Introduction to Digital Forensics

Cybersecurity

Digital Forensics Day 1

Class Objectives

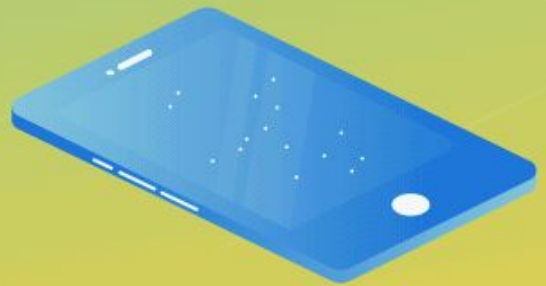
By the end of class, you will be able to:

- Summarize the basic principles and methodologies of digital forensics.
- Describe various skill sets needed in digital forensics jobs.
- Outline the approach to collecting, preserving, analyzing, and reporting forensic evidence.
- Conduct a preliminary review for a forensic case.
- Preserve and document evidence using Autopsy.

In previous units, we covered the extensive skill sets of offensive and defensive security practices.

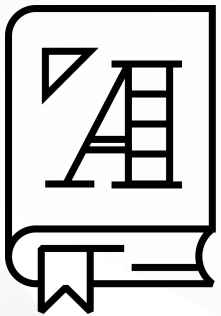
Despite the measures put into place, cybercrime still occurs.

Digital forensics is used to investigate it.



(Source)

Introduction to Digital Forensics



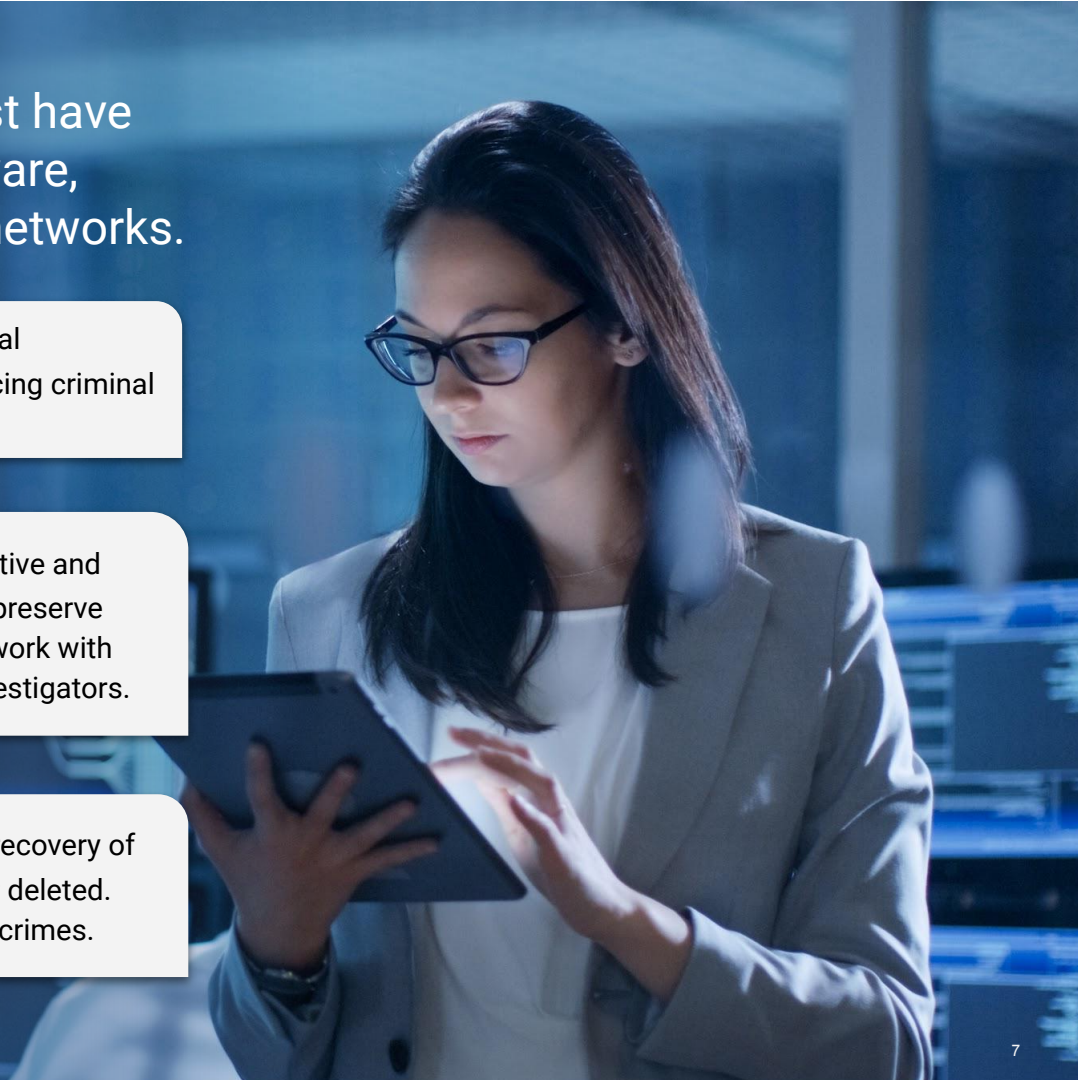
Digital forensics is the process of using scientific procedures to collect, analyze, and present evidence from digital devices, usually in relation to criminal investigations.

Digital forensics professionals must have a thorough understanding of hardware, operating systems, and computer networks.

Computer forensics investigators gather digital information for computer system investigations, producing criminal evidence that can be used in a court of law.

Computer forensics technicians use investigative and computer analysis techniques to acquire, analyze, and preserve digitized evidence to be used for legal purposes. They work with law enforcement, government entities, or as private investigators.

Forensics computer analysts specialize in the recovery of deleted emails or other data that has been encrypted or deleted. This material is used in legal cases involving computer crimes.



Digital Forensics and Legal Requirements

Why is it important to preserve the integrity of digital evidence?

Forensic evidence intended to be used in legal proceedings must satisfy a set of legal standards to be admissible.

To avoid losing months of work searching through computer and network systems and collecting evidence, only to have it considered inadmissible and thrown out due to improper procedures.

Forensic evidence is held to the same standards as any other evidence submitted in a legal case. All evidence must be wholly intact and unaltered from the scene of the crime.

