

Lab 14: Mobile_App_Investigations_Messaging

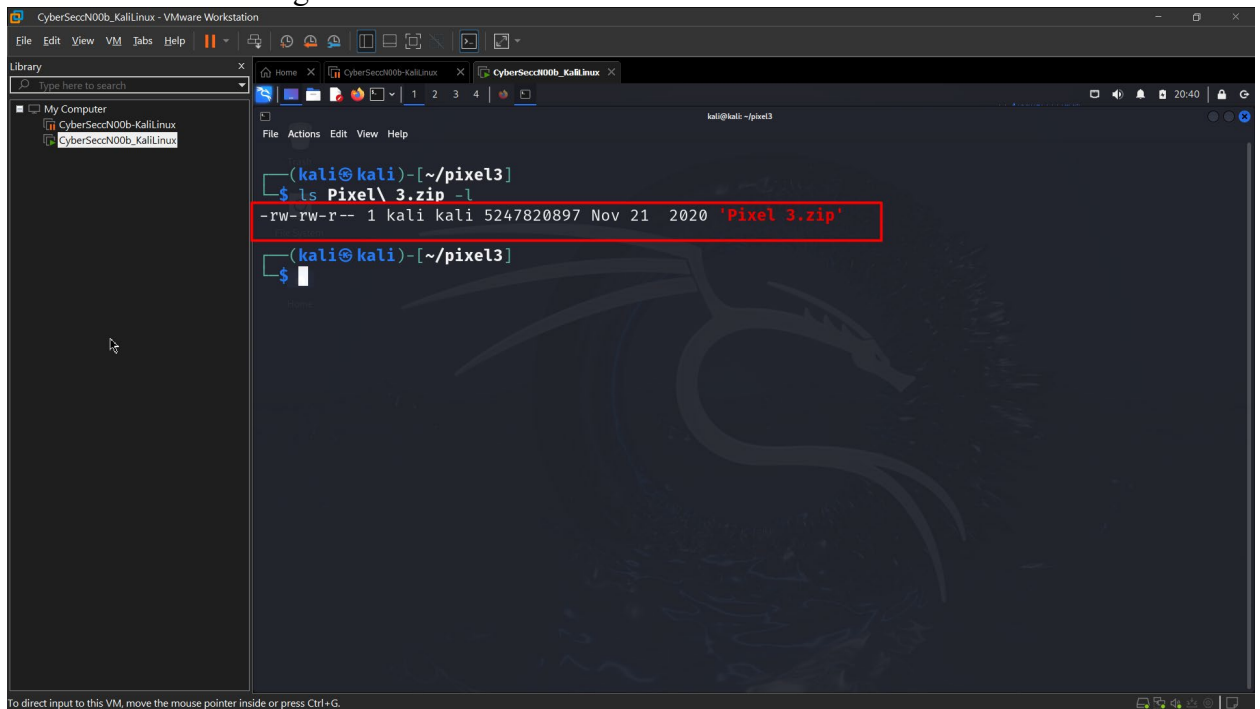
Group: CyberSec_N00b

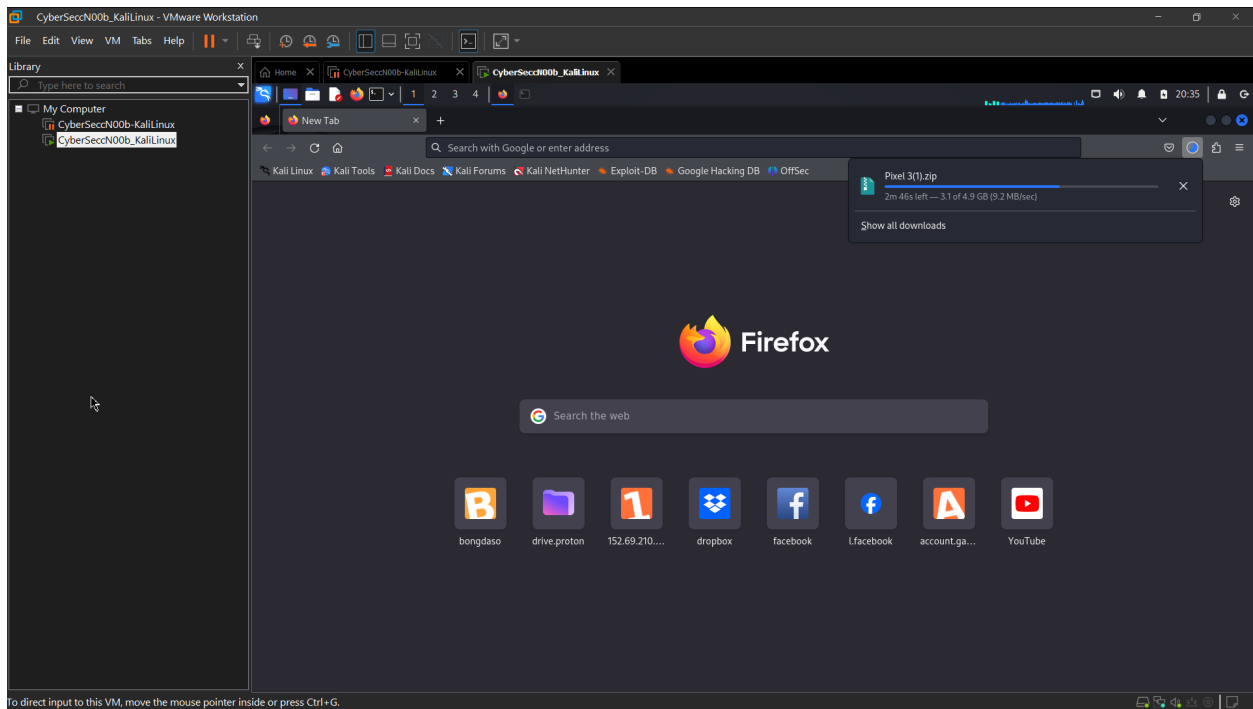
Member:

- 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

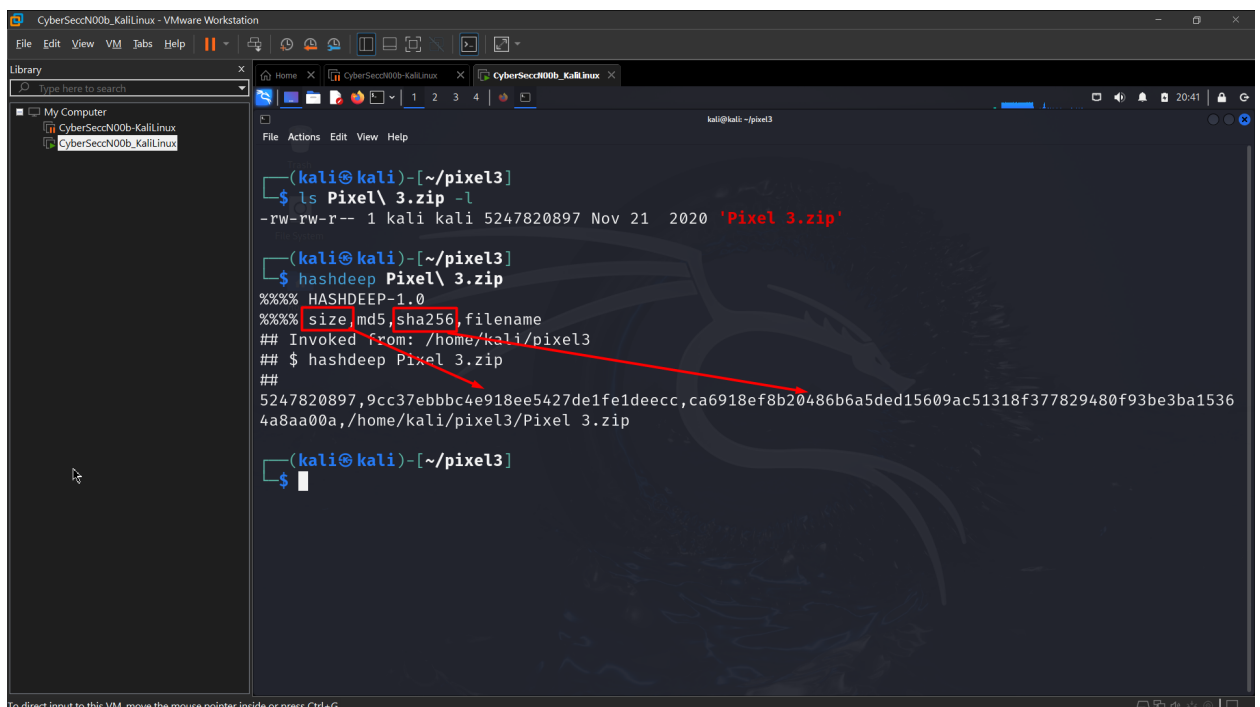
- Download Pixel 3 image





Verify hashes

hashdeep Pixel\ 3.zip



unzip to get Pixel 3 image

```
(kali@kali)-[~/pixel3]
$ ls -l
total 5124836
drwxrwxr-x 11 kali kali      4096 Oct 27 20:45 'Pixel 3'
-rw-rw-r-- 1 kali kali 5247820897 Nov 21 2020 'Pixel 3.zip'
-rw-rw-r-- 1 kali kali       0 Oct 26 01:55 wget-log

(kali@kali)-[~/pixel3]
$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
(kali@kali)-[~/pixel3]
$ ls 'Pixel 3/data/data'
com.android.chrome
com.android.hotwordenrollment.okgoogle
com.android.hotwordenrollment.xgoogle
com.android.keychain
com.android.mtp
com.android.nfc
com.android.providers.calendar
com.android.providers.contacts
com.android.providers.downloads
com.android.providers.media
com.android.providers.telephony
com.android.providers.userdictionary
com.android.service.ims.presence
com.android.traceur
com.android.vending
com.discord
com.enflick.android.TextNow
com.facebook.orca
com.google.android.apps.chromecast.app
com.google.android.apps.docs
com.google.android.apps.docs.editors.docs
com.google.android.apps.dreamliner
com.google.android.apps.enterprise.dmagent
com.google.android.apps.gcs
com.google.android.GoogleCamera
com.google.android.googlequicksearchbox
com.google.android.gsf
com.google.android.ims
com.google.android.inputmethod.latin
com.google.android.keep
com.google.android.markup
com.google.android.music
com.google.android.onetimeinitializer
com.google.android.partnersetup
com.google.android.pixel.setupwizard
com.google.android.projection.gearhead
com.google.android.settings.intelligence
com.google.android.setupwizard
com.google.android.syncadapters.contacts
com.google.android.tts
com.google.android.videos
com.google.android.webview
com.google.android.wfcactivation
com.google.android.youtube
com.google.ar.core
