



D FE

Digital

Forensics Essentials

Module 02

Computer Forensics Investigation Process

Module Objectives

- 1 Understanding the Forensic Investigation Process and its Importance
- 2 Understanding the Pre-investigation Phase
- 3 Understanding the Investigation Phase
- 4 Understanding the Post-investigation Phase



Module Flow

**Forensic Investigation
Process - Pre-investigation
Phase**

**Forensic Investigation
Process - Investigation
Phase**

**Forensic Investigation
Process - Post-investigation
Phase**

**Understand the Forensic
Investigation Process and
its Importance**

01

02

03

04

Forensic Investigation Process



A methodological approach to **investigate**, **seize**, and **analyze digital evidence** and then manage the case from the time of search and seizure to reporting the investigation result

Importance of the Forensic Investigation Process



As digital evidence is fragile in nature, following strict guidelines and thorough forensic investigation process that **ensures the integrity** of evidence is critical to prove a case in the court of law



The forensics investigation process to be followed should **comply** with **local laws and established precedents**. Any breach/deviation may jeopardize the complete investigation.



The investigators **must follow a repeatable and well-documented set of steps** such that every iteration of analysis provides the same findings; else, the findings of the investigation can be invalidated during the cross examination in a court of law



Phases Involved in the Forensics Investigation Process



Pre-investigation Phase

- ❑ Deals with tasks to be performed prior to the commencement of the **actual investigation**
- ❑ Involves setting up a **computer forensics lab**, building a forensics workstation, developing an investigation toolkit, setting up an investigation team, getting approval from the relevant authority, etc.



Investigation Phase

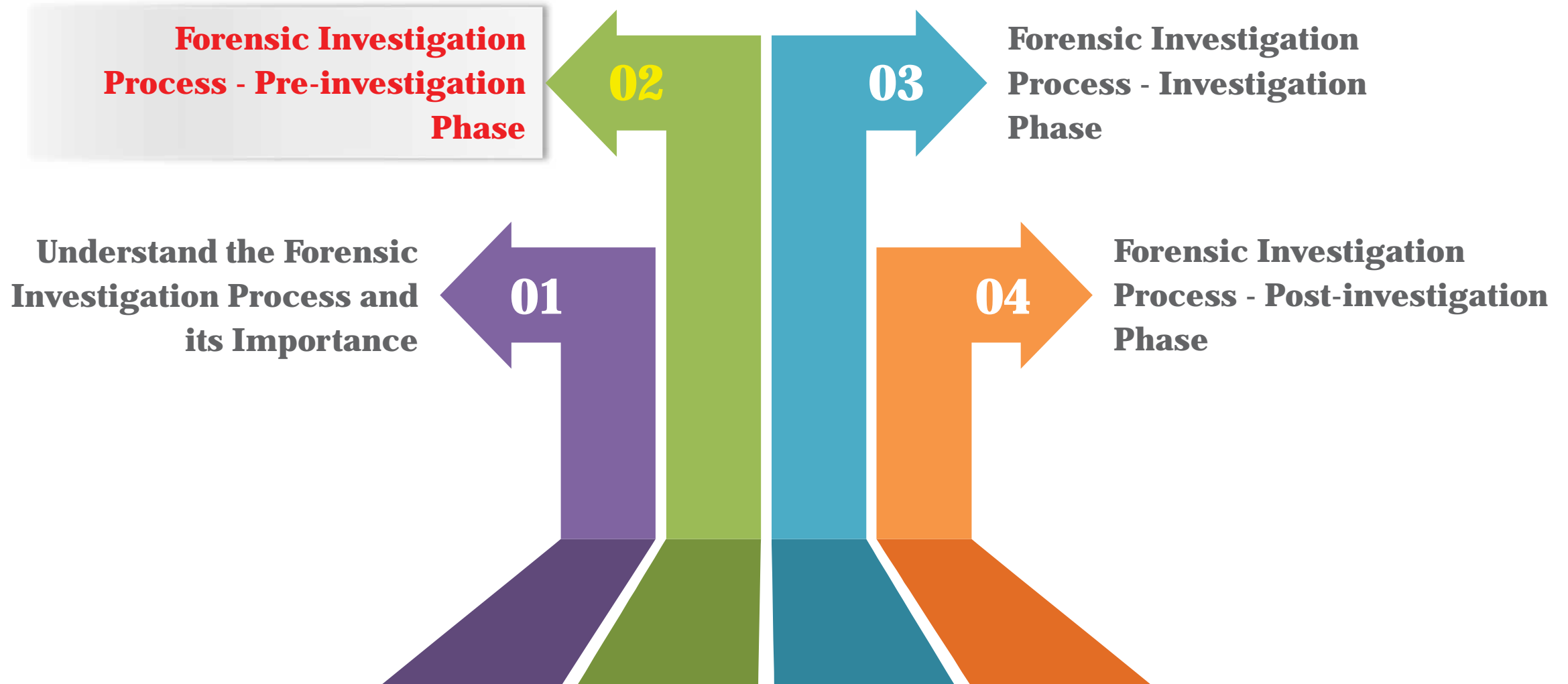
- ❑ The **main phase** of the computer forensics investigation process
- ❑ Involves acquisition, preservation, and analysis of **evidentiary data** to identify the **source of the crime** and the culprit behind it



