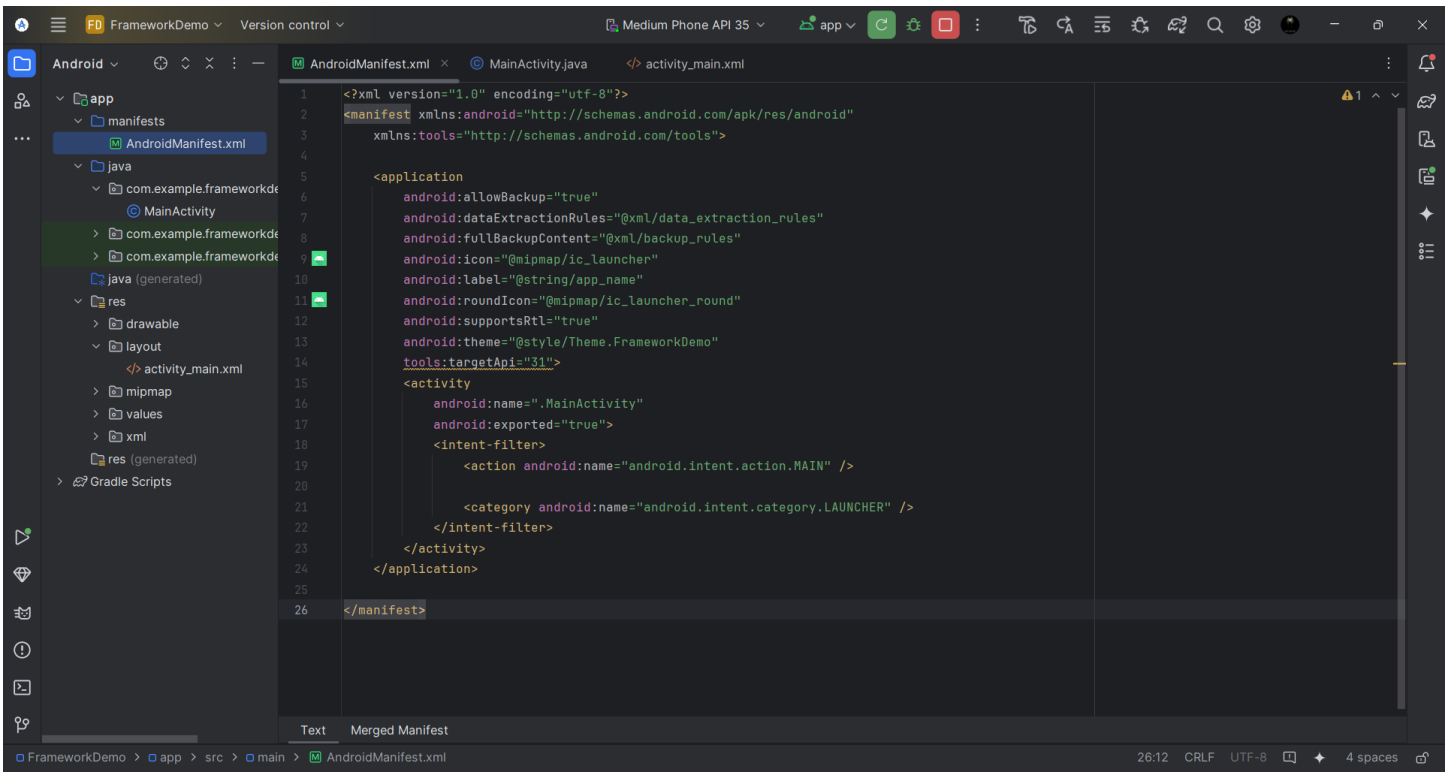
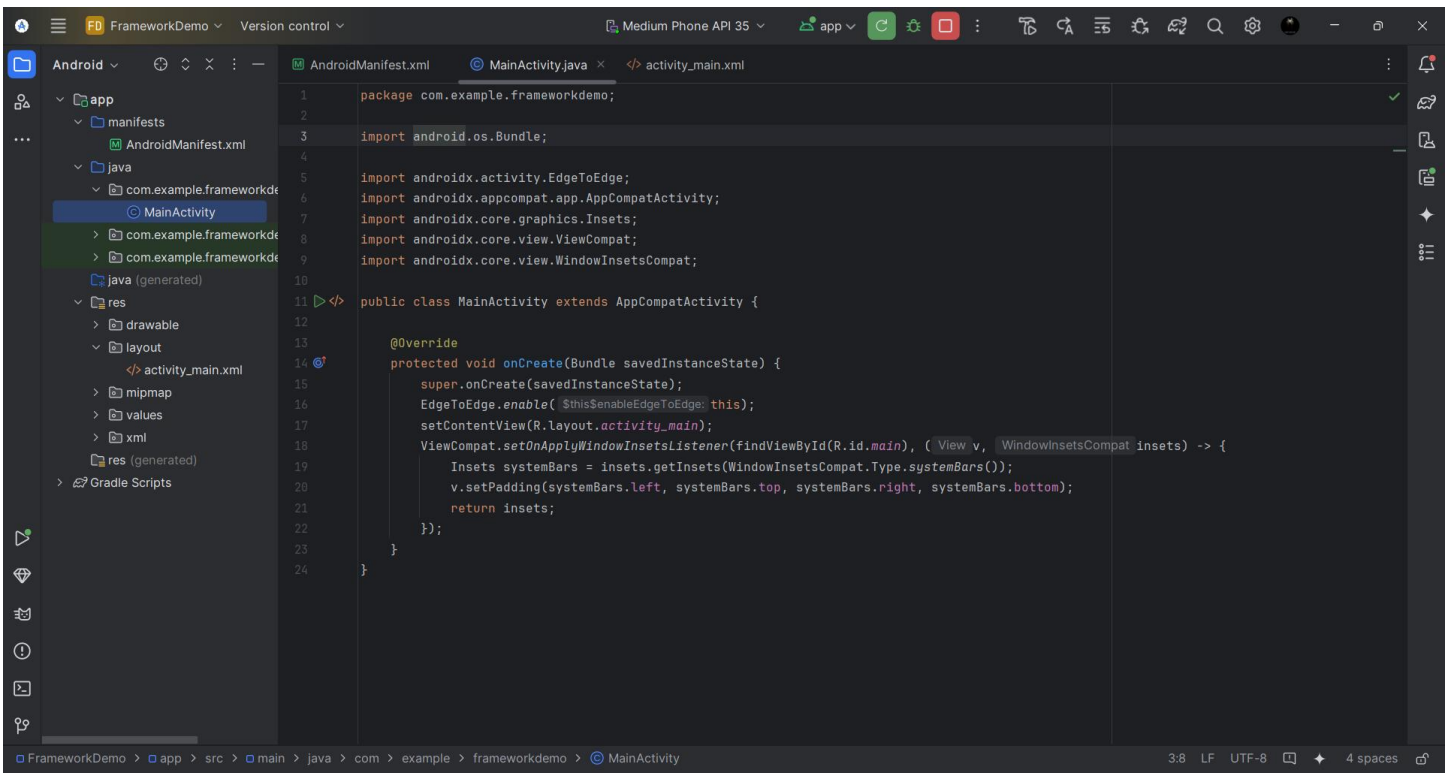
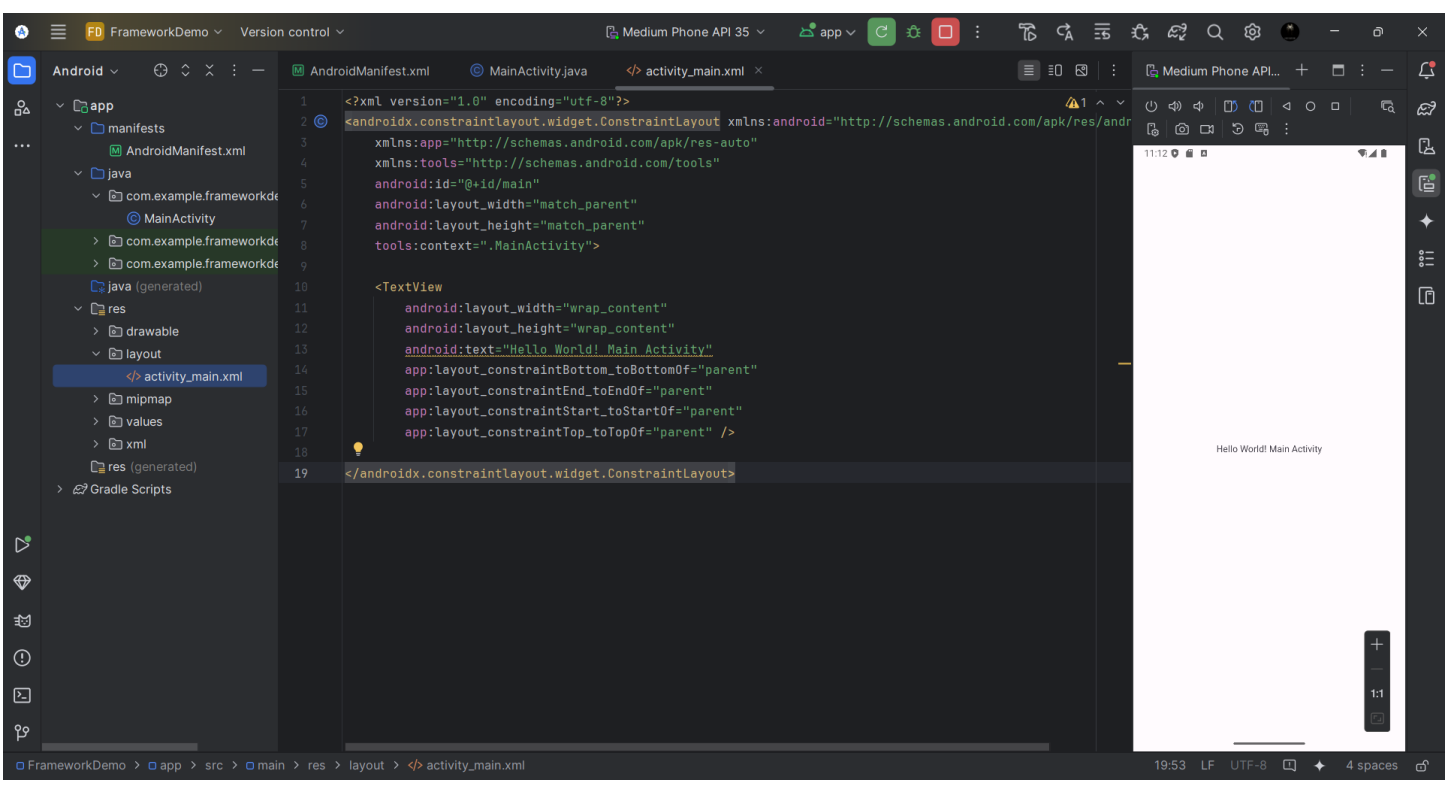
MSF TA2 Assignment

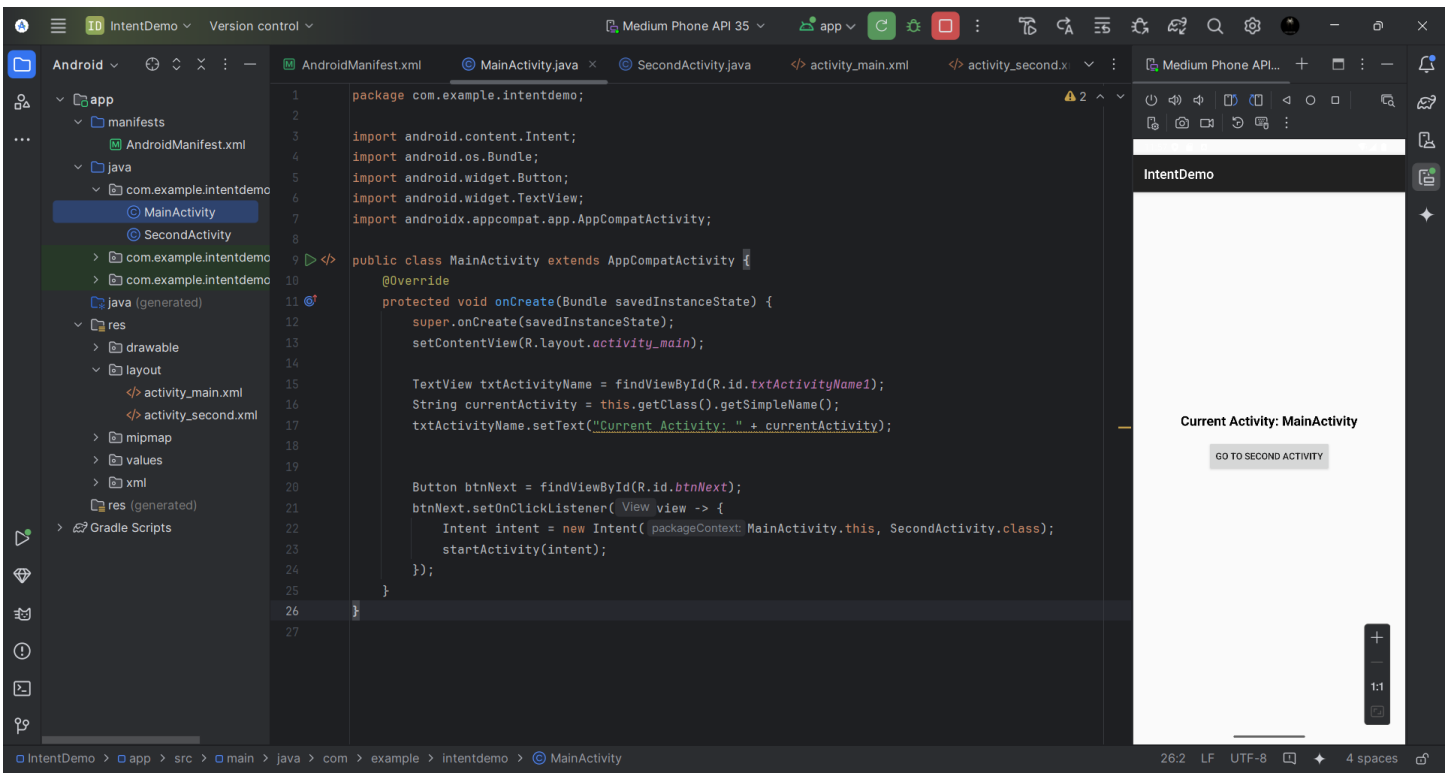
[1]. Demonstration of Android Application Framework component such as Activity and android manifest file etc. using Android Studio

