GH raisoni COLLEGE | Engineering and Management Nagpur

raisoni EDUCATION

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING (CYBER SECURITY)

Subject : Digital Forensics (PE-III)

(23BTCYL321)

7th Semester

2025-26

Course Objective

1. To understand underlying principles and many of the techniques associated with the digital forensic practices and cyber-crime.

2. To investigate attacks, IDS. Technical exploits and router attacks and “Trap and Trace” computer networks

3. To learn the importance of evidence handling and storage for various devices.

4. To apply digital forensic knowledge to use computer forensic tools and investigation report writing..

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING (CYBER SECURITY)

Course Outcomes

CO1: **Analyze** threats in order to protect or defend it in cyberspace from cyber-attacks

CO2: Develop appropriate security solutions against cyber attacks..

CO3: Select different types of tools for various phases of forensics investigation

CO4: Apply forensic techniques to analyze mobile and email communication evidence in digital investigations.

CO5: **Create** reports as per standards of digital forensics.

Unit	Contents	Hours
I	**Fundamentals of Digital Forensics** Foundations of Digital Forensic: Digital evidence, Awareness, Principles of Digital Forensic,Challenging aspects of digital evidence, Cyber trail. Language of Computer Crime Investigation:Role of Computers in crime, Cybercrime law, offenses, jurisdiction. Traffic analysis, Fraud, IT Act	6
II	**Computer Forensic** Digital Evidence : Digital evidence in courtroom: Duty of experts, Admissibility, Locard's exchange principle, Types of Evidence, The Rules of Evidence, Volatile Evidence, Evidence collection andArchiving , Methods of Collection , Collection Steps, Controlling Contamination: The Chain of Custody. Processing Computer Crime : Introduction to Crime Scenes, Seizing and storing digital evidence at scene, Documenting the Scene and the Evidence , Dealing with Live Systems and Dead Systems, Using Hashing to Verify the Integrity of Evidence.	7
III	**Data Acquisition and Data Recovery** Data acquisition- Understanding storage formats and digital evidence, determining the best acquisition method, acquisition tools, validating data acquisitions, performing RAID data acquisitions, remote network acquisition tools, other forensics acquisitions tools Data Recovery: Data Backup and Recovery, The Role of Backup in Data Recovery, The Data-Recovery Solution Hiding and Recovering Hidden Data, Data Handling tools, ISO 27001.	6
IV	**Mobile device Forensic and Email Forensics** Mobile Device Forensics, Types of evidence on mobile device, Handling mobile device as a sources of evidence, Forensic prevention of mobile devices, Forensic examination , analysis of mobile devices, Forensic acquisition , examination of SIM cards (Architecture, Data Storage, Files, Mobile Operating System), Investigative reconstruction using mobile devices, Mobile Forensics and its challenges, Email Forensics: EMail Header Analysis, Function & Forensics, Chat and Social Networking Evidence. Case study	7
V	**Forensic Investigation Report and Forensic Tools:** Goals of Report, Layout of an Investigative Report, Guidelines for Writing a Report, sample for writing a Forensic report. Computer Forensic Tools: need and types of computer forensic tools, task performed by computer forensic tools. Study of open source Tools like SFIT, Autopsy etc. to acquire, search, analyze and store digital evidence. Case study	7

Text Books	1. Digital Evidence & Computer Crime – Forensic science, Computers & The Internet', Eoghan Casey, 3rd edition 2. 'Computer Forensics Computer Crime scene investigation', 2nd edition, Johm R. Vacca 3. Cyber Law Simplified, Vivek Sood 4. Basics of Digital Forensics, Second edition – John Sammons
Reference Books	4.Computer Forensics Investigating Network Intrusions & Cybercrime', EC–Council press, Cengage Learning 5. Guide to Computer Forensics & Investigations, 4th edition, Bill Nelson, Amelia Phillips & Christopher Steuart, Cengage Learning 6. 'Guide to Integrating Forensic Techniques into Incident Response', NIST, Karen Kent, Suzanne Chevalier Tim Grance, Hung Dang

TAE

- **TAE-I : based on till 2.5 unit**

  Schedule 12th Jan 2026

- **TAE-II: based on 2.5 to 5**

  Schedule 4th March 2026

CAE

- **CAE-I : based on till 2.5 unit**

  Schedule ……. 2026

- **CAE-II: based on 2.5 to 5**

  Schedule 4th March 2026

Uses of the system in Cyber Crime

?

- Computer as Target
- Computer as Use

Cyber Crime

- **Cyber-trespass(**CT is act of tracing the boundaries & connect with the unauthorized network**)**

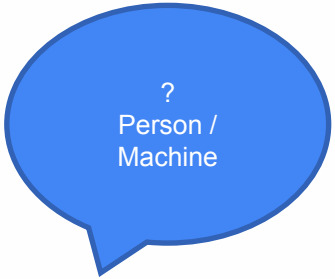
Coffee Shop

- **Cyber- Deception(**CD is like a phishing, to collect the Info. of the victim**)**

Lottery Email

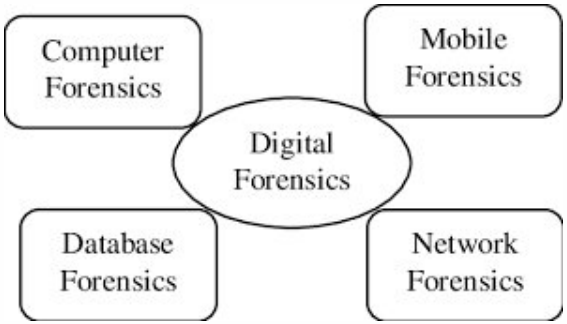
- **Cyber-Violence(**Promoting a social/economic/religious msg. Where an intension is to disurpt the society**)**

