QUALITATIVE ASSESSMENT OF DIGITAL FORENISC TOOLS

S. Singh[1] and S. Kumar[2]
Ambedkar Institute of Advanced Communication Technologies& Research, Delhi, India
[1]010sakshisingh@gmail.com, [2]sureshpoonia@aiactr.ac.in

ABSTRACT

Forensic science is a study of science to criminals and civil laws. Digital forensics is the part of forensic science relating to proof found in computers and advanced storage media. Forensic examiners gather, protect and break down logical confirmations over the span of examination. Digital information contains data as content, pictures, sound, video and so on. These days numerous cybercrime cases, for example, hacking, banking cheats, phishing, email spamming, etc., have developed which are connected with a computerized information. Since the digital investigation is turning into an expanding concern, numerous digital forensic tools have been created to manage the difficulties of exploring computerized wrongdoings. The motivation behind digital forensics strategies is to look, protect and extract data on advanced frameworks to discover potential confirmations to exhibit them in the courtroom. In this paper, we have discussed five kinds of forensics namely Network Forensics, Live Forensics, Cyber Forensics, Database Forensics, and Mobile Forensics. The paper depicts a list of digital forensic tools in detail and looks at them based on the characterized parameters to figure out which tool suits better for any investigation. The paper looks at network, database and mobile forensic tools and examines the silent features and uniqueness of each of the tools along with their functionalities.

Keywords: Database forensics, Digital forensic tools, Forensic phases, Mobile forensics and Network forensics

Introduction

Digital forensics is the utilization of investigation and analysis strategies to assemble and secure proof from a certain computerized device in a manner that is reasonable for introducing in an official courtroom. The purpose of digital forensics is to perform a structural investigation while maintaining a reputed chain of evidence to uncover what exactly happened on a digital device and who was responsible for it. We can say that digital forensics is a logical methodology of safeguarding, procuring, extracting, removing and representing evidence that originates from the advanced sources like PC, mobile, camera and so forth.

Digital forensic incorporates a few sub-branches with the investigation of different sorts of devices, media or artifacts. These branches are:

1. Network Forensics
2. Live Forensics
3. Cyber Forensics
4. Database Forensics
5. Mobile Forensics

Since there are number of digital forensic branches but we are working on Network forensics, Database forensics and Mobile forensics in this paper.

Network Forensics: Network forensics is a branch of advanced digital forensic identifying with the observing and investigation of computer system traffic to collect network traffic data, legitimate proof or interruption recognition. The significant objective of the forensics of the network is to gather proof from the network traffic. It attempts to investigate traffic information collected from various websites and network equipment, for example, IDS and firewalls. It screens on the system to distinguish assaults and examine the idea of attacks. It is also the way of distinguishing interruption examples concentrating on attackers' exercises. Network forensic manages unstable and dynamic data.

Database Forensics: Database forensic is the part of digital forensic and its database legal investigation and related metadata. It focuses on experimentally interrogating the

failed database and by attempting to remake the metadata and page data from inside an informational index. In this digital forensic, the read-only technique is utilized when interfacing with a database to guarantee that no information is undermined.

Mobile Forensics: Mobile forensics is the recovery research of computerized proof from a cell phone under forensic conditions. The objective of mobile crime scene investigation is the act of using sound philosophies for the securing of information contained inside the internal memory of a cell phone and related media giving the capacity to precisely report one's discoveries. Mobile device forensics is an advancing claim to fame in the field of computerized legal sciences. The procedure of Mobile device forensics is separated into three fundamental classes namely, a seizure that preserves the proof, Acquisition which is the way toward recovering the information from the gadget and the third one is an assessment that examines the recovered information.

The paper is structured as follows: Section 2 covers the previous comparative analysis and work done related to digital forensics. Section 3 digital forensic process is described with various phases. Section 4 covers the methodologies followed during the comparative analysis. Section 5 gives a detailed description of forensic tools that are categorized into network forensics, database forensics, and mobile forensics. Section 6 presents all the identified parameters based on which the comparative analysis is done. Section 7 consists of a comparative analysis table of all the selected tools and Section 8 describes the conclusion and future work.

