NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 1, June 2024
E – ISSN – 2583-7559

COMPARATIVE ANALYSIS OF COMMERCIAL AND OPEN-SOURCE DIGITAL FORENSIC TOOLS

Rajat Kumar

Ashish Singh Kuntal
CEO At Hawy Eye Forensic, Noida, Uttar Pradesh

Dr. Sachil Kumar

Assistant Professor
Amity University, Noida, Uttar Pradesh
Contact Information- E-Mail
Rajatku28489902gmail.Com
Phone No.- +91 7503201523

Abstract: ***Research into the capabilities and accuracy of computer forensics tools will increase as the number of cases and the weight of evidence based on digital evidence increases. This overview describes the capabilities of leading proprietary and open source digital forensics tools. The functionality of the tools has been tested separately on digital media formatted with Windows. Experiments have been conducted to determine whether open source computer forensics capabilities are similar to proprietary computer forensics tools and whether these tools can complement each other. The ability of these tools to create and analyse digital forensic images in a forensic manner has been tested. Tests were performed on each SSD media file after wiping the data from the media and repeated after formatting the media. The results of the experiments conducted show that both proprietary and open source computer forensics tools perform better in different scenarios and that the tools can be used to validate and complement each other. According to these findings, researchers have affordable tools to validate results and can study digital media more effectively.***

Keywords: Open source tools, digital forensic, data recovery, Proprietary Tools, Cybercrime.

I. INTRODUCTION

The increasing use of computers in financial transactions and personal information storage has led to a rise in cybercrime, emphasizing the importance of computer forensics. The process of gathering, handling, and presenting evidence to courts, investigations, or tribunals requires criteria to ensure admissibility. The choice between proprietary and open source tools in computer forensics has been a long-standing debate, as the accuracy of digital tools is scrutinized. The value of digital evidence is increasing, and its admissibility and weight are being assessed under common and fundamental law and IT law. This dissertation addresses this debate and explores the possibilities of both proprietary and open source tools for common computer-separated evidence artefacts [8]

Computer forensics is a scientific process that uses technology to examine digital resources and devices. Researchers must develop and prove hypotheses about events or chains of events, which can be presented as evidence to courts or investigations. Evidence includes documents, Internet activity, users, and computer-related activities. The process of identifying, extracting, preserving, and presenting evidence must be repeatable and comply with relevant laws and regulations.

II. LITERATURE REVIEW

ANALYSIS TOOLS

- *EnCase and EnCase Imager (version 22.4.0.167)*

EnCase is a digital forensic tool from Guidance Software, with version 1 released on February 20, 1998. That first version of EnCase was limited in that it could only run on Windows operating systems and could only read FAT 12/16/32 and NTFS systems. EnCase version 7.05, which is the version used in this study, is able to support multiple systems including FAT 12/16/32, NTFS, and EXT 2/3 (Digital Intelligence, 2014) [7]. EnCase can create forensic images from digital media, process and analyse acquired forensic images and generate reports. Therefore, it is a digital forensics tool that can be used by both defendants and investigators during the digital forensics investigation process (Guidance Software, 2012) [8]

- Ftk (forensic toolkit) (version 4.7.1.2)

Access Data Forensic Toolkit is a little younger than EnCase and version 1 has been in use since 2002 but now a day it is owned by Exterro. FTK version 1 was able to support FAT 12/16/32, NTFS as well as Ext 2/3 systems (Access Data, 2008) [1]. Since those early days FTK has seen a number of releases and at the time of writing this thesis, the most current version of FTK was 4.7.1.2. This research was performed using FTK version4.7.1.2, which was the most current version of the software at the time of performing the research. FTK is a comprehensive digital forensic toolkit that can be used to create, process and analyse digital forensic images. Access Data have also included a reporting function in FTK making it capable of producing all-inclusive reports (Access Data, 2011a). When installing FTK, the researcher was required to create users and assign permissions to them [25]. FTK was used to analyse the forensic images made using FTK Imager Lite. Registry viewer was further employed in the analysis of the Windows images to provide insight into the registries.

- Tableau forensic tx1(version 4.1)

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 1, June 2024
E – ISSN – 2583-7559

The Tableau TX1 is a forensic image processing device developed by Tableau, a subsidiary of technology company Opentext. It is widely used by digital forensic investigators and law enforcement agencies to create forensic copies of storage media such as hard drives, solid state drives and USB devices. It automatically detects encryption on connected devices and passes known credentials to unlock BitLocker and Opal encryption.

It provides high-speed imaging capability that enables fast data acquisition and maintains data integrity thanks to a write-lock mechanism [35]. It supports multiple interfaces, including SATA, USB and PCIe, making it versatile for different types of media.

- *Falcon NEO 2*

The Forensic Falcon NEO 2 is the next generation in digital forensics hardware for digital evidence acquisition, analysis, and processing from computers, mobile devices, and media [3]. Being a new and improved Forensic Falcon NEO, it opens up the possibility of running a long list of actions to conduct an all-round investigation in the digital space. Equipped with fast capture, Forensic Falcon NEO 2 quickly extracts data from a wide array of storage devices, including SSDs, hard drives, USB drives, and memory cards. The device visualizes several artifact types and analyzes them forthwith: computers, smartphones, and tablets [20][40].

