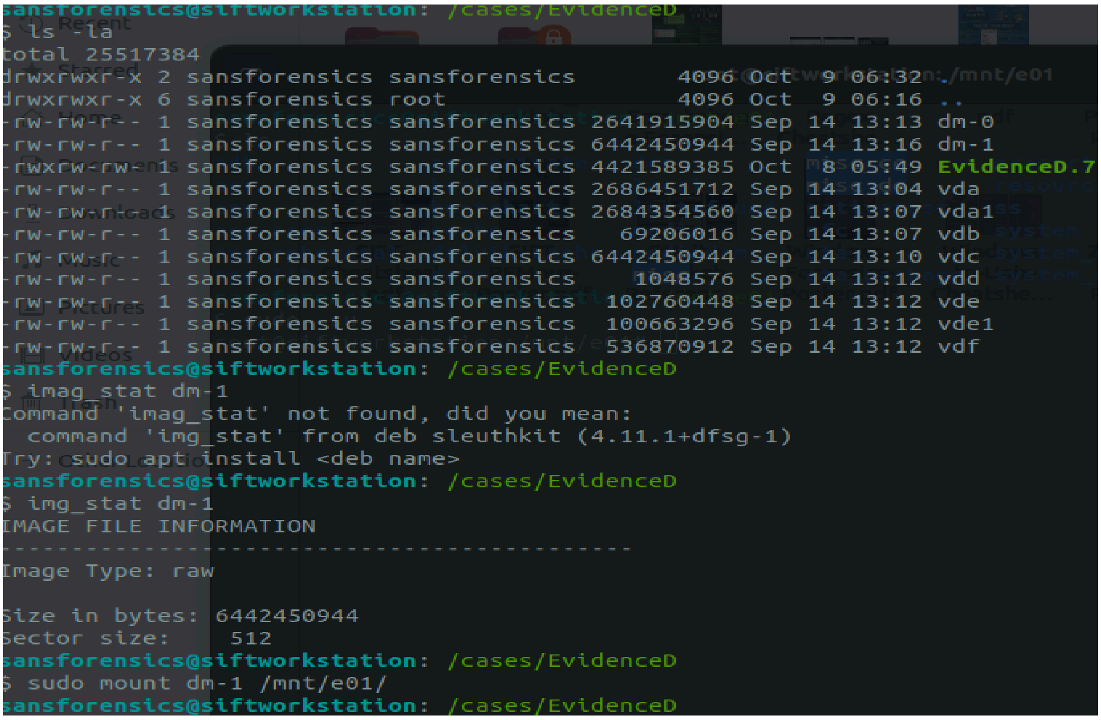
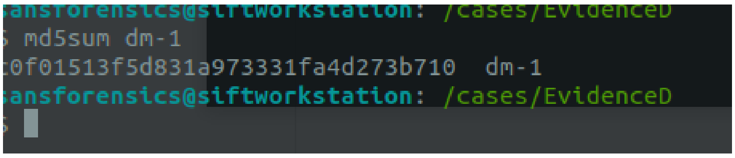
Evidence D – A disk image of a damaged mobile phone found in Alex's apartment under some furniture.

To investigate the disk image, I first unzipped it using the command 7z e EvidenceD.7z. After extraction, I checked the disk sizes and selected the largest disk image, assuming it would contain the most valuable data. I then mounted this disk directly to the /mnt/e01 directory, as it did not require any offsets. The system recognises the disk automatically. To ensure data integrity, I worked with a copy of the disk by mounting the duplicate image. Before proceeding, I verified the integrity of the copied disk using the md5sum command to confirm that no data had been altered. Since Android devices have many directories and files restricted to root access, I switched to root privileges to gain full access to the disk's contents.



