

HANDBOOK ON CYBER CRIME INVESTIGATION



Telangana State Police

HANDBOOK

ON

CYBER CRIME INVESTIGATION



TELANGANA POLICE

M. MAHENDAR REDDY, IPS.,
DIRECTOR GENERAL OF POLICE
Telangana State, Hyderabad.



Ph. Off : 040-23235170
040-23232831
Fax : 040-23296565
e-mail : dgp@tspolice.gov.in

14 FEB 2019

Foreword



As Police Officers, we all know that cybercrime incidents are undermining our nation's strategic and competitive advantages and are also negatively affecting our economy. However, we simply cannot grow and succeed in today's digital age without Information Technology as it has encompassed all walks of our lives.

Technology is a double-edged sword, as it provides new opportunities for those with criminal intentions as well. Every year several lakhs of citizens of our country are affected by cybercrimes, suffering huge personal and monetary losses.

In today's world, growing Cyber threats such as data thefts, phishing scams and other cyber-related crimes are affecting our lives more than ever before. Most of the Cybercrimes are happening due to negligence on the part of the users, and some existing vulnerabilities.

With the growing use of the Internet and Social Media Apps by people and organizations for various activities, it has become imperative for Law Enforcement Agencies to rise to the challenges and protect their privacy, assets, and critical information.

It is high time that we need to get a grasp of the situation and equip ourselves with new technologies to successfully counter and overcome the risks posed by cyber-related incidents.

I am of the strong opinion that cybercrimes can be effectively curtailed by suitably training the Police Officers of different ranks in various cyber domains such as Cyber Forensics, Cyber Security and in related landscapes.

It is with the above intention that we have prepared this *Handbook on Cybercrime Investigation* for use by Investigating Officers (IOs) and for the staff of related verticals.

In this regard, I would like to acknowledge the support rendered by the Experts from C-DAC, and CFSL, Hyderabad by providing invaluable insights and by reviewing the contents of this book.

I hope this handbook will aid the Police Officers in investigating Cyber-crimes in all their manifestations.


14/2/2019
(M. Mahendar Reddy)

Special Thanks to the following Experts for their valuable suggestions and support in preparing this Handbook:

Ch.A.S. Murthy, Joint Director, C-DAC, Hyderabad

Y. Surya Prasad, Deputy Director, CFSL, Hyderabad

Krishna Mangarai, Asst. Director, CFSL, Hyderabad

B. Ravi Kumar Reddy, DSP, CID, Telangana State

M.H. Noble, CEO, Zoom Technologies Pvt. Ltd., Hyderabad

Compiled by:

Eswara Sai Prasad Chunduru, Scientist-B, CFSL, Hyderabad

K. Srinath Reddy, DSP, Telangana Police

K. Nagendar Rao, Inspector, Telangana Police

First Edition: February, 2019

Disclaimer:

The information contained herein has been obtained from several sources believed to be reliable. While compiling the contents of this book care has been taken to provide the material in a lucid way. It would be happy to hear any suggestions, corrections, modifications and further topics to be addressed so that the same will be taken care in the future.

Distribution:

Restricted to Law Enforcement and Investigation Agencies.

CONTENTS

1. Computer Basics	01
2. Computer Architecture	03
3. Important parts of the Computer System	06
4. Basics of Networking	12
5. Hard Disk Drive	18
6. Identification of Media/Media types	19
7. File Systems	20
8. Introduction to Cybercrimes	21
9. Mobile Phones – Evidence to be considered	26
10. IP Address tracing	27
11. Email Investigation	28
12. Debit & Credit Card Frauds	29
13. Nigerian Frauds	31
14. Social Media	32
15. Computer Forensics	33
16. Crime Scene Security and Evaluation	39
17. Conduct Preliminary Interviews	40
18. Crime Scene Documentation	40
19. Evidence Collection	41
20. Flow Chart for collecting Electronic Evidence	45
21. Tools to be carried to Scene of Crime	46
22. SIM Card Investigation	48
23. Information that resides on Mobile Devices	52
24. Suggested Procedure for Search & Seizure of Mobile Phones	55
25. Flow chart for collecting Mobile Phone Evidence	59
26. CCTV/Digital Video Recorder – Basic Understanding	61
27. Procedure for downloading the Facebook Account	64
28. General Rules	70
29. Crime Scene Evidence Preservation	72

30. Important areas of Examination in Windows OS	74
31. Best Practices of Information Security – Do's & Don'ts	76
32. Social Networking	78
33. Phishing	78
34. Browser Security	79
35. Wi-Fi Security	80
36. Operating System Hardening	80
37. Password Security	81
38. Desktop Security	81
39. Important sections of Information Technology Act, 2000	83
40. Some useful Websites for investigation	85
41. Glossary	86
42. E-mail IDs of Various Agencies/Service Providers	106
43. Nodal Officers of Different Banks in India	110

FIGURES

Fig No.	Content	Page No.
Fig.1	Basic functions of Computer	02
Fig.2	Examples of Hardware devices	04
Fig.3	Operating System	04
Fig.4	Examples of Software	05
Fig.5	BIOS	09
Fig.6	Ports	09
Fig.7	Network diagram	12
Fig.8	Local Area Network (LAN)	13
Fig.9	Metropolitan Area Network (WAN)	13
Fig.10	Wide Area Network (WAN)	14
Fig.11	Internet	14
Fig.12	IP Address	15
Fig.13	Dynamic and Static IP Address	15
Fig.14	Public and Private IP Address	16
Fig.15	MAC Address	17
Fig.16	Parts of Hard Disk Drive	18
Fig.17	Connectors on a hard disk drive using ATA/SATA	18
Fig.18	Various File Systems	20
Fig.19	Types of Mobile Phone related crimes	27
Fig.20	Working of an E-mail	28
Fig.21	Camera, Card Skimmer and Keyboard Overlay	30
Fig.22	Shoulder Surfing	30
Fig.23	Various fields of Computer Forensics	33
Fig.24	Flow Chart for collecting Electronic Evidence	45
Fig.25	Tools to be carried to Scene of Crime	46
Fig.26	Flow Chart for collecting Mobile Phone Evidence	59
Fig.27	Internal view of a DVR	61
Fig.28	Flow Chart for seizure and retrieval of video footages from CCTV/DVR systems	63



A Computer is a machine or device that performs calculations, operations and process based on instructions provided by a software or hardware program.

Computer mainly consists of four parts – CPU, monitor, Keyboard and mouse. It takes input from the user, processes it and gives output in a systematic manner. Keyboard and mouse are input devices, monitor is output device.

The main characteristics of computers are speed, accuracy, diligence, versatility and storage capacity. The Computers work at an incredible speed. A powerful computer is capable of performing about 3-4 million simple instructions per second.

All digital data used in computer systems is represented binary system i.e. 0s and 1s. Binary coding systems have been developed to represent text, numbers, and other types of data.

There are five generations of computers. Each generation is characterized by a *major technological development* that fundamentally changed the way computers operate. Most major developments from the 1940's to present day have resulted in increasingly smaller, cheaper, more powerful and more efficient computing devices.

- First Generation (1940 – 1956):- Vacuum Tubes. These early computers used vacuum tubes as circuitry and magnetic drums for memory.
- Second Generation (1956 – 1963): Transistors.

- Third Generation (1964 – 1971): Integrated Circuits.
- Fourth Generation (1972 – 2010): Microprocessors.
- Fifth Generation (2011- till date): Artificial Intelligence

Functionalities of a Computer:

Computer carries out the following five functions –

Step 1 – Takes data as input.

Step 2 – Stores the data/instructions in its memory and uses them as required

Step 3 – Processes the data and converts it into useful information.

Step 4 – Generates the output.

Step 5 – Controls all the above four steps.

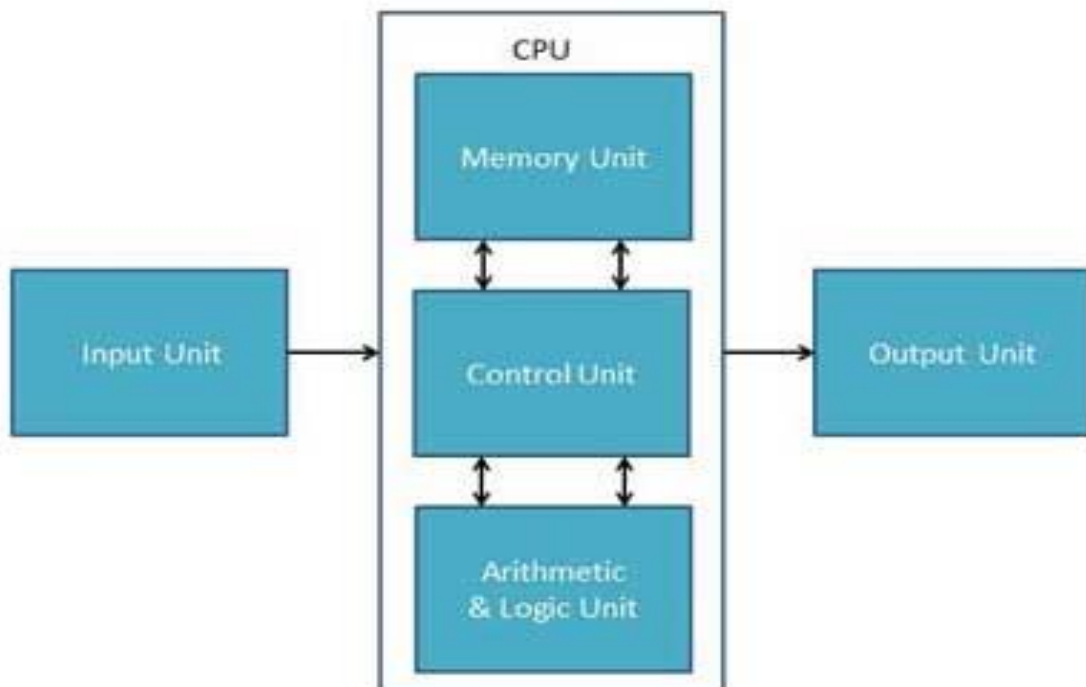


Fig 1. Basic functions of a Computer

COMPUTER ARCHITECTURE:

Computer architecture is a set of rules and methods that describe the functionality, organization, and implementation of computer systems. It is a specification detailing how a set of software and hardware technology standards interact to form a computer system or platform.

A Computer system is divided broadly into 3 parts based on their functionalities:

1. Hardware:

It is made up of the physical component of a computer i.e. Parts of the computer. They are two types – Input devices and Output devices. Following are some of the important input devices which are used in a computer –

- Keyboard
- Mouse
- Joy Stick
- Light pen
- Track Ball
- Scanner
- Graphic Tablet
- Microphone
- Magnetic Ink Card Reader(MICR)
- Optical Character Reader(OCR)
- Bar Code Reader
- Optical Mark Reader(OMR)

Following are some of the important output devices used in a computer.

- Monitors
- Graphic Plotter
- Printer



Fig 2. Examples of Hardware devices

2. Operating System:

It is a software that manages computer hardware and software resources and provides common services for various computer programs and allows hardware to communicate with the system. It performs all basic tasks like file management, memory management, process management, handling input and output, and controlling peripheral devices such as disk drives and printers. Some popular Operating Systems include **Linux**, **Windows**, iOS etc.



Fig 3. Operating System

3. Software:

It is a set of instructions or programs instructing a computer to do specific tasks. There are two major types of software – System Software and Application Software. System Software provides the basic functionality of the Computer. For eg. Operating System (OS), device drivers etc., whereas, Application Software is a programme that makes Computer to perform specific type of functionality. For eg. MS Office, Linux, Android, Mac OS etc.



Fig 4. Examples of software

➤ Relationship between Hardware and Software:

- Hardware and software are mutually dependent on each other. Both of them must work together to make a computer produce a useful output.
- Software cannot be utilized without supporting hardware.
- Hardware without a set of programs to operate upon cannot be utilized and is useless.
- To get a particular job done on the computer, relevant software should be loaded into the hardware.
- Hardware is a one-time expense.
- Software development is very expensive and is a continuing expense.

- Different software applications can be loaded on a hardware to run different jobs.
- A software acts as an interface between the user and the hardware.
- If the hardware is the 'heart' of a computer system, then the software is its 'soul'. Both are complementary to each other.

IMPORTANT PARTS OF THE COMPUTER SYSTEM

1. **Central Processing Unit (CPU):**



It is brain of the Computer. It does all the calculations and data processing.

CPU itself has following three components.

- Memory or Storage Unit
- Control Unit
- ALU(Arithmetic Logic Unit)

2. **Primary Storage Devices:**

Primary memory holds only those data and instructions on which the computer is currently working. It has a limited capacity and data is lost when power is switched off. It is generally made up of semiconductor device. These memories are not as fast as registers. The data and instruction required to be processed resides in the main

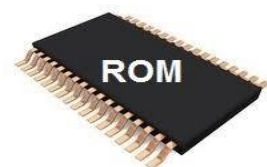
RAM (Random Access Memory) –

It is main memory. It requires power to store data.

Hence, volatile (temporary) in nature.



ROM (Read Only Memory) – It stores data permanently.



Characteristics of Main Memory:

- These are semiconductor memories.
- It is known as the main memory.
- Usually volatile memory.
- Data is lost in case power is switched off.
- It is the working memory of the computer.
- Faster than secondary memories.
- A computer cannot run without the primary memory.

3. **Secondary Storage Devices:**

This type of memory is also known as external memory or non-volatile. It is slower than the main memory. These are used for storing data/information permanently. CPU directly does not access these memories, instead they are accessed via input-output routines. The contents of secondary memories are first transferred to the main memory, and then the CPU can access it. For example, disk, CD-ROM, DVD, etc.

Characteristics of Secondary Memory:

- These are magnetic and optical memories.
- It is known as the backup memory.
- It is a non-volatile memory.
- Data is permanently stored even if power is switched off.
- It is used for storage of data in a computer.
- Computer may run without the secondary memory.
- Slower than primary memories.



RAM	ROM
1. Temporary Storage.	1. Permanent storage.
2. Store data in MBs.	2. Store data in GBs.
3. Volatile.	3. Non-volatile.
4.Used in normal operations.	4. Used for startup process of computer.
5. Writing data is faster.	5. Writing data is slower.

Difference between RAM and ROM

- The following table lists some higher storage units –

1 Kilobyte (KB)	1024 Bytes
1 Megabyte	1024 KB
1 Gigabyte	1024 MB
1 Terabyte	1024 GB
1 Petabyte	1024 TB

4. **Mother Board:**

It is the main circuit board of the Computer System. It controls all the physical devices and components that are connected to the Computer. CPU, RAM, Hard disk, Expansion cards are connected to it.



5. **BIOS (Basic Input Output System):**

It boots the system, recognizes the hardware devices, locates and loads the operating system.

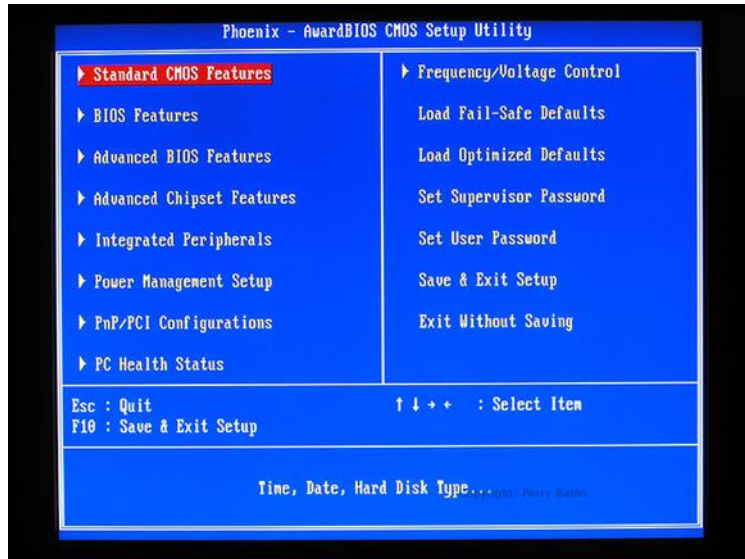


Fig 5. BIOS

6. Ports:

A port is a physical docking point using which an external device can be connected to the computer through which information flows from a program to the computer or over the Internet.

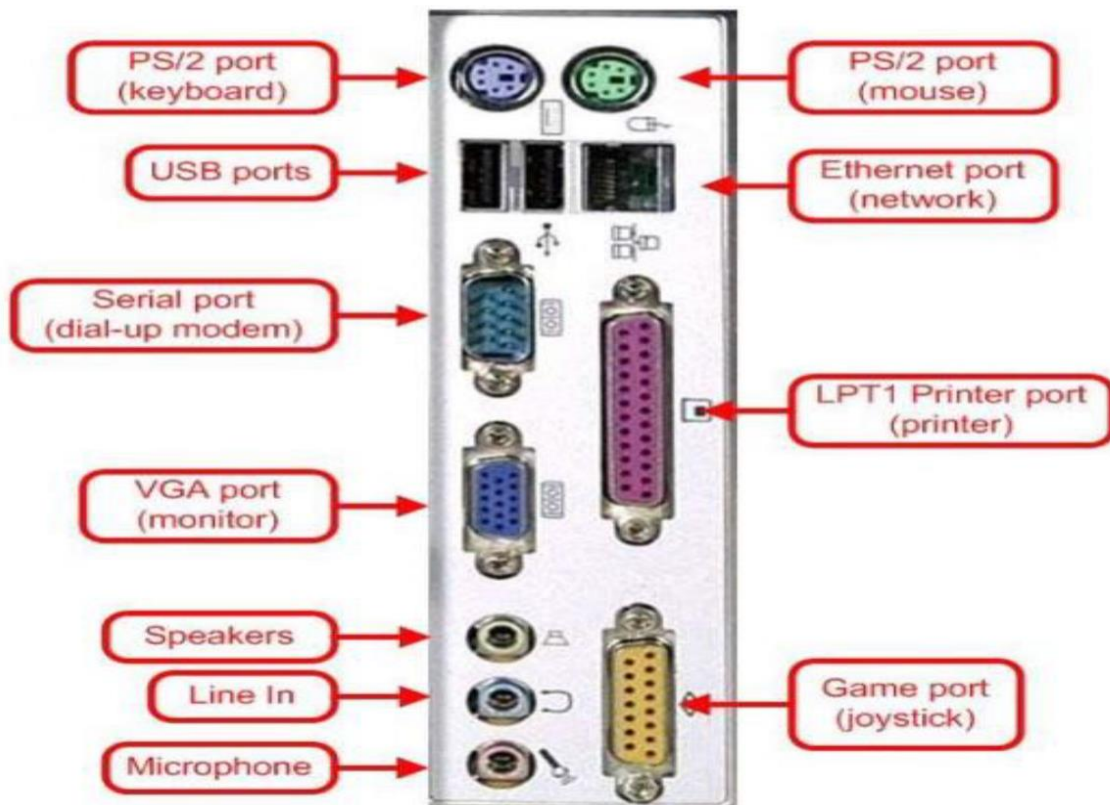


Fig 6. Ports

Explanation of few important types of ports –

Serial Port:

- Used for external modems and older computer mouse
- Two versions: 9 pin, 25 pin model
- Data travels at 115 kilobits per second

Parallel Port:

- Used for scanners and printers
- Also called printer port
- 25 pin model
- IEEE 1284-compliant Centronics port

PS/2 Port:

- Used for old computer keyboard and mouse
- Also called mouse port
- Most of the old computers provide two PS/2 port, each for the mouse and keyboard
- IEEE 1284-compliant Centronics port

Universal Serial Bus (or USB) Port:

- It can connect all kinds of external USB devices such as external hard disk, printer, scanner, mouse, keyboard, etc.
- It was introduced in 1997.
- Most of the computers provide two USB ports as minimum.
- Data travels at 12 megabits per seconds.
- USB compliant devices can get power from a USB port.

VGA Port:

- Connects monitor to a computer's video card.

- It has 15 holes.
- Similar to the serial port connector. However, serial port connector has pins, VGA port has holes.

Power Connector:

- Three-pronged plug.
- Connects to the computer's power cable that plugs into a power bar or wall socket.

FireWire Port:

- Transfers large amount of data at very fast speed.
- Connects camcorders and video equipment to the computer.
- Data travels at 400 to 800 megabits per seconds.
- Invented by Apple.
- It has three variants: 4-Pin FireWire 400 connector, 6-Pin FireWire 400 connector, and 9-Pin FireWire 800 connector.

Modem Port:

- Connects a PC's modem to the telephone network.

Ethernet Port:

- Connects to a network and high speed Internet.
- Connects the network cable to a computer.
- This port resides on an Ethernet Card.
- Data travels at 10 megabits to 1000 megabits per seconds depending upon the network bandwidth.

Game Port:

- Connect a joystick to a PC
- Now replaced by USB

Digital Video Interface, DVI port:

- Connects Flat panel LCD monitor to the computer's high-end video graphic cards.
- Very popular among video card manufacturers.

Sockets:

- Sockets connect the microphone and speakers to the sound card of the computer

BASICS OF NETWORKING:

Connecting to two or more PCs to a switch or Hub is called Network. Many different types of devices can be connected to Network like PCs, Servers, Printers, Smart phones, Tablets etc.

Network Diagram

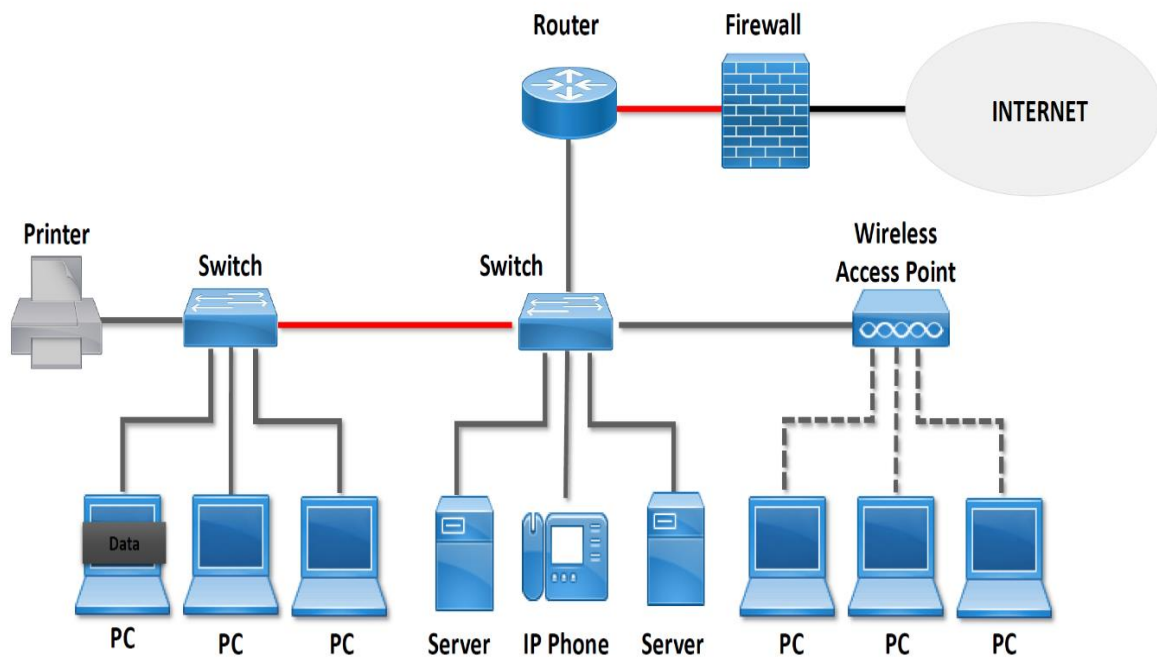


Fig 7. Network Diagram

Different types of Network:

- LAN (Local Area Network):

LAN is interconnections of PCS and other network devices that are very close together in a limited area such as same building, same floor etc.