Post-investigation Phase

- ❑ Includes **documentation** of all actions undertaken and all findings uncovered during the investigation
- ❑ Ensures that the **report** is easily explicable to the target audience and that it provides **adequate** and **acceptable** evidence

Module Flow



Setting Up a Computer Forensics Lab



A Computer Forensics Lab (CFL) is a location that houses instruments, **software** and **hardware** tools, and **forensic workstations** required for conducting a **computer-based investigation** with regard to the collected evidence

1

Planning & budgeting considerations

- ✓ Number of expected cases
- ✓ Type of investigation
- ✓ Manpower
- ✓ Equipment and software requirement

2

Physical & Structural design considerations

- ✓ Lab size
- ✓ Access to essential services
- ✓ Space estimation for work area and evidence storage
- ✓ Heating, ventilation, and air-conditioning

3

Work area considerations

- ✓ Workstation requirement
- ✓ Ambience
- ✓ Internet, network and communication line
- ✓ Lighting systems and emergency power

4

Physical security considerations

- ✓ Electronic sign-in
- ✓ Intrusion alarm systems
- ✓ Fire suppression systems

5

Human resource considerations

- ✓ Number of required personnel
- ✓ Training and certification

6

Forensic lab licensing

- ✓ ASCLD/LAB accreditation
- ✓ ISO/IEC 17025 accreditation

Building the Investigation Team



- ❑ Keep the **team small** to protect the confidentiality of the investigation and to guard against **information leaks**
- ❑ Identify team members and **assign them responsibilities**
- ❑ Ensure that every team member has the necessary **clearance** and **authorization** to conduct assigned tasks
- ❑ Assign one team member as the technical lead for the **investigation**

People Involved in an Investigation Team	
Photographer	Photographs the crime scene and the evidence gathered
Incident Responder	Responsible for the measures to be taken when an incident occurs
Incident Analyzer	Analyzes the incidents based on their occurrence
Evidence Examiner/Investigator	Examines the evidence acquired and sorts the useful evidence
Evidence Documenter	Documents all the evidence and the phases present in the investigation process
Evidence Manager	Manages the evidence in such a way that it is admissible in the court of law
Evidence Witness	Offers a formal opinion in the form of a testimony in the court of law
Attorney	Provides legal advice

Understanding the Hardware and Software Requirements of a Forensic Lab

- ❑ A digital forensic lab should have all the necessary **hardware and software tools** to support the investigation process, starting from searching and seizing the evidence to reporting the outcome of the analysis



