Phoning it in: Heather talks about Smartphone Forensics

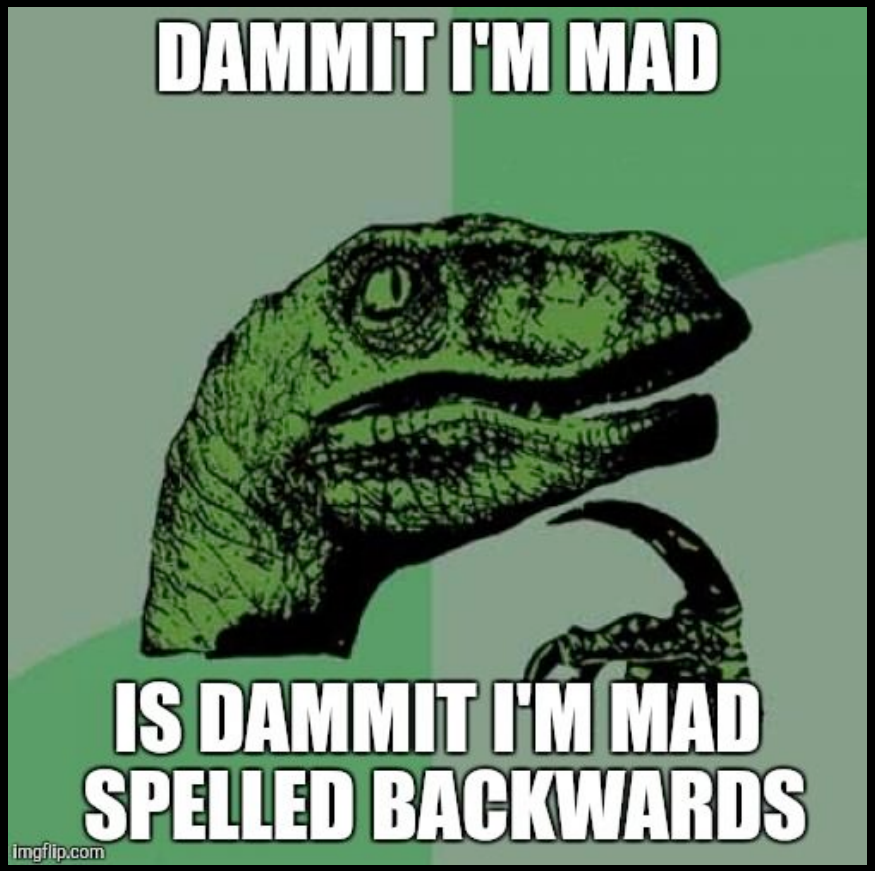
Heather Mahalik

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 FOR500
- Co-Author of Practical Mobile Forensics (1st and 2nd Editions)
- Mom and a wife
- Dog, horse, wine and bourbon lover ☺

Agenda

- What to expect with smartphone security
- Secure apps
- Location data
- Tools….
- Testing, tips and tricks




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?
- 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!!!

Application “Protection”

Transforming/converting data into code

Encoding Schemes

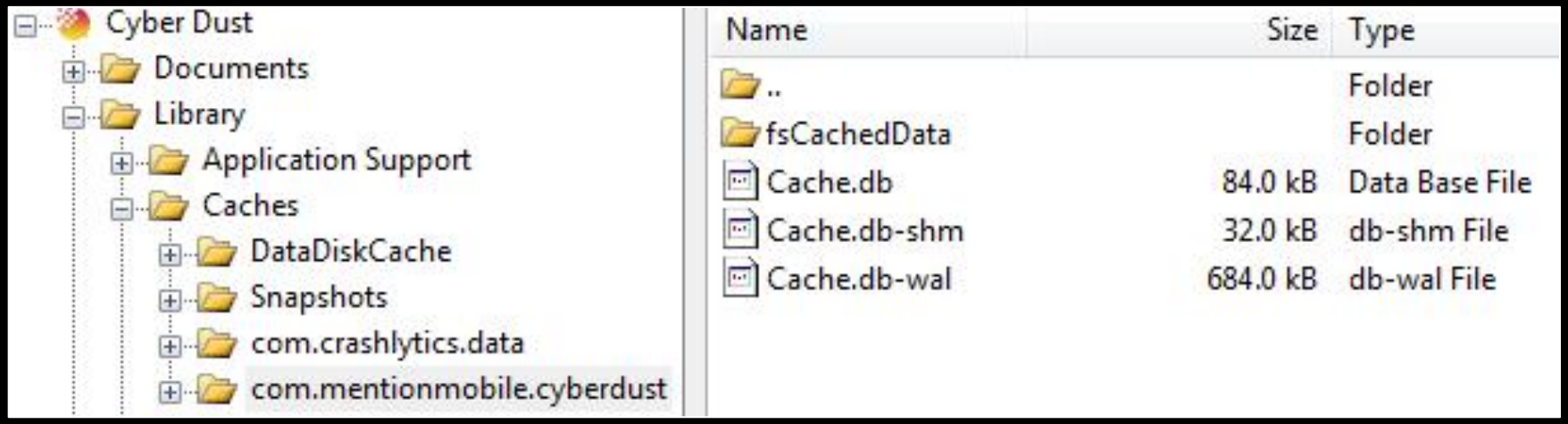
- ASCII
- Unicode
- UTF-8
- Base64

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



Example: Cyber Dust (2)

