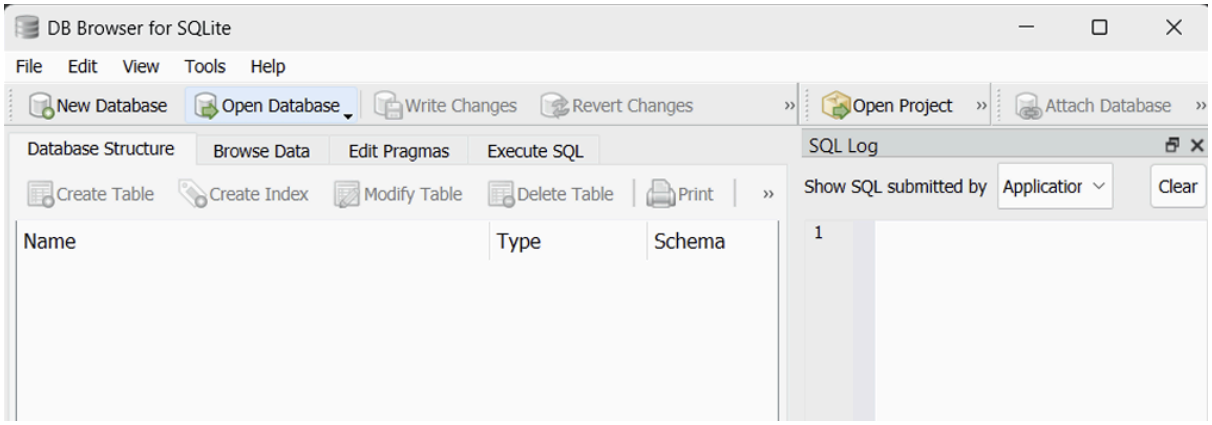
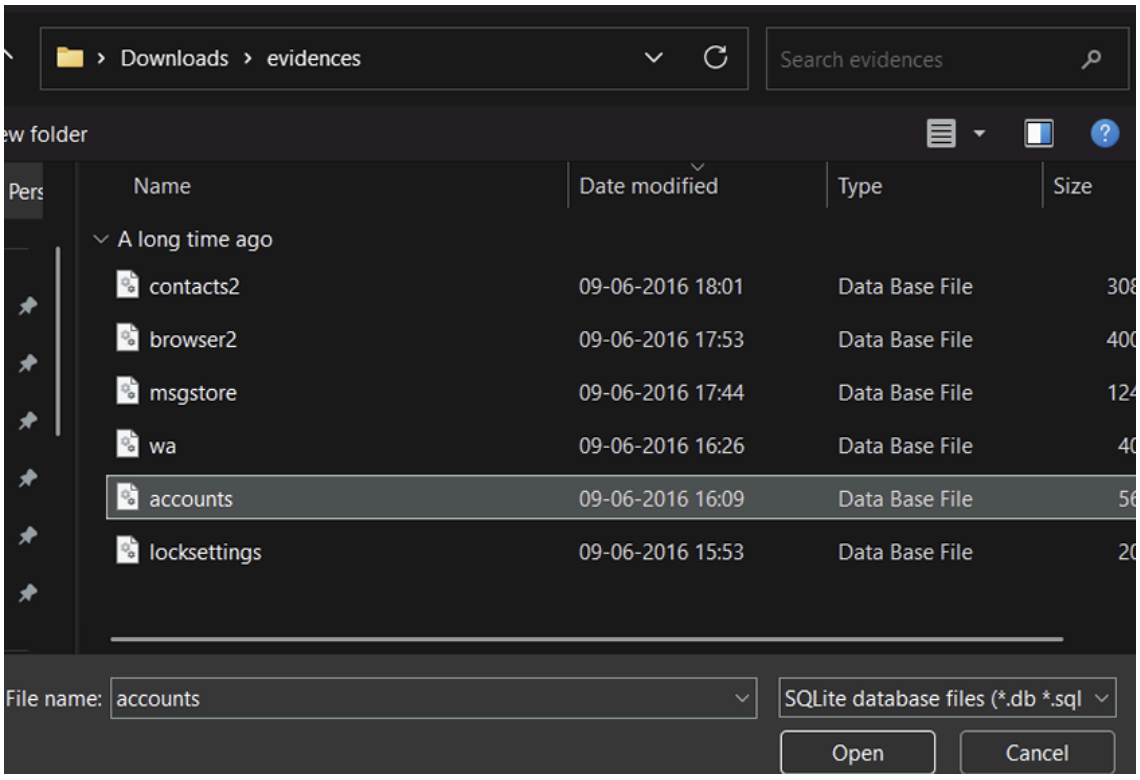
Praneesh R V
CB.SC.U4CYS23036

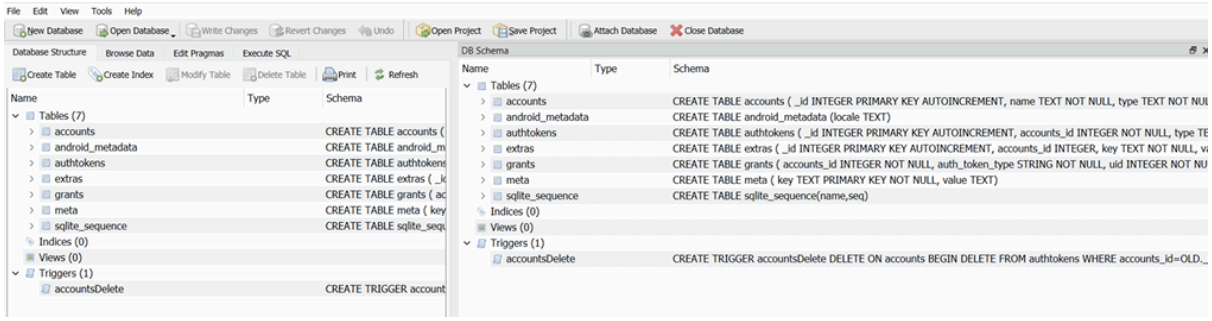
Cyber Forensics Lab - 7 - Database Forensics

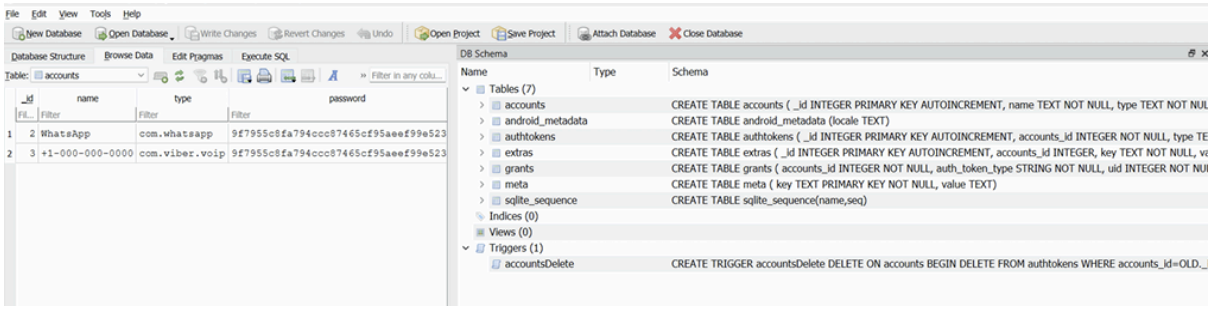
TASK 1: Exploring evidence in DB Browser for SQLite. Loading the accounts.db evidence file. Loading the accounts.db evidence file:

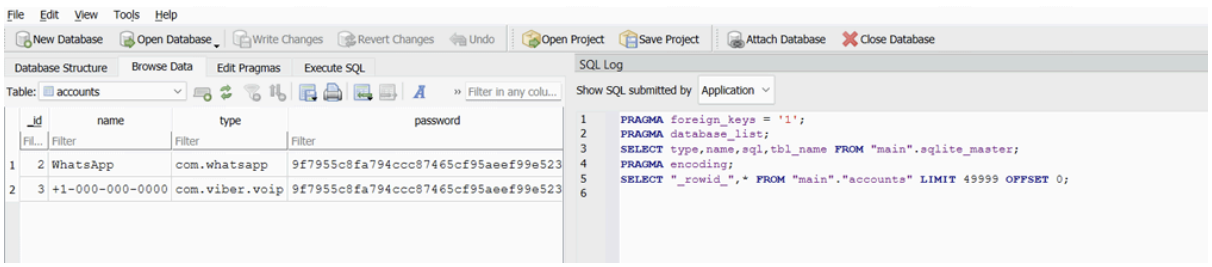




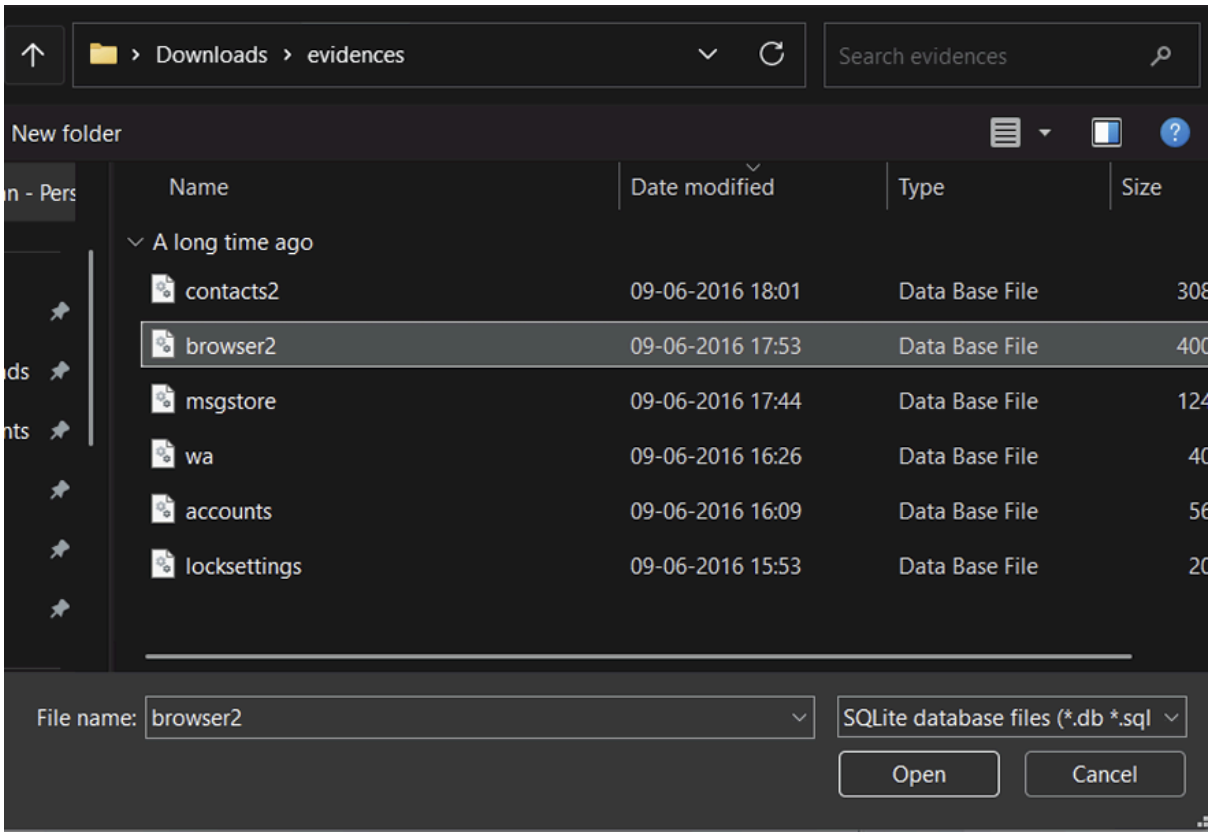
Loading the wa.db evidence file:

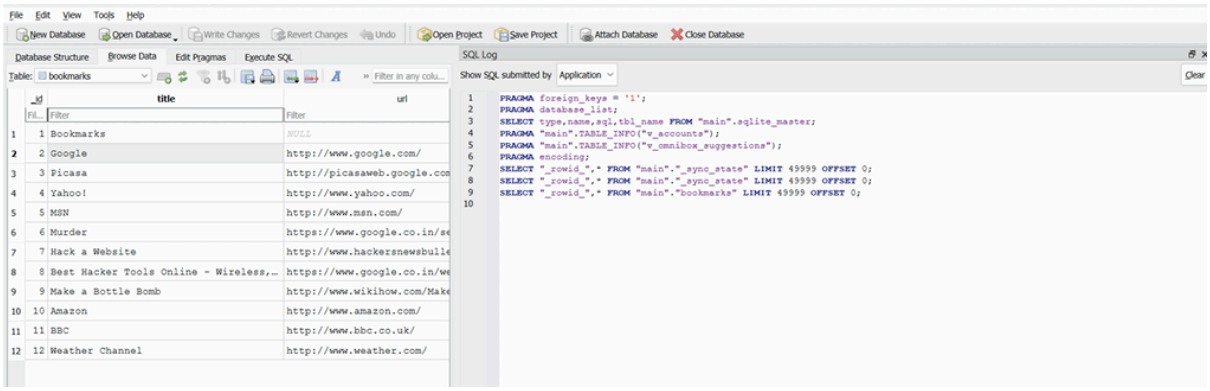




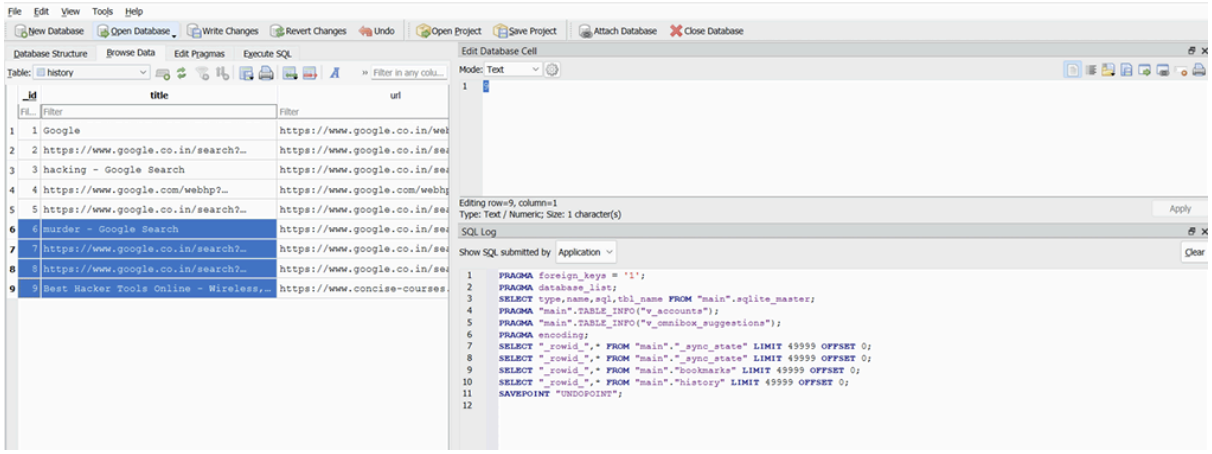


browser2.db evidence file:

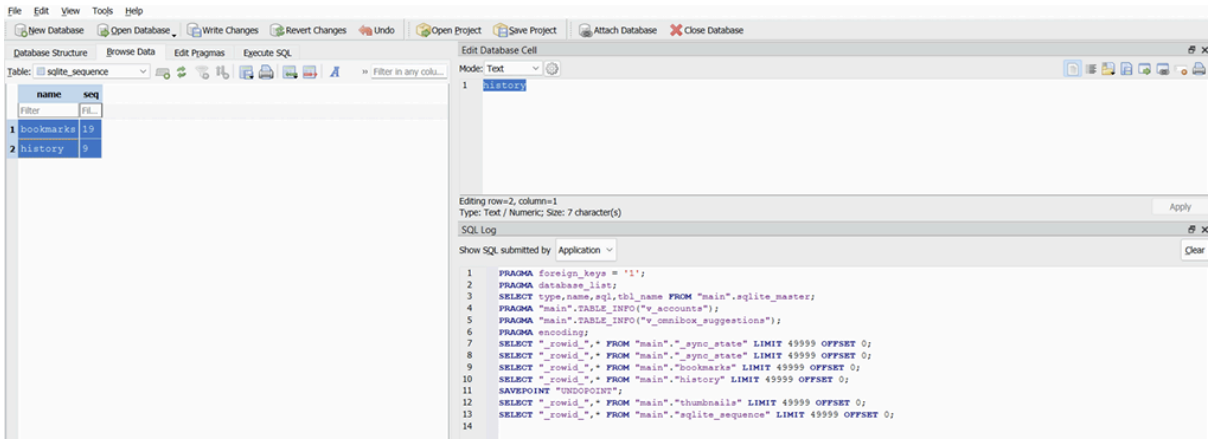




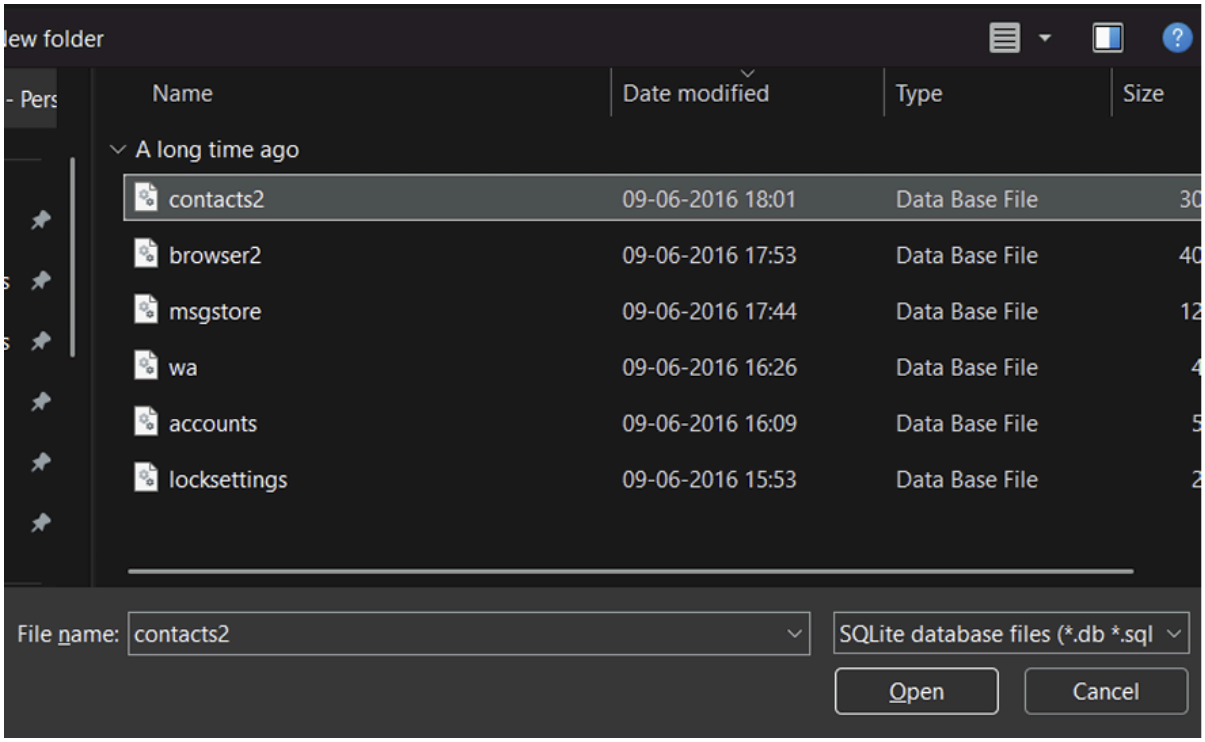
Bookmarks tab in browse data:

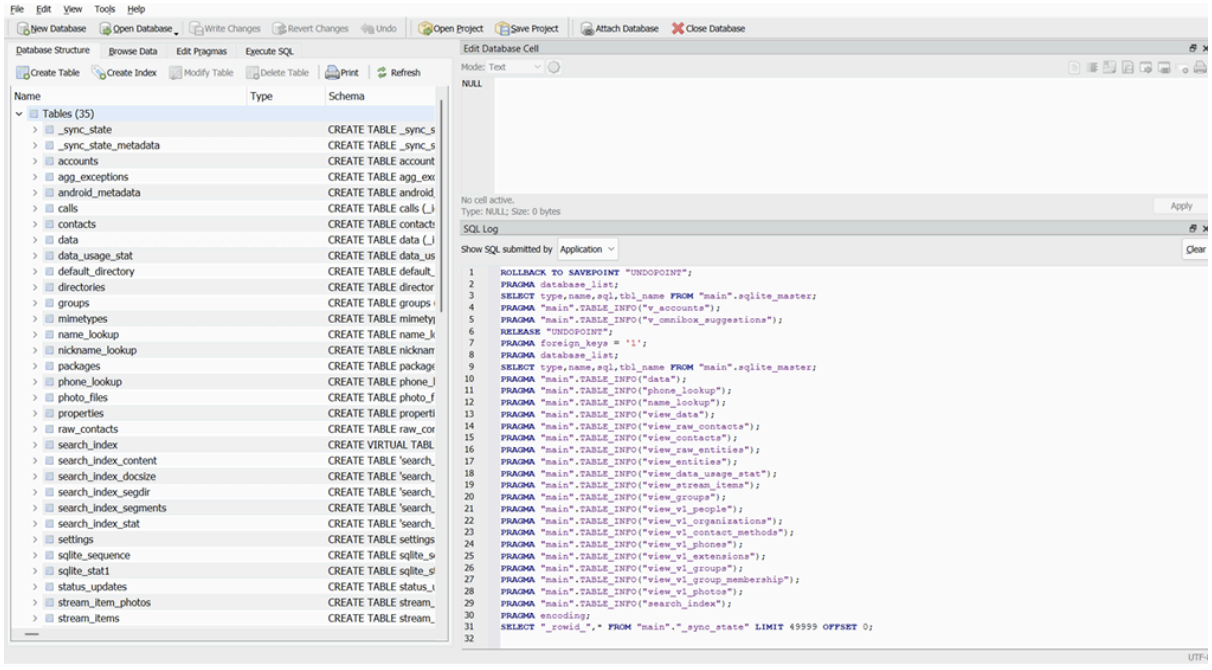


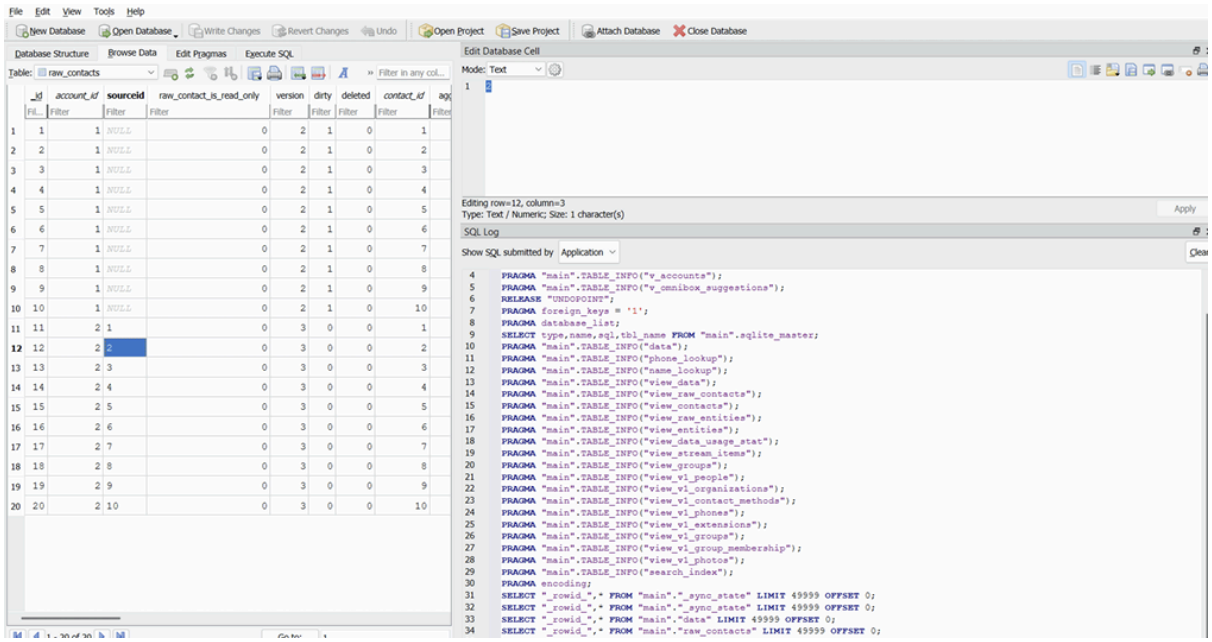
History tab in browse data:

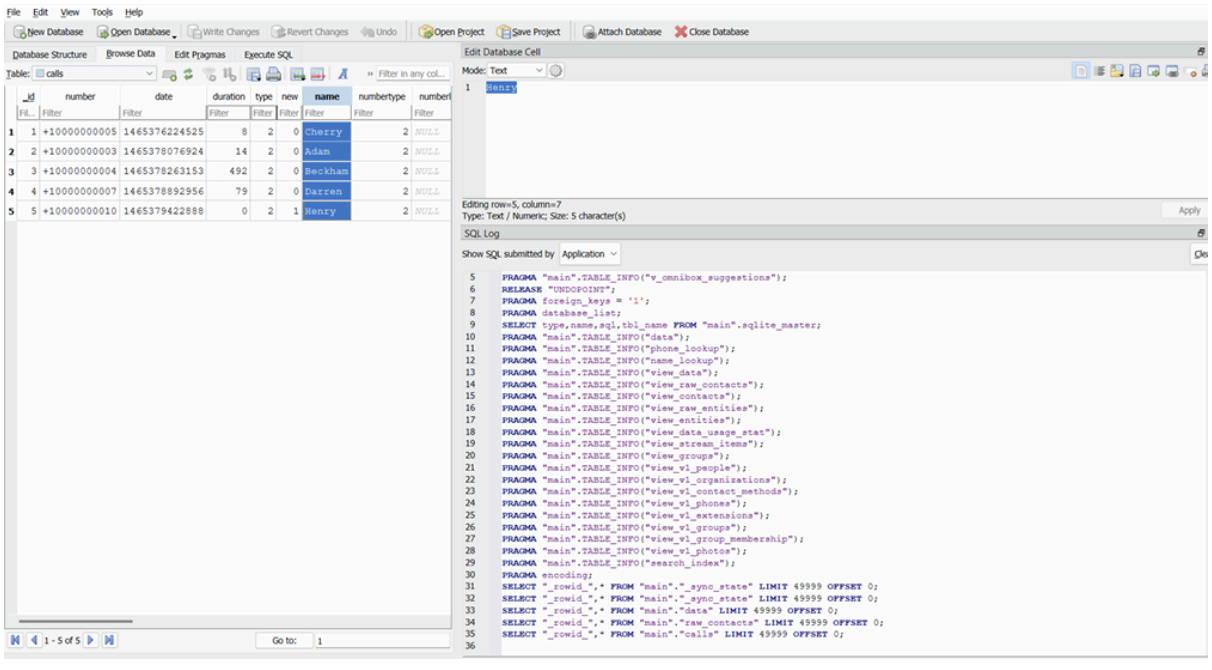


contacts2.db evidence file:

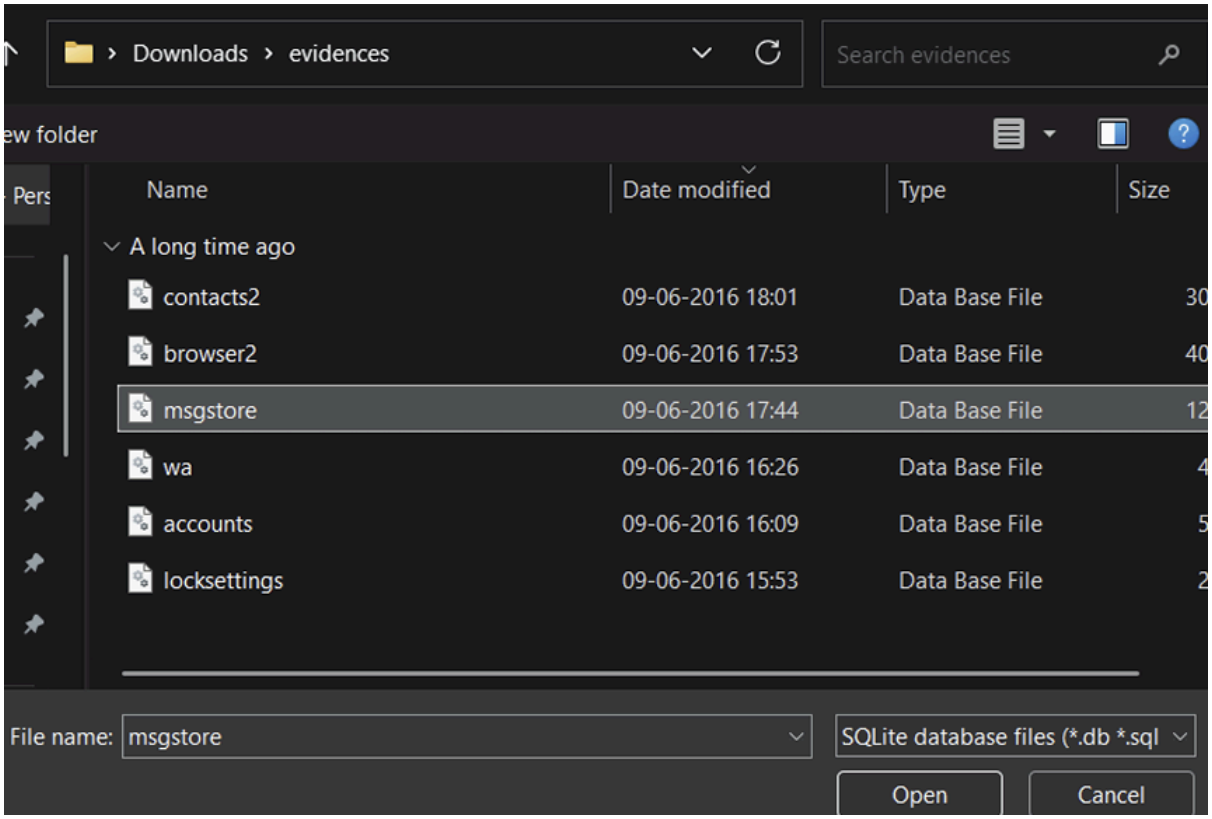

ew folder
- Pers
Name
Date modified
Type
Size
A long time ago
contacts2
09-06-2016 18:01
Data Base File
browser2
09-06-2016 17:53
Data Base File
msgstore
09-06-2016 17:44
Data Base File
wa
09-06-2016 16:26
Data Base File
accounts
09-06-2016 16:09
Data Base File
locksettings
09-06-2016 15:53
Data Base File
File name:
contacts2
SQLite database files (*.db *.sql
Open
Cancel

