

**Concordia Institute for Information Systems Engineering (CIISE)**

INSE 6610 Cybercrime investigation

The use of software and hardware tools in cybercrime investigations: Survey and Comparison

Instructor: Professor Dr. Ivan Pustogarov  
  
Submitted to: Professor Dr. Ivan Pustogarov  
  
Submitted by:

| Team Members | Student ID |
| --- | --- |
| Mansoureh Navidpanahtoupkanl | 40221901 |
| Md. Saiduzzaman | 40256249 |
| Taufiq al din | 40217260 |
| Md. Aminul Islam | 40203451 |
| Tejas Surani | 40248859 |
| Mustary Sultana Mim | 40219439 |
| Simanta Sen | 40187190 |
| Mohammad Zawad Tahmeed | 40196436 |
| Md Yeasin Arafat | 40181574 |
| Saif Manjar Ahmad | 40217056 |
| Reed Alsuwaidi | 40195502 |

* **Abstract :** The use of software and hardware tools in the field of cybercrime investigations is thoroughly surveyed and compared in this study. The study intends to investigate the typical procedures used by digital forensic specialists and law enforcement organizations to handle cybercrime cases. This study evaluates the function and efficiency of both software and hardware instruments in gathering, analyzing, and conserving digital evidence through a systematic analysis of numerous investigation scenarios. This study makes a significant contribution to a deeper understanding of the dynamic interaction between technology tools and investigation procedures in the field of cybercrime by drawing on a wide range of sources, including case studies, expert perspectives, and empirical data. The results provided insight into the crucial area's strengths, weaknesses, and changing patterns, enabling well-informed decision-making and the development of cybercrime investigation techniques.
* **Keywords :**  Cybercrime investigations, digital forensics tools (software vs hardware), evidence collection, law enforcement practices, data analysis, technological tools, case studies, investigative trends, cybersecurity, decision-making.
* **Introduction :**    
   There is no question that the rapid development of information, communication, and technology has benefited humanity because it has significantly influenced the successful conduct of business, comfortable lifestyles, and automated, streamlined operations. Therefore, as technology advances, information security suffers when it is saved or sent digitally. The quick development of digital technology has created new chances for attackers to devise novel and complex attack strategies to bypass defenses, trap targets, and bypass security measures. The involvement of digital forensics is required since the investigative process and diversity of tools provide an efficient way to extract evidence as well as a strategy to detect and protect against various cybercrimes. In order to use digital forensic methods to submit the recovered evidence in court, we must first assess it[1]. Digital forensics has been divided into a variety of groups, including computer, mobile, IoT, memory, networks, email forensics and so on. Each field has a set of resources available when a cybercrime occurs to help the investigators choose the most effective ways to obtain digital evidence from the evidence. A scientific approach of inquiry and analysis called computer forensics is used to collect evidence from digital devices, computer networks, and component parts that are appropriate for presentation in a court of law or other legal authorities. To determine precisely what occurred on a computer and who was accountable for it, a methodical investigation must be conducted while keeping a recorded chain of evidence. [2]

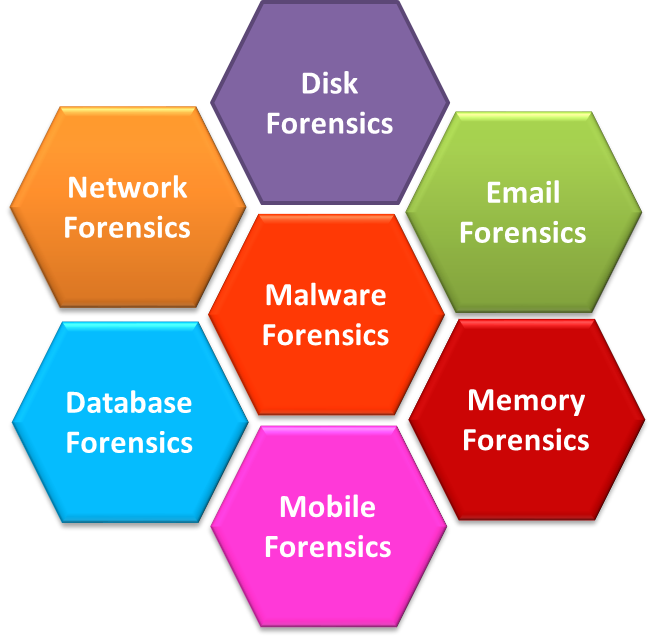
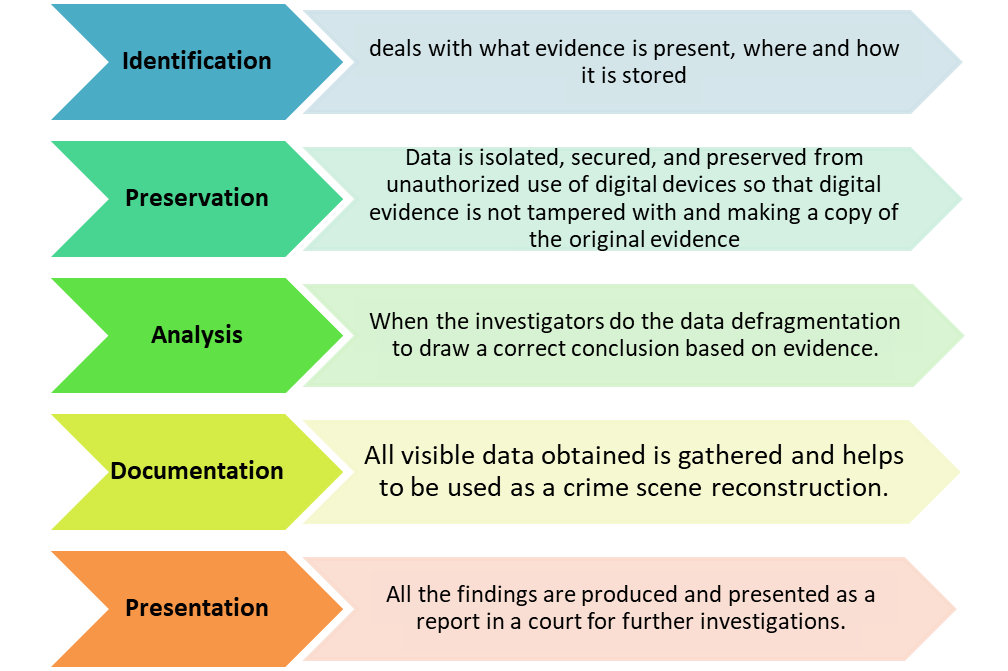


Fig- 1.0 : Areas of DigitalForensics The majority of digital forensics includes below mentioned areas

| **Digital Forensic Areas** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Disk** | **Network** | **Database** | **Malware** | **Email** | **Memory** | **Mobile** |
| extracts raw data such as active, modified, or deleted files from the storage of the device | involves monitoring and analyzing the computer network traffic | studies and examines databases and their metadata in a forensic perspective | identification of suspicious code to find any malware | deals with emails (and contact) and their recovery and analysis | collecting the data from system memory (system registers, cache, RAM) then analyzing it for further investigation | examination and analysis of phones and smartphones to retrieve contacts, call logs, SMS, etc |

Fig 1.1 Different Domain Based Distributed Digital forensic Areas [2]

**The digital forensic process can be divided in different phases such as below mentioned [2]:**



* **Methodology :**  The objective of this paper is to investigate software and hardware tools used in digital forensics, conduct an analysis, and compare them based on their features. We began by searching for papers that had analyzed digital forensics tools to gather information on the most commonly used ones. After carefully selecting 12 software tools and nine hardware tools, we divided them among the team members. We installed open-source software tools for further exploration, while the analysis of tools we didn't have access to was based on online descriptions, case studies, and tutorials. We have listed a description of each tool and their features categorized into the appropriate digital forensics phases.

To provide a detailed comparison, we categorized the software tools based on their domain, namely device forensics, network forensics, and memory forensics. Grouping the tools according to their domain allows us to distinguish their unique features better, as the tools operating in different domains may not have comparable features.

* **Digital Forensic Tools :**  All the tools used in digital forensic can be categorized into two major aspects. Those are
  + - **Software Forensic Analysis Tool**
    - **Hardware Forensic Analysis Tool**
* **Software Forensic Analysis Tool :**
* **Device Forensic Tools:**

Device Forensic Tools are specialized software applications or suites designed for digital forensic investigations on electronic devices such as computers, smartphones, tablets, digital cameras, and other storage media. These tools enable forensic investigators and law enforcement agencies to extract, preserve, analyze, and present digital evidence in a legally admissible manner. They play a crucial role in investigating criminal activities, data breaches, cybersecurity incidents, and other digital incidents.A brief description of some critical and widely used Device forensic analysis tools are given below -

* **FTK Imager:**  FTK Imager is a versatile and powerful tool that aids digital forensic investigators in acquiring and analyzing evidence during investigations. Its ability to create forensic images, analyze data, and generate reports makes it an essential component of digital forensic toolkits.

**Functional Features of FTK Imager :**

* **Create Disk Image**: FTK Imager to create a forensic image of the suspects storage media, such as a hard drive or USB drive. This step ensures preservation of the original evidence without any modifications.
* **Verify Disk Image Integrity:** Calculate cryptographic hash values (MD5, SHA-1, etc.) of the forensic image to verify its integrity and authenticity.
* **View Disk and File Information:** To examine the disk image's file system and view information about files, folders, and partitions.
* **Search for Keywords:** Conduct keyword searches within the disk image to find specific files or relevant information related to the investigation
* **Generate Reports:** Create comprehensive reports summarizing the findings from the disk image analysis. These reports can be used as evidence in legal proceedings ointernal reviews.

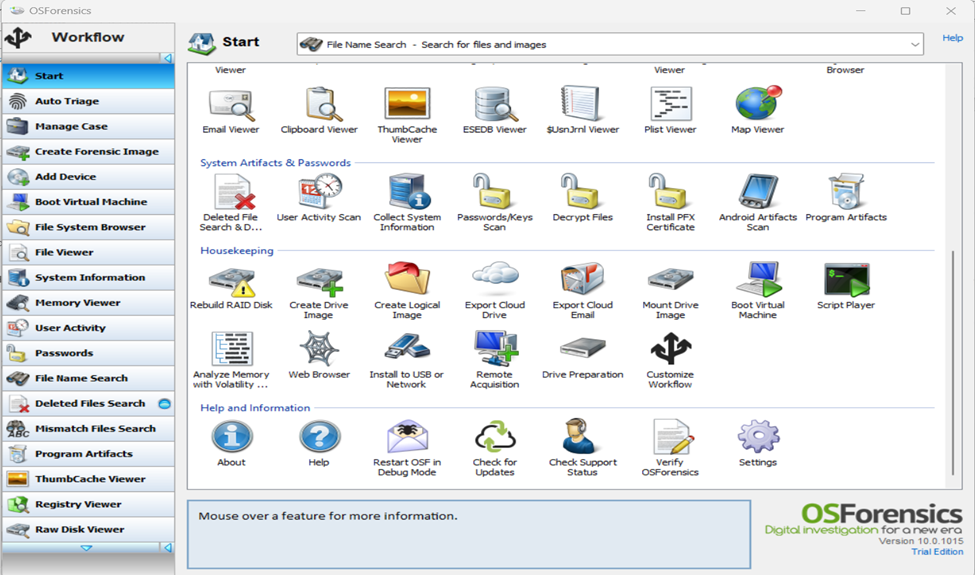
**(b) OSForensics**:  
 OSForensics is a comprehensive and versatile toolkit designed to provide deep insights into how a computer system is used and the files that are kept on it. It is an important digital forensics and investigation tool, allowing users to manage tasks, retrieve deleted data, track user activities, and generate specialised system reports. OSForensics provides a wide range of functionalities to assist in the process, whether it is for monitoring children's online activity, conducting legal investigations, or completing complete computer inspections.  
  


Fig 2.0 OSForensics Tool

**Features of OSForensics:**  
  
**=> Phase 1: Identification:**

* Identify Relevant Data: OSForensics includes extensive search features that allow users to do comprehensive searches for documents, files, and artefacts on the target system. The programme provides a variety of search parameters, such as filenames, file sizes, and timestamps, which assists investigators in quickly locating potentially valuable data. This functionality ensures that no significant piece of evidence is ignored, and investigators can exhaustively search the system for any relevant leads.
* Acquire Data for Analysis: Once relevant data has been identified, OSForensics makes it easy to acquire and collect this data for further analysis. Drive imaging is an important approach for data gathering. OSForensics enables users to make an exact and forensic-grade copy of a storage device, known as a "forensic image." This snapshot preserves the data's original condition, guaranteeing that the evidence remains untouched throughout the inquiry. The forensic image is used for analysis, lowering the danger of unintentional data change and preserving the chain of custody for legal and investigative purposes.
* Data Protection and Preservation**:**  During a digital inquiry, it is critical to maintain the integrity and security of the obtained data. OSForensics has the added benefit of being portable, as it can be installed on a USB flash drive. This capability enables investigators to work on several systems or locations while keeping evidence secure and secured. Strict protocols and best practices are followed throughout the process to ensure the integrity and trustworthiness of the evidence. Access to the obtained data is strictly regulated, and safeguards are in place to prevent tampering, whether unintentional or intentional. Investigators can maintain the integrity of the evidence and make it admissible in judicial proceedings by adhering to data security and preservation requirements.

**=> Phase 2: Preservation:**

* Discover Forensic Evidence More Quickly: With its excellent search capabilities, OSForensics is a dynamic forensic investigation application that enables users to swiftly locate pertinent files and data using filenames, file sizes, and timestamps. To investigate email files from well-known clients like Mozilla, Thunderbird, and Outlook, it provides an online search facility. The programme can recover deleted data, which is essential for locating concealed proof. It gathers information from the system and offers perceptions into user actions, system operations, and digital footprints. In addition, OSForensics has a password recovery option that can let researchers access locked or encrypted data.
* Keyword Searching and Indexing: OSForensics has advanced keyword searching and indexing capabilities. Users can construct keyword lists and search for certain terms, phrases, or patterns in the system's files and metadata. This tool is very useful for locating significant papers, identifying pertinent evidence, and connecting similar pieces of information within an investigation.
* Memory Forensics: Memory forensics capabilities are included in OSForensics, allowing users to examine a computer system's volatile memory (RAM). Memory forensics is critical for discovering ongoing programmes, open network connections, and other valuable information that normal file system analysis may not reveal. This functionality can provide critical insights into ongoing activities as well as uncover malicious programmes or hidden artifacts.

