# [Case Study] Mobile Forensics: Easy Solution for Apps Data Extraction

from Unrooted Android Phone

Editor's note: If you are a forensic investigator, I'm sure you are often bothered by the problem caused by Android operating system's securities of a smartphone.   Because of user authorization restrictions, you simply cannot directly read the digital data stored in the smartphone's memory chips. Therefore, the apps data cannot be extracted directly.
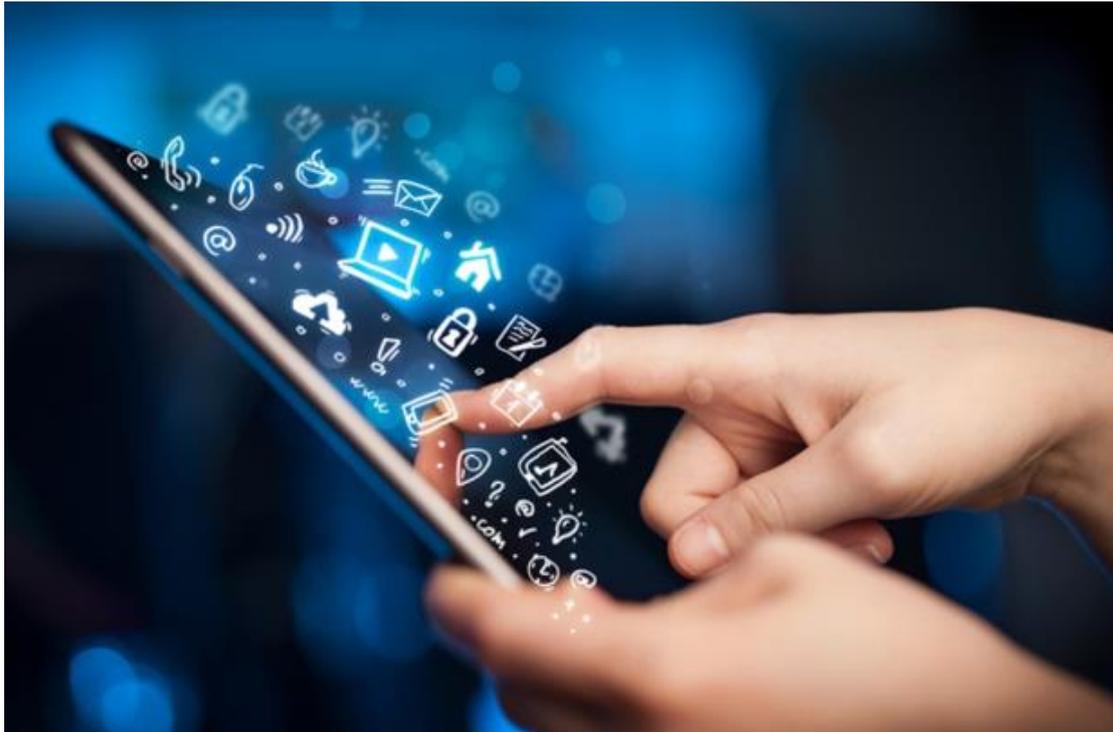

