[Case Study] Mobile Forensics: Unlock Evidentiary Data Hidden in Feature Phones

Editor's note: Smartphones are the most used in personal electronic devices. With the increasing prevalence of smartphones in peoples' daily lives and in crime, data acquired from smartphones become an invaluable source of evidence for investigations relating to criminal, civil, and even high-profile cases. It is rare to conduct a digital forensic investigation that does not include a smartphone.

Since advancement in smartphone forensics technology has made it harder for criminals to lurk under smartphones, they have turned to more traditional ways.

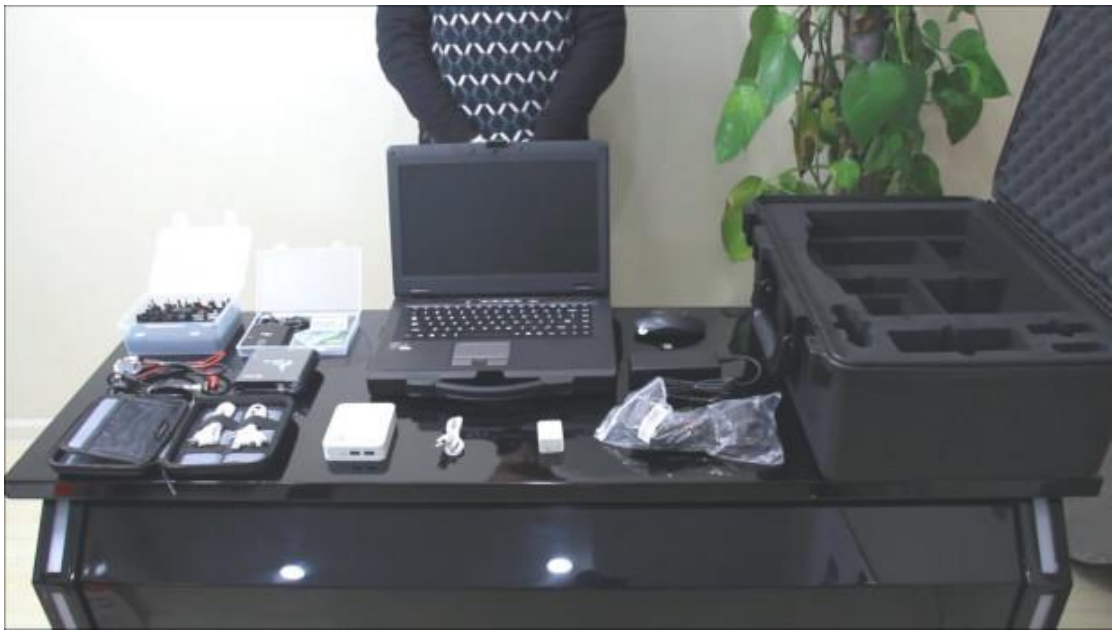
FEATURE PHONE!!!

According to statistics, there're about 0.47 billion features phones, occupying 21%, sold around the world. It seems to be just a small proportion, but in it hid those dirty tricks that we can't afford to overlook.

Feature phones have long been preferred by criminals as a medium of crime committing because to acquire evidentiary data from these devices is not as easy as acquiring data from smartphones. Nevertheless, there's always a way, such as SalvationDATA SmartPhone Forensic System(SPF), which excels at acquiring data from feature phones, including burner phones.

Procedure

2.1 Prepare all devices like rugged laptop and acquisition tool needed for acquiring data from a selected feature phone. (devices all wrapped in smartphone forensic toolkit)



2.2 Connection

Step 1

Connect 2 power cables to corresponding electrodes (red for positive; black for negative)

Step 2

Connect the communication cable to acquisition tool.

Step 3

Connect the acquisition tool to the rugged laptop.

