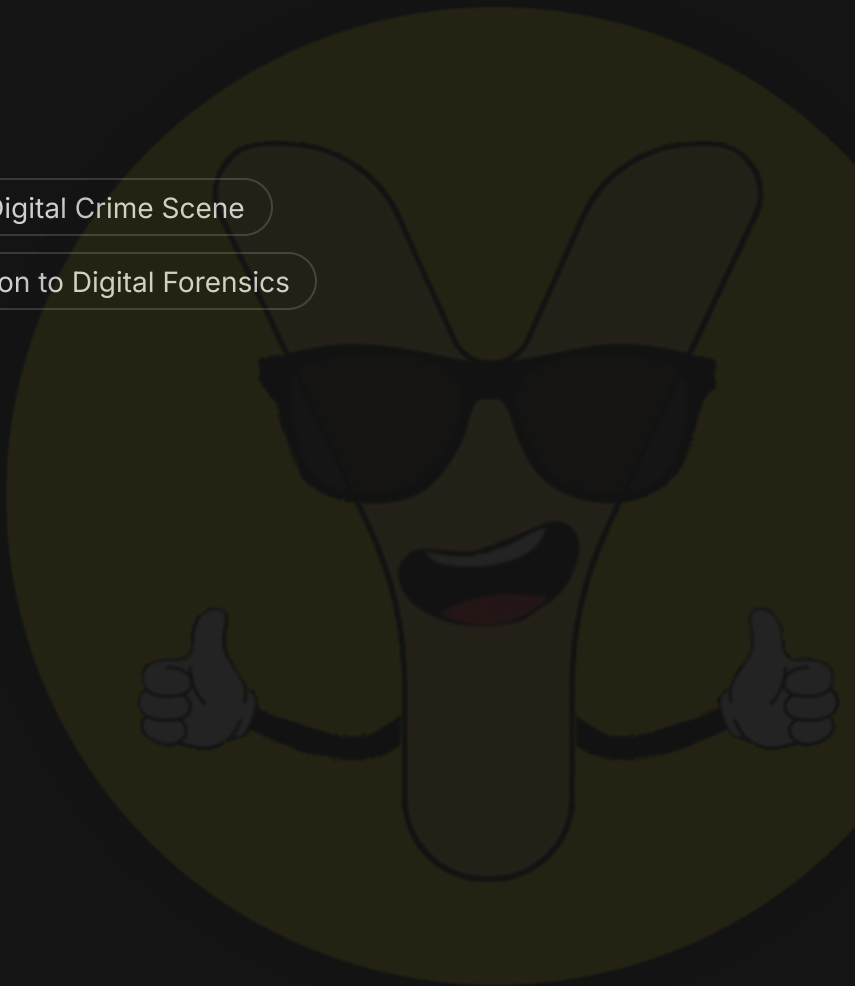
AKTU · 2ND YEAR · BCC301 / BCC401

Cyber Security

Unit 5 — Cybercrime and Forensics

- Introduction to Cyber Forensics
- Handling Preliminary Investigations
- Securing the Crime Scene
- The Digital Crime Scene
- Collection of Digital Evidence
- Preserving Digital Evidence
- Computer Forensics Challenges
- Introduction to Digital Forensics
- Forensic Analysis of E-mail
- Network Forensics
- Introduction to Security Auditing



DECODED BY

Chirag Jain

Founder, Ycotes · Gold Medalist in Artificial Intelligence, IIT Madras · taught 10,000+ students

