GIAC Certified Forensic Analyst (GCFA) Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The GIAC Certified Forensic Analyst training provides advanced, hands-on expertise in Digital Forensics, Incident Response, and Enterprise Threat Hunting. This course transforms security professionals into elite, lethal forensic analysts capable of tackling the most challenging cyber incidents, including Advanced Persistent Threats, internal/external data breaches, and sophisticated anti-forensic techniques. Participants will master the art of rapid volatile data acquisition, in-depth memory forensics, and complex timeline analysis to precisely reconstruct attack vectors and adversary tradecraft. The GCFA credential is recognized globally as the gold standard for demonstrating the ability to lead and execute high-stakes forensic investigations, ensuring legal defensibility and effective remediation.

GIAC Certified Forensic Analyst (GCFA) Training Course is meticulously designed to move beyond foundational knowledge, equipping practitioners with the scalable techniques necessary to investigate and remediate incidents across large, complex enterprise environments. Key areas of focus include leveraging native Windows and Linux artifacts for detection, identifying living off the land attacks, recovering and analyzing data from advanced file systems like NTFS, and applying threat intelligence to proactively search for hidden adversaries. By emphasizing practical, lab-based scenarios, the GCFA course builds the critical skills needed for root cause analysis, evidence handling with strict adherence to chain of custody, and delivering executive-level reporting to drive successful incident closure and significant cybersecurity career advancement for the modern DFIR specialist

Programme Curriculum

GIAC Certified Forensic Analyst (GCFA) Training Course

Introduction

The GIAC Certified Forensic Analyst training provides advanced, hands-on expertise in Digital Forensics, Incident Response, and Enterprise Threat Hunting. This course transforms security professionals into elite, lethal forensic analysts capable of tackling the most challenging cyber incidents, including Advanced Persistent Threats, internal/external data breaches, and sophisticated anti-forensic techniques. Participants will master the art of rapid volatile data acquisition, in-depth memory forensics, and complex timeline analysis to precisely reconstruct attack vectors and adversary tradecraft. The GCFA credential is recognized globally as the gold standard for demonstrating the ability to lead and execute high-stakes forensic investigations, ensuring legal defensibility and effective remediation.

GIAC Certified Forensic Analyst (GCFA) Training Course is meticulously designed to move beyond foundational knowledge, equipping practitioners with the scalable techniques necessary to investigate and remediate incidents across large, complex enterprise environments. Key areas of focus include leveraging native Windows and Linux artifacts for detection, identifying living off the land attacks, recovering and analyzing data from advanced file systems like NTFS, and applying threat intelligence to proactively search for hidden adversaries. By emphasizing practical, lab-based scenarios, the GCFA course builds the critical skills needed for root cause analysis, evidence handling with strict adherence to chain of custody, and delivering executive-level reporting to drive successful incident closure and significant cybersecurity career advancement for the modern DFIR specialist.

Course Duration

5 days

Course Objectives

1. Master advanced Incident Response processes and scale investigations across Enterprise Environments.
2. Perform deep-dive Memory Forensics to identify malicious processes, code injection, and advanced malware hiding techniques.
3. Utilize Timeline Analysis methodologies to reconstruct the sequence of events during a multi-stage intrusion with precision.
4. Effectively counter and compensate for modern Anti-Forensic Techniques, including file wiping and timestomping.
5. Conduct Host-Based Forensics on Windows and Linux systems to locate Indicators of Compromise (IOCs) and persistence mechanisms.
6. Perform proactive Threat Hunting using collected artifacts and threat intelligence to uncover hidden or dormant adversaries.
7. Analyze NTFS Artifacts and Volume Shadow Copies for deleted data recovery and evidence of user/attacker activity.
8. Identify and track Lateral Movement and Credential Theft using native system artifacts like logs, PowerShell, and WMI.
9. Develop legally sound and repeatable procedures for Evidence Acquisition and maintaining the Chain of Custody.
10. Determine the Root Cause Analysis and initial attack vector of a data breach or system compromise.
11. Apply forensic skills to investigate complex scenarios such as Ransomware attacks and Supply Chain Compromises.
12. Leverage automation and Triage Tools to perform rapid, scalable analysis on hundreds of endpoints simultaneously.
13. Integrate Cloud Forensics principles to analyze artifacts from cloud storage and platform services during investigations.