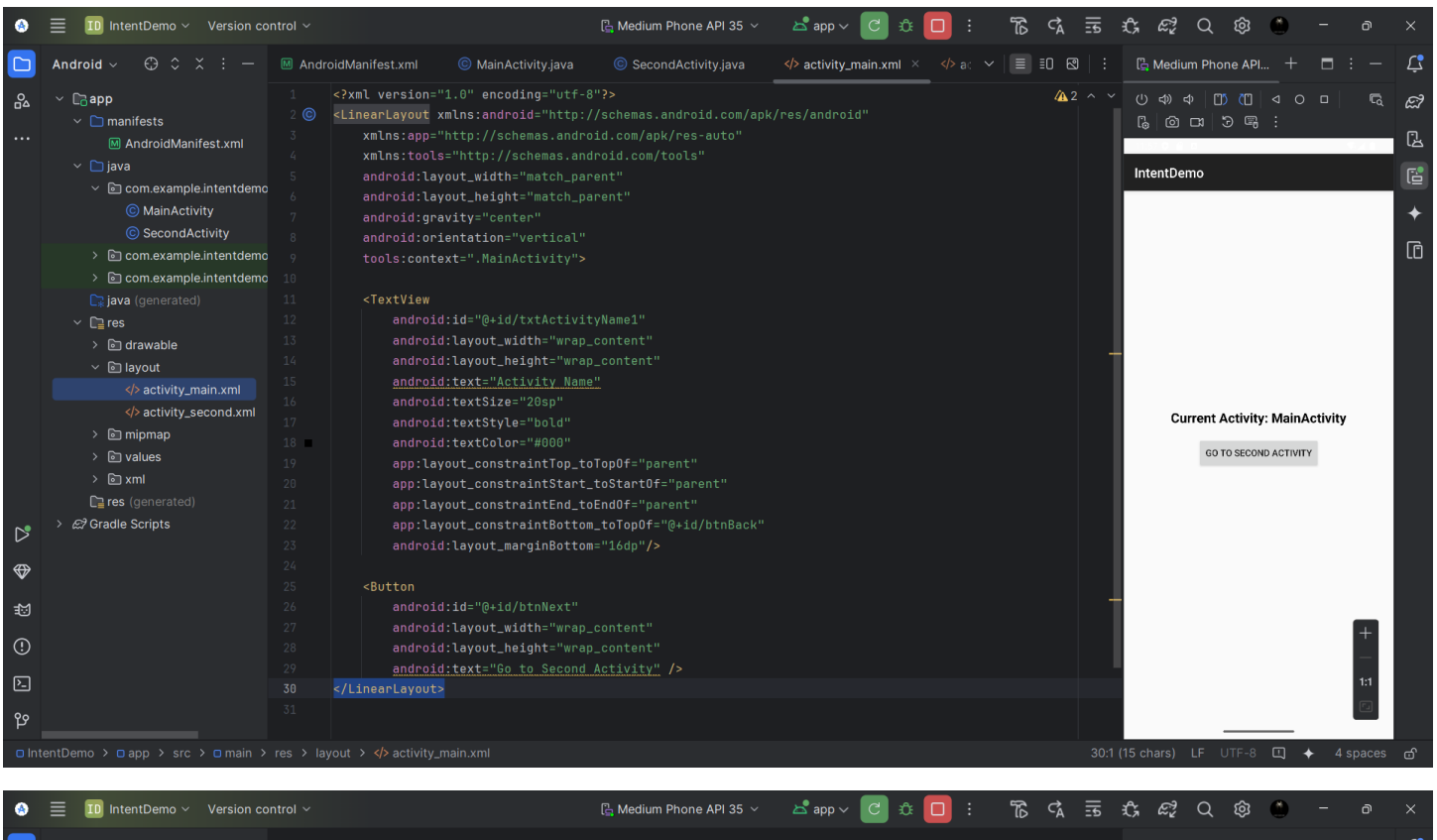


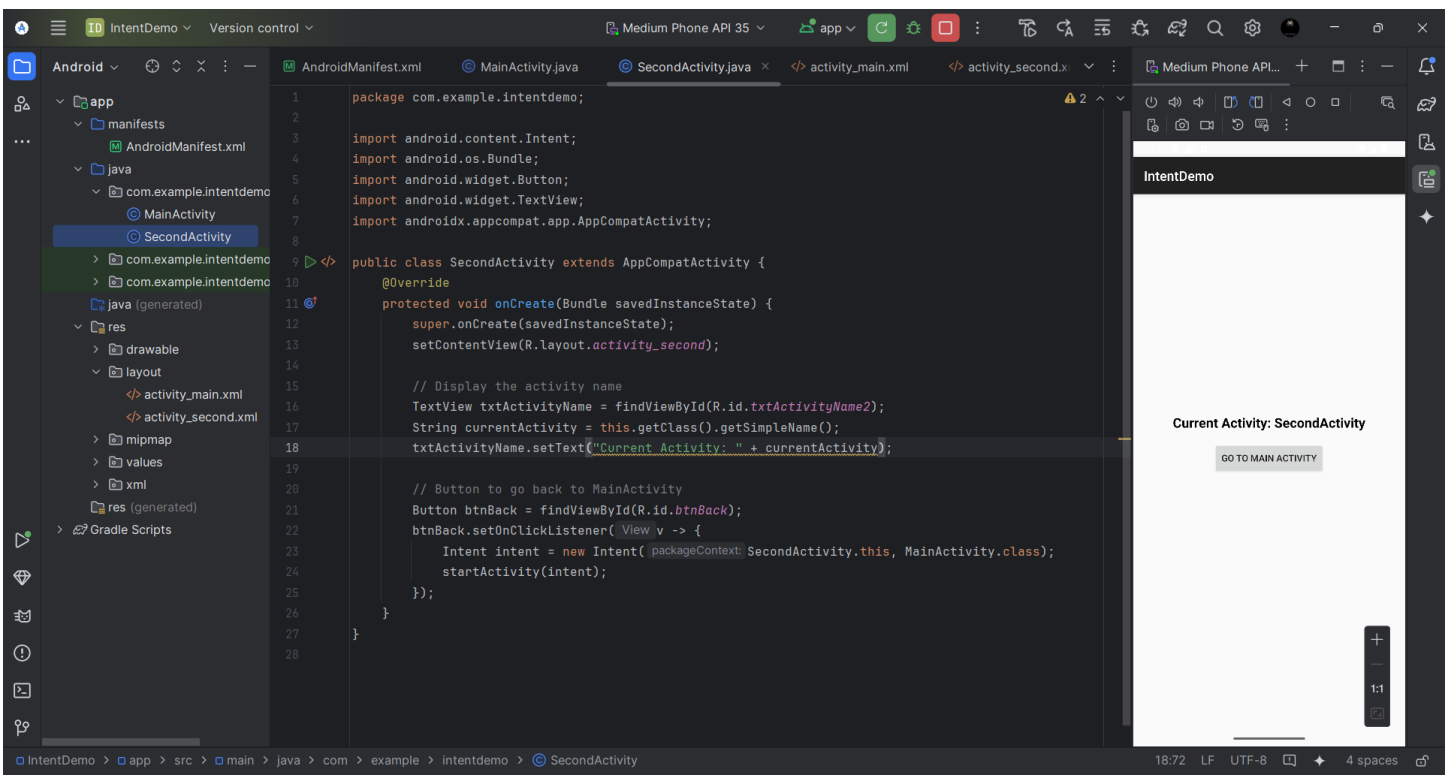


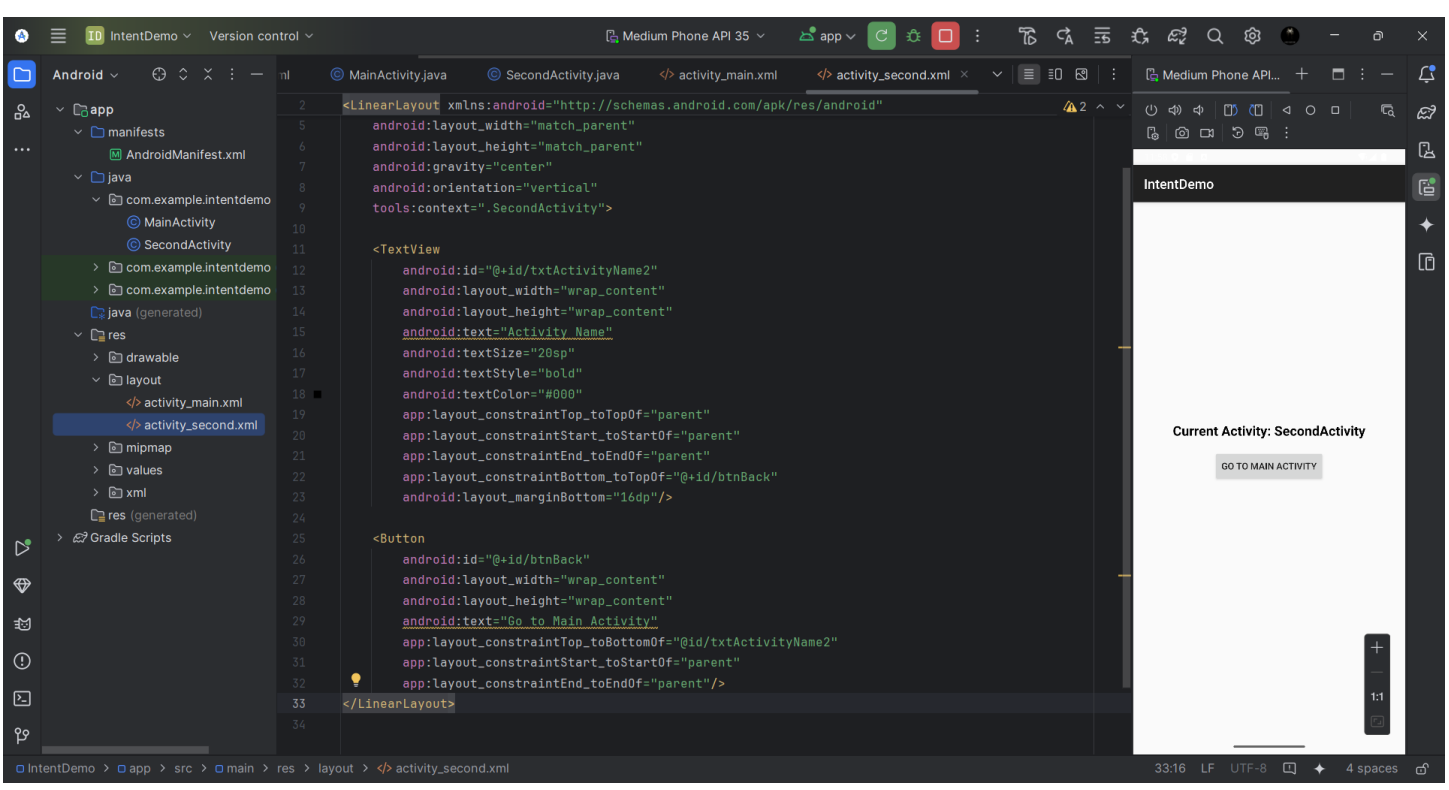


[2]. Demonstration of Android Intent

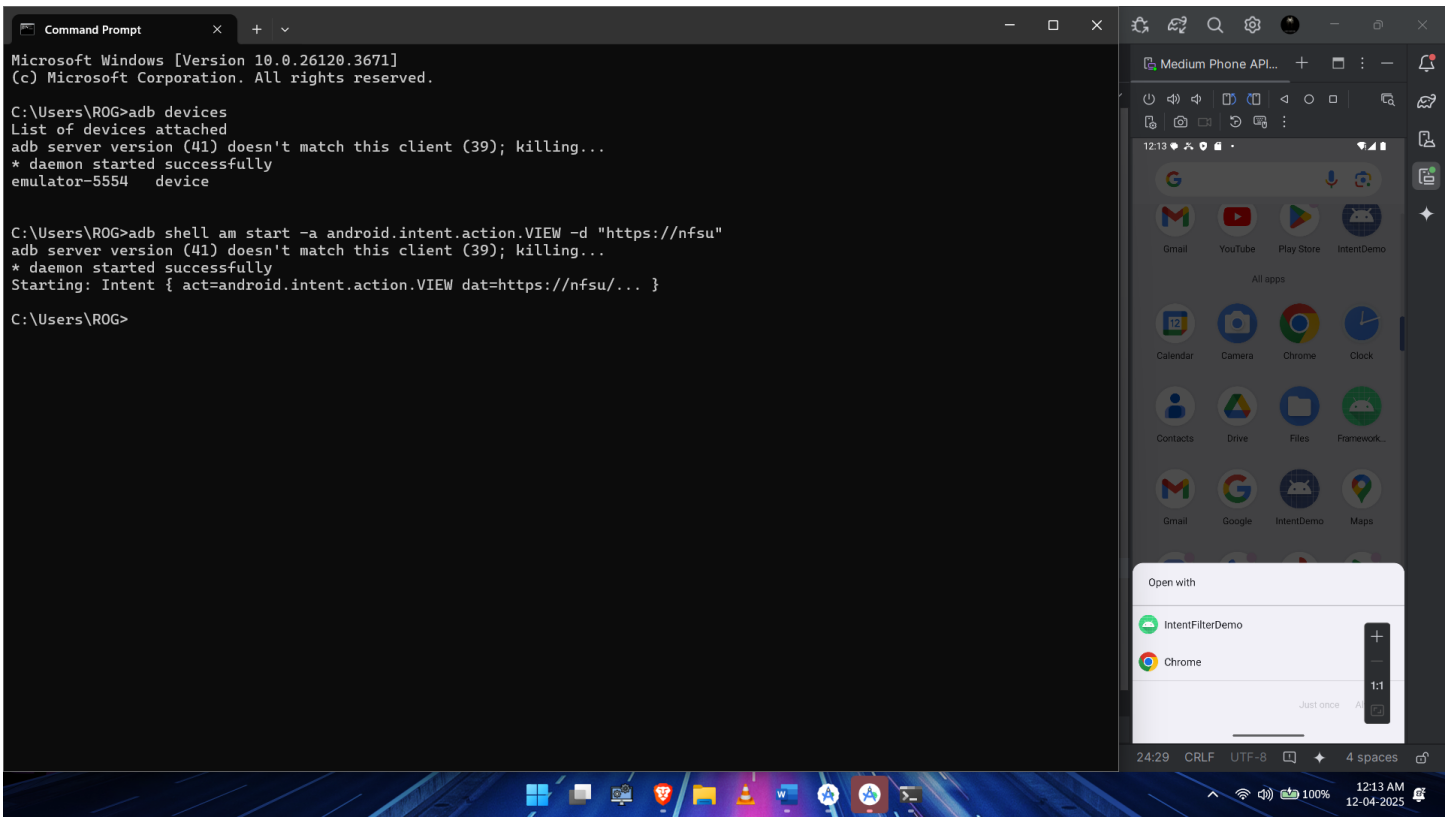


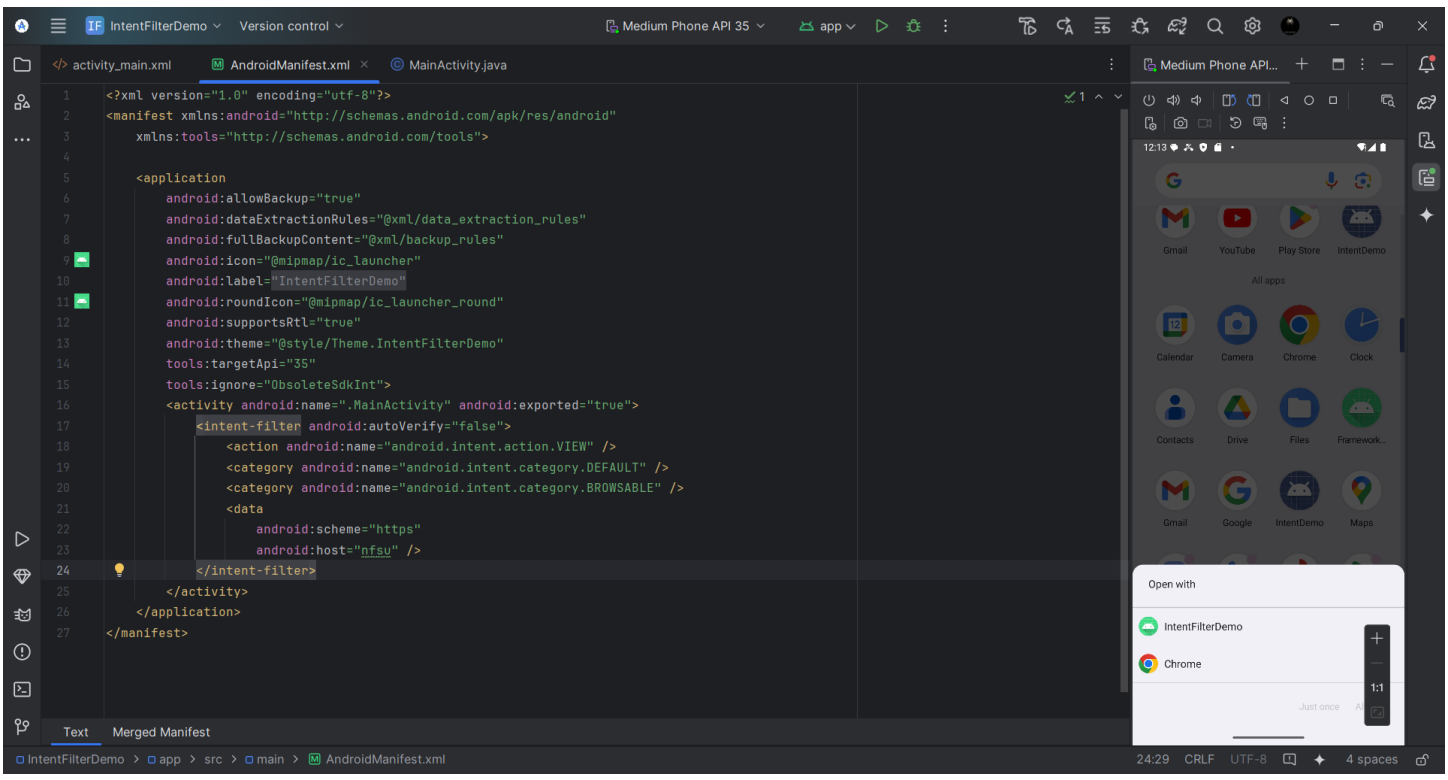


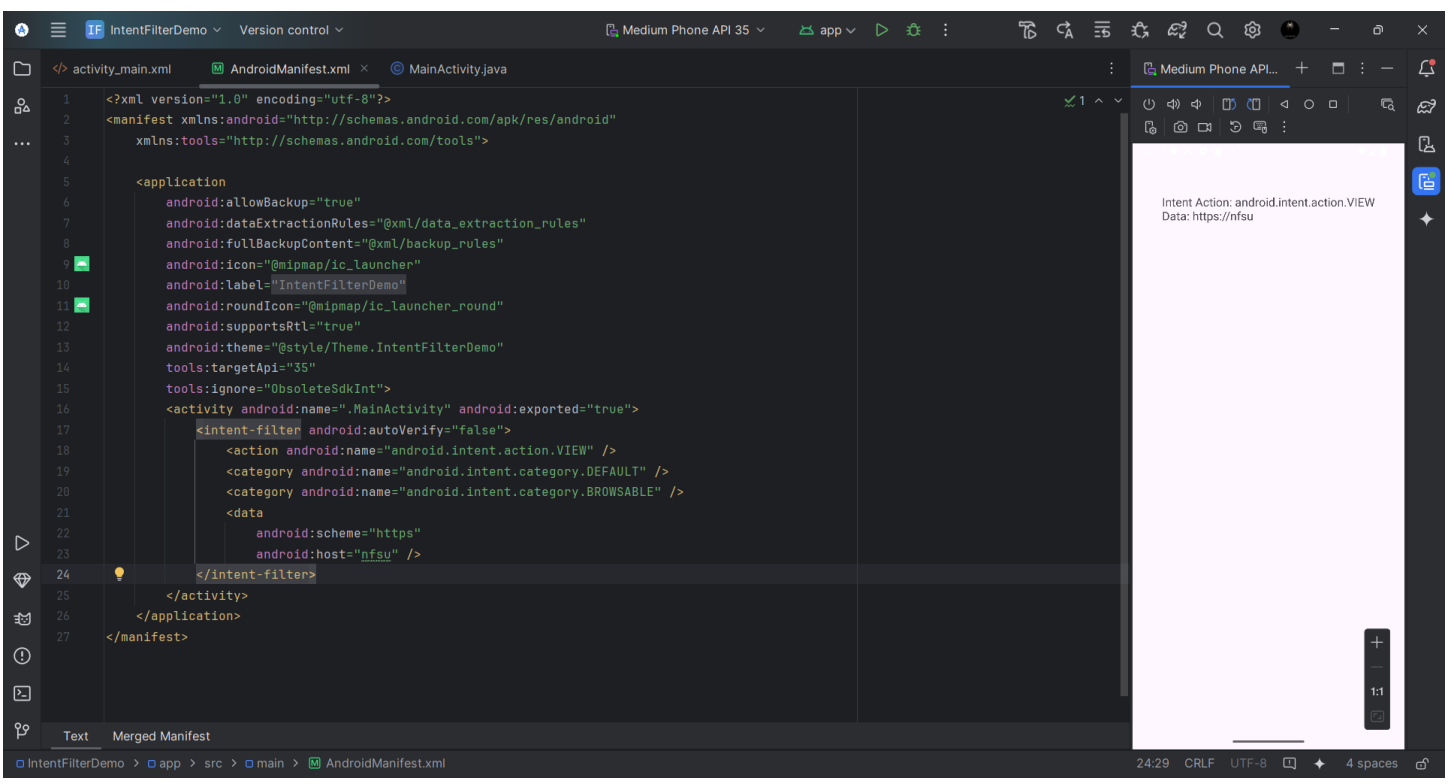




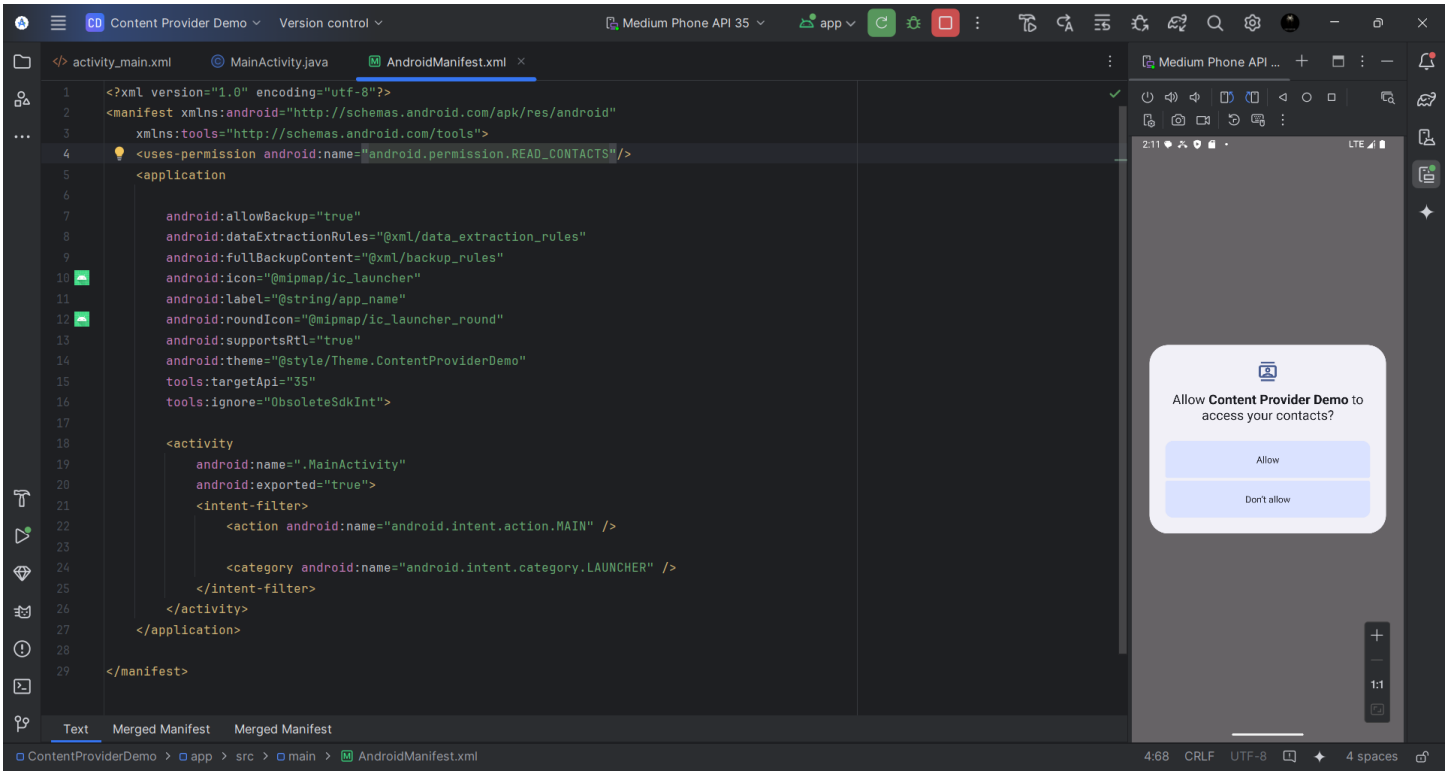
[3]. Demonstration of Android Intent Filter

