Macintosh Forensic Survival Course

Duration: 5 days/Level

Date: On demand

Venue: On demand

Language: English

Seat availability: On demand (recommended no more than 12)

Learning Objectives:

Macintosh Forensic Survival Course covers the process of examining a Macintosh computer from the first to the last step in logical order. Surprising to most is that the entire course is taught using a Mac to examine a Mac without the use of expensive automated forensic tools. Even more surprising is that the participants realize the they can find more evidence and find it faster!

This course is for:

The course is designed for both the beginner Mac examiner as well as the advanced.

Level 1

How and why you are missing evidence using Windows-based tools?

How to use a Mac to process a Mac?

No.	Topic	Description
1	**Non-Intel Mac Issues (PowerPC and Classic OS)**	An examiner many encounter antiquated Mac technology. It is important to know how to identify this technology and how to handle it. Additionally, a review of the Classic OS helps to understand modern life and operating system artifacts and features.
2	**Overview of Mac OS X Versions**	Identifies features of forensic importance in different Mac OS and when they appeared.
3	**Understanding the Mac File System**	A review of file system supported by Mac OS.
4	**Intel Mac Technology and Bootcamp**	Explains the forensic significance of Mac Intel technology.
5	**Mac Security Issues and FileVault Attacks**	Current best practices for dealing with Mac security.
6	**Macintosh Search and Seizure**	Best practices for seizing Mac and iOS hardware.
7	**Safely Obtaining System Information**	How to safely obtain system information without making changes to the evidence.
8	**Bypassing Open Firmware Passwords**	Explains OFP, how to remove OFP and if it is necessary.
9	**Volatile Data Collection**	How to build Trusted Utilities Disk and using it to collect volatile information.
10	**Manual and Automated Imaging and Acquisition**	Using the Mac to safely image media both manually and with PALANDIN.
11	**Imaging Mac RAM**	Exercises in imaging Mac RAM and recovering passwords.
12	**Verifying and Safely Mounting Forensic Images**	Safely mounting forensic images for processing.
13	**Indexing Forensic Images**	How to index forensic images using Mac OS.
14	**Search Techniques Using Mac OS X**	Creating custom search expressions from the command-line and GUI.
15	**Locating Evidence (Email, Graphics, Internet Artifacts, Documents, System Artifacts, Instant Messaging, logs and more)**	Identifying Mac artifacts in the file system.
16	**Recovering Deleted Files**	An exercise in manually recovering deleted files and the dangers of Mac optimization.
17	**Examining SQLite Databases and PLIST Files**	Examining the heart of Mac data storage.
18	**Using OS X for Forensics**	How to utilize built-in Mac OS technology for forensics.

No.	Topic	Description
19	**Report Development**	How to create native reports using the Mac to properly view data.
20	**Examining iOS Devices Artifacts**	Identifying and examining iOS artifacts found on a Mac.
21	**Working with NTFS**	Integrating Mac forensics in a Windows centric forensic lab.
22	**Review of Recommended Applications**	Our recommendations for commercial and non-commercial tools to assist with Max forensics.
23	**Review of Automated Forensic Tools**	Our review of current automated Mac forensic tools.
24	**Recommended Macintosh Hardware Requirements for Forensics**	Recommendations of hardware for Mac forensics.

Level 2

The forensic use of and analysis of Apple hardware, technology and applications.

No.	Topic	Description
1	**Advanced File System Analysis**	Students will be introduced to the concept of domains within the Mac OS X environment and be able to locate evidentiary artifacts in each. Additionally, students will learn how to manually deconstruct any installed applications.
2	**Advanced Command Line**	Underneath Mac OS X's interface and desktop is the Unix shell, including a Terminal that gives users endless power and control from the "command-line." Participants will learn advances tips using the "command line" to assist in forensic examinations of a Mac.
3	**AppleScript and Automator**	Included with Mac OS X are two native applications that allow the user to develop custom programs and workflows to automate almost any task. Participants will learn how to create their own AppleScript and Automator applications to simplify and enhance their forensic examinations.
4	**Identifying and Using Virtual Machines**	Participants will learn how to identify the use of a VM within Mac OS X, and the procedures necessary to analyze them. In addition, the participant will learn how to use a VM to assist in forensic examinations from within the Mac environment.
5	**Mac OS X Server Forensics**	Participants will learn about Mac OS X server technology, including services and user accounts. Instruction will be provided on best practice for acquiring data safely from live systems, as well as responding to an incident on compromised systems.
6	**Macintosh Timeline Analysis**	Building a timeline of a file system can retrace the suspects' history minute by minute or second by second. The course helps the participants understand Mac timestamps and use them for analysis.
7	**iCloud Forensics**	Participants will learn how to find and analyze documents and other data synced with an Apple iCloud account.
8	**Unique Apple Techniques**	Participants will be provided with best practices and resources to deal with troublesome and unique Apple technology.

No.	Topic	Description
9	**Advanced Search Techniques**	The course shows the participants how to conduct advanced indexed and live searches to find any data.
10	**Application Deconstruction**	Participants will learn how to find any or all artifacts left behind by any application.