IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Cyber Forensics Paradigm for security forces and LEA (India)

Sanjay Kumar Choudhary[1], Dr. Nitin Kumar[2]

[1]M.Tech Student, Department of Cyber Forensic and information Technology ,
[2]HoD, Department of Cyber Forensic and information Technology

Abstract - *The advent and necessity of Mobile and internet services have made people dependent on it for their daily activities. Simultaneously it has lured many cyber criminals and made the highly committed life of security forces more challenging. Cyber forensic demands basic behaviour leadership skill like perseverance, innovative thinking etc . Along with basic skill it requires multi Domain high technical skill to understand the way a cybercriminal can think. However the situation become very complicated in India as well as across globe due to lack of any fix standardization, policies ,protocols ,training labs and financial liabilities involved. This paper provide a centralised manual to understand the domain and challenges of cyber forensic ,establishment of low cost training labs for basic training and develop a basic framework for India (any country) to tame the future coming devil in the form of cyber criminals.*

Key Words: cyber Forensic process, Paradigm of cyber Forensic, Integrated web based Cyber forensic model, tools to collect Evidence,

1. INTRODUCTION

1.1 The world is evolving through a technological innovation in the field of Information technology and communication protocols since the starting of 1990s. Cyber and networked technological changes have greatly affected the functioning of every entities of our society. It includes human development, financial decisions and even the way sophisticated cybercrimes are happening. In highly dynamic technological revolution period the entities not adopting to these changes are meeting extinctions. The reasons behind this is that although these technological advancements have created faster and better digital communication yet they have also introduced new exploitable opportunities for those intent on engaging in criminal, espionage, terrorism or nefarious activities. These exploitations of rapidly evolving technologies, results into mental, physical and financial losses to naïve users. These exploitation and subsequent losses broadly come under the preview of cybercrime.

1.2 **Cybercrime Definition**:- In any statute, the Indian Legislature doesn't provide the exact definition of Cybercrime, in the Information Technology Act, 2000 or IT act 2008(Amended). However, in general the term cybercrime means any illegal activity which is carried over or with the help of internet or computers The U.S. Department of Justice (DOJ) broadly defines computer crime as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution."

1.3 **Categorization Of Cybercrime:-** Cybercrime is related to Cyberspace, which is a dynamically changing domain and hence the complication in detecting cybercrime further increase many folds due to innovation and involvement of niche technologies. The prevailing broad demarcation of Cybercrime can be discussed as Child Pornography, virus dissemination ,Dos/DDos, Phishing ,card/upi fraud ,salami attack ,data diddling, cyber squattingkey storke logging, dumpster diving etc. .

1.4**History :**-Incidentally the first cyber forensic expert was law enforcement officers in USA. In 1984 FBI Computer Analysis and Response Team (CART) started working on cyber forensics. In 1985 the Metropolitan Police of UK had set up a computer crime unit under John Austen termed as the Fraud Squad. A major progress was observed in 1990s when Investigators and technical support operatives within the UK law enforcement agencies, along with outside specialists, realised that cyber forensics required standard techniques, protocols and procedures. The term Computer Forensics was first used in the literature in 1992. Subsequently the formation of International organisation on Computer Evidence (IOCE) took place in 1995. There after a series of conferences, took place in UK and finally the modern British cyber forensic methodology was established. FBI in 2000 , setup the first Regional computer forensic laboratory in the USA. All this resulted into the publication of first book by the Scientific Working group on digital evidence (SWGDE), called "Best Practices for Computer Forensics" in the year 2002. In the year 2010, Simson Garfinkel incorporated digital evidences in the forensic investigation processes.

1.5 **CYBER FORENSIC IN INDIA** :- The slow progress in this field in India is due to role of three major elements.

(a) Legislative elements: Parliament to enact bills
(b) Executive elements: -Police /Military
(c) Judiciary elements: - Court to accept the evidence.

2. Prevailing system in India :- Ministry of Home affairs of GoI, has created a separate division called cyber and information security division(C&IS**)) .** Division deals with matters relating to Cyber Security, Cyber Crime, National Information Security Policy & Guidelines (NISPG) and implementation of NISPG, NATGRID etc . The workload has further divided in five Cyber and information security desk /center

(a) CIS-I Desk: Co-Ordination Wing
(b) CIS-II Desk: Cyber Crime Wing
(c) CIS-III Desk: Information Security
(d) CIS-IV Desk: Monitoring Unit
(e) I4C: Indian Cyber Crime Coordination Center

2.1 The other Ministries like Ministry of Electronics and information technologies (MeITY) and Ministry of Defence (MoD) are also progressing significantly in this domain. Resource Centre for Cyber Forensics (RCCF) is a pioneering institute, pursuing research activities in the area of Cyber Forensics The then Honourable union minister of India in August 2008 dedicated RCCF to the nation.

