Certified Computer Examiner 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

Certified Computer Examiner Training Course is designed to empower participants with the core skills and advanced techniques necessary to conduct legally sound and forensically meticulous digital investigations. In an era of escalating cybercrime and complex eDiscovery requirements, certified examiners are critical for organizations, law enforcement, and legal entities. This program provides a vendor-neutral methodology for acquiring, preserving, analyzing, and presenting digital evidence from various operating systems and devices, ensuring the integrity and admissibility of findings in a court of law. Graduates will be equipped to tackle real-world scenarios, from internal fraud and intellectual property theft to complex security breaches and criminal cases, solidifying their role as trusted forensic experts.

The curriculum emphasizes hands-on practical experience across the entire forensic process from the initial incident response and evidence acquisition to artifact analysis, data recovery, and professional report writing. Focus areas include deep dives into modern file systems, mobile device forensics, cloud forensics, and understanding anti-forensics techniques. By integrating ethical considerations, legal frameworks, and advanced tools, this certification positions the examiner at the forefront of the digital forensics field, ready to meet the burgeoning global demand for highly skilled cybersecurity investigators and computer forensics analysts who can deliver clear, defensible, and impactful findings.

Programme Curriculum

Certified Computer Examiner Training Course

Introduction

Certified Computer Examiner Training Course is designed to empower participants with the core skills and advanced techniques necessary to conduct legally sound and forensically meticulous digital investigations. In an era of escalating cybercrime and complex eDiscovery requirements, certified examiners are critical for organizations, law enforcement, and legal entities. This program provides a vendor-neutral methodology for

acquiring, preserving, analyzing, and presenting digital evidence from various operating systems and devices, ensuring the integrity and admissibility of findings in a court of law. Graduates will be equipped to tackle real-world scenarios, from internal fraud and intellectual property theft to complex security breaches and criminal cases, solidifying their role as trusted forensic experts.

The curriculum emphasizes hands-on practical experience across the entire forensic process from the initial incident response and evidence acquisition to artifact analysis, data recovery, and professional report writing. Focus areas include deep dives into modern file systems, mobile device forensics, cloud forensics, and understanding anti-forensics techniques. By integrating ethical considerations, legal frameworks, and advanced tools, this certification positions the examiner at the forefront of the digital forensics field, ready to meet the burgeoning global demand for highly skilled cybersecurity investigators and computer forensics analysts who can deliver clear, defensible, and impactful findings.

Course Duration

5 days

Course Objectives

1. Master the legal and ethical protocols to ensure chain of custody and the admissibility of digital evidence in civil and criminal proceedings.
2. Perform forensically sound data acquisition across Windows, Linux, and macOS platforms without compromising evidence integrity.
3. Deeply analyze complex file systems to recover and interpret hidden, deleted, or fragmented data.
4. Identify and extract critical user activity data from the Windows Registry, system logs, shellbags, and link files.
5. Utilize specialized techniques and tools for data carving and recovery from unallocated space, damaged media, and encrypted volumes.
6. Integrate forensic procedures seamlessly into an overall incident response and threat hunting framework.
7. Apply specialized techniques to acquire and analyze data from modern mobile devices and mobile application artifacts.
8. Investigate data and user activity residing in Cloud Computing environments
9. Analyze network traffic, logs, and firewall data to trace and reconstruct network intrusion events.
10. Perform static and dynamic analysis to understand the behavior of malware and isolate relevant system artifacts.
11. Understand the role of the examiner in the electronic discovery reference model and litigation support.
12. Recognize and counter techniques used by adversaries to obfuscate, encrypt, or destroy digital evidence.
13. Develop professional, defensible forensic reports and effectively present technical findings as an Expert Witness in court.

Target Audience

1. Law Enforcement Officials.
2. Corporate Investigators/Auditors.
3. Digital Forensics Analysts/Examiners.
4. Incident Response Team Members.
5. IT Security Professionals.
6. Legal Professionals.

7. Government/Military Personnel
8. Information Security Consultants.

Course Modules

Module 1: Foundational Principles & Legal Framework

- The Digital Forensics Methodology
- Legal & Ethical Considerations.
- Forensic Readiness.
- Hashing, Write-Blocking, Volatile and Non-Volatile Data.
- Case Study: Analyzing a corrupted hard drive where improper seizure led to the evidence being thrown out of court.

Module 2: Evidence Acquisition and Preservation

- Live and Dead Acquisition
- Imaging Tools and Validation.
- File System Fundamentals.
- RAID, Volume Shadow Copy, and Encryption.
- Case Study: Simulating a server shutdown scenario and executing a triage plan to capture volatile data before the system goes offline.

Module 3: Windows Operating System Forensics

- Registry Analysis.
- User Artifacts.
- System Logs and Timelines.
- Internet and Application Artifacts.
- Case Study: Tracking an employee who exfiltrated sensitive data using a USB drive by analyzing registry and link file artifacts.

Module 4: Advanced Data Recovery and Analysis

- Data Carving Techniques.
- File Signature Analysis.
- Recovering Deleted Files.
- Developing efficient search strategies using Regular Expressions for targeted evidence discovery.
- Case Study: Recovering highly incriminating financial records that a suspect believed they had permanently deleted by using data carving tools.

Module 5: Mobile Device and Emerging Technology Forensics

- Mobile Acquisition Methods.
- Mobile Artifacts.
- Introduction to Cloud Forensics.
- Mac and Linux Forensics.
- Case Study: Investigating a blackmail scheme by performing a physical extraction and analyzing chat logs and encrypted data from a seized smartphone.

Module 6: Network and Incident Forensics

- Network Fundamentals for the Examiner.
- Traffic Analysis
- Web Server Forensics.
- Malware and Reverse Engineering Basics.
- Case Study: Tracing the source of a network intrusion by analyzing firewall and IDS/IPS logs and correlating timestamps with forensic artifacts.

Module 7: Specialized Investigation and Anti-Forensics

- Email Forensics.
- Anti-Forensics Countermeasures.
- Internet of Things (IoT) Forensics.
- Memory Forensics.
- Case Study: Uncovering evidence hidden using steganography within innocent-looking image files found on a suspect's machine.

Module 8: Reporting, Presentation, and Expert Testimony

- Forensic Report Writing.
- Expert Witness Preparation.
- Tool Validation and Documentation.
- Peer Review and Quality Assurance.
- Case Study: Developing a mock report and participating in a simulated cross-examination session based on a complex insider threat case.

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.com 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
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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