



Phoning it in: Heather talks about Smartphone Forensics Heather Mahalik

Copyright ©2017 Heather Mahalik, All Rights Reserved

About me...

- Director, Forensic Eng. At ManTech CARD
- SANS Senior Instructor
- Involved with InfoSec/Forensics for 15+ years
- Co-author of FOR585
- Instructor of FOR585 and FOR408
- Co-Author of Practical Mobile Forensics (1st and 2nd Editions)
- Mom and a wife
- Dog, horse, wine and bourbon lover 😊

Agenda

- What is possible in smartphone forensics?
- Encryption and locks – are they a show stopper?
- Tools – can you trust them?
- Validation of tools and artifacts
- FOR585, GASF, blogs and more

A close-up, high-angle shot of Morpheus from the movie The Matrix. He is wearing his signature black sunglasses and has a serious, intense expression. The background is a blurred greenish-grey. The text 'WHAT IF I TOLD YOU' is written in large, white, bold, sans-serif font with a black outline, positioned at the top of the image. The text 'IT DEPENDS' is written in the same style at the bottom. A small watermark 'memegenerator.net' is visible in the bottom right corner.

**WHAT IF I TOLD
YOU**

"IT DEPENDS"

What's happening in smartphone security

- Full disk encryption readily available
 - More people are using it
 - Some devices require it
 - Hurts acquisition?
- Passwords encouraged
- Application security
- MDM



What does this mean?

- The state of every mobile device may vary
- You need to be prepared for all situations
- You will need more than one tool
- You will need the skills to manually carve for forensic artifacts
- You may be 100% blocked from the data

What should you do about it



- Consider the issue
 - Encryption, locks, lack of parsing support...
- Consider tools available to you
 - Commercial, open source and scripts
- Determine an action plan
- **Make sure your actions do not destroy your evidence!!!**

Full Disk Encryption

- iOS
 - Hardware level encryption stored between the flash memory and the system area in "Effaceable Storage"
- Android Lollipop/Marshmallow/Nougat
 - Offered for most devices
- Windows Phone 8/10
 - Incorporates Bitlocker Technology
- BlackBerry/Blackberry OS10
 - Hardware level encryption
 - Trusted as most secure*



User locks

- Most smartphones are often locked
- PIN or simple passcode
- Passphrase or complex passcode
- Biometric locks



Application “Protection”

Transforming/converting data into code

Encoding Schemes

ASCII

Unicode

UTF-8

Base64

Encryption Algorithms

AES

Blowfish

Twofish

Serpent

It's time to outsmart your tools
and the security features!