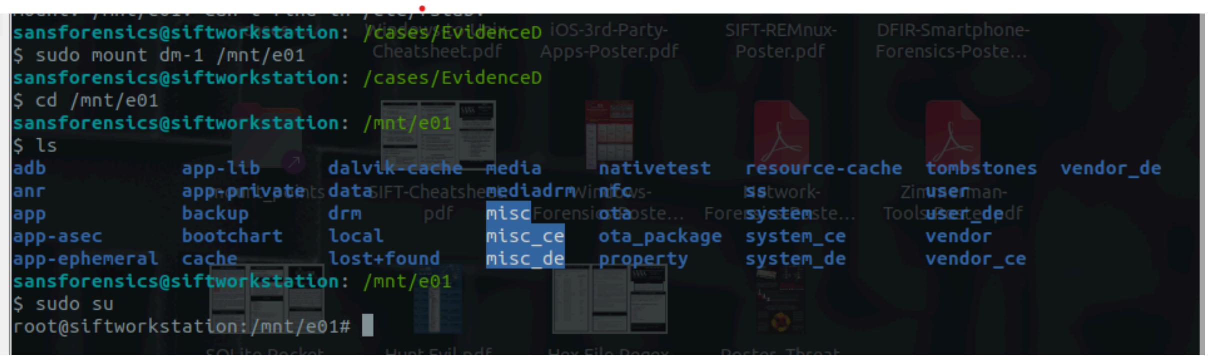
```
sansforensics@siftworkstation: /cases/EvidenceD
$ ls -la
total 25517384
drwxrwxr-x 2 sansforensics sansforensics       4096 Oct  9 06:32 .
drwxrwxr-x 6 sansforensics root                4096 Oct  9 06:16 ..
-rw-rw-r-- 1 sansforensics sansforensics 2641915904 Sep 14 13:13 dm-0
-rw-rw-r-- 1 sansforensics sansforensics 6442450944 Sep 14 13:16 dm-1
-rwxrw-rw- 1 sansforensics sansforensics 4421589385 Oct  8 05:49 EvidenceD.7
-rw-rw-r-- 1 sansforensics sansforensics 2686451712 Sep 14 13:04 vda
-rw-rw-r-- 1 sansforensics sansforensics 2684354560 Sep 14 13:07 vda1
-rw-rw-r-- 1 sansforensics sansforensics   69206016 Sep 14 13:07 vdb
-rw-rw-r-- 1 sansforensics sansforensics 6442450944 Sep 14 13:10 vdc
-rw-rw-r-- 1 sansforensics sansforensics    1048576 Sep 14 13:12 vdd
-rw-rw-r-- 1 sansforensics sansforensics  102760448 Sep 14 13:12 vde
-rw-rw-r-- 1 sansforensics sansforensics  100663296 Sep 14 13:12 vde1
-rw-rw-r-- 1 sansforensics sansforensics  536870912 Sep 14 13:12 vdf
sansforensics@siftworkstation: /cases/EvidenceD
$ imag_stat dm-1
Command 'imag_stat' not found, did you mean:
  command 'img_stat' from deb sleuthkit (4.11.1+dfsg-1)
Try: sudo apt install <deb name>
sansforensics@siftworkstation: /cases/EvidenceD
$ img_stat dm-1
IMAGE FILE INFORMATION
--------------------------------------------
Image Type: raw

Size in bytes: 6442450944
Sector size:    512
sansforensics@siftworkstation: /cases/EvidenceD
$ sudo mount dm-1 /mnt/e01/
sansforensics@siftworkstation: /cases/EvidenceD
```



```
sansforensics@siftworkstation: /cases/EvidenceD
$ md5sum dm-1
0f01513f5d831a973331fa4d273b710  dm-1
sansforensics@siftworkstation: /cases/EvidenceD
$ 
```

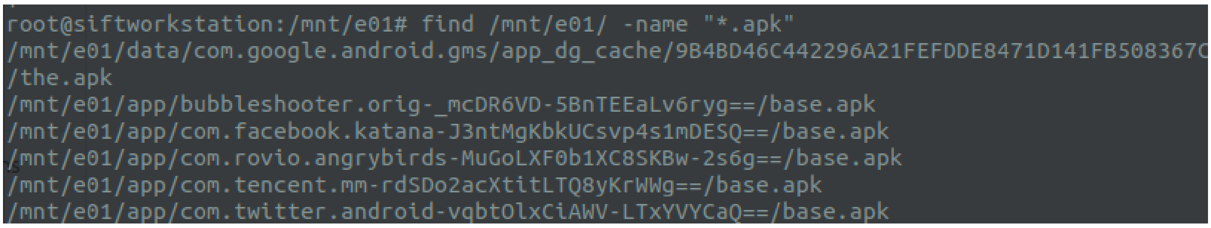
Switch to the root user, as many Android files and directories are restricted to root access only



```
mount: /mnt/e01: can't find in /etc/fstab.
sansforensics@siftworkstation: /cases/EvidenceD
$ sudo mount dm-1 /mnt/e01
sansforensics@siftworkstation: /cases/EvidenceD
$ cd /mnt/e01
sansforensics@siftworkstation: /mnt/e01
$ ls
adb            app-lib      dalvik-cache  media     nativetest   resource-cache  tombstones  vendor_de
anr            app-private  data          mediadrm  nfc          ss              user
app            backup       drm           misc      ota          system          user_de
app-asec       bootchart    local         misc_ce   ota_package  system_ce       vendor
app-ephemeral  cache        lost+found    misc_de   property     system_de       vendor_ce
sansforensics@siftworkstation: /mnt/e01
$ sudo su
root@siftworkstation:/mnt/e01# 
```

