D|FE
Digital Forensics Essentials

Module 01

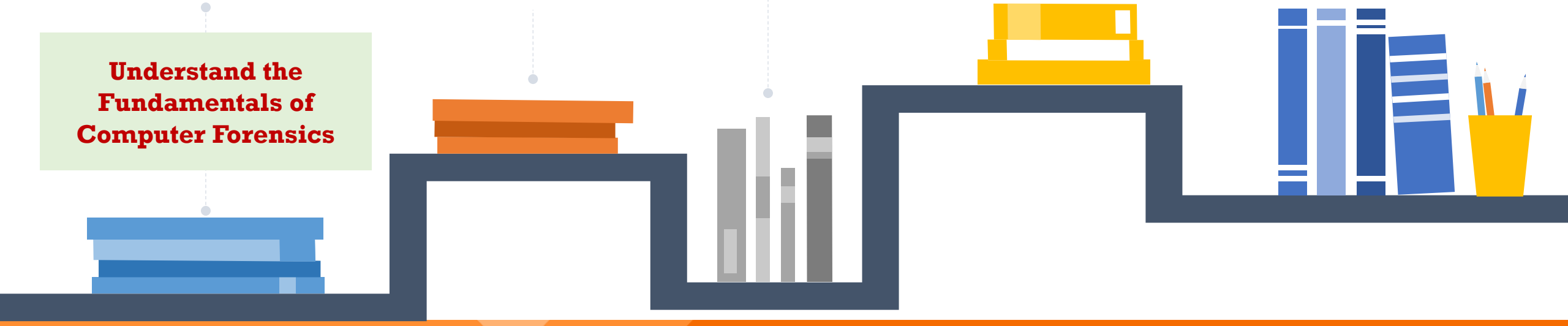
Computer Forensics Fundamentals

Module Objectives

1. Understanding the Fundamentals of Computer Forensics
2. Understanding Different Types of Cybercrimes
3. Overview of Indicators of Compromise (IoCs)
4. Overview of Different Types of Digital Evidence and Rules of Evidence
5. Understanding Forensic Readiness Planning and Business Continuity
6. Understanding the Roles and Responsibilities of a Forensic Investigator
7. Understanding the Legal Compliance in Computer Forensics

Module Flow

1. Understand the Fundamentals of Computer Forensics
2. Understand Digital Evidence
3. Understand Forensic Readiness
4. Identify the Roles and Responsibilities of a Forensic Investigator
5. Understand Legal Compliance in Computer Forensics



Understanding Computer Forensics

Computer forensics refer to a set of **methodological procedures** and **techniques** that help identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment, such that any discovered evidence is acceptable during a legal and/or administrative proceeding

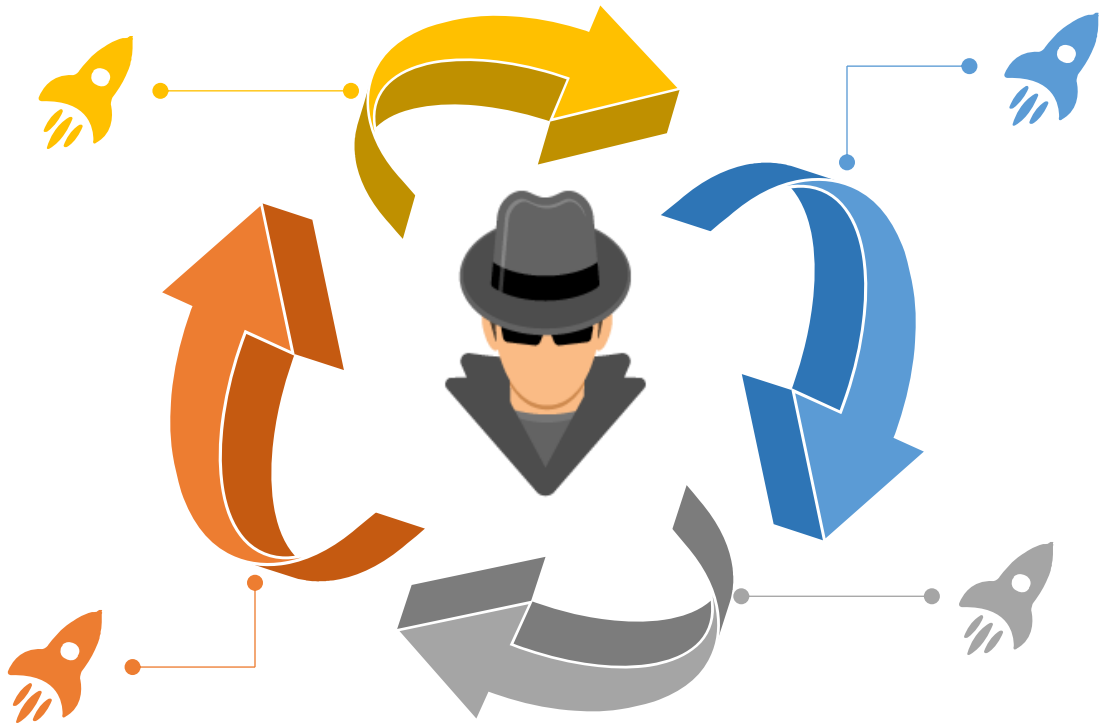
Objectives of Computer Forensics

- Identify, gather, and preserve the evidence of a cybercrime
- Gather evidence of cyber crimes in a forensically sound manner
- Estimate the potential impact of malicious activity on the victim and assess the intent of the perpetrator
- Minimize the tangible and intangible losses to the organization
- Protect the organization from similar incidents in the future
- Support the prosecution of the perpetrator of an incident

Need for Computer Forensics

01

To ensure the overall **integrity** and **continued existence** of IT systems and network infrastructure within the organizations



02

To extract, process, and interpret the factual evidence such that it proves the **attacker's actions in court**

03

To efficiently **track down perpetrators** from different parts of the world

04

To protect the **organization's financial resources** and valuable time

When Do You Use Computer Forensics?

