**Lab 14: Mobile\_App\_Investigations\_Messaging**

**What You Need for this lab**

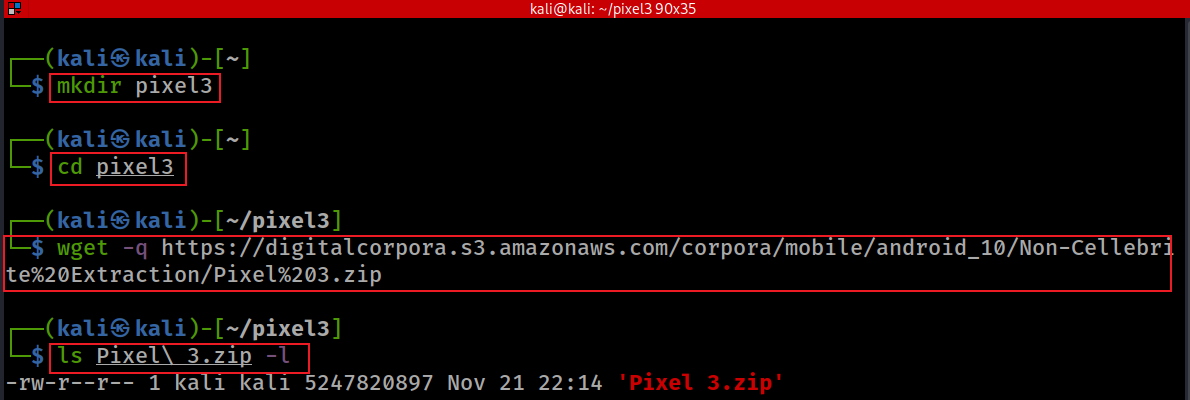
* + Install Virtualbox : <https://www.virtualbox.org/wiki/Downloads>
  + Install Kali 2021.4. : <https://old.kali.org/kali-images/kali-2021.4/>

Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+

* + Android Open-Source Project Apps :
  + <https://digitalcorpora.s3.amazonaws.com/corpora/mobile/android_10/Non-Cellebrite%20Extraction/Pixel%203.zip>