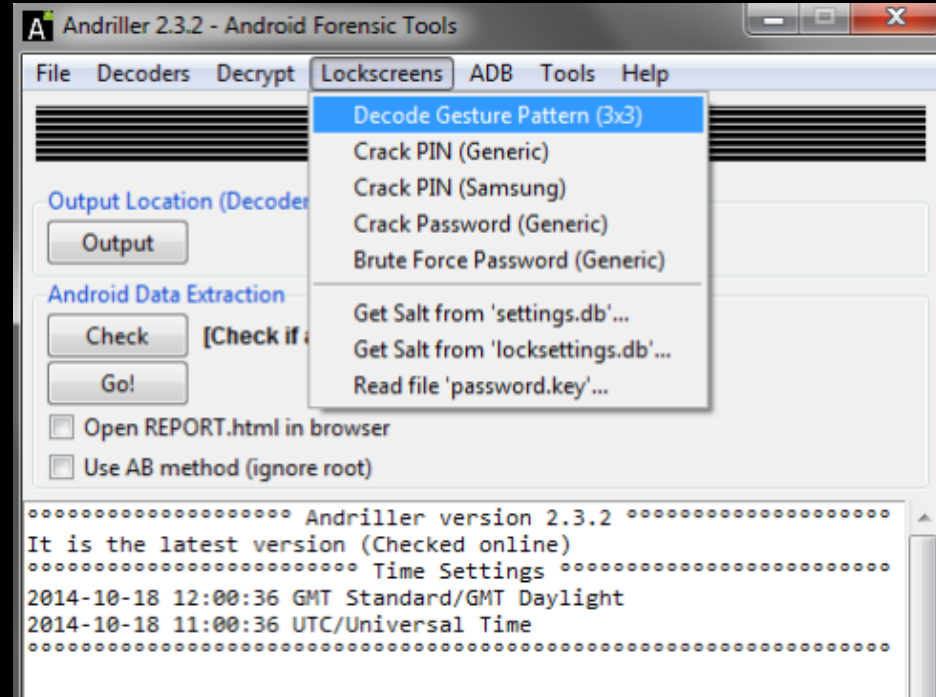
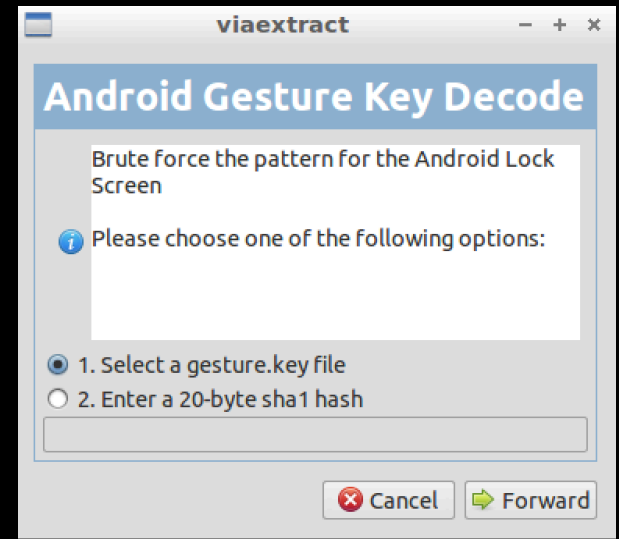


Full Disk Encryption

- Can you disable it?
- Can your tool bypass it or interject prior to booting?
- Can you bypass it after the fact?
- Consider the other components

User locks

- Try to crack that \$@!%
- Consider tools to help you
- Using “Smart Locks”



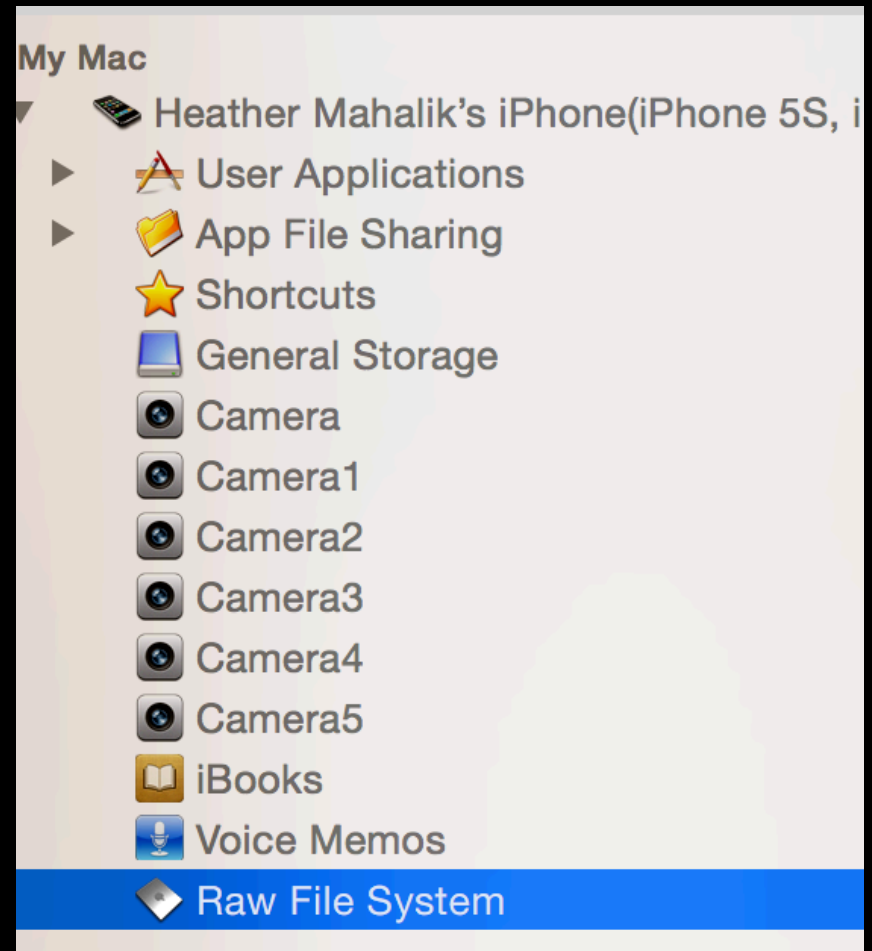
What about the Lockdown Files?

