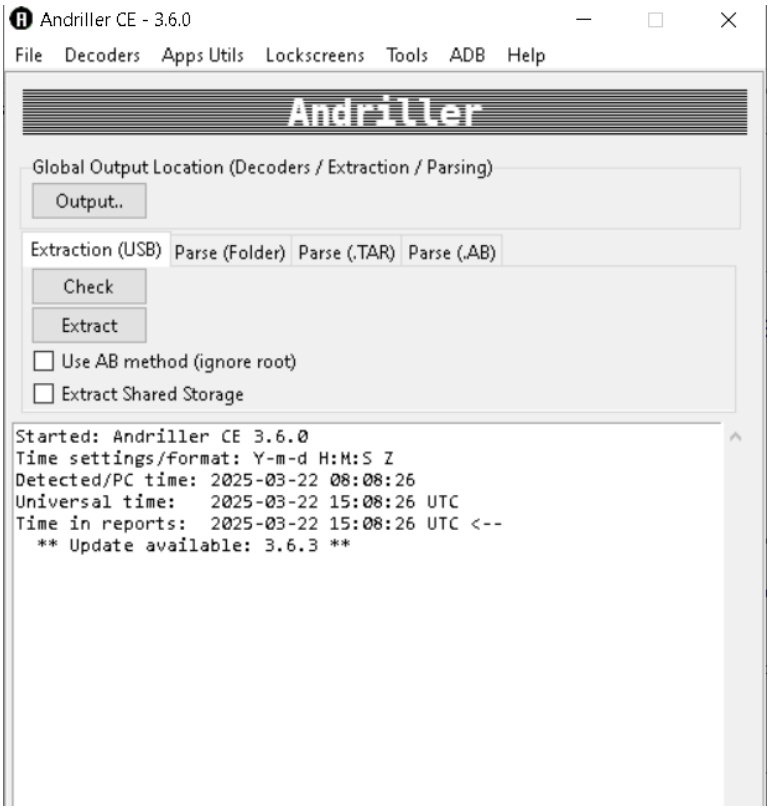
Digital Forensics Lab 8

Database Forensics

1) Extracting the Database of an Android Device Using Andriller

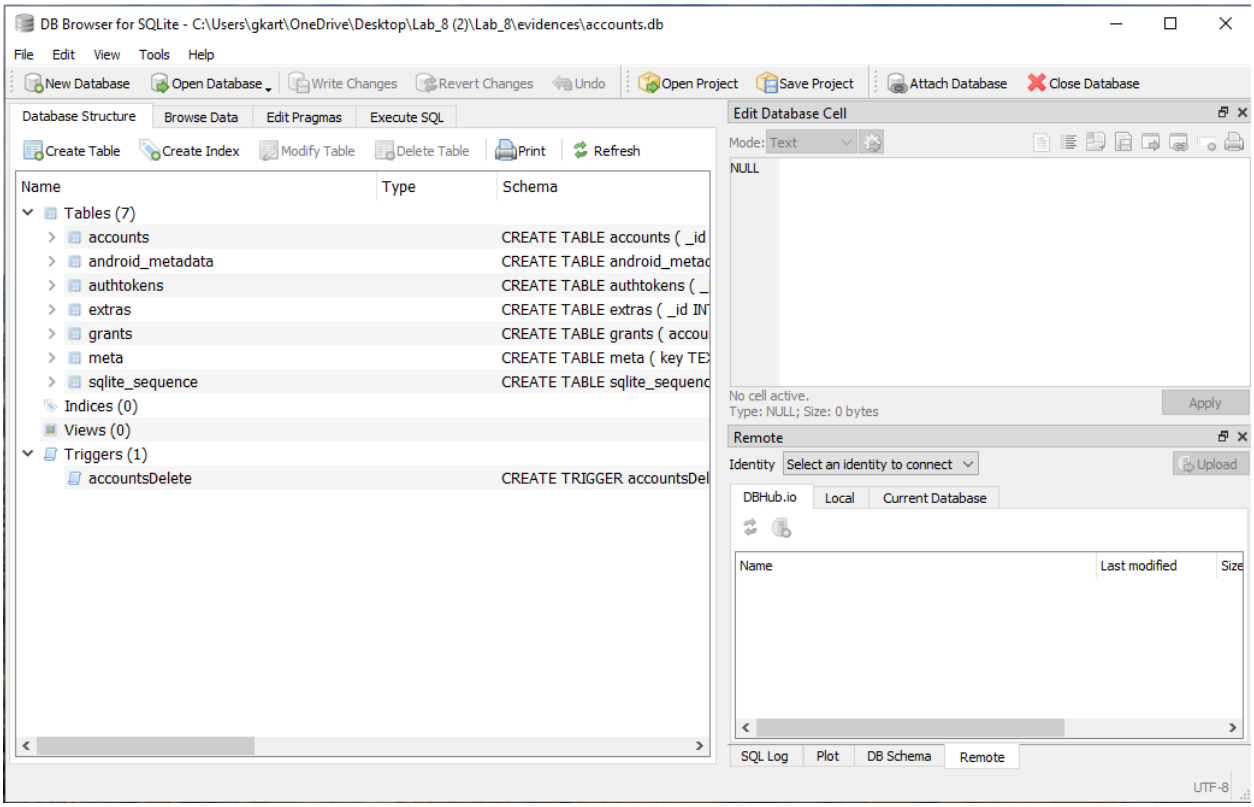


Launch Andriller to perform the analysis. However, we cannot use an emulator at the moment because Windows is running inside a VirtualBox environment, which prevents the emulator from functioning properly.

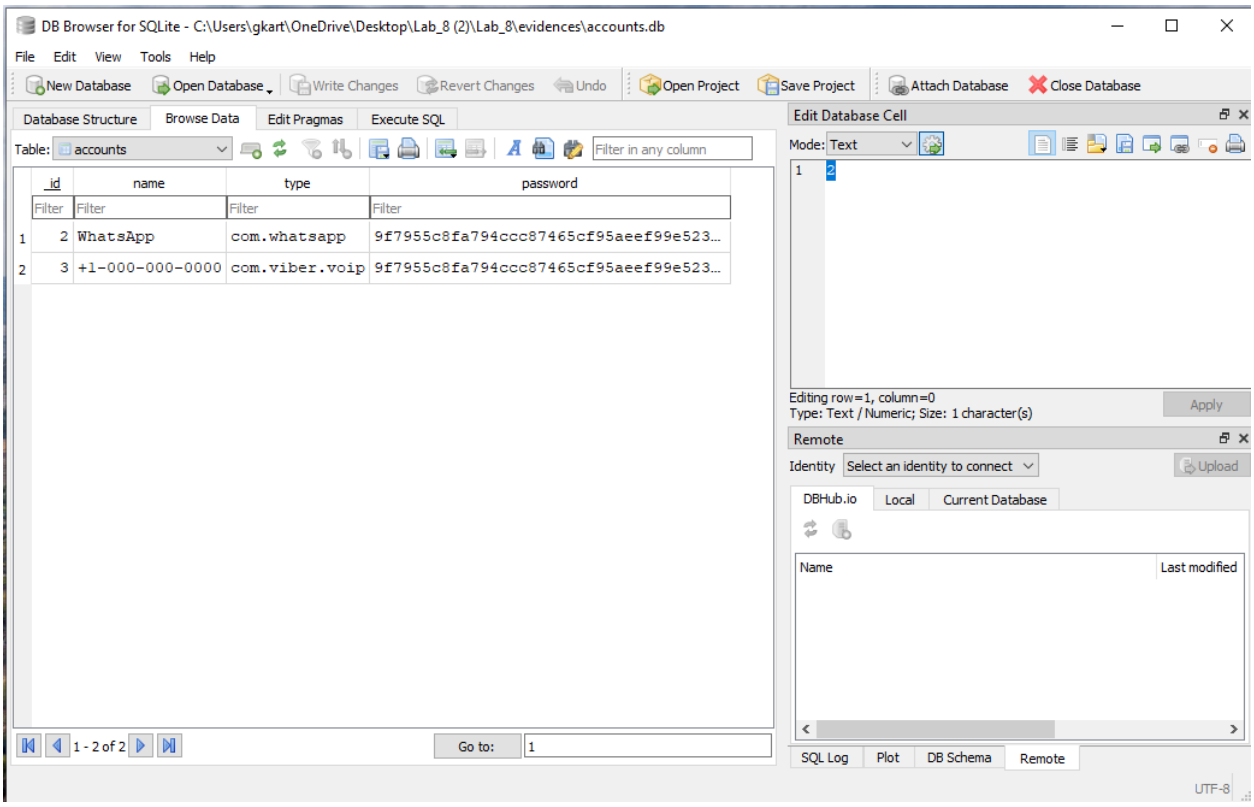
Lab 2: Examining an SQLite Database Using DB Browser for SQLite

