Chapter 1

INTRODUCTION TO CYBER CRIME

Cybercrime may be defined as “Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime”. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both -- i.e., target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks.

A primary effect of cybercrime is financial; cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals may also target an individual's private information, as well as corporate data for theft and resale.

TYPES OF CYBER CRIME

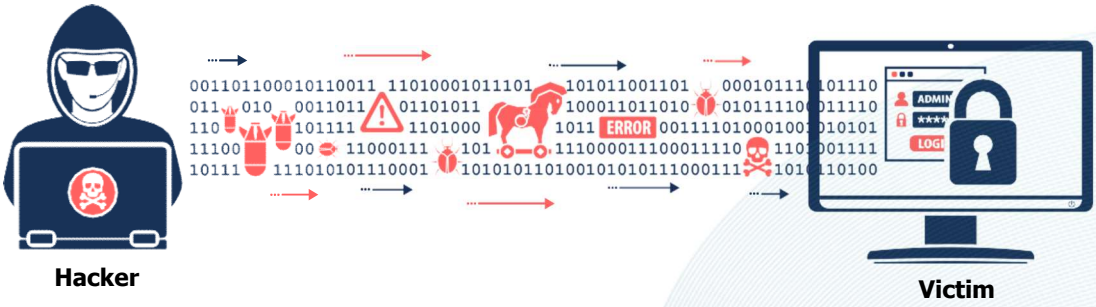
Malicious domain, Ransomware, Data-harvesting malware, Botnets, Crypto jacking, the Darknet, words and phrases that scarcely existed a decade ago are now part of our everyday language, as criminals use new technologies to commit cyberattacks against governments, businesses and individuals. These crimes know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide. Cybercrime is progressing at an incredibly fast pace, with new trends constantly emerging. Some types are discussed below.

I. E MAIL RELATED CRIME

Email has fast emerged as the world's most preferred form of communication. Billions of email messages traverse the globe daily. Like any other form of communication, email is also misused by criminal elements. The ease, speed and relative anonymity of email has made it a powerful tool for criminals. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. Some of the major email related crimes are explained below

Email Spoofing

A spoofed email is one that appears to originate from one source but has emerged from another source. Falsifying the name and / or email address of the originator of the email usually does email spoofing. The result is that the email recipient sees the email as having come from the address in the 'From: header'. They may sometimes be able to find the MAIL FROM address, and if they reply to the email it will go to either the address presented in the From: or Reply-to: header, but none of these addresses are typically reliable, so automated bounce messages may generate backscatters.

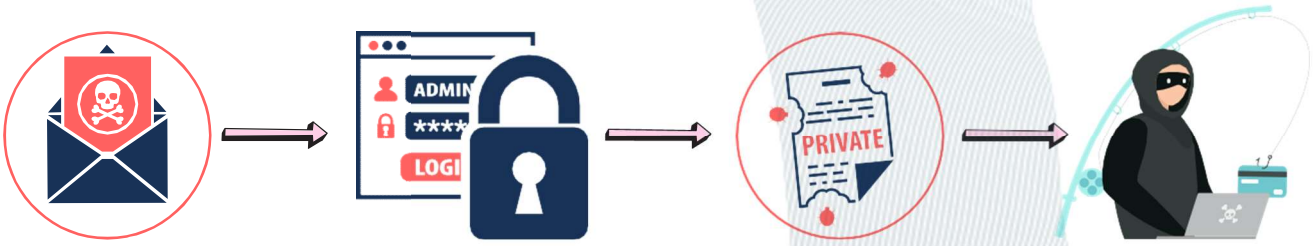


Hacker

Victim

Phishing

Phishing is a two time scam, first steals a company's identity and then use it to victimize consumers by stealing their credit identities. The term Phishing comes from the fact that Internet scammers are using increasingly sophisticated lures as they "fish" for user's financial information and password data. It is the act of attempting to trick customers into disclosing their personal security information by masquerading as trustworthy businesses in an e-mail.



Spam

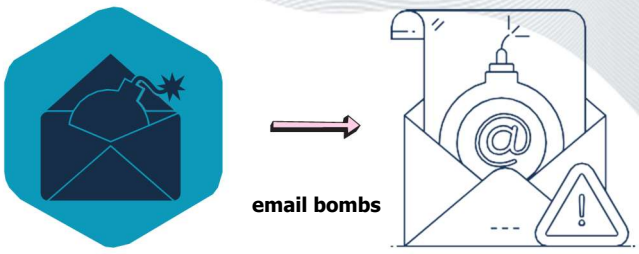
Hacked ID

Hacked Informations

Phishing datas

Email Bombing

An email bomb is an attack against an email inbox or server designed to overwhelm an inbox or inhibit the server's normal function, rendering it unresponsive, preventing email communications, degrading network performance, or causing downtime.

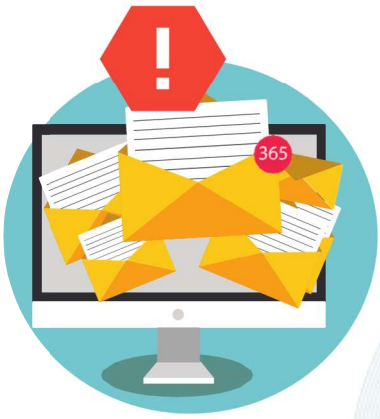


email bombs

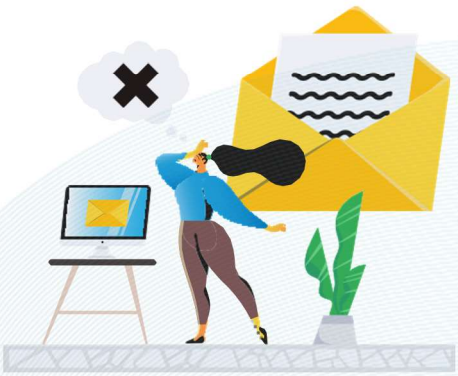
Spamming

Spam mail is the distribution of bulk e-mails that advertise products, services or investment schemes, which may well turn out to be fraudulent. The purpose of spam mail is to trick or con customers into believing that they are going to receive a genuine product or service, usually at a reduced price. However, the spammer asks for money or sensible security information like credit card number or other personal information before the deal occur. After disclosing their security information, the customer will never hear from the spammer.

Hacker



Spam



Hacked personal information and loss of money from victim

Spear-phishing

Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons. This is achieved by acquiring personal details on the victim. The attackers then disguise themselves as a trustworthy friend or entity to acquire sensitive information, typically through email or other online messaging. Phishing attacks are not personalized to their victims, and are usually sent to masses of people at the same time while spear-phishing attacks, are personalized to their victims.

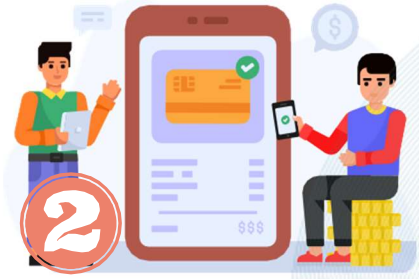
Phishing all the data from victim

II. ILLEGAL ONLINE TRANSACTION

Any type of false or illegal transaction completed by a cybercriminal comes under Payment fraud. The perpetrator deprives the victim of funds, personal property, interest or sensitive information via the Internet.
Payment fraud is characterized in three ways:

- Fraudulent or unauthorized transactions
- Lost or stolen merchandise
- False requests for a refund, return or bounced checks

Fraudulent



Stolen Merchandise

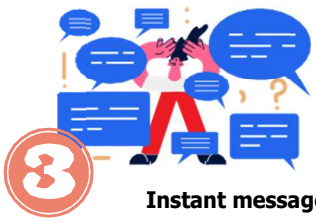
False information

Ecommerce businesses rely on electronic transactions to charge customers for products and services. The increased volume of electronic transactions has also resulted in an increase in fraudulent activities. Hackers often pose as a legitimate representative and contact credit card owners asking for sensitive information, then use the following means of interaction to steal personal data:

- Email
- Texting malware to smartphones
- Instant messaging
- Rerouting traffic to fraudulent websites
- Phone calls
- Online auctions

E-mail

Texting Malware



Instant messages

Fraudulent website

Phone Calls

Online auctions

III. JOB FRAUDS

It involves deceiving people seeking employment by giving them the false hope of earning high salaries or extra income. There are numerous methods where scammers come up with attractive offers such as easy hire, easy work, high wages, flexible working hours etc., Some common job spams are as follows:

- Data Entry Scams
- Pyramid Marketing
- Unsolicited Job Offers

Data entry

Pyramid marketing

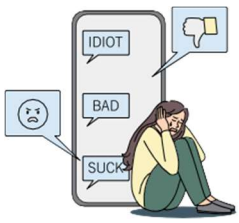
Unsolicited Job

IV. CYBER DEFAMATION

Any intentional false communication, either written or spoken, that harms a person's reputation, decreases the respect, regard or confidence in which a person is held; or includes disparaging opinions or feelings against a person is known as defamation. Defamation may be either in the way of 'Slander' or 'Libel'. The term Slander means 'the crime of damaging someone's reputation by false spoken statement', while Libel is an 'false published or written statement by damaging someone's reputation'.

The term 'Cyber Defamation' basically means publishing of false statement about an individual in cyberspace that can injure or demean the reputation of that individual.

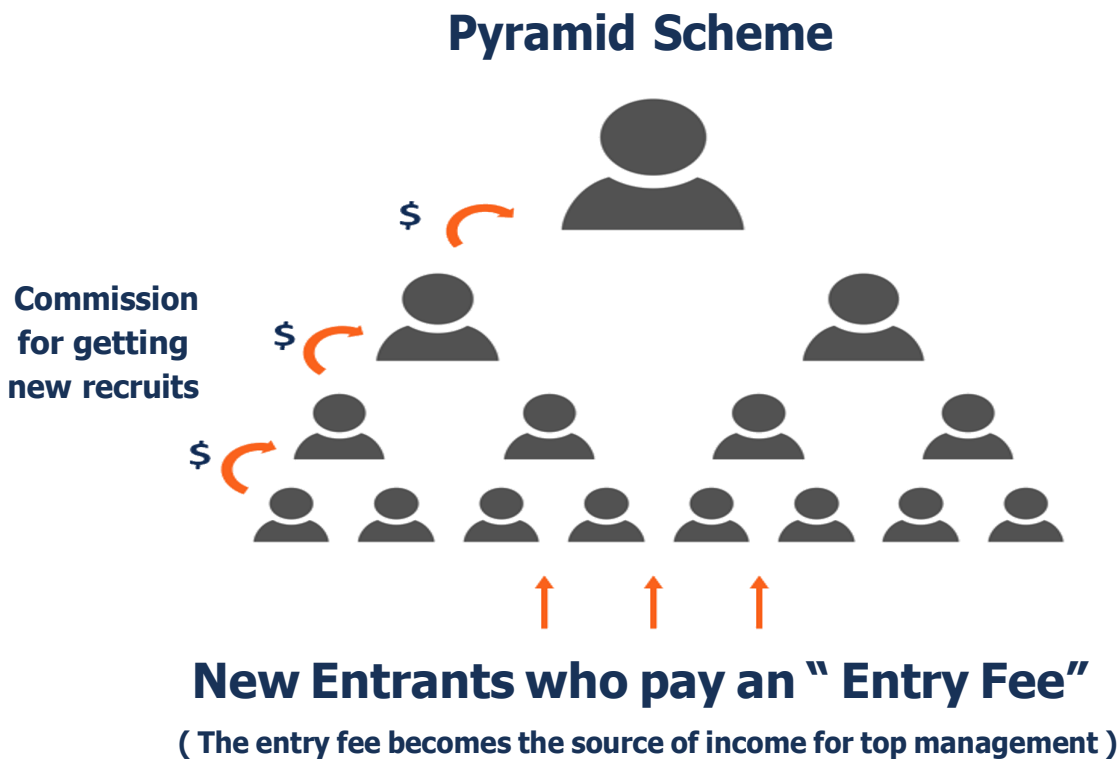
· Publishing/posting derogatory remarks against individual(s)/organization(s) on websites.
· Publishing/posting derogatory remarks against individual/ organization on the social media/networking.
. Spreading false information against individual/organization through e-mails.



Phishing individual

Posting on Social media

Spreading false information



V. PONZI SCHEME

A Ponzi scheme is a form of fraud that lures investors and pays profits to earlier investors with funds from more recent investors. The scheme leads victims to believe that profits are coming from legitimate business activity (e.g., product sales or successful investments), and they remain unaware that other investors are the source of funds

Ponzi schemes or pyramid schemes are easy to structure and enable a cyber attacker to hide behind layers of lies and distractions. These cyber schemes use well-known bank names without consent to gain credibility and lure more investors.

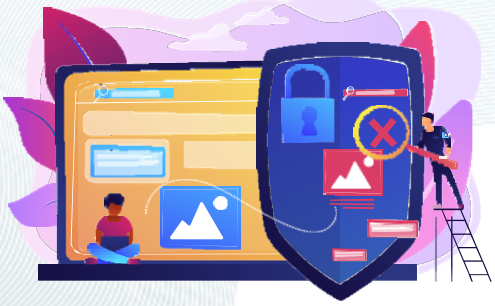
VI. CYBER STALKING

Cyberstalking's definition is quite simply, “the use of the internet, or other electronic means, to harass and intimidate a selected victim”. i.e. Stalking or harassment that takes place via online channels such as social media, forums or email is called Cyber Stalking. It is typically planned and sustained over a period of time.

e.g. State of Maharashtra Vs Atul Ganesh Patil

A women had come for job interview to a company and wrote her mobile number in the entry register. The guard saved her contact details and started sending multiple obscene WhatsApp messages and even called her repeatedly to talk obscene things thereby committing crime of stalking her. In this case, victim blocked his number. However, the guard started sending her obscene messages from his friend’s mobile phone. A case was registered under IPC 354D. The police acted swiftly completing the investigation and prepared a charge sheet within 24 hours.

texting and calling a particular person continuously



VII. CYBER BULLYING

Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behaviour.

The most common places where cyberbullying occurs are:

- Social Media, such as Facebook, Instagram, Snapchat, and Tik Tok
- Text messaging and messaging apps on mobile or tablet devices
- Instant messaging, direct messaging, and online chatting over the internet
- Online forums, chat rooms, and message boards, such as Reddit
- Email
- Online gaming communities

VIII. CYBER PORNOGRAPHY

Cyber Pornography means the publishing, distributing or designing pornography by using cyberspace. Cyber pornography is the act of using cyberspace to create, view, distribute, import, or publish pornography or obscene materials.

IX. CYBERCRIMES/ ATTACKS OF ADVANCED TYPES

Advanced cyber attacks include any kind of attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems. A cyber attack can be launched from anywhere by any individual or group using one or more various attack strategies. Some of the major types of cyber attacks are explained below:

Hacking

A commonly used hacking definition is the act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals.

Hacking refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity.

Virus

Computer Virus means any computer instruction, information, data or programme that destroys, damages degrades or adversely affects the performance of a computer resource. It generally attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

Worm

It is a self-replicating malicious software that replicates itself to spread across other devices that are connected to a network.

Trojan

It is a malicious software that is camouflaged as a legitimate software e.g. Microsoft office, web browsers, media players, gaming applications etc. When this legitimate software installed the malicious code will also get installed at the background and start doing it's malicious activity.

Website defacement

It is an attack intended for a Website, which will change the visual appearance of a website and the attacker may post some other indecent, hostile and obscene images, messages, videos, etc., and sometimes make the Website dysfunctional. The most common cases of website defacement are, hackers of one country try to deface the websites of rival countries to display their technological superiority by infecting with malware.

Salami Attack

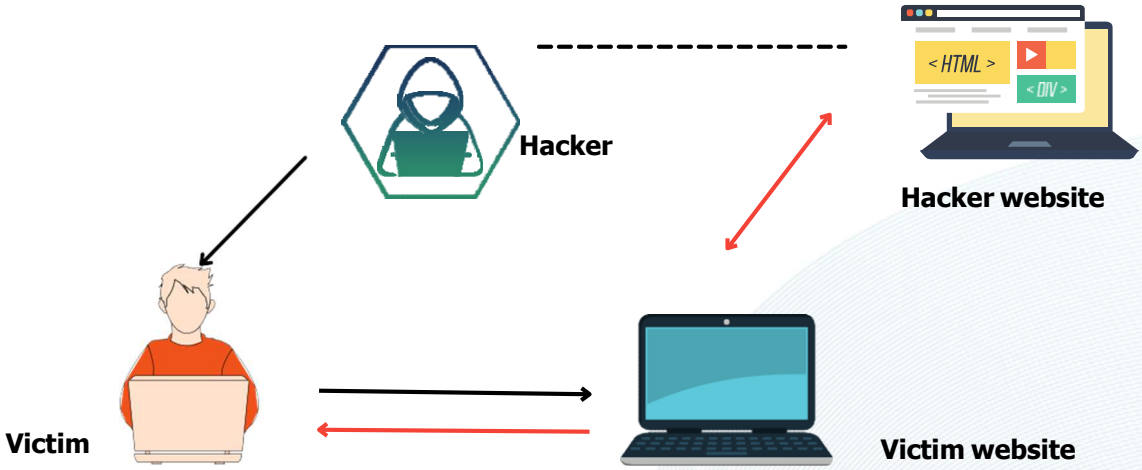
An attack is made on a system or network that involves making minor alteration so insignificant that in a single case it would go completely unnoticed. These attacks are generally used for the commission of financial crimes.

Cross-site scripting

Cross-Site Scripting (XSS) is a type of vulnerability in which malicious scripts are injected into content from otherwise trusted websites. The injection occurs when a user clicks on an unsuspected link that is specially designed for attacking a website they are visiting.

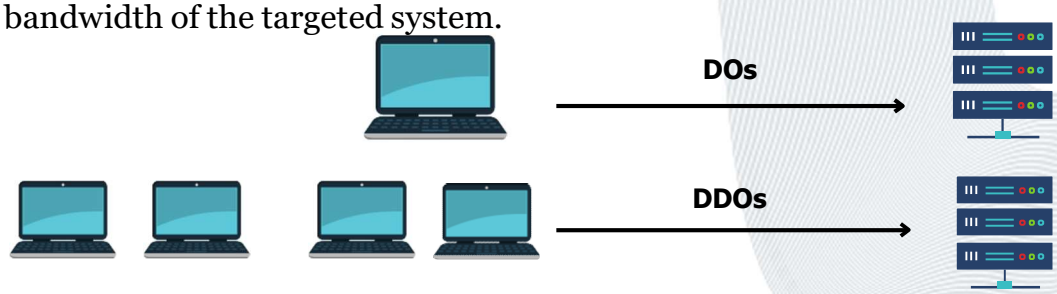
Web Jacking

The Web Jacking Attack is an advanced phishing technique where attackers make a clone of a website and send that malicious link to the victim. Once, the victims click the link that looks real he will be redirected to a fake page where attackers try to extract sensitive data such as card numbers, user names, passwords etc., from the victims.



