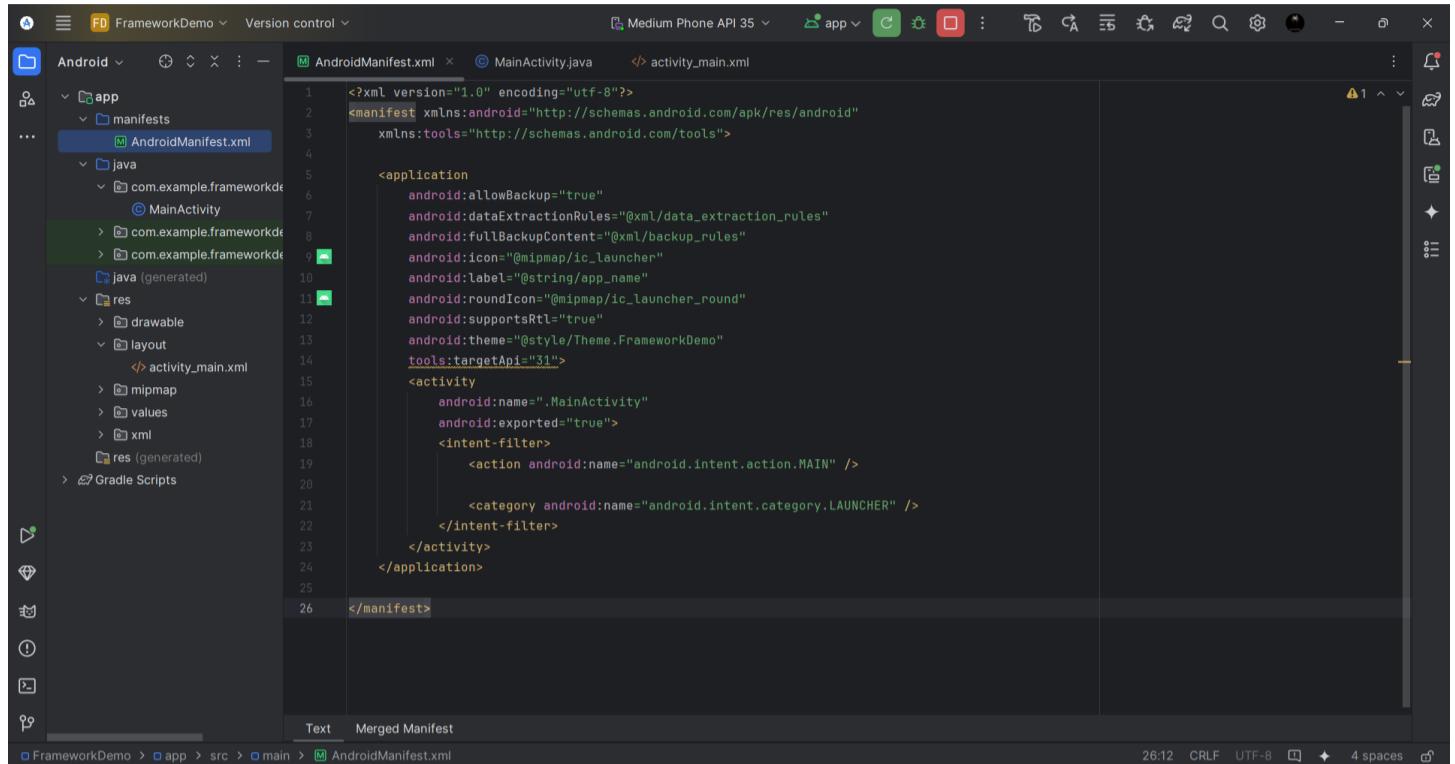


# MSF TA2 Assignment

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



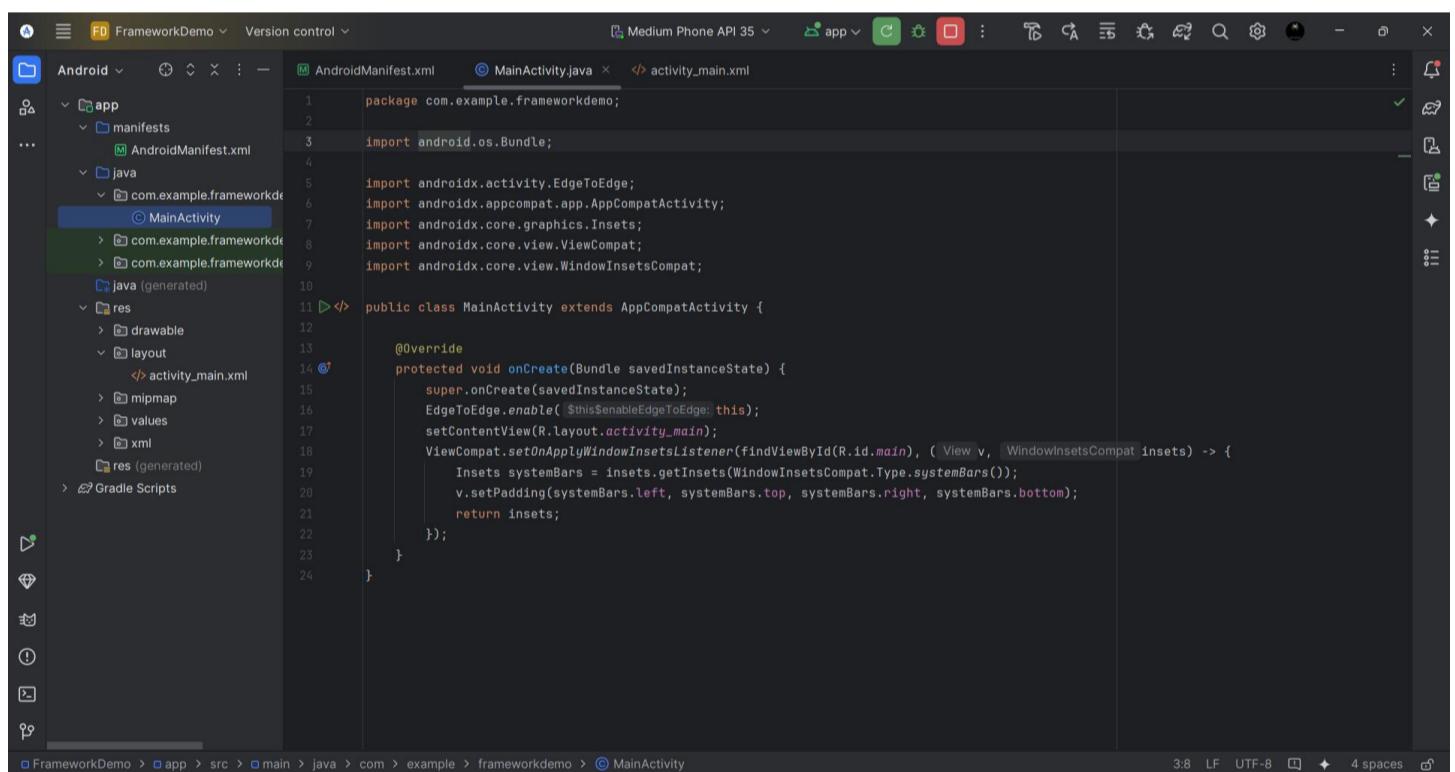
The screenshot shows the Android Studio interface with the project navigation bar at the top. The left sidebar displays the project structure under 'app'. The main editor window shows the 'AndroidManifest.xml' file. The code defines an application with a target API of 31, containing one activity named 'MainActivity' which is exported and has an intent filter for the launcher category.

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools">

    <application
        android:allowBackup="true"
        android:dataExtractionRules="@xml/data_extraction_rules"
        android:fullBackupContent="@xml/backup_rules"
        android:icon="@mipmap/ic_launcher"
        android:label="@string/app_name"
        android:roundIcon="@mipmap/ic_launcher_round"
        android:supportsRtl="true"
        android:theme="@style/Theme.FrameworkDemo"
        tools:targetApi="31">

        <activity
            android:name=".MainActivity"
            android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>

</manifest>
```



The screenshot shows the Android Studio interface with the project navigation bar at the top. The left sidebar displays the project structure under 'app'. The main editor window shows the 'MainActivity.java' file. The code defines a class 'MainActivity' that extends 'AppCompatActivity'. It overrides the 'onCreate' method to set up edge-to-edge functionality and handle window insets.

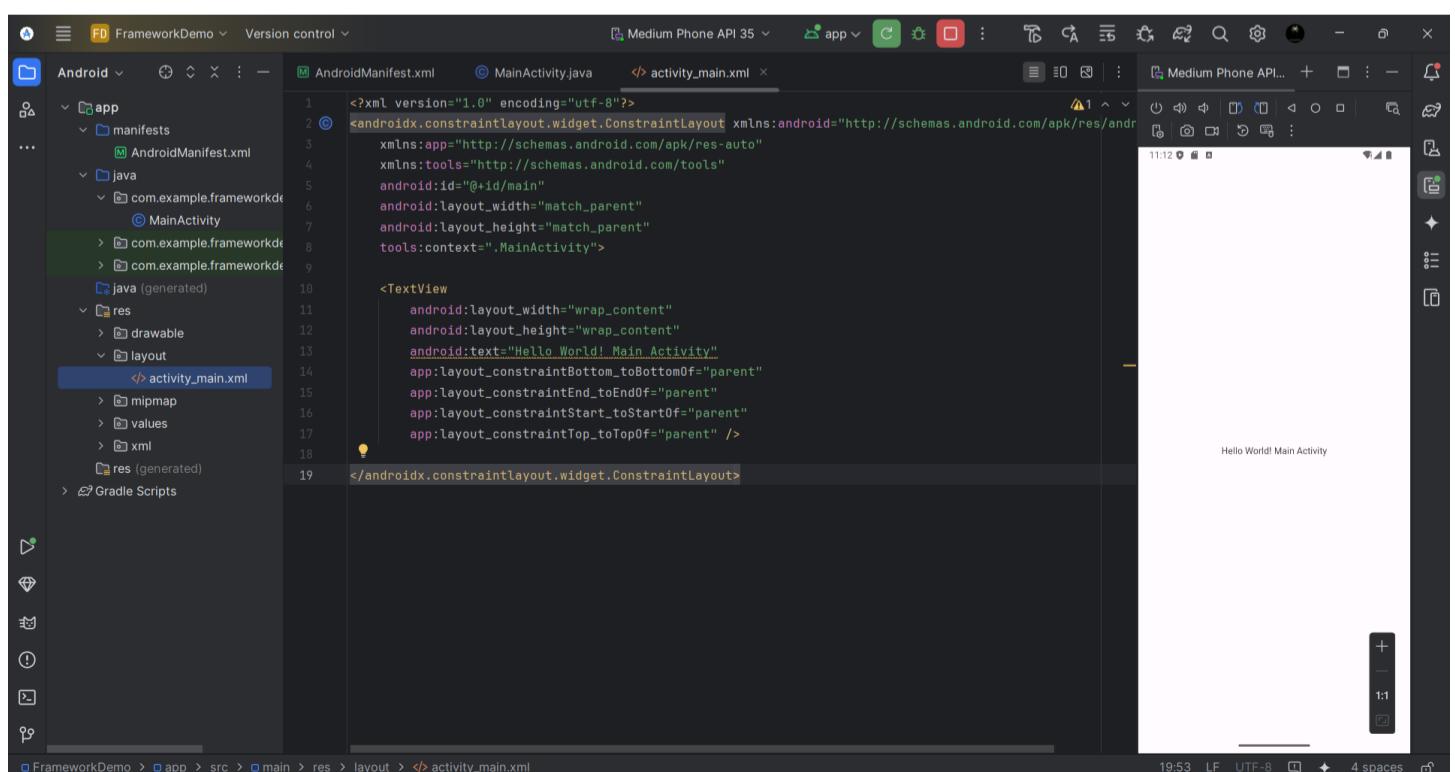
```
package com.example.frameworkdemo;

import android.os.Bundle;

import androidx.activity.EdgeToEdge;
import androidx.appcompat.app.AppCompatActivity;
import android.core.graphics.Insets;
import android.core.view.ViewCompat;
import android.core.view.WindowInsetsCompat;

public class MainActivity extends AppCompatActivity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        EdgeToEdge.enable(this);
        setContentView(R.layout.activity_main);
        ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main), (View v, WindowInsetsCompat insets) -> {
            Insets systemBars = insets.getInsets(WindowInsetsCompat.Type.systemBars());
            v.setPadding(systemBars.left, systemBars.top, systemBars.right, systemBars.bottom);
            return insets;
        });
    }
}
```



The screenshot shows the Android Studio interface with the project navigation bar at the top. The left sidebar displays the project structure under 'app'. The main editor window shows the 'activity\_main.xml' file. The XML layout defines a single 'TextView' with a wrap\_content width and height, containing the text 'Hello World! Main Activity'. The right side of the screen shows a preview of the activity with the text displayed.

