Digital Forensic Tools Used in Analyzing Cybercrime

D.O.I - 10.51201/Jusst12621
http://doi.org/10.51201/Jusst12621

Mohammad Dweikat[1], Derar Eleyan[2], Amna Eleyan[3]

[1,2]Applied Computing,Palestine Technical UniversityKadoorie,Tulkarem,Palestine
[3] Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, UK

Abstract**:** *With the development of technology, crime has become not limited to traditional crimes, but has evolved in its modern sense into electronic crimes that have their own tools for penetration, extortion, theft, money laundering and electronic exchange, and concealing the effects of these crimes increases the difficulty of investigation. Therefore, there is an urgent need to develop electronic tools in forensic medicine to keep pace with this type of crime, search for criminals and collect evidence to be used against them before the court, and from here the topic of these tools has evolved, and we will also address in this scientific paper these tools and identify their strengths and weaknesses and suggest appropriate solutions and tools. That covers all aspects of the evidence to assist the investigators in selecting the appropriate tool.*

Keywords: Forensic tools, cyber-criminal, attacks, computer forensic, cyber-crime.

I. INTRODUCTION

After the cyber-crime occurs the criminal leaves a trace which indicates some critical information needed to prove the characteristics of that criminal like the attack time, and the date and where it happened and the tool used, the investigators need tools to match between the criminal and the cyber-crime using evidence. can be indicated by using special tools[1] (Forensic Tools) or cyber-forensic are tools using a branch of science, used in recovery and investigation of data and evidence by collecting it from a different type of devices such as computers or mobile phones.

According to [2] one of the most important rules that must be taken into account when collecting digital evidence and information using digital forensic tools is that will no change is happened in evidence obtained, and evidence collectors who use these tools should document all activities, in addition to the undertook to keep the original documents and preventing them from being modified or changed to preserve the evidence.
In this research, a group of electronic forensic tools related to computers, networks, and portable devices were dealt with, and it was found that most of these tools cover specific aspects and do not cover other aspects in the search for evidence, just as there is no complete crime, there are also incomplete tools. On the computer side, and based on the comparison, the following tools (FTK, Encase, COFEE, DFF) are considered complementary to each other. As for mobile phones, (Oxygen Forensic) is considered very suitable.As for networks, it is considered a tool (Nmap) that is closest to carrying out most of the tasks.On the other hand,I advise companies that work to produce these tools in cooperation with each other to benefit from practical and programming experiences to come up with a near-perfect tool that meets all the requirements of investigators in cyber-crimes or to collect these tools as a framework for investigation as special tools such as Sherlock Holmes tools for investigating actual crimes.

II. LITERATURE REVIEW

The new technology over the world in computer and cellphones using communications and transferring and storing data. this data became more precious than ever for every institute and individual and because of that, and cybercrimes increase over time and its most sophisticated to identify the cybercriminal, new forensic tools need to keep abreast of developments features to the new technology and cybercrimes.As mentioned [2] these days, with the increase in data storage and processing, there is a great risk of losing it, and also data that is collected manually or through devices may be exposed to electronic attacks, with the presence of these dangers. There are many digital forensic tools through which evidence is collected and studied. It was conducted a study by [2] on these tools that governments, companies, and people use to extract digital evidence through comparison based on different determinants so that the appropriate tool is chosen based on needs and the study also includes the problems facing the users of these tools. In this analysis or study for forensic tools, these tools are compared based on a list of parameters, based on study these tools does not cover all features that can be used for all situations in the case of study and cybercrime investigation to get all the evidence that can be found in the crime scene, the (EnCase) tool covers most benefits but not do live analysis and (Pro-Discover tool) although covers the live analysis but don't work on multiple OS like the previous tool and do not have feature mail analysis.

In [3], a simulation was done by running an alternative Linux server to the Minecraft server and creating a collective hosting for the players, and other players were connected via a computer with a Windows 7 system, and these hosting for both systems were in a (VM) environment on the same local network in addition to taking multiple screenshots with a VMware program, A comparison of the screenshots was made when the activities in the case of using the server and the client, and other tools were used in these simulations to implement specific functions (VMware fusion to create Linux server and windows client imager to create a forensic image.VMDK, Autopsy to analyze windows files ad directors and system files, HXD to capture live memory data, Volatility to carve artifacts from memory, Wireshark to capture and analyze network traffic inside VMware , Network Miner to analyze network traffic was captured, windows event viewer to analyze all recorded event in the windows system) and this experiment resulted in the following:
1- The Minecraft server is managed by the perpetrator, where directories are located on the connected players' devices and through which the parent addresses and user names can be determined.
2- The Minecraft server is the directory store, and violators can access the user name and contact information stored on the server.
3- The Minecraft Windows client is used by the victim to carry out some crimes as the exchanged communication between others is information and other information can be known to other users such as the server operator and they can provide sufficient information about the offending connected user.
4- Unique identification information is available for each user inside the Jason file and also in the Linux server's memory after the game ends.
5- In the event of impersonation of a player, it should be noted that the identification numbers expire one month before the date of contacting the server.
6- The artifacts were stored on the Linux Minecraft server and the program that was installed was run to see activities while playing with the Windows client.
As for the timestamps in the local memory and the hard disk, a link was found between the user's unique identification numbers and the parent's addresses, and it remained stored for a month. As for the Windows client, it stored the e-mail linked to the registered Minecraft.