It has user-friendly interfaces complemented with intuitive controls that assist in forensic imaging and analysis of data without a fuss. Furthermore, it is also equipped with forensic analysis tools for data exploration, extraction, keyword searches, and report generation. In terms of security and integrity, the Forensic Falcon NEO 2 protects the data at each instance of collection and analysis and maintains the chain of custody of evidence. Its scalability empowers it with the potential to deal with vast data, thus very appropriate for both small and extensive forensic investigations

III. TERMS AND CONCEPT

- Unallocated space

Deleting data actually removes the reference to the data in the file allocation table. In other words, the data may still be on the storage medium, but the operating system does not know how to access the data. Deleted data or files are hereinafter referred to as unreferenced data or files. When a computer user deletes a file in Windows 95, the operating system can target the clusters where the data resides. Until then, this "deleted" data remains in the so-called unused or unallocated file space. This space has mostly proven to contain information related to research, so it is necessary to analyze it.

- *Files slacks*

When files are created, their length varies depending on the content. DOS-, WINDOWS-, and WINDOWS-NT-based computers store files in fixed-length blocks of data called clusters. File sizes rarely exactly match the size of one or more clusters. Therefore, the unallocated storage that exists from the end of a file to the end of the last cluster for that file is called file slack. Such unallocated space should be examined because it may contain previously created and relevant evidence. Forensic tools exploit this vulnerability during investigation.

- *Computer critical scale functions*

Numerous forensic software tools offer several functions. However, the focus of this article is disk imaging and hashing. Disc imaging is an important feature because research should never be performed on the original recording medium. Therefore, disk imaging is used to protect the integrity of all media being examined. If the integrity of the recording medium is not maintained, the results of the investigation may be overturned in court, as defence attorneys may question the investigation process. Hashes and hash functions then become important because they ensure that the imaged device is indeed the same as the original. These two functions are expanded upon in the following sections.

- *Disk Image*

Usually, the first goal of CFS is to create an image of the storage device under study. This image is and should be an exact copy of the original recording medium. Before that, it is very important to immediately disconnect the suspect/owner from the computer. If this is not done, the suspect may be able to run a process on the target machine that overwrites the contents of the storage device.

A disk image can be defined formally as a physical sector-specific copy of a storage medium and compression of the image into a file for forensic purposes. Further, imaging tools also contain an internal verification mechanism to show that the copy is authentic and has not been tampered with. The image does not need the same geometry as the original storage device. This is because the geometry can be simulated when the acquired image needs to be processed. In computer forensics, the priority and focus is accuracy, integrity of evidence and security.

As such, the National Institute of Standards and Technology (NIST) provides some guidance on how table mapping should occur. They recommend that:

1) The tool should make a copy or image of the bit stream from the original disk or partition.
2) The tool must not modify the original disk.
3) The tool should be able to verify the integrity of the disk image file.
4) The tool should log I/O errors.
5) Tool documentation must be correct.

- *Hashing Functions*

A hash function is a process represented by the symbol H. The process transforms an input M to a fixed-size string. That fixed-size string is called a hash value, and H is used as the notation for the output of the hashing function from the input M. Hash functions form the basis of the internal verification mechanism used by forensic tools to ensure the integrity of the original media and the resulting image file. Message Digest 5 and the Secure Hash Algorithm are the most commonly used hashing algorithms so far and these will be explained in the next two sections.

- *Message Digest 5 (MD5)*

MD5 was created by MIT Professor Ronald L. Rivest. The algorithm ensures integrity of a file image as the hash value or 128-bit message digest of an image file is made. The message digest, it is said, is like a fingerprint for an image file: unique to a person, as unique as a fingerprint for a human being. It is, according to the Internet Engineering Task Force, "computational infeasible" for any two data inputs to have the same message digest. The author of MD5 also claims, "it is conjectured that the difficulty of coming up with two messages having the same message digest is in the order of 264 operations, and that the hardness of finding any message with a given message digest is in the order of 2128 operations". These guarantees make MD5 a reliable hashing function.

- *Secure Hash Algorithm (SHA) 1*

This is the second widely used hashing algorithm today. The algorithm is based on principles similar to those used in the design of MD4, the predecessor to MD5. It produces a 160-bit message digest when an image file of size less than 264 bits is given as input to the algorithm. The SHA1 is dubbed secure because, like its MD5 counterpart, the algorithm is computationally impractical to determine data from a given message digest, or to ascertain two different data files which produce a like message digest.

IV. METHODOLOGY

- **PREPARATION OF HARDWARE FOR FTK AND ENCASE**

Autopsy V4.7.1 was downloaded from exterro.com and installed on a HP Pavilion laptop computer with the following specifications

Processor: Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz
RAM: 16.0 GB (15.9 GB usable)
Hard Disk Drive: SSD (Model- FM512GDJTNI-82A0A) of 476.94 GB
Operating System: window11 home 64-bit operating system, x64-based processor

- **PREPARATION OF SOURCE MEDIA**

We have to create the artefacts on the Pen drive for the imaging, Pen drive with the following specifications

Model: Kingston DataTraveler G3
Serial number: G320CF302E25F1FE219C0A275B
Capacity: 7.21GB
Block Size: 512
File system: 512 FAT32

- **PREPARATION OF DESTINATION DRIVE**

We have use a hard drive for storing the images created by using the forensic tools for analysis, hard drive with the following specification

Model: HFM512GDJTNI-82A0A
Serial number: WXF2A11LBX12
Capacity: 1.81TB
Block Size: 512
File system: exFAT

- **OPEN SOURCE TOOL**

Open-source forensic tools are crucial in digital software design, offering a transparent and collaborative platform for researchers, security professionals, and law enforcement agencies to extract information and evidence [12][18]. Key features include availability, transparency, community participation, modification capabilities, reliability, interoperability, and educational value. Users can download and customize tools to suit specific requirements, gaining a deeper understanding of their functionality. The open nature of these tools instills trust in their use, and their compatibility with other software enhances the effectiveness of forensic investigations [24]. Open-source forensic tools not only facilitate investigations but also serve as valuable resources for learning and skill development in digital forensics.