- **Prepare for incidents** by securing and strengthening the defense mechanism as well as closing the loopholes in security
- **Identify the actions** needed for incident response
- Act against copyright and intellectual property theft/misuse
- **Estimate** and minimize the **damage** to resources in a corporate setup
- **Set a security parameter** and formulate security norms for ensuring forensic readiness

Types of Cybercrimes

Cybercrime is defined as **any illegal act** involving a computing device, network, its systems, or its applications

Cybercrime can be categorized into two types based on the line of attack

Internal/Insider Attack

- It is an attack performed on a corporate network or on a single computer by an **entrusted person (insider)** who has authorized access to the network
- Such **insiders** can be former or current employees, business partners, or contractors

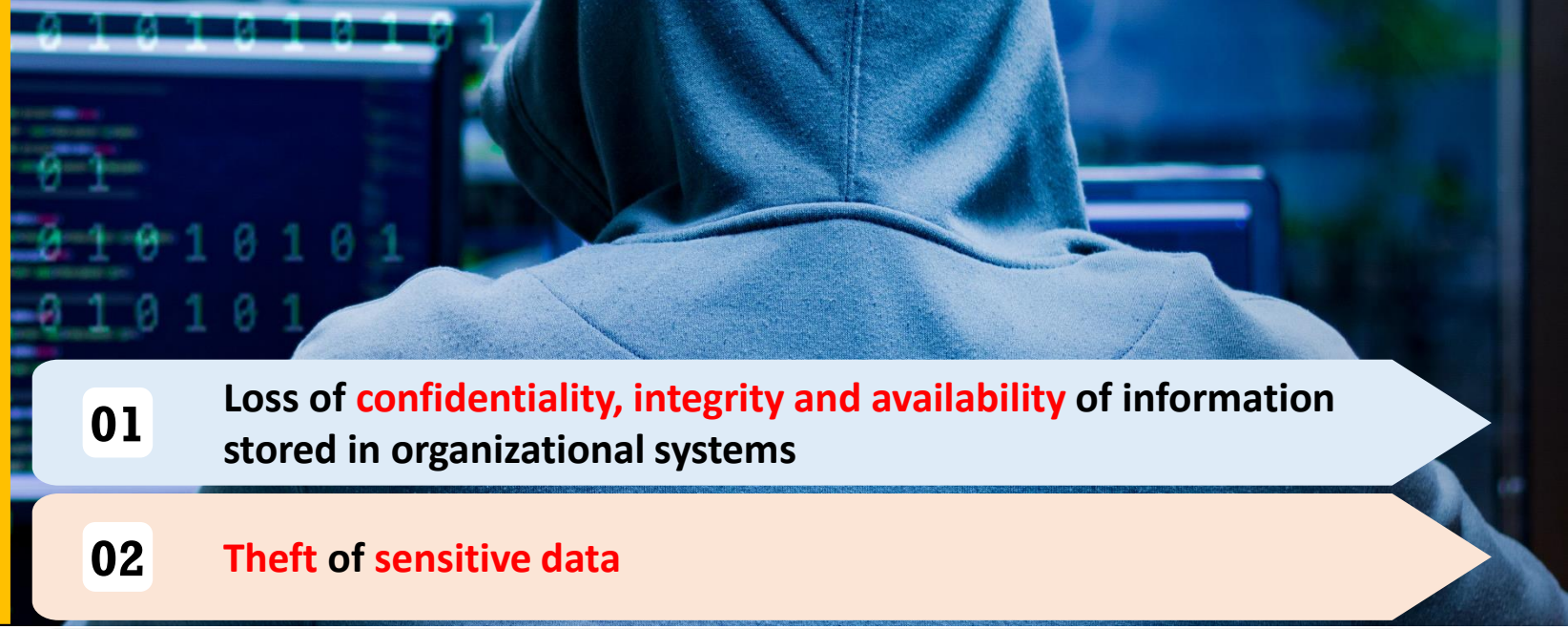
External Attack

- This type of attack occurs when an **attacker from outside the organization** tries to gain unauthorized access to its computing systems or informational assets
- These attackers **exploit security loopholes** or use **social engineering techniques** to infiltrate the network

Examples of Cybercrimes

1. Espionage
2. Intellectual Property Theft
3. Data Manipulation
4. Trojan Horse Attack
5. Structured Query Language Attack
6. Brute-force Attack
7. Phishing/Spoofing
8. Privilege Escalation Attacks
9. Denial of Service Attack
10. Cyber Defamation
11. Cyberterrorism
12. Cyberwarfare

