**Lab 2: Android Application Analysis**

**Objective:** Analyze an application and it’s associated data on your device

**References:** <https://www.frida.re/>  
<https://ibotpeaches.github.io/Apktool/>  
<https://github.com/skylot/jadx>  
<https://apkscan.nviso.be/>

**Due Date:**

**TASKS**

1. Make sure that you have Discord installed on your phone and that you have sent and received some data to a partner
2. Install apktool on your desktop
3. Use **adb** to pull back the Discord .apk from the phone to the desktop for analysis
4. Unzip the application using unzip or winzip
5. Decompile the Discord apk using apktool and look around the smali code
6. Re-build the Discord apk using apktool and digitally sign it using jarsigner
7. View the Discord apk in jadx

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

1. Demonstrate that you completed the above tasks.
2. Where did Discord store it’s files on the phone? What file types are they? Can you read them? Why or why not?
3. After you unzipped the application, how many directories and files do you see inside the apk file? Can you read the AndoridManifest file after unzipping? Can you read classes.dex after unzipping? Why or why not?
4. What types of permissions does Discord appear to have? What types of information is it designed to collect?
5. Does discord use any third-party libraries? If yes, then what are they?
6. Can you find a website associated with this application?
7. How challenging is it to modify the .smali code and re-deploy a tampered application? Do some open source research to find out if this is a common practice. Are there any legitimate reasons for doing this?
8. What things would you look for to ensure the application you are installing on your android phone have not been tampered?
9. What kinds of information could an adversary learn about the application from the .smali code?

**USEFUL ADB SHELL COMMANDS**

**#enter into command shell on device**$ adb shell

**#once on device, elevate to root level**$ su

**#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