Maria Valencia

CSC 154

Lab 14

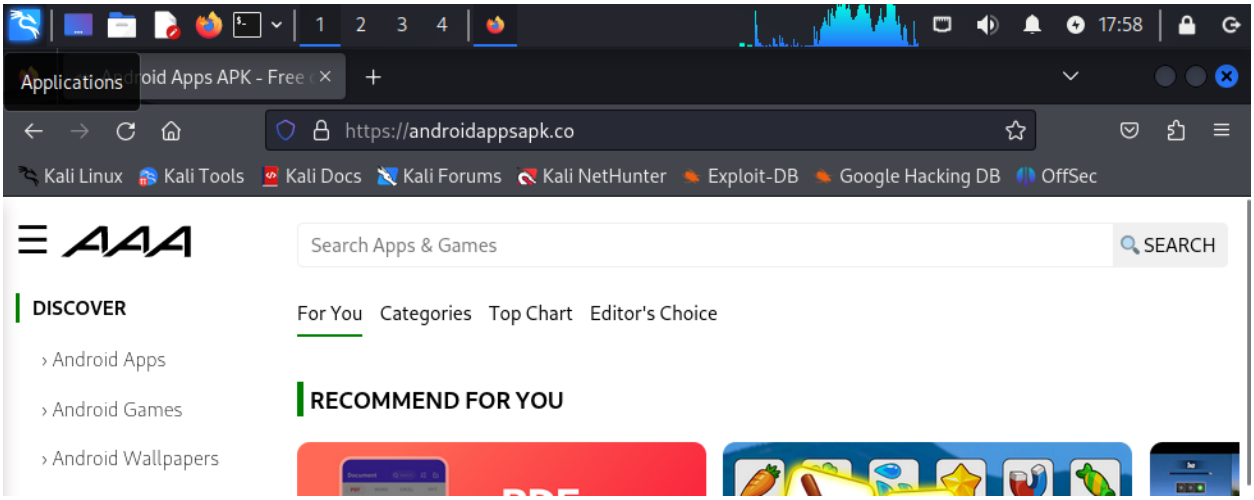
Lab 14 – Mobile Security

14.1 Static Analysis

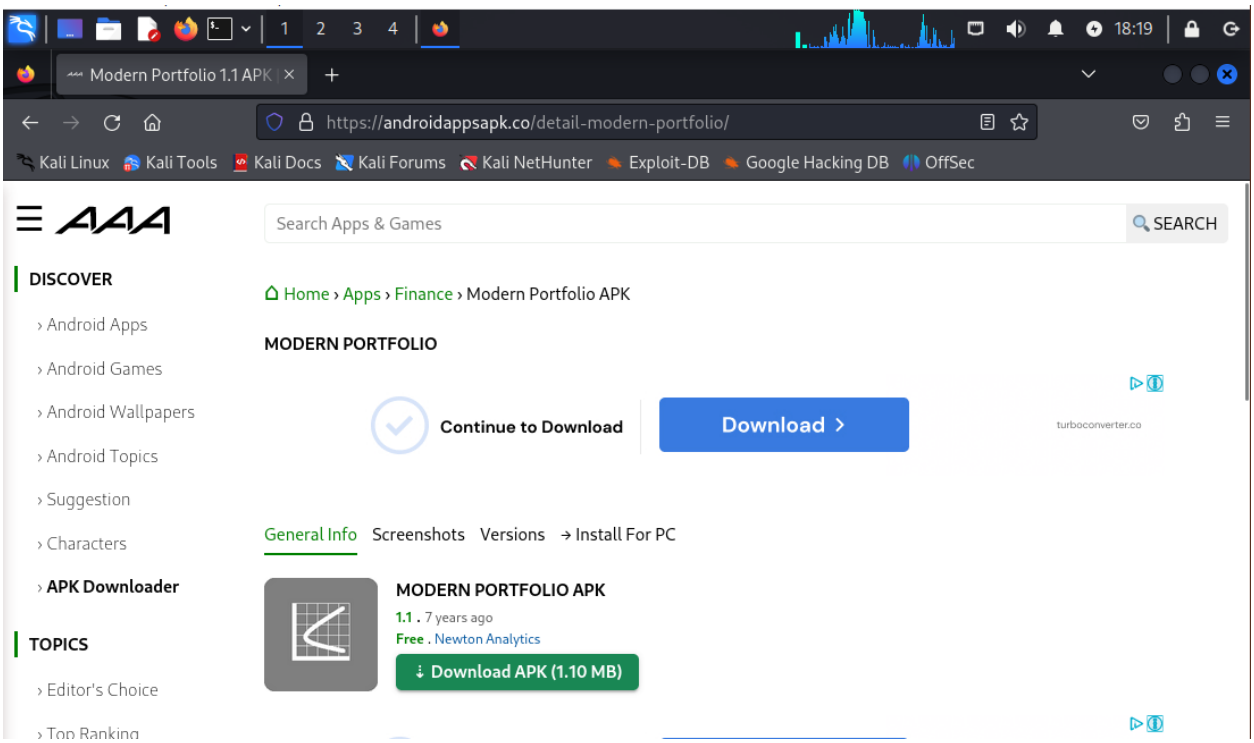
Static analysis of Android applications starts with acquiring the app file APK. Unzipping the file and then decompiling/disassembling the application allows for review of the app's source code and settings. The process of preparing and analyzing the app can be automated using the Qark tool.