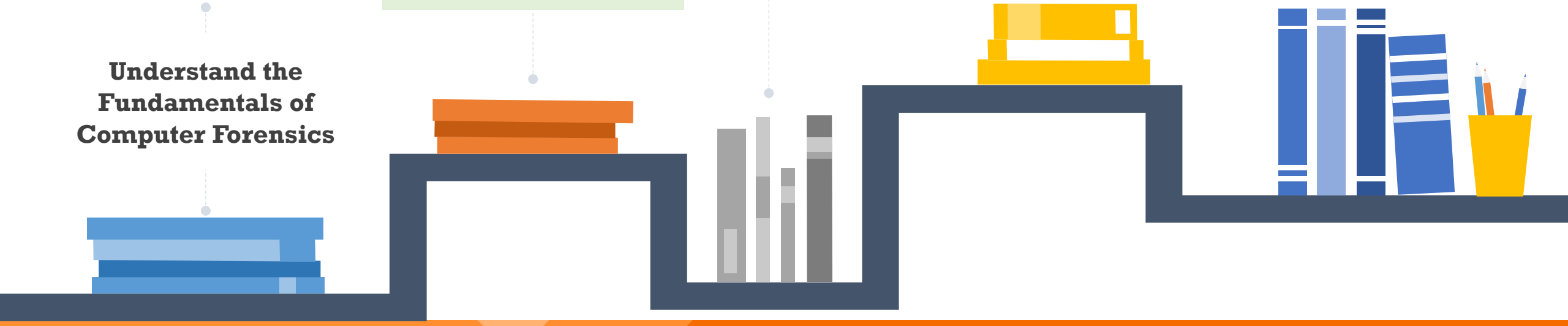
Impact of Cybercrimes at the Organizational Level



1. Loss of **confidentiality, integrity and availability** of information stored in organizational systems
2. **Theft** of **sensitive data**
3. Sudden **disruption of business activities**
4. Loss of **customer and stakeholder trust**
5. Substantial **reputational damage**
6. Huge **financial losses**
7. **Penalties** arising from the failure to comply with regulations

Module Flow

1. Understand the Fundamentals of Computer Forensics
2. Understand Digital Evidence
3. Understand Forensic Readiness
4. Identify the Roles and Responsibilities of a Forensic Investigator
5. Understand Legal Compliance in Computer Forensics



Introduction to Digital Evidence

Digital evidence is defined as “any information of **probative value** that is either stored or transmitted in a digital form”

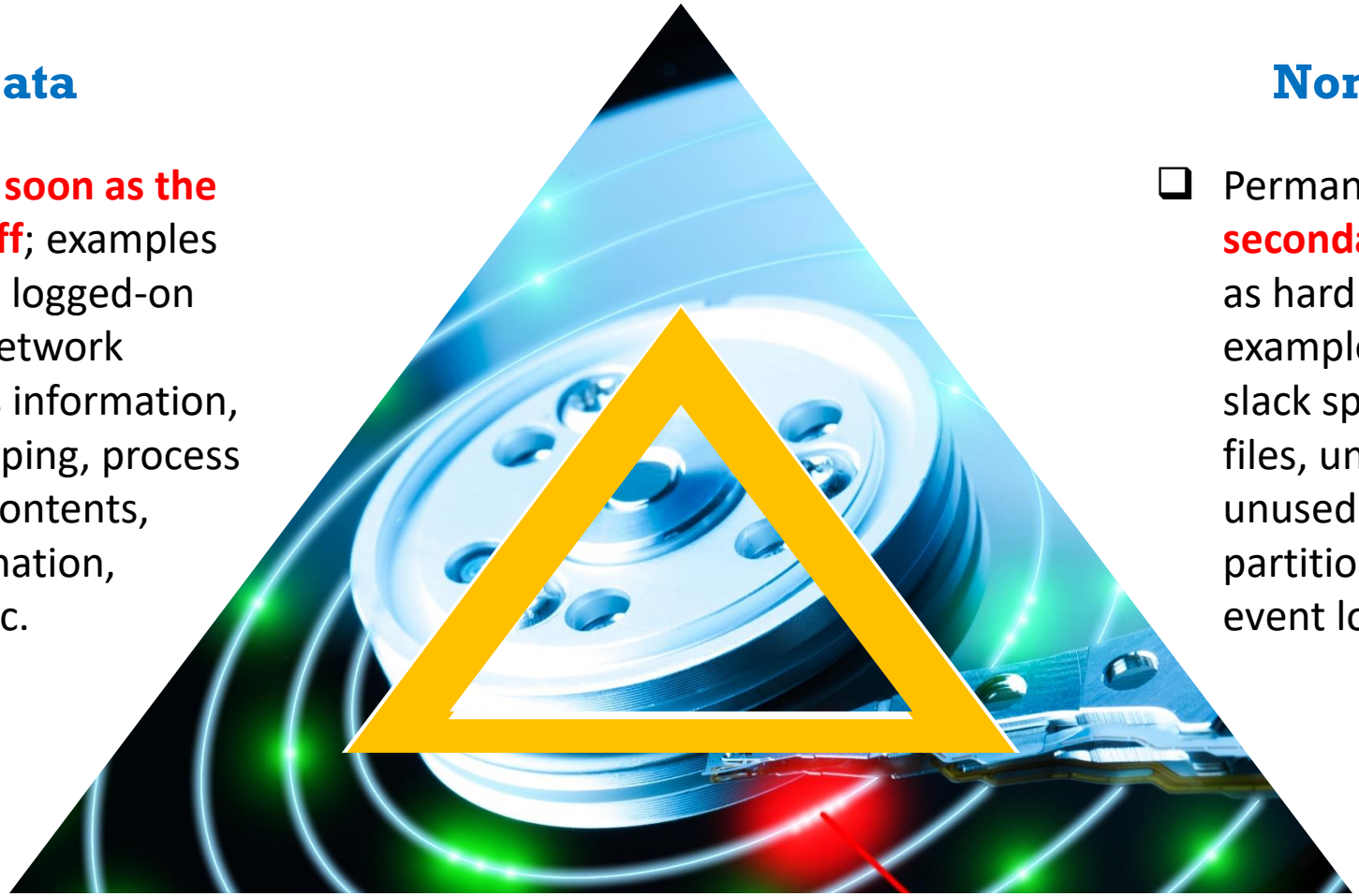
Digital evidence is **circumstantial** and **fragile** in nature, which makes it difficult for a forensic investigator to trace criminal activities

According to **Locard's Exchange Principle**, “anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave”

Types of Digital Evidence

Volatile Data

- Data that are **lost as soon as the device is powered off**; examples include system time, logged-on user(s), open files, network information, process information, process-to-port mapping, process memory, clipboard contents, service/driver information, command history, etc.