Literature Review

Numerous authors have given a relative investigation of various forensic tools. Mayank Lovanshi and Paritosh Bansal [1] clarified a comparative study on digital forensic tools, for example, desktop, live and network forensic tools based on the parameters like imaging, seizer, packet-sniffing and so on. Khaleque Md Aashiq Kamal [2] looked at memory forensic Tools based on-time processing and left artifacts of volatile memory. He analyzed the variation in Tool time processing in terms of distinct volatile memory size. With his experimentation, he proved that the processing time ’x’ of the tool does not increase by expanding the memory size 'x' times. S Mc Combie and M. Warren [3] focuses on different methodologies to characterize computer forensics at the most fundamental level. They additionally depicted various models like the Lucent model, KPMG model, Miter model, etc. and methodologies that have been created in computer forensic fields. Pratima Sharma[4] played out an experiment using a prodiscover tool to decrease the search space by recognizing and separating the known documents to accelerate the searching procedure of evidence identification. She looked into the image files to know the area of interest within documents, erased records, and slack documents. The experimental result demonstrated that REGEX looks empowered to get yield with only one hunt rather than numerous endeavours in less time. Varsha Sanap and Vanita Mane [5] displayed a correlation of three scientific instruments WinHex, Active record Recovery and Prodiscover Basic based on the parameters, for example, document assessment, log assessment, memory dump investigation and so on. They additionally explored a contextual investigation of pornography. Priyanka Dhaka and Rahul Johari [6] proposed a thought and strategy of utilizing digital- crime investigation tool to extract the information which produced a record and sent the information in big data tool, for example, MongoDB to oversee enormous information and removed the structured informational collection. Hamda Bariki, Mariam Hashmi and Ibrahim Baggili [7] present a standard information prerequisite for digital evidence products that could be used with computer forensic tools to create reports. The principles

proposed secure the essential data on the case, the sources of evidence, the intrigue and the custody chain of digital evidence. The author Charles Lim, Meily, Nicsen and HerryAhamdi[8] did experimental research that aimed to reveal the rest of the data inside USB flash drives. The exploration demonstrated that there were plentiful delicate data recouped from the USB flash drives and the data was related to the educational institute, individual and government.

Digital Forensic Process

The digital forensic process has the following eight components-

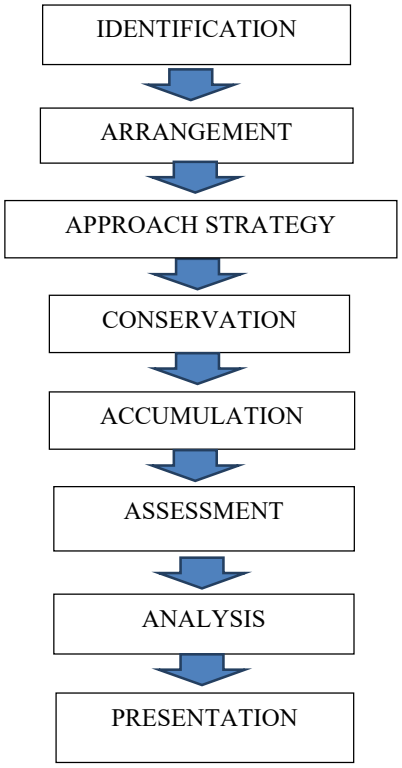

Figure 1: Digital Forensic Phases

a. **Identification Phase:** In this stage, the evidence and their locations are recognized from the digital sources. It principally deals with the detection of incidents, the accumulation of proofs and monitoring of the evidence.

b. **Arrangement Phase:** In the arrangement stage, the choice and preparation of tool, methods, court orders and backing of the executives are pictured.

c. **Approach Strategy:** In this stage, the improvement of the technique that will amplify the accumulation of untainted proof while limiting the effect to the victim is done.

d. **Conservation Phase:** In this stage, isolation, verifying and saving of the condition of physical and digital evidence takes place.

e. **Accumulation Phase:** In this stage, the chronicle of the Physical scene, use of standardized and duplicated digital evidence and acknowledged method takes place.

f. **Assessment Phase:** An efficient inquiry of proof recently gathered is finished in this phase.

g. **Analysis Phase:** In this stage, the confirmations are analyzed using digital forensic tools and determine the important data. It gathers the gained information and analyze it to discover the bits of confirmations. This stage also recognizes that the framework was tempered.

h. **Presentation Phase:** In this stage, extracted data and other metadata are accounted for after the fulfillment of the investigation. This stage is based primarily on cyber laws and provides the findings for the investigation's respective proof.