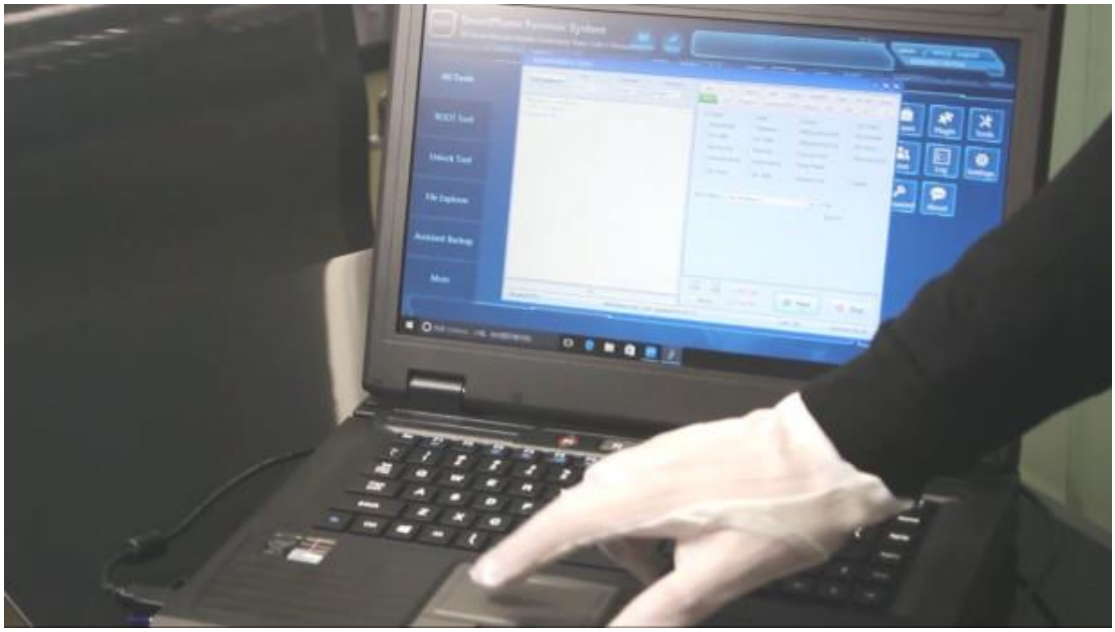
Step 4

Power on acquisition tool, then launch SPF.

2.3 Create image file via acquisition tool. (Click Tools, then select corresponding data acquisition tool)

Step 1

Click Start button in UI of the software.



Step 2

Long press power button on selected feature phone until it prompts to stop.

Step 3

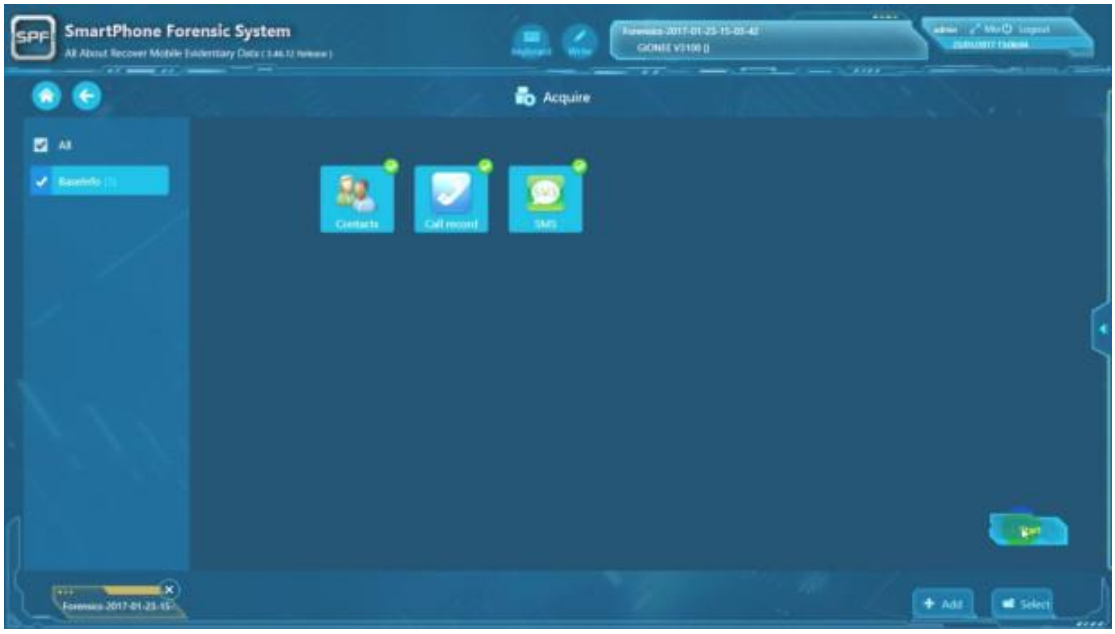
Wait for the physical extraction process and Save image file into the local directory.

