Introduction to Digital Forensics

Cybersecurity

Digital Forensics, Day 1

Class Objectives

By the end of class today, students will be able to:

□ Summarize the basic principles and methodologies of digital forensics.

□ Describe various types of jobs and skill sets needed for digital

□ forensics.

□ Outline the proper way to collect, preserve, analyze, and report.

□ Demonstrate how to conduct a preliminary review of a forensics case.

- Demonstrate preserving and documenting evidence using Autopsy 4.0.

Introduction to Digital Forensics

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

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** assures integrity and accountability of the investigation by

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

Defense attorneys will look for mistakes in the chain of custody form to render the evidence inadmissible.

National Initiative for Cybersecurity Education (NICE)

Explore the NICE site and check out some jobs for these various speciality areas:

1 Analyze

Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

2 Collect and Operate

Provides specialized denial and deception operations and collection of cyber information used to develop intelligence.

3 Investigate

Investigates cybersecurity events or crimes related to IT systems, networks, and digital evidence.

4 Operate and Maintain

Provides support, administration, and maintenance to ensure effective and efficient IT system performance and security.

5 Oversee and Govern

Provides leadership, management, direction, or development advocacy so the organization can effectively operate.

6 Protect and Defend

Identifies, analyzes, and mitigates threats to internal IT systems and networks.

7 Securely Provision

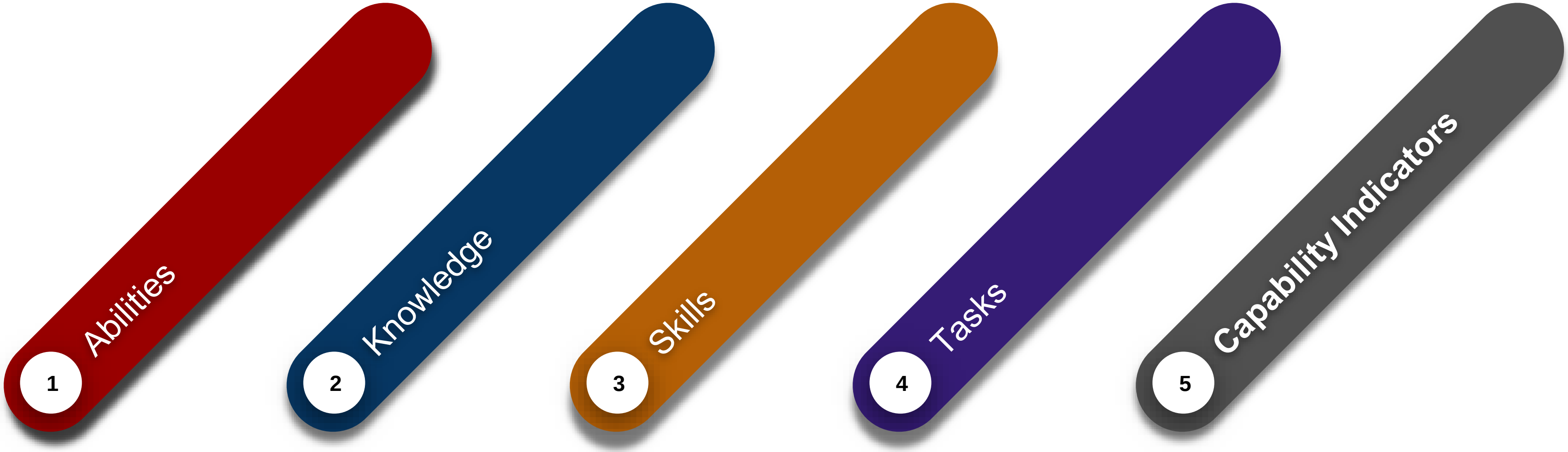
Conceptualizes, designs, procures, and builds secure IT systems with responsibility for aspects of systems and network development.

