Lab-02

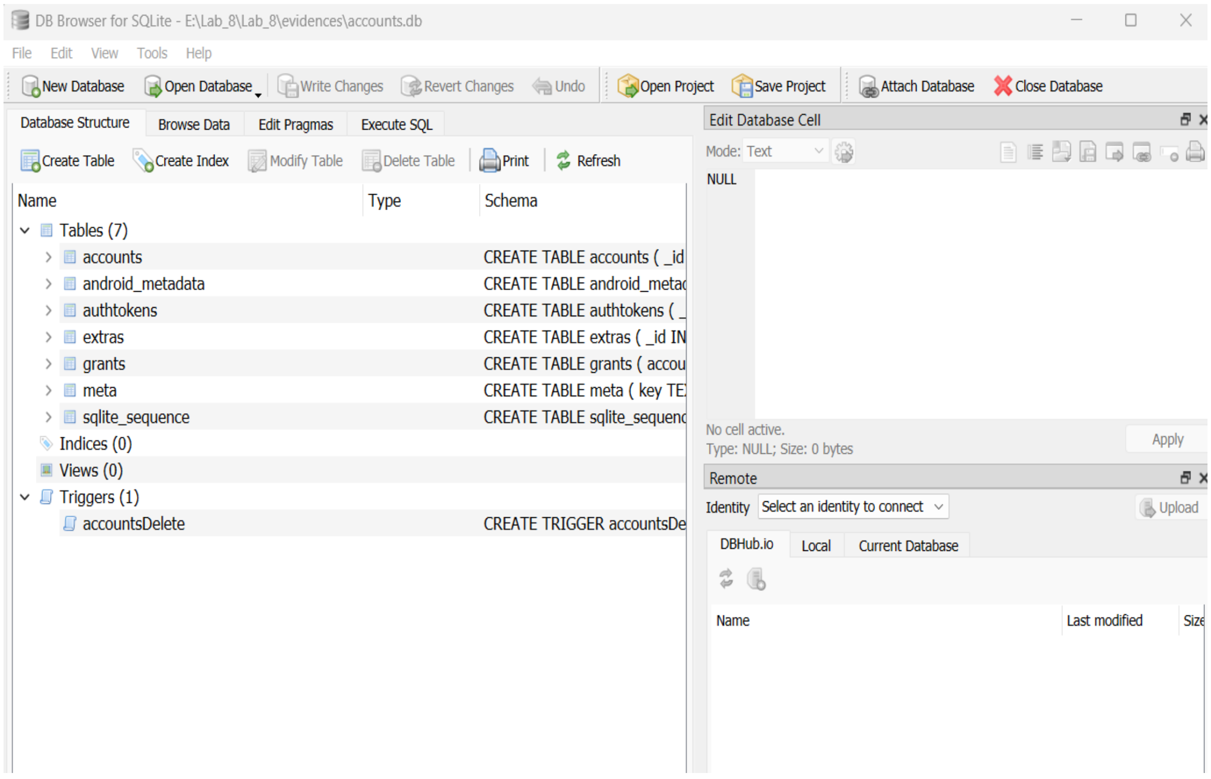
Analyzing SQLite Database using DB Browser for SQLite

Lab objective: In this lab, we will learn how to analyze the SQLite Databases using the open source tool DB Browser for SQLite.

DB Browser for SQLite installed.

Choose a database file window appears.select accounts.db

The application displays the structure of accounts database under the Database structure tab



Name	Type	Schema
Tables (7)		
accounts		CREATE TABLE accounts (_id
android_metadata		CREATE TABLE android_metad
authtokens		CREATE TABLE authtokens (_
extras		CREATE TABLE extras (_id IN
grants		CREATE TABLE grants (accou
meta		CREATE TABLE meta (key TE
sqlite_sequence		CREATE TABLE sqlite_sequenc
Indices (0)		
Views (0)		
Triggers (1)		
accountsDelete		CREATE TRIGGER accountsDe

Click browse data tab to view the data in the account database.

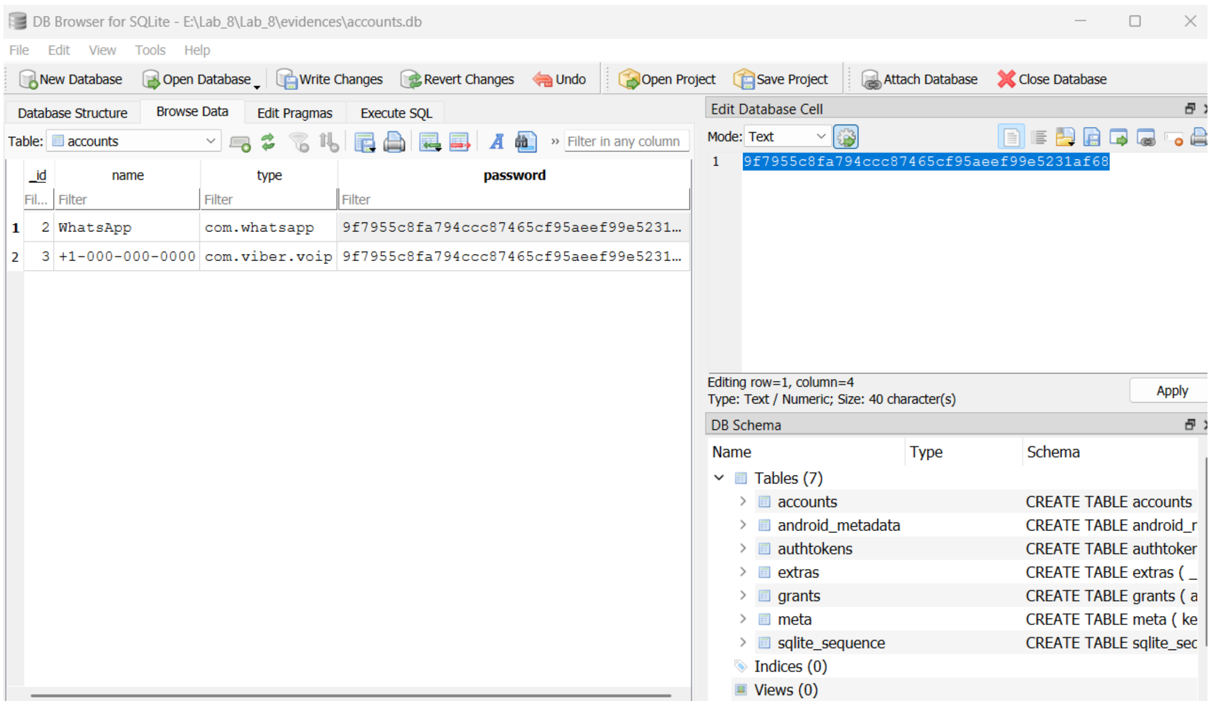

DB Browser for SQLite - E:\Lab_8\Lab_8\evidences\accounts.db

Table: accounts

	_id	name	type	password
1	2	WhatsApp	com.whatsapp	9f7955c8fa794ccc87465cf95aeef99e5231…
2	3	+1-000-000-0000	com.viber.voip	9f7955c8fa794ccc87465cf95aeef99e5231…

Edit Database Cell — Mode: Text

```
1  9f7955c8fa794ccc87465cf95aeef99e5231af68
```

Editing row=1, column=4
Type: Text / Numeric; Size: 40 character(s)

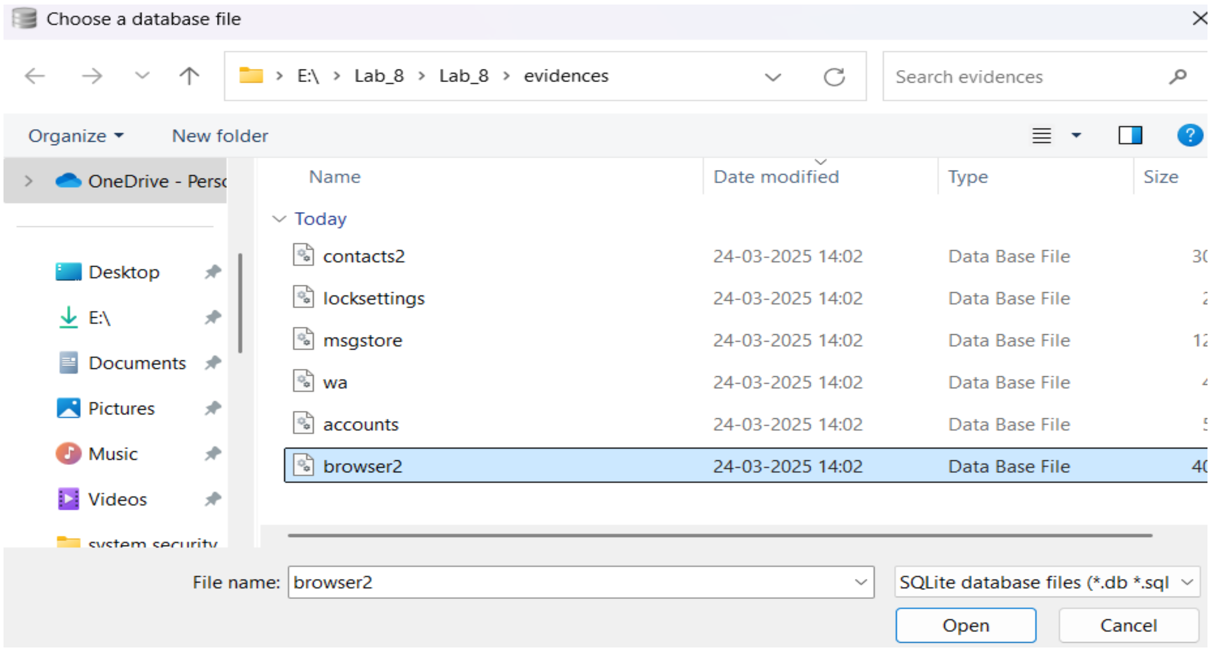
DB Schema

Name	Type	Schema
Tables (7)		
accounts		CREATE TABLE accounts
android_metadata		CREATE TABLE android_r
authtokens		CREATE TABLE authtoker
extras		CREATE TABLE extras (_
grants		CREATE TABLE grants (a
meta		CREATE TABLE meta (ke
sqlite_sequence		CREATE TABLE sqlite_sec
Indices (0)		
Views (0)		

we can observe that the device was synchronized with two accounts:whatsapp and viber.

In the same way we may also view the contents of other tables by selecting them from the table drop-down list.

Now we shall view the information stored in the browser database.To go to the database, click open Database from the toolbar.Select browser2.db file.


Choose a database file

E:\ > Lab_8 > Lab_8 > evidences

Name	Date modified	Type	Size
Today			
contacts2	24-03-2025 14:02	Data Base File	3(
locksettings	24-03-2025 14:02	Data Base File	2
msgstore	24-03-2025 14:02	Data Base File	1:
wa	24-03-2025 14:02	Data Base File	4
accounts	24-03-2025 14:02	Data Base File	5
browser2	24-03-2025 14:02	Data Base File	4(

File name: browser2

SQLite database files (*.db *.sql

Select Browse data tab and select bookmark table from table dropdown list.This displays all the urls that were bookmarked on the device