In [4], a set of nodes were made using a Hadoop 2.7.4 running on the Ubuntu 16.04.3LTS environment, which is four nodes (Master NameNode,Two DataNodes, secondary NameNode). Screenshots were taken in each case of the device after the implementation of one of the basic functions of the Hadoop system, the internal and basic distributed file system, and the procedures that will be analyzed.The (HDFS) Hadoop Distributed File Systemenvironment has been forensically searched to obtain forensic artifacts that can be used in forensic investigations. This was done by applying a set of important HDFS commands and monitoring the results to analyze the artefacts generated from each command, focusing on analyzing the Linux filesystem and network files as well as the main memory during work periods. HDFS is a complex and large master structure made up of configuration files, different systems and logs in the form of a network in which various information about the procedures that take place within it can be obtained by analyzing it.The built-in commands within HDFS for the Editing Viewer and Offline Image Viewer have proven to be very important in recovering important forensic data during the investigation. These tools have resulted in investigators with important information from the FSimages and Edit log, and the output of these tools gives a broad overview of special activities. By mass in implementing each of its actions.It turns out that the Hadoop log files contain a huge amount of information related to the procedures that were carried out using Hadoop and the file record(hadoop-crime-namenode-masternamenode.log)contains all the procedures for HDFS, and this file is very important for forensic investigators and the output of this record is important when forensic analysis in the Hadoop environment.As for the analysis of processes in the main memory of the HDFS evaluation, the result was that there was no important information related to the investigation from a forensic point of view because the HDFS processes operate as an abstract block.In addition to analyzing the communications that take place between the nodes and analyzing the existence of criminal artifacts that are important and in determining the activity, some information was obtained, but not sufficient, due to the presence of encryption between the nodes to increase security.

A Ceph file system that provides high availability and self-repairing features for data, and provides a permanent access to data and saves it from loss and damage[5].This system is considered better for cloud service providers and its importance and the activities of users on this system are considered as a priority.In the research paper, the remaining evidence was extracted from the users' use for the system that was running in Linux Ubuntu 12.4 to discuss the extracted evidence, in addition to analyzing the forensic framework and cloud in the CephFS residue that was saved and analyzing it on the server and the client.The experiment contains a set of simulation devices that provide two OSDs, a monitor with an MDS node, responsible for the plaster for the node, and one customer device, individual nodes are created and tested based on Ceph values. The environment that was built for the forensic experiment contains special configuration for the Ceph node (operating system- Linux Ubuntu 12.4, Ceph distribution-Giant) and the forensic tools used for this experiment (HxD Hexeditor,CapLoader, Wireshark,Vmware Workstation, OSFMount ,Ext2 Volume Manager,OSForensics,Autopsy Meld).The difficulty in collecting big data, which results from ten simple text files, is not suitable for forensic investigators, and there is a need for an appropriate framework and automated tools to help in dealing with and processing data in an automated manner instead of a manual method, and the emergence of a problem in the manner of different file systems such as XtremeFStone and Ceph system, where these systems provide different solutions to provide improved and innovative products, including the forensic solutions of these cloud systems that fit one type and fail to deal with another system. The tools that were used in this investigation gave results in determining the information related to the investigation, but automated systems must be developed to avoid manual searches.

SeaFile service is considered an open-source cloud storage service, defects have been discovered on the server and the client that can be restored legally, by specifying the client's synchronization, encryption, file and data management for authentication and forensic analysis, by creating eight virtual accounts for the role of clients and administrators and assigning an emoji and a unique name For each user account[6].The test consists of two VM workstations for servers, three virtual machines for clients, an iOS device and an Android device that have been restored to factory settings, and VMware was used to host the VMware Fusion Professional version 7.0.0 on a MacBook Pro with a Mac OSX Mavericks 10.9.5 system with Intel i7 2.6GHz processor specifications quickly. With a 16 GB main memory, virtual drives have been used because the use of physical devices to perform the procedures is tiring in terms of copying, scanning and reinstallation, as the virtual machine offers an acceptable error rate through the use of restore points in the event of unacceptable results, in addition to using Physical mobile devices instead of the emulator for the ineffectiveness of the emulator because it deletes some of the features of these devices and provides unsatisfactory results, using devices with few spaces to save time and effort in analyzing snapshots, in addition to breaking the protection of mobile devices to access the main system of portable devices (root).The test resulted in the fact that the private cloud is important to users and medium and small enterprises, but it is not without flaws in terms of forensicsSeaFile. As a result of the investigation, large data can be recovered from user devices, whether desktop or mobile, and data that passes through the network when using the SeaFile client application, such as logging out, logging in, installing and uninstalling these tools, chats, and files shared that have been synchronized and managed calculation.The scope of the investigation is known from the recovered artifacts and the scope of the search expanded, and the proposed framework provides forensic investigators with an effective process in private cloud services investigations.

Spoke about the history of cybercrime and when these electronic forensic tools were created and classified digital forensic tools into these categories (computer forensics, mobile forensics, database forensic, network forensics, and forensic data analysis) and different types of framework[1]. Forensic work, in addition to[1] writing a brief text about each tool and making a comparison in terms of applicable tools and usage for each tool, for example, the tools used in email analysis,there are many tools to do this task (Mail, MBOX, OST) viewers.

