

# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

Episode 4 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](#).

**APPLE CERTIFIED TECHNICAL COORDINATOR (ACTC)**

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

Reggie Chapman: LE State Police, Computer Forensics Instructor (*in absentia*)

### Welcome News:

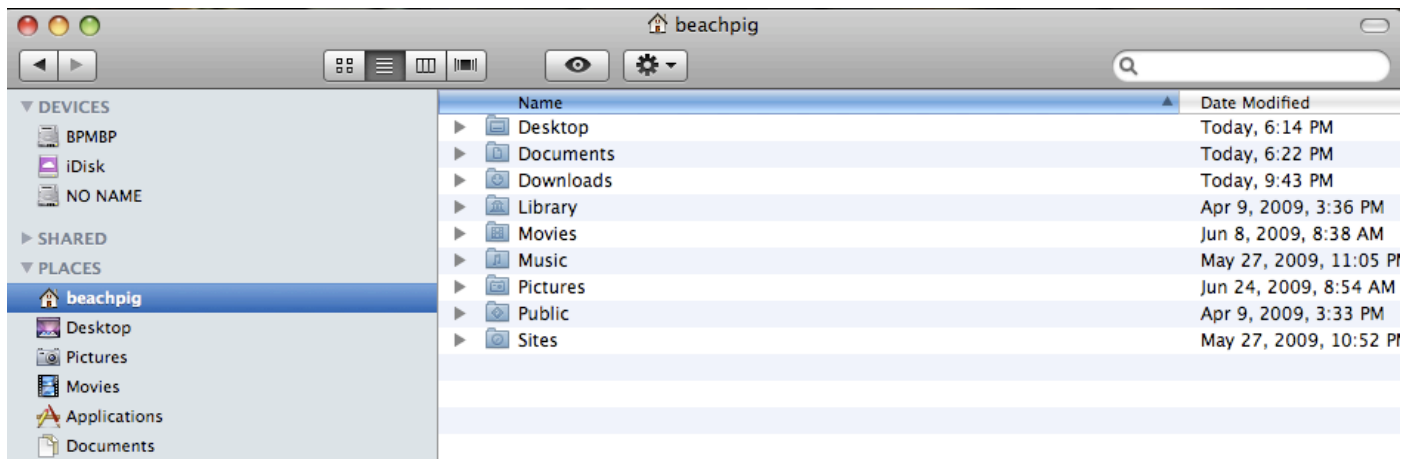
Apple Teaching: 4-5 Converts

[Dr. Schatz](#) : [Write-up](#) on Inside the Core and MacOSXForensics.com

Forensic 4Cast: Annual awards: Take a look and vote.

### Home Folder:

- Most of the evidence is located in the User's Home Folder
- Majority of the Preference PLists with user-specific settings are in User/Library/Preferences
- Check for single or multiple users
- Leopard: Directory Services: Identifies Home Folder to corresponding User
- Tiger: Netinfo.db



# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

Episode 4 Shownotes

Within User Home Folder:

-Nine "Default" OS created folders:

- Desktop
- Documents
- Downloads
- Library
- Movies
- Music
- Pictures
- Public
- Sites

Sample of User or Application created folder in the User Home Folders:

-Frostwire:

- Peer to Peer program
- Related to all the file sharing of that User
- Integral to the examination of a User
- "Incomplete", "Saved", and "Store Purchased" are the new folders with application installation

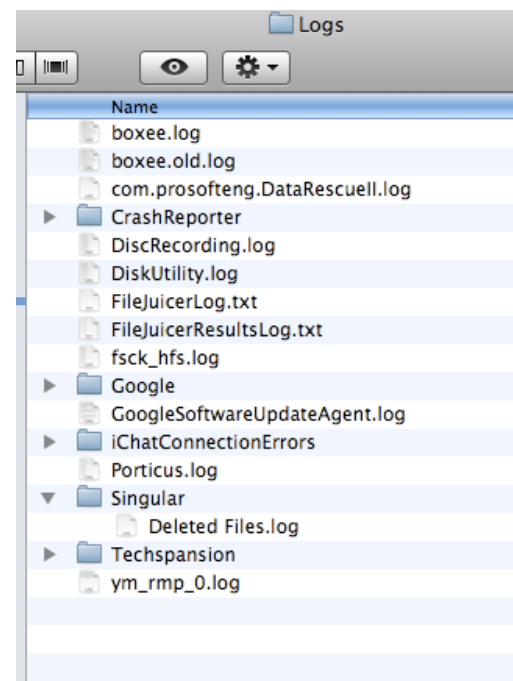
-Limewire:

