INFOSEC Skills
LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

Computer and Mobile Forensics Boot Camp

Learn how to investigate cybercrime! This popular boot camp goes in-depth into the tools, techniques and processes used by forensics examiners to find and extract evidence from computers and mobile devices.

Course description

Infosec's Computer and Mobile Forensics Boot Camp teaches you how to identify, preserve, extract, analyze and report forensic evidence on computers and mobile devices. You will learn about the challenges of computer and mobile forensics, walk through the process of analysis and examination of operating systems and mobile devices, and gain a deep understanding of differences in evidence locations and examination techniques on Windows and Linux computers and Android, iOS and Windows phones.

More than 30 hands-on labs simulating a real cybercrime investigation provide you with practical experience using commercial and open-source forensic tools. The boot camp also prepares you to earn two popular certifications: the Certified Computer Forensics Examiner (CCFE) and the Certified Mobile Forensics Examiner (CMFE).

Who should attend

- Law enforcement professionals looking to expand into computer crime investigations
- Legal professionals
- IT and information security professionals being tasked with corporate forensics and incident handling
- Anyone with a desire to learn about computer forensics and develop their skills

Boot camp at a glance

Hands-on training

- ✓ Build your skills with dozens of hands-on labs
- ✓ Extract and analyze different types of data
- ✓ Explore forensics via memory, browsers, email and more!

Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 7-day boot camp
- ✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

What's included

- Seven days of expert, live forensics training
- Exam Pass Guarantee
- Exam voucher
- Unlimited practice exam attempts
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Onsite proctoring of exam
- Pre-study learning path
- Knowledge Transfer Guarantee

Prerequisites

Students must have no criminal record. Basic computer skills, including the ability or desire to work outside the Windows GUI interface, are necessary. A+ certification and/or similar training and experience is not required, but recommended.

This is a very in-depth training course and is not intended for individuals who have limited or no computer skills.

Boot camp overview

After completing this boot camp, you will be certified with the following certifications:

- **Certified Computer Forensics Examiner (CCFE):** The CCFE certification validates your knowledge of nine domains related to the computer forensics evidence recovery and analysis process.
- **Certified Mobile Forensics Examiner (CMFE):** The CMFE certification validates your knowledge of five domains related to performing the mobile forensics process on different types of mobile devices.

Hands-on labs

Play the part of a forensic examiner in our custom lab environment. More than 30 labs containing over a hundred exercises follow a cohesive scenario, providing you with a complete experience of a forensic investigation, from identifying evidence in a crime scene to extracting and examining artifacts from the suspect's and victim's computers. You will use popular commercial and open-source tools to practice and learn new skills in forensics image creation and analysis, examining file signatures and metadata, memory forensics, browser and email forensics, examining social media and cloud artifacts, and many other areas of forensic analysis.

What you'll learn

- Provisions of IT law
- Complex technical forensics concepts
- How to apply forensics concepts to forensic investigations
- Evidence-handling procedures and the general rules of evidence
- Key technologies used in computers and mobile devices
- Full range of computer forensics tools
- Acquiring forensic evidence
- Locating forensic artifacts in various operating systems
- Analyzing extracted evidence
- Properly reporting findings
- Skills needed to track an offender on the internet
- How to work with law enforcement
- How to design an incident response strategy

Skill up and get certified, guaranteed

Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

What our students are saying

I really appreciate that our instructor was extremely knowledgeable and was able to provide the information in a way that it could be understood. He also provided valuable test-taking strategies that I know not only helped me with this exam, but will help in all exams I take in the future.

Michelle Jemmott

Pentagon

Excellent! Our instructor had a vast background and related the materials to real life. Much better than just teaching the materials to pass an exam ... but he did that as well. He went out of his way in class. The extra materials really benefited us when we returned to our real jobs! Great experience!

John Peck

EPA

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

Sylvia Swinson

Texeltek

The instructor was able to take material that prior to the class had made no sense, and explained it in real world scenarios that were able to be understood.

Erik Heiss

United States Air Force

The course was extremely helpful and provided exactly what we needed to know in order to successfully navigate the exam. Without this I am not confident I would have passed.

Robert Caldwell

Salient Federal Solutions

Computer and Mobile Forensics details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
Morning session	Introduction	Forensic science fundamentals Hardware	File and operating system forensics	Network forensics Packet analysis	New and emerging tech Mobile forensics introduction	Mobile forensics process	iOS forensics Windows phone
Afternoon session	Digital evidence — legal issues	File systems	Web and application forensics	Anti-forensics	Take CCFE exam	Android forensics	Feature phone Take CMFE exam
Evening session	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

Day 1

Course introduction

» Computer forensics and investigation as a profession

» Define computer forensics

» Describe how to prepare for computer investigations and explain the difference between law enforcement agency and corporate investigations

» Explain the importance of maintaining professional conduct

Digital evidence — legal issues

» Identifying digital evidence

» Evidence admissibility

» Federal rules of evidence

» Daubert standard

» Discovery

» Warrants

» What is seizure?

» Consent issues

» Expert witness

» Roles and responsibilities

» Ethics

» (ISC)^2

» AAFS

» ISO

Investigations

» Investigative process

» Chain of custody

» Incident response

» E-discovery

- Criminal vs. civil vs. administrative investigations
- Intellectual property
  - Markman hearing
- Reporting
- Quality control
  - Lab and tool
  - Investigator
  - Examination
  - Standards
- Evidence management
  - SOPS
  - Collection
  - Documentation
  - Preservation
  - Transport/tracking
  - Storage/access control
  - Disposition
- Current computer forensics tools and hardware
  - Commercial
  - Free/open source

Day 2

Forensic science fundamentals

- Principles and methods
  - Locard's Principle
  - Inman-Rudin Paradigm
  - Scientific method
  - Peer review
- Forensic analysis process

Hardware

- Storage media
  - Hard disk geometry
  - Solid state drives
  - RAIDS
- Operating system
  - Boot process
  - BIOS/CMOS
  - The Swap File

File systems

- File systems
  - NTFS file system
  - FAT file system
  - HFS+
  - Ext2/3/4
  - Embedded
- Erased vs. deleted
- Live forensics

Day 3

File and operating system forensics

- Keyword searching
- Metadata
- Timeline analysis
- Hash analysis
- File signatures
  - File filtering (KFF)
- Volume Shadow Copies
- Time zone issues
- Link files
- Print spool
- Deleted files
  - Recycle bin forensics
- File slack
- Damaged media
  - Physical damage
  - Logical damage
  - File carving
- Registry forensics
  - USB devices
  - HKLM
- Multimedia files
  - EXIF data
- Compound files
  - Compression
  - Ole
  - AD
  - Passwords

Web and application forensics

- Common web attack vectors
  - SQL injection
  - Cross-site scripting
  - Cookies

- Browser artifacts
- Email investigations
  - Email headers
  - Email files
- Messaging forensics
- Database forensics
- Software forensics
  - Traces and application debris
  - Software analysis (hashes, code comparison techniques, etc.)
- Malware analysis
  - Malware types and behavior
  - Static vs. dynamic analysis

Day 4

Network forensics

- TCP/IP
  - IP addressing
  - Proxies
  - Ports and services
- Types of attacks
- Wired vs. wireless
- Network devices forensics
  - Routers
  - Firewalls
  - Examining logs

Packet analysis

- OS utilities
  - Netstat
  - Net sessions
  - Openfles
- Network monitoring tools
  - SNORT
  - Wireshark
  - NetworkMiner

Anti-forensics

- Hiding
  - Encryption
  - Symmetric
  - Asymmetric
  - TrueCrypt hidden partitions
- Steganography
- Packing
- Hidden devices (NAS)
- Tunneling/Onion routing
- Destruction
  - Wiping/overwriting
  - Corruption/degaussing
- Spoofing
  - Address spoofing
  - Data spoofing
  - Timestomping
- Log tampering
- Live operating systems

Day 5

New & emerging technology

- Legal issues (privacy, obtaining warrants)
- Social networks forensics
- Types of social networks
- Types of evidence
- Collecting data
- Virtualization
- Virtualization forensics
- Use of virtualization in forensics
- Cloud forensics
- Types of cloud services
- Challenges of cloud forensics
- Big data
- Control systems and IOT

Mobile forensics introduction

- Types of devices
- GPS
- Cell phones
- Tablets
- Vendor and carrier identification
- Obtaining information from cellular provider
- GSM vs. CDMA
- Common tools and methodology

Day 6

Mobile forensics process

- Mobile forensics challenges
  - OS variety
  - Differences in hardware and filesystems
  - Security features
  - Data volatility
  - Cloud storage
- Types of evidence found on mobile devices
- Collecting mobile devices at the scene
  - Locating devices
  - Preserving volatile data
  - Physical components and accessories (SIM cards, SD cards, chargers, etc.)
  - Older phones and devices
- Comparison of mobile operating systems
  - Android
  - iOS
  - Windows phone
  - Blackberry OS
- Data acquisition methods
  - Logical acquisition
  - Physical acquisition
  - Manual acquisition
- Reporting findings

Android forensics

- Android platform
  - Hardware
  - SDK and debug bridge
  - File systems and data structures
- Android security model
  - Secure kernel and permissions
  - Full disk encryption
  - App security
- Bypassing Android security features
  - Bootloader/recovery mode
  - Rooting an Android device
  - Lock screen bypassing techniques
- Android logical data acquisition and analysis
  - Extracting the /data directory
  - Device information
  - SMS/MMS, email, browsing and social networking data
  - App and cloud data
- Android physical data acquisition
  - Hardware-based techniques
  - JTAG
  - Chip-off
  - Android data recovery techniques

Day 7

iOS forensics

- Apple iOS platform
  - iOS devices and hardware
  - iOS versions, file system and architecture
- iOS security
  - Passcode and Touch ID
  - Privilege separation
  - ASLR and data execution prevention
  - Encryption
- Bypassing iOS security features
  - Operating modes of iOS devices
  - Custom RAMDisk
  - Jailbreaking
  - Bypassing passcode
  - Breaking iOS device encryption keys
  - Establishing trusted communication with desktop computer
- iOS data acquisition and analysis
  - SQLite databases
  - Property lists
  - Other important files (cookies, keyboard cache, recordings, etc.)
- iPhone/iCloud backups
  - Backup structure
  - Extracting and examining unencrypted backups
  - Encrypted backups (extracting and decrypting the keychain)
- iOS data recovery techniques

Windows phones

- Windows Phone OS: partitions and filesystems

- Windows Phone security features
  - Secure boot
  - Application security and data protection
- Windows Phone logical acquisition and analysis
  - Sideloading
  - Extracting SMS, email and application data
- Windows 10 mobile OS forensics

Feature phones forensics

- Acquiring and examining data from feature phones

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.