com.google.intelligence.sense
com.google.vr.apps.ornament
com.google.vr.vrcore
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 2. Investigating Messaging Services

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

```
(kali@kali)-[~/pixel3]
$ ls 'Pixel 3/data/data' | grep -i com.android
com.android.chrome
com.android.hotwordenrollment.okgoogle
com.android.hotwordenrollment.xgoogle
com.android.keychain
com.android.mtp
com.android.nfc
com.android.providers.calendar
com.android.providers.contacts
com.android.providers.downloads
com.android.providers.media
com.android.providers.telephony
com.android.providers.userdictionary
com.android.service.ims.presence
com.android.traceur
com.android.vending

(kali@kali)-[~/pixel3]
$
```

- To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Find the location of Java package

```
(kali@kali)-[~/pixel3]
$ tree 'Pixel 3/data/data com.android.providers.telephony' -L 1
Pixel 3/data/data com.android.providers.telephony [error opening dir]
0 directories, 0 files

(kali@kali)-[~/pixel3]
$ tree 'Pixel 3/data/data/com.android.providers.telephony' -L 1
Pixel 3/data/data/com.android.providers.telephony
├── databases
└── shared_prefs

3 directories, 0 files

(kali@kali)-[~/pixel3]
$
```

- To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Find the database location

```

(kali@kali)-[~/pixel3]
$ tree 'Pixel 3/data/data/com.android.providers.telephony' -L 1
Pixel 3/data/data/com.android.providers.telephony [error opening dir]

0 directories, 0 files

(kali@kali)-[~/pixel3]
$ tree 'Pixel 3/data/data/com.android.providers.telephony' -L 1
Pixel 3/data/data/com.android.providers.telephony
├── databases
└── shared_prefs

3 directories, 0 files

(kali@kali)-[~/pixel3]
$ tree 'Pixel 3/data/data/com.android.providers.telephony/databases'
Pixel 3/data/data/com.android.providers.telephony/databases
└── mmssms.db