Hardware

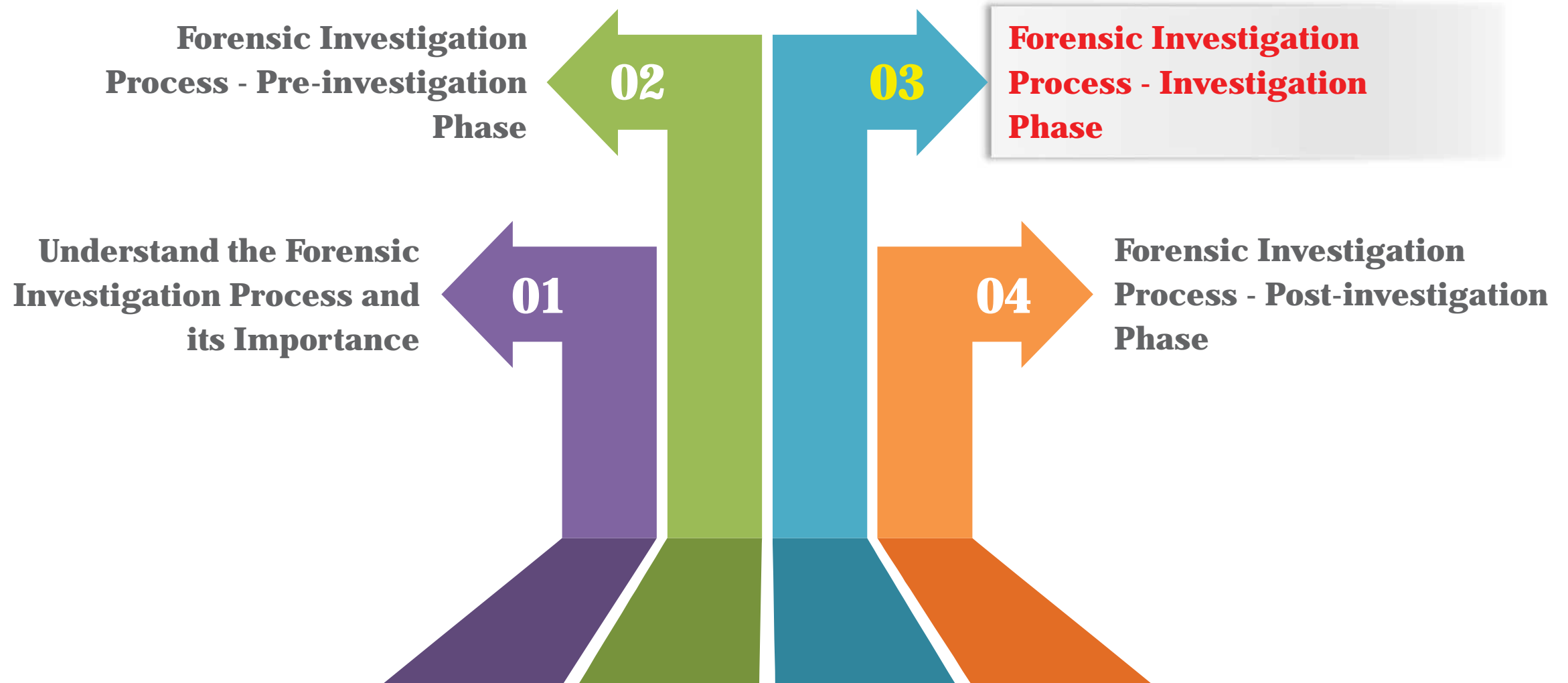
- Two or more forensic workstations with good processing power and RAM
- Specialized cables
- Write-blockers and drive duplicators
- Archive and Restore devices
- Media sterilization systems
- Other equipment that allow forensic software tools to work
- Computer Forensic hardware toolkit, such as Paraben's First Responder Bundle, DeepSpar Disk Imager, FRED forensic workstation etc.



