

Bueller...Bueller...

Smartphone Forensics

Moves Pretty Fast. If you

don't Stay Current, You'll

Miss Evidence

Hank Mahalik

heather@smarterforensics.com

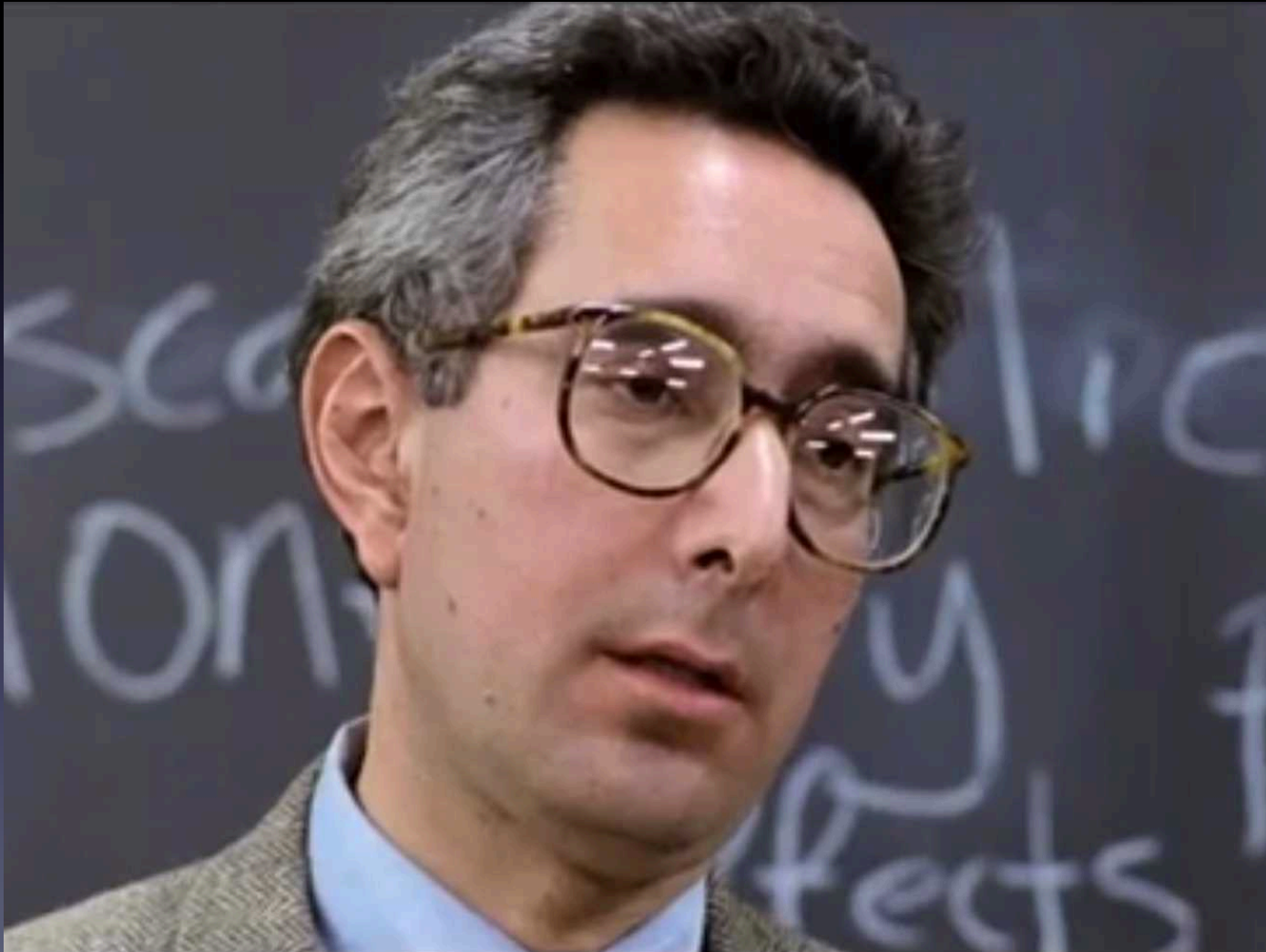
Twitter: @HeatherMahalik

<http://smarterforensics.com>

About me...

