School of Computing
IT2514 Digital Forensics and Investigation

Practical 2: Mobile Forensic Analysis

Introduction

Based on the previous practical in Computer forensics using AXIOM Process and AXIOM Examine. You have learned basic navigation within AXIOM Process and AXIOM Examine and observing different artifacts once processing has been done. Thus, we will begin to perform Mobile Forensic analysis using AXIOM Examine.

At times before you even go looking for the relevant artifacts, you must be able to understand the device that you are analyzing such as what is the operating system is the device running on etc. This will then be able to further aid you in the forensic analysis as you can provide basic information regarding the device. In addition, not all system structure is the same due to Manufacture, versions, and platforms.

Objectives

Upon completing this lab student will be able to perform navigation of the data and review of individual data areas that is required for mobile forensic.

Before you Begin

Please navigate to "**C:\Baseimages\ForensicV6**". Look for "**Practical_2_Android_CaseFile.zip**" and extract/copy the file to your preferred location. Run AXIOM Examine and navigate to the file "**case.mfdb**".

Lab Questions and Answers

1. What is the device IMEI?

   Answer: 353302094086470

2. Based on the IMEI number. Are you able to determine the model of the Device (Brand etc.)? (Hint: you can google for the IMEI)

   Answer: Redmi Note 8 Pro

3. What is ICCID? (Provide the serial number and Explain)

   Answer: ICCID stands for Integrated Circuit Card Identifier. It is a unique serial number used to identify individual SIM (Subscriber Identity Module) cards in mobile devices. The ICCID is typically a 19 to 20-digit long number and is stored on the SIM card itself.
   8901100330000596478

4. What is IMSI? (Provide the serial number and Explain)

   Answer: 313100000596478 IMSI stands for International Mobile Subscriber Identity

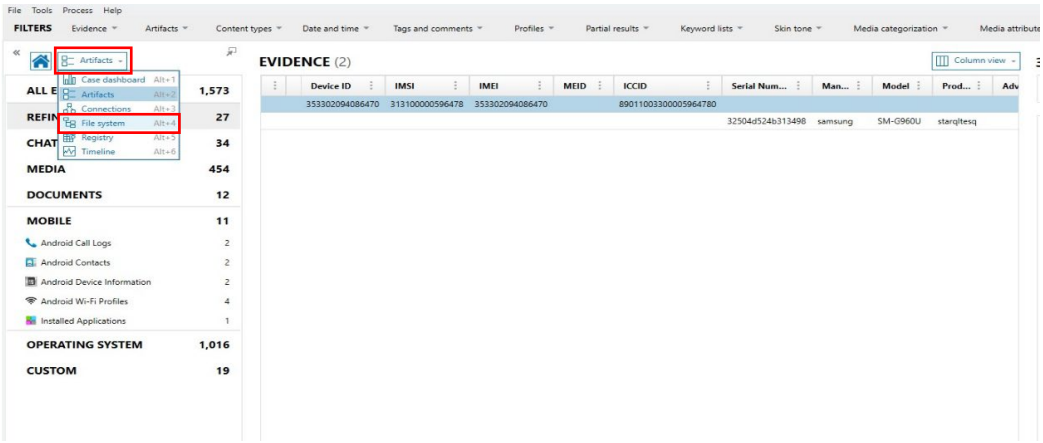
5. What is the Phone Number?

