INCS-712: Digital Forensics

Chapter 2 - Processes and Domains

Baljeet Malhotra, PhD

Cybersecurity Domains

Part 1: Various Cybersecurity Domains

Book Chapter: 2

Cybersecurity Domains

- **Cryptography**
- **Network Security**
- **Application Security**
- **Cloud/API Security**
- **Endpoint/IoT Security**
- **Operational Security**
- **Information Security**
- **Social Engineering and Training**
- **Identity and Access Management**
- **Incident Response and Recovery**
- **Governance Risk and Compliance**
- **Forensics and Legal Aspects**

Cryptography

Features	Details
Techniques	Involves using encryption techniques to secure communication and data.
Infrastructure	Public-key infrastructure (PKI), digital certificates, and cryptographic protocols like TLS/SSL.

Cybersecurity Domains

- Cryptography
- Network Security
- Application Security
- Cloud/API Security
- Endpoint/IoT Security
- Operational Security
- Information Security
- Social Engineering and Training
- Identity and Access Management
- Incident Response and Recovery
- Governance Risk and Compliance
- Forensics and Legal Aspects

Network Security

Features	Details
Techniques	Focuses on securing an organization's network infrastructure from unauthorized access, misuse, and attacks.
Infrastructure	Includes firewalls, intrusion detection/prevention systems (IDS/IPS), and VPNs.

Cybersecurity Domains

- Cryptography
- Network Security
- Application Security
- Cloud/API Security
- Endpoint/IoT Security
- Operational Security
- Information Security
- Social Engineering and Training
- Identity and Access Management
- Incident Response and Recovery
- Governance Risk and Compliance
- Forensics and Legal Aspects

Application Security

Features	Details
Techniques	Protects applications from vulnerabilities during development and deployment.
Infrastructure	Involves practices like secure coding, application testing, and patch management.
Applications	Web Application Firewalls (WAFs), pen testing SAT, DAT, and Vulnerability management.

Cybersecurity Domains

- **Cryptography**
- **Network Security**
- **Application Security**
- **Cloud/API Security**
- **Endpoint/IoT Security**
- **Operational Security**
- **Information Security**
- **Social Engineering and Training**
- **Identity and Access Management**
- **Incident Response and Recovery**
- **Governance Risk and Compliance**
- **Forensics and Legal Aspects**

Cloud/API Security

Features	Details
Techniques	Protects data and applications hosted in cloud environments.
Infrastructure	Involves securing cloud platforms like AWS, Azure, and Google Cloud.
Applications	Addresses challenges like shared responsibility models, misconfigurations, and cloud-specific attacks.

Cybersecurity Domains

- Cryptography
- Network Security
- Application Security
- Cloud/API Security
- **Endpoint/IoT Security**
- Operational Security
- Information Security
- Social Engineering and Training
- Identity and Access Management
- Incident Response and Recovery
- Governance Risk and Compliance
- Forensics and Legal Aspects

Endpoint/IoT Security

Features	Details
Techniques	Involves using encryption Secures devices (endpoints) like laptops, servers, smartphones, and Internet of Things (IoT) from threats. to secure communication and data.
Infrastructure	Includes antivirus software, endpoint detection and response (EDR), and mobile device management (MDM).

Cybersecurity Domains

- Cryptography
- Network Security
- Application Security
- Cloud/API Security
- Endpoint/IoT Security
- Operational Security
- Information Security
- Social Engineering and Training
- Identity and Access Management
- Incident Response and Recovery
- Governance Risk and Compliance
- Forensics and Legal Aspects

Operational Security

Features	Details
Techniques	Involves protecting day-to-day business operations by identifying and mitigating risks.
Infrastructure	Includes monitoring and maintaining security controls for ongoing business activities.

Cybersecurity Domains

- **Cryptography**
- **Network Security**
- **Application Security**
- **Cloud/API Security**
- **Endpoint/IoT Security**
- **Operational Security**
- **Information Security**
- **Social Engineering and Training**
- **Identity and Access Management**
- **Incident Response and Recovery**
- **Governance Risk and Compliance**
- **Forensics and Legal Aspects**

Information Security

Features	Details
Techniques	Ensures the confidentiality, integrity, and availability (CIA) of data.
Infrastructure	Protects sensitive information both in transit and at rest.
Applications	Covers data encryption, access controls, and compliance with regulations like GDPR or HIPAA.

Cybersecurity Domains

- Cryptography
- Network Security
- Application Security
- Cloud/API Security
- Endpoint/IoT Security
- Operational Security
- Information Security
- Social Engineering and Training
- Identity and Access Management
- Incident Response and Recovery
- Governance Risk and Compliance
- Forensics and Legal Aspects

Social Engineering

Features	Details
Techniques	Addresses human factors in cybersecurity by training employees to recognize phishing, scams, and other social engineering attacks.
Infrastructure	People training software, red team, blue team and

Cybersecurity Domains

- **Cryptography**
- **Network Security**
- **Application Security**
- **Cloud/API Security**
- **Endpoint/IoT Security**
- **Operational Security**
- **Information Security**
- **Social Engineering and Training**
- **Identity and Access Management**
- **Incident Response and Recovery**
- **Governance Risk and Compliance**
- **Forensics and Legal Aspects**

Identity and Access

Features	Details
Techniques	Manages user identities and controls access to systems and data.
Infrastructure	Implements authentication (e.g., multi-factor authentication) and authorization mechanisms.
Applications	Single Sign-On (SSO) and role-based access control (RBAC).

