[Case Study] Mobile Forensics: How to Extract data from a bricked phone?

Editor's note:

Jan-2018, the Sichuan police solved a gambling case, a Samsung smartphone was found when capturing the suspect. And the suspect refused to give up the password. The investigator mistakenly corrupted the phone's operating system when trying to flash it, and the phone couldn't power up. Let's see how SalvationDATA forensic experts managed to extract data from such corrupted device.

Analysis

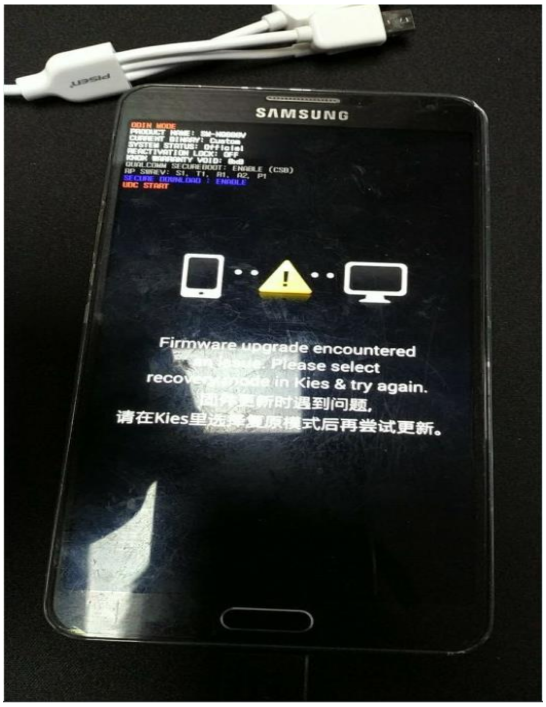
1. The phone couldn't boot up, the firmware is corrupted. This is caused by some error when flashing the phone. So we have two options to deal with this: 1. Flash the phone with official package except for the data partition. 2.Flash third-party ROM.

2. In order to extract the smartphone data after flashing, choosing a third-party ROM seems more reasonable.

3. After system restored, we can use SPF to extract and analyze the smartphone data.

Operation

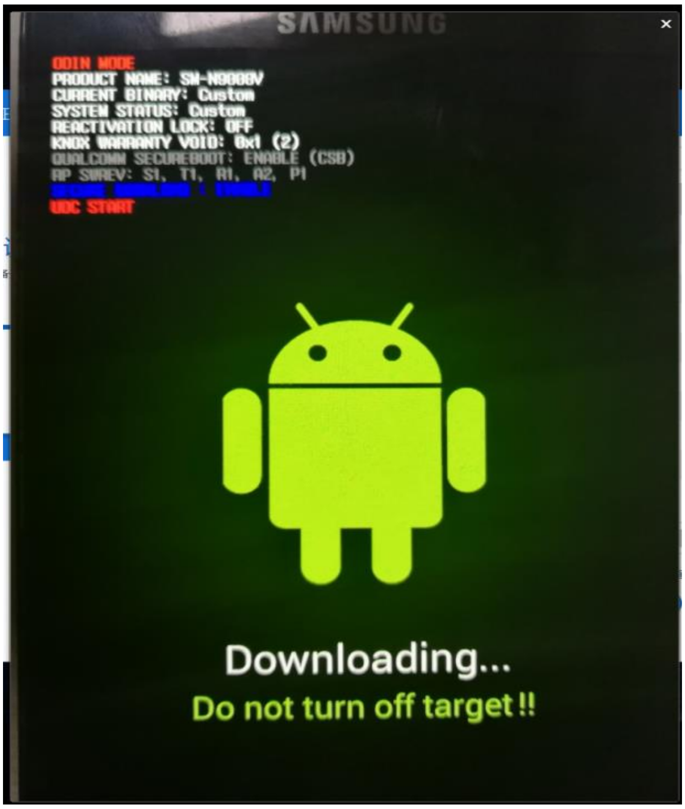
Step 1. Below picture shows the system failed to boot up



```
ODIN MODE
PRODUCT NAME: SM-N9008V
CURRENT BINARY: Custom
SYSTEM STATUS: Official
REACTIVATION LOCK: OFF
KNOX WARRANTY VOID: 0x0
QUALCOMM SECUREBOOT: ENABLE (CSB)
AP SWREV: S1, T1, R1, A2, P1
SECURE DOWNLOAD : ENABLE
UDC START
```

Firmware upgrade encountered an issue. Please select recovery mode in Kies & try again.
固件更新时遇到问题,
请在Kies里选择复原模式后再尝试更新。

