Introduction & Acquisition

Digital Forensics

Course Introduction

Course Layout:

- Introduction to Digital Forensics
  - Definition & History
  - Forensic Fundamentals
  - The Digital Forensic Process
  - Phase One: Identification

Course Layout:

- Digital Forensic Acquisition
  - Phase Two: Preservation
  - Acquisition Methodology
  - Image Formats
  - Validating Evidence
  - Examining Evidence

At the end of this module, you will be able to:

- Understand the digital forensics field.
- Define common techniques
- Preserve evidence

Introduction to Digital Forensics

Module Layout:

- Module Introduction
- Definition & History
- Forensic Fundamentals
- The Digital Forensic Process
- Phase One: Identification

At the end of this module, you will be able to:

+ Understand key principles
+ Define common techniques
+ Scope an investigation

Definition & History

The Background of Digital Forensics

- Forensic Science
- Includes
  - Preservation
  - Investigation
  - Analysis
  - Reporting

With technology entering every aspect of our lives, the application of digital forensics has grown rapidly.

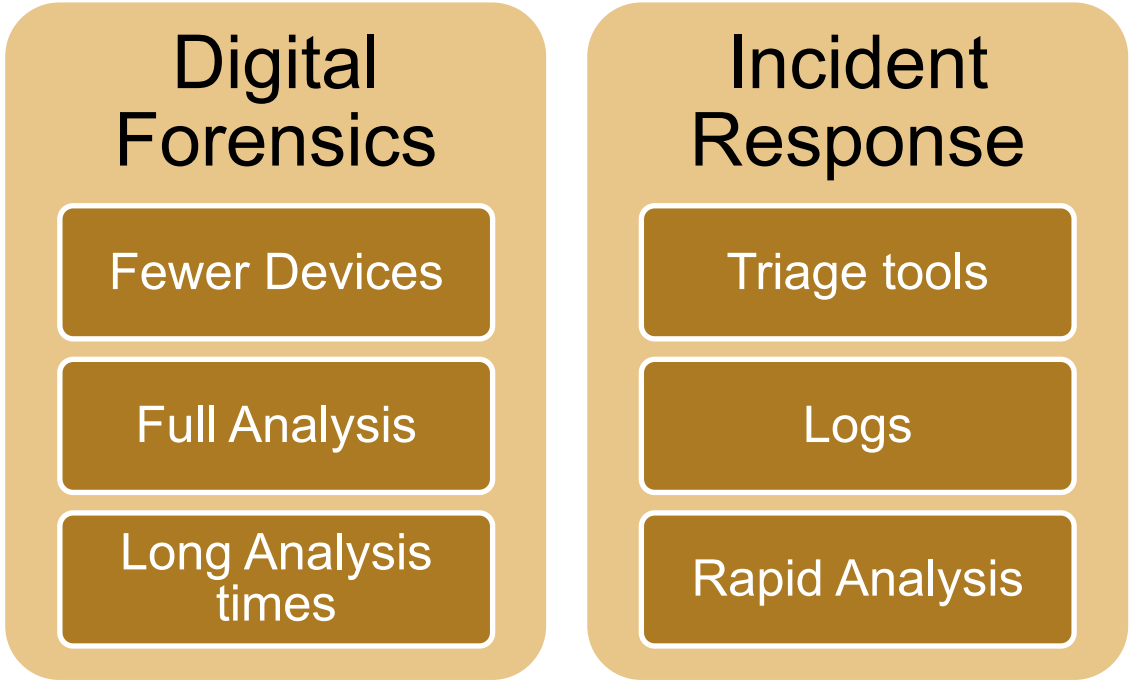
In general, the main goal of digital forensics is to answer the five W's regarding an event with digital evidence left behind.

Digital Forensics vs. Incident Response

+ Sometimes grouped together
+ Focus on Digital Forensics

However, the fields are quite unique today, as the skills necessary to practice each have diverged due to changes in technology and its use.