What are the non-stock applications installed on the phone?

To identify non-stock applications installed on the phone, I used the command: find /mnt/e01/ -name "*.apk". From the resulting list, I determined the non-stock apps by comparing the package names. All applications listed, except the first, were non-stock, indicating third-party apps installed by the phone owner.



```
root@siftworkstation:/mnt/e01# find /mnt/e01/ -name "*.apk"
/mnt/e01/data/com.google.android.gms/app_dg_cache/9B4BD46C442296A21FEFDDE8471D141FB508367C
/the.apk
/mnt/e01/app/bubbleshooter.orig-_mcDR6VD-5BnTEEaLv6ryg==/base.apk
/mnt/e01/app/com.facebook.katana-J3ntMgKbkUCsvp4s1mDESQ==/base.apk
/mnt/e01/app/com.rovio.angrybirds-MuGoLXF0b1XC8SKBw-2s6g==/base.apk
/mnt/e01/app/com.tencent.mm-rdSDo2acXtitLTQ8yKrWWg==/base.apk
/mnt/e01/app/com.twitter.android-vqbtOlxCiAWV-LTxYVYCaQ==/base.apk
```

Who is in the contacts list? What messages and calls have been sent and received by the phone?

To retrieve the phone’s contacts, messages, and call logs, I searched for specific databases in the device’s storage. I first searched for SMS data using “find /mnt/e01 -name "*sms*".

This search revealed the mmssms.db file, which I copied to the cases folder. The file was originally owned by root, so I had to modify the file permissions and accessing it using SQLite Browser. Similarly, for the call log and contacts, I located the respective databases in these paths:

- Call log: /mnt/e01/data/com.android.providers.contacts/databases/calllog.db
- Contacts: /mnt/e01/data/com.android.providers.contacts/databases/contacts2.db

After adjusting the permissions, I opened both databases using SQLite Browser.

Contacts:

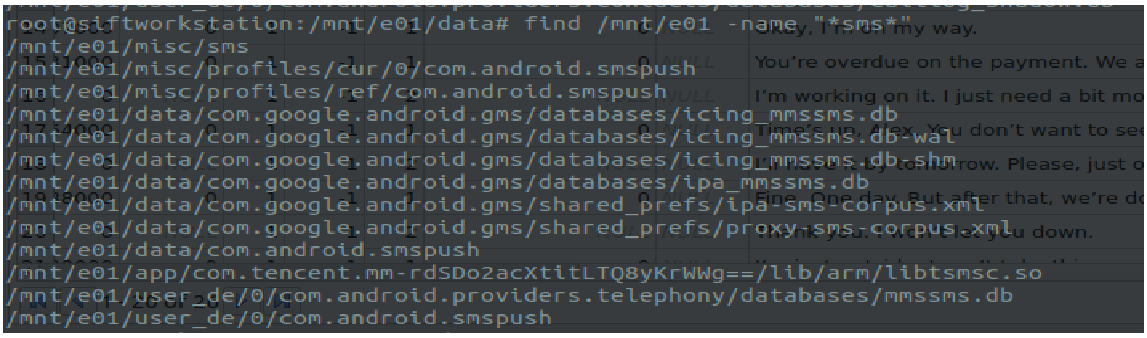
- The contacts list included: Lily, Sophia, Mom, and Dad.

