CYBER502x
Computer Forensics

Unit 1: Computer Forensics Fundamentals

What is Computer Forensics

- **“Gathering and analyzing data** in a manner **as free from distortion or bias as possible** to **reconstruct** data or what has happened in the past on a system” --*Farmer and Venema, 1999*
- A science and process of collecting, preserving, analyzing and reporting **legally admissible** evidence to court.

Types of Computer Forensics Technology

- System forensics (*inux, Windows, etc.)
  - Memory forensics
- Mobile device forensics
- Network forensics
- Internet and cloud forensics

Digital Forensics vs Anti-Digital-Forensics

- Digital Forensics
  - Meant to discover information about illegal activities of a user
- Anti Digital Forensics (or ADF)
  - Designed to thwart discovery of information about illegal activities of a user
  - to manipulate, erase, or obfuscate digital data
  - to make its examination difficult, time consuming, or virtually impossible

Anti-Digital-Forensics (ADF)

- ADF techniques can be categorized based upon their intended actions or the effect they have
  - overwriting data and metadata (wiping)
  - hiding/obfuscation data (steganography, cryptography, and low-tech methods)
  - exploitation of bugs in forensic tools.
- Examples
  - Timestomp, slacker, ccleaner etc.
  - Conferences: DEFCON, BlackHat, BlueHat, ToorCon, ShmooCon…

Expert Witness

- One of a computer forensic expert’s most important functions
  - following the procedures of the court
  - testifying the **scientific basis** of findings, analyses, and conclusions in court.
  - demonstrating the **scientific knowledge** associated with their areas of expertise.

Verification ……

- Confirms or dispels the existence of an incident
- Document activities on the electronic devices
  - What kind of incident
  - Which systems directly/indirectly affected
  - What are/were they used for?
    - Criticality
    - sensitivity
  - What is the damage
  - Potential business impact

Verification

- Against
  - Dead System
  - Live System
- Follow policies and procedures
- Gather as much information as possible prior to doing anything

If the system is up and connected

- Should we disconnect it from network?
- Once we confirmed the incident, should we turn the compromised system off?
  - Lose system memory and volatile data
- **Gracefully** shutdown the system vs **forcefully** shutdown

Loss of volatile data when system is off

- System date and time
- A list of the users who are currently logged on
- Open files
- A list of currently running processes
- A list of currently open sockets
- The applications listening on open sockets
- A list of the systems that have current or had recent connections to the system

Forensic Investigation Procedure

- Step 1:
  Establish detailed chain-of-custody!

Chain of Custody

- Maintain a record of how evidence has been handled **from the moment it was collected to the moment it was presented in a court**
  - Who owns it
  - When
  - timeline
  - location of the evidence
- The evidence is stored in a tamper-proof manner

Forensic Investigation Procedure

- Step 2: Working with evidence
  - Acquire the Evidence
  - Authenticate the Evidence
  - Analysis the Evidence
  - Present the Evidence

Acquire evidence

- What is “evidence”?
  - Information processed, stored, or transmitted in binary form that may be relied on in court
  - Data and info about the data
    (files, meta-data, non-filesystem data, anything at all!)

Acquire evidence

- Where to glean evidence?
  - Different cyber crimes result in different types of digital evidence
    - Cyber stalkers: e-mail
    - Computer hackers: malware, backdoors
    - Child pornographers: digitized images, audio files.

Acquire evidence

- How to glean evidence?
  - Acquire volatile data first
    - For example, to acquire network interface info
    - ipconfig /all > myWindowsNetworkSettings.txt
    - ifconfig –a > myUnixNetworkSettings
  - **Bitstream copy** the digital evidence from the hard drives

What is a bitstream copy?

- It is often called a hard drive imaging, bit stream imaging or forensic imaging
- It makes a bit-for-bit copy of all sectors on the media
- It is performed on the hard drive level, therefore ignores the EOF marker.

Examples of copies that are NOT bitstream copies

- *cp, tar, cpio, dump, restore*
- These tools will copy all the content until the End-of-File marker
- They do not copy any deleted data
- They have their place – it’s NOT in forensics!