Step 1: Get APK

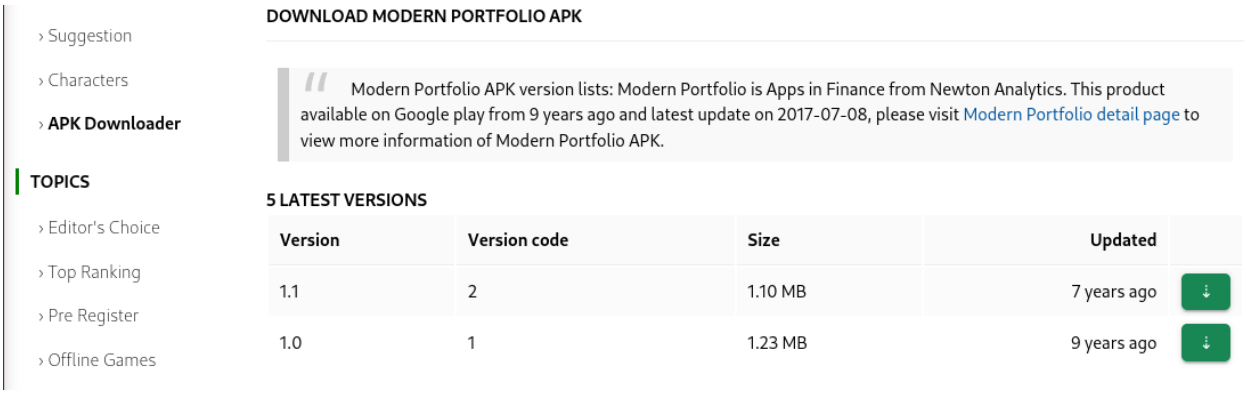
After I started my kali VM in Bridge Adapter network mode, I opened a browser and navigated to https://androidappsapk.co/.

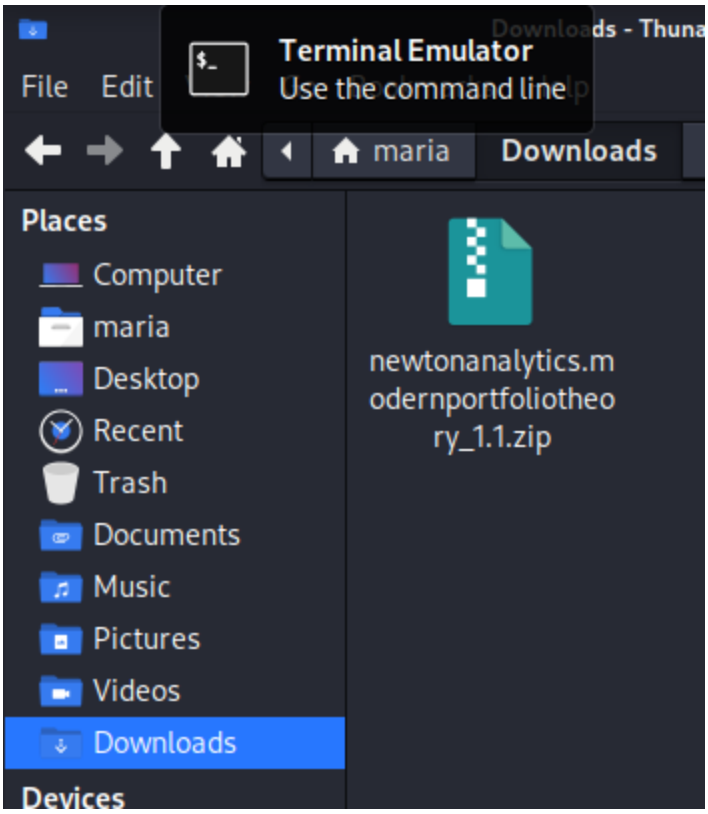


I searched for newtonanalytics.modernportfoliotheory and followed the link of the Newton Analytics application.



