

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](#).

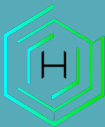
INSTALLATION

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

The screenshot shows the GitHub repository page for `den4uk/andriller`. The repository is public and has 981 stars, 180 forks, and 49 watchers. The repository contains 6 issues, 2 branches, and 14 tags. The file list shows the following files and their commit history:

File	Commit History
<code>.github</code>	support for py10
<code>andriller</code>	support for py10
<code>tests</code>	adb conn class improved and t
<code>.gitignore</code>	support for py10
<code>CHANGELOG.md</code>	support for py10
<code>LICENSE</code>	support for py10
<code>MANIFEST.in</code>	initial commit
<code>README.md</code>	Remove unsupported <code>brew cask</code> command. Just use <code>brew</code> 6 months ago
<code>andriller-gui.py</code>	initial commit 3 years ago
<code>pyinst.spec</code>	Bugfix for the package gui modules not being included when building. last year
<code>requirements-dev.txt</code>	support for py10 8 months ago

The 'Code' button is highlighted with a green box and a blue arrow. The 'Download ZIP' option in the dropdown menu is also highlighted with a green box and a blue arrow.

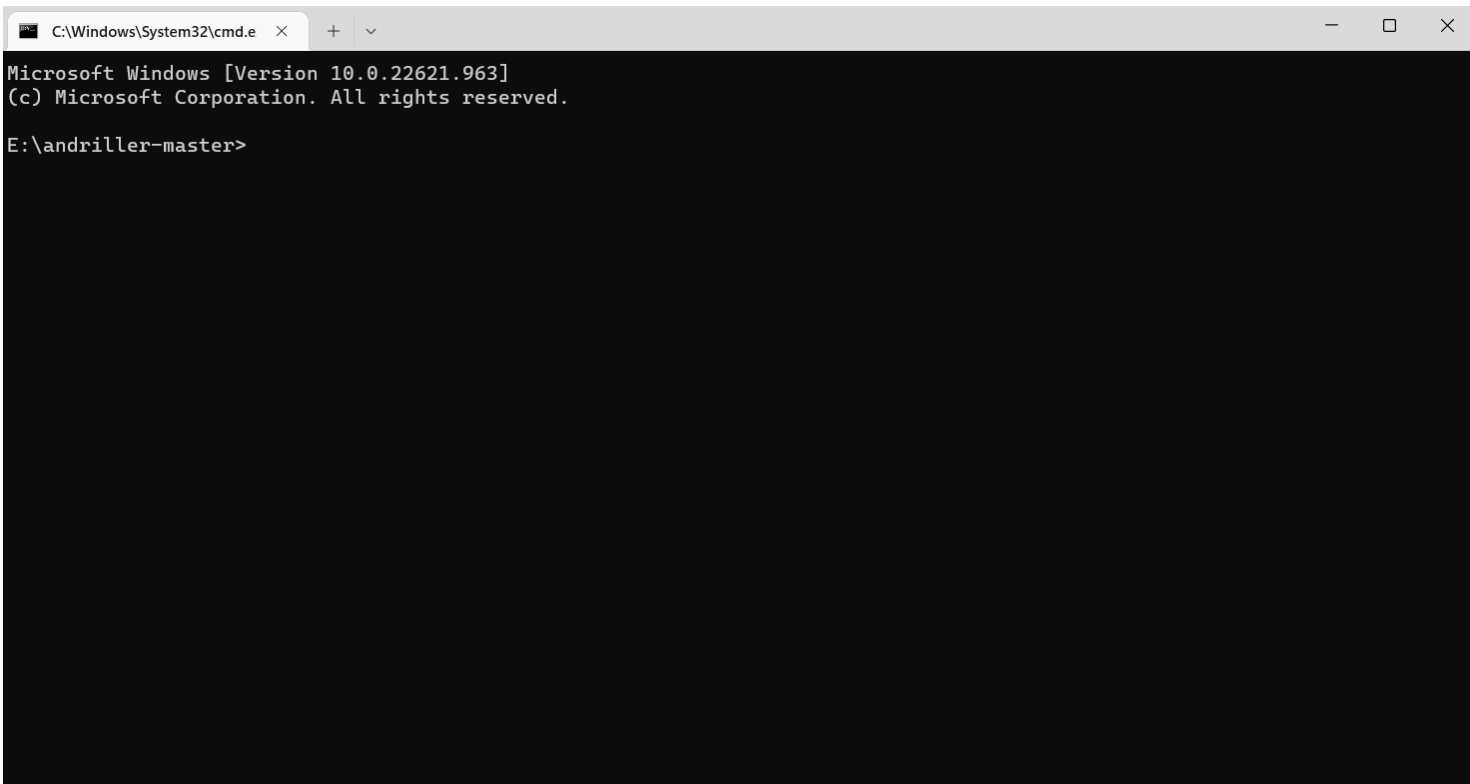


In the top tool bar, type "CMD" and click "Enter".