Cybersecurity Domains

- **Cryptography**
- **Network Security**
- **Application Security**
- **Cloud/API Security**
- **Endpoint/IoT Security**
- **Operational Security**
- **Information Security**
- **Social Engineering and Training**
- **Identity and Access Management**
- **Incident Response and Recovery**
- **Governance Risk and Compliance**
- **Forensics and Legal Aspects**

Incident Response

Features	Details
Techniques	Focuses on detecting, responding to, and recovering from cybersecurity incidents.
Infrastructure	Includes developing and implementing incident response plans (IRPs) and disaster recovery plans (DRPs).

Cybersecurity Domains

- **Cryptography**
- **Network Security**
- **Application Security**
- **Cloud/API Security**
- **Endpoint/IoT Security**
- **Operational Security**
- **Information Security**
- **Social Engineering and Training**
- **Identity and Access Management**
- **Incident Response and Recovery**
- **Governance Risk and Compliance**
- **Forensics and Legal Aspects**

GRC

Features	Details
Techniques	Establishes policies, procedures, and frameworks for managing cybersecurity risks and compliance.
Infrastructure	Examples: ISO 27001, NIST Cybersecurity Framework, and PCI-DSS compliance.

Cybersecurity Domains

- **Cryptography**
- **Network Security**
- **Application Security**
- **Cloud/API Security**
- **Endpoint/IoT Security**
- **Operational Security**
- **Information Security**
- **Social Engineering and Training**
- **Identity and Access Management**
- **Incident Response and Recovery**
- **Governance Risk and Compliance**
- **Forensics and Legal Aspects**

Digital Forensics

Features	Details
Techniques	Involves investigating cyber incidents and collecting digital evidence in a legally admissible manner.
Infrastructure	Works closely with law enforcement and legal teams.

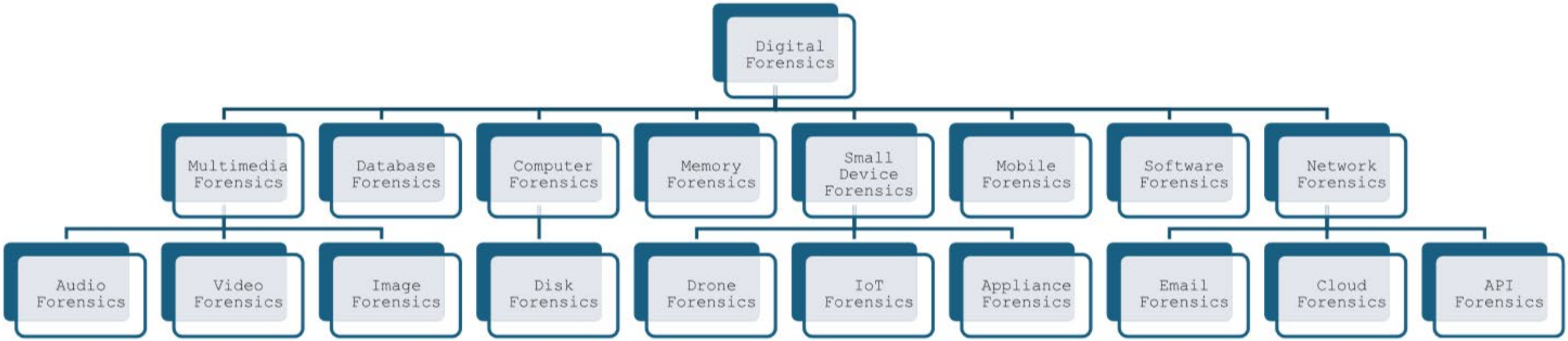
Cybersecurity Domains for Digital Forensics

Computers	Smart Devices	Internet of Things
Clouds	Networks	Applications and APIs
Databases	Intellectual Property	....

Subdomains of Digital Forensics

What are subdomains of digital forensics ?

Subdomains of Digital Forensics



Subdomain Specificities

- **Network Forensics:** primarily involves data collection by capturing packets from network traffic in real time

- **Cloud Forensics**: applied to cloud computing environments due to the distributed nature of cloud services, multitenancy, and the involvement of Cloud Service Providers (CSPs).
- **Database Forensics**: Deals with database-specific crimes by examining a diversity of existing database frameworks.
- **Mobile Forensics**: Retrieving data from mobile devices in a systematic manner is the primary objective of mobile forensics.