- **LEGAL ISSUES WITH THE OPENS SOURCE TOOLS**

Open source forensic image processing tools face legal challenges such as credibility, trustworthiness, chain of custody, admissibility, and expertise. Key challenges include the lack of formal validation by established standards bodies, questions about their effectiveness and reliability compared to commercially certified tools, and difficulties in adhering to the Daubert Standard for litigation admission [24]. Additionally, the tools lack official features to record every step of the process, making it difficult to adhere to a strict chain of custody [18]. Technical capability and expertise are also crucial for the operation and validation of open source tools in a court of law, as they do not guarantee customer support and updates. Addressing these legal challenges is crucial to establish the credibility, reliability, and neutrality of these tools.

EXAMPLE OF OPEN SOURCE IMAGING TOOLS:

- Open source imaging tools play a crucial role in digital forensics and data preservation. One such tool is **Guymager,** a powerful disk imager with a user friendly graphical interface [8]. It supports various image formats, including Raw (dd), EWF, and AFF, ensuring effective preservation and integrity control. Guymager also offers features like compression and validation, multithreading for optimized performance, and detailed device and disk image management. Additionally, it provides error handling capabilities and allows for automatic image sharing and pausing/resuming of the rendering process.
- **Partimage** is an open-source disk imager that creates and restores partitioned disk images, supporting multiple file systems like ext2, ext3, ext4, reiserfs, FAT16/32, NTFS, HFS, and JFS. It allows for compressed image files using gzip or bzip2 compression, saving disk space [16]. Partimage also supports network support, allowing users to save and restore images from network shares using protocols like NFS and SMB/CIFS. It supports incremental backups, saving time and storage space. Partimage's text-based user interface makes it user friendly and efficient for command line environments.

• ***FTK Imager***, developed by AccessData, is a forensic imager that is widely utilized in the field of digital forensics. This tool is instrumental in creating disc images, mounting and examining forensic images, and analyzing data on various media [20]. FTK Imager offers a comprehensive overview of its capabilities, providing users with a powerful tool for forensic analysis. With its advanced features and functionality, FTK Imager is a valuable asset for digital forensic investigations [7][9].

Installation

FTK Imager is available for Windows operating systems. Follow these steps to download and install FTK Imager.

Download FTK Imager:

- Visit EXTERRO FTK Imager Download Page (https://www.exterro.com/ftk product-downloads/ftk-imager-version-4-7-1)

Run the installer:

- Find the downloaded file (usually called `FTKImager.exe`) and run it.
- Follow the installation instructions to complete the installation.

Procedure of creating disk Image

Create a disk image

Run FTK imager:

- Open FTK imager from the start menu or desktop shortcut.

Create a new image:

- Go to "File" > "Create Disk Image".

Select Source:

- Select the image source type (eg physical disk, logical disk, image file).
- Select the specific device or drive you want to image.

Set destination:

- Choose where you want to save the image file.
- Select the image type (eg E01, raw) and enter a file name.

Add evidence information:

- Enter information such as case, evidence number, name of examiner, and comments if applicable

Start shooting:

- Click Start to start the shooting.
- FTK Imager creates an image file and calculates hash values for integrity.

Adding an Image

Start FTK viewer

Mount the image:

- Go to "File" > "Image mounting".
- Select an image file to attach.

EXAMPLE OF OPEN SOURCE ANALYSIS TOOLS

• One of the most commonly used open-source digital forensics platforms is Autopsy, developed by Basis Technology (Autopsy.com). It offers a graphical interface for The Sleuth Kit, which is a set of tools for conducting forensic analysis from the command-line environment [1].

Autopsy is a powerful tool used by police, military, corporate investigators, and academic researchers for forensic analysis of digital devices [17]. Its graphical interface allows for easy data analysis, including disk images and local drives, searching through keywords, file analysis, and timeline analysis. It also features hash set filtering for identifying known good or bad files, file carving for recovering files from unallocated space, email analysis, web and email analysis artifacts, and customizable reporting.

To create autopsy results, follow these steps: general installation, case creation, data sources addition, data processing and analysis, major findings commenting and bookmarking, report details commenting, and verification and validation of findings for clarity and conciseness. Autopsy is a great tool for complete documentation that conforms to the legal process in digital forensics research.

COMMERCIAL IMAGING TOOLS

Commercial forensic imaging tools are special software and hardware solutions used within the forensic field to collect, analyze, and interpret digital evidence emerging from different resources. These tools play a crucial part to enable forensic professionals in collecting, storing, and examining data in a way that their integrity is maintained for legal proceeding.

LEGAL ASPECT OF COMMERCIAL TOOL

Commercial forensic imagers provide legal advantages over open-source tools, such as better reliability, support, and ease of use. They are tested and certified against industry standards, ensuring precision and acceptance by courts [26] [24]. They have built-in functions, vendor-specific technical support, frequent software updates, expert opinions, user training, and certification programs. Quality assurance from vendors is crucial, and peer reviews and independent validations reduce disputes [25]. Vendor liability ensures tool reliability and credibility, leading to greater oversight and higher standards in maintenance and enhancement. Overall, commercial forensic imagers offer numerous benefits over open-source alternatives.

COMMERCIAL TOOL EXAMPLE:

• Encase is a forensic digital analysis tool developed by Guidance Software, now part of OpenText, for examining data on computers, mobile devices, and digital evidence(OPenText.com). It substantiates data integrity by creating incremental copies of media through data acquisition features [8]. EnCase offers functions for data analysis, searching for specific files, keywords, and patterns, and recovering deleted files or partitions. It excels at file carving and can assist in file recovery from data broken into multiple pieces. The tool's strong reporting capability allows researchers to compile comprehensive reports of findings. EnCase supports mobile forensics and network and cloud forensics.

