

Android Mobile Pentest 101

© tsug0d, September 2018

Lecture 10.1 – Creating Exploit: HelloWorld

Goal: Known how to code an android application

Introduction

- This lecture will help you understand how to create an android app
- No worries, very basic starter 😊

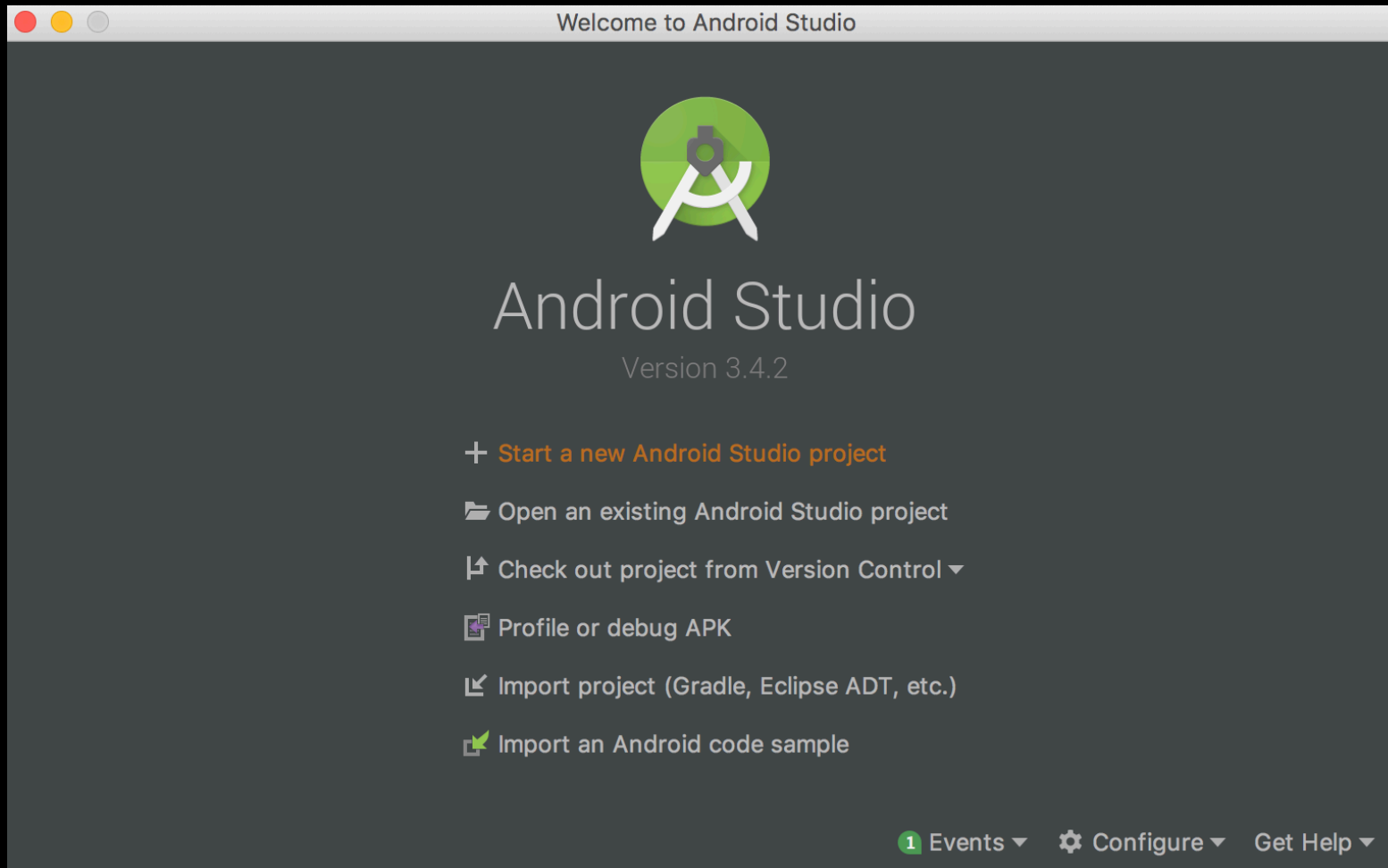
Requirement

- Java Installed (java.com/download)
- Android Studio (developer.android.com/studio)



