SANS DFIR Webcast Series

DIGITAL FORENSICS & INCIDENT RESPONSE

THE WEBCAST WILL BEGIN SHORTLY

To Trust or Not To Trust:

The Relationship Between You and Your Mobile Forensics Tool

Heather Mahalik @HeatherMahalik

Take FOR585: Advanced Smartphone Forensics at these training events:

SANSFIRE

Washington, DC | Jun 13-18

Featuring: Heather Mahalik

sans.org/sansfire

DFIR Summit

Austin, TX | Jun 25-30

Featuring: Cindy Murphy

sans.org/dfirsummit

TO TRUST OR NOT TO TRUST: THE RELATIONSHIP BETWEEN YOU AND YOUR MOBILE FORENSIC TOOLS

HEATHER MAHALIK

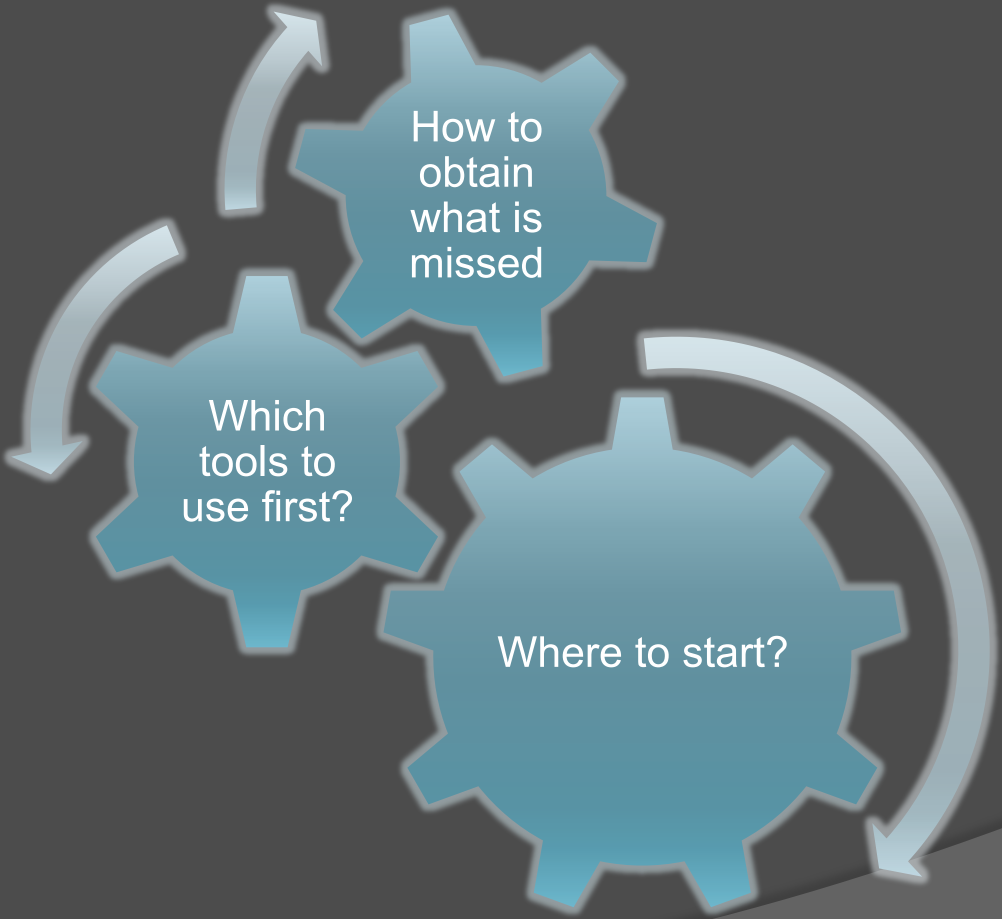
About me…

- Principal Forensic Scientist at Oceans Edge, Inc.
- SANS Senior Instructor
- Involved with Infosec/Forensics for 13+ years
- Co-author of FOR585 and FOR518
- Instructor of FOR585 and FOR408
- Co-Author of Practical Mobile Forensics
- Mom and a wife
- Dog, horse and wine lover ☺

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

Consider your actions

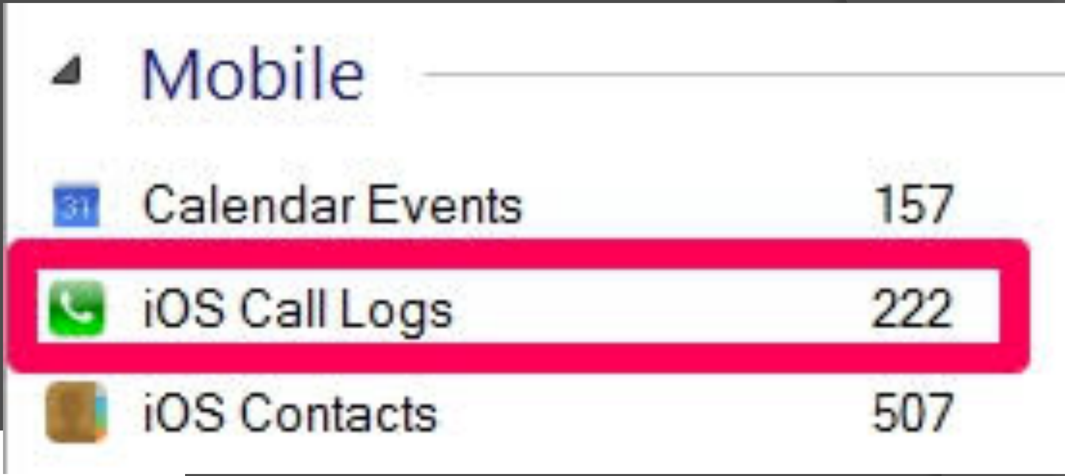


Why the tools fail…

- 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!