• Falcon Neo is a digital forensic tool developed by Digital Intelligence that combines hardware and software to extract, store, and analyze data from various digital sources. Its fast data acquisition capabilities, including high-speed imaging of

hard drives and SSDs, allow for automation of tasks and faster data collection. Falcon Neo also features a Write Only Image function to maintain index integrity [27]. It can produce various forensic image formats, including E01, Ex01, and raw (dd) formats, and supports data encryption. It also supports mobile devices, allowing recovery on iOS and Android platforms. Falcon Neo also enables the collection of network evidence from devices not under the researcher's control. It has a triage feature for quick assessments and prioritizes digital evidence before detailed analysis. The tool offers inbuilt analysis tools like keyword searches, detection facility, file types, and timeline analytics. Overall, Falcon Neo is a must-advanced digital forensic tool with comprehensive capabilities for investigators.

- The Tableau TX1 Forensic Imager is a next-generation device designed for high speed data collection during forensic investigations [34]. It can be used in outdoor environments without relying on a connected computer. The device offers fast imaging at up to 330 megabytes per second and supports various storage devices like SATA, SAS, USB 3.0, PCIe, and FireWire(OpenText.com).

It also features encryption features for data confidentiality and a touch screen interface for easy installation and operation. The TX1 acquires targeted files and folders instead of producing a complete forensic image and generates MD5, SHA-1, and SHA-256 hashes for data integrity. Its powerful processor and portable design make it suitable for outdoor use.

To install TX1, connect it to power and turn it on. Connect the source drive to one of the available interfaces (e.g., SATA, SAS, USB). Choose a destination drive (e.g., USB, SATA) and configure image settings using the touch screen interface. Set capture options such as image format and hash algorithms.

Start the imaging process by mounting the source and target disks and selecting "Start" or an equivalent interface. TX1 starts creating a forensic image, copies data from the source disk to the target disk, and generates a hash to ensure data integrity. Track the process on the touch screen interface, which displays information such as data copied, transfer speed, and estimated remaining time.

After the imaging process is complete, TX1 generates a report detailing procedures and hash values for data verification. Verify the image by comparing generated hash values with raw data values, using built-in control tools.

After the imaging and verification processes are completed, safely disconnect the source and destination drives.

EXAMPLE OF COMMERCIAL ANALYSER:

- Encase was originally developed by Guidance Software, a company founded in 1997 by Shawn McCreight. Guidance Software has become a leading expert in digital forensics technology, known for its EnCase product line of forensics, endpoint security and electronic information services tools [7].

In 2017, Canadian enterprise information management company OpenText acquired Leadership Software. OpenText continued to develop and support the EnCase product line by integrating it into its broader information management and information security solutions.

USING THE ENCASE FORENSIC ANALYZER:

To use EnCase, install the forensics workstation software and ensure it meets hardware and software requirements. Create a new case by entering case information, adding evidence, and specifying acquisition options. Start the data acquisition process to create a forensic image, and EnCase generates hash values to ensure data integrity [25].

Analyze the data using EnCase's tools, including file system analysis, keyword searches, and recovery of deleted files. Mark and bookmark important files and objects for research, adding notes and comments for documentation purposes. Build a timeline of user actions to understand the sequence of events.

Generate detailed reports of findings using EnCase's reporting feature, including file analysis, keyword search results, and timeline. Export the reports in various formats like HTML, PDF, or Excel. Validate findings by comparing them with other evidence and using hash values to ensure data integrity (Qucik, Daren and Kim-Kwang Raymond manchoo, vol.35,2010 pp.62-74). Provide clear and concise presentations of findings, ensuring documentation is complete and meets legal process requirements.

IMAGING OF DRIVE BY COMMERCIAL TOOL

- Tableau TX1 is a forensic imager developed by Tableau, a subsidiary of Guidance Software, now part of OpenText. It is designed for fast and reliable forensic data collection. The TX1 is a standalone device that does not require a connected computer to operate, making it convenient to use outdoors [39] [10] [8] .

Fast Imaging:
Capable of high-speed forensic imaging and supports data transfer speeds up to 330MB/s.
Multiple Source and Target Interface:
Supports multiple interfaces including SATA, SAS, USB 3.0, PCIe and FireWire, enabling flexible data collection from multiple storage devices.
Simultaneous Imaging:
Capable of performing multiple imaging operations simultaneously, increasing the efficiency of the data collection process.
Encryption:
Supports encrypted drives and can encrypt forensic images for secure storage and transmission.
Touch Screen Interface:
Equipped with a friendly touch screen interface for easy installation and operation.
Logical Image:
Supports logical image that allows extracting specific files and folders instead of creating a full forensic image.
Hashing and Verification:
Automatically generates MD5, SHA-1 and SHA-256 hashes during rendering to ensure data integrity.
Efficient Processing:

Equipped with a powerful processor that efficiently solves complex imaging tasks.
Portability:
Designed to be portable, making it suitable for outdoor use.
Generating a disk image with Tableau TX1:
Install TX1:
- Connect the source drive (the drive you want to image) to one of the available source interfaces (eg SATA, SAS, USB).
Choose a destination:
- Connect the destination drive (where the forensic image is stored) to one of the available destination interfaces (eg USB, SATA).
Configure Image Settings:
- Use the touch screen interface to navigate menu options.
- Select "Duplicate" or similar from the main menu.
- Set capture options such as image format (eg E01, dd), hash algorithms (MD5, SHA-1, SHA-256) and other relevant settings.
Start the imaging process:
- Mount the source and target disks.
- Select "Start" or an equivalent touch screen interface to start the image processing process.
- TX1 starts creating a forensic image, copies data from the source disk to the target disk, and generates a hash to ensure data integrity.
Track the Process:
- Track the progress on the touch screen interface. The TX1 displays information such as the amount of data copied, the transfer speed, and the estimated remaining time.
- When the image processing process is complete, TX1 generates a report detailing the procedures, including hash values for data verification.
Verify the Image:
- Once the imaging process is complete, you can verify the integrity of the forensic image by comparing the generated hash values with the raw data values.
- TX1 includes built-in control tools to help with this process.
Disconnect Safely:
- After the imaging and verification processes are completed, safely disconnect the source and destination drives

ANALYSIS OF IMAGES CREATED BY OPEN SOURCE TOOL

• Using Autopsy for digital forensic analysis involves a series of steps that help investigators examine, extract, and interpret digital evidence from various types of storage media. Here's a detailed guide on how to conduct an analysis with Autopsy:
Creating a New Case
Start Autopsy: Launch Autopsy and select "Create New Case."
Enter Case Details: Provide a name for the case, case number, and a brief description. Specify the base directory where case files will be stored.
Ingesting Data
Add Data Source: Choose the type of data source you want to analyze (disk image, local drive, logical files, etc.). Common formats include E01, dd, raw, and VHD.
Configure Ingest Modules: Select the ingest modules you want to run. These modules perform various types of analysis, such as extracting files, keyword searches, and web artifact analysis.
File System Analysis
Browse File Systems: Autopsy provides a hierarchical view of the file system. Navigate through folders and files to understand the structure and locate key files.
File Metadata: Examine metadata of individual files, including creation date, modification date, access date, and file attributes.
Keyword Search
Define Keywords: Enter specific keywords related to your investigation. These could be names, phrases, email addresses, or any other relevant terms.
Run Searches: Autopsy will search through the entire data set for occurrences of these keywords. The results will be displayed in an organized manner.
Web Artifact Recovery
Browser Data: Use modules designed to extract data from web browsers. This can include browsing history, cookies, cache, bookmarks, and download history.
Web Mail Analysis: If applicable, analyze web-based email accounts for communications relevant to the investigation.
File Carving and Recovery
Deleted Files: Utilize file carving techniques to recover deleted files. Autopsy can reconstruct files from fragments found in unallocated space.
Carving Results: Examine the carved files to identify useful evidence.
Generating Reports
Report Configuration: Configure the report to include the relevant findings, such as recovered files, keyword search results, web artifacts, and email data.
Export Options: Autopsy allows exporting reports in various formats, including HTML, PDF, and Excel, making it easy to present the findings in a court or to other stakeholders.

COMMERCIAL ANALYSER

OpenText's EnCase Forensic is one of the leading tools in this realm, aimed at enabling digital investigators to perform their examinations by means of digital forensic analysis, acquisition, and reporting on digital evidence. EnCase Forensic is known as one of the best and most widely used solutions among law enforcement, corporate investigators, and the cybersecurity community, because of several robust features that it offers. This guide elaborates on how one can conduct an analysis using EnCase Forensic [8].
Creating a New Case
Start EnCase: Launch the EnCase Forensic application.
Case Creation Wizard: Use the Case Creation Wizard to create a new case. Enter the case details, including the case name, examiner's name, and case number.
Case Directory: Specify the directory where case files will be stored.
File System Analysis

Examine File Systems: Browse the file systems of the acquired evidence. EnCase provides a detailed view of the directory structure and file contents.
File Metadata: Analyze metadata associated with files and folders, such as creation, modification, and access times.
Keyword Search
Search Terms: Define a list of keywords relevant to the investigation.
Search Execution: Perform searches across the entire dataset or specific areas. EnCase allows for advanced search options including GREP and boolean operators.
Review Results: Examine the search results to identify relevant files and artifacts.
Email Analysis
Email Evidence: Import and analyze email archives from clients like Outlook (PST/OST), Lotus Notes, and web-based emails.
Email Metadata: Review metadata such as sender, recipient, subject, and timestamps.
Attachments: Extract and analyze attachments for further evidence.
File Carving and Recovery
Deleted Files: Use file carving techniques to recover deleted files from unallocated space.
File Signatures: EnCase uses file signatures to identify and reconstruct fragmented files.

V. RESULTS

We used all four tools for imaging as well as analysis purposes for our review. We find that there are many limitations to the open source tools, and they are not able to do all the functions in comparison to the commercial tools, and these tools can also provide access to others, which plays a crucial role in the admissibility of the evidence in the court of law, whereas commercial tools have high admissibility in the court of law and also provide more function and features than the open source tools. As in the open source analyzer, we are not able to open all the files, videos, and images, but in the commercial analyzer, we were able to. And open source can only support a few file extensions, but commercial tools were able to run all the file extensions. As we added all types of files to our evidence and also performed the same analysis on the imaged file, we also found that in the pen source tool, the files were shown in an image format other than a file, or we were not able to see the context of some files as their pictures were present only during the analysis. In Encase, we were able to see the files properly and also the context of the file.