**=> Phase 3: Analysis:**

* Web Browser Analysis : The analysis of web browser artifacts such as browser history, bookmarks, cookies, and downloads is supported by OSForensics. This function provides investigators with information about users' online activity, such as their surfing habits, visited websites, and potential evidence related to online activities.
* Thumbnail and Media Analysis: The application can extract and analyze thumbnail pictures from a variety of formats, such as photographs and movies. This capability helps investigators detect potentially sensitive or illegal media content and connects media files to certain user activity.
* Email Analysis: OSForensics contains email analysis features for examining email client data and message metadata. This feature might be useful in investigations involving communication patterns, attachments, and email exchanges.
* Hash Set and File Signature Analysis: For file identification and verification, OSForensics supports hash sets and file signatures. To identify known malicious files, verify file integrity, and flag potential security hazards, investigators can compare files to established hash databases or customized hash sets.
* TimeLine Viewer: OSForensics' TimeLine Viewer allows users to visualize events and actions in a chronological order. This feature assists investigators in creating timelines, identifying patterns of behavior, and comprehending the sequence of events during an investigation.
* File Carving: OSForensics includes file carving capabilities, allowing users to recover deleted or fragmented files using file signatures and headers. This feature can be useful in reconstructing deleted papers, photos, or other data that may be pertinent to the investigation.
* Registry Analysis: The utility allows users to perform in-depth registry examination on Windows. The Windows registry includes a lot of information about system configurations, user activities, and installed software. OSForensics enables investigators to read and analyze registry hives, aiding the finding of user profiles, installed applications, recent activity, and system settings.

=> Phase 4: Documentation:

* Creating HTML case report: OSForensics is a potent forensic analysis programme with case management features that can organise and compile information from investigations. It allows investigators to produce concise, well-organized HTML case reports that highlight significant findings and supporting documentation. For legal experts and other interested parties, these reports are crucial resources that make it simpler to assess the findings and reach pertinent conclusions. Even non-technical people may successfully traverse OSForensics' capabilities thanks to its user-friendly interface.

=> Phase 5: Presentation:

* Performing Presentation: The OSForensics presentation phase entails creating HTML case reports that include a summary of the investigation's results. These papers are thorough and highlight significant findings, research findings, and pertinent data. Legal experts, law enforcement, and other stakeholders need the reports to assess the results and develop conclusions. They are made to provide information in an understandable, straightforward manner that is visually appealing. The presentation phase provides reliable data collection and convenient access to relevant data for analysis, successfully presenting the investigation's findings to all parties.

.

**(c) Foremost**: Foremost is an open-source CLI based File recovery and data carving tool, that recovers files from various data storage devices and disk images, through reading headers, footer, and data structures. Foremost is compatible with unix and linux based systems. Supports many file types (jpg, .gif, .png, .bmp, .avi, .exe, .mpg, .wav, .riff, .wmv .mov, .pdf, .ole, .doc, .zip, .rar, .htm, .cpp, and .mp4.)

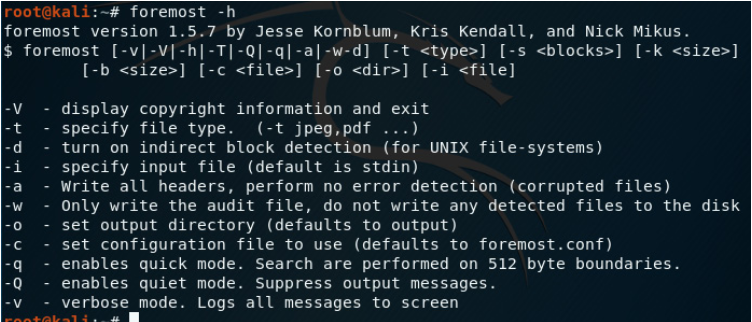


Figure # : Foremost tool interface (help options)

Functional features of foremost:

Foremost tool features can be categorized into 4 of the digital forensics features, identification, analysis, documentation, and report. Even though it does not conduct the preservation phase, it has a non intrusive feature that prevents the original evidence from being damaged.

Phase 1 - identification

* File type selection: foremost at the default setting would search for all file types. However, investigators have the option to customize the file types to expand or limit the search. Specifying file types can make searching faster than searching the entire disk.

Phase 3 - analysis

* Data carving and file recovery: this feature enables file reassembly from raw data fragments, data carving extracts data from disk even if files have been damaged. it recovers files through reading headers, footers, and data structures.
* Non-intrusive: the tools do not alter the original data; it will dump all recovered files into the specified folder. This ensures that the integrity of the evidence is not compromised.

Phase 4 - documentation

* Audit file: foremost create an output .txt file (Audit.txt) that contains information related to the findings. This file logs the details of the processing and recovery activities such as date, time, and file type.

Phase 5 - report

* Report and summary: foremost produces a summary of the statistics including the total number of recovered files with the type and the size of the files.

**(d) Autopsy** An open-source application called Autopsy, created in the Perl programming language, gives Sleuth Kit a graphical user interface based on HTML that resembles a file manager and displays information about deleted data and file system architecture. Users can retrieve the results using an HTML browser. In contrast to Lazarus, Autopsy doesn't need any prior tool execution. It may operate over image files created by the **dd** tool or directly over mounted volumes. As everything done through its interface creates Sleuth Kit commands, which are then parsed and shown again by Autopsy, it may be said that Autopsy serves as an interface for Sleuth Kit. Autopsy is easy to use; after installation, the user launches the autopsy programme, which will display the address/port that a browser can access. In an Autopsy config file, this information can be modified [11].

Functional Features of Autopsy:

In general, autopsy asks to open an existing Case or the creation of a new Case when it is being executed. To make it simpler to search for audits that a case has created, each one is maintained as a directory. Each Case must have one or more Hosts, which are subdirectories of Cases that, for instance, state that more than one machine will be audited concurrently. After that, Sleuth Kit functions are available on every menu and can be used whenever the web/gui interface makes a request [11] [12]. Autopsy tool’s features [11] [13][14] have been listed below.

* User-Friendly Interface: This is an intuitive graphical user interface designed for ease of use and accessibility. It is suitable for both novice and experienced digital forensic professionals.
* Disk Imaging and Acquisition: It can create forensic images of storage media, preserving the original data in a forensically sound manner and support for various image formats, ensuring compatibility with other forensic tools.
* Keyword Search and Filtering: It has powerful keyword and text search capabilities across acquired data. It can filter and identify relevant information quickly from large datasets.
* File Analysis and Carving: This tool can perform automatic categorization and ensure analysis of various file types, including images, documents, and more. Also, it has the ability to recover fragmented and deleted files using carving techniques.
* Artifact Analysis: It can recover and analyze artifacts like browser history, emails, chat logs, and user activity data along with gaining insights into user interactions and digital footprints.
* Metadata Examination: It can view and analyze metadata associated with files, providing valuable context to evidence. Also, it can extract information such as creation dates, modification dates, and more.
* Timeline Analysis: It can create chronological timelines based on timestamps, aiding in reconstructing events and user activities.
* Hashing and Integrity Verification: This tool can generate hash values (MD5, SHA-1, SHA-256) to verify the integrity of acquired files and compare hashes with known databases for identification of known malicious files.
* Integrated Plugins and Tools: It can perform integration with various third-party plugins and tools to extend functionality. Also, it can perform specialized tasks like analyzing SQLite databases or recovering specific data types.
* Media Playback and Viewing: This tool can preview and play multimedia files directly within the tool. Also, it can efficiently review images, videos, and audio files during analysis.
* Report Generation: It can create comprehensive reports summarizing investigation findings, methods, and conclusions by facilitating communication of results and presentation of evidence.
* Communication Analysis: It can analyze communication artifacts like emails, chat messages, and social media interactions and reveal patterns of communication and relationships.
* Automation and Scripting: It ensures automation support for streamlining repetitive tasks and workflows and, it has scripting capabilities to customize and enhance analysis processes.
* Collaboration and Shared Cases: It has the ability to share case data and collaborate with other investigators. It can enhance teamwork and knowledge sharing within forensic teams.
* Open-Source and Community Driven: It’s developed as an open-source project with contributions from the digital forensics community. So, regular updates, improvements, and a responsive user community are there.

These features collectively make the Autopsy Forensic Tool a powerful solution for digital forensic investigations. It aids professionals in examining digital evidence thoroughly, efficiently, and in accordance with forensic best practices.

**(e)** **Encase Forensic [e1]:** It is a [case management software tool](https://www.einvestigator.com/case-management-software/) developed in 1998 and is named the “Best Computer Forensic Solution” for seven consecutive years by SC Magazine. Encase is recognized globally as the standard for digital forensics and is a court-proven solution built for deep-level digital forensic investigation, powerful processing and integrated investigation workflows with flexible reporting options. It is built with a deep understanding of the digital investigation lifecycle and the importance of maintaining evidence integrity. It empowers any examiner to seamlessly complete any investigation, including investigations of mobile devices. This product is not free, and its Perpetual License allows users to pay a one-time licensing fee and a small yearly maintenance fee for access to software updates, tech support, and the forensic community portal.

Functional features of Encase Forensic:

* Data Acquisitions and Identification:It can acquire data from
  + Previewed memory or local devices such as hard drives, memory cards, or flash drives
  + Evidence files such as (.E01), and (.L01).
  + DD images, SafeBack images, VMware files (.vmdk), or Virtual PC files (.vhd)
  + Single files
  + Mobile Devices.
  + *Cloud data : by o*btaining user data *from Internet online services, such as:* Facebook, Gmail, Google Drive, Twitter, and Amazon Alex
* Examines Volume Shadow Snapshot (VSS) backups, generated by Microsoft Windows, allowing investigators to recover deleted or modified files, as well as full volumes and learn what may have taken place on a system before the investigation
* Automated Process:The evidence processor provides industry-leading processing capabilities that can automate evidence preparation, making it easier to complete an investigation. The evidence process is driven by an indexing engine that is designed for scale and performance. Use it to automate complex queries across evidence sources to save time and improve efficiency
* Image Analysis:Process images into 12 categories using visual threat intelligence technology. Examiners can quickly filter by confidence level and identify previously unidentified contraband with near-zero false positives.
* Preservation of data : Using a Write Blocker to Prevent Inadvertent or Intentional Writing
* Data encryption and decryption : It has strong decryption capabilities for products such as Dell Data Protection, Symantec, McAfee, and many more. Decryption capabilities can be further expanded with Tableau Password Recovery, a cost-effective hardware solution that is used to identify and unlock password-protected files.

This product is suitable for performing both fast triage analysis and deep full forensic analysis based on user requirement. ***This Product is not free.***

**(f) AntAnalyzer Forensic Workstation[f2]**:The AntAnalyzer is the right choice when it comes to indexing and processing IT forensic cases at the workplace. The AntAnalyzer series ,as a commercial, product is globally recognized and popular for its speed, reliability and durability.All AntAnalyzer are certified and tested for the use of the programs of the leading software manufacturers software such as [EnCase](https://www.dataexpert.eu/products/digital-forensics-opentext/encase-forensic-edition/), [FTK](https://www.dataexpert.eu/products/digital-forensics-exterro/forensic-toolkit-ftk/), [AXIOM](https://www.dataexpert.eu/products/forensic-hardware-mh-service/antanalyzer-forensic-workstation/), etc. They can be customized in detail according to customer requirements, very quiet and can be used everywhere in offices without hesitation. There is a unique [IceTray](https://mh-service.de/en/products/ice-tray/) cooling fan beneath the Tableau **T356789iu** forensic bridge and the source drives air-cooled. The aluminum cooling fins ensure the reading of the suspect drives at maximum speed without reaching damaging temperature ranges.Antanalyzer is available in AMD and [Intel edition](https://www.mh-service.de/en/products/antanalyzer/#intel) ***for Basic, Advanced, Extreme and Enterprise configuration*** .

**(g) Sleuth KIT** The Sleuth Kit is an open-source forensic toolkit for the purpose of analyzing Microsoft and UNIX file systems and disk images. The Sleuth Kit enables investigators to identify and recover evidence from images acquired during incident response or from the live systems. The Sleuth Kit is open source, which allows investigators to verify the actions of the tools or customize it to a specific need. The Sleuth Kit is developed independently from commercial and academic organizations by Brian Carrier who also develops the Autopsy Forensic Browser. The main objective of sleuth kit is to investigate files and file systems components in digital forensic investigation. The file system allows the user to analyze the file system of a computer which belongs to the suspect without being intrusive.

Functional features of Sleuth KIT:

* Data and File Recovery: The Sleuth kit can be used by the investigators to recover deleted files or files from damaged disk image.
* File System Analysis: The sleuth kit is also used in the analysis of different file systems which includes NTFS and FAT etc. It is able to provide insights into the files system structure including metadata such as file creation, modification, and access times, file attributes and paths, image, video, webpage.
* File Carving: Data Carving is a great way to find data which cannot be retrieved otherwise or shown in the file hierarchy. Data Carving is the process of extracting data from a disc image where the data is typically in the unallocated space, slack space, or even hidden inside other files. Sleuthkit supports manual carving by going to the Data Unit section and specifying the sector to start at and indicating how many sectors to carve out.
* Keyword Search: Investigators can perform keyword searches by using The Sleuth Kit within the file system or unallocated space to locate specific words, or patterns related to the investigation.
* Timeline Analysis: Sleuth kit is also used to analysis the timeline of the file activity depends on the filesystem metadata such as when the file was created, deleted or modified.
* Hash Calculation: The sleuth kit can be used to calculate hash values for example in MD5 for files in disk image to verify the file integrity.

The sleuth kit is a commad line toolset which is used in the digital forensic analysis. Along with this tool there are also user graphical interfaces (GUI) such as autopsy where investigator can easily navigate in a visual interfaces.

