Lab 14: Mobile_App_Investigations_Messaging

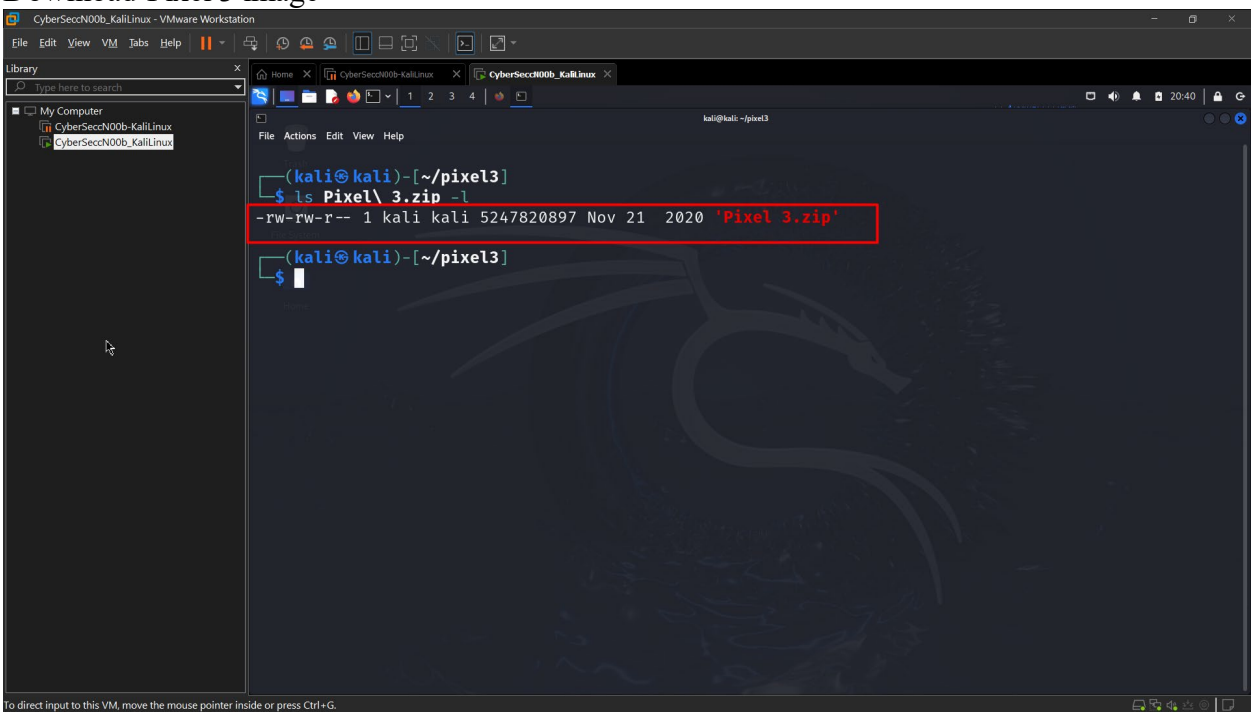
Group: CyberSec_N00b

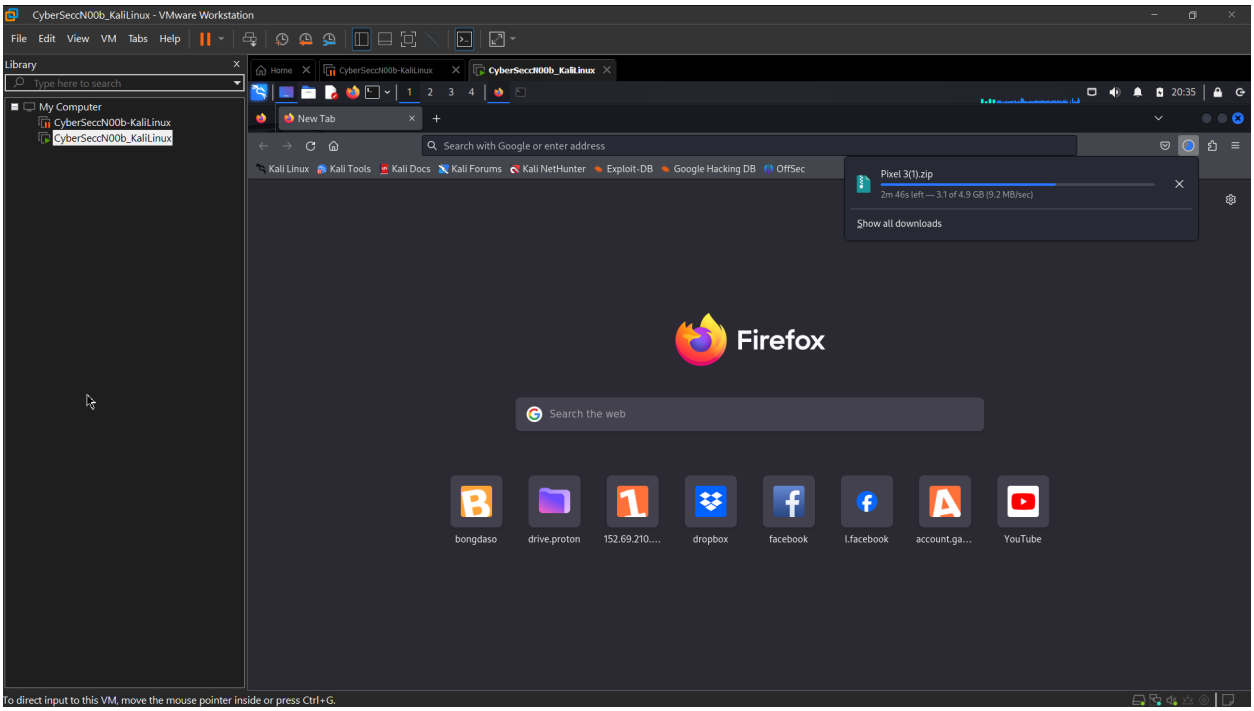
Member:

