

Josh Longhurst 2205415

Assignment

by Josh Longhurst

Submission date: 29-Apr-2026 08:01PM (UTC+0100)

Submission ID: 281562301

File name: 60799_Josh_Longhurst_Josh_Longhurst_2205415_Assignment_737277_2031832284.docx (1.19M)

Word count: 4172

Character count: 24809



ASSIGNMENT 1

Computer Forensics - ACCD5000

Joshua Longhurst

2205415

2205415@student.uwtsd.ac.uk

Cybersecurity and Computer Networks

DDA

Contents

Task 1	1
Task 2	2
Methodology and Investigation Plan	3
Task 3	5
Legal Report.....	5
Task 4	13
Invoice.....	16
TROY SIMPSON FORENSICS	16
INVOICE	16
Qty/Hrs/Days	16
Total.....	16
Rate.....	16
Services/Items.....	16

Acronyms

CHFI: Computer Hacking Forensic Investigator

ACPO: Association of Chief Police Officers

CMMC: Cyfusion Mobile Manufacturing Company

TPM: Trusted Platform Module

USB: Universal Serial Bus

RD: Rich Daley

Task 1

Forensic Tool	Usage	Cost	Key Features	Supported File Systems	Type of Evidence analysed	Reporting Capability	Strengths	Limitations
FTK Imager	Free Commercial imaging tool [1]	Free (£0) [1]	Disk Imaging, hashing	FAT, NTFS, exFAT, EXT [2]	Disk Images, USB Drives, Memory Captures [3]	Basic Export and Hash reporting	Fast ingest speed, high forensic integrity,	Limited analysis no mobile or cloud supported,

							user friendly GUI	built for Windows Install Only [4]
Magnet AXIOM	Commercial	Reported around – \$5k [5]	Artifact-based analysis, automation, cloud and mobile integration	NTFS, FAT, EXT, APFS, HFS+ [6]	Mobile devices, cloud, including chats, logs and apps [7]	Automated reports with timelines and dashboards	All in one, automation, covers a wide variety of devices and evidence [8]	Expensive and resource intensive when installed [8]
Autopsy	Open Source	Free (£0) [8]	File Carving, Keyword searching, timeline analysis	NTFS, FAT, EXT, HFS+ [9]	Disk Images, deleted files, RAM	Customisable reporting using html and keyword search results	Cost-effective, transparent and extensible	Slow with limited cloud and mobile support/integration
Cellebrite	Commercial	£16,500 [10]	Mobile extraction, decryption, app analysis, cloud extraction [11]	Mobile OS file systems such as IOS or Android Proprietary FS	Mobile data, app data, cloud backups and communications	Provides high detailed and structured reports which includes location data, calls and chats	Industry leader in mobile forensics, supported across almost all mobile OS's and can retrieve evidence from iCloud and Google Drive	Expensive, narrow scope [12]

Research and Critical Evaluation Discussion

FTK Imager

FTK Imager is a free strong and dependable resource used in imaging devices. Its ability to create validated forensic level images is unequalled when compared to other free resources used in the digital forensic world. It holds the capabilities to analyse external drives, Disk images and Memory captures. The tool includes multiple supported file types, which includes FAT, NTFS, exFAT and EXT. However, whilst it functions across many file types it has limited analysis features such as lacking in complex file carving, cloud analysis and mobile analysis. In complete investigations the tool should be used in combination with more thorough analysis tools due to its limitations with analysis and basic capabilities. FTK Imager, does come with its own strengths such as fast ingest speed within its user-friendly GUI. [13]

Magnet AXIOM

Magnet AXIOM is a high-level forensic tool, which is backed by professionals in the digital forensics field. It is favoured by professionals as it includes functionality to analyse mobile devices, the cloud, computers and the depth of analysis it covers such as chats, logs and application data. However, whilst it is backed by professionals, it does have areas of weakness such as bottlenecks during processing due to rapid processing on large data amounts. The tool also is resource intensive due to its deep scanning capabilities; it requires high powered workstations. In a complete investigation, it is advised Magnet AXIOM is used in a conjunction with another tool to further verify findings. [14]

Autopsy

Autopsy is a widely used, open-source resource which is considered strong in industry. The tool is used to analyse deleted files, RAM and disk images. Autopsy is highly regarded by professionals for robustness, reporting capabilities and cost effectiveness. It acts as a GUI for the Sleuth Kit and offers functions such as timeline analysis, automated ingestion and keyword searching function. It is highly effective as a primary tool for triage and comprehensive disk analysis. However, Autopsy does have its limitations such as slowness when handling large datasets and interpretation of results requires expertise. It also has limitations on the analysis of mobile artifacts this is where tools such as Cellebrite excel. [15]