Name	Date modified	Type	Size
.github	6/27/2022 4:00 PM	File folder	
andriller	6/27/2022 4:00 PM	File folder	
tests	6/27/2022 4:00 PM	File folder	
.gitignore	6/27/2022 4:00 PM	GITIGNORE File	4 KB
andriller-gui.py	6/27/2022 4:00 PM	Python File	1 KB
CHANGELOG.md	6/27/2022 4:00 PM	MD File	2 KB
LICENSE	6/27/2022 4:00 PM	File	2 KB
MANIFEST.in	6/27/2022 4:00 PM	IN File	1 KB
pyinst.spec	6/27/2022 4:00 PM	SPEC File	3 KB
README.md	6/27/2022 4:00 PM	MD File	4 KB
requirements.txt	6/27/2022 4:00 PM	Text Document	1 KB
requirements-dev.txt	6/27/2022 4:00 PM	Text Document	1 KB
setup.cfg	6/27/2022 4:00 PM	CFG File	1 KB
setup.py	6/27/2022 4:00 PM	Python File	2 KB
tox.ini	6/27/2022 4:00 PM	Configuration sett...	1 KB

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).

```
C:\Windows\System32\cmd.e x + v
Requirement already satisfied: appdirs<2,>=1.4.4 in c:\users\sarah\appdata\local\programs\python\python39\lib\site-packa
ges (from andriller) (1.4.4)
Requirement already satisfied: cli-exit-tools in c:\users\sarah\appdata\local\programs\python\python39\lib\site-packages
 (from wrapt-timeout-decorator==1.3.10->andriller) (1.2.3.2)
Requirement already satisfied: multiprocessing in c:\users\sarah\appdata\local\programs\python\python39\lib\site-packages (
from wrapt-timeout-decorator==1.3.10->andriller) (0.70.14)
Requirement already satisfied: dill in c:\users\sarah\appdata\local\programs\python\python39\lib\site-packages (from wra
pt-timeout-decorator==1.3.10->andriller) (0.3.6)
Requirement already satisfied: wrapt in c:\users\sarah\appdata\local\programs\python\python39\lib\site-packages (from wr
apt-timeout-decorator==1.3.10->andriller) (1.14.1)
Requirement already satisfied: lib-detect-testenv in c:\users\sarah\appdata\local\programs\python\python39\lib\site-pack
ages (from wrapt-timeout-decorator==1.3.10->andriller) (2.0.2.2)
Requirement already satisfied: pytz in c:\users\sarah\appdata\local\programs\python\python39\lib\site-packages (from dat
eutils->andriller) (2022.6)
Requirement already satisfied: six>=1.5 in c:\users\sarah\appdata\local\programs\python\python39\lib\site-packages (from
python-dateutil->andriller) (1.16.0)
Requirement already satisfied: charset-normalizer<3,>=2 in c:\users\sarah\appdata\local\programs\python\python39\lib\sit
e-packages (from requests->andriller) (2.1.1)
Requirement already satisfied: idna<4,>=2.5 in c:\users\sarah\appdata\local\programs\python\python39\lib\site-packages (
from requests->andriller) (3.4)
Requirement already satisfied: certifi>=2017.4.17 in c:\users\sarah\appdata\local\programs\python\python39\lib\site-pack
ages (from requests->andriller) (2022.12.7)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in c:\users\sarah\appdata\local\programs\python\python39\lib\site-p
ackages (from requests->andriller) (1.26.13)
Requirement already satisfied: click in c:\users\sarah\appdata\local\programs\python\python39\lib\site-packages (from cl
i-exit-tools->wrapt-timeout-decorator==1.3.10->andriller) (8.1.3)
Requirement already satisfied: colorama in c:\users\sarah\appdata\local\programs\python\python39\lib\site-packages (from
click->cli-exit-tools->wrapt-timeout-decorator==1.3.10->andriller) (0.4.6)
E:\andriller-master>
```

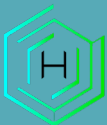
Next command is “python -m andriller” and press “Enter”.

