



Phoning it in: Heather talks about Smartphone Forensics Heather Mahalik

Copyright ©2018 Heather Mahalik, All Rights Reserved

About me...

- Director, Forensic Eng. at ManTech CARD
- SANS Senior Instructor
- Involved with InfoSec/Forensics for 16 years
- Co-author of FOR585
- Instructor of FOR585 and FOR500
- Co-Author of Practical Mobile Forensics (1st and 2nd Editions)
- Mom and a wife
- Dog, horse, wine and bourbon lover 😊

DOIN' A SELFIE?

**LOL NAH JUST TRYING
TO UNLOCK MY IPHONE**



What's happening in smartphone security

- Full disk encryption readily available
 - More people are using it
 - Some devices require it & others don't ask
 - Hurts acquisition?
- Application security
 - How secure is it?
- Tools are failing us
- Cloud is stealing all the good stuff!!!

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!!!**

Acquisition



Copyright ©2015 Heather Mahalik, All Rights Reserved

Application “Protection”

Transforming/converting data into code

Encoding Schemes

ASCII

Unicode

UTF-8

Base64

Encryption Algorithms

AES

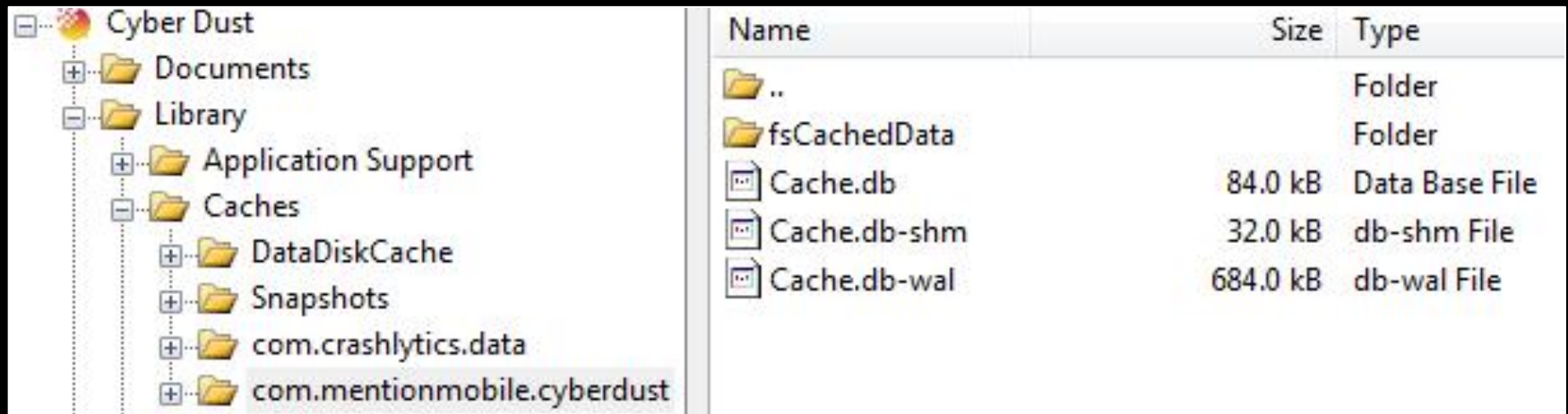
Blowfish

Twofish

Serpent

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

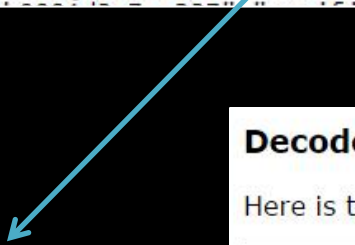


Name	Size	Type
..		Folder
fsCachedData		Folder
Cache.db	84.0 kB	Data Base File
Cache.db-shm	32.0 kB	db-shm File
Cache.db-wal	684.0 kB	db-wal File

Example: Cyber Dust (2)

- Messages are encoded twice using Base64

```
Cache.db-wal - Notepad
File Edit Format View Help
+ qe{"result":{"chatRoomContainer":{"account":
{"id":"545ce910e4b0994d3e7aa237","verified":false,"uniqueHash":",545ce910e4b0994d3e7aa237","us
erName":",.com","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":
```

