FOR526: **Advanced Memory Forensics & Threat Detection**

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- SIFT Workstation 3
  This course extensively uses the SIFT Workstation 3 to teach incident responders and forensic analysts how to respond to and investigate sophisticated attacks. SIFT contains hundreds of free and open-source tools, easily matching any modern forensic and incident response commercial tool suite.
  - Ubuntu LTS base
  - 64 bit-based system
  - Better memory utilization
  - Auto-DFIR package update and customizations
  - Latest forensic tools and techniques
  - VMware Appliance ready to tackle forensics
  - Cross-compatibility between Linux and Windows
  - Expanded filesystem support (NTFS, HFS, EXFAT, and more)
- Windows 8.1 Workstation with license
  - 64 bit-based system
  - A licensed virtual machine loaded with the latest forensic tools
  - VMware Appliance ready to tackle forensics
- 32 GB Course USB 3.0
  - USB loaded with memory captures, SIFT Workstation 3, tools, and documentation
- SANS Memory Forensics Exercise Workbook
  - Exercise book is over 200 pages long with detailed step-by-step instructions and examples to help you become a master incident responder
- SANS DFIR cheat sheets to help use the tools
- MP3 audio files of the complete course lecture

Digital Forensics and Incident Response (DFIR) professionals need Windows memory forensics training to be at the top of their game. Investigators who do not look at volatile memory are leaving evidence at the crime scene. RAM content holds evidence of user actions, as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the smoking gun that unravels the story of what happened on a system.

FOR526: Memory Forensics In-Depth provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyze captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

In today's forensics cases, it is just as critical to understand memory structures as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand. For those investigating platforms other than Windows, this course also introduces OSX and Linux memory forensics acquisition and analysis using hands-on lab exercises.

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

FOR526:Memory Forensics In-Depth will teach you:

- Proper Memory Acquisition: Demonstrate targeted memory capture ensuring data integrity and overcoming obstacles to acquisition/anti-acquisition behaviors
- How to Find Evil in Memory: Detect rogue, hidden, and injected processes, kernel-level rootkits, Dynamic Link Libraries (DLL) hijacking, process hollowing, and sophisticated persistence mechanisms
- Effective Step-by-Step Memory Analysis Techniques: Use process timelining, high-low level analysis, and walking the Virtual Address Descriptors (VAD) tree to spot anomalous behavior
- Best Practice Techniques: Learn when to implement triage, live system analysis, and alternative acquisition techniques and how to devise custom parsing scripts for targeted memory analysis

MALWARE CAN HIDE, BUT IT MUST RUN

> **"The training opened my eyes to the need to collect memory images, as well as physical images for single computer analysis, such as theft of IP or other employee investigations."**
>
> -Greg Caouette, **Kroll**

Course Day
Descriptions

DAY 1: Foundations in Memory Analysis and Acquisition

Simply put, memory analysis has become a required skill for all incident responders and digital forensics examiners. Regardless of the type of investigation, system memory and its contents often expose the first piece of the evidential thread that, when pulled, unravels the whole picture of what happened on the target system. Where is the malware? How did the machine get infected? Where did the attacker move laterally? Or what did the disgruntled employee do on the system? What lies in physical memory can provide answers to all of these questions and more.

Topics: Why Memory Forensics?; Investigative Methodologies; The Ubuntu SIFT and Windows 8.1 Workstations; The Volatility Framework; System Architectures; Triage versus Full Memory Acquisition; Physical Memory Acquisition

DAY 2: Unstructured Analysis and Process Exploration

Structured memory analysis using tools that identify and interpret operating system structures is certainly powerful. However, many remnants of previously allocated memory remain available for analysis, and they cannot be parsed through structure identification. What tools are best for processing fragmented data? Unstructured analysis tools! They neither know nor care about operating system structures. Instead, they examine data, extracting findings using pattern matching. You will learn how to use Bulk Extractor to parse memory images and extract investigative leads such as email addresses, network packets, and more.

Topics: Unstructured Memory Analysis; Page File Analysis; Exploring Process Structures; List Walking and Scanning; Pool Memory; Exploring Process Relationships; Exploring DLLs; Kernel Objects

DAY 3: Investigating the User via Memory Artifacts

An incident responder (IR) is often asked to triage a system because of a network intrusion detection system alert. The Security Operations Center makes the call and requires more information due to outbound network traffic from an endpoint and the IR team is asked to respond. In this section, we cover how to enumerate active and terminated TCP connections – selecting the right plugin for the job based on the OS version.

Topics: Network Connections; Virtual Address Descriptors; Detecting Injected Code; Analyzing the Registry via Memory Analysis; User Artifacts in Memory

DAY 4: Internal Memory Structures

Day 4 focuses on introducing some internal memory structures (such as drivers), Windows memory table structures, and extraction techniques for portable executables. As we come to the final steps in our investigative methodology, "Spotting Rootkit Behaviors" and "Extracting Suspicious Binaries," it is important to emphasize again the rootkit paradox. The more malicious code attempts to hide itself, the more abnormal and seemingly suspicious it appears. We will use this concept to evaluate some of the most common structures in Windows memory for hooking, the IDTs and SSDTs.

Topics: Interrupt Descriptor Tables; System Service Descriptor Tables; Drivers; Direct Kernel Object Manipulation; Module Extraction; Hibernation Files; Crash Dump Files

DAY 5: Memory Analysis on Platforms Other than Windows

Windows systems may be the most prevalent platform encountered by forensic examiners today, but most enterprises are not homogeneous. Forensic examiners and incident responders are best served by having the skills to analyze the memory of multiple platforms, including Linux and Mac—that is, platforms other than Windows.

Topics: Linux Memory Acquisition and Analysis; Mac Memory Acquisition and Analysis

DAY 6: Memory Analysis Challenge

This final course section provides students with a direct memory forensics challenge that makes use of the SANS NetWars Tournament platform. Your memory analysis skills are put to the test with a variety of hands-on scenarios involving hibernation files, Crash Dump files, and raw memory images, reinforcing techniques covered in the first five sections of the course. These challenges strengthen students' ability to respond to typical and atypical memory forensics challenges from all types of cases, from investigating the user to isolating the malware. By applying the techniques learned earlier in the course, students consolidate their knowledge and can shore up skill areas where they feel they need additional practice.

Topics: Malware and Rootkit Behavior Detection; Persistence Mechanism Identification; Code Injection Analysis; User Activity Reconstruction; Linux Memory Image Parsing; Mac OSX Memory Image Parsing; Windows Hibernation File Conversion and Analysis; Windows Crash Dump Analysis (Using Windows Debugger)

Who Should Attend

- Incident response team members
- Experienced digital forensic analysts
- Red team members, penetration testers, and exploit developers
- Law enforcement officers, federal agents, and detectives
- SANS FOR508 and SEC504 graduates
- Forensics investigators

> **"This class gives good insights into incident response skills when interacting with your team doing memory forensics."**
>
> -Venkat Luckyreddy, **BMS**

FOR526 Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast