SANS Cyber Camp



Domenica Lee Crognale

About Me

Lee Crognale

- Cybersecurity Engineer at ManTech
- SANS Certified instructor and Course Author for FOR585
- BS in Business Administration/MS in Cybersecurity MGMT
- Involved with InfoSec/Forensics for 15 years
  - **LE / Intel support – case work**
  - **Cybersecurity**
  - **Research/Instruction**

Copyright @2020 Lee Crognale All Rights Reserved

Do you like to solve puzzles and figure out how things work?

- MOBILE DEVICE FORENSIC ANALYSTS
- APPLICATION DEVELOPERS
- SECURITY RESEARCHERS

What we will cover

- Accessing user data via backup methods
  - iOS/Android
- Locating the data of interest
- Limited access to data: Rooting and jailbreaking and why they matter
- What kind of artifacts can you find and how to access and review the data
- A few FREE tools/methods to get you started!

Copyright @2020 Lee Crognale, All Rights Reserved

Why are we doing this?

- Almost everyone has access to a smartphone
- Mobile operating systems have numerous files that track every aspect of a phone's behavior
- Even simple, seemingly mundane items are tracked:
  - Turning your phone or or off
  - How you log into your device (pin, passcode, swipe, biometrics)
  - Network connections
  - Plugging your device in to charge/transfer data, play music, ask for directions (Android Auto/Apple Carplay
  - Locations
- Third-party applications are specifically designed to create/store user data.
  - Even more items tracked which can be investigated

Copyright @2020 Lee Crognale, All Rights Reserved

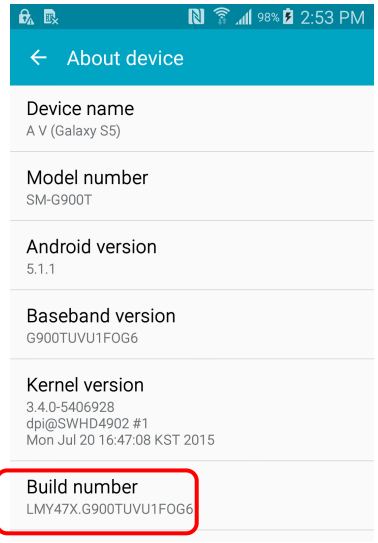
Getting Started:

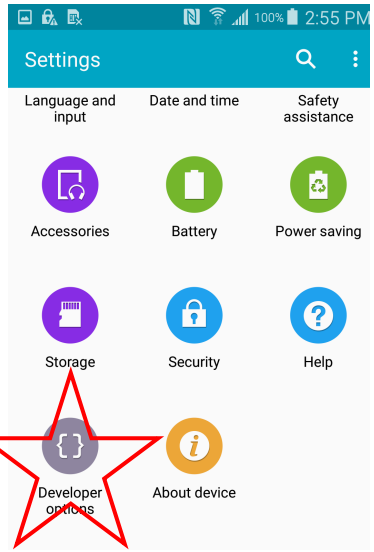
So what phones will this work on?

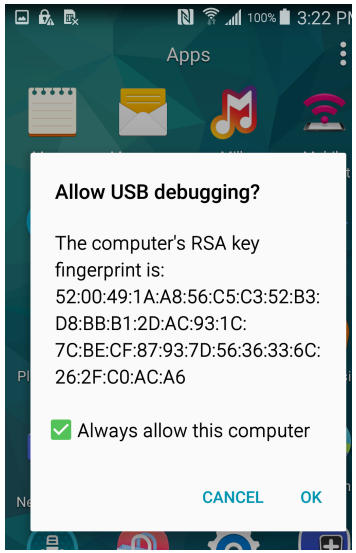


Prepare your computer and your device: ANDROID

- *Install ADB Platform tools on your host machine*
- *Configure device settings to allow for backup creation*
- *Using ADB commands, backup your device*
- ***IMPORTANT:*** *Following the backup* ***turn OFF USB debugging***







