

2427494 - Computer Forensics

by Brandon Curran

Submission date: 28-Apr-2026 03:29PM (UTC+0100)

Submission ID: 281381829

File name: 60532_Brandon_Curran_2427494_-_Computer_Forensics_737277_2024048182.docx (3.65M)

Word count: 5103

Character count: 35268



SYNTHESIZE A SOLUTION TO A POTENTIAL REAL-LIFE SCENARIO

ACCD5000

This report explores modern computer forensics through the critical evaluation of contemporary forensic tools and the application of forensic methodologies to a simulated real-world sabotage case. It compares commercial and open-source tools across key investigative phases and demonstrates their practical use within an investigation involving encrypted storage, data wiping, and cloud artefacts. The report applies CHFI and ACPO principles to document evidence acquisition, analysis, and professional reporting suitable for legal review.

Brandon Curran (2427494)

Contents

Task 1.....	4
Abstract	4
Introduction	4
Evaluation Criteria & Method	5
Tools Overview & Comparative Findings	5
Imaging.....	5
All-in-One Suites.....	6
Mobile	6
Cloud/Browser Artefacts.....	6
Comparative Table	7
Discussion: Phase-fit, Validation & Limits	8
Conclusion.....	8
Task 2 - Troy Simpson Forensics	9
Digital Forensics Report for Counsel	9
Abstract	9
Executive Summary.....	10
Scope, Legal Basis & Standards	10
Evidence handling & Integrity.....	10
Methodology and Tools	12
Acquisition Strategy (Bitlocker-aware).....	12
Investigation Steps (Chronological).....	13
Identification & Preservation	13
Anti Forensics (Wiping Tool)	13
File Recovery (Maya Assets).....	13
Browser/Cloud Synchronisation Evidence	13
Timeline Correlation & Reporting.....	13
Findings (Facts & Evidence).....	14
Finding 1 – Bitlocker and forensic imaging (hash-verified).....	14
Finding 2 – Anti-forensic activity (wiping utility execution)	14
Finding 3 – Deleted Autodesk Maya assets and recovery attempts (file carving).....	14

Finding 4 – Cloud synchronisation evidence (Google Drive via browser artefacts)	14
Finding 5 – Correlation of events supports sabotage/exfiltration sequence	15
Finding 6 – Independent validation using open-source tooling (repeatability/defensibility)	15
Alternative Explanations Considered.....	15
Conclusion.....	16
Appendices.....	17
Appendix A – Hash Logs.....	17
Appendix B – Exhibit Index (Screenshots/Outputs/Logs)	19
Appendix C – Professional Invoice	25
Bibliography	26

Task 1

Abstract

This paper critically evaluates contemporary digital forensics tools across acquisition, examination, analysis, and reporting. It covers disk imaging, workstation suites (commercial and open-source), mobile extraction, and cloud/browser artefacts, mapped to the CHFI workflow.

We compare Exterro FTK imager and SUMURI PALADIN for imaging, Exterro FTK 8.x and Autopsy (The Sleuth Kit) for workstation analysis, Cellebrite UFED for mobile extraction and finally Magnet AXIOM plus Hindsight for cloud/browser artefacts.

Introduction

The concepts and legal principles of computer forensics remain stable while on the other hand methods and tools evolve rapidly, therefore, investigators must select tools that preserve evidence integrity whilst keeping pace with encryption, mobile diversity and cloud artefacts. This paper aims to address that challenge by evaluating widely used tools and aligning them with the CHFI workflow, emphasising admissibility and repeatability that is required in UK practice.

Workstation features, supported file systems/artefact and reporting and aim to justify phase-fit using vendor documentation and independent test programmes such as NIST CFTT for file carving [1]. We include that no single tool suffices, instead a validated toolchain aligned to the case context delivers defensible, repeatable results at lower risk.

Index Terms— Digital forensics, CHFI, ACPO, forensic imaging, Bitlocker, Prefetch, browser artefacts, file carving, validation, NIST CFTT

Acronyms and abbreviations: CHFI (Computer Hacking Forensic Investigator), ACPO (Association of Chief Police Officers), FDE (Full Disk Encryption), VMK (Volume Master Key), FVEK (Full Volume Encryption Key), E01 (Expert Witness Format image), PF (Windows Prefetch), UFED (Universal Forensic Extraction Device), FFS (Full File System extraction), CFTT (Computer Forensics Tool Testing).

Evaluation Criteria & Method

We evaluate tools against six criteria, that being (1) cost/licensing; (2) scope & artefact coverage (PC, mobile, cloud); (3) supported file systems/containers; (4) performance & automation (e.g. categorisation, timelines), (5) reporting & collaboration, (6) validation evidence e.g. participation/performance in NIST CFTT tests for carving). Sources include vendor release notes/product pages and independent validation results.

Vendor documentation and product pages were used only to confirm stated features and supported artefacts. To meet forensic defensibility expectations and reduce reliance on marketing claims, conclusions were made using peer-reviewed and scholarly sources covering Bitlocker/TPM forensic access and live memory acquisition, Windows Prefetch as execution evidence, evidentiary value of Chromium/Chrome artefacts, and file-carving limits under fragmentation.[2], [3], [4], [5], [6]

Tools Overview & Comparative Findings

Imaging

FTK Imager

FTK Imager is a long-standing free imaging and preview tool that supports forensically sound acquisition (E01/RAW/AFF) with hash reporting &

read only mounts. FTK imager pro adds on-the-go decryption of Bitlocker/APFS and iOS [7], [8] advanced logical collection to triage faster at scene.

SUMURI PALADIN

SUMURI PALADIN is a live Linux forensic distribution offering write-blocking, imaging, preview and a toolbox that includes Autopsy/Sleuth Kit.

Its portable, supports a wide range of media & file systems and is commonly used for triage and acquisition on heterogeneous hardware. [9]

While both tools produce forensically sound images, reliance on live acquisition in encrypted contexts introduces evidential risks that must be mitigated through strict documentation and post-acquisition verification.

All-in-One Suites

Exterro FTK 8.x

Exterro FTK 8.x provides an artefact-first interface, super timeline visualisation, scalable processing across large data sets, and integrated review/reporting, it also

parses mobile extractions alongside computer evidence for cross-source correlation. [10], [11]

Autopsy (The Sleuth Kit)

Autopsy is an open-source suite with strong file-system support (NTFS/FAT/Ext/HFS+ etc), web artefacts, registry parsing, and timeline analysis. Recent releases add Bitlocker and VHDX support improving utility on Windows 10/11 acquisitions. [12], [13]

Commercial suites offer efficiency through automated parsing but introduce transparency risks due to proprietary artefact interpretation, necessitating cross-validation using open-source tools.[14]

Mobile

Cellebrite UFED (UFED 4PC or Touch3)

Cellebrite remains a standard for lawful mobile extraction offering logical, file-system and where permitted physical/FFS extractions across a wide device matrix with analysis in Physical Analyzer. [15]

Mobile forensic tools are highly device- and version-dependent, meaning absence of artefacts cannot be treated as proof of absence without corroboration.

