Day 14 of Learning Cyber Security

Platform: Kali Linux

Name: Ayesha Nadeem

Topic: Android Penetration Testing

Contact Me: ayeshanm8@gmail.com

Date: 14th July, 2025

Andriller

⚠️ *This guide is intended for **educational and authorized forensic use only**. Extraction techniques and exposure of device identifiers (e.g., serial numbers) should only be performed on **devices you own or have explicit permission to analyze**. Unauthorized access or data handling may **violate privacy laws** and ethical standards. Use responsibly.*

Initial Setup:

Command 1:

```
┌──(ayeshanadeem㉿ayeshanadeem)-[~]
└─$ git clone https://github.com/den4uk/andriller.git

Cloning into 'andriller' ...
remote: Enumerating objects: 499, done.
remote: Counting objects: 100% (72/72), done.
remote: Compressing objects: 100% (30/30), done.
remote: Total 499 (delta 42), reused 42 (delta 42), pack-reused 427 (from 1)
Receiving objects: 100% (499/499), 1.31 MiB | 20.00 KiB/s, done.
Resolving deltas: 100% (302/302), done.

┌──(ayeshanadeem㉿ayeshanadeem)-[~]
```

Command 2:

```
┌──(ayeshanadeem㉿ayeshanadeem)-[~]
└─$ cd andriller
```

Command 3:

```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/andriller]
└─$ sudo chmod +x setup.py andriller-gui.py
```

Command 4:

```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/andriller]
└─$ pip install build
Defaulting to user installation because normal site-packages is not writeable
Collecting build
  Downloading build-1.2.2.post1-py3-none-any.whl.metadata (6.5 kB)
Requirement already satisfied: packaging ≥ 19.1 in /usr/lib/python3/dist-packages (from build) (24.0)
Collecting pyproject_hooks (from build)
  Downloading pyproject_hooks-1.2.0-py3-none-any.whl.metadata (1.3 kB)
Downloading build-1.2.2.post1-py3-none-any.whl (22 kB)
Downloading pyproject_hooks-1.2.0-py3-none-any.whl (10 kB)
Installing collected packages: pyproject_hooks, build
  WARNING: The script pyproject-build is installed in '/home/ayeshanadeem/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed build-1.2.2.post1 pyproject_hooks-1.2.0
```

Command 5:

```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/andriller]
└─$ sudo apt install python3-venv
The following packages were automatically installed and are no longer required:
  cpp-13             ibverbs-providers  libboost-iostreams1.83.0  libcephfs2    libgfapi0  libg
  fonts-liberation2  libarmadillo12     libboost-thread1.83.0     libgdal34t64  libgfrpc0  libg
Use 'sudo apt autoremove' to remove them.

Upgrading:
  blueman                       libgnutls30t64       libsharpyuv0     onboard-data            py
  curl                          libgpg-error0        libsmbclient0    openssl                 py
  faraday                       libgpgme11t64        libsnappy1v5     python-apt-common       py
  gdal-data                     libgvc6              libssh2-1t64     python-matplotlib-data  py
  gdal-plugins                  libgvpr2             libssl3t64       python-tables-data      py
  gnutls-bin                    libhogweed6t64       libtalloc2       python3                 py
  graphviz                      libicu-dev           libtdb1          python3-aardwolf        py
  icu-devtools                  libjs-sphinxdoc      libtevent0t64    python3-aiohttp         py
  ldap-utils                    liblab-gamut1        libtiff6         python3-anyio           py
  libavif16                     libldap-common       libwbclient0     python3-apt             py
  libbrlapi0.8                  libldb2              libwebp7         python3-arc4            py
  libbrotli1                    libltdl7             libwebpdemux2    python3-bitstruct       py
  libcairo-gobject2             libnettle8t64        libwebpmux3      python3-bottleneck      py
  libcairo-script-interpreter2  libnewt0.52         libxaw7          python3-brlapi          py
  libcairo2                     libpathplan4         libxtst6         python3-brotli          py
  libcdt5                       libpng16-16t64       libyuv0          python3-cairo           py
  libcgraph6                    libpoppler-glib8t64  libzstd1         python3-cbor            py
  libcurl3t64-gnutls            libprotobuf32t64     mitmproxy        python3-cffi            py
  libcurl4t64                   libpython3-dev       onboard          python3-cffi-backend    py
  libgnutls-dane0t64            libpython3-stdlib    onboard-common   python3-contourpy       py

Installing:
  python3-venv
```

Command 6:

```
┌──(ayeshanadeem㉿ayeshanadeem)-[~/andriller]
└─$ python3 -m venv venv

┌──(ayeshanadeem㉿ayeshanadeem)-[~/andriller]
└─$ source venv/bin/activate
```

