CYBER LAWS
DIGITAL EVIDENCE
HANDLING OF DIGITAL EVIDENCE

Presentatiton by:
Shri Jabyang Dorjee Sherpa
Chief Judicial Magistrate- Civil Judge (Sr Divn)

WHAT ARE CYBER LAWS

Cyber laws are the laws that governs activities in cyberspace—covering issues like online crimes, data protection, digital signatures, electronic commerce etc.

The backbone of India's cyber law system is the:

1. Information Technology Act, 2000

This is the primary Cyber Law in our Country.

Important sections:

- **Section 43** – Unauthorized access, data theft, virus attacks
- **Section 66** – Computer-related offences (hacking)
- **Section 66C** – Identity theft
- **Section 66D** – Online cheating (phishing, fraud)
- **Section 67** – Publishing obscene content online

2. Information Technology (Amendment) Act, 2008

This amendment strengthened the original IT Act.

Key additions:

- Introduced data protection and privacy provisions
- Recognized cyber terrorism (Section 66F)

WHAT ARE CYBER LAWS

- Defined intermediary liability
- Introduced sensitive personal data rules
- Section 2(1)(w) of the Information Technology Act, 2000 states that 'intermediary, concerning any particular electronic records, means any person who on behalf of another person receives, stores, or transmits that record or provides any service concerning that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places, and cyber cafes (e.g., social media platforms face book, instagram, X, online commerce website)

WHAT ARE CYBER LAWS

CLASH BETWEEN IPC and IT ACT

- *Sharat Babu Digumarti v. Govt. of NCT of Delhi* [AIR 2017 SC 150], the Supreme Court held that when the actions of an accused fall within the scope of offences under both the IT Act and the IPC which have the same ingredients, a charge under the former makes a charge under the latter impermissible. The reasoning given was twofold – first, that the IT Act, being a special law, overrides the general law and second, that the IT Act contains a non-obstante provision under Section 81 which gives its provisions an overriding effect over any law in force. Accordingly, the Court held that that the test to determine obscenity under Section 67 IT Act [punishment for publishing obscene material in electronic form] was of an "*identical nature*" to the test under Section 292 IPC [obscenity]. Therefore, a discharge under Section 67 IT Act made a charge under Section 292 IPC impermissible.

3. Digital Personal Data Protection Act, 2023

India's modern data protection law.

Key highlights:

- Governs how companies collect and process personal data
- Requires user consent
- Gives individuals rights over their data
- Imposes penalties for data breaches

CYBER LAWS

RIGHT TO PRIVACY

The **conflict between Apple Inc. and the Federal Bureau of Investigation (FBI) over privacy** is one of the most important modern legal battles about encryption, digital evidence, and individual rights.

Background: The San Bernardino Attack (2015)
In December 2015, a terrorist attack occurred in San Bernardino, California killing 14 people.

One of the attackers, Syed Rizwan Farook, had an iPhone (5C). After the attack, the FBI recovered the phone but couldn't access its data because it was locked and encrypted.

The Government's Demand
The FBI asked Apple to help unlock the phone.
Specifically, they wanted Apple to:
Create a special version of iOS (Apple's operating system)
Disable security features like:

- Auto-erase after 10 wrong passcode attempts
- Delay between password guesses

Apple’s Refusal Apple, led by CEO Tim Cook, refused.
Apple’s main arguments:
Creating such software would be a “backdoor”
It would weaken security for all iPhone users
Once created, it could be misused by:

- Governments
- Hackers

It violated user privacy and trust
Tim Cook publicly stated that complying would be dangerous for civil liberties.
Legal Battle Begins
In 2016, a U.S. court ordered Apple to help the FBI.
Apple challenged the order. Before the appeal case could be decided, the FBI announced:
They had unlocked the phone without Apple’s help
Australian security firm Azimuth Security

So the case was withdrawn
Raises key questions:

- Should tech companies assist law enforcement?
- Where is the limit of state power?

VARIOUS KINDS OF DIGITAL EVIDENCE

- Emails, SMS, WhatsApp chats
- Social media posts (Instagram, Facebook, X)
- CCTV footage, call recordings
- Server logs, Pictures
- Documents stored in computers, mobiles, cloud.