Digital Forensics and the Chain of Custody

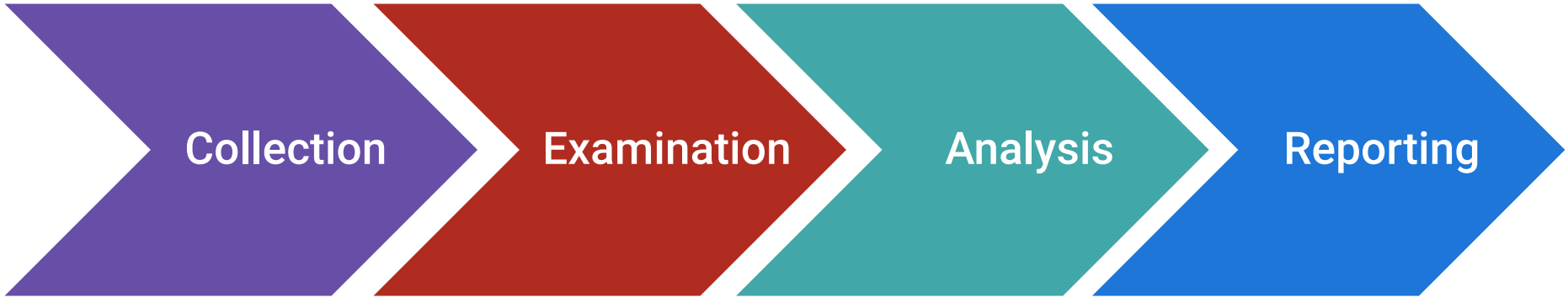
The goal of digital forensics is to present evidence that can be used **in a court of law**.

A **chain of custody** is documentation of possession of evidence that proves integrity and accountability of the investigation by:

- Documenting every step of the investigation.
- Showing uninterrupted control.
- Ensuring evidence is not tampered with or contaminated.

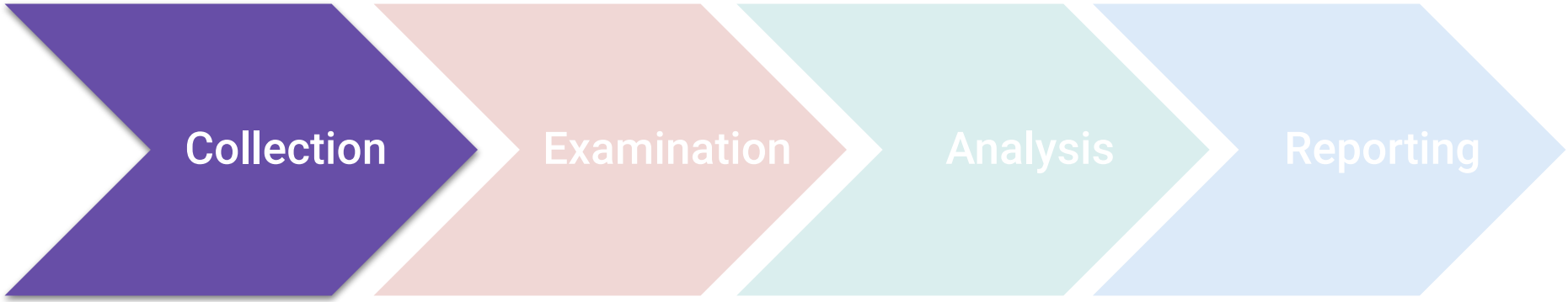
The Digital Forensic Process

The National Institute of Standards and Technology defines a process for performing digital forensics in Special Publication 800-86:



The Digital Forensic Process

The National Institute of Standards and Technology defines a process for performing digital forensics in Special Publication 800-86:



We must first collect the data before we can examine and analyze it.

The collection phase is the springboard to the digital forensics process. It includes identifying, labeling, recording, and acquiring data from sources while following procedures to preserve the integrity of the data.

The Digital Forensic Process

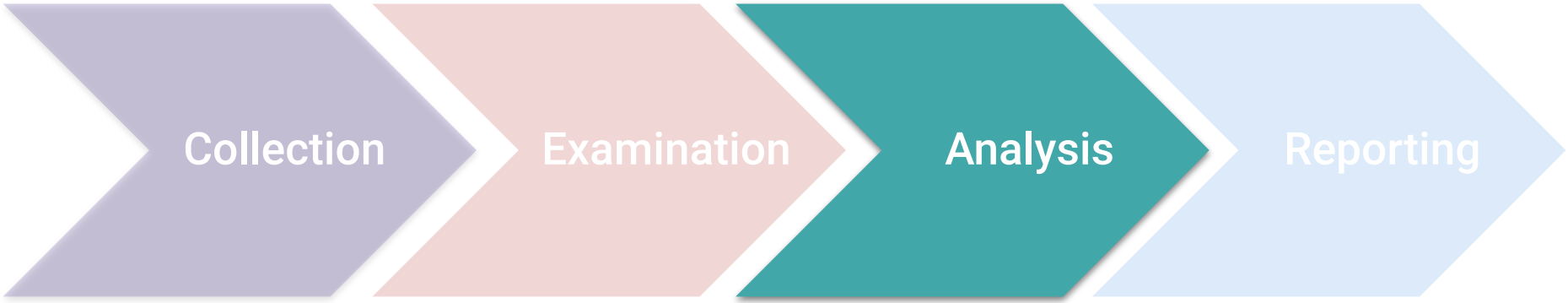
The National Institute of Standards and Technology defines a process for performing digital forensics in Special Publication 800-86:

The examination phase ensures that all data collected is relevant to the case.

This includes forensically processing collected data and assessing and extracting data of interest while preserving the integrity of the data. This usually means working from a copy, not the original.

The Digital Forensic Process

The National Institute of Standards and Technology defines a process for performing digital forensics in Special Publication 800-86:

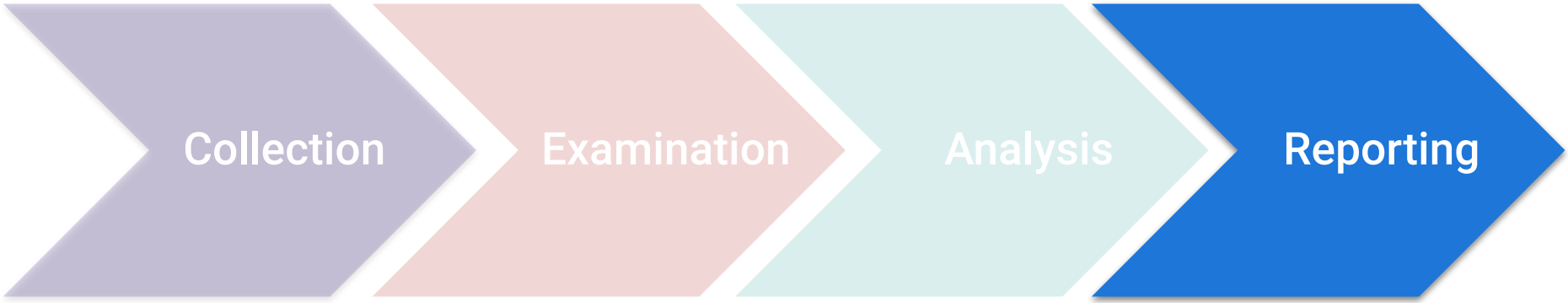


The analysis phase analyzes the results of the examination.