Cellebrite

Cellebrite is a widely recognised and highly dominant platform used in the digital forensics industry. The tool supports a variety of devices including mobile phone operating systems such as IOS and Android. It also excels in data extraction as it has the functionality to bypass lock screens and decryption of data. However, it also comes with weakness such as overall costs as it requires significant hardware, specialised training and of course the software licence. The average cost per licence for Cellebrite comes in at around £16,500 and as the software is resource intensive a powerful device is required which stretches the cost further. Along with the product costs, specialised training is required to operate this powerful tool which adds to the cost an average of around £3,500. So before even starting an investigation, costs can total over £20,000 and that is before staff wages to support the operation. Whilst it supports a variety of devices which is thought to be over 4000 device types it does have technical limitations such as limited capability to support older phones and devices such as GSM Phones. This is due to rapid delivery and keeping up with new handsets and operating systems. [16] [17]

Task 2

Methodology and Investigation Plan

The investigation into Rich Daley who previously worked at Cyfusion Mobile Manufacturing Company (CMMC) will be conducted in accordance with digital forensic principles CHFI and ACPO. This will ensure all evidence is handled with care and in a manner, that's observes

its integrity and tolerance to be used in a court of law. The principles outline that no action should alter original evidence, all processes must be carried out by competent personnel, and a full audit trail must be created and maintained throughout the full investigation ensuring all actions are documented.

Throughout the investigation a strict chain of custody will be maintained to document the evidence and the handling of the evidence ensuring its integrity and tolerability in a court of law. [18]

The first part of the investigation will be the acquisition of evidence from the encrypted drive based on the CHFI and ACPO principles. The device is protected using BitLocker which is a full disk encryption tool provided by Microsoft. I will identify the BitLocker encryption Authentication. There are 6 different authentication methods of BitLocker, listed below –

1. TPM Only
2. TPM + PIN
3. Password
4. TPM + PIN + USB Key
5. External Key
6. Azure stored Recovery Key

Should Rich Daley's system be unlocked, this will allow for me to start in a strong position. I will prioritise preserving the live condition of the device as BitLocker will already be unlocked and drives decrypted. As the decryption keys will be stored in RAM it will enable direct acquisition. It will also permit for capturing volatile data such as active browser sessions, potentially Google Drive Authentication Tokens and recently accessed files held in RAM. To preserve the integrity of the evidence, I will follow a forensic bit-by-bit image of encryption which will be in RAW format. The data acquisition will occur using a write-blocker, this will prevent potential accidental or malicious modification to the original data that may need to be used in a court of law as evidence. FTK Imager will then be used to acquire the disk image before generating cryptographic hash values to verify its integrity. On the basis the laptop is powered on, live acquisition techniques will be deployed to capture volatile memory to extract potential encryption keys. Detailed analysis will be then conducted to identify traces of the wiped project files.

Following the acquisition stage, the route of the investigation will inspect the system for evidence of potential anti-forensic activity carried out by Rich Daley before tendering his resignation. We are aware that Rich used a file wiping tool to erase Autodesk Maya project files prior to his departure from CMMC. Anti-Forensic techniques are often used to conceal malicious actions by deleting or overwriting data. My analysis will focus on identifying traces of tools or installations and system logs. Additionally, the disk can be analysed for signs of overwritten or adjustments to sectors which are strong indicators of secure deletion which falls under Anti-Forensic techniques. Autopsy will be used to detect any potential malicious actions and provide evidence of deliberate data destruction. However, the identification and awareness of Rich erasing Autodesk Maya project files prior to his

departure would strongly support the conclusion that deletion was intentional, and this was an anti-forensic technique used by Rich Daley at CMMC.

The next phase of the investigation involves file carving which is the recovery of the deleted Autodesk Maya design files. As the file system metadata has been removed, file carving techniques will need to be deployed to recover data directly from unallocated disk space which requires scanning the disk image and reconstructing files from headers and footers. Autopsy will carry out this process and will analyse RAW data. In file carving even partial files could provide crucial evidence.

In addition to data destruction there is evidence that suggests Rich uploaded files from this company system to a Personal Google Drive. To investigate this, browser details on the system will be examined to identify interactions with cloud services. In order to carry this out, information on browsing history, cookies and cached files will be analysed to determine whether files were uploaded or accessed through a Google Drive. Magnet AXIOM is well-suited for this part of the investigation as it can extract cloud artefacts and reconstruct user activity. Identifying evidence such as this would be critical for demonstrating that company data was transferred out of the organisation.

Finally using all evidence collected, examined and analysed during the investigation will be connected through timeline analysis to reconstruct the clear timeline of events to implement into a report. The reporting stage will include the integration of evidence from disk analysis, file recovery and browser artefacts. It will allow investigators to present a consistent and clear comprehensive timeline and report that will narrate the defendant's actions.