DOS/DDOS attacks

In the Denial of service attack (DoS), an important service offered by a Web site or a server is denied or disrupted thereby causing loss to the intended users of the service. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. In some cases, DoS attacks have forced the Websites to temporarily cease operation. This often involves sending a large amount of traffic in the form e-mails and other requests to the targeted network or server so that it occupies the entire bandwidth of the system and ultimately results in a crash. The Distributed Denial of Service (DDoS) is a type of attack in which multiple systems are used by distributing the attaching BOTS to flood the bandwidth of the targeted system.

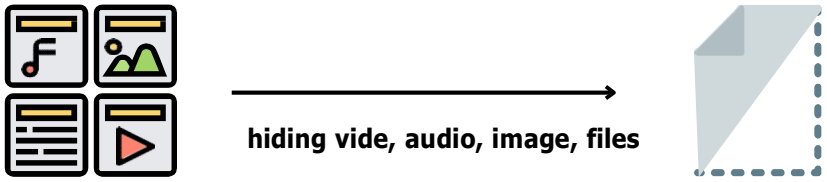


Ransomware

Ransom is defined as the practice of holding someone or something important to the victim with the intent to extort money or property to secure their release. Ransomware is a type of computer malware that locks the files, storage media on communication devices like desktops, Laptops, Mobile phones etc., holding data/information as a hostage. There is no guarantee that the victim will get the data back after paying the ransom

X. DATA HIDING TECHNIQUE- STEGANOGRAPHY

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos, meaning "covered, concealed, or protected," and meaning "writing".



XI. DEEP WEB & DARK WEB

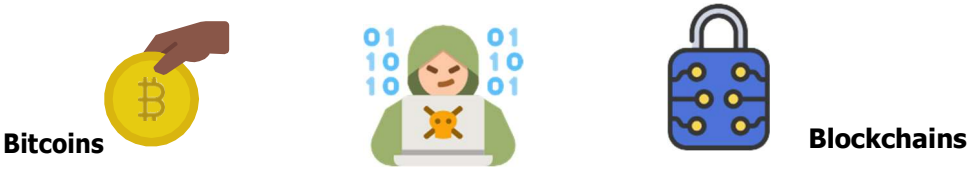
The deep web is part of the internet where a typical search engine cannot index. The dark web/ darknets is a subset of deep web that is intentionally made hidden through overlay networks and require specific software, configurations or authorization to access.

Frauds are openly discussed on the underground forums of the Dark Web where illicit vendors offer fraudulent services. These services include but not limited to, launching a DoS attack on websites, the sale of malware, illegal drugs, weapons, cyber espionage on behalf of clients and the list goes on. Most of the vendors accept the payment through crypto-currencies and specially Bitcoins due to its popularity.

XII. CRYPTOCURRENCY

Cryptocurrency Crypto derives from Greek for hidden or to hide. A cryptocurrency is created by solving complex mathematical problem based on the cryptography to regulate the generation of units of currency and verify the transfer.

A cryptocurrency like Bitcoin consists of a network of peers. Every peer has a record of the complete history of all transactions and thus of the balance of every account. The validity of each cryptocurrency's coins is provided by a blockchain. A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, block chains are inherently resistant to modification of the data. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.



Chapter 2

BASICS IN CYBER CRIME

I. DOMAIN NAME LOOKUP

Who is

Whois is a widely used Internet record listing that identifies who owns a domain and how to get contact with them. A Whois record contains all the contact information associated with the person, group or company that registers a particular domain name. Typically each WHOIS record contains information such as the name and contact information of the Registrant, the name and contact information of the Registrar, the registration dates, the name servers, the most recent update and the expiration date. Whois records may also provide the administrative and technical contact information (which is often, but not always, the registrant).

Registry: A domain name registry is an organization that manages top-level domain names. They create domain name extensions, set the rules for that domain name, and work with registrars to sell domain names to the public. For example, VeriSign manages the registration of .(dot)com domain names and their domain name system (DNS).

Domain Registrar: The registrar is an accredited organization, like GoDaddy, that sell domain names to the public. Some have the ability to sell top-level domain names (TLDs) like .com, .net, and .org or country code Top-level domain names (ccTLDs) such as .in, .ca, and .us.

Registrant: A registrant is the person or company who registers the domain name. Registrants can manage their domain name's settings through their registrar. When changes are made to the domain, their registrar will send the information to the registry to be updated and saved in the registry database.

The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership. Whois records have proven to be extremely useful and have developed into an essential resource for maintaining the integrity of the domain name registration and website ownership process. Below mentioned are some of the utility URLs for accessing the 'Whois' record.

https://in.godaddy.com/whois
https://lookup.icann.org/
https://whois.net/
http://whois.domaintools.com/
https://manytools.org/network/online-whois-query/
www.centralops.net

II IP LOOKUP

IP Address:
An IP address is a unique address that identifies a device on the internet or a local network. IP stands for “Internet Protocol,” which is the set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

How are IP Address assigned?

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.
IP addresses are not random. They are mathematically produced and allocated by the Internet Assigned Numbers Authority (IANA), a division of the Internet Corporation for Assigned Names and Numbers (ICANN).

Various tools for IP Lookup:

https://www.ip2location.com/dem/ https://whatismyipaddress.com/ip-looup Tools for bulk IP lookup: https://www.showmyip.com/
https://www.infobyip.com/ipbulklookup.pp

II. TOOL TO CHECK WHETHER A MAIL IS COMPROMISED

HaveIbeenPwned
If you suspect that any complainant account has been compromised, hacked, this is the perfect tool. It can track down web compromise from many sources like Gmail, Hotmail, Yahoo accounts, as well as LastFM, Kickstarter, Wordpress.com, Linkedin and many other popular websites.

Firefox Monitor
The browser developer Mozilla has offered a web tool you can use to check whether any complainant email has been hacked.
You enter the e-mail address and then click on “Search Firefox Monitor”. After a short while, you will receive a message stating whether the e-mail account has been hacked or if the address has been affected by known data leaks.

III. TOOL TO GET SPECIFIC INFORMATION IN GOOGLE SEARCH

Google Dorks

A Google Dork query, sometimes just referred to as a dork, is a search string that uses advanced search operators to find information that is not readily available on a website. In other words, we can use Google Dorks to find vulnerable websites, servers and discover hidden information buried deep in online databases. Since Google has a searching algorithm andindexes most websites, it can be useful to a hacker to find vulnerabilities on a target.

The basic syntax for advanced operators in Google is: operator_name:keyword

Most common dork commands:

intitle – This allows a hacker to search for pages with specific text in their HTML title. So intitle: “login page” will help a hacker scour the web for login pages.

allintitle – Similar to the previous operator, but only returns results for pages that meet all of the keyword criteria.

inurl – Allows a hacker to search for pages based on the text contained in the URL (i.e., “login.php”).

allinurl – Similar to the previous operator, but only returns matches for URLs that meet all the matching criteria.

filetype – Helps a hacker narrow down search results to specific files such as PHP, PDF, or TXT file types. ext – Very similar to filetype, but this looks for files based on their file extension.

intext – This operator searches the entire content of a given page for keywords supplied by the hacker.

allintext – Similar to the previous operator but requires a page to match all of the given keywords.

site – Limits the scope of a query to a single website.

Examples of dork queries:

1. To search within social media sites, use the symbol @ followed by a social media name; then enter a colon in your search query. For example, enter @facebook:keyword to search for the term keyword within Facebook.

2. To search for hashtags, put a # sign before your search term. For example, enter #USAelection.

3. To search for the unknown words, use the asterisk (*) to substitute it with one or more words.
For example, enter data hiding in *.

4. Use the keyword map: followed by location name, and Google will show you map-based results.

For example, enter map:New York.

Chapter 3

SOCIAL MEDIA INVESTIGATION

I. INTRODUCTION TO SOCIAL MEDIA

Social networking is one of the leading online activities worldwide. In 2020, experts estimate 2.95 billion people to access social networks regularly. Most of this growth is projected to come from mobile devices, as emerging markets catch up on online connectivity. Social networking is one of the most popular ways for online users to spend their time, enabling them to stay in contact with friends and families as well as catching up with news and other content.

Social networking allows users to create an online profile through which they will share or post personal and professional information about them. This includes pictures, videos, and other personally identifiable information. Undoubtedly, social media is becoming the scene of the crime in many types of emerging crimes.

II. DIFFERENT TYPES OF CRIMES REPORTED ON SOCIAL MEDIA

Below you'll find four common crimes being committed on, or as a result of, social media.

Creating Impersonating/Fake accounts on Social Media

Impersonating/Fake profiles on social media like Facebook, google plus, twitter etc. is a problem that most of the users face in their daily life. Creating fake accounts or impersonating accounts is a punishable offense. In most of the cases, the purpose of making an impersonated social media profile is to harass and defame the victim. Fake accounts are created to commit the crimes such as cyberstalking, cheating, post defamatory images, post defamatory articles against an individual, organization or government, create communal hatred contents, create hoax information etc.,

Fake Profile

Cyber Stalking & Cyberbullying

Cyberstalking refers to foster personal interaction repeatedly targeting a person despite the clear indication of disinterest by such person. Cyberbullying is the use of technology to harass, threaten, embarrass or target another person.

Cyber Bullying

Buying Illegal Things

Social media allows creating closed groups, communities of like-minded people on many social media networks to discuss events, the topic of interest. This is also an opportunity for many sellers to come online and sell contraband items, alcohol, arms, fake goods such as sports shoes, watches, sunglasses, designer wear, gadgets bags of famous brands etc.,

Illegal Purchase

III. SOCIAL MEDIA MONITORING AND INTELLIGENCE PLATFORMS

It is very vital to understand how social media is changing and so the cybercrimes committed through social media and their impact on one's life. Perpetrators commit crimes without hesitation, whereas, in real life, they have to assume the power of consequences bears a heavier weight.

How does Social Media Monitoring work?

As opposed to traditional forms of monitoring, social media monitoring is real-time and continuous. Social media monitoring can be performed in two ways.

· The first involves feeding the algorithm with a string of keywords, which leads to "producing an overview of the instances of online communication and their locations (forums, Facebook pages, Twitter accounts, etc.) in which these keywords are used".

· The second way entails directing the algorithm towards a specific set of discussion forums and social networking sites, and to search them for a number of keywords.

IV. SOCIAL MEDIA MONITORING TOOLS

There are two types of tools available to monitor social media:

1. Sentiment analysis: Sentiment analysis refers to the class of computational and natural language processing study of people's opinions, appraisals, and emotions toward events, institutions or other subject matter in order to extract subjective information, such as opinions expressed in a given piece of text.
2. Social network analysis: Social network analysis is a technique used to map and measure social relations. They are used as investigative tools to discover, analyse, and visualize the social networks of criminal suspects.

Sentiment analysis

Social Network analysis

V. INVESTIGATION PROCEDURES ON SOCIAL MEDIA

The most common crimes in social media are, Impersonation by identity theft, creating fake account, uploading content viz private photos/ videos with contact number details, spreading fake news/ rumour, defaming or harassing or abusive postings, posting online shopping message with the intent to cheat, trolling and threat for ransom messages.

Finding the culprit from fakes news on social media

STANDARD OPERATING PROCEDURES – FACEBOOK/ INSTAGRAM/ TWITTER

STEP 1: Collect the suspected URL of the accused/ victim social media profile. Example:

FACEBOOK	INSTAGRAM	TWITTER
www.facebook.com/ctoviswa	www.instagram.com/xxxxxxxx	www.twitter.com/abcabcabc123

STEP 2: Open the Social media account and collect screenshot and URL. In case of fake/ impersonated profile mention both the suspect and victim's original URL.

STEP 3: A legal notice u/s 91 CRPC addressing the respective Social media mentioned below has to be sent on our official letterhead duly signed by the authorised signatory and sealed with the official seal.

FACEBOOK	INSTAGRAM	TWITTER
Meta Platforms, Inc. 1601 Willow Road, Menlo Park, CA 94025.	Meta Platforms, Inc. 1601 Willow Road, Menlo Park, CA 94025.	, Twitter, Inc. c/o Jeremy Kessel 1355 Market Street, Suite 900, San Francisco, CA 94103, United States

STEP 4: Send the scanned copy of the notice to the respective online portals mentioned below from Government mail ID.

FACEBOOK	https://www.facebook.com/records/login
INSTAGRAM	https://www.facebook.com/records/login
TWITTER	https://legalrequests.twitter.com

STEP 5: For content removal send notice u/s 79(3)(b) of IT Act.

STEP 6: After collecting IP logs along with date and time – convert the Time Zone to IST using www.thetimezoneconverter.com

STEP 7: Identify the Internet Service Provider of the given IP logs using www.whois.domaintools.com website.

STEP 8: After receiving the IP details from the legal team of the particular Social media platform, send request to the Internet Service Provider along with IP address, date, time (converted time zone IST) and request for IP user details for the given IP Address.

STEP 9: ISP (Internet Service Provider) will provide the IP User details like suspect Phone Number, CDR, location etc.,

STEP 10: Field Enquiry/ Physical verification.

STEP 11: Result of Investigation/ Enquiry: Removal of account, Deletion of post.

STANDARD OPERATING PROCEDURES – GOOGLE/ YAHOO/ MICROSOFT OUTLOOK

STEP 1: Collect the mail IDs of the sender/ victim. Example: artimishra@gmail.com

STEP 2: Address a mail request in the prescribed format to concerned service provider to collect the sender/ suspect mail ID.

STEP 3: The legal request should be sent to below mentioned email ID addressing to respected Nodal officer on our official letterhead duly signed by the authorised signatory and sealed with the official seal, send the scanned copy of the request

GMAIL	YAHOO	MICROSOFT
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Yahoo India Private Limited, Unit No. 304 3rd floor, Satellite Gazebo, East Wing, Guru Hargovindji Marg, (AG Link road), Andheri (East), Mumbai – 400093	Microsoft Corporation, Law Enforcement National Security Redmond, WA, USA
gitanjli@google.com lis-apac@googl.com	In-legalpoc@oath.com	indiacc@microsoft.com, domains@microsoft.com

STEP 4: In case of Google products, send notice to google LERS and get account information and IP logs.

STEP 5: After collecting IP logs along with date and time – convert the Time Zone to IST using www.thetimezoneconverter.com

STEP 6: Identify the Internet Service Provider of the given IP logs using www.whois.domaintools.com website.

STEP 7: Send request to the Internet Service Provider along with IP address, date, time (converted time zone IST) and request for IP user details for the given IP Address.

STEP 8: ISP (Internet Service Provider) will provide the IP User details like suspect Phone Number, CDR, location etc.,

STEP 9: Field Enquiry/ Physical verification.

STEP 10: Result of Investigation/ Enquiry: Identify the accused/ suspect based on the verification and arrest the accused and seize the evidence (materials) used to commit offence.
Note: The legal team of the intermediary receives the complainant's personal ID proofs, Aadhar card, PAN Card, any residential proof to delete the alleged Instagram account.

STANDARD OPERATING PROCEDURES – WHATSAPP

Some common crimes in Whatsapp are Spreading fake news, threat for ransom, impersonation by identity theft, non whatsapp user phone numbers are used for whatsapp by the fraudster and post inappropriate things in the whatsapp status, violating the misuse of profile picture privacy of someone, blackmailing, obscene comments in whatsapp.

STEP 1: Collect the suspected Whatsapp number of the accused/ suspect.
Example: +134-698-623, +917854608569

STEP 2: Collect screenshot of the message sent by accused.

STEP 3: Prepare a legal notice u/s 91 CRPC to

Law Enforcement Response Team,
WhatsApp LLC
1601 Willow Road
Menlo Park, California 94025
United States of America.

addressing the respective Social media and the request has to be sent on our official letterhead duly signed by the authorized signatory and sealed with the official seal.

STEP 4: Sign and seal the Notice and send the scanned copy to the Nodal officer from the Government email ID to online portals https://www.whatsapp.com/records/. In case of emergency like life threat, kidnapping, suicide attempt emergency request must be sent to the legal portal of the whatsapp company.

STEP 5: After collecting IP logs along with date and time – convert the Time Zone to IST using www.thetimezoneconverter.com

STEP 6: Identify the Internet Service Provider of the given IP logs using www.whois.domaintools.com website.

STEP 7: Send request to the Internet Service Provider along with IP address, date, time (converted time zone IST) and request for IP user details for the given IP Address.

STEP 8: ISP (Internet Service Provider) will provide the IP User details like suspect Phone Number, CDR, location etc.,

STEP 9: Field Enquiry/ Physical verification.

STEP 10: Result of Investigation/ Enquiry: Removal of account, Deletion of post. The accused person will be arrested after the physical verification based on the IP user details.

STANDARD OPERATING PROCEDURES – YOUTUBE

STEP 1: Collect the suspected URL of the accused/ victim social media profile.
Example: https://www.youtube.com/watch?v=QVEp781Welg

STEP 2: Prepare a verbatim by converting the video content in written format in the language spoken in the said video.

STEP 3: Address a mail request in the prescribed format to YouTube nodal officer to collect IP logs of the accused/ suspect YouTube Channel.

STEP 4: For content removal send notice u/s 79(3)(b) of IT Act.

STEP 5: A legal notice should be sent from Government mail ID to YouTube portal https://support.google.com/youtube/contact/yt_gov_india on official letterhead duly signed by the authorized signatory and sealed with the official seal. YouTube, 901, Cherry Ave, San Bruna, CA 94066, USA, legal@support.youtube.com, lis-apac@google.com.

STEP 6: After collecting IP logs along with date and time – convert the Time Zone to IST using www.thetimezoneconverter.com

STEP 7: Identify the Internet Service Provider of the given IP logs using www.whois.domaintools.com website.

STEP 8: Send request to the Internet Service Provider along with IP address, date, time (converted time zone IST) and request for IP user details for the given IP Address.

STEP 9: ISP (Internet Service Provider) will provide the IP User details like suspect Phone Number, CDR, location etc.,

STEP 10: Field Enquiry/ Physical verification.

STEP 11: Result of Investigation/ Enquiry: Removal of videos, Deletion of Channel. The accused person will be arrested after the physical verification based on the IP user details.

NAME	TYPE	DESCRIPTION
Advanced Application for social media Analytic	Free*	Advanced Application for Social Media Analytics (AASMA) is the tool for social media monitoring and analysis. It is developed at IIIT Delhi and funded/supported by Ministry of Electronics and Information Technology (MeitY)
X1 Social discovery	Commercial	Ability to collect and search data from social networks and the Internet.
Maltego	Commercial/ Freeware available with limited caps	It is an open source intelligence gathering tool capable of a significant amount of information gathering about a prospective target
Amped Authenticate	Commercial	Amped Authenticate is a software package for forensic image authentication and tamper detection on digital photos. Authenticate provides a suite of different tools to determine whether an image is an unaltered original, an original generated by a specific device, or the result of a manipulation with a photo editing software.
Hootsuite	Commercial	Social media management platform. The system's user interface takes the form of a dashboard, and supports social network integrations for Twitter, Facebook, Instagram, LinkedIn, Google+, YouTube etc.,
SocialPilot	Commercial	Measure your social media page's performance by understanding the growth of your fans/audience. Also, understand what content works the most with users from social networking audience. It provides insights for Twitter, Facebook, Instagram, LinkedIn, Google+, YouTube etc.,
Netglub	Open source	Open source tools for information gathering. It collects open data like DNS name, Domain name, IP address, IP Sub network, Message Exchanger record, Nameserver Record, URL, Website
Poortego	Open source	Open source tools for visualizing and linking the information available online.