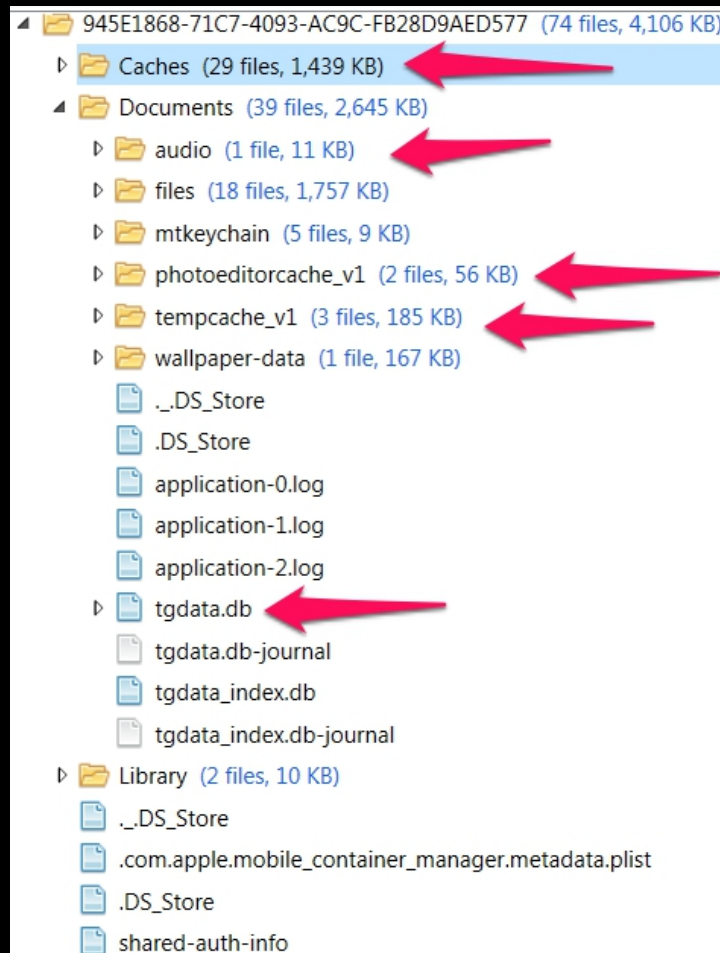


Decoded Output
Here is the decoded output of your Base 64 input:
V2hhdCdzIHVwIG15IGJveT8=

Decoded Output
Here is the decoded output of your Base 64 input:
What's up my boy?

VjJoaGRDZHpJSFZ3SUCxNUlHSnZlVDg9

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
317	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



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!



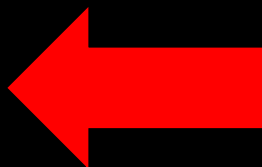
Example: Call Logs (1)

Magnet
IEF/AXIOM



Mobile	
Calendar Events	157
iOS Call Logs	222
iOS Contacts	507

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



UFED Physical
Analyzer

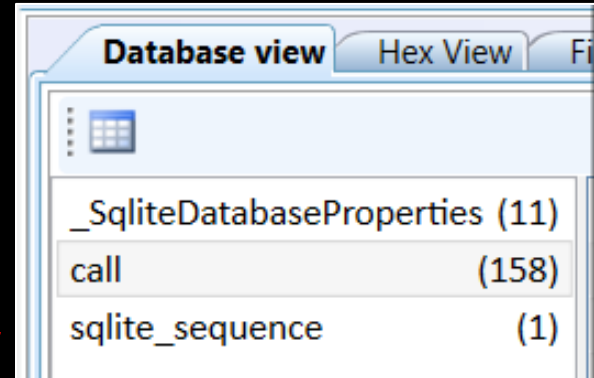
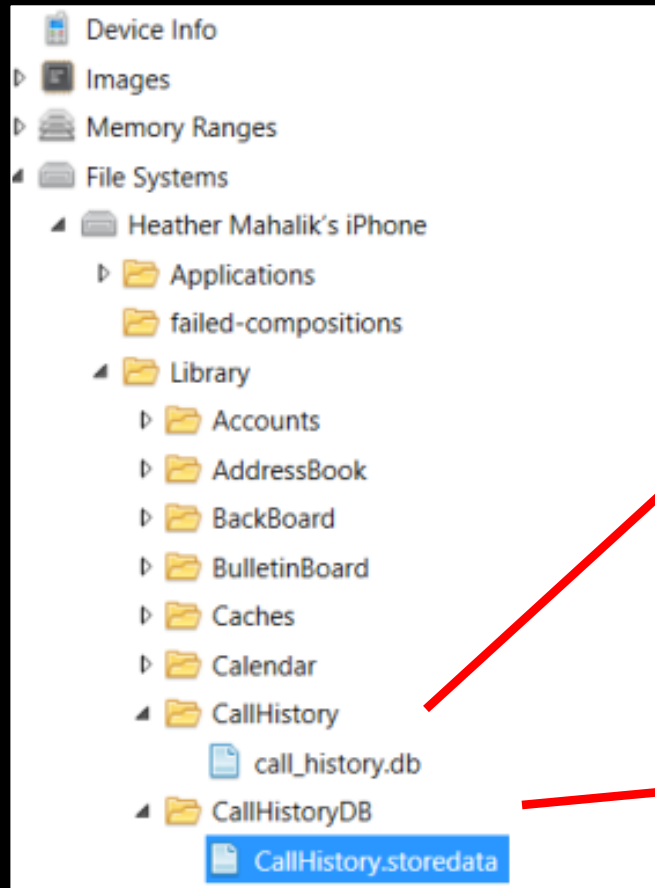
Call Logs

