International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Understanding Digital Forensic Tools: Their Features, Applicability and Key Short Comings. A Compendium

John Sitima

Student of MBA Forensic Accounting and Fraud Investigations at National Forensic Sciences University (India).

Abstract

The Paper provides a comprehensive overview of various digital forensic tools used in investigations. The paper outlines the significance of digital forensics in collecting and preserving evidence for computer crimes and cybersecurity incidents. It discusses several prominent tools, including Encase Professional, Magnet Axiom, Passware Kit Forensic, Falcon Neo, Tableau USB Write Blocker, FTK Imager, and Autopsy, detailing their features, applications, and shortcomings. Key features highlighted include data acquisition methods, advanced file analysis capabilities, and reporting functionalities. The paper also addresses the potential limitations of these tools, such as issues with user authentication, performance under load, and chain of custody concerns. By examining these tools' strengths and weaknesses, the document aims to provide insights into their applicability in various investigative contexts and emphasize the importance of selecting appropriate tools for effective digital evidence management.

Keywords: Evidences, Investigations, Digital, Artifacts.

1.0 Introduction

Digital forensics tools are defined by (Kumari, N. and Mohapatra, A.K., , 2016) as software and hardware used to collect and preserve digital evidence for investigations. They are used to investigate computer crimes and cybersecurity incidents and can be used by law enforcement to support or refute hypotheses in court.

1.1 Encase Professional

Encase Professional, developed by OpenText (formerly Guidance Software), is a leading digital forensic tool widely utilized in various investigative fields. It provides a comprehensive suite of features designed for the acquisition, analysis, and reporting of digital evidence from multiple sources, including computers, mobile devices, and cloud storage.

1.1.1 Key Features of Encase Professional

1. Data Acquisition

Encase enables secure and forensically sound data acquisition from a wide variety of devices, ensuring the integrity of digital evidence. It supports over 25 types of mobile devices and various file systems, making it versatile for different investigative scenarios

2. Advanced File Analysis

The tool offers sophisticated capabilities for file analysis, including the recovery of deleted files, examination of file metadata, and identification of hidden or encrypted data. This allows investigators to uncover critical information that might otherwise remain hidden.

3. Search and Filtering

Encase features powerful keyword search and filtering options that help investigators quickly locate relevant information within large datasets. This speeds up the investigative process significantly.

4. Timeline Analysis

The software includes timeline analysis tools that allow users to reconstruct sequences of events based on digital evidence, which is essential for understanding the context and chronology of incidents.

5. Comprehensive Reporting

Encase generates detailed reports documenting findings, analysis processes, and the chain of custody for evidence. These reports are crucial for legal proceedings and ensure compliance with judicial standards

1.1.2 Application Areas of Encase professional

Encase Professional has got multi-sectoral and cross-sectoral application as stated by (Kang & Wei, 2008) the following are application areas:

Law Enforcement: It assists in investigating cybercrimes, financial fraud, and other digital offenses.

Corporate Investigations: Organizations utilize it to uncover insider threats, misconduct, and compliance violations.

Legal Proceedings: The software's reports serve as vital evidence in court cases.

Incident Response: During cybersecurity incidents, Encase helps identify breaches and mitigate risks

1.1.3 Key Mechanisms for Integrity Assurance

EnCase ensures the integrity of digital evidence through a combination of secure data acquisition methods, hashing techniques, and adherence to best practices in forensic investigations (Ieong, 2006).

1. Forensically Sound Data Acquisition

EnCase creates an exact binary duplicate of the original storage media, ensuring that the evidence is preserved in its original state. This process prevents any alteration of the original data during acquisition.

2. Hashing Techniques

Upon creating a forensic image, EnCase generates cryptographic hash values (MD5 and SHA-1) for the extracted data. These hashes serve as unique fingerprints for the data, allowing investigators to verify that

the evidence remains unchanged over time. If the hash values match during subsequent analyses, it confirms that the data has not been tampered with.

3. Use of Write Blockers

EnCase recommends using write-blocking hardware during evidence collection. This ensures that no changes can be made to the original media, further safeguarding its integrity during the imaging process.

4. Evidence File Formats

The software stores evidence in standardized formats like E01 and L01, which are widely accepted in legal contexts. These formats support integrity checks and are designed to maintain a reliable chain of custody.