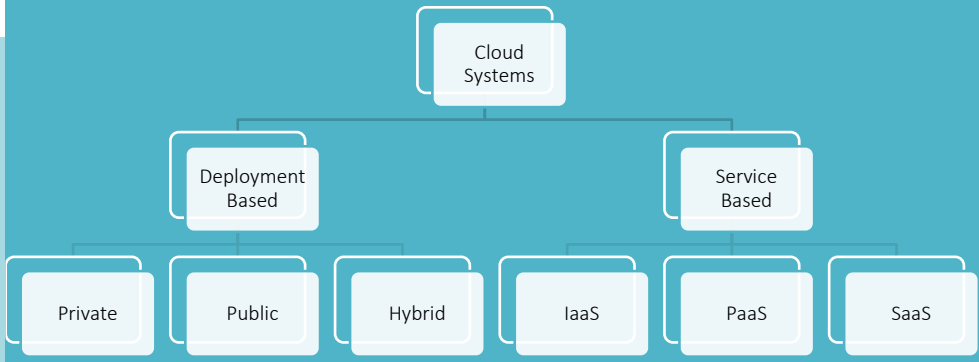
Network Forensics

Characteristics	Features
Data Source	Devices, networks, logs, and architecture details
Data Collection	Real-time traffic
Analysis Tools	1. Wireshark 2. TCPdump 3. Snort
Analysis Steps	Traffic pattern analysis, anomaly detection, and scenario reconstruction
Challenges	1. Big data processing 2. Real-time analysis 3. Encrypted traffic

Subdomain Specificities

- **Network Forensics:** primarily involves data collection by capturing packets from network traffic in real time
- **Cloud Forensics**: applied to cloud computing environments due to the distributed nature of cloud services, multitenancy, and the involvement of Cloud Service Providers (CSPs).
- **Database Forensics**: Deals with database-specific crimes by examining a diversity of existing database frameworks.
- **Mobile Forensics**: Retrieving data from mobile devices in a systematic manner is the primary objective of mobile forensics.

Cloud Forensics



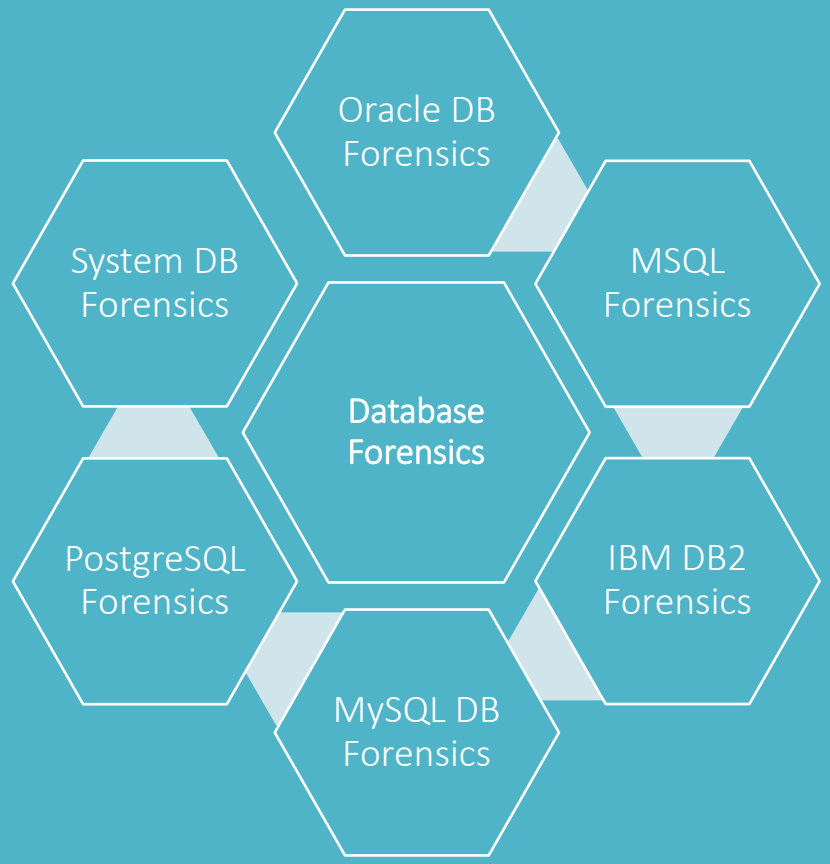
	SaaS	PaaS	IaaS	On Premise
Application				
Data				
Runtime				
Middleware				
Operating System				
Virtualization				
Servers				
Storage				
Networking				

Managed by Client | *Managed by CSP*

Subdomain Specificities

- **Network Forensics:** primarily involves data collection by capturing packets from network traffic in real time
- **Cloud Forensics**: applied to cloud computing environments due to the distributed nature of cloud services, multitenancy, and the involvement of Cloud Service Providers (CSPs).
- **Database Forensics**: Deals with database-specific crimes by examining a diversity of existing database frameworks.
- **Mobile Forensics**: Retrieving data from mobile devices in a systematic manner is the primary objective of mobile forensics.

