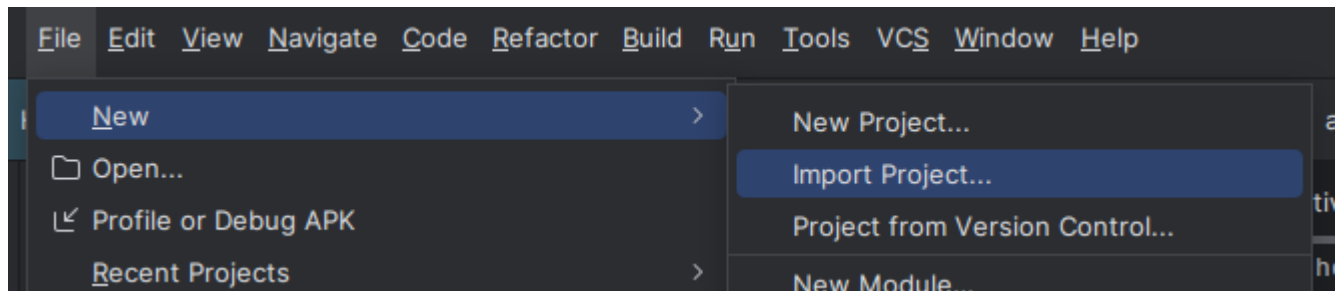


1-Your First Android App

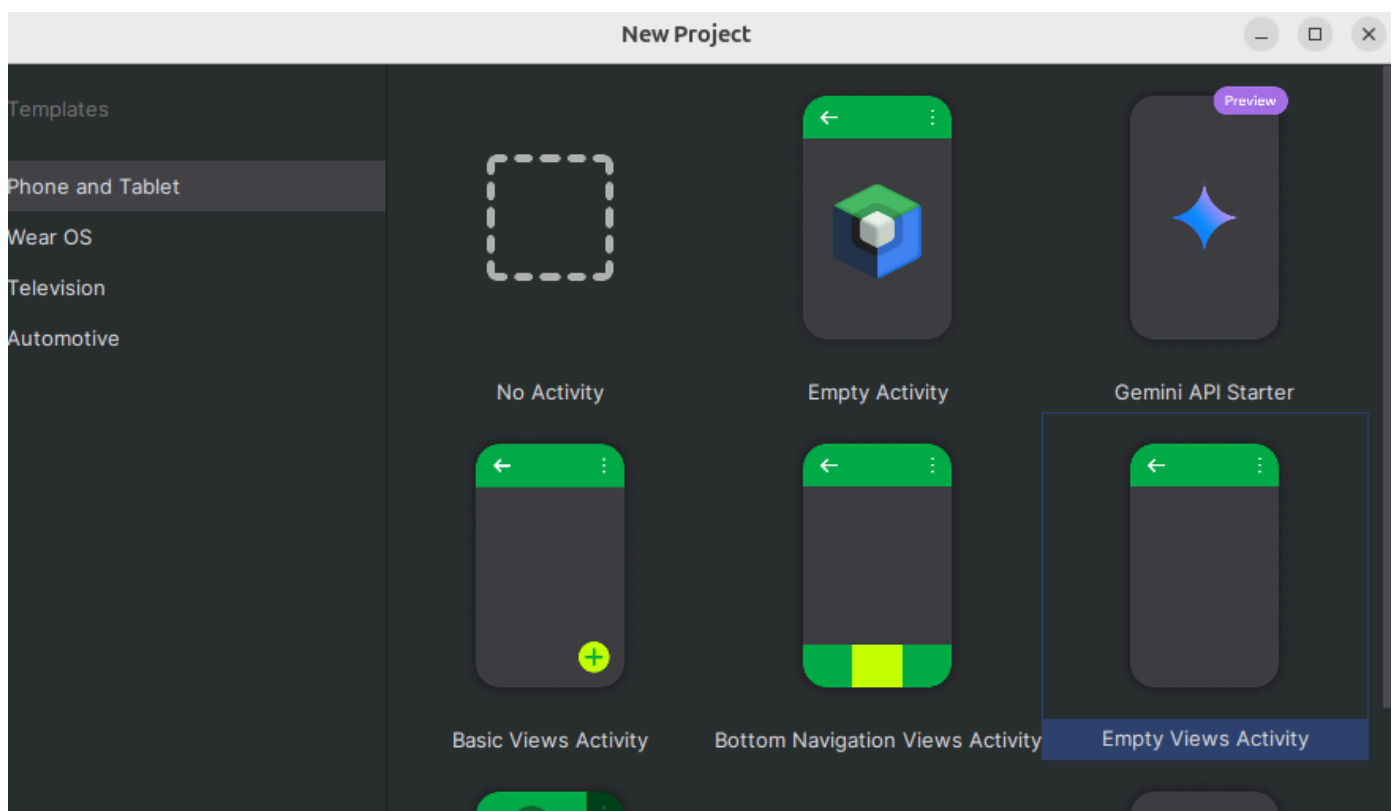
هنا هنتكلم ازاي تنشئ اول app باستخدام java on android studio

