FOR518: Mac and iOS Forensic Analysis and Incident Response™

GIME
iOS and macOS Examiner
giac.org/gime

6	36	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Understand the nuances between macOS and iOS devices
- Dive into how the Apple magic works between devices, and how that can help investigations
- Determine the importance of each file system domain and how data is organized
- Conduct temporal analysis of a system by correlating data files and log analysis
- Profile how individuals used the system, including how often they used the system, what applications they frequented, and their personal system preferences
- Identify remote or local data backups, disk images, or other attached devices
- Find encrypted containers and FileVault volumes, understand keychain data, and crack Mac passwords
- Analyze and understand macOS metadata and their importance in the Spotlight database, Time Machine, and Extended Attributes
- Develop a thorough knowledge of the Safari Web Browser, Apple Mail and many more applications by looking that their internal databases
- Identify communication with other users and systems though Messages, FaceTime, SSH remote login, Screen Sharing, and AirDrop
- Conduct an intrusion analysis of an Apple devices for signs of compromise or malware
- Understand the APFS file system and its significance with a bonus Lab to parse the APFS file system by hand, using only a reference sheet and a hex editor
- Understand how the Apple Ecosystem of devices work and interact with each other—from AirTags, to VisionPro, to the Apple Watch, to HomeKit—all these Apple technologies will have artifacts on macOS and iOS devices

Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

This consistently updated FOR518 course provides the techniques and skills necessary to take on any Mac or iOS case without hesitation. The intense hands-on forensic analysis and incident response skills taught in the course will enable analysts to broaden their capabilities and gain the confidence and knowledge to comfortably analyze any Mac or iOS device. In addition to traditional investigations, the course presents intrusion and incident response scenarios to help analysts learn ways to identify and hunt down attackers that have compromised Apple devices.

What Is macOS and iOS Forensics Analysis?

MacOS and iOS Forensic Analysis is the recovery, analysis, and interpretation of data stored on Apple devices.

Business Takeaways

- Empower employees to investigate various crimes such as computer misuse, malicious device intrusions, corporate espionage, insider threats, and fraud
- Learn how various Apple data is stored and how to analyze using tool agnostic methods without the requirement for expensive commercial forensic tools
- Identify different forensic artifacts and nuances between the Apple platforms (macOS and iOS)
- Understand the wealth of user related information that can show how a device was used or abused
- Learn the differences of performing forensics and security assessments when Apple devices are involved versus other industry-standard operating systems

Hands-On macOS and iOS Forensics Training

The hands-on portion of FOR518 is unique and especially suited to those who love to dig into the data. The labs were created to show how Apple data is stored and how to interpret it without the need for an expensive commercial utility. These labs will allow a student to get a hands-on perspective of the data that is shown in the class presentations and apply the concepts to the course dataset. The labs in this course are a major component of the learning experience and enables the student to increase their success in applying various analysis course topics after they leave the classroom.

"It was very interesting to learn that certain 'forensic' tools could report data as being encrypted even though one could still get other data."

—Gary Titus, **Stroz Friedberg LLC**

"Within the first two days or training, I had enough knowledge to go back to work and solve two outstanding issues."

—Beau G., **Information Systems Solutions**

Section Descriptions

SECTION 1: Mac and iOS Essentials

This section introduces the student to Mac and iOS essentials such as acquisition, timestamps, logical file system, and disk structure. Acquisition fundamentals are the same with Mac and iOS devices, but there are a few tips and tricks that can be used to successfully and easily collect Mac and iOS systems for analysis. Students comfortable with Windows forensic analysis can easily learn the slight differences on a Mac system—the data are the same, only the format differs.