VI. PRELIMINARY INVESTIGATION OF CYBER HARASSMENT CASES

STEP 1: Obtain a detailed description of the incident as well as the time of occurrence of incident from the complainant.

STEP 2: Ask the complainant if he or she knows who is sending the harassing messages. If he/she knows the suspect then Investigation Officer (IO) may ask for information about the suspect: name, age, address, telephone number, vehicle information, and relationship to victim.

. Web page images
· Mailing list messages

STEP 3: Ask the complainant, if he or she knows the reason why he or she is being harassed. If so, record the complainant's explanation.

STEP 4: If there is any communication in between the complainant and the harasser, collect the copies of the responses. It is necessary for the investigation.

STEP 5: Ascertain when and how the harassment began. Find out if it has happened only via the Internet (e-mail messages, chat rooms, mailing lists, instant messages, Web site) or through telephone calls, cell phone calls or texts, postal letters as well.

STEP 6: Determine whether the complainant has been threatened with violence, rape, and even death. The Investigating officer needs to establish the details of how these threats were communicated.

- Chat room messages
- Message Board messages
- Instant messages
- Phone conversation recordings
- E-mail messages and e-mail headers
- Text Messages
- Social network messages/wall posts

STEP 7: Obtain a copy (hard/soft) of the messages for the case file showing the e-mail address, Website URL and the content(s) of the message(s). If he or she has any of the following material evidence, collect them. Hard copies of the screenshot taken should be signed by the victim.

STEP 8: Secure any physical evidence available and start the chain of custody to protect the evidence from getting tampered. The evidence should be recorded in both paper printouts and electronic files or on an electronic media such as a disk or CD/DVD-ROM.

STEP 9: After getting the relevant details and identifying the category of crime, IO shall register the FIR under section 154 Cr.P.C .

STEP 10: Further proceed with the investigation steps based on the Standard Operating Procedures.

Chapter 4

COMMUNICATION DEVICE BASED INVESTIGATION

I. COMMUNICATION DEVICE

As per IT Act, “communication device" means cell phones, personal digital assistants or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.

II. CELLULAR NETWORKS

Cellular networks provide coverage based on dividing up a large geographical service area into smaller areas of coverage called cells.

As a mobile device moves from one cell to another, a cellular arrangement requires active connections to be monitored and effectively passed along between cells to maintain the connection. To administer the cellular network system, data about the service contract and associated service activities is captured and maintained by the network system. The main components are
Radio Transceiver Equipment: Communicates with mobile devices

Controller: Manages the transceiver equipment and performs channel assignment
Mobile Switching Centre (MSC): Manages overall communications throughout the cellular network, including registration, authentication, location updating, handovers, and call routing.

Home Location Register (HLR): It is the central repository system for subscriber data and service information.

Visitor Location Register (VLR): Another database, used for mobile devices roaming outside of their service area.

Account information, such as data about the subscriber (e.g., a billing address), the subscribed services, and the location update last registered with the network are maintained at the HLR and used by the MSC to route calls and messages and to generate usage records called Call Detail Records (CDR).

III. INFORMATION OBTAINED FROM THE NETWORK SERVICE PROVIDER

· Subscriber name and address
· The phone number associated with SIM
· Billing account details
· Call Data Record
· ICCID – Integrated Circuit Card ID
· IMSI – International Mobile Subscriber Identity
· PUK (Personal Unlocking Key) for the SIM.
· Tower Location (BTS Address)
· Subscribed Services (Voice Mails, Caller-tunes, Classifieds, etc.)

IV. LAWS RELATED TO INTERCEPTION

Lawful interception of telephonic communication is governed by the provisions of Section5(2) of the Indian Telegraph Act, 1885.

Authorisation of agency of Government:

The competent authority may authorize an agency of the Government to intercept, monitor or decrypt information generated, transmitted received or stored in any computerresource for the purpose specified in sub-section (1) of section 69 of the Act.

How to seek information from a Mobile Service Provider?
Information from mobile service provider can be requested with the help of a 91 / 92 Cr.P.C. notice with a respective phone number or IMEI number. The service provider willrespond with a Call Detail Record (CDR) if it is available in his network. The service provider will be unable to handover CDR if the suspect has opted for Mobile Number Portability (MNP). The following details can be obtained from the MSP,

· Call Detail Record (CDR)
· Subscriber Detail Record (SDR)
· Customer Application form (CAF)

V. CALL DETAIL RECORD (CDR)

A Call Data Record (CDR) is a detailed record of SMS and calls that are sent and received by a subscriber of a service provider. It provides a wealth of information which can help in identifying suspect's day location, night location, handset details, maximum contacted number, date, time, tower location etc.,

VI. CDR FORMATS

The service provider does not have a guideline on which format has to be given to the requestor. All the formats are auto generated by the systems at service providers and can be emailed by the nodal agency /officer of that particular Mobile Service Provider (MSP). The CDR can be given in following formats,

- Text (plain text)
- Html (hypertext markup Lang)
- .xls (Excel file format)
- .csv (comma-separated value)- flat file
- .pdf (portable document format)

There are many investigation data sources that can be obtained from the service provider like:

- Cell phone details
- Tower info (TDR)
- Landline call details International call details (call route through a gateway)
- Subscriber details
- Cell phone forensic tools
- SIM card data extraction
- Telephone interception records

VII. CDR ANALYSIS

The following are the steps to perform a basic CDR analysis using MS-excel. The CDR obtained from the service provider is in the CSV format.

STEP 1: Open the CSV file in MS-excel

STEP 2: Convert the .CSV file to .XLS file for analysis using save as option.

Calling No	Called No	Cdr no	other no	Date	Time	Dur(s)	Cell1	Cell2	Call Type	IMEI	IMSI No	Type	SMSC	Roam Nw
[redacted]	[redacted]	[redacted]	=A2&B2	01-Nov-16	00:09:58	45	21791_634	21791_634	OUT	8.69E+14	4.04E+14	PRE	-	KK-0
				01-Nov-16	08:32:41	45	21791_634	21791_634	IN	8.69E+14	4.04E+14	PRE	-	KK-0
				01-Nov-16	09:10:21	20	21791_634	21791_634	OUT	8.69E+14	4.04E+14	PRE	-	KK-0
				01-Nov-16	09:11:24	180	21791_634	21791_634	OUT	8.69E+14	4.04E+14	PRE	-	KK-0
				01-Nov-16	10:30:20	70	21791_307	21791_307	IN	8.69E+14	4.04E+14	PRE	-	KK-0

STEP 3: Remove merged cells or additional cells (Detailing service provider, needs no signature etc.)

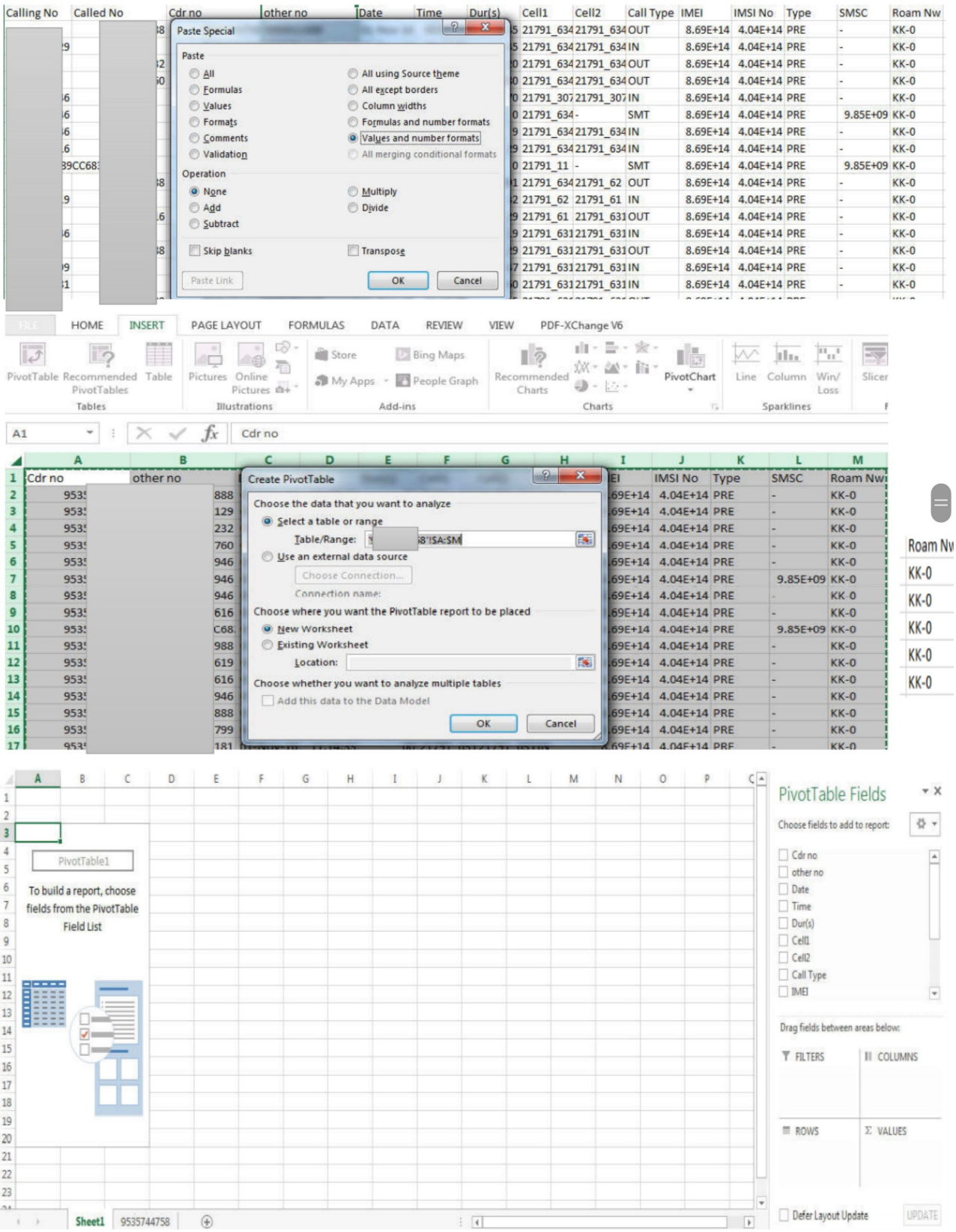
STEP 4: Insert two columns after Calling No, Called No (Column c & column D) and copy CDR number in column C and leave the column D empty you can mention CDR no as heading in column C and Other no as heading in Colum D as shown below

STEP 5: Select Calling No and Called No (Column A & column B) and press control and H key simultaneously. Copy the CDR number in Find what field and replace with Space.

STEP 6: In column D or Other No use this formula (=a2&b2) and press enter. Double clicking on the edge of the green box inserts the number to all the columns till the end of the CDR.

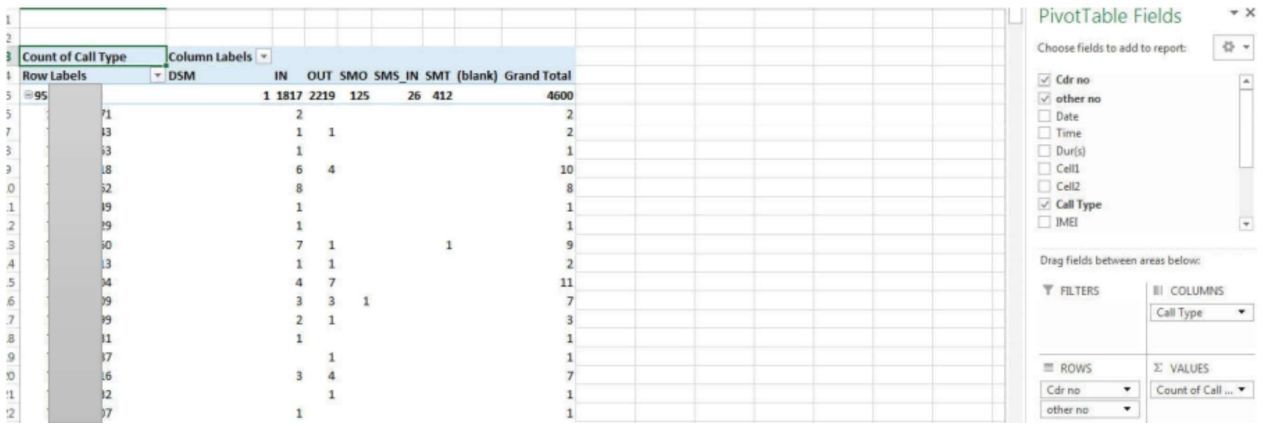
STEP 7: Right click on column D and copy the entire column and again right click on the same column you will get an option of paste special. Select paste special and select values and number formats as shown below

STEP 8: Select the entire sheet and select insert option and click on the pivot table and the following option shown below appears. Click ok.



STEP 9: The following sheet will open in your xls sheet.

STEP 10: Select CDR no and other number, Drag and drop both numbers on Rows.



Count of Call Type	Column Labels							
Row Labels	DSM	IN	OUT	SMO	SMS_IN	SMT	(blank)	Grand Total
95		1	1817	2219	125	26	412	4600
	71		2					2
	43		1	1				2
	63		1					1
	18		6	4				10
	62		8					8
	49		1					1
	29		1					1
	60		7	1			1	9
	13		1	1				2
	84		4	7				11
	09		3	3	1			7
	99		2	1				3
	81		1					1
	37			1				1
	16		3	4				7
	82			1				1
	07		1					1

PivotTable Fields

Choose fields to add to report:

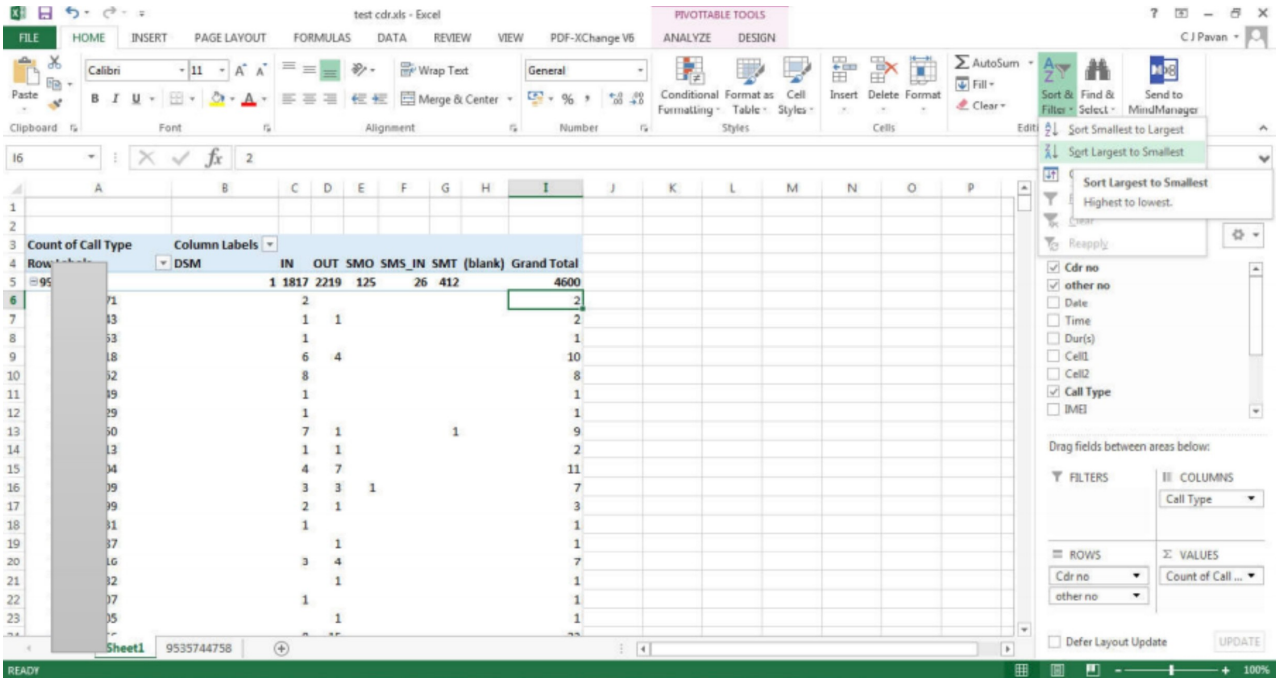
Cdr no
other no
Date
Time
Dur(s)
Cell1
Cell2
Call Type
IMEI

Drag fields between areas below:

FILTERS | COLUMNS: Call Type | ROWS: Cdr no, other no | VALUES: Count of Call ...

Select call type and drag and drop on values, select call type again and drag and drop in column.

STEP 11: Select any number in the last column (In the below fig “2” is selected) click on home and select sort Largest to Smallest.



Count of Call Type		Call Type							
Cdr No	Other No	DSM	IN	OUT	SMO	SMS_IN	SMT	(blank)	Grand Total
95	95		34	213	4	1	3		255
	94		58	112	3		1		174
	73		57	56			1		114
	96		58	47	1		5		111

STEP 12: The following is the maximum contacted numbers to the CDR number.

VIII. ROLE OF TOWER DUMP ANALYSIS IN INVESTIGATIONS

It is a very important tool of investigation in cases where there is no suspect for a crime and only a few peripheral details are available with the crime investigation agency. The precise reason for any tower dump analysis is to find out the unknown suspects. In short, tower dump is the CDR of a tower.

Example, A major theft of gold worth Rs. 1 crore was reported from the jewellery owner. The CCTV footage was retrieved, however, faces of the suspects were covered.

IX. INTERNET PROTOCOL DETAIL RECORD (IPDR)

IPDR is the record of internet activities of mobile subscribers when they are assigned with an IP address when they are connected to the internet. An IP data record can tell you a number of things about incoming and outgoing traffic like source and destination IP address, Ports, time of access. A sample is shown below.