```
<?xml version="1.0" encoding="utf-8"?>
<androidx.constraintlayout.widget.ConstraintLayout xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:app="http://schemas.android.com/tools"
    android:id="@+id/main"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    tools:context=".MainActivity">

    <TextView
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:text="Hello World! Main Activity"
        app:layout_constraintBottom_toBottomOf="parent"
        app:layout_constraintEnd_toEndOf="parent"
        app:layout_constraintStart_toStartOf="parent"
        app:layout_constraintTop_toTopOf="parent" />

</androidx.constraintlayout.widget.ConstraintLayout>
```

## [2]. Demonstration of Android Intent

The screenshot shows the Android Studio interface with the following details:

- Project Structure:** The left sidebar shows the project structure under "Android". It includes the "app" module, "manifests" (with "AndroidManifest.xml"), "java" (with "com.example.intentdemo" package containing "MainActivity" and "SecondActivity"), "res" (with "drawable", "layout" containing "activity\_main.xml" and "activity\_second.xml", "mipmap", "values", and "xml"), and "res (generated)".
- MainActivity.java Code:** The main code block shows the implementation of the `MainActivity` class. It sets the content view to `activity_main`, finds a `TextView` with ID `txtActivityName`, and sets its text to "Current Activity: " + `currentActivity`. It also finds a `Button` with ID `btnNext` and sets its `onClick` listener to start `SecondActivity`.
- Run Tab:** The top right shows the "Medium Phone API 35" tab and the "app" configuration.
- Bottom Status Bar:** The status bar at the bottom indicates the current time as 26:2, the font size as LF, the encoding as UTF-8, and the code editor settings as 4 spaces.

```
1 package com.example.intentdemo;
2
3 import android.content.Intent;
4 import android.os.Bundle;
5 import android.widget.Button;
6 import android.widget.TextView;
7 import androidx.appcompat.app.AppCompatActivity;
8
9 public class MainActivity extends AppCompatActivity {
10     @Override
11     protected void onCreate(Bundle savedInstanceState) {
12         super.onCreate(savedInstanceState);
13         setContentView(R.layout.activity_main);
14
15         TextView txtActivityName = findViewById(R.id.txtActivityName);
16         String currentActivity = this.getClass().getSimpleName();
17         txtActivityName.setText("Current Activity: " + currentActivity);
18
19
20         Button btnNext = findViewById(R.id.btnNext);
21         btnNext.setOnClickListener( View view -> {
22             Intent intent = new Intent( packageContext, MainActivity.this, SecondActivity.class );
23             startActivity(intent);
24         });
25     }
26 }
27
```

On the right side, there is a preview window titled "IntentDemo" showing the current activity state. A button labeled "GO TO SECOND ACTIVITY" is present.

The screenshot shows the Android Studio interface with the following details:

- Project Structure:** The left sidebar shows the project structure under the `app` module. It includes `manifests`, `java` (containing `MainActivity` and `SecondActivity`), `res` (containing `drawable`, `layout` (with `activity_main.xml` selected), `mipmap`, `values`, and `xml`), and `res (generated)`.
- Code Editor:** The main area displays the XML code for `activity_main.xml`. The code defines a `LinearLayout` with a `TextView` and a `Button`. The `TextView` has constraints relative to the top, start, end, and bottom of its parent, and a margin at the bottom of 16dp. The `Button` has an onClick event linked to the `btnNext` resource.
- Preview Pane:** On the right, the preview pane shows a mobile device screen with the text "Activity Name" and a button labeled "Go to Second Activity". A tooltip indicates "Current Activity: MainActivity".
- Bottom Bar:** The bottom bar shows the file path `IntentDemo > app > src > main > res > layout > activity_main.xml`, and the status bar indicates `30:1 (15 chars) LF UTF-8 4 spaces`.

```
1 package com.example.intentdemo;
2
3 import android.content.Intent;
4 import android.os.Bundle;
5 import android.widget.Button;
6 import android.widget.TextView;
7 import androidx.appcompat.app.AppCompatActivity;
8
9 public class SecondActivity extends AppCompatActivity {
10     @Override
11     protected void onCreate(Bundle savedInstanceState) {
12         super.onCreate(savedInstanceState);
13         setContentView(R.layout.activity_second);
14
15         // Display the activity name
16         TextView txtActivityName = findViewById(R.id.txtActivityName2);
17         String currentActivity = this.getClass().getSimpleName();
18         txtActivityName.setText("Current Activity: " + currentActivity);
19
20         // Button to go back to MainActivity
21         Button btnBack = findViewById(R.id.btnBack);
22         btnBack.setOnClickListener(v -> {
23             Intent intent = new Intent(getApplicationContext(), MainActivity.class);
24             startActivity(intent);
25         });
26     }
27 }
28 }
```

Current Activity: SecondActivity

GO TO MAIN ACTIVITY

The screenshot shows the Android Studio interface with the project structure on the left and the code editor on the right.

**Project Structure:**

- app
- manifests
- AndroidManifest.xml
- java
  - com.example.intentdemo
    - MainActivity
    - SecondActivity
  - com.example.intentdemo (generated)
- res
  - drawable
  - layout
    - activity\_main.xml
    - activity\_second.xml
  - mipmap
  - values
  - xml
- res (generated)

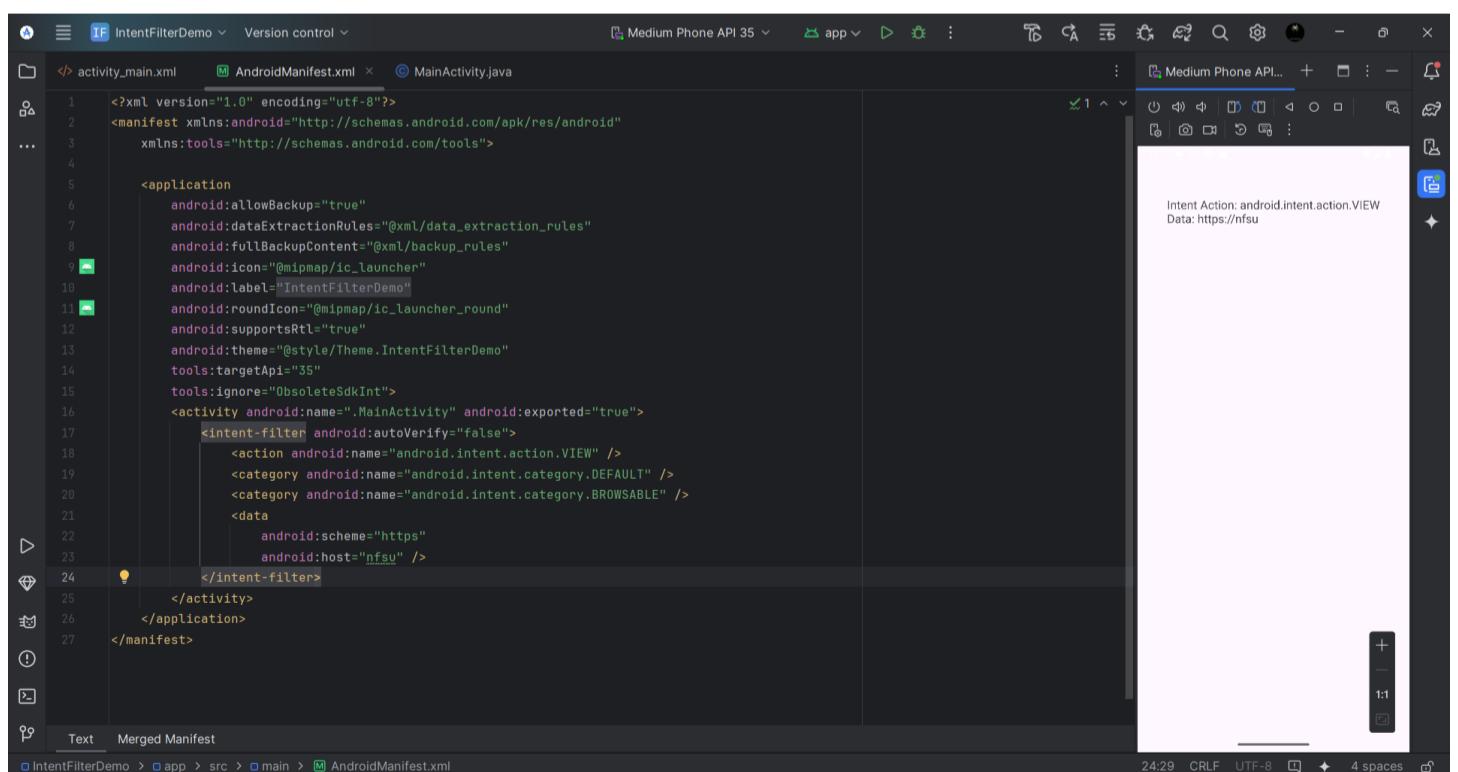
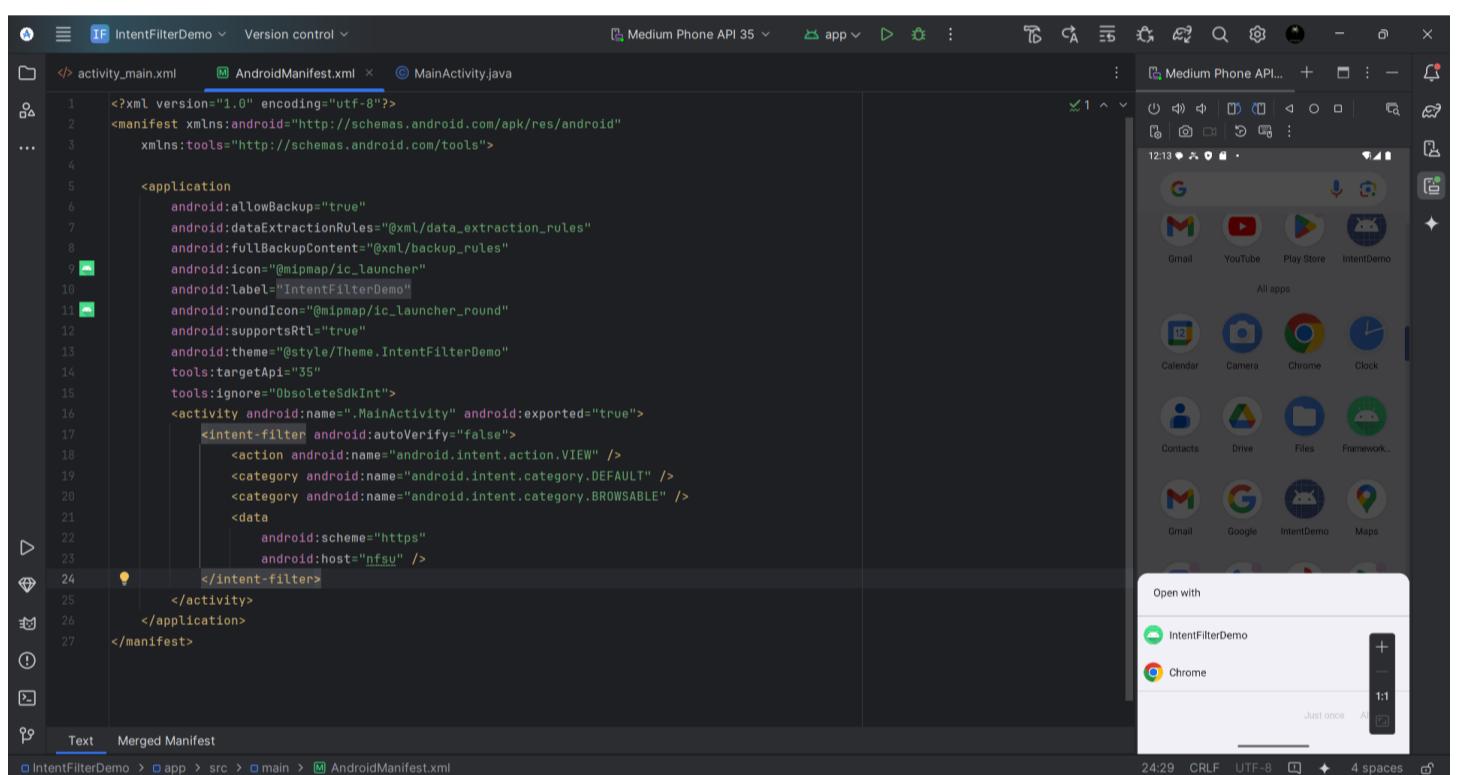
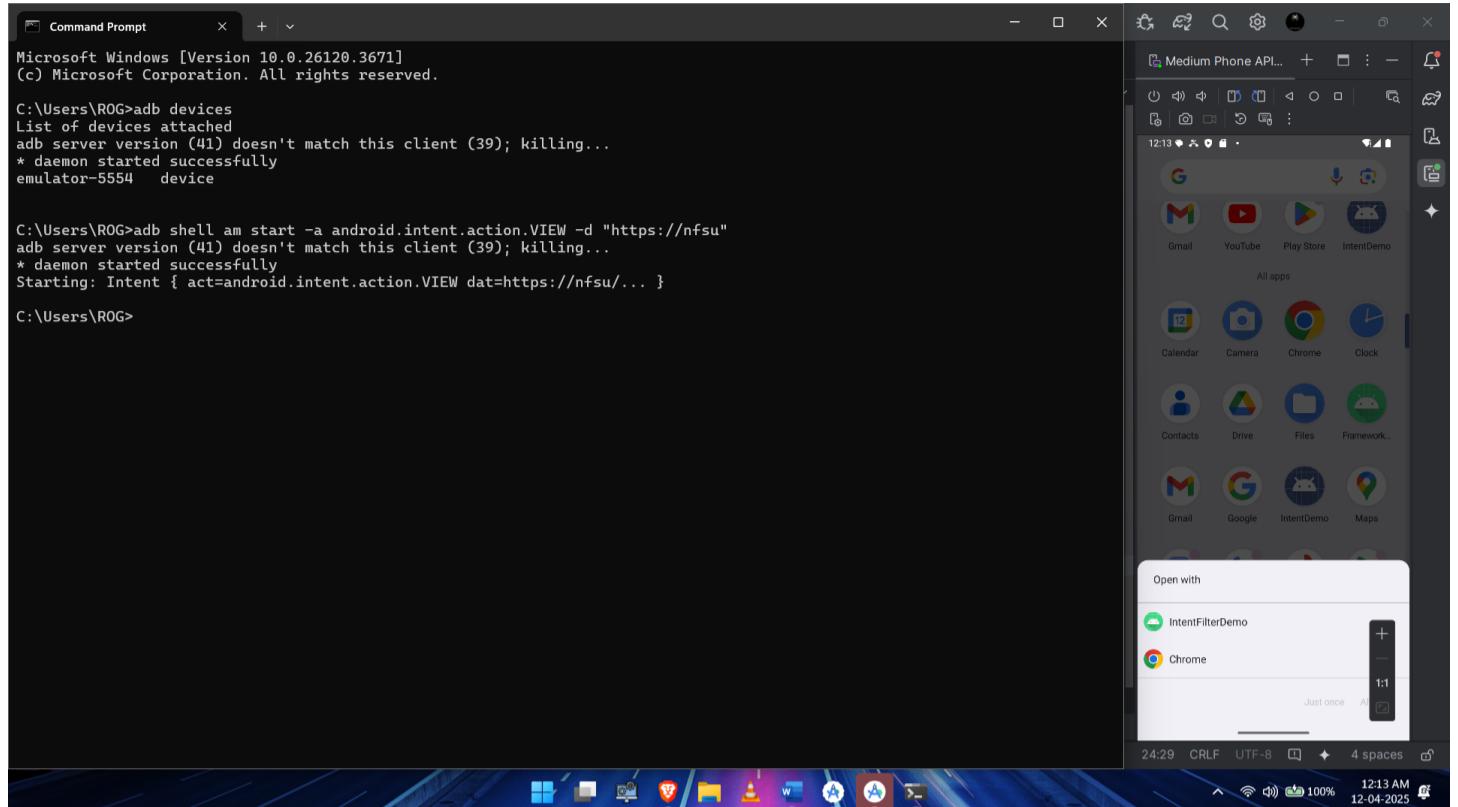
**Code Editor (SecondActivity.java):**

```
2 <LinearLayout xmlns:android="http://schemas.android.com/apk/res/android"
3     android:layout_width="match_parent"
4     android:layout_height="match_parent"
5     android:gravity="center"
6     android:orientation="vertical"
7     tools:context=".SecondActivity">
8
9     <TextView
10         android:id="@+id/txtActivityName2"
11         android:layout_width="wrap_content"
12         android:layout_height="wrap_content"
13         android:text="Activity Name"
14         android:textSize="20sp"
15         android:textStyle="bold"
16         android:textColor="#0000"
17         app:layout_constraintTop_toTopOf="parent"
18         app:layout_constraintStart_toStartOf="parent"
19         app:layout_constraintEnd_toEndOf="parent"
20         app:layout_constraintBottom_toTopOf="@+id	btnBack"
21         android:layout_marginBottom="16dp"/>
22
23     <Button
24         android:id="@+id	btnBack"
25         android:layout_width="wrap_content"
26         android:layout_height="wrap_content"
27         android:text="Go to Main Activity"
28         android:textSize="16sp"
29         android:textStyle="bold"
30         android:textColor="#0000"
31         app:layout_constraintTop_toBottomOf="@+id/txtActivityName2"
32         app:layout_constraintStart_toStartOf="parent"
33         app:layout_constraintEnd_toEndOf="parent"/>
34 
```

**Right Panel:**

- Medium Phone API 35
- IntentDemo
- Current Activity: SecondActivity
- GO TO MAIN ACTIVITY

### [3]. Demonstration of Android Intent Filter



## [4]. Demonstration of Android Content Provider

The screenshot shows the Android Studio interface with the AndroidManifest.xml file open. The manifest includes permissions for reading contacts and specifies the MainActivity as the launcher activity. A permission request dialog is displayed on the screen, asking for permission to access contacts, with 'Allow' and 'Don't allow' buttons.

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools">
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <application
        android:allowBackup="true"
        android:dataExtractionRules="@xml/data_extraction_rules"
        android:fullBackupContent="@xml/backup_rules"
        android:icon="@mipmap/ic_launcher"
        android:label="@string/app_name"
        android:roundIcon="@mipmap/ic_launcher_round"
        android:supportsRtl="true"
        android:theme="@style/Theme.ContentProviderDemo"
        tools:targetApi="35"
        tools:ignore="ObsoleteSdkInt">
        <activity
            android:name=".MainActivity"
            android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

The screenshot shows the MainActivity.java code where the developer is handling contact permissions. It checks if the READ\_CONTACTS permission is granted and requests it if not. The emulator displays a list of contacts from two devices: Google Pixel and Google Nexus.

```
package com.example.contentproviderdemo;

import ...

public class MainActivity extends AppCompatActivity {

    ListView contactListView;
    ArrayList<String> contacts = new ArrayList<>();
    final int REQUEST_CONTACT = 1;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        contactListView = findViewById(R.id.contactListView);

        if (ActivityCompat.checkSelfPermission(this, Manifest.permission.READ_CONTACTS) != PackageManager.PERMISSION_GRANTED)
            ActivityCompat.requestPermissions(this, new String[]{Manifest.permission.READ_CONTACTS}, REQUEST_CONTACT);
        else {
            fetchContacts();
        }
    }

    @Override
    public void onRequestPermissionsResult(int requestCode, String[] permissions, int[] grantResults) {
        if (requestCode == REQUEST_CONTACT && grantResults.length > 0 && grantResults[0] == PackageManager.PERMISSION_GRANTED)
            fetchContacts();
        else {
            Toast.makeText(this, "Permission denied to read contacts", Toast.LENGTH_SHORT).show();
        }
    }

    private void fetchContacts() {
        Cursor cursor = getContentResolver().query(ContactsContract.Contacts.CONTENT_URI, null, null, null, null);
        if (cursor.moveToFirst()) {
            do {
                String name = cursor.getString(cursor.getColumnIndex(ContactsContract.Contacts.DISPLAY_NAME));
                contacts.add(name);
            } while (cursor.moveToNext());
        }
        cursor.close();
        ArrayAdapter<String> adapter = new ArrayAdapter<String>(this, android.R.layout.simple_list_item_1, contacts);
        contactListView.setAdapter(adapter);
    }
}
```

## [5]. Demonstration of Android Broadcast Receiver

The screenshot shows the Android Studio interface with the project 'BroadcastReceiverDemo' open. The left pane displays the code for `MainActivity.java`, which contains Java code for handling battery level changes. The right pane shows a preview of the app running on a 'Medium Phone API 35' emulator, displaying the text 'Battery Level: 77%'.

```
1 package com.example.broadcastreceiverdemo;
2
3 import ...
4
5 public class MainActivity extends AppCompatActivity {
6
7     TextView batteryLevelText;
8
9     BroadcastReceiver batteryReceiver;
10
11    @Override
12    protected void onCreate(Bundle savedInstanceState) {
13        super.onCreate(savedInstanceState);
14        setContentView(R.layout.activity_main);
15
16        batteryLevelText = findViewById(R.id.batteryLevelText);
17
18        // Create broadcast receiver
19        batteryReceiver = (BroadcastReceiver) (context, intent) -> {
20            int level = intent.getIntExtra(BatteryManager.EXTRA_LEVEL, defaultValue: -1);
21            batteryLevelText.setText("Battery Level: " + level + "%");
22        };
23
24        // Register the receiver dynamically
25        IntentFilter filter = new IntentFilter(Intent.ACTION_BATTERY_CHANGED);
26        registerReceiver(batteryReceiver, filter);
27    }
28
29    @Override
30    protected void onDestroy() {
31        super.onDestroy();
32    }
33
34    ...
35
36    ...
37
38    ...
39
40    ...
41}
```

Battery Level: 77%

## [6]. Demonstration of Android Security Permission Model

The screenshot shows the Android Studio interface with the manifest file open. The manifest includes a camera permission request:

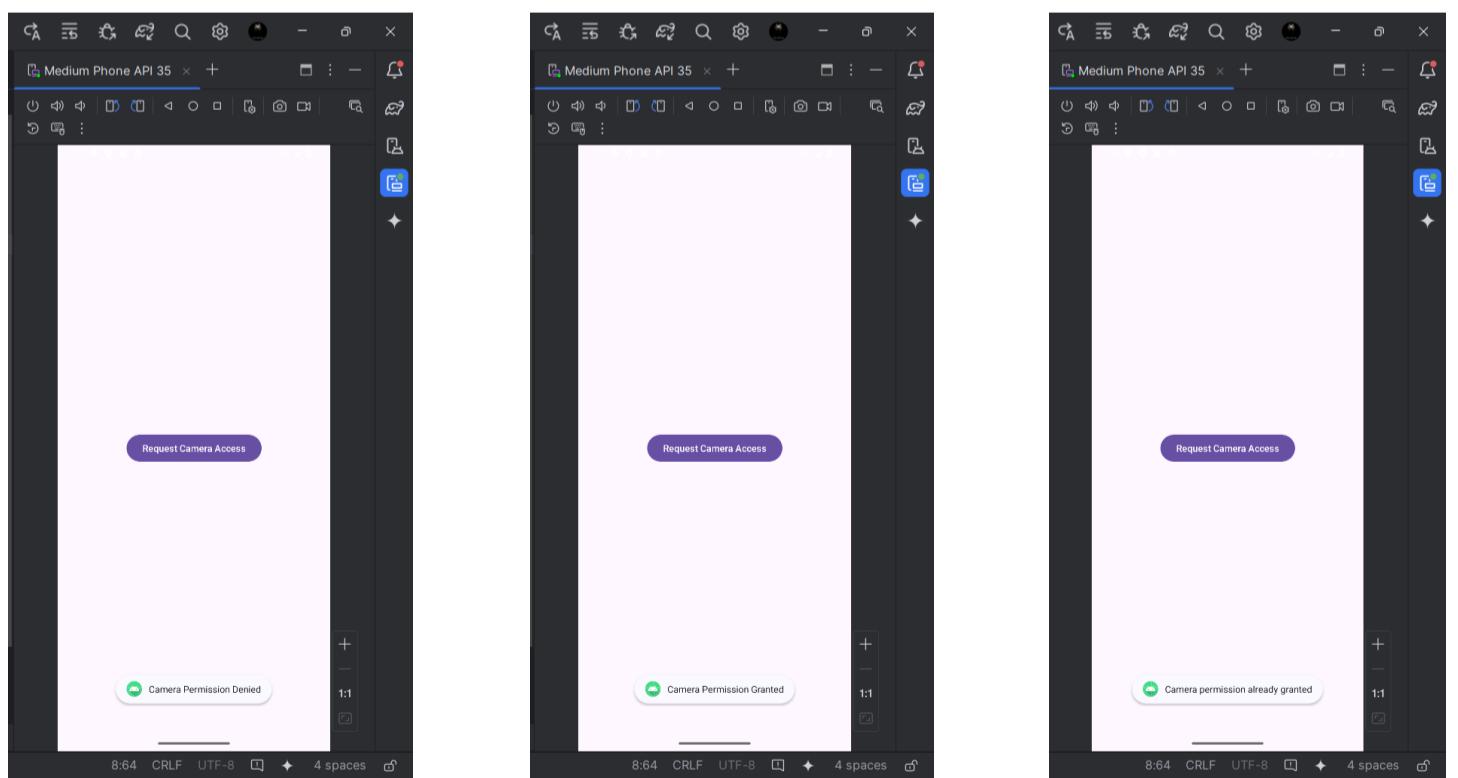
```
<uses-permission android:name="android.permission.CAMERA"/>
```

The right side of the screen shows a preview of the app's user interface with a "Request Camera Access" button.

The screenshot shows the Android device screen displaying a permission dialog from the app:

Allow Security Permission Model Demo to take pictures and record video?

While using the app  
Only this time  
Don't allow



## [7]. Demonstration of Android Services

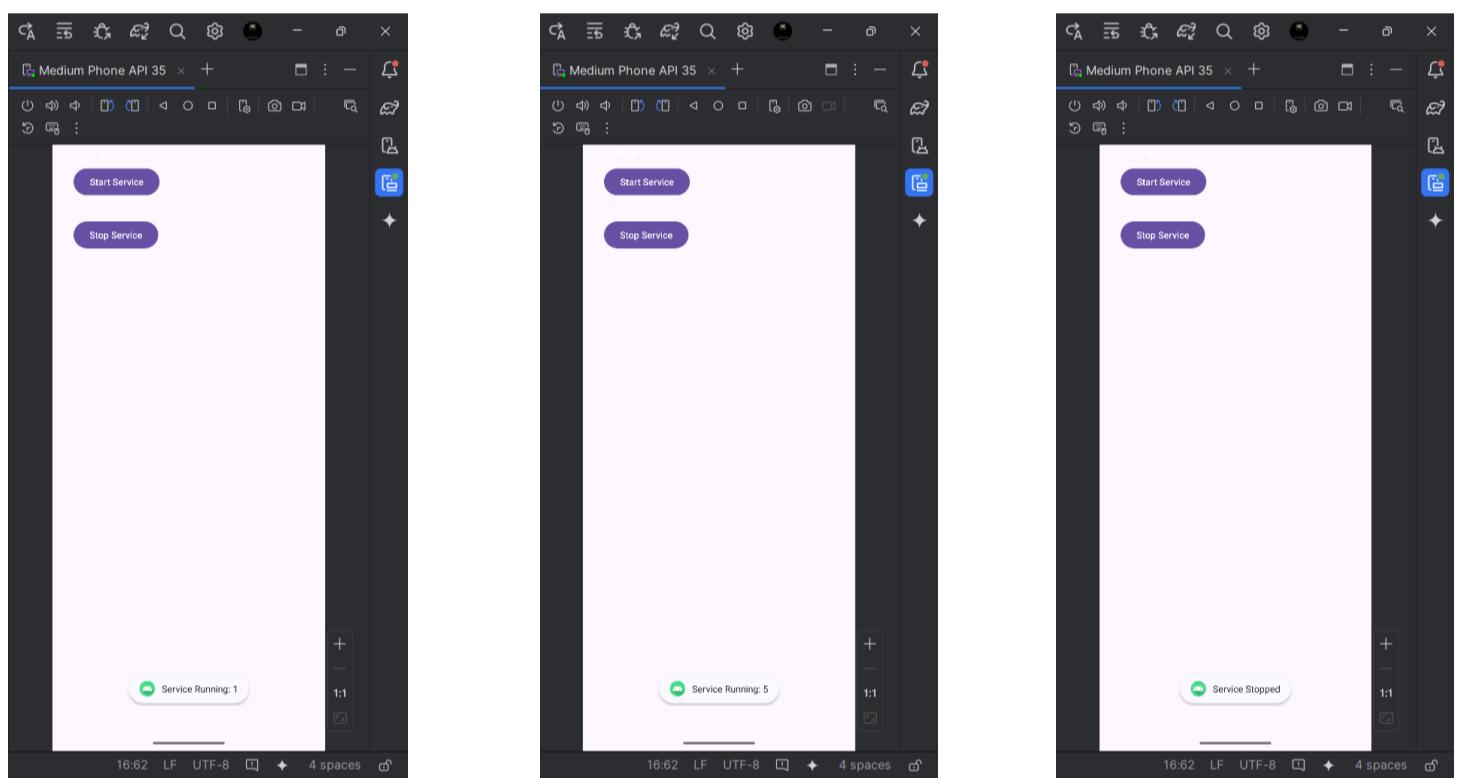
The screenshot shows the Android Studio interface with the project structure on the left and the code editor on the right. The code editor displays the `AndroidManifest.xml` file. It contains the declaration for the service `MyService` with the attribute `android:exported="false"`. The manifest also defines an activity `MainActivity` with its intent filter and category.

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools">

    <application
        android:allowBackup="true"
        android:dataExtractionRules="@xml/data_extraction_rules"
        android:fullBackupContent="@xml/backup_rules"
        android:icon="@mipmap/ic_launcher"
        android:label="ServiceDemo"
        android:roundIcon="@mipmap/ic_launcher_round"
        android:supportsRtl="true"
        android:theme="@style/Theme.ServiceDemo"
        tools:targetApi="35"
        tools:ignore="ObsoleteSdkInt">

        <service android:name=".MyService" android:exported="false"/>

        <activity
            android:name=".MainActivity"
            android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```



The screenshot shows the Android Studio interface with the code editor displaying `MainActivity.java`. The code includes the creation of two buttons, `startServiceBtn` and `stopServiceBtn`, and their corresponding listeners. The Logcat tab at the bottom shows the service being started and destroyed multiple times, with log entries indicating the service's state and the toast messages from the UI.