- Places Shared and Incomplete folder in the User Home Folder
- Shared in the USERS folder is the Shared folder for all Users
- If Shared folder within User Home Folder, that is specific to the User

User Home Folder --> Library Folder (3 sample sub-folders)

-Logs:

- Indicative of the user's activity
- Not system activity, but user specific logs
- Examples of User Logs:
  - AIM log:AOL Instant Messenger activity
  - Crash Reporter:Indicates specific crashes with that User
  - DiskUtility:Keeps track of burns, ISO's, etc.
  - Filejuicer
  - Yahoo

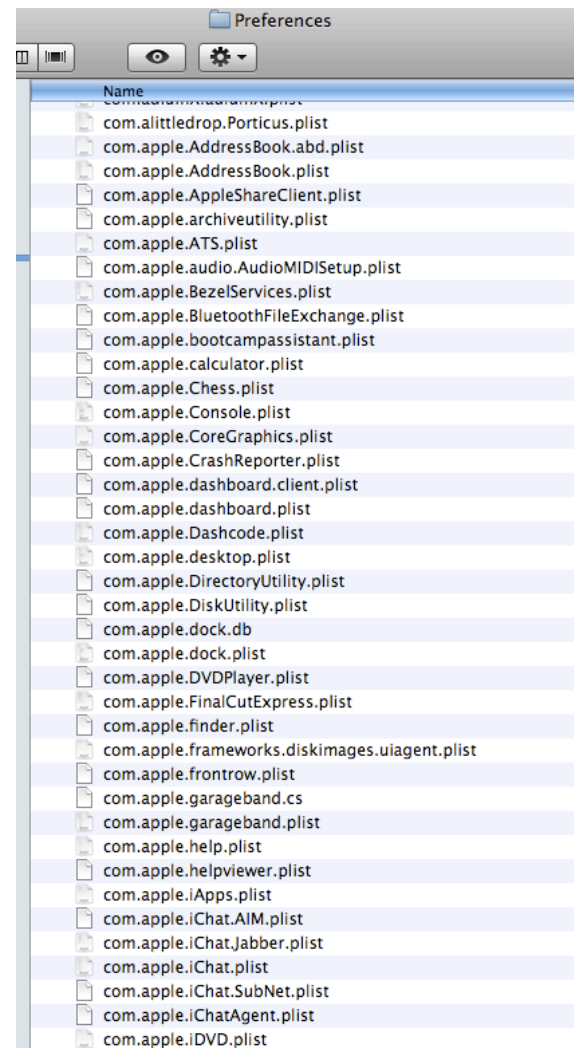


# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

### Episode 4 Shownotes

- Preferences:
  - PLists files or proprietary format files for the User
  - Contains configurations and settings for the User
  - I.E. Online activity, buddy lists, email logins, etc.



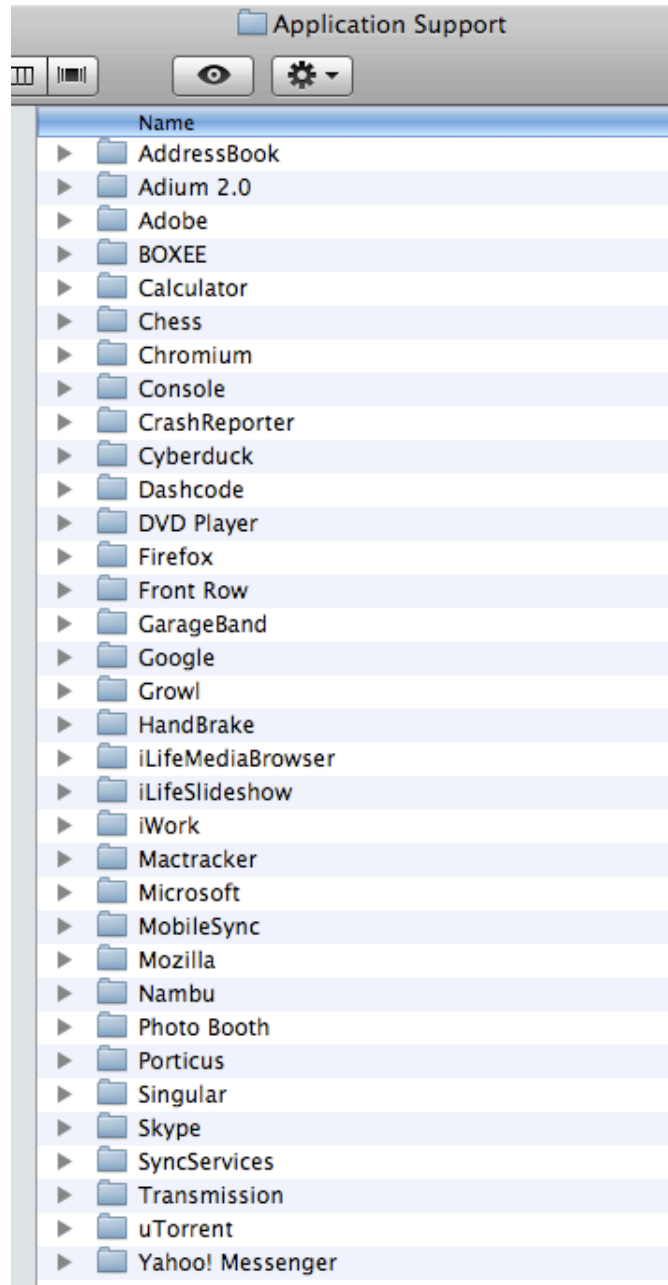
## INSIDE THE CORE:

# The Macintosh and Apple Device Forensics Podcast

Episode 4 Shownotes

-Application Support:

- Mozilla Cache, iPhone backup files from MobileSync folder
- Application PLists with information



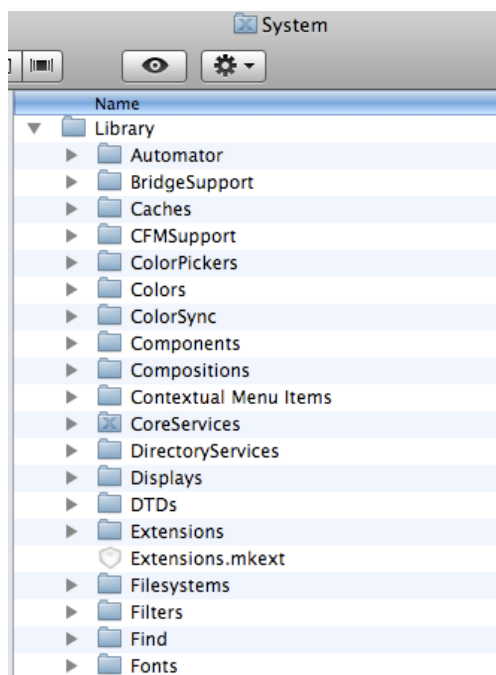
# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

### Episode 4 Shownotes

Other things to look at:

- Red Flag: Any folders in addition to the default nine folders in the User Folder
- Desktop: Lazy Users keeping stuff on their desktop
- System Folders: On a future podcast we will emphasize this important source of evidentiary data



## Disk Arbitration:

- On Windows machine, normally use write block devices to allow for imaging
- On MAC, can control the mounting mechanism without expensive write block devices
- This is called Disk Arbitration

## REFERENCE WEBSITE:

[MACOSXFORENSICS.COM](http://MACOSXFORENSICS.COM) --> Technologies --> Disk Arbitration

Tiger: More Dangerous to utilize and will address second

# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

### Episode 4 Shownotes

LEOPARD:

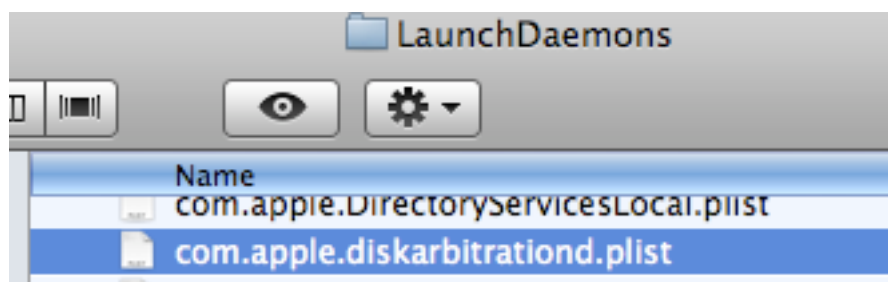
-Disk Arbitration looks at devices and Mounts the device and makes Icon to access this device available to the user

-On Boot, Disk Arbitration recognizes the internal hard drive. Recognizes file system. Mounts partitions on desktop.

-In order to prevent writes, we must prevent the mount.

