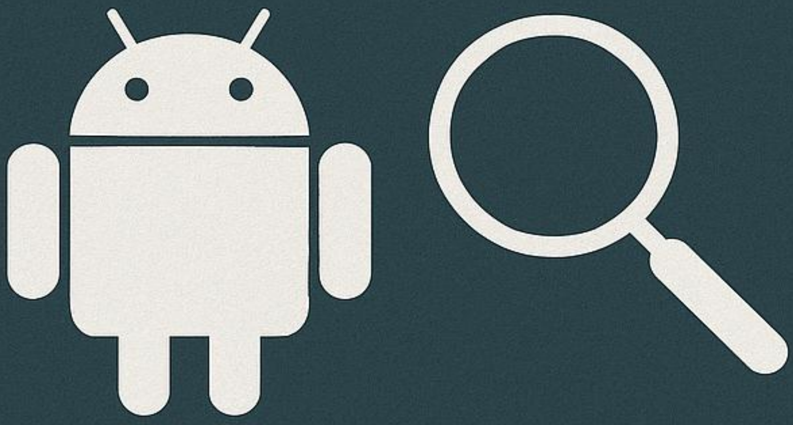
# Android Penetration Testing and Forensics



MADE BY

**Moeez Javed**

# 📱 Mobile Penetration Testing Manual

## 🔰 Introduction

Mobile devices have become a primary target for attackers due to their widespread usage and storage of sensitive personal data. This manual serves as a professional guide for conducting penetration testing on Android mobile devices using Kali or Parrot Linux environments. It outlines necessary configurations, installations, tools (such as **Drozer**, **APKTool**, and **Andriller**), and commands, while also explaining their purposes and use cases.

The goal is to provide a step-by-step, professional-grade workflow for ethical hackers, security testers, and learners interested in mobile application security.

---

⚙ Device Preparation

✅ Enable Developer Mode on Android

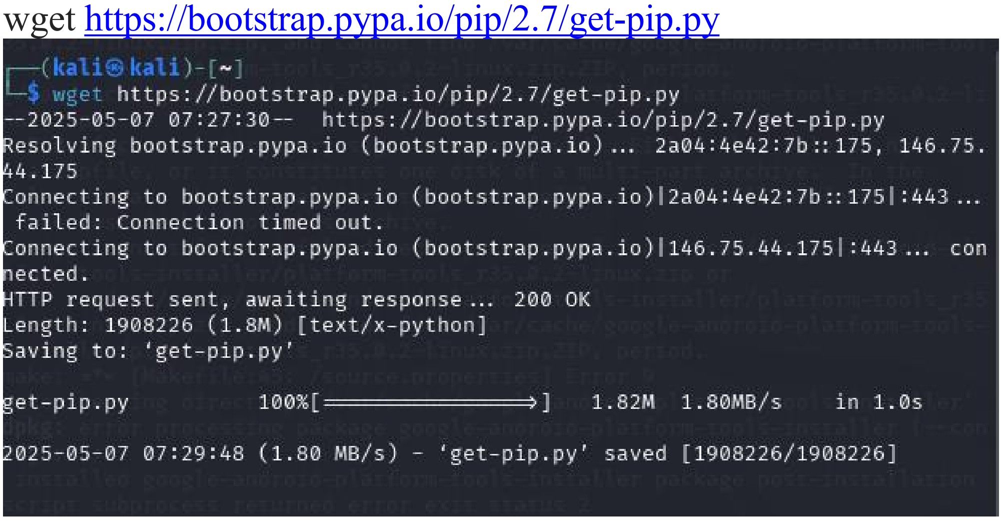
In your phone
Setting -> About Phone -> Build Number -> Tap 7 times -> Developer Setting mode turned on -> Go to USB Debug -> Enabled.

Enabling **Developer Options** allows USB debugging, which is essential for direct device interaction during testing.

Tool Setup and Installation

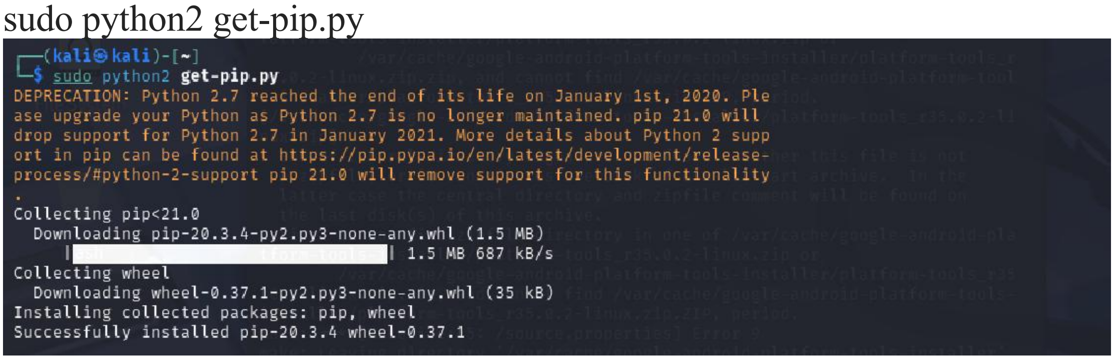
🔧 1. Drozer

Drozer is a comprehensive security testing framework for Android.
Now in Kali linux
wget https://bootstrap.pypa.io/pip/2.7/get-pip.py



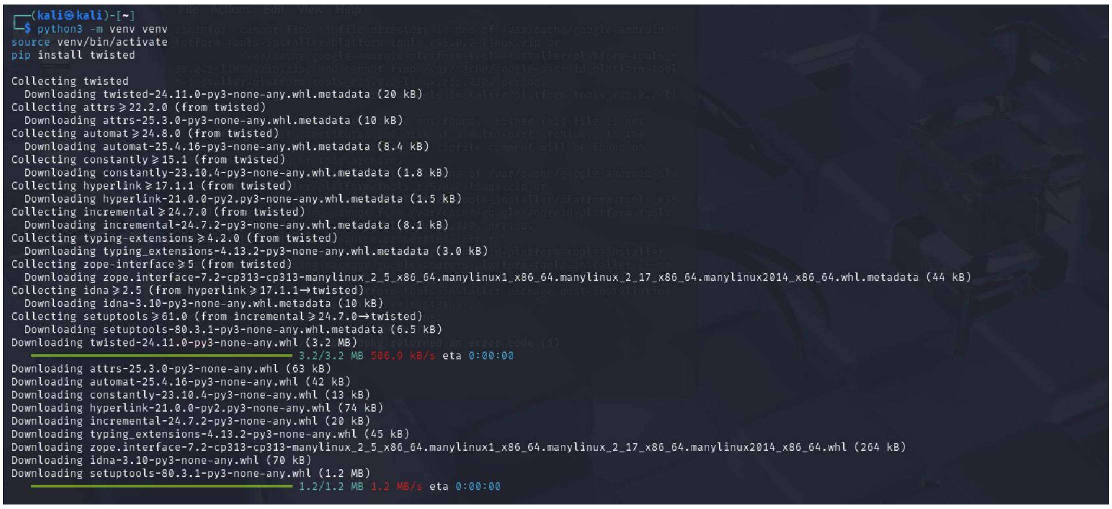
```
┌──(kali㉿kali)-[~]
└─$ wget https://bootstrap.pypa.io/pip/2.7/get-pip.py
--2025-05-07 07:27:30--  https://bootstrap.pypa.io/pip/2.7/get-pip.py
Resolving bootstrap.pypa.io (bootstrap.pypa.io)... 2a04:4e42:7b::175, 146.75.
44.175
Connecting to bootstrap.pypa.io (bootstrap.pypa.io)|2a04:4e42:7b::175|:443...
 failed: Connection timed out.
Connecting to bootstrap.pypa.io (bootstrap.pypa.io)|146.75.44.175|:443... con
nected.
HTTP request sent, awaiting response... 200 OK
Length: 1908226 (1.8M) [text/x-python]
Saving to: ‘get-pip.py’

get-pip.py          100%[===================>]   1.82M  1.80MB/s    in 1.0s

2025-05-07 07:29:48 (1.80 MB/s) - ‘get-pip.py’ saved [1908226/1908226]
```

sudo python2 get-pip.py



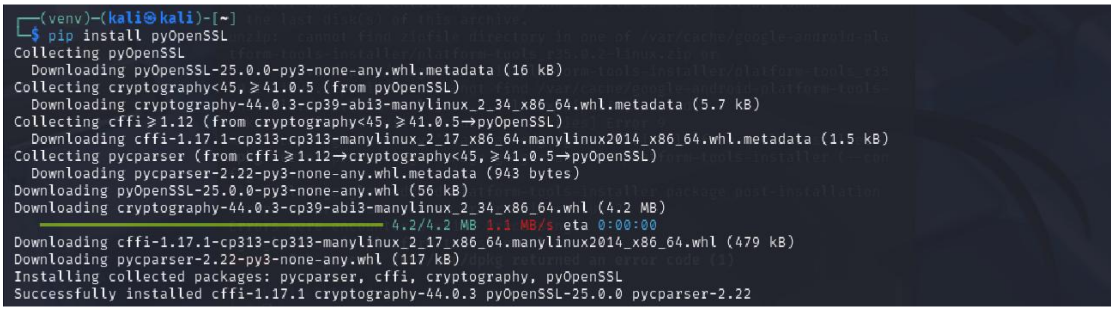
```
┌──(kali㉿kali)-[~]
└─$ sudo python2 get-pip.py
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Ple
ase upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will
drop support for Python 2.7 in January 2021. More details about Python 2 supp
ort in pip can be found at https://pip.pypa.io/en/latest/development/release-
process/#python-2-support pip 21.0 will remove support for this functionality
.
Collecting pip<21.0
  Downloading pip-20.3.4-py2.py3-none-any.whl (1.5 MB)
     |████████████████████████████████| 1.5 MB 687 kB/s
Collecting wheel
  Downloading wheel-0.37.1-py2.py3-none-any.whl (35 kB)
Installing collected packages: pip, wheel
Successfully installed pip-20.3.4 wheel-0.37.1
```

python3 -m venv venv
source venv/bin/activate
pip install twisted



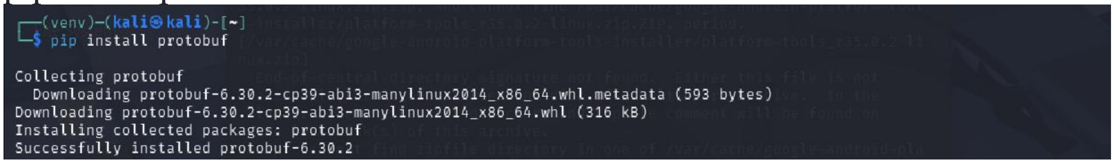
```
┌──(kali㉿kali)-[~]
└─$ python3 -m venv venv
source venv/bin/activate
pip install twisted

Collecting twisted
  Downloading twisted-24.11.0-py3-none-any.whl.metadata (20 kB)
Collecting attrs>=22.2.0 (from twisted)
  Downloading attrs-25.3.0-py3-none-any.whl.metadata (10 kB)
Collecting automat>=24.8.0 (from twisted)
  Downloading automat-25.4.16-py3-none-any.whl.metadata (8.4 kB)
Collecting constantly>=15.1 (from twisted)
  Downloading constantly-23.10.4-py3-none-any.whl.metadata (1.8 kB)
Collecting hyperlink>=17.1.1 (from twisted)
  Downloading hyperlink-21.0.0-py2.py3-none-any.whl.metadata (1.5 kB)
Collecting incremental>=24.7.0 (from twisted)
  Downloading incremental-24.7.2-py3-none-any.whl.metadata (8.1 kB)
Collecting typing-extensions>=4.2.0 (from twisted)
  Downloading typing_extensions-4.13.2-py3-none-any.whl.metadata (3.0 kB)
Collecting zope-interface>=5 (from twisted)
  Downloading zope.interface-7.2-cp313-cp313-manylinux_2_5_x86_64.manylinux1_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (44 kB)
Collecting idna>=2.5 (from hyperlink>=17.1.1->twisted)
  Downloading idna-3.10-py3-none-any.whl.metadata (10 kB)
Collecting setuptools>=61.0 (from incremental>=24.7.0->twisted)
  Downloading setuptools-80.3.1-py3-none-any.whl.metadata (6.5 kB)
Downloading twisted-24.11.0-py3-none-any.whl (3.2 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 3.2/3.2 MB 506.9 kB/s eta 0:00:00
Downloading attrs-25.3.0-py3-none-any.whl (63 kB)
Downloading automat-25.4.16-py3-none-any.whl (42 kB)
Downloading constantly-23.10.4-py3-none-any.whl (13 kB)
Downloading hyperlink-21.0.0-py2.py3-none-any.whl (74 kB)
Downloading incremental-24.7.2-py3-none-any.whl (20 kB)
Downloading typing_extensions-4.13.2-py3-none-any.whl (45 kB)
Downloading zope.interface-7.2-cp313-cp313-manylinux_2_5_x86_64.manylinux1_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl (264 kB)
Downloading idna-3.10-py3-none-any.whl (70 kB)
Downloading setuptools-80.3.1-py3-none-any.whl (1.2 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.2/1.2 MB 1.2 MB/s eta 0:00:00
```

