



# CYBER FRAUDS

KAPIL GARG  
DIRECTOR  
STATE CRIME RECORDS BUREAU  
RAJASTHAN POLICE


---



Crime that utilizes  
technology, particularly  
(but not exclusively) the  
Internet and Computers.



Any criminal activity in  
which a computer is  
either -

- An instrumentality or a tool
  - A target
- 

# CYBER CRIME

---



## COMPUTER AS A TOOL

- Financial crimes
- Sale of illegal articles
- Pornography
- Online gambling
- Intellectual property crime
- E-mail spoofing
- Forgery
- Cyber defamation
- Cyber stalking
- Counterfeiting



## COMPUTER AS A TARGET

- Unauthorized access
- Theft of information
- E-mail bombing
- Data diddling
- Viruses, Logic bombs, Trojan attacks
- Internet time thefts
- Theft and physical damage of computer system
- Denial of Service Attacks/ DDoS

# **RISE OF THE MACHINES**

---

# fraud

*noun* | \ 'frɒd \

## Simple Definition of FRAUD

- : the crime of using dishonest methods to take something valuable from another person
- : a person who pretends to be what he or she is not in order to trick people
- : a copy of something that is meant to look like the real thing in order to trick people

Source: Merriam-Webster's Learner's Dictionary

- ✓ Deception
- ✓ Wrongful Gain or Loss

---

SAD AS IT MAY SEEM, FRAUD WILL ALWAYS TAKE PLACE WHEREVER THERE IS AN OPPORTUNITY.



---

Banking Fraud

---

Fraud to get government benefits

---

Counterfeiting of currency etc.

---

Confidence tricks

---

Creation of false companies

---

Embezzlement

---

Credit Card Frauds

---

False advertising

---

False billing

---

False insurance claims

---

Franchise Fraud

---

Fraud upon the court

---

Health Fraud

---

ATM Fraud

---

Identity theft

---

Insurance Fraud

---

Intellectual property theft

---

Investment Frauds

---

Marriage Fraud

---

Religious Fraud

---

Rigged gambling games

---

Securities Frauds

---

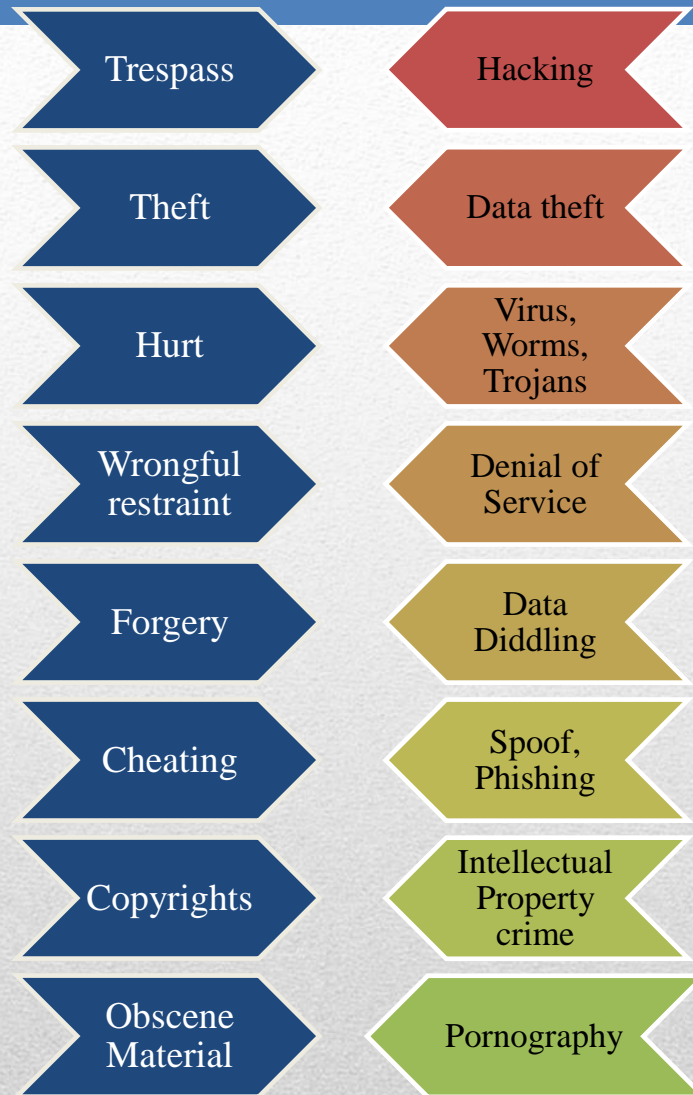
Tax Fraud

---

Tax Evasion

# FRAUD TYPES

---



# TRADITIONAL v/s CYBER SPACE



Fraud using computer/ technology  
compared to traditional methods

Virtual victim = Data

Vulnerabilities of technology exhaust  
valuable resources belonging to entity  
using that technology

Type of fraud is only limited by the  
imagination of the fraudster

Wrongful access

Alter by false entries  
(data entry level)

Alter by conceal/ edit/ delete

Misuse

# CYBER FRAUDS

---

Over 40,000 incidents reported  
each year in India

---

69% increase in Cyber Crime

---

About 30,000 Indian websites  
hacked every year

---

74% increase in arrests of Cyber  
criminals

---

Over 50,000 spam email reported  
to CERT-In every year

---

54% criminals between 18-30 yrs.  
Age

---

Culprits - 7% neighbors or family,  
5% students, 3% employee, 2.5%  
business competitor

---

Out of 12248 cases, 65% pending  
investigation

---

(2014, Crime in India, NCRB)