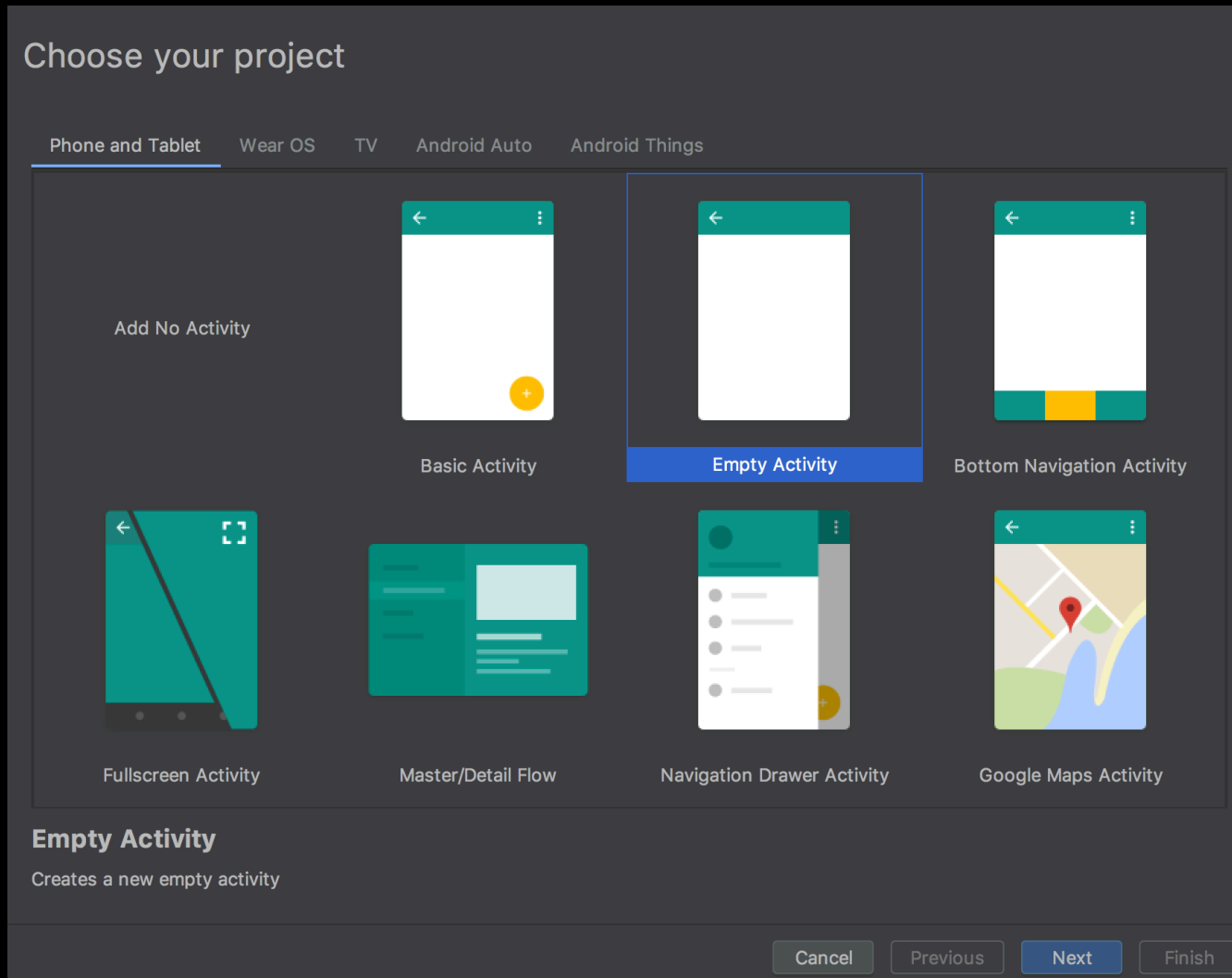
Let's dev!

