COURSE CATEGORY: DIGITAL FORENSIC INVESTIGATIONS
COURSE LEVEL: ESSENTIALS
COURSE CODE: IFIS DF1/02
COURSE NAME: MAC AND iOS FORENSIC ANALYSIS AND INCIDENT RESPONSE

0101 010 IFIS
Institute of Forensics & ICT Security
Forensics. Security. Training

With practical skills, You succeed

Institute of Forensics & ICT Security
Forensics. Security. Training

With practical skills, You succeed

About this Course

This course aims to enable investigators to investigate the apple devices they encounter. The increasing popularity of Apple devices can be seen everywhere, from college reading rooms, television, restaurants to corporate boardrooms. Dealing with these devices as an investigator is no longer a niche skill.

Learning Outcomes

- Mac and iOS Fundamentals: How to analyze and parse the Hierarchical File System (HFS+) and Apple File System (APFS) by hand and recognize the specific domains of the logical file system and Mac-specific file types.
- User Activity: How to understand and profile users through their data files and preference configurations.
- Advanced Intrusion Analysis and Correlation: How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
- Apple Technologies: How to understand and analyze many Mac and iOS-specific technologies, including Time Machine, Spotlight, iCloud, Document Versions, FileVault, Continuity, and FaceTime.

Course Outline

Topic 1: Mac and iOS Essentials

This topic introduces the student to Mac and iOS essentials such as acquisition, timestamps, logical file system, and disk structure.

Apple Essentials

- Mac and iOS Systems
- Mac Analysis in a Windows World
- Apple Fundamentals

Mac Essentials and Acquisition

- Mac File System Domains
- Mac Directory Structures
- Containers and Sandboxes
- Acquisition Pitfalls and Considerations
- Hard Drive, Network, and Memory Acquisition Tools
- Image Mounting Using Open-Source Utilities

iOS Essentials and Acquisition

- Differences between iOS and macOS
- Security and Encryption
- Jailbreaks
- Acquisition Types and Differences
- Local and iCloud Backups
- Tools for Acquisition and Analysis
- Passcode Bypass and Cracking

Disks and Partitions
- Disk Layout
- Partition Schemes
- GPT
- FileVault
- Disk Images
- CoreStorage
- APFS Containers
- Bootcamp
- Fusion Drives

Topic 2: File Systems & System Triage

In this topic, students will learn the basic principles of the primary file system implemented on MacOS systems. Students will then use that information to look at a variety of great artifacts that use the file system and that are different from other operating systems students have seen in the past. Rounding out the day, students will review Mac and iOS triage data.

File Systems
- Overview of HFS+ & APFS
- Data Structures
- Manual Parsing
- APFS Clones
- APFS Snapshots
- APFS Benefits and Caveats
- Tool Output and Caveats

Extended Attributes
- Contents
- Analysis
- Tool Support
- Interesting Attributes

File System Events Store Database
- Usage
- Parsing with Tools
- Practical Analysis

Spotlight
- Analysis Methods and Tools
- Practical Queries
- Portable Artifacts
- Artifacts Left Behind by Macs
- Differences from Various File Systems

Mac and iOS Triage
- OS Version
- Device Identifying Data
- System Installation
- Network Settings
- Time Zone and Location Services
- User Accounts
- Managed Devices
- Mail and Internet Account Settings

Most Recently Used (MRUs)
- Recent iOS Apps
- Recent Folders
- Recent Applications
- Recent Documents
- Recent Servers
- Recent Files
- Parsing Methods and Tools
- Alias and Bookmark BLOBs
- NSKeyed Archiver Plist File Manual Parsing

Topic 3: User Data, Configuration, and Log Analysis

This topic contains a wide array of information that can be used to profile and understand how individuals use their computers. The topic also details basic system information, GUI preferences, and system application data. A basic analysis of system logs can provide a good understanding of how a system was used or abused.

User Data and System Configuration
- Bash History
- Keychains
- Printing
- Firewall Settings
- Sharing Settings
- Bluetooth
- Autoruns
- Application Bundles
- Software Updates
- GUI Settings

Log Parsing and Analysis
- Log Basics
- Log Formats
- Log Recovery
- Log Types (Unix, BSM Audit, Apple System Logs (ASL) and Unified)
- Log Configuration
- Analysis Methods and Parsing Tools

Timeline Analysis and Data Correlation
- Temporal Context and Timestamps
- Volume Analysis
- Temporal Changes
- System Information and State
- Network Analysis
- User Access
- Privilege Escalation
- Account Creation/Deletion
- Software Installation
- Backup Activity
- Locational Data

Topic 4: Application data Analysis

This topic will explore the various databases and other files where data are being stored.

Application Permissions
- Privacy Settings
- Location Services

Native Application Fundamentals
- Locations
- Snapshots

Safari Browser
- History
- Cache
- Syncing
- Private Mode
- Data Retention

Apple Mail
- Locations and Data Access
- Mail Accounts and Configuration
- Attachments
- Metadata

Communication
- iChat/Messages
- FaceTime
- SMS
- iMessage
- Call History
- Voicemail

Calendar and Reminders
- Files
- Database Analysis

Contacts
- Files
- Database Analysis

Notes
- Files
- Database Analysis
- Version Differences
- Media Analysis

Apple Pay, Wallet, Passes
- Files
- Database Analysis

Photos
- Files
- Database Analysis
- iCloud Syncing

Maps
- Files
- Database Analysis
- Caveats

Location Data
- Routine, WiFi, Cellular Locations
- Files
- Database Analysis
- Tools and Parsing

Apple Watch
- Files
- Capabilities
- Synced Data

Third-Party Apps
- Locations
- Analysis Caveats
- Data Structure
- Analysis Tools

Topic 5: Advanced Analysis

Time Machine
- Backup Settings
- Backup Volumes
- Snapshot Analysis
- Local Snapshots
- Encrypted Backups
- Mounting and Analysis

Document Versions
- Versions Metadata
- Versions Database
- Generations
- Chunk Storage

iCloud
- Synced Accounts
- Mobile Documents
- Synced Preferences

Malware and Intrusion Analysis
- Intrusion Analysis
- Java Cache and IDX Files
- File Quarantine
- XProtect
- Gatekeeper

Live Response
- Live Triage Techniques
- Volatile Data Collection

Memory Acquisitions and Analysis
- Acquisition Tools
- Analysis Tools

Password Cracking and Encrypted Containers
- Password Shadow Files
- Cracking Software
- Keychains
- FileVault
- Encrypted Volumes and Disk Images

Topic 6: Mac Forensics & Incident Response

- In-Depth File System Examination
- File System Timeline Analysis
- Advanced Computer Forensics Methodology
- Mac Memory Analysis
- File System Data Analysis
- Metadata Analysis
- Recovering Key Mac Files
- Volume and Disk Image Analysis
- Advanced Log Analysis and Correlation
- iDevice Analysis and iOS Artifacts

Prerequisites

- In-Depth File System Examination
- File System Timeline Analysis
- Advanced Computer Forensics Methodology
- Mac Memory Analysis
- File System Data Analysis

2 Days at $250

- Metadata Analysis
- Recovering Key Mac Files
- Volume and Disk Image Analysis

Target Audience

- In-Depth File System Examination
- File System Timeline Analysis
- Advanced Computer Forensics Methodology
- Mac Memory Analysis
- File System Data Analysis
- Metadata Analysis
- Recovering Key Mac Files
- Volume and Disk Image Analysis
- Analysis of Mac Technologies including Time Machine, Spotlight, and FileVault
- Advanced Log Analysis and Correlation
- iDevice Analysis and iOS Artifacts