

SQLITE BROWSER GUIDED EXERCISE

Video walkthrough available on the Tool Walkthrough Playlist at <https://youtube.com/@hexordia>

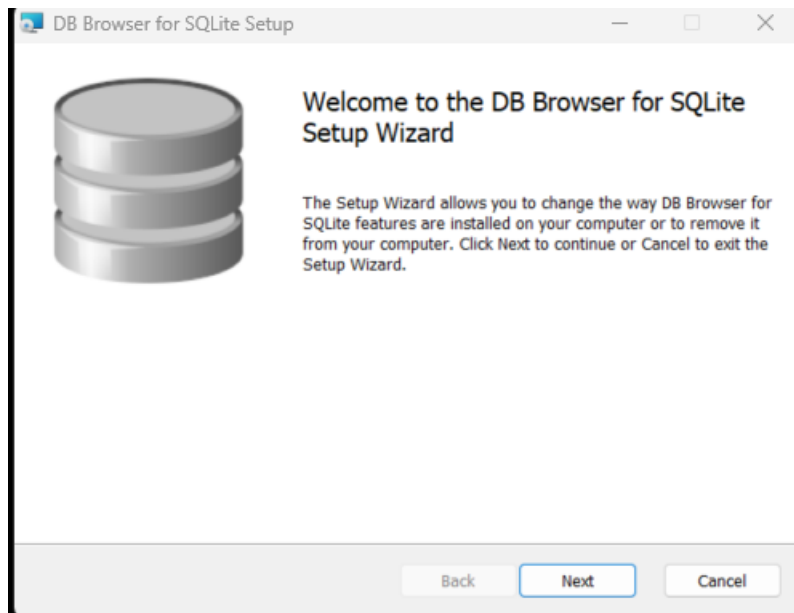
To start, please download SQLite Browser from: <https://sqlitebrowser.org/dl/>

Prior to installation, verify the hash value to the known good from the syllabus for students enrolled in the HMFA Virtual Live course. The MD5 hash value for the DB.Browser.for.SQLite-3.12.2-win64.msi version 3.12.2 is f7f7264820a5acbe199f8caf92ea9c4c. Please note, Windows Defender may flag this file, if the hash matches, you should be good to proceed and install using the SQLite Setup Wizard.

At the site listed above, select which OS and what version. The below walkthrough will show Standard installer for 64-bit Windows.

**If you already have SQLite Browser Installed, please move on to [Set Up and Use](#).

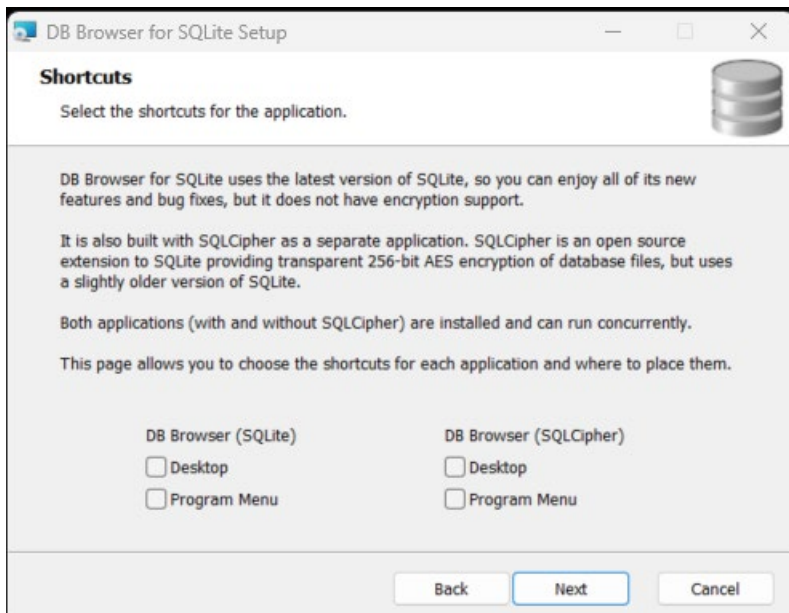
INSTALLATION:



Select "Next".

