SQLite Browser Guided Exercise

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

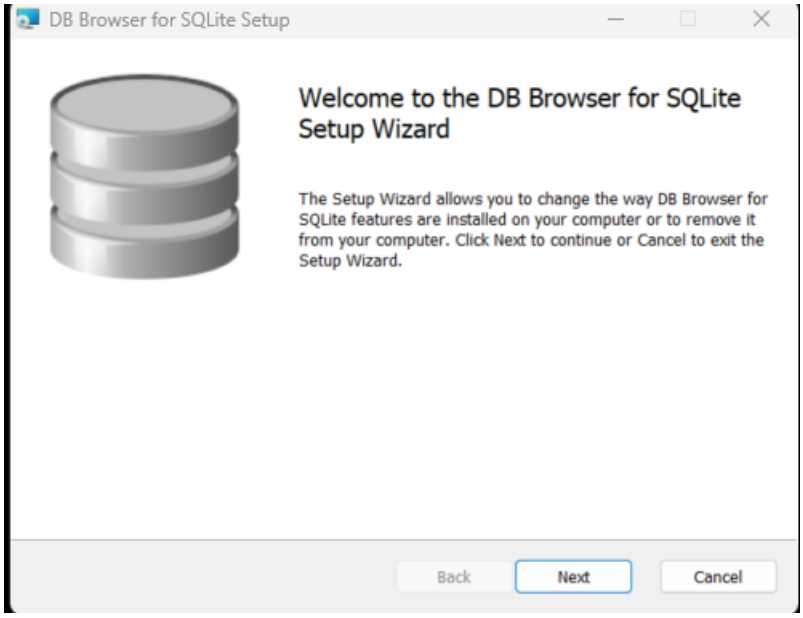
To start, please download SQLite Browser from: https://sqlitebrowser.org/dl/

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.

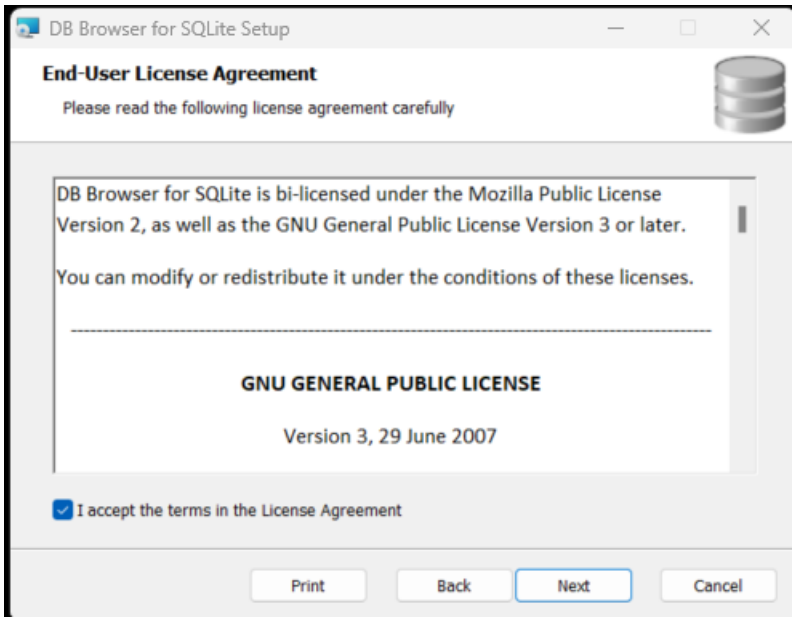
**If you already have SQLite Browser Installed, please move on to Set Up and Use.

Installation:

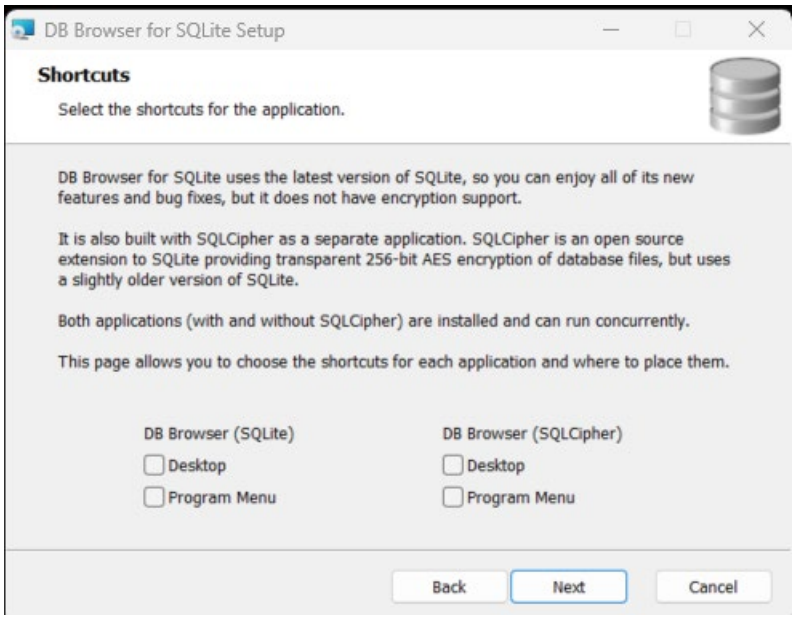


Select “Next”.

© Hexordia| ALL RIGHTS RESERVED

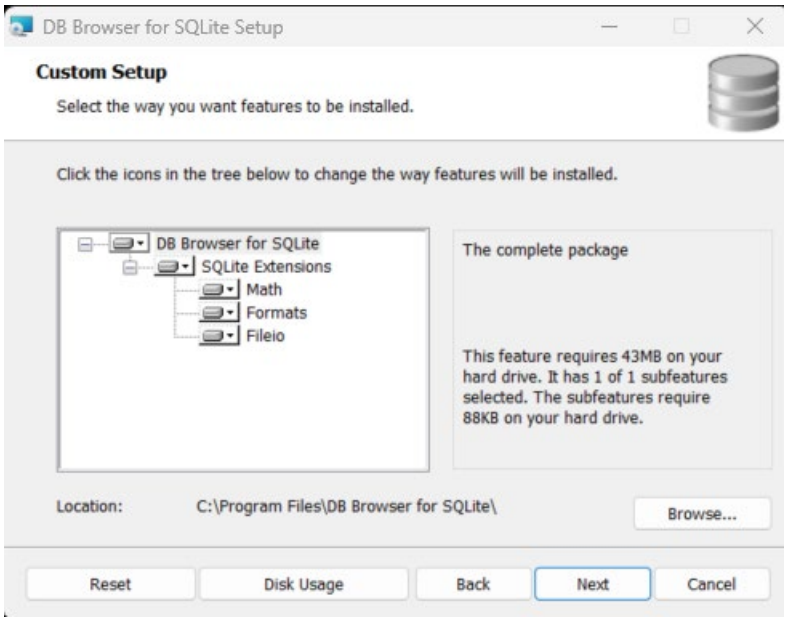


Accept the terms and click “next”.

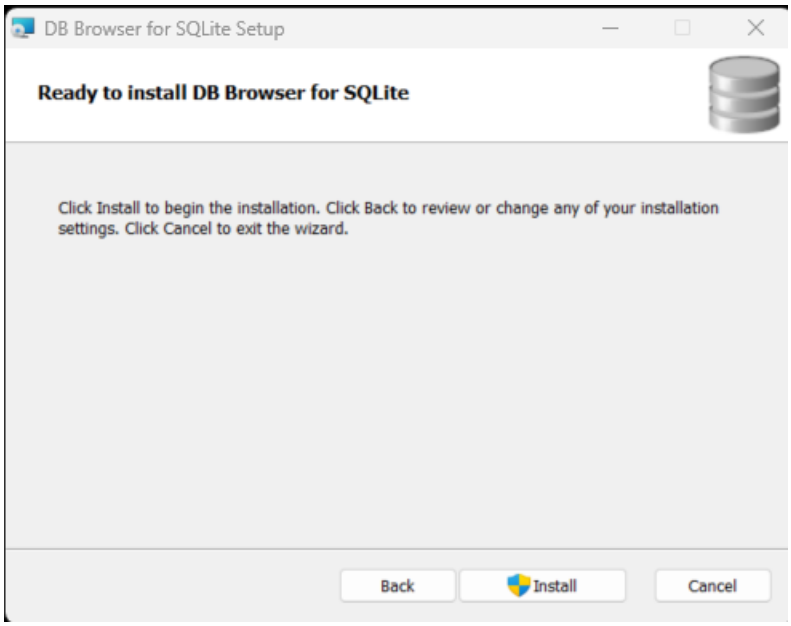


Select the shortcuts of your choice and click “next.”

