Course Description

DF320 ADFA-Mac	Advanced Digital Forensic Analysis: macOS
Digital Forensics	This course teaches students 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, and use multiple methods to acquire forensically-sound images of Apple Macintosh computers. Topics include how the macOS 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. Forensic artifacts covered include password recovery, recently-opened files and applications, encryption handling, Mail, Safari, Messages, FaceTime, Photos, Chrome, and Firefox.
Classroom course	
4 days	
Prerequisite: None	

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; 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; how files and directories are tracked and saved.

Artifacts. Operating system and application artifacts.

To register, visit our training site at:

www.nw3c.org

Questions? Call 877-628-7674

Version 4.0.1, updated January 2019

"This project was supported by Grant No. 2018-MU-BX-K001 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."