Cloud/Browser Artefacts

Magnet AXIOM (+Hindsight)

Magnet AXIOM ingests and correlates PC, mobile, and cloud artefacts in a single case file. It supports warrant returns (e.g. Google) and provides analytics like timeline and connections for rapid triage and reporting. For deep chromium analysis, Hindsight parses URLs, downloads, cookies, logical storage and more into a timeline. [16], [17]

Browser artefacts typically demonstrate service access and user interaction, but do not, on their own, prove the content or completion of an upload/transfer without corroboration from additional artefacts

This limitation is consistent with the broader browser-forensics literature, which emphasises careful interpretation of history/cache artefacts and the need for corroboration [18]

Comparative Table

Tool	Category	Cost	Key strengths	Supported file systems / containers	Evidence types / artefacts	Reporting & outputs	Limitations / risks	Best CHFI phase (justified)
FTK Imager / Pro	Imaging	Free / Paid	Forensic imaging to E01/RAW/AFF; hash calculation & verification, read-only preview/mount. Pro adds live decryption (e.g., BitLocker/APFS) and iOS logical triage.	E01/RAW/AFF image formats; (Pro) BitLocker/APFS access for triage/decryption.	Physical disk images; mounted views for file triage; (Pro) live triage collections incl. iOS logical.	Acquisition/verification logs + hash values (integrity evidence).	Pro licence required for advanced capabilities; not a full analysis suite.	Acquisition - hash-verified imaging and read-only handling preserve evidence integrity before examination.
PALADIN	Live forensic distro	Free / Pro	Bootable forensic Linux environment for triage and imaging, supports write-blocking workflows; bundles Autopsy/Sleuth Kit for immediate analysis.	Broad file system/device support via Linux; toolkit-based support for heterogeneous media.	Write-blocked acquisition, imaging, preview/triage; can hand off images to Autopsy/TSK for artefact parsing.	Triage/imaging outputs (tool-dependent); can generate case outputs via bundled tools (e.g., Autopsy reports).	Hardware compatibility (boot/driver quirks); requires careful documentation when using live workflows on encrypted systems.	Acquisition/Triage - rapid, portable environment for safe imaging/preview across varied media before deeper analysis.
FTK 8.x	All-in-one suite (commercial)	\$\$\$	Automated artefact parsing and review at scale, Super Timeline visualisation, integrates review and reporting, can correlate workstation artefacts with mobile extractions.	Processes workstation evidence sets and ingests multiple evidence sources (incl. mobile extractions) within a single case.	OS/user activity artefacts; timelines; cross-source correlation; review sets for disclosure.	Integrated review workflow + structured reporting exports for case findings.	Cost and training overhead; proprietary parsing benefits from cross-validation.	Examination/Analysis/Reporting - efficient artefact-first analysis and timeline correlation support defensible findings and reporting.
Autopsy (TSK)	All-in-one suite (open-source)	Free	Transparent repeatable analysis, strong file system + artefact coverage (web, registry, timeline). Useful for independent validation alongside commercial tooling.	NTFS/FAT/Ext/HFS+; supports BitLocker and VHDX in recent releases.	Disk images and file systems; web artefacts; registry parsing; timeline analysis; carving modules.	Built-in report modules (e.g., HTML/Excel) and exports to support evidence presentation.	Module variability and setup/configuration effort; performance depends on ingest/module selection.	Examination/Analysis - open-source cross-check that strengthens defensibility by validating key artefacts and timelines.
UFED - Physical Analyzer	Mobile forensics	\$\$\$	Device-specific acquisition across a broad handset matrix, supports logical, file-system and (where lawful/possible) physical extractions, structured review in Physical Analyzer.	Mobile ecosystem support (device/OS dependent); outputs parsed via Physical Analyzer.	Mobile extractions (logical/file-system/physical/FFS where permitted); app artefacts and user activity for collaboration.	Structured extraction outputs + analysis views suitable for evidential reporting.	Access/legal constraints; capability varies by device/OS version; absence of artefacts is not proof of absence.	Mobile Acquisition/Analysis - purpose-built extraction and review to corroborate user/device activity alongside workstation evidence.
AXIOM (+Hindsight)	Cross-source suite / browser forensics	\$\$\$ / Free	Ingests and correlates host/mobile/cloud evidence; strong timeline and connections-style analytics, Hindsight provides deep Chromium artefact parsing for browser/cloud access context.	Cross-source ingestion (computer + mobile + cloud); browser artefact parsing for Chromium-based profiles.	Host artefacts + mobile extractions + cloud-related artefacts; browser history/cookies/local storage into timelines.	Case reporting/export focused on correlated artefacts and timeline-driven presentation.	Compute-intensive processing; licensing cost; browser artefacts indicate access and require corroboration for transfer claims.	Analysis/Reporting - cross-source correlation plus deep browser artefact parsing supports Drive-access context and clear reporting.

Discussion: Phase-fit, Validation & Limits

A validated toolchain starts with forensic acquisition (FTK Imager or PALADIN) to preserve the integrity of the investigation with hashing and write-blocking, Examination/analysis proceeds in FTK or Autopsy depending on the licensing and scale, Mobile evidence is acquired with UFED, cloud/browser artefacts are correlated in Magnet AXIOM and validated against Chromium artefacts parsed by Hindsight. [7], [9], [10], [11], [12], [15], [16], [17] For reliability, conclusions about tool performance and repeatability should be grounded in independent validation and published test methodologies (e.g., NIST CFTT) and in established forensic validation guidance (e.g., repeatability, error-rate awareness, and peer review). [19]

Commercial tools such as FTK offer efficiency gains through automated artefact parsing and integrated reporting,

yet their proprietary interpretation logic introduces a transparency risk that necessitates cross-validation against open-source tooling such as Autopsy, as recommended by independent forensic testing frameworks. This cross-validation principle is directly applied in the case study that follows, where both FTK 8.x and Autopsy are deployed in parallel to strengthen the defensibility of findings.