Messages:

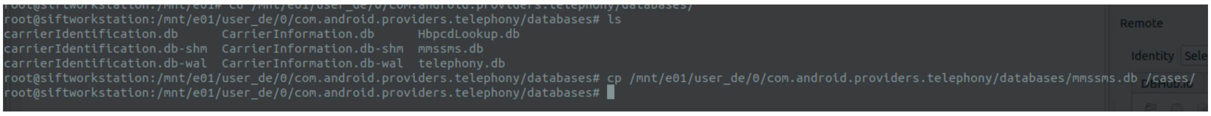
- Messages were exchanged with Lily, Sophia, and unknown person.

Call Logs:

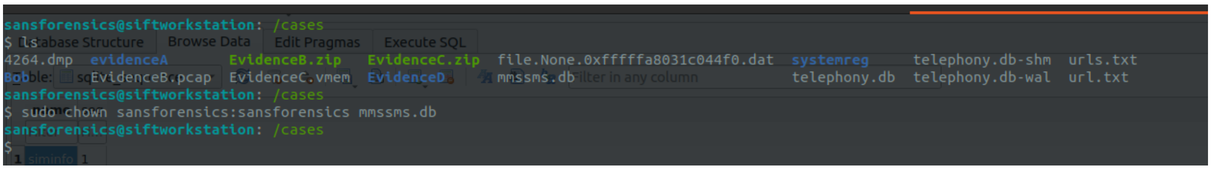
- Lily and Sophia both called Alex.



```
root@siftworkstation:/mnt/e01/data# find /mnt/e01 -name "*sms*"
/mnt/e01/misc/sms
/mnt/e01/misc/profiles/cur/0/com.android.smspush
/mnt/e01/misc/profiles/ref/com.android.smspush
/mnt/e01/data/com.google.android.gms/databases/icing_mmssms.db
/mnt/e01/data/com.google.android.gms/databases/icing_mmssms.db-wal
/mnt/e01/data/com.google.android.gms/databases/icing_mmssms.db-shm
/mnt/e01/data/com.google.android.gms/databases/ipa_mmssms.db
/mnt/e01/data/com.google.android.gms/shared_prefs/ipa-sms-corpus.xml
/mnt/e01/data/com.google.android.gms/shared_prefs/proxy-sms-corpus.xml
/mnt/e01/data/com.android.smspush
/mnt/e01/app/com.tencent.mm-rdSDo2acXtitLTQ8yKrWWg==/lib/arm/libtsmsc.so
/mnt/e01/user_de/0/com.android.providers.telephony/databases/mmssms.db
/mnt/e01/user_de/0/com.android.smspush
```

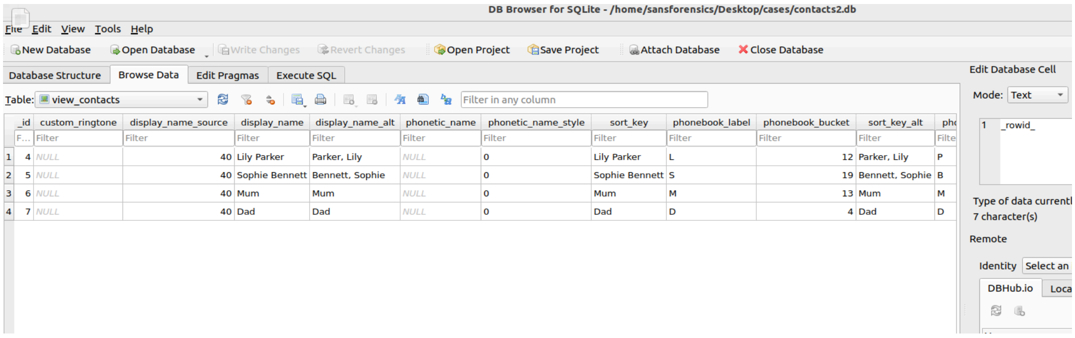


```
root@siftworkstation:/mnt/e01# cd /mnt/e01/user_de/0/com.android.providers.telephony/databases/
root@siftworkstation:/mnt/e01/user_de/0/com.android.providers.telephony/databases# ls
carrierIdentification.db      CarrierInformation.db      HbpcdLookup.db
carrierIdentification.db-shm  CarrierInformation.db-shm  mmssms.db
carrierIdentification.db-wal  CarrierInformation.db-wal  telephony.db
root@siftworkstation:/mnt/e01/user_de/0/com.android.providers.telephony/databases# cp /mnt/e01/user_de/0/com.android.providers.telephony/databases/mmssms.db /cases/
root@siftworkstation:/mnt/e01/user_de/0/com.android.providers.telephony/databases# 
```

