

INSIDE THE CORE:

The Macintosh and Apple Device Forensics Podcast

Episode 5 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, 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 (in absentia)

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

No Chris No Reggie, All Ryan and Dave!

Welcome News:

-Listener tip: Don't write notes for podcast while driving



TEXT MESSAGING

lol no im nt bsy im only drving

INSIDE THE CORE:

The Macintosh and Apple Device Forensics Podcast

Episode 5 Shownotes

Stork arrives for MacLovin:

Mac Mini
Macbook Pro on the way



WHAT? WHAT? WHAT?...Maclovin has a powerbook 12"

iPhone backup files:

Processing:

user//library/applicationsupport/mobilesync/backup

-another folder with uuid for each phone

-prior to itunes 8.1 used to be mddbckup (plist file w/data)

-iPhone extractor: extracts all the data from the iPhone

-After 8.1 , this didn't work...

-iPhone now using mddata and mdinfo file, 1 of each for each file

-mdinfo:a plist

-mddata-data of the file

-can drop on and juice it

-also in the backup folder are info.plist

-iphone name, imei, iphone #

-status.plist: last sync info

-manifest.plist: list of all files backed up, time/data, sha1

-Each file has unique name by sha1 hash

-MDHelper extracts manifest.plist information

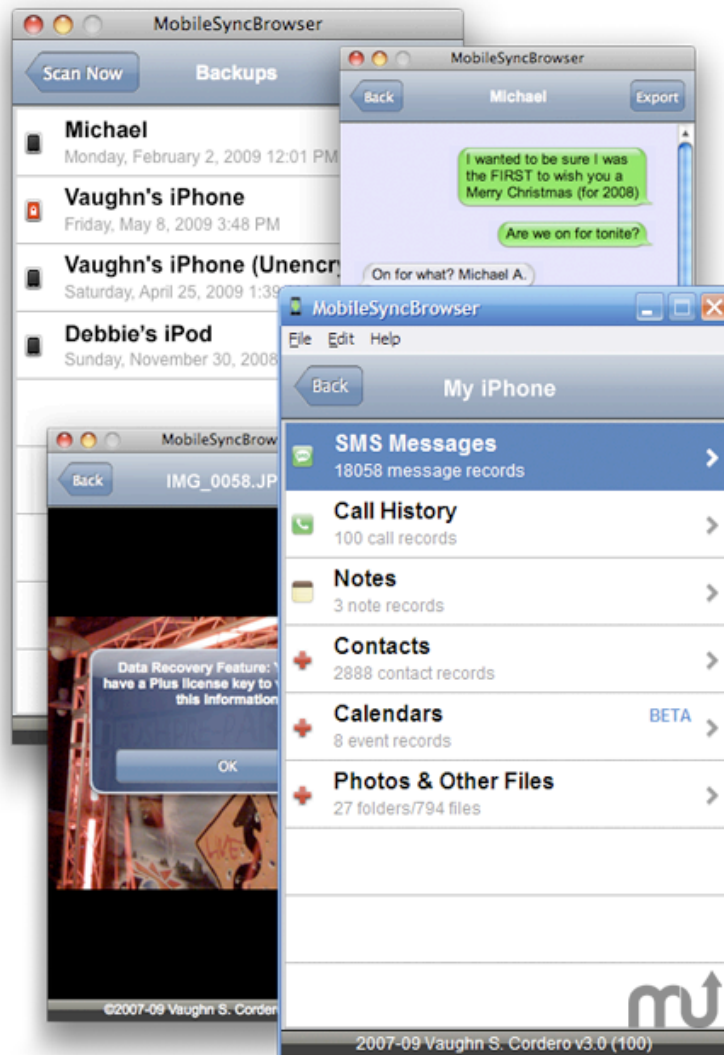
-iphone backup: safari history, bookmarks, photos, youtube search, email info, google map history, SMS, calendar, call history no emails or voicemails,



INSIDE THE CORE: The Macintosh and Apple Device Forensics Podcast Episode 5 Shownotes

Mobile Sync Browser:

Vaughn Cordero homepage.mac.com/vaughnmssync \$20 Plus, \$10 for the classic



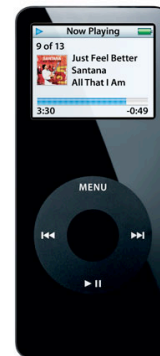
INSIDE THE CORE:

The Macintosh and Apple Device Forensics Podcast

Episode 5 Shownotes

iPod Acquisitions:

- Notes on MacOSXForensics.com Analysis/iPod Acquisition
- iPod: Ipod Classic, Mini, Nano: can be put in disk mode
- Touch/iPhone Do not support disk mode
- Trying to make an image to analyze the data
- Data could be anything
- Can be used as disk: Fat 32 or HFS
- Determined by the computer first plugged into
- If Windows, FAT32, if Mac its HFS
- User can add additional data outside the standard Itunes functionality
- Prior to connecting iPod:
 - Open Terminal
 - Check for currently attached disks: type `LS /dev/disk?`
 - Will show disks attached to Mac
 - Turn off DiskArbitration..Go to Files and download diskarbitration tools for on/off
 - Ask for Admin PW
 - Validate this
 - Plug in test media and see if it mounts, if not its off, if it does, the script erred
 - If Off, plug in iPod w/iPod cable for imaging
 - In terminal `ls /dev/disk?` , see which disk file exists now that was not there before
 - Use built in DD executable, command: `sudo dd if=/dev/disk#(for iPod) of=/~/Desktop/iPodImage.dmg` Will require admin pw
 - DMG compatible with OSX for mounting purposes
 - Will image the iPod to the Desktop
 - Will hang out at PW prompt until image done
 - Calculate MD5 or SHA1 of original device: command: `sudo open ssl dgst-md5 /dev/disk#(of the iPod) > ~/Desktop/iPodImage.dmg.md5.text`
 - Now calculate for the image. Command: `sudo open ssl dgst-md5 ~/Desktop/iPodImage.dmg >> ~/Desktop/iPodImage.dmg.md5.text`
 - >> means append the results to the text file
 - Need to lock the file. Need to take ownership of the DMG.
 - `sudo chown "USERNAME" ~/Desktop/iPodImage.dmg` -Make Me the user the owner
 - Right Click or Control Click..Get Info.Check box in the Locked box.
 - Prevents changes without explicit permission from Owner
 - Other users cannot make changes
 - Disconnect the cable
 - Turn DiskArb back on
- DCFLDD may be installed and used. It will provide feedback during the imaging
- Options to consider. Check ""MAN" page for DD
- REMEMBER TO LOCK DOWN THE FILES
- DC3DD from Sourceforge



INSIDE THE CORE:

The Macintosh and Apple Device Forensics Podcast

Episode 5 Shownotes

Derrick Donnelly: Guest Hint:

Wanted to run strings command against 4GB swapfile

- Swapfile is pagefile for Mac
- Swapfile location: private/var/vm
- Mac System pages RAM as necessary
- Great information from system in this location, to poss include passwords
- Ran strings and got nothing..could see text in Raw file
- Strings cant handle 4GB
- Use DD to handle sudo DD if=swapfile0 bs=32768 | strings > ~/Desktop/dictionary.txt
- will create a dictionary file in text format
- use sort and uniq command
- sort puts hits together,
- uniq command will strip out duplicates
- strings 2gb worked, 4gb failed
- dd, sudo, & strings worked against 4gb

PLOW (Plist of the Week): **com.apple.quicktimeplayer.plist**

GLOBAL: Owner/Serial # i the Global

User-->Library-->Preferences-->com.apple.quicktimeplayer.plist

Capture location: shows default save to location

- Can be changed
- By Default it is the desktop
- Can be changed in Preferences
- Player settings
- NsNavLastRootDirectory: Shows last saved directory, in the event user set it for a different directory
- QTPRRecentDocuments: Shows recent docs accessed and played. Chronological order/Name of file/Location
 - For website activity: shows the website as the alternative site
 - i.e. String: couples Retreat-Http://movies.apple.com/movies/Universal/couplesretreat.mov
 - String Type: URL
 - Allows to view files/file locations/URL or if suspect poss moved them, or name changed them
 - Poss check for deletion/other media



INSIDE THE CORE: The Macintosh and Apple Device Forensics Podcast Episode 5 Shownotes

INSIDETHECORE CONTACT:

Email: coreforensics@gmail.com

Twitter: @insidethecore

Phone #: 562-502-7464 for VM or SMS

<http://www.insidethecore.com>

<http://insidethecore.libsyn.com>

Amazon store: Any purchase done can help benefit the hosting of Inside the Core!

Resources:

Ryan:

-Other World Computing: Offer in video form <http://eshop.macsales.com/installvideos/>

-MacOSXForensics: Resources papers and readings

-ArsTechnica: State of Mac Data Forensics

Dave:

-<http://www.iclarified.com>: News on Apple/Macs, tutorials, User comments

-<http://secrets.blacktree.com>: hidden settings for MacOSX, discussion/forum for additional macosx secrets

i