1- After install AndroidStudio : open it and select from file tap new project



2- create project and select Language Java

هنا بقي هنختار ايه الشكل بتاع app وبعد كده هنكتب اسمه ونختار Java



Empty Views Activity

Creates a new empty activity

Name

Package name

Save location

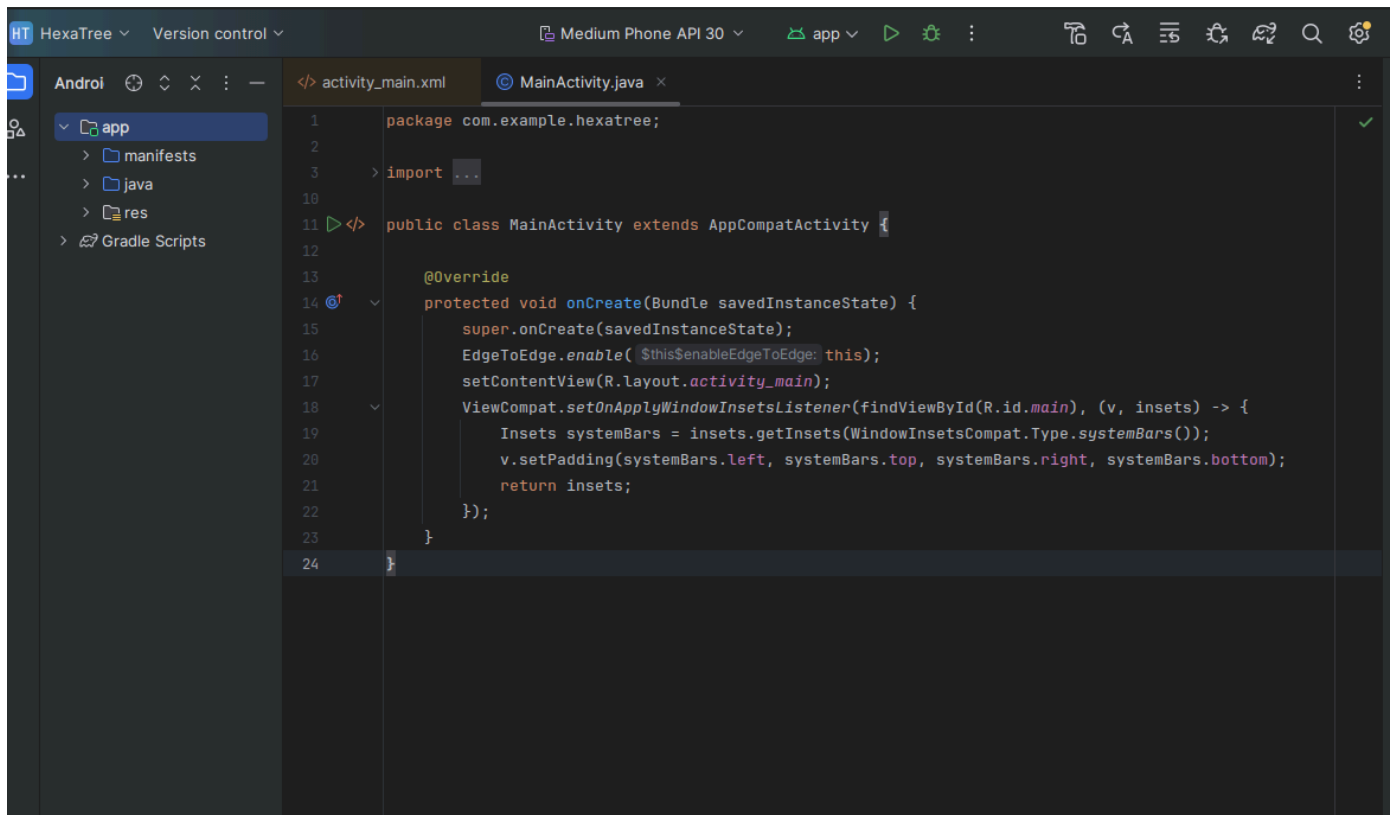
Language

Minimum SDK

*📘 Your app will run on approximately 98.6% of devices.
[Help me choose](#)*

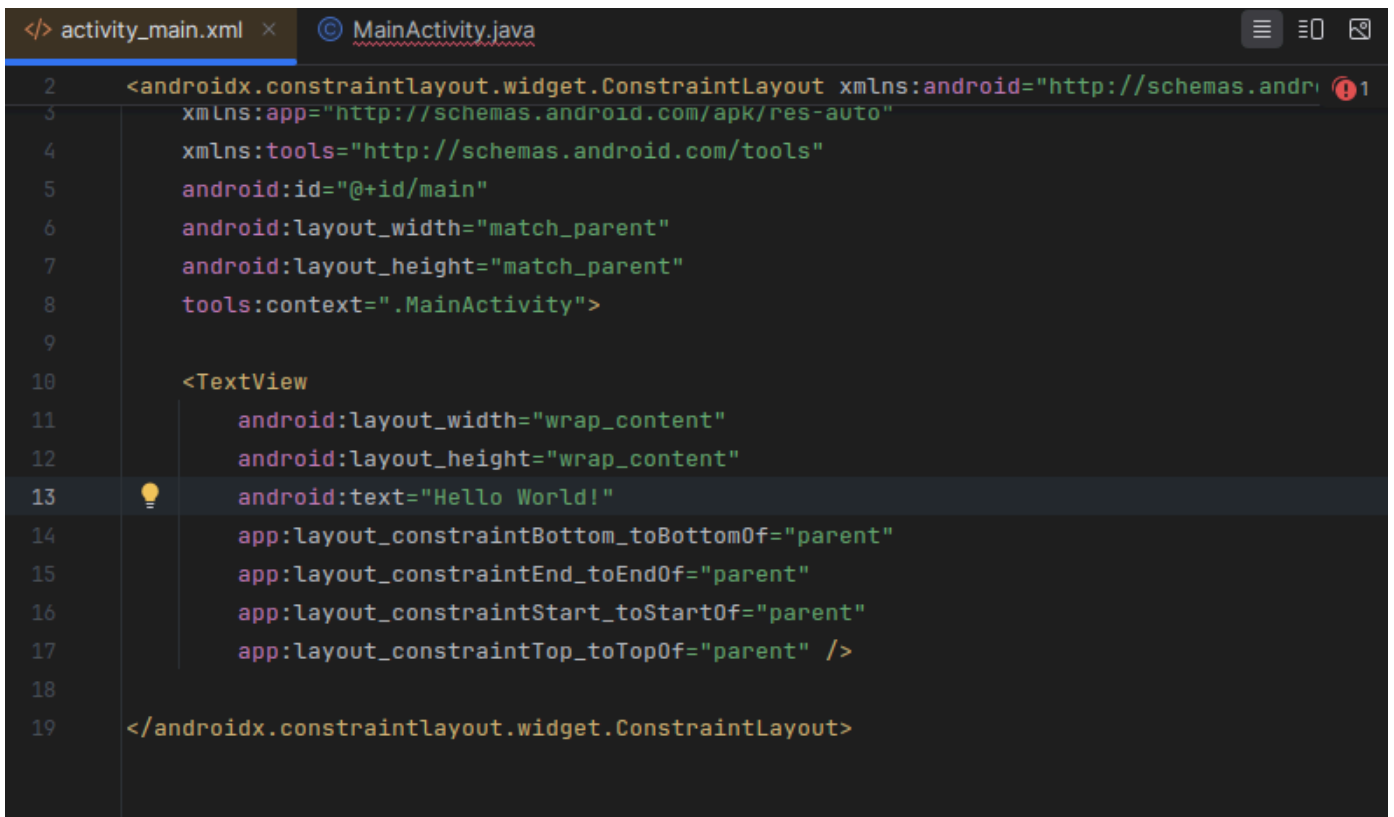
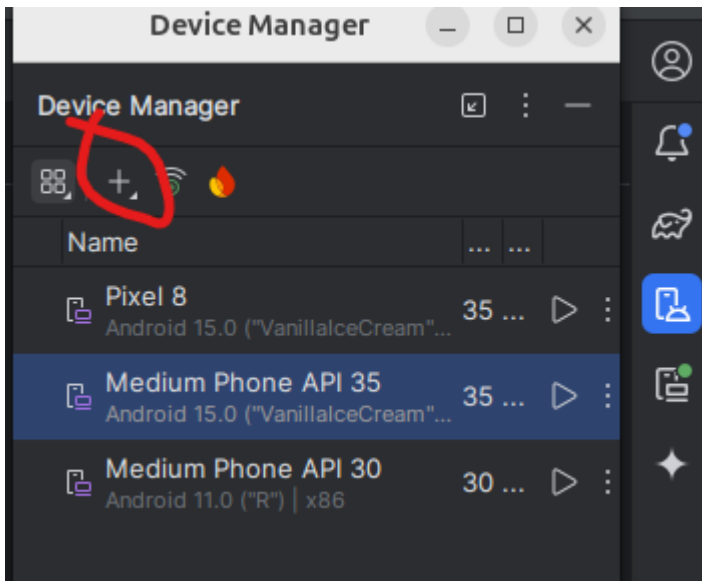
Build configuration language

دلوقتي بقي بعد ما عملناه هنفتحه ونشوف MainActivity وده عبارة عن الصفحة الرئيسية الخاصة بالتطبيق



```
1 package com.example.hexatree;
2
3 > import ...
4
5
6
7
8
9
10
11 </> public class MainActivity extends AppCompatActivity {
12
13     @Override
14     protected void onCreate(Bundle savedInstanceState) {
15         super.onCreate(savedInstanceState);
16         EdgeToEdge.enable(this);
17         setContentView(R.layout.activity_main);
18         ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main), (v, insets) -> {
19             Insets systemBars = insets.getInsets(WindowInsetsCompat.Type.systemBars());
20             v.setPadding(systemBars.left, systemBars.top, systemBars.right, systemBars.bottom);
21             return insets;
22         });
23     }
24 }
```

2-Create emulator to run app click add and select the emulator



دلوقتي بقي لو عاوزين نعرض حاجة في screen بتاعت emulator بنستخدم `TextView` :
ال `home_text` دي عبارة عن id احنا بنعرفه لل attribute بتاع عرض text

```
// update the text from code
TextView homeText = findViewById(R.id.home_text);
homeText.setText("Hello!");
```

As you can see the ID is not referenced by a string `"home_text"`, but as an identifier `R.id.home_text`. The resource reference class `R` is automatically generated based on various resources, including the IDs referenced in the layout .xml files.

If you run into `findViewById()` crashes, go back to the layout editor and make sure the ID `"home_text"` is really set on the `TextView` element.