Here are the steps in a concise format for Word:

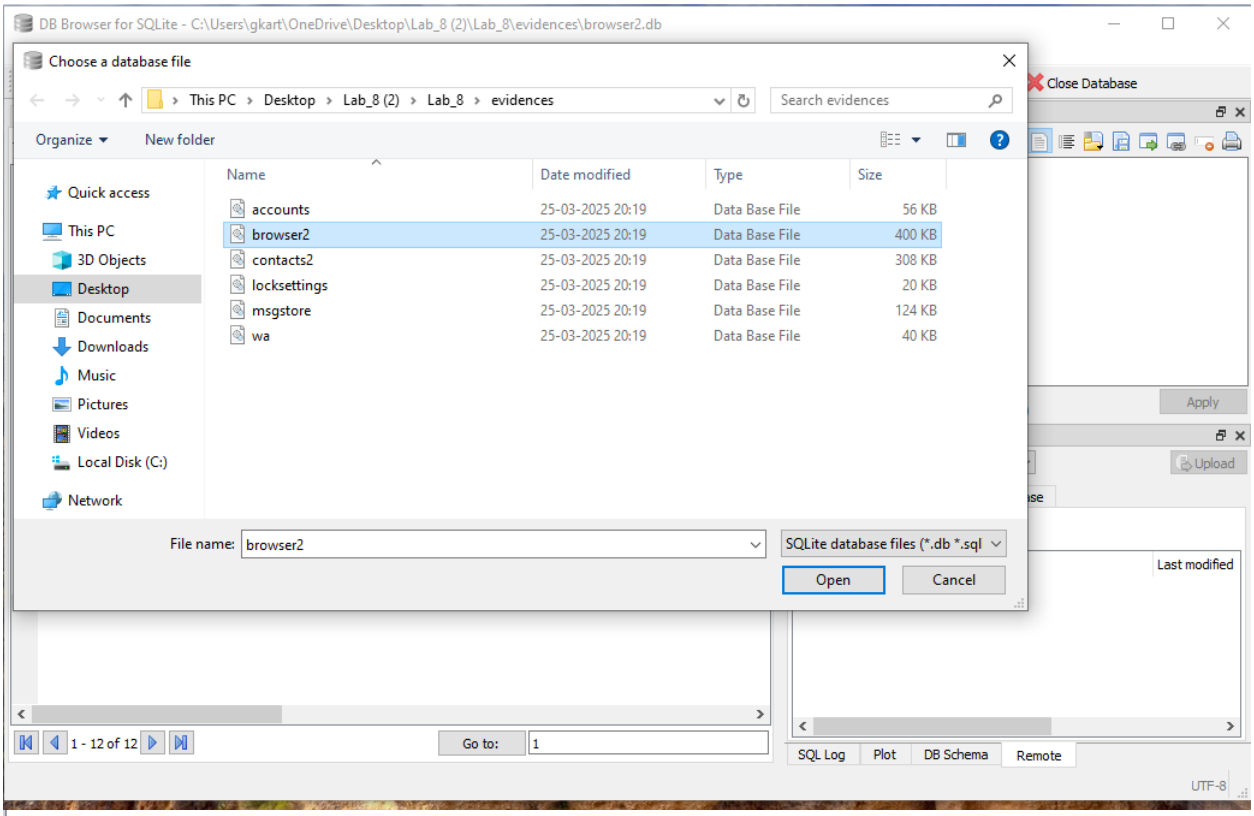
1. Open **DB Browser for SQLite**.
2. Click **Database** in the **toolbar**.
3. View the **accounts database structure** under the **Database Structure** tab.

