8. Digital Forensics

I. Investigation Process

1. Identification
    a. Confirm an incident has taken place
    b. Sources of Identification
        i. Victim Reports
        ii. Detections and controls
        iii. Audits
    c. Preparing to respond and collect evidence
        i. Locating
        ii. Preserving
    d. Devine scope and focus efforts
2. Preservation
    a. Ensuring evidence remains intact and unaltered
        i. System is a crime scene
    b. Capture a snapshot of the device current state
        i. Maintain integrity
    c. Identify relevant data
        i. Data volatility
        ii. Data location
    d. Chain of Custody
        i. Document handling of evidence
        ii. Track everyone who had possession
    e. Secure the evidence
        i. Physical and digital security controls
3. Collection
    a. Gather all identified evidence
        i. Primary devices
        ii. Peripherals
    b. Legal authority
        i. Warrant

    ii. Signed consent
    iii. Collection scope
  c. Volatility
    i. Collect evidence before its lost
  d. Data reduction
  e. Documentation
    i. Chain of Custody
4. Examination
  a. Inspect, analyze, interpret evidence
    i. Extract meaningful information from the data
    ii. Draw conclusions
  b. Maintain evidence integrity
    i. Work with forensic images of data
  c. Data extraction and interpretation
    i. Translate raw data into workable human-readable data
  d. Examination Checklist
  e. Data Discovery
    i. Hidden or deleted data
    ii. File carving, file extraction
5. Analysis
  a. Interpret the evidence
    i. How does it support hypothesis
    ii. How does evidence refute hypothesis
    iii. What does info actually mean in context
  b. Data context
    i. Dont analyze in a vacuum
  c. Iteration
    i. Analyze, ask new questions, re-analyze
  d. Relational Analysis
    i. Links between people, places, things
  e. Functional Analysis
    i. How operational configs relate to the incident
  f. Temporal Analysis
    i. Timeline or pattern analysis
6. Presentation
  a. Communicate the results
  b. Ensure findings are communicated clearly
    i. Understood by all technical backgrounds

    c. Guide the audience through the investigation
    d. Executive summaries
        i. Key results
        ii. Significant findings
        iii. Clear explanations
    e. Comprehensive documentation
7. Decision
    a. Evaluate the results
    b. Make a decision
    c. Prosecution

II. The Order of Volatility

Data Acquisition

- Evidence
    - Data that supports or refutes an investigative hypothesis
    - Digital forensic artifacts
    - Evidence is circumstantial
- Evidence Sources
    - Desktops and laptops
    - Smartphones and Tablets
    - Hard Drives and External Storage
    - Servers and VMs
    - Network Devices
    - Cloud Services

CPU Registers and Cache

- Processor registers
    - Fast storage
    - Memory built directly into CPU
    - Holds instructions, storage addresses etc
- Cache memory
    - Returns frequently used instructions and data
    - Helps the CPU process quicker
- Running processes

    - Programs or binaries currently running on the system
    - Paths, command-line invocations, PIDs, hierarchy

RAM and Active Network Connections

- Random Access Memory
    - Short-lived data storage
    - Session data, unsaved documents, process data
- Network connections
    - TCP/UDP connections
    - Open ports
- Routing table
    - Lists the pathways to network destinations
- ARP cache
    - Maps IP addresses to MAC addresses

Temp Files and System Logs

- Temporary files
    - Downloads, temporary configs
    - %TEMP%
    - C:\WINDOWS\Temp
    - /tmp
- Swap files
    - Temporary memory space allocation on disk
- System and application logs
    - Can be overwritten or cleared

Disk Storage Data

- Hard Disk Drives
- Solid State Drives
    - Garbage collection
    - TRIM
- System configs
    - OS components
    - Installed software
    - User files, configs, preferences

    - Documents, executables, backups

Remote Logging

- Endpoint telemetry
    - System, security, application logs etc
    - Historical events
    - Processes, network connections, DNS queries, services
- Centralized log collection
    - Logging server, SIEM, cloud storage
    - Replicated
    - Centralized
    - Log rotation policies

Archive Media

- Long-term Storage Media
    - Backup tapes
    - Optical disks (CDs, DVDs, Blu-rays)
    - Archival hard drives
    - Cloud-based archival storage
- Backups
    - Files
    - Databases
- Security Controls
    - Confidentiality
    - Integrity
    - Availability

III. Chain of Custody

Forensic Data Integrity

- Write Blockers
    - Preserve integrity of storage and devices
    - Hardware or software
    - Prevent write commands that could alter data

    - Analysis should be conducted on forensic images, not original data
- Evidence Bags
    - Contain and protect evidence
    - Tamper-resistant / Tamper-evident
    - Label for documenting case information
- Legal Holds
    - Litigation Hold
    - Preserve relevant case data until resolution
- Documentation
    - Collection procedure, tools, condition, observations

Chain of Custody

https://www.nist.gov/document/sample-chain-custody-formdocx

- Tracks evidence throughout entire investigation
- Documents evidence possession
    - Stakeholders, law enforcement, investigators, examiners
    - Whenever evidence transfers, Chain of Custody entry must be signed
- Storage Conditions
    - Date
    - Time
    - Reason
    - Sending and receiving parties

IV. Windows Forensic Artifacts

Common Artifacts

%SYSTEMROOT%\System32\Config

DEFAULT	HKEY_USERS\.DEFAULT
SAM	HKEY_LOCAL_MACHINE\SAM
SECURITY	HKEY_LOCAL_MACHINE\SECURITY
SOFTWARE	HKEY_LOCAL_MACHINE\SOFTWARE
SYSTEM	HKEY_LOCAL_MACHINE\SYSTEM

%USERPROFILE%

NTUSER.DAT	HKEY_CURRENT_USER
USRCLASS.DAT	HKEY_CURRENT_USER\Software\Classes

C:\Windows\System\32\config\

- DEFAULT
- SAM
- SECURITY
- SYSTEM
- \RegBack\