نفس الكلام لو عاوزين ننشئ button نعرف id برده وننشئ button

To handle button events we need to reference the button `R.id.home_button` and add an `OnClickListener` handler:

```
Button homeButton = findViewById(R.id.home_button);
homeButton.setOnClickListener(new View.OnClickListener() {
    @Override
    public void onClick(View v) {
        Log.v("HEXTREE", "Button has been clicked!");
    }
});
```



دلوقتي بقي لو عاوزين نعمل simple app في button وفي counter بيعد كل ما نضغط علي button ال counter يزد

```
public class MainActivity extends AppCompatActivity {
    int counter=0;
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        EdgeToEdge.enable(this);
        setContentView(R.layout.activity_main);
        ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main),
```

```
(v, insets) -> {  
    Insets systemBars =  
insets.getInsets(WindowInsetsCompat.Type.systemBars());  
    v.setPadding(systemBars.left, systemBars.top, systemBars.right,  
systemBars.bottom);  
    return insets;  
});  
TextView homeText = findViewById(R.id.home_text);  
homeText.setText("Hello!");  
Button button=findViewById(R.id.button);  
button.setOnClickListener(new View.OnClickListener() {  
    @Override  
    public void onClick(View v) {  
        counter++;  
        homeText.setText("Clicked : "+counter);  
    }  
});  
  
}  
}
```

Clicked: 28

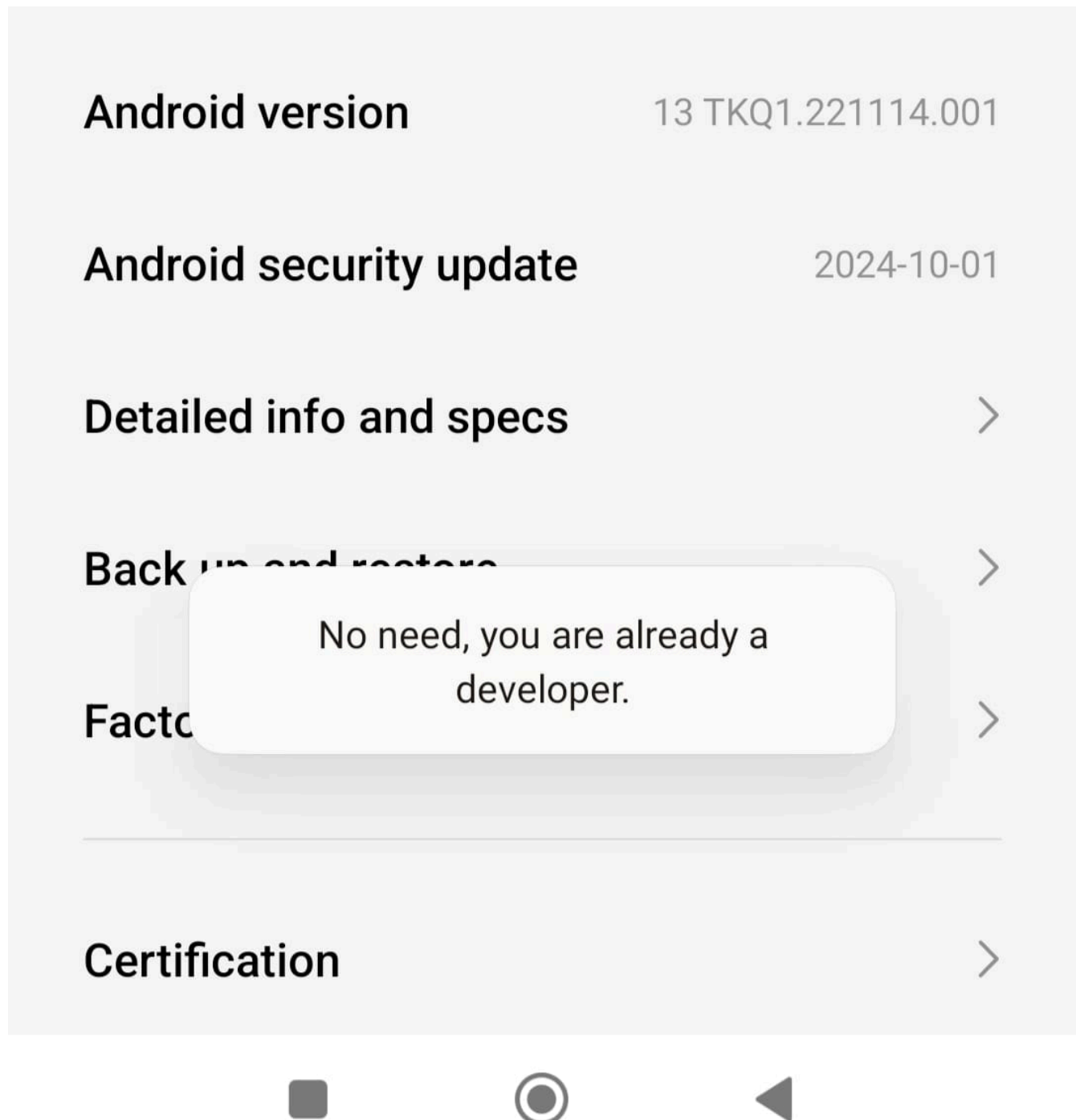
Click Me!



هنا اه كل ما اضغط علي button ال counter will increase

How to connect real mobile to emulator

1- go to setting and click multi times on OS version to be developer



2- open developer option and enable USB debugging



Developer options

Demo mode



Quick settings developer tiles



Debugging

USB debugging

Switch to debugging mode when USB is connected



Revoke USB debugging authorizations



Wireless debugging

Debug mode when Wi-Fi is connected



Install via USB

Allow installing apps via USB



Install via USB



USB debugging (Security settings)

Allow granting permissions and simulating input via USB debugging



Disable adb authorization timeout

Disable automatic revocation of adb authorizations for systems that have not reconnected within the default (%1\$d days) or user-configured (minimum %2\$d day) amount of time.