Command 7:

```
┌──(venv)─(ayeshanadeem㉿ayeshanadeem)-[~/andriller]
└─$ pip install build
Collecting build
  Using cached build-1.2.2.post1-py3-none-any.whl.metadata (6.5 kB)
Collecting packaging>=19.1 (from build)
  Downloading packaging-25.0-py3-none-any.whl.metadata (3.3 kB)
Collecting pyproject_hooks (from build)
  Using cached pyproject_hooks-1.2.0-py3-none-any.whl.metadata (1.3 kB)
Using cached build-1.2.2.post1-py3-none-any.whl (22 kB)
Downloading packaging-25.0-py3-none-any.whl (66 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 66.5/66.5 kB 109.9 kB/s eta 0:00:00
Using cached pyproject_hooks-1.2.0-py3-none-any.whl (10 kB)
Installing collected packages: pyproject_hooks, packaging, build
Successfully installed build-1.2.2.post1 packaging-25.0 pyproject_hooks-1.2.0
```

Command 8:

```
Successfully built andriller-3.6.3.tar.gz and andrill

┌──(venv)─(ayeshanadeem㉿ayeshanadeem)-[~/andriller]
└─$ sudo rm -rf andriller.egg-info
[sudo] password for ayeshanadeem:
```

Command 9:

```
┌──(venv)─(ayeshanadeem㉿ayeshanadeem)-[~/andriller]
└─$ sudo chown -R $ayeshanadeem:$ayeshanadeem ~/andriller
```

Command 10:

```
┌──(venv)─(ayeshanadeem㉿ayeshanadeem)-[~/andriller]
└─$ pip install jinja2
WARNING: Retrying (Retry(total=4, connect=None, read=None, redirect=None, status=None)) after connect
 connection: [Errno -3] Temporary failure in name resolution')': /simple/jinja2/
Collecting jinja2
  Downloading jinja2-3.1.6-py3-none-any.whl.metadata (2.9 kB)
Collecting MarkupSafe≥2.0 (from jinja2)
  Downloading MarkupSafe-3.0.2-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (4
Downloading jinja2-3.1.6-py3-none-any.whl (134 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 134.9/134.9 kB 32.2 kB/s eta 0:00:00
Downloading MarkupSafe-3.0.2-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (23 kB)
Installing collected packages: MarkupSafe, jinja2
Successfully installed MarkupSafe-3.0.2 jinja2-3.1.6
```

Command 11:

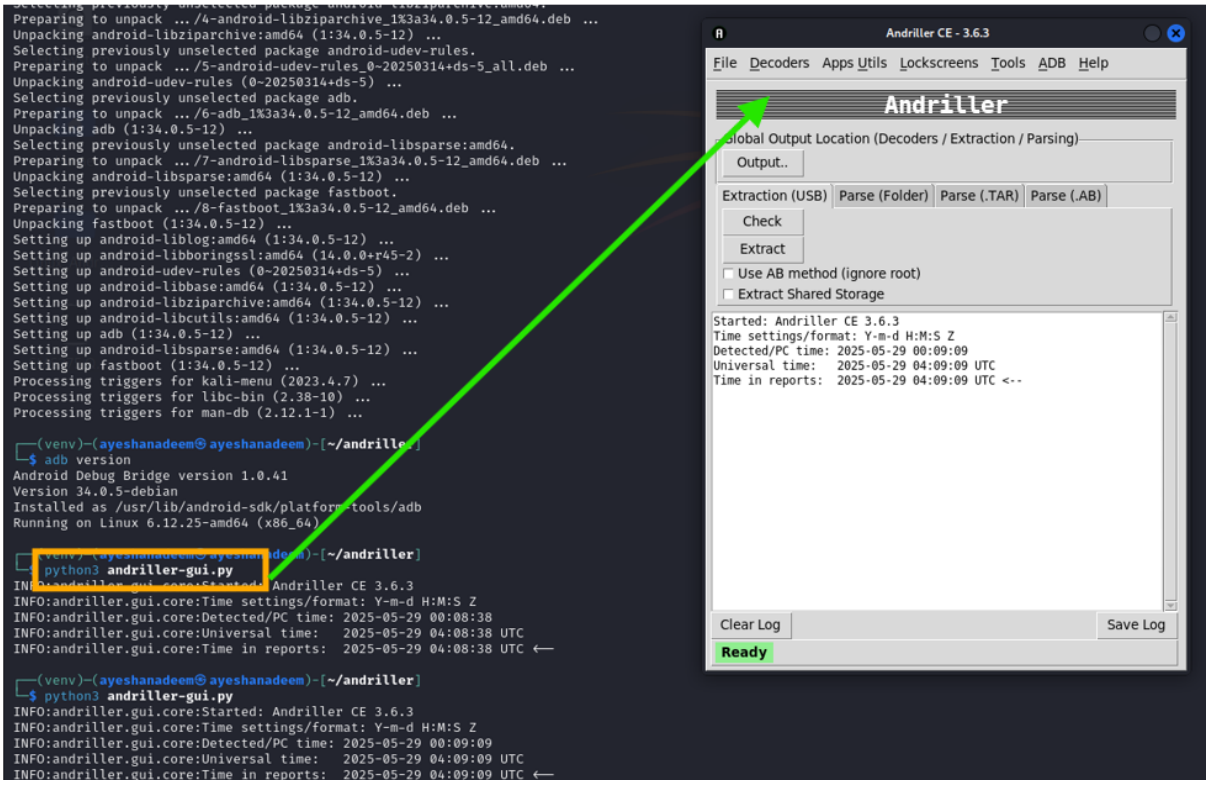
```
┌──(venv)─(ayeshanadeem㉿ayeshanadeem)-[~/andriller]
└─$ pip install -r requirements.txt
Ignoring dataclasses: markers 'python_version == "3.6"' don't match your environment
Collecting dateutils (from -r requirements.txt (line 1))
  Downloading dateutils-0.6.12-py2.py3-none-any.whl.metadata (1.3 kB)
Collecting javaobj-py3≥0.4.3 (from -r requirements.txt (line 2))
  Downloading javaobj_py3-0.4.4-py2.py3-none-any.whl.metadata (17 kB)
Collecting pycryptodomex (from -r requirements.txt (line 3))
  Downloading pycryptodomex-3.23.0-cp37-abi3-manylinux_2_17_x86_64.manylinux2014_x86_6
Collecting python-dateutil (from -r requirements.txt (line 4))
  Downloading python_dateutil-2.9.0.post0-py2.py3-none-any.whl.metadata (8.4 kB)
Collecting XlsxWriter (from -r requirements.txt (line 5))
  Downloading XlsxWriter-3.2.3-py3-none-any.whl.metadata (2.7 kB)
Collecting Jinja2<3,≥2.11.3 (from -r requirements.txt (line 6))
  Downloading Jinja2-2.11.3-py2.py3-none-any.whl.metadata (3.5 kB)
Collecting MarkupSafe==2.0.1 (from -r requirements.txt (line 7))
  Downloading MarkupSafe-2.0.1.tar.gz (18 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Collecting wrapt-timeout-decorator==1.3.10 (from -r requirements.txt (line 8))
  Downloading wrapt_timeout_decorator-1.3.10-py3-none-any.whl.metadata (36 kB)
Collecting appdirs<2,≥1.4.4 (from -r requirements.txt (line 9))
  Downloading appdirs-1.4.4-py2.py3-none-any.whl.metadata (9.0 kB)
Collecting requests (from -r requirements.txt (line 10))
  Downloading requests-2.32.3-py3-none-any.whl.metadata (4.6 kB)
```

