International Journal of All Research Education and Scientific Methods (IJARESM), ISSN: 2455-6211
Volume 10, Issue 4, April-2022, Impact Factor: 7.429, Available online at: www.ijaresm.com

Relevance of Computer Forensics in Security

S Danvi Sai Sapthasw Reddy[1], C Prudhvi Raj[2], Dr. S Balaji[3], S.V. Swetha[4]

[1,2,3]CSE, KLEF (Deemed to be University)
[4]XIME Bangalore

--*****************--

ABSTRACT

Cyber-attacks are on the rise, both in terms of quantity and intensity. When an assault occurs, the attacked company performs a series of preset activities. One of these acts is the use of digital forensics to aid in the recovery and examination of data stored on digital media and networks. Capture and analysis of digital data are used in cyber forensic investigations to establish or deny whether or not an internet-related theft has occurred. Previously, computers were simply used to store enormous amounts of data and execute a variety of operations on them, but they have since grown and taken on a more prominent role in criminal investigations. The selection and use of forensic technologies is critical in order to tackle these cyber-related issues. Many cyber forensic tools have been developed by the creators for improved study and investigation. The instruments are chosen by police departments and investigative organizations depending on a variety of variables, including funding and the availability of professionals on the team. This article discusses the relevance of computer forensics and its origins, as well as the forensic framework and many types of existing computer forensic tools and their applications.

INTRODUCTION

Digital forensics is a branch of forensic science concerned with the recovery and evaluation of data from digital devices, and it is widely employed in computer crime investigations. It comprises solving a crime and providing evidence to support a claim utilizing computer-assisted investigation and analysis. It is the process of locating, preserving, assessing, and presenting digital evidence in a legal-admissible manner. Using cyber forensic methods, it is rather straightforward to analyze the evidence. It may be used for a number of things, such as checking food quality and predicting fire disasters.

The vast majority of the first computer-related criminal convictions were for financial fraud, which is now combated by Biometric Smart Cards . Cyber security is supported by biometrics and digital forensics. In criminal investigations, biological evidence is crucial. It contains Deoxyribose Nucleic Acid (DNA) [4, which may be used to link a perpetrator to a crime scene. It examines evidence from crime sites to check if any biological material is present Biological traits include fingerprint, hair, Olfactory, teeth, palm veins, DNA, skin, bones, blood, nails, exhaled breath etc.,

HISTORY

Digital forensics is approximately 40 years old, having started in the late 1970s in response to a need from the law enforcement community for the service. As the number of computer crimes increased in the 1980s, investigators began to consider computers as sources of evidence. The first steps in digital forensics training have been taken by law enforcement. In 1984, the FBI's Computer Analysis and Response Team assisted FBI field offices with the search and seizure of computer evidence, as well as forensic exams and technical support for FBI investigations. During this time, the Federal Law Enforcement Training Center was established. The use of the internet began in the 1990s, and the consumerization of technology increased. This implies that technology is used in criminal activity, and the fast rise of the Internet has made cyber-attacks easier.[1] The International Law Enforcement Academy was founded in 1995 with the goal of reducing crime, combating terrorism, and sharing information and training. The Scientific Working Group on Digital Evidence (SWGDE) was founded in 1997 to set standards in the field of digital evidence. Forensics. Various law enforcement authorities have been developing guidelines during this time. The private sector's training and development remains stagnant. SANS Institute was also invited. In the 2000s, cybercrime flourished, and the incorporation of technologies such as mobile phones grew tremendously as key sources of technological evidence, as well as the use of technology in crimes. The creation of research for the Digital Forensic Research Workshop (DFRWS) began in 2001. It is utilized to bring together researchers, industry, tool developers, academia, law enforcement, and the military in order to address the issues of digital forensics science. Digital forensics has progressed from being a set of investigation procedures to a full-fledged forensic science. [2]In the commercial sector, there has been a lot of progress in terms of digital forensics training courses and programmes.