- *Huỳnh Ngọc Quang (SE181838)*
- *Hồ Tài Liên Vy Kha (SE181818)*
- *Hoàng Kim Long (DE180860)*
- *Phạm Thành Long (SE181692)*
- *Nguyễn Lê Hoàng Thông (SE182533)*

Step 1

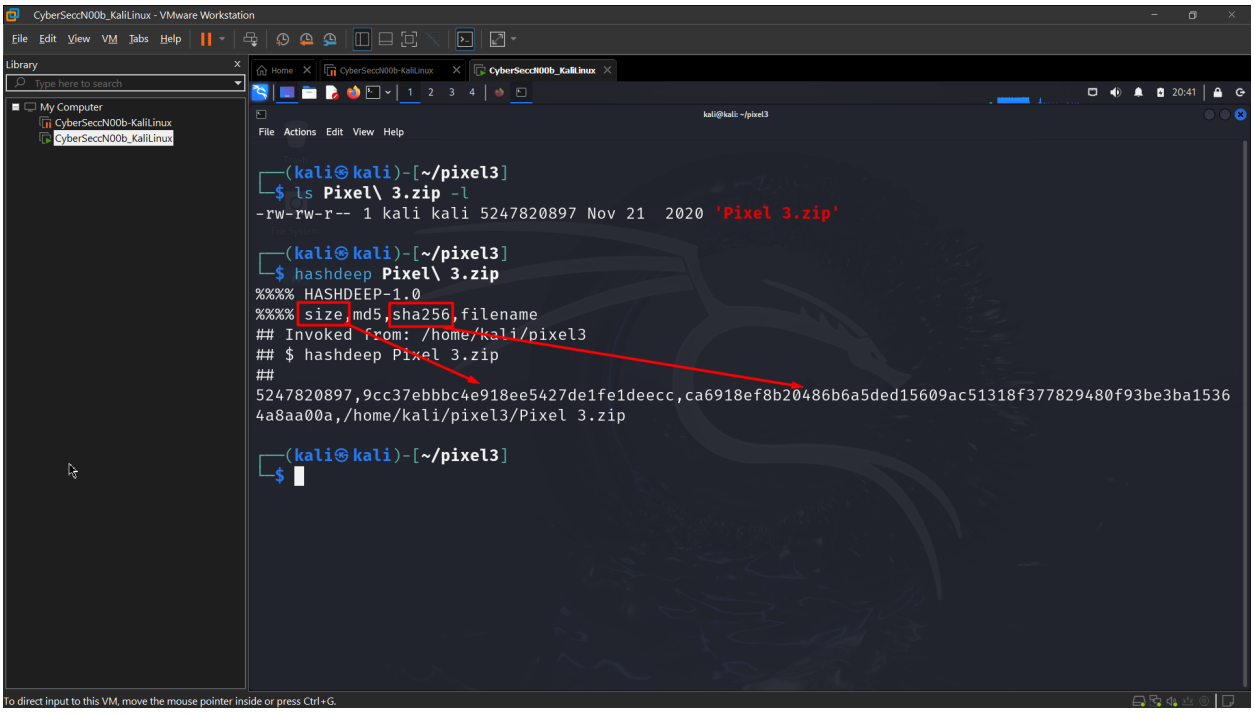
- Download Pixel 3 image



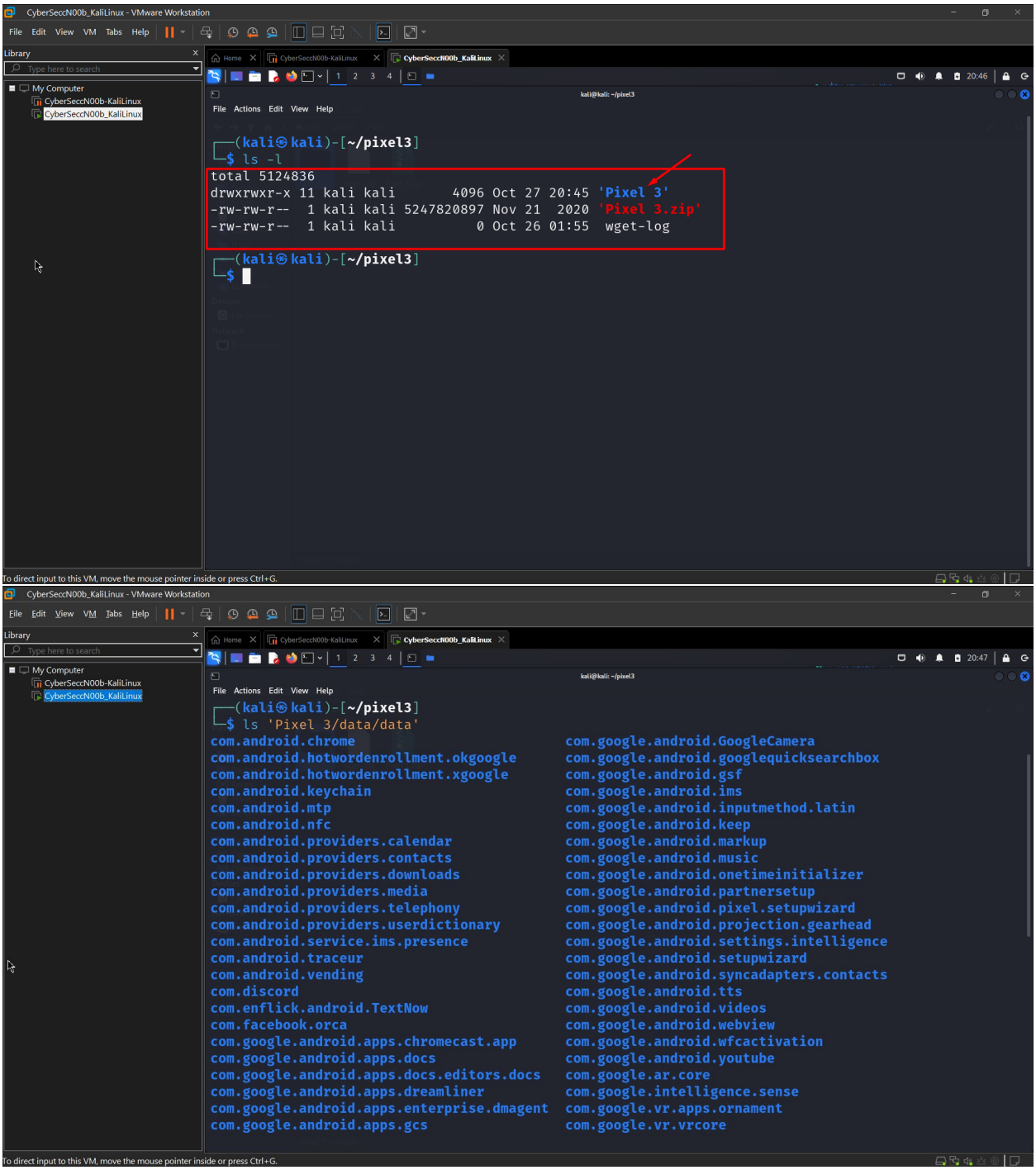


Verify hashes

hashdeep Pixel\ 3.zip

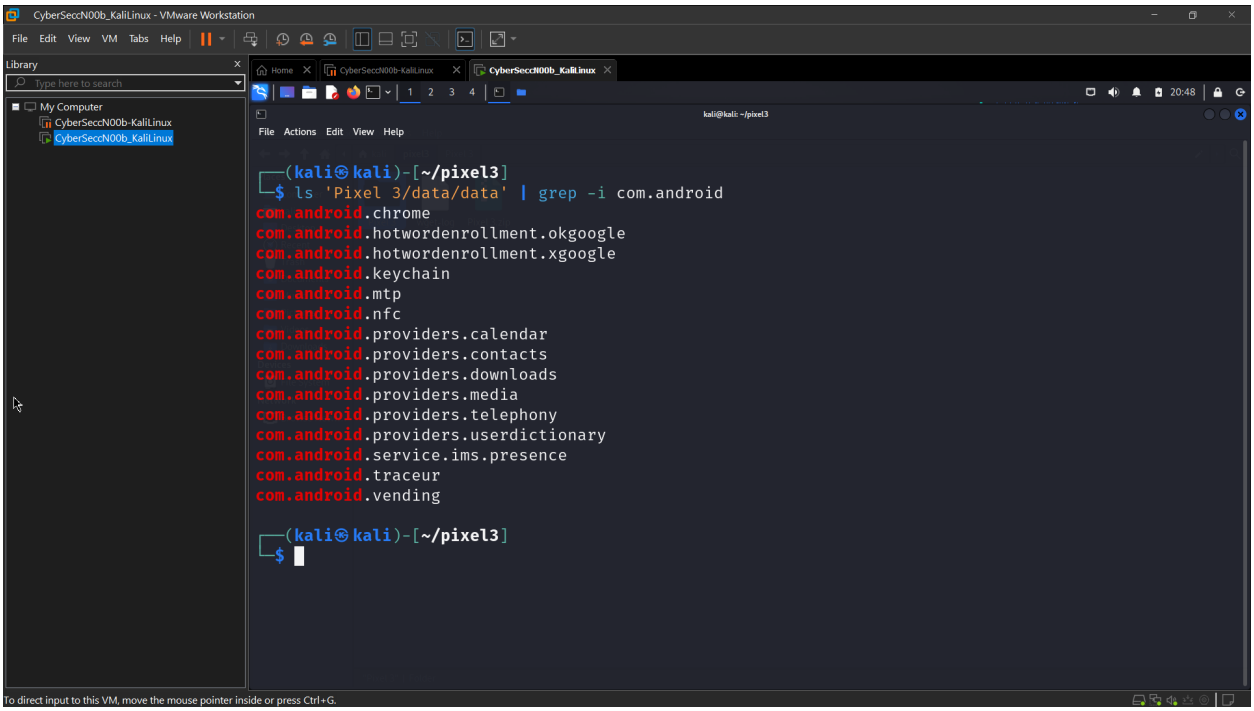