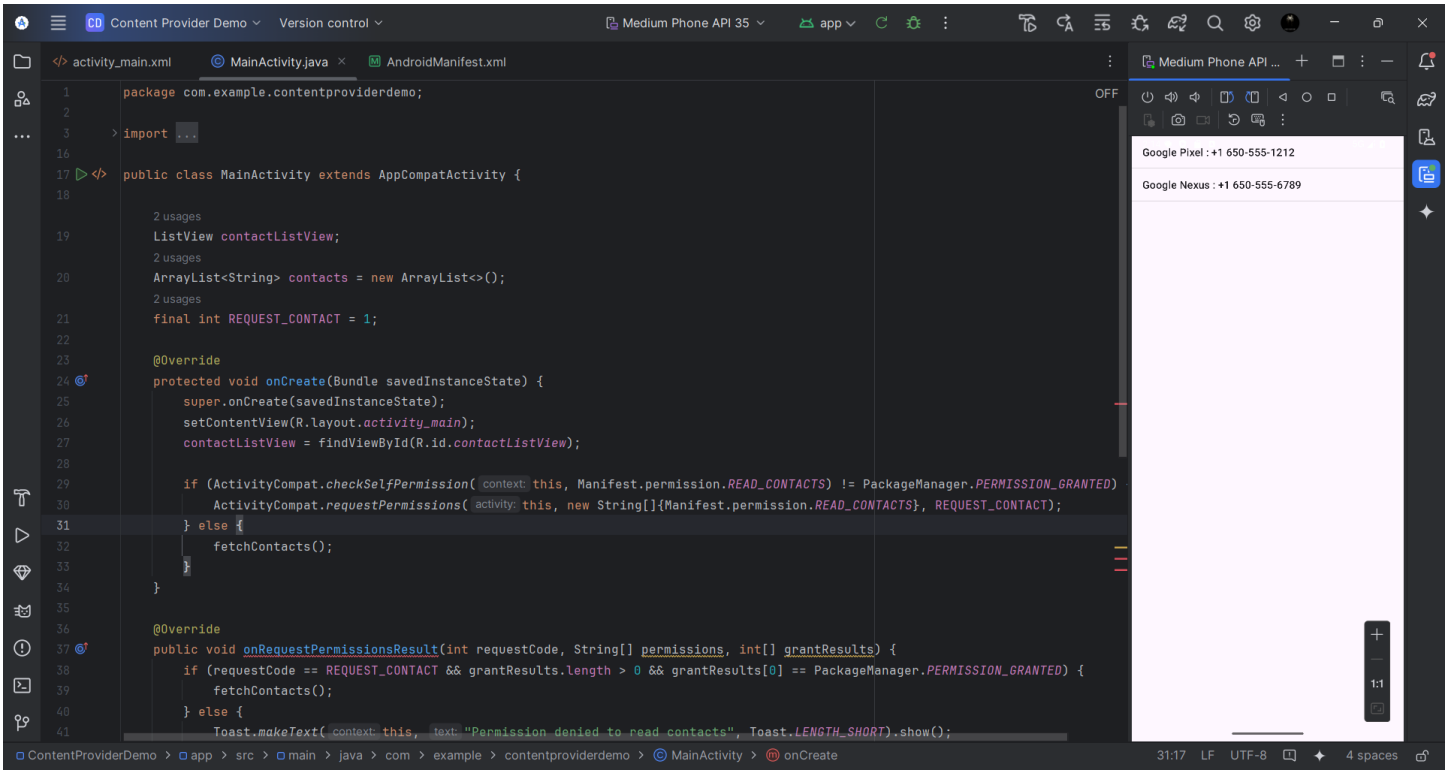




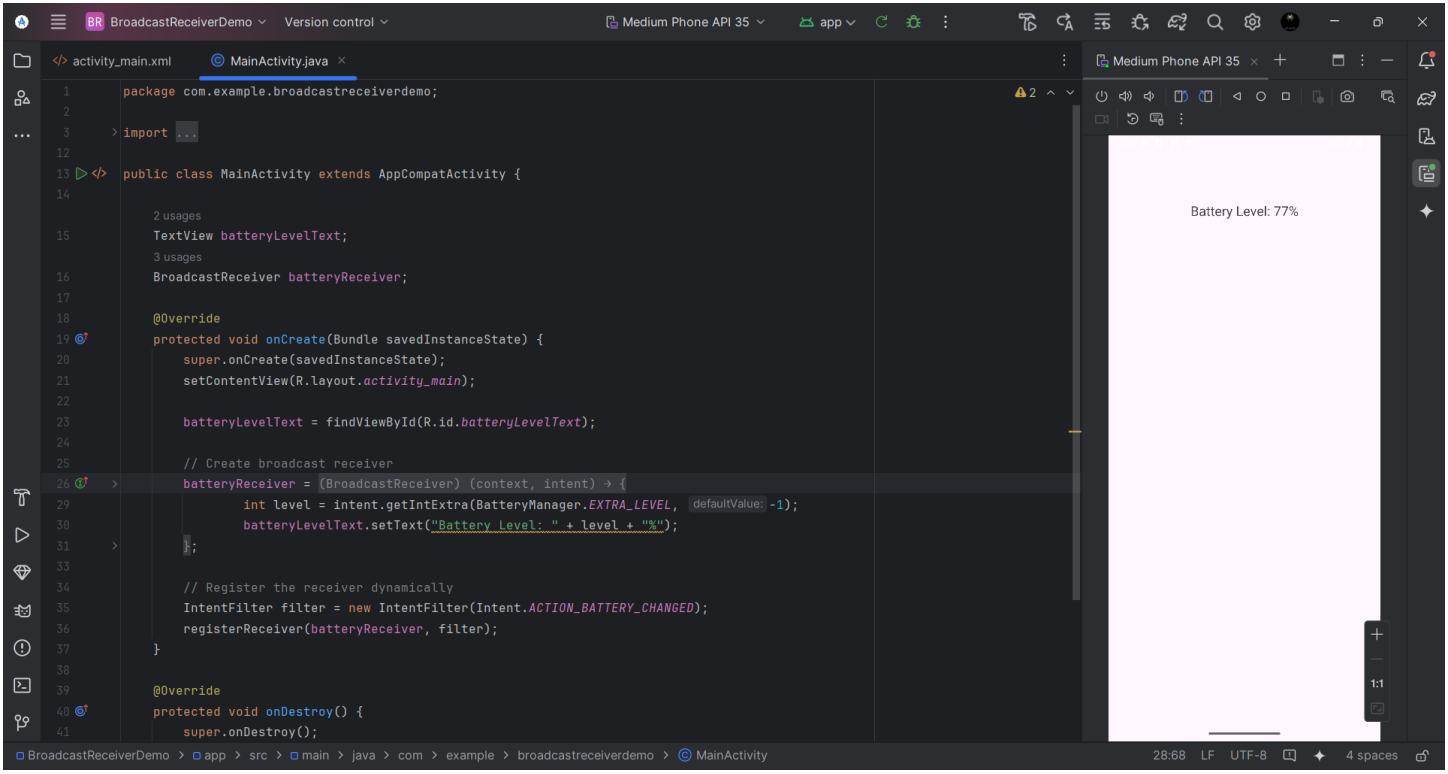


[4]. Demonstration of Android Content Provider

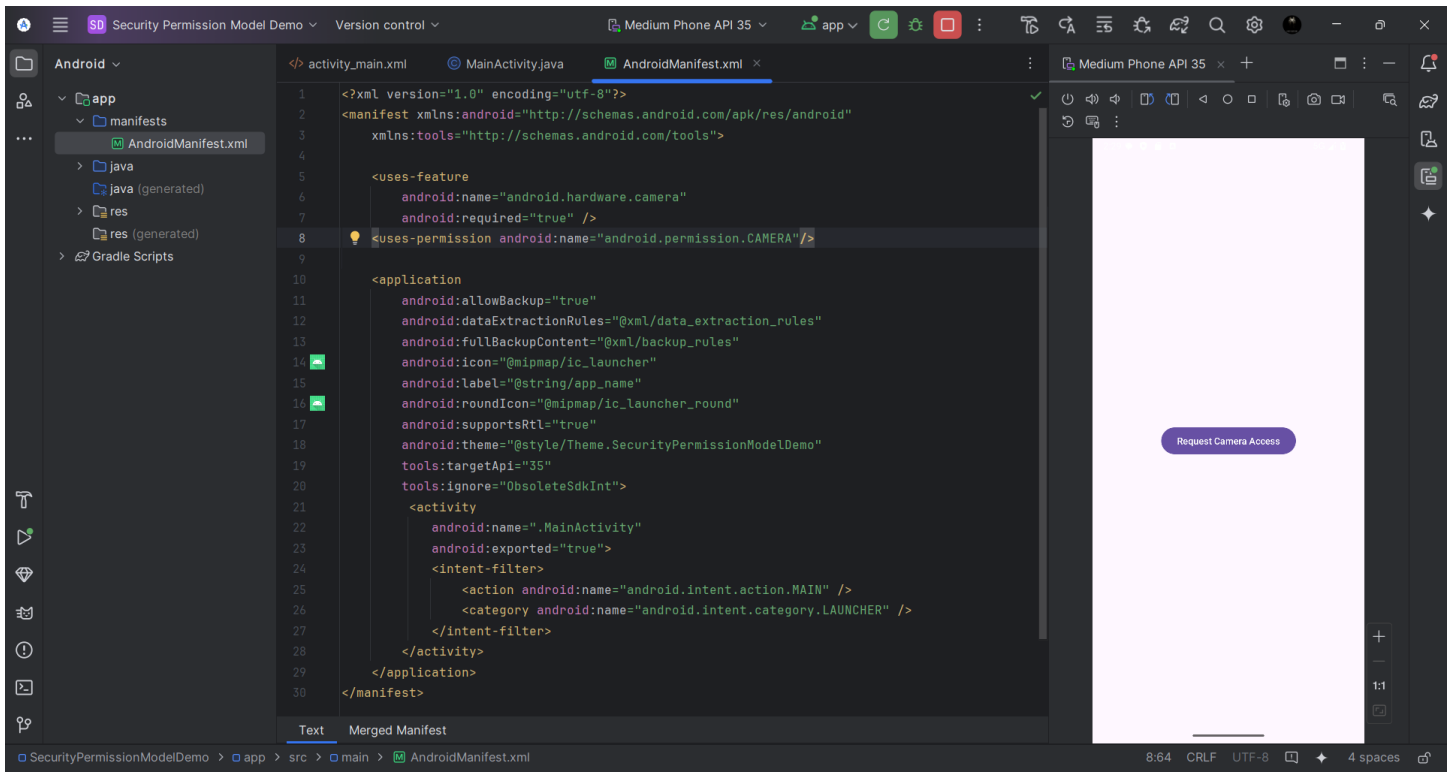


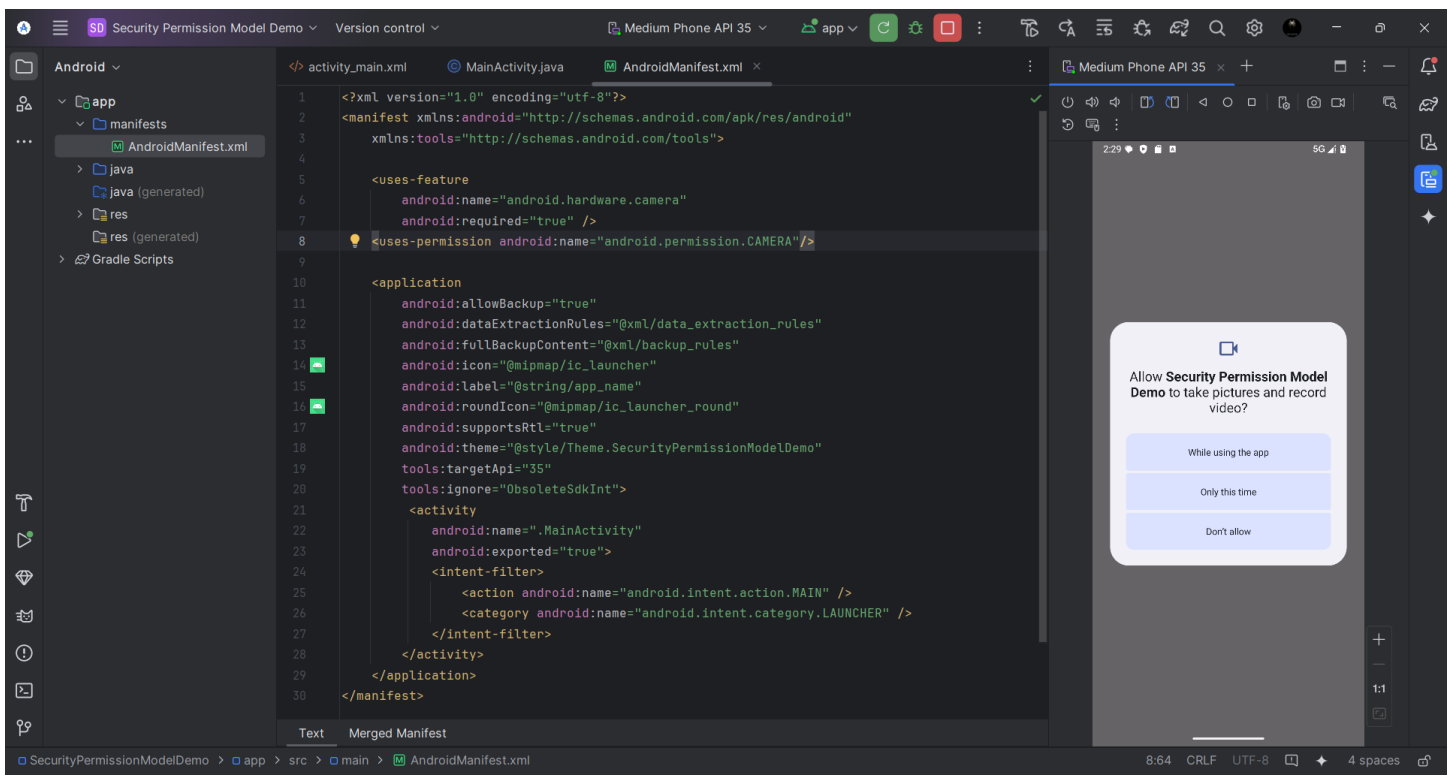


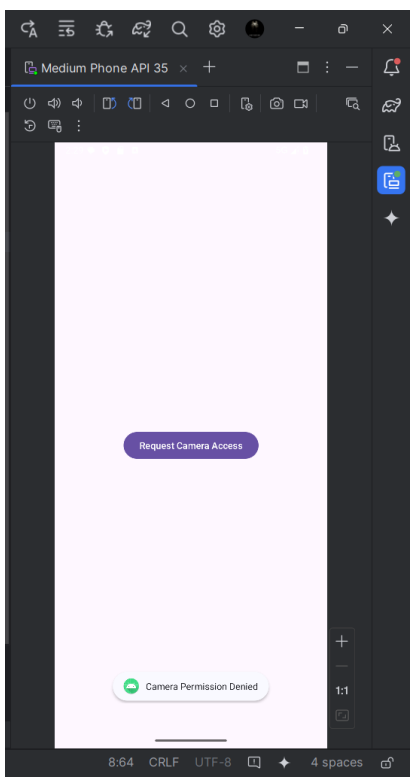
[5]. Demonstration of Android Broadcast Receiver

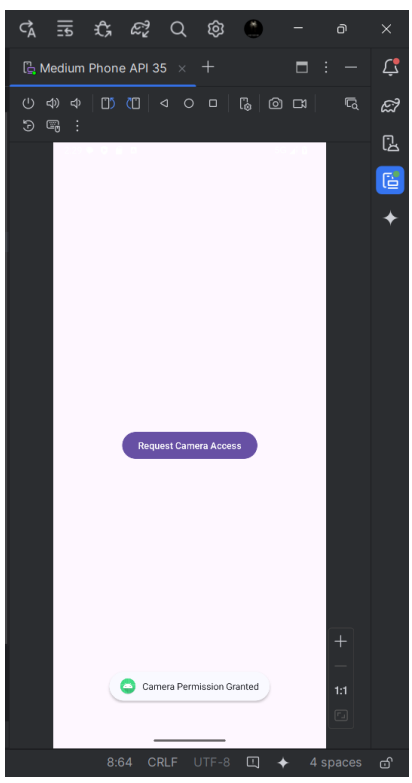


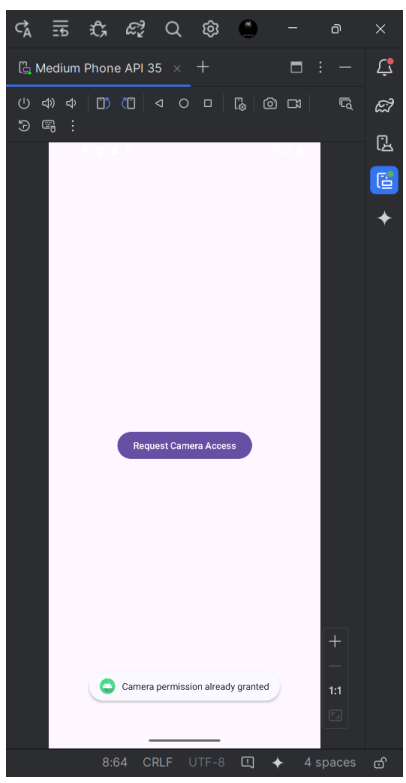
[6]. Demonstration of Android Security Permission Model