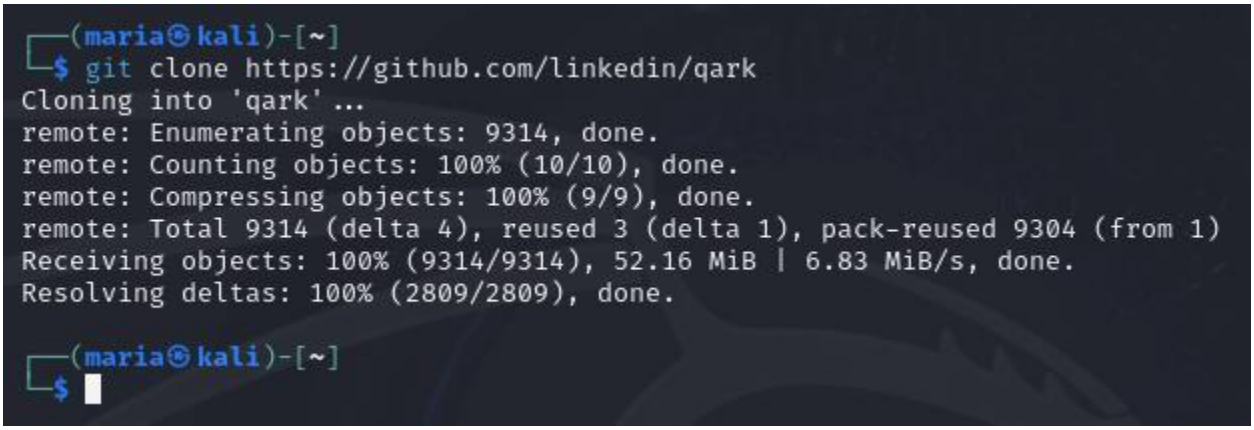
After pressing the “Download APK” button, I was directed to the download page. I pressed the download icon next to the app to start the download. I observed that the APK file is downloaded to my download folder.





Step 2: Install and Run Qark

I cloned the Github Repository qark to my Kali VM.



I changed the directory into the qark folder and then set up a python environment. I observed that the command line now shows (venv). Then, i installed and ran qark form this virtual environment.

```
┌──(maria㉿kali)-[~]
└─$ cd qark

┌──(maria㉿kali)-[~/qark]
└─$ virtualenv -p python3 venv
created virtual environment CPython3.11.9.final.0-64 in 200ms
  creator CPython3Posix(dest=/home/maria/qark/venv, clear=False, no_vcs_ignor
e=False, global=False)
  seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bun
dle, via=copy, app_data_dir=/home/maria/.local/share/virtualenv)
    added seed packages: pip==24.1.1, setuptools==68.1.2, wheel==0.43.0
  activators BashActivator,CShellActivator,FishActivator,NushellActivator,Pow
erShellActivator,PythonActivator

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

┌──(venv)─(maria㉿kali)-[~/qark]
└─$
```

Next, I installed the requirements and ran the qark setup.

```
┌──(venv)─(maria㉿kali)-[~/qark]
└─$ sudo pip install -r requirements.txt
[sudo] password for maria:
Ignoring enum34: markers 'python_version < "3.4"' don't match your environmen
t
Collecting asn1crypto==0.24.0 (from -r requirements.txt (line 1))
  Downloading asn1crypto-0.24.0-py2.py3-none-any.whl (101 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 101.6/101.6 kB 2.1 MB/s eta 0:00:00
Collecting certifi==2018.1.18 (from -r requirements.txt (line 5))
  Downloading certifi-2018.1.18-py2.py3-none-any.whl (151 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 151.6/151.6 kB 5.3 MB/s eta 0:00:00
Collecting cffi==1.11.5 (from -r requirements.txt (line 9))
  Downloading cffi-1.11.5.tar.gz (438 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 438.5/438.5 kB 11.1 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
```

```
┌──(venv)─(maria㉿kali)-[~/qark]
└─$ sudo python setup.py install
running install
/usr/lib/python3/dist-packages/setuptools/_distutils/cmd.py:66: SetuptoolsDep
recationWarning: setup.py install is deprecated.
!!

        ********************************************************************
**********
        Please avoid running ``setup.py`` directly.
        Instead, use pypa/build, pypa/installer or other
        standards-based tools.

        See https://blog.ganssle.io/articles/2021/10/setup-py-deprecated.html
 for details.
        ********************************************************************
**********
```

