INDEX

CERTIFIED DIGITAL FORENSICS EXAMINER
TRAINING COURSE

Table of contents

I. Detailed agenda of the training course

Day 1 Foundations of digital forensics

Day 2 File system analysis and reverse engineering

- The stack in x86 memory models
- The heap in x86 memory models

Day 3 Malware analysis and threat hunting

Day 4 Advanced forensic analysis and incident response

Day 5 Certification exam

II. Bibliography

Section 2: Introduction to digital forensics

[1[Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd ed. Elsevier, 2011.

[2] Saferstein, Richard. *Forensic Science: From the Crime Scene to the Crime Lab*. 2nd ed. Pearson, 2014.

[3]Scientific Working Group on Digital Evidence (SWGDE). *SWGDE Best Practices for Digital Evidence Collection, Version 1.0*. Approved July 11, 2018. https://www.swgde.org/18-f-002/.

[4] Carrier, Brian. File System Forensic Analysis. Pearson Education, Inc. 2005.

[5] Association of Chief Police Officers (ACPO). *ACPO Good Practice Guide for Digital Evidence. Version 5.0.* ACPO/National Police Chiefs' Council, 2012.

[6] Pollitt, Mark. "A History of Digital Forensics." In Advances in Digital Forensics VI: 6th IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China, January 2010, Revised Selected Papers, edited by Kam-Pui Chow and Sujeet Shenoi, 3–15. Berlin: Springer, 2010. https://doi.org/10.1007/978-3-642-15506-2_1.

[7] National Institute of Justice. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (Washington, DC: U.S. Department of Justice, 2004), https://www.ojp.gov/pdffiles1/nij/199408.pdf.

[8] Ligh, Michael Hale, Andrew Case, Jamie Levy, and AAron Walters. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. John Wiley & Sons, 2014. ISBN 978-1-118-82509-9.

Section 3: Digital forensics tools and techniques

[1] Cellebrite. "UFED Physical Analyzer 7.23: Enhance Your Investigation Management Process With New Tools and Capabilities - Cellebrite." September 5, 2019. https://cellebrite.com/en/productupdates/ufed-physical-analyzer-7-23-enhance-your-investigation-management-process-with-new-tools-and-capabilities/.

[2] Carrier, Brian. *File System Forensic Analysis. Pearson Education*, Inc. 2005.

[3] CGSecurity. TestDisk & PhotoRec Documentation. Last modified 2021. https://www.cgsecurity.org/testdisk_doc/index.html.

[4] Garfinkel, Simson. *Anti-Forensics: Techniques, Detection and Countermeasures*. Paper presented at the 1st USENIX Workshop on Offensive Technologies (WOOT '07), Boston, MA, 2007. https://calhoun.nps.edu/server/api/core/bitstreams/08673dae-fa60-40ff-a68d-00ab96d222fb/content.

[5] Harris, Ray. *Arriving at an Anti-Forensics Consensus: Examining How to Define and Control the Anti-Forensics Problem*. Presented at the Digital Forensic Research Workshop (DFRWS), 2006. https://dfrws.org/sites/default/files/session-files/2006_USA_pres-arriving_at_an_anti-forensics_consensus_-_examining_how_to_define_and_control_the_anti-forensics_problem.pdf.