Library/CallHistory/call_history.db

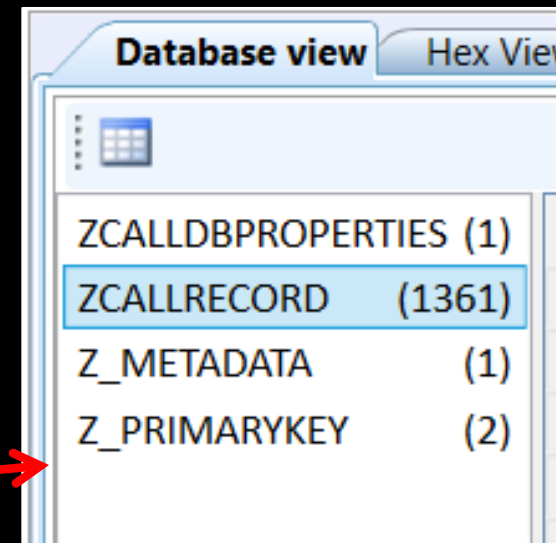
Library/CallHistory/callhistory.storedata (iOS 8,9 & 10)

Example: Call Logs (2)

Call logs



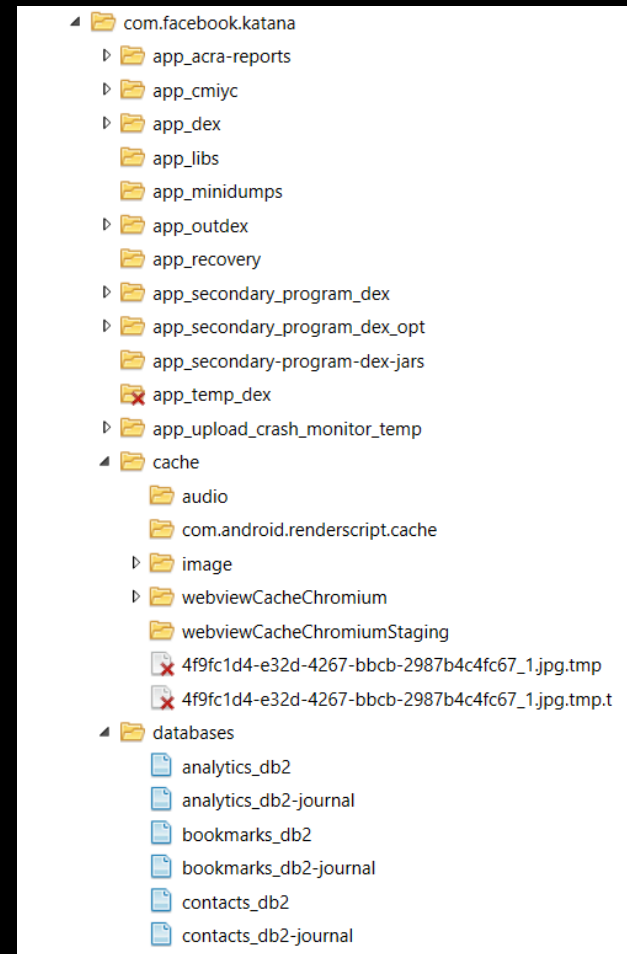
iOS 7



iOS 8-11

Wait...my phone was where?


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



But it was really here?