**Network Forensic Tools:** Network forensic investigation is an imperative process of cyber-crime investigation which involves obtaining, evaluating, categorizing, and identifying crucial evidence based on the activity involving the network devices. Network Forensic Tools (NFTs) and Network Forensic Processes (NFPs) can gather the entire network stream of traffic, allow clients to assess the network stream of traffic based on their needs, and the key components of traffic. NFTs enable aggregation of captured, gathered, and examined network traffic packets, enabling the investigator to gather information about the traffic patterns between several machines. [S1] [S2]  
  
A wide variety of security tools are provided for network forensics. Some of the tools are: Xplico, Network Miner, Tcpdump, Nmap, Omnipeek, NetDetector, NetIntercept and Wireshirk.

* Network: Wireshark/ Nmap/ Tcpdump/ Network miner/ Xplico - simanto

**(h) Xplico:** Xpplico is an open-source GUI network forensics analysis tool for unix based systems. Extract artifacts from network and internet captures. It is commonly used for HTTP, Voip, email, and network analysis. However, it can also perform MMS, DNS, Facebook, and WhatsApp chat analysis. Protocols supported: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv6

Functional features of xplico:

Xplico tool does not conduct the preservation phase so we will be categorizing its features based on identification, analysis, documentation, and report phases.

Phase 1 - identification

* Automatic decoding: it contains a decoder that can parse through the packet capture (pcap) and displays the captured web activities. Decoder uses IP decoder and decoder manager components.
* Live capture: this feature allows investigators to capture live network traffic. Investigators are able to specify the interface and filter the rules, and configure the live capture to their desired goals.

Phase 3 - analysis

* pcap analysis: supports online and offline analysis of pcap. protocols that can be investigated ( TCP, UDP, HTTP, FTP, TFTP, SIP, POP, IMAP, SMTP, and more. Traffic encrypted with SSL cannot be viewed with xplico
* Multithreading: enabling simultaneous packet or stream processing significantly improves the performance of the tool. Which allows heavy network traffic load to be handled efficiently.
* Modularity: breaking the software into modules where each module is in charge of specific tasks achieve scalability and flexibility. This feature allows investigators to tailor the tool to its needs.

Phase 4 - documentation

* Case management: this feature aids in organization of investigations. It enables categorization of cases to help keep track of different cases and the evidence related to each case.

Phase 5 - report

* Reporting: Output data and information in SQLite database or MySQL database and/or files making it easier to review, analyze, and present the data found in the investigation.
* Graphic user interface: the xplico system has a user-friendly GUI that can be viewed via a web browser, it allows for easier understanding and analysis.

Pending for Tcpdump/ Network miner

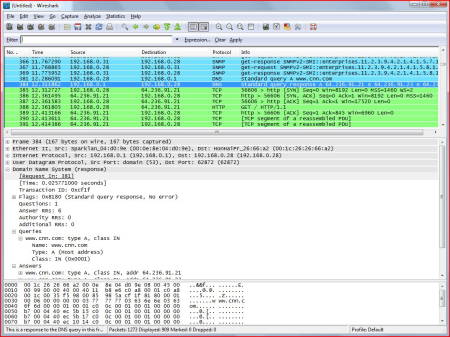
**(i) Wireshark:** Open-source network protocol analyzer Wireshark is also referred to as a "packet sniffer." It enables the collecting and examination of network traffic in real time. Formerly known as Ethereal, Wireshark can analyse traffic at many levels, delivering information ranging from connection-level data to specific packet bits. To learn about packet specifics including transmit time, source, destination, protocol type, and header data, network managers utilise this tool. For evaluating security events and resolving problems with network security devices, this information is helpful. The operating systems Windows, macOS, and Linux are all compatible with Wireshark.  
  


Fig G.1.0  
  
  
 Features of wireshark:  
  
=> Phase 1: Identification:

* Capturing network traffic and packets filtering: The network interface is configured to promiscuous mode in Wireshark at the identification step so that it can record all network packets, even those not meant for the host. To focus on packets of interest based on particular characteristics like IP addresses, protocols, or links to questionable servers, investigators employ comprehensive packet filtering in Wireshark. This filtering aids in focusing attention on essential packets for more research.
* Searching patterns and Identify unusual behaviour: Investigators in Wireshark look for specific words or patterns in the captured packet payloads during the identification stage. This aids in the identification of packets linked to malicious behaviour or attack-related instructions. Additionally, when analysing network traffic, investigators look for any odd or suspect activity, such as traffic directed at a particular location, links to known malicious IP addresses, or patterns associated with well-known attack strategies. The detection of possible threats and comprehension of the nature of the cyber incident are both aided by this pattern and behaviour analysis.
* Examining traffic patterns and file extraction: Investigators can use Wireshark to perform many types of network traffic analysis, such as following TCP streams or listening in on UDP talks. Investigators can uncover communication trends and maybe spot malicious activity by analysing traffic flows. As well Extraction of data or artefacts from the recorded network traffic may sometimes be required during the identification stage. This can entail downloading dubious files or removing email attachments for additional investigation.
* Timestamp analysis and finding relevant data: Examining the network traffic's timestamps can reveal information about the sequence of events. This aids in retracing the course of events leading up to the cyber incident. Investigators can export the pertinent data for additional research and reporting once they have located the packets of interest. Specific packets or complete conversations can be exported from Wireshark for offline examination.

=> Phase 2: Preservation

* Capture Data Non-Destructively and Store data in protected location: Wireshark makes sure that the original network traffic is not changed or altered while it is being captured. It does not alter the content of the packets when capturing them, so-called non-destructive packet capture. It is crucial to store the data in a safe and impenetrable area after capturing the network traffic. To avoid any unintentional alterations to the data, investigators typically save the collected data to a storage medium like an external hard drive or a write-protected media.
* Use Proper Data Handling Techniques and measure hash value: To ensure that the chain of custody is upheld during the preservation phase, investigators must follow proper data management protocols. Every step of the process, as well as the day, time, and details of the data collection, must be documented. Hash values (such MD5 or SHA-256) are computed for the data collected.By acting as the data's digital fingerprint, these hash values maintain its integrity throughout the investigation. Any modifications to the data will result in a new hash value.
* Cryptographic Signatures and Enable Read-Only Access: It is possible to utilise digital signatures to confirm the veracity and consistency of the collected data. By using digital signatures, it is possible to verify that the data hasn't been changed by unauthorised parties. To avoid unintentional changes, investigators work with read-only copies of the material they have obtained. This reduces the possibility of unintentional alterations by guaranteeing that the original data is retained in its original state and that any analysis or examination is performed on copies.
* Protection from erasing or corruption and Save meta data: Investigators must take precautions to guard against unintentional deletion, corruption, or manipulation with the collected data. To restrict who can access and edit the data, access controls and permissions are utilised. The metadata associated with each packet, such as timestamps, source and destination addresses, protocols, etc., is also stored by Wireshark in addition to the packet payloads. For reenacting events and examining network traffic, this metadata is useful.
* Keep records of the preservation process: The preservation approach is meticulously documented, down to the tools used and the steps that were taken. This documentation is necessary for later review, confirmation, and presentation in court cases.

=> Phase 3: Analysis

* Filtering Data and Follow UDP Conversations and TCP Streams: Investigators can track TCP streams or UDP talks using Wireshark, which presents all the packets connected to a certain session in chronological order. This aids in figuring out the order of events and the flow of communication between hosts. Furthermore, Investigators employ a variety of filtering methods in Wireshark during the analysis phase to focus on particular packets or traffic of interest. IP addresses, protocols, port numbers, packet content, timestamps, and any other relevant investigation-related criteria may be used as the basis for filters.
* Analyze Protocol Headers and Data Reassembly: The headers of various network protocols found in the packets that were collected are examined by the investigators. They can determine the type of traffic, source and destination addresses, and other crucial details about the communication by looking at protocol headers. Data is divided into numerous packets by some network protocols, such as HTTP or email protocols. Investigators can observe the entire content of web pages, emails, or file transfers using Wireshark's ability to reassemble data from several packets.
* Detecting Criminal Activity and Timestamp Analysis: Investigators search for signals of harmful behaviour during the analysis phase, such as anomalous traffic patterns, suspicious IP addresses, unauthorised access attempts, or indications of malware infestations. Network packet timestamps offer information about the timing of occurrences. Timestamp analysis can be used by investigators to reassemble the events leading up to the tragedy.
* Exporting Useful Information and Analytical Statistics: Investigators have the option to export particular packets, conversations, or complete captures that are pertinent to the case for later offline analysis or use as evidence in court. Statistical techniques offered by Wireshark might help in finding abnormalities or patterns in the network data that has been collected. The analysis of packet counts, packet size distributions, and other statistical information can be done by investigators using these tools
* Collaborative Analysis and Reporting: Collaboration between numerous investigators or forensic professionals is typical in complicated cases. A more thorough investigation is possible because to Wireshark's ability to collaborate in real time or share capture files. The findings and observations are documented throughout the analysis phase. The analysis is summarized in reports by the investigators, who also include chronology reconstruction, detected threats, and other pertinent data

=> Phase 4: Documentation

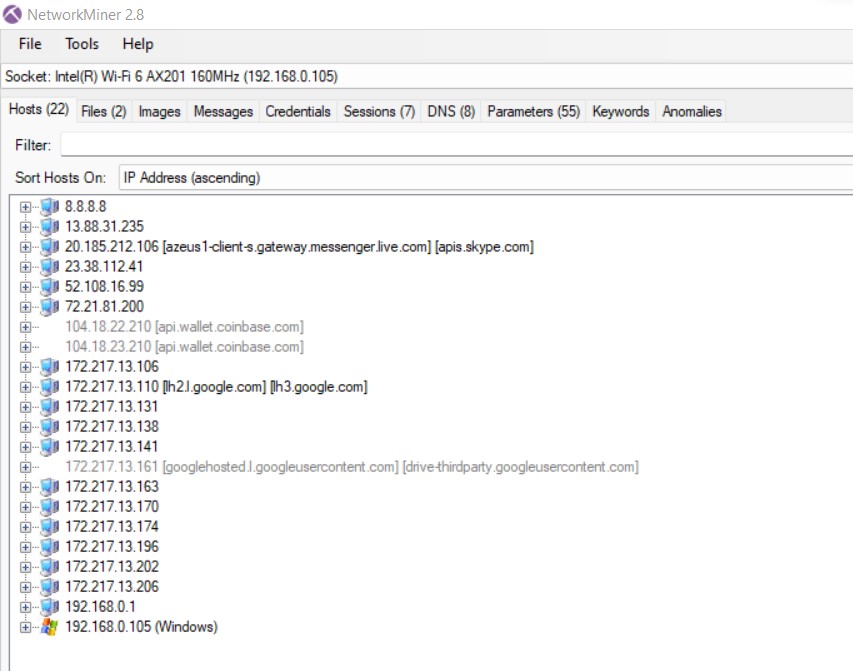
* Create case file: Investigators establish a case file at the start of the inquiry to house all the paperwork pertinent to that particular investigation. All of the data obtained during the analysis is housed in this file, which serves as its core repository.
* Collecting Packet information: The details of the packet capture are recorded by the investigators, including the date and time of the capture, the length of the capture, the network interface used, and any filters that were used during the capture.
* Final report: A final report that summaries the entire analysis process, major discoveries, and any conclusions is produced at the end of the inquiry. The report should be organized, clear, and succinct to make it simple for interested parties to grasp.

=> Phase 5: Presentation

* Data Visualization: To present the analysis results in a way that is both aesthetically pleasing and simple to understand, Wireshark offers a variety of data visualization capabilities, including graphs, charts, and timelines. Stakeholders can rapidly understand complex information when it is presented visually.
* Summary Reports: making executive briefs that highlight essential results, noteworthy occurrences, and crucial information. These summaries give a broad summary of the findings of the inquiry and can be used to swiftly inform interested parties.
* Use of Visual Aids and Concise Explanations: using graphics to demonstrate key findings and underline crucial points, such as screenshots, graphs, and other visual aids. Visual aids can help to clarify difficult ideas and improve presentation quality. providing clear and easy explanations of analysis results and words with sophisticated technical meanings. It is easier for everyone to understand the material if there is no jargon used and clear explanations are given.

**(j) Network Miner:**

By monitoring recorded network traffic, the network forensics tool NetworkMiner can extract several artifacts from PCAP files, including files, photos, emails, and passwords. It can also serve as a live network traffic sniffer, allowing for in-depth surveillance of a network interface in real-time. The programme compiles comprehensive data about each IP address in the network traffic that has been analyzed, producing a network host inventory that makes it easier to find passive assets and gives a general picture of device communications. NetworkMiner can be used on Linux systems even though it was initially created for Windows systems.  
  
=> Phase 1: Identification

******

During the "Identify" phase, NetworkMiner acts as a data collector by processing pre-captured files or live network traffic. By incorporating live sniffing and support for a variety of file types, NetworkMiner provides a versatile and complete approach to data identification, simplifying the subsequent steps of digital forensics.  
  
Live Sniffing: By sniffing a network interface, NetworkMiner is able to record live network traffic. This implies that it is capable of passively observing and recording network communications as they take place. For detecting ongoing activities and potential security incidents on the network, live sniffing is useful.

**Parse PCAP Files**: Network traffic capture data is typically stored in PCAP (Packet Capture) files. These pre-captured PCAP files can be parsed by NetworkMiner to extract and analyse the data they contain. This enables researchers to review previous network activity and retrace the order in which they occurred.

**Parse PcapNG Files**: PcapNG (Packet Capture Next Generation) is an updated version of the PCAP format that provides more flexibility and additional metadata. NetworkMiner's ability to parse PcapNG files extends its capabilities to work with the latest capture formats, improving data identification and extraction.

**Parse ETL Files**: ETL (Event Trace Log) files are generated by Microsoft Windows for logging various events. NetworkMiner can handle ETL files, making it possible to include Windows event logs in the data analysis process. This enhances the ability to identify system-level events and activities that may be crucial for investigations.