Various process models are proposed by different authors:

- DFaaS Process Model, 2014
- Integrated Digital Forensic Process Model, 2013
- The Advanced Data Acquisition Model (ADAM), 2012
- The Systematic Digital Forensic Investigation Model (SRDFIM), 2011

- The Digital Forensic Investigation Framework, 2008
- The Two- Dimensional Evidence Reliability Amplification Process Model, 2008

Digital Forensics: Case Study from India

In the trial, the accused served in a BPO that managed the activities of a global bank [9]. During the process of their research, the accused had collected personal identification numbers (PIN) and other confidential information from the clients of the bank. With these, the accused and the accomplices, through various internet cafes, diverted large sums of money from specific clients' accounts to false accounts.

Investigation

Following receipt of the lawsuit, the entire business structure of the plaintiff company was analyzed and a network review was performed to assess the possible source of the data theft. The police were successful in capturing two suspects because they had placed a trap in a local bank where the accused had fake accounts for unlawfully transferring money.

During the inquiry, the BPO device file logs were retrieved. The IP addresses were traced back to the Internet service provider and, eventually, to the cyber cafes through which illicit downloads were made.Registers held in cyber cafes and cyber cafe operators helped to recognize the other defendants in the trial. Email IDs and phone call printouts were also collected and analyzed to assess the identities of the suspects. The records of the detained accused were scanned, and provided crucial details to identify the other accused. Some of the accused's mail accounts contained fast codes that were needed for Internet money transfer.

All 17 of the suspects in the case were charged within a brief amount of time the indictment sheet was sent to the court within a prescribed period of time. An amount of around INR 19 million has been allocated to the whole wire transfer scheme.

The event received the Indian Cyber Cop Award for Investigation Officer Mr. Sanjay Jadhav, Assistant Commissioner for Police Crime, Pune Police. The panel of judges held the opinion that this case was the most important case for the Indian IT industry in 2005 and was prosecuted in a competent manner, with a considerable portion of the swindled funds being immobilized, a vast number of persons convicted and the matter referred to the court for trial within 90 days.

Methodology

The approach adjusted focus on the investigation of various computerized criminological tools as talked about in the previous sections. These devices portray different functionalities. In our study, we pursue a procedure as discussed in Fig. 2. The initial phase in the process includes the choice of tool. The following stage-manages the extraction of features which helps us in distinguishing the parameters. The last step compares the tools based on parameters.

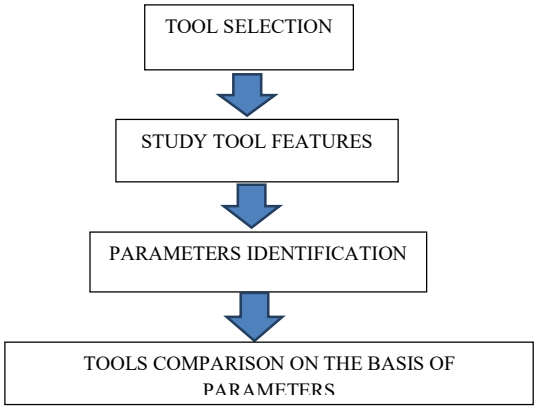

Figure 2: Flow Chart of Strategy

Digital Forensic Tools

The digitalization of the world is getting all the more dominant step by step. So the field of digital forensic is additionally developing extremely quickly. In this segment, we will talk about three digital forensic tools under their respective categories:

1. Network Forensics

Network Forensic is the field of Digital criminology where the investigators focus on packets travelling in a network and the details of the computer systems connected to that network. Following are the tools to test the network forensic applications:

1.1 Wireshark

Wireshark is free and analyzer of open source network protocols that empowers the investigator to intelligently browse the computer network data traffic [9]. The author of Wireshark is Gerald Combs and created by the Wireshark group. It catches live information from a network interface [11]. It captures traffic and converts it into a readable arrangement. This makes simple to recognize how much traffic crosses the network, how often and how much latency there is between some hops and so on. Wireshark supports over 2,000 network protocols. Live information is perused from various kinds of the network like IEEE 802.11, Ethernet, PPP (Point-to-Point Protocol) and loopback [12]. Wireshark colors data packets to assist the client by identifying the sorts of traffic.

