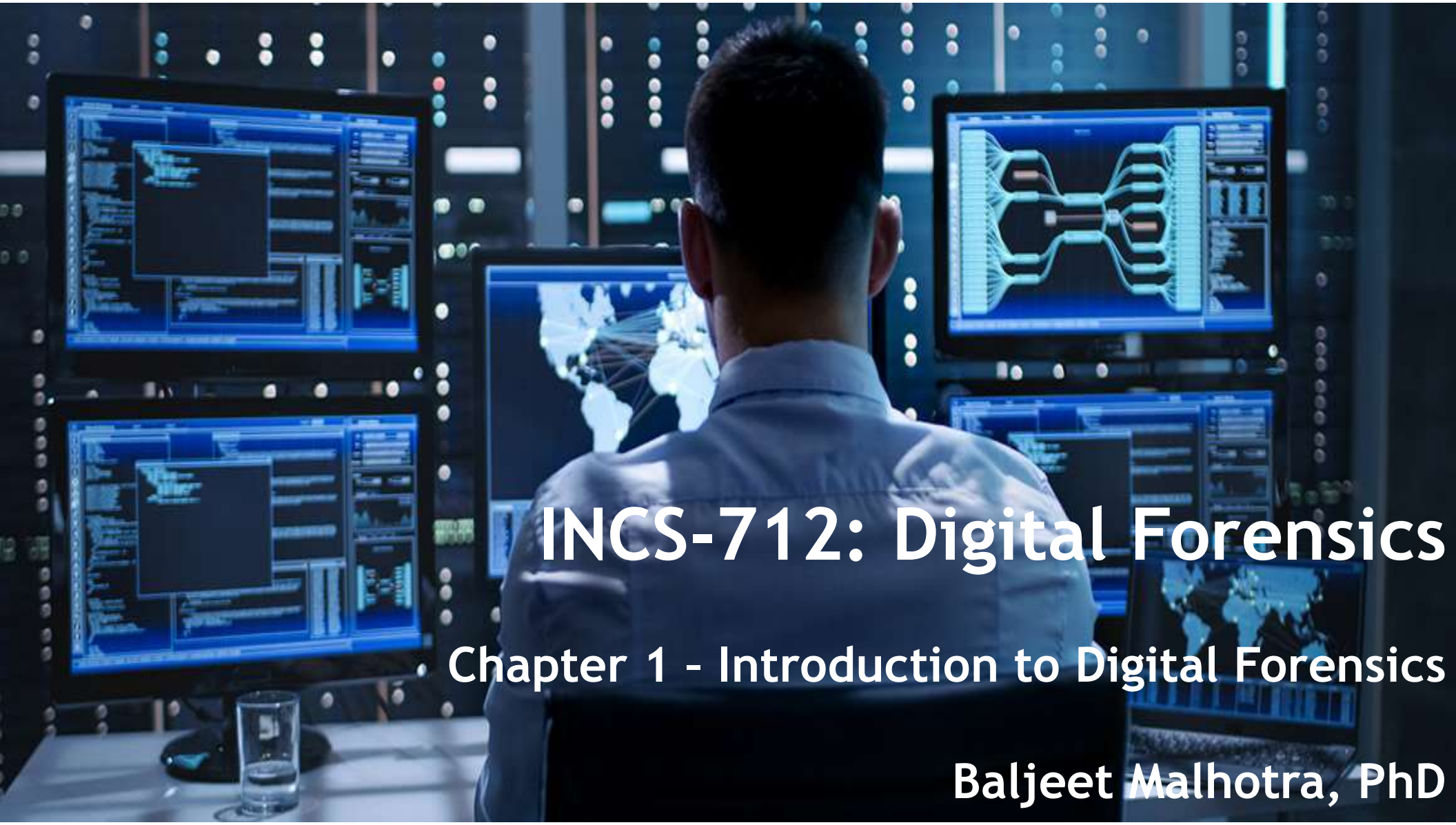


INCS-712: Digital Forensics

Chapter 1 - Introduction to Digital Forensics

Baljeet Malhotra, PhD

Introduction to Digital Forensics

Part One: What is Digital Forensics

What is Digital Forensics

- Collecting, analyzing, and reporting digital information, often related to incidents involving digital devices, systems, and environments, in a way that is legally admissible in courts.