```
import ...

public class MainActivity extends AppCompatActivity {
    Button startServiceBtn, stopServiceBtn;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        startServiceBtn = findViewById(R.id.startServiceBtn);
        stopServiceBtn = findViewById(R.id.stopServiceBtn);

        startServiceBtn.setOnClickListener(v -> {
            ...
        });
    }
}
```

Logcat Output:

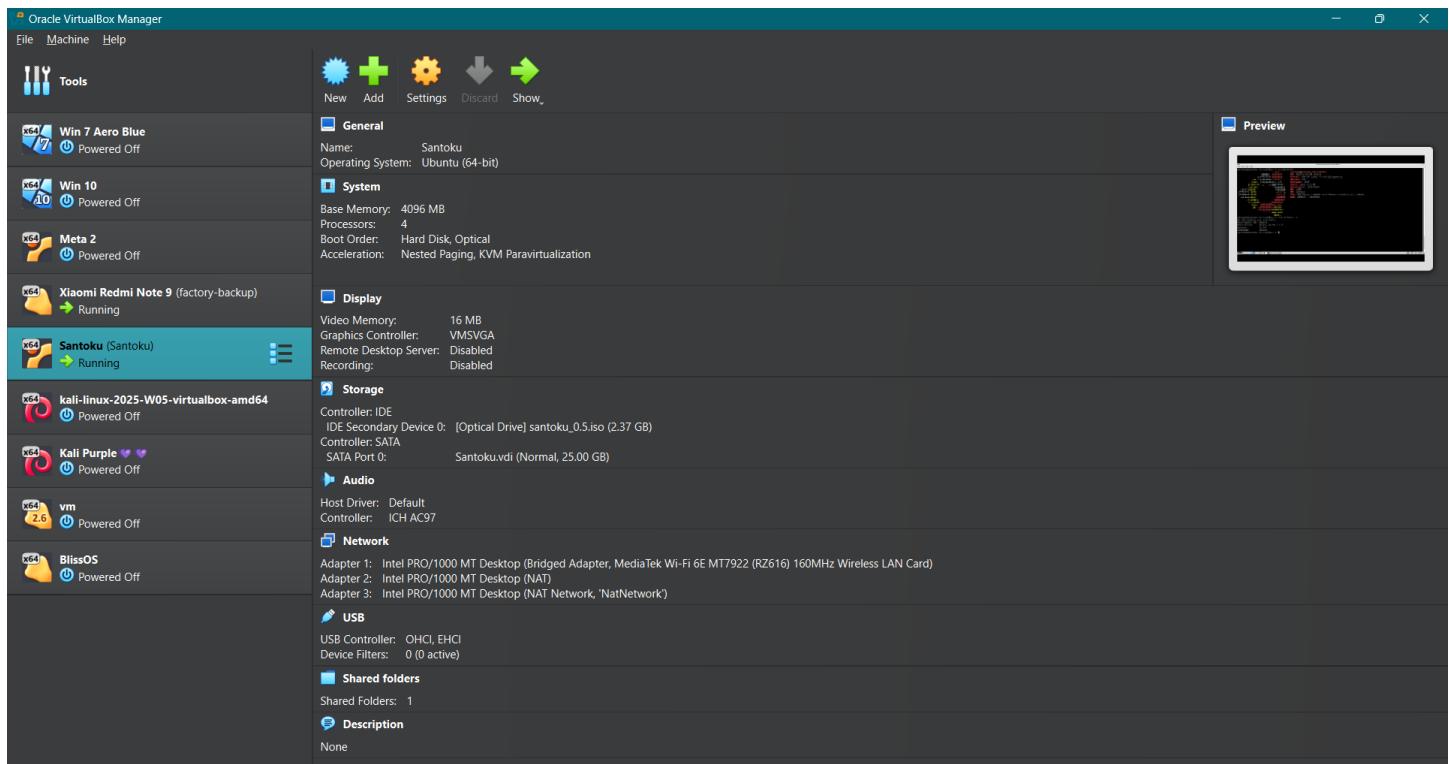
```
2025-04-12 16:03:48.555 615-1620 ActivityManager system_server
2025-04-12 16:06:00.102 615-940 ActivityManager system_server
2025-04-12 16:06:27.455 6341-6457 MyService com.example.servicedemo
2025-04-12 16:06:29.456 6341-6457 MyService com.example.servicedemo
2025-04-12 16:06:31.457 6341-6457 MyService com.example.servicedemo
2025-04-12 16:06:33.459 6341-6457 MyService com.example.servicedemo
2025-04-12 16:06:35.461 6341-6457 MyService com.example.servicedemo
2025-04-12 16:06:37.467 6341-6341 MyService com.example.servicedemo

W Scheduling restart of crashed service com.example.servicedemo/.MyService in 1s
I Force stopping service ServiceRecord{7b8af1d} u0 com.example.servicedemo/.MyService
D Running... 1
D Running... 2
D Running... 3
D Running... 4
D Running... 5
D Service Destroyed
```

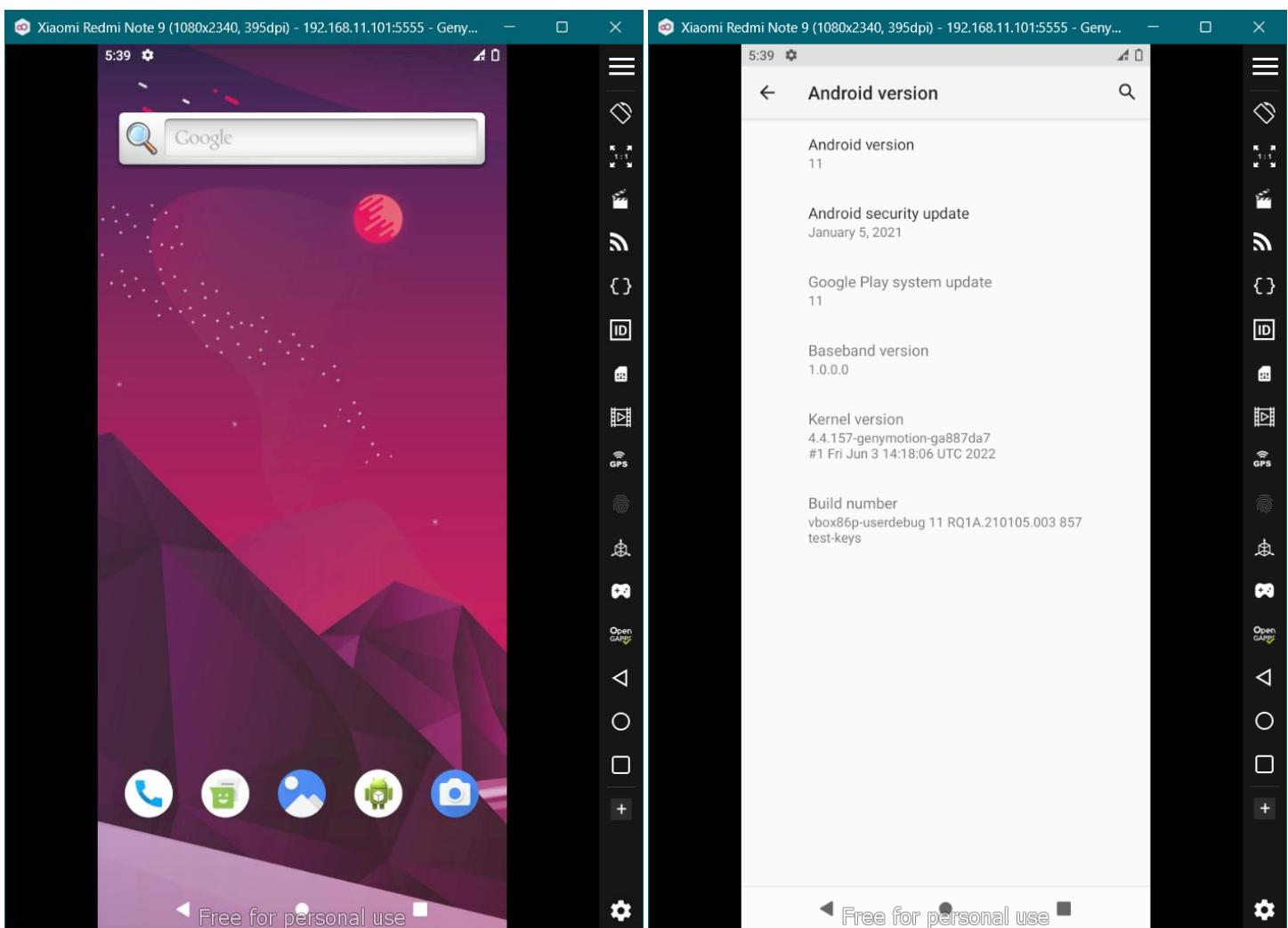
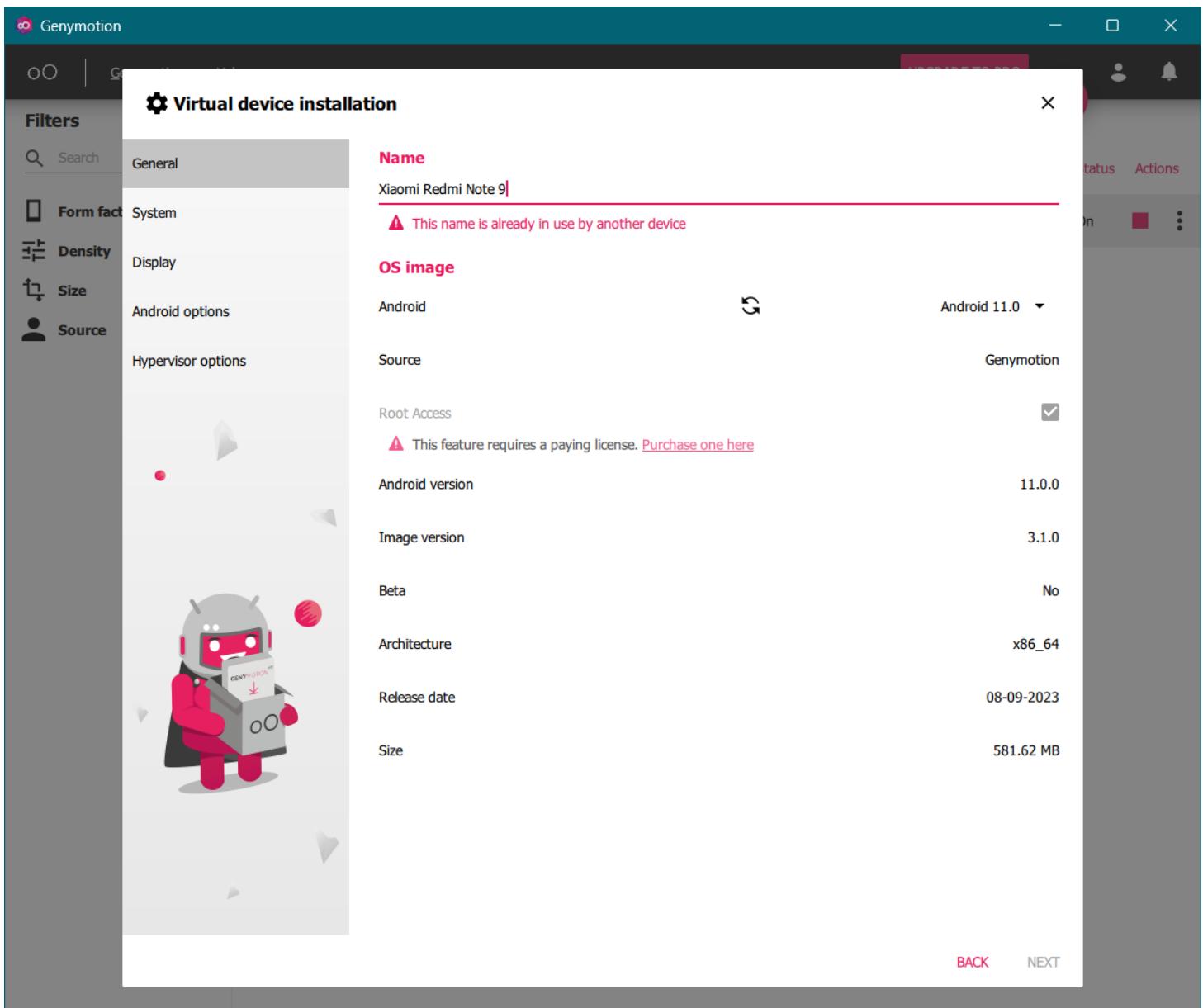
## [8]. Configuration of Santoku OS

