Cyber Forensic Science to Diagnose Digital Crimes- A study

B. V. Prasanthi[#1], Prathyusha Kanakam[*2], S Mahaboob Hussain[#3]

[#]*Assistant Professor, Dept. of CSE, Vishnu Institute of Technology*
Bhimavaram, Andhra Pradesh, India
[*]*Assistant Professor, Dept. of CSE, MVGR College of Engineering*
Vizianagaram, Andhra Pradesh, India

Abstract — *Crimes in this digital world are of different types and the one among is Cyber-crime. As everything is digitized, there is rapid increase in use of internet and at the same time more number of cyber-crimes happens that raised by the attackers. Some of the cyber-attacks are hacking, banking frauds, and email spamming etc. In order to investigate these fraudulent activities, the investigation agencies (enforcement law) should make use of technology which is a crucial part. Digital forensic investigation is a branch of cyber forensics in which scientific methods and tools are used ,that allows the prevention and analysis of digital evidence, that to be produced in a court of law. This paper explores the detailed explanation of existing digital forensics tools and its uses which assists to probe the evidence.*

Keywords— *Digital Forensics, Crimes, Cyber-Attacks, Cyber-Forensics, Forensic Science, Security, Forensic Tools.*

I. Introduction

As Internet is growing day-by-day which dealt with explosion of technology requires vast storage of data and information. Every individual possess their devices such as their smartphones, computers are fell under attacks by fraudulent persons that leads to the increase of cyber-crimes dramatically. Digital forensics and Cyber Forensics are the vast areas to investigate such crimes that include hacking, banking frauds, and email spamming etc.

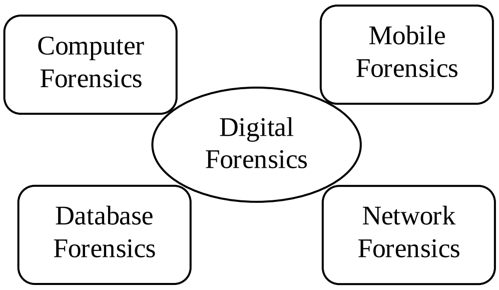

Fig 1: Representation of various categories of forensics study from digital forensics

Digital forensics is the science that encompasses all the investigations and research used in solving these types of computer crimes [1]. Digital forensics and Cyber Forensics are semantically related to each other. It deals with investigation over devices capable of storing digital data. Digital forensics challenges for direct evidence of crimes and it is annotated as branch of forensic sciences as in Fig. 1. For instance, document authentication processes credits nominal suspects for confirmation. While analysing with various types of forensics, digital forensics extremely focuses on investigating specific procedures. The main difference in the case of digital forensics is that an entire causal chain has to be proven to be either right or wrong before going to court, in opposition with other specific forensics where providing answers to unrelated questions based on simple research is enough.

II. Exploring the Tools of Digital Forensics

Digital forensics is a vast area of forensic science that includes the investigation of cyber attacked data which is stored electronically [2]. It furcates forensic science into different types of specializations in which each one looks over certain functionalities as in Fig. 2. There exist various tools for specific domain that makes the process of investigation easy.

A. Database Forensics

Database forensics is a branch of digital forensic sciences that incorporates the process of scrutinize the critical and sensitive information related to data (metadata) stored in various places like Files, Disk drives, etc. Database Forensics aims at reverting of unauthorized access to manipulate information and also observes the abnormal behaviour of the data [3].

*1) **Disk tools and data capture.*** Data capturing involves the process of retrieving a document from various storage devices. For instance, barcode scanners at supermarkets and hospitals are some of the data capture tools. Disk is the peripheral device that stores the information and applies methods to retrieve data from them.

