CONCEPT

Mobile Forensics: iOS and Android Acquisition, App Artefacts and Evidential Reporting

7 – 11 June 2027
Amsterdam - Zuidas business district hotel

Mobile Forensics: iOS and Android Acquisition, App Artefacts and Evidential Reporting

Ref: 471_14420 **Date:** 7 – 11 June 2027 **Location:** Amsterdam - Zuidas business district hotel **Fees:** 23500 SAR

Introduction:

Mobile forensics now supplies the decisive evidence in fraud, harassment, data theft and security incidents, yet handset examinations are still lost to devices left connected to the network, acquisitions chosen without a written rationale and tool output reported without any validation. This Core Concept course trains examiners to preserve, acquire and analyse iOS and Android devices in lawful, authorised cases and to explain each step. Working on test images in a lab, participants produce a Mobile Device Examination Report and Acquisition Decision Record ready for evidential scrutiny.

Course Objectives:

- Isolate, label and preserve seized handsets, SIM cards and memory cards so that their data stays unchanged from seizure to examination
- Explain iOS and Android storage, encryption and app sandbox design and the effect each has on recoverable evidence
- Select and justify a logical, file system, full file system or physical acquisition for a given device state and case question
- Analyse messaging, location, media and browser artefacts and recover deleted records from SQLite databases on test images
- Validate forensic tool output against known reference data and cross-check results between two independent tools
- Write an examination report that states method, findings, limitations and examiner opinion to an evidential standard

Target Audience:

- Digital forensic examination functions that acquire and analyse phones and tablets for criminal, civil or internal cases
- Investigation functions in policing, anti-fraud and corporate security that submit handsets for examination and use the findings
- Incident response functions that must preserve mobile evidence when an employee device is involved in a breach
- Forensic laboratory quality functions responsible for tool validation, method records and peer review
- Cyber crime and electronic evidence units that present handset findings to prosecutors, tribunals or courts

Course Outline:

Day 1: Mobile Evidence Foundations and Handset Seizure

- Mobile Device Forensics Scope: Phones, Tablets, Wearables and Removable Memory Cards
- Lawful Authority and Examination Request Review Before a Handset Is Handled
- Seizure Decisions for Powered-On, Powered-Off and Screen-Locked Devices
- Radio Isolation with Faraday Bags and Shielded Enclosures Versus Airplane Mode
- Handset Exhibit Labelling, Photography and Custody Continuity for SIM and Memory Cards

Day 2: Mobile Forensic Guidance and iOS and Android Architecture

- NIST Guidelines on Mobile Device Forensics: Preservation, Acquisition, Examination and Reporting
- ISO/IEC 27037 Identification, Collection, Acquisition and Preservation Applied to Handsets
- iOS Platform Architecture: APFS Volumes, Sandboxed App Containers and Property Lists
- Android Platform Architecture: Partitions, ext4 and F2FS File Systems and Per-App Data Directories
- Encryption at Rest, Lock States and Their Effect on Recoverable Data

Day 3: Acquisition Types, SIM, Backup and Cloud Evidence

- Acquisition Hierarchy: Logical, File System, Full File System and Physical Extraction Concepts
- Acquisition Decision Matrix by Device State, Authority and Case Question
- Local Device Backups as Evidence: Backup Structure and Encrypted Backup Handling
- SIM and UICC Evidence: ICCID, IMSI, Stored Contacts and SMS Records
- Cloud Account and Synchronised Data: Legal Process, Scope Limits and Provenance

Day 4: App Artefacts, Deleted Data and Tool Validation

- Messaging App Databases: Conversations, Attachments, Group Membership and Read States
- Location Artefacts: Photo EXIF Geotags, Wi-Fi Connection History and Cell Records
- Browser History, Media Metadata and Thumbnail Caches as Corroborating Artefacts
- SQLite Deleted Record Recovery: Freelists, Write-Ahead Logs and Unallocated Pages
- Forensic Tool Validation with Reference Test Images and Cross-Tool Result Comparison

Day 5: Handset Examination Lab Cases and Evidential Reporting

- Lab Case: Android Test Image Messaging and Location Reconstruction
- Lab Case: iOS Test Image Media, Browser and Deleted Message Recovery
- Handset Event Timeline Build with Time Zone and Clock Offset Normalisation
- Mobile Device Examination Report and Acquisition Decision Record Drafting
- Peer Review and Expert Witness Questioning on Handset Findings

Skills You Will Gain:

- Handset Seizure and Isolation
- Mobile Platform Architecture
- Acquisition Method Selection
- App Artefact Analysis
- SQLite Record Recovery
- Forensic Tool Validation
- Mobile Timeline Reconstruction
- Expert Witness Reporting

Why Attend This Course:

- Return with a Mobile Device Examination Report and Acquisition Decision Record built from full lab cases on iOS and Android test images
- Defend the choice of acquisition method and every limitation in plain terms under cross-examination
- Catch parsing gaps and misattributed artefacts before they reach a report by checking one tool against another
- Compare handset examination practice with examiners and investigators from policing, banking, telecoms and corporate security

Conclusion:

A handset finding carries weight only when the device was isolated, the acquisition was justified and the tool output was checked. The course moves from seizure and radio isolation, through the NIST guidelines, ISO/IEC 27037 and iOS and Android architecture, to acquisition types, SIM, backup and cloud evidence, then to app artefacts, SQLite recovery and tool validation. The final day applies the method to lab cases and produces a Mobile Device Examination Report and Acquisition Decision Record for evidential use.