***Phase 2: Preservation***

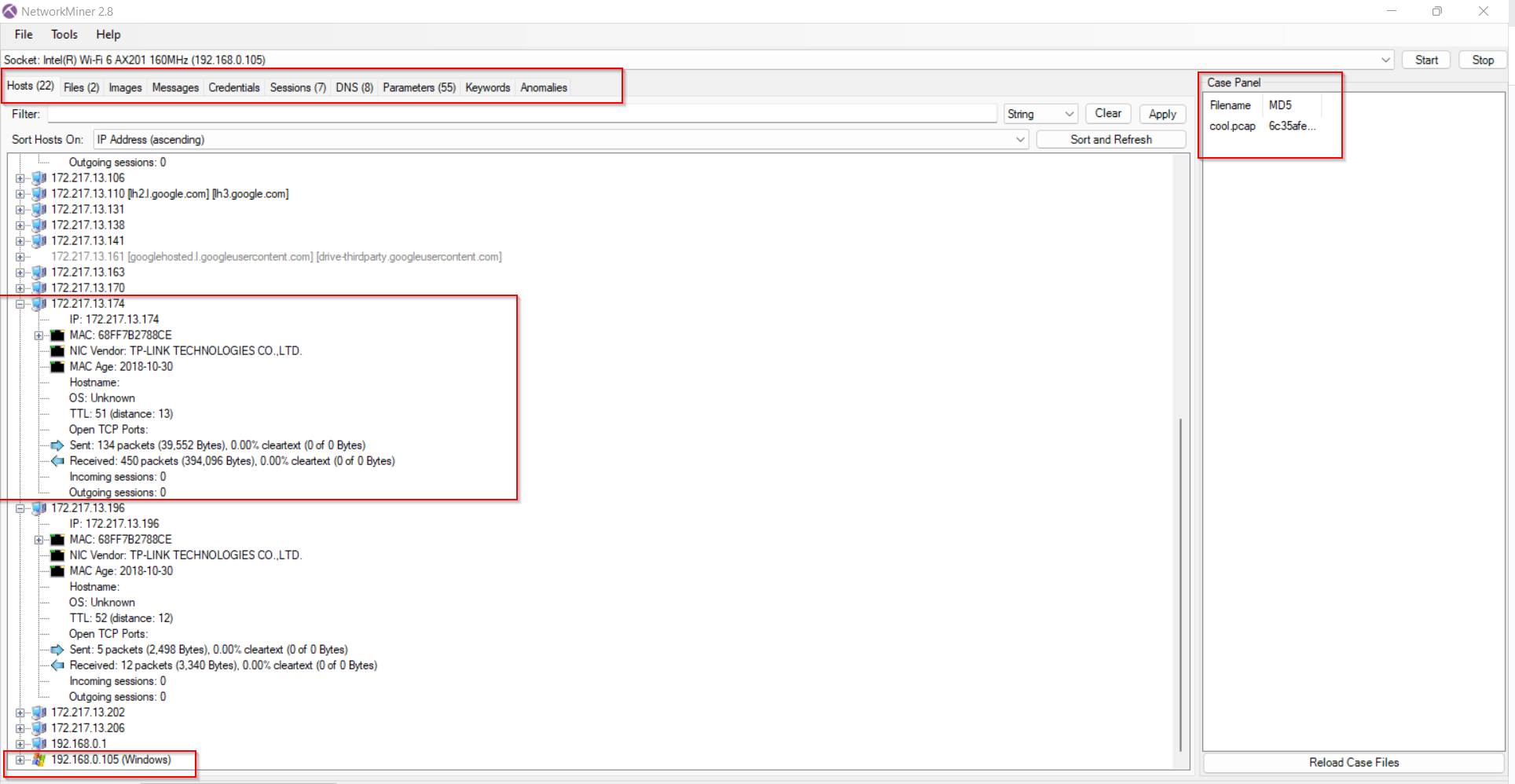
It is crucial to avoid altering or contaminating the original data to ensure its admissibility and integrity for future analysis. NetworkMiner's features assist in data collection and analysis, but it is always advisable to use dedicated tools and best practices for data preservation as it is not as effective as other dedicated tools for data preservation.

**Forensic Hashing**: Network Miner generates hashes like MD5 or SHA-256 from the network data that has been recorded or parsed and stores them with the relevant data. Investigators can recalculate the hashes of the preserved data and contrast them with the original hashes during the Analysis step. It guarantees that the data has not been corrupted, altered, or tampered with if the hash values match. Any difference in the hash values suggests possible data alteration or tampering, raising questions about the reliability of the evidence.

**Chain of Custody:**

Time stamps, user access details, and operations made on the data are just a few of the metadata that keeps track of. A trail of custody is established from the initial data collection to the last analysis thanks to the addition of this information to the chain of custody log. Information on who accessed the data, when it was accessed, and for what reason is included in the chain of custody record.

***Phase 3: Analysis***

******

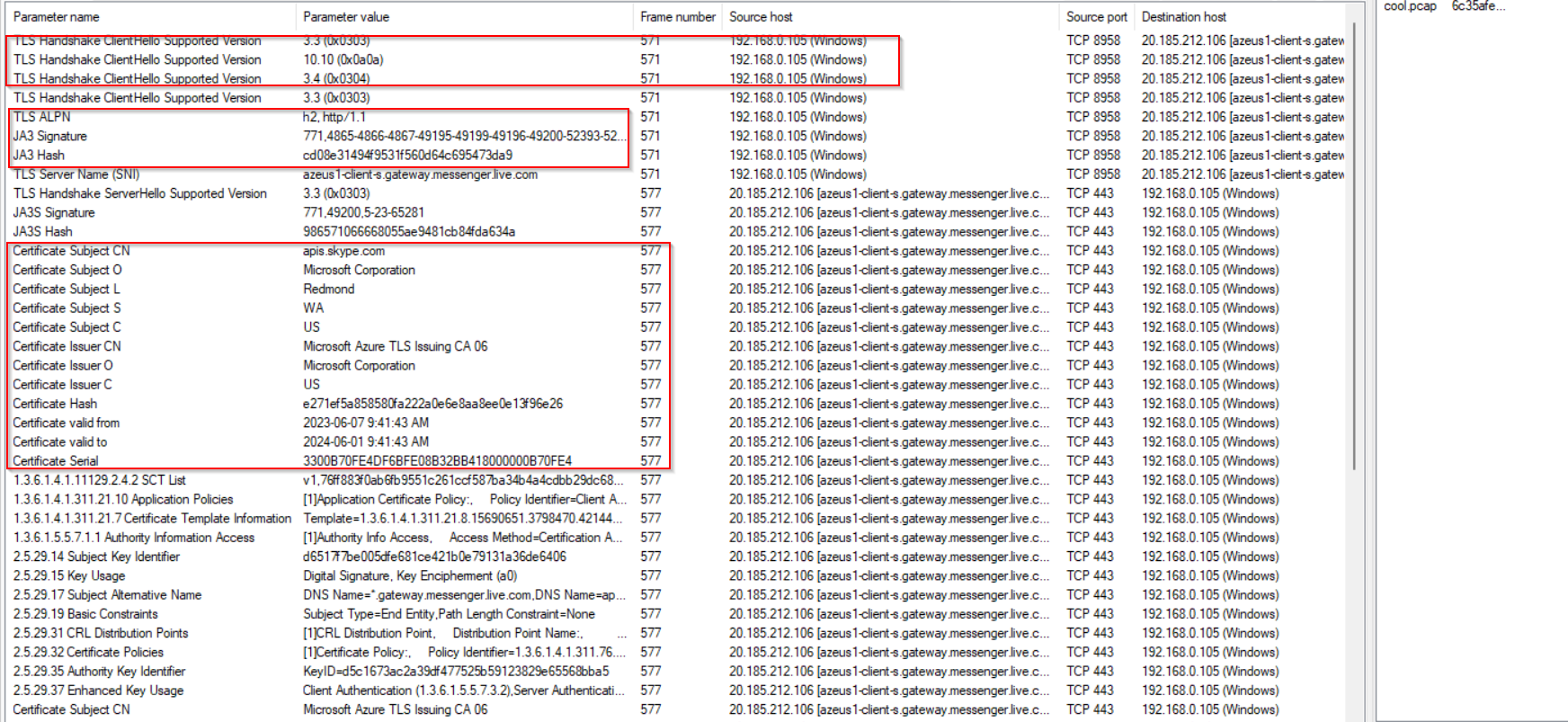
Analysis and information extraction from the recorded network traffic and data are the main goals in this phase. In order to help investigators find insightful information, this phase entails a thorough analysis and conversion of raw network data into an understandable format.

**Network Packet Carver:** This powerful tool extracts files and other artefacts from the network packets that have been collected. It uses cutting-edge techniques to recognise and recreate different file kinds from network data, including photos, documents, executables, and more. Critical evidence pertinent to the inquiry may be found in the extracted files, which can also offer helpful leads and prospective clues.

**IPV6 Support:** The ability of NetworkMiner to handle IPv6 traffic is crucial for thorough data analysis as current networks increasingly use IPv6 as their principal communication protocol. The tool's support for IPv6 guarantees that investigators can efficiently handle and understand data from networks that make use of the newest internet protocol version, keeping up with the rapid advancement of technology.

**Protocol Decapsulation:** NetworkMiner is able to decapsulate a number of network protocols, including MPLS, EoMPLS, SOCKS, VXLAN, 802.1Q, PPPoE, VXLAN, OpenFlow, and ERSPAN. Decapsulation includes opening up the encapsulated data to reveal the underlying data, improving network traffic visibility and analysis. With this feature, investigators can learn more about the various communication tiers within the network.

**JA3 and JA3S Hash Extraction:** This toolsupports the extraction of JA3 and JA3S hashes from SSL/TLS communications. JA3 and JA3S are hash representations of the SSL/TLS client behavior, aiding in the identification of specific SSL/TLS clients. This feature is particularly



valuable in identifying potential threats, tracking malicious actors, and understanding the SSL/TLS handshake behavior within the network.

**OS Fingerprinting:** NetworkMiner analyzes network traffic to identify the operating systems (OS) involved in communication. By recognizing OS-specific characteristics in the traffic, investigators can gain insights into the devices and systems communicating on the network.

**Port Independent Protocol Identification (PIPI):** It can can identify network protocols independently of the port used. This ability allows the tool to recognize protocols even if they are running on non-standard ports, contributing to more accurate protocol identification.

**User-Defined Port-to-Protocol Mappings:** This feature allows investigators to customize port-to-protocol mappings. By defining specific port associations, NetworkMiner can correctly interpret network traffic that uses non-default or non-standard port configurations.

**OSINT lookups:** NetworkMiner can conduct Open Source Intelligence (OSINT) lookups using file hashes, IP addresses, domain names, and URLs. By querying external databases, investigators can enrich their findings with additional information about these entities.

**DNS Whitelisting:** This feature allows investigators to analyze and whitelist legitimate DNS traffic, filtering out noise and focusing on potentially malicious DNS activities during analysis.

**Web browser tracing and online ad/tracker detection:** NetworkMiner can trace web browser activities and detect online advertisements and trackers. This capability is useful in understanding user behavior and identifying privacy concerns.

***Phase 4: Documentation***

In this phase, the focus is on meticulously recording and documenting all relevant findings, analysis procedures, and investigative activities conducted using the tool. Investigators can create detailed reports containing valuable insights extracted during data analysis, preserved evidence, and observed network behaviors. NetworkMiner enables the generation of reports in various formats such as CSV, Excel, XML, CASE, and JSON-LD, ensuring compatibility with different reporting standards and tools. Additionally, the tool allows customization of file output directories and time zones, enabling investigators to maintain accurate timestamps and organize evidence systematically.

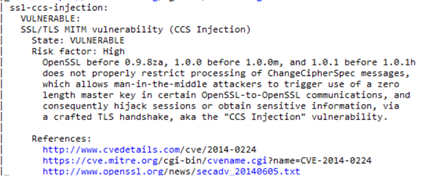
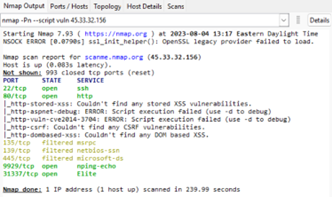
***Phase 5: Presentation***

In this phase, the documented data and findings obtained from the previous phases are compiled and organized into a visually engaging and coherent format. NetworkMiner provides several ways to present the data effectively:

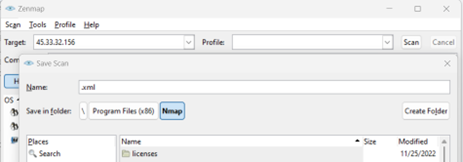
**Graphs and Charts:** NetworkMiner can generate graphs and charts to visualize network traffic patterns, communication trends, and protocol distribution. These graphical representations make it easier for investigators to understand complex data and identify significant patterns or anomalies.

**Tabular Data**: The tool allows investigators to present the extracted data in tabular formats, providing a structured view of the information. This includes details like source and destination IP addresses, timestamps, protocol information, and extracted files.

**Visual Network Maps:** NetworkMiner can create network maps to illustrate the communication flow between devices and hosts. These visualizations help identify connections, relationships, and potential points of interest within the network.

