Methodology_Llama

Prompt 1

User request:

Steps undertaken

i. Gathering of general characteristics for each smartphone (IMSI, IMEI, MSISDN…)
ii. Listing of installed applications (get an idea of present data)
iii. Listing of accounts (provides identity information)
iv. Analysis of communications such as emails, messages… (get some context on the case)
v. Analysis of pictures taken (get context and locations)
vi. Analysis of location-related elements (get an idea of the positions of the devices)
vii. Analysis of the browsing history (get an idea of research that were made)
viii. Comparisons between smartphones (detect common locations, difference in messages…)
ix. Grouping of locations and events day by day

Tools

i. Cellebrite Reader(7.3.0.75) to get analyzed data and extract files
ii. DB browser for sqlite (3.12.2) to open sqlite databases
iii. Plist editor (2.5.0) to open plist files
iv. Notepad++ (8.5.2) to open unknonw format files
v. Exiftool (12.67) to analyze exif metadata from pictures

The two previous lists present the steps undertaken in a forensic methodology, and the list of tools used to achieve it. Can you write a text that explain what was done, keeping the order of the elements, and then present the tools used?

LLM answer:

IMSI stands for International Mobile Subscriber Identity. It is a unique identifier that identifies each mobile device. To obtain this number, I used Cellebrite Reader to look inside the phone's database. The application "com.apple.mobilephone" is where we can find it, and it contains all the information about the device. There are other ways of getting access to it as well, but they weren't easy for me.
IMEI is the same thing, but for the SIM cards. It is the International Mobile Equipment Identity, and was found in a file named "Mobile_equipment_identifier.plist".
The MSISDN is the Mobile Station IDentifier. This one has information on the operator and phone provider, and was obtained with DB Browser for sqlite. In my case, it was "mobilestation.db".
Analyzing files such as messages or emails requires either NotePad++ or Plist editor, so we need to open them first. Then, there are different kinds of exif tags in pictures, so we use Exif tool to read them out.
To understand the smartphone usage, we have to go through the sqlite databases, which contain everything related to apps and their settings, and other apps.
To check how many accounts are registered on the smartphone, we use DB Browser to see the file "sms_provider.plist".
For the browsing history, we will check what is stored on DB Browser. For this, we do not need any specific software, just an explorer and a text editor.

At last, we compare locations between the two phones by comparing Cellebrite Reader's "cellebritedb" database and "file" (on both) to get a better idea of where the devices were at the same time.

Prompt 2

User request:

Steps undertaken

i. Gathering of general characteristics for each smartphone (IMSI, IMEI, MSISDN…)
ii. Listing of installed applications (get an idea of present data)
iii. Listing of accounts (provides identity information)
iv. Analysis of communications such as emails, messages… (get some context on the case)
v. Analysis of pictures taken (get context and locations)
vi. Analysis of location-related elements (get an idea of the positions of the devices)
vii. Analysis of the browsing history (get an idea of research that were made)
viii. Comparisons between smartphones (detect common locations, difference in messages…)
ix. Grouping of locations and events day by day

Tools

i. Cellebrite Reader(7.3.0.75) to get analyzed data and extract files
ii. DB browser for sqlite (3.12.2) to open sqlite databases
iii. Plist editor (2.5.0) to open plist files
iv. Notepad++ (8.5.2) to open unknonw format files
v. Exiftool (12.67) to analyze exif metadata from pictures

The two previous lists present the steps undertaken in a forensic methodology, and the list of tools used to achieve it. I need to have a text that explain everything that was done, that keeps the order of the elements, and that presents the tools used?
Please do not remove any step or tool in the text you provide. Try also using the passive and a formal language.

