

# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

Episode 3 Shownotes

### 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

Reggie Chapman: LE State Police, Computer Forensics Instructor

### Welcome News:

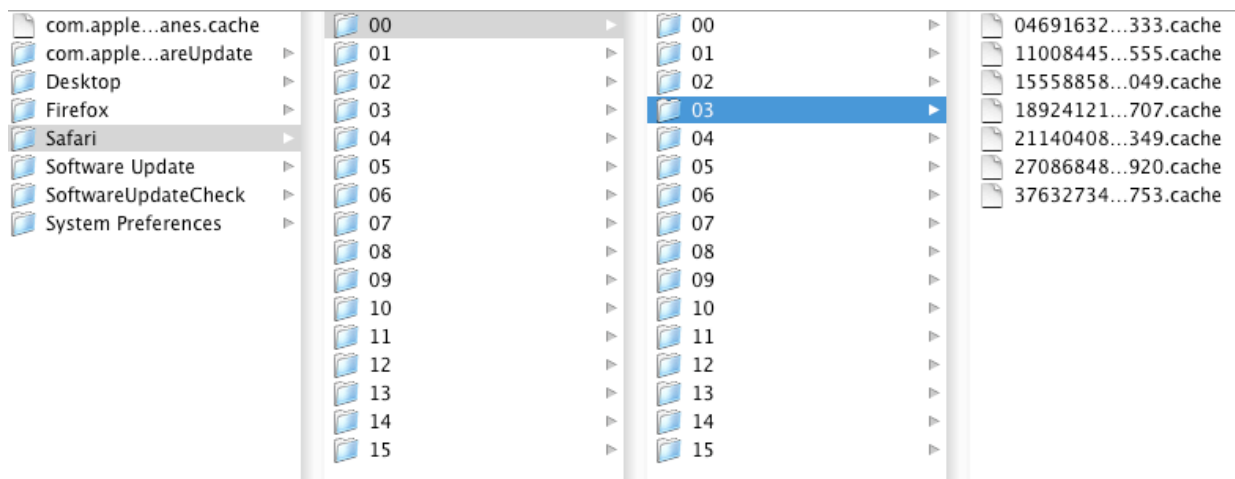
Pre Released: 3 People in Line

Help Wanted: Are you a rock-ette? Rock-man-in-nuf? Rock-n-roller? Ryan is looking for assistance at his State funded landscaping project in New York. Contact Ryan for details.

### Safari Cache:

Times they are a changing....

Original location: Users/USERNAME/Library/Caches/Safari/  
-Files were given Unique ID and extension of .cache



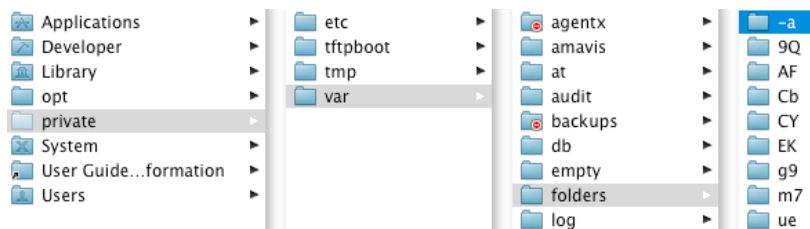
# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

### Episode 3 Shownotes

Version 3: switched to sqlite database file and moved to var/folders

- Location var/folders/(UniqueID)/(UniqueID)/caches/com.apple.Safari
- Cache.db file
- If in Windows environment, ie. Encase, you will not see “var/folders”
  - private/var/folders/(UniqueID)/(UniqueID)/caches/com.apple.Safari is what you will find
  - var/folders view on Mac is called “soft link” as Private is implied



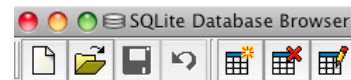
Safari Version 3 Late & Version 4: Back to Users/USERNAME/Library/Caches \com.apple.safari

- The Cache.db file is in that folder

Probable change was security based as it placed the file back in the users folder.

### Viewing Safari Cache:

[SQLite DB Browser 1.3:](#)

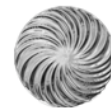


Database: can use sqlite DB browser 1.3 from Sourceforge

- Breaks it in tables
- Example: “Response Table”: has website URL and Date/Time Stamp in GMT

[Filejuicer:](#)

- Drop the Cache.db on Filejuicer and it will parse the data out
- Images, HTML, TXT, etc.



# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

Episode 3 Shownotes

### Incident Response/Trusted Utilities:

- Oftentimes whenever out on scene, it is an unknown environment
- Must consider all machines to be unknown and applications possibly altered
- Best way to prepare is to have our own trusted utilities disk
- Recommend a flash drive, minimum 4 GB to use
- If PowerPC: recommend Firewire, if Intel: recommend USB

### Trusted Utilities Drive:

1. Disk Initialization (formatting for you Microsofties): Use Disk Utility to initialize the drive and wipe it prior to placing tools on it.
2. Put on utilities: i.e. Terminal, System Profiler, etc.
3. Rule of thumb: Command Line Tools/GUI Tools/Evidence Collection.
4. Name the Volume/Disk something you will recognize i.e. "Ryans Trusted Utilities:
  - Eliminate confusion on Suspect's desktop
5. Run Trusted Utilities: Date, Systemprofiler and export information to Evidence Collection.
6. Keep record of the commands run for later review and reporting, i.e. use PDF printout from Mac builtin utilities.
7. Remember to direct your path to the Trusted Utilities Disk as you are never sure what the suspect has done to their machine. Control your environment.

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

#### Address Book:

##### **Users/USERNAME/Library/Preferences/addressbookme.plist:**


- This PList originates information entered at Registration
- Can contain: First Name, Last Name, Local Phone #, Street Address 1 and 2, City, State, Zip, Area Code, Local Phone#, Company, Existing email address


##### **Users/USERNAME/Library/Preferences/com.apple.addressbook.plist:**

- Covers the settings for the address book entries
- Print Dialog Setting

##### **Users/USERNAME/Library/ApplicationSupport/addressbook/metadata:**

- Unique User ID # for each "address book entry"
- File saved as "UUID/ABPerson.abcdp"
- Viewable with Plist Editor or by copying out and dropping in AddressBook

 BAA330F5-5630-4AB3-8D50-DEF684CBAE35/ABPerson.abcdp

 BAA330F5-5630-4AB3-8D50-DEF684CBAE35.jpeg

# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

### Episode 3 Shownotes

#### **Users/USERNAME/Library/ApplicationSupport/AddressBook/images:**

- UUID matches the Metadata UUID
- This is the image that represents the corresponding address book entry



Name BAA330F5-5630-4AB3-8D50-DEF684CBAE35/ABPerson.abcdp  
Kind Address Book Person Data  
Size 4 KB on disk  
Created 6/3/08 9:44 PM  
Modified Today at 6:10 PM  
Last opened Today at 6:10 PM

#### To View in Address Book:

1. Create a clean User account.
2. Copy the suspect com.apple.AddressBook folder and drop into the corresponding location in the new account. Also, copy and drop AddressBookMe.plist
3. Open Address Book and then you can view and print out the entries.



**Dave Melvin**  
Inside the Core

home 555-555-1212

work coreforensics@gmail.com

other maclovin@insidethecore.com

friend MacZorro

work iforensics@gmail.com (AIM)

home 1000 Infinate Loop  
MacLand CA 90000  
United States

INSIDE THE CORE:  
The Macintosh and Apple Device Forensics Podcast  
Episode 3 Shownotes

**Host at Large (HAL) Reggie “Good Stuff” Chapman:**

**Terminal:**

- ”Good Stuff” loves his Terminal
- Darwin: Open Source Unix Core of MacOSX
- Terminal located in /Applications/Utilities
  - Drag and place on your dock for quick access
  
- Change the Terminal to fit your settings, color, size
  - Click on “Terminal --> Preferences” (LEOPARD)
  - ”Settings” box allows to change:
    - Text, Window, Shell, Keyboard, and other Advanced Changes
  - RYAN’s TEMPLATE OF CHOICE: OCEAN is a good setting for Court Presentation



**Websites of the Week**

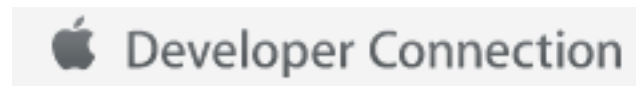
[MACOSXHINTS.com](http://MACOSXHINTS.com):

- Site that has a blog theme
- People post ideas/ways to solve problems
- Has Forum to help research issues and find answers
- Good App and Scripting resource



[Developer.Apple.Com](http://Developer.Apple.Com):

- Has the technical notes for Macs
- Tech Note 1150: HFS File System
- Free Utilities and information



INSIDE THE CORE:  
The Macintosh and Apple Device Forensics Podcast  
Episode 3 Shownotes

THANKS AND LOOK FORWARD TO EPISODE 4 TO DROP SOON

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

On [Twitter @insidethecore](https://twitter.com/insidethecore)



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

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