- Messages are encoded twice using Base64

Cache.db-wal - Notepad

File Edit Format View Help


```
{"result":{"chatRoomContainer":{"account":
{"id":"545ce910e4b0994d3e7aa237","verified":false,"uniqueHash":"[illegible]==,545ce910e4b0994d3e7aa237","us
erName":"[illegible]","emailAddress"[illegible].com","hashedPassword":"EgJr3mdO7[illegible]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
{"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":nul[illegible]"encryptedMessage":"VjJoaGRDZHpJSFZ3SUcxNUlHSnZlVDg9"[illegible]mageData":null,"videoThumbnailImageData":
null,"type":"BlastChat"[illegible]"date":"2014-11-07 18:41:12.661
+0000","longitude":0.0,"latitude":0.0,"locationName":""}]},"error":null,"warning":null}
{"result":
{"chatRoomContainer":{"account":
```


VjJoaGRDZHpJSFZ3SUcxNUlHSnZlVDg9

Decoded Output

Here is the decoded output of your Base 64 input:

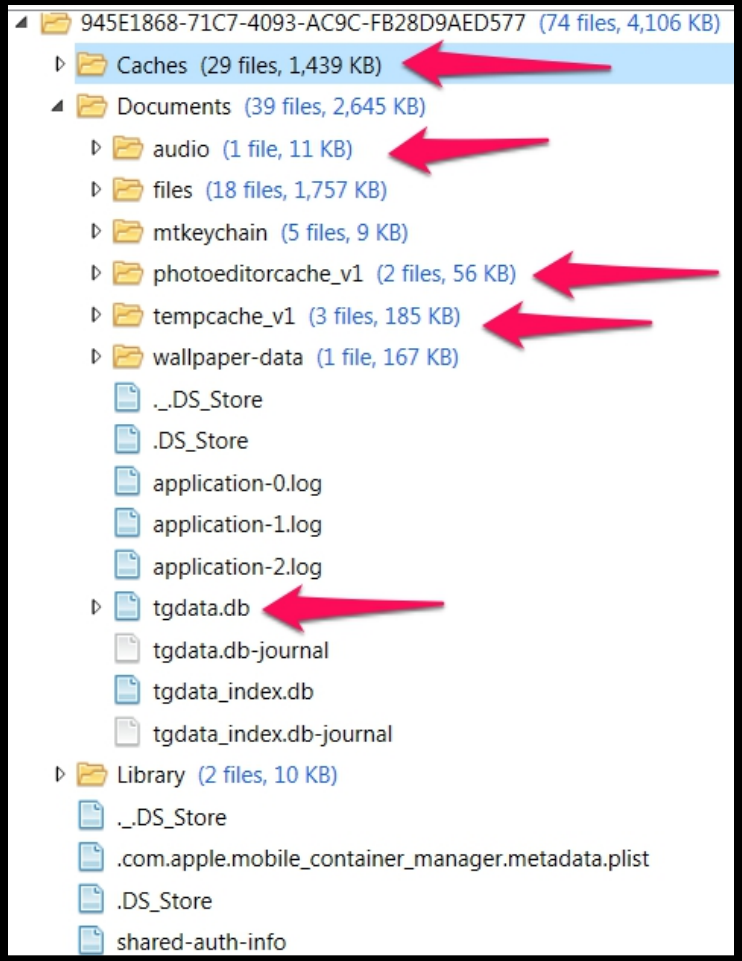
V2hhdCdzIHVwIG15IGJveT8=

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							Received
41	P Nasty							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

5a50d642c808bc33786aa57bbfca7d97	2/6/2016 4:48 PM	File	19 KB
8b8fd24b6f791d0d0df941604d2d0b40	2/6/2016 4:46 PM	File	23 KB

Will your tool catch you when you fall?