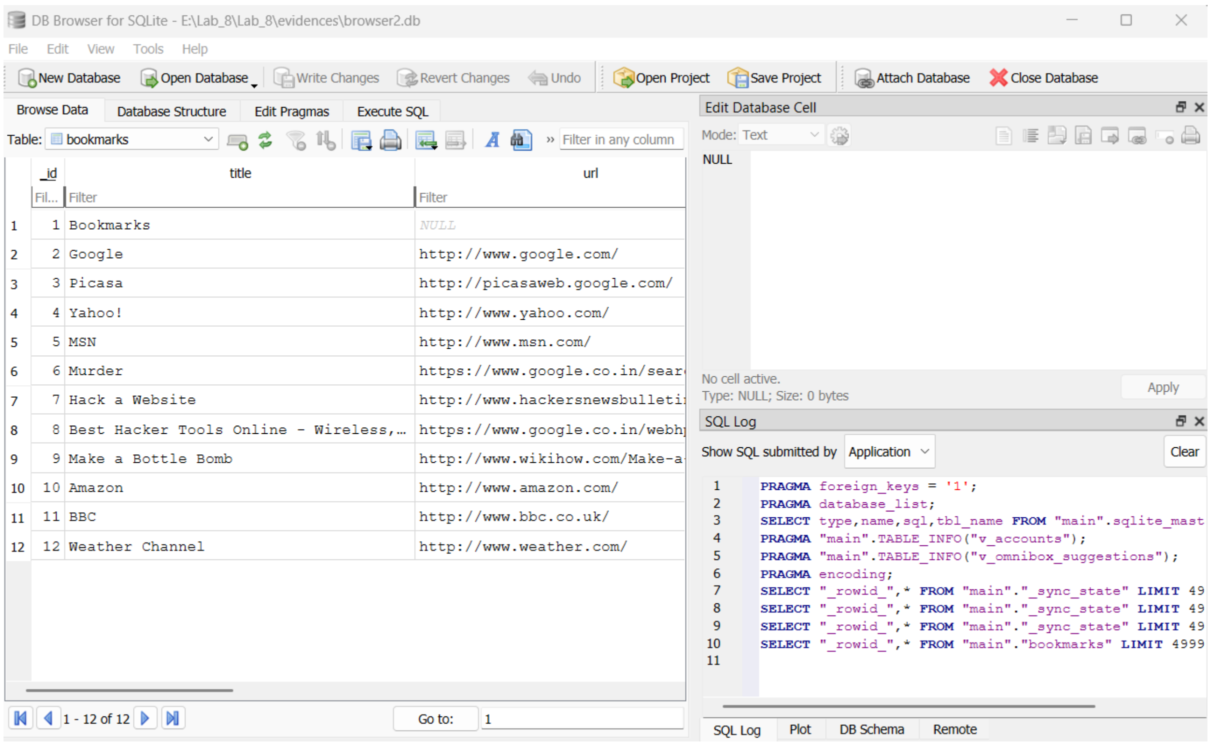

DB Browser for SQLite - E:\Lab_8\Lab_8\evidences\browser2.db

Table: bookmarks

	_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/sear
7	7	Hack a Website	http://www.hackersnewsbulleti
8	8	Best Hacker Tools Online - Wireless,...	https://www.google.co.in/webh
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/

1 - 12 of 12

Edit Database Cell — Mode: Text — NULL — No cell active. Type: NULL; Size: 0 bytes

SQL Log — Show SQL submitted by Application

```
PRAGMA foreign_keys = '1';
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_mast
PRAGMA "main".TABLE_INFO("v_accounts");
PRAGMA "main".TABLE_INFO("v_omnibox_suggestions");
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT 49
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT 49
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT 49
SELECT "_rowid_",* FROM "main"."bookmarks" LIMIT 4999
```

Select history table from the Table drop down list to view the browser history.

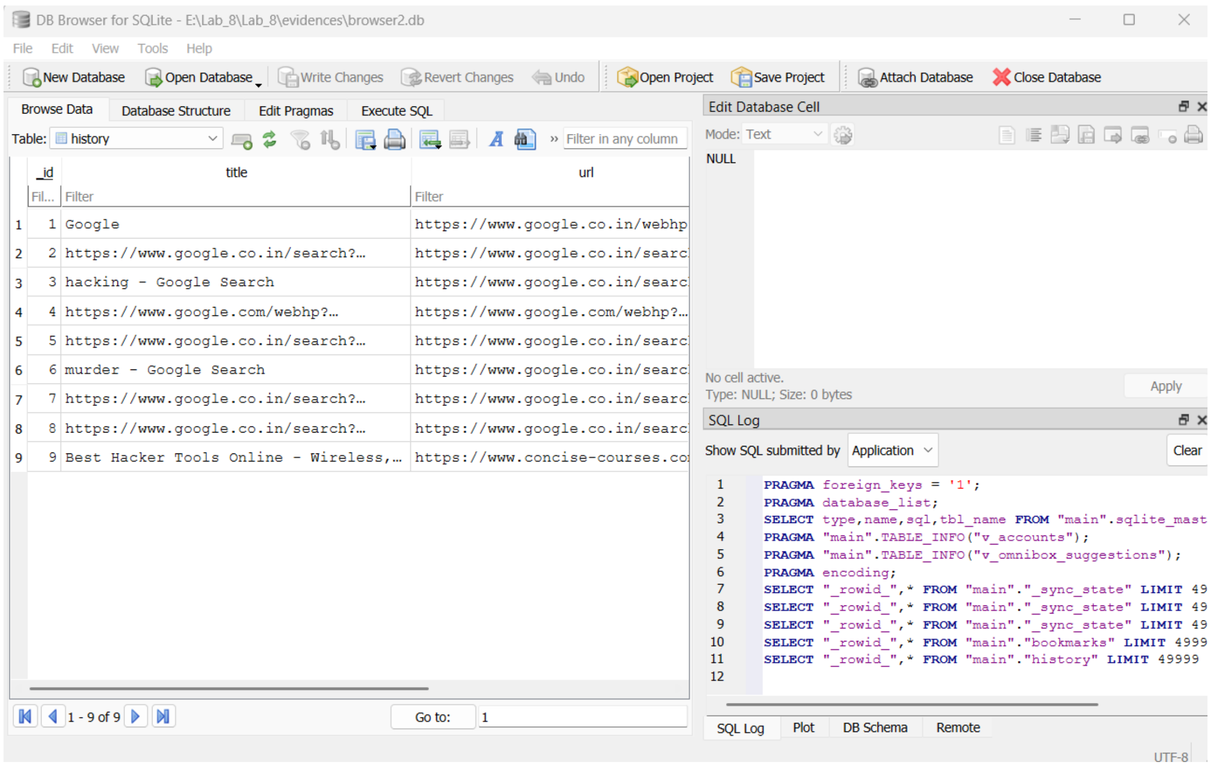

DB Browser for SQLite - E:\Lab_8\Lab_8\evidences\browser2.db

Table: history

	_id	title	url
1	1	Google	https://www.google.co.in/webhp
2	2	https://www.google.co.in/search?...	https://www.google.co.in/searc
3	3	hacking - Google Search	https://www.google.co.in/searc
4	4	https://www.google.com/webhp?...	https://www.google.com/webhp?...
5	5	https://www.google.co.in/search?...	https://www.google.co.in/searc
6	6	murder - Google Search	https://www.google.co.in/searc
7	7	https://www.google.co.in/search?...	https://www.google.co.in/searc
8	8	https://www.google.co.in/search?...	https://www.google.co.in/searc
9	9	Best Hacker Tools Online - Wireless,...	https://www.concise-courses.co

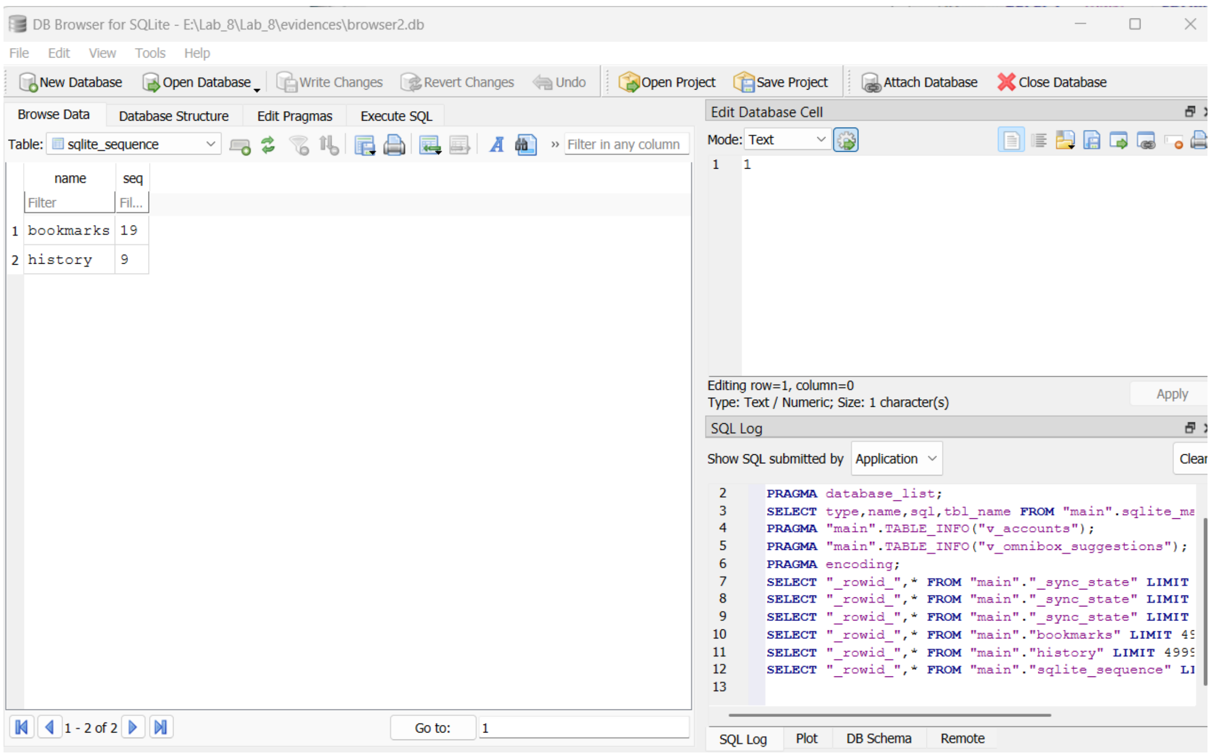
1 - 9 of 9

Edit Database Cell — Mode: Text — NULL — No cell active. Type: NULL; Size: 0 bytes

SQL Log — Show SQL submitted by Application

```
PRAGMA foreign_keys = '1';
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_mast
PRAGMA "main".TABLE_INFO("v_accounts");
PRAGMA "main".TABLE_INFO("v_omnibox_suggestions");
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT 49
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT 49
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT 49
SELECT "_rowid_",* FROM "main"."bookmarks" LIMIT 4999
SELECT "_rowid_",* FROM "main"."history" LIMIT 49999
```

The sqlite _sequence table stores information related to history and bookmarks To view this data select sqlite-sequence table from the Table dropdown list.



DB Browser for SQLite - E:\Lab_8\Lab_8\evidences\browser2.db

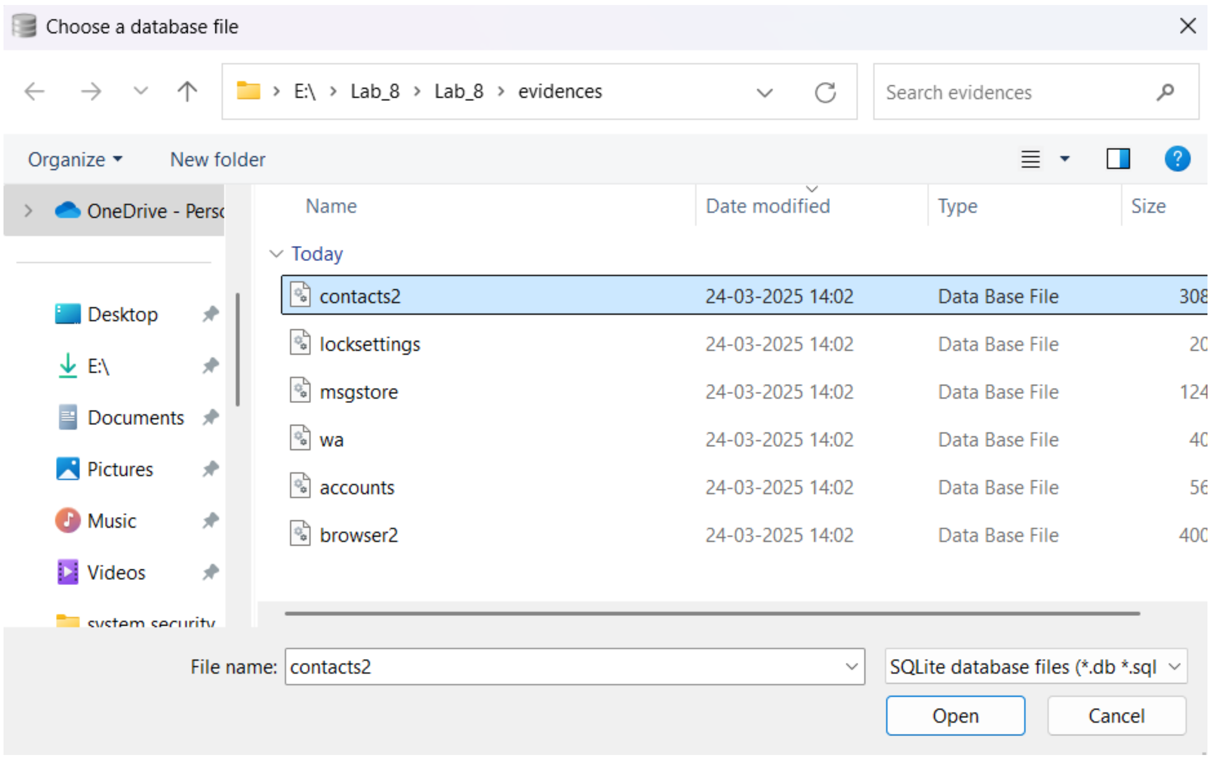
Table: sqlite_sequence

	name	seq
1	bookmarks	19
2	history	9

```
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_ma
PRAGMA "main".TABLE_INFO("v_accounts");
PRAGMA "main".TABLE_INFO("v_omnibox_suggestions");
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT
SELECT "_rowid_",* FROM "main"."_sync_state" LIMIT
SELECT "_rowid_",* FROM "main"."bookmarks" LIMIT 49
SELECT "_rowid_",* FROM "main"."history" LIMIT 4999
SELECT "_rowid_",* FROM "main"."sqlite_sequence" LI
```

Now,we shall examine the contact database inorder to view the contact in the device and the call history.

