

# FOR500: Windows Forensic Analysis



**GCCE**  
Forensic Examiner  
giac.org/gcfe

6 Day Program | 36 CPEs | Laptop Required

## You Will Be Able To

- Perform proper Windows forensic analysis by applying key techniques focusing on Windows 7, Windows 8/8.1, and Windows 10
- Use state-of-the-art forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geolocation, browser history, profile USB device usage, cloud storage usage, and more
- Uncover the exact time that a specific user last executed a program through Registry and Windows artifact 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
- Audit cloud storage usage, including detailed user activity, identifying deleted files and even documenting files available only in the cloud
- Identify keywords searched by a specific user on a Windows system to pinpoint the data and information that the suspect was interested in finding, and accomplish detailed damage assessments
- Use Windows Shellbag analysis tools to articulate every folder and directory a user or attacker interacted with while accessing local, removable, and network drives
- Determine each time a unique and specific USB device was attached to the Windows system, the files and folders accessed on it, and what user plugged it in by parsing Windows artifacts such as Registry hives and Event Log files
- Learn Event Log analysis techniques and use them to determine when and how users logged into a Windows system, whether via a remote session, at the keyboard, or simply by unlocking a screensaver
- Determine where a crime was committed using Registry data and pinpoint the geolocation of a system by examining connected networks and wireless access points
- Use browser forensic tools to perform detailed web browser analysis, parse raw SQLite and ESE databases, and leverage session recovery artifacts to identify web activity, even if privacy cleaners and in-private browsing software are used
- Specifically determine how individuals used a system, who they communicated with, and files that were downloaded, modified, and deleted

## MASTER WINDOWS FORENSICS – YOU CAN'T PROTECT THE UNKNOWN

All organizations must prepare for cyber-crime occurring on their computer systems and within their networks. Demand has never been greater for analysts who can investigate crimes such as fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover vital intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation experts capable of piecing together what happened on computer systems second by second.

FOR500: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and available artifacts is a core component of information security. You will learn how to recover, analyze, and authenticate forensic data on Windows systems, track individual user activity on your network, and organize findings for use in incident response, internal investigations, intellectual property theft inquiries, and civil or criminal litigation. You'll be able to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unbelievable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data and use it to your advantage.

Proper analysis requires real data for students to examine. This continually updated course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest technologies, including Microsoft Windows 7, Windows 8/8.1, Windows 10, Office and Microsoft 365, Google Workspace (G Suite), Cloud Storage, SharePoint, Exchange, and Outlook. Students will leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows 7 systems to just-discovered Windows 10 artifacts.

FOR500: Windows Forensic Analysis will teach you to:

- Conduct in-depth forensic analysis of Windows operating systems and media exploitation focusing on Windows 7, Windows 8/8.1, Windows 10, and Windows Server 2008/2012/2016
- Identify artifact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geolocation, file download, anti-forensics, and detailed system usage
- Focus your capabilities on analysis instead of on how to use a particular tool
- Extract critical answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation

FOR500 starts with an intellectual property theft and corporate espionage case that took over six months to create. You work in the real world, so your training should include real-world practice data. Our instructor course development team used incidents from their own investigations and experiences to create an incredibly rich and detailed scenario designed to immerse students in an actual investigation. The case demonstrates the latest artifacts and technologies an investigator might encounter while analyzing Windows systems. The detailed workbook shows the tools and techniques that each investigator should employ step by step to solve a forensic case. The tools can be used long after the end of class.

**“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

# Section Descriptions

## SECTION 1: Digital Forensics and Advanced Data Triage

The Windows Forensic Analysis 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. Hard drive and digital media sizes are increasingly difficult and time-consuming to handle appropriately in digital cases. Being able to acquire data in an efficient and forensically sound manner is crucial to every investigator today. In this course section, we review the core techniques while introducing new triage-based acquisition and extraction capabilities that will increase the speed and efficiency of the acquisition process. We demonstrate how to acquire memory, the NTFS MFT, Windows logs, Registry, and critical files in minutes instead of the hours or days currently spent on acquisition. We also begin processing our collected evidence using stream-based and file-carving-based extraction capabilities employing both commercial and open-source tools and techniques. Students come away with the knowledge necessary to target the specific data needed to rapidly answer fundamental questions in their cases.

**TOPICS:** Windows Operating System Components; Core Forensic Principles; Live Response and Triage-Based Acquisition Techniques; Windows Image Mounting and Examination; NTFS File System Overview; Document and File Metadata; File and Stream Carving; Memory, Pagefile, and Unallocated Space Analysis

## SECTION 3: Shell Items and Removable-Device Profiling

Being able to show the first and last time a file or folder was opened is a critical analysis skill. Utilizing shortcut (LNK), jump list, and Shellbag databases through the examination of SHELL ITEMS, we can quickly pinpoint which file or folder was opened and when. The knowledge obtained by examining SHELL ITEMS is crucial in tracking user activity in intellectual property theft cases internally or in tracking hackers. Removable storage device investigations are often an essential part of performing digital forensics. We will show you how to perform in-depth USB device examinations on Windows 7, 8/8.1, and 10. You will learn how to determine when a storage device was first and last plugged in, its vendor/make/model, and even the unique serial number of the device used.