- 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"><plist 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>.
```

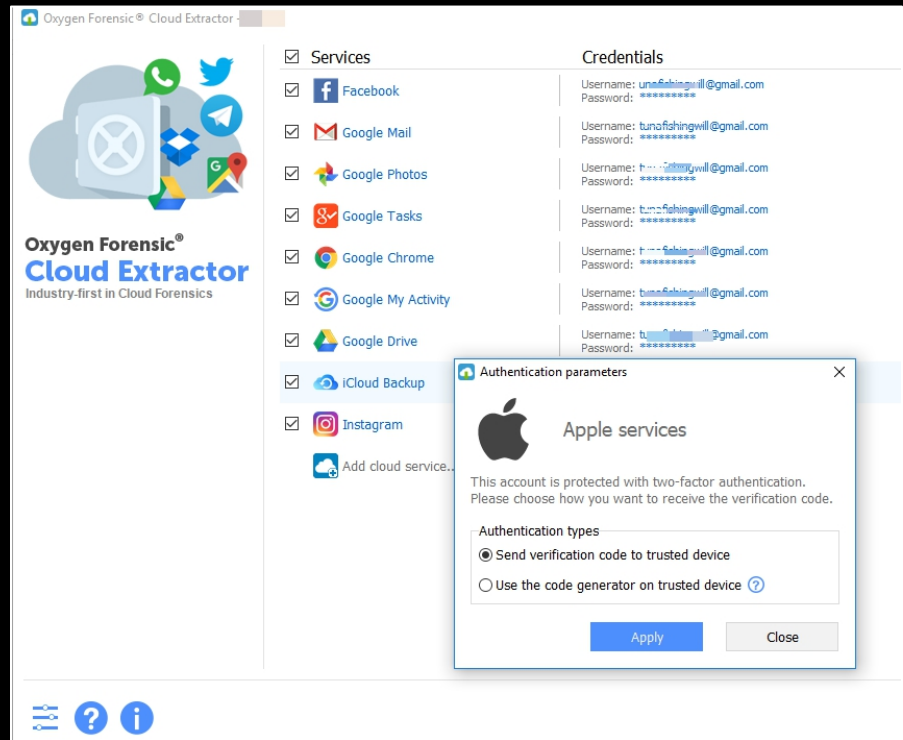
The Clouds have opened...



Copyright ©2015 Heather Mahalik, All
Rights Reserved

Cloud Extraction Techniques

- Many tools support cloud extraction
- Know which each are good at and select accordingly
- Multiple pulls may force the user to reset their passcode for iCloud



Elcomsoft Cloud eXplorer

Download snapshot ?

Select data categories to download

- User Info
- Dashboard
- Chats
- Contacts
- Google Keep

- Chrome
- Calendars
- Locations
- Media (0 files)
- History

- Calls
- Wi-Fi
- Mail (25379 mails)
[Add date filter](#)
- Messages

[Check All](#) [Uncheck All](#)

For accounts with 2FA, if the Dashboard category is selected, you will be required to enter the secure code or backup code once more.

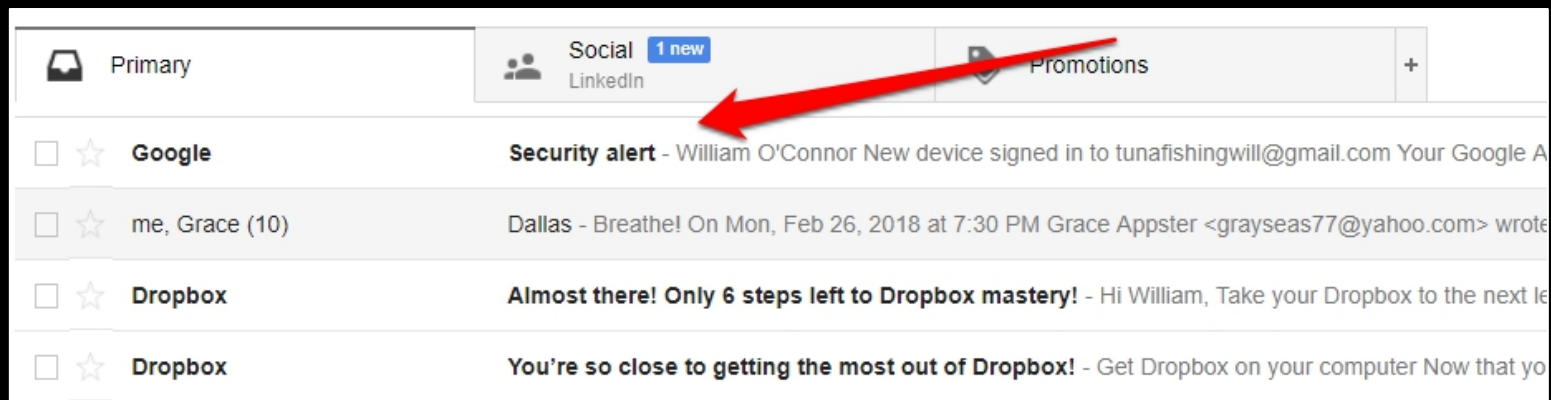
Cancel Download

Passwords Export... ▲

Date created (UTC) ▼	URL	User name	Password	Times used
2018-01-03 14:53:34	https://www.exciations.com/	nmanaik@gmail.com	*****	
2018-01-03 04:01:01	https://www.blackriflecoffee.com/	heather@smarterforensics.com	*****	1
2018-01-02 20:48:05	https://profile.oracle.com/	heather@smarterforensics.com	*****	5