Non-volatile Data

- Permanent data **stored on secondary storage** devices such as hard disks and memory cards; examples include hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings, event logs, etc.

Roles of Digital Evidence

- Examples of cases where **digital evidence may assist** the forensic investigator in the prosecution or defense of a suspect:

01 **Identity theft**

02 **Malicious attacks on the computer systems themselves**

03 **Information leakage**

04 **Unauthorized transmission of information**

05 **Theft of commercial secrets**

06 **Use/abuse of the Internet**

07 **Production of false documents and accounts**

08 **Unauthorized encryption/ password protection of documents**

09 **Abuse of systems**

10 **Email communication between suspects/ conspirators**

Sources of Potential Evidence

User-Created Files

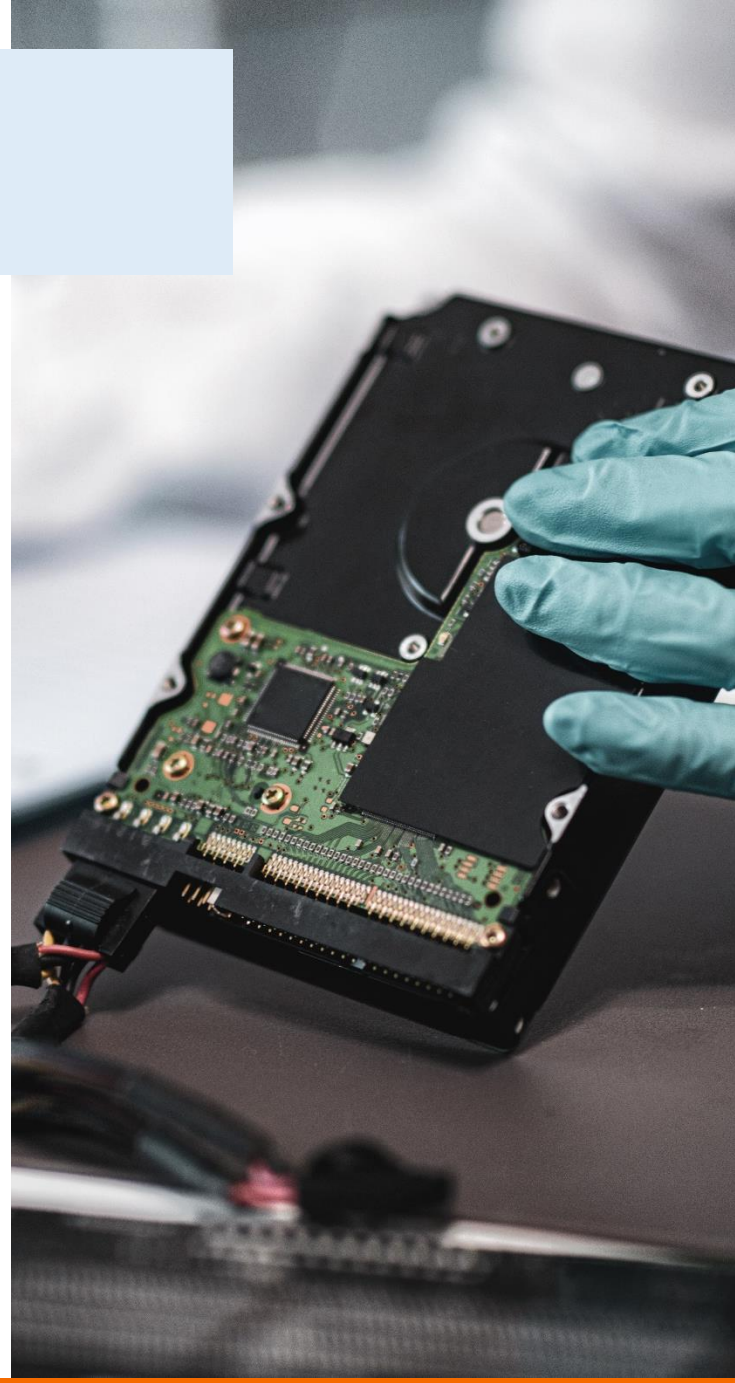
- Address books
- Database files
- Media (images, graphics, audio, video, etc.) files
- Documents (text, spreadsheet, presentation, etc.) files
- Internet bookmarks, favorites, etc.

User-Protected Files

- Compressed files
- Misnamed files
- Encrypted files
- Password-protected files
- Hidden files
- Steganography

Computer-Created Files

- Backup files
- Log files
- Configuration files
- Printer spool files
- Cookies
- Swap files
- System files
- History files
- Temporary files



Sources of Potential Evidence (Cont'd)