Select contact2.db



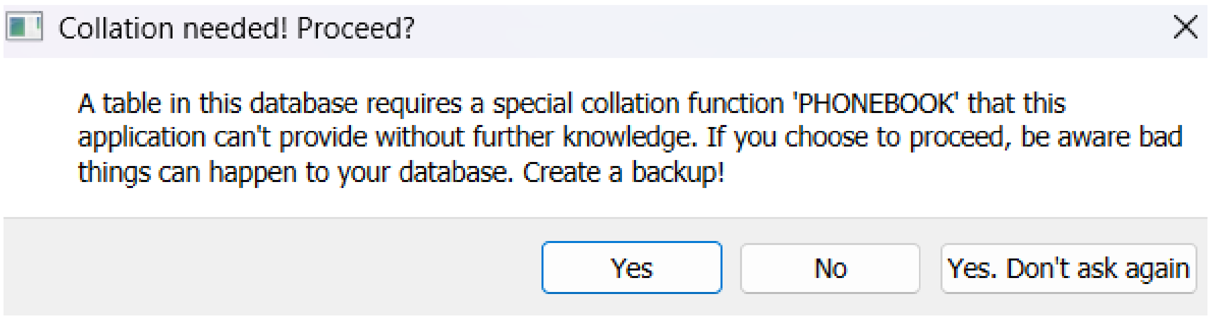
Choose a database file

E:\ › Lab_8 › Lab_8 › evidences

Name	Date modified	Type	Size
contacts2	24-03-2025 14:02	Data Base File	308
locksettings	24-03-2025 14:02	Data Base File	20
msgstore	24-03-2025 14:02	Data Base File	124
wa	24-03-2025 14:02	Data Base File	40
accounts	24-03-2025 14:02	Data Base File	56
browser2	24-03-2025 14:02	Data Base File	400

File name: contacts2

SQLite database files (*.db *.sql



Collation needed! Proceed?

A table in this database requires a special collation function 'PHONEBOOK' that this application can't provide without further knowledge. If you choose to proceed, be aware bad things can happen to your database. Create a backup!

The application displays _sync_state table by default. To view the contact by stored in database ,select raw_contacts table from the Table drop-down list. The raw_contact table stores the informationsuch as display name ,account id,last time contacted, etc.

The content of the table raw_contacts are displayed as shown in following screenshot.

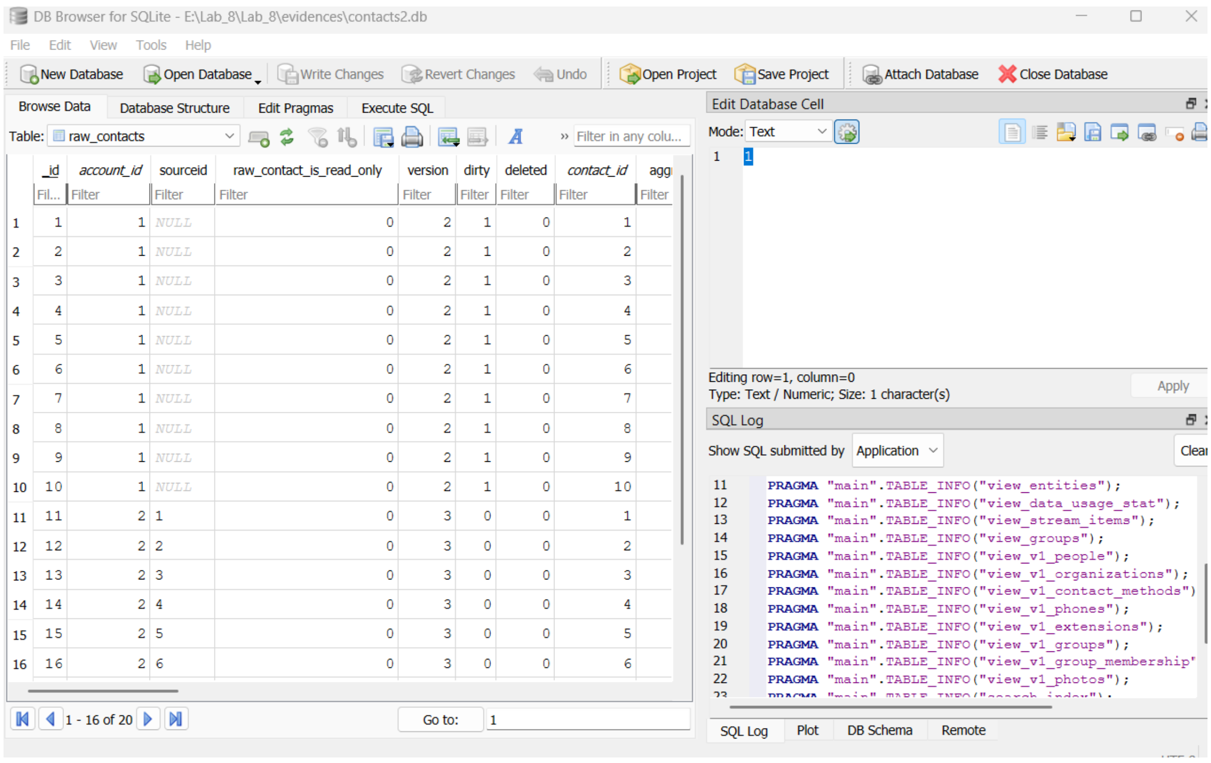


Table: raw_contacts

	_id	account_id	sourceid	raw_contact_is_read_only	version	dirty	deleted	contact_id	agg
	Fil...	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
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	

1 - 16 of 20

Go to: 1

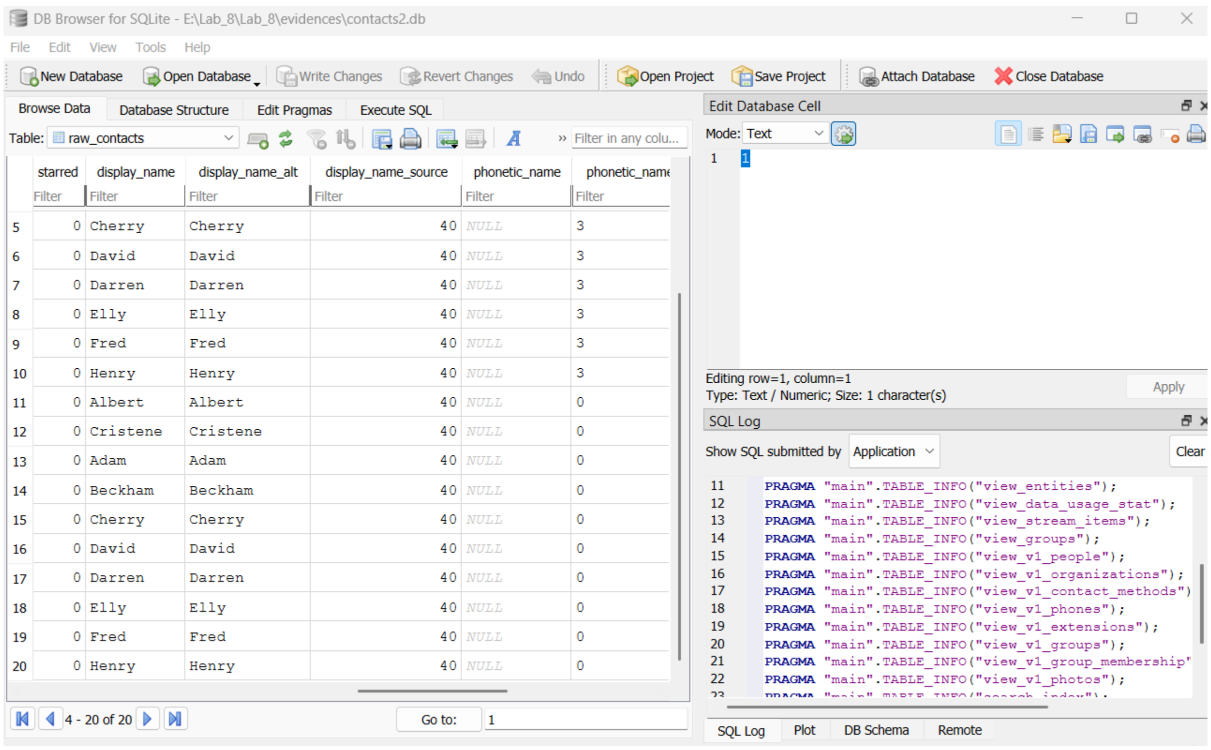
Mode: Text

```
1
```

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

Show SQL submitted by Application

```
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");
```



DB Browser for SQLite - E:\Lab_8\Lab_8\evidences\contacts2.db

Table: raw_contacts

	starred	display_name	display_name_alt	display_name_source	phonetic_name	phonetic_name
5	0	Cherry	Cherry	40	NULL	3
6	0	David	David	40	NULL	3
7	0	Darren	Darren	40	NULL	3
8	0	Elly	Elly	40	NULL	3
9	0	Fred	Fred	40	NULL	3
10	0	Henry	Henry	40	NULL	3
11	0	Albert	Albert	40	NULL	0
12	0	Cristene	Cristene	40	NULL	0
13	0	Adam	Adam	40	NULL	0
14	0	Beckham	Beckham	40	NULL	0
15	0	Cherry	Cherry	40	NULL	0
16	0	David	David	40	NULL	0
17	0	Darren	Darren	40	NULL	0
18	0	Elly	Elly	40	NULL	0
19	0	Fred	Fred	40	NULL	0
20	0	Henry	Henry	40	NULL	0

4 - 20 of 20   Go to: 1

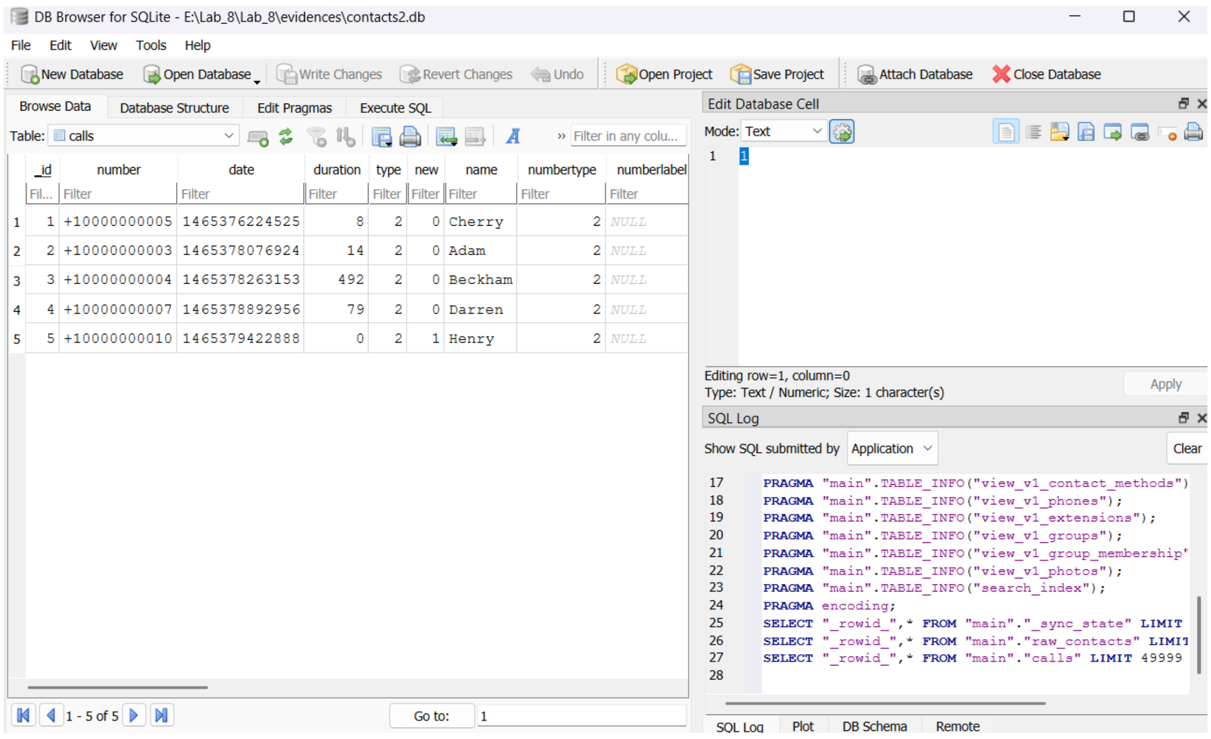
Edit Database Cell
Mode: Text
Editing row=1, column=1
Type: Text / Numeric; Size: 1 character(s)

SQL Log
Show SQL submitted by Application

```
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");
```

The calls table contain the call history, associated with the device. This table contains details such as the dialed numbers , dialed contact name, timestamp, call duration etc.