Introduction to Cyber Forensics

CYBER FORENSICS

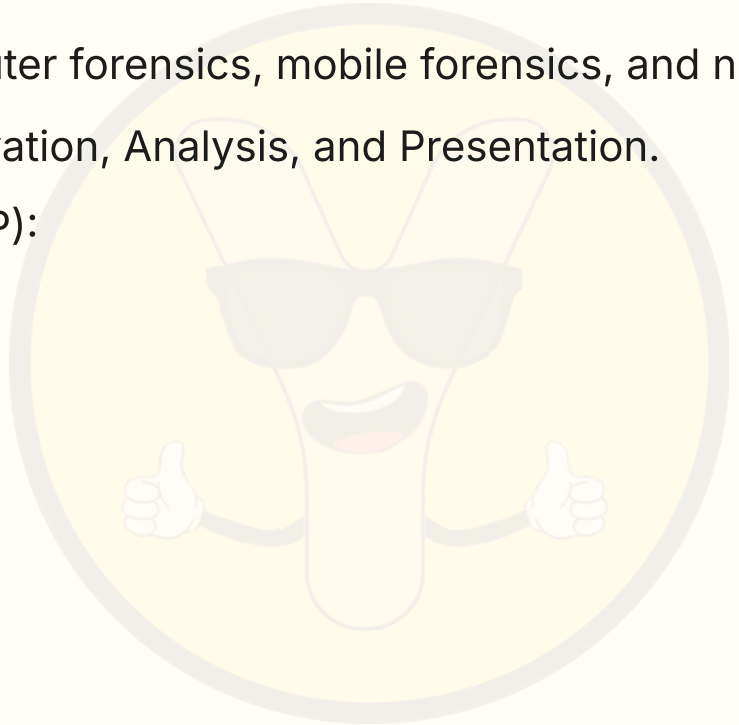
The discipline of collecting, analyzing, and preserving digital evidence from computer systems, networks, and storage devices in a legally admissible manner.

- Extends computer science and law enforcement.
- Aims to uncover electronic data for use in courts of law.
- Follows strict chain of custody protocols to maintain data integrity.

Introduction to Digital Forensics

Digital forensics encompasses the recovery and investigation of material found in digital devices.

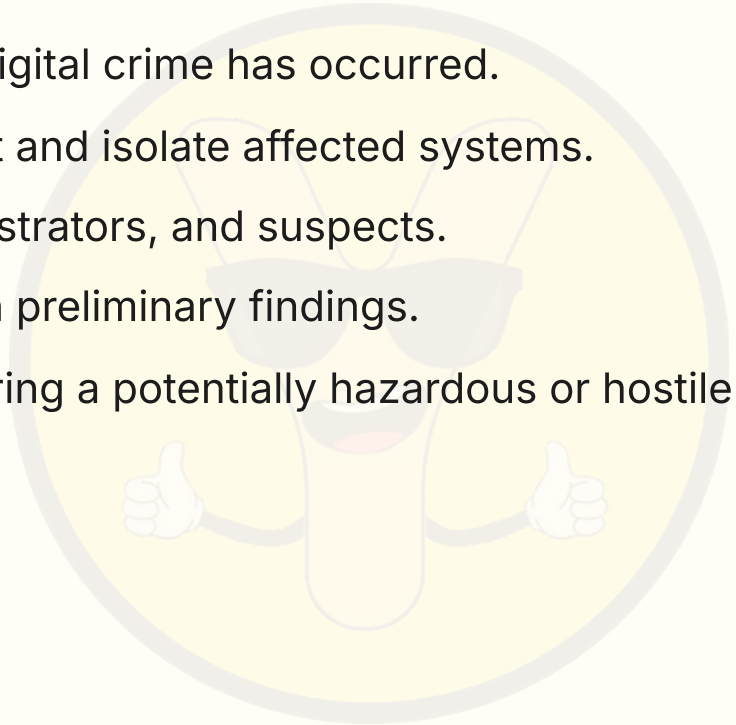
- Broader term encompassing computer forensics, mobile forensics, and network forensics.
- Core phases: Identification, Preservation, Analysis, and Presentation.
- Standard Operating Procedure (SOP):
  - Never work on original media
  - Always create bit-stream images
  - Document every step taken



Handling Preliminary Investigations

The initial response phase determines the overall success of a digital forensic investigation.