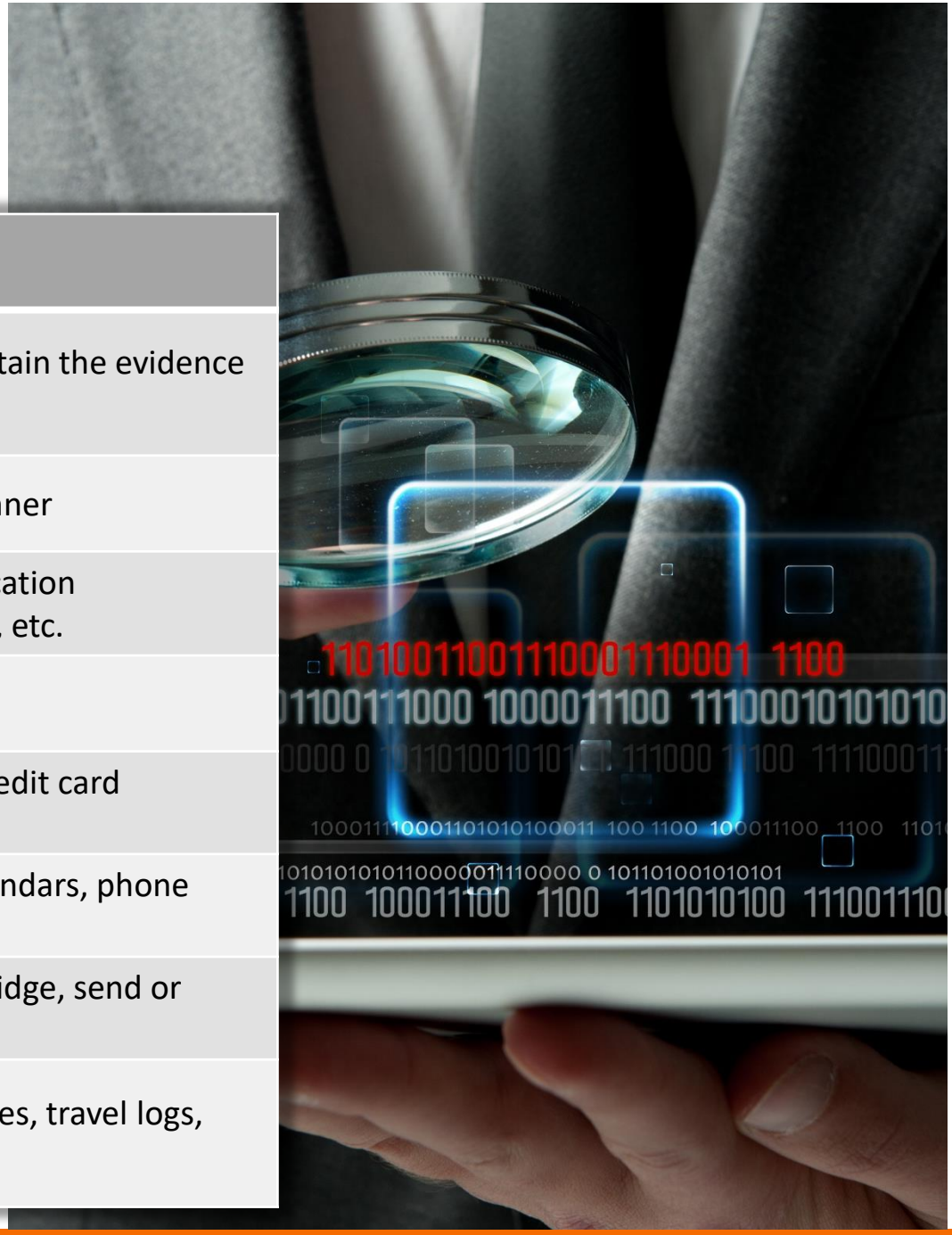
Device	Location of Potential Evidence
Hard Drive	Text, picture, video, multimedia, database, and computer program files
Thumb Drive	Text, graphics, image, and picture files
Memory Card	Event logs, chat logs, text files, image files, picture files, and internet browsing history
Smart Card	Evidence is found by recognizing or authenticating the information of the card and the user, through the level of access, configurations, permissions, and in the device itself
Dongle	
Biometric Scanner	
Answering Machine	Voice recordings such as deleted messages, last called number, memo, phone numbers, and tapes
Digital Camera/Surveillance cameras	Images, removable cartridges, video, sound, time and date stamp, etc.
Random Access Memory (RAM) and Volatile storage	Evidence is located and can be acquired from the main memory of the computer

Sources of Potential Evidence (Cont'd)

Device	Location of Potential Evidence
Handheld Devices	Address book, appointment calendars or information, documents, email, handwriting, password, phone book, text messages, and voice messages
Local Area Network (LAN) Card/ Network Interface Card (NIC)	MAC (Media Access Control) address
Routers, Modem, Hubs, and Switches	For routers, evidence is found in the configuration files For hubs, switches, and modems evidence is found on the devices themselves
Network Cables and Connectors	On the devices themselves
Server	Computer system
Printer	Evidence is found through usage logs, time and date information, and network identity information, ink cartridges, and time and date stamp
Internet of Things and wearables	Evidence can be acquired in the form of GPS, audio and video recordings, cloud storage sensors, etc.

Sources of Potential Evidence (Cont'd)

Device	Location of Potential Evidence
Removable Storage Device and Media	Storage device and media such as tape, CD, DVD, and Blu-ray contain the evidence in the devices themselves
Scanner	Evidence is found by looking at the marks on the glass of the scanner
Telephones	Evidence is found through names, phone numbers, caller identification information, appointment information, electronic mail and pages, etc.
Copiers	Documents, user usage logs, time and date stamps, etc.
Credit Card Skimmers	Evidence is found through card expiration date, user's address, credit card numbers, user's name, etc.
Digital Watches	Evidence is found through address book, notes, appointment calendars, phone numbers, email, etc.
Facsimile (Fax) Machines	Evidence is found through documents, phone numbers, film cartridge, send or receive logs
Global Positioning Systems (GPS)	Evidence is found through previous destinations, way points, routes, travel logs, etc.