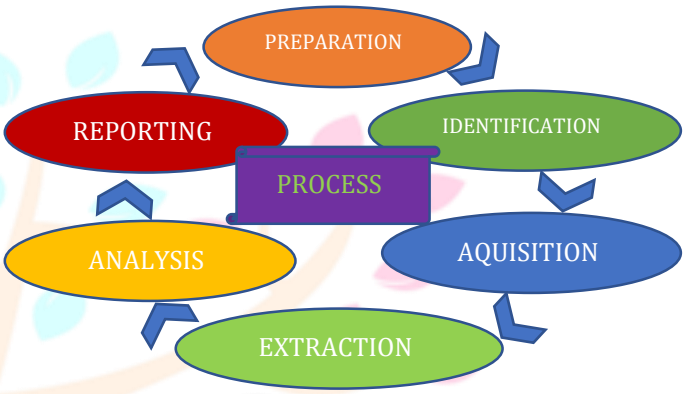
3. **Cyber forensic Paradigm: -** This paper brings out the challenges before security forces and suggest a paradigm to mitigate the challenges. It is imperative to bring out the domain to be covered to address the complete perspective holistically**.**

3.**1 Challenges: -** The security forces like Army, Police, Intelligence agencies are trained to handle subjects related to their respective fields. Since Cybercrime possess threat to the National Security and law and order of any country, Cyber forensic becomes an important role for these agencies**.** The major challenges before them are unavailability of cyber forensics labs, dynamically and swift change in domain with invent of technologies , lack of training infrastructure , lack of standard policies, Law of land for dealing with cyber evidences and Financial availability to meet the challenges of rapid changing fields in cyber forensic.

3.2 **Fields of Cyber forensics:-** Although fields covered in Cyber forensic is evolving and dynamic in nature, yet the important area as of now are as under.

- **Mobile forensics** covers the examination, analysis, and recovery of data from a mobile device like SIM contacts, call logs, SMS/MMS, audio/video, etc.
- **Network forensics** covers the monitoring and analysis of IP packet on network traffic to collect data and evidence.
- **Wireless forensics** deals in collecting and analyzing wireless network traffic data.
- **Database forensics** handles examining databases and their metadata and extracting data essential.
- **Email forensics** handles the recovery, analysis, and retrieval of emails, calendars, and contacts.
- **Cloud forensics covers** investigating cloud environments and extracting information.
- **Malware forensics** relates to examining and identifying malicious code to study the payload, viruses, worms, etc.
- **Disk Forensics deals in e**extracting the forensic information from the digital drive such as hard disk drive, USB devices, floppy, CD, DVD, and Flash drives
- **Memory forensics:** Retrieval and analysis of data stored on a computer's RAM.

3.3 Process of cyber forensic:- All fields of cyber forensic consist of following process



3.4 **Preparation**: - Firstly investigator is required to create case base directories and ensure that it is free from any malware/unwanted files .

3.5 **Identification**:-Important steps containing details about physical and software evidences in the form of questions like what type of evidence ,where it was found, and what format it has etc .

3.6 **Acquisition** :-Step involves making bit by bit copy of evidence. acquisition can be live or offline. Live bootable disk using DD command. (*syntax: dd if= of= filename.dd).* Offline acquisition using tools with inbuilt write blockers.

3.7 **Extraction** :-It is done either physically or logically .Physical extraction is raw method with no emphasis on file system. Logical extraction caters for active files, recovering deleted files, looking at the file slack /unallocated file space and decryption of files.

3.8 **Analysis** :-now interpretation and extraction of data to fix their significance to the case happens. Legal authority to search and collect evidence is verified here. ownership, data hiding and timeframe are some of the methods used here.

3.9 **Reporting** :-Investigator's notes ,findings and reports are documents that form part of reporting along with details of chain of custody. So that it becomes admissible before court of Law.

4. Model/Paradigm for forensic

It is impossible for the criminal to act, especially considering the intensity of a crime, without leaving traces of his presence
Locard

4.1 There are various model proposed by scientist and researcher from time to time some of imp model are as under.

- **Lee model**: - The forensic scientist Henry Lee formulated a Scientific Crime Scene Investigation model. Process in Lee's model are

Lee = {*Recognise* ⇒ *Identify* ⇒ *Individualise* ⇒ *Reconstruct*}

- **Kruse and Heiser Model** :-In 2001 K&H presented model which consists of three main processes within a framework

Kruse and Heiser ={*Acquire* ⇒ *Authenticate* ⇒ *Analyse*}

- **National Institute of Justice (NIJ)**of USA created a working group. The group presented two separate processes for cybercrime investigation.