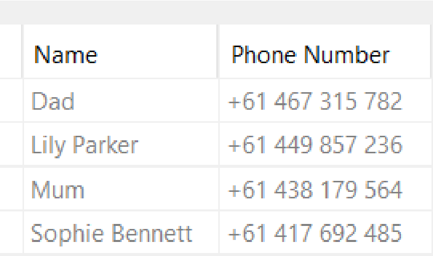


```
sansforensics@siftworkstation: /cases
$ ls
4264.dmp  evidenceA          EvidenceB.zip   EvidenceC.zip  file.None.0xfffffa8031c044f0.dat  systemreg     telephony.db-shm  urls.txt
Bob       EvidenceB.pcap     EvidenceC.vmem  EvidenceD      mmssms.db                         telephony.db  telephony.db-wal  url.txt
sansforensics@siftworkstation: /cases
$ sudo chown sansforensics:sansforensics mmssms.db
sansforensics@siftworkstation: /cases
$
```

Contacts list

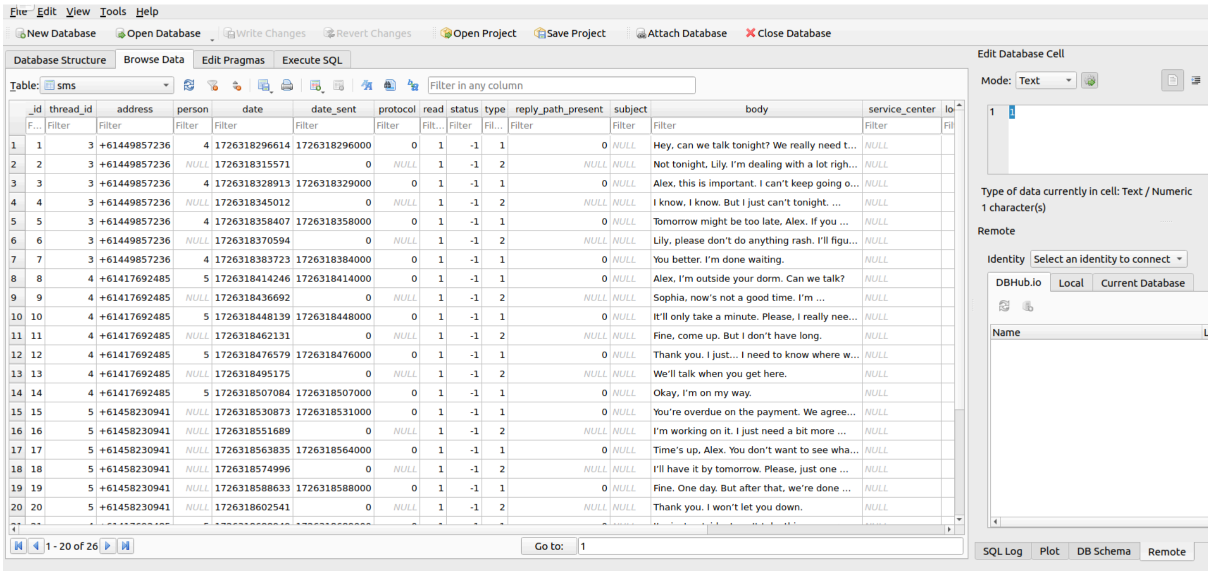


	_id	custom_ringtone	display_name_source	display_name	display_name_alt	phonetic_name	phonetic_name_style	sort_key	phonebook_label	phonebook_bucket	sort_key_alt	phc
1	4	NULL	40	Lily Parker	Parker, Lily	NULL	0	Lily Parker	L	12	Parker, Lily	P
2	5	NULL	40	Sophie Bennett	Bennett, Sophie	NULL	0	Sophie Bennett	S	19	Bennett, Sophie	B
3	6	NULL	40	Mum	Mum	NULL	0	Mum	M	13	Mum	M
4	7	NULL	40	Dad	Dad	NULL	0	Dad	D	4	Dad	D