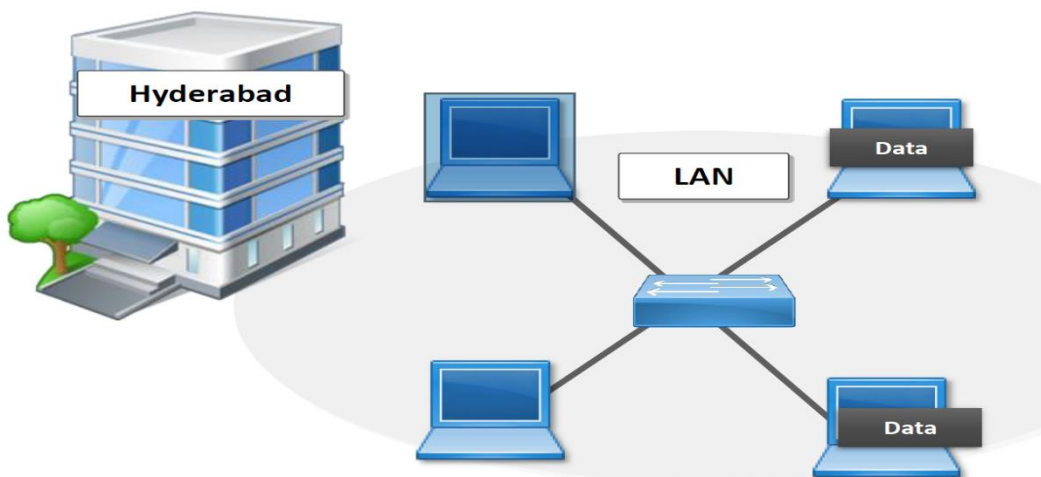


Fig 8. Local Area Network

- MAN (Metropolitan Area Network):

- Metropolitan Area Network are used to connect networking devices that may span around the entire city.

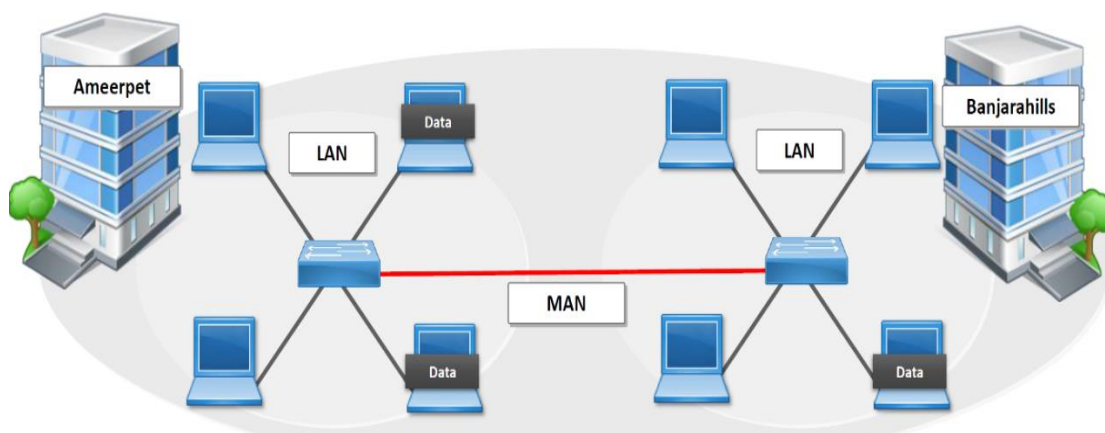


Fig 9. Metropolitan Area Network

WAN (Wide Area Network):

- Wide Area Networks which connects two or more LANs present at different geographical locations.

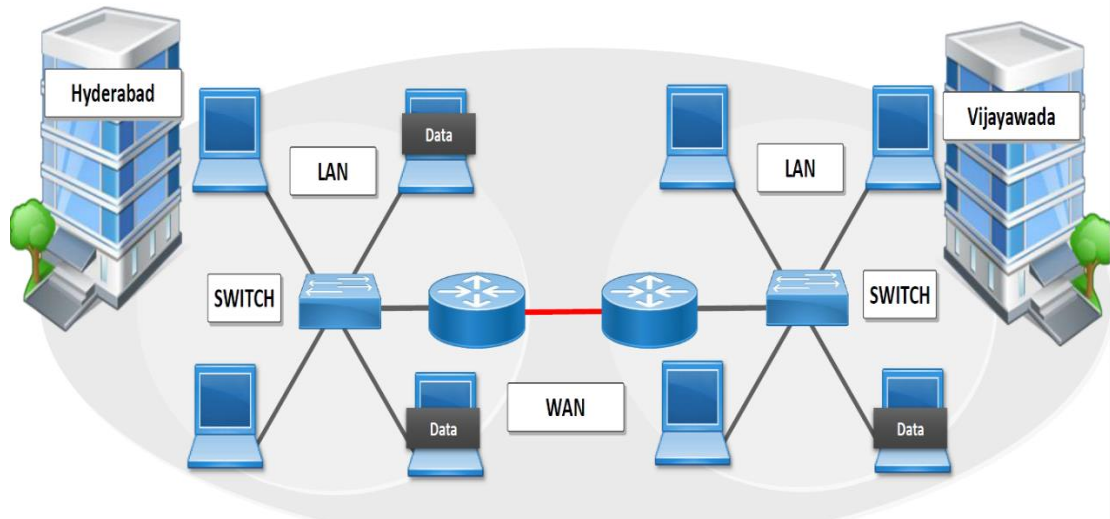


Fig 10. Wide Area Network

• INTERNET:

- Internet is a massive network of networks, a networking infrastructure.
- It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet.

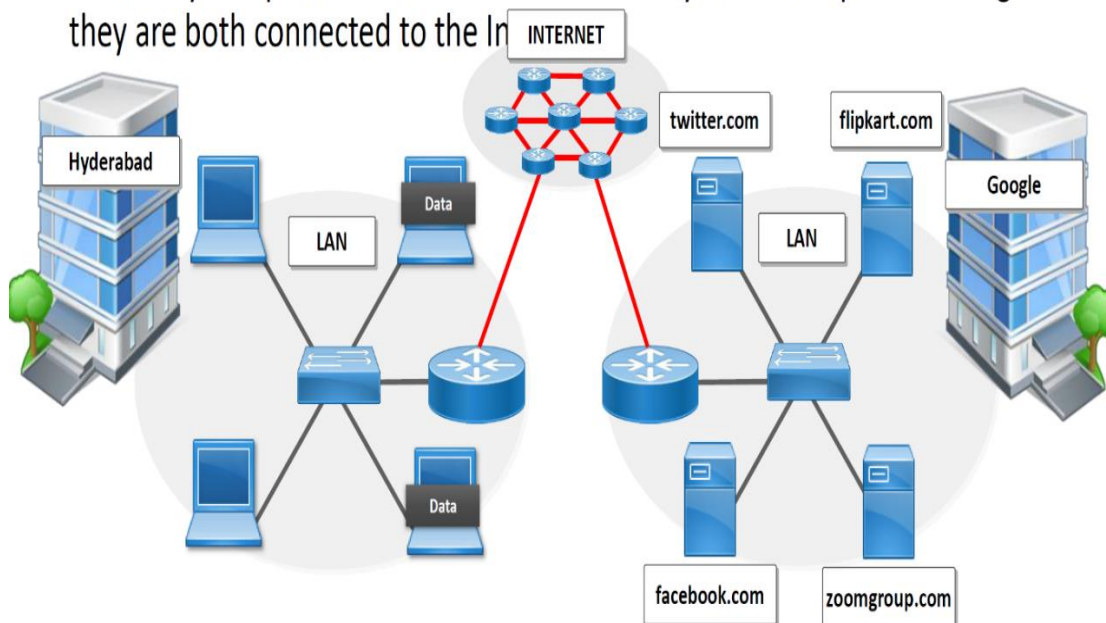


Fig 11. Internet

Internet Protocol (IP) Address:

- IP Address is a unique number that is assigned to each computer that participates in a network. This number is used to identify and locate each device.

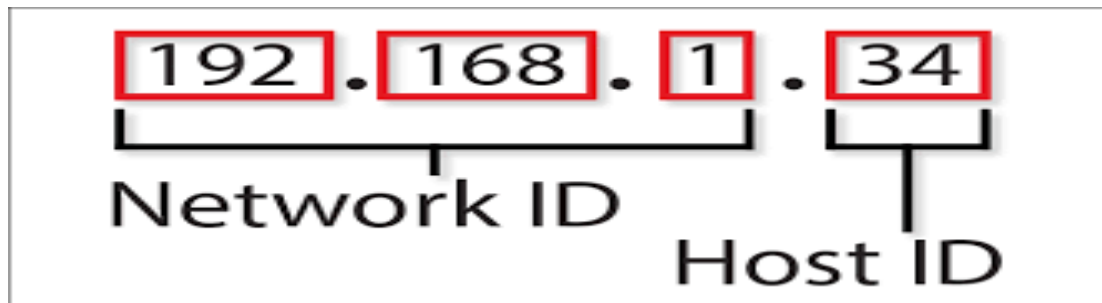


Fig 12. Internet Protocol Address

Each IP address includes a network ID and a host ID. The network ID identifies the systems and the host ID identifies a workstation, server, and router within the network.

➤ **Types of IP Addresses:**

- Static IP Address: It is also called as permanent address assigned to each device in a network.
- Dynamic IP Address: It is a temporary address assigned to the device when it is connected to the network

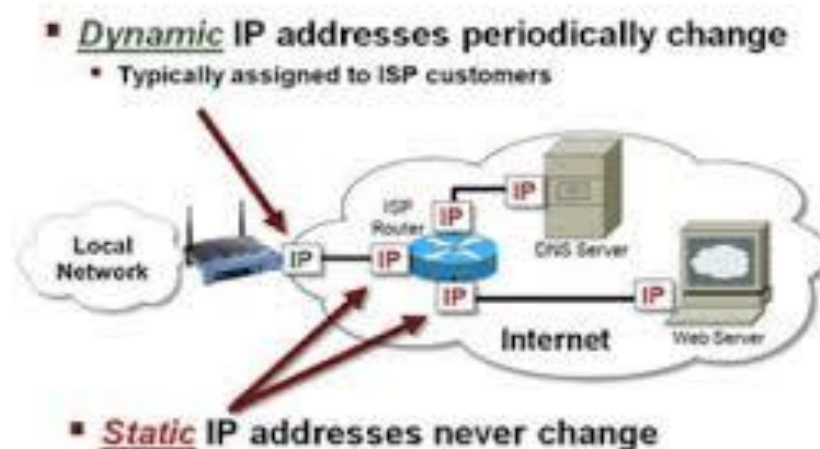


Fig 13. Dynamic and Static IP Addressing

- Public (external) IP Address: It is assigned by Internet Service Provider to identify a network to the outside world
- Private (internal) IP Address: It is assigned by the Router to each network device inside the network. This provides unique identification for devices that are within the network such as computer, mobile etc.

192.168.0.0 - 192.168.255.255 (65,536 IP addresses)

172.16.0.0 - 172.31.255.255 (1,048,576 IP addresses)

10.0.0.0 - 10.255.255.255 (16,777,216 IP addresses)

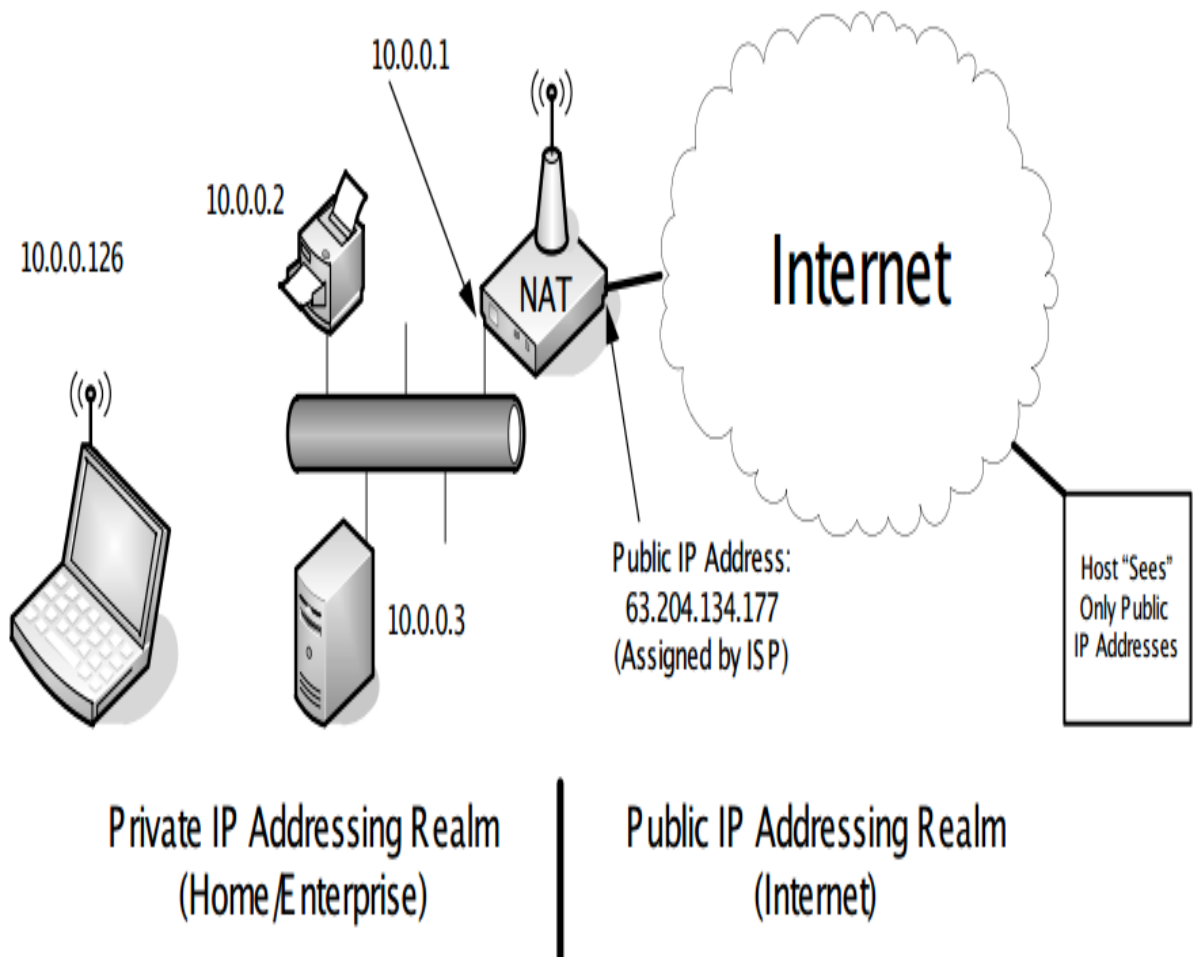


Fig 14. Public and Private IP Addressing

- There are two versions of IP.
 - IP Version 4 is a 32-bit address (A bit is represented by either 0 or 1). IPv4 Address range is from 0.0.0.0 to 255.255.255.255
 - IP Version 6 is a 128-bit address and the most recent version of the Internet Protocol (IP)
 - e.g. 2001:0055:0092:0034:0000:0000:0011:0065

➤ Media Access Control (MAC) Address:

It is a unique hardware address or physical address of the computer. It is assigned by the manufacturer and useful in identifying the computer.

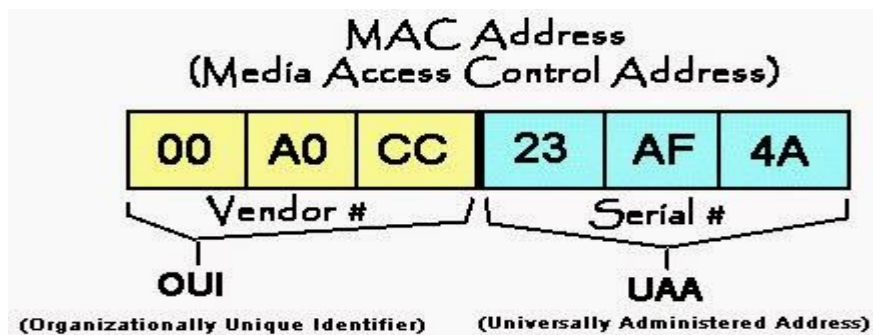
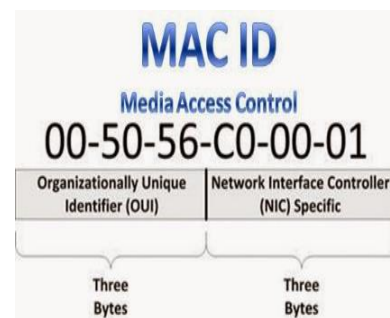
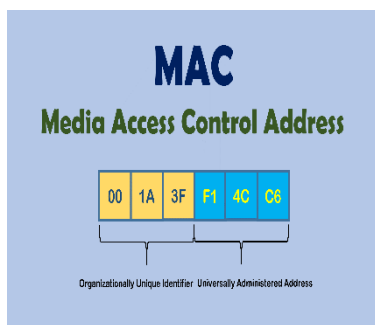


Fig 15. MAC Address

For searching the Vendor details from the MAC use the online resources like: <https://regauth.standards.ieee.org/standards-raweb/pub/view.html#registries>

Hard Disk Drive (HDD):

Hard drives have two kinds of components - internal and external. External components are located on a printed circuit board called logic board while internal components are in a sealed chamber called HDA or Hard Drive Assembly.

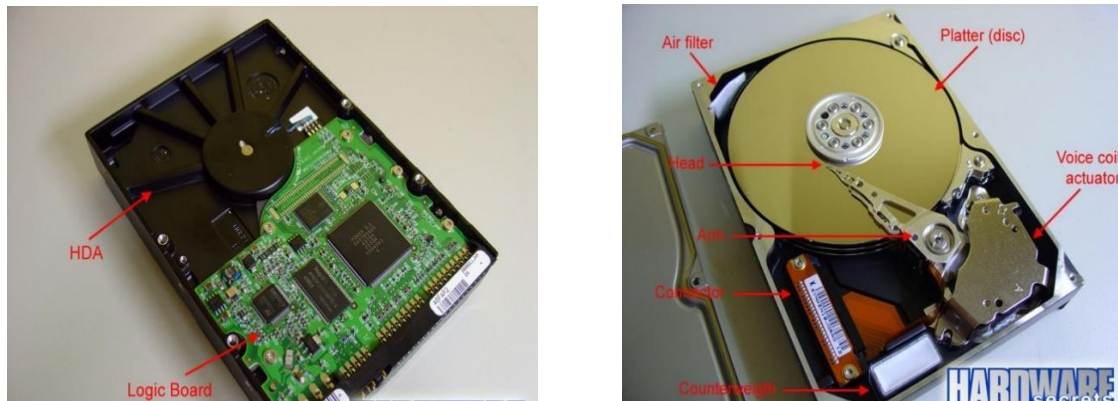


Figure 16: Parts of Hard Disk Drive.

The most common hard disk drive interface for end-users is called ATA (Advanced Technology Attachment) and SATA (Serial ATA)

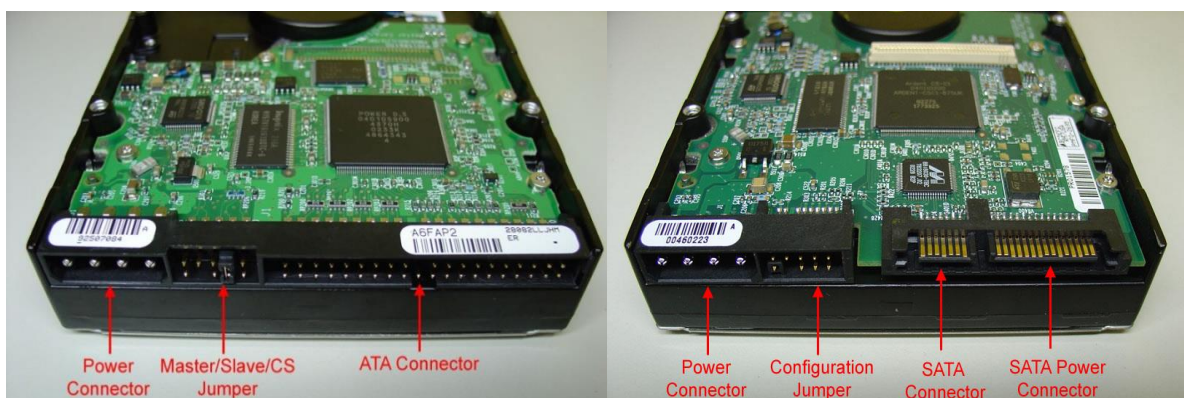


Figure 17: Connectors on a hard disk drive using ATA/SATA interface.

IDENTIFICATION OF MEDIA/MEDIA TYPES

Media Type	Reader	Typical Capacity	Comments
Primarily Used in Personal Computers			
Floppy disk	Floppy disk drive	1.44 megabytes (MB)	3.5 inch disks; decreasing in popularity
CD-ROM	CD-ROM drive	650 MB – 800 MB	Includes write-once (CD-R) and rewriteable (CD-RW) disks; most commonly used media
DVD-ROM	DVD-ROM drive	1.67 gigabytes (GB) – 15.9 GB	Includes write-once (DVD±R) and rewriteable (DVD±RW) single and dual layer disks
Hard drive	N/A	20 GB – 300 GB	Higher capacity drives used in many file servers
Zip disk	Zip drive	100 MB – 750 MB	Larger than a floppy disk
Jaz disk	Jaz drive	1 GB – 2 GB	Similar to Zip disks; no longer manufactured
Backup tape	Compatible tape drive	80 MB – 320 GB	Many resemble audio cassette tapes; fairly susceptible to corruption due to environmental conditions
Magneto Optical (MO) disk	Compatible MO drive	600 MB – 9.1 GB	5.25 inch disks; less susceptible to environmental conditions than backup tapes
ATA flash card	PCMCIA slot	8 MB – 2 GB	PCMCIA flash memory card; measures 85.6 x 54 x 5 mm
Used by Many Types of Digital Devices			
Flash/Jump drive	USB interface	16 MB – 2 GB	Also known as thumb drive because of their size
CompactFlash card	PCMCIA adapter or memory card reader	16 MB – 6 GB	Type I cards measure 43 x 36 x 3.3 mm; Type II cards measure 43 x 36 x 5 mm
Microdrive	PCMCIA adapter or memory card reader	340 MB – 4 GB	Same interface and form factor as CompactFlash Type II cards
MultiMediaCard (MMC)	PCMCIA adapter or memory card reader	16 MB – 512 MB	Measure 24 x 32 x 1.4 mm
Secure Digital (SD) Card	PCMCIA adapter or memory card reader	32 MB – 1 GB	Compliant with Secure Digital Music Initiative (SDMI) requirements; provides built-in data encryption of file contents; similar in form factor to MMCs
Memory Stick	PCMCIA adapter or memory card reader	16 MB – 2 GB	Includes Memory Stick (50 x 21.5 x 2.8 mm), Memory Stick Duo (31 x 20 x 1.6 mm), Memory Stick PRO, Memory Stick PRO Duo; some are compliant with SDMI requirements and provide built-in encryption of file contents
SmartMedia Card	PCMCIA adapter or memory card reader	8 MB – 128 MB	Measure 37 x 45 x 0.76 mm
xD-Picture Card	PCMCIA adapter or xD-Picture card reader	16 MB – 512 MB	Currently used only in Fujifilm and Olympus digital cameras; measure 20 x 25 x 1.7 mm

FILE SYSTEMS:

A *filesystem* defines the way that files are named, stored, organized, and accessed on logical volumes. Many different filesystems exist, each providing unique features and data structures. e.g., File Allocation Table [FAT], NT File System [NTFS].