- Determining the past actions that have taken place on digital and non-digital devices and systems using forensic techniques.

Background - Digital Forensics Ecosystem

- **Digital Devices**: Smart or Internet of Things (IoT) devices, traditional computers, servers, and networks.
- **Digital Incidents**: Unauthorized events involving digital devices, networks, or systems that may
- **Incident Impact**: Data integrity, confidentiality, and availability (due malware, phishing, unauthorized access).
- **Incident Scope**: Origin, methods, and impact of the digital incident, to mitigate further risks, and support actions.
- **Data Types**: Beyond typical computer files, including SMSs, emails, GPS data, and metadata found in various digital formats such as logs from servers and networks.

Background - Digital Forensics Ecosystem

- **Applications**: While often the context is criminal investigations, but also involves civil litigations, corporate investigations, data breach analysis, and compliance audits.
- **Networks and Clouds**: Encompasses data that moves across networks or is stored in cloud environments, reflecting the interconnected nature of modern digital activities.
- **Scientific Principles**: Key scientific principles of structured methodology, hypothesis testing, reproducibility, use of validated tools, and evidence-based conclusions.
- **Interpretive skills**: Creativity, adaptability, subjective presentation, and personal style, intuition and experience.

Digital Forensics is a Science

Systematic Methodology

Structured, scientific process for evidence identification, collection and preservation.

Hypothesis and Analysis

Form hypothesis about how digital incidents occurred to test them systematically.

Repeatability and Reproducibility

Methods applied to the same evidence should produce same/consistent results.

Specialized Tools and Techniques

Use of specialized acceptable, verified tools and techniques.

Evidence Based Conclusions

Interpret data objectively in an unbiased way to draw evidence-based conclusions.

Digital Forensics is a Science

SYSTEMATIC METHODOLOGY: STRUCTURED, SCIENTIFIC PROCESS FOR EVIDENCE IDENTIFICATION, COLLECTION AND PRESERVATION.

HYPOTHESIS AND ANALYSIS: FORM HYPOTHESIS ABOUT HOW DIGITAL INCIDENTS OCCURRED TO TEST THEM SYSTEMATICALLY.

REPEATABILITY AND REPRODUCIBILITY: METHODS APPLIED TO THE SAME EVIDENCE SHOULD PRODUCE SAME/CONSISTENT RESULTS.

SPECIALIZED TOOLS AND TECHNIQUES: USE OF SPECIALIZED ACCEPTABLE, VERIFIED TOOLS AND TECHNIQUES.

EVIDENCE BASED CONCLUSION: INTERPRET DATA OBJECTIVELY IN AN UNBIASED WAY TO DRAW EVIDENCE-BASED CONCLUSIONS.

Digital Forensics is a Science

Systematic Methodology: Structured, scientific process for evidence identification, collection and preservation.

Hypothesis and Analysis: Form hypothesis about how digital incidents occurred to test them systematically.

Repeatability and Reproducibility: Methods applied to the same evidence should produce same/consistent results.

Specialized Tools and Techniques: Use of specialized acceptable, verified tools and techniques.

Evidence based Conclusion: Interpret data objectively in an unbiased way to draw evidence-based conclusions.

Digital Forensics is an Art

Interpretive Skills

Interpret complex, ambiguous data while dealing with partial, corrupted and encrypted information.

Problem Solving

Requires creativity or out-of-box thinking to uncover hidden or obfuscated information.

Adoptability

Must adopt to new techniques and technologies while developing new/custom solutions.

Subjectivity

Requires subjective judgement, especially to present technical info to non-technical people.

Personal Style

Brings unique style influenced by training, background and personal experiences.

Digital Forensics is an Art

Interpretive Skills:

Interpret complex, ambiguous data while dealing with partial, corrupted and encrypted information.

Creative Problem Solving:

Requires creativity or out-of-box thinking to uncover hidden or obfuscated information.

Adoptability and Flexibility:

Must adopt to new techniques and technologies while developing new/custom solutions.

