

Android Mobile Pentest 101

© tsug0d, September 2018

Lecture 10.1 – Creating Exploit: HelloWorld

Mục tiêu: Biết code 1 android app

Introduction

- Bài này hướng dẫn bạn code 1 app android
- Đừng lo, cơ bản thôi 😊

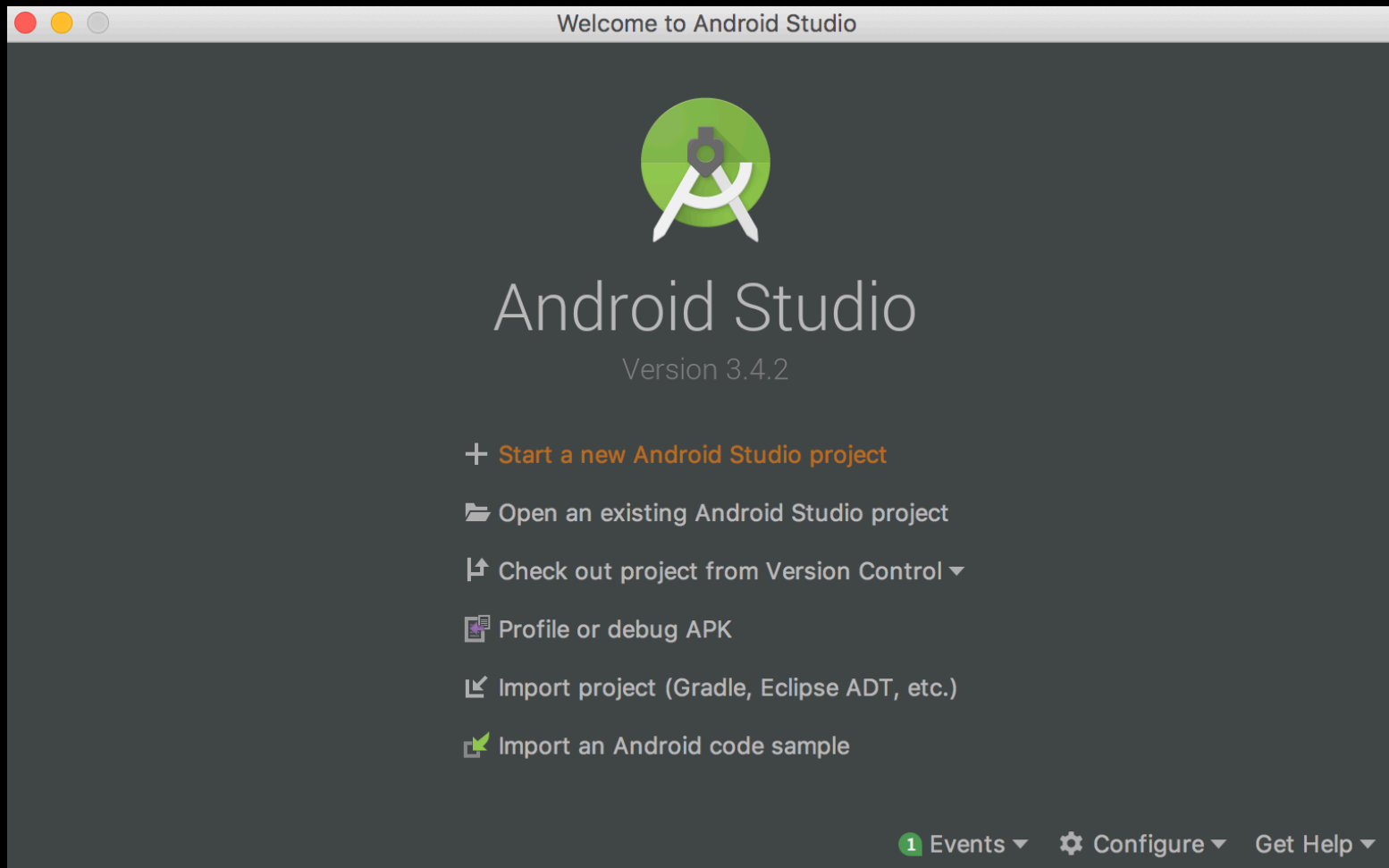
Requirement