2017-12-28 17:08:51	https://accounts.silentcircle.com/	hmahalik	*****	9
2017-12-27 19:36:59	https://mvspendingaccount.wageworks.com/		*****	5
2017-12-21 14:10:21	https://www.southwest.com/	hmahalik	*****	1
2017-12-12 17:59:12	https://www.sephora.com/	hmahalik@gmail.com	*****	0
2017-12-08 16:16:37	https://login.verizonwireless.com/		*****	2

Warning: The User Will Be Alerted!

- The user will receive a notification stating that a new device signed into their Google account
- **This is not recommended if you are conducting covert operations as you have to assume the user will know you were there!**



Elcomsoft Cloud eXplorer – NOT just for Android

The screenshot displays the Elcomsoft Cloud eXplorer dashboard for user hmahalik@gmail.com. The dashboard title is "Dashboard". A search bar is located below the header. A navigation bar contains several icons, with the Android icon highlighted by a red square. Below the navigation bar, the "Chrome Sync" section is expanded, showing a list of sync data: Bookmarks: 77, Last Synced: 25.02.2018 22:14:11, Passwords: 490, Extensions: 5, and Other: 2560. To the right, a user profile card for Heather Mahalik is shown, including her email, creation date (26.02.2018 22:20:33), and size (2.25 GB). Below the profile card is a grid of application categories with their respective counts: Contacts (3613), Calendars (1642), Calls (0), Chrome (2648), Dashboard (6), Locations (1141), Mail (25375), Media (3670), Messages (0), Google Keep (0), History (48493), Wi-Fi (0), Chats (1537), and User Info (1). Buttons for "Create report..." and "Export data..." are visible next to the user profile card.

hmahalik@gmail.com

Dashboard

Chrome Sync

Chrome Sync

Bookmarks: 77
Last Synced: 25.02.2018 22:14:11
Passwords: 490
Extensions: 5
Other: 2560

User: Heather Mahalik
Email: [redacted]
Created: 26.02.2018 22:20:33
Size: 2.25 GB

Create report...
Export data...

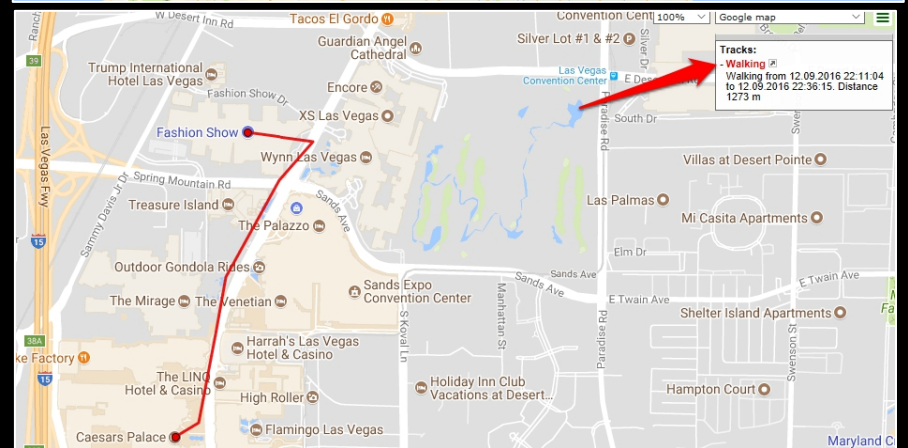
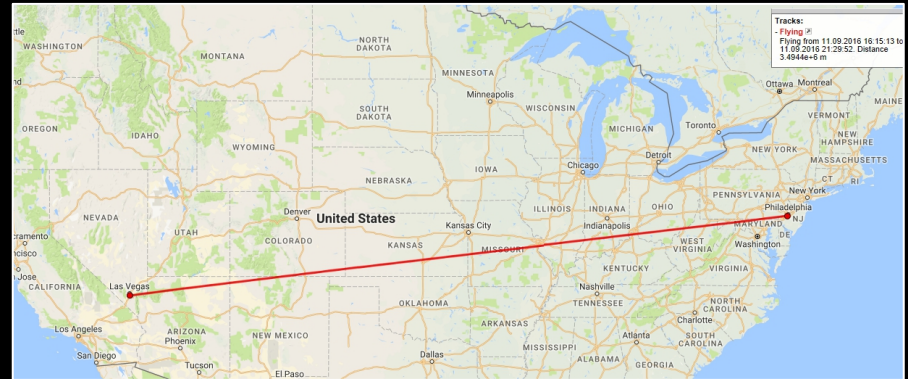
Contacts (3613) Calendars (1642) Calls (0) Chrome (2648) Dashboard (6)
Locations (1141) Mail (25375) Media (3670) Messages (0) Google Keep (0)
History (48493) Wi-Fi (0) Chats (1537) User Info (1)

Google Cloud Artifacts

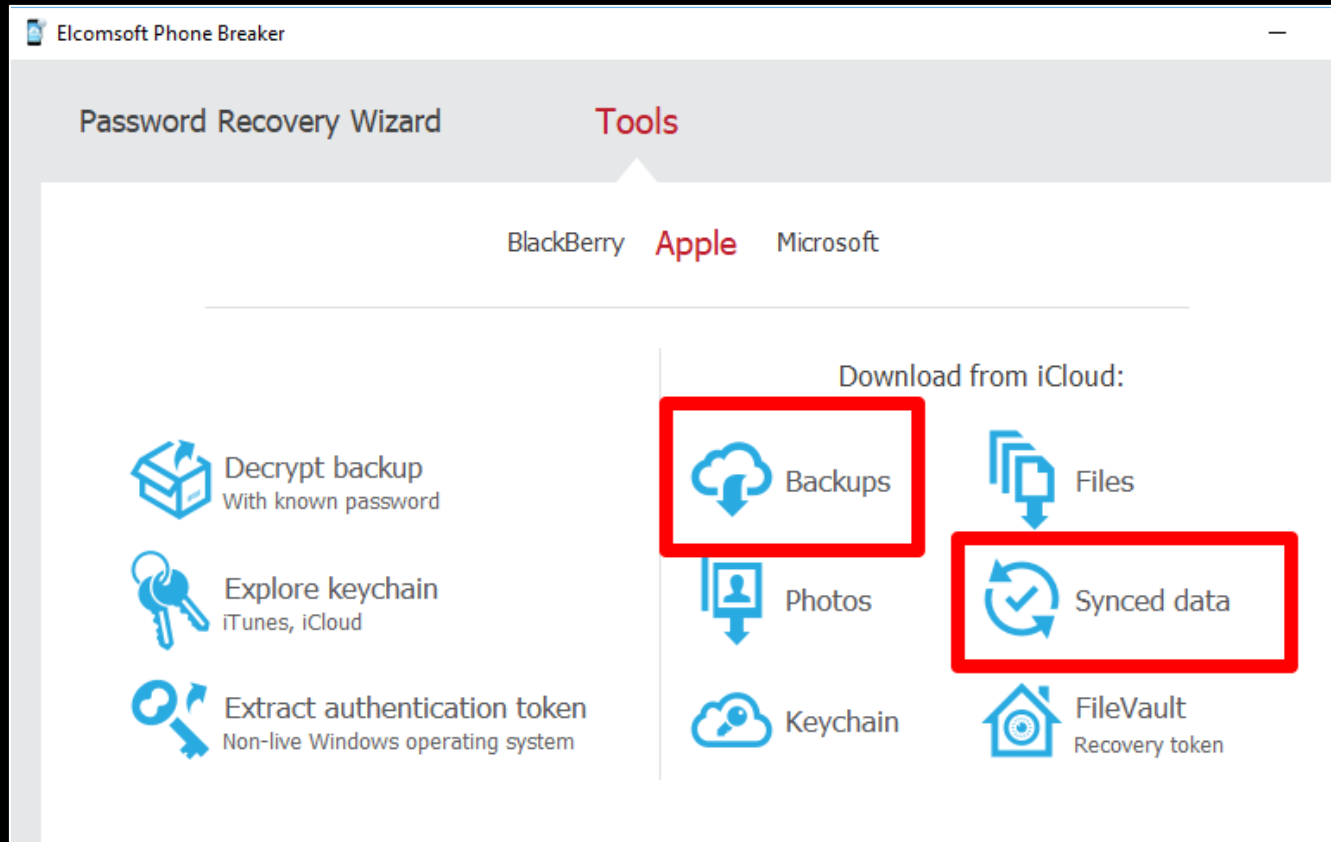
Routes Show track Export...

Locations: 559
 Most recent: 04.10.2016 12:29:15 [40.0671110-75.6434110](#)
 Oldest: 19.05.2016 11:02:02 [37.3853390-121.9970750](#)

Start Point	Finish Date	Finish Point	Show Track	Type	Distance, km