Subjective in Presentation:

Requires subjective judgement, especially to present technical info to non-technical people.

Personal Style

Brings unique style influenced by training, background and personal experiences.

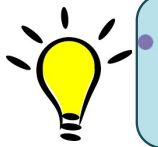
Digital Forensics vs. Computer Forensics

Book reading exercise:
Find similarities and differences

Cybercrime Forensics

- **Cybercrime**: Specifically targets the criminal aspect, dealing with broken laws and securing evidence for prosecution.

- **Cybersecurity**: Wider scope, encompassing situation where digital data are analyzed including noncriminal scenarios.

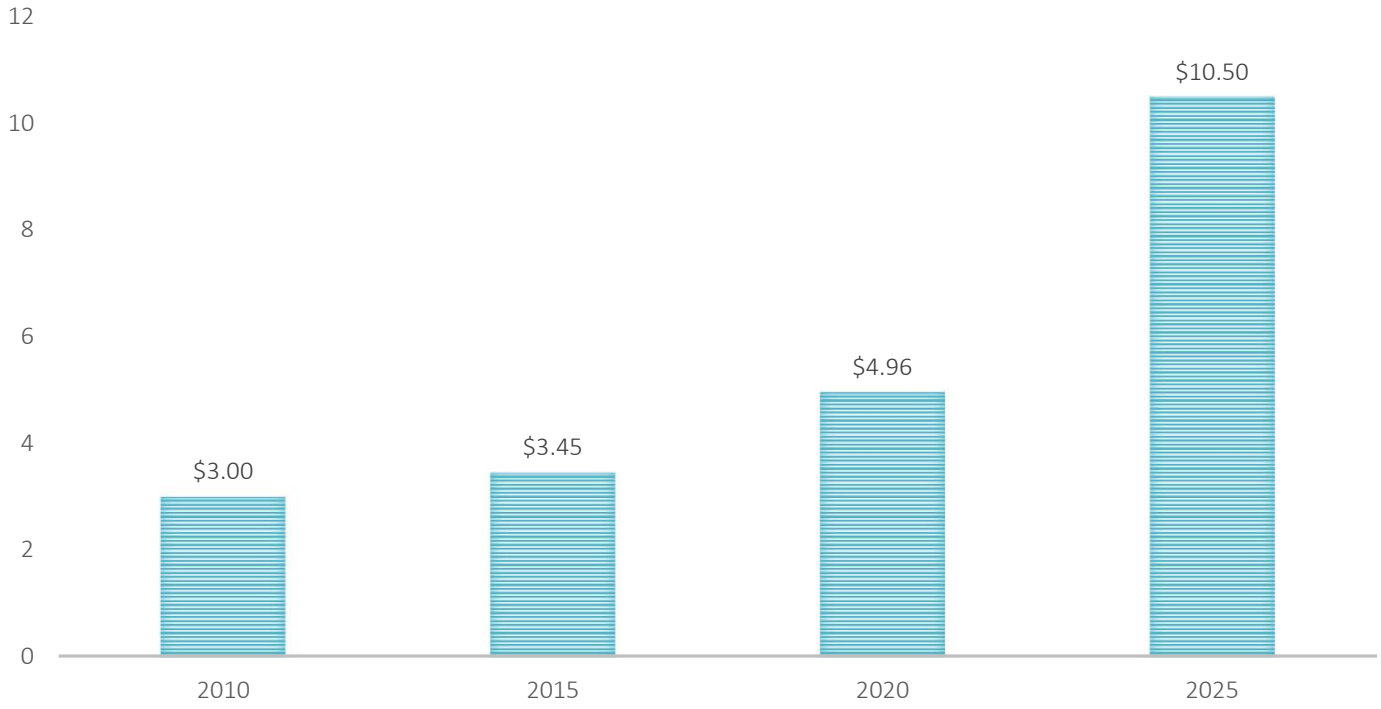


- **Digital Forensics**: The purpose can extend beyond crime to include data recovery, debugging, audits, business disputes.

- **Cybercrime Forensics**: Predominantly used to support the legal process in criminal cases.

