USING APPLE "BUG REPORTING" FOR FORENSIC PURPOSES

Heather Mahalik

Guest Starring: Mattia Epifani

Primary Scripting: Adrian Leong

OSDFCON

OCTOBER 2019

APPLE PROFILE AND LOGS

- Apple provides “*a web-based tool that developers can use to report issues with Apple software and services, request enhancement to APIs and tools and track the status of their feedback*”
- To correctly use this tool and submit Apple relevant information to identify the issue, it is mandatory to “**Collect and attach any relevant logs**”

APPLE PROFILE AND LOGS

- The Apple web page “**Profiles and Logs**” contains instructions about how to extract logs from different Apple operating systems, including Mac OS X, iOS, tvOS and WatchOS
- Some logs (e.g. **Crash Logs**) are **automatically generated** by the operating system during its execution while others (e.g. **sysdiagnose**) **can be generated with specific user actions**
- Moreover, some logs **require the installation of a profile on the device** (e.g. Disk Space Diagnostics and Battery Life)

Using Apple "Bug Reporting" for forensic purposes

- We wrote a document describing our research into these logs
- This document is freely available from

https://www.for585.com/sysdiagnose

- We also developed various scripts to parse some of the files available during sysdiagnose acquisition
- These scripts are available from GitHub

https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts

CRASH LOGS

Automatically generated by the operating system when an application crashes

Can be used to understand the **conditions under which the application terminated**

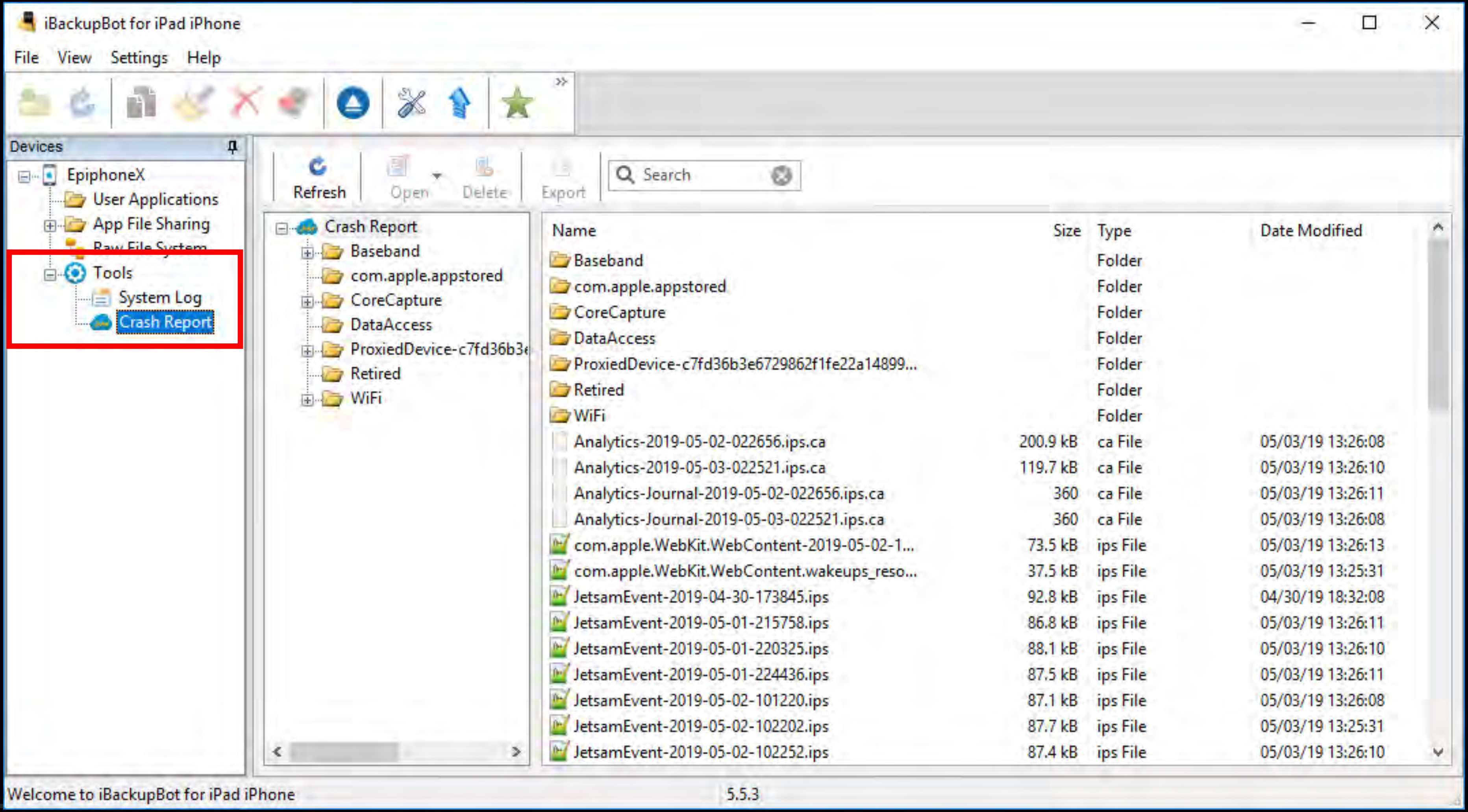
/private/var/mobile/Library/Logs/CrashReporter/

/private/var/root/Library/Logs/CrashReporter/

Methods…

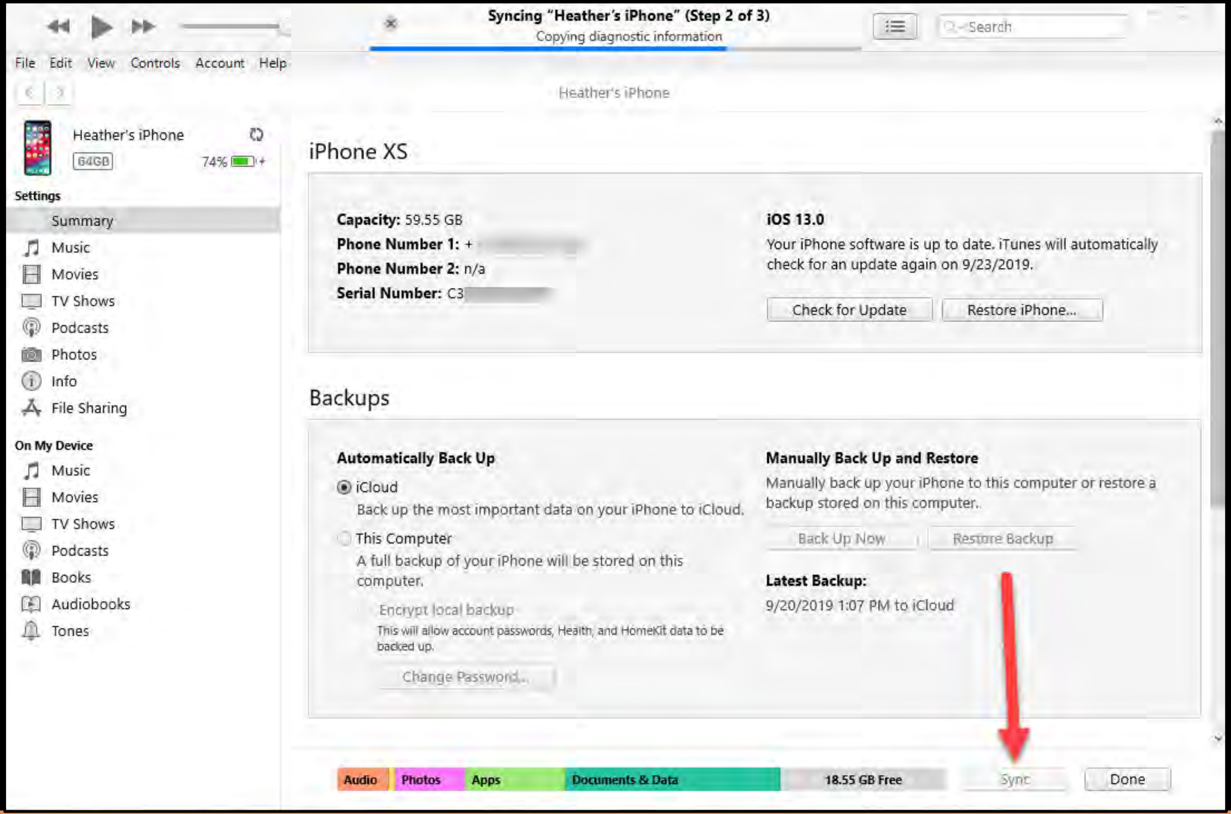
COLLECTING THE LOGS

1 -Using an iOS device manager tool



Name	Size	Type	Date Modified
Baseband		Folder	
com.apple.appstored		Folder	
CoreCapture		Folder	
DataAccess		Folder	
ProxiedDevice-c7fd36b3e6729862f1fe22a14899...		Folder	
Retired		Folder	
WiFi		Folder	
Analytics-2019-05-02-022656.ips.ca	200.9 kB	ca File	05/03/19 13:26:08
Analytics-2019-05-03-022521.ips.ca	119.7 kB	ca File	05/03/19 13:26:10
Analytics-Journal-2019-05-02-022656.ips.ca	360	ca File	05/03/19 13:26:11
Analytics-Journal-2019-05-03-022521.ips.ca	360	ca File	05/03/19 13:26:08
com.apple.WebKit.WebContent-2019-05-02-1...	73.5 kB	ips File	05/03/19 13:26:13
com.apple.WebKit.WebContent.wakeups_reso...	37.5 kB	ips File	05/03/19 13:25:31
JetsamEvent-2019-04-30-173845.ips	92.8 kB	ips File	04/30/19 18:32:08
JetsamEvent-2019-05-01-215758.ips	86.8 kB	ips File	05/03/19 13:26:11
JetsamEvent-2019-05-01-220325.ips	88.1 kB	ips File	05/03/19 13:26:10
JetsamEvent-2019-05-01-224436.ips	87.5 kB	ips File	05/03/19 13:26:11
JetsamEvent-2019-05-02-101220.ips	87.1 kB	ips File	05/03/19 13:26:08
JetsamEvent-2019-05-02-102202.ips	87.7 kB	ips File	05/03/19 13:25:31
JetsamEvent-2019-05-02-102252.ips	87.4 kB	ips File	05/03/19 13:26:10

2 – Sync the iOS device with iTunes



Syncing “Heather’s iPhone” (Step 2 of 3)
Copying diagnostic information

Heather's iPhone

iPhone XS

Capacity: 59.55 GB
Phone Number 1: + [redacted]
Phone Number 2: n/a
Serial Number: C3[redacted]

iOS 13.0
Your iPhone software is up to date. iTunes will automatically check for an update again on 9/23/2019.

Backups

Automatically Back Up

● iCloud
Back up the most important data on your iPhone to iCloud.

○ This Computer
A full backup of your iPhone will be stored on this computer.

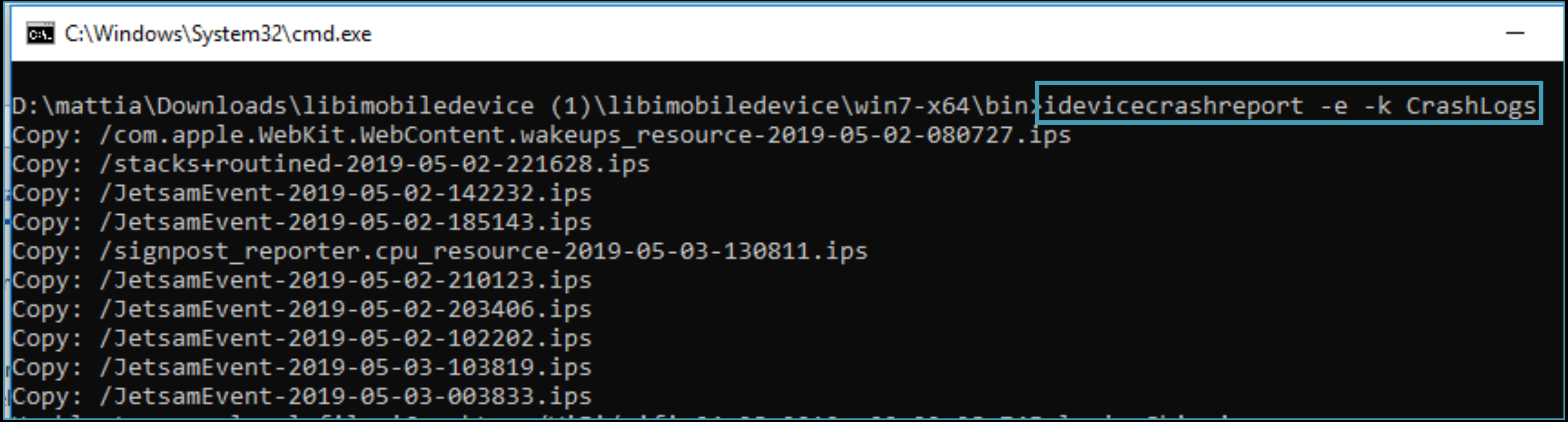
□ Encrypt local backup
This will allow account passwords, Health, and HomeKit data to be backed up.

