CCIRC: Cyber Crime Investigation & Research Center

How to Decrypt or Read WhatsApp DataBase File in Android?

Contributor: Sakshi Baliyan, Vineet Kumar and in association with CCIRC team (http://www.ccirc.in/)

Table of Content:

Abstract:

This article contains a precise overview of WhatsApp – a popular mobile messenger application. It provides an explanation on how WhatsApp gets installed, works, and deals with its data using XMPP network. This research paper also describes that WhatsApp uses **"msgstore.db"** and **"wa.db"** (which is a SQLite database) file to save the message and relevant media like; images, audio, video, etc. on an Android device. Along with explaining each basic attribute of WhatsApp application, the paper also tells about the encrypted form of "**msgstore.db**" and how forensic strategy should be used in an effective way to break out the secret database of "**msgstore.db**". Execution and retrieval of "**msgstore.db**" hidden data using WhatsApp Xtractor and pyCrypto command are also mentioned in the given paper.

Keywords: *WhatsApp, msgstore.db.crypt, XMPP, Python*

Introduction:

“WhatsApp Messenger” is a free messaging application. It is a proprietary, cross–platform, instant messaging subscription service available for various feature phones and smartphone platforms such as iPhone, Android, Blackberry, Nokia and Windows. In a simple term, it’s an instant messaging application which has been introduced as a replacement of slump SMS function in 2009 by former employees of Yahoo – *Brian Action & Jan Koum*. WhatsApp uses same internet access (2G, 3G, 4G & Wifi) to exchange messages over a network, which usually a phone device utilizes to execute other internet based applications (browser, apps).

Recently, WhatsApp was acquired by world’s youngest entrepreneur **“Mr. Mark Zukerberg”** after gaining popularity and being listed among one of the popular messaging application.

A Brief of How WhatsApp Works

First, find out the right app store for your device and start downloading the WhatsApp application from it. Get more clarification from the given options:

Android Devices *– Google Play Store*
Symbian Devices *– OVI Store*
Apple Devices *– iTunes*
BlackBerry World *– BlackBerryWorld*
Windows Devices *– Windows App Store*

It is really a smart app as it automatically synchronizes all the contacts on the device once it gets installed on it. After complete installation, **"com.WhatsApp"**automatically starts receiving signals and begins the execution of **"ExternalMediaMange"** & **"MessageService"** programs. Thereafter, execution of these services, WhatsApp initiates the transformation of data using the phone network and saves the entire database into a SQLite database file format (*msgstore.db and wa.db*).

But unfortunately, WhatsApp endows strong encryption over these SQLite database files and converts them to simple **"msgstore.db"** into **"msgstore.db.crypt"** using a python script. Reading an SQLite file using SQLite Viewer is a quite simple task, but becomes a strenuous work when it comes to open encrypted **"msgstore.db.crypt file"** of WhatsApp, and that is where WhatsApp Forensic comes in the limelight.

Ideal Protocol For WhatsApp: XMPP (Extensible Messaging and Presence Protocol)

XMPP protocol is a core factor behind the real heroic execution of absolute data handling in WhatsApp data transformation.

XMPP is the abbreviation for Extensible Messaging and Presence Protocol. This protocol is the most popular communication protocol for real-time, instant messaging, presence information and contact list maintenance. It is an open standard and uses an open system approach of development and application. The protocol is designed for signaling VoIP, video, file transfer, gaming, Internet of Thing.

Why XMPP??

- **Security:** The XMPP provides strong security for communication over the network. Actually, it provides encryption during both; connection establishment and authentication. It uses the Simple Authentication and Security Layer (SASL) encryption for connection establishment. And Transport Layer Security (TSL) for encryption at the time of Authentication. XMPP servers can be isolated from public XMPP network.

- **Open Standard:** XMPP is introduced by the Internet Engineering Task Force for instant messaging and presence technology. When it comes to claiming the royalty, there is no issue of implementing support.
- **Flexibility:** XMPP provides custom functionality, to maintain interoperability. This application also includes a group chat, network management, content syndication, collaboration tools, file sharing, gaming, remote system control and monitoring, Geo-location; cloud computing, VoIP and middleware.
- **Decentralization:** The XMPP network works similarly to the emails; anyone can run their own server like individual email accounts. None of them can act as master server so, decentralized client-server architecture is used to deploy XMPP with an unlimited number of server establishment.

