FORENSICS 572

Hands On | Six Days | Laptop Required | 36 CPEs | GIAC Cert: GNFA

NEW

FOR572: Advanced Network Forensics and Analysis

Forensic casework that does not include a network component is a rarity in today's environment. Performing disk forensics will always be a critical and foundational skill for this career, but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, or employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, or even definitively prove that a crime actually occurred.

What you will receive with this course

- Linux version of the SIFT Workstation Virtual Machine with over 500 digital forensics and incident response tools prebuilt into the environment, including network forensic tools added just for this course
- Windows Virtual Machine with preinstalled network forensic tools
- Windows 8 Standard Full Version License and Key for the Windows VMware Image
- Realistic case data to examine during class, from multiple sources including:
  - Network captures in pcap format
  - NetFlow data
  - Web proxy, firewall, and intrusion detection system logs
  - Network service logs
- 64GB USB disk loaded with case examples, tools, and documentation

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we'll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence, as well as how to place new collection platforms while an incident is already under way.

Whether you are a consultant responding to a client's site, a law enforcement professional assisting victims of cybercrime and seeking prosecution of those responsible, or an on-staff forensic practitioner, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS security curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS forensics alumni from FOR408 and FOR508 can take their existing knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without any convenient hard drive or memory images.

The hands-on exercises in this class cover a wide range of tools, including the venerable tcpdump and Wireshark for packet capture and analysis; commercial tools from Splunk, NetworkMiner, and SolarWinds; and open-source tools including nfdump, tcpxtract, ELSA, and more. Through all of these exercises, your shell scripting abilities will come in handy to make easy work of ripping through thousands of data records.

giac.org sans.edu digital-forensics.sans.org

Who Should Attend

- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- IT professionals
- Network engineers
- IT lawyers and paralegals
- Anyone interested in computer network intrusions and investigations

You Will Be Able To

- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determinations
- Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- Reverse-engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- Decrypt captured SSL traffic to identify attackers' actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation's findings
- Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- Learn how attackers leverage man-in-the-middle tools to intercept seemingly secure communications
- Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- Analyze wireless network traffic to find evidence of malicious activity
- Use visualization tools and techniques to distill vast, complex data sources into management-friendly reports
- Learn how to modify configuration on typical network devices such as firewalls and intrusion detection systems to increase the intelligence value of their logs and alerts during an investigation
- Apply the knowledge you acquire during the week in a full-day capstone exercise, modeled after real-world nation-state intrusions

572.1 HANDS ON: Off the Disk and Onto the Wire

Network data can be preserved, but only if captured directly from the wire. Whether tactical or strategic, packet capture methods are quite basic. You will re-acquaint yourself with tcpdump and Wireshark, the most common tools used to capture and analyze network packets, respectively. However, since long-term full-packet capture is still uncommon in most environments, many artifacts that can tell us about what happened on the wire in the past come from devices that manage network functions. You will learn about what kinds of devices can provide valuable evidence and at what level of granularity. We will walk through collecting evidence from one of the most common sources of network evidence, a web proxy server, then go hands-on to find and extract stolen data from the proxy yourself. The Linux SIFT virtual machine, which has been specifically loaded with a set of network forensic tools, will be your primary toolkit for the week.

Topics: Goals of Forensic Investigation; Hypothesis Management Fundamentals; Foundational Network Forensics Tools: tcpdump and Wireshark; Network Evidence Sources and Types; Case Management and Evidence Collection/Handling; Web Proxy Server Examination; Network Architectural Challenges and Opportunities; Packet Capture Applications and Data

572.2 HANDS ON: Network Protocols and Commercial Network Forensics

This section covers some of the most common and fundamental network protocols that you will likely face during an investigation. We will cover a broad range of protocols including the Dynamic Host Configuration Protocol, which glues together layers two and three on the OSI model, and Microsoft's Remote Procedure Call protocol, which provides all manners of file, print, name resolution, authentication, and other services.

Topics: Dynamic Host Configuration Protocol (DHCP) and Domain Name Service (DNS); Hypertext Transfer Protocol (HTTP); Secure HTTP (HTTPS) and Secure Sockets Layer (SSL); File Transfer Protocol (FTP); Network Time Protocol (NTP); Commercial Network Forensics; Microsoft Protocols; Simple Mail Transfer Protocol (SMTP)

FOR572 Training Formats

(subject to change)

Live Training
sans.org/security-training/by-location/all

OnSite
sans.org/onsite

vLive Events
sans.org/vlive

Simulcast
sans.org/simulcast

SelStudy
sans.org/selfstudy

572.3 HANDS ON: Netflow Analysis and Wireless Network Forensics

In this section, you will learn what data items NetFlow can provide, and the various means of collecting those items. As with many such monitoring technologies, both commercial and open-source solutions exist to query and examine NetFlow data. We will review both categories and discuss the benefits and drawbacks of each. Finally, we will address the forensic aspects of wireless networking. We will cover similarities with and differences from traditional wired network examination, as well as what interesting artifacts can be recovered from wireless protocol fields. Some inherent weaknesses of wireless deployments will also be covered, including how attackers can leverage those weaknesses during an attack, and how they can be detected.

Topics: Introduction to NetFlow; NetFlow Collection Approaches; Open-Source Flow Tools; Commercial Flow Analysis Suites; Profiling and Behavior Analysis; Visualization Techniques and Tools; Wireless Network Forensics

572.4 HANDS ON: Logging, OPSEC, and Footprint

In this section, you will learn about various logging mechanisms available to both endpoint and network transport devices. You will also learn how to consolidate log data from multiple sources, providing a broad corpus of evidence in one location. As the volume of log data increases, so does the need to consider automated analytic tools. You will learn various solutions that accomplish this, from tactical to enterprise-scale.

Topics: Syslog; Microsoft Event Logging; HTTP Server Logs; Firewall and Intrusion Detection Systems; Log Data Collection, Aggregation, and Analysis; Investigation OPSEC and Footprint Considerations

572.5 HANDS ON: Encryption, Protocol Reversing, and Automation

Encryption is frequently cited as the most significant hurdle to effective network forensics, and for good reason. When properly implemented, encryption can be a brick wall in between an investigator and critical answers. However, technical and implementation weaknesses can be used to our advantage. Even in the absence of these weaknesses, the right analytic approach to encrypted network traffic can still yield valuable information about the content. We will discuss the basics of encryption and how to approach it during an investigation. The section will also cover flow analysis to characterize encrypted conversations.

Topics: Introduction to Encryption; Man-in-the-Middle; Encrypted Traffic Flow Analysis; Payload Reconstruction; Network Protocol Reverse Engineering; Automated Tools and Libraries

572.6 HANDS ON: Network Forensics Capstone Challenge

This section will combine all of what you have learned prior to and during this week. In groups, you will examine network evidence from a real-world compromise by an advanced attacker. Each group will independently analyze data, form and develop hypotheses, and present findings. No evidence from endpoint systems is available – only the network and its infrastructure.

Topics: Network Forensic Case