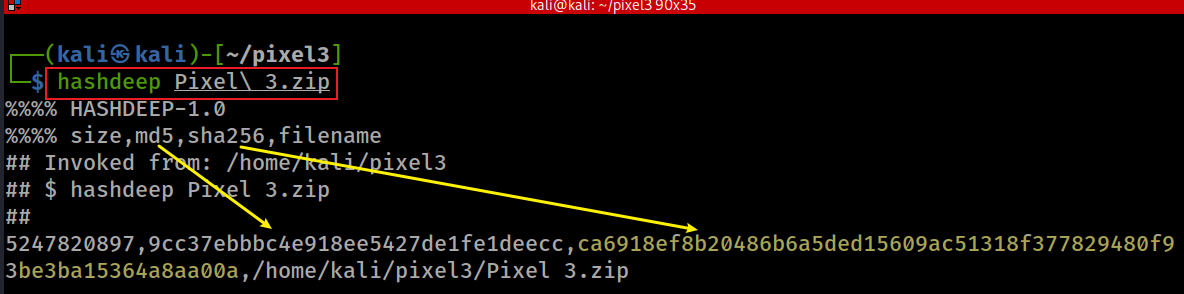
**Step 1**

* Download Pixel 3 image

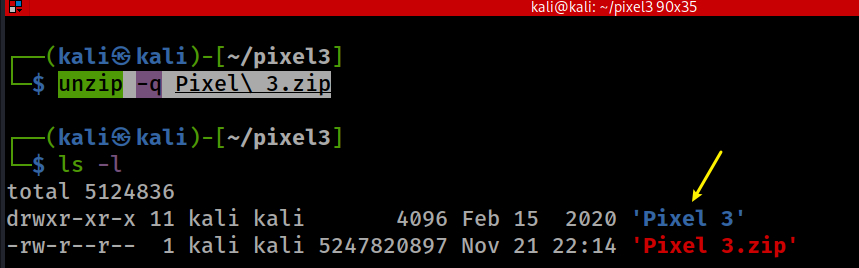


Verify hashes

hashdeep Pixel\ 3.zip



* unzip to get Pixel 3 image

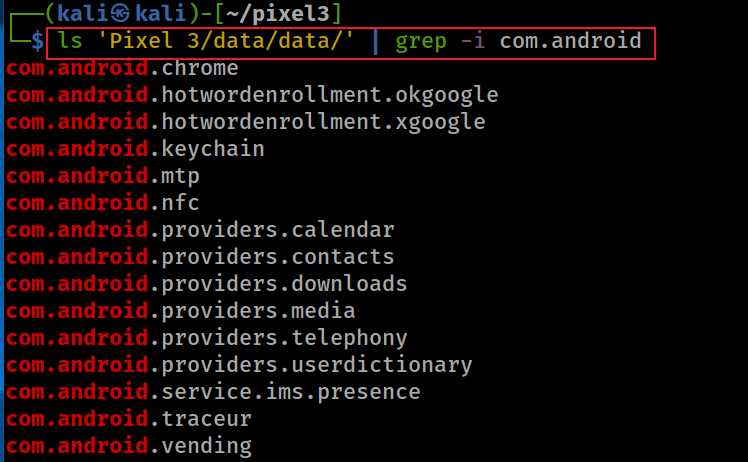


*ls 'Pixel 3/data/data/'*



**Step 2. Investigating Messaging Services**

* Show all AOSP Apps/Packages: *com.andriod.\**



* Find the location of Java package

Graphical user interface, text

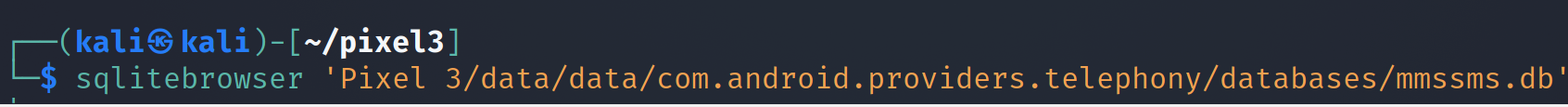
Description automatically generated

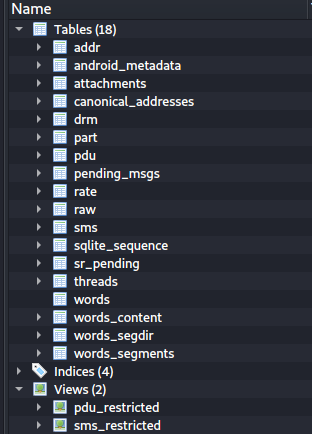
* Find the database location

Graphical user interface, text