- Employee of Ocean's Edge, Inc.
- SANS Senior Instructor
- Involved with Forensics/infosec for 13 years
- Co-author FOR585 and FOR518
- Co-Author of Practical Mobile Forensics
- Available on social media

How have OS upgrades changed the game of Smartphone Forensics?



Copyright ©2015 Heather Mahalik, All Rights Reserved

What does this mean?

- You need to fully understand the OS on the device
- The state of every mobile device may vary
- You will need more than one tool
- You will need the skills to manually carve for forensic artifacts
- Reality – Your tool may miss relevant data!

Upgrades

- Operating System

- Android L & M

- iOS 9

- Applications

- All 3rd Party Applications on both devices



Lollipop, Lollipop...

- Multiple user accounts
- Factory reset protection
 - Must have password
- Full disk encryption
 - User is prompted at first startup
- Smart Lock
 - Device automatically unlocks when near specific Bluetooth, WiFi or NFC tags



Marshmallow!!!!



Updated fingerprint scan

Visual Voicemail

- T-Mobile and Orange France

Rotating home screen

RAM Manager

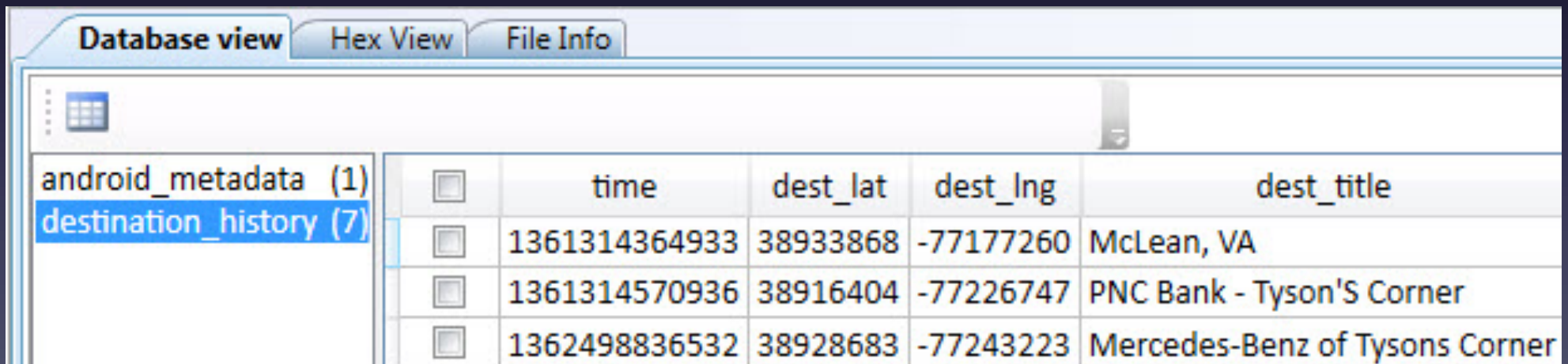
Network Setting Reset

Oh Evidence, Where are You?

- The location of the evidence hasn't really changed (yet)
- Getting to the evidence may be harder
- Acquisition may be more difficult and more expensive!

Understanding the Evidence (1)