Section 65B(4) requires a certificate stating:

✔ Contents of Certificate:

1. Identification of the electronic record
2. Description of how it was produced
3. Details of the device/system used
4. Statement that:
    - Device was in regular use
    - Data was regularly fed
    - System was functioning properly
5. Signature of a responsible official/person

Who Issues the Certificate?

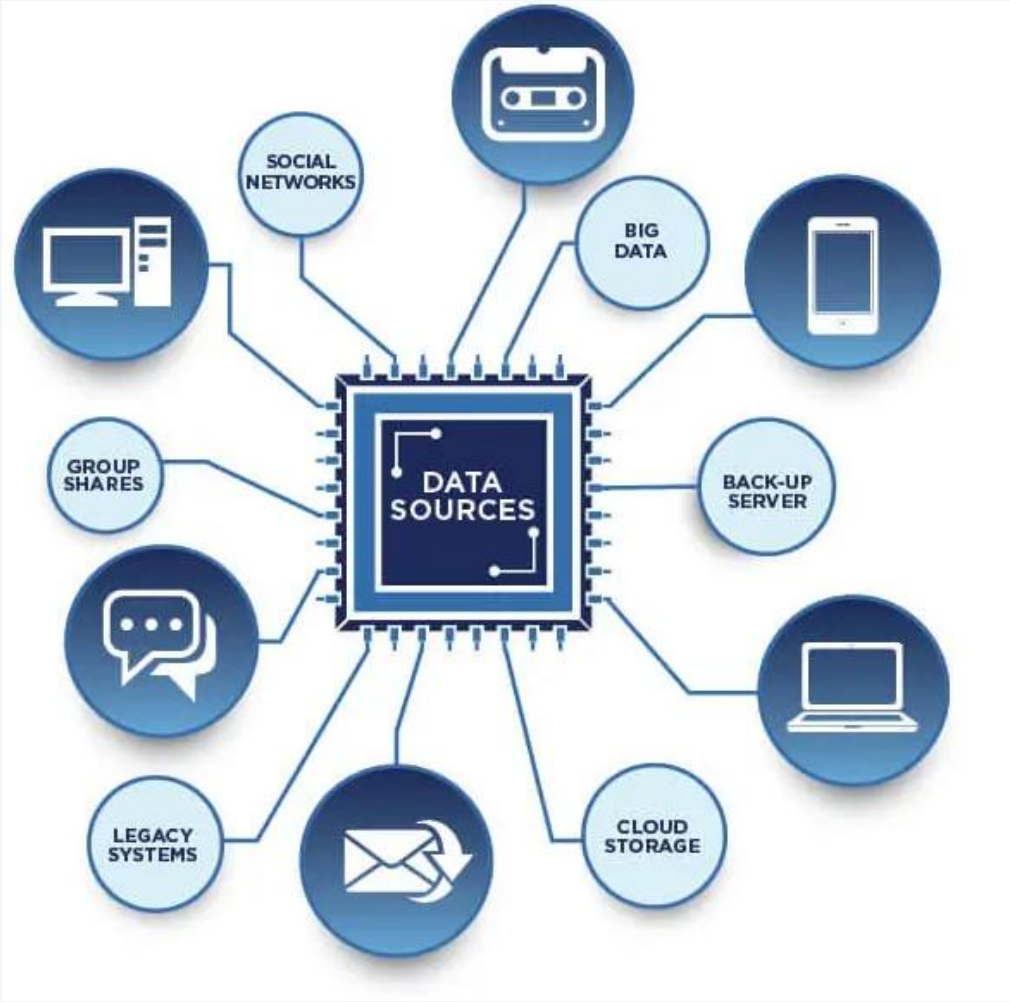
Person in control of the device/system

Example:

Company IT officer

मोबाइल owner (in some cases)

Service provider (telecom, server admin)



VARIOUS KINDS OF DIGITAL EVIDENCE

Landmark Judgments

1. Anvar P.V. v. P.K. Basheer 2014
- Made certificate mandatory

2. Shafhi Mohammad v. State of Himachal Pradesh (2018)

The Court took a liberal view and held
- Requirement of certificate is procedural, not mandatory in all cases