- unzip to get Pixel 3 image

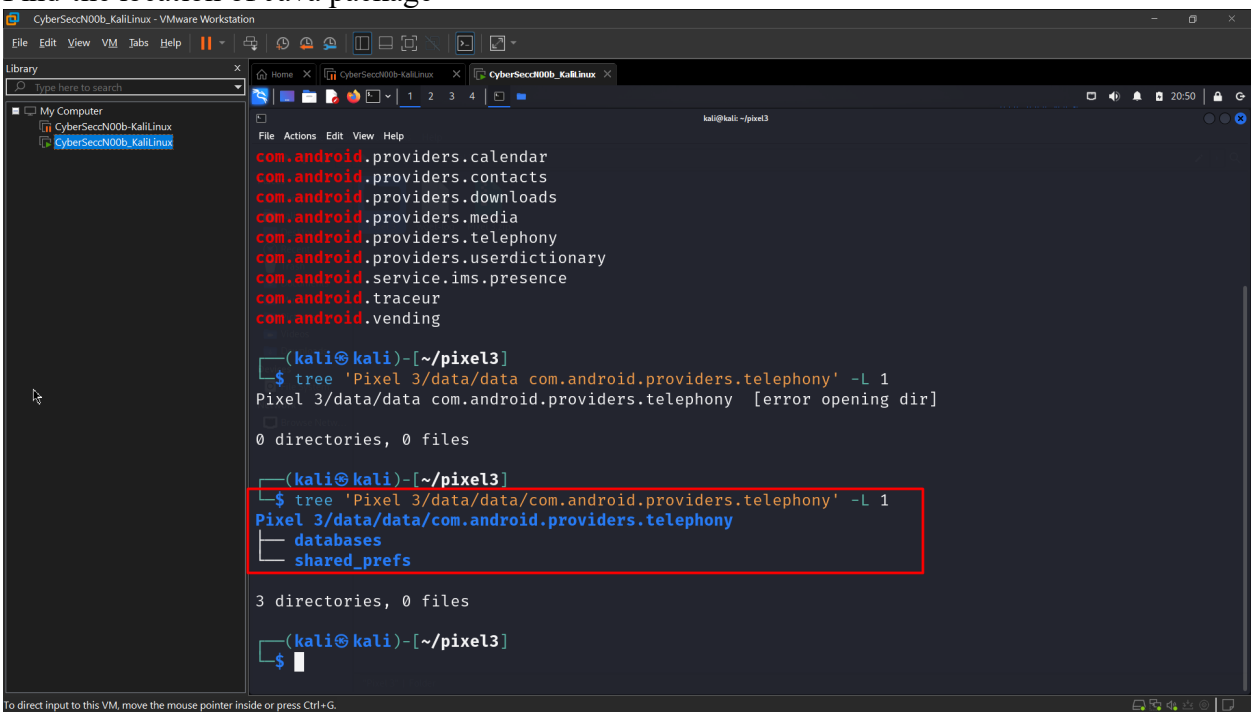


Step 2. Investigating Messaging Services

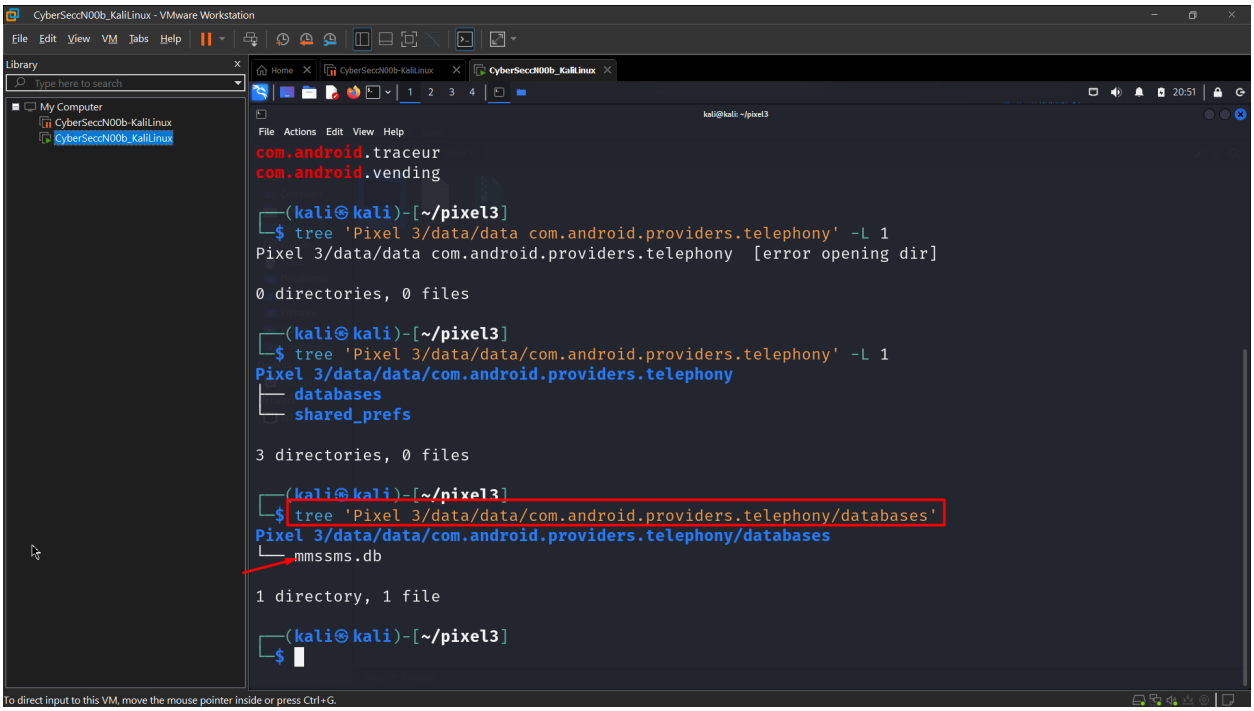
- Show all AOSP Apps/Packages: *com.andriod.**