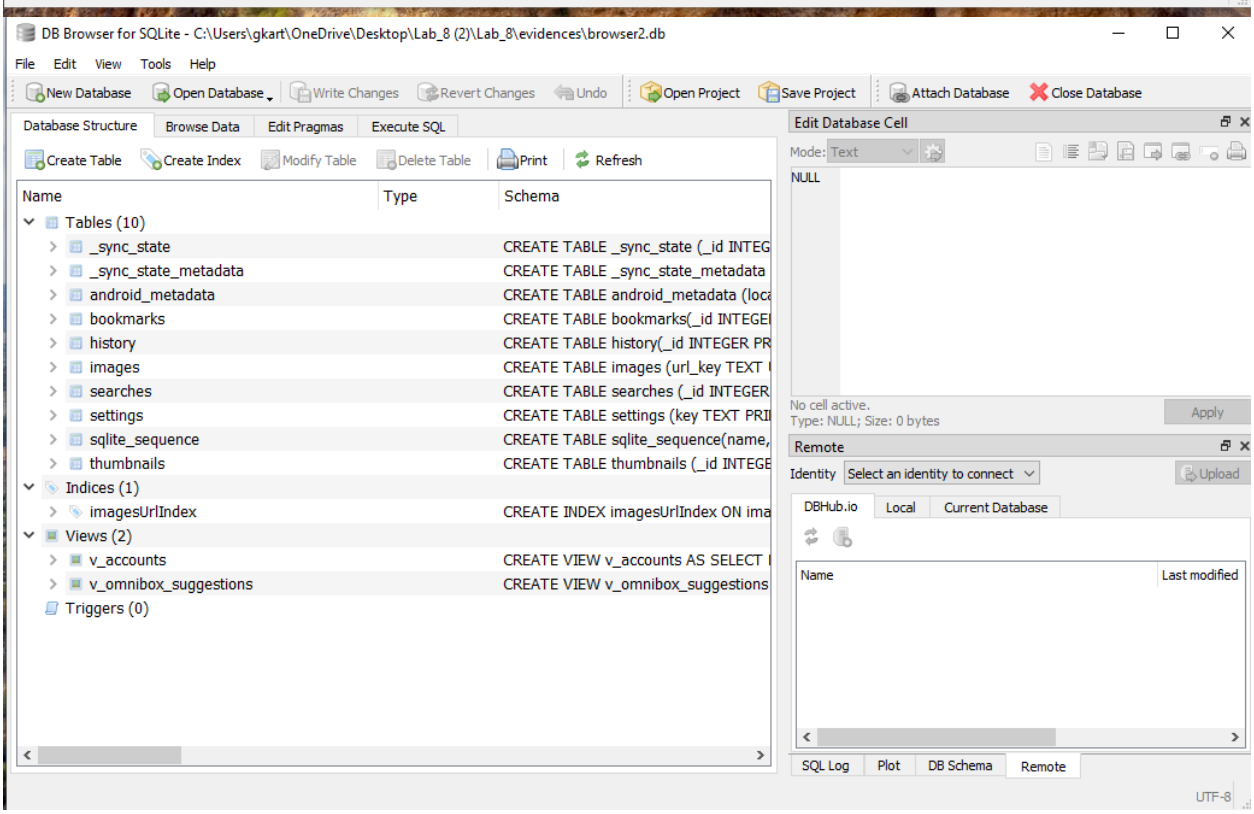


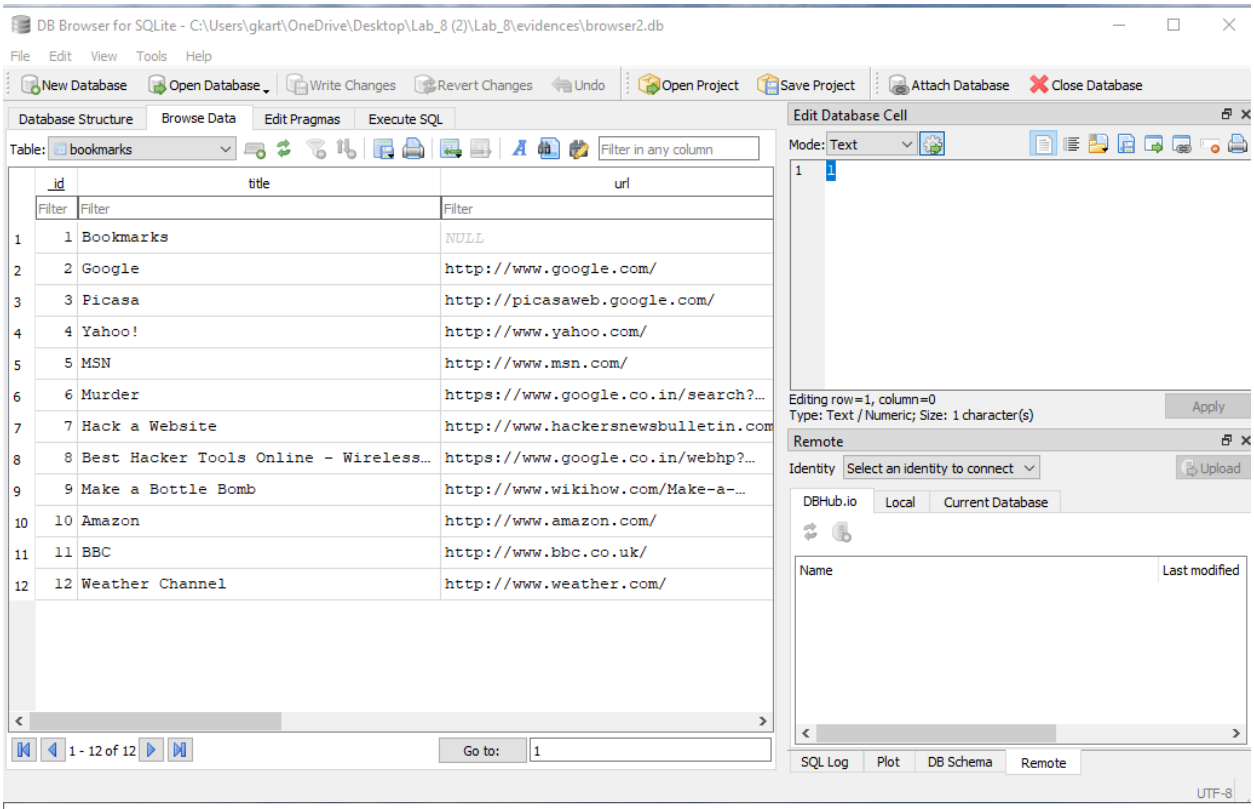
4. Click **Browse Data** to view table contents.



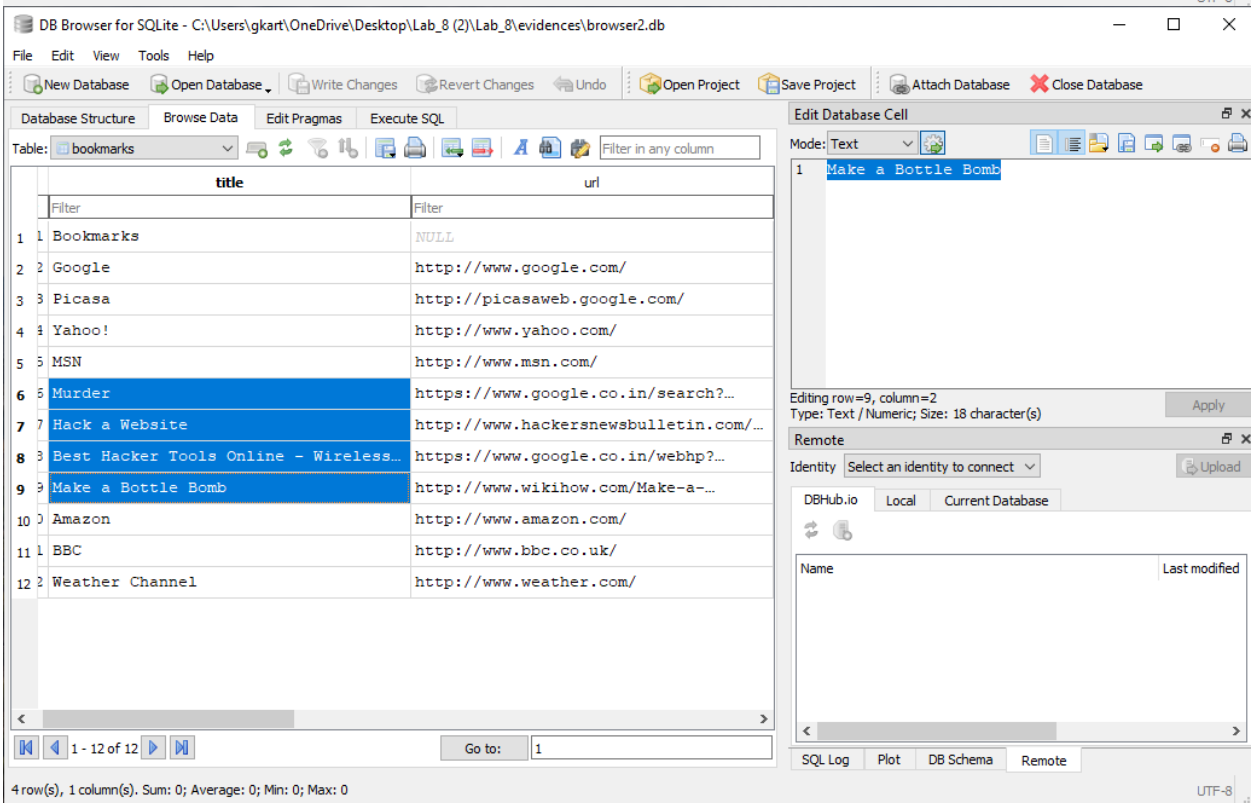
5. Click **Open Database** to open another database file.
6. Navigate to the database folder path and select the browser database file.
7. View different tables like **bookmarks**, **history**, **sqlite_sequence**, etc.


DB Browser for SQLite - C:\Users\gkart\OneDrive\Desktop\Lab_8 (2)\Lab_8\evidences\browser2.db
Choose a database file
This PC › Desktop › Lab_8 (2) › Lab_8 › evidences
Search evidences
Organize
New folder
Quick access
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Name
Date modified
Type
Size
accounts 25-03-2025 20:19 Data Base File 56 KB
browser2 25-03-2025 20:19 Data Base File 400 KB
contacts2 25-03-2025 20:19 Data Base File 308 KB
locksettings 25-03-2025 20:19 Data Base File 20 KB
msgstore 25-03-2025 20:19 Data Base File 124 KB
wa 25-03-2025 20:19 Data Base File 40 KB
File name: browser2
SQLite database files (*.db *.sqlt
Open
Cancel
Close Database
Apply
Upload
Last modified
1 - 12 of 12
Go to: 1
SQL Log
Plot
DB Schema
Remote
UTF-8