---

# PROBLEM SIZE

---





MySpace

164,000,000 Personal details made public



Ebay

• 145,000,000 Credentials of users copied



Heartland – Payment processor

130,000,000 Credit card scam, \$110 million paid to Card Coys. to settle claims



LinkedIn

• 117,000,000 User data accessed



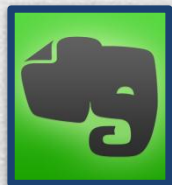
AOL

• 92,000,000 Screen names/ email details stolen



Dropbox

• 68,700,000 User credentials stolen



Evernote

• 50,000,000 User IDs & Passwords suspected compromised



Adobe

• 36,000,000 User IDs & Passwords used, data corrupted



Apple

• 12,367,232 FBI Laptop hacked, Apple UDIDs compromised



Sony Pictures

• 100 terrabytes Unreleased films, scripts etc. stolen



Gmail

• 5,000,000 Account IDs & Passwords leaked



Twitter

• 250,000 User ID & contact info stolen

# HOW SAFE ARE YOU

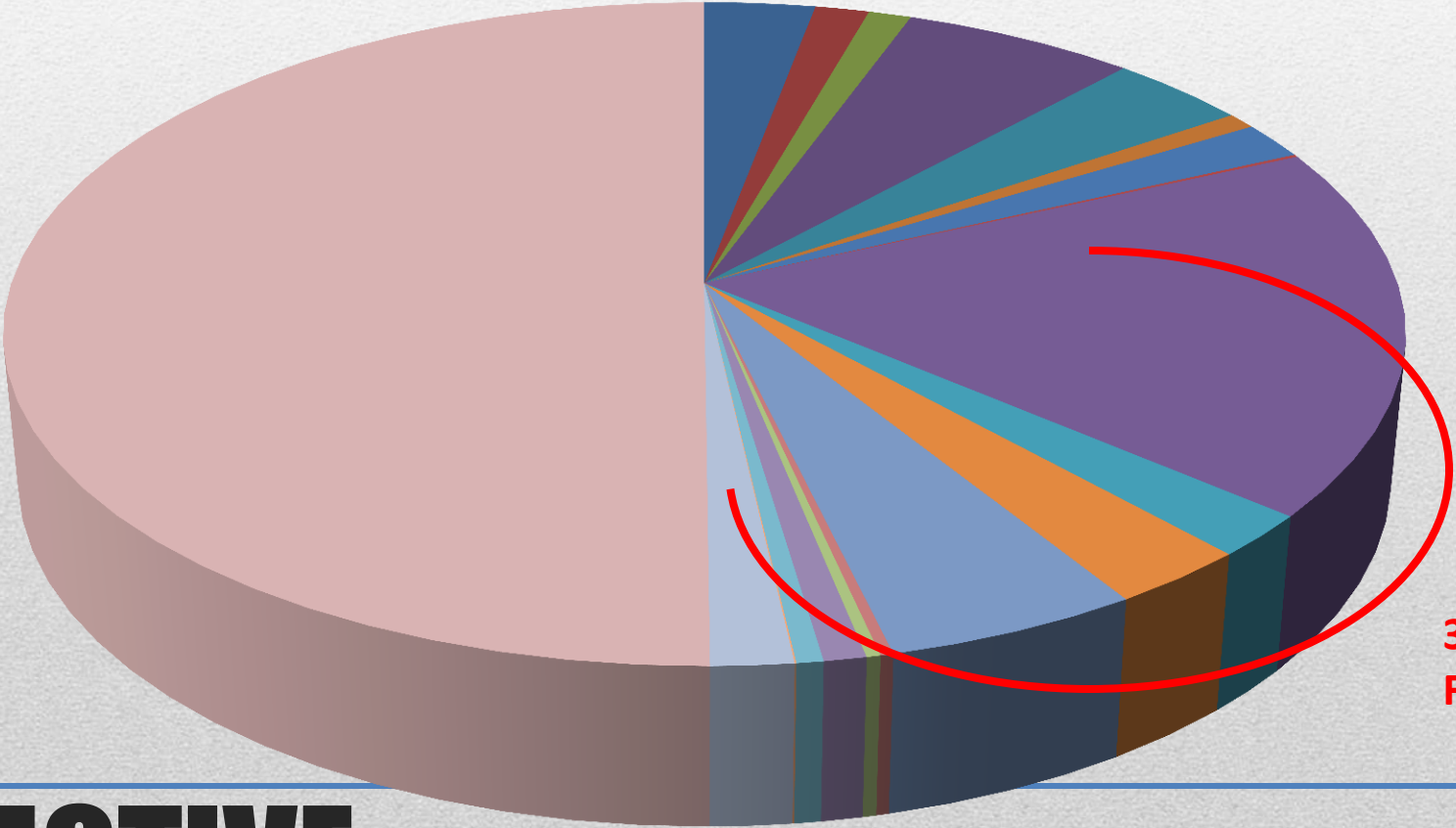


# MOTIVE

- Personal Revenge / Settling scores
- Insult to Modesty of Women
- Inciting Hate Crimes Against Community
- Greed / Financial Gain
- Fraud/ Illegal Gain
- For Developing Own Business/Interest
- Motives of Blackmailing

- Emotional Motives like Anger, Revenge, etc
- Sexual Exploitation
- Inciting Hate Crimes Against Country
- Extortion
- Disrupt Public Services
- For Spreading Piracy
- Others

- Prank / Satisfaction of Gaining Control
- Political Motives
- Serious Psychiatric Illness viz. Perversion, etc
- Causing Disrepute
- Sale/ Purchase of Illegal Drugs/ Items
- Steal Information for Espionage



