# Cyber Forensic Tools: A Review

B. V. Prasanthi

*Assistant Professor & Department of Computer Science & Engineering*
*Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, India*

***Abstract*—***Cyber attacks are fast moving and increasing in number and severity. When the attacks occur, the attacked enterprise responds with a collection of predetermined actions. Applying digital forensics helps in the recovery and investigation of material on digital media and networks is one of these actions. Cyber Forensic Investigation includes the Capture & Analysis of digital data either to prove or disprove whether the internet related theft has committed or not. Earlier Computer are used only for storing large volumes of data & perform many operations on it ,but now a days it has expanded & occupied prior role in Crime Investigation. In order to solve this cyber related problems, selection & usage of Forensic tools is very important. For better research and quick investigation, the developers have created many cyber forensic tools. Cop departments and investigation agencies select the tools based on various factors including budget and available experts on the team. This paper describes includes importance of computer forensics & its origin, forensic framework and different types of existing computer forensic tools and its usage.*

**Keywords —** *Digital Forensics and its frame work, Cyber forensics tools.*

## I. INTRODUCTION

Digital forensics [1] is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. Computer forensics is also known as cyber forensics. It involves applying computer investigation and analysis techniques to solve a crime and provide evidence to support a case. It is the process of identifying, preserving, analysing and presenting the digital evidence in such a manner that the evidences are legally acceptable. By using cyber forensic [2] tools it is very easy to probe the evidence. It involves various applications like analysing the quality of food and predicting the fire disasters etc.

Most of the first criminal cases that involved computers were for financial frauds which are now overcome by Biometric Smart Card [3] .Energising Cyber security with biometrics & Digital Forensics. Biological evidence also plays major role in crime investigation. It contains Deoxyribo Nucleic Acid (DNA) [4], which connects an offender to a crime scene. It examines evidence from crime scenes to determine if biological material [5][6] is present. Biological traits includes fingerprint, hair, Olfactory, teeth, palm veins, DNA, skin, bones, blood, nails, exhaled breath etc.,

## II. HISTORY

Digital forensics [7] is nearly 40 years old, beginning in the late 1970s as a response to a requirement for the service from the law enforcement community. The rise of computer crimes started in the 1980's meant that investigators began to look at computers as sources of proof. The Law enforcement began initial training efforts in digital forensics. In the year 1984 Computer Analysis and Response Team provided assistance to FBI field offices in the search and seizure of computer evidence as well as forensic examinations and technical support for Federal Bureau of Investigation investigations. Establishment of Federal Law Enforcement Training Centre during this period.

In the year 1990's the usage of internet has started and increase in consumerization of technology has done. This means that technology is involved in crimes, and the rapid growth in Internet facilitated cyber attacks. International Law Enforcement Academy is established in 1995 to reduce crime, combat terrorism, and share in knowledge and training.

In the year 1997 Scientific Working Group on Digital Evidence (SWGDE) was established to develop standards in Forensics .The development standards by various law enforcement bodies has done during this period. There is little growth in private sector training and development. SANS Institute also came into.

Cyber crime exploded in the 2000's and the integration of technologies such as mobile devices expanded as primary sources of technological evidence exponentially and as well as the use of technology in criminality. Digital Forensic Research Workshop (DFRWS) development of research was developed in the year 2001.It is used to bring together researchers, industry, tool, academics, enforcement, and military to tackle the challenges in digital forensics science. Digital forensics evolved from investigative techniques to a full forensic science. There is significant development in the private sector with regards to training courses and programs in digital forensics. Development of formal academic programs at universities had come into around the world during this period.

