Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

GIAC Certified Forensic Examiner

Course Description & Overview

SecureNinja's GIAC* Certified Forensic Examiner (GCFE) certification training provides cybersecurity professionals with the skills necessary to conduct formal digital forensic investigations and analysis. This course focuses on the use of forensic tools and methodologies to collect, examine, and interpret digital evidence from Windows-based systems, supporting both internal incident response and legal proceedings.

Designed by GIAC (Global Information Assurance Certification), the GCFE certification is ideal for professionals investigating cybercrimes, data breaches, insider threats, and policy violations. Students will gain hands-on experience with industry tools and learn to analyze artifacts such as Windows Registry entries, browser histories, file systems, and log data. Participants will walk away with practical skills to support corporate investigations, legal cases, and security incident analysis.

Why Choose GCFE

- Digital Forensics Expertise: Validates the ability to perform deep forensic analysis of Windows operating systems.
- Hands-On Training: Real-world case scenarios and exercises to develop practical investigative skills.
- Legal and Incident Response Support: Covers evidence handling, documentation, and report writing for legal defensibility.
- Respected Industry Certification: Recognized globally by government agencies, law enforcement, and private sector organizations.

Topics Covered

- Windows Forensic Fundamentals: Core concepts, forensic imaging, and acquisition techniques.
- File System Forensics: Analysis of NTFS, FAT, and file metadata.
- Windows Registry and Event Logs: Interpreting system artifacts and audit trails.
- Browser and Email Analysis: Recovering data from browsers, mail clients, and internet traces.
- Timeline and Evidence Correlation: Constructing timelines and correlating events across multiple artifacts.
- Evidence Handling and Documentation: Ensuring chain of custody and preparing forensic reports.

Who is it for

- Digital Forensic Analysts: Professionals responsible for conducting internal or legal forensic investigations.
- Incident Responders: Security teams responding to data breaches and policy violations.
- Security Consultants: Experts supporting forensic and investigation efforts across clients.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Law Enforcement Personnel: Officers and agents involved in cybercrime and electronic evidence gathering.

Who Would Benefit

- System Administrators: IT pros seeking skills to support internal investigations.
- IT Auditors: Professionals evaluating system integrity and evidence trails.
- Legal Advisors: Attorneys and compliance officers seeking understanding of digital evidence handling.

Prerequisites

Familiarity with Windows operating systems, file systems, and general cybersecurity concepts is recommended. No prior forensic experience is required, but basic knowledge of incident response and IT administration is helpful.

Course Outline

1. Module 1: Introduction to Forensics

   - Forensic principles, evidence handling, and legal considerations.
   - Digital evidence lifecycle and chain of custody.

2. Module 2: Windows Operating System Artifacts

   - User activity logs, Registry keys, and event log interpretation.
   - Prefetch, link files, and shellbags analysis.

3. Module 3: File and Application Forensics

   - Browser history, cache, cookies, and email artifacts.
   - Analyzing document metadata and shadow copies.

4. Module 4: Timeline Analysis and Reporting

   - Creating and analyzing event timelines.
   - Correlating evidence across multiple sources and writing reports.

Course Length

- 5 Days
- 40 Hours

Exam Details

- OPEN BOOK EXAM
- Number of Questions: 82
- Question Types: Multiple-choice
- Duration: 3 Hours
- Passing Score: 70%

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

The GIAC Certified Forensic Examiner (GCFE) certification is a vital credential for professionals working in digital forensics, incident response, and internal investigations. With a focus on real-world skills and legal readiness, this course ensures that participants are well-prepared to support security operations, conduct forensic analysis, and present findings with confidence and accuracy.