- Open Android Studio, looks like:



Let's dev!

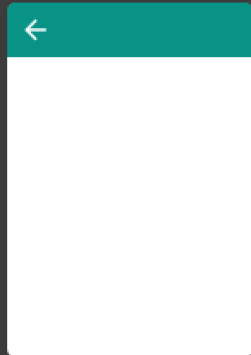
- File -> New -> New Project -> Empty Activity



Let's dev!

- Fill some value -> Finish

Configure your project



Empty Activity

Creates a new empty activity

Name

HelloWorld

Package name

com.example.helloworld

Save location

/Users/tsug0d/AndroidStudioProjects/HelloWorld

Language

Java

Minimum API level API 15: Android 4.0.3 (IceCreamSandwich)

i Your app will run on approximately **100%** of devices.

[Help me choose](#)

☐ This project will support instant apps

☐ Use androidx.* artifacts

Cancel

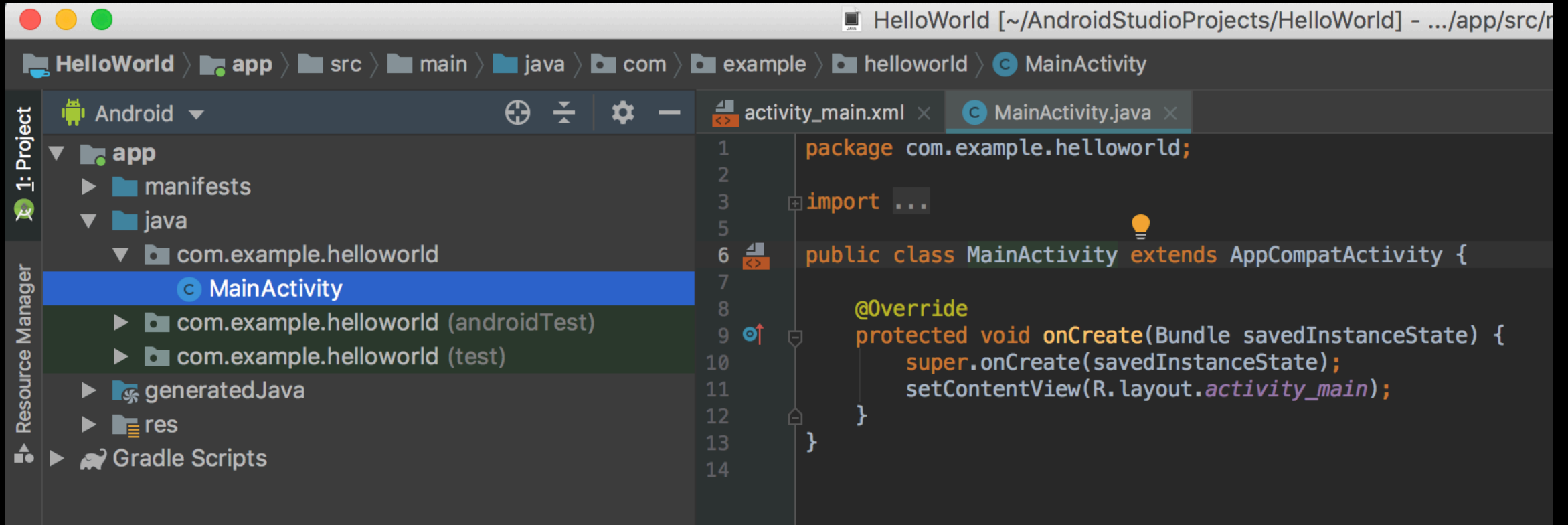
Previous

Next

Finish

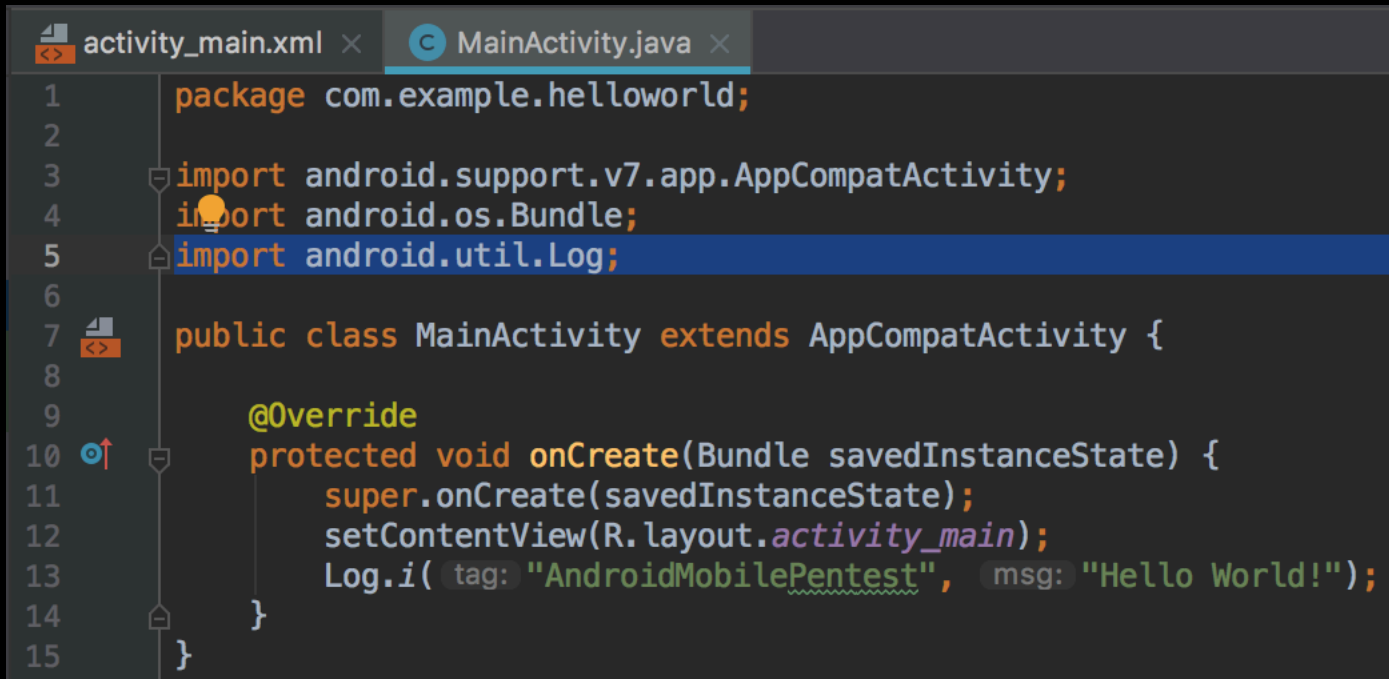
Let's dev!

- Our code in this lecture is located in MainActivity.java



Let's dev!

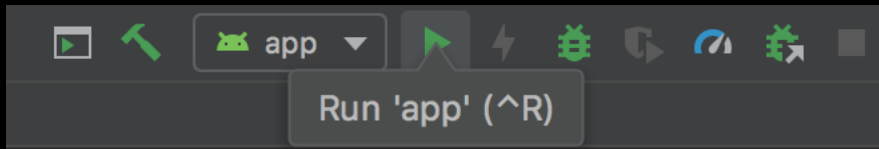
- We will code our very first app, Hello World!
- This will print "Hello World!" in android log (logcat)