- 

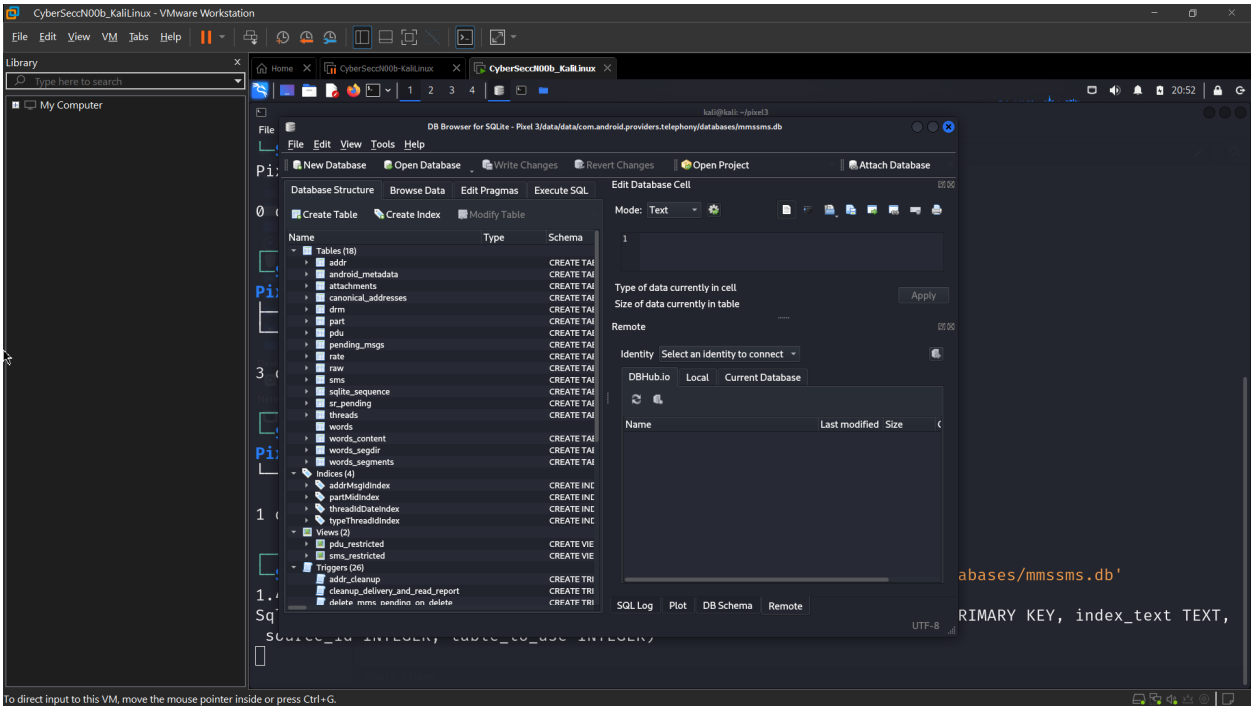
Find the location of Java package

- 

Find the database location

- 

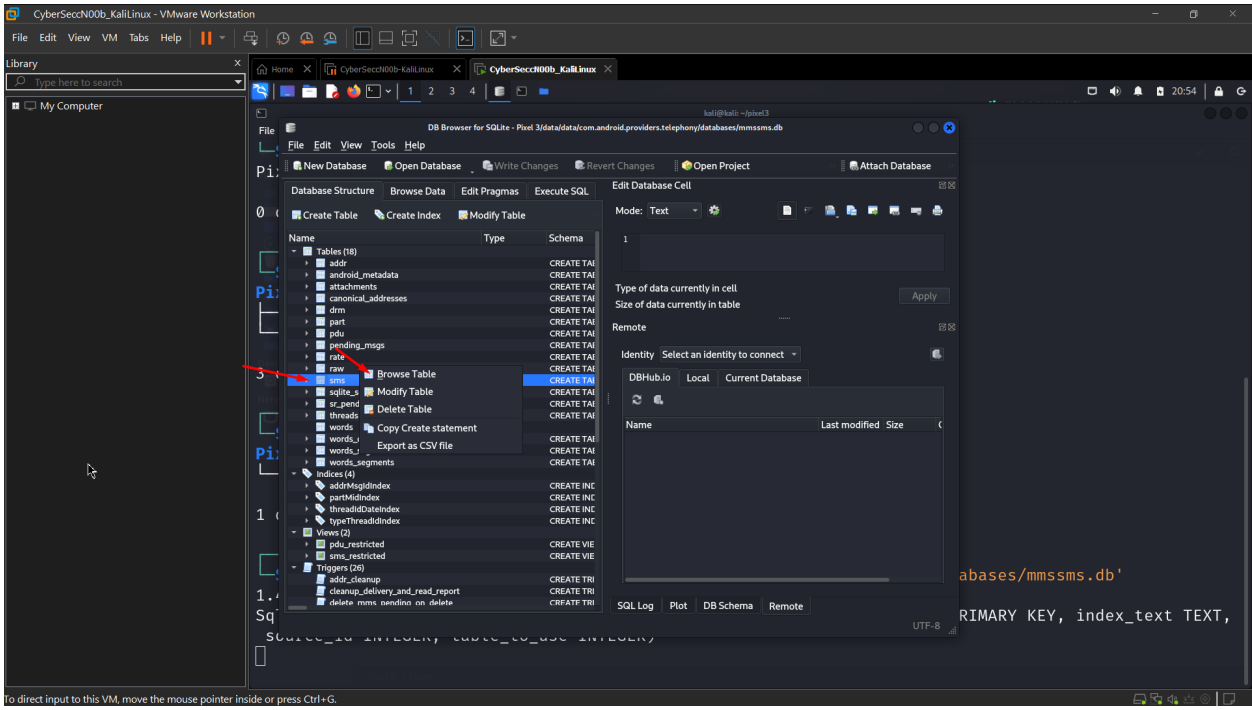
Show all tables in the database

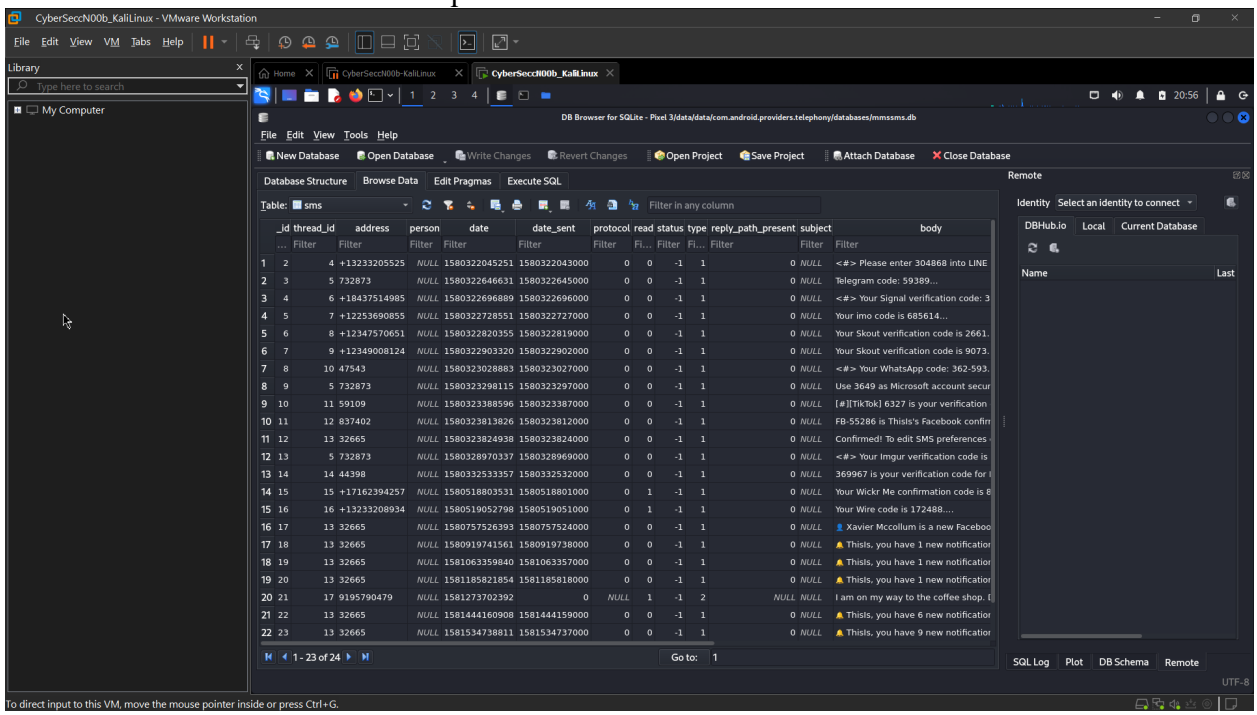
- 

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.

