INFOSEC Skills

LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

Mobile Forensics Boot Camp

Learn how to use mobile forensics to investigate cybercrime! Our Mobile Forensics Boot Camp builds your skills in a hands-on lab environment so you can apply what you learned the day you leave training.

Course description

This highly technical, hands-on boot camp is designed to provide you with in-depth coverage of critical techniques and information about identifying, preserving, extracting, analyzing and reporting forensic evidence on mobile devices through the use of the most popular mobile forensic tools. You will learn about the challenges of mobile forensics, walk through the analysis and examination of mobile devices, and gain a deep understanding of differences in evidence locations and examination techniques in Android, iOS and Windows phones. Extracting cloud data and examining feature phones is also covered.

This boot camp also prepares you to become a Certified Mobile Forensics Examiner (CMFE) and provides practical, hands-on labs that help you to hit the ground running the day your boot camp ends.

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 emails, SMS, deleted items and more!

Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 2-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

» Two 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

This boot camp prepares you to become a Certified Mobile Forensics Examiner. The CMFE certification validates your knowledge of five domains related to the mobile forensics evidence recovery and analysis process:

- Mobile forensics process
- Android forensics
- iOS forensics
- Windows phones
- Feature phone forensics

Hands-on labs

Our scenario-based, hands-on labs simulate a real cybercrime investigation. You'll gain practical skills in locating and examining evidence on devices and forensic images, as well as analyzing and reporting findings. You'll work with with various commercial and open-source forensic tools within our unique cloud-based learning environment.

What you'll learn

- Applying advanced computer forensics analysis concepts to mobile devices
- File carving tools and techniques
- The HFS+ file system
- Browsing the devices with SSH
- Reading SQLlite data stores
- Jailbreaking
- Breaking device encryption keys
- Data protection for keychain items
- Recovering keyboard caches
- Recovering deleted photo library and camera roll images
- Recovering deleted browser cache items and other personal data
- Recovering hidden call history data
- Recovering map tiles from maps application
- Analyzing cached and deleted email messages
- Analyzing recovered SMS messages with timestamp data
- Analyzing deleted voicemails
- Establishing trusted pairing relationships with one or more desktop computers
- Writing forensic reports

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

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
Morning session	Mobile forensics process	iOS forensics Windows phone
Afternoon session	Android forensics	Feature phone Take CMFE exam
Evening session	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

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 2

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.

INFOSEC