable for this task because it creates a bit by bit copy of the disk and generates hash values (MD5 and SHA1) to verify integrity. Hash values must be recorded before and after imaging to ensure that the data has not been altered.

Examination of File System and Metadata

After acquisition, the forensic image is analysed using Autopsy.

This stage involves examining the file system to identify relevant data. Investigators should analyse:

- Directory structures
- File metadata (timestamps, size, ownership)
- Deleted file records

Even if files have been deleted, metadata often remains in the MFT (Master File Table). This can provide important information such as file names and timestamps.

Investigators should look for:

- Missing Autodesk Maya project files
- Unusual file activity before resignation
- Evidence of large scale deletion

Autopsy provides tools for analysing file systems and identifying deleted files making it suitable for this stage.

Deletion of Anti Forensic Activity

One of the main objectives is to prove that Rich used a file wiping tool to destroy evidence.

Wiping tools overwrite data multiple times to prevent recovery. However, they often leave traces behind.

The investigators should look for:

- Installed wiping software
- Registry entries showing installation and execution
- Prefetch files indicating program usage
- Event logs showing deletion activity

Prefetch files are especially useful because they record when a program was last executed. If a wiping tool was run shortly before Rich resigned, this suggests intentional deletion.

Magnet AXIOM can also detect patterns such as sudden deletion of large numbers of files, which may indicate sabotage.

File Carving and Data Recovery

Recovering the deleted Autodesk Maya files is a key objective.

File carving works by scanning the disk for file signatures rather than relying on the file system. This allows recovery of deleted data even if the file records are missing.

Autopsy can be used to perform file carving, focussing on:

- .ma and .mb file formats
- Temporary files
- Autosave backups

Autodesk Maya often creates autosave files, which may still exist even if the main files were deleted. These files can contain significant portions of the original data.

Investigators should also examine:

- Unallocated space
- Slack space
- Shadow copies

However, if a wiping tool has been used effectively, recovery may be limited. This is because the data may have been overwritten.

Even partial recovery can still provide useful evidence, such as proving that the designs existed.

Browser and Cloud Synchronisation Analysis

Since Rich uploaded files to Google Drive, analysing browser artifacts is essential.

Magnet AXIOM can extract:

- Browser history
- Cookies and session data
- Cached files
- Cloud artifacts

Investigators should look for:

- Access to Google Drive
- Timestamps of activity
- Login sessions
- File names or metadata

Even if the actual files are not present locally, evidence of upload activity can still be found. This can be used to prove that the data was transferred outside of the company.

Timeline Reconstruction

Timeline analysis is used to reconstruct events in chronological order.

By combining data from file systems, logs, and browser artifacts, investigators can build a timeline showing:

- When files were accessed and deleted
- When wiping software was executed
- When Google Drive was accessed
- Login and logout times

Magnet AXIOM provides automated timeline features that make this process easier.

This helps provide a clear sequence of events that led up to Rich's resignation.

Tool Justification

The tools used in this investigation were selected based on their capabilities:

- FTK Imager: Used for acquisition because it ensures the data remains unchanged.
- Autopsy: Used for file system analysis and file recovery.
- Magnet AXIOM: Used for advanced analysis, cloud artifacts, and timelines.

Using multiple tools improves reliability and allows results to be verified.

Professional Forensic Report

Executive Summary

This report presents the finding of a forensic investigation into suspected sabotage and data theft carried out by Rich Daley at Cyfusion Mobile Manufacturing Company (CMMC).

The investigation focused on analysing a BitLocker encrypted Windows 11 system. Evidence indicates that Rich intentionally deleted Autodesk Maya design files using a file wiping program and transferred sensitive data to a personal Google Drive account.

Despite attempts to remove evidence, forensic analysis identified traces of anti forensic activity, partial recovery of deleted data and browser artifacts showing cloud access.

The findings strongly support the conclusion that Rich Daley deliberately sabotaged company data and attempted to exfiltrate confidential designs.

Investigation Steps

Step 1 – The system was secured and isolated to preserve evidence.
Step 2 – A forensic image was created using FTK Imager, and RAM was captured.
Step 3 – Autopsy was used to examine file systems and metadata.
Step 4 – Magnet AXIOM was used for advanced analysis and timeline reconstruction.
Step 5 – Findings were documented for legal purposes.

Findings

Anti Forensic Activity

- Wiping software was installed and executed
- Prefetch files confirm execution shortly before resignation
- Registry entries confirm usage

Deleted File Evidence

- Missing Autodesk Maya files identified
- Metadata confirms previous existence
- Partial file fragments recovered

Cloud Activity

- Browser history shows access to Google Drive
- Login sessions linked to personal account
- Timestamps match suspicious activity

Timeline Evidence

- Increased activity before resignation
- Execution of wiping software
- Cloud uploads occurred

System Observations

- No backups were present
- Only one user had access
- High value data stored locally

Conclusion

The evidence strongly suggests that Rich Daley intentionally sabotaged company data.