Reasoning of the Court
- Law should not create impossible situations
- Justice should not fail due to technical requirements
- Focus should be on truth and relevance, not rigid procedure

3. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)
- Reaffirmed mandatory rule
- Clarified exceptions

Exceptions / Relaxations Explained

1. When Original Electronic Device is Produced
- If the original device itself is produced in court No need for certificate. Example:Producing the actual mobile phone or DVR. Reason: This is treated as primary evidence, not secondary

VARIOUS KINDS OF DIGITAL EVIDENCE

2. When Certificate is Impossible to Obtain
Applies when:
- Party does NOT have control over the device/system
- Cannot reasonably obtain the certificate

 Examples:
- Call Detail Records from telecom company
- CCTV footage from a third party
- Server data from company

What Court Said:
- Party can apply to court to:
  - Summon the person/authority
  - Direct them to produce certificate.

3. Court Can Allow Later Filing of Certificate
- Certificate need not always be filed with evidence initially
- It can be:
  - Filed later
  - Produced when court directs

HANDLING OF DIGITAL EVIDENCE

The Indian government does not have one single codified SOP or Act or Rules for handling of digital evidence, but there are well-recognized Standard Operating Procedures (SOPs) issued through agencies, manuals, and guidelines. These are followed by police, investigators, and forensic experts.

Key SOP Sources in India

1. Ministry of Home Affairs
   - Cyber Crime Investigation Manuals
   - Advisories for police
2. Indian Cyber Crime Coordination Centre
   - Practical SOPs for cyber investigations
3. CERT-In
   - Incident response and evidence preservation guidelines
4. National Cyber Crime Portal
   - Reporting + handling procedures

HANDLING OF DIGITAL EVIDENCE

Standard SOP for Handling Digital Evidence

1. Identification

- Identify potential digital evidence:
  - Mobile phones
  - Laptops
  - Hard drives
  - CCTV systems
  - Cloud accounts

Do not tamper or switch on/off unnecessarily

2. Preservation (Most Critical Step)

Prevent alteration or deletion

Steps include:

- Isolate device (airplane mode / Faraday bag)
- Disconnect from network
- Secure power supply (for volatile data)

Maintain **original state of evidence**

HANDLING OF DIGITAL EVIDENCE

3. Seizure

Follow legal procedure (search & seizure)

Document:

- Device details (IMEI, serial number)
- Location and condition

Use proper seizure memo (panchnama)