The various features that make Wireshark stand differently are:

a. **Decoding packets and exporting objects:** Wireshark has a powerful feature of decoding the captured packets into the client's readable format. It also export captured objects as packet streams which helps in retrieving the different file types downloaded during packets capturing.

b. **Captured packet statistics:** Wireshark can generate an overview of network activities statistically. The various tools that come under the statistics menu option are, summary that returns a quick report about the entire capturing process; protocol hierarchy presents statistical information about various protocols seen during network analysis; and flow graphs that represent timeline-based communication statistics of the captured packets [13].

c. **Name resolution:** The identified address is converted into an understandable format and the process is called name resolution. Various name resolution tools are Network name resolution, MAC name resolution, and transport name resolution.

d. **Packet Assembling:** The process of transferring large chunks of data by splitting it into smaller packets and later combining them again to form the complete data is called packet assembling. This is done to reproduce the captured packet efficiently [13].

e. **Color Coding:** Wireshark has customized coloring rule which is applied to the captured packets for quick and effective analysis. It highlights the packets of interest.

1.2 Nmap (Network Mapper)

Nmap is a network scanner used by sending packets and reviewing replies to find host and equipment on a computer network [13]. The developer of Nmap is Gordon Lyon (Fyodor). It identifies the open ports on target hosts and interrogates remote network facilities to determine the name and version number of the application. It also helps to identify the operating system (OS).

Various features of Nmap are:

a. **Network mapping**: Nmap identifies the devices connected to the network which is known as host discovery. It also detects the servers, switches, and routers and identifies how they are physically connected.

b. **Operating System Detection:** Nmap detects the connected operating system to the network. The detection process is called OS fingerprinting. It provides the details of the operating system like software version, vendor's name.

c. **Service Discovery:** Nmap can also detect services like HTTP, telnet, SMTP running on the connected systems and identifies their applications and versions.

d. **Security Auditing:** Since Nmap can detect the versions of OS, it helps the network manager to determine the vulnerabilities and loopholes in the network that may harm in the future.

e. **Port scanning:** Nmap scans the ports available on the network and identifies their status based on the response received for an SYN (synchronization) request. Six port states are perceived by Nmap namely closed, open, unfiltered, filtered, closed|filtered and open|filtered.

1.3 NESSUS

Nessus is a vulnerability scanner for open-source networks that uses the normal vulnerabilities and architecture of the exposition. It has a web-based interface that contained a web customer and a simple HTTP server. It does not require any software installation apart from the Nessus server. It can distinguish potential vulnerabilities in the frameworks [14]. It incorporates configuration reviewing, resource profiling, rapid discovery, and delicate information revelation and defenselessness analysis of a security act. It is created by Tenable. Inc.

The principle highlights of Nessus are:

a. **Remote security and local security:** Nessus can distinguish not only the distant host defects on the network but the missing patches and nearby defects too.

b. **Updated safety for the database**: The Nessus safety check can be retrieved by using the Nessus-update-modules path.

c. **NASL:** NASL (Nessus Attack Scripting Language) is included in Nessus to compose safety tests rapidly.

d. **Smart administration acknowledgment**: Nessus can differentiate between a non-standard port running FTP server and the internet server port 8080.

e. **Full SSL support:** The tool has the capacity testing SSLizied administrations, for example, HTTPS, SMTP, IMPS and can even be provided with a certificate so it can very well coordinate with PKI type condition.