Manually Back Up and Restore
Manually back up your iPhone to this computer or restore a backup stored on this computer.

Latest Backup:
9/20/2019 1:07 PM to iCloud

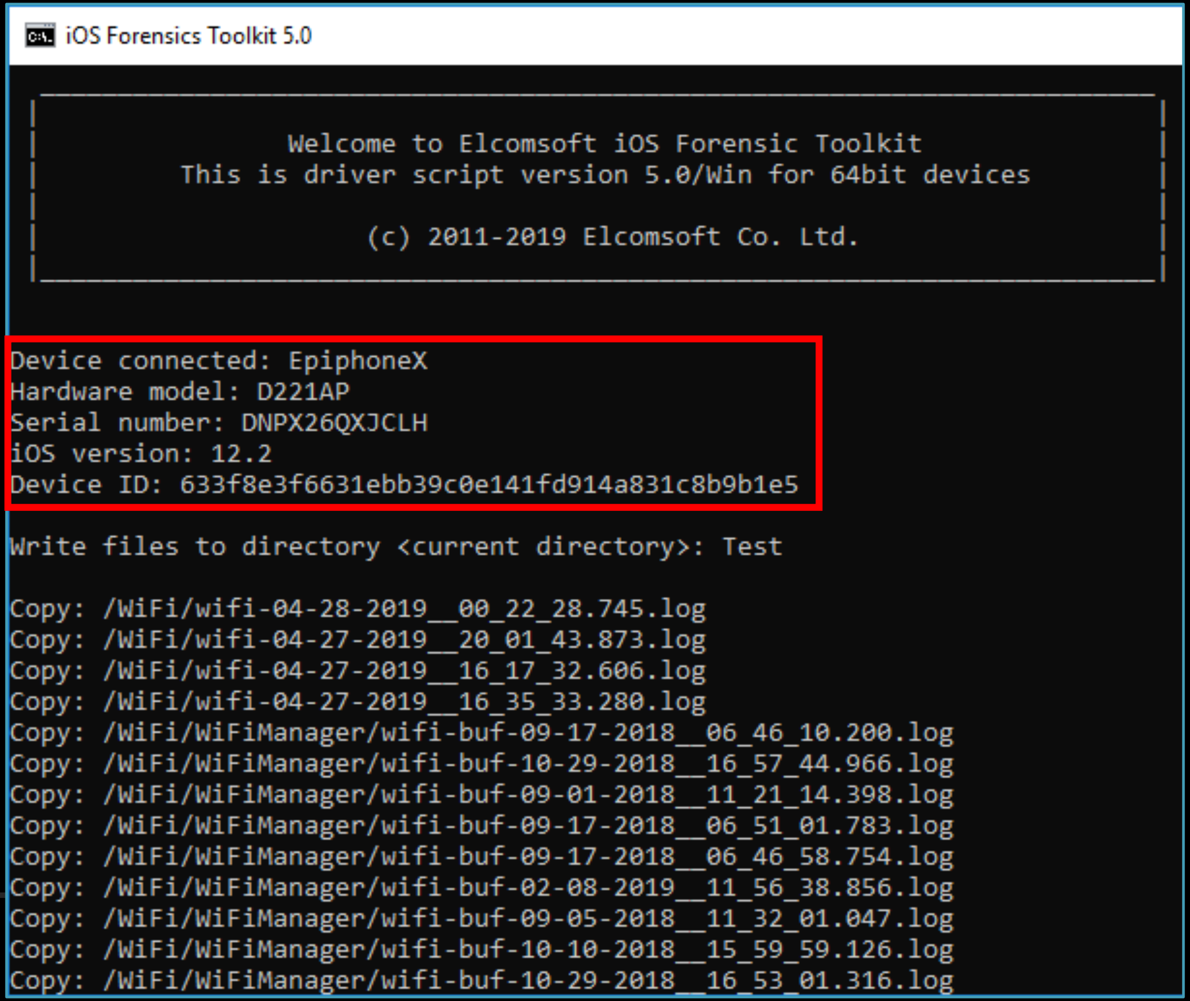
OS	Path
macOS	/Users/<username>/Library/Logs/CrashReporter/MobileDevice/[Device_Name]/
Windows	C:\Users\<username>\AppData\Roaming\Apple Computer\Logs\CrashReporter\MobileDevice\[Device_Name]\

3 - Using idevicecrashreport tool

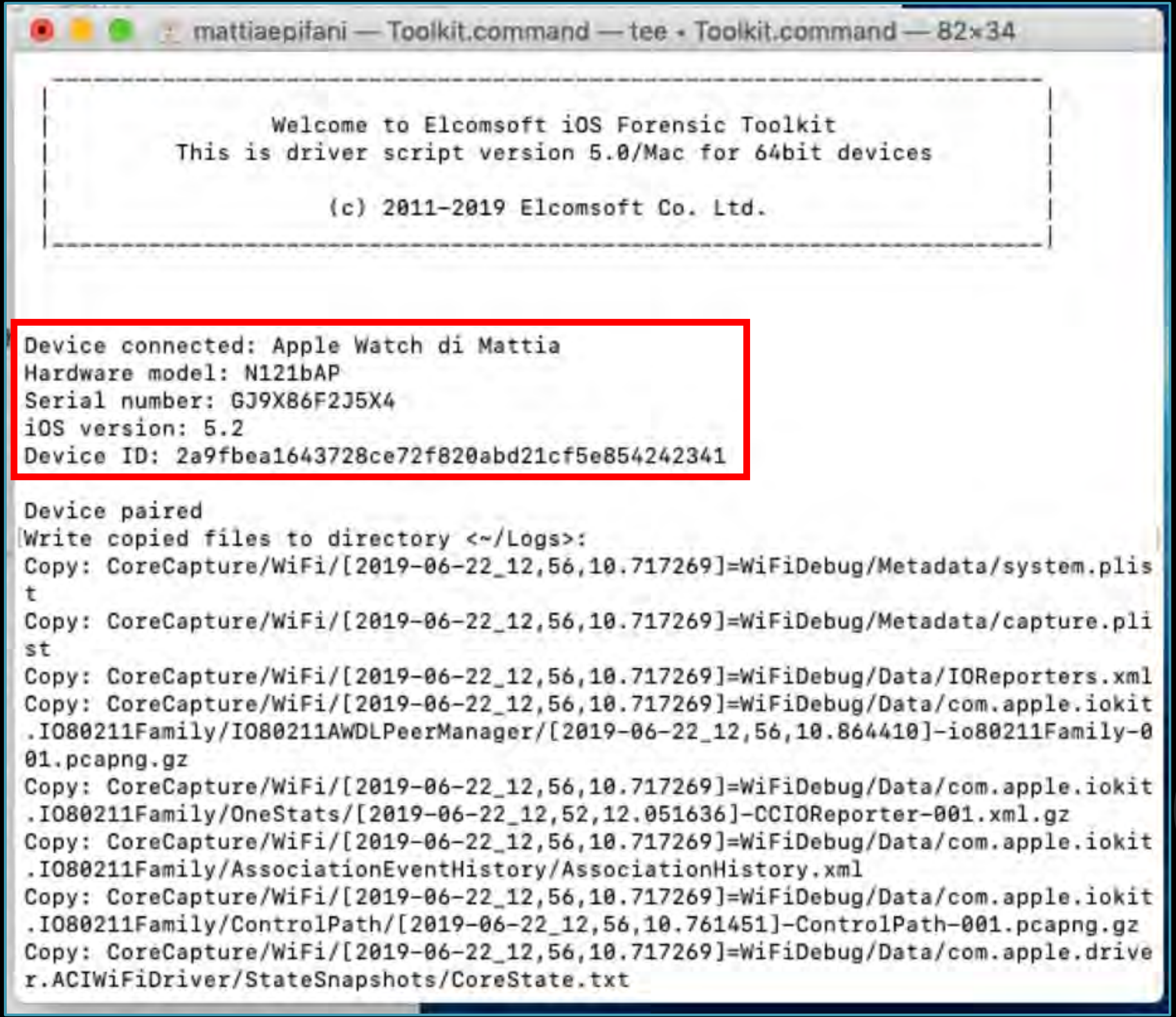


```
D:\mattia\Downloads\libimobiledevice (1)\libimobiledevice\win7-x64\bin>idevicecrashreport -e -k CrashLogs
Copy: /com.apple.WebKit.WebContent.wakeups_resource-2019-05-02-080727.ips
Copy: /stacks+routined-2019-05-02-221628.ips
Copy: /JetsamEvent-2019-05-02-142232.ips
Copy: /JetsamEvent-2019-05-02-185143.ips
Copy: /signpost_reporter.cpu_resource-2019-05-03-130811.ips
Copy: /JetsamEvent-2019-05-02-210123.ips
Copy: /JetsamEvent-2019-05-02-203406.ips
Copy: /JetsamEvent-2019-05-02-102202.ips
Copy: /JetsamEvent-2019-05-03-103819.ips
Copy: /JetsamEvent-2019-05-03-003833.ips
```