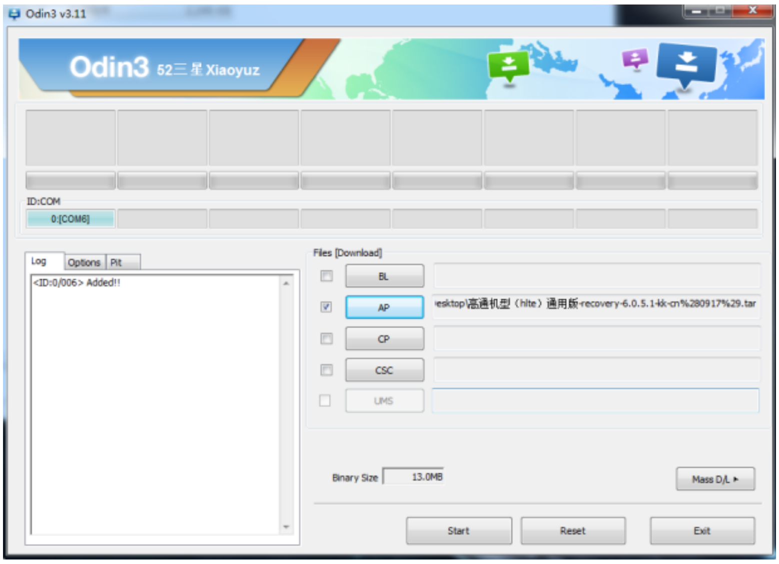
Step 2. Hold "power" button to power off, then hold "power" "home" and "Volume-" to enter download mode



ODIN MODE
PRODUCT NAME: SM-N9008V
CURRENT BINARY: Custom
SYSTEM STATUS: Custom
REACTIVATION LOCK: OFF
KNOX WARRANTY VOID: 0x1 (2)
QUALCOMM SECUREBOOT: ENABLE (CSB)
AP SWREV: S1, T1, R1, A2, P1
[illegible]
UDC START

Downloading...
Do not turn off target!!

Step 3. Flash third-party recovery, then power off and hold power" "home" and "Volume+" to enter recovery mode



Odin3 v3.11

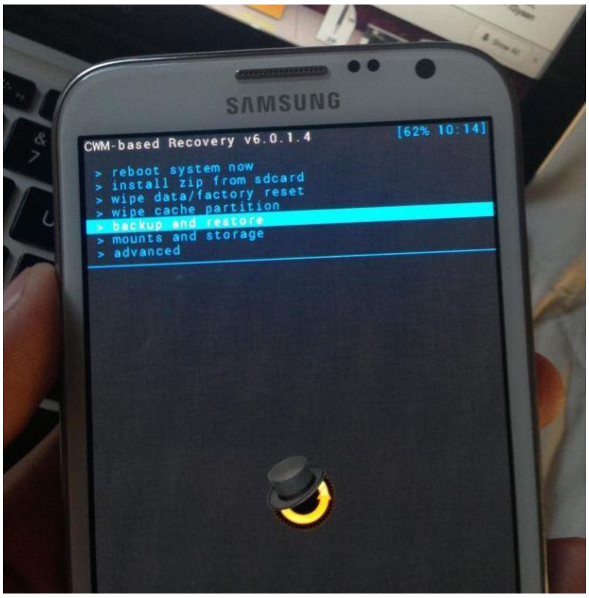
ID:COM
0:[COM6]

Log: <ID:0/006> Added!!

Files [Download]
□ BL
☑ AP esktop\高通机型（hlte）通用版-recovery-6.0.5.1-kk-cn%280917%29.tar
□ CP
□ CSC
□ UMS

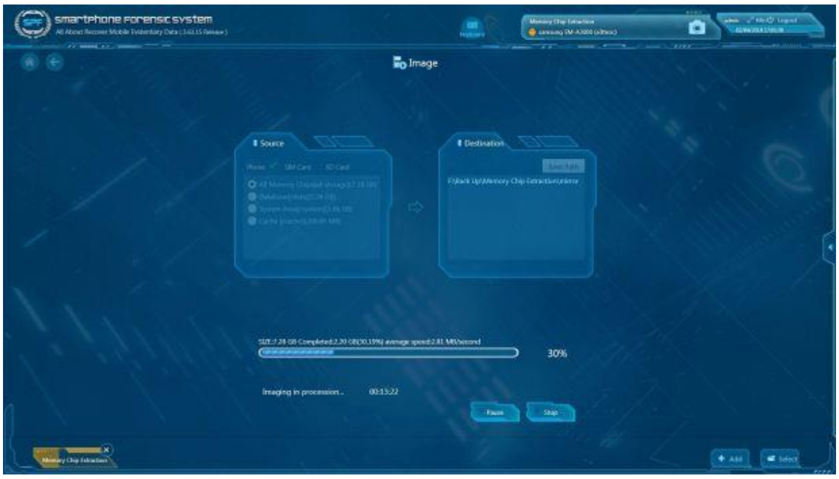
Binary Size 13.0MB

Step 4. Smartphone failed to enter recovery mode and automatically enters the system. After analysis we found that this phone must be flashed with v6.0.5 cwm recovery, remove the battery and enter recovery mode.



```
CWM-based Recovery v6.0.1.4                [62% 10:14]
> reboot system now
> install zip from sdcard
> wipe data/factory reset
> wipe cache partition
> backup and restore
> mounts and storage
> advanced
```