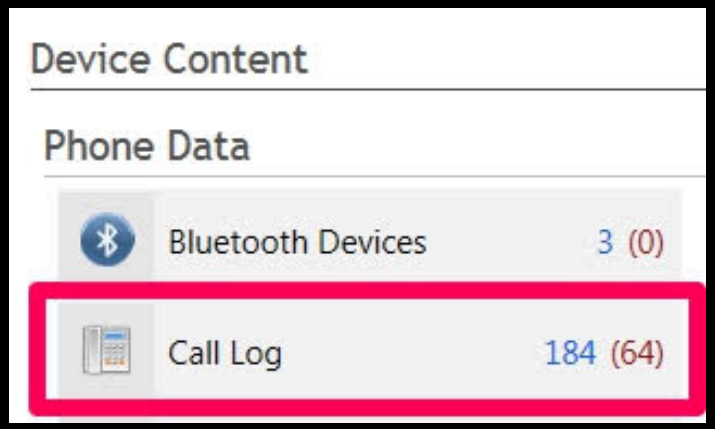
- Will you be able to defend the evidence?
- Can you find the data?
- What if the tools contradict one another?
- Understand the artifacts
- Don’t know just enough to be dangerous

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



UFED Physical Analyzer

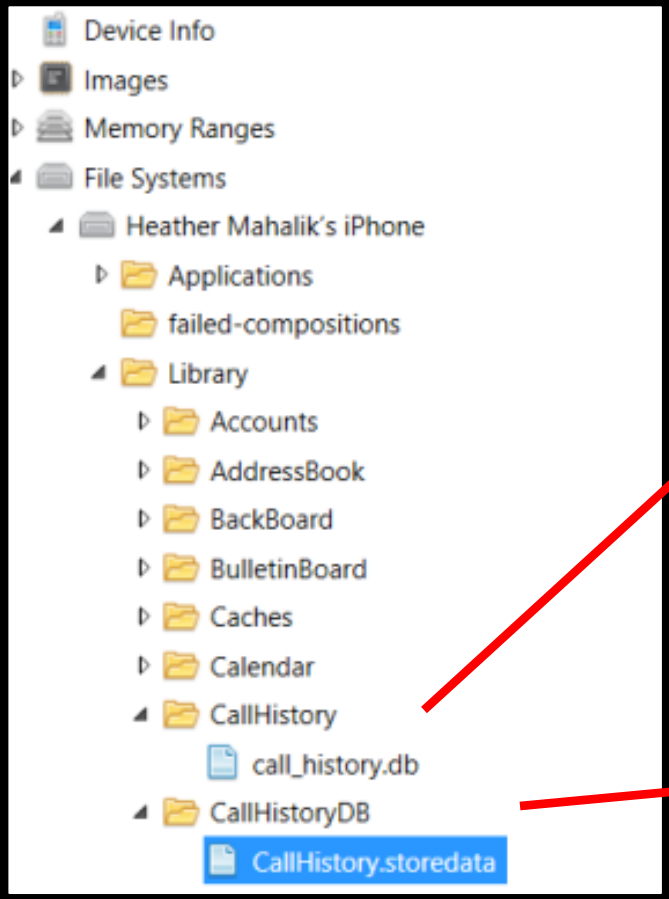
Call Logs

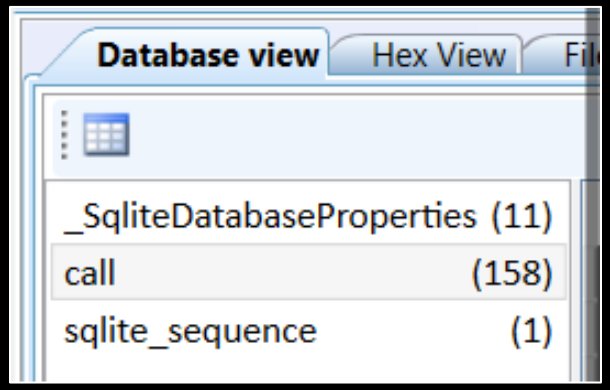
Library/CallHistory/call_history.db

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

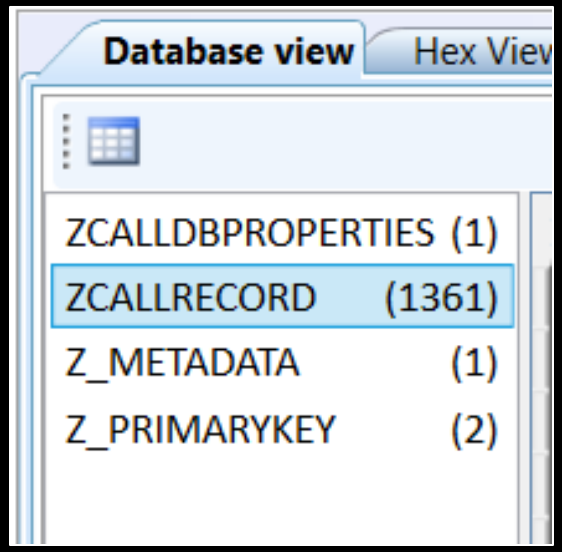
Example: Call Logs (2)