As[7]proposed a framework and based on it, he created a table to identify any deficiencies in 25 forensic tools, and his conclusion is that there is no tool capable of covering the conditions of the proposed framework. In addition to proposing a tool to be designed based on the proposed framework and explaining all possible operations in this framework. It was adopted in building the tool on the NetBeans IDE 7.1.1 tool and the Oracle 10g database and used the operating system for testing. Among the features of the proposed tool:

- Protection of personal login information, whether for the user or even the administrator
- Reducing the rate of cybercrime by assisting law enforcement agencies in determining the percentage of crimes in each city
- Providing the ideal solution as it matches the proposed framework
- Increase the investigator's investigation experience through the feedback on the history of operations
- The production of automatic reports on the cases that have been investigated

A comparison was made between two tools for analyzing data for Android devices, which are the commercial tool Paraben E3:DS and the open Autopsy tool[8]. In the experiment, all activities were restored on the Android phone using the first tool, but Autopsy was unable to perform the necessary restoration, using the tool. In the first tool, the activities were restored with a time stamp, unlike the second tool, and the result is that using the appropriate tool, data can be recovered from Android phones and this data is of great value for forensic investigators to investigate the crime.

In the study conducted by [9], he surveyed the techniques used as forensic tools for phones based on the manual acquisition and physical acquisition, logical data acquisition from Android-based devices and classified into a table containing the following characteristics (private or free, basic operating systems, number of supported devices) For example, the free volatility tool provides support for multiple APIs to forensic workers to expand the work horizon, and the free forensic tool Oxygen contains many of the techniques used for reporting and features from a graphical data interface, a graphical user interface, and support for many devices.

Case study of [10] SCADA systems was used, which is a set of tools used to extract forensic evidence and collect information about the devices related to the case and networks, and the data collected was used to determine the penetration, the percentage of system penetration and examine the functional processes of the system that were affected, the experiment is a group of simple attacks Accurately described, and evidence is gathered after each attack by applying the methodology and tools for each attack method. The three attack experiments were conducted on the environment of the SCADA system and the attacks were Man in the Middle, remote access, and a USB pin drive infected with a malicious program. As a result of the experience that was conducted, each attack needs different tools from the other, and the extracted digital evidence varies in different operating systems, and there is a difference due to the fact that SCADA devices differ from one provider to another and different generations.

The result of a test he did [11] on the forensic tools for phones Belkasoft Evidence trial and WhatsApp Key/DB extractor, it was found that the two tools passed the repeat test, which results in the same number of artifacts, and they also passed the reproduction test because they give the same image files in all the artifacts, also there is a difference in the result of the tool The first is to recover both pictures and videos with higher clarity beside files, while text messages are not recovered, while the second tool is able to recover photos and text messages only. The equipment and software used in the test is (Samsung galaxy s4 android v5.0.1, WhatsApp Ver2.17.147, workstation with windows 7 64bit, USB Cable, Belkasoft Evidence trial, WhatsApp Key/DB 4.7, SQLite studio for analysis).

“Digital Forensic Chain of custody (CoC) can be defined as a process used to maintain and document the chronological history of handling digital evidence” [12] Recording the minute details related to digital evidence across the different levels of the hierarchy, that is, from the hierarchy rule to the highest authority responsible for cybercrime

It is also used as a reference for collecting, analyzing and preserving evidence, the people responsible for it, the time and place of collecting evidence, and in some cases the evidence may be subject to change during its course in the absence of proper maintenance and preservation, which leads to its not being accepted by the Internet Crime Court[12]they categorize the attempts for improving the CoC

to direct attempts including:

- (DEMP) Digital Evidence Management Framework gives secure and reliable for CoC.
- (DEC) Digital Evidence Cabinets for enhancing handling digital evidence.

Indirect attempts including

- (UMML) Unified Modelling methodology framework for planning, documenting and performing forensics tasks.
- "Flow thing Model (FM) that involves six operations (create, release, transfer, arrive, accept, and process)"[12].

III. METHODOLOGY

This paper explores the existing forensic tools available in Cybersecurity investigations, classify them according to their usage. Then full analysis has been performed highlighting the advantages and disadvantages.

IV. DIGITAL FORENSIC MODEL

Digital Forensics [13] “is a branch of forensic science focused on recovery and investigation of material found in digital devices” (computers, mobile phones, servers, network) related to cyber-crime. defined as the process of preservation, identification, extraction, and documentation of computer evidence that can be used by the court of law.

When a cybercrime occurs and the perpetrator must be searched, those responsible for the investigation process follow the process as Figure1 shows. Carefully to ensure that the evidence is not tampered with and that a dead end is reached in the case, and so that the officials ensure that the evidence is accepted in court when these proper procedures are taken.

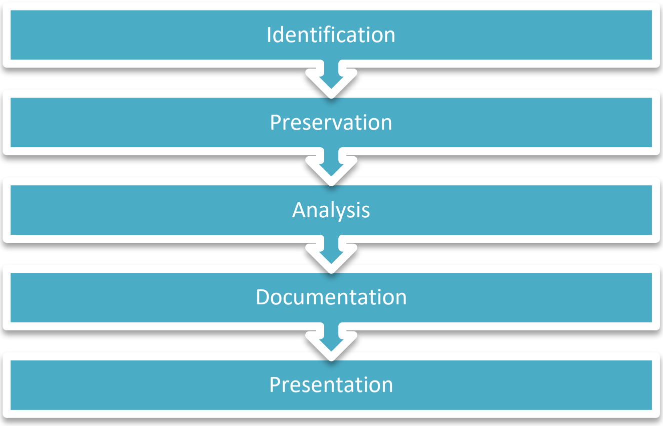

Fig .1 Process of Digital Forensic

A. *Identification*

The first responders to what (network administrator, law enforcement officer, investigating office) responsibilities are identified and securing the crime scene and searching for digital evidence and determining where it is stored. Professional officials search for devices related to the execution of the crime and properly seize them to extract evidence from them.