pip install pyOpenSSL



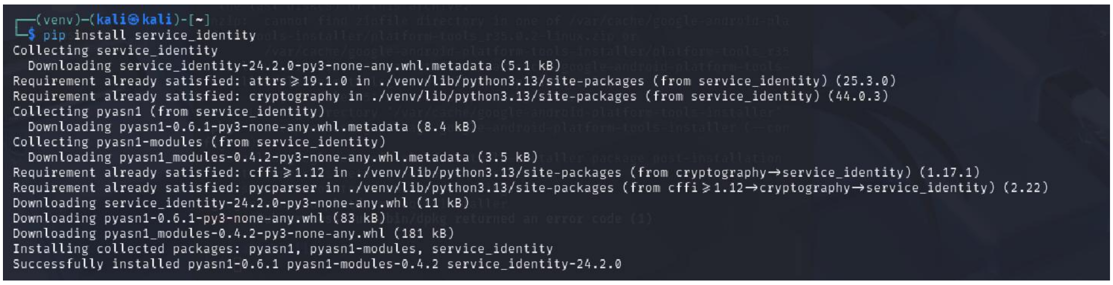
```
┌──(venv)─(kali㉿kali)-[~]
└─$ pip install pyOpenSSL
Collecting pyOpenSSL
  Downloading pyOpenSSL-25.0.0-py3-none-any.whl.metadata (16 kB)
Collecting cryptography<45,>=41.0.5 (from pyOpenSSL)
  Downloading cryptography-44.0.3-cp39-abi3-manylinux_2_34_x86_64.whl.metadata (5.7 kB)
Collecting cffi>=1.12 (from cryptography<45,>=41.0.5->pyOpenSSL)
  Downloading cffi-1.17.1-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (1.5 kB)
Collecting pycparser (from cffi>=1.12->cryptography<45,>=41.0.5->pyOpenSSL)
  Downloading pycparser-2.22-py3-none-any.whl.metadata (943 bytes)
Downloading pyOpenSSL-25.0.0-py3-none-any.whl (56 kB)
Downloading cryptography-44.0.3-cp39-abi3-manylinux_2_34_x86_64.whl (4.2 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 4.2/4.2 MB 1.1 MB/s eta 0:00:00
Downloading cffi-1.17.1-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (479 kB)
Downloading pycparser-2.22-py3-none-any.whl (117 kB)
Installing collected packages: pycparser, cffi, cryptography, pyOpenSSL
Successfully installed cffi-1.17.1 cryptography-44.0.3 pyOpenSSL-25.0.0 pycparser-2.22
```

pip install protobuf



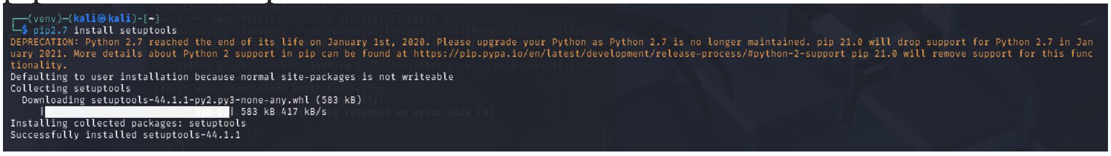
```
┌──(venv)─(kali㉿kali)-[~]
└─$ pip install protobuf

Collecting protobuf
  Downloading protobuf-6.30.2-cp39-abi3-manylinux2014_x86_64.whl.metadata (593 bytes)
Downloading protobuf-6.30.2-cp39-abi3-manylinux2014_x86_64.whl (316 kB)
Installing collected packages: protobuf
Successfully installed protobuf-6.30.2
```

pip install service_identity



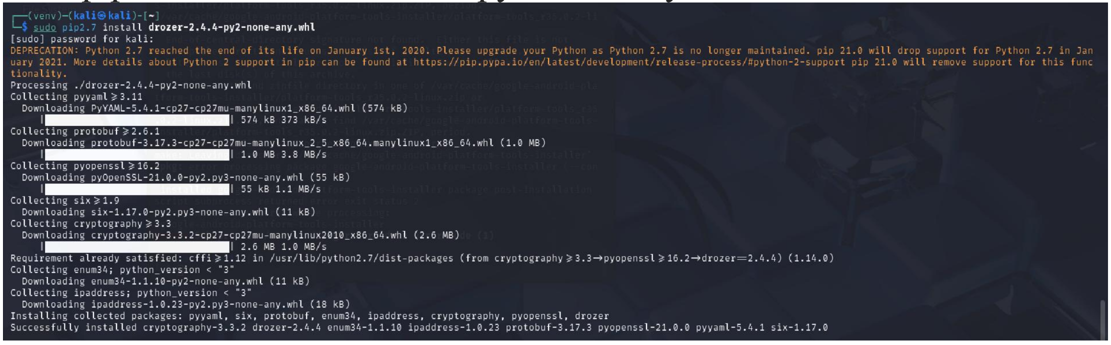
```
┌──(venv)─(kali㉿kali)-[~]
└─$ pip install service_identity
Collecting service_identity
  Downloading service_identity-24.2.0-py3-none-any.whl.metadata (5.1 kB)
Requirement already satisfied: attrs≥19.1.0 in ./venv/lib/python3.13/site-packages (from service_identity) (25.3.0)
Requirement already satisfied: cryptography in ./venv/lib/python3.13/site-packages (from service_identity) (44.0.3)
Collecting pyasn1 (from service_identity)
  Downloading pyasn1-0.6.1-py3-none-any.whl.metadata (8.4 kB)
Collecting pyasn1-modules (from service_identity)
  Downloading pyasn1_modules-0.4.2-py3-none-any.whl.metadata (3.5 kB)
Requirement already satisfied: cffi≥1.12 in ./venv/lib/python3.13/site-packages (from cryptography→service_identity) (1.17.1)
Requirement already satisfied: pycparser in ./venv/lib/python3.13/site-packages (from cffi≥1.12→cryptography→service_identity) (2.22)
Downloading service_identity-24.2.0-py3-none-any.whl (11 kB)
Downloading pyasn1-0.6.1-py3-none-any.whl (83 kB)
Downloading pyasn1_modules-0.4.2-py3-none-any.whl (181 kB)
Installing collected packages: pyasn1, pyasn1-modules, service_identity
Successfully installed pyasn1-0.6.1 pyasn1-modules-0.4.2 service_identity-24.2.0
```

pip2.7 install setuptools



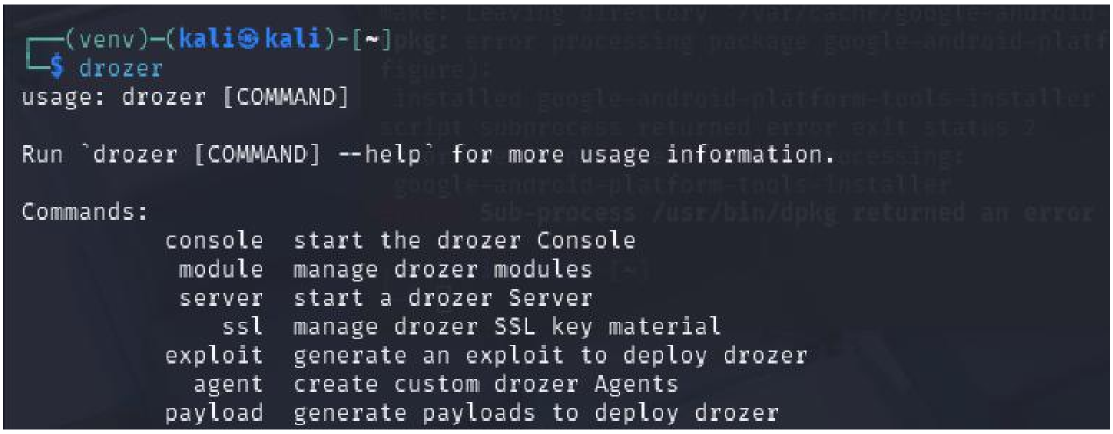
```
┌──(venv)─(kali㉿kali)-[~]
└─$ pip2.7 install setuptools
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in Jan
uary 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this func
tionality.
Defaulting to user installation because normal site-packages is not writeable
Collecting setuptools
  Downloading setuptools-44.1.1-py2.py3-none-any.whl (583 kB)
     |████████████████████████████████| 583 kB 417 kB/s
Installing collected packages: setuptools
Successfully installed setuptools-44.1.1
```

sudo pip2.7 install drozer-2.4.4-py2-none-any.whl



```
┌──(venv)─(kali㉿kali)-[~]
└─$ sudo pip2.7 install drozer-2.4.4-py2-none-any.whl
[sudo] password for kali:
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in Jan
uary 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this func
tionality.
Processing ./drozer-2.4.4-py2-none-any.whl
Collecting pyyaml≥3.11
  Downloading PyYAML-5.4.1-cp27-cp27mu-manylinux1_x86_64.whl (574 kB)
     |████████████████████████████████| 574 kB 373 kB/s
Collecting protobuf≥2.6.1
  Downloading protobuf-3.17.3-cp27-cp27mu-manylinux_2_5_x86_64.manylinux1_x86_64.whl (1.0 MB)
     |████████████████████████████████| 1.0 MB 3.8 MB/s
Collecting pyopenssl≥16.2
  Downloading pyOpenSSL-21.0.0-py2.py3-none-any.whl (55 kB)
     |████████████████████████████████| 55 kB 1.1 MB/s
Collecting six≥1.9
  Downloading six-1.17.0-py2.py3-none-any.whl (11 kB)
Collecting cryptography≥3.3
  Downloading cryptography-3.3.2-cp27-cp27mu-manylinux2010_x86_64.whl (2.6 MB)
     |████████████████████████████████| 2.6 MB 1.0 MB/s
Requirement already satisfied: cffi≥1.12 in /usr/lib/python2.7/dist-packages (from cryptography≥3.3→pyopenssl≥16.2→drozer==2.4.4) (1.14.0)
Collecting enum34; python_version < "3"
  Downloading enum34-1.1.10-py2-none-any.whl (11 kB)
Collecting ipaddress; python_version < "3"
  Downloading ipaddress-1.0.23-py2.py3-none-any.whl (18 kB)
Installing collected packages: pyyaml, six, protobuf, enum34, ipaddress, cryptography, pyopenssl, drozer
Successfully installed cryptography-3.3.2 drozer-2.4.4 enum34-1.1.10 ipaddress-1.0.23 protobuf-3.17.3 pyopenssl-21.0.0 pyyaml-5.4.1 six-1.17.0
```

drozer

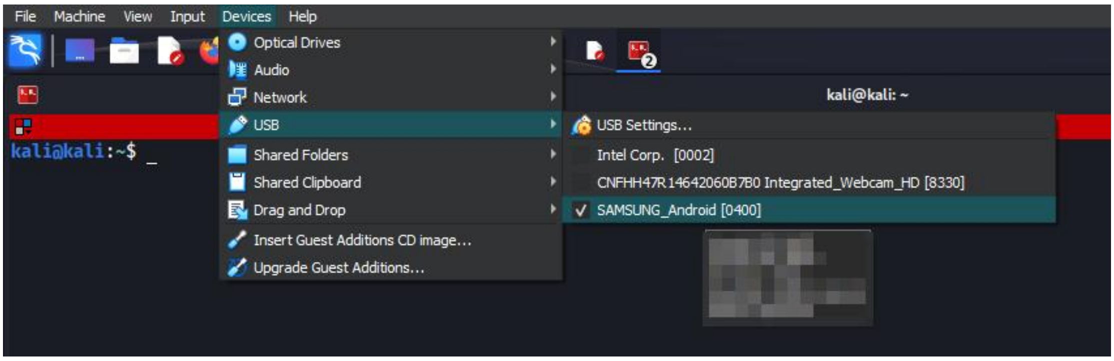


```
┌──(venv)─(kali㉿kali)-[~]
└─$ drozer
usage: drozer [COMMAND]

Run `drozer [COMMAND] --help` for more usage information.

Commands:
          console  start the drozer Console
           module  manage drozer modules
           server  start a drozer Server
              ssl  manage drozer SSL key material
          exploit  generate an exploit to deploy drozer
            agent  create custom drozer Agents
          payload  generate payloads to deploy drozer
```

First, We have to install the Drozer agent(drozer-agent.apk) on the Android device we are using, so the drozer client can connect to the server.

Then connect to the Android device through USB and check whether it’s connected by ADB.

Note: You have to select the device on your virtual box via the Devices tab.