To view this information,select calls from the Table drop-down list.



DB Browser for SQLite - E:\Lab_8\Lab_8\evidences\contacts2.db

Table: calls

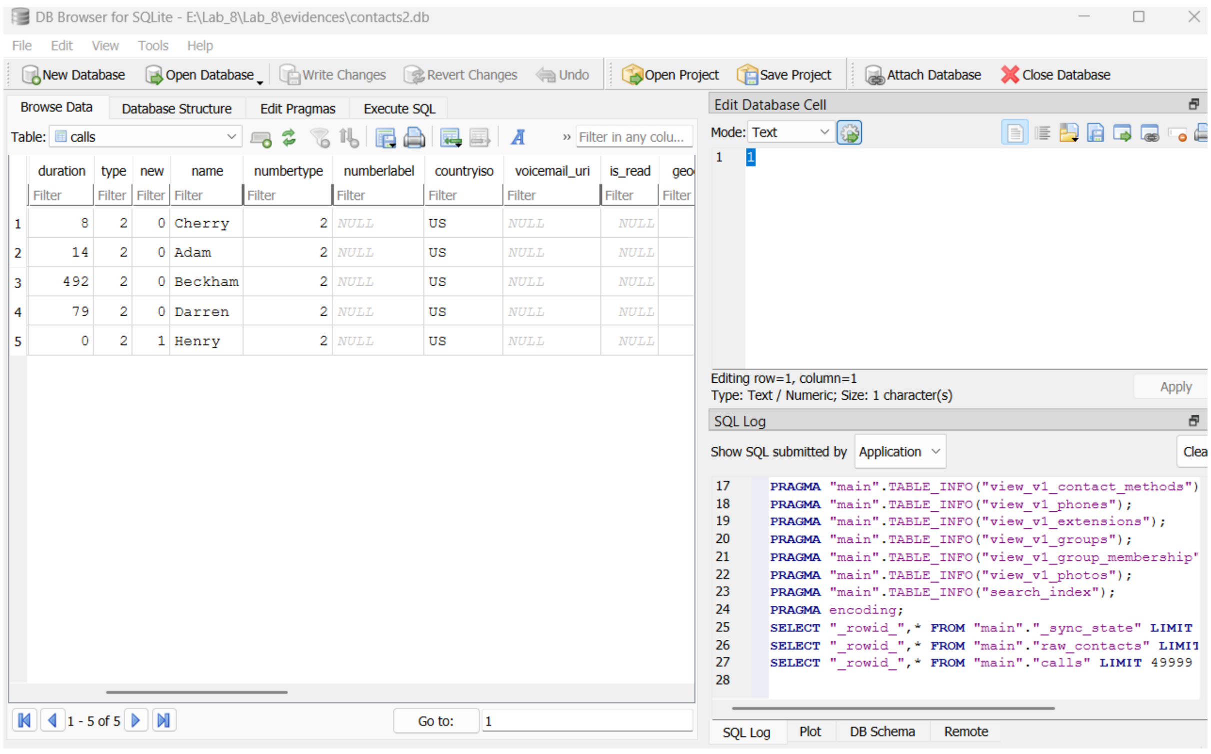
	_id	number	date	duration	type	new	name	numbertype	numberlabel
1	1	+10000000005	1465376224525	8	2	0	Cherry	2	NULL
2	2	+10000000003	1465378076924	14	2	0	Adam	2	NULL
3	3	+10000000004	1465378263153	492	2	0	Beckham	2	NULL
4	4	+10000000007	1465378892956	79	2	0	Darren	2	NULL
5	5	+10000000010	1465379422888	0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

SQL Log
Show SQL submitted by Application

```
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
SELECT "_rowid_",* FROM "main"."raw_contacts" LIMI
SELECT "_rowid_",* FROM "main"."calls" LIMIT 49999
```

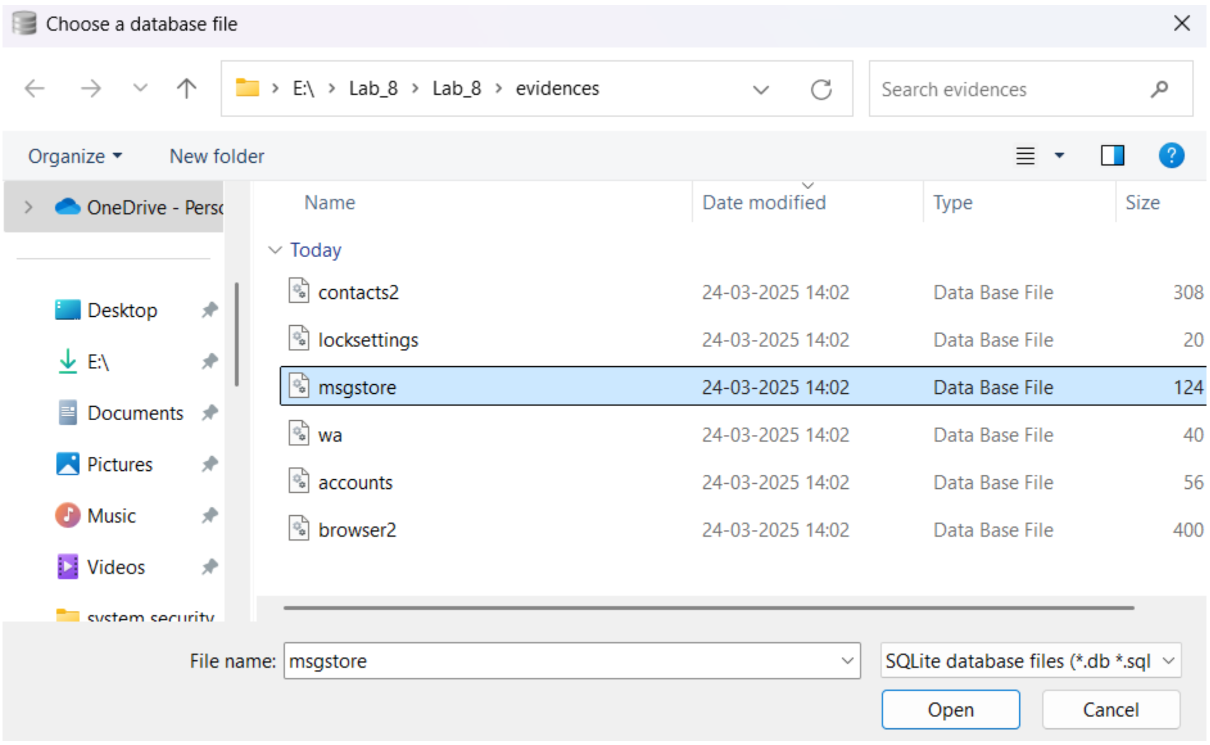


	duration	type	new	name	numbertype	numberlabel	countryiso	voicemail_uri	is_read	geo
1	8	2	0	Cherry	2	NULL	US	NULL	NULL	
2	14	2	0	Adam	2	NULL	US	NULL	NULL	
3	492	2	0	Beckham	2	NULL	US	NULL	NULL	
4	79	2	0	Darren	2	NULL	US	NULL	NULL	
5	0	2	1	Henry	2	NULL	US	NULL	NULL	

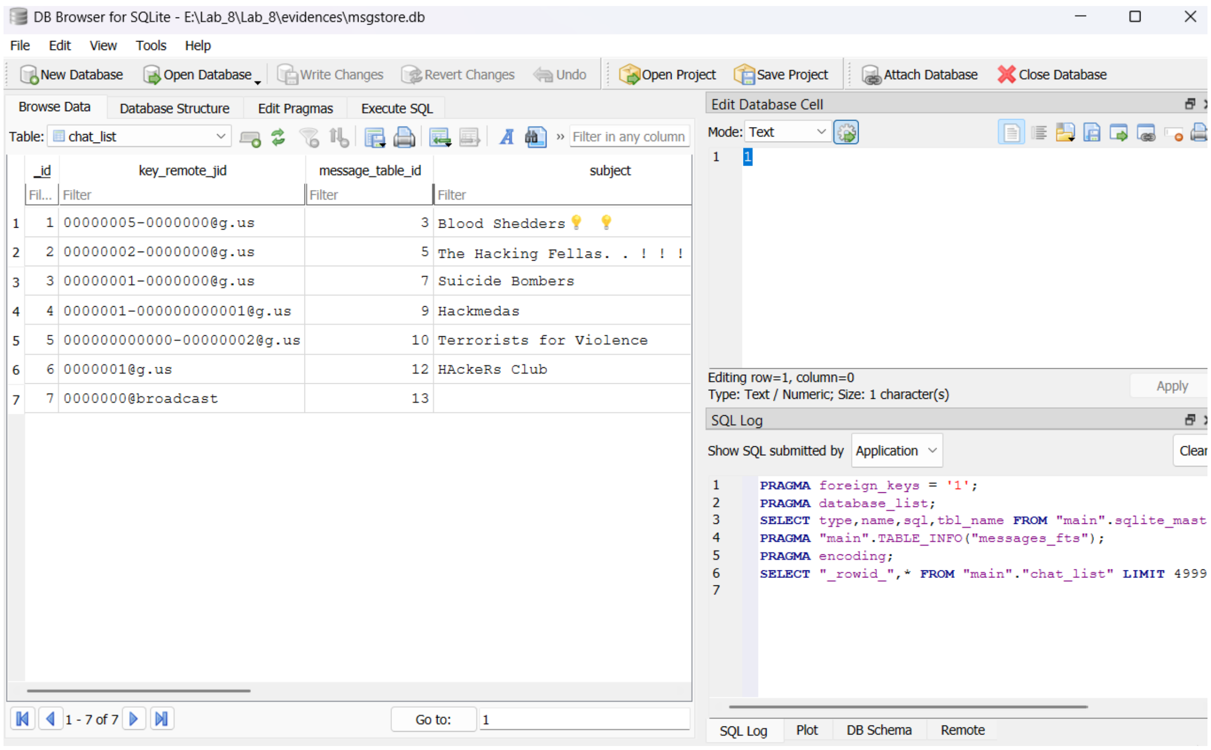
Editing row=1, column=1
Type: Text / Numeric; Size: 1 character(s)

```
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
SELECT "_rowid_",* FROM "main"."raw_contacts" LIMIT
SELECT "_rowid_",* FROM "main"."calls" LIMIT 49999
```

Now we shall view the data stored in msgstore database. The msgstore database contains information related to the message stored on the device ,timestamps of the sent and the received messages, subject of message etc.