A screenshot of an IDE window with two tabs: 'activity_main.xml' and 'MainActivity.java'. The 'MainActivity.java' tab is active, showing Java code for a 'Hello World' app. The code includes package declarations, imports for AppCompatActivity, Bundle, and Log, and an override of the onCreate method that logs 'Hello World!'. Line numbers 1 through 15 are visible on the left margin. The 'import android.util.Log;' line is highlighted in blue.

```
1 package com.example.helloworld;
2
3 import android.support.v7.app.AppCompatActivity;
4 import android.os.Bundle;
5 import android.util.Log;
6
7 public class MainActivity extends AppCompatActivity {
8
9     @Override
10    protected void onCreate(Bundle savedInstanceState) {
11        super.onCreate(savedInstanceState);
12        setContentView(R.layout.activity_main);
13        Log.i("AndroidMobilePentest", "Hello World!");
14    }
15 }
```

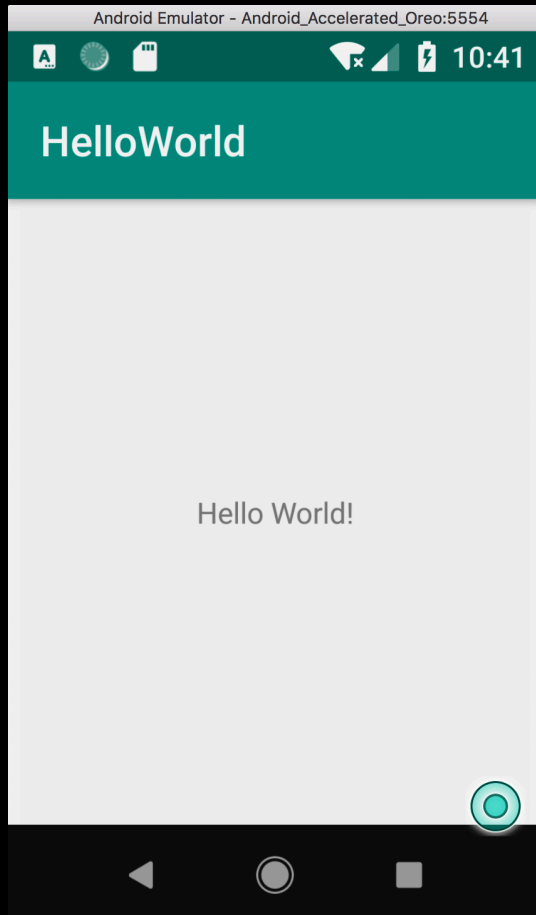
Let's dev!

- Click here to run (you have to create emulator device first)