- Can be used to bypass a locked device for acquisition
- May not always work, but it's worth a shot



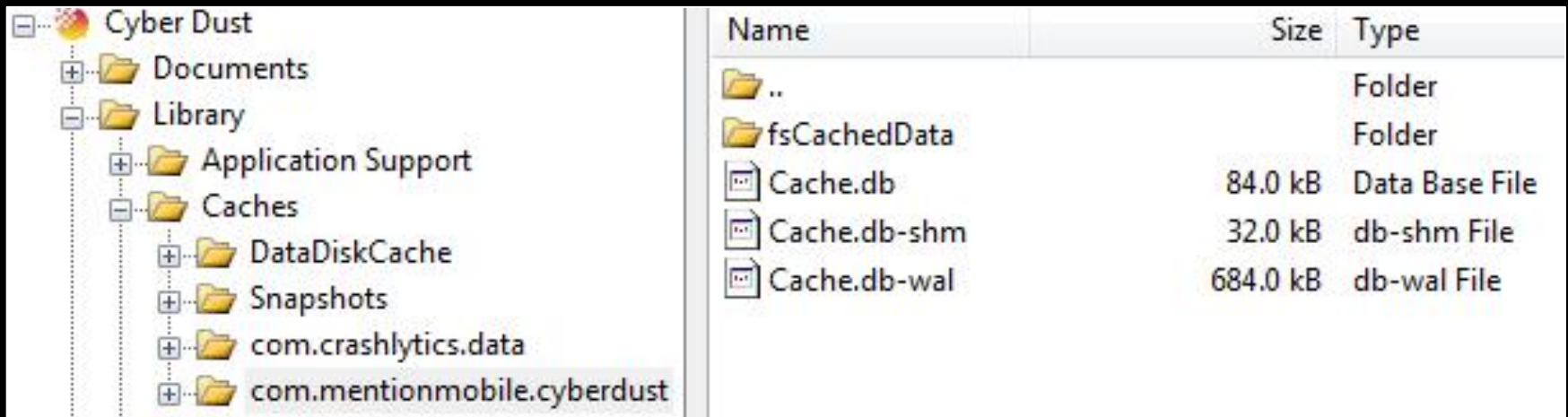
Application Encryption

- Use a tool to view the file system
- Export application files of interest
- Manually carve for user artifacts that are not parsed



Example: Cyber Dust (1)

- *Older versions claim* to remove all user data upon transmission/receipt
 - Never trust claims or your tool
 - Review App files for user activity



Name	Size	Type
..		Folder
fsCachedData		Folder
Cache.db	84.0 kB	Data Base File
Cache.db-shm	32.0 kB	db-shm File
Cache.db-wal	684.0 kB	db-wal File

Example: Cyber Dust (2)