3- Connect mobile to laptop by using usb run app on android studio and choose the mobile

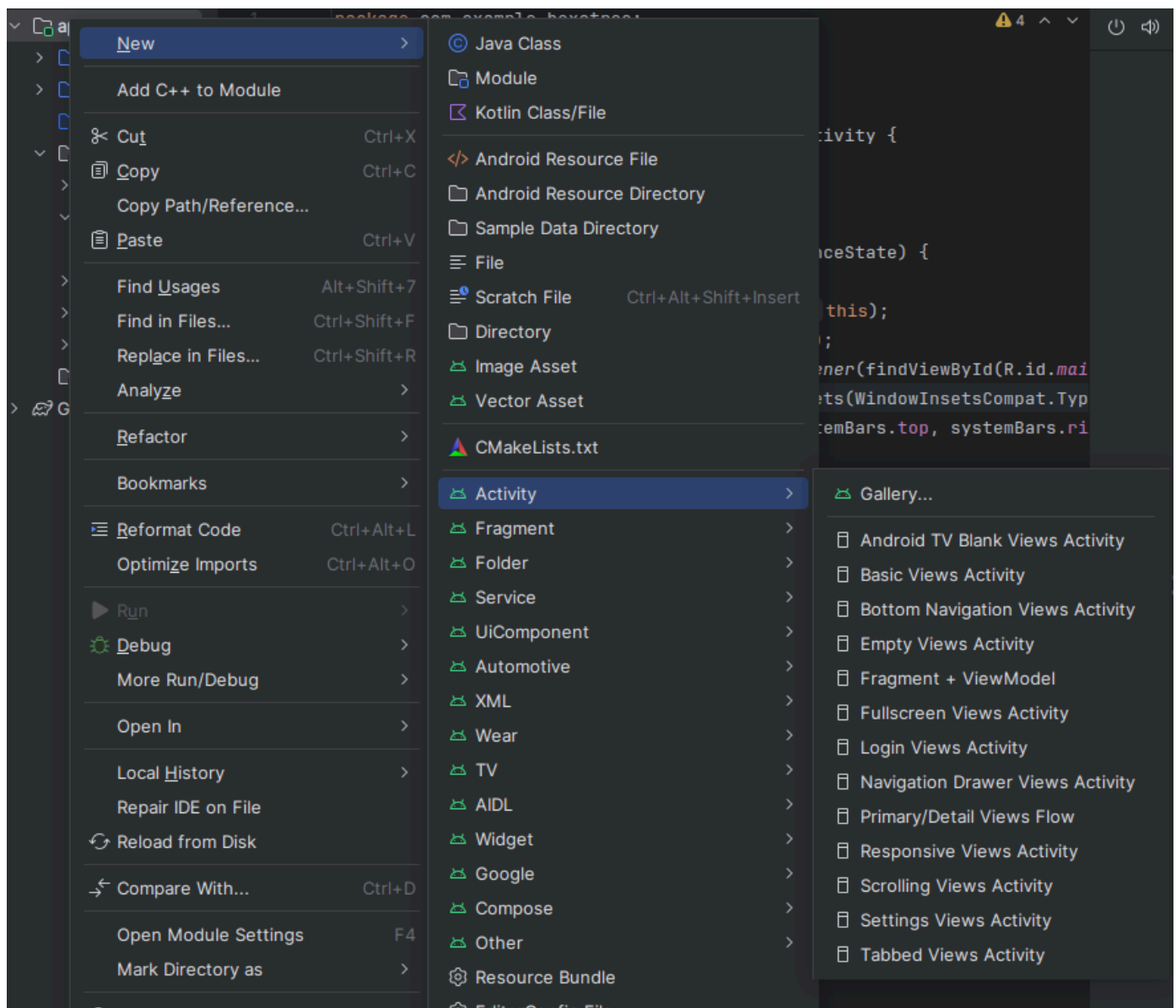
Intent

دلوقتي هنشوف ازاي ننشئ intent وده شارحينه بالتفصيل في slide of AndroidStructure والخالصة ان هي بيمنح ان تطبيق تاني يستخدمها او مش لازم تطبيق ممكن يبقي activity تاني داخل التطبيق

how to create intent for browse

```
Intent browserIntent=new
Intent(Intent.ACTION_VIEW,Ui.Parse("https://hextree.io"));
startActivities(browserIntent);
```