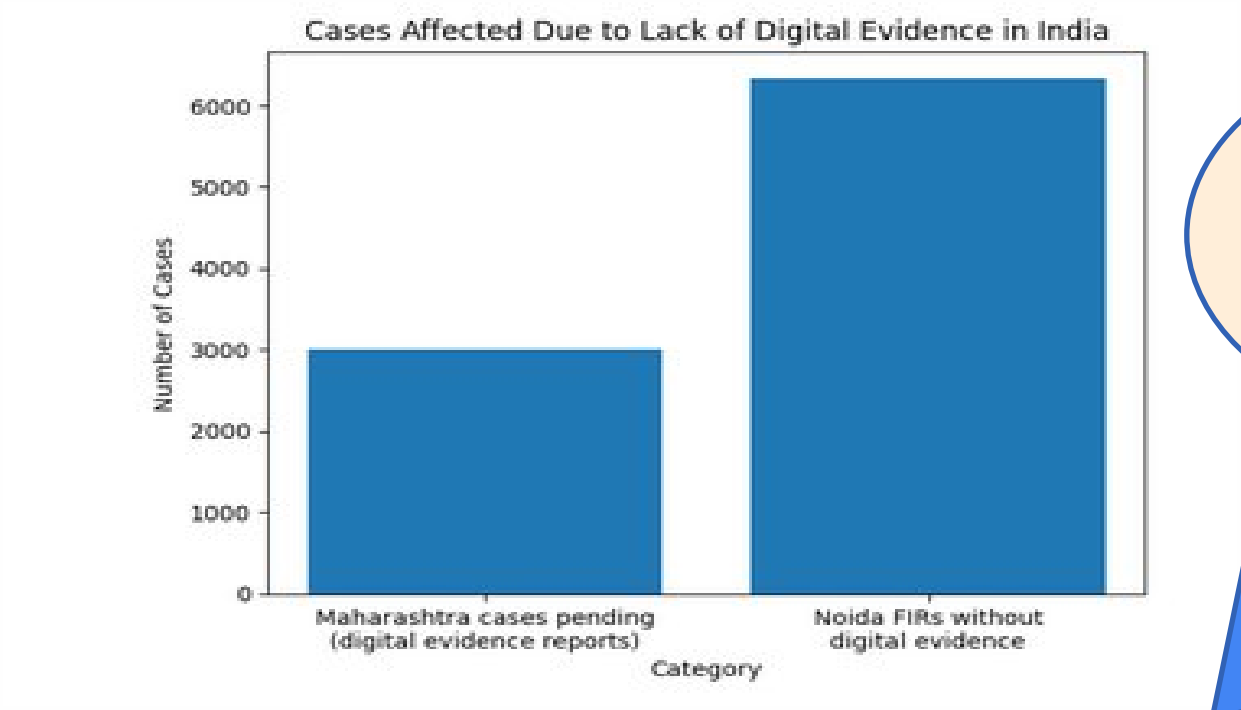
Water Plant/ATS



What is Digital Forensic?

Digital forensics is a part of **forensic science** that focuses on ***identifying***, ***acquiring***, ***processing***, ***analyzing***, and ***reporting*** on data stored electronically.



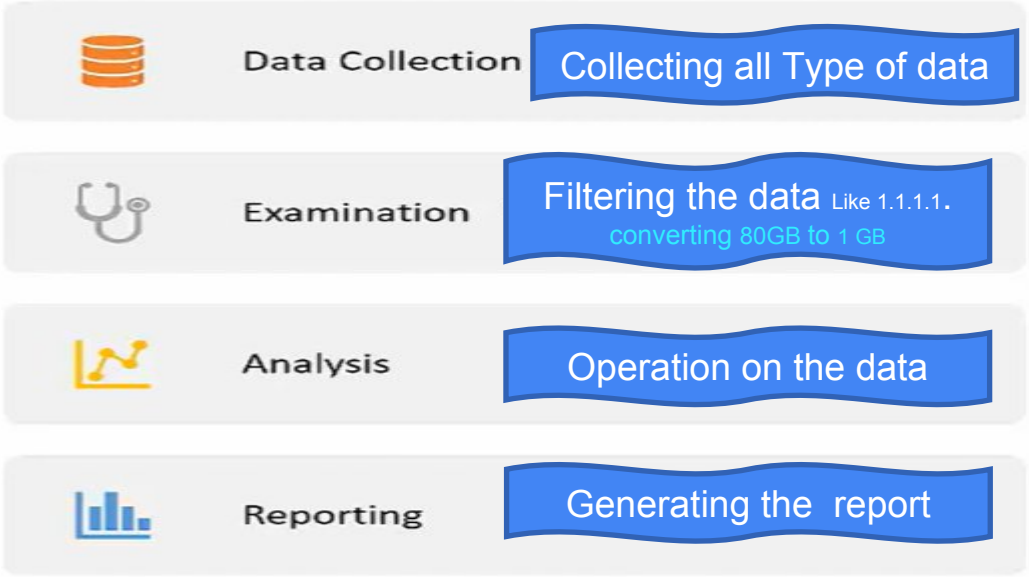


Noida, out of **7,322 FIRs** filed over one year, only **~978 cases (13%)** had digital evidence uploaded in the required ***e-Sakshya system.***