- Messages are encoded twice using Base64

```
Cache.db-wal - Notepad
File Edit Format View Help
+ qè${"result":{"chatRoomContainer":{"account":
{"id":"545ce910e4b0994d3e7aa237","verified":false,"uniqueHash":"545ce910e4b0994d3e7aa237","us
erName":"","emailAddress":"","hashedPassword":"EgJr3md07L...xmas",
resetPassword:false,"phoneNumber":null},"chatRooms":[{"chatRoom":
{"id":"545ce911e4b083b91217c697","lmac":"53a3671ae4b0fa51763e269a","acnts":
[{"id":"53a3671ae4b0fa51763e269a","userName":"cdteam"},"blocked":null,"dateNum":1415375121130},"messages":
[{"id":"545ce911e4b083b91217c698","roomId":"545ce911e4b083b91217c697","accountId":"53a3671ae4b0fa51763e269a","message"
:"welcome to Cyber Dust! This is the Cyber Dust Team. we are here to answer any questions you may have about Cyber
Dust. want to know how something works? Just ask. We will have a team member working to get you an ans., | %B
{"result":{"chatRoom":{"id":"545d1248e4b03b0f39738647","lmac":"545d11eae4b00f8f7d387a49","acnts":
[{"id":"545d11eae4b00f8f7d387a49","userName":"calvincakes"},"blocked":null,"dateNum":1415385672312},"messages":
[{"id":"545d1248e4b03b0f39738648","roomId":"545d1248e4b03b0f39738647","accountId":"545d11eae4b00f8f7d387a49","message"
:"what's up my
boy?","videoId":null,"encryptedMessage":"VjJoaGRDZHpJSFZ3SUCxNUlHSnZlVDg9","imageData":null,"videoThumbnailImageData":
null,"type":"BlastChat","date":"2014-11-07 18:41:12.661:
+0000","longitude":0.0,"latitude":0.0,"locationName":""}}]},"error":null,"warning":null}}^E
{"result":
{"chatRoomContainer":{"account":
```

Decoded Output

Here is the decoded output of your Base 64 input:

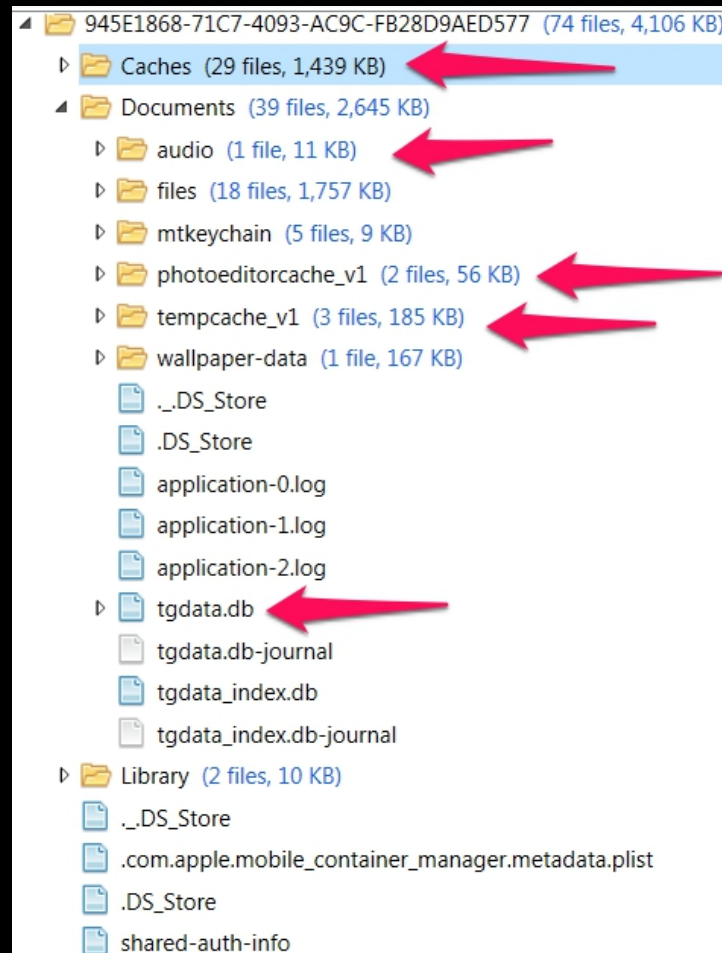
V2hhdCdzIHVwIG15IGJveT8=

Decoded Output

Here is the decoded output of your Base 64 input:

What's up my boy?

Example: Telegram (1)



Example: Telegram (2)



46		777000	Martha Vines	162132182	New in version 3.4:...	02/06/2016 09:46:07			
38	Martha Vines	162132182	P Nasty	153339917		02/06/2016 09:46:54	<click to view>	Sent	
39	Martha Vines							Sent	
40	P Nasty				5a50d642c808bc33786aa57bbfca7d97	2/6/2016 4:48 PM	File	19 KB	Received
41	P Nasty				8b8fd24b6f791d0d0df941604d2d0b40	2/6/2016 4:46 PM	File	23 KB	Received
6	P Nasty								Received
917			Martha Vines	162132182	I drank your wine	02/06/2016 09:48:44			Received
182				-2147483650	Oh no!!!!	02/06/2016 09:49:03			Sent
182				-2147483650	Must chug the beer	02/06/2016 09:49:10			Sent



Have you exhausted all options?

