Lesson 18

Explaining Digital Forensics

Topic 18A

Explain Key Aspects of Digital Forensics Documentation

Syllabus Objectives Covered

- 4.5 Explain the key aspects of digital forensics

Key Aspects of Digital Forensics

- Collecting evidence from computer systems to a standard that will be accepted in a court of law
- Evidence, documentation, and admissibility
  - Latent evidence
  - Collection must be documented
  - Due process
- Legal hold
- Chain of custody
  - Integrity and proper handling of evidence from collection, to analysis, to storage, and finally to presentation

Digital Forensics Reports

- Summarizes contents of the digital data
- Conclusions from the investigator's analysis
- Professional ethics
  - Analysis must be performed without bias
  - Analysis methods must be repeatable
  - Evidence must not be changed or manipulated

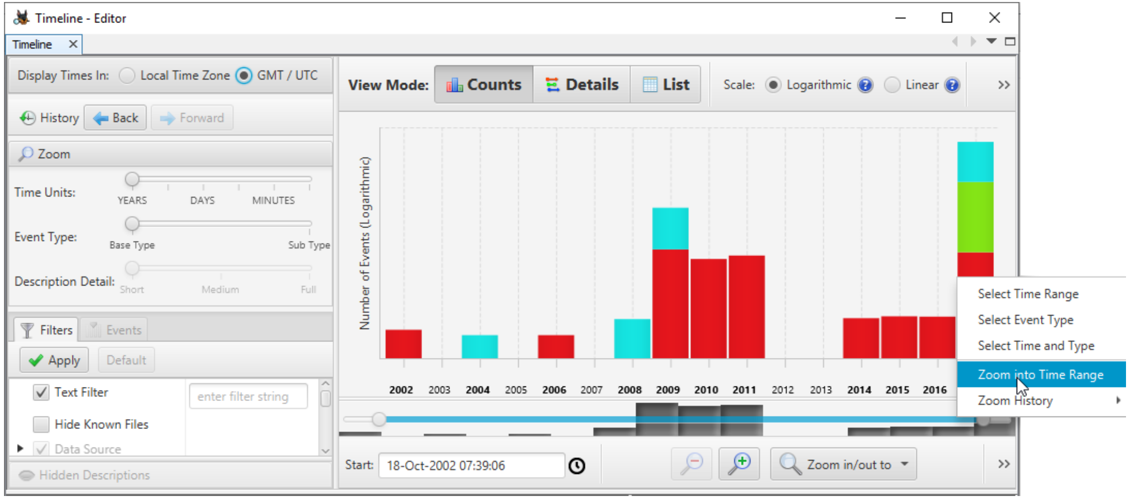
E-discovery

- Electronically Stored Information (ESI)
- Identify and de-duplicate files and metadata
- Search
- Tags
- Security
- Disclosure

Video and Witness Interviews

- Video
  - Record all actions
  - Log/video steps taken
- Witness interviews
  - Informal statements
  - Avoid leading questions
  - Formal questioning

Timelines



Timeline - Editor

Display Times In: ○ Local Time Zone ● GMT / UTC

View Mode: Counts | Details | List

Scale: ● Logarithmic ○ Linear

☑ Text Filter [enter filter string]

□ Hide Known Files

☑ Data Source

Start: 18-Oct-2002 07:39:06

Screenshot: Autopsy - the Sleuth Kit (sleuthkit.org/autopsy.)

- Sequence of events
- Time stamps
  - OS/file system methods for recording time
  - Correct synchronization of local time source
- Time offset
  - Coordinated Universal Time (UTC)
  - Local time
- Date/time settings tampering

Event Logs and Network Traffic

- Collect data from network logging servers
- Packet captures
    - Retrospective Network Analysis (RNA)
- Record collection methods to establish provenance

Strategic Intelligence and Counterintelligence

- Re-examine logs for signs of intrusion
- Counterintelligence
    - Analyze adversary tactics, techniques, and procedures (TTP)
    - Develop better control configurations
- Strategic intelligence
    - Inform risk management and security control provisioning to build mature cybersecurity capabilities

CompTIA Security+ Lesson 18 | Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved. | CompTIA.org

Topic 18B

Explain Key Aspects of Digital Forensics Evidence Acquisition

Syllabus Objectives Covered

- 4.1 Given a scenario, use the appropriate tool to assess organizational security
- 4.5 Explain the key aspects of digital forensics