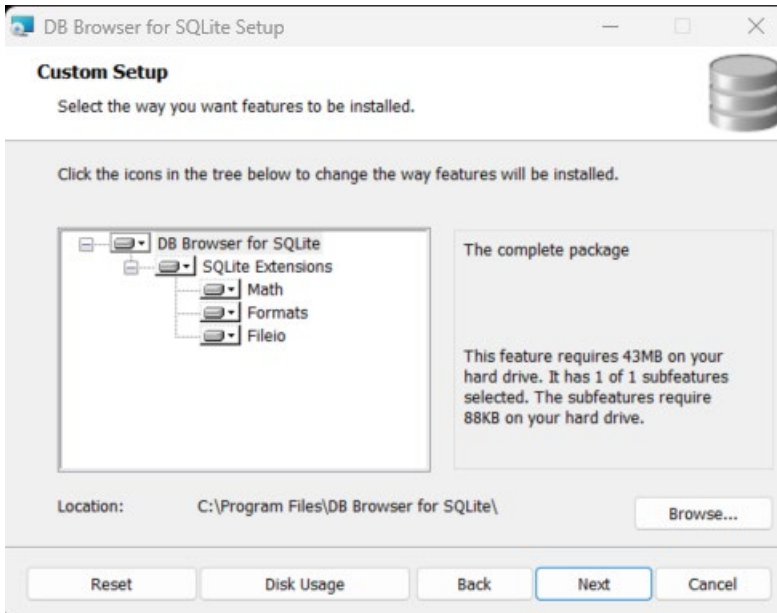


Accept the terms and click “next”.

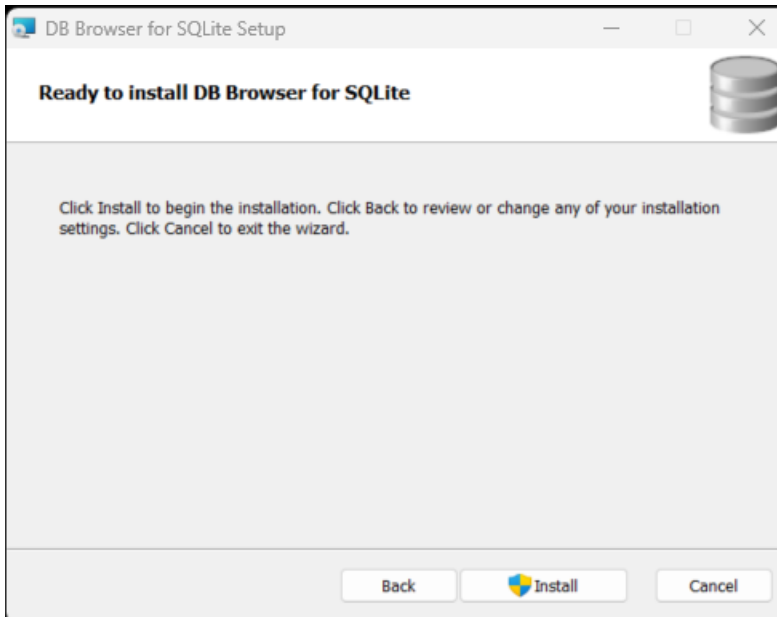


Select the shortcuts of your choice and click “next.”



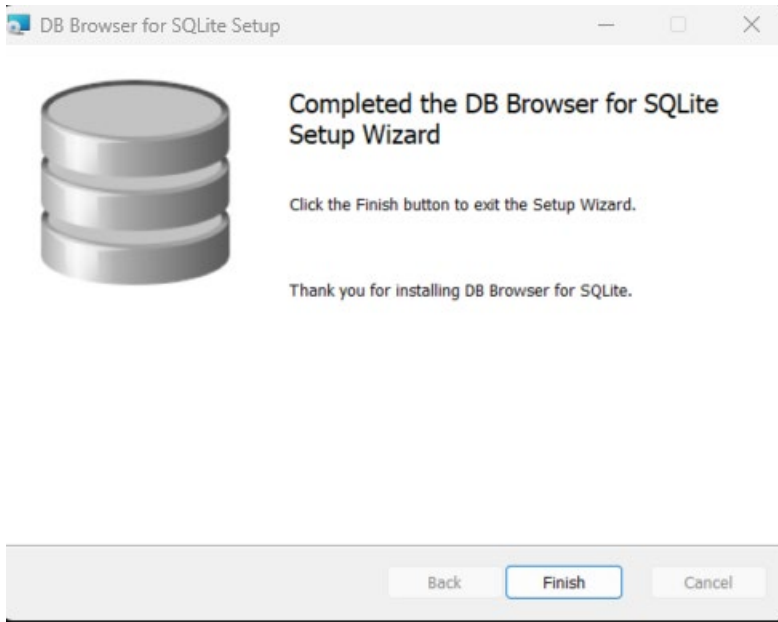


Here are disk usage and change location if necessary. Once done, select “next.”