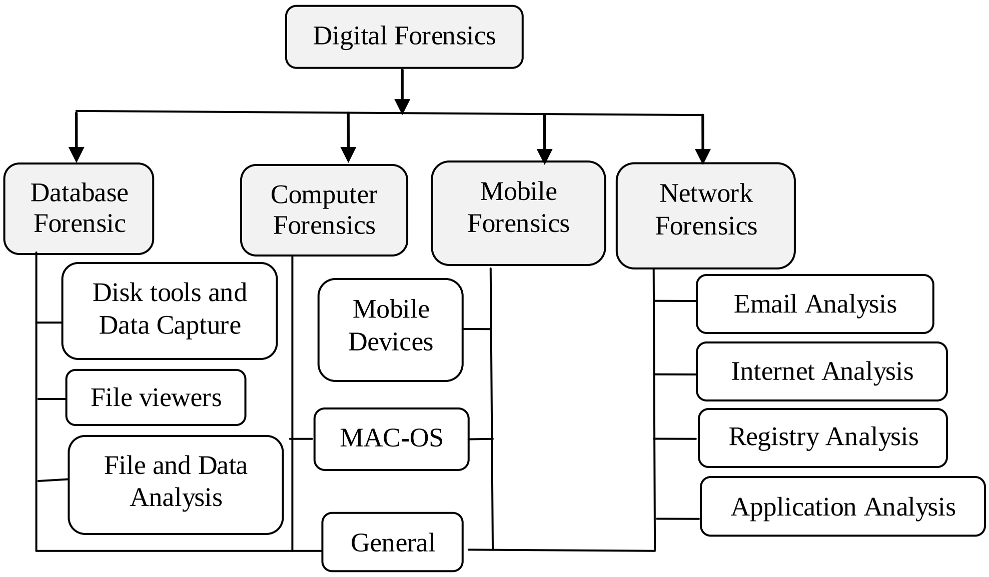

Fig 2: Representation of various branches and their tools for digital forensics

These disk drives include hard disks, floppy disks and optical discs. Most of the attacks happen on Hard Disk Drive (HDD) which is a disk-based storage device that stores the core thing of the computer system- operating system, installed software and files [4]. The following is tabular list of various forensic tools to explore the para-activity of data as shown in Table 1.

TABLE I
FORENSIC TOOLS OF PARA-ACTIVITY ON DATA

Tool	Description
Autopsy	It is Graphical interface used to the command line digital investigation analysis tools in The Sleuth Kit
Backtrack	It is a Penetration testing and security audit with forensic boot capability.
Caine	It is Linux based live CD, featuring a number of analysis tools.
Deft	It is known as Linux based ,purpose of running on live without tampering and corrupting devices
Digital Forensics Framework	It used for analysing volumes, file systems, user and applications data, extracting metadata, deleted and hidden items.
Forensic Scanner	It is used for Automating 'repetitive tasks of data collection'.
Paladin	It is Ubuntu based live boot CD for imaging and analysis.
SIFT	It is VMware Appliance pre-configured with multiple tools allowing digital forensic examinations.
The Sleuth Kit	It is collection of UNIX-based command line file and volume system forensic analysis tools.
Volatility Framework	It is collection of tools for the extraction of artefacts from RAM.

*2) **File Viewers:*** File viewer is application software that can be used to view the information stored in a computer file. The file contents are generally deleted files, memory sections, and raw sectors [5]. Investigative tools applied to observe these contents and to analyse the streaming data. Each and every tool has a specific functionality to investigate on various areas and the tools are described in Table 2.

TABLE II
TOOLS FOR FILE VIEWERS

Tool	Description
BKF Viewer	It is used for viewing (not save or export from) contents of BKF backup files.
DXL Viewer	It is used for viewing (not save or export) Loutus Notes DXL file emails and attachments.
E01 Viewer	It is used for viewing (not save or export from) E01 files & view messages within EDB, PST & OST files
MDF Viewer	It is used for viewing (not save or export) MS SQL MDF files
MSG Viewer	It is used for viewing (not save or export) MSG file emails and attachments
OLM Viewer	It is used for viewing (not save or export) OutLook for Mac(OLM) file emails and attachments
Microsoft PowerPoint 2007 Viewer	It is used for viewing PowerPoint presentations
Microsoft Visio 2010 Viewer	It is used for viewing Visio diagrams
VLC	It is used for viewing most multimedia files and DVD, Audio CD, VCD, etc.