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



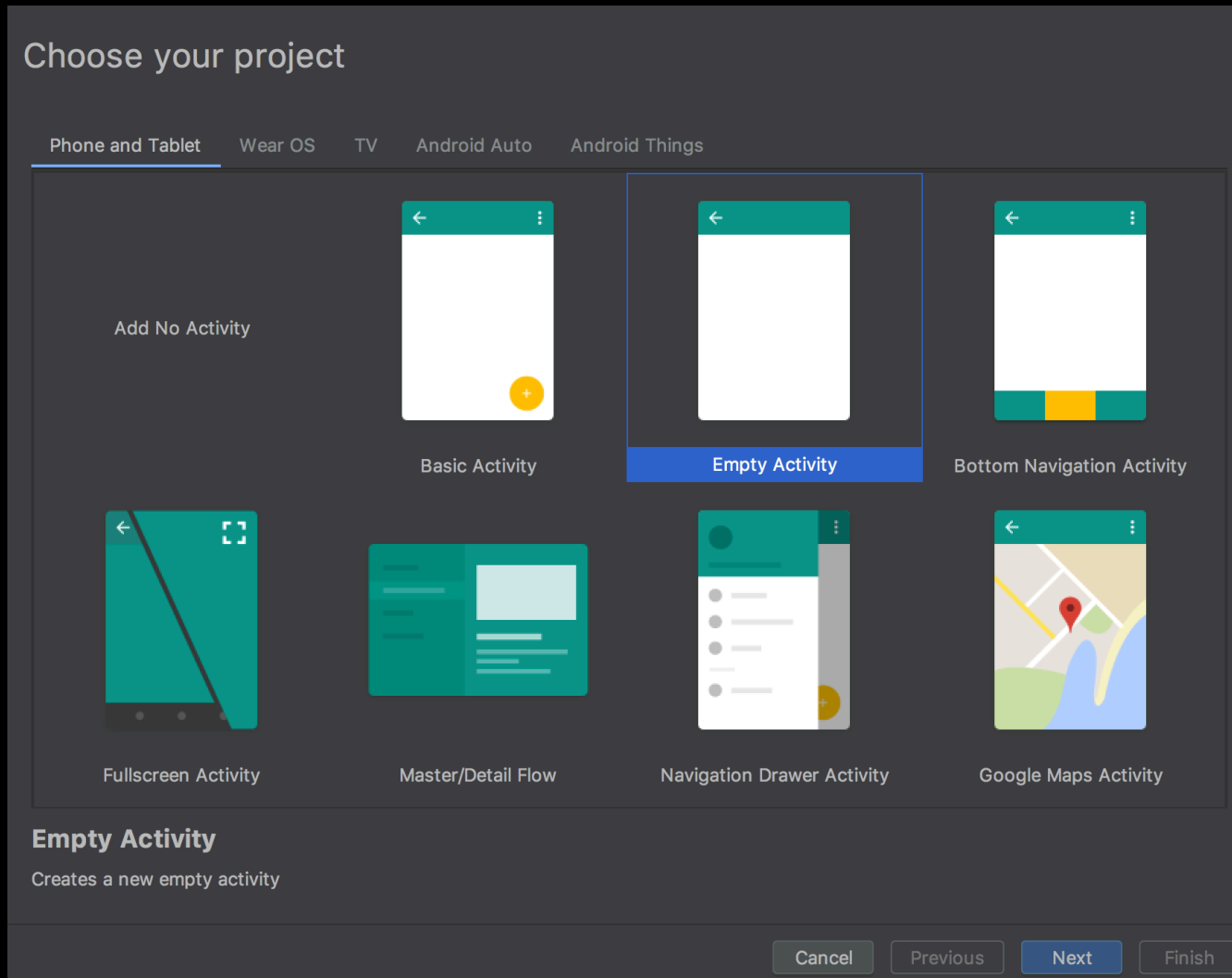
Let's dev!

- Mở Android Studio lên, nó nhìn như này



Let's dev!

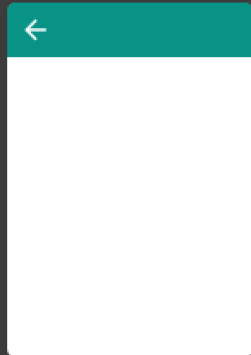
- File -> New -> New Project -> Empty Activity



Let's dev!