**(k) NMAP:** NMAP is an effective open-source network scanning tool, and can be a useful tool for network forensics in cybercrime investigations. NMAP enables investigators to obtain thorough insights into a targeted network's topology, open ports, services, and operating systems by using a variety of scanning techniques. NMAP assists in locating probable entry points, unauthorized access, and other malicious actions when analyzing a cyber incident. Additionally, its capacity to carry out covert scans aids investigators in staying undiscovered, maintaining the validity of the inquiry. In order to identify anomalies and suspicious behavior, NMAP's detailed output and capacity to provide graphical representations make it easier to visualize network architecture. Therefore, by including NMAP into the network forensics toolkit, cybercrime investigators can hasten their inquiries, increase their body of proof, and eventually help counteract cyber threats more successfully. [SS3][SS4][SS5]  
  
**1. Identification & Preservation**Nmap can be a valuable tool during the identification phase, which involves gathering information about the network and the systems connected to it. Nmap can help us to **identify** active hosts on the **network**. By running a basic scan (nmap -sn <address>) with Nmap, we can discover live hosts, their IP addresses, and even the operating systems they are running. This information provides a starting point for further investigation. Then, Nmap can perform **port scans** (nmap -p- <ip address>) to determine which ports are open on the target systems. Open ports may indicate running services and applications, potentially hinting at the purpose and role of the system. Once open ports are identified, we can use Nmap to identify **the services running on those ports (**nmap -sV -p 80,443 <ip address>**)**. This can provide insights into the applications and services hosted on the systems. There are two types of **OS fingerprinting** that can be performed (nmap -O <ip address>) to identify the anomalies in the network. NMAP uses active OS fingerprinting which involves 15 probes to conduct the OS fingerprinting. Lastly, Nmap has a powerful **scripting engine** (NSE - Nmap Scripting Engine) that allows us to create custom scripts (nmap -p 22 --script ssh2-enum-algos <ip address>) or use pre-existing scripts to gather specific information or detect vulnerabilities on the network. [SS3] [SS4]  
   
  
**2. Analysis**After the identification it is important to analyze the following evidence to know what has exactly happened during the event. Nmap's port scanning capabilities can help identify open ports on target systems. By knowing which ports are open and the corresponding services running on them, we can determine the potential attack surface and identify any unauthorized services. Nmap can be used with options like "--packet-trace" and "--packet-trace-file" to capture raw packets during the scan. This feature allows us to analyze the actual packets exchanged during the scan, which can be beneficial in reconstructing potential attack patterns and methods. By running Nmap scans at different points in time or against known-good configurations, we can identify changes in the network's status or detect potential intrusions. [SS2]

3. **Documentation and Presentation**After the identification of the pattern or crimes that has happened in the specific cybercrime it is required to document the finding for further procedure to pass it to the court. There are several ways and processes to document all the evidence in this process. We can export our scanning results to external files. For example, we will not be reading from a file by this process, but exporting/saving our results into a text file using such commands:

(nmap -oN output.txt scanme.nmap.org)  


Also, Nmap can export files into XML format as well (nmap -oX output.xml scanme.nmap.org).

**Memory Based Investigation:**   
  
A particular branch of digital forensics that investigates data in RAM is referred to as memory-based digital forensics. It attempts to wring out useful data from active processes, network connections, and user behaviors. Memory capture, analysis, virus identification, data extraction, rootkit detection, and timeline reconstruction are important elements. It is essential for looking into active systems, spotting complex threats, and thwarting anti-forensic strategies. Memory forensics is a supplement to more established techniques and aids in gathering important data that could be lost if the machine is turned off.

**Volatility Workstation**

In the field of digital forensics, the Volatility Workstation is a potent and specialized tool made to help investigators and analysts examine and comprehend the inner aspects of computer memory. In order to help legal investigations, digital forensics entails examining and obtaining digital evidence from various electronic devices.

Volatility The idea of memory forensics, a technique that entails collecting and analyzing volatile data stored in a computer's RAM (random access memory), lies at the core of workstation software. Understanding the actions that have occurred on a computer, such as running processes, open network connections, and possibly harmful software, depends heavily on this kind of data.

Digital forensic specialists may explore memory dumps using the Volatility Workstation program to unearth information about cybersecurity events, cyberattacks, malware infections, and illegal access. The program offers a variety of functions, such as memory image analysis, process inspection, network connection tracking, and artifact extraction, all of which are helpful in putting together a whole digital story.

In conclusion, the Volatility Workstation is a crucial tool for experts working in the field of digital forensics since it enables them to retrieve important data from computer memory and retrace the chain of actions that led to a digital incident or breach.

**Phase 1: Identification**

The Volatility Workstation is essential for locating possible evidence and abnormalities in a computer system's memory during the identification stage of digital forensics. In this stage, essential information that can be useful for an inquiry is identified and categorized. The Volatility Workstation operates as follows during the identification stage:

Analysis of Memory Dump: The procedure starts with obtaining a memory dump from the target machine. A memory dump is a record of the volatile memory (RAM) of the computer at a certain moment in time. This memory dump is consumed by the Volatility Workstation program for analysis.

Profile Selection: Each operating system and each of its iterations uses a different set of memory architectures. The investigator can choose the proper memory profile that complements the features of the target machine using the Volatility Workstation. This process guarantees reliable memory data interpretation.

Artifact Recognition: The Volatility Workstation analyzes the memory dump using a range of plugins and analysis methods. These plugins gather data on open files, network connections, running processes, loaded modules, and more.

Malware and Suspicious Activity Detection: By examining process behaviours, network connections to known malicious servers, and memory areas that potentially contain evidence of compromise, the program can assist in identifying suspicious or malicious activity.

Volatility Workstation may help in the detection of abnormalities that could point to illegal access, data breaches, or other odd actions. For further analysis, unusual communication patterns, unanticipated operations, or updated system components might be marked.

Evidence Cataloguing: The program can catalogue and arrange the findings as it unearths possible evidence. This may consist of logging operations, the network connections they need, pertinent timestamps, and other artifacts.

Correlation: The program could allow users to compare data from memory with other types of digital evidence, such network logs or filesystem artifacts. This might aid in creating a more thorough picture of the circumstances leading up to the occurrence.

Reporting: To summarize the facts and anomalies found during the identification step, reports are frequently produced. These reports may act as the basis for additional investigation and legal actions.

In summary, the Volatility Workstation assists in the identification stage by enabling investigators to gather crucial data from memory dumps, identify relevant cues, and find unusual or suspicious activity that may call for additional inquiry. It is a crucial instrument in the larger field of digital forensics.

**Phase 2: Preservation**

The objective of the digital forensics’ preservation phase is to guarantee the validity and integrity of the digital evidence gathered throughout an investigation. This stage entails taking precautions to ensure that the evidence is not changed or tampered with in any way so that it may be confidently utilized for analysis or presented in court. The Volatility Workstation contributes to the preservation phase in the following ways as part of the digital forensics process:

Making Forensic Copies: The memory dump may be made forensic copies using the Volatility Workstation before any analysis is done. These copies, which are exact replicas of the original memory picture, are frequently made utilizing write-blocking technology to protect the integrity of the original data.

The Volatility Workstation is capable of computing the memory dump and forensic copies' cryptographic hashes (for example, MD5, SHA-256). Data is given a distinctive digital fingerprint by hashing. Investigators can confirm that the data has not been altered by comparing the hash values of the original memory dump with its duplicates.

Chain of Custody: The software can help to ensure that the evidence has a valid chain of custody. This entails recording each action performed, from the time the evidence is gathered until it is presented in court. Actions taken on the evidence may be recorded by the Volatility Workstation, ensuring accountability and transparency.

Read-Only Analysis: It's critical to prevent any write operations that can change the evidence during the preservation stage. The Volatility Workstation is made to analyze the RAM dump in read-only mode, preventing accidental changes.

Volatility Workstation can aid in the preservation of crucial metadata related to the memory dump, like creation timestamps, system details, and more. The context of the evidence may be established with the use of this information.

Documentation: The program is able to produce reports outlining the preservation phase's procedures, including information on the construction of forensic copies, hashing, and any actions done with regard to the evidence.

Backup and storage: The Volatility Workstation can let investigators store the evidence in safe, secure locations. It could also provide choices for making backups in order to avoid data loss.

Volatility Workstation may include capabilities that assist assure adherence to statutory and regulatory obligations. To protect the validity of the evidence, techniques like digital signatures, timestamping, and encryption could be used.

Overall, the Volatility Workstation's job in the preservation phase is on preserving the validity and integrity of the digital evidence gathered, making sure that it endures an inquiry and any following legal actions unmodified and dependable.

**Phase 3: Analysis**

The Volatility Workstation is essential in the analysis stage of digital forensics for drawing conclusions and important data from the gathered memory dump. This stage entails carefully going over the evidence in order to recreate the events, spot trends, and make judgments. The Volatility Workstation offers the following benefits to the analysis stage:

Plugin-Based Analysis: The Volatility Workstation offers several plugins, each of which is intended to extract a particular kind of data from the memory dump. These plugins can reveal information about open files, registry entries, loaded modules, active processes, network connections, and more.

Process reconstruction: Using the Volatility Workstation, investigators may retrace the order of the processes that were active at any given time. This aids in comprehending the events that occurred throughout the pertinent time period.

Network Activity Analysis: The program may show details about the connections made by processes in the memory dump to networks. Data exfiltration efforts, possible command and control operations, and contact with external servers can all be found by investigators.

Malware Analysis: Volatility Workstation has the ability to spot malware and other dangerous activity. It can find malicious processes, code injection, and malware-related artifacts.

Timeline generation: The program can assist in creating a timeline of events by comparing timestamps and events recovered from the memory dump. Reconstructing the sequence of events leading up to and during an incident is made easier with the help of this timeline.

Artifact Extraction: For further in-depth research, investigators can utilize the program to extract particular artifacts, including process memory or registry keys. This can assist in decrypting information that is encrypted or concealed.

Volatility Workstation can help in the identification of patterns of behaviour or abnormalities. Investigators can spot suspicious activity by comparing acquired data to established trends.

Cross-Reference with additional Evidence: Using additional digital evidence, such as filesystem information, logs, or metadata, investigators may be able to compare information from the memory dump with other discoveries. This thorough approach aids in developing a thorough knowledge of the occurrence.

Keyword Search: Some Volatility Workstation products let forensic analysts to run keyword searches on the memory dump. Using this, you may find particular words, URLs, IP addresses, or other identifiers.

Reporting: The Volatility Workstation can produce thorough summaries of the analysis phase's findings. These summaries give a thorough summary of the uncovered data and may be used to future actions, such legal actions.

In conclusion, the Volatility Workstation helps investigators collect, organize, and analyse data from memory dumps as part of the analysis phase of digital forensics. Insights that are essential for comprehending the scale and type of digital events may be uncovered using its broad collection of tools and plugins.

**Phase 4: Documentation**

The Volatility Workstation is an essential tool for investigators to gather and display their results in-depth during the documentation phase of digital forensics. By automatically merging the data gleaned from the memory dump and the findings of the study, it speeds the process of producing comprehensive reports. The program arranges this data into a systematic way, enabling researchers to coherently communicate their findings. It incorporates information from multiple analytic plugins and approaches, ensuring a complete depiction of the research.

To retain context and authenticity, Volatility Workstation-generated reports frequently include information such case numbers, investigator names, and pertinent dates. These reports give a clear description of the chain of custody, outlining the methods used to gather, examine, and store the evidence. Graphs, timelines, and process trees are examples of visual aids that make it easier to communicate complicated information to both technical and non-technical audiences.

Annotations, comments, and notes can be included by researchers to offer context and insights to their findings. The program enables explanations of the analysis procedure, the plugins used, and the justification for analytical choices. The investigation's findings can be summarized, supported by the data acquired, and recommendations for more action can be made. The created reports are significant in that they comply with legal criteria, guaranteeing their acceptance as evidence in court actions.

The Volatility Workstation makes it easy to share results with stakeholders, coworkers, and legal experts by enabling the export of reports in a variety of formats, such as PDF or HTML. Utilizing the Volatility Workstation for documentation allows investigators to efficiently communicate their meticulous analysis and results, enhancing the openness, reliability, and overall effectiveness of the investigation.

**Phase 5: Presentation**

The Volatility Workstation makes it easier to create thorough reports for digital forensic investigations during the documentation stage. It merges data from memory dumps and analytical outputs automatically into an organized manner. For perspective, metadata including case specifics and investigator details are supplied. The software's reports keep track of evidence handling from collection to preservation while maintaining the chain of custody. Timelines and graphs are visual tools that improve the presentation of complicated data. Annotations and remarks provide more context for the results and analytical process.

The investigation's findings can be reported and backed by evidence, and suggestions for more action can be made. Reports comply with legal criteria, guaranteeing their validity in court. Export options in several formats make it easier to share information with stakeholders and legal experts, which increases the investigation's openness and credibility.

**Exif Tool**

ExifTool is a robust and adaptable program created by Phil Harvey that enables you to read, write, and change metadata in a number of different file types, primarily picture and multimedia files. When a file is formed, the settings that were used on the camera, the GPS locations, and many other characteristics are recorded as metadata, which is information that is contained inside the file. ExifTool is frequently used to work with Exchangeable Image File Format (EXIF) metadata, but it also supports many other metadata formats, such as IPTC, XMP, and others.

ExifTool can be used from the command line or integrated into various software applications. Here's how it works, and the phases involved:

**Phase 1: Identification**

ExifTool's identification phase is the step when metadata from a given file is extracted and displayed. Without altering the file, itself, this stage enables users to quickly acquire comprehensive information about a file, such as an image. ExifTool operates as follows during the identification stage:

1. File input: You provide the path of the file you want to identify in the file input field. This might be a multimedia file that supports audio and/or video, such as a JPEG, TIFF, or PNG picture file. This stage does not include any changes to the input file.

2. Extraction of Metadata: ExifTool scans the input file and extracts the different metadata that are present within. Depending on the file type and the particular metadata formats it supports, this metadata may include details about the file's origin, creation date, camera settings, GPS coordinates (if available), and much more.

3. Metadata Display: ExifTool presents the extracted metadata on the screen in a way that is readable by humans. Key-value pairs are used to organize and convey this data, making it simple to comprehend and analyze. Details like camera brand and model, exposure options, lens length, shutter speed, aperture, geolocation information, software utilized, and much more may be included in the displayed metadata.

4. Optional Formatting and Filtering: ExifTool offers choices to format the output to meet your needs. It also offers filters. The output may be sorted, particular metadata fields can be excluded, you can define which tags or groups of tags you're interested in, and you can choose how dates and other values are shown. This enables you to concentrate on finding the precise information you need.

5. Command-Line Usage: Using the Command Line: The command line is often used to carry out the identification step. A command that specifies the file you wish to identify would be run after you launch a terminal or command prompt, go to the directory where ExifTool lives, and then open the desired file. The fundamental command arrangement would be as follows:

exiftool [options] filename

Here, options can include any formatting or filtering preferences you want to apply to the output, and filename is the path to the file you're identifying.

**Phase 2: Preservation**

ExifTool may be used to facilitate the preservation phase of digital preservation by managing and upholding the metadata linked to digital files through time. Activities that guarantee the long-term usefulness, authenticity, and accessibility of digital material are part of the preservation phase. ExifTool can contribute to this stage by assisting with the upkeep and documentation of file metadata. ExifTool operates as follows during the preservation stage:

1. Metadata Verification: Verification of Metadata It's crucial to ensure that the metadata of digital files is correct and undamaged during the preservation process. Preservationists can use ExifTool to extract and display metadata from files so they can compare the derived metadata to the expected metadata. Any anomalies or inconsistencies may be found, assisting in maintaining the integrity of the material over time.