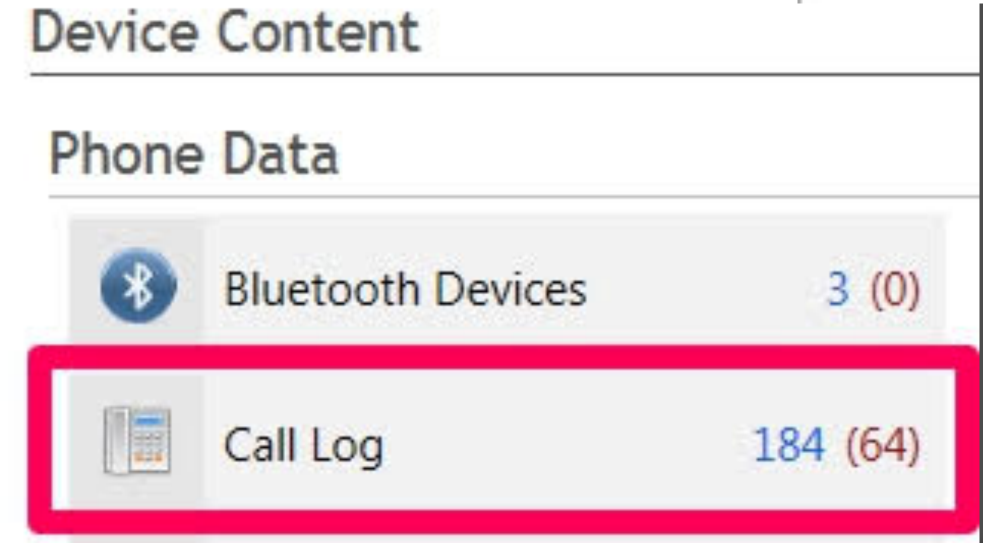
Example 1: Call Logs

Magnet IEF



Mobile

Calendar Events	157
iOS Call Logs	222
iOS Contacts	507



Device Content

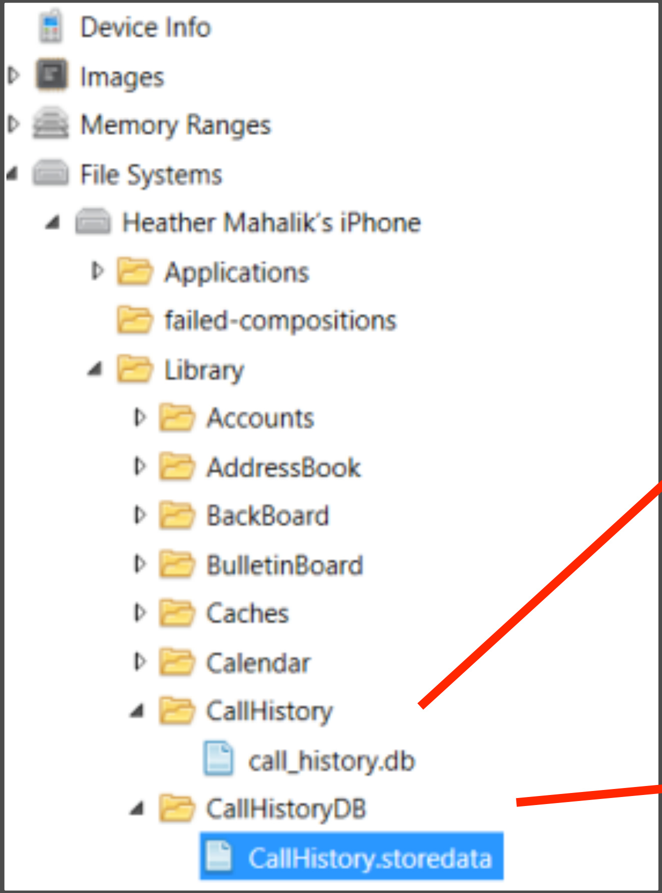
Phone Data

Bluetooth Devices	3 (0)
Call Log	184 (64)

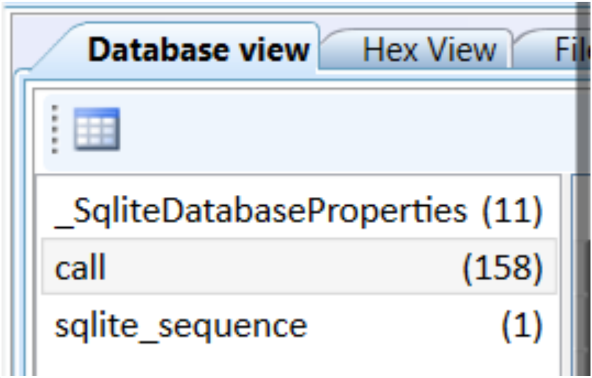
UFED Physical Analyzer

Example 1: Call Logs

Call logs

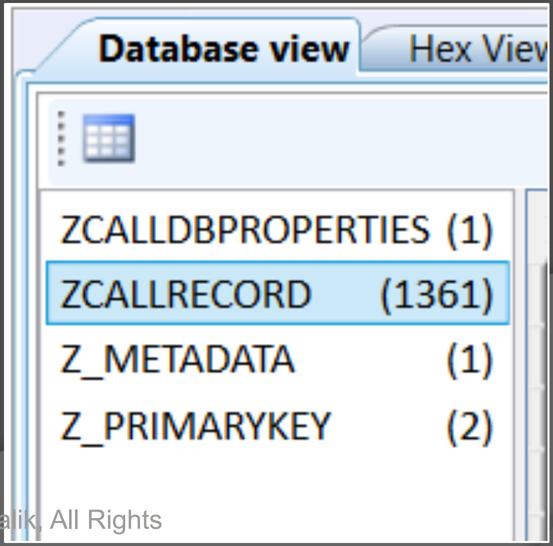


- Device Info
- Images
- Memory Ranges
- File Systems
  - Heather Mahalik's iPhone
    - Applications
    - failed-compositions
    - Library
      - Accounts
      - AddressBook
      - BackBoard
      - BulletinBoard
      - Caches
      - Calendar
      - CallHistory
        - call_history.db
      - CallHistoryDB
        - CallHistory.storedata



_SqliteDatabaseProperties	(11)
call	(158)
sqlite_sequence	(1)

iOS 7



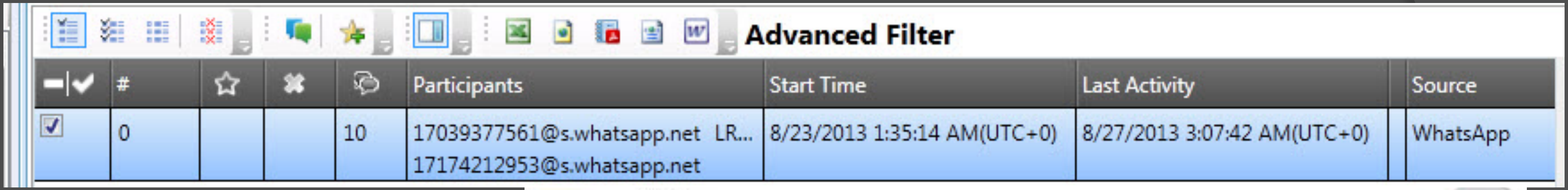
ZCALLDBPROPERTIES	(1)
ZCALLRECORD	(1361)
Z_METADATA	(1)
Z_PRIMARYKEY	(2)

iOS 8

Example 2: WhatsApp

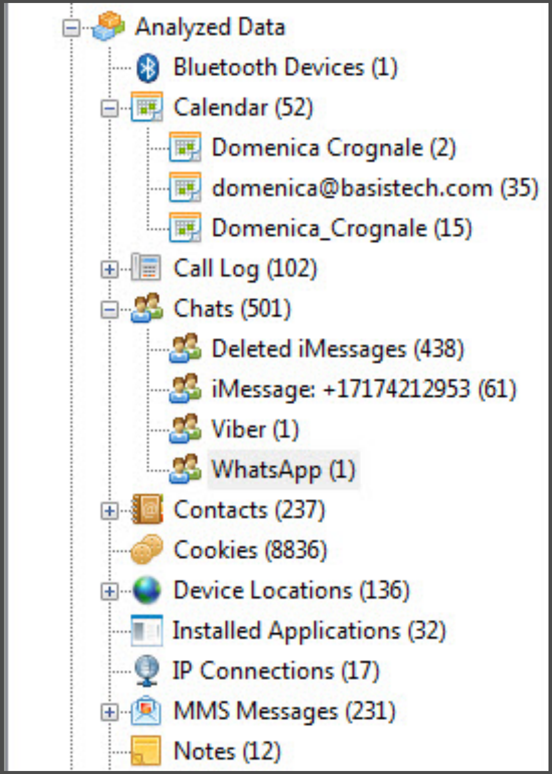
- Yes, I know that they are claiming encryption now
  - Stay tuned…
  - I never trust developer claims
- I love to prove them wrong
- FOR585 teaches you how to do this for almost every app

