[Case Study] WhatsApp Forensics: Decrypt Encrypted WhatsApp Database Files with SalvationDATA’s Free Forensic Tool

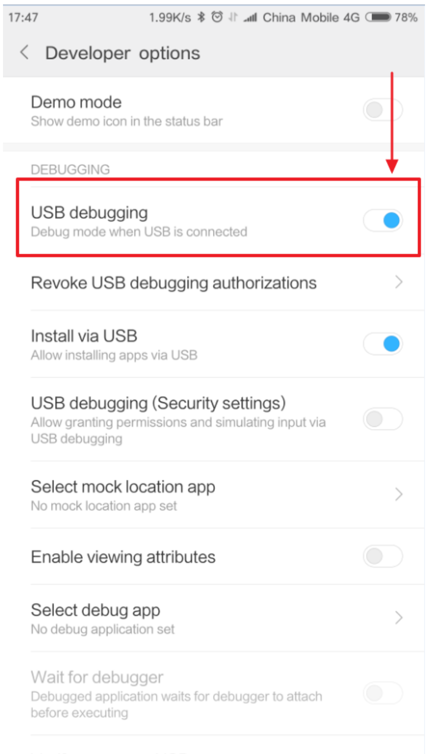
Editor’s note:

At the beginning of this month, we held a webinar talking about the forensic technics to extract WhatsApp data, bypass WhatsApp security mechanism, and decrypt encrypted WhatsApp database files. And we released a free forensic tool that is capable of decrypting the database and extract an unencrypted database of WhatsApp. In this article, SalvationDATA forensic experts will explain how to use this free tool to acquire important evidentiary data from WhatsApp.

Now let’s see how to use this free tool to carry out a WhatsApp forensic workflow.

I. Extraction or decrypt WhatsApp database backup

Step 1. Connect your smartphone to the PC with USB debugging enabled.



17:47 1.99K/s China Mobile 4G 78%

Developer options

Demo mode
Show demo icon in the status bar ○

DEBUGGING

USB debugging
Debug mode when USB is connected ●

Revoke USB debugging authorizations ›

Install via USB
Allow installing apps via USB ●

USB debugging (Security settings)
Allow granting permissions and simulating input via USB debugging ○

Select mock location app
No mock location app set ›

Enable viewing attributes ○

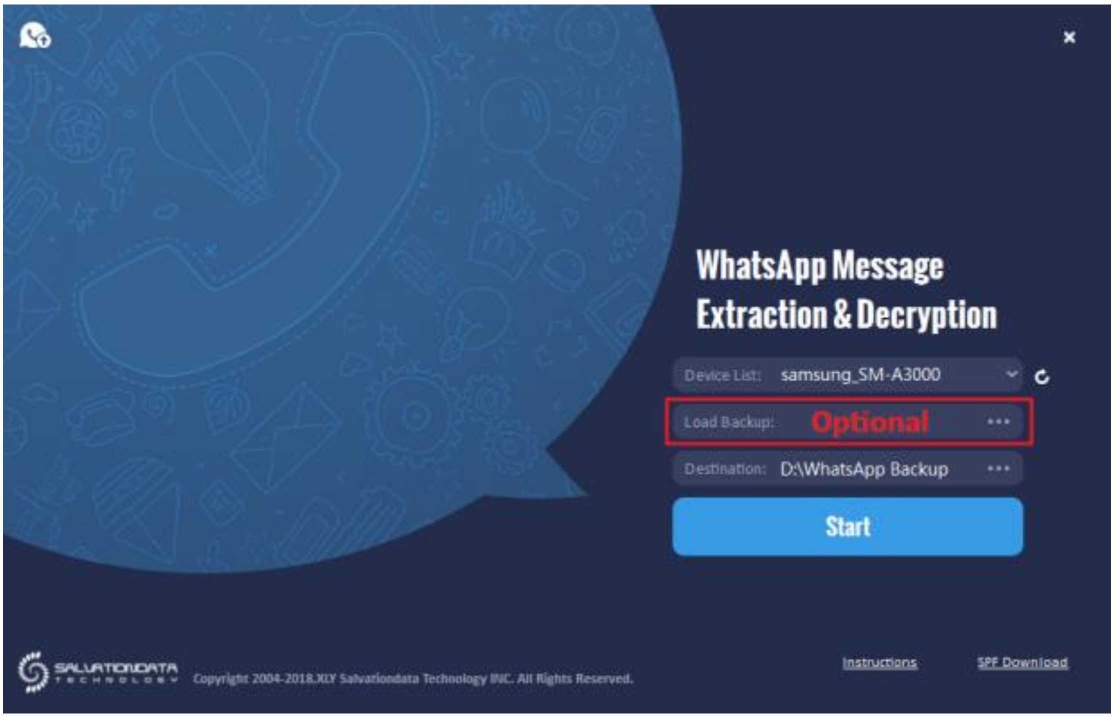
Select debug app
No debug application set ›

Wait for debugger
Debugged application waits for debugger to attach before executing ○

Step 2. Start the WhatsApp forensic tool, select the target smartphone from the device list.