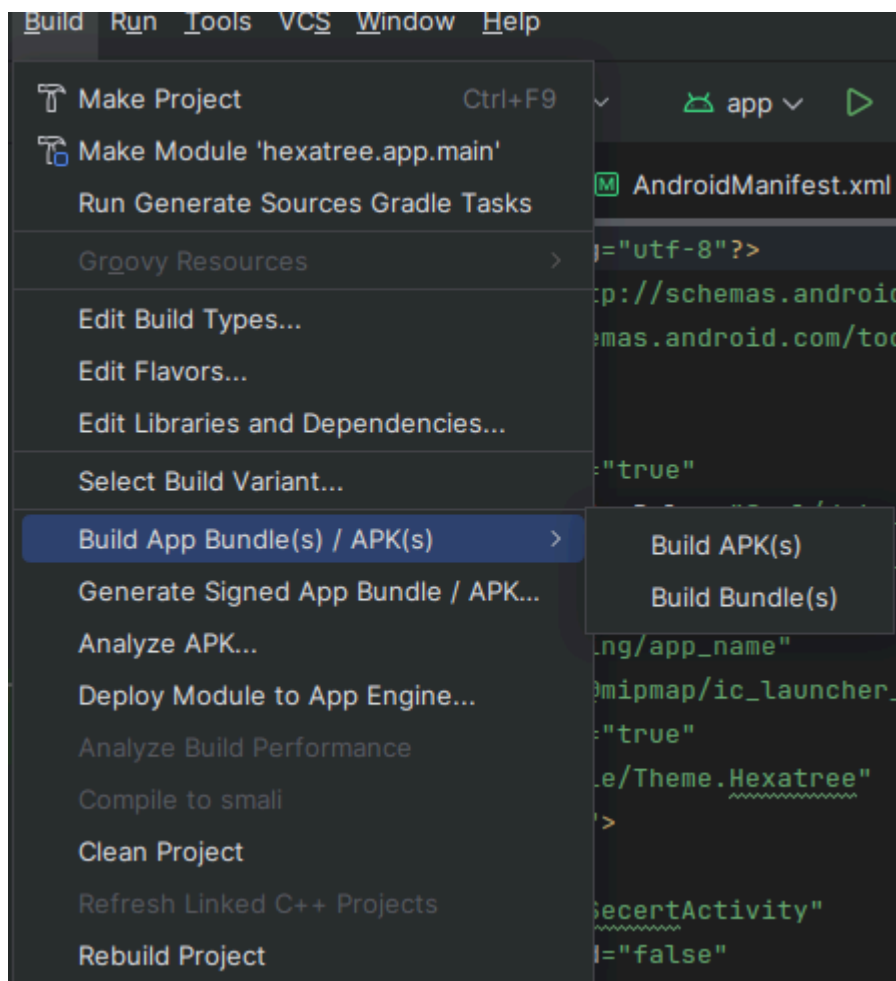
لو عاوز بقي ننشئ activity



اي activity بقي بتنشئه بيبقي موجود في AndroidManifest.xml

```
ity_main.xml  MainActivity.java  AndroidManifest.xml  x  v  :  Ru
1  <?xml version="1.0" encoding="utf-8"?>
2  <manifest xmlns:android="http://schemas.android.com/apk/re
3      xmlns:tools="http://schemas.android.com/tools">
4
5      <application
6          android:allowBackup="true"
7          android:dataExtractionRules="@xml/data_extraction_
8          android:fullBackupContent="@xml/backup_rules"
9          android:icon="@mipmap/ic_launcher"
10         android:label="@string/app_name"
11         android:roundIcon="@mipmap/ic_launcher_round"
12         android:supportsRtl="true"
13         android:theme="@style/Theme.Hexatree"
14         tools:targetApi="31">
15         <activity
16             android:name=".SecertActivity"
17             android:exported="false"
18             android:theme="@style/Theme.Hexatree" />
19         <activity
20             android:name=".MainActivity"
21             android:exported="true">
22             <intent-filter>
23                 <action android:name="android.intent.actio
24
25                 <category android:name="android.intent.cat
26             </intent-filter>
27         </activity>
28     </application>
29
30 </manifest>
```

لو عاوزين بقي الكود اللي عملناه نحوله لتطبيق ونحمله علي emulator نعمل build for app وبع كده
نستخدم adb علشان ننزله



use adb

```
adb install app.apk
```

Capture flag

هنا بقيعلشان نعرف flag الفكرة ان هو لازم 9999 > counter علشان يروح للصفحة الثانية اللي فيها لازم تختار من الاختيارات صفحة رقم 9 وفي الصفحة دي لازم نخلي يجيب 42% علشان يطلع flag

1-First Solution :

لما يجيب 1 بحيث نروح للصفحة الثانية علي طول counter ونعدل الرقم مثلا بدل من 9999 يبقي 1 بحيث نخلي smali هو ان نغير في كود

1- clone the project from github

```
git clone https://github.com/hextreeio/android-challenge1.git
```

2- open project with AndroidStudio and bulicd app

3- open app with jadx-gui

1- function for check counter > 9999

هنا اه لو لاقى ان counter > 9999 بيعمل start activity لل activity اللي هو
this.ChallengeActivity يعني بيروح لل ChallengeActivity.java

startActivity(new Intent(MainActivity.this, ChallengeActivity.class));

```
        counter++;
        text.setText("Counter: "+counter);
        if(counter>9999) {
            startActivity(new Intent(MainActivity.this,
ChallengeActivity.class));
        }
    }
});
```

2- function for call flag activitiy

هنا اهو ChallengeActivity بيستدعي FlagActivity

```
        public void onClick(View v) {
            startActivity(new Intent(ChallengeActivity.this,
FlagActivity.class));
        }
    });
```

3- FlagActivity

هنا اه لما بيلاقى القيمة 42 بيستدعي decryptflag function

```
        public void onStopTrackingTouch(SeekBar seekBar) {
            // Success!!! Show the flag now!
            if(progressTracking==42) {
                text.setText(decryptFlag());
            }
        }
    });
```