## III. TYPES OF DIGITAL FORENSICS

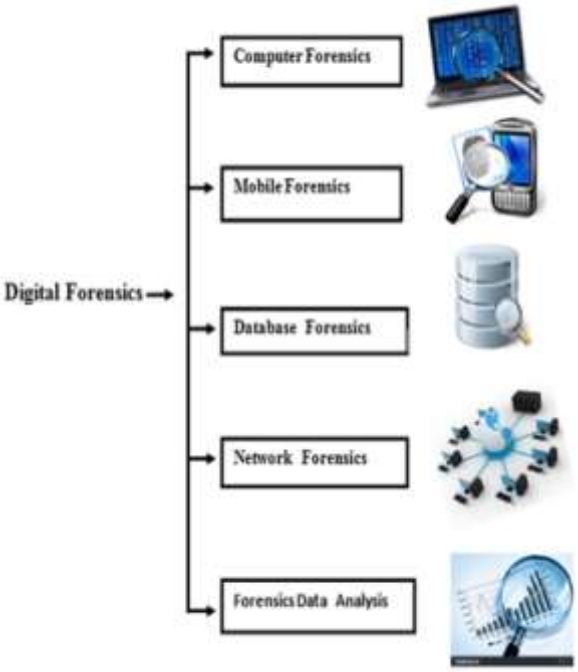


Fig.1 Types in Digital Forensics

### A. *Computer Forensics*

Computer Forensics reveals the present state of automatic data processing system and it obtains evidence from various media like computers, embedded systems, USB pen drives etc., It examines system logs and web history. Some of the artefacts can get from such investigations includes hidden, deleted, temporary and password-protected files, Sensitive documents and spreadsheets, File transfer logs, Text communication logs, Internet browsing history, Pictures, graphics, videos and music, Checking Event logs and System Logs is done. Checking of Illicit, pirated or legitimate code installations.

### B. *Mobile Device Forensics*

It recovers digital evidence from a mobile device and investigates call logs and text messages (SMS/Email).It provides location information via GPS or cell website logs. It also investigates communication stores like BBM, WhatsApp, Web Chat, etc. Phone number and service provider information can be viewed. History of Incoming and outgoing call logs,SMS, Emails, IRC chat logs, Contact details from address books and calendars are revealed. Security issues are more concerned here.

### C. *Network forensics:*

Network Forensics monitors and analyses LAN/WAN/internet traffic (even at the packet level).It
Retrieves and analyses logs from a wide variety of sources. It determines the extent of intrusion and therefore the quantity of data retrieved.

### D. *Database forensics:*

It is forensic study of databases and their data. Investigation is done on database contents, log files and in-RAM data. Many software tools are used to manipulate and analyse the data. This tools provides audit logging capabilities.

### E. *Forensic data analysis:*

It deals with Investigation for financial frauds and correlating with financial documents. Working closely with Certified Fraud Examiners is carried.

## IV. DIFFERENT TYPES OF FORENSICS FRAMEWORK

### A. *VIRTUAL FORENSICS FRAMEWORK*

Digital Forensics Framework is a famous platform dedicated to digital forensics. The device is open source and is derived beneath GPL License. It could be used both via experts or non-professionals with none hassle. It can be used for virtual chain of custody, to get right of entry to the far off or local devices, forensics of home windows or Linux OS, healing hidden of deleted files, short search for documents, meta data, and diverse other things.

### B. *OPEN COMPUTER FORENSICS ARCHITECTURE*

Open Computer Forensics Architecture (OCFA) [8] is one of the famous distributed open-source Cyber forensics frameworks. This framework builds on Linux platform and makes use of postgreSQL database for storing records. It was constructed by the Dutch National Police business enterprise for automating virtual forensics manner. It is to be downloaded under GPL license.

### C. *CAINE*

CAINE (Computer Aided Investigative Environment) [9] is the Linux distro created for virtual forensics. It offers a surroundings to combine present software program tools as software modules in a user friendly way. This tool is open source.

### D. *X-WAYS FORENSICS*

X-ways Forensics [10] is a prior platform for digital forensics examiners. It runs on all available versions of windows. It claims to not be very resource hungry and to perform effectively.
The features are as follows:
Disk imaging and cloning is done. It has the capacity to read document gadget systems inner numerous photo files. It supports maximum of the document systems together with FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3®, CDFS/ISO9660/Joliet, UDF. Automatic detection of deleted or lost hard disk partition is done. Diverse

information recovery strategies and effective file carving is carried. Bulk hash calculation & Viewing and enhancing binary facts structure the use of templates. Record header is well maintained and retrieved. Computerized interest logging and statistics authenticity is done. Entire case management, Memory and RAM evaluation, Gallery view for pictures is performed. Internal viewer for windows registry document and automatic registry report is evaluated. It Extracts metadata from numerous report types and it has the capability to extract emails from diverse available electronic mail clients.

### E. SANS Investigative Forensics Toolkit – SIFT

SANS Investigative Forensics Toolkit or SIFT [11] is a multi-cause forensic running device which comes with all the necessary tools used within the digital forensic technique. It is built on Ubuntu with many devices associated with digital forensics. Even SIFT 3.0 was released. It comes free of charge and incorporates unfastened open-source forensic tools.

### F. EnCase

EnCase [12] is another popular multi-reason forensic platform with many exceptional tools for numerous areas of the digital forensic system. This tool can swiftly gather facts from diverse devices and unearth potential proof. It additionally produces a record based totally at the evidence.