4. Chain of Custody. Maintain complete record of:

- Who handled evidence
- When and where

Must be unbroken

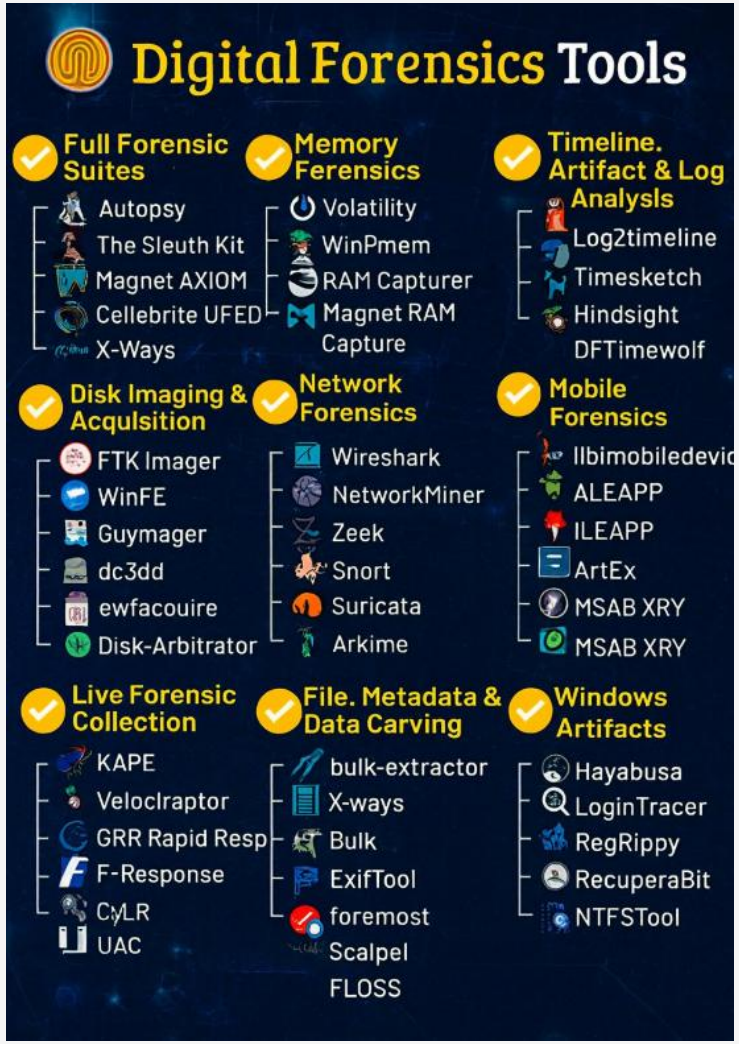
5. Imaging / Cloning

Create forensic image (bit-by-bit copy)

Original device should NOT be examined directly

Use:

- Write blockers
- Forensic tools



HANDLING OF DIGITAL EVIDENCE

6. Hash Value Generation

Generate hash value

Ensures:

Data integrity

No tampering

Same hash value same data

7. Analysis

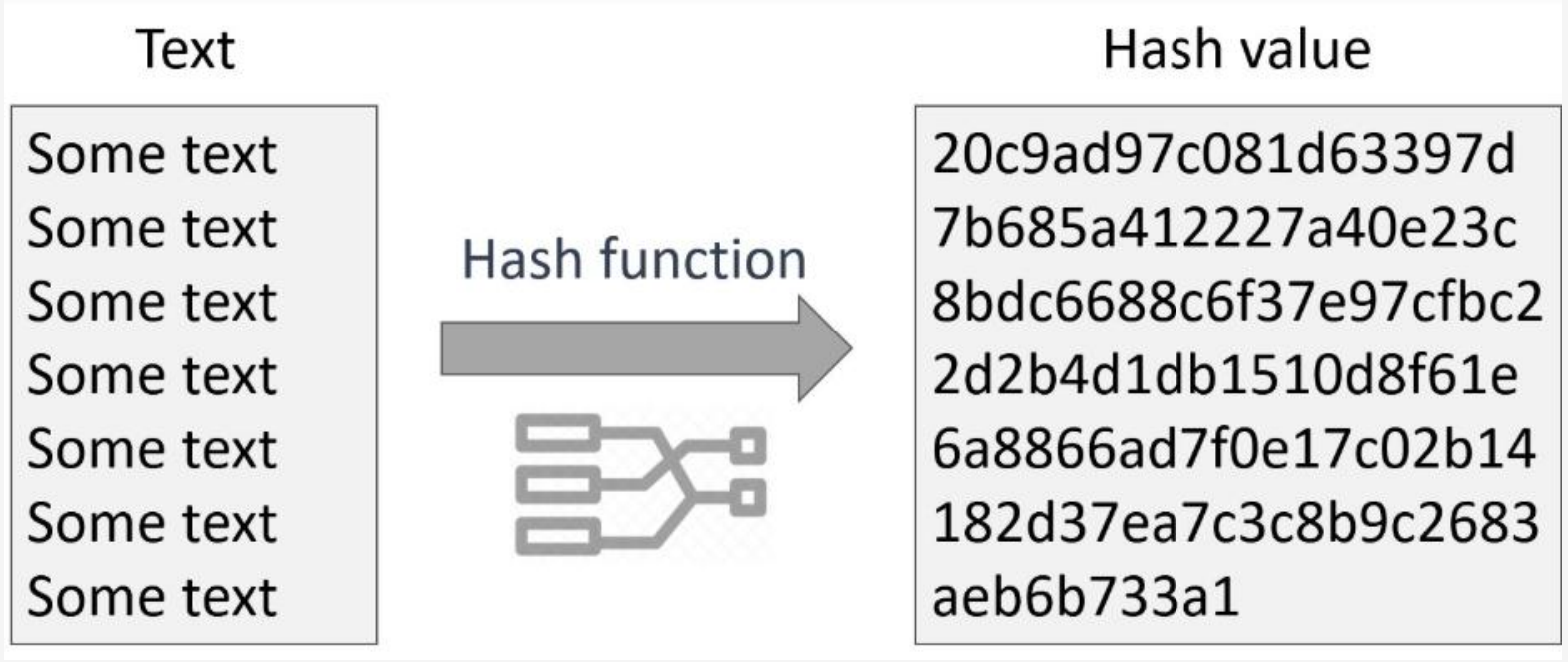
Done in forensic lab:

- Recover deleted files
- Extract chats, logs
- Analyze metadata

8. Documentation

• Every step must be recorded:

• Courts rely heavily on documentation



HANDLING OF DIGITAL EVIDENCE

9. Certification (Very Important)

- Prepare Section 63 BSA / earlier 65B certificate
- Required for admissibility in court

10. Presentation in Court

Submit:

- Report
- Certificate
- Chain of custody
- Expert testimony

BASIC CYBERSPACE TERMS AND CONCEPTS

Cyberspace

A virtual environment created by interconnected computers, networks, and digital systems where communication and data exchange happen.

- World Wide Web (WWW)

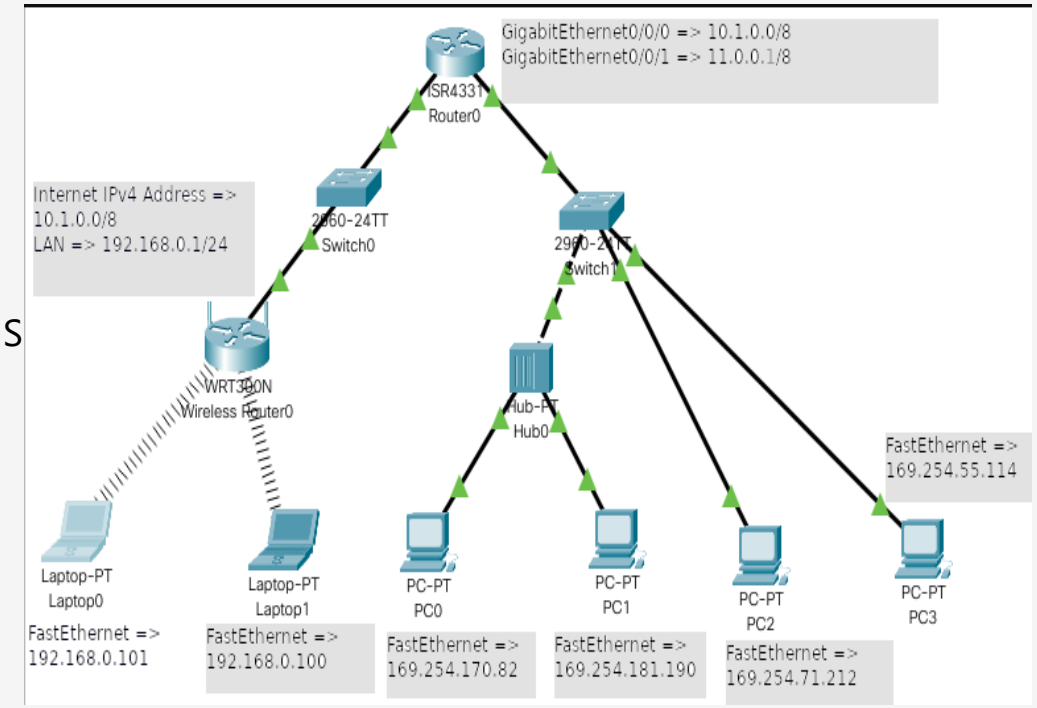
A system of interlinked web pages accessed via browsers using HTTP/HTTPS.

- IP Address

A unique numerical label assigned to devices on a network (e.g., IPv4, IPv6).

- Domain Name

Human-readable website address (e.g., google.com) mapped to IP addresses via DNS



- Encryption

Process of converting data into unreadable form to prevent unauthorized access.

- Firewall

Security system that monitors and controls network traffic.

- Antivirus / Anti-malware

Software designed to detect and remove malicious programs.