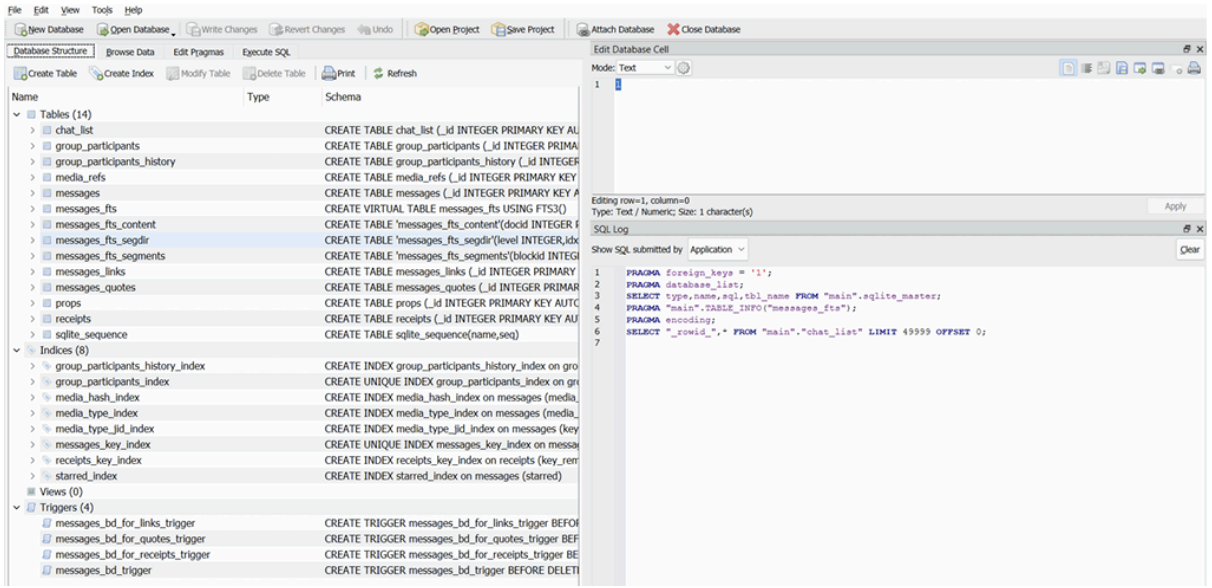

File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Undo
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Create Table
Create Index
Modify Table
Delete Table
Print
Refresh
Name
Type
Schema
Tables (35)
_sync_state
_sync_state_metadata
accounts
agg_exceptions
android_metadata
calls
contacts
data
data_usage_stat
default_directory
directories
groups
mimetypes
name_lookup
nickname_lookup
packages
phone_lookup
photo_files
properties
raw_contacts
search_index
search_index_content
search_index_docsize
search_index_segdir
search_index_segments
search_index_stat
settings
sqlite_sequence
sqlite_stat1
status_updates
stream_item_photos
stream_items
Edit Database Cell
Mode: Text
NULL
No cell active.
Type: NULL; Size: 0 bytes
Apply
SQL Log
Show SQL submitted by
Application
Clear
ROLLBACK TO SAVEPOINT "UNDOPOINT";
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_master;
PRAGMA "main".TABLE_INFO("v_accounts");
PRAGMA "main".TABLE_INFO("v_omnibox_suggestions");
RELEASE "UNDOPOINT";
PRAGMA foreign_keys = '1';
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_master;
PRAGMA "main".TABLE_INFO("data");
PRAGMA "main".TABLE_INFO("phone_lookup");
PRAGMA "main".TABLE_INFO("name_lookup");
PRAGMA "main".TABLE_INFO("view_data");
PRAGMA "main".TABLE_INFO("view_raw_contacts");
PRAGMA "main".TABLE_INFO("view_contacts");
PRAGMA "main".TABLE_INFO("view_raw_entities");
PRAGMA "main".TABLE_INFO("view_entities");
PRAGMA "main".TABLE_INFO("view_data_usage_stat");
PRAGMA "main".TABLE_INFO("view_stream_items");
PRAGMA "main".TABLE_INFO("view_groups");
PRAGMA "main".TABLE_INFO("view_v1_people");
PRAGMA "main".TABLE_INFO("view_v1_organizations");
PRAGMA "main".TABLE_INFO("view_v1_contact_methods");
PRAGMA "main".TABLE_INFO("view_v1_phones");
PRAGMA "main".TABLE_INFO("view_v1_extensions");
PRAGMA "main".TABLE_INFO("view_v1_groups");
PRAGMA "main".TABLE_INFO("view_v1_group_membership");
PRAGMA "main".TABLE_INFO("view_v1_photos");
PRAGMA "main".TABLE_INFO("search_index");
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT 49999 OFFSET 0;

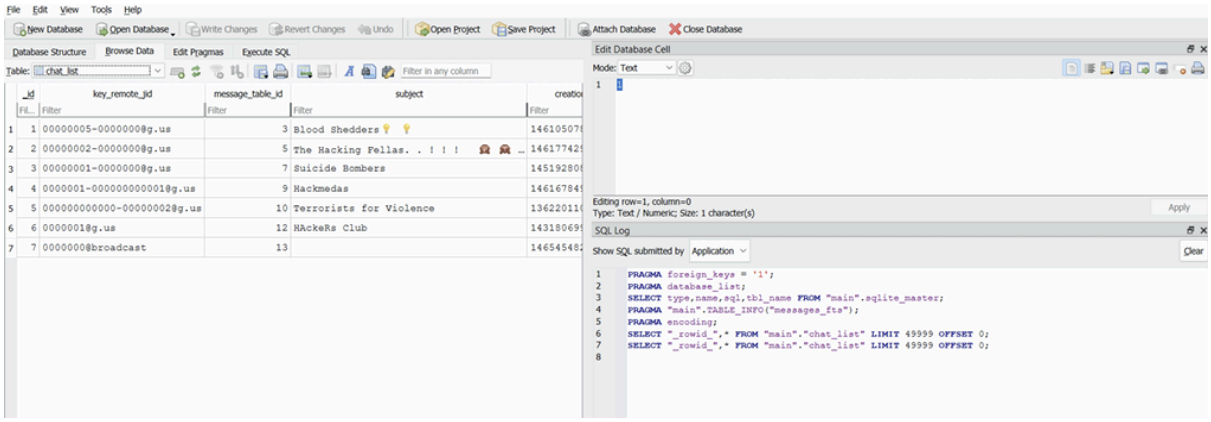

File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Undo
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: raw_contacts
Filter in any col...
_id account_id sourceid raw_contact_is_read_only version dirty deleted contact_id
1 1 1 NULL 0 2 1 0 1
2 2 1 NULL 0 2 1 0 2
3 3 1 NULL 0 2 1 0 3
4 4 1 NULL 0 2 1 0 4
5 5 1 NULL 0 2 1 0 5
6 6 1 NULL 0 2 1 0 6
7 7 1 NULL 0 2 1 0 7
8 8 1 NULL 0 2 1 0 8
9 9 1 NULL 0 2 1 0 9
10 10 1 NULL 0 2 1 0 10
11 11 2 1 0 3 0 0 1
12 12 2 2 0 3 0 0 2
13 13 2 3 0 3 0 0 3
14 14 2 4 0 3 0 0 4
15 15 2 5 0 3 0 0 5
16 16 2 6 0 3 0 0 6
17 17 2 7 0 3 0 0 7
18 18 2 8 0 3 0 0 8
19 19 2 9 0 3 0 0 9
20 20 2 10 0 3 0 0 10
1 - 20 of 20
Go to: 1
Edit Database Cell
Mode: Text
2
Editing row=12, column=3
Type: Text / Numeric; Size: 1 character(s)
Apply
SQL Log
Show SQL submitted by Application
Clear
PRAGMA "main".TABLE_INFO("v_accounts");
PRAGMA "main".TABLE_INFO("v_omnibox_suggestions");
RELEASE "UNDOPOINT";
PRAGMA foreign_keys = '1';
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_master;
PRAGMA "main".TABLE_INFO("data");
PRAGMA "main".TABLE_INFO("phone_lookup");
PRAGMA "main".TABLE_INFO("name_lookup");
PRAGMA "main".TABLE_INFO("view_data");
PRAGMA "main".TABLE_INFO("view_raw_contacts");
PRAGMA "main".TABLE_INFO("view_contacts");
PRAGMA "main".TABLE_INFO("view_raw_entities");
PRAGMA "main".TABLE_INFO("view_entities");
PRAGMA "main".TABLE_INFO("view_data_usage_stat");
PRAGMA "main".TABLE_INFO("view_stream_items");
PRAGMA "main".TABLE_INFO("view_groups");
PRAGMA "main".TABLE_INFO("view_v1_people");
PRAGMA "main".TABLE_INFO("view_v1_organizations");
PRAGMA "main".TABLE_INFO("view_v1_contact_methods");
PRAGMA "main".TABLE_INFO("view_v1_phones");
PRAGMA "main".TABLE_INFO("view_v1_extensions");
PRAGMA "main".TABLE_INFO("view_v1_groups");
PRAGMA "main".TABLE_INFO("view_v1_group_membership");
PRAGMA "main".TABLE_INFO("view_v1_photos");
PRAGMA "main".TABLE_INFO("search_index");
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT 49999 OFFSET 0;
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT 49999 OFFSET 0;
SELECT "_rowid_",* FROM "main"."data" LIMIT 49999 OFFSET 0;
SELECT "_rowid_",* FROM "main"."raw_contacts" LIMIT 49999 OFFSET 0;