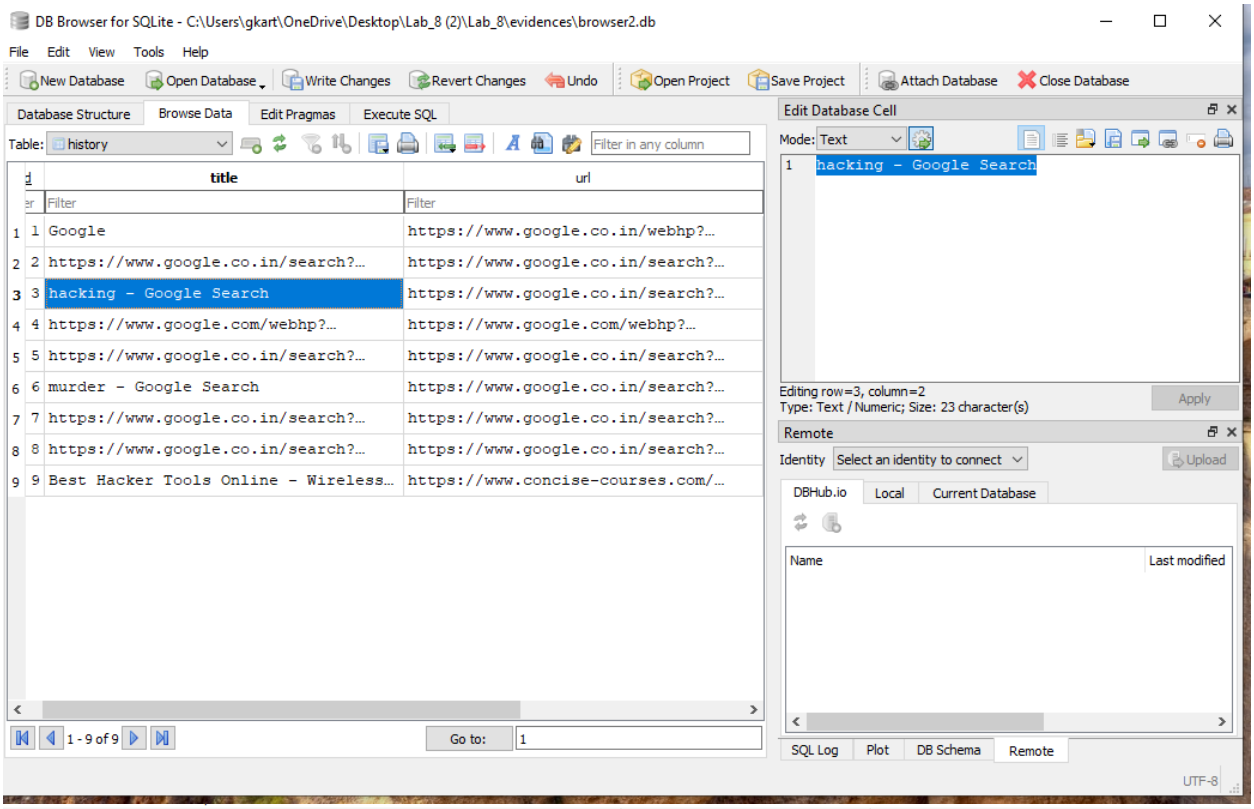

DB Browser for SQLite - C:\Users\gkart\OneDrive\Desktop\Lab_8 (2)\Lab_8\evidences\browser2.db
File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Undo
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Create Table
Create Index
Modify Table
Delete Table
Print
Refresh
Name
Type
Schema
Tables (10)
_sync_state CREATE TABLE _sync_state (_id INTEG
_sync_state_metadata CREATE TABLE _sync_state_metadata
android_metadata CREATE TABLE android_metadata (loca
bookmarks CREATE TABLE bookmarks(_id INTEGE
history CREATE TABLE history(_id INTEGER PR
images CREATE TABLE images (url_key TEXT
searches CREATE TABLE searches (_id INTEGER
settings CREATE TABLE settings (key TEXT PRI
sqlite_sequence CREATE TABLE sqlite_sequence(name,
thumbnails CREATE TABLE thumbnails (_id INTEGE
Indices (1)
imagesUrlIndex CREATE INDEX imagesUrlIndex ON ima
Views (2)
v_accounts CREATE VIEW v_accounts AS SELECT
v_omnibox_suggestions CREATE VIEW v_omnibox_suggestions
Triggers (0)
Edit Database Cell
Mode: Text
NULL
No cell active.
Type: NULL; Size: 0 bytes
Apply
Remote
Identity
Select an identity to connect
Upload
DBHub.io
Local
Current Database
Name
Last modified
SQL Log
Plot
DB Schema
Remote
UTF-8

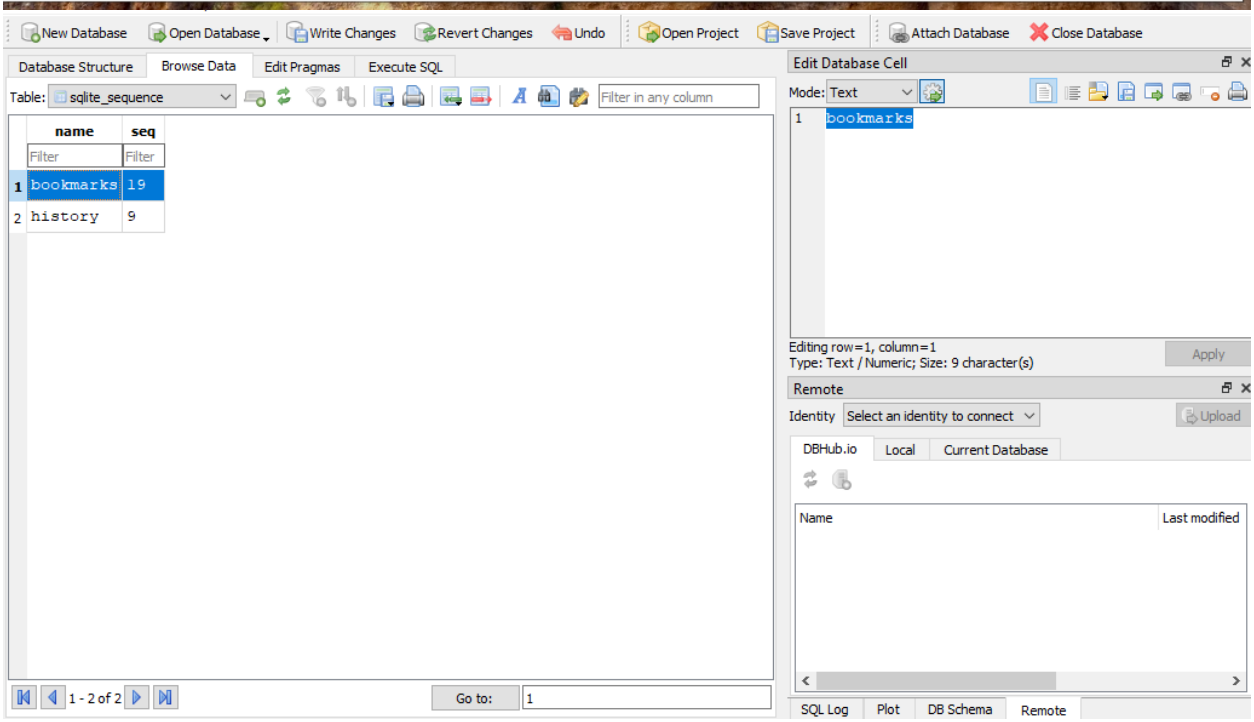


	_id	title	url
1	1	Bookmarks	NULL
2	2	Google	http://www.google.com/
3	3	Picasa	http://picasaweb.google.com/
4	4	Yahoo!	http://www.yahoo.com/
5	5	MSN	http://www.msn.com/
6	6	Murder	https://www.google.co.in/search?...
7	7	Hack a Website	http://www.hackersnewsbulletin.com
8	8	Best Hacker Tools Online - Wireless...	https://www.google.co.in/webhp?...
9	9	Make a Bottle Bomb	http://www.wikihow.com/Make-a-...
10	10	Amazon	http://www.amazon.com/
11	11	BBC	http://www.bbc.co.uk/
12	12	Weather Channel	http://www.weather.com/