B. Preservation

In this step, the evidence is secured, isolated, and saved. By preventing others from tampering with this evidence, the forensic team must secure digital evidence after ensuring a safe environment exists, in addition to ensuring the accuracy of the data and whether it is original or not that has been collected and easy to access.

C. Analysis

Draw conclusions by reconstructing parts of data from the existing evidence. These data that were accessed by officials are scanned to determine the evidence that will be presented to the court. This phase includes identifying, examining, separating, transforming and modeling data into valuable data.

D. Documentation

Reconstructing the crime scene through records containing crime data. The detailed report contains all documents, reports and documented results, and this report contains sufficient evidence accepted by the legal court.

E. Presentation

Summarize and draw a conclusion,after completing the collection and analysis of evidence, [14] an offer report is built upon which the decision is made against the person who caused the event or crime, and the decision is saved in a database for future reference. The decision is a legal procedure in court cases and the main focus thereof.

V. DIGITAL FORENSIC TOOLS

Because the crime occurred in virtual world now it called cyber-crime [2],because of that crime forensic tools founded to detect the cyber-criminal by collecting evidence based on [15] digital forensic models that categorized to at scene includes (planning, identification, collection, preservation) and in the lab includes (examination, analysis, report).Forensic Tools are categorized based on the environment and devices (computer forensic, mobile forensic, network forensic) and these classifications have subcategories as shown in Figure 2

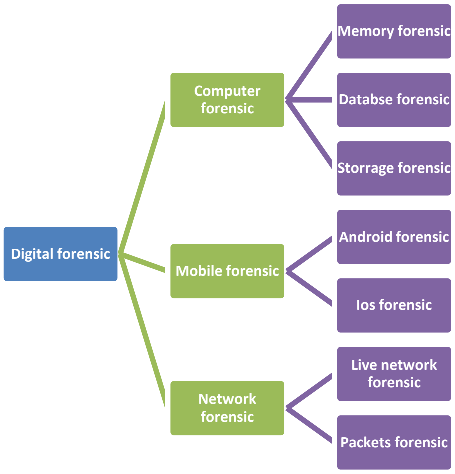

Fig .2 Digital Forensic Tool Classification

1. Computer forensic
   - Memory forensic
   - Database forensic
   - Storage forensic
2. Mobile forensic
   - android forensic
   - iOS forensic
3. Network forensic
   - Live forensic
   - service forensic

VI. COMPUTER FORENSIC

The special type of forensic tools it is used to extract, recover and analyze this information from computer and any hardware component such as memory, hard disk, and hided information and retrieve the evidence from databases and peripherals like USB pin drive, SD card,and external storage equipment’s related to extracting evidence about cybercrime to use it in the law court against the cyber-criminal.

A. *EnCase*

As [1] define this Encase is a tool used for collecting facts from various devices and discovers any possible digital evidence by extract the full evidence report.[2] is a tool created by guidance software its used in the whole world 93% of banks,1005 federal agencies ,75% power distributors and 80% of USA universities use it for investigation lifecycle.

B. *Digital Forensics Framework (DFF)*

An open-source platform with a customizable interface, used by educational institutions, companies, and law enforcement agencies around the world, it has three versions and options for a paid DFF Pro license, free DFF, direct DFF with a backing license.[7] Used in computer forensics to collect, save and disclose digital evidence without changing the system and data, reading evidence file types RAW, AFF, and EWF also can access remote devices and recover deleted and hidden files[2]
.

C. *Computer Online Forensic Evidence Extractor (COFEE)*

This Forensic tool founded by Microsoft; the investigators used it to extract digital evidence from computer operates with Windows Operating System.[2] it is used by law enforcement only and operates a live analysis by installing it on a USB stick or Hard Drive, Microsoft corporate with (NW3C) National White Collar Crime Center and also Interpol to create forensic investigation.[1] it has 150 special tools with a special (GUI) graphical user interface, it can collect and analyze evidence within 20 minutes by plug the USB pen COFEE in a criminal device to begin live evaluations[7].

D. *ProDiscover*

A court-backed forensic tool used to collect and create images of data and analyze recovered data, and it has the ability to easily search for recovered data and there are two ways to view it by group or content. [2] It was developed by ARC Group and has three variants, a ProDiscover Basic license $ 50, a ProDiscover Forensic Edition license of $ 1679, and a Pro Discover Incident Response Edition license of $ 2,799, and it has the ability to collect browsing data, device and time zone information, as well as retain original metadata. Such as access time and there is an incident response version used for live analysis using the Connect Collect Protect process during security issues and data breaches[16].

E. *Recuva*

A tool used for recovering data in windows OS, created by Piriform company, it has the ability to recover deleted files from SD card, USB pen drive, and other multimedia devices such as music players. It has a free and paid license and anyone can use it[7].

F. *Computer Aided Investigative Environment (CAINE)*

Linux based tool with friendly GUI with half automatized create report used for mobile, network, data recovery forensics ,used live CD to run.[17] it is open source and Italian GNU/Linux live distribution and it has a write-blocking method that assures all disks are really preserved from accidentally writing operations because they are locked in Read-Only mode used “Mounter” to unblock writing policy for rewritable mode[7].

G. *Forensic Toolkit (FTK)*

Developed by Access Data Group they provide forensic tools for training and gives certificate over 130000 in governing, law permits to use FTK in the world, it can analyze computers, networks, mobiles, and laptops, the main characteristics faster search and filtering than competitor tools.[15] it allows responder to take an image from criminal system using special equipment (write-blockers) and verifying acquired images raw/dd or experts witness known as “Encase”,they also support FAT,NTFS,ext2 and ext3 system formats[2].

