CS 527

Lab 1: Static Analysis on Android Applications

Presenter: Sajad Meisami

21 Sep 2022

Soot

A framework for analyzing and transforming Java and Android applications

- http://soot-oss.github.io/soot/

- Download Soot directly:
- https://soot-build.cs.uni-paderborn.de/public/origin/develop/soot/soot-develop/build/sootclasses-trunk-jar-with-dependencies.jar

Soot Tutorial -wiki

- https://github.com/soot-oss/soot/wiki

- **Soot as a command line tool:**
- https://github.com/soot-oss/soot/wiki/Introduction:-Soot-as-a-command-line-tool
- **Instrumenting Android Apps with Soot:**
- https://github.com/soot-oss/soot/wiki/Instrumenting-Android-Apps-with-Soot

Helpful Soot Tutorial

- https://github.com/noidsirius/SootTutorial

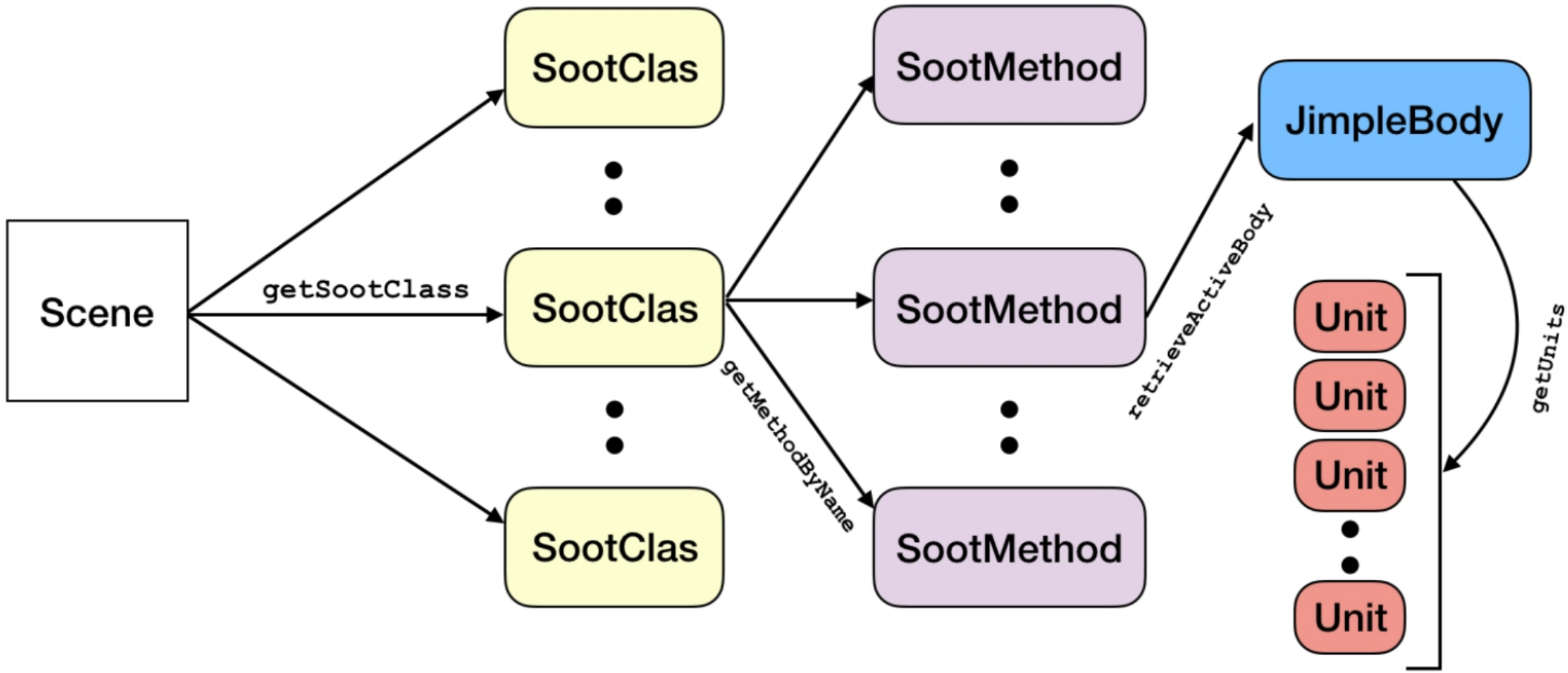
For running Soot and see the result:

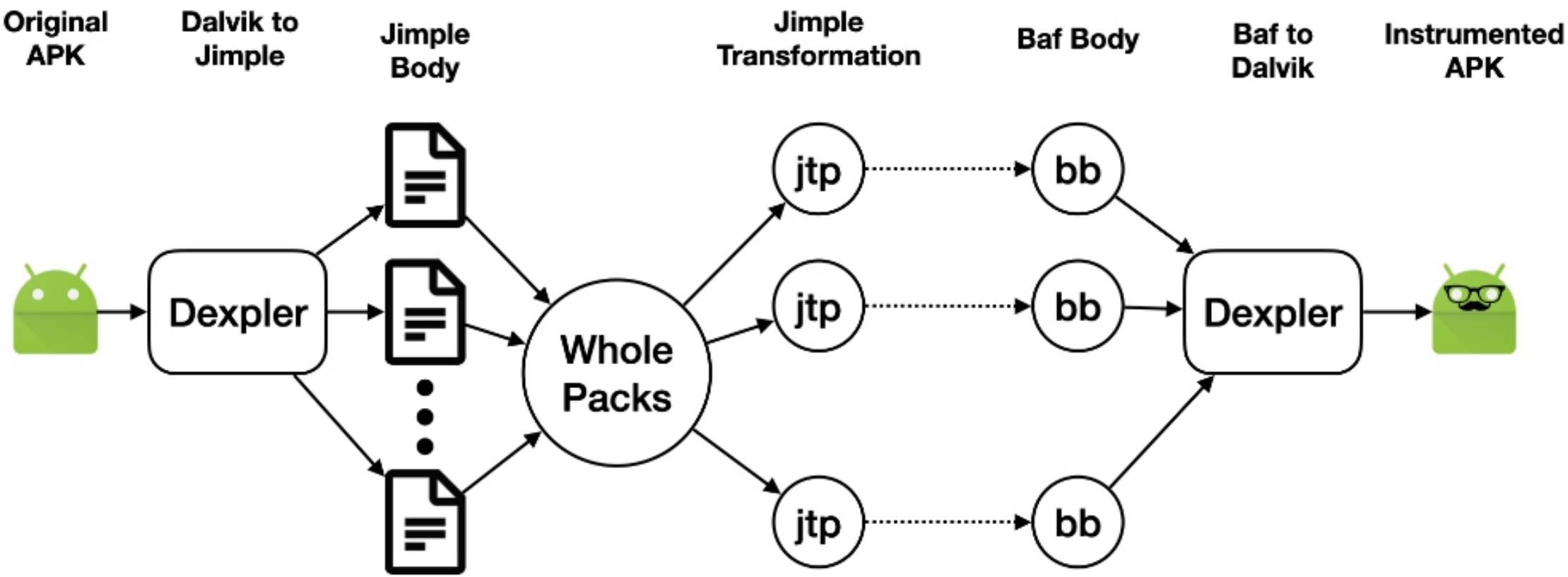
- You need to **setup** environment:

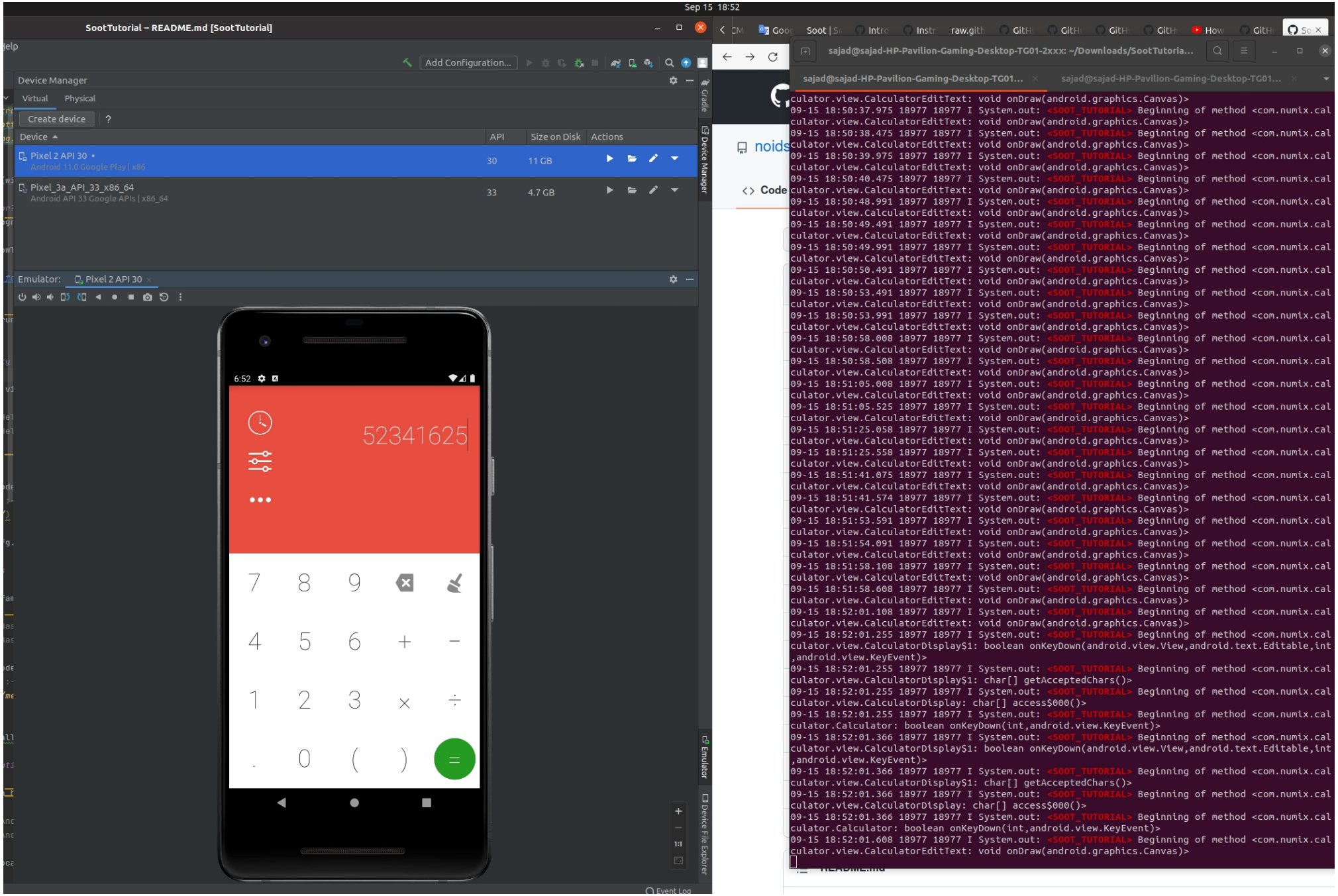
https://github.com/noidsirius/SootTutorial/tree/master/docs/Setup

How to Install Docker On Ubuntu:

https://www.youtube.com/watch?v=aMKUuaga85A


Scene
getSootClass
SootClas
SootClas
SootClas
getMethodByName
SootMethod
SootMethod
SootMethod
retrieveActiveBody
JimpleBody
getUnits
Unit
Unit
Unit
Unit