Database Forensics



Subdomain Specificities

- **Network Forensics:** primarily involves data collection by capturing packets from network traffic in real time
- **Cloud Forensics**: applied to cloud computing environments due to the distributed nature of cloud services, multitenancy, and the involvement of Cloud Service Providers (CSPs).
- **Database Forensics**: Deals with database-specific crimes by examining a diversity of existing database frameworks.
- **Mobile Forensics**: Retrieving data from mobile devices in a systematic manner is the primary objective of mobile forensics.

Mobile Forensics

Text Messages	Deleted Text Messages	Call Logs
Photos and Videos	Contact and Calanders	GPS Locations
App Data and Usage	Voice Recordings	Web Browsing History

Subdomain Specificities

Measure	Process	Network Subdomain	Cloud Subdomain	Database Subdomain	Mobile Subdomain
Differences	Acquisition phase	Capture traffic network packets	Data location involves multiple locations	There are two types of information: volatile and nonvolatile data	Data acquisition depends on the type of device and its security features
	Analysis phase	The analysis is conducted over packets from the traffic collected	The analysis requires establishing the architecture diagram to establish the information location and the relationship among the multiple data centers	The analysis requires the reconstruction of the database at the incident time	The analysis involves data interpretation to understand the activities that occurred on the mobile device
Similarities	Analysis	Logs verification, in this case from Firewalls, Sniffers, and IDS	Logs analysis from the cloud provider	Logs verification from the database servers	Logs from calls and messages received
	Preservation	Information preservation of the packet captured	Information preservation creating forensic copies	Information preservation verifying hash integrity	Information preservation creates byte-to-byte copies
	Presentation	The last step of the process is reporting results in a nontechnical way	The last step of the process is reporting results in a nontechnical way	The last step of the process is reporting results in a nontechnical way	The last step of the process is reporting results in a nontechnical way

Comparison of Domain Processes

Book reading exercise: Study variations in device-based procedures?

Cybersecurity Processes

Part 2: Processes for Digital Forensics

Book Chapter: 2

General Process of Forensic Investigations

Identification

Source of evidence subject to legal considerations, which depends on understanding an incident and

defining its nature.

Preservation

Securing and maintaining the integrity of digital evidence from identification to analysis to legal proceedings.

Collection

Identifying, isolating, labeling, recording, and collecting data and other physical evidence related to the incident.

Examination

Extracting information from the collected data.

Analysis

Study the collected information to answer questions that arose during the previous phases of the forensic process.

Reporting

Documenting the results of the analysis, including relevant findings, actions performed, actions pending, and recommendations

Company Data Breach - An Example Scenario

Book reading exercise:
Which tools can be useful in this situation ?

Digital Crime Incidents

Part 2: What is a digital crime incident ?

Book Chapter: 2

Digital Incident and Digital Crime Incident

- **What is an Incident ?**
  - **Older definition:** Any unlawful, unauthorized, or unacceptable action that involves a computing system or computer network
  - **Recent definition**: Any unlawful, unauthorized, or unacceptable action that involves a computer system, cell phone, tablet, and any other electronic device with an operating system or that operates on a computer network
  - **NIST definition**: Any observable occurrence in a system or network
  - **Resource:** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
  - **Digital Crime Incident:** Refers to any event in which laws or policies are violated through the use or targeting of digital technologies. This type of crime involves activities that are facilitated or executed via electronic systems, particularly computers and the internet

Digital Crime Incidents

What are some of the examples of digital crime incidents?

Digital Crime Incidents

Identity Theft | Financial Fraud | IP Theft

Cyber Theft

This includes identity theft, financial fraud, and theft of intellectual property

Digital Crime Incidents

Cyber Attacks

These can be attacks on data, such as hacking or breaches, and attacks on infrastructure, such as denial-of-service attacks.

Digital Crime Incidents

Illegal Content

This involves activities like distributing child pornography or trafficking illegal goods online.

Digital Crime Incidents

Cyber Espionage

Unauthorized access to confidential data primarily for strategic, economic, or military advantage.

Digital Crime Incidents

Cyber Terrorism

Attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Digital Crime Incidents

What are the characteristics of digital crime incidents ?

Characteristics of Digital Crime Incidents

Virtual Nature

Unlike traditional crimes, digital crime incidents do not necessarily require the physical presence of the perpetrators at the crime scene. They can be conducted remotely, sometimes from another country.

Characteristics of Digital Crime Incidents

Anonymity

Perpetrators can often conceal their identities using various online anonymizing tools which makes tracking and prosecuting them challenging.

Characteristics of Digital Crime Incidents

Speed & Scale

Digital crimes can be carried out quickly and on a large scale, affecting thousands or even millions of users or systems simultaneously.

Characteristics of Digital Crime Incidents

Inter-jurisdictional

Because digital crimes can cross geographical and jurisdictional boundaries, they often require coordination across different law enforcement agencies internationally.

Digital Crime Scenes

Part 3: Nature of Digital Crime Scenes

Book Chapter: 2

Digital Crime Scene - Definition

- **Digital Crime Scene**: A "Digital Crime Scene" refers to the concept of an environment where a crime involving digital devices or networks has occurred. Unlike traditional crime scenes that involve physical spaces and tangible evidence, digital crime scenes involve data, electronic devices, and network infrastructures.