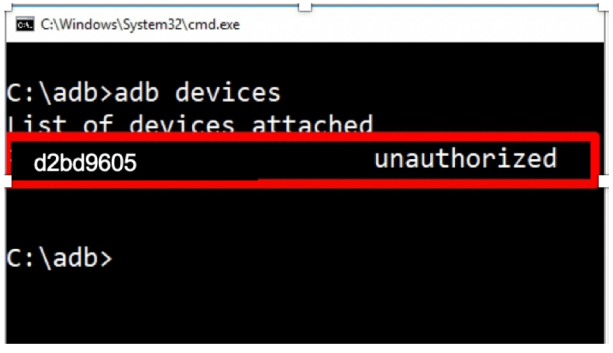
Copyright @2020 Lee Crognale, All Rights Reserved

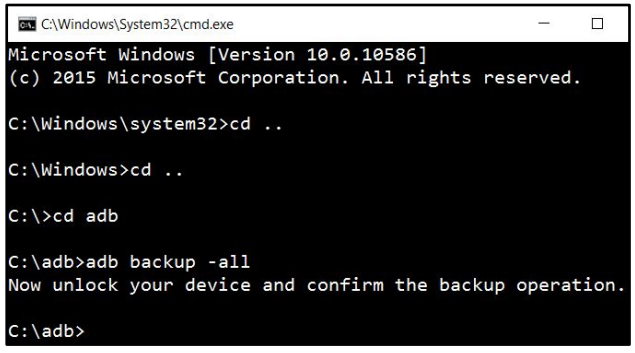
Create a backup: ANDROID

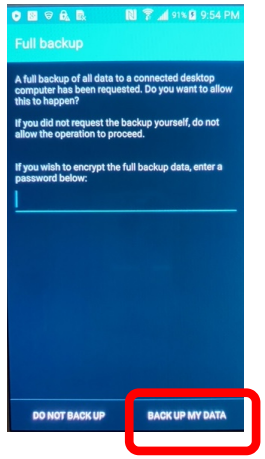
- Open a command prompt
- Navigate to the directory where adb tools is installed
- If you trusted your host machines, issuing the command: **adb devices** will return your serial number
- Issue the command:

  adb backup –all
- Once issues you will need to select **"backup my data"** on your phone
- Do not choose to encrypt your backup if you wish to use Andriller to dump the .ab file to a folder