WhatsApp Chat – Physical Analyzer

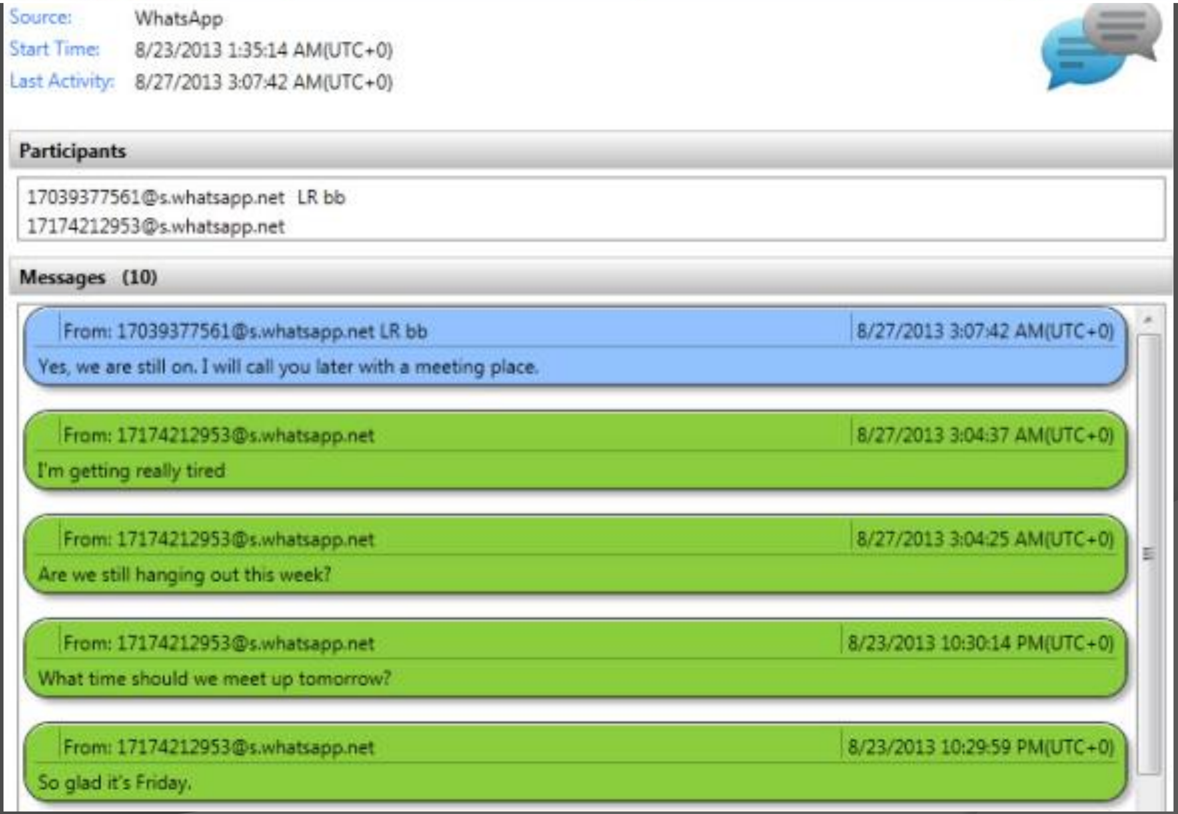


Advanced Filter

▬|✓	#	☆	✖	💬	Participants	Start Time	Last Activity	Source
☑	0			10	17039377561@s.whatsapp.net LR... 17174212953@s.whatsapp.net	8/23/2013 1:35:14 AM(UTC+0)	8/27/2013 3:07:42 AM(UTC+0)	WhatsApp



- Analyzed Data
  - Bluetooth Devices (1)
  - Calendar (52)
    - Domenica Crognale (2)
    - domenica@basistech.com (35)
    - Domenica_Crognale (15)
  - Call Log (102)
  - Chats (501)
    - Deleted iMessages (438)
    - iMessage: +17174212953 (61)
    - Viber (1)
    - WhatsApp (1)
  - Contacts (237)
  - Cookies (8836)
  - Device Locations (136)
  - Installed Applications (32)
  - IP Connections (17)
  - MMS Messages (231)
  - Notes (12)



Source: WhatsApp
Start Time: 8/23/2013 1:35:14 AM(UTC+0)
Last Activity: 8/27/2013 3:07:42 AM(UTC+0)

Participants

17039377561@s.whatsapp.net LR bb
17174212953@s.whatsapp.net

Messages (10)

From: 17039377561@s.whatsapp.net LR bb — 8/27/2013 3:07:42 AM(UTC+0)
Yes, we are still on. I will call you later with a meeting place.

From: 17174212953@s.whatsapp.net — 8/27/2013 3:04:37 AM(UTC+0)
I'm getting really tired

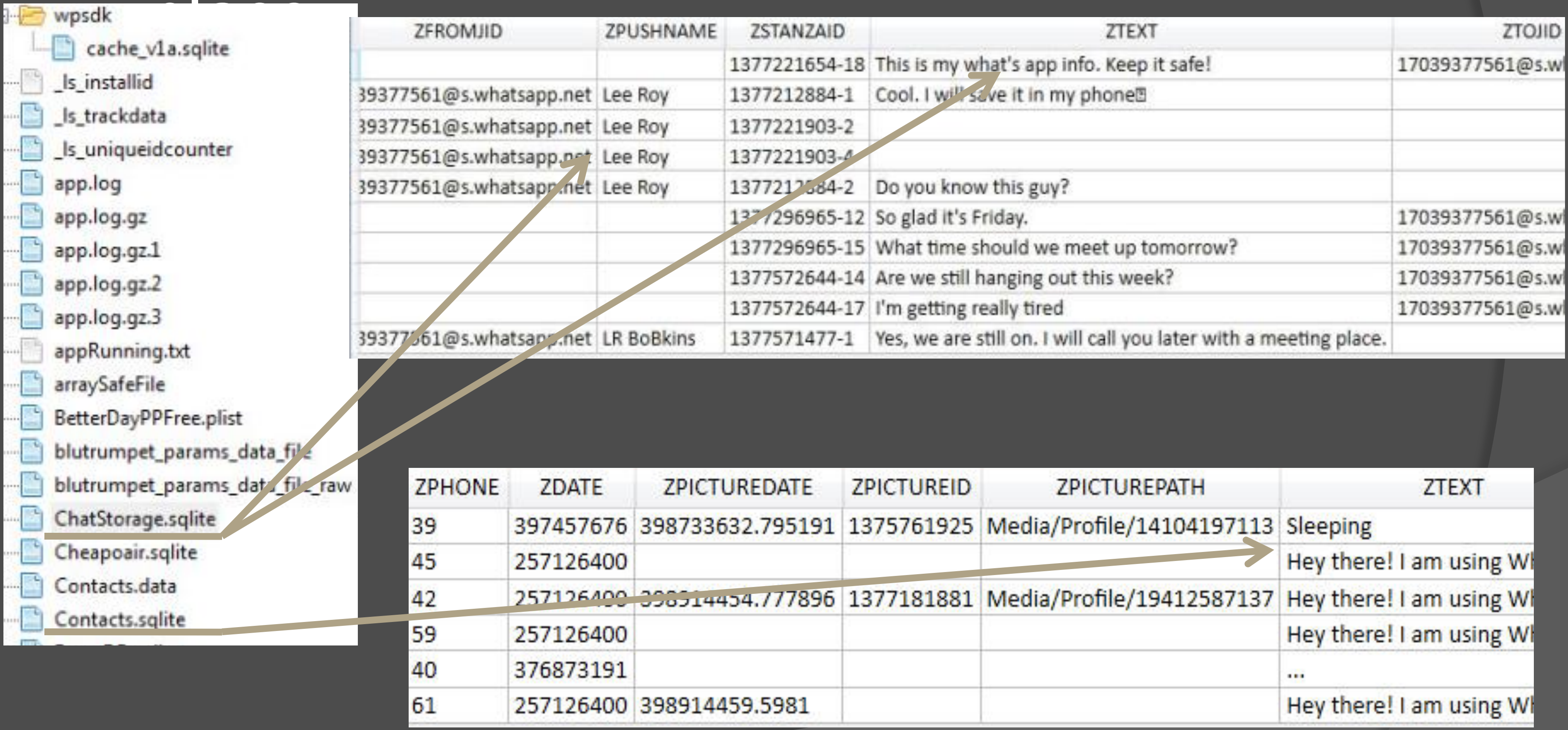
From: 17174212953@s.whatsapp.net — 8/27/2013 3:04:25 AM(UTC+0)
Are we still hanging out this week?

From: 17174212953@s.whatsapp.net — 8/23/2013 10:30:14 PM(UTC+0)
What time should we meet up tomorrow?

From: 17174212953@s.whatsapp.net — 8/23/2013 10:29:59 PM(UTC+0)
So glad it's Friday.

