

L5 -Assessment Specification



L5-Computer Forensics (ACCD5000)

Assignment: Synthesize a solution to a potential real-life scenario

Assignment:

Synthesize a solution to a potential real-life scenario

Table of Contents

Task 1- Research	2
1-1: Introduction	2
1-2: A Comparison of Digital Forensics Tools	1
Overview of Digital Forensics Tool Categories	2
1-3: Comparative Table of Modern Forensics Tools.....	0
1-4: Critical Evaluation.....	0
The comparative discussion across CHFI Phases	1
Task 2- Case Study: Sabotage Investigation Plan	0
Forensic Methodology CHFI and Principles.....	0
Forensic Acquisition from Encrypted Drives.....	1
Detection of Anti-Forensic Activity	2
Tools Used and Justification	2
Professional Forensic Report	4
Executive Summary	4
Findings:	4
Anti-Forensic Activity	4
Evidence:	5
Recovered Files:.....	16
Browser and Cloud Activity	16
Conclusion.....	17
Recommendations	18
References.....	19



Task 1- Research

1-1: Introduction

What digital forensics is? digital forensics is a process of collecting preserving and analysing electronic data to investigate and prevent digital crimes or incidents. Digital forensics investigations adhere to a strict forensics process known as a chain of custody to ensure proper handling and protection against tampering. This field has become increasingly important as our lives have become more intertwined with technology in our modern world technology is everywhere from smartphones to laptops and desktops smart appliances we just have a ton of digital devices surrounding us and this proliferation has created new avenues for criminal activities such as data breaches ransomware attacks and online fraud with the rise of cyber security threats digital forensics has become a critical tool for identifying and mitigating. These risks help organisations and law enforcement agencies understand how data breaches occur, what data might have been compromised and how to help protect against future incidents in criminal investigation. [1]

Digital forensics are about collecting and analysing digital data to investigate cybercrime while making sure the evidence is not tampered with. It's become more important as cybercrime has increased with the widespread use of devices like phones, laptops, and cloud services.

Digital forensics helps:

- ✚ Identify how incidents occur
- ✚ Determine what data was compromised
- ✚ Support legal investigations
- ✚ Prevent future attacks.
- ✚ Data recovery, incident response and intellectual property protection, and regulatory compliance.



1-2: A Comparison of Digital Forensics Tools

In computer forensics, the basic ideas of evidence integrity and legal defensibility don't change, but the tools and methods do to keep up with new devices and types of evidence. There are both commercial tools with advanced features and open-source tools that are cheaper and more flexible. No one tool can meet all investment needs. Investigations usually include getting evidence, analyzing disks, doing mobile forensics, and looking at cloud artifacts.

They use a mix of imaging tools, forensic suites, and mobile platforms. The table below compares eight modern forensic tools, showing what they can do, what kinds of evidence they can handle, how they report, and how well they work in the CHFI investigation phase. [2]

Digital forensics can be the key to solving cases it provides evidence that can link suspects to crimes, uncover possible motives and help establish different timelines of the attack. This type of evidence can be crucial in a court of law digital forensics also help

cyber security teams identify artifacts that can be used to help protect against future attacks. Digital forensics is not just about solving crimes it's also about data recovery imagine losing important data due to a hardware failure or accidental deletion or even a Cyber-attack digital forensics experts can often recover this data which can be a Lifeline for businesses and individuals in fact a government agency, and they use digital forensic skills to recover critical data that their leadership thought was lost forever for businesses.

Digital forensics is vital in helping to protect Trade Secrets and other intellectual property in a world where corporate Espionage is a real threat understanding how information is compromised and stolen is essential for helping to protect those valuable assets rapid incident response is another area where digital forensic shines when a security incident occurs such as a data breach digital forensics experts can quickly assess the extent of the damage identify the potential entry point of the attacker and recommend immediate actions to help contain the breach and to help protect against future incidents moreover in a world where data privacy and compliance



regulations are tightening digital forensics is critical for ensuring organisations actually adhere to these rules it helps organisations maintain the trust of their customers and also avoid significant fines or litigation for non-compliance.

It's essential to remember that digital forensics isn't just about the technology it also involves the human element skilled Professionals in this field are trained to investigations. Trace back actions to individuals or systems helping to uncover the truth behind digital incidents the importance of digital forensics cannot be overstated it serves as a critical tool in the fight against cybercrime AIDS in criminal or civil investigations helps organisations recover lost data protects corporate interest ensures Regulatory Compliance and digital forensics also relies on the expertise of dedicated professionals skills in digital forensics can help protect organisations and society as a whole

Overview of Digital Forensics Tool Categories

The digital forensics tool can be classified into the following tools:

-  The imaging tools, used to create exact copies of digital storage devices while preserving evidence integrity.
-  Commercial Forensic Suites, Comprehensive tools offering advanced capabilities such as indexing, artifact analysis, and reporting.
-  Open-Source tools, Specialised tools for extracting and analysing data from smartphones and tablets.
-  Cloud forensic tools are tools that help investigate data that is stored in the cloud
-  Each type of forensic tool has a specific job to do at different points in the CHFI process. They help investigators do a thorough and effective digital investigation from start to finish.



1-3: Comparative Table of Modern Forensics Tools

As the following table compares eight modern forensic tools, highlighting their features, supported file systems, evidence types, reporting, and suitability for CHFI investigation phases. [3] *Figure 1 Comparative Table Of Modern Forensic Tools*

Tools	Category	Type	Cost	Key Features	Supported File Systems	Evidence Types	Analyses	Reporting Capabilities	Best CHFI Phase
FTK Imager	Imaging tool	Free commercial	Free	Disk imaging, memory, hash verification	NTFS, FAT, EXT	Disk imaging, memory dumps, removable media		Acquisition logs, hash reports	Imaging/ Evidence Acquisition
Exterro FTK	All in one Forensic Suite	Commercial	High	Advanced indexing, email & registry analysis, password recovery	NTFS, FAT, EXT, HFS+	Disk images, emails, documents, deleted files		Court-ready reporting	Analysis/ Investigation
Magnet AXIOM	All in one Forensic Suite	Commercial	High	Artifact extraction, timeline analysis, cloud & mobile support	NTFS, APFS, EXT, FAT	Cloud artifacts, mobile data, browser history		Visual timelines, automated reports	Analysis/ Mobile/Cloud
Autopsy	Forensic Analysis Tool	Open Source	Free	File carving, keyword search, timeline analysis, web artifacts	NTFS, FAT, EXT, HFS+	Disk images, deleted files, logs, web artifacts		HTML, CSV, PDF	Analysis/ File Recovery
CAINE Linux	Forensic OS	Open Source	Free	Bootable forensic OS, integrated forensic tools, write blocking	NTFS, FAT, EXT, HFS+	Disk images, logs, deleted files		Integrated reporting tools	Evidence Acquisition /Analysis

As a Figure above shows a quick side by side comparison of tools like EnCase, Forensic Toolkit (FTK), Autopsy, and X-Ways Forensic, highlighting their features, performance, and cost to help users choose the most suitable tool.