31%  
Frauds



Remote operation, trans-national crimes

Anonymity

Growing penetration of technology – Internet of things

Negligent/ uninformed users

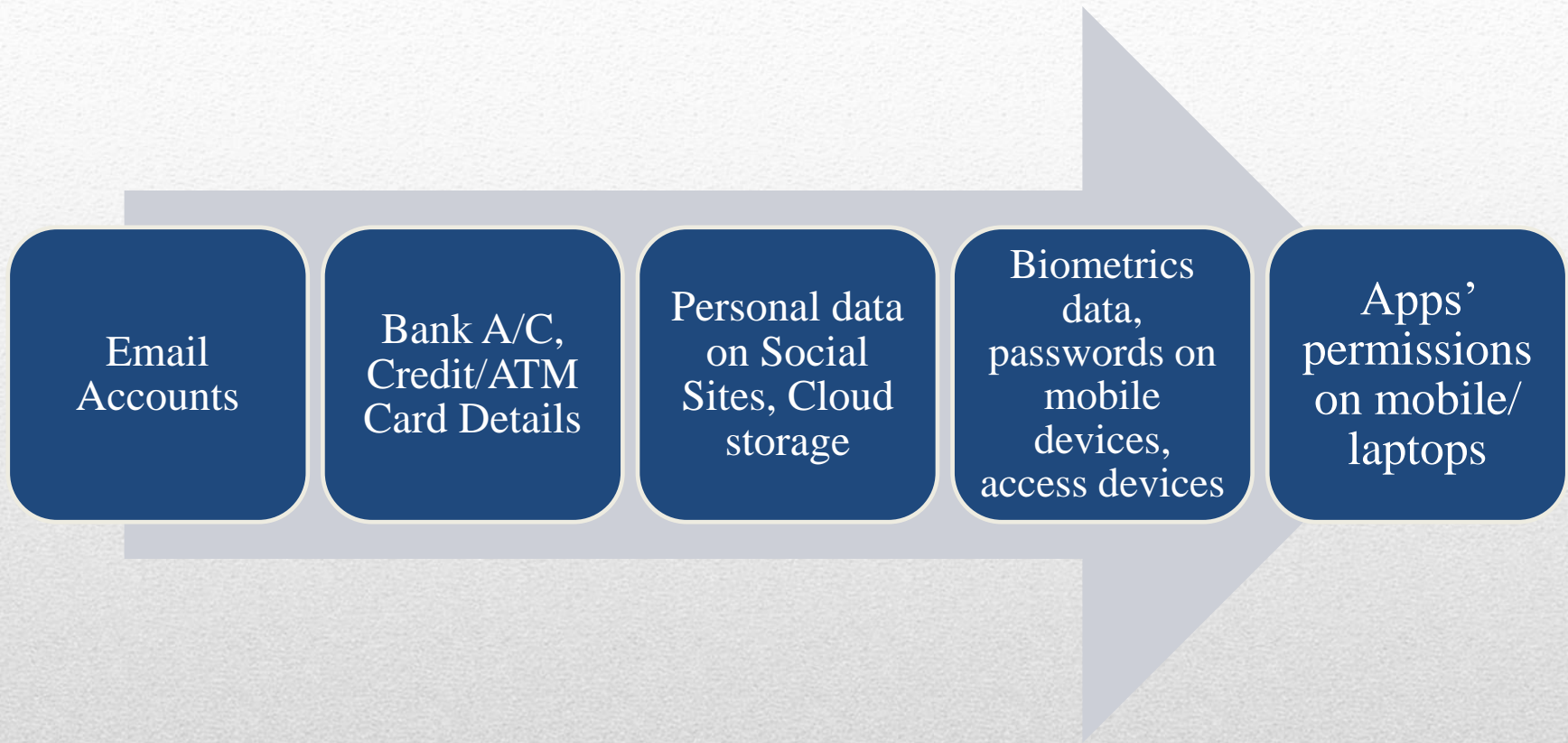
Improved connectivity

Vulnerabilities in existing technology

Law & LEAs still evolving

# **PREFERRED CHOICE**

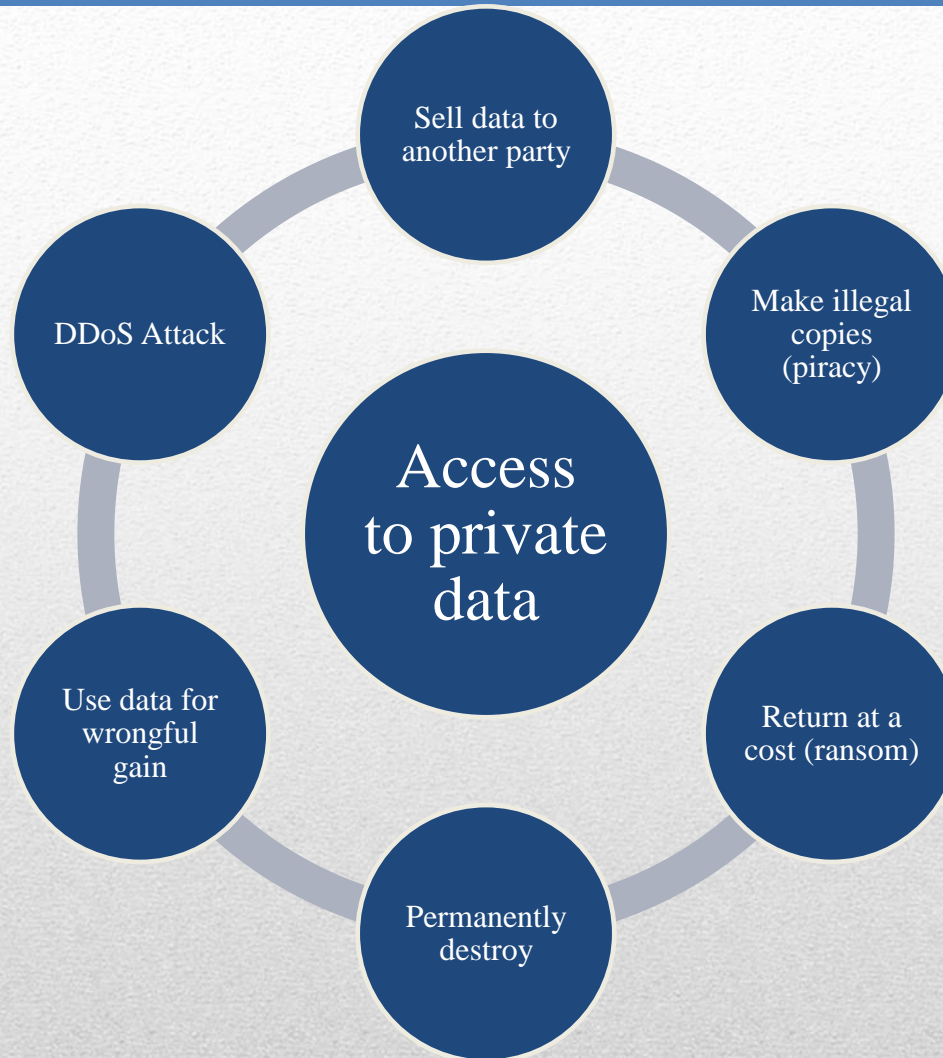
---



# SOFT TARGETS

---





# NOW TRENDING : HACKING

---



# **NOW TRENDING : CREDIT CARDS**

---



## Phishing

Email

Phone  
calls

Social  
Media

## Spear Phishing

Effective  
attack with  
personal  
details

## Whaling

Target  
senior  
executives

---

Obtain sensitive  
information

---

Bait offered to victim

---

Social engineering  
techniques

# NOW TRENDING : PHISHING

---

## Spoofing

Caller ID

IP Address

Website

Emails

## Pharming

Redirect  
to fake  
site where  
user  
enters  
details

---

Conceal real source of  
phone/ VoIP call, email

---

Send packet data with false  
source IP address

---

Same design + similar URL  
website

# NOW TRENDING : SPOOFING

---



## Honey Trap

- Advance fee for processing lottery etc.
- Dating
- Charity
- Ponzy/ Pyramid Schemes
- Online auction/ retail
- Money transfer fraud
- Internet marketing of rare items

Unbelievable  
returns offered

Processing cost  
has to be paid

Followed by  
more hidden  
costs

Followed by  
additional  
unbelievable  
returns

# NOW TRENDING : HONEY TRAP

## Call Tag Scam

- Credit card fraud
- Online purchase
