Comparative Study of Digital Forensic Tools

Mayank Lovanshi and Pratosh Bansal

1 Introduction

Digital data prevails all around us and plays a crucial role in any kind of investigation when cybercrime comes in a picture. Digital data comprises of binary representations and contains information in the form of text, images, audio, video, etc. In the present scenario, many cybercrime cases such as hacking, banking frauds, phishing, email spamming, etc., have emerged which are linked with digital data. Digital forensics is a new and demanding branch in the field of Computer Science [1]. Digital forensics is a scientific approach of preserving, acquiring, analyzing, extracting, and reporting of Digital evidences which come from the Digital sources like computer, mobile, camera, etc. It is categorized into various subbranches that are listed below as shown in Fig. 1.

- Computer Forensic
- Network Forensic
- Cyber Forensic
- Mobile Forensic
- Operating System Forensic
- Live forensic, etc.

There are many branches of forensic science present as discussed above, but we are working on desktop forensic, network forensic, and live network forensics.

1. **Desktop Forensic**: Desktop Forensic is a branch of digital forensic which is used for the extraction of digital evidence from the secondary memory. It deals with the recovery of the deleted files. Recovery is an important concept in cybercrime.

M. Lovanshi (✉) · P. Bansal
Department of Information Technology, IET, Devi Ahilya Vishwavidyalaya, Indore, MP, India
e-mail: lovanshi123mayank@gmail.com

P. Bansal
e-mail: pratosh@hotmail.com

R. K. Shukla et al. (eds.), *Data, Engineering and Applications*,
https://doi.org/10.1007/978-981-13-6351-1_15

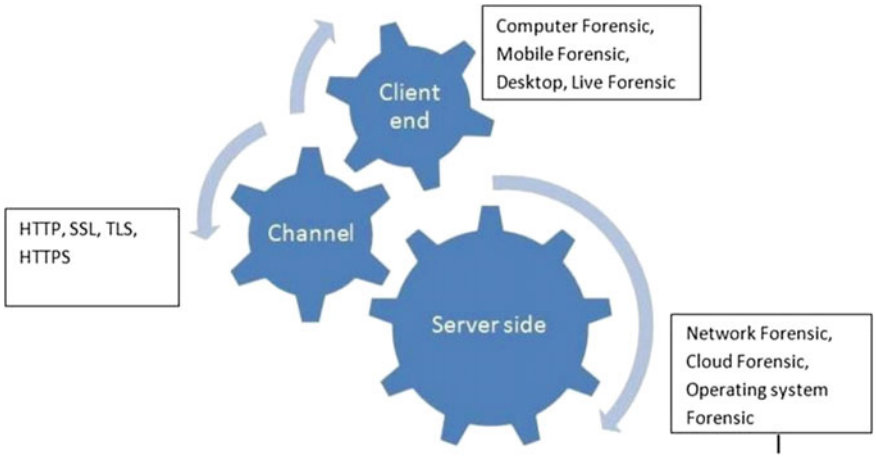

Fig. 1 Digital forensic classifications

Here, computer is used as a target or as a source of digital crime. Desktop forensic is a type of digital forensic where we can determine the information from the hard disk, operating system. There are many software tools required for the recovery of the deleted file, i.e., Prodiscover basic, Cyber check suit, FTK analyzer, Recuva, Ease Us, etc. [2].

2. **Live forensics**: Live forensics is a branch of digital forensics which is used for the extraction of the digital evidence from the primary memory mainly focused on the RAM data. Here, RAM data like browsers information, cookies, registry, etc., are used as digital evidence in the live forensic case. It deals with the RAM dumping. Dumping of RAM means to extract information related to the RAM. There are many software tools present for extraction of the RAM data. Some tools are open source tools while some are licensed version tools like OSF Mount, Win-Lift, Belkasoft, Volatility Framework, etc. [2].
3. **Live network forensics**: Live network forensic tool is the branch of digital forensics. It deals with the live packet sniffing, packet spoofing, identification of the topology, etc. Here, mainly focused on the extraction of the digital evidence through the live network. In the live network, forensic packet information can be extracted. There are many live network forensic tools present like NMAP, wireshark, Ettercap, Nessus, etc. [2].