India recorded **123,672 "digital arrest" scam cases in 2024 (₹*1,935 crore*)**

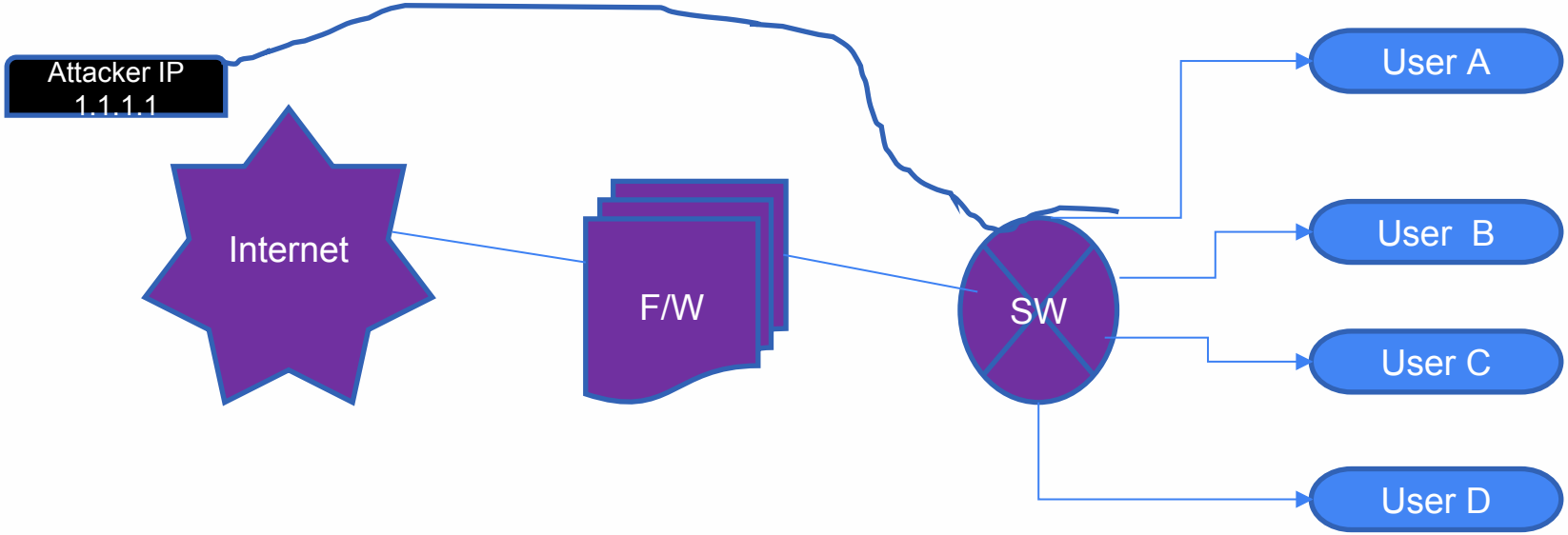
Source: TOI

Digital Forensic Process



Next Page
Dia.

Why Digital Forensic Important



Comparative Summary Table for Process of Digital Forensic

Stage	Role	Outcome
Data Collection	Preserve evidence	Authentic, admissible data
Examination	Extract relevant data	Organized evidence
Analysis	Interpret data	Conclusions & timelines
Reporting	Present findings	Court-ready report

Digital Evidence

purpose of Section 79A of the IT Act, 2000

Digital evidence is defined as ***information*** and ***data*** of value to an **investigation** that is **stored** on, **received** or **transmitted** by an *electronic device.*

Example of DE:
Files (documents, images, videos)
Emails and chat messages
Call logs and SMS
Social media data
System logs
Browser history
Network traffic records
Metadata (date, time, location)

Types of Digital Evidence

1. Based on Nature of Data

Types of Digital Evidence

Digital Evidence Types

Volatile Evidence

- Memory
- Network Connections
- Running Process
- Open Files

Non-Volatile Evidence

- Hard Drives
- USB Storage
- Floppy Disks
- CD/DVD



2. Based on Source of Evidence

Mobile Device Evidence

- Call logs, SMS, WhatsApp chats
- App data, GPS location
- Photos, videos, contacts

Network & Internet Evidence

- IP addresses, firewall logs
- Server logs
- Network traffic captures

Cloud-Based Evidence

Emails (Gmail, Outlook)

- Cloud storage (Google Drive, OneDrive)
- Social media data

Principles of Digital Forensics

Proper documentation of who handled the evidence, **when, where, and why**.



Creating a **forensic image** instead of working on the original hard disk.

Challenges of Digital Evidence

WHAT'S THE CHALLENGE ?



Digital evidence has a **wider scope**, can be **more personally sensitive**, is **mobile**, and **requires different training and tools** compared to physical evidence



Challenges of Digital Evidence





Volatility of Digital Data
Data can be easily altered, deleted, or overwritten



Maintaining Integrity and Authenticity
Small changes can question credibility of evidence



Chain of Custody Issues
Improper documentation breaks the chain of custody



Encryption and Password Protection
Encrypted devices and data are hard to access



Large Volume of Data (Big Data Problem)
Time-consuming analysis of massive datasets



Cloud and Cross-Border Jurisdiction
Foreign data storage leads to legal complications



Rapid Technological Change
New devices and methods emerge frequently

Cyber trail

Path that shows *who did what, when, where, and how* in the digital environment.

Cyber Trail

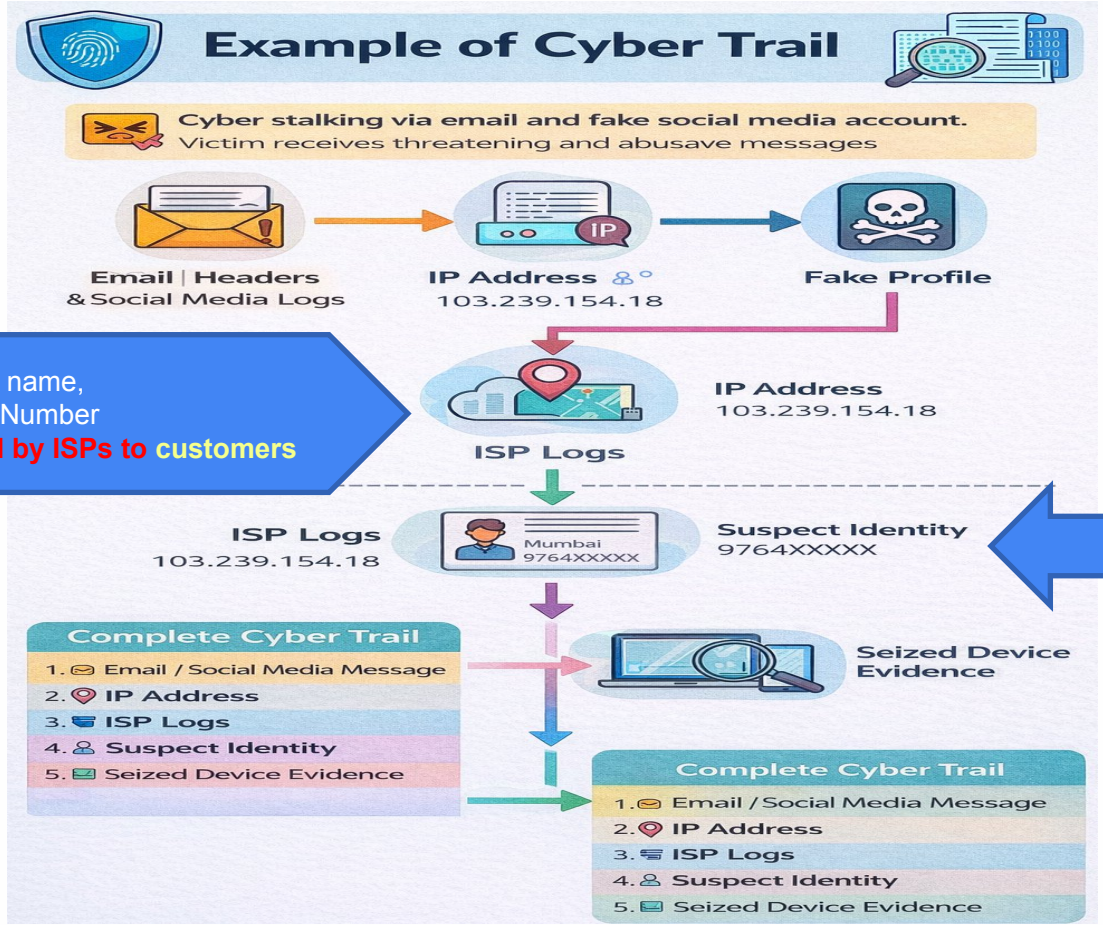
The sequence of digital footprints or traces left behind by a user's /attacker activities in cyberspace, which can be collected, analyzed, and presented as **digital evidence** during an investigation or in court.