Digital Forensics vs. Incident Response



Digital Forensics vs. Incident Response

Incident response and analysis is typically trying to answer a specific question

Digital forensics can apply to digital crimes, but it can also be used in the investigation of non-digital criminal or civil cases, including establishing circumstantial evidence of intent or capability.

<FULL CAMERA SCENE>

Incident response and analysis is typically trying to answer a specific question: how was an organization compromised and what was impacted?

Digital forensics can apply to digital crimes, but it can also be used in the investigation of non-digital criminal or civil cases, including establishing circumstantial evidence of intent or capability

+ And what I mean by that is that for Incident Response we use skills and techniques from Digital Forensics, but sometimes our objective is

Conventional Crime, Digital Evidence

Marty Theer

+ 77,000 emails recovered
+ Used as evidence in the murder

Conventional Crime, Digital Evidence

Social media and device usage

+ Apps can track location
+ Providers retain data

Conventional Crime, Digital Evidence

William McGuire was murdered in 2004, police found on his wife's computer.

Digital Evidence in Conventional Crimes

Many conventional crimes can involve digital evidence today. Some examples are:

+ Fraud
+ Child Exploitation
+ Terrorism
+ Drug Trafficking
+ Homicide

Forensic Fundamentals

This section goes through the fundamentals of digital investigations, which include:

+ Digital Evidence
+ Digital Forensic Tools
+ Daubert Standard
+ Scientific Method

Evidence is Everything...

Evidence is the foundation of any crime investigation – DNA in a homicide case, a fingerprint in a burglary, tire tread in a hit-and-run.

In the digital world, evidence is defined as any digital information that is stored, transmitted, or produced from electronic devices or software.

...And Everything is Evidence

Some examples of digital evidence are:

- Web browsing history
- Downloaded or temporary files
- Event logs and system logs
- Pictures produced by digital cameras
- Print logs saved on printers
- Email messages
- Deleted or hidden files
- Applications and associated data

Evidence Preservation

It’s very important for digital forensic practitioners to understand how digital devices, operating systems, and applications function so that they can preserve evidence to the utmost degree.

If data is not acquired correctly for the given situation, evidence could be lost or altered during the process. This could cause the evidence to be deemed inadmissible for use in court proceedings.

Evidence Preservation <FULL CAMERA>

An analyst's tools play a very important role in the digital forensic process.

However, being a digital forensic practitioner isn't just about using the correct tools in a correct way.

Practitioners are expected to have a deep and thorough understanding of the underlying technologies they are handling.

Practitioner Responsibility

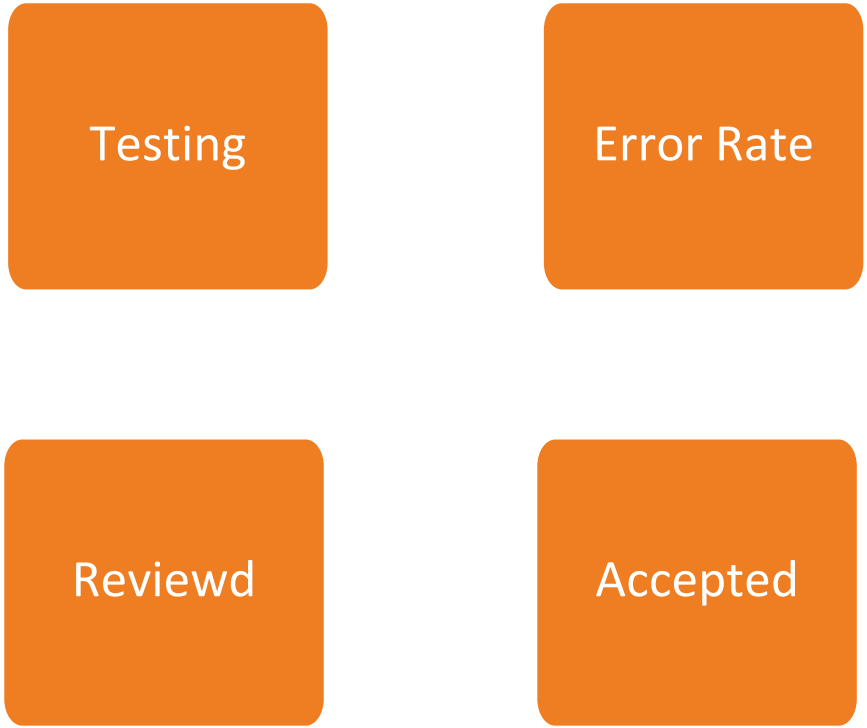
Being able to point-and-click in the right order isn't enough. We must understand what our tools are actually doing as they acquire, process, interpret, and display data.