A number of authors suggested several scientific approaches for digital forensic investigation and defined some phases for the same which are shown in Fig. 2 and summarized as below

- **Identification**: In this phase, the evidence is identified from a digital source.
- **Collection**: Here, the evidence is seized, collected, or recorded from some digital source.

Fig. 2 Digital forensic phases

- **Preservation**: In this phase, digital evidence is preserved which helps in successful investigation, litigation, or incident response.
- **Examination**: Here, the evidence is examined or tested by the forensic expert which results in the correctness of evidence.
- **Analysis**: In this phase, digital forensic tools can be used and determine the relevant information from an image which has been seized during the preservation phase.
- **Reporting**: When an investigation is completed, then auditing and other meta information are reported under this phase [3].

Several digital forensics tools play a significant role in the process of digital forensics to carry out the investigation effectively. Some of the advantages of using tools are

- Used for producing digital evidences that are justifiable by the court of law.
- Helpful in proving the authenticity of evidences.
- Effective in reporting and documentation of evidences.
- Used for recovery of deleted data in various organizations.
- Helpful in research purposes in the domain.

In this paper, an effort has been made to compare different digital forensic tools and to provide a comparative study between them. This study determines the best tool on the basis of available parameters.

2 Literature Review

There are many authors who have given a comparative study of different forensic tools. Garber Lee explains the Encase tool which is a desktop forensic tool. The

Table 1 Issues related with tools

Tool name	Tool category	Description	Issues
Encase	Computer Forensic	Multipurpose forensic tool	Searching time and cost is too high
Prodiscover	Computer Forensic	Data recovery tool	Performance issue
Cyber check suite	Computer Forensic	Recovery and multipurpose tool	Low accuracy then other tool
Wire shark	Network Forensic	Analyzer of packet send on network	No intrusion detection system
Win-Lift	Live Forensic	Analyze RAM detail	Security issue
Mobile check	Mobile Forensic	Extract the mobile information	Incompatible with most of mobile

author also described the features and functionalities of the tool. As per the author, Encase is a traditional tool whose results can be used in the court of law [3]. Abbas Cheddad explained a comparative study on cyber forensics tools such as Minitool, Hard Drive, and Pen drive Recovery tool based on the parameters like paper size and time, cost, tools availability, etc., and considered mapping as the biggest issue [4]. Nilakshi Jain tested digital forensic tools on different parameters in network, live, and desktop applications. The author also tested various other tools such as Clonezilla, Image USB, Etthercap, OSF Mount, etc. [5]. Kresimir Duretec worked on benchmarking of different forensic tools and also has used some data sets to verify the results. In his paper, he also suggested the reliability and security of digital evidences [6]. Ryan tested digital forensic tools such as Ease US, Encase, Ftk analyzer, etc., on the different parameters in the desktop forensic [7]. Abbas suggested [4] that comparative study of cyber forensic tools is present and gives the comparative study on Minitool, Hard Drive, Pen drive Recovery tool. In this paper, size and time is compared. Selection of the best tool is the biggest issue which was shown in this paper. Nilakshi Jain suggested [5] many Desktop Forensic tools tested on the different parameter for the Network, Live, and Desktop application. In this paper, traditional investigation process is used for the comparative study which will be not suitable for the court. Duretec et al. [6] suggested benchmarking of different forensic tools under which some data sets used to check the results on the different parameters. There are many tools issue extracted which will be shown in Table 1.

The review of the literature identified some problems which are as below

- Selection of tool—To select the best suitable tool based on the comparative study.
- Large computational time—It refers to huge computational time incurred while running some of the forensic tools.