```
santoku@santoku-VirtualBox:~$ screenfetch
      ./+o+-
     yyyy- -yyyyyy+
 //++++/-yeyyyyo
 .++ .:/+++++/-+ssss/
 .:+o: /++++++/:---/
 .:+o:+. ...`-/oo++++/
 .:+o:+o/ . +sssoo+/
 .++/+o+o+: /sssooo.
 /++/+o: oo+o /:::::
 +/+o+++ o++o +////
 .++o+++o+: ` /dddhhh.
 .+o+o+: ` oddhhh+
 \+o+o+o ``-`` .:ohdhhhhh+
 `:o++ `ohhhhhhyo++o:
 .o: `syhhhhhh/.oo+o:
 /osyyyyyoo+ooo+++/
 +oo++o\:
 `oo++.

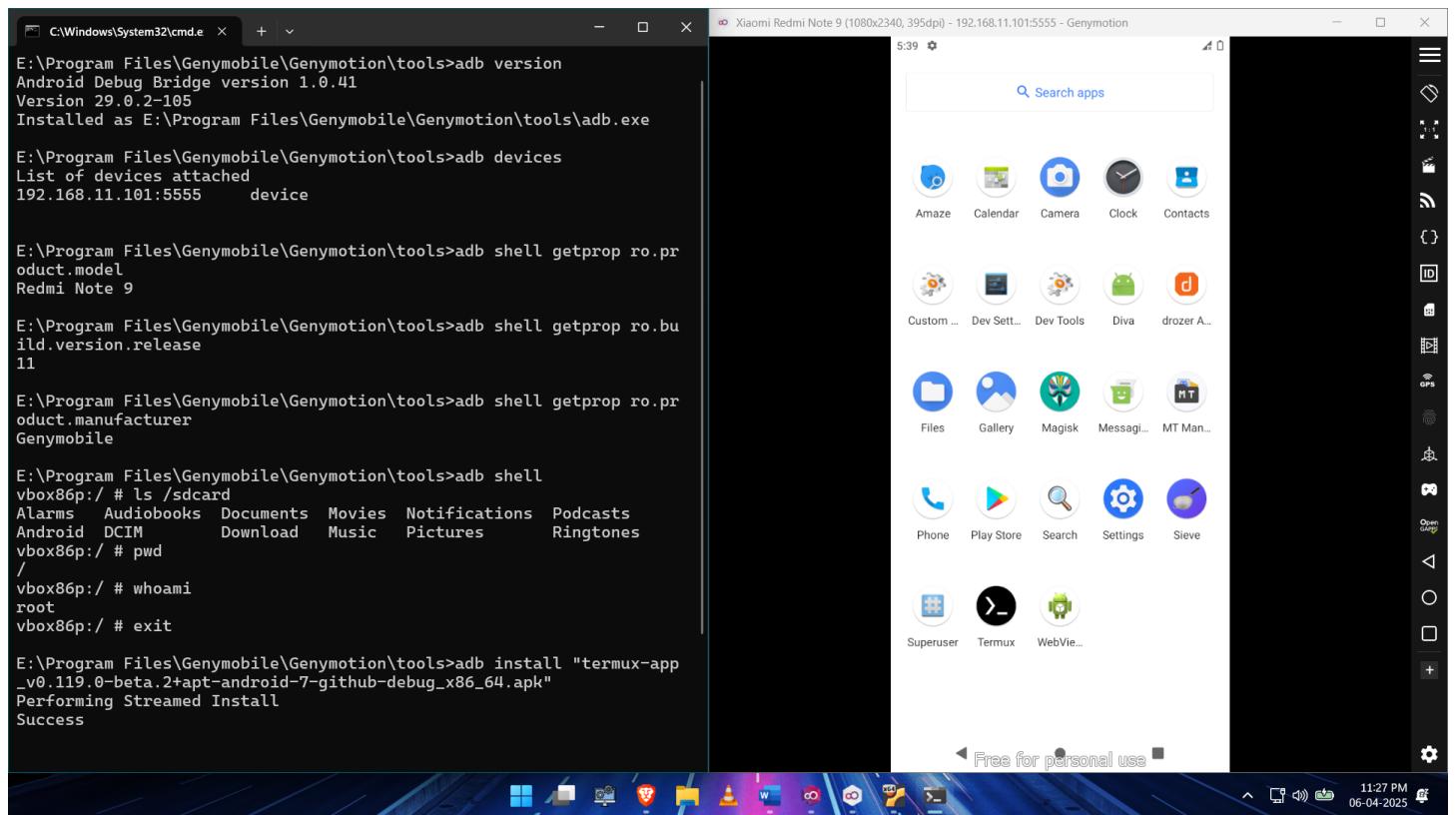
santoku@santoku-VirtualBox:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.7 LTS
Release:        16.04
Codename:       xenial
santoku@santoku-VirtualBox:~$
```



## [9]. Configuration of Genymotion



## [10].Demonstration of ADB commands



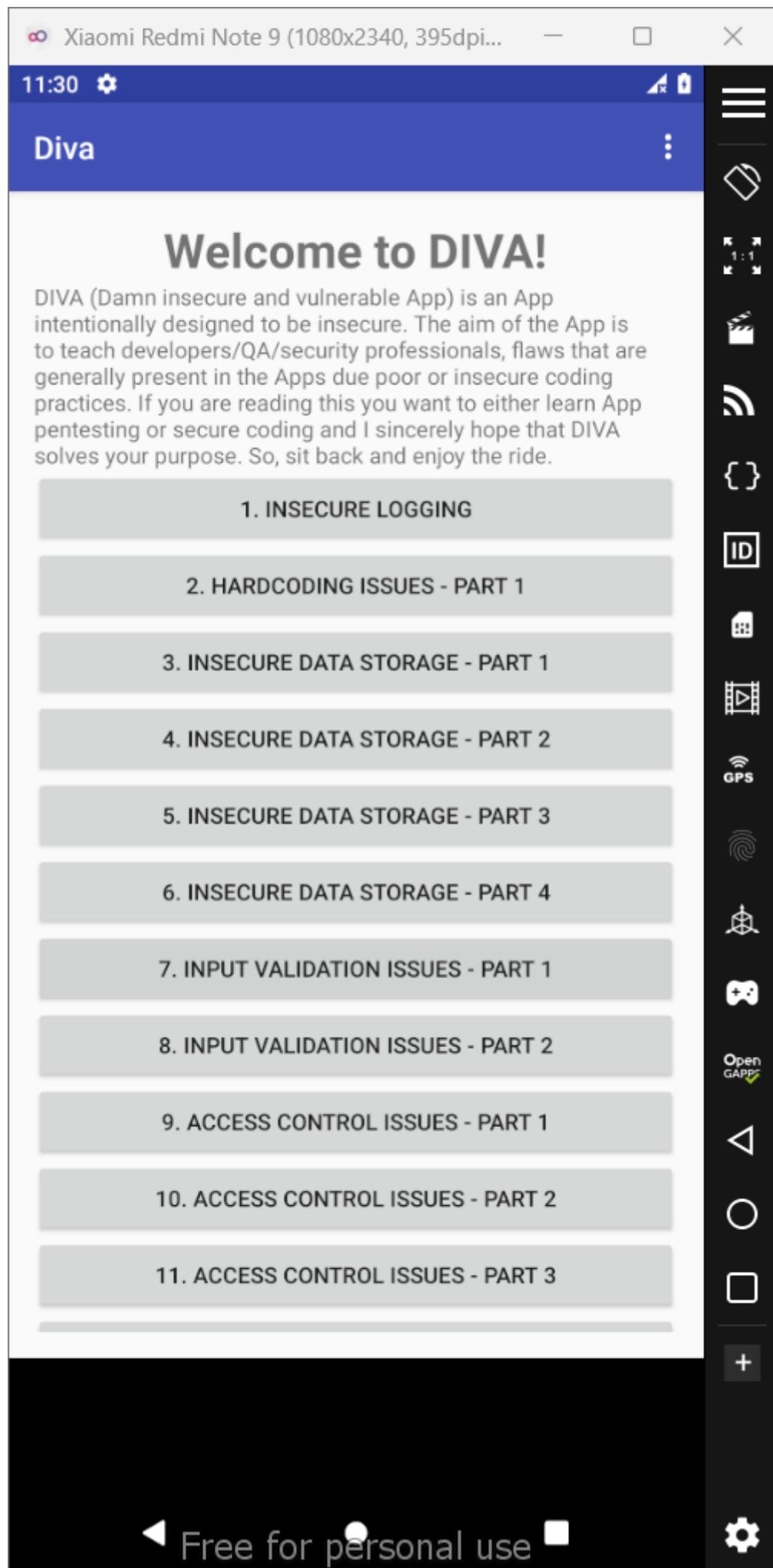
```
E:\Program Files\Genymobile\Genymotion\tools>adb shell pm list packages
package:com.google.android.carriersetup
package:com.genymotion.settings
package:com.android.cts.priv.ctsshim
package:com.android.internal.display.cutout.emulation.corner
package:com.google.android.ext.services
package:com.example.android.livecubes
package:com.android.internal.display.cutout.emulation.double
package:com.android.providers.telephony
package:com.android.dynsystem
package:com.android.theme.color.amethyst
package:com.android.theme.icon.pebble
package:com.android.providers.calendar
package:com.android.providers.media
package:com.google.android.onetimeinitializer
package:com.google.android.ext.shared
package:com.android.internal.systemui.navbar.gestural_wide_back
package:com.android.theme.color.sand
package:com.android.wallpapercropper
package:com.android.theme.icon.vessel
package:com.android.theme.color.cinnamon
package:com.android.theme.icon_pack.victor.settings
package:com.android.theme.icon_pack.rounded.systemui
package:com.android.theme.icon.taperedrect
package:com.android.documentsui
package:com.android.externalstorage
package:com.android.htmlviewer
package:com.android.companiondevicemanager
package:com.android.quicksearchbox
package:com.android.mms.service
package:com.android.providers.downloads
package:com.android.messaging
package:com.android.theme.icon_pack.rounded.android
package:com.android.theme.icon_pack.victor.systemui
package:com.android.theme.icon_pack.circular.themepicker
package:com.google.android.configupdater
package:com.android.theme.color.tangerine
package:com.android.providers.downloads.ui
package:com.android.vending
package:com.android.pacprocessor
```

## [11]. Demonstration of Android Boot Process using ADB