Examples of bitstream copy

- Examples
  - Unix utility: *dd*
  - *FTK imager*
  - …

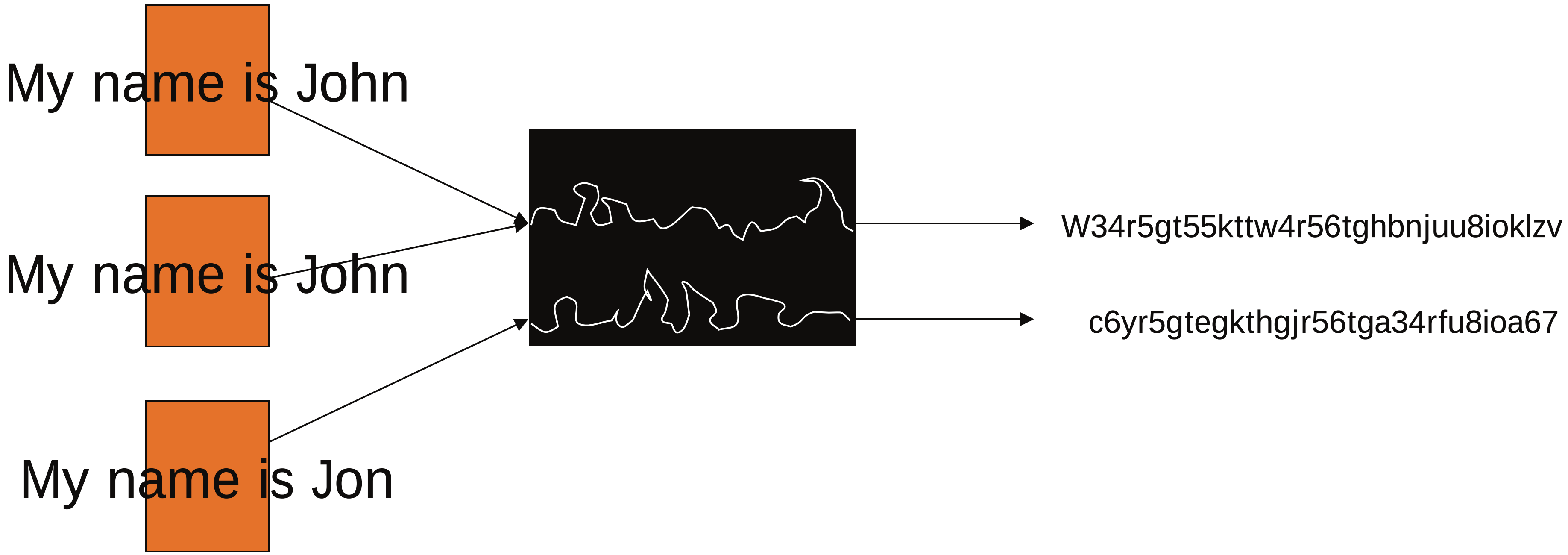
Authenticate the Evidence

- Digital evidence must be preserved in its original state.
- Law requires that evidence be authentic and unaltered.

Cryptographic Hash algorithm for authentication

- What is a cryptographic hash algorithm
  - One-way form of encryption
  - Always produces the same bits for a given data input
  - Collision free algorithm:
    Functionally impossible to create a document that has the same hash value as another document

Cryptographic Hash algorithm (cont’d)



My name is John

My name is John

My name is Jon

W34r5gt55kttw4r56tghbnjuu8ioklzv

c6yr5gtegkthgjr56tga34rfu8ioa67

Commonly used cryptographic hash algorithms

- MD5
- Secure Hash Algorithm (SHA) from NIST
  - SHA-1
  - SHA-2
  - SHA-3

Hash functions used by forensic examiners

- Three ways
  - Preserve evidence:
    verify that evidence is intact and has not changed
  - Conduct a hash analysis:
    match evidence to certain file(s) or group
  - Positively verify that a file has been altered

Analysis

- General steps:
  - Start an analysis by looking at the partition table on the suspect drive
  - Generate a timeline
  - Retrieve deleted files.
  - Check for hidden data
  - Hash analysis
  - Keyword search for terms related to your case
  - Signature Analysis
  - OS specific Media Analysis
    - Glean evidence from Registry
    - Collect information through Recycle bin

Reporting

- The task assigned and a factual statement
- The steps followed, the equipment and methodologies used
- the facts or data
  - Supports the statement
  - Rejects the statement
- Findings and conclusions written
  - Could be used in court
  - Used by your organization

Reporting (cont’d)

- Start your report from beginning
- Include analysis details along with data (recovered files, registry value, keyword search hits, etc.)
- Your statements and conclusion should be stated in an accurately way, useful phrases include
    - “It is my professional opinion...”
    - “The evidence indicates...”
    - “Based on my knowledge…”

Report Outlines by Melia Kelley

- **Title page:** case name, date, investigator name, and contact information
- **Table of Contents**
- **Executive Summary:** high level view of important findings
- **Objectives**
- **Evidence Analyzed:** Serial numbers, hash values, pictures taken at the scene, etc.
- **Steps Taken:** Your results should be reproducible including software and hardware used, and version numbers.
- **Relevant Findings:** Documents of Interest; Internet Activity; Software of Note; USB Devices, etc
- **Timeline:** a concise timeline of important events, possibly using a good graphic
- **Conclusion:** Highlight the important issues in a list of concise findings
- **Signature:** be signed
- **Exhibits:** your curriculum vitae, chain of custody documentation, supporting document linked from the body of the report, etc.
- http://www.forensicmag.com/article/2012/05/report-writing-guidelines

Challenges in Digital Forensics

- Technological progress is making this job harder.
  - Increasing storage densities
  - Cloud Computing
  - Pervasive Encryption
  - Solid State Drive
  - …...

Reference links

- http://www.dfrws.org/ since 2001
  - http://www.dfrws.org/archive/papers
- Volatility foundation/Open Memory Forensics Workshop (OMFW) Since 2008
  - http://www.volatilityfoundation.org/
  - http://www.volatilityfoundation.org/#!omfw/component_74511
- SANS Investigative Forensic Toolkit (SIFT)
  - http://forensics.sans.org/community/downloads/