Call logs





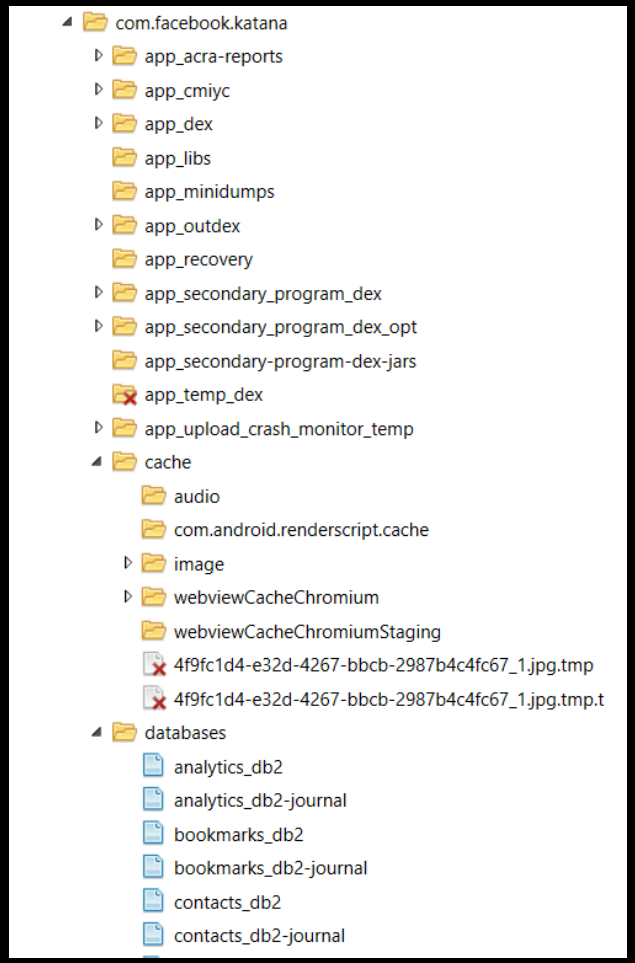
iOS 7



iOS 8,9 & 10

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?

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

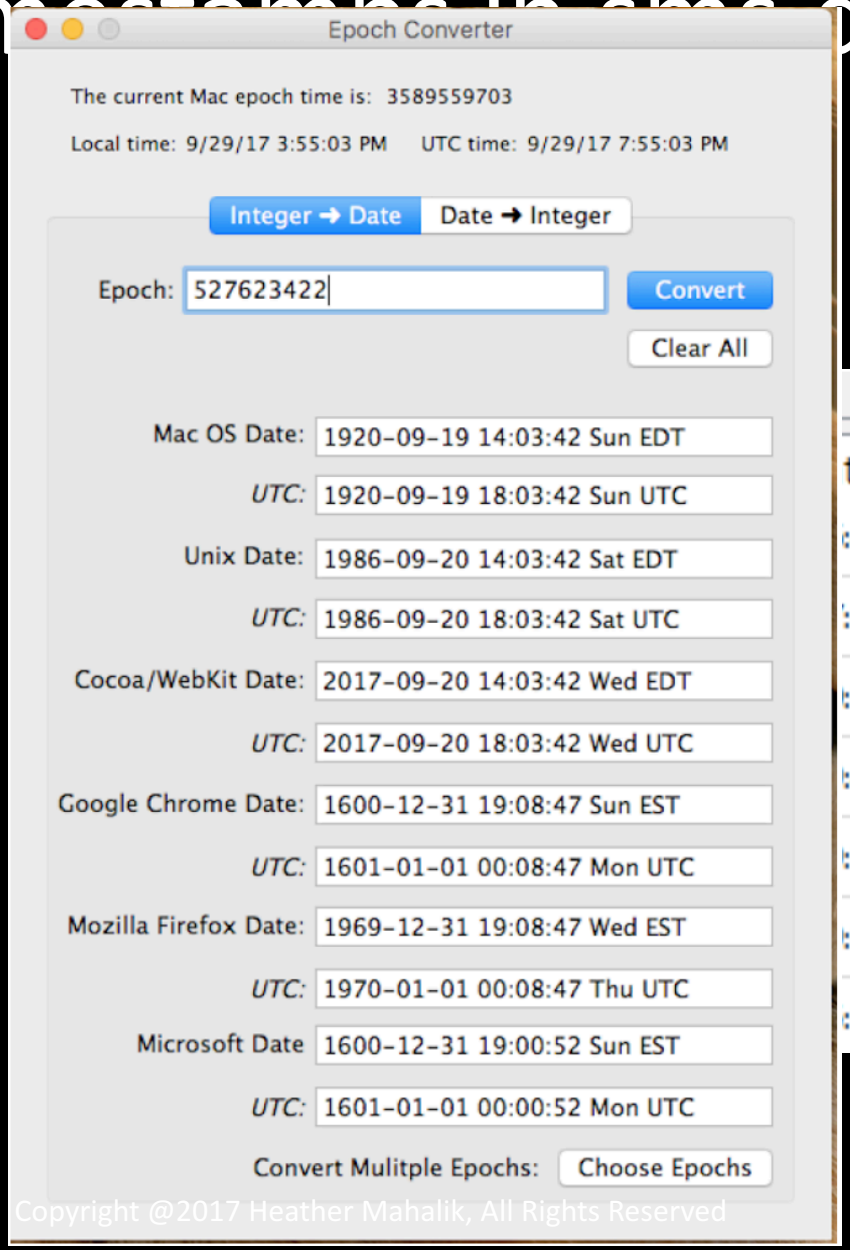

```
version="1.0" encoding="UTF-8"?>.<!DOCTYP
t PUBLIC "-//Apple//DTD PLIST 1.0//EN" "h
www.apple.com/DTDs/PropertyList-1.0.dtd">
t version="1.0">.<dict>..<key>Creation Da
ey>..<date>2013-07-08T23:22:35Z</date>..<k
ey>Entry Text</key>..<string>First tomatoes fro
m my garden!</string>..<key>Location</key>..<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>.
```