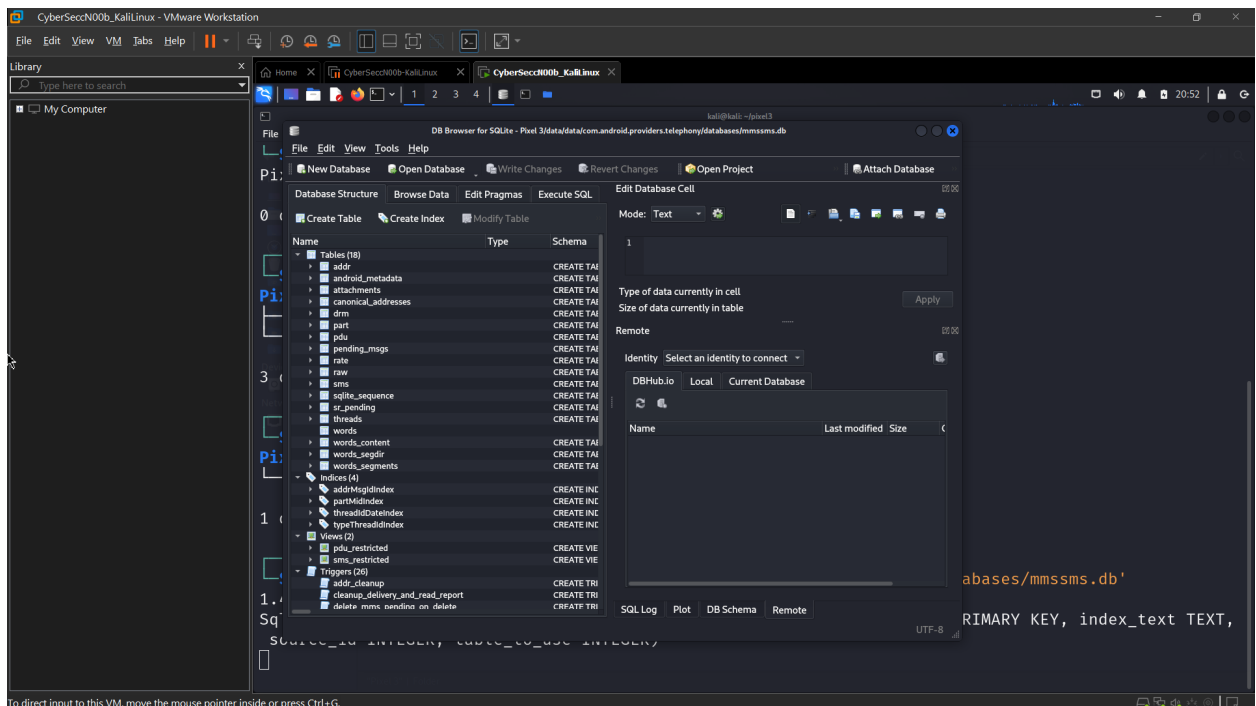
1 directory, 1 file

(kali@kali)-[~/pixel3]
$

```

- To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Show all tables in the database

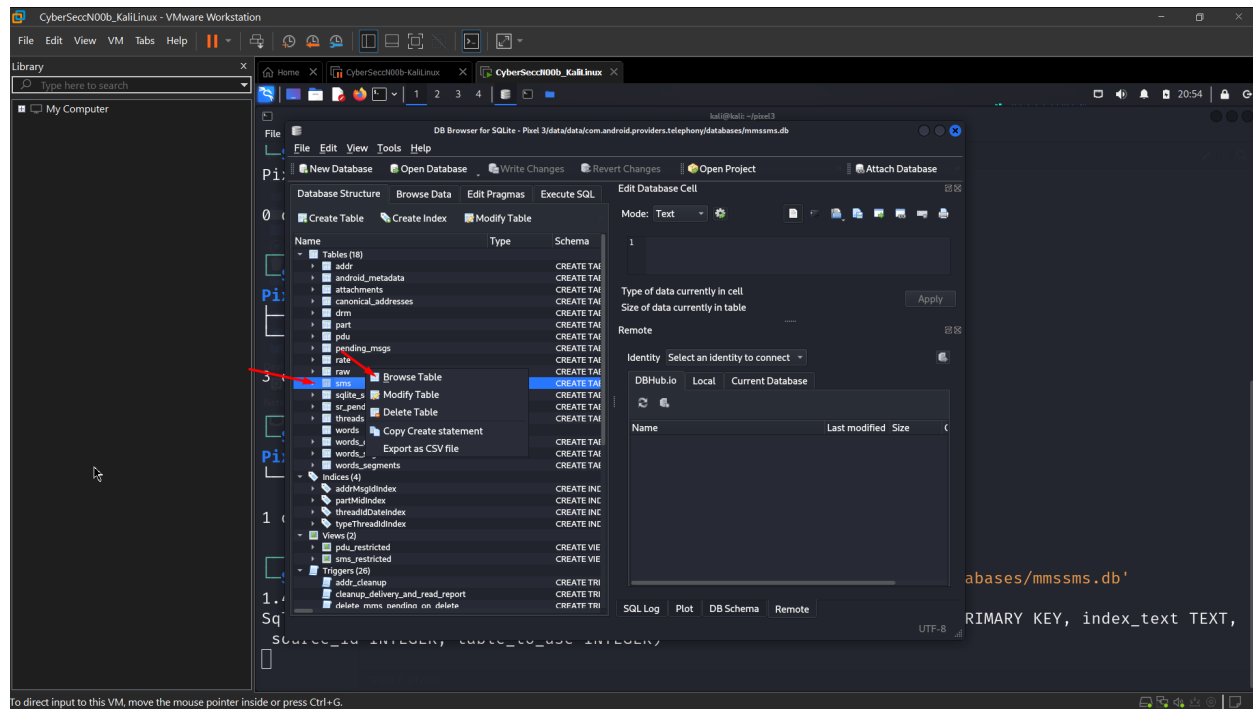


- To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

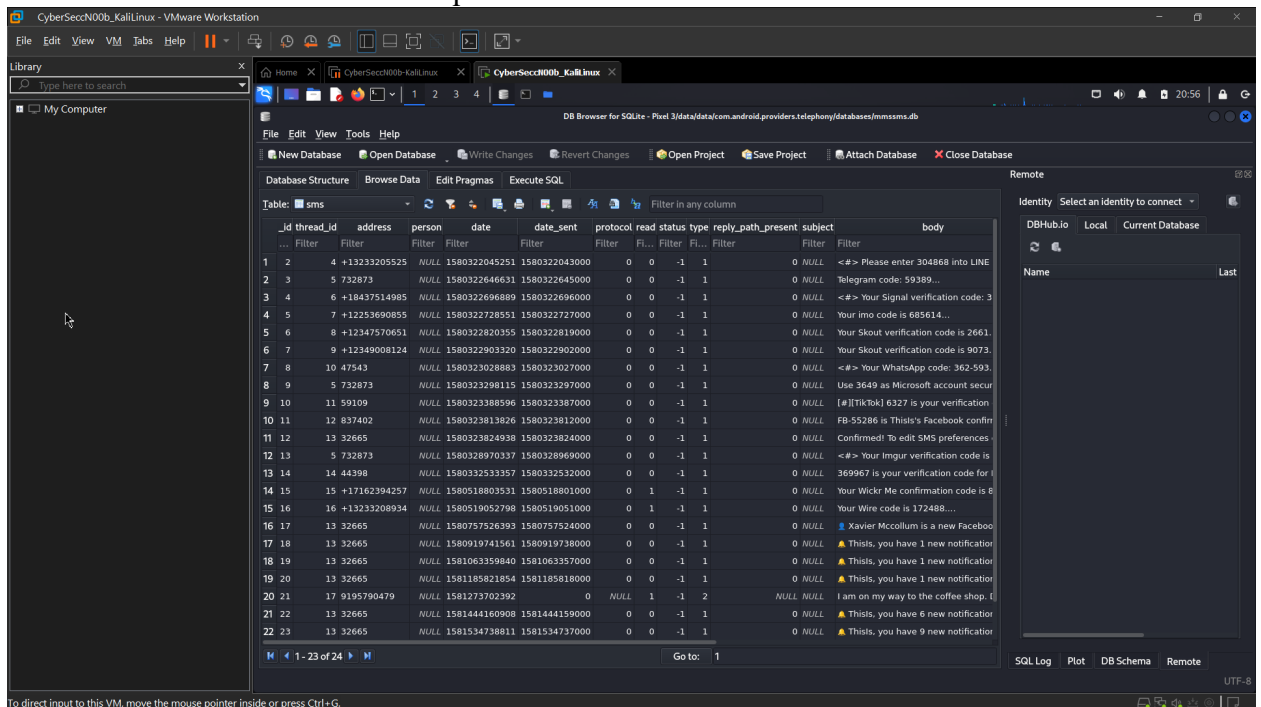
sms: message log

- 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

CyberSecN00b_KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer

DB Browser for SQLite - Plot3 (/data/com.android.providers.telephony/databases/mmsms.db)