In conclusion, the investigation will adopt a systematic approach to investigating evidence of sabotage and data exfiltration. The investigation will see a combination of forensic imaging, anti-forensic techniques detection, file recovery and cloud examinations. The aim of the investigation is to provide clear, detailed and defensible evidence of wrongdoings in the workplace. The use of industry-recognised tools and software will be used to gather this evidence. The investigation will need to adhere to digital forensic principles CHFI and ACPO which will allow for the evidence to be heard in a court of law.

Task 3

Forensic Report

CMMC Digital Forensic Examination Report

Prepared For: Ms Ker Walters

Prepared By: Troy Simpson Forensics

Subject: Forensic Investigation into Rich Daley

April 2026

Forensic Summary 1.0

Introduction 1.1

This report will present the findings of the digital forensic investigation conducted by Troy Simpson Forensics on behalf of Cyfusion Mobile Manufacturing Company on a organisation issued Windows 11 machine assigned to former Cyfusion Mobile Manufacturing Company employee and user Rich Daley. Throughout this report Rich Daley, will be referred to as Mr Daley.

Projects 1.2

Mr Daley was involved in high level projects which included designs for the latest Samsung Galaxy Z Flip 6 and a GUI interface for the new Apple iPhone 17 flip which all represent a high financial investment from CMMC. It is understood Mr Daley contacted competitors of CMMC and had planned to release the designs and further confidential information to the competition, it is confirmed he contacted 360Tech and had struck a deal to sell the design to them. CMMC use a software called Autodesk Maya to conduct designs for the new upcoming technology.

The project represented significant intellectual property value for CMMC with the designs being strong areas for patent protection and it could provide CMMC with a competitive advantage commercially and financially.

Following Mr Daley's Resignation, it was confirmed, CMMC engineers discovered several Autodesk Maya Files to be missing from the workstation. Subsequent concerns were raised internally which suggested that Mr Daley had intention to sabotage the project and organisation by selling designs to 360Tech.

Investigation Overview 1.3

The conducted investigation confirms Mr Daley used a secure file wiping tool called Eraser to delete Autodesk Maya Files. It is also confirmed that he accessed a personal Google Drive account via the web browser to sync files from the workstation in question. His company workstation was the only device available to conduct the investigation. All evidence analysed was acquired and analysed in accordance with ACPO and CHFI principles allowing admissibility in legal proceedings, should CMMC consider legal proceedings.

Investigation Steps 2.0

Forensic Acquisition 2.1

The workstation was protected with BitLocker Full-Disk Encryption. Upon triage of the device, it was found to be powered on and unlocked which provided with immediate access to the decrypted storage volume and volatile memory. The live condition of the device was preserved to prevent BitLocker re-enabling which would cause volatile memory to be lost and encryption of the storage volume. A hardware write-blocker was used to ensure no modification occurred to the original primary evidence source. FTK Imager was then deployed to create a forensic bit-by-bit RAW image of the internal drive and generate MD5

The screenshot displays the Windows Security Event Viewer interface. The top pane shows a list of events, including 'Windows_Evidence' (ID 1822) and 'Windows_Evidence' (ID 1823). The bottom pane provides a detailed view of the selected event, showing the event data, including the event ID, category, and the event description. The event description indicates that the event was triggered by a user named 'Administrator' and that the event was triggered by a user named 'Administrator'.

FTK Evidence History file can be found here and uploaded separately in Moodle:

Suspicious files Can be found here and also uploaded separately in Moodle:

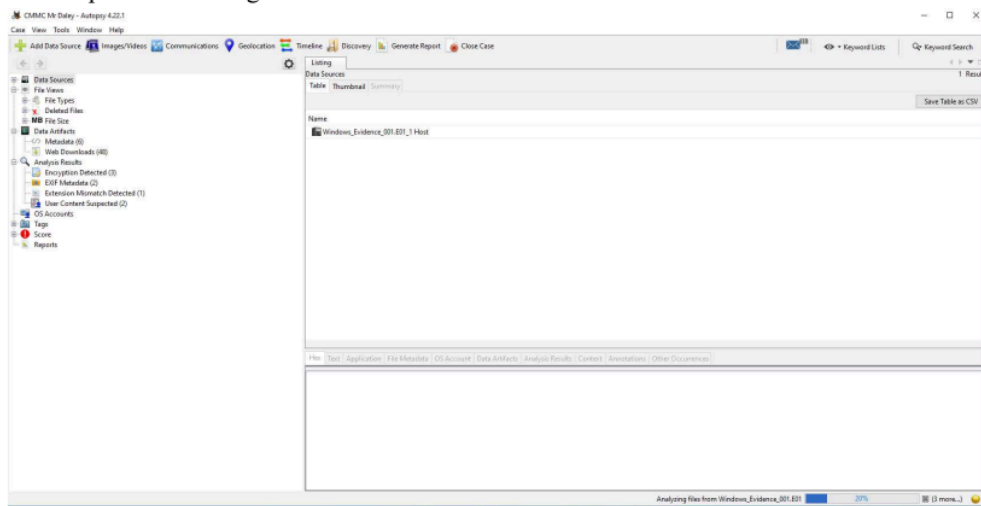


Bad Items can be found here and also uploaded separately in Moodle:

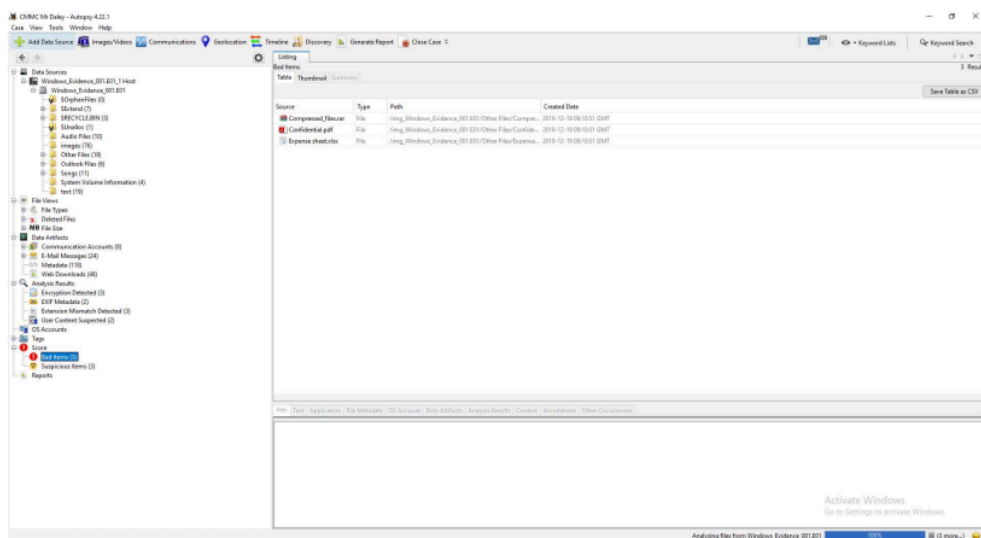
Anti-Forensic Activity 2.2

Autopsy was used to analyse the copied image from the write-blocker for signs of deliberate data destruction and Anti-Forensic Methods. Analysis of system logs, application artefacts and records from the local file system all displayed a consistent correlation of a secure wiping tool/agent being used.

Overwritten sectors, missing file system metadata and inconsistent timestamp patterns were discovered which all indicated intentional secure deletion by Mr Daley on the Autodesk Maya Files. The findings strongly support hypothesis Mr Daley attempted to conceal his actions prior to his resignation at CMMC.



3 - Autopsy evidence upload



4 - Bad Items



Bad Items.csv

Bad Items File can be found here and also uploaded separately in Moodle:

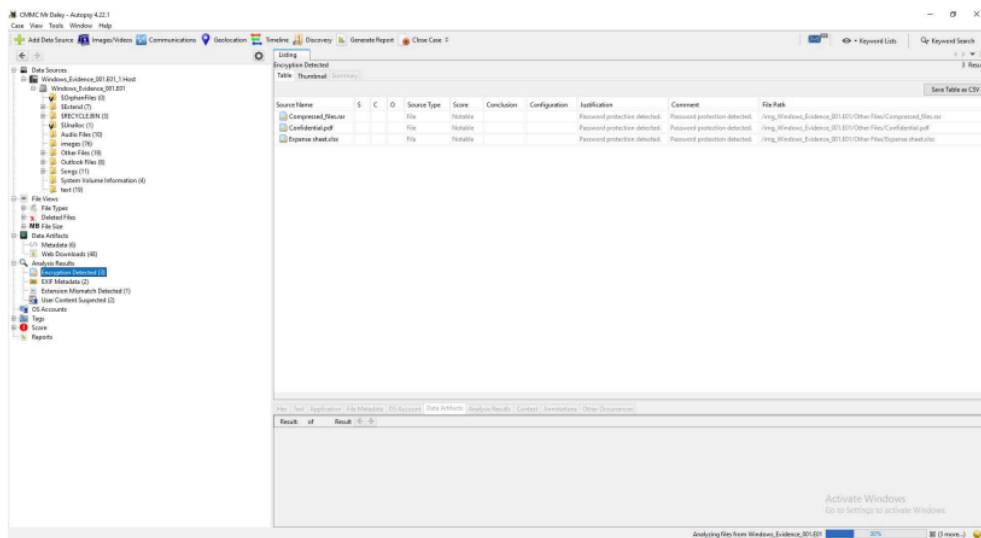
File Carving 2.3

Removal of file metadata meant traditional methods of recovery were ineffective. The use of Autopsy's file carving function was used to scan unallocated space for Autodesk Maya files. RAW analysis identified partial fragments of files relating to Autodesk Maya which included the headers. Full reconstruction of the files was not possible but recovered fragmentations confirm prior presence of deleted files from Autodesk Maya which supports the hypothesis Mr Daley intentionally destroyed the files as part of a Anti-Forensic technique.