5. Reporting and Documentation

EnCase generates comprehensive reports that document every step of the evidence handling process, including acquisition methods and hash values. This transparency is crucial for maintaining chain of custody and ensuring that evidence can be presented reliably in court

1.1.4 Potential shortcomings of EnCase professional

EnCase, while a leading digital forensic tool, has several potential shortcomings regarding the integrity of digital evidence. These issues can impact the reliability and admissibility of evidence in legal contexts (Carrier B. D., Basic Digital Forensic Investigation Concepts, 2016). They are as follows:

Lack of User Authentication

EnCase does not provide robust functionality to verify or authenticate the identity of the individual extracting the forensic image. This lack of authentication raises questions about who performed the extraction and whether they were authorized, potentially undermining the integrity of the evidence collected.

2. Vulnerability of Hashing Methods

Although EnCase uses cryptographic hashes (MD5 and SHA-1) to ensure data integrity, these methods alone are insufficient. If evidence is modified and the hashes are recalculated and stored without detection, any alterations could go unnoticed, compromising the integrity of the evidence.

3. Concerns with Metadata and Digital Certificates

The use of Message Digest Codes (MDCs) to provide integrity is also problematic, as these can be forged. Even with encryption, there remains a risk that modifications could occur without detection, raising further doubts about the authenticity of the evidence.

4. Chain of Custody Issues

EnCase lacks features that enforce strict chain of custody protocols. Proper documentation of every individual who handles the evidence is crucial; any gaps or irregularities can lead to challenges regarding the reliability of the evidence presented in court.

5. Human Error and Cognitive Bias

The effectiveness of EnCase can be compromised by human error during evidence collection and analysis. Factors such as lack of training or oversight can lead to mishandling, which may affect data integrity and reliability.

6. Limited Formal Testing and Validation

There is a noted absence of formal testing protocols for EnCase and similar tools, which makes it difficult to ascertain their reliability under various conditions. This lack of standardized testing can lead to inconsistencies in performance and results.

1.2 Magnet Axiom

Magnet Axiom is a comprehensive digital forensic tool designed to streamline the acquisition, analysis, and reporting of digital evidence from various sources (Sammons, 2012). It is particularly noted for its ability to handle data from mobile devices, cloud services, computers, and even vehicles.

1.2.1 Key Features of Magnet Axiom

1. Unified Evidence Collection

Axiom allows investigators to acquire and analyze evidence from multiple sources in a single case file. This includes data from mobile devices, cloud services (like Google and Facebook), and computers, enhancing efficiency in investigations.

2. Advanced Artifact Recovery

The tool supports recovery of over 500 artifact types, including deleted files, chat histories, and geolocation data. Its artifact-first approach helps users discover the full context of evidence, which is crucial for building cases.

3. Intuitive Analytics Tools

Axiom features several analytical tools that utilize machine learning to surface relevant evidence quickly. Tools like Magnet.AI can automatically flag potential illicit content and help identify connections between artifacts.

4. Mobile Workflows

The software integrates seamlessly with various mobile extraction tools (e.g., Magnet Graykey, Cellebrite) and provides a specialized Mobile View to facilitate easy navigation of mobile evidence for both technical and non-technical stakeholders.

5. Memory Analysis

Enhanced memory analysis capabilities allow investigators to examine live system memory and crash dumps effectively, which is vital for uncovering malicious activity that may not leave traditional traces.

6. Collaboration Features

Magnet Axiom includes functionalities that enable real-time collaboration among team members. This ensures that all stakeholders are informed throughout the investigation process, improving overall efficiency.

1.2.2 Application areas of Magnet Axiom

Magnet Axiom is utilized across various sectors:

Law Enforcement: Assists in criminal investigations by providing comprehensive data recovery and analysis.

Corporate Investigations: Helps organizations investigate internal misconduct or compliance issues.
Incident Response: Supports cybersecurity teams in identifying breaches or malicious activities

1.2.3 Key Shortcomings of Magnet Axioms

(Guarino, 2013) highlights that Magnet Axiom, while it is a powerful tool in digital forensics, has several potential shortcomings that can impact its effectiveness and reliability in investigations which are as follows:

1. Processing Speed and Resource Intensity

Users have reported that Magnet Axiom can be slow, especially when processing large datasets. The software's performance is heavily dependent on the hardware specifications, with optimal performance requiring substantial resources (e.g., 32GB RAM and multiple CPU cores) to avoid lengthy processing times. Some benchmarks indicate that processing can take several hours, which may not be practical in time-sensitive investigations.

2. Complexity of Use

The interface and workflow can be complex for users who are not well-versed in digital forensics. While it offers advanced features, the learning curve may hinder less experienced users from effectively utilizing the tool, potentially leading to oversights in evidence analysis.

3. Lack of Formal Testing Protocols

There is a noted absence of standardized, formal testing protocols to validate the accuracy and reliability of Axiom's functionalities. This lack of established error rates and testing methods raises concerns about the tool's consistency across different environments and scenarios.