He used a file wiping tool to delete important files and attempted to remove evidence. He also accessed Google Drive and likely transferred confidential designs.

Even though full recovery of the files was not possible, enough evidence exists to demonstrate intent and support legal action.

Simulated Hash Log

Evidence	Algorithm	Hash Value
Disk Image	MD5	a3f5c9d82b1e4a7c9d3e5f7a1b2c3d4e
Disk Image	SHA1	b7c8d9e0f1a2b3c4d5e6f7a8b9c0d1e2f3a4b5c6
RAM Dump	MD5	c4d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9
RAM Dump	SHA1	d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0b1c2d3e4

Evaluation of Investigation Effectiveness

The investigation was effective in identifying key evidence, despite the use of encryption and anti forensic techniques.

One strength was the use of multiple forensic tools, which allowed cross-verification of results. Another strength was focussing on artifacts such as logs and metadata, rather than relying only on file recovery.

However, there were limitations. The use of a wiping tool reduced the chances of recovering full files. The lack of backups also made recovery more difficult.

Despite these challenges, enough evidence was found to support the conclusion.

Professional Invoice

Troy Simpson Forensics – London, UK

Description	Hours	Rate (£/hr)	Total (£)
Evidence Acquisition	8	120	960
Forensic Analysis	28	120	3360
Data Recovery Attempts	18	120	2160
Cloud & Browser Analysis	16	120	1920
Report Writing	16	120	1920
Expert Testimony Prep	12	120	1440

Subtotal : £11,760
VAT (20%) : £2,352
Total: £14,112

Works Cited

- [1] Wikipedia, "Forensic Toolkit (FTK)," [Online]. Available: https://en.wikipedia.org/wiki/Forensic_Toolkit. [Accessed April 2026].
- [2] Exterro, "Digital Forensics Exterro FTK Imager," [Online]. Available: <https://www.exterro.com/digital-forensics-software/ftk-imager>. [Accessed April 2026].
- [3] Cotocus, "Top 10 Digital Forensics Tools: Features, Pros, Cons & Comparison," 3 January 2026. [Online]. Available: <https://www.cotocus.com/blog/top-10-digital-forensics-tools-features-pros-cons-comparison/>. [Accessed April 2026].
- [4] Magnet Forensics, "All Your Case Data in Magnet AXIOM: Pt 3 — Bringing in Computer Data," 6 August 2020. [Online]. Available: <https://www.magnetforensics.com/blog/all-your-case-data-in-magnet-axiom-pt-3-bringing-in-computer-data/>. [Accessed April 2026].
- [5] Wikipedia, "Autopsy (software)," [Online]. Available: [https://en.wikipedia.org/wiki/Autopsy_\(software\)](https://en.wikipedia.org/wiki/Autopsy_(software)). [Accessed April 2026].
- [6] Priteshgeek, "Top 10 Digital Forensics Tools in 2026: Features, Pros, Cons & Comparison," 24 October 2025. [Online]. Available: <https://www.scmgalaxy.com/tutorials/top-10-digital-forensics-tools-in-2025-features-pros-cons-comparison/>. [Accessed April 2026].
- [7] Cellebrite, "UFED," [Online]. Available: <https://cellebrite.com/en/products/ufed/>. [Accessed April 2026].

Forensics Assignment

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

51 /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

DREW MCCLENNON

51

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)



Your report demonstrates engagement with relevant forensic concepts, investigative methodologies, and forensic technologies. Appropriate references are included regarding forensic imaging, anti-forensic activity, browser artefacts, and forensic reporting procedures. However, much of the discussion remains descriptive rather than critically synthesised, and stronger engagement with peer-reviewed forensic literature would improve the academic depth further.

12

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 understanding of forensic acquisition, evidence preservation, anti-forensic activity, browser analysis, and forensic workflow procedures.

The report applies CHFI and ACPO principles throughout the investigation discussion. However, some technical explanations remain generalised and lack deeper precision.

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 some analytical reasoning and understanding of investigative workflow sequencing. The discussion identifies relevant forensic procedures and investigative considerations.

However, much of the report remains procedural and descriptive, with limited sustained critical evaluation of evidential reliability, investigative limitations, anti-forensic complexity, or forensic validation challenges. Greater analytical depth and evidential interpretation would significantly strengthen the intellectual quality of the submission.

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 submission demonstrates limited practical forensic evidence and investigative artefact integration. While an invoice and general investigative workflow are included, the practical evidence required by the assessment brief is only partially demonstrated. The report lacks sufficient annotated forensic screenshots, contextualised wiping-tool analysis outputs, and properly evidenced forensic artefacts expected. The practical application therefore remains limited and insufficiently evidenced compared to stronger submissions.

7.5

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)



You have not use the IEEE report format for task 1. The report is generally readable and logically structured. Appropriate headings and technical terminology are used throughout. However, formatting consistency, paragraph presentation, grammar, and academic writing

4.5

fluency are inconsistent in several sections.
Referencing and presentation standards require
further refinement to meet stronger professional
expectations