All Deleted Items.csv

Deleted Items File can be found here and also uploaded separately in Moodle:



5 - Autopsy Encrypted Files

Cloud Analysis 2.4

Cloud Analysis was deployed to analyse potential stealing of files relating to the designs CMMC planned to Patent. Magnet AXIOM was used to examine artefacts relating to cloud-based data. Analysis conducted included browsing history, cookies, cache content, session data and tokens. The evidence showed access to a Google Drive account and timestamps correlate in the period of which Mr Daley destroyed the files. Authentication tokens confirm files were transferred which supports the argument that Mr Daley uploaded these to a personal drive account. The concerns raised by CMMC and evidence discovered supports the suspicion of intellectual property theft.

Along with Cloud Analysis, with suspicions Mr Daley was involved in contact with CMMC competitors, we also carried out analysis into email items of Mr Daley which showed access to a personal inbox. The investigation into the mailbox was carried out with Data Protection and GDPR guidelines in consideration making sure we had valid reason to investigate the mailbox, outlined above. As this is a live investigation, in guidance from the UK Data Protection and GDPR Law delayed notification is justified due to suspect of wrongdoings, this is documented. Controlled access and minimal access to this information has been carried out. I have attached the email items CSV file below which is attached and stored on Lawful Basis and as this a live investigation stored of such information is justified. Upon conclusion of the aforementioned investigation, all files attached to this report will be disposed of securely and in accordance with UK guidelines.

The Email Items can be seen here logged in a spreadsheet and also uploaded seperatly in



Email Items.csv

Moodle:

3.3 Google Drive Access

Analysis of the browser on Mr Daley's device found multiple visits to a URL relating to Google Cloud Drive access (drive.google.com). The visits to this URL occurred in the same timeframe as the deletion of Autodesk Maya files. Cache data, Cookies and Authentication tokens also indicated the access was to a personal account which was unknown and unrelated to Cyfusion Mobile Manufacturing Company. The use of Magnet AXIOM allowed a reconstruction of the activity carried out by Mr Daley which is consistent with file uploads.

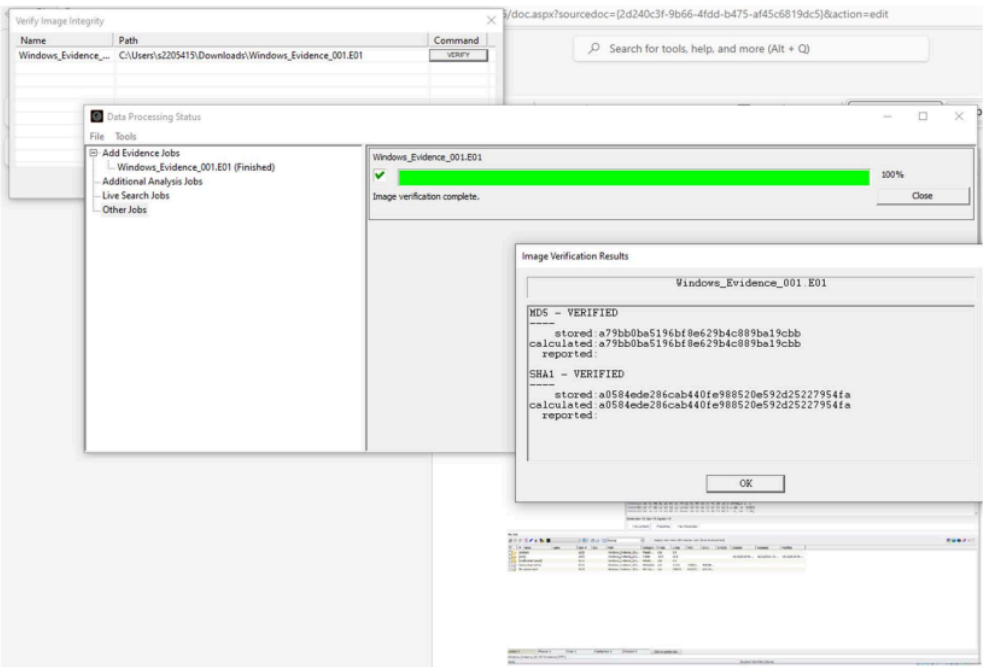
3.4 Considerations and Justifications

During the course of the investigation it's important to consider the possibility that Mr Daley may attempt to justify his actions as protective measures rather than deliberate actions to sabotage CMMC. Mr Daley may consider the actions of deletion of the Autodesk Maya files and protective to the organisation to prevent unauthorised access, leakage of highly sensitive designs particularly given the sensitivity around competition and competitive advantage within the market CMMC operate in. However, presence of secure wiping activities and access to a personal Google Drive account with synchronisation of files contradicts this explanation.