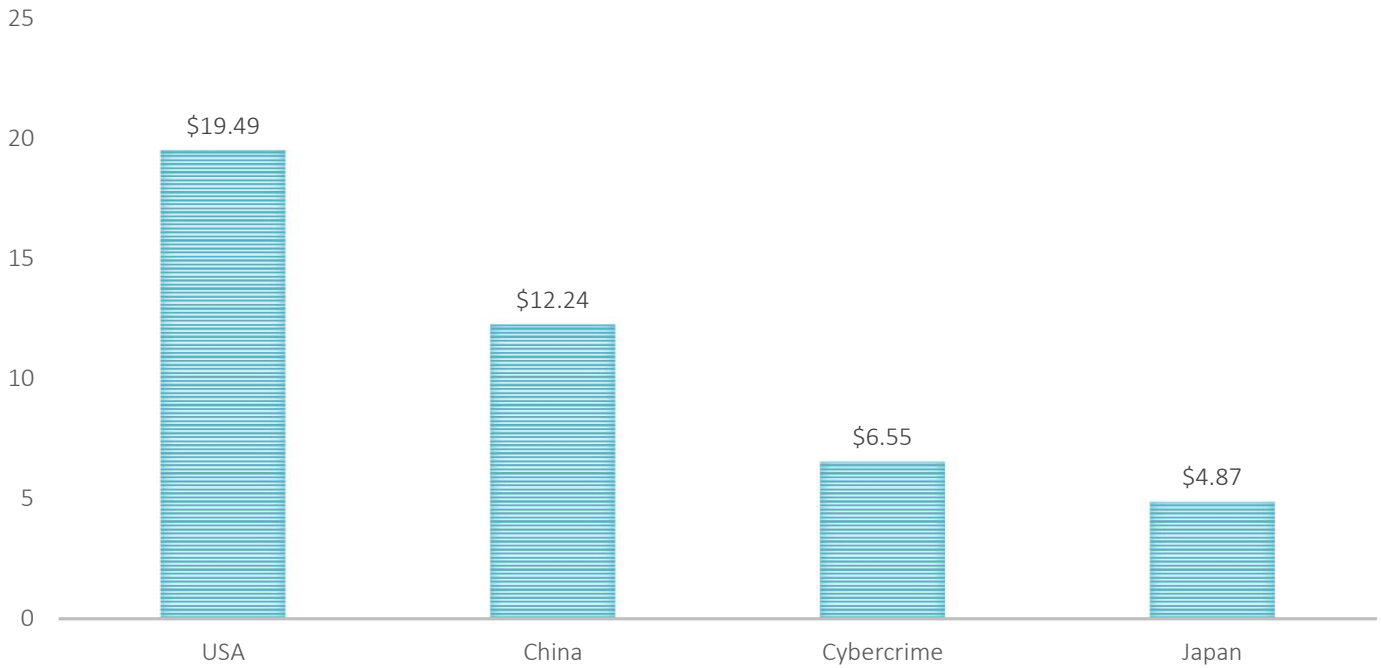
Motivations - Cybercrime Losses

Source: World Economic Forum, Global Risk Report 2023. Amounts in trillions.