Process-1

NIJ First Responder = {*Recognise* ⇒ *Document* ⇒ *Collect* ⇒ *Package*}

Process-2

NIJ Investigator = {*Collect* ⇒ *Examine* ⇒ *Analyse* ⇒ *Report*}

- Casey Model :- In 2001 ,Casey model involves the following listed processes:

Casey = {*Recognition* ⇒ *Preservation* ⇒ *Classification* ⇒ *Reconstruction*}

- **Carrier and Spafford Model**: - they proposed a model with five groupings and seventeen phases in total. the model has

Carrier and Spafford = {*Readiness* ⇒ *Deployment* ⇒ *Physical Investigation/ Digital Investigatio* ⇒ *Review*}

- **Cohen Model** :- Cohen consists of seven listed processes or phases

Cohen = {*Identification* ⇒ *Collection* ⇒ *Transportation* ⇒ *Storage* ⇒ *Examination and Traces* ⇒ *Presentation* ⇒ *Destruction*}

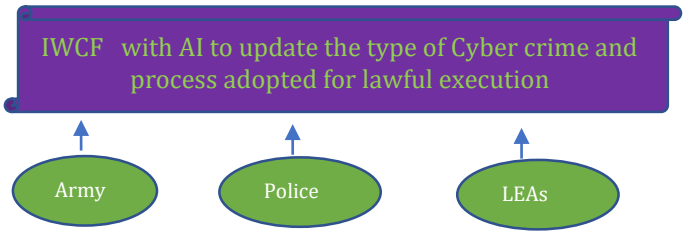
- **Ciardhu´ain** Model:- Ciardhu´ain is the most all-inclusive and comprehensive up to date model . The steps or phases are called activities.

Ciardhua´in = {*Awareness* ⇒ *Authorise* ⇒ *Plan* ⇒ *Notify* ⇒ *Search/Identify* ⇒ *Collect* ⇒ *Transport* ⇒ *Store* ⇒ *Examine*⇒ *Hypothesise* ⇒ *Present* ⇒ *Prove/Defend* ⇒ *Disseminate*

4.1 Paradigm **of cyber forensic in India** :- The proposed model is based on the factor of adaptability and practical experience of past from various models and evolving a paradigm for operation of Security forces and LEAs .

"Adaptability is not imitation. It means power of resistance and assimilation." – Mahatma Gandhi

4.2 **Proposal of IWCF**(Integrated web based Cyber forensic model) for Security forces and LEAs is a web based cyber forensic Platform . It integrates all type of security agencies operating in India through a date centre. The component of various security models like Bell lapadula, Clarke Wilson, Biba etc to meet the requirements and security concerns of all such agencies may be incorporated in this model . This paper presents a unified structure and working of separate modules addressing all fields mentioned in Para 3.2 of this paper.



Internal modules of IWCF

5. the modules should consist of all known fields of cyber forensics and should have adaptability to accommodate future ready features. The modules are covered individually in succeeding paragraph.

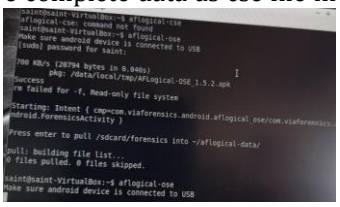
5.1 Mobile forensic Modules :- Mobile forensic have potential to produce credential evidences which could execute the cyber criminals before court of Law .The innovation plays an important role in cyber forensic so along with R&D by IWCF the existing tools of mobile forensic may be used . Some of the important tools are as under:

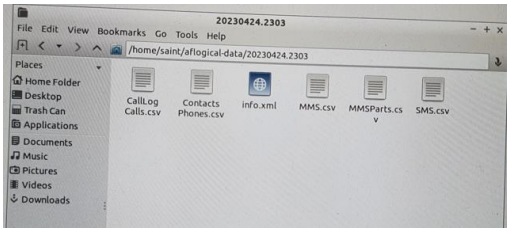
AFLogical,	LIME	MOBILedit
OSAF,	Oxygen	Cellebrite UFED
Andriller,	Cellebrite	Autopsy
FTK imager	Encase,	

5.2 Mobile forensic involves collection of information like text messages, iMessages, internet history and searches, photographs, application data, call logs, voice mails, GPS locations and encrypted data on phone.

5.3 Demo on Mobile Forensic:- The Mobile Forensic demonstration is carried out on Santuku Linux platform with AFLogical tool to extract information from a mobile .For demo purpose Android model created using android virtual device manager .

5.4 Now on terminal type command aflogical-ose. The tool will execute and come to the data extraction window. the data is extracted and ready to be captured . capture option ,extracts and store complete data as cse file in home directory .





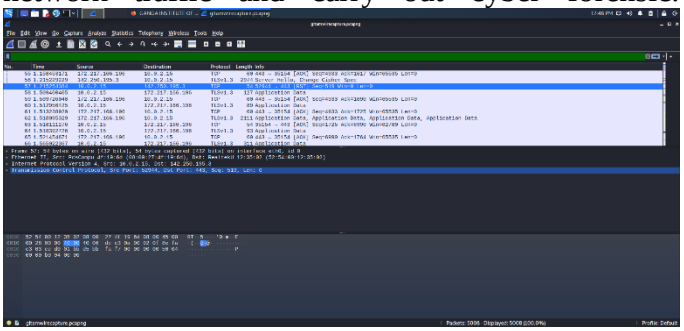
5.5 **Network forensic** :- Network forensic handles the information like data leakage, data theft or suspicious network traffic for production before authorities as an evidence. Here the information are most volatile and dynamic in nature .Thus most challenging field and require professional attitude. NW forensic involve two type of data. either it is done anonymously in real time or after happening of incident by analysing logs, login credentials and reassembling transferred files. Hence it involves three steps capturing, recording and analysis.