Data Acquisition: Hardware & Software (In Android Device)

We have already highlighted in the above section of this research paper about the data storage method of WhatsApp. WhatsApp stores its all the database in a **"msgstore.db"** and **"wa.db"** files which a paradigm of SQLite data files.

What is SQLite DataBase?

SQLite Database is a RDMS (Relational Database Management System) but don't function like common email-client server structure as other database engine works. Means, it does need to bring data from a server to the local machine. SQLite contains set of library to read, write and execute the database itself instead of driving data from the server to an application. It directly performs actions on disk file which contains all the attributes of SQL database such as tables, indices, triggers and view. It is fast and reliable which gives it a unique popularity among database management systems. E.g. Web browsers, android apps, Whatsapp.

In our task, we have to extract or read these files as they carry every data which helps in crucial investigation while examining a forensic episode. A phone devices or WhatsApp can be a vital point of concern if a crime has been done using WhatsApp such as image violation, disclosing important details and anything.

A non-encrypted SQLite **"msgstore.db"** data file can be viewed using several SQLite applications like SQLite Viewer, SQLite Manager, etc. (*These apps are available in Google Play Store*).

Decrypting WhatsApp “msgstore.db.crypt” – A cumbersome Task

Encrypted WhatsApp data files makes acquisition of database more complicated. These data encrypted by implementing Advanced Encrypted Standard (AES) cipher. AES is a technology which specially used to encrypt the electronic data and using the same symmetric-key algorithm to lock the data. Means a single cipher key used to decrypt or encrypt the same **“msgstore.db”** file.

In further section, we will discuss about how to break the cipher key of encrypted WhatsApp SQLite data file and extract data from volatile memory using python script and WhatsApp Xtractor.

Volatile & Non Volatile Memory:

It’s a memory space which works like as RAM in an Android device. Means, volatile memory does not permanently save any data and clean itself when the power supply goes off. In contrast to volatile memory, non-volatile memory which is also called as NAND flash stores the entire WhatsApp database at a specific location in SD card.

Location of **“msgstore.db.crypt”** file in Android device: *SDCard/WhatsApp/Databases*

Note: The location of “**msgstore.db.crypt”** can be varied in various phone devices.

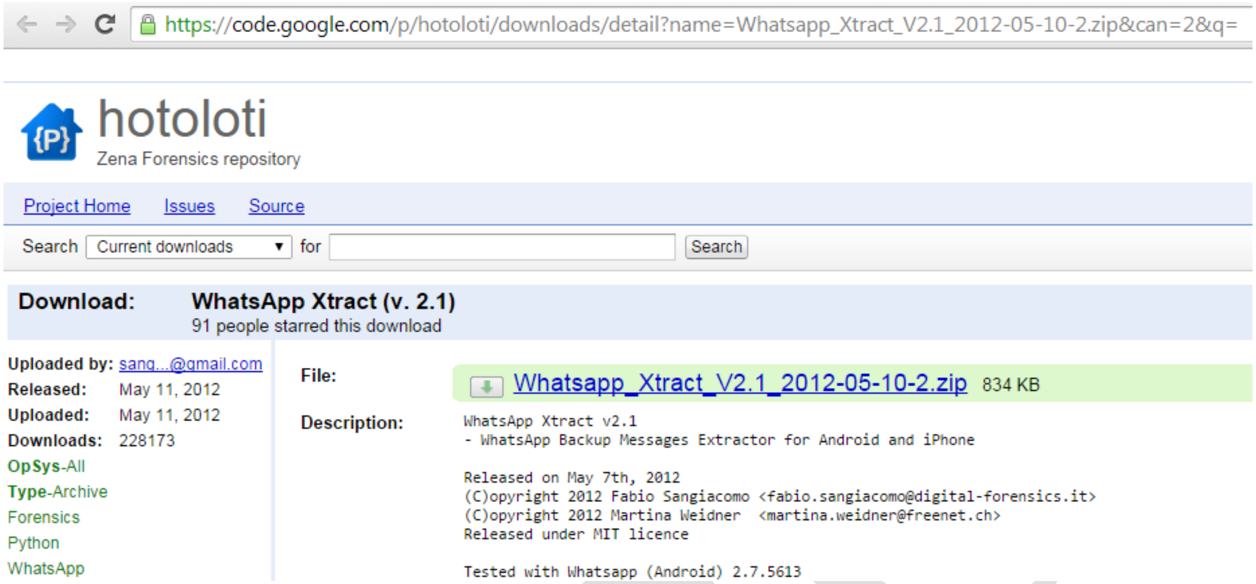
How to Extract Encrypt data of “msgstore.db.crypt” File from Non-Volatile Memory?