Source: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

National Initiative for Cybersecurity Careers and Studies (NICCS)

THe NICCS site provides resources for determining the knowledge, skills, and abilities (KSAs) of digital forensics positions

Check out some of the KSAs for Cyber Defense Forensics Analysts on the NICCS page:



1 Abilities

2 Knowledge

3 Skills

4 Tasks

5 Capability Indicators

Source: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/digital-forensics

Digital Forensics Types

Types of Digital Forensics

Type	Skills/Knowledge	More Info / Examples
Disk forensics involves acquiring and analyzing information on physical storage media.	Requires extensive knowledge of hardware's inner workings and the operations of hard drives.	Works with hard drives, smart phones, GPS systems, and removable media.
Memory forensics inspects a computer's memory to identify activities on a system.	High skill set: You must have knowledge of CPU architectures, operating systems and memory management, page tables and virtual addressing	An attacker will attempt to leave as little evidence on storage media as possible. Your goal is to find that evidence.
Network forensics examines network traffic.	Excellent understanding of communication and network protocols and the tools needed to capture and analyze data.	Works with transaction logs and real-time monitoring.
Email forensics analyzes the source and content of emails.	Identify the sender, recipient, date, time, and origination location of an email.	*Can you think of an email forensics case that consumed the headlines a few years ago?*
Mobile forensics captures and analyzes the contents of cell phones and smartphones.	Knowledge of mobile device hardware; ability to analyze what is happening on a phone at the time of an incident.	In distracted driving cases, forensics experts can determine what happened at the time of the accident. *Don't text and drive!*

Forensics Types

There are many other forensics areas, such as:

- Software
- Internet
- Malware
- Drone
- Cloud forensics, which poses unique challenges. (see the next activity)

Activity: Digital Forensics in the Cloud

In this activity, you will read about a case concerning a Denial of Service Attack (DoS) at a shopping website.

Then you will compare cloud forensics to other forensic areas and provide two examples of how to maintain a chain of custody in the cloud.

Activities/Stu_Cloud_Forensics

Suggested Time:
20 minutes

Review: Digital Forensics in the Cloud

List at least four components that make digital forensics in the cloud different than other forensics areas:

Review: Digital Forensics in the Cloud

List at least four components that make digital forensics in the cloud different than other forensics areas:

- There is no physical access to the computer where the crime took place.
- If the crime takes place on a cloud server, a malicious user can claim that everyone in the world with internet access should be a suspect.
- When the crime takes place on a cloud server, it's difficult to pinpoint where their data ends and where another company, that police do not have a warrant for, begins.

Review: Digital Forensics in the Cloud

List at least four components that make digital forensics in the cloud different than other forensics areas:

- Because many people will often use the same cloud server, there are SLA's that have to be recognized when dealing with other companies.
- Volatile memory, such as RAM, would be lost if the cloud server is rebooted.
- It would be difficult to trace which cloud server is storing the users data.

Review: Digital Forensics in the Cloud

How do these differences affect the chain of custody?

Review: Digital Forensics in the Cloud

How do these differences affect the chain of custody?

- It is difficult to pinpoint where and which cloud server has been compromised.
- This would also present the problem of the cloud server being in another county’s jurisdiction.

Review: Digital Forensics in the Cloud

Challenges of Maintaining a Chain of Custody in Cloud Forensics

No Physical Access

- The exact location of where the data may not be known.

Preserving the evidence

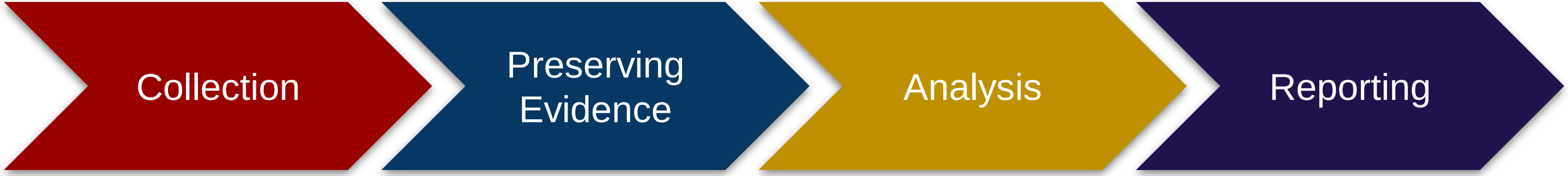
- Isolating and securing the evidence is challenging when data is located in multiple locations.

Data Integrity

- Evidence may be captures live and the evidence can be altered if not collected correctly.