4- DecryptFlag function

```
String decryptFlag() {

    String z1 = a(getResources().getString(b(c.d.e)));
```

```

int z2 = z1.length(), z3 = 0x10;
byte[] z4 = new byte[z2 / 2];
for (int z5 = 0; z5 < z2; z5 += 2) {
    z4[z5 / 2] = (byte) ((Character.digit(z1.charAt(z5), z3) << 4)
        + Character.digit(z1.charAt(z5 + 1), z3));
}

String z6 = a(getResources().getString(b(c.f.g)));
byte[] z7 = Base64.decode(z6, Base64.DEFAULT);
//byte[] z7 = z6.getBytes();
byte[] z8 = new byte[z7.length];
for (int z9 = 0; z9 < z7.length; z9++) {
    z8[z9] = (byte) (z7[z9] ^ z4[z9 % z4.length]);
}

Log.i("FLAG", new String(z8));
Log.i("base64.FLAG", new String(Base64.encode(z8, Base64.DEFAULT)));

return new String(z8);
}

```

5- decompile app with apktool

```
apktool d app.apk
```

6- change the value on smali file from 9999 to 0 : from 0x270f to 0x1 --> to click 1 counter

```

const/16 v1, 0x270f

    if-le v0, v1, :cond_0

```

to

```

const/16 v1, 0x1

    if-le v0, v1, :cond_0

```

7- Build app

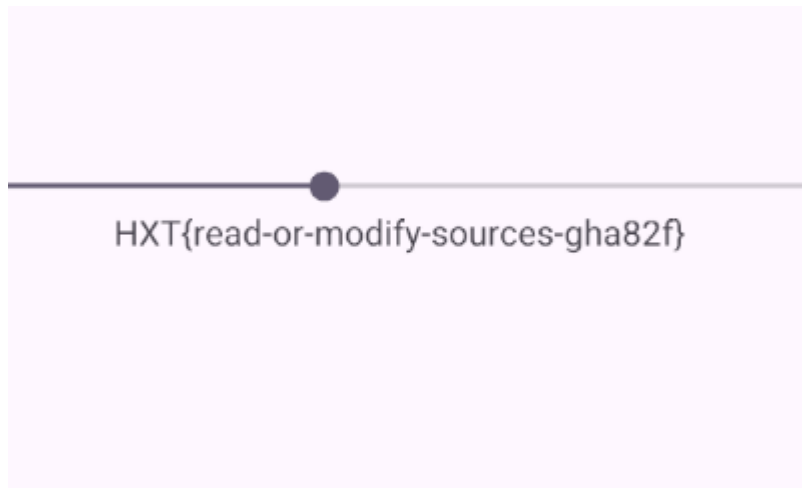
```
apktool b app-debug
```

8- sign applicaton

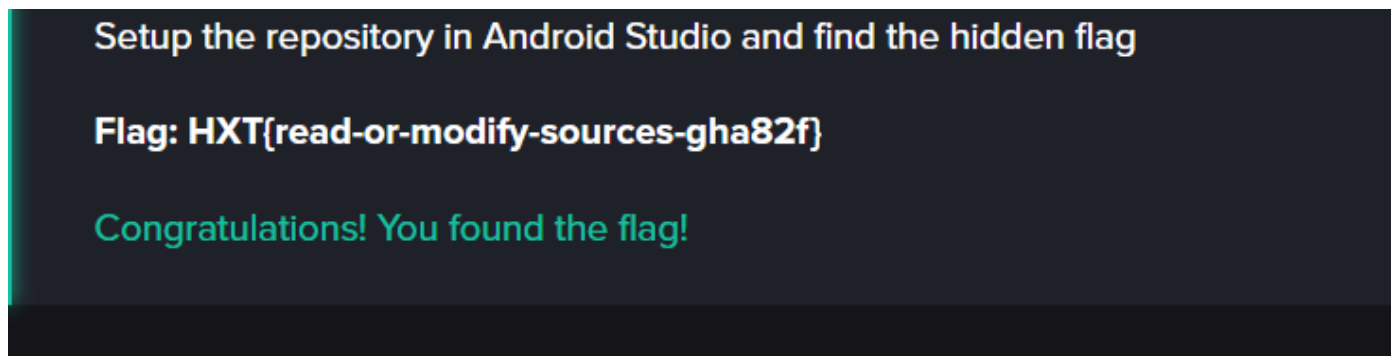
```
→ dist git:(master) X zipalign -v 4 app-debug.apk out.apk
→ dist git:(master) X apksigner sign --ks-key-alias root_detection_key -ks
~/android-app-hack.keystore out.apk
WARNING: A restricted method in java.lang.System has been called
WARNING: java.lang.System::loadLibrary has been called by
org.conscrypt.NativeLibraryUtil in an unnamed module
(file:/home/ubuntu/Android/Sdk/build-tools/35.0.1/lib/apksigner.jar)
```