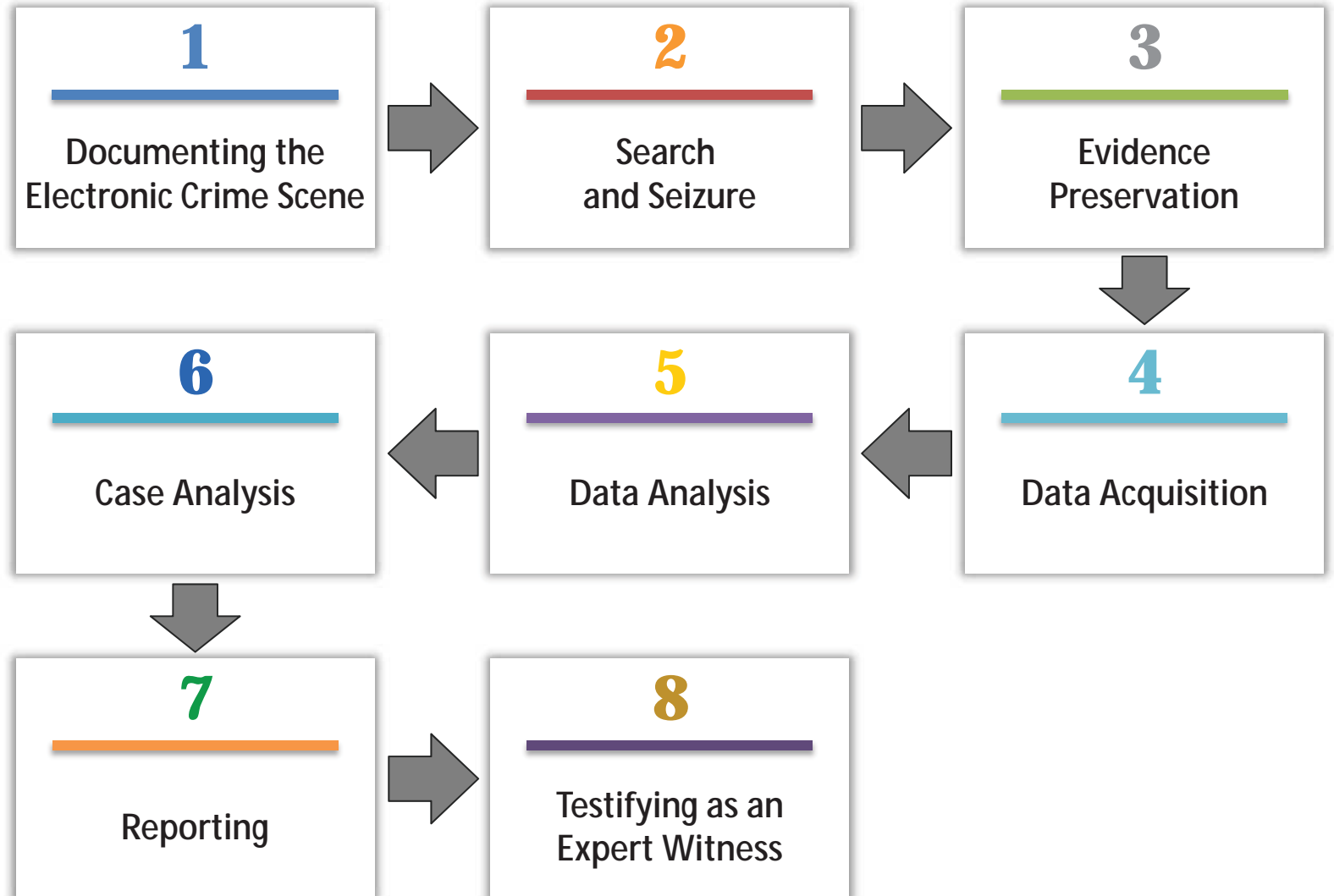
Software

- OSes
- Data discovery tools
- Password-cracking tools
- Acquisition tools
- Data analyzers
- Data recovery tools
- File viewers (Image and graphics)
- File type conversion tools
- Security and Utilities software
- Computer forensic software tools such as Wireshark, Access Data's FTK etc.

Module Flow



Computer Forensics Investigation Methodology



Documenting the Electronic Crime Scene

- ❑ Documentation of the electronic crime scene is necessary to **maintain a record** of all the **forensic investigation processes** performed to identify, extract, analyze, and preserve the evidence

Points to remember when documenting the crime scene

- Document the **physical crime scene**, noting the position of the system and other equipment, if any
- Document details of any related or difficult-to-find **electronic components**
- Record the **state of computer systems**, digital storage media, and electronic devices, including their power status



Search and Seizure

☐ Planning the search and seizure

- ✓ Seeking consent
- ✓ Obtaining witness signatures
- ✓ Obtaining warrant for search and seizure
- ✓ Collecting incident information

☐ Securing and evaluating the crime scene

☐ Initial search of the scene

☐ Seizing evidence at crime scene

- ✓ Dealing with powered-on computers
- ✓ Dealing with powered-off computers
- ✓ Dealing with networked computers
- ✓ Operating System shutdown procedure
- ✓ Dealing with mobiles and other handheld devices