-To turn off Disk Arbitration, enter COMMAND LINE and type:

**sudo launchctl unload System/Library/LaunchDaemons/com.apple.diskarbitrationd.plist**



-When typed and you hit enter, it will prompt for admin password and after entered it drops to next command line

-Now when you connect a disk, the disk will not mount

-If Activity Monitor is viewed, you will see the process, however it is neutralized.

-Now you can connect a device, image it using "DD" in Terminal, and you can make raw image

-To turn back on, enter COMMAND LINE and type:

**sudo launchctl load System/Library/LaunchDaemons/com.apple.diskarbitrationd.plist**

**or** Reboot system and diskarbitration will become active again

# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

### Episode 4 Shownotes

#### TIGER:

-Not controlled by LaunchCtl process

-Need to move the PList from one location to another

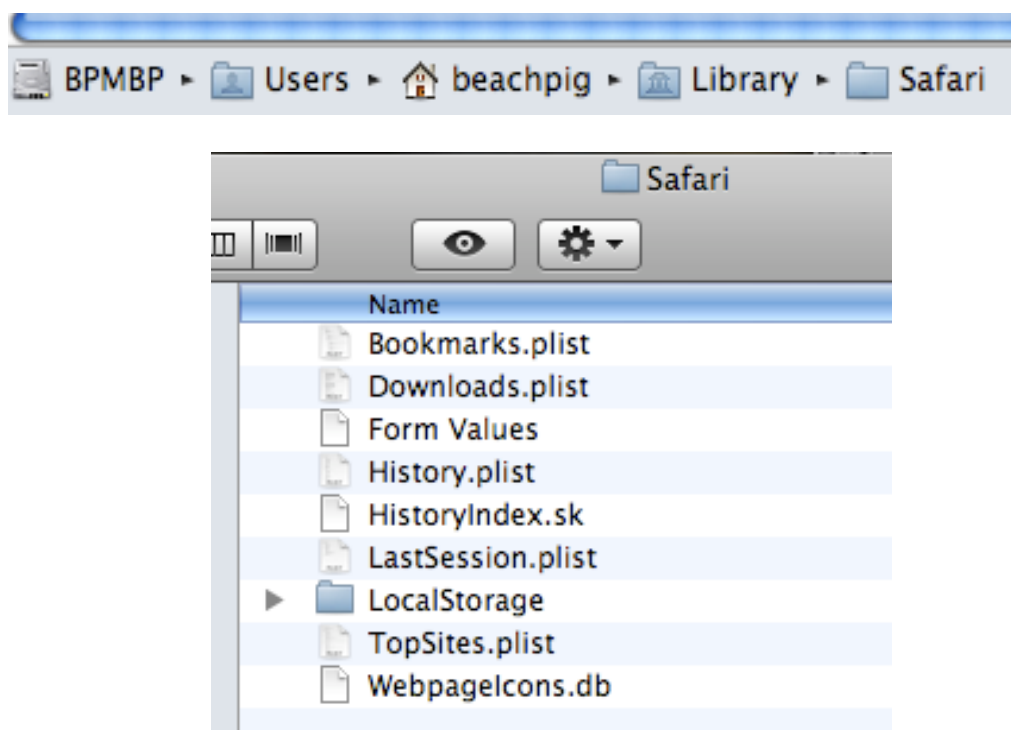
-Method:

1. Make copy of the diskarbitrationd.plist
2. DO NOT MOVE IT: YOU CAN CRASH THE MAC WITHOUT DISKARBITRATION.
3. \*\*\*\*DO NOT DISABLE DISK ARBITRATION WITH FILEVAULT ENABLED. DO NOT USE FILEVAULT ON YOUR FORENSIC MACHINE!!!!!!
  - a. In TIGER, it will not be available at all.
  - b. In LEOPARD, it has occasionally worked with FV on, however not recommended.
4. sudo remove com.apple.diskarbitrationd.plist from /etc/mach\_init.d folder
5. Reboot system
6. Only OS Boot partition will mount.
7. To UNDO, Copy the diskarbitrationd.plist back to the /etc/mach\_init.d folder.
8. Reboot

-See [MACOSXFORENSICS.COM](http://MACOSXFORENSICS.COM) for [AppleScripts](#) to run the Diskarbitration On/Off tools.