3 Digital Forensic Tools

There are many forensic tools available in the category of freely available tools as well as the licensed version. Authors suggested the tools to identify evidences on the basis of digital forensic classification. Various types of digital forensic are discussed in Sect. 1 such as desktop forensic, live forensic, network forensic, etc., which are discussed below

3.1 Desktop Forensic

This is the computer forensic branch where the investigator focuses on the recovery of the secondary memory, i.e., hard disk of the system. Following are the tools to test desktop forensics applications:

a. **ProDiscover Basic**: The ProDiscover Basic is used to test the hard disk data. It is a forensic tool which is used to take legal action in court of law. It helps to collect data and imaging of that data and then to examine their recovery. It has very nice searching capability which allows data to be searched easily which is to be recovered. It allows data into a cluster view and content view [8].
b. **Encase**: Encase Digital Forensic tool is used to get, analyze, classify, recover, and reconstruct the evidence and test the digital evidence which is obtained from Digital Forensic investigation process. Encase is also a known traditional tool and its result is used into the court of law [8].
c. **Recuva**: Recuva is a data recovery tool program for Windows which is freely available in the market. It is used to recover permanently deleted files which are not overwritten. This tool can also be used to recover deleted files from USB, Hard Disk, and MP3Player [8].
d. **Cyber Check Suit**: This is also a cyber forensics tool for data recovery and analysis of digital evidence. Cyber Check needs imaging created by True Back image tool.
   The graphical user interface of the cyber check is very easy for a beginner. Cyber Check can also generate a report of the analysis findings by the investigative expert to submit in a court of law. The tool can report unallocated and disk slack area and gives options to do analysis based on file hashing and file's signatures [8].
e. **Autopsy**: Autopsy is an open source tool which is plugged-in with the Sleuth Kit collection. The GUI of this tool displays the results from the forensic searching of tool done by investigators to show an important part of the data. The development company provides the proper guidance of the tool [8].

3.2 Live Forensic

Live Forensic is a branch of Digital forensics where investigator focuses on the RAM feature extraction. Following are the tools to test live forensics applications:

a. **Win-Lift**: Win-Lift Analyzer is a forensic tool used for live analysis for analyzing RAM data collected by Win-Lift Imager. It results into forensic evidence and produces a full report. The analyzed information will be used for the proper reporting of the data. It results in different memory forensic object. It will extract the running files, log, open socket file, etc. [9].
b. **Belkasoft**: Belkasoft tool helps an investigator to acquire, search, analyze, and allocate digital evidence inside a computer. This tool is used to extract digital evidence from many sources by analyzing from various volatile memory data in term of evidence. This tool automatically exams the data source and put the RAM data for an expert to review, examine evidence data which has been analyzed by the tool [9].
c. **Magnet RAM**: Magnet RAM Capture is a tool which supports Windows systems including XP, Vista, 7, 8, and 10. It will extract the full live memory evidence and analyzes a volatile trace. This tool is used for memory analysis which is important for detection of malware and recovering valuable data. It extracts the running program and processes, active network connections, registries, password, keys, etc. These are just a few examples of the evidence that can be extracted from memory [9].
d. **OSF Mount**: OSF Mount is used to create RAM disk and this disk is mounted into RAM. This is used for the high-speed memory over the hard disk. This tool is useful in various applications like database application, cache files and browsers files. Another benefit is security, like data in the volatile disk will be automatically erased when a system is shutdown [9].
e. **Volatility Framework**: Volatility is open source tool for analyzing RAM evidence. This tool supports Linux, Windows OS. It is coded in Python and run On Windows, Linux system. It can examine RAM dump, crash dumps, virtual box dumps, etc. [9].