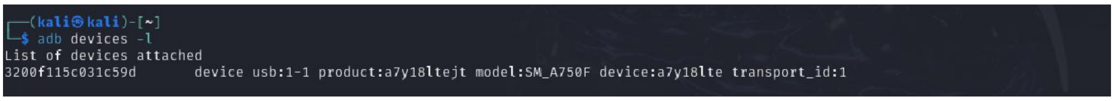


[redacted]

```
kali@kali:~$ _
```

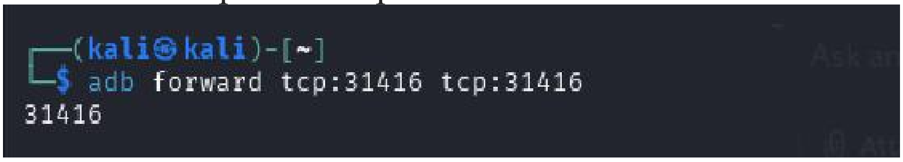
## 💻 Connect Android Device via ADB

adb devices -l



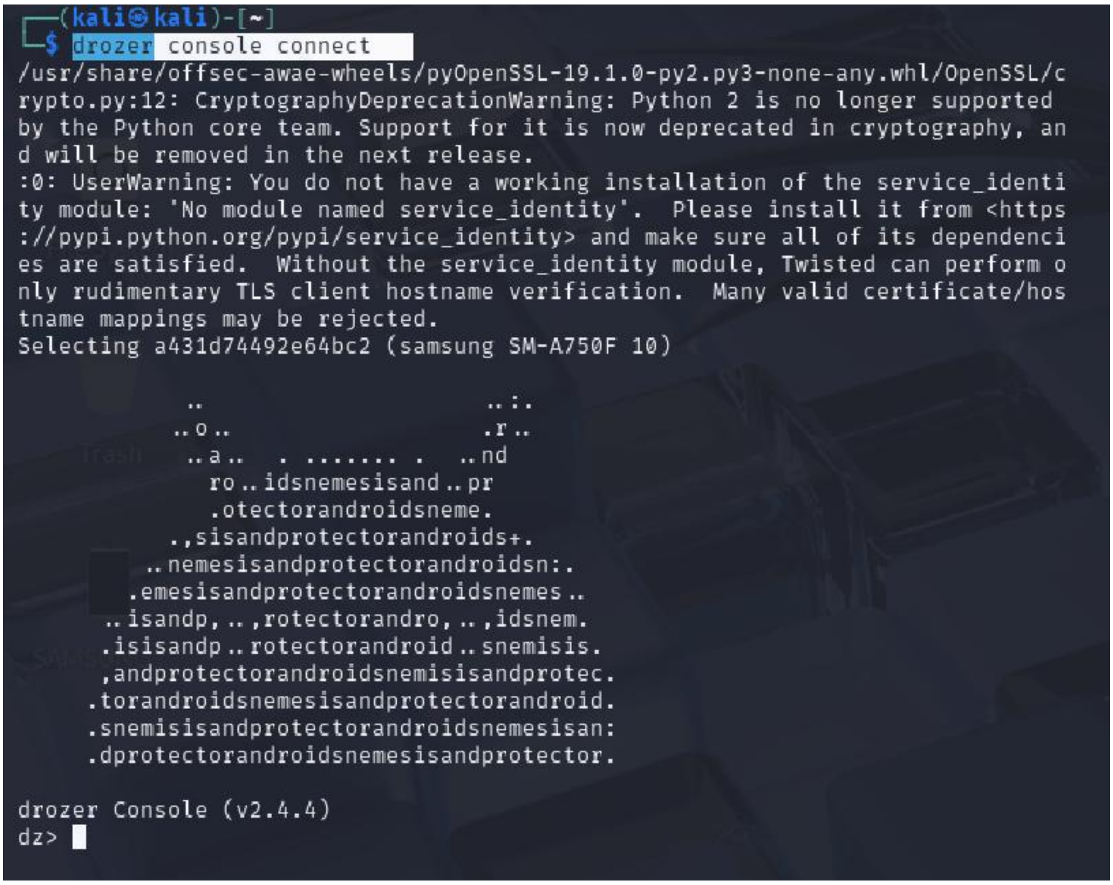
```
┌──(kali㉿kali)-[~]
└─$ adb devices -l
List of devices attached
3200f115c031c59d       device usb:1-1 product:a7y18ltejt model:SM_A750F device:a7y18lte transport_id:1
```

adb forward tcp:31415 tcp:31415



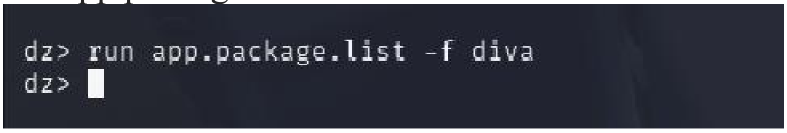
```
┌──(kali㉿kali)-[~]
└─$ adb forward tcp:31416 tcp:31416
31416
```

drozer console connect



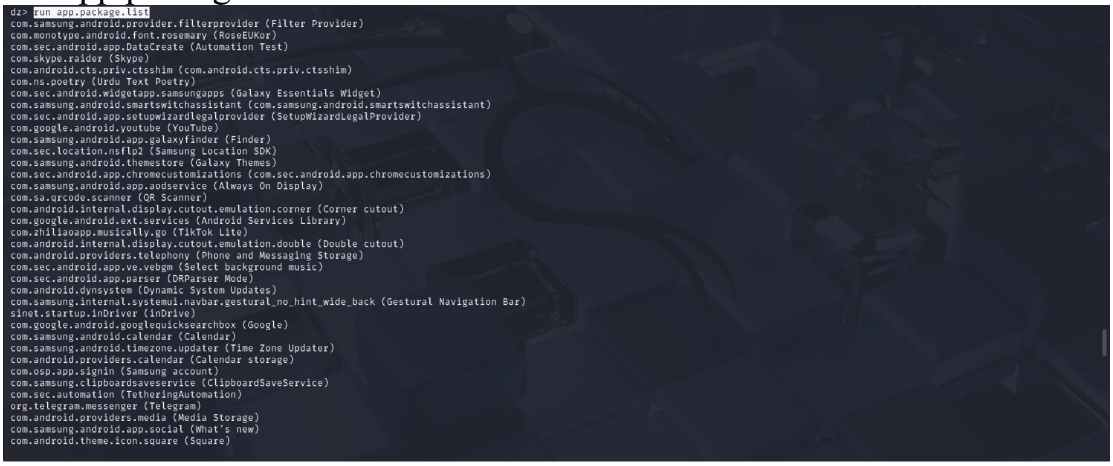
```
┌──(kali㉿kali)-[~]
└─$ drozer console connect
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/c
rypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported
by the Python core team. Support for it is now deprecated in cryptography, an
d will be removed in the next release.
:0: UserWarning: You do not have a working installation of the service_identi
ty module: 'No module named service_identity'.  Please install it from <https
://pypi.python.org/pypi/service_identity> and make sure all of its dependenci
es are satisfied.  Without the service_identity module, Twisted can perform o
nly rudimentary TLS client hostname verification.  Many valid certificate/hos
tname mappings may be rejected.
Selecting a431d74492e64bc2 (samsung SM-A750F 10)

             ..                    ..:.
            ..o..                  .r..
             ..a..  . ....... .   ..nd
               ro..idsnemesisand..pr
               .otectorandroidsneme.
            .,sisandprotectorandroids+.
          ..nemesisandprotectorandroidsn:.
         .emesisandprotectorandroidsnemes..
       ..isandp,..,rotectorandro,..,idsnem.
      .isisandp..rotectorandroid..snemisis.
      ,andprotectorandroidsnemisisandprotec.
     .torandroidsnemesisandprotectorandroid.
     .snemisisandprotectorandroidsnemesisan:
     .dprotectorandroidsnemesisandprotector.

drozer Console (v2.4.4)
dz> █
```

run app.package.list -f diva



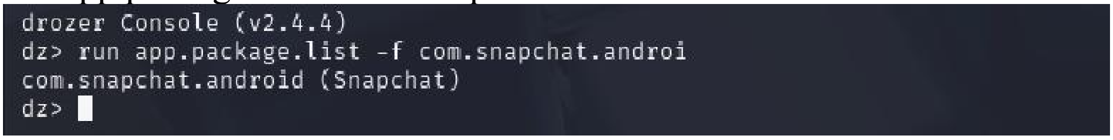
```
dz> run app.package.list -f diva
dz> █
```

run app.package.list



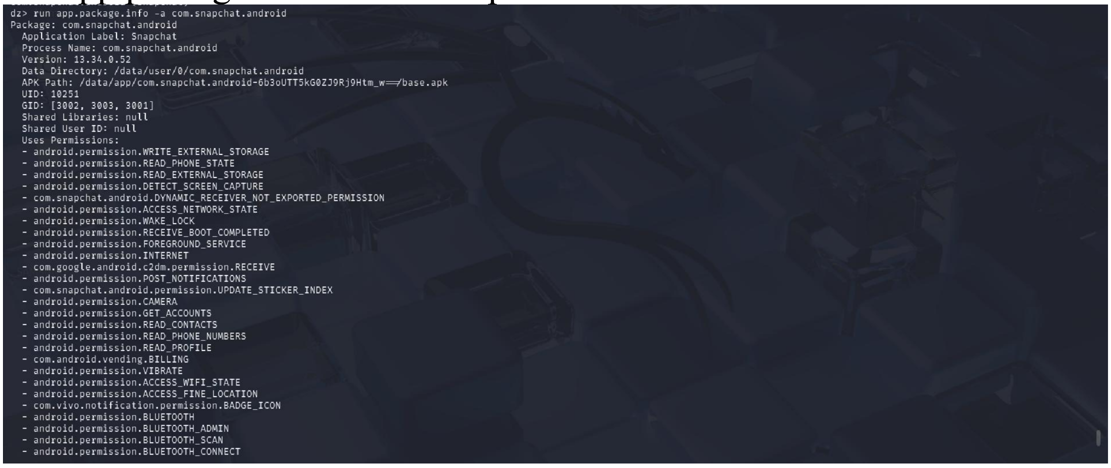
```
dz> run app.package.list
com.samsung.android.provider.filterprovider (Filter Provider)
com.monotype.android.font.rosemary (RoseEUKor)
com.sec.android.app.DataCreate (Automation Test)
com.skype.raider (Skype)
com.android.cts.priv.ctsshim (com.android.cts.priv.ctsshim)
com.ns.poetry (Urdu Text Poetry)
com.sec.android.widgetapp.samsungapps (Galaxy Essentials Widget)
com.samsung.android.smartswitchassistant (com.samsung.android.smartswitchassistant)
com.sec.android.app.setupwizardlegalprovider (SetupWizardLegalProvider)
com.google.android.youtube (YouTube)
com.samsung.android.app.galaxyfinder (Finder)
com.sec.location.nsflp2 (Samsung Location SDK)
com.samsung.android.themestore (Galaxy Themes)
com.sec.android.app.chromecustomizations (com.sec.android.app.chromecustomizations)
com.samsung.android.app.aodservice (Always On Display)
com.sa.qrcode.scanner (QR Scanner)
com.android.internal.display.cutout.emulation.corner (Corner cutout)
com.google.android.ext.services (Android Services Library)
com.zhiliaoapp.musically.go (TikTok Lite)
com.android.internal.display.cutout.emulation.double (Double cutout)
com.android.providers.telephony (Phone and Messaging Storage)
com.sec.android.app.ve.vebgm (Select background music)
com.sec.android.app.parser (DRParser Mode)
com.android.dynsystem (Dynamic System Updates)
com.samsung.internal.systemui.navbar.gestural_no_hint_wide_back (Gestural Navigation Bar)
sinet.startup.inDriver (inDrive)
com.google.android.googlequicksearchbox (Google)
com.samsung.android.calendar (Calendar)
com.samsung.android.timezone.updater (Time Zone Updater)
com.android.providers.calendar (Calendar storage)
com.osp.app.signin (Samsung account)
com.samsung.clipboardsaveservice (ClipboardSaveService)
com.sec.automation (TetheringAutomation)
org.telegram.messenger (Telegram)
com.android.providers.media (Media Storage)
com.samsung.android.app.social (What's new)
com.android.theme.icon.square (Square)
```

run app.package.list -f com.snapchat.android



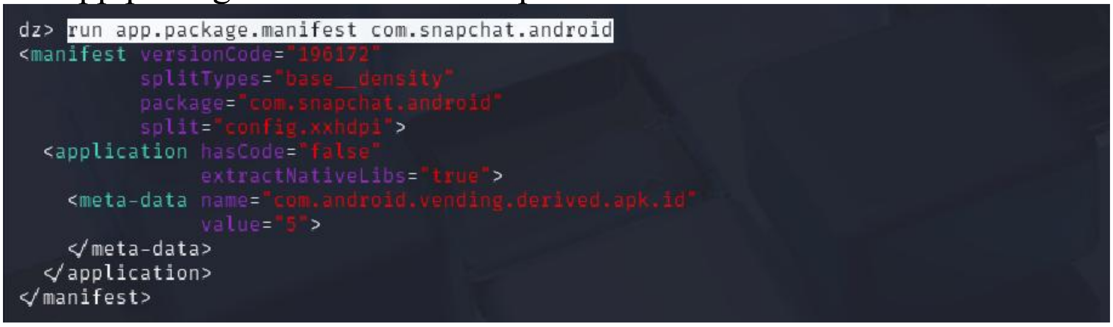
```
drozer Console (v2.4.4)
dz> run app.package.list -f com.snapchat.androi
com.snapchat.android (Snapchat)
dz> █
```