4 - Using Elcomsoft iOS Forensic Toolkit

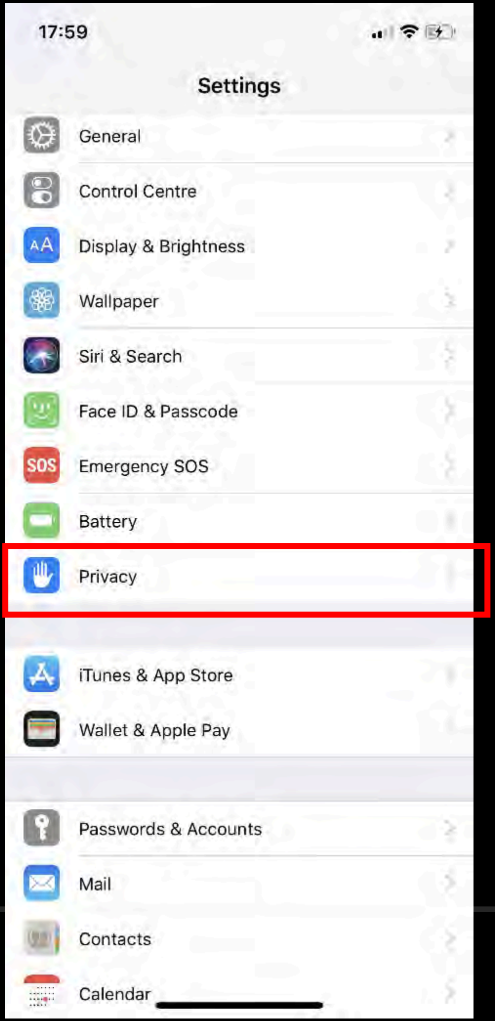


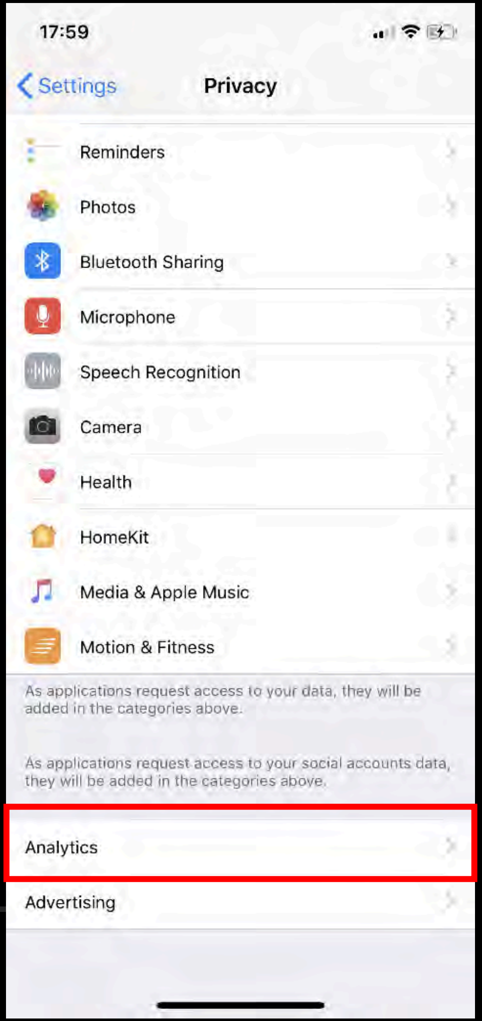
```
 ______________________________________________________________________
|                                                                      |
|                 Welcome to Elcomsoft iOS Forensic Toolkit             |
|          This is driver script version 5.0/Win for 64bit devices      |
|                                                                      |
|                     (c) 2011-2019 Elcomsoft Co. Ltd.                 |
|______________________________________________________________________|


Device connected: EpiphoneX
Hardware model: D221AP
Serial number: DNPX26QXJCLH
iOS version: 12.2
Device ID: 633f8e3f6631ebb39c0e141fd914a831c8b9b1e5

Write files to directory <current directory>: Test

Copy: /WiFi/wifi-04-28-2019__00_22_28.745.log
Copy: /WiFi/wifi-04-27-2019__20_01_43.873.log
Copy: /WiFi/wifi-04-27-2019__16_17_32.606.log
Copy: /WiFi/wifi-04-27-2019__16_35_33.280.log
Copy: /WiFi/WiFiManager/wifi-buf-09-17-2018__06_46_10.200.log
Copy: /WiFi/WiFiManager/wifi-buf-10-29-2018__16_57_44.966.log
Copy: /WiFi/WiFiManager/wifi-buf-09-01-2018__11_21_14.398.log
Copy: /WiFi/WiFiManager/wifi-buf-09-17-2018__06_51_01.783.log
Copy: /WiFi/WiFiManager/wifi-buf-09-17-2018__06_46_58.754.log
Copy: /WiFi/WiFiManager/wifi-buf-02-08-2019__11_56_38.856.log
Copy: /WiFi/WiFiManager/wifi-buf-09-05-2018__11_32_01.047.log
Copy: /WiFi/WiFiManager/wifi-buf-10-10-2018__15_59_59.126.log
Copy: /WiFi/WiFiManager/wifi-buf-10-29-2018__16_53_01.316.log
```


mattiaepifani — Toolkit.command — tee • Toolkit.command — 82×34

```
 ----------------------------------------------------------------------------
|                                                                            |
|                  Welcome to Elcomsoft iOS Forensic Toolkit                 |
|           This is driver script version 5.0/Mac for 64bit devices          |
|                                                                            |
|                      (c) 2011-2019 Elcomsoft Co. Ltd.                      |
|----------------------------------------------------------------------------|


Device connected: Apple Watch di Mattia
Hardware model: N121bAP
Serial number: GJ9X86F2J5X4
iOS version: 5.2
Device ID: 2a9fbea1643728ce72f820abd21cf5e854242341

Device paired
Write copied files to directory <~/Logs>:
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Metadata/system.plis
t
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Metadata/capture.pli
st
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Data/IOReporters.xml
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Data/com.apple.iokit
.IO80211Family/IO80211AWDLPeerManager/[2019-06-22_12,56,10.864410]-io80211Family-0
01.pcapng.gz
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Data/com.apple.iokit
.IO80211Family/OneStats/[2019-06-22_12,52,12.051636]-CCIOReporter-001.xml.gz
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Data/com.apple.iokit
.IO80211Family/AssociationEventHistory/AssociationHistory.xml
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Data/com.apple.iokit
.IO80211Family/ControlPath/[2019-06-22_12,56,10.761451]-ControlPath-001.pcapng.gz
Copy: CoreCapture/WiFi/[2019-06-22_12,56,10.717269]=WiFiDebug/Data/com.apple.drive
r.ACIWiFiDriver/StateSnapshots/CoreState.txt
```

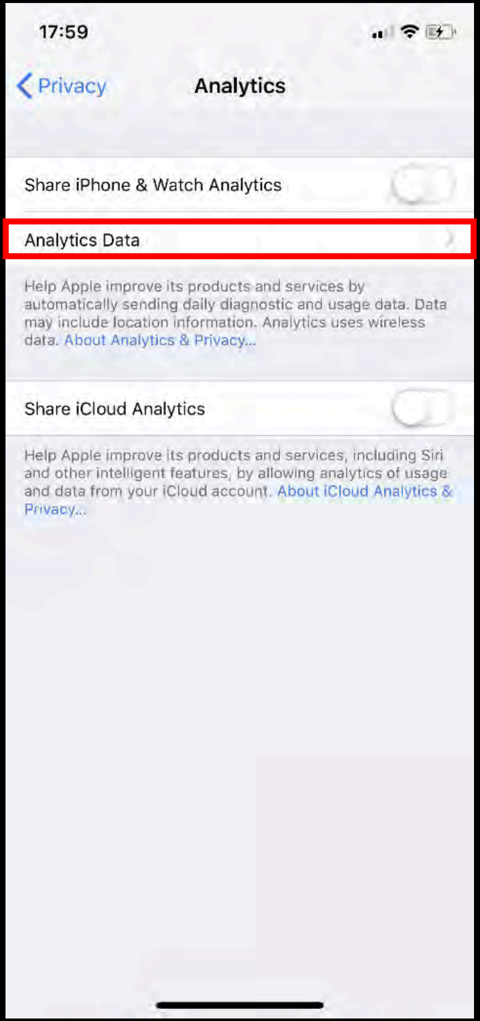
5 - Last effort…Using AIRDROP





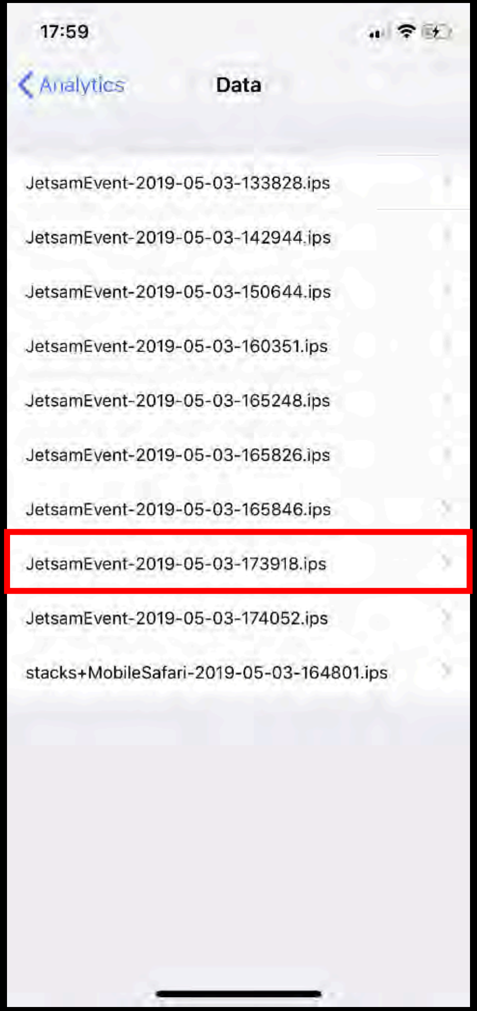
As applications request access to your data, they will be added in the categories above.

As applications request access to your social accounts data, they will be added in the categories above.



Help Apple improve its products and services by automatically sending daily diagnostic and usage data. Data may include location information. Analytics uses wireless data. About Analytics & Privacy...

Help Apple improve its products and services, including Siri and other intelligent features, by allowing analytics of usage and data from your iCloud account. About iCloud Analytics & Privacy...



JetsamEvent-2019-05-03-133828.ips

JetsamEvent-2019-05-03-142944.ips

JetsamEvent-2019-05-03-150644.ips

JetsamEvent-2019-05-03-160351.ips

JetsamEvent-2019-05-03-165248.ips

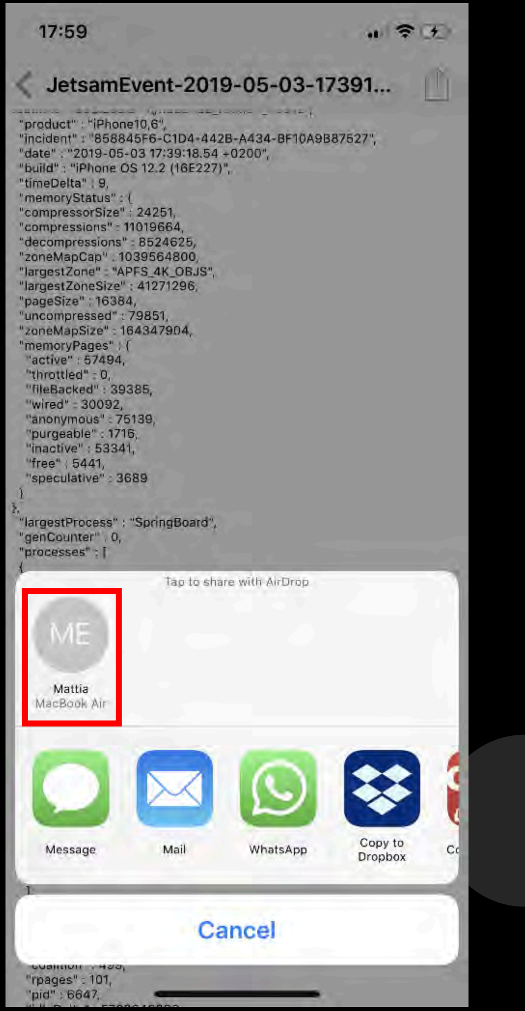
JetsamEvent-2019-05-03-165826.ips

JetsamEvent-2019-05-03-165846.ips

JetsamEvent-2019-05-03-173918.ips

JetsamEvent-2019-05-03-174052.ips

stacks+MobileSafari-2019-05-03-164801.ips



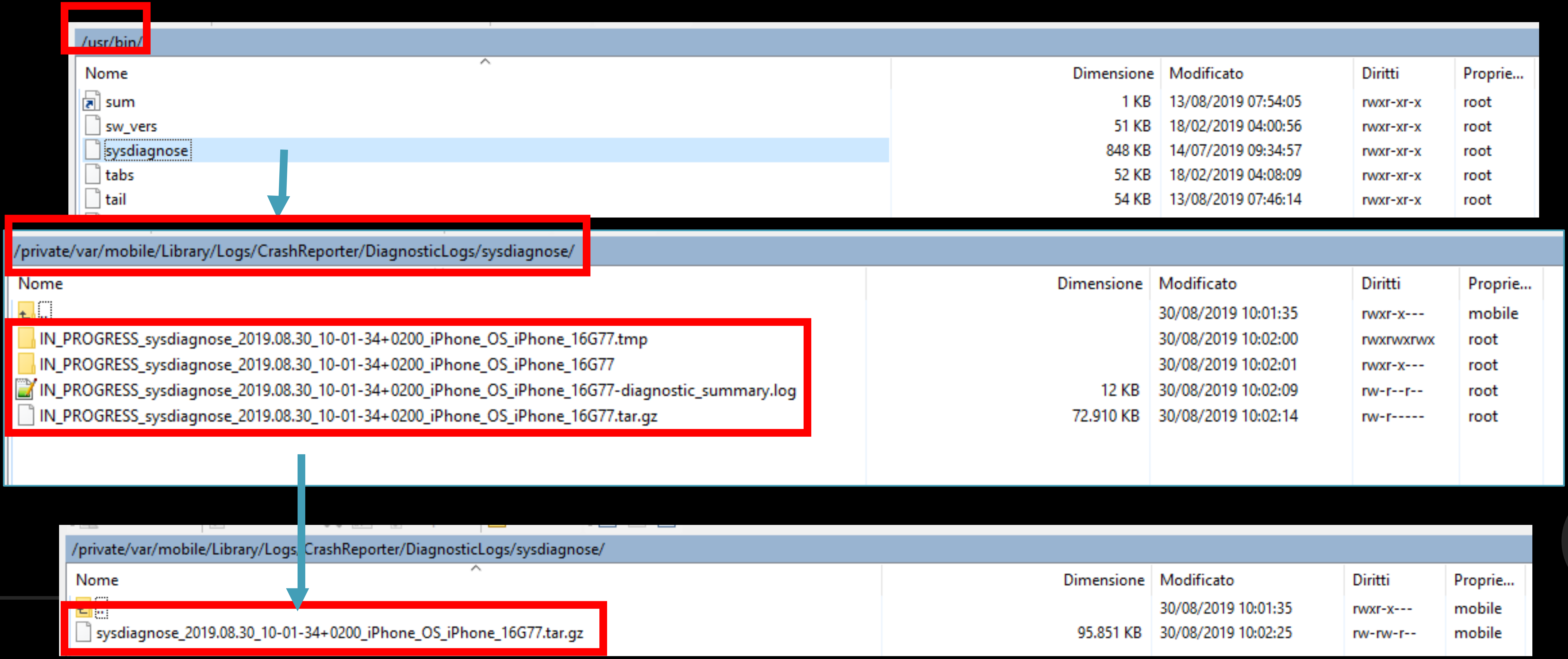
```
 "product" : "iPhone10,6",
 "incident" : "858845F6-C1D4-442B-A434-BF10A9B87527",
 "date" : "2019-05-03 17:39:18.54 +0200",
 "build" : "iPhone OS 12.2 (16E227)",
 "timeDelta" : 9,
 "memoryStatus" : {
 "compressorSize" : 24251,
 "compressions" : 11019664,
 "decompressions" : 8524625,
 "zoneMapCap" : 1039564800,
 "largestZone" : "APFS_4K_OBJS",
 "largestZoneSize" : 41271296,
 "pageSize" : 16384,
 "uncompressed" : 79851,
 "zoneMapSize" : 164347904,
 "memoryPages" : {
  "active" : 57494,
  "throttled" : 0,
  "fileBacked" : 39385,
  "wired" : 30092,
  "anonymous" : 75139,
  "purgeable" : 1716,
  "inactive" : 53341,
  "free" : 5441,
  "speculative" : 3689
 }
},
 "largestProcess" : "SpringBoard",
 "genCounter" : 0,
 "processes" : [
 {
 ...
 "rpages" : 101,
 "pid" : 6647,
```