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragma Execute SQL

Table: sms

_id	thread_id	address	person	date	date_sent	protocol	read	status	type	reply_path_present	subject
1	2	+13233205525	NULL	1580322045251	1580322043000	0	0	-1	1	0	NULL <#> Please
2	3	+132873	NULL	1580322646631	1580322645000	0	0	-1	1	0	NULL telegram co
3	4	+18437514985	NULL	1580322696889	1580322696000	0	0	-1	1	0	NULL <#> Your Sh
4	5	+12253690855	NULL	1580322728551	1580322727000	0	0	-1	1	0	NULL Your lmo cod
5	6	+12347570651	NULL	1580322820355	1580322819000	0	0	-1	1	0	NULL Your Skout v
6	7	+12349008124	NULL	1580322803320	1580322902000	0	0	-1	1	0	NULL Your Skout v
7	8	10 47543	NULL	1580323028883	1580323027000	0	0	-1	1	0	NULL <#> Your W
8	9	5 732873	NULL	1580323298115	1580323297000	0	0	-1	1	0	NULL Use 3649 as
9	10	11 59109	NULL	1580323388596	1580323387000	0	0	-1	1	0	NULL [#]TikTok 6
10	11	12 837402	NULL	1580323813826	1580323812000	0	0	-1	1	0	NULL FB-55286 is
11	12	13 32665	NULL	1580323824938	1580323824000	0	0	-1	1	0	NULL Confirmed! T
12	13	5 732873	NULL	1580328970337	1580328969000	0	0	-1	1	0	NULL <#> Your ltr
13	14	14 44398	NULL	1580332533357	1580332532000	0	0	-1	1	0	NULL 369967 is yo
