Introductions

Introductions

Dr. Clemente Izurieta (Clem)

- Professor of Computer Science (13 years)
- Director of the Software Engineering and Cybersecurity Laboratory at MSU
- Formerly at Hewlett Packard and Intel (14 years)

Acknowledgements: William Peteroy for slide contents

Digital Forensics Outline

Section Outline

- Introduction to digital forensics
- Conducting an investigation
- Planning and preparation
- Reporting
- Disk forensics
- Windows Registry Forensics
- Network Forensics
- Live Forensics
- Memory Forensics

Digital Forensics

Digital forensics is the **collection, analysis and interpretation** of **digital evidence**.

Digital Evidence

“Any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or an alibi”

“Digital evidence is information and data of investigative value that are stored on or transmitted by a computer.”

“Digital data that support(s) or refutes a hypothesis about digital events or the state of digital data”

Types of Digital Data

Open Computer Systems

- A.k.a. computers (laptops, desktops, servers)
- Standard system (HDD, RAM, etc.)

Communication Systems

- Networks including:
  - Traditional telecommunications systems.
  - Wireless telecommunications systems.
  - Internet

Embedded Computer Systems

- Mobile devices, smart cards, “smart devices”

Digital Evidence Processing

Critical to follow appropriate processes and procedures when collecting and processing digital evidence.

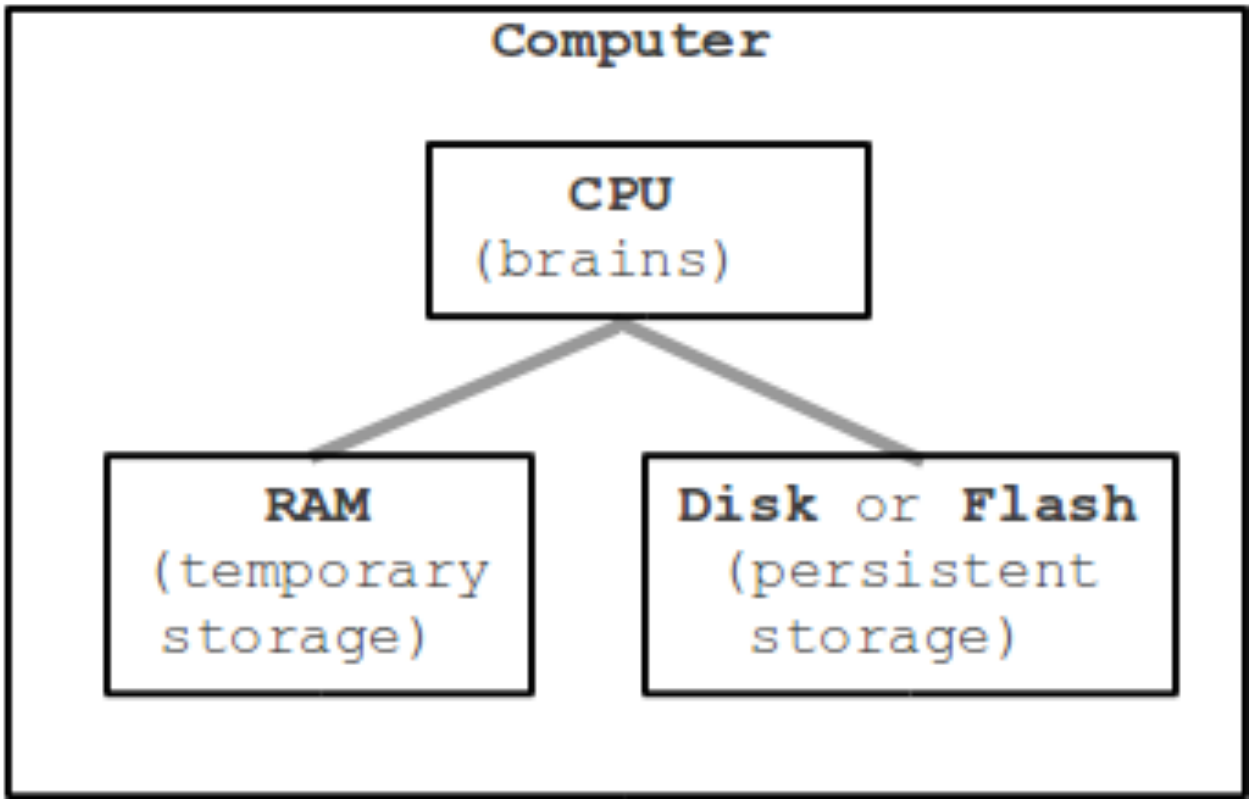
- Not following processes could put an investigator at legal risk (collecting without authorization).
- Improperly collected or tracked evidence could be inadmissible in court.

Context

Context is critical.

- Always important to understand the “why” of the case that you’re working on.
- Timelines can be critical.
- Will directly influence what data you collect, how you process it.
- Corporate vs. Legal vs. Law Enforcement.