Data Acquisition and Order of Volatility

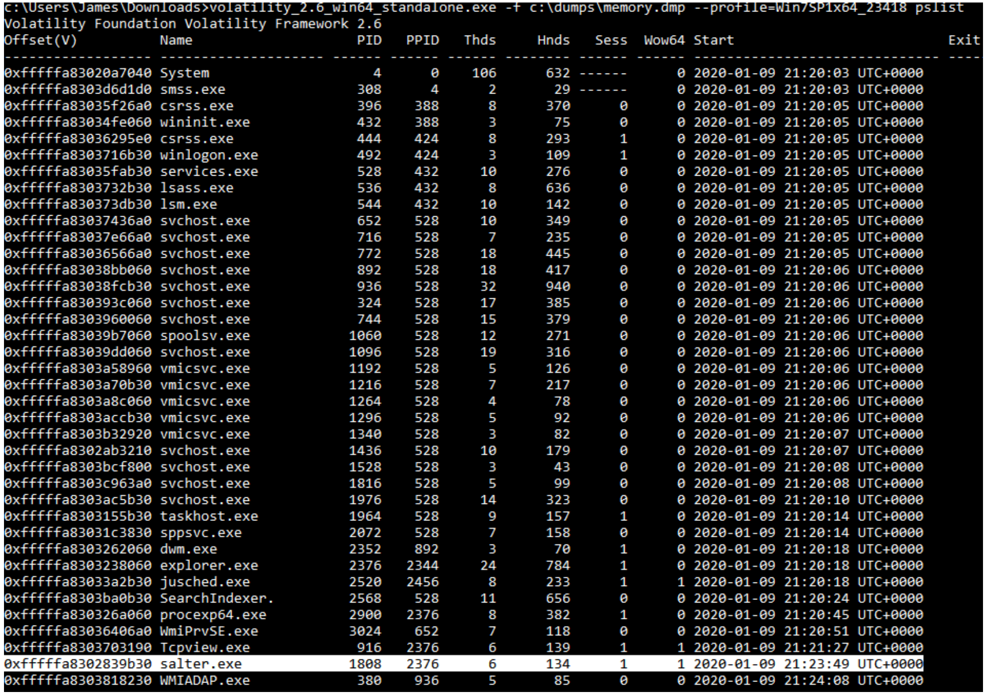
- Legal seizure and search of devices
- Computer on/off state
- Order of volatility
  1. CPU registers and cache memory
  2. Non-persistent system memory (RAM)
  3. Data on persistent storage
     - Partition data and file system artefacts
     - Cached system memory data (pagefiles and hibernation files)
     - Temporary file caches
     - User, application, and OS files and directories
  4. Remote logging and monitoring data
  5. Physical configuration and network topology
  6. Archival media

Digital Forensics Software

- EnCase Forensic and The Forensic Toolkit (FTK)
  - Commercial case management and evidence acquisition and analysis
- The Sleuth Kit/Autopsy
  - Open-source case management and evidence acquisition and analysis
- WinHex
  - Forensic recovery and analysis of binary data
- The Volatility Framework
  - System memory analysis