Police use cyber trails to uncover large-scale fraud networks,

Cyber Trail

- **Logs**,
- **browsing history**,
- **emails**,
- **chat records**, and
- **file systems**

that investigators analyze to understand **how a cyber attack happened** and **who was involved**.



Subscriber name,
Reg.Mobile Number
IP addresses are assigned by ISPs to customers

Purpose:
Moves the case from ***unknown*** **offender to known suspect**.

Delhi Police's "Cyber Hawk" operation that tracked **Rs 944 cr.** in fraud..(They found the various Mule a/c)

Sections | EDITION India | Friday, Dec 26, 2025 | EPAPER | TODAY'S PAPER

ENGLISH | தமிழ் | বাংলা | മലയാളം | ગુજરાતી | हिंदी | मराठी | BUSINESS | बिज़नेस | Newsletters

The Indian EXPRESS
JOURNALISM OF COURAGE

Home | ePaper | India | UPSC | Premium | Entertainment | Politics | Sports | World | Explained | Opinion | Business | Cities | Lifestyle | Tech | Subscribe

TRENDING | New Year Offer | Legal News | Yearenders 2025 | UPSC Offer | Research | Games | Archives | Fresh Take | Podcast

ADVERTISEMENT

Over 1,100 held, Rs 944 crore traced: Crackdown on cybercrime networks under Operation CyHawk 2.0 in Delhi

Delhi Police said Operation CyHawk 2.0 led to over 1,000 arrests and the tracing of ₹944 crore in defrauded money, marking a sharp rise in action against organised cybercrime networks compared to the first phase of the drive.