So how do we extract the apps data from smartphones? Normally we need to root the devices to get full access to the system before we extract the data.   But rooting is not easy, if you've been doing mobile forensics for a while, you've probably noticed gaining root access on most devices is much harder than it once was.
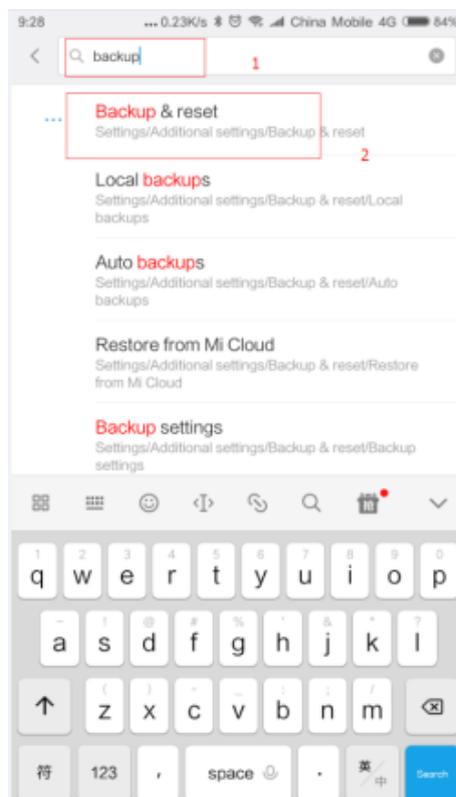
But, there is a solution for you to avoid rooting Android devices. Let's take a look at how SalvationDATA forensic experts extract the apps data without rooting the device: Demonstration on MI(Xiaomi) Note 3.
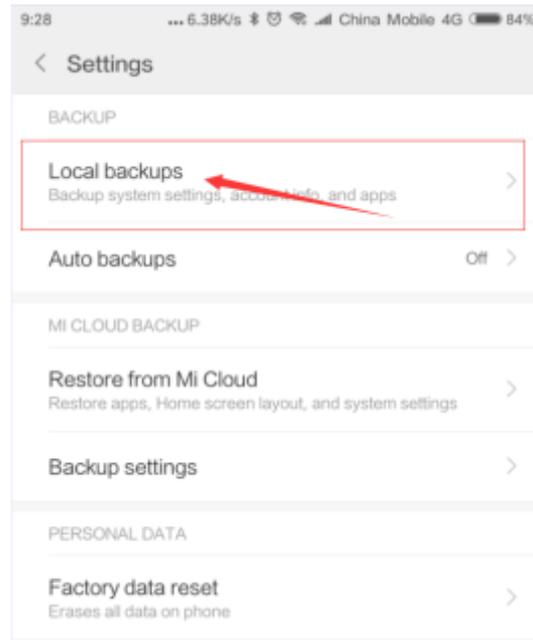
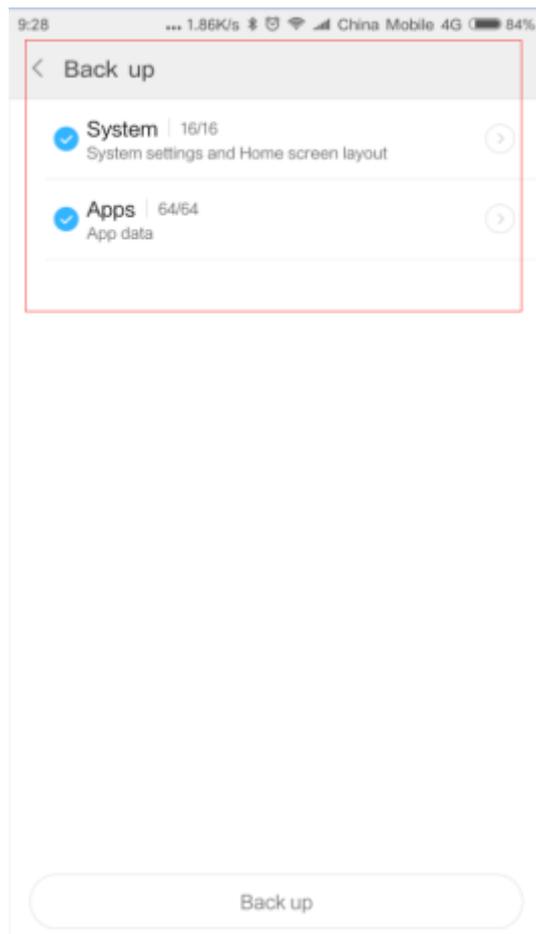## Create BACKUP file from (Xiaomi) Note 3