I ran qark while targeting the APK downloaded in the previous step. Here, qark will decompile and analyze the APK and produce a report of its findings. When the tool finished, I copied down the path of the report on the last output.

```
┌──(venv)─(maria㉿kali)-[~/qark]
└─$ unzip -d ~/Downloads ~/Downloads/newtonanalytics.modernportfoliotheory*.z
ip
Archive:  /home/maria/Downloads/newtonanalytics.modernportfoliotheory_1.1.zip
warning [/home/maria/Downloads/newtonanalytics.modernportfoliotheory_1.1.zip]
:  7985 extra bytes at beginning or within zipfile
  (attempting to process anyway)
 extracting: /home/maria/Downloads/newtonanalytics.modernportfoliotheory_1.1.
apk

┌──(venv)─(maria㉿kali)-[~/qark]
└─$ sudo qark --apk ~/Downloads/newtonanalytics.modernportfoliotheory*.apk
Decompiling ...
dex2jar /home/maria/qark/build/qark/classes.dex → /home/maria/qark/build/qar
k/newtonanalytics.modernportfoliotheory_1.1.jar
Traceback (most recent call last):
  File "/usr/local/bin/qark", line 33, in <module>
    sys.exit(load_entry_point('qark==4.0.0', 'console_scripts', 'qark')())
             ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

Step 3: Manually Analyze the App

With eh app decompiled and analyzed, I navigated to the build/qark directory and listed the outputs.

```
┌──(venv)─(maria㉿kali)-[~/qark]
└─$ cd build/qark

┌──(venv)─(maria㉿kali)-[~/qark/build/qark]
└─$ ls -la
total 1512
drwxr-xr-x  4 root root   4096 Dec  5 12:06 .
drwxr-xr-x  5 root root   4096 Dec  5 12:06 ..
-rw-r--r--  1 root root   2804 Dec  5 12:08 AndroidManifest.xml
drwxr-xr-x  2 root root   4096 Dec  5 12:06 META-INF
-rw-r--r--  1 root root 652804 Dec  5 12:08 classes.dex
-rw-r--r--  1 root root 463307 Dec  5 12:06 newtonanalytics.modernportfolioth
eory_1.1.jar
drwxr-xr-x 10 root root   4096 Dec  5 12:06 res
-rw-r--r--  1 root root 404672 Dec  5 12:08 resources.arsc

┌──(venv)─(maria㉿kali)-[~/qark/build/qark]
└─$
```

I displayed the AndroidManifest.xml contents using cat. (it should be in xml format, not like below)

```
┌──(venv)─(maria㉿kali)-[~/qark/build/qark]
└─$ cat AndroidManifest.xml
◆
,$◆▒4Rv◆◆◆◆◆◆◆TXj◆◆◆4>Fdx◆◆◆j◆◆◆◆(◆
(
 versionCode
minSdkVersiontargetSdkVersionname
                                    allowBackupiconlabelthemescreenOrientationan
droid*http://schemas.android.com/apk/res/androidpackage▒platformBuildVersionC
ode▒platformBuildVersionNammanifest%newtonanalytics.modernportfoliotheory1.11
4.3.1-142564uses-sdkuses-permissionndroid.permission.INTERNET
                                                              applicatioactivi
intent-filteraction▒android.intent.action.MAIcategory android.intent.category
.LAUNCHER4newtonanalytics.modernportfoliotheory.DisplayContact9newtonanalytic
Your Settings)newtonanalytics.modernportfoliotheory.Run0
                                                          ◆▒◆◆◆◆