H. *Bulk Extractor*

A tool used to extract important information without changing system file structures by scanning directory, files, disk image, and store extract files in other location for inspection, passed, processing it by automated tools. [2] supported by windows, MAC and Linux the main point of this tool ignoring file system [7].

I. *The Sleuth Kit*

Is kind of library it has command line tools collection, supports virtual machine in a new version, this library(libvhdi , libvmdk) helps in analyzing system files,analyze disk images and recover files related to an investigation and recovers data from SD card,used by law enforcement bodies,corporate examiners and military, it has a framework give the user ability to build an automated digital forensic application [2].

J. SANS Investigative Forensic Toolkit (SIFT) SIFT

A device running multi cause forensic has all tools used digital forensic techniques, based on ubuntu support several devices related to digital forensics, free license and open source tool[1]**. The** Toolkit used in investigation using a virtual machine as computer forensic suit deals with raw images and NTFS, HFS, UFS file systems[7].

VII. MEMORY FORENSIC

Volatile memory or computer memory is so named because it loses the data stored on it when the power is cut off from us by shutting down the computer or when writing on it from other programs, compared to permanent storage devices, because of the constant change it is difficult to predict and extract data. Useful from it, knowing that this data A type of artifact that is very important in the investigation process and sometimes cannot be obtained from the hard disk[18].

A. Mandiant RedLine

Used to analysis memory in a criminal host which obtains information about processes and drivers running in memory and collect system metadata, event logs, registry data, network information, all services and running tasks[7]**.**

B. HxD (Hex Editor)

It has the ability of low-level editing, modifying raw disks and (ram) random access memory, by searching, replacing, exporting checksums/digests file shredder, concatenation or splitting files to create statistics[7].

C. VOLATILITY

Listed forensic memory framework used for incidents actions and can extract information such as running procedures, network ports, registry and DLLs, useful for collecting records that windows crash dump, its free license. [9] Open source released in October 2015, written in python language users can build their own web interface and GUI and also adding new plugins and updating exist to create a framework as they need[1].

D. Magnet RAM Capture

Forensic tool designed especially for capture physical memory of a criminal computer, let the investigators recover and analyze valuable artifacts founded in memory,can capture data in raw (.DMP/.RAW/.BIN) formats and using magnet Axion and Magnet IEF, the evidence discovers like malware intrusion, registry hives, password and username, network connection, decrypted files not located in the hard disk, support windows operating systems until Windows 10[19].

E. Plain Sight

It collecting digital evidence such as internet histories usage information, analysis ram dumps to extract stored password hashes[7].

F. Nigilant32

Describe this tool as an incident response tool used for extract (RAM) random access memory content developed by Aigle Risk Management and open source tool to create snapshot reports about live machine working include system, user information system process, network sockets and processes[20].

G. Memoryze

A free tool developed by Mandiant used to collect, analyze the image of memory was taken, this tool using special batch files for this process using a live system to acquiring image that contains network sockets, system process, and other digital evidence will be founded[20].

H. Helix3

Helix3 has GUI used to obtain RAM image, and create reports includes special information need in an investigation such as operating system version, host information name, IP, existed logical drives, the investigator using time and date labeled command it has the ability for creating md5 hash log files[20]. This tool [1] says is based on Live cd live suite , open source used in an incident reaction that contains hex editor,password cracking its commercial version ,can obtain memory information such as network configuration , services ,schedule jobs, windows registry chat logs,display snapshot,drivers, analysis the collected information to generate reports. As [21] the result of the different processing time between memory forensic tools showing in Fig .3

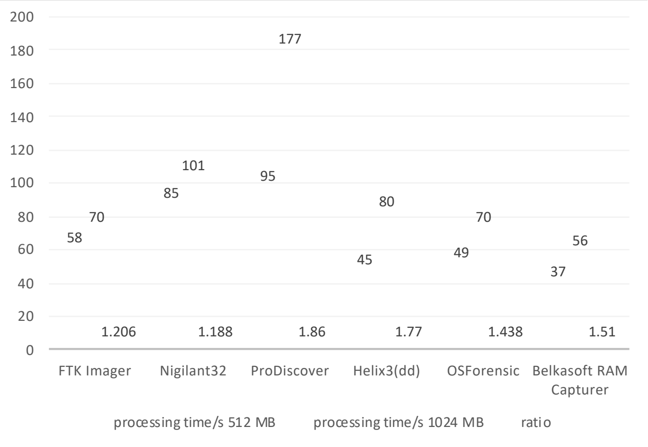

Fig.3 Processing Time for Memory Forensic Tools

VIII. MOBILE FORENSIC

A. MOBILedit

The mobile forensic tool used for view, extract data from mobile contact list, calling history, message,multimedia SMS,files,notes, reminders, calendar,application raw data,IMEI,Mobile OS, sim card details, ICCID, and locations,also used for retrieving data from mobile memory with the ability to bypass security pin phone backup, passcode, it supports physical consumption of Android devices and the SD card[9].

B. Andriller

Free tool compatible with latest smartphones, and widely used tool because its multiple functions, it retains the original recovered data without altering (read only type) and accepted forensically, it has the ability to bypass screen pattern lock and pin code,and it can decrypt the application data using android databases for communication decoder, export the report as excel,HTML files,it contains a large list for decrypt files and databases[9].

C. WhatsApp Key/DB Extractor WhatsApp

Based on experiment for [11], this tool specially used for social WhatsApp for extract text messages and photos but could not retrieve videos, text messages located in ”msgstore.db” and contain information such as sender, reception,content, time for all participations and attachment useful for investigation,WhatsApp group members and information about the group located in “wa.db”, contact can be read using SQLite studio and the information is contact numbers, and it is detailed.