Step1. Go to the settings page.
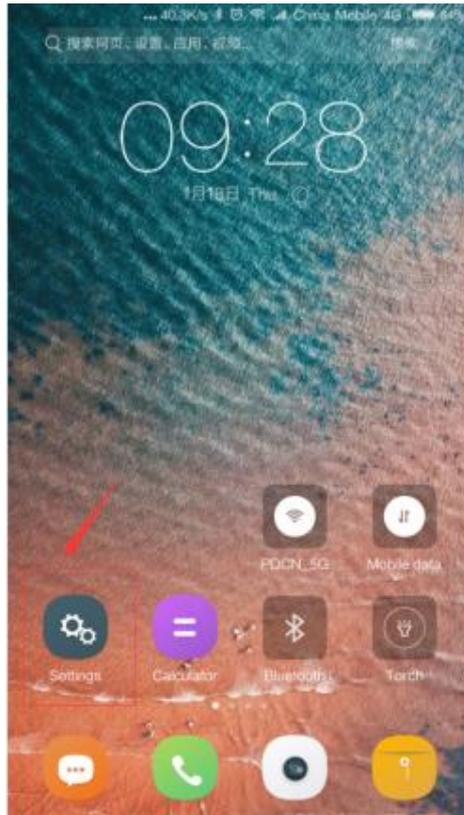
Step2. Type "backup" on the top to search and quickly locate "Backup & reset", select it.
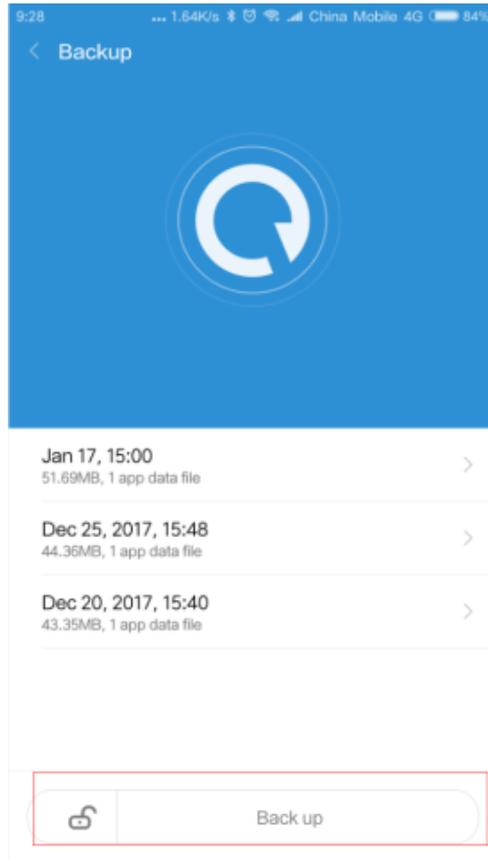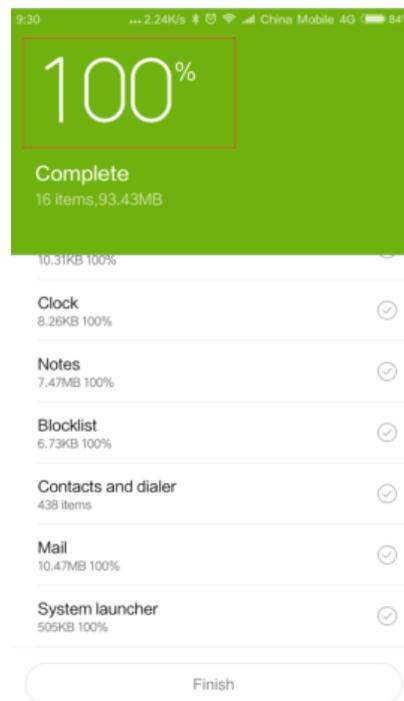

Step3. Select "Local Backups"

Step4. Now select the items you would like to backup, although all the items are already selected by default.

Step5. Tap on the "Back up" button to start.