Step 3. Set your destination path for backup file storage.

Step 4 (optional). Load your encrypted backup. P.S. this step is optional, only load back up when you already have encrypted WhatsApp database files at hand.



WhatsApp Message Extraction & Decryption

Device List: samsung_SM-A3000

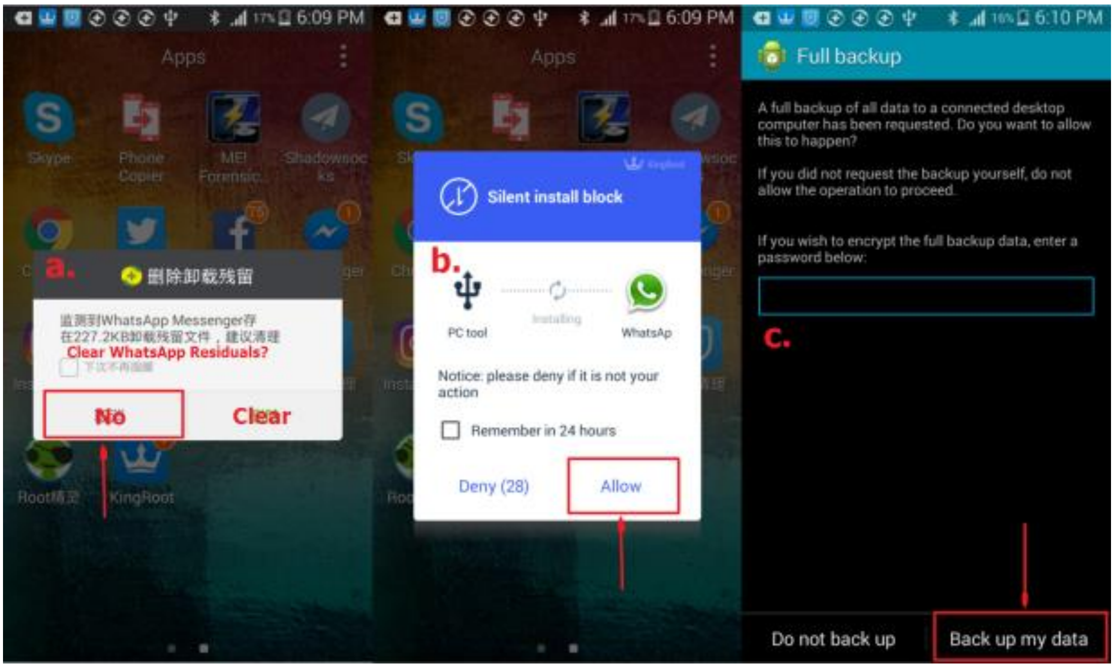
Load Backup: Optional

Destination: D:\WhatsApp Backup

Copyright 2004-2018.XLY Salvationdata Technology INC. All Rights Reserved.

Step 5. Press Start and follow the instructions to proceed. Be extremely cautious,

The tool will first delete the current WhatsApp application, make sure to press No if smartphone notifies you to clear residuals.
Then the tool will install an old version WhatsApp, make sure to allow installation if a notification pops up.
After downgrade successful, the tool will create and extract backup, press “Backup my data” to allow backup.



a. 删除卸载残留

监测到WhatsApp Messenger存在227.2KB卸载残留文件，建议清理

Clear WhatsApp Residuals?