Forensic Tools

There are three basic categories of tools available for digital forensic practitioners. These are:

- Proprietary or closed-source
- Open-source
- Custom-built

Daubert Standard



An investigator is also expected to be able to:

+ Apply
+ Analyze
+ Detect

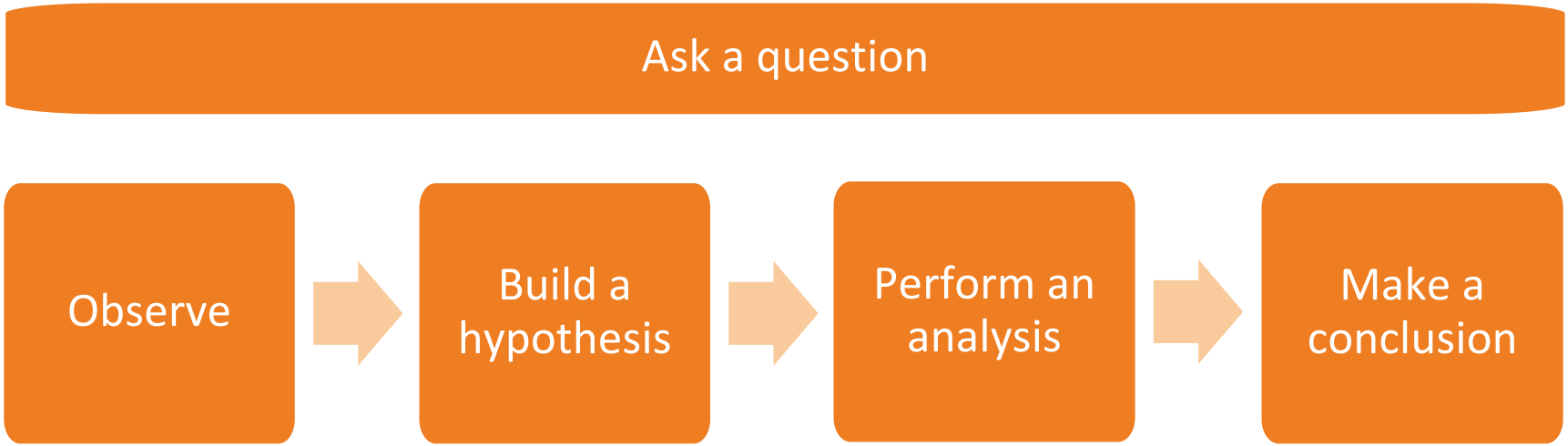
The Scientific Method

The Scientific Method is a body of techniques for:

+ Investigating phenomena,
+ Acquiring new knowledge, or
+ Correcting and integrating previous knowledge.

The Scientific Method is the investigator's most useful ally in their mission to present reliable evidence.

The methodology is simple:



I have a hypothesis, now what?

The next step for the investigator is to start making predictions based on the hypothesis formulated. These predictions must be testable and provable; otherwise, they are meaningless.

To minimize the chances of error, it is essential that they consider and test alternative hypotheses.

Proving or disproving a prediction is achieved by collecting specific data which supports or contradicts it.

Important Note!

There are incredibly few, possibly zero, cases where an investigator can use digital evidence to conclusively attribute digital activity to an individual.

It is essential to remember that digital evidence is almost always circumstantial, with photographic or videographic evidence coming the closest to qualifying as direct evidence.