Name	Date modified	Type	Size
contacts2	24-03-2025 14:02	Data Base File	308
locksettings	24-03-2025 14:02	Data Base File	20
msgstore	24-03-2025 14:02	Data Base File	124
wa	24-03-2025 14:02	Data Base File	40
accounts	24-03-2025 14:02	Data Base File	56
browser2	24-03-2025 14:02	Data Base File	400

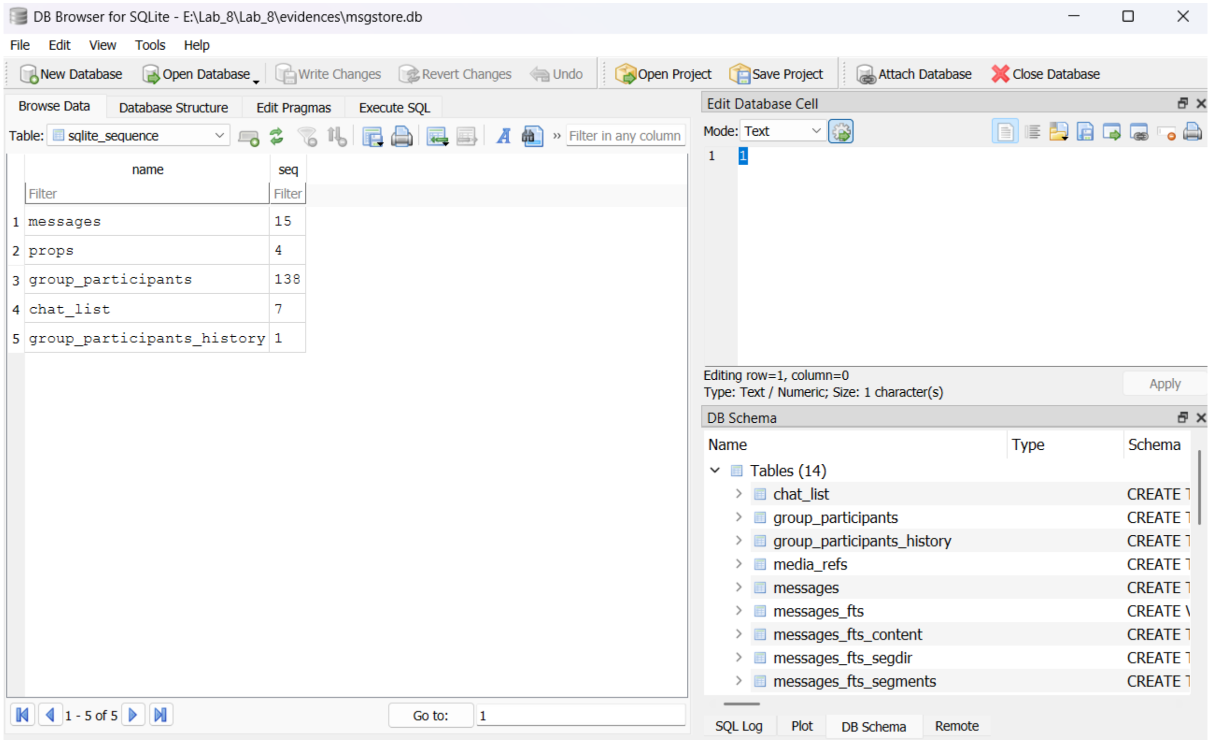

DB Browser for SQLite - E:\Lab_8\Lab_8\evidences\msgstore.db
File Edit View Tools Help
New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database
Browse Data Database Structure Edit Pragmas Execute SQL
Table: chat_list
Filter in any column
Edit Database Cell
Mode: Text
Apply
SQL Log
Show SQL submitted by Application
Clear
1 - 7 of 7
Go to: 1
SQL Log Plot DB Schema Remote

	_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	

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

```
PRAGMA foreign_keys = '1';
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_mast
PRAGMA "main".TABLE_INFO("messages_fts");
PRAGMA encoding;
SELECT "_rowid_",* FROM "main"."chat_list" LIMIT 4999
```

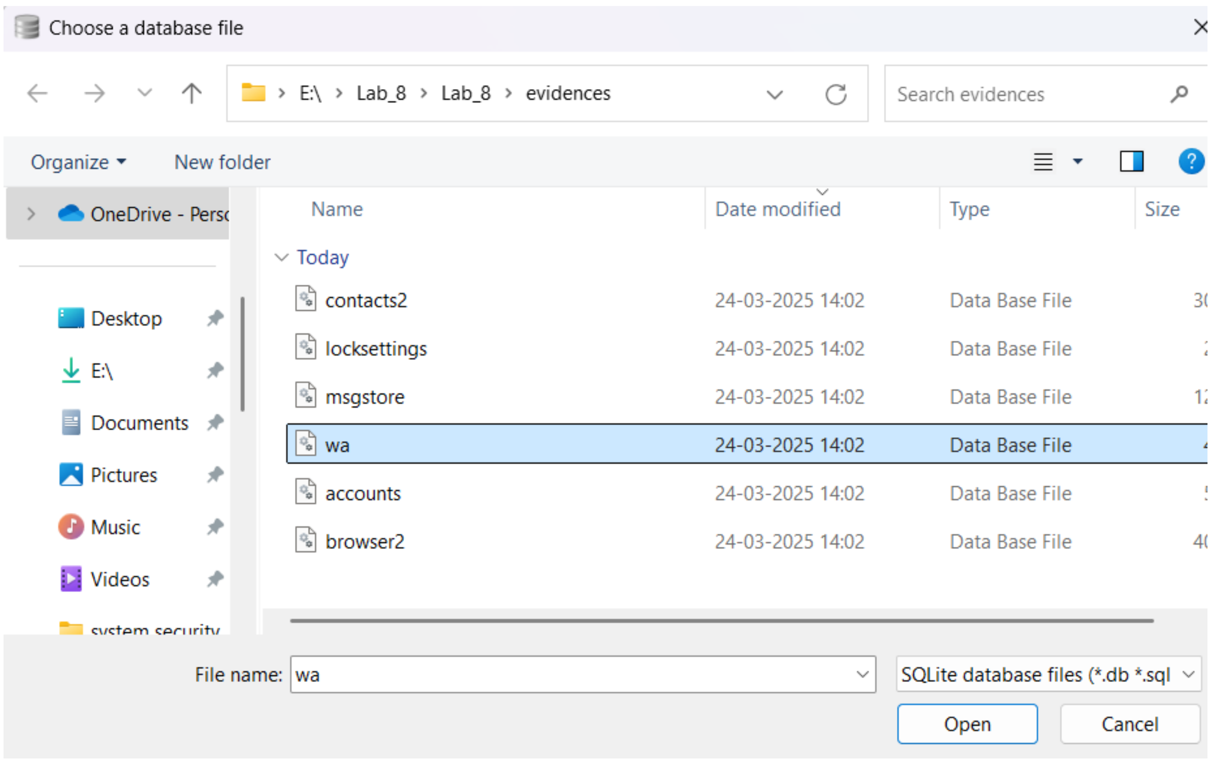
In the sameway ,we may analyze the other tables in the database inorder to find more information associated with the database.


DB Browser for SQLite - E:\Lab_8\Lab_8\evidences\msgstore.db
File Edit View Tools Help
New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database
Browse Data Database Structure Edit Pragmas Execute SQL
Table: sqlite_sequence
Filter in any column
Edit Database Cell
Mode: Text
Apply
DB Schema
1 - 5 of 5
Go to: 1
SQL Log Plot DB Schema Remote

	name	seq
1	messages	15
2	props	4
3	group_participants	138
4	chat_list	7
5	group_participants_history	1

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

Name	Type	Schema
Tables (14)		
chat_list		CREATE T
group_participants		CREATE T
group_participants_history		CREATE T
media_refs		CREATE T
messages		CREATE T
messages_fts		CREATE V
messages_fts_content		CREATE T
messages_fts_segdir		CREATE T
messages_fts_segments		CREATE T



Name	Date modified	Type	Size
Today			
contacts2	24-03-2025 14:02	Data Base File	3
locksettings	24-03-2025 14:02	Data Base File	
msgstore	24-03-2025 14:02	Data Base File	1
wa	24-03-2025 14:02	Data Base File	
accounts	24-03-2025 14:02	Data Base File	
browser2	24-03-2025 14:02	Data Base File	4

