:

CYBER CRIME INVESTIGATION & DIGITAL FORENSICS – 23CY602

Prasanjit Singh,
Assistant Professor,
Computer Science and Engineering
(CYBER SECURITY)

UNIT-I

UNIT-I: Foundations of Digital Forensics

This unit lays the groundwork for understanding what digital forensics is, its core components, and the legal landscape it operates within.

Digital Evidence: The Silent Witness

Digital evidence refers to any probative information stored or transmitted in digital form that a party to a court case may use at trial. It's often transient, easily altered, and requires specialized techniques for proper handling.

Emails, documents, spreadsheets
Images, videos, audio files
Browser history, social media posts
Server logs, network traffic data
Mobile device data (SMS, call logs, GPS)

Core Principles of Digital Forensics

Preservation

Ensure that no alterations are made to the original digital evidence during the investigation.

Authenticity

Verify that the evidence is what it purports to be and has not been tampered with.

Integrity

Maintain the completeness and accuracy of the evidence throughout its lifecycle.

Confidentiality

Protect sensitive information within the evidence from unauthorized access.

Challenging Aspects of Digital Evidence

Unlike physical evidence, digital evidence presents unique challenges that require specialized approaches for collection, analysis, and presentation.

Volatility: Data can be easily lost or overwritten.

Volume: Sheer amount of data can be overwhelming.

Encryption: Data often protected by complex encryption methods.

Jurisdiction: Crimes often cross national borders.

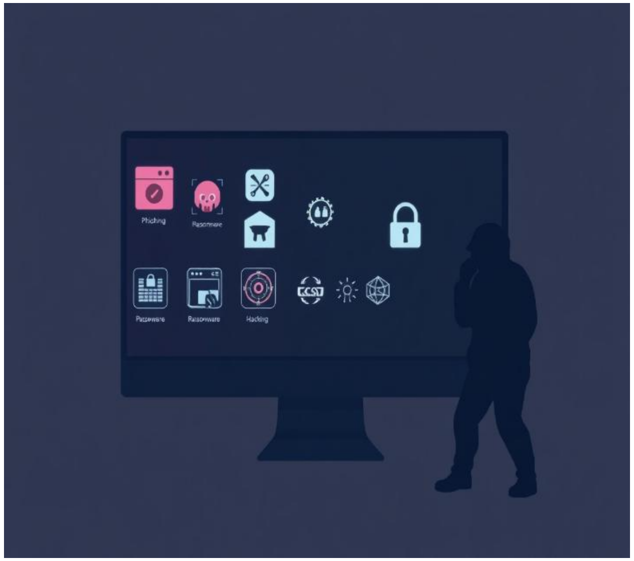
Obfuscation: Perpetrators actively try to hide or delete evidence.

Rapid Technological Changes: Constant evolution of devices and software.

The Ubiquitous Role of Computers in Crime

Computers are no longer just tools for work or entertainment; they have become integral to nearly all types of criminal activity, both as targets and instruments.

- Instrument of crime: Used to commit fraud, theft, harassment, terrorism.
- Target of crime: Hacking, data breaches, denial-of-service attacks.
- Storage of evidence: Digital photos, communications, plans related to traditional crimes.
- Communication facilitator: Planning and executing crimes via online platforms.
- Financial exploitation: Ransomware, phishing, identity theft.



Understanding Cyber Crime Law

- Cyber crime law provides the legal framework for prosecuting digital offenses and defines how digital evidence can be lawfully collected and used.
- Jurisdictional challenges: Determining where a cybercrime occurred.
- International cooperation: Need for global agreements and treaties.
- Data privacy concerns: Balancing investigation needs with individual rights.
- Defining digital offenses: Specific laws for hacking, data theft, online fraud.
- Admissibility of evidence: Rules for presenting digital evidence in court.

UNIT-II

UNIT-II: Digital Investigations

This unit focuses on the systematic approach to conducting digital investigations, from process models to handling the actual crime scene.

Digital Investigation Process Models

Scientific Working Group on Digital Evidence (SWGDE) Model

Emphasizes the scientific method: identification, collection, acquisition, preservation, analysis, reporting.

Abstract Digital Forensics Model (ADFM)

Focuses on identification, preparation, approach, evaluation, conclusion, and presentation stages.

Iterative Digital Forensics Model (IDFM)

A flexible model that allows for revisiting stages as new information emerges.

