Mobile Device Forensics

Digital Forensics

What is special about MDF?

- Mobile Device Forensics are computer forensics with some special challenges
- Androids are Linux-based, Apples are IOS, there are other weirdos out there
- The device vendors are much more focused on device security and privacy than OS vendors for Windows or ChromeOS, even MacOS is easier to do forensics on than IOS
- The hardware is not usually accessible in a useful way for device imaging although there are jailbreaks that may already be done to the device being investigated
- Far more of what is stored on a mobile device is encrypted than is typical for desktop or server computers
- They are highly network-dependent in most uses and even complete device access doesn't necessarily give you access to information stored in cloud accounts or apps
- Some apps that would be of interest to us (messaging and file sharing apps) are specifically written to encrypt and protect their data from people like us

How can we get data from a mobile device?

- Unlocking the user interface is the major goal, otherwise we have to rely on jailbreaks, vulnerabilities, and zero-days to try to get in
- Fingerprint scan, facial recognition, PIN codes and other UI locks usually require cooperation from the individual who uses the device
- Brute forcing PIN codes is an option in some cases, e.g. https://santoku-linux.com/howto/mobile-forensics/how-to-brute-force-android-encryption/
- Device backups on user computers or in the cloud may be useful although unlocking them can be as much of a challenge as unlocking the device
- If what we want is to see what the device is being used for, as opposed to what is stored on it, mitm proxy and network snooping may be helpful to see what the device is communicating with although communication content may not be usable due to encryption
- MDM software may provide access to a device, and may provide useful data about what apps are in use on the device, where it has been, and when it was there

Device Examination

- If you have access to the UI
  - review the apps
  - identify ones relevant to the investigation you are doing
  - screenshot, screenshot, screenshot
  - check for cloud account settings in cloud apps
  - check for password managers
  - check for filing apps, multimedia apps, communications apps, social networking apps
  - pull location history if relevant
- If you don't have access to the UI, see previous topic re: challenges

Tools

- There are both free and commercial tools to help with mobile device forensics
- Jailbroken IOS devices can be acquired using the Magnet Acquire image acquisition tool, Belkasoft X, and others like them, providing full filesystem extraction
- iLEAPP is a good example tool for examining IOS images, see https://www.youtube.com/watch?v=fEYV5vVAdu4&ab_channel=13Cubed for an overview and demo of using it on an IOS device
- Major forensic software vendors provide mobile device forensic capabilities as part of their software suites, e.g. Belkasoft has extensive analysis tools and acquisition tools for mobile devices, see