Then came iOS 11

- The sms.db is *not* the same
- Timestamps *may* have an 18 digit value
  - Tools don't really like this…
- New columns were added to the database
- Old columns contain both new and old data
  - Tools don't really like this either…

Timestamps in sms.db

last date read
0
527625024
0
0
527623425000000000
527623425000000000
527623425000000000
527623425000000000
527623425000000000
527625024

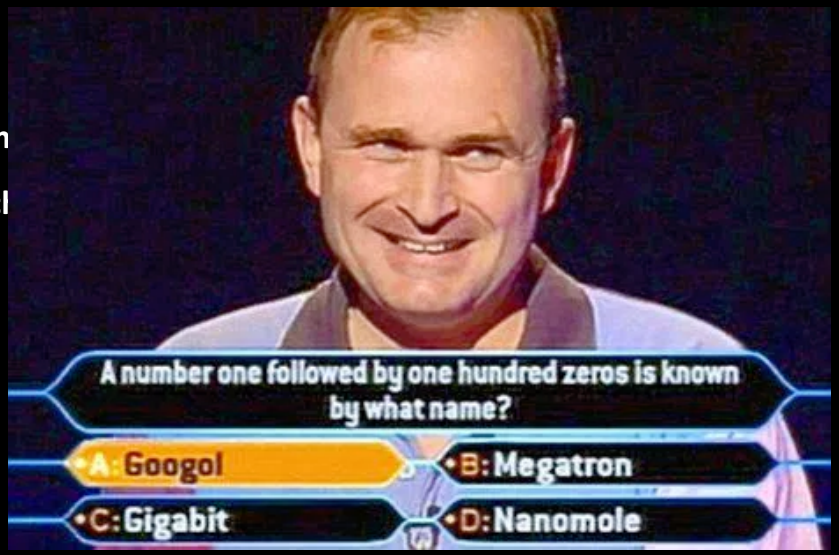


	-1413-03-01 08:07:12
:09	2017-09-19 19:47:09
:05	2017-09-19 17:10:05
:42	2017-09-19 11:19:42
:28	2017-09-19 11:19:28
:08	2017-09-19 11:19:08
:02	2017-09-19 11:05:02