Here, we are going to extract data from **“msg.db.crypt”** database file using python so we need to save WhatApp database file on our system. The process involve some files and software and these are listed below:

- WhatsApp Database file (msgstore.db.crypt)
- Whatsapp_ Xtract Xtract_V2.1
- ActivePython (32bit version or 64 bit version)

For an Android:

1. **Firstly**, we need to download Whatsapp_Xtract_V2.1 and Extract this Archive file to a folder on your computer.


https://code.google.com/p/hotoloti/downloads/detail?name=Whatsapp_Xtract_V2.1_2012-05-10-2.zip&can=2&q=
hotoloti
Zena Forensics repository
Project Home
Issues
Source
Search
Current downloads
for
Search

Download: **WhatsApp Xtract (v. 2.1)**

91 people starred this download

Uploaded by: sang...@gmail.com
Released: May 11, 2012
Uploaded: May 11, 2012
Downloads: 228173
OpSys-All
Type-Archive
Forensics
Python
WhatsApp

File: Whatsapp_Xtract_V2.1_2012-05-10-2.zip 834 KB

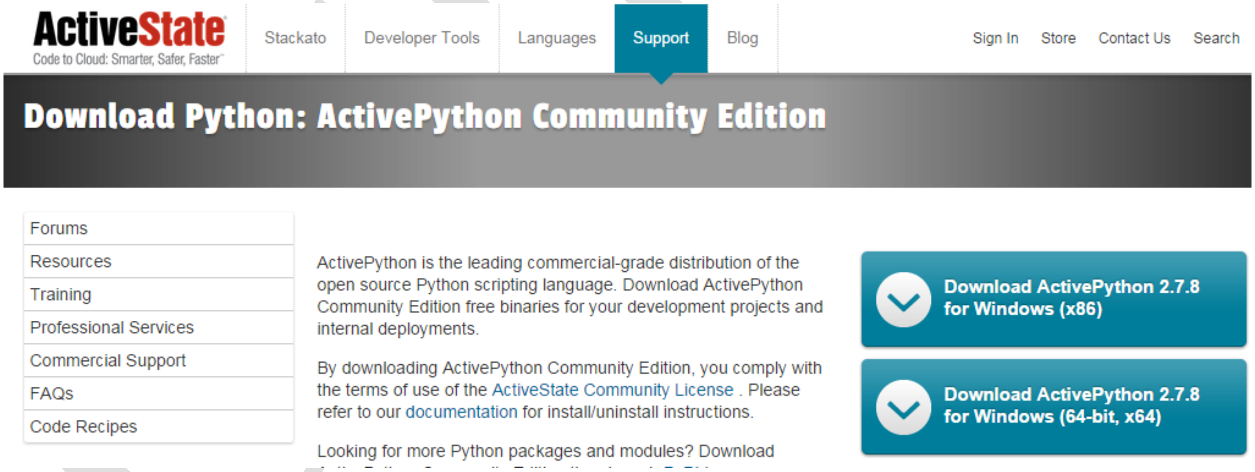
Description:

```
WhatsApp Xtract v2.1
- WhatsApp Backup Messages Extractor for Android and iPhone

Released on May 7th, 2012
(C)opyright 2012 Fabio Sangiacomo <fabio.sangiacomo@digital-forensics.it>
(C)opyright 2012 Martina Weidner  <martina.weidner@freenet.ch>
Released under MIT licence

Tested with Whatsapp (Android) 2.7.5613
```

2. **Secondly**, you need python setup and PyCrypto library (for android msgstore.db.crypto file). You can easily use it by downloading ActivePython (available for Windows 32bit version and 64 version).



