FOR408: Windows Forensic Analysis

Master computer forensics. What Do You Want to Uncover Today?

Every organization will deal with cyber-crime occurring on the latest Windows operating systems. Analysts will investigate crimes including fraud, insider threats, industrial espionage, traditional crimes, and computer hacking. Government agencies use media exploitation of Windows systems to recover key intelligence available on adversary systems. To help solve these cases, organizations are hiring digital forensic professionals, investigators, and agents to uncover what happened on a system.

FOR408: Windows Forensic Analysis focuses on critical knowledge of the Windows OS that every digital forensic analyst must know in order to investigate computer incidents successfully. You will learn how computer forensic analysts collect and analyze data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 8.1, Office365, Skydrive, Sharepoint, Exchange Online, and Windows Phone). This will ensure that students are prepared to investigate the latest trends and capabilities they might encounter. In addition, students will have labs that cover both Windows XP and Windows 7 artifacts.

Updated FOR408 Course in 2014: This course utilizes a brand-new Windows 8.1-based case exercise for which it took over six months to create the data in real time. Our development team has developed an incredibly realistic scenario. Working with in the Windows 8.1-based image, students use Windows Phone, Office 365, Sharepoint, MS Portal Online, Skydrive/Onedrive, Dropbox, and USB external devices. The case demonstrates the latest technologies an investigator would encounter analyzing a Windows operating system. The brand new case workbook will detail step-by-step what each investigator needs to know to examine the latest Windows 8.1.

What you will receive with this course

- Windows 8.1 version of the SIFT Workstation Virtual Machine with over 150 commercial, open source and freeware Digital Forensics and Incident Response tools prebuilt into the environment
- Windows 8.1 Standard License and Key for the Windows SIFT Workstation
- Full license to:
  - AccessData FTK for a three-month trial
  - Full license to MagnetForensics Internet Evidence Finder for a 15-day trial
  - TZWorks Toolset for a three-month trial
  - NUIX for a month trial
- 64 GB USB Key with four full real-world cases to examine during and after class
  - Windows 8.1 - Windows 7 - Windows Vista - Windows XP
- SANS exercise workbook with detailed step-by-step instructions
- Wiebetech Ultradock v5 Write Blocker Kit
  - IDE and SATA Cable Connector - Three FireWire Ports
  - USB 3.0 Port

digital-forensics.sans.org

giac.org

sans.edu

Who Should Attend

- Information technology professionals
- Incident response team members
- Law enforcement officers, federal agents & detectives
- Media exploitation analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in computer forensic investigations

You Will Be Able To

- Perform proper Windows forensic analysis by applying key analysis techniques covering Windows XP through Windows 8
- Use full-scale forensic tools and analysis methods to detail every action a suspect accomplished on a Windows system, including how and who placed an artifact on the system, program execution, file/folder opening, geo-location, browser history, profile USB device usage, and more
- Uncover the exact time that a specific user last executed a program through Registry analysis, Windows artifact analysis, and email analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker breached systems, and traditional crimes
- Determine the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), email analysis, and Windows Registry parsing
- Use automated analysis techniques via AccessData's Forensic ToolKit (FTK)
- Identify keywords searched by a specific user on a Windows system in order to pinpoint the files and information the suspect was interested in finding and to accomplish damage assessments
- Use shellbags analysis tools to articulate every folder and directory that a user opened up while browsing the hard drive
- Determine each time a unique and specific USB device was attached to the Windows system, the files and folders that were accessed on it, and who plugged it in by parsing key Windows artifacts such as the Registry and log files
- Use event log analysis techniques to determine when and how users logged into a Windows system via a remote session, at the keyboard, or simply by unlocking their screensaver
- Determine where a crime was committed using FTK Registry Viewer to pinpoint the geo-location of a system by examining connected networks, browser search terms, and cookie data
- Use Mandiant Web Historian, parse raw SQLite databases, and leverage browser session recovery artifacts and flash cookies to identify web activity of suspects, even if privacy cleaners and in-private browsing are used

408.1 HANDS ON: Windows Digital Forensics and Advanced Data Triage

The Windows Forensics course starts with an examination of digital forensics in today's interconnected environments and discusses challenges associated with mobile devices, tablets, cloud storage, and modern Windows operating systems. We will discuss how modern hard drives, such as Solid State Devices (SSD), can affect the digital forensics acquisition process and how analysts need to adapt to overcome the introduction of these new technologies.

Topics: Windows Operating System Components; Core Forensic Principles; Live Response and Triage-Based Acquisition Techniques; Acquisition Review with Write Blocker; Advanced Acquisition Challenges; Windows Image Mounting and Examination; FAT and NTFS File System Overview; Key Word Searching and Forensics Suites (FTK, EnCase, and Autopsy); Document and File Metadata; File Carving

408.2 HANDS ON: CORE WINDOWS FORENSICS PART 1 – Registry and USB Device Analysis

This day focuses on Windows XP, Windows 7, and Windows 8/8.1 Registry Analysis, and USB Device Forensics. Throughout the section, investigators will use their skills in a real hands-on case, exploring evidence and analyzing evidence.

Topics: Registry Basics; Profile Users and Groups; Core System Information; User Forensic Data; External and Bring Your Own Device (BYOD) Forensic Examinations; Tools Utilized

408.3 HANDS ON: CORE WINDOWS FORENSICS PART 2 – Email Forensics

You will learn how major forensic suites can facilitate and expedite the investigative process, and how to recover and analyze email, the most popular form of communication. Client-based, server-based, mobile, and web-based email forensic analysis are discussed in depth.

Topics: Evidence of User Communication; How Email Works; Determining Sender's Geographic Locations; Examination of Email; Types of Email Formats

408.4 HANDS ON: CORE WINDOWS FORENSICS PART 3 – Artifact and Log File Analysis

Suspects unknowingly create hundreds of files that link back to their actions on a system. Learn how to examine key files such as link files, the Windows prefetch, pagefile/system memory, and more. The latter part of the section will center on examining the Windows log files and the usefulness in both simple and complex cases.

Topics: Memory, Pagefile, and Unallocated Space Analysis; Forensicating Files Containing Critical Digital Forensic Evidence; Windows Event Log Digital Forensic Analysis

408.5 HANDS ON: CORE WINDOWS FORENSICS PART 4 – Web Browser Forensics: Firefox, Internet Explorer, and Chrome

This section looks at Internet Explorer and Firefox Browser Digital Forensics. Learn how to examine exactly what individuals did while surfing via their web browser. The results will give you pause the next time you use the web.

Topics: Browser Forensics: History, Cache, Searches, Downloads, Understanding of Browser Timestamps, Internet Explorer; Firefox

408.6 HANDS ON: Windows Forensic Challenge

This section revolves around a Digital Forensic Challenge based on Windows Vista/7. It is a capstone exercise for every artifact discussed in the class. You will use this section to consolidate the skills that you have learned over the past week.

Topics: Digital Forensic Case; Mock Trial

FIGHT CRIME. UNRAVEL INCIDENTS...ONE BYTE AT A TIME

"This is a very high-intensity course with extremely current course material that is not available anywhere else in my experience."

-Alexander Applegate, Auburn University

FOR408 Training Formats

(subject to change)

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

Summit Events
sans.org/summit

Community SANS
sans.org/community

Mentor Program
sans.org/mentor

OnSite
sans.org/onsite

vLive
sans.org/vlive

Simulcast
sans.org/simulcast

OnDemand
sans.org/ondemand

SelStudy
sans.org/selfstudy