ANDRILLER GUIDED EXERCISE

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

This exercise shows installation and usage of Andriller to parse an existing Android image file.

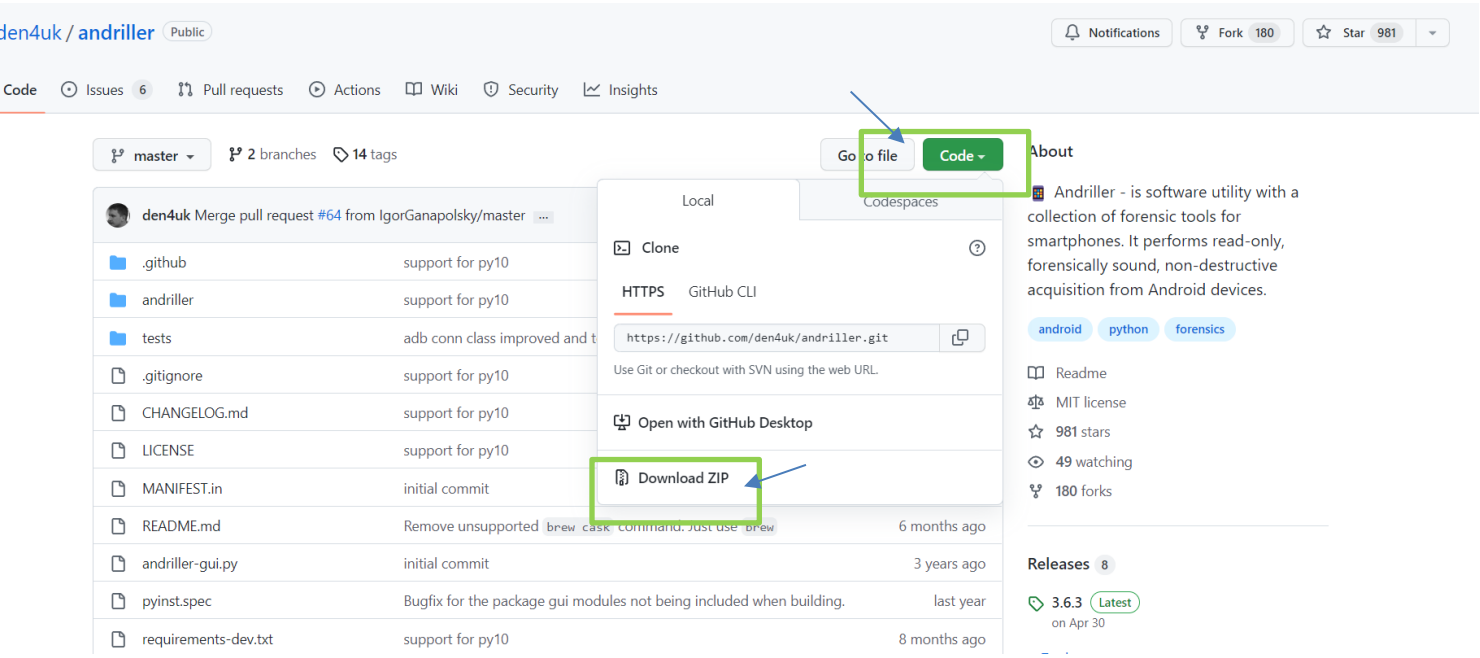
To get started, please install Andriller from https://github.com/den4uk/andriller

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 andriller-master.zip for version 3.6.3 is 0c4e97123a723d091440fa06aee3cd03