Name	Phone Number
Dad	+61 467 315 782
Lily Parker	+61 449 857 236
Mum	+61 438 179 564
Sophie Bennett	+61 417 692 485

SMS



	_id	thread_id	address	person	date	date_sent	protocol	read	status	type	reply_path_present	subject	body	service_center
1	1	3	+61449857236	4	1726318296614	1726318296000	0	1	-1	1	0	NULL	Hey, can we talk tonight? We really need t...	NULL
2	2	3	+61449857236	NULL	1726318315571	0	NULL	1	-1	2	NULL	NULL	Not tonight, Lily. I’m dealing with a lot righ...	NULL
3	3	3	+61449857236	4	1726318328913	1726318329000	0	1	-1	1	0	NULL	Alex, this is important. I can’t keep going o...	NULL
4	4	3	+61449857236	NULL	1726318345012	0	NULL	1	-1	2	NULL	NULL	I know, I know. But I just can’t tonight. ...	NULL
5	5	3	+61449857236	4	1726318358407	1726318358000	0	1	-1	1	0	NULL	Tomorrow might be too late, Alex. If you ...	NULL
6	6	3	+61449857236	NULL	1726318370594	0	NULL	1	-1	2	NULL	NULL	Lily, please don’t do anything rash. I’ll figu...	NULL
7	7	3	+61449857236	4	1726318383723	1726318384000	0	1	-1	1	0	NULL	You better. I’m done waiting.	NULL
8	8	4	+61417692485	5	1726318414246	1726318414000	0	1	-1	1	0	NULL	Alex, I’m outside your dorm. Can we talk?	NULL
9	9	4	+61417692485	NULL	1726318436692	0	NULL	1	-1	2	NULL	NULL	Sophia, now’s not a good time. I’m ...	NULL
10	10	4	+61417692485	5	1726318448139	1726318448000	0	1	-1	1	0	NULL	It’ll only take a minute. Please, I really nee...	NULL
11	11	4	+61417692485	NULL	1726318462131	0	NULL	1	-1	2	NULL	NULL	Fine, come up. But I don’t have long.	NULL
12	12	4	+61417692485	5	1726318476579	1726318476000	0	1	-1	1	0	NULL	Thank you. I just... I need to know where w...	NULL
13	13	4	+61417692485	NULL	1726318495175	0	NULL	1	-1	2	NULL	NULL	We’ll talk when you get here.	NULL
14	14	4	+61417692485	5	1726318507084	1726318507000	0	1	-1	1	0	NULL	Okay, I’m on my way.	NULL
15	15	5	+61458230941	NULL	1726318530873	1726318531000	0	1	-1	1	0	NULL	You’re overdue on the payment. We agree...	NULL
16	16	5	+61458230941	NULL	1726318551689	0	NULL	1	-1	2	NULL	NULL	I’m working on it. I just need a bit more ...	NULL
17	17	5	+61458230941	NULL	1726318563835	1726318564000	0	1	-1	1	0	NULL	Time’s up, Alex. You don’t want to see wha...	NULL
18	18	5	+61458230941	NULL	1726318574996	0	NULL	1	-1	2	NULL	NULL	I’ll have it by tomorrow. Please, just one ...	NULL
19	19	5	+61458230941	NULL	1726318588633	1726318588000	0	1	-1	1	0	NULL	Fine. One day. But after that, we’re done ...	NULL
20	20	5	+61458230941	NULL	1726318602541	0	NULL	1	-1	2	NULL	NULL	Thank you. I won’t let you down.	NULL