Computer Overview



Principles of Computer-based Electronic Evidence

1. No action should change data.
2. If accessing original data – must be competent, explain relevance and implications of actions.
3. Audit trail or record of all processes applied must be created and preserved.
4. Person in charge of the case has overall responsibility for ensuring laws and principles are followed.

Digital Evidence Collection

- Digital evidence is typically collected through software or hardware tools.
- Hardware tools are used when the device is physically in the possession of the investigator and provide power and an interface to access on the target device.
- Implications of these choices on the principles of computer-based evidence exchange.

Volatile vs. Non-Volatile Artifacts

Volatile

- Does not persist across power cycles.
- Examples: RAM contents.

Non-volatile

- Does persist across power cycles.
- Examples: hard drive contents.

Disk Capture

- Hard drive (hard disk) capture
- Creating a copy of the contents of a hard drive to a file for analysis.
- Disk capture can be done physically (connecting to the disk) or virtually

Principles of Digital Forensics

Certainty

- We're almost never "certain" --this is a protected term that must be used with extreme care.
- We cannot be certain of what occurred at a crime scene or other situation when we have only a limited amount of information.
- We present possibilities and hypotheses and the evidence and information that support or refute these hypotheses.

Evidence Exchange

Locard's Exchange Principle: contact between two items will result in an exchange.

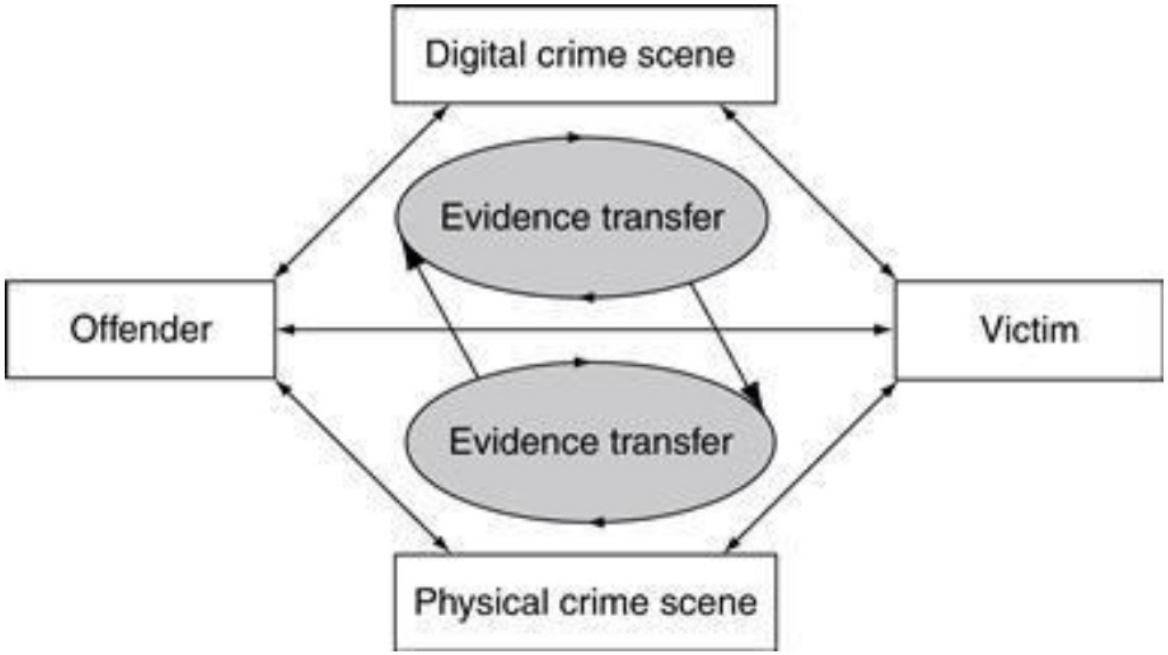


Figure 1.1 Evidence transfer in the physical and digital dimensions helps investigators establish connections between victims, offenders, and crime scenes.

Evidence Characteristics

Class characteristics:

- Similar traits between a group of items
- Common traits
- Examples: File format characteristics

Individual characteristics:

- Unique traits that can be tied to an individual
- Examples: MAC address

Forensic Soundness

How the evidence was handled (preserved and examined).

Two key concepts:

- Non-modification of evidence
- Documentation
  - Time
  - Tools
  - Methods
  - Hash values for everything.

