Training Course on Memory Forensics, Volatile Data Acquisition and Analysis

Professional Development Training Course Outline

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

Course Introduction

Introduction

In the rapidly evolving landscape of cybersecurity and digital forensics, the ability to effectively analyze volatile data residing in a computer's Random Access Memory (RAM) has become an indispensable skill. Training Course on Memory Forensics, Volatile Data Acquisition and Analysis provides an intensive, hands-on experience in understanding and leveraging memory artifacts to uncover sophisticated malware infections, advanced persistent threats (APTs), and stealthy attacker activities that often leave minimal traces on disk-based evidence. Participants will delve into live system forensics, mastering the techniques to forensically acquire memory dumps and meticulously analyze them for crucial indicators of compromise (IOCs) and threat intelligence.

This comprehensive program will guide attendees through the intricacies of Windows, Linux, and macOS memory internals, equipping them with proficiency in industry-leading open-source tools like the Volatility Framework and commercial solutions for memory acquisition and analysis. From identifying hidden processes and injected code to extracting network connections, registry hives, and decrypted data, the course emphasizes practical application and real-world scenarios. By the end of this training, participants will be empowered to conduct in-depth memory investigations, significantly enhancing their capabilities in incident response, threat hunting, and malware analysis within any organizational environment.

Programme Curriculum

Training Course on Memory Forensics, Volatile Data Acquisition and Analysis

Introduction

In the rapidly evolving landscape of cybersecurity and digital forensics, the ability to effectively analyze volatile data residing in a computer's Random Access Memory (RAM) has become an indispensable skill. Training

Course on Memory Forensics, Volatile Data Acquisition and Analysis provides an intensive, hands-on experience in understanding and leveraging memory artifacts to uncover sophisticated malware infections, advanced persistent threats (APTs), and stealthy attacker activities that often leave minimal traces on disk-based evidence. Participants will delve into live system forensics, mastering the techniques to forensically acquire memory dumps and meticulously analyze them for crucial indicators of compromise (IOCs) and threat intelligence.

This comprehensive program will guide attendees through the intricacies of Windows, Linux, and macOS memory internals, equipping them with proficiency in industry-leading open-source tools like the Volatility Framework and commercial solutions for memory acquisition and analysis. From identifying hidden processes and injected code to extracting network connections, registry hives, and decrypted data, the course emphasizes practical application and real-world scenarios. By the end of this training, participants will be empowered to conduct in-depth memory investigations, significantly enhancing their capabilities in incident response, threat hunting, and malware analysis within any organizational environment.

Course Duration

10 Days

Course Objectives

1. Master volatile data acquisition techniques from live Windows, Linux, and macOS systems.
2. Utilize the Volatility Framework for comprehensive memory image analysis across various operating systems.
3. Identify and analyze active and terminated processes within memory dumps.
4. Detect hidden processes and injected code indicating advanced malware activity.
5. Extract network connection artifacts and open sockets for C2 communication analysis.
6. Perform registry hive analysis from memory to uncover system configuration changes and user activity.
7. Recover user credentials, encryption keys, and other sensitive data from RAM.
8. Analyze kernel structures and modules to detect rootkits and kernel-level compromise.
9. Investigate application-specific memory artifacts for targeted evidence collection.
10. Correlate memory forensics findings with other digital evidence sources for holistic investigations.
11. Generate comprehensive reports detailing memory forensics findings and their implications.
12. Develop custom Volatility plugins or scripts for specialized analysis needs.
13. Stay current with evolving memory forensics techniques and anti-forensic measures.

Organizational Benefits

1. Enhanced Incident Response Capability: Rapidly identify and contain advanced threats.
2. Deeper Threat Visibility: Uncover stealthy malware and sophisticated attacker techniques.
3. Improved Threat Hunting: Proactively detect hidden compromises within the network.
4. Reduced Mean Time to Detect (MTTD): Quicker identification of security incidents.
5. More Accurate Root Cause Analysis: Pinpoint the origin and extent of breaches.
6. Better Data Breach Assessment: Understand what sensitive data was in memory during an attack.
7. Stronger Cybersecurity Posture: Proactive defense based on advanced threat understanding.
8. Internal Expertise Development: Build a highly skilled in-house memory forensics team.

9. Cost Savings: Reduce reliance on external forensic consultants for complex investigations.
10. Legal Defensibility: Collect and preserve volatile evidence critical for legal proceedings.

Target Participants

- Digital Forensic Investigators
- Incident Response Team Members
- Cybersecurity Analysts
- Malware Analysts
- Threat Hunters
- Security Operations Center (SOC) Analysts
- System Administrators with security responsibilities
- Reverse Engineers
- Law Enforcement Digital Evidence Specialists

Course Outline

Module 1: Introduction to Memory Forensics & Volatile Data

- **Volatile vs. Non-Volatile Data:** Understanding the ephemeral nature of RAM.
- **Why Memory Forensics Matters:** Uncovering stealthy threats, rootkits, fileless malware.
- **Memory Acquisition Principles:** Minimizing impact, chain of custody for volatile data.
- **Memory Structures Overview:** Virtual memory, paging, kernel vs. user space.
- **Case Study:** Discussing a real-world scenario where memory forensics was crucial for a breach investigation.

