Section 3: BONUS Lab – iOS Device Information Pull

Objectives

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

Exercise Preparation

(Note: Not everyone has an iOS device, which is why this is a bonus lab. If you didn't bring an iOS device 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, navigate to the libimobiledevice directory in your VM at C:\Forensic Program Files\libimobiledevice. You may have to select "Trust" on the iOS device. You can try to use **idevicepair pair** to pair it via CLI.

1. Type **idevice_id.exe -l**
   What is the 40-digit UDID of the attached device?

   _____

   _____

2. Type **ideviceinfo**
   Is the device activated?
   What is the PhoneNumber?
   What is the Time Zone?
   What iOS version is running on the device?

3. Type **idevicename**
   What is the DeviceName?

4. Type **idevicecrashreport –e <path for output>**
   List three applications or services that were reported.

Exercise: Key Takeaways

- **Although the tools often pull data for you from iOS devices, you may come across an unsupported device that requires manual interaction.**
- **You can extract a good amount of information from even locked iOS devices using tools like libimobiledevice**