What's Coming Next - The Choice is Yours…

SYSDIAGNOSE

- Unlike Crash Logs, sysdiagnose logs are **not** executed and written automatically by the operating system
- The generation **must be triggered manually by the user**
- There are two documented procedures to generate sysdiagnose logs :
  1. By simultaneously pressing and releasing both volume buttons + the Side (or Top) button for 1 to 1.5 seconds
  2. By using **AssistiveTouch**
- The sysdiagnose logs can be extracted from an iOS device using the same methods described for the extraction of Crash Logs

GENERATING SYSDIAGNOSE – IN THE BACKGROUND…



/usr/bin/

Nome	Dimensione	Modificato	Diritti	Proprie...
sum	1 KB	13/08/2019 07:54:05	rwxr-xr-x	root
sw_vers	51 KB	18/02/2019 04:00:56	rwxr-xr-x	root
sysdiagnose	848 KB	14/07/2019 09:34:57	rwxr-xr-x	root
tabs	52 KB	18/02/2019 04:08:09	rwxr-xr-x	root
tail	54 KB	13/08/2019 07:46:14	rwxr-xr-x	root

/private/var/mobile/Library/Logs/CrashReporter/DiagnosticLogs/sysdiagnose/

Nome	Dimensione	Modificato	Diritti	Proprie...
..		30/08/2019 10:01:35	rwxr-x---	mobile
IN_PROGRESS_sysdiagnose_2019.08.30_10-01-34+0200_iPhone_OS_iPhone_16G77.tmp		30/08/2019 10:02:00	rwxrwxrwx	root
IN_PROGRESS_sysdiagnose_2019.08.30_10-01-34+0200_iPhone_OS_iPhone_16G77		30/08/2019 10:02:01	rwxr-x---	root
IN_PROGRESS_sysdiagnose_2019.08.30_10-01-34+0200_iPhone_OS_iPhone_16G77-diagnostic_summary.log	12 KB	30/08/2019 10:02:09	rw-r--r--	root
IN_PROGRESS_sysdiagnose_2019.08.30_10-01-34+0200_iPhone_OS_iPhone_16G77.tar.gz	72.910 KB	30/08/2019 10:02:14	rw-r-----	root

/private/var/mobile/Library/Logs/CrashReporter/DiagnosticLogs/sysdiagnose/

Nome	Dimensione	Modificato	Diritti	Proprie...
..		30/08/2019 10:01:35	rwxr-x---	mobile
sysdiagnose_2019.08.30_10-01-34+0200_iPhone_OS_iPhone_16G77.tar.gz	95.851 KB	30/08/2019 10:02:25	rw-rw-r--	mobile

SYSDIAGNOSE PARSING SCRIPTS

Open source

Developed with Python3 standard libraries (e.g. plistlib)

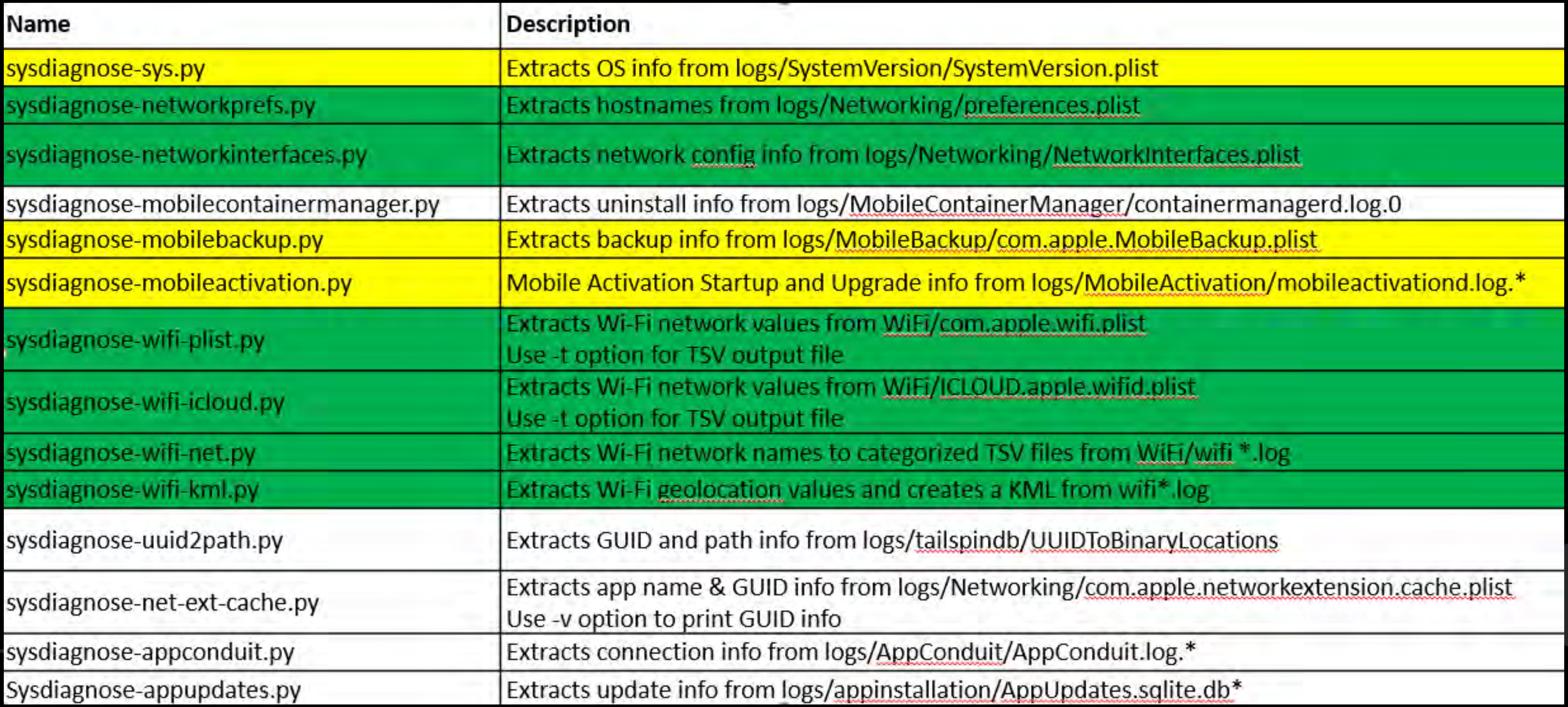
Avoids third party libraries as forensic workstations may not be connected to the Internet

Written/prototyped on Ubuntu 16.04 LTS running Python 3.5

14 scripts (so far) with 3 categories of script:

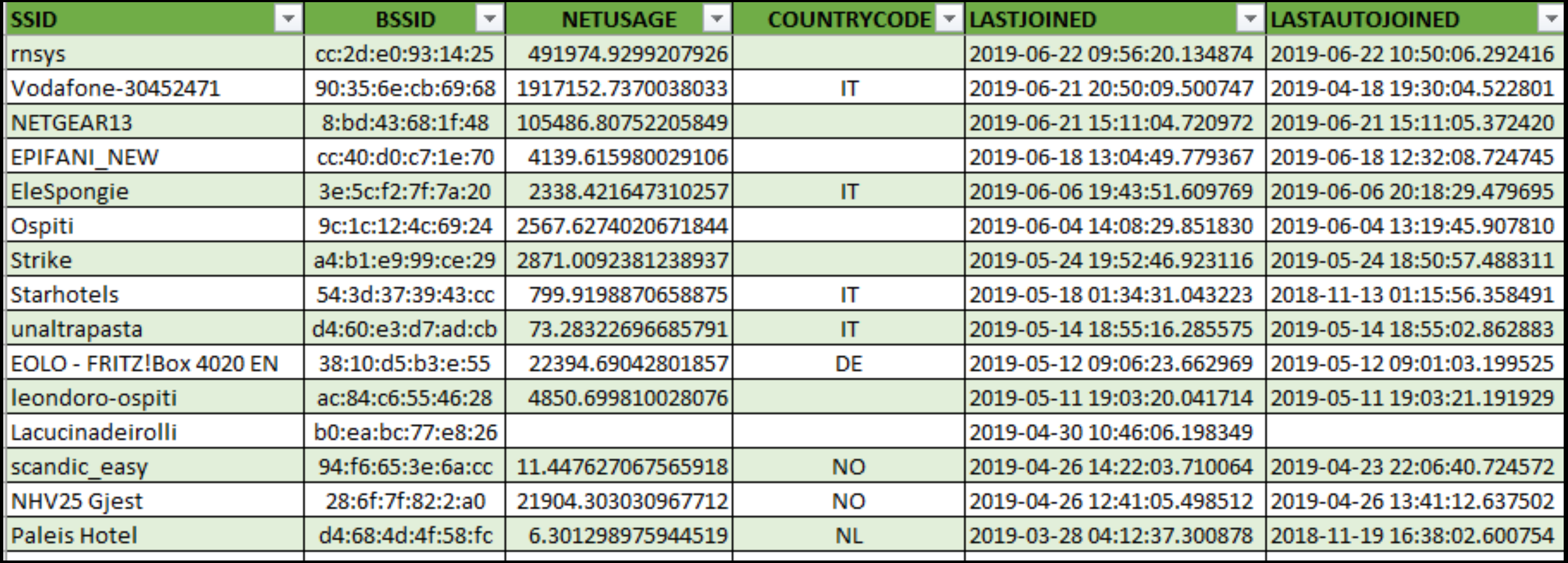
- **iOS Configuration**
- **Network Info**
- **App Info**