Planning the Search and Seizure


A search and seizure plan should contain the following details:


- | | |
|--|--|
|  Description of the incident |  Creating a chain of custody document |
|  Case name or title of the incident |  Details of equipment to be seized |
|  Location of the incident |  Search and seizure type (overt/covert) |
|  Applicable jurisdiction and relevant legislation |  Approval from local management |
|  Determining the extent of authority to search |  Health and safety precautions |




Evidence Preservation

- 

1 Evidence preservation refers to the proper **handling and documentation** of evidence to ensure that it is **free from any contamination**
- 

2 Any physical and/or digital evidence seized should be **isolated, secured, transported** and preserved to protect its true state
- 

3 At the time of evidence transfer, both the sender and the receiver need to provide information about the **date and time of transfer** in the chain of custody record
- 

4 The procedures used to **protect** the evidence and document it while collecting and shipping are as follows:

 - The logbook of the project
 - A tag to uniquely identify any evidence
 - A chain of custody record

Data Acquisition



Forensic data acquisition is a **process of imaging** or **collecting information** from various media in accordance with certain standards for analyzing its forensic value



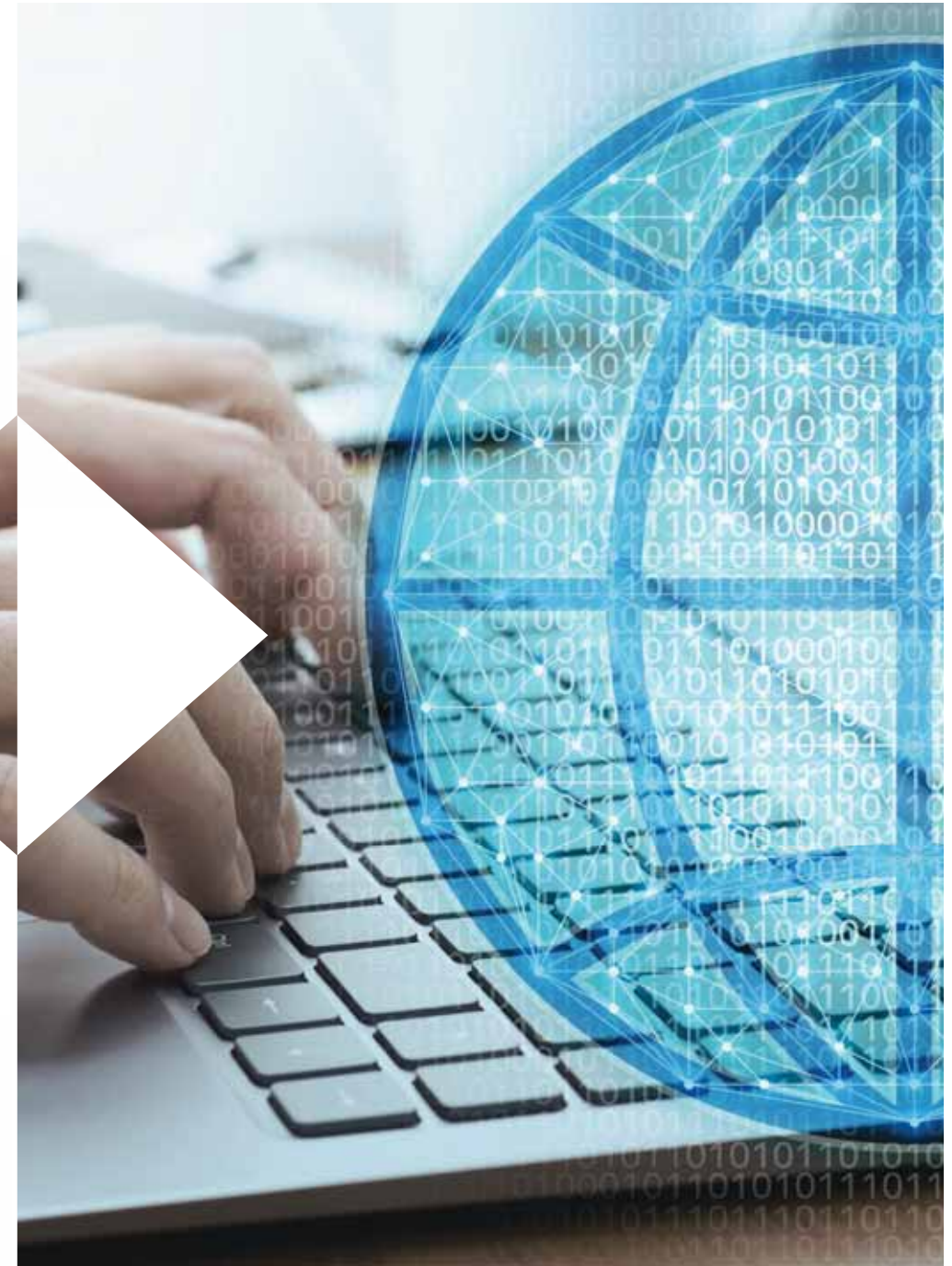
Investigators can then **forensically process** and **examine the collected data** to extract information relevant to any particular case or incident while protecting the integrity of the data



