Digital Forensics on macOS and Mobile Devices 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

In the contemporary digital landscape, the exponential proliferation of macOS and diverse Mobile Devices has created a significant challenge and a new frontier for Digital Forensics and Incident Response professionals. Traditional forensic methodologies often fall short due to platform-specific artifacts, sophisticated encryption mechanisms, and the pervasive shift towards Cloud Forensics. Digital Forensics on macOS and Mobile Devices Training Course is designed to equip investigators, security analysts, and law enforcement with the advanced technical skills necessary to navigate the complex architectures of Apple?ÇÖs operating systems and modern mobile platforms. Attendees will master forensically sound data acquisition, intricate file system analysis, and the manual and automated decoding of critical user-generated and system-level artifacts, ensuring the preservation of digital evidence and maintaining an unbreakable chain of custody.

This intensive course will deliver hands-on experience with industry-leading commercial and open-source forensic tools, focusing on practical application in real-world cybercrime investigations and corporate security breaches. By diving deep into areas like encrypted backups, third-party application analysis, volatile memory forensics, and location data reconstruction, participants will gain the ability to uncover hidden data and create comprehensive, legally sound forensic reports. The curriculum addresses key 2025 trending keywords such as AI in forensics, IoT device evidence, and the forensic challenges posed by advanced data encryption and anti-forensics techniques, positioning graduates as subject matter experts in this high-demand, rapidly evolving field of cybersecurity

Programme Curriculum

Digital Forensics on macOS and Mobile Devices Training Course

Introduction

In the contemporary digital landscape, the exponential proliferation of macOS and diverse Mobile Devices has created a significant challenge and a new frontier for Digital Forensics and Incident Response professionals. Traditional forensic methodologies often fall short due to platform-specific artifacts, sophisticated encryption mechanisms, and the pervasive shift towards Cloud Forensics. Digital Forensics on macOS and Mobile Devices Training Course is designed to equip investigators, security analysts, and law enforcement with the advanced technical skills necessary to navigate the complex architectures of Apple?ÇÖs operating systems and modern mobile platforms. Attendees will master forensically sound data acquisition, intricate file system analysis, and the manual and automated decoding of critical user-generated and system-level artifacts, ensuring the preservation of digital evidence and maintaining an unbreakable chain of custody.

This intensive course will deliver hands-on experience with industry-leading commercial and open-source forensic tools, focusing on practical application in real-world cybercrime investigations and corporate security breaches. By diving deep into areas like encrypted backups, third-party application analysis, volatile memory forensics, and location data reconstruction, participants will gain the ability to uncover hidden data and create comprehensive, legally sound forensic reports. The curriculum addresses key 2025 trending keywords such as AI in forensics, IoT device evidence, and the forensic challenges posed by advanced data encryption and anti-forensics techniques, positioning graduates as subject matter experts in this high-demand, rapidly evolving field of cybersecurity

Course Duration

5 days

Course Objectives

1. Master Forensically Sound Acquisition techniques for both locked macOS and encrypted mobile devices.
2. Perform in-depth analysis of the Apple File System and HFS+ for file carving and metadata recovery.
3. Utilize Live and Memory Forensics methods to extract volatile data from running macOS systems.
4. Acquire and decrypt data from iOS and Android full file systems and logical extractions using advanced tools.
5. Analyze platform-specific artifacts, including Unified Logging, Spotlight, plist files, and user account activity on macOS.
6. Investigate data from popular third-party messaging and social media applications on mobile devices.
7. Reconstruct user activity timelines and analyze geolocation artifacts from mobile and macOS devices.
8. Identify and analyze traces of mobile malware and spyware on both Android and jailbroken/non-jailbroken iOS devices.
9. Address the challenges of Cloud Forensics, specifically iCloud and Google backup analysis, and data retrieval.
10. Apply scripting for custom artifact parsing and automating large-scale data analysis, leveraging principles of AI in Forensics.
11. Implement proper Chain of Custody and evidence handling procedures that comply with legal and ethical standards.
12. Detect and overcome common Anti-Forensics Techniques like data wiping, encryption, and artifact obfuscation.
13. Prepare clear, concise, and Court-Admissible Forensic Reports detailing findings, methodologies, and conclusions.