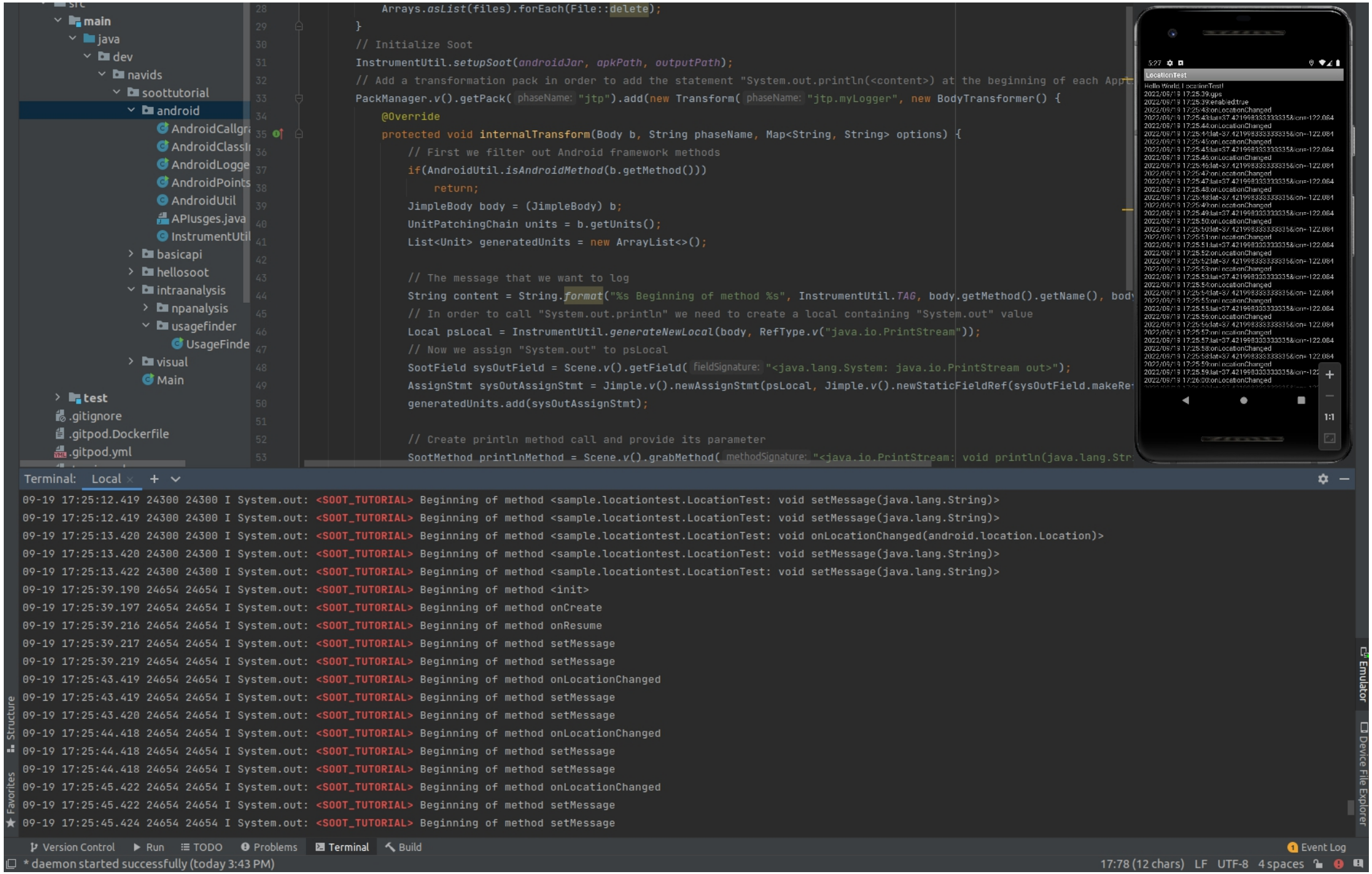

Original APK
Dalvik to Jimple
Jimple Body
Jimple Transformation
Baf Body
Baf to Dalvik
Instrumented APK
Dexpler
Whole Packs
jtp
jtp
jtp
bb
bb
bb
Dexpler


Sep 15 18:52
SootTutorial – README.md [SootTutorial]
Add Configuration...
Device Manager
Virtual
Physical
Create device
Device
API
Size on Disk
Actions
Pixel 2 API 30
Android 11.0 Google Play | x86
30
11 GB
Pixel_3a_API_33_x86_64
Android API 33 Google APIs | x86_64
33
4.7 GB
Emulator:
Pixel 2 API 30
6:52
52341625
7 8 9
4 5 6 + −
1 2 3 × ÷
. 0 ( )
=
sajad@sajad-HP-Pavilion-Gaming-Desktop-TG01-2xxx: ~/Downloads/SootTutoria...
sajad@sajad-HP-Pavilion-Gaming-Desktop-TG01...
sajad@sajad-HP-Pavilion-Gaming-Desktop-TG01...
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:50:37.975 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:50:38.475 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:50:39.975 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:50:40.475 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:50:48.991 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:50:49.491 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:50:49.991 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:50:50.491 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:50:53.491 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:50:53.991 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:50:58.008 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:50:58.508 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:51:05.008 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:51:05.525 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:51:25.058 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:51:25.558 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:51:41.075 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:51:41.574 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:51:53.591 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:51:54.091 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:51:58.108 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:51:58.608 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:52:01.108 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>
09-15 18:52:01.255 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorDisplay$1: boolean onKeyDown(android.view.View,android.text.Editable,int
,android.view.KeyEvent)>
09-15 18:52:01.255 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorDisplay$1: char[] getAcceptedChars()>
09-15 18:52:01.255 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorDisplay: char[] access$000()>
09-15 18:52:01.255 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.Calculator: boolean onKeyDown(int,android.view.KeyEvent)>
09-15 18:52:01.366 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorDisplay$1: boolean onKeyDown(android.view.View,android.text.Editable,int
,android.view.KeyEvent)>
09-15 18:52:01.366 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorDisplay$1: char[] getAcceptedChars()>
09-15 18:52:01.366 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorDisplay: char[] access$000()>
09-15 18:52:01.366 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.Calculator: boolean onKeyDown(int,android.view.KeyEvent)>
09-15 18:52:01.608 18977 18977 I System.out: <SOOT_TUTORIAL> Beginning of method <com.numix.cal
culator.view.CalculatorEditText: void onDraw(android.graphics.Canvas)>

Sensitive APIs:

onInterceptTouchEvent
<init>
onRelease
draw
ondraw
run
startUpdate
setPrimaryItem
finishUpdate
writeToParcel

...