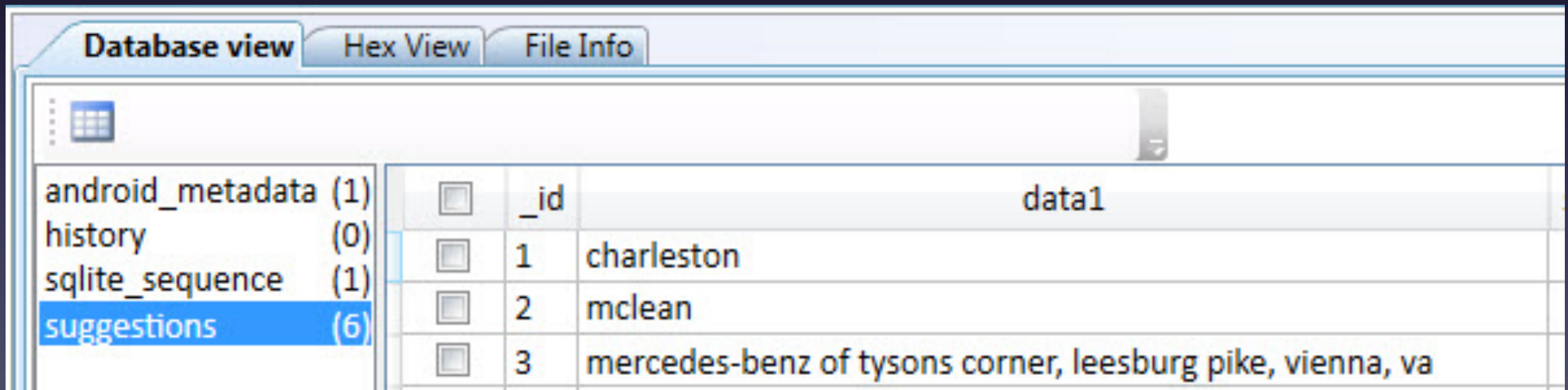
- Maps - com.google.android.apps.maps
 - Database: da_destination_history



android_metadata (1)		time	dest_lat	dest_lng	dest_title
destination_history (7)	<input type="checkbox"/>	1361314364933	38933868	-77177260	McLean, VA
	<input type="checkbox"/>	1361314570936	38916404	-77226747	PNC Bank - Tyson'S Corner
	<input type="checkbox"/>	1362498836532	38928683	-77243223	Mercedes-Benz of Tysons Corner

Understanding the Evidence (2)

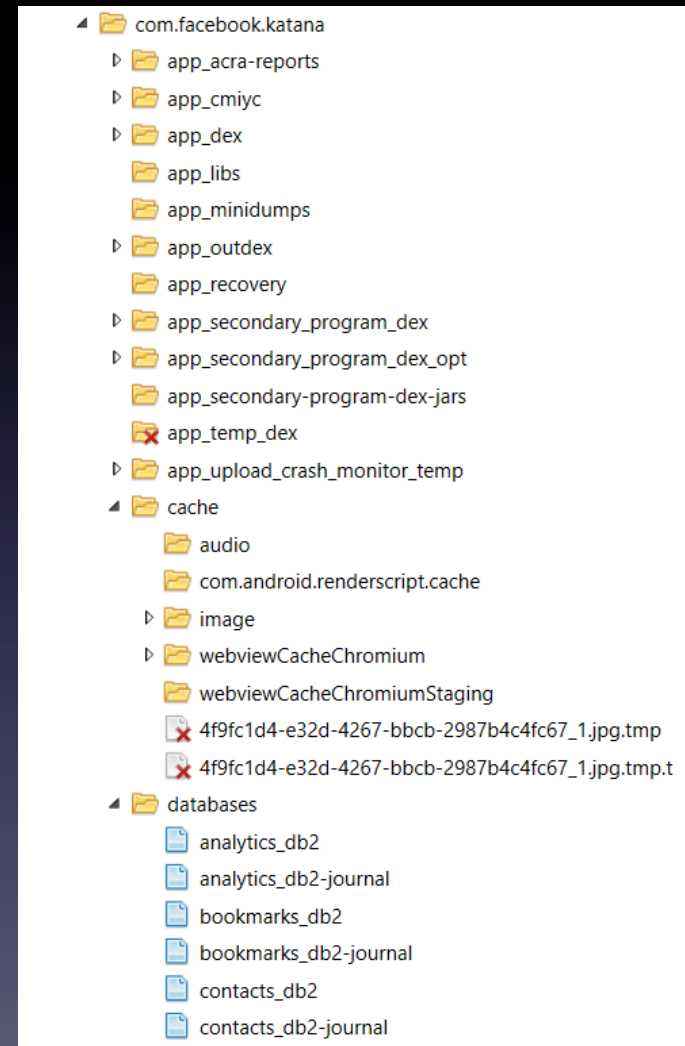
- Maps - com.google.android.apps.maps
 - Database: search_history.db