3.3 Network Forensic

Network forensic is a field of Digital Forensic where the investigator focuses on packets traveling in a network. Following are the tools to test network forensics applications:

a. **Wireshark**: Wireshark is an industry standard packet analyzer tool that analyzes the packets into a network. It is required in many projects that can be developed using the network. This tool is used to read and write the packet and capture file. This capture file will be analyzed by Wireshark tool. Many more tools are present but Wireshark is one of the best among them [2].

b. **Ettercap**: This tool is used to analyze the man in the middle attack and is a free and open source tool. This tool is used to analyze the packet tracing, security auditing, and computer network protocols. It is able to manage traffic on the network segment and capturing password [2].
c. **Nmap**: Nmap is a port scanner tool inside the network protocol which provides security features. It is used to discover host and provide services on the computer network. So it is used to map the services with network. Basically, Nmap (Network Mapper) is used to send a craft packet to target host and analyze the content and port of the target and source information [2].
d. **Nessus**: Nessus is a security auditing tool which is used to scan the network. It will scan a computer and create a warning about the vulnerability generated by malicious hackers. It can enter any computer which is connected with the network. This tool is testing different attacks into the computer which harm our computer system [2].
e. **Snort**: Snort is an open source tool which is used to detect network traffic, analyzes and packet logging on different IP logging system. It helps in protocol searching and packet tracing. Snort is used for providing QOS in a network. So this tool is capable of analyzing bulky data into a network [2].

4 Methodology

The methodology adopted by us focuses on the study of different digital forensic tools as discussed in the previous section. These tools describe various functionalities with respect to digital evidences. In our study, we follow a process as discussed in Fig. 3. The first step in the process involves selection of tools where we have chosen the digital forensic tools. The next step deals with the extraction of features which helps us in identifying the parameters. At last, we compare the tools on the basis of parameters.

The process helps us to determine whether the parameters are present in the respective tool or not. The parameters being considered are listed below

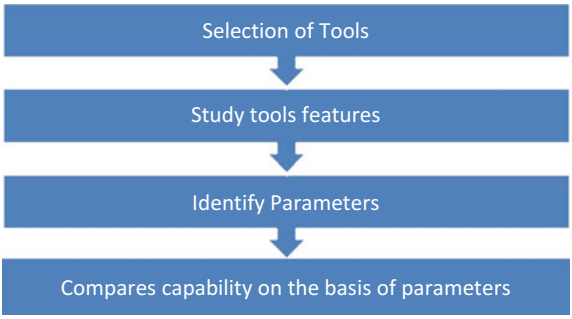

Fig. 3 Flow chart of work

- Imaging: Imaging is a bit to bit copy of the hard drive. It takes every 0 and 1 from one hard drive to another.
- Hashing: Hashing uses the hash function to check the integrity of data used to verify the image of the drives.
- Recovery: Recovery is a process of getting back of data from the deleted drive. It is used to extract existing data.
- Acquire: It refers to identify the digital evidence inside the hard drive.
- Seizer: Seizer is used to preserve the hard drive by imaging.
- RAM Dumping: It refers to extract the RAM data such as cookies, browser history, registry information, etc.
- Live Log: It contains the logical files that are generated in live cases.
- Live Analysis: Live analysis helps to extract the RAM information from the dumping image of the RAM.
- Search: Search means to find some content into the image as well as the analyzed hard drive.
- Log: Log is a logical file that can be extracted from the analysis of the data.
- Reporting: Reporting means proper documentation generates after performing of the forensic tool.
- Packet Sniffing: It extracts information about the packets traveling in the network.
- Packet Analyzer: It is used to analyze the packet information such as IP, MAC, Firewall information etc.
- Packet Spoofing: Spoofing means hiding the information of the sender. Here, IP information is extracted.
- Protocol: It displays the rules followed by the tools.
- Open Port: It helps us to detect the open ports in IP connection that is required for application and servers.
- Topology: It refers to the arrangement of network representation.

5 Results

The comparative table contains the results of the different forensic tools based on the given parameters which are used to determine which tool is better in context to the parameters. Table 2 shows the comparative results for the tools.

6 Conclusion

In today's scenario, many digital forensics tools and techniques are used for cybercrime prevention and investigation. The paper provides a comparative study between forensics application tools and a set of parameters. This approach is useful for forensics experts and investigators to select the best possible forensic tool based on their requirements. So, the investigation process can be carried out smoothly.