SYSDIAGNOSE PARSING SCRIPTS



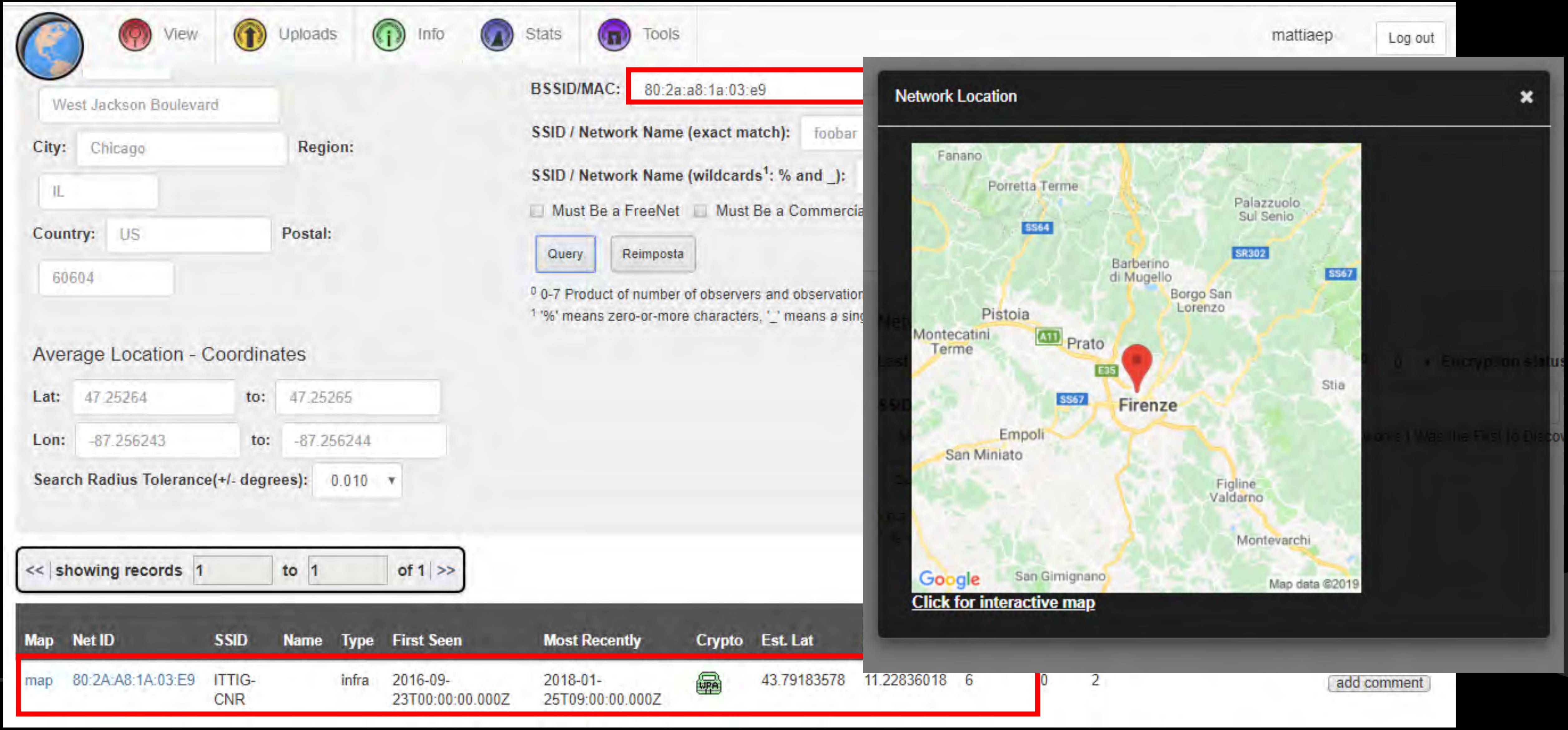
Name	Description
sysdiagnose-sys.py	Extracts OS info from logs/SystemVersion/SystemVersion.plist
sysdiagnose-networkprefs.py	Extracts hostnames from logs/Networking/preferences.plist
sysdiagnose-networkinterfaces.py	Extracts network config info from logs/Networking/NetworkInterfaces.plist
sysdiagnose-mobilecontainermanager.py	Extracts uninstall info from logs/MobileContainerManager/containermanagerd.log.0
sysdiagnose-mobilebackup.py	Extracts backup info from logs/MobileBackup/com.apple.MobileBackup.plist
sysdiagnose-mobileactivation.py	Mobile Activation Startup and Upgrade info from logs/MobileActivation/mobileactivationd.log.*
sysdiagnose-wifi-plist.py	Extracts Wi-Fi network values from WiFi/com.apple.wifi.plist Use -t option for TSV output file
sysdiagnose-wifi-icloud.py	Extracts Wi-Fi network values from WiFi/ICLOUD.apple.wifid.plist Use -t option for TSV output file
sysdiagnose-wifi-net.py	Extracts Wi-Fi network names to categorized TSV files from WiFi/wifi *.log
sysdiagnose-wifi-kml.py	Extracts Wi-Fi geolocation values and creates a KML from wifi*.log
sysdiagnose-uuid2path.py	Extracts GUID and path info from logs/tailspindb/UUIDToBinaryLocations
sysdiagnose-net-ext-cache.py	Extracts app name & GUID info from logs/Networking/com.apple.networkextension.cache.plist Use -v option to print GUID info
sysdiagnose-appconduit.py	Extracts connection info from logs/AppConduit/AppConduit.log.*
Sysdiagnose-appupdates.py	Extracts update info from logs/appinstallation/AppUpdates.sqlite.db*

WIFI PLIST (I)



SSID	BSSID	NETUSAGE	COUNTRYCODE	LASTJOINED	LASTAUTOJOINED
rnsys	cc:2d:e0:93:14:25	491974.9299207926		2019-06-22 09:56:20.134874	2019-06-22 10:50:06.292416
Vodafone-30452471	90:35:6e:cb:69:68	1917152.7370038033	IT	2019-06-21 20:50:09.500747	2019-04-18 19:30:04.522801
NETGEAR13	8:bd:43:68:1f:48	105486.80752205849		2019-06-21 15:11:04.720972	2019-06-21 15:11:05.372420
EPIFANI_NEW	cc:40:d0:c7:1e:70	4139.615980029106		2019-06-18 13:04:49.779367	2019-06-18 12:32:08.724745
EleSpongie	3e:5c:f2:7f:7a:20	2338.421647310257	IT	2019-06-06 19:43:51.609769	2019-06-06 20:18:29.479695
Ospiti	9c:1c:12:4c:69:24	2567.6274020671844		2019-06-04 14:08:29.851830	2019-06-04 13:19:45.907810
Strike	a4:b1:e9:99:ce:29	2871.0092381238937		2019-05-24 19:52:46.923116	2019-05-24 18:50:57.488311
Starhotels	54:3d:37:39:43:cc	799.9198870658875	IT	2019-05-18 01:34:31.043223	2018-11-13 01:15:56.358491
unaltrapasta	d4:60:e3:d7:ad:cb	73.28322696685791	IT	2019-05-14 18:55:16.285575	2019-05-14 18:55:02.862883
EOLO - FRITZ!Box 4020 EN	38:10:d5:b3:e:55	22394.69042801857	DE	2019-05-12 09:06:23.662969	2019-05-12 09:01:03.199525
leondoro-ospiti	ac:84:c6:55:46:28	4850.699810028076		2019-05-11 19:03:20.041714	2019-05-11 19:03:21.191929
Lacucinadeirolli	b0:ea:bc:77:e8:26			2019-04-30 10:46:06.198349	
scandic_easy	94:f6:65:3e:6a:cc	11.447627067565918	NO	2019-04-26 14:22:03.710064	2019-04-23 22:06:40.724572
NHV25 Gjest	28:6f:7f:82:2:a0	21904.30303096771 2	NO	2019-04-26 12:41:05.498512	2019-04-26 13:41:12.637502
Paleis Hotel	d4:68:4d:4f:58:fc	6.301298975944519	NL	2019-03-28 04:12:37.300878	2018-11-19 16:38:02.600754

WIFI PLIST (II)



West Jackson Boulevard

City: Chicago

Region: IL

Country: US

Postal: 60604

Average Location - Coordinates

Lat: 47.25264 to: 47.25265

Lon: -87.256243 to: -87.256244

Search Radius Tolerance(+/- degrees): 0.010

BSSID/MAC: 80:2a:a8:1a:03:e9

SSID / Network Name (exact match): foobar

SSID / Network Name (wildcards[1]: % and _):

□ Must Be a FreeNet □ Must Be a Commercia

[0] 0-7 Product of number of observers and observatio

[1] '%' means zero-or-more characters, '_' means a sin

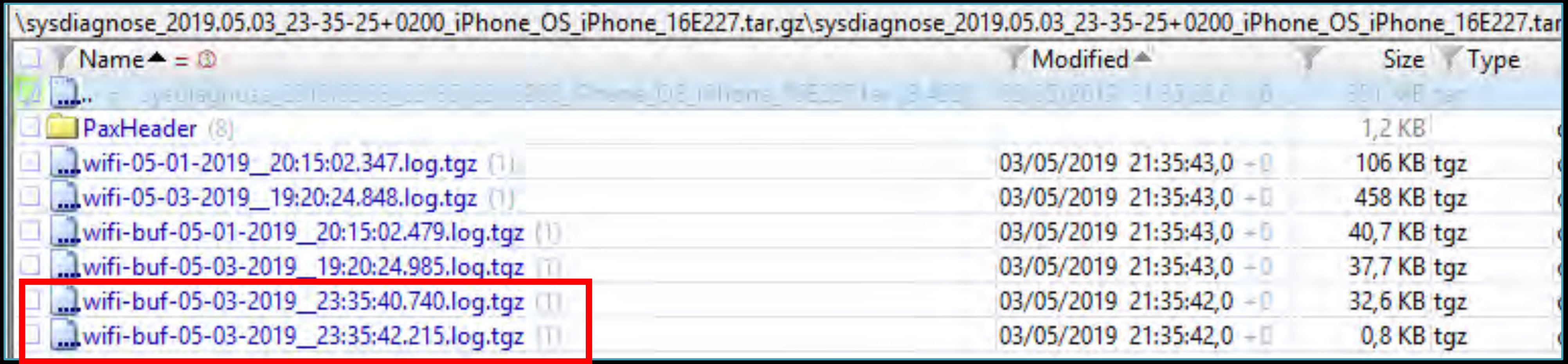
<< showing records 1 to 1 of 1 >>

Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat					
map	80:2A:A8:1A:03:E9	ITTIG-CNR		infra	2016-09-23T00:00:00.000Z	2018-01-25T09:00:00.000Z	WPA	43.79183578	11.22836018	6	0	2	add comment