4. Chain of Custody Concerns

Similar to other forensic tools, Magnet Axiom may not have robust mechanisms to enforce chain of custody protocols. Any gaps or irregularities in documentation can lead to challenges regarding the admissibility of evidence in court.

5. Limited Authentication Features

Axiom does not provide strong user authentication features to verify who is extracting and analysing data. This raises concerns about unauthorized access and the integrity of the evidence collected, as it is difficult to confirm whether the evidence was handled by an authorized individual (Alharbi, Weber-Jahnke, & Traore, 2011).

6. Dependency on Third-Party Tools

Axiom often relies on third-party tools for mobile device extraction and other specialized tasks. This dependency can complicate workflows and create potential points of failure if those tools are not compatible or fail during an investigation.

1.3 Passware Kit Forensic (PKF)

Passware Kit Forensic (PKF) is a powerful digital forensic tool designed for password recovery and decryption of encrypted files across various platforms. (Sindhu & Meshram, 2012) states that it is widely used in law enforcement and corporate investigations to access protected data efficiently.

1.3.1 Key Features of Passware Kit Forensic

1. Comprehensive Password Recovery

PKF supports the recovery of passwords for over 370 file types, including MS Office documents, PDFs, ZIP files, QuickBooks databases, and more. It employs advanced techniques like dictionary and brute-force attacks, utilizing GPU acceleration for faster processing.

2. Live Memory Analysis

The tool can analyze live memory images and hibernation files to extract encryption keys and passwords for both Windows and Mac accounts. This feature is crucial for uncovering information that may not be stored on disk.

3. Distributed Password Recovery

PKF allows for distributed password recovery across multiple computers or cloud environments (like Amazon EC2), enhancing processing speed and efficiency. Users can manage multiple agents remotely, making it scalable for larger investigations.

4. Batch Processing

The software supports batch processing, enabling users to recover passwords from multiple files simultaneously without manual intervention. This significantly reduces the time required for investigations.

5. Portable Version

A portable version of PKF can run from a USB drive, allowing investigators to perform password recovery without installing the software on the target machine. This is particularly useful in preserving the integrity of the original evidence.

6. Encryption Detection and Analysis

PKF can detect encrypted files and analyse their types, providing insights into the complexity of the encryption used. This helps investigators prioritize which files to attempt decryption on first.

1.3.2 Application areas of PKF

Passware Kit Forensic is utilized in the following fields:

Law Enforcement: Assists in criminal investigations by accessing encrypted evidence.

Corporate Investigations: Helps organizations recover sensitive data related to compliance or misconduct.
Incident Response: Supports cybersecurity teams in recovering data during breaches.

1.3.3 Key Shortcomings of Passware Kit Forensic

1. Dependency on Hardware Resources

PKF's performance heavily relies on the hardware specifications of the machine it runs on. Users may experience slow processing times if their systems do not meet the recommended requirements, particularly when handling large datasets or complex encryption types. This can delay investigations, especially in time-sensitive situations.

2. Complexity of Use

While PKF offers powerful features, its interface and functionalities can be complex for users who are not well-versed in digital forensics. The learning curve may hinder less experienced investigators from effectively utilizing the tool, potentially leading to oversights or errors during evidence analysis.

3. Lack of Formal Testing and Validation

There is a noted absence of standardized testing protocols to validate the accuracy and reliability of PKF's functionalities. This lack of established error rates raises concerns about the tool's consistency across different environments and scenarios, which is crucial for its acceptance in legal contexts.

4. Chain of Custody Concerns

Like many forensic tools, PKF may not have robust mechanisms to enforce chain of custody protocols. Any gaps or irregularities in documentation can lead to challenges regarding the admissibility of evidence in court, undermining the integrity of the investigation.

5. Limited User Authentication Features

PKF does not provide strong user authentication capabilities to verify who is extracting and analysing data. This raises concerns about unauthorized access and the integrity of the evidence collected, as it is difficult to confirm whether the evidence was handled by an authorized individual.

6. Potential for Data Loss During Recovery

While PKF excels at recovering passwords, there is always a risk that data could be lost or corrupted during the recovery process, especially if improper settings are used or if there are issues with the source files being decrypted.

7. Cost Considerations

Passware Kit Forensic can be relatively expensive compared to other forensic tools, which may limit its accessibility for smaller organizations or independent investigators. The cost may also increase with additional agents needed for distributed processing.

1.4 Falcon Neo (Disk Imager)

(Smith, Dietrich, & Choo, 2017) highlights that Falcon Neo is a high-performance digital forensic tool designed for efficient data imaging and duplication. Developed by Logicube, it is known for its speed and versatility in creating forensic copies of various storage devices while ensuring data integrity.