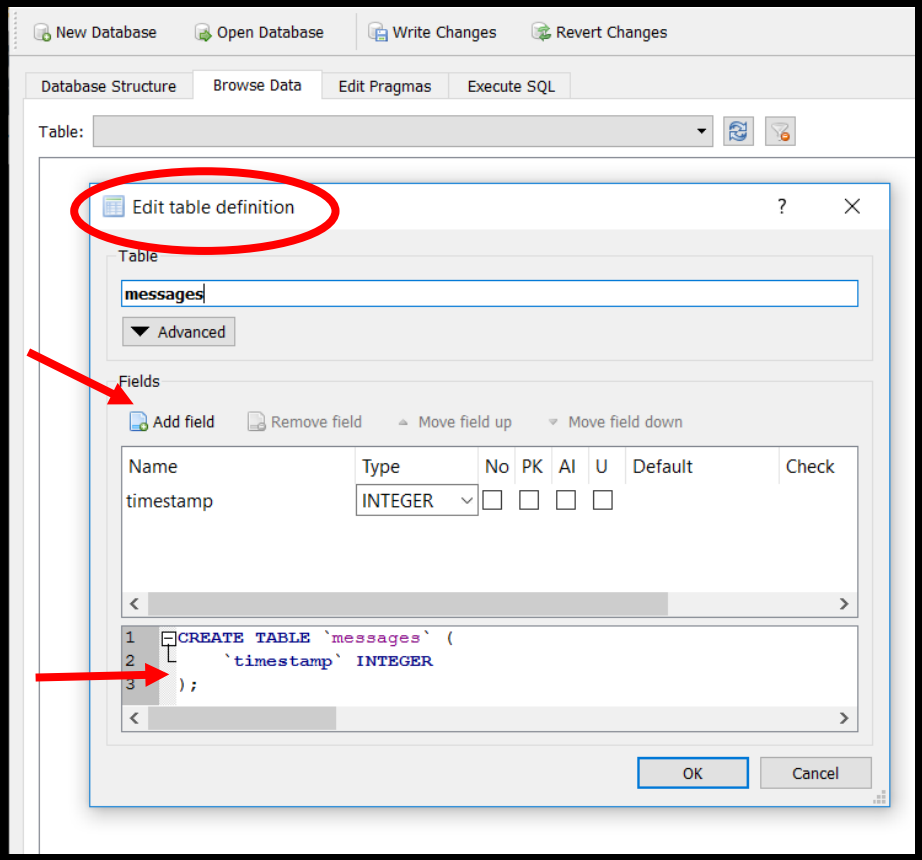
The query that **“almost”** could

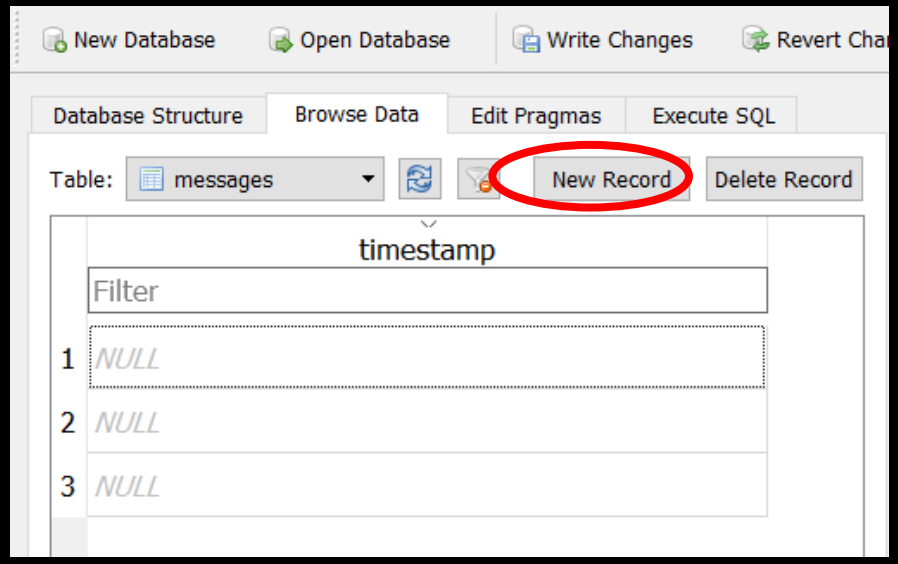
```
SELECT
message.rowid,
chat_message_join.chat_id,
message.handle_id,
message.text,
message.service,
message.account,
chat.account_login,
chat.chat_identifier AS “Other Party”,
datetime(message.date + 978307200,’unixepoch’,’localtime’) AS “conv start date”,
datetime(chat_message_join.message_date +978307200,’unixepoch’,’localtime’) AS “conversation start date”,
datetime(message.date_read + 978307200,’unixepoch’,’localtime’) AS “date read”,
message.is_read AS “1=Incoming, 0=Outgoing”,
datetime(chat.last_read_message_timestamp + 978307200,’unixepoch’,’localtime’)
datetime(chat.last_read_message_timestamp +978307200,’unixepoch’,’localtime’) AS “last date read”,
attachment.filename,
attachment.created_date,
attachment.mime_type,
attachment.total_bytes
FROM
message
left join chat_message_join on chat_message_join.message_id=m
left join chat on chat.ROWID=chat_message_join.chat_id
left join attachment on attachment.ROWID=chat_message_join.cl
order by message.date_read desc
```

The problem



Create a sample test database





Converting the time

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: messages

	timestamp
1	494278904000000000
2	527623421824887040
3	527623975464060800

Database Structure | Browse Data | Edit Pragmas | Execute SQL

SQL 1

```
SELECT
datetime(timestamp/1000000000+978307200,'unixepoch','localtime') AS "Timestamp"
FROM messages
```

	Timestamp
1	2017-09-20 14:12:55
2	2017-09-20 14:03:41
3	2016-08-30 15:41:44

```
3 rows returned in 0ms from: SELECT
datetime(timestamp/1000000000+978307200,'unixepoch','localtime') AS &quot;Timestamp&quot;
FROM messages
```

But how do we account for differences?

SAMPLE DATA

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: messages

	timestamp
1	527623975464060800
2	527623421824887040
3	494278904000000000
4	527623975
5	527623421
6	494278904
7	0
8	0
9	0

RESULTS

Database Structure | Browse Data | Edit Pragmas | Execute SQL

SQL 1

```
SELECT
datetime(timestamp/1000000000+978307200,'unixepoch','localtime') AS "Timestamp"
FROM messages
```

	Timestamp
1	2017-09-20 14:12:55
2	2017-09-20 14:03:41
3	2016-08-30 15:41:44
4	2000-12-31 19:00:00
5	2000-12-31 19:00:00
6	2000-12-31 19:00:00
7	2000-12-31 19:00:00
8	2000-12-31 19:00:00
9	2000-12-31 19:00:00

New date format

Mac Absolute

Zeros

Tell the query to handle each format differently

- Length of 18 – iOS 11 format
- Length of 9 – Mac Absolute format
- Anything else…