Network Location

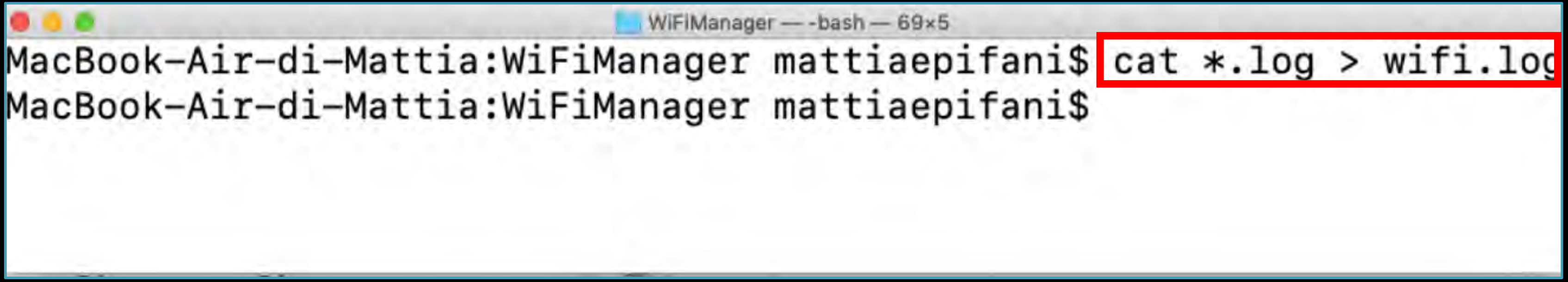
Click for interactive map

Step 1 - WIFI KML Script



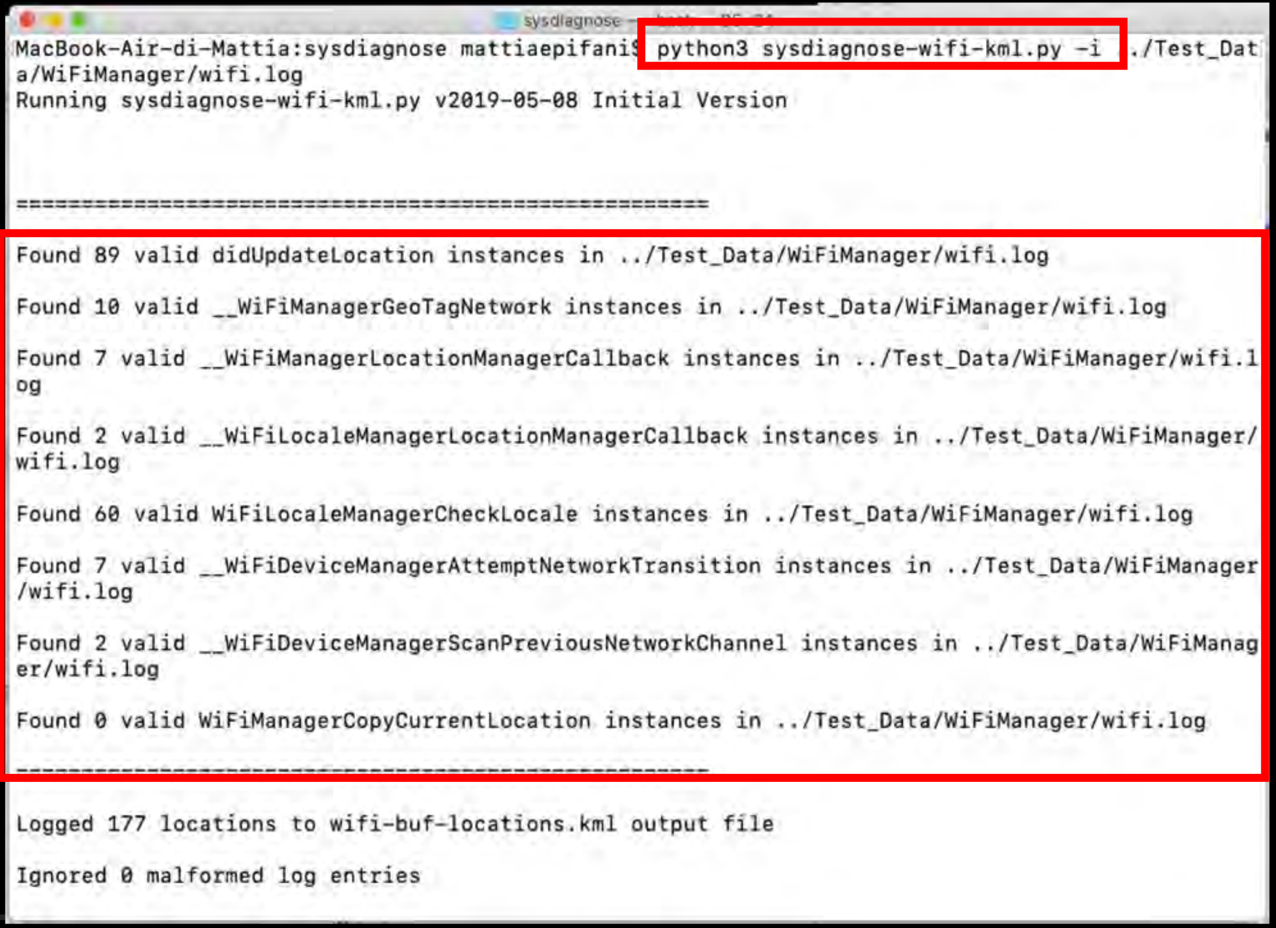
\sysdiagnose_2019.05.03_23-35-25+0200_iPhone_OS_iPhone_16E227.tar.gz\sysdiagnose_2019.05.03_23-35-25+0200_iPhone_OS_iPhone_16E227.tar

Name	Modified	Size	Type
.. [illegible]	[illegible]	[illegible]	[illegible]
PaxHeader (8)		1,2 KB	
wifi-05-01-2019__20:15:02.347.log.tgz (1)	03/05/2019 21:35:43,0	106 KB	tgz
wifi-05-03-2019__19:20:24.848.log.tgz (1)	03/05/2019 21:35:43,0	458 KB	tgz
wifi-buf-05-01-2019__20:15:02.479.log.tgz (1)	03/05/2019 21:35:43,0	40,7 KB	tgz
wifi-buf-05-03-2019__19:20:24.985.log.tgz (1)	03/05/2019 21:35:43,0	37,7 KB	tgz
wifi-buf-05-03-2019__23:35:40.740.log.tgz (1)	03/05/2019 21:35:42,0	32,6 KB	tgz
wifi-buf-05-03-2019__23:35:42.215.log.tgz (1)	03/05/2019 21:35:42,0	0,8 KB	tgz

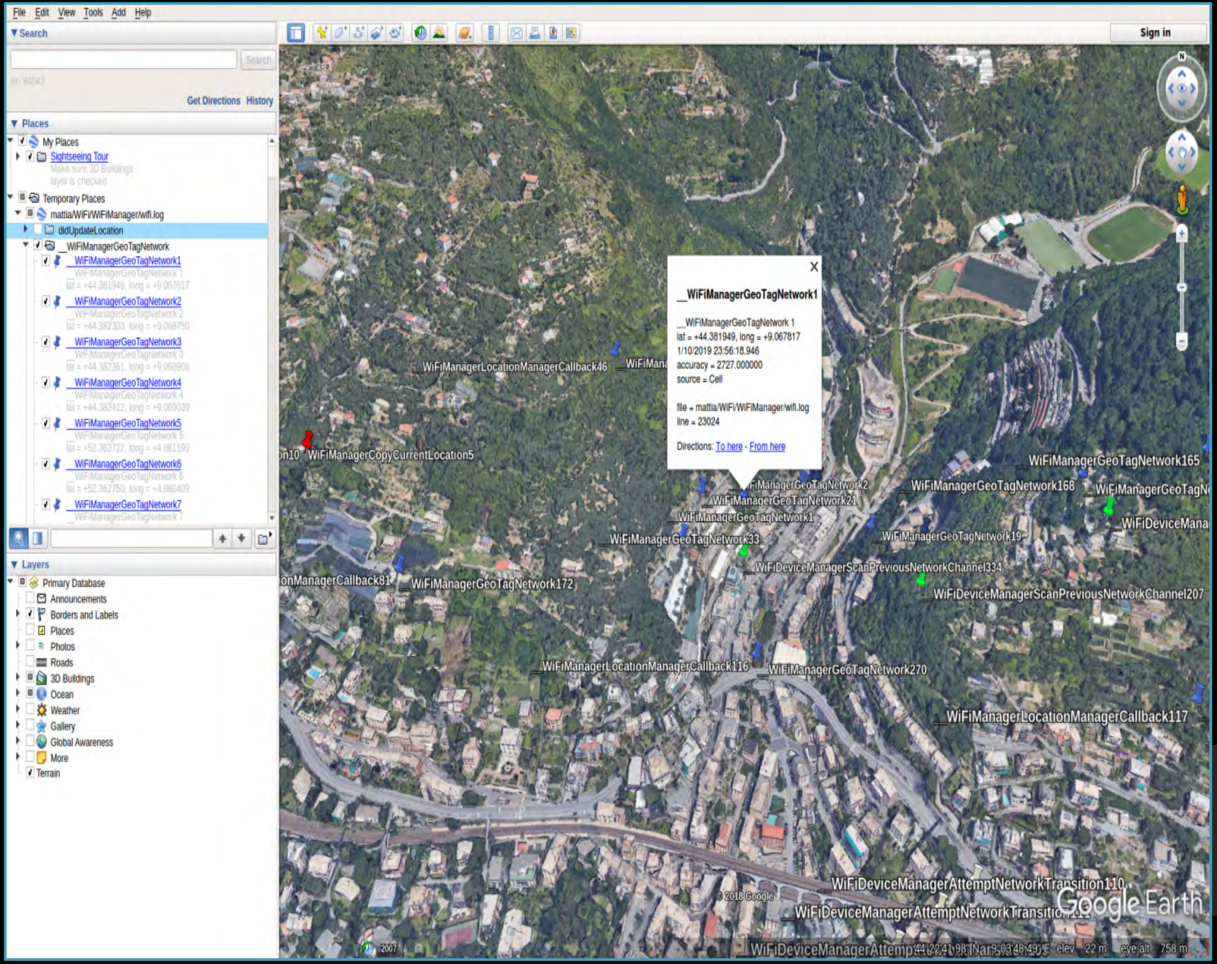


```
MacBook-Air-di-Mattia:WiFiManager mattiaepifani$ cat *.log > wifi.log
MacBook-Air-di-Mattia:WiFiManager mattiaepifani$
```

Step 2 - WIFI KML Script



```
MacBook-Air-di-Mattia:sysdiagnose mattiaepifani$ python3 sysdiagnose-wifi-kml.py -i ../Test_Dat
a/WiFiManager/wifi.log
Running sysdiagnose-wifi-kml.py v2019-05-08 Initial Version



=====================================================

Found 89 valid didUpdateLocation instances in ../Test_Data/WiFiManager/wifi.log

Found 10 valid __WiFiManagerGeoTagNetwork instances in ../Test_Data/WiFiManager/wifi.log

Found 7 valid __WiFiManagerLocationManagerCallback instances in ../Test_Data/WiFiManager/wifi.l
og

Found 2 valid __WiFiLocaleManagerLocationManagerCallback instances in ../Test_Data/WiFiManager/
wifi.log

Found 60 valid WiFiLocaleManagerCheckLocale instances in ../Test_Data/WiFiManager/wifi.log

Found 7 valid __WiFiDeviceManagerAttemptNetworkTransition instances in ../Test_Data/WiFiManager
/wifi.log

Found 2 valid __WiFiDeviceManagerScanPreviousNetworkChannel instances in ../Test_Data/WiFiManag
er/wifi.log

Found 0 valid WiFiManagerCopyCurrentLocation instances in ../Test_Data/WiFiManager/wifi.log

=====================================================

Logged 177 locations to wifi-buf-locations.kml output file

Ignored 0 malformed log entries
```



__WiFiManagerGeoTagNetwork1

__WiFiManagerGeoTagNetwork 1
lat = +44.381949, long = +9.067817
1/10/2019 23:56:18.946
accuracy = 2727.000000
source = Cell

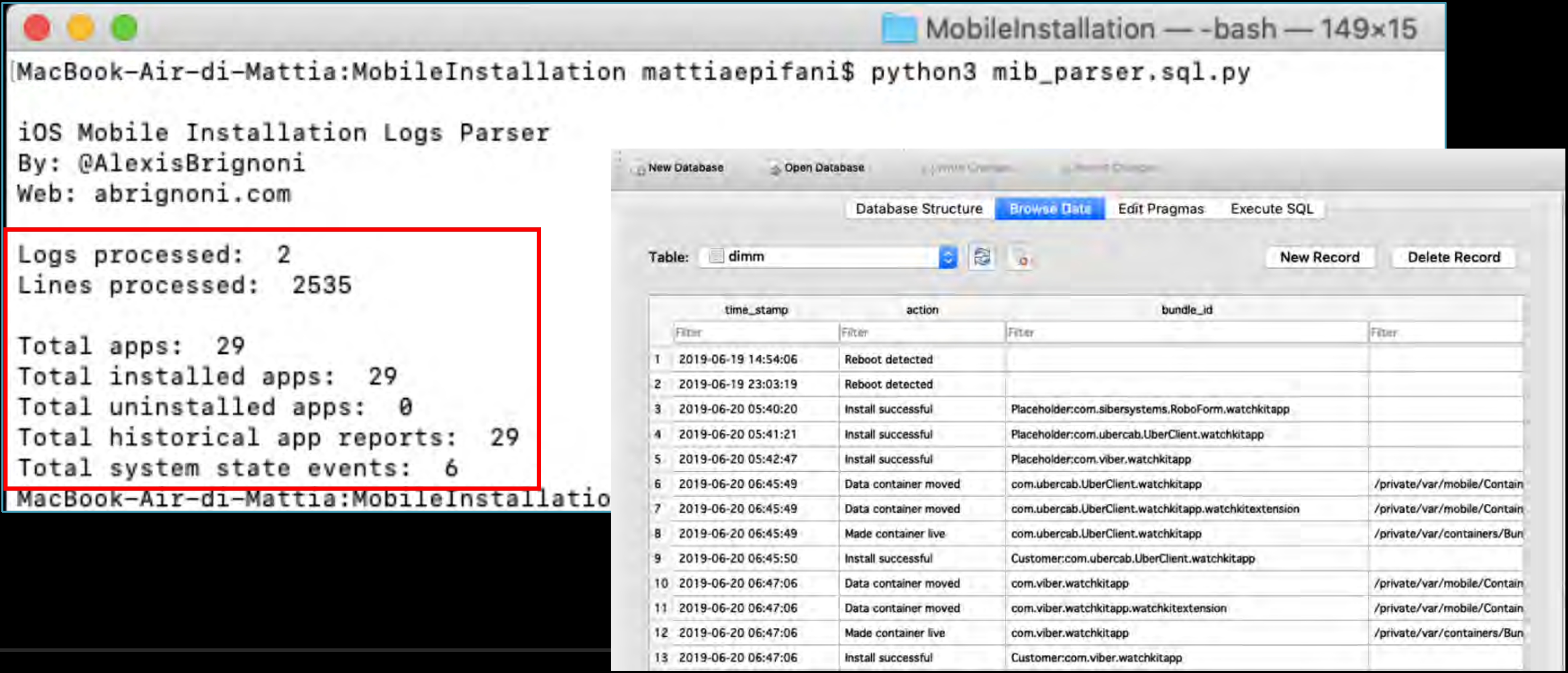
file = mattia/WiFi/WiFiManager/wifi.log
line = 23024