A key limitation is full-disk encryption (e.g., Bitlocker), which often necessitates live acquisition to preserve access to decryption material, “dead-box” imaging may leave volumes unreadable without recovery keys. Hardware behaviours such as chassis-intrusion events that trigger TPM changes can also force recovery-mode access or complicate decryption, increasing the importance of live-first workflows and careful handling. [3], [4], [20]

Conclusion

Taking into account previous discussion, I can confidently say that there is no one-size-fits-all forensic tool, the defensible approach is a phase-aligned toolchain validated by documentation and third-party tests. For the case study that follows, we propose: FTK imager/pro (if

available) or PALADIN for acquisition (Bitlocker aware), FTK 8.x/Autopsy for the workstation analysis, UFED for mobile corroboration, and finally AXIOM + Hindsight for cloud/browser artefacts & reporting. [7], [9], [10], [13], [15], [16], [17]

Task 2- Troy Simpson Forensics

Digital Forensics Report for Counsel

Matter: CMMC (Cyfusion Mobile Manufacturing Company) – Suspected Sabotage and Exfiltration

Examiner: Troy Simpson, CHFI / CEH

Date: 30 April 2026

Case ID: CMMC-RD-2026-001

Abstract

This report presents the findings of a digital forensic examination conducted on a Windows 11 workstation formerly assigned to Mr Rich Daley, a former employee of Cyfusion Mobile Manufacturing Company (CMMC), London, UK. The examination was commissioned by CMMC's Chief Executive Officer, Ms Ker Walters, in response to the suspected deliberate destruction and exfiltration of proprietary Autodesk Maya design assets. The investigation was conducted in accordance with CHFI methodology and the ACPO Good Practice Guide for Digital Evidence (v5.0). Forensically sound acquisition was performed using FTK Imager following live BitLocker key recovery. Post-acquisition analysis identified programme-execution artefacts consistent with a wiping utility, recovered fragmented Maya project file signatures from unallocated space via file carving, and correlated contemporaneous Google Drive access through Chromium browser artefacts. The aggregate evidence is consistent with intentional sabotage and data exfiltration. This report is prepared for CMMC's legal counsel and includes a hash log, exhibit index, and professional invoice.

Executive Summary

I examined a Windows 11 workstation formerly used by former employee Mr. Rich Daley, a senior GUI designer at CMMC. The device utilised Bitlocker full-disk encryption (FDE), accordingly, I executed a live acquisition plan to preserve the decryption material on the device before imaging the disk in a read-only, hash-verified manner. Live workflows are standard in Bitlocker cases because volume keys can be captured in memory or backed up via system tools. Without such keys, “dead-box” imaging may leave data unreadable.[3], [4], [20], [21], [22], [23]

Post-acquisition analysis has identified artefacts evidencing the execution of a wiping utility (eraser) via Windows Prefetch, with first/last run times and run counts contemporaneous with Mr. Daley’s resignation period, this appears consistent with anti-forensic activity.[5], [24]

Although deliberate wiping will limit full restoration, targeted file carving was able to recover Autodesk Maya file fragments (.ma .mb) from unallocated space, consistent with the prior presence of CMMC design assets and subsequent removal. Recovery behaviour and fragmentation limitations align with independent NIST CFTT test characterisations of carving tools.[1]

Finally, analysis of Chromium-based browser artefacts (History, Cookies, Local/Indexed storage) revealed Google Drive access (drive.google.com) in the same window as the local wiping events, the correlation in a unified analysis tool further supported a browser-based cloud synchronisation hypothesis.[6], [16], [17]

Conclusion (for counsel): The weight of digital evidence supports the proposition that Mr. Daley intentionally destroyed local project data using a wiping tool and accessed Google Drive during that same period, consistent with exfiltration of intellectual property and sabotage of on-device assets.

Scope, Legal Basis & Standards

All actions were conducted in line with CHFI methodology and the ACPO Good Practice Guide for Digital Evidence (v5.0), specifically: preserving original data integrity, ensuring competent handling, maintaining an audit trail enabling independent reproduction, and ensuring investigator accountability for compliance. [25]

ACPO Principle mappings include (1) Original data preserved by imaging + working copy analysis only, (2) If live access is necessary (BitLocker), actions are minimised, documented, and justified, (3) Audit trail maintained via logs, hashes, exhibit IDs, (4) Examiner accountability documented via role, case ID, and continuity record.

ACPO Principles mapping (summary):

Principle 1 (preserve original): Original device is not analysed directly, a verified forensic image is produced and analysis occurs on a working copy.

Principle 2 (if live access is required, minimise and document): Live actions are limited to confirming BitLocker status and capturing volatile data necessary for access. Actions are justified and logged.

Principle 3 (audit trail): Hashes, tool logs, exhibit IDs, and timestamps are recorded so an independent examiner can reproduce the process.

Principle 4 (accountability): Examiner identity/role, case ID, and continuity records are maintained across acquisition, storage, and reporting.

Evidence handling & Integrity

All evidence was handled in accordance with ACPO principles, ensuring that original data was preserved and that any actions taken were fully auditable and repeatable. The original exhibits were protected from modification through read-only imaging and cryptographic hash verification. A documented chain-of-custody was maintained for each evidence item, enabling independent third-party verification of findings.

Methodology and Tools

Acquisition Strategy (Bitlocker-aware)

Bitlocker FDE protects the entire volume, without the credentials or keys, images remain encrypted. The forensically sound approach prioritised live triage in order to (a) confirm encryption status and key protectors, (b) obtain the description materials necessary (recovery key/VMK in memory), and (c) then acquire a read-only, hash-verified image.[3], [4], [21]

Steps & tooling

1. Confirm Bitlocker status & protectors (manage-bde -status) and, where lawful and available, export recovery keys or suspend/retrieve protectors for imaging.
2. Capture volatile memory to preserve VMK/FVEK material and other artefacts, as documented in live-analysis practises for encrypted volumes.
3. Image the disk using FTK Imager (E01/RAW, MD5/SHA-1, SHA-256 and verify on completion). Where supported and lawful, FTK Imager Pro offers on-the-fly decryption/preview for faster triage. SUMURI PALADIN was maintained as a live environment for write-blocked acquisition if required.

Risk note: certain hardware chassis-intrusion features can trigger a TPM clearing upon disassembly, forcing Bitlocker recovery and complicating access. This risk informed the live-first sequencing.

