

INSIDE THE CORE:

The Macintosh and Apple Device Forensics Podcast

Show Notes

Episode 1

Introductions:

Host Intros:

Dave: Federal Law Enforcement Special Agent, Computer Forensics Instructor (College/Private), 9 Years of Forensic experience

Ryan: State L.E. Investigator, Mac Forensics Instructor, Owner of macosxforensics.com, co-author of [Mac OS X, IPOD, and iPhone Forensic Analysis DVD Toolkit](#)

Chris: Municipal L.E. Forensic Specialist, Computer Forensics Instructor (College/Private), 5 years of forensic experience

Single User Mode:

GOLDEN RULE: Use **OPTION** key to boot first and confirm no Firmware Password

-If Firmware Password in use, power off.

(Firmware Password Options will be covered in a later podcast)



-Single User Mode can be used to find Date/Time of the system without making changes

-After OPTION key boot and confirmation of no firmware password

-REBOOT holding OPTION + 'S' Key to boot into Single User Mode

-Will be similar to a Verbose boot

-After boot stops, type "Date" at cursor and date and time will be displayed.

-Can also run System Profiler to access information about the system

INSIDE THE CORE:

The Macintosh and Apple Device Forensics Podcast Training:

Forward Discovery:

- Non-Tool Specific Mac Forensics Survival Course
- Teaches how to do Mac Forensics using Mac
- Basic and Advanced Courses being offered Internationally



BlackBag Technologies:

- Offers both training for non-tool and Blackbag Tool Training
- Suite of Proprietary tools for using a Mac to do Mac Forensics
- Beginner, Intermediate, and Advanced Courses



SubRosaSoft:

- Also offers tool specific training
- MacForensicsLab:Proprietary software



Purdue University: (Law Enforcement Only):



- 3 day class
- Traveling Class and at the University
- Beginning and Advanced Course

Apple:



- Several certifications:
 - Apple Certified Support Professional (ACSP)
 - Apple Certified Technical Coordinator (ACTC)
 - Apple Certified System Administrator (ACSA)
 - Range of Apple Software Pro Certifications as well

INSIDE THE CORE:

The Macintosh and Apple Device Forensics Podcast

PList of the Week(PLOW):



This week's PLOW is: **com.apple.ipod.plist**

1. It is located in both Global and User: Library --> Preferences
2. Contains information about all iPod/iPhone devices connected to system.
3. Includes (not comprehensive):
 - a. UUID: Unique ID for the Device
 - b. Connected: Last Connected Date/Time
 - c. Device Class: iPod/iPhone
 - d. Firmware Version
 - e. Serial Number
 - f. IMEI (iPhone)
 - g. Use Count