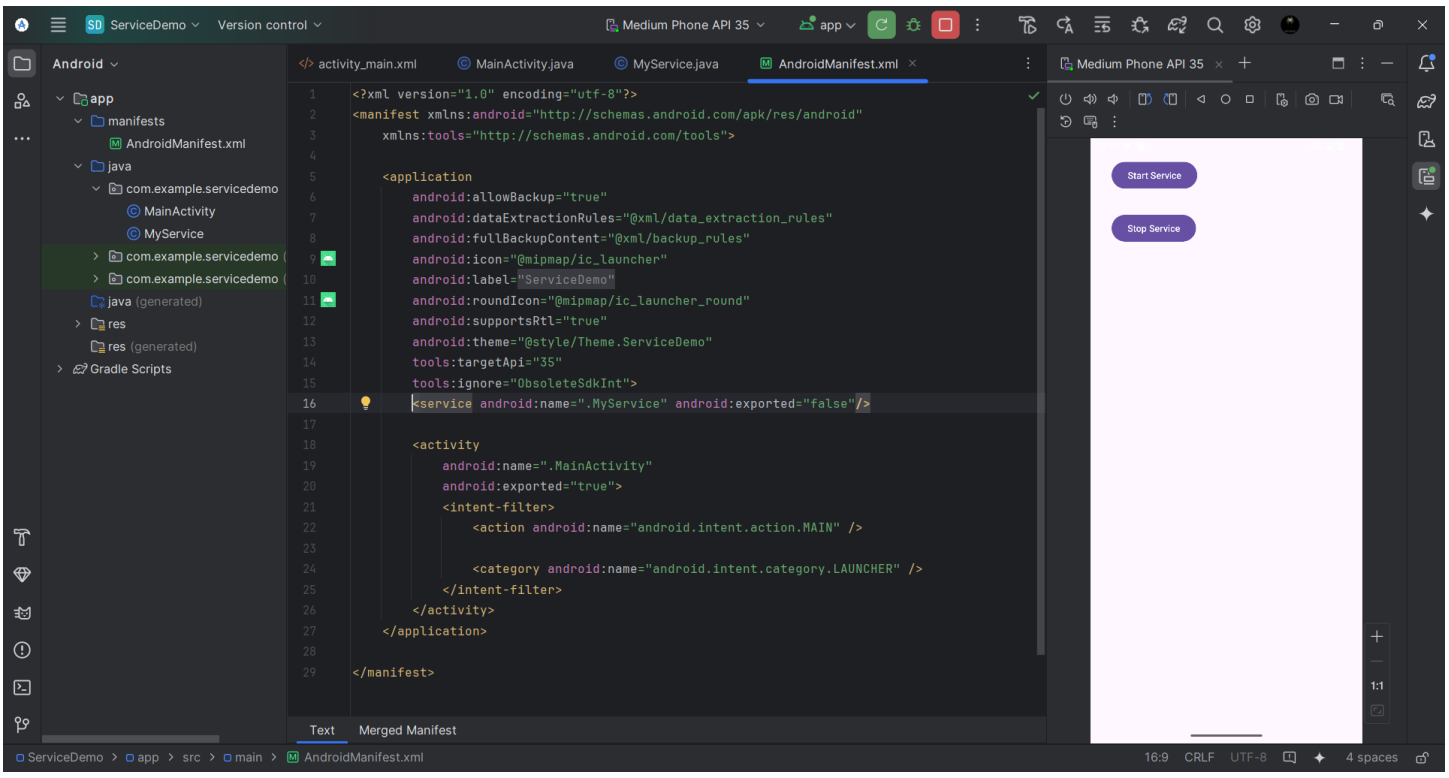


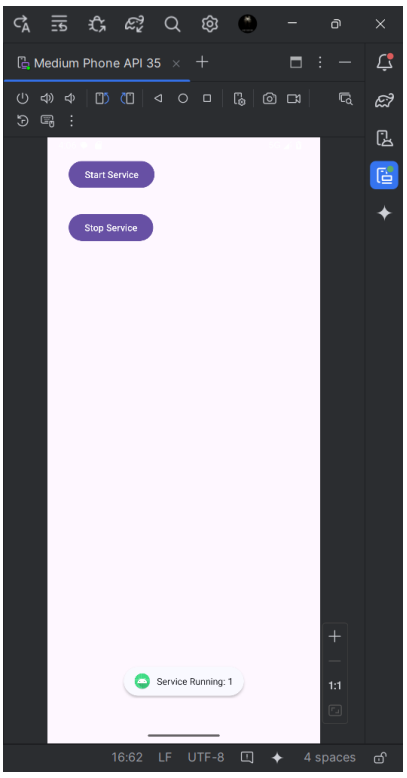


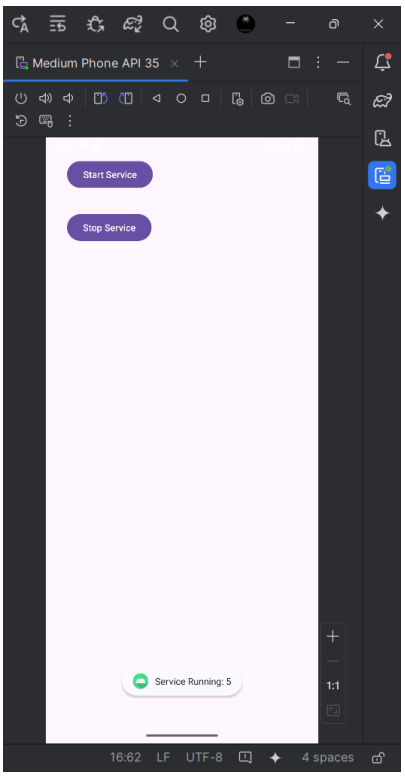


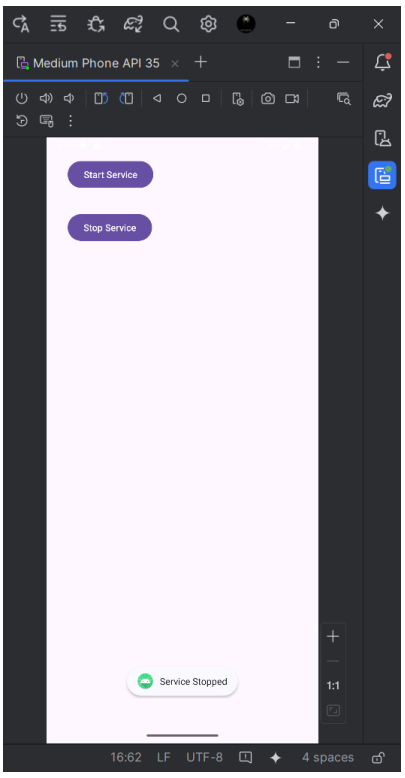


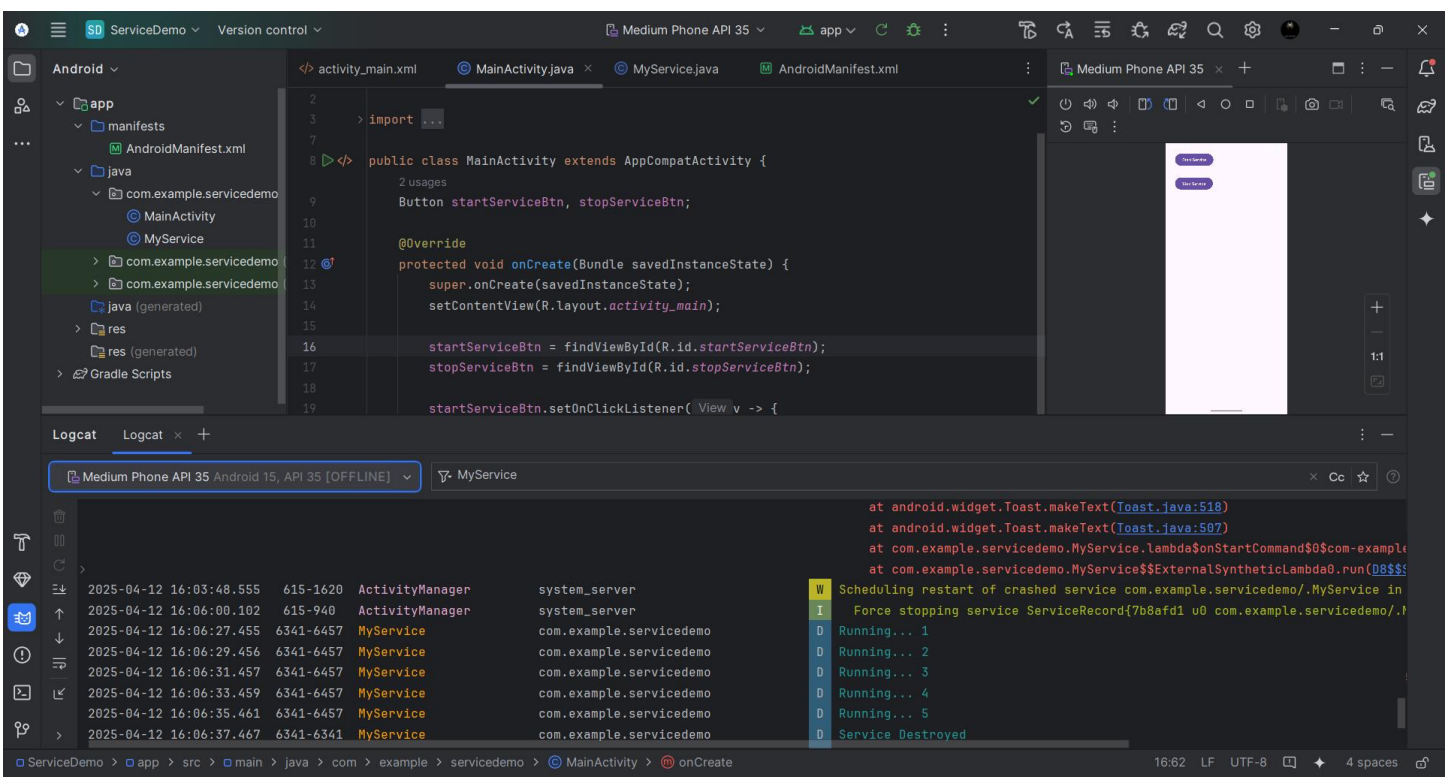
[7]. Demonstration of Android Services



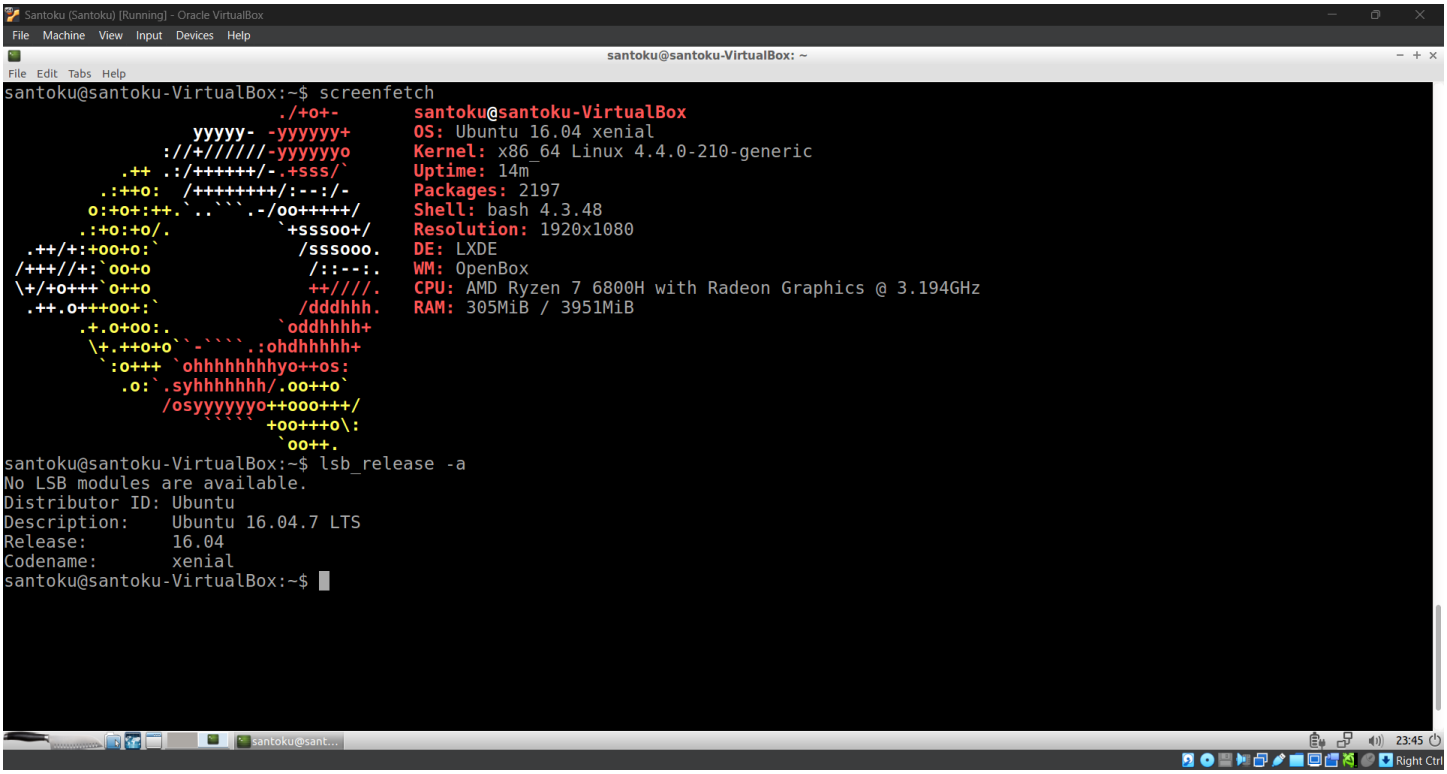


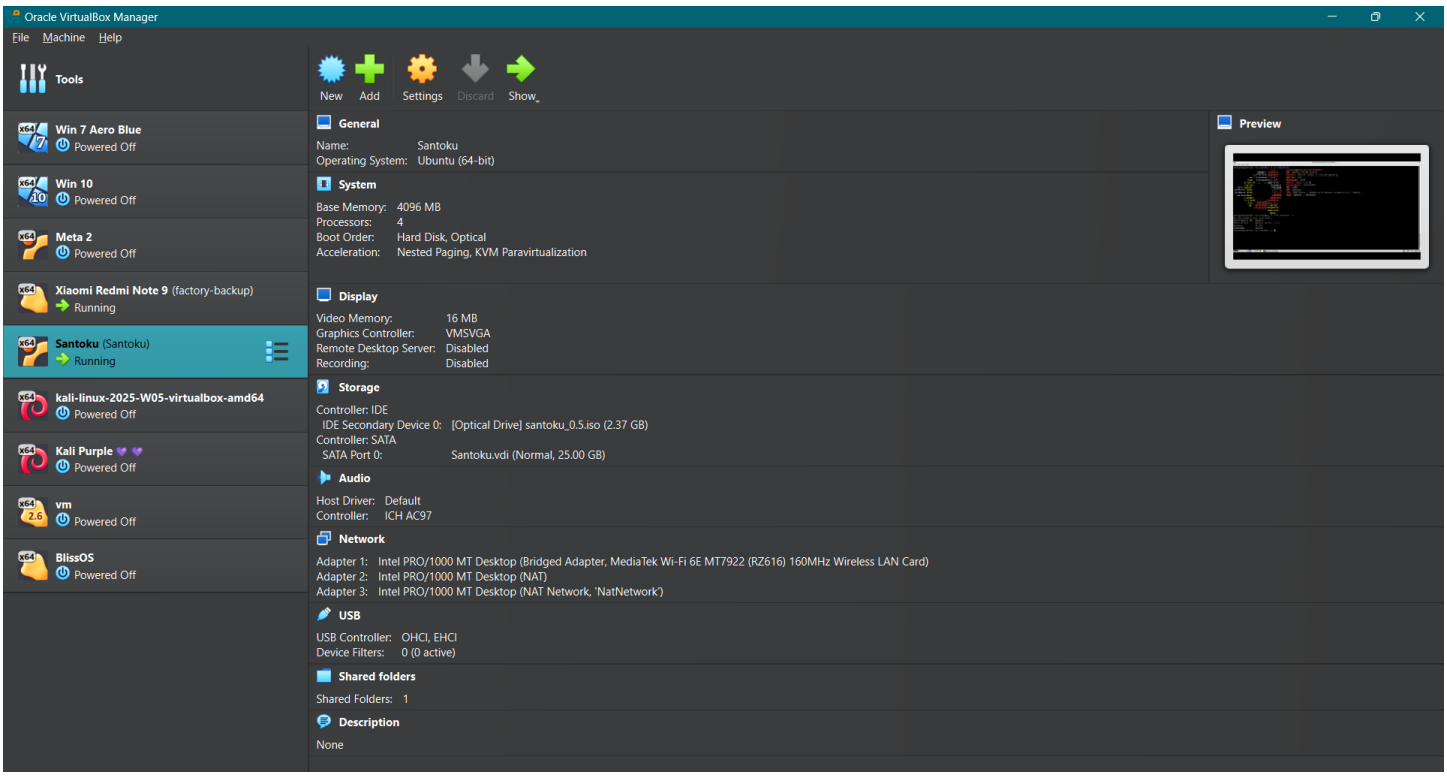




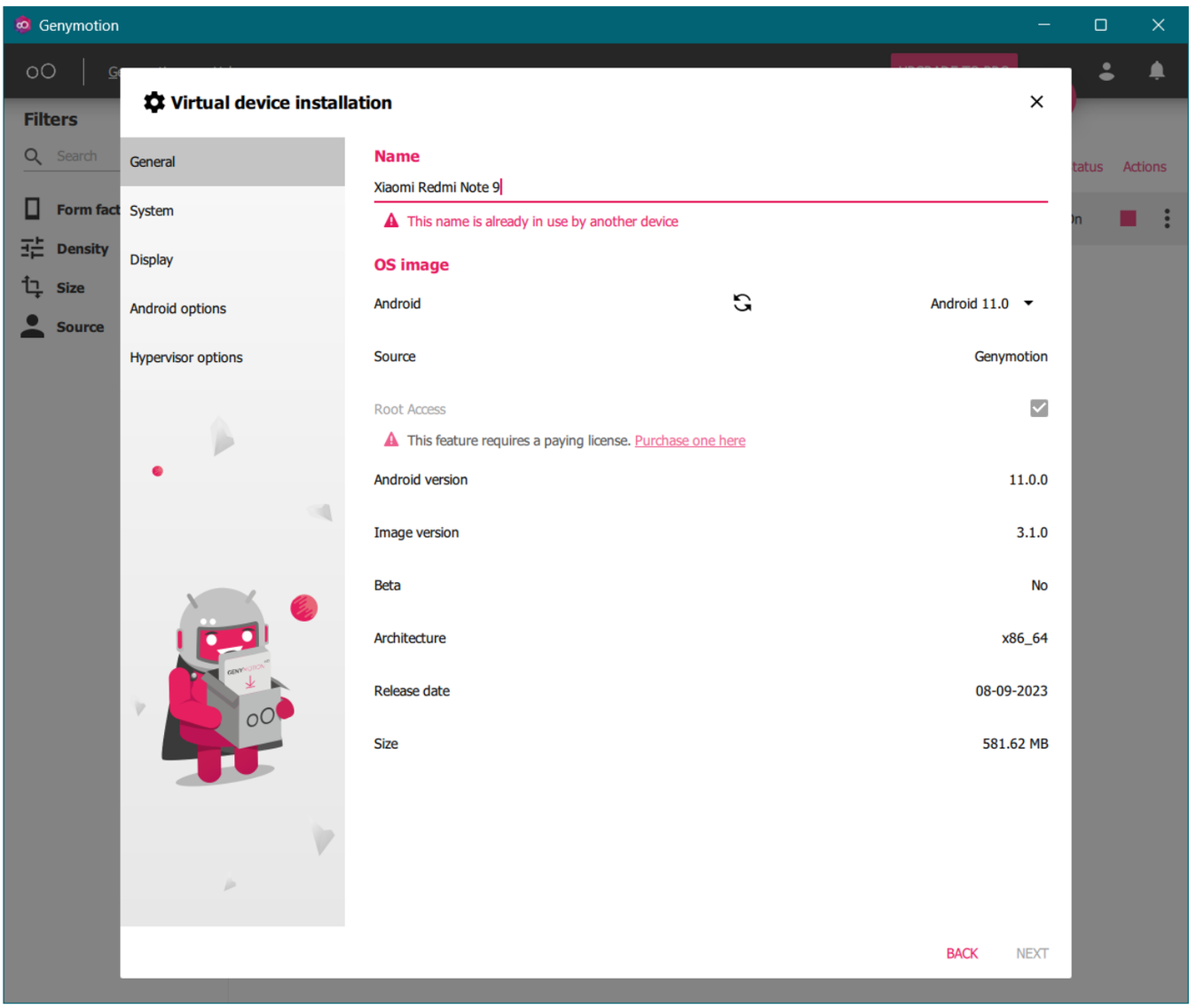


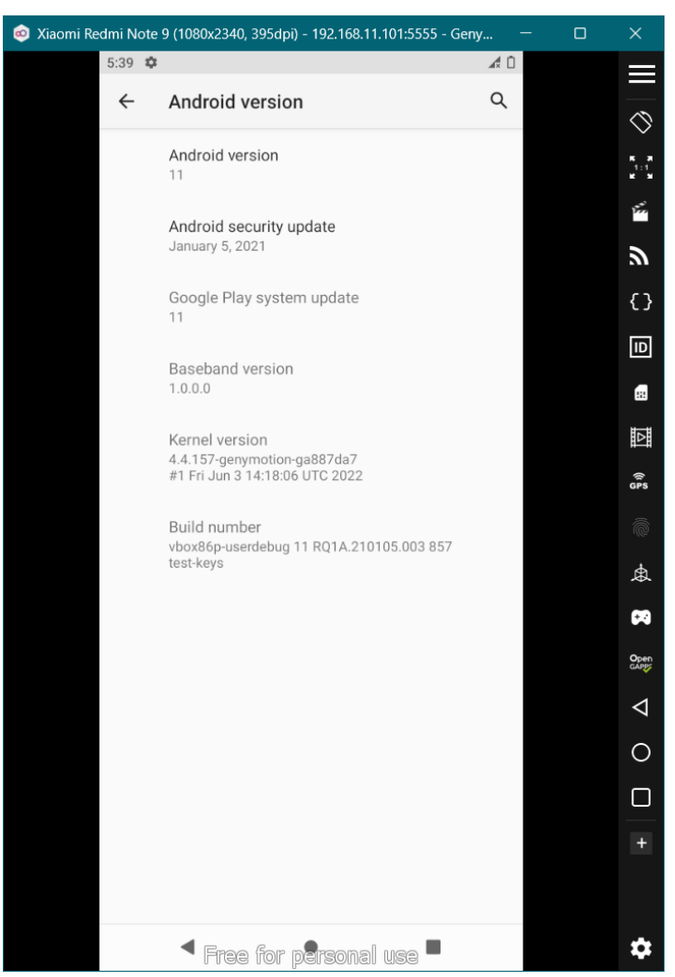
[8]. Configuration of Santoku OS



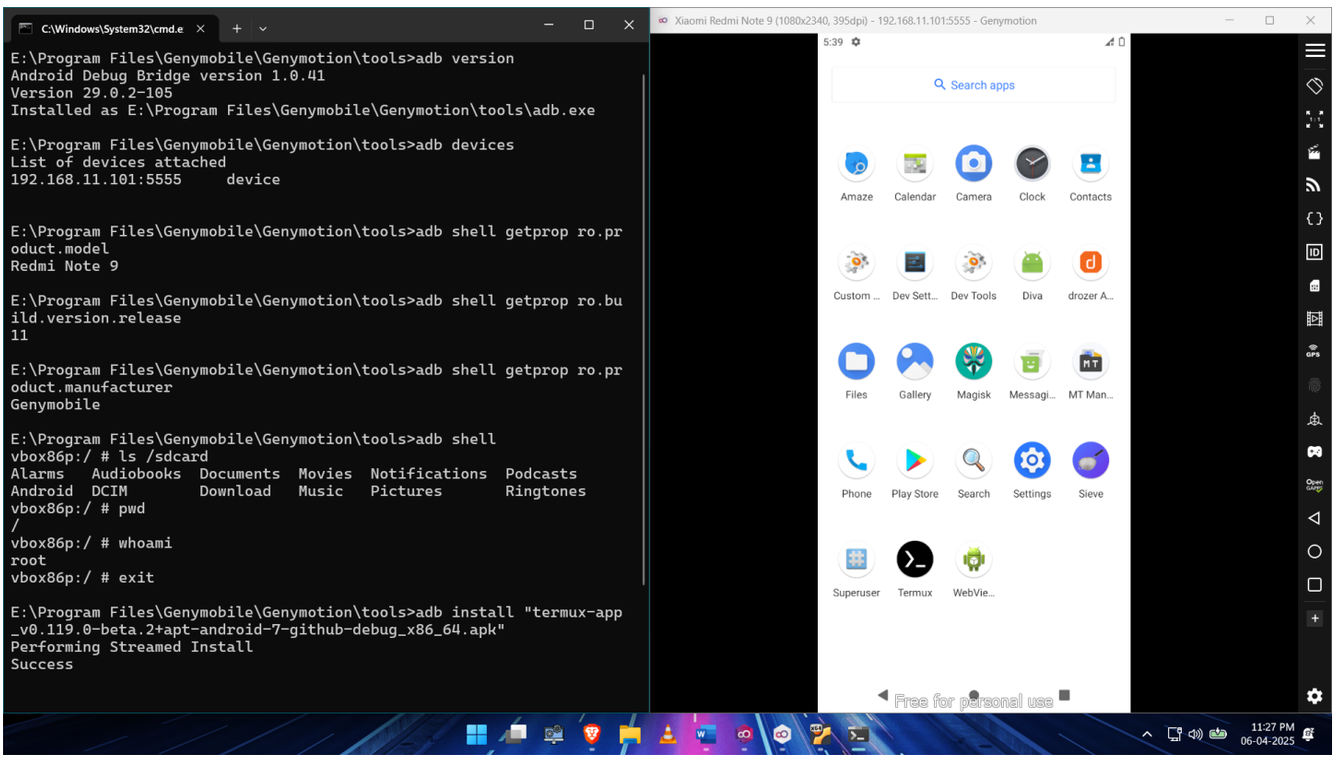


[9]. Configuration of Genymotion

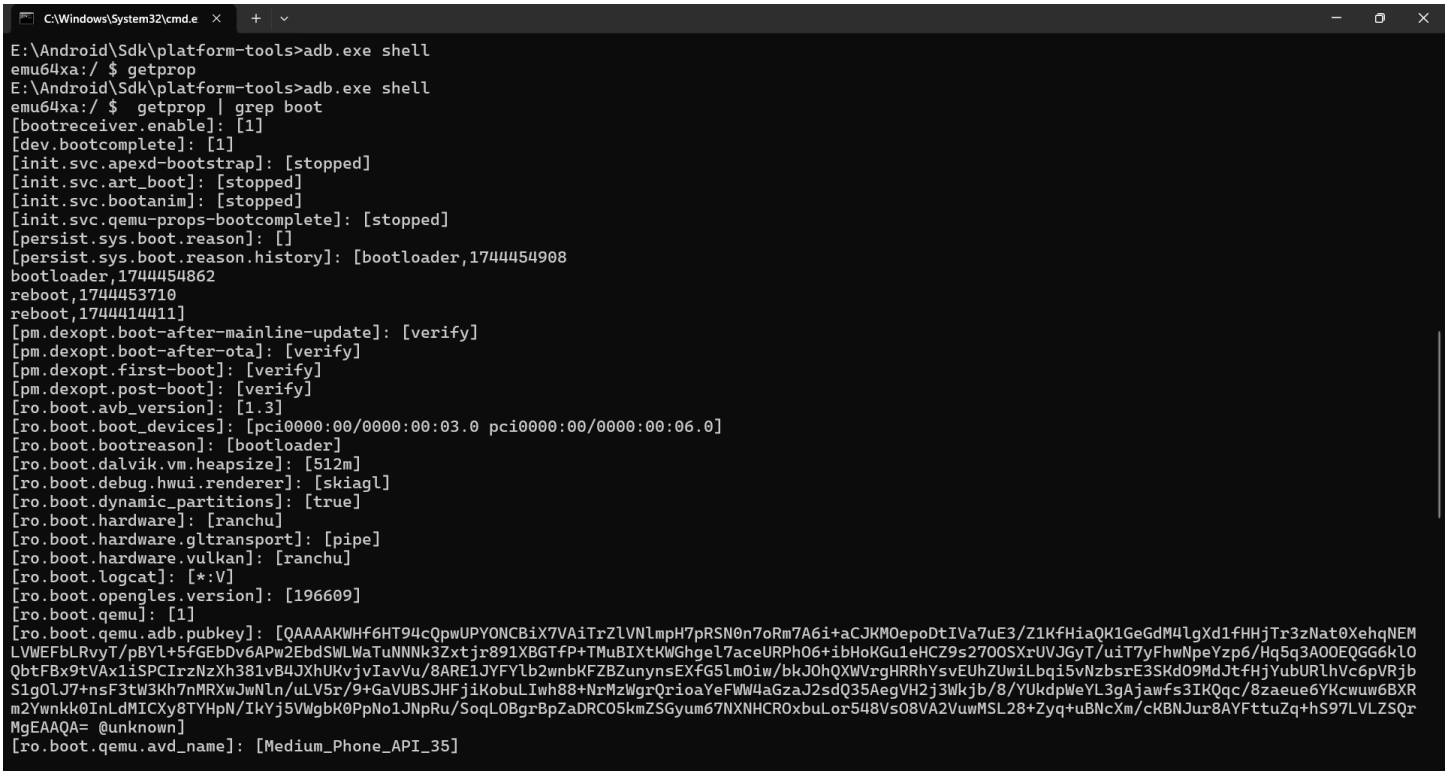




[10].Demonstration of ADB commands



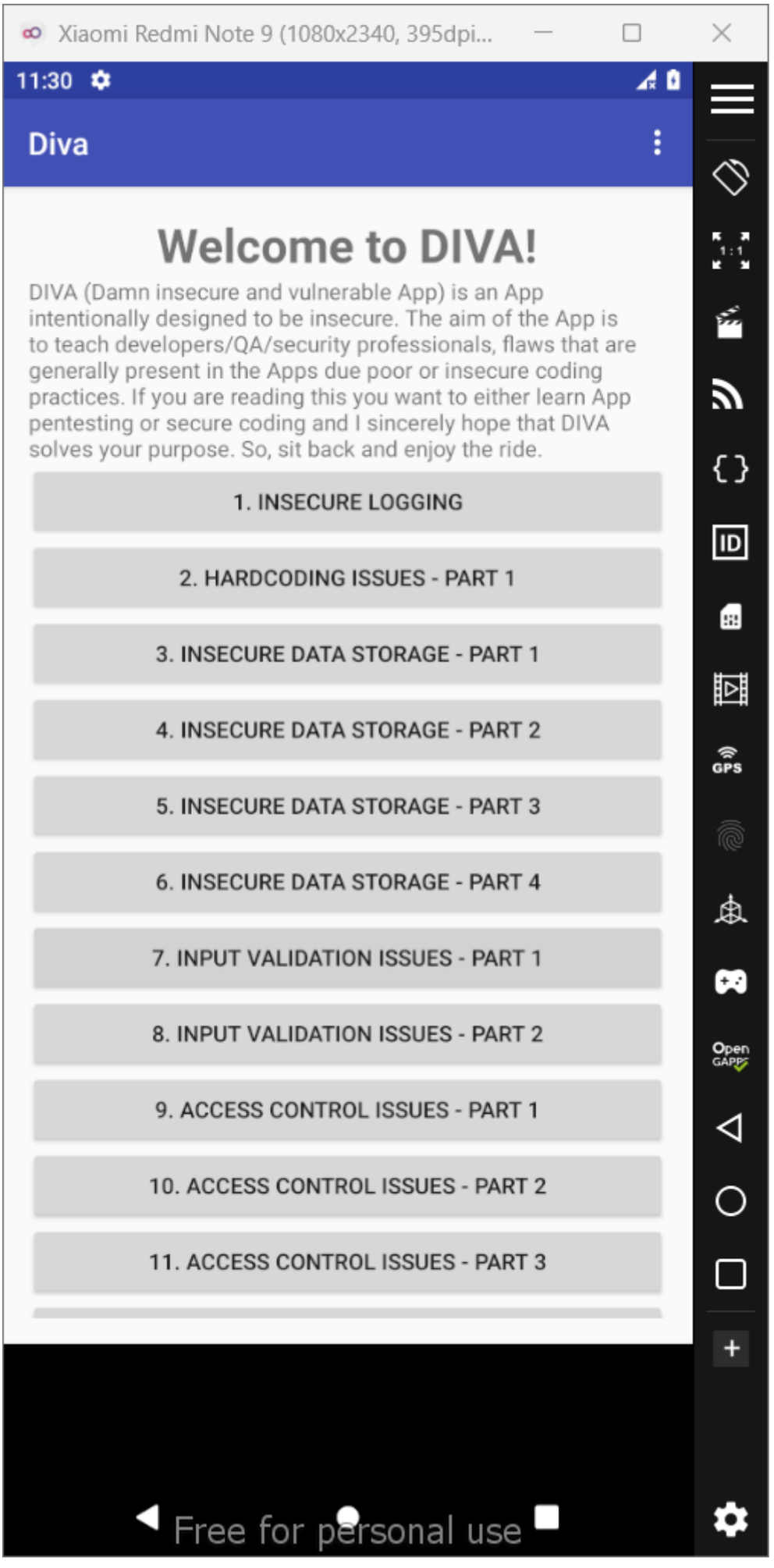
[11].Demonstration of Android Boot Process using ADB



```
C:\Windows\System32\cmd.e
E:\Android\Sdk\platform-tools>adb.exe shell
emu64xa:/ $ getprop
E:\Android\Sdk\platform-tools>adb.exe shell
emu64xa:/ $  getprop | grep boot
[bootreceiver.enable]: [1]
[dev.bootcomplete]: [1]
[init.svc.apexd-bootstrap]: [stopped]
[init.svc.art_boot]: [stopped]
[init.svc.bootanim]: [stopped]
[init.svc.qemu-props-bootcomplete]: [stopped]
[persist.sys.boot.reason]: []
[persist.sys.boot.reason.history]: [bootloader,1744454908
bootloader,1744454862
reboot,1744453710
reboot,1744414411]
[pm.dexopt.boot-after-mainline-update]: [verify]
[pm.dexopt.boot-after-ota]: [verify]
[pm.dexopt.first-boot]: [verify]
[pm.dexopt.post-boot]: [verify]
[ro.boot.avb_version]: [1.3]
[ro.boot.boot_devices]: [pci0000:00/0000:00:03.0 pci0000:00/0000:00:06.0]
[ro.boot.bootreason]: [bootloader]
[ro.boot.dalvik.vm.heapsize]: [512m]
[ro.boot.debug.hwui.renderer]: [skiagl]
[ro.boot.dynamic_partitions]: [true]
[ro.boot.hardware]: [ranchu]
[ro.boot.hardware.gltransport]: [pipe]
[ro.boot.hardware.vulkan]: [ranchu]
[ro.boot.logcat]: [*:V]
[ro.boot.opengles.version]: [196609]
[ro.boot.qemu]: [1]
[ro.boot.qemu.adb.pubkey]: [QAAAAKWHf6HT94cQpwUPYONCBiX7VAiTrZlVNlmpH7pRSN0n7oRm7A6i+aCJKMOepoDtIVa7uE3/Z1KfHiaQK1GeGdM4lgXd1fHHjTr3zNat0XehqNEM
LVWEFbLRvyT/pBYl+5fGEbDv6APw2EbdSWLWaTuNNNk3Zxtjr891XBGTfP+TMuBIXtKWGhgel7aceURPhO6+ibHoKGu1eHCZ9s27OOSXrUVJGyT/uiT7yFhwNpeYzp6/Hq5q3AOOEQGG6klO
QbtFBx9tVAx1iSPCIrzNzXh381vB4JXhUKvjvIavVu/8ARE1JYFYlb2wnbKFZBZunynsEXfG5lmOiw/bkJOhQXWVrgHRRhYsvEUhZUwiLbqi5vNzbsrE3SKdO9MdJtfHjYubURlhVc6pVRjb
S1gOlJ7+nsF3tW3Kh7nMRXwJwNln/uLV5r/9+GaVUBSJHFjiKobuLIwh88+NrMzWgrQrioaYeFWW4aGzaJ2sdQ35AegVH2j3Wkjb/8/YUkdpWeYL3gAjawfs3IKQqc/8zaeue6YKcwuw6BXR
m2Ywnkk0InLdMICXy8TYHpN/IkYj5VWgbK0PpNo1JNpRu/SoqLOBgrBpZaDRCO5kmZSGyum67NXNHCROxbuLor548VsO8VA2VuwMSL28+Zyq+uBNcXm/cKBNJur8AYFttuZq+hS97LVLZSQr
MgEAAQA= @unknown]
[ro.boot.qemu.avd_name]: [Medium_Phone_API_35]
```

```
C:\Windows\System32\cmd.e
qLOBgrBpZaDRCO5kmZSGyum67NXNHCROxbuLor548VsO8VA2VuwMSL28+Zyq+uBNcXm/cKBNJur8AYFttuZq+hS97LVLZSQrMgEAAQA= @unknown]
[ro.boot.qemu.avd_name]: [Medium_Phone_API_35]
[ro.boot.qemu.camera_hq_edge_processing]: [0]
[ro.boot.qemu.camera_protocol_ver]: [1]
[ro.boot.qemu.cpuvulkan.version]: [4202496]
[ro.boot.qemu.gltransport.drawFlushInterval]: [800]
[ro.boot.qemu.gltransport.name]: [pipe]
[ro.boot.qemu.hwcodec.avcdec]: [2]
[ro.boot.qemu.hwcodec.hevcdec]: [2]
[ro.boot.qemu.hwcodec.vpxdec]: [2]
[ro.boot.qemu.settings.system.screen_off_timeout]: [2147483647]
[ro.boot.qemu.virtiowifi]: [1]
[ro.boot.qemu.vsync]: [60]
[ro.boot.serialno]: [EMULATOR35X3X11X0]
[ro.boot.vbmeta.digest]: [9b597927025d4f62f4594a14632a8d3763239f29c0b7af229e0b6ebcddcdea60]
[ro.boot.vbmeta.hash_alg]: [sha256]
[ro.boot.vbmeta.size]: [6720]
[ro.boot.veritymode]: [enforcing]
[ro.bootimage.build.date]: [Fri Nov  1 16:39:47 UTC 2024]
[ro.bootimage.build.date.utc]: [1730479187]
[ro.bootimage.build.fingerprint]: [google/sdk_gphone64_x86_64/emu64xa:15/AE3A.240806.036/12592187:user/dev-keys]
[ro.bootimage.build.id]: [AE3A.240806.036]
[ro.bootimage.build.tags]: [dev-keys]
[ro.bootimage.build.type]: [user]
[ro.bootimage.build.version.incremental]: [12592187]
[ro.bootimage.build.version.release]: [15]
[ro.bootimage.build.version.release_or_codename]: [15]
[ro.bootimage.build.version.sdk]: [35]
[ro.bootloader]: [unknown]
[ro.bootmode]: [unknown]
[ro.product.bootimage.brand]: [google]
[ro.product.bootimage.device]: [emu64xa]
[ro.product.bootimage.manufacturer]: [Google]
[ro.product.bootimage.model]: [sdk_gphone64_x86_64]
[ro.product.bootimage.name]: [sdk_gphone64_x86_64]
[sys.boot.reason]: [bootloader]
[sys.boot.reason.last]: [bootloader]
[sys.boot_completed]: [1]
[sys.bootstat.first_boot_completed]: [1]
emu64xa:/ $
E:\Android\Sdk\platform-tools>
```