System Memory Acquisition

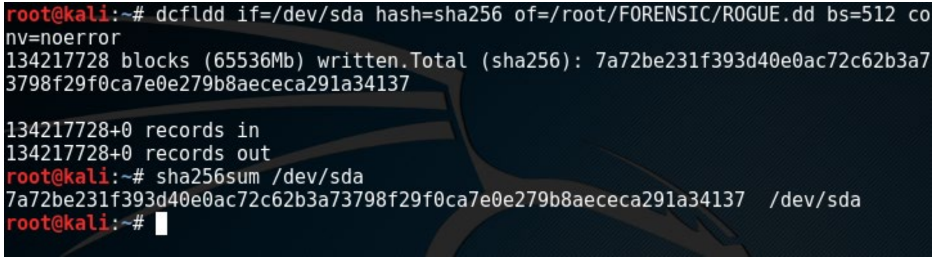
- Evidence recovery from non-persistent memory
  - Contents of temporary file systems, registry data, network connections, cryptographic keys, …
- Live acquisition
  - Pre-install kernel driver
- Crash dump
  - Recover from fixed disk
- Hibernation and page file
  - Recover from fixed disk



```
c:\Users\James\Downloads>volatility_2.6_win64_standalone.exe -f c:\dumps\memory.dmp --profile=Win7SP1x64_23418 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ----
0xfffffa83020a7040 System                    4      0    106      632 ------      0 2020-01-09 21:20:03 UTC+0000
0xfffffa8303d6d1d0 smss.exe                308      4      2       29 ------      0 2020-01-09 21:20:03 UTC+0000
0xfffffa83035f26a0 csrss.exe               396    388      8      370      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83034fe060 wininit.exe             432    388      3       75      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83036295e0 csrss.exe               444    424      8      293      1      0 2020-01-09 21:20:05 UTC+0000
0xfffffa8303716b30 winlogon.exe            492    424      3      109      1      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83035fab30 services.exe            528    432     10      276      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa8303732b30 lsass.exe               536    432      8      636      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa830373db30 lsm.exe                 544    432     10      142      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83037436a0 svchost.exe             652    528     10      349      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83037e66a0 svchost.exe             716    528      7      235      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83036566a0 svchost.exe             772    528     18      445      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83038bb060 svchost.exe             892    528     18      417      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa83038fcb30 svchost.exe             936    528     32      940      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa830393c060 svchost.exe             324    528     17      385      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303960060 svchost.exe             744    528     15      379      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa83039b7060 spoolsv.exe            1060    528     12      271      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa83039dd060 svchost.exe            1096    528     19      316      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303a58960 vmicsvc.exe            1192    528      5      126      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303a70b30 vmicsvc.exe            1216    528      7      217      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303a8c060 vmicsvc.exe            1264    528      4       78      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303accb30 vmicsvc.exe            1296    528      5       92      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303b32920 vmicsvc.exe            1340    528      3       82      0      0 2020-01-09 21:20:07 UTC+0000
0xfffffa8302ab3210 svchost.exe            1436    528     10      179      0      0 2020-01-09 21:20:07 UTC+0000
0xfffffa8303bcf800 svchost.exe            1528    528      3       43      0      0 2020-01-09 21:20:08 UTC+0000
0xfffffa8303c963a0 svchost.exe            1816    528      5       99      0      0 2020-01-09 21:20:08 UTC+0000
0xfffffa8303ac5b30 svchost.exe            1976    528     14      323      0      0 2020-01-09 21:20:10 UTC+0000
0xfffffa8303155b30 taskhost.exe           1964    528      9      157      1      0 2020-01-09 21:20:14 UTC+0000
0xfffffa83031c3830 sppsvc.exe             2072    528      7      158      0      0 2020-01-09 21:20:14 UTC+0000
0xfffffa8303262060 dwm.exe                2352    892      3       70      1      0 2020-01-09 21:20:18 UTC+0000
0xfffffa8303238060 explorer.exe           2376   2344     24      784      1      0 2020-01-09 21:20:18 UTC+0000
0xfffffa83033a2b30 jusched.exe            2520   2456      8      233      1      1 2020-01-09 21:20:18 UTC+0000
0xfffffa8303ba0b30 SearchIndexer.         2568    528     11      656      0      0 2020-01-09 21:20:24 UTC+0000
0xfffffa830326a060 procexp64.exe          2900   2376      8      382      1      0 2020-01-09 21:20:45 UTC+0000
0xfffffa83036406a0 WmiPrvSE.exe           3024    652      7      118      0      0 2020-01-09 21:20:51 UTC+0000
0xfffffa8303703190 Tcpview.exe             916   2376      6      139      1      1 2020-01-09 21:21:27 UTC+0000
0xfffffa8302839b30 salter.exe             1808   2376      6      134      1      1 2020-01-09 21:23:49 UTC+0000
0xfffffa8303818230 WMIADAP.exe             380    936      5       85      0      0 2020-01-09 21:24:08 UTC+0000
```

Screenshot: Volatility Framework volatilityfoundation.org.)

Disk Image Acquisition



```
root@kali:~# dcfldd if=/dev/sda hash=sha256 of=/root/FORENSIC/ROGUE.dd bs=512 co
nv=noerror
134217728 blocks (65536Mb) written.Total (sha256): 7a72be231f393d40e0ac72c62b3a7
3798f29f0ca7e0e279b8aececa291a34137

134217728+0 records in
134217728+0 records out
root@kali:~# sha256sum /dev/sda
7a72be231f393d40e0ac72c62b3a73798f29f0ca7e0e279b8aececa291a34137  /dev/sda
root@kali:~# 
```

- Non-volatile storage media and devices
- Acquisition types
  - Live acquisition
  - Static acquisition by shutting down the host
  - Static acquisition by pulling the plug
- Imaging utilities
  - Forensic software suites and file formats
  - dd

Preservation and Integrity of Evidence

- Provenance
  - Record process of evidence acquisition
  - Use a write blocker
- Data acquisition with integrity and non-repudiation
  - Cryptographic hashing and checksums
  - Take hashes of source device, reference image, and copy of image for analysis
- Preservation of evidence
  - Secure tamper-evident bagging
  - Protection against electrostatic discharge (ESD)
  - Chain of custody
  - Secure storage facility

Acquisition of Other Data

- Network
- Cache
  - File system cache (temporary files)
  - Hardware cache
- Artifacts and data recovery
  - Windows Alternate Data Streams (ADS)
  - File caches (prefetch and Amcache)
  - Slack space and file carving
- Snapshot
  - Acquisition of VM disk images
- Firmware

Digital Forensics for Cloud

- Right to audit clauses
- Limited opportunities for recovery of ephemeral images
    - Ability to snapshot instances
    - Recover log and monitoring data
- Complex chain of custody issues
- Complex regulatory/jurisdiction issues
- Data breach notification laws

Lesson 18

Summary