Table 2 Comparative table result

	Parameter																	
Tools	Digital forensic type	Tools availability	Imaging	Hashing	Recovery	Acquire	Seizer	RAM dumping	Live log	Live analysis	Search	Logs	Reporting	Packet sniffing	Packet analyzer	Packet spoofing	Protocol	Open port	Topology
Prodicover basic	Desktop	Trial		✓	✓		✓	–	–	–	✓	✓	✓	–	–	–	–	–	–
Encase		Trial	✓	✓	✓	✓	✓	–	–	–	✓	–	✓	–	–	–	–	–	–
Recuva		Free	–	–	✓	✓		–	–	–	–	–	–	–	–	–	–	–	–
Cyber check suit		License	✓	✓	✓	✓	✓	–	–	–	✓	–	✓	–	–	–	–	–	–
Autopsy		Trial	✓	–	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
Win-Lift	Live	License	✓	✓	–		✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–
Belkasoft		Trial	✓	–	–	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–
Magnet RAM		Trial	✓	✓	–	–	✓	✓	✓	✓	–	–	–	–	–	–	–	–	–
OSF mount		Trial	✓		–	–	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–	–
Volatility framework		Trial	–	✓	–	–	✓	✓	✓	✓	–	✓	–	–	–	–	–	–	–
Wireshark	Network	Free	–	–	–	–	–	–	–	–	–	✓	–	✓	✓	✓	✓		
Ettercap		Free	–	–	–	–	–	–	–	–	–	–	–	✓	✓	✓	✓		✓
Nmap		Free	–	–	–	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓	✓
Nessus		Free	–	–	–	–	–	–	–	–	–	–	–	✓	✓	✓	✓		✓
Snort		Free	–	–	–	–	–	–	–	–	–	–	–	✓	✓	✓	✓	✓	–

After reviewed the comparative table we analyzed that some freely available tools are as useful as the license tool. Some tools are user-friendly in their GUI, some are better according to accuracy while some are used because of their lower data rate. This research is useful to show which tool is better on which condition and also concluding its usefulness of tool for stopping the digital crime.

7 Future Work

The future works include the mapping of digital forensic tools and enhancement of data accuracy, reliability, security, and other privacy measures by performing a comparative study on a large number of forensic tools.

In the next years, many other tools and many other features can also be used for future research. And provide the comparative result between that tool and parameter and we will try to be getting some CFTT research for testing the tools, also several other parameters may also include for comparison.

References

1. Baryamureeba, V., Tushabe, F.: The enhanced digital forensic investigation process model. In: Proceedings of the 4th Annual Digital Forensic Research Workshop, Baltimore, MD, Citeseer (2004)
2. Mukkamala, S., Sung, A.H.: Identifying significant features for network forensic analysis using artificial intelligent techniques. Int. J. Digit. Evid. **1**(4), 1–17 (2003)
3. Ani, L.: Cyber crime and national security: the role of the penal and procedural law. Law and Security in Nigeria, 200–202 (2011)
4. Cheddad, A., et al.: Digital image steganography: survey and analysis of current methods. Signal Process. **90**(3), 727–752 (2010)
5. Jain, N., Kalbande, D.R.: A comparative study based digital forensic tool: complete automated tool. Int. J. Forensic Comput. Sci. (2014)
6. Duretec, K., Kulmukhametov, A., Rauber, A., Becker, C.: Benchmarks for digital preservation tools. In: Proceedings of IPRES 2015 (2015)
7. Hankins, R., Uehara, T., Liu, J.: A comparative study of forensic science and computer forensics. In: Third IEEE International Conference on Secure Software Integration and Reliability Improvement, 2009. SSIRI 2009. IEEE (2009)
8. Garber, L. Encase: a case study in computer-forensic technology. In: IEEE Computer Magazine January (2001)
9. System Administration Networking and Security Institute (SANS). Computer Forensics and Incident Response. https://www.sans.org/course/advancedcomputerforensic-analysis-incident-response (2015)