

## FOR508: Advanced Computer Forensic Analysis and Incident Response

This course focuses on providing incident responders with the necessary skills to hunt down and counter a wide range of threats within enterprise networks, including economic espionage, hactivism, and financial crime syndicates. The completely updated FOR508 addresses today's incidents by providing real-life, hands-on response tactics.

**DAY 0:** A 3-letter government agency contacts you to say that critical information was stolen from a targeted attack on your organization. Don't ask how they know, but they tell you that there are several breached systems within your enterprise. You are compromised by an Advanced Persistent Threat, aka an APT – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

Over 90% of all breach victims learn of a compromise from third-party notification, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Gather your team – it's time to go hunting.

**FOR508: Advanced Computer Forensic Analysis and Incident Response will help you determine:**

- How did the breach occur?
- What systems were compromised?
- What did they take?
- What did they change?
- How do we remediate the incident?

*“FOR508 gives you the skills necessary to work effectively on a high performing security team, and the timeline analysis is extremely useful and interesting.”*

*-MANNY ORTIZ, AT&T*

FOR508 trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats. A hands-on lab – developed from a real-world targeted attack on an enterprise network – leads you through the challenges and solutions. You will identify where the initial targeted attack occurred and which systems an APT group compromised. The course will prepare you to find out which data were stolen and by whom, contain the threat, and provide your organization the capabilities to manage and counter the attack.

During a targeted attack, an organization needs the best incident responders and forensic analysts in the field. FOR508 will train you and your team to be ready to do this work.

*“Everything you need to learn for the basics of forensics in just six days; any more knowledge and your head would explode!”*

*-MATTHEW HARVEY, U.S. DEPARTMENT OF JUSTICE*



giac.org



sans.org/  
cyber-guardian



sans.edu



DoD 8570 Required  
sans.org/8570



digital-forensics.sans.org

### Who Should Attend

- Information security professionals
- Incident response team members
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates

### You Will Be Able To

- Apply incident response processes, threat intelligence, and digital forensics to investigate breached enterprise environments from Advanced Persistent Threat (APT) groups, organized crime syndicates, or hacktivists
- Discover every system compromised in your enterprise utilizing incident response tools such as F-Response and digital forensic analysis capabilities in the SIFT Workstation to identify APT beach head and spear phishing attack mechanisms, lateral movement, and data exfiltration techniques
- Use the SIFT Workstation's capabilities, and perform forensic analysis and incident response on any remote enterprise hard drive or system memory without having to image the system first, allowing for immediate response and scalable analysis to take place across the enterprise
- Use system memory and the Volatility toolset to discover active malware on a system, determine how the malware was placed there, and recover it to help develop key threat intelligence to perform proper scoping activities during incident response
- Detect advanced capabilities such as Stuxnet, TDSS, or APT command and control malware immediately through memory analysis using Redline's Malware Rating Index (MRI) to quickly ascertain the threat to your organization and aid in scoping the true extent of the data breach
- Track the exact footprints of an attacker crossing multiple systems and observe data it has collected to exfiltrate as you track your adversary's movements in your network via timeline analysis using the log2timeline toolset
- Begin recovery and remediation of the compromise via the use of Indicators of Compromise (IOC), Threat Intelligence, and IR/Forensics key scanning techniques to identify active malware and all enterprise systems affected by the breach
- Perform filesystem surgery using the sleuthkit tool to discover how filesystems work and uncover powerful forensic artifacts such as NTFS \$130 directory file indexes, journal parsing, and detailed Master File Table analysis
- Use volume shadow snapshot examinations, XP restore point analysis, and NTFS examination tools in the SIFT Workstation, and recover artifacts hidden by anti-forensic techniques such as timestomping, file wiping, rootkit hiding, and privacy cleaning
- Discover an adversary's persistence mechanisms to allow malware to continue to run on a system after a reboot using command-line tools such as autoruns, psexec, jobparser, group policy, triage-ir, and IOCFinder

### 508.1 HANDS ON: Enterprise Incident Response

Incident responders should be armed with the latest tools, memory analysis techniques, and enterprise scanning methodologies in order to identify, track and contain advanced adversaries, and remediate incidents. Incident response and forensic analysts must be able to scale their examinations from the traditional one analyst per system toward one analyst per 1,000 or more systems. Enterprise scanning techniques are now a requirement to track targeted attacks by APT groups or crime syndicate groups that propagate through thousands of systems.