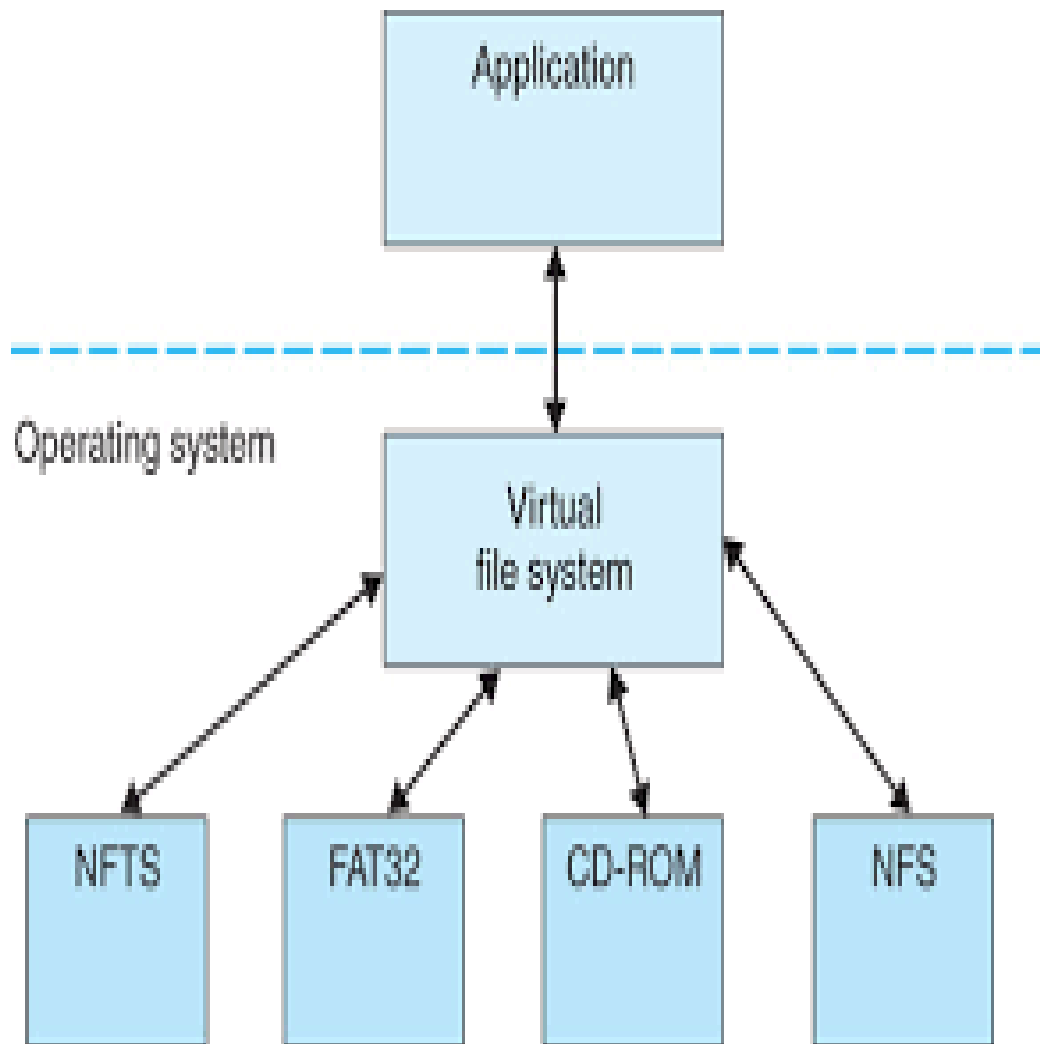


Fig 18. Different file systems

INTRODUCTION TO CYBER CRIMES



- **What is Cyber Crime?**

“Any illegal or unauthorized activity involving computers can be termed as Cyber crime. The crime can be against an individual or an organization. It can even be against the nation endangering or threatening to endanger its integrity and security”.

- **What is a Malware?**

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim.

- **What is a Sniffer?**

A program and/or device that monitors data traveling over a [network](#). Sniffers can be used both for legitimate [network management](#) functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network’s security because they are virtually impossible to detect and can be inserted almost anywhere.

- **What is Rootkit?**

A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker’s activities on the host and permit the attacker to maintain root-level access to the host through covert means.

- **What is Spoofing?**

Refers to sending information that appears to come from a source other than its actual source.

- [What is Spyware?](#)

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

- [What is Steganography?](#)

The art and science of communicating in a way that hides the existence of the communication.

- [What is Trojan?](#)

A non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose.

- [What is a Virus?](#)

A self-replicating program that runs and spreads by modifying other programs or files.

- [What is a Worm?](#)

A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

- [What is Zombie?](#)

A program that is installed on a system to cause it to attack their systems.

- [What is Phishing?](#)

Using spoof E-mails or directing the people to fake web sites to fool them into divulging personal financial details so that criminals can access their accounts.

- [What is Data Diddling?](#)

Involves altering the raw data just before a computer processes it and then changing it back after processing is completed.

- [What is Salami Attack?](#)

This attack involves making alteration so insignificant that in a single case it would go completely unnoticed. Attacks are used for commission of financial crimes.

- [What is Social engineering?](#)

A hacker term for deceiving or manipulating unwitting people into giving out information about a network or how to access it.

- [What is Cyber Defamation?](#)

Defaming an individual or a company's web site thereby causing embarrassment and also loss.

- [What is Identity theft?](#)

Theft of one's identity for illegal use.

- [What is Cyber squatting?](#)

Preemptively reserving domain names which are Trademarks of others

- [What is Cyber pornography?](#)

Using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc).

- [What is Hacking?](#)

Unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network.

- [What is Cyber Stalking?](#)

Defined as the repeated acts harassment or threatening behavior of the cyber-criminal towards the victim by using internet services. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects.

- [What is Vishing?](#)

Vishing" or "Voice Phishing" is the act of leveraging a new technology called Voice over Internet Protocol (VoIP) in using the telephone system to falsely claim to be a legitimate enterprise in an attempt to scam users into disclosing personal information. Government, financial institutions, as well as online auctions and their payment services, can be targets of Voice Phishing

- [What is denial-of-service attack \(DoS attack\)?](#)

An attempt to make a computer resource unavailable to its intended users.

- [What is distributed denial-of-service \(DDoS\) attack?](#)

It is a multitude of compromised systems attack a single target computer, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

- [What is Spyware?](#)

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet.

- [What is backdoor?](#)

Is a method of bypassing normal authentication or securing remote access to a computer, while attempting to remain hidden from casual inspection.

- [What is Cracker?](#)

Cracker is a cyber burglar or vandal, an individual or group intent on causing malicious harm to a network or computer.

- [What is Root kit?](#)

Rootkit is a type of malicious [software](#) that is activated each time your system [boots](#) up. Rootkits are difficult to detect because they are activated before your system's [Operating System](#) has completely booted up. A rootkit often allows the installation of hidden files, processes, hidden user accounts, and more in the systems OS. Rootkits can intercept data from terminals, [network](#) connections, and the [keyboard](#).

- [What is buffer overflow?](#)

The condition wherein the data transferred to a [buffer](#) exceeds the storage capacity of the buffer and some of the data “overflows” into another buffer, one that the data was not intended to go into.

- [What is spamming?](#)

Spamming is receiving the unsolicited material.

- [What is logic bomb?](#)

Also called *slag code*, [programming code](#) added to the [software](#) of an [application](#) or [operating system](#) that lies dormant until a event occurs, [triggering](#) the code into action such as terminating the programmers employment

- [What is Email bombing?](#)

Email bombing is sending many emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing

- [What is Web jacking?](#)

Occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

➤ MOBILE PHONES - Evidence to be considered:



Mobile phone services offer different types of electronic evidences. During the investigation, the IO shall analyse the following services of mobile phone.

- Outgoing calls
- Incoming calls
- SMS/MMS messages
- Phone book
- Social Media activity (Facebook, Twitter etc.)
- WhatsApp/Telegram- chats/photos/videos/voice messages/call logs
- Stored information e.g. PDFs, documents, videos, audios
- Screen shots
- Captured pictures/videos
- To do list/ reminders
- E-mail activity

➤ Types of Mobile Crimes:

- Threatening calls/SMS
- Obscene Calls/SMS
- Blackmailing
- Handset Theft
- Hacking mobile set through Bluetooth
- Cloning of SIM cards
- IMEI change
- MMS crimes

TYPES OF MOBILE PHONE RELATED CRIMES



Fig 19. Mobile phone crimes

INTERNET PROTOCOL (IP) ADDRESS TRACING:

IP Address is a unique number assigned to a computer that is connected to the Internet. In the Internet world, computers are differentiated from one another based on the IP Address. Hence, IP Address is an address of a computer that is connected on the Internet. Tracing of IP Address is useful to identify the cyber criminals.

The Internet Service Providers (ISPs) provide access to Internet to users. Whenever any user is accessing their Internet service the IP Address of the user computer is captured and preserved in their server logs. Based on such data culprit can be traced. Hence, IOs shall obtain IP address details from Service Providers for the purpose of investigation.



E-Mail involves composing, sending, storing and receiving messages over electronic communication systems. It contains three parts-

- E-mail Envelope: Email is enclosed in a digital envelop
- E-mail Header: It contains the Meta information of the e-mail. That is originator's e-mail address, recipient's e-mail address, e-mail date/time, information of intermediate email servers etc.
- E-mail Body: It contains email text/attachments

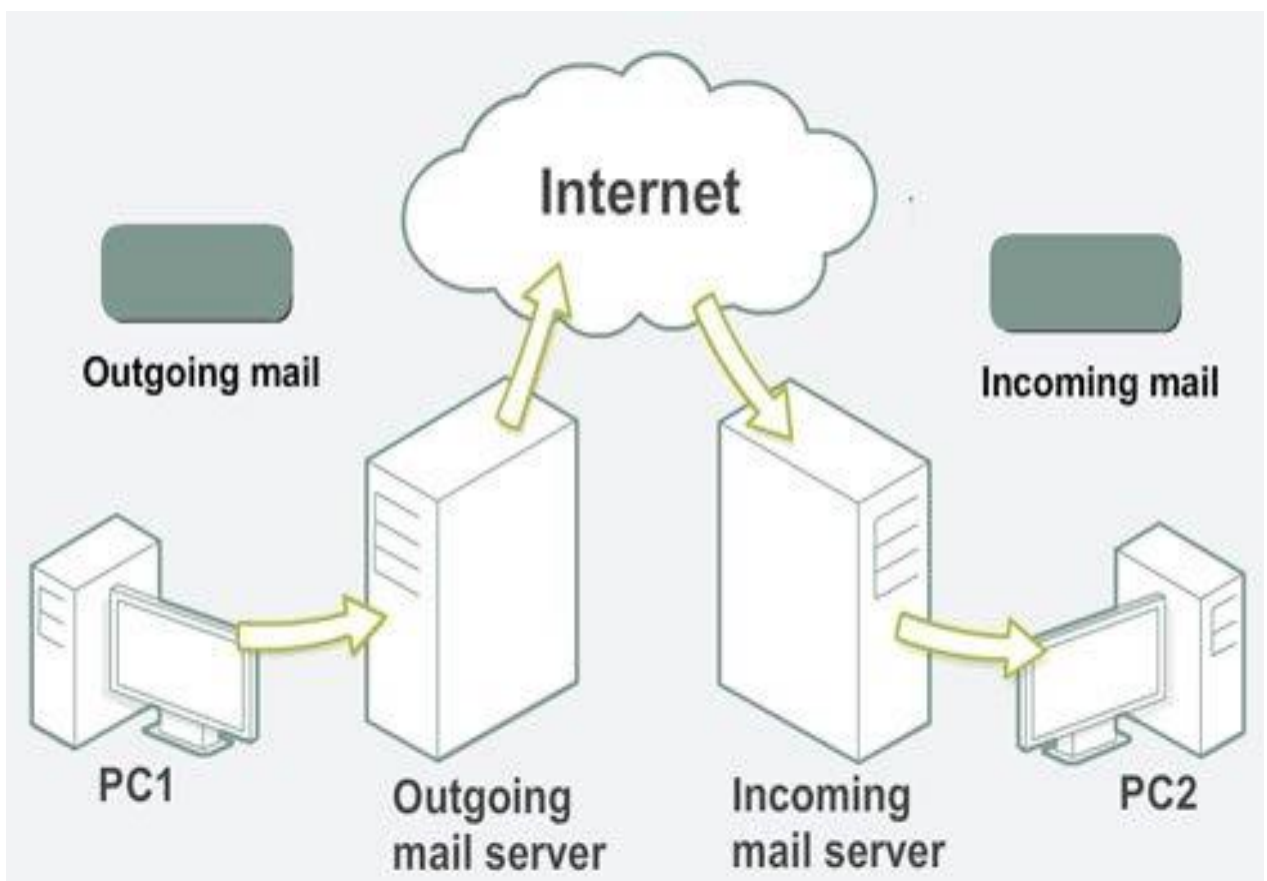


Fig 20. Working of an E-mail

➤ Steps in tracing the E-Mail:

- Identify the e-mail/s of relevance by accessing the mail box of the complainant.
- Take print of the e-mail/s in presence of two independent witnesses and draw a panchanama.
- Try to save the mails of relevance into a separate folder in the mailbox like evidence.
- Take the backup of the e-mail/s in to **msg** format and calculate the hash value. Document the entire procedure.
- If possible, take the backup of the entire mailbox in to PST/OST via eM Client/Outlook/Thunderbird/Opera Mail/Hiri/Mail Bird.
- Collect full header of the e-mail
- Identifying the IP Address of the sender/mail service provider from the mail header.
- Contact the mail service provider with copy of the full header with 92 Cr.PC to get the details of the IP address of the sender.
- Now use the online resources like **whois** databases to find out the internet service provider details.
- Contact the nodal officer of the concerned internet service provider to get the subscriber/originator details.

DEBIT & CREDIT CARD FRAUDS:

Debit Cards and Credit Cards are accepted as legal tender at ATM centres, shops and establishments. The frauds include skimming and cloning, shoulder surfing, swapping of cards at ATM centres.





Fig 21. Camera, Card Skimmer and Keyboard Overlay



Fig 22. Shoulder Surfing

NIGERIAN FRAUDS:

These are called Nigerian Frauds because in most of the cases nationals of Nigeria are involved. In these types of frauds, a message is sent to victim's mobile phone/e-mail that they have won millions of dollars/pounds Lottery and victims are asked to send some advance fee/processing fee/transfer charges to get Lottery money.

From: Columns [info@qnet.com]
Sent: 21 November 2011 01:18
Subject: 20:11:2011

Good day,

I am Johnson Ahmad, a close confidant of the daughter of the late Colonel Muammar Gadhafi. I am a financial analyst based here in the United Kingdom. If you are conversant with what is going on in the World, you would have heard that Colonel Muammar Gadhafi has being killed. Presently the United Nations is doing everything in their power to ensure that all the family funds stashed in different banks all over the World are confiscated, of which they have succeeded 100%. As a close confidant and Financial adviser to the daughter of the late Libyan leader, i am privy to a secret deposit amounting to Sixteen million British pounds sterling (?16,000,000). These funds is deposited with a financial firm. This is the only deposited funds that has not being confiscated by the United Nations due to the fact that it was deposited with the name of one of her maid and personal assistant. But due to the current investigation going on and the nature of things surrounding the Gadhafi family presently, it is unsafe and unwi

This is the reason i am sending you this email on behalf of the daughter of the late Libyan leader, Ayeesha, to help receive this funds in your name as the depositor and owner of the funds. If you are willing to help out please do reply back to this mail as soon as you can, as time is of a great excess, before the funds is discovered.

As soon as i get a response from you, i will give you full details on what needs to be done to achieve it. Ayeesha would not mind how much percentage you would want for your help and assistance provided the deposit is changed to your name and that it remains in your custody until the whole investigation dies off as this money is the last hope for her to live a normal life.

I will be expecting to hear from you.

Johnson Ahmad.

Fig. Example of Nigerian fraud mail

SOCIAL MEDIA:

Social media is collection of online communications channels dedicated to community-based interaction, and content-sharing. Eg. Forums, blogging sites, wikis etc.



Popular social media sites are:

1. Facebook
2. Twitter
3. Instagram
4. Snapchat
5. Myspace
6. LinkedIn
7. Flickr
8. Vimeo
9. Google +
10. Skype
11. Youtube
12. WhatsApp etc.



- **What are Cyber Forensics?**

Cyber forensics is the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. It can be also defined as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.

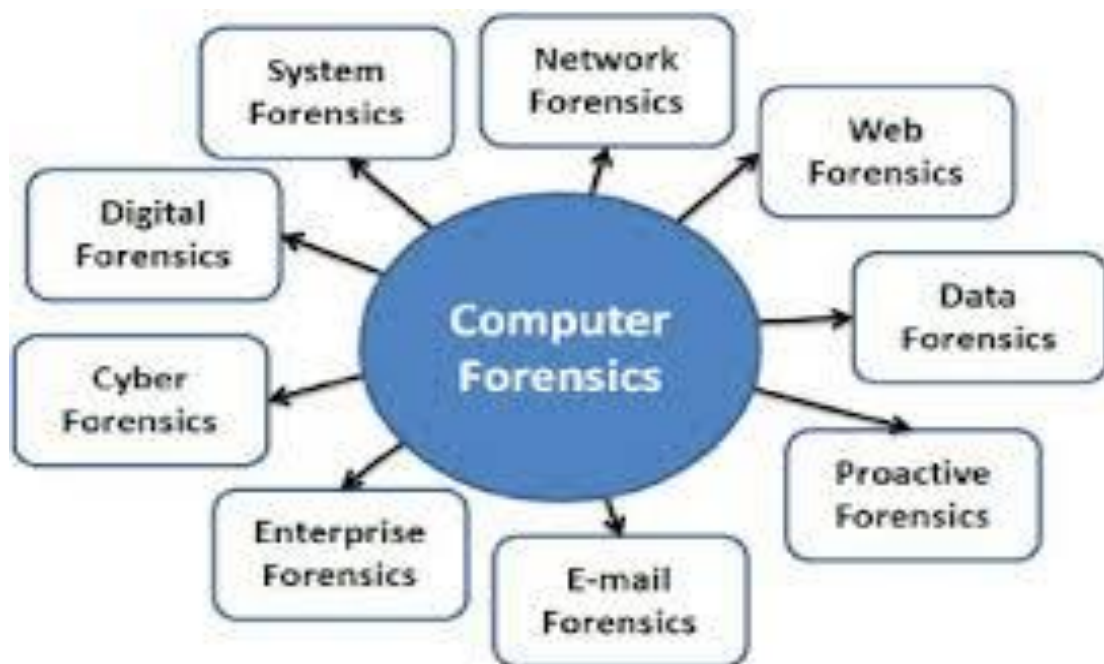


Fig 23. Various fields of Computer Forensics

- **What are Network Forensics?**

Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. It involves log analysis and a real time analysis.

- **Why organizations require Cyber Forensics Services?**

In a recent survey conducted by the FBI, it is estimated that over 85% of all crimes and infractions committed today contain digital evidence. A computer crime survey of medium and large companies revealed that 99.6% of respondents were victim of an unauthorized access, and 85% had detected security breaches the previous year. Even more disconcerting, 99% of reported intrusions result through exploitation of known vulnerabilities and configurations errors. In a 2004 survey of 400 companies revealed an estimated \$70 million in losses of intellectual property or digital information. In another survey Business Week, it is estimated that over 90% of all data created today is in electronic format. As business relay more and more on computers to conduct their day to day business, the amount of electronic data will continue to rise.

- **What are Disk Forensics/ media Forensics?**

Disk forensics is the process of acquiring and analyzing the data stored on some form of physical storage media. It includes the recovery of hidden and deleted data.

- **Source Code Forensics?**

It deals with determination of software ownership or software liability issues. It involves review of actual source code, examination of the entire development process, e.g., development procedures, documentation review, and review of source code revisions.

- **Mobile Forensics?**

Mobile forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods.

- **What are Cardinal Rules of Computer Forensics?**

- Never work on original evidence.
- Never mishandle evidence.
- Use proper software utilities.

- Never trust the subject operating system.
- Document everything
- [What is E-mail forensics?](#)
Email forensics is the study of source and content of electronic mail as evidence. It deals with the identifying the actual sender and recipient of a message, date/ time it was sent.
- [What is digital evidence?](#)
Digital evidence is any information of probative value that is either stored or transmitted in a binary form. The three forms of digital evidence are stored data, transmitted data and volatile data.
- [What are PDA Forensics?](#)
Forensic Analysis of personal digital assistants (PDA's) to retrieve information like messages, documents, telephone numbers etc.,
- [What is forensic imaging?](#)
Generating a bit for bit copy of the original media including free space and slack space, also called physical back up.
- [What happens when you 'delete' a file?](#)
Think of a card catalogue in a library. When you delete something, all that you are doing is throwing out the card from the card catalogue. The book remains on the shelf. The computer has only been told that the space on the shelf is available for use if necessary. If the computer does use that space, then the old file is overwritten and is gone. With our software tools we can find those 'old books' still on the shelves. Often, even if we can't get all the 'book,' we can get substantial parts of it.
- [Who requires cyber forensics?](#)
 - Victim (Organizations / Government / individuals)
 - Law Enforcement
 - As a part of network security life cycle

- [What is logical back up?](#)

A logical backup copies the directories and file of a logical volume. It does not capture other data that may be present on the media such as deleted files or residual data stored in the slack space.

- [What's the difference between formatting, de-fragmenting and wiping?](#)

Formatting, de-fragmenting, and wiping are three of the most common processes used by people attempting to destroy computer records. Formatting a drive is a quick and easy housekeeping task that eliminates the document indexes and file/folder pointers on a computer hard drive. In most cases, the formatting does not harm the data on the hard drive. The contents of the documents, files, and folders still physically exist on the drive and are fully recoverable by computer forensic experts using best practice industry standards. De-fragmenting is easily thought of as a reorganization of the computer's filing cabinet. To make the computer run more efficiently, all the files are condensed to the smallest space possible, reorganized, and placed at the front of the drive. De-fragmenting a computer will not harm the active data (the data that a user can access on their own from the desktop) but may render normally recoverable deleted data (the data that only a forensic engineer can recover) virtually unrecoverable. However, depending on the size the drive, amount of data, and order of operations, in certain circumstances deleted files might be recoverable after de-fragmentation. Wiping involves the use of a software program to intentionally overwrite data with a specific or randomly generated pattern of "1s" and "0s". If run properly, a wiping utility will make the data unrecoverable by commercial computer forensic experts. Depending on the software program that was run, computer forensic experts might be able to tell the date, time, and specific program used to conduct the wiping.

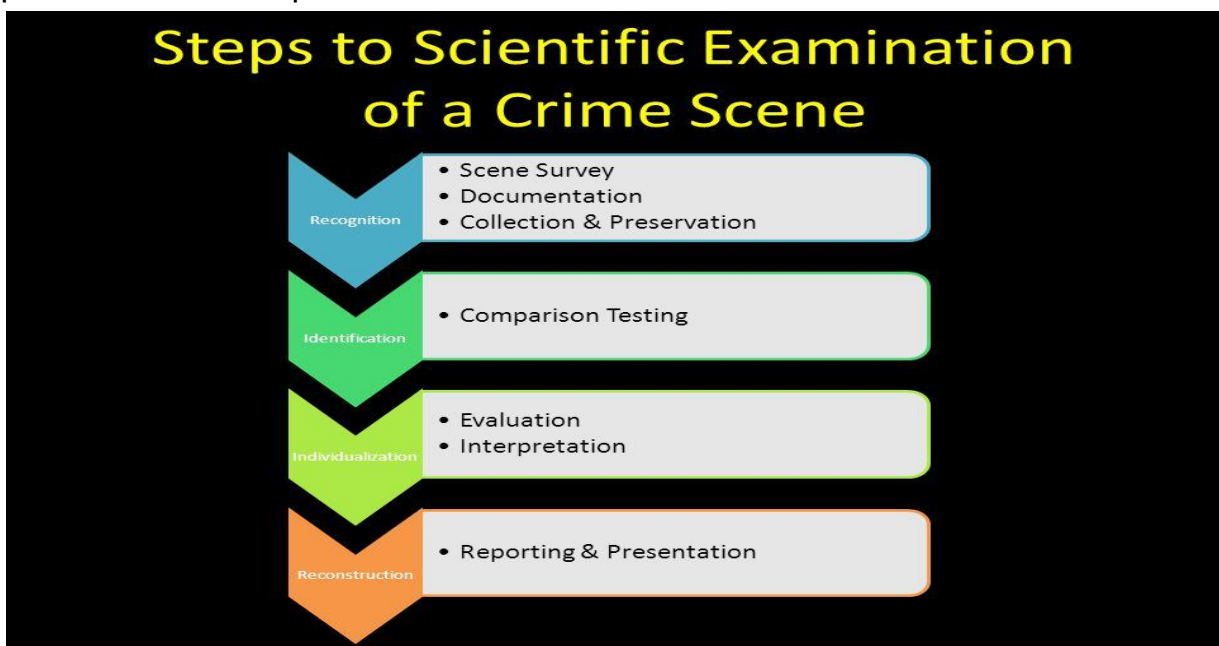
- What are the stages of cyber forensic process?
 1. There are six stages
 2. Identification of evidence
 3. Acquiring the digital evidence (forensic imaging)
 4. Authentication of forensic image
 5. Analysis of the image
 6. Documentation of all the findings
 7. Providing testimony in court of law
- What are the types of forensic requests?
 - Intrusion analysis
 - Damage assessment
 - Suspect Examination
 - Toll analysis & Log file analysis
 - Evidence Search
 - System Audit
- What are points to be considered regarding digital evidence by a cyber forensic analyst?
 - NO possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer
 - Evidence is properly handled
 - A continuing chain of custody is established and maintained
 - All the procedures and findings are thoroughly documented.
- What are the steps taken by Cyber Forensic Expert during investigation and analysis?
 - Protects the suspected system during examination.
 - Discover and recover all files.
 - Access the contents of password protected and encrypted file
 - Look for evidence in slack space, unallocated space, hidden Partitions, etc.
 - Analyse the relevant data obtained from the suspected system.
 - Provides testimony in the court of law if required.