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

### User/Library/Safari:





# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

### Episode 4 Shownotes

#### History.plist (cont.):

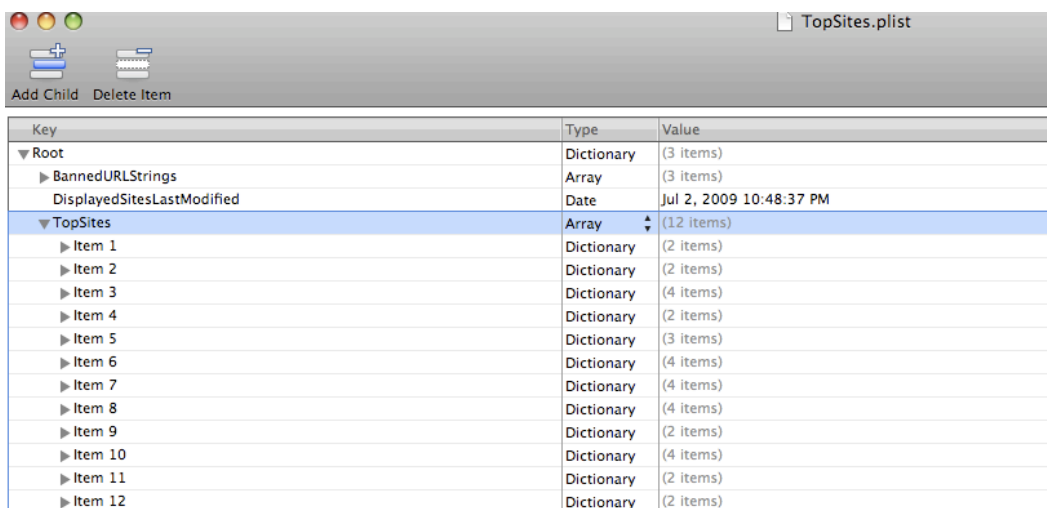
-Shows:

- URL String: Site visited
- Title for the site
- Visit Count

▼ Item 1638	Dictionary	(6 items)
	String	http://scores.espn.go.com/golf/leaderboard
▼ D	Array	(1 item)
Item 1	Number	1
displayTitle	String	U.S. Open Championship Golf Leaderboard and Results – ESPN
lastVisitedDate	String	267382936.6
title	String	U.S. Open Championship Golf Leaderboard and Results – ESPN
visitCount	Number	1

#### TopSites.plist

- Came with Safari 4
- Similar to Google Chrome's browser
- When a New Tab is opened, it opens thumbnails of your most visited sites
- Instead of typing URL, can just click on the thumbnail and it opens the site.
- View a site more frequently it bumps the site off.
- From Non-Forensic side, WIFE MAY CATCH WHAT YOU REALLY LOOK AT :)
- Can be edited, decide from settings to remove a site or pin it to always keep it in Top Sites



Key	Type	Value
▼ Root	Dictionary	(3 items)
▶ BannedURLStrings	Array	(3 items)
DisplayedSitesLastModified	Date	Jul 2, 2009 10:48:37 PM
▼ TopSites	Array	(12 items)
▶ Item 1	Dictionary	(2 items)
▶ Item 2	Dictionary	(2 items)
▶ Item 3	Dictionary	(4 items)
▶ Item 4	Dictionary	(2 items)
▶ Item 5	Dictionary	(3 items)
▶ Item 6	Dictionary	(4 items)
▶ Item 7	Dictionary	(4 items)
▶ Item 8	Dictionary	(4 items)
▶ Item 9	Dictionary	(2 items)
▶ Item 10	Dictionary	(4 items)
▶ Item 11	Dictionary	(2 items)
▶ Item 12	Dictionary	(2 items)

▼ TopSites	Array	(12 items)
▼ Item 1	Dictionary	(2 items)
TopSiteTitle	String	Google
TopSiteURLString	String	http://www.google.com/
▼ Item 2	Dictionary	(2 items)
TopSiteTitle	String	DRUDGE REPORT 2009®
TopSiteURLString	String	http://drudgereport.com/

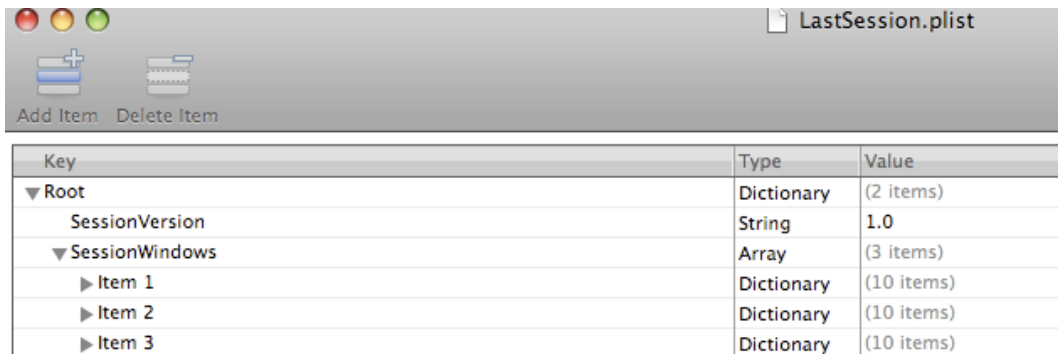
# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