Analysis uses legally approved methods and techniques to derive information that addresses the questions that inspired the collection and examination of the data.

The Digital Forensic Process

The National Institute of Standards and Technology defines a process for performing digital forensics in Special Publication 800-86:



Investigators are required to formally report results of the analysis.

This may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed, and recommending improvements to the forensic process.

Evidence Collection

Digital forensics data has one of two classifications:

Network-based Data

Comes from data communications captured by network-based systems such as IDS, IPS, and firewalls, in the form of a packet capture or similar.

- Packet captures are useful for reconstructing events involving computer break-ins.
- Logs from firewalls also provide insight into network activity.

Host-based Data

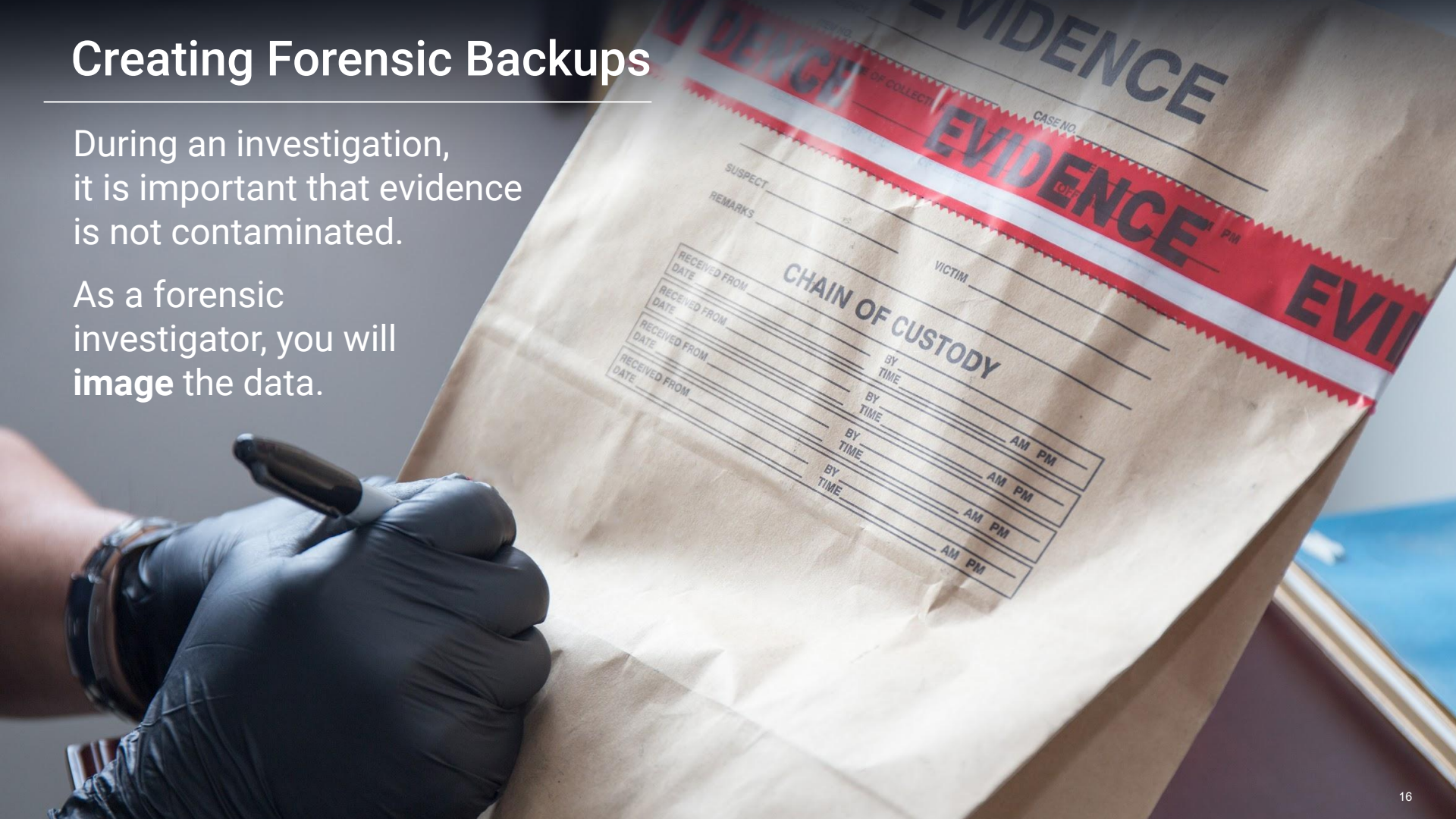
Typically found on a system that has a wide variety of artifacts.

- Investigations involving computer break-ins may involve the forensic examination of local file systems, programs, access to critical documents, and/or alterations to system files and directories.
- Host-based examinations may involve reconstructing internet use, unauthorized activity, email recovery, and the identification of malicious files.

Creating Forensic Backups

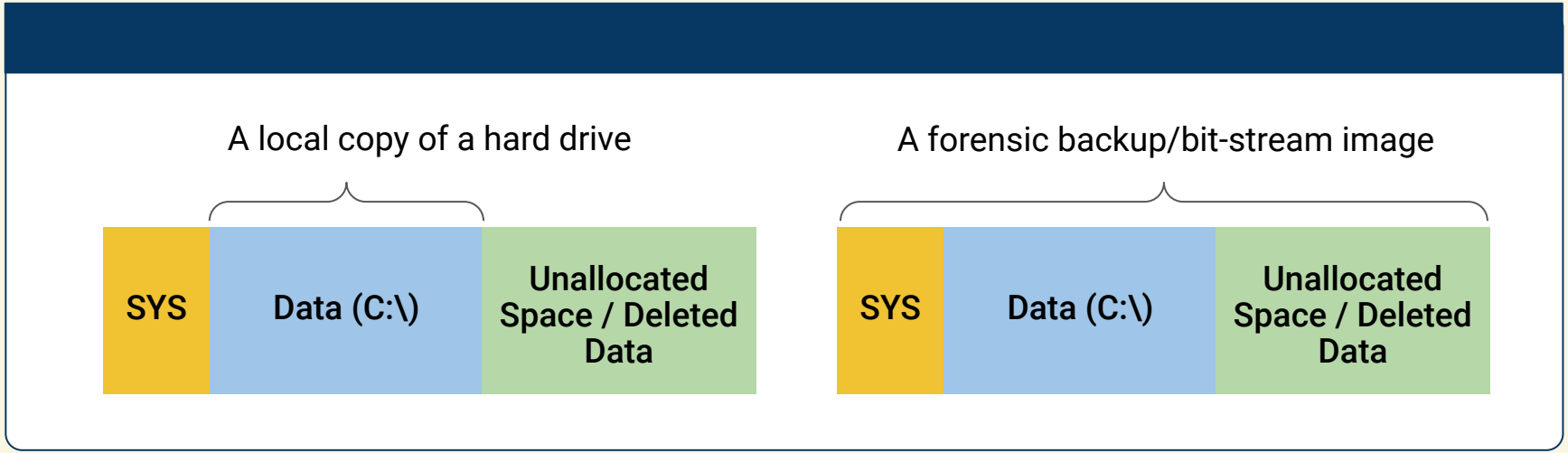
During an investigation, it is important that evidence is not contaminated.