*3) **File and data analysis:*** Data analytic process is a key to analyse the invisible information stored in a file and unlock it. Forensic science for data analytics is used to prevent and detect fraud, waste and abuse by leveraging information that is incorporated in various data assets. It empowers identification of meaningful patterns and relationships in existing historic information to predict future activities and evaluate the reasons for various frauds [6]. Such sensitive information is mostly not visible but used to predict future so that top level of the business organisations can make a decision related to fraud, disputes and misconduct. The following Table 3 indicates some of the data analysis forensic tools.

TABLE III

TOOLS FOR FILE AND DATA ANALYSIS

Tool	Description
Advanced Prefetch Analyser	It is used to speedup application startup process & it reads Windows XP,Vista and Windows 7 to prefetch files
analyzeMFT	It is a python tool used to parse the Master File Table(MFT) from an New Techology File System(NTFS) allowing results to be analysed with other tools.
Bstrings	It find strings in binary data, including searching of regular expression .
CapAnalysis	It is a web visual tool used for deep inspection of packets.It is used as pacjetCapturing(PCAP) viewer.
Crowd Reponse	It is Windows console application to aid gathering of system information for incident response and security engagements.
Crowd Inspect	It gives the details of network processes, listing binaries associated with each process. Queries VirusTotal, other malware repositories & reputation services to produce “at-a-glance” state of the system.
DCode	It converts various data types to date/time values.
Defraser	It detects full and partial multimedia files in unallocated space.
eCryptfs Parser	It recursively parses headers of every eCryptfs file in selected directory. Outputs encryption algorithm used, original file size, signature used, etc in eCryptfs Parser.
Encryption Analyzer	It scans a computer for password-protected & encrypted files, reports encryption complexity and decryption options for each file.
ExifTool	It is used to read, write and edit Exif data in a large number of file types.
File Identifier	It is used to drag and drop web-browser JavaScript tool for identification of over 2000 file types.
Forensic Image Viewer	It is used to view various picture formats, image enhancer, extraction of embedded Exif, GPS data.
Ghiro	Ghiro is used to examine in-depth analysis of image (picture) files.
Highlighter	It examines log files using text, graphic or histogram views.
Link Parser	It recursively parses folders extracting 30+ attributes from Windows .lnk (shortcut) files.
LiveContactsView	It views and export Windows Live Messenger contact details.
PECmd	It is used as Prefetch Explorer or tool.
PlatformAuditProbe	It is command Line Windows forensic/ incident response tool that collects many artefacts.
RSA Netwitness Investigator	Is is used as network packet capture and analysis.
Memoryze	It acquires and/or analyse RAM images, including the page file on live systems.
MetaExtractor	It recursively parses folders to extract meta data from MS Office, OpenOffice and PDF files.
MFTview	It displays and decodes contents of an extracted MFT file.
PictureBox	It lists EXIF, and where available, GPS data for all photographs present in a directory. Export data to .xls or Google Earth KML format.
PsTools	It is suite of command-line Windows utilities.
Shadow Explorer	It is used to browse and extract files from shadow copies.
SQLite Manager	It is a firefox add-on enabling viewing of any SQLite database.
Strings	It is a command-line tool for searching text .
Structured Storage Viewer	It is used to view and manage MS OLE Structured Storage based files.
Switch-a-Roo	It is a text replacement/converter/decoder for when dealing with URL encoding
Windows File Analyzer	It analyses thumbs.db, Prefetch, INFO2 and .lnk files.
Xplico	It is a Network forensics analysis tool.

B. Computer Forensics:

Computer forensics is a very crucial category of forensic science that deals with computer and Internet related crimes. Earlier, computers were only used to produce data but now it has expanded to all devices related to digital data. The goal of Computer forensics is to perform crime investigations by using evidence from digital data to find the root cause for that particular crime with various tools [7].

It includes forensic tools associated with digital data analysis, MAC –OS analysis and Mobile device tools. General forensic tools and data analytic tools are listed in appendix as they are common to every stream of forensic science.

*1) **MAC-OS:*** MAC is one of the operating system that constitutes information repository to analyse. This information is sensitive to fraudulent activities. MAC data analysis tools for forensics are listed in Table 4.