run app.package.info -a com.snapchat.android



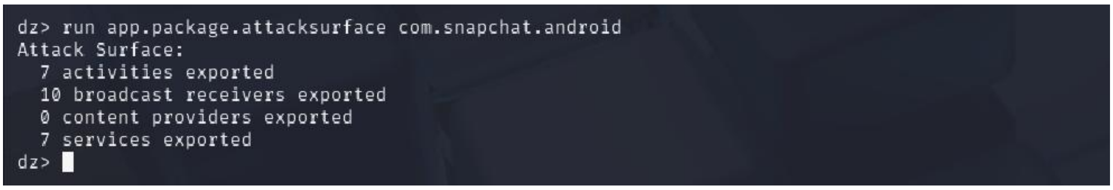
```
dz> run app.package.info -a com.snapchat.android
Package: com.snapchat.android
  Application Label: Snapchat
  Process Name: com.snapchat.android
  Version: 13.34.0.52
  Data Directory: /data/user/0/com.snapchat.android
  APK Path: /data/app/com.snapchat.android-6b3oUTT5kG0ZJ9Rj9Htm_w==/base.apk
  UID: 10251
  GID: [3002, 3003, 3001]
  Shared Libraries: null
  Shared User ID: null
  Uses Permissions:
  - android.permission.WRITE_EXTERNAL_STORAGE
  - android.permission.READ_PHONE_STATE
  - android.permission.READ_EXTERNAL_STORAGE
  - android.permission.DETECT_SCREEN_CAPTURE
  - com.snapchat.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION
  - android.permission.ACCESS_NETWORK_STATE
  - android.permission.WAKE_LOCK
  - android.permission.RECEIVE_BOOT_COMPLETED
  - android.permission.FOREGROUND_SERVICE
  - android.permission.INTERNET
  - com.google.android.c2dm.permission.RECEIVE
  - android.permission.POST_NOTIFICATIONS
  - com.snapchat.android.permission.UPDATE_STICKER_INDEX
  - android.permission.CAMERA
  - android.permission.GET_ACCOUNTS
  - android.permission.READ_CONTACTS
  - android.permission.READ_PHONE_NUMBERS
  - android.permission.READ_PROFILE
  - com.android.vending.BILLING
  - android.permission.VIBRATE
  - android.permission.ACCESS_WIFI_STATE
  - android.permission.ACCESS_FINE_LOCATION
  - com.vivo.notification.permission.BADGE_ICON
  - android.permission.BLUETOOTH
  - android.permission.BLUETOOTH_ADMIN
  - android.permission.BLUETOOTH_SCAN
  - android.permission.BLUETOOTH_CONNECT
```

run app.package.manifest com.snapchat.android



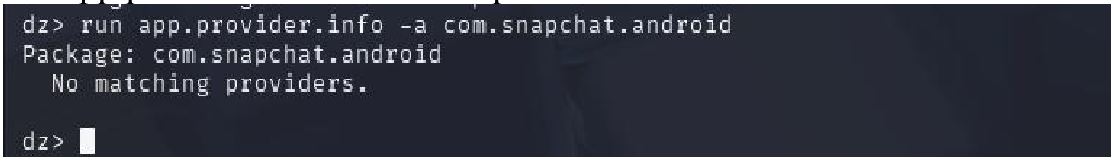
```
dz> run app.package.manifest com.snapchat.android
<manifest versionCode="196172"
          splitTypes="base__density"
          package="com.snapchat.android"
          split="config.xxhdpi">
  <application hasCode="false"
               extractNativeLibs="true">
    <meta-data name="com.android.vending.derived.apk.id"
               value="5">
    </meta-data>
  </application>
</manifest>
```

run app.package.attacksurface com.snapchat.android



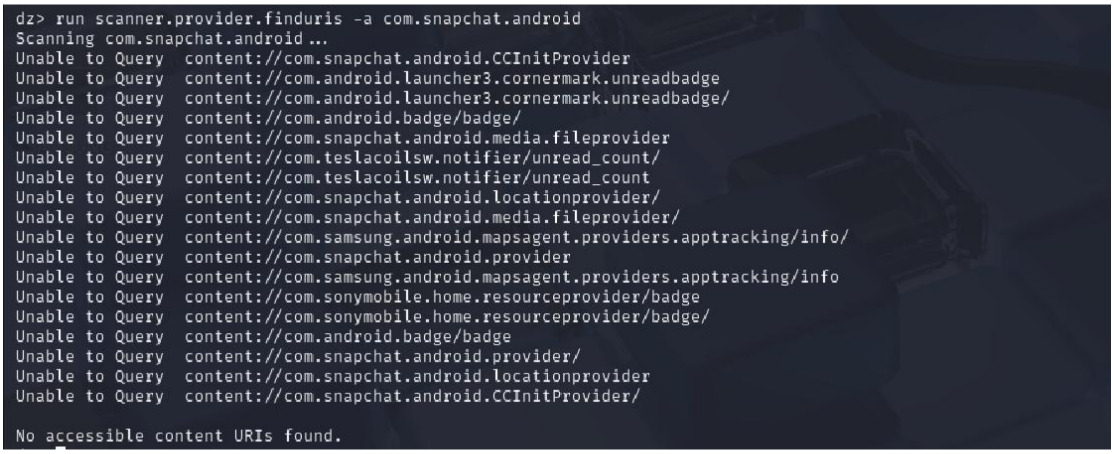
```
dz> run app.package.attacksurface com.snapchat.android
Attack Surface:
  7 activities exported
  10 broadcast receivers exported
  0 content providers exported
  7 services exported
dz> █
```

## run app.provider.info -a com.snapchat.android



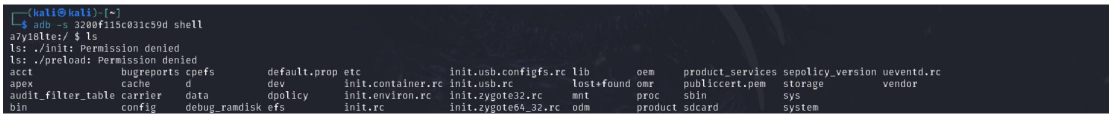
```
dz> run app.provider.info -a com.snapchat.android
Package: com.snapchat.android
  No matching providers.

dz> █
```

## run scanner.provider.finduris -a com.snapchat.android



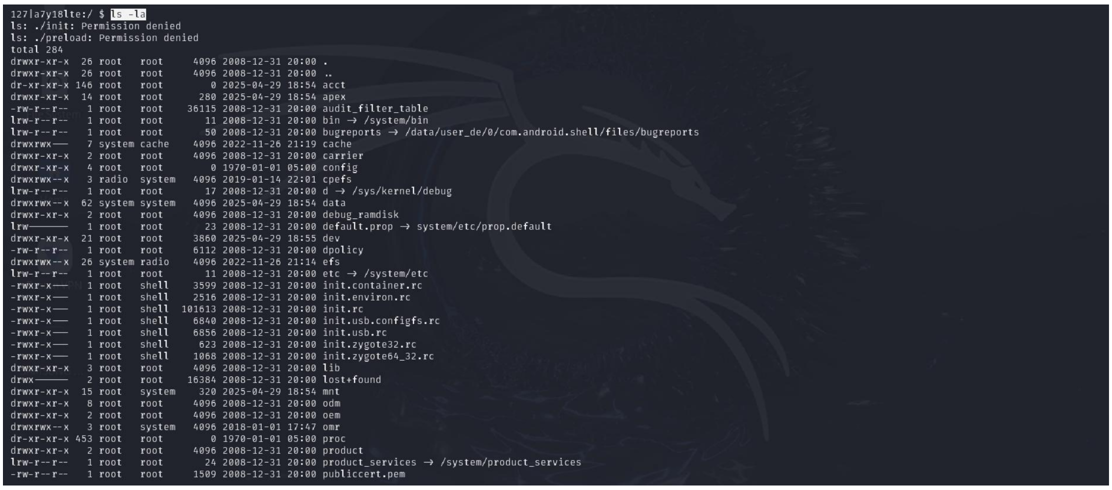
```
dz> run scanner.provider.finduris -a com.snapchat.android
Scanning com.snapchat.android...
Unable to Query  content://com.snapchat.android.CCInitProvider
Unable to Query  content://com.android.launcher3.cornermark.unreadbadge
Unable to Query  content://com.android.launcher3.cornermark.unreadbadge/
Unable to Query  content://com.android.badge/badge/
Unable to Query  content://com.snapchat.android.media.fileprovider
Unable to Query  content://com.teslacoilsw.notifier/unread_count/
Unable to Query  content://com.teslacoilsw.notifier/unread_count
Unable to Query  content://com.snapchat.android.locationprovider/
Unable to Query  content://com.snapchat.android.media.fileprovider/
Unable to Query  content://com.samsung.android.mapsagent.providers.apptracking/info/
Unable to Query  content://com.snapchat.android.provider
Unable to Query  content://com.samsung.android.mapsagent.providers.apptracking/info
Unable to Query  content://com.sonymobile.home.resourceprovider/badge
Unable to Query  content://com.sonymobile.home.resourceprovider/badge/
Unable to Query  content://com.android.badge/badge
Unable to Query  content://com.snapchat.android.provider/
Unable to Query  content://com.snapchat.android.locationprovider
Unable to Query  content://com.snapchat.android.CCInitProvider/

No accessible content URIs found.
```

## adb -s device name shell



```
┌──(kali㉿kali)-[~]
└─$ adb -s 3200f115c031c59d shell
a7y18lte:/ $ ls
ls: ./init: Permission denied
ls: ./preload: Permission denied
acct               bugreports cpefs        default.prop etc                init.usb.configfs.rc lib        oem     product_services sepolicy_version ueventd.rc
apex               cache      d            dev          init.container.rc  init.usb.rc          lost+found omr     publiccert.pem   storage          vendor
audit_filter_table carrier    data         dpolicy      init.environ.rc    init.zygote32.rc     mnt        proc    sbin             sys
bin                config     debug_ramdisk efs         init.rc            init.zygote64_32.rc  odm        product sdcard           system
```

## ls -la



```
127|a7y18lte:/ $ ls -la
ls: ./init: Permission denied
ls: ./preload: Permission denied
total 284
drwxr-xr-x  26 root   root     4096 2008-12-31 20:00 .
drwxr-xr-x  26 root   root     4096 2008-12-31 20:00 ..
dr-xr-xr-x 146 root   root        0 2025-04-29 18:54 acct
drwxr-xr-x  14 root   root      280 2025-04-29 18:54 apex
-rw-r--r--   1 root   root    36115 2008-12-31 20:00 audit_filter_table
lrw-r--r--   1 root   root       11 2008-12-31 20:00 bin -> /system/bin
lrw-r--r--   1 root   root       50 2008-12-31 20:00 bugreports -> /data/user_de/0/com.android.shell/files/bugreports
drwxrwx---   7 system cache    4096 2022-11-26 21:19 cache
drwxr-xr-x   2 root   root     4096 2008-12-31 20:00 carrier
drwxr-xr-x   4 root   root        0 1970-01-01 05:00 config
drwxrwx--x   3 radio  system   4096 2019-01-14 22:01 cpefs
lrw-r--r--   1 root   root       17 2008-12-31 20:00 d -> /sys/kernel/debug
drwxrwx--x  62 system system   4096 2025-04-29 18:54 data
drwxr-xr-x   2 root   root     4096 2008-12-31 20:00 debug_ramdisk
lrw-------   1 root   root       23 2008-12-31 20:00 default.prop -> system/etc/prop.default
drwxr-xr-x  21 root   root     3860 2025-04-29 18:55 dev
-rw-r--r--   1 root   root     6112 2008-12-31 20:00 dpolicy
drwxrwx--x  26 system radio    4096 2022-11-26 21:14 efs
lrw-r--r--   1 root   root       11 2008-12-31 20:00 etc -> /system/etc
-rwxr-x---   1 root   shell    3599 2008-12-31 20:00 init.container.rc
-rwxr-x---   1 root   shell    2516 2008-12-31 20:00 init.environ.rc
-rwxr-x---   1 root   shell  101613 2008-12-31 20:00 init.rc
-rwxr-x---   1 root   shell    6840 2008-12-31 20:00 init.usb.configfs.rc
-rwxr-x---   1 root   shell    6856 2008-12-31 20:00 init.usb.rc
-rwxr-x---   1 root   shell     623 2008-12-31 20:00 init.zygote32.rc
-rwxr-x---   1 root   shell    1068 2008-12-31 20:00 init.zygote64_32.rc
drwxr-xr-x   3 root   root     4096 2008-12-31 20:00 lib
drwx------   2 root   root    16384 2008-12-31 20:00 lost+found
drwxr-xr-x  15 root   system    320 2025-04-29 18:54 mnt
drwxr-xr-x   8 root   root     4096 2008-12-31 20:00 odm
drwxr-xr-x   2 root   root     4096 2008-12-31 20:00 oem
drwxrwx--x   3 root   system   4096 2018-01-01 17:47 omr
dr-xr-xr-x 453 root   root        0 1970-01-01 05:00 proc
drwxr-xr-x   2 root   root     4096 2008-12-31 20:00 product
lrw-r--r--   1 root   root       24 2008-12-31 20:00 product_services -> /system/product_services
-rw-r--r--   1 root   root     1509 2008-12-31 20:00 publiccert.pem
```

## 📜 Drozer Command Descriptions

| Command | Description |
|---|---|
| run app.package.list | Lists all installed applications. |
| run app.package.list -f <filter> | Filters apps (e.g., diva, com.snapchat.android). |
| run app.package.info -a <package> | Provides package info. |

| Command | Description |
|---|---|
| run app.package.manifest <package> | Retrieves AndroidManifest.xml. |
| run app.package.attacksurface <package> | Identifies exposed components. |
| run app.provider.info -a <package> | Displays content provider info. |
| run scanner.provider.finduris -a <package> | Finds URI paths vulnerable to attacks. |

## 🛠 **2.** APKTool

Used to reverse engineer Android APKs.

```
wget https://raw.githubusercontent.com/iBotPeaches/Apktool/master/scripts/linux/apktool
chmod +x apktool
sudo mv apktool /usr/local/bin/
```

```
wget https://bitbucket.org/iBotPeaches/apktool/downloads/apktool_2.9.3.jar
```

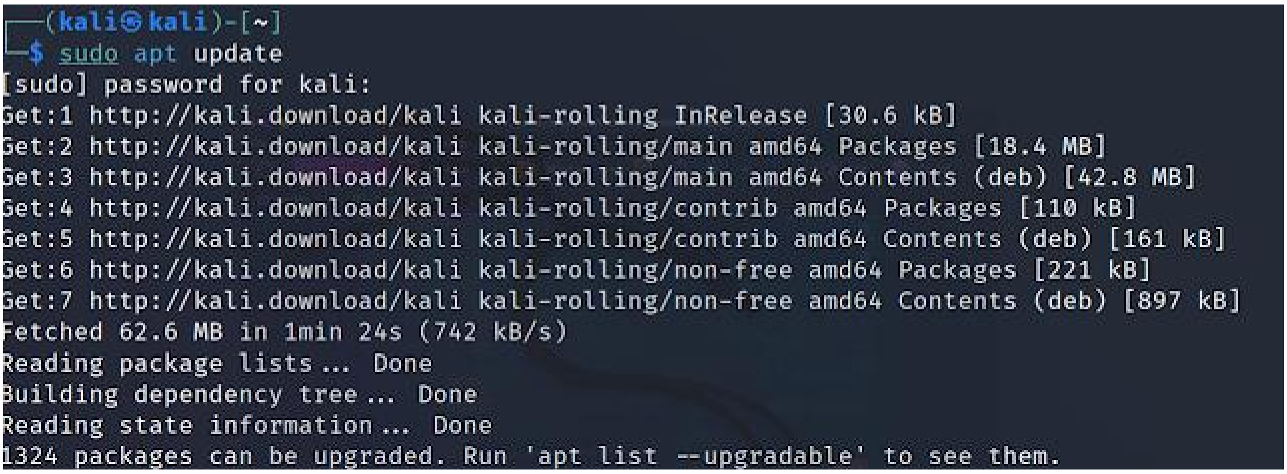
```
sudo mv apktool_2.9.3.jar /usr/local/bin/apktool.jar
```

## Mobile Forensics :

A mobile forensic tool to extract data from Android devices.