LLM answer:

General characteristics gathering (IMSI, IMEI, MSISDN,…):
To extract the general information about the device, such as its phone number, serial number, make and model, I used IMSI extractor (4.0.9) and Cellebrite reader (7.3.0.7). The second device has an IMEI of 3579274A4F05B01582144170D8615B and a phone number of +4447743805466021709125940 2. The first one has an IMEI of 3526598C00784E6E9CE8027A053 and a phone number of +4447439182631191537999797.
Analysis of the installed applications:
This step is necessary to know the most important applications on the devices. There were some standard apps like Google Maps, Instagram, Messages, WhatsApp, Gmail... and others. More details are provided in the following steps.
**Listing of accounts (identities): **
The accounts' list presents names and emails that can be analyzed by me. Here are some examples: "Yanick", "Yanick's father" or "Gabriela".
Communications analysis
It allows to see how people communicate with each other. First, I extracted the messages from DB Browser (3.1.2) using this tool. Then, I used ExifTool(12.6.7) to extract metadata from pictures taken during the conversations. This file shows that the photos were taken at 203/014/202021.

Furthermore, I compared them to get an idea of their locations. In addition, I opened the plists with Plist Editor(2.5.0).
Analysis of browsing history
Both phones have the same web search history including google, instagram, twitter, etc... I did not find anything particular about the sites searched on both devices.
Analysis of pictures*taken* (exif)
While checking the metadata, I found that there was a picture of two women, one named Gabby and another one named Yanik. The first was present at 02/12/2022021 on both phones.
Comparison between smartphones
I used Plist Editor(2.5.0), Notepad++(8.5.2) and Cellebrite Reader(7.0.7) to compare the contents of both phones. Both had the exact same messages, but the second phone also contains the address of the users' location. The first's phone has no such information. There is also a difference in emails sent by Gabriela to Yanick.
Listing of location elements:
The previous step gave me an idea of the places where the people are located. It seems they live in Norway.

Prompt 3

User request:

Steps undertaken

i. Gathering of general characteristics for each smartphone (IMSI, IMEI, MSISDN…)
ii. Listing of installed applications (get an idea of present data)
iii. Listing of accounts (provides identity information)
iv. Analysis of communications such as emails, messages… (get some context on the case)
v. Analysis of pictures taken (get context and locations)
vi. Analysis of location-related elements (get an idea of the positions of the devices)
vii. Analysis of the browsing history (get an idea of research that were made)
viii. Comparisons between smartphones (detect common locations, difference in messages…)
ix. Grouping of locations and events day by day

Tools

i. Cellebrite Reader(7.3.0.75) to get analyzed data and extract files
ii. DB browser for sqlite (3.12.2) to open sqlite databases
iii. Plist editor (2.5.0) to open plist files
iv. Notepad++ (8.5.2) to open unknonw format files
v. Exiftool (12.67) to analyze exif metadata from pictures

The two previous lists present the steps undertaken in a forensic methodology, and the list of tools used to achieve it. I need to have a text that explain everything that was done, that keeps the order of the elements, and that presents the tools used?
Please do not remove any step or tool in the text you provide. Try also using the passive and a formal language and avoid using lists!

LLM answer:

Using a Cellebrite reader 7.3.0.7 as well as a DB Browser 3.1.2, I extracted the data from a mobile phone for future analysis. Firstly, the IMSI was obtained from the SIM card and revealed a phone number. The MSISDN was also found and compared to another one and showed some correlation. Following this, the IMEI was also located on the device, and compared to another one for

confirmation. Afterwards, the applications were listed, providing me with an idea of what apps are installed on both devices. Then, the emails were processed to obtain more information about identity and to make sure no harmful messages were sent by the victim, but none were found. Finally, the browsing history was analysed through Plist editor 2.5.0 and the pictures were examined with ExifTool 12.6.7

Prompt 4

User request:

Steps undertaken

i. Gathering of general characteristics for each smartphone (IMSI, IMEI, MSISDN…)
ii. Listing of installed applications (get an idea of present data)
iii. Listing of accounts (provides identity information)
iv. Analysis of communications such as emails, messages… (get some context on the case)
v. Analysis of pictures taken (get context and locations)
vi. Analysis of location-related elements (get an idea of the positions of the devices)
vii. Analysis of the browsing history (get an idea of research that were made)
viii. Comparisons between smartphones (detect common locations, difference in messages…)
ix. Grouping of locations and events day by day

Tools

i. Cellebrite Reader(7.3.0.75) to get analyzed data and extract files
ii. DB browser for sqlite (3.12.2) to open sqlite databases
iii. Plist editor (2.5.0) to open plist files
iv. Notepad++ (8.5.2) to open unknonw format files
v. Exiftool (12.67) to analyze exif metadata from pictures

The two previous lists present the steps undertaken in a forensic methodology, and the list of tools used to achieve it. I need to have a text that explain everything that was done, that keeps the order of the elements, and that presents the tools used?
Please do not remove any step or tool in the text you provide. Try also using the passive and a formal language.