1.4.1 Key Features of Falcon Neo

1. High-Speed Imaging

Falcon Neo achieves impressive imaging speeds, capable of over 50 GB per minute for SATA/SSD drives and up to 90 GB per minute for PCIe-to-PCIe cloning. The Falcon-NEO2 variant surpasses these speeds, reaching up to 115 GB per minute for SAS-3 SSDs.

2. Multi-Tasking Capabilities

The device supports simultaneous imaging from multiple sources, allowing users to clone or image from up to five sources at once. This includes the ability to image and verify concurrently, significantly reducing the time required for these processes.

3. Wide Compatibility

Falcon Neo supports various formats and interfaces, including PCIe SSDs, M.2 NVMe, SATA, and USB drives. It can also handle different file systems such as NTFS, HFS+, and exFAT, making it versatile for different forensic scenarios.

4. Targeted Imaging

The tool features targeted or logical imaging capabilities that allow investigators to select specific files or directories for imaging. This functionality is useful in cases where only certain data is relevant, thus optimizing the acquisition process.

5. Network and Cloud Acquisition

Falcon Neo can capture data from network locations and cloud services like OneDrive and Google Drive. It also has the capability to capture network traffic, which is beneficial for investigations involving online activities.

6. Write-Blocked Preview

The device allows for write-blocked previews of data on source drives, enabling investigators to triage data without risking alteration of the original evidence.

7. Resume Functionality

If an imaging task is interrupted (e.g., due to power loss), Falcon Neo can resume the process without starting over, preserving efficiency in data acquisition.

1.4.2 Application Areas of Falcon Neo (Disk Imager)

Falcon Neo is utilized in various sectors as stated by (Hirwani, Pan, Stackpole, & Johnson, 2012):

Law Enforcement: Assists in criminal investigations by providing rapid access to digital evidence.

Corporate Investigations: Helps organizations recover sensitive information related to compliance or misconduct.

Cybersecurity: Supports incident response teams in capturing data during security breaches.

1.4.3 Key Shortcomings of Falcon Neo

1. Physical Durability

The construction of Falcon Neo is primarily plastic, which may not withstand heavy handling in challenging environments such as to rough conditions, limiting its practicality in certain situations.

2. User Confusion with Controls

Some users have reported confusion regarding the labelling of the device's ports, particularly distinguishing between write-protected source and read/write destination ports. Although the ports are marked, additional labelling on the top could enhance clarity and reduce the risk of user error during setup.

3. Limited Customization Options

The default naming convention for formatted drives is set to "Repository," which may not be ideal for all users. The inability to customize drive titles at the time of formatting can hinder organization and clarity in data management.

4. Speed Limitations Under Load

While Falcon Neo boasts impressive imaging speeds, some users have noted that performance can degrade when multiple tasks are running simultaneously. As the number of concurrent sessions increases, speed may be affected, which could slow down investigations that require rapid processing.

5. Complexity in Advanced Features

The advanced features, such as targeted imaging and network capture, may require a steep learning curve for less experienced users. This complexity can lead to inefficiencies or mistakes if users are not fully familiar with the tool's capabilities.

6. Potential Software Limitations

Although Falcon Neo supports various file systems and formats, there may be limitations in handling certain proprietary or less common formats that could arise during investigations. This could restrict its effectiveness in specific cases where unique data types are involved.

7. Remote Operation Concerns

While remote operation via a web interface is a feature, it may introduce vulnerabilities if not properly secured. Relying on remote access for critical forensic tasks can pose risks if appropriate security measures are not implemented.

1.5 Concept of Write Blockers (software based write blockers)

Software-based write blockers are defined by (Falayleh & Al-Karaki, 2013) as essential tools in digital forensics, designed to prevent any write operations to storage devices during data acquisition and analysis. They play a crucial role in maintaining the integrity of digital evidence by ensuring that the original data remains unaltered throughout the investigative process.

1.5.1 Key Concepts of Software-Based Write Blockers

1. Purpose and Functionality

The primary purpose of a software write blocker is to create a virtual barrier between the operating system and the storage device, intercepting and filtering commands that could modify the data on the device. This

ensures that while the forensic analyst can read data, no changes can be made to it.

2. Operation Mechanism

Software write blockers operate by monitoring Input/Output (I/O) commands sent from applications or the operating system to the storage device. They block any write commands while allowing read commands to pass through, effectively preserving the original state of the data.

3. Installation and Use

These blockers are typically installed on a forensic workstation as applications or drivers. They can be used with various types of storage devices, including hard drives, SSDs, and USB drives, making them versatile for different forensic scenarios.