### Episode 4 Shownotes

#### LastSession.plist:

- Indicates what was open on last Safari session
- If multiple windows opened, it will indicate each as a different Item
- Under each Item, it will indicate quantity of tabs open as multiple URLs listed.



Key	Type	Value
▼ Root	Dictionary	(2 items)
SessionVersion	String	1.0
▼ SessionWindows	Array	(3 items)
▶ Item 1	Dictionary	(10 items)
▶ Item 2	Dictionary	(10 items)
▶ Item 3	Dictionary	(10 items)

▼ Item 1	Dictionary	(10 items)
FavoritesBarHidden	Boolean	<input type="checkbox"/>
LocationBarHidden	Boolean	<input type="checkbox"/>
Miniaturized	Boolean	<input type="checkbox"/>
SelectedTabIndex	Number	2
StatusBarHidden	Boolean	<input checked="" type="checkbox"/>
TabBarHidden	Boolean	<input type="checkbox"/>
▼ TabLabels	Array	(3 items)
Item 1	String	
Item 2	String	
Item 3	String	
▼ TabURLs	Array	(3 items)
Item 1	String	<a href="https://mail.google.com/mail/#inbox">https://mail.google.com/mail/#inbox</a>
Item 2	String	<a href="http://images.google.com/">http://images.google.com/</a>
Item 3	String	<a href="http://www.google.com/">http://www.google.com/</a>
WindowContentRect	String	{{33, 52}, {1246, 925}}
WindowStateVersion	String	1.0

▶ Item 1	Dictionary	(10 items)
▼ Item 2	Dictionary	(10 items)
FavoritesBarHidden	Boolean	<input type="checkbox"/>
LocationBarHidden	Boolean	<input type="checkbox"/>
Miniaturized	Boolean	<input type="checkbox"/>
SelectedTabIndex	Number	3
StatusBarHidden	Boolean	<input checked="" type="checkbox"/>
TabBarHidden	Boolean	<input type="checkbox"/>
▼ TabLabels	Array	(4 items)
Item 1	String	
Item 2	String	
Item 3	String	
Item 4	String	
▼ TabURLs	Array	(4 items)
Item 1	String	<a href="http://www.cnn.com/">http://www.cnn.com/</a>
Item 2	String	<a href="http://drudgereport.com/">http://drudgereport.com/</a>
Item 3	String	<a href="http://nascar.com/">http://nascar.com/</a>
Item 4	String	<a href="http://mlb.com/">http://mlb.com/</a>
WindowContentRect	String	{{54, 52}, {1246, 925}}
WindowStateVersion	String	1.0

# INSIDE THE CORE:

## The Macintosh and Apple Device Forensics Podcast

Episode 4 Shownotes

### WEBSITES OF THE WEEK:

#### [everymac.com](http://everymac.com):

- Site has information about each specific Mac/Apple hardware device and the specifications.
- Also has pricing and shopping information



#### [Mactracker](http://Mactracker.dreamhosters.com):

- Website/Application: (can use on Windows or Mac)
- Can access and look at specs of the Mac you are dealing with in the field
- Gives a break down of the Mac: Intel vs. PPC, Memory, HDD, etc.
- Can access their phone friendly site and do the same as well
- Mactracker.dreamhosters.com



### OTHER FORENSIC PODCAST RECOMMENDATIONS:

#### [Cyberspeak](http://Cyberspeak.com):

- Ovie and Brett-Former Feds
- Not Tool or OS specific



#### [Forensic4Cast](http://Forensic4Cast.com):

- Lee Whitfield
- Interviews, Debates, and discussions.

**Forensic 4cast**

INSIDE THE CORE:  
The Macintosh and Apple Device Forensics Podcast  
Episode 4 Shownotes

THANKS AND LOOK FORWARD TO EPISODE 5 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/> :



INSIDE THE CORE:

The Macintosh and Apple Device Forensics Podcast

Episode 4 Shownotes