

HOW TO USE SQLITE WALKER

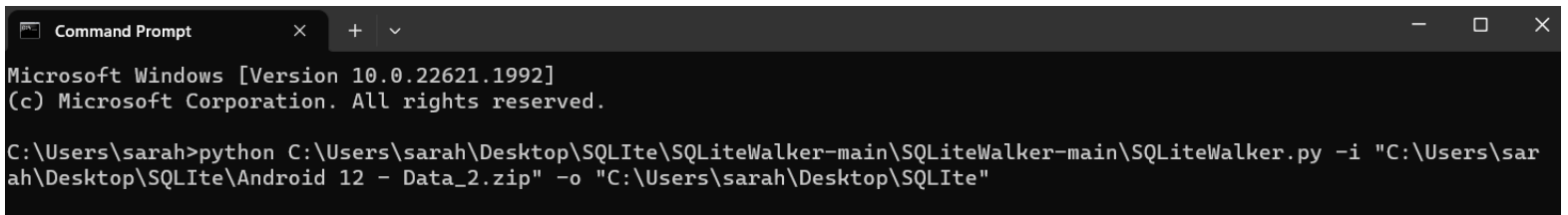
Obtain download from <https://github.com/stark4n6/SQLiteWalker>.

Once the file is downloaded, extract the file. For instructions on this please review 7-zip guided exercise found here [7-Zip](#).

**Of note, the image that is being searched for databases must be in a zipped state.

Open Command Prompt and run command: **python <insert path for SQLiteWalker.py> -i <insert path for image -o <insert path for output>**

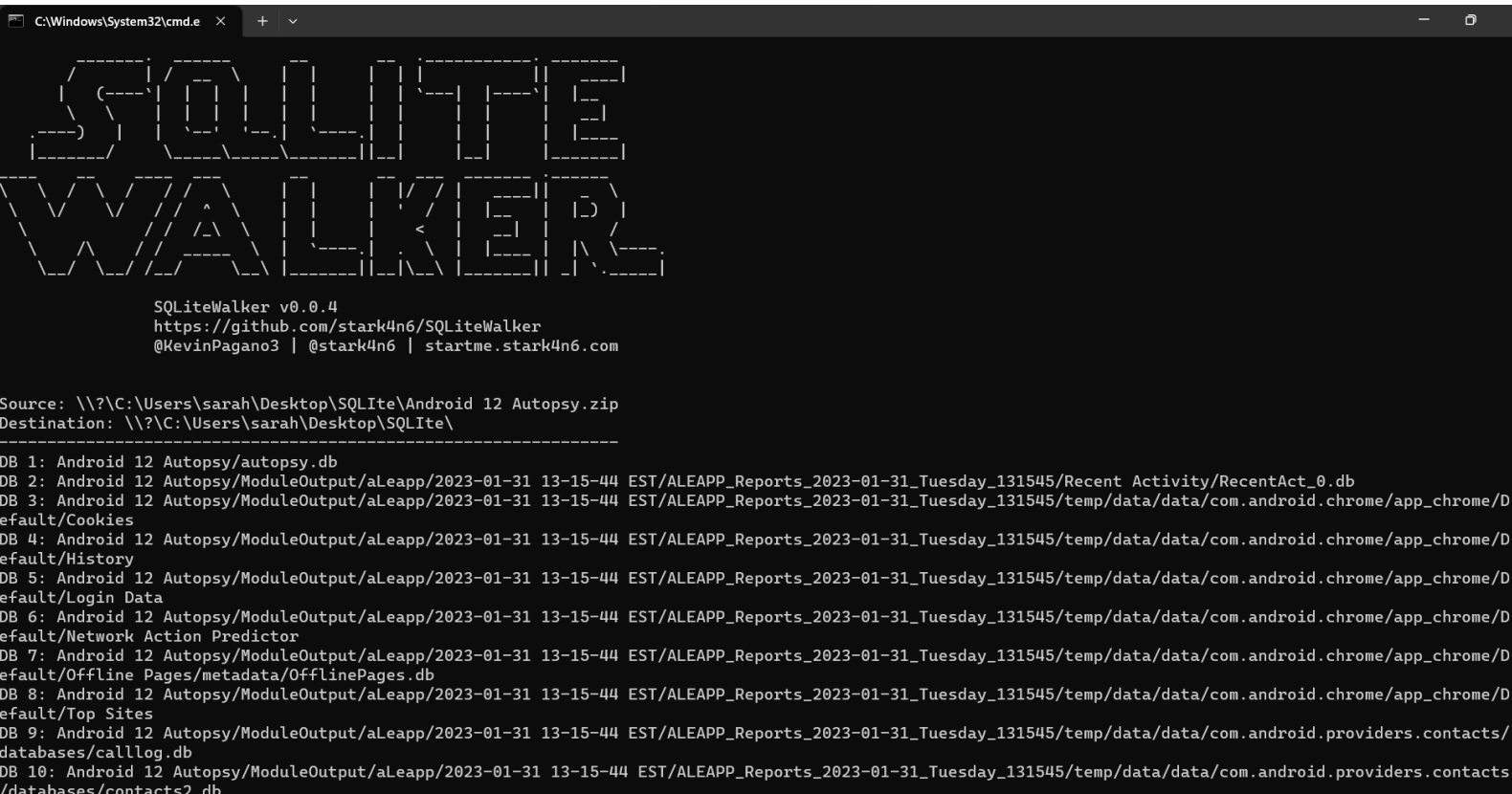
Example: `python "C:\Users\sarah\Downloads\SQLiteWalker.py" -i "D:\Archive\Android 12\Android 12 Autopsy.zip" -o "C:\Users\sarah\Desktop\SQLite"`



```
Command Prompt
Microsoft Windows [Version 10.0.22621.1992]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sarah>python C:\Users\sarah\Desktop\SQLite\SQLiteWalker-main\SQLiteWalker-main\SQLiteWalker.py -i "C:\Users\sarah\Desktop\SQLite\Android 12 - Data_2.zip" -o "C:\Users\sarah\Desktop\SQLite"
```