File name: wa

SQLite database files (*.db *.sql

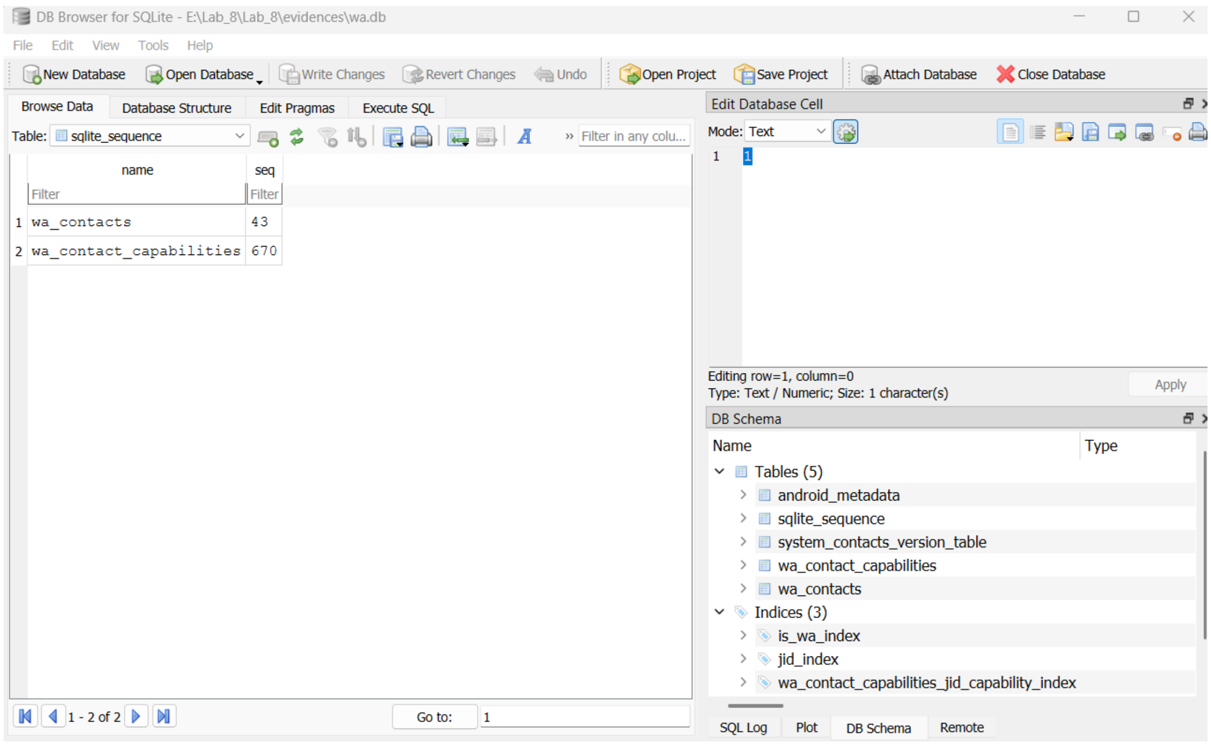

DB Browser for SQLite - E:\Lab_8\Lab_8\evidences\wa.db

Table: sqlite_sequence

	name	seq
1	wa_contacts	43
2	wa_contact_capabilities	670

1 - 2 of 2   Go to: 1

Mode: Text

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

Name	Type
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_index	

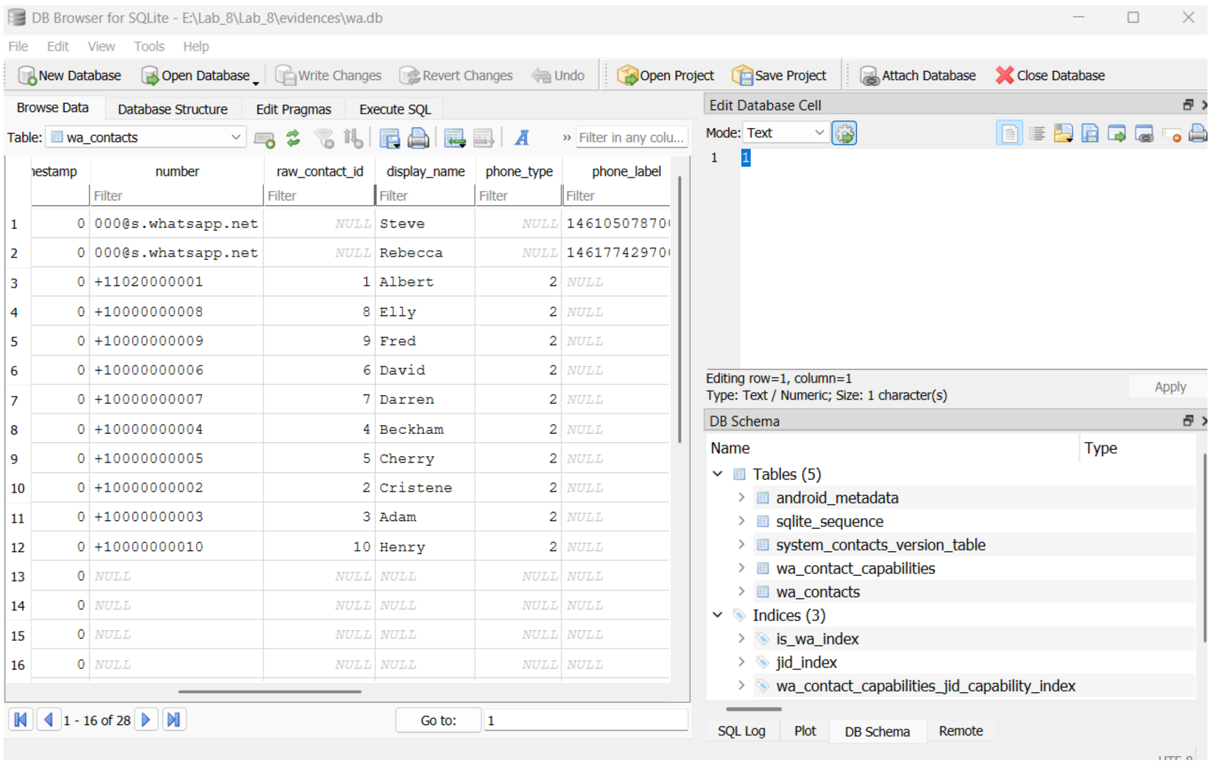


Table: wa_contacts

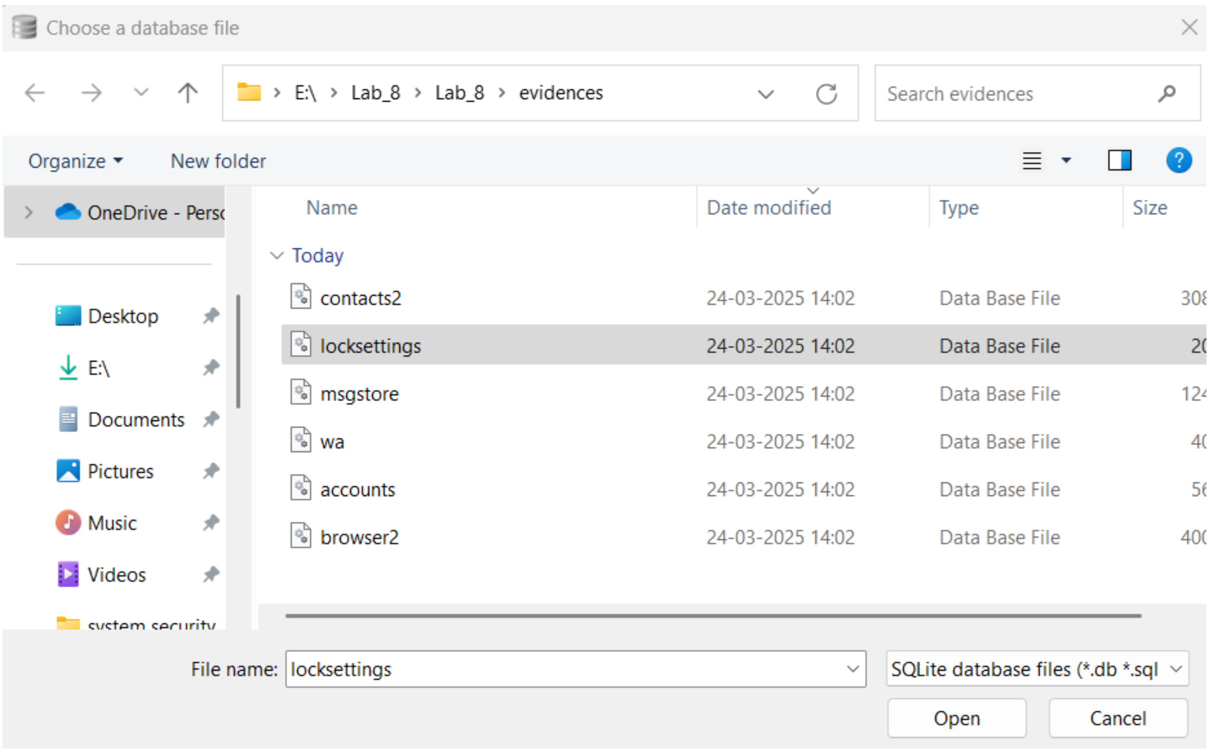
	estamp	number	raw_contact_id	display_name	phone_type	phone_label
1	0	000@s.whatsapp.net	NULL	Steve	NULL	14610507870
2	0	000@s.whatsapp.net	NULL	Rebecca	NULL	14617742970
3	0	+11020000001	1	Albert	2	NULL
4	0	+10000000008	8	Elly	2	NULL
5	0	+10000000009	9	Fred	2	NULL
6	0	+10000000006	6	David	2	NULL
7	0	+10000000007	7	Darren	2	NULL
8	0	+10000000004	4	Beckham	2	NULL
9	0	+10000000005	5	Cherry	2	NULL
10	0	+10000000002	2	Cristene	2	NULL
11	0	+10000000003	3	Adam	2	NULL
12	0	+10000000010	10	Henry	2	NULL
13	0	NULL	NULL	NULL	NULL	NULL
14	0	NULL	NULL	NULL	NULL	NULL
15	0	NULL	NULL	NULL	NULL	NULL
16	0	NULL	NULL	NULL	NULL	NULL

1 - 16 of 28 Go to: 1

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

Name	Type
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_index	

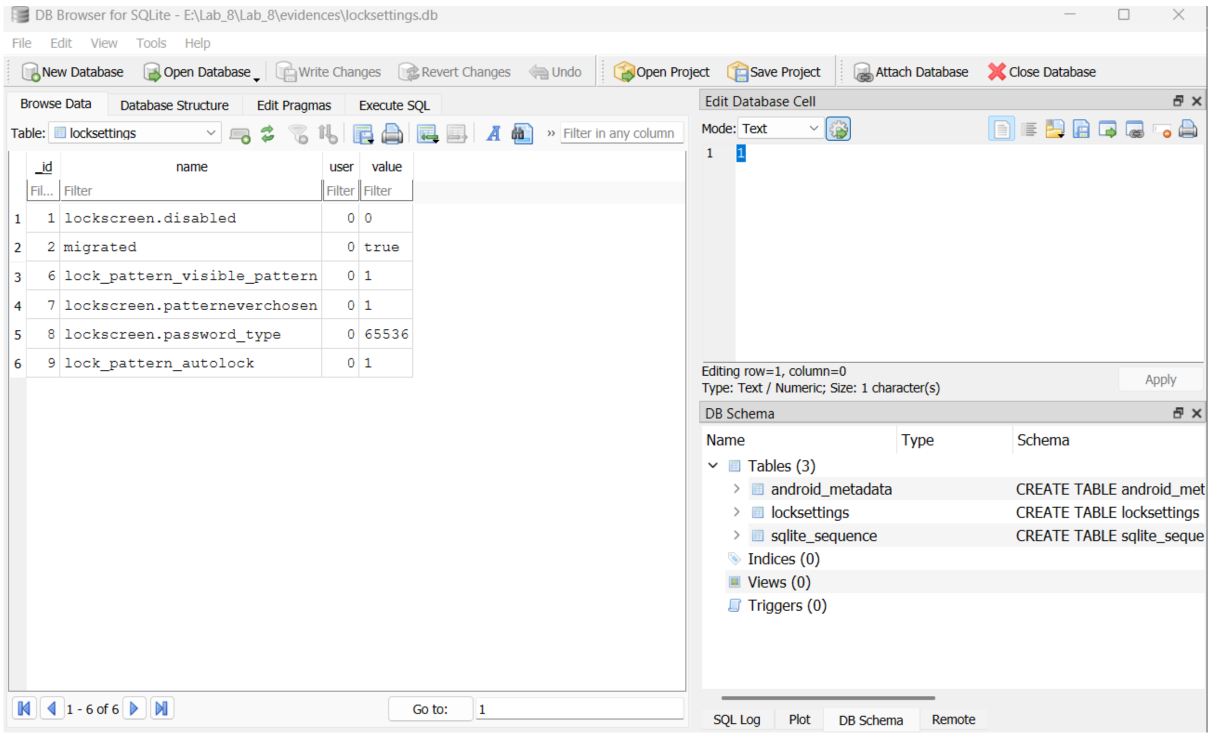
The locksetting database contains the settings such as the status of the lock screen ,lock screen password type, status of the lockscreen pattern autolock , visibility of the lockscreen pattern ,etc.



Name	Date modified	Type	Size
Today			
contacts2	24-03-2025 14:02	Data Base File	308
locksettings	24-03-2025 14:02	Data Base File	20
msgstore	24-03-2025 14:02	Data Base File	124
wa	24-03-2025 14:02	Data Base File	40
accounts	24-03-2025 14:02	Data Base File	56
browser2	24-03-2025 14:02	Data Base File	400

File name: locksettings
SQLite database files (*.db *.sql

Select locksetting from the Table drop-down list , to view settings associated with the lock screen pattern as shown in the following screenshot.



	_id	name	user	value
1	1	lockscreen.disabled	0	0
2	2	migrated	0	true
3	6	lock_pattern_visible_pattern	0	1
4	7	lockscreen.patterneverchosen	0	1
5	8	lockscreen.password_type	0	65536
6	9	lock_pattern_autolock	0	1

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

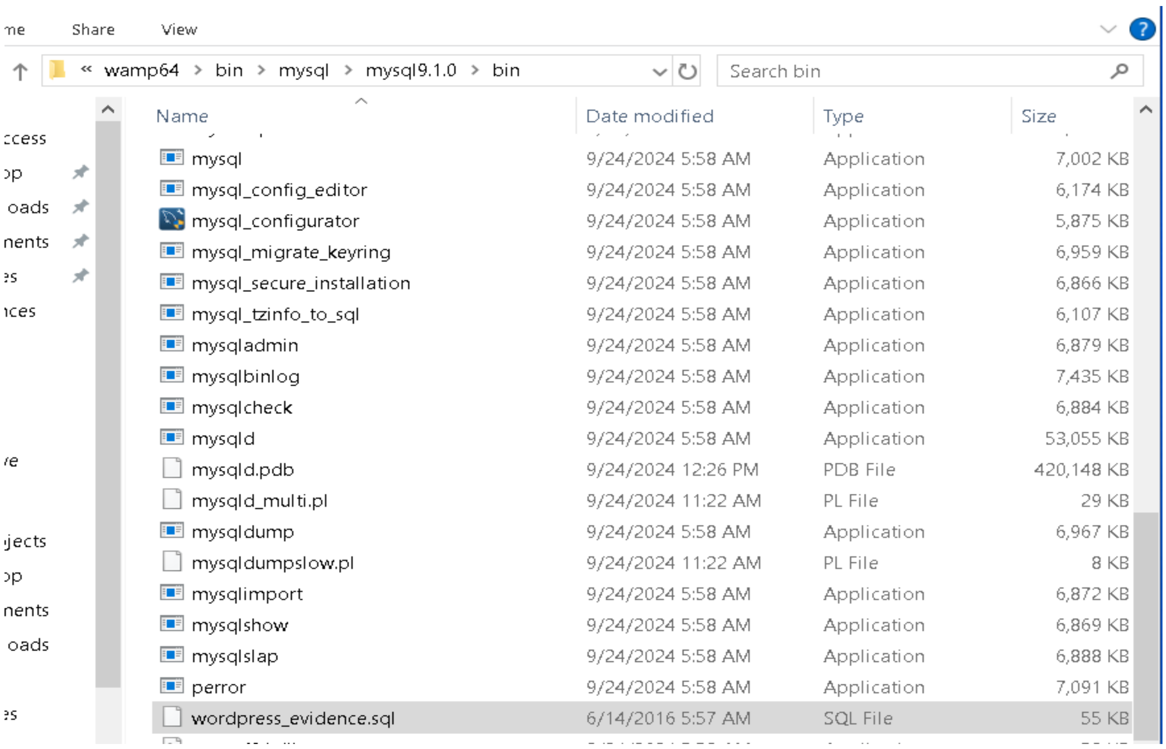
Name	Type	Schema
Tables (3)		
android_metadata		CREATE TABLE android_met
locksettings		CREATE TABLE locksettings
sqlite_sequence		CREATE TABLE sqlite_seque
Indices (0)		
Views (0)		
Triggers (0)		

This way as forensic investigator,we may analyze all the databases that were extracted from the mobile devices.