upload app

```
adb install out.apk
```

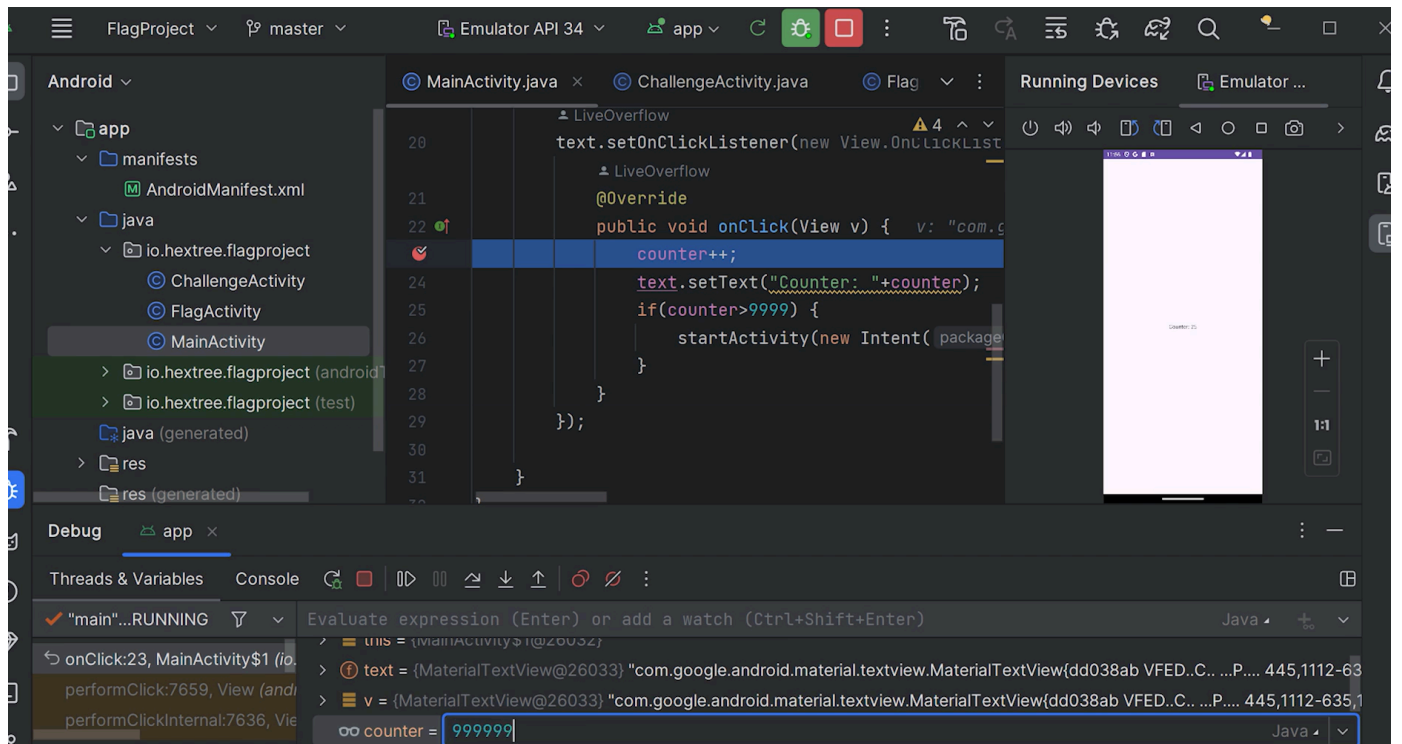


HXT{read-or-modify-sources-gha82f}



2- Second Solution : by using debug mode on AndroidStudio

هو ان نعمل debug لل counter يعني نمشي مع التطبيق وهو ب run واول ما يجي عندي السطر اللي
هو counter++ نخليه ب نعمله ب 9999 بدل ما نروح نعمل click 9999 times



كده لما نعدل ونخليه رقم اكبر من 9999 هيجيب الصفحة الثانية علي طول

3-Third Solution

هو في الكود بتاع flag هو اصلا بيعمل run للكود فب الصفحة بتاعت Flag


```

© MainActivity.java © ChallengeActivity.java © FlagActivity.java ×
12 public class FlagActivity extends AppCompatActivity {
47     // How do you get to this FlagActivity? What actions do you have to perform?
48     // Run this project in the emulator and perform those actions to reveal the flag.
    1 usage
49     String decryptFlag() {
50
51         String z1 = a(getResources().getString(b(c.d.e)));
52         int z2 = z1.length(), z3 = 0x10;
53         byte[] z4 = new byte[z2 / 2];
54         for (int z5 = 0; z5 < z2; z5 += 2) {
55             z4[z5 / 2] = (byte) ((Character.digit(z1.charAt(z5), z3) << 4)
56                 + Character.digit(z1.charAt(z5 + 1), z3));
57         }
58
59         String z6 = a(getResources().getString(b(c.f.g)));
60         byte[] z7 = Base64.decode(z6, Base64.DEFAULT);
61         //byte[] z7 = z6.getBytes();
62         byte[] z8 = new byte[z7.length];
63         for (int z9 = 0; z9 < z7.length; z9++) {
64             z8[z9] = (byte) (z7[z9] ^ z4[z9 % z4.length]);
65         }
66
67         Log.i(tag: "FLAG", new String(z8));
68         Log.i(tag: "base64.FLAG", new String(Base64.encode(z8, Base64.DEFAULT)));
69
70         return new String(z8);
71     }
    2 usages
72     String a(String s) { return s; }
    2 usages
73     int b(int i) { return i; }
    2 usages
74     interface c {
        1 usage
75         interface d { int e = R.string.challenge_secret_key; }
        1 usage
76         interface f { int g = R.string.secret; }
77     }

```

الجزء ده هو اللي بيعمل create for flag احنا ممكن ناخذ الجزء ده ونحطه في MainActivity ونعمله عرض باستخدام TextView يبقى كده