### Installation on Kali/Parrot Linux

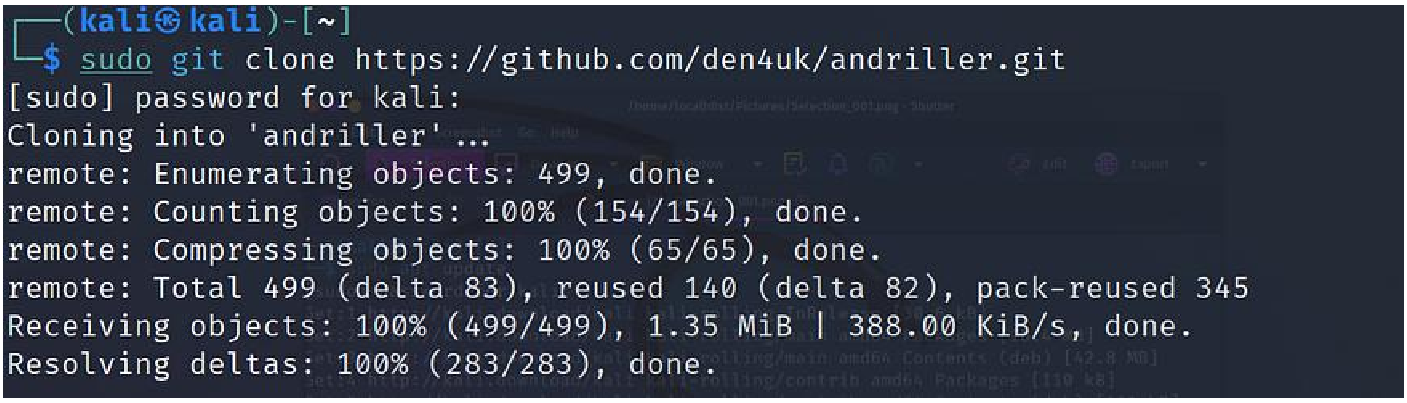
Since both Kali and Parrot are debian-based, installation is the same. First let’s update our Kali system (advisable) then we clone the repo from github using the git command



```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.4 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [42.8 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [110 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [161 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [221 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [897 kB]
Fetched 62.6 MB in 1min 24s (742 kB/s)
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
1324 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Now let’s clone the repo by using the following command

```
git clone https://github.com/den4uk/andriller.git
```

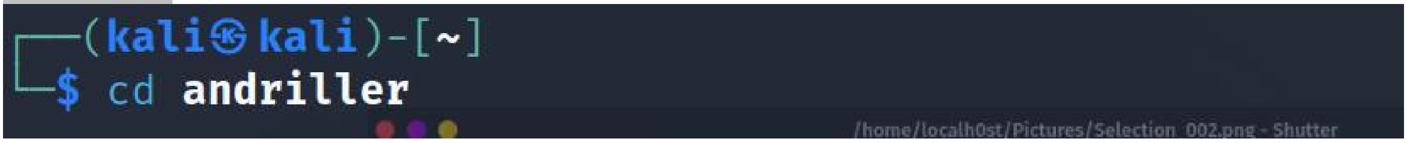


```
┌──(kali㉿kali)-[~]
└─$ sudo git clone https://github.com/den4uk/andriller.git
[sudo] password for kali:
Cloning into 'andriller'...
remote: Enumerating objects: 499, done.
remote: Counting objects: 100% (154/154), done.
remote: Compressing objects: 100% (65/65), done.
remote: Total 499 (delta 83), reused 140 (delta 82), pack-reused 345
Receiving objects: 100% (499/499), 1.35 MiB | 388.00 KiB/s, done.
Resolving deltas: 100% (283/283), done.
```

cloning the github repo

After cloning let’s move into the directory

cd andriller

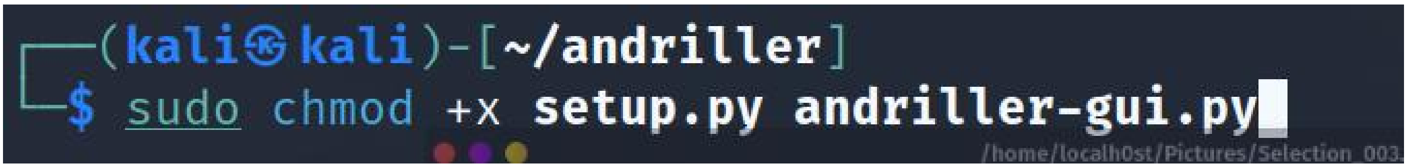


```
┌──(kali㉿kali)-[~]
└─$ cd andriller
```

changing into the directory

We now need to setup permissions for the two files inside the directory using the command below

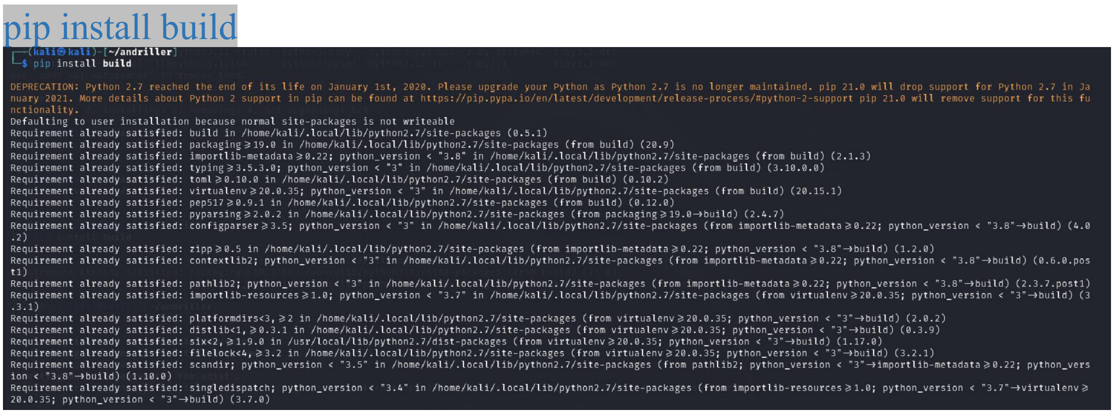
sudo chmod +x setup.py andriller-gui.py



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

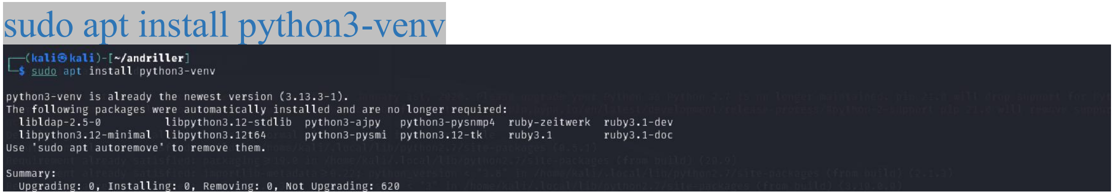
Now we can run the setup & install andriller. To do that we run the following command on our terminal:

pip install build



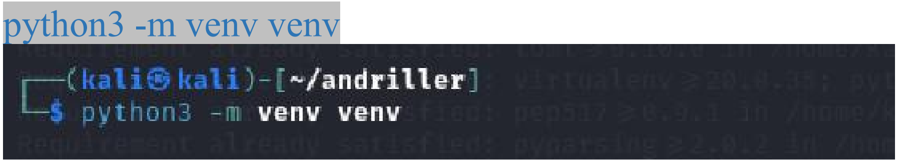
```
┌──(kali㉿kali)-[~/andriller]
└─$ pip install build

DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in Ja
nuary 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this fu
nctionality.
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: build in /home/kali/.local/lib/python2.7/site-packages (0.5.1)
Requirement already satisfied: packaging≥19.0 in /home/kali/.local/lib/python2.7/site-packages (from build) (20.9)
Requirement already satisfied: importlib-metadata≥0.22; python_version < "3.8" in /home/kali/.local/lib/python2.7/site-packages (from build) (2.1.3)
Requirement already satisfied: typing≥3.5.3.0; python_version < "3" in /home/kali/.local/lib/python2.7/site-packages (from build) (3.10.0.0)
Requirement already satisfied: toml≥0.10.0 in /home/kali/.local/lib/python2.7/site-packages (from build) (0.10.2)
Requirement already satisfied: virtualenv≥20.0.35; python_version < "3" in /home/kali/.local/lib/python2.7/site-packages (from build) (20.15.1)
Requirement already satisfied: pep517≥0.9.1 in /home/kali/.local/lib/python2.7/site-packages (from build) (0.12.0)
Requirement already satisfied: pyparsing≥2.0.2 in /home/kali/.local/lib/python2.7/site-packages (from packaging≥19.0→build) (2.4.7)
Requirement already satisfied: configparser≥3.5; python_version < "3" in /home/kali/.local/lib/python2.7/site-packages (from importlib-metadata≥0.22; python_version < "3.8"→build) (4.0
.2)
Requirement already satisfied: zipp≥0.5 in /home/kali/.local/lib/python2.7/site-packages (from importlib-metadata≥0.22; python_version < "3.8"→build) (1.2.0)
Requirement already satisfied: contextlib2; python_version < "3" in /home/kali/.local/lib/python2.7/site-packages (from importlib-metadata≥0.22; python_version < "3.8"→build) (0.6.0.pos
t1)
Requirement already satisfied: pathlib2; python_version < "3" in /home/kali/.local/lib/python2.7/site-packages (from importlib-metadata≥0.22; python_version < "3.8"→build) (2.3.7.post1)
Requirement already satisfied: importlib-resources≥1.0; python_version < "3.7" in /home/kali/.local/lib/python2.7/site-packages (from virtualenv≥20.0.35; python_version < "3"→build) (3
.3.1)
Requirement already satisfied: platformdirs<3,≥2 in /home/kali/.local/lib/python2.7/site-packages (from virtualenv≥20.0.35; python_version < "3"→build) (2.0.2)
Requirement already satisfied: distlib<1,≥0.3.1 in /home/kali/.local/lib/python2.7/site-packages (from virtualenv≥20.0.35; python_version < "3"→build) (0.3.9)
Requirement already satisfied: six<2,≥1.9.0 in /usr/local/lib/python2.7/dist-packages (from virtualenv≥20.0.35; python_version < "3"→build) (1.17.0)
Requirement already satisfied: filelock<4,≥3.2 in /home/kali/.local/lib/python2.7/site-packages (from virtualenv≥20.0.35; python_version < "3"→build) (3.2.1)
Requirement already satisfied: scandir; python_version < "3.5" in /home/kali/.local/lib/python2.7/site-packages (from pathlib2; python_version < "3"→importlib-metadata≥0.22; python_vers
ion < "3.8"→build) (1.10.0)
Requirement already satisfied: singledispatch; python_version < "3.4" in /home/kali/.local/lib/python2.7/site-packages (from importlib-resources≥1.0; python_version < "3.7"→virtualenv≥
20.0.35; python_version < "3"→build) (3.7.0)
```

sudo apt install python3-venv



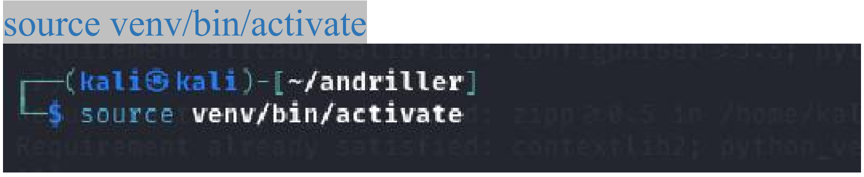
```
┌──(kali㉿kali)-[~/andriller]
└─$ sudo apt install python3-venv