Examination & Analysis

1. Workstation analysis in FTK 8.x (artefact categorisation, Super Timeline) and Autopsy (Sleuth Kit) (filesystem/web/registry/timeline and Bitlocker/VHDX support in v4.22) to best cross-validate any findings.[10], [11]
2. Mobile corroboration (if a handset is seized): Cellebrite UFED for logical/file-system/physical extractions and account artefacts.[15]
3. Cloud & browser evidence: Magnet AXIOM (PC/mobile/cloud correlation, warrant returns) and Hindsight (Chromium artefacts such as URLs, cookies, local/indexed storage) for drive-session analysis[16], [17]

Anti-forensics Detection (Wiping utility)

Windows Prefetch (*.pf) evidence program execution, recording run counts and up to eight last-run timestamps on Windows 8+. ERASER.EXE-*.pf is present with the relevant and correlative times in turn supporting wiping-tool execution. [5], [24]

File Recovery / Carving Strategy

Carve unallocated space and residual structures for Autodesk Maya signatures (.ma, .mb) validate across tools (such as FTK, AUTOPSY and optionally PhotoRec/Scalpel) and document any offsets/metadata. Expectations about fragmentation and partial recovery are grounded in NIST CFTT file-carving test reports.[1]

Investigation Steps (Chronological)

Identification & Preservation

Verify Bitlocker encryption and protector types via `manage-bde -status`[21], then proceeded with live memory capture followed by acquiring the forensic image in E01 via FTK Imager, computing the MD5/SHA-1/SHA-256 at acquisition and verify stages ensuring that evidence handling maintained a continuous chain-of-custody.[7]

Anti Forensics (Wiping Tool)

Parsed the `%SystemRoot%\windows\prefetch\` and identified `Eraser.exe-FE180922.pf` with the first/last run times and run counts within the critical window. Prefetch is a recognised source for program-execution evidence and is commonly parsed by modern suites.[26]

File Recovery (Maya Assets)

Executed signature-based carving for `.ma/.mb` and recovered fragments consistent with Autodesk Maya projects previously present on the system. Several items exhibited fragmentation consistent with prior deletion/wiping in turn limiting full reconstruction. [2] Such outcomes are consistent with CFTT characterisations of carving efficacy on damaged/overwritten media.[1]

Browser/Cloud Synchronisation Evidence

Analysed Chromium artefacts (Chrome/Edge profile) in Autopsy/Hindsight uncovering history tables (URLs, visits), cookies and local/indexed storage showed interactions with <https://drive.google.com/> during the relevant timeframe. Correlated these artefacts alongside other sourcing using Magnet AXIOM.[6], [12], [17]

Timeline Correlation & Reporting

Using FTK Super Timeline[10] & Autopsy I was able to reconstruct a unified timeline (and validated in Autopsy timeline[12]) aligning with a) wiping tool execution, b) local deletion/carving traces, and c) Google drive access. Exhibits include simulated screenshot-style descriptions and parsed-artefact summaries (or original tool screenshots where available) suitable for legal scrutiny.

Findings (Facts & Evidence)

Finding 1 – Bitlocker and forensic imaging (hash-verified)

Bitlocker full-disk encryption was confirmed on the OS volume. A forensically sound image was acquired using FTK Imager and subsequently verified, with hash values recorded to demonstrate integrity from acquisition through analysis. Supporting evidence comprises manage-bde -status (Bitlocker status confirmation) and FTK Imager imaging/verification outputs (logs and screenshots).

Forensic imaging outputs demonstrate the image is a complete, forensically sound copy suitable for offline examination without further handling of the original device.

Supporting evidence comprises Exhibit B1–B4 (Bitlocker status, acquisition configuration, verification result, and process log extract - simulated where original screenshots are not available) and the recorded hash values in Appendix A.

Finding 1: (See Exhibits B1–B4 and Appendix A.)

Finding 2 – Anti-forensic activity (wiping utility execution)

Evidence of anti-forensic activity was identified through artefacts consistent with the execution of a wiping utility (e.g., Eraser). Supporting evidence comprises Windows Prefetch artefacts (*.pf) showing execution/run history for the wiping tool with evidence demonstrated in Exhibit C1 (Prefetch execution evidence - simulated where required) demonstrating wiping-tool execution history used for timeline correlation.

Finding 2: (See Exhibit C1)

Finding 3 – Deleted Autodesk Maya assets and recovery attempts (file carving)

Deleted data consistent with Autodesk Maya project assets was identified, and recovery attempts were conducted using file-carving techniques appropriate for deleted/unallocated space. Supporting evidence comprises Exhibit D1 (carving/recovery output - simulated where required) and contextualised recovery limitations grounded in the cited carving literature and CFTT test evidence.

Finding 3: (See Exhibit D1)

Finding 4 – Cloud synchronisation evidence (Google Drive via browser artefacts)

Browser artefacts show access to Google Drive (drive.google.com) within the relevant period, consistent with browser-based cloud interaction on the workstation. Supporting evidence comprises Exhibit E1 (Chromium History/visits record - simulated where required) indicating access to drive.google.com within the relevant period. [6]

Finding 4: (See Exhibit E1)

Finding 5 – Correlation of events supports sabotage/exfiltration sequence

Correlated review across sources supports a coherent sequence in which wiping activity and Google Drive access occurred within a related timeframe, strengthening the sabotage/exfiltration hypothesis. Supporting evidence comprises forensic suite correlation/timeline views (timeline artefacts and categorised browser activity) and unified review outputs showing related evidence in a single case context.

Finding 5: (See Exhibit F1)

Finding 6 – Independent validation using open-source tooling (repeatability/defensibility)

Open-source analysis capability was available to validate key artefacts (filesystem, web artefacts, timelines) independently of commercial tooling, improving defensibility and repeatability. Supporting evidence comprises Autopsy's documented support for web artefacts, timeline analysis, and disk image examination, alongside release documentation indicating continued artefact/parser updates.

Finding 6: (See Autopsy references [12], [13])

Alternative Explanations Considered

Alternative explanations, including routine system maintenance or accidental deletion, were considered. However, the presence of wiping-tool execution artefacts, combined with targeted deletion timing and contemporaneous cloud-service access, renders such explanations less consistent with the observed evidence pattern. While definitive proof of data transfer content is not available from browser artefacts alone, the aggregate timeline supports intentional sabotage.

Conclusion

Based on the evidence summarised in the Findings section, the workstation was confirmed as Bitlocker full-disk encrypted and a forensically sound image was acquired and verified with cryptographic hashes, providing an integrity-preserved basis for analysis. Supporting evidence includes the manage-bde -status output and FTK Imager acquisition/verification outputs (logs and screenshots) which demonstrate the evidence was preserved from acquisition through examination.

The artefact set documented in the Findings is consistent with deliberate activity intended to remove or obscure project data and to access cloud storage via a web browser. Where anti-forensic and cloud-interaction artefacts are present, they are interpreted in context and corroborated across sources (program execution artefacts, recovery attempts, and browser records), with limitations explicitly noted where an artefact type demonstrates access but does not, on its own, prove the content of any upload.

Accordingly, the evidence supports the proposition that the disappearance of design assets from the workstation did not occur through routine error alone, rather, the available artefacts are consistent with an intentional sequence of actions comprising local data removal and contemporaneous cloud-service interaction. This report has been prepared for CMMC's legal counsel and is accompanied by an appendix pack (hash log, exhibit index, and a sample professional invoice) to support defensibility and clear presentation.