As a forensic investigator, you will **image** the data.



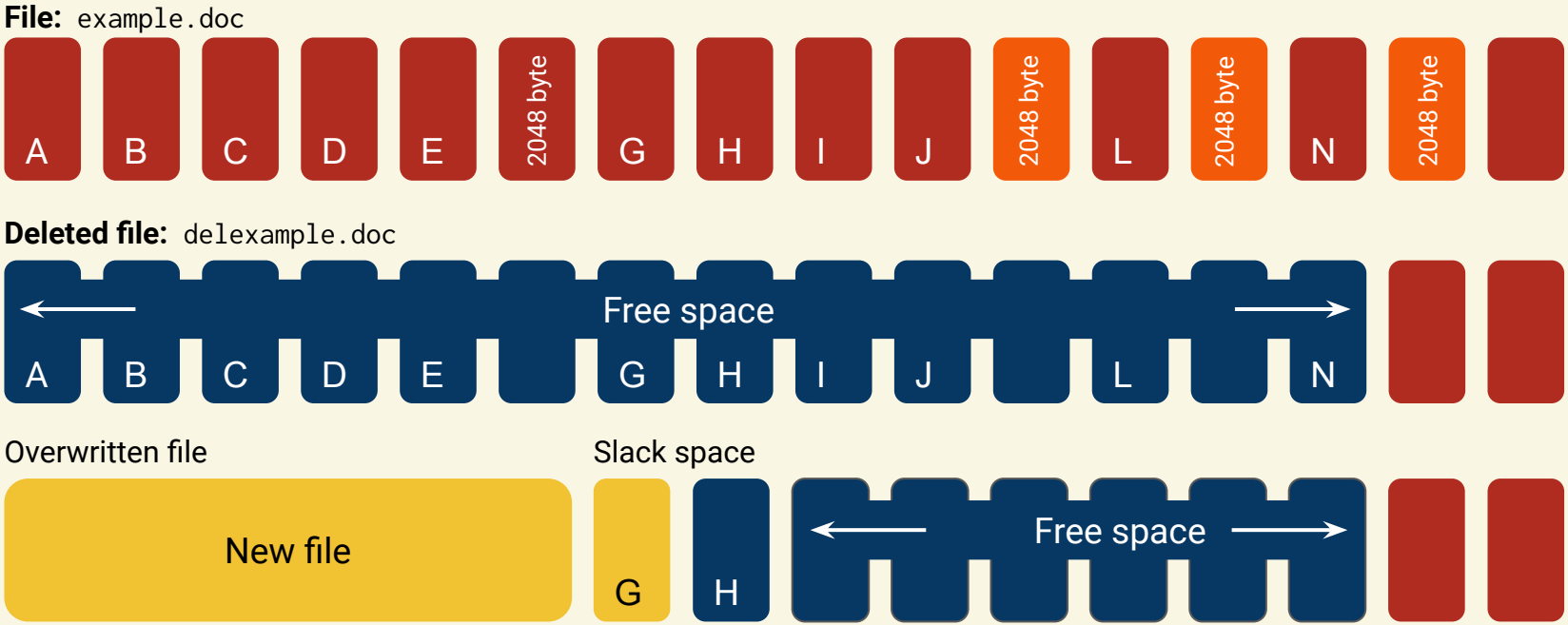
Creating Forensic Backups

A **bit-stream image** captures all created sections of a hard drive (partitions), whether used or not, and all unallocated drive space that doesn't belong to partitions. This method allows forensic examiners to recover deleted files and fragments of data that may exist on the hard drive.



Creating Forensic Backups

A **local file system** copy is inadequate for forensic analysis. If you make a copy through the file or operating system level, you can access only the data that the operating system can access. This won't capture deleted files or slack space. Therefore, you need to obtain a **bit-level copy.**



Forensic Disk Image Formats

Forensic backups (system image or bit-stream image) create an exact replica of all contents on the hard drive, including slack space, free space, and deleted files.

Forensic backup images are created in the following formats:

Raw Format	Advanced Forensic Format (AFF)
Created with programs like `dd`, `ddfldd`, and `ddcdd`.	For disk image and related forensic metadata.
Examples: .bin .dd .img .raw	**Examples:** .AFF .AFF4

Working with Live Systems

Always use caution when working with live systems. It is possible that an attacker is waiting for the user to log back in before completing an attack.

The primary reason for working on a live system is to capture items that will not survive a power loss, such as volatile memory, swap files, running processes, and active network connections.

Mistakes such as writing data to memory or disk can potentially destroy evidence. This is why it is critical to use forensic tools like write blockers.

A **write blocker** is a device that allows anything connected to it to only perform read operations. This prevents the drive from being written to and evidence from being overwritten.

File Systems

During an investigation, you might encounter these file systems:

- **New Technology File System (NTFS)**, supported by Windows 10, 8, 7, Vista, XP, and NT.
- **File Allocation System (FAT)**, supported by older and newer versions of Windows.
- **Apple File System (AFS)**, used by the macOS system.
- **Fourth Extended File System (Ext4)**, used in RedHat, Kali, and Ubuntu.

Overview of Storage Media

To extract valuable resources and information from devices, digital forensics experts need to have broad knowledge of various storage media.

Mechanical Hard Drives

Mechanical hard drives have...

...far larger storage capacities than other types of drives. This means the imaging process can take a very long time when performing a bit-level copy.

...very delicate moving parts that can be damaged if not handled properly.

FORENSIC IMPLICATION

You can recover data from badly damaged devices, as long as you have the required knowledge of mechanical hard drives.

A Closer Review of Storage Media

Flash Storage

Flash storage devices have no moving parts and use flash memory, allowing for quicker read and write access.

Solid State Drives (SSD)

SSD storage devices use flash memory chips and have no moving parts. They also have larger storage capacity and faster read–write access.

SD/MicroSD Cards

SD cards store data inside a flash memory chip, similar to solid-state devices.

FORENSIC IMPLICATIONS

Flash memory or flash storage is non-volatile, meaning it holds data even when disconnected from power.