**TOPICS:** Shell Item Forensics; USB & BYOD Forensic Examinations

## SECTION 5: Web Browser Forensics

With the increasing use of the web and the shift toward web-based applications and cloud computing, browser forensic analysis is a critical skill. During this section, students will comprehensively explore web browser evidence created during the use of Internet Explorer, Microsoft Edge, Firefox, and Google Chrome. The hands-on skills taught here, such as SQLite and ESE database parsing, allow investigators to extend these methods to nearly any browser they encounter. Students will learn how to examine every significant artifact stored by the browser, including cookies, visit and download history, Internet cache files, browser extensions, and form data. We will show you how to find these records and identify the common mistakes investigators make when interpreting browser artifacts. You will also learn how to analyze some of the more obscure (and powerful) browser artifacts, such as session restore, HTML5 web storage, zoom levels, predictive site prefetching, and private browsing remnants. Finally, we'll explore browser synchronization, providing investigative artifacts derived from other devices in use by the subject of the investigation. Throughout the section, students will use their skills in real hands-on cases, exploring evidence created by Chrome, Firefox, Microsoft Edge, Internet Explorer, and Tor correlated with other Windows operating system artifacts.

**TOPICS:** Browser Forensics

## SECTION 2: Registry Analysis, Application Execution, and Cloud Storage Forensics

Our journey continues with the Windows Registry, where the digital forensic investigator will learn how to discover critical user and system information pertinent to almost any investigation. You'll learn how to navigate and analyze the Registry to obtain user profile and system data. During this course section, we will demonstrate investigative methods to prove that a specific user performed keyword searches, executed specific programs, opened and saved files, perused folders, and used removable devices. Throughout this course section, students will use their skills in a real hands-on case, exploring and analyzing a rich set of evidence.

**TOPICS:** Registry Forensics In-Depth; Registry Core; Profile Users and Groups; Core System Information; User Forensic Data; Cloud Storage Forensics

## SECTION 4: Email Analysis, Windows Search Index, SRUM, and Event Logs

Depending on the type of investigation and authorization, a wealth of evidence can be unearthed through the analysis of email files. Recovered email can bring excellent corroborating information to an investigation, and its informality often provides very incriminating evidence. It is common for users to have an email that exists locally on their workstation, on their company email server, in a private cloud, and in multiple webmail accounts. The exciting Windows 10 Timeline database shows great promise in recording detailed user activity, including additional application execution artifacts, mapping file usage to specific programs and users, and additional device identification via synchronized artifacts. Similarly, the System Resource Usage Monitor (SRUM), one of our most exciting digital artifacts, can help determine many important user actions, including network usage per application and VPN and wireless network usage. Imagine the ability to audit network usage by cloud storage and backdoors even after execution of counter-forensic programs! Finally, Windows event log analysis has solved more cases than possibly any other type of analysis. Windows 10 now includes over 300 logs, and understanding the locations and content of the available log files is crucial to the success of any investigator. Many researchers overlook these records because they do not have adequate knowledge or tools to get the job done efficiently. This section arms investigators with the core knowledge and capability to maintain and build upon this crucial skill for many years to come.

**TOPICS:** Email Forensics; Forensics Additional Windows OS Artifacts; Windows Event Log Analysis

## SECTION 6: Windows Forensics Challenge

Nothing will prepare you more as an investigator than a full hands-on challenge that requires you to use the skills and knowledge presented throughout the week. In the morning, you will have the option to work in teams on a real forensic case. Students will be provided new evidence to analyze, and the exercise will step you through the entire case flow, including proper acquisition, analysis, and reporting in preparation for a possible trial. Teams will work on the case with the objective of profiling computer usage and discovering the most critical pieces of evidence to present. This complex case will involve an investigation into one of the most recent versions of the Windows Operating System. The evidence is real and provides the most realistic training opportunity currently available. Solving the case will require that students use all of the skills gained from each of the previous sections. The section will conclude with a mock trial involving presentations of the evidence collected. The team with the best in-class presentation and short write-up wins the challenge...and the case!

**TOPICS:** Digital Forensic Case; Presentation

## Who Should Attend

- Information security professionals who want to learn the in-depth concepts of Windows digital forensics investigations
- Incident response team members who need to use deep-dive digital forensics to help solve their Windows data breach and intrusion cases and perform damage assessments
- Law enforcement officers, federal agents, and detectives who want to become deep subject-matter experts on digital forensics for Windows-based operating systems
- Media exploitation analysts who need to master tactical exploitation and Document and Media Exploitation (DOMEX)
- Anyone interested in a deep understanding of Windows forensics who has a background in information systems, information security, and computers



**GCFE**  
Forensic Examiner  
[giac.org/gcfe](http://giac.org/gcfe)

## GIAC Certified Forensic Examiner

The GIAC Certified Forensic Examiner (GCFE) certification validates a practitioner's knowledge of computer forensic analysis, with an emphasis on core skills required to collect and analyze data from Windows computer systems. GCFE certification holders have the knowledge, skills, and ability to conduct typical incident investigations including e-Discovery, forensic analysis and reporting, evidence acquisition, browser forensics and tracing user and application activities on Windows systems.

- Windows Forensics and Data Triage
- Windows Registry Forensics, USB Devices, Shell Items, Email Forensics and Log Analysis
- Advanced Web Browser Forensics (Chrome, Edge, Firefox, Internet Explorer)