**Day 4 - Digital Forensics Basics (23.6.)**

**1. Fundamentals & Chain of Custody**

**Topics**

* Definition and scope of **Digital Forensics**
* Key principles: **Immutability**, **Preservation**, **Repeatability**
* **Chain of Custody**: Documentation of evidence handling
* Legal considerations: admissibility, tampering, jurisdiction
* Types of digital evidence: live vs. static, volatile vs. persistent

**Required Infrastructure & Components**

* Chain of custody template or digital evidence log
* Sample evidence images (disk image, memory dump)
* Guidelines from NIST SP 800-101 and ISO/IEC 27037
* Write blockers or simulated tools in lab environment

**To-Dos & Steps**

1. Discuss importance of maintaining evidence integrity
2. Practice documenting an acquisition process using a sample form
3. Compare live acquisition vs. dead box analysis
4. Review common mistakes in evidence handling
5. Role-play: analyst vs. legal examiner reviewing a breach case

**Webinars**:

* [SANS Digital Forensics Fundamentals Webinar (Free On-Demand](https://www.youtube.com/watch?v=YFbbB9cCoaI)) – 00:59
* [Magnet Forensics Webinar](https://www.youtube.com/watch?v=pjj1OO1N424) – 01:02

**YouTube**:

* [What is Chain of Custody in Digital Forensics?](https://www.youtube.com/watch?v=vimQuaC3RYM) – 00:07
* [Introduction to Digital Forensics](https://www.youtube.com/watch?v=giv0DQDSsjQ) – 00:22

**Reading Material**:

* [NIST SP 800-101 Rev. 1: Guidelines on Mobile Device Forensics](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf) – page 15 - 37
* [ISO/IEC 27037: Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence](https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf) *(Summary page) –* page 1- 18
* [National Institute of Justice: Digital Evidence and Forensics](https://nij.ojp.gov/taxonomy/term/digital-evidence-forensics)
* [Chain of Custody Form Template (Sample)](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.nist.gov%2Fsystem%2Ffiles%2Fdocuments%2F2017%2F04%2F28%2FSample-Chain-of-Custody-Form.docx&wdOrigin=BROWSELINK)

**2. Memory, Disk & Network Forensics**

**Topics**

* **Memory Forensics**: RAM analysis, volatile artifacts
* **Disk Forensics**: File systems, deleted files, partition tables
* **Network Forensics**: PCAPs, flow data, session reconstruction
* Key artifacts: browser history, registry hives, log files, timelines

**Required Infrastructure & Components**

* Sample memory dumps (from TryHackMe or Volatility repo)
* Disk images (e.g., E01, DD format)
* PCAP files for network forensic analysis
* Tools: **Volatility**, **Wireshark**, **Autopsy**, **FTK Imager**

**To-Dos & Steps**

1. Analyze a memory dump using Volatility (list processes, connections)
2. Mount and explore a forensic disk image using Autopsy
3. Extract deleted files and search for user activity traces
4. Review PCAP for suspicious sessions and extract transferred files
5. Correlate disk and memory findings in a short summary

**Webinars**:

* [Volatility Framework Webinar Series: Memory Forensics Deep Dive](https://www.dfir.training/video-playlists/introduction-to-memory-forensics) – 00:23
* [SANS Forensics Summit Talk: Memory Forensics Essentials](https://www.youtube.com/watch?v=QzPk1oyzMzc) – 00:36

**YouTube**:

* [Memory Forensics with Volatility](https://www.youtube.com/watch?v=2S_pi9qnIo8) – 00:35
* [PCAP Analysis with Wireshark](https://www.youtube.com/watch?v=qTaOZrDnMzQ) – 00:20
* [Disk Forensics Walkthrough | Autopsy Tutorial](https://www.youtube.com/watch?v=o6boK9dG-Lc&t=92s) – 00:53

**Reading Material**:

* [Volatility Documentation](https://volatility3.readthedocs.io/en/latest/)
* [Wireshark User Guide](https://www.wireshark.org/docs/wsug_html_chunked/)
* [Autopsy User Guide](https://sleuthkit.org/autopsy/docs/user-docs/4.0/)
* [NIST CFReDS Project: Sample Digital Evidence Files](https://www.cfreds.nist.gov/) *(Free practice images)*
* [Memory Analysis Cheat Sheet](https://sansorg.egnyte.com/dl/4QwNVeoj02)

**3. Tools: Volatility, Autopsy, FTK Imager**

**Topics**

* Overview of commonly used forensic tools:
  + **Volatility** (memory analysis)
  + **Autopsy** (GUI-based disk forensics)
  + **FTK Imager** (evidence acquisition & preview)
* Command-line vs. GUI workflows
* Hashing and integrity validation (MD5, SHA1)
* Creating forensic timelines and activity maps

**Required Infrastructure & Components**

* Preinstalled forensic toolkits (or portable versions)
* Training datasets or case images (e.g., NIST CFReDS)
* Hash calculator tools
* Timeline generators (e.g., Plaso/log2timeline)

**To-Dos & Steps**

1. Use FTK Imager to create a forensic image from a given source
2. Validate image integrity with hash comparison
3. Launch Autopsy and explore user activity (recent docs, deleted files)
4. Perform plugin-based analysis in Volatility (malfind, pslist, netscan)
5. Export and document key artifacts from the analysis

**Webinars**:

* [Magnet Forensics: FTK Imager and Autopsy Basics Webinar](https://www.youtube.com/watch?v=8Ro9PU8oSEc) – 00:06
* [SANS DFIR Webcast: Modern Forensics Toolset Overview](https://www.youtube.com/watch?v=w1ygCP2TeCY) – 01:05

**YouTube**:

* [Using FTK Imager for Disk Imaging | Practical Forensics](https://www.youtube.com/watch?v=8Hrz5P2D6CA) – 00:16
* [Complete Guide to Autopsy | CSIRT Tutorials](https://www.youtube.com/watch?v=S6V66G2tVr8) – 00:23
* [Volatility Memory Forensics | Live Walkthrough](https://www.youtube.com/watch?v=Uk3DEgY5Ue8) – 00:32

**Reading Material**:

* [Volatility GitHub Repository (Latest Volatility 3)](https://github.com/volatilityfoundation/volatility3)
* [Autopsy Download (Free and Open Source)](https://www.autopsy.com/download/)
* [FTK Imager User Guide](https://d1kpmuwb7gvu1i.cloudfront.net/Imager/4_7_1/FTKImager_UserGuide.pdf)
* [Plaso (log2timeline) Project: Timeline Analysis](https://plaso.readthedocs.io/en/latest/)

**Afternoon Lab: TryHackMe – Digital Forensics Rooms**

* **Intro to Digital Forensics**: Basic tool use, disk image exploration
* **Linux Forensics**: Investigate compromised Linux system, user activity
* Document evidence trails and interpret system logs
* Hands-on experience with real forensic images and scenarios
* [TryHackMe: Intro to Digital Forensics Room](https://tryhackme.com/)
* [TryHackMe: Linux Forensics Room *(Hands-on disk and memory forensics)*](https://tryhackme.com/)

*Alternative Labs*:

* [Hack The Box – Digital Forensics Challenges](https://www.hackthebox.com/) *(HTB Academy for DFIR labs – subscription needed)*

**🎯 End-of-Day Goal**

Participants should be able to:

* Follow forensic procedures and maintain proper chain of custody
* Acquire and analyze digital evidence from memory, disk, and network sources
* Use key tools like Volatility, Autopsy, and FTK Imager effectively
* Correlate findings to reconstruct incidents
* Produce a short forensics report with validated artifacts