TABLE IV
OPERATING SYSTEM BASED TOOLS

Tool	Description
Audit	It audits Preference Pane and Log Reader for OS X
ChainBreaker	It parses keychain structure, extracting user's confidential information such as application account/password, encrypted volume password (e.g. filevault),
IDisk Arbitrator	It blocks the mounting of file systems, complimenting a write blocker in disabling disk arbitration.
Epoch Converter	It is used to converts epoch times to local time and UTC.
FTK Imager CLI for Mac OS	It is termed as Command line Mac OS version of AccessData's FTK Imager
IORegInfo	It contains list of items connected to the computer (e.g., SATA, USB and FireWire Drives, software RAID sets). It is also used to locate partition information, including sizes, types, and the bus to which the device is connected.
PMAP Info	It displays the physical partitioning of the specified device and to map out all the drive information, accounting for all used sectors also display the memory usage of processors.
Volafox	It is known as Memory forensic toolkit used for Mac OS X

C. Mobile Forensics:

The forensic science is a vast area that constitutes various sub-divisions among them mobile forensics is another stream to investigate for evidence sourced from mobile devices and various gadgets [8].

*2) **Mobile devices:*** Mobile devices refer to any device that stores digital data and have internal memory and communication ability such as PDA devices, GPS services and tablet computers. Each mobile device used to store several types of personal information like contacts, photos, calendars and notes, SMS and MMS messages. Smartphones may additionally contain video, email, web browsing information, location information, and social networking messages and contacts. As the usage with these devices increased, there is growing the need for mobile forensics to tackles transmitting of personal information, online transactions and many more. The forensic tools related to mobile devices are listed below in Table 5.

TABLE V
TOOLS FOR MOBILE DEVICES

Tool	Description
iPBA2	It is used to explore iOS backups.
iPhone Analyzer	It is used to explore the internal file structure of Pad, iPod and iPhones.
ivMeta	It extracts phone model and software version and created date and GPS data from iPhone videos.
Last SIM Details	It parses physical flash dumps and Nokia PM records to find details of previously inserted SIM cards.
Rubus	It deconstructs Blackberry .ipd backup files.
SAFT	SAFT used to perform logical forensics analysis for android devices. It obtains SMS Messages, call logs and contacts from Android devices.

D. Network Forensics:

It is an offshoot of digital forensic science that deals mostly with the analysis of information during the communication in networks. It monitors the flow of data from an authenticated source to destination for information gathering, intrusion detection and legal evidence. It deals with extremely unpredictable and dynamic information. Network investigations focus on supervising network to identify intrusions and anomalous traffic.

*1) **Email analysis:*** Electronic messages are the best application of internet for communication of data. The analysis of this information during the communication is necessary to predict the intruders. Spam, phishing, cyber bullying, racial abuse, disclosure of confidential information, child pornography and sexual harassment are some of the examples for illegitimate uses of email. The following Table 6 presents various forensic tools to monitor the communication over networks by analysing these electronic messages.

TABLE VI
E-MAIL ANALYSING TOOLS

Tool	Description
EDB Viewer	Open and view (not export) Outlook Exchange Server Database(EDB) files .
Mail Viewer	It is Viewer for Outlook Express, Windows Mail/Windows Live Mail, Mozilla Thunderbird message databases and single Electronic mail(EML) files.
MBOX Viewer	It is used to view MBOX emails and attachments
OST Viewer	It opens and view (not export) Outlook Offline Storage table(OST) files without connecting to an Exchange server
PST Viewer	Open and view (not export) Outlook PST files without needing Outlook.PST is also reffered as PFF(Personal Folder File).

*2) **Internet Analysis:*** Internet analysis incorporates the procedure of monitoring and identifying user's online activities for gathering evidence [9]. The tools in the Table 7 give the fingerprints left over in hard disk drive during their wide usage of internet. These fingerprints include log files, history files, cached data and as well as information stored in volatile memory (RAM).