BRANCHES OF DIGITAL FORENSICS

A. Computer Forensics

Computer forensics shows the current condition of an automated data processing system and collects evidence from a variety of media such as PCs, embedded systems, USB pen drives, and other similar devices. It looks at system logs and web browsing history. Hidden, erased, temporary, and password-protected files, sensitive documents and spreadsheets, file transfer logs, text chat logs, Internet browser history, pictures, graphics, videos, and music are some of the artifacts that may be obtained through such investigations. The event logs and system logs have been checked. Inspection of illegal, pirated, and legal code installations.[1]

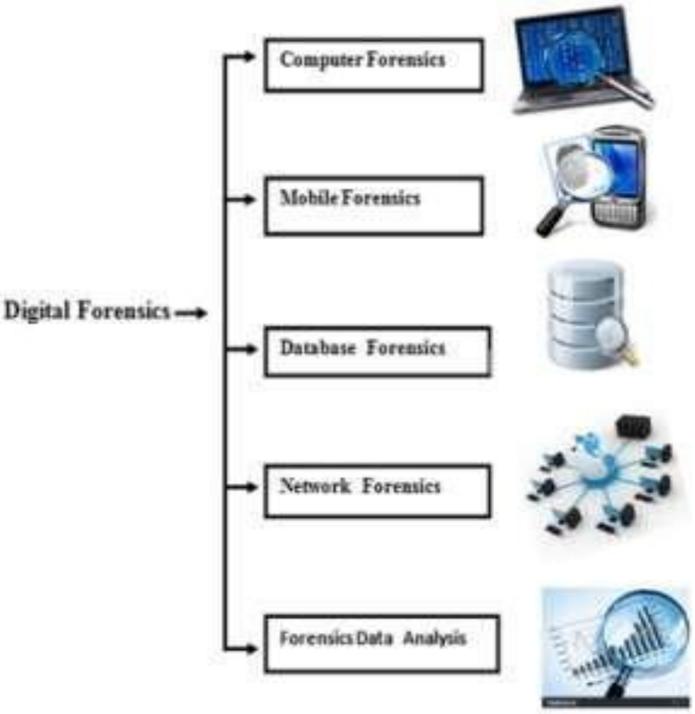

Fig.1 Types in Digital Forensics

B. Mobile Device Forensics

It examines call records and text messages (SMS/Email) and recovers digital evidence from a mobile device. It uses GPS or cell website records to offer location information. It also looks at communication apps like BBM, WhatsApp, and Web Chat. It is possible to see the phone number and information about the service provider. Incoming and outgoing phone records, SMS, Emails, IRC conversation logs, and contact information from address books and calendars are all exposed. Here, security is a bigger worry.

C. Network forensics:

LAN/WAN/internet traffic is monitored and analyzed by Network Forensics (even at the packet level). It collects and analyses logs from many different sources. [5]It determines the scope of the incursion and, as a result, the amount of data obtained.

D. Database forensics:

It is a forensic investigation of databases and their contents. Database contents, log files, and in-RAM data are all investigated. To alter and analyze the data, a variety of software applications are utilized. This programme allows you to keep track of audits.

E. Forensic data analysis:

It deals with financial fraud investigations and financial document correlation. It is carried out in collaboration with

Certified Fraud Examiners.

TYPES OF FORENSICS FRAMEWORKS

A. *VIRTUAL FORENSICS FRAMEWORK*

A well-known framework for digital forensics is the Digital Forensics Framework. The gadget is open source and distributed under the terms of the GNU General Public License. Both professionals and non-professionals may use it without trouble. It may be used to construct a virtual chain of custody, get access to distant or local devices, do forensics on Windows or Linux, recover lost files, search for documents and metadata, and execute a range of other activities.[4]

B. OPEN COMPUTER FORENSICS ARCHITECTURE

One of the most well-known distributed open-source Cyber forensics frameworks is the Open Computer Forensics Architecture (OCFA) . This framework is based on the Linux platform and stores records in a PostgreSQL database. It was developed by the Dutch National Police with the purpose of automating virtual forensics procedures. It is available for download under the GPL license.

C. CAINE

CAINE (Computer Aided Investigative Environment) is the Linux distro created for virtual forensics. Free to use(open source).

D. X-WAYS FORENSICS

X-ways Forensics was once used by digital forensics examiners. It is compatible with all versions of Windows. It claims to be resource efficient as well as perform well. The following are the characteristics: The imaging and cloning of discs is completed. It can read document gadget systems contained inside a variety of picture files. FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3®, CDFS/ISO9660/Joliet, and UDF are among the document systems it supports. It is possible to discover deleted or missing hard drive partitions automatically. It is used to carry out a variety of information recovery procedures as well as effective file cutting. The usage of templates allows for bulk hash computation and visualization, as well as improving binary facts structure.[1] The record heading is well-kept and retrievable. Interest logging is done using computers, and figures are verified. The entire case is managed, memory and RAM are evaluated, and a gallery view for photographs is used. The internal reader for the Windows registry document is analyzed, as well as the automated registry report. It can extract metadata from a variety of report formats, and it can also retrieve emails from a variety of email clients.[5]

E. SANS INVESTIGATIVE FORENSICS

TOOLKIT – SIFT

The SIFT Workstation is a collection of free and open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. It can match any current incident response and forensic tool suite.