python3-venv is already the newest version (3.13.3-1).
The following packages were automatically installed and are no longer required:
  libldap-2.5-0          libpython3.12-stdlib  python3-ajpy   python3-pysnmp4  ruby-zeitwerk  ruby3.1-dev
  libpython3.12-minimal  libpython3.12t64      python3-pysmi  python3.12-tk    ruby3.1        ruby3.1-doc
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 620
```

python3 -m venv venv



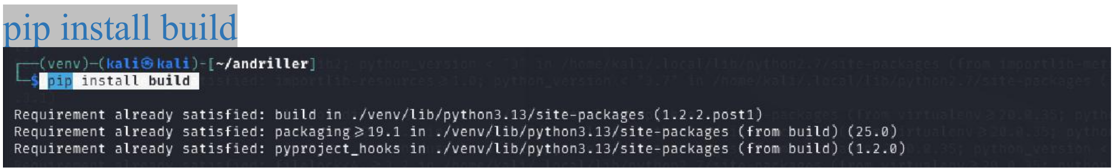
```
┌──(kali㉿kali)-[~/andriller]
└─$ python3 -m venv venv
```

source venv/bin/activate



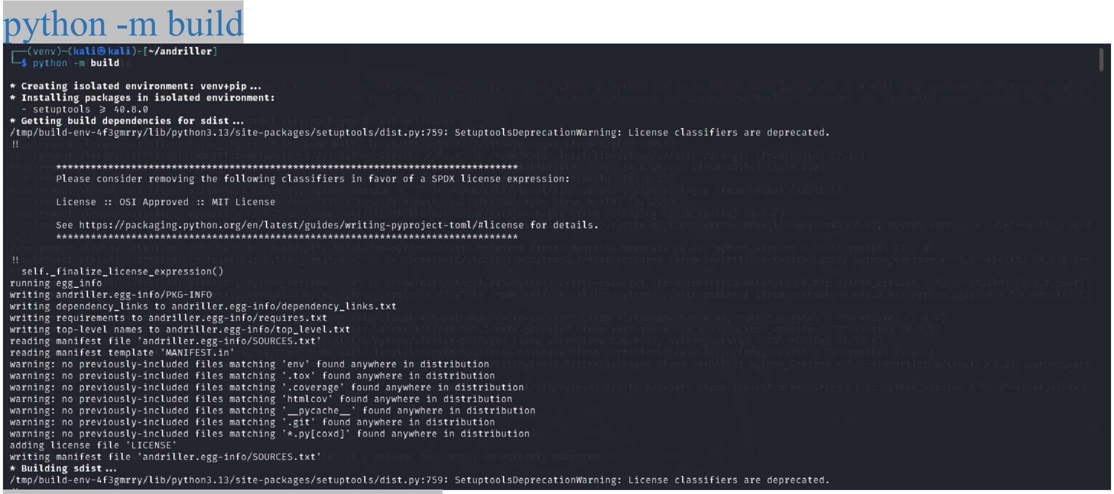
```
┌──(kali㉿kali)-[~/andriller]
└─$ source venv/bin/activate
```

pip install build



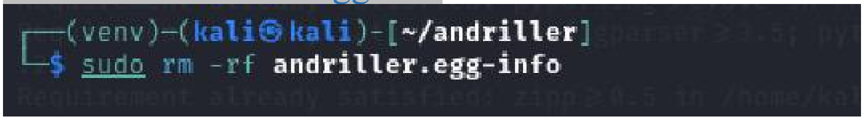
```
┌──(venv)─(kali㉿kali)-[~/andriller]
└─$ pip install build

Requirement already satisfied: build in ./venv/lib/python3.13/site-packages (1.2.2.post1)
Requirement already satisfied: packaging≥19.1 in ./venv/lib/python3.13/site-packages (from build) (25.0)
Requirement already satisfied: pyproject_hooks in ./venv/lib/python3.13/site-packages (from build) (1.2.0)
```

python -m build



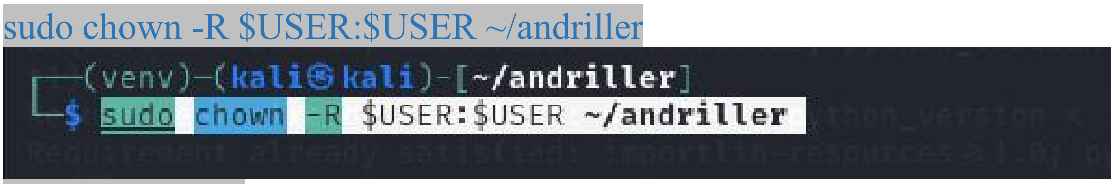
```
┌──(venv)─(kali㉿kali)-[~/andriller]
└─$ python -m build

* Creating isolated environment: venv+pip ...
* Installing packages in isolated environment:
  - setuptools ≥ 40.8.0
* Getting build dependencies for sdist ...
/tmp/build-env-4f3gmrry/lib/python3.13/site-packages/setuptools/dist.py:759: SetuptoolsDeprecationWarning: License classifiers are deprecated.
!!

        ********************************************************************************
        Please consider removing the following classifiers in favor of a SPDX license expression:

        License :: OSI Approved :: MIT License

        See https://packaging.python.org/en/latest/guides/writing-pyproject-toml/#license for details.
        ********************************************************************************

!!
  self._finalize_license_expression()
running egg_info
writing andriller.egg-info/PKG-INFO
writing dependency_links to andriller.egg-info/dependency_links.txt
writing requirements to andriller.egg-info/requires.txt
writing top-level names to andriller.egg-info/top_level.txt
reading manifest file 'andriller.egg-info/SOURCES.txt'
reading manifest template 'MANIFEST.in'
warning: no previously-included files matching 'env' found anywhere in distribution
warning: no previously-included files matching '.tox' found anywhere in distribution
warning: no previously-included files matching '.coverage' found anywhere in distribution
warning: no previously-included files matching 'htmlcov' found anywhere in distribution
warning: no previously-included files matching '__pycache__' found anywhere in distribution
warning: no previously-included files matching '.git' found anywhere in distribution
warning: no previously-included files matching '*.py[coxd]' found anywhere in distribution
adding license file 'LICENSE'
writing manifest file 'andriller.egg-info/SOURCES.txt'
* Building sdist ...
/tmp/build-env-4f3gmrry/lib/python3.13/site-packages/setuptools/dist.py:759: SetuptoolsDeprecationWarning: License classifiers are deprecated.
```

sudo rm -rf andriller.egg-info



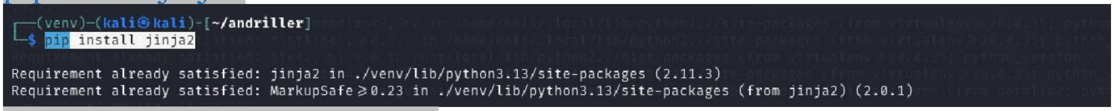
```
┌──(venv)─(kali㉿kali)-[~/andriller]
└─$ sudo rm -rf andriller.egg-info
```

sudo chown -R $USER:$USER ~/andriller



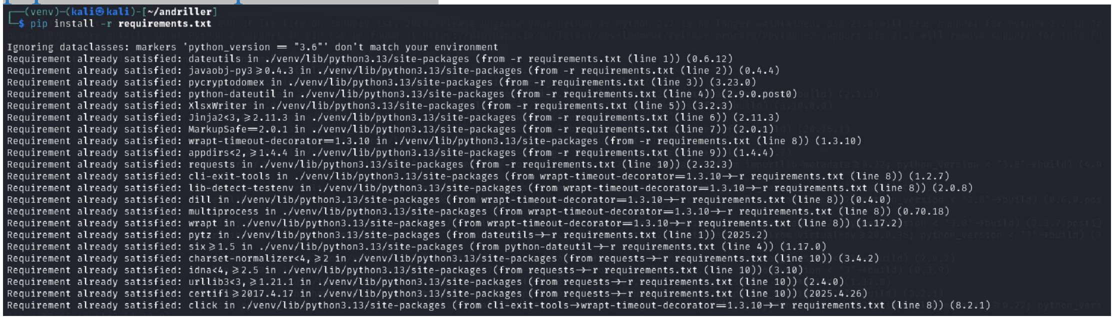
```
┌──(venv)─(kali㉿kali)-[~/andriller]
└─$ sudo chown -R $USER:$USER ~/andriller
```

pip install jinja2



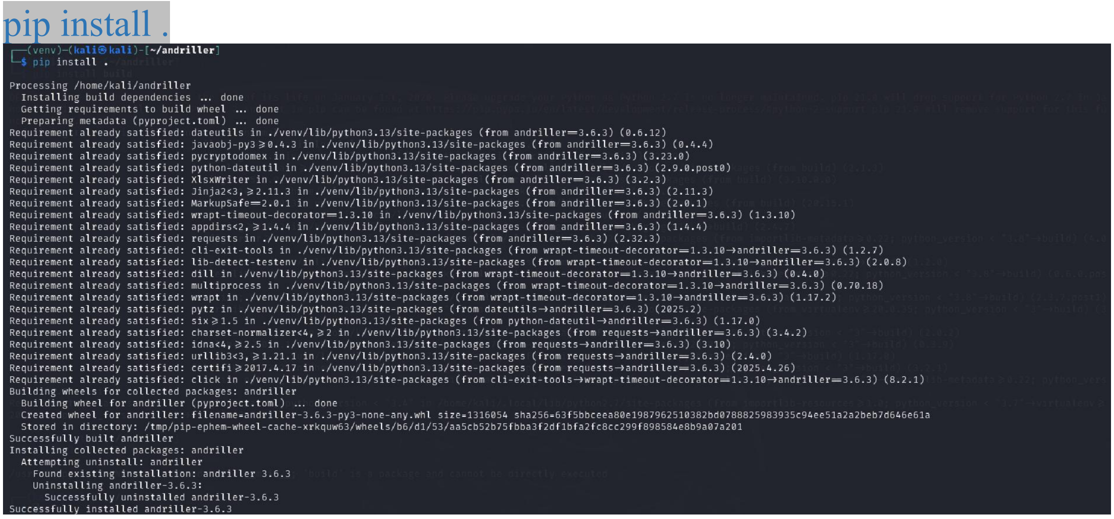
```
┌──(venv)─(kali㉿kali)-[~/andriller]
└─$ pip install jinja2

Requirement already satisfied: jinja2 in ./venv/lib/python3.13/site-packages (2.11.3)
Requirement already satisfied: MarkupSafe≥0.23 in ./venv/lib/python3.13/site-packages (from jinja2) (2.0.1)
```

pip install -r requirements.txt



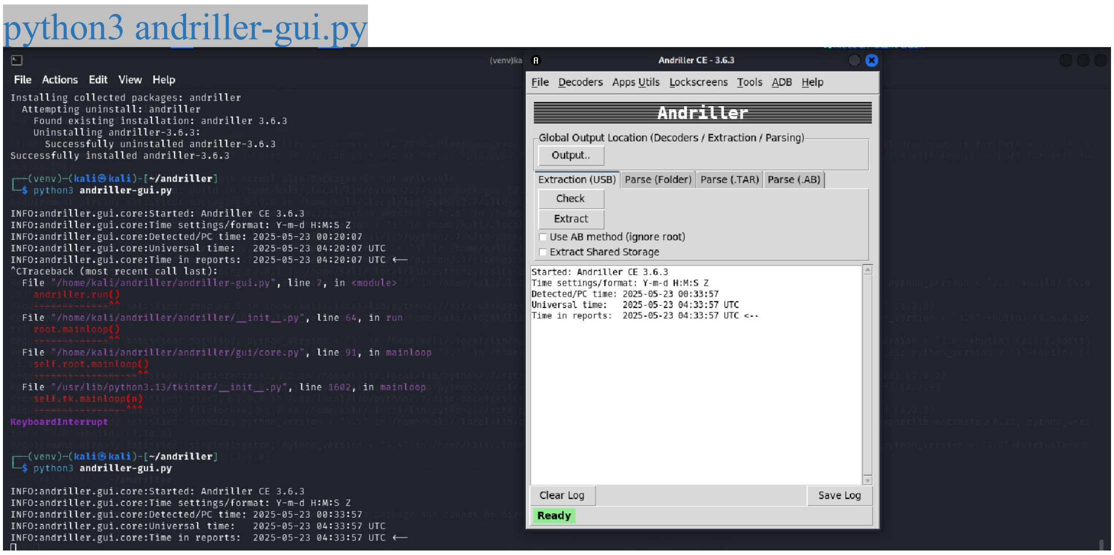
```
┌──(venv)─(kali㉿kali)-[~/andriller]
└─$ pip install -r requirements.txt