5.6 Tools used for network forensics: -Command and GUI based tools to carry out NW forensic are available as open source tools as well as commercial tools . Important tools are

Wireshark	TcpDump	NMAP
Network Miner	Snort	Splunk
Etherape	XPlico	Dshell
Netminer	Angry IPscanner	Kismat

5.7 Demo on NETWORK FORENSIC using wireshark

Wireshark in standard three-pane packet browser which performs deep inspection of the hundreds of protocols. It involves live analysis using sort and filter options .It is also useful in VoIP analysis and capture raw USB traffic. However it can only capture packet on the PCAP (an application programming interface used to capture the network) supported networks. It supports a variety of well-documented capture file formats for storing the captured data ,such as the PcapNg and Libpcap. The captured screen depicting series of events from DNS resolution to tcp handshake is placed below, when a request to https request to website (https://www.gangainstitute.com/) was made. Similarly other tools can be used to analyse the network traffic and carry out cyber forensic.



5.8 **Wireless forensic**:- the cumbersomeness of wired NW has resulted into genesis of WiFi NW. Wi-Fi networks rather than using UTP/OFC uses radio waves for its connection and communication. IEEE working group on WLAN has defined WiFi in 802.11. It is now a widely used protocol and hence become a potential target for many cyber criminals . Wireless forensic also covers the domain of RFID, Bluetooth and all variants of 802.11. The Forensic expert looks for data relating to radio frequency interface (DSSS,FHSS etc,), attributes of wifi services (Association, Re-association, Disassociation, Authentication, Privacy) ,raw data packet capture and radio signal strength.

5.9 Tools used for wireless forensic .It is pertinent to mention that these tools does not reveal the WiFi password just by running them by targeting it on a particular SSID. It is a series of analysis combined with connecting efforts which assist in obtaining the desired results. It is also important that wifi adaptor by default is in promiscuous mode. We are required to switch to Monitor mode to sniff all packets passing our WiFi adaptor. some important tools are as under.

PCAP or Packet Capture	WIFi Pineapple
Kismat	Aircrack-ng
Fl0p	Autopsy

5.6 Demo of wireless forensic :- Firstly check the wireless configuration of your system by command iwconfig and if required install aircrack-ng on your system. Now switch wireless adaptor to “Monitor mode” from “managed mode”.now type command

root@kali:-#airodump-ng wlan0mon(adaptor name).

On executing this command ,all wifi nw signals will be searched and listed with BSSID, Pwr, Encryption and ESSID details. Now we will target the machine or NW we are interested in by feeding specific details.

root@kali:-#airodump-ng -d 34:4e:88:03:n4:45(mac of source router) -c15(channel no) -w test wlan0mon

NOW KEEP LISTENING TILL user disconnect. We can also disconnect it by deauthorizing all connection on router but now from a pacific role we are active hence exposed .

root@kali:-#airplay -ng –deauth 0 -a BSSID (router) -c BSSID (connected user) wlan0mon

now during handshake hash value of password is captured and using brute force attack it could be broken.we have created a wordlist.txt file with set of password .Command

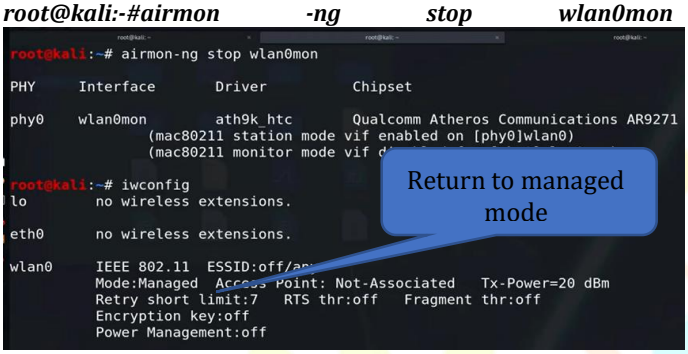
will initiate a brute force attack and finally password is

sanjay

broken as key found (sanjay) shown below.

Now it is important to reinstate the wifi adaptor to managed or promiscuous mode . The command is

