

# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

Show Notes Episode 2

### Show Hosts:

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](http://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

### Open Firmware Password:



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

OFP: Prevents any other startup option other than "option" or "startup disk"  
If OFP and you attempt alternative boot sequence, the system will default to the normal "Startup Disk" and possible writes will be made.  
-Dont want to make writes....

1. Boot with option key to confirm Open Firmware Password exist
2. To get around:
  - A. Pull hard drive and image via write block (24 screws or less)
  - B. Reconfigure the ram:
    - 1) Shut down
    - 2) Disconnect power (if laptop remove battery)
    - 3) Remove stick or add stick of ram to reconfigure
    - 4) Close up, connect battery/power
    - 5) Command+Option+P+R key all at once "Vulcan Death Grip"



# INSIDE THE CORE: The Macintosh and Apple Device Forensics Podcast

- 6) Listen for 3 Chimes-Indicates reset
- 7) Restart and use Option key to check

NOTE: Time will be reset. The clock will possibly be off.  
Logs may be important.



## Mobile Forensics World Conference:

<http://www.mobileforensicsworld.com/>

Idea of Purdue University's [Rick Mislán](#)

iPhone Panel:

- [Ryan Kubasiak](#): Macosxforensics.com
- [Jonathan Zdziarski](#) : iPhone Forensics author
- [Sean Morrissey](#) :Dept. of Defense
- [Andrew Hoag](#) : Moderator
- Took questions from audience after moderated question session.



Different ways to get data:

Hardware/Software Suites:

[Wolf](#): Good for unlocked phone, and if you unlock can use.



[Cellebrite](#):



Different Methods:

Raw Disk info John Z and Sean Morrissey

- Concerns as to what is being changed from data standpoint

Dont forget about the Macintosh for completing Forensic exam including reviewing the backups a wealth of informaiton

It is essential that you not just follow instructions or programs and that you must test and educate yourself.

# INSIDE THE CORE: The Macintosh and Apple Device Forensics Podcast

Plist: Manual rip of Plists from iPhone and analysis with Plist Editor on the Mac

Locked Phone Experiences:

- Not excessive amounts
- Dave has had a couple typically unlocked iPhones
- Usually it has been a phone Jailbroken and being used on a different network
- Due to this frequently, firmware not being updates

## PList(s) of the Week(PLOW):

Plist-Registry files like but corruption of one file doesnt corrupt the entire system.

3rd party plist:

Quicktime:

Global: Library--> Preferences--> **com.apple.quicktime.plist**

- Shows Registered User and Registered Key
- Can indicate the key for verification of legal software



QuickTime

iWork (Mac Office Suite):

Global-->Library-->Preferences-->

iWork08: **com.apple.iwork08.plist**

- User License
- user Name
- Registration information



iWork09: **com.apple.iwork09.plist**

- Registration
- Quantity of times reference registrations

Google Gears:

Global--Library-->Preferences--> **com.google.gears.plist**

- indicates if gears installed
- Stats for gears enabled

User-->Library-->Preferences--> **com.google.gmailnotifier.plist**

- Indicates:
  - gmail address
  - application launched



# INSIDE THE CORE: The Macintosh and Apple Device Forensics Podcast

## MAC RESOURCES:

### Mac Shadows:

- Mac Commands for OS Terminal Lines A-Z
- Security information



### MacEnstein:

- Once a month popular site
- Lots of great information and articles
- Interviewed Ryan about Macosxforensics.com



### Twitter:

- Good new Social Media for sharing info
- Remember its public info
- Follow Inside the Core at: [www.twitter.com/insidethecore](http://www.twitter.com/insidethecore)



THANKS AND LOOK FORWARD TO EPISODE 3 TO DROP SOON

Visit us at [www.insidethecore.com](http://www.insidethecore.com) or [insidethecore.libsyn.com](http://insidethecore.libsyn.com)

Questions, Comments, or Suggestions: [coreforensics@gmail.com](mailto:coreforensics@gmail.com)

For more introduction music, see the creator  
<http://www.bradsucks.net/> :

at