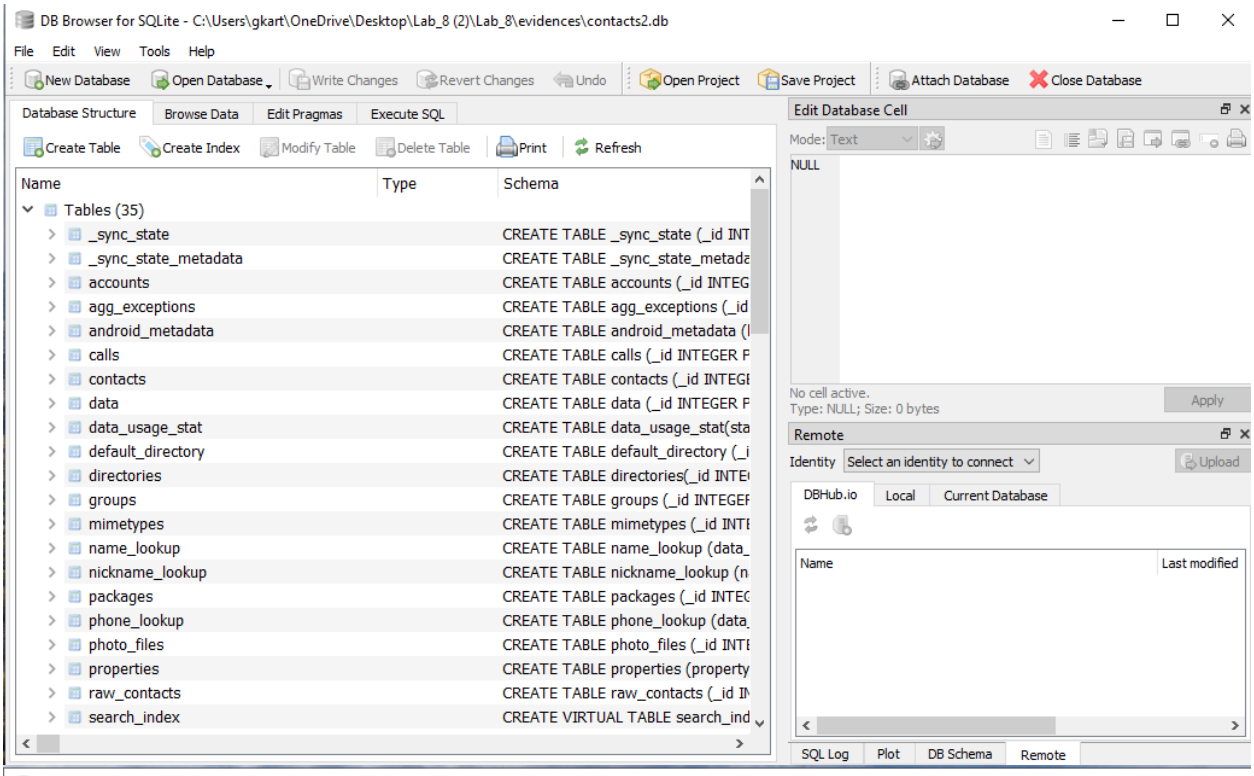


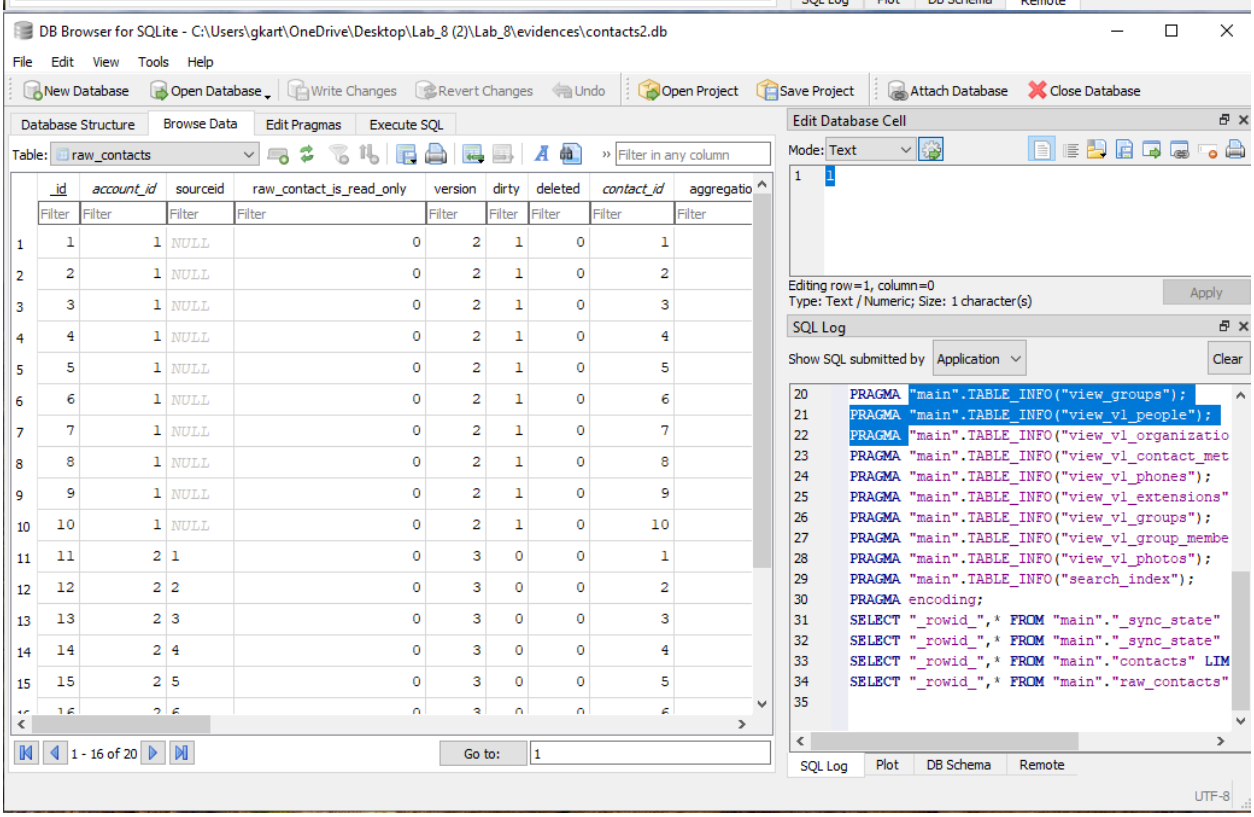
		title	url
1	1	Bookmarks	NULL
2	2	Google	http://www.google.com/
3	3	Picasa	http://picasaweb.google.com/
4	4	Yahoo!	http://www.yahoo.com/
5	5	MSN	http://www.msn.com/
6	6	Murder	https://www.google.co.in/search?...
7	7	Hack a Website	http://www.hackersnewsbulletin.com/...
8	8	Best Hacker Tools Online - Wireless...	https://www.google.co.in/webhp?...
9	9	Make a Bottle Bomb	http://www.wikihow.com/Make-a-...
10	10	Amazon	http://www.amazon.com/
11	11	BBC	http://www.bbc.co.uk/
12	12	Weather Channel	http://www.weather.com/





8. Navigate to the database folder path and select the contact database file.
9. For contacts, open **contacts2.db** and select **raw_contacts** or **calls** table.


DB Browser for SQLite - C:\Users\gkart\OneDrive\Desktop\Lab_8 (2)\Lab_8\evidences\contacts2.db
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 CREATE TABLE _sync_state (_id INT
_sync_state_metadata CREATE TABLE _sync_state_metada
accounts CREATE TABLE accounts (_id INTEG
agg_exceptions CREATE TABLE agg_exceptions (_id
android_metadata CREATE TABLE android_metadata (
calls CREATE TABLE calls (_id INTEGER P
contacts CREATE TABLE contacts (_id INTEGE
data CREATE TABLE data (_id INTEGER P
data_usage_stat CREATE TABLE data_usage_stat(sta
default_directory CREATE TABLE default_directory (_i
directories CREATE TABLE directories(_id INTE
groups CREATE TABLE groups (_id INTEGER
mimetypes CREATE TABLE mimetypes (_id INTE
name_lookup CREATE TABLE name_lookup (data_
nickname_lookup CREATE TABLE nickname_lookup (n
packages CREATE TABLE packages (_id INTEG
phone_lookup CREATE TABLE phone_lookup (data_
photo_files CREATE TABLE photo_files (_id INTE
properties CREATE TABLE properties (property
raw_contacts CREATE TABLE raw_contacts (_id IN
search_index CREATE VIRTUAL TABLE search_ind
Edit Database Cell
Mode: Text
NULL
No cell active.
Type: NULL; Size: 0 bytes
Apply
Remote
Identity Select an identity to connect
Upload
DBHub.io Local Current Database
Name Last modified
SQL Log Plot DB Schema Remote


DB Browser for SQLite - C:\Users\gkart\OneDrive\Desktop\Lab_8 (2)\Lab_8\evidences\contacts2.db
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 column
_id account_id sourceid raw_contact_is_read_only version dirty deleted contact_id aggregatio
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
1 - 16 of 20
Go to: 1
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 "main".TABLE_INFO("view_groups");
PRAGMA "main".TABLE_INFO("view_v1_people");
PRAGMA "main".TABLE_INFO("view_v1_organizatio
PRAGMA "main".TABLE_INFO("view_v1_contact_met
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_membe
PRAGMA "main".TABLE_INFO("view_v1_photos");
PRAGMA "main".TABLE_INFO("search_index");
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."_sync_state"
SELECT "_rowid_",* FROM "main"."_sync_state"
SELECT "_rowid_",* FROM "main"."contacts" LIM
SELECT "_rowid_",* FROM "main"."raw_contacts"
SQL Log Plot DB Schema Remote
UTF-8

DB Browser for SQLite - C:\Users\gkart\OneDrive\Desktop\Lab_8 (2)\Lab_8\evidences\contacts2.db