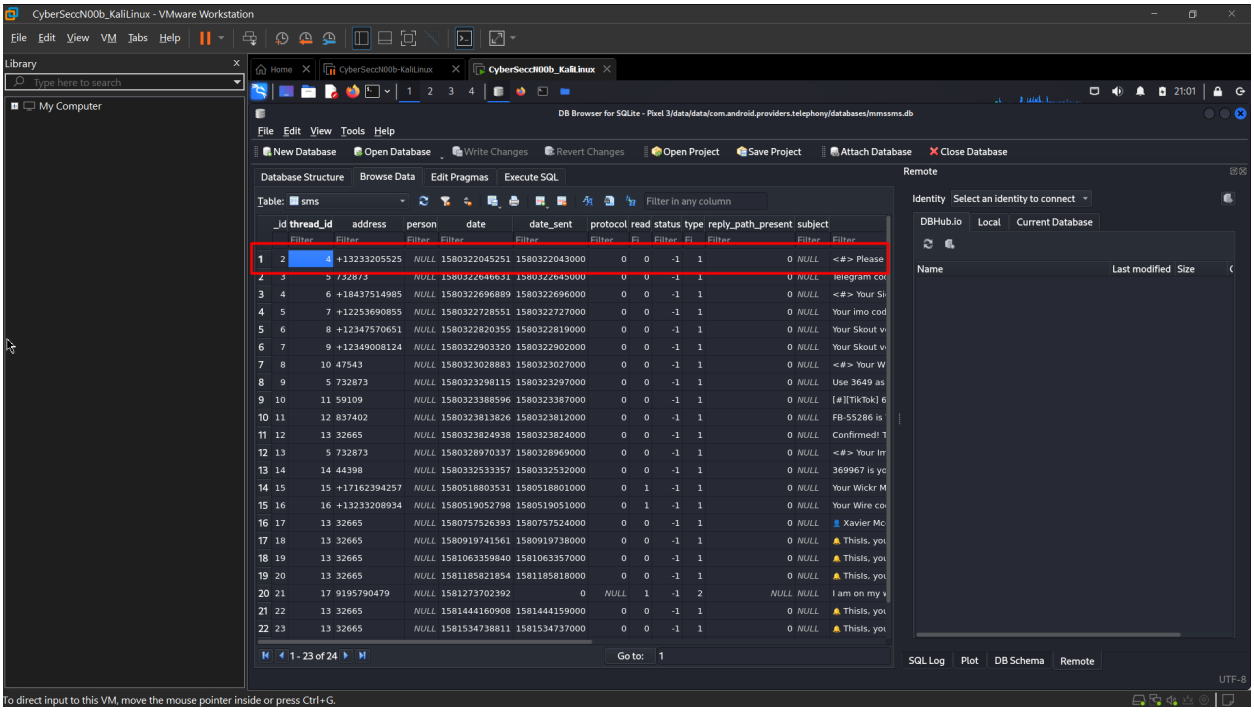
- *threads*
    - Group all messages based on incoming phone numbers and time period?
- Exam *sms* table structure
    - 

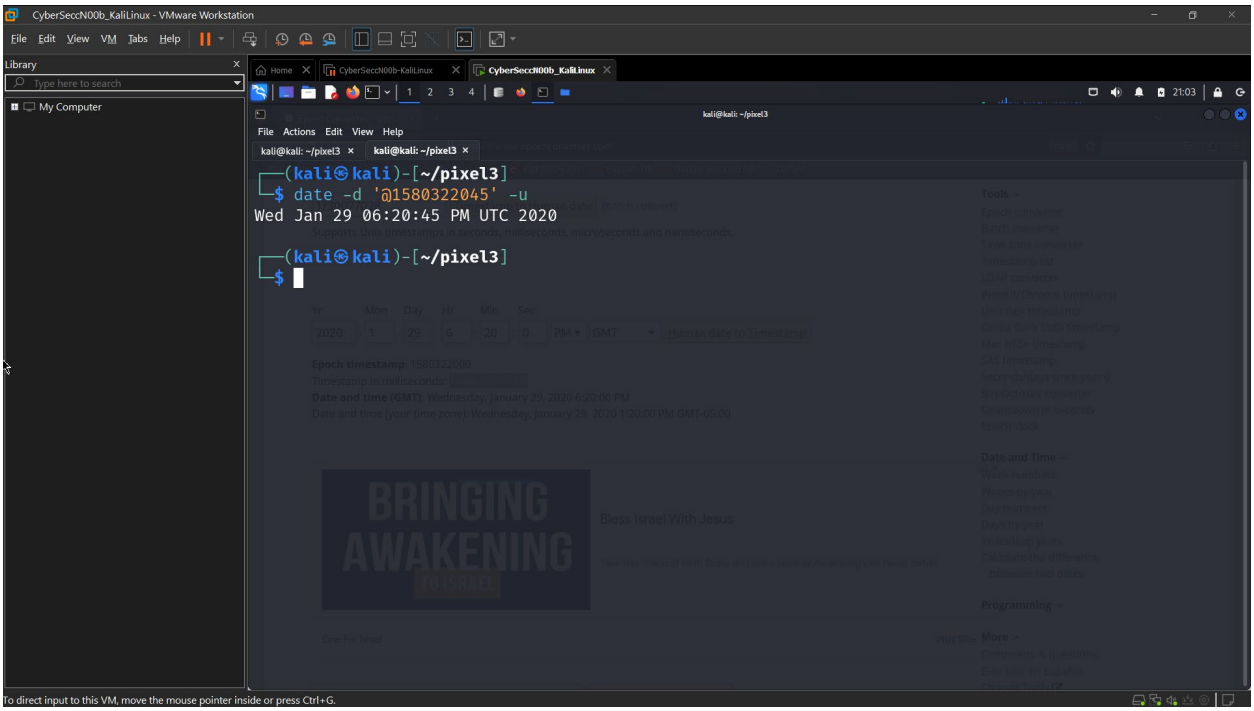
    Find clues to answer the question
    - 