Validation of Data

- Integrity of data / records being analyzed.
- Must be able to show:
  - Contents of record are unchanged
  - Information in record originates from purported source
  - Extraneous information such as date of collection / record is accurate

Chain of Custody

- Documentation that proves continuity of possession of evidence.

cmdLabs Continuity of Possession Form				
Case Number:	2010-05-27-00X		Client/Case Name:	Digifinger Intrusion
Evidence Type:	hard drive		Evidence Number:	0023
Details:	Mac storage <network share>			
Date of Transfer	Transferred From	Transferred To	Location of Transfer	Action Taken by Recipient
5/27/10	Sam Spade	Philip Marlowe	Digifinger HQ Northview MD	Collected evidence for examination

Evidence Integrity

- Showing that evidence has not been modified since time of collection
- We use message digest (hash) functions to perform this work for us
- Message digests always produce the same output for a given input
- Most practitioners use SHA256, however, some tools only support MD5 and SHA1

Repeatability

- It is critical that for a given piece of evidence, the process by which it is analyzed is repeatable
- Enables independent verification

Evidence Dynamics

- The real world is imperfect
- Any influence that
  - Changes
  - Relocates
  - Obscures
  - Obliterates

  evidence must be documented
- Regardless of intent
- Timeframe is from the time evidence is transferred and the time the case is solved

DFIR Research

Digital Forensics Incident Response

- The state of the art forensics research is done across academic, public and private sectors.
- The premier DFIR venue globally is DFRWS.
  - https://dfrws.org/
- The premier DFIR conference focused on incident response is FIRST.
  - https://first.org/

Capturing Digital Evidence

Review of Evidence Types

Volatile

- Must be captured while system is running.
- Faster is better.

Non-volatile

- Can be captured from a running system or an offline system.
- Need to check in on what the purpose of the investigation is to determine best way to capture non-volatile data.

Capturing Non-volatile Evidence

Interacting with a data storage device that does not modify (or lose) data when powered off.

- Typically have to figure out how to:
  - Access data.
  - Power on the device.
- Prevent writing/modifying data.
- Investigation scope and logical data captures.

Physical Disk Capture

Capturing the physical contents of a drive.

- Pros:
  - May get deleted files.
  - Will be able to parse the entire “raw” disk and data structures.
- Cons:
  - Capture used and “unused” disk space
  - Time consuming.
  - Large output file.

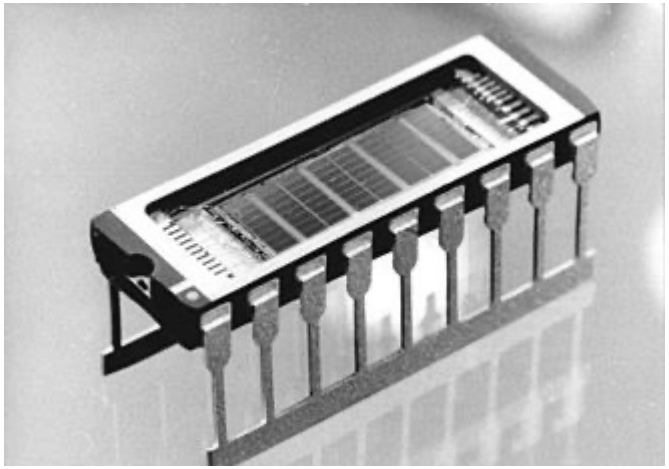
Logical Disk Capture

Capturing the logical contents of a drive.

- Pros:
  - Gives us all the files from the operating system's point of view.
  - Quick
  - Small(er) output files.
- Cons:
  - Won't get unused disk space.
  - No chance of recovering deleted files.

Capturing Volatile Evidence

- Volatile evidence is non-persistent when power is lost to the device.
- Main component that affects us is any system with a RAM component.
- RAM loses all contents when a system is powered off.



Capturing Volatile Evidence

- Volatile evidence capture requires interacting with a running system.
- Typically done remotely over SSH using RAM capture tools (Volatility Surge).
- Need to be careful to understand how you're capturing RAM as
  - You need administrative access.
  - You could be creating new files on disk.
  - You can fill disk and crash the machine.

Capturing Network Forensics Data

- Capturing network data either requires a dedicated (and pre-positioned) network tap.
- A network allows for a copy of all traffic coming and going (RX and TX) to be sent to an additional interface.
- A capture interface can be leveraged to get access to process or capture traffic.

Network Forensic Capture

- Typically talking about “full” packet capture (not just metadata).
- Uses a monitor port. Can use copper or a fiber network interface
- Output / capture format: PCAP (short for packet capture).
- Line rate: Capable of capture at same bandwidth as source device.
- Can leverage tools to do this (NetWitness)

Network Forensic Capture Cont'd

- Pros:
  - Full capture of everything.
  - Can include files, non-standard protocols, and a lot more.
- Cons:
  - Typically have to decrypt in-line / MITM traffic.
  - Newer TLS versions are making "passive" decryption difficult.
  - Encryption not always possible (TLS1.3)
  - Harder and harder as people move to cloud environments.

Network Metadata Capture

- Capture is becoming less and less feasible due to data transmission and storage limitations
  - 100 MBPS x 7d = 7.56TB
  - 10 GBPS x 7d = 756TB
  - 10 GBPS x 30d = 3.26PB

Network Metadata Capture Cont'd

Network metadata by environment

- Cloud
  - Typically netflow data, e.g., AWS VPC Flow logs
- On-premise
  - Alert metadata: Suricata (most popular), other Network Intrusion Detection (NIDS) tools
  - Flow data: typically collected by a netflow collector
  - Network Security Monitoring (NSM) metadata: typically collects protocol metadata for some or all protocols