Training Course on Memory Forensics for Malware Detection and Extraction

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's advanced cybersecurity landscape, memory forensics has emerged as a critical skill in identifying sophisticated malware threats, detecting zero-day exploits, and conducting in-depth incident response. Training Course on Memory Forensics for Malware Detection and Extraction is a comprehensive, hands-on program that equips cybersecurity professionals with the tools and knowledge needed to extract volatile data from memory, analyze it for indicators of compromise (IOCs), and isolate advanced persistent threats (APTs). Using industry-standard tools like Volatility, Rekall, and Redline, participants will master real-world techniques to detect rootkits, ransomware, fileless malware, and stealthy backdoors.

With growing threats targeting memory-resident payloads, traditional disk-based forensics is no longer sufficient. This course fills a critical gap by diving deep into RAM analysis, malware behavior analytics, and live memory extraction techniques. Through a combination of theory and hands-on labs, participants will engage with real-world case studies from cybercrime, nation-state attacks, and ransomware incidents. This course is ideal for digital forensics investigators, malware analysts, SOC analysts, and cybersecurity practitioners looking to strengthen their incident response capabilities using memory forensics.

Programme Curriculum

Training Course on Memory Forensics for Malware Detection and Extraction

Introduction

In today's advanced cybersecurity landscape, memory forensics has emerged as a critical skill in identifying sophisticated malware threats, detecting zero-day exploits, and conducting in-depth incident response. Training Course on Memory Forensics for Malware Detection and Extraction is a comprehensive, hands-on program that equips cybersecurity professionals with the tools and knowledge needed to extract volatile data from memory, analyze it for indicators of compromise (IOCs), and isolate advanced persistent threats (APTs). Using industry-standard tools like Volatility, Rekall,

and Redline, participants will master real-world techniques to detect rootkits, ransomware, fileless malware, and stealthy backdoors.

With growing threats targeting memory-resident payloads, traditional disk-based forensics is no longer sufficient. This course fills a critical gap by diving deep into RAM analysis, malware behavior analytics, and live memory extraction techniques. Through a combination of theory and hands-on labs, participants will engage with real-world case studies from cybercrime, nation-state attacks, and ransomware incidents. This course is ideal for digital forensics investigators, malware analysts, SOC analysts, and cybersecurity practitioners looking to strengthen their incident response capabilities using memory forensics.

Course Objectives

1. Understand the fundamentals of memory architecture and how malware interacts with volatile memory.
2. Perform live memory acquisition using industry-standard tools.
3. Utilize Volatility and Rekall frameworks to analyze memory dumps effectively.
4. Identify and extract fileless malware from RAM dumps.
5. Detect stealth malware such as rootkits and injected DLLs.
6. Analyze process hollowing, code injection, and reflective DLL loading.
7. Recognize and reconstruct command-and-control (C2) activities in memory.
8. Trace malware persistence mechanisms via registry and memory hooks.
9. Extract encryption keys and malware configuration data from volatile memory.
10. Build a malware detection pipeline using automated memory scanning scripts.
11. Correlate memory indicators of compromise (IOCs) with host-based data.
12. Practice real-time triage of compromised endpoints using memory forensics.
13. Create comprehensive forensics reports for legal or compliance use.

Target Audience

1. Digital Forensics Investigators
2. SOC Analysts and Threat Hunters
3. Incident Response Teams
4. Malware Analysts
5. Cybersecurity Engineers
6. Penetration Testers
7. Law Enforcement & Intelligence Analysts
8. Cybersecurity Students and Enthusiasts

Course Duration: 10 days

Course Modules

Module 1: Introduction to Memory Forensics

- Role of memory in digital investigations
- Types of malware in memory
- Volatile vs non-volatile data
- Importance of live analysis
- Tools overview: Volatility, Redline, Rekall
- **Case Study**: Ransomware detection via live RAM analysis

Module 2: Memory Acquisition Techniques

- Memory acquisition principles
- Windows, Linux, and macOS memory dump techniques
- Live acquisition risks and ethics