D. Belkasoft Evidence

A Forensic tool used to extract WhatsApp information such as videos with file size and access date but deferent resolution than original,images information like file name and access date,pixel and file size it has the same original information,the document information such as creators name,apps used, file size, name and this tool capable of viewing the photos and showing document content and playing the retrieved videos[11].

E. Oxygen Forensic

Based on experiment for [22], this tool has the ability to perform logical and physical acquisition, and retrieve information from smartphones such as IMEI, IMSI,according to NIS MDT-CA-06 parameters,it has features to collect all data and not support selecting individual acquired data, it can obtain photos, document,videos information such name, format and size with fine quality, it has own video player for showing content.

IX. NETWORK FORENSIC

These tools are a branch of digital forensic that inhales live packets. The main goal is to extract digital evidence within live networks, and this is done by extracting evidence from live packet information, such as these tools[16].

A. NMAP

This tool is used within the network to scan ports for network protocols that control network security, and also provide services on a computer network such as host discovery, in addition to mapping network services. It is used to manually send some packets to the target host and analyze the content and ports information of the target and the source[16].

B. WinPcap

Use this tool to capture packets from networks, it can support obtain remote packet capture,and kernel-level filtering for packets,it supports IEEE 802.11b/g wireless networks, also it is compatible with Windows OSes, it can capture CTS,RTS control frames,and capture Probe Response and request as management frames, also capture traffic based on 802.11 data frames that responsible on authentication[23].

C. Ethereal

It is used to analyze network packets by capturing them directly from the network and it also filters according to the user's need and displays the information for all the protocols used to transfer the captured packets and displays the results in color for each type of packet, it is considered a program that supports many operating systems (Windows, UNIX,Linux) and is open source. In addition, it can be run in a mixed mode suitable for capturing multi-protocol packets, such as the (TCP)transport control protocol, the (ARP) address resolution protocol, and the (UDP) datagram protocol, and at the end, it displays the packages with detailed information about them[24].

X. CONCLUSION

The development in computers and smart phones from the hardware, software, and operating systems that operate on it, there have become many electronic crimes that use these devices as masterminds of electronic crime and exploit communication means such as local networks and the Internet to reach the victim without the presence of deterrent limits in most cases, considering the crime consists From three elements (the criminal, the tool, and the victim) we dealt in this research with electronic forensic tools specialized in identifying the tool of the crime and the criminal alike, and it resulted that there are many tools that need updates to close the existing gap, to find the appropriate tool that serves the investigation in a way Whole. At the end of the research, there is Table.1 that contains the requirements, strengths, weaknesses, and training needed by most of the electronic forensic tools that have been talked about.

In future work, we will analyze part of the forensic tools in a practical way for comparison in terms of speed of performance and accuracy of results in finding evidence.

XI. References

[1] B. V Prasanthi, "Cyber Forensic Tools: A Review," Int. J. Eng. Trends Technol., vol. 41, no. 5, pp. 266–271, 2016, doi: 10.14445/22315381/ijett-v41p249.

[2] K. Ghazinour, D. M. Vakharia, K. C. Kannaji, and R. Satyakumar, "A study on digital forensic tools," IEEE Int. Conf. Power, Control. Signals Instrum. Eng. ICPCSI 2017, pp. 3136–3142, 2018, doi: 10.1109/ICPCSI.2017.8392304.

[3] D. C. P. J. Taylor et al., "Forensic investigation of cross platform massively multiplayer online games: Minecraft as a case study," Sci. Justice, vol. 59, no. 3, pp. 337–348, 2019, doi: https://doi.org/10.1016/j.scijus.2019.01.005.

[4] M. Asim, D. R. McKinnel, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, and G. Epiphaniou, "Big Data Forensics: Hadoop Distributed File Systems as a Case Study BT - Handbook of Big Data and IoT Security," A. Dehghantanha and K.-K. R. Choo, Eds. Cham: Springer International Publishing, 2019, pp. 179–210.

[5] K. Nagrabski et al., "Distributed Filesystem Forensics: Ceph as a Case Study BT - Handbook of Big Data and IoT Security," A. Dehghantanha and K.-K. R. Choo, Eds. Cham: Springer International Publishing, 2019, pp. 129–151.

[6] Y.-Y. Teing et al., "Private Cloud Storage Forensics: Seafile as a Case Study BT - Handbook of Big Data and IoT Security," A. Dehghantanha and K.-K. R. Choo, Eds. Cham: Springer International Publishing, 2019, pp. 73–127.

[7] N. Jain and D. R Kalbande, "A Comparative Study based Digital Forensic Tool: Complete Automated Tool," Int. J. Forensic Comput. Sci., vol. 9, no. 1, pp. 22–29, 2014, doi: 10.5769/j201401003.

[8] M. Raji, H. Wimmer, and R. J. Haddad, "Analyzing Data from an Android Smartphone while Comparing between Two Forensic Tools," Conf. Proc. - IEEE SOUTHEASTCON, vol. 2018-April, pp. 1–6, 2018, doi: 10.1109/SECON.2018.8478851.

[9] N. R. Roy, A. K. Khanna, and L. Aneja, "Android phone forensic: Tools and techniques," Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2016, pp. 605–610, 2017, doi: 10.1109/CCAA.2016.7813792.

[10] M. Betts, J. Stirland, F. Olajide, K. Jones, and H. Janicke, "Developing a State of the Art Methodology & Toolkit for ICS SCADA Forensics," vol. 1, no. 2, pp. 44–56, 2016.