root@kali:-#airmon -ng stop wlan0mon

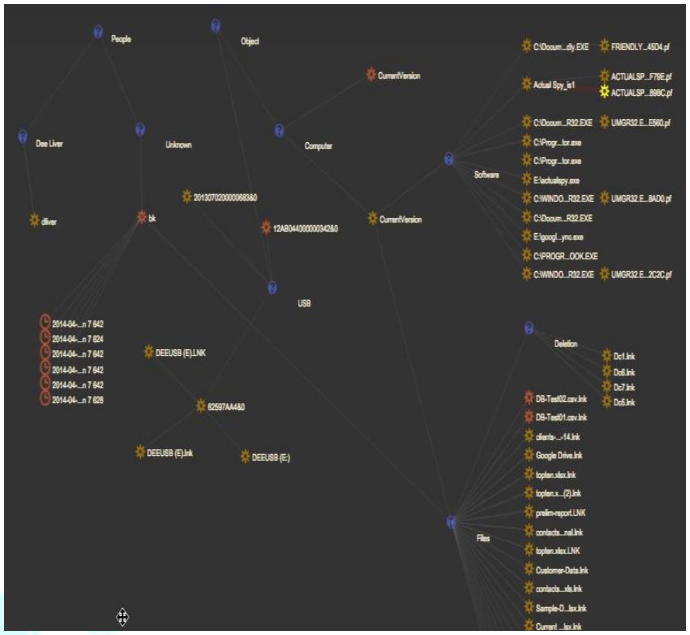


5.7 Database forensics :-A database is structured collection of data to be used in decision making and references in future event handlings. Databases forensic deals with database and their metadata which help to reconstruct the clues, detect crime, and accomplish case cracking .It also involves inspecting and validating the timestamps associated with the update time of a row in a relational table to validate a database user's actions. Some of the important database are MySQL, Oracle, PostgreSQL , Microsoft SQL Server, MongoDB etc.

5.8 Tools for database forensics :- The knowledge of database management is an important parameter for database forensic experts.Some of the major tools are

DB Browser for SQLite	**Database Forensic Analysis System**	**Forensic Toolkit for SQLite**
Log Analyzer for SQL	**SQLite Forensics Explorer**	**SQLite Viewer**
dbResponder	**Orientdb analyser**	

5.9 Demo:- The challenges in database forensic are database specific data models, no file header ,records reconstruction and values are encoded with metadata. The database challenge further enhances because there are no backups available or disk is corrupted or files are deleted. A sequence of events connecting people , places and artifacts using OrientDB analyser which helps in forensic analysis.



6.0 **Email forensic** :- emails are widely used by cybercriminals to carry out cyber attacks . The phishing attack and other forms of social engineering attacks are some technique used in email attacks. Analysis of emails and its content/attachments to determine the legitimacy, source, date, time, the actual sender, and recipients comes under the preview of Email forensics. The aim is to provide admissible digital evidence for use in court of law. Email forensics starts with the study of email **header** as it contains a vast amount of information about the email message.

Forensic of Email Header look like

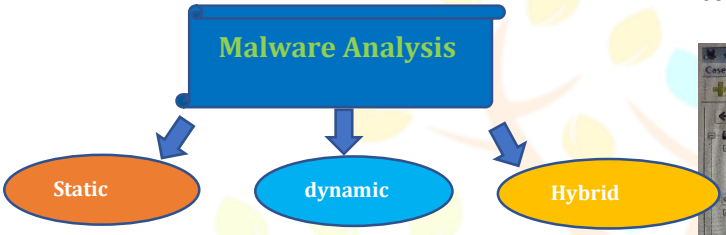
Delivered-To: HODCFIS@gitam.edu.in
Received: by 2023:a0c:f2c8:0:0:0:0:0 with SMTP id c8csp401046qvm;
Wed, 03 May2023 05:51:21 -0700 (PDT)
X-Received: by 2023:a92:5e1d:: with SMTP id s29mr19048560ilb.245.1596027080539;
Wed,03 May 2023 05:51:20 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1596027080; cv=none;
d=google.com; s=arc-20160816;
b=Um/is48jrrqKYQMfAnEgRNLvGaaxOHC9z9i/
ARC-Message-Signature: i=1; a=rsa-sha256; c
ARC-Authentication-Results: i=1

This field tells whether the received mail from the given domain has passed **DKIM** signatures and **Domain keys** signature or not, , "from" and "subject" fields,MIME header.This analysis consists of both the study of the content body and the email header containing the info about the given email. Email header analysis helps in identifying most of the email related crimes like spear phishing, spamming, email spoofing etc. Spoofing is a technique using which one can pretend to be someone else, and a normal user would think for a moment that it's his friend or some person he already knows. It's just that someone is sending emails from their friend's spoofed email address, and it is not that their account is hacked.

6.1 Tools used in Email Forensics:- These tools assist in Viewing email header, properties, hex value of email messages, Search option , data from email messages in multiple file formats etc.

MailXaminer	4n6 Email Forensics Wizard	Advik Email Forensic Wizard
MailPro+	Aid4Mail	Forensic
Xtraxtor	Sintelix	Autopsy

6.2 **Malware forensics :-** Malware is malicious code causing damage to data and systems by gaining unauthorized access. Malware forensic detect the purpose, functioning, or behaviour of the suspicious codes. It is helpful in the detection and mitigation of any potential threats. This can be done manually, using tools and techniques to reverse engineer and analyze the code, or using automated tools and analysis platforms to identify and classify malware. It is classified into three types. They are static, Dynamic and Hybrid.



