iPhone Backup Forensics

Kinga Kieczkowska
@kieczkowska

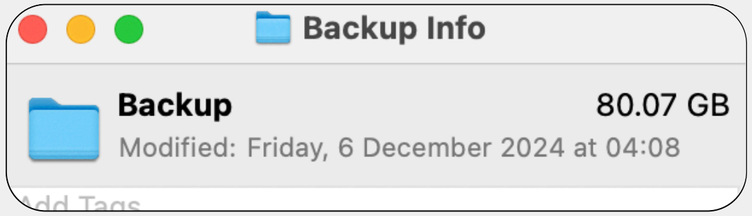
25th July 2025
Objective for the We v3.0

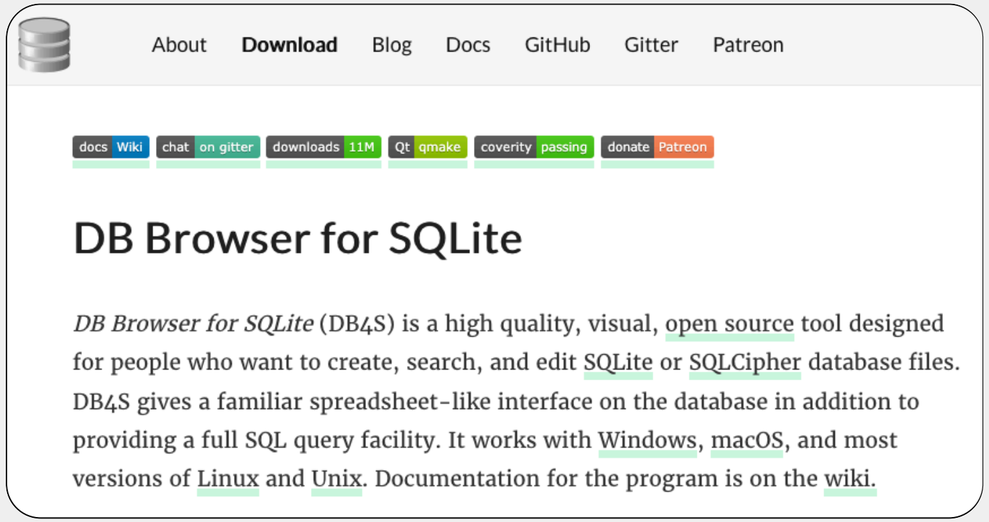
about me

- by day: cyber security consultant in security architecture at a large bank + consulting for small to medium businesses
  - used to do security at SaaS companies
- by night: macOS forensics geek
  - wrote a dissertation on thumbnail cache forensics
- love cyber & infosec community

What will you need?

- iPhone
- enough storage
- Music
- DB Browser for SQLite





What’s an iPhone backup?

A backup allows you to copy and save the information from your iPhone, iPad, or iPod touch. If you replace your device, you can use a backup to transfer your information to a new device.

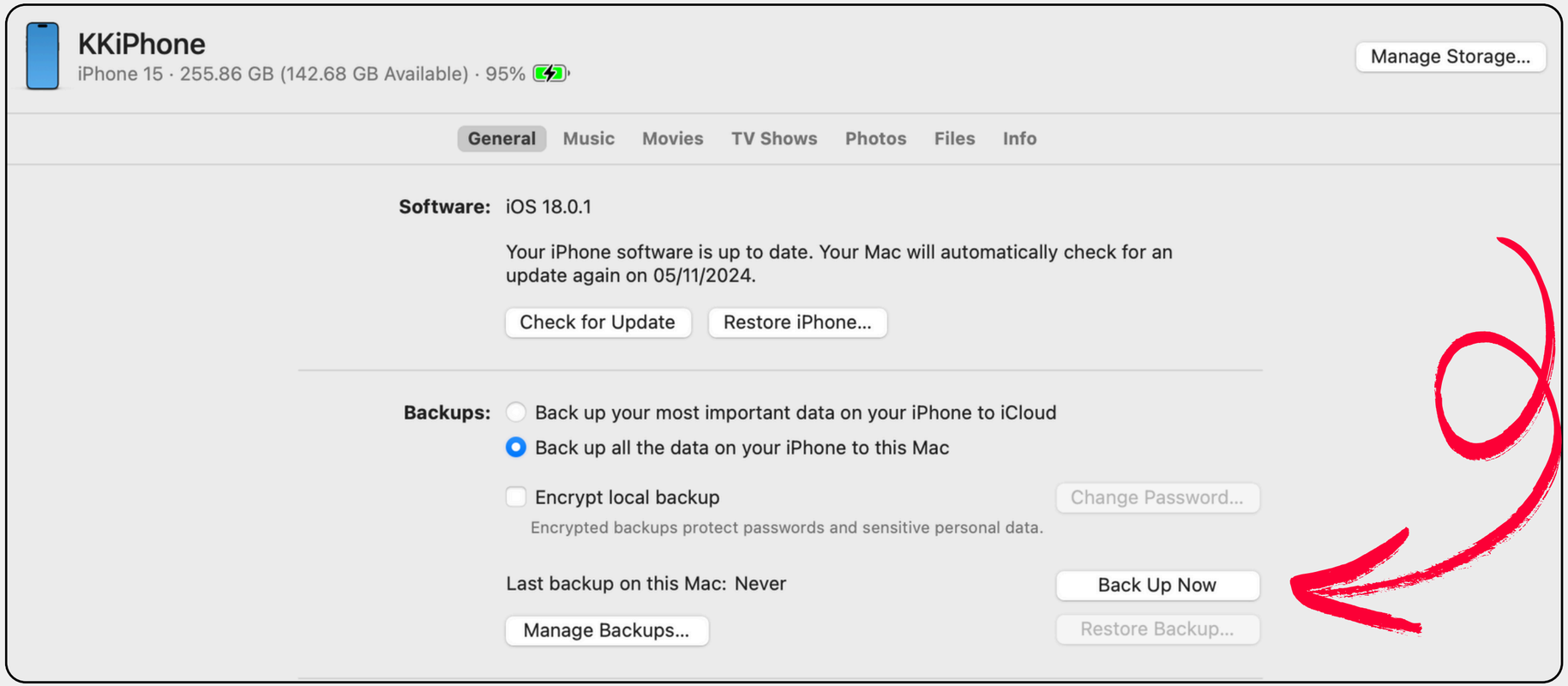
Which method is best for you?