Ignoring dataclasses: markers 'python_version == "3.6"' don't match your environment
Requirement already satisfied: dateutils in ./venv/lib/python3.13/site-packages (from -r requirements.txt (line 1)) (0.6.12)
Requirement already satisfied: javaobj-py3≥0.4.3 in ./venv/lib/python3.13/site-packages (from -r requirements.txt (line 2)) (0.4.4)
Requirement already satisfied: pycryptodomex in ./venv/lib/python3.13/site-packages (from -r requirements.txt (line 3)) (3.23.0)
Requirement already satisfied: python-dateutil in ./venv/lib/python3.13/site-packages (from -r requirements.txt (line 4)) (2.9.0.post0)
Requirement already satisfied: XlsxWriter in ./venv/lib/python3.13/site-packages (from -r requirements.txt (line 5)) (3.2.3)
Requirement already satisfied: Jinja2<3,≥2.11.3 in ./venv/lib/python3.13/site-packages (from -r requirements.txt (line 6)) (2.11.3)
Requirement already satisfied: MarkupSafe==2.0.1 in ./venv/lib/python3.13/site-packages (from -r requirements.txt (line 7)) (2.0.1)
Requirement already satisfied: wrapt-timeout-decorator==1.3.10 in ./venv/lib/python3.13/site-packages (from -r requirements.txt (line 8)) (1.3.10)
Requirement already satisfied: appdirs<2,≥1.4.4 in ./venv/lib/python3.13/site-packages (from -r requirements.txt (line 9)) (1.4.4)
Requirement already satisfied: requests in ./venv/lib/python3.13/site-packages (from -r requirements.txt (line 10)) (2.32.3)
Requirement already satisfied: cli-exit-tools in ./venv/lib/python3.13/site-packages (from wrapt-timeout-decorator==1.3.10→-r requirements.txt (line 8)) (1.2.7)
Requirement already satisfied: lib-detect-testenv in ./venv/lib/python3.13/site-packages (from wrapt-timeout-decorator==1.3.10→-r requirements.txt (line 8)) (2.0.8)
Requirement already satisfied: dill in ./venv/lib/python3.13/site-packages (from wrapt-timeout-decorator==1.3.10→-r requirements.txt (line 8)) (0.4.0)
Requirement already satisfied: multiprocess in ./venv/lib/python3.13/site-packages (from wrapt-timeout-decorator==1.3.10→-r requirements.txt (line 8)) (0.70.18)
Requirement already satisfied: wrapt in ./venv/lib/python3.13/site-packages (from wrapt-timeout-decorator==1.3.10→-r requirements.txt (line 8)) (1.17.2)
Requirement already satisfied: pytz in ./venv/lib/python3.13/site-packages (from dateutils→-r requirements.txt (line 1)) (2025.2)
Requirement already satisfied: six≥1.5 in ./venv/lib/python3.13/site-packages (from python-dateutil→-r requirements.txt (line 4)) (1.17.0)
Requirement already satisfied: charset-normalizer<4,≥2 in ./venv/lib/python3.13/site-packages (from requests→-r requirements.txt (line 10)) (3.4.2)
Requirement already satisfied: idna<4,≥2.5 in ./venv/lib/python3.13/site-packages (from requests→-r requirements.txt (line 10)) (3.10)
Requirement already satisfied: urllib3<3,≥1.21.1 in ./venv/lib/python3.13/site-packages (from requests→-r requirements.txt (line 10)) (2.4.0)
Requirement already satisfied: certifi≥2017.4.17 in ./venv/lib/python3.13/site-packages (from requests→-r requirements.txt (line 10)) (2025.4.26)
Requirement already satisfied: click in ./venv/lib/python3.13/site-packages (from cli-exit-tools→wrapt-timeout-decorator==1.3.10→-r requirements.txt (line 8)) (8.2.1)
```

pip install .



```
┌──(venv)─(kali㉿kali)-[~/andriller]
└─$ pip install .

Processing /home/kali/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=63f5bbceea80e1987962510382bd0788825983935c94ee51a2a2beb7d646e61a
  Stored in directory: /tmp/pip-ephem-wheel-cache-xrkquw63/wheels/b6/d1/53/aa5cb52b75fbba3f2df1bfa2fc8cc299f898584e8b9a07a201
Successfully built andriller
Installing collected packages: andriller
  Attempting uninstall: andriller
    Found existing installation: andriller 3.6.3
    Uninstalling andriller-3.6.3:
      Successfully uninstalled andriller-3.6.3
Successfully installed andriller-3.6.3
```

python3 andriller-gui.py



File Actions Edit View Help
(venv)ka
Andriller CE - 3.6.3
File Decoders Apps Utils Lockscreens Tools ADB Help
Andriller
Global Output Location (Decoders / Extraction / Parsing)
Output..
Extraction (USB) Parse (Folder) Parse (.TAR) Parse (.AB)
Check
Extract
☐ Use AB method (ignore root)
☐ Extract Shared Storage
Clear Log
Save Log
Ready

```
Installing collected packages: andriller
  Attempting uninstall: andriller
    Found existing installation: andriller 3.6.3
    Uninstalling andriller-3.6.3:
      Successfully uninstalled andriller-3.6.3
Successfully installed andriller-3.6.3

┌──(venv)─(kali㉿kali)-[~/andriller]
└─$ python3 andriller-gui.py

INFO:andriller.gui.core:Started: Andriller CE 3.6.3
INFO:andriller.gui.core:Time settings/format: Y-m-d H:M:S Z
INFO:andriller.gui.core:Detected/PC time: 2025-05-23 00:20:07
INFO:andriller.gui.core:Universal time:   2025-05-23 04:20:07 UTC
INFO:andriller.gui.core:Time in reports:  2025-05-23 04:20:07 UTC ⟵
^CTraceback (most recent call last):
  File "/home/kali/andriller/andriller-gui.py", line 7, in <module>
    andriller.run()
    ~~~~~~~~~~~~~^^
  File "/home/kali/andriller/andriller/__init__.py", line 64, in run
    root.mainloop()
    ~~~~~~~~~~~~~^^
  File "/home/kali/andriller/andriller/gui/core.py", line 91, in mainloop
    self.root.mainloop()
    ~~~~~~~~~~~~~~~~~~^^
  File "/usr/lib/python3.13/tkinter/__init__.py", line 1602, in mainloop
    self.tk.mainloop(n)
    ~~~~~~~~~~~~~~~~^^^
KeyboardInterrupt

┌──(venv)─(kali㉿kali)-[~/andriller]
└─$ python3 andriller-gui.py

INFO:andriller.gui.core:Started: Andriller CE 3.6.3
INFO:andriller.gui.core:Time settings/format: Y-m-d H:M:S Z
INFO:andriller.gui.core:Detected/PC time: 2025-05-23 00:33:57
INFO:andriller.gui.core:Universal time:   2025-05-23 04:33:57 UTC
INFO:andriller.gui.core:Time in reports:  2025-05-23 04:33:57 UTC ⟵
```

```
Started: Andriller CE 3.6.3
Time settings/format: Y-m-d H:M:S Z
Detected/PC time: 2025-05-23 00:33:57
Universal time:   2025-05-23 04:33:57 UTC
Time in reports:  2025-05-23 04:33:57 UTC <--
```

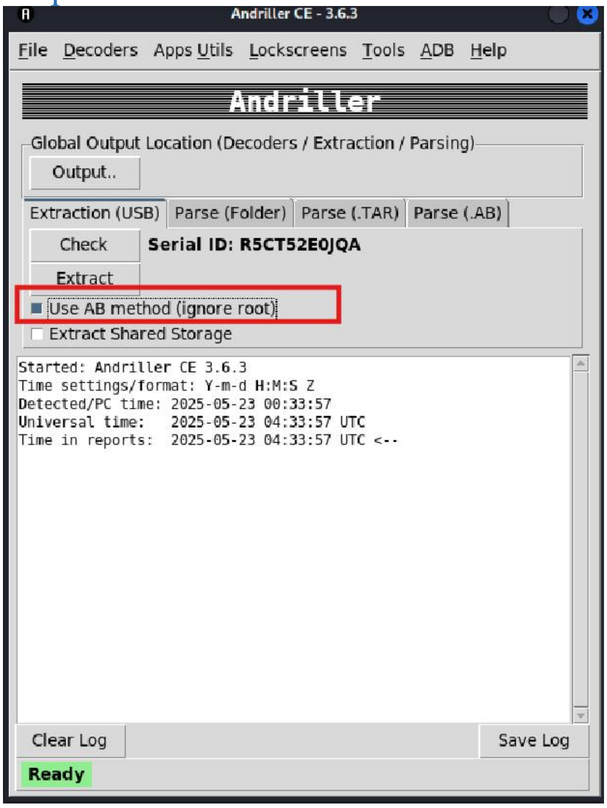
Now once you installed than reopened it.

cd andriller
python3 -m venv venv
source venv/bin/activate

```
python3 andriller-gui.py
```

## Now Steps

## Step1:



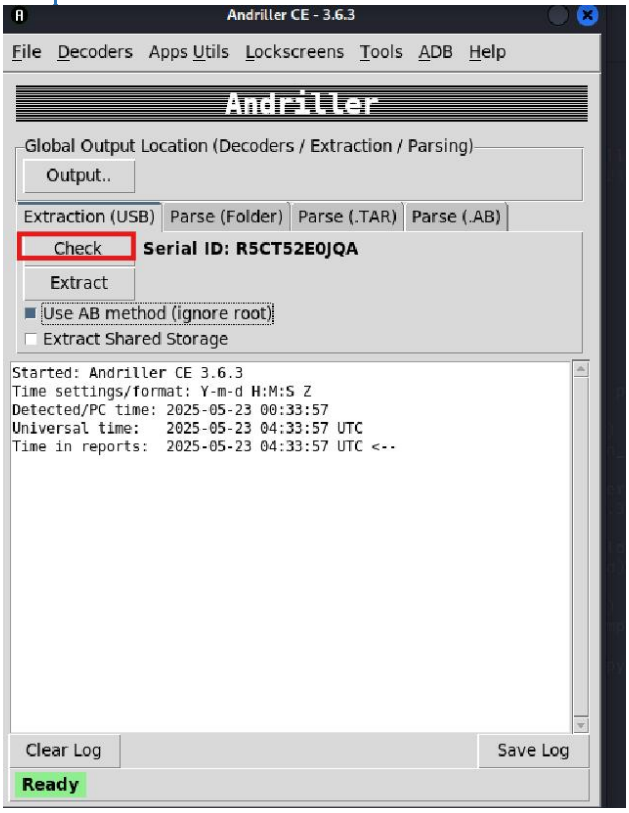
Serial ID: R5CT52E0JQA

☑ Use AB method (ignore root)

□ Extract Shared Storage

```
Started: Andriller CE 3.6.3
Time settings/format: Y-m-d H:M:S Z
Detected/PC time: 2025-05-23 00:33:57
Universal time:    2025-05-23 04:33:57 UTC
Time in reports:   2025-05-23 04:33:57 UTC <--
```

## Step2:



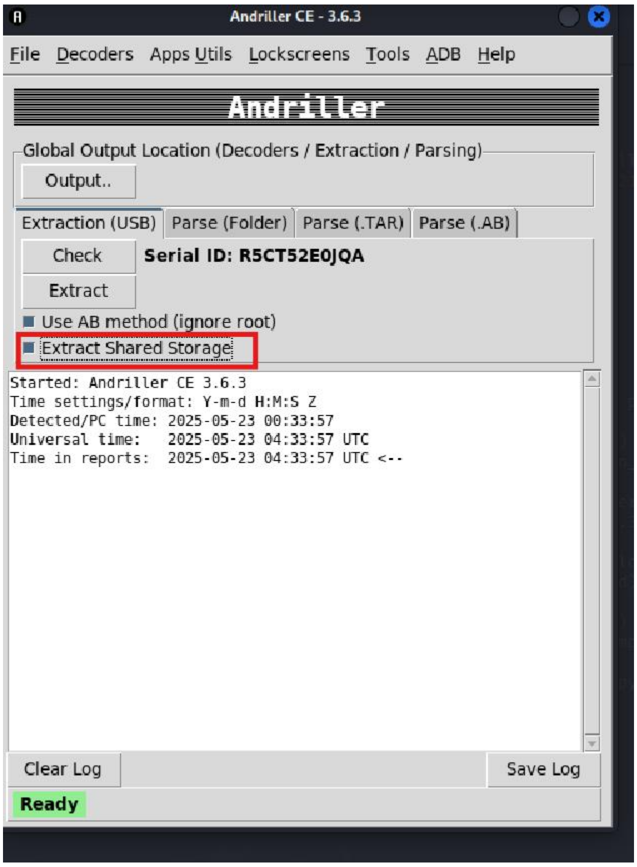
Serial ID: R5CT52E0JQA

☑ Use AB method (ignore root)

□ Extract Shared Storage

```
Started: Andriller CE 3.6.3
Time settings/format: Y-m-d H:M:S Z
Detected/PC time: 2025-05-23 00:33:57
Universal time:    2025-05-23 04:33:57 UTC
Time in reports:   2025-05-23 04:33:57 UTC <--
```

## Step 3:


Andriller CE - 3.6.3
File Decoders Apps Utils Lockscreens Tools ADB Help
Andriller
Global Output Location (Decoders / Extraction / Parsing)
Output..
Extraction (USB) Parse (Folder) Parse (.TAR) Parse (.AB)
Check
Extract
Clear Log
Save Log
Ready

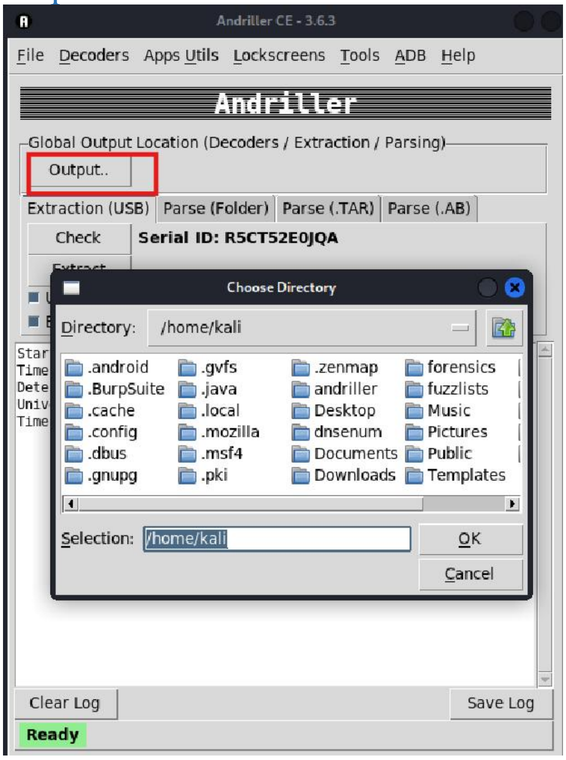
Serial ID: R5CT52E0JQA

■ Use AB method (ignore root)

■ Extract Shared Storage