Rules of Evidence

- Digital evidence collection must be governed by **five basic rules** that make it **admissible in a court of law**:

1. **Understandable**

   Evidence must be **clear and understandable** to the judges

2. **Admissible**

   Evidence must be **related to the fact** being proved

3. **Authentic**

   Evidence must be **real and** appropriately **related** to the incident

4. **Reliable**

   There must be no doubt about the **authenticity or veracity** of the evidence

5. **Complete**

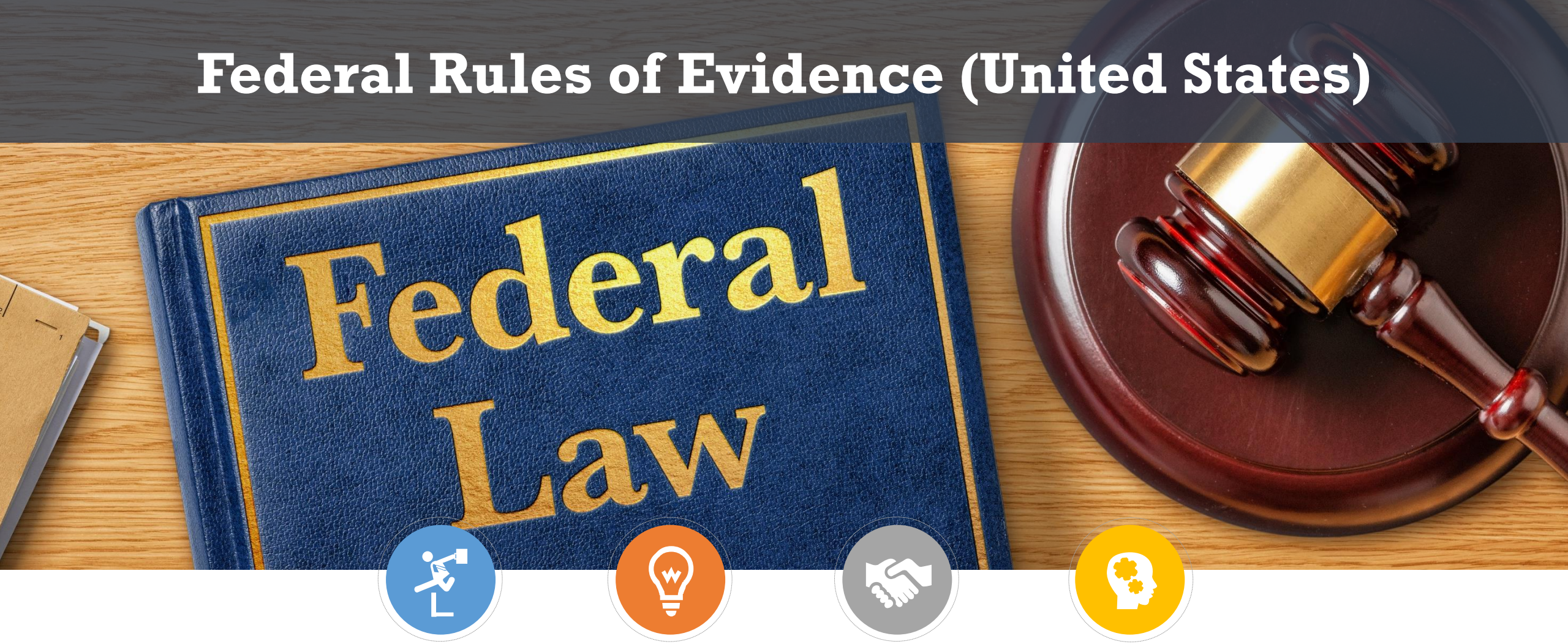
   The evidence must prove the attacker's **actions or** his/her **innocence**

Best Evidence Rule

It states that the court only allows the **original evidence of a document**, **photograph**, or **recording** at the trial rather than a copy. However, the duplicate can be accepted as evidence, provided the court finds the party's reasons for submitting the duplicate to be genuine.

The principle underlying the best evidence rule is that the original evidence is considered as the best evidence

Federal Rules of Evidence (United States)



These rules shall be construed to **secure fairness in administration**, **elimination of unjustifiable expense and delay**, and promotion of growth and development of the law of evidence to the end that the truth may be ascertained and proceedings justly determined

https://www.rulesofevidence.org

Scientific Working Group on Digital Evidence (SWGDE)

Principle 1

- In order to ensure that the digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the **accuracy and reliability of the evidence**, law enforcement and forensic organizations must establish and maintain an effective quality system

Standards and Criteria 1.1

- All agencies that **seize and/or examine** digital evidence must maintain an appropriate SOP document. All elements of an agency's policies and procedures concerning digital evidence must be clearly set forth in this SOP document, which must be issued under the agency's management authority.

Standards and Criteria 1.2

- Agency management must **review the SOPs** on an annual basis to ensure their continued suitability and effectiveness

Standards and Criteria 1.3

- Procedures used must be generally accepted in the field or supported by data **gathered and recorded** in a scientific manner

https://www.swgde.org

Scientific Working Group on Digital Evidence (SWGDE) (Cont'd)

1

Standards and Criteria 1.4

The agency must **maintain written copies** of appropriate technical procedures

2

Standards and Criteria 1.5

The agency must **use hardware and software** that are appropriate and effective for the seizure or examination procedure

3

Standards and Criteria 1.6

All activity relating to the seizure, storage, examination, or transfer of the digital evidence must be recorded in writing and be **available for review and testimony**

4

Standards and Criteria 1.7

Any action that has the potential to alter, damage, or destroy any aspect of the original evidence must be performed by qualified persons **in a forensically sound manner**

https://www.swgde.org

The Association of Chief Police Officers (ACPO) Principles of Digital Evidence

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be **relied upon in court**

Principle 2: In exceptional circumstances, where a person finds it necessary **to access original data** held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court