Select “install”. Here there may be a User Control Account pop-up. If “no” is selected the installation will discontinue. If “yes” is selected, the installation will continue.





Select "finish".



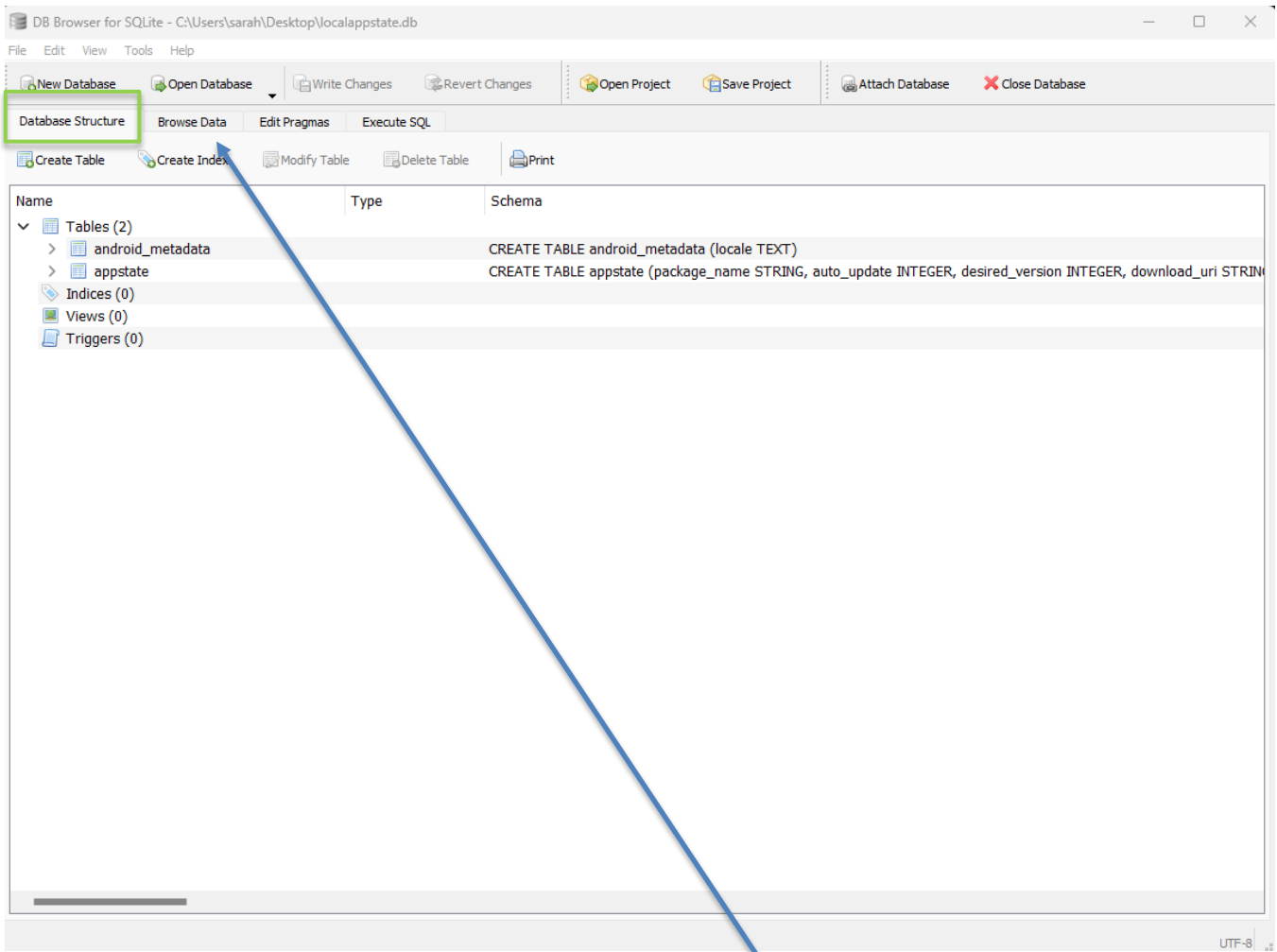


SET UP AND USE

For the purpose of this course, we will open a database that was pulled from Autopsy.