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

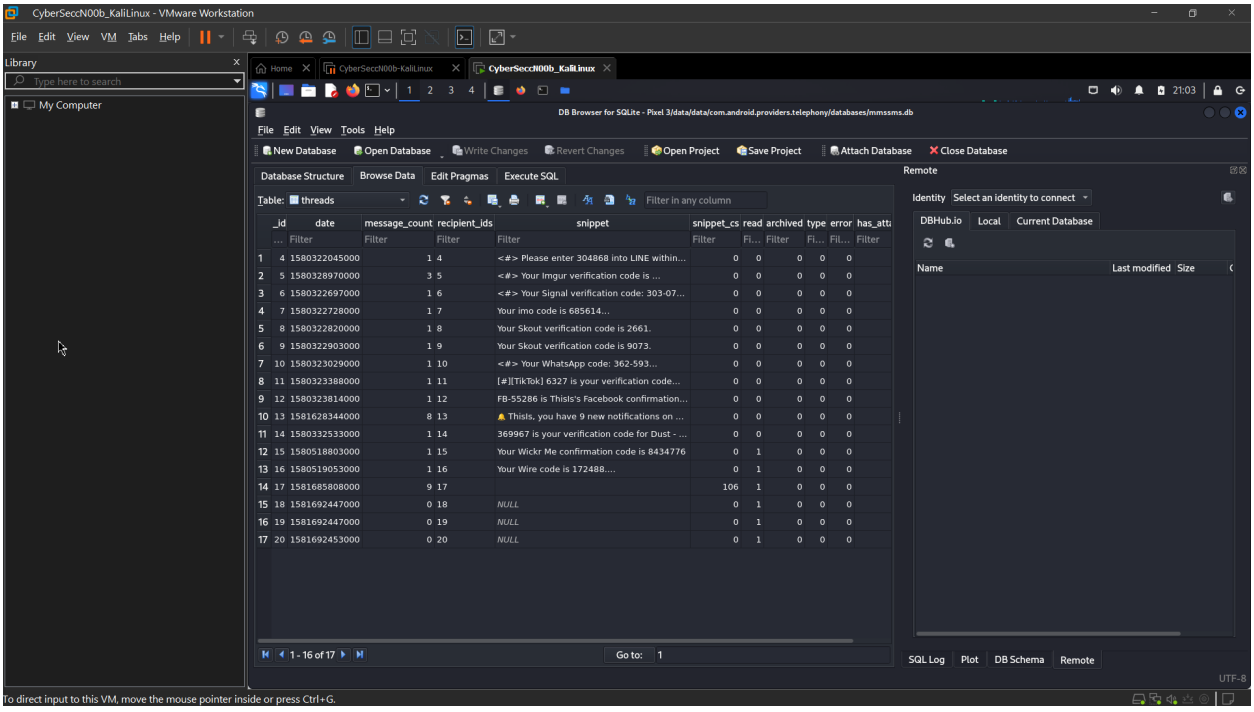
Yr	Mon	Day	Hr	Min	Sec			
2020	- 1	- 29	6	: 20	: 0	PM	GMT	Human date to Timestamp

Epoch timestamp: 1580322000
Timestamp in milliseconds: 1580322000000
Date and time (GMT): Wednesday, January 29, 2020 6:20:00 PM
Date and time (your time zone): Wednesday, January 29, 2020 1:20:00 PM GMT-05:00





What table describes conversation?