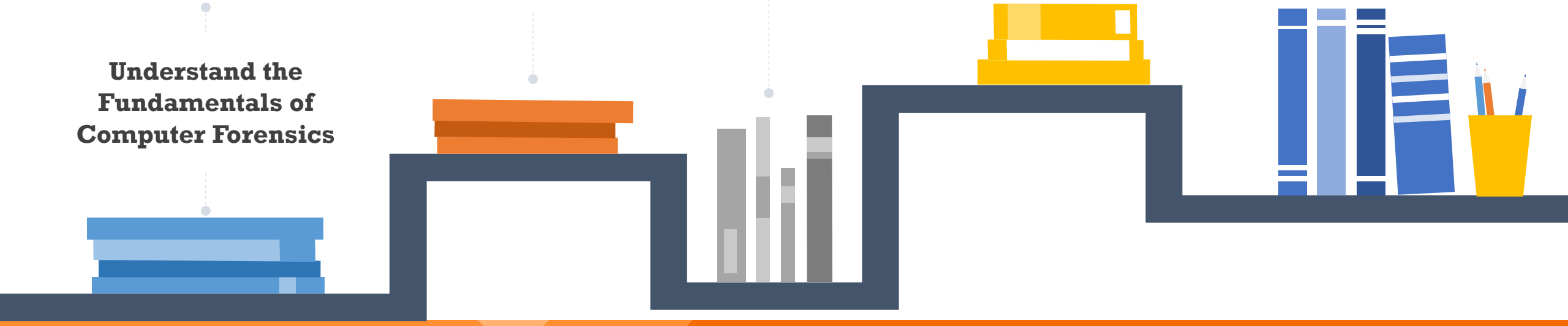
Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An **independent third party** should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for **ensuring that the law and these principles** are adhered to

https://www.college.police.uk

Module Flow

1. Understand the Fundamentals of Computer Forensics
2. Understand Digital Evidence
3. Understand Forensic Readiness
4. Identify the Roles and Responsibilities of a Forensic Investigator
5. Understand Legal Compliance in Computer Forensics



Forensic Readiness

- Forensic readiness refers to an organization's ability to **optimally use digital evidence** in a limited period of time and with minimal investigation costs

Benefits:

- Fast and efficient investigation with **minimal disruption** to the **business**
- Provides **security** from cybercrimes such as intellectual property theft, fraud, or extortion
- Offers structured storage of evidence that reduces the **cost** and time of an **investigation**
- Improves **law enforcement interface**
- Helps the organization use the **digital evidence** in its own defense

Forensic Readiness and Business Continuity

- Forensic readiness helps **maintain business continuity** by allowing quick and easy identification of the impacted components and replacing them to continue the services and business

Forensic readiness allows businesses to:

- Quickly determine the incidents
- Collect legally sound evidence and analyze it to identify attackers
- Minimize the required resources
- Quickly recover from damage with less downtime
- Gather evidence to claim insurance
- Legally prosecute the perpetrators and claim damages

Lack of forensic readiness may result in:

- Loss of clients due to damage to the organization's reputation
- System downtime
- Data manipulation, deletion, and theft
- Inability to collect legally sound evidence

Forensics Readiness Planning

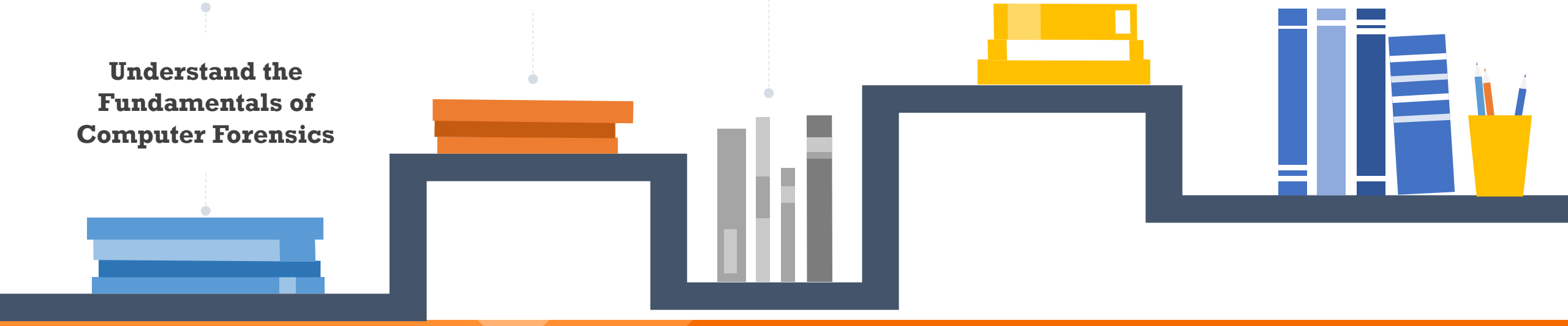
- Forensic readiness planning refers to a **set of processes** to be followed to achieve and maintain forensics readiness

1. Identify the **potential evidence** required for an incident
2. Determine the **sources of evidence**
3. Define a **policy that determines the pathway** to legally extract electronic evidence with minimal disruption
4. Establish a **policy** to **handle and store** the acquired evidence in a secure manner

5. Identify if the incident requires **full or formal investigation**
6. Create a **process** for documenting the procedure
7. Establish a **legal advisory board** to guide the investigation process
8. Keep an **incident response** team ready to review the incident and preserve the evidence