```
C:\Windows\System32\cmd.exe + x
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.gltrransport]: [pipe]
[ro.boot.hardware.vulkan]: [ranchu]
[ro.boot.logcat]: [*:V]
[ro.boot.opengles.version]: [196609]
[ro.boot.qemu]: [1]
[ro.boot.qemu.adb.pubkey]: [QAAAKWWhF6HT94cQpwUPYONCBiX7VAiTrZlVNlmpH7pRSN0n7oRm7A6i+aCJkM0epoDtIVa7uE3/Z1KfHiaQK1GeGdM4lgXd1fHHjTr3zNat0XehqNEM
LVWEFFbLrVvytPbVlyfGEBDv6APw2EbdlWaTuNNNk3Zxtjr891XBGTfp+TMuBIXtKWGhgeL7aceURPh06+ibHoKGulcHeCZ9s2700SxUVJGyT/uiT7yFhwNpeYzp6/Hq5q3AOOEQGGkl0
QbtFBx9tVAx1iSPCIrzNzXh381vB4JXhUkvjIavVu/8ARE1JVFYlb2wnbKFZBZunynsExfG5lm0iw/bkJohQXWVrgHRRhYsvEuHlZuwlBqi5vNzsxE3Skd09MdJtfhjYubURLhVc6pVRjb
S1gOlJ7+nsF3tW3Kh7nMRXwJwNln/uLV5r/9+GaVUBSJHFjiKobuIwh88+NrmZwgrQrioaYeFWW4aGzaJ2sdQ35AegVH2j3Wkjeb/8/YukdpWeYL3gAjawfs3IKQqc/8zaeue6YKcwuw6BXR
m2Ywnkk0InLdMICXy8TYhpN/Ikjy5Vgbk0PpNo1JNpRu/SqoL0BgrBpzaDRC05kmZSGyum67NXNHCROxbuLor548Vs08VA2VuwMSL28+Zyq+uBNcXm/cKBNJur8AYFttuZq+hS97LVLZSQR
MgEAAQA= @unknown]
[ro.boot.qemu.avd_name]: [Medium_Phone_API_35]
```

```
C:\Windows\System32\cmd.exe + x
qLOBgrBpZaDRC05kmZSGyum67NXNHCROxbuLor548Vs08VA2VuwMSL28+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.hwcdecoder.avcdec]: [2]
[ro.boot.qemu.hwcdecoder.hevdec]: [2]
[ro.boot.qemu.hwcdecoder.vpxdec]: [2]
[ro.boot.qemu.settings.system.screen_off_timeout]: [2147483647]
[ro.boot.qemu.virtiowifi]: [1]
[ro.boot.qemu.vsynccl]: [60]
[ro.boot.serialno]: [EMULATOR35X3X11X0]
[ro.boot.vbmeta.digest]: [9b597927025d4f62f4594a14632a8d3763239f29c0b7af229e0b6ebcdccdea60]
[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
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.all@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:~$
```

20:15

```
santoku@santoku [Running] - Oracle VirtualBox
File Machine View Input Devices Help
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$
```

20:17

```
santoku@santoku [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Edit Search Options Help
AndroidManifest.xml
<?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/api2_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/api2_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/notes" android:name="jakhar.aseem.diva.AccessControlNotesActivity"/>
<activity android:label="@string/d13" android:name="jakhar.aseem.diva.InputValidation3Activity"/>
</application>
</manifest>
```

20:21

```
santoku@santoku [Running] - Oracle VirtualBox
File Machine View Input Devices Help
MainActivity.smali
File Edit Search Options Help
MainActivity.smali
.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()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
```

20:23

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

```
santoku@santoku-VirtualBox:~$ unzip diva-beta.apk -d diva_apk_unzipped
Archive: diva-beta.apk
inflating: diva_apk_unzipped/AndroidManifest.xml
inflating: diva_apk_unzipped/classes.dex
inflating: diva_apk_unzipped/lib/arm64-v8a/libdivajni.so
inflating: diva_apk_unzipped/lib/armeabi-v7a/libdivajni.so
inflating: diva_apk_unzipped/lib/armeabi/libdivajni.so
inflating: diva_apk_unzipped/lib/mips/libdivajni.so
inflating: diva_apk_unzipped/lib/mips64/libdivajni.so
inflating: diva_apk_unzipped/lib/x86/libdivajni.so
inflating: diva_apk_unzipped/lib/x86_64/libdivajni.so
inflating: diva_apk_unzipped/res/anim/abc_fade_in.xml
inflating: diva_apk_unzipped/res/anim/abc_fade_out.xml
inflating: diva_apk_unzipped/res/anim/abc_grow_fade_in_from_bottom.xml
inflating: diva_apk_unzipped/res/anim/abc_popup_enter.xml
inflating: diva_apk_unzipped/res/anim/abc_popup_exit.xml
inflating: diva_apk_unzipped/res/anim/abc_shrink_fade_out_from_bottom.xml
inflating: diva_apk_unzipped/res/anim/abc_slide_in_bottom.xml
inflating: diva_apk_unzipped/res/anim/abc_slide_in_top.xml
inflating: diva_apk_unzipped/res/anim/abc_slide_out_bottom.xml
inflating: diva_apk_unzipped/res/anim/abc_slide_out_top.xml
inflating: diva_apk_unzipped/res/anim/design_fab_in.xml
inflating: diva_apk_unzipped/res/anim/design_fab_out.xml
inflating: diva_apk_unzipped/res/anim/design_snackbar_in.xml
inflating: diva_apk_unzipped/res/anim/design_snackbar_out.xml
inflating: diva_apk_unzipped/res/color-v11/abc_background_cache_hint_selector_material_dark.xml
inflating: diva_apk_unzipped/res/color-v11/abc_background_cache_hint_selector_material_light.xml
inflating: diva_apk_unzipped/res/color-v23/abc_color_highlight_material.xml
inflating: diva_apk_unzipped/res/color/abc_background_cache_hint_selector_material_dark.xml
inflating: diva_apk_unzipped/res/color/abc_background_cache_hint_selector_material_light.xml
```

```
santoku@santoku-VirtualBox:~/diva_apk_unzipped
```

Address	Hex	Dec	Description
00000000	50 4b 03 04 14 00 08 08 08 00 c6 68 41 49 00 00	PK.....hAI..	
00000010	00 00 00 00 00 00 00 00 00 00 13 00 00 41 6e	.....An	
00000020	64 72 6f 69 64 4d 61 6e 69 66 65 73 74 2e 78 6d	droidManifest.xm	
00000030	6c b5 58 4b 6f 5b 45 18 fd 1c 3b 8e f3 aa 9d 34	l.XKo[E...;....4	
00000040	69 de ef 97 f3 ba 49 9c 34 4d 53 16 b8 49 4a 22	i....I.4MS..IJ"	
00000050	42 09 09 84 ee 5a 93 17 69 5e 56 ec 94 c7 86 0a	B....Z..i^V....	
00000060	10 42 fc 02 84 2a 04 05 0b 76 54 08 21 c4 8a 35	.B....*....vT!.5	
00000070	42 88 5f c0 8a 05 e2 07 b0 85 33 9f 67 ec 2f e3	B.....3.g./.	
00000080	6b b8 b7 6d ae 75 3c d7 67 66 ce f9 e6 9b c7 bd	k..m.u<.gf.....	
00000090	49 90 22 f4 b8 85 28 40 ed f4 75 0d 0b 54 b8	I."....(@..u..T.	
000000a0	6a 02 85 fb 56 60 06 58 07 1e 00 1f 02 8f 80 ef	j....V..X.....	
000000b0	80 9f 80 5f 81 3f 81 bf 81 18 fa f5 02 b3 c0 32	....?.....2	
000000c0	f0 18 f8 0a f8 1e f8 0b e8 2c 23 4a 00 77 80 7b	.....,#J.w.{	
000000d0	c0 fb c0 c7 c0 e7 c0 8f 40 2c 48 b4 0d 7c 09 fc	.....@,H. ..	
000000e0	00 fc 02 d4 84 88 46 80 79 e0 14 f8 04 f8 19 88	.....F.y.....	
000000f0	94 13 ad 01 f4 80 58 98 28 0d fc 06 74 57 10 7d	.....O.X(...,tw.)	
00000100	06 fc 0e 0c 46 c0 03 df 02 e1 4a b4 07 1e 01 4f	....F.....J....0	
00000110	80 50 15 d1 2d e0 0b e0 0f e0 66 35 51 35 46 b8	P.....f5Q5F.	
00000120	43 a7 94 a1 7d 3a a1 63 5a c0 f7 36 98 e2 9a db	C...):.cZ..6....	
00000130	94 a2 23 ae a9 45 b9 0f 66 03 2d 0f 68 f3 5c 2b	.#..E..f.-.h.\+	
00000140	44 46 59 b4 3c a5 3d f0 d9 12 6d 42 f8 36 6a d5	DFY.<.=.mB.6j.	
00000150	b8 3b c4 7f 84 de a1 9b b8 df 42 fb 33 4a a3 a6	.....,B.3j..	
00000160	8a 23 79 0b bf f6 0f 49 e1 ee 90 7b 84 a0 b3 a5	#y....I...{....	
00000170	95 ca c1 a9 9a 1d 94 4a 2b c3 7d d3 a8 3d 85 7b	.....J+.}..={.	
00000180	06 73 98 e5 9a 72 94 6f a3 55 c1 f3 8c 19 d5 6e	s....r.o.U.....n	
00000190	1f 77 fb e0 33 a8 a9 40 79 9c f7 da 06 13 41 f9	.w..3..@y.....A.	
000001a0	6e 5e 31 c7 55 a0 c5 31 ee 4e c1 ee 33 33 02 ad	n^1.U..1.N..33..	
000001b0	2c 3e 69 9a a7 09 7c 32 88 30 e7 97 c2 bd 63 b5	,>i... 2.0....c..	
000001c0	77 38 fe 23 b4 4b a1 c7 01 ca 53 f6 9f 28 d2 25	w8.#.K....S..(.%	
000001d0	76 4b eb bc a4 38 ab 44 cd 60 d4 b8 b3 b4 cb 71	vk...8.D.....q	
000001e0	1d 21 73 67 e8 71 88 3e 9b 25 e6 d3 7b 9f c2 4c	.!sg.q.>.%{..L	
000001f0	47 38 fe 63 f0 bb 1c 5f 16 5c 1d dd 07 77 80 d1	G8.c....\....w..	

```
santoku@santoku-VirtualBox:~/diva_apk_unzipped$ hexdump -C ./diva-beta.apk | less
santoku@santoku-VirtualBox:~/diva_apk_unzipped$ hexdump -C classes.dex | head -n 20
00000000 64 65 78 0a 30 33 35 00 d5 5a 2b e3 ae 00 25 15 |dex.035..Z+....%
00000010 18 a2 7d aa 97 ce 1e d7 7f ad b0 77 97 f3 f2 90 |.....W.....
00000020 50 78 21 00 70 00 00 00 78 56 34 12 00 00 00 00 |Px!.p...xV4.....
00000030 00 00 00 00 74 77 21 00 ca 4d 00 00 70 00 00 00 |....tw!..M..p...
00000040 6e 09 00 00 98 37 01 00 bf 0d 00 00 50 5d 01 00 |n....7.....P]...
00000050 d6 26 00 04 44 02 02 00 4b 4b 00 00 f4 38 03 00 |&..D...KK..8..
00000060 ff 06 00 00 4c 93 05 00 24 05 1b 00 2c 73 06 00 |....L...$.s...
00000070 2c 73 06 00 2e 73 06 00 31 73 06 00 34 73 06 00 ,s...s..ls..4s..
00000080 38 73 06 00 3d 73 06 00 43 73 06 00 48 73 06 00 |8s..=.Cs..Hs..
00000090 57 73 06 00 6e 73 06 00 a1 73 06 00 c9 73 06 00 |Ws..ns...s...s..
000000a0 d9 73 06 00 fc 73 06 00 16 74 06 00 33 74 06 00 |.s...s..t..3t..
000000b0 54 74 06 00 6c 74 06 00 93 74 06 00 bb 74 06 00 |Tt..lt...t...
000000c0 e2 74 06 00 0a 75 06 00 2b 75 06 00 33 75 06 00 |.t..u..u..3u..
000000d0 50 75 06 00 73 75 06 00 90 75 06 00 9e 75 06 00 |Pu..su..u...u..
000000e0 ad 75 06 00 bb 75 06 00 c9 75 06 00 ea 75 06 00 |.u...u...u...u..
000000f0 fd 75 06 00 0b 76 06 00 1a 76 06 00 28 76 06 00 |.u...v...v...(v..
00000100 3b 76 06 00 45 76 06 00 5c 76 06 00 74 76 06 00 ;v..Ev..\v..tv..
00000110 8f 76 06 00 9b 76 06 00 aa 76 06 00 b6 76 06 00 |.v...v...v...v...
00000120 c9 76 06 00 df 76 06 00 f5 76 06 00 0c 77 06 00 |.v...v...v...w..
00000130 17 77 06 00 2d 77 06 00 31 77 06 00 35 77 06 00 |.w...-w..1w..5w..|
```

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@... 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:[L
android/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