Answer: (574) 220-9526

6. Is a SIM present in the device?

Answer: Yes

7. What mobile operating system the device running*?(Part A and B) (Navigate to the Drop-down box beside the Home icon and click on "**File system**", This view gives you a raw format view as compared to the beautiful layout in "Artifacts")*



A. Expand the zip and navigate to folder called "**Live Data**" within this folder there is a text file can "**device_properties.txt**" select the file. On your right you have Preview Pane, scroll down within the Preview Pane until you see the following Fields shown below *(Notice the Bootloader field. Do a google search):*

```
[ro.bootloader]: [G960USQU3CSAB]
[ro.bootmode]: [unknown]
[ro.build.2ndbrand]: [false]
[ro.build.PDA]: [G960USQU3CSAB]
[ro.build.changelist]: [15119402]
[ro.build.characteristics]: [nosdcard]
[ro.build.date]: [Tue Jan 15 19:32:27 KST 2019]
[ro.build.date.utc]: [1547548347]
[ro.build.description]: [starqltesq-user 9 PPR1.180610.011
G960USQU3CSAB release-keys]
```

(Note* if you don't see any information in "**device_properties.txt**". Click on "**LOCATE SOURCE**" in the preview pane. Browse to the file "**Android_Quick Image.zip**" which was done in Practical 1)

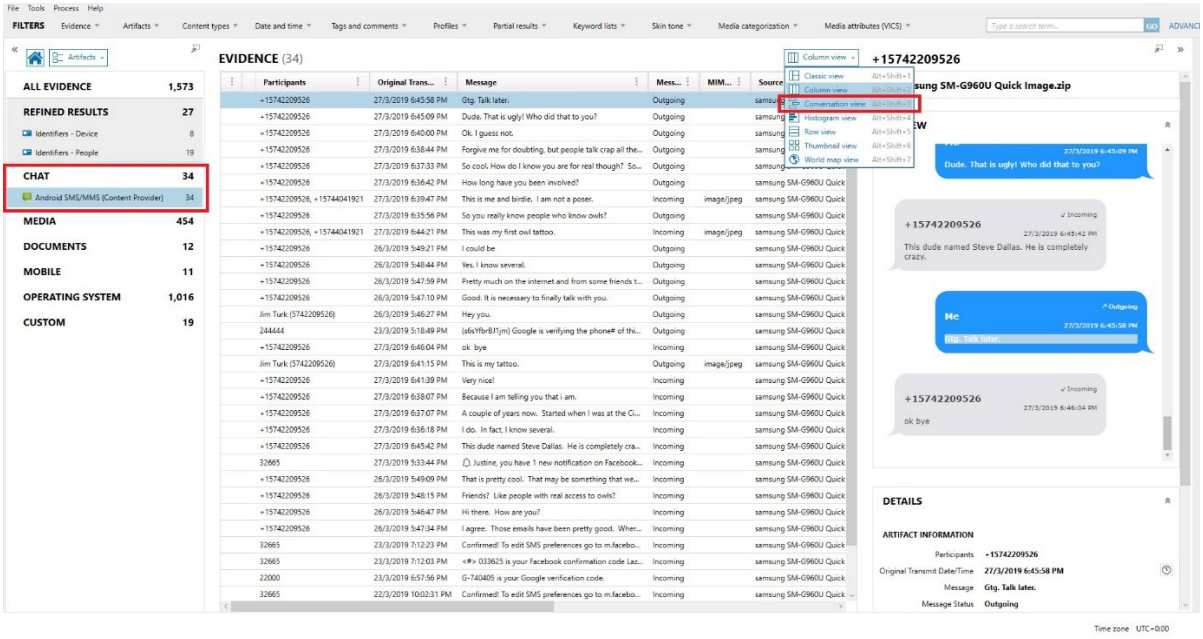
Answer: Samsung Galaxy S9 (model number G960U)

B. Notice the Build Date. Based on the information you have found from google searches. Does the time resemble the information you have found?

Answer: IMEI.info: 15/01/2019, yes when is the bootloader built

8. How many contacts are on the device? Can you determine the name of the contacts?
Answer: 33

9. Who did the owner of the phone chat with via SMS? Summarize the overall chat based on your review. *(Navigate to "**Chats**" on the left column and click on it, then navigate and change the view from "**Column View**" to "**Conversation view**").*



Answer: They were talking about owls

10. Can you determine who is the owner of the device?
Answer: Jim

---END---