By: Express News Service
December 13, 2025 07:43 AM IST
2 min read

As Trusted Source on



ADVERTISEMENT

TOP STORIES

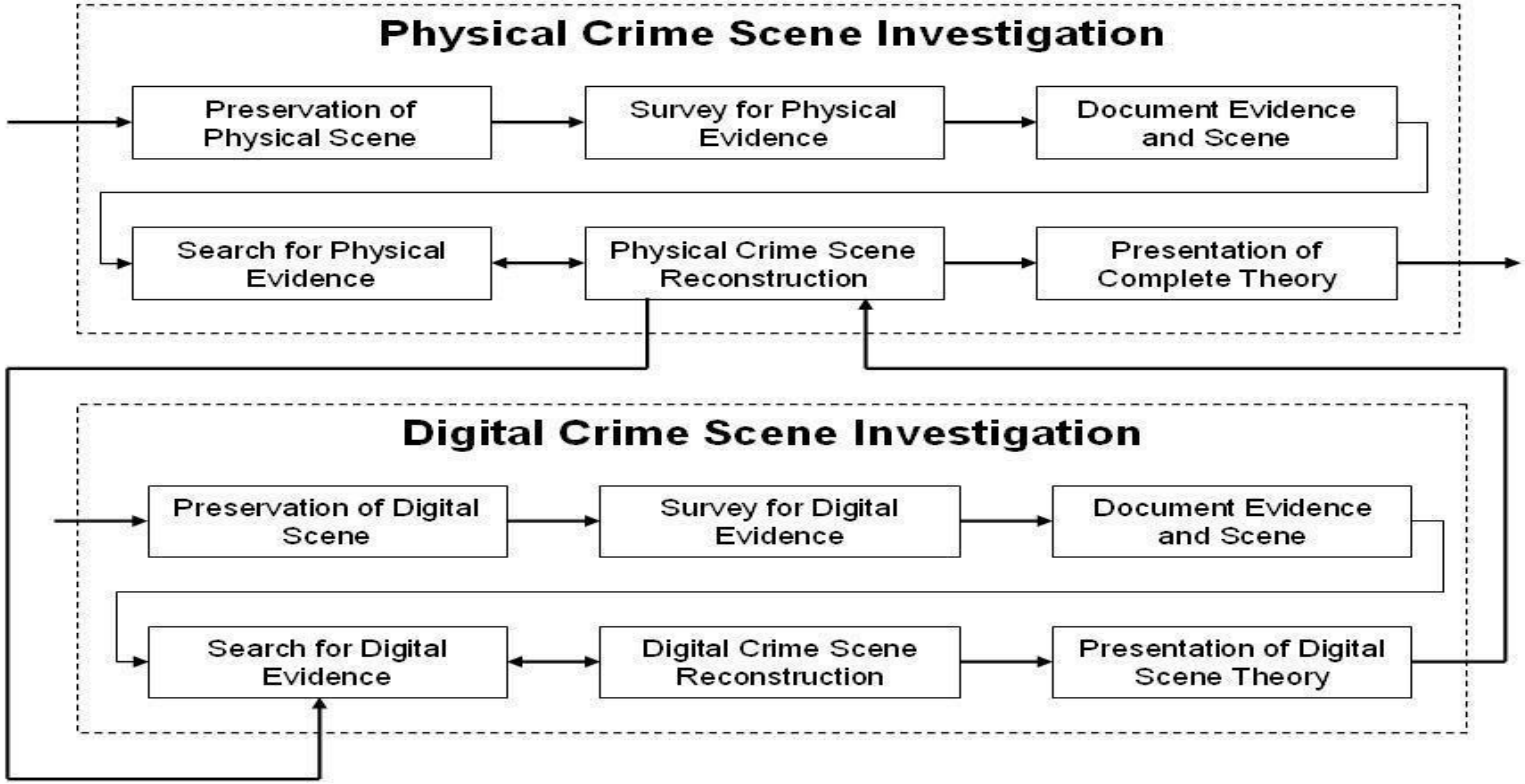


Computer Crime Investigation

Delhi Police's "Cyber Hawk" operation that tracked Rs 944 crore in fraud

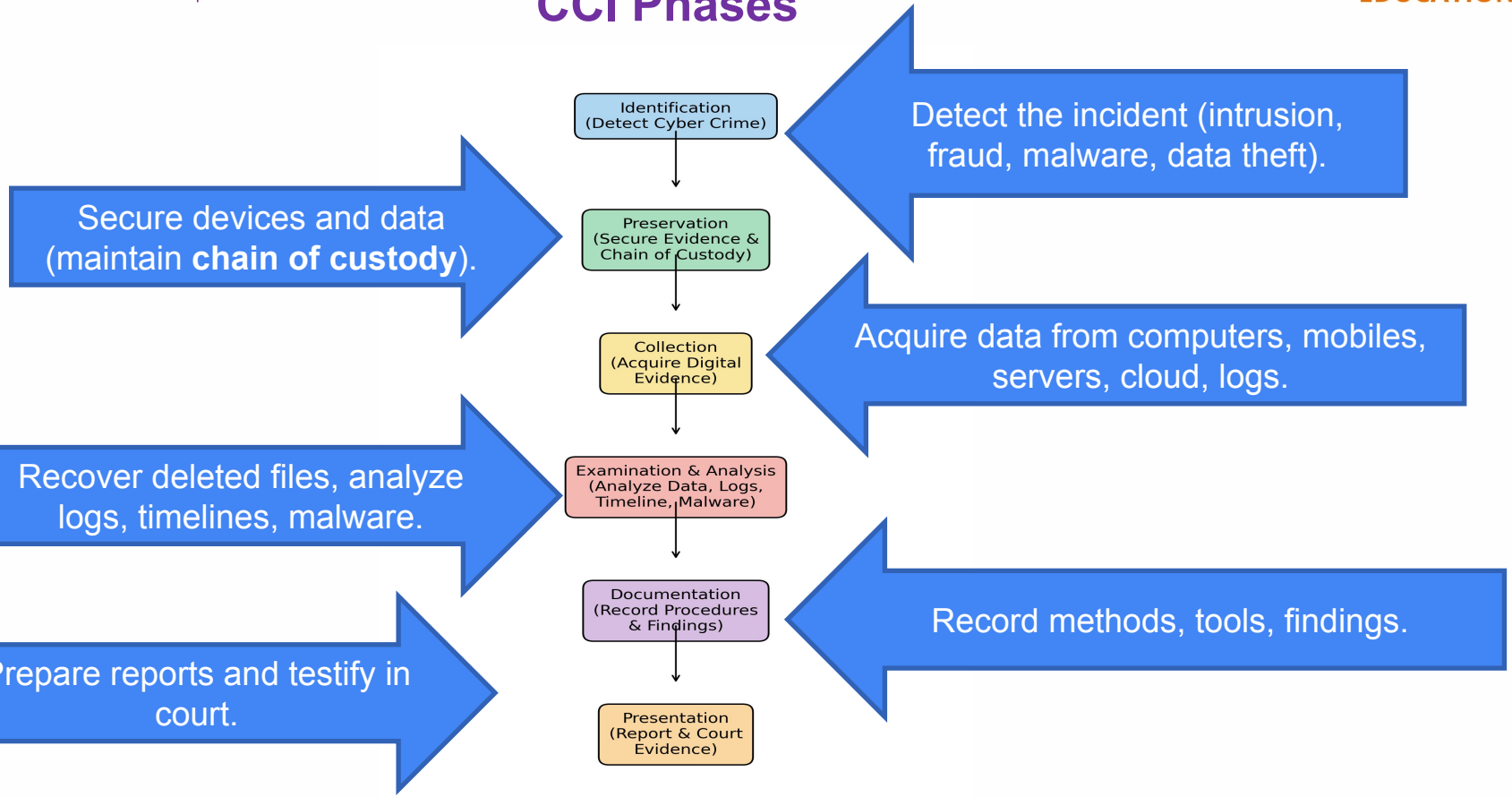
Investigating computer crimes is about finding and stopping bad activities that happen on computers and digital devices.

Difference between Physical Crime Investigation & Digital Crime Investigation


Physical Crime Scene Investigation
Preservation of Physical Scene
Survey for Physical Evidence
Document Evidence and Scene
Search for Physical Evidence
Physical Crime Scene Reconstruction
Presentation of Complete Theory
Digital Crime Scene Investigation
Preservation of Digital Scene
Survey for Digital Evidence
Document Evidence and Scene
Search for Digital Evidence
Digital Crime Scene Reconstruction
Presentation of Digital Scene Theory

Physical Crime Investigation	Digital Crime Investigation
Investigation of crimes involving tangible objects, people, or locations.	Investigation of crimes involving computers, networks, and digital devices.
Physical location (home, street, office).	Digital environment (computer system, networks, mobile devices, cloud servers).
Evidence like fingerprints, weapons, blood, fibers, documents.	Digital evidence like emails, log files, databases, images, browser history, metadata.
Crime scene kits, fingerprint kits, cameras, chemical tests.	Forensic software (EnCase, FTK, Autopsy), network analyzers (Wireshark), malware analysis tools.
Knowledge of criminal law, physical evidence handling, observation skills.	Knowledge of computers, networks, operating systems, encryption, forensic tools.
Ex. Murder, burglary, assault.	Ex. Hacking, phishing, ransomware attack, online fraud.

CCI Phases


Identification (Detect Cyber Crime)
Detect the incident (intrusion, fraud, malware, data theft).
Preservation (Secure Evidence & Chain of Custody)
Secure devices and data (maintain **chain of custody**).
Collection (Acquire Digital Evidence)
Acquire data from computers, mobiles, servers, cloud, logs.
Examination & Analysis (Analyze Data, Logs, Timeline, Malware)
Recover deleted files, analyze logs, timelines, malware.
Documentation (Record Procedures & Findings)
Record methods, tools, findings.
Presentation (Report & Court Evidence)
Prepare reports and testify in court.