6.3 **Tools for Malware Forensic: -**

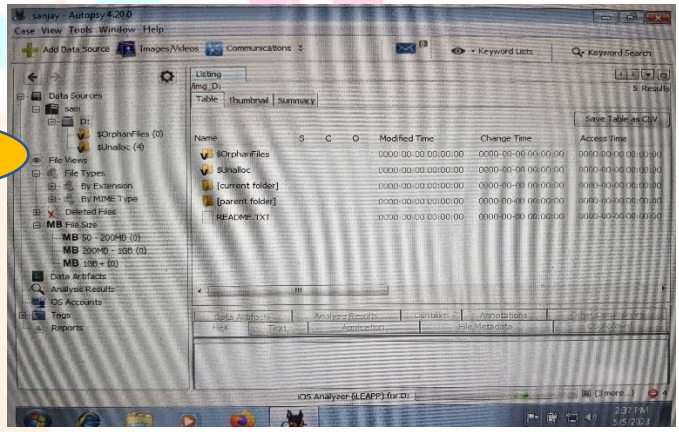
PeStudio	Process Hacker	Process Monitor
ProcDot	Autoruns	Fiddler
Wireshark	Radare2r	Ghidra
Cuckoo	Sandbox	Cutter

6.5 **Disk Forensic** :- Disk forensics involves extracting forensic information from digital storage media like like hard disks with IDE/SATA/SCSI interfaces, CD, DVD, Floppy disk, Mobiles, PDAs, flash cards, SIM, USB/ Fire wire disks, Magnetic Tapes, Zip drives, Jazz drives etc. First step in Disk Forensics is identification and segregation of any or all of the storage devices at the scene of crime . In the next step, a hash value of the storage media to be seized is computed using appropriate hashing algorithm. After computing the hash value, the storage media is securely sealed ,kept in Faraday's box and taken for further processing. An exact copy of the original evidence is created for analysis by using bit stream copying method. A record of chain of custody is maintained. Thereafter analysis by searching for keywords, picture analysis, time line analysis, registry analysis, mailbox analysis, database analysis, cookies, temporary and Internet history files analysis, recovery of deleted items and analysis, data carving and analysis, format recovery and analysis, partition recovery and analysis, etc are carried out. Now the reporting is carried out keep requirement of demanding party . the reports should contain nature of the case, details of examination requested, details of material objects and hash values, result of evidence verification, details of analysis conducted and digital evidence collected, observations of the examiner and conclusion. Lastly the Presentation of the report should be in simple terms and precise way so that non-technical persons should be able to understand the content of the report.

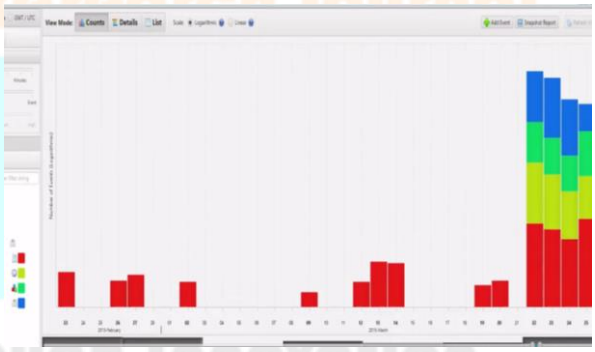
6.6 Tools for disk forensics: - The usage of toolkit in disk forensic assists in collection of disk, imaging of disks , decryption of encrypted disks, organising files and folders and preparation of reports in simple terms , which could be understood by court of Law.

Autopsy	FTK,	Bulk Extractor
Clonezila	Digital forensic framework	Ddrescue
paladin	encase	Sift workstation

6.7 Demo on disk forensics:- The toolkit autopsy is used to create a disk image and analysis of local hard disk created in Virtual machine with windows -7 installed on it .The complete database is depicted below.



The display of maximum usage of file system on specific date is obtained by forensic experts.



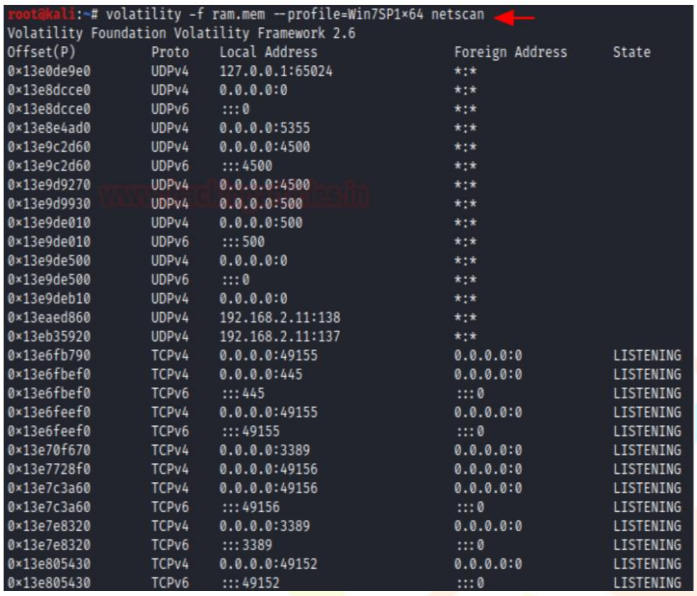
6.6 **Memory Forensic**:- It involves capturing and dumping the contents of a volatile content from RAM into a non-volatile storage device to preserve it for future investigation. Volatile data doesn't exist after the system reboot . Volatile memory is also prone to alteration of any sort due to the continuous processes running in the background. The memory (RAM)consist details of on-going processes and recently terminated processes , Files mapped in the memory (.exe, .txt, shared files, etc.) ,details of open TCP/UDP ports or any active connections , Caches data (clipboard data, databases, edited files, passwords, web

addresses, commands etc) and Presence of hidden data, malware.