TABLE VII
TOOLS FOR INTERNET ANALYSIS

Tool	Description
Browser History Capturer	It Captures history from Firefox, Chrome, Internet Explorer and Edge web browsers running on Windows computers
Browser History Viewer	It is used to view and analyse internet history from Firefox, Chrome, Internet Explorer and Edge web browsers.
Chrome Session Parser	It is Python module for performing off-line parsing of Chrome session files ("Current Session", "Last Session", "Current Tabs", "Last Tabs")
ChromeCacheView	It is used to reads the cache folder of Google Chrome Web browser, and displays the list of all files currently stored in the cache.
Cookie Cutter	It extracts embedded data held within Google Analytics cookies. It also shows search terms used as well as dates of and the number of visits.
Dumpzilla	It runs in Python 3.x, extracting forensic information from Firefox, Iceweasel and Seamonkey browsers.
Facebook Profile Saver	It captures information publicly available in Facebook profiles.
IECookiesView	It extracts various details of Internet Explorer cookies.
IEPassView	It extracts stored passwords from Internet Explorer versions 4 to 8.
MozillaCacheView	It reads the cache folder of Firefox/Mozilla/Netscape Web browsers.
MozillaCookieView	It parses the cookie folder of Firefox/Mozilla/Netscape Web browsers.
MozillaHistoryView	It reads the history.dat of Firefox/Mozilla/Netscape Web browsers, and displays the list of all visited Web page.
MyLastSearch	It extracts search queries made with popular search engines (Google, Yahoo and MSN) and social networking sites (Twitter, Facebook, MySpace).
PasswordFox	It extracts the user names and passwords stored by Mozilla Firefox Web browser
OperaCacheView	It reads the cache folder of Opera Web browser, and displays the list of all files currently stored in the cache.
OperaPassView	It decrypts the content of the Opera Web browser password file, wand.dat.
Web Historian	It reviews list of URLs stored in the history files of the most commonly used browsers.
Web Page Saver	It contains the list of URLs saving scrolling captures of each page. Produces HTML report file containing the saved pages.

*3) **Registry analysis:*** Registry is a central repository for configuration data that is stored in a hierarchical manner. It is used to store and access this configuration information also replaces text based configuration files related to system users, application and hardware in the operating system [10]. Most of the sensitive data in the registry may be information on user accounts, typed URLs, network shared, and Run command history. To protect this data against fraudulent activities, different tools applied tabulated in Table 8.

TABLE VIII
REGISTRY ANALYSING TOOLS

Tool	Description
AppCompat Cache Parser	It dumps list of entries showing which executables were run and their modification dates.
ForensicUse	It extracts user information from

rInfo	the SAM, Software and System hives files and decrypts the LM/NT hashes from the SAM file.
Process Monitor	It examines Windows processes and registry threads in real time.
RECmd	It is a command line access to offline Registry hives. It supports simple & regular expression searches as well as searching by last write timestamp.
Registry Decoder	It is used for the acquisition, analysis, and reporting of registry contents.
Registry Explorer	It is an Offline Registry viewer. It Provides deleted artefact recovery, value slack support, and robust searching.
RegRipper	It is Registry data extraction and correlation tool.
Regshot	It takes snapshots of the registry allowing comparisons e.g., show registry changes after installing software
ShellBags Explorer	It presents visual representation of what a user's directory structure looked like. Additionally exposes various timestamps (e.g., first explored, last explored for a given folder.
USB Device Forensics	It gives the details of previously attached USB devices on exported registry hives.
USB Historian	It displays 20+ attributes relating to USB device use on Windows systems.
USBDeview	It gives the details of previously attached USB devices.
User Assist Analysis	It extracts SID, User Names, Indexes, Application Names, Run Counts, Session, and Last Run Time Attributes from UserAssist keys.
UserAssist	It displays list of programs run, with run count and last run date and time
Windows Registry Recovery	It extracts configuration settings and other information from the Registry.

4) ***Application Analysis:*** When security arises in the top level hierarchy, application's (either software or product) security plays a crucial part in most of the entrepreneurs. Application analysis concerned with identifying vulnerability in software before it is deployed or purchased, Web application testing tools help ward off threats and the negative impact they can have on competitiveness and profits [11]. Some of the application tools for scrutinizing software used in most of the enterprises [12]-[14]. some applications are listed in Table 9.

TABLE IX
TOOLS FOR APPLICATION ANALYSIS

Tool	Description
Dropbox Decryptor	It decrypts the Dropbox filecache.dbx file which stores information about files that have been synced to the cloud using Dropbox
Google Maps Tile Investigator	It takes x,y,z coordinates found in a tile filename and downloads surrounding tiles providing more context.
KaZAlyser	It extracts various data from the KaZA application
LiveContactsView	It is used to View and export Windows Live Messenger contact details
SkypeLogView	It is used to view Skype calls and chats

5) ***General Tools:*** Despite of categories of forensics, generalised tools used for all domains in forensic sciences are presented in Table 10.