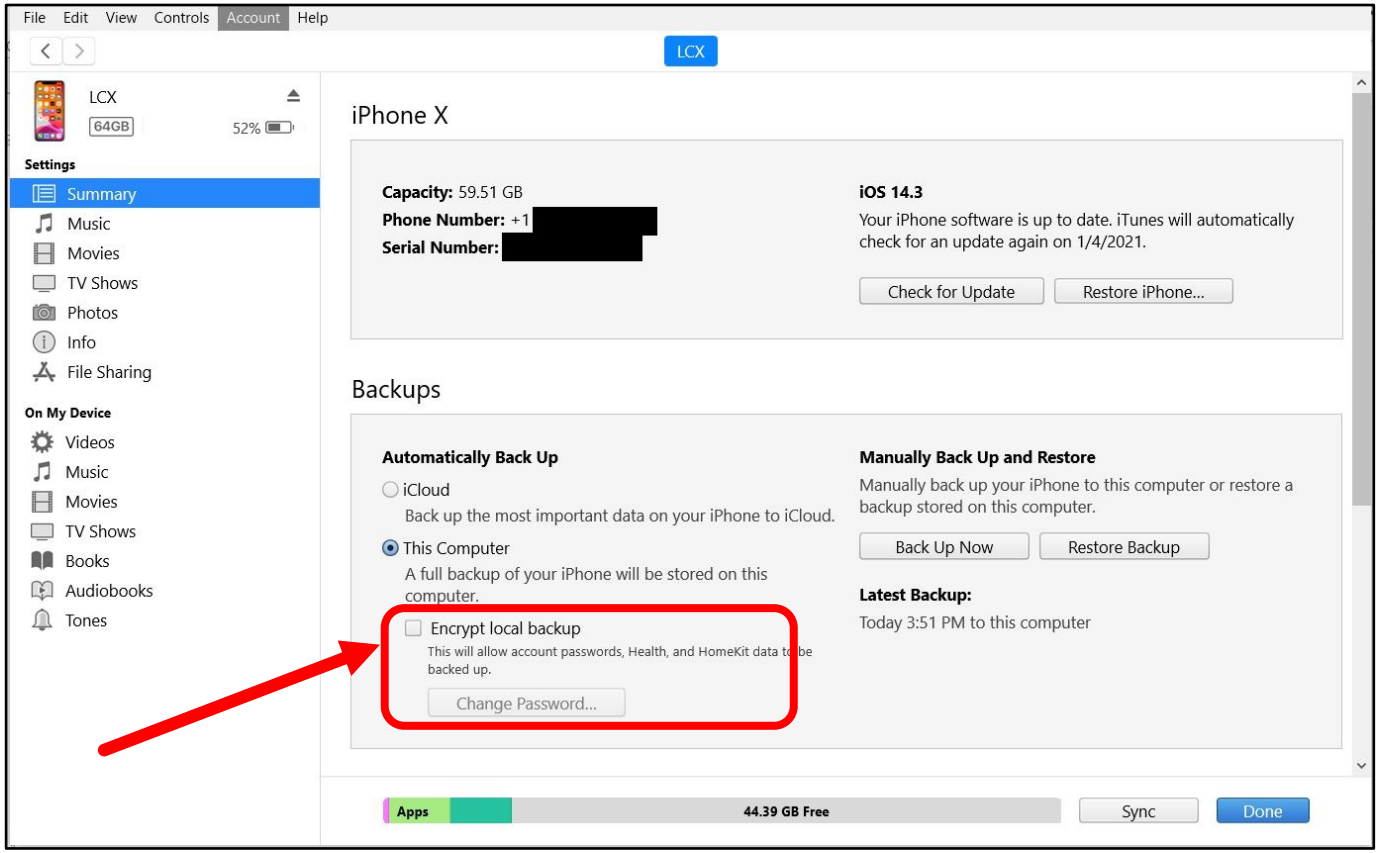


Prepare your computer and your device : iOS

- *Install iTunes on your Windows host or use Finder window on Mac OS*
- *Trust your computer (enter your device passcode)*
- *Choose to encrypt backup (get access to more data Homekit, Health, Passwords)*
  - for iOS 13+ and later you **MUST** encrypt the local backup in order to extract Calls, Health, Safari History, Maps and Wallet.
  - If you encrypt the backup, you will also need a utility for decryption
- REMEMBER your password! You will need it.

Copyright @2020 Lee Crognale, All Rights Reserved

Create a backup: iOS



Copyright @2020 Lee Crognale, All Rights Reserved

Open the backup and start digging…ANDROID

Andriller

- *Andriller (free) will unpack android backup (.ab) files and can analyze a handful of apps*
  - ***Download Andriller from Github***
  - ***Extract the zip file***
  - ***Open a command prompt and navigate to the extracted master repo***
  - ***Install dependencies***
  - ***Run the GUI***

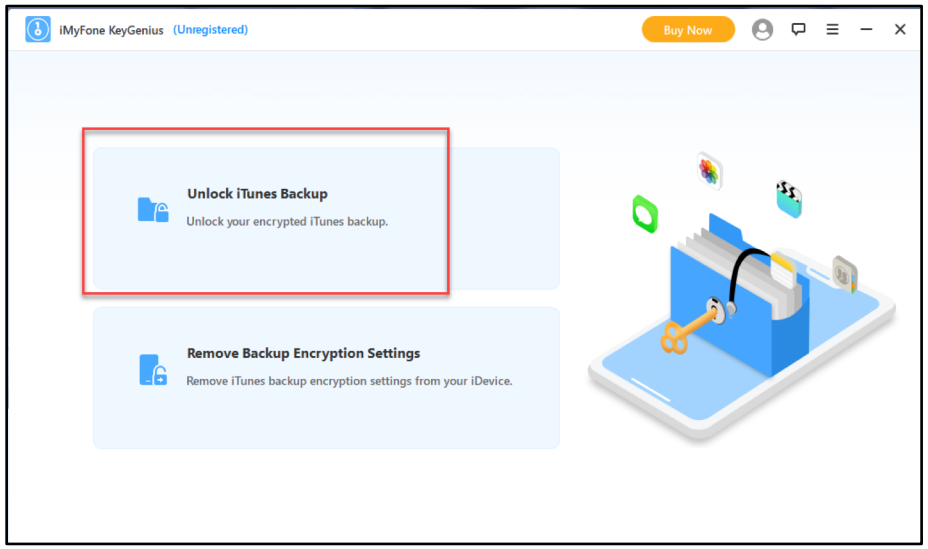
Autopsy

- *Autopsy (free) will mount the uncompressed .ab archive so you can view the contents of each native and third-party application folder*

Copyright @2020 Lee Crognale, All Rights Reserved

Open the backup and start digging…iOS

- ***iBackupBot*** *(free) can be used to view iTunes backups*
- *Encrypted backups must be decrypted (AnyTrans, iMyFone)*
- *Access to Native iOS and third-party applications*



Copyright @2020 Lee Crognale, All Rights Reserved

So where is all of my data?