Think outside the box... or “inside”
the box and cloud

Consider the backup files

- Do you have access to the host computer?
 - Assuming the user has synced with iTunes
 - Use a tool like Elcomsoft to crack the password
- Use the pairing record to access the device
 - The pairing record is a unique key associated to the iOS device
 - Pairing records are required for communication with the device since iOS7
- Will not work on a freshly restarted device
- Limited data may be recovered

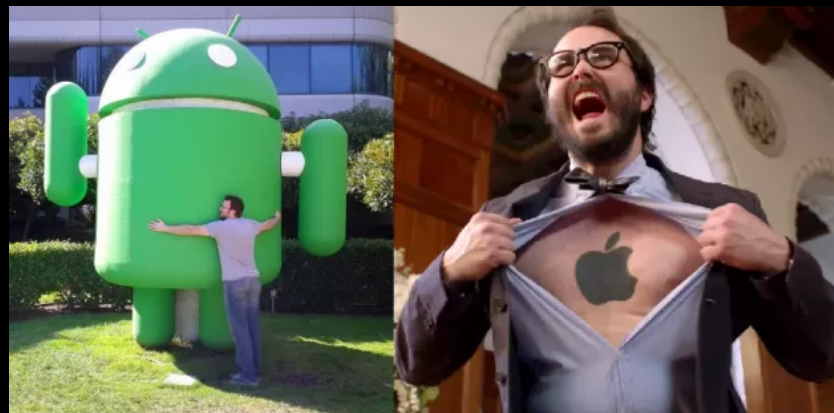
Will your tool catch you when you fall?

- Will you be able to defend the evidence?
- Can you find the data?
- What if the tools contradict one another?
- Understand the artifacts
- Don't know just enough to be dangerous



Why the tools fail...

- There is so much data
- Too many applications
- OS updates
- Knowing where to find this information is the hardest part
- Knowing how the artifact was created is key!



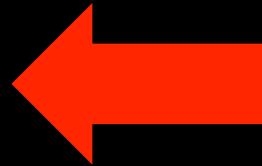
Example 1: Call Logs (1)

Magnet IEF



Mobile	
Calendar Events	157
iOS Call Logs	222
iOS Contacts	507

UFED Physical Analyzer



Device Content	
Phone Data	
Bluetooth Devices	3 (0)
Call Log	184 (64)

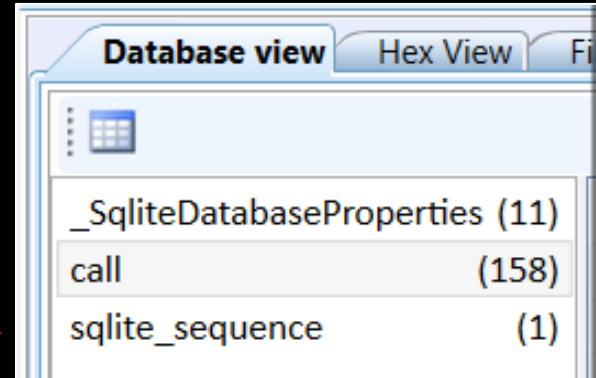
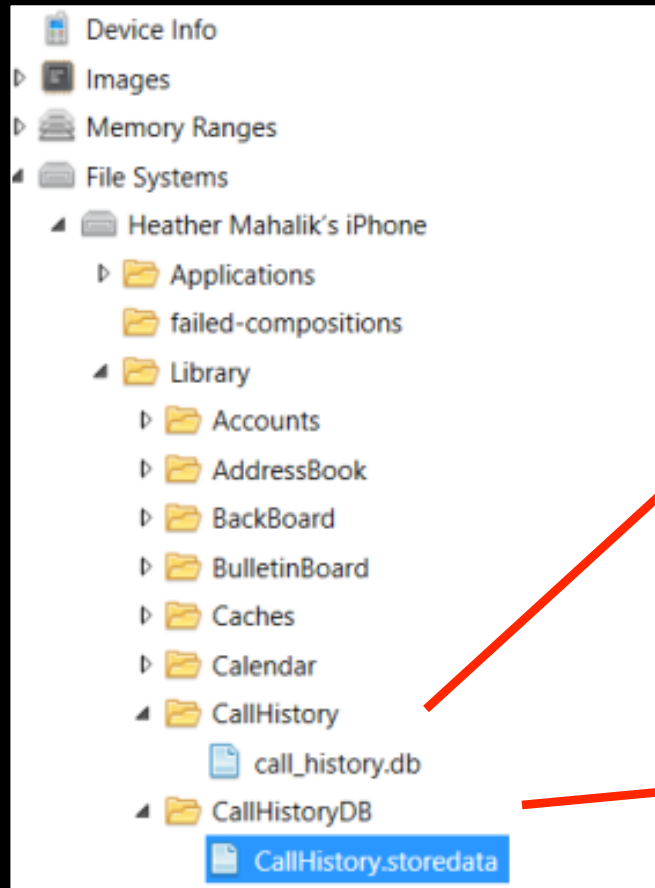
Call Logs