GH raisoni COLLEGE | Engineering and Management Nagpur

raisoni EDUCATION

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING (CYBER SECURITY)

Subject : Digital Forensics (PE-III)

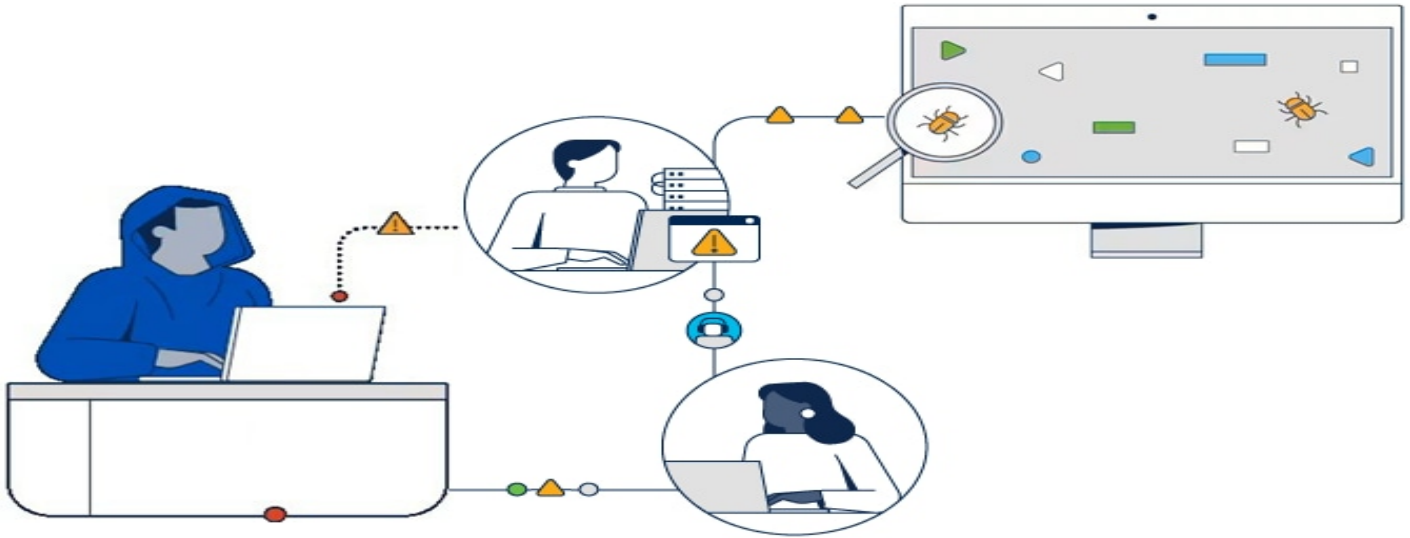
(23BTCYL321)

7th Semester

2025-26

Role of Computers in crime

Role of Computer



1. Computer as a Target

- Hacking and unauthorized access
- Malware, ransomware attacks
- Data theft or data destruction

Example: Stealing confidential data from a server

2. Computer as a Tool

- Online fraud and phishing
- Identity theft
- Cyber stalking and harassment
- Spreading malware or fake news

Example: Sending phishing emails to steal banking credentials.

3. Computer as a Storage Device

- Storing illegal files, images, videos
- Maintaining fraud records
- Saving communication logs and transaction details

Example: Laptop containing fake account details.

Example: Call logs and emails used in court proceedings..

4. Computer as an Evidence

- Emails, chat records
- Browsing history and logs
- Transaction details

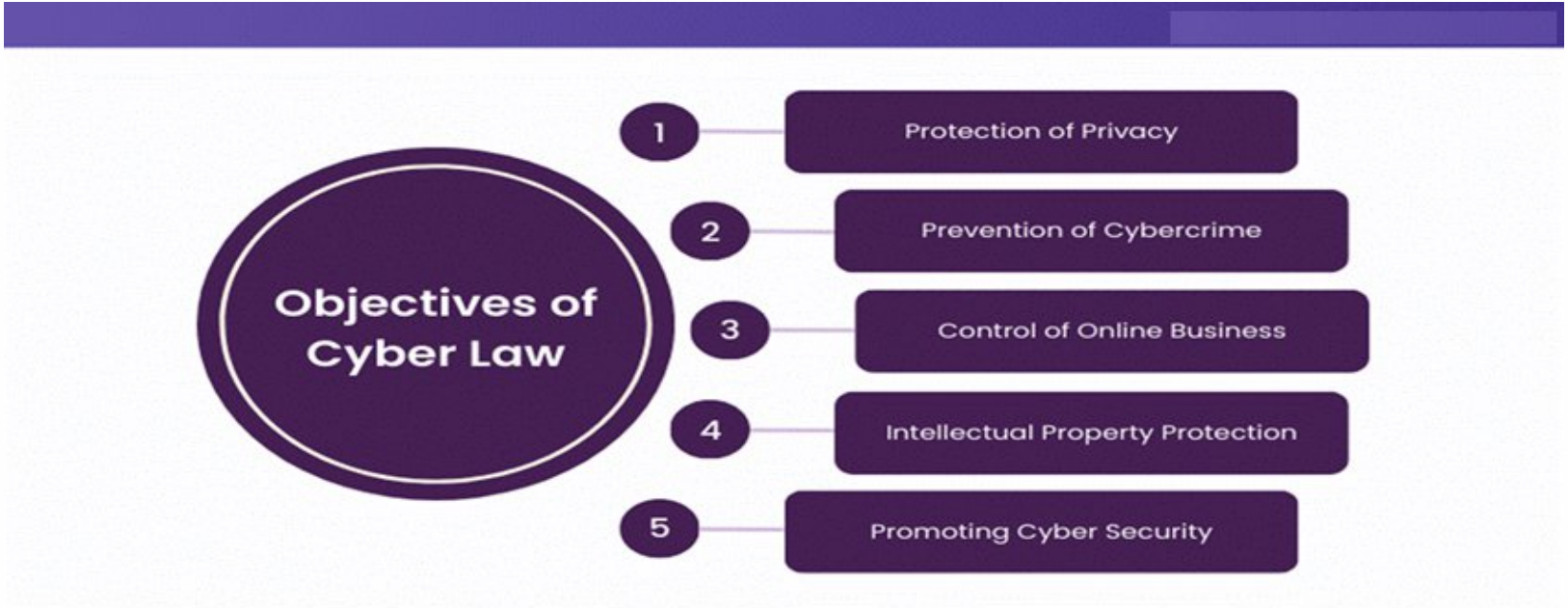
5. Computer as Communication Medium

- Encrypted messaging apps
- Dark web platforms
- Social media misuse

Example: Criminal coordination through messaging apps.