© HEXORDIA| ALL RIGHTS RESERVED

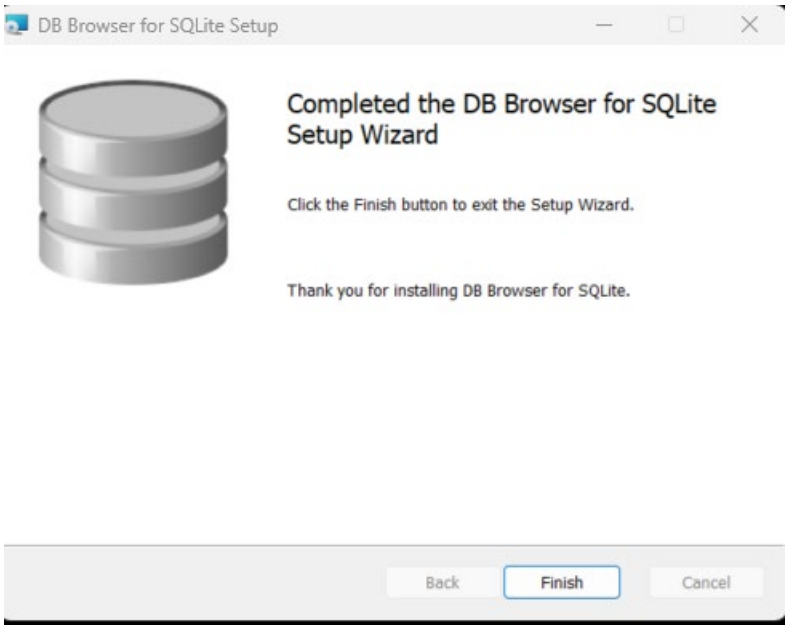


Here are disk usage and change location if necessary. Once done, select “next.”



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.

© HEXORDIA| ALL RIGHTS RESERVED



Select “finish”.