Directions: To here - From here

File Edit View Tools Add Help
Search
Get Directions History
Places
My Places
Sightseeing Tour
Temporary Places
mattia/WiFi/WiFiManager/wifi.log
didUpdateLocation
__WiFiManagerGeoTagNetwork
__WiFiManagerGeoTagNetwork1
__WiFiManagerGeoTagNetwork2
__WiFiManagerGeoTagNetwork3
__WiFiManagerGeoTagNetwork4
__WiFiManagerGeoTagNetwork5
__WiFiManagerGeoTagNetwork6
__WiFiManagerGeoTagNetwork7
Layers
Primary Database
Announcements
Borders and Labels
Places
Photos
Roads
3D Buildings
Ocean
Weather
Gallery
Global Awareness
More
Terrain
Sign in
WiFiManagerLocationManagerCallback46
WiFiManagerCopyCurrentLocation5
WiFiManagerGeoTagNetwork165
WiFiManagerGeoTagNetwork168
WiFiManagerGeoTagNetwork2
WiFiManagerGeoTagNetwork21
WiFiManagerGeoTagNetwork1
WiFiManagerGeoTagNetwork33
WiFiManagerGeoTagNetwork19
WiFiDeviceManagerScanPreviousNetworkChannel334
WiFiDeviceManagerScanPreviousNetworkChannel207
WiFiManagerGeoTagNetwork172
WiFiManagerLocationManagerCallback116
WiFiManagerGeoTagNetwork270
WiFiManagerLocationManagerCallback117
WiFiDeviceManagerAttemptNetworkTransition110
© 2018 Google
Google Earth

MOBILE INSTALLATION LOGS

https://abrignoni.blogspot.com/2019/01/ios-mobile-installation-logs-parser.html



```
MacBook-Air-di-Mattia:MobileInstallation mattiaepifani$ python3 mib_parser.sql.py

iOS Mobile Installation Logs Parser
By: @AlexisBrignoni
Web: abrignoni.com

Logs processed:  2
Lines processed:  2535

Total apps:  29
Total installed apps:  29
Total uninstalled apps:  0
Total historical app reports:  29
Total system state events:  6
MacBook-Air-di-Mattia:MobileInstallatio
```

	time_stamp	action	bundle_id	
	Filter	Filter	Filter	Filter
1	2019-06-19 14:54:06	Reboot detected		
2	2019-06-19 23:03:19	Reboot detected		
3	2019-06-20 05:40:20	Install successful	Placeholder:com.sibersystems.RoboForm.watchkitapp	
4	2019-06-20 05:41:21	Install successful	Placeholder:com.ubercab.UberClient.watchkitapp	
5	2019-06-20 05:42:47	Install successful	Placeholder:com.viber.watchkitapp	
6	2019-06-20 06:45:49	Data container moved	com.ubercab.UberClient.watchkitapp	/private/var/mobile/Contain
7	2019-06-20 06:45:49	Data container moved	com.ubercab.UberClient.watchkitapp.watchkitextension	/private/var/mobile/Contain
8	2019-06-20 06:45:49	Made container live	com.ubercab.UberClient.watchkitapp	/private/var/containers/Bun
9	2019-06-20 06:45:50	Install successful	Customer:com.ubercab.UberClient.watchkitapp	
10	2019-06-20 06:47:06	Data container moved	com.viber.watchkitapp	/private/var/mobile/Contain
11	2019-06-20 06:47:06	Data container moved	com.viber.watchkitapp.watchkitextension	/private/var/mobile/Contain
12	2019-06-20 06:47:06	Made container live	com.viber.watchkitapp	/private/var/containers/Bun
13	2019-06-20 06:47:06	Install successful	Customer:com.viber.watchkitapp	

What's Coming Next – Be Smart About Your Choice…

INSTALLING PROFILES ON THE DEVICE

- Other logs can be generated by installing specific "**profiles**" on the device
- Profiles can be downloaded from the Apple website
- The most interesting profiles from a digital forensics perspective are:
  - **Battery Life**
  - **Disk Space Diagnostics (FS Metadata)**
  - **WiFi (may already be there)**

Just Tell Me The Proper Order Already

If the "iTunes encryption" is haunting you

- The "Reset Network Settings" will scrub the com.apple.wifi.plist
- The "Reset All Settings" may scrub other logs – need more testing here
- Get at least Sysdiagnose first

When "PowerLogs" matter

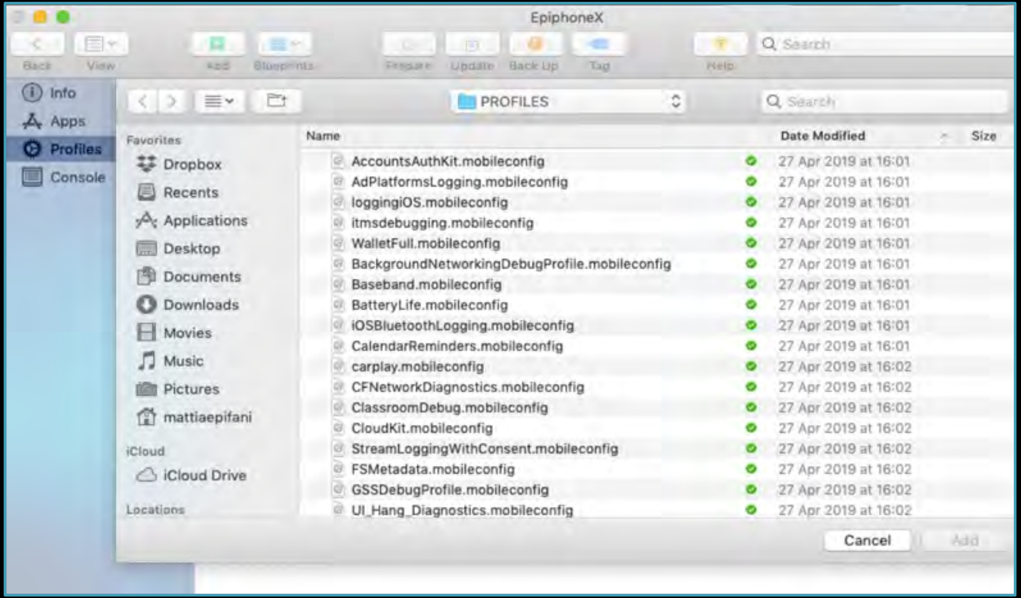
- i.e. What happened in the last 10 mins on the device?
- Here, you would install the Battery Life profile first
- Regular acquisition methods impact the logs
- APOLLO can be used to parse them

Yes, you are installing a profile on the device

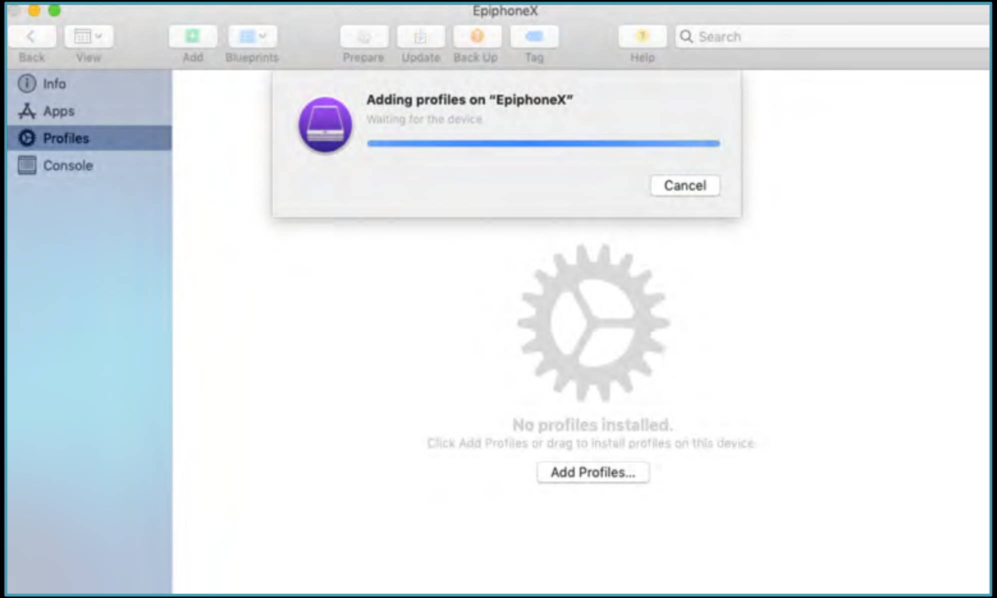
- We do this all of the time with logical extractions

Documentation and reasoning are key!

INSTALLING A PROFILE ON A DEVICE (I)



Name		Date Modified	Size
AccountsAuthKit.mobileconfig	✓	27 Apr 2019 at 16:01	
AdPlatformsLogging.mobileconfig	✓	27 Apr 2019 at 16:01	
loggingiOS.mobileconfig	✓	27 Apr 2019 at 16:01	
itmsdebugging.mobileconfig	✓	27 Apr 2019 at 16:01	
WalletFull.mobileconfig	✓	27 Apr 2019 at 16:01	
BackgroundNetworkingDebugProfile.mobileconfig	✓	27 Apr 2019 at 16:01	
Baseband.mobileconfig	✓	27 Apr 2019 at 16:01	
BatteryLife.mobileconfig	✓	27 Apr 2019 at 16:01	
iOSBluetoothLogging.mobileconfig	✓	27 Apr 2019 at 16:01	
CalendarReminders.mobileconfig	✓	27 Apr 2019 at 16:01	
carplay.mobileconfig	✓	27 Apr 2019 at 16:02	
CFNetworkDiagnostics.mobileconfig	✓	27 Apr 2019 at 16:02	
ClassroomDebug.mobileconfig	✓	27 Apr 2019 at 16:02	
CloudKit.mobileconfig	✓	27 Apr 2019 at 16:02	
StreamLoggingWithConsent.mobileconfig	✓	27 Apr 2019 at 16:02	
FSMetadata.mobileconfig	✓	27 Apr 2019 at 16:02	
GSSDebugProfile.mobileconfig	✓	27 Apr 2019 at 16:02	
UI_Hang_Diagnostics.mobileconfig	✓	27 Apr 2019 at 16:02	



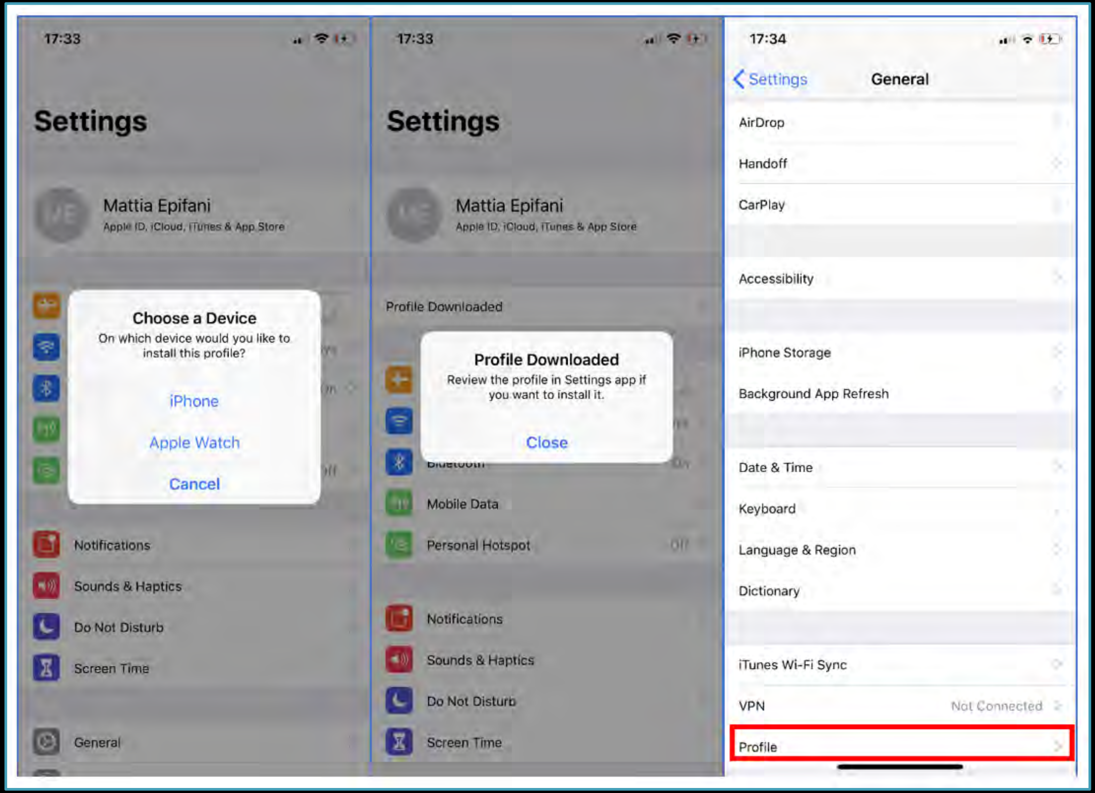
Adding profiles on "EpiphoneX"

Waiting for the device

No profiles installed.