What are the characteristics of digital crime scenes?

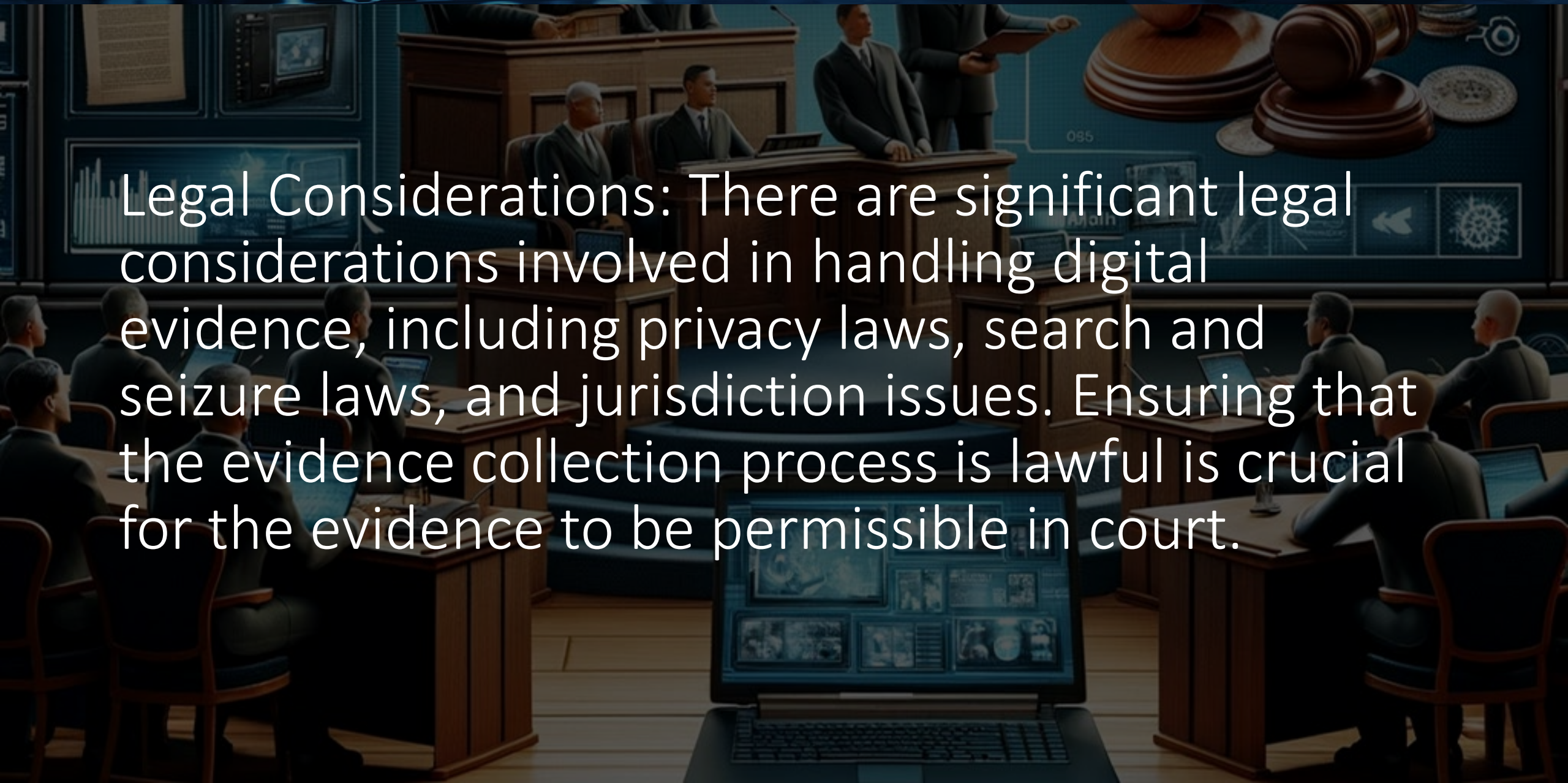
Nature of Digital Crime Scenes

Location and Accessibility: A digital crime scene may not be confined to a single location. It can be distributed across multiple jurisdictions or even globally, thanks to the interconnected nature of devices and networks. Accessing these scenes might require cooperation across different legal frameworks and regions.

Nature of Evidence at Crime Scenes

Nature of Evidence: The evidence at a digital crime scene is primarily digital data. This can include data from computers, smartphones, tablets, servers, and other connected devices. Digital evidence can be files, logs, emails, messages, images, and even metadata that provides insights into the activities performed on these devices.``

Nature of Jurisdiction involving Crime Scenes



Legal Considerations: There are significant legal considerations involved in handling digital evidence, including privacy laws, search and seizure laws, and jurisdiction issues. Ensuring that the evidence collection process is lawful is crucial for the evidence to be permissible in court.

Use of Software and Data at Crime Scenes

Investigation Tools: Investigators use specialized software and tools for digital forensics to recover, analyze, and preserve data from digital devices. These tools help in examining file systems, recovering deleted files, and tracing user activities.