- Track shipment
- Call card holder, ask for permission to pick item quoting mistaken shipment

## Transaction Account Scam

- Email hack – information of clients
- Spoof mail to merchant from “client”, request payment in “new” account
- Launder money in various international accounts

## Bank A/C Compromise

- Credit Card fraud
- Change message alert mobile number or Get duplicate SIM issued quoting loss of SIM
- Quick ATM withdrawals, online purchase or launder money

## Stock Market Manipulation

- Spam email/ chat/ internet boards
- Pump & Dump or Scalping
- Sell/ buy quickly and launder money

# COCKTAILS

---





## Acquisition

- Skimmer
- Hack
- Intercept PoS
- Phish

## Resale

- Darknet
- Other resellers

## Processing

- Pin code filter
- Block check
- Filter Credit rating

## Laundering

- Online Payment Gateways
- Pre-paid Cards
- Bitcoins

# EVOLVING MODUS OPERANDI

---

---

Dark  
Web

Part of www on dark-nets which uses public internet but requires specific software, configuration and authorization access

---

Dark Net

Peer-to-peer or Private overlay networks, popular for illegal online trade involving drugs, weapons, fake currency

---

TOR

*The Onion Router* directs traffic through free, worldwide, volunteer network of over 7000 relays

---

Crypto-  
Currency

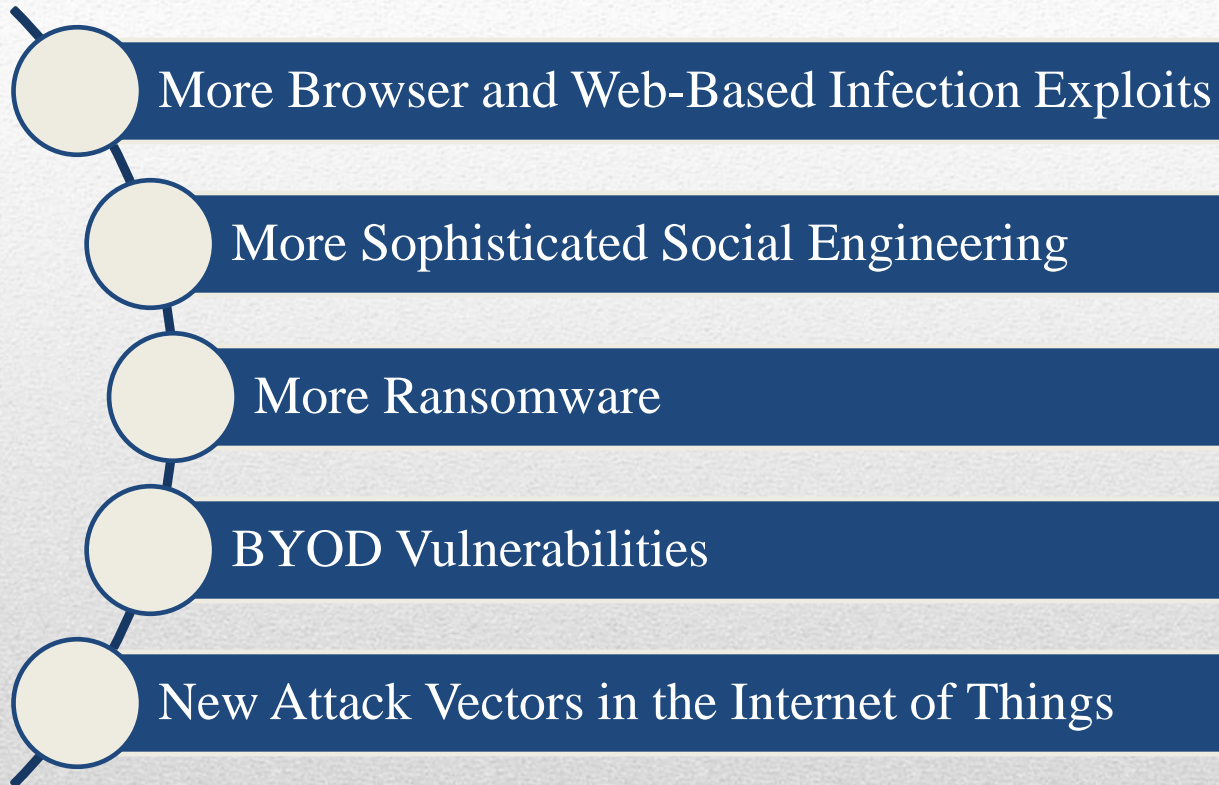
Bitcoin, Monero etc. are tradable digital assets for peer-to-peer transactions, esp. on the Dark Net further hardened by tumblers