◆◆◆◆◆◆◆◆◆
         ◆◆◆◆
◆◆◆◆◆◆L◆◆◆◆◆◆◆◆
               ◆◆◆◆
```

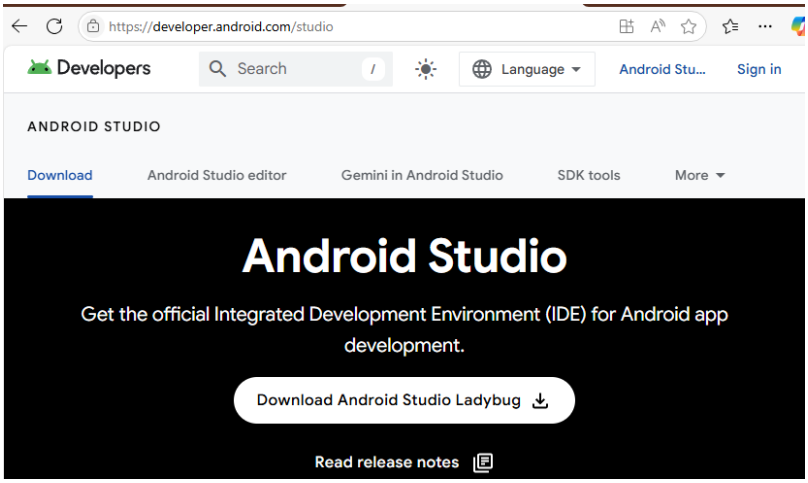
I could not get the next steps to work after this):

Exercise 14.2 - Dynamic Analysis

In this task, I use my host pc (windows). I will install Android Studio/SDK and sideload the "Modern Portfolio" application. Then, I will enter exploit the vulnerable Activity component using the Android debugger utility.

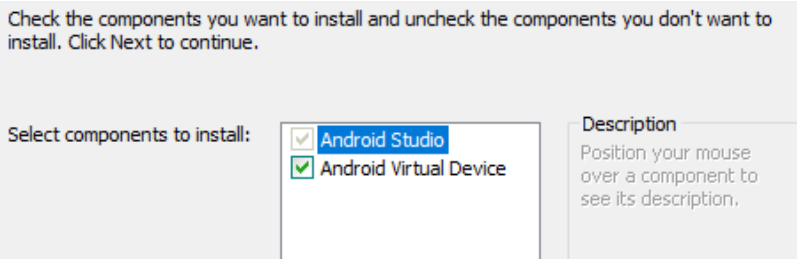
Step 1: Install Android Studio

From my Host PC, I navigated to https://developer.android.com/studio and pressed the "Download Android Studio" button to download the installer.

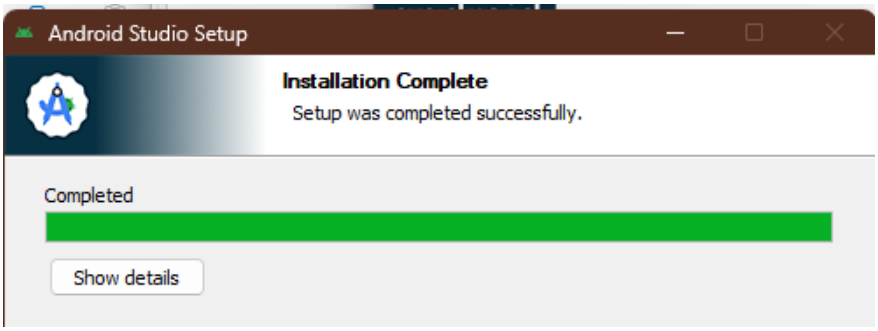


Once it was downloaded, I found the EXE file in my downloads and double clicked it to launch the installation. I accepted the UAC prompts and then clicked next when the Android Studio Wizard Setup popped up.