THE MAIN STEPS THAT ARE TO BE FOLLOWED IN CYBERCRIME SCENE OF OFFENCE ARE:

- Identification of the scene of offence
- Secure the scene of offence by cordoning it
- Documentation of the scene of offence
- Collection of electronic evidence from the systems
- Examination of witnesses acquainted with the offence
- Documentation of the recovered evidence
- Imaging of the memory devices, if required
- Proper packing, labelling & transportation of the collected material objects.

Besides securing two independent witnesses, the Investigating Officer (IO) while going to the scene of offence shall carry seizure proformas, search warrant, camera, white papers, note book, packing material and portable cyber forensic tools for on-site analysis.

After recovery/seizure of any electronic material objects like hard disks, pen drives, mobile phones or any smart devices, the IO shall not operate them as it alters the time stamps of the material objects which may prove fatal to the prosecution case.



CRIME SCENE SECURITY AND EVALUATION

The investigator should take steps to ensure the safety of all persons at the crime scene and protect the integrity of all evidence, both traditional and electronic. All activities should follow state and local laws. After securing the scene and all persons on the scene, the investigator should visually identify potential evidence (both physical and electronic) and determine if perishable evidence exists. He should then evaluate the scene and formulate a search plan.

SECURE AND EVALUATE THE CRIME SCENE:

The investigator should secure and evaluate the crime scene by—

- Following jurisdictional policy for securing the crime scene. This would include ensuring that all persons are removed from the immediate area where evidence is to be collected. At this point in the investigation, do not alter the condition of any electronic devices. **If it is off, leave it off. If it is on, leave it on.**
- Protecting perishable data (physical and electronic). Perishable data may be found on pagers, caller identification (ID) boxes, electronic organizers, cell phones, and other similar devices. The first responder should always keep in mind that any device containing perishable data should be immediately secured, documented, and/or photographed.
- Identifying telephone lines attached to devices such as modems and caller ID boxes. Document, disconnect, and label each telephone line from the wall rather than the device, when possible. There may also be other communications lines present for local area network (LAN), wide area network (WAN), or other network technologies. Consult the appropriate personnel or agency in these cases.
- Preserving the computer mouse, keyboard, diskettes, compact disks (CDs), or other components that may have latent fingerprints or other physical evidence. Chemicals used in processing latent fingerprints can

damage equipment and data. Therefore, latent prints should be collected after the completion of electronic evidence recovery.

CONDUCT PRELIMINARY INTERVIEWS:

The investigator should conduct preliminary interviews by—



- Separating and identifying all individuals (witnesses, subjects, or others) at the scene and recording their location at the time of entry.
- Being consistent with departmental policy and applicable laws in obtaining information from these individuals, such as—
 - Passwords and user names of owners and/or users of electronic devices found at the crime scene and the Internet service provider (ISP). Obtain any passwords required to access the system, software, or data. An individual may have multiple passwords, such as basic input-output system (BIOS), system login, network ISP, application files, encryption pass phrase, e-mail, access token, scheduler, or contact list.
 - The purpose of the system.
 - Any unique security schemes or destructive devices.
 - Any off-site data storage.
 - Any documentation/manuals explaining the hardware or software installed on the system.

CRIME SCENE DOCUMENTATION:

Documentation of the crime scene creates a permanent historical record of the crime scene. Documentation is an ongoing process throughout the investigation. It is important to accurately record the location and condition of computers, storage media, other electronic devices, and conventional evidence. Moving of a computer system while the system is running may cause changes to system data. Therefore, the system should not be moved until it has been safely powered



down. The initial documentation of the physical crime scene should include—

- Observing and documenting the physical crime scene, such as the position of the mouse and the location of components relative to each other (a mouse on the left side of the computer may indicate a left-handed user).
- Documenting the condition and location of the computer system, including the power status of the computer (on, off, or in sleep mode). Most computers have status lights to indicate that the computer is on. Likewise, if fan noise is heard, the system is probably on. Furthermore, if the computer system is warm, it may also indicate that it is on or was recently turned off.
- Identifying and documenting related electronic components that will not be collected.
- Photographing/videography of the entire scene creates a visual record as noted by the first responder. The complete room should be recorded with 360° coverage, when possible.
- Photographing/videography of the front of the computer, monitor screen, and other components. Take written notes on what appears on the monitor screen. Active programs may require videotaping or more extensive documentation of monitor screen activity.
- Performing additional documentation of the system during the collection phase.

EVIDENCE COLLECTION:

Computer evidence, like all other evidence, must be handled carefully and in a manner that preserves its evidentiary value. This relates not just to the physical integrity of an item or device, but also to the electronic data it contains. Certain types of computer evidence, therefore, require special collection, packaging, and transportation. Consideration should be given to protect data that may be



susceptible to damage or alteration from electromagnetic fields, such as those generated by static electricity, magnets, radio transmitters, and other devices.

Electronic evidence should be collected according to departmental guidelines. In the absence of departmental procedures for electronic evidence collection, use the procedures outlined below.

NONELECTRONIC EVIDENCE COLLECTION:

Recovery of non-electronic evidence can be crucial in the investigation of electronic crimes. Take proper care to ensure that such evidence is recovered and preserved. Items relevant to subsequent examination of electronic evidence may exist in other forms (written passwords and other handwritten notes, blank pads of paper with indented writing, hardware and software manuals, calendars, literature, text or graphical computer printouts, and photographs) and should be secured and preserved for future analysis.

These items are frequently near the computer or related hardware items. All evidence should be identified, secured, and preserved in compliance with departmental procedures.

STAND-ALONE AND LAPTOP COMPUTER EVIDENCE COLLECTION:

Multiple computers may indicate a computer network. Likewise, computers located at businesses are often networked. In these situations, specialized knowledge about the system is required to effectively recover evidence and reduce your potential for civil liability. When a computer network is encountered, contact the forensic computer expert in your department or an outside consultant identified by your department for assistance.

A stand-alone personal computer (PC) is a computer that is not connected to a network or another computer. Standalones may be desktop machines or laptops.

Laptops incorporate a computer, monitor, keyboard, and mouse into a single portable unit. Laptops differ from other computers in that they can be powered by electricity or a battery source. Therefore, they require the removal of the battery in addition to stand-alone, power-down procedures.

If the computer is on, document existing conditions and call your expert or consultant. If an expert or consultant is not available, document all actions taken and any changes observed in the monitor, computer, printer, or other peripherals that result from actions taken. Observe the monitor and determine if it is on, off, or in sleep mode. Then decide which of the following situations applies and follow the steps for that situation.

SITUATION 1: THE MONITOR IS ON AND THE WORK PRODUCT AND/OR DESKTOP ARE VISIBLE.

Step 1 - Photograph the screen and record the information displayed.

Step 2 - Proceed to situation 3, step 3.

SITUATION 2: THE MONITOR IS ON AND THE SCREEN IS BLANK (SLEEP MODE) OR THE SCREENSAVER (PICTURE) IS VISIBLE.

Step 1 - Move the mouse slightly (without pushing buttons). The screen should change and show the work product or request a password.

Step 2 - Do not perform any other keystrokes or mouse operations if mouse movement does not cause a change in the screen.

Step 3 - Photograph the screen and record the information displayed.

Step 4 - Proceed to situation 3, step 3.

SITUATION 3: THE MONITOR IS OFF.

Step 1 - Make a note of the "off" status.

Step 2 - Turn the monitor on, then determine if the monitor status is as described in either situation 1 or 2 above and follow those steps.

Step 3 - Regardless of the power state of the computer (on, off, or sleep mode), **remove the power source cable from the computer, not from the wall outlet.** If dealing with a laptop, in addition to removing the power cord, remove the battery pack. The battery is removed to prevent any power to the system. Some laptops have a second battery in the multipurpose bay instead of a floppy drive or CD drive. Check for this possibility and remove that battery as well.

Step 4 - Check for outside connectivity (telephone modem, cable, integrated services digital network [ISDN], and digital subscriber line [DSL]). If a telephone connection is present, attempt to identify the telephone number.

Step 5 - Avoid damage to potential evidence by removing any floppy disks that are present, packaging the disk separately, and labelling the package. If available, insert either a seizure disk or a blank floppy disk. Do not remove CDs or touch the CD drive.

Step 6 - Place tape over all the drive slots and over the power connector.

Step 7 - Record the **make, model, and serial numbers.**

Step 8 - Photograph and diagram the connections of the computer and the corresponding cables.

Step 9 - Label all connectors and cable ends (including connections to peripheral devices) to allow for exact reassembly later. Label unused connection ports as "unused." Identify laptop computer docking stations to identify other storage media.

Step 10 - Record or log evidence according to departmental procedures.

Step 11 - Package any components as fragile, if transport is required.

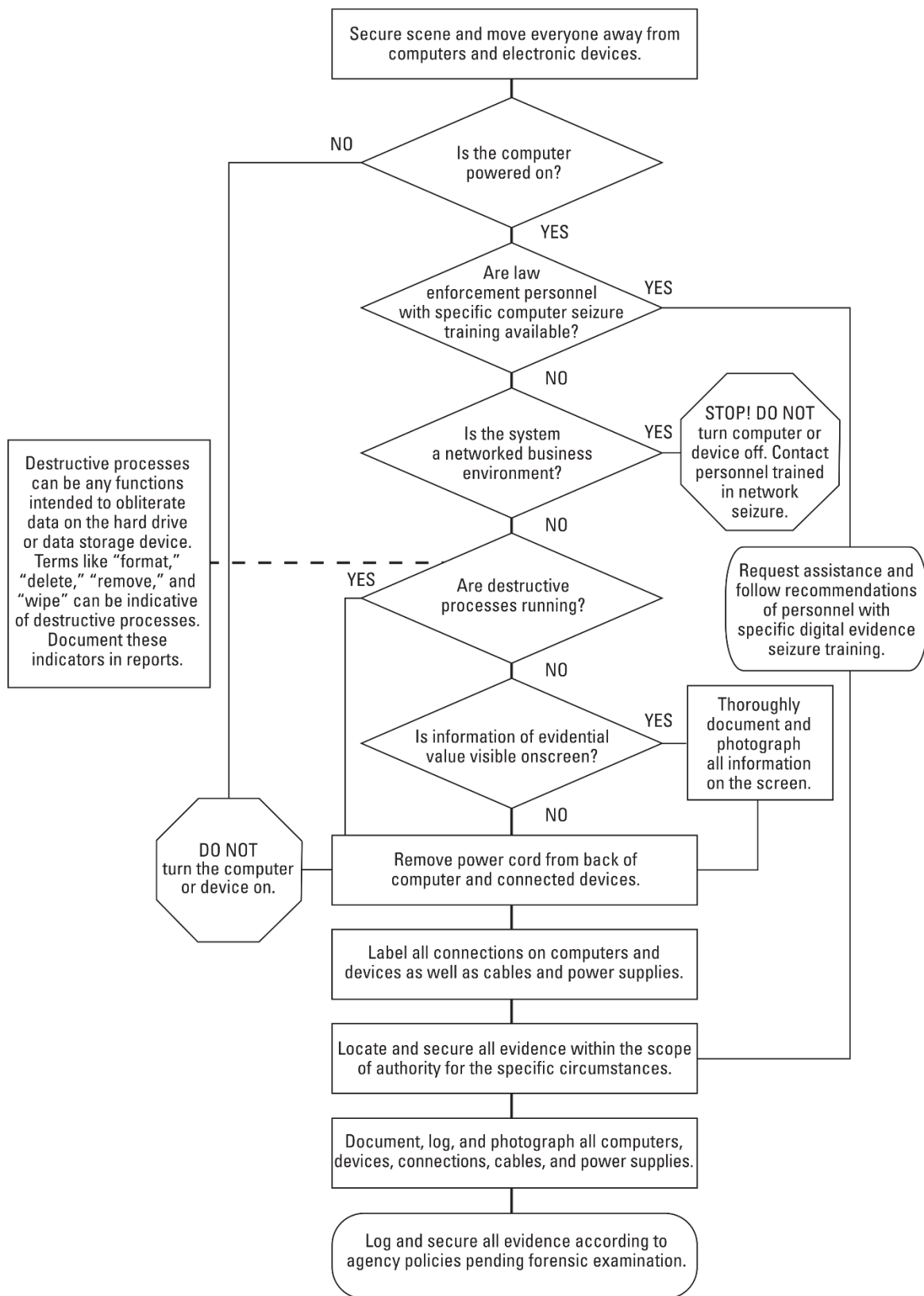


Fig 24. Flow Chart for collecting Electronic Evidence

TOOLS TO BE CARRIED TO SCENE OF CRIME:

In addition to tools for processing crime scenes in general, Investigators should have the following items in their digital evidence collection toolkit:

- Cameras (photo and video) and Cardboard boxes.
- Notepads and Gloves.
- Evidence inventory logs.
- Evidence tapes and Paper evidence bags.
- Evidence stickers, labels, or tags.
- Crime scene tape and Antistatic bags.
- Permanent markers.



Toolkit



Antistatic Covers



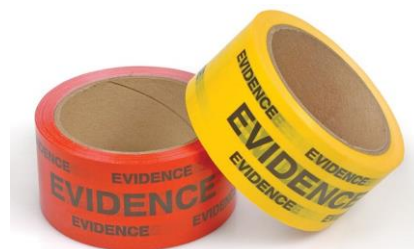
Antistatic Covers



Bubblewrap Covers



Crime Scene Tape



Evidence Tapes

Fig25. Various Tools

FIR No.:	Date:	Date:	Time:
Place of Seizure:		P.S.:	U/s:
Details of the Media:			
Desktop/Laptop:		Assembled/Branded:	
If Branded:			
	Make:	Model:	S/N:
Photography/Videography Done:			
Whether the System is ON/OFF:			
If OFF:			
Details of the Storage Media:			
Make:	Model:	S/N:	Capacity:
Whether Hash Value calculated		Yes/No.:	
Write Blocker Used:			
Forensic Tool Used for Calculating the Hash:			
Type of Hash Algorithm Used: MD5/SHA1/SHA256			
Hash Value:			
If ON:			
Date of the System:		Time of The System:	
Current Date:		Current Time:	
Whether IR/LR Performed:			
Forensic Tool used for IR/LR:			
Details of the RAM dump and its Hash value:			
Name:	Hash Type: MD5/SHA1/SHA256	Hash Value:	
Details of any Unsaved Information Saved before shutting down the System:			
Location of File:		Name of the File:	
After Shutting Down remove the Storage media and note down the details			
Details of the Storage Media:			
Make:	Model:	S/N:	Capacity:
Whether Hash Value calculated: Yes/No			
Write Blocker Used:			
Forensic Tool Used for Calculating the Hash:			
Type of Hash Algorithm Used: MD5/SHA1/SHA256			
Hash Value:			
Signatures with Date and Time:			
Investigator	Technician	Accused	Witness

* * *

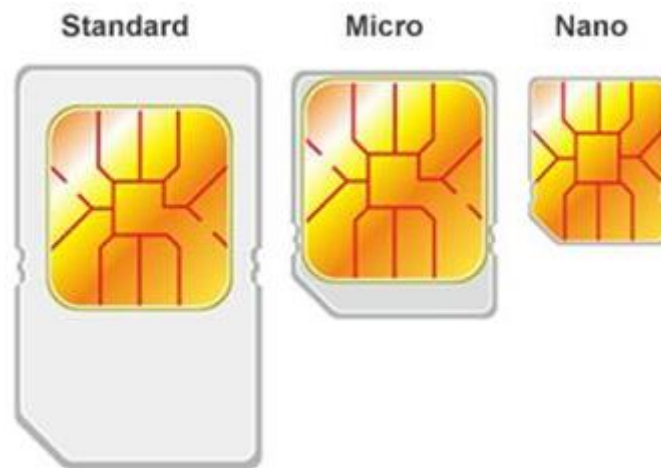
SIM CARD INVESTIGATION

A smart card, also known as an Integrated Circuit Card (ICC), is a micro-controller-based access module. It is a physical/logical entity and can be either a Subscriber Identity Module (SIM) or a Universal Integrated Circuit Card (UICC). Originally, the ICC defined for 2G networks was the SIM. In 3G networks, the SIM may also be a logical entity (application) on a 3G UICC thereby making it functionally the same as a 2G SIM. The Universal Subscriber Identity Module (USIM) is a logical application running on a UICC smart card, which normally only accepts 3G Universal Mobile Telecommunications Service (UMTS) commands. A USIM can have multiple phone numbers assigned to it, thus allowing one phone to have multiple numbers. If the USIM and SIM applications reside on the same UICC, they cannot be active at the same time.

SIM Technology and Functionality:

Subscriber Identity Module (SIM)s are found in GSM, iDEN, and Blackberry handsets and are also used by satellite phone networks such as Iridium, Thuraya, and Inmarsat. Under the GSM framework, a cell phone is termed a Mobile Station, consisting of a SIM card and a handset (Mobile Equipment–ME). One very important and functional feature of a SIM card is that it can be moved from one GSM compatible phone to another, thereby transferring all the subscriber's information.

The first SIM cards were about the size of a credit card. As cell phones began to shrink in size, the mini-SIM (about one-third the size of a credit card) was developed. Today an even smaller version, the micro-SIM, is available. Each of these three iterations varies in physical size and the functionality supported. Normally, a SIM card provides functionality for both the identification and authentication of the subscriber's phone to its network; contains storage for phone numbers, SMS, and other information; and allows for the creation of applications on the card itself.



Security in SIM:

SIM cards have built-in security features. The three file types, MF, DF, and EF contain the security attributes. These security features filter every execution and allow only those with proper authorization to access the requested functionality. There is different level of access conditions in DF and EF files. They are:

- Always—This condition allows to access files without any restrictions.
- Card holder verification 1 (CHV1)—This condition allows access to files after successful verification of the user’s PIN or if PIN verification is disabled.
- Card holder verification 2 (CHV2)—This condition allows access to files after successful verification of the user’s PIN2 or if the PIN2 verification is disabled.
- Administrative (ADM)—The card issuer who provides SIM to the subscriber can access only after prescribed requirements for administrative access are fulfilled.
- Never (NEV)—Access of the file over the SIM/ME interface is forbidden.

Data of Investigative Value from SIM Card:

Depending upon the phone's technology and access scheme, the same data, such as a contact list, may be stored on the SIM, in the handset, or on the phone's memory card. SIM cards themselves contain a repository of data and information, some of which is listed below:

- Integrated Circuit Card Identifier (ICCID):

Every SIM card is uniquely identified by its Integrated Circuit Card ID (ICCID) which is comprised of either nineteen or twenty digits. It is normally printed on the SIM card itself. The numbering of ICCIDs is based upon ITU-T recommendation E.118. A nineteen-digit ICCID includes the Issuer Identification Number (IIN), the Individual Account Identification, and a single "Check Digit" that is used for error detection. Twenty-digit ICCIDs have an additional "Checksum" digit.

- International Mobile Subscriber Identity (IMSI):

The International Mobile Subscriber Identity (IMSI) is a fifteen-digit code that is used to uniquely identify an individual subscriber on a GSM network. It is stored in the EF(IMSI). IMSI conforms to ITU E.212 and consists of three components, the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Mobile Subscriber Identity Number (MSIN). An example of interpreting a hypothetical fifteen-digit IMSI (302 720 123456789) is shown below:

- MCC - the first three digits identify the country. "404" refers to India.
- MNC- the next two digits (European Standard) or three digits (North American Standard) identify the operator. "720" refers to Rogers Communications.
- MSIN - the next nine digits "123456789," identifies the mobile unit within a carrier's GSM network.

- Service Provider Name (SPN)
 - Mobile Country Code (MCC)
 - Mobile Network Code (MNC)
 - Mobile Subscriber Identification Number (MSIN)
- Mobile Station International Subscriber Directory Number (MSISDN):

More than one definition exists for MSISDN. The most common is Mobile Subscriber Integrated Services Digital Network Number. Another definition is Mobile Station International Subscriber Directory Number. The MSISDN can be thought of as a SIM card's unique telephone number (i.e., the telephone number of the GSM phone). It is stored in the EF(MSISDN). The MSISDN numbering format conforms to ITU-T E.164 and consists of three components, a Country Code (CC), the National Destination Code (NDC), and the Subscriber Number (SN). An example of the MSISDN format is shown below:

 - CC: can be up to 3 digits.
 - NDC: usually 2 or 3 digits.
 - SN: can be up to a maximum 10 digits.
 - Together, the MSISDN and IMSI are used to identify the mobile subscriber. While an IMSI is uniquely associated with a SIM, a SIM can have different MSISDNs associated with it. Also, the MSISDN is an optional EF and it can be updated by the subscriber.
- Abbreviated Dialling Numbers (ADN)
 - Last Dialed Numbers (LDN)
 - Short Message Service (SMS)
 - Language Preference (LP)
 - Card Holder Verification (CHV1) and (CHV2)
 - Ciphering Key (Kc)
 - Ciphering Key Sequence Number
 - Emergency Call Code

- Fixed Dialling Numbers (FDN)
- Local Area Identity (LAI)
- Own Dialling Number
- Temporary Mobile Subscriber Identity (TMSI)
- Routing Area Identifier (RIA) network code
- Service Dialling Numbers (SDNs)

INFORMATION THAT RESIDES ON MOBILE DEVICES (a non-exhaustive list):

- Incoming, outgoing, missed call history
- Phonebook or contact lists
- SMS text, application based, and multimedia messaging content
- Pictures, videos, and audio files and sometimes voicemail messages
- Internet browsing history, content, cookies, search history, analytics information
- To-do lists, notes, calendar entries, ringtones
- Documents, spreadsheets, presentation files and other user-created data
- Passwords, passcodes, swipe codes, user account credentials
- Historical geolocation data, cell phone tower related location data, Wi-Fi connection information
- User dictionary content
- Data from various installed apps
- System files, usage logs, error messages
- Deleted data from all the above.

Steps in the Mobile Forensics Seizure

Process:

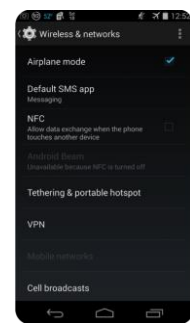
There are two major risks concerning this phase of the mobile forensic process: Lock activation (by user/suspect/inadvertent third party) and Network / Cellular connection.

Network isolation is always advisable, and it could be achieved either through 1) Airplane Mode + Disabling Wi-Fi and Hotspots, or 2) Cloning the device SIM card.



Airplane Mode:

Mobile devices are often seized switched on; and since the purpose of their confiscation is to preserve evidence, the best way to transport them is to attempt to keep them turned on to avoid a shutdown, which would inevitably alter files.