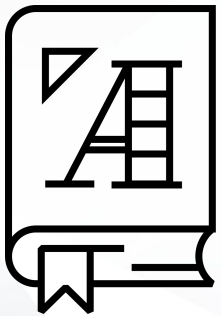
It's used in devices such as USB drives, mobile phones, cameras, and tablet computers.

SSD data can be lost or wiped out in seconds, so investigators must be careful when using forensic tools to image and recover data.

It is possible to retrieve SD card data even if it has been deleted or the disk has been formatted. Rather than being erased, data is set aside for reuse.

It's used in cell phones and smartphones.


During collection, we may encounter password-protected storage media and firmware.



Firmware is a specific class of computer software that provides the low-level control for a device's specific hardware.

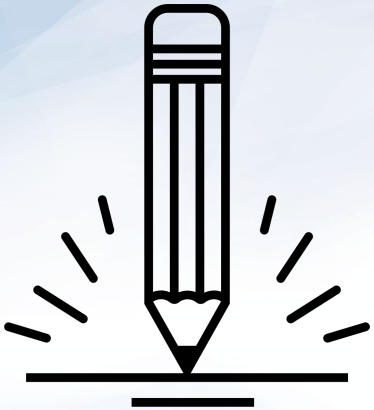
These situations present extreme challenges to forensic investigators and must be considered during the initial stages of the investigation.

Working With Cloud-Based Evidence

Working with online evidence such as hard drives and volatile memory located on cloud-based hardware presents a whole new set of challenges.

We'll explore these challenges in the next activity.

(Source)



Activity: Digital Forensics in the Cloud

In this activity, you will read about a case concerning a denial of service (DoS) attack at a shopping website, analyze the challenges for investigators, and recommend how to validate a chain of custody in cloud forensics cases.

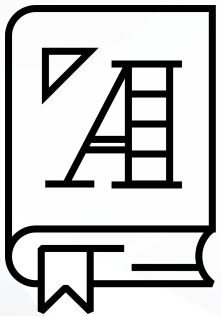
Suggested Time:
20 minutes

Time’s Up! Let’s Review.

Digital Forensics Types

In addition to cloud-based forensics, digital forensics is a continuously evolving scientific field that incorporates many subdisciplines.

- Computer forensics
- Disk forensics
- Memory forensics
- Network forensics
- Email forensics
- Mobile device forensics



Computer forensics is the identification, preservation, collection, analysis, and reporting of evidence acquired from computers, notebooks, and storage media.

It is used to support investigations and legal proceedings.

Computer Forensics

Computer forensics subtopics include:

Disk Forensics

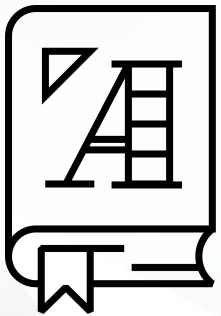
This involves acquiring and analyzing information stored on physical storage media, such as hard drives, smartphones, GPS systems, and removable media.

It includes the recovery process of hidden data, deleted data, and slack space information.

Memory Forensics

This inspects computer memory to identify an attacker's activities on a system.

This area requires the broadest skill set, including knowledge of CPU architectures, operating systems and memory management, page tables, and virtual addressing, among other things.

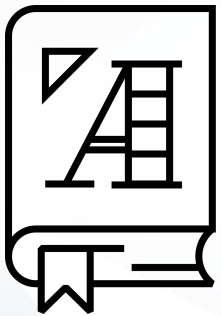


Network forensics is the monitoring, recording, storing, and analysis of all network traffic to determine the source of security events.

Network Forensics

Network forensics tools include Wireshark, NetworkMiner, and Snort, among others.

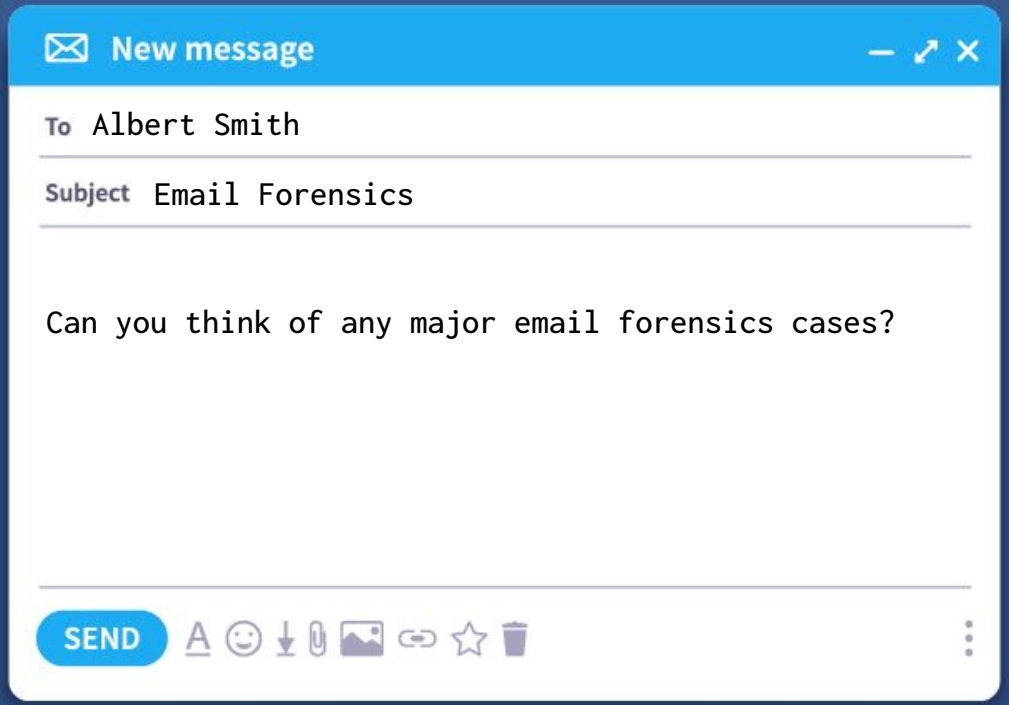
Investigators in this area must have an excellent understanding of communication and network protocols, and the tools needed to capture and analyze data.



Email forensics analyzes the source and content of an email as evidence.