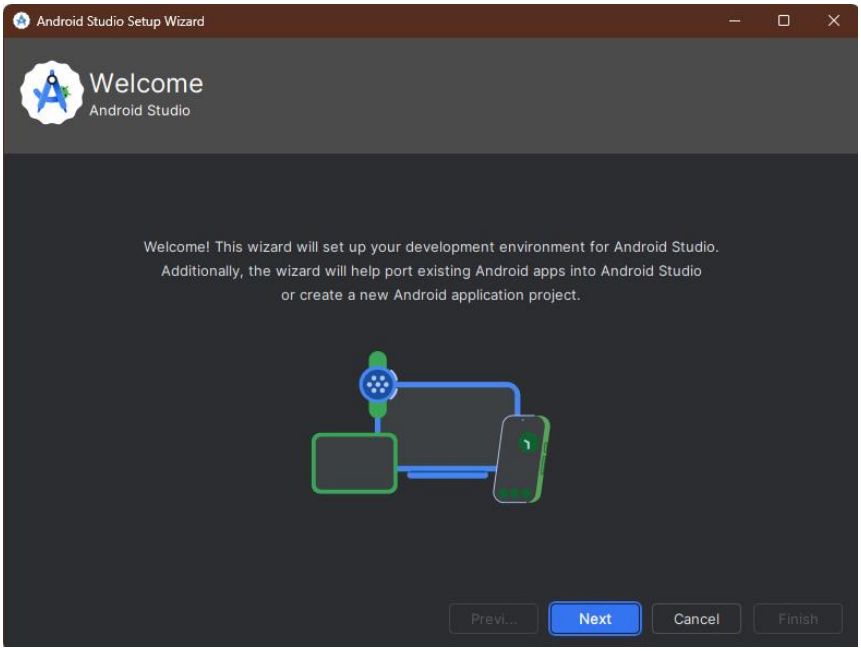
I ensured that the “Android Studio” and the “Android Virtual Device” are selected and pressed next.



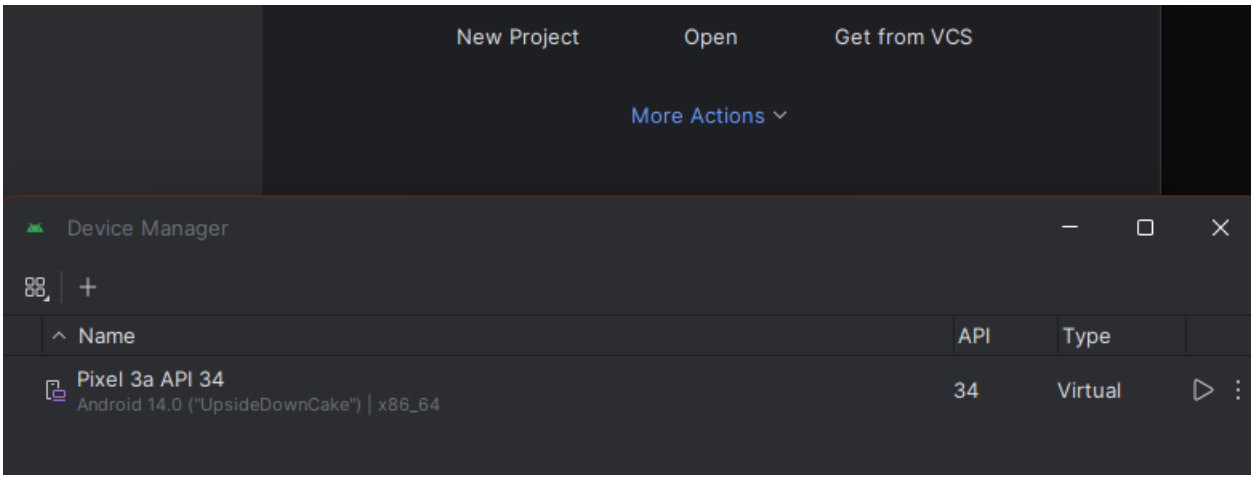
I accepted the default configuration and clicked install.



The “Welcome to Android Studio” window appeared. I have successfully downloaded Android Studio.

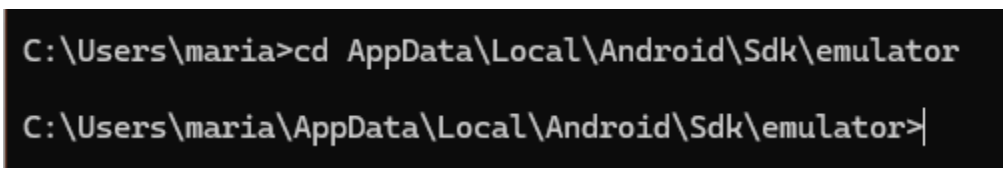


I made sure I had a virtual device created during installation by clicking “more actions” and selected “Virtual Device Manager” and there popped up my virtual device.



Step 2: Launch Emulator

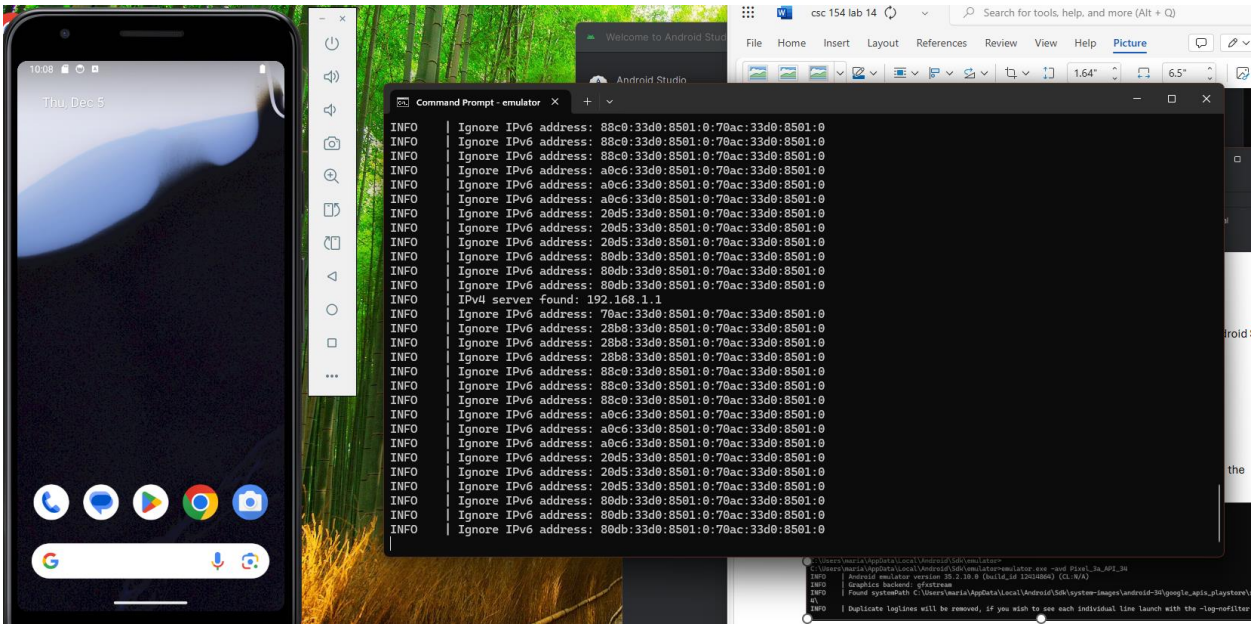
On my Host, I launched a command prompt and changed the directory to the Android SDK emulator folder in my user’s AppData folder.



I listed the Android Virtual Devices (AVD) using the emulator binary. I then started the device emulator .