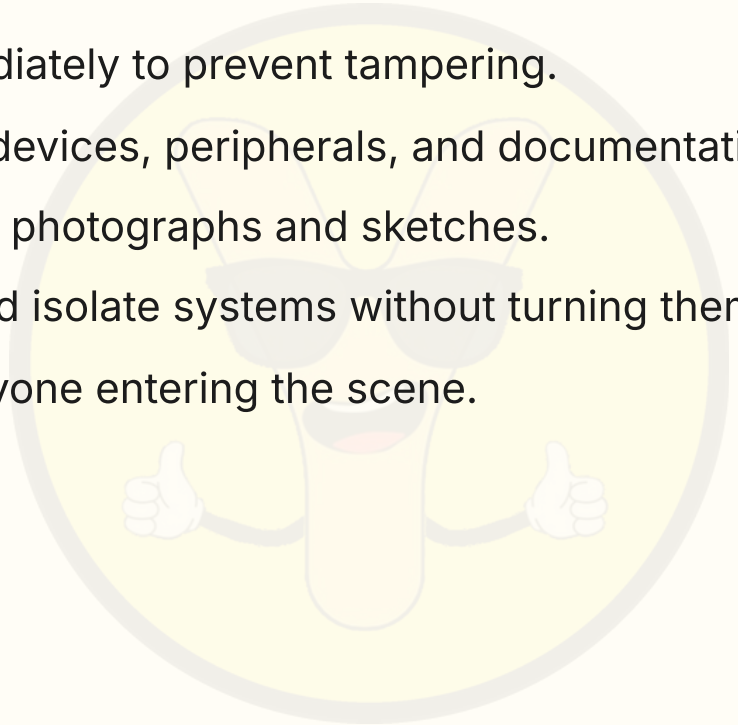
- First responders must identify if a digital crime has occurred.
- Determine the scope of the incident and isolate affected systems.
- Interview witnesses, system administrators, and suspects.
- Formulate a plan of action based on preliminary findings.
- Ensure personal safety before entering a potentially hazardous or hostile physical crime scene.



Securing the Crime Scene

Physical security of the digital crime scene prevents contamination or destruction of evidence.

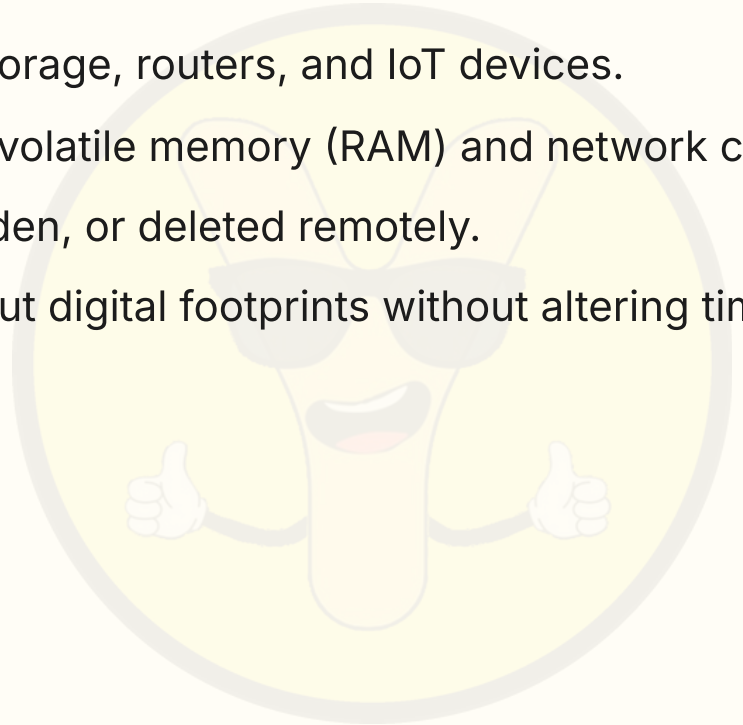
- Restrict unauthorized access immediately to prevent tampering.
- Identify all potential digital storage devices, peripherals, and documentation.
- Document the physical layout using photographs and sketches.
- Check for active network cables and isolate systems without turning them off improperly.
- Maintain a strict access log of everyone entering the scene.



The Digital Crime Scene

The digital crime scene is virtual, volatile, and spans across physical and cloud boundaries.