**Topics:** SIFT Workstation Overview; Incident Response Methodology; Threat and Adversary Intelligence; Intrusion Digital Forensics Methodology; Remote and Enterprise IR System Analysis; Windows Live Incident Response

### 508.2 HANDS ON: Memory Forensics

Critical to many incident response teams detecting advanced threats in the organization, memory forensics has come a long way in just a few years. It can be extraordinarily effective at finding evidence of worms, rootkits, and advanced malware used by an APT group of attackers. While traditionally solely the domain of Windows internals experts, recent tools now make memory analysis feasible for anyone. Better interfaces, documentation, and built-in detection heuristics have greatly leveled the playing field. This section will introduce some of the newest free tools available and give you a solid foundation in adding core and advanced memory forensic skills to your incident response and forensics armory.

**Topics:** Memory Acquisition and Analysis; Memory Analysis Techniques with Redline; Live Memory Forensics; Advanced Memory Analysis with Volatility

### 508.3 HANDS ON: Timeline Analysis

Timeline analysis will change the way you approach digital forensics and incident response...forever. Learn advanced analysis techniques uncovered via timeline analysis directly from the developers who pioneered timeline analysis tradecraft. Temporal data are located everywhere on a computer system. Filesystem modified/access/creation/change times, log files, network data, registry data, and Internet history files all contain time data that can be correlated into critical analysis to successfully solve cases. New timeline analysis frameworks provide the means to conduct simultaneous examinations of a multitude of time-based artifacts. Analysis that once took days now takes minutes. This section will step you through the two primary methods of creating and analyzing timelines established during advanced incidents and forensic cases.

**Topics:** Timeline Analysis Overview; Filesystem Timeline Creation and Analysis; Windows Time Rules (File Copies vs. File Moves); Filesystem Timeline Creation Using Sleuthkit and fls; Super Timeline Creation and Analysis; Super Timeline Artifact Rules; Timeline Creation with log2timeline; Super Timeline Analysis

### 508.4 HANDS ON: Deep Dive Forensics and Anti-Forensics Detection

A major criticism of digital forensic professionals is that many tools simply require a few mouse clicks to have the tool automatically recover data for evidence. This "push button" mentality has led to inaccurate case results in the past few years in high-profile cases such as the Casey Anthony murder trial. You will stop being reliant on "push button" forensic techniques as we cover how the engines of digital forensic tools really work. To understand how to carve out data, it is best to understand how to accomplish it by hand and show how automated tools should be able to recover the same data.

**Topics:** Windows XP Restore Point Analysis; VISTA, Windows 7, Server 2008 Shadow Volume Copy Analysis; Deep Dive Forensics Analysis; Data Layer Analysis; Stream-Based Data Carving; File-Based Data Carving; NTFS Filesystem Analysis; FAT/exFAT Filesystem Overview

### 508.5 HANDS ON: Intrusion Forensics – The Art of Finding Unknown Malware

The adversaries are good, we must be better. Over the years, we have observed that many incident responders have a challenging time finding malware without effective indicators of compromise (IOCs) or threat intelligence gathered prior to a breach. This is especially true in APT group intrusions. This advanced session will demonstrate techniques used by first responders to discover malware or forensic artifacts when very little information exists about their capabilities or hidden locations. We will discuss techniques to help funnel possibilities down to the candidates most likely to be evil malware trying to hide on the system.

**Topics:** Step-by-Step Finding Unknown Malware on a System; Anti-Forensics Detection Methodologies; Methodology to Analyze and Solve Challenging Cases

### 508.6 HANDS ON: The Incident Response & Intrusion Forensic Challenge

This brand-new exercise brings together some of the most exciting techniques learned earlier in the week and tests your newly acquired skills in a case that simulates an attack by an advanced adversary such as an APT. This challenge brings it all together using a simulated intrusion into a real enterprise environment consisting of multiple Windows systems. You will be asked to uncover how the systems were compromised in the initial intrusion, find other systems the adversary moved to laterally, and identify intellectual property stolen via data exfiltration. You will walk out of the course with hands-on experience investigating realistic scenarios, which were put together by a cadre of individuals with many years of experience fighting advanced threats such as an APT group.

## FOR508 Training Formats

(subject to change)



### Live Training

[sans.org/security-training/by-location/all](https://sans.org/security-training/by-location/all)



### Summit Events

[sans.org/summit](https://sans.org/summit)



### Mentor Program

[sans.org/mentor](https://sans.org/mentor)



### OnSite

[sans.org/onsite](https://sans.org/onsite)



### vLive

[sans.org/vlive](https://sans.org/vlive)



### Simulcast

[sans.org/simulcast](https://sans.org/simulcast)



### SelfStudy

[sans.org/selfstudy](https://sans.org/selfstudy)