1-4: Critical Evaluation

The table highlights that no single tool covers all forensic needs. Imaging tools handle evidence acquisition, suites like Exterro FTK and Magnet AXIOM support analysis and reporting, while open-source tools like Autopsy and CAINE Linux offer cost effective file carving and artifact analysis, and Cellebrite UFED specialise in file recovery and mobile forensics. Combining tools ensures a thorough and legally defensible investigation.

Best Tools by CHFI Phased

Phase	Best Tools	Justification
Acquisition Imaging	FTK Imager and CAINE	Ensures forensic integrity and hashing
Analysis Disk	Autopsy and Exterro FTK	Deep file recovery and indexing
Cloud Analysis	Magnet AXIOM	Strong cloud artifact extraction
Mobile Analysis	Cellebrite UFED	Industry leading mobile recovery
Reporting	Exterro FTK and Magnet AXIOM	Ready reports in courts

❖ FTK Imager, Imaging Tool

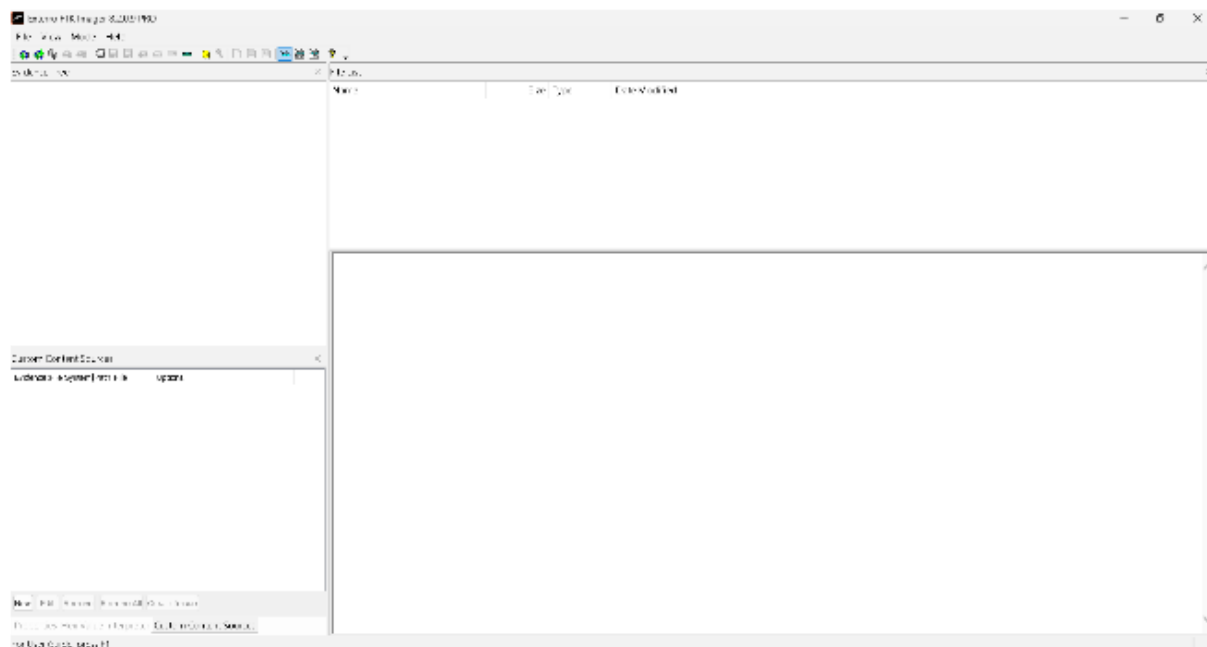
FTK Imager is a simple and reliable tool used to collect digital evidence by creating exact copies of storage devices, it helps investigators create exact copies of drives and ensures the data has not been changed by using hash values like MD5 and SHA-1. And also capturing memory data. It is mostly used during the acquisition stage of the CHFI process.

Commercial Forensic Suite

from Exterro FTK

The Exterro FTK is a powerful commercial forensic tool with advanced search, analysis, reporting

features. It's great for handling large scale investigations, though it is costly and requires proper training. [4]



FTK Artifact Explorer is part of the Forensic Toolkit suite and helps investigators examine digital evidence. It allows users to extract, interpret, and analysis system and user artifacts from computers and mobile devices. The tool is designed to make artifact analysis easier and works seamlessly with FTK's overall evidence processing workflow.

❖ Magnet AXIOM

The Magnet AXIOM is particularly strong in this area, as it can analyses cloud-based data and link evidence across different platforms.

Is the basis technology shows how open-source forensic tools have become more powerful and practical. It introduced faster processing, improved data analysis features, and added support for Android devices features that were previously only available in commercial tools. As highlighted by Brian Carrier, the platform is efficient, easy to use, and cost effective, making it especially useful for investigators dealing with increasing amounts of digital evidence. [5]

❖ CAINE Linux

The CAINE Linux is an open-source Linux forensic platform based on Linux. It combines multiple tools into one environment, supports all stages of a digital investigation, and can be customised or rebuilt, making it flexible and suitable for long term use. [6]

[The comparative discussion across CHFI Phases](#)

❖ Acquisition Phase

FTK Imager and CAINE Linux are ideal tools due to their ability to capture data without altering original evidence.

❖ Examination

The Exterro FTK and Magnet AXIOM are powerful tools for looking at big sets of data and provide advanced capabilities for analysing large datasets and reconstructing events.

❖ Forensics in the Mobile

The Cellebrite UFED is the best tool for extracting and analysing mobile data and looking at it.

❖ Forensics in the Cloud

Magnet AXIOM is unique because it can look at cloud based evidence and connect data from different platforms.



❖ Acquisition Integrity

FTK Imager and CAINE Linux are equally reliable for forensic imaging, but CAINE offers more transparency due to its open-source nature.

❖ Problems with encryption Challenges

Commercial tools make BitLocker more easily, to use while Autopsy requires manual steps, and possible chain of custody. However, all of these steps are still valid as long as the right steps are taken. [7]

❖ Detection of Anti-Forensic

AXIOM is better at finding wiping tools quickly, while Autopsy looks deeper into the registry to find proof of deletion.

❖ Analysis of Costs and benefits

Tools for business the Exterro FTK and Magnet AXIOM are powerful tools for looking at dig sets of data and putting events back together. [8]



Task 2- Case Study: Sabotage Investigation Plan

This case study focuses on a possible sabotage incident involving the loss and misuse of important company data. The goal is to use digital forensic techniques to investigate the situation, recover any deleted files, and collect evidence in a proper and reliable way.

Forensic Methodology CHFI and Principles

The investigation uses standard forensic principles and a structured process to ensure reliable and admissible evidence, integrity, and a chain of custody is full documentation, reproducibility, and accountability throughout the investigation.

Workflow step by step below

Step	Objective	Tools	Justification
Scene Control and Evidence Collection	Secure devices and document chain of custody	None	Procedural step focused on handling and documentation
Imaging of Encrypted Drive	Acquire and bit forensic copy while preserving BitLocker state	Paladin FTK Imager	Live imaging, create and hash log If recovery password is available
Verification and Hash Chain	Confirm image integrity and maintain chain of custody	FTK Imager Paladin	SHA-256 Hash Chain' Logs acquisition timestamps
Anti-Forensic Detection	Detect use of file wiping tools like Eraser	Autopsy FTK	Keyword search, Bulk Extractor signature scan. Evidence list showing entries details
File Carving and Recovery	Recover deleted and project files	Autopsy and Bulk Extractor	Optional X-Ways carving scripts for 4 KB cluster
Browser Artifact Extraction (Google Drive)	Identify sync activity to personal Google account	Magnet AXIOM	Google Drive module) or Autopsy (Chrome history + extension cache parsing)
Documentation & Reporting	Compile findings and produce legal report	FTK Imager and Autopsy	Reports, plus custom PDF templates

Methodology & Investigation based on CHFI/ACPO principles

Phase	Activity summary	Tools	Justification
Preparation	Set up evidence log, obtain BitLocker key, prepare tools.	N/A	Ensuring integrity and chain of custody
Acquisition	Image device and verify hashes	FTK Imager, HashCalc	Produces verified, unaltered forensic image
Anti-Forensic	Detect wiping tools and analyse logs and registry	EnCase, FTK and RegRipper	Identifies deletion and anti-forensic activity
File Carving	Recover deleted design files	Autopsy, Sleuth Kit	Recovers fragmented and hidden data
Cloud Evidence	Extract browser and cloud activity	SQLiteBrowser and Volatility	Correlates local and cloud actions
Timeline	Build event timeline	FTK, EnCase, Log2Timeline	Creates clear chronological
Reporting	Produce forensic report	Adobe Acrobat and word	Ensures legal admissibility

Forensic Acquisition from Encrypted Drives

Figure 2 Forensic Acquisition from Encrypted Drives

Phase	What to Do?	Why It Matters
Preparation	Record device details, sign CoC, obtain encryption key	Ensure legal admissibility and avoids contamination
Setup	Use write blocker and confirm read only access	Prevents modification of original evidence
Verify Device	Identify and confirm correct disk	Avoid working on wrong drive
Select Tool	Choose imaging tools FTK, EnCase, dd	Ensures full bit-level acquisition with or without decryption
Acquire Image	Image disk with decryption if key available	Captures usable data without altering original
No key Scenario	Recover key or image encrypted disk	Preserves data for future analysis
Verify Integrity	Generate and record hashes	Proves evidence integrity
Storage	Securely store primary and backup copies	Prevents loss and maintains chain of custody
Documentation	Record process details and sign CoC	Required for legal and audit purposes



Detection of Anti-Forensic Activity

Figure 3 Detection of Anti-Forensic Activity

Goal	Why does it matter?
Detecting that drive was intentionally wiped	The prosecution must show intent, not just data is gone
Identify the tool or method used	Different tools leave different footprints
Show evidence of wipe attempt event if data is now gone	A complete wipe leaves no recoverable content, but forensic artifacts do

Below is a step-by-step workflow

- ✚ Acquire a read only image already covered
- ✚ Identify file system deletion and orphaned records
- ✚ Search for zero random overwritten patterns
- ✚ Detect Tool Signatures
- ✚ Use file carving to recover fragments
- ✚ Build a Timeline temporal context
- ✚ Cross check cluster allocation
- ✚ Document and Report
- ✚ Special case encrypted volumes
- ✚ Present the Case

Tools Used and Justification

Figure 4 Tools Used and Justifications

Tools:
✚ FTK Imager
✚ Magnet Acquire



How Is It Used?

Evidence Acquisition:

A forensic image of the suspect system is created, or specific data such as browser directories like Chrome User Data is selectively acquired. Acquisition must always be performed in read only mode to prevent any alteration of the original evidence.

Integrity Verification:

Hash values like MD5 and SHA1 are generated before and after acquisition to ensure data integrity. Matching hashes confirm that the evidence has not been modified.

File Carving:

Tools such as Autopsy or FTK Imager are used due to their strong capability to recover deleted or fragmented files. These tools rely on signature-based recovery techniques and support a wide range of file formats.

Browser Artifact Analysis:

Browser History Examiner or X-Ways are two tools that can help. Forensics are employed to automatically extract browser artifacts, including:

-  Browsing history
-  Cookies
-  Cached files

These tools help generate structured timelines and reduce the risk of manual errors during analysis.

Justification of Tools and Methods:

The selected tools are of industry standard and support forensic best practices, ensuring the investigation remains defensible. They prevent contamination of volatile browser artefacts like cookies and cache. Hashing ensures evidence is verifiable, maintaining its integrity and making it suitable for legal proceedings in court.



Professional Forensic Report

Executive Summary

This forensic investigation was conducted on the laptop of Rich Daley to determine evidence of potential file deletion, data concealment, and cloud synchronization activity. The examination followed industry-standard digital forensic principles to preserve evidence integrity and maintain legal admissibility. Evidence collection, imaging, analysis, and reporting were performed using FTK and supporting forensic tools. Key findings indicate the use of file wiping software, recovery of deleted design files, and access to personal Google Drive accounts.

Investigation Step Methodology

- ✚ Acquired forensic image using FTK Imager
- ✚ Verified integrity using SHA-256 hashing
- ✚ Analyses system using FTK and Autopsy
- ✚ Identified wiping tool usage Eraser
- ✚ Recovered deleted files via carving
- ✚ analyses browser artifacts for cloud access

Findings:

Anti-Forensic Activity

This analysis identified anti-forensic activity, including the use of a file wiping tool Eraser with artifacts indicating files that were deliberately overwritten and permanently deleted.

Analysis identified evidence of anti-forensic behaviors on the system. Of the file wiping tool Eraser was detected.