Download Python: ActivePython Community Edition

ActivePython is the leading commercial-grade distribution of the open source Python scripting language. Download ActivePython Community Edition free binaries for your development projects and internal deployments.

By downloading ActivePython Community Edition, you comply with the terms of use of the ActiveState Community License . Please refer to our documentation for install/uninstall instructions.

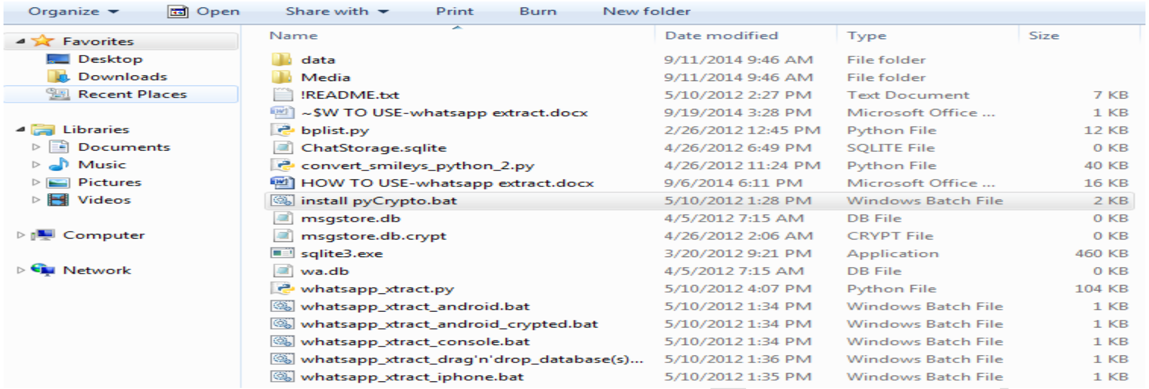
Looking for more Python packages and modules? Download

3. **After all this**, we need to copy the **“msgstore.db.crypt”** file from the WhatsApp database.

Location: */sd card /whatsApp/databases/msgStore.db.crypt.*

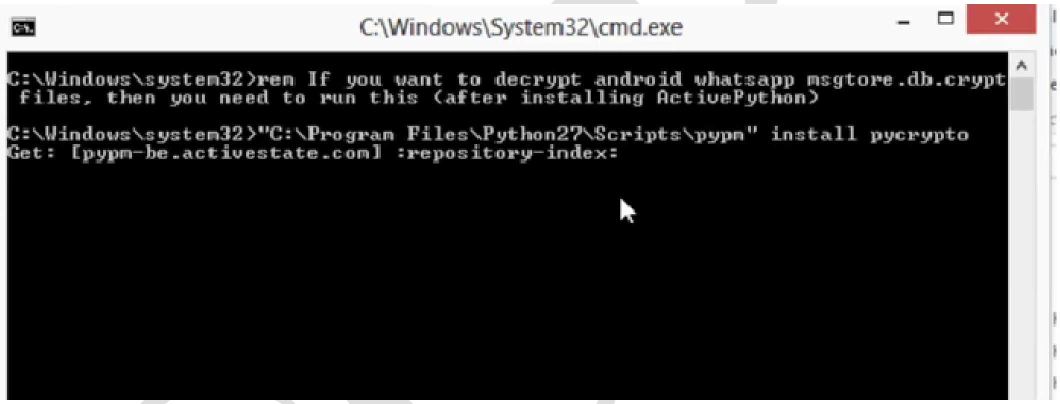
4. Then you need to install **ActivePython** at *C:\Program files\Python27* location.