□ 下次不再提醒

b. Silent install block

Notice: please deny if it is not your action

□ Remember in 24 hours

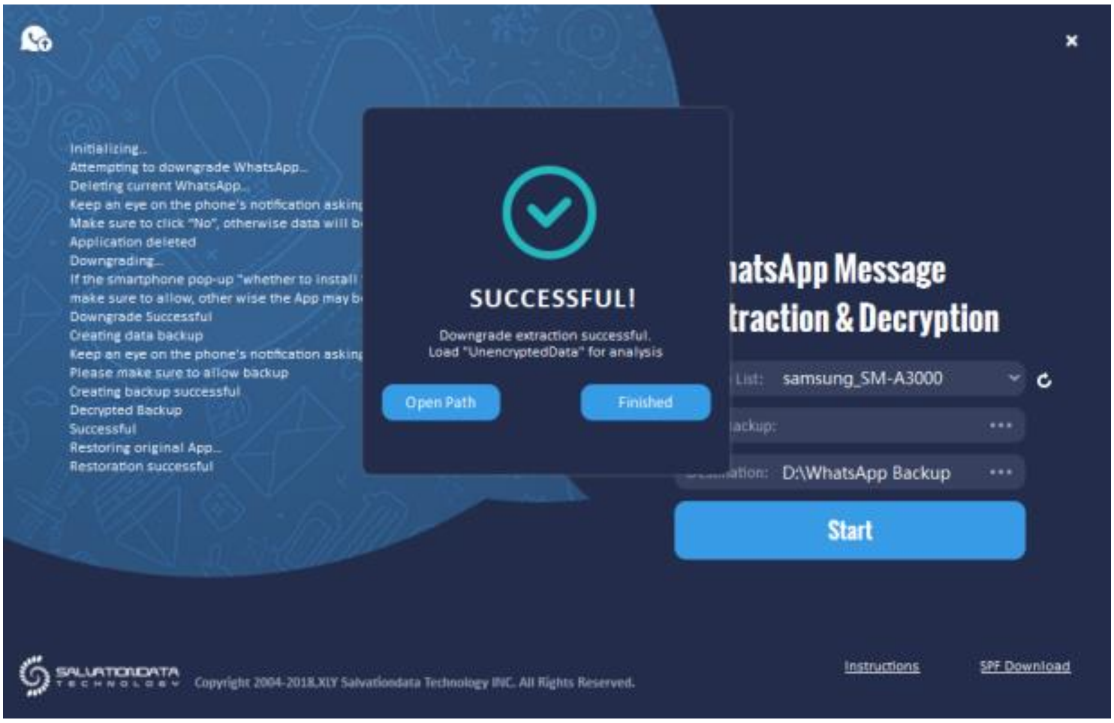
c. Full backup

A full backup of all data to a connected desktop computer has been requested. Do you want to allow this to happen?

If you did not request the backup yourself, do not allow the operation to proceed.

If you wish to encrypt the full backup data, enter a password below:

Step 6. After the backup is complete, wait for the tool to restore the original WhatsApp application and finish the process.



```
Initializing...
Attempting to downgrade WhatsApp...
Deleting current WhatsApp...
Keep an eye on the phone's notification askin
Make sure to click "No", otherwise data will b
Application deleted
Downgrading...
If the smartphone pop-up "whether to install
make sure to allow, other wise the App may b
Downgrade Successful
Creating data backup
Keep an eye on the phone's notification askin
Please make sure to allow backup
Creating backup successful
Decrypted Backup
Successful
Restoring original App...
Restoration successful
```

SUCCESSFUL!

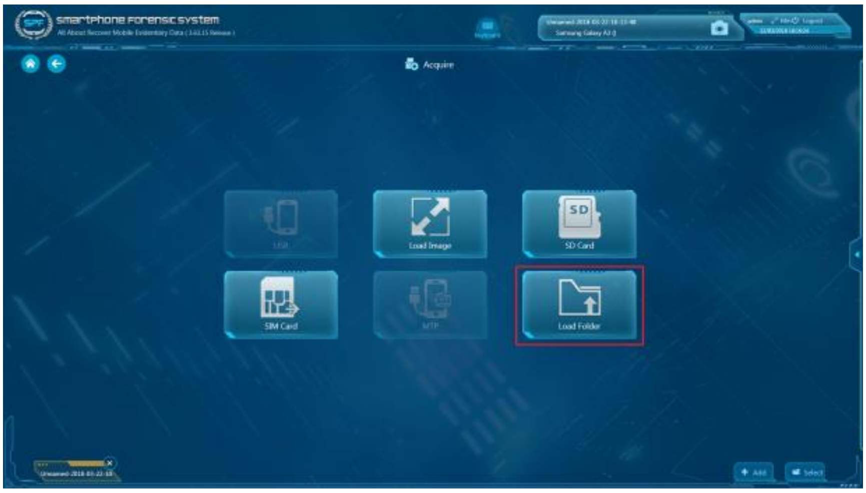
Downgrade extraction successful.
Load "UnencryptedData" for analysis