Database Structure | Browse Data | Edit Pragmas | Execute SQL

SQL 1

```
1  SELECT
2  case when LENGTH(timestamp)=18 then
3  datetime(timestamp/1000000000+978307200,'unixepoch','localtime')
4  when LENGTH(timestamp)=9 then
5  datetime(timestamp+978307200,'unixepoch','localtime')
6  else 'N/A'
7  END AS "Time"
8  FROM messages
```

	Time
1	2017-09-20 14:12:55
2	2016-08-30 15:41:44
3	2017-09-20 14:03:41
4	2017-09-20 14:04:04
5	N/A
6	N/A

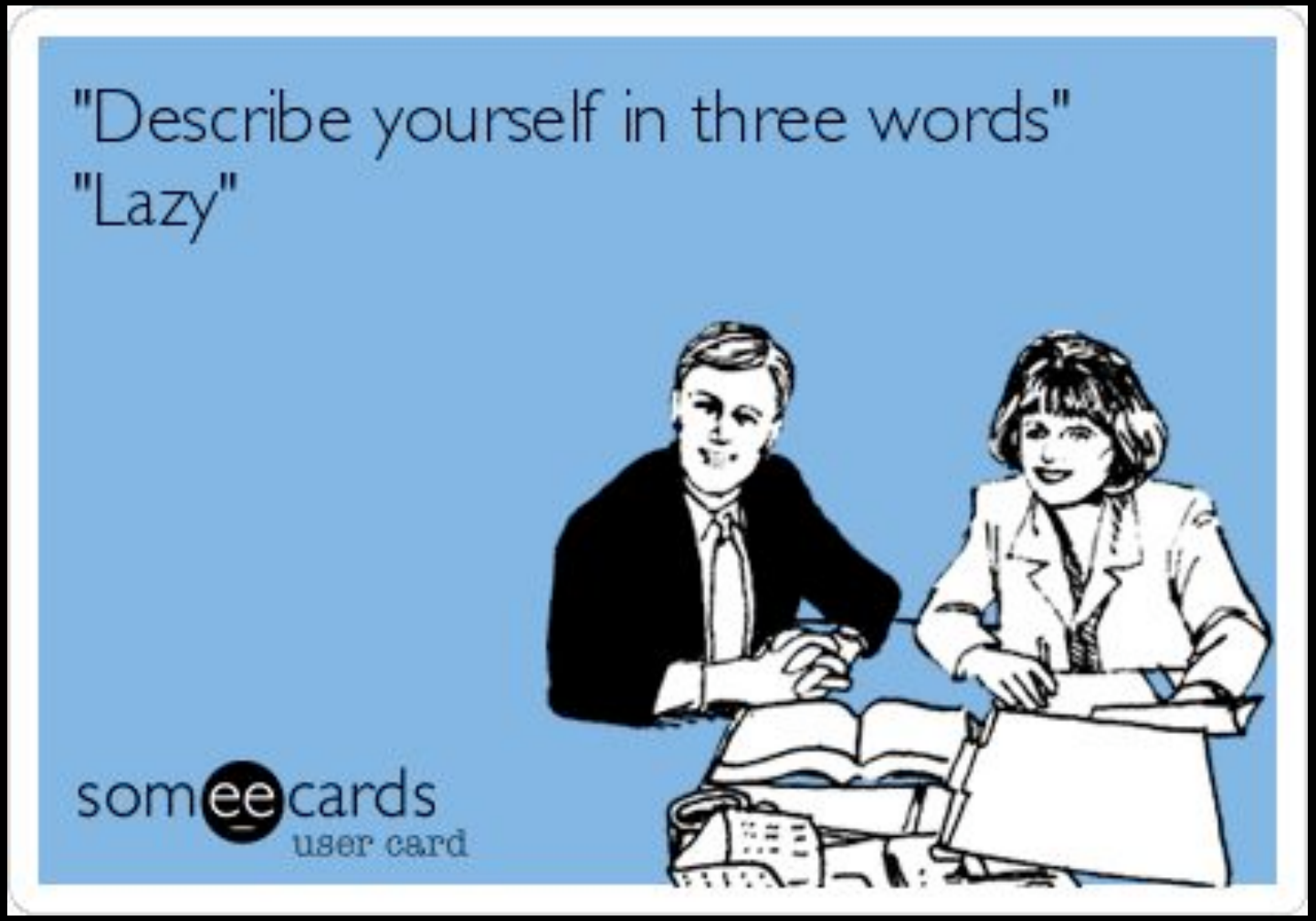
The mother of all queries

```
SELECT
message.rowid,
chat_message_join.chat_id,
message.handle_id,
message.text,
message.service,
message.account,
chat.account_login,
chat.chat_identifier AS “Other Party”,
datetime(message.date/1000000000 + 978307200,’unixepoch’,’localtime’) AS “conv start date”,
case when LENGTH(chat_message_join.message_date)=18 then
datetime(chat_message_join.message_date/1000000000+978307200,’unixepoch’,’localtime’)
when LENGTH(chat_message_join.message_date)=9 then
datetime(chat_message_join.message_date +978307200,’unixepoch’,’localtime’)
else ‘N/A’
END AS “conversation start date”,
datetime(message.date_read + 978307200,’unixepoch’,’localtime’) AS “date read”,
message.is_read AS “1=Incoming, 0=Outgoing”,
case when LENGTH(chat.last_read_message_timestamp)=18 then
datetime(chat.last_read_message_timestamp/1000000000+978307200,’unixepoch’,’localtime’)
when LENGTH(chat.last_read_message_timestamp)=9 then
datetime(chat.last_read_message_timestamp +978307200,’unixepoch’,’localtime’)
else ‘N/A’
END AS “last date read”,
attachment.filename,
attachment.created_date,
attachment.mime_type,
attachment.total_bytes
FROM
message
left join chat_message_join on chat_message_join.message_id=message.ROWID
left join chat on chat.ROWID=chat_message_join.chat_id
left join attachment on attachment.ROWID=chat_message_join.chat_id
order by message.date_read desc
```