Android

- *In an Android backup, the Native Android applications and third-party applications are located in the "apps" folder under <App_Name>*
  - ***Ex:***
    - ***apps/kik.android***
    - ***shared/kik.android***

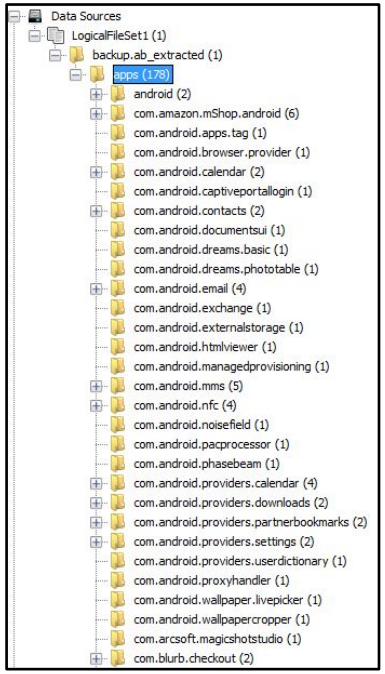
iOS

- *In iBackupBot, Most Native to iOS apps can be found in* ***System Files > HomeDomain > Library***
- *Look for Third-party applications in the Application(s) folder* ***User App Files and/or App Group Files*** *in iBackupBot under the <App_Name> of interest*
  - ***Ex:***
    - ***com.kik.chat***
      group.com.kik.chat

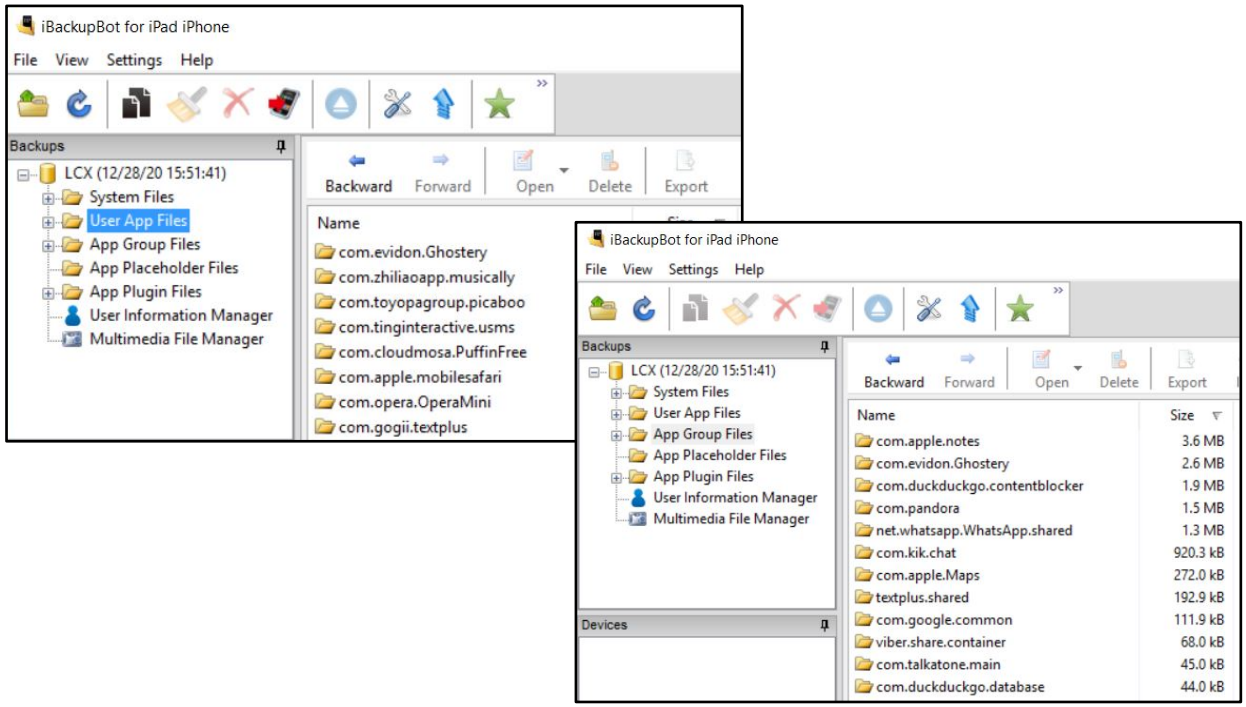
Copyright @2020 Lee Crognale, All Rights Reserved