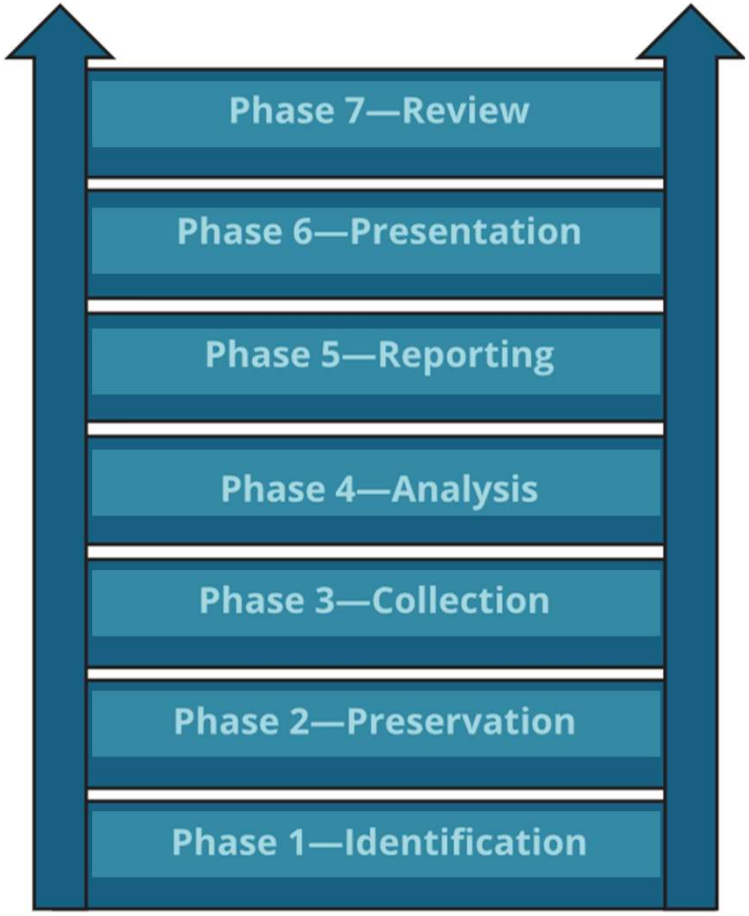
Motivations - Cybercrime Losses

Source: Investopedia, 2022. Amounts in trillions.



Phases of Cybercrime Forensics

Refer to the book for more details !



Challenges in Cybercrime Forensics

- **Encryption**: Accessing important data.

- **Anonymity**: Technologies like Tor and VPNs.

- **Volume and Complexity**: Data from a variety.

- **Jurisdiction**: Privacy, data, jurisdiction boundaries.

- **Legal and Ethical**: Balance between privacy and analysis.

Future of Cyber Forensics

- Cloud, AR, VR

- Artificial Intelligence

- Internet of Things (IoT)

- Blockchain and Cryptocurrencies

- Quantum Computing and Advanced Encryption

Forensic Sciences

- Serology
- Toxicology
- Entomology
- DNA analysis
- Tool mark analysis
- Fingerprint analysis
- Hair and fiber analysis
- Blood stain pattern analysis
- Ballistics study, examination of firearms and other weapons

- Serology
- Toxicology
- Entomology
- DNA analysis
- Tool mark analysis
- Fingerprint analysis
- Hair and fiber analysis
- Blood stain pattern analysis
- Ballistics study, examination of firearms and other weapons

Other Forensic Sciences - 1

Book reading exercise: Find similarities and differences

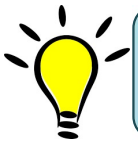
- Serology
- Toxicology
- Entomology
- DNA analysis
- Tool mark analysis
- Fingerprint analysis
- Hair and fiber analysis
- Blood stain pattern analysis
- Ballistics study, examination of firearms and other weapons

Other Forensic Sciences - 2

Book reading exercise: Find similarities and differences

- Pathology
- Odontology
- Epidemiology
- Anthropology
- Drug chemistry
- Paint and glass analysis
- Footwear and tire analysis
- Digital Forensics (text, audio video, logs, sensors, and devices)

Brief History of Digital Forensics



- In early 1990s, the International Association of Computer Investigative Specialists (IACIS) introduced training on software for digital forensics.

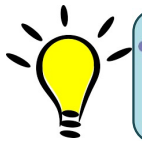
- IRS (Internal Revenue Service) created search-warrant programs.

- ASR Data created Expert Witness for Macintosh.

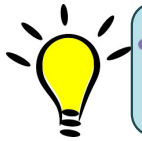
- AccessData Forensic Toolkit (FTK) is a popular commercial product.

Digital Forensics Standards/Frameworks

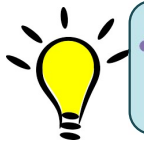
- The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation.



- In October 2012, an ISO standard for digital forensics was ratified - ISO 27037 Information technology - Security techniques.



- The US Federal Rules of Evidence (FRE) was created to ensure consistency in federal proceedings.



- The Fourth Amendment to the U.S. Constitution protects everyone's right to be secure from search and seizer.