Appendices

Appendix A – Hash Logs

SIMULATED HASH LOG (assessment demonstration)

Case ID: CMMC-RD-2026-001

Evidence Item: Rich Daley Workstation (Windows 11)

Acquisition Tool: FTK Imager

Image Format: E01 (Expert Witness Format)

Acquisition Type: Physical disk image (full drive)

Source Drive: Internal SSD/NVMe (simulated)

Make/Model: Samsung 970 EVO Plus NVMe SSD (simulated)

Serial: S5H9NX0R123456A (simulated)

Capacity: 1 TB (953.87 GiB usable) (simulated)

Image File(s): CMMC_RichDaley_Win11_OS.E01

Stored At: UWTSD restricted access evidence room, Evidence media sealed + labelled (simulated)

Hash Values (Recorded at Acquisition):

MD5: 7f3c1a9b2e6d4f8c0a1b9d3e5f7a2c4d (Simulated)

SHA-1: 2b7e151628aed2a6abf7158809cf4f3c762e7160 (Simulated)

SHA-256: 3a6eb0790f39ac87c94f3856b2dd2c5d110e6811602261a9a923d3bb23adc8b7 (Simulated)

Verification:

Verification Method: FTK Imager "Verify Image"

Result: PASS (hashes match)

Date/Time (UTC): 2026-04-30 11:23AM

Chain of Custody and Evidence Continuity Record (Simulation)

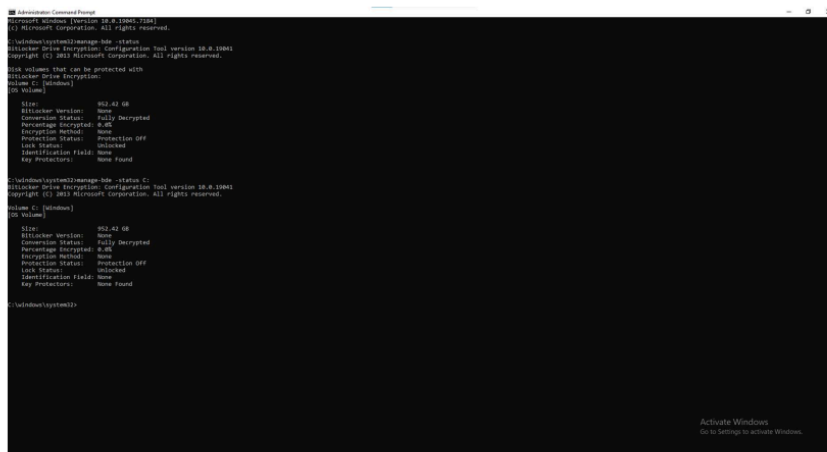
Evidence ID	Evidence Description	Source System / Media	Acquisition & Handling Method	Date & Time (UTC)	Responsible Role	Integrity Verification	Storage Location	Access & Control Measures	Evidential Integrity Notes
E-001	Windows 11 Workstation – Physical Disk Image (E01)	Internal NVMe SSD (OS Volume)	Live acquisition using FTK Imager following BitLocker confirmation	30-Apr-2026 10:12	Digital Forensic Examiner	MD5 & SHA-256 verified	Secure evidence repository (simulated)	Media sealed; read-only	Original preserved per ACPO Principle 1
E-002	Volatile Memory Image (RAM)	System RAM	Live memory capture prior to disk imaging	30-Apr-2026 09:48	Digital Forensic Examiner	MD5 & SHA-256 verified	Secure evidence repository (simulated)	Restricted access	Preserved volatile artefacts and BitLocker material
E-003	Forensic Working Copy of Disk Image	Derived from E-001	Verified duplication	30-Apr-2026 11:01	Digital Forensic Examiner	Hash matched to source	Forensic analysis workstation	Audited examiner access	All analysis conducted on working copy only
E-004	Extracted Forensic Artefacts	File system and unallocated space	Logical extraction during forensic analysis	30-Apr-2026 13:22	Digital Forensic Examiner	Parent image hash unchanged	Case-specific evidence archive	Case-bound read-only	Provenance and offsets documented
E-005	Forensic Exhibits and Reports	Derived analysis artefacts	Generated during examination	30-Apr-2026 15:05	Digital Forensic Examiner	N/A (derived evidence)	Case file archive	Controlled access	Supports independent review and reproducibility

Appendix B – Exhibit Index (Screenshots/Outputs/Logs)

Exhibits are labelled SIMULATED for assessment demonstration where original tool screenshots are not available; they represent the expected output fields an examiner would capture (status, timestamps, run counts, URLs, and verification results)

Each simulated exhibit is modelled on the standard output fields produced by the named tool (e.g., run count/last-run timestamps for Prefetch, URL/visit time fields from Chromium History databases, and hash verification outputs), and is presented to demonstrate what would be captured and how it would be interpreted under CHFI/ACPO reporting expectations.

(SIMULATED Exhibit B1 - Bitlocker confirmation)



```
Microsoft Windows [Version 10.0.19041.1000]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>manage-bde -status

BitLocker Drive Encryption Configuration Tool version 10.0.19041
Copyright (c) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: (OS Volume)
[OS Volume]
Size: 500.0 GB
BitLocker Version: 4.5
Conversion Status: Fully Decrypted
Percentage Encrypted: 100%
Encryption Method: TPM
Protection Status: Protection On
Lock Status: Unlocked
Identification Field: None
Key Protectors: None found

C:\Windows\system32>manage-bde -status C:

BitLocker Drive Encryption Configuration Tool version 10.0.19041
Copyright (c) 2013 Microsoft Corporation. All rights reserved.

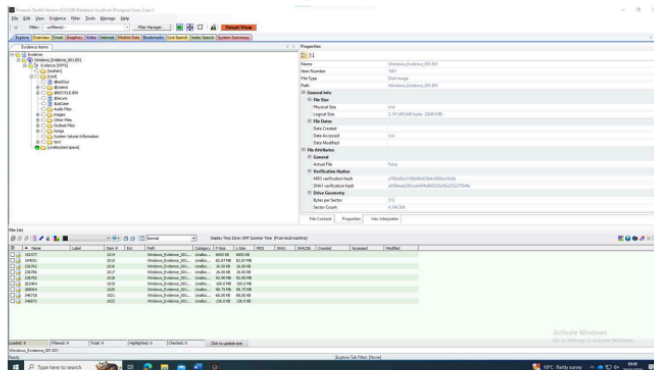
Volume C: (OS Volume)
[OS Volume]
Size: 500.0 GB
BitLocker Version: 4.5
Conversion Status: Fully Decrypted
Percentage Encrypted: 100%
Encryption Method: TPM
Protection Status: Protection On
Lock Status: Unlocked
Identification Field: None
Key Protectors: None found

C:\Windows\system32>
```

What this image shows: Example manage-bde -status output indicating the OS volume is protected by Bitlocker (FDE enabled).