[12].Configuration of DIVA



[13].Reverse Engineering using APKTools

Santoku (Santoku) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

santoku@santoku-VirtualBox: ~

File Edit Tabs Help

```
santoku@santoku-VirtualBox:~$ apktool --version
2.11.1
santoku@santoku-VirtualBox:~$ apktool
Apktool 2.11.1 - a tool for reengineering Android apk files
with smali 3.0.9 and baksmali 3.0.9
Copyright 2010 Ryszard Wiśniewski <brut.alll@gmail.com>
Copyright 2010 Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
 -advance,--advanced   Print advanced information.
 -version,--version    Print the version.
usage: apktool if|install-framework [options] <framework.apk>
 -p,--frame-path <dir>   Store framework files into <dir>.
 -t,--tag <tag>          Tag frameworks using <tag>.
usage: apktool d[ecode] [options] <file_apk>
 -f,--force              Force delete destination directory.
 -o,--output <dir>       The name of folder that gets written. (default: apk.out)
 -p,--frame-path <dir>   Use framework files located in <dir>.
 -r,--no-res             Do not decode resources.
 -s,--no-src             Do not decode sources.
 -t,--frame-tag <tag>    Use framework files tagged by <tag>.
usage: apktool b[uild] [options] <app_path>
 -f,--force-all          Skip changes detection and build all files.
 -o,--output <file>      The name of apk that gets written. (default: dist/name.apk)
 -p,--frame-path <dir>   Use framework files located in <dir>.

For additional info, see: https://apktool.org
For smali/baksmali info, see: https://github.com/google/smali
santoku@santoku-VirtualBox:~$
```

Santoku (Santoku) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

santoku@santoku-VirtualBox: ~/diva_decompiled/smali/jakhar/aseem/diva

File Edit Tabs Help

```
santoku@santoku-VirtualBox:~$ apktool d diva-beta.apk -o diva_decompiled
I: Using Apktool 2.11.1 on diva-beta.apk with 4 threads
I: Baksmaling classes.dex...
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: /home/santoku/.local/share/apktool/framework/1.apk
I: Decoding values */* XMLs...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Copying original files...
I: Copying lib...
I: Copying unknown files...
santoku@santoku-VirtualBox:~$ cd diva_decompiled
santoku@santoku-VirtualBox:~/diva_decompiled$ ls
AndroidManifest.xml  apktool.yml  lib  original  res  smali
santoku@santoku-VirtualBox:~/diva_decompiled$ less AndroidManifest.xml
santoku@santoku-VirtualBox:~/diva_decompiled$ cd smali/jakhar/aseem/diva/
santoku@santoku-VirtualBox:~/diva_decompiled/smali/jakhar/aseem/diva$ less InsecureDataStorage1Activity.smali
santoku@santoku-VirtualBox:~/diva_decompiled/smali/jakhar/aseem/diva$
```

Santoku (Santoku) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

AndroidManifest.xml

File Edit Search Options Help

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="jakhar.aseem.diva" platformBuildVersionCode="23" platformBuildVersionName="6.0-2438415">
  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
  <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
  <uses-permission android:name="android.permission.INTERNET"/>
  <application android:allowBackup="true" android:debuggable="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:supportsRtl="true" android:theme="@style/AppTheme">
    <activity android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity" android:theme="@style/AppTheme.NoActionBar">
      <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
      </intent-filter>
    </activity>
    <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
    <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
    <activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
    <activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
    <activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
    <activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
    <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
    <activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity"/>
    <activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity"/>
    <activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APICredsActivity">
      <intent-filter>
        <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
        <category android:name="android.intent.category.DEFAULT"/>
      </intent-filter>
    </activity>
    <activity android:label="@string/d10" android:name="jakhar.aseem.diva.AccessControl2Activity"/>
    <activity android:label="@string/apic2_label" android:name="jakhar.aseem.diva.APICreds2Activity">
      <intent-filter>
        <action android:name="jakhar.aseem.diva.action.VIEW_CREDS2"/>
        <category android:name="android.intent.category.DEFAULT"/>
      </intent-filter>
    </activity>
    <provider android:authorities="jakhar.aseem.diva.provider.notesprovider" android:enabled="true" android:exported="true" android:name="jakhar.aseem.diva.NotesProvider"/>
    <activity android:label="@string/d11" android:name="jakhar.aseem.diva.AccessControl3Activity"/>
    <activity android:label="@string/d12" android:name="jakhar.aseem.diva.Hardcode2Activity"/>
    <activity android:label="@string/pnotes" android:name="jakhar.aseem.diva.AccessControl3NotesActivity"/>
    <activity android:label="@string/d13" android:name="jakhar.aseem.diva.InputValidation3Activity"/>
  </application>
</manifest>
```

Santoku (Santoku) [Running] - Oracle VirtualBox

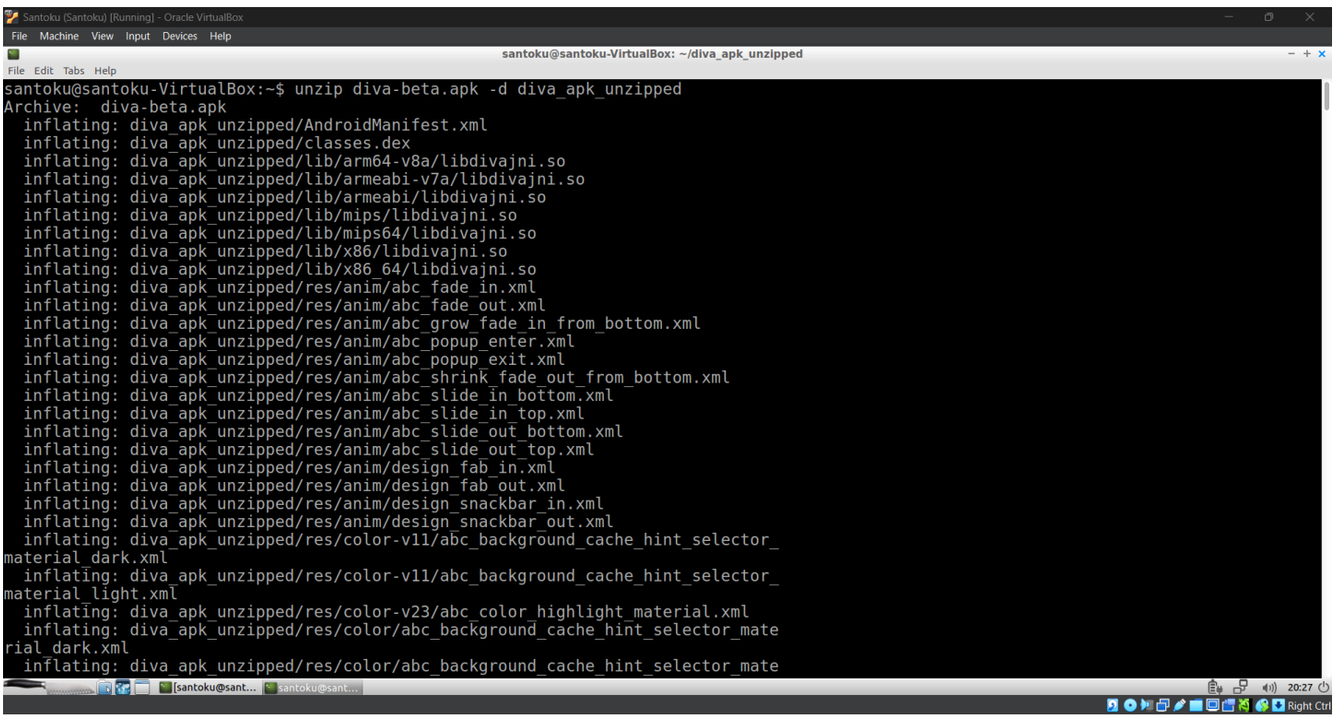
File Machine View Input Devices Help

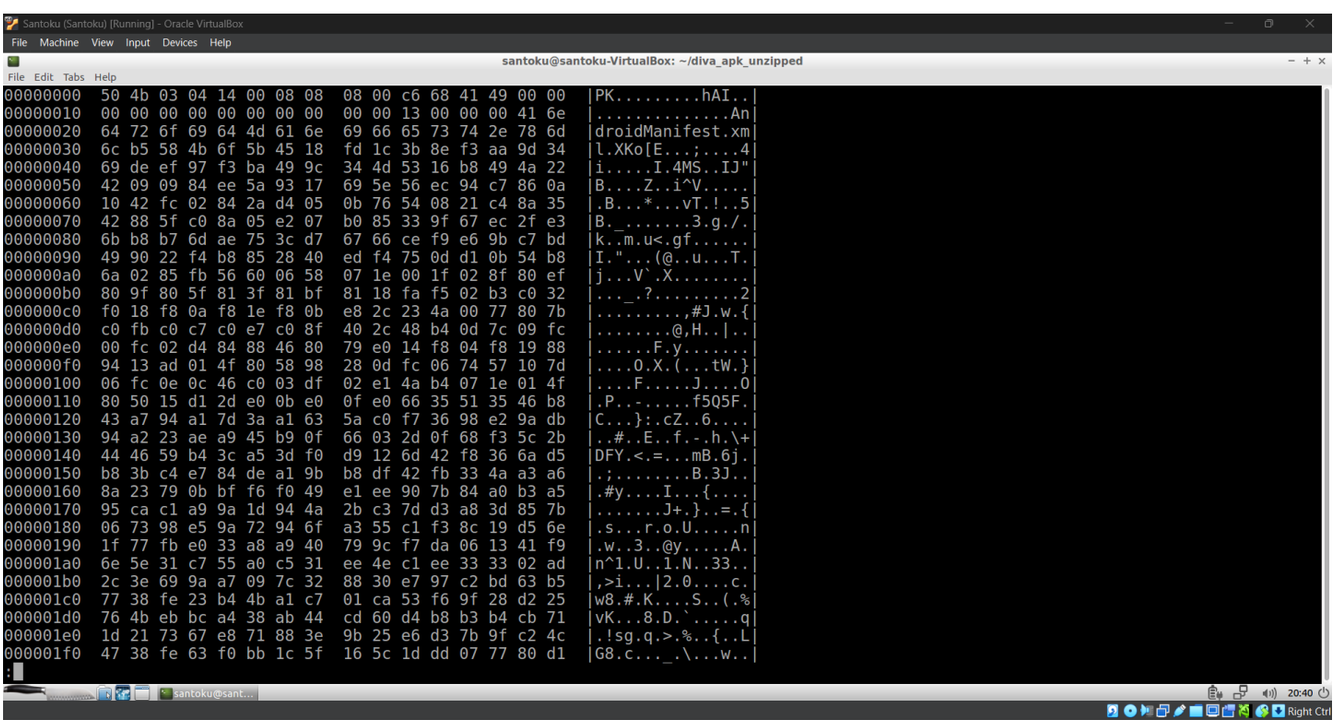
MainActivity.smali

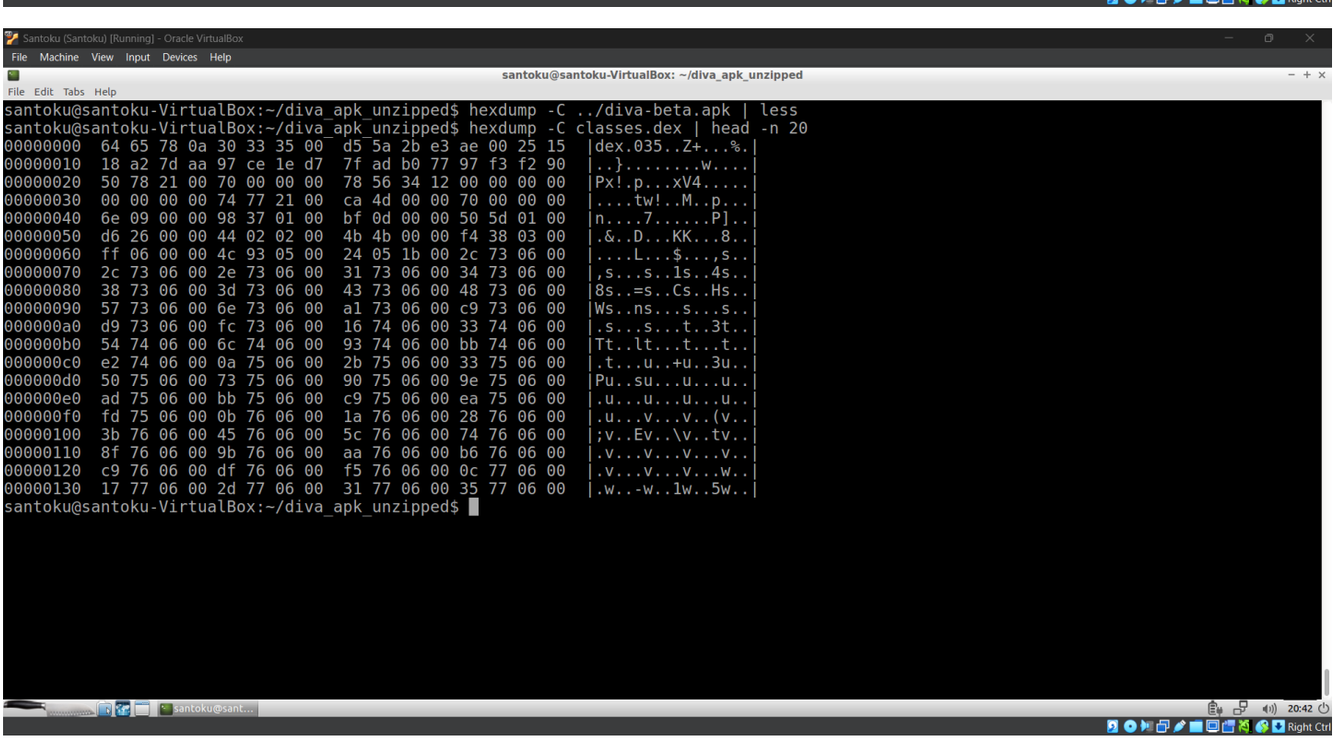
File Edit Search Options Help

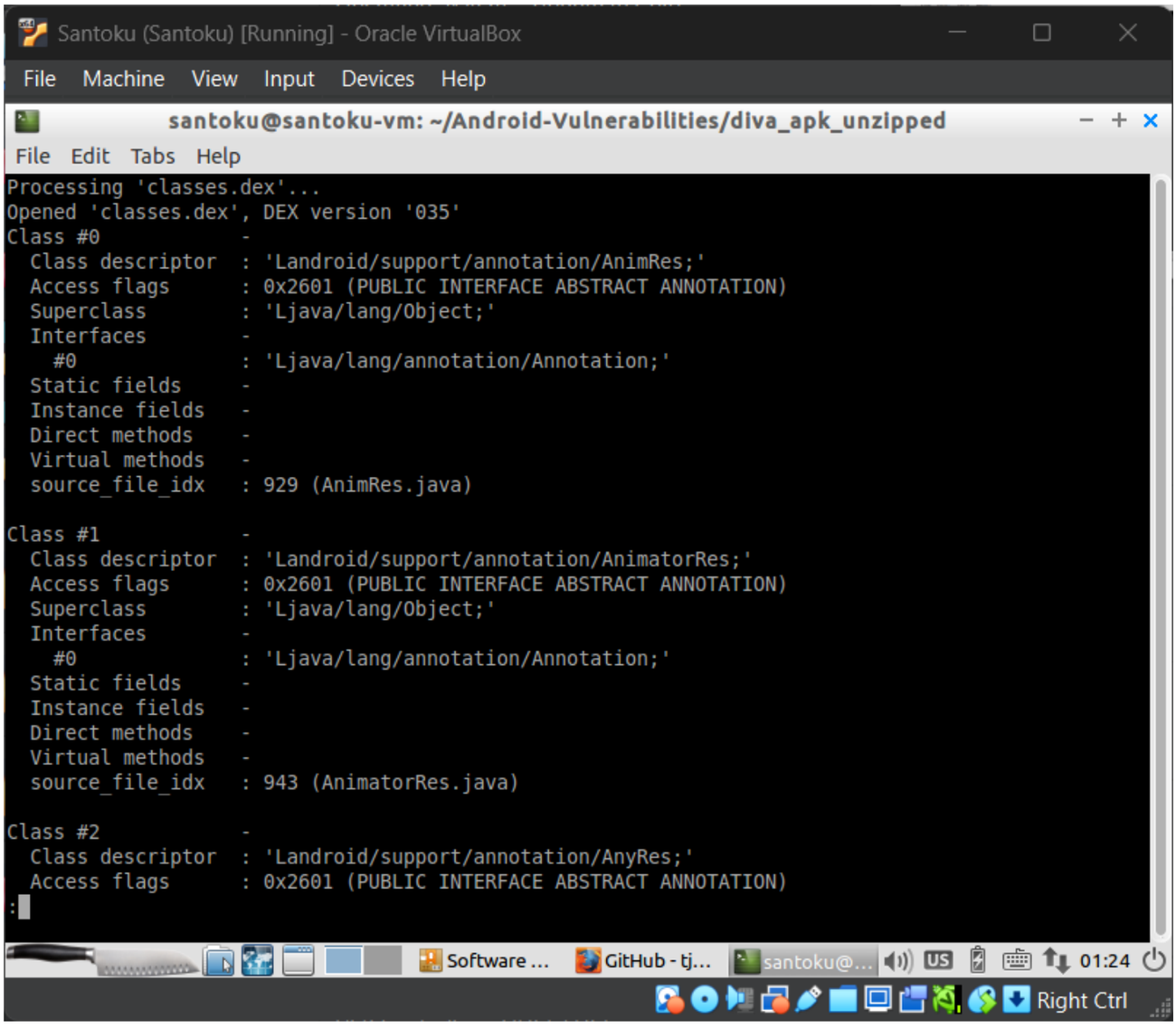
```
.class public Ljakhar/aseem/diva/MainActivity;
.super Landroid/support/v7/app/AppCompatActivity;
.source "MainActivity.java"


# direct methods
.method public constructor <init>()V
  .locals 0

  .prologue
  .line 13
  invoke-direct {p0}, Landroid/support/v7/app/AppCompatActivity;-><init>()V

  return-void
.end method


# virtual methods
.method protected onCreate(Landroid/os/Bundle;)V
  .locals 2
  .param p1, "savedInstanceState"    # Landroid/os/Bundle;

  .prologue
  .line 17
  invoke-super {p0, p1}, Landroid/support/v7/app/AppCompatActivity;->onCreate(Landroid/os/Bundle;)V

  .line 18
  const v1, 0x7f040028

  invoke-virtual {p0, v1}, Ljakhar/aseem/diva/MainActivity;->setContentView(I)V

  .line 19
  const v1, 0x7f0c0097

  invoke-virtual {p0, v1}, Ljakhar/aseem/diva/MainActivity;->findViewById(I)Landroid/view/View;

  move-result-object v0

  check-cast v0, Landroid/support/v7/widget/Toolbar;

  .line 20
  .local v0, "toolbar":Landroid/support/v7/widget/Toolbar;
  invoke-virtual {p0, v0}, Ljakhar/aseem/diva/MainActivity;->setSupportActionBar(Landroid/support/v7/widget/Toolbar;)V