### G. Registry Recon

Registry Recon [13] is a popular registry analysis tool. It extracts the registry information from the proof and then rebuilds the registry illustration. It could rebuild registries from both present day and former home windows installations. It isn't a free tool.

### H. The Sleuth Kit

The Sleuth Kit [14] is a UNIX and windows based totally tool which allows in forensic analysis of computers. It comes with numerous equipment which helps in digital forensics. These tools help in analysing disk images, performing in-intensity analysis of document systems, and numerous different matters.

### I. libforensics

Libforensics [15] is used for developing digital forensics applications. It was developed in Python and springs with diverse demo gear to extract information from numerous forms of evidence.

### J. Volatility

Volatility [16] is the memory forensics framework. It used for incident reaction and malware evaluation. With this tool, we can extract data from running procedures, network sockets, network configuration, DLLs and registry hives. It additionally has support for extracting records from windows crash dump files and hibernation files. This device is of free of cost below GPL license.

### K. Windows Scope

Windows SCOPE [17] is any other memory forensics and reverse engineering device used for analysing unstable memory. It is largely used for reverse engineering of malwares. It offers the functionality of studying the home windows kernel, drivers, DLLs, digital and physical memory.

### L. The Coroner's Toolkit

The Coroner's Toolkit or TCT [18] is likewise a great virtual forensic analysis tool. It runs beneath several Unix-associated operating systems. It is used as useful resource evaluation of pc disasters and information healing.

### M. Oxygen Forensic Suite

Oxygen Forensic Suite [19] is best software to collect proof from a mobile phone to help any case. This device helps in accumulating tool statistics (which include producer, OS, IMEI number, serial range), contacts, messages (emails, SMS, MMS), get better deleted messages, name logs and calendar information. It also lets us get entry to and examine mobile device statistics and documents. It generates clean to recognize reports for higher knowledge.

### N. Bulk Extractor

Bulk Extractor [20] is one of the famous virtual forensics devices. It scans the disk snap shots, file or directory of documents to extract beneficial data. In this process, it ignores the document system structure, so it is quicker and had similar varieties of tool. It is largely utilized by intelligence and law enforcement agencies in solving cyber crimes.

### O. Xplico

Xplico [21] is an open source network forensic analysis device. It is largely used to extract useful records from applications which uses net and network protocols. It helps in most of the famous protocols such as HTTP, IMAP, POP, SMTP, SIP, TCP, UDP, TCP and others. Output statistics of the tool is saved in SQLite database of MySQL database. It also helps IPv4 and IPv6 both.

### P. Mandiant RedLine

Mandiant RedLine [22] is a popular tool for memory and file analysis. It collects information about current process on host, drivers from memory and gathers different information like Meta facts, registry statistics, responsibilities, services, network statistics and net history to build a proper file.

### Q. Computer Online Forensic Evidence Extractor (COFEE)

Computer On-line Forensic Evidence Extractor (COFEE) [23] is a device package advanced for computer forensic specialists. This tool turned into evolved by using Microsoft to accumulate evidence from windows devices. It could be mounted on a USB pen drive or external hard disk. Just plug within the USB tool inside the target pc and it begins a live evaluation. It comes with 150 different kind 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 [24] is a forensic picture mounting tool which pursuits to assist investigating officials with examination of a case. With this image, you can mount forensic snap shots as a read-most effective neighbourhood and physical disc and then discover the contents of the photo with report explorer. It is easy to view deleted facts and unallocated area of the image.It is able to mount several images at a time. It supports most of image formats consisting of EnCasem, safe Back, PFR, FTK DD, Win Image from Linux DD, and VMware snap shots. It helps both logical and physical image formats.

### *S. PLAINSIGHT*

PlainSight [25] is another useful virtual forensics device. It is a CD primarily based Knoppix that is a Linux distribution. Some of its uses encompass 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. For the usage of this tool, insert the CD and follow the instructions.

### *T. XRY*

XRY [26] is the mobile forensics tool advanced by using Micro Systemation. Its miles used to analyse and get better crucial statistics from cellular devices. This device comes with a hardware tool and software. Hardware connects cellular phones to pc and software program performs the evaluation of the tool and extract statistics. Its miles designed to get better statistics for forensic evaluation. The ultra-modern model of the tool can recover facts from all kind of smart phones along with Android, iPhone and BlackBerry. It gathers deleted facts like call statistics, pictures, SMS and textual content messages.