4. Compliance with Standards

Software write blockers must comply with guidelines set by organizations like the National Institute of Standards and Technology (NIST), which stipulate that they should not prevent obtaining information from or about any drive while ensuring that protected drives remain unchanged.

1.5.2 Advantages of Software-Based Write Blockers

Cost-Effectiveness: They are often less expensive than hardware write blockers, making them accessible for smaller forensic teams or individual investigators.

Flexibility: Software write blockers can be used with multiple devices simultaneously without needing additional hardware.

Ease of Use: Many software solutions come with user-friendly interfaces that simplify the process of managing write protection.

1.5.3 Limitations and Considerations

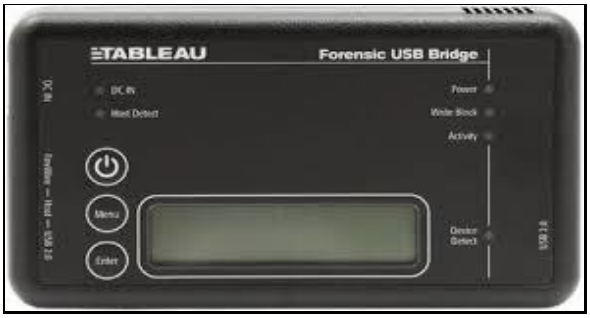
(The NoScript Firefox extension provides extra protection for Firefox, 2023) highlighted that despite their advantages, software-based write blockers have some limitations:

Reliability Concerns: The effectiveness of software write blockers can vary based on the operating system and specific configurations. If not properly configured, there is a risk of inadvertently allowing writes to the device.

Potential for System Vulnerabilities: Running software on a forensic workstation introduces risks if the system is compromised or if there are vulnerabilities in the software itself.

Compatibility Issues: Some software write blockers may not work seamlessly with all types of storage devices or file systems, which could limit their applicability in certain investigations.

1.6 Tableau USB Write Blocker



The Tableau USB Write Blocker is a specialized forensic tool designed to prevent any write operations to a storage device during data acquisition, ensuring the integrity of digital evidence. (Tobin, Le-Khac, &

Kechadi, 2016) affirms that it is particularly valuable in forensic investigations, where maintaining the original state of data is crucial.

1.6.1 Key Features of Tableau USB Write Blocker

1. High-Speed Imaging

The Tableau USB Write Blocker supports USB 3.0 connections, allowing for rapid data transfer rates of up to 340 MB per second. This speed is essential for imaging larger drives efficiently, especially in time-sensitive investigations.

2. Hardware-Based Write Blocking

Unlike software write blockers, which may be susceptible to system vulnerabilities, the Tableau device provides hardware-based write blocking. This means it physically prevents any write commands from being sent to the connected storage device, ensuring that the original data remains unaltered.

3. User-Friendly Interface

The device features an integrated LCD display that provides real-time information about the connection status, write-block status, and activity indicators through multiple LEDs. This makes it easier for forensic investigators to monitor operations during imaging.

4. Versatile Compatibility

The Tableau USB Write Blocker is compatible with various operating systems, including Windows, macOS, and most modern Linux distributions. It supports a wide range of USB mass storage devices, making it versatile for different forensic scenarios.

5. Firmware Update Capability

The device includes a firmware update feature that allows users to maintain the latest software versions easily. This ensures optimal performance and compatibility with newer devices.

6. Portability and Ease of Use

Designed for both lab and field environments, the Tableau USB Write Blocker is portable and easy to set up. Users can connect it with minimal hassle—simply plug it in, power it up, and begin imaging.

1.6.2 Application areas of tableau write blockers

Tableau USB Write Blockers are utilized in various sectors including the following:

Law Enforcement: Essential for collecting evidence without altering original data.

Corporate Investigations: Useful for recovering sensitive information while ensuring compliance with legal standards.

Cybersecurity: Supports incident response teams in capturing data during breaches without risking data integrity.

1.6.3 Key short comings of tableau write blocker

1. Physical Durability

The construction of the Tableau USB Write Blocker may not be as rugged as desired for field use. Its plastic casing could be susceptible to damage if subjected to rough handling or adverse environmental conditions, which might limit its practicality in certain investigative scenarios.

2. User Interface and Controls

Some users have reported that the labelling on the ports can be confusing, particularly when distinguishing between write-protected source and read/write destination ports. This could lead to user errors during setup

and operation, potentially compromising the integrity of evidence collection.

3. Limited Customization Options

The default naming convention for formatted drives may not meet all users' organizational needs. The inability to customize drive titles at the time of formatting can hinder effective data management and tracking during investigations.

