Introductions

Slides contribution from Blackthorne Consulting and ESOF 422 Montana State University
Introductions

Clemente Izurieta
- Professor of Computer Science at Montana State University
- Joint Appointment (INL, PNNL)
- Co-director of the Software Engineering and Cybersecurity Lab (SECL)
  - Funding: Army, Air Force, DHS S&T, Raytheon, NSF, National Labs (INL, PNNL)
  - 8 Phd.D., 5 MS, many undergraduates, professional staff
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.
“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, HID, RAM, etc.)

Communication Systems
• Networks including:
  ─ Traditional telecommunications systems.
  ─ Wireless telecommunications systems.
  ─ Internet

Embedded Computer Systems
• Mobile devices, smart cards, “smart devices”
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

![Diagram of Computer Components]

- **Computer**
  - **CPU** (brains)
  - **RAM** (temporary storage)
  - **Disk or Flash** (persistent storage)
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.
Authentication

- 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.
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 and information from that analysis is repeatable.

• Enables independent verification.
Evidence Dynamics

- The real world is imperfect.
- Any event that
  - Changes
  - Relocates
  - Obscures
  - Obliterates
  regardless of intent, can easily occur.
- Timeframe is from the time evidence is transferred and the time the case is solved.
DFIR Research

• The state of the art forensics research is done across the 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.

• Investigation scope
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 of 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.
  - You can trigger AV (LSASS memory access).
Capturing NetworkForensics 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, Wireshark, Snort)
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

• Pros
  — Fast
  — Low storage requirements

• Cons
  — Processing overhead is also a challenge without hardware offloading and specialized drivers (raw packet access).
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
Exercises
Volatility plugins

• After installing Volatility 3
  • Python3 ./volatility3/vol.py –f <path to .vmem>
    – windows.pslst
    – windows.netscan
    – windows.pstree
  • Outputs of Volatility can be piped. For example:
    – ... pstree | grep “LISTENING”
    – ... netscan | grep <IP address>
• Dump a process
  • Python3 ./volatility3/vol.py –f <path to .vmem> -o <dump dir> windows.memmap –pid <PID>
Tools

• Swiss Army knife to decode/encode strings
  — https://gchq.github.io/CyberChef/

• Check for presence of Malware
  — https://www.virustotal.com/gui/home/upload

• Review calendar and emails

• Compare Volatility commands
  — https://blog.onfvp.com/post/volatility-cheatsheet/
Incident Management
Investigations and Incident Handling

• Investigations and incidents have defined processes.

• For criminal investigations and best practices – ACPO Good Practice Guide

• For incident response – NIST 800-61r2
NIST 800-61r2

- NIST 800-series – information security series.
- 800-61r2 – Computer Security Incident Handling Guide
Investigation Preparation

• Communications:
  – Contact information
  – On-call information
  – Incident reporting mechanisms
  – Issue tracking systems
  – Encryption software
  – War room
  – Secure storage facility
Attack Lifecycle
Attack Vectors

• External/Removable Media
• Web-based attacks
• Email attacks
• Impersonation
• Improper usage
• Loss or theft of equipment
• Other
Signs of an Incident

Precursors

• Web server logs indicate the presence of unauthorized vulnerability scanning.
• Announcement of a new, relevant vulnerability.
• A threat group stating privately or publicly that they are targeting the organization.
Signs of an Incident

Indicators of Compromise
• Alerts from a NIDS or HIDS (AV / EDR)
• Suspicious log / audit log entries for key services.
• Configuration changes
• Multiple failed login or access attempts
Analysis

• Profile networks and systems
• Baseline normal behavior
• Perform event correlation
• Maintain and use a knowledge base of information
• Use Internet search engines for research
• Collect additional data
• Filter the data
• Seek assistance from others
Documentation

• Current status of the incident
• Summary of the incident
• Indicators of the incident
• Other related incidents
• Actions taken by incident handlers
• Chain of custody, if applicable
• Impact assessments related to the incident
• List of gathered evidence
• Next steps to be taken
Prioritization

• Prioritization of incidents is critical
• Functional impact
  — impact of the incident on IT systems functionality
• Information impact
  — What’s the impact on confidentiality, integrity and availability of information
• Recoverability
  — Size of the incident, degree of compromise, and type of resources it affects will impact the amounts of resources needed for recovery
Notification

• Key stakeholders must be notified based on the incident severity and impacts
• This is typically documented in an organization’s incident response plan
• Notification requirements may vary by the data involved in the incident or contractual requirements
Containment

- Containment strategies vary and they must balance the need to prevent additional damage or theft with a need to maintain and collect evidence
- Premature containment can lead to situations where an adversary is thought to be “evicted” but is not
- Containment cannot occur without root cause analysis
- Containment typically involves parallel network and identity efforts
- Examples: APT actor war stories
Evidence Collection

- Once containment is established / it’s time to figure out what happened, and to do that a scope of systems and a collections plan are needed
- Scoping systems is critical while prioritizing timelines and resources for collection
Analysis

• Identify attacking hosts
• Identify the root cause of the incident
• Build a timeline of the incident including the sequence of events from the root cause of the incident
Eradication and Recovery

- Similar to containment strategies, good eradication and recovery strategies will take inputs from evidence collection and analysis and balance the business capabilities against attacker access.
- Phased approaches generally work better.
- Eradication - removing adversary access.
- Recovery - ensuring systems are functional within expected parameters.
- Don’t forget to address the root cause!
Lessons Learned

• What happened, when?
• Did staff and organizations perform as expected?
• What would staff do differently the next time an incident like this occurs?
• What corrective actions can prevent similar incidents in the future?
Post-incident Analysis