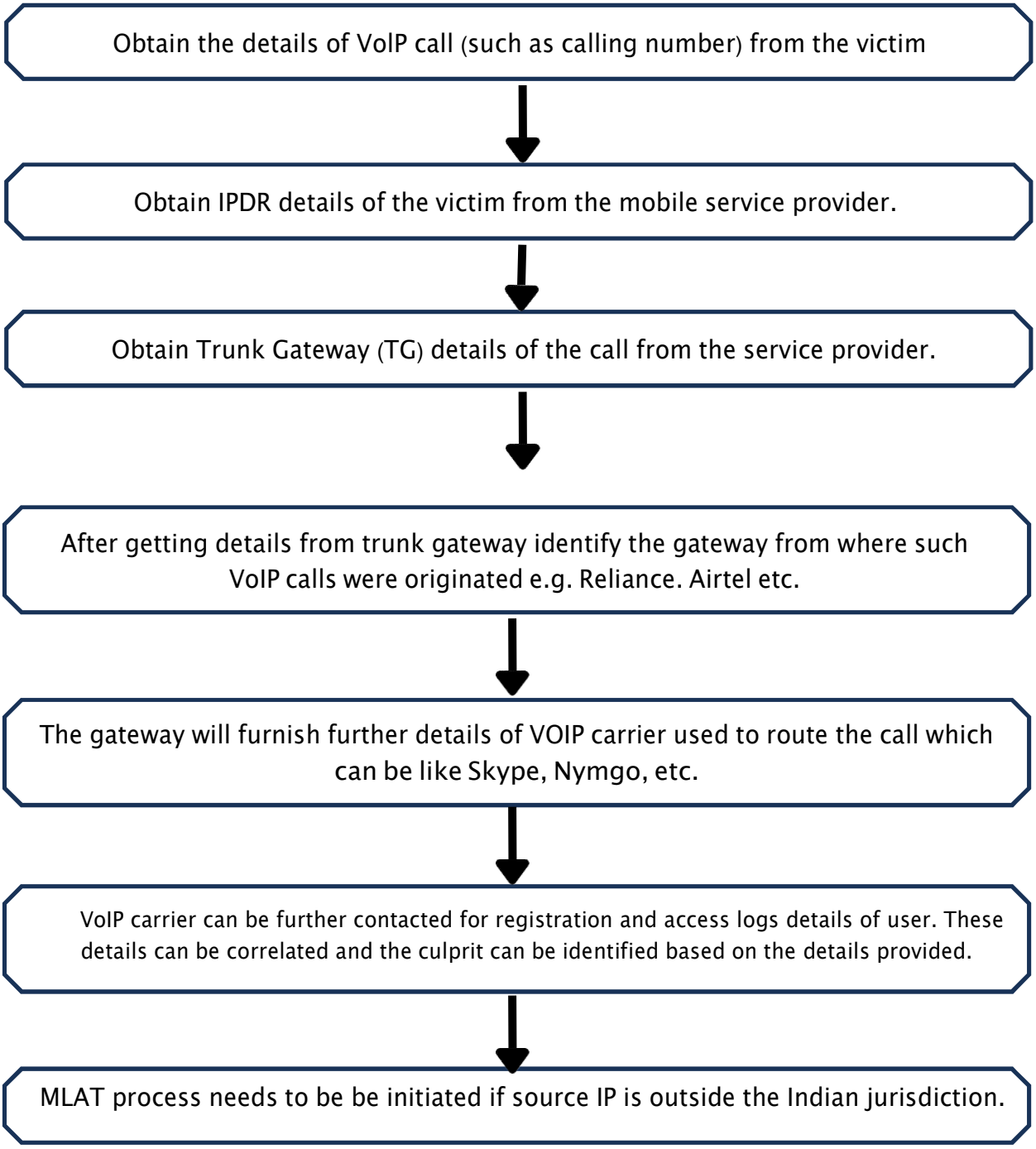
PRIVATEIP	PRIVATEPORT	PUBLICIP	PUBLICPORT	DESTIP	DESTPORT	MSISDN	IMSI	START_DA	START_TI	END_DATI	END_TIME	IMEI	CELL_ID
10.1	56614	1.	43452	50.	5222	9.19737E+11	4.06E+14	#########	04:11:47	########	19:27:11	3.52E+15	4.06E+15
10.2	33073	1.	4267	216	443	9.18377E+11	4.04E+14	#########	14:22:08	########	15:48:08	3.52E+15	4.04E+14
10.2	33073	1.	4267	216	443	9.18377E+11	4.04E+14	#########	14:22:08	########	16:04:10	3.52E+15	4.04E+14
10.2	43764	1.	1539	31.	443	9.18586E+11	4.04E+14	#########	15:34:47	########	15:38:19	3.58E+15	4.04E+14
10.2	43766	1.	55865	31.	443	9.18586E+11	4.04E+14	#########	15:34:47	########	15:38:19	3.58E+15	4.04E+14

X. VOICE OVER IP (VOIP) BASED INVESTIGATIONS

Voice over IP (VOIP) technology enables the transfer of voice and multimedia content over Internet Protocol (IP) networks. Voice over Internet Protocol (VoIP) is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. In simple words, VoIP is basically a telephone connection over the Internet.

Voice over IP has made the communication easier and cheaper and with the introduction of lower fares for 3G/4G services, there has been a spurt in the number of mobile applications which make people capable of making voice calls using the data services. VoIP can be used for fraud purpose as it is difficult to detect frauds committed using VoIP calls.

XI.INVESTIGATION OF VOIP



STANDARD OPERATING PROCEDURE

For instance, if a Cybercrime police station received a complaint from a complainant that he has received a threatening call on his mobile. The number displayed on complainant mobile was +177777.

STEP 1: Send a request for CDR of the complainant's cell number for the said period and check if the same number was found even in the CDR

STEP 2: Ask the Mobile Service Provider to provide an incoming gateway of that particular call.

STEP 3: Search for the originating telecom company which was based out of India.

STEP 4: Contact the company through e-mail from the cybercrime police station.

STEP 5: The received response from them has the following details.

- Name
- Email
- IP from where he created an account
- Last Login
- Phone Number

STEP 6: The IP was traced outside India. However, obtain the e-mail logs from the Email Service Provider and if the IP address belonged to Indian Service Provider.

STEP 7: A notice should be sent under 91 CrPC to obtain the physical address of the IP.

STEP 8: Arrest the suspect.

Chapter 5

MOBILE FORENSICS

I. INTRODUCTION TO MOBILE FORENSICS

Internet and mobile phones are the most used technology in the world. A mobile phone stores a wide array of personal data such as pictures, images, videos, call logs, SMS, e-mails and data pertaining to various applications installed etc. The penetration of smartphones in our daily lives has enabled communication as well as other cyber and network related works such as banking, shopping, paying bills, booking travel tickets etc. However, it has also provided easy avenues to commit cyber-frauds leading to increase in forensic cases.

II. DEFINITION

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

Mobile phone forensics is the utilization of scientific methodologies to recover data stored by a mobile phone for legal purposes

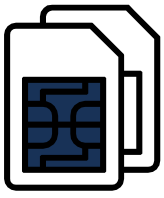
III. MAJOR MOBILE PHONE RELATED CYBER CRIMES

- Threatening/ Harassing through call or message

- VOIP

- Vishing

- Stalking



- Fraudulently Obtaining Duplicate SIM of Victims

IV. EVIDENCE IN MOBILE DEVICES

1) Evidence that can be extracted from a Traditional Mobile Device

Hardware
- Handset make, Model, Serial Number
- International Mobile Equipment Identity (IMEI)

User-created evidence
- Address book
- Message logs (SMS, MMS) – sent, received deleted
- calendar
- memos, to-do lists, notes

Mobile Device created evidence
- Call logs - Calls received, dialled numbers, missed calls, etc.
- Deleted calls, service SMS etc.

2) Evidence that can be extracted from a smartphone

User Created evidence
- Photographs (including EXIF metadata); video/audio; maps
- MMS, GPS waypoints; stored voicemail

Internet-related evidence
- Online accounts; purchased media (often discoverable in embedded metadata)
- Email content; Internet usage; social networking information, etc.

Third party installed apps
- Alternate messaging and communication systems; additional capabilities; malware applications;

e-commerce applications etc.,
- Chat Logs, spoofing apps, VPNs etc.

3) Evidence related to the intermediaries (Mobile Service Provider)
- CDR
- CAF
- IMEI
- IMSI
- Location
- PUK

V. TYPES OF MEMORY ON MOBILE PHONES

1. Mobile Phone Internal Memory: it is also called as phone main memory.
2. Mobile Phone External Memory: The size of the secondary memory depends on the support provided by the handset manufacturer. Few smartphone models support till 2TB of external memory.
3. Subscriber identity module (SIM): It is a smart card that stores data for GSM cellular telephone subscribers. Such data includes user identity, location and phone number, network authorization data, personal security keys, contact lists and stored text messages.
4. Cloud storage: Users can store data on cloud storage as well. For e.g., Once a user registers with Gmail, the user is entitled to get 15GB free google drive space where the user can store pictures, video, synchronized data of WhatsApp etc.,

VI. TECHNIQUES OF MOBILE FORENSICS

Physical acquisition implies a bit-by-bit copy of an entire physical store (e.g., a memory card, internal memory, SIM card).
Logical acquisition implies a bit-by-bit copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a file system partition).

VII. LIST OF MOBILE FORENSICS TOOL

S.No.	ITEM	PURPOSE
1	Cellebrite UFED 4PC with Chinex	Standalone mobile forensic extraction device and software's that combines multiple mobile device support with universal data extraction technology to perform physical, file system and logical extractions of all data from the widest range of mobile devices.
2	Oxygen Forensics Detective	
3	MOBILedit Forensic express	
4	Elcomsoft iOS Forensic Toolkit/ Elcomsoft Phone Breaker	
5	XRY Physical/Logical	
6	MOBILedit Forensic	
7	Paraben's Device Seizure	
8	Access Data MPE+	
9	Logicube CellXtract	
10	Berla Blackthorn	GPS forensics

VIII. CHALLENGES IN EXTRACTION OF FORENSIC EVIDENCE FROM COMMUNICATION DEVICES

Mobile forensics is dynamic in nature, where there are no standards and every device is proprietary with different operating systems. As phones tend to have embedded operating systems, generally you have to turn them on to recover the data, which is not the same as computer forensics. The challenges will grow as the technology advances.

· Getting smaller and using complex hardware.
· Huge diversity of Operating systems.
· No standard protocol for data extraction.
· Encryption
· Different Data Cables and Data Communication Ports
· Made in China Phones
· Cloud storage

IX.INVESTIGATIVE PROCEDURES

Investigative methods are procedures the investigative team can apply, which require no forensic software or hardware tools. The most obvious methods are listed below.

Ask the owner – If a device is protected with a password, PIN or other authentication mechanism involving knowledge-based authentication, the owner may be queried for this information during an investigation.

Know the service provider – Unstructured Supplementary Service Data (USSD) sometimes referred as short codes can be used by dialing these codes on the mobile phones of suspects and victims to find out their mobile numbers.

Some indicative codes are listed below

SERVICE PROVIDER	CODE
Airtel	*121*1# or *121*9#
Vodafone	*111*2#
Idea	*131*1#
BSNL	*222# OR *888# OR *1# OR *785# OR *555#
Reliance mobile	*1#

Mobile forensic Process – The mobile forensics process aims to recover digital evidence or relevant data from a mobile device in a way that will preserve the evidence in a forensically sound condition.

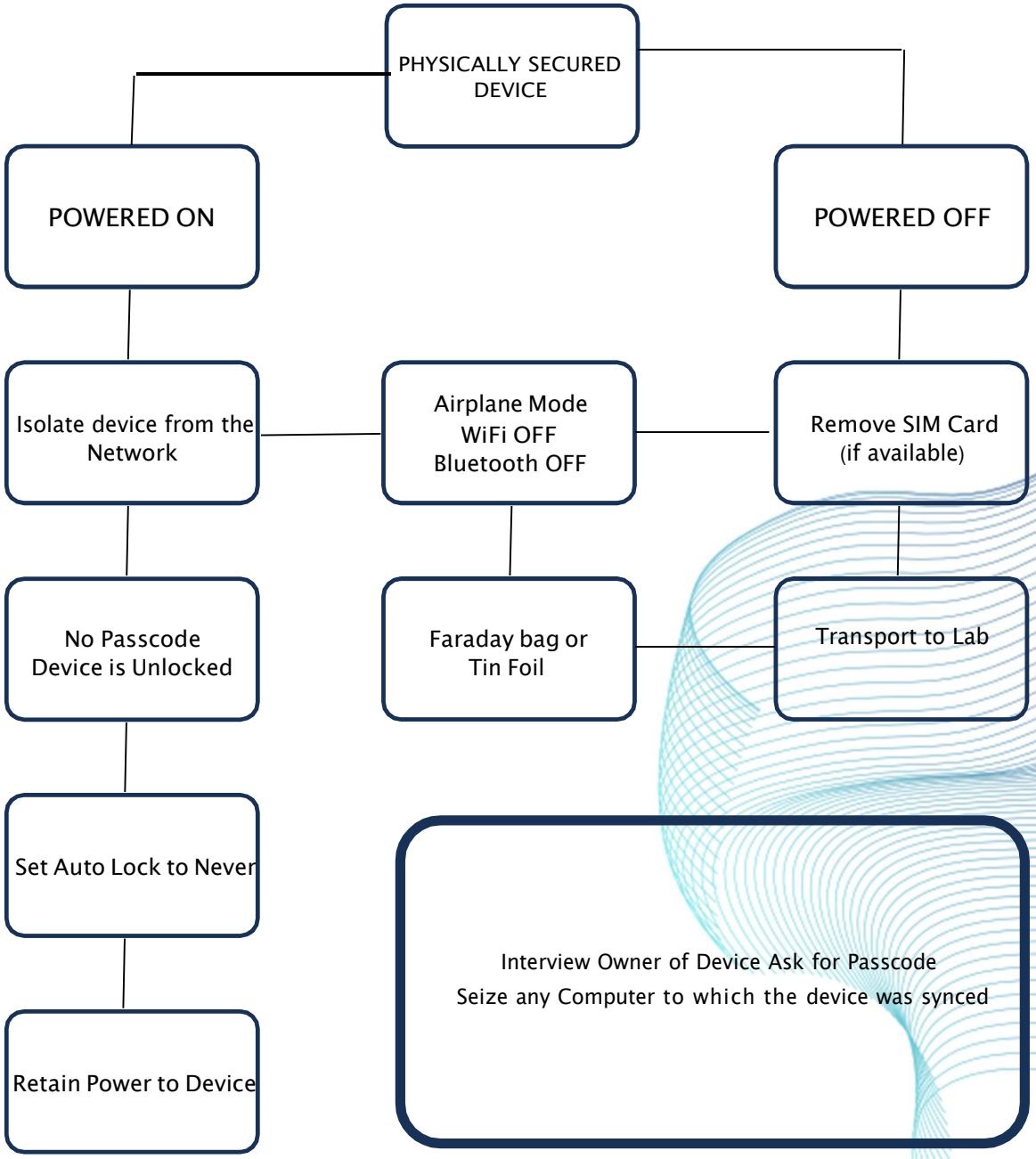
X. STEPS INVOLVED IN THE ANALYSIS OF MOBILE DEVICES

1. Identification is the process of identifying the mobile device in scene of crime or through IMEI lookup in CDR.
2. Isolation of mobile device from external communication is very important to avoid further logging of calls and messages after seizure which may lead to loss of critical evidence.
3. Documentation of each and every aspect of procedures followed in seizure of mobile is also very important.
4. Labelling: It's very important to label the number of devices, memory cards, SIM cards mobile phone cover, if any and other relative accessories while seizure.
5. Charge the battery to its full capacity before sending it to the forensic examination. The forensic experts can directly start acquisition of mobiles without charging the phones making the analysis of devices less time consuming.
6. Preservation without changing the data integrity is also very important in after acquisition.

XI. PRECAUTIONS TO BE TAKEN BEFORE AN INVESTIGATION

· Occasionally, there may be a need to conduct traditional forensic processes on a mobile phone (e.g., DNA and latent prints).
· Isolate the mobile device by switching off the phone or use the flight mode option if available.
· Take photos of the crime scene which include cell phones, wires, connectors, etc.
· Search for papers, sticky-notes, diaries and any other evidence which may give out passwords or other vital information.
· Label all the wires, connectors and devices and bag them with evidence.
· Make sure to maintain proper chain of custody details for each evidence items seized.

XII. PROCEDURE FOR ACQUISITION OF MOBILE PHONE



STANDARD OPERATING PROCEDURE FOR RECOVERING A MOBILE DEVICE FROM A SCENE OF CRIME

STEP 1: Use hand gloves or other clean sterile cotton cloth while recovering the mobile device from the scene of the crime.

IF CELL PHONE IS SWITCHED ON

STEP 2: If the phone is in on condition, keep the device isolated by selecting flight mode option. If the flight mode option is not available use the faraday bag to isolate the phone. If the faraday bag is also not available wrap the mobile in aluminium foil.

STEP 3: Mobile device should be plugged to a power bank so that the device does not switch off.

STEP 4: If the mobile device is synced to a computer or laptop and data transfer is occurring, do not pull the phone away from the computer / laptop as data in transfer will be lost.

STEP 5: Send the phones to Forensic experts i.e. FSL and CFSL for recovering physical (e.g. finger prints, DNA) and digital evidence (e.g. call logs, SMS etc.) associated with the phone.

IF CELL PHONE IS OFF

STEP 2: Remove Battery and Take a photo of the position of SIM(s)

STEP 3: Pack Battery, SIM, and Handset separately.

STEP 4: Note Down the details of SIM and Handsets like Make, Model, IMEI, ICCID etc.

STEP 5: If the phone is immersed in a liquid, take the phone out, remove battery, SIM card(s) & also, collect a small quantity of the liquid in which phone was immersed to prove the effect of the liquid on the present state of the phone

STEP 6: Send the phones to Forensic experts i.e. FSL and CFSL for recovering physical (e.g. finger prints, DNA) and digital evidence (e.g. call logs, SMS etc.) associated with the phone.

Chapter 6

INVESTIGATION OF FINANCIAL FRAUDS & CYBER CRIMES

I. INTRODUCTION TO INVESTIGATION OF CYBERCRIMES & FINANCIAL FRAUDS

At present, the banking systems of most countries provide broad enough opportunities for online (remote/distant) management of financial resources. “Customer-Bank”, “Customer-Internet-Bank” and “Telephone Banking” are the most widespread online (remote/distant) banking services. This has created vast opportunities for cybercrime & financial frauds. The Investigation challenge is to collect the required data in time and to co-relate with the suspect.

II. STEPS TO FOLLOW IN CASE OF A FRAUDULENT ONLINE TRANSACTION

1. Collect the bank statement from the concerned bank and identify the fraudulent transactions happened in the statement with the date and time.
2. Request the bank to provide the complete details of fraudulent transactions.

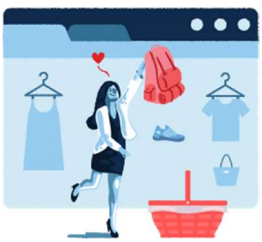
III. INVESTIGATION OF ATM WITHDRAWAL CASES

1. Identify the ATM Location in consultation with the bank.
2. Request for ATM CCTV footage & external CCTV Footages from the bank. Identify other CCTV cameras (If available) in the vicinity of the ATM and collect the same.

IV. INVESTIGATION OF ONLINE TRANSACTION CASES

1. Collect the details of a merchant from the bank and merchant account details.
2. In cases of an e-commerce transaction, contact the e-commerce platforms like flipkart, Amazon, Snapdeal etc., and collect the delivery address, transaction IP, mobile number etc.,
3. In case of wallet transfer, contact the service provider and get the Know your Customer (KYC) details, mobile number, transaction details, and beneficiary details if the money is transferred to a bank account.