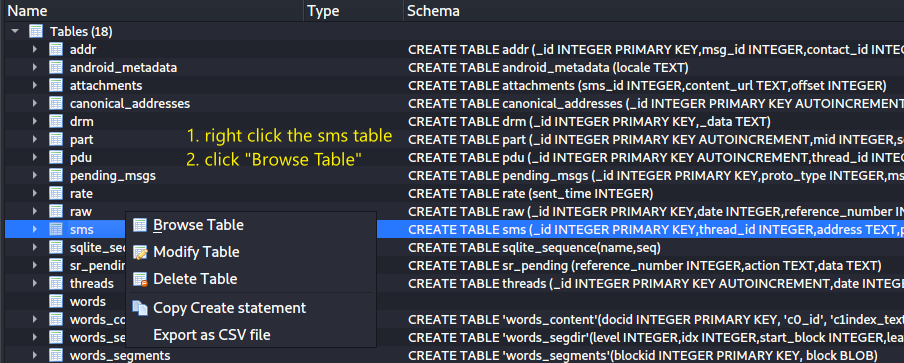
Description automatically generated

* Show all tables in the database

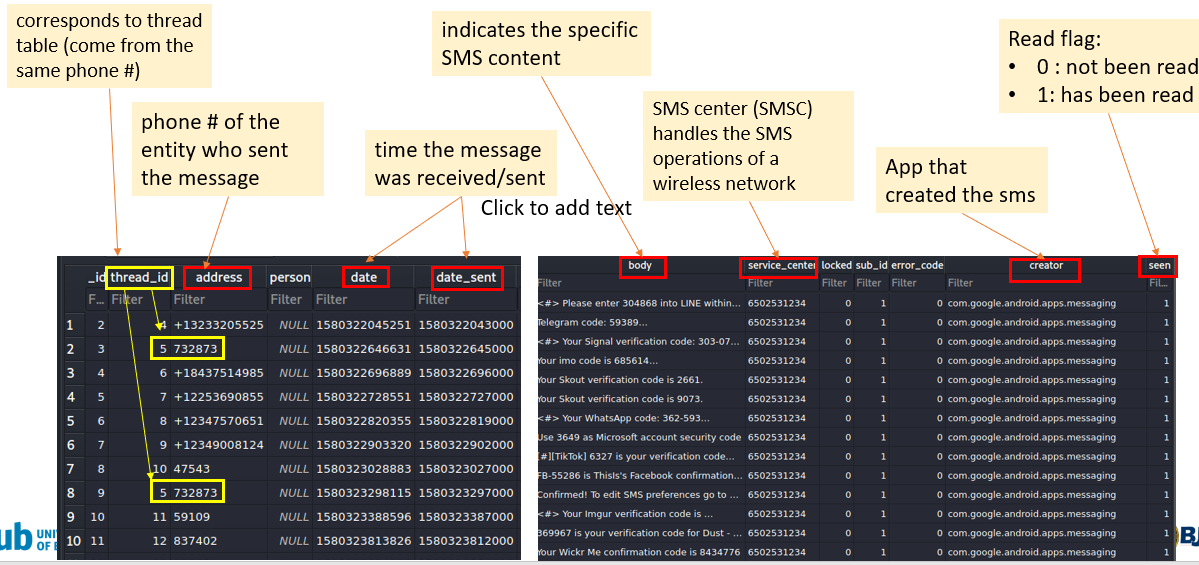




* *sms*: message log
  + Only system, phone or the default message app can have full access of sms data
* *sms\_restricted*:
  + Only contains sent or received messages.
* *threads*
  + Group all messages based on incoming phone numbers and time period?
  + Exam *sms* table structure

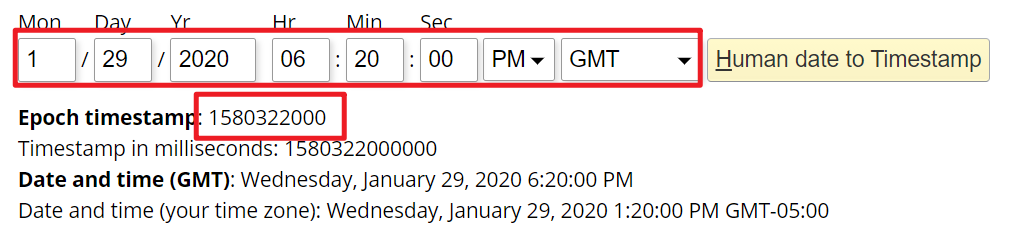


* Find clues to answer the question



* Which message was received on Jan 29, 2020 around 6:20 pm?

<https://www.epochconverter.com/>



* Who sent the message?