Database view		Hex View	File Info
android_metadata (1)	<input type="checkbox"/>	_id	data1
history (0)	<input type="checkbox"/>	1	charleston
sqlite_sequence (1)	<input type="checkbox"/>	2	mclean
suggestions (6)	<input type="checkbox"/>	3	mercedes-benz of tysons corner, leesburg pike, vienna, va

Understanding the Evidence (3)

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



iOS 9

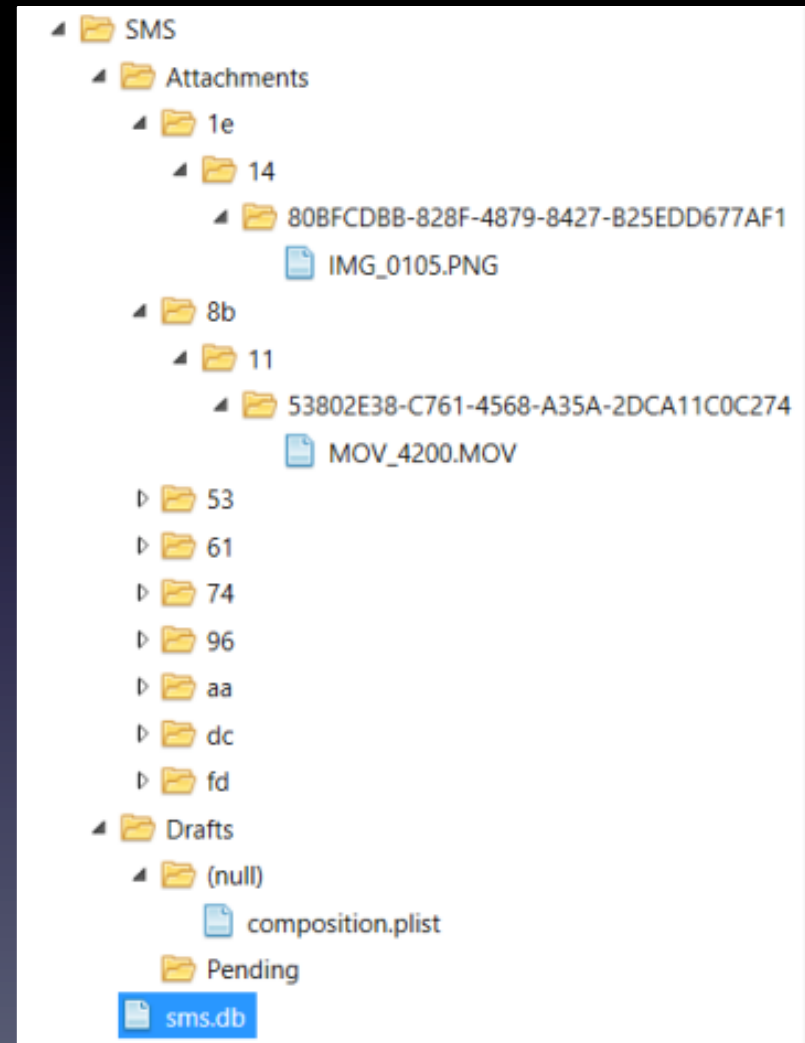
- Added functionality
- “Remembers” things for you
- Let’s you “undelete” pictures/videos
- Changed several data locations...

Your Past May Haunt You!

- iOS 8 & 9 “Recall”

Feature

- Scary that you thought it was gone...
- But guess what?

