

Android Mobile Pentest 101

© tsug0d, September 2018

Lecture 10.3 – Creating Exploit: Android Activity

Goal: Understand basic android activity

Introduction

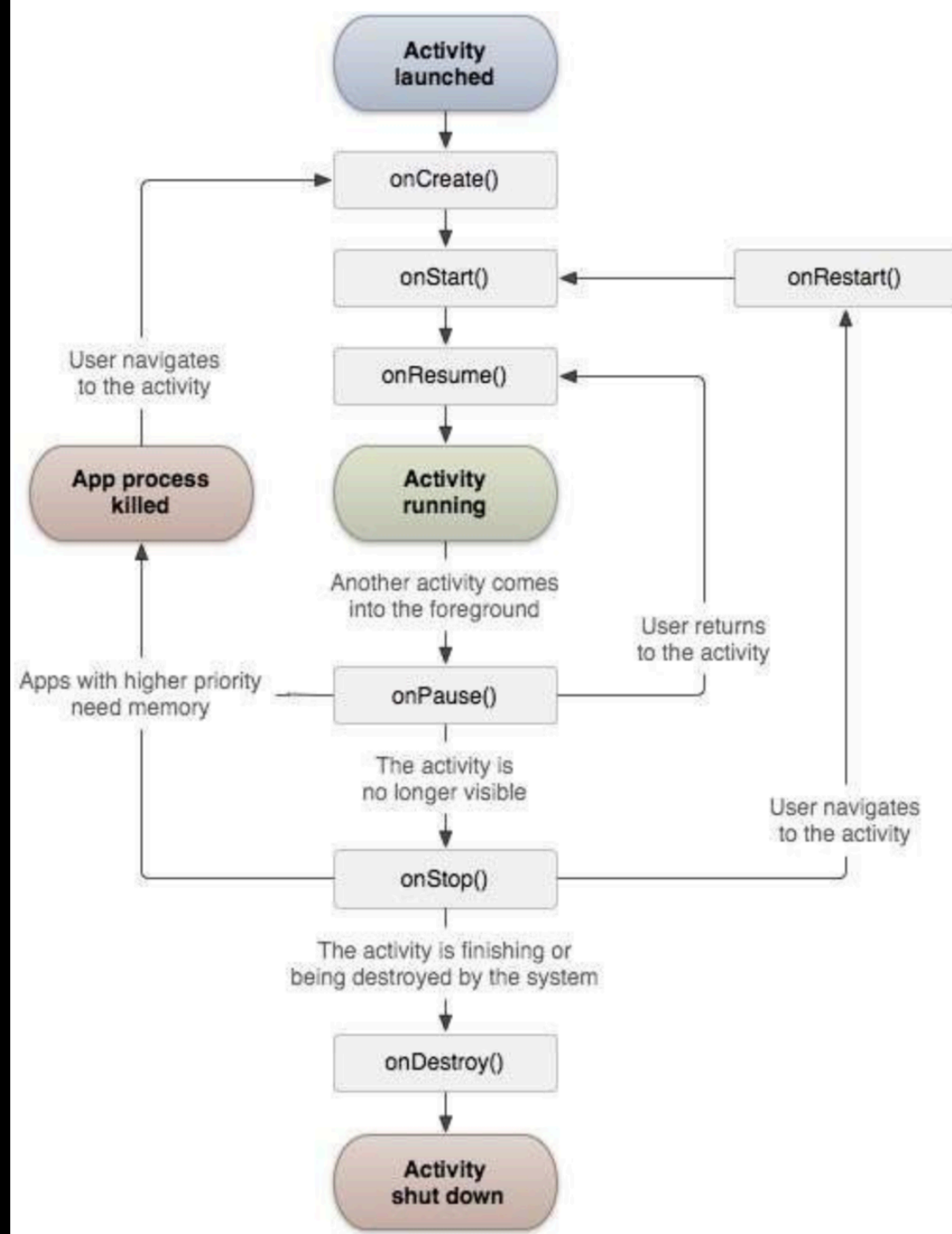
- This lecture will help you understand android activity and its component.

What's Activity?

- Mentioned here: <https://developer.android.com/reference/android/app/Activity>
- An activity is a single, focused thing that the user can do, Android system initiates its program with in an Activity starting with a call on onCreate() callback method.
- If you have worked with C, C++ or Java programming language then you must have seen that your program starts from main() function. Similar in android activity.

What's Activity?

- There is a sequence of callback methods that start up an activity and a sequence of callback methods that tear down an activity



What's Activity?

<code>onCreate()</code>	This is the first callback and called when the activity is first created.
<code>onStart()</code>	This callback is called when the activity becomes visible to the user.
<code>onResume()</code>	This is called when the user starts interacting with the application.
<code>onPause()</code>	The paused activity does not receive user input and cannot execute any code and called when the current activity is being paused and the previous activity is being resumed.
<code>onStop()</code>	This callback is called when the activity is no longer visible.
<code>onDestroy()</code>	This callback is called before the activity is destroyed by the system.
<code>onRestart()</code>	This callback is called when the activity restarts after stopping it.