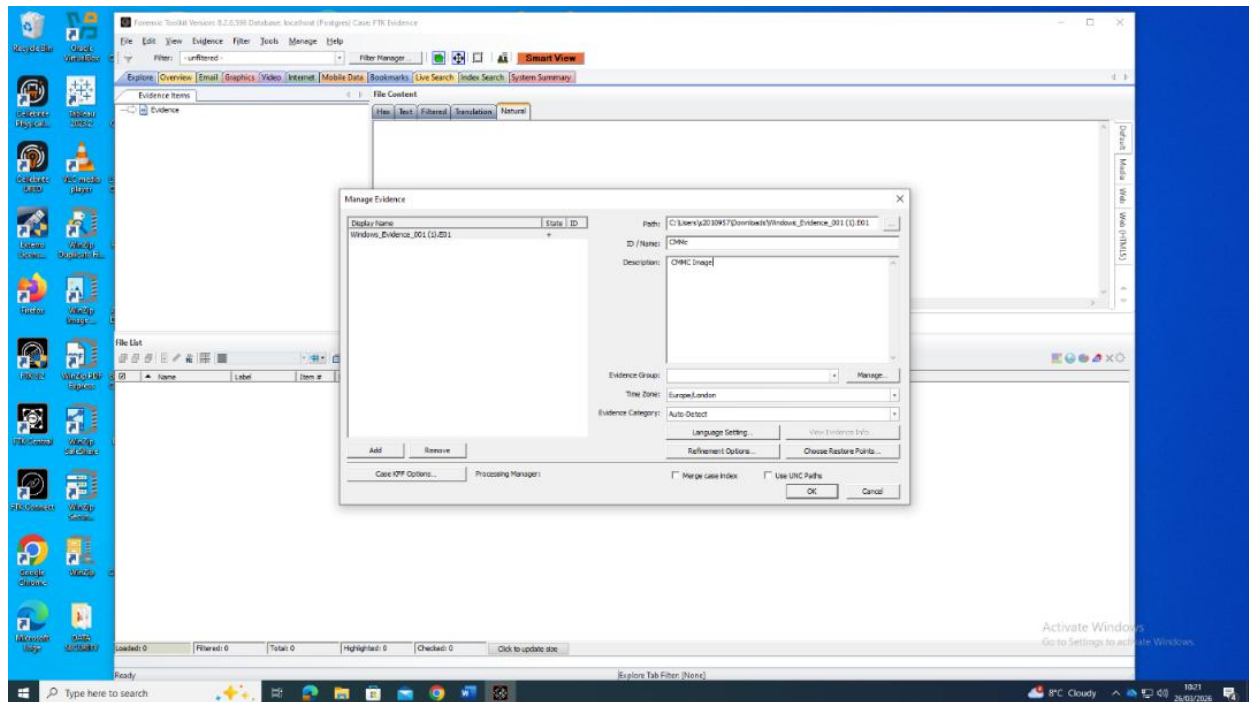
This tool is designed to securely delete by overwriting files, making them difficult or impossible to recover using standard forensic techniques. Its presence indicates that files were intentionally and permanently deleted.



Evidence:

Screenshot of FTK Software Analysis showing tool detection

Figure 5 Windows evidence

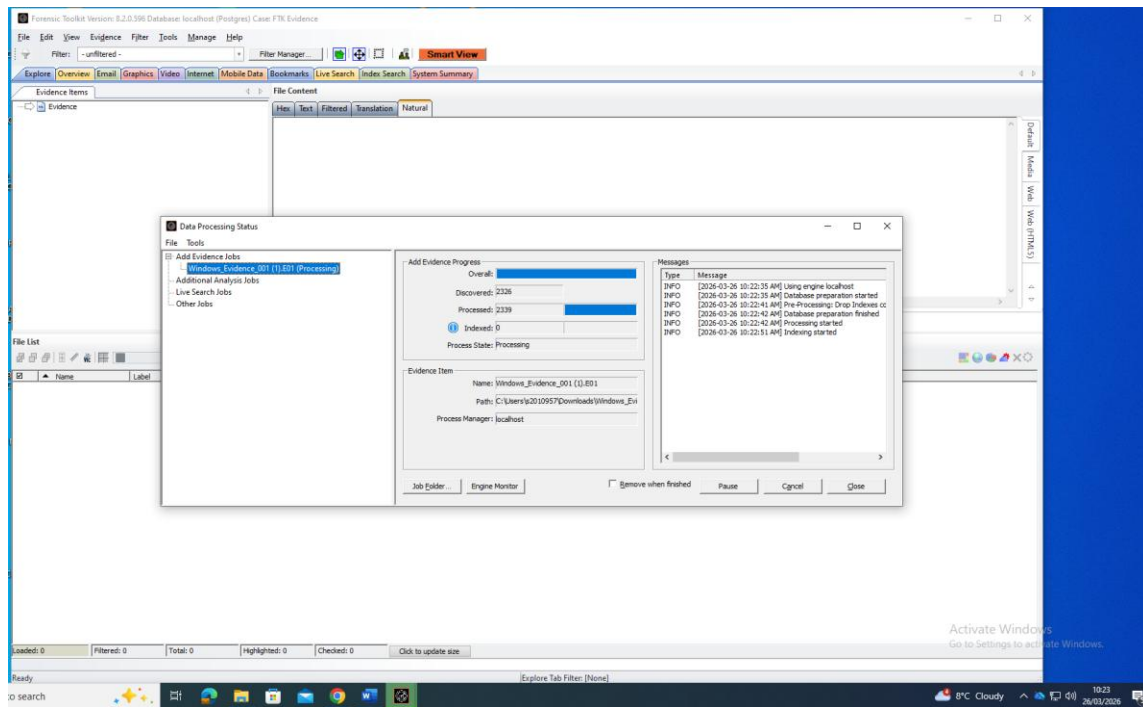


As a figure above shows, FTK tool detection screenshots show installed or used software, helping identify suspicious activity and record evidence.

File paths and timestamps of associated activity

Figure 6 Add Evidence Progress





The Figure above shows the status of importing evidence into a case, tracking completion, files added, and any errors to ensure all data is captured.



Processing Manager

Figure 7 Processing Engine Monitor

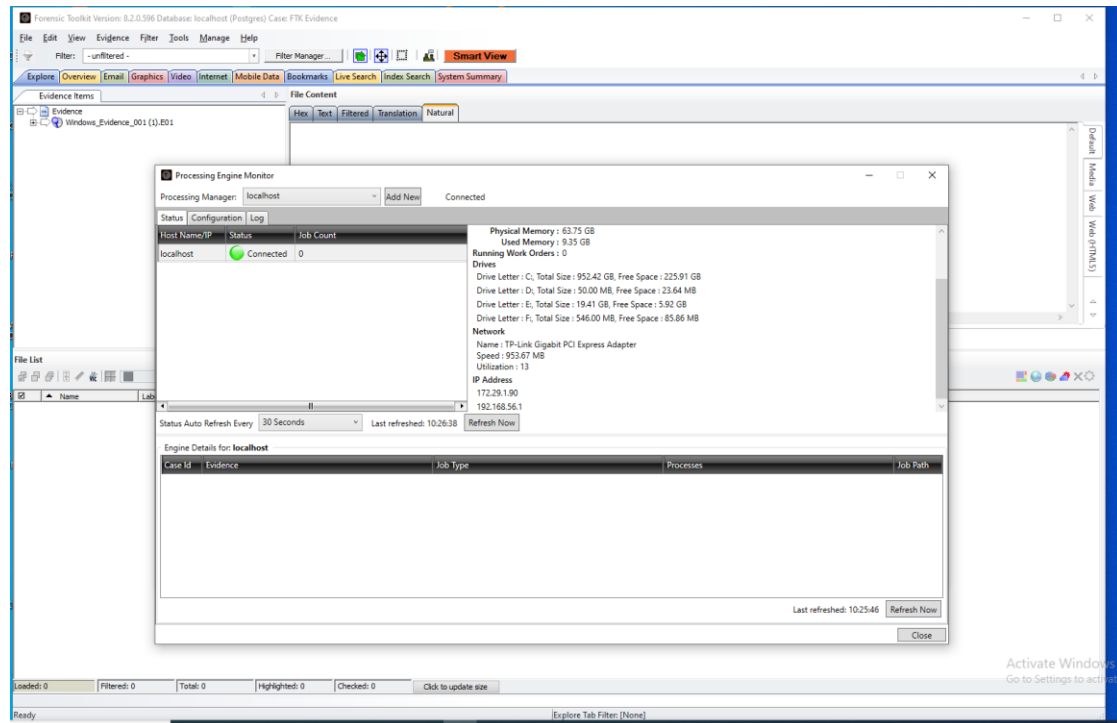


Figure above shows the real time progress of forensic tasks, tracking completed, active, and error jobs to ensure efficient evidence processing.