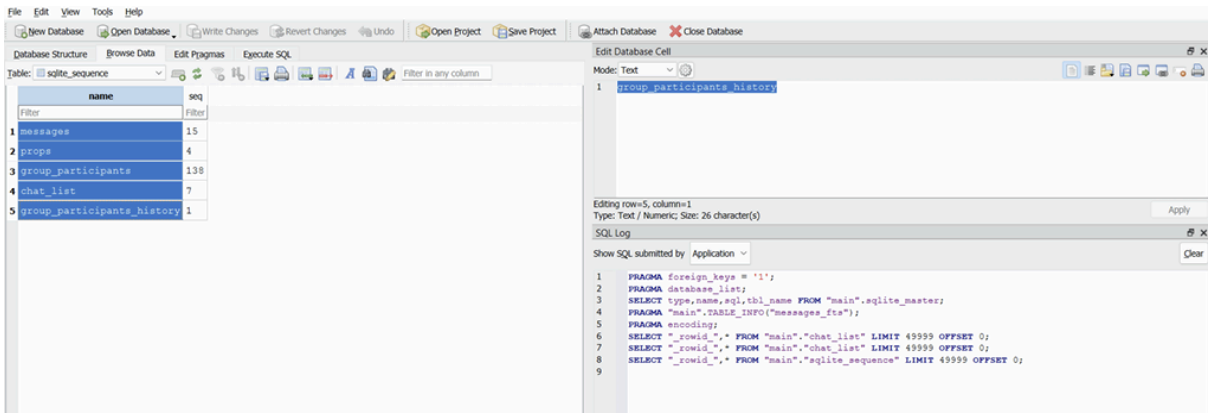

File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Undo
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: calls
Filter in any col...
_id number date duration type new name numbertype
1 1 +10000000005 1465376224525 8 2 0 Cherry 2
2 2 +10000000003 1465378076924 14 2 0 Adam 2
3 3 +10000000004 1465378263153 492 2 0 Beckham 2
4 4 +10000000007 1465378892956 79 2 0 Darren 2
5 5 +10000000010 1465379422888 0 2 1 Henry 2
1 - 5 of 5
Go to: 1
Edit Database Cell
Mode: Text
Henry
Editing row=5, column=7
Type: Text / Numeric; Size: 5 character(s)
Apply
SQL Log
Show SQL submitted by Application
PRAGMA "main".TABLE_INFO("v_omnibox_suggestions");
RELEASE "UNDOPOINT";
PRAGMA foreign_keys = '1';
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_master;
PRAGMA "main".TABLE_INFO("data");
PRAGMA "main".TABLE_INFO("phone_lookup");
PRAGMA "main".TABLE_INFO("name_lookup");
PRAGMA "main".TABLE_INFO("view_data");
PRAGMA "main".TABLE_INFO("view_raw_contacts");
PRAGMA "main".TABLE_INFO("view_contacts");
PRAGMA "main".TABLE_INFO("view_raw_entities");
PRAGMA "main".TABLE_INFO("view_entities");
PRAGMA "main".TABLE_INFO("view_data_usage_stat");
PRAGMA "main".TABLE_INFO("view_stream_items");
PRAGMA "main".TABLE_INFO("view_groups");
PRAGMA "main".TABLE_INFO("view_v1_people");
PRAGMA "main".TABLE_INFO("view_v1_organizations");
PRAGMA "main".TABLE_INFO("view_v1_contact_methods");
PRAGMA "main".TABLE_INFO("view_v1_phones");
PRAGMA "main".TABLE_INFO("view_v1_extensions");
PRAGMA "main".TABLE_INFO("view_v1_groups");
PRAGMA "main".TABLE_INFO("view_v1_group_membership");
PRAGMA "main".TABLE_INFO("view_v1_photos");
PRAGMA "main".TABLE_INFO("search_index");
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT 49999 OFFSET 0;
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT 49999 OFFSET 0;
SELECT "_rowid_",* FROM "main"."data" LIMIT 49999 OFFSET 0;
SELECT "_rowid_",* FROM "main"."raw_contacts" LIMIT 49999 OFFSET 0;
SELECT "_rowid_",* FROM "main"."calls" LIMIT 49999 OFFSET 0;

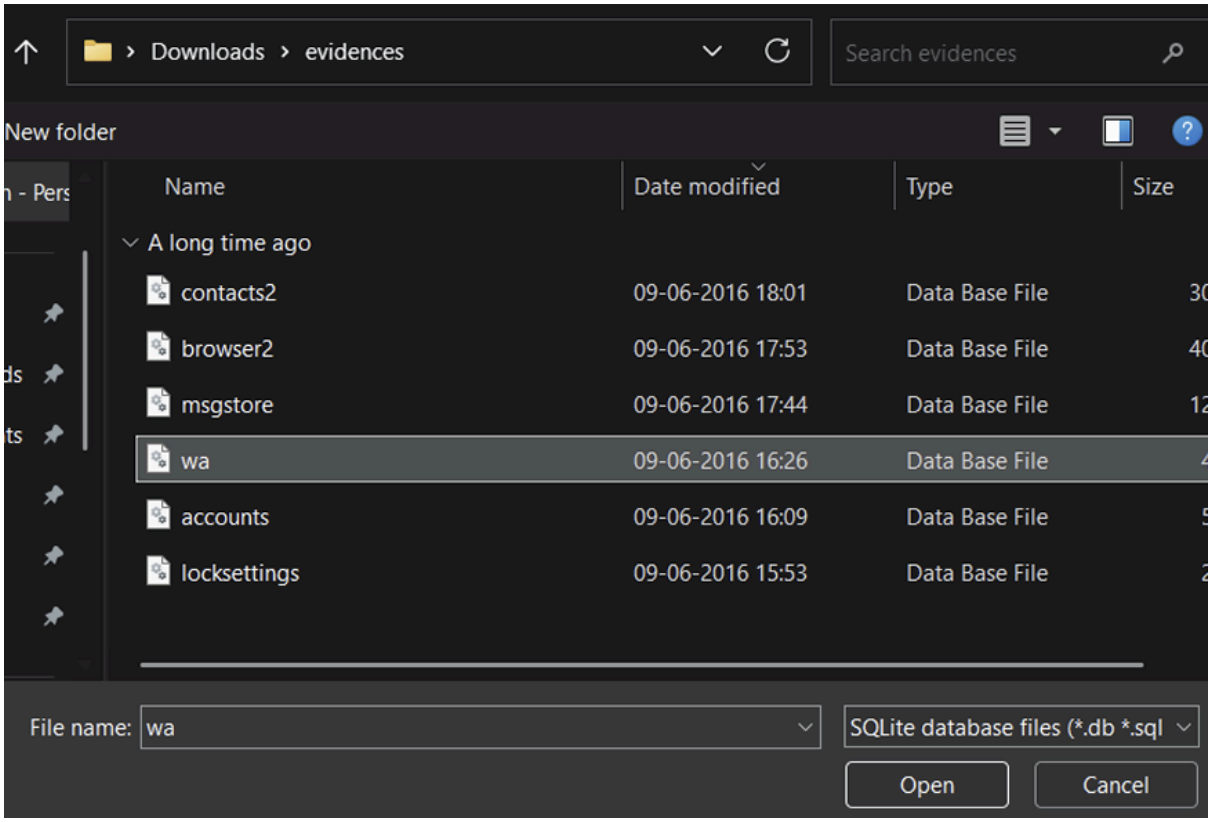
msgstore.db evidence file:

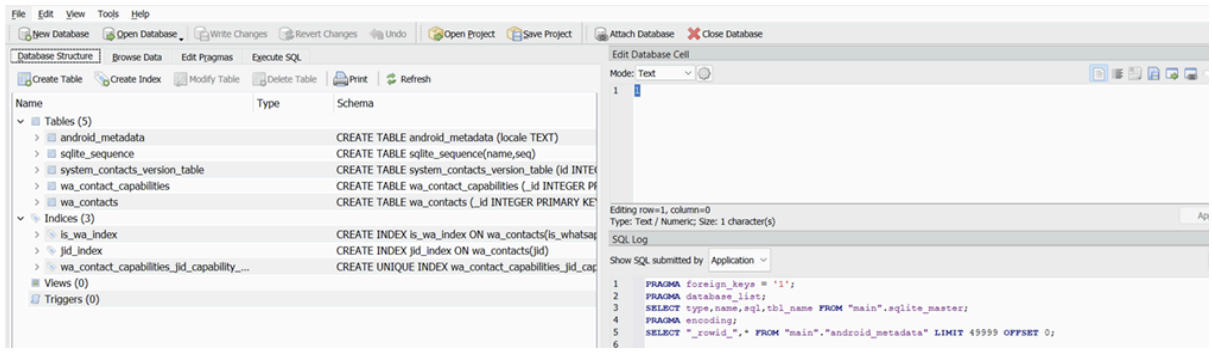


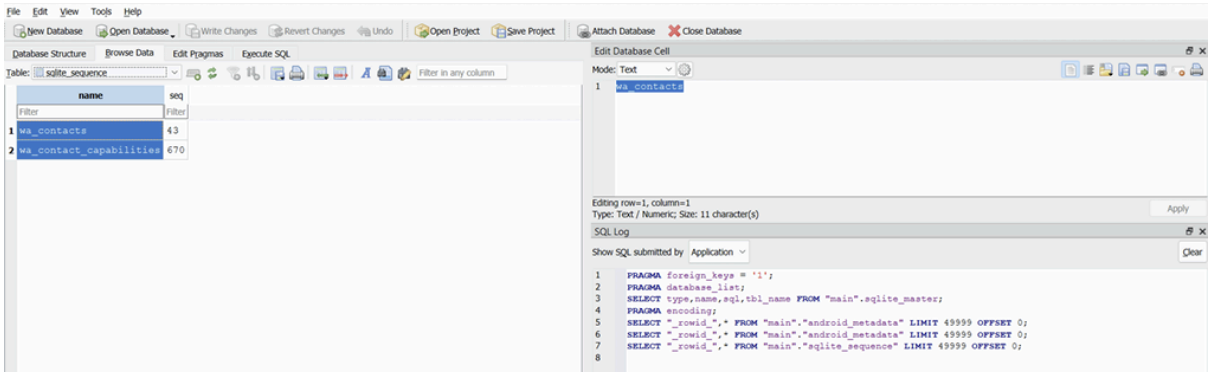



File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Undo
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: chat_list
Filter in any column
_id
key_remote_jid
message_table_id
subject
1 1 00000005-0000000@g.us 3 Blood Shedders
2 2 00000002-0000000@g.us 5 The Hacking Fellas. . ! ! !
3 3 00000001-0000000@g.us 7 Suicide Bombers
4 4 0000001-000000000001@g.us 9 Hackmedas
5 5 000000000000-00000002@g.us 10 Terrorists for Violence
6 6 0000001@g.us 12 HAckeRs Club
7 7 0000000@broadcast 13
Edit Database Cell
Mode: Text
Editing row=1, column=0
Type: Text / Numeric; Size: 1 character(s)
Apply
SQL Log
Show SQL submitted by Application
Clear
PRAGMA foreign_keys = '1';
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_master;
PRAGMA "main".TABLE_INFO("messages_fts");
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."chat_list" LIMIT 49999 OFFSET 0;
SELECT "_rowid_",* FROM "main"."chat_list" LIMIT 49999 OFFSET 0;