5. After that, **open whatsApp Xtract archive file** and right click on **install PyCrypto.bat** to **run it as administrator.**



Name	Date modified	Type	Size
data	9/11/2014 9:46 AM	File folder	
Media	9/11/2014 9:46 AM	File folder	
!README.txt	5/10/2012 2:27 PM	Text Document	7 KB
~$W TO USE-whatsapp extract.docx	9/19/2014 3:28 PM	Microsoft Office ...	1 KB
bplist.py	2/26/2012 12:45 PM	Python File	12 KB
ChatStorage.sqlite	4/26/2012 6:49 PM	SQLITE File	0 KB
convert_smileys_python_2.py	4/26/2012 11:24 PM	Python File	40 KB
HOW TO USE-whatsapp extract.docx	9/6/2014 6:11 PM	Microsoft Office ...	16 KB
install pyCrypto.bat	5/10/2012 1:28 PM	Windows Batch File	2 KB
msgstore.db	4/5/2012 7:15 AM	DB File	0 KB
msgstore.db.crypt	4/26/2012 2:06 AM	CRYPT File	0 KB
sqlite3.exe	3/20/2012 9:21 PM	Application	460 KB
wa.db	4/5/2012 7:15 AM	DB File	0 KB
whatsapp_xtract.py	5/10/2012 4:07 PM	Python File	104 KB
whatsapp_xtract_android.bat	5/10/2012 1:34 PM	Windows Batch File	1 KB
whatsapp_xtract_android_crypted.bat	5/10/2012 1:34 PM	Windows Batch File	1 KB
whatsapp_xtract_console.bat	5/10/2012 1:34 PM	Windows Batch File	1 KB
whatsapp_xtract_drag'n'drop_database(s)...	5/10/2012 1:36 PM	Windows Batch File	1 KB
whatsapp_xtract_iphone.bat	5/10/2012 1:35 PM	Windows Batch File	1 KB

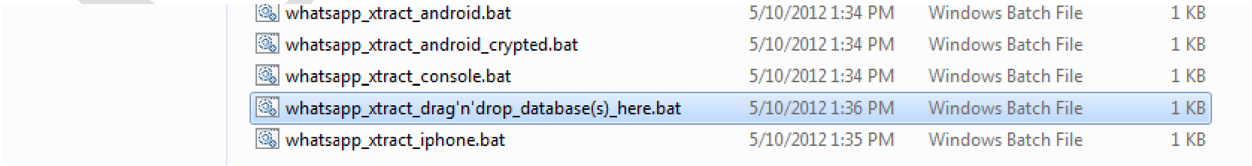
As you run the file the following cmd will run some commands automatically.



```
C:\Windows\system32>rem If you want to decrypt android whatsapp msgtore.db.crypt
 files, then you need to run this (after installing ActivePython)

C:\Windows\system32>"C:\Program Files\Python27\Scripts\pypm" install pycrypto
Get: [pypm-be.activestate.com] :repository-index:
```

6. Or you can simply **drag and drop** the **database file** to s **Whatapp_xtract_drag'n'drop_database _here.bat**



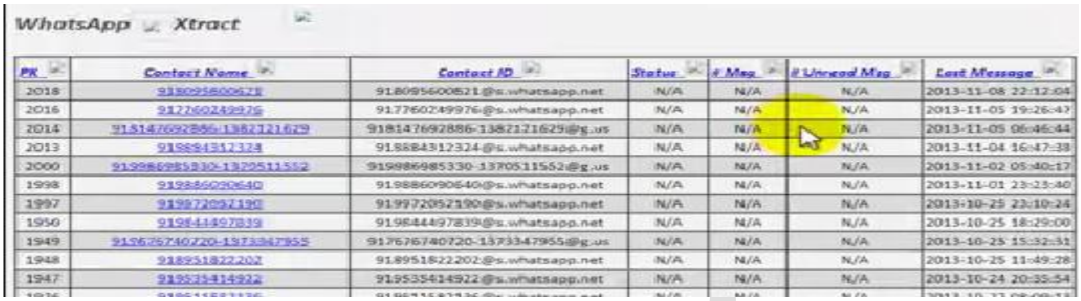
whatsapp_xtract_android.bat	5/10/2012 1:34 PM	Windows Batch File	1 KB
whatsapp_xtract_android_crypted.bat	5/10/2012 1:34 PM	Windows Batch File	1 KB
whatsapp_xtract_console.bat	5/10/2012 1:34 PM	Windows Batch File	1 KB
whatsapp_xtract_drag'n'drop_database(s)_here.bat	5/10/2012 1:36 PM	Windows Batch File	1 KB
whatsapp_xtract_iphone.bat	5/10/2012 1:35 PM	Windows Batch File	1 KB