Target Audience

1. Digital Forensics Investigators

2. Cybersecurity Incident Responders
3. eDiscovery Professionals and Legal Technologists
4. Information Security Analysts
5. Malware Analysts specializing in mobile and macOS threats
6. Corporate Security and Internal Audit teams
7. IT Professionals seeking a specialization in digital evidence
8. Government and Intelligence Agency analysts

Course Modules

1. Fundamentals of macOS and Mobile Forensics

- Preservation, Acquisition, Examination, Analysis, and Reporting.
- Understanding macOS architecture, HFS+ and APFS, and user/system directories.
- Mobile OS architectures
- Setting up a fully secure and compliant Forensic Workstation and lab environment.
- Case Study: Investigating a corporate data leak traced to a former employee's encrypted MacBook Pro running APFS.

2. macOS Data Acquisition and Triage

- Live Forensics techniques
- Imaging methods.
- Analyzing Unified Logging system
- Extracting evidence from plist files, Keychain, and Spotlight metadata.
- Case Study: Responding to a persistent threat actor on a live Mac server; capturing and analyzing the system's volatile memory.

3. Deep-Dive iOS Forensics

- iOS data acquisition.
- Analysis of system artifacts
- Encrypted Backup analysis and decryption techniques.
- Location services forensics.
- Case Study: Extracting communication logs and deleted photos from a seized, locked, and fully encrypted iPhone involved in a criminal investigation.

4. Advanced Android Forensics

- Android acquisition methodologies.
- File system analysis.
- Investigating third-party applications and their data storage
- Analyzing device health, usage, and connection artifacts
- Case Study: Recovering chat data and a deleted video from a rooted Android device used in an intellectual property theft case.

5. Application and Artifact Analysis

- Detailed analysis of web browser artifacts for internet history and downloads.
- Email forensics and recovery from native clients on both mobile and macOS.
- Reconstructing event timelines using data correlation across multiple devices and operating systems.
- Scripting with Python for forensics.

- Case Study: Correlating browser history from a macOS desktop with location data from an Android phone to establish a coherent timeline of user actions.

6. Cloud, Malware, and IoT Forensics

- Fundamentals of Cloud Forensics.
- Identifying and analyzing mobile spyware and ransomware artifacts on both platforms.
- Forensics on companion devices.
- Understanding and mitigating Anti-Forensics techniques such as secure erase and steganography.
- Case Study: Tracing the command-and-control communication of a sophisticated piece of macOS-specific ransomware and identifying the encryption key fragments in memory.

7. Advanced Data Recovery and Analysis

- Deep dive into SQLite database forensics.
- Advanced File Carving techniques for fragmented or corrupted mobile and macOS storage.
- Data correlation and visualization techniques for complex investigations.
- Automating analysis using professional forensic suites
- Case Study: Performing an SSD file carving operation on a degraded MacBook SSD to recover key financial documents thought to be permanently deleted.

8. Legal Procedures and Reporting

- Maintaining the Chain of Custody and preparing evidence for legal proceedings.
- Admissibility of digital evidence in court.
- Drafting comprehensive, defensible Forensic Examination Reports for technical and non-technical audiences.
- Preparing for and delivering expert witness testimony.
- Case Study: Critiquing a sample forensic report to identify procedural and technical flaws that could lead to evidence exclusion in a court of law.

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	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100
05 Oct 2026	09 Oct 2026	Online	$1,100
12 Oct 2026	16 Oct 2026	Online	$1,100
19 Oct 2026	23 Oct 2026	Online	$1,100
26 Oct 2026	30 Oct 2026	Online	$1,100

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

Register Online Now

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