1.4. Xplico

Xplico is a Network Forensic Analysis Tool (NFAT) which is an application that reproduces the acquisition contents conducted with a packet sniffer. It is created by Giauluca Costa and Andrea de Franceshi. The objective of Xplico is to extract web traffic to catch the application's information it contained. It permits simultaneous access by various investigators. The tool analyzes web packet and catches them to remove and parse certain protocols and return web action, for example, VoIP, email and HTTP [15]. The Xplico framework underpins various protocols with the most steady being: HTTP, ARP, SMTP, PPP, SIP, VLAN, DNS, IPv4, IPv6, TCP, UDP, FTP and so on. To prevent protocol misidentification, every application protocol is recognized using Port Independent Protocol Identification (PIPI).

The scientific necessities for Xplico are characterized as pursues:

a. To distinguish between various hubs on the network.

b. To gather information precisely as it was seen "on the network".

c. To parse the information into a format that does not "lose" data.

d. To enable the analyst to see any parsed output in the applicable setting.

2 Database Forensics

Database forensic is the part of advanced digital forensic that manages the

investigation of databases and distinguishes the reason for failure. Following are the tools to test the database forensic applications:

2.1Cuckoo Sandbox

Cuckoo sandbox is an automated malware investigation system. It is utilized to consequently test and extract records and gather exhaustive investigation results that Specify what the malware does in an isolated operating system. The originator and core developer of Cuckoo Sandbox is Claudio Guarnieri in 2011.

It can recover the accompanying kinds of results:

a. Traces of calls made by all malware-generated processes.

b. Files produces, deleted and downloaded during the implementation of the malware.

c. Malware memory dumps

d. Network traffic follow in PCAP format

e. Screenshots taken during malware implementation

f. Complete memory dumps of the computer.

Cuckoo is intended to be an independent application just as to be incorporated in bigger structures. It tends to be utilized to extract DLL records, generic windows executable, PDF archives, URLs and HTML documents, Microsoft Office reports, Visual Basic (VB) scripts, PHP scripts [16] and so forth. Cuckoo sandbox comprises a focal administration programming that handles test execution and investigation. Cuckoo's foundation's main sections are a host machine (the software for administration) and multiple guest machines (for inquiry, virtual or physical machines). The Host runs the central section of the sandbox that deals with the whole inquiry process, while the Guests are in an isolated environment where the samples of malware get performed and analyzed.

2.2 ForensicToolKit (FTK)

Forensic Toolkit (FTK) is a computerized inquiry phase designed to support the job of experts working in the field of data security, innovation, and law permission. It is created by AccessData. It can acquire and analyze digital devices, for example, computer hard drives, flash memory devices, USB drives, cell phones, tablets, and other advanced media [17]. Its approach is linked to a method called post- mortem computer forensics that occurs when the computer has been turned off. It makes exact copies (forensic images), known as bit-to-bit or bitstream, to ensure the honesty of the information collected. It generates pictures and processes a broad variety of data types that shape forensic pictures into email archives, conducts an inquiry, analyzes the registry, decrypts files, cracks passwords, and produces a single solution report.

The real capacities FTK incorporate are:

a. **Email Analysis**: The tool provides forensic experts with an intuitive e-mail investigation interface. It includes particular word parsing messages, header reviews for the IP address of the source, and so on.

b. **File Decryption**: the most well-known use of the product is a key component of FTK file decoding. Whether breaking the password or decoding whole documents. FTK can recover passwords for over a hundred applications.

c. **Data Carving:** The tool includes a powerful cutting engine for data. Specialists can search for documents depending on the information type and pixel size.

d. **Data Visualization:** Evidence perception in computer forensics is an up-and-coming worldview. Instead of examining textual information, forensic experts can make use of techniques of perception of data to create a gradually instinctive picture of a situation. FTK

provides schedule creation, cluster graphs and geo-area for this element.

e. **Cerberus:** FTK has built-in Cerberus, an incredible automated malware discovery feature. It sniffs malware on a computer using machine understanding. It proposes actions along these lines to handle it whenever discovered.

f. **OCR:** The optical character recognition motor of FTK enables to convert images to readable material quickly. Also, multi-language assistance is included.