4.0 Investigation Conclusion

The investigation carried out by Troy Simpson Forensics on behalf of CMMC concludes Mr Daley engaged in sabotage, unauthorised copying and data removal prior to resigning at CMMC. The evidence in which was discovered shows he used secure wiping tools to destroy project files. It also revealed cloud synchronisation activity on a personal Google account which supports concerns Mr Daley uploaded these for sale to competitors within the market which includes 360Tech. The actions of Mr Daley represent breach of trust, theft of designs and files and intentional commercial and financial damage to CMMC. All findings outlined in this report are supported by forensic sound acquisition of data and analysis procedures inline with ACPO and CHFI principles. The report is also available for presentation in future Legal Proceedings should CMMC decide to follow legal proceedings.

5.0 Hash Log



7 - FTK Hash Values

File Attributes	
General	False
Verification Hashes	
MD5 verification hash	a79bb0ba5196bf8e629b4c889ba19cbb
SHA1 verification hash	a0584ede286cab440fe988520e592d25227954fa
Drive Geometry	
Bytes per Sector	512
Sector Count	4,194,304
Image	
Image Type	E01
Case number	
Evidence number	
Examiner	

8 - FTK Hash Values 2

The Hash logs generated by FTK are shown in the above screenshots.

The hash logs have been generated from FTK in which sees an investigation into Mr Daley a previous CMMC employee for potential sabotage against CMMC. FTK produced a MD5 and SHA-256 Hash value to verify the acquired data. The hash values are used throughout the investigation to verify the integrity of the evidence and demonstrates that no modifications to the evidence occurred during forensic analysis.

6.0 Appendix: Chain of Custody

Date/Time	Examiner/Person	Action	Evidence	Purpose
06/04/2026 9:15 – 9:30	Ms Ker Walters	Meeting and handing over evidence for investigation	Workstation	Investigation
06/04/2026 09:32	Joshua Longhurst	Evidence triage	Workstation (Win 11) assigned to CMMC user Mr Rich Daley	Investigation into potential wrongdoings whilst in post by Mr Daley
06/04/2026 10:03	Joshua Longhurst	Evidence photographed, logged, labelled	Workstation documented and labelled with CMMC-RD-W11-DEVICE	Documentation start
06/04/2026 10:27	Joshua Longhurst	Device in Live state, volatile data and live state captured	Volatile image taken – CMMC-RD-VOL1	Bitlocker keys captured for decryption in future, browser session activity captured and volatile artefacts
06/04/2026 11:15	Joshua Longhurst	Forensic Imaging conducted	FTK Hash Log	Verifies image for admissibility
06/04/2026 12:01	Joshua Longhurst	Autopsy Case opened	CMMC Mr Daley Case named	Examination of deleted files and further data on the device
06/04/2026 13:30	Joshua Longhurst	Evidence stored securely for next day investigation	Artefacts stored under locked conditions	Next day return
07/04/2026 09:55	Joshua Longhurst	Autopsy Deleted Files Investigated	Deleted Files Spreadsheet	Examination deleted files – file carving used
07/04/2026 13:00	Joshua Longhurst	Autopsy Web Downloads analysed	Downloads checked for suspicious activity	Examined downloads from web for activity relating to sabotage against CMMC
07/04/2026 15:43	Joshua Longhurst	Autopsy + FTK Files Analysed	Analysis into files stored on device	Examined files relating to suspected activity
07/04/2026 17:53	Joshua Longhurst	Evidence stored securely for next day investigation	Artefacts stored under locked conditions	Next day return
08/04/2026 8:45	Joshua Longhurst	Autopsy Email analysis	Examined mailbox	Examination to sent and received emails
08/04/2026 10:37	Joshua Longhurst	Autopsy Bad Items examined	Bad Items artefact list	Review into damaged/corrupted or irregular objects

08/04/2026 13:00	Joshua Longhurst	Autopsy Suspicious Items examined	Suspicious Items artefact list	Review into anomalies in the system
08/04/2026 16:49	Joshua Longhurst	Evidence secured and stored in securely	Forensic Images and Artefacts	Final storage and evidence security

Task 4

Invoice

Note: Due to Layout, design and text size please see my next page for one full page layout of the invoice.