Module Flow

1. Understand the Fundamentals of Computer Forensics
2. Understand Digital Evidence
3. Understand Forensic Readiness
4. Identify the Roles and Responsibilities of a Forensic Investigator
5. Understand Legal Compliance in Computer Forensics



Need for a Forensic Investigator

Cybercrime Investigation

Forensic investigators, by virtue of their skills and experience, help organizations and law enforcement agencies **investigate and prosecute** the perpetrators of cybercrimes

Sound Evidence Handling

If a **technically inexperienced** person examines the evidence, it might become inadmissible in a court of law

Incident Handling and Response

Forensic investigators help organizations maintain forensics readiness and implement **effective incident handling and response**

Roles and Responsibilities of a Forensics Investigator

A forensic investigator performs the following tasks:

- Determines the **extent of any damage** done during the crime
- **Recovers data** of investigative value from computing devices involved in crimes
- Creates an image of the original evidence without tampering with it to **maintain its integrity**
- **Guides** the **officials** carrying out the investigation

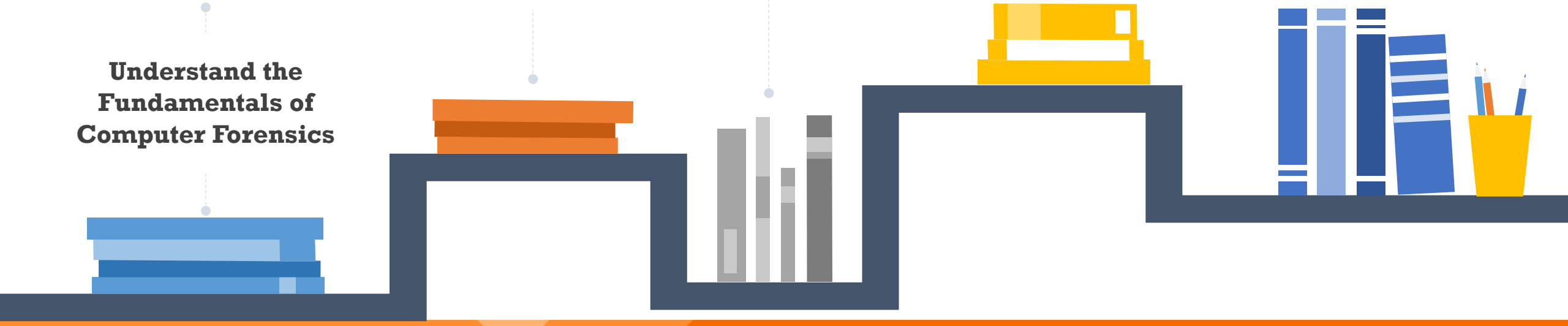
- Analyzes the evidence data found
- Prepares the analysis report
- **Updates** the **organization** about various attack methods and data recovery techniques, and maintains a record of them
- Addresses the issue in a court of law and attempts to win the case by **testifying in court**

What Makes a Good Computer Forensics Investigator?

- Interviewing skills to **gather** extensive **information** about the case from the client or victim, witnesses, and suspects
- Excellent writing skills to **detail findings** in the report
- Strong analytical **skills to find** the evidence and link it to the suspect
- Excellent communication skills to explain their findings to the audience
- Remains updated about new methodologies and **forensic technology**
- Well-versed in more than one computer platform (including Windows, Macintosh, and Linux)
- Knowledge of various technologies, hardware, and software
- Develops and maintains contact with computing, networking, and investigating professionals
- Has **knowledge of the laws** relevant to the case

Module Flow

1. Understand the Fundamentals of Computer Forensics
2. Understand Digital Evidence
3. Understand Forensic Readiness
4. Identify the Roles and Responsibilities of a Forensic Investigator
5. Understand Legal Compliance in Computer Forensics



Computer Forensics and Legal Compliance

- Legal compliance in computer forensics ensures that any evidence that is collected and analyzed is **admissible in a court of law**
- Compliance with certain regulations and standards plays an important part in computer forensic investigation and analysis, some of which are as follows:

01 **Gramm-Leach-Bliley Act (GLBA)**

02 **Federal Information Security Modernization Act of 2014 (FISMA)**

03 **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

04 **Payment Card Industry Data Security Standard (PCI DSS)**

05 **Electronic Communications Privacy Act**

06 **General Data Protection Regulation (GDPR)**

07 **Data Protection Act 2018**

08 **Sarbanes-Oxley Act (SOX) of 2002**

Other Laws Relevant to Computer Forensics

United States	Foreign Intelligence Surveillance Act	https://www.fas.org
	Protect America Act of 2007	https://www.congress.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.congress.gov
	Computer Security Act of 1987	https://www.congress.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov
United Kingdom	Regulation of Investigatory Powers Act 2000	https://www.legislation.gov.au
Australia	Cybercrime Act 2001	https://www.legislation.gov.au
	Information Privacy Act 2014	https://www.findandconnect.gov.au
India	Information Technology Act	http://www.dot.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net
Italy	Penal Code Article 615 ter	http://www.cybercrimelaw.net
Canada	Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
Belgium	Computer Hacking	http://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Philippines	Data Privacy Act of 2012	https://www.privacy.gov.ph
Hong Kong	Cap. 486 Personal Data (Privacy) Ordinance	https://www.pcpd.org.hk

Module Summary

1. This module has discussed the fundamentals of computer forensics
2. It has covered various types of digital evidence and rules of evidence
3. It also discussed in detail on various laws and rules to be considered during digital evidence collection
4. This module also discussed the forensic readiness planning and business continuity
5. It has also discussed the roles and responsibilities of a forensic investigator
6. Finally, this module ended with a detailed discussion on legal compliance in computer forensics
7. In the next module, we will discuss in detail on computer forensics investigation process