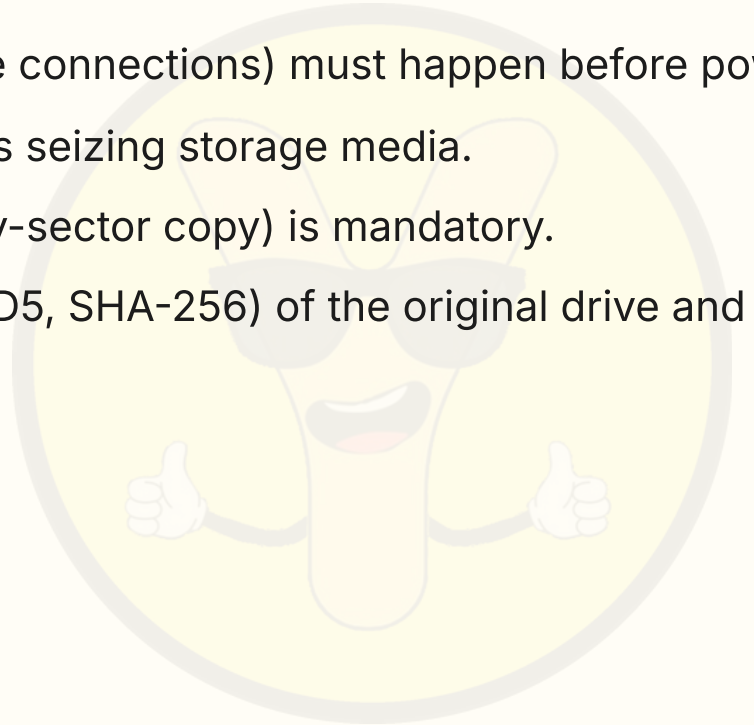
- Includes hard drives, RAM, cloud storage, routers, and IoT devices.
- Data is highly volatile, especially in volatile memory (RAM) and network caches.
- Evidence can be easily altered, hidden, or deleted remotely.
- Requires specialized tools to map out digital footprints without altering timestamps.



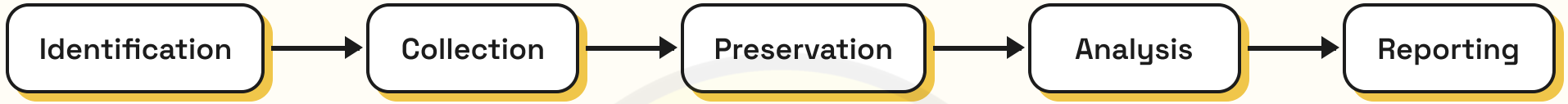
Collection of Digital Evidence

Gathering digital data while maintaining its forensic integrity.

- Volatile data collection (RAM, active connections) must happen before powering down.
- Non-volatile data collection involves seizing storage media.
- Bit-stream imaging (exact sector-by-sector copy) is mandatory.
- Calculate cryptographic hashes (MD5, SHA-256) of the original drive and image to prove identity.



Digital Evidence Collection Lifecycle

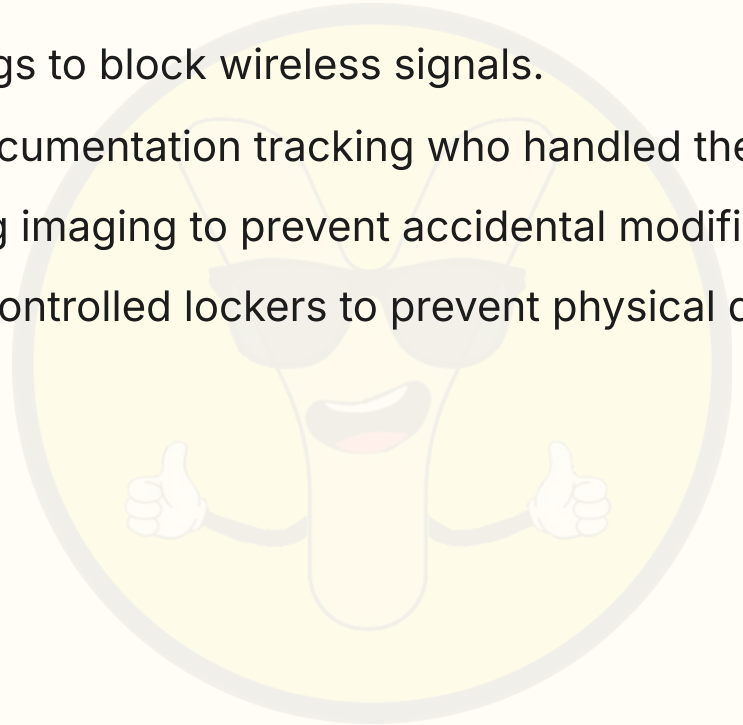


Sequential flow of handling digital evidence in a forensic investigation.

Preserving Digital Evidence

Ensuring collected data remains untampered throughout the legal lifecycle.

- Store physical media in Faraday bags to block wireless signals.
- Maintain strict Chain of Custody documentation tracking who handled the evidence and when.
- Write-blockers must be used during imaging to prevent accidental modification.
- Store evidence in secure, climate-controlled lockers to prevent physical degradation.