Methodology for Conducting an Investigation

Investigation Methodology


Collection

Preserving Evidence

Analysis

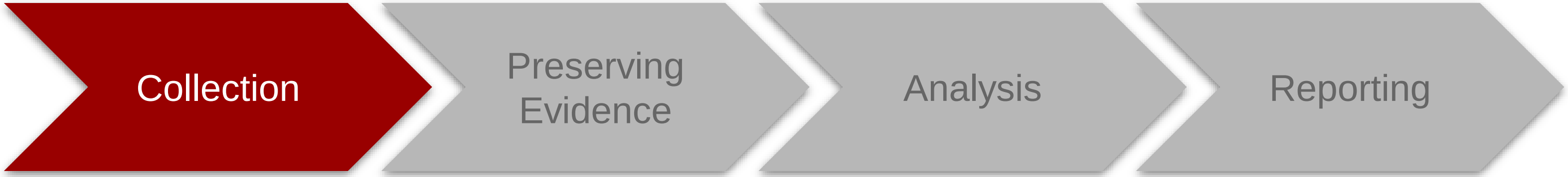
Reporting

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

In preparation, an investigator needs to consider:

- Is this incident remote or local?
- What laws are relevant?
- What tools should be used (GUI or CLI)?

Collecting Evidence



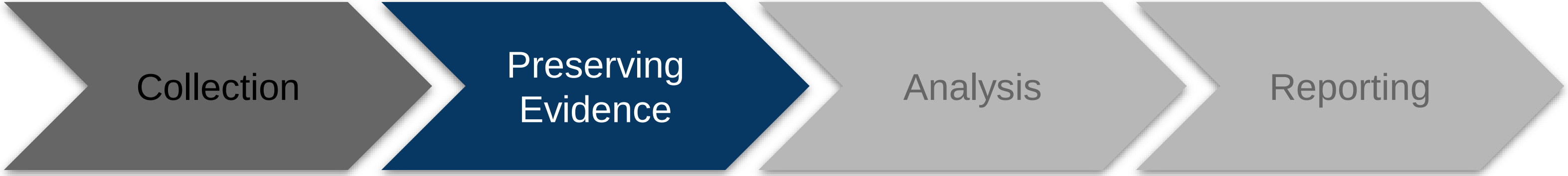
The success of the investigation relies on the collection phase.

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

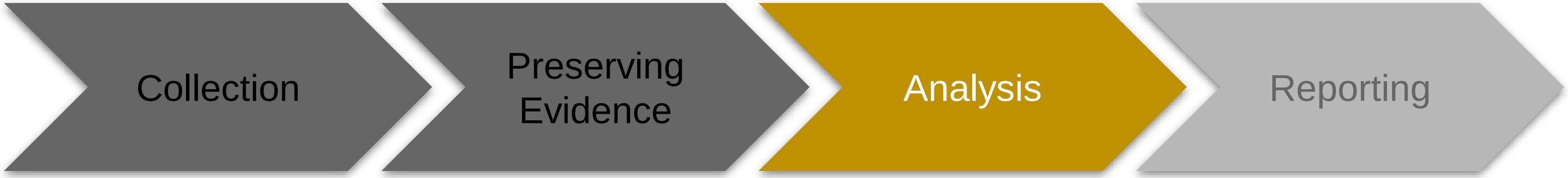


Investigators never work with the original copy of evidence.

Instead, a **read-only master copy** is made and stored in a digital vault. Then, all the 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

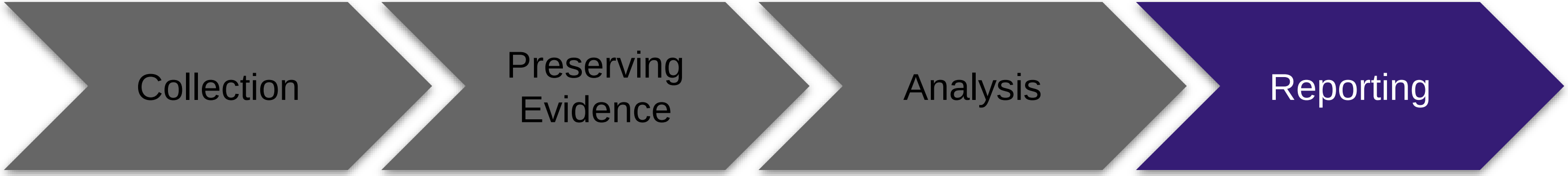


Analysis is completed after data is collected. This process is also known as **dead analysis**.

Investigators document everything, including time, dates, applications used, etc.

If your 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

The 2012 National Gallery Case

Over the next two days, we’ll work on a real-life 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.

Activity: 2012 Nat’l Gallery Case

In this activity, you will be acting as novice investigators working for the *We-Carve-4-U* digital forensics company. Your supervisor has given you a training case to prepare for field work. The seized evidence has been processed by the ingest team at the Crime Laboratory.