F. ENCASE

EnCase is another popular multi-reason forensic platform with many exceptional tools for numerous areas of the digital forensic system. This tool is accurate and fast in collecting/extracting facts from diverse devices and potential proof.

G. REGISTRY RECON

A prominent registry analysis tool is Registry Recon. The registry information is extracted from the evidence, and the registry illustration is rebuilt. [3]It has the ability to re-create registries from both current and previous Windows installations. It is not a free programme.

H. THE SLEUTH KIT

The Sleuth Kit is a UNIX and windows based tool which allows forensic analysis of computers. It provides users with multiple equipment which helps in digital forensics. These tools help in analyzing disk images, performing in-intensity analysis of document systems, and numerous different matters.

I. LIB FORENSICS

For designing digital forensics apps, Libforensics is used. It was built in Python and Spring with a variety of demo gear to extract data from various types of evidence.

J. VOLATILITY

The memory forensics framework is called volatility. It's used for malware analysis and incident response. We can extract information from ongoing operations, network sockets, network settings, DLLs, and registry hives with this programme. It also has the ability to extract data from Windows crash dump files and hibernation files. This gadget is available for free under the GPL license.

K. WINDOWS SCOPE

Any other memory forensics and reverse engineering device used to analyze unstable memory is known as Windows SCOPE.[2] It's mostly used for malware reverse engineering. It has the ability to research the Windows kernel, drivers, DLLs, and digital and physical memory.

L. THE CORONER'S TOOLKIT

The Coroner's Toolkit or TCT is likewise a great virtual forensic analysis tool. It is executed in multiple Unix-associated operating systems. It is used to get lost data and works great during disasters.

M. OXYGEN FORENSIC SUITE

Oxygen Forensic Suite is the best programme for gathering evidence from a mobile phone to assist with any case. This gadget aids in the collection of tool statistics (such as the manufacturer, operating system, IMEI number, and serial range), contacts, messages (emails, SMS, MMS), improved deleted messages, name logs, and calendar information. It also allows us to access and analyze data and documents from mobile devices. It creates easy-to-understand reports for better understanding.

N. BULK EXTRACTOR

Bulk Extractor is a well-known virtual forensics tool. It extracts useful data from disc snapshots, files, or directories of documents. This procedure ignores the document system's structure, making it faster and offering equivalent tool options. Intelligence and law enforcement organizations use it extensively to combat cybercrime. It has a comparable structure, thus it is faster and has similar types of

O. XPLICO

Xplico is a network forensic analysis device that is free source. It's mostly used to extract meaningful data from apps that employ network and internet protocols. It supports a wide range of well-known protocols, including HTTP, IMAP, POP, SMTP, SIP, TCP, UDP, TCP, and others. The tool's output statistics are recorded in the MySQL database's SQLite database. It also aids both IPv4 and IPv6 Mandiant. RedLine is a well-known memory and file analysis programme. To create an appropriate file, it gathers information about the current process on the host, drivers from memory, and Meta facts, registry statistics, responsibilities, services, network statistics, and net history.[4]

Q. COMPUTER ONLINE FORENSIC EVIDENCE

EXTRACTOR (COFEE)

Computer On-line Forensic Evidence Extractor (COFEE) is a device package advanced for computer forensic specialists. This tool has been further developed by Microsoft and used in windows. It can be uploaded on a USB pen drive or external hard disk. Connect the usb/external disk to the target PC and it begins a live evaluation. It comes with 150 different kinds of tools with a GUI based totally interface to command the equipment. It is rapid and can perform the complete analysis in as few as 20 mins. To law enforcement agencies, Microsoft provides free technical support for the tool.

R. P2 EXPLORER

P2 Explorer is a forensic image mounting tool that aims to aid investigators in their investigation of a case. You may use this image to mount forensic snap photos as a read-most effective neighborhood and physical disc, and then use a report explorer to find the contents of the photo. It's simple to see erased facts and unallocated image space. It has the ability to mount many photos at once. EnCasem, Safe Back, PFR, FTK DD, Win Image from Linux DD, and VMware snapshots are among the image formats supported. Both logical and physical picture formats benefit from it.