A snippet of the output

	ROWID	chat ic	handle ic	text	service	ccour	ount Ic	ther Par	conv start date
1	187996	5282	979	On my way home	iMessage	p:+1...	P:+17..	+15712..	2017-09-20 14:22:43
2	187997	5282	979	Discuss when I get there	iMessage	p:+1...	P:+17..	+15712..	2017-09-20 14:22:58
3	187992	5282	979	Not sure	iMessage	p:+1...	P:+17..	+15712..	2017-09-20 14:20:43
4	187993	5282	979	I will let you know	iMessage	p:+1...	P:+17..	+15712..	2017-09-20 14:20:48
5	187991	5876	5062	No worries! Thanks. Will let you know if I hea	iMessage	p:+1...	P:+17..	chat649.	2017-09-20 14:12:55
6	187989	5362	3816	👍	iMessage	p:+1...	P:+17..	+17174..	2017-09-20 14:03:41
7	187985	5362	3816	We can just plan for tomorrow then	iMessage	p:+1...	P:+17..	+17174..	2017-09-20 13:54:22
8	187980	5876	5062	Ufed 4 pic	iMessage	p:+1...	P:+17..	chat649.	2017-09-20 13:52:04
9	187981	5876	5062	Cool	iMessage	p:+1...	P:+17..	chat649.	2017-09-20 13:52:08
10	187982	5876	5062	Lol! Darn auto correct! 4PC!	iMessage	p:+1...	P:+17..	chat649.	2017-09-20 13:52:30
11	187977	5876	5062	Yes... taking screen shots in the iOS acquisition menu.	iMessage	p:+1...	P:+17..	chat649.	2017-09-20 13:51:34

```
46200 rows returned in 901ms from: SELECT
message.rowid,
chat_message_join.chat_id,
message.handle_id,
```



https://github.com/hmahalik

Don’t fear the unknown

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

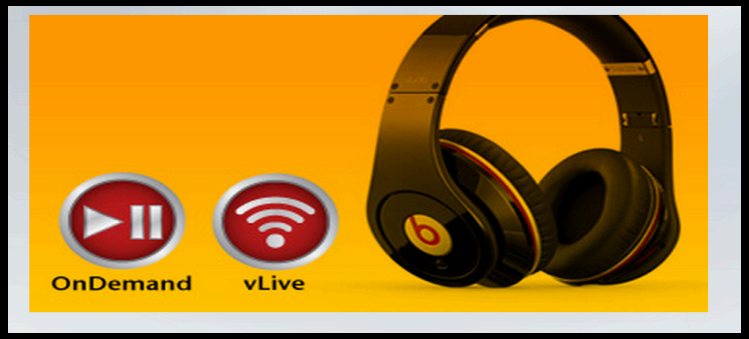
About 585…

- 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

- http://smarterforensics.com/2017/09/time-is-not-on-our-side-when-it-comes-to-messages-in-ios-11/
- https://github.com/hmahalik
  - iOS SMS “stuff”
- FOR585 Advanced Smartphone Forensics
- https://www.gillware.com/forensics/blog/
- https://github.com/threeplanetssoftware/sqlite_miner


How To Smash A Mobile Phone
With A Sledge Hammer



FOR585 Advanced Smartphone Forensics Course Available At:

FOR585.com/course

Apr: SANS 2018 Orlando - Heather
May: San Diego, CA – Cindy Murphy
June: DFIR Summit, TX & Paris
July: SANSFIRE, DC – Heather
August: NYC – Lee
Sept: Las Vegas – Heather
Oct: Denver, CO – Lee
Nov: Miami, Austin & Stockholm
Dec: DC & Saudi Arabia

Heather Mahalik

heather@smarterforensics.com

@HeatherMahalik

Blog: for585.com/blog

QUESTIONS?