CONCEPT

Memory Forensics and Malware Analysis: Volatility 3, YARA and Windows Timelines

3 – 7 May 2027
Dubai - Five-star CBD venue



Memory Forensics and Malware Analysis: Volatility 3, YARA and Windows Timelines

Ref: 468_14381 **Date:** 3 – 7 May 2027 **Location:** Dubai - Five-star CBD venue **Fees:** 21450 SAR

Introduction:

Memory forensics and malware analysis decide whether an intrusion is scoped correctly or only partly cleaned up. Many response teams still reimage a host before capturing RAM, miss injected code that never touched the disk, and pass vague hashes to the SOC instead of detections that survive a recompile. This Core Concept course gives examiners a repeatable lab routine: acquire volatile data, analyse memory images with Volatility 3, rebuild a Windows timeline and triage suspicious binaries safely in an isolated sandbox. Participants produce a Compromised Host Examination Report and Detection Handover Pack.

Course Objectives:

- Acquire RAM and other volatile data from a live Windows host in order of volatility while recording hashes and examiner notes
- Analyse memory images with Volatility 3 plugins to identify rogue processes, injected code, network connections and persistence
- Reconstruct attacker activity from Windows registry, event log, prefetch and file system artefacts in a merged super-timeline
- Triage suspicious binaries through static properties and behaviour observed in an isolated sandbox, without running samples on production systems
- Convert examination findings into indicators of compromise and YARA rules that the SOC can deploy and test
- Write an examination report that states findings, confidence and limitations for technical and management readers

Target Audience:

- Incident responders who contain compromised endpoints and must decide what to collect before remediation
- SOC analysts at escalation tier who investigate alerts that point to hands-on-keyboard intrusion
- Forensic examiners who process host images and memory captures for internal cases
- Detection engineers who turn examination findings into endpoint and network detection content
- Threat intelligence analysts who enrich indicators from recovered samples and share them with defenders

Course Outline:

Day 1: DFIR Process, Evidence Integrity and Lab Setup

- NIST SP 800-86 Collection, Examination, Analysis and Reporting Phases
- Order of Volatility and First Responder Decision Checklist
- Evidence Hashing, Examiner Notes and Custody Log for Host Captures
- Isolated Analysis Lab Build: Snapshots, Host-Only Networking and Sample Handling Rules
- Compromised Host Readiness Review: Telemetry, Retention and Collection Tooling Gaps

Day 2: Volatile Data Acquisition and Memory Analysis with Volatility 3

- Live RAM Capture, Hibernation Files and Crash Dumps as Memory Sources
- Volatility 3 Symbol Tables, Plugin Structure and Image Validation
- Process Listing Cross-Check: pslist, psscan and pstree Discrepancies
- Network Sockets, Command Lines and Loaded DLL Review in Memory
- Code Injection and Hollowed Process Detection with malfind

Day 3: Windows Artefacts and Super-Timeline Analysis

- Registry Hives: Run Keys, Services, ShimCache and Amcache Evidence
- Windows Event Log Channels for Logon, Process Creation and Service Installation
- Prefetch, LNK Files and Jump Lists as Execution Evidence
- NTFS Master File Table, USN Journal and Timestamp Manipulation Checks
- Super-Timeline Build with log2timeline and Plaso Filtering Techniques

Day 4: Malware Triage for Defenders and Detection Content

- Static Property Review: PE Headers, Imports, Strings, Entropy and Packer Signs
- Sandbox Behaviour Observation: Process Tree, File, Registry and Network Activity
- Anti-Analysis and Sandbox Evasion Indicators and How to Record Them
- Indicator of Compromise Extraction, Quality Rating and Pyramid Placement
- YARA Rule Writing, False Positive Testing and YARA-X Compatibility

Day 5: Examination Lab Case and the Detection Handover Pack

- Mobile Device Forensics Overview: Acquisition Types, Backups and App Data Limits
- Lab Case: Credential Theft Host with Memory-Resident Loader
- Lab Case: Persistence Hunt Across Registry, Services and Scheduled Tasks
- Compromised Host Examination Report Drafting with Confidence Statements
- Detection Handover Pack Review: Indicators, YARA Rules and SOC Hunting Queries

Skills You Will Gain:

- Volatile Data Acquisition
- Memory Image Analysis
- Windows Artefact Interpretation
- Timeline Reconstruction
- Static Malware Triage
- Sandbox Behaviour Analysis
- Detection Rule Authoring
- Forensic Report Writing

Why Attend This Course:

- Return with a Compromised Host Examination Report and Detection Handover Pack built from a full lab case
- Spend most of each day on keyboard with memory images, disk artefacts and lab samples rather than slides
- Find injected code and persistence that disk-only examination and antivirus scans overlook
- Compare examination practice with responders and examiners from finance, energy, telecoms and public service teams

Conclusion:

An intrusion is closed only when the team knows what ran, how it persisted and how to catch it next time. The course moves from the NIST SP 800-86 process and evidence integrity, through RAM acquisition and Volatility 3 analysis, to Windows artefacts and super-timelines, then to defensive malware triage and YARA detection content. The final day applies the routine to lab cases and produces a Compromised Host Examination Report and Detection Handover Pack ready for the SOC.