2.3 HELIX

Helix Pro is an advanced forensic tool suite CD that offers both live response and bootable criminological environment. The live response utility furnishes the computerized investigator with an intuitive graphical interface and simplest methods for imaging a subject framework's physical memory [18]. It is created by CarneronMalin and James Aquilia in 2013. Helix Pro gets physical memory from a subject (client/ victim) system by imaging the character device document. At the point when the system is live, its state is continually changing, however, gathering data from such a system is helpful when they can't be killed. Because of closing all the proof available in volatile memory, cache and sometimes disk is lost down a hacked or compromised machine. The system is not impacted while working with Helix, which is essential because if it were to be installed in the scheme, the system's initial state would be changed. Hence, some criminal tracks may be lost.

From images to dissecting, Helix produces an MD5 checksum [18] document for each record generated or imported to ensure the integrity of the records, e.g. nobody changes the documents.

The Helix has applications, for example, Windows Forensic Toolchest, FTK Imager, and Incident Response Collection Report. It is very well utilized as a versatile criminological environment as it provides access to countless Windows-based tools such as putty, VNC cut-off document recovery tool, Registry Viewer and Asterisk Logger.

2.4 X-Ways

X-Ways is an incredible investigation report generation application for law enforcement, intelligence organizations, and the private sectors. It runs under windows. It is created by X-Ways software technology in 2015. It is a propelled workplace for digital forensic analysts. This forensics is increasingly proficient to use. It's not an application starving for the resource. Rather it often goes very fast and discovers documents that have been erased. It is small and operates a USB stick without installation on any window system. It is based on WinHex and Disk Editor as well as part of a productive process model in which computer criminological examiner shares data and teams with experts.

X-Ways crime scene investigation contains all of WinHex's overall and special characteristics, for example,

a. It can clone all the images and data available in the disk.

b. Reading, partitioning and documenting raw (.dd) picture records, ISO, VHD, VHDX, VDI pictures

c. Automatic ID of lost/erased allotments

d. Access to logical running process memory

e. Use formats to view and alter binary information structures, etc.

3. Mobile Forensics

Mobile forensics is the part of advanced digital forensics which manages the advanced investigation in cell phones. Following are the tools to analyze the versatile criminological applications:

3.1 BitPim

BitPim is an open-source cross-platform application to monitor cell phone data using

the CDMA communication protocol. BitPim is developed by Roger Binns in 2003. BitPim can be used to back up phone-saved information and to synchronize contacts and calendars. It is consistent with multiple schedules and contact management systems that help the CSV (Comma Separated Vales), including Google Apps, Microsoft Office, and other software applications [20].

Additionally, BitPim supports customizing a few other kinds of information, including contact information, schedules, ring tones, images, and wallpapers. BitPim allows immediate access to key telephone features and data by the researcher. The researcher can deactivate the functioning capacity of the phone. Most phones with a Qualcomm-made CDMA chipset are BitPim-compatible.

3.2 MOBILedit

MOBILedit is advanced forensics that Inspects and reports GSM / CDMA / PCS wireless gadget data. This tool is developed by Compleson Laboratories. MOBILedit associates with Mobile gadgets through an IR port such as a Wi-Fi, Bluetooth connection or a connection module. After network building, model number, sequential number, and its manufacturer recognize the mobile model. The data obtained from the mobile devices is stored in the file .med format. The associated areas are filled with data after a fruitful lawful acquisition: subscriber information, phonebook, missed calls, ringing last numbers, received calls, SIM phonebook, inbox, drafts, sent items and files folder. MOBILedit is a platform that operates with a variety of devices and cell phones and examines the phone's contents through an envelope structure similar to MS Outlook. This allows the data stored on the phone to be reinforced, stored on a laptop or duplicated information to another phone via the copier function of the phone.

2.3 Belkasoft Evidence Center

Belkasoft Evidence Center is a forensic option for securing, discovering, finding, extracting and investigating advanced evidence stored inside cell phones, RAM and cloud. This tool is developed by Belkasoft. It makes it simple for an examiner to gain, search, extract, store and offer computerized proof found inside cell phones. By examining cloud, hard drives, memory dumps, drive pictures, and chip-off dumps, the toolbox will quickly extract digital proofs from various sources.