Activities/Stu_CaseScenario

Suggested Time:
20 minutes

2012 National Gallery Case Review

What is the case?

Who are the suspects?

What evidence was confiscated?

What could be admissible as evidence.

National Gallery Case Evidence

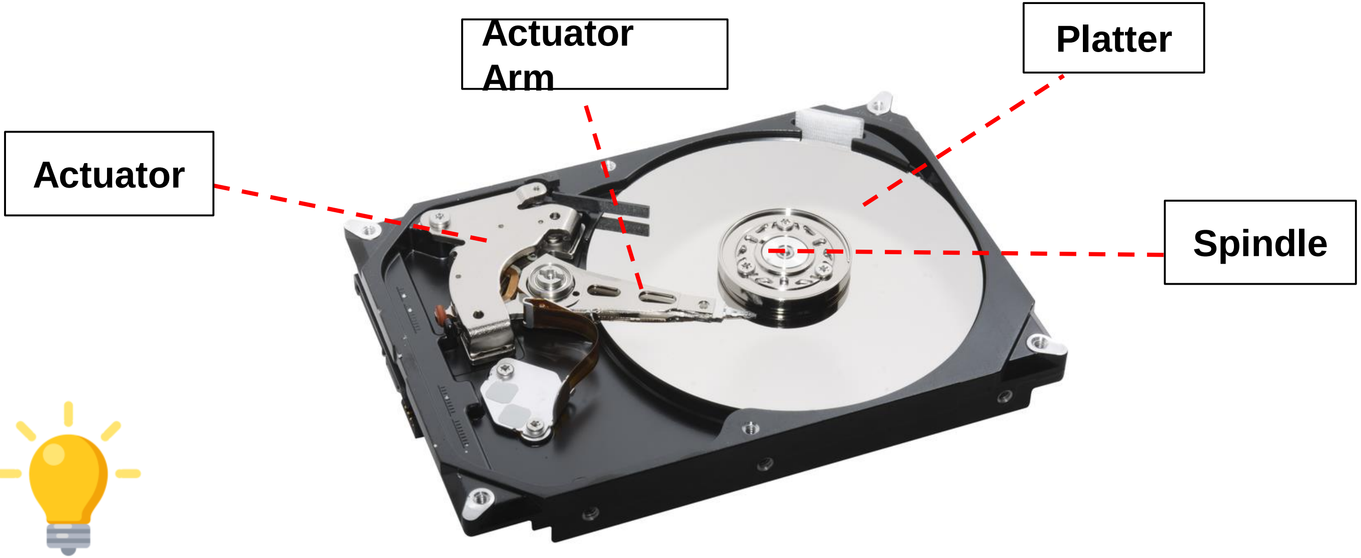
Storage Media Overview

The various storage devices you'll encounter hold content such as operating and file system data, applications, documents, pictures, videos, and music.

	Optical devices such as CD ROMS, DVDs, and Blu-Ray are used for mobile storage. They hold from 700 MB to 50 GB of data.
	Hard Disk Drives (HDD) are used in computer devices and store up to 16 terabytes of data.
	Solid State Drives (SSD) can store up to 16 terabytes of data.
	SD cards are used in smartphones like Android and store up to 521 GB of data.

Hard Drives

Hard drives are made up of an actuator, an actuator arm, a platter, and a spindle.



Data is read and written by the actuator arm and attached head moving over the spinning platter.

Data is stored in a series of concentric circles called tracks, which are then divided into sectors.

Information about free and used sectors are stored in the file allocation table (FAT).

Implication for forensics: A solid knowledge of the inner workings of hard drives lets you recover data from badly damaged devices.

A Closer Look at Storage Media

Flash Storage Memory

Hard drives are limited by the speed at which they send and receive information.

Flash storage devices use flash memory to quickly access data.

Holds data without external power source .

Non-volatile storage found in USB drives, mobile phones, cameras, and tablets.

Solid State Drives (SSD)

Use flash memory chips.

Not a mechanical device.

Forensic Implication:

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

SD / MicroSD Cards

SD cards store data in a flash memory chip similar to solid state devices.

Used in cell phones and smartphones.

Forensic Implication:

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.