iCloud backups

Backups from your computer

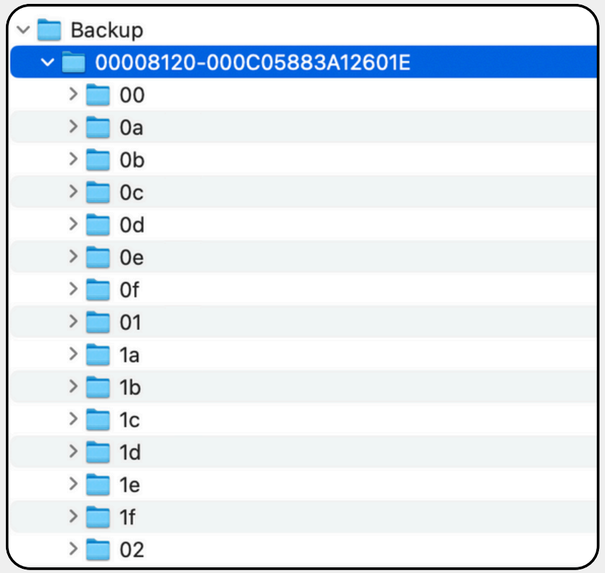
Can I use my device's backup for another kind of device?

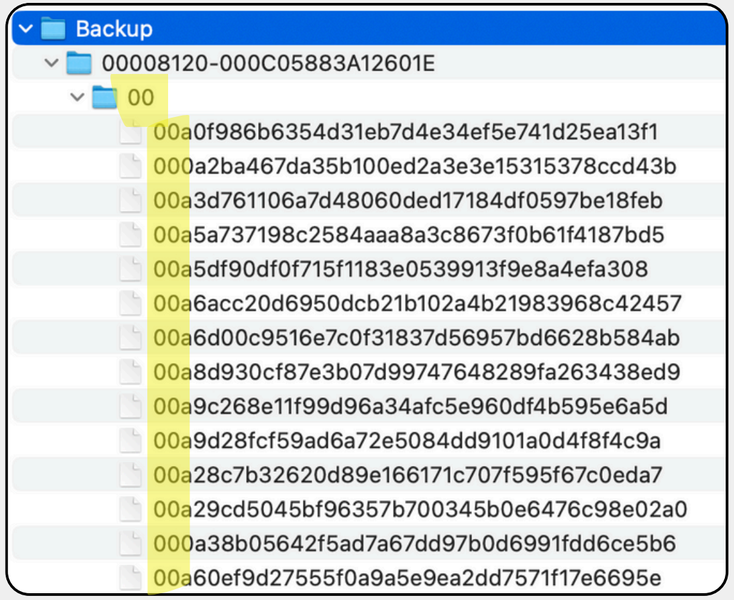
Backup basics

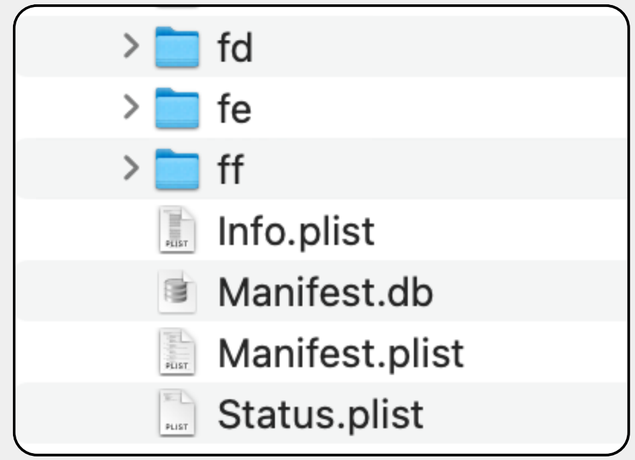


Anatomy of a backup

- located in ~/Library/Application Support/MobileSync/Backup
- name of the folder is the Unique Identifier of the device
  - 256 folders with data
  - 4 key files with info & backup metadata