Example of SQLiteWalker running



```
C:\Windows\System32\cmd.e x
SQLiteWalker v0.0.4
https://github.com/stark4n6/SQLiteWalker
@KevinPagano3 | @stark4n6 | startme.stark4n6.com

Source: \\?\C:\Users\sarah\Desktop\SQLite\Android 12 Autopsy.zip
Destination: \\?\C:\Users\sarah\Desktop\SQLite\
-----
DB 1: Android 12 Autopsy/autopsy.db
DB 2: Android 12 Autopsy/ModuleOutput/aLeapp/2023-01-31 13-15-44 EST/ALEAPP_Reports_2023-01-31_Tuesday_131545/Recent Activity/RecentAct_0.db
DB 3: Android 12 Autopsy/ModuleOutput/aLeapp/2023-01-31 13-15-44 EST/ALEAPP_Reports_2023-01-31_Tuesday_131545/temp/data/data/com.android.chrome/app_chrome/Default/Cookies
DB 4: Android 12 Autopsy/ModuleOutput/aLeapp/2023-01-31 13-15-44 EST/ALEAPP_Reports_2023-01-31_Tuesday_131545/temp/data/data/com.android.chrome/app_chrome/Default/History
DB 5: Android 12 Autopsy/ModuleOutput/aLeapp/2023-01-31 13-15-44 EST/ALEAPP_Reports_2023-01-31_Tuesday_131545/temp/data/data/com.android.chrome/app_chrome/Default/Login Data
DB 6: Android 12 Autopsy/ModuleOutput/aLeapp/2023-01-31 13-15-44 EST/ALEAPP_Reports_2023-01-31_Tuesday_131545/temp/data/data/com.android.chrome/app_chrome/Default/Network Action Predictor
DB 7: Android 12 Autopsy/ModuleOutput/aLeapp/2023-01-31 13-15-44 EST/ALEAPP_Reports_2023-01-31_Tuesday_131545/temp/data/data/com.android.chrome/app_chrome/Default/Offline Pages/metadata/OfflinePages.db
DB 8: Android 12 Autopsy/ModuleOutput/aLeapp/2023-01-31 13-15-44 EST/ALEAPP_Reports_2023-01-31_Tuesday_131545/temp/data/data/com.android.chrome/app_chrome/Default/Top Sites
DB 9: Android 12 Autopsy/ModuleOutput/aLeapp/2023-01-31 13-15-44 EST/ALEAPP_Reports_2023-01-31_Tuesday_131545/temp/data/data/com.android.providers.contacts/databases/calllog.db
DB 10: Android 12 Autopsy/ModuleOutput/aLeapp/2023-01-31 13-15-44 EST/ALEAPP_Reports_2023-01-31_Tuesday_131545/temp/data/data/com.android.providers.contacts/databases/contacts2.db
```