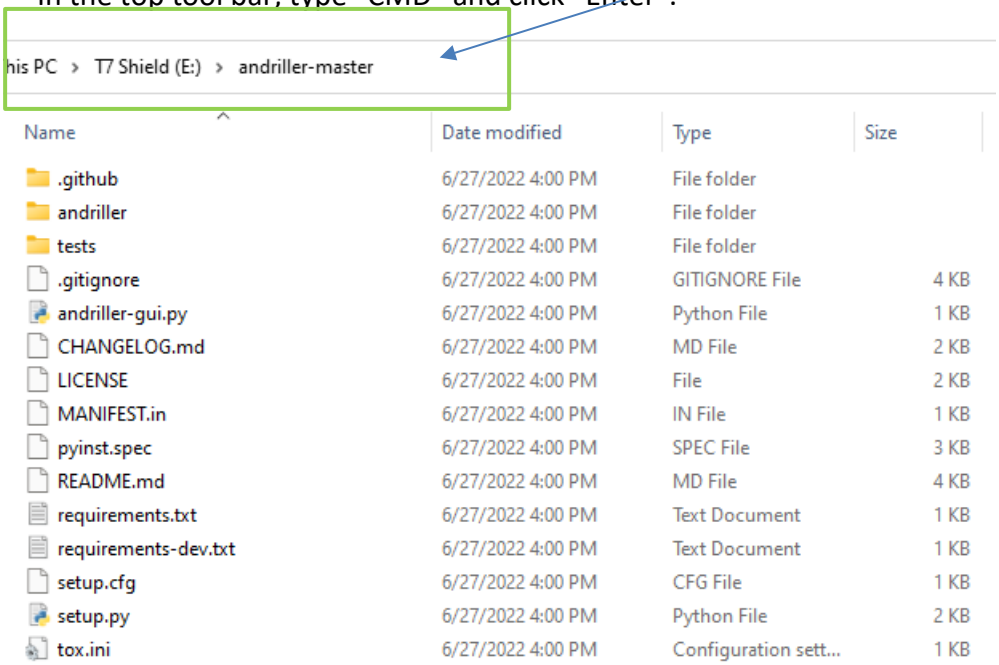
**If you already have Andriller Installed, please move on to Set Up and Use.

INSTALLATION

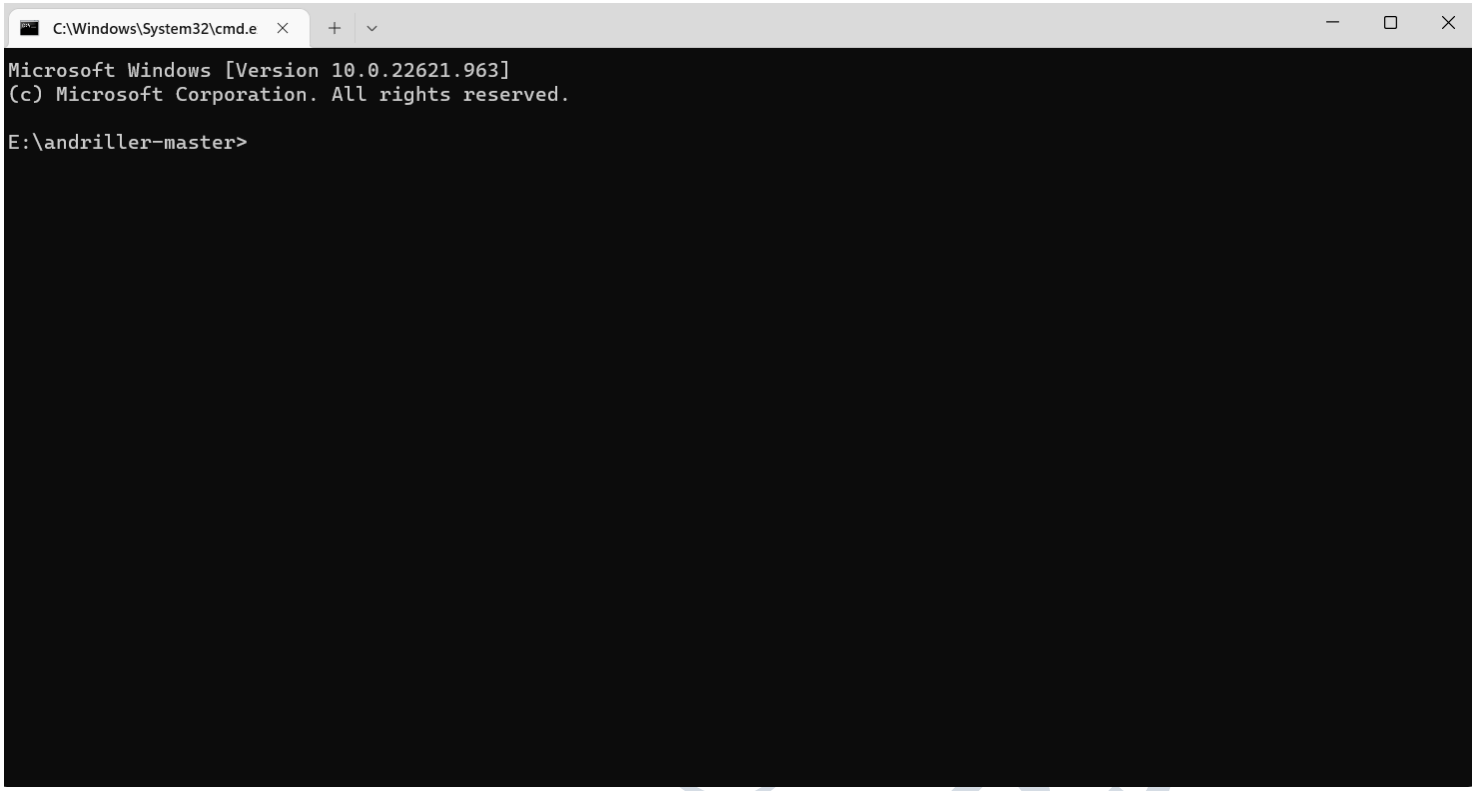
To start click “Code” and then “Download ZIP.”