Merchant Bank



E-commerce

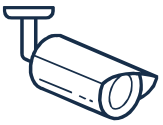
online transaction

V. INVESTIGATION OF BANK TO BANK TRANSFER

Collect the beneficiary account details to which the funds were transferred and request account access IP Logs. Once you receive IP address perform WHOIS lookup of the IP to identify the service provider and issue a notice under 91CrPC to obtain the physical address.

VI. INVESTIGATION TRANSACTIONS INVOLVINGCHEQUES

1. Collect the copy of the cheque from the Bank and enquire in which bank was the cheques withdrawn and collect the CCTV Footage of the same to identify the person who has withdrawn the money using the cheque.
2. If the Cheque has been transferred to another account via normal cheque processing then collect the beneficiary bank account details.



VII. SUMMARY OF COMMON INVESTIGATION STEPS

1. Take the CDR and SDR of mobile numbers associated with the concerned bank account(s).
2. Collect CAF(s) & KYC(s) from Mobile Service Providers (MSP) & Banks
3. Sometimes mobile numbers present in KYC of the bank is different than the registered mobile number for SMS alert. In such cases, collect the CDR, SDR & CAF of the same.

VIII. KEY DEFINITIONS

Customer ID and account number: These are unique numbers that belong to you. A single ID is assigned to you even if you hold more than one account with the bank. However, each account will have a different account number.

Account type: Whether it is a savings or a current account.
Account status: Actively operated accounts are marked 'Regular'. No transaction for six months makes them dormant. To re-activate or make a transaction, the branch has to be contacted.
Nomination: The beneficiaries of your account, especially if held by a single person, are mentioned at the start of the statement. It is important to have a beneficiary as it is difficult to make claims in case of a mishap or the account holder's death.

XIV. KEY ABBREVIATIONS

IFSC: Indian Financial System Code

NEFT: National Electronic Fund Transfer

RTGS: Real-time Gross Settlement Systems

IMPS: Immediate Payment Service

MICR: Magnetic Ink Character Recognition

IB, INF, NEFT, TPT: some banks use the terms 'IB' (internet banking) fund transfer and 'INF' (internet fund transfer). 'NEFT' (National Electronic Funds Transfer) to transfer between two banks and 'TPT' in case of a third party transfer

ATW (NWB/VAT/MAT/NFS): ATM withdrawals. When withdrawals occur at another bank's ATM, a few more abbreviations are added (as shown in the bracket)

VMT: Visa money transfer through ATM

MMT: MasterCard money transfer through ATM

XV. WALLET TRANSFERS

In case of wallet money transfers. Contact the nodal officers of the wallet service providers & obtain registered mobile numbers, IP logs and KYC details, transaction details from them.

- If the money is deposited to bank, collect the beneficiary details.
- In case of e-commerce transaction. Identify the service provider and obtain the account details of the recipient.

XVI. ADVANCE FEE FRAUD

It is when fraudsters target victims to make advance or upfront payments for goods, services and/or financial gains that do not materialize. They deceive victims to deposit money as processing fee or transfer charges or charges for their services etc. Few types of Advance Fee Frauds are explained as follows.

Lottery Scam: It begins with an unexpected email notification, phone call explaining that "You have won!" a large sum of money in a lottery. After contacting the agent, the target of the scam will be asked to pay "processing fees" but will never receive any lottery payment.

Job Offer Frauds: Fraudsters create numerous attractive schemes like easy hire in MNC, high salary etc.

Matrimonial Scam: Fraudsters create fake profiles on leading matrimonial websites for cheating.

Loan Frauds: Scammers are skilled at convincing people that their loan offer is real by communicating e-mail, classifieds online and on newspapers etc., They make fake schemes that is willing to fund without any apparent due diligence.

Some other Advance Fee Frauds are,

QR Code Fraud, Gift Fraud, OLX Fraud

STANDARD OPERATING PROCEDURE FOR INVESTIGATION OF ADVANCE FEE FRAUD

STEP 1: Collect the suspected beneficiary bank account number, IFSC code, date, amount. Beneficiary's mobile wallet, UPI ID, Transaction Id, Google Pay ID, Paytm Number etc.

Example:
If Fraudster use Bank Account Number

S.NO	Account Number	Name	IFSC Code	Amount	Date
1	50200010605210	Priyanka Naik	BDBL0001778	20,000/-	10.06.2020

If Fraudster use Mobile e wallet

S.NO	Fraudster UPI	Google Transaction ID	UPI Transaction ID
1	Suprdaily.razorpay@hdfcbank	CICAgKCnpHMeQ	021218584319

STEP 2: Send notice (u/s 91 CrPC / Bankers book of evidence Act) in the prescribed format to concerned Bank Nodal officer/ Mobile e wallet Nodal officer to collect the Name, address, phone number, email id connected to the suspected Bank account/Mobile E wallet and documents: Account opening form, KYC documents and account statement.

STEP 3: The Legal request should be sent on your official letterhead duly signed by the authorized signatory and sealed with the official seal.

STEP 4: After collecting Bank account statement, KYC Form, address proof, ID proof, Aadhar Number, PAN card, ATM CCTV Clipping, IP logs. Accused can be fixed through further detailed investigation.

STEP 5: Follow the instructions given in circular No.131/COP/GCP/Camp/2021 dated 24-06-2021 regarding seizure and freezing of Account.

XIV. STANDARD OPERATING PROCEDURE TO INVESTIGATE THE ATM CARD SKIMMING CASE

When ATM card is with the customer, he will receive SMS for debit.

STEP 1: Collect the following documents from victim

a) Collect Credit/Debit card number, expiry year & month, bank name
b) Debit message content in victim mobile with ATM location or ATM ID
c) Victim bank account statement, transaction time and date

STEP 2: Action to be taken by investigating officer:

a) Notice /email sent to the local branch to find the ATM location.
b) Notice to concerned bank official for the CCTV footage & pin hole image.
c) Scrutinize all the similar M.O Complaints to fix point of contact.
d) Request the bank concern for the charge back procedure.

STEP 3: ATM Withdrawal

To identify whether the case is ATM skimming or physical theft of the card, identify how ATM withdrawal was made out

a) ATM Pin Misused
b) ATM card lost

STEP 4: Investigation

a) Verify the bank statement and SMS obtained on victim's mobile
b) Send mail to the Victim's bank to get the ATM ID's, Bank Name & Location
c) After getting ATM ID's, send a mail to the concerned bank to get the EJ Log, CCTV, Doom Camera Footages, DVSS footages
d) Verify the time period of money withdrawn to identify the fraudsters
e) Verify the location of phone number used by the fraudster in time with the ATM's location.

XV. STANDARD OPERATING PROCEDURE FOR INVESTIGATION OF CRIMES THROUGH REMOTE DESKTOP APPLICATION

Remote access applications are used legitimately by millions of IT professionals around the world, to remotely connect to their clients' devices and help them with technical issues. However, scammers can try to misuse such apps or any other remote software to connect to your computers or Cellphones to steal data, access codes and even money. Some Remote Desktop Applications are,

- Anydesk
- Quicksupport
- Teamviewer

Methods used by Fraudster

· When a user searches for the contact of customer care of any firm, via, a search engine, he/she finds a contact number which is not the correct number.
· Conmen upload their own numbers, which are displayed in the search results. When users call the number, the Fraudster asks them to download the Remote access app and share the access code. This grants them access to the user's phone or computer.
· Once the Fraudster has remote access, he uses the UPI payment apps installed on the victim's phone to transfer money to his/her own account.
· The Fraudster still needs the one-time-password (OTP) to complete the transaction, which the user provides him, still under the impression that the Fraudster is a customer care personnel. Thus, the fraudster cheats the victim for money.

Investigation

STEP 1: Verify the statement of account, SMS and what type of transactions

STEP 2: CDR to the fraudster's mobile numbers.

STEP 3: If the transaction is done through Wallet/Merchant, Mail to the Wallet/Merchant to block the account and get beneficiary details. Also get CDR for the given register mobile number of Wallet/Merchant.

STEP 4: If the transaction is done through UPI, IMPS, NEFT, RTGS

· Mail to the victim bank with transaction ID (UPI, IMPS, NEFT) to get beneficiary account number, IFSC
· After getting beneficiary, debit freeze the account immediately
· Then verify the KYC, AOF of the fraudster using account and collect CDR for the linked phone number.
· If the fraudulent money is transferred to another account, get the details of beneficiary. In case of ATM withdrawal, get CCTV footages.

XVI. BUSINESS E-MAIL COMPROMISE FRAUDS

The cyber criminals will identify and compromise corporate/business email account of individual who has the authority to perform fund transfers. They will compromise the account and monitor for the communication for financial transaction. Once they come to know the victim is going to receive funds they will impersonate themselves as victim company to the sender and mention reasons for change in bank account due to audit in the company, income tax etc., or they will create an e-mail id similar to the victim company. In such cases, following the money trail will help in identification of victims. Often, BEC attackers impersonate CEO or any executive authorized to do wire transfers. In addition, fraudsters also carefully research and closely monitor their potential target victims and their organizations.

Cyber criminal mimics a senior company and e-mails finance department for funds

Finance department wires fund to cyber criminal's account, not checking the email address

Cybercriminal receives funds

STANDARD OPERATING PROCEDURE FOR INVESTIGATION

STEP 1: Collect the e-mail headers from the complainant-look for sender IP.

STEP 2: If the email domain is unknown, search Domain name, nodal e-mail ID to send notice.

STEP 3: If money transferred to foreign Bank account, initiate MLAT/LR process.

STEP 4: Ask Buyer/seller who is in abroad to lodge complaint there & take steps to stop the payments and for legal proceedings.

STEP 5: If the fraudster account is any of the Indian Bank, then send notice to freeze the account and then collect the details of the Account holder and other relevant details.

STEP 6: If the fraudulent money transferred to another Account, get the details of beneficiary and freeze the account. In case of ATM withdrawal get CCTV footages.

STEP 7: Verify the address of the suspect/ accused physically.

STEP 8: Arrest the accused person after complete verification and seize the evidence and other relevant details from the accused.

XVII. STANDARD OPERATING PROCEDURE – INVESTIGATION OF CYBER EXTORTION

Social media sites help connecting with people across the world. By exploiting the increasing usage of social media sites, these Cybercriminals are using fake identities on social media to befriend unsuspecting people, trap them and extort money.

Cyber extortion is the act of cyber-criminals demanding payment through the use of or threat of some form of malicious activity against a victim, such as data compromise or denial of service attack.
Tactics of Cyber Criminals:

1. Cybercriminals scout random social media page/handle to collect information available in public profile.

2. Create a profile on individuals and analyze for "Soft Targets"-Vulnerable people.

3. Create fake account on social media sites, usually as individual from opposite gender.

4. The cybercriminals could also create fake accounts by impersonating real people.

5. Using the details collected, they sweet-talk the victim to make them fall into relationship.

6. The victim is convinced to send private images or have intimate video call, which is recorded by the Cybercriminal.

7. Using Video editing tools, the video call is converted to Obscene content.

8. The edited video is sent to the victim with a threat note, demanding ransom (and/or sexual favors) to prevent the video from published online or sent to their friends/family.

Investigation

STEP 1: Collect the screen shot from the complainant and relevant details

STEP 2: If whatsapp chat send request and get details from whatsapp.

STEP 3: If the complainant transferred money to the accused/ suspect through UPI, (Google pay, Phonepe, Paytm) get linked account holders, statements and freeze and charge back.

STEP 4: Analyse account statement, analyse CDR of the Mobile number linked with the account.

STEP 5: Collect the address of the accused person based on the available details, verify physically.

STEP 6: Arrest the accused person after the physical verification and seize the evidences from the accused person.

XVIII. STANDARD OPERATING PROCEDURE – INVESTIGATION OF OTP FRAUD

Victims received anonymous calls as a bank manager from fraudster for reasons such as Credit card issuing, Reward Points, Limit increase, Card Activation, Block/ Unblock the Card and Card KYC Verification to get OTP (CVV, Card Details).
Documents to be collected from the complainant

1. Collect Credit/Debit card details, expiry year & month, bank name
2. Debit Message content-identifying the beneficiary/Merchant. Example: (Amazon/Flipkart)
3. Victim's mobile no, transaction date, time
4. Fraudulent caller phone number

Investigation

STEP 1: Send legal notice to Freeze the account of illegal transaction made over the Victim's credit/debit card of the issued bank or Seller.

STEP 2: If, UPI transaction, send legal notice to the debit freeze the victim's account to stop further illegal transactions. If the transaction is done through UPI, IMPS, NEFT, RTGS

· Mail to the victim bank with transaction ID (UPI, IMPS, NEFT) to get beneficiary account number, IFSC
· After getting beneficiary, debit freeze the account immediately

. Then verify the KYC, AOF of the fraudster using account and collect CDR forthe linked phone number.
· If the fraudulent money transferred to another account, get the details of beneficiary.
· In case of ATM withdrawal then get CCTV footages.

STEP 3: Send legal notice to revert the amount to the victim's card/account/wallet.

STEP 4: Send legal notice to bank manager to charge back if, the alert SMS not delivered by the bankers to the registered mobile number.

STEP 5: CDR request sent for Account/ linked mobile number for the particular period of time.

STEP 6: Verify the statement of account, SMS and what type of transactions.

STEP 7: If the transaction is done through Wallet/Merchant. Mail to the Wallet/Merchant to block the account and get beneficiary details, CDR to the given register mobile number of Wallet/Merchant.

STEP 8: Field Enquiry/ Physical Verification.

STEP 9: Arrest the accused person after the physical verification and seize the evidences from the accused person.

XIX.STANDARD OPERATING PROCEDURE – INVESTIGATION OF SIM SWAP

Documents to be collected from the complainant

1. Collect victim's mobile number and bank account statement
2. Date and time of transaction
3. Date and time of Victim's mobile number switched out of network
4. Fraudulent bank account number (available in victim bank statement)

Investigation

STEP 1: Immediately, assist victim to get new sim card by following SIM change procedure in nearby Mobile Network store and get bill copy.

STEP 2: Send notice to Mobile Nodal Officer to provide Name, address, Phone number, SIM lost request letter, address proof, ID Proof of the person who got the duplicate SIM card and also collect store address in which fraudster approached for SIM Swap.

STEP 3: Conduct enquiry at Mobile network store and collect CCTV footage, documents submitted, enquire witness who attended the fraudster.

STEP 4: Request Bank Nodal officer to provide the beneficiary account statement, KYC, address proof, ID Proof and request to debit freeze the account.

STEP 5: Collect ATM withdrawal clippings to identify the culprit.

STEP 6: Send legal notice to bank manager to charge back, if the alert SMS not delivered by the bankers to the registered mobile number.

STEP 7: Send CDR request for Account linked mobile number.

STEP 8: If it is online transaction, send mail to merchant for beneficiary details.

STEP 9: Field Enquiry/ Physical Verification.

STEP 10: Arrest the accused person after the physical verification and seize the evidences from the accused person.

XX. WEBSITE INVESTIGATION

STEP 1: Obtain the screenshot of the content from the victim. Soft copy as well as hard copy of the screenshots can be kept for evidence purpose. Make sure the exact URL is visible while taking screenshots along with the date and time. Also URL shall be securely recorded in the case file. By using Website Preservation Tools (Camtasia, Snagit, FAW1, Httrack, OSIRTetc.) the evidence may be preserved for forensic examination purpose.

STEP 2: If uploaded content is an image, video or audio etc., download the content from target website and calculate the hash value and keep it as an evidence for admissibility purpose. Procedure for calculating hash value is explained in detail in Chapter 7.

STEP 3: Extract the name of website on which offence has taken place and shall use websites such as www.who.is, www.domaintools.com, www.centralops.net etc. to get details of the defined domain such as “ebay.in”. Specifically look for Domain Registrar and Registrant and web hosting details

STEP 4: Verify from ‘Whois’ record whether the domain registrar is from India or outside India.

STEP 5: If domain registrar belongs to India, then a notice can be issued to registrar to get details such as

- Uploader of the content (IP address of the uploader)
- Date and timestamp of the uploaded content (along with the time zone)
- User details if any (such as e-mail address, mobile number while creating account)

Make sure that the URLs hosting abusive content are mentioned properly in the notice.

STEP 6: The notice to block/remove the content can also be issued to the registrar. Specify exact URL of the content

STEP 7: If required court notice can also be obtained and sent to ISP to block/remove the content from the website.

STEP 8: If the domain registrar is not from India then MLAT process can be followed to obtain information mentioned in step 5.

STEP 9: If the suspect has been identified then his/her mobile device/computer system can also be seized for further investigation.

Chapter 7

SCENE OF CRIME MANAGEMENT

I. INTRODUCTION

Understanding and implementing good forensic practices is an essential part of being a good cybercrime investigator. It is important to understand both law and technology being a police officer.

According to IT ACT 2008, computer is defined as any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.

II. THE PRINCIPLES OF DIGITAL EVIDENCE

· No action taken by law enforcement agencies, persons employed within those agencies, or their agents should change data which may subsequently be relied upon in court.

· In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

· An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

· The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

III. STEPS TO FOLLOW IN THE SCENE OF CRIME

STEP 1: What to take along

1. Evidence Tape
2. Chain of custody form
3. Inventory forms
4. Digital camera
5. Toolkit (Screwdriver set with Penta lobe Screwdriver for removing HDDs from Mac laptops)
6. Adhesive tape, Sticky note
7. New/ wiped pen drives, hard drives
8. Gloves, static wrist band
9. Write blockers (e.g. ATA, SATA, SCSI, firewire, USB, e-sata, SSD) with cables.
10. Hardware for Imaging (TD2U, Falcon, TrueImager) if available
11. Laptop with FTK (Crossover Tested)
12. Card readers 13. Magnifying glass, Flashlight
13. Faraday bag/Aluminium foil, Bubble wraps
14. Consent search or search warrant

STEP 2: POTENTIAL SOURCES OF DIGITAL EVIDENCE

1. RAM
2. HDD
3. Pen drives
4. Memory card
5. Mp3 player
6. CD/DVD/Blu-ray disk and other medias
7. Docs, notes, documentation etc.,

STEP 3: seize what?

1. HDD
2. Removable media (pen drives, external hard disk)
3. RAM

STEP 4: Search or Seizure where?

