SANS Cyber Camp

Move Along; Nothing to See Here...Or Is There?



DOMENICA CROGNALE

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

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!

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

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

debuaaina	டி 🖳 🗋 🕅 🕅 🕅 🕅 🕅 🕅 🕅	🖬 🔂 🖳	h. 8 Ø	100% İ 2:55 PM		N 🗟 📶 10	00% 📕 3:22 PM
	← About device	Settings		Q :		Apps	
	Device name A V (Galaxy S5)	Language and input	Date and time	Safety assistance			E
	Model number SM-G900T	6	0	a	Allow	USB debugging?	?
	Android version 5.1.1	Accessories	Battery	Power saving	The comp fingerprin	omputer's RSA key print is:	(
	Baseband version		ß	0	52:00: D8:BB	52:00:49:1A:A8:56:C5:C3:52: D8:BB:B1:2D:AC:93:1C: 7C:BE:CE:87:93:7D:56:36:33:	3:52:B3:
	Kernel version	Storage	Security	Help	PI 26:2F:	.CO:AC:A6	J.00.00.
	dpi@SWHD4902 #1 Mon Jul 20 16:47:08 KST 2015		71		🗹 Alw	ays allow this con	nputer
	Build number LMY47X.G900TUVU1F0G6	Developer options	About device		Ne	CANCE	L ОК

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

N 🔋 🖌 91% 🛙 9:54



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.

Create a backup: iOS

File Edit View Controls Account Help		
	LCX	
LCX ▲ 64GB 52%	iPhone X	
Settings		
🔲 Summary	Capacity: 59.51 GB	iOS 14.3
🎵 Music	Phone Number: +1	Your iPhone software is up to date. iTunes will automatically
Movies	Serial Number:	check for an update again on 1/4/2021.
TV Shows		Check for Update Restore iPhone
i Photos		
(î) Info		
🙏 File Sharing	Packups	
On My Device	Баскирз	
🛱 Videos		
Music	Automatically Back Up	Manually Back Up and Restore
Movies	◯ iCloud	Manually back up your iPhone to this computer or restore a
TV Shows	Back up the most important data on your iPhone to iCloud.	backup stored on this computer.
Books	This Computer	Back Up Now Restore Backup
Audiobooks	A full backup of your iPhone will be stored on this	Latect Rackup
1 Tones		Today 3:51 PM to this computer
	This will allow account passwords, Health, and HomeKit data to be	loady sist if it is compared
	backed up.	
	Change Password	
		~
	Apps 44.39 GB Free	Sync
4		

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

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



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

So where is all of my data?

Android



🖣 iBackupBot for iPad iPhone File View Settings Help X Backups E- LCX (12/28/20 15:51:41) Delete Backward Forward Open Export + Dystem Files 🖶 🍋 User App Files Name iBackupBot for iPad iPhone + Droup Files com.evidon.Ghostery App Placeholder Files File View Settings Help com.zhiliaoapp.musically App Plugin Files com.toyopagroup.picaboo C ĥ User Information Manager com.tinginteractive.usms Multimedia File Manager Backups com.cloudmosa.PuffinFree LCX (12/28/20 15:51:41) g com.apple.mobilesafari Backward Forward Open Delete Export 🗄 🗁 System Files com.opera.OperaMini 🗄 🧀 User App Files Name Size V com.gogii.textplus App Group Files com.apple.notes 3.6 MB App Placeholder Files a com.evidon.Ghostery 2.6 MB App Plugin Files com.duckduckgo.contentblocker 1.9 MB User Information Manager 1.5 MB com.pandora Multimedia File Manager met.whatsapp.WhatsApp.shared 1.3 MB i com.kik.chat 920.3 kB 272.0 kB acom.apple.Maps textplus.shared 192.9 kB a com.google.common 111.9 kB Devices iber.share.container 68.0 kB arcom.talkatone.main 45.0 kB 44.0 kB com.duckduckgo.database

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

iOS

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

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.

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

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!

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/iphonebackup-unlocker/
- > **AnyTrans:** https://www.imobie.com/anytrans/
- **iOS jailbreaks:** https://theiphonewiki.com/wiki/Jailbreak

Questions?



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