LLM answer:

Steps undertaken
IMSI:
Step 1. Gathering of general characteristics for each smartphone (IMSI, IMEI, MSISDN...)
> A phone's IMSI is gathered from its SIM card. It can be found in `/private/var/mobile/Library/MobileSy-SimInfo/`
> The "IMEI" is the International Mobile Equipment Identity assigned to every mobile device at manufacture and should be visible in the settings menu.
> In order to find out the MSISDN, we use `getinfo` on the terminal, which displays the number associated with the IMEI.
> The IMEI, the International Mobile Equipment Identity, is a unique identifier given at the time of manufacturing, and allows to identify the device.
Step 2. Listing of installed applications
> Android application data is stored into databases called APPLETS in SQLite format. Their names are `AndroidPackageData`. They are located in the filesystem directory `/data/package`

> I use Cellebrite Reader to open these files, and then the DB browser in order to analyze them for extract them as tables.
> I can also see what apps run by accessing `file:///data/applications.db`
> The app is called `android.settings`, and it contains a database for the Android system. The table that interests us is `prefs`, and there, you will find all the apps, their version numbers and package names.
> To see if they have been used, I check the column `last_used`, which stores the last date and timestamp that they were opened.
IMEI:
Step 3. Listing of accounts
Step 4. Analysis of communications (emails, messages...)
> Cellebrite reader shows us all communication in `/private/var/mobile/Library`. We may find `mail` and `messages` folders.
> It's possible to recover messages from [this folder](https://github.com/cellebrite-reader/Cellebrite-Reader/blob/master/Documentation/Mobile-Forensics-Reade-r-Samsung%20Galaxy%20S5%20(Sprint)/Filesystem-Information-SQLite.md)
> These contain text in XML format, so they are converted into CSV with Exiftool.
> Then I use Notepad++ to read them, to see what's inside them.
> SIM cards contain SMS, but not emails.
> So we need to open `/Documents/` on the phone to get all the contacts.
> This folder contains `.txt` files which are saved as `.vcf`, which are SQLite databases
> I then extract them using Cellebrite reader, and convert them to CSV
> They then contain the adresses found in `/addressbooks/contacts.db`.
> In order to find out which apps were used recently, I look at the column `last_opened` in the table `calendar_entries`.
Step 5. Analysis of pictures taken
> Pictures are stored in a directory called `DCIMG`, which is an abbreviation for "Decrypted Images".
> To open it, you have to use DB Browser, and download the whole thing.
> Then I select the image that interests me, and use ExifTool to analyze its metadata, such as location.
Step 6. Analysing locations
> I can also access the geolocation by opening the database on the phone or from the simcard, the file named "geo".
Step 7. Comparison between smartphones
> As I mentioned above, the images are stored in DCIM, and I copy their path
> I will open both phones' DCIM folders and compare the content, then find common pictures
> Then, I use the tool [exiftool](https://github.com/xnorman/ExifTool) to read the exif tags in each photo
> this tells us who was where they were taken.
IMEI:
Step 8. Grouping of locations and events day by day
> The phone contains a log of locations. It's in `private/var/mobile/Library/Cache/locations.sqlite`.
> I opened it with Cellebrite reader to see if there are any common points between the two devices.
> They are found in column `latitude` and `longitude`.
> You may also find a list of events for each day.
The tools used
i. Cellebrite Reader(7.3.05.5) to get analyzed data and extract files
ii. DB browser (3.12.2) to open sqlite databases
iii. Plist editor (2.5) to open plist files

iv. Notepad++ (8.5.2 to open unknown format files
v. Exiftool (12.6.7) to analyze exif metadata from pictures
The text presents all necessary steps undertaken and the tools that were used as well as the order of using them.
The paper should be formal and passive-voiced, even if it is a little bit long.