36.1161690-115.1...	14.09.2016 10:03:41 (UTC -4)	36.1161690-115.1...		Walking	3.007
36.1167110-115.1...	13.09.2016 00:16:46 (UTC -4)	36.1161690-115.1...		Moving	1.627
36.1161690-115.1...	12.09.2016 22:36:15 (UTC -4)	36.1274110-115.1...		Walking	1.273
36.1161690-115.1...	12.09.2016 21:15:11 (UTC -4)	36.1161690-115.1...		Walking	0.698
36.0832330-115.1...	11.09.2016 22:31:35 (UTC -4)	36.1161690-115.1...		Driving	9.933
39.8743960-75.24...	11.09.2016 21:29:52 (UTC -4)	36.0840000-115.1...		Flying	3494.4
40.0909060-75.64...	11.09.2016 14:50:47 (UTC -4)	39.8743960-75.24...		Driving	53.843
40.0502530-75.66...	11.09.2016 12:04:08 (UTC -4)	40.0909060-75.64...		Driving	6.206




Accessing iCloud Data (1)



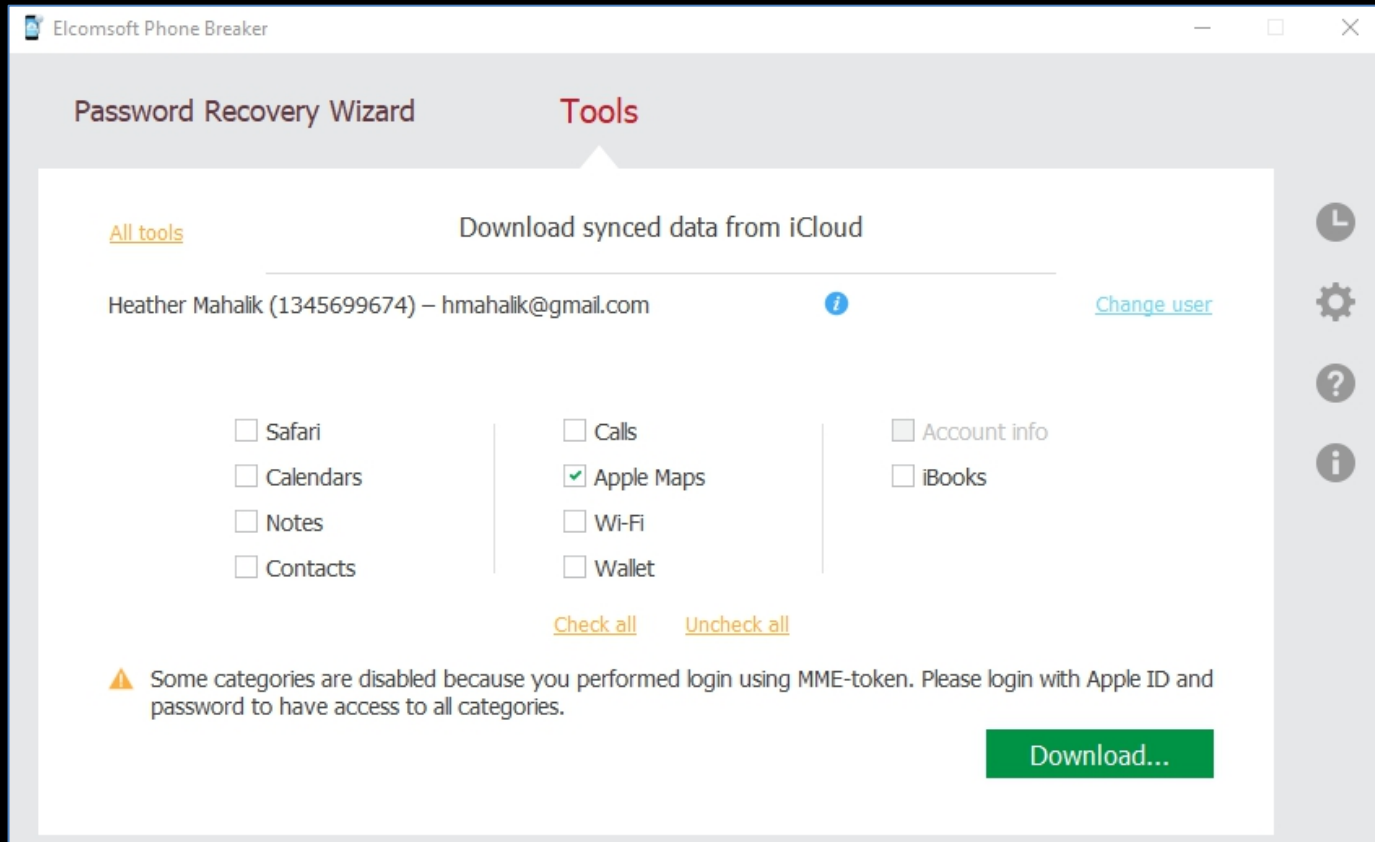
Accessing iCloud Backup Data (2)

Download backup from iCloud

Apple ID (example@example.com)

Password 

Reality: Apple Maps



Don't fear the unknown

- Create your own test data
 - I wish we could do it all for you, but I run out of time
- Keep digging when the results don't make sense
- Take training to learn the proper methods

About 585...

- Course launched in 2014
- GASF Cert – Vendor neutral available to everyone
- Co-authored by Heather Mahalik, Lee Crognale and Cindy Murphy