```
C:\Users\maria\AppData\Local\Android\Sdk\emulator>emulator.exe -lists-avds
INFO    | Android emulator version 35.2.10.0 (build_id 12414864) (CL:N/A)
INFO    | Graphics backend: gfxstream
ERROR   | No AVD specified. Use '@foo' or '-avd foo' to launch a virtual device named 'foo'


C:\Users\maria\AppData\Local\Android\Sdk\emulator>
C:\Users\maria\AppData\Local\Android\Sdk\emulator>emulator.exe -avd Pixel_3a_API_34
INFO    | Android emulator version 35.2.10.0 (build_id 12414864) (CL:N/A)
INFO    | Graphics backend: gfxstream
INFO    | Found systemPath C:\Users\maria\AppData\Local\Android\Sdk\system-images\android-34\google_apis_playstore\x86_6
4\
INFO    | Duplicate loglines will be removed, if you wish to see each individual line launch with the -log-nofilter flag
.
```



Step 3: Download the APK

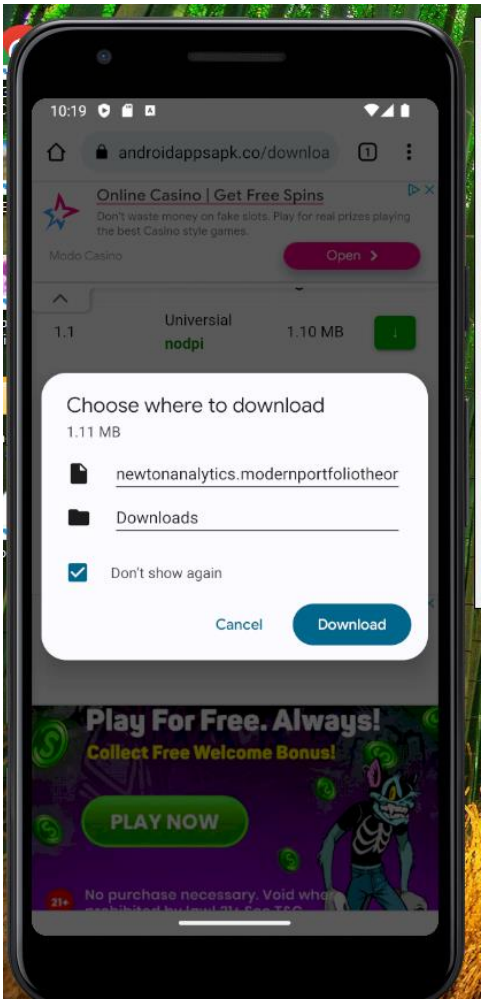
(skipped because it is not needed as I have already downloaded it)

Step 4: Exploit Vulnerable Intent

I opened another Terminal on my host computer and navigated to my user's AppData\Local\Android\Sdk\platform-tools directory.