- Điền 1 số giá trị, như hình cũng được -> bấm 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

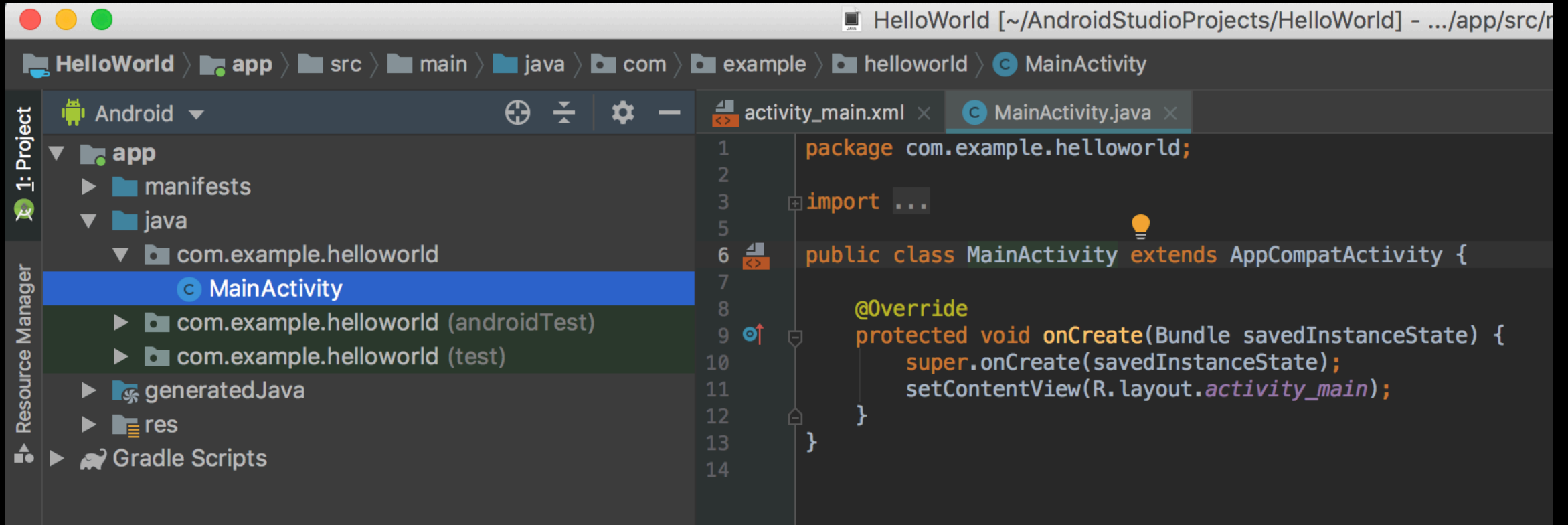
Previous

Next

Finish

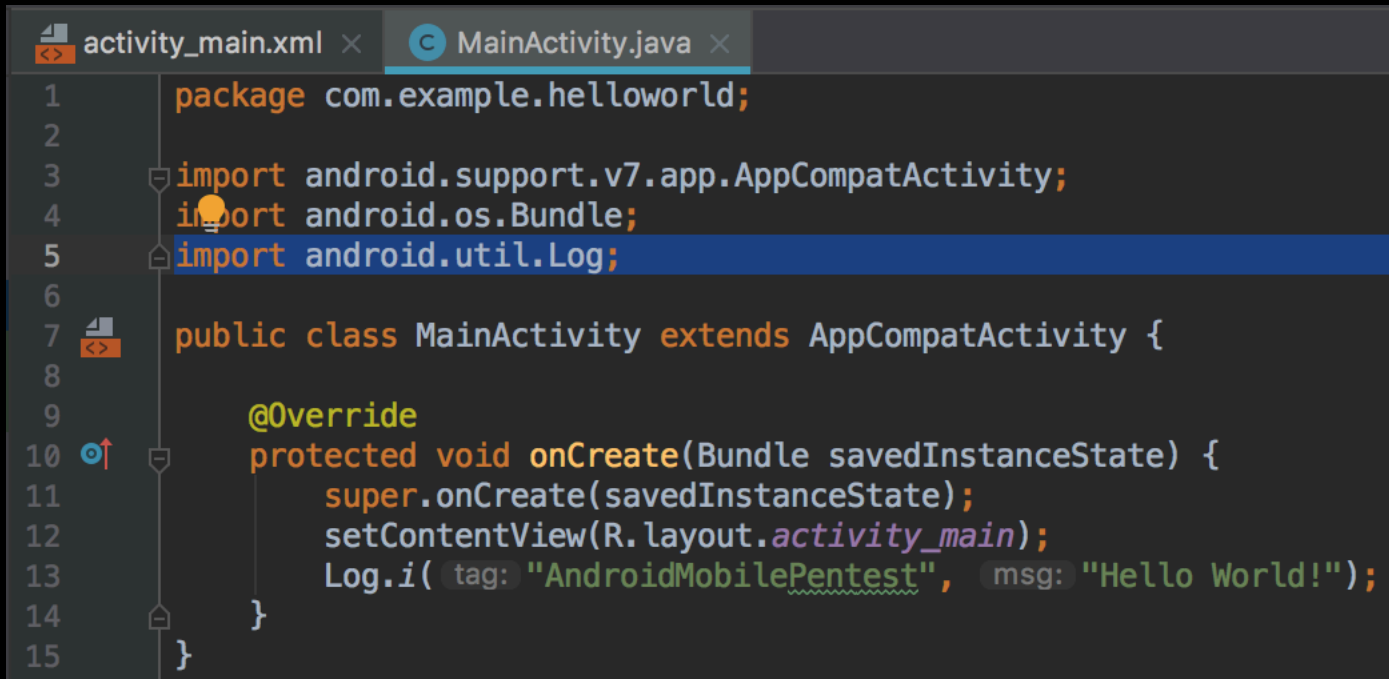
Let's dev!

- Code của chúng ta sẽ nằm ở file MainActivity.java



Let's dev!

- Bắt đầu code thôi, bài khởi đầu với mọi bài code: Hello World!
- App này sẽ in ra "Hello World!" ở trong log của android (logcat)

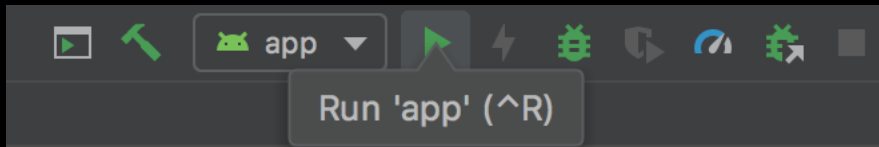