SET UP AND USE

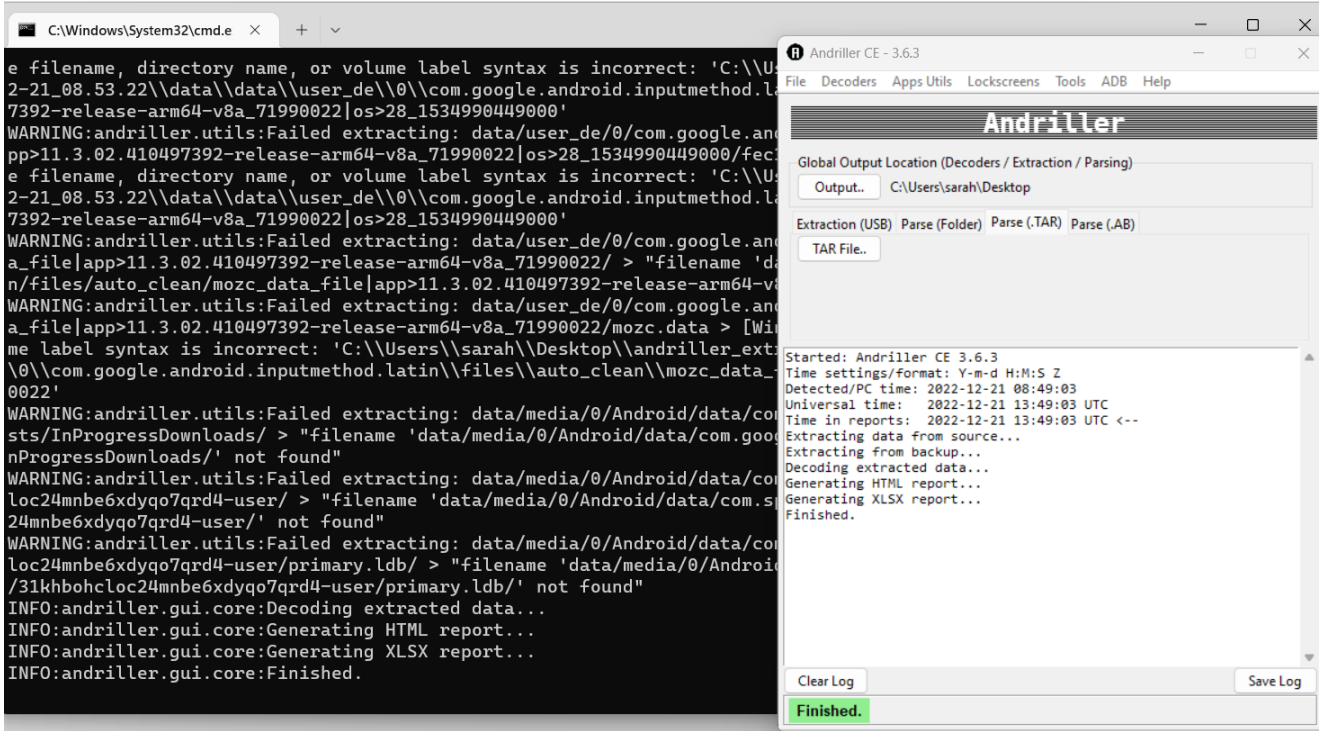
There will be a pop-up screen, select the output location. Select the type of file that will be worked with. Examples: Extraction, Parse (folder), Parse (.Tar), or Parse (.AB)

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

The screenshot displays two windows side-by-side. On the left is a Windows Command Prompt window titled 'C:\Windows\System32\cmd.e' showing the output of a pip install command. The output lists various dependencies that are already satisfied, such as appdirs, cli-exit-tools, multiprocessing, dill, wrapt, lib-detect-testenv, pytz, six, charset-normalizer, idna, certifi, urllib3, click, and colorama. At the bottom of the command prompt, the user has entered 'E:\andriller-master>python -m andriller' and the output shows 'INFO:andriller.gui.core:Started: Andriller CE 3.6.3' and 'INFO:andriller.gui.core:Time settings/format: Y-m-d H:M:S Z'. On the right is the 'Andriller CE - 3.6.3' GUI window. The title bar includes 'File', 'Decoders', 'Apps Utils', 'Lockscreens', 'Tools', 'ADB', and 'Help'. The main window has a dark header with the word 'Andriller' in white. Below the header, there is a section for 'Global Output Location (Decoders / Extraction / Parsing)' with an 'Output..' button and the path 'C:\Users\sarah\Desktop'. There are four radio buttons for file types: 'Extraction (USB)', 'Parse (Folder)', 'Parse (.TAR)', and 'Parse (.AB)'. The 'Extraction (USB)' option is selected. Below this is a 'TAR File..' input field. At the bottom of the GUI, a status bar shows 'Started: Andriller CE 3.6.3', 'Time settings/format: Y-m-d H:M:S Z', 'Detected/PC time: 2022-12-21 08:49:03', 'Universal time: 2022-12-21 13:49:03 UTC', 'Time in reports: 2022-12-21 13:49:03 UTC <--', and 'Extracting data from source...' and 'Extracting from backup...'.