1. Secure the scene, restrict access
2. Preserve the area, no more fingerprints
3. Ensure the safety of all concerned
4. Nobody touch nothing
5. Onsite, in the field office, In a lab
6. Disposal of seized items
7. Consider the size of seizure
8. Suspects

a) Interview

b) Passwords

c) Location of data

d) Installed software

e) Network

STEP 5: Tag & Bag

1. Photograph all components and connections
2. Pack it for transport and keep it away from EM Fig: Sources of evidence
3. Collect all printed material

a) Docs, Records, notes

STEP 6: Seizure

1. If the network is active

a) Do not power down any networking gear

b) They have no hard drives

c) All evidence is volatile

d) Acquire volatile evidence if required

e) Seize the servers & workstations

2. Get the network admin to help

3. If the device is off leave it off, Tag & Bag

4. If the device is ON

a) Photographs and document especially communication ports

b) An attempt may be made to access memory

c) Disconnect the coms interface, Tag & Bag

STEP 7: security systems

1. Ingress/egress logs – timeline, ID's

2. Service provider

3. System information

4. Photograph & document location of all devises

5. Tag & bag all stored data & recorded data

6. Detailed documentation – you can't tag & bag

STEP 8: Print

1. Dial list, e-mail address, times, logs, headers

2. Stored documents
a) Sent
b) To be sent
c) Received – not opened
d) Received – opened e. Photograph & personal information

STEP 9: For a PC in ON Condition

1. If the computer is a standalone PC
a) Pull the plug
b) Do not turn it off

2. If it is a laptop
a) Pull the plug
b) If it is still on it has a functioning battery
c) Remove the battery
d) Keep the battery separate

STEP 10: Capture Photos

1. Each item
a) Placement
b) Model/serial numbers
c) Front
d) Back
e) Cables
f) Anything that might be of interest
g) You only get one chance to record the original evidence

2. Floor plan
a) Locate all equipment
b) Number all equipment on the floor plan
c) You will have to reconstruct

3. Photography or videography
a) The entire area containing hardware & cables
b) The screen of each computer that is ON

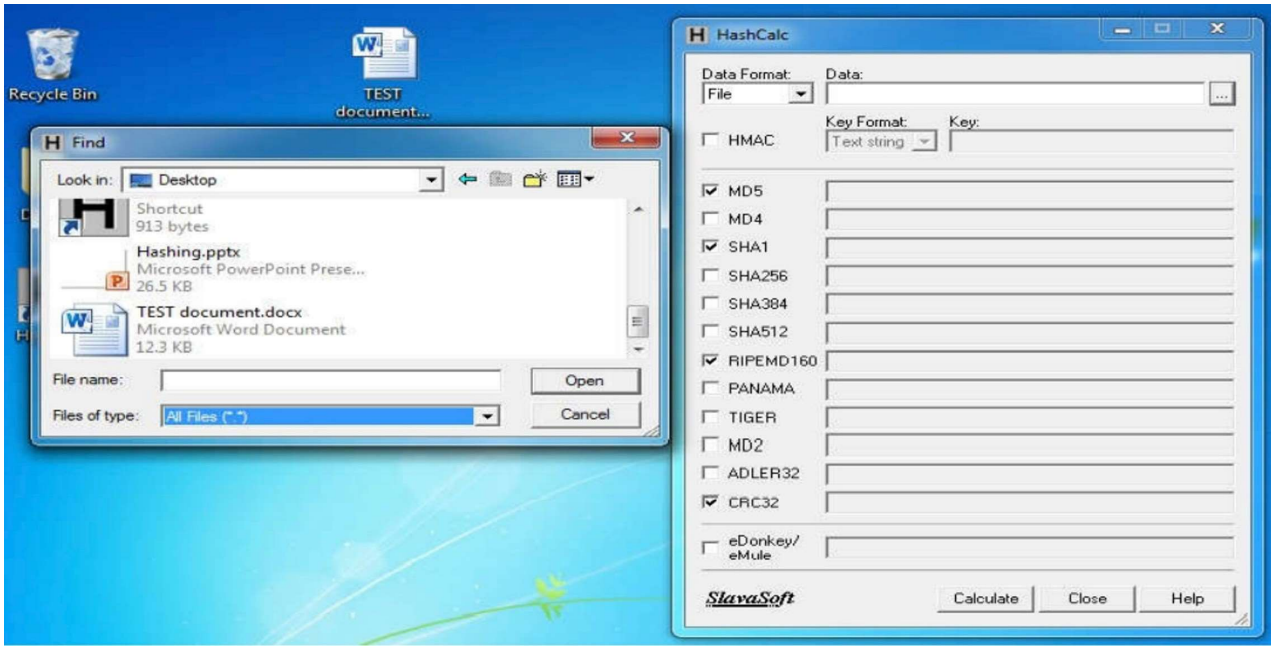
IV. INTRODUCTION TO HASHING

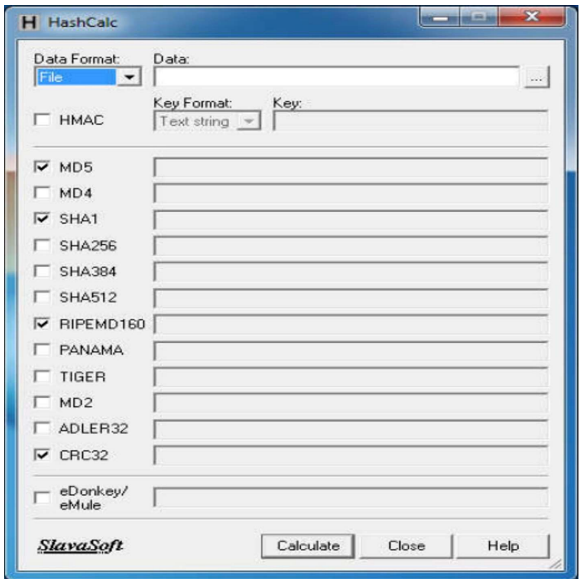
A hash value is a result of a calculation (hash algorithm) that can be performed on electronic file or entire hard drives contents. The result is also referred to as a checksum, hash code or hashes. The hash value is generated by a formula in such a way that it is extremely unlikely that some other file or entire hard drive will produce the same hash value.

A hash value is used to ensure that the examined copy has not been altered i.e. the integrity of the digital evidence is ensured upon hashing. The hash value generated from a file becomes its "digital fingerprint". MD5 and SHA are the two most common hash algorithms used in computer forensics.

V. HASHING DEMONSTRATION

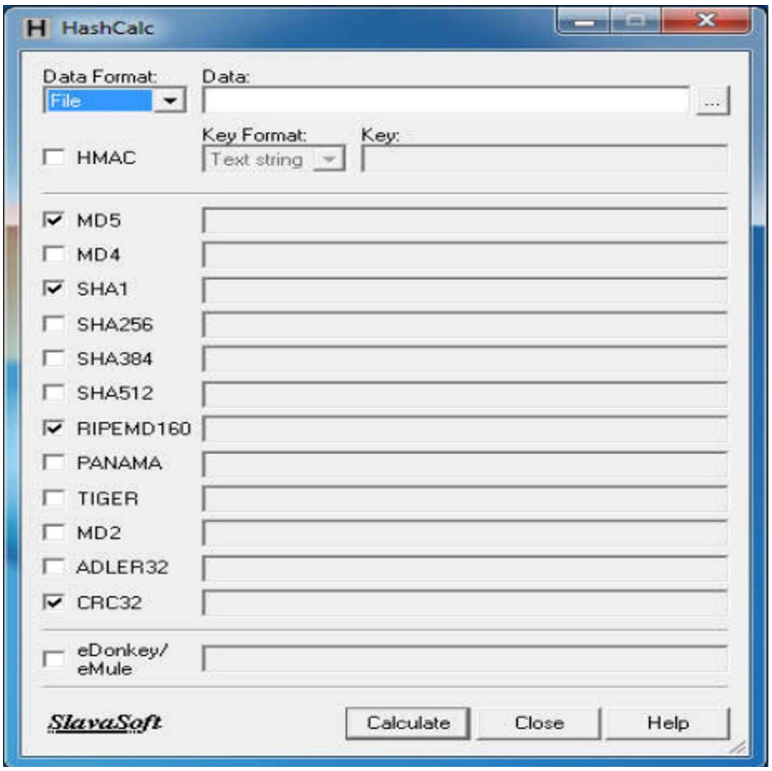
In this demonstration Hashcalc software is used to calculate the hash of the file





STEP 1: Selecting a document to perform hashing

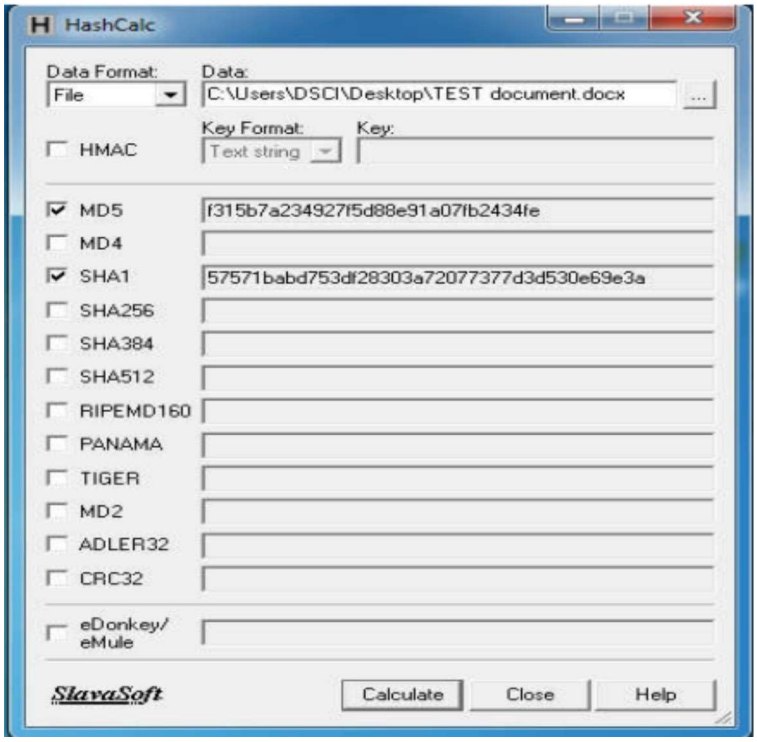
STEP 2: Press calculate button to generate hash value of a file.



There is change in the hash value when the original document is tampered

VI. INDICATIVE FREE TOOLS FOR HASH VALUE CALCULATION

- FTK Imager
- EnCase Forensic Imager
- Tableau Imager
- HashCalc
- Hashtab
- HashTool etc.



Chapter 8

LEGAL FRAMEWORK FOR THE INVESTIGATION OF CYBER CRIME CASES

GENERAL GUIDELINES FOR INVESTIGATION

Cyber Crime is one of the increasing areas of criminality. More than 100 million people use internet in India today. Information Technology Act 2000 is an omnibus Act which was promulgated for promotion of e-commerce and e-governance, acceptance of electronic documents at par with paper documents, acceptance of digital signatures at par with normal handwritten signatures and for dealing with cyber crimes.
The Information Technology Act 2000 was amended in December 2008 as the IT (Amendment) Act, 2008 (ITAA 2008), and notified for implementation from 27th October 2009. The Indian Penal Code and the Indian Evidence Act were also amended to include cyber crimes and digital evidences covered by ITA 2000. Various aspects of cyber crimes can be handled with the application of Information Technology Amendment Act 2008 along with Indian Penal Code 1860,The Indian Evidence Act 1872, The Indian Telegraph Act 1885 and Bankers' Book of Evidence Act 1891.

Some Salient Features of the Information Technology (Amendment) Act, 2008

- The act applies to any offence or contravention committed outside India by any person, irrespective of his nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India (Section 75)
- Officers of the rank of Police Inspectors and above are empowered to investigate offences under the ITAA 2008.
- CERT-In designated as the National Nodal Agency for Critical Information Infrastructure Protection.

Computer offences as per the ITAA 2008 are

- Computer related offences (include source code tampering, unauthorized access, disruption, damage etc of computer resources) defined under Section 65, 66 and 66 B to D.
- Obscenity and related offences as defined in Sections 66E, 67, 67A and, 67B.
- Threat to unity and integrity of India (cyber terrorism), Section 66F
- All the offences with upto three years punishment have been made bailable and, as such only sections 66F, 67A, 67B, 69, 69A and 70 of the IT(A) Act are non-bailable.

Computer Forensics

Computer Forensics is a branch of forensic science, wherein computer investigation and analysis techniques are applied to determine the potential legal evidence in a computer environment.
The cardinal rules have been evolved to facilitate a forensically sound examination of computer media and enable a forensic scientist to testify in count in respect of their handling a particular piece of evidence. Essentially, a forensically sound is one, which is conducted under such controlled conditions that it is completely documented, it is repeatable, and its results are verifiable. The methodology does not change the original evidence and preserves it in pristine condition. If appropriate forensic tools and techniques are used, same results are obtained irrespective of the fact who examines the media or which specific tools and techniques are employed.

The five cardinal rules are:

1. Never mishandle the evidence.
2. Never work on the original evidence.
3. Never trust the subject‘s operating system.
4. Document everything.
5. The results should be repeatable and verifiable by a third party.

Digital Evidence

1. Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination.
2. Digital evidence may not be visible to our eyes as physical evidence found in murder, rape cases etc., but, digital evidences may be available in the electronic devices and these electronic devices are called Physical evidences in the electronic crime.
3. These Physical evidences should be preserved for appropriate examination. Precaution should be taken in handling digital evidence at the Crime Scene, collection, preservation and transportation of digital evidences.
4. Scientific Officers may follow the steps listed below to guide their handling of digital evidence at an electronic crime scene:

- Recognize, identify, seize, and secure all digital evidence at the scene.
- Document the entire scene and the specific location of the evidence found.
- Collect, label, and preserve the digital evidence.
- Package and transport digital evidence in a secure manner.

It may not be advisable that without proper training and skills, Investigating Officer should not attempt to explore the contents of or to recover information from a computer or other electronic device other than to record what is visible on the display screen. Do not press any keys or click the mouse.

Other Forms of Evidence

Be alert to the crime scene environment. Look out for pieces of paper with possible passwords, handwritten notes, blank pads of paper with impressions from prior writings, hardware and software manuals, calendars, literature, and text or graphic material printed from the computer that may reveal information relevant to the investigation. These forms of evidence also should be documented and preserved in compliance with departmental policies.

Other Electronic and Peripheral Devices of Potential Evidential Value

Electronic devices such as those listed below may contain information of evidentiary value to an investigation. Except in emergency situations, such devices should not be operated and the information they might contain should not be accessed directly. If a situation warrants accessing these devices and the information they contain immediately, all actions taken should be thoroughly documented. Data may be lost if a device is not properly handled or its data properly accessed.

The following are examples of electronic devices, components, and peripherals that Scientific Officers may need to collect as digital evidence:

- Audio recorders.
- GPS accessories.
- Answering machines.
- Computer chips.
- Pagers.
- Cordless landline telephones.
- Copy machines.
- Cellular telephones.
- Hard drive duplicators.
- Facsimile (fax) machines.
- Printers.
- Multifunction machines (printer, scanner,copier, and fax).
- Wireless access points.
- Laptop power supplies and accessories.
- Smart cards.
- Videocassette recorders (VCRs).
- Scanners.
- Telephone caller ID units.
- Personal Computer Memory Card and International Association
- (PCMCIA) cards.
- PDAs.

When collecting electronic devices, components, and peripherals such as those listed above, remember to collect the power supplies, cables, and adapters for those devices as well.

Pre-Investigation assessment and Investigation:

Depending on the nature of each incident reported, the I.O should collect necessary information from complainant(s)/victims as part of the pre-investigation assessment, to understand the full scope of the incident and, the possible outcomes. This will help the I.O to build the plan of action/next steps in the investigation. Investigators and technical personnel are aware of the fact that, the digital evidence is very critical and volatile. Hence it is necessary to protect and collect the right evidences for the pre-investigation assessment.

Once the information reveals the commission of cognizable offence under the ITAA 2008 and other acts, the I.O should

i. Elicit the information regarding the act under report in detail and, ensure that the details of the offences are captured in the complaint, in full.

ii. Indicate the nature/modus operandi of the cyber crime in detail (including the e-mail address, systems, time zones etc).

iii. Indicate all the details that can be identified from the complaint like,

a) IP address in case of e-mail and Internet.
b) Profile name or username in case of social networking abuse.
c) Bank details/Internet banking, branch, etc., in case of online fraud.
d) Credit card details and nature of purchase, etc., in case of card fraud, etc.

iv. Include the time and date in the exact format the complainant mentioned or noted in any of the documentation attached with the complaint (such as e-mails) and, Time zone conversion will have to be taken care during the course of investigation.

Investigative Tools

In addition to tools for processing crime scenes in general, Scientific Officers/Investigating officers should have the following tools and materials in their digital evidence collection toolkit to collect Digital Evidence:

- Cameras (photo and video).
- Cardboard boxes.
- Notepads.
- Gloves.
- Evidence inventory logs.
- Evidence tape
- Paper evidence bags.
- Evidence stickers, labels, or tags.
- Crime scene tape.
- Antistatic bags.
- Permanent markers.
- Nonmagnetic tools.
- Radio frequency-shielding material such as faraday isolation bags
- Aluminium foil to wrap cell phones, smart phones, and other mobile communication devices.
- Wrapping the phones in radio frequency-shielding material prevents the phones from receiving a call, text message, or other communications signal that may alter the evidence.

Scene of crime

The scene of crime for a Cyber Crime incident may be

- Home of individuals with one or more computers.
- Cyber Cafe/Public places.
- Companies / organizations, with one or more computers and in some cases with vast and complicated network of systems

At the scene of crime (irrespective of the type of the scene of crime), the I.O should carefully survey the scene, observe and assess the situation and decide on the steps for proceeding further. The digital evidence is highly fragile and volatile. It will be available in a number of devices, locations and in various formats. For example, the copiers, fax machines, routers, hubs etc., apart from the standard storage / computer devices can also contain vital information relevant to the case / incident. Hence, it is utmost important for the I.O to do a preliminary review of the entire scene of offence and also take some additional steps before identifying the evidence and conduct search and seizure. It is very important to include such observations/preliminary review notes in the questionnaire that needs to be sent to FSL for expert opinion. As a matter of practice, IO should videograph / photograph and draw the network architecture sketch in ‘asis where is’ condition of the crime scene and document it in the seizure mahazar

Evaluating the scene of Crime

a) After identifying the scene of crime, I.O should secure it and, take note of every individual physically present at the scene of offence and, their role at the time of securing the scene of offence.

b) From the information gathered and based on visual inspection of the scene of offence, I.O should identify all the potential evidences. These physical evidences may include conventional physical evidences like the manuals, user guides and, other items left behind like passwords on slips, bank account numbers etc. It is also important to note of the position of various equipments and items at the scene of offence. For example, a mouse on the left hand side of the desktop possibly indicates the person operating the computer is a left-handed user.

c) While identifying the digital evidence, I.O should make sure that, the potentially perishable evidence is identified and, all the precautions are put in place for its preservation. At the time of review, disturbing or altering the condition of electronic evidences should be avoided.

d) If the systems are OFF, they should not be turned ON for the inspection. If systems are on, it is advised to leave them ON.

e) If systems are ON at the scene of offence, I.O should take appropriate steps to photograph it, plan for the seizure of the evidences at the earliest and document it. I.O should notify appropriate technical personnel to support during the seizure process, so that the perishable evidences (volatile data) are appropriately recovered without loss.

f) I.O should make note of the attached network cables and power lines to the systems. With the help of the complainant or the technical personnel at the agency, make a note of all the network connections, modems, telephone lines and, mark them both the equipment connection end and, from the source in the walls.

Measures to be taken for containment of the offence:

1. In case of financial frauds, the I.O should immediately contact the concerned branches of the banks to freeze the beneficiary/suspect/accused person's bank accounts in case of fraudulent money transfers.
2. The I.O should request the Service Providers to block/remove and at the same time preserve the access details of the fake/defamatory profiles in social networking/community Web sites. The I.O should also notify the Service Providers to preserve the access details of the defamatory/ obscene contents.