- Use of DumpIt, FTK Imager, Belkasoft RAM Capturer
- Anti-forensics techniques used by attackers
- **Case Study**: Acquiring memory in a suspected data breach

Module 3: Volatility Framework Essentials

- Volatility installation and plugin ecosystem
- Navigating memory images
- Process and thread analysis
- Detecting hidden processes
- Automating analysis with plugins
- **Case Study**: Rootkit detection using Volatility

Module 4: Detecting Fileless Malware

- Fileless malware behavior and lifecycle
- Memory-resident payloads
- Registry-based persistence
- PowerShell abuse and WMI persistence
- Detection strategies using memory forensics
- **Case Study**: Fileless malware in enterprise network

Module 5: Process Hollowing and Code Injection

- Process injection techniques explained
- Indicators of process hollowing in memory
- PE header manipulation
- Suspicious parent-child relationships
- Detecting hollowed processes using Volatility
- **Case Study**: Detection of Emotet variant via code injection

Module 6: Advanced Memory Structures

- Understanding page tables and kernel memory
- Kernel object manipulation
- Parsing memory pools and session memory
- Kernel-mode vs user-mode malware
- Virtual address space analysis
- **Case Study**: Kernel-mode rootkit evasion technique

Module 7: Analyzing Windows Artifacts in RAM

- Extracting registry hives from memory
- Parsing SAM, SYSTEM, and NTUSER.DAT
- Extracting user activities
- Locating clipboard, MRU, and shell bags
- Registry-based malware persistence
- **Case Study**: Identifying credential harvesting malware

Module 8: Rekall Framework Overview

- Differences from Volatility
- Interactive GUI usage
- Timeline analysis in Rekall
- Rekall plugins for malware detection
- Custom analysis workflows

- **Case Study**: Use of Rekall to map attacker's timeline

Module 9: Memory Analysis for Linux and macOS

- Linux memory structure basics
- Capturing and analyzing Linux RAM
- macOS forensic artifacts in memory
- Tools: LiME, Mac Memory Reader
- Identifying ELF-based malware
- **Case Study**: Linux crypto-miner in compromised cloud server

Module 10: Credential and Key Extraction

- Extracting passwords and hashes from memory
- Accessing LSASS and dumping credentials
- Gaining access to encrypted malware config
- Key extraction from RAM for ransomware samples
- Legal and ethical considerations
- **Case Study**: Extracting ransomware decryption keys

Module 11: Real-Time Memory Triage

- Memory triage vs full memory analysis
- Fast IOC detection in RAM
- Process scoring for suspicious activity
- Automation with scripts
- Incident response decision-making
- **Case Study**: Triage of a breached workstation in real time

Module 12: Malware Configuration Extraction

- Understanding config storage in memory
- Detecting malware C2 addresses
- Pulling out obfuscated configurations
- Config decoder scripts
- Analyzing P2P botnets
- **Case Study**: Zeus banking trojan configuration dump

Module 13: Reporting and Legal Readiness

- Creating chain-of-custody documentation
- Writing effective forensic reports
- Including screenshots, memory maps, hash values
- Addressing legal admissibility
- Redacting sensitive data
- **Case Study**: Report submitted to law enforcement for prosecution

Module 14: Integration with SOC Tools

- Memory forensics in SIEM environments
- Using memory IOCs in threat intelligence
- Correlation with EDR and XDR systems
- Integrating memory forensics into playbooks
- Alert prioritization using volatile evidence
- **Case Study**: SIEM-assisted memory investigation in large org

Module 15: Final Lab and Capstone Project

- Multi-platform memory analysis challenge
- Memory acquisition and full Volatility scan
- Malware extraction and classification
- Forensic report presentation
- Peer feedback and expert evaluation
- **Case Study**: Full analysis of APT attack on hospital network

Training Methodology

- Hands-on labs with memory dumps from real incidents
- Instructor-led walkthroughs and live demonstrations
- Interactive quizzes and scenario-based challenges
- Downloadable scripts and toolkits for offline practice
- Final capstone project with peer review and certification

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com