Target Audience

1. Experienced Digital Forensic Analysts
2. Senior Incident Response Team Leaders/Engineers
3. Advanced Security Operations Center (SOC) Analysts
4. Dedicated Threat Hunters
5. Information Security Consultants specializing in breach investigations
6. Law Enforcement and Government Agency Cyber Investigators
7. Red Team Members/Penetration Testers
8. Security Managers

Course Modules

1. Advanced Incident Response and Triage Methodology

- Defining the phases of the Incident Response Lifecycle in an enterprise context.
- Implementing scalable triage for rapid data collection from hundreds of endpoints.
- Understanding the Pyramid of Pain and applying Threat Intelligence to investigations.
- Leveraging command-line and scripting for remote evidence acquisition and analysis.
- Case Study: Investigating a large-scale phishing campaign where the initial compromise vector needed to be rapidly identified across a distributed network to contain the breach.

2. Deep-Dive Memory Forensics and Volatile Data

- Acquisition techniques for preserving volatile data and live system state.
- Using the Volatility Framework to analyze malicious processes and hidden artifacts.
- Identifying evidence of code injection, rootkits, and direct kernel object manipulation.
- Analyzing network connections, handles, and threads for Command and Control beaconing.
- Case Study: Analyzing memory from a system infected with fileless malware to identify the unique process injection technique and the attacker's communication method, which was invisible to disk-based scans.

3. File System and Anti-Forensics Detection

- Detailed analysis of the NTFS filesystem structure.
- Techniques for recovering deleted data and examining Alternate Data Streams.
- Identifying and countering anti-forensics activities such as timestomping and file wiping.
- Forensic examination of Volume Shadow Copies for pre-incident evidence and data recovery.
- Case Study: Uncovering a rogue insider who used file wiping tools to destroy evidence; the team recovered critical documents and executables by analyzing the residual data in the MFT and Volume Shadow Copies.

4. Windows Artifact Analysis and Evidence of Execution

- Analyzing Windows Registry artifacts for user activity, program execution, and system configuration changes.
- Interpreting Prefetch, ShellBags, and LNK files to determine application execution and lateral file access.
- In-depth analysis of Windows Event Logs and security auditing for critical security events.
- Tracking USB device usage and external media connection history.
- Case Study: Tracing an attacker's pivot point and privilege escalation path by correlating evidence from a suspicious Service Control Manager event log entry with a newly created Run key in the Registry.

5. Timeline Creation and Correlation

- Developing a comprehensive Super Timeline by integrating disparate sources of data.
- Methodology for normalizing and visualizing event data to pinpoint critical moments in the attack.
- Using timelines for rapid Root Cause Analysis and identifying the initial breach vector.
- Correlating activities across multiple compromised systems to track Lateral Movement.
- Case Study: Creating a timeline that successfully correlated an outbound C2 beacon, a suspicious PowerShell command, and a new account creation to map out an entire APT intrusion over a three-week period.

6. Attacker Tradecraft and Advanced Techniques

- Investigating "Living Off the Land" attacks using native tools like PowerShell and WMI.
- Detecting and tracking Credential Theft techniques, including Mimikatz and Pass-the-Hash.
- Analyzing Malware Persistence Mechanisms beyond simple Run keys and services.
- Identifying data staged for exfiltration and tracking its movement.
- Case Study: Discovering a sophisticated attacker who used WMI event subscriptions for long-term persistence, requiring forensic analysis of the WMI repository to uncover the hidden scheduled task.

7. Threat Hunting and Proactive Forensics

- Shifting from reactive IR to proactive Threat Hunting using forensic artifacts as data sources.
- Developing and deploying IOCs and custom detection rules based on unique adversary signatures.
- Applying intelligence-driven hunting loops
- Leveraging large-scale data analysis platforms for enterprise-wide hunting.
- Case Study: Proactively hunting for a known adversary's TTPs by searching for specific PowerShell command strings in endpoint telemetry logs, leading to the discovery of a long-term dormant backdoor on a critical server.

8. Enterprise Response, Reporting, and Legal Readiness

- Developing an effective remediation plan and leading the incident containment strategy.
- Structuring forensic findings into legally sound, executive-level forensic reports.
- Ensuring meticulous Chain of Custody documentation for potential litigation.
- Briefing management on attack scope, impact, and essential next steps for hardening defenses.
- Case Study: Presenting forensic findings to a corporate legal team following a major data breach, demonstrating the strict adherence to the chain of custody and the technical evidence required for a civil lawsuit against the perpetrators.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com