14	15	+17162394257	NULL	1580518803531	1580518801000	0	1	-1	1	0	NULL Your Wickr M
15	16	+13233208934	NULL	1580519052798	1580519051000	0	1	-1	1	0	NULL Your Wire co
16	17	13 32665	NULL	1580757526393	1580757524000	0	0	-1	1	0	NULL Xavier Mc
17	18	13 32665	NULL	1580919741561	1580919738000	0	0	-1	1	0	NULL Thisis, yot
18	19	13 32665	NULL	1581063359840	1581063357000	0	0	-1	1	0	NULL Thisis, yot
19	20	13 32665	NULL	1581185821854	1581185818000	0	0	-1	1	0	NULL Thisis, yot
20	21	17 9195790479	NULL	1581273702392	0	NULL	1	-1	2	0	NULL I am on my v
21	22	13 32665	NULL	1581444160908	1581444159000	0	0	-1	1	0	NULL Thisis, yot
22	23	13 32665	NULL	1581534738811	1581534737000	0	0	-1	1	0	NULL Thisis, yot

1 - 23 of 24

Go to: 1

Remote

Identity Select an identity to connect

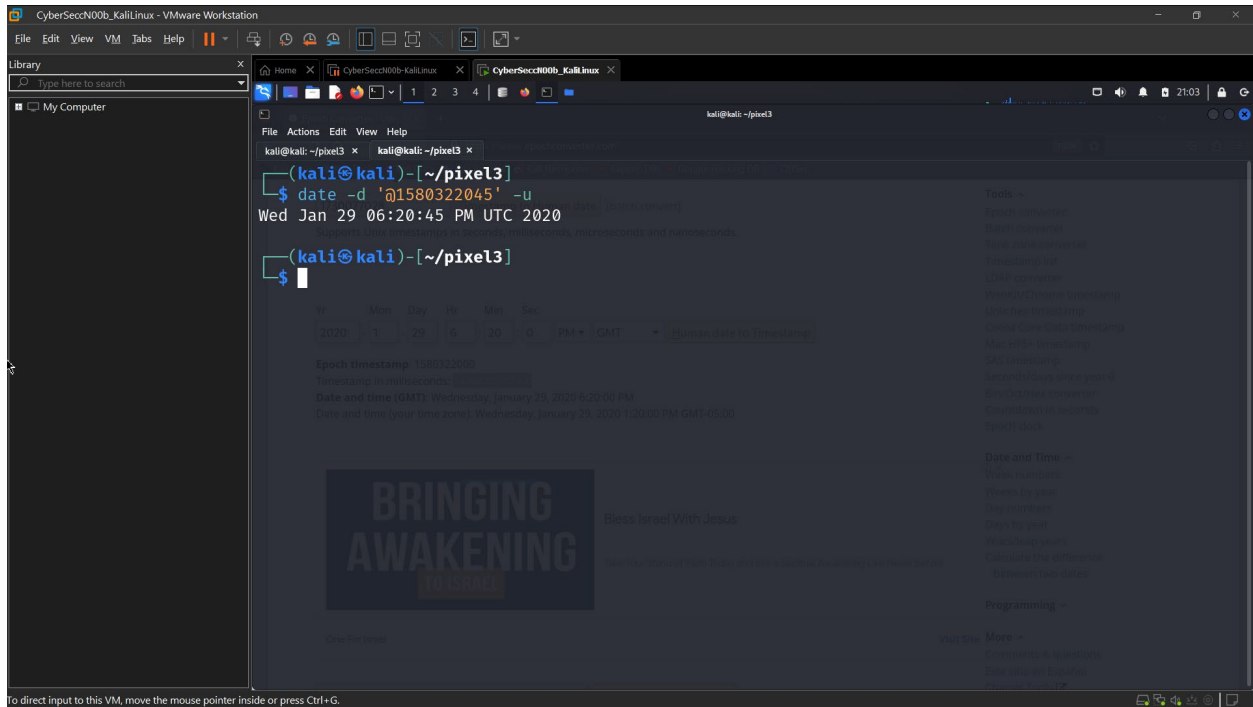
DBHub.io Local Current Database

Name Last modified Size

SQL Log Plot DB Schema Remote

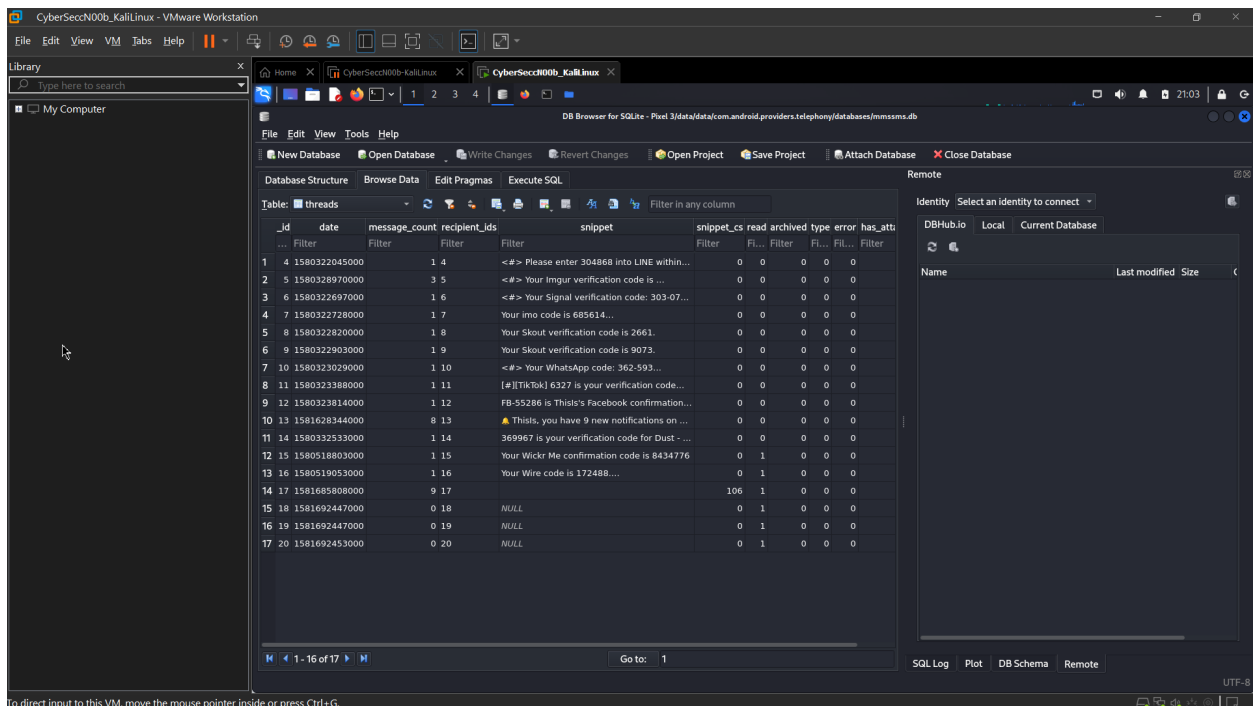
UTF-8

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

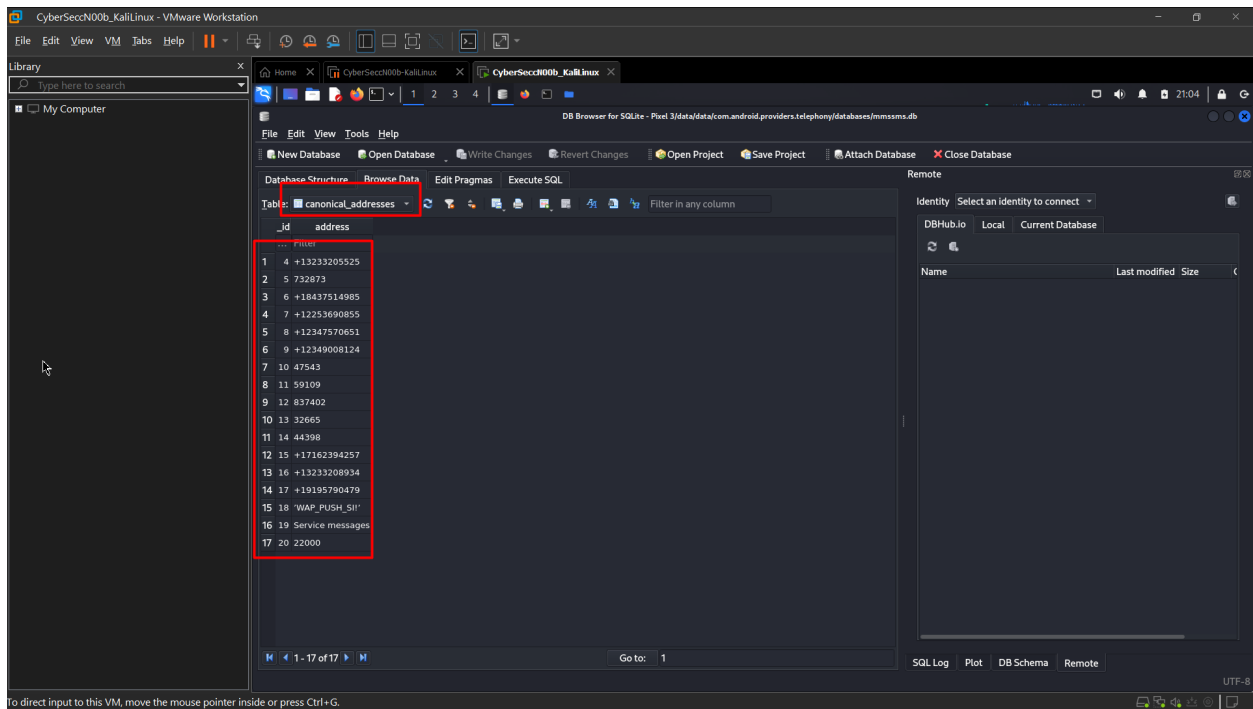
What table describes conversation?



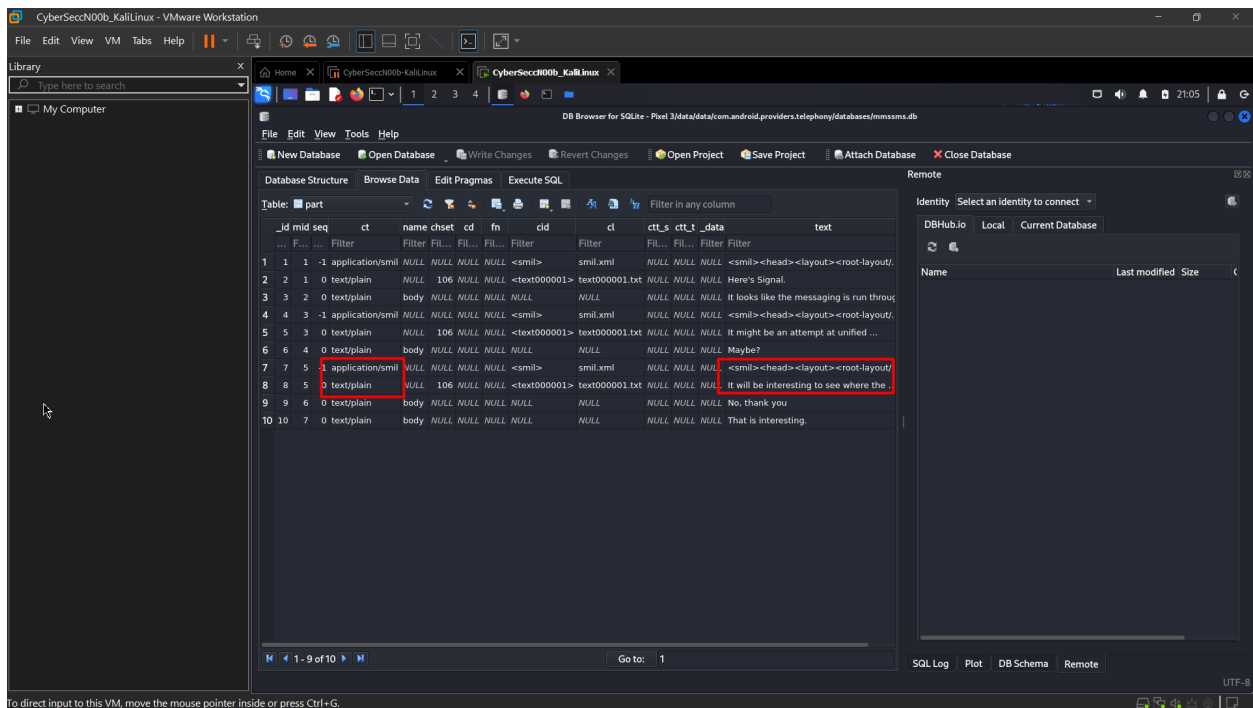
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

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.