```
Started: Andriller CE 3.6.3
Time settings/format: Y-m-d H:M:S Z
Detected/PC time: 2025-05-23 00:33:57
Universal time:   2025-05-23 04:33:57 UTC
Time in reports:  2025-05-23 04:33:57 UTC <--
```

## Step 4:


Andriller CE - 3.6.3
File Decoders Apps Utils Lockscreens Tools ADB Help
Andriller
Global Output Location (Decoders / Extraction / Parsing)
Output..
Extraction (USB) Parse (Folder) Parse (.TAR) Parse (.AB)
Check
Choose Directory
.android .gvfs .zenmap forensics
.BurpSuite .java andriller fuzzlists
.cache .local Desktop Music
.config .mozilla dnsenum Pictures
.dbus .msf4 Documents Public
.gnupg .pki Downloads Templates
OK
Cancel
Clear Log
Save Log
Ready

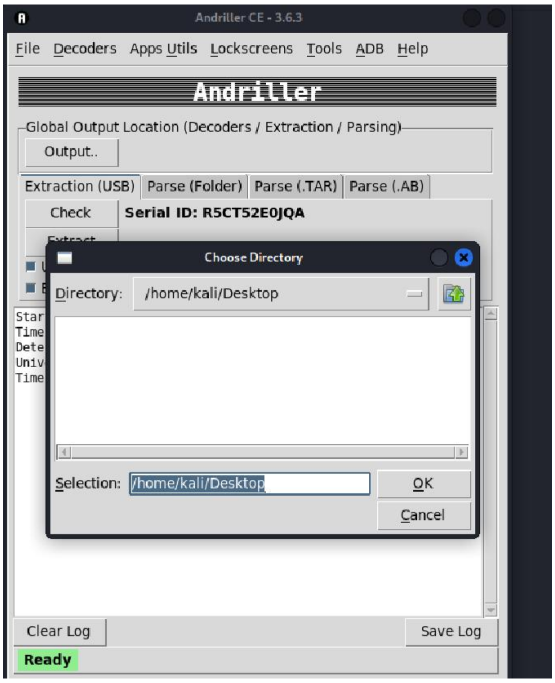
Serial ID: R5CT52E0JQA

Directory: /home/kali

Selection: /home/kali

## Step5:

Select the output file location.



Global Output Location (Decoders / Extraction / Parsing)

Serial ID: R5CT52E0JQA

Choose Directory

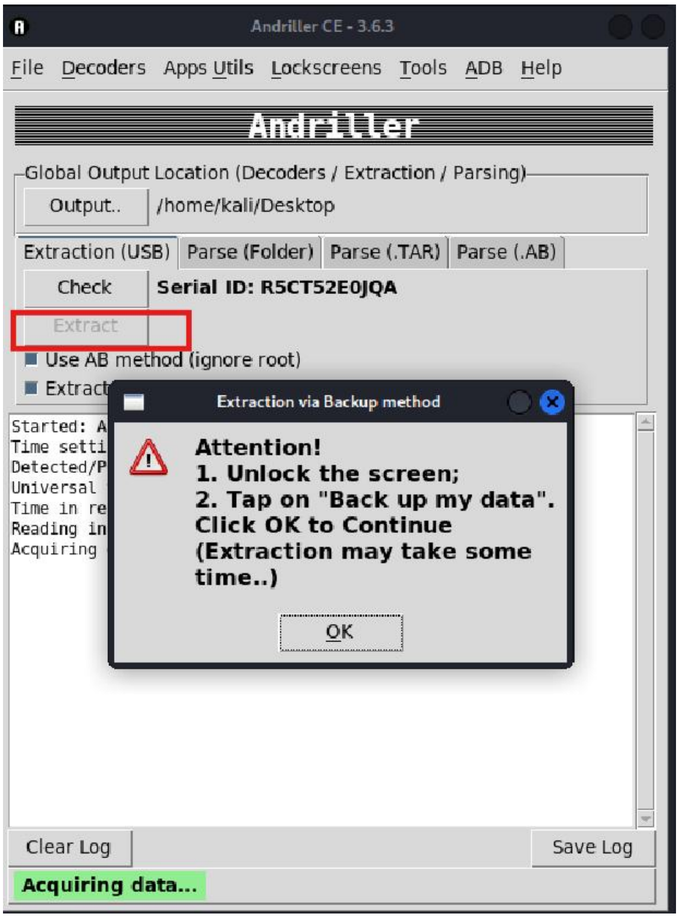
Directory: /home/kali/Desktop

Selection: /home/kali/Desktop

```
Star
Time
Dete
Univ
Time
```

Ready

Step 6:
After selecting the output file location press th extract button.



Global Output Location (Decoders / Extraction / Parsing)

Output.. /home/kali/Desktop

Serial ID: R5CT52E0JQA

■ Use AB method (ignore root)

■ Extract

```
Started: A
Time setti
Detected/P
Universal
Time in re
Reading in
Acquiring
```

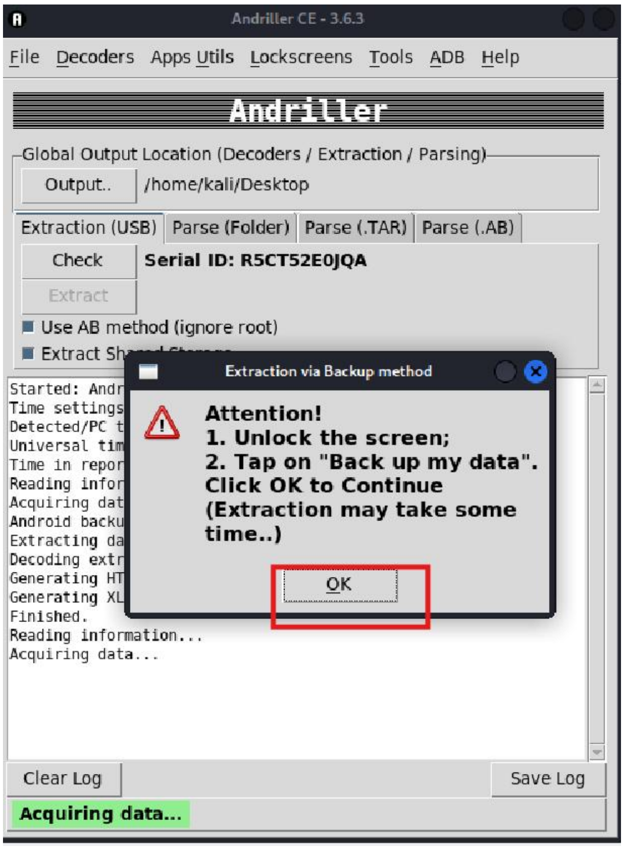
Extraction via Backup method

Attention!
1. Unlock the screen;
2. Tap on "Back up my data".
Click OK to Continue
(Extraction may take some time..)

Acquiring data...

Step7:

In your phone click on backup my data than click ok on it.



Andriller CE - 3.6.3
File Decoders Apps Utils Lockscreens Tools ADB Help
Andriller
Output..
Extraction (USB) Parse (Folder) Parse (.TAR) Parse (.AB)
Check
Extract
Extraction via Backup method
OK
Clear Log
Save Log

Global Output Location (Decoders / Extraction / Parsing)

/home/kali/Desktop

Serial ID: R5CT52E0JQA

■ Use AB method (ignore root)

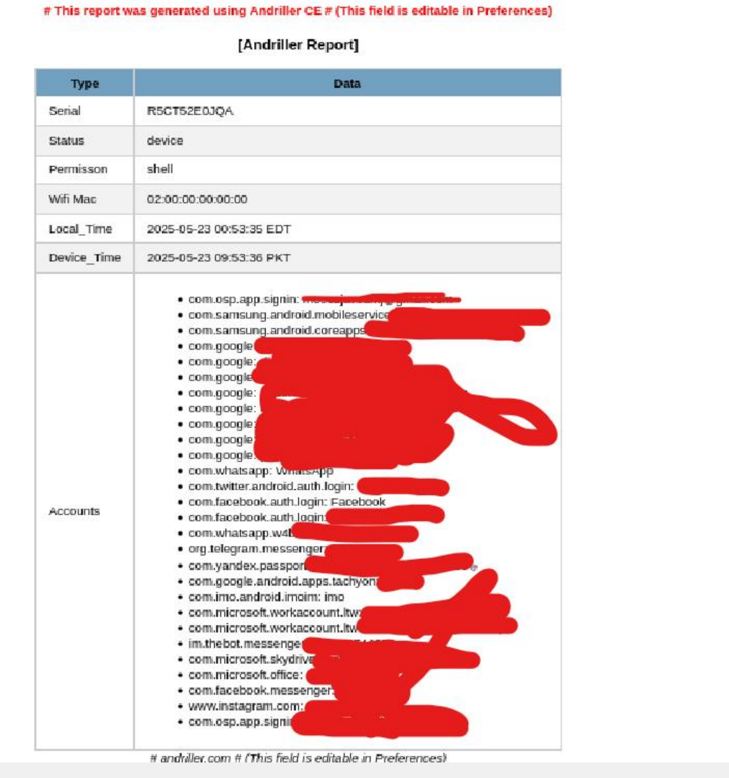
■ Extract Sh

```
Started: Andr
Time settings
Detected/PC t
Universal tim
Time in repor
Reading infor
Acquiring dat
Android backu
Extracting da
Decoding extr
Generating HT
Generating XL
Finished.
Reading information...
Acquiring data...
```

Attention!
1. Unlock the screen;
2. Tap on "Back up my data".
Click OK to Continue
(Extraction may take some time..)

Acquiring data...

## Than in browser it display:



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

[Andriller Report]

| Type | Data |
|---|---|
| Serial | R5CT52E0JQA |
| Status | device |
| Permisson | shell |
| Wifi Mac | 02:00:00:00:00:00 |
| Local_Time | 2025-05-23 00:53:35 EDT |
| Device_Time | 2025-05-23 09:53:36 PKT |
| Accounts | • com.osp.app.signin: [redacted]<br>• com.samsung.android.mobileservice [redacted]<br>• com.samsung.android.coreapps [redacted]<br>• com.google [redacted]<br>• com.google: [redacted]<br>• com.google [redacted]<br>• com.google: [redacted]<br>• com.google: [redacted]<br>• com.google: [redacted]<br>• com.google: [redacted]<br>• com.google. [redacted]<br>• com.whatsapp: WhatsApp<br>• com.twitter.android.auth.login: [redacted]<br>• com.facebook.auth.login: Facebook<br>• com.facebook.auth.login: [redacted]<br>• com.whatsapp.w4 [redacted]<br>• org.telegram.messenger [redacted]<br>• com.yandex.passpor [redacted]<br>• com.google.android.apps.tachyon [redacted]<br>• com.imo.android.imoim: imo<br>• com.microsoft.workaccount.ltw [redacted]<br>• com.microsoft.workaccount.ltw [redacted]<br>• im.thebot.messenge [redacted]<br>• com.microsoft.skydrive [redacted]<br>• com.microsoft.office: [redacted]<br>• com.facebook.messenger: [redacted]<br>• www.instagram.com: [redacted]<br>• com.osp.app.signi [redacted] |

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

## Sample Task: Android App Attack Surface Analysis

📝 Task Overview:

Identify the exposed components and data leakage potential of a target Android application.

🛠 Tools Required:

- Android Device (with USB Debugging)
- Kali Linux (with Drozer installed)
- ADB enabled

Steps:

1. **Connect Android device** via USB and verify:

```
adb devices -l
```

2. **Forward TCP port for Drozer communication**:

```
adb forward tcp:31415 tcp:31415
```

3. **Launch Drozer Console**:

```
drozer console connect
```

4. **List all packages**:

```
run app.package.list
```

5. **Identify the target app (e.g., Snapchat)**:

```
run app.package.list -f com.snapchat.android
```

6. **Gather app info and attack surface**:

```
run app.package.info -a com.snapchat.android
run app.package.manifest com.snapchat.android
run app.package.attacksurface com.snapchat.android
```

7. **Scan for vulnerable URIs**:

```
run scanner.provider.finduris -a com.snapchat.android
```

8. **Analyze Results and Document Findings**

---

## Notes and Best Practices

- Always obtain **legal authorization** before conducting any pentesting.
- Use **virtual machines** (e.g., VirtualBox with USB pass-through).
- Maintain a **clean environment** by activating/deactivating virtual environments when switching projects.
- Use **APKTool** to inspect or decompile APKs for static analysis.

---

## 🎯 Final Output

Upon successful execution of the tools and commands, you will gain insights into:

- Installed applications
- AndroidManifest permissions

- Exported and unprotected components
- Vulnerable content providers
- Possible URI exposure

These insights can inform further attack simulations or defense mechanisms.