Select “Open Database” and navigate to (the selected file) and select “open”.

The first tab is the Database Structure:

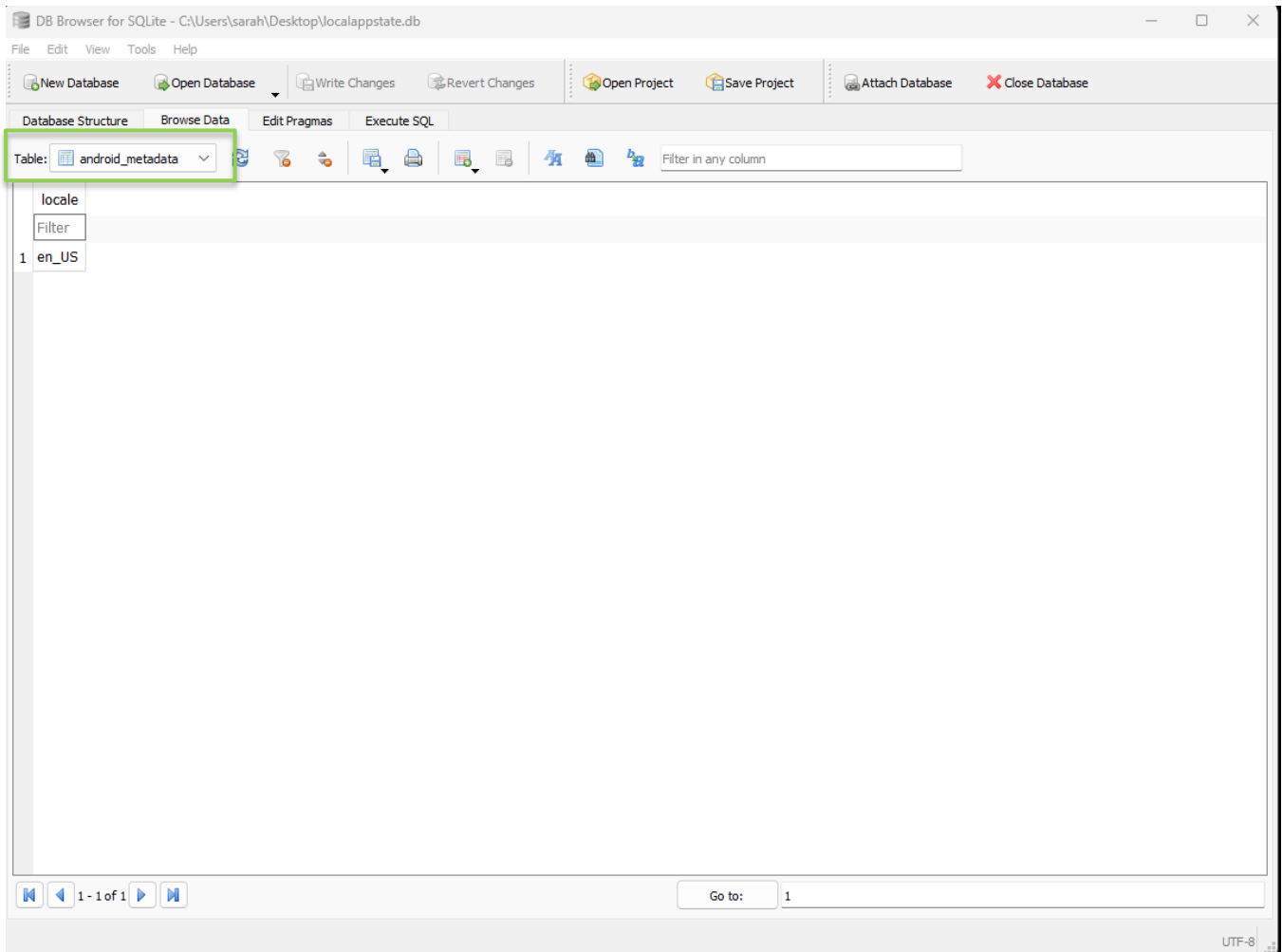


Again, for the purpose of this course we are going to use browse data.