- Canadian Centre for Cyber Security

INCS-712: Digital Forensics

Chapter 1 - Cybersecurity Ecosystem

Baljeet Malhotra, PhD

Cybersecurity - Incidents

Cyber Theft	Data Breaches	Illegal Possession
Espionage	Financial Frauds	Identity Theft
Human Right Violations	Intellectual Property Theft	Employment Discrimination

Cybersecurity - Investigations

Theft of Company Secrets	Employee Sabotage	Credit Card Fraud
Financial Crimes	Economic Crimes	Harassment
Child Pornography	Major Crimes	Identity Theft

Cybersecurity - Example Investigation

Windows Operating System (PCs)

- File Allocation Table (FAT)
- Master File Table (MFT)
- FAT/MFT reveal where files begin and end

When files are deleted from PCs

- Pointers to the file (in FAT/MFT) are deleted
- FAT/MFT space occupied by the file is marked as available

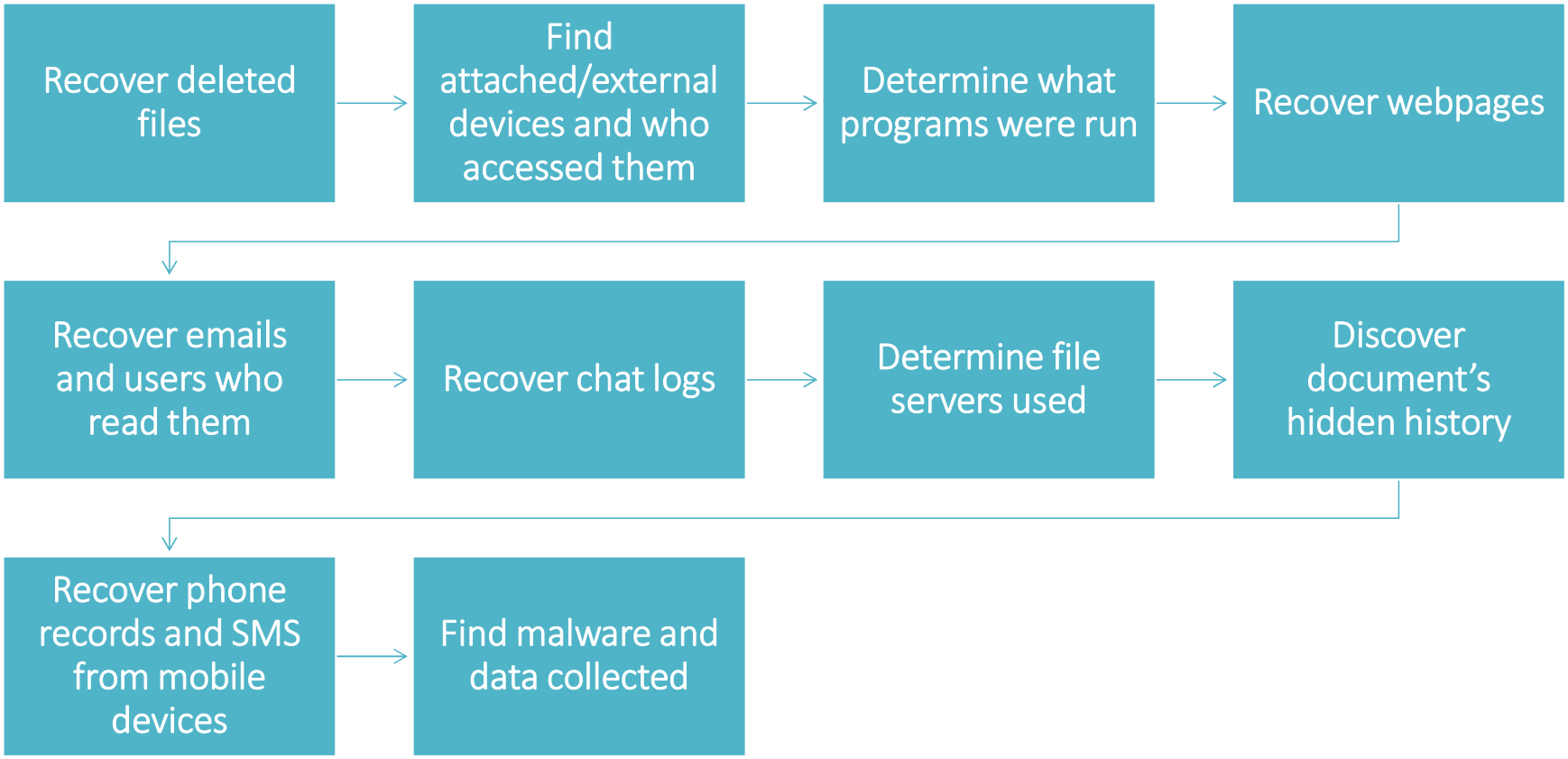
The unallocated space remains entact

- The actual data that was contained in the file is **NOT** deleted

Cybersecurity - Media and Data

Desktop computers and laptops	iPads, iPods, etc.	Smartphones and other cell phones	MP3 music players, CD-ROMs & DVDs
Hard Drives	Digital Cameras	USB Memory Devices, memory cards	Backup Tapes
Emails	Audio, Images and Videos	Messages	Logs

Cybersecurity - Digital Forensic Activities



Cybersecurity - Stakeholders

Law Enforcement

Academia and Research

Private and Public Organizations