[11] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile forensic tools evaluation for digital crime investigation," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 3, pp. 949–955, 2018, doi: 10.18517/ijaseit.8.3.3591.

[12] A. H. Lone and R. N. Mir, "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer," Digit. Investig., vol. 28, pp. 44–55, 2019, doi: 10.1016/j.diin.2019.01.002.

[13] EC-council, "What is Digital Forensics | Phases of Digital Forensics | EC-Council." https://www.eccouncil.org/what-is-digital-forensics/#phase-ix---testify-as-an-expert-witness (accessed Dec. 18, 2020).

[14] D. R. Kamble and N. Jain, "Digital Forensic Tools : a Comparative Approach," Int. J. Adv. Res. Sci. Eng. IJARSE, vol. 8354, no. 4, 2015.

[15] V. R. Ambhire, "Digital Forensic Tools," IOSR J. Eng., vol. 02, no. 03, pp. 392–398, 2012, doi: 10.9790/3021-0203392398.

[16] M. Lovanshi and P. Bansal, Data, Engineering and Applications. Springer Singapore, 2019.

[17] N. Bassetti, "CAINE Live USB/DVD - computer forensics digital forensics." https://www.caine-live.net/ (accessed Dec. 19, 2020).

[18] R. J. Mcdown, C. Varol, L. Carvajal, and L. Chen, "In-Depth Analysis of Computer Memory Acquisition Software for Forensic Purposes," J. Forensic Sci., vol. 61, no. January, pp. 110–116, 2016, doi: 10.1111/1556-4029.12979.

[19] forensics Magnet, "MAGNET RAM Capture - Magnet Forensics." https://www.magnetforensics.com/resources/magnet-ram-capture/ (accessed Dec. 19, 2020).

[20] L. Carvajal, C. Varol, and L. Chen, "Tools for collecting volatile data: A survey study," 2013 Int. Conf. Technol. Adv. Electr. Electron. Comput. Eng. TAEECE 2013, no. May 2019, pp. 318–322, 2013, doi: 10.1109/TAEECE.2013.6557293.

[21] K. M. A. Kamal, M. Alfadel, and M. S. Munia, "Memory forensics tools: Comparing processing time and left artifacts on volatile memory," IWCI 2016 - 2016 Int. Work. Comput. Intell., no. December, pp. 84–90, 2017, doi: 10.1109/IWCI.2016.7860344.

[22] R. Umar, I. Riadi, and G. Maulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 12, pp. 69–75, 2017, doi: 10.14569/ijacsa.2017.081210.

[23] B. Bikash and S. Priya, "Survey on Real Time Security Mechanisms in Network Forensics," Int. J. Comput. Appl., vol. 151, no. 2, pp. 1–4, 2016, doi: 10.5120/ijca2016911676.

[24] N. Meghanathan, S. R. Allam, and L. A. Moore, "Tools and techniques for Network Forensics," no. 1, pp. 14–25, 2010, doi: 10.5281/zenodo.1216806.

[25] Michael, "DFSP # 025 – RAM Extraction Tools – Part 2 – Digital Forensic Survival Podcast," 2016, Aug. 09, 2016. https://digitalforensicsurvivalpodcast.com/2016/08/09/dfsp-025-ram-extraction-tools-part-2/ (accessed Jan. 01, 2021).

Table .1 Comparison Between Forensic Tools

#	Comparison Between Forensic Tools				
	Tools	Requirement	Advantages	Disadvantages	Training
1	Encase	Windows, DOS, Linux ,MAC	[7]Authenticate /court acceptance Disk imaging Data carving Data recovery Password recovery Decryption Memory dump analysis Email Analysis File Supported System (NTFS, UFS ,FAT12/16/ 32, JFS, ext3, ext2, aixj journaling)	Static Analysis Hard to use Paid software [15] Does Not have log file for investigators Confusing when searching	Need full course training (certificate)
2	Digital Forensic Framework (Dff)	Windows , Linux	open Source Authenticate /court acceptance Disk imaging Data carving Data recovery Decryption Memory dump analysis File Static and Live Analysis Supported System (HFS and NTFS, FAT32/12/16, ext3, ext2)	No Password recovery No Email Analysis	Required minimum training
3	Computer Online Forensic Evidence Extractor (Cofee)	Windows	Authenticate /court acceptance Incident Response Disk imaging Data carving Data recovery Decryption Memory dump analysis File Static and Live Analysis Supported System (HFS and HFS+, ext2, ext 3, ext4, XFS, FAT12/16/ 32, exfat, NTFS, HPF S, APFS, UFS,)	No Email Analysis Only Live Analysis Support windows only Some tools used command line	Required full course training
4	Prodiscover	Windows , Linux	GUI Commercial Disk imaging Data carving Data recovery Password recovery Decryption Memory dump analysis File Supported system (FAT12/16/ 32, ext2, ext3 NTFS and UFS)	Only Live Analysis No Email Analysis Not Authenticate /court acceptance	[20]Required minimum training
5	Computer Aided Investigative Environment (Caine)	Windows, Linux, and some Unix Systems Live Linux distribution	open-source Authenticate /court acceptance Half-automated report generator GUI- user friendly File Systems support: ISO 9660,FAT/exfat, HFS ,NTFS, Ext3, Ext2	Needs background on Linux	Required minimum training
6	Forensic Toolkit (Ftk)	Windows XP/Vista /7/8/10	GUI Authenticate /court acceptance Disk imaging Data carving [2]Data recovery Password recovery Decryption Memory dump analysis email viewer build in Live Analysis [15](KFF) Known File Filter feature aids [2] File Supported system (FAT16/3 2, NTFS, ext2 and ext3) Uses MD5 Hash	Only Static Analysis [20]Do not provide report Slower importing image to FTK Hard to use Paid software Support windows only [15]The time to import the image restricts the image analysis process Weak customizable interface than others	Need full course training (certificate)
7	Bulk Extractor	Windows, Linux and Mac	Authenticate /court acceptance Disk imaging Data carving Data recovery Password recovery Decryption	No Memory dump analysis [2]only Live Analysis	Required minimum training