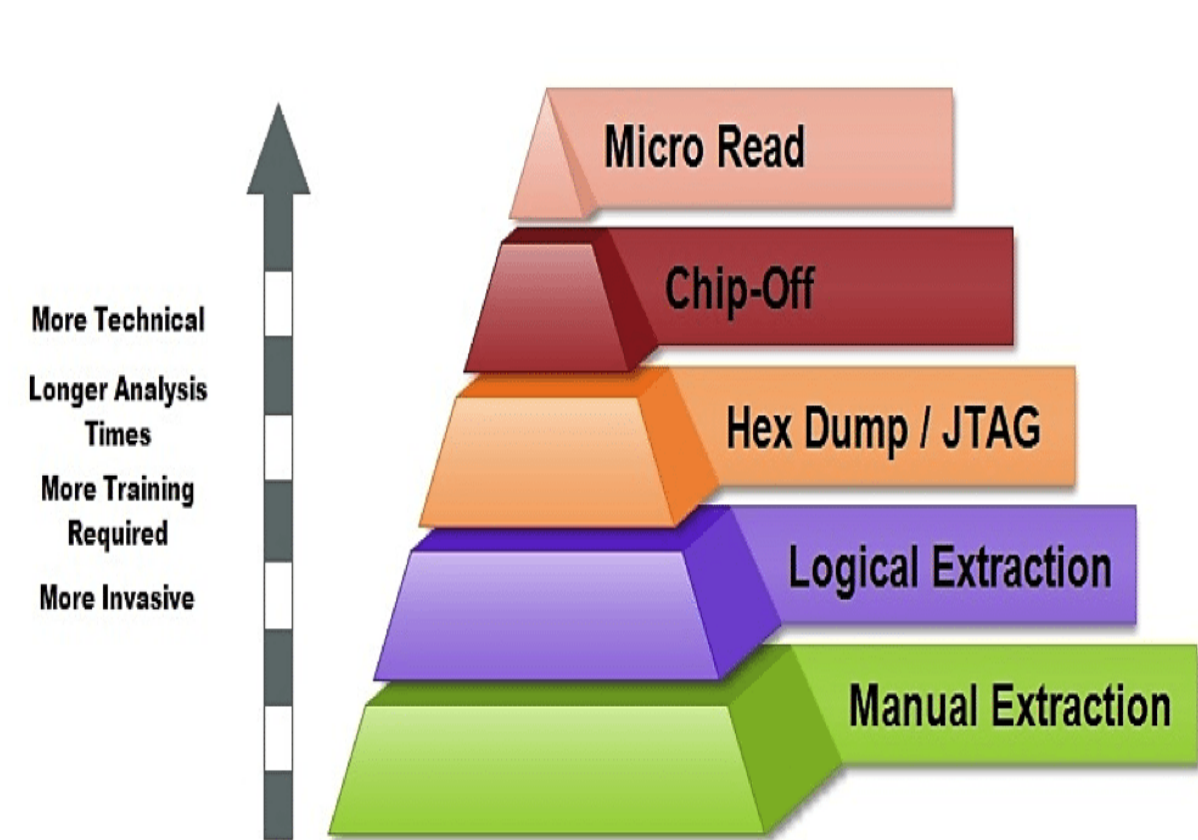
Phone Jammer:

A Faraday box/bag and external power supply are common types of equipment for conducting mobile forensics. While the former is a container specifically designed to isolate mobile devices from network communications and, at the same time, help with the safe transportation of evidence to the laboratory, the latter, is a power source embedded inside the Faraday box/bag. Before putting the phone in the Faraday bag, disconnect it from the network, disable all network connections (Wi-Fi, GPS, Hotspots, etc.), and activate the flight mode to protect the integrity of the evidence.



Faraday bag:

Finally, investigators should beware of mobile devices being connected to unknown incendiary devices, as well as any other booby trap set up to cause bodily harm or death to anyone at the crime scene. The various stages of analysis levels for Mobile Phones is shown in the below fig.



SUGGESTED PROCEDURE FOR SEARCH AND SEIZURE OF MOBILE PHONES:

- If OFF
 - Remove the back cover
 - Note Device details
 - Manufacturer
 - Model
 - UID(IMEI/ESN/SI.No.)
 - Locate the SIM(s)
 - Note the service Provider details and ICC ID if available.
(never try to find the Service provider/subscriber details via making a missed call).
 - Locate expandable memory i.e., Micro SD, MMC, Mini SD etc.,
 - Note the details via FOUR parameters:
 - Make
 - Model
 - S/N
 - Capacity
 - Place back the SIM(s) and Expandable Memory to their original location, place Battery and close the back cover.
 - Switch ON the Device by placing inside a Faraday bag/Faraday Cage only.
 - If a Faraday bag/Faraday Cage not available put the phone into flight mode by removing the SIM(s) if the feature is supported.
 - Other wise not to switch on the phone.
 - For protecting the Location information and to isolate the device from Network.
 - If the device opens normally, Key in the string ***#06#** to get the UID (IMEI/ESN)
 - Cross check the UIDs

- Printed vs Electronically stored: indication of Device Cloning
- If security credentials are required while switching on the phone.
 - a PIN or Password is requested, try to get it from the original user of the phone.
 - For SIM
 - PIN
 - For Phone
 - Passcode/PIN
 - Password
 - Pattern Lock
 - Biometric Lock
 - Figure Print Lock
 - Face Lock
 - Voice Lock
 - For PIN of SIM
 - not to worry PUK can be obtained from the service provider
 - For Password
 - Try to disable the security settings of the Phone with valid security credential. (while doing so try only with the credentials provided by the actual user, if available, for 02 times).

➤ If ON

- Key in the string ***#06#** to get the UID
- Check Security Credential:
 - For SIM
 - PIN
 - For Phone
 - Passcode/PIN
 - Password
 - Pattern Lock
 - Biometric Lock
 - Figure Print Lock
 - Face Lock
 - Voice Lock
 - Once again for PIN no worry service provider is at our rescue with PUK
 - Issue with security credential for Phone.
 - Try to disable the security settings of the Phone with valid security credential. (while doing so try only with the credentials provided by the actual user, if available, for 02 times).
- Switch off the Device.
- Remove the back cover
 - Note Device details Printed
 - Manufacturer
 - Model
 - UID (IMEI/ESN/SI.No.)
 - Cross check the UIDs
 - Printed vs Electronically stored: indication of Device Cloning
 - Locate the SIM(s)
 - Note the service Provider details, ICC ID if available. (**Never try to find the Service**

provider/subscriber details via making a missed call).

- Locate expandable memory i.e., Micro SD, MMC, Mini SD etc.,
 - Note the details via FOUR parameters:
 - Make
 - Model
 - S/N
 - Capacity
 - Place the SIM(s) and the expandable memory back to their original location, place the battery back and close the back cover.

Packing of the Mobile phones:

- Three-layer Packing is the best suggested one.
 - First layer – Antistatic Anti electromagnetic cover.
 - Second layer – a cushioning material like thermo coal sheet/bubble wrap cover.
 - Third layer – paper cover or cloth cover and wax/evidence tape sealing.

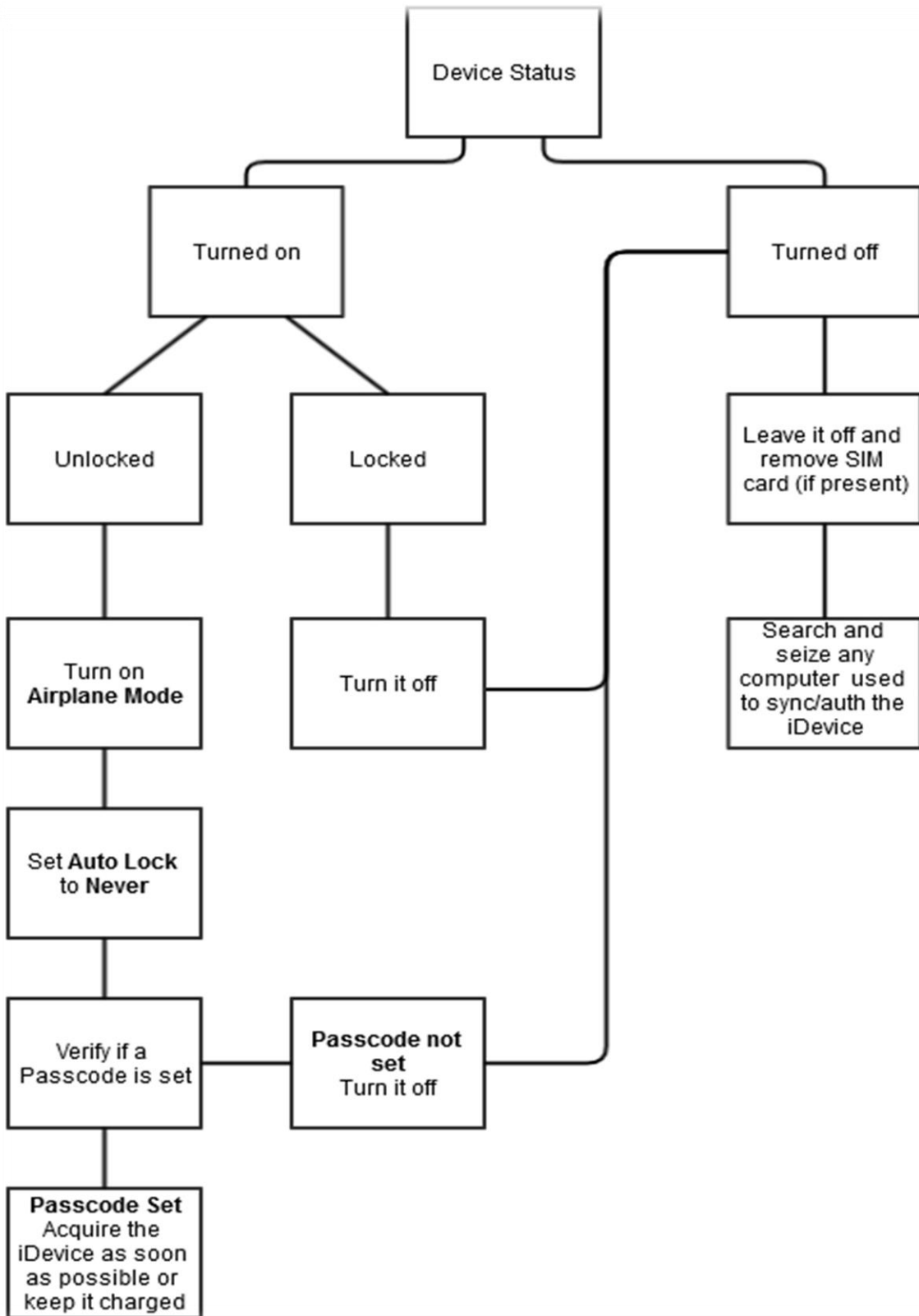


Fig 26. Flow Chart for collecting Mobile Phone Evidence

Model Seizure memo for Mobile Phones:

Case Details

Evidence Item Number _____

Date/Time Seized _____

Primary Offense _____

Device Details

Handheld Device Seized From _____

Handheld Device Owner _____

Manufacturer _____

Model _____

Serial Number (if available) _____

IMEI/ESN _____

Cell Telephone Number (if known) _____

Service Provider (if known) _____

PIN Number _____

SIM Card Number _____

IMSI Number _____

Type of Seizure	Device Status When Seized	Device Secured By	Device Items Recovered	Device Security
Warrant <input type="checkbox"/>	Power off <input type="checkbox"/>	Airplane mode <input type="checkbox"/>	Charger <input type="checkbox"/>	Pin/Password _____
(Attach copy)	Power on <input type="checkbox"/>	Faraday bag <input type="checkbox"/>	Manual <input type="checkbox"/>	
Incident to Arrest <input type="checkbox"/>		Other <input type="checkbox"/> (Explain in notes)	Other <input type="checkbox"/> (Explain in notes)	Pattern lock ● ● ● ● ● ● ● ● ●
Abandoned <input type="checkbox"/>				Other _____
Other <input type="checkbox"/>				
(Explain in notes)				

CCTV/DVR – Basic Understanding:

- DVR-Digital Video Recorder is a surveillance system that records videos in a digital format to hard drive or any mass storage service.
- The cameras in DVR capture images with date, time, location/channel details and is used to record, replay, fast forward videos.
- DVR can relate to PCs for live recording and comes with Graphical User Interface for visual capture management.



Types of CCTV/DVR Systems:

1. Integrated TV-set Digital Video Recorders
2. VESA Compatible Digital Video Recorders
3. PC-Based Digital Video Recorders
4. Over-the-Air Digital Video Recorders
5. Network Attached Storage (NAS) DVR



Fig27. Internal view of a DVR

Points to be noted while collecting CCTV/DVR Systems:

- DVR make, model and number.
- Whether DVR is PC based or Standalone or Networked.
- No. of camera inputs supports.
- No. of recording units installed.
- No. of Active and Inactive cameras.
- Camera Make and Model.
- Is the cameras IR sensitive?
- System date and time.
- Actual date and time.
- Correlation between System and actual date and time.
- Recording capacity of the System and method of overwriting.
- System Password.
- System settings
- Quality of recording i.e., high, medium, low.
- Frames/pictures per second.
- Frame size.
- Details of HDDs. - Make, Model, S/N, Capacity.
- System Firmware version.
- Event logs.
- Playback software name and version.
- Any recent backup of the recordings available?
- Details of any incident of importance, its date and time details.
- Details of Camera Positions.
- Details of native/proprietary file formats the system uses for storing the recordings.

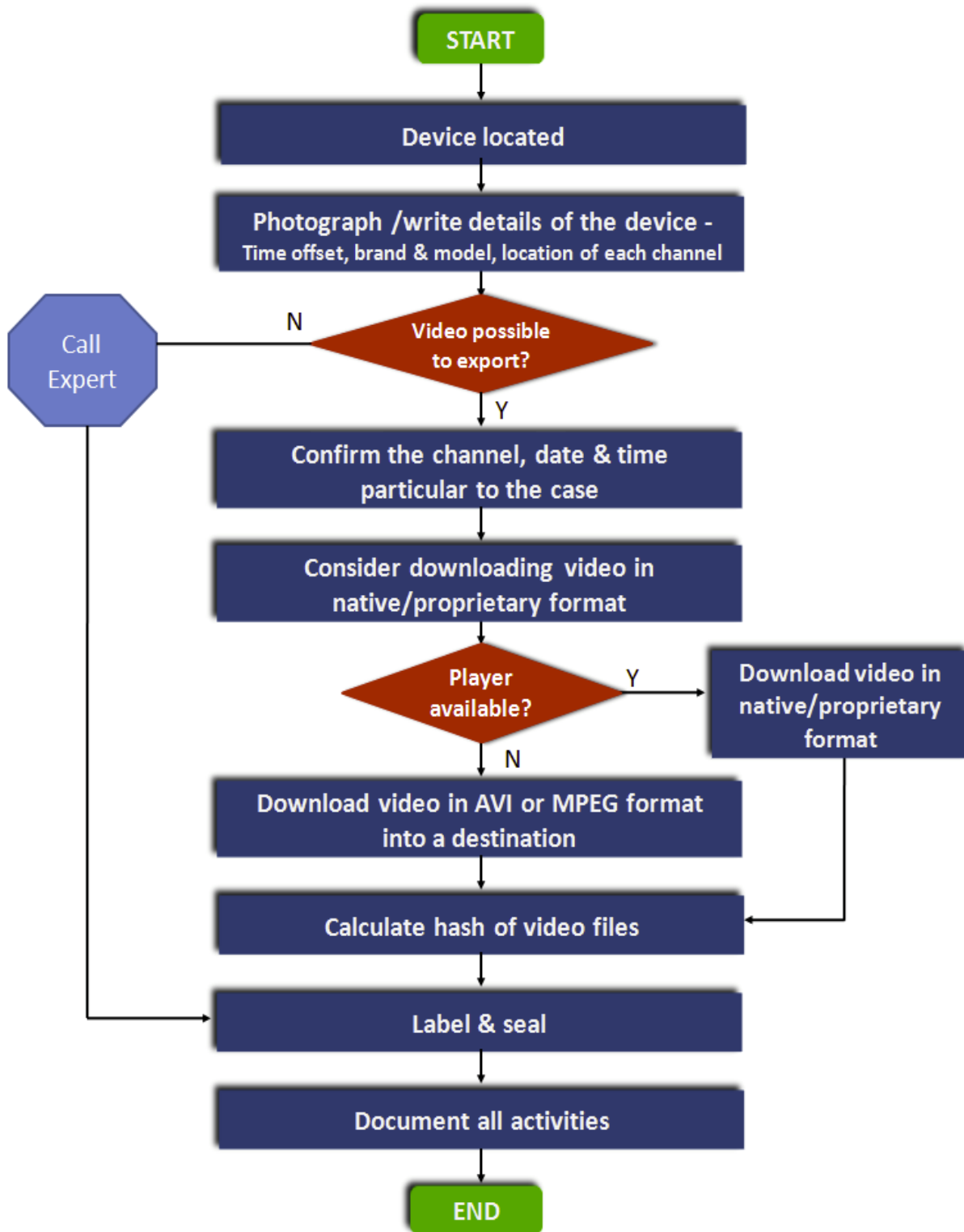


Fig 28. Flow Chart for seizure and retrieval of video footages from CCTV/DVR systems:

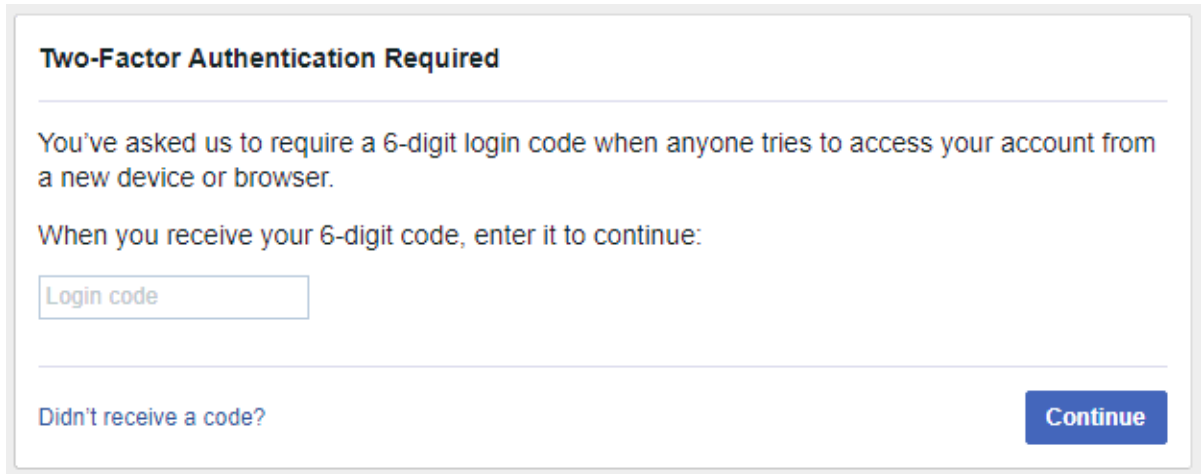
PROCEDURE FOR DOWNLOADING THE FB ACCOUNT

We will now go through the suggestive procedure how to acquire a Facebook account. Of course, you can use commercial tools such as: Cloud Analyzer (Cellebrite), Cloud Extractor (Oxygen Forensics), E3 Platform (Paraben Corporation), etc. However, this can be done manually and, in this article, will show how to do this step-by-step. Documentation as part of panchanama is a must in this procedure.

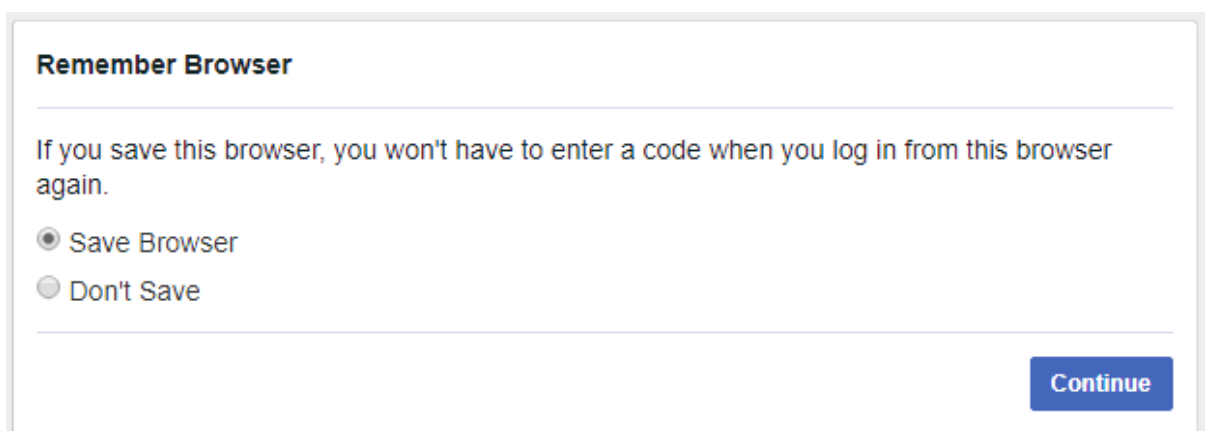
NOTE: This method requires the login credentials of the user.

Open your browser and go to the Facebook page. Enter the Login and Password of the account that you want to acquire, click the Log in button.

If the account has 2 factor authentication, you will see the window in which you will be asked to enter the code sent to the trusted device of the account holder.

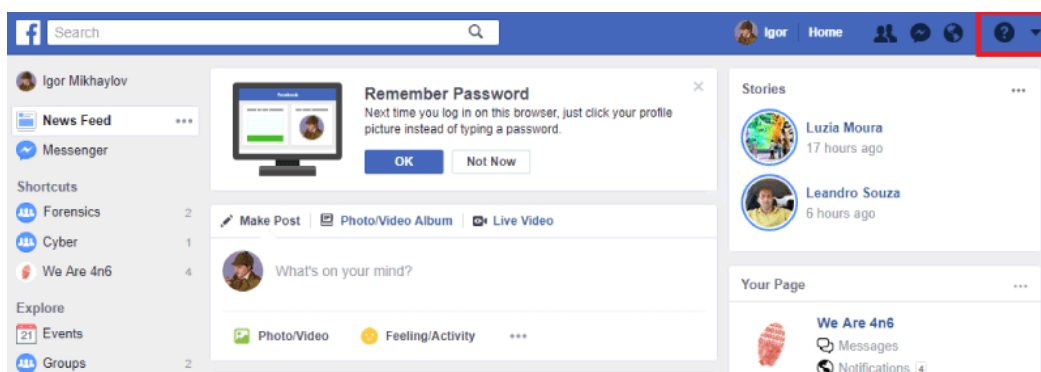


Enter the code and click the Continue button.



In the next window, select 'Save Browser' and click the Continue button.

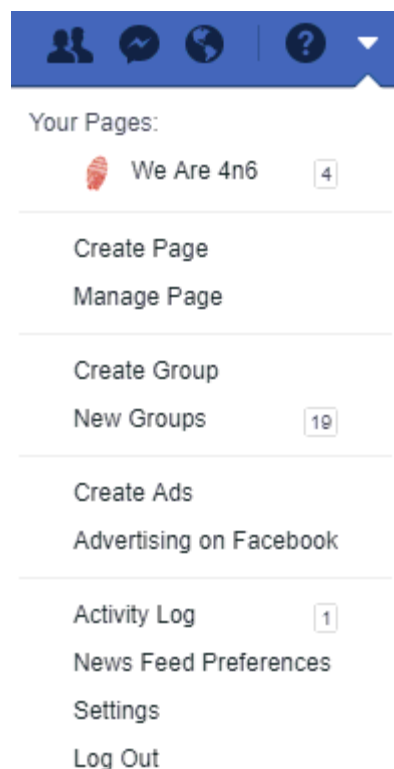
Congratulations! You are currently signed in to this account. Click the triangle located in the upper right corner.



In the menu that opens, select the Settings option.

