Section 2: BONUS Lab – Android Information Pull

Objectives

- Interact with an Android device to access data that the tools may miss
- Gain experience with ADB and accessing information from Android devices

Exercise Preparation

(Note: Not everyone has an Android device, which is why you will see another lab like this for iPhone in section 3. If you didn't bring an Android to class and you don't have access to one, your instructor may have one available for you. If that is not an option, we suggest taking this with you and trying it on a test device at some point.)

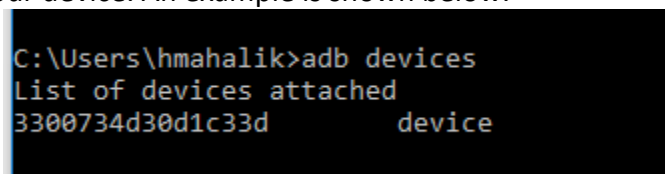
1. *If not done so already, start your FOR585 WIN 10 ENT VM.*

2. *Log in to the Windows FOR585 SIFT.*
- *LOGIN =* **`FOR585`**
- *PASSWORD =* **`forensics`**

Exercise: Answer the Following Questions

Launch a command prompt by going to the Windows Search bar and typing CMD or pressing the Windows Key + R and typing CMD. From here, type the following commands below and record your answers. NOTE: There are no answers because every device will be different. The goal is for you to get more experience using command line solutions to pull specific artifacts of interest.

1. Type **adb devices**
   Ensure you see that your Android is attached. If not, make sure you allow connection to the computer by selecting “allow” on your device. An example is shown below.



2. Type **adb.exe shell service list**
   How many services were found on your device? List three of them.

   _____

   _____

   _____

3. Type **adb.exe shell dumpsys wifi**
   Is Wi-Fi enabled?
   Can you find a Wi-Fi connection?
   What was the last BSSID used?
   Is Wi-Fi sharing enabled?

   _____

   _____

   _____

4. Type **adb.exe shell dumpsys usagestats**
   List three third party applications that were used on the device including the last time used.

   _____

   _____

   _____

Exercise: Key Takeaways

- **Although the tools often pull data for you from Android devices, you may come across an unsupported device that requires manual interaction.**
- **You can extract a good amount of information from ADB!**