Volatility of Evidence at Crime Scenes

Challenges: Unlike physical evidence, digital evidence can be highly volatile and easily manipulated, altered, or destroyed. Investigators must carefully handle and document the digital crime scene to maintain the integrity and admissibility of evidence.

Preservation of Evidence at Crime Scenes

Preservation: Ensuring that digital evidence is not tampered with during the collection process is crucial. Techniques like creating digital images of storage devices and using write blockers to prevent data modification are standard practices.

Digital Crime Evidence

Part 4: Types of Digital Crime Evidence

Book Chapter: 2

Digital Crime Evidence - Definition

- **Digital Crime Evidence** : Digital crime evidence refers to any information or data that is stored or transmitted in digital form that can be used by law enforcement agencies to support or refute a theory of how a crime occurred or to identify the responsible parties. This type of evidence is crucial in the investigation and prosecution of crimes that involve the use of computers, smartphones, and other digital devices.

Type of Digital Crime Evidence

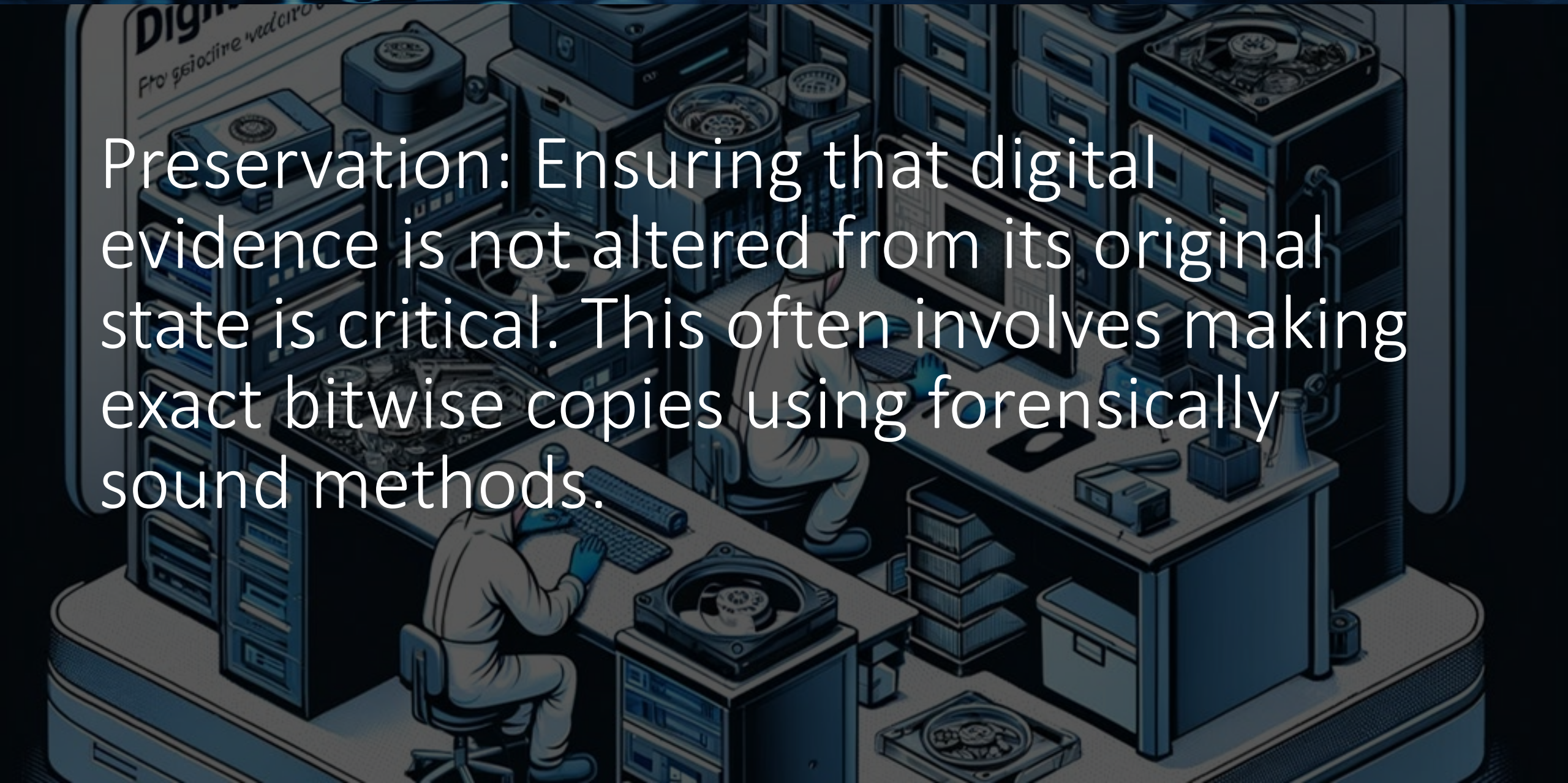
- **Stored Data**: This includes files saved on a device, such as documents, emails, photos, and videos. It also encompasses system files that can tell investigators when a device was used and what operations it performed.
- **Transient Data**: Temporary and includes memory data such as RAM, which can contain information about open files and programs that were running at a specific time.
- **Metadata**: Data about other data, which can include the time and date stamps of files, authorship data, and location information that helps to contextualize how other data was created, modified, or accessed.
- **Logs**: These are records kept by the system or applications detailing actions taken on the device or within software. This includes web server logs, system logs, and history files.
- **Communications**: Emails, social media messages, chats, and browsing history, which can reveal content/context of conversations as well as patterns of communication between parties.