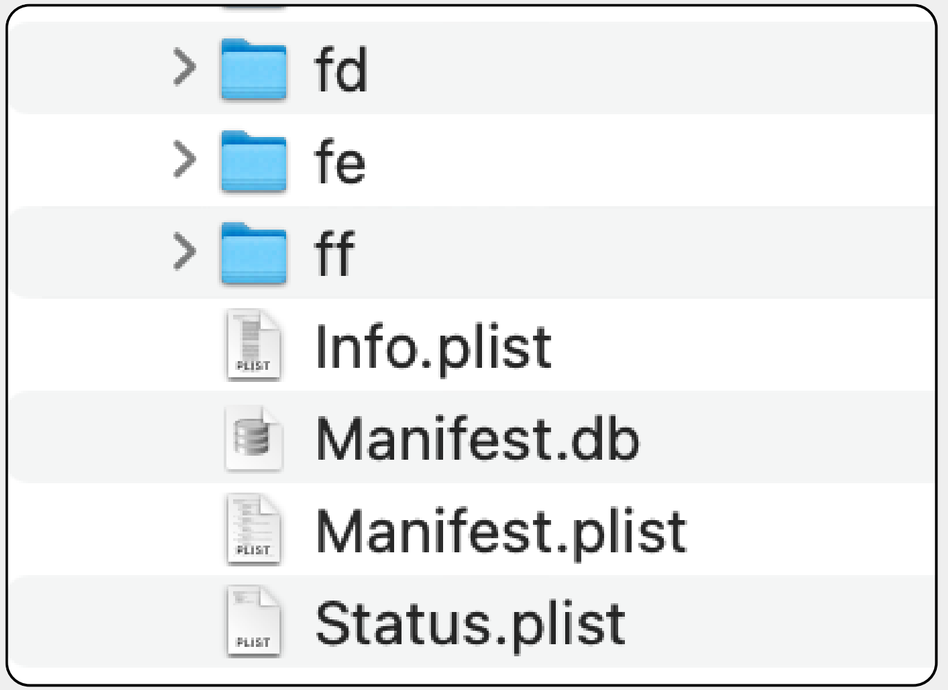






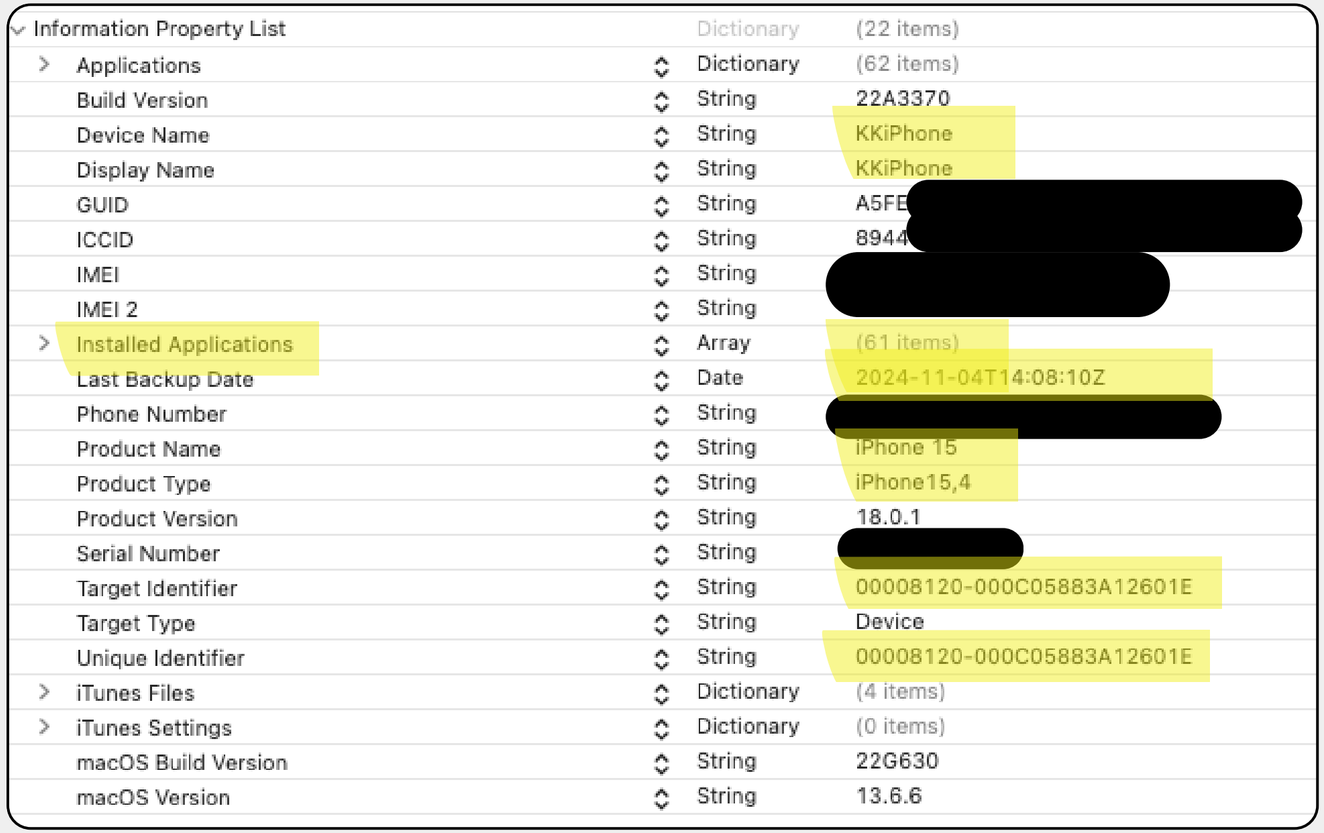
Key files

- Info.plist
- Status.plist
- Manifest.plist
- Manifest.db



Info.plist

- general information about the device and its state at the moment of backup
  - device name
  - phone number
  - UID
  - last backup **completion** date
  - list of applications installed on the device

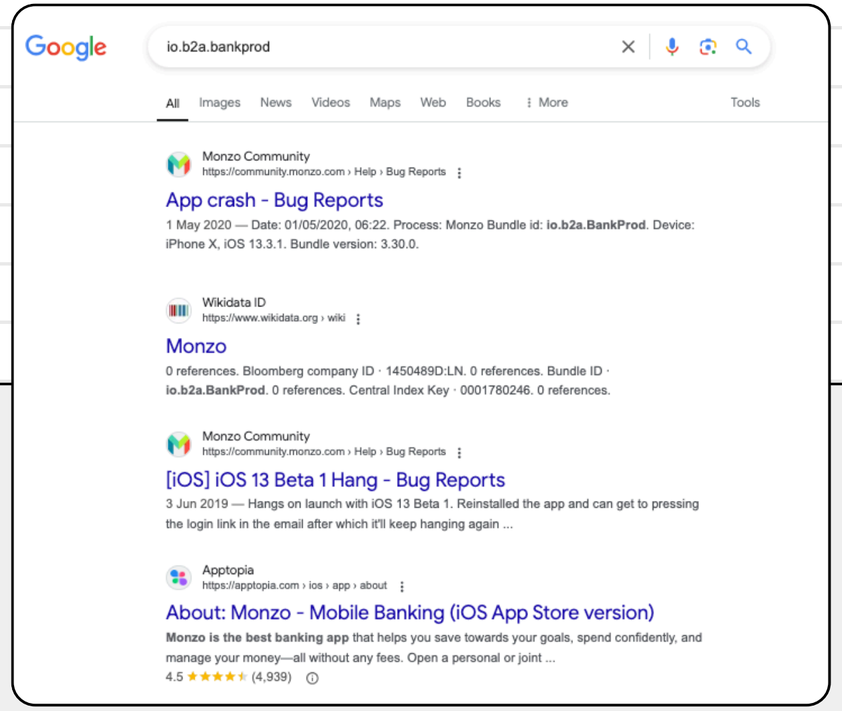


Information Property List		Dictionary	(22 items)
Applications		Dictionary	(62 items)
Build Version		String	22A3370
Device Name		String	KKiPhone
Display Name		String	KKiPhone
GUID		String	A5FE[redacted]
ICCID		String	8944[redacted]
IMEI		String	[redacted]
IMEI 2		String	
Installed Applications		Array	(61 items)
Last Backup Date		Date	2024-11-04T14:08:10Z
Phone Number		String	[redacted]
Product Name		String	iPhone 15
Product Type		String	iPhone15,4
Product Version		String	18.0.1
Serial Number		String	[redacted]
Target Identifier		String	00008120-000C05883A12601E
Target Type		String	Device
Unique Identifier		String	00008120-000C05883A12601E
iTunes Files		Dictionary	(4 items)
iTunes Settings		Dictionary	(0 items)
macOS Build Version		String	22G630
macOS Version		String	13.6.6