---

# CHALLENGES

---





# FUTURE

---

- Offences Defined
  - Tampering of Source Code
  - Damage to computer system
  - Hacking
  - Data theft/ stolen password/ identity/ impersonation
  - Pornography
  - Access of Protected Systems
- Digital evidence is admissible
- Inspector & above can investigate
- Power to search public places - Cyber cafes
- CCA can order interception/ decryption
- Cases will be tried by normal courts

# **INFORMATION TECHNOLOGY ACT 2000 (Amended in 2008)**

---



Sl. No	Nature of complaint	Applicable section(s) and punishments under ITAA 2008	Applicable section(s) under other laws and punishment
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 IPC - 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 up to 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 66C of ITAA 2008- upto 3 years imprisonment and fine up to Rupees one lakh Section 66D 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 66C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	
6	A biometric thumb impression is misused	Section 66C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	
7	An electronic signature or digital signature is misused	Section 66C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	
8	A Phishing e-mail is sent out in your name, asking for login credentials	Section 66D 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

Sl. No	Nature of complaint	Applicable section(s) and punishments under ITAA 2008	Applicable section(s) under other laws and punishment
9	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
10	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	
11	Data Modification	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to Rupees five lakh or both	



Sl. No	Nature of complaint	Applicable section(s) and punishments under ITAA 2008	Applicable section(s) under other laws and punishment
12	Sending offensive messages through communication service, etc.	Section 66A of ITAA 2008 - upto 3 years imprisonment and fine	Section 500 IPC — upto 2 years or fine or both Section 504 IPC — upto 2 years or fine or both 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
13	Publishing or transmitting obscene material in electronic form	Section 67 of ITAA 2008 first conviction - upto 3 years and 5 lakh Second or subsequent conviction - upto 5 years and up to 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
14	Publishing or transmitting of material containing sexually explicit act, etc., in electronic form	Section 67A of ITAA 2008 first conviction - upto 5 years and up to 10 lakh Second or subsequent conviction - upto 7 years and up to 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
15	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	Section 67B of ITAA 2008 first conviction - upto 5 years and up to 10 lakh Second or subsequent conviction - upto 7 years and up to 10 lakh	Section 292 IP - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction

Sl. No	Nature of complaint	Applicable section(s) and punishments under ITAA 2008	Applicable section(s) under other laws and punishment
16	Misusing a Wi-Fi connection if done, against the state	Section 66 - upto 3 years imprisonment or fine up to Rupees five lakh or both Section 66F- life imprisonment of ITAA 2008	
17	Planting a computer virus if done, against the state	Section 66 - upto 3 years imprisonment or fine up to Rupees five lakh or both 66F- life imprisonment	
18	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 66F of ITAA 2008- life imprisonment	



Sl. No	Nature of complaint	Applicable section(s) and punishments under ITAA 2008	Applicable section(s) under other laws and punishment
19	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	
20	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	
21	Intermediaries not providing access to information stored on their computer to the relevant authorities	Section 69 of ITAA 2008 - imprisonment upto 7 years and fine	
22	Failure to Block Web sites, when ordered	Section 69A of ITAA 2008 - imprisonment upto 7 years and fine	
23	Sending threatening messages by e- mail	Section 66A of ITAA 2008 - upto 3 years imprisonment and fine	Section 504 - upto 2 years or fine or both
24	Word, gesture or act intended to insult the modesty of a woman		Section 509 IPC - upto 1 year or fine or both - IPC as applicable
25	Sending defamatory messages by e- mail	Section 66A of ITAA 2008 upto 3 years imprisonment and fine	Section 500 IPC - upto 2 years or fine or both
26	Bogus Web sites, cyber frauds	Section 66D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 419 - upto 3 years imprisonment or fine Section 420 IPC - upto 7 years imprisonment and fine
27	E-mail Spoofing	Section 66C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC — upto 2 years or fine or both Section 468 IPC — upto 7 years imprisonment and fine