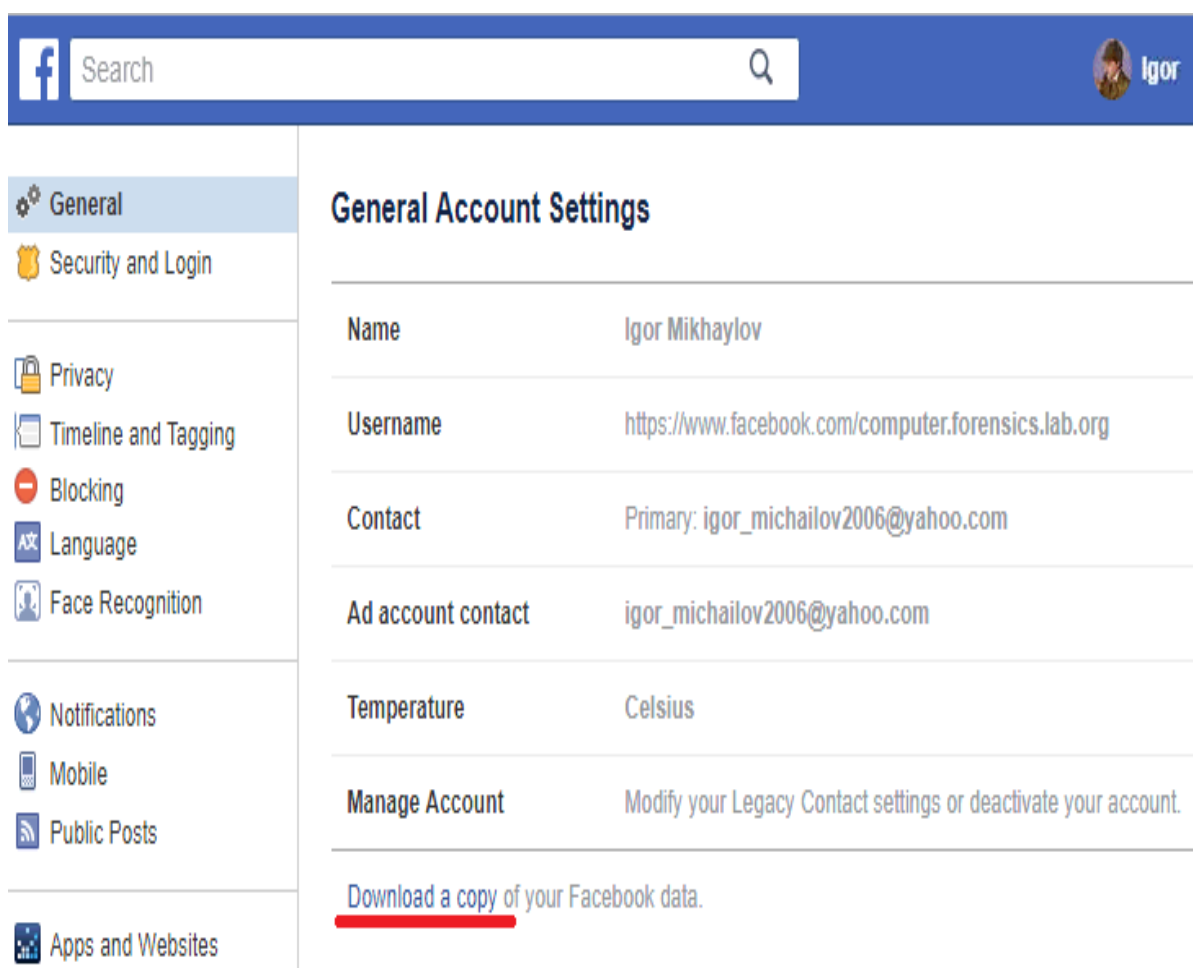
In the 'General Account Settings' window, click Download a copy.

In the next window, click the Start My Archive button.



Facebook navigation menu with icons for Friends, Messages, Events, and Help. Below the icons is a dropdown menu titled 'Your Pages:' containing the following items:

- We Are 4n6 (4)
- Create Page
- Manage Page
- Create Group
- New Groups (19)
- Create Ads
- Advertising on Facebook
- Activity Log (1)
- News Feed Preferences
- Settings
- Log Out



Facebook 'General Account Settings' page. The left sidebar contains the following settings categories:

- General
- Security and Login
- Privacy
- Timeline and Tagging
- Blocking
- Language
- Face Recognition
- Notifications
- Mobile
- Public Posts
- Apps and Websites

The main content area displays the following settings:

Name	Igor Michaylov
Username	https://www.facebook.com/computer.forensics.lab.org
Contact	Primary: igor_michailov2006@yahoo.com
Ad account contact	igor_michailov2006@yahoo.com
Temperature	Celsius
Manage Account	Modify your Legacy Contact settings or deactivate your account.

[Download a copy of your Facebook data.](#)

Download Your Information

Get a copy of what you've shared on Facebook.

Start My Archive



What's included?

- Posts, photos and videos you've shared
- Your messages and chat conversations
- Info from the About section of your profile
- And more

You can access your Facebook data by visiting your Activity Log or by downloading your information, or by simply logging into your account. You can learn more about accessing your Facebook data and what categories of information this includes in our [Help Center](#)

After that you will see a warning window. Click the Start My Archive button.

Request My Download

It may take a little while for us to gather your photos, wall posts, messages, and other information. We will then ask you to verify your identity in order to help protect the security of your account.

Start My Archive

Cancel

After that, two emails will be sent to the Facebook owner's account. The first one explains what data will be copied and how to behave if there is a suspicion that the account was hacked.



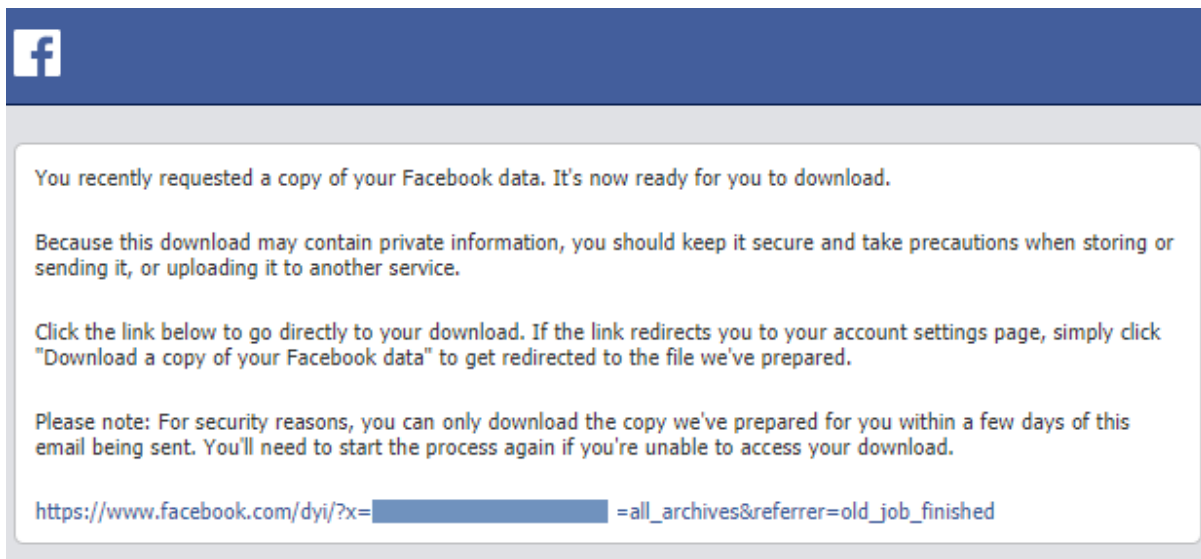
You recently requested a copy of your Facebook data. We'll send you another email with a link to your download when it's ready. For security reasons, the link will only work for a few days after being sent, so please monitor your email for our message. If the link doesn't work by the time you read your email, you'll have to restart the download.

Learn what data may be in your download: <https://www.facebook.com/help/405183566203254>

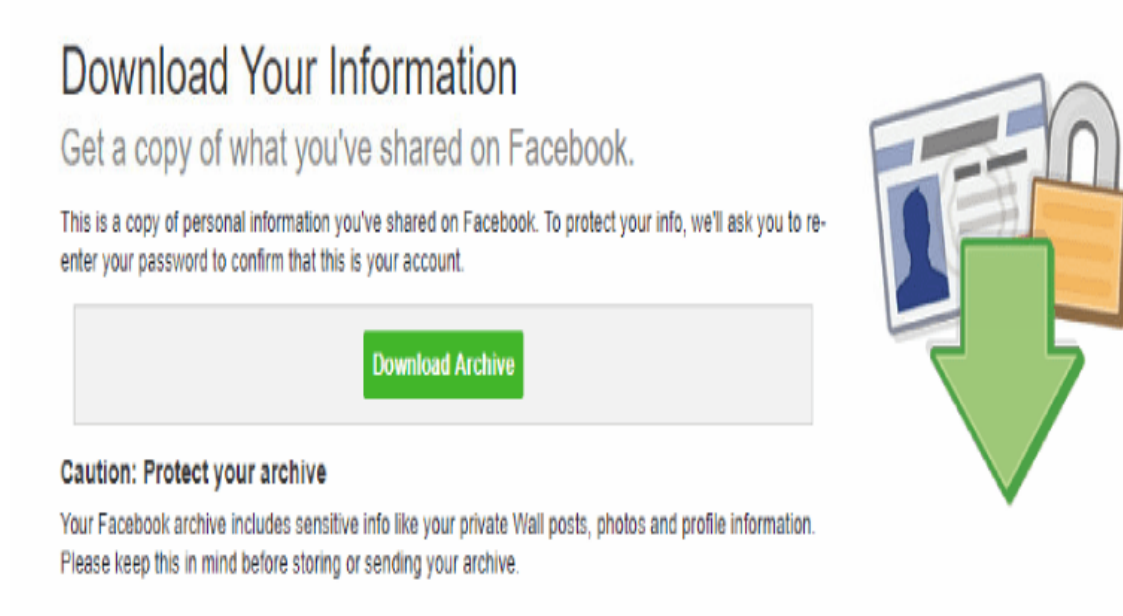
If you didn't request a download of your information, your account may be compromised. Please visit the Help Center to secure it: <https://www.facebook.com/help/203305893040179>

Thanks, The Facebook Team

In the second letter there will be a link to download the archive of this Facebook account.




Copy the link to the browser window and press Enter.
In the window that opens, click the Download Archive button.



Re-enter the password for the account and click Submit.

Please Re-enter Your Password
✕


Igor Mikhaylov

For your security, you must re-enter your password to continue.





Password:

Forgot your password?

Cancel
Submit

After that, the download of the archive of data from this Facebook account will begin.

To view the acquiring data, unpack the archive and double click the index.htm file.

 html			File folder
 messages			File folder
 photos			File folder
 index.htm	4,863	2,267	Chrome HTML

This method of acquiring of the Facebook account is not forensically sound. However, if you do not have expensive cloud forensic tools, or even have these tools but do not have token of the Facebook account, your sequence of actions, when acquiring the Facebook account will not differ much from the sequence described in the article. Besides, Facebook often changes the Facebook API, so some cloud forensic tools may not acquire the Facebook account. The downloaded file/s must be authenticated by third party hashing tools.

GENERAL RULES:

- If the device is off, leave it off.
- If the device is on, consult a Forensic Expert.
- If a Forensic Expert is not available:
 - Photograph the device (screen/display), then disconnect all power sources; unplug from the back of the device. If unable to do so, acquire the device and consult with a specialist as soon as possible.
 - Place tape over areas of access (e.g., drive and media slots).
 - Photograph/diagram and label the back of components with existing connections.
 - Label all connector/cable ends to allow reassembly as needed.
 - If transport is required, package components and transport/store components as fragile cargo.
 - Delays in conducting the examination may result in loss of information.

Last but not the Least:

- If the computer or device is turned off, leave it off.
- Do not try to access devices or data unless you are qualified to do so. If you have to act in an emergency, provide written and, if possible, photo documentation of what was done and why.
- Identify potential sources of evidence/electronic devices and/or storage media.
- Keep everyone away from the target computer, cell phone or storage media.
- Identify who owns/has control of the device or media.
- Determine whether consent has been provided to collect and preserve the computer, cell phone or storage device.
- Determine whether there is remote access to the device.
- Determine whether there is off-site data storage.

- Preserve evidence (Three Layer Packing).
- Gather all software, power cords/adapters, peripheral devices, etc. used to support or power the collected devices and/or media.
- Attain passwords, encryption keys, physical keys, and other security access control devices located at the scene or collected through interviews.
- Determine suspect, victim, or witness knowledge (e.g., system, hardware, software, Internet, email, chat rooms, person or located target, etc.).
- Determine suspect(s) level of access or control of areas and devices.

CRIME SCENE – EVIDENCE PRESERVATION:



➤ **Equipment:**

The following may be included in the Cyber forensic portable field response kit.

1. Digital Camera or video camera and torch light
2. Wiped/sterile removable media (thumb drives, external hard drives)
3. Portable/mini-computer Forensic Workstation with suitable power/data cables.
4. Hardware write blockers or kit
5. Forensic Boot CDs/DVD's
6. Mobile phone acquisition kit with faraday bags.
7. Hardware Toolkit (Screwdrivers etc.)
8. Evidence packing material (Antistatic and bubbled aerated wrappers, evidence tapes, rubber bands, permanent markers, seal proof envelopes etc.)
9. Field Triage Kit (Contains hardware and software necessary for conducting an on-site forensic triage)
10. Chain of custody forms and other documentation material.

➤ **Computers:**

1. The scene should be thoroughly searched for the presence of any network (wired and wireless) devices (routers and hubs)
2. Document all connections to the computer.
3. If the Computer System to be seized / analyzed is connected to a network, it must be isolated from the rest of the network with the help of the system/network administrator or the expert in the area concerned. If the system administrator himself is the suspect in the case, help of another person who has the knowledge about the system, or the network can be sought.

4. Before disconnecting the computer from the network, details such as shared network connections, active network connections etc. should be captured.
5. If the System cannot be taken off the network (Servers) live imaging of the full data/relevant data from the computer should be carried out by using appropriate tools.
6. Document the location of all the computers and/or devices with details such as IP addresses, type of the servers, written/pasted usernames and passwords.
7. Document the programs that are running on the computer system, open files, processes running etc. Save any open documents to the external media. Avoid saving the info into the system drive.
8. Capture Live Memory by taking RAM dumps (several tools are available to capture the RAM contents as a dump on to a USB thumb drive)

IMPORTANT AREAS OF EXAMINATION ON WINDOWS OS

- **Windows Registry Analysis:** Analysis of windows Registry for System and User specific settings such as Computer Name, Operating system installed, Installed date, Network related information such as IP and MAC addresses, USB & other external devices attached, Programs installed and Uninstalled, Recently opened files etc.
- **Recycle bin File Analysis:** Analysis Recycle bin INFO2, \$R&\$I files (Windows Vista, Win7 and Win8) for information related to the files that have been deleted using the Recycle bin. The details such as filenames, sizes and the actual path from where the files have been deleted can be obtained in the analysis.
- **Event log files Analysis:** Windows Event logs record the changes that are made to the system. The files are usually located at path "C:\Windows\System32". Event logs are stored in files "SecEvent, SysEvent, and AppEvent" which can be parsed to identify and analyze the data.
- **Prefetch Files Analysis:** The details about all the applications that are run using the Windows Explorer get documented in Prefetch files (.pf). Prefetch files are located at the path "C:\Windows\Prefetch".
- **Taskbar Jump lists:** Jump lists are a feature in Windows 7 that present the user with the links to recently accessed files grouped on per application basis (Word files, PDF files etc.) Jump lists come as different types of files such as Automatic (autodest, or *.automaticDestination-ms) files and Custom (custdest, or

*.customDestination-ms). The jump lists are located in the user profile path "C:\Users\%USERNAME%\Recent\AppData\Roaming\Microsoft\Windows\Recent\".

- **Sticky notes:** Sticky notes are features in Windows7 operating system that allows the user to create sticky notes on the desktop. Sticky notes are maintained in a single file "Stickynotes.snt" located in the user profile (Userprofile\AppData\Roaming\Microsoft\Sticky Notes) and the file is based on the MS OLE/compound file binary format.
- **Volume shadow copies:** Volume shadow copy service is a feature of windows operating system started with Windows XP. The service created differential backups periodically to create restore points for the user. Mounting and analysis of volume shadow copies gives information about system state at different intervals and information about what files and applications are affected.



▪ **DO'S:**

- Always download e-mail attachments after scanning with Anti-virus
- Always properly log out after completion of online transactions
- Destroy the magnetic strip on the bank card once it expires
- For safe internet banking use virtual keyboards
- Disable auto login facility in your computer
- Always clear the temporary files in your browser after their usage
- Use https:// websites only for online transactions and downloading
- Be careful at public Wi-Fi hotspots
- Use separate Passwords for separate accounts
- Scan the files with anti-virus software after you download it from the Internet
- Enable desktop firewall
- Always scan the USB pen drive and external hard disks before using them
- Always take backup of important files using removable media
- Disconnect computer from the Internet when not in use
- Use different pen-drives for personal and official use
- Disable auto play option while using Pen-drives, CDs, DVDs etc.
- Take care of shoulder surfing
- Keep the number of emails in your mailbox to a bare minimum
- Delete temporary files regularly to avoid remembering personal information
- Connect only to the trusted networks
- Beware while connecting to public networks as they are less secure
- Delete chain mails and junk mails

▪ **DON'TS:**

- Do not disclose sensitive information to others unless they have a business need to know
- Report any suspected unauthorized access of computer systems to your immediate officer
- Never share your personal information to any one on Internet
- Never download files through Chat sessions from unknown persons
- Prevent anonymous users from viewing your profile on Internet
- Never open files with double file extensions such as infor.BMP.EXE or info. TXT.VBS
- Never open web-links in your e-mail. Always type links in Web browser
- Never click links in e-mail which starts with IP address
- Do not pursue links that offer free Anti-virus or Anti-Spyware software
- Do not install unauthorised software programmes on your computer
- Never auto-connect to open Wi-Fi Networks in public places
- Never click 'X' (Cross mark) for closing the browser while you are in online transaction
- Do not use PIN numbers that match your personal information like date of birth, vehicle number, house number etc.
- Do not believe everything which you read online
- Do not give out sensitive information while working on Internet at public places like cyber cafes.
- Do not download any software from non-trusted websites.
- Never leave an email account unattended, if it is logged
- Do not keep sensitive documents on desktop
- Do not forward or reply to Junk mails

1. SOCIAL NETWORKING:

In Internet World, people across the world using social networking sites collect and share information, meet friends.



▪ MAJOR RISKS:

- Online bullying
- Child Abuse
- Disclosure of personal information
- Cyber-Stalking
- Phishing
- Malicious applications
- Access to inappropriate content

▪ TIPS TO AVOID RISKS:

- Put limited information in the Social Networking Sites
- Change default setting
- Give access to only known persons
- Do not click suspicious links
- Install a good and latest version of Anti-virus
- Do not share your password with any one
- Keep changing your password (minimum 8 characters)
- Login into only https sites only
- Use virtual Keyboard, wherever possible

2. PHISHING:

This technique is carried out by sending fake e-mails & redirecting to spoofed websites and prompt the users to enter personal information, which look and feel similar to original sites, but in-fact they are not.



- **DO'S:**
 - Cross check the URL in the browser, don't enter your information that start with numbers
 - Check for the misspelled URL
 - Always perform online banking in secure channel
 - Never respond to e-mails that ask for your credit card/debit card information
 - Be cautious about opening any new attachments
 - Always update your Anti-virus software
 - Use different passwords for different online accounts
- **DON'TS:**
 - Do not open ZIP files unless it is from known source
 - Never run .exe files
 - Do not open any spam e-mail
 - Do not open suspicious images
 - Never respond to phone calls asking for bank details

3.



- Browser is a software which acts as a medium to retrieve content from World Wide Web (WWW) and present us.
- Examples of browser are Google, Mozilla fire fox, Yahoo search etc.
- Always update the browser to new version for safe online activity.
- Browser based attacks – Tab-napping, Clickjacking, Cookie Hijacking
- Open only https:// sites
- Regularly delete browser cookies

- Before doing online transactions close all open browsers, tabs and applications
- Never select remember password option for browser
- Do not click on advertisements which open up in new small window
- Never access Bank websites or any other important websites through search engine generated results

4.



- Wi-Fi is the wireless networking technology that uses radio waves to provide internet to the user
- Through Wi-Fi, we can connect desktop, laptop, mobile phones within the range of Access point
- Always use strong password (minimum 8 characters)
- Change the default username and Password of the Access point
- Shut down the access point when not in use

5. OPERATING SYSTEM HARDENING:

- By hardening the PC we reduce a large number of vulnerabilities which can be exploited by attacker
- OS hardening is the process of securing a system by implementing the latest OS patches, updates and policies to reduce systems and network attacks
- Installing Anti-virus software
- Turn on firewall
- Always ensure that only authorized services are running
- Update all applications regularly



- Protect the system with a strong password
- Take data back periodically
- Change the password regularly
- Disable unused ports

6.



- Your brain is the best place to remember passwords, do not write anywhere
- Change your passwords regularly
- The password should a minimum of 8 characters in length (Alpha-numeric-special characters)
- Use separate Passwords for separate accounts
- Do not keep same password for different accounts
- Never share your passwords with any one like a underwear
- Avoid using dictionary words as passwords
- Do not use your name/family name/birth place/children names as passwords
- Do not save your passwords in files or web browsers
- Never reuse your old password

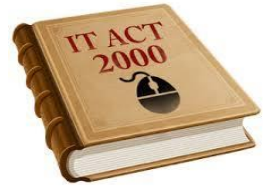
7. DESKTOP SECURITY:

- A computer without proper security measure could lead to exploiting the system for illegal activities
- Always install Licensed Software to get regular updates of Operating System



- Properly shutdown and switch off your personal computer after the use along with external devices like Monitor, Modem, Speakers etc.
- Do not place any magnet near the PC

THE INFORMATION TECHNOLOGY ACT, 2000



The main objective of Information Technology (IT) Act, 2000 is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication.

Some Important sections of IT Act, 2000 are:

Section	Description
43	Penalty and Compensation for damage to Computer System
65	Tampering with Computer source documents
66	Computer related offences
66-A	Punishment for sending offensive messages through communication service (Repealed by the Honourable Supreme Court of India)
66-B	Punishment for dishonestly receiving stolen computer resource or communication device
66-C	Punishment for Identity theft
66-D	Punishment for cheating by personation by using computer resource
66-E	Punishment for violation of privacy
66-F	Punishment for Cyber Terrorism
67	Punishment for publishing or transmitting obscene material in electronic form
67-A	Punishment for publishing or transmitting of material containing sexually explicit act in electronic form
67-B	Punishment for publishing or transmitting of material depicting children in sexually explicit act in electronic form
69-A	Power to issue directions for blocking for public access of any information through any computer resource
72	Breach of confidentiality and privacy

75	Act to apply for offence or contraventions committed outside India
78	A Police Officer not below the rank of Inspector shall investigate any offence under this Act
80	Power of Police Officer and Other Officers to Enter, Search etc.
84-B	Punishment for abetment of offences
84-C	Punishment for attempt to commit offences

SOME USEFUL WEBSITES FOR INVESTIGATION



1. **Trace.bharatiyamobile.com** – to find out Mobile Service Provider, Location and State
2. **www.numberingplans.com** – to find out national/international number, IMEI number and manufacturer details
3. **www.bsnl.co.in** – to find out BSNL land line details
4. **www.whatismyipaddress.com** – to find out IP address of the Computer system
5. **www.pipl.com** – to find out person using e-mail address
6. **www.whois.com** - to find out IP address and domain name
7. **<https://www.tineye.com/>** - Reverse Image Search and can be used to verify whether a photo/image is fake one or genuine one.
8. **<http://blasze.com/>** - for iP Logging.
9. **<https://iplogger.org/>** - for iP Logging.
10. **<https://keyhole.co/>** - for gathering intelligence from hashtags and keywords focussing twitter.
11. **<https://www.echosec.net/>** - for location-based search and discovering the social media activities based on geographical location.
12. **[Maltego](#)** – tool for various OSINT activities.
13. **<https://inteltechniques.com/menu.html>** - for various OSINT activities.



BIOS:

BIOS stands for Basic Input Output System, which is information written in computer code and stored in the ROM so that it is available when the computer is turned on. BIOS information tells the computer how to read information contained on the computer's various drives, and includes the boot strap loader, which is the first code executed when the computer is turned on.

BIT:

This is an abbreviation for binary digit and is the smallest unit of computer data. A bit consists of either 0 or 1. Eight bits make up a byte

BOOT SECTOR:

The very first sector on a hard drive. It contains the codes necessary for the computer to start up. It also contains the partition table, which describes how the hard drive is organized. Also called the Master Boot Record.

BOOT STRAP LOADER:

The first code executed when the computer is turned on.

BYTE:

This is an abbreviation for binary term. A byte is a measurement unit of computer data that consists of a single character. A single byte usually consists of 8 bits.

CARDINAL RULES :

Never work on original evidence.

Never mishandle evidence.
Use proper software utilities.
Never trust the subject operating system.
Document everything.

CLUSTERS :

Clusters are groups of sectors where folders and files are stored on the hard drive.

CLUSTER BITMAPS:

Used in NTFS to keep track of the status (free or used) of clusters on the hard drive.