Characteristics of Digital Crime Evidence

- **Latent**: Digital evidence can be hidden or encrypted and may require special tools or expertise to retrieve.
- **Volatile**: Some forms of digital evidence can be easily lost or altered, either intentionally or unintentionally, such as data stored in temporary memory.
- **Distributed**: Digital evidence can be spread across multiple devices and locations, including cloud storage services and servers located in different jurisdictions.

What are the challenges with digital crime evidence?

Preservation of Evidence

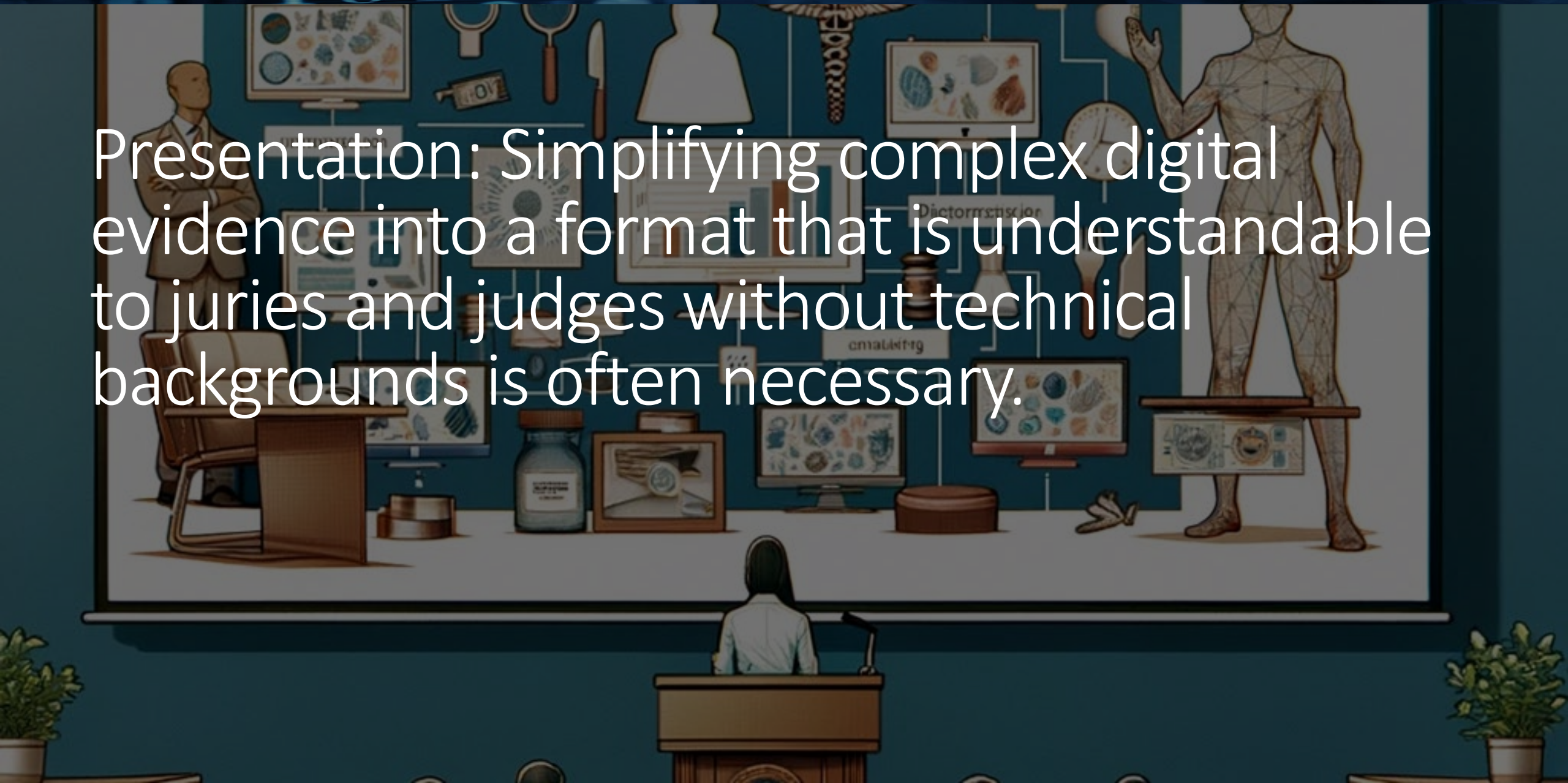


Preservation: Ensuring that digital evidence is not altered from its original state is critical. This often involves making exact bitwise copies using forensically sound methods.