Info.plist - installed apps

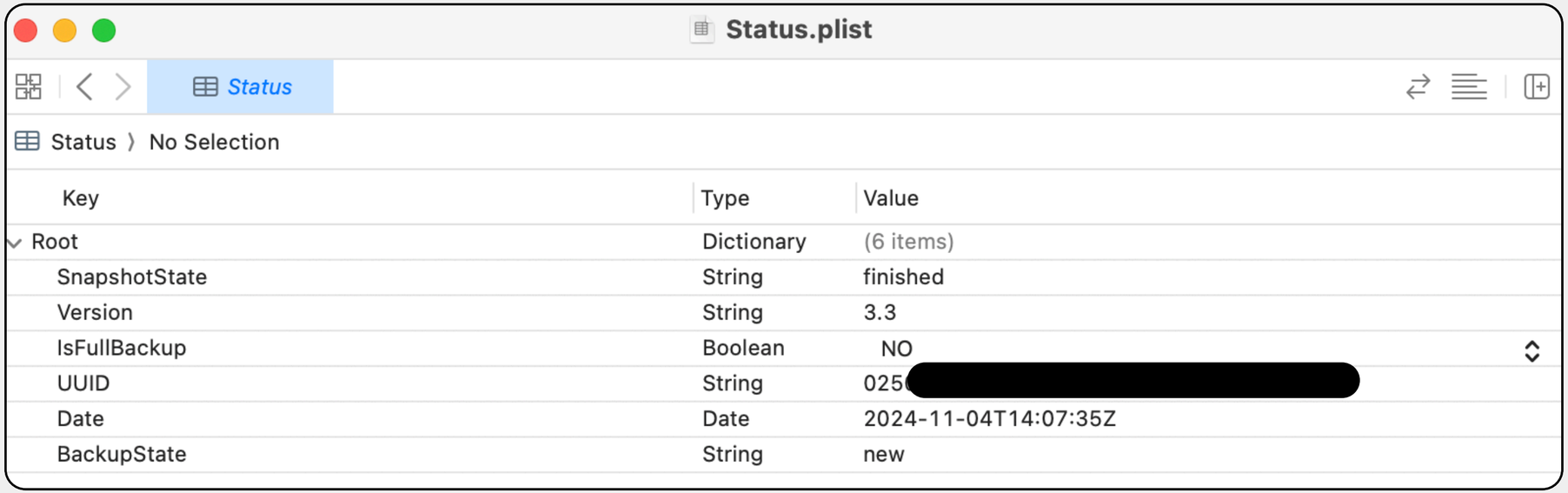
- bundle names - not always intuitive, but Google helps

Installed Applications	Array	(61 items)
Item 0	String	com.ryanair.cheapflights
Item 1	String	com.ctt.co.uk.[illegible]qgo
Item 2	String	io.b2a.BankProd
Item 3	String	[illegible].co.hsbc.hsbcukmobilebanking
Item 4	String	com.facebook.Messenger
Item 5	String	net.whatsapp.WhatsApp
Item 6	String	org.whispersystems.signal