Lab-03

Performing Forensic Investigation on a MySQL Server Database

Copy the wordpress evidence file to the wampserver bin of sql and open the command prompt in it.



me Share View

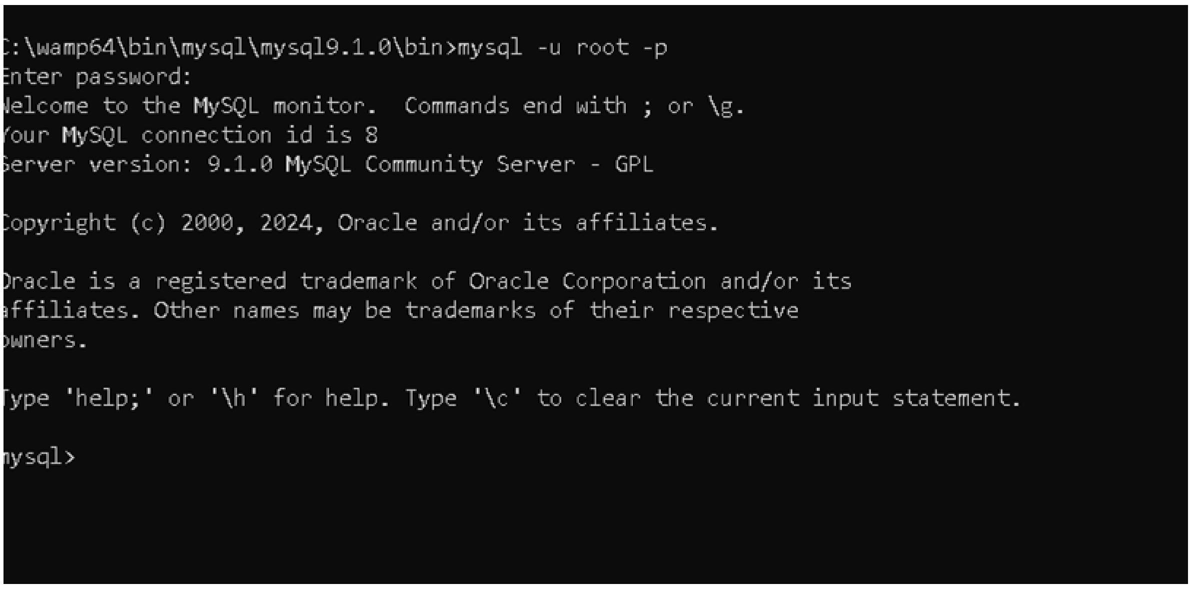
« wamp64 > bin > mysql > mysql9.1.0 > bin

Search bin

ccess
op
oads
nents
es
nces
ve
jects
op
nents
oads
es

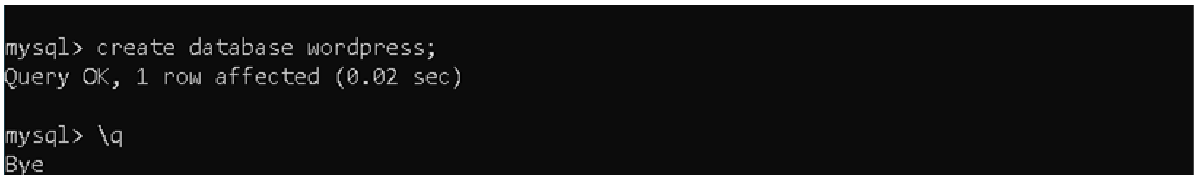
Name	Date modified	Type	Size
mysql	9/24/2024 5:58 AM	Application	7,002 KB
mysql_config_editor	9/24/2024 5:58 AM	Application	6,174 KB
mysql_configurator	9/24/2024 5:58 AM	Application	5,875 KB
mysql_migrate_keyring	9/24/2024 5:58 AM	Application	6,959 KB
mysql_secure_installation	9/24/2024 5:58 AM	Application	6,866 KB
mysql_tzinfo_to_sql	9/24/2024 5:58 AM	Application	6,107 KB
mysqladmin	9/24/2024 5:58 AM	Application	6,879 KB
mysqlbinlog	9/24/2024 5:58 AM	Application	7,435 KB
mysqlcheck	9/24/2024 5:58 AM	Application	6,884 KB
mysqld	9/24/2024 5:58 AM	Application	53,055 KB
mysqld.pdb	9/24/2024 12:26 PM	PDB File	420,148 KB
mysqld_multi.pl	9/24/2024 11:22 AM	PL File	29 KB
mysqldump	9/24/2024 5:58 AM	Application	6,967 KB
mysqldumpslow.pl	9/24/2024 11:22 AM	PL File	8 KB
mysqlimport	9/24/2024 5:58 AM	Application	6,872 KB
mysqlshow	9/24/2024 5:58 AM	Application	6,869 KB
mysqlslap	9/24/2024 5:58 AM	Application	6,888 KB
perror	9/24/2024 5:58 AM	Application	7,091 KB
wordpress_evidence.sql	6/14/2016 5:57 AM	SQL File	55 KB

Command prompt appears .point location on bin folder.



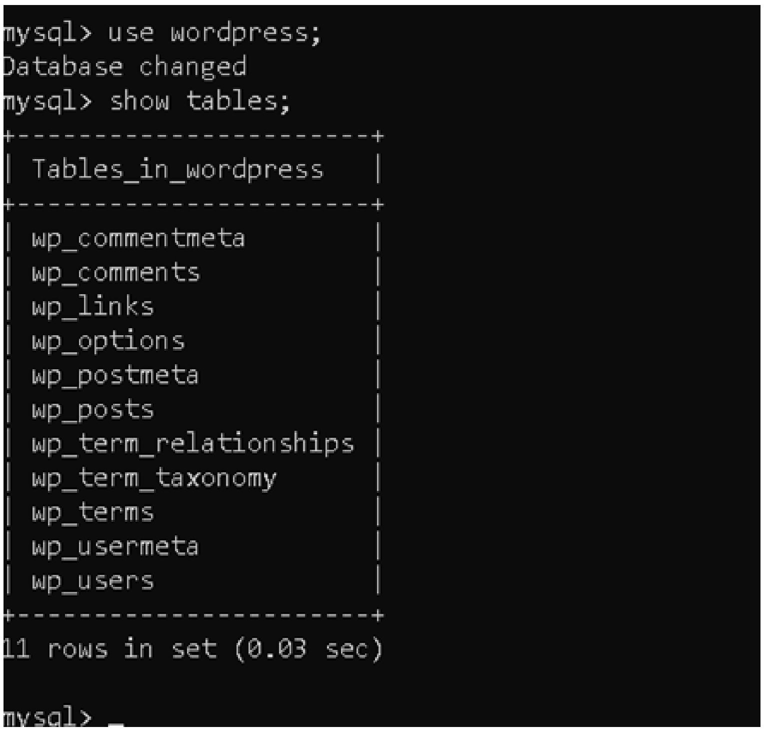
```
:\wamp64\bin\mysql\mysql9.1.0\bin>mysql -u root -p
nter password:
elcome to the MySQL monitor.  Commands end with ; or \g.
our MySQL connection id is 8
erver version: 9.1.0 MySQL Community Server - GPL

opyright (c) 2000, 2024, Oracle and/or its affiliates.

racle is a registered trademark of Oracle Corporation and/or its
ffiliates. Other names may be trademarks of their respective
wners.

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

ysql>
```

Create a databse as wordpress and quit it.



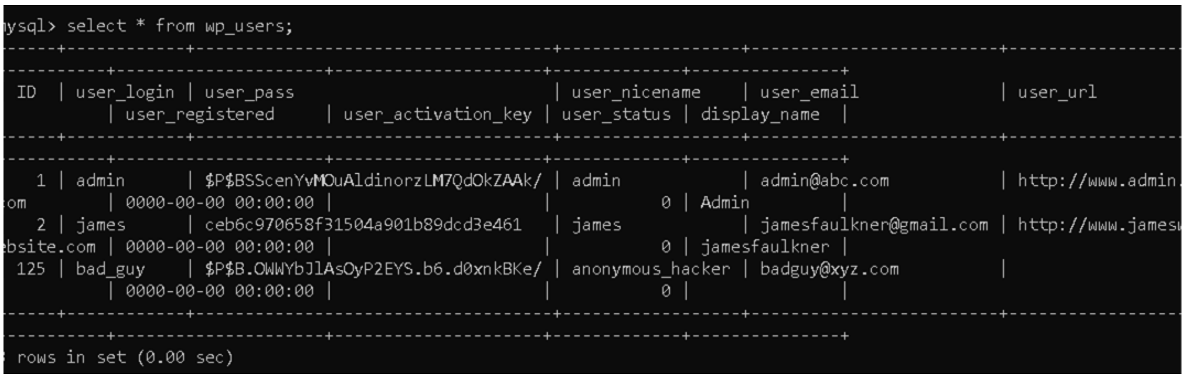
```
mysql> create database wordpress;
Query OK, 1 row affected (0.02 sec)

mysql> \q
Bye
```

Dump the files in the wordpressevidence.sql to wordpress we created database



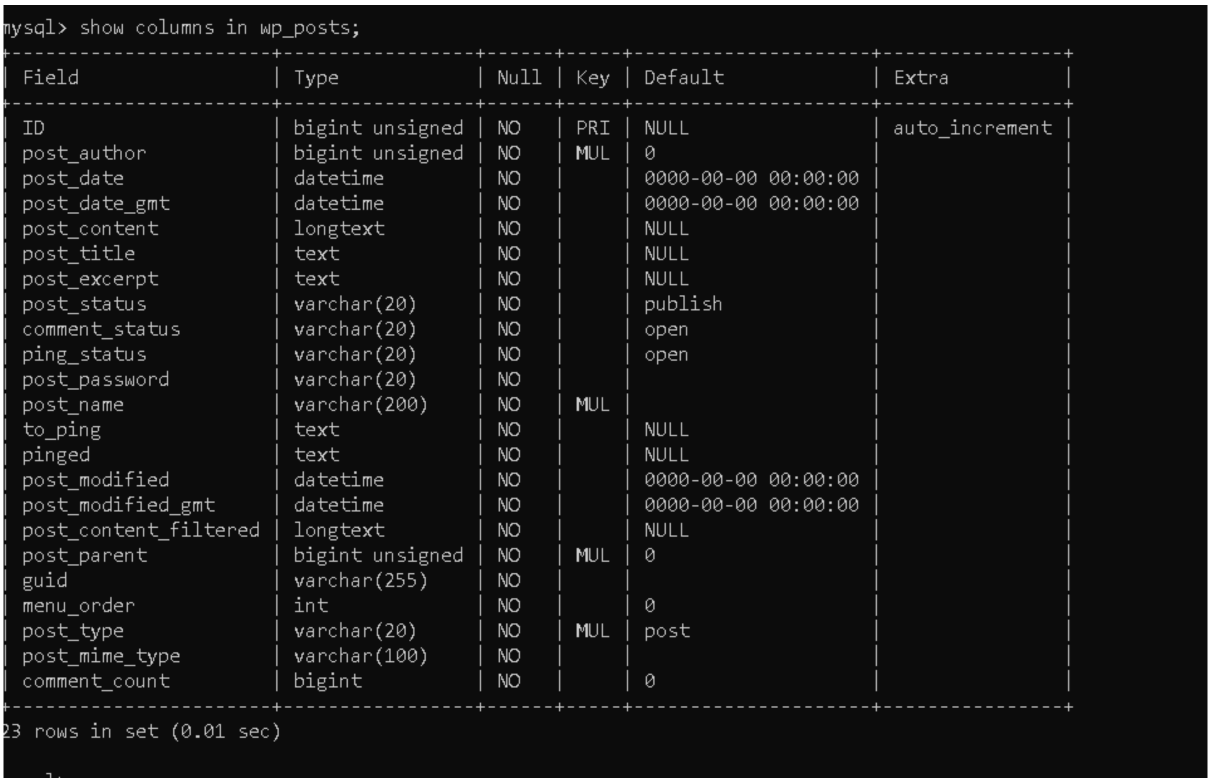
```
ysql> use wordpress;
atabase changed
ysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
11 rows in set (0.03 sec)

ysql> _
```

Enter into the database to see the following tables and we get the details of user byfollowing command.



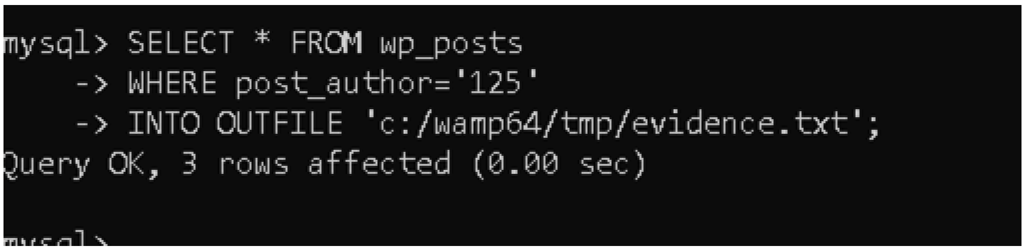
```
ysql> select * from wp_users;
-----+------------+------------------------------------+------------------+-------------------------+------------------
----------+---------------------+---------------------+-------------+--------------+
 ID  | user_login | user_pass                          | user_nicename    | user_email              | user_url
          | user_registered     | user_activation_key | user_status | display_name  |
-----+------------+------------------------------------+------------------+-------------------------+------------------
----------+---------------------+---------------------+-------------+--------------+
   1 | admin      | $P$BSScenYvMOuAldinorzLM7QdOkZAAk/ | admin            | admin@abc.com           | http://www.admin.
om        | 0000-00-00 00:00:00 |                     |           0 | Admin         |
   2 | james      | ceb6c970658f31504a901b89dcd3e461   | james            | jamesfaulkner@gmail.com | http://www.jamesw
bsite.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 |               |
-----+------------+------------------------------------+------------------+-------------------------+------------------
----------+---------------------+---------------------+-------------+--------------+
 rows in set (0.00 sec)
```

It shows the list of users in the table.