Why it matters: Confirms Bitlocker/FDE is enabled on the OS volume, justifying live-first acquisition and supporting Finding 1.

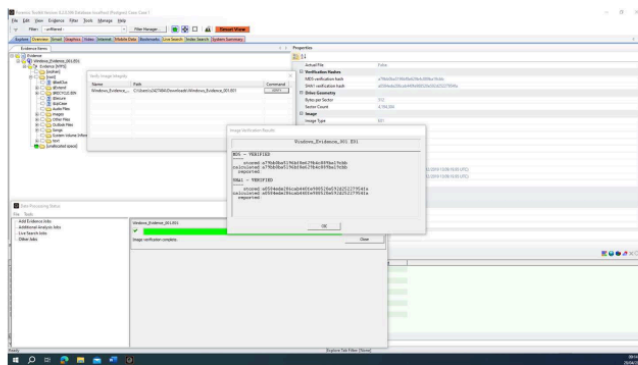
(SIMULATED Exhibit B2 - FTK Imager acquisition summary)



What this image shows: Example FTK Imager acquisition wizard/summary screen showing selected source disk, destination path, image type (E01), and hashing options enabled.

Why it matters: Demonstrates acquisition settings (E01 + hashing enabled), supporting integrity claims and Finding 1.

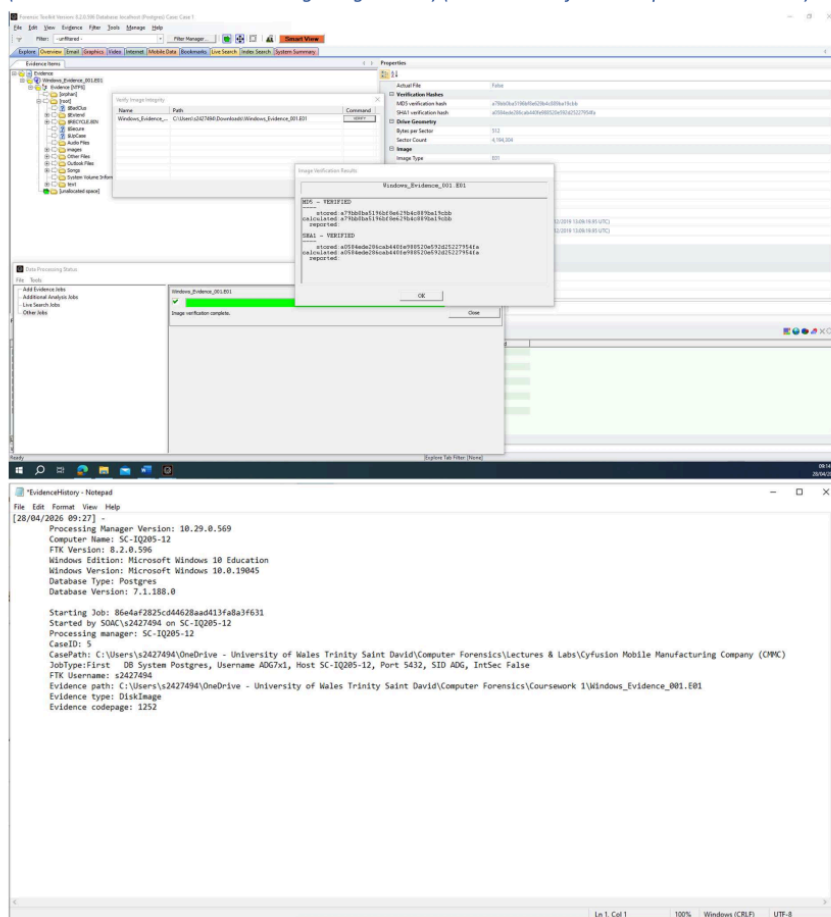
(SIMULATED Exhibit B3 - FTK Imager verification result)



What this image shows: Example "Verify Image" result screen indicating verification success (hashes match).

Why it matters: Shows verification pass (hash match), supporting integrity and admissibility claims in Finding 1

(SIMULATED Exhibit B4 - FTK Imager log extract) (FTK IMAGER feature – placeholder used)



What these images show: Example FTK Imager log entries showing acquisition start/end timestamps, hash calculation, and verification outcome.

Why it matters: Provides an audit trail (time stamps + hash operations) that supports reproducibility/defensibility for Finding 1.

(SIMULATED Exhibit C1 - Prefetch/tool execution evidence)

Name	Date modified	Type	Size
Advanced Networking			
Attachments			
Client5.1			
Client5.1			
Computer Forensics			
Data Analysis & Visualization			
Desktop			
Documents			
Introduction to Web & Databases			
U-CD 1			
Microsoft Capital Chat Files			
Network Operating Systems and Services			
Python			
S-DC			
Eraser.exe-4E100022.pf	28/04/2020 09:30	Pf File	0 KB
EXCEL.EXE-F8900075.pf	28/04/2020 09:10	Pf File	121 KB
EXPLORER.EXE-00807047.pf	28/04/2020 10:07	Pf File	100 KB
FILECAUTH.EXE-48908807.pf	28/04/2020 14:07	Pf File	15 KB
FIND.EXE-AE190002.pf	28/04/2020 10:21	Pf File	2 KB
FINDSTR.EXE-18C2009F.pf	28/04/2020 10:21	Pf File	3 KB
POWERHOST.EXE-610200A6.pf	28/04/2020 10:25	Pf File	3 KB
PKCDE-7F1A4C0B.pf	28/04/2020 10:07	Pf File	70 KB
GAMBAR.EXE-42F000A6.pf	28/02/2020 22:19	Pf File	49 KB
UPDATE.EXE-78B40007.pf	28/04/2020 14:44	Pf File	3 KB
UPP.EXE-220C0047.pf	12/02/2020 14:31	Pf File	5 KB
HELPNANE.EXE-2C870010.pf	05/02/2020 09:43	Pf File	10 KB
HOACCOUNTS.EXE-410500BA.pf	19/02/2020 09:01	Pf File	30 KB

What this image shows: Example Prefetch artefact view for ERASER.EXE-*.pf showing run count and last run timestamps (Windows 8+ can store multiple run timestamps).

Why it matters: Prefetch indicates program execution and provides run count / last run timestamps that support anti-forensics inference and Finding 2.