Command 12:

```
┌──(venv)─(ayeshanadeem㉿ayeshanadeem)-[~/andriller]
└─$ pip install .
Processing /home/ayeshanadeem/andriller
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Requirement already satisfied: dateutils in ./venv/lib/python3.13/site-packages (from andriller==3.6.3) (0.6.12)
Requirement already satisfied: javaobj-py3≥0.4.3 in ./venv/lib/python3.13/site-packages (from andriller==3.6.3) (0.4.4)
Requirement already satisfied: pycryptodomex in ./venv/lib/python3.13/site-packages (from andriller==3.6.3) (3.23.0)
Requirement already satisfied: python-dateutil in ./venv/lib/python3.13/site-packages (from andriller==3.6.3) (2.9.0.post0)
Requirement already satisfied: XlsxWriter in ./venv/lib/python3.13/site-packages (from andriller==3.6.3) (3.2.3)
Requirement already satisfied: Jinja2<3,≥2.11.3 in ./venv/lib/python3.13/site-packages (from andriller==3.6.3) (2.11.3)
Requirement already satisfied: MarkupSafe==2.0.1 in ./venv/lib/python3.13/site-packages (from andriller==3.6.3) (2.0.1)
Requirement already satisfied: wrapt-timeout-decorator==1.3.10 in ./venv/lib/python3.13/site-packages (from andriller==3.6.3) (1.3.10)
Requirement already satisfied: appdirs<2,≥1.4.4 in ./venv/lib/python3.13/site-packages (from andriller==3.6.3) (1.4.4)
Requirement already satisfied: requests in ./venv/lib/python3.13/site-packages (from andriller==3.6.3) (2.32.3)
Requirement already satisfied: cli-exit-tools in ./venv/lib/python3.13/site-packages (from wrapt-timeout-decorator==1.3.10→andriller==3.6.3) (1.2.7)
Requirement already satisfied: lib-detect-testenv in ./venv/lib/python3.13/site-packages (from wrapt-timeout-decorator==1.3.10→andriller==3.6.3) (2.0.8)
Requirement already satisfied: dill in ./venv/lib/python3.13/site-packages (from wrapt-timeout-decorator==1.3.10→andriller==3.6.3) (0.4.0)
Requirement already satisfied: multiprocess in ./venv/lib/python3.13/site-packages (from wrapt-timeout-decorator==1.3.10→andriller==3.6.3) (0.70.18)
Requirement already satisfied: wrapt in ./venv/lib/python3.13/site-packages (from wrapt-timeout-decorator==1.3.10→andriller==3.6.3) (1.17.2)
Requirement already satisfied: pytz in ./venv/lib/python3.13/site-packages (from dateutils→andriller==3.6.3) (2025.2)
Requirement already satisfied: six≥1.5 in ./venv/lib/python3.13/site-packages (from python-dateutil→andriller==3.6.3) (1.17.0)
Requirement already satisfied: charset-normalizer<4,≥2 in ./venv/lib/python3.13/site-packages (from requests→andriller==3.6.3) (3.4.2)
Requirement already satisfied: idna<4,≥2.5 in ./venv/lib/python3.13/site-packages (from requests→andriller==3.6.3) (3.10)
Requirement already satisfied: urllib3<3,≥1.21.1 in ./venv/lib/python3.13/site-packages (from requests→andriller==3.6.3) (2.4.0)
Requirement already satisfied: certifi≥2017.4.17 in ./venv/lib/python3.13/site-packages (from requests→andriller==3.6.3) (2025.4.26)
Requirement already satisfied: click in ./venv/lib/python3.13/site-packages (from cli-exit-tools→wrapt-timeout-decorator==1.3.10→andriller==3.6.3) (8.2.1)
Building wheels for collected packages: andriller
  Building wheel for andriller (pyproject.toml) ... done
  Created wheel for andriller: filename=andriller-3.6.3-py3-none-any.whl size=1316054 sha256=8aa2cb90c493462075a8fd95c87f690cc6a9c923b0e9295e38095e2ee6f46a24
  Stored in directory: /tmp/pip-ephem-wheel-cache-rbbz82mo/wheels/27/ec/c7/e01bae9510e09d9fa818730707ad1126783a36ba520b9cadb8
Successfully built andriller
Installing collected packages: andriller
Successfully installed andriller-3.6.3
```

Launch andriller-gui.py

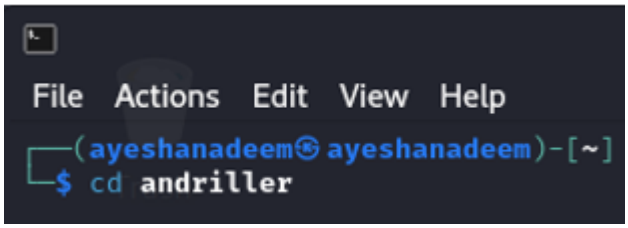
Command 13:



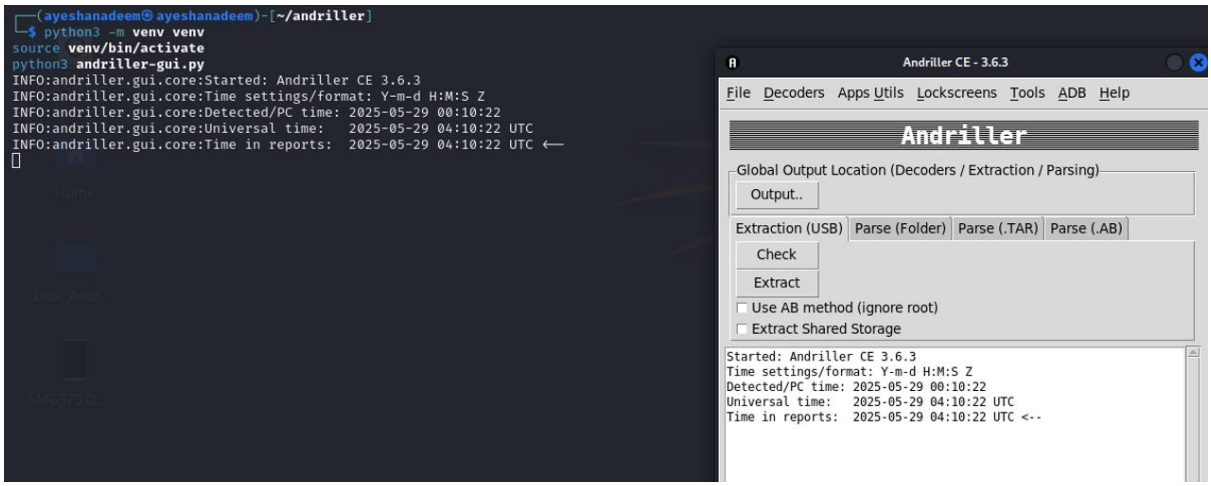
Verfied the installation:

Close all previous terminals and in new terminal write these commands.

Command 14:



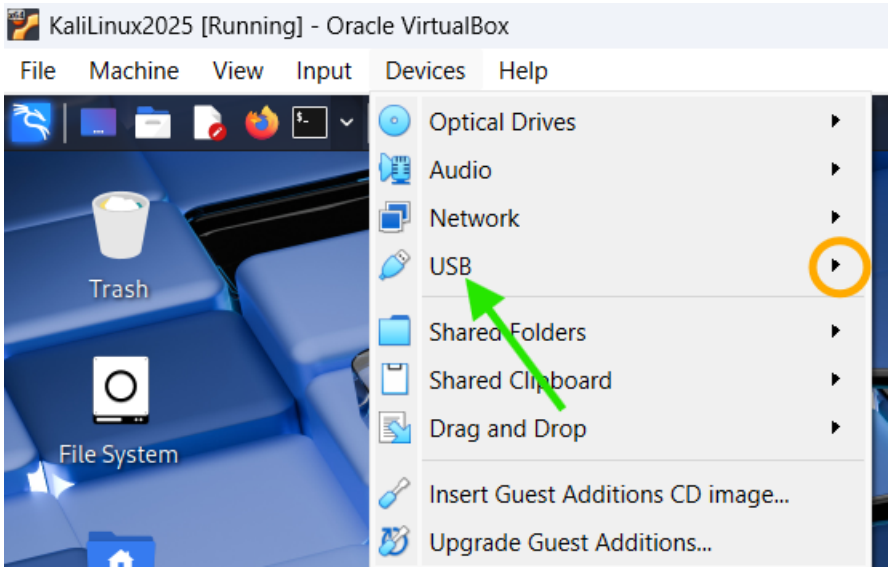
Command 15:



Verified device conectivity:

Connect your android device with help of data cable with laptop/computer.

Then go to Device > USB > [your device]



Click on your respective device.

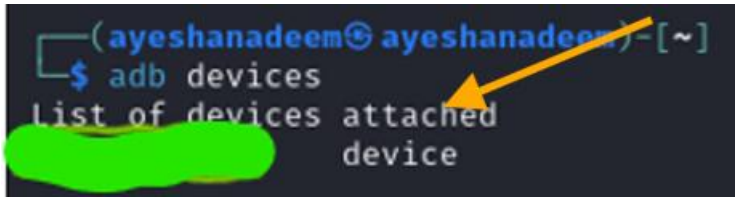
Command 16:

```
┌──(ayeshanadeem㉿ayeshanadeem)-[~]
└─$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 80ee:0021 VirtualBox USB Tablet
Bus 001 Device 005: ID 04e8:6860 Samsung Electronics Co., Ltd Galaxy series, misc. (MTP mode)
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
```

Command 17:

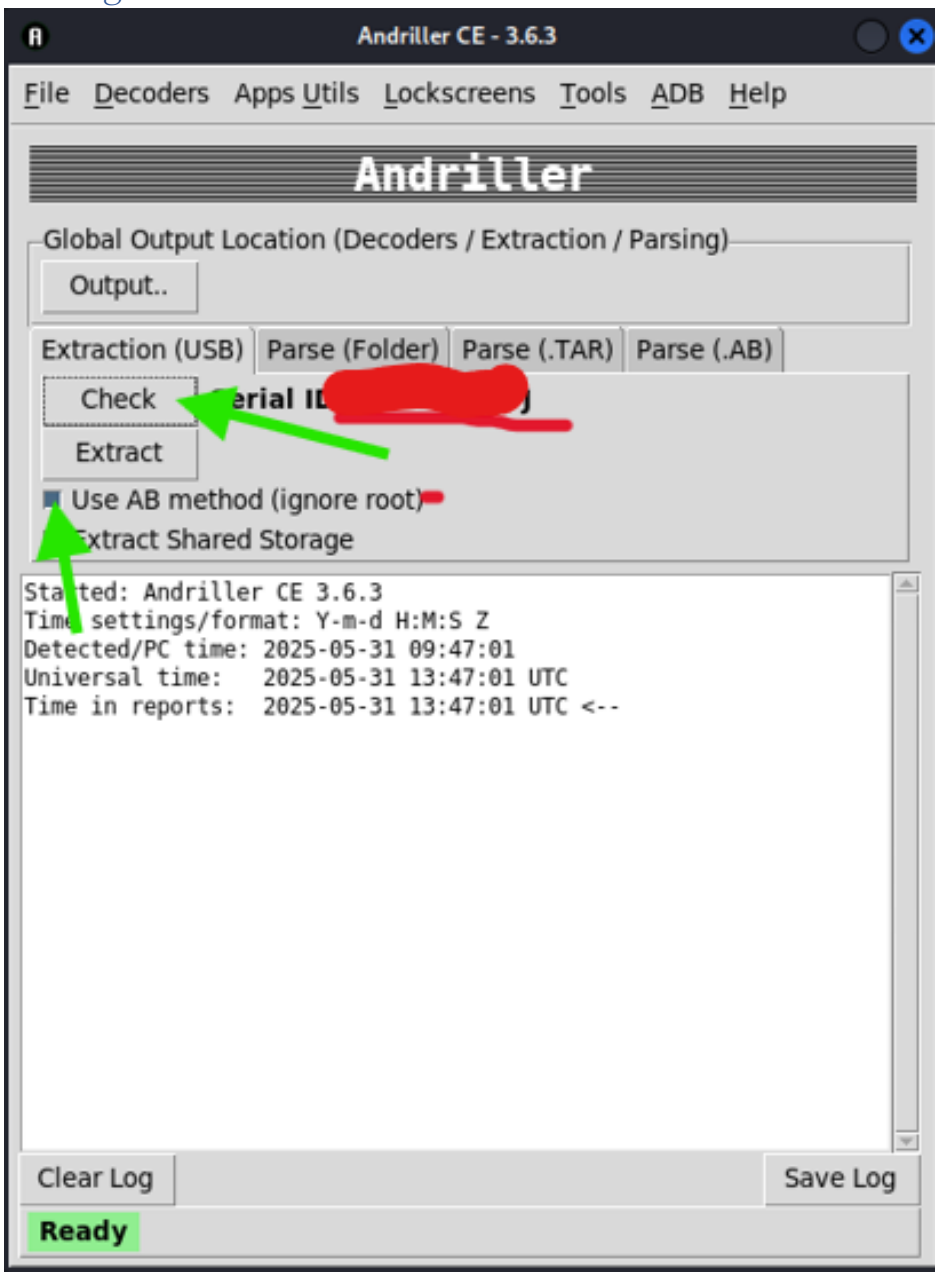
To recognize device in andriller, you need to enable developers mode from your mobile.

Command 18:

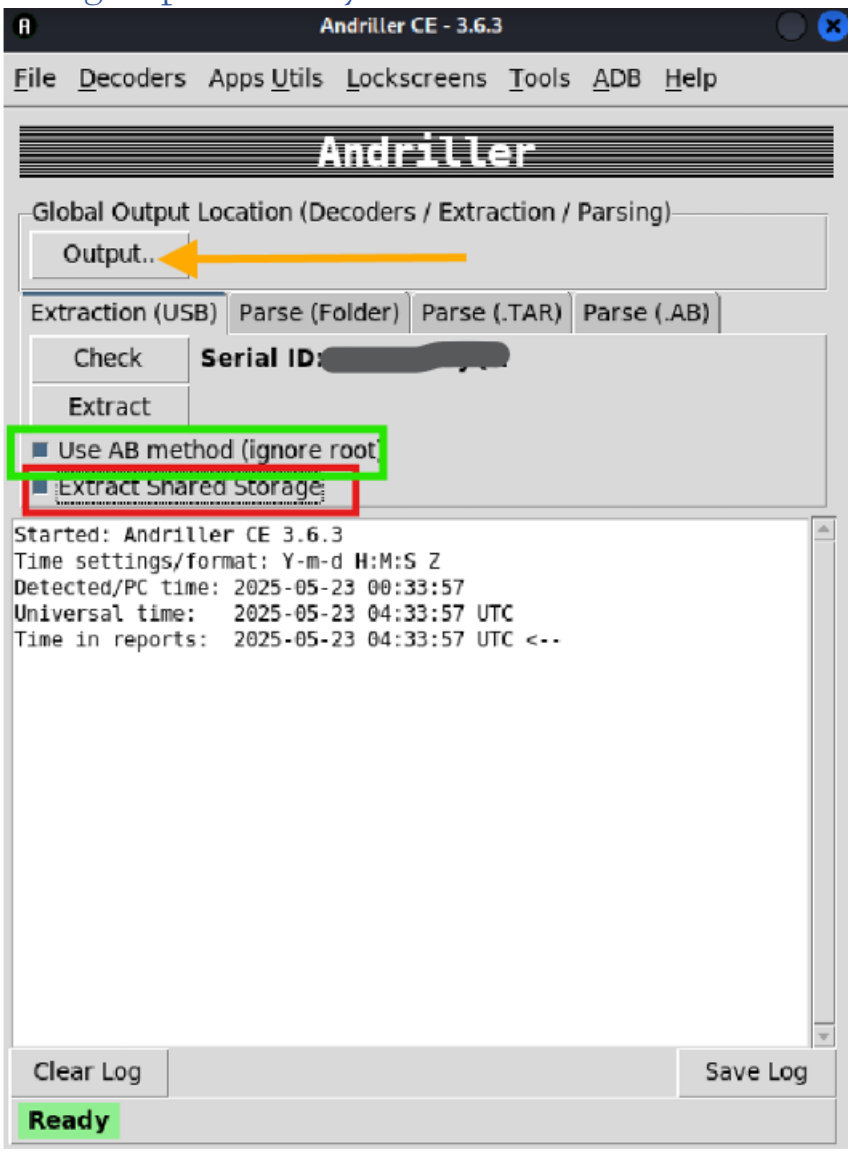


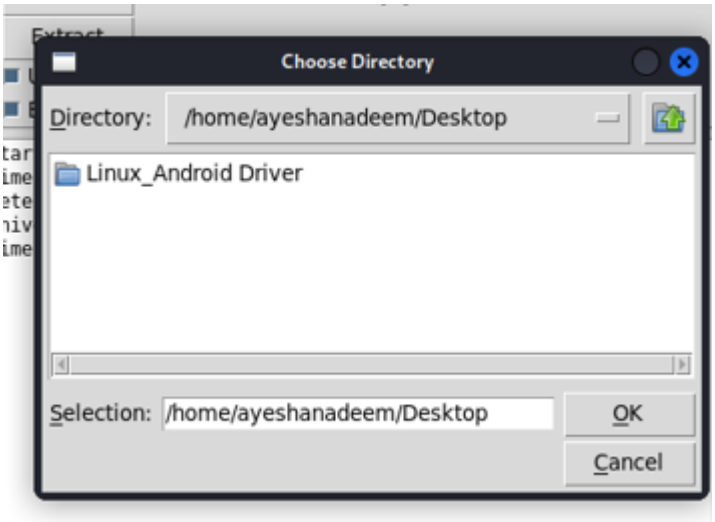
Starting Penetration Test:

Getting serial ID



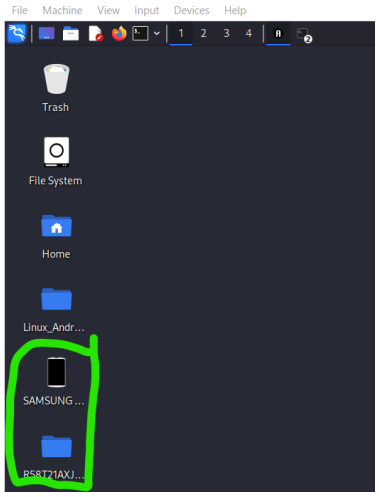
Saving output directory:



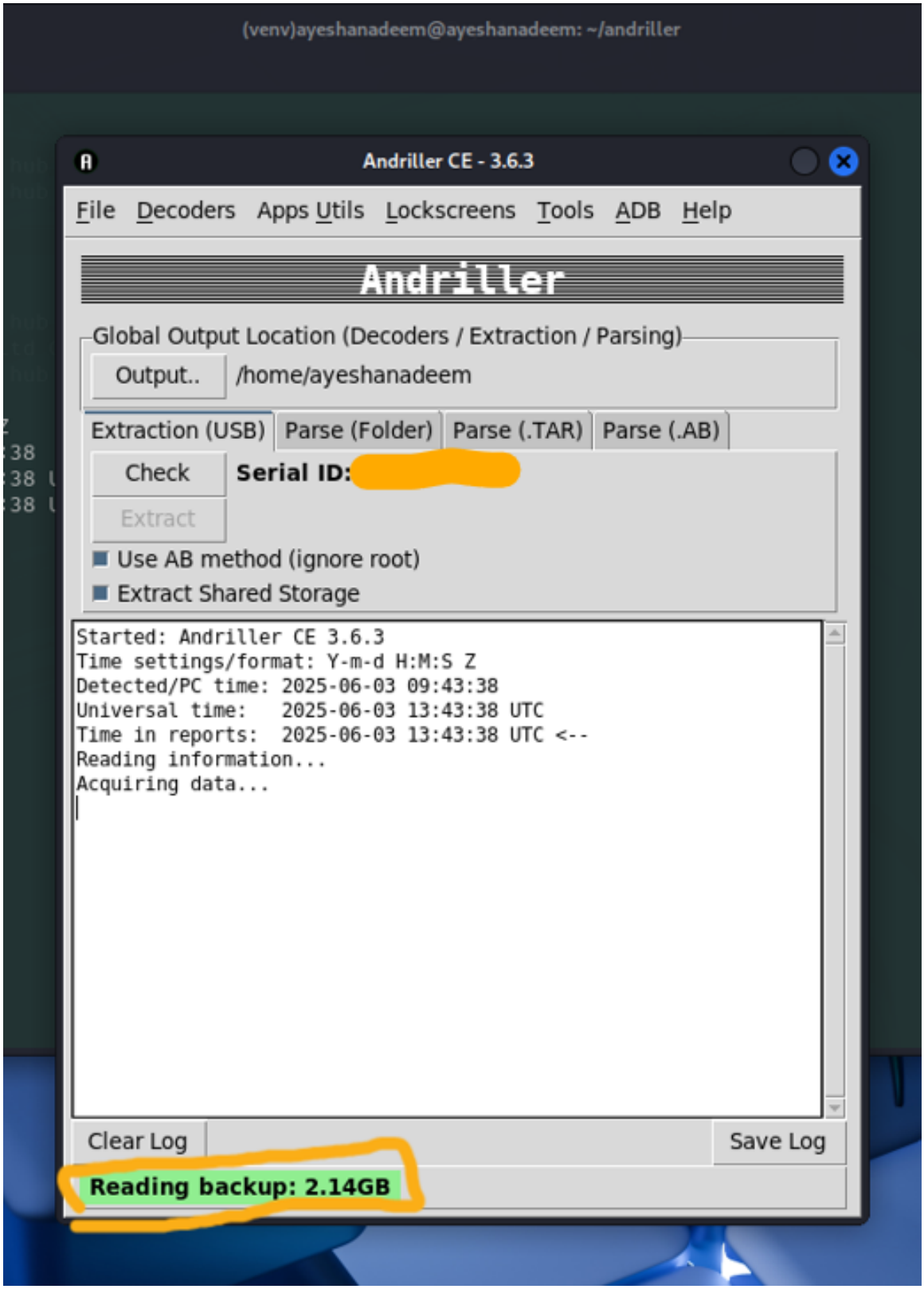


Save it to desktop, so when all data is extracted from android device it will save here.

Note: Use a device having less amount (GBs) data for testing, making extraction faster.



Extract Data:



Final Result in andriller browser

This report was generated using Andriller CE # (This field is editable in Preferences)

[Andriller Report]

Type	Data
Serial	[redacted]
Status	device
Permisson	shell
Wifi Mac	02:00:00:00:00:00
Local_Time	[redacted]
Device_Time	[redacted]
Accounts	• com.osp.app.signin: [redacted] • com.samsung.android.mobileservice[redacted] • com.samsung.android.coreapps[redacted] • com.google[redacted] • com.google:[redacted] • com.google[redacted] • com.google:[redacted] • com.google:[redacted] • com.google[redacted] • com.google[redacted] • com.google[redacted] • com.whatsapp: WhatsApp • com.twitter.android.auth.login: [redacted] • com.facebook.auth.login: Facebook • com.facebook.auth.login:[redacted] • com.whatsapp.w4[redacted] • org.telegram.messenger[redacted] • com.yandex.passpor[redacted] • com.google.android.apps[redacted] • com.imo.android.imoim: imo • com.microsoft.workaccount.ltw[redacted] • com.microsoft.workaccount.ltw[redacted] • im.thebot.messenge[redacted] • com.microsoft.skydrive[redacted] • com.microsoft.office:[redacted] • com.facebook.messenger:[redacted] • www.instagram.com:[redacted] • com.osp.app.signi[redacted]

 # andriller.com # (This field is editable in Preferences)