Computer Forensics Challenges

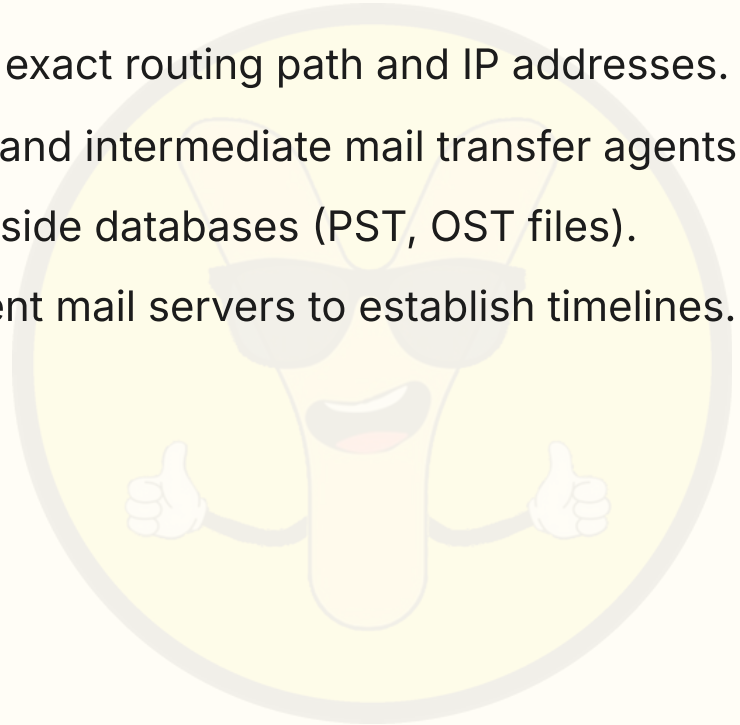
Modern technical hurdles faced by digital forensic investigators.

- Massive storage capacities leading to prolonged analysis times.
- Advanced encryption (AES-256, ransomware) hiding critical evidence.
- Anti-forensic techniques (wiping tools, steganography, timestamp altering).
- Cloud computing and distributed data jurisdictions across international borders.
- Proliferation of proprietary mobile operating systems and secure messaging apps.

Forensic Analysis of E-mail

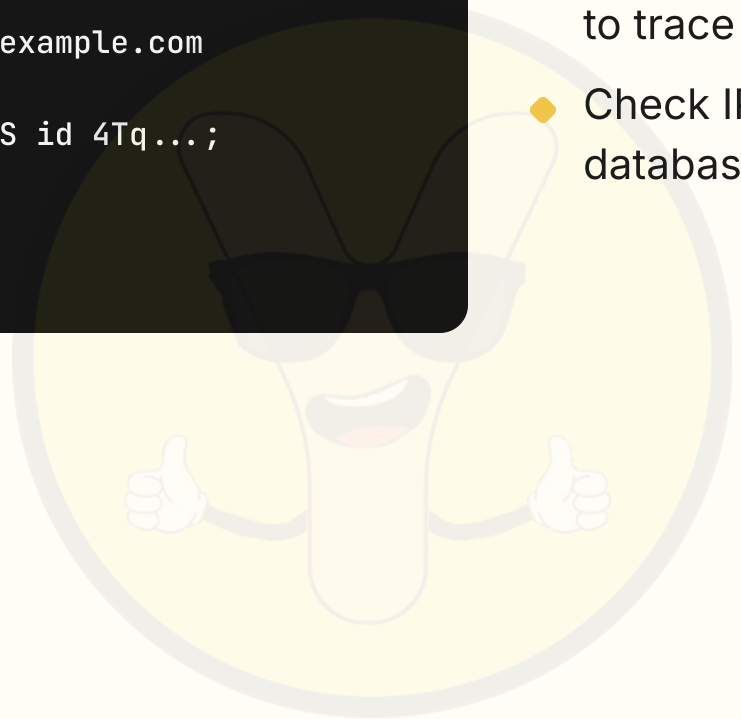
Tracing and authenticating electronic mail messages for legal proceedings.