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

	last_time_contacted	starred	display_name	display_name_alt	display_name_source	phonetic_nam
1	1465378166550	0	Albert	Albert	40	NULL
2	1465378867603	0	Cristene	Cristene	40	NULL
3	1465378095684	0	Adam	Adam	40	NULL
4	1465379244898	0	Beckham	Beckham	40	NULL
5	1465376242521	0	Cherry	Cherry	40	NULL
6	NULL	0	David	David	40	NULL
7	1465379090907	0	Darren	Darren	40	NULL
8	NULL	0	Elly	Elly	40	NULL
9	NULL	0	Fred	Fred	40	NULL
10	1465379517233	0	Henry	Henry	40	NULL
11	NULL	0	Albert	Albert	40	NULL
12	NULL	0	Cristene	Cristene	40	NULL
13	NULL	0	Adam	Adam	40	NULL
14	NULL	0	Beckham	Beckham	40	NULL
15	NULL	0	Cherry	Cherry	40	NULL
16	NULL	0	David	David	40	NULL

1 - 16 of 20 Go to: 1

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 "main".TABLE_INFO("view_groups");
PRAGMA "main".TABLE_INFO("view_v1_people");
PRAGMA "main".TABLE_INFO("view_v1_organizatio
PRAGMA "main".TABLE_INFO("view_v1_contact_met
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_membe
PRAGMA "main".TABLE_INFO("view_v1_photos");
PRAGMA "main".TABLE_INFO("search_index");
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."_sync_state"
SELECT "_rowid_",* FROM "main"."_sync_state"
SELECT "_rowid_",* FROM "main"."contacts" LIM
SELECT "_rowid_",* FROM "main"."raw_contacts"
```

SQL Log | Plot | DB Schema | Remote

UTF-8

DB Browser for SQLite - C:\Users\gkart\OneDrive\Desktop\Lab_8 (2)\Lab_8\evidences\contacts2.db

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

	_id	number	date	duration	type	new	name	numbertype	numberlabel	countryiso	voicemail_uri	is_read	geocoded_location	
1	1	+10000000005	1465376224525	8	2	0	Cherry	2	NULL	US	NULL	NULL		content://