4. Speed Limitations Under Load

While the Tableau USB Write Blocker is designed for high-speed imaging, some users have noted that performance may degrade when multiple tasks are running simultaneously. This can slow down the imaging process, which is critical in time-sensitive investigations.

5. Complexity in Advanced Features

The advanced features of the device may require a learning curve for less experienced users. This complexity can lead to inefficiencies or mistakes if users are not fully familiar with the tool's capabilities and functionalities.

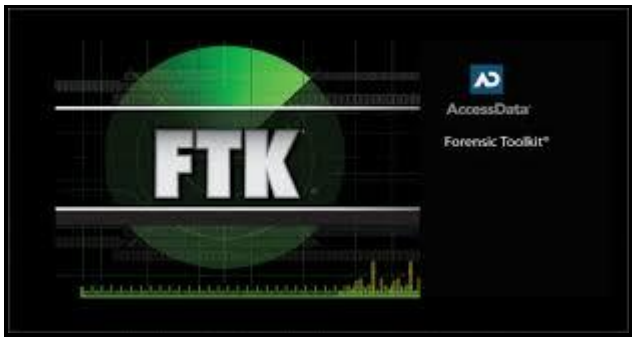
6. Compatibility Issues

Although it supports a wide range of devices, there may still be limitations in handling certain proprietary or less common formats, which could restrict its effectiveness in specific forensic cases.

7. Power Supply Dependency

The device requires an external power supply to operate, which can be an inconvenience during fieldwork where power sources may not always be available. This dependency can limit flexibility in certain situations.

1.7 FTK Imager



FTK Imager, developed by Access Data, is a widely used digital forensic tool designed for the acquisition, analysis, and preservation of digital evidence. It is particularly valued for its ability to create exact copies of data from various storage devices without altering the original content, making it essential for forensic investigations.

1.7.1 Key Features of FTK Imager

1. Forensic Imaging

FTK Imager can create forensic images of hard drives, USB drives, CDs, DVDs, and memory cards. These images are exact replicas of the original data, including file slack and unallocated space, which is crucial for maintaining the integrity of evidence during investigations. It supports multiple image formats such as E01, DD, and SMART.

2. Data Preview

The tool allows users to preview the contents of files and folders before acquisition. This feature helps

investigators identify relevant data quickly, saving time and resources by focusing on specific files or criteria like file types or dates.

3. Logical and Physical Imaging

FTK Imager can perform both logical imaging (capturing specific files and folders) and physical imaging (capturing entire drives). This flexibility enables forensic professionals to tailor their data acquisition based on the needs of each investigation.

4. RAM Capture

The tool can capture memory (RAM) from live systems, which is vital for recovering volatile data such as passwords or encryption keys that may not be stored on disk.

5. Hashing and Integrity Verification

FTK Imager generates hash values (MD5 and SHA-1) during the imaging process to verify that the copied data matches the original. This capability ensures that any analysis performed on the forensic image is reliable and that the evidence has not been tampered with.

6. Data Recovery

It includes features for recovering deleted files, even those that have been partially overwritten. FTK Imager can analyze various file systems such as NTFS, FAT, HFS+, EXT, and UFS to locate recoverable data.

7. Export Options

Users can export data from forensic images in various formats (e.g., CSV, HTML) for reporting purposes or further analysis in other forensic tools.

1.7.2 Application areas of FTK imager

FTK Imager is utilized in various sectors including the following:

Law Enforcement: Essential for collecting and preserving digital evidence in criminal investigations.

Corporate Investigations: Useful for internal audits and compliance investigations.

Cybersecurity: Assists incident response teams in capturing evidence during security breaches.

1.7.3 Key Shortcomings of FTK Imager

1. Limited Analysis Capabilities

While FTK Imager excels at imaging and data acquisition, it lacks advanced analysis features found in full forensic suites like FTK Forensic Toolkit. Users may need to transfer images to another tool for in-depth analysis, which can complicate workflows and extend investigation times.

2. No Support for Mobile Device Imaging

FTK Imager cannot directly extract data from mobile devices. Instead, it relies on third-party tools (e.g., Cellebrite, XRY) to obtain mobile data, which must then be imported into FTK for analysis. This reliance can create additional steps in the forensic process and may limit its utility in mobile forensics.

3. Resource Intensive

The tool can be resource-intensive, requiring a stable and powerful hardware configuration to function optimally. Users have reported performance issues when processing large datasets or complex file systems on less capable machines.