Step6. After the backup progress completed, you will get the Finish message on your device screen. just tap the Finish button and you have already successfully created the backup.
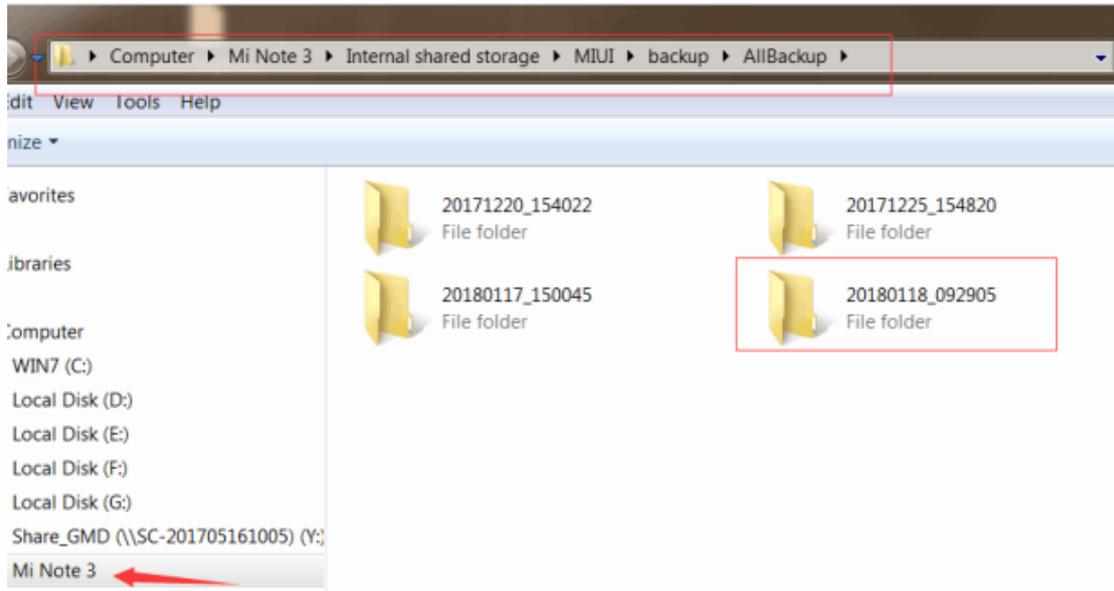
Start to extract the backup file by using SPF (Smartphone Forensic System)

Step1. Connect your phone to a computer, and find the backup in the SD card, from the following path:
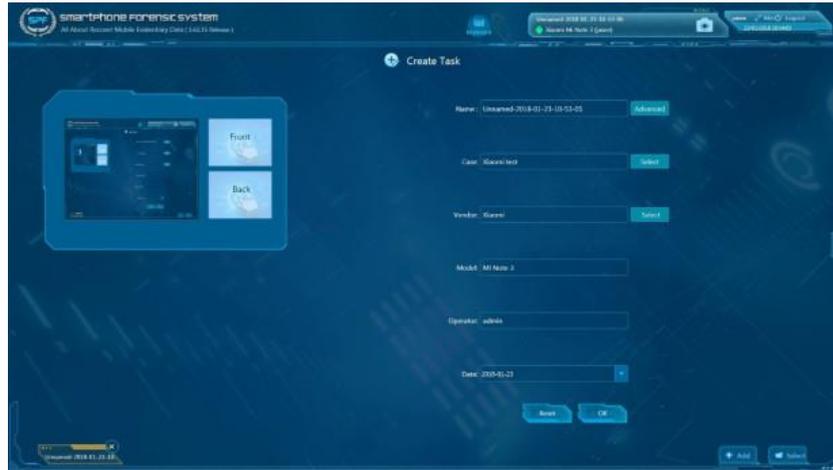
SD card/MIUI/backup/Allbackup

The backup folder is named according to the time it is created.
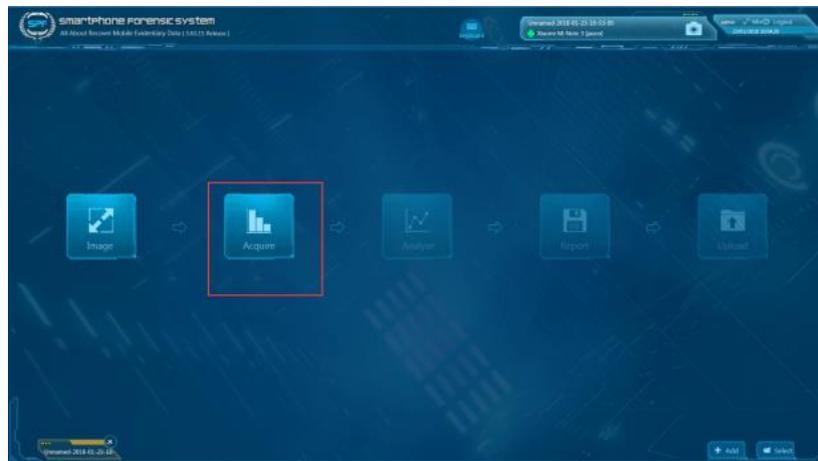