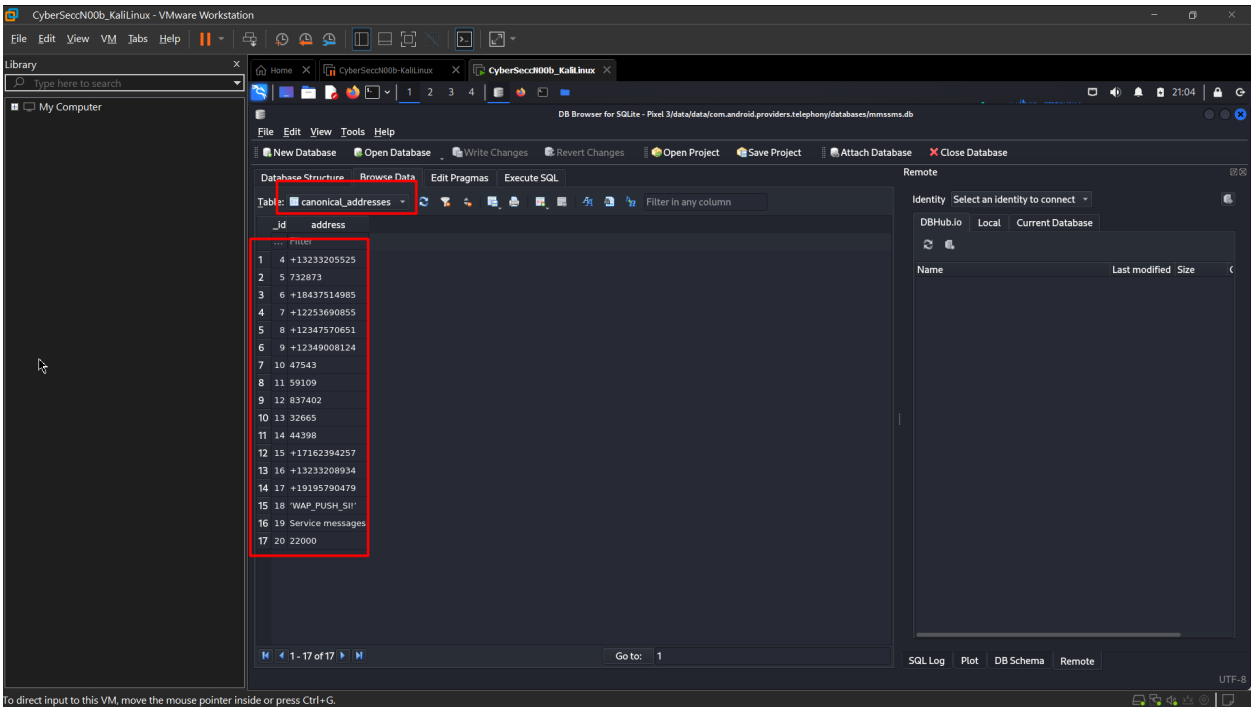


	_id	date	message_count	recipient_ids	snippet	snippet_cs	read	archived	type	error	has_atti
1	4	1580322045000	1	4	<#> Please enter 304868 into LINE within...	0	0	0	0	0	
2	5	1580328970000	3	5	<#> Your Imgur verification code is ...	0	0	0	0	0	
3	6	1580322697000	1	6	<#> Your Signal verification code: 303-07...	0	0	0	0	0	
4	7	1580322728000	1	7	Your imo code is 685614...	0	0	0	0	0	
5	8	1580322820000	1	8	Your Skout verification code is 2661.	0	0	0	0	0	
6	9	1580322903000	1	9	Your Skout verification code is 9073.	0	0	0	0	0	
7	10	1580323029000	1	10	<#> Your WhatsApp code: 362-593...	0	0	0	0	0	
8	11	1580323388000	1	11	[#][TikTok] 6327 is your verification code...	0	0	0	0	0	
9	12	1580323814000	1	12	FB-55286 is Thisis's Facebook confirmation...	0	0	0	0	0	
10	13	1581628344000	8	13	Thisis, you have 9 new notifications on ...	0	0	0	0	0	
11	14	1580332533000	1	14	369967 is your verification code for Dust - ...	0	0	0	0	0	
12	15	1580518803000	1	15	Your Wickr Me confirmation code is 8434776	0	1	0	0	0	
13	16	1580519053000	1	16	Your Wire code is 172488....	0	1	0	0	0	
14	17	1581685808000	9	17		106	1	0	0	0	
15	18	1581692447000	0	18	NULL	0	1	0	0	0	
16	19	1581692447000	0	19	NULL	0	1	0	0	0	
17	20	1581692453000	0	20	NULL	0	1	0	0	0	

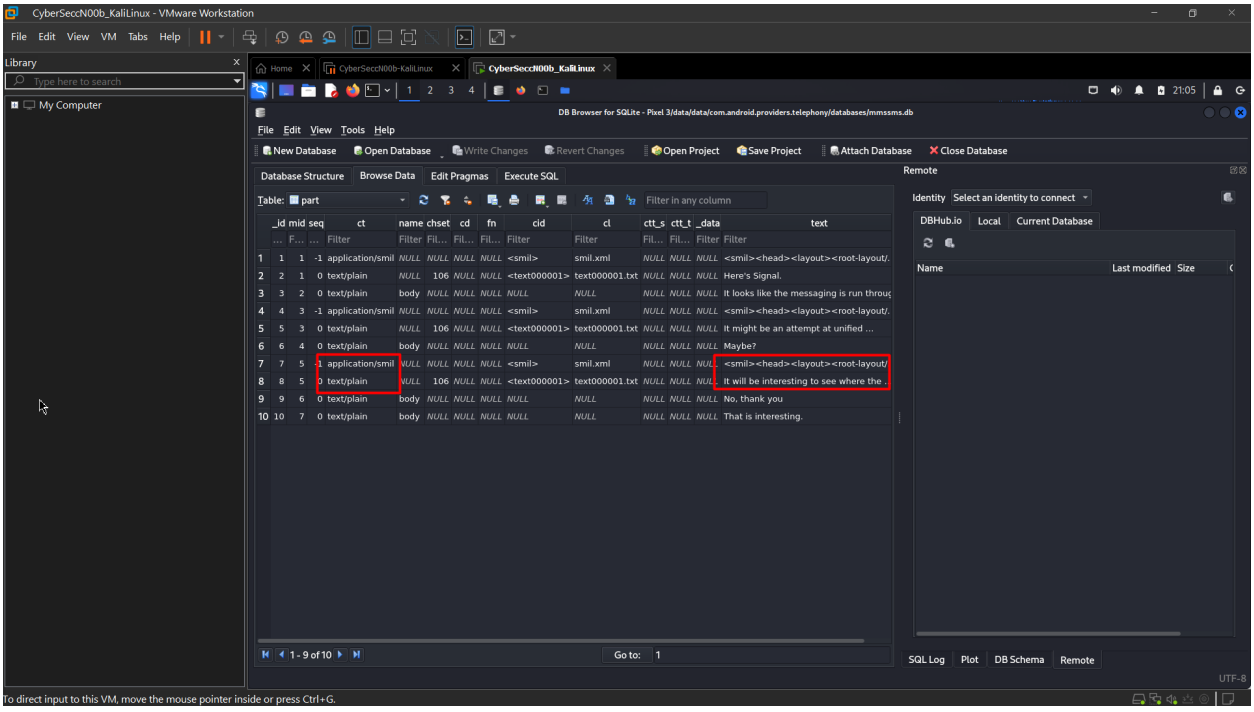
1 - 16 of 17 Go to: 1

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.