File Systems

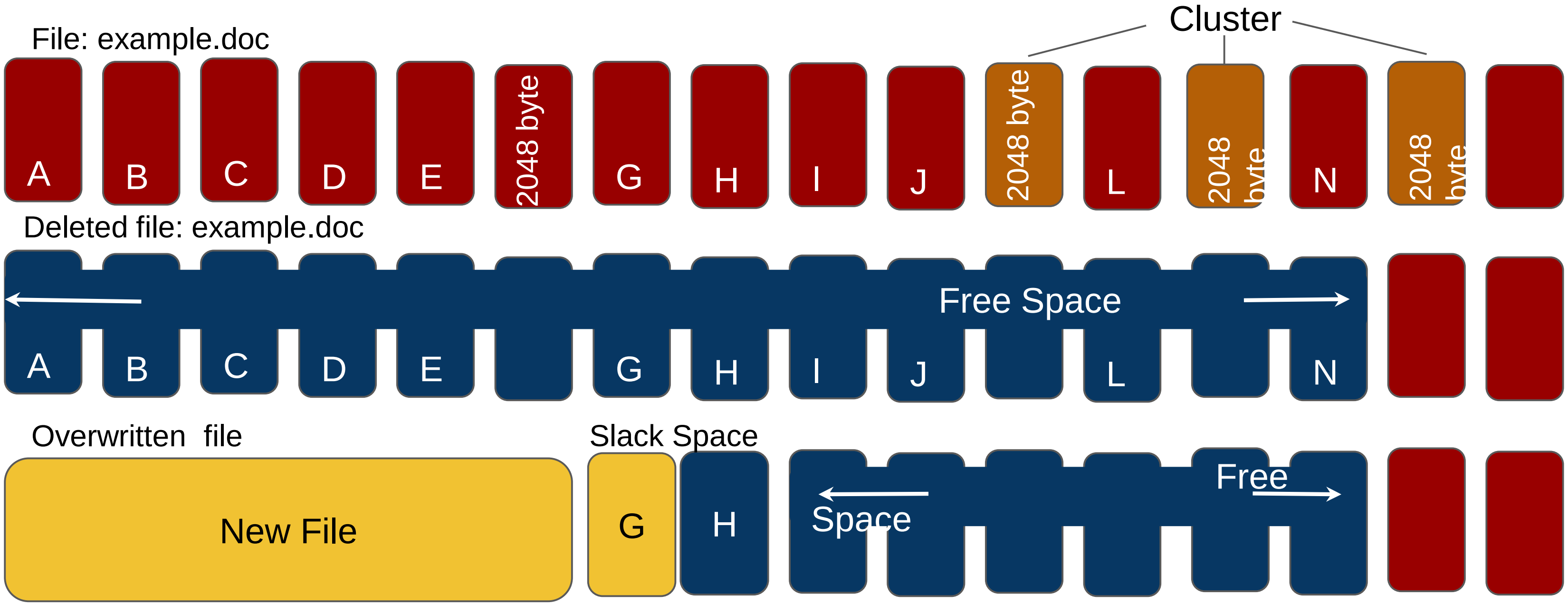
During an investigation, you might encounter these file systems:

- **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 Mac OS system
- **Fourth Extended File System (Ext4)**, used in RedHat, Kali, and Ubuntu