### *U. HELIX3*

HELIX3 [27] is a live CD-based totally virtual forensic suite created for use in incident reaction. It comes with many open source virtual forensics tools which include hex editors, information carving and password cracking equipment. Free model in it is Helix3 2009R1. After this release, this project was overtaken by a commercial vendor. This device can acquire statistics from physical memory, network configuration, consumer debts, executing methods and services, scheduled jobs, home windows Registry, chat logs, display screen captures, SAM documents, programs, drivers, environment variables and internet records. Then it analyses and critiques the records to generate the complied results based totally on reports.

### *V. CELLEBRITE UFED*

Cellebrite's UFED [28] solution presents a unified workflow to allow examiners, investigators and first responders to acquire, defend and act decisively on mobile statistics with the speed and accuracy a scenario needs – without ever compromising one for the other. The UFED pro series is designed for forensic examiners and investigators who require the maximum comprehensive, up to date cell information extraction and deciphering help available to deal with the influx of recent records resources. Platform agnostic, the UFED field is designed to unify workflows between the field and lab, making it viable to view, gets right access and share mobile data via in-car workstations, laptops, tablets or a secure, self-service kiosk located at a station.

## V. FREE COMPUTER FORENSIC TOOLS

Some of the existing free computer forensic tools [29] are explained in Table I.

## VI. CONCLUSION

The field of digital forensics has become popular over the last few years as both the computer and the cellular market has expanded. With the increasing use of digital data and mobile phones, cyber forensics has become more prominent, even Cyber thefts are also increasing as day advances. This paper helps to show few existing & popular digital forensics tools [30] used by various law enforcement agencies in performing crime investigations. This field will enable crucial electronic evidence to be found, whether it was lost, deleted, damaged, or hidden, and used to prosecute individuals that believe they have successfully beaten the system.

## ACKNOWLEDGMENT

I am very much thankful to Ms. Prathyusha Kanakam, Asst. Prof., CSE & Mr. S. Mahaboob Hussain, Asst. Prof., CSE & Research Coordinator, Vishnu Institute of Technology for their guidance throughout this paper.

**TABLE I**
**COMPUTER FORENSIC TOOLS**

| Application of Forensic Issues | Tools used |
|---|---|
| Disk tools and data capture | Arsenal Image Mounter; DumpIt; EnCase Forensic Imager; Encryted Disk Dectector; EWF MetaEditor; FAT32 Format; Forensics Acquisition of Websites; FTK Imager; Guymager; Live RAM Capturer; NetworkMiner; Nmap; Magnet RAM Capture; OSFClone; OSFMount; Wireshark; Disk2vhd |
| Email Analysis | EDB Viewer; Mail Viewer; MBOX Viewer; OST Viewer; PST Viewer |
| General Tools | Agent Ransack; Computer Forensic Reference Data Sets; EvidenceMover FastCopy; File Signatures; HexBrowser; HashMyFiles; MobaLiveCD; Mouse Jiggler; Notepad ++; NSRL; Quick Hash; USB Write Blocker Volix;Windows Forensic Environment |
| File and Data Analysis | Advanced Prefetch Analyser; analyzeMFT; bstrings; CapAnalysis; Crowd Reponse; Crowd Inspect; DCode; Defraser; eCryptfs Parser; Encryption Analyzer; ExifTool; File Identifier; Forensic Image Viewer; Ghiro; Highlighter; Link Parser; LiveContactsView; PECmd; PlatformAuditProbe; RSA Netw itness Investigator; Memoryze; MetaExtractor; MFTview; PictureBox; PsTools; Shadow Explorer; SQLite Manager; Strings; Structured Storage Viewer; Switch-a-Roo; Windows File Analyzer; Xplico |
| Mac OS tools | Audit; ChainBreaker; Disk Arbitrator; Epoch Converter; FTK Imager CLI for Mac OS; IORegInfo; PMAP Info; Volafox |
| Mobile devices | iPBA2; iPhone Analyzer; ivMeta; Last SIM Details; Rubus; SAFT |
| Data Analysis Suites | Autopsy; Backtrack ; Caine ; Deft; Digital Forensics Framework; Forensic Scanner; Paladin ; SIFT; The Sleuth Kit; Volatility Framework |
| File Viewers | BKF Viewer; DXL Viewer; E01 Viewer; MDF Viewer; MSG Viewer; OLM Viewer; Microsoft PowerPoint 2007 Viewer; Microsoft Visio 2010 Viewer; VLC |
| Internet Analysis | Browser History Capturer; Browser History Viewer; Chrome Session Parser; ChromeCacheView; Cookie Cutter; Dumpzilla; Facebook Profile Saver; IECookiesView; IEPassView; MozillaCacheView; MozillaCookieView; MozillaHistoryView; MyLastSearch; PasswordFox OperaCacheView; OperaPassView; Web Historian; Web Page Saver |
| Registry analysis | AppCompatCache Parser; ForensicUserInfo; Process Monitor; RECmd Registry Decoder; Registry Explorer; RegRipper; Regshot; ShellBags ; Explorer; USB Device Forensics; USB Historian; USBDeview; User Assist Analysis; UserAssist; Windows Registry Recovery |
| Application Analysis | Dropbox Decryptor ; Google Maps Tile Investigator; KaZAlyser; LiveContactsView; SkypeLogView |