WhatsApp Chat – Manual Examination

- WhatsApp stores data in more than one place

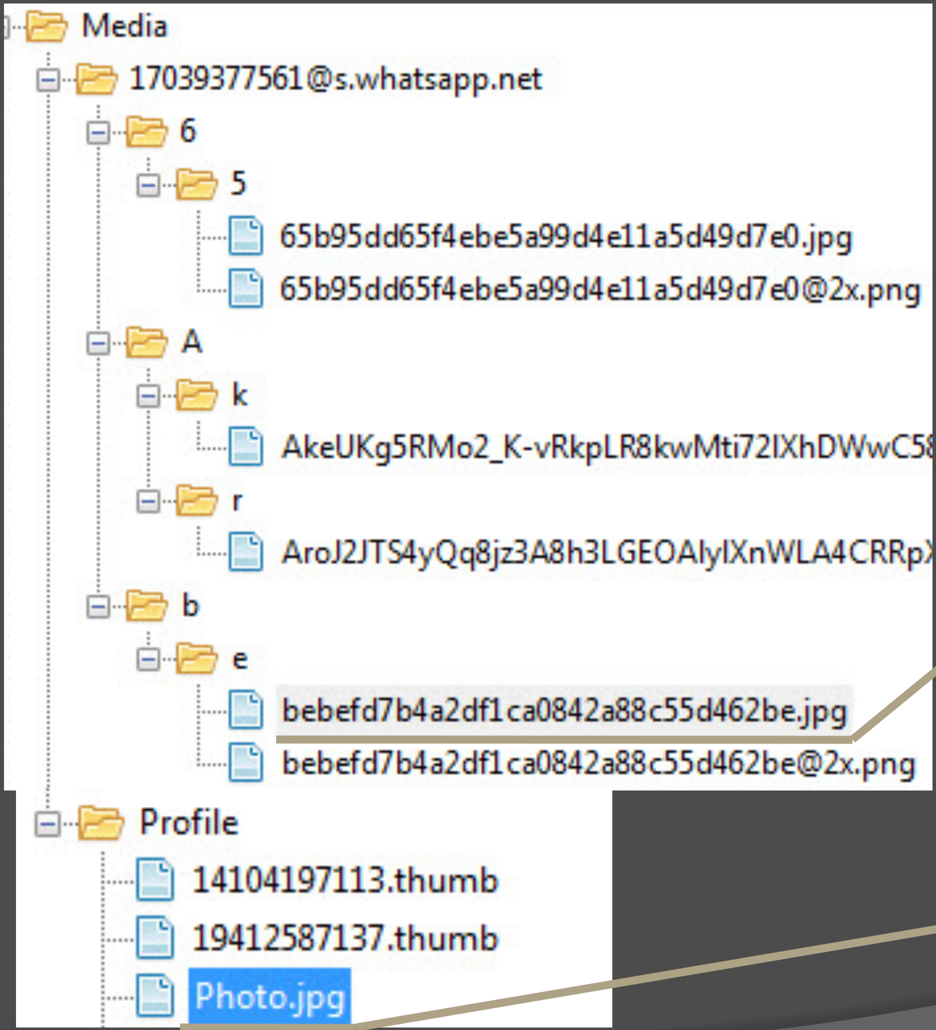


- wpsdk
  - cache_v1a.sqlite
- _ls_installid
- _ls_trackdata
- _ls_uniqueidcounter
- app.log
- app.log.gz
- app.log.gz.1
- app.log.gz.2
- app.log.gz.3
- appRunning.txt
- arraySafeFile
- BetterDayPPFree.plist
- blutrumpet_params_data_file
- blutrumpet_params_data_file_raw
- ChatStorage.sqlite
- Cheapoair.sqlite
- Contacts.data
- Contacts.sqlite

ZFROMJID	ZPUSHNAME	ZSTANZAID	ZTEXT	ZTOJID
		1377221654-18	This is my what's app info. Keep it safe!	17039377561@s.w
39377561@s.whatsapp.net	Lee Roy	1377212884-1	Cool. I will save it in my phone	
39377561@s.whatsapp.net	Lee Roy	1377221903-2		
39377561@s.whatsapp.net	Lee Roy	1377221903-4		
39377561@s.whatsapp.net	Lee Roy	1377212884-2	Do you know this guy?	
		1377296965-12	So glad it's Friday.	17039377561@s.w
		1377296965-15	What time should we meet up tomorrow?	17039377561@s.w
		1377572644-14	Are we still hanging out this week?	17039377561@s.w
		1377572644-17	I'm getting really tired	17039377561@s.w
39377561@s.whatsapp.net	LR BoBkins	1377571477-1	Yes, we are still on. I will call you later with a meeting place.	

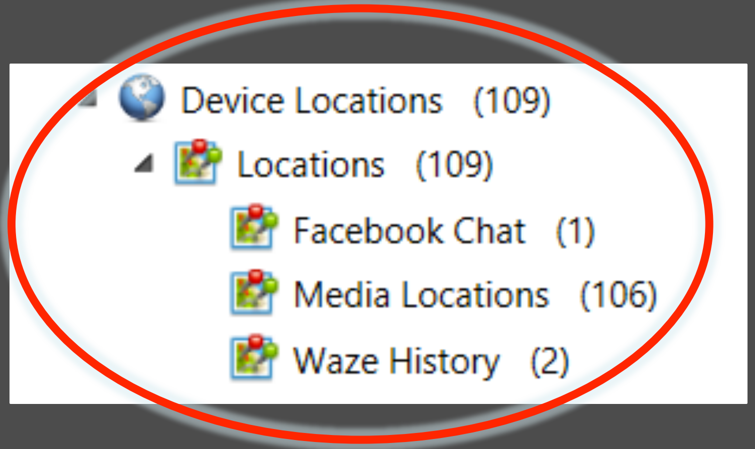
ZPHONE	ZDATE	ZPICTUREDATE	ZPICTUREID	ZPICTUREPATH	ZTEXT
39	397457676	398733632.795191	1375761925	Media/Profile/14104197113	Sleeping
45	257126400				Hey there! I am using Wh
42	257126400	398914454.777896	1377181881	Media/Profile/19412587137	Hey there! I am using Wh
59	257126400				Hey there! I am using Wh
40	376873191				...
61	257126400	398914459.5981			Hey there! I am using Wh

WhatsApp – Residual Artifacts

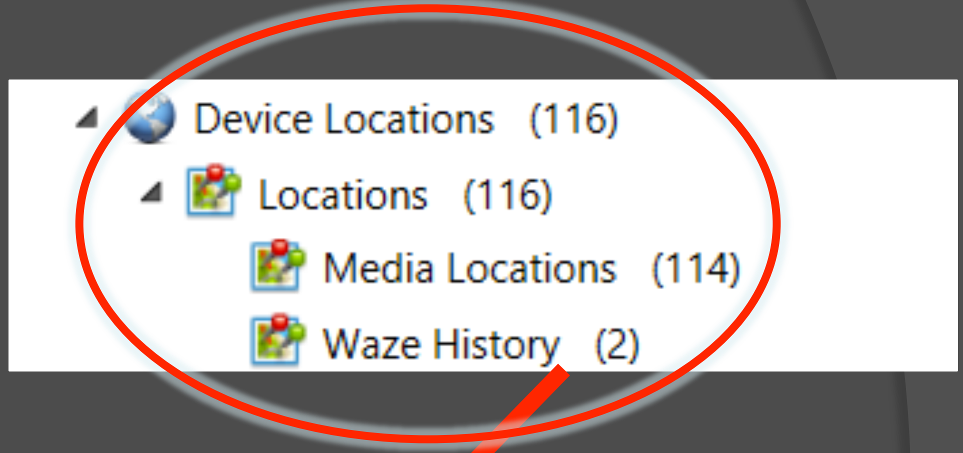


```
Media
  17039377561@s.whatsapp.net
    6
      5
        65b95dd65f4ebe5a99d4e11a5d49d7e0.jpg
        65b95dd65f4ebe5a99d4e11a5d49d7e0@2x.png
    A
      k
        AkeUKg5RMo2_K-vRkpLR8kwMti72IXhDWwC58
      r
        AroJ2JTS4yQq8jz3A8h3LGEOAlylXnWLA4CRRpX
    b
      e
        bebefd7b4a2df1ca0842a88c55d462be.jpg
        bebefd7b4a2df1ca0842a88c55d462be@2x.png
  Profile
    14104197113.thumb
    19412587137.thumb
    Photo.jpg
```

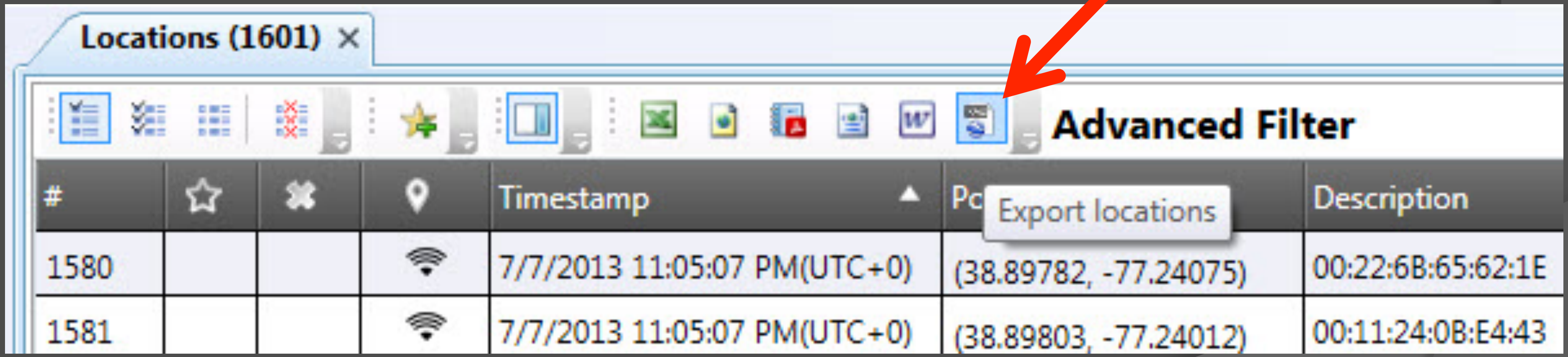
Example 3: Location Artifacts



- Device Locations (109)
  - Locations (109)
    - Facebook Chat (1)
    - Media Locations (106)
    - Waze History (2)