4. Lack of Multi-Tasking Features

FTK Imager does not support multi-tasking capabilities, meaning users can only perform one imaging or analysis task at a time. This limitation can slow down the overall investigation process, particularly when

dealing with multiple data sources.

5. No Progress Indicators

The absence of a progress bar or time estimate during imaging tasks can lead to uncertainty about how long operations will take to complete. This lack of feedback can be frustrating for users who need to manage their time effectively during investigations.

6. Steep Learning Curve for New Users

Although seasoned users find the interface user-friendly, new users may encounter a steep learning curve when first using the software. This complexity can lead to inefficiencies if users are not fully familiar with the tool's functionalities.

7. Limited Customization Options

FTK Imager offers limited options for customizing imaging settings and output formats compared to other forensic tools, which may restrict users' ability to tailor the tool to specific investigative needs.

1.8 Autopsy

Autopsy is a powerful open-source digital forensics platform that provides a graphical interface for The Sleuth Kit, a collection of command-line tools for forensic analysis. It is widely used by law enforcement, military, and corporate investigators to analyze digital evidence from various sources, including hard drives, disk images, and mobile devices (The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools, 2019).

1.8.1 Key Features of Autopsy

(Altheide, Cory; Carvey, Harlan, 2011) point different functionalities of Autopsy including the following:

1. Disk Image Analysis

Autopsy can analyze disk images in various formats, including raw (dd) and E01 formats. It allows users to examine the contents of these images without altering the original data, ensuring the integrity of the evidence.

2. Modular Architecture

The tool features a modular design that enables users to add various plugins and modules for specific tasks. This extensibility allows for tailored investigations based on the unique requirements of each case.

3. Multi-User Collaboration

Autopsy supports multi-user cases, allowing multiple examiners to collaborate on large investigations simultaneously. This feature is beneficial for complex cases that require input from several forensic experts.

4. Comprehensive Reporting

The platform includes an extensible reporting infrastructure that allows users to generate customizable

reports in formats such as HTML, PDF, and XLS. This capability is essential for documenting findings and presenting evidence in legal contexts.

5. Advanced Search Capabilities

Autopsy offers robust search functionalities, including keyword searches and regular expression pattern matching. It can also perform hash lookups against known good or bad files to filter relevant data quickly.

6. Timeline Analysis

The tool provides timeline analysis features that graphically display system events over time, helping investigators identify patterns of activity related to user behavior or potential criminal actions.

7. Web Artifacts and Registry Analysis

Autopsy can extract web activity artifacts from common browsers and analyze Windows registry files to uncover user actions and system interactions, which are critical for understanding the context of an investigation.

8. File Recovery and Carving

The software includes capabilities for recovering deleted files and performing file carving, which allows investigators to retrieve data fragments from unallocated space on a disk image.

1.8.2 Application Areas

Autopsy is a cross sectoral applicable tool of digital forensics the following are as highlighted by (Ademu, Imafidon, & Preston, 2011):

Law Enforcement: Essential for criminal investigations involving digital evidence.

Corporate Investigations: Useful for internal audits, compliance checks, and misconduct investigations.

Cybersecurity: Assists incident response teams in analysing breaches and gathering evidence.

1.8.3 Key Shortcomings of Autopsy

(Altheide, Cory; Carvey, Harlan, 2011) highlights key weaknesses of the applicability of Autopsy digital forensics tool below:

1. Limited Advanced Features

While Autopsy offers a robust set of core features, it may lack some advanced functionalities found in commercial forensic suites like EnCase or FTK. This includes comprehensive data analysis tools and integrated workflows that are often more polished in proprietary software.

2. Performance Issues with Large Data Sets

Users have reported that Autopsy can struggle with very large disk images or complex file systems, leading to slow performance or even crashes during analysis. This can hinder investigations where time is critical.

3. User Interface Complexity

Although Autopsy aims to be user-friendly, some users find the interface complex and less intuitive compared to other forensic tools. This complexity can create a steeper learning curve for new users, potentially leading to inefficiencies in investigations.

4. Incomplete Support for Certain File Types

Autopsy may not effectively handle certain file types or formats, such as embedded images within Microsoft Office documents. This limitation can result in missing critical evidence during an investigation.

5. Dependency on Additional Tools

While Autopsy is powerful on its own, it often requires integration with other tools for specific tasks, such as mobile device extraction or advanced data recovery. This reliance on additional software can complicate

workflows and increase the time needed for investigations.

6. Less Established Court Acceptance

As an open-source tool, Autopsy may not have the same level of acceptance in court as established commercial tools like EnCase and FTK. This could affect the perceived credibility of evidence collected using Autopsy in legal proceedings.

