FOR518: Mac and iOS Forensic Analysis and Incident Response

GIME
iOS and macOS Examiner
giac.org/gime

6	36	Laptop
Day Program	CPEs	Required

IMPORTANT NOTE: MAC HARDWARE REQUIRED

You Will Be Able To

- Parse the HFS+ file system by hand, using only a cheat sheet and a hex editor
- Determine the importance of each file system domain
- Conduct temporal analysis of a system by correlating data files and log analysis
- Profile individuals' usage of the system, including how often they used it, what applications they frequented, and their personal system preferences
- Determine 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 Mac metadata and their importance in the Spotlight database, Time Machine, and Extended Attributes
- Develop a thorough knowledge of the Safari Web Browser and Apple Mail applications
- Identify communication with other users and systems through iChat, Messages, FaceTime, Remote Login, Screen Sharing, and AirDrop
- Conduct an intrusion analysis of a Mac for signs of compromise or malware infection
- Acquire and analyze memory from Mac systems
- Acquire iOS and analyze devices in-depth

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

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.

The constantly updated FOR518: Mac and iOS Forensic Analysis and Incident Response 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.

FORENSICATE DIFFERENTLY!

FOR518: Mac and iOS Forensic Analysis and Incident Response will teach you:

- 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 and Device Activity: How to understand, profile, and conduct advanced pattern-of-life on users and they devices 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.

FOR518: Mac and iOS Forensic Analysis and Incident Response aims to train a well-rounded investigator by diving deep into forensic and intrusion analysis of Mac and iOS. The course focuses on topics such as the HFS+ and APFS file systems, Mac-specific data files, tracking of user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac-exclusive technologies. A computer forensic analyst who completes this course will have the skills needed to take on a Mac or iOS forensics case.

> **"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; Mac Essentials and Acquisition; iOS Essentials and Acquisition; Disks and Partitions

SECTION 2: File Systems and System Triage

The building blocks of Mac and iOS forensics start with a thorough understanding of the HFS+. Utilizing a hex editor, 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.

TOPICS: File Systems; Extended Attributes; File System Events Store Database; Spotlight; Mac and iOS Triage; Most Recently Used

SECTION 3: User Data, System Configuration, and Log Analysis

This section contains a wide array of information that can be used to profile and understand how individuals use their computers. The logical Mac file system is made up of four domains: User, Local, System, and Network. The User Domain contains most of the user-related items of forensic interest. This domain consists of user preferences and configurations. The Local and System Domains contain system-specific information such as application installation, system settings and preferences, and system logs. This section 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. The Network domain is more ethereal and we can find this in many places throughout the course as well as in the logs. Timeline analysis tells the story of how the system was used. Each entry in a log file has a specific meaning and may be able to tell how the user interacted with the computer. The log entries can be correlated with other data found on the system to create an in-depth timeline that can be used to solve cases quickly and efficiently. Analysis tools and techniques will be used to correlate the data and help the student put the story back together in a coherent and meaningful way.

TOPICS: User Data and System Configuration; Log Parsing and Analysis; Timeline Analysis and Data Correlation

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, etc. 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 Permissions; Native Application Fundamentals; Safari Browser; Apple Mail; Communication; Calendar and Reminders; Contacts; Notes; Apple Pay, Wallet, Passes; Photos; Maps; Location Data; Apple Watch; Third-Party Apps

SECTION 5: Advanced Analysis Topics

Mac systems implement some technologies that are available only to those with Mac and iOS devices. These include data backup with Time Machine, Document Versions, and iCloud; and disk encryption with FileVault. Other advanced topics include data hidden in encrypted containers, live response, Mac intrusion and malware analysis, and Mac memory analysis.

TOPICS: Time Machine; Document Versions; iCloud; Malware and Intrusion Analysis; Live Response; Memory Acquisitions and Analysis; Password Cracking and Encrypted Containers

SECTION 6: Mac Forensics and Incident Response Challenge

In this final course section, students will put their new Mac forensic skills to the test by running through a real-life scenario with team members.

TOPICS: 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

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, FOR526, FOR585, and FOR610 alumni looking to round out their forensic skills

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

— Paul Sieberth, **Tulane University**

"Best Mac class anywhere."

— Eric Koebelen,
Incident Response US