## REFERENCES


[1] M. Pollitt, “A History of Digital Forensics,” in *Advances in Digital* Forensics *VI*, vol. 337, K.-P. Chow and S. Shenoi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 3–15.

[2] Nilakshi Jain1 , Dr. Dhananjay R Kalbande2,”A Comparative Study based Digital Forensic Tool: Complete Automated Tool” The International Journal of Forensic Computer Science,2014 DOI: 10.5769/J201401003

[3] Hussain, S. Mahaboob, A. S. N. Chakravarthy, and G. S. Sarma. "BSC: A Novel Scheme for Providing Security using Biometric Smart Card." *International Journal of Computer Applications* 80.1 (2013).

[4] B.V.Prasanthi, U.Padma Jyothi, B.Sridevi , T.Vamsi Krishna,“ Security Enhancement of ATM System with Fingerprint and DNA Data” International Journal of Advanced Research in Computer Science and Software Engineering( 2014)

[5] Kanakam, Prathyusha, S. Mahaboob Hussain, and A. S. N. Chakravarthy. "Electronic noses: Forestalling fire disasters: A technique to prevent false fire alarms and fatal casualties." 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). IEEE, 2015.

[6] Prasanthi, B. V., et al. "Palm Vein Biometric Technology: An Approach to Upgrade Security in ATM Transactions." *International Journal of Computer Applications* 112.9 (2015).

[7] F. N. Dezfoli, A. Dehghantanha, R. Mahmoud, N. F. B. M. Sani, and F. Daryabar, “Digital Forensic Trends & Future,” *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 2, no. 2, pp. 48–76, 2013.

[8] Schatz, Bradley, and Andrew J. Clark. "An open architecture for digital evidence integration." (2006): 15-29.

[9] Computer Aided Investigative Environment http://www.caine-live.net/

[10] X-Ways Forensics, Available http://www.x-ways.net/, accessed August 2007.

[11] SANS Investigative Forensics Toolkit – SIFT Available:http://digitalforensics.sans.org/community/downloads

[12] Guidance Software. EnCase Legal Journal, Second Edition. March 2002. Available at: http://www.encase.com/support/downloads/LegalJournal.pdf

[13] Registry Recon http://arsenalrecon.com/apps/recon/

[14] TSK tools, Brian Carrier site, http://www.sleuthkit.org/sleuthkit/, 14/1/2009
[15] Libforensics http://code.google.com/p/libforensics/
[16] Volatility http://code.google.com/p/volatility/
[17] WindowsSCOPE http://www.windowsscope.com/index.php?page=shop.product_details&flypage=flypage.tpl&product_id=35&category_id=3&option=com_virtuemart
[18] TheCoroner'sToolkit http://www.porcupine.org/forensics/tct.html
[19] Oxygen Forensic Suite http://www.oxygen-forensic.com/en/features
[20] BulkExtractor http://digitalcorpora.org/downloads/bulk_extractor/
[21] Xplico Available http://www.xplico.org/about
[22] MandiantRedLine Available https://www.mandiant.com/resources/download/redline
[23] Computer Online Forensic Evidence Extractor Available: https://cofee.nw3c.org/
[24] P2 eXplorer https://www.paraben.com/p2-explorer.html
[25] PlainSight http://www.plainsight.info/index.html
[26] XRY http://www.msab.com/xry/what-is-xry
[27] HELIX3 https://efenseinc.sharefile.com/d/sda4309a624d48b88
[28] Cellebrite UFED http://www.cellebrite.com/Mobile-Forensics
[29] Free computer forensic tools Available http://resources.infosecinstitute.com/computer-forensics-tools/
[30] Roman, Rodrigo Fernando Morocho, et al. "Digital Forensics Tools." International Journal of Applied Engineering Research 11.19 (2016): 9754-9762