Call logs

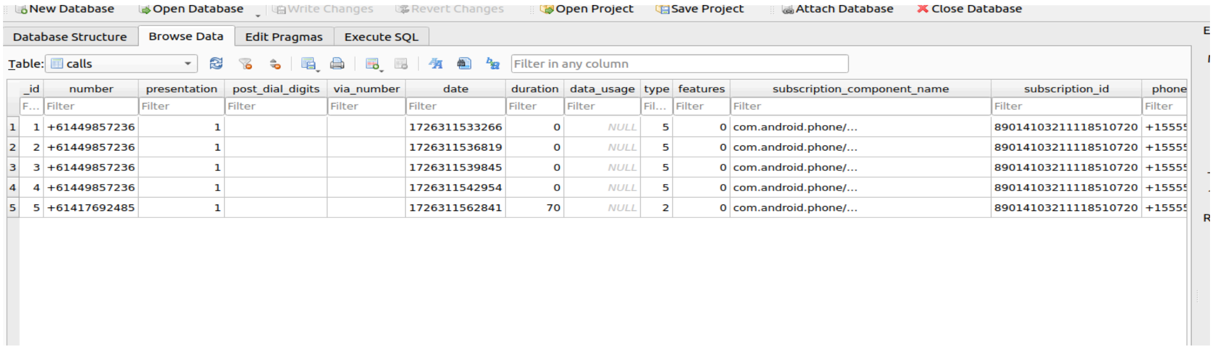


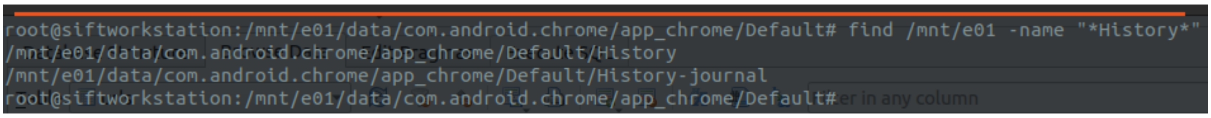
Table: calls

	_id	number	presentation	post_dial_digits	via_number	date	duration	data_usage	type	features	subscription_component_name	subscription_id	phone
	F...	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Fil...	Filter	Filter	Filter	Filter
1	1	+61449857236	1			1726311533266	0	NULL	5	0	com.android.phone/...	89014103211118510720	+15555
2	2	+61449857236	1			1726311536819	0	NULL	5	0	com.android.phone/...	89014103211118510720	+15555
3	3	+61449857236	1			1726311539845	0	NULL	5	0	com.android.phone/...	89014103211118510720	+15555
4	4	+61449857236	1			1726311542954	0	NULL	5	0	com.android.phone/...	89014103211118510720	+15555
5	5	+61417692485	1			1726311562841	70	NULL	2	0	com.android.phone/...	89014103211118510720	+15555

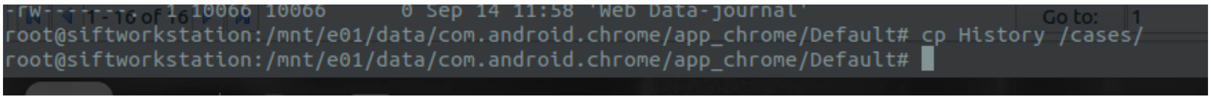
What Internet searches has the owner of the phone made?

To find evidence of the owner's internet activity, I searched for Chrome history using: find /mnt/e01 -name "*History*".

This command located the Chrome history database, which I copied to the cases folder. After changing the necessary file permissions, I was able to analyse the owner’s internet search history using SQLite Browser.