6.7 **Tools of memory forensic:-**

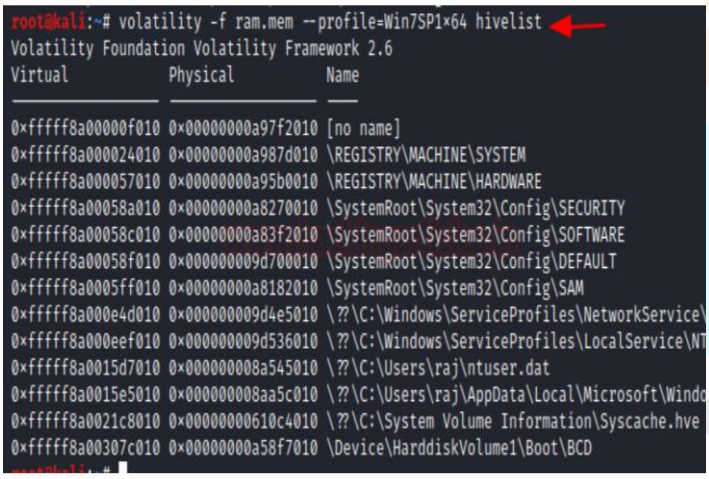
varc	volatility	Magnet RAM
rekall	windbg	LIME
Ftk imager	surge	AVML
fmem	winpmem	RAM Capturer

6.8 Demo on Memory forensics:- the command line for finding network-related artifacts present in the memory dump



```
root@kali:~# volatility -f ram.mem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State
0x13e0de9e0        UDPv4    127.0.0.1:65024                *:*
0x13e8dcce0        UDPv4    0.0.0.0:0                      *:*
0x13e8dcce0        UDPv6    :::0                           *:*
0x13e8e4ad0        UDPv4    0.0.0.0:5355                   *:*
0x13e9c2d60        UDPv4    0.0.0.0:4500                   *:*
0x13e9c2d60        UDPv6    :::4500                        *:*
0x13e9d9270        UDPv4    0.0.0.0:4500                   *:*
0x13e9d9930        UDPv4    0.0.0.0:500                    *:*
0x13e9de010        UDPv4    0.0.0.0:500                    *:*
0x13e9de010        UDPv6    :::500                         *:*
0x13e9de500        UDPv4    0.0.0.0:0                      *:*
0x13e9de500        UDPv6    :::0                           *:*
0x13e9deb10        UDPv4    0.0.0.0:0                      *:*
0x13eaed860        UDPv4    192.168.2.11:138               *:*
0x13eb35920        UDPv4    192.168.2.11:137               *:*
0x13e6fb790        TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING
0x13e6fbef0        TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING
0x13e6fbef0        TCPv6    :::445                         :::0                 LISTENING
0x13e6feef0        TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING
0x13e6feef0        TCPv6    :::49155                       :::0                 LISTENING
0x13e70f670        TCPv4    0.0.0.0:3389                   0.0.0.0:0            LISTENING
0x13e7728f0        TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING
0x13e7c3a60        TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING
0x13e7c3a60        TCPv6    :::49156                       :::0                 LISTENING
0x13e7e8320        TCPv4    0.0.0.0:3389                   0.0.0.0:0            LISTENING
0x13e7e8320        TCPv6    :::3389                        :::0                 LISTENING
0x13e805430        TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING
0x13e805430        TCPv6    :::49152                       :::0                 LISTENING
```

Command line to locate the virtual addresses of RAM present in the registry hives in memory, and their paths to hive on the disk.



```
root@kali:~# volatility -f ram.mem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----

0xfffff8a00000f010 0x00000000a97f2010 [no name]
0xfffff8a000024010 0x00000000a987d010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000057010 0x00000000a95b0010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a00058a010 0x00000000a8270010 \SystemRoot\System32\Config\SECURITY
0xfffff8a00058c010 0x00000000a83f2010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a00058f010 0x000000009d700010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a0005ff010 0x00000000a8182010 \SystemRoot\System32\Config\SAM
0xfffff8a000e4d010 0x000000009d4e5010 \??\C:\Windows\ServiceProfiles\NetworkService\
0xfffff8a000eef010 0x000000009d536010 \??\C:\Windows\ServiceProfiles\LocalService\NT
0xfffff8a0015d7010 0x00000008a545010 \??\C:\Users\raj\ntuser.dat
0xfffff8a0015e5010 0x00000008aa5c010 \??\C:\Users\raj\AppData\Local\Microsoft\Windo
0xfffff8a0021c8010 0x0000000610c4010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a00307c010 0x00000000a58f7010 \Device\HarddiskVolume1\Boot\BCD
```

7.0 **Essentials for cyber forensic professionals:-** the Security forces and LEA are facing a new domain where they are required to be proactive and alert always in updating them selves to face the evolving challenges in cyber crime. The essential qualities that our security professional are required to develop are as under