S. PLAINSIGHT

PlainSight is another useful virtual forensics device. It is a CD primarily based on Knoppix that is a Linux distribution. Its uses are viewing internet histories, statistics carving, checking USB device usage, memory dumps extracting password hashes, statistics amassing, inspecting windows firewall configuration, seeing current files, and different useful duties.

T. XRY

Micro Systemation has enhanced XRY, a mobile forensics tool. It's used to analyze and improve vital statistics from mobile devices. A hardware tool and software are included with this device. Hardware links mobile phones to computers, while software evaluates the tool and extracts statistics. It's all about obtaining superior statistics for forensic analysis. The tool's most recent version can recover data from many types of smartphones, including Android, iPhone, and BlackBerry. It collects information such as call statistics, photographs, SMS, and textual content messages that have been erased.

U. HELIX3

HELIX3 is a live CD-based forensic suite that is totally virtual. It was created with incident response in mind. It provides a number of free virtual forensics tools, including as hex editors, data carving software, and password cracking software. In it, there is a free model called Helix3 2009R1. Following its release, this project was picked up by a commercial vendor. This device's data comes from a variety of sources, including physical memory, network configuration, consumer debts, operating methods and services, scheduled jobs, Windows Registry, chat logs, display screen captures, SAM documents, programmes, drivers, environment variables, and internet records.[2] The system then analyses and assesses the information before compiling the final conclusions, which are totally based on reports.

FREE COMPUTER FORENSIC TOOLS

Few existing free computer forensic tools are explained in Table I.

CONCLUSION

As the computer and cellphone markets have grown in recent years, the area of digital forensics has grown in popularity. Cyber forensics has grown increasingly prevalent as the usage of digital data and mobile phones has increased, and cyber thefts have also increased as the day progresses. This article demonstrates a few existing and widely used digital forensics technologies used by law enforcement organizations to conduct criminal investigations. This area will allow for the recovery of critical electronic evidence that has been lost, erased, destroyed, or hidden, and will be used to prosecute anyone who feels they have defeated the system.

TABLE I : COMPUTER FORENSIC TOOLS

Application of Forensic Issues	**Tools used**
Disk tools and data capture	Autopsy, The Sleuth Kit, X-Ways Forensics, AccessData FTK, EnCase, Mandiant RedLine, Paraben Suite, Bulk Extractor
Email Analysis	eMailTrackerPro, EmailTracer, Adcomplain, Aid4Mail Forensic, AbusePipe, AccessData's FTK, Paraben (Network) E-mail Examiner
Mac OS tools	RECON for Mac OS X, PALADIN, File XRAY, DCFLDD, File Juicer, Xcode, SQLITE Database Browser,PASSWARE
Internet Analysis	Belkasoft Evidence Center, BURP, Cellebrite Inspector, Cellebrite Physical Analyzer, Chrome Thief, E3:Universal, Elcomsoft Cloud Explorer, Elcomsoft Internet Password Breaker
Registry analysis	Registry analysis

Application Analysis	Dropbox Decryptor ; Google Maps Tile Investigator; KaZAlyser; LiveContactsView; SkypeLogView
Memory forensics	Volatility, WindowsSCOPE
Network analysis	Wireshark, Network Miner, Xplico
Mobile device forensics	Oxygen Forensic Detective, Cellebrite UFED, XRY,
Linux distros	CAINE, SANS SIFT, HELIX3

REFERENCES

[1]. Berners-Lee T, Masinter L. RFC 1738:Uniform Resource Locator(URL), http://tools.ietf.org/html/rfc1738.

[2]. Nicole Beebe Digital forensics research: the good, the bad, and the unaddressed Fifth annual IFIP WG 11.9 international conference on digital forensics (January 2009)

[3]. M. Reith, C. Carr, and G. Gunsch, “An examination of digital forensic models,” International Journal of Digital Evidence, vol. 1, no. 3, Fall 2002.

[4]. Development of fusion biometric system for atm machines Balaji, S., Janga Reddy, M., Khan, H., Mounika, K. International Journal of Mechanical Engineering and Technology, 2017, 8(7), pp. 649–655

[5]. A novel method for enhancing biometric systems security using watermarking Balaji, S., Janga Reddy, M., Khan, H. Journal of Engineering and Applied Sciences, 2017, 12(Specialissue8), pp. 8421–8425