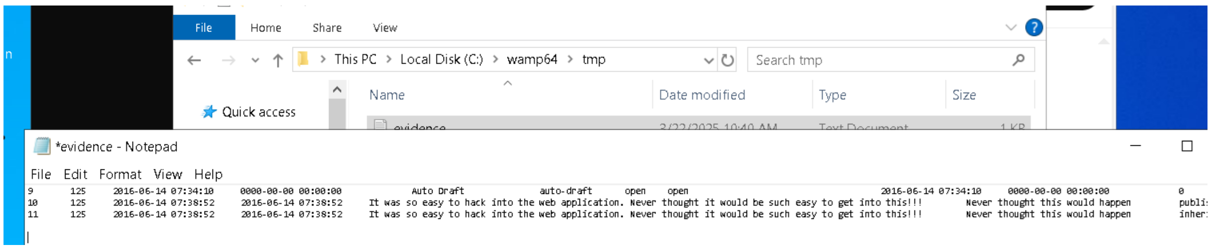
```
ysql> show columns in wp_posts;
+-----------------------+-----------------+------+-----+---------------------+----------------+
| Field                 | Type            | Null | Key | Default             | Extra          |
+-----------------------+-----------------+------+-----+---------------------+----------------+
| 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                   |                |
+-----------------------+-----------------+------+-----+---------------------+----------------+
3 rows in set (0.01 sec)
```

We can see the author and details available



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

Now we stored the details of badguy in evidence.txt



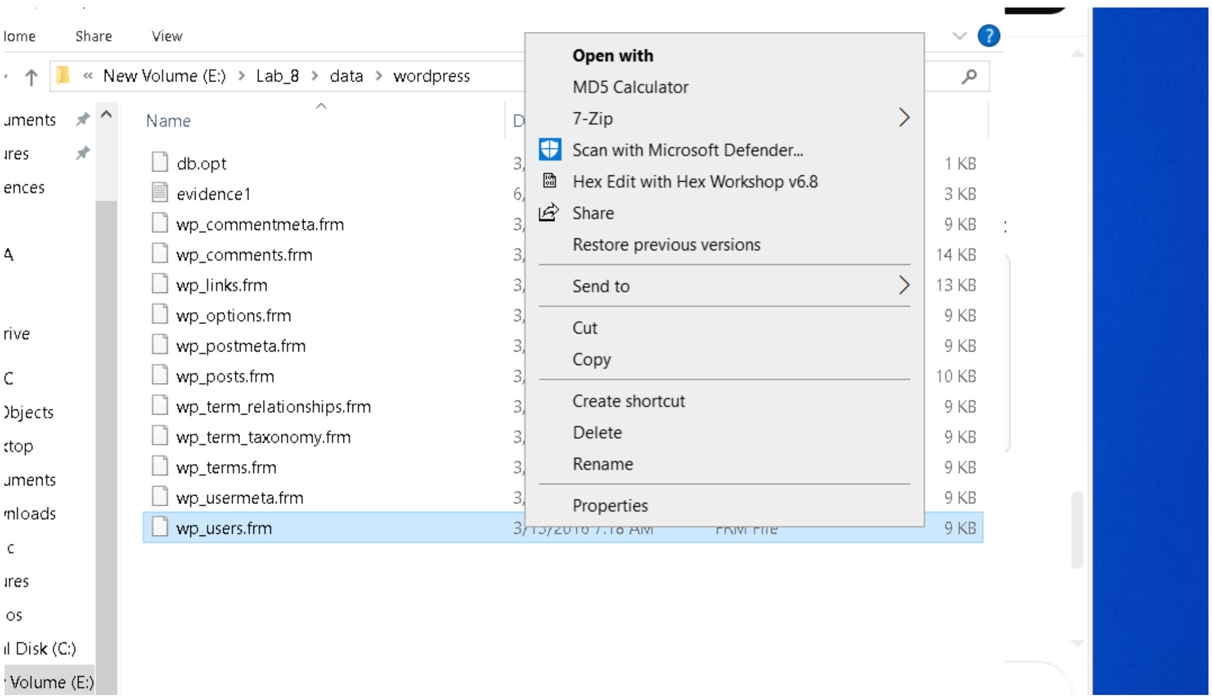
This PC > Local Disk (C:) > wamp64 > tmp

Name	Date modified	Type	Size
evidence	3/22/2025 10:40 AM	Text Document	1 KB

*evidence - Notepad

```
9       125     2016-06-14 07:34:10     0000-00-00 00:00:00             Auto Draft              auto-draft      open    open                            2016-06-14 07:34:10     0000-00-00 00:00:00             0
10      125     2016-06-14 07:38:52     2016-06-14 07:38:52     It was so easy to hack into the web application. Never thought it would be such easy to get into this!!!        Never thought this would happen         publi
11      125     2016-06-14 07:38:52     2016-06-14 07:38:52     It was so easy to hack into the web application. Never thought it would be such easy to get into this!!!        Never thought this would happen         inher
```

Evidence we got is correct

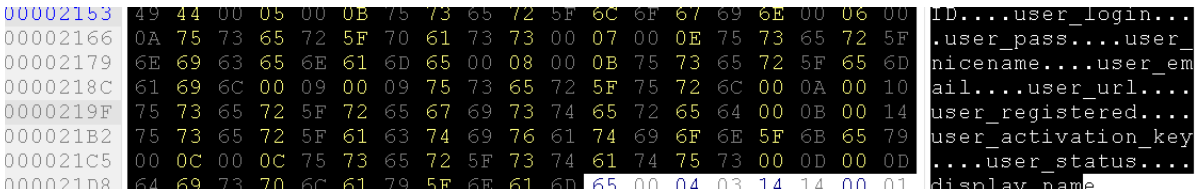


Home
Share
View
New Volume (E:) › Lab_8 › data › wordpress

Name		
db.opt	3	1 KB
evidence1	6	3 KB
wp_commentmeta.frm	3	9 KB
wp_comments.frm	3	14 KB
wp_links.frm	3	13 KB
wp_options.frm	3	9 KB
wp_postmeta.frm	3	9 KB
wp_posts.frm	3	10 KB
wp_term_relationships.frm	3	9 KB
wp_term_taxonomy.frm	3	9 KB
wp_terms.frm	3	9 KB
wp_usermeta.frm	3	9 KB
wp_users.frm	3/15/2016 7:18 AM FRM File	9 KB

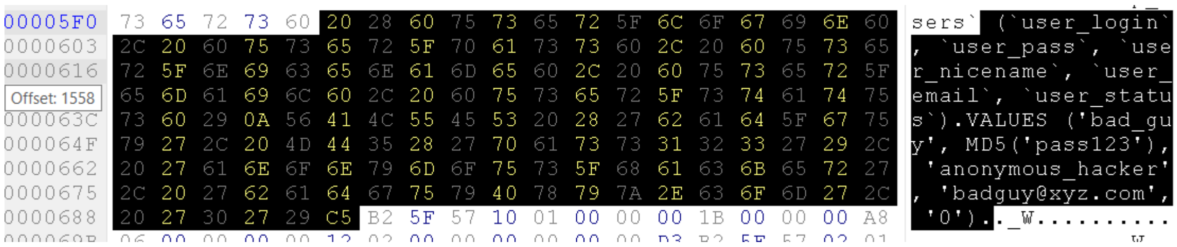
Open with
MD5 Calculator
7-Zip
Scan with Microsoft Defender...
Hex Edit with Hex Workshop v6.8
Share
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties

Using hex editor we can see the binaries of the datbase for the bad guy by the file .frm



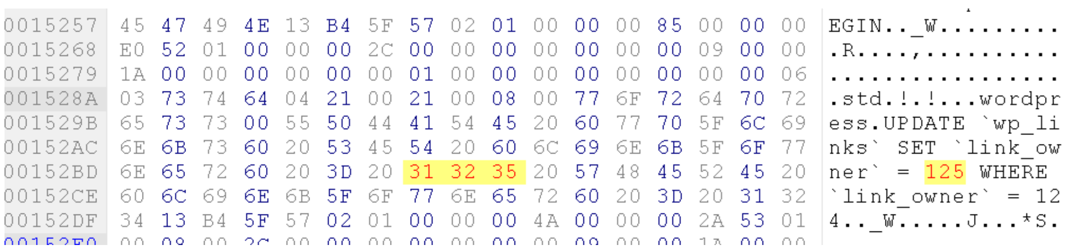
```
00002153  49 44 00 05 00 0B 75 73 65 72 5F 6C 6F 67 69 6E 00 06 00  ID....user_login...
00002166  0A 75 73 65 72 5F 70 61 73 73 00 07 00 0E 75 73 65 72 5F  .user_pass....user_
00002179  6E 69 63 65 6E 61 6D 65 00 08 00 0B 75 73 65 72 5F 65 6D  nicename....user_em
0000218C  61 69 6C 00 09 00 09 75 73 65 72 5F 75 72 6C 00 0A 00 10  ail....user_url....
0000219F  75 73 65 72 5F 72 65 67 69 73 74 65 72 65 64 00 0B 00 14  user_registered....
000021B2  75 73 65 72 5F 61 63 74 69 76 61 74 69 6F 6E 5F 6B 65 79  user_activation_key
000021C5  00 0C 00 0C 75 73 65 72 5F 73 74 61 74 75 73 00 0D 00 0D  ....user_status....
000021D8  64 69 73 70 6C 61 79 5F 6E 61 6D 65 00 04 03 14 14 00 01  display_name
```

we can observe that login names stored under the user login column, by this analysis we go for the log files to verify and get the details

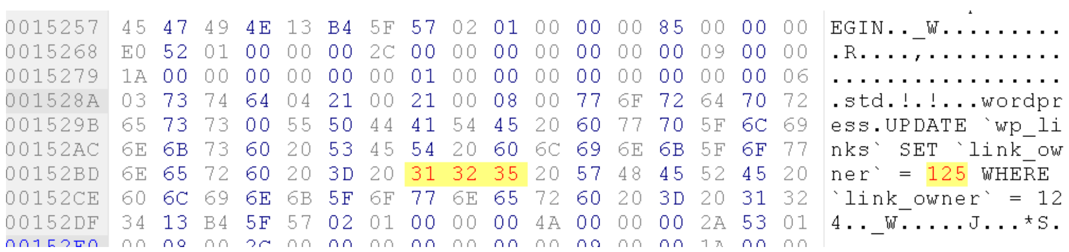


```
00005F0  73 65 72 73 60 20 28 60 75 73 65 72 5F 6C 6F 67 69 6E 60  sers` (`user_login`
0000603  2C 20 60 75 73 65 72 5F 70 61 73 73 60 2C 20 60 75 73 65  , `user_pass`, `use
0000616  72 5F 6E 69 63 65 6E 61 6D 65 60 2C 20 60 75 73 65 72 5F  r_nicename`, `user_
Offset: 1558  65 6D 61 69 6C 60 2C 20 60 75 73 65 72 5F 73 74 61 74 75  email`, `user_statu
000063C  73 60 29 0A 56 41 4C 55 45 53 20 28 27 62 61 64 5F 67 75  s`).VALUES ('bad_gu
000064F  79 27 2C 20 4D 44 35 28 27 70 61 73 73 31 32 33 27 29 2C  y', MD5('pass123'),
0000662  20 27 61 6E 6F 6E 79 6D 6F 75 73 5F 68 61 63 6B 65 72 27   'anonymous_hacker'
0000675  2C 20 27 62 61 64 67 75 79 40 78 79 7A 2E 63 6F 6D 27 2C  , 'badguy@xyz.com',
0000688  20 27 30 27 29 C5 B2 5F 57 10 01 00 00 00 1B 00 00 00 A8   '0')._W.........
000069B  06 00 00 00 00 12 02 00 00 00 00 00 00 D3 B2 5F 57 02 01
```

By the analysis we can get the user name and password used by the attacker.



```
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 09 00 00  .R....,..........
0015279  1A 00 00 00 00 00 00 01 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.
00152F0  00 08 00 2C 00 00 00 00 00 00 00 09 00 00 1A 00 00
```



```
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 ctrl+f we can search based text or hex criteria to analyse, now I searched for 125 and got the query of update by badguy