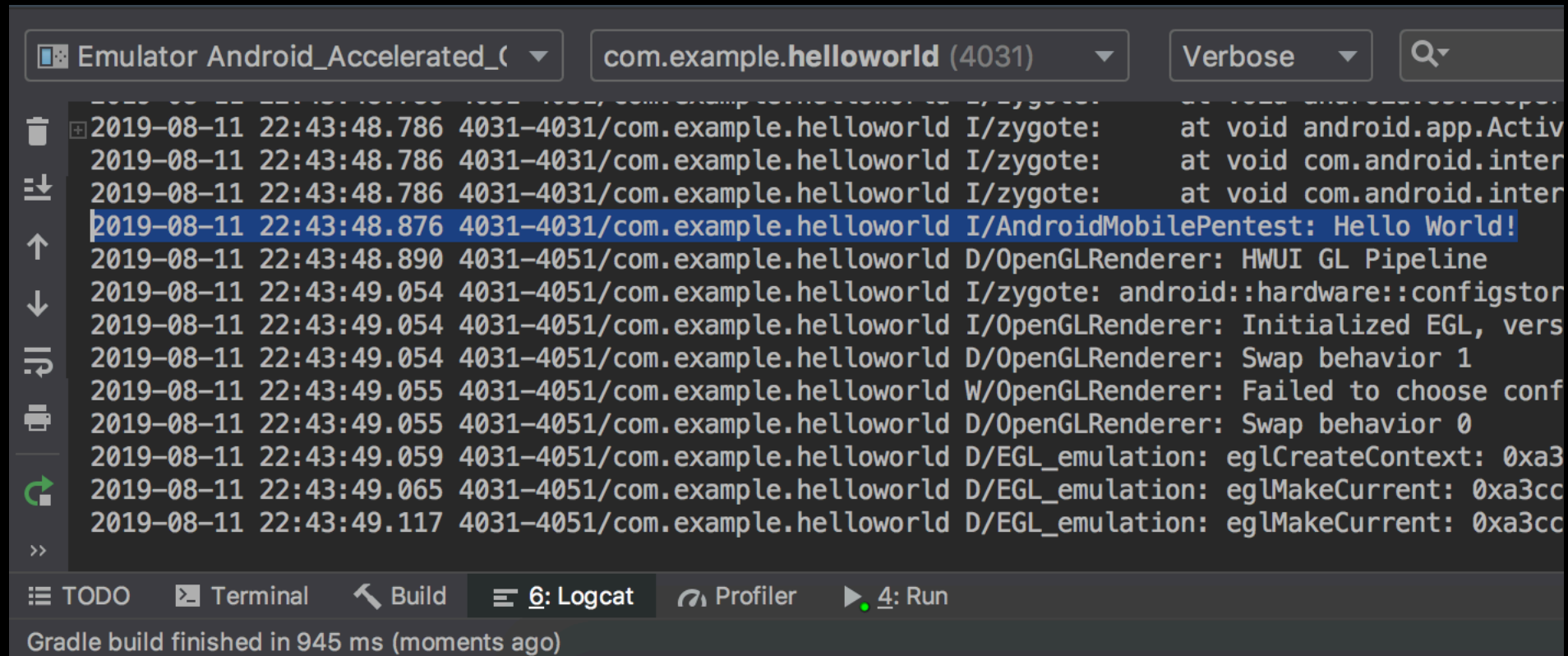
Let's dev!

- Emulator will show your app!



Let's dev!

- Congratz! You've successfully developed your Hello World! app
- Your log code is printed here!



```
Emulator Android_Accelerated_... com.example.helloworld (4031) Verbose Q
```