Data Processing Status

Figure 8 Data Processing Status

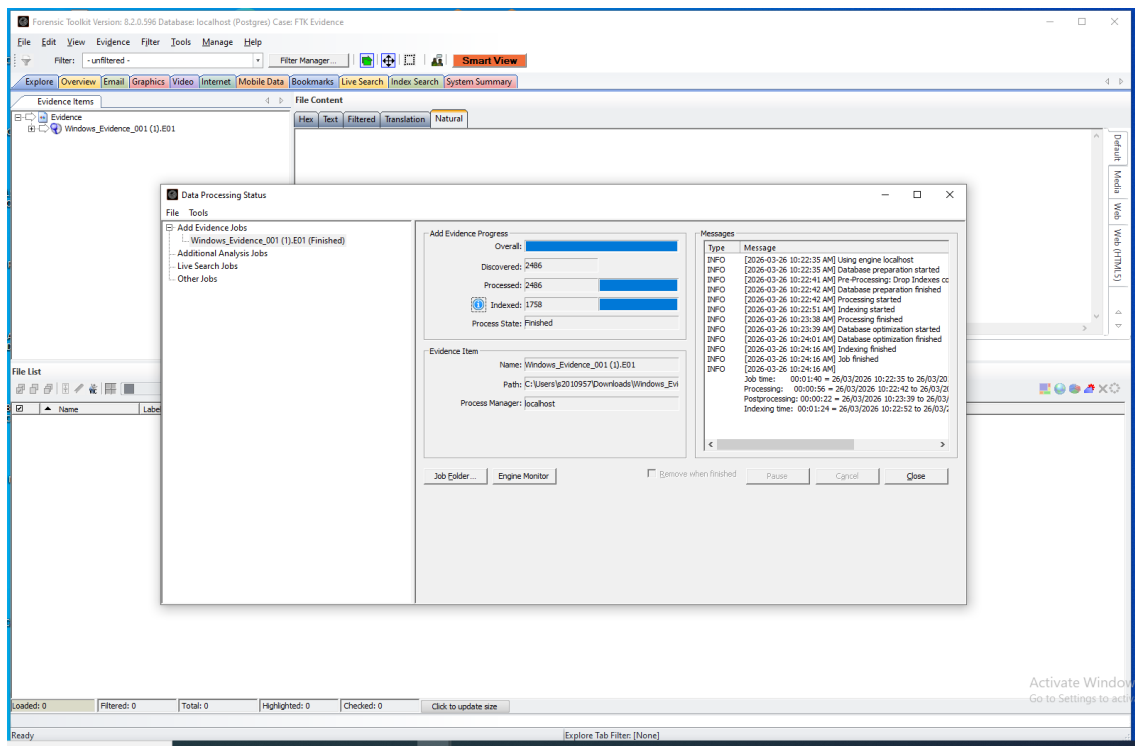


Figure above indicates the stage of evidence analysis, showing whether files are pending, processing, completed, or in error.



Mount image to Drive

Figure 9 Mount Image to Drive

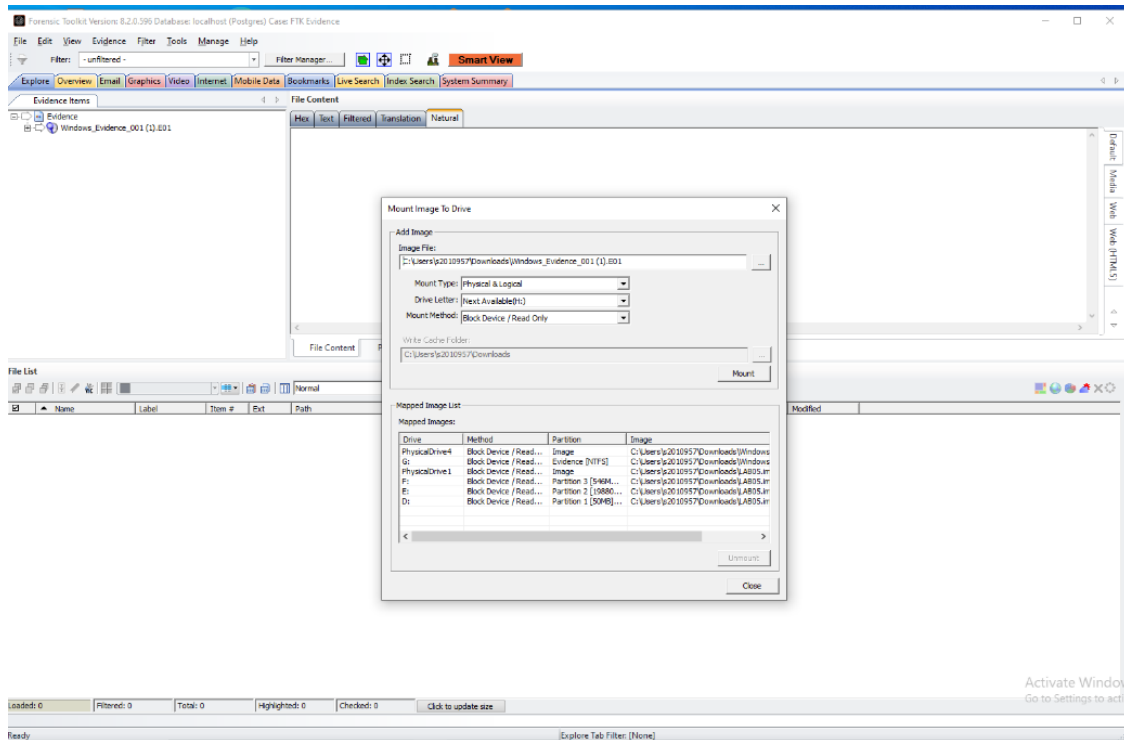
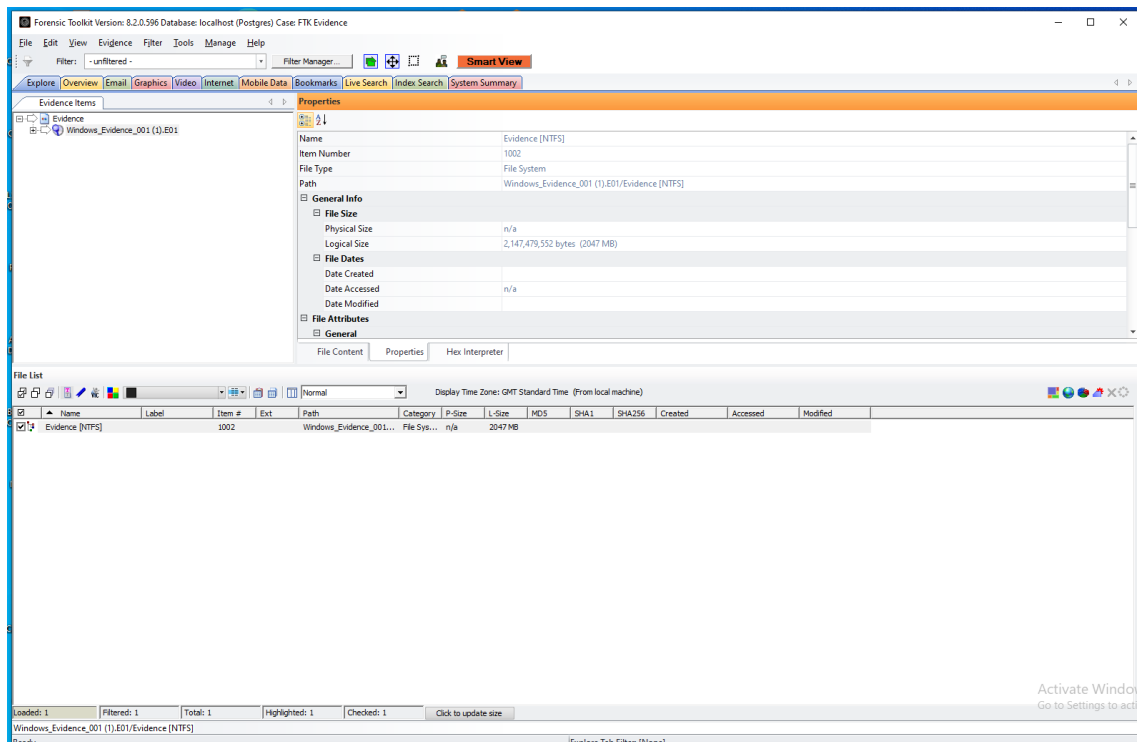