MOBILE FORENSICS

```
****JOB FINISHED****  
Runtime: 21.985103845596313 seconds  
DBs Found: 188  
Error Count: 0
```

Navigate to the output folder. Within this folder, there will be a folder named "SQLiteWalker_OUT"

Folder path: Desktop > SQLite

Name	Date modified
SQLiteWalker_Out_20230725-154117	7/25/2023 3:41 PM
Android 12 Autopsy.zip	5/9/2023 8:09 AM

Within the db_list.tsv file, there will be a list of the databases found. This can be opened with tools like notepad++ and sublime.

Folder path: Desktop > SQLite > SQLiteWalker_Out_20230725-154117

Name	Date modified	Type
db_out	7/25/2023 3:41 PM	File folder
db_list.tsv	7/25/2023 3:41 PM	TSV File

MOBILE FORENSICS

db_list.tsv output example.

```
C:\Users\sarah\Desktop\SQLite\SQLiteWalker_Out_20230725-154117\db_list.tsv - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
db_list.tsv x
1 File Name Export Path Tables
2 autopsy.db
C:\Users\sarah\Desktop\SQLite\SQLiteWalker_Out_20230725-154117\db_out\Android 12
Autopsy\autopsy.db ['tsk_db_info', 'tsk_db_info_extended', 'tsk_objects',
'tsk_persons', 'tsk_hosts', 'tsk_host_addresses', 'tsk_host_address_map',
'tsk_host_address_dns_ip_map', 'tsk_host_address_usage', 'account_types',
'accounts', 'account_relationships', 'tsk_os_account_realms', 'tsk_os_accounts',
'tsk_image_info', 'tsk_image_names', 'tsk_vs_info', 'tsk_vs_parts',
'tsk_pool_info', 'data_source_info', 'tsk_fs_info', 'tsk_files',
'file_encoding_types', 'tsk_files_path', 'tsk_files_derived',
'tsk_files_derived_method', 'tsk_file_layout', 'reports',
'blackboard_artifact_types', 'blackboard_attribute_types', 'review_statuses',
'blackboard_artifacts', 'blackboard_attributes', 'tsk_analysis_results',
'tsk_aggregate_score', 'tsk_tag_sets', 'tag_names', 'tsk_examiners',
'content_tags', 'blackboard_artifact_tags', 'ingest_module_types',
'ingest_job_status_types', 'ingest_modules', 'ingest_jobs', 'ingest_job_modules',
'tsk_event_types', 'tsk_event_descriptions', 'tsk_events', 'tsk_file_attributes',
'tsk_os_account_attributes', 'tsk_os_account_instances', 'tsk_data_artifacts',
'image_gallery_db_info', 'image_gallery_groups', 'image_gallery_groups_seen',
'beta_tag_app_data']
3 RecentAct_0.db
C:\Users\sarah\Desktop\SQLite\SQLiteWalker_Out_20230725-154117\db_out\Android 12
Autopsy\ModuleOutput\aleapp\2023-01-31 13-15-44
EST\ALEAPP_Reports_2023-01-31_Tuesday_131545\Recent Activity\RecentAct_0.db
['recent']
```