No matter how much digital evidence you have, it is unlikely that you can prove whose fingers were on the keyboard when it was generated.

Backed by Science

The reason we follow scientific procedures in extracting artifacts and building a hypothesis is that you need a scientific base to validate and explain your conclusions and how you reached them.

If there is no scientific reason to support your procedure or findings, the credibility of your forensic analysis and the resulting evidence will be undermined and it may be deemed inadmissible in court proceedings.

The Digital Forensic Process

The Digital Forensic Lifecycle

The process of conducting a digital forensic investigation can be broken into five basic steps:

Identification	Determine potential sources of relevant data
Preservation	Acquire data in a manner that secures and preserves its integrity
Analysis	Correlate and studying the data
Documentation	Recording relevant findings
Presentation	Preparing a report to share findings

Each of these phases will be covered in depth through the courses of the Digital Forensic program!

For now, a general understanding of the investigative process will suffice.

Digital Evidence

The possible types and sources of digital evidence is an all-but infinite list.
Each case you investigate could have different types of evidence.

Sources of Digital Evidence

Your investigation could involve any device that is capable of storing digital data, including (but not limited to):

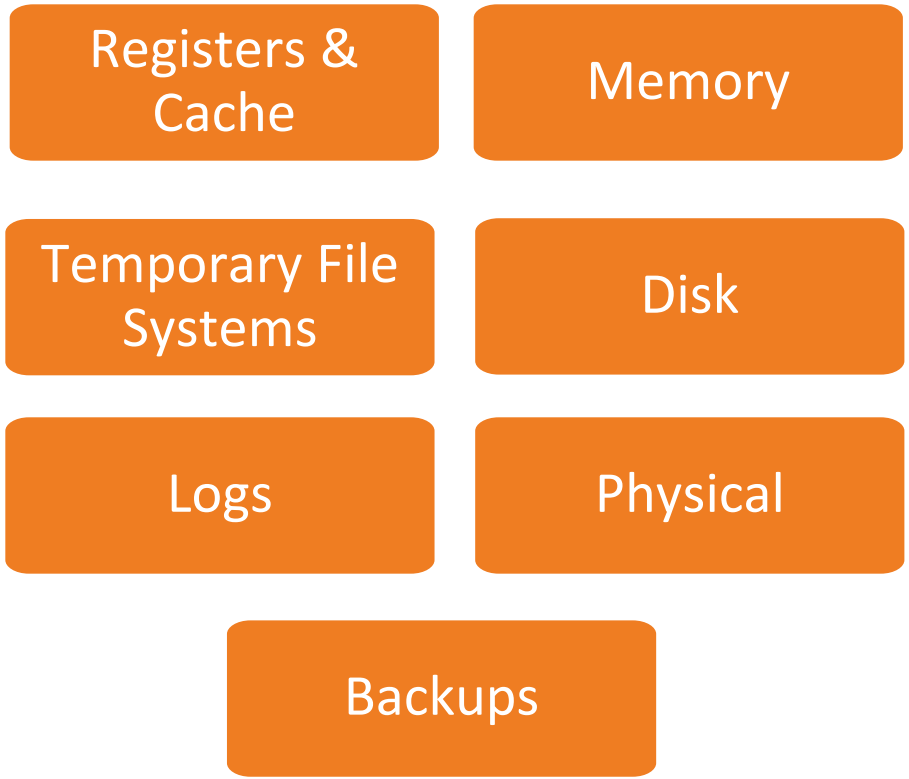
- Computers: such as laptops and desktops, and their internal storage.
- External storage devices: such as external hard drives
- Removable media: such as flash drives, CDs/DVDs
- Mobile devices: such as cell phones and tablets
- Peripheral devices: such as printers and scanners
- Network devices: such as routers and wireless access points

Let’s Talk Volatility

Data can be generally categorized into volatile and non-volatile forms.

- Volatile data: typically refers to the data stored in RAM. This data is generally unrecoverable once the device is turned off, and is tricky to acquire and analyze due to its changeable nature.
- Non-volatile data: refers to data that can still be retrieved for acquisition and analysis when the device is turned off.

