California Department of Justice

Advanced Computer Forensics-Macintosh

Advanced Training Center, Cyber Classroom
4949 Broadway, Rm.C107, Sacramento, CA 95820
May 20-24, 2024

Course Description:
This 40 hour class is designed to provide unparalleled vendor neutral and tool agnostic instruction in advanced topics relating to the forensic use and analysis of Apple hardware, technologies and applications. The training is de-signed for the participant to learn in a team work environment, and is taught by Sumuri instructors who maintain a “no one left behind” attitude. In addition, complicated topics are made easy to understand through instructor led exercises and real-life scenarios—supported by a quality student manual to be utilized as a supplemental resource at the completion of the course. Students will be introduced to the concept of domains within the macOS environment and be able to locate evidentiary artifacts in each. Additionally, students will learn how to manually deconstruct any installed application.

Who Should Attend –Law enforcement personnel assigned to a cybercrime unit/task force, and responsible for investigating Apple digital device cases.

Pre-requisites – Students must have completed the Advanced Training Center’s Computer Forensics-Maintosh (D425), and should be currently working on doing forensics

Course Objectives: - The objective of this course is to build upon the lessons taught in Sumuri’s Best Practices in Mac Forensics. Advanced Practices in Mac Forensics provides new skills and goes deeper into understanding the Apple file system and artifacts, capturing the footprint of any application running on a Mac to discover evidence, advanced search techniques, automating forensic tasks, log analysis, proper use of Apple timestamps in forensic analysis and more.

Course Outline

- Advanced File System Analysis
- Advanced Command Line
- Apple Script and Automater
- MacOS Log Analysis
- File System Event Monitoring and Analysis
- Indentifying and Using Virtual Machines
- Macinotosh Timeline Analysis
- iCloud Forensics
- Time Machine Analysis
- Unique Apple Technology
- Advanced Search Techniques
- Application Deconstruction

STUDENTS NEED TO BRING THEIR OWN MAC LAPTOP TO TRAINING. The Laptop must include the current version of macOS 14 Sonoma installed and the User Account must have administrator privileges.

Cost: This is a tuition free course for Law Enforcement.

Additional Information - For further information contact Tricia Nelson,-Program Manager at (916) 210-4442, or tricia.nelson@doj.ca.gov