Library/CallHistory/call_history.db

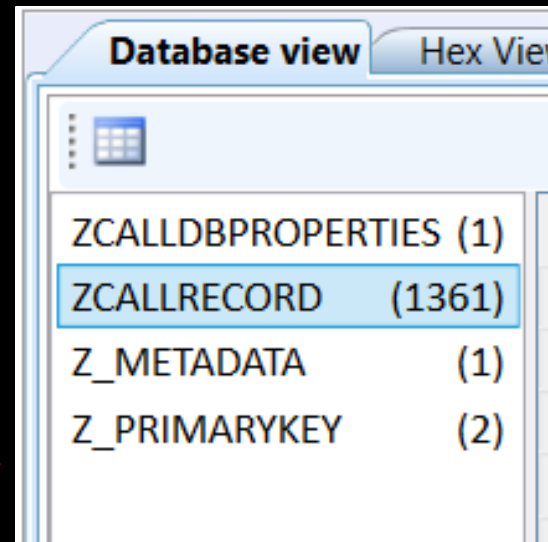
Library/CallHistory/callhistory.storedata (iOS 8,9 & 10)

Example 1: Call Logs (2)

Call logs



iOS 7

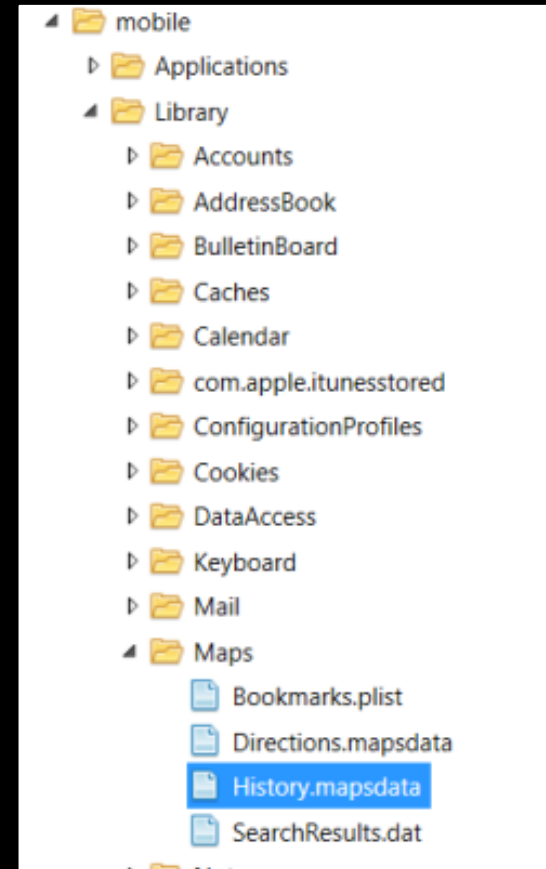
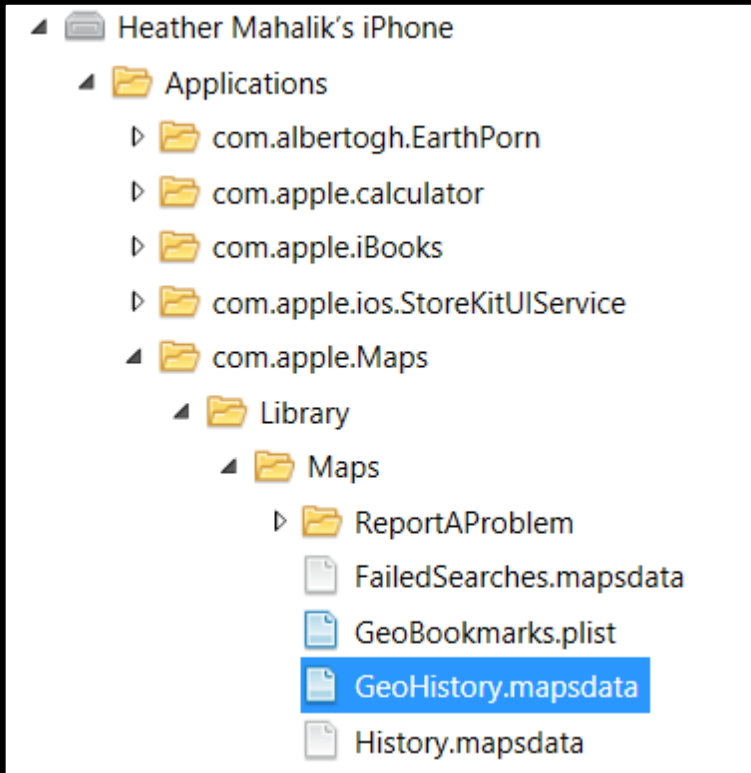