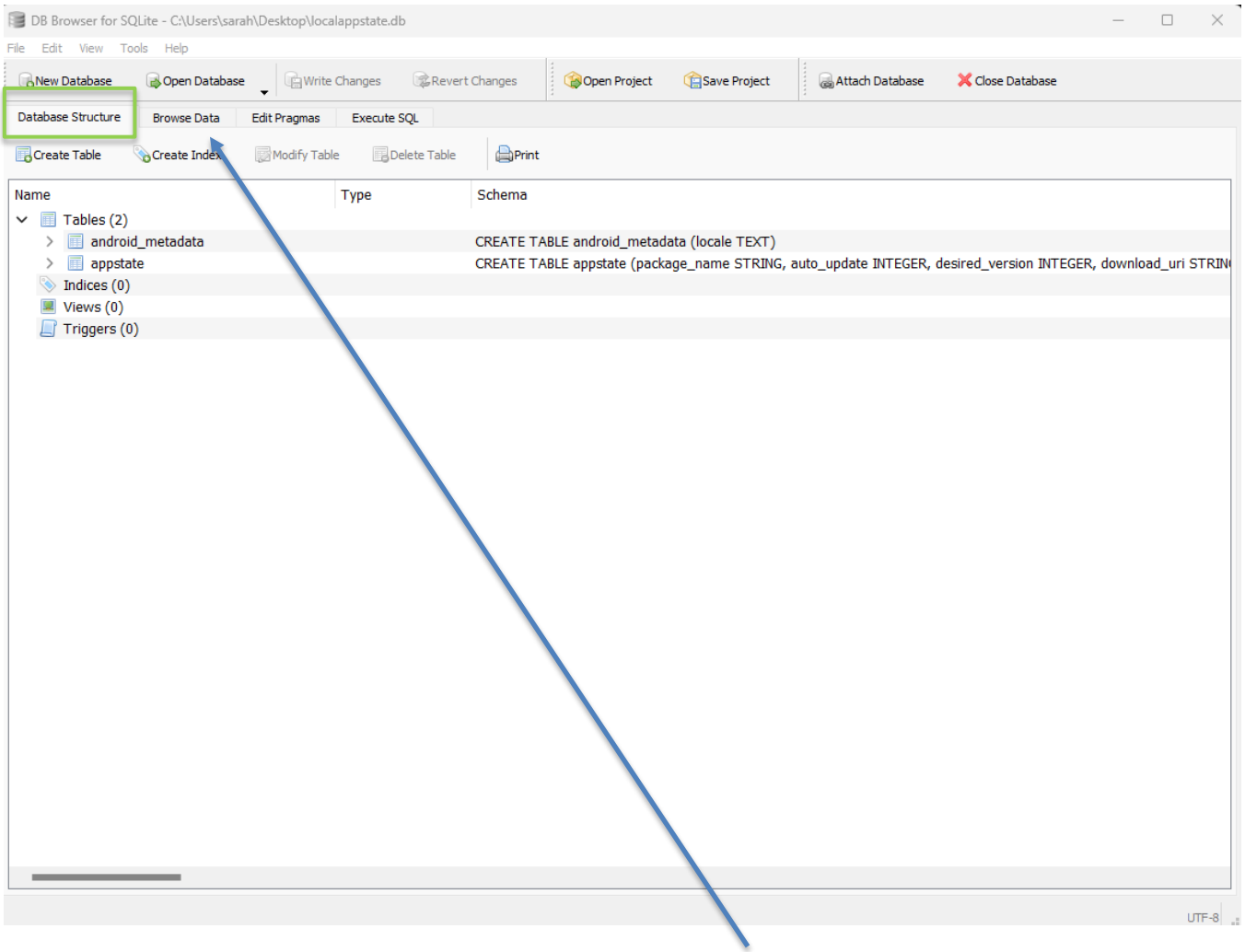
© HEXORDIA| ALL RIGHTS RESERVED

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”.

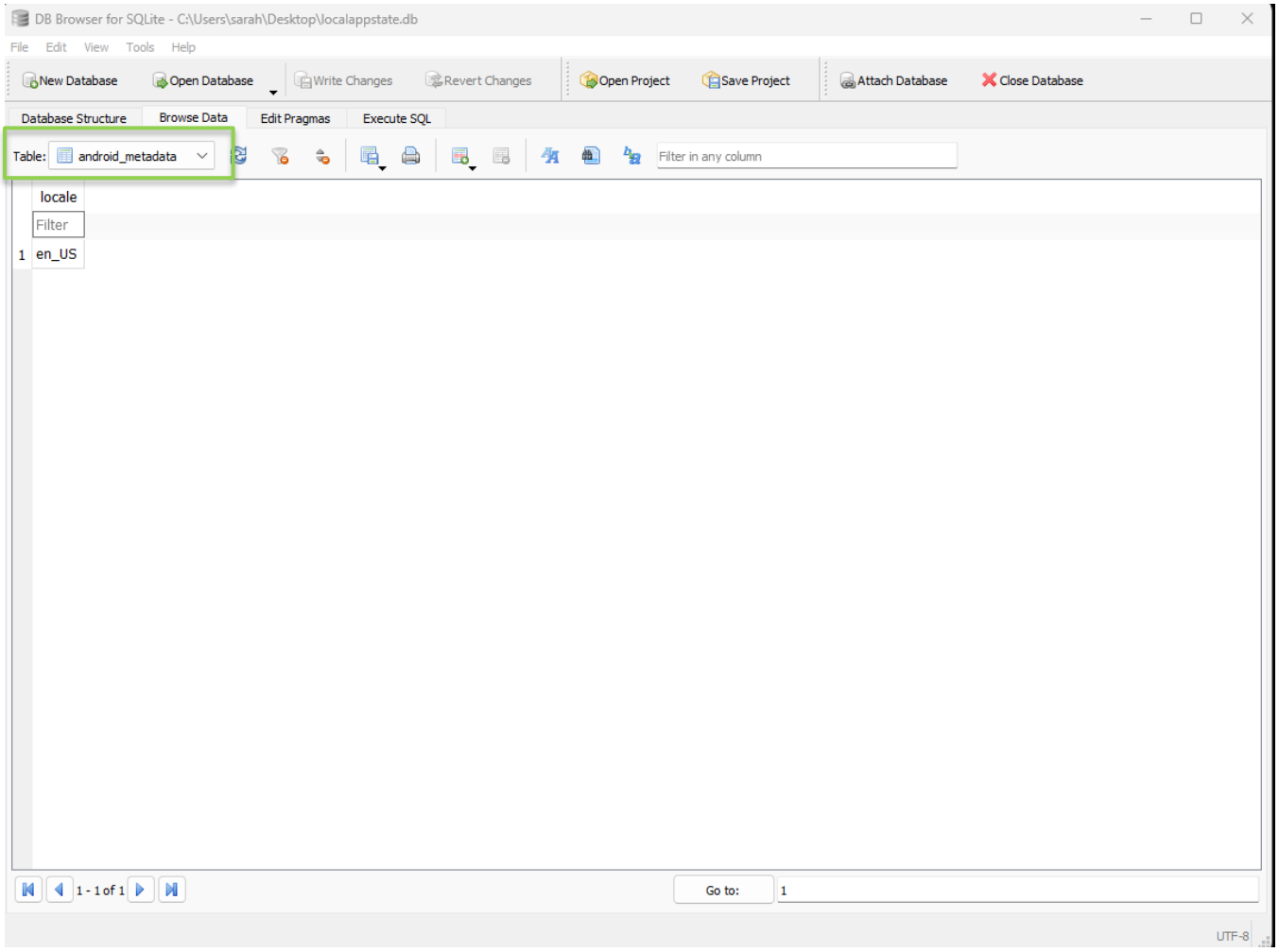
The first tab is the Database Structure:



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

© Hexordia| ALL RIGHTS RESERVED

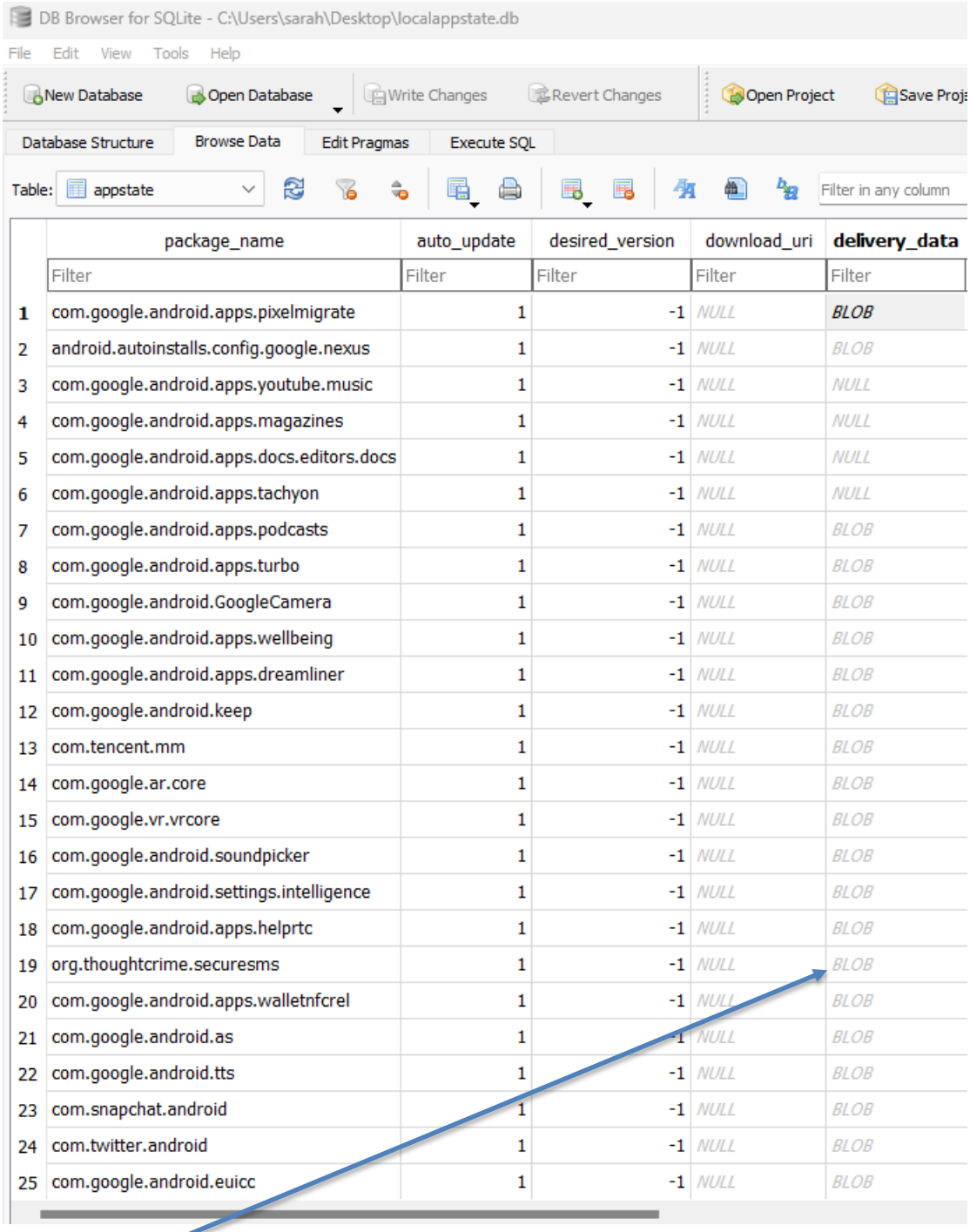
In this view, there is a table with a drop down for options.