Cybercrime law

Cybercrime law is the branch of law that deals with **offences committed** through **computers, networks**, and the **internet** and prescribes **legal action** against such crimes.


Objectives of Cyber Law
1
Protection of Privacy
2
Prevention of Cybercrime
3
Control of Online Business
4
Intellectual Property Protection
5
Promoting Cyber Security

Core Laws

Information Technology Act, 2000 (IT Act): The foundational law, addressing digital records, e-governance, e-banking, and cybercrimes like unauthorized access (Sec 66) and publishing obscene content (Sec 67).

IT Act, 2000 deals with cyber activities and cyber offences.
The bill was passed by Parliament in **May-June 2000**.
Enforcement:- 17th October 2000.

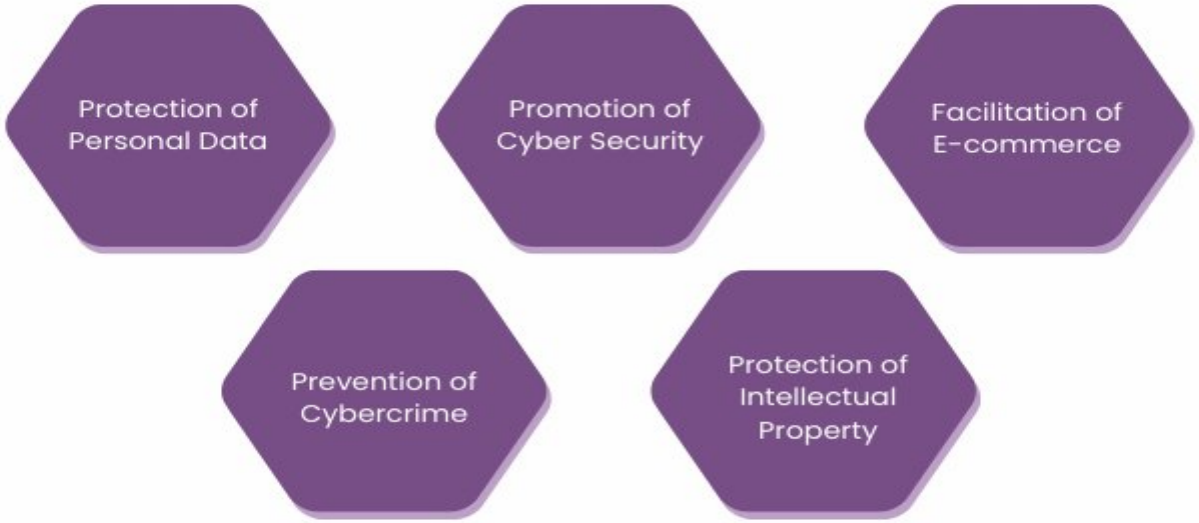
Digital Personal Data Protection Act, 2023 (DPDP Act): A key recent law focusing on consent, data processing, user rights (access, correction), and data breach notifications.

DPDP Act, 2023 deals with protection of personal data and privacy.
7th August 2023 – Bill Passed in Parliament .
Enforcement:- November 2025

Importance of Cyber Law



Benefits of Cyber Law



IT Act

IT Act

It provides a legal framework for the use of computers, the internet, and digital communication.

Bharatiya Nyaya Sanhita (BNS): Effective from July 1, 2024, the BNS (replacing the Indian Penal Code) includes provisions for traditional crimes committed in cyberspace, such as cheating (Section 318) and forgery (Section 336).

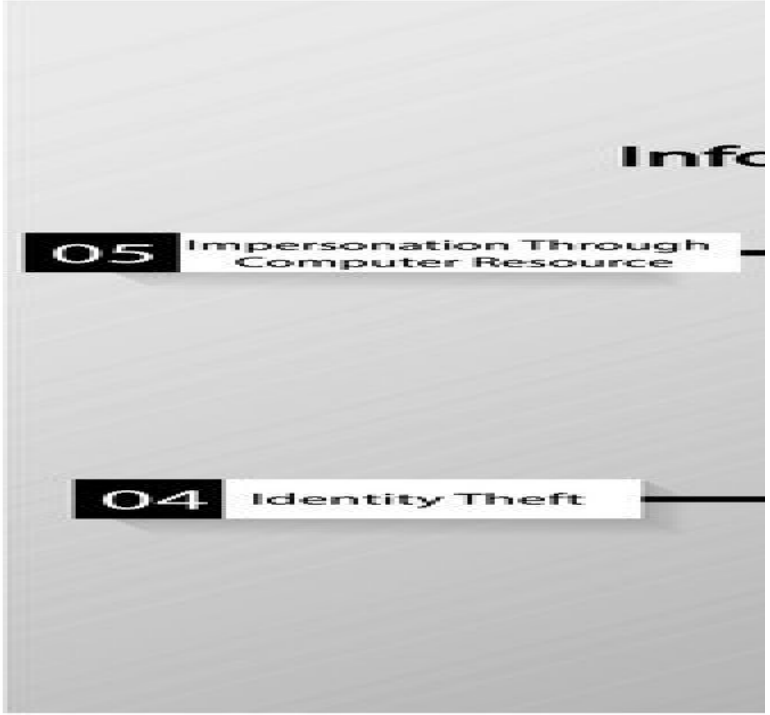
- **2008 Amendment:** Introduced comprehensive cybersecurity provisions, including the role of **CERT-In** (Indian Computer Emergency Response Team) and updated data protection standards for corporate bodies.