			Email Analysis [2] File Supported system (FAT12/16 /32, NTFS, UFS, JFS, ext2, ext3, reiserfs)		
8	The Sleuth Kit	Unix ,Windows, Mac OSX ,BS Dpartition s,DOS	open-source suite Autopsy browser for GUI support Authenticate /court acceptance Disk imaging Data carving Data recovery Email Analysis File Supported system (ISO9660, HFS+, NTFS, Yaffs2 and UFS, FAT32/12/16/exf AT, Ext2/Ext3 /Ext4, CD-rom)	No Memory dump analysis No Password recovery Only Live Analysis [2]not support Decryption Needs background on Linux	Required minimum training
9	Sans Investigative Forensic Toolkit (Sift) Sift	Ubuntu	Incident Response Disk imaging Data carving Data recovery Memory dump analysis File Supported system (FAT12 /16/32,HFS+, ext2,ext3,ext4, UFS1, FS2, NTFS)	No Password recovery No Email Analysis Only Live Analysis [2]no Decryption	Need full course training (certificate)
10	Hxd (Hex Editor)	Windows XP, 2003, Vista, 7, 8 or 10	GUI Authenticate /court acceptance Commercial Available in portable or installer Checksum-generator SHA-1,MD5,SHA-512,CRC Fast and flexible search Export data to several types (plan text, rich text , html , tex)	Support windows only	Required minimum training
11	Volatility	Windows/server2012, Linux, Mac OSX	Free software GUI or WEB interface Incident Response Running Processes list Each process has list of uploaded DDL Display names of the open files for each process Profiles of new OS quite fast appear in the repository Working with loadable kernel module, addressable memory List of open network sockets Stores profiles for various operating systems in a large repository	Paid software Not Authenticate /court acceptance Command line To run need python	Required minimum training
12	Magnet Ram Capture	Windows XP, Vista, 7, 8, 10, 2003, 2008, 2012 (32 and 64 bit support)	Free software Export data from memory as raw (.dmp/. Raw/.bin) Malware intrusion evidence Registry hives Decrypted files and keys	[25]Heavy ram footprint Not display extracted mount of ram	Required minimum training (software certificate)
13	Nigilant32	MS Windows	GUI Commercial open source Incident response [20]Live machine snapshot current network ports and processes	Limited features	Required minimum training
14	Memoryze	MS Windows	output reports XML format Results of batch process analysis live system or acquired image	[20]Command line	[20]Required minimum training
15	Helix3	MS Windows, Linux	[20]GUI freeware Incident Response About system information extracted as PDF report	Do change to existing OS Change the registry	[20]Required minimum training
16	Oxygen Forensic	Apple ios, Android devices Windows, macos, and Linux	GUI zero-footprint operation detect malicious and spyware apps [22]Logical and physical Acquisition Artifact (whatsapp Contact List , Call Log, Text, Image Video, Document)	[9]Paid software	Need full course training (certificate)
17	Mobiledit	Support iphone and Android, Blackberry, Windows Mobile, Symbian, Windows Phone, Chinese phones, Meego, Bada, and CDMA phones	GUI bypass passcode, pin code restore deleted information from phone memory physical acquisition extraction and viewing data	Paid software Not Authenticate /court acceptance	Required minimum training (product certificate)
18	Andriller	Android devices and some apple IOS Ubuntu/Debian,Windows,	GUI Bypass pattern, passcode, PIN code Excel and HTML format reports	Paid software Python requirement	Required minimum training

		Linux/Mac	Data extraction with root permissions Data extraction of non-rooted and rooted android		
19	Whatsapp Key/DB Extractor Whatsapp	Support Android 4.0 or higher Run on Mac OS X ,Windows, and Linux	GUI [22]Logical Acquisition Artifact for whatsapp (Contact, List, Call Log ,Text , Image)	Not support Logical Acquisition Artifact for whatsapp (Video, document) Not support physical Acquisition Artifact	Required minimum training
20	Belkasoft Evidence	Windows including XP, Vista, Windows 7/8/10, 2003 and 2008 Server	GUI Commercial [22] Logical Acquisition Artifact for whatsapp (Image, video, document) Physical Acquisition Artifact GUI Authenticate /court acceptance Incident response	Not support Logical Acquisition Artifact for whatsapp (Contact List, , Call Log, Text) No split RAM Image Extraction path must enter manually	Need full course training (certificate)
21	Nmap	Linux (all distributions) Microsoft Windows Mac OS X Freebsd, openbsd, and netbsd Sun Solaris Amiga, HP-UX, and Other Platforms	[16]Free software Packet sniffing Packet analyzer Packet spoofing Scan open port Support ipv6 Faster network scanning v7.0 Best TLS/SSL Scanning	NSE scripts are written in lua language Scanning weaker devices cause an Unintentional DOS or network slowdown	Required medium Training
22	Winpcap	MS Windows OS	Open source and commercial GUI [24]kernel-level packet filtering remote packet capture Capture control frames (ACK, RTS, CTS) measure wireless transmission efficiency	Only support windows	Required minimum training