A screenshot of an Android Studio code editor. The top bar shows two tabs: 'activity_main.xml' and 'MainActivity.java', with the latter being the active tab. The code is written in Java and is as follows:

```
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 }
```

The line numbers 1 through 15 are visible on the left side of the editor. The code is color-coded: package names are orange, imports are orange, annotations like @Override are green, and the log message is green. The 'Log.i' method call is on line 13.

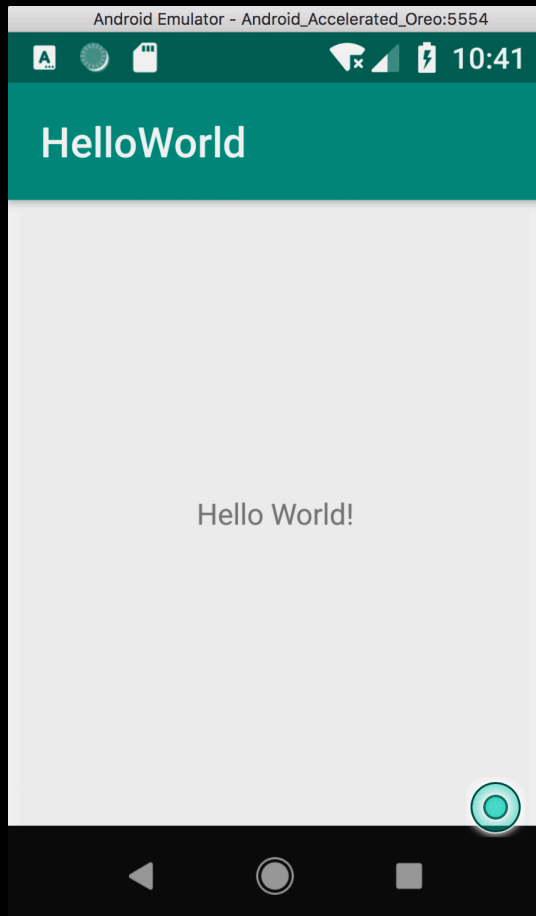
Let's dev!