2	2	+10000000003	1465378076924	14	2	0	Adam	2	NULL	US	NULL	NULL		content://
3	3	+10000000004	1465378263153	492	2	0	Beckham	2	NULL	US	NULL	NULL		content://
4	4	+10000000007	1465378892956	79	2	0	Darren	2	NULL	US	NULL	NULL		content://
5	5	+10000000010	1465379422888	0	2	1	Henry	2	NULL	US	NULL	NULL		NULL

1 - 5 of 5 Go to: 1

Edit Database Cell

Mode: Text

Editing row=1, column=0
Type: Text / Numeric; Size: 1 character(s)

Apply

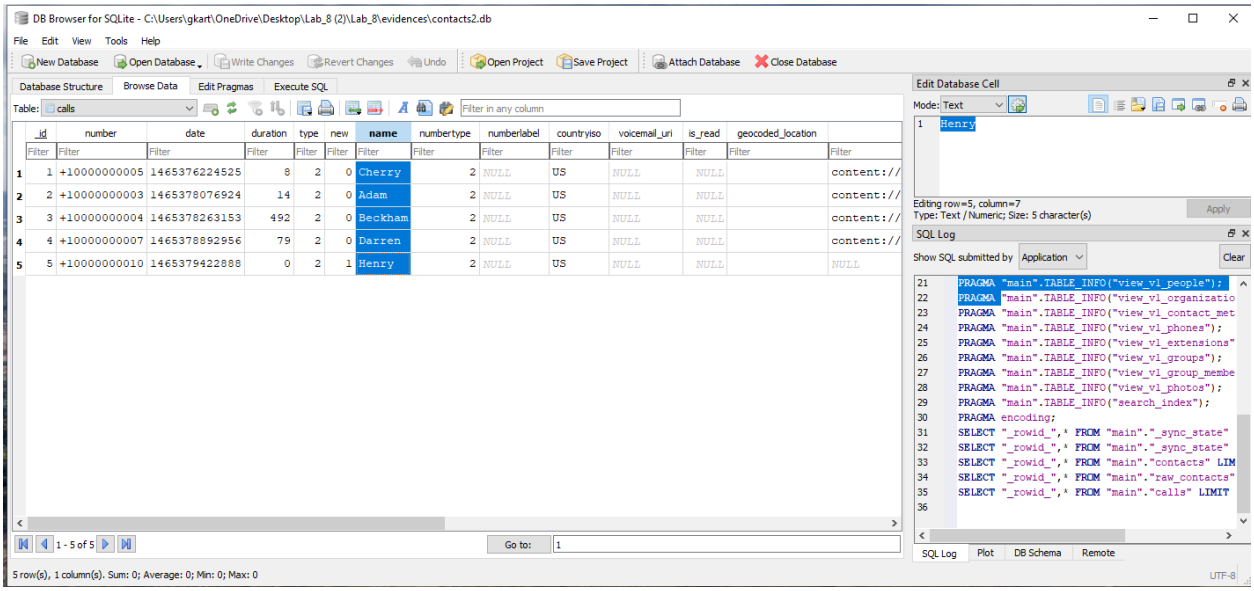
SQL Log

Show SQL submitted by Application Clear

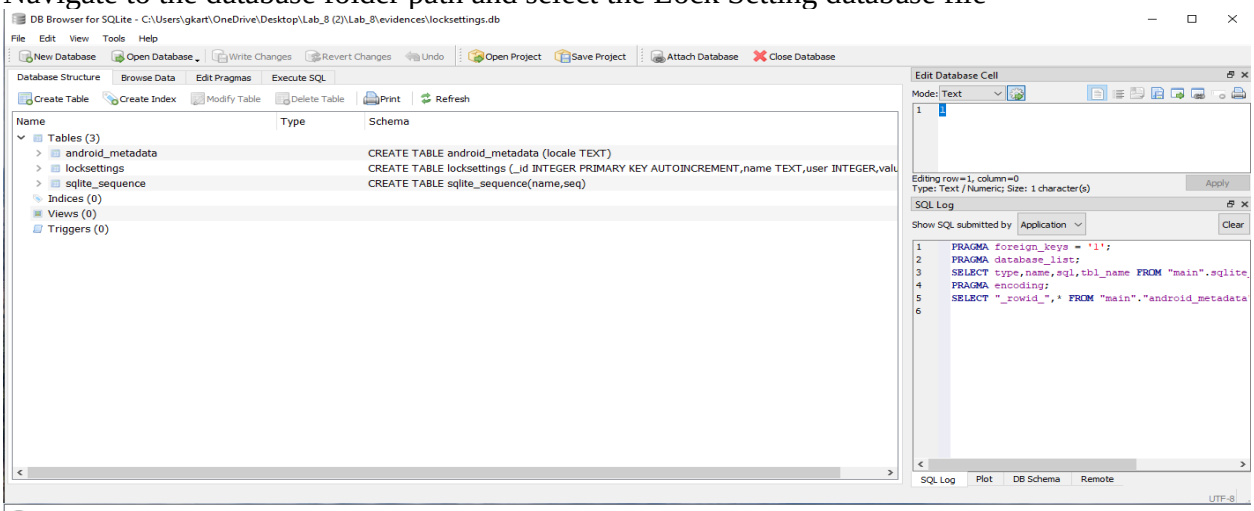
```
PRAGMA "main".TABLE_INFO("view_v1_people");
PRAGMA "main".TABLE_INFO("view_v1_organizatio
PRAGMA "main".TABLE_INFO("view_v1_contact_met
PRAGMA "main".TABLE_INFO("view_v1_phones");
PRAGMA "main".TABLE_INFO("view_v1_extensions"
PRAGMA "main".TABLE_INFO("view_v1_groups");
PRAGMA "main".TABLE_INFO("view_v1_group_membe
PRAGMA "main".TABLE_INFO("view_v1_photos");
PRAGMA "main".TABLE_INFO("search_index");
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."_sync_state"
SELECT "_rowid_",* FROM "main"."_sync_state"
SELECT "_rowid_",* FROM "main"."contacts" LIM
SELECT "_rowid_",* FROM "main"."raw_contacts"
SELECT "_rowid_",* FROM "main"."calls" LIMIT
```

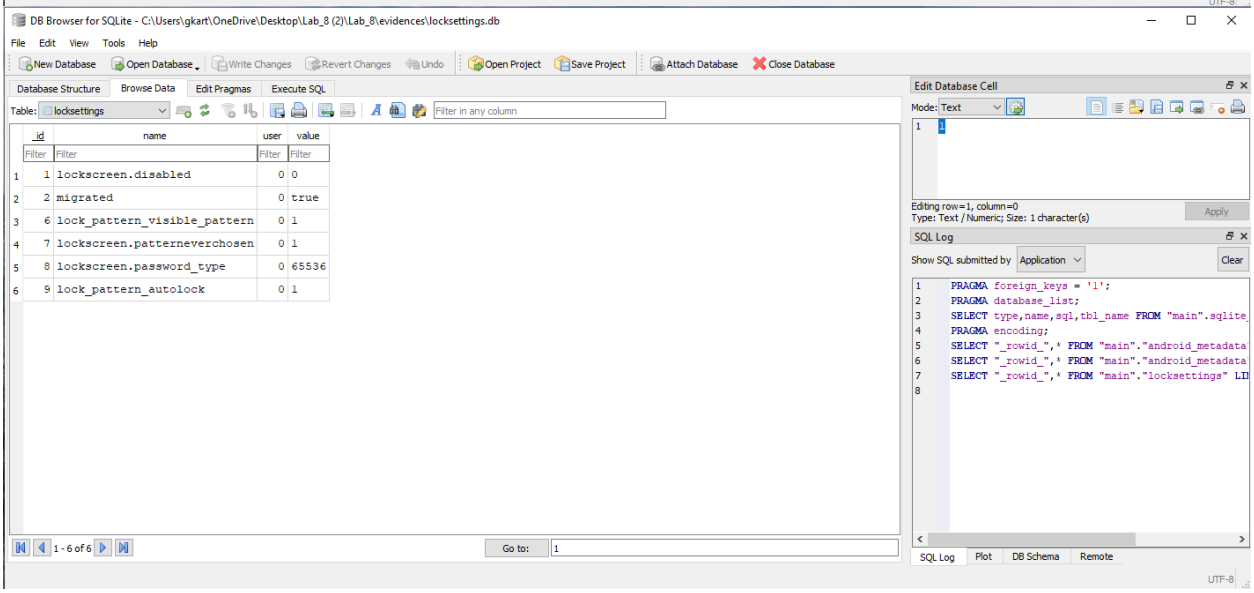
SQL Log | Plot | DB Schema | Remote

UTF-8

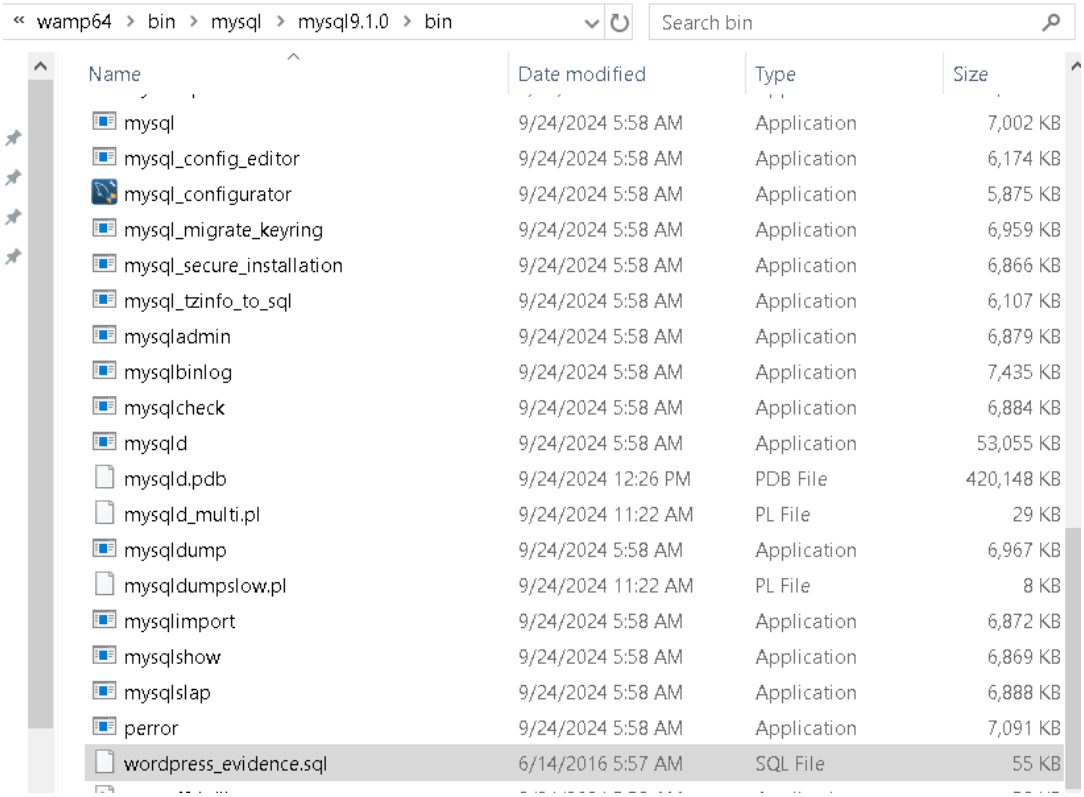


10. Navigate to the database folder path and select the Lock Setting database file





3) Conducting a forensic investigation on a MySQL server database.



Transfer the WordPress evidence file to the WampServer **bin** directory of MySQL and launch the Command Prompt from there.

Run the following command:

mysql -u root -p