7. Limited Documentation and Support

Although there is a community around Autopsy, users may find that documentation and official support are not as extensive or responsive as those available for commercial products. This can make troubleshooting and learning the tool more challenging.

1.9 Conclusion

The above-mentioned digital forensics tools are valuable paid, subscription based and open-source tool for digital forensics. Their limitations regarding advanced features, performance with large datasets, user interface complexity, file type support, dependency on other tools, court acceptance, and documentation highlight areas that could benefit from improvement. Addressing these shortcomings can enhance overall effectiveness in digital forensic investigations.

While these tools offer valuable features for digital forensics, its shortcomings in user authentication, reliance on hashing methods, chain of custody enforcement, and formal validation processes highlight areas that need improvement. Addressing these issues is essential for enhancing the tool's credibility in legal proceedings and ensuring the integrity of digital evidence.

References

Alharbi, S., Weber-Jahnke, J. H., & Traore, I. (2011). The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review. Rundbrief Der Gi-fachgruppe 5.10 Informationssystem-architekturen, 87-100. Retrieved 10 30, 2024, from https://link.springer.com/chapter/10.1007/978-3-642-23141-4_9

2. Carrier, B. D. (2016). Basic Digital Forensic Investigation Concepts. Retrieved 10 29, 2024, from http://www.digital-evidence.org/di_basics.html
3. Carrier, B. D. (n.d.). Basic Digital Forensic Investigation Concepts. Retrieved 10 29, 2024, from http://www.digital-evidence.org/di_basics.html
4. Carrier, B. (n.d.). Open Source Digital Forensic Tools: The Legal Argument. Retrieved 10 30, 2024, from @stake Research Report: http://www.digital-evidence.org/papers/opensrc_legal.pdf
5. Digital Forensics. (n.d.). Retrieved 10 29, 2024, from Basis Technology Corp.: http://www.basistech.com/digital-forensics/
6. Falayleh, M. A., & Al-Karaki, J. (2013). ON THE SELECTION OF WRITE BLOCKERS FOR DISK ACQUISITION: A COMPARATIVE PRACTICAL STUDY. Retrieved 10 30, 2024, from http://sdiwc.net/digital-library/web-admin/upload-pdf/00000545.pdf
7. Guarino, A. (2013). Digital Forensics as a Big Data Challenge. Innovations in Systems and Software Engineering, 197-203. Retrieved 10 29, 2024, from http://studioag.pro/wp-content/uploads/2013/10/digitalforensicsbigdata.pdf
8. Hirwani, M., Pan, Y., Stackpole, B., & Johnson, D. (2012). Forensic Acquisition and Analysis of VMware Virtual Hard Disks. Retrieved 10 30, 2024, from http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1300&context=other

9. Ieong, R. S. (2006). FORZA - Digital forensics investigation framework that incorporate legal issues. Digital Investigation, 3, 29-36. Retrieved 10 29, 2024, from http://dfrws.org/sites/default/files/session-files/paper-forza_-_digital_forensics_investigation_framework_that_incorporate_legal_issues.pdf
10. Kang, X., & Wei, S. (2008). Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics. Computer Systems: Science & Engineering, 3, 926-930. Retrieved 10 29, 2024, from http://ieeexplore.ieee.org/document/4722494
11. Kumari, N. and Mohapatra, A.K., . (2016). An insight into digital forensics branches and tools. In 2016 (pp. . IEEE. International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT) 2016, March. (pp. 243-250)). India: IEEE.
12. Sammons, J. (2012). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Retrieved 10 29, 2024, from https://amazon.com/basics-digital-forensics-getting-started/dp/0128016353
13. Sindhu, K. K., & Meshram, B. B. (2012). Digital Forensics and Cyber Crime Datamining. Journal of Information Security, 3(3), 196-201. Retrieved 10 30, 2024, from http://file.scirp.org/pdf/jis20120300002_13729911.pdf
14. Smith, C., Dietrich, G. B., & Choo, K.-K. R. (2017). Identification of Forensic Artifacts in VMWare Virtualized Computing. Retrieved 10 30, 2024, from https://link.springer.com/chapter/10.1007/978-3-319-78816-6_7
15. The NoScript Firefox extension provides extra protection for Firefox, F. S.-b. (2023). The NoScript Firefox extension provides extra protection for Firefox, Flock, Seamonkey and other Mozilla-based browsers. Retrieved 10 30, 2024, from http://noscript.net/
16. Tobin, P., Le-Khac, N.-A., & Kechadi, M.-T. (2016). A lightweight software write-blocker for virtual machine forensics. Retrieved 10 30, 2024, from http://researchrepository.ucd.ie/handle/10197/8150