Module 2: Memory Acquisition Tools and Techniques

- **Windows Memory Acquisition:** DumpIt, WinPMem, FTK Imager Lite (memory acquisition feature).
- **Linux Memory Acquisition:** LiME, fmem, acquiring from virtual machines.
- **macOS Memory Acquisition:** Specific tools and challenges for Apple systems.
- **Cloud & Container Memory Acquisition:** Conceptual approaches for volatile data in cloud environments.
- **Case Study:** Practicing memory acquisition from a live Windows virtual machine and a Linux server.

Module 3: Introduction to the Volatility Framework

- **Volatility Installation & Setup:** Kali Linux, REMnux, and standalone installations.
- **Image Identification & Profile Selection:** Using `imageinfo` to determine OS and architecture.
- **Basic Volatility Commands:** `pslist`, `pstree`, `dlllist`, `connscan`.
- **Volatility Plugin Architecture:** Understanding how plugins work and extending functionality.

- **Case Study:** Initial triage of a suspect memory dump using core Volatility plugins.

Module 4: Process Analysis & Execution Tracing

- **Hidden Processes Detection:** psxview, apihooks, and other techniques to uncover stealthy processes.
- **Process Injections & DLL Analysis:** Identifying malicious code injection and loaded DLLs.
- **Parent-Child Relationships:** Tracing execution flows (pstree, psscan).
- **Process Environment Blocks (PEB) & Process Heap Analysis:** Gaining insights into process state.
- **Case Study:** Identifying a process injecting malicious code into a legitimate application.

Module 5: Network Artifacts & Communication Analysis

- **Active Network Connections:** netscan, sockscan for open ports and connections.
- **DNS Cache Analysis:** dnscache to uncover resolved malicious domains.
- **Raw Socket Data Extraction:** Capturing data from network buffers.
- **Identifying C2 Channels:** Recognizing patterns of command and control communication.
- **Case Study:** Tracing malware's outbound connections and identifying C2 server IP addresses.

Module 6: Registry Forensics from Memory

- **Registry Hive Recovery:** Extracting SAM, SECURITY, SYSTEM, NTUSER.DAT from RAM.
- **Startup Programs & Persistence:** autoruns plugin for identifying malware persistence mechanisms.
- **User Activity in Registry:** shellbags, userassist, shimcache from memory.
- **Deciphering Registry Keys:** Understanding common forensic artifacts within the registry.
- **Case Study:** Uncovering evidence of user execution of a malicious file that was subsequently deleted from disk.

Module 7: Malware Triage & Signature Detection in Memory

- **Malware Detection Techniques:** malfind, yarascan for pattern matching in memory.
- **Extracting Executables from Memory:** procdump, moddump for analysis.
- **Packed Malware Identification:** Recognizing indicators of packed or obfuscated code.
- **Rootkit Detection:** apihooks, driverirp for kernel-level compromise.
- **Case Study:** Identifying a fileless malware implant active in system memory.

Module 8: Kernel & Driver Analysis

- **Kernel Structures Overview:** EPROCESS, KTHREAD, MM_VAD.
- **Loaded Drivers & Modules:** modules, driverscan for suspicious kernel modules.
- **Direct Kernel Object Manipulation (DKOM):** Detecting rootkit techniques.
- **Interrupt Descriptor Table (IDT) & Hooking:** Identifying system call table modifications.
- **Case Study:** Uncovering a kernel-mode rootkit attempting to hide processes and files.

Module 9: Password & Credential Extraction

- **LSASS Process Analysis:** Extracting cleartext passwords and hashes from Windows memory.
- **DPAPI Master Key Recovery:** Decrypting protected data.
- **Browser Credential Extraction (from memory):** Recovering login details from running browser processes.
- **Encryption Keys & Certificates:** Identifying cryptographic material in memory.

- **Case Study:** Recovering user account passwords from a compromised domain controller's memory dump.

Module 10: File Carving & Data Extraction from Memory

- **Memory Carving Principles:** Extracting files from raw memory buffers.
- **Specific File Type Carving:** Documents, images, executables, scripts from RAM.
- **Data Reconstruction:** Piecing together fragmented data found in memory.
- **Clipboard & Screenshot Analysis:** Recovering sensitive data copied to clipboard or screen.
- **Case Study:** Extracting sensitive documents or images that were open in an application at the time of memory acquisition.

Module 11: Advanced Volatility Features & Plugins

- **Command Line History & Console Output:** cmdscan, consoles for attacker commands.
- **Shellbags & User Activity:** Reconstructing user interactions with files and folders.
- **VAD Tree Analysis:** Understanding process memory layout and suspicious regions.
- **Custom Volatility Plugin Development (Basic):** Introduction to extending Volatility.
- **Case Study:** Using advanced plugins to identify post-exploitation activities and attacker tools.

Module 12: Linux Memory Forensics Deep Dive

- **Linux Kernel Internals for Forensics:** Process management, memory layout.
- **Linux Memory Acquisition Tools:** LiME, fmem and their usage.
- **Volatility for Linux Analysis:** Specific plugins for Linux memory dumps.
- **Process, Network, and File System Artifacts on Linux:** Key differences from Windows.
- Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

Register Online Now

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