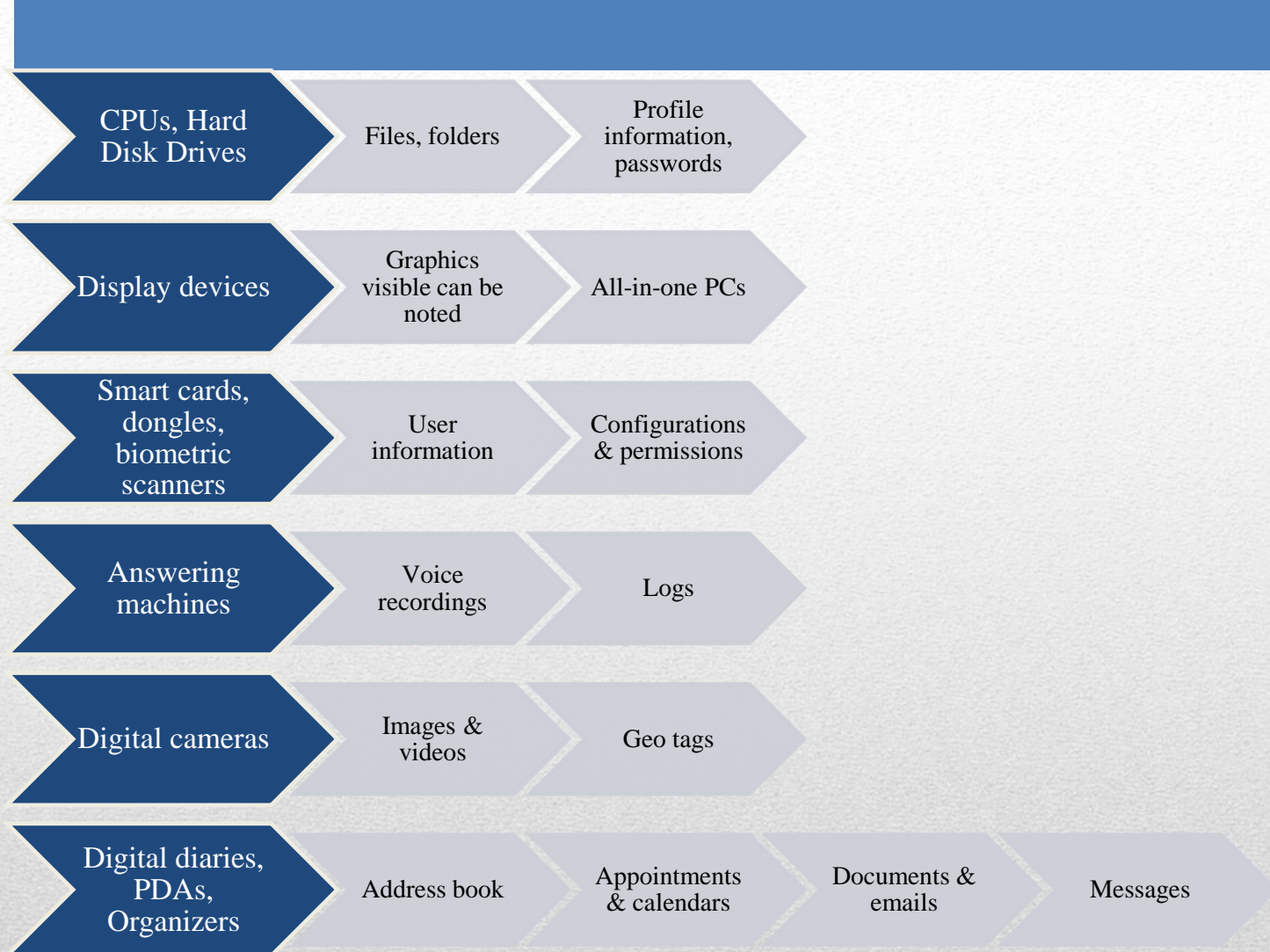
Sl. No	Nature of complaint	Applicable section(s) and punishments under ITAA 2008	Applicable section(s) under other laws and punishment
28	Making a false document	Section 66D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC - upto 2 years or fine or both
29	Forgery for purpose of cheating	Section 66D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section 468 IPC - upto 7 years imprisonment and fine
30	Forgery for purpose of harming reputation	Section 66D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh	Section. 469 IPC - upto 3 years and fine
31	E-mail Abuse	Section 66A of ITAA 2008 - upto 3 years imprisonment and fine	Sec. 500 IPC - upto 2 years or fine or both
32	Punishment for criminal intimidation	Section 66A of ITAA 2008 - upto 3 years imprisonment and fine	Sec. 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
33	Criminal intimidation by an anonymous communication	Section 66A of ITAA 2008 - upto 3 years imprisonment and fine	Sec. 507 IPC - upto 2 years along with punishment under section 506 IPC
34	Copyright infringement	Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to Rupees five lakh or both	Sec. 63, 63B Copyrights Act 1957
35	Theft of Computer Hardware		Sec. 379 IPC upto 3 years imprisonment or fine or both
36	Online Sale of Drugs		NDPS Act
37	Online Sale of Arms		Arms Act



- Sec. 65 A & B, IEA: Admissibility of digital evidence
  - Sec. 5: Evidence only for relevant facts
  - Sec. 136: Judge to decide admissibility
- Sec. 165 CrPC: Search by a police officer
- Sec. 100 CrPC: Persons I/C of closed place to allow search
- Sec. 80 ITAA: Power of police officer to enter, search and arrest without warrant
- Sec. 84-B ITAA: Punishment for abetment
- Sec. 84-C ITAA: Punishment for attempt

