**Lab 4: Android Application Development**

**Objective:** Develop an application and dynamically reverse it.

**References:** <https://www.androidauthority.com/create-android-app-in-10-days-687960/>  
<https://ibotpeaches.github.io/Apktool/>  
<http://www.ninoishere.com/frida-learn-by-example/>  
<https://www.frida.re/>  
<https://www.frida.re/docs/android/>  
<https://www.frida.re/docs/javascript-api/#java>  
<https://developer.android.com/studio/command-line/logcat>

**Due Date:**

**TASKS**

1. Install Android Studio on your desktop
2. Create an application that takes input from the user and stores it on the device filesystem.
3. Build, sign, and install the application on your device (you can do all this from inside Android Studio).
4. Statically reverse your created apk and find the function in smali that writes the user-inputed data to the filesystem (hint – it’s easier to find this name if you give the function an easy find name when you write the app).
5. Install Frida server on the device
6. Use Frida to dynamically inject code (maybe a print statement) into the running application. You can use logcat from the command line of the android device to display the injected code

**Write-up (limit 2 sheets)**

1. Demonstrate that you completed the above tasks.
2. How could you use Frida to assess the security of an application?

**USEFUL ADB SHELL COMMANDS**

**#Launch Frida and an app**frida -U --no-pause -f com.<appname> -l js\_script.js -o output\_from\_hook.txt  
 **#enter into command shell on device**$ adb shell   
 **#once on device, elevate to root level**$ su

**#printing to the console in JavaScript**console.log("some text”);  
 **#Search for text string in files recursively from the home directory**$grep -Hrn 'invoke-' .  
 **#get list of commands you can run:**$ adb shell cmd package  
 **#show all third party packages installed:**$ adb shell pm list packages -3  
 **#Get apk from phone**$adb shell pm list packages -3  
$adb shell pm path com.example.someapp  
$adb pull /data/app/com.example.someapp-2.apk path/to/desired/destination  
 **#Find files modified since certain date/time** $touch -d "2017-03-15T10:25:00" data\_marker  
 $find . -newer data\_marker