iOS
8,9 &
10

Example 2: Apple Maps

iOS 8, 9 & 10*

iOS 7



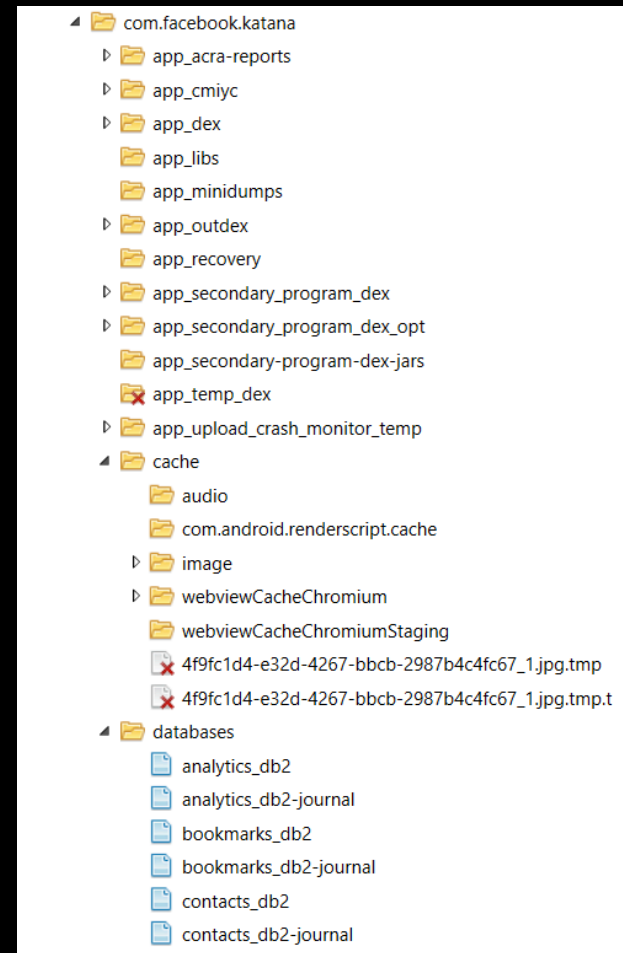
Apple Maps

Library/Maps/History.mapsdata

Library/Maps/GeoHistory.mapsdata (iOS 8, 9 & 10?)

Why data is missed (1)


- Social media geo-tagging
 - Facebook
 - Google+
 - Twitter
 - Etc.
- Consider what traces are left behind when the user “checks-in” and tags a location



Why data is missed (2)

- Digging deeper into the apps
 - What are they really doing?