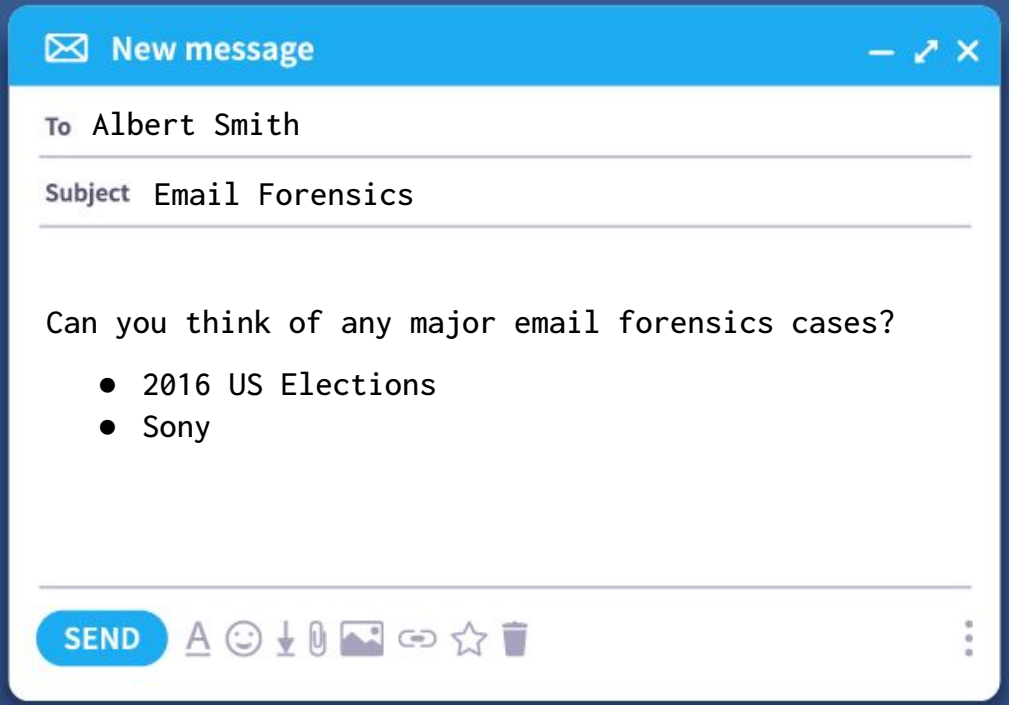
Email Forensics

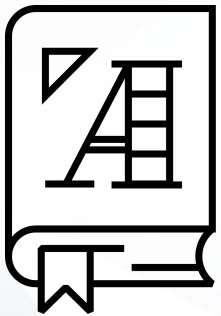
Email forensics includes the process of identifying the sender, recipient, date, time, and original location of an email.



Email Forensics

Email forensics includes the process of identifying the sender, recipient, date, time, and original location of an email.





Mobile device forensics is the recovery of digital evidence from smartphones, GPS devices, SIM cards, PDAs, tablets, and game consoles.

Mobile Device Forensics

For example:

- Cell phone forensics might be used in a distracted driving case.
- A forensic expert could analyze what was happening at the time of the accident.

Methodology for Conducting an Investigation

Now that we understand the importance of maintaining an accurate chain of custody, we will explore the methodology for conducting digital forensic investigations.

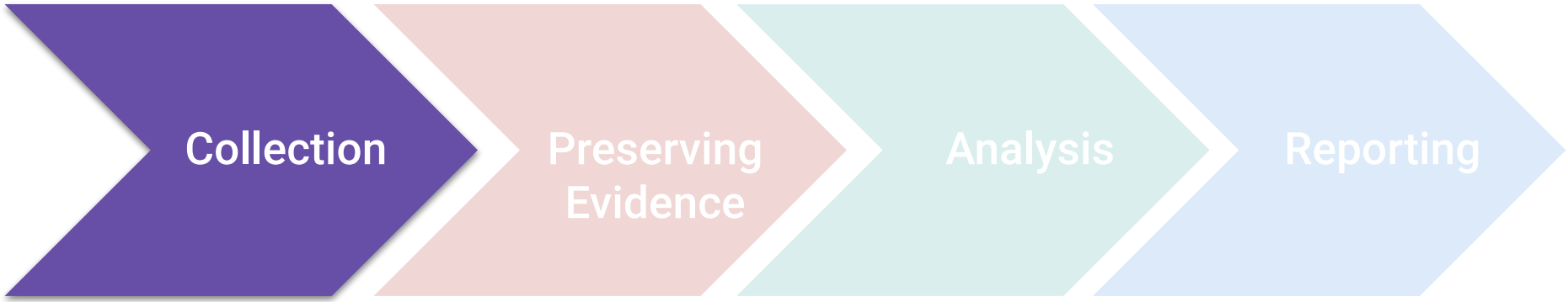
Investigation Methodology

The **National Institute of Standards and Technology** provides one of many frameworks for forensic investigation phases.

Collecting Evidence

The success of the investigation relies on the collection phase.

- During this phase, an investigator makes decisions about what data to collect and the best way to collect it.
- Evidence is extracted from a device and a master copy is made.
- **How** you collect the evidence determines whether it will be **admissible in court**.



Preserving Evidence

Investigators never work with the original copy of evidence.

- Instead, a **read-only master copy** is made and stored in a digital vault. All processes are worked on the copy.
- A **cryptographic digest** is made to ensure that evidence has not been altered in any way.

Electronic Discovery and Analysis

Analysis is completed after data is collected.

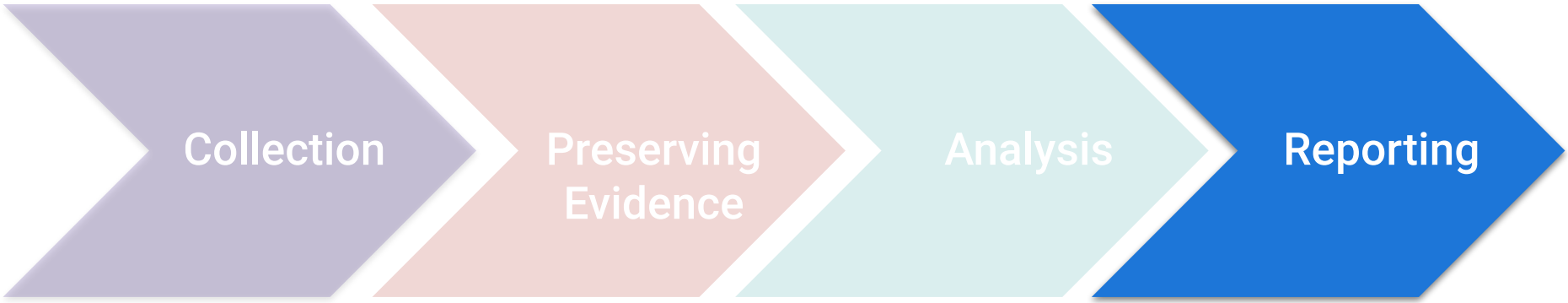
- This process is also known as **dead analysis**.
- Investigators document everything, including time, dates, applications used, etc.
- If evidence cannot be reproduced, it may be ruled as inadmissible in court.

Presenting and Reporting

Investigators write an expert report that explains:

- What tests were conducted.
- When, how, and what was found.
- The conclusions of the investigation.

Digital forensics analysts may testify as expert witnesses in a trial or deposition.



2012 National Gallery Case

Over the next two classes, we will use a case scenario to go through some of the most important tools and concepts of digital forensics.