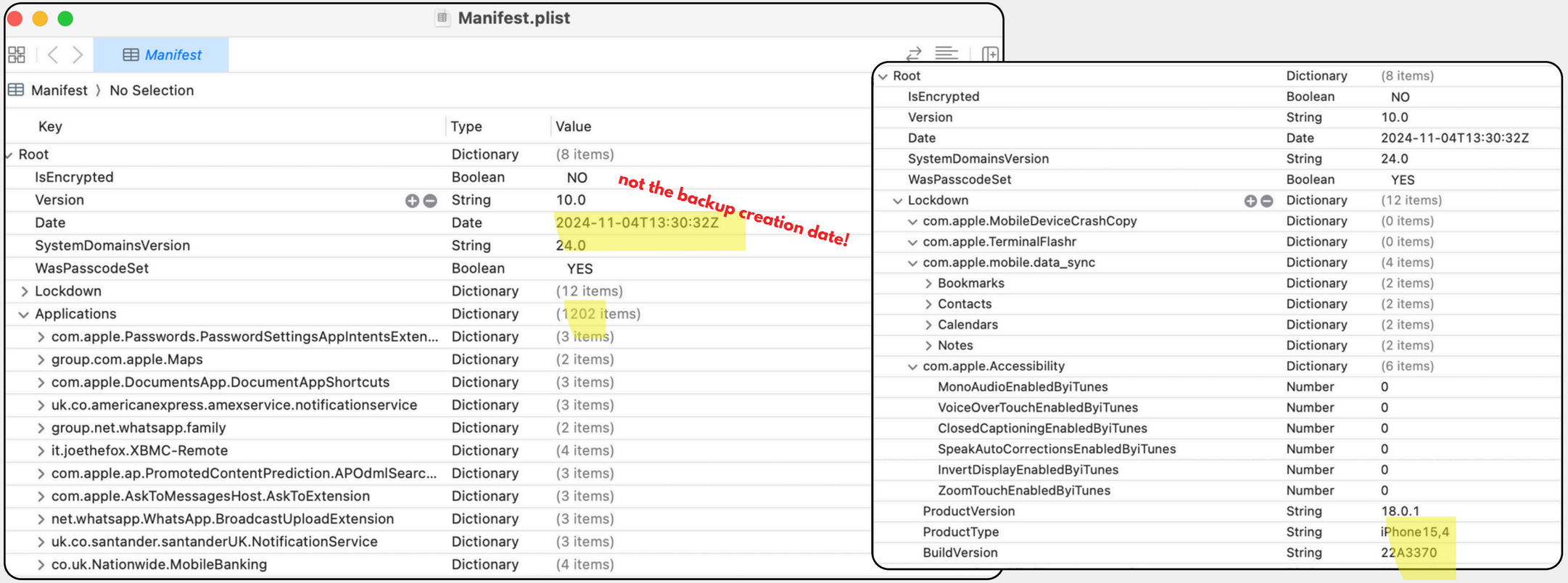
Status.plist

- general info about the backup
  - backup creation **start** date
  - backup state



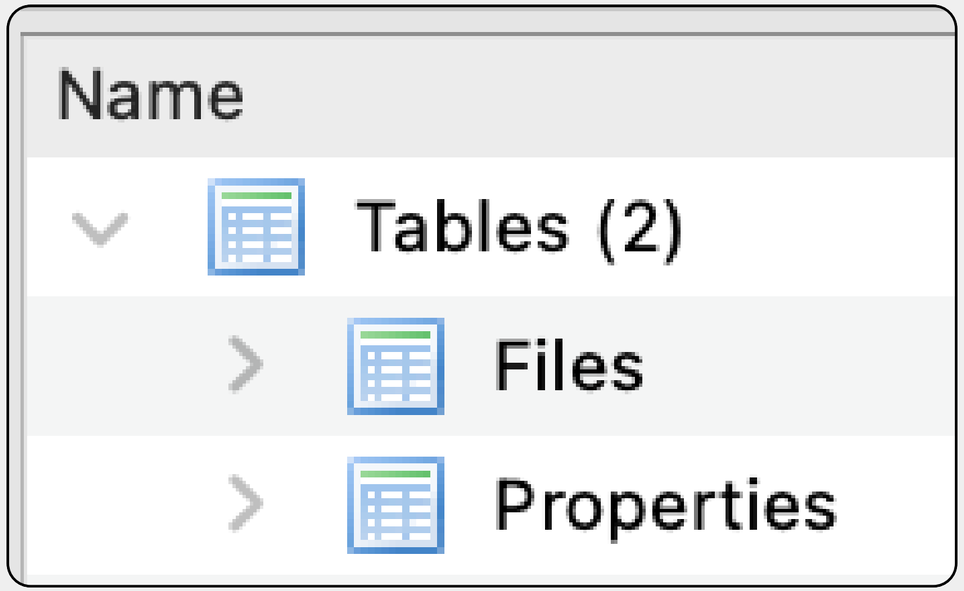
Manifest.plist

- details on application bundles installed on the device, native and third party



Manifest.db

- SQLite database
- two tables - Files & Properties



Manifest.db - Files table

Table: Files

Filter in any column

	fileID	domain	relativePath	flag
	Filter	Filter	Filter	Filt
1	c02652d85f9ef6daa9a4e3a68ec2e48	SysSharedContainerDomain-systemgroup.com.apple.icloud.ifccd		
2	0a51c6a85c5c889704b120a572cc47d	SysSharedContainerDomain-systemgroup.com.apple.icloud.ifccd	Library	
3	16dc686119a70d854061d725751022	AppDomainPlugin-com.klm.mobile.iphone.klmmobile.widget		
4	f0a6e7b071d26dfd09ebbec880da505	AppDomainPlugin-com.klm.mobile.iphone.klmmobile.widget	Library	
5	e4a56228566959fc358597e4505067c	AppDomainPlugin-com.klm.mobile.iphone.klmmobile.widget	Library/HTTPStorages	
6	ea4f4b82484b2e5bce95c9d7025c8ff8	AppDomainPlugin-com.klm.mobile.iphone.klmmobile.widget	Library/Preferences	
7	11a536c83c7b1dcc07d990898daa840	AppDomainPlugin-com.klm.mobile.iphone.klmmobile.widget	Documents	
8	68daeeb0366adfa51239d4b07c9c0d6	AppDomain-com.apple.StoreDemoViewService		
9	fae9d0745b56eecfce2e26ef3a7b0959	AppDomain-com.apple.StoreDemoViewService	Library	
10	0a644d248f4cc97f0eb0af042f3b175a	AppDomain-com.apple.StoreDemoViewService	Library/Preferences	
11	fd78e41106f1431160992d8dfe580681	AppDomain-com.apple.StoreDemoViewService	Documents	
12	a9203a5180e4213e8d3d8a9aaed784	AppDomainPlugin-com.apple.SafetyCheckAppIntents		
13	04a8986603dec06084e795008c90f9f	AppDomainPlugin-com.apple.SafetyCheckAppIntents	Library	
14	37b7bc7985a0c1045595dcef8bb26f6	AppDomainPlugin-com.apple.SafetyCheckAppIntents	Library/Preferences	
15	03f44be7e23545367c363f58d43520b	AppDomainPlugin-com.apple.SafetyCheckAppIntents	Documents	
16	2492f02e62dab5d6b5564c0202df3fc8	AppDomainPlugin-…		