  .line 22
```

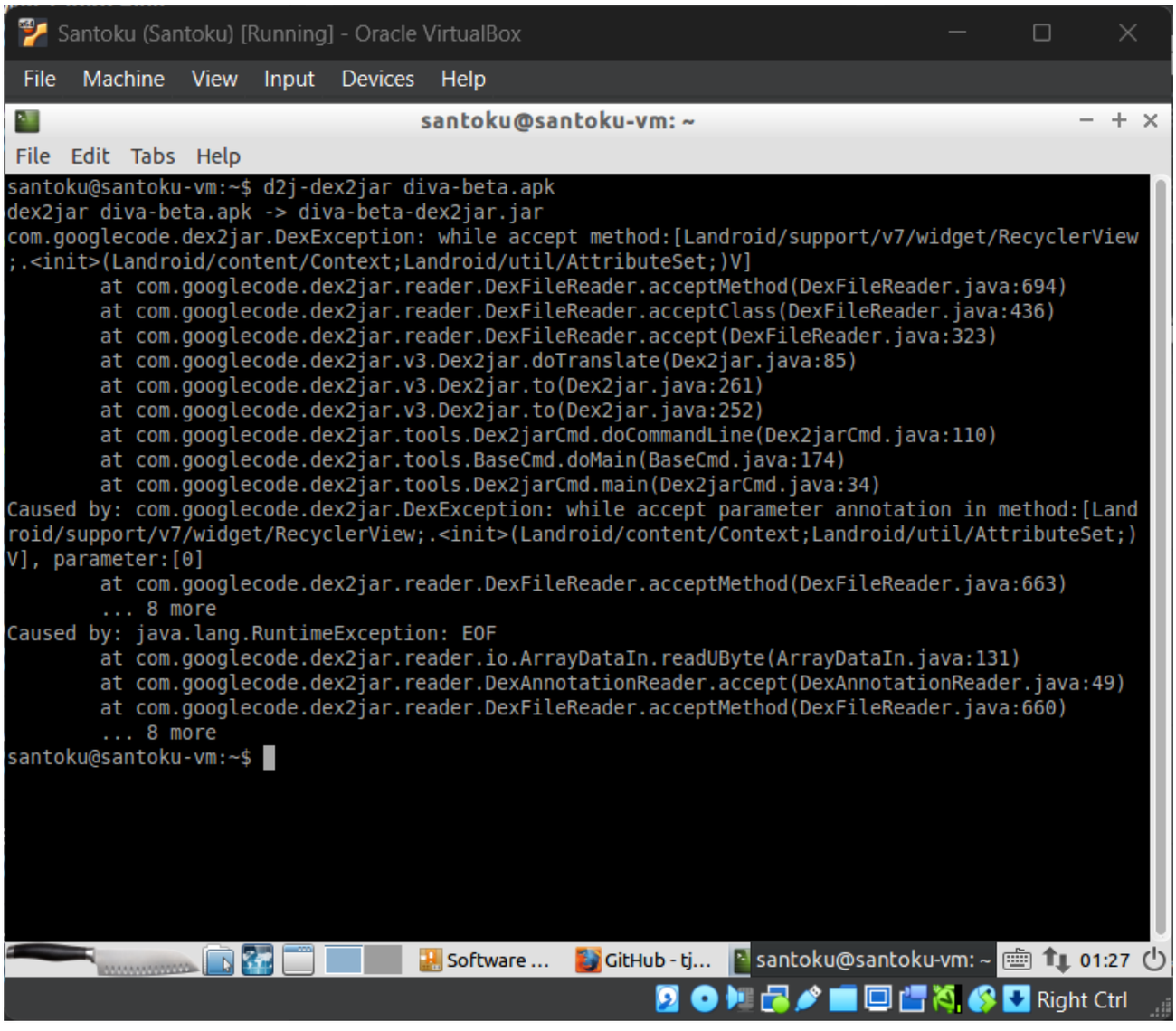
[14].Reverse Engineering using Haxdump Dex Dump and d2j



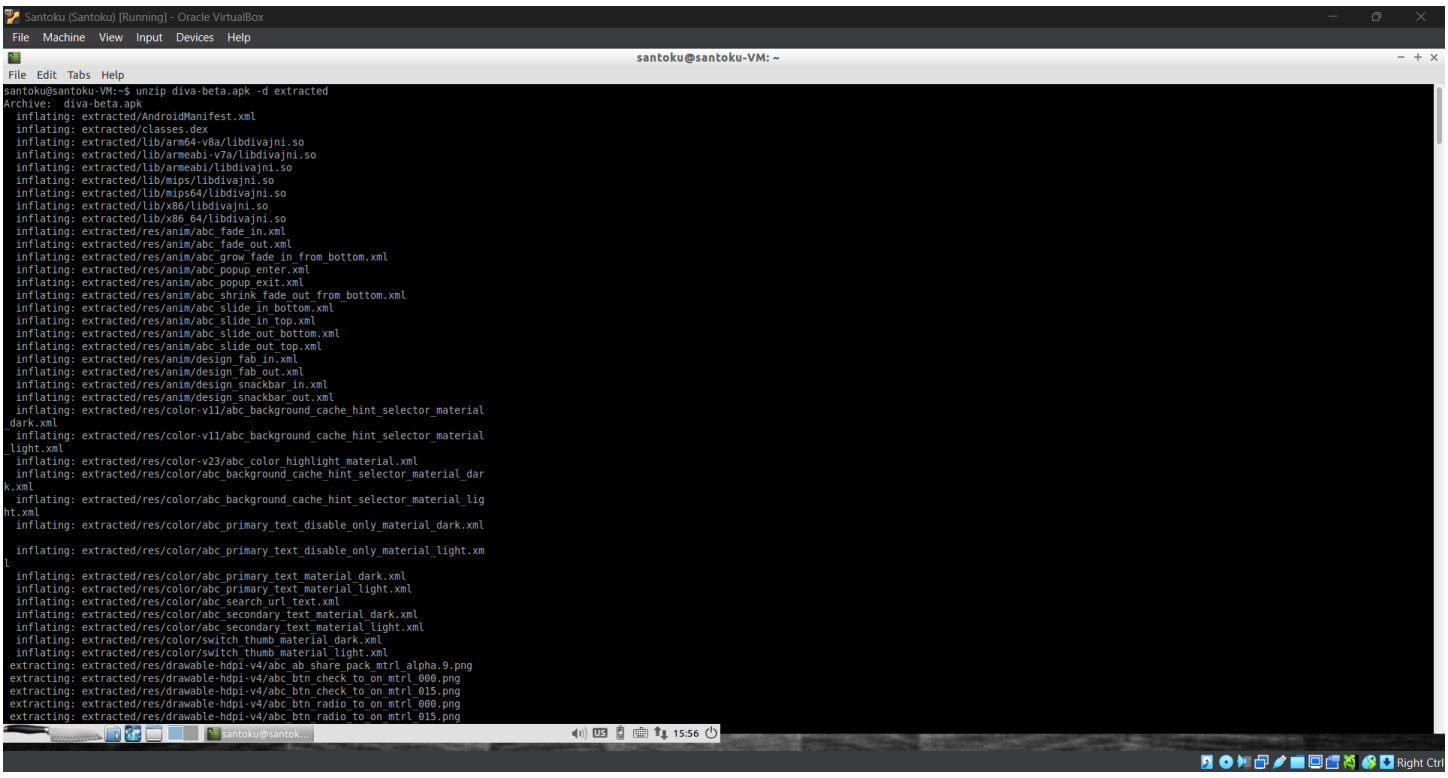


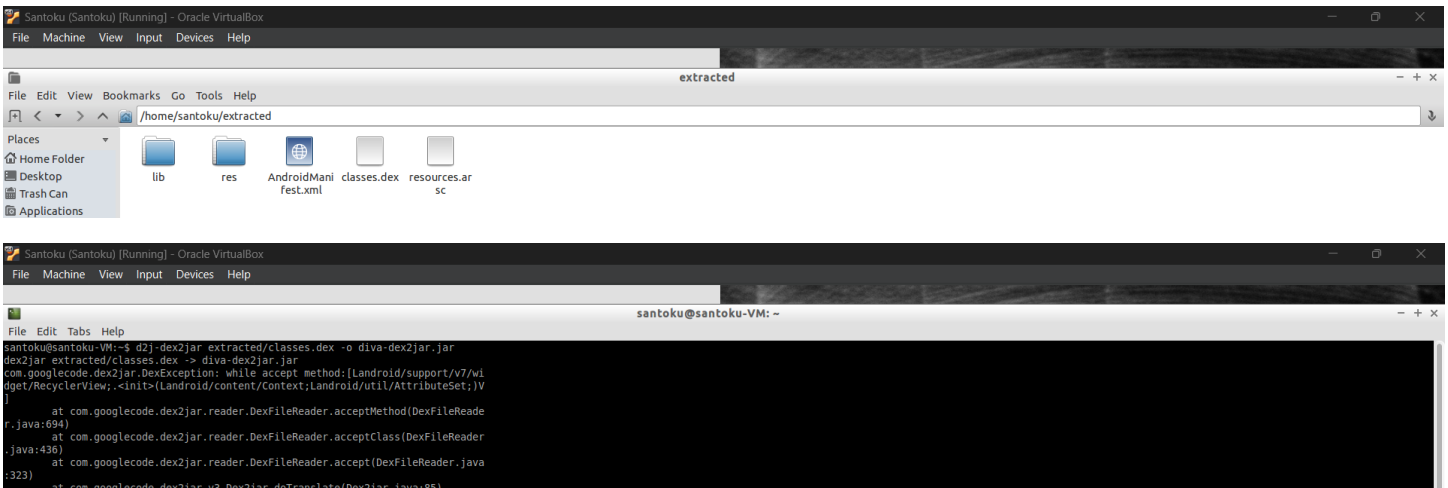


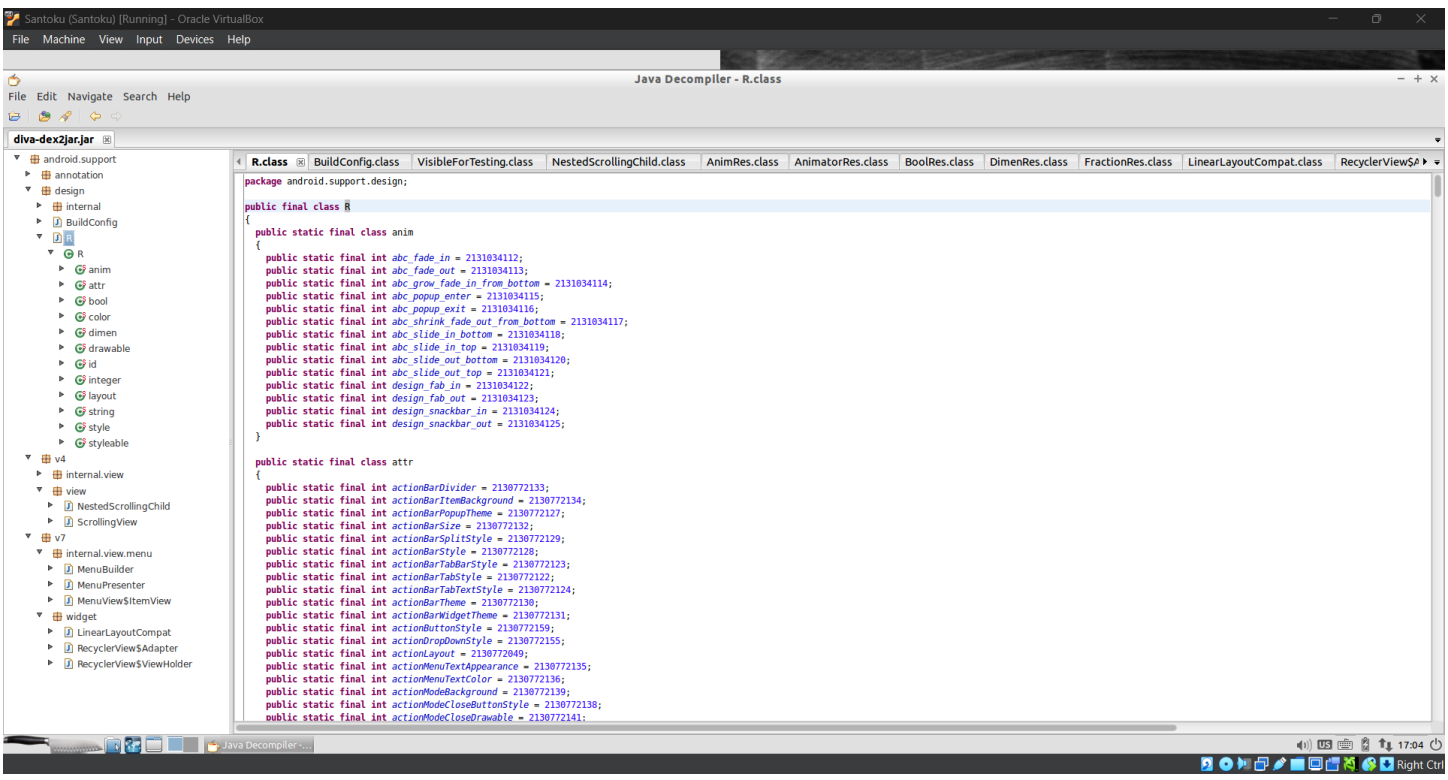

Santoku (Santoku) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
santoku@santoku-vm: ~/Android-Vulnerabilities/diva_apk_unzipped
File Edit Tabs Help
Processing 'classes.dex'...
Opened 'classes.dex', DEX version '035'
Class #0 -
Class descriptor : 'Landroid/support/annotation/AnimRes;'
Access flags : 0x2601 (PUBLIC INTERFACE ABSTRACT ANNOTATION)
Superclass : 'Ljava/lang/Object;'
Interfaces -
#0 : 'Ljava/lang/annotation/Annotation;'
Static fields -
Instance fields -
Direct methods -
Virtual methods -
source_file_idx : 929 (AnimRes.java)
Class #1 -
Class descriptor : 'Landroid/support/annotation/AnimatorRes;'
Access flags : 0x2601 (PUBLIC INTERFACE ABSTRACT ANNOTATION)
Superclass : 'Ljava/lang/Object;'
Interfaces -
#0 : 'Ljava/lang/annotation/Annotation;'
Static fields -
Instance fields -
Direct methods -
Virtual methods -
source_file_idx : 943 (AnimatorRes.java)
Class #2 -
Class descriptor : 'Landroid/support/annotation/AnyRes;'
Access flags : 0x2601 (PUBLIC INTERFACE ABSTRACT ANNOTATION)
:
Software ...
GitHub - tj...
santoku@...
US
01:24
Right Ctrl


Santoku (Santoku) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
santoku@santoku-vm: ~
File Edit Tabs Help
santoku@santoku-vm:~$ d2j-dex2jar diva-beta.apk
dex2jar diva-beta.apk -> diva-beta-dex2jar.jar
com.googlecode.dex2jar.DexException: while accept method:[Landroid/support/v7/widget/RecyclerView;.<init>(Landroid/content/Context;Landroid/util/AttributeSet;)V]
at com.googlecode.dex2jar.reader.DexFileReader.acceptMethod(DexFileReader.java:694)
at com.googlecode.dex2jar.reader.DexFileReader.acceptClass(DexFileReader.java:436)
at com.googlecode.dex2jar.reader.DexFileReader.accept(DexFileReader.java:323)
at com.googlecode.dex2jar.v3.Dex2jar.doTranslate(Dex2jar.java:85)
at com.googlecode.dex2jar.v3.Dex2jar.to(Dex2jar.java:261)
at com.googlecode.dex2jar.v3.Dex2jar.to(Dex2jar.java:252)
at com.googlecode.dex2jar.tools.Dex2jarCmd.doCommandLine(Dex2jarCmd.java:110)
at com.googlecode.dex2jar.tools.BaseCmd.doMain(BaseCmd.java:174)
at com.googlecode.dex2jar.tools.Dex2jarCmd.main(Dex2jarCmd.java:34)
Caused by: com.googlecode.dex2jar.DexException: while accept parameter annotation in method:[Landroid/support/v7/widget/RecyclerView;.<init>(Landroid/content/Context;Landroid/util/AttributeSet;)V], parameter:[0]
at com.googlecode.dex2jar.reader.DexFileReader.acceptMethod(DexFileReader.java:663)
... 8 more
Caused by: java.lang.RuntimeException: EOF
at com.googlecode.dex2jar.reader.io.ArrayDataIn.readUByte(ArrayDataIn.java:131)
at com.googlecode.dex2jar.reader.DexAnnotationReader.accept(DexAnnotationReader.java:49)
at com.googlecode.dex2jar.reader.DexFileReader.acceptMethod(DexFileReader.java:660)
... 8 more
santoku@santoku-vm:~$
Software ...
GitHub - tj...
santoku@santoku-vm: ~
01:27
Right Ctrl

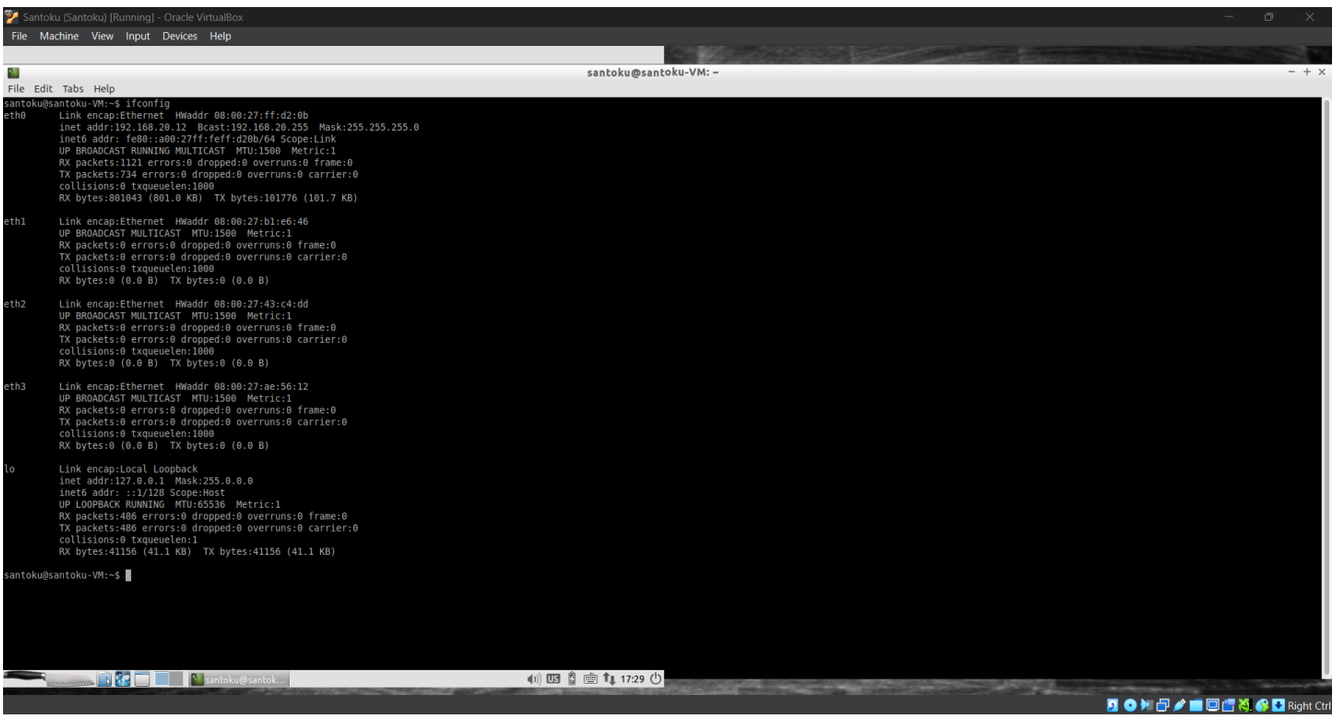
[15].Reverse Engineering using dex2jar and JDGUI

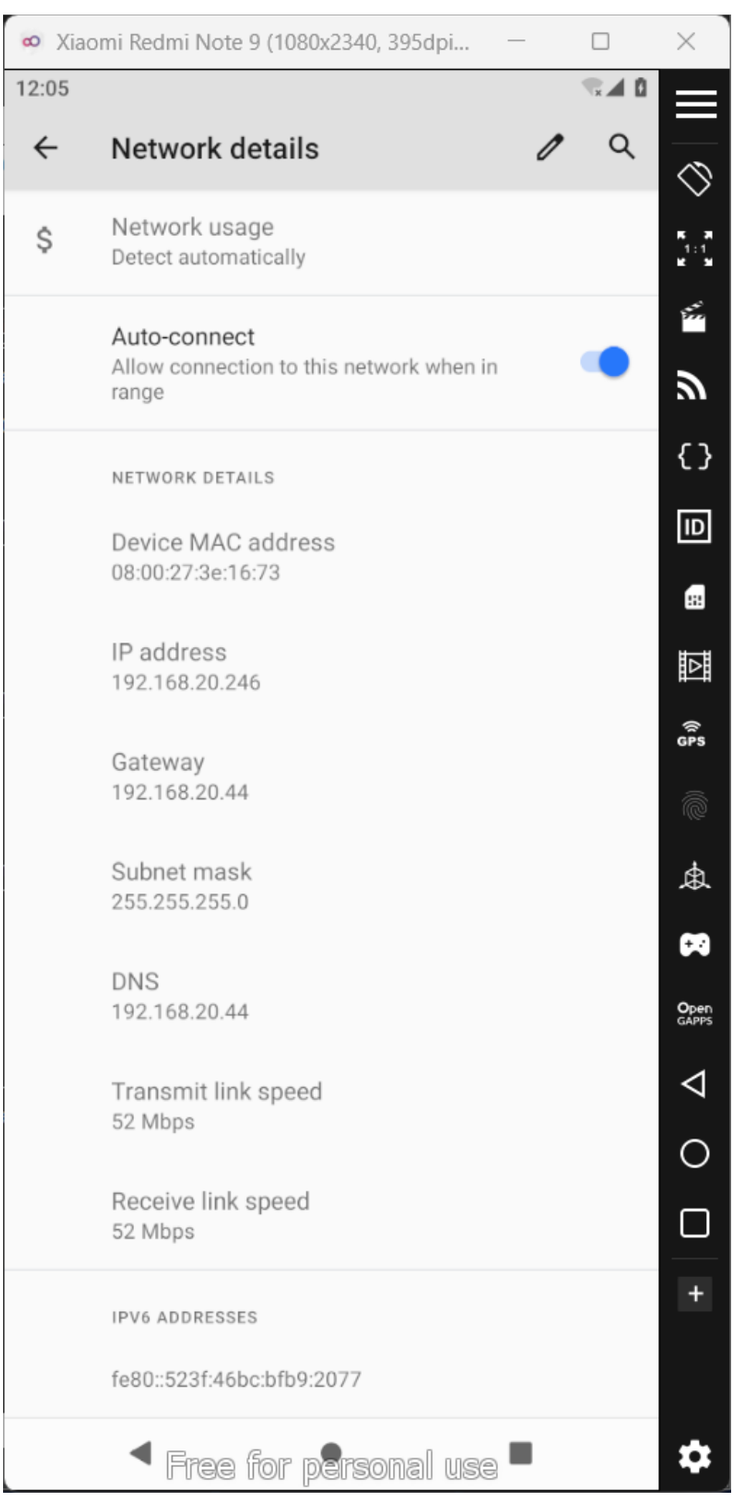






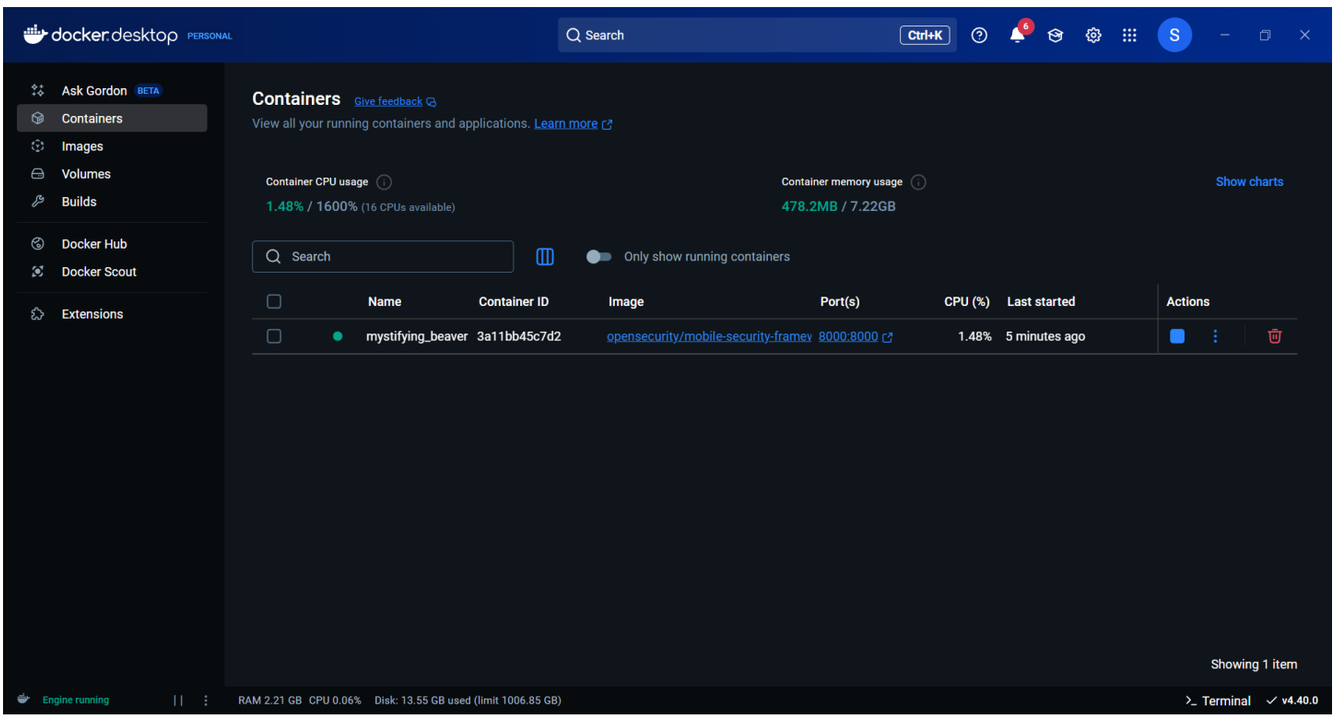
[16]. Request interception using BurpSuit

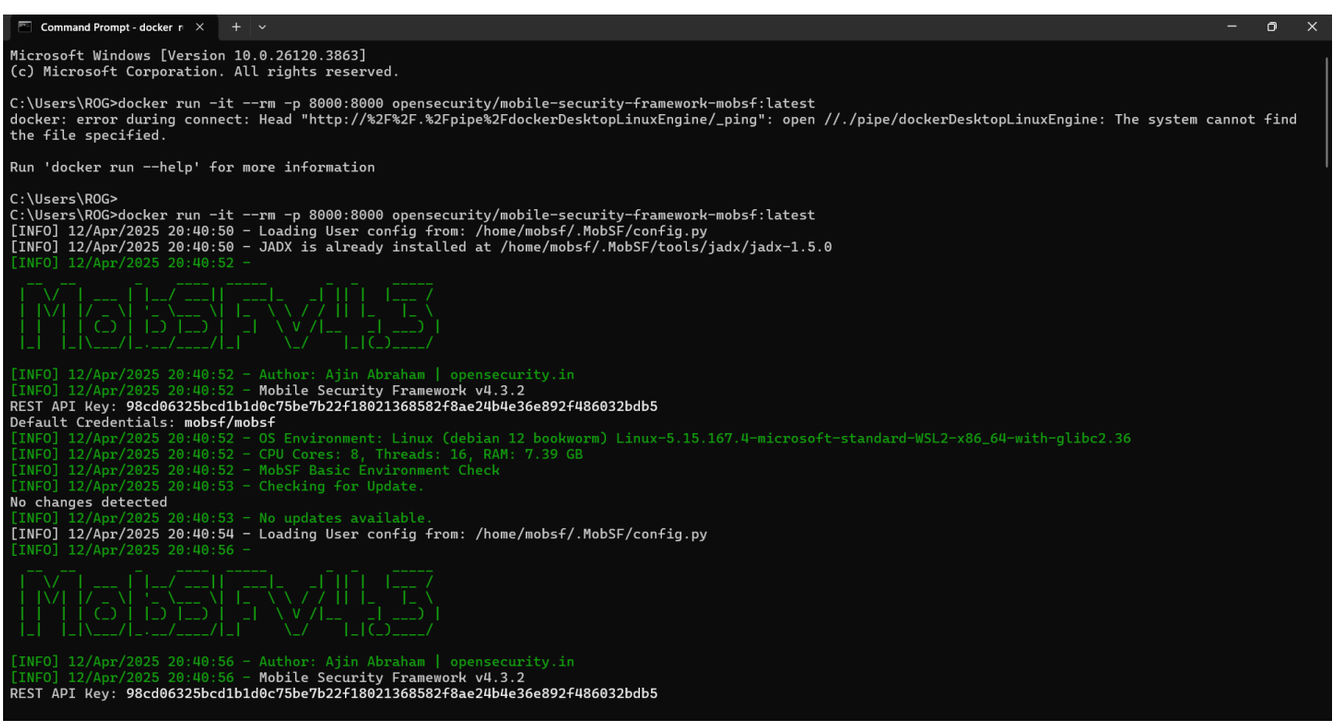


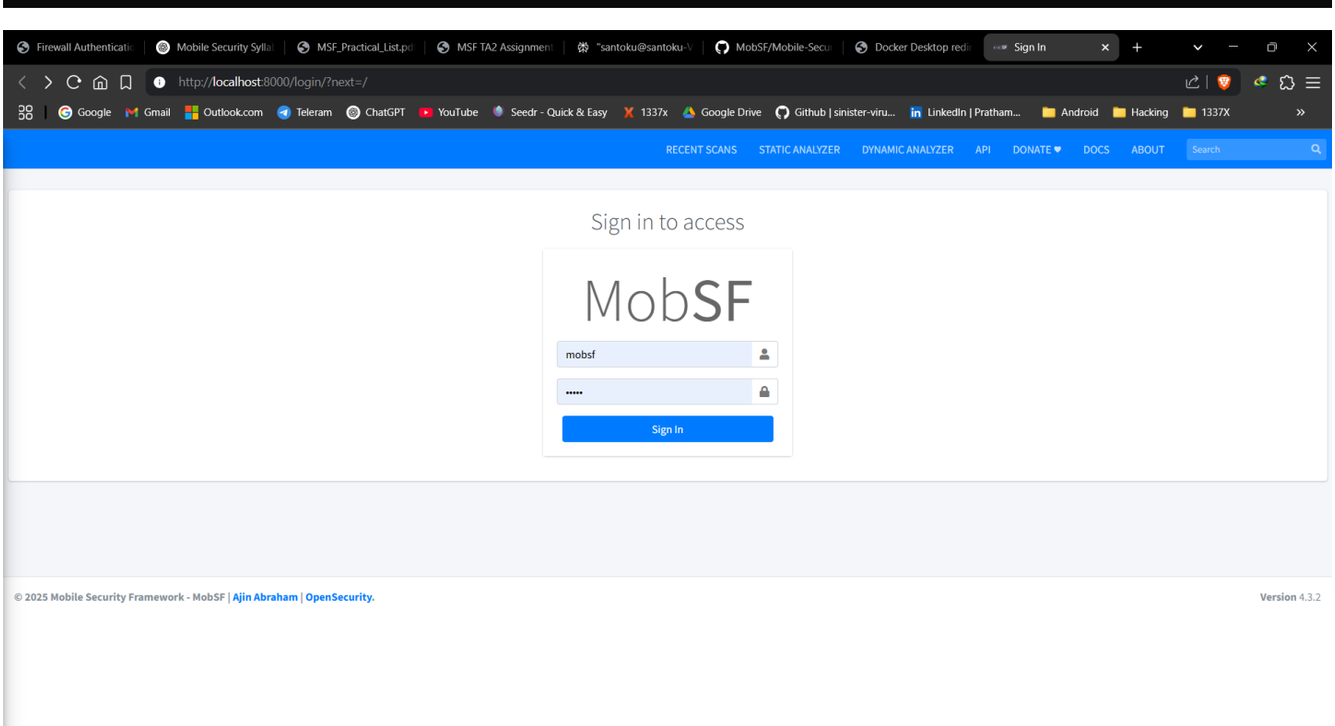


[17]. Configuration of Insecure Bank2
[18]. Configuration of OWASP GoatDroid
[19]. Configuration of Open GApps
[20]. Insecure Logging – Vulnerability
[21]. Hard Coding Issue – Vulnerability
[22]. Insecure Data Storage (Shared Preference) – Vulnerability
[23]. Insecure Data Storage (SD Card) – Vulnerability
[24]. Insecure Data Storage (Temp File) – Vulnerability
[25]. Insecure Data Storage (SQLight Database) – Vulnerability
[26]. Input Validation and Data Sanitization (SQL Injection) – Vulnerability
[27]. Input Validation and Data Sanitization (Web View) – Vulnerability
[28]. Access Control Issue – Vulnerability
[29]. Authentication Based Access Control – Vulnerability
[30]. Configuration of Drozer
[31]. Security Auditing of DIVA using Drozer
[32]. Security Auditing of Insecure Bank using Drozer
[33]. Security Auditing of OWASP GoatDroid using Drozer
[34]. Package listing of android app using app.package.list
[35]. Find Debuggable android application
[36]. Find attack surface of DIVA
[37]. SQL Injection Vulnerability of DIVA using Drozer Modules

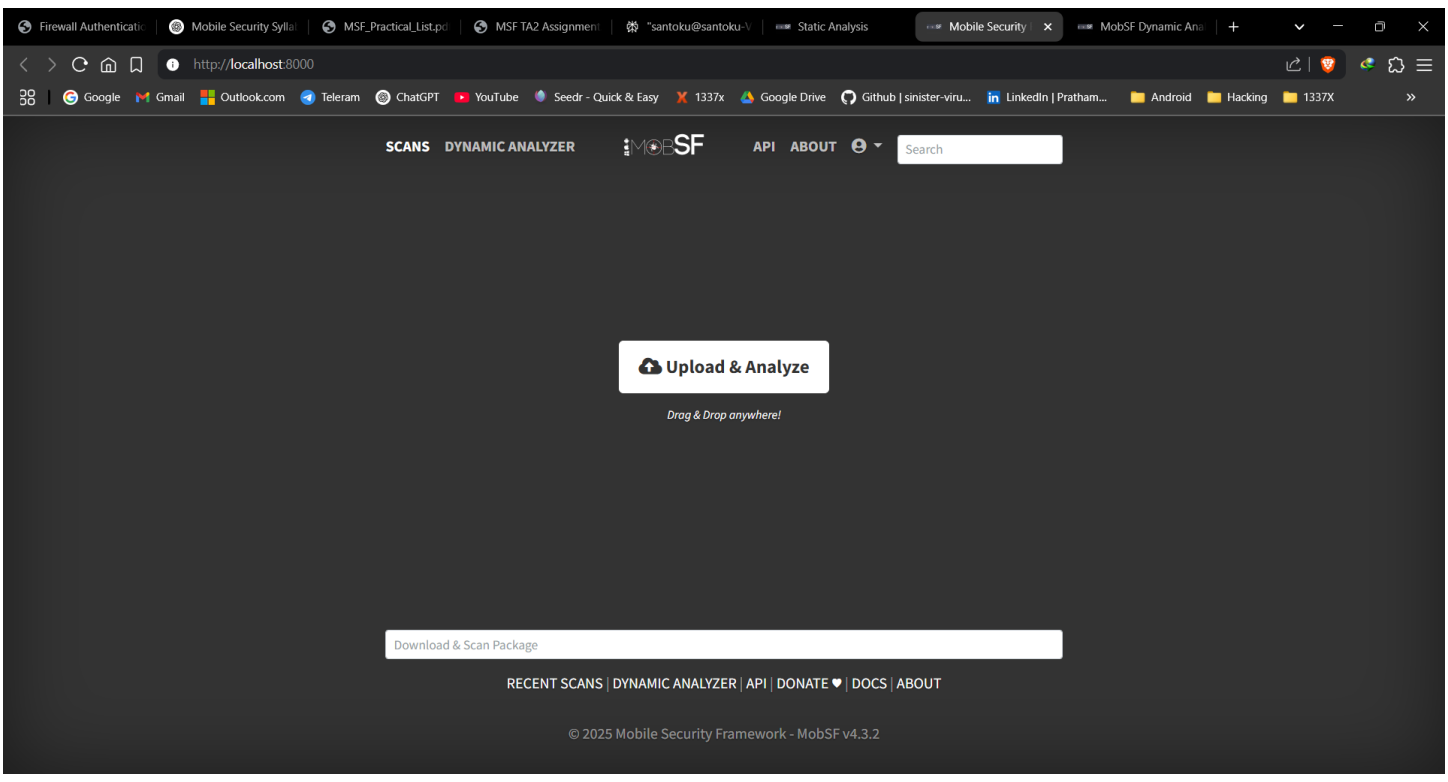
[38].Configuration of MobSF (Mobile Security Framework)

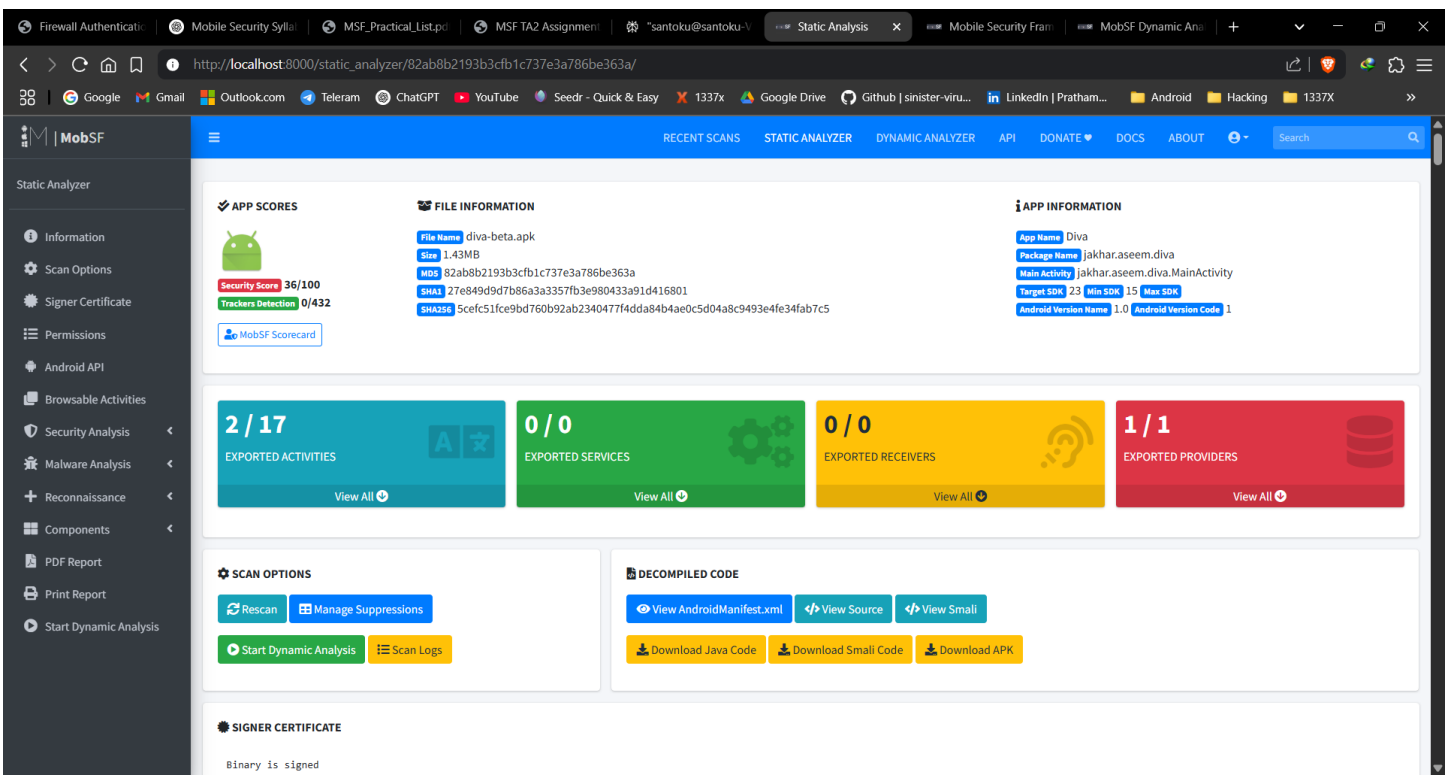


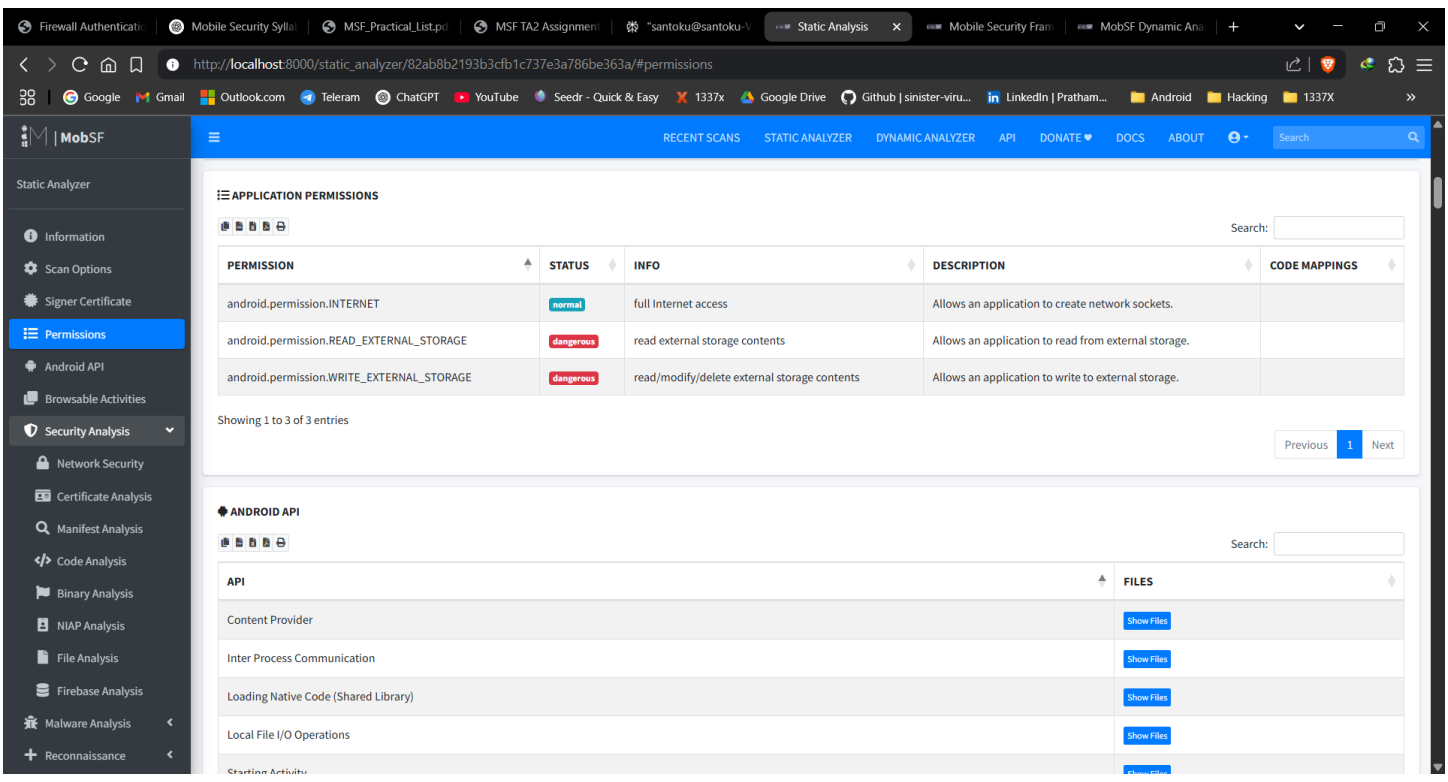


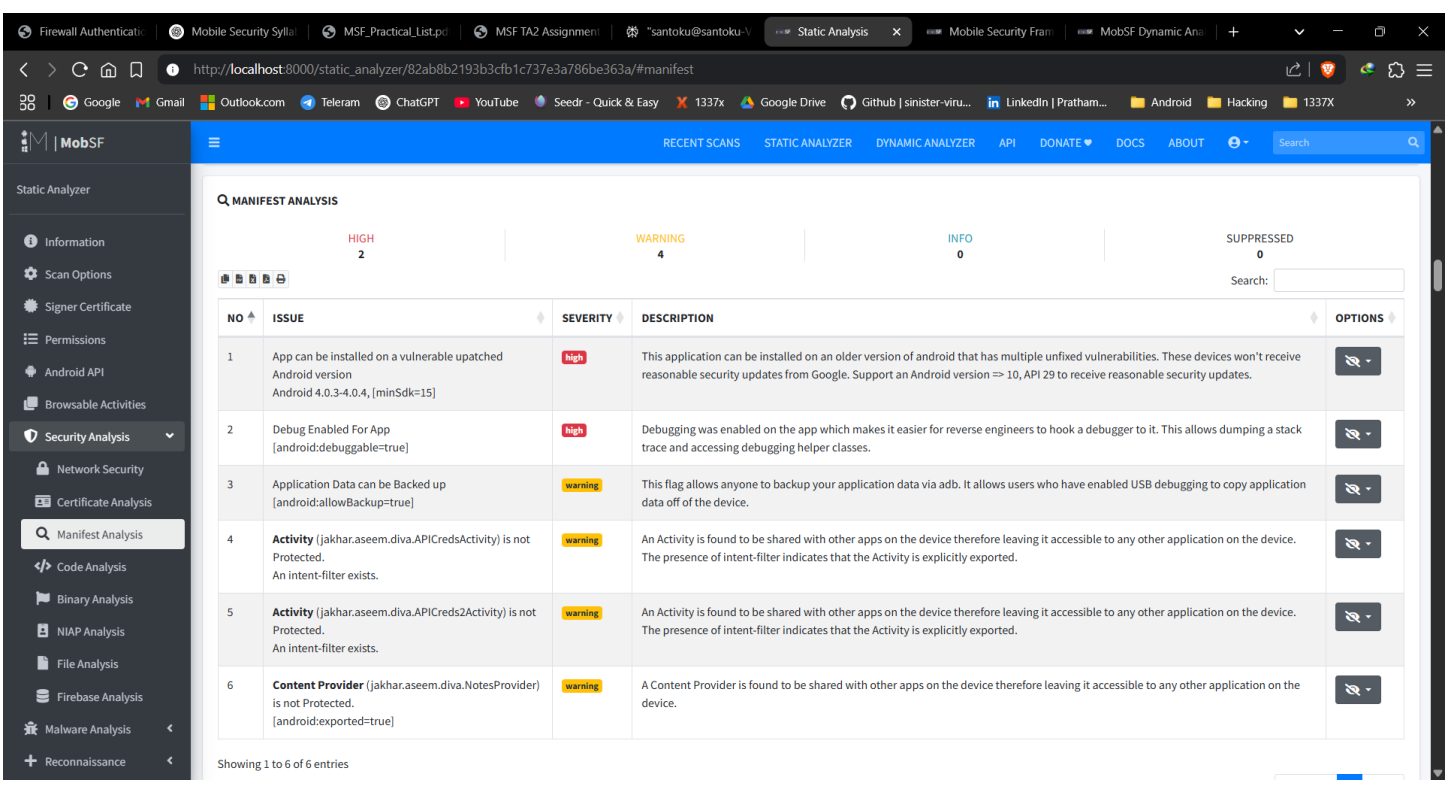


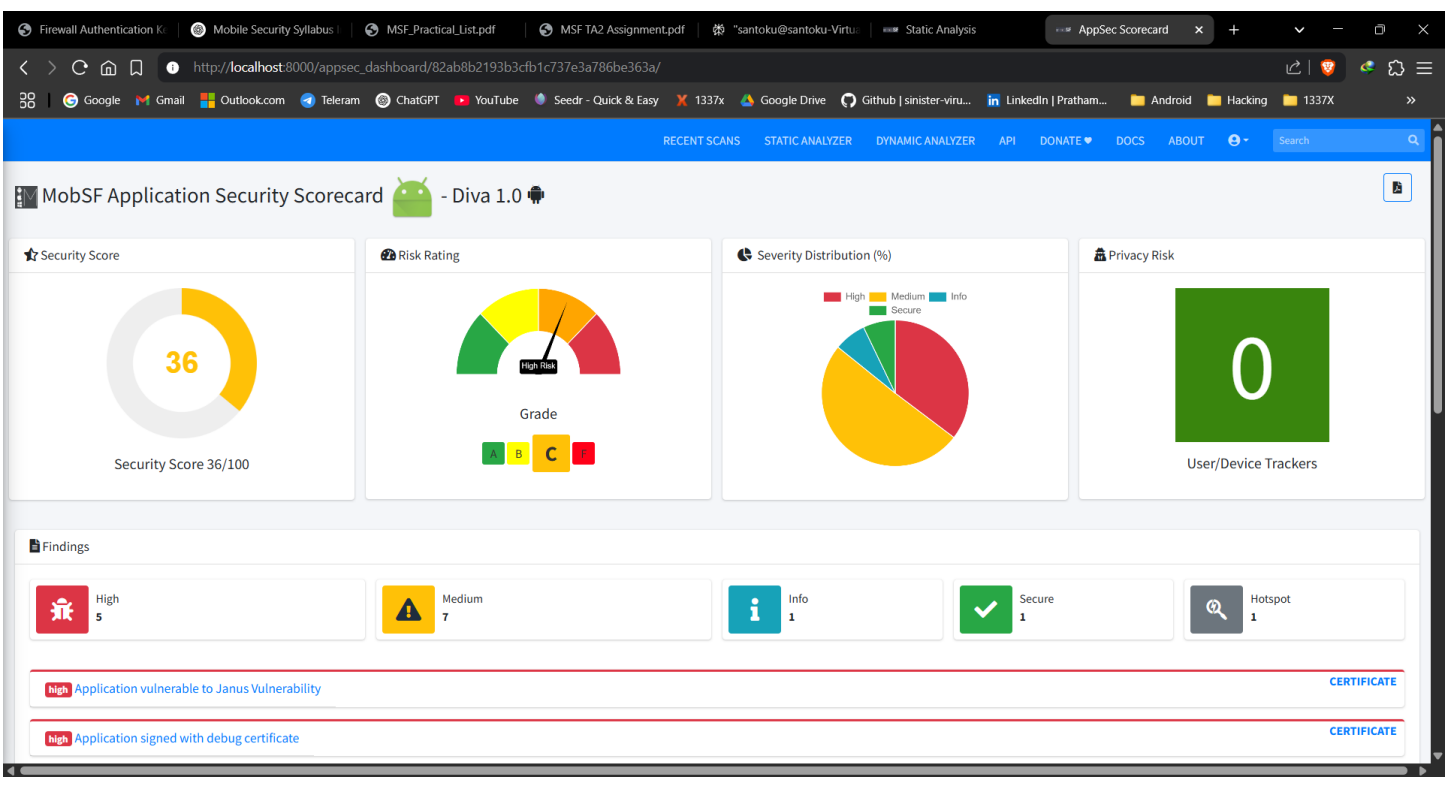
[39].Security Auditing using MobSF (Mobile Security Framework)











[40].Configuration of Frida