It is one of the most critical steps of digital forensics as **improper acquisition** may alter data in evidence media, and render it inadmissible in the court of law



Investigators should be able to **verify the accuracy of acquired data**, and the complete process should be auditable and acceptable to the court



Data Analysis



- ❑ Data analysis refers to the process of **examining, identifying,** separating, converting, and **modeling data** to isolate useful information

- ❑ Data analysis techniques depend on the **scope of the case** or the **client's requirements**



- ❑ This phase includes the following:

- Analysis of the file's content, date and time of file creation and modification, users associated with file creation, access and file modification, and physical storage location of the file
- Timeline generation
- Identification of the root cause of the incident

Case Analysis



Investigators can relate the evidential data to the case details for understanding how the complete incident took place and determining the future actions such as the following:



Determine the **possibility of exploring** other investigative procedures to gather additional evidence (e.g., checking host data and examining network service logs for any information of evidentiary value, collecting case-specific evidence from social media, identifying remote storage locations etc.)

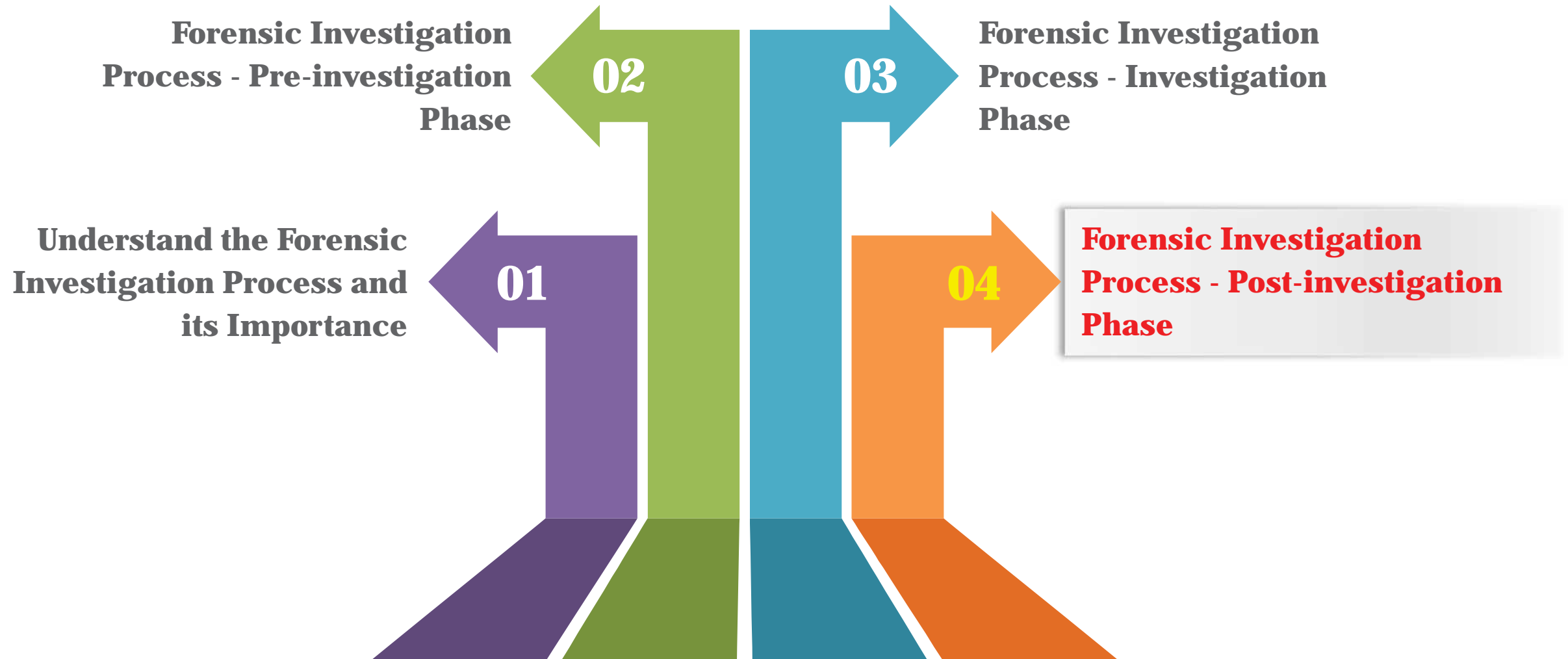


Gather **additional information** related to the case (e.g., aliases, email accounts, ISP used, names, network configuration, system logs, and passwords) by interviewing the respective individuals



Consider the **relevance of components** that are out of the scope of investigation; for example, equipment such as laminators, check paper, scanners, and printers in case of any fraud

Module Flow



Gathering and Organizing Information

Identification

- ❑ Documentation in each phase should be identified to decide whether it is **appropriate to the investigation** and should be organized in specific categories

Procedures



Following are the procedures for gathering and organizing the required documentation:

- Gather all notes from different phases of the investigation process
- **Identify the facts** to be included in the report for supporting the conclusions
- List all the **evidence** to submit with the report
- List the **conclusions** that need to be in the report
- Organize and classify the information gathered to create a concise and accurate report



Writing the Investigation Report



Report writing is a crucial stage in the **outcome of the investigation**



The report should be clear, concise, and written for the **appropriate audience**



Important aspects of a good report:



- ✓ It should accurately define the details of an incident
- ✓ It should **convey all necessary information** in a concise manner
- ✓ It should be technically sound and understandable to the target audience
- ✓ It should be structured in a logical manner so that information can be easily located
- ✓ It should be able to **withstand legal inspection**
- ✓ It should **adhere to local laws** to be admissible in court

Forensics Investigation Report Template

➞ A forensics investigation report template contains the following:

☐ Executive summary

- ✓ Case number
- ✓ Names and Social Security Numbers of authors, investigators, and examiners
- ✓ Purpose of investigation
- ✓ Significant findings
- ✓ Signature analysis