In the top tool bar, type “CMD” and click “Enter”.

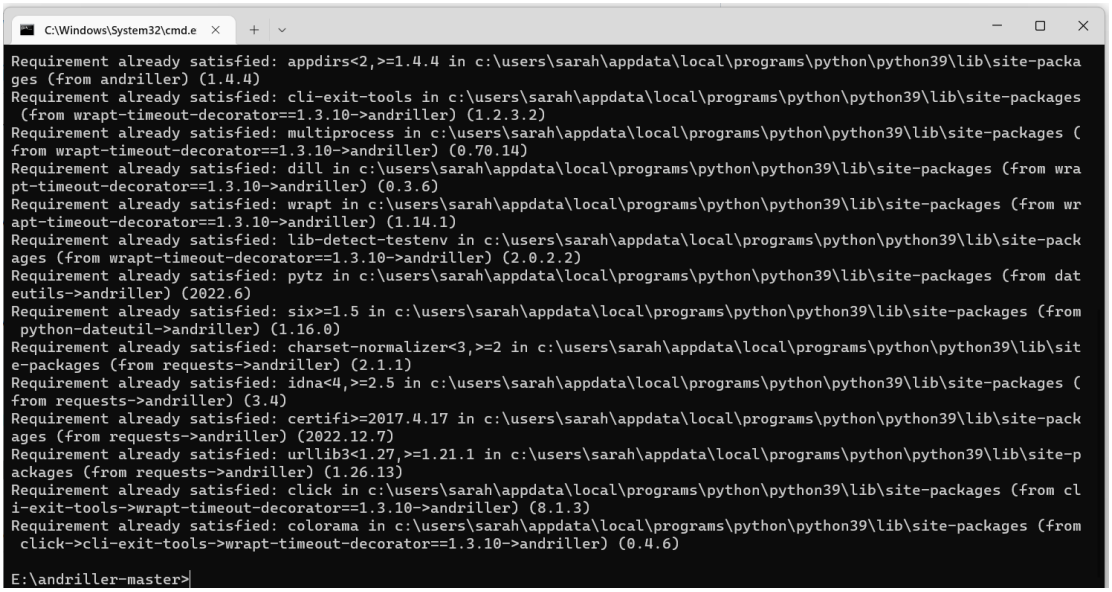


The Command Prompt should appear:



Please read the Dependencies as the next step may depend on what Operating System is being used.