IT/Security Professionals

Military and National Security

Cybersecurity Stakeholders - Law Enforcement

Local, State and Federal levels	Detectives at local levels	State or provincial police
FBI's Computer Analysis and Response Team (CART)	Regional Digital Forensics Laboratories (RCFLs)	EnCase Trainers
Canadian Security Intelligence Service	Canadian Centre for Cyber Security.	Global Cyber Alliance

Cybersecurity Stakeholders - Organizations

- Canadian Forensics Inc. (Fingerprinting, Background and DNA Tests Services for RCMP)
- The Centre of Forensic Sciences
- Digital Forensics Associates
- Empire Investigation LLC
- Advanced Forensic Recovery of Electronic Data
- Philadelphia Digital Forensics
- Philadelphia Digital Forensics Analysis and Investigations
- New York Computer Forensic Services

Cybersecurity Stakeholders - Military

Test, identify, and gather evidence in the field

Specialized training in imaging and identifying multiple sources of electronic evidence

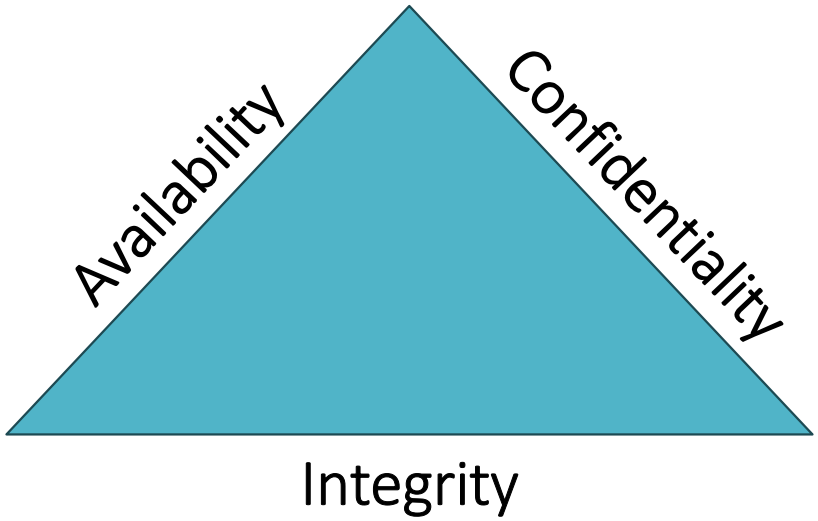
Analyze the evidence for rapid intelligence gathering and responding to security breach incidents

Desktop, server and network forensic techniques

Cybersecurity Triad

Digital Forensics Related Other Disciplines

Different types of teams in a typical corporate work together to secure their digital assets (computers, APIs, networks)