It finds over a thousand kinds of the most significant forensic artifacts, including over two hundred mobile applications, all main document formats, browsers, email clients, social networks, dozens of image and video formats, system files and registry files, instant messenger, etc.

Belkasoft evidence center does not adjust and alter information on hard drives or disk images that are being researched. It empowers full-content pursuit through all procured proof and offers a complete analysis of periods of intrigue using a graphic timeline.

3.4 Oxygen Forensic

Oxygen Forensic is versatile criminological software for sensible investigation of phones, cell phones and PDAs (Personal Digital Assistant). Oxygen Software has developed this tool. It can remove device information, contacts, calendar activities, SMS messages, logs of occurrences and files. It discovers passwords to encode reinforcements and images. It sidesteps screen lock on well-known Android operating devices. It gains location, history and media documents from automatons and extracts information from cloud administrations, for example, iCloud, Google, Microsoft and so forth. It also gets information from IoT(Internet of Things) gadgets and savvy watches. It offers import and investigation of call information records.

Identified Parameters

The procedure for our analysis process helps us in deciding the best tool which is reasonable for a specific investigation. The parameters being considered are underneath:

a. **Imaging:** Imaging is a bit- by- bit, sector- by- sector direct copy of a physical storage device that includes all files, folders and unallocated, free and slack space [1].

b. **Hashing:** Hashing refers to the utilization of the hash function to check the integrity of the information used to confirm that the image is indistinguishable from the source media.

c. **Recovery:** Recovery is the way toward getting back the information from the erased drive. It is utilized to extricate the current information.

d. **Data Analysis:** Data analysis is a way of examining the extracted data from digital devices.

e. **Reporting:** Reporting alludes to the best possible document generation after perform by the forensic tool.

f. **Packet Analyzer:** It is utilized to investigate the packet data, for example, IP, MAC, firewall data.

g. **Packet Sniffing:** Packet sniffing separates data about the packet going into the network.

h. **Packet Spoofing:** In packet spoofing, IP information is extracted.

i. **Open Port:** It encourages us to distinguish the open ports in the IP association that is required for application and servers.

j. **Protocol:** It shows the principles pursued by the tool.

k. **Topology:** It alludes to the course of action of network portrayal.

l. **Acquire:** It alludes to recognize the advanced proof inside the hard drive.

m. **File System:** The strategy for document framework securing empowers the investigator to gain logical acquisition since it gives access to file system information.

n. **History:** It recovers the browsing history, calls history of the cell phone.

o. **SIM Analyzer:** It gets ICCID (Integrated Circuit Card Identifier) without knowing the PIN and furthermore recovers Location Area Information. It likewise gives access to SIM card status data, for example, IMSI, LAI, PIN, PUK.

p. **Multiple Source:** It gives complete support of contact account records, for example, Gmail, Skype, or Facebook contacts without knowing the account passwords.

Comparative Analysis

Table 1 given below gives the comparative analysis of various digital forensic tools based on the identified parameters. This analysis is used to determine which forensic tool suits better in terms of parameters for any investigation. All these parameters have been discussed in section 6. All the tools that are mentioned in the table have been also discussed. In this section, we have compared only three categories of Digital Forensic tools. And the other two categories have been already analyzed in paper [1].