7. You can execute the above task using **python commands**, python commands are as follows:

python Whatsapp_Xtract.py –i msgstore.db –w wa.db (if wa.bd is available)

else use python whatsapp_xtract.py –i msgstore.cd
or (for crypted db)

python whatsapp_xtract.py –i msgstore.db.crypt



WhatsApp Xtract

PK	Contact Name	Contact ID	Status	# Msg	# Unread Msg	Last Message
2018	918095600621	918095600621@s.whatsapp.net	N/A	N/A	N/A	2013-11-08 22:12:04
2016	917760249976	917760249976@s.whatsapp.net	N/A	N/A	N/A	2013-11-05 19:26:47
2014	918147692886-1382121629	918147692886-1382121629@g.us	N/A	N/A	N/A	2013-11-05 06:46:44
2013	918884312324	918884312324@s.whatsapp.net	N/A	N/A	N/A	2013-11-04 16:47:38
2000	919986985330-1370511552	919986985330-1370511552@g.us	N/A	N/A	N/A	2013-11-02 05:40:17
1998	919886090640	919886090640@s.whatsapp.net	N/A	N/A	N/A	2013-11-01 23:23:40
1997	919972052190	919972052190@s.whatsapp.net	N/A	N/A	N/A	2013-10-25 23:10:24
1950	919844497839	919844497839@s.whatsapp.net	N/A	N/A	N/A	2013-10-25 18:29:00
1949	917676740720-1373347955	917676740720-1373347955@g.us	N/A	N/A	N/A	2013-10-25 15:32:31
1948	918951822202	918951822202@s.whatsapp.net	N/A	N/A	N/A	2013-10-25 11:49:28
1947	919535414922	919535414922@s.whatsapp.net	N/A	N/A	N/A	2013-10-24 20:35:54

8. **Once you are finished** with the command, your browser will open and show all the

The size of resultant file in .html format will be slightly larger than .db database file.

Conclusion:

WhatsApp Forensic is the methodology to decrypt and read hidden WhatsApp database by enforcing the python command over it. It's an effective and easy way, but you need to get a little tricky to deal with all these technical terms such as SQLite Database, XMPP, Python language, etc. You can also become a forensic expert and unfold the data of WhatsApp by using the above given set of instructions.

Sources:

- http://en.wikipedia.org/wiki/WhatsApp
- http://en.wikipedia.org/wiki/AdvancedEncryption_Standard
- http://en.wikipedia.org/wiki/SQLite
- http://www.sqlite.org/about.htm
- https://code.google.com/p/hotoloti/downloads/list Python
- http://blog.digital-forensics.it/2012/05/whatsapp-forensics.html
- http://sch3m4.github.io/wforensic
- http://www.manejandodatos.es/2014/02/whatsapp-database-decrypt/
- https://www.facebook.com/prakhar.tricks/posts/119341444931820inAndroid76373.S.585 2503662949072897

- http://bas.bosschert.nl/steal-whatsapp-database/
- http://www.triadsquare.com/mobile-security
- http://www.caseite.com/content/smartphone-forensics-recovering-evidence-3rd-party-apps
- http://www.backuptrans.com/tutorial/decrypt-read-chats-from-whatsapp-backup-file-on-android.html
- http://www.triadsquare.com/mobile-security/66-how-to-extract-chats-from-whatsapp-with-db-file
- https://www.youtube.com/watch?v=pkfNKlI01Y8