- Bấm vào đây để chạy (Nhớ tạo emulator device trước đã nhé)



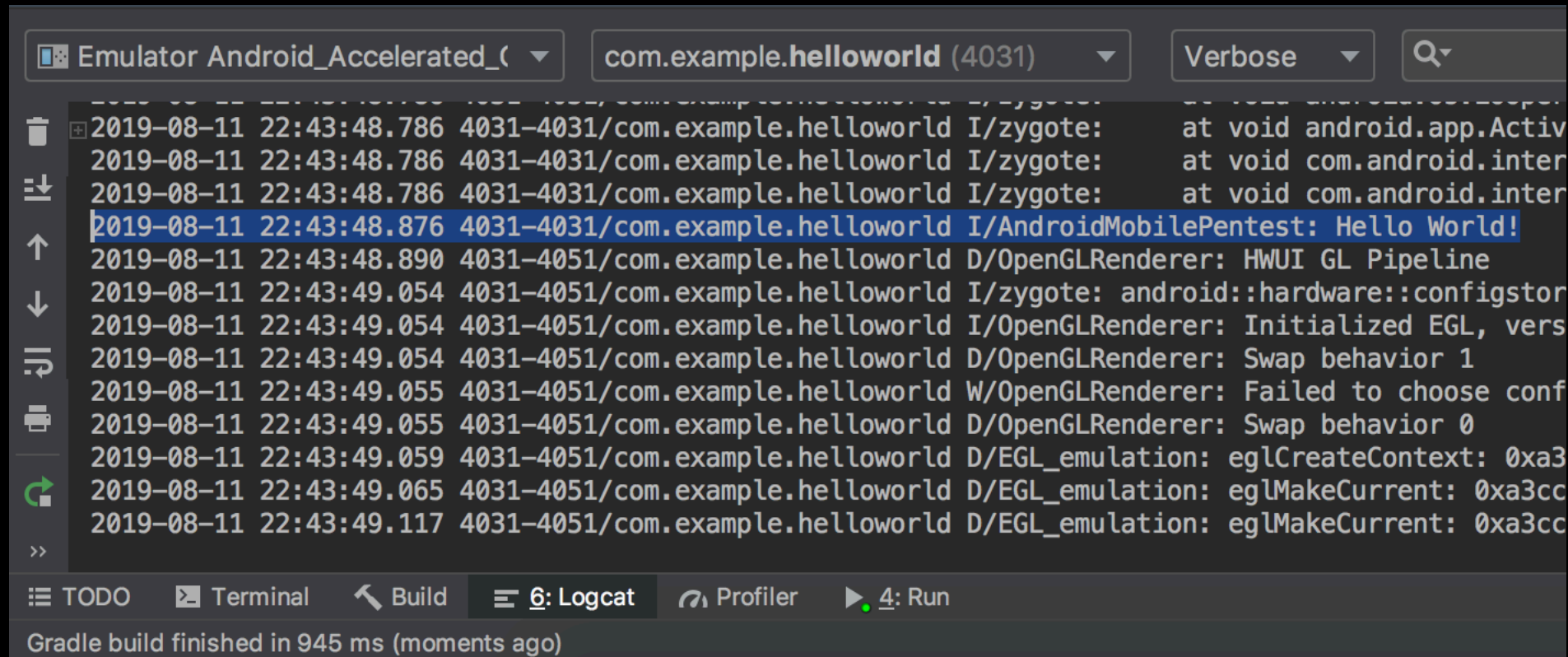
Let's dev!

- App mới code đây:



Let's dev!