main
java
dev
navids
soottutorial
android
AndroidCallgr
AndroidClassI
AndroidLogge
AndroidPoints
AndroidUtil
APIusges.java
InstrumentUtil
basicapi
hellosoot
intraanalysis
npanalysis
usagefinder
UsageFinde
visual
Main
test
.gitignore
.gitpod.Dockerfile
.gitpod.yml
Arrays.asList(files).forEach(File::delete);
}
// Initialize Soot
InstrumentUtil.setupSoot(androidJar, apkPath, outputPath);
// Add a transformation pack in order to add the statement "System.out.println(<content>) at the beginning of each Appl
PackManager.v().getPack(phaseName: "jtp").add(new Transform(phaseName: "jtp.myLogger", new BodyTransformer() {
@Override
protected void internalTransform(Body b, String phaseName, Map<String, String> options) {
// First we filter out Android framework methods
if(AndroidUtil.isAndroidMethod(b.getMethod()))
return;
JimpleBody body = (JimpleBody) b;
UnitPatchingChain units = b.getUnits();
List<Unit> generatedUnits = new ArrayList<>();
// The message that we want to log
String content = String.format("%s Beginning of method %s", InstrumentUtil.TAG, body.getMethod().getName(), body
// In order to call "System.out.println" we need to create a local containing "System.out" value
Local psLocal = InstrumentUtil.generateNewLocal(body, RefType.v("java.io.PrintStream"));
// Now we assign "System.out" to psLocal
SootField sysOutField = Scene.v().getField(fieldSignature: "<java.lang.System: java.io.PrintStream out>");
AssignStmt sysOutAssignStmt = Jimple.v().newAssignStmt(psLocal, Jimple.v().newStaticFieldRef(sysOutField.makeRe
generatedUnits.add(sysOutAssignStmt);
// Create println method call and provide its parameter
SootMethod printlnMethod = Scene.v().grabMethod(methodSignature: "<java.io.PrintStream: void println(java.lang.Str
LocationTest
Hello World, LocationTest!
1:1
Terminal: Local
09-19 17:25:12.419 24300 24300 I System.out: <SOOT_TUTORIAL> Beginning of method <sample.locationtest.LocationTest: void setMessage(java.lang.String)>
09-19 17:25:12.419 24300 24300 I System.out: <SOOT_TUTORIAL> Beginning of method <sample.locationtest.LocationTest: void setMessage(java.lang.String)>
09-19 17:25:13.420 24300 24300 I System.out: <SOOT_TUTORIAL> Beginning of method <sample.locationtest.LocationTest: void onLocationChanged(android.location.Location)>
09-19 17:25:13.420 24300 24300 I System.out: <SOOT_TUTORIAL> Beginning of method <sample.locationtest.LocationTest: void setMessage(java.lang.String)>
09-19 17:25:13.422 24300 24300 I System.out: <SOOT_TUTORIAL> Beginning of method <sample.locationtest.LocationTest: void setMessage(java.lang.String)>
09-19 17:25:39.190 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method <init>
09-19 17:25:39.197 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method onCreate
09-19 17:25:39.216 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method onResume
09-19 17:25:39.217 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method setMessage
09-19 17:25:39.219 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method setMessage
09-19 17:25:43.419 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method onLocationChanged
09-19 17:25:43.419 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method setMessage
09-19 17:25:43.420 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method setMessage
09-19 17:25:44.418 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method onLocationChanged
09-19 17:25:44.418 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method setMessage
09-19 17:25:44.418 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method setMessage
09-19 17:25:45.422 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method onLocationChanged
09-19 17:25:45.422 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method setMessage
09-19 17:25:45.424 24654 24654 I System.out: <SOOT_TUTORIAL> Beginning of method setMessage
Structure
Favorites
Emulator
Device File Explorer
Version Control
Run
TODO
Problems
Terminal
Build
Event Log
* daemon started successfully (today 3:43 PM)
17:78 (12 chars)
LF
UTF-8
4 spaces

Soot Packages

- https://santos.cs.ksu.edu/bandera/internal/sootdocs/overview-summary.html

- https://www.sable.mcgill.ca/soot/doc/soot/util/cfgcmd/CFGToDotGraph.html

Your Assignment

- a) **Collect sensitive API usage information.**

Given an Android application, your job is to perform static analysis to extract sensitive API usage information, and dump the info into a text file.

- Each line should read: API_name: frequency: residing functions
- For example: ***getLastLocation:2:foo(),bar()*** means the sensitive API *getLastLocation()* is called twice within the whole application, in functions *foo()* and *bar()* repectively.

- b) **Control-flow graph printing**. For each function within the Android app, please print out its control-flow graph and