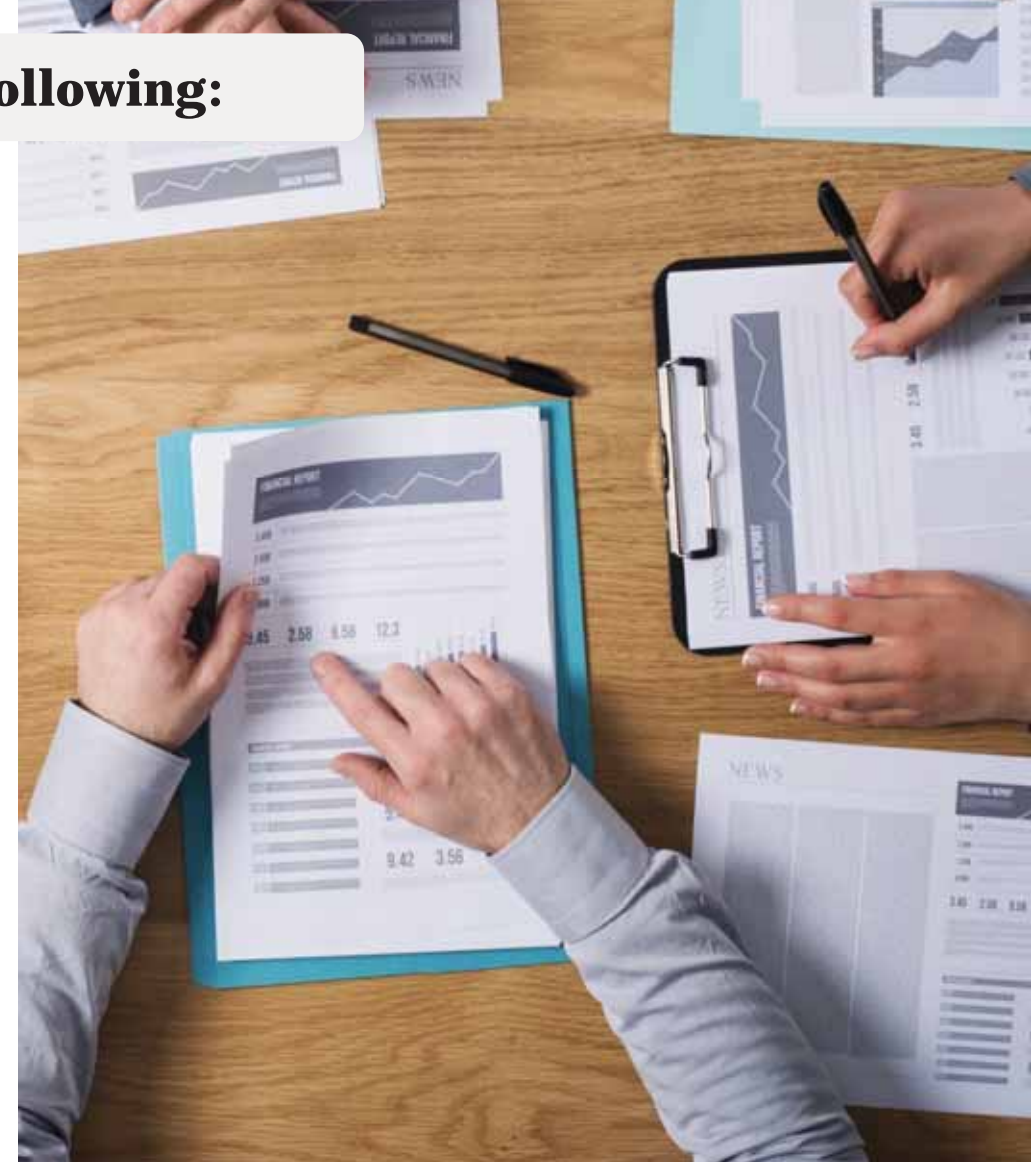
☐ Investigation objectives

☐ Details of the incident

- ✓ Date and time the incident allegedly occurred
- ✓ Date and time the incident was reported to the agency's personnel
- ✓ Details of the person or persons reporting the incident

☐ Investigation process

- ✓ Date and time the investigation was assigned
- ✓ Allotted investigators
- ✓ Nature of the claim and information provided to the investigators



Forensics Investigation Report Template (Cont'd)

❑ Evidence information

- ✓ Location of the evidence
- ✓ List of the collected evidence
- ✓ Tools involved in collecting the evidence
- ✓ Preservation of the evidence

❑ Evaluation and analysis Process

- ✓ Initial evaluation of the evidence
- ✓ Investigative techniques
- ✓ Analysis of the computer evidence (Tools involved)



❑ Relevant findings

❑ Supporting Files

- ✓ Attachments and appendices
- ✓ Full path of the important files
- ✓ Expert reviews and opinion

❑ Other supporting details

- ✓ Attacker's methodology
- ✓ User's applications and Internet activity
- ✓ Recommendations

Testifying as an Expert Witness



Presenting digital evidence in the court requires **knowledge of new, specialized, evolving**, and sometimes complex technology

Things that take place in the court room



Familiarize the expert witness with the **usual procedures** that are followed during a trial



The **attorney** introduces the expert witness



The opposing counsel may try to **discredit** the expert witness



The attorney leads the **expert witness** through the evidence



Later, it is followed by the opposing counsel's **cross-examination**



Module Summary



This module has discussed the forensic investigation process and its importance



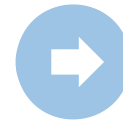
It has covered various activities involved in the pre-investigation phase



It also discussed in detail on activities performed in the investigation phase



Finally, this module ended with a detailed discussion on the post-investigation phase activities



In the next module, we will discuss in detail on understanding hard disks and file systems