Applying the Scientific Method

The scientific method provides a robust framework for digital investigations, ensuring objectivity, reproducibility, and admissibility of findings.

Observation: Identify potential digital evidence.

Hypothesis: Formulate theories about the incident.

Experimentation: Use forensic tools to test hypotheses.

Analysis: Interpret results from forensic examinations.

Conclusion: Draw findings based on analyzed evidence.

Reporting: Document the entire process and findings.

Handling a Digital Crime Scene: Principles

No Alteration

The primary rule: never alter, damage, or delete data on the original evidence.

Documentation

Every step taken, every observation made, must be meticulously documented.

Chain of Custody

Maintain a clear, unbroken record of who has had possession of the evidence, when, and for what purpose.

Competence

Only trained and authorized personnel should handle digital evidence.

Surveying the Digital Investigation

The surveying phase involves assessing the digital crime scene to understand its scope, identify potential evidence sources, and plan the acquisition strategy.

Initial assessment: Quick evaluation of devices and network topology.

Prioritization: Determine which evidence sources are most critical.

Resource allocation: Plan for personnel, tools, and time.

Risk assessment: Identify potential data loss or alteration risks.

Legal considerations: Confirm search warrants and legal authority.

Preserving Digital Evidence

Preservation is paramount. It ensures the original evidence remains untainted, allowing for accurate analysis and admissibility in court.

Forensic imaging: Creating bit-for-bit copies of storage devices.

Write-blockers: Hardware devices preventing writes to original media.

Hashing: Using algorithms (MD5, SHA1, SHA256) to verify data integrity.

Documentation: Photographing, sketching, and noting device states.

Live acquisition: Carefully collecting volatile data from running systems.

UNIT-III

UNIT-III: Violent Crime and Digital Investigation

This unit explores the intersection of traditional violent crimes with digital evidence, highlighting how technology can both aid and complicate investigations.

B157
B1SH
TIIBS
CIAP
UIATS
EE, SUT; VILETHG VILAE, SELY DO AT WIS NOE SCE, UG NT NETE, CRIVIIE VILAN, SEPT VIICITEE, 3CT IINE SC

The Role of Computers in Violent Crime

While not always the primary weapon, computers and digital devices frequently serve as critical components in the planning, execution, and aftermath of violent crimes.

Communication: Planning, recruitment, threats via messages, social media.

Surveillance: Monitoring victims or crime scenes using digital tools (GPS, cameras).

Research: Gathering information on victims, methods, locations.

Exploitation: Online grooming, child exploitation material storage/sharing.

Post-crime activity: Disposing of digital evidence, communication with accomplices.

Processing the Digital Crime Scene (Violent Crime)

Investigating violent crimes often involves securing both physical and digital crime scenes. The digital component requires specialized skills and tools to avoid contaminating evidence.

Integrated approach: Physical and digital evidence collection must be coordinated.

Urgency: Volatile data from active devices (phones, smart devices) may be crucial.

Victim considerations: Trauma-informed approach when dealing with victims' devices.

Data correlation: Linking digital activities to physical events.

Digital context: Understanding online relationships and motivations.

Investigative Reconstruction

Digital evidence plays a pivotal role in reconstructing events, timelines, and motives in violent crime investigations. It helps paint a clearer picture of 'what happened' and 'how'.

Timeline creation: Using timestamps from logs, emails, and device activity.

Location tracking: GPS data from phones or vehicle systems.

Communication patterns: Identifying who communicated with whom and when.

Activity logs: Web browsing, file access, application usage.

Visual evidence: Analysis of photos and videos for context.

UNIT-IV

UNIT-IV: Deep Dive into Computer Forensics

This unit delves into specific areas of computer forensics, from the challenges of cyber stalking to extracting evidence from various operating systems.

Cyber Stalking: Definition and Impact

Cyber stalking involves using electronic communication to harass or frighten an individual, typically by repeatedly sending messages, making threats, or engaging in other forms of intimidation.

Repetitive, unwanted online contact.

Threats, harassment, or intimidation through digital means.

Exploitation of public online information.

Often escalates to real-world stalking.

Significant psychological and emotional impact on victims.

Investigating Cyber Stalking

Digital forensics plays a crucial role in tracing cyber stalkers, collecting evidence of their online activities, and building a case for prosecution.

- IP address tracing: Identifying source locations of messages.
- Email header analysis: Revealing sending pathways and spoofing attempts.
- Social media forensics: Analyzing profiles, posts, and connections.
- Device examination: Finding evidence of communication on victim's or suspect's devices.
- Correlation with physical evidence: Linking online threats to real-world actions.