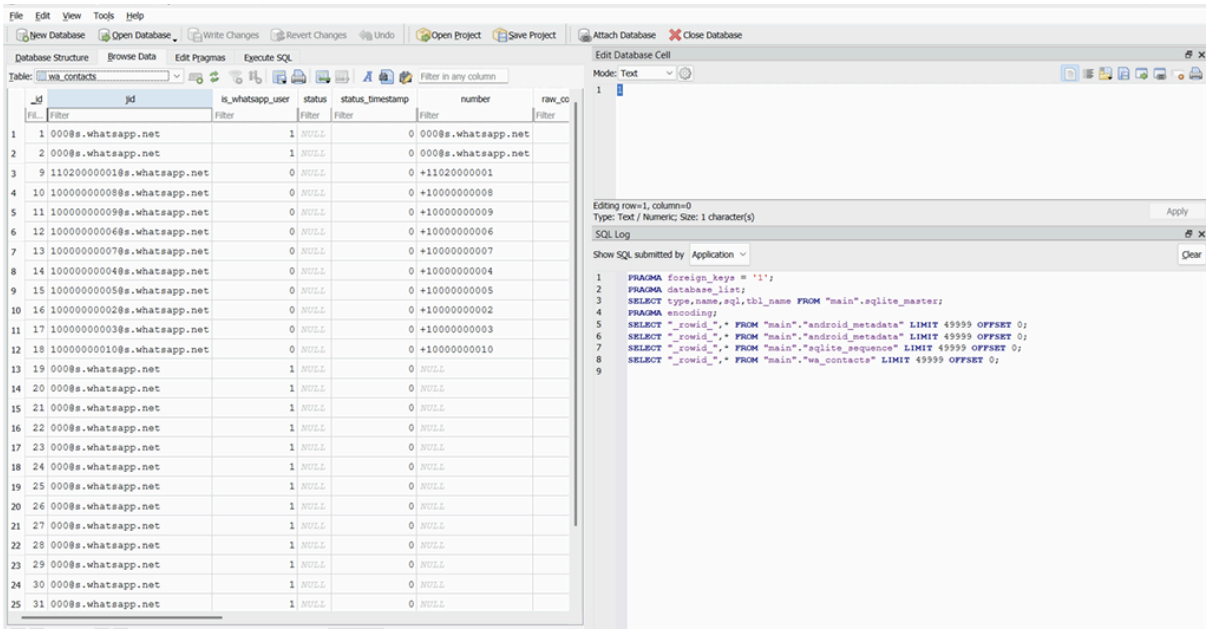

File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Undo
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: sqlite_sequence
Filter in any column
name
seq
1 messages 15
2 props 4
3 group_participants 138
4 chat_list 7
5 group_participants_history 1
Edit Database Cell
Mode: Text
group_participants_history
Editing row=5, column=1
Type: Text / Numeric; Size: 26 character(s)
Apply
SQL Log
Show SQL submitted by Application
Clear
PRAGMA foreign_keys = '1';
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_master;
PRAGMA "main".TABLE_INFO("messages_fts");
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."chat_list" LIMIT 49999 OFFSET 0;
SELECT "_rowid_",* FROM "main"."chat_list" LIMIT 49999 OFFSET 0;
SELECT "_rowid_",* FROM "main"."sqlite_sequence" LIMIT 49999 OFFSET 0;

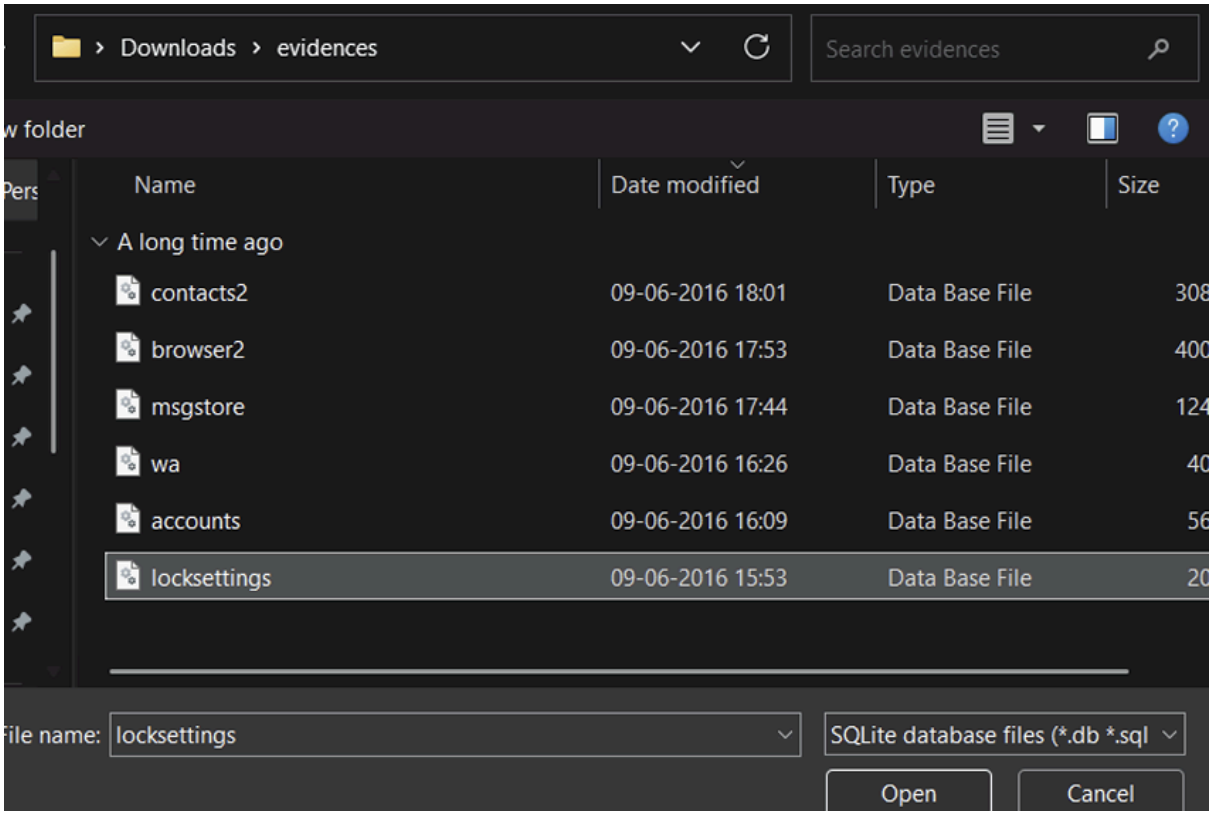

Downloads › evidences
Search evidences
New folder
Name
Date modified
Type
Size
A long time ago
contacts2 09-06-2016 18:01 Data Base File
browser2 09-06-2016 17:53 Data Base File
msgstore 09-06-2016 17:44 Data Base File
wa 09-06-2016 16:26 Data Base File
accounts 09-06-2016 16:09 Data Base File
locksettings 09-06-2016 15:53 Data Base File
File name: wa
SQLite database files (*.db *.sql
Open
Cancel