In this view, there is a table with a drop down for options.



Select “apppstate” which will provide data.





In the table view there are various packages, and options for data.

	package_name	auto_update	desired_version	download_uri	delivery_data
	Filter	Filter	Filter	Filter	Filter
1	com.google.android.apps.pixelmigrate	1	-1	NULL	BLOB
2	android.autoinstalls.config.google.nexus	1	-1	NULL	BLOB
3	com.google.android.apps.youtube.music	1	-1	NULL	NULL
4	com.google.android.apps.magazines	1	-1	NULL	NULL
5	com.google.android.apps.docs.editors.docs	1	-1	NULL	NULL
6	com.google.android.apps.tachyon	1	-1	NULL	NULL
7	com.google.android.apps.podcasts	1	-1	NULL	BLOB
8	com.google.android.apps.turbo	1	-1	NULL	BLOB
9	com.google.android.GoogleCamera	1	-1	NULL	BLOB
10	com.google.android.apps.wellbeing	1	-1	NULL	BLOB
11	com.google.android.apps.dreamliner	1	-1	NULL	BLOB
12	com.google.android.keep	1	-1	NULL	BLOB
13	com.tencent.mm	1	-1	NULL	BLOB
14	com.google.ar.core	1	-1	NULL	BLOB
15	com.google.vr.vrcore	1	-1	NULL	BLOB
16	com.google.android.soundpicker	1	-1	NULL	BLOB
17	com.google.android.settings.intelligence	1	-1	NULL	BLOB
18	com.google.android.apps.helptrc	1	-1	NULL	BLOB
19	org.thoughtcrime.securesms	1	-1	NULL	BLOB
20	com.google.android.apps.walletnfcrel	1	-1	NULL	BLOB
21	com.google.android.as	1	-1	NULL	BLOB
22	com.google.android.tts	1	-1	NULL	BLOB
23	com.snapchat.android	1	-1	NULL	BLOB
24	com.twitter.android	1	-1	NULL	BLOB
25	com.google.android.euicc	1	-1	NULL	BLOB

If there is a BLOB there is different data available.

Double click the “BLOB”, this can be viewed in a pop out or can view it right in the browser (just move over the file).





File Edit View Tools Help

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

Database Structure Browse Data Edit Pragmas Execute SQL Edit Database Cell

Table: items Filter in any column Mode: Binary

row_id	server_perm_id	item_summary_proto	recurrence_id	hidden	write_sec
1	thread-f:1722965523609767320	BLOB	NULL	0	
2	thread-f:1722965453747558581	BLOB	NULL	0	
3	thread-f:1722965629921835925	BLOB	NULL	0	
4	thread-f:1721245532971274687	BLOB	NULL	0	
5	thread-f:1722967067257735742	BLOB	NULL	0	
6	thread-f:1723255926736375964	BLOB	NULL	0	

```

0000 0a 8c 01 0a 1c 74 68 72 65 61 64 2d 66 3a 31 37 .....thread-f:17
0010 32 32 39 36 35 35 32 33 36 30 39 37 36 37 33 32 2296552360976732
0020 30 12 55 52 61 66 61 65 6c 2c 20 74 61 6b 65 20 0U Rafael, take
0030 74 68 65 20 6e 65 78 74 20 73 74 65 70 20 6f 6e the next step on
0040 20 79 6f 75 72 20 57 69 6e 64 6f 77 73 20 62 79 your Windows by
0050 20 63 6f 6e 66 69 72 6d 69 6e 67 20 79 6f 75 72 confirming your
0060 20 47 6f 6f 67 6c 65 20 41 63 63 6f 75 6e 74 20 Google Account
0070 73 65 74 74 69 6e 67 73 20 ea fa 80 9a e9 2f 55 settings ...../U
0080 be 3d f6 3e 68 00 71 98 4d 01 db 03 34 e9 17 12 .=.>h.q.M...4...
0090 80 04 0a 19 6d 73 67 2d 66 3a 31 37 32 32 39 36 ...msg-f:172296
00a0 35 35 32 33 36 30 39 37 36 37 33 32 30 12 2e 08 5523609767320...

```

This mode can be changed if necessary, however for this course binary will primarily be used. Depending on the database selected there may be able to see data such as email context (as shown above).