Digital Forensics and Other Related Disciplines

Vulnerability/Threat Assessment and Risk Management

- Verify the integrity of stand-along workstations and network servers

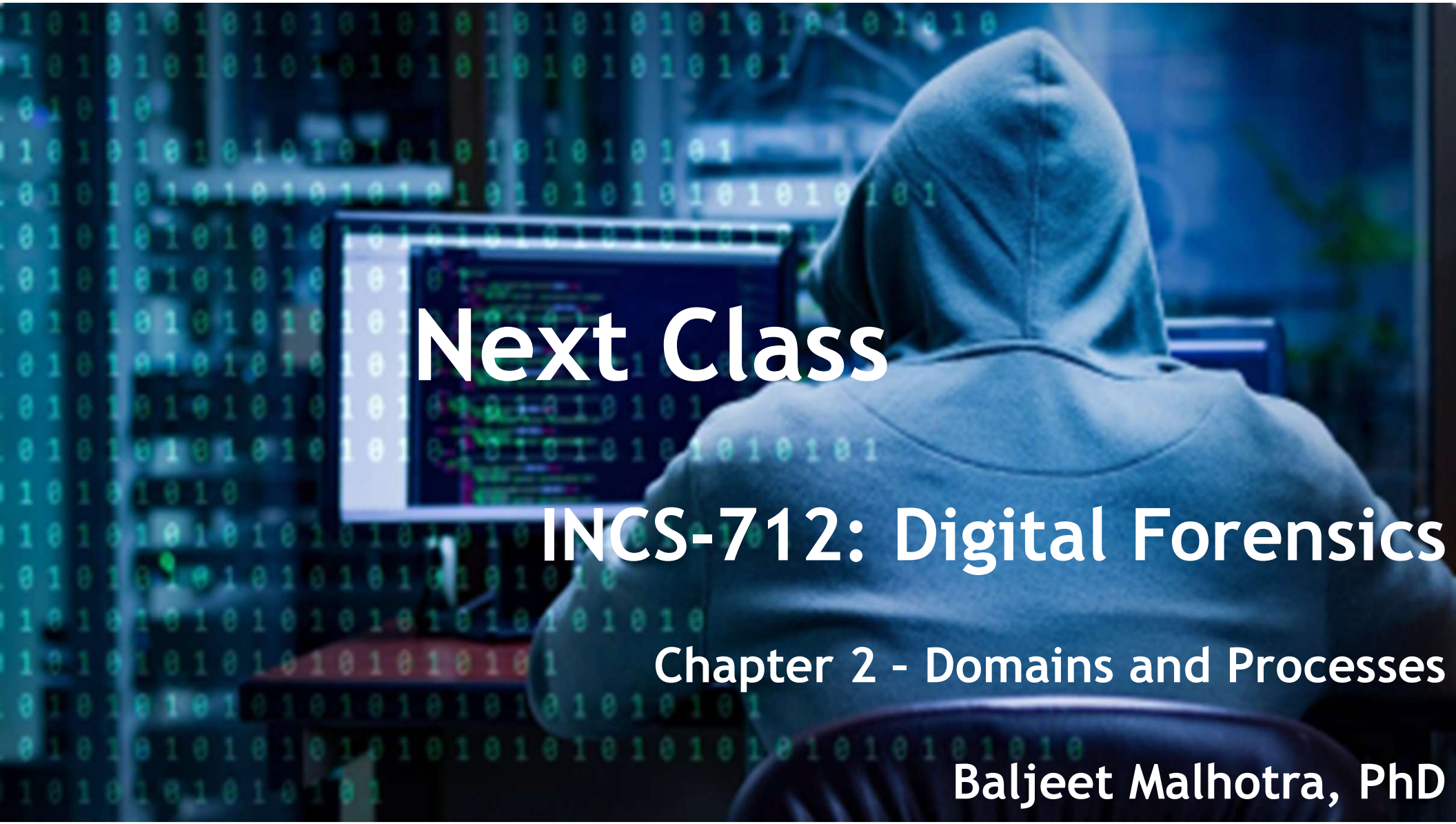
Network Intrusion Detection and Incident Response

- Detect intruder attacks by monitoring network firewall logs

Private Corporate Investigations

- Conduct forensics analysis of systems containing evidence

Data Recovery



Next Class

INCS-712: Digital Forensics

Chapter 2 - Domains and Processes

Baljeet Malhotra, PhD