Step 5. Then use SPF to image the smartphone data, create a task and image the whole memory chip

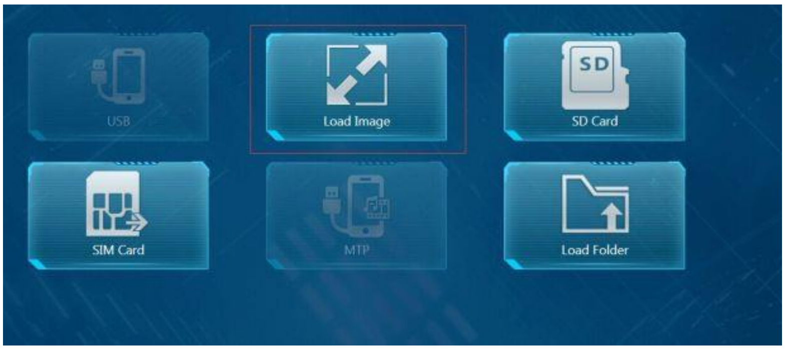


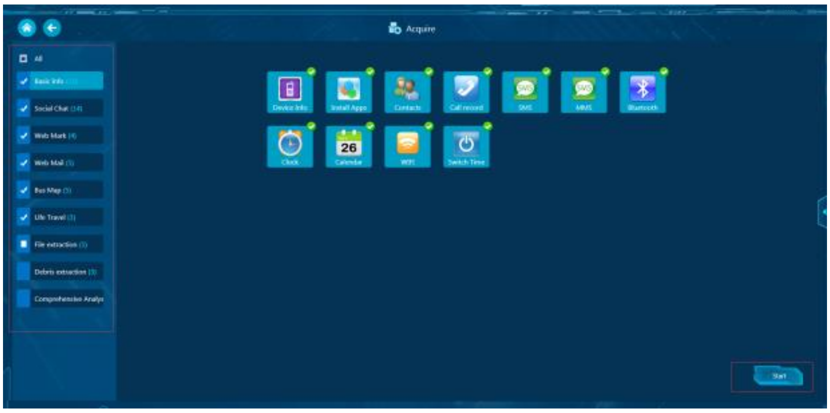
F:/Back Up/Memory Chip Extraction/mirror

SIZE:7.28 GB Completed:2.20 GB(30.15%) average speed:2.81 MB/second 30%

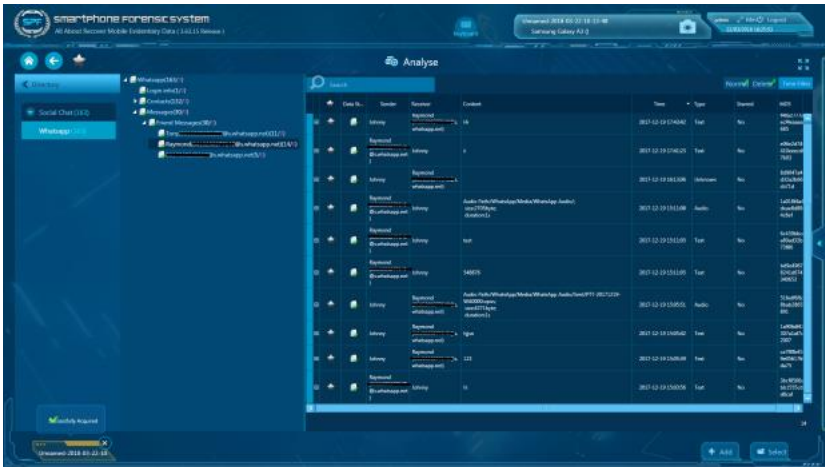
Imaging in procession... 00:13:22

Step 6. After imaging complete, load and analyze the image with SPF





Step 7. SPF will automatically switch to analysis page, users can also generate a report with SPF



4. Conclusion

For some of the old Samsung models, there is no CROM lock. So if the screen cannot be unlocked, we can try to use Samsung's download mode to flash third-party recovery. And then use SPF to create an image of the smartphone. For some models, we may need to remove the battery when failed to enter recovery mode.