Order of Volatility:
This list can provide guidance on what data to prioritize for acquisition due to its potential lifespan. Some of these sources are only available if the device is on at the time of acquisition.



Non-volatile Data Classification

Non-volatile data is classified into three basic types:

- Active data
- Archive and backup data
- Hidden data

Hidden data is then further classified into three basic types:

- Metadata
- Residual data
- Replicant data

Active Data

Active data includes everything the user can see and interact with when using a device.

Archive & Backup Data

This is all data that is in long-term storage to avoid data loss.

Hidden Data

This data is not readily accessible by users and requires specialized tools to access.

Hidden Data: Metadata

- Defined as “data about data.”
- One of the most valuable pieces of evidence
- Essential for building an accurate timeline of events.

+ File Attributes
+ File location’s
+ File access
+ Timestamps

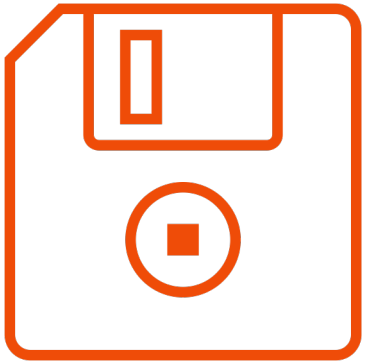
Types of Metadata: An Abbreviated List

Hidden Data: Residual Data

This is deleted data still on the disk.

Residual Data & Metadata Team Up!

BTK Killer
Dennis Rader



Hidden Data: Replicant Data

- Data is generated when a program creates a temporary copy of an opened or accessed file
- Can help build a timeline
- Files can be retrievable

Presence ≠ Proof

- In 2007, person was convicted of possession of child pornography.
- No evidence to support the person's intent
- The conviction was overturned

Phase One: Identification

The Identification Phase

The first phase of the digital forensic process – Identification – focuses on defining the components of the investigation. That includes:

+ Establishing authority based on the type of case
+ Defining the scope and affected parties
+ Identifying potential sources of relevant evidence
+ Coordinating access with custodians of evidence sources

Establishing Authority

We don’t get to run around acquiring and analyzing whatever devices we want, that’d be an invasion of privacy – we need to have permission.

Defining Scope

In collaboration with the authorizing party, you will need to define the initial scope of the investigation. This can be done in many ways, and some examples are:

- Particular device(s)
- Particular user(s) across all devices within authority
- All devices located in a defined location
- Particular type(s) of devices in a defined location
- Particular type(s) of activity across a defined part of the network

Get it in Writing

And approved by all parties

Under Contract

Considerations during for the investigation agreement:

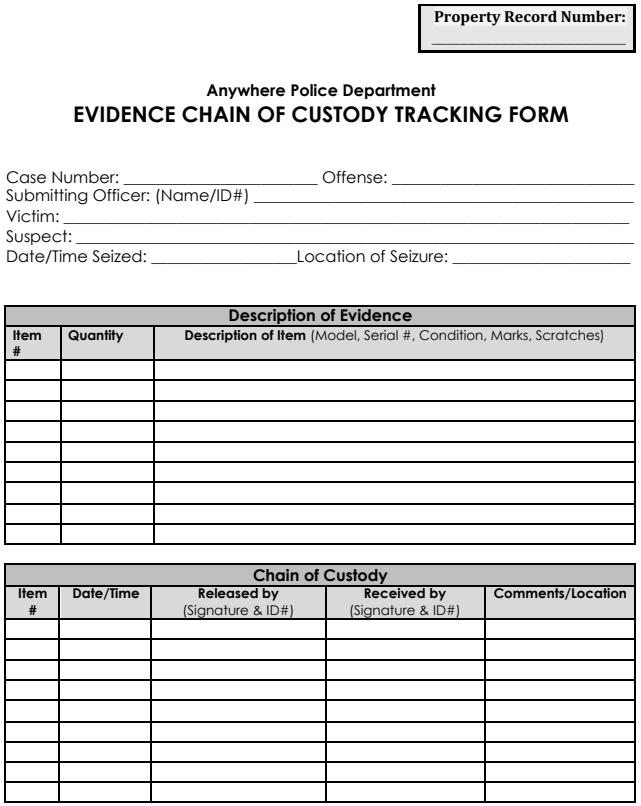
+ Where will they be acquired
+ Estimated timeline
+ Confidentiality