• Prioritization of incidents is critical
• Functional impact
  — impact of the incident on IT systems functionality
• Information impact
  — What’s the impact on confidentiality, integrity and availability of information
• Recoverability
  — Size of the incident, degree of compromise, and type of resources it affects will impact the amounts of resources needed for recovery
Conducting an Investigation: Investigation Models
Formal Investigation Process Models

• Digital investigations must uncover and produce the truth
• Early models described stepwise approaches to specific investigative problems (and focused solely on computer crime on networked computer systems)
• Real-world digital investigations are diverse
Figure 6.2 Categories of the investigative process model (depicted as a flight of stairs) from Digital Evidence and Computer Crime, 2nd edition.
Distillation

- Preparation
- Survey / Identification
- Preservation
- Examination and Analysis
- Presentation (Reporting)
Preparation

• Plan of action, tool preparations and resource preparation
• Case management (or case management preparation)
• Logistical / collection considerations
Survey / Identification

• Review all potential sources of digital evidence to get a familiarity with the totality of evidence
• Determine which items may be of potential relevance to the investigation
• Example: compromised systems vs. all systems
Preservation

- Preventing changes of in-situ digital evidence
- Critical for maintaining the integrity of the investigation
Investigation Scoping
In-depth Investigations

Overview

• Forensic policy approach
• Digital evidence maps
• Scope of an investigation
• Forensic preparedness
• Real-world lessons learned on investigation scoping
Realities of Real-world Forensics

- Surveys by nature must be initially broad
- Once the investigation starts, it will be constrained by the law, time, resources and the interests of the victim (person, business, or organization)
Forensic Policy Approach

• Specification and enforcement of policies
• What events must be handled
• What data surrounding events must be preserved
• What logs are collected, how long are they retained, do they have required detail
Digital Evidence Maps

• Layout of evidence survey
  – Systems
  – Network layout
  – How they relate
  – What data we have from each

• Can help with rapid scoping / targeting and prioritization of analysis
Investigation Critical Focus Areas
Common Core Investigation Areas

• Despite every investigation being unique, there are core investigation focus areas almost all investigations include

• Core areas:
  – Customer data
  – Intellectual property
  – Payments and financial systems
Core Investigation Tech.

• Certain systems appear in investigations more often than not

• Core systems:
  – Active Directory Domain Controller(s)
  – Email Server (could be server or SaaS)
  – Web Application Servers
  – Remote Access Servers (Virtual Private Network (VPN) or Remote Desktop / Secure Shell)
Analysis and Reporting
Examination and Analysis

• Searching for evidence
• Interpreting evidence
• Analysis of the evidence in the context of the incident / investigation
Analysis In-Depth

• Useful to think of graphs and timelines
• Use investigative loops to process evidence:
  – Determine hypothesis
  – Recover / extract data from available sources
  – Harvest data and metadata about all items of interest
  – Organize and search data
  – Reduce data to aid in analysis
Attack Lifecycle

- Internal Threats
  - Existing Access
  - Perimeter Compromise
- External Threats
- NETWORK PERIMETER

1. Perform Reconnaissance
2. Escalate Privileges
3. Move Laterally
4. Disrupt Business
5. Exfiltrate Data
Example Analysis

• Map out a theoretical attack / walk through with a phishing attack and malware installation
• Walk through attack lifecycle, sample artifacts, timeline
• Work backwards / forwards in the timeline
• Practice discovery / filtering (reduction)
Example Analysis

1. Initial Phish
   - Email message, contents, malicious link or attachment.

2. Initial execution
   - Evidence of document executing on system.
   - Evidence of malware loader / execution (powershell, rundll32, etc.)

3. Malware installation
   - Evidence of malware binary execution (Amcache, etc.)
   - Evidence of malware persistence (Autoruns, registry, etc.)
Analysis In-Depth

- Hypothesis
- Recover
- Harvest
- Organize
- Search
- Reduce
Scientific Method

• When in doubt, use the scientific method:
  – Observation
  – Hypothesis
  – Prediction
  – Experimentation / testing
  – Conclusions
Temporal Analysis

- Using a chronological list of events, focus on people and events (when).
- Look for patterns, gaps, and anomalies.
Spreadsheet of Doom Walkthrough

• Spreadsheet of doom (SOD)

• Colloquialism for a central tracking document used by analyst(s) coordinating on a project

• Key store for technical notes so that things don’t get “lost” and so that it’s easy to “show work” and talk to what happened and what specific evidence supports that
Reporting
Presentation

• Without good reporting, great forensic work will go un-noticed
• Findings from the investigation must be reported in a manner which satisfies the context of the investigation
Understand Objectives

• The first step to good reporting is understanding the report format and objectives
• This should be done during investigation planning and must be done before analysis starts
Take Good Technical Notes

• The second step to good reporting is good notes
• Good technical notes are critical to good reporting
• Track every action and the outcome
• Use a scratch sheet to track key outputs and characteristics:
  — Key filenames, IP addresses, Hash values, File paths, tool outputs
• At any point you should be able to describe what your output is and how you got there
Reporting

All good forensic reports include:

- Affected assets (computers, identities, etc.)
- Description of how the activity started
- Sequential timeline of relevant events
- Statements related how evidence supports / doesn’t support hypotheses related to the goals of the investigation
Lab 1

- An employee reported that their system started to act strangely after receiving a suspicious email

  - What malicious processes are running on the image?
    - Hint: Use malfind plugin
  
  - What is the C2 IP address?
    - Hint: Use netscan plugin
  
  - Who sent the phishing email?
    - Hint: Use the dumpfile plugin, search for “From: ” strings in files
  
  - Can you find the email?
    - Use Goldfynch PST reader