VI. DISCUSSION

Tableau TX1 is a dedicated hardware that offers several advantages over the FTK Imager. Its rendering speed is faster, allowing it to be used in open environments without connecting to another computer. The TX1 has an easy-to-use touch-screen interface, making it suitable for people with little to no technical expertise. It also has multitasking capabilities, such as simultaneous shooting, hashing, and checking tasks, making investigations easier. Its wide port diversity supports various storage devices, ensuring data integrity. TX1's proprietary hardware ensures reliable performance, minimizing software conflicts. The device works independently of the computer system, minimizing software conflicts. TX1 is designed to handle harsh field conditions and is highly appreciated in various climates and environments for forensic inspections. Its versatile power options, including standard power supplies and portable sources, make it ideal for a wide range of work settings.
EnCase Forensic and Autopsy represent the two major digital forensic tools available, each with different strengths targeted at different users and uses cases. EnCase Forensic has a professional UI with an integrated workflow process, advanced analysis tools, and automated analysis. It also offers better imaging and acquisition options, thus able to remotely acquire evidence. Data management and scalability in large-scale investigation use cases are some of its key design considerations. It supports advanced file-carving and recovery methods with the aid of file signature analysis. This tool also has EnCase custom reports and audit trails so that one can take care of the chain of custody and integrity of evidence. It also provides professional support with a large user community. However, due to its advanced features, EnCase may have a steeper learning curve compared to Autopsy. In summary, EnCase Forensic is a multifaceted tool for effective professional digital forensic investigations; however, such use needs to be determined by the specific aims, budget, and expertise of an investigative team.

VII. CONCLUSION

The choice between commercial and open-source tools for imaging forensic digital data analysis depends on the case's specific needs, budget constraints, and forensic team expertise. Commercial tools like EnCase Forensic offer professional support and scalability, but are expensive and have a steeper learning curve. Open-source tools like Autopsy are suitable for small organizations, academics, or individuals but may struggle with large datasets or complex investigations. Commercial tools are considered superior due to advanced support, features, reliable performance, and compliance with industry standards and legal requirements.

FIGURES

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 1, June 2024
E – ISSN – 2583-7559

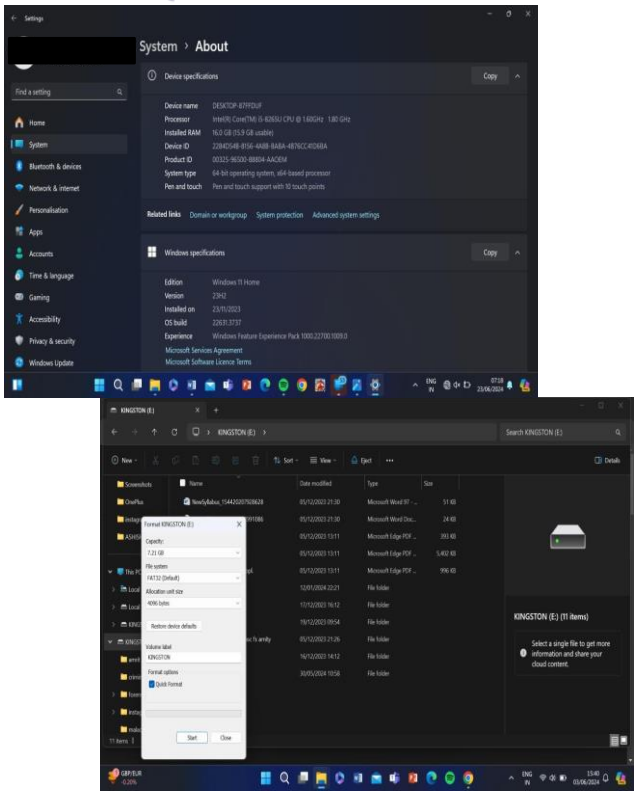

Figure 1: computer description.

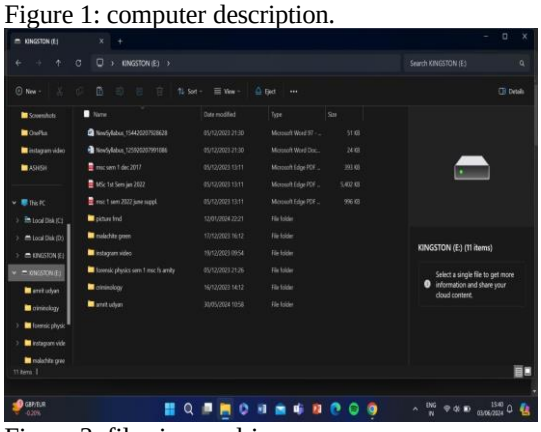

Figure 3: files in pen drive.