```
C:\wamp64\bin\mysql\mysql9.1.0\bin>mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 9.1.0 MySQL Community Server - GPL

Copyright (c) 2000, 2024, 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>
```

After executing this command, it will prompt you to enter a password. If there is no password set, simply press **Enter** to proceed.

```
mysql> create database wordpress;
Query OK, 1 row affected (0.02 sec)

mysql> \q
Bye
```

Create a database named **wordpress** and then exit the MySQL prompt.

```
C:\wamp64\bin\mysql\mysql9.1.0\bin>mysql -u root -p wordpress < wordpress_evidence.sql
Enter password:

C:\wamp64\bin\mysql\mysql9.1.0\bin>
```

Import the data from **wordpressevidence.sql** into the **wordpress** database we created.

```
mysql> use wordpress;
Database changed
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 (0.03 sec)
```

Access the database to view the tables, then retrieve user details using the following command.

```
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.
com        | 0000-00-00 00:00:00 |                     |           0 | Admin         |
|   2 | james      | ceb6c970658f31504a901b89dcd3e461   | james           | jamesfaulkner@gmail.com | http://www.
ebsite.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)
```

It The command displays a list of users stored in the table.

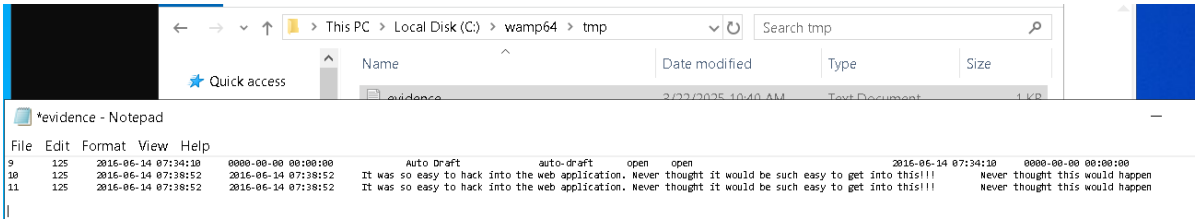
```
mysql> show columns in wp_posts;
+-----------------------+-----------------+------+-----+---------------------+----------------+
| Field                 | Type            | Null | Key | Default             | Extra          |
+-----------------------+-----------------+------+-----+---------------------+----------------+
| ID                    | bigint unsigned | NO   | PRI | NULL                | auto_increment |
| post_author           | bigint unsigned | NO   | MUL | 0                   |                |
| post_date             | datetime        | NO   |     | 0000-00-00 00:00:00 |                |
| post_date_gmt         | datetime        | NO   |     | 0000-00-00 00:00:00 |                |
| post_content          | longtext        | NO   |     | NULL                |                |
| post_title            | text            | NO   |     | NULL                |                |
| post_excerpt          | text            | NO   |     | NULL                |                |
| post_status           | varchar(20)     | NO   |     | publish             |                |
| comment_status        | varchar(20)     | NO   |     | open                |                |
| ping_status           | varchar(20)     | NO   |     | open                |                |
| post_password         | varchar(20)     | NO   |     |                     |                |
| post_name             | varchar(200)    | NO   | MUL |                     |                |
| to_ping               | text            | NO   |     | NULL                |                |
| pinged                | text            | NO   |     | NULL                |                |
| post_modified         | datetime        | NO   |     | 0000-00-00 00:00:00 |                |
| post_modified_gmt     | datetime        | NO   |     | 0000-00-00 00:00:00 |                |
| post_content_filtered | longtext        | NO   |     | NULL                |                |
| post_parent           | bigint unsigned | NO   | MUL | 0                   |                |
| guid                  | varchar(255)    | NO   |     |                     |                |
| menu_order            | int             | NO   |     | 0                   |                |
| post_type             | varchar(20)     | NO   | MUL | post                |                |
| post_mime_type        | varchar(100)    | NO   |     |                     |                |
| comment_count         | bigint          | NO   |     | 0                   |                |
+-----------------------+-----------------+------+-----+---------------------+----------------+
23 rows in set (0.01 sec)
```

Exploring WordPress Database: Author and Post Metadata Overview

The image showcases the structure of the `wp_posts` table in a WordPress database. This table contains crucial details related to posts, including the `post_author`, `post_title`, `post_content`, `post_date`, and other metadata. The `post_author` field links each post to a specific user, enabling us to track the creator of the content. Additionally, attributes like `post_status`, `comment_status`, and `ping_status` provide insights into the post's visibility, interaction settings, and publishing status. This database structure is essential for forensic investigations and content management analysis.

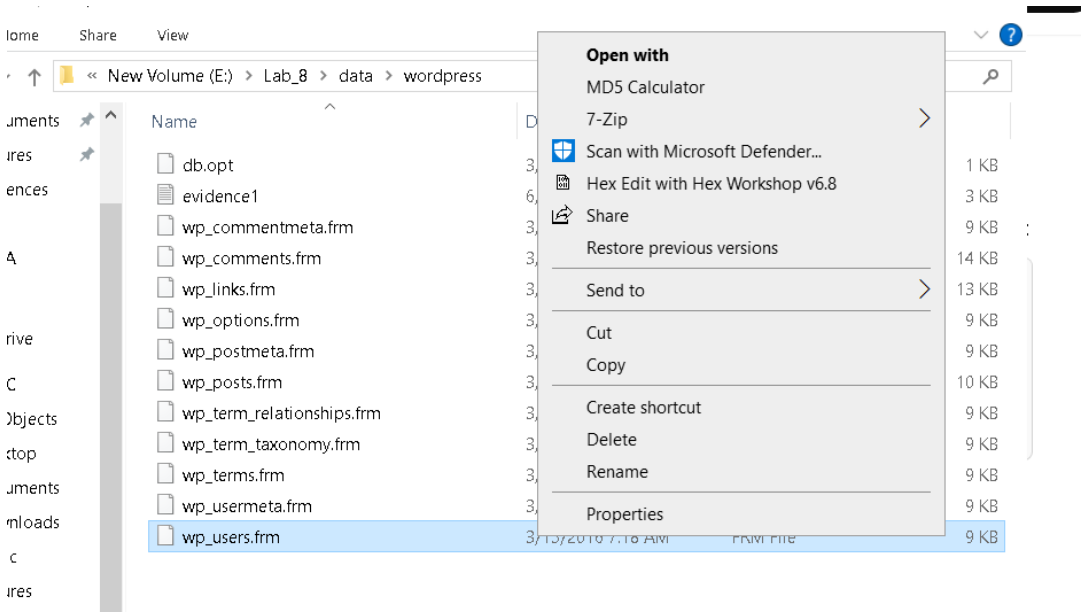
```
mysql> SELECT * FROM wp_posts
    -> WHERE post_author='125'
    -> INTO OUTFILE 'c:/wamp64/tmp/evidence.txt';
Query OK, 3 rows affected (0.00 sec)

mysql>
```

The details of "badguy" have now been stored in the `evidence.txt` file for further analysis and documentation.

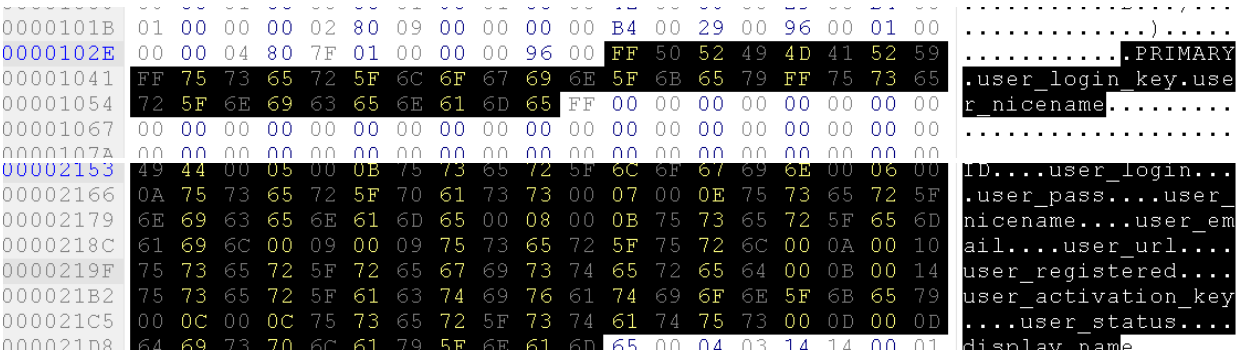


Captured Evidence Verification

The extracted evidence file, `evidence.txt`, contains crucial details confirming unauthorized access to the web application. The stored data verifies the integrity and accuracy of the gathered forensic evidence.



Using a hex editor, we can analyze the binary contents of the database file (`.frm`) to examine the structure and potential evidence related to the bad guy. This allows us to inspect hidden or low-level data stored within the database file.



By examining the database structure, we can observe that login names are stored under the `user_login` column. Through this analysis, we can proceed to investigate log files to verify user activity and gather further details related to the case.

```
5F0  73 65 72 73 60 20 28 60 75 73 65 72 5F 6C 6F 67 69 6E 60  sers` (`user_login`
603  2C 20 60 75 73 65 72 5F 70 61 73 73 60 2C 20 60 75 73 65  , `user_pass`, `use
616  72 5F 6E 69 63 65 6E 61 6D 65 60 2C 20 60 75 73 65 72 5F  r_nicename`, `user_
: 1558  65 6D 61 69 6C 60 2C 20 60 75 73 65 72 5F 73 74 61 74 75  email`, `user_statu
63C  73 60 29 0A 56 41 4C 55 45 53 20 28 27 62 61 64 5F 67 75  s`).VALUES ('bad_gu
64F  79 27 2C 20 4D 44 35 28 27 70 61 73 73 31 32 33 27 29 2C  y', MD5('pass123'),
662  20 27 61 6E 6F 6E 79 6D 6F 75 73 5F 68 61 63 6B 65 72 27  'anonymous_hacker'
675  2C 20 27 62 61 64 67 75 79 40 78 79 7A 2E 63 6F 6D 27 2C  , 'badguy@xyz.com',
688  20 27 30 27 29 C5 B2 5F 57 10 01 00 00 00 1B 00 00 00 A8  '0').._W..........
```

By Through this analysis, we can extract the username and password utilized by the attacker, providing crucial evidence for the investigation.

```
0015257  45 47 49 4E 13 B4 5F 57 02 01 00 00 00 85 00 00 00  EGIN.._W.........
0015268  E0 52 01 00 00 00 2C 00 00 00 00 00 00 00 09 00 00  .R....,..........
0015279  1A 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 06  ................
001528A  03 73 74 64 04 21 00 21 00 08 00 77 6F 72 64 70 72  .std.!.!...wordpr
001529B  65 73 73 00 55 50 44 41 54 45 20 60 77 70 5F 6C 69  ess.UPDATE `wp_li
00152AC  6E 6B 73 60 20 53 45 54 20 60 6C 69 6E 6B 5F 6F 77  nks` SET `link_ow
00152BD  6E 65 72 60 20 3D 20 31 32 35 20 57 48 45 52 45 20  ner` = 125 WHERE
00152CE  60 6C 69 6E 6B 5F 6F 77 6E 65 72 60 20 3D 20 31 32  `link_owner` = 12
00152DF  34 13 B4 5F 57 02 01 00 00 00 4A 00 00 00 2A 53 01  4.._W.....J...*S.
```

By using **Ctrl + F**, we can search based on text or hexadecimal criteria for analysis. In this case, searching for **125** revealed an **UPDATE query** executed by **badguy**, providing key insights into unauthorized modifications.