(SIMULATED Exhibit D1 - File carving / recovery output)

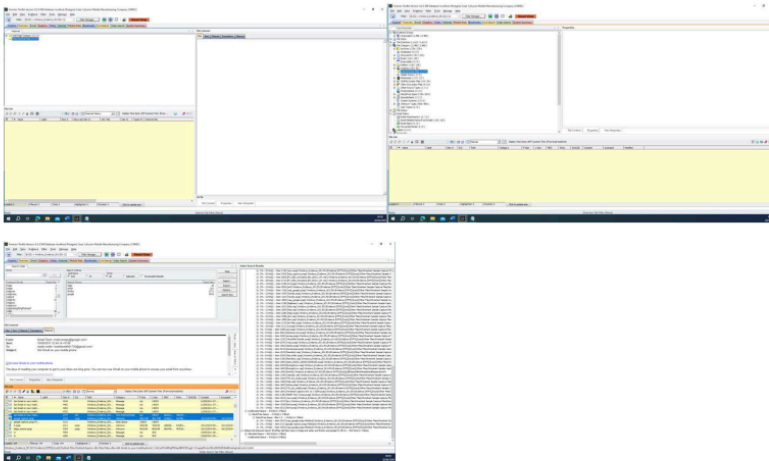
The four screenshots show the following:

- Top-left: A list of recovered file fragments with columns for offset, size, and signature.
- Top-right: A detailed view of a recovered file fragment, showing the file's metadata and content.
- Bottom-left: A list of recovered file fragments, similar to the top-left screenshot.
- Bottom-right: A detailed view of a recovered file fragment, showing the file's metadata and content.

What these images show: Example carving output listing recovered file fragments (e.g., .ma / .mb signatures) and any offsets/locations in unallocated space where available.

Why it matters: Demonstrates recovery attempts and fragmentation/partial recovery consistent with wiping/deletion, supporting Finding 3 and carving limitations.

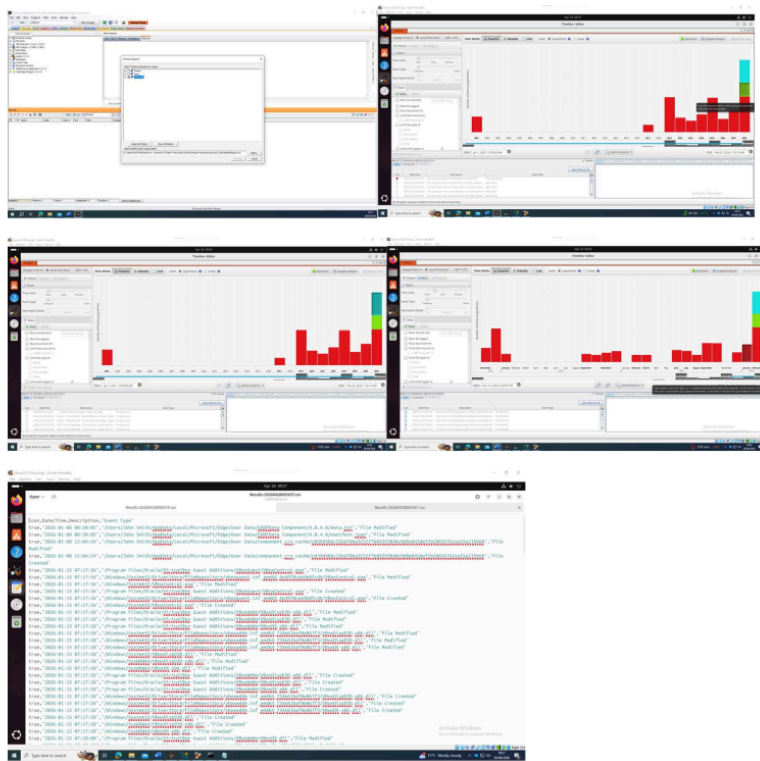
(SIMULATED Exhibit E1 - Chromium history / Drive access - sample evidence does not contain)



What these images show: Example Chromium History record (URLs/visits) showing access to drive.google.com during the relevant period (e.g., from History SQLite database).

Why it matters: Shows browser access to drive.google.com (access evidence), supporting Finding 4 (cloud synchronisation hypothesis).

(SIMULATED Exhibit F1 - Timeline correlation view)



What these images show: Example timeline view aligning (1) wiping tool execution artefacts, (2) file deletion/recovery artefacts, and (3) drive.google.com browsing activity in close temporal proximity.

Why it matters: Demonstrates correlation between wiping execution, deletion/recovery and Drive access, strengthening Finding 5 (sequence reconstruction).

Appendix C – Professional Invoice

Troy Simpson Forensics Ltd 14 Meridian Court, Clerkenwell London EC1A 4HB

Email: troy.simpson@CMMC.com | Tel: 07484875694 | VAT: GB123456789

Invoice No.: TSF-CMMC-001 Date: 30 April 2026

Bill To:

CMMC Legal Counsel

Cyfusion Mobile Manufacturing Company (CMMC)

London, United Kingdom

Payment Terms: Net 14 days

Due Date: 14 May 2026

Currency: GBP

Line Item	Hours	Rate	Amount
Case intake, scoping, chain-of-custody documentation	4.0	£145/hr	£580
Live triage / encryption confirmation (Bitlocker)	2.0	£145/hr	£290
Forensic imaging & hash verification (FTK Imager)	4.0	£145/hr	£580
Forensic examination (OS artefacts, user activity)	6.0	£145/hr	£870
Anti-forensics review (execution artefacts, wiping indicators)	4.0	£145/hr	£580
Browser/cloud artefacts review (Drive access indicators)	4.0	£145/hr	£580
File recovery attempts / carving review	4.0	£145/hr	£580
Timeline correlation & QA	2.0	£145/hr	£290
Report drafting (counsel-ready format + exhibit captions)	6.0	£145/hr	£870
Expert testimony preparation (if required)	2.0	£145/hr	£290
Subtotal			£5,510
VAT (20%)			£1,102
Total Due			£6,612