For Windows: type “pip install andriller -U” (or copy and paste it).

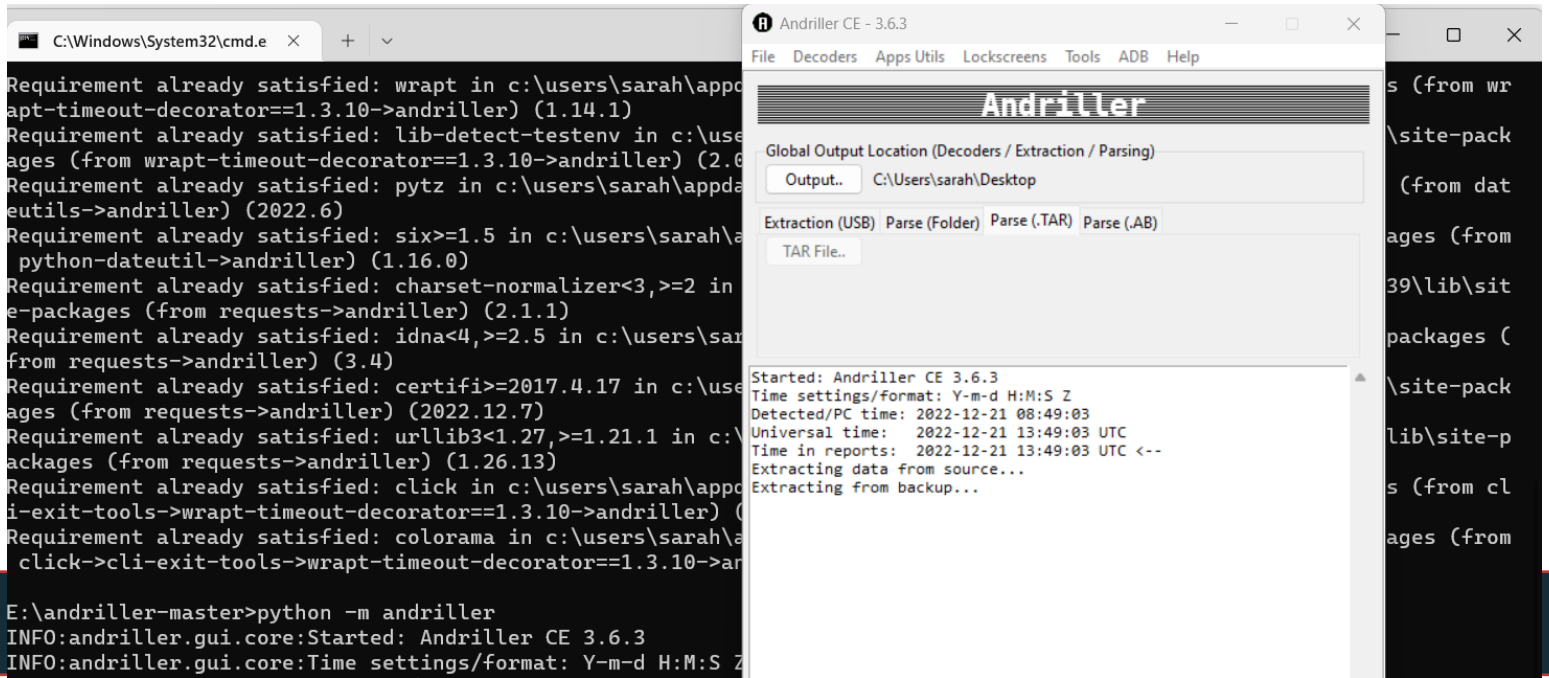


Next command is “python -m andriller” and press “Enter”.

