FORENSICS ANALYSIS OF iOS MESSAGING APPS

PASQUALE STIRPARO (@PSTIRPARO)

HACKLU

LUXEMBOURG, 20 OCTOBER 2016

HOW AND WHERE DATA IS STORED

Starting from iOS8, application data have been separated from their bundles and current directory structure is the following

- **/private/var/mobile/Containers/Bundle/Application/<APP_UUID>/**: This path is the actual path where the application bundle is stored.
- **/private/var/mobile/Containers/Data/Application/<APP_UUID>/**: This path is the actual path where most of the application data is stored.
- **/private/var/mobile/Containers/Shared/AppGroup/<APP_UUID>/**: As the name of the folder suggests, this path is the path where applications can store data with the aim of sharing it with other apps or extensions.

File formats are the usual plist files and SQLite databases

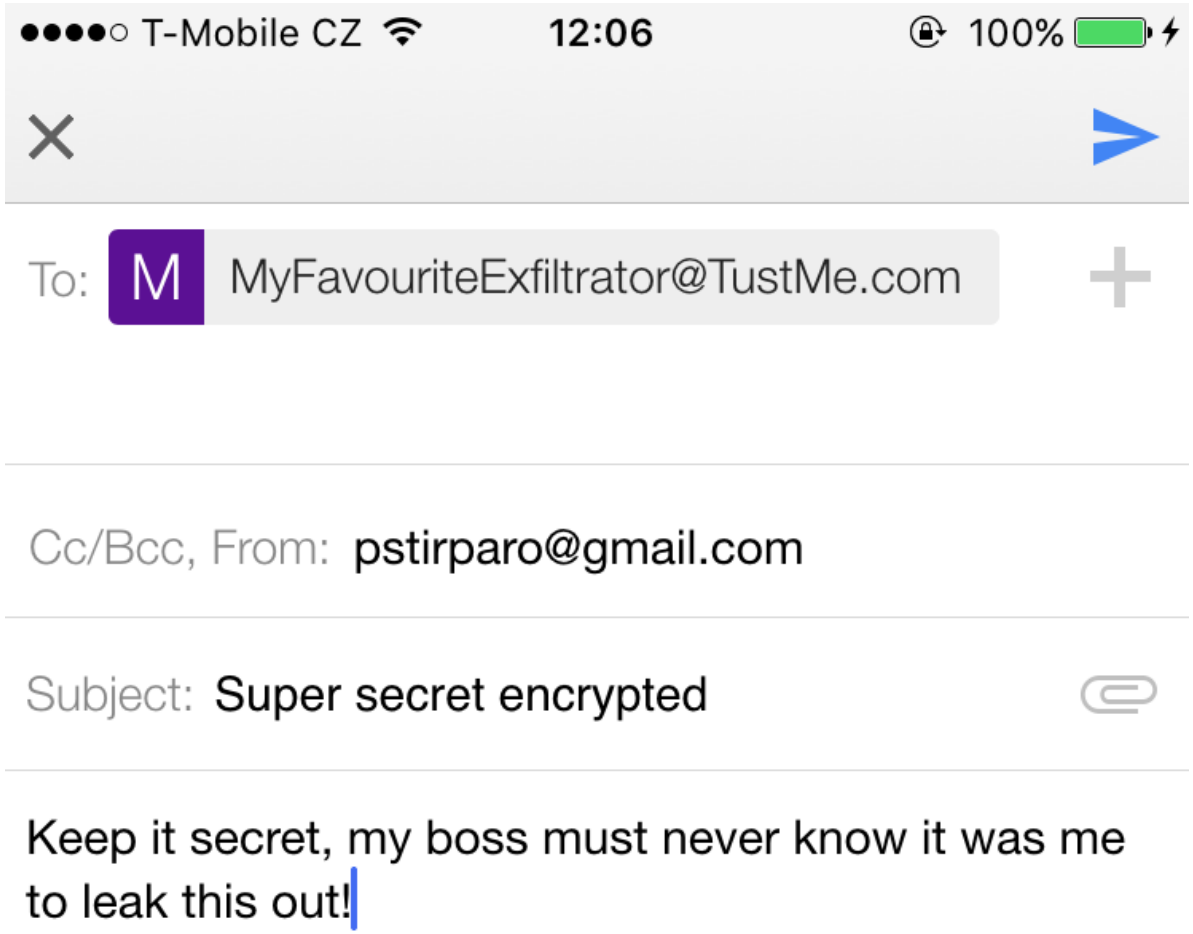
WHAT ABOUT DELETED DATA?

- When a SQLite record is being deleted, for performance reasons it is not actually wiped/ purged from the database immediately, but marked as free and eventually overwritten later on when that storage space is needed.
- With tools like SQLite-parser [1][2], you can quickly carve out deleted record from SQLite database if not explicitly handled by the developer.
- However, you will find this "feature" in most applications using SQLite storage databases, … keep that in mind.