Figure 4: Logo of FTK imager by Exterro

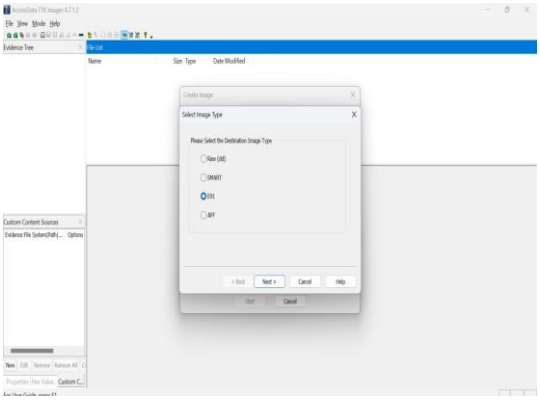

Figure 5: Image type of FTK Imager

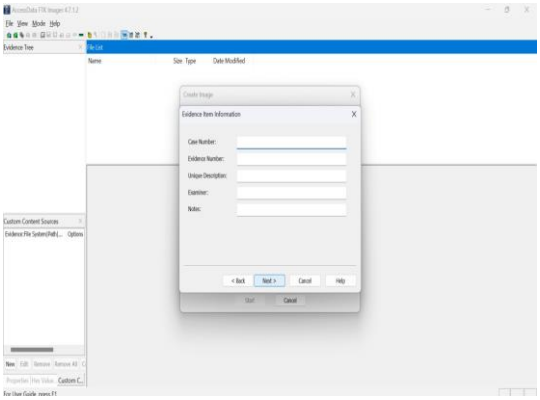

Figure 6: Case information bar

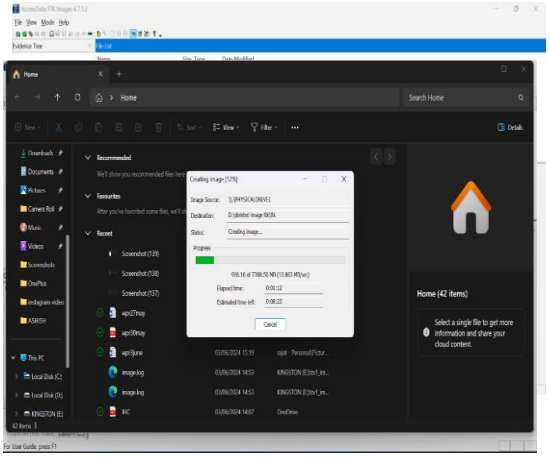

Figure 7: Destination of disk image

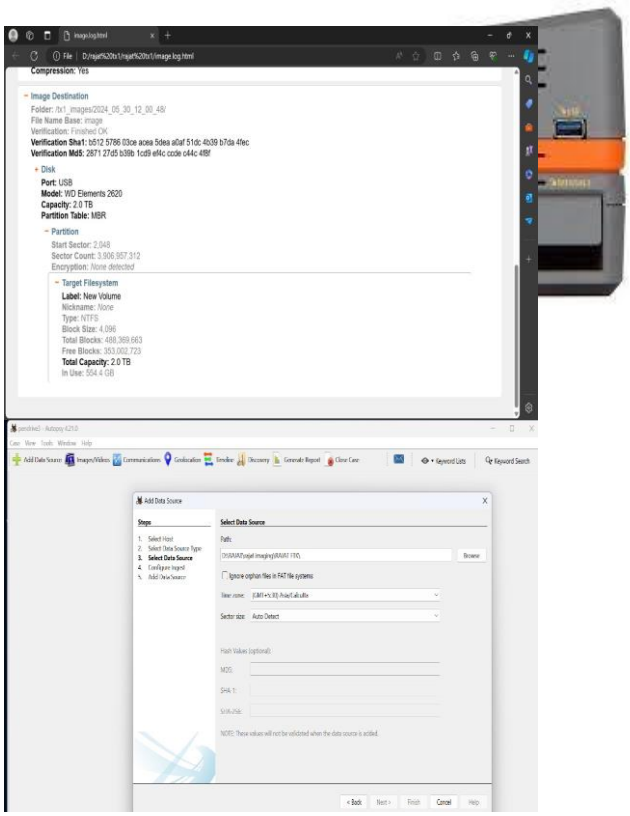

Figure 8: FTK imager processing interphase

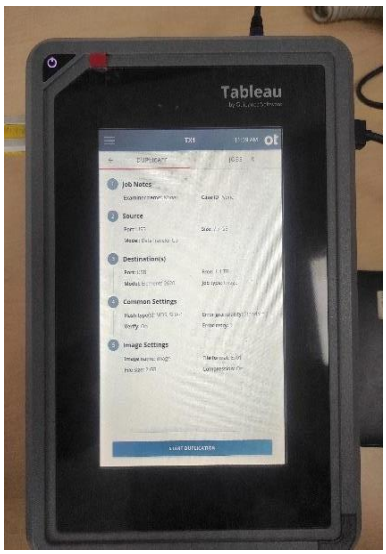

Figure 9: Tableau TX1

Figure 10: Destination side of TX1

Figure 11: Created disk image information by TX1

Figure 12: Uploading disk image interphase in Autopsy

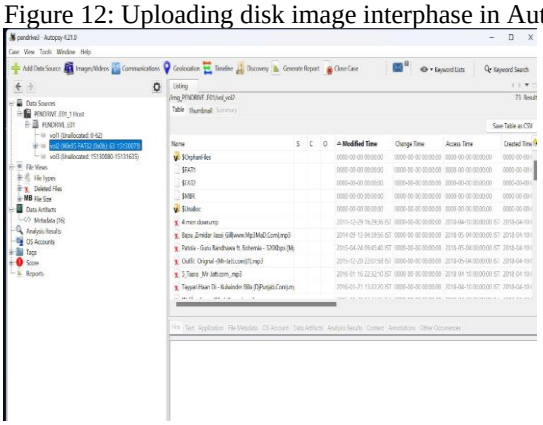

Figure 13: View of created image details and files in Autopsy

REFERENCE

[1] Hidayat, Arif. "Comparative Analysis of Applications OSforensics, GetDataBack, Genius, and Diskdigger on Digital Data Recovery in the Computer Device." International Journal of Engineering & Technology, vol. 7, 2018, pp. 445–448. DOI: 10.14419/ijet.v7i4.7.27356.

[2] Singh, Vinay, et al. "Efficacy of Open Source Tools for Recovery of Unconventionally Deleted Data for Forensic Consideration." Journal of Information Security and Applications, 2015.

[3] Lovanshi, Mayank, and Pratosh Bansal. "Comparative Study of Digital Forensic Tools." Advances in Intelligent Systems and Computing, Springer, 2019. DOI: 10.1007/978-981-13-6351-1_15.

[4] Abdillah, Muhammad, and Yudi Prayudi. "Data Recovery Comparative Analysis using Open-Source Forensic Tools on Linux." International Journal of Advanced Computer Science and Applications, vol. 13, 2022, pp. 633–639. DOI: 10.14569/IJACSA.2022.0130975.

[5] Eka Pratama, I Putu Agus. "Computer Forensic Using Photorec for Secure Data Recovery Between Storage Media: A Proof of Concept." International Journal of Science, Technology & Management, vol. 2, 2021, pp. 1189–1196. DOI: 10.46729/ijstm.v2i4.256.