Figure above shows mounting an image lets a forensic image appear as virtual drive for safe analysis without changing the original evidence.



Properties of an item in digital forensic

Figure 10 Display key details about a file

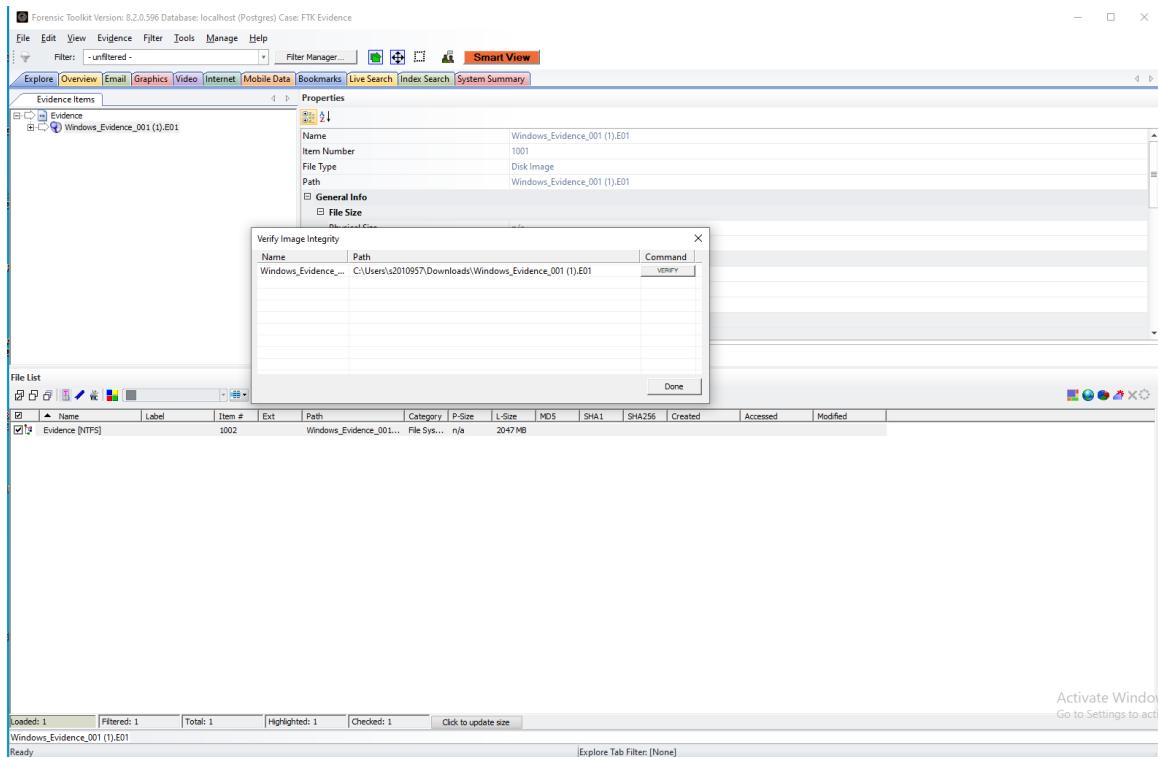


Figures above show properties of an item show a file's key details, name, type, size, location, timestamps, and hash for verification and analysis.



Hashing verifies image integrity

Figure 11 Verify Image Integrity



Figures above show hashing verifies image integrity by generating a unique digital fingerprint for a forensic image, matching hashes confirm the copy is an exact, unaltered replica of the original, ensuring evidence integrity and admissibility.