Next Up: The Scavenger Hunt

Inventory the devices that are in scope

Next Up: The Scavenger Hunt

Start the chain of custody process



Property Record Number: _____

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

Behind Locked Doors

+ Access
+ Work with the legal team
+ Schedule and be conscious of production and work schedule
+ Clearly communicate

Module Review

This module covered:

+ Definition & History
+ Forensic Fundamentals
+ The Digital Forensic Process
+ Phase One: Identification

Now you are able to:

- Understand what the field of digital forensics encompasses
- Define common techniques used in digital forensics
- Perform forensically sound data acquisitions.

Digital Forensic Acquisition

Module Layout:

- Module Introduction
- Phase Two: Preservation
- Acquisition Methodology
- Image Formats
- Validating Evidence
- Examining Evidence

At the end of this module, you will be able to:

- Understand the process to perform forensic acquisitions,
- Define common techniques used in forensic acquisition, and
- Effectively perform acquisitions of various data sources.

Phase Two: Preservation

The Preservation Phase

The second phase of the digital forensic process – Preservation – focuses on ensuring that evidence maintains its integrity and authenticity. That includes:

+ Protecting
+ Acquiring
+ Documenting

A Note About Storage

Consider where to store the images you need to acquire. There are several options, with key considerations being sanitation and speed:

+ External hard drives (wiped if used before)
+ Storage Area Networks (SANs)
+ Cloud storage

Can It Communicate?

+ Wireless connectivity
+ Devices with a SIM card / Cellular / WiFi capabilities.
+ Automatically connect to wireless networks.

Skipping acquisition for a second, let's talk documentation:

Document:

+ Manufacturers, makes, & models
+ Serial numbers
+ Dates & times
+ Storage capacities
+ Verification hash values
+ Software & hardware used
+ Custodian or owner name
+ Contact information
+ Physical or content description
+ Relevant case number(s)

What is forensic acquisition?

Forensic acquisition is the process of creating an exact copy of the evidence.

A note on why we acquire

We never almost never perform analysis on the evidentiary device

Copies on Copies

Ideally, you won't even be performing forensic analysis against the initial image you take.

Since that image has been hash verified against the source, it is ideal to then make a copy of the verified image to work from.

All of this copying reduces the risk of data alteration or corruption, ensuring integrity.

Acquisition Methodology

Two (Ways) to Tango

There are two basic styles of data acquisition:

Dynamic / Live Disk Acquisition

Static / Dead Disk Acquisition

Dynamic or Static... Or Both!

If dynamic acquisition is performed for volatile data, static acquisition of non-volatile data can also be performed.

Switching to static acquisition can reduce the amount of data alteration and the risk of corruption.

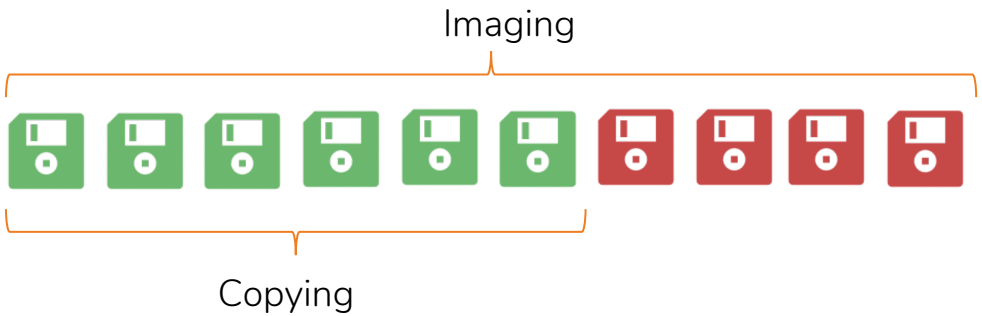
After acquiring relevant volatile data, gracefully shutdown the device and then proceed with static acquisition.