[1] – "Python Parser to Recover Deleted SQLite Database Data", http://az4n6.blogspot.ch/2013/11/python-parser-to-recover-deleted-sqlite.html
[2] – "SQLite-parser", https://github.com/mdegrazia/SQLite-Deleted-Records-Parser

DO NOT FORGET THE FADE-OUT EFFECT

- Every time a user presses the Home button or receives a call while using an application, iOS will make a "snapshots" of the current screen in order to be able to do the fade-out effect transition between the two screens.
- **/private/var/mobile/Library/Caches/Snapshots/** for the pre-installed Apple applications;
- **/private/var/mobile/Containers/Data/Applications/<UUID>/Library/Caches/Snapshots/**, for each third-party application



DO NOT FORGET THE FADE-OUT EFFECT

"SECURE" MESSAGING IN iOS

- WhatsApp, Telegram and Signal among the most widespread applications for instant messaging.
- All of them claim "secure" messaging to a certain extent.
- All of them have end-to-end encryption (data-in-transit), but we will focus on the artifacts left on the device (data-at-rest).

WHATSAPP

- Data is stored in the Shared directory instead of the application data directory
  `/private/var/mobile/Containers/Shared/AppGroup/332A098D-368C-4378-A503-91BF33284D4B`
  `|-- Axolotl.sqlite`
  `|-- ChatSearch.sqlite`
  `|-- **ChatStorage.sqlite**`
  `|-- Contacts.sqlite`
- Some of the tables of interest are:
  - *ZWACHATSESSION*, *ZWAGROUPMEMBER*, *ZWAGROUPINFO* and *ZWAMEDIAITEM*, which stores references to the multimedia files exchanged, indication of the users involved, timestamps, the path where the file has been stored, etc.

WHATSAPP

- *ZWAMESSAGE* contains, among others, the messages exchanged, their timestamp, the name of the user involved in the chat.

