+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 09/17/2026

Sign Up

GIAC GCFA Certification Training

5 days (35 hours)

Overview

The GIAC GCFA Certification Training prepares you for the official GIAC Certified Forensic Analyst certification and enables you to master advanced methods in digital forensics, incident response, and threat hunting.

This course guides you through preparing for the GIAC GCFA exam, a recognized certification that validates your ability to conduct formal investigations on compromised systems. You will develop a rigorous approach to analyzing intrusions, identifying adversarial techniques, and producing actionable findings.

You will learn to examine Windows artifacts, NTFS structures, execution traces, restore data, and volatile memory contents. Practical exercises will help you reconstruct an attacker's activity, detect anti-forensic mechanisms, and prioritize relevant evidence.

Upon completion of the training, you will be able to conduct an investigation at the enterprise level, build timelines, analyze indicators of compromise, and document an appropriate response. You will also prepare your exam strategy, written materials, and time management plan for the CyberLive hands-on exercises.

Finally, the course covers the requirements for the GIAC Certified Forensic Analyst certification, the expected procedures during a proctored exam, and best practices to help you consolidate your knowledge before taking the exam.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Master the skills assessed by the GIAC Certified Forensic Analyst certification
- Analyze Windows artifacts and NTFS structures as part of an investigation
- Examine RAM to identify processes, connections, and malicious activities
- Reconstruct a timeline of an intrusion and characterize an attacker’s techniques
- Conduct a structured incident response in an enterprise environment
- Effectively prepare for the GIAC GCFA exam and its practical scenarios

Target Audience

- Forensic Analyst
- SOC analyst
- Incident response analyst
- Threat hunter
- Cybersecurity Consultant

Requirements

- Experience investigating Windows systems
- Knowledge of the fundamentals of incident response and log analysis
- Proficiency in the basics of NTFS file systems
- Practical knowledge of Windows processes, services, and persistence mechanisms
- Ability to read technical documentation in English

Technical Prerequisites

- Windows lab environment set up for forensic investigation exercises
- Forensic analysis tools configured to examine disk images, Windows artifacts, and NTFS structures
- Memory analysis environment for examining processes, network connections, code injections, and other volatile artifacts
- Evidence sets comprising disk images, memory dumps, and Windows logs prepared for investigation scenarios
- Timeline creation and analysis tools configured to correlate various sources of evidence

Our GIAC GCFA® Training Curriculum

[Day 1 - Morning]

Certification framework and forensic methodology

- Overview of the GIAC Certified Forensic Analyst certification and the skills assessed

- Exam format, proctored environment, time management, and preparation of authorized materials
- The analyst’s role in incident response and coordination with the SOC
- Investigation cycle: preparation, collection, analysis, qualification, and reporting
- Chain of custody, evidence integrity, and traceability of actions
- Hands-on workshop: analyzing an intrusion scenario and defining a prioritized investigation plan

[Day 1 - Afternoon]

Fundamentals of Windows Artifacts

- Windows architecture, accounts, services, processes, and key locations
- Sources of evidence on disk, in memory, and in system logs
- Execution and persistence artifacts: principles of interpretation
- Targeted collection and distinguishing between normal, suspicious, and malicious activity
- Note-taking methods and creating a review index for the examination
- Hands-on Workshop: Identifying Relevant Artifacts in a Compromised Windows Image

[Day 2 - Morning]

NTFS Analysis and Disk Investigation

- Organization of the NTFS file system and data layers, metadata, and filenames
- Reading MFT entries and interpreting key attributes
- Analysis of timestamps and detection of temporal inconsistencies
- Deleted files, resident and non-resident data, links, and alternate data streams
- Searching for evidence of data concealment and anti-forensic techniques on storage media

[Day 2 - Afternoon]

Execution, persistence, and user traces

- Analysis of evidence of program and script execution
- Artifacts related to users, recent documents, and devices
- Persistence points: registry, scheduled tasks, services, and startup folders
- Correlating traces to characterize an attack chain
- Preparation for certification questions regarding Windows artifacts
- Hands-on Workshop: Reconstructing the Execution of a Malicious Tool and Its Persistence Mechanism

[Day 3 - Morning]

Memory Forensics and Volatile Activity

- Principles of RAM Acquisition and Analysis
- Processes, threads, handles, drivers, and network connections in memory
- Detection of abnormal processes, code injections, and rootkits
- Analysis of command lines, resident objects, and volatile network artifacts
- Evaluating memory evidence in the context of the system

[Day 3 - Afternoon]

Detection of adversarial techniques

- Stages of an advanced intrusion and reasoning based on adversarial behavior
- Identification of initial access, lateral movement, and privilege escalation
- Evasion, obfuscation, and anti-forensic techniques
- Indicators of Compromise and Threat Hunting Hypotheses
- Moving from technical observation to incident qualification
- Hands-on workshop: Analyzing a memory dump to identify a code injection and a suspicious connection

[Day 4 - Morning]

Timeline and evidence correlation

- Building a multi-source timeline for an investigation
- Standardizing timestamps, time zones, and managing time drifts
- Correlating disk, memory, registry, and log data
- Detection of attack sequences and breaks in a timeline
- Prioritizing events and formulating verifiable conclusions

[Day 4 - Afternoon]

Enterprise-wide incident response

- Rapid assessment of a compromised environment in an enterprise setting
- Large-scale collection and analysis strategies
- Coordination among analysts, systems, network, and security teams
- Containment, eradication, and validation of remediation
- Production of a clear, factual, and actionable investigation report
- Hands-on workshop: Prioritizing incident response actions in a multi-workstation compromise scenario

[Day 5 - Morning]

Targeted preparation for the GCFA exam

- Structured review of the areas assessed by the GIAC GCFA® certification
- Analysis of common pitfalls and decision-making criteria in forensic cases
- Organizing an effective paper index for a document-based exam
- Problem-solving strategies for theoretical questions and CyberLive exercises
- Time management, review of answers, and maintaining analytical rigor

[Day 5 - Afternoon]

Certification Simulation

- Review of the exam’s objectives, format, and rules
- Solving cross-functional cases combining disk, memory, and Windows artifacts
- Justifying conclusions based on correlated technical evidence
- Self-assessment of learning outcomes and identification of individual areas for review
- Final preparation plan before the official certification exam
- Hands-on workshop: Conduct a simulated investigation, then present the timeline and conclusions

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific professional knowledge or modern methods.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth operation of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.