Let's dev

- We will develop an android app that log the callback method event of an activity when being called
- We create all callback in **MainActivity.java**, then we put the Log.i event in this to see how it works

Example:

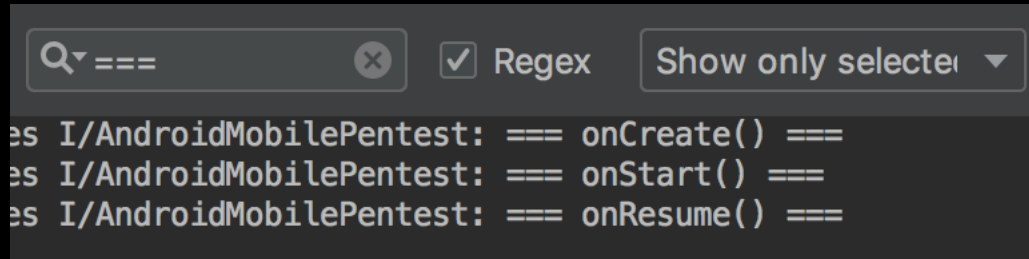
```
@Override
protected void onStart()
{
    super.onStart();
    Log.i(msg, "=== onStart() ===");
}
```

- Sample code here:

<https://github.com/tsug0d/AndroidMobilePentest101/blob/master/lab/MainActivity.java> activities

Let's dev

- When we run the program, the log appears in logcat:



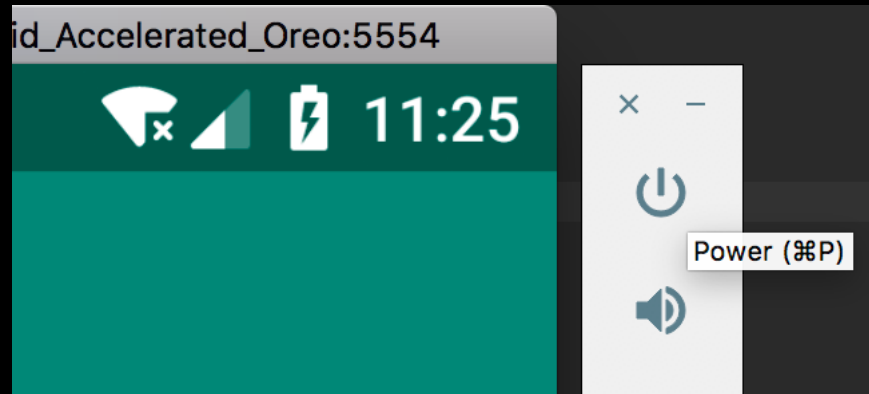
The screenshot shows the Android Studio logcat interface. At the top, there is a search bar with the text "===", a close button (X), a checkbox labeled "Regex" which is checked, and a button labeled "Show only selected" with a dropdown arrow. Below the search bar, the logcat displays three log messages from the package "I/AndroidMobilePentest":

```
I/AndroidMobilePentest: === onCreate() ===  
I/AndroidMobilePentest: === onStart() ===  
I/AndroidMobilePentest: === onResume() ===
```

- When the activity is created, onCreate() is triggered
- When the activity is about to become visible, onStart() triggered
- When the activity has become visible, onResume() triggered

Let's dev

- We try click the shutdown button of the virtual device to lock the phone:



- Logcat:

```
I/AndroidMobilePentest: === onCreate() ===  
I/AndroidMobilePentest: === onStart() ===  
I/AndroidMobilePentest: === onResume() ===  
I/AndroidMobilePentest: === onPause() ===  
I/AndroidMobilePentest: === onStop() ===
```

- When another activity is taking focus, onPause() triggered, yes, we just call the Phone Lock activity
- When the activity is no longer visible, onStop() triggered.

Let's dev

- Click the shutdown button again to unlock phone:

```
I/AndroidMobilePentest: === onCreate() ===  
I/AndroidMobilePentest: === onStart() ===  
I/AndroidMobilePentest: === onResume() ===  
I/AndroidMobilePentest: === onPause() ===  
I/AndroidMobilePentest: === onStop() ===  
I/AndroidMobilePentest: === onStart() ===  
I/AndroidMobilePentest: === onResume() ===
```

- onStart() & onResume() appears in logcat, you know why 😊
- Now we close our app:

```
I/AndroidMobilePentest: === onCreate() ===  
I/AndroidMobilePentest: === onStart() ===  
I/AndroidMobilePentest: === onResume() ===  
I/AndroidMobilePentest: === onPause() ===  
I/AndroidMobilePentest: === onStop() ===  
I/AndroidMobilePentest: === onStart() ===  
I/AndroidMobilePentest: === onResume() ===  
I/AndroidMobilePentest: === onPause() ===  
I/AndroidMobilePentest: === onStop() ===  
I/AndroidMobilePentest: === onDestroy() ===
```