- Examine email headers to trace the exact routing path and IP addresses.
- Identify spoofed sender addresses and intermediate mail transfer agents (MTAs).
- Recover deleted emails from client-side databases (PST, OST files).
- Correlate timestamps across different mail servers to establish timelines.



Sample Email Header Analysis

```
Return-Path: <sender@example.com>
Received: from mail.example.com (mail.example.com
[192.0.2.1])
    by target.org (Postfix) with ESMTPS id 4Tq...;
    Thu, 25 Oct 2023 10:00:00 +0000
Message-ID: <12345@example.com>
Subject: Confidential Report
```

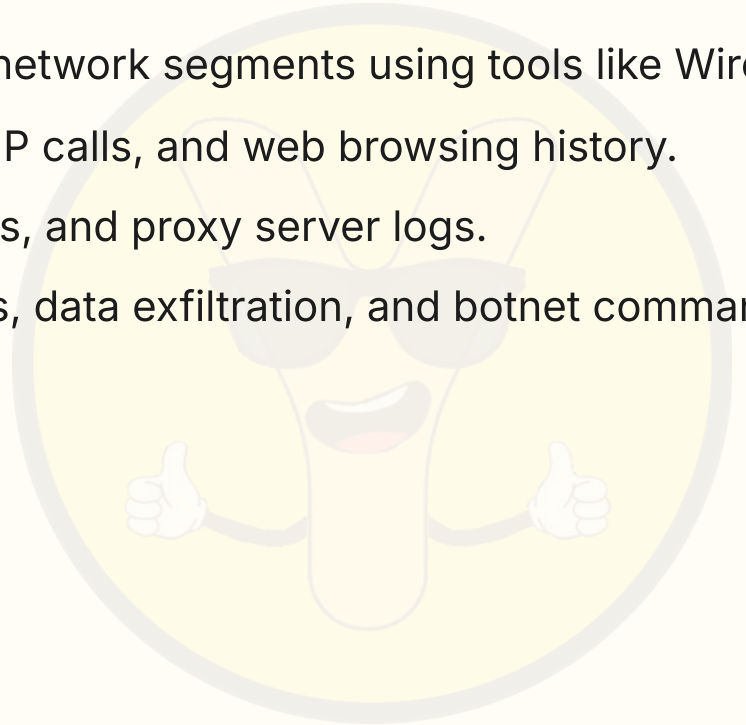


- Analyze 'Received' fields from bottom to top to trace the true origin.
- Check IP addresses against known malicious databases.

Network Forensics

Monitoring and analyzing network traffic for information gathering and intrusion detection.

- Captures packets passing through network segments using tools like Wireshark.
- Reconstructs network sessions, VoIP calls, and web browsing history.
- Analyzes firewall logs, IDS/IPS alerts, and proxy server logs.
- Crucial for identifying active attacks, data exfiltration, and botnet command channels.



Introduction to Security Auditing

SECURITY AUDIT

A systematic, measurable technical assessment of an organization's security policies, controls, and compliance status.

- Identifies vulnerabilities, misconfigurations, and policy gaps.
- Ensures adherence to regulatory frameworks (ISO 27001, PCI-DSS, HIPAA).
- Proactive measure contrasted with reactive forensic investigations.

Comparison: Computer Forensics vs Network Forensics

Feature	Computer Forensics	Network Forensics
Primary Focus	Stored data on local media (HDDs, SSDs, RAM)	Data in transit across network links
Volatility	Data persists until overwritten	Data is highly volatile and ephemeral
Main Tools	EnCase, FTK, Autopsy	Wireshark, Snort, NetFlow analyzers
Primary Use	Post-incident analysis of local compromise	Real-time monitoring and intrusion tracking

Exam Corner

Q1 Define cyber forensics and explain its core objectives in a legal investigation.

Q2 What is a chain of custody? Why is it crucial during the collection of digital evidence?

Q3 Differentiate between volatile and non-volatile evidence collection procedures.

Q4 Explain the process of forensic email analysis using email headers.

Q5 Discuss the major challenges faced by computer forensic investigators today.

Q6 What is network forensics? How does it differ from traditional computer forensics?

Q7 Explain the importance of security auditing in organizational cyber defense.

Unit 5 done. You are exam-ready.

Revise the Exam corner once more, then open Unit 1 on theycotes.com. Every AKTU subject, unit by unit, free. Notes by Chirag Jain, Ycotes.