Computer Basics for Digital Forensics: Hardware

CPU (Central Processing Unit)
The 'brain' that executes instructions; volatile data in registers and cache can be critical.
RAM (Random Access Memory)
Volatile memory holding active programs and data; crucial for live forensics.
Storage Devices (HDD/SSD)
Non-volatile memory where data is persistently stored; primary source for most forensic analyses.
Peripherals
Keyboards, mice, USB drives; their connections and usage patterns can provide clues.

Computer Basics for Digital Forensics: Operating Systems

Windows

Focus on Registry, Event Logs, NTFS artifacts, Prefetch files, Recycle Bin.

Linux

Examine file system metadata (ext4), bash history, syslog, user accounts.

macOS

Investigate HFS+ or APFS file systems, unified logs, Spotlight databases, Time Machine backups.

Applying Forensic Science to Computers: Imaging & Analysis

Applying forensic science to computers involves a systematic process of creating exact copies of storage media and then analyzing these copies for digital artifacts.

•Forensic Imaging: Bit-for-bit duplication of entire drives (e.g., creating E01 files).

•Hashing: Verifying the integrity of the image to ensure it's an exact replica.

•File System Analysis: Examining the structure (NTFS, ext4, APFS) to locate files, deleted data, and metadata.

•Keyword Searching: Using specific terms to find relevant information quickly across large datasets.

•Data Carving: Recovering deleted or fragmented files based on their headers and footers.

UNIT-V

UNIT-V: Network Forensics – Tracing the Digital Footprints

This final unit focuses on network forensics, the art and science of monitoring, capturing, storing, and analyzing network traffic to discover evidence of security incidents.

.

Network Basics for Digital Investigators: Concepts

A fundamental understanding of network architecture and protocols is crucial for effective network forensic investigations.

- IP Addressing: Identifying devices and their locations on a network.
- Ports: Communication endpoints for different services (e.g., HTTP on port 80).
- Protocols: Rules governing data exchange (TCP, UDP, HTTP, FTP, DNS).
- Network Topologies: How devices are connected (star, bus, ring, mesh).
- OSI Model: Understanding the seven layers of network communication.

Applying Forensic Science to Networks: Data Capture

The core of network forensics is the ability to capture and store network traffic. This 'packet capture' is like recording a conversation happening on the network.

•Packet Sniffing: Intercepting and logging data packets traveling over a network.

•Taps & Port Mirroring: Methods for passively copying network traffic without interference.

•Full Packet Capture (FPC): Storing all network packets for later analysis.

•NetFlow/IPFIX: Collecting metadata about network traffic flows, rather than full packets.

•Intrusion Detection Systems (IDS): Generate alerts and logs for suspicious network activity.

Digital Evidence on Physical & Data Link Layers

The lowest layers of the OSI model provide foundational evidence about network connectivity and device identification.

Physical Layer (Layer 1)

Evidence from cabling, physical connections, fiber optic cables; can indicate physical access.

Data Link Layer (Layer 2)

MAC addresses (hardware addresses), ARP tables, switch logs; identifies specific devices on a local segment.

Wireless Access Points

SSID, BSSID, client connection logs, signal strength; can determine presence and activity on Wi-Fi.

Digital Evidence on Network & Transport Layers

These layers reveal how data travels across networks and how applications communicate.

Network Layer (Layer 3)

IP addresses, routing tables, firewall logs; tracks data across different networks.

Transport Layer (Layer 4)

TCP/UDP ports, connection states, session data; shows which applications are communicating.

Packet Analysis

Deep inspection of headers and payloads to understand traffic content and anomalies.

Essential Network Forensic Tools

Specialized tools are indispensable for capturing, analyzing, and interpreting the vast amounts of data found in network traffic.

- Wireshark: The industry standard for deep packet inspection and protocol analysis.
- Snort / Suricata: Intrusion Detection/Prevention Systems (IDS/IPS) for real-time traffic analysis and alerting.
- Network Miner: Recovers files, images, emails, and credentials from network traffic.
- tcpdump: Command-line packet analyzer for capturing and filtering network traffic.
- Argus: Generates comprehensive network flow data and statistics.
- Bro/Zeek: Network Security Monitor that provides high-level transaction logs and file content.

NRCM
your roots to success...

THANK YOU