- Device Locations (116)
  - Locations (116)
    - Media Locations (114)
    - Waze History (2)

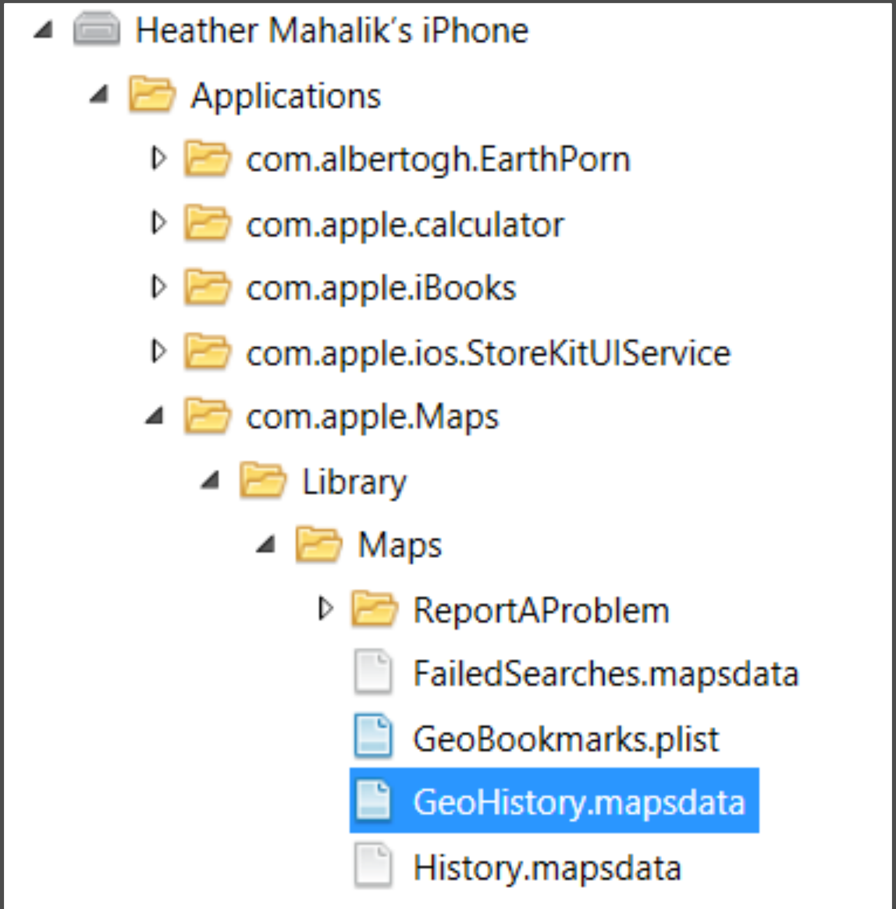


Locations (1601) ×

#	☆	✖	📍	Timestamp	Pc	Description
1580			📶	7/7/2013 11:05:07 PM(UTC+0)	(38.89782, -77.24075)	00:22:6B:65:62:1E
1581			📶	7/7/2013 11:05:07 PM(UTC+0)	(38.89803, -77.24012)	00:11:24:0B:E4:43

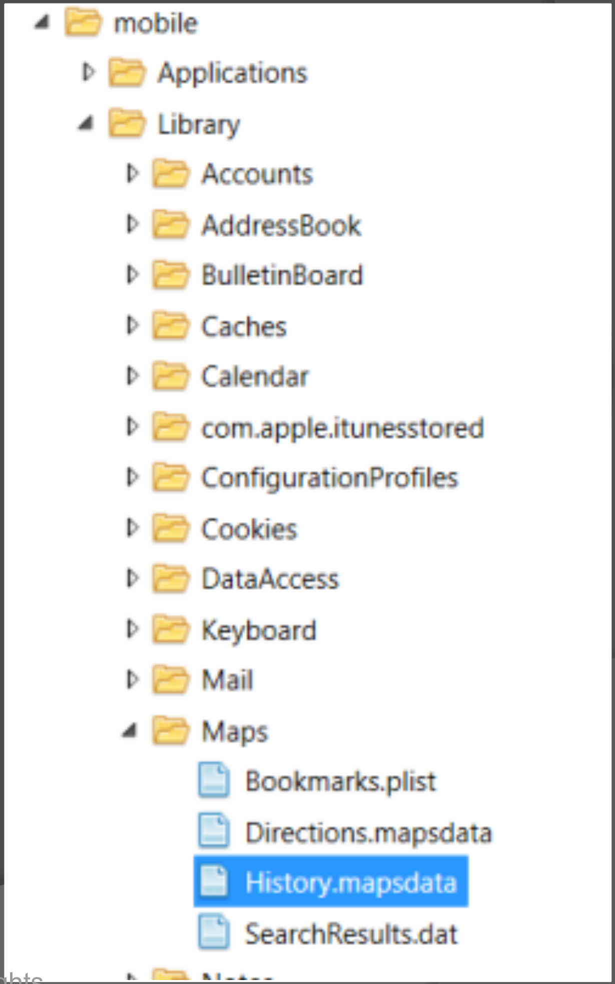
Why data is missed (1)

iOS 8 and iOS 9



```
Heather Mahalik's iPhone
  Applications
    com.albertogh.EarthPorn
    com.apple.calculator
    com.apple.iBooks
    com.apple.ios.StoreKitUIService
    com.apple.Maps
      Library
        Maps
          ReportAProblem
          FailedSearches.mapsdata
          GeoBookmarks.plist
          GeoHistory.mapsdata
          History.mapsdata
```

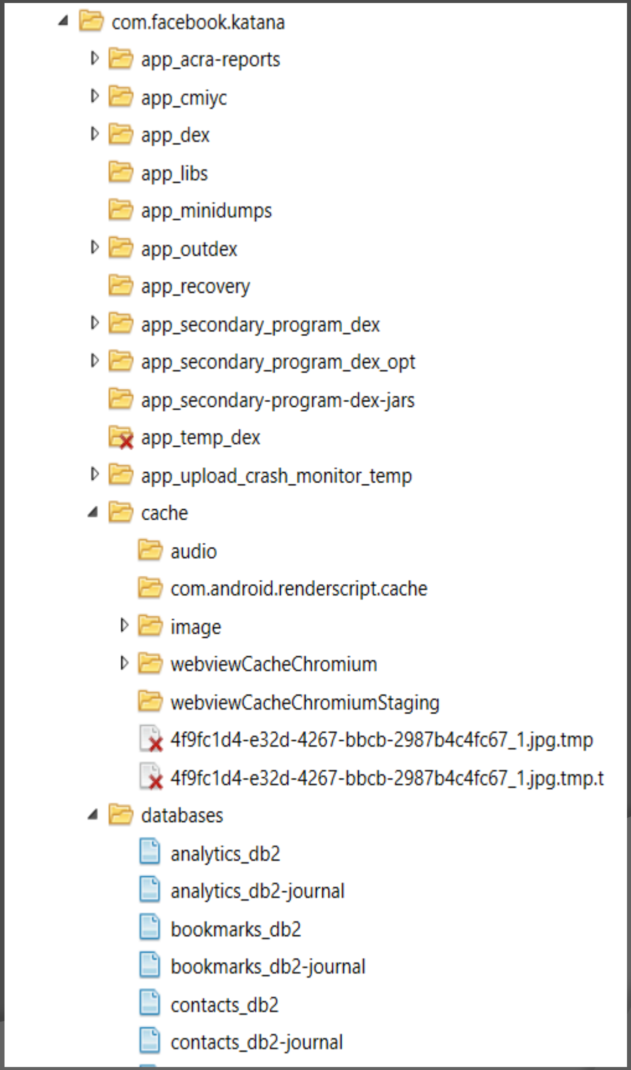
iOS 7



```
mobile
  Applications
  Library
    Accounts
    AddressBook
    BulletinBoard
    Caches
    Calendar
    com.apple.itunesstored
    ConfigurationProfiles
    Cookies
    DataAccess
    Keyboard
    Mail
    Maps
      Bookmarks.plist
      Directions.mapsdata
      History.mapsdata
      SearchResults.dat
```