INVOICE

TROY SIMPSON FORENSICS

Accounts@Troysimpsonforensics.com

Bill to:

Ms Ker Walters
Cyfusion Mobile Manufacturing Company
Westminster
SW1 1KW
London
United Kingdom

0800 978 7713

Company Number: 00110236

Vat Number: 22061211

Invoice: INV000123

Issue Date: 25/04/2026

Payment Date Due: 16/05/2026

Balance Due: £2880

Services/Items	Qty/Hrs/Days	Rate	Total
Initial Assessment	1	£250	£250
Data Acquisition	1	£300	£300
Legal Report & Secure Evidence Storage	1	£400	£400
Software usage charge (FTK – Licence cost Paid)	1	£80	£80
Investigator Day Rate	20hrs	£40/hr	£800
Expert Testimony	2 days	£525/Per Day	£1050
Thank you for choosing Troy Simpson Forensics for your Digital Forensic needs			TOTAL £2880

Terms & Conditions

Payment is to be made within 21 days of Invoice Issue Date

Payment is to be made to the Accounts Team at Troy Simpson Forensics

Late Payments are subject to a 2.9% Interest Fee

Payments not made within 12 months are subject to legal action

If Cash or Cheque payment is preferred, please contact us

Payment Details

Barclays PLC

Business Name: Troy Simpson Forensics

Account Number: 12345678

Sort-Code: 81-56-11

(Note: Should the above invoice not show on 1 singular page, I have added a screenshot below for improved context and viewing.)

INVOICE

TROY SIMPSON FORENSICS

Bill to:

Ms Ker Walters

~~Cyfusion~~ Mobile Manufacturing Company

Westminster

SW1 1KW

London

United Kingdom

Accounts@Troysimpsonforensics.com

0800 978 7713

Company Number: 00110236

Vat Number: 22061211

Invoice: INV000123

Issue Date: 25/04/2026

Payment Date Due: 16/05/2026

Balance Due: £2880

Services/Items	Qty/Hrs/Days	Rate	Total
Initial Assessment	1	£250	£250
Data Acquisition	1	£300	£300
Legal Report & Secure Evidence Storage	1	£400	£400
Software usage charge (FTK – Licence cost Paid)	1	£80	£80
Investigator Day Rate	20hrs	£40/hr	£800
Expert Testimony	2 days	£525/Per Day	£1050
Thank you for choosing Troy Simpson Forensics for your Digital Forensic needs			TOTAL
			£2880

Terms & Conditions

Payment is to be made within 21 days of Invoice Issue Date

Payment is to be made to the Accounts Team at Troy Simpson Forensics

Late Payments are subject to a 2.9% Interest Fee

Payments not made within 12 months are subject to legal action

If Cash or Cheque payment is preferred, please contact us

Payment Details

Barclays PLC

Business Name: Troy Simpson Forensics

Account Number: 12345678

Sort-Code: 81-56-11

Other Files Upload Link: <https://moodle.uwtsd.ac.uk/mod/assign/view.php?id=737580>

References

[1 R. Das, "INFOSEC," 06 07 2019. [Online]. Available:

] <https://www.infosecinstitute.com/resources/digital-forensics/comparison-popular->

computer-forensics-tools/#:~:text=a%20several%20formats.-
,Pros:,not%20have%20a%20timeline%20view.. [Accessed 12 04 2026].

[2 A. Agrawal, "Hawk Eye Forensic," 11 10 2025. [Online]. Available:

] <https://hawkeyeforensic.com/comparison-of-popular-digital-forensic-tools-ftk-encase-and-x-ways/>. [Accessed 14 04 2026].

[3 "Geeks for Geeks," 23 07 2025. [Online]. Available:

] <https://www.geeksforgeeks.org/ethical-hacking/how-to-create-a-forensic-image-with-ftk-imager/>. [Accessed 12 04 2026].

[4 Exterro, "Digital Forensics Exterro FTK Imager," [Online]. Available:

] <https://www.exterro.com/digital-forensics-software/ftk-imager>. [Accessed 10 04 2026].

[5 "Forensic Focus," 18 03 2022. [Online]. Available:

] <https://www.forensicfocus.com/forums/general/cost-of-magnetic-axiom-licence/>. [Accessed 10 04 2026].

[6 "Magnet Forensics," 06 08 2020. [Online]. Available:

] <https://www.magnetforensics.com/blog/all-your-case-data-in-magnet-axiom-pt-3-bringing-in-computer-data/#:~:text=Magnet%20AXIOM%20supports%20a%20wide%20variety%20of,devices%20like%20USB%20and%20SD%20Flash%20drives>. [Accessed 10 4 2026].

[7 "Magnet Forensics," [Online]. Available:

] https://www.magnetforensics.com/resources/introduction-magnet-axiom/#:~:text=Magnet%20Axiom%20is%20a%20digital%20investigation%20platform,report%20views**%20Share%20findings%20quickly%20and%20easily. [Accessed 10 04 2026].

[8 "Cyber Triage," 27 02 2026. [Online]. Available:

] <https://www.cybertriage.com/blog/computer-forensic-tools-comparison-2026/#:~:text=Magnet%20AXIOM%20Cyber,develop%20their%20own%20YARA%20rules..> [Accessed 10 04 2026].

[9 "EForensics," 03 10 2023. [Online]. Available: [https://eforensicsmag.com/autopsy-](https://eforensicsmag.com/autopsy-the-digital-forensics-toolkit/)

] [the-digital-forensics-toolkit/](https://eforensicsmag.com/autopsy-the-digital-forensics-toolkit/). [Accessed 10 04 2026].