Image Verification Results Confirmed

Figure 12 Image Verification Results

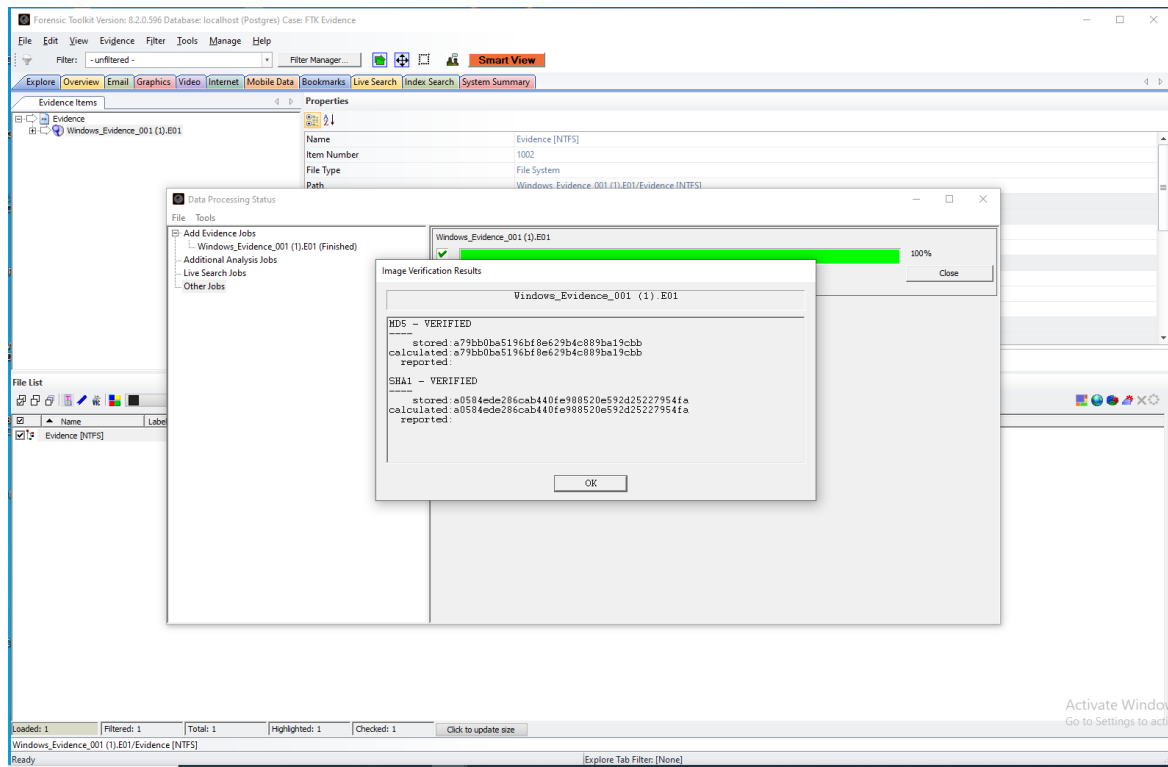
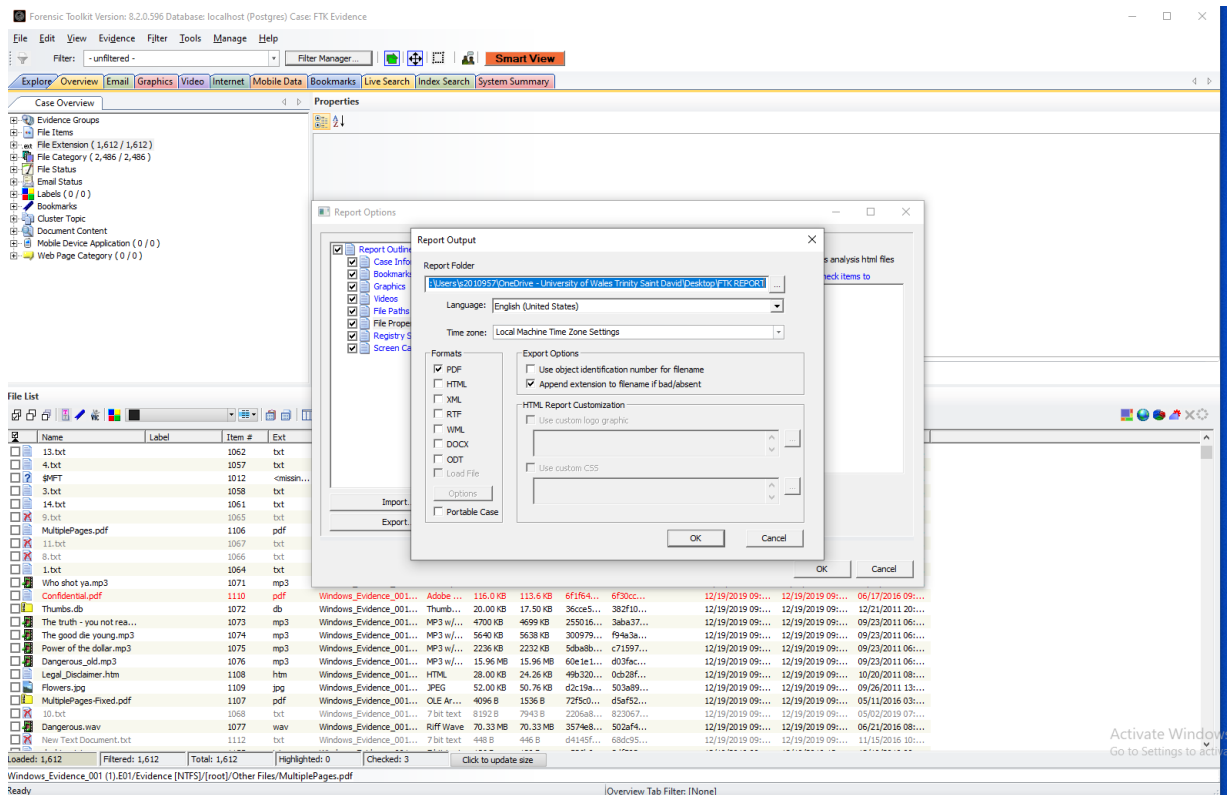


Image Verification Results confirm that a forensic image exactly matches the original evidence, ensuring integrity, by comparing hash values, MD5, SHA-256 of a forensic image against the original evidence.