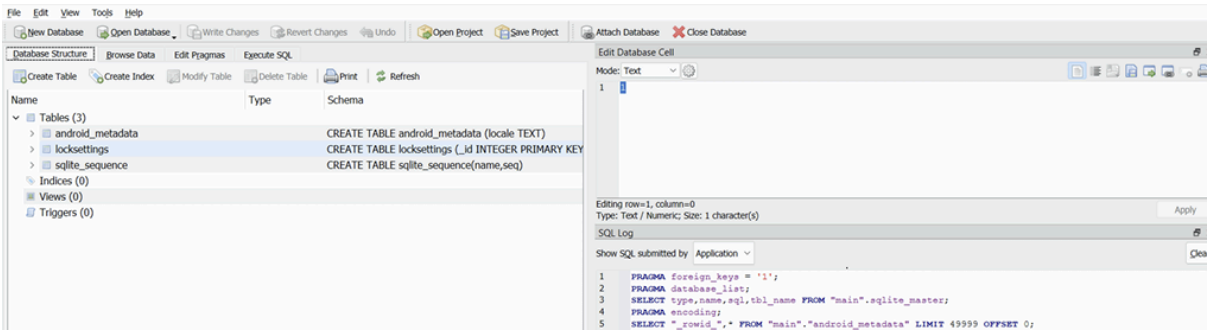

File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Undo
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Create Table
Create Index
Modify Table
Delete Table
Print
Refresh
Name
Type
Schema
Tables (5)
android_metadata
sqlite_sequence
system_contacts_version_table
wa_contact_capabilities
wa_contacts
Indices (3)
is_wa_index
jid_index
wa_contact_capabilities_jid_capability_...
Views (0)
Triggers (0)
Edit Database Cell
Mode: Text
Editing row=1, column=0
Type: Text / Numeric; Size: 1 character(s)
SQL Log
Show SQL submitted by
Application
PRAGMA foreign_keys = '1';
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_master;
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."android_metadata" LIMIT 49999 OFFSET 0;

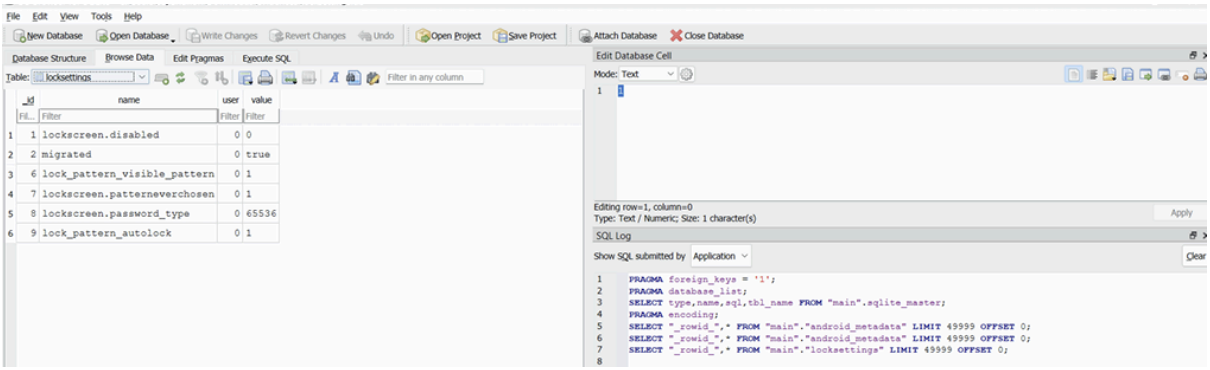

File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Undo
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: sqlite_sequence
Filter in any column
name
seq
wa_contacts 43
wa_contact_capabilities 670
Edit Database Cell
Mode: Text
wa_contacts
Editing row=1, column=1
Type: Text / Numeric; Size: 11 character(s)
Apply
SQL Log
Show SQL submitted by
Application
Clear
PRAGMA foreign_keys = '1';
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_master;
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."android_metadata" LIMIT 49999 OFFSET 0;
SELECT "_rowid_",* FROM "main"."android_metadata" LIMIT 49999 OFFSET 0;
SELECT "_rowid_",* FROM "main"."sqlite_sequence" LIMIT 49999 OFFSET 0;

locksettings.db evidence file:









Task 2: Performing Forensics Investigation on a MySQL Server Database

Creating database:

```
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.4.7 MySQL Community Server - GPL

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database wordpress
    -> ;
Query OK, 1 row affected (0.01 sec)
```

Copying contents of wordpress_evidence.sql:

```
C:\Users>cd ..

C:\>cd wamp64

C:\wamp64>cd bin

C:\wamp64\bin>cd mysql

C:\wamp64\bin\mysql>cd mysql8.4.7

C:\wamp64\bin\mysql\mysql8.4.7>cd bin

C:\wamp64\bin\mysql\mysql8.4.7\bin>mysql -u root -p wordpress < wordpress_evidence.sql
Enter password:

C:\wamp64\bin\mysql\mysql8.4.7\bin>
```

Content in wordpress:

```
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
11 rows in set (0.02 sec)
```

Wp_users content;

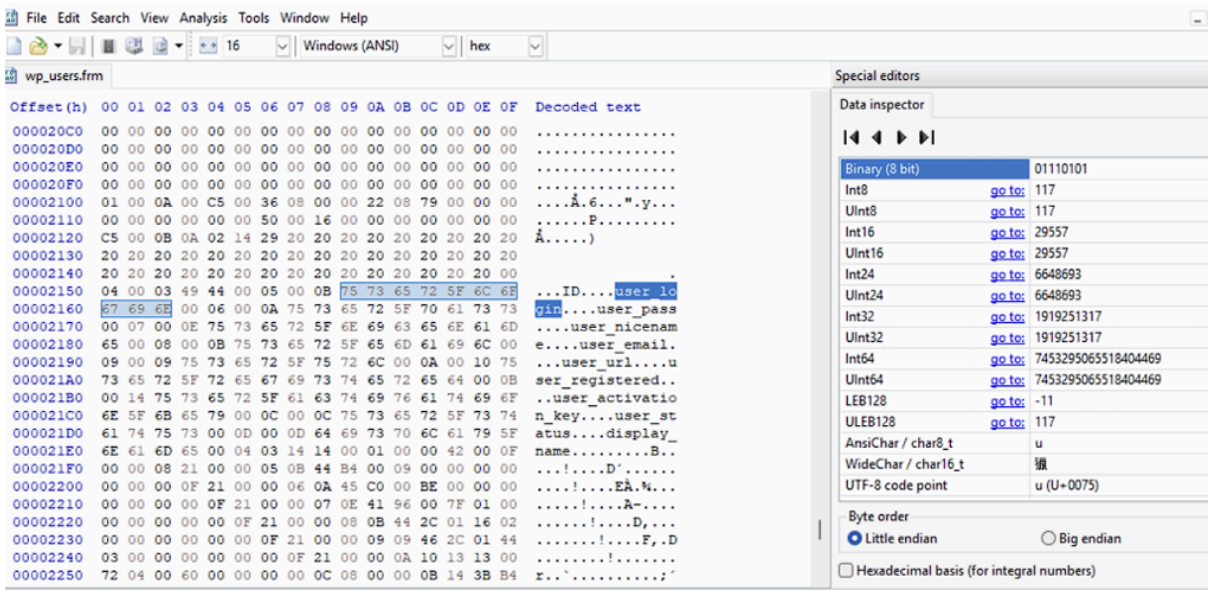
```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+------------------+-----------------------+---------------------+---------------------+-------------+--------------+
| ID | user_login | user_pass                          | user_nicename | user_email       | user_url              | user_registered     | user_activation_key | user_status | display_name |
+----+------------+------------------------------------+---------------+------------------+-----------------------+---------------------+---------------------+-------------+--------------+
|  1 | admin      | $P$BSScenYvMOuAldinorzLM7QdOkZAAk/ | admin         | admin@abc.com    | http://www.admin.com  | 0000-00-00 00:00:00 |                     |           0 | Admin        |
|  2 | james      | ceb6c970658f31504a901b89dcd3e461   | james         | jamesfaulkner@gmail.com | http://www.jameswebsite.com | 0000-00-00 00:00:00 |                     |           0 | jamesfaulkner |
|125 | bad_guy    | $P$B.OWWYbJlAsOyP2EYS.b6.d0xnkBKe/ | anonymous_hacker | badguy@xyz.com |                       | 0000-00-00 00:00:00 |                     |           0 |              |
+----+------------+------------------------------------+---------------+------------------+-----------------------+---------------------+---------------------+-------------+--------------+
3 rows in set (0.00 sec)

mysql>
```

Saved evidence in evidence.txt:

```
mysql> select * from wp_posts
    -> where post_author = '125'
    -> into outfile 'c:/wamp64/tmp/evidence.txt';
Query OK, 3 rows affected (0.01 sec)
```

Hex editor:



Got details from mysqlbin.000034

Username - bad_guy
Password – pass123
Nice name – anonymous_hacker
Email ID – badguy@xyz.com

Additional info