Step2. Run SPF (Smartphone Forensic System) and the phone will be automatically detected when it is connected to the computer.
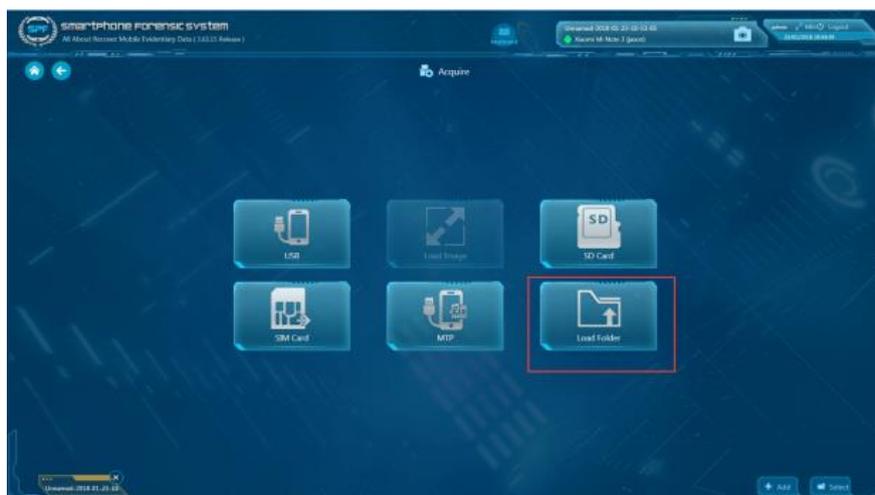

Step3. Create a task.

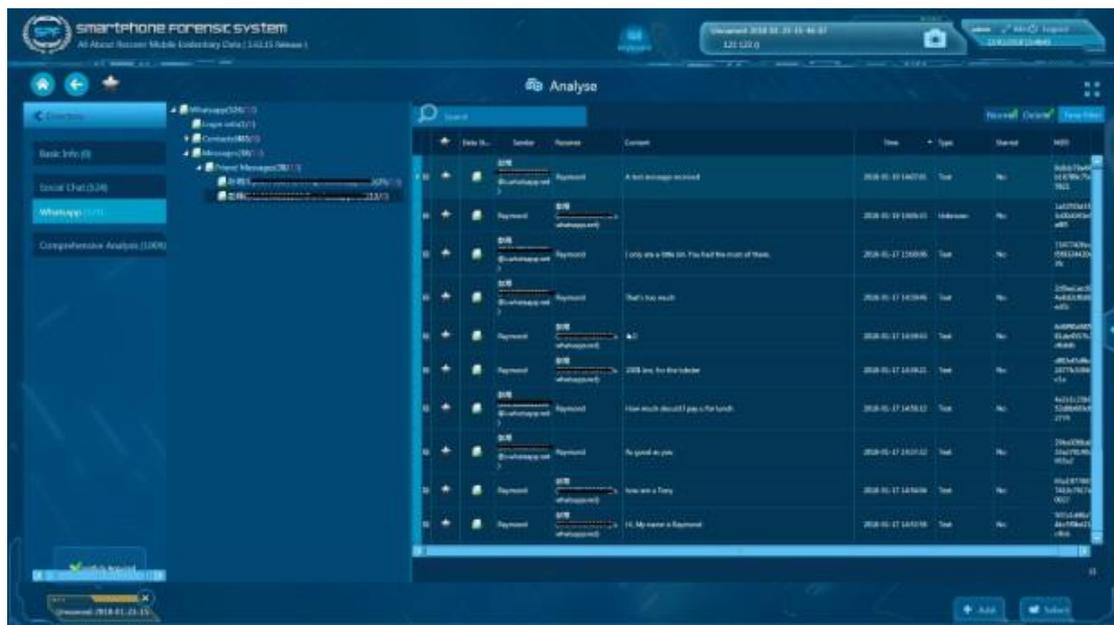**Step4.** Select acquire to choose which method you need.

Step5. Click load folder and load backup file folder.

Step6. Now select the items you would like to extract data. (For demonstration we selected WhatsApp only).

Step7. After acquisition process is done, you will see this analysis page below.

Conclusion

In this demonstration, we successfully extracted data from WhatsApp without rooting the device and analyzed the backup file by using SmartPhone Forensic System (SPF) to find the evidentiary data. So, this method mentioned above provides you an easy solution to extract apps data from unrooted android phones.