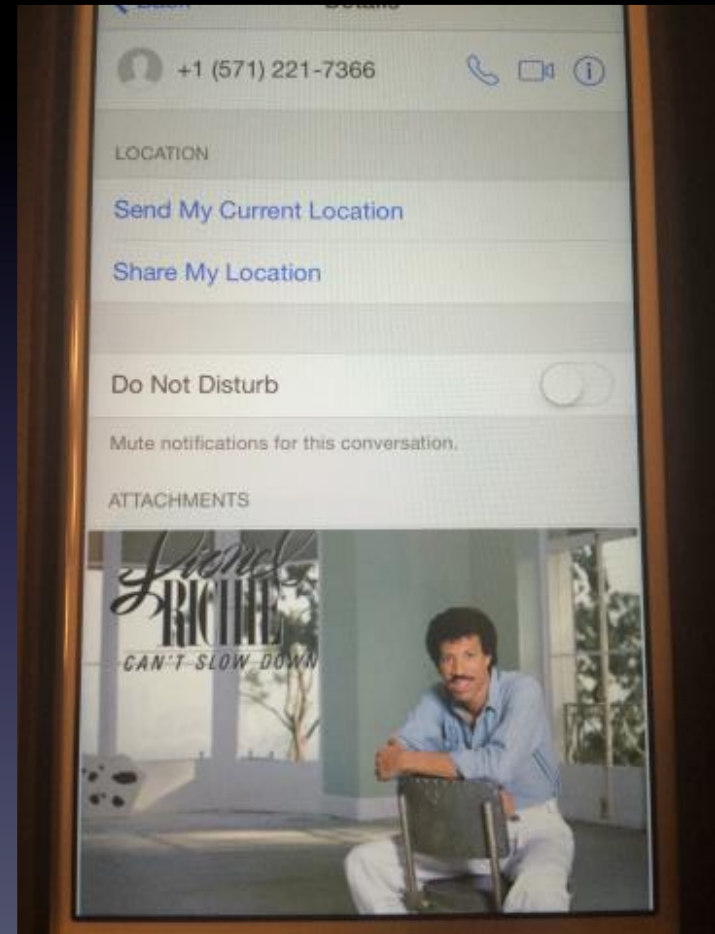
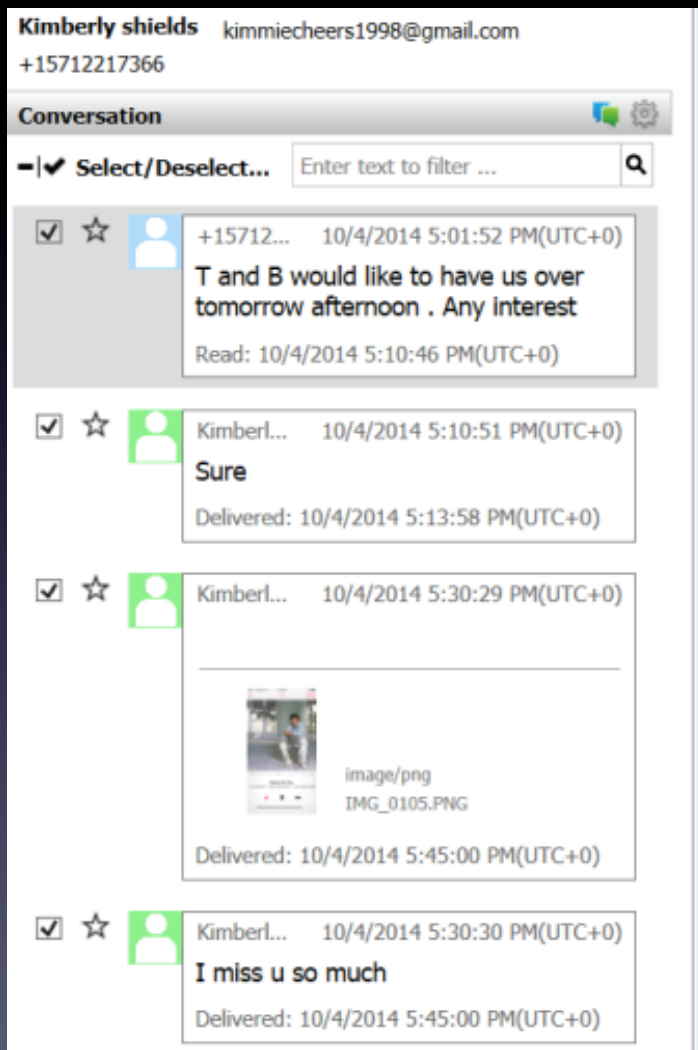