Tips: For Chinese Chipsets Physical Extraction, SPF can allow you to access many chipsets manufacturers as MTK, Spreadtrum, Mstar, CoolSand/RDA, Infineon, OM, Skyworks, TI, ADI, SI, AnyKa, AGERE, AD6905, etc.

2.4 Use SPF to acquire data

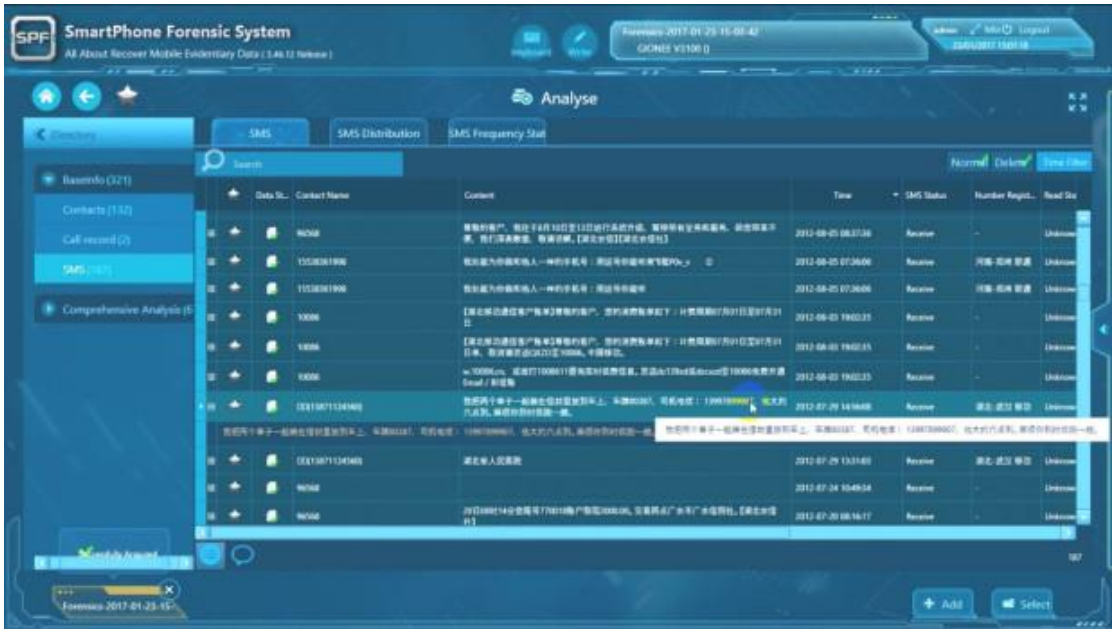
Step 1

Select Acquire module. Load the image file and Select chip type(phone platform). Then click OK to start data acquisition.



Step 2

SPF will automatically switch to Analyse module. The user can view and check acquired data.



2.5 Back to main UI and select report module.

Change setting and format if needed, then create a forensic report.