Table 1- Comparative Analysis of Digital Forensic Tools

Tools	Digital forensic type	Tools availability	Imaging	Hashing	Recovery	Data Analysis	Reporting	Packet Analyzer	Packet Sniffing	Packet Spoofing	Open Port	Protocol	Topology	Acquire	File system	History	Sim Analyzer	Multiple Source
Wireshark	Network	Free	-	-	-	-	-	✓	✓	✓	-	✓	-	-	-	-	-	-
Nmap		Free	-	-	-	-	-	✓	✓	✓		✓	✓	-	-	-	-	-
Nessus		Free	-	-	-	-	-	✓	✓	✓	-	✓	✓	-	-	-	-	-
Xplico		Free	✓	✓	✓	-	✓	✓	✓	✓		✓	-	✓	-	-	-	-
Cuckoo Sandbox	Database	Free	-	✓	✓	✓	✓	✓	-	-	-	-	-	-	-	-	-	-
FTK		Free	✓	✓	✓	✓	✓	-	-	-	-	-	-	-	-	-	-	-
Helix		Free	✓	✓	✓	✓	✓	-	-	-	-	-	-	✓	-	-	-	-
X-Ways		License	✓	✓	✓	✓	✓	-	-	-	-	-	-	✓	-	-	-	-
Bitpim	Mobile	Free	-	-	-	-	-	-	-	-	✓	✓	-	-	✓	✓	✓	✓
MOBILedit		Trial	-	✓	✓	-	✓	-	-	-	-	-	-	✓	✓	✓	✓	✓
Belkasoft evidence center		Trial	✓	-	✓	✓	✓	-	-	-	-	-	-	✓	✓	✓	✓	✓
Oxygen Forensic		Free	✓	✓	✓	✓	✓	-	-	-	-	-	-	✓	✓	✓	✓	✓

In this table, check mark (√) indicates that the particular parameter is available in the concerned tool and minus sign (-) indicates the absence of that parameter in the concerned tool.

Conclusion

Nowadays, many digital forensic tools and techniques are used for cybercrime investigation. The paper provides a comparative study between different forensic tools concerning a set of parameters like imaging, hashing, packet analyzer, SIM analyzer, etc. This comparative study definitely will help forensic investigators to select the best possible forensic tool based on their requirements. In this paper, we have broadly categorized three types of digital forensic tools namely Network forensics, Database Forensics, and Mobile forensics. Some tools are user- friendly because of their GUI and some tools are based on commands. In the future, we will find the limitations of the Wireshark Forensic tool and try to rectify them experimentally

References

1. **Lovanshi M., Bansal P. (2019).** Comparative Study of Digital Forensic Tools, Springer Nature Singapore.
2. **Khaleque Md A.K., Mahmoud A.l, Munawara S.M. (2016).**Memory Forensic Tools: Comparing Processing Time and left Artifacts on volatile memory, International workshop on Computational Intelligence (IWCI).
3. **McCombie S,, Warren M. (2003)**.Computer Forensic: An issue of definition, 1st Australian Computer, Network and Information Forensics Conference.
4. **Sharma P., Jain K., Nagpal B., Tanvi (2017)**.REGEX: An Experimental Approach for Searching in Cyber Forensic, IEEE Conference, March.
5. **Sanap V., Mane V. (2015)**.Comparative Study and Digital Forensic Tools, International Journal of Computer Applications, ICAST 2015.
6. **Dhaka P., Johari R. (2006)**.CRIB: Cyber Crime Investigation, Data Archival and analysis using Big Data Tool, ICCCA.
7. **Bariki H., Hashmi M., Baggili I. (2011)**.Defining a Standard of Reporting Digital Evidence Items in Computer Forensic Tools, Institute of Computer Sciences, Social Informatics and Telecommunication Engineering.
8. **Lim C., Meily, Micsen, Ahmadi H. (2014)**, Forensic Analysis of USB Flash Drives in Educational Environment, IEEE.
9. **Singh S., Kumar S. (2020).** Capability of Wireshark as Intrusion Detection System, International Journal of Recent Technology and Engineering, Volume-8 Issue-5, January.
10. http://prateek-paranjpe.blogspot.com/p/cyber-forensics-case-studies.html
11. https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html
12. https://learning.oreilly.com/library/view/instant-wireshark-starter/9781849695640/ch01s04.html
13. https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html
14. https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/uploads/documents/nessus_4.4_user_guide.pdf
15. https://www.xplico.org/archives/540
16. https://buildmedia.readthedocs.org/media/pdf/cuckoo/latest/cuckoo.pdf
17. https://www.forensicswiki.org/wiki/Forensic_Toolkit
18. https://www.pcquest.com/forensic-analysis-helix/
19. https://digital-forensics.sans.org/blog/2009/11/20/helix-3-pro-first-impressions
https://searchmobilecomputing.techtarget.com/definition/BitPim