This is what it will look like when complete:



andriller_extraction_2022-12-21_08.53.22

Name	Date modified	Type	Size
data	12/21/2022 8:53 AM	File folder	
DataStore.tar	12/21/2022 8:56 AM	TAR File	10 KB
DataStore.tar.md5	12/21/2022 8:56 AM	MD5 File	1 KB
REPORT.html	12/21/2022 8:56 AM	Chrome HTML Document	3 KB
REPORT.xlsx	12/21/2022 8:56 AM	Microsoft Excel Workshe...	6 KB

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



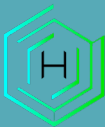


This is a view of the data folder once opened.

andriller_extraction_2022-12-21_08.53.22 > data > data

Name	Date modified	Type
adb	12/21/2022 8:56 AM	File folder
anr	1/14/2022 12:47 PM	File folder
app	12/21/2022 8:56 AM	File folder
app-asec	1/14/2022 12:47 PM	File folder
app-ephemeral	1/14/2022 12:47 PM	File folder
app-lib	1/14/2022 12:47 PM	File folder
app-private	1/14/2022 12:47 PM	File folder
backup	12/21/2022 8:56 AM	File folder
bootchart	1/14/2022 12:47 PM	File folder
cache	12/21/2022 8:56 AM	File folder
dalvik-cache	12/21/2022 8:56 AM	File folder
data	12/21/2022 8:55 AM	File folder
drm	12/21/2022 8:56 AM	File folder
local	12/21/2022 8:53 AM	File folder
lost+found	1/14/2022 12:47 PM	File folder
magisk_backup_bde7ad0bad6ce8e4e133...	12/21/2022 8:56 AM	File folder
media	12/21/2022 8:56 AM	File folder
mediadrms	1/14/2022 12:47 PM	File folder
misc	12/21/2022 8:53 AM	File folder
misc_ce	12/21/2022 8:56 AM	File folder
misc_de	12/21/2022 8:56 AM	File folder
nfc	12/21/2022 8:56 AM	File folder
ota	1/14/2022 12:47 PM	File folder
ota_package	12/21/2022 8:56 AM	File folder
preloads	12/21/2022 8:56 AM	File folder
property	12/21/2022 8:56 AM	File folder
resource-cache	12/21/2022 8:56 AM	File folder
ss	1/14/2022 12:47 PM	File folder
svstem	12/21/2022 8:56 AM	File folder

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



is PC > T7 Shield (E:) > Andriллер > andriller_extraction_2022-12-20_13.28.22 > data > data > data

Name	Date modified	Type
android	1/14/2022 12:47 PM	File folder
android.auto_generated_rr_	1/14/2022 12:47 PM	File folder
android.autoinstalls.config.google.nexus	1/14/2022 12:47 PM	File folder
android.telephony.overlay.cmcc	1/14/2022 12:47 PM	File folder
com.alltrails.alltrails	2/13/2022 1:44 AM	File folder
com.android.backupconfirm	1/14/2022 12:47 PM	File folder
com.android.bips	1/14/2022 12:47 PM	File folder
com.android.bluetooth	1/14/2022 12:47 PM	File folder
com.android.bluetoothmidiservice	1/14/2022 12:47 PM	File folder
com.android.bookmarkprovider	1/14/2022 12:47 PM	File folder
com.android.calllogbackup	1/14/2022 12:47 PM	File folder
com.android.captiveportallogin	1/25/2022 4:48 PM	File folder
com.android.carrierdefaultapp	1/14/2022 12:47 PM	File folder
com.android.cellbroadcastreceiver	1/14/2022 12:47 PM	File folder
com.android.certinstaller	1/14/2022 12:47 PM	File folder
com.android.chrome	2/6/2022 4:02 PM	File folder
com.android.companiondevicemanager	1/14/2022 12:47 PM	File folder
com.android.connectivity.metrics	1/14/2022 12:47 PM	File folder
com.android.cts.ctsshim	1/14/2022 12:47 PM	File folder
com.android.cts.priv.ctsshim	1/14/2022 12:47 PM	File folder
com.android.defcontainer	1/14/2022 12:47 PM	File folder
com.android.documentsui	1/14/2022 1:58 PM	File folder
com.android.dreams.basic	1/14/2022 12:47 PM	File folder
com.android.egg	1/14/2022 12:47 PM	File folder
com.android.emergency	1/14/2022 12:47 PM	File folder
com.android.etc	1/14/2022 12:47 PM	File folder