Why data is missed (2)

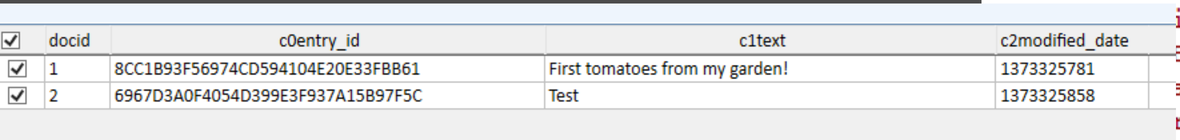
- Social media geo-tagging
  - Facebook
  - Google+
  - Twitter
  - Etc.
- Consider what traces are left behind when the user “checks-in” and tags a location



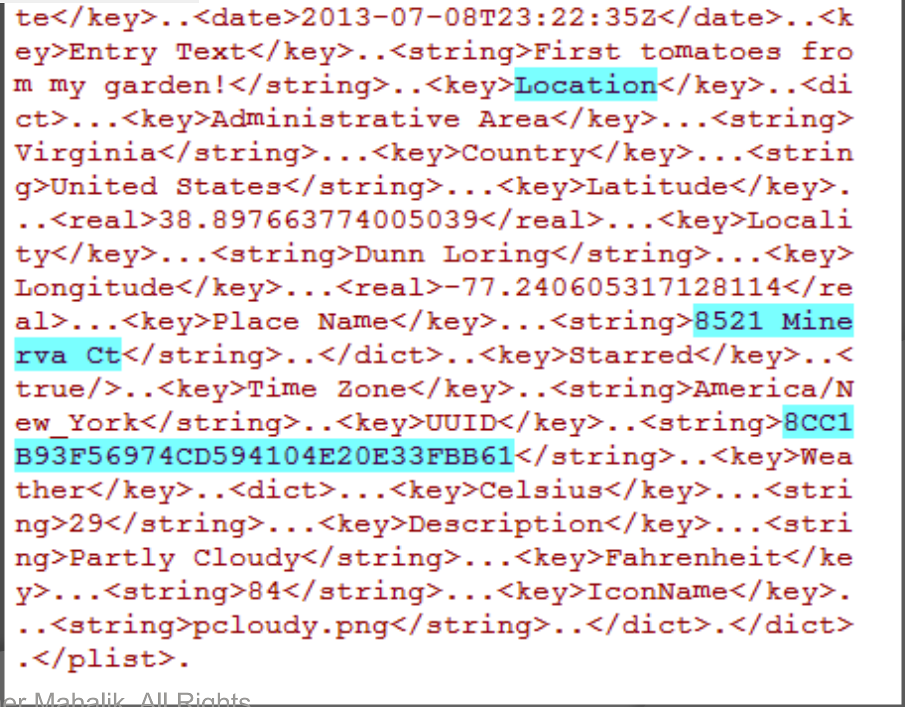
```
com.facebook.katana
    app_acra-reports
    app_cmiyc
    app_dex
    app_libs
    app_minidumps
    app_outdex
    app_recovery
    app_secondary_program_dex
    app_secondary_program_dex_opt
    app_secondary-program-dex-jars
    app_temp_dex
    app_upload_crash_monitor_temp
    cache
        audio
        com.android.renderscript.cache
        image
        webviewCacheChromium
        webviewCacheChromiumStaging
        4f9fc1d4-e32d-4267-bbcb-2987b4c4fc67_1.jpg.tmp
        4f9fc1d4-e32d-4267-bbcb-2987b4c4fc67_1.jpg.tmp.t
    databases
        analytics_db2
        analytics_db2-journal
        bookmarks_db2
        bookmarks_db2-journal
        contacts_db2
        contacts_db2-journal
```

How much does your phone know?

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



☑	docid	c0entry_id	c1text	c2modified_date
☑	1	8CC1B93F56974CD594104E20E33FBB61	First tomatoes from my garden!	1373325781
☑	2	6967D3A0F4054D399E3F937A15B97F5C	Test	1373325858