## **OTHER USEFUL PROVISIONS**

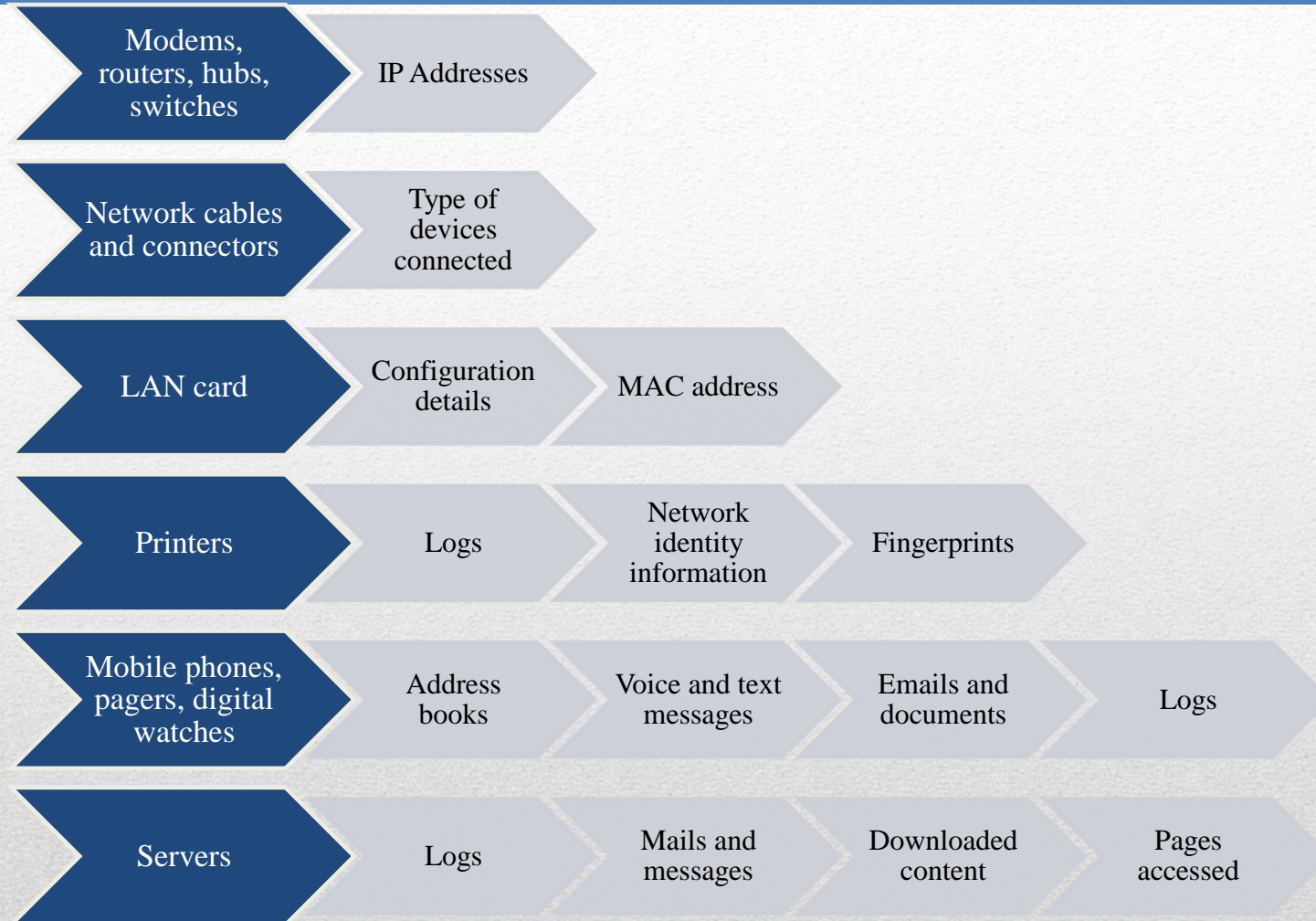
---



# SOURCES OF DIGITAL EVIDENCE

---

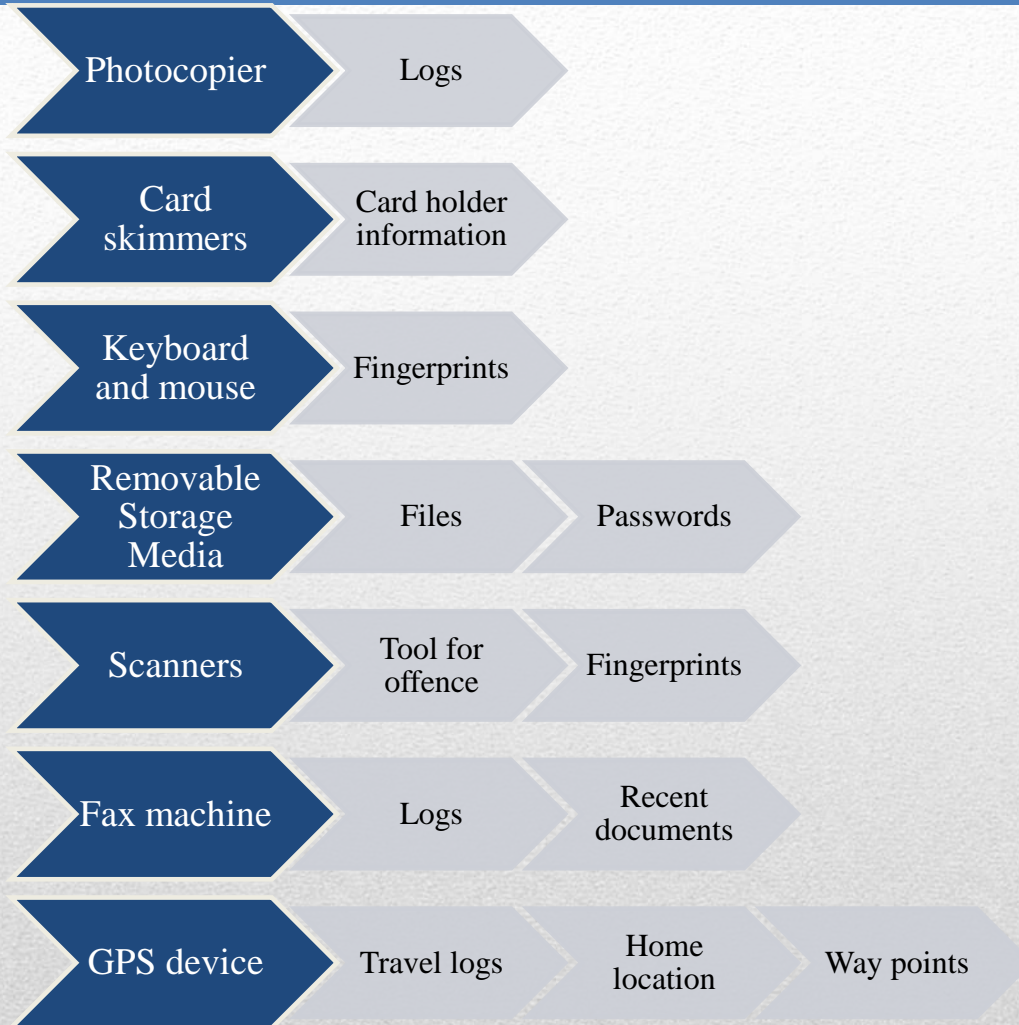




# SOURCES OF DIGITAL EVIDENCE

---





# SOURCES OF DIGITAL EVIDENCE

---

## Cyber Café or Office

- Number of computers – present; connected to internet
- Network topology and architecture
- CCTV camera recordings
- User management software?
- Log register
- Policy for formatting of storage devices
- Policy for removable media storage
- Recent hardware replacements

## Home

- Type of connection
- Number of computers
- Location of systems with details of persons accessing them
- Removable storage media
- Network topology
- Peripherals – printer, scanner, modem

# SCENE OF CRIME

---

What is the nature of incident?

Who discovered? How? When?

What is the loss?

What is the access level? Physical security? People in/ around?

What are the applications/ software/ database used?

Who are the developers of the applications?

Who provides support and maintenance?

Where are the servers?

Who is the administrator?

What is the intrusion prevention/ detection system?