Manifest.db - Files filtering

fileID	domain	relativePath	flags	file
Filter	Filter	.sqlite	Filter	Filter
bd5ae49148bb98e516ae660	AppDomainGroup-…	Accounts/CFB1DCDD-3ED7-4D9A-ACB8-B8FC5F1ED262/Paper/…	1	*BLOB*
51a2cc45c5657c0e0822079	AppDomainGroup-…	Accounts/CFB1DCDD-3ED7-4D9A-ACB8-B8FC5F1ED262/Paper/…	1	*BLOB*

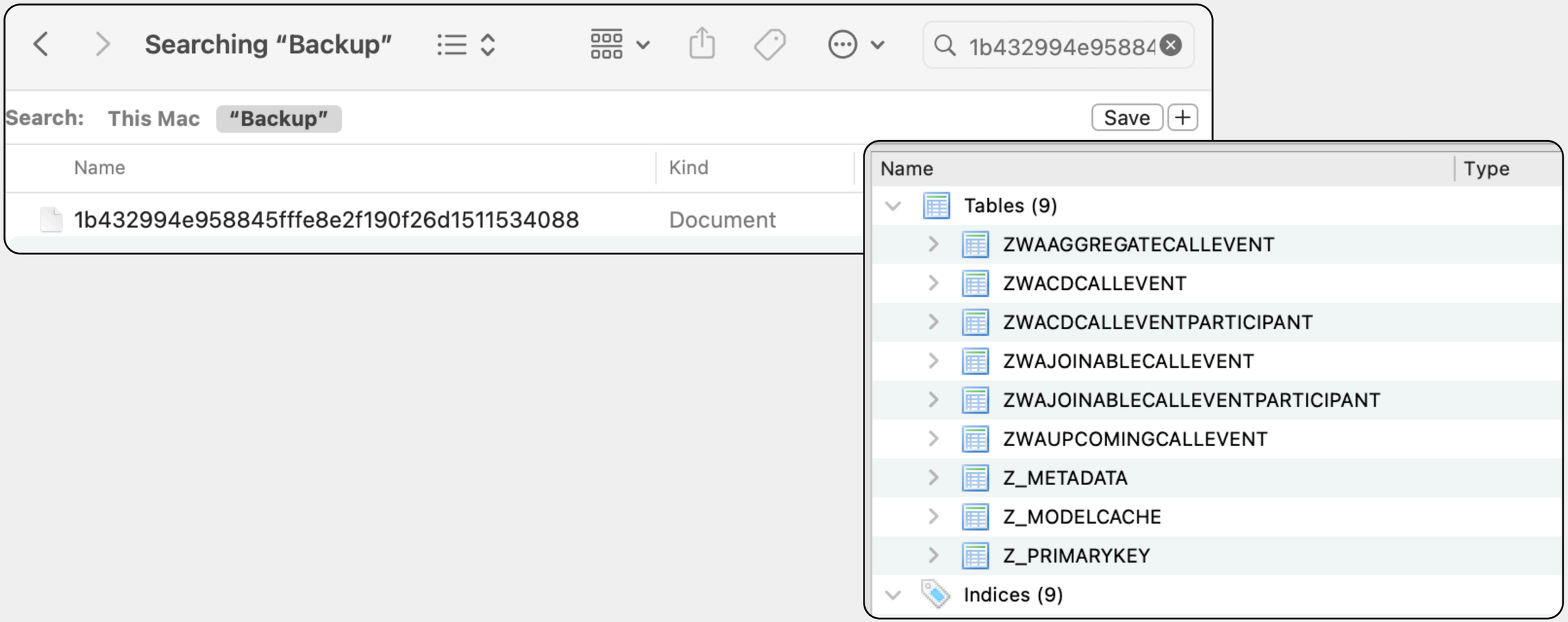
fileID	domain	relativePath	flags	file
Filter	Filter	.jpg	Filter	Filter
3efa945c4d58a8583e45d75	AppDomainGroup-…	Accounts/CFB1DCDD-3ED7-4D9A-ACB8-B8FC5F1ED262/…	1	*BLOB*
df25a05aa9c2b91b7b1516f1	AppDomainGroup-…	Accounts/CFB1DCDD-3ED7-4D9A-ACB8-B8FC5F1ED262/…	1	*BLOB*
dcf87c7d4ebd4d2ba557bfab	AppDomainGroup-…	Accounts/CFB1DCDD-3ED7-4D9A-ACB8-B8FC5F1ED262/…	1	*BLOB*
647c61a9a0476252470a193	AppDomain-…	Documents/pets/1.jpg	1	*BLOB*
945a49c9937f12df8b7ea835	AppDomain-…	Documents		
1eb96242f5188c2fd7b2e2f2	AppDomain-…	Documents		
11c96f3a38b88a33ff2a7fe71	AppDomain-…	Documents		
ceb4022b03a6bb24f415d31	AppDomain-…	Documents		