- Congratz! Bạn đã dev xong Hello World! app
- Nhìn trong logcat, code của chúng ta đã in "Hello World!" ra



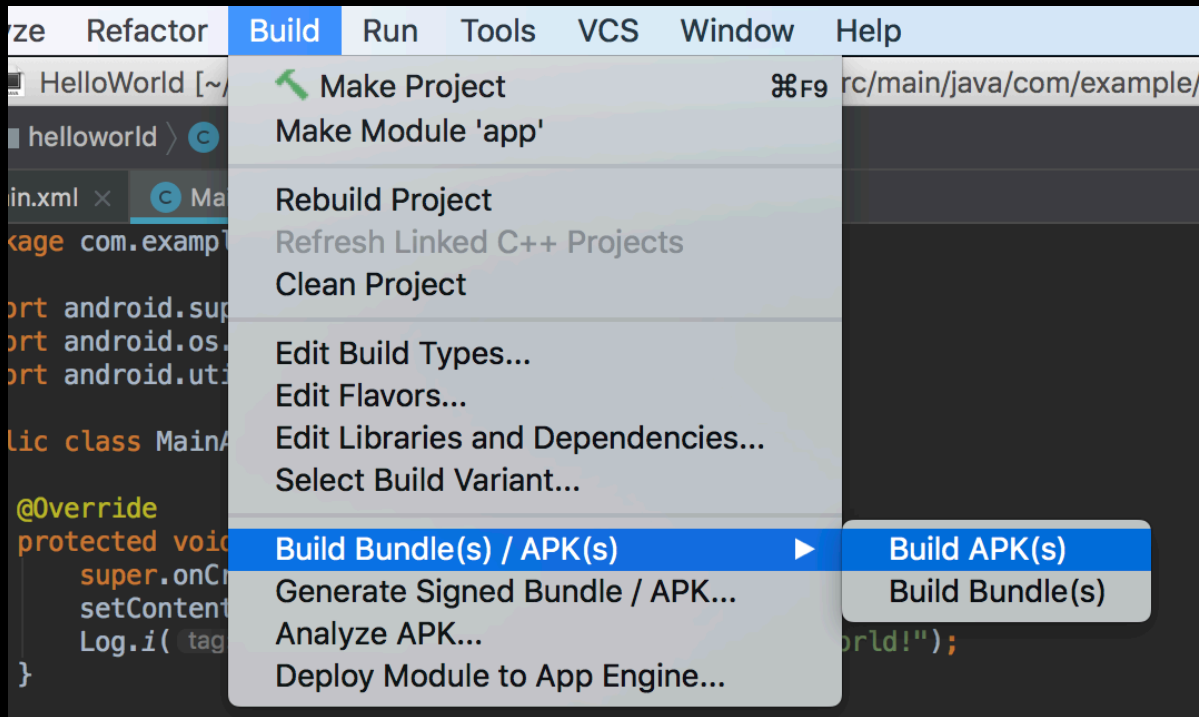
The screenshot shows the Logcat window in Android Studio. The top bar indicates the emulator is 'Emulator Android_Accelerated_...' and the package is 'com.example.helloworld (4031)'. The log level is set to 'Verbose'. The log entries are as follows:

```
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
```

The bottom bar shows the status of the build: 'Gradle build finished in 945 ms (moments ago)'. The tabs at the bottom are: TODO, Terminal, Build, 6: Logcat, Profiler, and 4: Run.

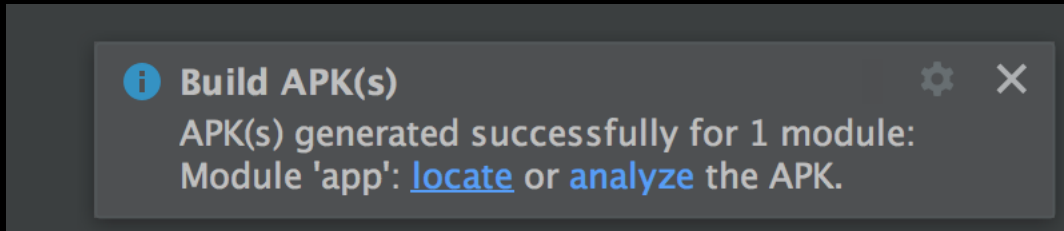
Let's build apk!

- Bây giờ chúng ta cần biến cái code này thành file apk
- Build -> Build Bundle(s) / APK(s) -> Build APK(s)



Let's build apk!

- Nếu thành công thì nó sẽ hiện ra như này



- Bấm vào “locate”, chúng ta sẽ đến được thư mục chứa file apk vừa build, quất nó vào phone nào bạn muốn cài nhé

Lưu ý: Để đem nó lên Play Store, bạn cần thêm bước sign cái apk nữa, ở đây không đề cập.