```
C:\Windows\System32\cmd.e

(frida+mobsf) E:\Santoku\frida\frida+mobsf>pip install frida-tools
Requirement already satisfied: frida-tools in e:\santoku\frida\frida+mobsf\lib\site-packages (13.7.1)
Requirement already satisfied: colorama<1.0.0,>=0.2.7 in e:\santoku\frida\frida+mobsf\lib\site-packages (from frida-tools) (0.4.6)
Requirement already satisfied: frida<17.0.0,>=16.2.2 in e:\santoku\frida\frida+mobsf\lib\site-packages (from frida-tools) (16.7.10)
Requirement already satisfied: prompt-toolkit<4.0.0,>=2.0.0 in e:\santoku\frida\frida+mobsf\lib\site-packages (from frida-tools) (3.0.50)
Requirement already satisfied: pygments<3.0.0,>=2.0.2 in e:\santoku\frida\frida+mobsf\lib\site-packages (from frida-tools) (2.19.1)
Requirement already satisfied: websockets<14.0.0,>=13.0.0 in e:\santoku\frida\frida+mobsf\lib\site-packages (from frida-tools) (13.1)
Requirement already satisfied: wcwidth in e:\santoku\frida\frida+mobsf\lib\site-packages (from prompt-toolkit<4.0.0,>=2.0.0->frida-tools) (0.2.13)

(frida+mobsf) E:\Santoku\frida\frida+mobsf>frida --version
16.7.10

(frida+mobsf) E:\Santoku\frida\frida+mobsf>
```

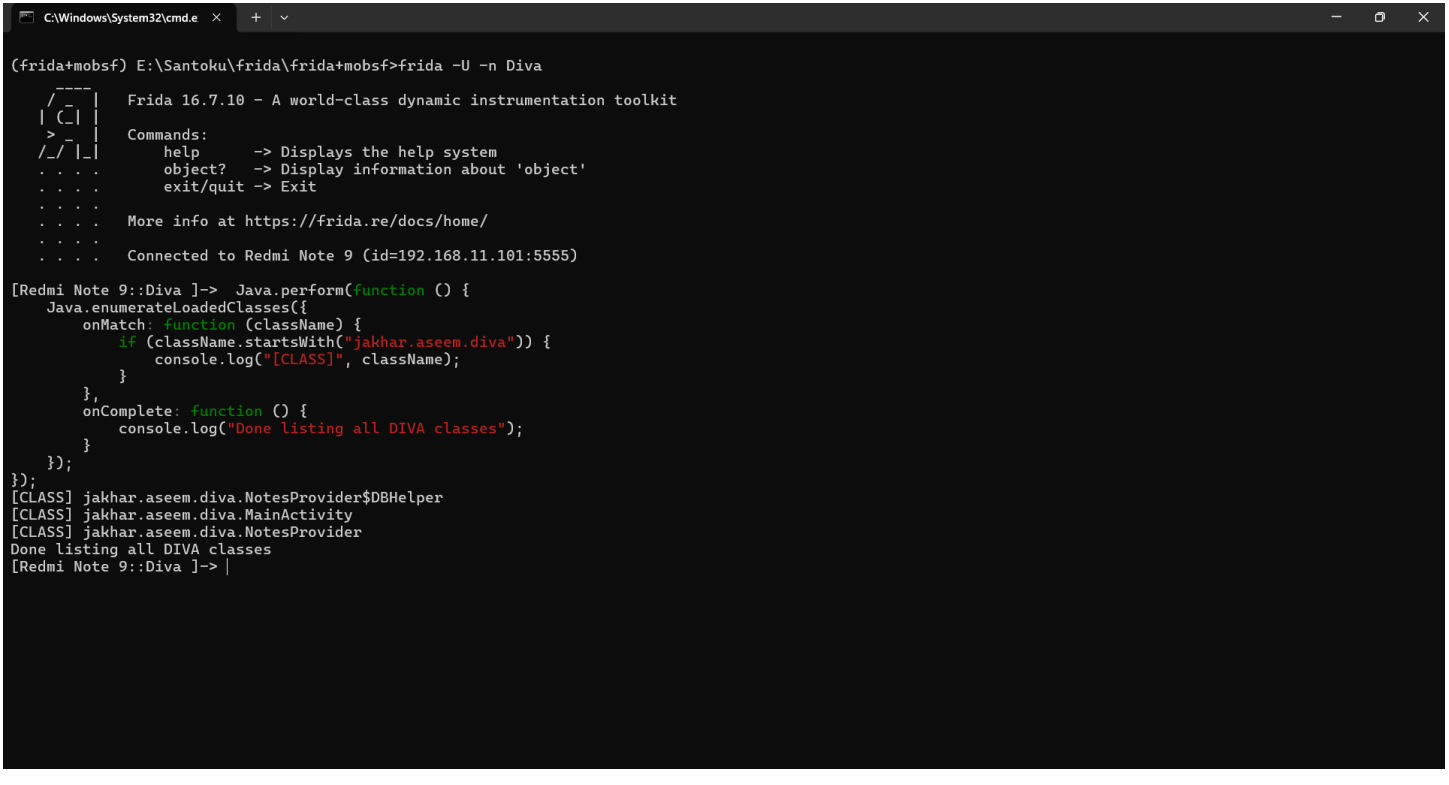
```
C:\Windows\System32\cmd.e

Microsoft Windows [Version 10.0.26120.3863]
(c) Microsoft Corporation. All rights reserved.