Manual Exam: SMS Attachments

Database view			Hex View	File Info
_SqliteDatabaseProperties	(7)	<input checked="" type="checkbox"/>	message_id	attachment_id
attachment	(8)	<input checked="" type="checkbox"/>	4	1
chat	(38)	<input checked="" type="checkbox"/>	8	2
chat_handle_join	(40)	<input checked="" type="checkbox"/>	13	3
chat_message_join	(161)	<input checked="" type="checkbox"/>	18	4
handle	(37)	<input checked="" type="checkbox"/>	25	5
message	(161)	<input checked="" type="checkbox"/>	27	6
message_attachment_join	(8)	<input checked="" type="checkbox"/>	181	7
sqlite_sequence	(4)	<input checked="" type="checkbox"/>	198	8

<input checked="" type="checkbox"/>	197	32B3E581-1E56-49A5-9D0F-EC3B08886AA4	Sure
<input checked="" type="checkbox"/>	198	9858D291-BA55-493B-80C5-DCBBA4EB6568	
<input checked="" type="checkbox"/>	199	EC4E42F2-7757-47F6-A2F9-4767FF84A887	I miss u so much

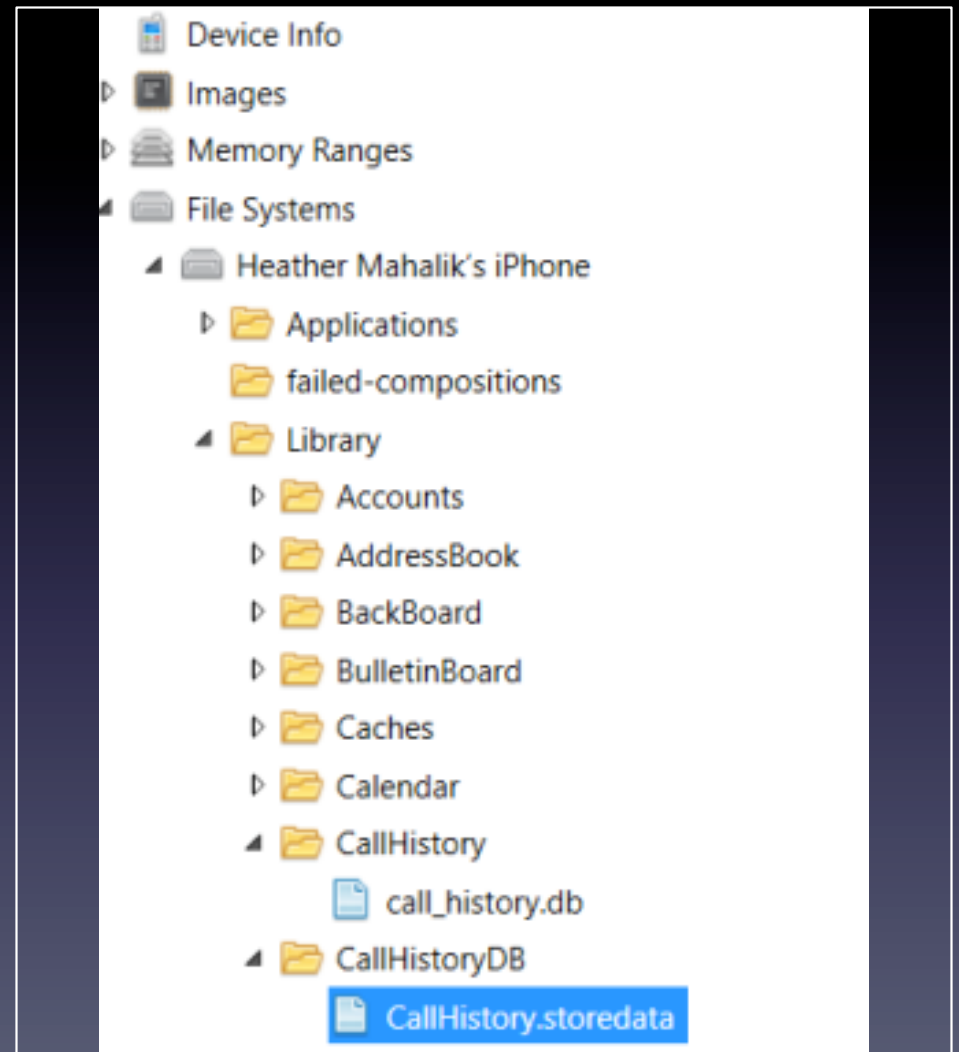
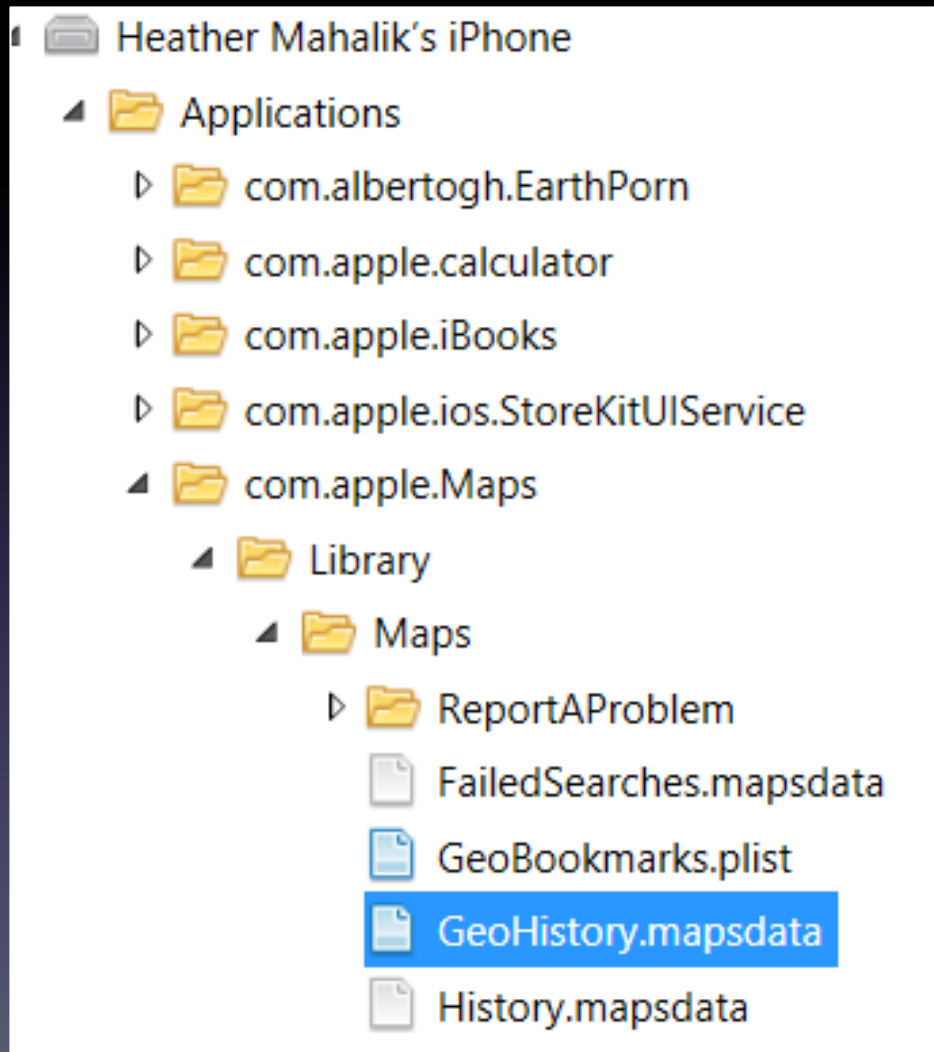
Can the Tool do That?



Oh Evidence, Where are You?