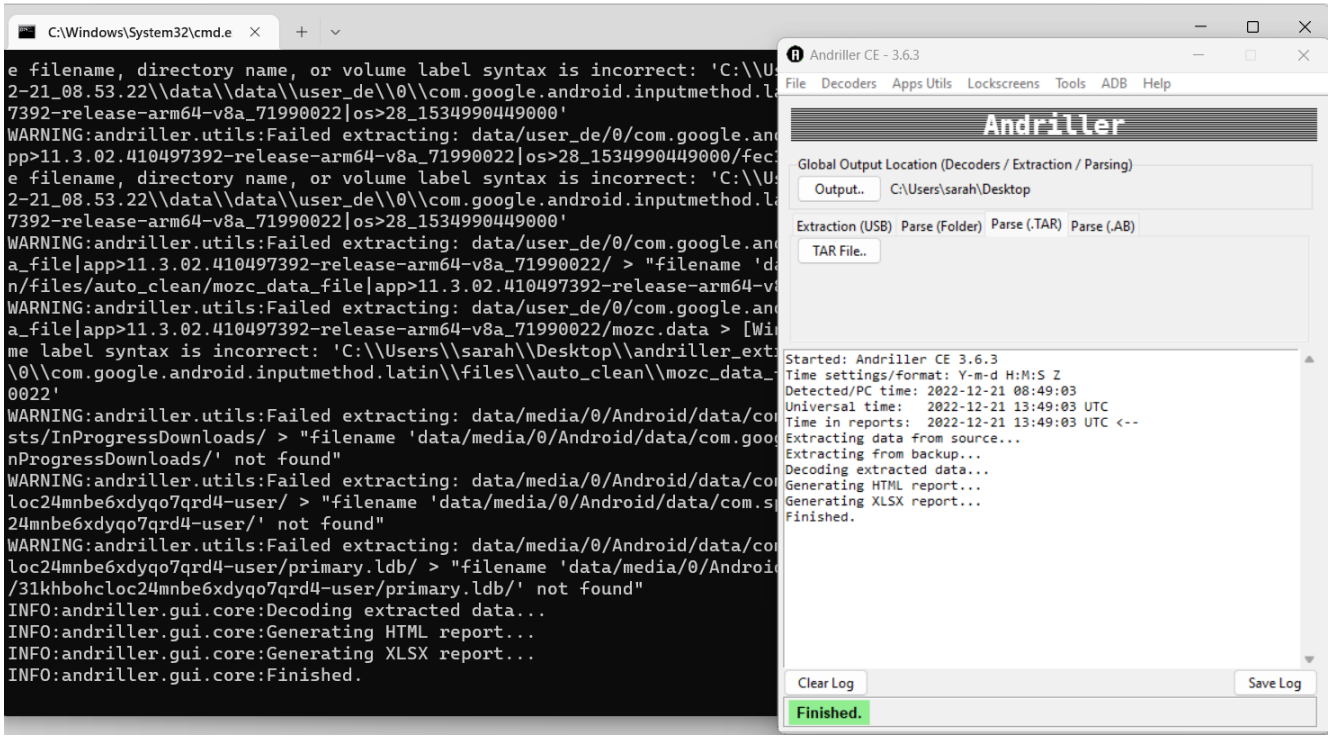
Set Up and Use

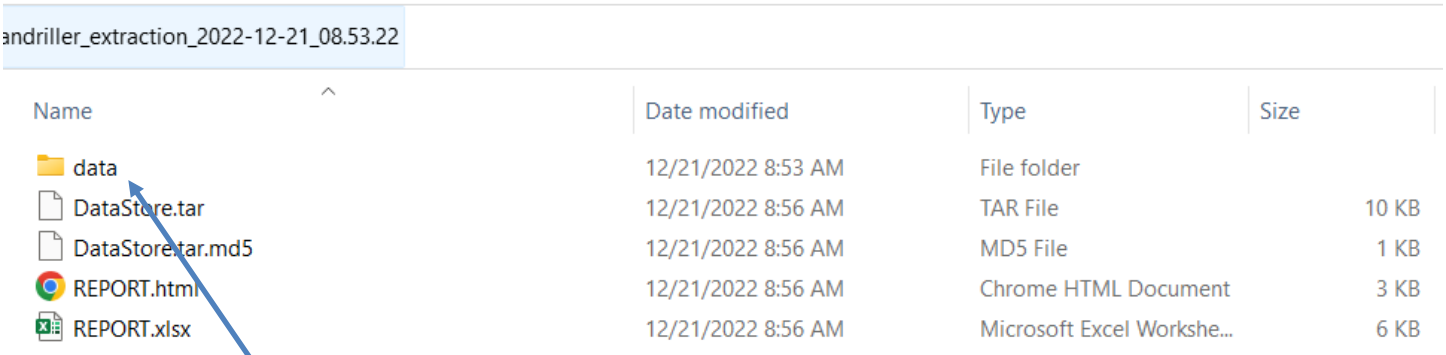
There will be a pop-up screen, select the output location. Select the type of file that will be worked with. Examples: Extraction, Parse (folder), Parse (.Tar), or Parse (.AB)

The CMD and the Andriller will run at the same time. CMD may have