TOPICS: Apple Essentials and Device Security; Disks and Volumes; macOS Acquisition Tools and Methods; iOS Acquisition Tools and Methods; Data Organization, Triage, and iCloud; Forensic Testing

SECTION 2: Log Analysis, User Data, and System Configuration

Mac and iOS devices contain many system settings that can show how a device was used (or abused). A user of the device may change a specific configuration that can provide useful forensic insight. Often these configuration actions can be also found in the logs and provide historical context to create a detailed story of how the device was used. This section focuses on system and data configurations alongside log analysis. These devices have many different types of logs each with their own method for analysis and content. The log entries can be correlated with user and system data found on the system to create an in-depth timeline that can be used to solve cases quickly and efficiently.

TOPICS: Parsing System Logs; User Account; User Interface; Volumes; Printing; System State; Network; Bluetooth

SECTION 3: File Systems and Related Artifacts

After a review of how APFS works, students will look at a variety of fascinating artifacts that are used by the file system and that are quite different from other operating systems students have seen in the past. This includes many artifacts that contain metadata and can provide more context into investigations. In an additional bonus lab students will learn the building blocks of Mac and iOS forensics with a thorough deep-dive understanding of the Apple File system (APFS). Utilizing a hex editor, students will learn the basic structures of the primary file system implemented on MacOS and iOS systems.

TOPICS: Volume File System Artifacts; Extended Attributes; Spotlight; Document Versions; File System Events Store Database

SECTION 4: Application Data Analysis

In addition to all the configuration and preference information found in the User Domain, the user can interact with a variety of native Apple applications, including the Internet, email, communication, photos, locational data, and others. These data can provide analysts with the who, what, where, why, and how for any investigation. This section will explore the various databases and other files where data are being stored. The student will be able to parse this information by hand without the help of a commercial tool parser.

TOPICS: Application Fundamentals; Safari Browser; Wallet; Mail; Communication; Notes; Photos; Maps

SECTION 5: Advanced Analysis Topics

Apple systems implement some technologies that are available only to those with Mac and iOS devices. In this section, students will learn about a variety of topics that can be used in a variety of investigations. Topics such as pattern of life will detail very specific user and device activities which can determine which app was being used at precise time, how many steps did they walk, was the device unlocked, or where the device was. Other advanced topics include cracking into data hidden in encrypted containers, indicators of compromise, security enhancements, and all other Apple "things" including FindMy, AirTags, TimeMachine and more!

TOPICS: Pattern of Life; Password Cracking; Malware and Live Response; One More Thing

SECTION 6: Mac Forensics and Incident Response Challenge

In this final course section, students will put their new All-Things-Apple forensic skills to the test by running through a real-life scenario.

TOPICS: In-Depth File System Examination; File System Timeline Analysis; Advanced Computer Forensics Methodology; File System Data Analysis; Metadata Analysis; Recovering Key Mac Files; Database Analysis; Volume and Disk Image Analysis; Analysis of Apple-specific Technologies; Advanced Log Analysis and Correlation

"With so much focus on Windows forensics, the Mac class is really necessary."

—Paul Sieberth, **Tulane University**

Who Should Attend

- Experienced digital forensic analysts who want to solidify and expand their understanding of file system forensics and advanced Mac analysis
- Law enforcement officers, federal agents, and detectives who want to master advanced computer forensics and expand their investigative skill set
- Media exploitation analysts who need to know where to find the critical data they need from a Mac system
- Incident response team members who are responding to complex security incidents and/or intrusions from sophisticated adversaries and need to know what to do when examining a compromised system
- Information security professionals who want to become knowledgeable with Mac OS X and iOS system internals
- SANS FOR500, FOR508, FOR585, and SEC575 alumni looking to round out their forensic skills

Who Should Attend

- Cyber Defense Incident Responder (OPM 531)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

GIME
iOS and macOS Examiner
giac.org/gime

GIAC Cloud Forensics Responder

The GIME certification validates a practitioner's knowledge of Mac and iOS computer forensic analysis and incident response skills. GIME-certified professionals are well-versed in traditional investigations as well as intrusion analysis scenarios for compromised Apple devices.

- Mac and iOS File Systems, System Triage, User and Application Data Analysis
- Mac and iOS Incident Response, Malware, and Intrusion Analysis
- Mac and iOS Memory Forensics and Timeline Analysis