- Addresses the hardest to tackle topics (Encryption, Parsing, Query drafting, decompiling malware, etc.)
- Covers iOS, Android, 3rd Party Apps, Malware, BlackBerry 10, Windows Phone and more
- Includes 19 hands-on labs + 1 capstone challenge of current smart devices (bonus take home case + 6 bonus labs)
- Is vendor NEUTRAL – We teach you the best methods, not how to use commercial tools

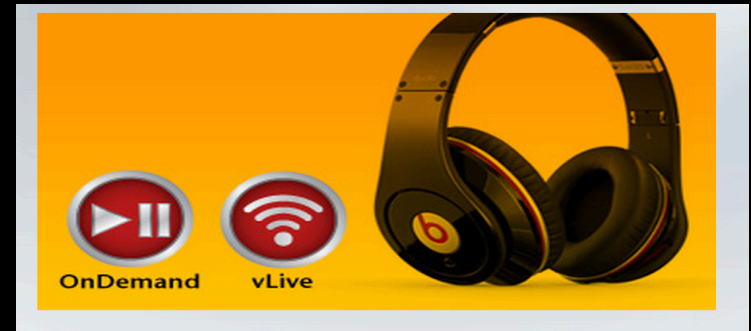
References, Sources and Suggested Reading

- <https://github.com/hmahalik>
- FOR585 Advanced Smartphone Forensics
- https://github.com/threeplanetssoftware/sqlite_miner
- mac4n6.com/blog
- smarterforensics.com/blog
 - First the Grinch Now the Easter Bunny
 - How the Grinch Stole Apple Maps
 - Smartphone Acquisition: Adapt, Adjust and Get Smarter!

How To Smash A Mobile Phone



With A Sledge Hammer



FOR585 Advanced Smartphone Forensics Course Available At:

FOR585.com/course

July: SANSFIRE, DC – Heather – SOLD OUT – SIMULCAST!

August: NYC

Sept: Las Vegas - SIMULCAST Available

Oct: Denver, CO

Nov: Miami, Austin & Stockholm

Dec: DC & Saudi Arabia - - SIMULCAST Available

OnDemand ANYTIME!

Heather Mahalik

heather@smarterforensics.com

@HeatherMahalik

Blog: for585.com/blog

QUESTIONS?