2. Metadata Migration: To maintain accessibility when file formats change, it may be required to move digital material to newer forms. Sometimes, metadata might be lost or changed during this procedure. Metadata may be migrated with the aid of ExifTool by being extracted from the original file, converted to the necessary format, and then embedded into the migrated file.

3. Metadata Backup: Backups of the metadata must be made since they are essential to the preservation process. File metadata may be extracted using ExifTool and saved in a standardized, readable format. Even if the original file format becomes outdated, these backup copies of the metadata can be used to provide proof of the file's features and place of origin.

4. Metdada Enhancement: Metadata enhancement is a common part of preservation efforts since it adds more context. Copyright details, provenance information, and preservation-related annotations are just a few of the metadata fields that may be added to or changed with ExifTool. Future users will better comprehend the file's relevance and history thanks to the additional metadata.

5. Batch Processing: Processing in batches: In preservation circumstances, it may be necessary to handle several files at once. By applying consistent metadata updates to a group of files in a batch using ExifTool, preservationists may ensure that metadata is universally standard and maintained.

6. Documentation: ExifTool can provide reports that go into great depth on a file's metadata. These reports can be used as proof of the preservation efforts, showing the properties of the file and the measures taken to retain its metadata.

7. Format-Specific Preservation: Each file format has its own set of metadata requirements. ExifTool's compatibility with a variety of metadata standards, including EXIF, IPTC, and XMP, enables preservationists to efficiently handle metadata unique to diverse formats.

**Phase 3: Analysis**

ExifTool is a useful program for extracting, deciphering, and organizing information from digital files during the analysis process. In order to obtain knowledge, develop opinions, and make defensible judgments, this step entails looking at the metadata included within files. ExifTool operates as follows during the analysis stage:

1. Metadata Extraction: ExifTool is used for the extraction of metadata from digital files. This metadata may contain facts about the file itself as well as information on how the file was made, edited, and used. Examples of metadata in the context of photos include camera settings, the date and time the image was created, its location, and more.

2. Data organization: The extracted metadata is put into an organized, readable manner by ExifTool. The metadata is presented in a way that makes it simple for analysts to evaluate and comprehend the data. Typically, metadata values are shown along with the labels or tags that they correlate with.

3. Analysis: To get insights and conclusions, analysts analyze the retrieved metadata. For instance, while looking at photos, metadata can include details about the camera that was used, which may aid in determining the image's source. Similarly, metadata may give details about an image's past editing processes, or the programs used to make it.

4. Contextual Understanding: Understanding the context in which a file was generated or utilized is important when analyzing metadata. For instance, examining the geolocation information contained in photos might reveal information about the place where the picture was shot. In situations involving investigations or research, this contextual knowledge may be essential.

5. Comparative Analysis: ExifTool makes it simple to compare the metadata of several files. By comparing metadata values across a group of files, analysts can spot trends, inconsistencies, or abnormalities. This might be useful for finding discrepancies or confirming the legitimacy of files.

6. Automation and batch processing: ExifTool's batch processing features might be used when a lot of files need to be analyzed. Automated processing and metadata extraction from many files may be done by analysts, saving them time and effort.

7. Custom Analysis: The metadata output of ExifTool may be customized in terms of presentation and filtering. The output of the tool may be customized by analysts to display only the particular metadata fields of relevance, making it simpler to concentrate on pertinent data for the study.

8. Documentation and Reporting: ExifTool may provide reports that summarize the metadata that has been extracted from files for documentation and reporting. These reports may be used to provide a clear record of the insights and conclusions derived from the metadata and to document the results of the analysis process.

**Phase 4: Documentation**

ExifTool may be used to create thorough, well-organized reports that record the metadata and other pertinent details about digital files during the documentation process. These reports act as a sort of documentation, aiding in the long-term preservation and communication of crucial information about the files. ExifTool operates as follows during the documentation stage:

1. Metadata Extraction: ExifTool retrieves metadata from digital files, which is similar to the analysis stage. These metadata may contain a variety of features, including production dates, camera preferences, geolocation information, author information, copyright information, and more.

2. Customization of Output: ExifTool gives users the option to modify the generated reports' output. Which metadata tags or groups of tags you wish to include in the report can be specified. This enables you to concentrate on particular metadata elements that are pertinent to the documentation needs.

3. Formatting and Organization: ExifTool puts the extracted info in a legible and structured manner. It may display the metadata in a variety of ways, such as tabular formats, HTML tables, or even JSON for reports that can be read by machines.

4. Batch Processing: ExifTool's batch processing features are useful if you need to document a lot of files. Multiple file report generation may be automated, assuring consistency and saving time.

5. Addition of more Information: You may add more pertinent information to the documentation reports in addition to the metadata. This might entail providing explanations, background data, or comments that deepen our knowledge of the files.

6. Timestamps and Provenance: Timestamps can be used in documentation reports to show when the documentation was created. This contributes to the provenance of the files and their related information by creating a chronology of the documenting process.

7. Digital Signatures: ExifTool can also provide digital signatures for the documentation reports in situations where authenticity and integrity are important.This increases security and trust by making sure that the documentation wasn't changed after it was created.

8. File connections: ExifTool can assist in establishing and documenting the connections between several files in documentation if those files are connected in some way.This is very helpful when working with groups of files.

9. Storage of Documentation Reports: The generated documentation reports may be kept in the same place as the source files or in a separate archive. By doing this, it is made sure that the documentation can be quickly found and linked to the appropriate files.

10. Reporting Formats: Text, HTML, XML, JSON, and other output formats are all supported by ExifTool. You may select the style of documentation that best serves your purposes and the target audience.

**Phase 5: Presentation**

ExifTool may be used to produce aesthetically beautiful and instructive presentations or displays of metadata and other pertinent information collected from digital files during the presentation stage. These presentations are made to explain to diverse audiences the traits, background, and context of the files. ExifTool can function as follows during the presenting stage:

1. Metadata Extraction: ExifTool's metadata extraction function pulls data from digital files, including creation dates, camera settings, location data, and more.

2. Selection of Relevant Information: You may choose the particular metadata tags or sets of tags that are most pertinent to the audience, depending on the goal of the presentation. For instance, if you're giving a presentation to a photography class, you can concentrate on the technical aspects and camera settings. If you're giving a presentation to a large group of people, you could put more emphasis on the narrative or the historical setting of the photos.

3. Presentation Personalization: You may modify how the metadata is displayed with ExifTool. There are several presentation forms available, including tables, slides, infographics, and interactive displays.

4. Visual Enhancements: You may add images, icons, graphs, and charts to your presentation to make it more appealing to the audience. These images can aid in simplifying complicated material for easier understanding.

5. Contextual Information: You may include contextual information to your presentation in addition to metadata. This might entail giving background data on the files' subject, the project's goal, or the files' importance in a larger context.

6. Storytelling: During the presentation phase, you may use the files' metadata and actual content to tell a narrative. The data may be used to create a story that highlights their journey, the persons involved, and the feelings they arouse.

7. Interactivity: Depending on the presentation format, you could incorporate interactive components that let viewers go further into the information. This may include interactive maps with geolocational data, pop-up information, or links that may be clicked on.

8. Consider your desired audience while designing your presentation. You may concentrate on specific technical information for technical audiences. You might stress the artistic elements and the human stories hidden inside the files for non-technical readers.

9. Presentation Equipment: You may use a variety of presentation tools to make aesthetically appealing slides, papers, or interactive displays, depending on your preferences and the platform you're using. To make a cogent and educational presentation, include the metadata ExifTool collected into these tools.

10. Accessibility: Make sure that all viewers can access the presentation. Use alt text for photos, captions for graphics, and think about choosing a format that is simple for those with impairments to use.

* **Hardware tools:**   
   The number of cybercrime though information technology is increasing day by day. The investigation using various resources comes from the authorities who are responsible to investigate the crime and are collected by different groups. The basis of the investigation depends on data analysis, image analysis and voice analysis. To perform better research and investigation, the investigator uses different kinds of hardware and software tools. This is very crucial to perform very accurate and exact analysis using these tools. The process of collecting evidence for hardware tools is generally bring evidence from the crime scene to analyze department or collecting evidence from the crime scene. Normally, transporting tools, secure deleting data tools, adapters and collecting data systems are used.   
  + Some of the hardware tools that are discussed here :
    - Forensic workstation (AntAnalyzer)
    - Fly Away Kit (mh)
    - Forensic Laptop (mh)
    - Forensic Van (mh)
    - Tableau TX1 Forensic Imager
    - Tableau TD2U Forensic Duplicator
    - Tableau Forensic Universal Bridge
    - CRU Write blocker
    - Tableau Write blocker Kit

**Forensic Van (mh):** The mh systems, made in Germany, are specially developed for IT-forensic hardware solutions. These are developed in cooperation with international IT-forensic investigators, fully configurable and always upgradeable. Forensic Van is one of the hardware forensic tools developed by mh. It is a fully independent, fully equipped mobile laboratories ranging from minivans through luxurious roll-off containers up to 40 ton trucks. Forensic vans or mobile laboratories are completely self-sufficient and fully equipped mobile laboratories for a whole range of laboratory applications in the field: command center, crisis management and much more [15].

Following are the available forensic vans or mobile laboratories:

* Paladin - "Truck"
* LabCube - "Cube"
* Paladin - "Delivery Van"
* Paladin - "Small Van"

* **Paladin - "Truck":** The PALADIN is a truck-based, fully stocked lab for IT forensic investigations. Data recovery, eDiscovery, and IT forensics are now feasible in even the most challenging situations. Systems that are otherwise only available in the control center can be installed to the integrated rack server's globally exclusive SwingRack. It is a fully equipped lab with space for 12 to 16 researchers with a kitchen and restroom to make it comfortable even during lengthy workdays. The total weight limit is 40 tonnes. Even on uneven travels, the very sensitive IT equipment is protected by the globally exclusive SwingRack [15].
* **LabCube - "Cube":** The Lab Cube is one of the models in an existing line of mobile forensic laboratory trucks. From a transporter to a semi-trailer container, every size is feasible. The body, interior, equipment, and design of the cars, as well as their proportions, can differ. The customer is coordinated in advance to ensure maximum workflow, and intelligent room conceptions are integrated with great hardware and software components. We can build a customized vehicle for each customer based on their specific requirements. The LAB Cube, the only fully independent forensic laboratory that arrives in a luxurious roll-off cube on a truck, operates both on wheels and without them. The autonomous cube can be positioned anywhere you need it for your IT-forensic investigations and has its own electric generator. It has an office space and a server room that are divided by a contemporary cabinet wall made of frosted glass and illuminated by LEDs. A central control desk at a comfortable working height can regulate the generator, air conditioner, and lighting. The various server modules are securely held in place by the distinctive swing rack that mh SERVICE designed and built.It is made up of a steel frame that is securely fastened to the car's frame. Within the outer frame is another steel structure that supports the server components. Air shock absorbers that connect the two steel structures ensure that any road roughness is balanced out while the vehicle is in motion. There are four workstations set in a row in the fully furnished office. On the other side of the workstations, there is a conference table that can be folded up or down as needed. The table has a large presentation screen over it. The adjustable designer chairs may be transported by being fastened to the desk. For extended work hours, the cube also contains a kitchenette furnished with a stove, microwave, sink and coffee maker. The interior of the cube, which has a total area of 11,5 m2, appears to be very roomy. Four people can easily work side by side [15].
* **Paladin - "Delivery Van":** The specialized mobile forensic vehicle described operates with a Class B driving license, offering easy handling and accommodating 3-4 investigators within its 3.5-5 tons total weight. Equipped with a SwingRack system ensuring secure IT component operation, the vehicle maintains self-sufficiency for approximately one work week. It provides all essential tools for digital evidence collection and analysis, including IT forensics, eDiscovery, and data recovery capabilities, even in challenging environments. The integrated rack server enables the deployment of typically central systems, and the unique SwingRack permits IT equipment operation during transit. The current configuration features Evidence Talks' Cascade solution, serving as a mobile triage lab that expedites data acquisition, benefiting both first responders and HQ experts by minimizing exposure to distressing material while accelerating the examination of pertinent data [15].
* **Paladin - "Small Van":**  
   Mobile minivan laboratory - perfect for your on-site investigations. The specialized minivan Paladin offers a convenient solution for digital forensic operations, accessible with a Class B driving license. Designed for ease of use and efficient space utilization, it accommodates 2-3 investigators within a total weight of up to 3 tons. Its innovative SwingRack technology ensures secure operation of IT components by mitigating vibrations. Featuring 2 full workstations, a rotating passenger seat for an extra investigator, and a strategically separated office and technical area for optimal insulation, the minivan offers a tranquil working environment. It is equipped with an AntAnalyzer workstation, centralized storage server, integrated WIFI, external network connectivity, and support for mobile devices, constituting a comprehensive IT forensics lab. The minivan boasts an independent power supply system with a generator for up to 99 hours of self-sufficient operation, enhanced by a fail-safe online UPS with 10 hours of battery backup. The vehicle's reinforced air conditioning system extends its usability to humid and hot regions. Further, an integrated rack server enables the use of headquarters-level systems, and the unique Swing rack permits system operation even while in motion [15].
* **Fly Away Kit:**  
   In forensic investigation, a Fly Away Kit can be organized based on the different phases of the forensic process. Here are the features of a Fly Away Kit, categorized according to the various forensic phases:

Crime Scene Assessment and Documentation

* Digital cameras with macro lenses
* Tripods and scales for accurate measurement and photography
* Notebooks, pens, and evidence collection forms for documentation
* Evidence markers for marking and labeling items at the crime scene
* Measuring tapes and rulers for recording dimensions
* Flashlights and alternate light sources (e.g., UV lights) for examining evidence in various lighting conditions
* Crime scene barrier tape to cordon off the area and control access
* Personal Protective Equipment (PPE) - gloves, masks, shoe covers, and disposable overalls
* Evidence Collection and Packaging
  + Fingerprint kits (brushes, powder, lifting tape) for latent print recovery
  + Swabs for biological sample collection
  + Containers for preserving trace evidence
  + Evidence bags with proper seals for safe transportation
  + Forensic casting materials (e.g., plaster of Paris) for impression evidence
  + Cutting and sampling tools (scalpels, scissors, tweezers) for precise collection
* Preliminary Evidence Processing
  + Presumptive drug test kit for initial on-site drug testing
  + Gunshot residue kit for testing for firearms discharge residues
  + Decontamination supplies for cleaning tools and equipment after use
  + Packaging and Preservation for Transportation
  + Tamper-evident evidence seals
  + Anti-static bags for electronic evidence
  + Proper containers to prevent contamination or degradation of evidence
  + Portable evidence processing kits for specific tests or examinations

It's essential for forensic investigators to be prepared with a well-organized Fly Away Kit to ensure the efficient and effective processing of a crime scene and the preservation of evidence. The kit should be tailored to the specific requirements of the investigation and comply with established forensic procedures and guidelines to maintain the chain of custody and the integrity of the collected evidence. A Flyaway kit must enable agile rapid response by CPT teams. These kits need to easily scale up and scale down while traveling to meet the mission and be able to respond at a moment’s notice, and not have to carefully schedule additional travel assets. Fly-away kits must:

* + Be "carry-on" accessible for commercial aircraft, staying close to the analyst
  + Lifted by a single person
  + Easily transported by rental car, sedan, or SUV vehicles
  + Make travel less conspicuous by carrying smaller items
  + Reduce operation costs, by simplifying procurement
  + Reduce travel costs by leveraging commercial travel options
  + Reduce setup time & tear down time
  + Reduce size, so less space used on the site/location, expanding the potential sites where space is a constraint

In order to determine the state of the critical networks or to run a deployable network, cyber teams, IT infrastructure teams, and data analytics teams require:

* + Packet visibility and access into the network
  + Network data from sensors from deployable servers
  + Analytic capability from the hardware and software
  + A user interface typically via their laptops

This Fly Away Kit is designed for mobile IT-forensic analysis. The powerful Forensic Laptop comes with all the necessary equipment for mobile operations. Its housing is designed to easily dissipate the heat created by the processor and the graphics card. This makes it possible to operate both components permanently with a full load, without a break in the number of cycles. Accessories include all Tableau writeblockers and sufficient destination drives to image every medium found out in the field. As with all products from mh-Service, the Fly Away Kit is individually configurable, because we want to have perfectly fitted equipment for the job at hand.

* **Tableau TD2u forensic duplicator features:** The Tableau TD2u is a forensic duplicator capable of performing 1:1, 1:2, and 1:3 duplications. It has many functions traditionally found in general-purpose, IT- oriented hard disk duplicators and provides features and functions that serve the specialized needs of forensic analysis which includes:  
  + Sustained data transfer rates of up to 16 GB/minute, while performing calculations of
  + MD5, SHA-1, and SHA-256 hash values, also known as fingerprints.
  + Native support for USB 3.0, SATA and IDE hard disks from the source interface.
  + Parallel duplication to two SATA and one USB 3.0 destination hard disks.
  + Parallel image and clone duplication.
  + Optional destination disk encryption to ensure security of imaged source data.
  + Detailed log generation for case documentation.
  + Automatic blank checking of source and destination drives.
  + HPA, DCO, and AMA support for the detection and handling of hidden/protected data

areas on source and destination drives.

• Automatic shutdown/standby of idle drives.

• Multi-lingual support for the UI and character input.

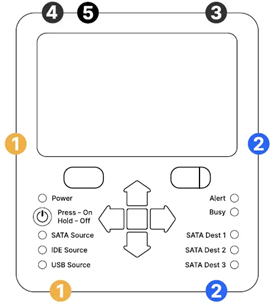
 

Fig: Tableau TD2u forensic duplicato

The Tableau TD2u is only used in preservation and collection phase:

**Phase 1- Preservation:**

The goal of preservation phase in digital forensics is to ensure the integrity and preservation of the original evidence. The Tableau TD2u has a very important role in this by creating a forensic duplicate (forensic image) of the original storage media, for example hard drive or memory card without altering the data on the source drive. The write-blocking feature ensures that no data can be written to the source drive during the duplication process so that the modification of the evidence can be avoided.

**Phase 2- Collection:**

The Tableau TD2u plays an important role in this phase by collecting forensic images from storage media. It assists different sources and destination media such as SATA, USB drives etc, to allow investigators to acquire data from various devices. The TD2u has a high-speed duplication capability that enables investigators to collect forensic images quickly, which is essential when dealing with large volumes of data or time-sensitive investigations.

* **Tableau TX1 Forensic Imager   
    
    
  Fig 1.1 Tableau TX1 Forensic Imager**

Features of Tableau TX1 Forensic Imager:  
  
  
=> Phase 1 Identification:

* The data or content on the storage medium is not identified by forensic write-blocking devices.

=> Phase 2 Preservation:

* When conducting a forensic investigation, a forensic write-blocking device is used to stop data writes or storage medium alterations. The protection of data and preservation of the original evidence are its two key goals. The device prevents any unintentional or intentional alterations to the data on the storage media by restricting write access. Data integrity is ensured by forensic write-blocking technology, which stops unauthorized changes to the original data on storage media. It restricts write access to avoid contamination and unintentional modifications. This preservation guarantees the integrity of the evidence without affecting its admissibility in court, safeguards against malicious activity, and permits read access for investigation. The tool is essential to digital forensics because it guarantees a trustworthy investigative process and upholds faith in the analysis of digital evidence.

=> Phase 3 Preservation:

* Forensic write-blocking devices do not perform any analysis of the data themselves.

=> Phase 4 Documentation:

* The primary purpose of forensic write-blocking devices is not normally to produce documentation. During digital forensics investigations, they serve to block data writes to storage media and preserve the integrity of the original evidence. The usage of a forensic write-blocking device is an essential part of that documentation, which is why it is so critical to the complete digital forensics process. In the case notes, evidence logs, or chain of custody documents, it should be properly noted when a forensic write-blocking device is employed during an investigation.

=> Phase 5 Presentation:

* Forensic write-blocking devices do not perform any presentation functions.

**Tableau Foresic Universal Bridge:**

The Tableau Forensic Universal Bridge is designed to facilitate the examination and acquisition of data from various storage media devices, including hard drives, solid-state drives, USB drives, memory cards, and more. It acts as a bridge between the source drive and the forensic workstation, allowing investigators to access and analyze the content of these devices without altering their original data.

1. **Identification**: Tableau Forensic Universal Bridge is a write-blocker used in digital forensic investigations. It supports six different types of storage media types: USB 3.0/2.0/1.0, PCIe, SATA, FireWire 800/400, IDE, and SAS. Data can be collected through all these types. It offers new features such as PCIe write-blocking, read and write capabilities for all device ports via an internal DIP Switch. [SS6][SS7]
2. **Preservation:** The Tableau T356789iu provides write-blocking functionality, ensuring that the data on the source drive remains unaltered during the acquisition process. It supports multiple storage media types, allowing forensic investigators to preserve data from various devices. [SS6][SS7]
3. **Analyze:** This device does not provide any specific feature to analyze the data on the device itself.
4. **Documentation and Presentation:** It is necessary to maintain acquisition logs for hardware tools during documentation. Maintaining detailed logs of all data acquisitions made using the hardware tool. It is also required to include information such as the date and time of acquisition, the source drive details, the destination of the acquired data, and the examiner's name. Also, Associating the hardware tool's documentation with specific case information, including the case number, the nature of the cybercrime investigation, and the target devices or storage media to be examined. [SS6][SS7]

**Tableau Write Blocker Kit**

Tableau Write Blocker Kit represents a critical advancement in the field, addressing the complex challenges of handling and preserving digital evidence. This kit not only streamlines the investigation process but also ensures the integrity and admissibility of evidence, maintaining the highest standards of accuracy and reliability.

***Phase 1: Identification***

The Tableau Write Blocker Kit plays a pivotal role in this aspect, offering compatibility with a wide range of storage devices, including hard drives, solid-state drives, and USB drives. By establishing a secure connection between the suspect's device and the forensic workstation, the write blocker allows investigators to access and examine digital evidence without altering or contaminating the original data. This ensures that the evidence collected is authentic and untainted, establishing a strong foundation for the subsequent phases.

***Phase 2: Preservation***

The Tableau Write Blocker Kit deals with this issue with its proprietary write-blocking capability, which blocks any data changes on the associated storage devices. By acting as an intermediate, the kit ensures that no written instructions are executed, preserving the evidence's clean status. This method creates a verifiable chain of custody, guaranteeing the court that the evidence is authentic and has not been tampered with.

***Phase 3: Analysis***

This device does not provide any specific feature to analyze the data on the device itself.

***Phase 4: Documentation***

The Tableau Write Blocker Kit aids investigators in producing thorough and accurate reports. Investigators can create an unambiguous trail of their examination process by painstakingly noting all actions taken, such as device connections, data collections, and instructions run. The extensive documentation also aids in peer evaluations, collaborative efforts, and, most crucially, legal actions, strengthening the investigation's results' credibility and defensibility.

***Phase 5: Presentation***

The Tableau Write Blocker Kit assures that the evidence gathered is admissible in court, enhancing the investigator's credibility and the case's strength. The kit enables investigators to confidently deliver their results without fear of criticism or controversy because it maintains data integrity from the start. Furthermore, its connection with top forensic software simplifies data visualisation and aids in the creation of compelling presentations that appeal to judges, juries, and other stakeholders.

**Forensic laptops:**

A forensic laptop, often known as a forensic workstation, is a specialized computer system developed for digital forensic investigations. It is a powerful and secure tool used by forensic analysts and investigators to do data analysis, evidence collecting, and examination of digital devices in a controlled and forensically sound manner. These laptops are provided with hardware and software capabilities that protect the integrity and preservation of evidence during the investigative process.

Identification

Forensic laptops have unique characteristics for data gathering and identification while preserving data integrity with write-blocking capability. These computers are offered by reputable companies like Tableau and Guidance Software.

Processing

Forensic laptops, which are equipped with analysis tools such as EnCase, FTK, X-Ways Forensics, and Cellebrite UFED, assist investigators in evaluating and retrieving critical data. Data integrity is ensured by hashing algorithms like SHA-1, MD5, and SHA-256. AccessData specialises in FTK-equipped forensic laptops.

Analysis

Forensic software enables in-depth data analysis, recovering deleted files, analysing information, constructing timelines, and doing keyword searches. Operating in discrete environments ensures the integrity of the investigation. Cellebrite laptops excel at mobile device data extraction.

Reporting:

Forensic laptops allow for the development of detailed reports and the systematic presentation of evidence to stakeholders and legal specialists. Secure boot and encryption secure data while maintaining confidentiality and investigation integrity.

Significance:

Forensic laptops are essential tools for digital analysts who follow industry standards and best practises. They create a dependable framework for evidence processing, assisting in cybercrime prevention and successful data analysis.

**Comparing tools based on domains:**

Device Forensic Tools:

|  | EnCase | FTK Imager | Osforensic | Autopsy | Foremost | Sleuth Kit |
| --- | --- | --- | --- | --- | --- | --- |
| Open-source |  |  |  | ✓ | ✓ | ✓ |
| GUI | ✓ |  | ✓ | ✓ |  |  |
| Forensic Imaging | ✓ | ✓ | ✓ | ✓ |  | ✓ |
| Disk and File Analysis | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Hash Calculation | ✓ | ✓ | ✓ | ✓ |  |  |
| File Carving | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Keyword Searching | ✓ | ✓ | ✓ | ✓ |  | ✓ |
| Registry Analysis | ✓ | ✓ | ✓ | ✓ |  |  |
| Email Analysis | ✓ | ✓ | ✓ | ✓ |  | ✓ |
| Reporting | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Disk & Memory Capture | ✓ | ✓ | ✓ | ✓ |  |  |
| Write Blocking | ✓ | ✓ | ✓ | ✓ |  |  |
| Integration with Tools | ✓ | ✓ |  | ✓ | ✓ | ✓ |
| Data and file recovery | ✓ |  | ✓ | ✓ | ✓ | ✓ |
| Give real time alert | ✓ |  |  | ✓ |  | ✓ |
| Give slack space |  |  | ✓ | ✓ |  | ✓ |
| Conduct live analysis | ✓ |  |  | ✓ |  | ✓ |
| Malware Detection |  |  | ✓ |  |  |  |
| Social Media Analysis |  |  |  | ✓ |  |  |
| Encryption Analysis | ✓ |  |  | ✓ |  |  |
| Cloud Service Forensics | ✓ |  | ✓ | ✓ |  |  |
| Mobile Device Forensics | ✓ |  | ✓ | ✓ |  |  |
| User Activity Visualization |  |  | ✓ | ✓ |  |  |

Network:

|  | Wireshark | Nmap | Tcpdump | Network miner | Xplico |
| --- | --- | --- | --- | --- | --- |
| Open-source |  | ✓ |  | ✓ | ✓ |
| GUI |  | ✓ |  | ✓ | ✓ |
| Live data acquisition |  |  |  | ✓ | ✓ |
| Automatic decoding |  |  |  | ✓ | ✓ |
| Packet capture analysis |  |  |  | ✓ | ✓ |
| Analysis of encrypted SSL traffic |  |  |  | ✓ |  |
| Multithreading |  | ✓ |  |  | ✓ |
| Modularity |  | ✓ |  |  | ✓ |
| Realtime elaboration |  |  |  |  | ✓ |
| Reporting |  | ✓ |  | ✓ | ✓ |
| Intrusion detection |  | ✓ |  | ✓ | ✓ |
| Advance OS Fingerprint |  | ✓ |  | ✓ |  |
| Protocol Parsing |  | ✓ |  | ✓ |  |
| Network Visualization |  |  |  | ✓ |  |
| Output data and information in SQLite database or MySQL database and/or files |  | ✓ |  |  | ✓ |