```
PS C:\Users\maria> cd .\AppData\Local\Android\Sdk\platform-tools\
PS C:\Users\maria\AppData\Local\Android\Sdk\platform-tools>
```

I installed the APK application using Android debugger.




```
PS C:\Users\maria\AppData\Local\Android\Sdk\platform-tools> .\adb.exe install --bypass-low-target-sdk-block C:\Users\mar
ia\Downloads\newtonanalytics.modernportfoliotheory_1.1_androidappsapk.co.apk
Performing Streamed Install
Success
PS C:\Users\maria\AppData\Local\Android\Sdk\platform-tools>
```

Then, I entered an Android Debugger shell that launches a terminal session on the emulator device.

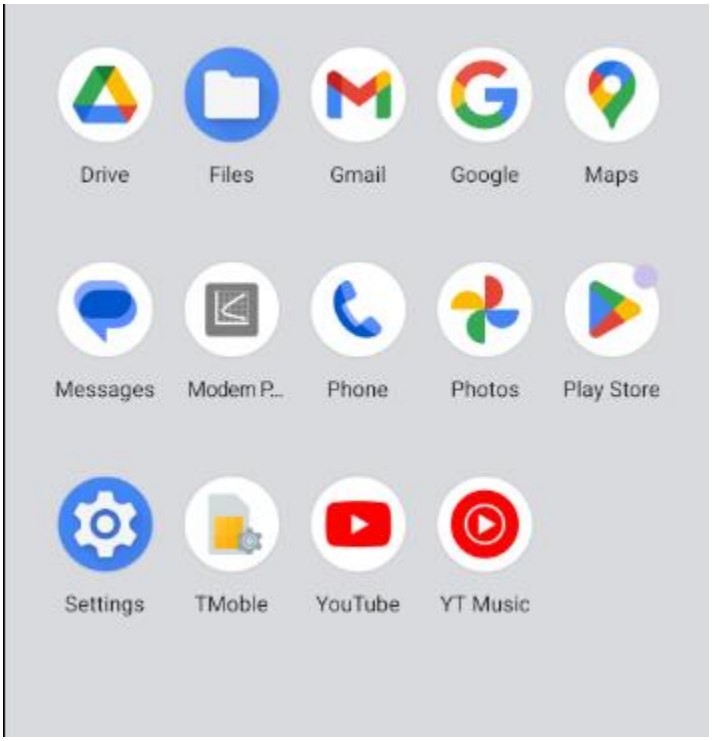
```
PS C:\Users\maria\AppData\Local\Android\Sdk\platform-tools> .\adb.exe shell
emu64xa:/ $
```

Next, I listed the packages installed on the device while in the adb shell. I observed Modern Portfolio is included in the list.

```
emu64xa:/ $ pm list packages
package:com.android.systemui.auto_generated_rro_vendor__
package:com.google.android.providers.media.module
package:com.google.android.overlay.permissioncontroller
package:com.google.android.overlay.googlewebview
```

```
package:com.google.android.health.connect.backuprestore
package:com.android.systemui.emulation.pixel_8_pro
package:com.google.android.settings.intelligence
package:newtonanalytics.modernportfoliotheory
package:com.android.systemui.emulation.pixel_3
package:com.android.systemui
package:com.android.wallpapercropper
```

I opened the apps page on my emulator and observed Modern Portfolio is installed.



I sent an intent from the debugger to evidence open Activity using the Android debugger.