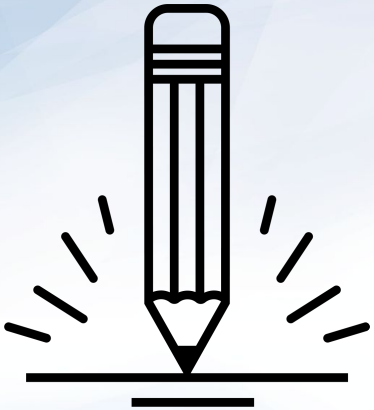
The 2012 National Gallery Case

The case involves an art theft and defacement at the National Gallery in Washington D.C.

Law enforcement seized electronic devices from an employee after suspicious activity was reported.

The evidence was processed by the Crime Laboratory ingest team and backed up using Encase.

This scenario was created by the U.S. Naval Postgraduate School and the U.S. Military Academy at West Point for educational purposes.



Activity: 2012 National Gallery Case

In this activity, you will act as forensic investigators beginning an investigation of the 2012 National Gallery Case.

Suggested Time:
15 Minutes

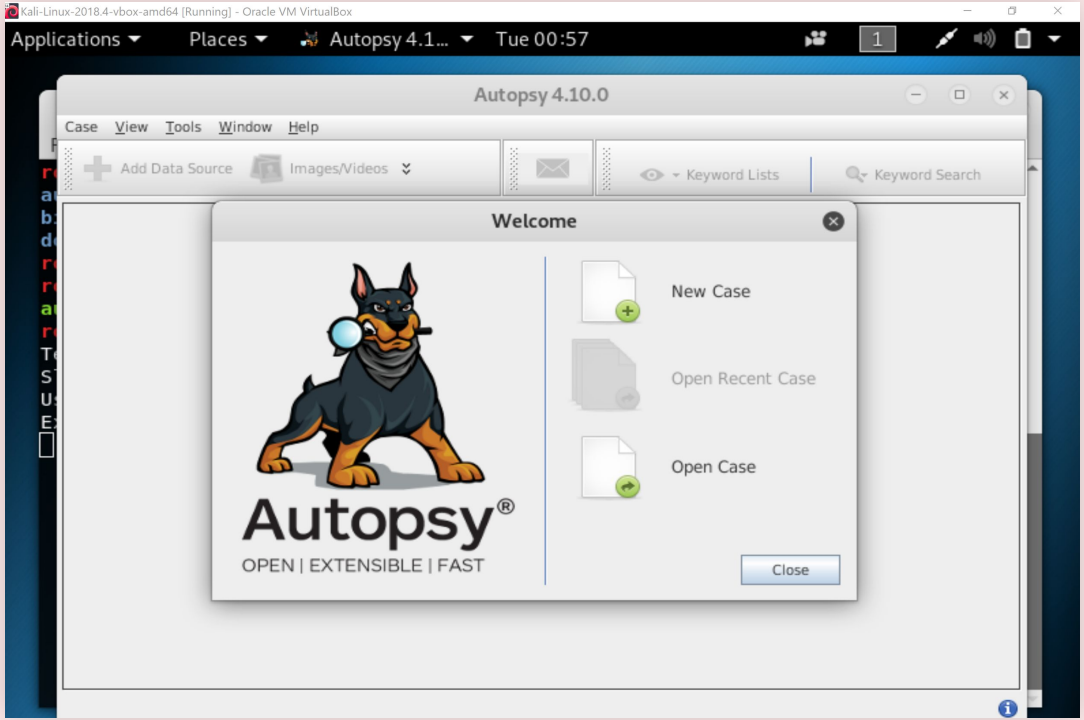
Time’s Up! Let’s Review.

Introduction to Autopsy

Now we'll explore the software used to analyze the image file.

Autopsy | Digital Forensics

We will use **Autopsy**, an open-source graphical tool from Sleuth Kit that runs on Windows, Ubuntu, Kali, and OS X.



Autopsy

First we'll prepare the data by:

01 Running a virus scan on the image.

02 Generating an MD5 and SHA-256 hash for the evidence. This is to validate that nothing was changed during the investigation.

03 Opening a terminal window in Kali and navigating to the `Evidence` directory.

- Run `md5sum tracy-phone-2012-07-15.final.E01 > tracy.original.md5log.txt`
- Run `sha256sum tracy-phone-2012-07-15.final.E01 > tracy.original.sha256log.txt`

The Autopsy Workflow

01 **Create a case:** Add case name, investigator information, and optional info.

02 **Add an image:** Autopsy supports Raw, Encase, and Virtual Disk image formats.

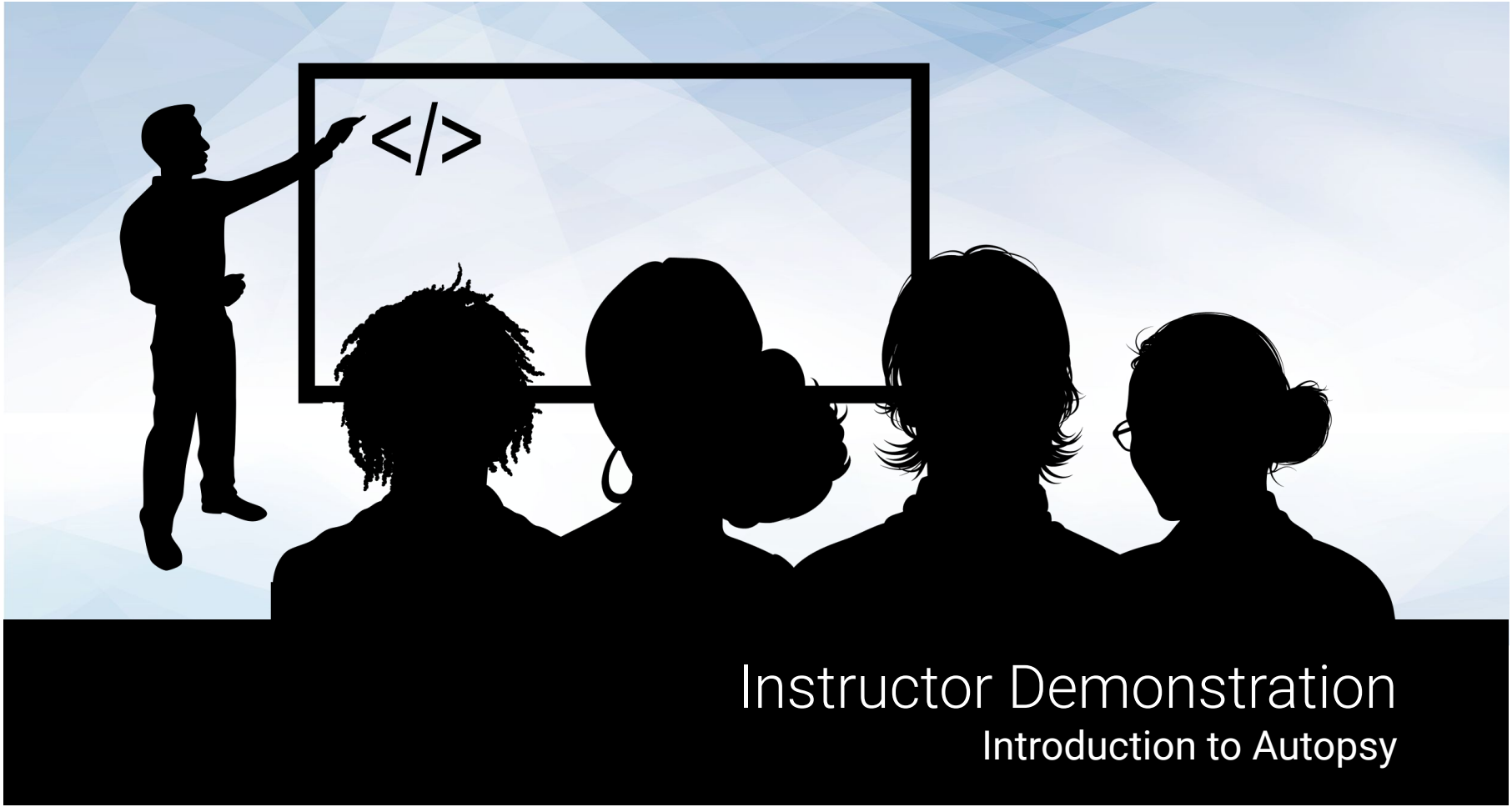
03 **Configure ingest module:** Modules label and categorize evidence during the file ingestion process.