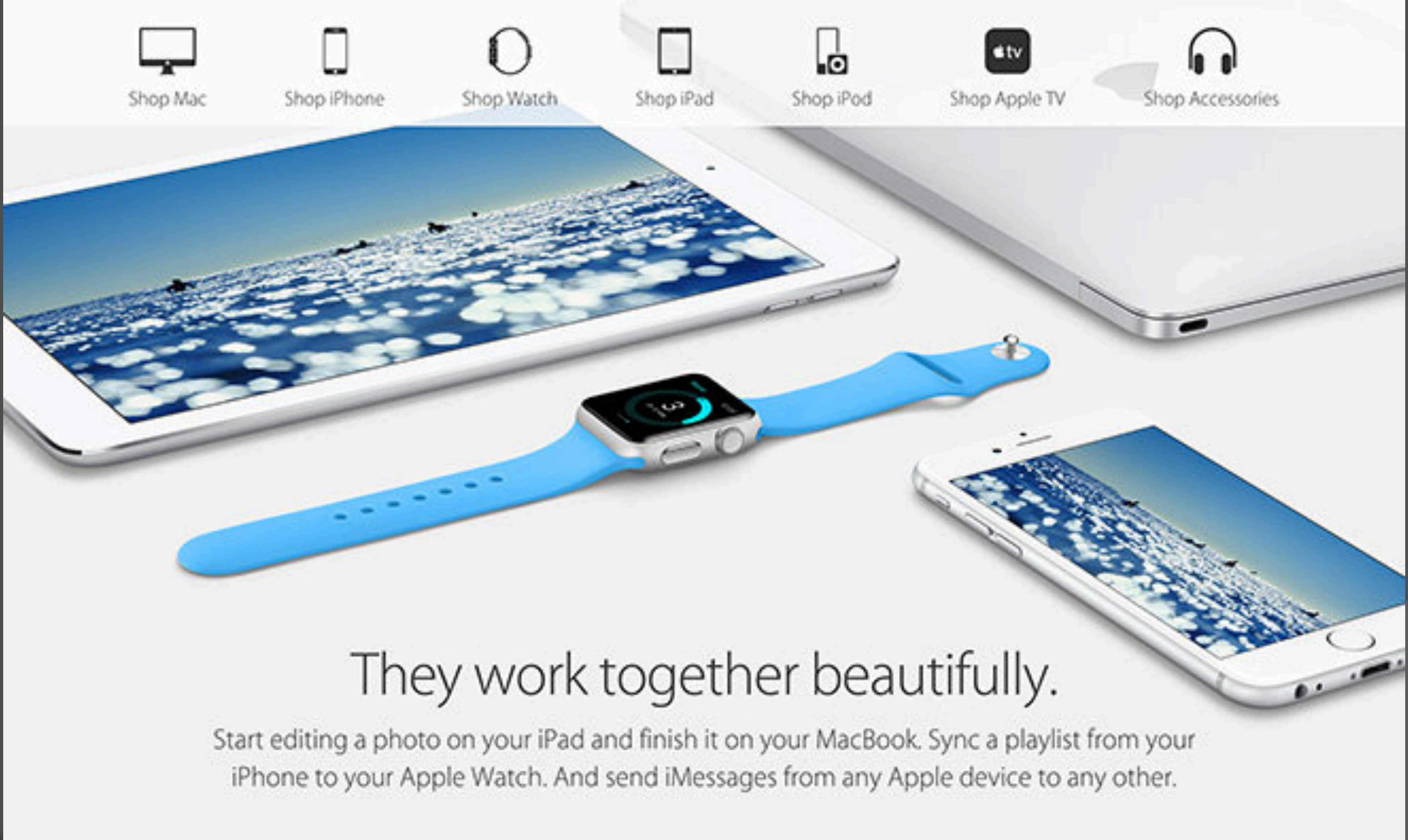


```
ion="1.0" encoding="UTF-8"?>.<!DOCTYP
BLIC "-//Apple//DTD PLIST 1.0//EN" "h
apple.com/DTDs/PropertyList-1.0.dtd">
rsion="1.0">.<dict>..<key>Creation Da
te</key>..<date>2013-07-08T23:22:35Z</date>..<k
ey>Entry Text</key>..<string>First tomatoes fro
m my garden!</string>..<key>Location</key>..<di
ct>...<key>Administrative Area</key>...<string>
Virginia</string>...<key>Country</key>...<strin
g>United States</string>...<key>Latitude</key>.
..<real>38.897663774005039</real>...<key>Locali
ty</key>...<string>Dunn Loring</string>...<key>
Longitude</key>...<real>-77.240605317128114</re
al>...<key>Place Name</key>...<string>8521 Mine
rva Ct</string>..</dict>..<key>Starred</key>..<
true/>..<key>Time Zone</key>..<string>America/N
ew_York</string>..<key>UUID</key>..<string>8CC1
B93F56974CD594104E20E33FBB61</string>..<key>Wea
ther</key>..<dict>...<key>Celsius</key>...<stri
ng>29</string>...<key>Description</key>...<stri
ng>Partly Cloudy</string>...<key>Fahrenheit</ke
y>...<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

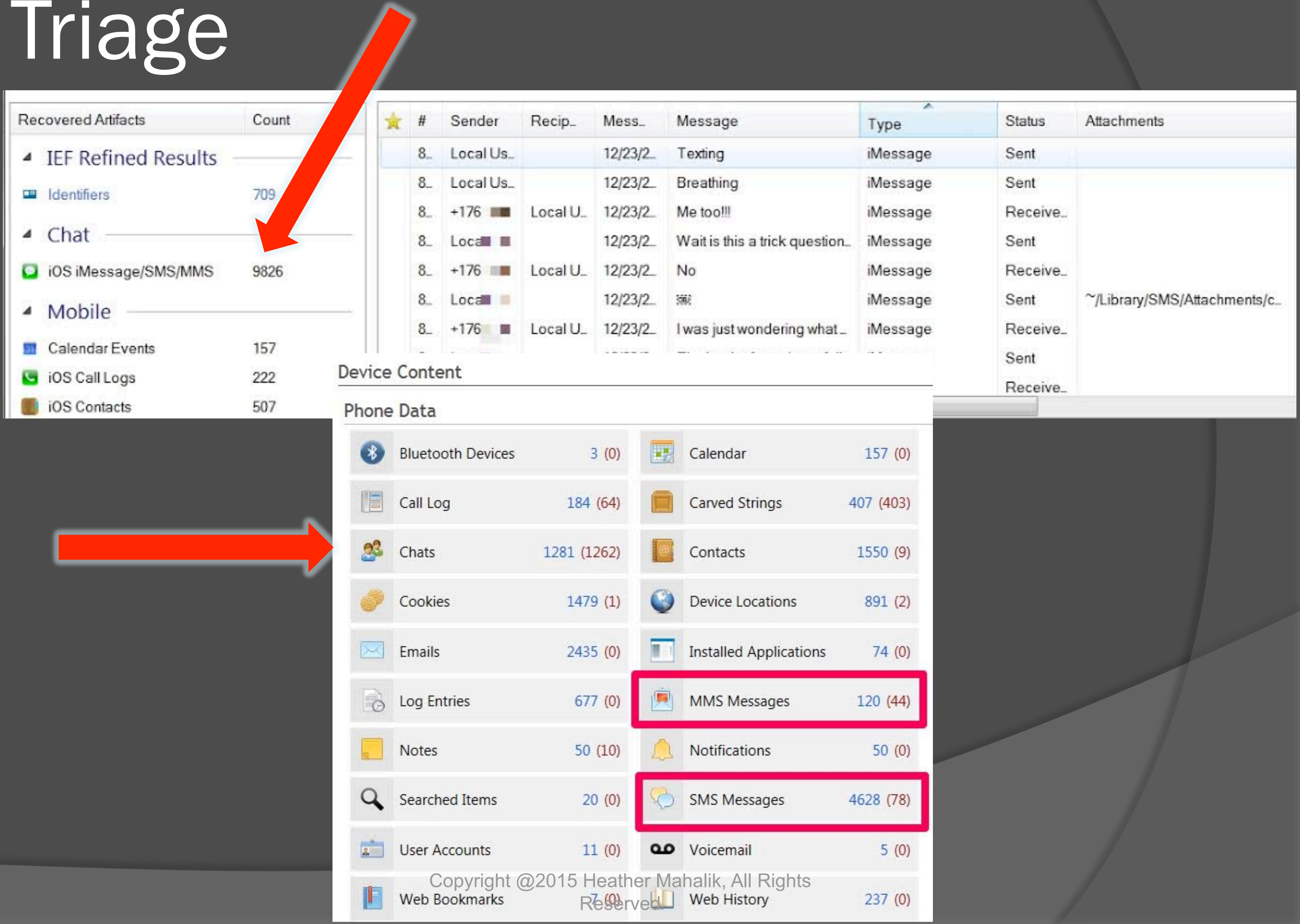
How did that get there?



They work together beautifully.

Start editing a photo on your iPad and finish it on your MacBook. Sync a playlist from your iPhone to your Apple Watch. And send iMessages from any Apple device to any other.

Triage



Recovered Artifacts	Count
IEF Refined Results	
Identifiers	709
Chat	
iOS iMessage/SMS/MMS	9826
Mobile	
Calendar Events	157
iOS Call Logs	222
iOS Contacts	507

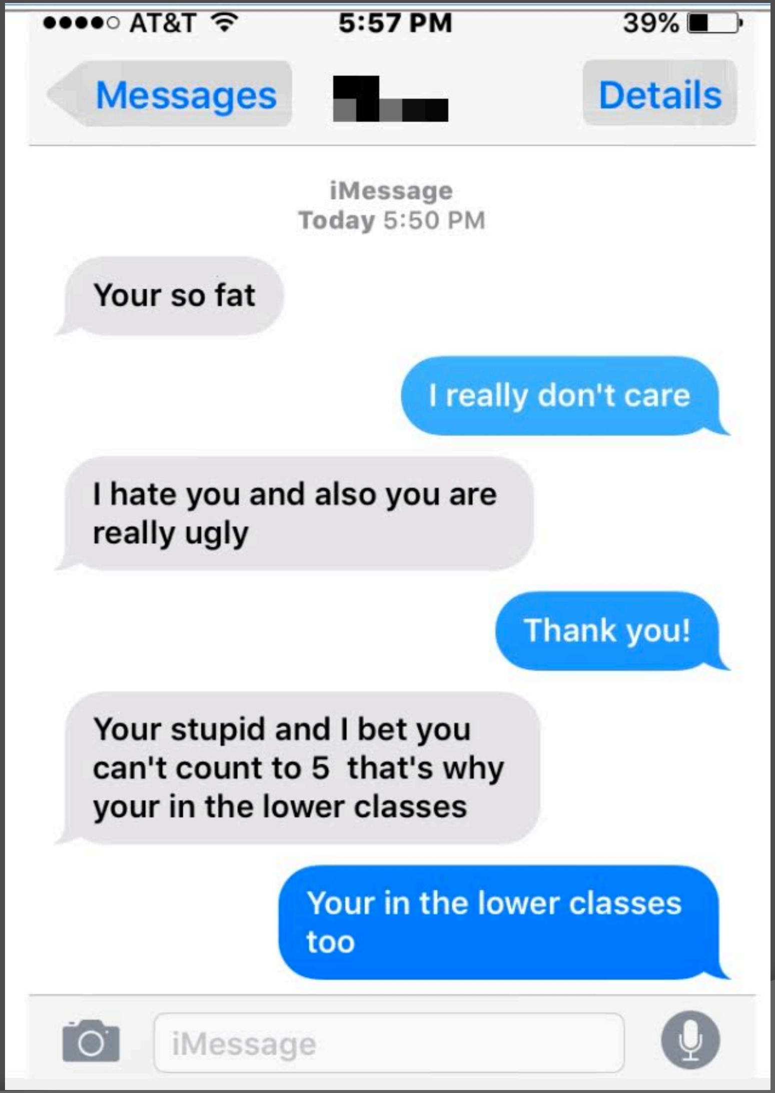
★	#	Sender	Recip..	Mess..	Message	Type	Status	Attachments
	8..	Local Us..		12/23/2..	Texting	iMessage	Sent	
	8..	Local Us..		12/23/2..	Breathing	iMessage	Sent	
	8..	+176 [redacted]	Local U..	12/23/2..	Me too!!!	iMessage	Receive..	
	8..	Loca[redacted]		12/23/2..	Wait is this a trick question..	iMessage	Sent	
	8..	+176 [redacted]	Local U..	12/23/2..	No	iMessage	Receive..	
	8..	Loca[redacted]		12/23/2..	[illegible]	iMessage	Sent	~/Library/SMS/Attachments/c..
	8..	+176 [redacted]	Local U..	12/23/2..	I was just wondering what..	iMessage	Receive..	
							Sent	
							Receive..	

Device Content

Phone Data

Bluetooth Devices	3 (0)	Calendar	157 (0)
Call Log	184 (64)	Carved Strings	407 (403)
Chats	1281 (1262)	Contacts	1550 (9)
Cookies	1479 (1)	Device Locations	891 (2)
Emails	2435 (0)	Installed Applications	74 (0)
Log Entries	677 (0)	MMS Messages	120 (44)
Notes	50 (10)	Notifications	50 (0)
Searched Items	20 (0)	SMS Messages	4628 (78)
User Accounts	11 (0)	Voicemail	5 (0)
Web Bookmarks	7 (0)	Web History	237 (0)

Digging Deeper



[redacted]

iMessage
Today 5:50 PM

Your so fat

I really don't care

I hate you and also you are really ugly

Thank you!

Your stupid and I bet you can't count to 5 that's why your in the lower classes

Your in the lower classes too

Concerns

Small Budget?

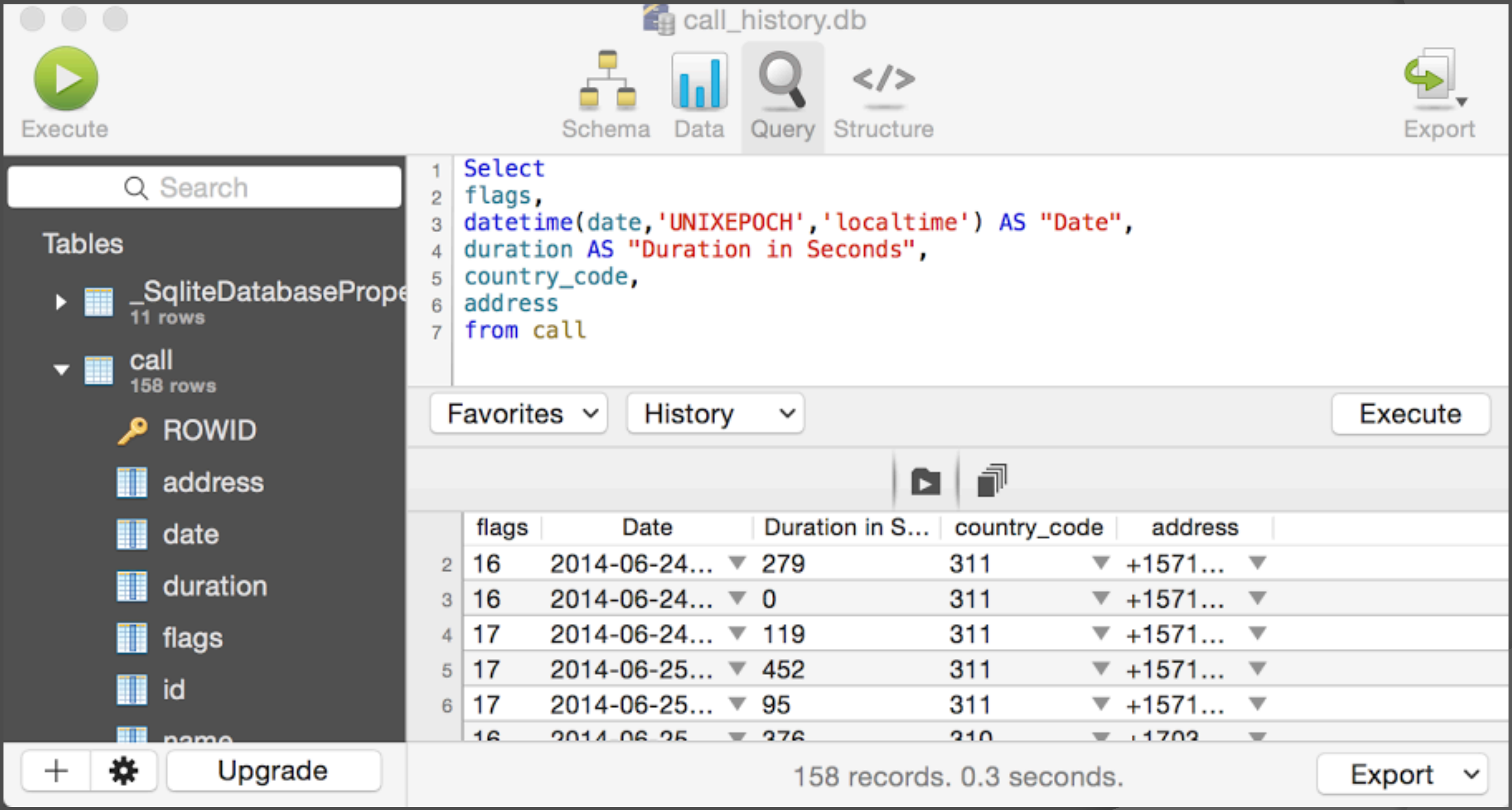
- Autopsy
- Magnet Acquire
- NowSecure CE
- SSH (Sarah's blog post)
- FTK Imager
- ADB pull

Acquisition Solutions

- Autopsy
- Andriller
- Sanderson SQLite Forensic Browser
- SQLPro for SQLite
- Hex editor
- Notepad
- SSH
- Live Analysis

Analysis Solutions

Creating a Query