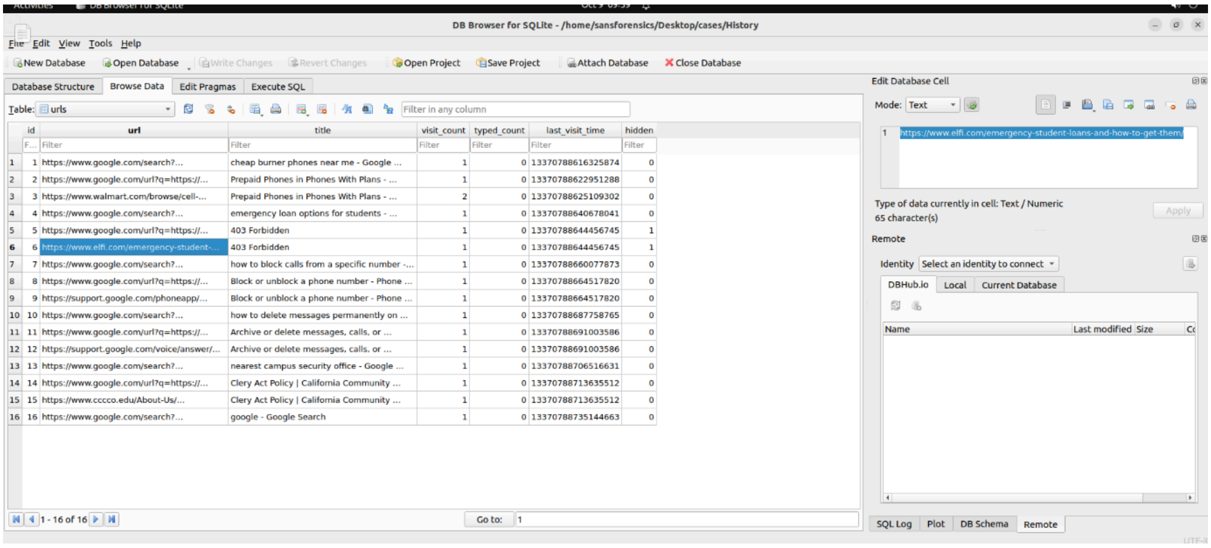


```
root@siftworkstation:/mnt/e01/data/com.android.chrome/app_chrome/Default# find /mnt/e01 -name "*History*"
/mnt/e01/data/com.android.chrome/app_chrome/Default/History
/mnt/e01/data/com.android.chrome/app_chrome/Default/History-journal
root@siftworkstation:/mnt/e01/data/com.android.chrome/app_chrome/Default#
```



```
-rw------- 1 10066 10066        0 Sep 14 11:58 'Web Data-journal'
root@siftworkstation:/mnt/e01/data/com.android.chrome/app_chrome/Default# cp History /cases/
root@siftworkstation:/mnt/e01/data/com.android.chrome/app_chrome/Default# 
```

Internet Searches on Chrome



DB Browser for SQLite - /home/sansforensics/Desktop/cases/History

Table: urls

	id	url	title	visit_count	typed_count	last_visit_time	hidden
	F...	Filter	Filter	Filter	Filter	Filter	Filter
1	1	https://www.google.com/search?...	cheap burner phones near me - Google ...	1	0	13370788616325874	0
2	2	https://www.google.com/url?q=https://...	Prepaid Phones in Phones With Plans - ...	1	0	13370788622951288	0
3	3	https://www.walmart.com/browse/cell-...	Prepaid Phones in Phones With Plans - ...	2	0	13370788625109302	0
4	4	https://www.google.com/search?...	emergency loan options for students - ...	1	0	13370788640678041	0
5	5	https://www.google.com/url?q=https://...	403 Forbidden	1	0	13370788644456745	1
6	6	https://www.elfi.com/emergency-student-...	403 Forbidden	1	0	13370788644456745	1
7	7	https://www.google.com/search?...	how to block calls from a specific number -...	1	0	13370788660077873	0
8	8	https://www.google.com/url?q=https://...	Block or unblock a phone number - Phone ...	1	0	13370788664517820	0
9	9	https://support.google.com/phoneapp/...	Block or unblock a phone number - Phone ...	1	0	13370788664517820	0
10	10	https://www.google.com/search?...	how to delete messages permanently on ...	1	0	13370788687758765	0
11	11	https://www.google.com/url?q=https://...	Archive or delete messages, calls, or ...	1	0	13370788691003586	0
12	12	https://support.google.com/voice/answer/...	Archive or delete messages, calls, or ...	1	0	13370788691003586	0
13	13	https://www.google.com/search?...	nearest campus security office - Google ...	1	0	13370788706516631	0
14	14	https://www.google.com/url?q=https://...	Clery Act Policy | California Community ...	1	0	13370788713635512	0
15	15	https://www.cccco.edu/About-Us/...	Clery Act Policy | California Community ...	1	0	13370788713635512	0
16	16	https://www.google.com/search?...	google - Google Search	1	0	13370788735144663	0

1 - 16 of 16

Go to: 1

Edit Database Cell

Mode: Text

1 https://www.elfi.com/emergency-student-loans-and-how-to-get-them/

Type of data currently in cell: Text / Numeric
65 character(s)

Is there other evidence on the phone that might indicate the role of the owner in Alex’s death?

I checked the media/0 directory and found photos of Alex and Sophia, including mumdad.png and Sophia.png.