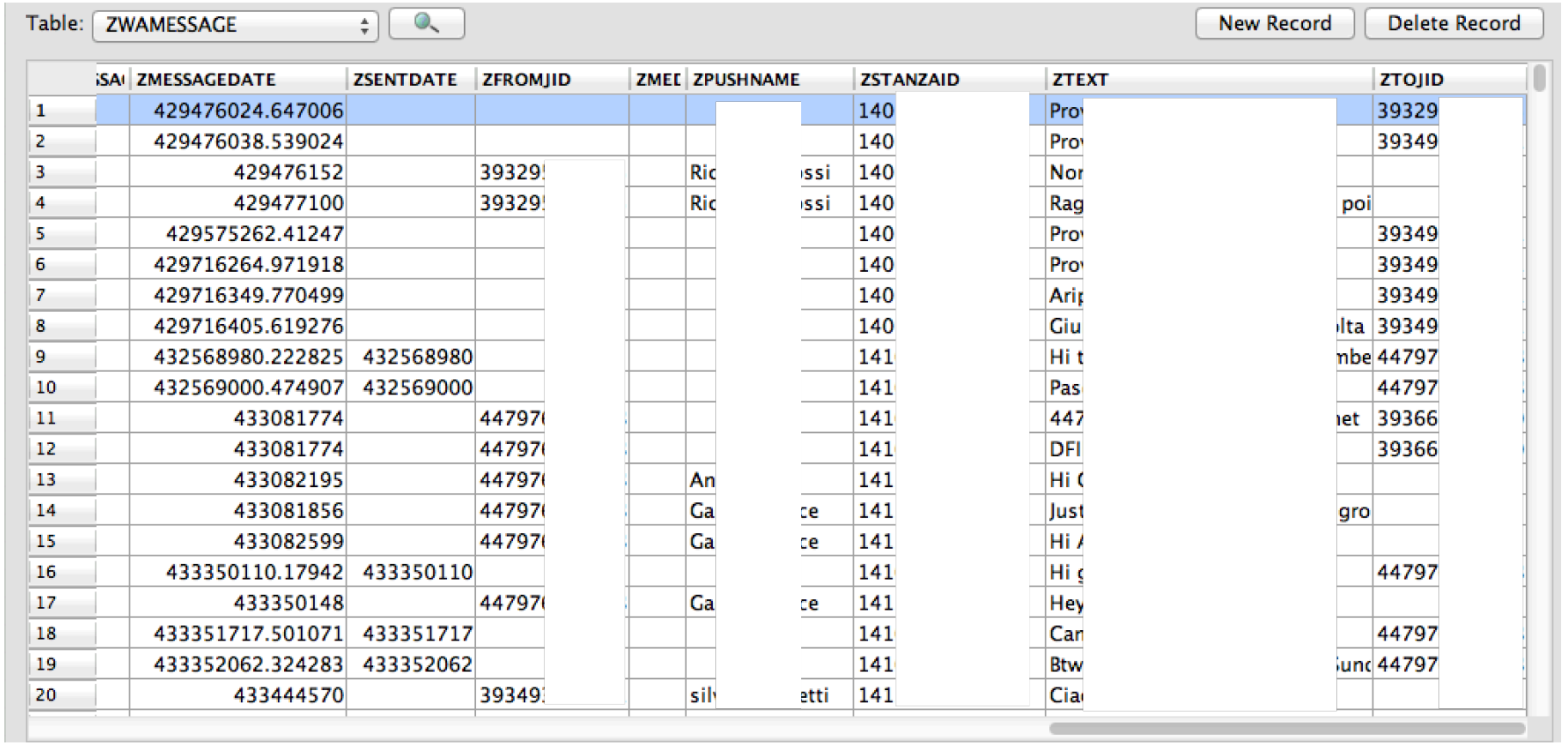


Table: ZWAMESSAGE

New Record | Delete Record

	ZMESSAGEDATE	ZSENTDATE	ZFROMJID	ZPUSHNAME	ZSTANZAID	ZTEXT	ZTOJID
1	429476024.647006				140	Pro	39329
2	429476038.539024				140	Pro	39349
3	429476152		39329	Ric ssi	140	Nor	
4	429477100		39329	Ric ssi	140	Rag poi	
5	429575262.41247				140	Pro	39349
6	429716264.971918				140	Pro	39349
7	429716349.770499				140	Arip	39349
8	429716405.619276				140	Giu lta	39349
9	432568980.222825	432568980			141	Hi t mbe	44797
10	432569000.474907	432569000			141	Pas	44797
11	433081774		44797		141	447 et	39366
12	433081774		44797		141	DFI	39366
13	433082195		44797	An	141	Hi (	
14	433081856		44797	Ga ce	141	Just gro	
15	433082599		44797	Ga ce	141	Hi A	
16	433350110.17942	433350110			141	Hi g	44797
17	433350148		44797	Ga ce	141	Hey	
18	433351717.501071	433351717			141	Can	44797
19	433352062.324283	433352062			141	Btw unc	44797
20	433444570		39349	sil etti	141	Cia	

TELEGRAM

- Like WhatsApp, also Telegram stores many of its data in the *Shared* directory.
- The **tgdata.db** database, under the *Documents* folder, contains all information about contacts, conversations, exchanged files, etc.:
  - `messages_v29` contains the list of all messages exchanged
  - `convesations_v29` contains the list of active conversations as showed in the "Chats" screen of the app
  - `encrypted_cids_v29` contains the conversation ids of the secret chats.

TELEGRAM

```
sqlite> select * from encrypted_cids_v29;
encrypted_id = -1913433264
         cid = -2147483648

encrypted_id = -232713407
         cid = -2147483650

encrypted_id = 2055195409
         cid = -2147483649

...
```

```
sqlite> select * from messages_v29;
...
        mid = 800000023
        cid = -2147483648
    localMid = 0
    message = Secret...? :D
      media =
    from_id = 243610671
      to_id = -2147483648
        ...

...
```

TELEGRAM

- As expected, also with Telegram is possible to carve out deleted records from SQLite database… but there is one more "feature".
- Telegram **messages from secret chats are stored in clear** in the `messages_v29` table, like all the other messages.
- On the other hand **we will not find the screen snapshot**, as apparently Telegram properly clears the screen when the fade-out event happens.

SIGNAL

- Less popular than the previous two, but still important to know.
- It delivers what promises: its database **/Document/Signal.sqlite**, containing all its data, **is fully encrypted**. However, two things that are in clear:
  - The attachments exchanged are stored in clear in the /Document/Attachments/ folder.
  - Screen Snapshots can be retrieved as well. Signal has an option "**Enable Screen Security**" that would prevent this, but for some reason is not set by default.

iOS MESSAGING RECAP

	WhatsApp	Telegram	Signal
Standard message content in clear?			
“Secret chat” message content in clear?	n/a		
Sender/recipient information?			
Timestamps?			
SQLite carving of deleted records?			
Snapshot?			

THANK YOU

Pasquale Stirparo, Ph.D.

- Threat Intelligence Analyst and Incident Responder
- Incident Handler @ SANS ISC, Advisor @ Europol EC3
- GCFA, GREM, OPST, OWSE, ECCE

 **pstirparo@gmail.com**

 **@pstirparo**

 **http://www.linkedin.com/in/pasqualestirparo**

 **https://isc.sans.edu**

 **https://github.com/pstirparo/mac4n6**