Select “appstate” which will provide data.

© HEXORDIA| ALL RIGHTS RESERVED

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

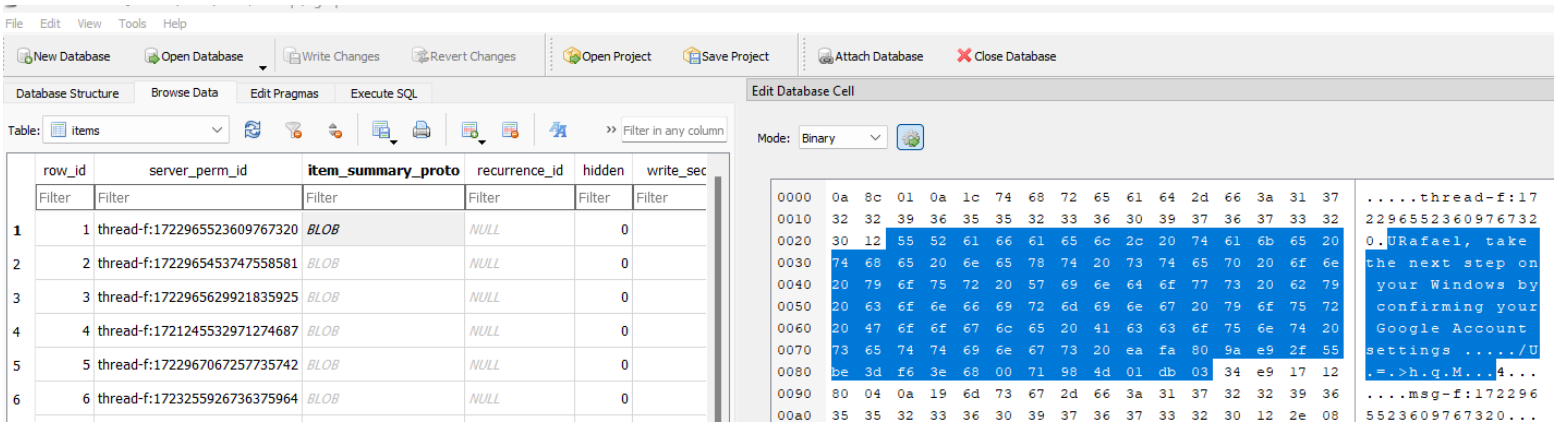


	package_name	auto_update	desired_version	download_uri	delivery_data
	Filter	Filter	Filter	Filter	Filter
1	com.google.android.apps.pixelmigrate	1	-1	NULL	BLOB
2	android.autoinstalls.config.google.nexus	1	-1	NULL	BLOB
3	com.google.android.apps.youtube.music	1	-1	NULL	NULL
4	com.google.android.apps.magazines	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.helprtc	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).

© HEXORDIA| ALL RIGHTS RESERVED



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).

© HEXORDIA| ALL RIGHTS RESERVED