04 **Ingest in process:** Process of loading the .E01 file into Autopsy. This takes some time.

05 **Manual analysis:** Research the system for relevant information and analyze the data.

06 **Create timeline:** Determine times, data, and data sources.

07 **Report:** Consolidate evidence into a single document. Format is HTML or Excel.



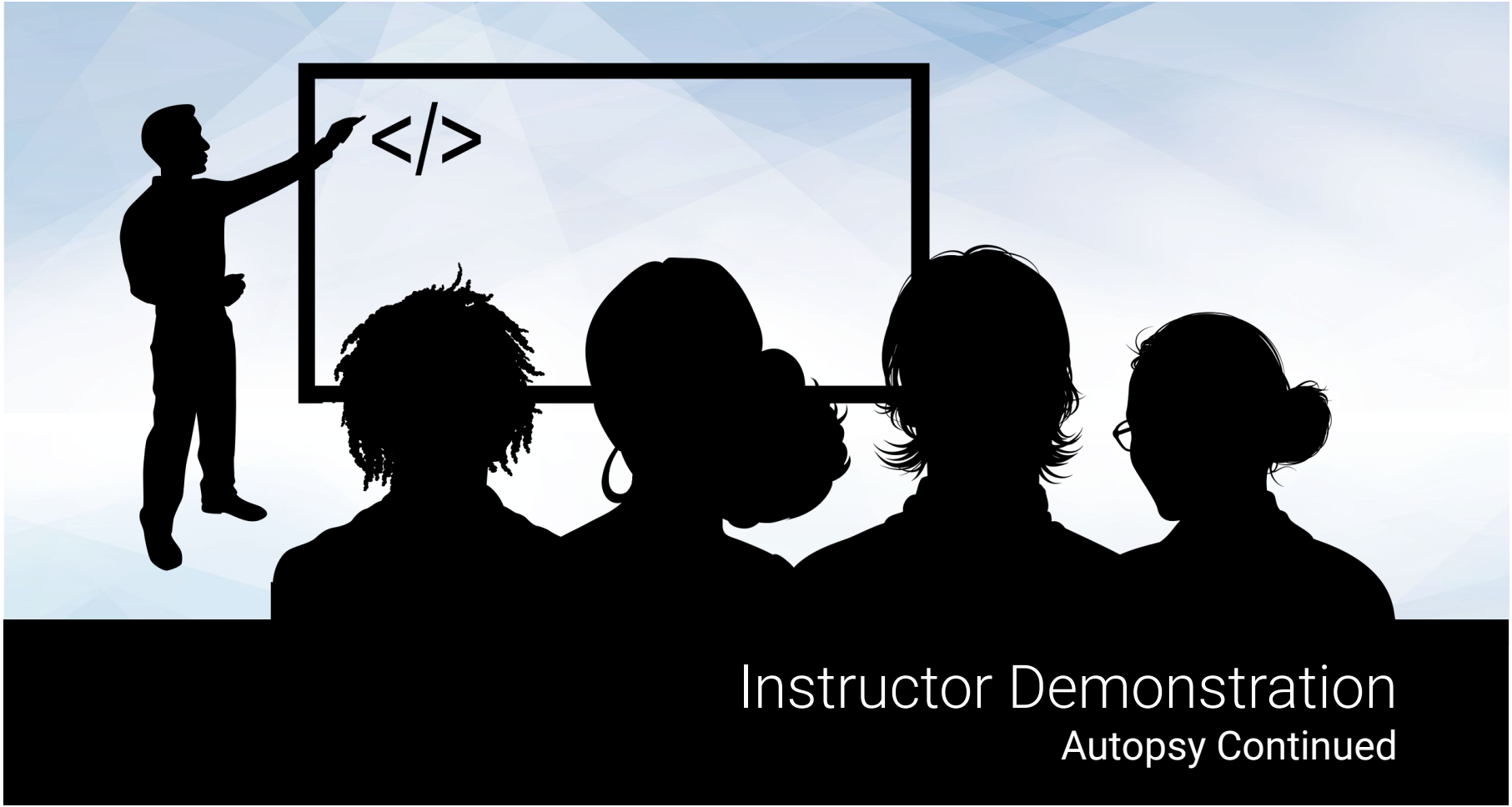
Instructor Demonstration

Introduction to Autopsy

(As Autopsy analyzes the files.)

Now we'll pick back up at

Step 5: Manual Analysis with Keyword Search



Instructor Demonstration

Autopsy Continued

Autopsy Review

In our first Autopsy investigation, we completed the following steps:

- Generated MD5 and SHA-256 hashes to ensure the integrity of the evidence.
- Specified a case name and number to help keep track of files and progress.
- Selected the file type to be ingested (.E01) and specified a working directory to save progress.
- Specified the time zones as a standard point of reference for the case.
- Configured ingest modules to help categorize, label, and organize data.
- Set up our central SQLite database repository to allow us to review SMS messages.
- Accessed the encrypted `documents.zip` file by expanding its directory tree for further analysis.

Questions?


The End