```
Select
flags,
datetime(date,'UNIXEPOCH','localtime') AS "Date",
duration AS "Duration in Seconds",
country_code,
address
from call
```

	flags	Date	Duration in S...	country_code	address
2	16	2014-06-24...	279	311	+1571...
3	16	2014-06-24...	0	311	+1571...
4	17	2014-06-24...	119	311	+1571...
5	17	2014-06-25...	452	311	+1571...
6	17	2014-06-25...	95	311	+1571...
	16	2014-06-25	376	310	+1703

158 records. 0.3 seconds.

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?

GIAC GASF Certification

- Beta test in progress
- 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 be one of the first with this sought after cert

Heather Mahalik

heather@smarterforensics.com

@HeatherMahalik

Blog: for585.com/blog

Questions?

FOR585.com/course

- SANSFIRE – June – Washington, DC
- DFIR Summit – June – Austin, TX
- VA Beach – August
- Network Security – Sept – Las Vegas
- Baltimore – Oct
- Prague – Oct
- OnDemand/Self-Study
- Onsites

References

- http://smarterforensics.com/blog/
- http://www.mac4n6.com/
- FOR585.com/course
- https://www.magnetforensics.com
- https://andriller.com
- http://www.sleuthkit.org
- http://www.cellebrite.com

THANK YOU FOR ATTENDING

To Trust or Not To Trust:

The Relationship Between You and Your Mobile Forensics Tool

Heather Mahalik @HeatherMahalik

GASF is coming soon!

Focused on mobile forensics analysis, the new GASF certification will be the only vendor-agnostic mobile forensics certification in the industry. Take the FOR585 course now and get your certification as soon as it is available in the next few months.

Take FOR585: Advanced Smartphone Forensics at these training events:

SANSFIRE

Washington, DC | Jun 13-18

Featuring: Heather Mahalik

sans.org/sansfire

DFIR Summit

Austin, TX | Jun 25-30

Featuring: Cindy Murphy

sans.org/dfirsummit