[6] Microsoft Learn "NTFS Overview." https://learn.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview.
[7] Exterro, 2024. *Forensic Toolkit (FTK) User Guide*. https://d1kpmuwb7gvu1i.cloudfront.net/8.x/8.0.0/Doc/Exterro_FTK_8.0-User_Guide.pdf.
[8] Microsoft Learn. "Overview of FAT, HPFS, and NTFS File Systems - Windows Client." https://learn.microsoft.com/en-us/troubleshoot/windows-client/backup-and-storage/fat-hpfs-and-ntfs-file-systems.
[9] Apple Inc. APFS Overview: Introduction. Last modified June 4, 2018. https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/APFS_Guide/Introduction/Introduction.html#//apple_ref/doc/uid/TP40016999-CH1-DontLinkElementID_15.
[10] Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd ed. Elsevier, 2011.
[11] Microsoft Learn. "Registry." https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry.
[12] Microsoft Learn "Event Logging." Last modified January 1st, 2021. https://learn.microsoft.com/en-us/windows/win32/eventlog/event-logging.
[13] Microsoft Learn. "Windows Event Viewer." Last modified February 15, 2022. https://learn.microsoft.com/en-us/host-integration-server/core/windows-event-viewer1.
[14] Carvey, Harlan. 2018. *Investigating Windows Systems*. Elsevier 2018.
[15] The Linux Documentation Project. *Guides*. https://tldp.org/guides.html.
[16] GNU Bash Manual - GNU Project - Free Software Foundation, n.d. https://www.gnu.org/software/bash/manual/.
[17] Apple Inc. *Property List Programming Guide: Introduction to Property Lists*. Last modified March 24, 2010. https://developer.apple.com/library/archive/documentation/Cocoa/Conceptual/PropertyLists/Introduction/Introduction.html#//apple_ref/doc/uid/10000048-CJBGDEGD.
[18] Apple Inc. "Logging." Apple Developer Documentation. Last modified 2021. https://developer.apple.com/documentation/os/logging.
[19] Edwards, Sarah. "New macOS Sierra (10.12) Forensic Artifacts – Introducing Unified Logging." *mac4n6*. November 13, 2016. https://www.mac4n6.com/blog/2016/11/13/new-macos-sierra-1012-forensic-artifacts-introducing-unified-logging.
[20] Apple Support. "About Time Machine Local Snapshots - Apple Support," March 18, 2025. https://support.apple.com/en-us/HT204015.

Section 4: Network analysis with Wireshark

[1] Sharpe, Richard, Ed Warnicke, and Ulf Lamping Lamping. "Wireshark User's Guide," n.d. Version 4.5.0. https://www.wireshark.org/docs/wsug_html_chunked/.
[2] Tcpdump/Libpcap. Tcpdump & Libpcap Project. Accessed July 29, 2025. https://www.tcpdump.org/.

[3] Bejtlich, Richard. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. *No Starch Press*, 2013.

Section 5: Network analysis with Zeek

[1] Zeek Project. “About Zeek.” n.d. https://docs.zeek.org/en/master/about.html.

Section 6: File system forensics

[1] Carrier, Brian. File System Forensic Analysis. Addison-Wesley Professional, 2005.
[2] Maskel Ryan, “File systems explained”. Last updated February 14, 2022. https://winbuzzer.com/2021/06/30/filesystems-explained-whats-the-difference-between-fat32-ntfs-exfat-hfs-and-ext4-xcxwbt/
[3] SleuthKit. “Open Source Digital Forensics.” SleuthKit. Accessed December 12, 2024. https://www.sleuthkit.org/

Section 8: Reverse engineering in Windows (PE files)

[1] Microsoft. “PE Format.” Windows Dev Center: Win32 Apps Documentation. Last modified June 29, 2022. Accessed August 19, 2025. https://learn.microsoft.com/en-us/windows/win32/debug/pe-format.
[2] Tambe, Shreyash. “Mastering Malware Analysis: Exploring PE Header, Static and Dynamic Malware Analysis.” Medium, October 31, 2023. Accessed [date you accessed the page]. https://medium.com/@shreyash_tambe/mastering-malware-analysis-305b1c5efc27.