COMPUTER FORENSICS:

The scientific collection, examination, analysis and presentation of information held on or retrieved from computer storage media in such a way that it can be used as potential legal evidence.

CYLINDER:

The set of tracks on both sides of each platter in the hard drive that are located at the same head position. A cylinder can be visualized as a cross section taken across all the platters of a hard drive at the same head position.

DIGITAL EVIDENCE:

Digital evidence or electronic evidence is any information of probative value i.e. either stored or transmitted in a binary form.

DRIVE GEOMETRY:

A computer hard drive is made up of a number of rapidly rotating platters that have a set of read/write heads on both sides of each platter. Each platter is divided into a series of concentric rings called tracks. Each track

is further divided into sections called sectors, and each sector is sub-divided into bytes. Drive geometry refers to the number and positions of each of these structures.

DISK PARTITION :

A hard drive containing a set of consecutive cylinders. Before files can be stored on a disk partition it must be formatted to create a logical volume.

DRIVER:

A driver is a computer program that controls various devices such as the keyboard, mouse, monitor, etc.

EXTENDED PARTITIONS:

If a computer hard drive has been divided into more than four partitions, extended partitions are created. Under such circumstances each extended partition contains a partition table in the first sector that describes how it is further subdivided.

FAT:

This stands for File Allocation Table. It is used in Windows® to keep track of where the files are stored on a hard drive, which is formatted as a FAT volume or file system.

FILE SLACK :

The unused space on a cluster that exists when the logical file space is less than the physical file space

FILE SYSTEM:

A disk partition organized so that files can be stored on it. In Windows®, a disk partition with a file system on it is called a volume. The most common types of file systems used by Windows® are FAT and NTFS.

FILE SIGNATURE:

Many file types contain a few bytes at the beginning that constitute a unique "signature" of that file type. Most graphic and document file types contain a signature. For example, the first 6 bytes at the beginning of a GIF file are either GIF89A or GIF87A.

FORMAT, FORMATTING, FORMATTED:

Preparation of computer media such as hard drives, floppy disks, CD-ROM disks, etc. so that computers can read and write information to the medium.

FORENSIC IMAGE:

An exact copy of computer's hard disk. Disk imaging takes sector-by-sector copy which includes all the partition information, boot sectors, the file allocation table, operating system installation and application software usually for forensic purposes and as such it will contain some mechanism (internal verification) to prove that the copy is exact and has not been altered.

FRAGMENTED:

In the course of normal computer operations when files are saved, deleted, moved, etc. the files or parts thereof may be scattered in various locations on the computer's hard drive or other storage medium. Regarding computer forensics, fragmented data can frequently yield important evidence. Computer forensics techniques allow technicians to locate and examine fragmented files.

HASH VALUE:

A hash function is a reproducible method of turning data into a small number that may serve as a digital "fingerprint" of the data. The algorithm "chops and mixes" (i.e. substitutes or transposes) the data to create such fingerprints called hash value or simply hash or message digest.

HARD COPY:

A hard copy is a printed copy of information from a computer.

HARD DISK:

A hard disk contains several hard-round platters coated on both sides with a magnetic material designed to store information as binary numbers, magnetic patterns of 0's and 1's. The platters are mounted on a spindle that rotates at high speed, generally 5,000 to 10,000 rpm.

HEAD :

Each platter on a hard drive contains a head for each side of the platter. The heads are devices which ride very closely to the surface of the platter and allow information to be read from and written to the platter. The heads are physically attached to an arm, which is in turn attached to the head stack assembly. Usually all heads move together and are positioned together on the same track.

INTER-PARTITION SPACE:

Unused sectors on a track located between the start of the partition and the partition boot record. This space is important because it is possible for a user to hide information here.

LOGICAL FILE SPACE:

The actual amount of space occupied by a file on a hard drive. The amount of logical file space differs from the physical file space because when a file is created on a computer, a enough clusters (physical file space) are assigned to contain the file. If the file (logical file space) is not large enough to completely fill the assigned clusters (physical file space) then some unused space will exist within the physical file space. This unused space is referred to as file slack and can contain unused space, or previously deleted/overwritten files or fragments thereof.

LOGICAL VOLUME:

An area on the hard drive that has been formatted so that files can be stored there. A hard drive may contain a single or multiple volume. Each volume appears as if it is a single hard drive. In Windows®, the first volume is referred to as "C:", while subsequent letters, such as "D:", "E:", etc., may refer to additional volumes or may identify devices such as a CD-ROM drive.

MASTER BOOT RECORD:

The very first sector on a hard drive. It contains the codes necessary for the computer to start up. It also contains the partition table, which describes how the hard drive is organized. Also called the Boot Sector.

MEDIA:

Media refers to various types of devices used for data storage, such as hard drives, floppy disks, CD-ROM disks, etc.

META DATA :

Refers to small bits of information stored by some computer programs such as Microsoft Word®. Meta data can contain the history of the document, including all users who have modified and/or saved it, the directory structure of all machines it was saved on, and names of printers it was printed on.

MD5 HASH VALUE:

MD5 hash is a 128-bit (16 byte) number that uniquely describes the contents of the file. It is used to create digital signature. MD5 is a one-way hash function, it takes a message and converts it into a fixed string of digits called message digest.

MIRROR IMAGE:

A bit-by-bit copy of a computer hard drive that ensures the operating system is not altered during the forensic examination.

NTFS:

Stands for New Technology File System. This is a newer type of computer file system that was developed for use by Windows NT®, Windows 2000®, and Windows XP®.

PAGE OR PAGING FILE:

A file used to temporarily store code and data for programs that are currently running. This information is left in the swap file after the programs are terminated and may be retrieved using forensic techniques. Also referred to as a swap file.

PARTIAL FILE:

When a user deletes information from a computer, the data is not actually erased. Instead, the space the data occupied is marked as available for reuse. If new data is stored in that location but does not occupy as much storage space as the old data, the result is a partial file, which still contains bits of the old data. This old data can be examined using forensic techniques.

PARTITION :

A partition is an individual section of computer storage media such as a hard drive. For example, a single hard drive may be divided into several partitions. When a hard drive is divided into partitions, each partition is designated by a separate drive letter, i.e., C, D, etc.

PARTITION TABLE:

The partition table indicates each logical volume contained on a disk and its location.

PARTITION WASTE SPACE:

After the boot sector of each volume or partition is written to a track, it is customary for the system to skip the rest of that track and begin the actual

useable area of the volume on the next track. This results in unused or "wasted" space on that track where information can be hidden. This "wasted space" can only be viewed with a low-level disk viewer. However, forensic techniques can be used to search these "wasted space" areas for hidden information.

PHYSICAL DISK:

An actual piece of computer media, such as the hard disk or drive, floppy disks, CD-ROM disks, Zip disks, etc.

PHYSICAL FILE SPACE:

When a file is created on a computer, an enough cluster (physical file space) are assigned to contain the file. If the file (logical file space) is not large enough to completely fill the assigned clusters (physical file space) then some unused space will exist within the physical file space. This unused space is referred to as file slack and can contain unused space, previously deleted/overwritten files or fragments thereof.

PLATTER:

One of several components that make up a computer hard drive. Platters are thin, rapidly rotating disks that have a set of read/write heads on both sides of each platter. Each platter is divided into a series of concentric rings called tracks. Each track is further divided into sections called sectors, and each sector is sub-divided into bytes.

RAM:

Stands for Random Access Memory -- the area on the computer where the operating system (i.e. Windows®), programs and drivers are loaded when the computer is started up. The content of a computer's RAM is lost each time the computer is turned off.

RAM SLACK :

The space from the end of the file to the end of the containing sector is called RAM slack. Before a sector is written to disk, it is stored in a buffer somewhere in RAM. If the buffer is only partially filled with information before being committed to disk, remnants from the end of the buffer will be written to disk. In this way, information that was never saved can be found in RAM slack on disk.

ROM:

Stands for Read Only Memory; this is a chip within the computer where a permanent program is stored that contains the necessary information for starting up the computer. Information in the computer's ROM is permanently maintained even when the computer is turned off.

SECTOR:

A group of bytes on any given track of a hard drive's platters and the smallest area of information that can be accessed on the drive. Sectors are numbered sequentially starting with 1 on each individual track. Thus, Track 0, Sector 1 and Track 5, Sector 1 refer to different sectors on the same hard drive. Usually, drives have sectors that contain 512 bytes each.

SLACK SPACE:

The unused space on a cluster that exists when the logical file space is less than the physical file space. Also known as file slack.

SOFT COPY :

An exact copy of computer's hard disk. Disk imaging takes sector-by-sector copy which includes all the partition information, boot sectors, the file allocation table, operating system

STERILE MEDIA:

Storage media that does not contain any data.

STORAGE MEDIA:

Objects on which data can be stored. These include hard disks, floppy disks, CD-ROMs and tapes.

SWAP FILE :

A file used to temporarily store code and data for programs that are currently running. This information is left in the swap file after the programs are terminated and may be retrieved using forensic techniques. Also referred to as a page file or paging file.

TEMPORARY FILE:

Temporary files are files stored on a computer for temporary use only and are most commonly created by Internet browsers. These "temp" files store information about Web sites that a user has visited and allows for more rapid display of the Web page when the user revisits the site. Forensic techniques can be used to track the history of a computer's Internet usage through the examination of these temporary files.

TRACK:

Each of the series of concentric rings contained on a hard drive platter.

UNALLOCATED SPACE:

The area of computer media, such as a hard drive, that does not contain normally accessible data. Unallocated space is usually the result of a file being deleted. When a file is deleted, it is not actually erased, but is simply no longer accessible through normal means. The space that it occupied becomes unallocated space, i.e., space on the drive that can be reused to store new information. Until portions of the unallocated space are used for new data storage, in most instances, the old data remains and can be retrieved using forensic techniques.

VOLUME:

A volume is a specific amount of storage space on computer storage media such as hard drives, floppy disks, CD-ROM disks, etc. In some instances, computer media may contain more than one volume, while in other cases; one volume may be contained on more than one disk.

VOLUME BOOT SECTOR:

When a partition is formatted to create a volume, a volume boot sector is created to store information about the volume. One volume contains the operating system and its volume boot sector contains code used to load the operating system when the computer is booted up.

VOLUME SLACK:

On a formatted volume, there are a certain number of available sectors. These sectors are grouped together in clusters or blocks depending on the file system. If the number of possible clusters does not divide evenly into the number of available sectors, there will be some sectors left over at the end of the partition. These sectors are not used to store file/folder information by the file system. This wasted space is known as volume slack and is usually less than the size of a cluster/block. Deleted files, hidden data and remnants of previous partitions could possibly be found in the volume slack.

GLOSSARY FOR MOBILE PHONES

CDMA:

Digital cellular technology that uses spread-spectrum techniques. Unlike competing systems, such as GSM, that use TDMA, CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum. Individual conversations are encoded with a pseudo-random digital sequence. CDMA consistently provides better capacity for voice and data communications than other commercial mobile technologies, allowing more subscribers to connect at any given time, and it is the common platform on which 3G technologies are built.

3G(Third Generation):

3G enabled phones can browse the Internet, receiving and sending email, live video streaming, and much more. High data speeds characterize this technology and turn your phone into a powerful tool for accessing online and mobile content. There are several different 3G technology standards. The most prevalent is UMTS, which is based on WCDMA

DELETED SMS:

These are text messages that have been deleted from the SIM card by the cell phone user. However, most mobile phones do not remove the message, but mark the message to be overwritten by incoming messages from the network.

BLUE TOOTH:

An ad-hoc wireless communication standard built into the majority of new mobile phones. In its most common form, Bluetooth provides direct communication between devices to a range of approximately 10 meters.

EMS:

An EMS enabled mobile phone can send and receive messages that have special text formatting (such as bold or italic), animations, pictures, icons, sound effects and special ring tones. EMS messages that are sent to devices that do not support it will be displayed as SMS transmissions.

IMEI:

A unique 15-digit number that serves as the serial number of the GSM handset. The IMEI appears on the label located on the back of the phone. The IMEI is automatically transmitted by the phone when the network asks for it. A network operator might request the IMEI to determine if a device is in disrepair, stolen or to gather statistics on fraud or faults.

IMSI:

IMSI is a unique number associated with all GSM and Universal Mobile Telecommunications System (UMTS) network mobile phone users. It is stored in the Subscriber Identity Module (SIM) inside the phone and is sent by the phone to the network. It is also used to acquire other details of the mobile in the Home Location Register (HLR) or as locally copied in the Visitor Location Register.

SIM:

The Subscriber Identification Module or Subscriber Identity Module C a "smart card" - holds all a subscriber's personal information and phone settings. It is the subscriber's authorization to use the network. It is the chip inside a GSM phone with the information such as the phone number, personal security key and other data necessary for the handset to function. The card can be switched from phone to phone, letting the new phone receive all calls to the subscriber's number.

ESN:

An electronic serial number (ESN) is the unique identification number embedded or inscribed on the microchip in a wireless phone by the manufacturer. Each time a call is placed, the ESN is automatically transmitted to the base station so the wireless carrier's mobile switching office can check the call's validity. The ESN cannot easily be altered in the field. The ESN differs from the mobile identification number, which is the wireless carrier's identifier for a phone in the network

SMS:

A messaging service, originally implemented for use in GSM networks, which enables short text messages to be sent between subscribers.

PIN:

A number which must be given to a mobile phone / SIM card before it will allow access to its features and/or connect to the network.

PUK (Pin Unlock Code):

A number which unlocks a SIM card if the incorrect SIM PIN is entered three times in succession. The PUK is stored by the service provider.

PDU (Protocol Data Unit):

A standard used by mobile phones in a GSM network for storing and sending SMS messages.

Mega Pixel:

Phones with mega pixel cameras typically produce much better-quality photos than VGA. The higher the number of mega pixels, the better the quality of photos. In some cases, camera phones with up to 2.0 mega pixels can produce photos as good as a standard digital camera.

MMS :

A messaging service like SMS which enables messages comprising of images, audio and/or video to be sent over a wireless communication network

MP3:

A popular digital audio encoding and compression format designed to greatly reduce the amount of data required to represent audio, yet still sound like a faithful reproduction of the original uncompressed audio to most listeners. In popular usage, MP3 also refers to files of sound or music recordings stored in the MP3 format on computers.

GPS:

Global Positioning System is a system where a receiver can capture signals from the orbiting satellites which permit it to determine the time very precisely, and its location very precisely.

GSM:

GSM is a digital cellular phone technology based on TDMA that is the predominant system Europe, the Middle East, Africa, Asia and in parts of America and Canada. First introduced in 1991, the GSM standard has been deployed at three different frequency bands: 900 MHz, 1800 MHz and 1900 MHz GSM 1900 is primarily deployed in North America. Named after its frequency band around 900 MHz, GSM-900 has provided the basis for several other networks using GSM technology. GSM uses narrowband TDMA which allows eight simultaneous calls on the same radio frequency. Along with CDMA and TDMA it represents the second generation of wireless networks.

IrDA:

A group of device manufacturers that developed a standard for transmitting data via infrared light waves. This enables you to transfer data from one device to another without any cables.

ICCID:

Integrated Circuit Card Id is a 19 or 20-digit serial number of the SIM card.

MCC:

Mobile Country Code – a part of the IMSE number which states which mobile network provider SIM card is registered to.

USIM:

Universal Subscriber Identity Module – An application running on a smartcard and which is issued by the network operator. Supports speeds between 384 Kb and 2 Mb.

MSISDN:

MSISDN (Mobile Subscriber Integrated Services Digital Network) is a number uniquely identifying a subscription in a GSM or UMTS mobile network. The MSISDN together with IMSI is two important numbers used to identify a mobile phone. MSISDN is the number normally dialled to connect a call to the mobile phone.

TDMA (Time Division Multiple Access):

TDMA is a technology used in digital cellular telephone communication that divides each cellular channel into three time slots in order to increase the amount of data that can be carried.

PLMN (Public Land Mobile Network) :

A Public Land Mobile Network area is the geographical area in which a PLMN operator provides land mobile communication services to the public. From

any position within a PLMN area, the mobile user can set up calls to another user of the same network, or to a user of another network. The other network may be a fixed network, another GSM PLMN, or another type of PLMN. Other network users, and users of other networks, can also call a mobile user who is active in the PLMN area. When there are several PLMN operators, the geographical areas covered by their networks may overlap. National borders normally limit the extent of a PLMN area.

WAP:

Wireless Application Protocol. An agreed standard which enables WAP-compatible mobile phones to access Internet-type services (such as news, travel, entertainment, finance, sport etc.) via their menu system and LCD screens.

WCDMA:

Wideband CDMA: Technology for wideband wireless access supporting 3G cell phone services, and allows very high-speed multimedia services like internet access and videoconferencing

WLAN:

Sometimes known as Wi-Fi, this technology gives mobile phones, laptops and other wireless devices the ability to access a local network. Users may then browse the internet and transfer content and data, all without the need to connect any cables. WLAN capable networks deliver much faster data speeds, longer signal ranges and a much richer mobile experience than Bluetooth or Infrared capable devices.

FAT12:

FAT12 is used only on floppy disks and FAT volumes smaller than 16 MB. FAT12 uses a 12-bit file allocation table entry to address an entry in the filesystem.

FAT16:

MS-DOS, Windows 95/98/NT/2000/XP, Windows Server 2003, and some UNIX operating systems support FAT16 natively. FAT16 is also commonly used for multimedia devices such as digital cameras and audio players. FAT16 uses a 16-bit file allocation table entry to address an entry in the filesystem. FAT16 volumes are limited to a maximum size of 2 GB in MS-DOS and Windows 95/98. Windows NT and newer operating systems increase the maximum volume size for FAT16 to 4 GB.

FAT32:

Windows 95 OEM Service Release 2 (OSR2), Windows 98/2000/XP, and Windows Server 2003 support FAT32 natively, as do some multimedia devices. FAT32 uses a 32-bit file allocation table entry to address an entry in the filesystem. The maximum FAT32 volume size is 2 terabytes (TB).

NTFS:

Windows NT/2000/XP and Windows Server 2003 support NTFS natively. NTFS is a recoverable filesystem, which means that it can automatically restore the consistency of the filesystem when errors occur. In addition, NTFS supports data compression and encryption, and allows user and group-level access permissions to be defined for data files and directories. The maximum NTFS volume size is 2 TB.

High-Performance File System (HPFS):

HPFS is supported natively by OS/2 and can be read by Windows NT 3.1, 3.5, and 3.51. HPFS builds upon the directory organization of FAT by providing automatic sorting of directories. In addition, HPFS reduces the amount of lost disk space by utilizing smaller units of allocation. The maximum HPFS volume size is 64 GB.

Second Extended Filesystem (ext2fs):

ext2fs is supported natively by Linux. ext2fs supports standard Unix file types and filesystem checks to ensure filesystem consistency. The maximum ext2fs volume size is 4 TB.

Third Extended Filesystem (ext3fs):

ext3fs is supported natively by Linux. ext3fs is based on the ext2fs filesystem and provides journaling capabilities that allow consistency checks of the filesystem to be performed quickly on large amounts of data. The maximum ext3fs volume size is 4 TB.

Hierarchical File System (HFS):

HFS is supported natively by Mac OS. HFS is mainly used in older versions of Mac OS but is still supported in newer versions. The maximum HFS volume size under Mac OS 6 and 7 is 2 GB. The maximum HFS volume size in Mac OS 7.5 is 4 GB. Mac OS 7.5.2 and newer Mac operating systems increase the maximum HFS volume size to 2 TB.

HFS Plus:

HFS Plus is supported natively by Mac OS 8.1 and later and is a journaling filesystem under Mac OS X. HFS Plus is the successor to HFS and provides numerous enhancements such as long filename support and Unicode filename support for international filenames. The maximum HFS Plus volume size is 2 TB.

Unix File System (UFS):

UFS is supported natively by several types of Unix operating systems, including Solaris, FreeBSD, Open BSD, and Mac OS X. However, most operating systems have added proprietary features, so the details of UFS differ among implementations.

Compact Disk File System (CDFS):

As the name indicates, the CDFS filesystem is used for CDs.

International Organization for Standardization (ISO) 9660:

The ISO 9660 filesystem is commonly used on CD-ROMs. Another popular CD-ROM filesystem is Joliet, a variant of ISO 9660. ISO 9660 supports filename lengths of up to 32 characters, while Joliet supports up to 64 characters. Joliet also supports Unicode characters within filenames.

Universal Disk Format (UDF):

UDF is the filesystem used for DVDs

E-MAIL IDs OF VARIOUS AGENCIES/ SERVICE PROVIDERS

Organisation	E-mail ID
INTERNET SERVICE PROVIDERS	
BSNL - (ISP)	sdetecvig@bsnl.co.in
Beam Cable (ACT)- ISP	Ajay.banda@actcorp.in
ONLINE SHOPPING MERCHANTS	
Flipkart	cs@flipkart.com & grievance.officer@flipkart.com
E-Bay	contactIndiafir@ebay.com
IRCTC	care@irctc.co.in
OLX	Grievance-officer@olx.in
PAYTM	security@paytm.com
RECHARGEITNOW	care@rechargeitnow.com
WAY2SMS	support@way2online.com
MOBILE SERVICE PROVIDERS	
AIRTEL	nodalofficer3.ap@in.airtel.com
BSNL	vightd10@bsnl.co.in
CELLONE	techcellone_hyd@bsnl.co.in
IDEA	inodal.ap1@idea.adityabirla.com
RELIANCE	rcom.apnodalofficer@relianceada.com
TATA	apsecurity.wing@tatatel.co.in
E-MAIL SERVICE PROVIDERS	
GOOGLE	lis-apac@google.com
MICROSOFT	indiacc@microsoft.com
YAHOOINDIA	robinfe@yahoo-inc.com

ORGANISATION	NODAL OFFICER	PHONE NO	EMAIL_ID
ACTTV	NODAL OFFICER		nodalofficer@acttv.in
BEAM CABLE	AJAY BANDA	9542445244	ajay.banda@beamtele.com
BEAM CABLE	BEAM		nodal.term@beamtele.com
BSNL	NARAYANA	9490120744	sdetecvig@bsnl.co.in
EXCELL MEDIA	RAMA	9866316212	ramakrishna@excellmedia.net

NETX	ADITYA		skept@netxconnect.com
PIONEER ONLINE	NODAL OFFICER		support@pol.net.in
SIFY	NODAL OFFICER		luithelp@sify.com
SKYTEL	RAJ KUMAR		rajskytel@gmail.com
SOUTHERN ONLINE	SOL		support@sol.net.in
SRITEL	VAMSI		vamsi@sritel.in
TIKONA	SAMPAT JAYDEEP		jaydeep.sampat@tikona.in
VAINAVI	PADMAJA		padmaja@vainavi.net
VAINAVI	NODAL OFFICER		nodal@vainavi.net
VSNL	SECTION VIGILANCE		VIGILANCE.mumbai@tatacommunications.com
YOU TELE	NODAL OFFICER		idc@youbroadband.co.in
ZYTEL	ANIL KUMAR		anilkumar.ch@zytel.com
ARZOO	RAJESH		rajesh.m@arzoo.com
BHARAT MATRIMONY	NODAL OFFICER		legal@consim.com
CLEARTRIP	SUPPORT		hotelcs@cleartrip.com
CLEARTRIP	MANGESH		mangesh.bhanu@cleartrip.com
EBAY	NODAL OFFICER		contactIndiafit@ebay.com
EBAY	MOHAN	9867712149	kchaudhary@ebay.com
FLIPKART	CUSTOMER SUPPORT		cs@flipkart.com
FLIPKART	NODAL OFFICER		grievance.officer@flipkart.com
IRCTC	CUSTOMER CARE		care@irctc.co.in
MOBIKWIK	NIKHIL		support@mobikwik.com
MOBIKWIK	AMIT		amit@mobikwik.com
MOBIKWIK	TAMANNA		tamanna@mobikwik.com
MOBIKWIK	HEENA		heena@mobikwik.com
OLX	OLX		grievance-officer@olx.in