<input checked="" type="checkbox"/>	docid	c0Entry_id	c1text	c2modified_date
<input checked="" type="checkbox"/>	1	8CC1B93F56974CD594104E20E33FBB61	First tomatoes from my garden!	1373325781
<input checked="" type="checkbox"/>	2	6967D3A0F4054D399E3F937A15B97F5C	Test	1373325858



```
version="1.0" encoding="UTF-8"?>.<!DOCTYPE PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">.<dict version="1.0">.<dict>.<key>Creation Date</key>.<date>2013-07-08T23:22:35Z</date>.<key>Entry Text</key>.<string>First tomatoes from my garden!</string>.<key>Location</key>.<dict>.<key>Administrative Area</key>.<string>Virginia</string>.<key>Country</key>.<string>United States</string>.<key>Latitude</key>.<real>38.897663774005039</real>.<key>Locality</key>.<string>Dunn Loring</string>.<key>Longitude</key>.<real>-77.240605317128114</real>.<key>Place Name</key>.<string>8521 Mineerva Ct</string>.</dict>.<key>Starred</key>.<true/>.<key>Time Zone</key>.<string>America/New_York</string>.<key>UUID</key>.<string>8CC1B93F56974CD594104E20E33FBB61</string>.<key>Weather</key>.<dict>.<key>Celsius</key>.<string>29</string>.<key>Description</key>.<string>Partly Cloudy</string>.<key>Fahrenheit</key>.<string>84</string>.<key>IconName</key>.<string>pcloudy.png</string>.</dict>.</dict>.</plist>.
```

Recommended Steps

- Use tools for Triage
 - Which tool – well, it depends...
- Use more than one tool
 - Acquisition
 - Analysis
- Don't be afraid to do it yourself!
- Always verify your results

Essential skill development

- Learn how data is stored on Android and iOS devices
- Learn how to identify traces of OS upgrades
- Learn decoding and manual examination techniques
- Find ways to outsmart your tools
- Take FOR585 to make sure you build the necessary skills to effectively examine the next smartphone you see (and you will see one...)

About 585...

- Course launched in 2014
- GASF Cert – Vendor neutral available to everyone
- Co-authored with Lee Crognale and Cindy Murphy
- Addresses the hardest to tackle topics
- Covers iOS, BlackBerry, Android, Windows Phone, Knock-off, Nokia, 3rd Party Apps, Malware, SQLite examinations and more
- Includes 17 hands-on labs of current smart devices
- Is vendor NEUTRAL – We teach you the best methods

Upcoming Courses

FOR585 Advanced Smartphone Forensics Course Available At:

Austin, TX – June 2017*

SANSFIRE: Washington, DC – July 2017*

Chicago – August 2017

San Fran – Sept 2017

NetSec: Las Vegas – Sept 2017*

Berlin – Oct 2017*

Sydney – Nov 2017

CDI: Washington, Dc – Dec 2017*

OnDemand – Anytime you want!

***FOR585 – vLive – Learn in your PJs with a beer this summer!**

GIAC GASF Certification

- All students who attend qualify for discounted, free or bundle-pricing
- Vendor-neutral
- Proves you know how to stand behind the artifacts!
- Take FOR585 now and join forces with those who earned this sought after cert

Bottom line...



- Jokingly: There are more people in the world with a smartphone than those who have access to a toilet!
- Seriously: Most investigations involve a smartphone
 - Will you know where to find the data?
 - Will you need to rely on your tools?
 - Do you have a cert to back you?

References, Sources and Suggested Reading

- FOR585 Advanced Smartphone Forensics
- Practical Mobile Forensics , 2nd edition
- Learning iOS Forensics, 2nd edition
- <http://smarterforensics.com>
- <https://andriller.com/>
- <https://sandersonforensics.com>
- <http://az4n6.blogspot.com/p/downloads.html>
- <http://cheeky4n6monkey.blogspot.com/>
- www.mac4n6.com

Heather Mahalik

heather@smarterforensics.com

@HeatherMahalik

Blog: for585.com/blog

QUESTIONS?