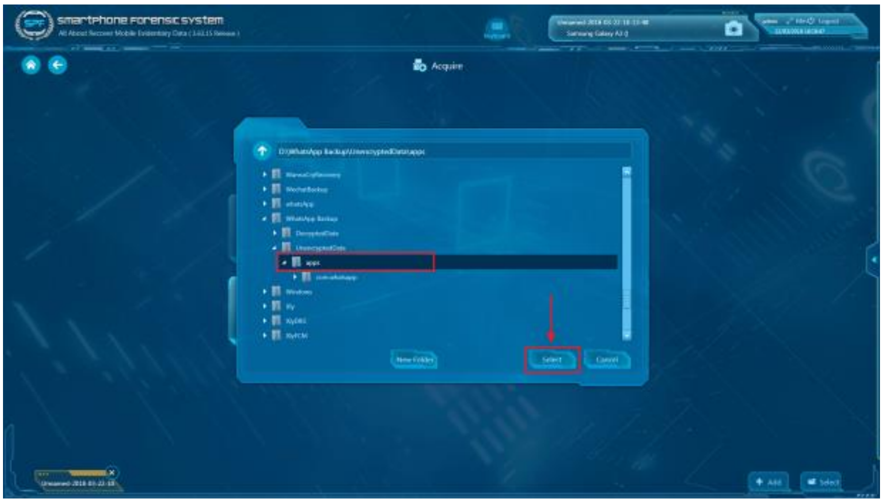
II. Load and analyze the extracted backup

Step 1. Start SPF(Smartphone Forensic System), or any other smartphone forensic tools you have that are capable of forensically extract and analyze data from smartphone backup files.

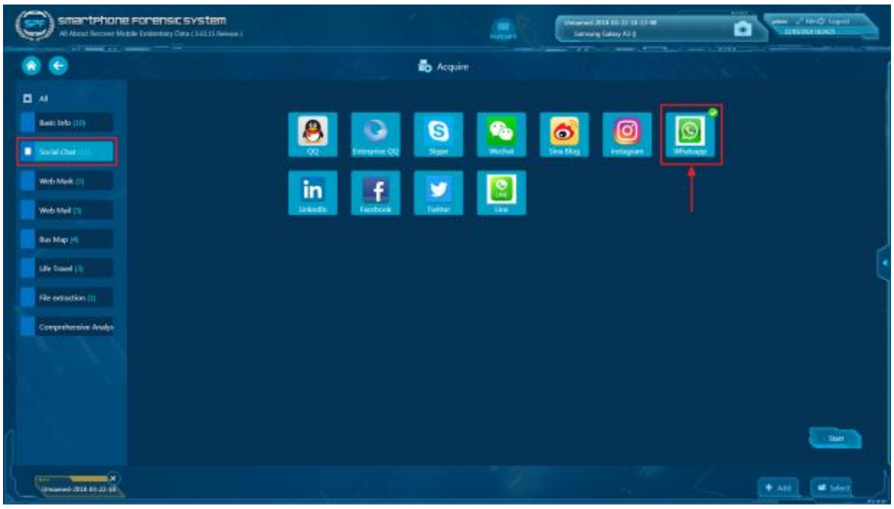
Step 2. Create Task-> Acquire, and in the source selection page, click "Load Folder", and then set the destination path to where you saved the WhatsApp backup files.

P.S. Choose "DecryptedData" or "UnencryptedData" for analysis. Remember the target folder must be "apps" or "com.WhatsApp", otherwise SPF will not be able to find WhatsApp data.

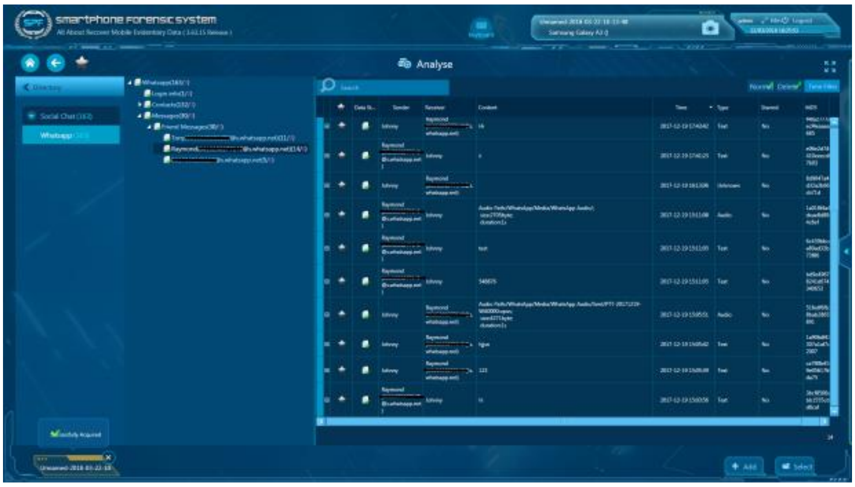




Step 3. Select WhatsApp for extraction and press "Start"



Step 4. Check out the extraction results and generate a report if needed.



Conclusion

This article is an operation guidance on how to use SalvationDATA's WhatsApp forensic tool and SPF to decrypt WhatsApp encryption and how to extract unencrypted WhatsApp backup from unrooted smartphones.

You can find the motioned tools form our resources page. Our WhatsApp forensic tool is completely free to use. We welcome all our customers to download this tool, and hope it could help the DFIR community to solve more cases!