TABLE X
GENERAL TOOLS

Tool	Description
Agent Ransack	Itis used for searching multiple files using Boolean operators and Perl Regex.
Computer Forensic Reference Data Sets	It contains collated forensic images used for training, practice and validation purpose.
EvidenceMover	It copies data between locations, with comparison of files, verification, logging details.
FastCopy	It is Self labelled 'fastest' copy/delete Windows software. It can verify with SHA-1, etc.
File Signatures	It contains list of file signatures.
HexBrowser	It identifies over 1000 file types by examining their signatures.
HashMyFiles	It calculate MD5 and SHA1 hashes on files and reduces larger input to smaller static output .
MobaLiveCD	It runs Linux live CDs from their ISO image without having to boot to them.
Mouse Jiggler	It automatically moves mouse pointer by stopping

	screen saver, hibernation etc.
Notepad ++	It is an advanced Notepad replacement.
National Software Reference Library(NSRL)	It contains hash sets of 'known' (ignorable) files
Quick Hash	It is a method used in Linux & Windows GUI for individual and recursive SHA1 hashing of files
USB Write Blocker	It enables for software write-blocking of USB ports.
Volix	It is an application that simplifies the use of the Volatility Framework
Windows Forensic Environment	It is a guide developed by Brett Shavers to creating and working with a Windows boot CD

III. Conclusion

In this digital era as the internet which is coined as network of networks is increasing day by day and all the communications related to information are become sensitive to various crimes that related to this digital world. In order to investigate these type of fraudulent activities, this paper presents various forensic tools belongs to specific domain. In this paper authors explored the various tools that focuses mostly on existing forensics tools which assist to increase the rate of protection and detection of attacks. These tools have its own features to extract evidence from digital data stored in a computer system.

References

[1] Richard III GG, Roussev V. Next-generation digital forensics. Communications of the ACM. 2006 Feb 1;49(2):76-80.

[2] Rogers MK, Seigfried K. The future of computer forensics: a needs analysis survey. Computers & Security. 2004 Feb 29;23(1):12-6.

[3] Khanuja HK, Adane DS. A framework for database forensic analysis. Computer Science & Engineering. 2012 Jun 1;2(3):27.

[4] Carrier B. Defining digital forensic examination and analysis tools using abstraction layers. International Journal of digital evidence. 2003 Jan;1(4):1-2.

[5] Kent, Karen, et al. "Guide to integrating forensic techniques into incident response." NIST Special Publication 10 (2006): 800-86.

[6] Breeuwsma, Marcel, et al. "Forensic data recovery from flash memory." Small Scale Digital Device Forensics Journal 1.1 (2007): 1-17.

[7] Prasanthi, B. V. "Cyber Forensic Tools: A Review." International Journal of Engineering Trends and Technology (IJETT) 41.Number-5 (2016): 6..

[8] Lessard, Jeff, and Gary Kessler. "Android Forensics: Simplifying Cell Phone Examinations." (2010).

[9] Sekar, Vyas, et al. "Toward a framework for internet forensic analysis." ACM HotNets-III. 2004.

[10] Dolan-Gavitt, Brendan. "Forensic analysis of the Windows registry in memory." digital investigation 5 (2008): S26-S32.

[11] Gunestas, Murat, Duminda Wijesekera, and Anoop Singhal. "Forensic web services." IFIP International Conference on Digital Forensics. Springer US, 2008: 163-176.

[12] S Mahaboob Hussain, Prathyusha Kanakam, A.S.N. Chakravarthy, "Inhibiting Cognitive Bias in Forensic Investigation Using DNA Smart Card with IOT", International Journal of Control Theory and Applications 10 (14), 251-255, 2017.

[13] 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).

[14] Prasanthi, B. V., et al. "Security Enhancement of ATM System with Fingerprint and DNA Data." International Journal of Advanced Research in Computer Science and Software Engineering (2014).