How Evidence Was Obtained: Disk Forensic Image

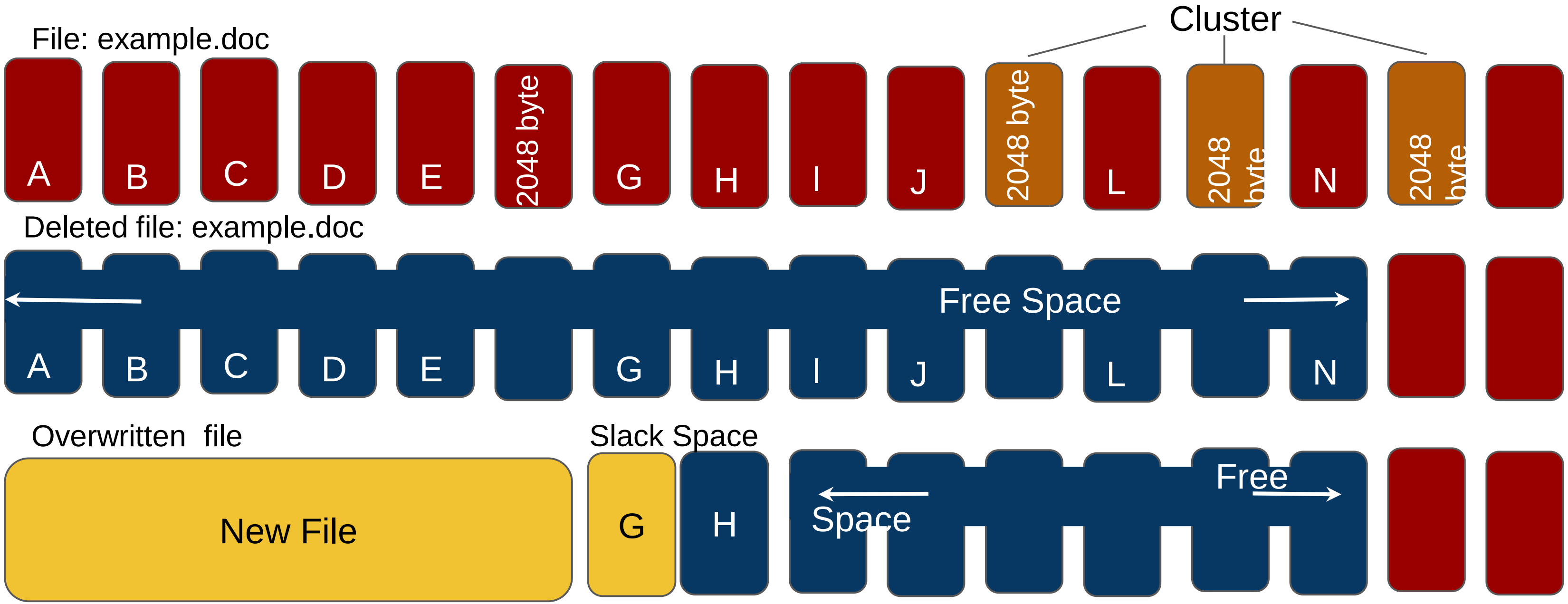
In the Gallery Case, evidence was gathered from an iPhone and saved in the Encase Eyewitness Format (*.E01) as a **disk forensic image** (a copy image of data that is analyzed).

Acquiring data from an image involves a bit-level-copy of the entire physical data source.



How Evidence Was Obtained: Disk Forensic Image

A **basic file system copy** is inadequate for forensic analysis. If you do a copy through the file or operating system, you can see only the data that the operating system sees. It will not capture deleted files or slack space. You need to obtain a **bit-level copy.**



Forensic Disk Image 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

Introduction to Autopsy

Autopsy

Now we’ll look at the software used to **analyze the image file**.

We will use **Sleuthkit Autopsy**, an open source, graphical tool that runs on Windows, Ubuntu, Kali, and OSX.

First we’ll prepare the data by:

- Running a virus scan on the image.
- Generating an md5 and sha256 hash for the evidence. (To validate that nothing was changed during the investigation.)
- Open a terminal window in Kali and navigate 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

1. **Create a case**
   - Case name, investigator information, and optional information
2. **Add an Image**
   - Autopsy supports Raw, Encase, and Virtual Disk image formats.
3. **Configure ingest modules**
   - For example: Email Parser, Embedded File Extractor, Android Analyzer
4. **Ingest in progress**
   - A time consuming process
5. **Manual Analysis**
   - Analysing data
6. **Create timeline**
   - Time, data, and data source
7. **Report**
   - Format (HTML, Excel)

Activity: Introduction to Autopsy

In this activity, you will load evidence into Autopsy for analysis. Please follow the directions in the checklist.

Activities/Stu_Intro_Autopsy

Suggested Time:
15 minutes

Activity: Introduction to Autopsy

Below is a breakdown of the steps you will take. Please refer to the slacked out file from detailed instructions.

Pre-Step 1: Prepare the Data

Pre-Step 2: Getting Started: Creating a Case

Step 1: Set Up Case Information + Optional Information

Step 2: Select Types of Data

Step 3: Configure Ingest Modules (Hash Data Sets + Additional Ingest Settings)

Step 4: View Output from Autopsy

Suggested Time: 15 minutes

Class Objectives

By the end of class today, students will be able to:

- Summarize the basic principles and methodologies of digital forensics.
- Describe various types of jobs and skill sets needed for digital forensics.
- Outline the proper way to collect, preserve, analyze, and report.
- Demonstrate how to conduct a preliminary review of a forensics case.
- Demonstrate preserving and documenting evidence using Autopsy 4.0.