warnings or errors, don’t worry until this is complete.



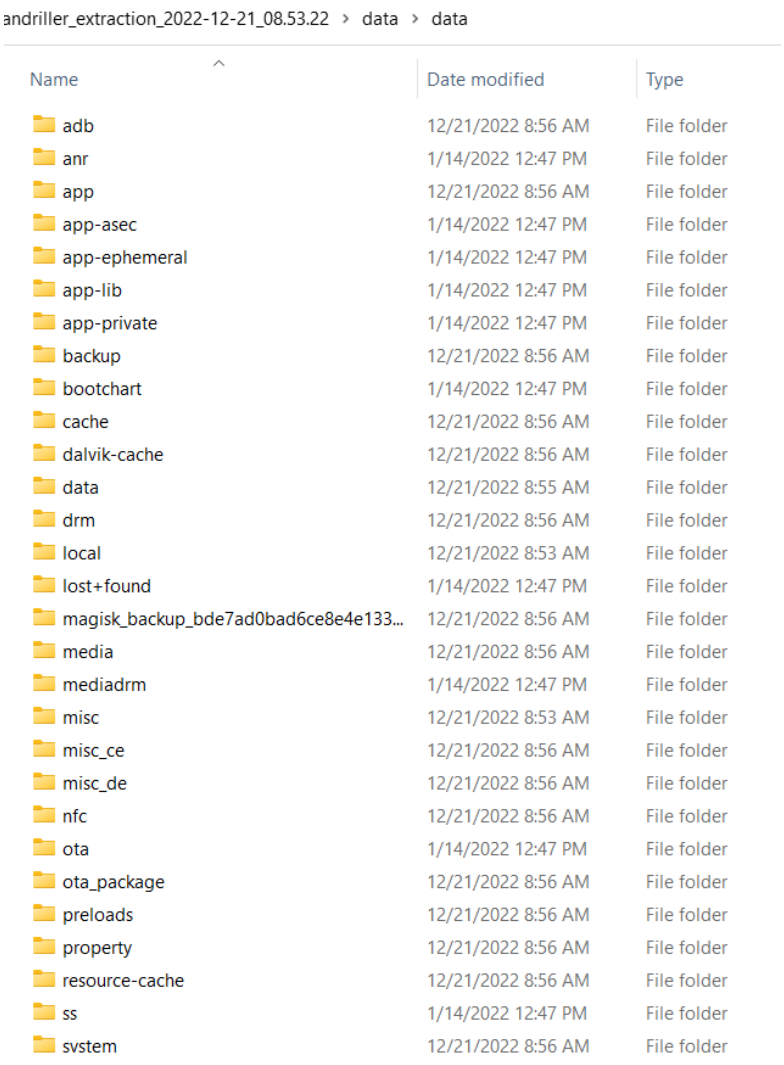
This is what it will look like when complete:





Once the data file is opened, there will be additional folders to navigate.

This is a view of the data folder once opened.



Within each folder there may be additional folders to navigate through.