

# NW3C

National White Collar Crime Center

To register, visit our training site at:

[www.nw3c.org](http://www.nw3c.org)

Questions? Call 877-628-7674

Cybercop

Classroom course

4 days

Prerequisites:

CI 106, CC 201

**CC 325**  
**MFA**

## Macintosh Forensic Analysis

Version 3.0, updated November 2017

This course provides the fundamental knowledge and skills necessary to identify and collect volatile data, acquire forensically-sound images of Apple Macintosh computers, and perform forensic analysis of macOS operating system and application artifacts. Students gain hands-on experience scripting and using automated tools to conduct a simulated live triage. Students will use multiple methods to acquire forensically-sound images of Apple Macintosh computers and identify unique challenges that this task may present. Students will also learn how the macOS's default file system stores data, what happens when files are sent to the macOS Trash, where operating system and application artifacts are stored, and how they can be analyzed. The forensic artifacts covered include password recovery, recently-opened files and applications, encryption handling, Mail, Safari, Messages, FaceTime, Photos, Chrome, and Firefox.

- **Performing live triage.**  
Preserving data from systems in different states. Commands for collecting non-persistent data. Introduction to shell scripting.
- **Macintosh imaging.**  
Manual and automated imaging methods. Identify imaging challenges.
- **Processing basics.**  
Mounting images, viewing hidden files, and the standard OS X directory structure.
- **Partitioning schemes.**  
Apple Partition Map, GUID Partition Table, Master Boot Record.
- **HFS+.**  
Structure of an HFS+ formatted storage volume and how files and directories are tracked and saved.
- **Operating system artifacts.**  
Trash, login passwords, keychains, system logs, OS X related property lists, and FileVault.
- **Application artifacts.**  
Mail, Contacts, Safari, Calendar, Reminders, Notes, Messages, FaceTime, Photos, Chrome, FireFox, and Skype.

**Huntsville, AL**  
**May 15–18, 2018**

**Click here**  
**to register**

262813637 Copyright rzoze19, 2015 Used under license from Shutterstock.com"



This project was supported by Grant No. 2015-BE-BX-0011 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

©2016, 2017. NW3C, Inc. d/b/a the National White Collar Crime Center. All rights reserved.