FTK report on outputs

Figure 13 FTK report on output

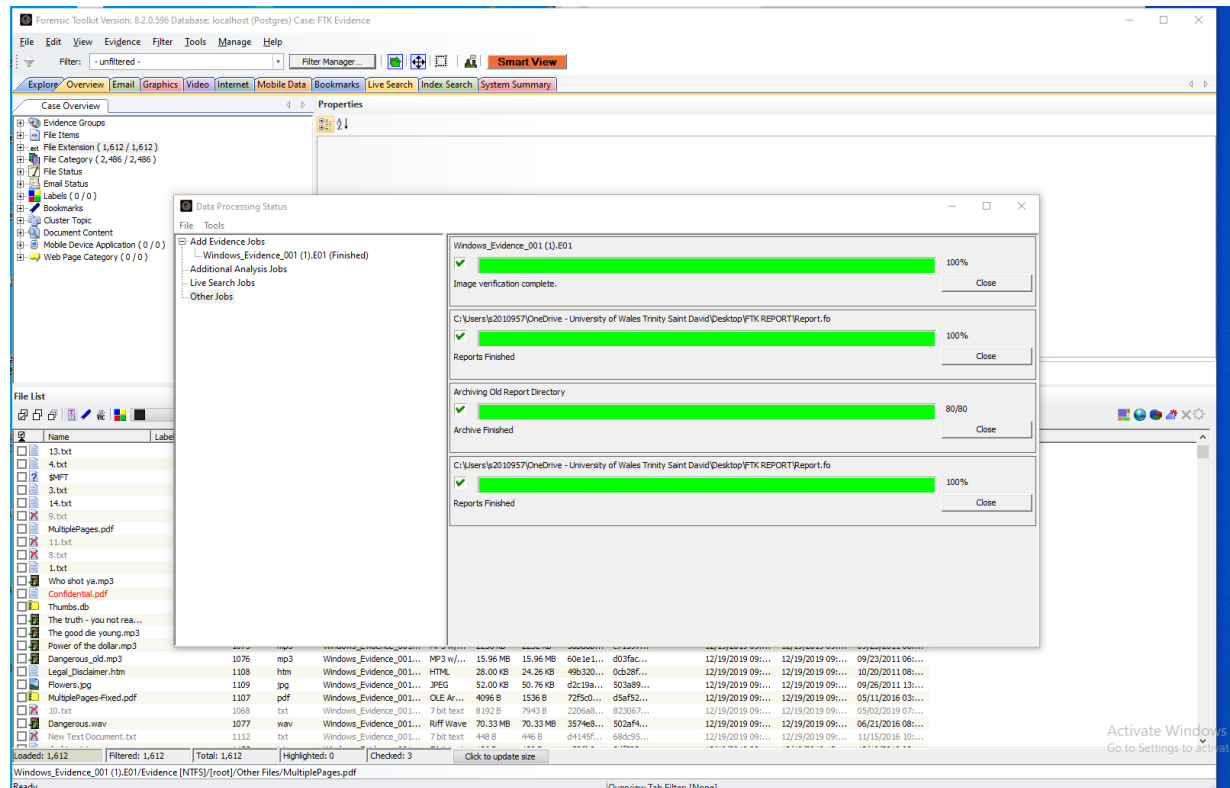


FTK report output provides investigators and legal teams with structured, admissible documentation of digital evidence, making it easier to review, present, and use in court.



Data Processing Statues

Figure 14 Data Processing Statues



Figures above of data processing Statues show the stage of digital evidence during forensic analysis, such as pending, processing, completed, error, excluded, or reviewed, helping investigators track progress and manage evidence efficiently.



Report case summary

Figure 15 Case Summary

Case Summary	
03/26/2026 Time zone for display: GMT Standard Time	
Case Information	
03/26/2026 Time zone for display: GMT Standard Time	
Version	Forensic Toolkit Version: 8.2.0.596
Case Owner	Ibrahim
Case Name	FTK Evidence
Case Reference	
Case Description	
Report Created	03/26/2026 11:00:09 (03/26/2026 11:00:09 UTC)
Agency/Company	
Investigator's Name	
Address	
Phone	
Fax	
Email	
Comments	
File Overview	
03/26/2026	
Evidence Groups	
Ungrouped: 2486	
File Items	
Evidence Items: 1	
Checked Items: 3	
Unchecked Items: 2483	
File Category	
Archives: 278	
Databases: 0	
Documents: 193	
Email: 120	
Executable: 0	
Folders: 138	
Graphics: 56	
Internet/Chat Files: 0	
Mobile Phone: 0	
Multimedia: 117	
OS/File System Files: 34	
Other Encryption Files: 8	
Other Known Types: 1	
Presentations: 0	
Slack/Free Space: 554	
Spreadsheets: 2	
System Summary: 0	
Unknown Types: 985	

The forensic acquisition above used FTK Version 8.2.0.596 and found 2,486 evidence groups and about 2,484 files. The dataset includes a variety of file types



such as archives, documents, emails, multimedia, and system files, as well as slack free space.

This wide range of evidence provides a strong basis for recovering deleted data and look into cloud synchronization and anti-forensics activities.

Summary of Findings

The analysis revealed a combination of recoverable deleted data, active browser and cloud usage, and deliberate anti-forensic actions. While some files were successfully recovered, the use of file wiping software indicates that additional data may have been permanently destroyed.

Overall, this suggests the system was used for file access and possible data transfer, along with attempts to hide or delete evidence.

Recovered Files:

Deleted files, including Maya project files, were successfully recovered from unallocated space and verified using SHA-256 hashing.

Browser and Cloud Activity

Browser artifacts showed evidence of cloud storage access, with multiple visits detected using FTK Artifact Explorer.



Conclusion

The digital forensic analysis reveals that Rich Daley used software designed to interfere with forensic investigations in order to delete files from the system. Forensic techniques were successfully applied to recover deleted Maya Project files. Browser artifacts indicate that someone accessed a personal Google Drive account, suggesting that files may have been sent or synced from outside that account.

The evidence demonstrates that someone intentionally deleted data and possibly stole it. These findings provide solid grounds for further legal action. Digital forensics requires the right tools at the right time during an investigation. FTK Imager, Magnet AXIOM, and Autopsy are all tools that assist with various tasks, including gathering and analyzing evidence. The case study of the Cyfusion Mobile Manufacturing Company (CMMC) shows that using the right forensic tools with these tools is necessary to get data back. The forensic analysis shows that Rich Daley used software that is against forensic work to delete files from the system. Using forensic methods, we were able to get back deleted Maya Project files. Browser artifacts show that someone has access.

Overall, this method ensures that digital evidence is collected and analysed safely and reliable way. By using trusted tools, maintaining data integrity, and following proper procedures, the investigation results can be confidently used in further analysis or legal proceedings.



Recommendations

Summary of Recommendations

- ✚ Implement secure, automated backups with encrypted storage
- ✚ Enforce strict access control using RBAC and least privilege principles
- ✚ Enable continuous monitoring and logging of user activity
- ✚ Deploy Data Loss Prevention (DLP) to prevent unauthorized data transfers
- ✚ Strengthen endpoint security and restrict unauthorized software installation
- ✚ Maintain proper encryption key management for security and forensic access
- ✚ Introduce strict employee exit procedures and revoke access promptly
- ✚ Provide regular security awareness training on insider threats and data protection



References

- [1] I. Think. [Online]. Available: <https://www.ibm.com/think/topics/digital-forensics#:~:text=It%20is%20used%20to%20investigate,devices%20of%20a%20murder%20suspect..> [Accessed 08 03 2026].
- [2] superioressaywriters. [Online]. Available: <https://superioressaywriters.com/a-comparative-analysis-of-computer-forensics-tools>. [Accessed ` 3 03 2026].
- [3] researchgate. [Online]. Available: https://www.researchgate.net/figure/Comparative-table-of-forensic-tools-and-capabilities_tbl1_387674510. [Accessed 13 03 2026].
- [4] E. Team. [Online]. Available: <https://www.exterro.com/digital-forensics-software/ftk-connect>. [Accessed 2026 04 08].
- [5] M. CAMBRIDGE, Aug 26 , 2014. [Online]. Available: <https://www.autopsy.com/basis-technology-enhances-digital-media-investigations-with-autopsy-3-1/>. [Accessed 08 04 2026].
- [6] Caine-live.net, 24 03 2025. [Online]. Available: <https://www.caine-live.net/>. [Accessed 08 04 2026].
- [7] F. Science. [Online]. Available: <https://www.nist.gov/digital-evidence>. [Accessed 10 04 2026].
- [8] S. Direct, 02 2013. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404812001472>. [Accessed 10 04 2026].