Avoiding alteration of evidence

The primary aim of the pre-investigation assessments is to "avoid alteration of evidences", which is crucial in successful prosecution of the cyber crimes. Please reach out for forensic examiner's assistance from any regional forensic labs as quickly as possible, if you are not clear or have any doubt regarding incident and, the understanding of the networks.

Crime Scene Investigation: Search and Seizure at the crime scene

As Cyber crime scene is completely different from the conventional crime scene and the digital evidences are highly fragile and can be tampered easily and stealthily, utmost care and precautions are to be taken during search, collection, preservation, transportation and examination of evidence.

The sequences of steps for digital crime scene investigations are,

i. Identifying and securing the crime scene
ii. 'As is where is' documentation of the scene of offence
iii. Collection of evidence -(Annexure-III)
(a) Procedure for gathering evidences from Switched-off Systems
(b) Procedure for gathering evidence from live systems
iv. Interrogation at the SOC (Annexure-II)
v. Labeling and documenting of the evidences
vi. Packaging and transportation of the evidences

The I.O shall keep in mind the following points while conducting search and seizure of digital evidences.

a) Make sure one of the technical people from the responder side along with two independent witnesses are part of the search and seizure proceedings, to identify the equipment correctly and to guide the I.O and witnesses.
b) Please refer to the notes made during the pre-investigation assessment for cross verifying and correctly documenting the technical information regarding equipment, networks and other communication equipment at the scene of crime.
c) Time Zone/System Time play a very critical role in the entire investigation. Please make sure this information is noted carefully in the seizure mahazar, from the systems that are in 'switched on' condition.
d) Please DON'T switch ON any device.
e) Please make sure a serial number is allotted for each device and the same should be duly noted not only in the seizure mahazar but also in the Chain of Custody and Digital Evidence Collection forms.
f) Make sure each device is photographed before starting of the investigation process at their original place along with respective reference like cubicle number or name room soundings, etc

g) Make sure to photograph the Hard Disk Drive or any other internal part along with the system, once removed from the system.
h) If possible, please paste the serial number along with Crime number/section of law.
i) Capture the information about the system and data you are searching and seizing in the seizure mahazar.
j) Brief the witnesses regarding the tools used to perform search and seizure of the digital evidence.
k) Make sure that the mahazar witnesses have some knowledge and ability to identify various digital devices.
l) Document the Chain of Custody
The procedure to be adopted during the collection of digital evidence and forwarding the same for forensic expert opinion are given in the Annexure – III & IV.
Detailed Standard Operating Procedure circulated vide the reference cited to be adopted in advance fee fraud cases and phishing cases are enclosed in Annexure-V, along with required formats/query forms to be sent to banks, ISPs, MSPs (Annexure- VI(A) & VI(B)) and the contact details of nodal officers (Annexure-VII).

Assess the Situation

After identifying the computer‘s power status, follow the steps listed below for the situation most like your own:
Situation 1: The monitor is on. It displays a program, application, work product, picture, e-mail, or Internet site on the screen.
1. Photograph the screen and record the information displayed.
2. Proceed steps given under sub heading —If the Computer is ON
Situation 2: The monitor is on and a screen saver or picture is visible.
1. Move the mouse slightly without depressing any buttons or rotating the wheel. Note any
2. onscreen activity that causes the display to change to a login screen, work product, or other visible display.
3. Photograph the screen and record the information displayed.
4. Proceed steps given under sub heading —If the Computer is ON
Situation 3: The monitor is on, however, the display is blank as if the monitor is off.
1. Move the mouse slightly without depressing any buttons or rotating the wheel. The display will change from a blank screen to a login screen, work product, or other visible display. Note the change in the display.
2. Photograph the screen and record the information displayed.
3. Proceed steps given under sub heading —If the Computer is ON
Situation 4a: The monitor is powered off. The display is blank.
1. If the monitor‘s power switch is in the off position, turn the monitor on. The display changes from a blank screen to a login screen, work product, or other visible display. Note the change in the display.
2. Photograph the screen and the information displayed.
3. Proceed steps given under sub heading —If the Computer is ON

Situation 4b: The monitor is powered off. The display is blank.
1. If the monitor 's power switch is in the off position, turn the monitor on. The display does not change; it remains blank. Note that no change in the display occurs.
2. Photograph the blank screen.
3. Proceed steps given under subheading – If the Computer is OFF
Situation 5: The monitor is on. The display is blank.
1. Move the mouse slightly without depressing any buttons or rotating the wheel; wait for a response.
2. If the display does not change and the screen remains blank, confirm that power is being supplied to the monitor. If the display remains blank, check the computer case for active lights, listen for fans spinning or other indications that the computer is on.
3. If the screen remains blank and the computer case gives no indication that the system is powered on, proceed steps under subheading —If the Computer Is OFF.

If the Computer is OFF

a) For desktop, tower, and minicomputers follow these steps:
(1) Document, photograph, and sketch allwires, cables, and other devices connected to the computer.
(2) Uniquely label the power supply cord
and all cables, wires, or USB drives attached to the computer as well as the corresponding connection each cord, cable, wire, or USB drive occupies on thecomputer.
(3) Photograph the uniquely labeled cords, cables, wires, and USB drives and the corresponding labeled connections.
(4) Remove and secure the power supply cord from the back of the computer and from the wall outlet, power strip, or battery backup device.
(5) Disconnect and secure all cables, wires, and USB drives from the computer and document the device or equipment connected at the opposite end.
(6) Place tape over the floppy disk slot, if present.
(7) Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.
(8) Place tape over the power switch.
(9) Record the make, model, serial numbers, and any user-applied markings or identifiers.
(10) Record or log the computer and all
its cords, cables, wires, devices, and components according to agency procedures.
(11) Package all evidence collected following agency procedures to prevent damage or alteration during transportation and storage.

b) For laptop computers follow these steps:

(1) Document, photograph, and sketch all wires, cables, and devices connected to the laptop computer.

(2) Uniquely label all wires, cables, and devices connected to the laptop computer as well as the connection they occupied.

(3) Photograph the uniquely labeled cords, cables, wires, and devices connected to the laptop computer and the corresponding labeled connections they occupied.

(4) Remove and secure the power supply and all batteries from the laptop computer.

(5) Disconnect and secure all cables, wires, and USB drives from the computer and document the equipment or device connected at the opposite end.

(6) Place tape over the floppy disk slot, if present.

(7) Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.

(8) Place tape over the power switch.

(9) Record the make, model, serial numbers, and any user applied markings or identifiers.

(10) Record or log the computer and all its cords, cables, wires, devices, and components according to agency procedures.

(11) Package all evidence collected following agency procedures to prevent damage or alteration during transportation and storage.

If the computer is ON

For practical purposes, removing the power supply when you seize a computer is generally the safest option. If evidence of a crime is visible on the computer display, however,you may need to request assistance from personnel who have experience in volatile data capture and preservation. In the following situations, immediate disconnection of power is recommended:

- Information or activity onscreen indicates that data is being deleted or overwritten.
- There is indication that a destructive process is being performed on the computer‘s data storage devices.
- The system is powered on in a typical Microsoft Windows environment. Pulling the power from the back of the computer will preserve information about the last user to login and at what time the login occurred, most recently used documents, most recently used commands, and other valuable information.

In the following situations, immediate disconnection of power is NOT recommended:

a. Data of apparent evidentiary value is in plain view onscreen. The Scientific Officers should seek out personnel who have experience and training in capturing and preserving volatile data before proceeding.

b. Indications exist that any of the following are active or in use:

- Chat rooms.
- Open text documents.
- Remote data storage.
- Instant message windows.
- Child pornography.
- Contraband.
- Financial documents.
- Data encryption.
- Obvious illegal activities.

c. For mainframe computers, servers, or a group of networked computers, the SO/IO should secure the scene and request assistance from personnel who have training in collecting digital evidence from large or complex computer systems.

Clues and Sample questions for Forensic Examination

Clues: As the following information may be very useful for the forensic examination of digital evidences at the laboratory, the IO/SO is here by suggested to get the followinginformation during the investigation by raising appropriate questions.

1. Case summary- investigative reports, witness statements
2. Internet Protocol(IP) if available
3. Key word list – names, locations, identities
4. Nicknames – all nicknames used by victims or suspect
5. Passwords – all passwords used by victim or suspect
6. Points of contacts – name of investigator making request
7. Supporting documents – consent form, search warrant
8. Type of Crime – provide specific information

Sample Questions

To get the maximum facilities available in the forensic laboratory, the IO may request the laboratory by raising suitable questions to make the findings of the forensic examination very fruitful in solving the crimes.

Since each case is unique in nature, the IOs may raise question based on the requirement to each case or consult the computer forensics division of Forensic Sciences Department. In this regard, some of the sample questions are given below for their ready reference.

1. The digital media has to be analyzed to ascertain the storage / deletion of all Information (photos/text messages/email messages/chat messages) relating to the email – ids abc@gmail.com ?
2. Please examine and find out the time stamp (creation/modification/transmission) of file or files under question?
3. Forensic analysis of the cell phone mentioned in the description is required with regard to the following points:

4. Recover all deleted/active SMS/MMS/ Wave (Sound) files, MP3, picture, video files, call logs, internet access details, email messages if any etc?

5. Any other evidences related to the case may be given?

6. Whether any of the enclosed documents / text contents either in full or in part is available in the material objects (digital media) mentioned in the item list? If so print outs of the said documents may be enclosed with the report.

7. Whether any data, designs and information found in the computer accessories seized from the accused mentioned vide reference are identical to the data, designs and information found in the compact discs produced by the complainant?

8. Whether the document marked S1 to S4 were sent to the email – id abc@yahoo. com from email –id xyz@gmail.com on dd.mm.yyyy as an attachment?

9. To find out the evidence for the illegal storage of source codes/files with names (abc, xyz, etc)

10. Check whether any files with extension ._ _ _ with the file name —abc‖ found stored in the seized hard disk as the same in complainant CD/any other item?

11. Details of bank accounts/Scanned copy of pay in slips/bank challans/credit cards/ debit cards/various bank account holder details/cheque leaves / Bank statement/ details of money transaction/password/ PIN number ?

12. Web site URLs/web pages/temporary internet files/ folders/ downloaded files containing information regarding online lottery /Job racket?

13. Whether any obscene pictures or movie clips are stored and any evidence for downloading or transmitting such images are found in the hard disk?

Annexure-I

Various types of offences mapped with ITAA 2008, IPC and Special and Local Laws.

S. No.	Nature of complaint	Applicable sections and Punishments under ITAA 2008	Applicable sections under other laws and punishments.
1	Mobile phone lost/stolen		Section 379 IPC upto 3 years imprisonment or fine or both
2	Receiving stolen computer/ mobile phone/ data (data or computer or mobile phone owned by you is found in the hands of someone else)	Section 66 B of ITAA 2008 - upto 3 years, imprisonment or Rupees one lakh fine or both	Section 411 I PC - upto 3 years imprisonment or fine or both
3	Data owned by you or your company in any form is stolen	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto rupees five lakh or both	Section 379 IPC upto 3 years imprisonment or fine or both
4	A password is stolen and used by someone else for fraudulent purpose.	Section 66 C of ITAA 2008- upto 3 years imprisonment and fine up to Rupees one lakh Section 66 D ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC - upto 3 years imprisonment or fine Section 420 IPC – upto 7 years imprisonment and fine
5	An e-mail is read by someone else by fraudulently making use of password	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees five lakh or both Section 66 C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	

S. No.	Nature of complaint	Applicable sections and Punishments under ITAA 2008	Applicable sections under other laws and punishments.
6	A Phishing e-mail is sent out in your name, asking for login credentials	Section 66 D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC - upto 3 years imprisonment or fine or both
7	Capturing, publishing, or transmitting the image of the private area without any person's consent or knowledge	Section 66E of ITAA 2008- upto 3 years imprisonment or fine not exceeding Rupees two lakh or both	Section 292 IPC - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and Rupees 5000 for second and subsequent conviction
8	Tampering with computer source Documents	Section 65 of ITAA 2008- upto 3 years imprisonment or fine upto Rupees two lakh or both Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees five lakh or both	
9	Data Modification	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to Rupees five lakh or both	
10	Sending offensive messages through communication service, etc.	As Section 66 A of ITAA 2008 is scrapped now this case can be booked under IPC	Section 500 IPC upto 2 years or fine or both Section 504 IPC Section 506 IPC - upto 2 years or fine or both - if threat be to cause death or grievous hurt, etc. - upto 7 years or fine or both Section 507 IPC - upto 2 years along with punishment under section 506 IPC Section 508 IPC - upto 1 year or fine or both Section 509 IPC - upto 1 years or fine or both of IPC as applicable

S. No.	Nature of complaint	Applicable sections and Punishments under ITAA 2008	Applicable sections under other laws and punishments.
11	Publishing or transmitting obscene material in electronic form	Section 67 of ITAA 2008 first conviction - upto 3 years and Rupees 5 lakh. Second or subsequent conviction - upto 5 years and up to Rupees 10 lakh	Section 292 IPC - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and Rupees 5000 for second and subsequent conviction
12	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form,	Section 67 B of ITAA 2008 first conviction - upto 5 years and up to Rupees 10 lakh Second or subsequent conviction - upto 7 years and up to Rupees 10 lakh	Section 292 IPC - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction
13	Conducting a denial of service attack against a government computer	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to Rupees five lakh or both Section 66 F of ITAA 2008- life imprisonment	
14	Stealing data from a government computer that has significance from national security perspective	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees five lakh or both, 66F - life imprisonment	
15	Sending threatening messages by e- mail	As Section 66 A of ITAA 2008 is scrapped now this case can be booked under IPC	Section 504 - upto 2 years or fine or both
16	Sending defamatory messages by e- mail	As Section 66 A of ITAA 2008 is scrapped now this case can be booked under IPC	Section 500 IPC - upto 2 years or fine or both

S. No.	Nature of complaint	Applicable sections and Punishments under ITAA 2008	Applicable sections under other laws and punishments.
17	Making a false document	Section 66 D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC - upto 2 years or fine or both
18	Forgery for purpose of cheating	Section 66 D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 468 IPC - upto 7 years imprisonment and fine
19	E-mail abuse	As Section 66 A of ITAA 2008 is scrapped now this case can be booked under IPC	See. 500 IPC - upto 2 years or fine or both
20	Punishment for criminal intimidation	As Section 66 A of ITAA 2008 is scrapped now this case can be booked under IPC	See. 506 IPC - upto 2 years or fine or both - if threat be to cause death or grievous hurt, etc. - upto 7 years or fine or both
21	Criminal intimidation by an anonymous communication	As Section 66 A of ITAA 2008 is scrapped now this case can be booked under IPC	See. 507 IPC - upto 2 years along with punishment under section 506 IPC
22	Copyright infringement	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to Rupees five lakh or both	See. 63, 63 B Copyrights Act 1957

Annexure-II

Points to be taken into consideration during the interrogation at SOC

Conducting preliminary interviews at the scene of offence will help I.O to identify and seize the potential evidences during pre-investigation. Some of the questions that I.O can make use during the investigation are,

1. What steps were taken to contain the issue? (Physical access denied for suspected persons, disconnecting the suspected computers from network, suspending the employee access and so on) along with list of all suspected names, address, etc.
2. Were there any logs (system access, etc.) present that cover the issue? Are there any suspicious entries present in them?
3. Did anyone use the system after the issue occurred?
4. Did you observe any similar instance before?
5. Were there any alarms that were set off by the firewall/IDS/network security devices?
6. Please give a detailed documentation on the set of commands or processes run on the affected system or on the network after the issue occurred. (Request a letter of confirmation from complaint)
7. Do they have similar systems in any of the branch/other offices?
8. Whether log register of the Internet users/ other users is maintained? (It is very crucial to fix the responsibility. In case of cyber cafes, it is a must to maintain log register of users for specific period as per the rules framed by several state governments.)
9. Are there any questions about the issue that have not been answered? (Affected system list, number of people involved, etc.)
10. What are the further plans for analysis of the issue?

At the scene of crime, I.O should

1. Identify the complainant/owner(s) of the various devices and obtain the access details, usernames, service providers' details. I.O. should ensure that these persons are available along with the search and seizure team for accessing various passwords protected/ secured information in the presence of the panch witnesses.
2. Gather information as provided in the questionnaire(s) above, on all the security systems including encryption policies and, off-site data storage and, data centre and disaster recovery policies of the organization or back-up plans etc.
3. Identify the list of the people who can identify the network and a schematic diagram of the network will be useful to be prepared during the interviews.

Scene of Offence: Cyber Cafe

1. Identify number of computer systems present in the cyber cafe.
2. Identify number of computer systems connected to Internet.
3. Obtain details about the network topology and architecture (client - Server).
4. Obtain the CCTV/Web camera clippings, if any.
5. Whether any user management software is used by the cyber cafe owner?
6. Obtain the log register of Internet users for the relevant period.
7. Check the formatting of storage devices policy adopted by the cyber cafe owner.
8. Check the hardware replacements done by the cyber cafe owner.
9. Check the policy regarding removal media usage on the cyber cafe systems.

Scene of Offence: Home

1. Identify the type of connection (Wi-Fi/ Ethernet).
2. How many computer systems are used for Internet connection?
3. Location of the system and details of persons with access to system(s).
4. Obtain the details about the removable storage media (including external hard disk) used/owned by the user.
5. Obtain details about the network topology and architecture (client - Server), if any.
6. Obtain the details about other computer peripherals (printer/scanner/modem, etc.).

Annexure –III
Collection of Digital Evidence

I. Procedure for gathering evidences from switched-off systems

(1) Secure and take control the scene of crime both physically and electronically. Physically means sending away all persons from scene of crime and electronically means, disabling the modems, network connections etc

(2) Make sure that the computer is switched OFF- some screen savers may give the appearance that the computer is switched OFF, but hard drive and monitor activity lights may indicate that the machine is switched ON. Be aware that some laptop computers may power ON by opening the lid. Remove the battery from laptop computers.

(3) Unplug the power and other devices from sockets.

(4) Never switch ON the computer, in any circumstances.

(5) Label and photograph (or video) all the components in-situ and if no camera is available, draw a sketch plan of the system.

(6) Label the ports and (in and out) cables so that the computer may be reconstructed ata later date, if necessary.
(7) Carefully open the side casing of CPU or laptop and identify the Hard disk. Detach the hard disk from mother board by disconnecting the data transfer cable and power cable.
(8) Take out the storage device (Hard disk) carefully and record unique identifiers like make, model, and serial number. If, entire CPU is seized, also note down the any unique identifiers.
(9) Get the signature of the accused and witness on Hard disk, by using permanent marker. Ensure that all items have signed and completed exhibit labels. Search scene of crime for non-electronic evidences like diaries, notebooks or pieces of paper with passwords on which are often stuck to or close to the computer. Ask the userif there are any passwords and if any off-site data storage. Also ask, for the operating system in the suspected system, the application packages, the various users of the com-puter etc.,
(11) After the Hard disk is removed from the suspected system, switch on the system and go to BIOS. Note down the date and time shown in BIOS.
(12) Prepare detailed notes giving "when, where, what, why & who" and overall actions taken in relation to the computer equipment.
(13) Allow any printers to finish printing.
(14) Connect the suspected hard drive to the investigator computer through write-block device for forensically previewing/ copying/ printing or for duplication. NEVER CONNECT DIRECTLY WITHOUT THE BLOCKER DEVICE.
(15) Make detailed notes of all actions taken in relation to the computer equipment.