Section 9: Reverse engineering in Linux (ELF files)

[1] Abissa. “Understanding the ELF Format: A Comprehensive Guide.” *Medium*, November 2, 2023. Accessed August 19, 2025. https://medium.com/@abissazaki133/understanding-the-elf-format-a-comprehensive-guide-bab04997001e.
[2] Linux Programming Training. Accessed August 19, 2025. https://man7.org/linux/man-pages/man5/elf.5.html
[3] Packt. “Reverse Engineering a Linux Executable: Hello World.” *Codementor*, April 12, 2017. Accessed August 19, 2025. https://www.codementor.io/@packt/reverse-engineering-a-linux-executable-hello-world-rjceryk5d.
[4] 4objdump. Accessed August 19, 2025. https://sourceware.org/binutils/docs/binutils/objdump.html
[5] Linux Programming Training. Accessed August 19, 2025. https://man7.org/linux/man-pages/man1/readelf.1.html
[6] x86 Assembly Guide. *Virginia Education*, Accessed August 19, 2025. https://www.cs.virginia.edu/~evans/cs216/guides/x86.html

Section 11: Malware analysis

[1] Sikorski, Michael, and Andrew Honig. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press, 2012

[2] VirusTotal. VirusTotal – Free Online Virus, Malware, and URL Scanner. https://www.virustotal.com/gui/home/upload.

[3] Cuckoo Sandbox. Cuckoo Malware Analysis System. Last modified 2023. https://cuckoo.cert.ee/.

[4] Rekall Project. *Rekall Memory Forensic Framework Documentation*. Version 1.7.2. Last modified July 29, 2025. https://rekall.readthedocs.io/_/downloads/en/latest/pdf/.

[5] The Volatility Foundation. "The Volatility Framework," 2007. https://volatilityfoundation.org/the-volatility-framework/.

[6] Egele, Manuel, Theodoor Scholte, Engin Kirda, and Christopher Kruegel. "A Survey on Automated Dynamic Malware-analysis Techniques and Tools." *ACM Computing Surveys 44*, no. 2. February, 2012: 1–42. https://doi.org/10.1145/2089125.2089126.

[7] NationalSecurityAgency. "GitHub - NationalSecurityAgency/Ghidra: Ghidra Is a Software Reverse Engineering (SRE) Framework." *GitHub*, n.d. https://github.com/NationalSecurityAgency/ghidra?tab=readme-ov-file.

Section 12: Advanced malware analysis techniques

[1] Fortinet. "What Is Malware Analysis?" n.d. https://www.fortinet.com/resources/cyberglossary/malware-analysis.

[2] Microsoft Threat Intelligence. "Analyzing Solorigate, the Compromised DLL File That Started a Sophisticated Cyberattack, and How Microsoft Defender Helps Protect Customers." Microsoft Security, December 18, 2020. https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/.

Section 14: YARA rule development for threat hunting

[1] Cymulate. "YARA Rules." https://cymulate.com/cybersecurity-glossary/yara-rules/#:~:text=YARA%20rules%20provide%20an%20open,and%20support%20proactive%20threat%20hunting.

III. List of acronyms

ACL: Access Control List
ACPO: Association of Chief Police Officers
ADS: Alternate Data Streams
AFF: Advanced Forensic Format
APFS: Apple File System
APT: Advanced Persisten Threats
BPF: Berkeley Packet Filter
CDFE: Certified Digital Forensic Examiner
DKOM: Direct Kernel Object Manipulation
E01: Expert Witness Format
EFL: Executable and Linkable Format
FAT: File Allocation Table
GPR: General-Purpose Registers
HFS+: Hierarchical File System Plus
HPA: Host Protected Ares
IACIS: International Association of Computer Investigative Specialists
IOC: Indicator Of Compromise
ISA: Instruction Set Architecture
ISFCE: International Society of Forensic Computer Examiners
LA: Lead Auditor
LI: Lead Implementer
MFT: Master File Table
MLAT: Mutual Legal Assistance Treaty
NTFS: New Technology File System
OPSEC: Operational Security
OS: Operating System
PE: Portable Executable
PECB: Professional Evaluation and Certification Board
SWGDE: Scientific Working Group on Digital Evidence
SWOT: Strengths, Weaknesses, Opportunities, and Threats
TIP: Threat Intelligence Platform
Tor: The Onion Router
VM: Virtual Machine
zkg: Zeek Package Manager