FOR500: **Windows Forensic Analysis™**

GCFE
Forensic Examiner
giac.org/gcfe

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Perform in-depth Windows forensic analysis by applying peer-reviewed techniques focusing on Windows 7, Windows 8/8.1, Windows 10, Windows 11, and Windows Server products
- 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
- Perform "fast forensics" to rapidly assess and triage systems to provide quick answers and facilitate informed business decisions
- 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
- Learning about USN Journal to uncover file activity and deletion by the user
- Audit cloud storage usage, including detailed user activity, identifying deleted files, signs of data exfiltration, and even uncovering detailed information and hash values on files available only in the cloud
- Identify items 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
- Mine the Windows Search Database to uncover a massive collection of file metadata and even file content from local drives, removable media, and applications like Microsoft Outlook, OneNote, SharePoint, and OneDrive
- 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, LevelDB, and ESE databases, and leverage memory forensics and session recovery artifacts to identify web activity, even if privacy cleaners and in-private browsing software are used
- Parse Electron and WebView2 application LevelDB databases allowing the investigation of hundreds of third-party applications including most chat clients
- 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 cybercrime occurring on computer systems and within corporate networks. Demand has never been greater for analysts who can investigate crimes such as fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Corporations, governments, and law enforcement agencies increasingly require trained forensics specialists to perform investigations, recover vital intelligence from Windows systems, and ultimately get to the root cause of the crime. 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 hands-on laboratory exercises incorporating evidence found on the latest technologies, including Microsoft Windows versions 10 and 11, Office and Microsoft 365, Google Workspace (G Suite), cloud storage providers, Microsoft Teams, 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 11 artifacts.

FOR500™ starts with an intellectual property theft and corporate espionage case taking 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. Example cases demonstrate the latest artifacts and technologies an investigator might encounter while analyzing Windows systems in the enterprise. The detailed workbook teaches the tools and techniques that every investigator should employ step by step to solve a forensic case. The tools provided form a complete forensic lab that can be used long after the end of class.

Please note that this is an analysis-focused course; FOR500™ does not cover the basics of evidentiary handling, the "chain of custody," or introductory drive acquisition. The course authors update FOR500™ aggressively to stay current with the latest artifacts and techniques discovered. This course is perfect for you if you are interested in in-depth and current Microsoft Windows Operating System forensics and analysis for any incident that occurs. If you have not updated your Windows forensic analysis skills in the past three years or more, this course is essential.

> **"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

Section 1 examines 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.

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; Volume Shadow Copies; Memory, Pagefile, and Unallocated Space Analysis

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

Data is moving rapidly to the cloud, constituting a significant challenge and risk to the modern enterprise. Cloud storage applications are nearly ubiquitous on both consumer and business systems, causing interesting security and forensic challenges. In a world where some of the most important data is only present on third-party systems, how do we effectively accomplish our investigations? In this section, we will dissect OneDrive and OneDrive for Business, Google Drive, Dropbox, and iCloud, deriving artifacts present in application logs and left behind on the endpoint. We'll demonstrate how to discover detailed user activity, the history of deleted files, content in the cloud, and content cached locally. Solutions to the very real challenges of forensic acquisition and proper logging are all discussed. Understanding what can be gained through analysis of these popular applications will also make investigations of less common cloud storage solutions easier. 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 3: Shell Items and Removable Device Profiling

Removable storage device investigations are an essential part of performing digital forensics. In this course section, students will learn how to perform in-depth USB device examinations on all modern Windows versions. You will learn how to determine when a storage device was first and last plugged in, its vendor/make/model, drive capacity, and even the unique serial number of the device used.

TOPICS: Shell Item Forensics; USB and BYOD Forensic Examinations

SECTION 4: Email Analysis, Windows Search, 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. Finding and collecting email is often one of our biggest challenges as it is common for users to have email existing simultaneously on their workstation, on the company email server, on a mobile device, and in multiple cloud or webmail accounts. Section 4 arms investigators with the core knowledge and capability to maintain and build upon this crucial skill for many years to come.

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

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 Google Chrome, Microsoft Edge, Internet Explorer, and Firefox. The hands-on skills taught here, such as SQLite, LevelDB, and ESE database parsing, allow investigators to extend these methods to nearly any browser they encounter.

TOPICS: Browser Forensics; Chrome; Edge; Internet Explorer; Electron and WebView2 Applications and Chat Client Forensics; Firefox; Private Browsing and Browser Artifact Recovery; SQLite and ESE Database Carving and Examination of Additional Browser Artifacts

SECTION 6: Windows Forensics Challenge

Nothing will prepare you more as an investigator than a complete hands-on challenge requiring you to use all the skills and knowledge presented throughout the course. With the option to work individually or in teams, students are provided new case evidence to analyze. Fast forensics techniques will be used to rapidly profile computer usage and discover the most critical pieces of evidence to answer investigative questions. The skills you learn in the class will prepare you for this ultimate CTF!

TOPICS: Digital Forensics Capstone; Solving

Who Should Attend

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics who has a background in information systems, information security, and computers

NICE Framework Work Roles

- Cyber Crime Investigator (OPM 221)
- Cyber Defense Forensics Analyst (OPM 212)
- Law Enforcement/Counter Intelligence Forensics Analyst (OPM 211)

GIAC CERTIFIED GCFE FORENSIC EXAMINER

GCFE
Forensic Examiner
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)

"As a member of the IR team, this course will aid in investigating compromised hosts."

—Mike Piclher, **URS Corp.**