- Call Logs
 - Library/CallHistory/call_history.db
 - Library/CallHistory/callhistory.storedata (iOS 8 & 9)
- Google Maps
 - Library/Maps/History.mapsdata
 - Library/Maps/GeoHistory.mapsdata (iOS 8 & 9)

What's Going on Here...

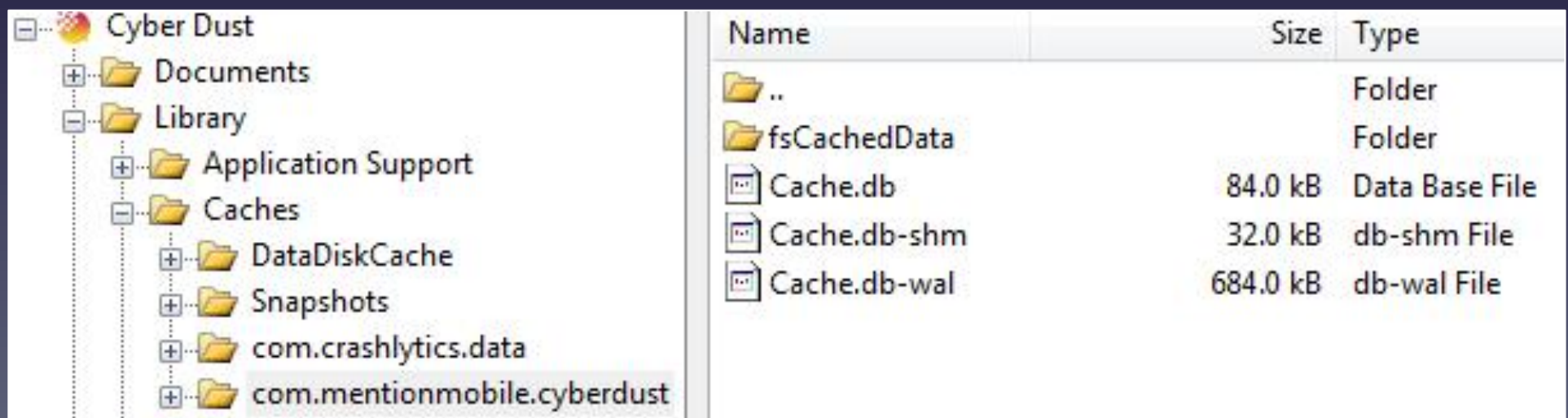


3rd Party Application Upgrades

- Encoding and Encryption changes
- Changes the file name containing the data
- Creates a new file for data storage
- Makes accessing the data more difficult
 - Sometimes...

Example: Cyberdust (1)

- Claims to remove all user data upon transmission/receipt
 - Never trust claims or your tool
 - Manually 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: Cyberdust (2)

```
Cache.db-wal - Notepad
File Edit Format View Help

+ pès{"result":{"chatRoomContainer":{"account":
{"id":"545ce910e4b0994d3e7aa237","verified":false,"uniqueHash":"545ce910e4b0994d3e7aa237","us
erName":"", "emailAddress":"", "hashedPassword":"EgJr3md07L", "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,,`| d%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":"VjJoaGRDZHpJSFZ3SUCxNUIHsnZlVDg9", "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 | pès{"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?

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 carving 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...)

References, Sources and Suggested Reading

- FOR585 Advanced Smartphone Forensics
- Practical Mobile Forensics
- <http://smarterforensics.com>
- <https://andriller.com/>
- <http://az4n6.blogspot.com/p/downloads.html>
- <http://cheeky4n6monkey.blogspot.com/>

Upcoming Courses

FOR585 Advanced Smartphone Forensics Course Available At:

**Chantilly, VA w/ Heather Mahalik – Dec
10 times in 2016!**

OnDemand – Anytime you want!

***FOR408 – vLive – Learn in your PJs with a beer!**



Questions?

Heather Mahalik

heather@smarterforensics.com

Twitter: @HeatherMahalik

www.smarterforensics.com

Heather.mahalik@oceansedgeinc.com

Copyright ©2015 Heather Mahalik, All
Rights Reserved