E:\Program Files\Genymobile\Genymotion\tools>adb push frida-server /data/local/tmp/
frida-server: 1 file pushed. 88.1 MB/s (114292696 bytes in 1.238s)

E:\Program Files\Genymobile\Genymotion\tools>adb shell "chmod 755 /data/local/tmp/frida-server"

E:\Program Files\Genymobile\Genymotion\tools>adb shell
su       # (Genymotion comes rooted!)
cd /data/local/tmp
./fvbox86p:/ # su       # (Genymotion comes rooted!)
rida-server &
:/ #
```

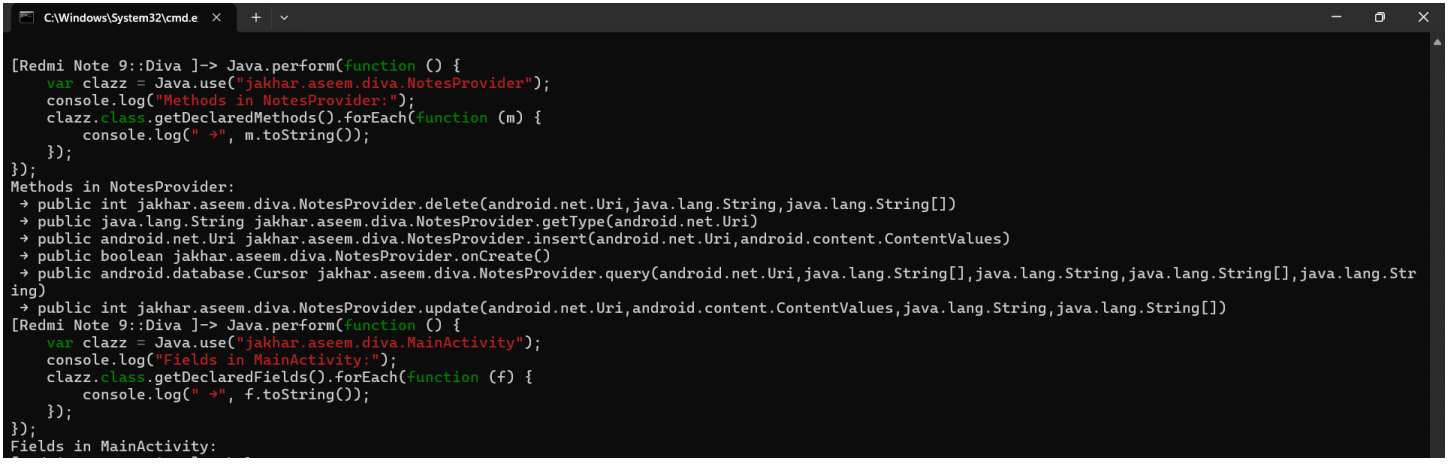
```
C:\Windows\System32\cmd.e

(frida+mobsf) E:\Santoku\frida\frida+mobsf>frida-ps -U
 PID  Name
----  ------------------------------------------------------------
2334  Google Play Store
1686  Phone
1670  adbd
1227  android.ext.services
 236  android.hardware.atrace@1.0-service
 881  android.hardware.audio.service
 346  android.hardware.authsecret@1.0-service
 347  android.hardware.bluetooth@1.1-service.sim
 351  android.hardware.camera.provider@2.4-service_64
 352  android.hardware.cas@1.2-service
 354  android.hardware.configstore@1.1-service
 356  android.hardware.drm@1.0-service
 359  android.hardware.drm@1.3-service.clearkey
 360  android.hardware.gatekeeper@1.0-service.software
 362  android.hardware.gnss@1.0-service
 363  android.hardware.graphics.allocator@2.0-service
 365  android.hardware.graphics.composer@2.3-service
 367  android.hardware.health@2.0-service.genymotion
 387  android.hardware.identity-service.example
 839  android.hardware.input.classifier@1.0-service.default
 239  android.hardware.keymaster@3.0-service
 370  android.hardware.light@2.0-service
 554  android.hardware.media.omx@1.0-service
 371  android.hardware.memtrack@1.0-service
 373  android.hardware.neuralnetworks@1.3-service-sample-all
 374  android.hardware.neuralnetworks@1.3-service-sample-float-fast
 376  android.hardware.neuralnetworks@1.3-service-sample-float-slow
 378  android.hardware.neuralnetworks@1.3-service-sample-minimal
 380  android.hardware.neuralnetworks@1.3-service-sample-quant
 390  android.hardware.power-service.example
 382  android.hardware.power.stats@1.0-service.mock
 383  android.hardware.sensors@1.0-service
 385  android.hardware.wifi@1.0-service
 341  android.hidl.allocator@1.0-service
1734  android.process.acore
2586  android.process.media
 233  android.system.suspend@1.0-service
 888  audioserver
```

```
C:\Windows\System32\cmd.e

1713  logcat
 190  logd
 277  magiskd
 651  mdnsd
 549  media.extractor
 550  media.metrics
 551  mediaserver
 558  mediaswcodec
 332  netd
 399  network_profile
 185  redis
 555  rild
 192  servicemanager
 401  settingsd
1711  sh
3494  sh
3503  sh
3518  sh
 331  statsd
 552  storaged
 545  su
3496  su
3497  su
3500  su
3501  su
 402  surfaceflinger
 746  system_server
 403  systempatcher_native
 274  tombstoned
 534  traced
 533  traced_probes
 171  ueventd
 405  vinput
 203  vold
1089  webview_zygote
 553  wificond
3481  wpa_supplicant.conf
 527  zygote
 334  zygote64

(frida+mobsf) E:\Santoku\frida\frida+mobsf>
```

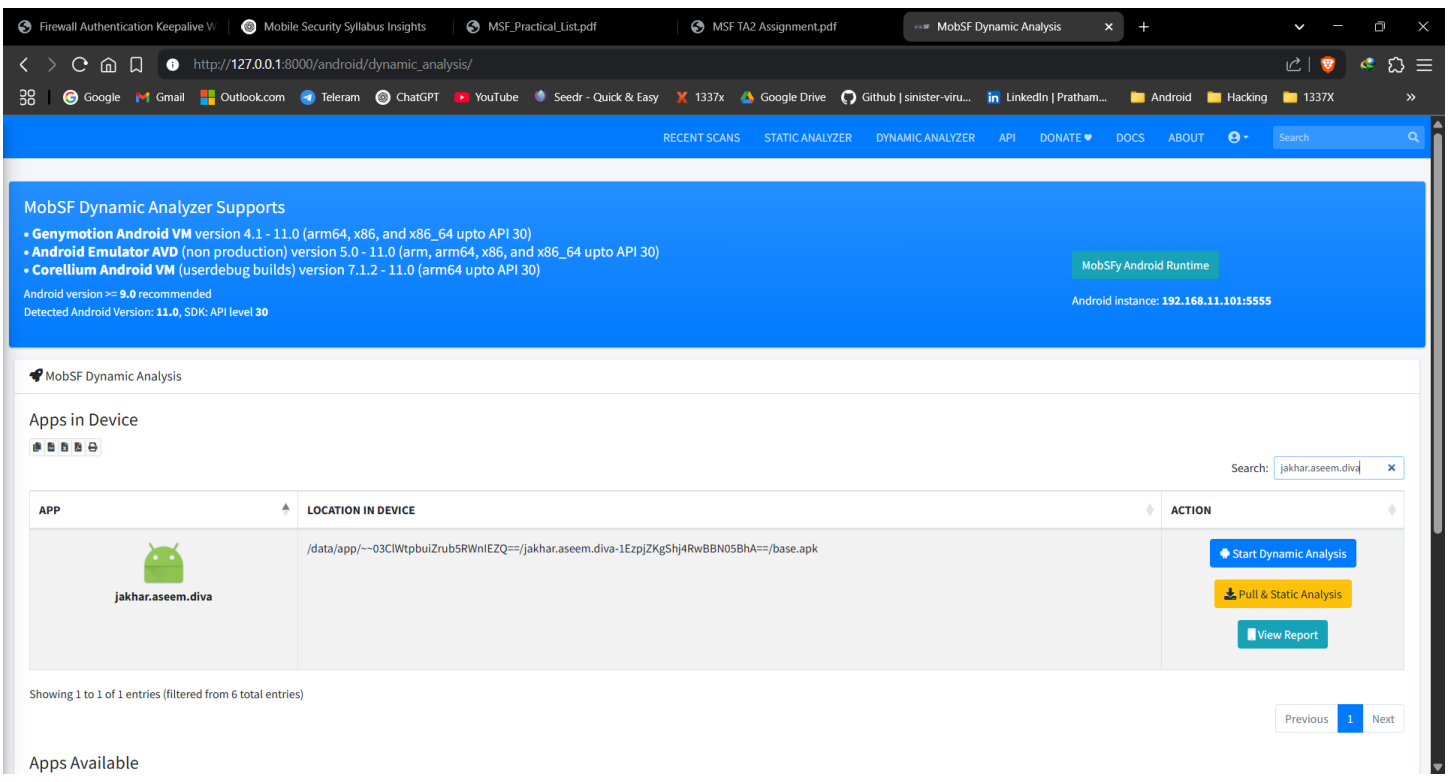
```
C:\Windows\System32\cmd.e

 334  zygote64

(frida+mobsf) E:\Santoku\frida\frida+mobsf>frida -U -n Diva

     ____
    / _  |   Frida 16.7.10 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Redmi Note 9 (id=192.168.11.101:5555)

[Redmi Note 9::Diva ]-> help
Available commands:
  %resume(0) - resume execution of the spawned process
  %load(1) - Load an additional script and reload the current REPL state
  %reload(0) - reload (i.e. rerun) the script that was given as an argument to the REPL
  %unload(0) - no description
  %autoperform(1) - receive on/off as first and only argument, when switched on will wrap any REPL code with Java.performNow()
  %autoreload(1) - disable or enable auto reloading of script files
  %exec(1) - execute the given file path in the context of the currently loaded scripts
  %time(1+) - measure the execution time of the given expression and print it to the screen
  %help(0) - print a list of available REPL commands

For help with Frida scripting API, check out https://frida.re/docs/

[Redmi Note 9::Diva ]->
```

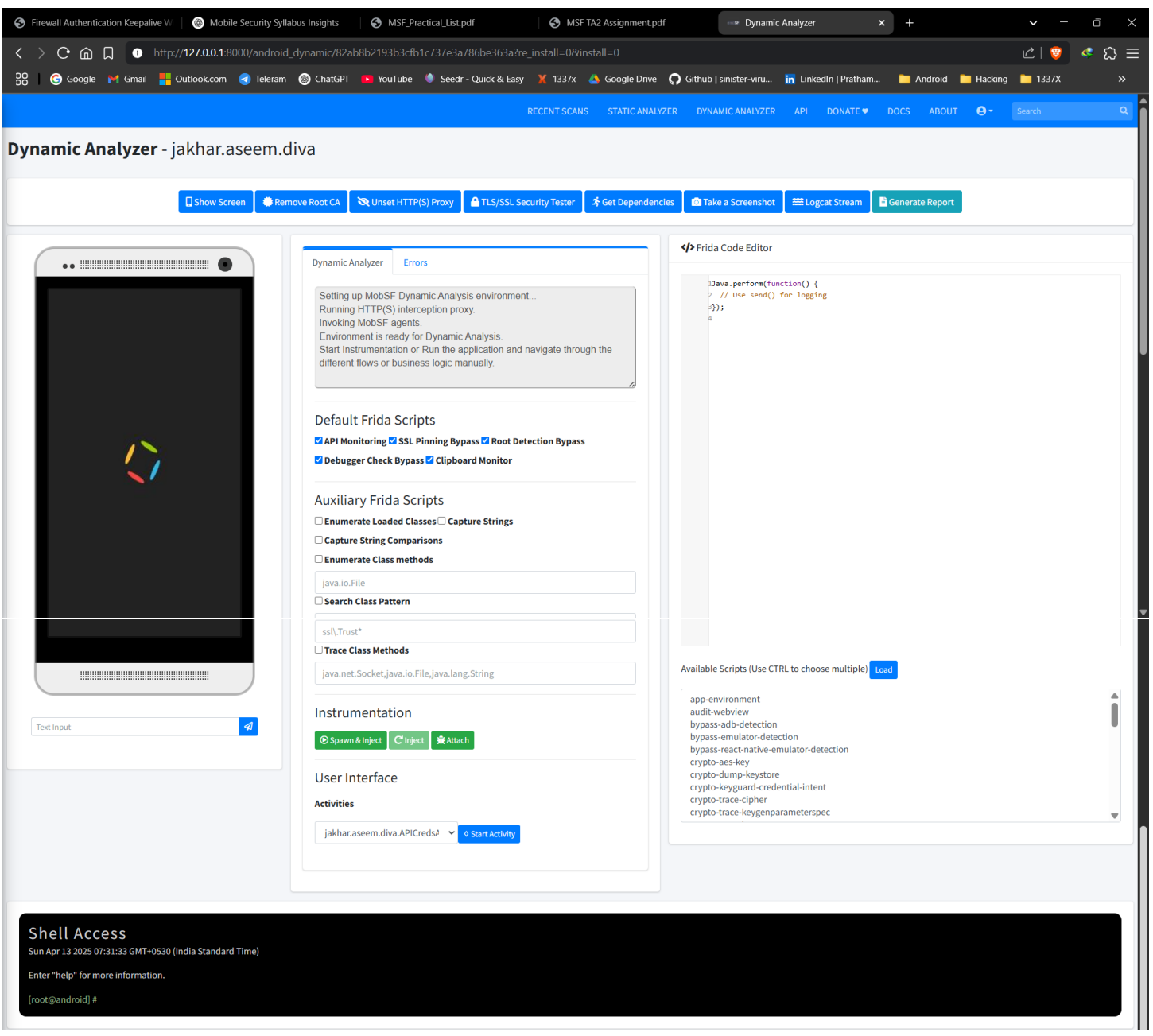
[41].Testing and Evaluation of Android App using Frida

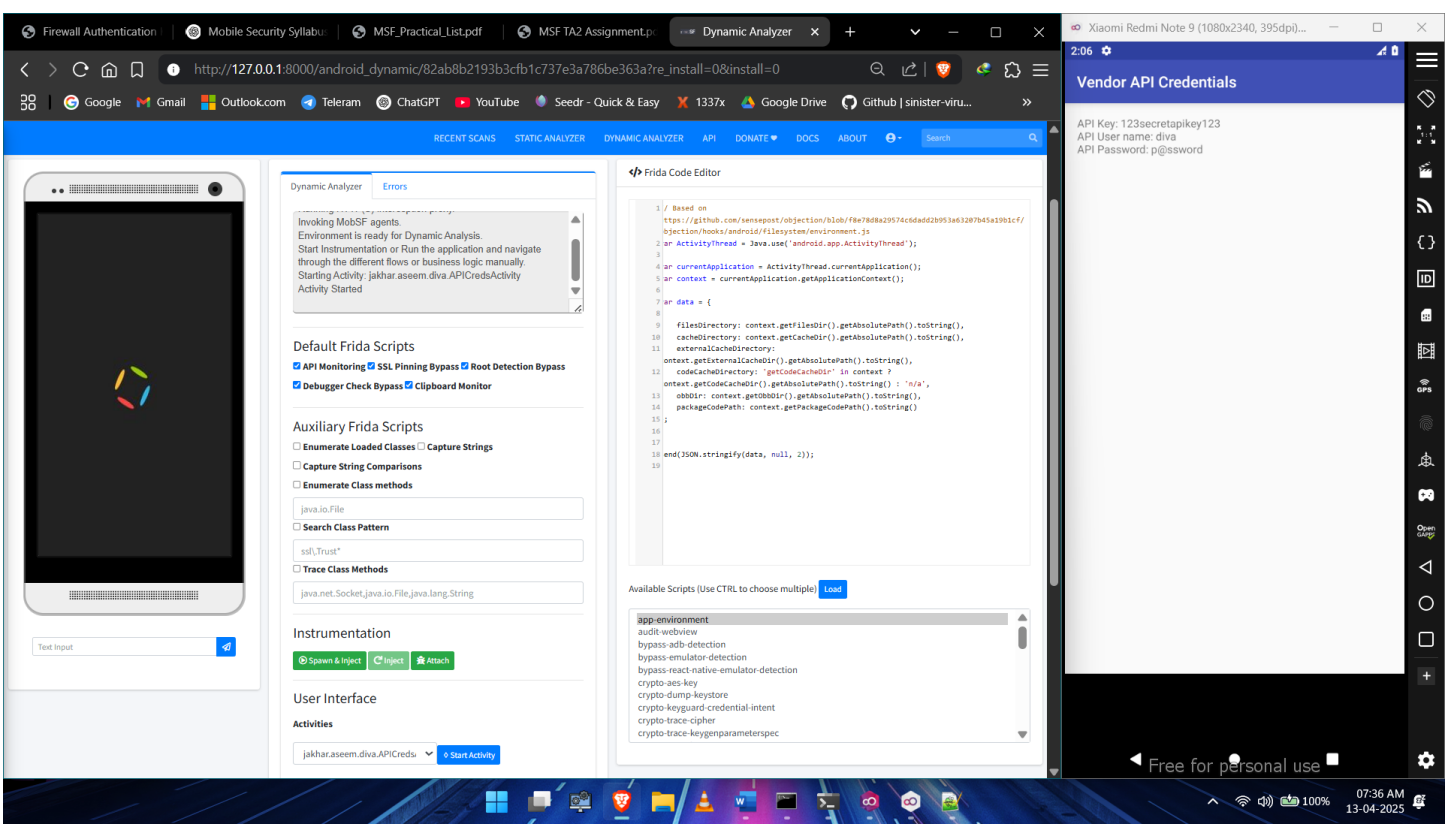


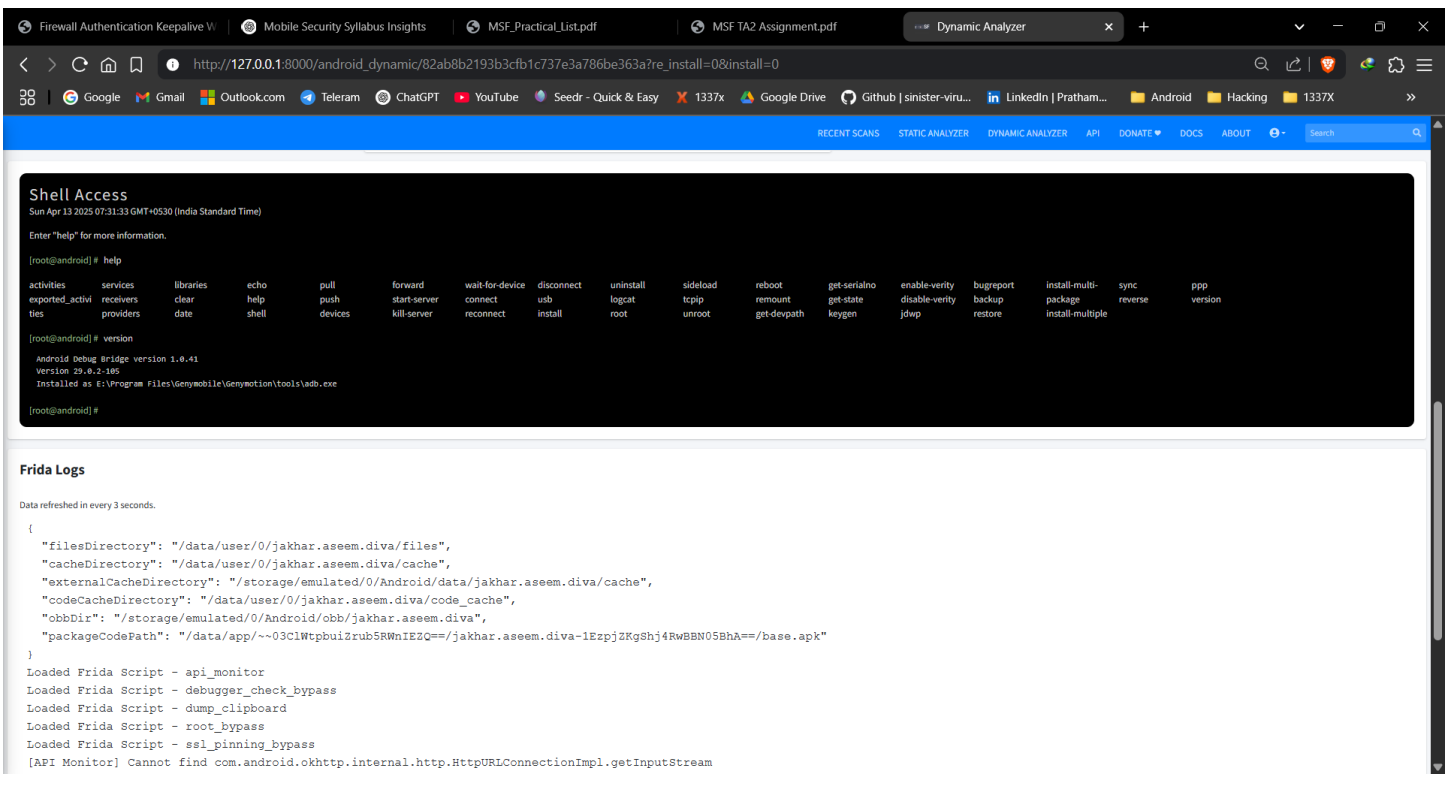


[42]. Dynamic Analysis using MobSF and Frida









[43]. Configuration of OWASP Security Shepherd – Mobile Security platform
[44]. Practical: 01 OWASP Security Shepherd – Mobile Security platform
[45]. Practical: 02 OWASP Security Shepherd – Mobile Security platform
[46]. Practical: 03 OWASP Security Shepherd – Mobile Security platform
[47]. Practical: 04 OWASP Security Shepherd – Mobile Security platform