```
santoku@santoku-VM:~$ unzip diva-beta.apk -d extracted
Archive: diva-beta.apk
inflating: extracted/AndroidManifest.xml
inflating: extracted/classes.dex
inflating: extracted/lib/arm64-v8a/libdivajni.so
inflating: extracted/lib/armeabi-v7a/libdivajni.so
inflating: extracted/lib/armeabi/libdivajni.so
inflating: extracted/lib/mips/libdivajni.so
inflating: extracted/lib/mips64/libdivajni.so
inflating: extracted/lib/x86/libdivajni.so
inflating: extracted/lib/x64/libdivajni.so
inflating: extracted/res/anim/abc_fade_in.xml
inflating: extracted/res/anim/abc_fade_out.xml
inflating: extracted/res/anim/abc_grow_fade_in_from_bottom.xml
inflating: extracted/res/anim/abc_popup_enter.xml
inflating: extracted/res/anim/abc_popup_exit.xml
inflating: extracted/res/anim/abc_shrink_fade_out_from_bottom.xml
inflating: extracted/res/anim/abc_slide_in_top.xml
inflating: extracted/res/anim/abc_slide_out_top.xml
inflating: extracted/res/anim/design_fab_in.xml
inflating: extracted/res/anim/design_fab_out.xml
inflating: extracted/res/color/abc_color_material_dark.xml
inflating: extracted/res/color/abc_color_material_light.xml
inflating: extracted/res/color/abc_primary_text_disable_only_material_dark.xml
inflating: extracted/res/color/abc_primary_text_disable_only_material_light.xml
inflating: extracted/res/color/abc_primary_text_material_dark.xml
inflating: extracted/res/color/abc_primary_text_material_light.xml
inflating: extracted/res/color/abc_search_url_text.xml
inflating: extracted/res/color/abc_secondary_text_material_dark.xml
inflating: extracted/res/color/color_material_dark.xml
inflating: extracted/res/color/color_material_light.xml
extracting: extracted/res/drawable-hdpi-v4/abc_ab_share_pack_mtrl_alpha.9.png
extracting: extracted/res/drawable-hdpi-v4/abc_btn_check_on_mtrl_000.png
extracting: extracted/res/drawable-hdpi-v4/abc_btn_radio_to_on_mtrl_001.png
extracting: extracted/res/drawable-hdpi-v4/abc_btn_radio_to_on_mtrl_000.png
extracting: extracted/res/drawable-hdpi-v4/abc_btn_radio_to_on_mtrl_015.png
santoku@santoku-VM:~$
```

```
santoku@santoku-VM:~$ cd extracted
santoku@santoku-VM:~/extracted$ ./dex2jar.sh
dex2jar: converted classes.dex to diva-dex2jar.jar
santoku@santoku-VM:~/extracted$ jd-gui diva-dex2jar.jar
JD-GUI 1.6.1
Java Decompiler - R.class
File Edit Tabs Help
santoku@santoku-VM:~/extracted$
```

```
santoku@santoku-VM:~/extracted$ jd-gui diva-dex2jar.jar
JD-GUI 1.6.1
Java Decompiler - R.class
File Edit Navigate Search Help
File Machine View Input Devices Help
Java Decompiler - R.class
diva-dex2jar.jar [R.class]
android.support
  annotation
  design
    BuildConfig
    R
    anim
    attr
    bool
    color
    dimen
    drawables
    id
    integer
    layout
    string
    style
    styleable
  v4
  internal.view
  view
    NestedScrollingChild
    ScrollView
  v7
    internal.view.menu
    MenuBuilder
    MenuPresenter
    MenuItemView
  widget
    LinearLayoutCompat
    RecyclerView$ViewHolder
  R.java [BuildConfig.class, VisibleForTesting.class, NestedScrollingChild.class, AnimRes.class, AnimatorRes.class, BoolRes.class, DimenRes.class, FractionRes.class, LinearLayoutCompat.class, RecyclerViewChild.class]
  package android.support.design;
  public final class R {
    public static final class anim {
      public static final int abc_fade_in = 2131034112;
      public static final int abc_fade_out = 2131034113;
      public static final int abc_grow_fade_in_from_bottom = 2131034114;
      public static final int abc_popup_enter = 2131034115;
      public static final int abc_popup_exit = 2131034116;
      public static final int abc_shrink_fade_out_from_bottom = 2131034117;
      public static final int abc_slide_in_bottom = 2131034118;
      public static final int abc_slide_in_top = 2131034119;
      public static final int abc_slide_out_bottom = 2131034120;
      public static final int abc_slide_out_top = 2131034121;
      public static final int design_fab_in = 2131034122;
      public static final int design_fab_out = 2131034123;
      public static final int design_snackbar_in = 2131034124;
      public static final int design_snackbar_out = 2131034125;
    }
    public static final class attr {
      public static final int actionBarDivider = 2130772113;
      public static final int actionBarItemBackground = 2130772134;
      public static final int actionBarPopupTheme = 2130772127;
      public static final int actionBarSize = 2130772123;
      public static final int actionBarStyle = 2130772129;
      public static final int actionBarTabBarStyle = 2130772128;
      public static final int actionBarTabStyle = 2130772123;
      public static final int actionBarTabTextStyle = 2130772124;
      public static final int actionBarTheme = 2130772130;
      public static final int actionBarWidgetTheme = 2130772131;
      public static final int actionBarStyle = 2130772159;
      public static final int actionBarDropDownStyle = 2130772155;
      public static final int actionLayout = 2130772249;
      public static final int actionMenuItemTextColor = 2130772135;
      public static final int actionModeBackground = 2130772136;
      public static final int actionModeCloseButtonStyle = 2130772138;
      public static final int actionModeCloseDrawable = 2130772141;
    }
  }
santoku@santoku-VM:~/extracted$
```

## [16].Request interception using BurpSuit

Santoku (Santoku) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

santoku@santoku-VM: ~

```
File Edit Tabs Help
santoku@santoku-VM:~$ ifconfig
eth0    Link encap:Ethernet HWaddr 00:00:27:ff:fd:00
        inet brd 192.168.20.255 Mask:255.255.255.0
              inet6 addr: fe80::200:ff:ff:fd%eth0 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:1211 errors:0 dropped:0 overruns:0 frame:0
        TX packets:734 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:801043 (801.0 KB)  TX bytes:101776 (101.7 KB)

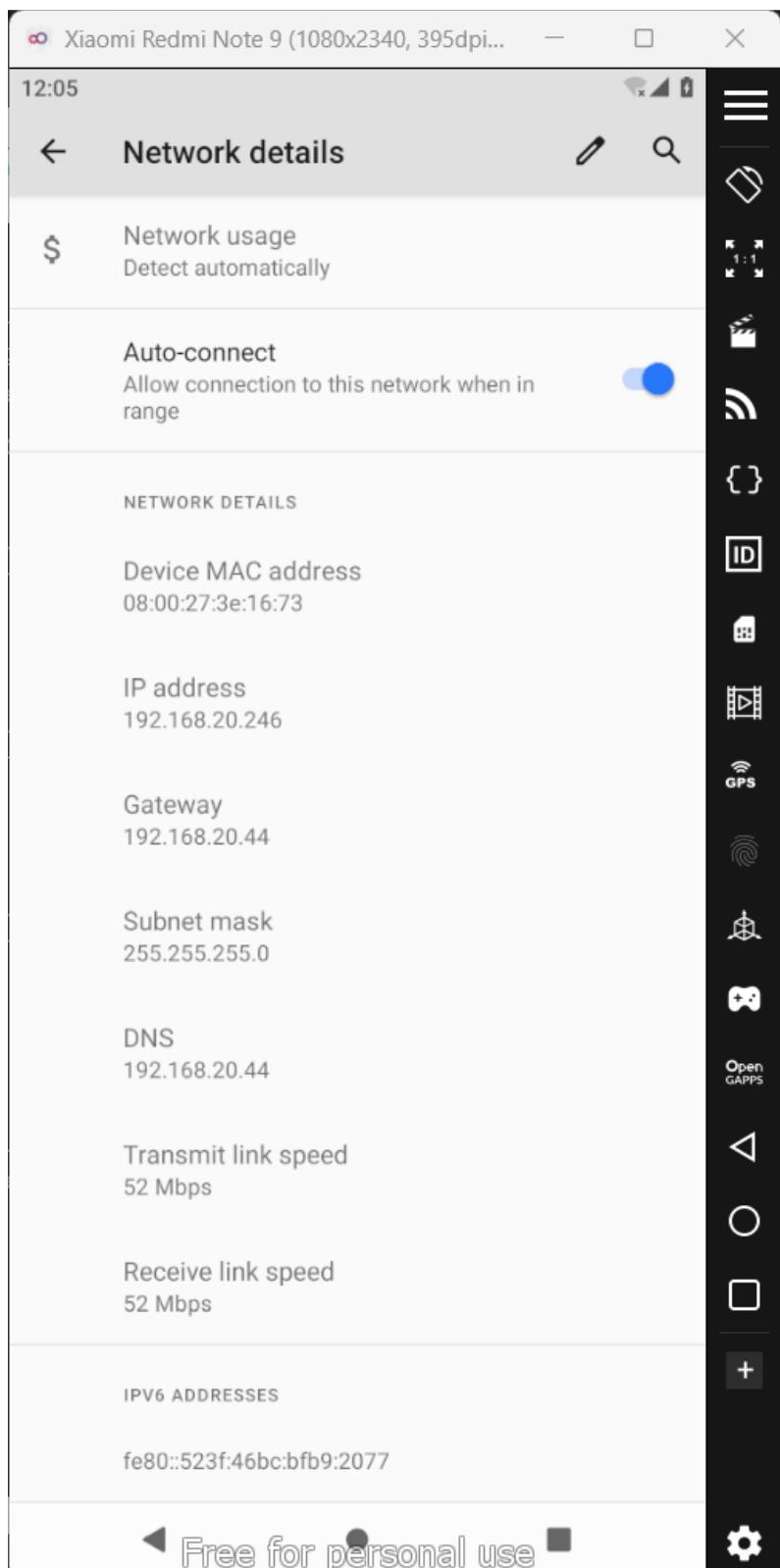
eth1    Link encap:Ethernet HWaddr 00:00:27:b1:e6:46
        UP BROADCAST MULTICAST MTU:1500 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth2    Link encap:Ethernet HWaddr 00:00:27:a3:c1:d4
        UP BROADCAST MULTICAST MTU:1500 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth3    Link encap:Ethernet HWaddr 00:00:27:a3:c1:d0
        UP BROADCAST MULTICAST MTU:1500 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo     Link encap:Local Loopback
        inet brd 127.0.0.1 Mask:255.0.0.0
              inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING MTU:65536 Metric:1
        RX packets:486 errors:0 dropped:0 overruns:0 frame:0
        TX packets:486 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:41156 (41.1 KB)  TX bytes:41156 (41.1 KB)

santoku@santoku-VM:~$
```



- [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)

The screenshot shows the Docker Desktop interface. On the left sidebar, 'Containers' is selected. In the main area, a table lists a single running container:

Name	Container ID	Image	Port(s)	CPU (%)	Last started	Actions
mystifying_beaver	3a1bb45c7d2	opensecurity/mobile-security-framework	8000:8000	1.48%	5 minutes ago	<span>Stop</span> <span>⋮</span> <span>Remove</span>

At the bottom, it says 'Showing 1 item'.

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

C:\Users\ROG>docker run -it --rm -p 8000:8000 opensecurity/mobile-security-framework-mobsf:latest
docker: error during connect: Head "http://<2F2F.%2Fpipe%2FdockerDesktopLinuxEngine/_ping": open //./pipe/dockerDesktopLinuxEngine: The system cannot find the file specified.

Run 'docker run --help' for more information

C:\Users\ROG>
C:\Users\ROG>docker run -it --rm -p 8000:8000 opensecurity/mobile-security-framework-mobsf:latest
[INFO] 12/Apr/2025 20:40:50 - Loading User config from: /home/mobsf/.MobSF/config.py
[INFO] 12/Apr/2025 20:40:50 - JADX is already installed at /home/mobsf/.MobSF/tools/jadx/jadx-1.5.0
[INFO] 12/Apr/2025 20:40:52 -
[INFO] 12/Apr/2025 20:40:52 - 
[INFO] 12/Apr/2025 20:40:52 - Author: Ajin Abraham | opensecurity.in
[INFO] 12/Apr/2025 20:40:52 - Mobile Security Framework v4.3.2
REST API Key: 98cd06325bcd1b1d0c75be7b22f18021368582f8ae24b4e36e892f486032bdb5
Default Credentials: mobsf/mobsf
[INFO] 12/Apr/2025 20:40:52 - OS Environment: Linux (debian 12 bookworm) Linux-5.15.167.4-microsoft-standard-WSL2-x86_64-with-glibc2.36
[INFO] 12/Apr/2025 20:40:52 - CPU Cores: 8, Threads: 16, RAM: 7.39 GB
[INFO] 12/Apr/2025 20:40:52 - MobSF Basic Environment Check
[INFO] 12/Apr/2025 20:40:53 - Checking for Update.
No changes detected
[INFO] 12/Apr/2025 20:40:53 - No updates available.
[INFO] 12/Apr/2025 20:40:54 - Loading User config from: /home/mobsf/.MobSF/config.py
[INFO] 12/Apr/2025 20:40:56 -
[INFO] 12/Apr/2025 20:40:56 - 
[INFO] 12/Apr/2025 20:40:56 - Author: Ajin Abraham | opensecurity.in
[INFO] 12/Apr/2025 20:40:56 - Mobile Security Framework v4.3.2
REST API Key: 98cd06325bcd1b1d0c75be7b22f18021368582f8ae24b4e36e892f486032bdb5
```

The screenshot shows a web browser with the URL <http://localhost:8000/login/?next=/>. The page displays a 'Sign in to access' message above a login form. The form has fields for 'mobsf' (username) and '.....' (password), and a 'Sign In' button.

At the bottom, it says '© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.' and 'Version 4.3.2'.

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

The screenshot shows the MobSF Static Analysis interface. At the top, there's a navigation bar with tabs like Firewall Authentication, Mobile Security Syllabus, MSF\_Practical\_List.pdf, MSF TA2 Assignment, santoku@santoku-V, Static Analysis, Mobile Security, and MobSF Dynamic Analysis. Below the navigation bar is a header with 'SCANS DYNAMIC ANALYZER' and the MobSF logo. A central 'Upload & Analyze' button with a cloud icon is prominently displayed. Below it is a placeholder text 'Drag & Drop anywhere!'. Further down are sections for 'Download & Scan Package' and 'RECENT SCANS | DYNAMIC ANALYZER | API | DONATE | DOCS | ABOUT'. At the bottom, a copyright notice reads '© 2025 Mobile Security Framework - MobSF v4.3.2'.