So where is all of my data?

Android



iOS



- *SAD REALITY: while we can still see a plethora of user-created and system related files, we are getting less access to the data we REALLY care about.*

Copyright @2020 Lee Crognale, All Rights Reserved

Proceed with CAUTION

But what if I want MORE?

ROOTS and JAILBREAKS: Modifying the OS in such a way that unofficial/unsigned code and applications can be installed and run

This can permanently brick devices and will VOID all warranties.

Android (root)

- Also allows for elevated admin or root level(super user) privileges
- Soft/shell temporary roots
- Full roots

iOS (jailbreak)

- Untethered
- Semi-untethered
- Semi-tethered
- Tethered

Copyright @2020 Lee Crognale, All Rights Reserved

Proceed with CAUTION

Android Considerations

- Nice to have a test device that has a PERMANENT root
- Newer devices and certain manufacturers/carriers are more restrictive
  - International models usually have less restrictions
- **Requires an unlocked bootloader**
  - Bootloaders can be locked by manufacturer or carrier
    - Purpose of the Bootloader: checks digital signature of original ROM so only approved Operating System is allowed to boot
  - Can be unlocked but will likely void warrantees
- **Do your research before you buy/brick!**
  - You need exact matches for make/model/firmware and build number is most cases.

Copyright @2020 Lee Crognale, All Rights Reserved

Proceed with CAUTION

iOS Considerations

- Do you have a device that is vulnerable to checkm8?
  - Affects devices with A5 – A11 chips
  - May require that you update the firmware to the latest available version
  - Checkra1n jailbreak then access device via SSH
    - Support for iPhone models 5s through X
- New hardware is not supported so we're back to jailbreaks that exploit firmware vulnerabilities
  - https://theiphonewiki.com/wiki/Jailbreak
- iOS is faster at phasing out hardware/software combos
  - Don't expect these vulnerable checkm8 devices to be around forever
- Applications require (a very current) minimum firmware version for installation

Copyright @2020 Lee Crognale, All Rights Reserved

Now what do we have here…

- With root, you can access physical partitions (including the **user data** partition where all of our app related data is stored) using ADB commands
- A jailbreak gives you access to the full filesystem on iOS devices which can then usually be accessed with the help of the added AFC2 service
- When developers say "don't include my data in the backup", it does not apply here, all that missing data is now accessible

Start Researching

- Start using certain features of your smart phone or an application of interest
- Generate unique user data (make calls, send messages, etc.)
- Create a backup
- Look for folders that correspond to that application package name in the backup
- If you can see a database or other files that are populated with data, start investigating!
- Generate more data to see how the application behaves: create, copy, send, receive, save, bookmark, delete, search, etc.
- EVERYTHNG you do creates unique artifacts!

Copyright @2020 Lee Crognale, All Rights Reserved

Resources

https://for585.com/phonelinks

- **Adb Platform Tools:** https://developer.android.com/studio/releases/platform-tools
- **Andriller:** https://github.com/den4uk/andriller
- **Autopsy:** https://www.autopsy.com/download/
- **iTunes:** https://www.apple.com/itunes/
- **IBackupBot:** https://www.icopybot.com/download.htm
- **iMyFone keygenius:** https://www.imyfone.com/iphone-backup-unlocker/
- **AnyTrans:** https://www.imobie.com/anytrans/
- **iOS jailbreaks:** https://theiphonewiki.com/wiki/Jailbreak

Questions?



Lee Crognale
domenica.crognale@gmail.com
Twitter: @domenicacrognal