Physical vs. Logical

Another consideration is whether you'll be performing a physical acquisition or a logical one.

Image Formats

Is Imaging Just a Fancy Word for Copying?



Pick a File Type, Any File Type

Forensic images can be stored as several file types:

+ RAW (.dd, .img, 001)
+ Expert Witness (EWF)

RAW vs. EWF

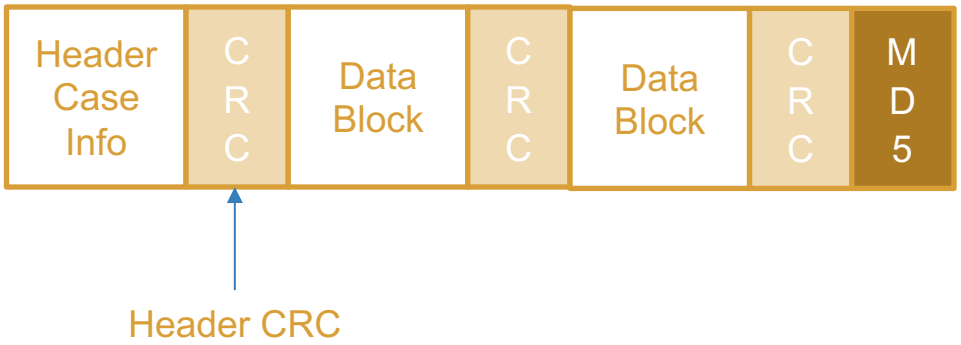
The RAW image format:

+ Can be created with common CLI tools (e.g. DD, DCFLDD, DC3DD, DDrescue)
+ Is a bit-by-bit copy of the source evidence
+ Can be saved to a disk of equal or greater size, or to a file
+ Can natively be mounted as a disk

The EWF image format:

+ Can be created and mounted by common forensic tools (e.g. FTK Imager, Autopsy, EnCase, EWFAcquire)
+ Applies compression during image creation
+ Performs image verification per sector as well as for the full disk
+ Includes case information in the file header

What is the EWF format?



Validating Evidence

Demonstrating Image Integrity is Essential

Regardless of the type of case, it's important that you can demonstrate that the data you analyzed was the same as the original data.

This is where hashing helps.

What in the Hash?

Hash functions are one-way cryptographic functions.

The Proof is in the Hash!

Hash strings are used as proof that evidentiary image is identical to the original source.

Many forensic acquisition tools include built-in options for performing hash verification of source and target data. Be sure to include these results with your documentation and reporting!

Examining Evidence

Mounting Images

Mounting an image let’s you peruse the contents much like inserting a USB flash drive or CD.

How to Mount Images

The technique for mounting image files varies based on the image format and available software.

A Short List of Tools

The following free tools can be used to mount images:

- *nix mount command – CLI, built-in
- Autopsy – GUI, open-source
- FTK Imager – GUI, free
- ewfmount – CLI, open-source

Module Review

This module covered:

- Phase Two: Preservation
- Acquisition Methodology
- Image Formats
- Validating Evidence
- Examining Evidence

Now you are able to:

- Understand the process to perform forensic acquisitions,
- Define common techniques used in forensic acquisition, and
- Effectively perform acquisitions of various data sources.

Course Conclusion

Course Layout:

- Introduction to Digital Forensics
  - Definition & History
  - Forensic Fundamentals
  - The Digital Forensic Process
  - Phase One: Identification
- Digital Forensic Acquisition
  - Phase Two: Preservation
  - Acquisition Methodology
  - Image Formats
  - Validating Evidence
  - Examining Evidence

Now you are able to:

- Understand what the field of digital forensics encompasses,
- Define common techniques used in digital forensics, and
- Perform forensically sound data acquisitions.