- **Knowledge of Information tech devices**:- Security forces when investigate any cybercrime ,they are required to handle various endpoint devices like mobile phone, printer, IoT, USB, external hard disk, iPad, notepad, digital camera, and projector. Hence, having a proper knowledge of digital devices and endpoint instruments will help in pre-accessing the functioning of devices and hence protect information loss.
- **Knowledge of Networking:-** Cybercrime investigation will not be limited to the individual IT system . the individual system will also be connected to LAN/WAN . Hence the knowledge of computer networking, LAN, Cloud computing ,cloud database and server is extremely important.
- **Knowledge of Operating system :- Security forces are required to conduct investigation on** Windows, Linux, Unix ,Mac and Android . The file system and knowledge of interacting with process will help in retrieving important artefacts.
- **Analytical Skills**:- The information are hidden at slack space /in hidden files etc etc . Hence it entirely depends on skill of cyber criminal . a good analytical skill and precise observational skill of security forces would be able to track the malafide intention of cyber criminal and bring out the evidences. Even a higher-level of analytical thinking is required by military and cyber intelligence professionals for handling International level of cyber expertise of cyber offender.
- **Knowledge of Cyber Law** :- the evidences are only admissible in court of law if the court get satisfied that the evidence are collected in legalise framework and a proper chain of custody is available . The security forces are required to produce the evidence and explain the technicalities in a way that is understood by the Judge. The knowledge of IT act 2000 , IT act 2008(amended) and International IT rules and regulations(ISO) , will make security forces aware of the integrities of the evidence collection and production in India as well abroad.
- **Knowledge of vulnerabilities**:- The cybercriminal always tries to exploit the vulnerabilities of a system and network. A proactive approach will always help security forces to handle vulnerabilities and protection from Zero day exploitation.
- **Good communication skill**:- A good communication skill helps in conveying the cybercrime in a manner that is well understood by authorities and Judges. The cyber forensic is a team work activities and conveying the details to team members will assist security forces experts to collect evidences in a lawful manner.
- **Perseverance and willingness to Learn:-** Cyber forensic is constantly evolving domain and require regular updating and patch up with latest technology. Hence this profession demand constantly upgrade to the latest trends and technologies . Cyber forensic demands a tedious and iterative investigation to cover all factors in detail. Hence security forces involved in this field requires a great sense of patience and perseverance .

8. **Conclusion:-** Cyber forensic involves deep diving into computer disk, Networks , memory segments ,software (malware) and communication Technology. These technologies are progressing rapidly to accommodate higher data rate and towards the use of complex and highly sophisticated protocols **.** The cybercrime is expanding at a relatively faster pace. The cybercrime record bureau data of India for 2020 as per table given below proves the significance of having a collective approach towards all security forces and LEAs.

Total Complaints Received and Cases Registered under IPC and SLL - 2020

S. No	Type of Complaint	Number of Complaints	No of FIR Registered	No of Online eFIR Registered
1	2	3	4	5
1	**Oral Complaints**	**9904696**	**679425**	
1.1	Narrated to O/C / SHO	883289	583690	
1.2	Distress call over phone/Dial 100 etc	9021407	95735	
2	**Written Complaints**	**9337418**	**5677958**	**243902**
2.1	To O/C / SHO	4767199	3268838	
2.2	To SP/Senior Officers	1075062	113329	
2.3	Court Complaints	86441	82971	
2.4	NHRC & SHRC	21018	970	
2.5	Commissions for SCs	6352	269	
2.6	Commissions for STs	1347	68	
2.7	National/State Commission for Women	29500	872	
2.8	Children Welfare Boards/Commission	1994	446	
2.9	Complaints Initiated Suo-moto by police	2210728	2050798	
2.10	Any Others Written Complaints	532108	144140	
2.11	Electronic/Online Form	605669	15257	243902
	Total Complaints/FIRs	**19242114**	**6357383**	**243902**
	Total FIRs Registered		**6601285**	

Thus this paper propose an integrated web based cyber forensic paradigm .This model is web based hence integrating latest technology into the model will be easily and maintaining the training and usage of various modules will too be a very easy.

Bibliography

1. International telecommunication union (ITU)publication on UNDERSTANDING CYBERCRIME:A GUIDE FOR DEVELOPING COUNTRIES(Accessed on 17/04/23)

2. https://www.legalserviceindia.com/legal/article-9498-an-overview-of-cyber-crimes-and-cyber-laws-in-india.html ((Accessed on 17/04/23 for def of cyber crime in india)

3. https://www.justice.gov/criminal-ccips/cybersecurity-unit(((Accessed on 17/04/23 for def of cyber crime in USA)

4. **INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES**
[ISSN 2581-5369] Volume 4 | Issue 3 2021 © *2021*
5. A Study PAPER to Examine Cyber Forensic:Trends and Patterns in India BY Ms. Shruti Verma AND Dr. Saurabh Mehta**
6. ***European Treaty Series - No. 185 on role of EU***
7. Inter-departmental Working Group on Computer Related Crime on Honkong
8. https://www.geeksforgeeks.org/mobile-forensics-definition-uses-and-principles/ for mobile forensics .