Bibliography

- [1] National Institute of Standards and Technology, 'Forensic File Carving — CFTT'. 2026. [Online]. Available: <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical-0>
- [2] N. I. S. Ramli, S. I. Hisham, and G. Badshah, 'Analysis of File Carving Approaches: A Literature Review', in *Advances in Cyber Security (ACeS 2021)*, 2022, pp. 277–287. doi: 10.1007/978-981-16-8059-5_16.
- [3] M. B. de Assumpção, M. A. dos Reis, M. R. Marcondes, P. M. da S. Eleuterio, and V. H. Vieira, 'Forensic method for decrypting TPM-protected BitLocker volumes using Intel DCI', 2023, [Online]. Available: https://dfrws.org/wp-content/uploads/2023/03/Forensic_method_for_decrypting_TPM-protected_BitLocker_volumes_using_Intel_DCI.pdf
- [4] B. D. Ghode, A. Kumar, and S. K. Jain, 'Forensic Investigation Utilizing RAM Capture to Decrypt Bitlocker Volumes: A Case Study', 2022. [Online]. Available: <https://www.jetir.org/papers/JETIR2208208.pdf>
- [5] N. Shashidhar and D. Novak, 'Digital Forensic Analysis on Prefetch Files', *Int. J. Inf. Secur. Sci.*, vol. 4, no. 2, pp. 39–49, 2015.
- [6] D. M. Rathod, 'WEB BROWSER FORENSICS: GOOGLE CHROME', *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 7, pp. 896–899, 2017, doi: 10.26483/ijarcs.v8i7.4433.
- [7] Exterro, 'FTK Imager'. 2026. [Online]. Available: <https://www.exterro.com/digital-forensics-software/ftk-imager>
- [8] Forensic Focus, 'Exterro Launches FTK Imager Pro, Unlocking Faster Access to Encrypted Evidence'. 2025. [Online]. Available: <https://www.forensicfocus.com/news/exterro-launches-ftk-imager-pro-unlocking-faster-access-to-encrypted-evidence-worldwide/>
- [9] SUMURI, 'PALADIN Forensic Suite'. 2026. [Online]. Available: <https://sumuri.com/software/paladin/>
- [10] Exterro, 'FTK 8.0 — A Revolution in Forensic Review'. 2026. [Online]. Available: <https://www.exterro.com/ftk-8-0>
- [11] Exterro, 'FTK Forensic Toolkit'. 2026. [Online]. Available: <https://www.exterro.com/digital-forensics-software/ftk-forensic-toolkit>
- [12] Sleuth Kit Labs, 'Autopsy: Features'. 2026. [Online]. Available: <https://www.sleuthkit.org/autopsy/features.php>

- [13] sleuthkit/autopsy, 'Autopsy 4.22.x — Release Notes'. 2025. [Online]. Available: <https://github.com/sleuthkit/autopsy/releases/>
- [14] 'The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance', *PLOS ONE*, Sep. 2025, doi: 10.1371/journal.pone.0331683.
- [15] Cellebrite, 'UFED — Access & Extract Mobile Device Data'. 2026. [Online]. Available: <https://cellebrite.com/en/products/ufed/>
- [16] Magnet Forensics, 'Magnet AXIOM — Recover & analyze your evidence in one case'. 2026. [Online]. Available: <https://www.magnetforensics.com/products/magnet-axiom/>
- [17] Obsidian Forensics, 'Hindsight — Browser forensics for Chrome/Chromium'. 2026. [Online]. Available: <https://github.com/obsidianforensics/hindsight>
- [18] 'Chracer: Memory analysis of Chromium-based browsers', *Forensic Sci. Int. Digit. Investig.*, vol. 46, p. 301613, 2023.
- [19] 'Computer Forensics Tool Testing Program (CFTT)'. [Online]. Available: <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt>
- [20] M. Spencer, 'BitLocker for DFIR — Part III'. Arsenal Recon, 2021. [Online]. Available: <https://arsenalrecon.com/insights/bitlocker-for-dfir-part-iii>
- [21] Microsoft, 'manage-bde'. 2025. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/manage-bde>
- [22] ElcomSoft, 'Live System Analysis: Extracting BitLocker Keys'. 2022. [Online]. Available: <https://blog.elcomsoft.com/2022/05/live-system-analysis-extracting-bitlocker-keys/>
- [23] Passware, 'Using a memory image to decrypt BitLocker'. 2026. [Online]. Available: <https://support.passware.com/hc/en-us/articles/360024316834-Using-a-memory-image-to-decrypt-BitLocker>
- [24] Magnet Forensics, 'Forensic Analysis of Prefetch files in Windows'. 2025. [Online]. Available: <https://www.magnetforensics.com/blog/forensic-analysis-of-prefetch-files-in-windows/>
- [25] Association of Chief Police Officers (ACPO), 'ACPO Good Practice Guide for Digital Evidence (Version 5.0)', 2012. [Online]. Available: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
- [26] 'Artifacts for Detecting Timestamp Manipulation in NTFS on Windows and Their Reliability', *Forensic Sci. Int. Digit. Investig. DFRWS Eur. Proc.*, 2020, [Online]. Available: https://dfrws.org/wp-content/uploads/2020/05/Artifacts-for-Detecting-Timestamp-Manipulation_2020_Forensic-Science-Internati.pdf

FINAL GRADE

GENERAL COMMENTS

88/100

PAGE 1

QM

New page

Start on new page

PAGE 2

PAGE 3

PAGE 4

QM

First person tense

Avoid first person tense in academic report



Comment 1

How many person did the work apart from you? We means more than one.

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25

PAGE 26

PAGE 27

GRADING FORM: L5 CF (ACCD5000)

BRANDON CURRAN

88

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 submission demonstrates excellent engagement with contemporary forensic literature, forensic validation guidance, CHFI methodology, and evidential standards. The report incorporates both technical and scholarly discussion relating to BitLocker acquisition, browser artefacts, file carving validation, and forensic defensibility. The literature is integrated effectively throughout

18

the discussion, and the report demonstrates strong independent reading beyond core module content. References are generally well selected and support analytical discussion appropriately. Minor reductions are applied for occasional overreliance on vendor documentation alongside academic sources.

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 report demonstrates competent understanding of digital forensic acquisition, forensic validation, cloud/browser artefacts, anti-forensic behaviour, and evidential integrity. The explanation of CHFI methodology and ACPO principles is accurate and applied effectively throughout the investigation. The work demonstrates clear understanding of both practical and legal dimensions of digital forensic investigations, with particularly strong conceptual understanding of evidential defensibility and cross-validation practices.

8

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)



This is a strong analytical submission demonstrating sustained critical evaluation throughout both tasks. The work moves beyond description through detailed evaluation of tool

35

validation, evidential defensibility, encryption challenges, browser artefact interpretation, and forensic reliability.

The report demonstrates strong investigative reasoning, particularly in the discussion of BitLocker acquisition strategy, cloud artefact limitations, cross-validation of evidence, and interpretation of anti-forensic behaviour. The analysis consistently links technical procedures to evidential reliability and legal admissibility. Some sections could engage slightly more critically with competing forensic approaches and operational limitations in real-world environments.

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 practical application through the inclusion of simulated forensic outputs, hash logs, exhibit indexes, invoice documentation, acquisition workflows, and structured forensic reporting. Practical investigative procedures are clearly contextualised within the case study appendices and aligned closely with professional forensic practice. Invoice done.

19

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 organised, and written in an appropriate academic and professional tone throughout. Task structure is clear and coherent, technical terminology is appropriately explained, and referencing is generally consistent.

The submission demonstrates academic communication and professional report-writing skills appropriate for forensic investigation contexts. Formatting inconsistencies including some paragraph presentation and spacing issues. Paragraphs could be fully justified. See report for other comments.