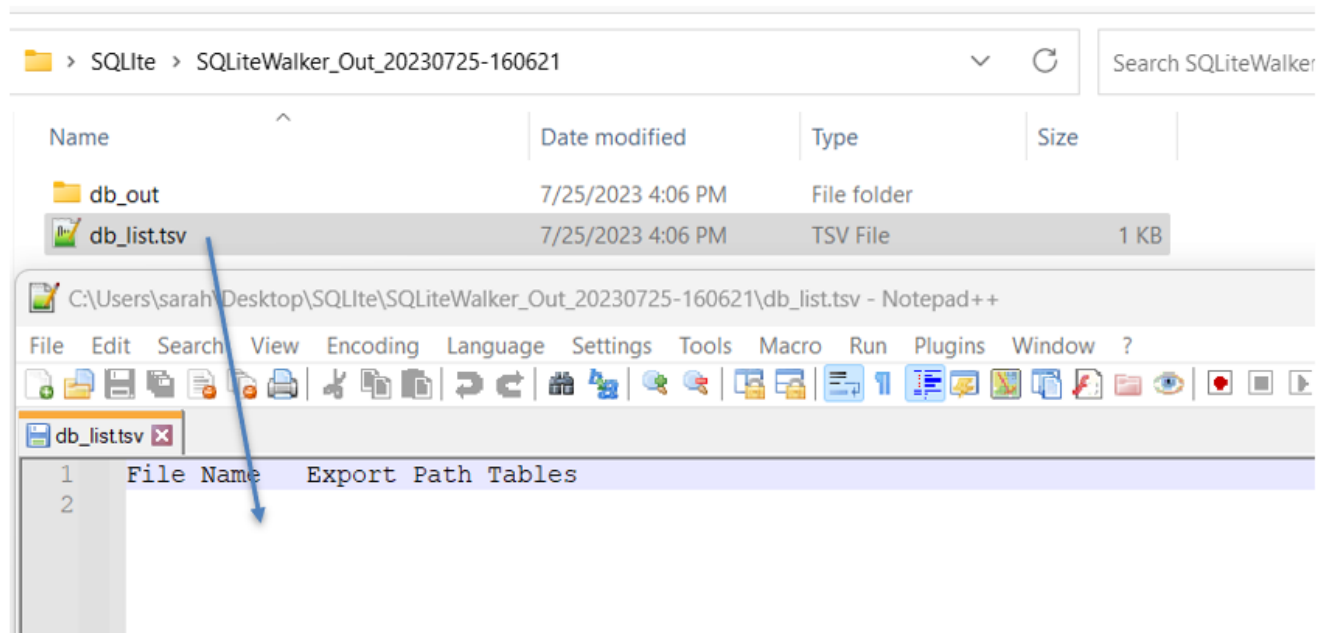
If no databases were found, this is an example of the result.

```
Source: \\?\C:\Users\sarah\Desktop\SQLite\2022 CTF - iOS Full File System.zip
Destination: \\?\C:\Users\sarah\Desktop\SQLite\
-----

****JOB FINISHED****
Runtime: 0.0 seconds
DBs Found: 0
Error Count: 0
```

MOBILE FORENSICS

The db_list.tsv file will be blank.



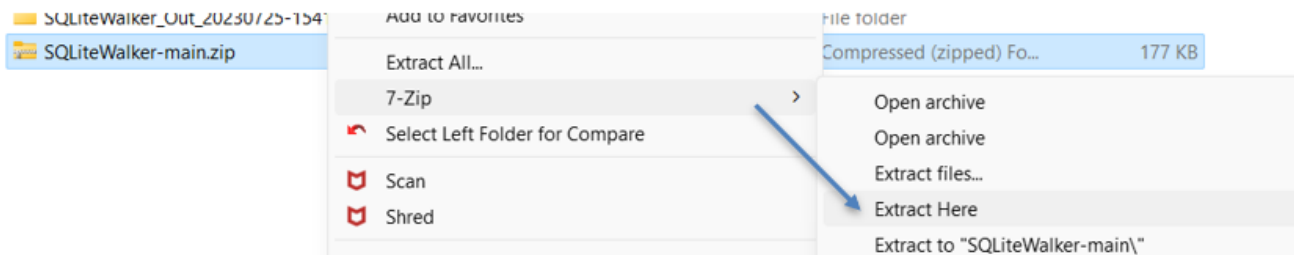
Some systems require command to be **py** instead of **python**, so example would be:

```
py "C:\Users\sarah\Desktop\SQLiteWalker-main\SQLiteWalker-main\SQLiteWalker.py" -i  
"C:\Users\sarah\Desktop\Android 12 Autopsy.zip" -o "C:\Users\sarah\Desktop\SQLiteWalker Output"
```

USING 7ZIP GUIDED EXERCISE

TO START, PLEASE DOWNLOAD 7ZIP FROM <https://www.7-zip.org/download.html>

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 7z2201-x64.exe is a6a0f7c173094f8dafef996157751ecf



Unzipped file

SQLiteWalker-main.zip	7/25/2023 2:29 PM	Compressed (zipped) Fo...	177 KB
SQLiteWalker-main	5/31/2023 9:51 AM	File folder	

Double click or right click "open" to see the contents of the folder.