OLX	OLX INTERNATIONAL		complaints@council.bbb.org
PAYTM	RAHUL		rahul.bali@paytm.com
PAYTM	SECURITY		security@paytm.com
RECHARGEITNOW	GANESH		ganesh.garg@rechargeitnow.com
RECHARGEITNOW	CUSTOMER CARE		care@rechargeitnow.com
RECHARGEITNOW	SARAT		sharat.jain@rechargeitnow.com
RECHARGEITNOW	MAHESH		mahesh.agarwal@esteltelecom.com
WAY2SMS	RAJASEKHAR	9390036006	support@way2online.com
PAYTM			cybercell@paytm.com
PAYU			reportfraud@payu.in disutes@payu.in care@payu.in
IRCTC			itaf@irctc.co.in care@irctc.co.in
MOBIKWIK			fraudalerts@mobikwik.com risk@mobikwik.com
BOOKMYSHOW			helpdesk@bookmyshow.com riskmanagement@bookmyshow.com
OLA CABS			cybercrimeescalations@olacabs.com anik@legaltrb.com security@olacabs.com
FREECHARGE			risk.team@freecharge.com care@freecharge.in
SBI eBUDDY	NODAL OFFICER		epg.cms@sbi.co.in dm1it.cms@sbi.co.in alert.buddy@sbi.co.in agm.nodcyb@sbi.co.in
AIRCEL	G JITHENDER	9700199501	ap.nodaldesk@aircel.co.in
AIRTEL	DEEPAK KUMAR	9959011456	nodalofficer3.ap@in.airtel.com
BSNL	NODAL OFFICER		vightd10@bsnl.co.in
CELLONE	BALA SINGH	9490682200	techcellone_hyd@bsnl.co.in

IDEA	B SANTHOSH	9848002245	Inodal.ap1@idea.adityabirla.com
LOOP	NODAL OFFICER		nodal.officer@loopmobile.in
MTNL	NODAL OFFICER		gmvigil@mtnl.net.in
RELIANCE	GUPTA	9347410041	RCom.APNodalOfficer@relianceada.com
TATA	NODAL OFFICER		APSecurity.Wing@tatatel.co.in
TATA	M SRINIVAS	9030099333	AP.TTSLNodalofficer@tatatel.co.in
UNINOR	JAGAN		jagan.vellanki@uninor.in
UNINOR	V JAGAN MOHAN RAO	9059112523	CNO.AP@uninor.in
VODAFONE	G SIVA KUMARI	9885018536	nodaldd.andhrapradesh@vodafone.com
GOOGLE	GITANJLI	9999300447	gitanjli@google.com
GOOGLE	GOOGLE LEGAL SERVICES		lis-apac@google.com
HOTMAIL	HOTMAIL		msnwwcc@microsoft.com
MICROSOFT	MICROSOFT		indiacc@microsoft.com
REDIFF			dixond@rediff.co.in
REDIFF	JYOTHI		jyotid@rediff.co.in
REDIFF	NODAL OFFICER		legal@rediff.co.in
YAHOO	ROBIN FERNANDEZ		robinfe@yahoo-inc.com
FACEBOOK INDIA	VIKRAM	8879222222	records@facebook.com
BILL DESK	GENIUS		genius@billdesk.com
CCA VENUES	NODAL OFFICER		risk@ccavenue.com

NODAL OFFICERS OF DIFFERENT BANKS IN INDIA

ORGANISATION	NODAL OFFICER	PHONE NO	EMAIL_ID
ANDHRA BANK	NODAL OFFICER		frmg@andhrabank.co.in
AXIS BANK	AJAY CHAKOTE	7893966698	Ajay.Chakote@axisbank.com
BANK OF BARODA	GM (OPERATIONS)		gm.ops.ho@bankofbaroda.com
HDFC BANK	SOMASEKHAR	9347052868	SomaSekhar.RaoDaduwai@hdfcbank.com
HSBC BANK	NODAL OFFICER	9703227575	nodalofficerinm@hsbc.co.in
HSBC BANK	HSBC		srinivas1naidu@hsbc.co.in
ICICI BANK	P NARASIMHA RAO	9000601267	narasimharao.ponnam@icicibank.com
ICICI BANK	K V RANGACHARY	9949612251	rangachary.kv@icicibank.com
ING VYSYA BANK	NODAL OFFICER		nodalofficer@ingvysyabank.com
IOB	IOB		creditcard@jobnet.co.in
KOTAK	ESCALATIONS		escalations@kotak.com
KOTAK	SHIVKUMAR	9885031691	shivkumar.sundaram@kotak.com
KOTAK	SUPPORT		service.bank@kotak.com
PNB	DGM		skbansal@pnb.co.in
PNB	GM		vsrinivasan@pnb.co.in
SBH	CM (GRIEVANCES)		cmgrievances@sbhyd.co.in
SBI	AGM (VIGILANCE)		agmwig.lhohyd@sbi.co.in
SBI	HELP LINE - HYDERABAD		helpline.lhohyd@sbi.co.in
SBI	AGM		agmcustomer.lhohyd@sbi.co.in
SBI-CARDS	CEO-SBI CARDS		CEO@sbicard.com
SBI-CARDS	NODAL OFFICER		Nodalofficer@sbicard.com
SCB	NODAL OFFICER		principal.nodalofficer@sc.com

S. No	Name of Bank	Name of the Nodal Officers	Address CPPC	Phone/Fax No. /e-mail
1	Allahabad Bank	Dr S R Jatav	Asst. General Manager, Allahabad Bank, CPPC Zonal Office Building, Ist floor, Hazratganj, Lucknow UP-226001	Office no: 0522 2286378, 0522 2286489 Mob: 08004500516 cppc@allahabadbank.in
2	Andhra Bank	Shri M K Srinivas	Sr. Manager, Andhra Bank, Centralized Pension Processing Centre(CPPC) 4th floor, Andhra Bank Building, Koti, Hyderabad-500095	Mob: 09666149852, 040- 24757153 abcppc@andhrabank.co .in
3	Axis Bank	Shri Hetal Pardiwala	Nodal Officer AXIS BANK LTD, Gigaplex Bldg. no.1, 4 th floor, Plot No. I.T.5, MIDC, Airoli Knowledge Park, Airoli, Navi Mumbai- 400708	Mob: 9167550333, hetal.pardiwala@axisba nk.com
4	Bank of India	Shri R. Ashok Nimrani	Chief Manager Bank of India, CPPC Branch, Bank of India Bldg. 87-A, 1st floor, Gandhibagh, Nagpur-440002.	0712-2764341, Ph.2764091,92 0712-2764091 (fax) cppc.nagpur@bankofind ia.co.in
5	Bank of Baroda	Shri S K Goyal,	Dy. General Manager, Bank of Baroda, Central Pension Processing Centre, Bank of Baroda Bldg. 16, Parliament Street, New Delhi – 110 001	011-23441347, 011- 23441342 cppc.telecom@bankofba roda.com cppc.delhi@bankofbaro da.com
6	Bank of Maharashtra	Shri D H Vardy	Manager Bank of Maharashtra Central Pension Processing Cell, 1177, Budhwar Peth, Janmangal, Bajirao Road Pune-411002	Ph: 020-24467937/38 Mob: 08552033043 bom1407@mahabank.c o.in
7	Canara Bank	Shri K S Hebbar	Asst. General Manager Canara Bank Centralized Pension Processing Centre Dwarakanath Bhavan 29, K R Road	Mob. 08197844215 Ph: 080 26621845 hebbarks@canarabank. com

			Basavangudi, Bangalore 560 004	
8	Central Bank of India	Shri V K Sinha	Chief Manager Central Bank of India (CPPC) Central Office, 2nd Floor, Central Bank Building, M.G. Road, Hutatma Chowk Fort, Mumbai - 400001	Ph: 022- 22703216/22703217, Fax- 22703218 cppc@centralbank.co.in cmcppc@centralbank.co .in
9	Corporation Bank	Shri B R Balia	Manager Corporation Bank (CPPC) Pandeshwar, Mangaladevi Temple Road, Post Box No. 88, Mangalore - 575001	0824-2425230, 2861471 Toll Free No. 1800-425- 3556 Mob: 8762363957 hogovt@corpbank.co.in hopension@corpbank.co .in
10	Dena Bank	Shri G Ratan,	Nodal Officer Dena Bank, Centralized Pension Processing Centre (CPPC), Mumbai Main Office, 17, Hornimon Circle Mumbai-400023	022-22690191 022- 22690192 gbd@denabank.co.in cppcdena@denabank.co .in
11	HDFC Bank	Shri Rahul Chandra	Chief Manager HDFC Bank A-111, First Floor, Pension Dept., Sec-4, Noida (UP) - 201301	0120-4894104 rahul.chandra@hdfc.co m
12	ICICI Bank	Shri Vinayak More	Nodal Officer ICICI Bank Ltd., Corporate Head Office, ICICI Bank Towers, Bandra - Kurla Complex Bandra (East), Mumbai	Mob: 9820150167 vinayak.more@icicibank .com
13	IDBI Bank	Shri Jigar Pandya	Nodal Officer IDBI Bank Ltd. Unit No. 2, Corporate Park Sion, Trombay Road, Near Swastik, Chambers, Chembur, Mumbai-400071	022 66908445 jigar_pandya@idbi.co.in
14	Indian Bank	Shri B D Mane	Nodal Officers Indian Bank CPPC, Fourth Floor, No. 66, Rajaji Salai,, Chennai-600001	044-25231756/7 044-28134027 Mob: 9445030402

				cppc@indianbank.co.in cmcppc@indianbank.co.in
15	Indian Overseas Bank	Shri G. Kumar	Manager Indian Overseas Bank Central Office, 763, Anna Salai, Chennai Tamilnadu - 600002	044-28889383/4(Ph) 044-28519433(Ph) Mob: 09840080166 044-28514903(fax) cppc@iobnet.co.in
16	Oriental Bank of Commerce	Shri Shayan Kumar	Chief Manager Oriental Bank of Commerce CPPC & GBC, Plot No. 5, Institutional Area, Sector-32, Gurgaon-122001	0124-4126950 0124-4126530 cppc@obc.co.in
17	Punjab National Bank	Shri M K Srivastav	Nodal Officer Punjab National Bank (CPPC) Gurudwara Road, Karol Bagh New Delhi-110055	Mob: 8800692335 cppcdel@pnb.co.in hogbd@pnb.co.in
18	Punjab & Sind Bank	Shri Abhishek Rana	Nodal Officer Punjab & Sind Bank, CPPC A-25, CPPC Cell, 1st Floor, Community Centre, Jwala heri, Paschim Vihar, New Delhi 110063	Mob: 09464554448 cppc@psb.co.in
19	State Bank of Bikaner & Jaipur	Shri Subhash Gupta	Chief Manager State Bank of Bikaner & Jaipur CPPC, 2nd floor, SMS Highway Jaipur, Rajasthan -302005	0141-5172101(Ph), 0141-2227758/5172259 0141-2316921(fax) Mob: 9413398707 scgupta@sbbj.co.in
20	State Bank of Hyderabad	Smt Sameer Janakidevi	Chief Manager, State Bank of Hyderabad, CPPC 1st floor, Methodist Complex, Opp.- Chermas Shop, Abids, Hyderabad - 500001	040-23387483, 23387811 Fax-040-23202104 cppc-hyd@sbhyd.co.in
21	State Bank of India	Shri Shirish Anant Patki,	Chief Manager, State Bank of India, Government Accounts Department, Corporate Centre, CBD Belapur, Navi Mumbai	Mob: 9867568262 shirish.patki@sbi.co.in
22	State Bank of Mysore	Shri Diwakara Poojary U	Asstt. General Manager State Bank of Mysore (CPPC) 2nd Floor, Manjusha Building, Bejai - Mangalore. PIN: 575004	Ph: 0824 - 2216173, 0824-2218775 Mob: 9448291386 cppcmangalore@sbm.co.in

23	State Bank of Patiala	Shri Kamal Garg	Chief Manager State Bank of Patiala, CPPC Pragati Bhawan, Ist Floor, Urban Estate-III, Patiala, Punjab-147002	0175-2392092, Fax: 0175-2392094 Mob. 9779586330 email: infocppc@sbp.co.in
24	State Bank of Travancore	Ms. Jaishri Ramchandran	Chief Manager State Bank of Travancore Chembikalam Buildings 3rd floor, Vazhuthacaud Trivandrum-695014	0471- 2351903/2324217/232 6525, 0471-2351137(fax) Toll free No.18004256525 cppc@sbt.co.in
25	Syndicate Bank	Shri A. G. Gopinath	Nodal Officer Syndicate Bank. Operations Department Central Pension Processing Centre HO: Manipal, Karnataka- 576104	Fax: 0820-2573363 Ph: 0820- 2575402/1196/4075 Ph: 0820- 2574075/2571181 syndcpppc@syndicatebank.co.in
26	Union Bank of India	Ms. Asha Sharma	Chief Manager, Union Bank of India CPPC, Union Bhavan CPPC 12th Floor 239 Vidhan Bhavan Marg Nariman Point, Mumbai 200 049	Tel. No 022-22020242 mobile 9869543267 ashabsharma@unionbankofindia.com
27	United Bank of India	Smt. Kajal Banerjee	Asstt. General Manager United Bank of India CPPC, Head Office, 4th floor 11, Hemanta Basu Sarani Kolkata-700001	033-22622549/1042 033-22422196(fax) 033-22622549 Mob: 9434810858 cppc@unitedbank.co.in cmcppc@unitedbank.co.in
28	United Commercial Bank	Shri M.S. Khobregade	Senior Manager United Commercial Bank Central Pension Processing Centre, Somalwar Bhawan I Floor Sadar Mount Road Extension Nagpur -420 001	Tel No. 0712 2559969. cppcna@ucobank.co.in gbmcell.kolkata@ucobank.co.in
29	Vijaya Bank	Shri Arava Amarnath	Senior Manager, Vijaya Bank, Merchant Banking Division Head Office, 41/2, M.G. Road, Trinity Circle, Bangalore- 560001	080-25584066(Ph) Ext 260. 080-25582915(fax) Mob: 9241001301 mbd.pension@vijayabank.co.in mbdagm@vijayabank.co.in

G MAIL

Google/ /Youtube
Google Inc.
1600 Amphitheatre Parkway
Mountain View CA 94043
USA
lis-apac@google.com

Face Book

Facebook Ireland Ltd.
Hanover Reach
5 5- -7 7 Hanover Quay
Dublin 2 2
Ireland
records@fb.com

Alliance Broadband Services Pvt.. Ltd.

Padmapukur (Entally).
P-89, C.I.T Road
Kolkata-700 014
support@alliancekolkata.com

IBIBO

Legal Support
Ibibo WebPvt Ltd
4 floor , Pearl Tower
Plot no 51
Sector-32,Gurgaon
Haryana 122001
ibibodomains@ibibogroup.com

World Phone

The Chief Operating Officer
The World Phone Internet Services Private Ltd
C - 153 Okhla Industrial Area, Phase - I
New Delhi- 110020
bandwidthsupport@worldphone.in
sandeepdugar@worldphone.in
dugar.hitesh@gmail.com
hiteshdugar@worldphone.in

EXCELL MEDIA

The Chief Operating Officer
Excell Media Pvt Ltd .
No-8-2-268/N/28/ A Quinn House
Road No-2, Sagar Society, Banjara Hills
Hyderabad - 500034
Andhra Pradesh
SUPPORT @ EXCELLMEDIA. . NET

WAY2SMS.COM

Mr. Raju Vanapala
No. 89, 2nd floor, Road No. 9, Jubilee Hills
Hyderabad- - 500033
Andhra Pradesh
Registrant Phone: +040.23556711
Registrant Email: raju@ @ way2online.net

LOCANTO SUPORT TEAM

The Chief Operating Officer
Locanto Support Team - support@locanto.com
MileWeb Inc
4701 Patrick Henry Drive #2101,
Santa Clara,
CA 95054,
United States
Contact us:
+1 (408) 634-8189
sales@mileweb.com

Yahoo.

Mr. Robin Fernandes
Yahoo a India e Private Limited
Building 12, 6th Floor
Solitaire e Corporate Park
Guru Hargovindji Marg, ,
Andheri (E), Mumbai 0 400 093
Kindly send any such request in future at email ID in-legalpoc@yahoo-
inc.com
PH. 022-33089693
Robin Fernandes robinfe@yahoo-inc.com

Quikr

The Quikr India Pvt Ltd.
1st Floor, Raghuvanshi Mansion,
Senapati Bapat Marg, Lower Parel,
Mumbai - 400 013
support@quikr.com

Naukri.com

The Legal Team
Naukri.Com
Noida
legal@naukri.com

Just Dial

Just Dial Limited
No: 703, Godrej Waterside Tower One Sector V,
Salt Lake City,
Kolkata - 700091.
Call : +91-33-4406 5599, +91-33-3982 6767
jobskolkata@justdial.com
Email : kolkata@justdial.com

LeaseWeb

The Technical Support Officer
RIP Mean
1090 BB Amsterdam
Netherlands
LeaseWeb - Security security@leaseweb.com

Tinkona Broad band

Mr. Sunil Nair
Designation - Head - Customer Service Quality
2nd Floor, 'Corpora', L.B.S. Marg,
Bhandup (West),
Mumbai - 400 078.
s.nair@tikona.in
customercare@tikona.in
Mr. Jaykrishnan Nair
Manager - Contact Center Operations
2nd Floor, 'Corpora', L.B.S. Marg,
Bhandup (West),
Mumbai - 400 078
j.nair@tikona.in

Hot Mail

The Legal Support Team
Hotmail.com
Microsoft
indiacc@microsoft.com
globalcc@microsoft.com

BackPage

Backpage Dom-Admin
Backpage.com LLC
PO Box 192307
Dallas
TX
75219
US
Phone: +1.8664566877
Email: dom-admin@backpage.com
abuse@backpage.com

Microsoft

globalcc@microsoftcc.com

Rediffmail

Legal Support
Rediff.com India Limited
Mahalaxmi Engineering Estate
L. J. First Cross Road
Mahim (West)
Mumbai 400 016
legal@rediff.co.in

You tube

YouTube Support support@youtube.com

Infinity Electric

Web Werks India Pvt. Ltd.
124 Unique Industrial Estate
Prabhadevi
Mumbai
MAHARASHTRA
400025
abuse@webwerks.com
westcom-int.com

G G C C k Link t Pvt d Ltd (Alliance Broadband)

Mr. Chunnilal Pal
G C Link Pvt Ltd
E167/B, Raja S C Mullick Road,
Opposite West Wind
Kolkata - 700047,
+(91)-33-2430-6203/0973
E-mail - gclinkpvtltd@gmail.com

AGRAHANDICRAFT.COM

AGRAHANDICRAFT.COM
Rahul Agarwal
Rahul Jewelers
503, Kaveri Apartment Khandari
Agra
Uttar pradesh
282005
Email: sandlus0036@gmail.com

USA.COM (E-mail provider)

World Media Group, LLC
90 Washington Valley Rd., #1128
Bedminster
New Jersey
USA
Sent to: LegalNotice@mail.com
Email: domains@world.com

BIG ROCK

The Chief Operating Officer
Bigrock s Solutions Limited
DirectiPlex
Old Nagardas Road
Near Andheri Subway
Andheri (E E)
Mumbai 400069
compliance@bigrock.com
@bigrock.com

dr.com

The Chief Operating Officer
World Media Group LLC
90 Washington Valley Rd, # 1128

Bedminster
New Jersey – – 07921
United States
E-Mail - domains@world.com
abuse@web.com

XHAMSTER. COM

WHOISGUARD PROTECTED
WHOISGUARD, INC
P.O. BOX 0823-03411
PANAMA
Mail ID : PROTECT@WHOISGUARD.COM

SITI CABLE NETWORK

Operations In charge
Rajib Chakraborty
29/F, B.T.Road, Peerless Nagar Complex,
Sodepur, Panihati, 24 Pgns (N),
Kolkata – 700114
Email: rajivc@wwil.net
Sanjoy Das <Sanjoy.Das@siticable.com>, Abdullah.Mullick@siticable.com
rajivchakraborty@siticable.com
Rajib Chakraborty
Mob: 9874476222

PayTM

Vijay Shekhar Sharma
PayTM Mobile Solutions Pvt Ltd
B-121, Sector 5
Noida, Uttar Pradesh
Pin- 201301
webadmin@one97.net , contact No... +91.01204770770

webdesktechnologies

The Chief Executive Officer
Webdesk Technologies
5, Tarapada Chakraborty Sarani
771/A, Block "P"
New Alipore
Kolkata- 700053
info@webdesktechnologies.com

Wish Net Private Limited

Wish Net Private Limited
86, Golaghata Road,
Saraswati Apartment, 6th Floor,
Kolkata - 700 048,
West Bengal, India
info@wishnet.co.in

SBI

AGM, Internet banking
State Bank of India
State Bank Global IT Center
Ground floor, A- Wing, Sector-11
C.B.D., Belapur
Navi Mumbai
Maharashtra
400614
agm.inb@sbi.co.in
alert.buddy@sbi.co.in

Baid Group

Anand Punjabi
Cumulative Tech
C14 Tagore Park
Kolkata-39
West Bengal
domains@cumulativetech.com

Meghbala Brodband

The Nodal Officer
Meghbela Cable & Broadband Services (P) Ltd Kolkata
[info @ meghbelabrodband.com](mailto:info@meghbelabrodband.com), , [support @ meghbelabrodband.com](mailto:support@meghbelabrodband.com),
[info @ pacenetmeghbela.com](mailto:info@pacenetmeghbela.com),
tapabrata@meghbelabroadband.com

Videocon Telecommunications Ltd (WB)

Videocon Telecommunications Ltd.
Parvati Shopping Arcade,
Block-C, 2nd floor,
Asansol, Pin:713303
"Suman.Pradhan@videocon.com" <Suman.Pradhan@videocon.com>
nodalofficer.wb@videocon.com

Sale2kart.in

http://sale2kart.in/
The Future Tree
PLOT NO.-1-C, NEW RZ-B-74,
UPPER GROUND FLOOR,
MAHAVIR VIHAR, NEW DELHI-110045
Tel +91-9971876990
E mail info@sale2kart.in

Westcom I International Co, Ltd. .

Westcom International Co., Ltd.
Kai Airas ()
17/21 Soi Pradipat 1,
Pradipat Road,
Samsennai, Phayathai
Bangkok
Bangkok,10400
Thailand
I Mail Address
kai.airas@westcom-int.com

Sify Limited Service Provider India

Sify Technologies Limited
II Floor, Tidel Park,
No.4, Canal Bank Road,
Taramani, Chennai - 600 113,
India.
gomathi.sitaram@sifycorp.com

Sify Technologies Limited

Mr. Debraj Bhattacharya
Senior Engineer
Customer Care Support
Sify Corporation
Kolkata
fcs_kol@sifycorp.com
Debraj Bhattacharya (m) : : 9836020024
office: 666323000
Add: 2/1A Sarat Bose rd. kol 20
Sify Technologies Limited.
II Floor, Tidel Park,
No. .4 Canal Bank Road, ,
Taramani, Chennai - - 600113, ,

India

E-mail: lea.support@sifycorp.com

Phone : + + 91- - 044- - 22540770/ / 77

Ext No: 2919, , 2847

Fax :+ + 91- - 044- - 22540771

myntra.com

The Associate Officer

Myntra.com

Maruthi Chambers

Annexe Building,Rupena Agrahara

Hosur Road

Bengalore 560068

support@myntra.com

Mobile no. 080-67996666

GET NETWORK LTD.

The Nodal Officer

Ariyan Glorry 1st Floor,

Panchasayar 1931 Chak Garia

Garia - Kolkata-700094

E Mail:prasad@getnetwork.in

Phone: : 033-64554555/ 7555/ 8555

18004190123 (Toll Free Number)

Fax: : 033 3008 2250

355932040265279 Hati Searching.

webadmin@one97.net , contact No... +91.01204770770

To

Vijay Shekhar Sharma

PayTM Mobile Solutions Pvt Ltd

B-121, Sector 5

Noida, Uttar Pradesh

Pin- 201301.

PayU.com,Contact0124-6624801

nitin.gupta@payu.in

To

The CEO

PayU Payments Private Limited ,7thFloor,PearlTower,PlotNo51.

InstitutionalArea,Sector32,Gurgaon:122001

Mobikwik bipin.p.singh@gmail.com

+91.7838693548

To

Bipin Singh

D-28B,MotiNagar

New Delhi Pin-110015

* * *

HANDBOOK

ON

CYBER CRIME INVESTIGATION



Telangana State Police

www.tspolice.gov.in