BASIC CYBERSPACE TERMS AND CONCEPTS

- Malware

Malicious software (virus, worm, trojan, ransomware).

- Phishing

Fraudulent attempt to obtain sensitive information by impersonation (emails, websites).

- Ransomware

Malware that locks data and demands payment for release.

Attacker secretly intercepts communication between two parties.

- Zero-Day Attack

Attack exploiting unknown vulnerabilities before they are patched.

- Identity Theft

Stealing personal information for fraud.

- Cyber Stalking

Online harassment or tracking of individuals.

- Data Breach

Unauthorized access to confidential data.

BASIC CYBERSPACE TERMS AND CONCEPTS

- Metadata

Data about data (e.g., timestamp, author, location).

- Digital Signature

Electronic method of signing documents using cryptography.

- Cloud Computing

Storing and accessing data over the internet instead of local devices.

- Forensic Imaging

Creating exact copies of storage devices.

- VPN (Virtual Private Network)

Secure connection over public networks.

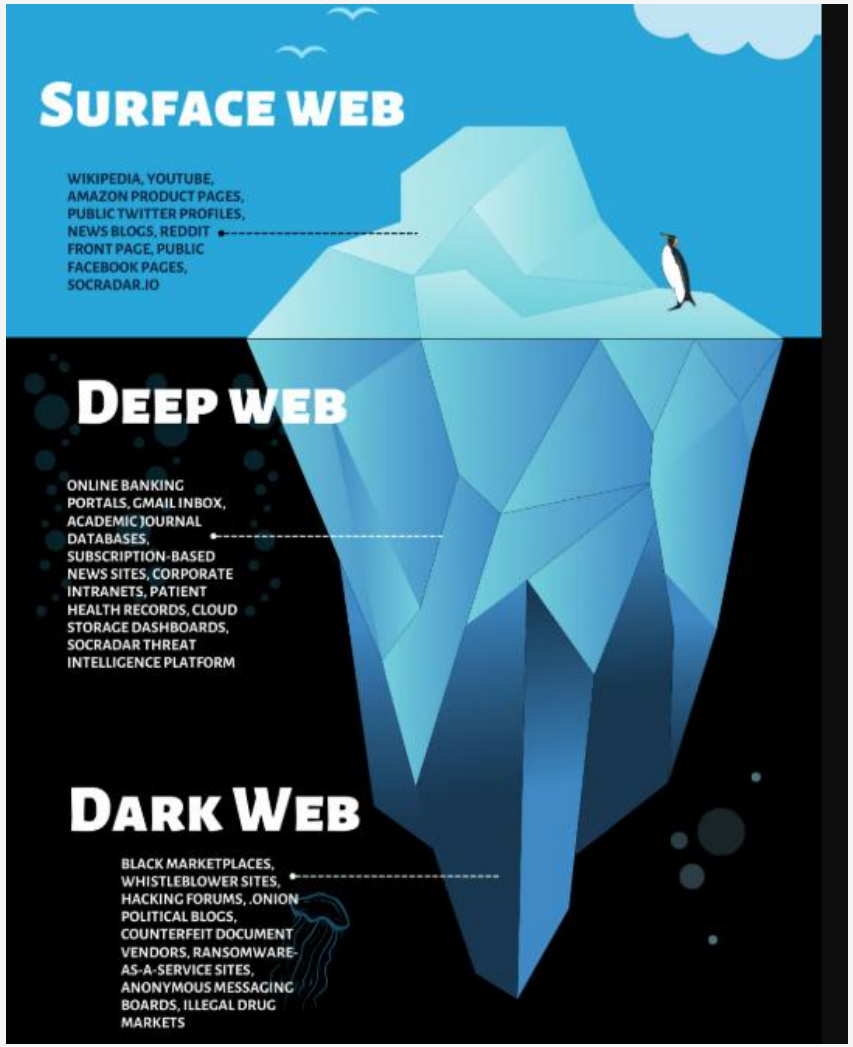
- Proxy Server

Acts as an intermediary between user and internet.

- Dark Web

Cyber space not visible to normal browsers where illegal activities happen.

- Onion Browser – browser that can access the Dark Web.



THANK YOU