This screenshot displays the static analysis results for the APK file 'diva-beta.apk'. The left sidebar shows the 'Static Analyzer' menu with various options like Information, Scan Options, Signer Certificate, Permissions, Android API, and Components. The main area is titled 'APP SCORES' and shows a security score of 36/100. It also lists 'Trackers Detection' at 0/432. Other sections include 'FILE INFORMATION' (File Name: diva-beta.apk, Size: 1.43MB, MD5: 82ab8b2193b3cfb1c737e3a786be363a, SHA1: 27e849d97b86a3a3357fb3e980433a91d416801, SHA256: 5cef51fce9bd760b92ab2340477fdda84b4ae05d0a8c9493e4fe34fab7c5), 'APP INFORMATION' (App Name: Diva, Package Name: jakhar.aseem.diva, Main Activity: jakhar.aseem.diva.MainActivity, Target SDK: 23, Min SDK: 15, Max SDK: 15, Android Version Name: 1.0, Android Version Code: 1), and four summary boxes: 'EXPORTED ACTIVITIES' (2/17), 'EXPORTED SERVICES' (0/0), 'EXPORTED RECEIVERS' (0/0), and 'EXPORTED PROVIDERS' (1/1). Below these are sections for 'SCAN OPTIONS' (Rescan, Manage Suppressions, Start Dynamic Analysis, Scan Logs) and 'DECOMPILED CODE' (View AndroidManifest.xml, View Source, View Small, Download Java Code, Download Smali Code, Download APK).

This screenshot shows the 'APPLICATION PERMISSIONS' section of the static analysis results. The left sidebar highlights the 'Permissions' option. The main table lists three permissions: android.permission.INTERNET (status: normal, info: full Internet access, description: Allows an application to create network sockets.), android.permission.READ\_EXTERNAL\_STORAGE (status: dangerous, info: read external storage contents, description: Allows an application to read from external storage.), and android.permission.WRITE\_EXTERNAL\_STORAGE (status: dangerous, info: read/modify/delete external storage contents, description: Allows an application to write to external storage.). Below the table, there are sections for 'ANDROID API' (Content Provider, Inter Process Communication, Loading Native Code (Shared Library), Local File I/O Operations) and 'Manifest Analysis'.

This screenshot displays the 'MANIFEST ANALYSIS' section. The left sidebar highlights 'Manifest Analysis'. The main table shows six issues: 1. App can be installed on a vulnerable uppatched Android version (Android 4.0.3-4.0.4, [minSdk=15]) with severity high. 2. Debug Enabled For App ([android:debuggable=true]) with severity high. 3. Application Data can Be backed up ([android:allowBackup=true]) with severity warning. 4. Activity (jakhar.aseem.diva.APIcredsActivity) is not Protected. An intent-filter exists. with severity warning. 5. Activity (jakhar.aseem.diva.APIcreds2Activity) is not Protected. An intent-filter exists. with severity warning. 6. Content Provider (jakhar.aseem.diva.NotesProvider) is not Protected. [android:exported=true] with severity warning. The table includes columns for NO, ISSUE, SEVERITY, DESCRIPTION, and OPTIONS.

This screenshot shows the 'MobSF Application Security Scorecard' for the app 'Diva 1.0'. The top section displays a summary: Security Score 36/100, Risk Rating (High risk, Grade C), Severity Distribution (High: 2%, Medium: 78%, Info: 20%, Secure: 0%), and Privacy Risk (User/Device Trackers: 0). Below this are sections for 'Findings' (High: 5, Medium: 7, Info: 1, Secure: 1, Hotspot: 1) and two certificate sections: 'Application vulnerable to Janus Vulnerability' and 'Application signed with debug certificate', both with a 'CERTIFICATE' link.

## [40]. Configuration of Frida

```
(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!)
frida-server &
:/ #
```

```
(frida+mobsf) E:\Santoku\frida\frida+mobsf>frida-ps -U
PID Name
-----
2334 Google Play Store
1686 Phone
1670 adb
1227 android.ext.services
236 android.hardware.atatrace@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
366 android.hardware.gatekeeper@1.0-service.software
362 android.hardware.gnss@1.0-service
363 android.hardware.graphicsallocator@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.hidlallocator@1.0-service
1734 android.process.acore
2586 android.process.media
233 android.system.suspend@1.0-service
888 audioserver
```

```
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>
```

```
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

```
C:\Windows\System32\cmd.exe + - 

(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 ]-> Java.perform(function () {
    Java.enumerateLoadedClasses({
        onMatch: function (className) {
            if (className.startsWith("jakhar.aseem.diva")) {
                console.log("[CLASS]", className);
            }
        },
        onComplete: function () {
            console.log("Done listing all DIVA classes");
        }
    });
});
[CLASS] jakhar.aseem.diva.NotesProvider$DBHelper
[CLASS] jakhar.aseem.diva.MainActivity
[CLASS] jakhar.aseem.diva.NotesProvider
Done listing all DIVA classes
[Redmi Note 9::Diva ]-> |
```

```
C:\Windows\System32\cmd.exe + - 

[Redmi Note 9::Diva ]-> Java.perform(function () {
    var clazz = Java.use("jakhar.aseem.diva.NotesProvider");
    console.log("Methods in NotesProvider:");
    clazz.class.getDeclaredMethods().forEach(function (m) {
        console.log("  " + m.toString());
    });
});
Methods in NotesProvider:
→ public int jakhar.aseem.diva.NotesProvider.delete(android.net.Uri,java.lang.String,java.lang.String[])
→ public java.lang.String jakhar.aseem.diva.NotesProvider.getType(android.net.Uri)
→ public android.net.Uri jakhar.aseem.diva.NotesProvider.insert(android.net.Uri,android.content.ContentValues)
→ public boolean jakhar.aseem.diva.NotesProvider.onCreate()
→ public android.database.Cursor jakhar.aseem.diva.NotesProvider.query(android.net.Uri,java.lang.String[],java.lang.String[],java.lang.String[])
→ public int jakhar.aseem.diva.NotesProvider.update(android.net.Uri,android.content.ContentValues,java.lang.String,java.lang.String[])
[Redmi Note 9::Diva ]-> Java.perform(function () {
    var clazz = Java.use("jakhar.aseem.diva.MainActivity");
    console.log("Fields in MainActivity:");
    clazz.class.getDeclaredFields().forEach(function (f) {
        console.log("  " + f.toString());
    });
});
Fields in MainActivity:
```

## [42].Dynamic Analysis using MobSF and Frida

MobSF Dynamic Analyzer Supports

- Genymotion Android VM version 4.1 - 11.0 (arm64, x86, and x86\_64 upto API 30)
- Android Emulator AVD (non production) version 5.0 - 11.0 (arm, arm64, x86, and x86\_64 upto API 30)
- Corelium Android VM (userdebug builds) version 7.1.2 - 11.0 (arm64 upto API 30)

Android version >= 9.0 recommended  
Detected Android Version: 11.0, SDK: API level 30

MobSF Dynamic Runtime

Android instance: 192.168.11.101:5555

RECENT SCANS STATIC ANALYZER DYNAMIC ANALYZER API DONATE DOCS ABOUT Search

### Apps in Device

APP	LOCATION IN DEVICE	ACTION
jakhar.aseem.diva	/data/app/~03CIWtpbuiZrb5RWnIEZQ==/jakhar.aseem.diva-1EzpjZKgShj4RwBBN05BhA==/base.apk	<button>Start Dynamic Analysis</button> <button>Pull &amp; Static Analysis</button> <button>View Report</button>

Showing 1 to 1 of 1 entries (filtered from 6 total entries)

Previous 1 Next

### Apps Available

Dynamic Analyzer - jakhar.aseem.diva

Show Screen Remove Root CA Unset HTTP(S) Proxy TLS/SSL Security Tester Get Dependencies Take a Screenshot Logcat Stream Generate Report

Dynamic Analyzer Errors

Setting up MobSF Dynamic Analysis environment...  
Running HTTP(S) interception proxy.  
Invoking MobSF agents.  
Environment is ready for Dynamic Analysis.  
Start Instrumentation or Run the application and navigate through the different flows or business logic manually.

Default Frida Scripts

API Monitoring SSL Pinning Bypass Root Detection Bypass Debugger Check Bypass Clipboard Monitor

Auxiliary Frida Scripts

Enumerate Loaded Classes Capture Strings Capture String Comparisons Enumerate Class methods

java.io.File  
Search Class Pattern  
ssl.Trust  
Trace Class Methods  
java.net.Socket,java.io.File,java.lang.String

Instrumentation

Spawn & Inject Inject Attach

User Interface

Activities

jakhar.aseem.diva.APIcreds# Start Activity

Frida Code Editor

```
Java.perform(function() {  
    // Use send() for logging  
});  
4
```

Available Scripts (Use CTRL to choose multiple) Load

app-environment audit-webview bypass-adb-detection bypass-emulator-detection bypass-react-native-emulator-detection crypto-aes-key crypto-dump-keystore crypto-keyguard-credential-intent crypto-trace-cipher crypto-trace-keygenparameterspec

### Shell Access

Sun Apr 13 2025 07:31:33 GMT+0530 (India Standard Time)  
Enter "help" for more information.  
[root@android] #

Xiaomi Redmi Note 9 (1080x2340, 395dp)... 2:06 Vendor API Credentials

API Key: 123secretapikey123  
API User name: diva  
API Password: p:password

Dynamic Analyzer RECENT SCANS STATIC ANALYZER DYNAMIC ANALYZER API DONATE DOCS ABOUT Search

Dynamic Analyzer Errors

Invoking MobSF agents.  
Environment is ready for Dynamic Analysis.  
Start Instrumentation or Run the application and navigate through the different flows or business logic manually.  
Starting Activity: jakhar.aseem.diva.APIcredsActivity  
Activity Started

Default Frida Scripts

API Monitoring SSL Pinning Bypass Root Detection Bypass Debugger Check Bypass Clipboard Monitor

Auxiliary Frida Scripts

Enumerate Loaded Classes Capture Strings Capture String Comparisons Enumerate Class methods

java.io.File  
Search Class Pattern  
ssl.Trust  
Trace Class Methods  
java.net.Socket,java.io.File,java.lang.String

Instrumentation

Spawn & Inject Inject Attach

User Interface

Activities

jakhar.aseem.diva.APIcreds# Start Activity

Frida Code Editor

```
1/ Based on https://github.com/sensepost/objection/blob/f8e78d8a29574cddd2b953a63207bd5a1901cf/bjection/hooks/android/filesystem/environment.js  
2 ar ActivityThread = Java.use('android.app.ActivityThread');  
3 ar Context = Java.use('android.content.Context');  
4 ar Data = {  
5     fileDescriptor: context.getFileDescriptor(),  
6     cacheDir: context.getCacheDir(),  
7     externalCacheDirectory:  
8         context.getExternalCacheDir(),  
9     absolutePath: context.getAbsolutePath(),  
10    absoluteDir: context.getAbsoluteDir(),  
11    packageCodePath: context.getPackageCodePath(),  
12    codeCacheDir: context.getCodeCacheDir(),  
13    onText: context.getText(),  
14    packageCodePathString: context.getPackageCodePath().toString(),  
15};  
16  
17 end(JSON.stringify(data, null, 2));  
18
```

Available Scripts (Use CTRL to choose multiple) Load

app-environment audit-webview bypass-adb-detection bypass-emulator-detection bypass-react-native-emulator-detection crypto-aes-key crypto-dump-keystore crypto-keyguard-credential-intent crypto-trace-cipher crypto-trace-keygenparameterspec

Xiaomi Redmi Note 9 (1080x2340, 395dp)... 2:06 Vendor API Credentials

API Key: 123secretapikey123  
API User name: diva  
API Password: p:password

### Shell Access

Sun Apr 13 2025 07:31:33 GMT+0530 (India Standard Time)  
Enter "help" for more information.  
[root@android] # help

activities services libraries echo push forward wait-for-device disconnect uninstall sideload reboot get-serialno enable-verity bugreport install-multi-package sync ppp  
exported\_activities receivers providers clear date help shell start-server connect reconnect usb install logat root tcpip unroot remount get-devpath get-state keygen disable-verity backup restore  
[root@android] # version  
Android Debug Bridge version 1.0.41  
Version 29.0.2-105  
Installed as E:\Program Files\Genymobile\Genymotion\tools\adb.exe  
[root@android] #

### Frida Logs

Data refreshed in every 3 seconds.

```
{  
    "filesDirectory": "/data/user/0/jakhar.aseem.diva/files",  
    "cacheDirectory": "/data/user/0/jakhar.aseem.diva/cache",  
    "externalCacheDirectory": "/storage/emulated/0/Android/data/jakhar.aseem.diva/cache",  
    "codeCacheDirectory": "/data/user/0/jakhar.aseem.diva/code_cache",  
    "obbDir": "/storage/emulated/0/Android/obb/jakhar.aseem.diva",  
    "packageCodePath": "/data/app/~03CIWtpbuiZrb5RWnIEZQ==/jakhar.aseem.diva-1EzpjZKgShj4RwBBN05BhA==/base.apk"  
}  
Loaded Frida Script - api_monitor  
Loaded Frida Script - debugger_check_bypass  
Loaded Frida Script - dump_clipboard  
Loaded Frida Script - root_bypass  
Loaded Frida Script - ssl_pinning_bypass  
[API Monitor] Cannot find com.android.okhttp.internal.http.HttpURLConnectionImpl.getInputStream
```

- [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