Money Trail

Likely negligence by victim

# INVESTIGATION

---

# QUESTIONS OF INTEREST



## Switched off machines

- Complete seizure
- Open and identify hard disk, disconnect and label
- Signature of accused/ witness

## Switched on machines

- Record screen shot
- Record any movement – mouse, enter key
- Forensic tools to extract info in RAM etc.
- Last option – remove power cables from the machine end

# SEIZURE

---

# General

- If device is off, do not turn it on
- If PDA/Mobile is on, do not turn it off, try to keep it charged
- Label all cables
- Seize all relevant devices
- Seize other relevant items like diaries, documents etc.
- Document all steps
- Record Time Zone/ System
- Photograph everything before you start
- Photograph every step, every seized item separately
- Technical resource (if possible), Witnesses (mandatory)
- Record events in correct chronology
- Keep digital media in anti-static covers

# SEIZURE

---



```
graph TD; A[Notify the court regarding details of seizure] --> B[Obtain orders to retain the seized property for further investigation]; B --> C[Obtain orders to make bit-stream image of seized media and forward for forensic analysis]; C --> D[If accused approaches for release of seized material, ensure its opposition and if unavoidable, only provide a forensically imaged copy of seized evidence and never the original]; D --> E[Ensure chain of custody and proper recording of all transactions];
```

Notify the court regarding details of seizure

Obtain orders to retain the seized property for further investigation

Obtain orders to make bit-stream image of seized media and forward for forensic analysis

If accused approaches for release of seized material, ensure its opposition and if unavoidable, only provide a forensically imaged copy of seized evidence and never the original

Ensure chain of custody and proper recording of all transactions

# POST SEIZURE

---



Brief history of case

Details of exhibits

Date & time of seizure

Condition of item (on/off) at the time of seizure

Photographs/video, if taken

Was the machine connected to any network

Questionnaire

# FORENSIC EXAMINATION

---

Full Header displays the entire journey of email

Successive 'Message Transfer Agents' put their stamps

### Information

- Sender's email ID – last from top, just above recipient
- Internet routing information – last from top, above sender's ID
- Email server information – message ID
- Date, Time and Time Zone

Different email services have different ways to reveal full header

- Gmail masks source IP with its own private IP

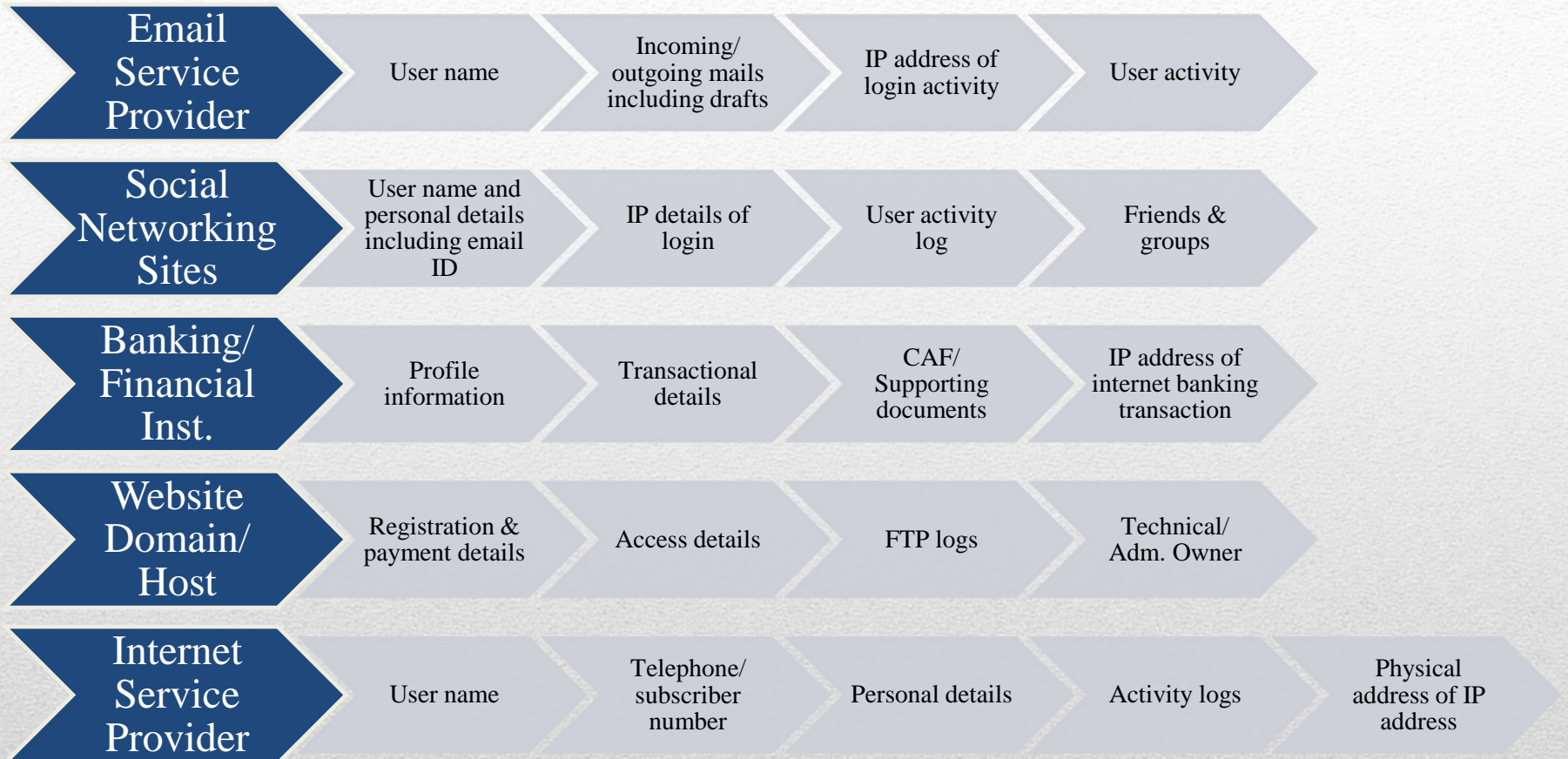
Who Is Search – APNIC, ARIN, LACNIC, RIPE NCC

Physical address from ISP

# EMAILS

---





# SERVICE PROVIDERS

---



Complaint



Preliminary information



Crime scene visit



Evidence identification, collection and preservation



Examination by FSL



Interpretation of FSL report



Reconstruction of case



Mapping of accused with each offence

# EVIDENCE IN COURT

---



# USEFUL RESOURCES

---



**THANKS**

---