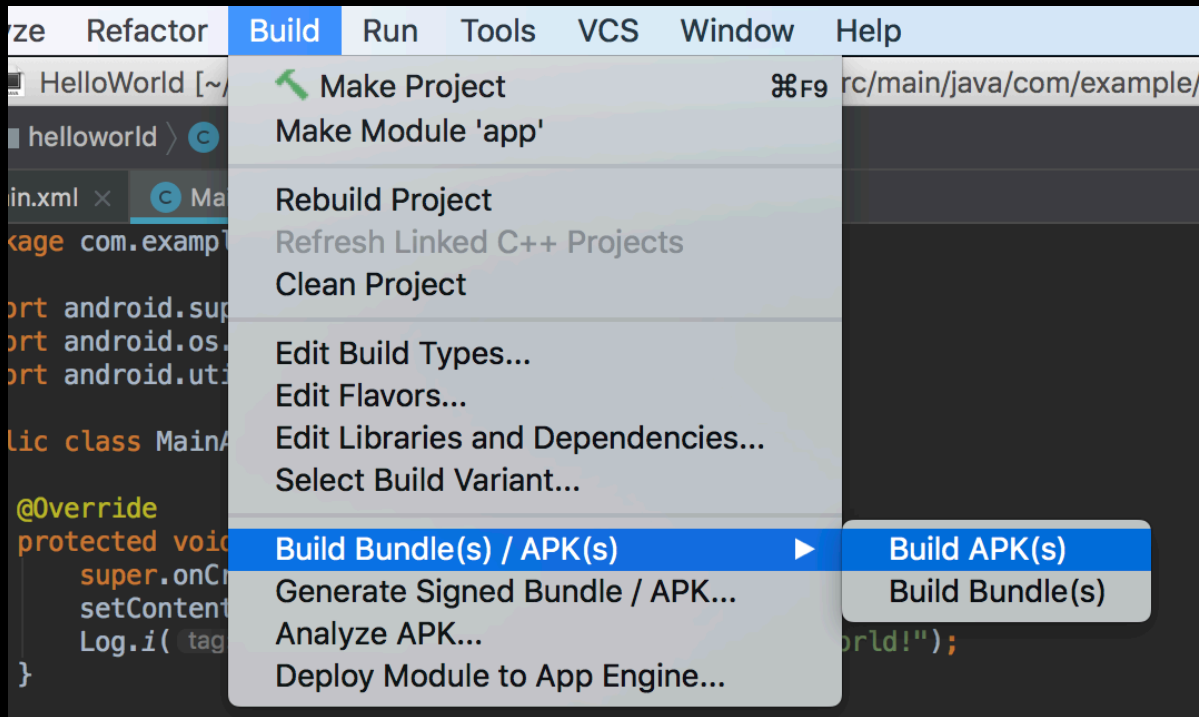
```
2019-08-11 22:43:48.786 4031-4031/com.example.helloworld I/zygote: at void android.app.Activ
2019-08-11 22:43:48.786 4031-4031/com.example.helloworld I/zygote: at void com.android.inter
2019-08-11 22:43:48.786 4031-4031/com.example.helloworld I/zygote: at void com.android.inter
2019-08-11 22:43:48.876 4031-4031/com.example.helloworld I/AndroidMobilePentest: Hello World!
2019-08-11 22:43:48.890 4031-4051/com.example.helloworld D/OpenGLRenderer: HWUI GL Pipeline
2019-08-11 22:43:49.054 4031-4051/com.example.helloworld I/zygote: android::hardware::configstor
2019-08-11 22:43:49.054 4031-4051/com.example.helloworld I/OpenGLRenderer: Initialized EGL, vers
2019-08-11 22:43:49.054 4031-4051/com.example.helloworld D/OpenGLRenderer: Swap behavior 1
2019-08-11 22:43:49.055 4031-4051/com.example.helloworld W/OpenGLRenderer: Failed to choose conf
2019-08-11 22:43:49.055 4031-4051/com.example.helloworld D/OpenGLRenderer: Swap behavior 0
2019-08-11 22:43:49.059 4031-4051/com.example.helloworld D/EGL_emulation: eglCreateContext: 0xa3
2019-08-11 22:43:49.065 4031-4051/com.example.helloworld D/EGL_emulation: eglMakeCurrent: 0xa3cc
2019-08-11 22:43:49.117 4031-4051/com.example.helloworld D/EGL_emulation: eglMakeCurrent: 0xa3cc
```

TODO Terminal Build 6: Logcat Profiler 4: Run

Gradle build finished in 945 ms (moments ago)

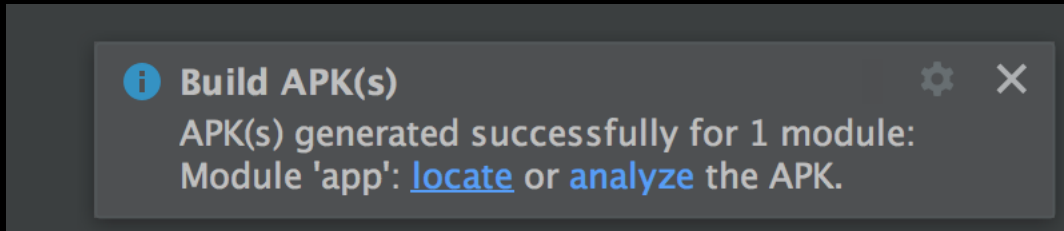
Let's build apk!

- Now we need to export our code to apk file
- Build -> Build Bundle(s) / APK(s) -> Build APK(s)



Let's build apk!

- If we build the apk successful, this popup will appear:



- Click “locate”, we can come to our new apk folder, grab this and install everywhere we want 😊
Note: To put it in Play Store, you have to sign your apk !