fileID	domain	relativePath	flags	file
Filter	Filter	.pdf	Filter	Filter
e7aa0e38e1c77bdecc4541b	AppDomain-…	Documents/PCISigning.pdf	1	*BLOB*
15b142b954b1fef32eefa42c	AppDomain-…	Documents/downloads/Airdrop Forensics WICCON.pdf.pdf	1	*BLOB*
a26f660595c5157e9b0dd2e	AppDomainGroup-…	File Provider Storage/1334_21_11_2022.pdf	1	*BLOB*
c41eba713ae01f81bde75e7	AppDomainGroup-…	File Provider Storage/CV - Kinga Kieczkowska - FT2024.pdf	1	*BLOB*
bc38d38dfa47c664f0efabd3	AppDomainGroup-…	File Provider Storage/D9193DD1-EC41-402B-ABC0-4582A21D592D.pdf	1	*BLOB*
9c7e73063f0663746292068	AppDomainGroup-…	File Provider Storage/DEPOSIT RECEIPT (2).pdf	1	*BLOB*

Manifest.db - fileID

fileID	domain	relativePath
Filter	Filter	callhistory.sqlite
1b432994e958845fffe8e2f190f26d1511534088	AppDomainGroup-group.net.whatsapp.WhatsApp.shared	CallHistory.sqlite

Manifest.db - fileID



Files of interest

- HomeDomain-Library/SMS/sms.db
- HomeDomain-Library/Notes/notes.sqlite
- AppDomainGroup-group.net.whatsapp.WhatsApp.shared-[ContactsV2.sqlite / ChatStorage.sqlite / CallHistory.sqlite]
- Might want to look for:
  - messenger apps
  - social media
  - travel apps - airlines, parking, taxi, bikes / scooters

Backup analysis tools

- commercial forensic software
- iLEAPP https://github.com/abrignoni/iLEAPP

iLEAPP

iOS Logs, Events, And Plists Parser
Details in blog post here: https://abrignoni.blogspot.com/2019/12/ileapp-ios-logs-events-and-properties.html

Supports iOS/iPadOS 11, 12, 13, 14, 15, 16, and 17. Select parsing directly from a compressed .tar/.zip file, or a decompressed directory, or an iTunes/Finder backup folder.

Features

Parses:
⚙️ Mobile Installation Logs
⚙️ iOS 12+ Notifications
⚙️ Build Info (iOS version, etc.)
⚙️ Wireless cellular service info (IMEI, number, etc.)
⚙️ Screen icons list by screen and in grid order.
⚙️ ApplicationState.db support for app bundle ID to data container GUID correlation.
⚙️ User and computer names that the iOS device connected to. Function updated by Jack Farley (@JackFarley248, http://farleyforensics.com/).
etc...

Why care about backups?

- easier to obtain than full physical acquisition
- sometimes available without physical access to the device
- contain key point-in-time information
- used in key cases IRL

National Review

> Earlier in 2019, law enforcement had received records from Biden's devices from Apple Inc. and later obtained a search warrant to collect Biden's iCloud data, Jensen said. Two iCloud backup files, one for Biden's iPad and the other for his iPhone XR, contain evidence the prosecution introduced at trial, in addition to the exhibits from the laptop archive.

Amnesty International

> iOS maintains records of process executions and their respective network usage in two SQLite database files called "*DataUsage.sqlite*" and "*netusage.sqlite*" which are stored on the device. It is worth noting that while the former is available in iTunes backup, the latter is not. Additionally, it should be noted that only processes that performed network activity will appear in these databases.

Thank you

blog post version of this talk is available at kieczkowska.com

Links

- https://smarterforensics.com/
- https://theapplewiki.com/wiki/ITunes_Backup
- https://www.nationalreview.com/news/prosecution-introduces-hunter-bidens-infamous-laptop-at-trial-uses-data-as-evidence-of-crack-addiction/
- https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/