Memory:

|  | Sleuth Kit | Volatility workstation | Exiftool |
| --- | --- | --- | --- |
| Network Forensics | ✓ | ✓ | ✓ |
| Malware Analysis | ✓ | ✓ | ✓ |
| Incident Response | ✓ | ✓ | ✓ |
| Digital Forensics | ✓ | ✓ | ✓ |
| Root Cause Analysis | ✓ | ✓ | ✓ |

Hardware tools:

|  | Fly Away Kit (mh) | Forensic Laptop (mh) | Forensic Van (mh) | E. Tableau TX1 Forensic Imager | Tableau TD2U Forensic Duplicator | Tableau Forensic Universal Bridge | CRU Write blocker | Tableau Write blocker Kit |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Parallel image and clone duplication |  | ✓ | ✓ |  | ✓ |  |  |  |
| Optional destination disk encryption |  | ✓ | ✓ |  | ✓ |  |  |  |
| Detailed log generation for case documentation |  | ✓ | ✓ |  | ✓ |  |  |  |
| Automatic blank checking of source and destination drives |  | ✓ | ✓ |  | ✓ |  |  |  |
| Automatic shutdown/standby of idle drives |  | ✓ | ✓ |  | ✓ |  |  |  |
| Multi-lingual support for the UI and character input. |  |  | ✓ |  | ✓ |  |  |  |
| Facilitate read-only access to digital evidence |  | ✓ |  |  |  | ✓ |  | ✓ |
| Write blocking |  | ✓ |  |  |  | ✓ |  | ✓ |
| Integrity Preserving |  | ✓ | ✓ |  |  | ✓ |  | ✓ |
| Crime Scene Assessment tools (Camera, Tripod, marker, tapes, flashlight, etc) | ✓ |  |  |  |  |  |  |  |
| Fingerprint kits (brushes, powder, lifting tape) | ✓ |  |  |  |  |  |  |  |
| biological sample collection (Swab) | ✓ |  |  |  |  |  |  |  |
| Forensic casting materials (plaster of Paris) | ✓ |  |  |  |  |  |  |  |
| Presumptive drug test kit | ✓ |  |  |  |  |  |  |  |
| Gunshot residue kit | ✓ |  |  |  |  |  |  |  |
| Decontamination supplies | ✓ |  |  |  |  |  |  |  |
| Tamper-evident evidence seals | ✓ |  |  |  |  |  |  |  |
| Anti-static bags for electronic evidence | ✓ |  |  |  |  |  |  |  |

Identify:

* software :
* Hardware:

Process:

* software :
* Hardware:

Analyze:

* software :
* Hardware:

Report

* software :
* Hardware:

**Recommendation**: pranto

The project primarily compared selective digital forensic tools based on their domain and functionalities, with limited usage of real-world case scenarios. While this method allows for a systematic assessment of the tools' capabilities, it is not without limits. Without real-world context and meaning, the findings may be inadequate. Since, digital forensics frequently involves complicated and dynamic situations, the project's capacity to demonstrate the tools' usefulness in practical investigations may be limited by the lack of actual events. Furthermore, the evaluation may fail to adequately take into account performance changes while dealing with specific sorts of scenarios or challenges. However, the study offers useful insights into the tools' strengths and weaknesses depending on their features, aiding users in selecting the best solutions for their digital forensic requirements. Future studies could add real case data to this analysis to evaluate and apply the findings to real-world situations, increasing the project's applicability and value to the digital forensic community.

Limitations and Challenges:

Digital forensics and cybersecurity both make extensive use of the techniques and technology you highlighted. It's crucial to remember that every instrument has unique restrictions and difficulties. Here is a list of some of the drawbacks and difficulties related to the tools you mentioned:

**Encase**: Privately held software, which might result in expensive license fees.

Its intricacy creates a learning curve for new users.

limited support for some platforms and file systems.

can demand a lot of resources and strong gear.

**Forensic Workstation**: Putting together a special forensic workstation might be expensive.

To stay up with the rapid advancement of technology, regular maintenance and upgrades are required.

**NetworkMiner**: May not be able to successfully gather encrypted network traffic.

little assistance with some network protocols and file types.

**Kit for Tableau Write Blocking:**

Physical restrictions since it's made for specific kinds of storage media.

Not all devices or storage media types may be compatible.

User interface might be intimidating for newcomers, autopsy.

More technical knowledge may be needed for advanced functionality.

When working with huge datasets, performance problems might occur.

**Forensic Van**: Expensive to set up and maintain.

Possibility of logistical issues with regard to accessibility and location.

A commercial tool with license fees is the "FTK" (Forensic Toolkit).

systems and file types with limited support.

For new users, the interface might be complicated.

**tcpdump**: Needs command-line experience and knowledge of networking principles.

be ineffective in capturing compressed or encrypted data.

Issues with specific devices and storage media types due to the CRU Write Blocker.

Physical restrictions on the supported connection types.

Issues with specific devices and storage media types due to the CRU Write Blocker.

Physical restrictions on the supported connection types.

**Sleuth Kit**: Less technical users may find the command-line interface difficult to use.

Some of the kit's tools need to be manually set up and configured.

Volatility Workstation: Mainly utilized for advanced memory analysis.

requires knowledge of the internal workings of the operating system and of memory architecture.

**ExifTool**: Non-technical users may find the command-line interface intimidating.

restricted to using metadata and excluding content analysis.

Nmap: Networking expertise is necessary for results interpretation.

Security warnings might be triggered, or intrusion detection systems could pick it up.

**Xplico**: Network traffic analysis is its main area of expertise, not thorough forensic investigation.

limited support for specific formats and protocols.

First and foremost: File carving and recovery are the main uses, not in-depth examination.

**Conclusion**: In conclusion, our project investigated a variety of prominent forensic tools that are critical in digital investigations. Each tool given has its own set of capabilities that are customized to the various needs of forensic analysts and investigators. Our journey began with an informative introduction to the world of forensic tools, emphasizing their critical role in locating digital evidence and assisting in investigation processes. We investigated the significance of these technologies in numerous fields, including law enforcement, cybersecurity, data recovery, and others. Following that, we thoroughly analyzed each tool, providing a comprehensive review of its features and functionalities. We identified the various characteristics that each tool brings to the table, from the sturdy EnCase to the dynamic Autopsy, from the analytical capability of FTK to the open-source potential of Osforensic. This in-depth examination allowed us to appreciate the complexities of their architecture and understand their applicability for various forensic endeavors. We extensively analyzed different elements of these tools in our attempt to compare them, ranging from their open-source nature and user-friendly GUI to their prowess in hash computations, network analysis, and more. We recognized the broad range of capabilities they provide, appealing to both novice and experienced investigators. This contrast allowed them to have a better grasp of their various areas and the distinct demographics they serve.

No tool, however, is without restrictions and obstacles. We investigated these elements, realizing that even the most modern solutions have flaws that need to be addressed. The study highlighted the importance of ongoing innovation in the forensic scene, which is fuelled by the ever-changing digital ecosystem and rising data complexities. Our investigation into these forensic instruments confirmed their critical function in modern investigative practices. They serve as sentinel partners for individuals attempting to navigate the difficult world of digital evidence, assisting in the decoding of complex data puzzles, unraveling riddles, and ensuring justice is served. Throughout the phases of our project, we are reminded that digital forensics is a dynamic field in which innovation is critical. We've made considerable progress in the art and science of digital exploration by learning about these tools, their features, and their limitations. As we embrace technology's ongoing evaluation, the extended capabilities of these tools will open the door to revealing even more possibilities in tackling the ever-increasing complexities of cybercrime case studies.

References:

[1]. N. Hamad, D. Eleyan, “Digital Forensics Tools Used in Cybercrime Investigation – Comparative Analysis”, esearchGate, Pub. 360463703, May 2022

[2]. “Introduction of Computer Forensics”, Available:https://www.geeksforgeeks.org/introduction-of-computer-forensics, [Accessed: July-2022]

[3]. “Tableau TD2U Forensic Duplicator User Guide.” *OpenText*, https://www.opentext.com/assets/documents/en-US/pdf/opentext-tableau-td2u-forensic-duplicator-user-guide-en.pdf. Accessed 5 August 2023.

[4]. Erhan AKBAL, Şengül DOĞAN, “Software and Hardware Tools used in Digital

Forensic Data Analysis”, SEEK DIGITAL LIBRARY,2016

[5]. SOURCEFORGE, "Foremost," [Online]. Available: <https://foremost.sourceforge.net/>.

[6]. S. V. N. Parasram, "File Recovery and Data Carving with foremost, Scalpel, and bulk\_extractor," in *Digital Forensics with Kali Linux - Second edition*, Packt, 2020, p. 335.

[7]. S. V. N. Parasram, "Chapter 10: Analysis with Xplico," in *Digital Forensics with Kali Linux - Second Edition*, Packt, 2020, p. 334.

[8]. Xplico – About", Xplico.org, 2016. [Online]. Available: http://www.xplico.org/about.

[9] Bennett DJ, Stephens P. A Usability Analysis of the Autopsy Forensic Browser. HAISA. 2008:105-15.

[10] Bennett DJ, Stephens P. A cognitive walkthrough of autopsy forensic browser. Information Management & Computer Security. 2009 Mar 20;17(1):20-9.

[11] Galvão RK. Computer Forensics with The Sleuth Kit and The Autopsy Forensic Browser. The International Journal of FORENSIC COMPUTER SCIENCE. 2006;1:41-4.

[12] Adamu H, Ahmad AA, Hassan A, Gambasha SB. Web browser forensic tools: Autopsy BHE and net analysis. Int. J. Res. Innov. Appl. Sci.. 2021;6(5):103-7.

[13] Carrier B. Performing an Autopsy examination on FFS and ext2fs partition images. InInSANSFIRE 2001 Conference 2001.

[14]<https://concordia.udemy.com/course/become-a-digital-forensics-investigator-with-autopsy/learn/lecture/32972448#overview>

[15] <https://www.mh-service.de/en/products/mh-service-systems/>

[16] “Carving - SleuthKitWiki.” Sleuthkit Wiki, 9 March 2013, https://wiki.sleuthkit.org/index.php?title=Carving. Accessed 5 August 2023.

[17] “The Sleuth Kit Overview and Automated Scanning Features.” OSDFCon, 9 June 2010, https://www.osdfcon.org/presentations/2010/carrier-sleuthkitoverview.pdf. Accessed 5 August 2023.

[18] “Tableau TD2U Forensic Duplicator User Guide.” OpenText,

https://www.opentext.com/assets/documents/en-US/pdf/opentext-tableau-td2u-forensic-duplicator-user-guide-en.pdf.

Accessed 5 August 2023.

[19] “opentext TD2u Tableau Forensic Duplicator User Guide.” device.report,

https://device.report/manual/5468606. Accessed 5 August 2023.

[20] Effectiveness of OSForensic in Digital Forensic Investigation to Curb cybercrime (Bandr Siraj Fakiha)(<https://medicopublication.com/index.php/ijfmt/article/view/15633/14014>)

[2]1. A Comparative Analysis of OS Forensics Tools(Venkata Ravi Kiran Kolla) (<http://surl.li/juoqt> )

[22].OSForensics by PassMark™ Software (<https://jarnobaselier.nl/files/pdf/OSForensics/OSF_help.pdf>)

[23]. <https://www.hackingarticles.in/digital-forensics-investigation-using-os-forensics-part1/>

[24] https://www.mh-service.de/en/products/forensic-laptop/

[25] <https://sumuri.com/hardware/forensic-laptop/>  
1) <https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>  
2) <https://www.wireshark.org/>  
3) https://www.techtarget.com/whatis/definition/Wireshark   
4) https://en.wikipedia.org/wiki/Wireshark  
5) https://www.networkworld.com/article/3663021/what-is-wireshark.html   
6) <https://github.com/wireshark/wireshark>  
7) https://digitalintelligence.com/storeproducts/d6280 2)   
8) https://sumuri.com/product/tableau-forensic-imager-tx1-kit/ 3)   
9) https://www.availforensics.com/Tableau-TX1-Forensic-Imaging-Kit-with-case-AF-MT-TX1

[E1]. “EnCase Forensic v8.07 User Guide”, Available :https:// [Encase Forensic V8.07 User Guide.pdf [ylygg2762zlm] (idoc.pub)](https://idoc.pub/documents/encase-forensic-v807-user-guidepdf-ylygg2762zlm), [Accessed: July-2022]

## [F2]. “AntAnalyzer – High end & extremely fast forensic workstation”, Available:// [AntAnalyzer - MH Service (mh-service.de)](https://new.mh-service.de/en/products/antanalyzer/), [Accessed: July-2022]

[SS1] Qureshi, Sirajuddin, et al. “Network Forensics: A Comprehensive Review of Tools and Techniques.” International Journal of Advanced Computer Science and Applications, vol. 12, no. 5, 2021. DOI.org (Crossref),<https://doi.org/10.14569/IJACSA.2021.01205103>.

[SS2] Ghabban, Fahad M., et al. “Comparative Analysis of Network Forensic Tools and Network Forensics Processes.” 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), IEEE, 2021, pp. 78–83. DOI.org (Crossref),<https://doi.org/10.1109/ICSCEE50312.2021.9498226>.

[SS3] Nmap: The Network Mapper - Free Security Scanner. https://nmap.org/. Accessed 5 Aug. 2023.  
[SS4] Passive Fingerprinting - an Overview | ScienceDirect Topics. https://www.sciencedirect.com/topics/computer-science/passive-fingerprinting#:~:text=The%20active%20process%20that%20Nmap,reveal%20subtle%20nuances%20in%20response. Accessed 5 Aug. 2023.  
[SS5] Liao, Si, et al. “A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments.” 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), IEEE, 2020, pp. 64–71. DOI.org (Crossref), <https://doi.org/10.1109/CyberC49757.2020.00020>  
[SS6] Tableau Forensic Universal Bridge (T356789iu) – e-Forensic Services. https://e-forensic.ca/products/tableau-forensic-universal-bridge-t356789iu/. Accessed 5 Aug. 2023.  
[SS7] Lyle, James R. “A Strategy for Testing Hardware Write Block Devices.” Digital Investigation, vol. 3, Sept. 2006, pp. 3–9. DOI.org (Crossref), https://doi.org/10.1016/j.diin.2006.06.001.