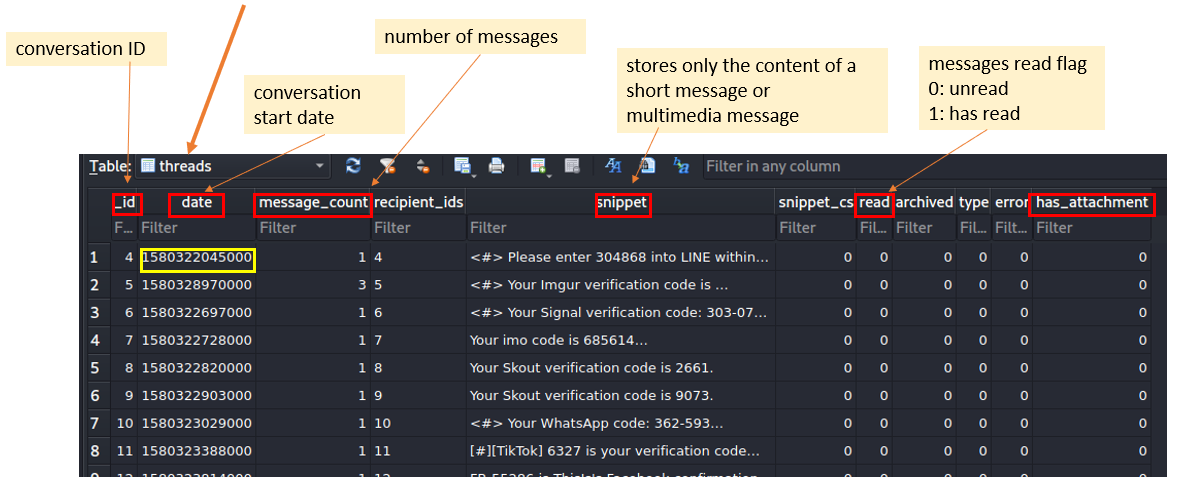
Text

Description automatically generated

Graphical user interface, text

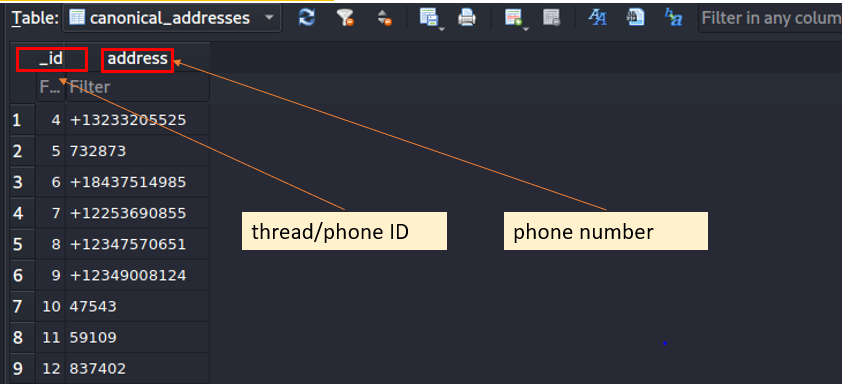
Description automatically generated

What table describes conversation?

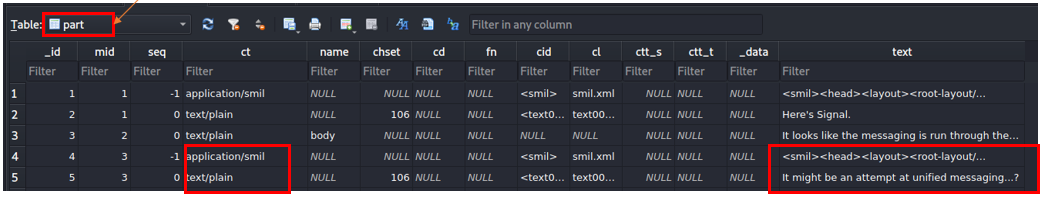


Where to find sender’s phone number?

Exam *canonical\_addresses* table



Which table contains MMS information ?



Part table stores below information:

* **\_id:** Distinguish between different attachments of a multimedia message (including text, picture, audio, video and other formats)
* **ct:** indicates what type of attachment
* **data:** indicate where the attachment is stored on the phone
* **text:** Represents the body of the MMS.

**YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!**

Save the document with the filename "**YOUR NAME Lab 14.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 14 From YOUR NAME**", replacing "YOUR NAME" with your real name.