[1 "Vendr," [Online]. Available: <https://www.vendr.com/marketplace/cellebrite>.

0] [Accessed 12 04 2026].

- [1 "Cellebrite," Cellebrite, [Online]. Available: <https://cellebrite.com/en/pa-cloud/>.
1] [Accessed 12 04 2026].
- [1 SC Staff, "SC Media," 01 05 2012. [Online]. Available:
2] <https://www.scworld.com/product-test/cellebrite-ufed-ultimate>. [Accessed 12 04 2026].
- [1 "Forensic Sciences," XOURNALS, 2023. [Online]. Available:
3] <https://www.xournals.com/journal/analysis-of-ftk-imager-as-a-recovery-tool-for-different-storage-devices#:~:text=FTK%20Imager%20is%20a%20powerful%20and%20widely,digital%20evidence%20from%20a%20variety%20of%20sources..> [Accessed 21 04 2026].
- [1 M. Siamukulule, "A Deep Dive into Magnet AXIOM's Workflow: Exploring the Roles of
4] AXIOM Process and AXIOM Examine in Digital Evidence Acquisition and Analysis," *International Journal for Multidisciplinary Research*, no. 1, p. 10.
- [1 A. Kajuna, "Exploring Autopsy," Medium, 02 02 2026. [Online]. Available:
5] <https://medium.com/@asfathkajuna/exploring-autopsy-a-free-open-source-digital-forensics-tool-e8137bd954f0>. [Accessed 2026 04 20].
- [1 "Cellebrite UFED Version 1.1.7.6 Evaluation Report," National Institute of Justice, 07
6] 2012. [Online]. Available: <https://nij.ojp.gov/library/publications/cellebrite-ufed-version-1176-evaluation-report>. [Accessed 2026 04 21].
- [1 "Capabilities of cellebrite universal forensics extraction device in mobile device
7] forensics," *Capabilities of cellebrite universal forensics extraction device in mobile device forensics*, p. 1, 2024.
- [1 "Chain of Custody," UpGrad KnowledgeHut, 16 10 2022. [Online]. Available:
8] <https://www.knowledgehut.com/blog/security/chain-of-custody-in-cyber-security>. [Accessed 14 04 2026].

Table of Figures

1 - FTK Evidence upload.....	7
2 - Evidence File Hex	7
3 - Autopsy evidence upload.....	8
4 - Bad Items.....	9
5 - Autopsy Encrypted Files.....	10
6 - Autopsy Web Downloads	11

7 - FTK Hash Values.....13

8 - FTK Hash Values 2.....13

Josh Longhurst 2205415 Assignment

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

78/100

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)

JOSH LONGHURST

78

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 good engagement with forensic literature, practitioner guidance, and technical documentation. Relevant references are used throughout the discussion of forensic acquisition, anti-forensic techniques, file carving, and cloud analysis. The work demonstrates awareness of contemporary forensic tools and investigative standards.

Some references rely more heavily on vendor or practitioner documentation rather than peer-reviewed academic research. Greater integration

15

and synthesis between sources would strengthen the academic depth further.
Referencing could be improved in some sections.

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, BitLocker encryption, anti-forensic behaviour, file carving, and browser/cloud artefact analysis. The explanation of CHFI methodology and ACPO principles is accurate and appropriately applied throughout the case study. The report demonstrates good awareness of forensic procedures and evidential handling requirements. Some conceptual explanations could be expanded further in technical depth.

7

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 strong investigative sequencing throughout the case study. The discussion appropriately evaluates anti-forensic behaviour,

30

encryption handling, cloud synchronisation evidence, and file carving limitations.

There is clear evidence of evaluative thinking in the discussion of forensic workflows and evidential interpretation. The report also demonstrates good awareness of alternative explanations and legal considerations. However, some sections remain descriptive in nature and would benefit from deeper critical evaluation of evidential reliability and forensic limitations.

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 excellent practical application through the inclusion of forensic workflows, hash logs, chain of custody documentation, investigative timelines, screenshot references, and forensic reporting structures. The work demonstrates strong linkage between forensic theory and investigative practice.

The investigation report is professionally organised and reflects strong awareness of real-world forensic investigation procedures. The inclusion of detailed investigative stages and evidential handling documentation significantly strengthens the professional realism of the report. Marks awarded based on

19

Screenshots of wiping tool in FTK's software analysis or any other tool used,
A simulated hash log for the evidence image in your appendix or as an additional upload
Provide a sample invoice

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 organisation and generally effective academic communication throughout. Technical terminology is appropriately used, and the investigation report structure aligns well with professional forensic reporting standards. Some grammatical inconsistencies, formatting issues, and presentation irregularities remain throughout the report. IEEE reporting format not used in task 1.

7