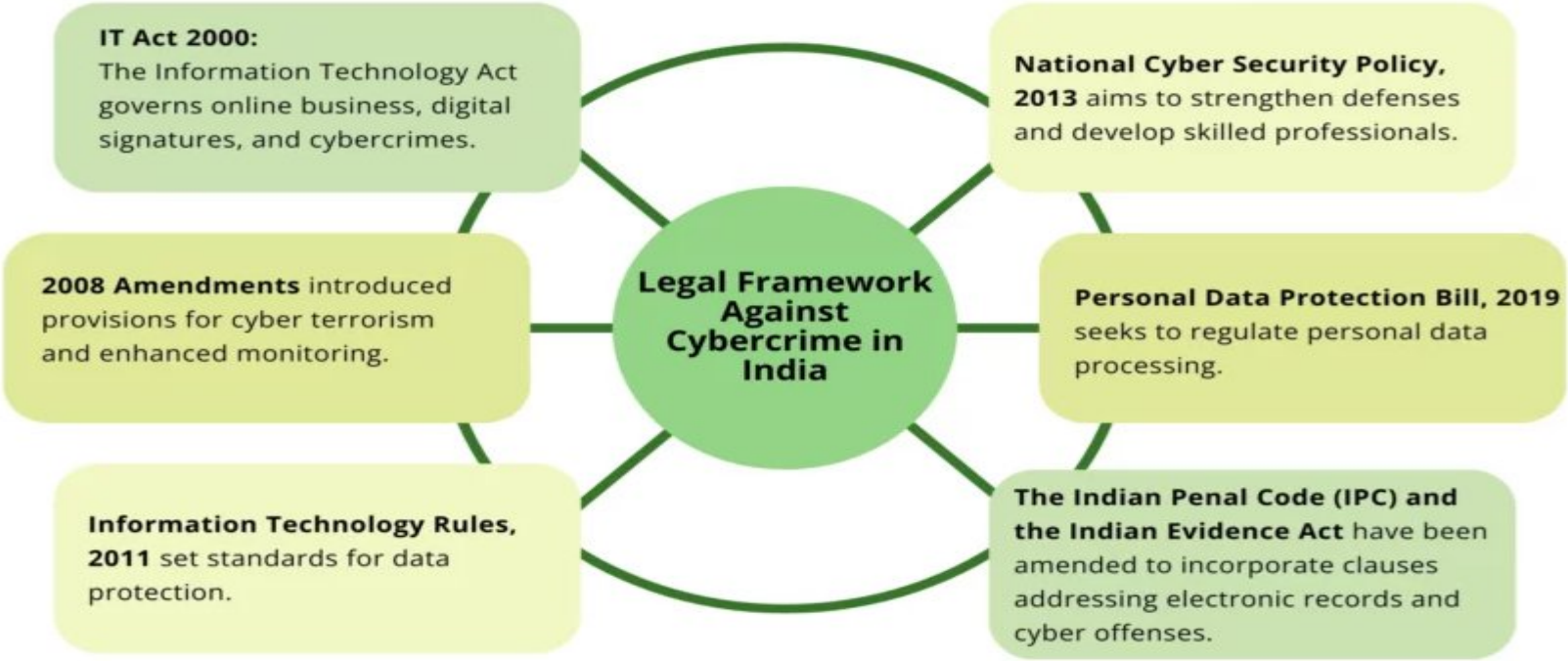
Section 66A Strike-down (2015): In the landmark *Shreya Singhal v. Union of India* case, the Supreme Court struck down Section 66A (which penalized "offensive" online messages) for violating the fundamental right to freedom of speech.

IT Rules, 2021/2023: Introduced stricter guidelines for social media intermediaries and digital media, requiring grievance redressal mechanisms and "safe harbor" compliance for content moderation.

2025 Amendment Rules: Effective from **November 15, 2025**, these rules introduce safeguards requiring senior-level authorization (Joint Secretary rank or higher) for content takedown orders to ensure transparency and accountability.

It is legal framework designed to **prevent, investigate, and punish crimes committed using computers, networks, and the internet**.




Legal Framework Against Cybercrime in India
IT Act 2000: The Information Technology Act governs online business, digital signatures, and cybercrimes.
National Cyber Security Policy, 2013 aims to strengthen defenses and develop skilled professionals.
2008 Amendments introduced provisions for cyber terrorism and enhanced monitoring.
Personal Data Protection Bill, 2019 seeks to regulate personal data processing.
Information Technology Rules, 2011 set standards for data protection.
The Indian Penal Code (IPC) and the Indian Evidence Act have been amended to incorporate clauses addressing electronic records and cyber offenses.

DPDP Act

The **Digital Personal Data Protection Act, 2023** is India's primary law governing the **processing of digital personal data**.

It aims to:

- Protect individuals' (Data Principals') privacy
- Enable lawful data use by organisations (Data Fiduciaries)
- Establish enforcement through the **Data Protection Board of India (DPBI)**

Data Protection Board of India (DPBI)

Its main job is **to look into complaints** and **take action** when someone misuses or mishandles your personal data online.

Workflow Process of Data Protection Board of India (DPBI) under the DPDP Act, 2023

- A Data Principal files a complaint after fiduciary grievance mechanisms fail.

Step 1: Complaint or Trigger

Board examines whether the complaint falls within its jurisdiction.

Step 2: Preliminary Scrutiny

Fiduciary receives formal notice with allegations.

Step 3: Notice to Fiduciary

Determines *why* (purpose) and *how* (means) personal data is collected- Believable

Board may call for documents, audit reports, and system logs.

Step 4: Inquiry and Investigation

Board decides whether breach occurred and assesses its gravity.
.

Step 5: Determination of Non-Compliance

- Monetary fines imposed based on statutory factors.
- Corrective actions (e.g., erasure, halting transfers) may also be ordered.

Step 6: Penalty or Corrective Order

Orders are published to ensure transparency.

Step 7: Publication of Order

Fiduciary may appeal to higher judicial forums.

Step 8: Appeal

Differentiate between
IT Act 2000 Vs DPDP Act 2023

Basis Content	Information Technology Act, 2000	Digital Personal Data Protection Act, 2023
Main Objective	Regulates electronic records, e-commerce, and cybercrimes	Protects digital personal data and privacy
Define Board	Not define any Special Board	Form a **Data Protection Board of India**
Nature of Law	Technology & cybercrime law	Data protection & privacy law
Year	2000 (amended in 2008)	2023 & Actually an enforced in 2025
Type of Data covered	Electronic data & computer resources	Digital **personal data** only
Focus Area	Cyber offences, electronic governance	Rights of individuals over personal data
Consent Requirement	Limited and indirect	Mandatory, free, informed, and revocable
Penalties	Compensation and fines (lower amounts)	Monetary penalties up to ₹250 **crore**