[6] Ghazinour, Kambiz, et al. "A Study on Digital Forensic Tools." Proceedings of IEEE International Conference on Power, Control, Signals, and Instrumentation Engineering, 2017, pp. 3136–3142. DOI: 10.1109/ICPCSI.2017.8392304.

[7] Hamad, Noura, and Derar Eleyan. "Digital Forensics Tools Used in Cybercrime Investigation: Comparative Analysis." Journal of Emerging Technologies and Applications in IT, 2022. DOI: 10.37896/JXAT14.04/314909.

[8] Garfinkel, Simson. "Digital Forensics Tool Testing: Open Source versus Commercial Tools." Digital Investigation, vol. 8, 2011, pp. 68–72.

[9] Casey, Eoghan. "Error, Uncertainty, and Loss in Digital Evidence." International Journal of Digital Evidence, vol. 1, 2002, pp. 1–45.

[10] Roussev, Vassil, et al. "Efficient Data Recovery in Digital Forensics." ACM Transactions on Information and System Security, vol. 13, 2010, pp. 1–30.

[11] Quick, Darren, and Kim-Kwang Raymond Choo. "Data Reduction and Data Mining Framework for Digital Forensic Evidence: Storage, Intelligence, and Challenges." Future Generation Computer Systems, vol. 35, 2014, pp. 62–74.

[12] Perumal, S., et al. "Digital Forensics: Open Source versus Commercial Tools." Journal of Digital Forensics, Security and Law, vol. 6, 2011, pp. 35–42.

[13] Parsonage, Tim. "Evaluation of Disk Imaging Tools." Forensic Science International, vol. 167, 2007, pp. 61–65.

[14] Arora, Anuja, and Rajeev Gupta. "A Comparative Study of Tools for Digital Evidence Acquisition." International Journal of Computer Applications, vol. 131, 2015, pp. 5–10.

[15] Ilyas, Muhammad, et al. "Performance Evaluation of Open Source Digital Forensic Tools." Journal of Digital Forensics, Security and Law, vol. 9, 2014, pp. 31–41.

[16] Beebe, Nicole L., and Jan G. Clark. "Digital Forensic Practices: A Study of Professional and Open Source Tools." Digital Investigation, vol. 6, 2010, pp. 5–13.

[17] Carrier, Brian. "Open Source Digital Forensics Tools: The Legal Argument." Journal of Digital Forensics Practice, vol. 1, 2007, pp. 15–27.

[18] Kaur, Amanpreet, et al. "Comparative Study of Various Open-Source and Commercial Digital Forensic Tools." Journal of Information Security and Cybercrimes Research, vol. 5, 2020.

[19] Vacca, John R. Computer and Information Security Handbook. Morgan Kaufmann, 2013.

[20] logickar, Swapnil, et al. "Digital Forensic Tools for Imaging and Analysis." International Journal of Advanced Research in Computer and Communication Engineering, vol. 6, 2017, pp. 295–299.

[21] Bhardwaj, Ramesh. "Evaluation of Open Source Digital Forensic Tools for Windows System Forensic Analysis." International Journal of Computer Science and Engineering, vol. 5, 2013.

[22] Kumar, Vivek, et al. "Data Recovery Using Forensic Tools: A Case Study." International Journal of Engineering Research & Technology, vol. 7, 2018.

[23] Rehman, Saif Ur, et al. "Performance and Limitations of Commercial Digital Forensic Tools." Journal of Network and Computer Applications, vol. 36, 2013.

[24] Robertson, Bill. "Data Recovery Challenges in Open Source Forensic Tools." Digital Investigation, vol. 15, 2016, pp. 101–109.

[25] Ahmed, Noor. "Testing and Evaluation of FTK and EnCase Tools for Digital Forensic Analysis." International Journal of Cyber Criminology, vol. 4, 2014.

[26] Seifert, Charles. "Disk Imaging in Forensic Investigations: Analysis of Free vs Paid Tools." IEEE Conference on Security and Privacy, 2015.

[27] Prabhu, R., et al. "Forensic Disk Imaging: Comparison of Hardware and Software-Based Approaches." ACM Digital Library, 2019.

[28] Srinivasan, Deepa. "File Recovery Challenges Using Autopsy and EnCase." Digital Forensics Research Workshop Proceedings, 2018.

[29] Bourne, Rupert, et al. "Open Source vs. Commercial Tools: Efficiency in Forensic Investigations." Forensic Science Review, vol. 11, 2015.

[30] Matthews, Aaron. "File System Analysis with Commercial and Open Source Tools." Journal of Forensic Science, vol. 62, 2017.

[31] Lee, Henry. "The Role of Open Source Tools in Digital Forensics." International Conference on Information Security and Cryptology, 2018.

[32] Patel, Vaishali. "Benchmarking FTK Imager and Autopsy for Data Recovery." International Journal of Advanced Computer Science and Applications, vol. 8, 2019.

[33] Garner, Blaise. "Open Source vs. Proprietary Tools in Digital Forensics." IEEE Forensic Science International, vol. 16, 2018.

[34] Wright, Scott. "Digital Forensics in

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 1, June 2024
E – ISSN – 2583-7559

Cybercrime Investigations." Journal of Law and Technology, vol. 22, 2016.

[35] Watson, Derek. "Analysis of EnCase and Tableau Forensic Imagers." Digital Investigation, vol. 14, 2017.

[36] https://www.exterro.com/digital-forensics-software/ftk-imager

[37] https://www.autopsy.com/

[38] https://www.opentext.com/products/encase-forensic

[39] https://www.opentext.com/products/tableau-tx1-forensic-imager

[40] https://www.logicube.com/shop/forensic-falcon-neo2/