II. Procedure for gathering evidences from live systems (Switched·ON Systems)
(1) Secure the area containing the equipment.
(2) Move people away from computer and power supply. Disconnect the modem if attached.
(3) If the computer is believed to be networked, seek advice from the technically trained officer, in-house forensic analyst or external specialist.
(4) Do not take advice from the owner / user of the computer.
(5) Label and photograph or video all the components including the leads in-situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that the computer may be reconstructed at a later date. Remove all other connection cables leading from the computer to other wall or floor sockets or devices.
6) Carefully remove the equipment and record the unique identifiers - the main unit, screen, keyboards and other equipment will have different numbers.
(7) Ensure that all items have signed exhibit labels attached to them as failure to do so may cause difficulty with continuity and cause the equipment to be rejected by the forensic examiners

8) Allow the equipment to cool down before removal

(9) Search area for diaries, notebooks or pieces of paper with passwords on which are often stuck to or close to the computer. Consider asking the user if there are any passwords and if these are given, record them accurately.

(10) Make detailed notes of all actions taken in relation to the computer equipment

(11) Record what is on the screen by photograph and by making a written note of the content of the screen.

(12) Do not touch the keyboard or click the mouse and if the screen is blank or a screen saver is present, the case officer should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse will restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph / video and note its content. If password protected is shown, continue as below without any further disturbing the mouse. Record the time and the activity of the use of the mouse in these circumstances.

(13) Take the help of technical expert to use live forensics tool to extract the information that is present in the temporary storage memory like RAM.

(14) If no specialist advice is available, remove the power supply from the back of the computer without closing down any programs. When removing the power supply cable, always remove the end attached to the computer and not that attached to the socket, this will avoid any data being written to the hard drive if an uninterruptible power protection device is fitted.

Annexure-IV

Guidelines for taking Expert Opinion from the Forensic Examiner

The following guidelines should be kept in mind by the IOs while forwarding the digital evidences for forensic analysis to TNFSL, Chennai.

The forwarding letter to the FSL for scientific analysis and opinion should mention the followfing information.

1. Brief history of the case
2. The details of the exhibits seized and their place of seizure
3. The model, make and description of the hard disk or any storage media
4. The date and time of the visit to the scene of crime
5. The condition of the computer system (on or off) at the scene of crime
6. Is the photograph of the scene of crime is taken?
7. Is it a stand-alone computer or a network?
8. Is the computer has any Internet connection or any means to communicate with external computers?

9. The investigating officer should interview the accused for obtaining the following information:

(a) The name of the operating system

(b) The application software packages used in the computer system with specific reference to the case like TALLY, FOCUS etc.

(c) Any files which were password protected and if the accused cooperates, the passwords for the files

(d) The employees who have access to the computer systems, their names, designations and their nature of work.

10. Is the BIOS date and time stamps were taken, or not? If taken the date and time should be mentioned?

11. Is the storage media forensically imaged and hashed for maintaining the integrity of the evidence? If so the HASH value should be mentioned & the algorithm used for hashing.

12. The signature of accused along with two witnesses should be taken on the suspected storage media.

13. Is the storage media previewed, if so, is the preview done forensically or not?

14. Some keywords useful and relevant to the case.

15. The date and time at which the panchanama of the seized computer system was written

16. The questionnaire should include the printout of important files relevant to the case Output from the application software packages

17. The investigating officer should avoid questions like

a) Printout of all the files existing in the computer system

b) In which country / place the operating system was loaded/any incriminating material relevant to the case.

c) Please list out all frauds committed by the accused using this laptop.

At the time of forensic analysis of the image of the suspected computer storage if the forensic expert feels that the investigating officer's presence is necessary at the forensic lab the investigating officer should be available for the same.

ANNEXURE - V

Cases on Advance fee frauds (online lottery/mobile draw etc.), online job racket and Phishing (Net banking fraud)

Complaint to be received

Complainant has to furnish the following information

Technical Leads

Bulk SMS code/Phone Nos. used by accused to communicate the victim (collect the print out of the SMS/photo)

Request the following details of complainant and accused mobile nos. from MSPs (Mobile Service Providers Airtel, BSNL, Aircel etc.)

1) SDR (Subscriber Data Record). 2) CDR (Call Data Record) for the period of communication.
3) CAF (Customer Acquisition Forms).
4) KYC (Know Your Customer) documents (ID / residential proof).
5) Also get the bulk SMS sender details from MSPs.
6) All above details can be collected through Nodal Officer of the districts through email.

E-mail ID's used by the accused (collect the print out of emails with full headers)

- available email headers → Ascertain sender IP address for all the mails communicated with date and time.
- If the headers not available → Request the email service provider (gmail,yahoo rediff etc.) to 3) provide the IP logs / account information / available contents.,

1) IP search who is look up for identifying the ISP (Internet Service Provider).
2) After identifications of ISP, request the ISP with IP date & time to furnish the address of internet connection.
3) After receiving the physical address the same should be verified and the system used should be seized, accused to be fixed by normal investigation. Seized media to be sent for forensic analysis.

Bank / Financial Leads (collect the pay in slips)

1) Request the bank to freeze the account immediately.
2) Request the bank and collect account Holder details (address)/ documents (AOF, KYC, photo, statement of account). AOF – Account Opening Form.
3) Collect the ATM clippings/cheque leaves from thebank for withdrawal.
4) Verify the address of the account holder physically along with the above documents.
5) If not traceable, collect more details through the KYC documents.
6) Seize the account documents/mobile phone/computer hard disk (if necessary).
7) Lead can be taken from the account holder about the main accused.
8) Analyze the mobile phone/Computer Hard disk for getting further lead.

ANNEXURE - VI(A)

SPECIMEN COPY

"TN Police Logo"

xxx Name xxxx
Inspector of Police,
Cyber Crime Cell.
Email id.

Unit Name
and Address,
Date,

TAMIL NADU POLICE DEPARTMENT
U/S 91 Cr.P.C. NOTICE

To
The xxxx,
----- Bank,
Legal Department.

Sir,

Sub: Cyber Crime Cell – On-line lottery scam case - Beneficiary account holder/accused details & Documents - Requested - Reg.

Ref: Cr.No.--

****

The reference cited case is under investigation by the Cyber Crime Police Station, (District). Some unknown person has sent an e-mail to the complainant, informing that in Online draw,"you have been awarded 5 lakh UK dollar" by Microsoft promotion award, London. The complainant was advised to deposit his money in various occasions, for the reasons ofdelivery charges, tax charges, customs charges, clearing charges, conversion charges, anti money laundering fees, anti-terrorism fees, anti drug trafficking fees and transfercharges in various banks in difference accounts. Accordingly, the complainant was paid Rs. xxxx in various accounts and thereby the complainant was cheated. The beneficiaryaccount holder details are as follows:

SI. No.	Name of A/c holder	A/c No.	Date of deposit	Amount Rs.

2) Hence it is requested to freeze the above accounts and also furnish the Name & address of the account holder, documents viz Account opening form (AOF) with legible colour photo., KYC documents viz. ID/ residential proof documents given by the account holder at the time of opening the account, and Statement of accounts from the date of opening to till date.

Treat this as most urgent.

(xxxx Name xxxx)

ANNEXURE - VI(B)

SPECIMEN COPY

"TN Police Logo"

xxx Name xxxx
Inspector of Police,
Cyber Crime Cell.
Email id.

Unit Name
and Address,
Date,

TAMIL NADU POLICE DEPARTMENT
U/S 91 Cr.P.C. NOTICE

To
Google Legal Investigation Support,
GoogleInc.
lis-global@google.com

Sir,

Sub: India - Tamil Nadu Police – Cyber Crime Police Station – (District) - Online job racketing – cheated to the tune of Rs.xxxxx Gmail - IP logs – Requested – Reg.

Ref: Cr.No.--

****

I am being empowered to investigate the crimes committed through Computer and Internet under Information Technology Act.

2) On receiving a complaint from Mr.xxxxx (address), a case has been registered as mentioned in the above cited reference. The crux of the offence is that some accused persons have approached the complainant with a malafide intention of online cheating and lend credence that they will arrange overseas job for him at M/s.xxxxx situated at (country name). The complainant was cheated to the tune of Rs.xxxxx.

3) In this case, lead could be taken from the e-mail id used by the accused for correspondence. Accused have used the e-mail Id (Exmple@gmail.com) to contact the complainant.

4) In this regard you are requested to furnish the IP logs & account information of the e-mail id (Exmple@gmail.com) for proceeding further investigation.

Treat this as most urgent.

(xxxx Name xxxx)

CHECK LIST - CYBER CRIME OFFENCES

The Investigation Officer will ensure that the particulars given in the Check List are available in the Final Report.

S. No.	PARTICULARS	YES/ AVAILABLE	NOT APPLICABLE
1.	First Information Report.		
2.	Complaint Copy.		
3.	Case Diary with page numbers.		
4.	Photograph / Videograph of SOC.		
5.	Observation Mahazar.		
6.	Rough Sketch.		
7.	Seizure Mahazar at SOC.		
8.	FP / Scientific Expert - Visit.(If necessary)		
9.	Statements of Witnesses.		
10.	Form 91 – to send properties.		
11.	CDR /IPDR /Tower Dump with Certificate u/s 65-B IEA		
12.	Notice under 91 Cr.P.C to Social Media sites/ Banks/ E- Wallet providers/ISP/MSP.		
13.	Reply given by Social Media sites/Banks/ E-Wallet Providers/ISP/MSP with Certificate u/s 65 B IEA		
14.	Screen shots in case of Social Media/Email/ Website / Other Online crimes with Certificate u/s 65 B IEA		
15.	Overt Act table - Accused – Motive- Cyber Tool/Type of Cyber attack/ Cyber Platform used against the victim -Loss (Money, Reputation etc)		
16.	Arrest of Accused person(s)		
17.	Arrest Intimation – Supreme Court guidelines.		
18.	Confession Statement of Accused Person(s).		
19.	Seizure Mahazar – S – 27 – IEA Recovery- Mobile/Login Credentials/ Computer/storage devices etc.		
20.	Photograph / Finger Print taken of Accused.		
21.	Remand Report.		
22.	Sections Alteration / Adding Report (If it is).		
23.	TNFSL, Computer Division report		

S. No.	PARTICULARS	YES/ AVAILABLE	NOT APPLICABLE
24.	Anticipatory Bail – Accused Surrender – Police Custody details.		
25.	Test Identification Parade conducted.		
26.	Statements u/s 164 – Cr PC (if necessary).		
27.	Any Accused turned Approver. (if necessary).		
28.	CDs date wise followed by connected documents.		
29.	IO's discussion with Law Officer - Draft Opinion.		
30.	Charge sheet.		
31.	Memo of Evidence.		
32.	List of documents.		
33.	Accused Adding / Deleting Report (If it is).		
34.	Entry of Accused in the Detention Forecast Register.		
35.	Victim Compensation Proposals.		

Content Reprinted from Handbook of Investigation

Chapter 9

INFORMATION TECHNOLOGY ACT

I. INTRODUCTION TO INFORMATION TECHNOLOGY (IT) ACT:

As our world changes and development in technology gets doubled up every year, there is always a possibility of crime happening online. Law enforcement should be competent enough to face such dreadful wrong doings and the technology being used by them.

In India Cyber law and IT Act 2000, modified in 2008 are being articulated to prevent computer crimes. IT Act 2000 is an act to provide legal recognition for transactions carried out by means of Electronic Data Interchange (EDI) and other means of electronic communication. It is the primary law in India dealing with cybercrime and electronic commerce (e-Commerce). e-Commerce is electronic data exchange or electronic filing of information.

UN General Assembly enacted Model Law adopted by United Nations Commission on International Trade Law (UNICITRAL) by the resolution A/RES/51/162, dated 30 January 1997. Then India passed the Information Technology ACT 2000 in May 2000 and came into effectiveness on 17th October 2000. This Information Technology Act is amended substantially through Information Technology Amendment Act 2008 which was passed by both the houses on 23 & 24 December 2008. This act got presidential assent on 5th Feb 2009 and came into effectiveness on 27th October 2009.

II. ESSENCE OF INFORMATION TECHNOLOGY (IT) ACT

1. IT Act 2000 addressed the following issues

a) Legal Recognition of Electronic Documents
b) Legal Recognition of Digital Signatures
c) Offenses and Contraventions
d) Justice Dispensation Systems for Cybercrimes

2. ITAA, 2008 is often referred as the enhanced version of IT Act 2000 as it additionally focused on Information Security.

3. Several new sections on offences like Cyber Terrorism, Data Protection were added in ITAA, 2008.

S.No	Nature of complaint	Applicable sections and Punishments under ITAA 2008	Applicable sections under other laws and punishments
1	Receiving stolen computer/ mobile phone/ data (data or computer or mobile phone owned by you is found in the hands of someone else)	Section 66 B of ITAA 2008 - upto 3 years, imprisonment or Rupees one lakh fine or both	Section 411 I PC - upto 3 years imprisonment or fine or both
2	Data owned by you or your company in any form is stolen	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto rupees five lakh or both	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto rupees five lakh or both
3	A password is stolen and used by someone else for fraudulent purpose.	Section 66 C of ITAA 2008- upto 3 years imprisonment and fine up to Rupees one lakh Section 66 D ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC - upto 3 years imprisonment or fine Section 420 IPC – upto 7 years imprisonment and fine
4	An e-mail is read by someone else by fraudulently making use of password	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees five lakh or both Section 66 C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	
5	A Phishing e-mail is sent out in your name, asking for login credentials	Section 66 D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC - upto 3 years imprisonment or fine or both
6	Capturing, publishing, or transmitting the image of the private area without any person's consent or knowledge	Section 66E of ITAA 2008- upto 3 years imprisonment or fine not exceeding Rupees two lakh or both	Section 292 IPC - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and Rupees 5000 for second and subsequent conviction
7	Sending defamatory messages by e- mail	As Section 66 A of ITAA 2008 is scrapped now this case can be booked under IPC	Section 500 IPC - upto 2 years or with fine or both
8	Data Modification	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to Rupees five lakh or both	

S.No	Nature of complaint	Applicable sections and Punishments under ITAA 2008	Applicable sections under other laws and punishments
9	Tampering with computer source Documents	Section 65 of ITAA 2008- upto 3 years imprisonment or fine upto Rupees two lakh or both Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees five lakh or both	
10	Sending offensive messages through communication service, etc.	As Section 66 A of ITAA 2008 is scrapped now this case can be booked under IPC	Section 500 IPC upto 2 years or with fine or both Section 504 IPC Section 506 IPC - upto 2 years or fine or both - if threat be to cause death or grievous hurt, etc. - upto 7 years or fine or both Section 507 IPC - upto 2 years along with punishment under section 506 IPC Section 508 IPC - upto 1 year or fine or both Section 509 IPC - upto 1 years or fine or both of IPC as applicable
11	Publishing or transmitting obscene material in electronic form	Section 67 of ITAA 2008 first conviction - upto 3 years and Rupees 5 lakh. Second or subsequent conviction - upto 5 years and up to Rupees 10 lakh	Section 292 IPC - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and Rupees 5000 for second and subsequent conviction
12	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form,	Section 67 B of ITAA 2008 first conviction - upto 5 years and up to Rupees 10 lakh Second or subsequent conviction - upto 7 years and up to Rupees 10 lakh	Section 292 IPC - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction
13	Conducting a Denial of Service attack against a government computer	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to Rupees five lakh or both Section 66 F of ITAA 2008- life imprisonment	
14	Sending threatening messages by e- maiL	As Section 66 A of ITAA 2008 is scrapped now this case can be booked under IPC	Section 504 - upto 2 years or fine or both

S.No	Nature of complaint	Applicable sections and Punishments under ITAA 2008	Applicable sections under other laws and punishments
15	Stealing data from a government computer that has significance from national security perspective	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees five lakh or both, 66F - life imprisonment	
16	Making a false document	Section 66 D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC - upto 2 years or fine or both
17	Forgery for purpose of cheating	Section 66 D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 468 IPC - upto 7 years imprisonment and fine
18	E-mail abuse	As Section 66 A of ITAA 2008 is scrapped now this case can be booked under IPC	See. 500 IPC - upto 2 years or with fine or both
19	Punishment for criminal intimidation	As Section 66 A of ITAA 2008 is scrapped now this case can be booked under IPC	See. 506 IPC - upto 2 years or fine or both - if threat be to cause death or grievous hurt, etc. - upto 7 years or fine or both
20	Criminal intimidation by an anonymous communication	As Section 66 A of ITAA 2008 is scrapped now this case can be booked under IPC	See. 507 IPC - upto 2 years along with punishment under section 506 IPC
21	Copyright infringement	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to Rupees five lakh or both	See. 63, 63 B Copyrights Act 1957
22	A Biometric thumb impression is misused	Section 66 C of ITAA 2008 - upto 3 years imprisonment and fine upto Rupees One Lakh	
23	An Electronic signature or Digital signature is misused	Section 66 C of ITAA 2008 - upto 3 years imprisonment and fine upto Rupees One Lakh	
24	Not allowing the authorities to decrypt all communication that passes through computer or network.	Section 69 of ITAA – 2008, Imprisonment upto 7 years and fine.	

S.No	Nature of complaint	Applicable sections and Punishments under ITAA 2008	Applicable sections under other laws and punishments
25	Misusing a Wi-Fi connection If done, against a state	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees five lakh or both, 66F - life imprisonment of ITAA 2008	
26	Planting a computer virus If done, against a state	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees Five Lakh or Both Section 66FF- Life imprisonment of ITAA 2008	
27	Intermediaries not providing access to information sorted on their computer to the relevant authorities.	Section 69 of ITAA – 2008, Imprisonment upto 7 years and fine.	
28	Failure to block Web sites when ordered.	Section 69 of ITAA – 2008, Imprisonment upto 7 years and fine.	
29	Word, gesture or act intended to insult the modesty of a woman		See. 509 IPC - upto 1 year or fine or both – IPC as applicable
30	Bogus Websites, Cyber frauds	Section 66D of ITAA – 2008, upto 7 years Imprisonment and fine upto Rupees One Lakh.	Section 419 – upto 3 years imprisonment or fine. Section 420 – upto 7 years imprisonment or fine.
31	Email Spoofing	Section 66C of ITAA – 2008, upto 7 years Imprisonment and fine upto Rupees One Lakh.	Section 465 – upto 2 years imprisonment or fine or both.Section 468 – upto 7 years imprisonment or fine.
32	Theft of computer hardware		See. 379 IPC – upto 3 year or fine or both
33	Online sales of Drugs		NDPS Act
34	Online sales of Arms		Arms Act