Volume of Data Related to Digital Evidence

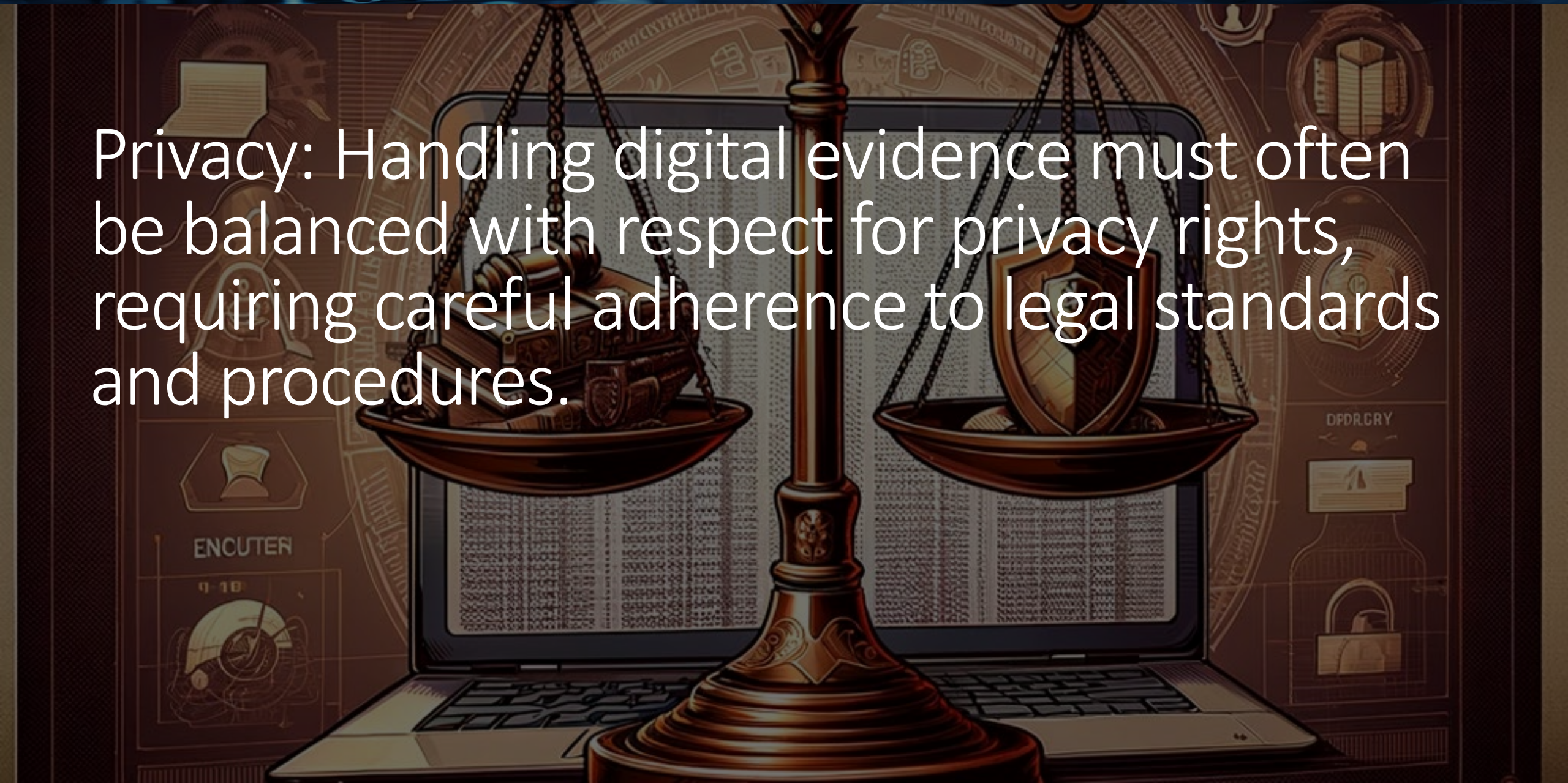
Analysis: The volume of data and the complexity of modern digital systems can make the analysis of digital evidence time-consuming and technically challenging.

Presentation of Digital Evidence



Presentation: Simplifying complex digital evidence into a format that is understandable to juries and judges without technical backgrounds is often necessary.

Handling Privacy (and corresponding laws)



Privacy: Handling digital evidence must often be balanced with respect for privacy rights, requiring careful adherence to legal standards and procedures.

Summary of Challenges

– **Preservation**: Ensuring that digital evidence is not altered from its original state is critical. This often involves making exact bitwise copies using forensically sound methods.

– **Analysis**: The volume of data and the complexity of modern digital systems can make the analysis of digital evidence time-consuming and technically challenging.

– **Presentation**: Simplifying complex digital evidence into a format that is understandable to juries and judges without technical backgrounds is often necessary.

– **Privacy**: Handling digital evidence must often be balanced with respect for privacy rights, requiring careful adherence to legal standards and procedures.

Next Class

INCS-712: Digital Forensics

Chapter 3 – Investigation Readiness

Baljeet Malhotra, PhD