Click Add Profiles or drag to install profiles on this device

INSTALLING A PROFILE ON A DEVICE (II)



Choose a Device

On which device would you like to install this profile?

iPhone

Apple Watch

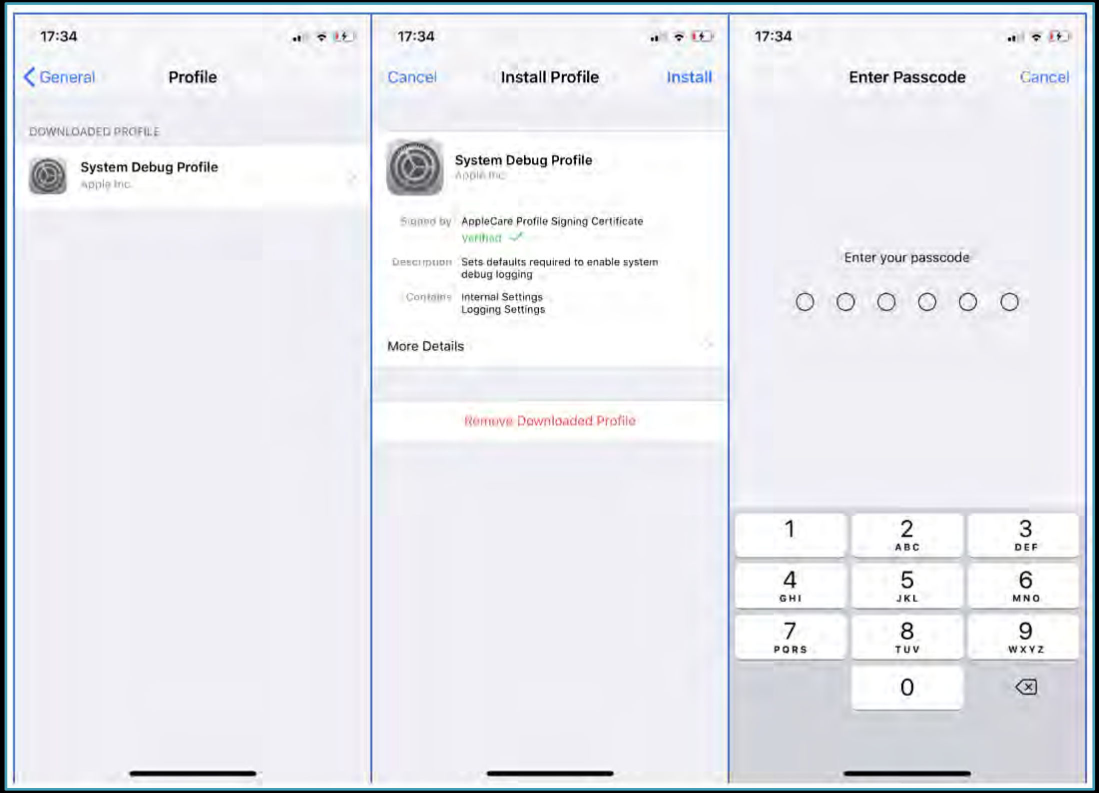
Cancel

Profile Downloaded

Review the profile in Settings app if you want to install it.

Close

VPN: Not Connected



System Debug Profile
Apple Inc.

System Debug Profile
Apple Inc.

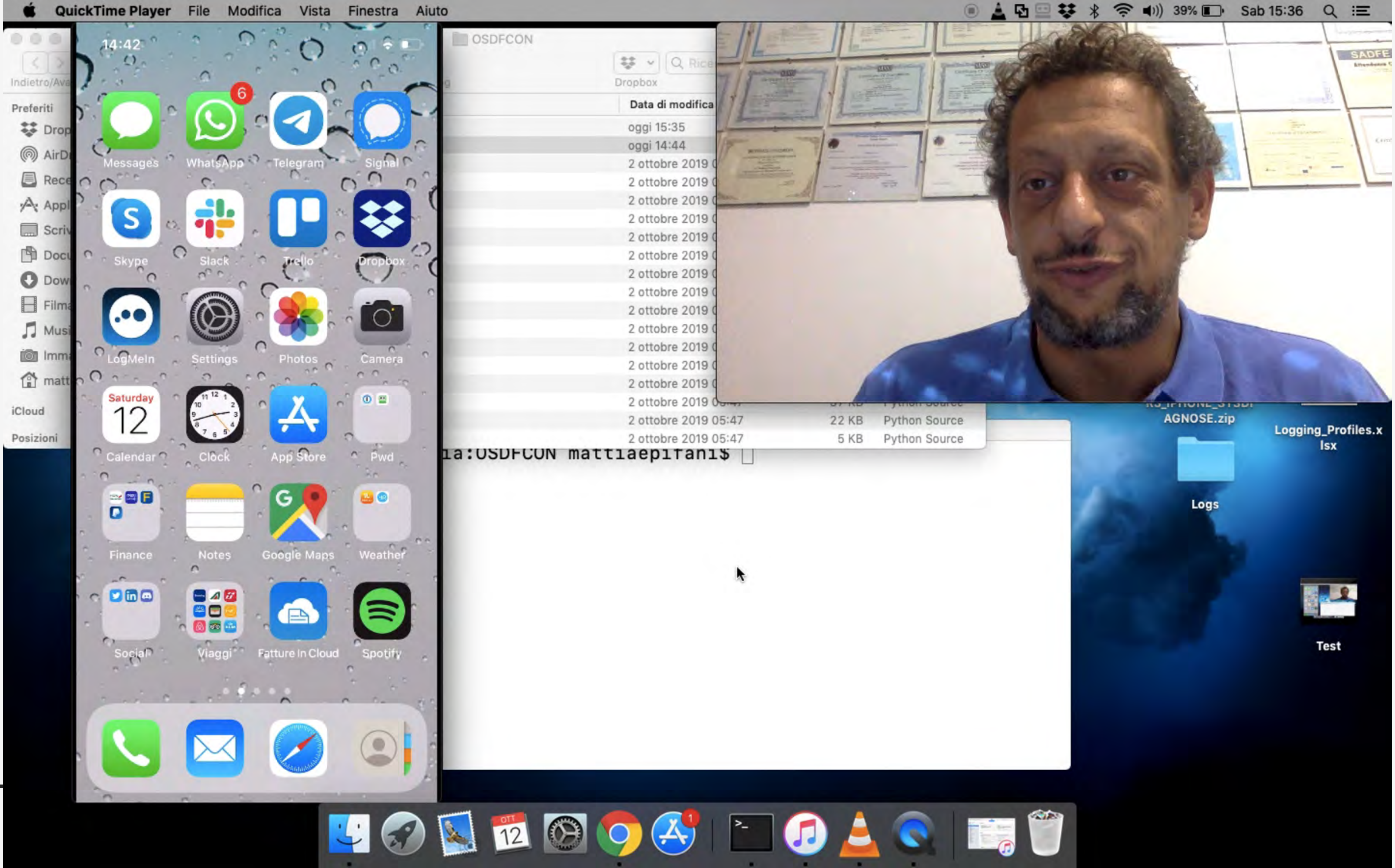
Signed by: AppleCare Profile Signing Certificate
Verified ✓

Description: Sets defaults required to enable system debug logging

Contains: Internal Settings
Logging Settings

Enter your passcode

○ ○ ○ ○ ○ ○



ogi 15:35
oggi 14:44
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 0
2 ottobre 2019 05:47   22 KB   Python Source
2 ottobre 2019 05:47   5 KB   Python Source

```
ia:OSDFCON mattiaepifani$ 
```

AGNOSE.zip

Logging_Profiles.xlsx

Considerations

- What if the device is locked?
- Is this forensically sound?
- What will your organizations/departments think?
- How can we get this peer reviewed?
- Profile Updates/Changes
  - File System profile went MIA ☹
- A full file system extraction gets some logs already
  - Cellebrite Premium, CAS and GrayKey
  - Sysdiagnose is NOT one of the logs captured by these methods – do it **after**
- Sysdiagnose is essentially us conducting "live forensics" on a Apple device
  - Research, Test, and Validate

SYSDIAGNOSE REFERENCES

- **Using Apple "Bug Reporting" for forensic purposes**
  https://www.for585.com/sysdiagnose
- **Apple Bug Reporting**
  https://developer.apple.com/bug-reporting/
- **Apple Profiles and Logs**
  https://developer.apple.com/bug-reporting/profiles-and-logs/
- **Understanding Crashes and Crash Logs**

  https://developer.apple.com/videos/play/wwdc2018/414/
- **Understanding and Analyzing Application Crash Reports**
  https://developer.apple.com/library/archive/technotes/tn2151/_index.html
- **Demystifying iOS Application Crash Logs**
  https://www.raywenderlich.com/2805-demystifying-ios-application-crash-logs
- **The ultimate diagnostic tool: sysdiagnose**
  https://eclecticlight.co/2016/02/06/the-ultimate-diagnostic-tool-sysdiagnose/
- **More useful information gleaned from sysdiagnose**
  https://eclecticlight.co/2016/02/08/more-useful-information-gleaned-from-sysdiagnose/
- **Running tools within sysdiagnose individually**
  https://eclecticlight.co/2016/02/08/running-tools-within-sysdiagnose-individually/
- **iOS Mobile Installation Logs**
  https://dfir.pubpub.org/pub/e5xlbw88

SYSDIAGNOSE TOOLS

- **Libimobiledevice** https://www.libimobiledevice.org/
- **iBackupBot** http://www.icopybot.com/itunes-backup-manager.htm
- **DB Browser for SQLite** https://sqlitebrowser.org/
- **Elcomsoft iOS Toolkit** https://www.elcomsoft.com/eift.html
- **iOS Sysdiagnose Forensic Scripts** https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts
- **iOS Mobile Installation Logs Parser** https://github.com/abrignoni/iOS-Mobile-Installation-Logs-Parser
- **APOLLO** https://github.com/mac4n6/APOLLO

Questions?

Mattia Epifani

- Digital Forensics Analyst
- CEO @ REALITY NET – System Solutions
- SANS Instructor, FOR585 / FOR500

mattia.epifani@realitynet.it
@mattiaep
http://www.linkedin.com/in/mattiaepifani
http://www.realitynet.it
http://blog.digital-forensics.it

Heather Mahalik

- Senior Director of Digital Intelligence
- Cellebrite
- SANS Senior Instructor, FOR585 / FOR500

Heather@cellebrite.com
@heathermahalik
https://it.linkedin.com/in/heathermahalik
www.smarterforensics.com/blog
www.cellebrite.com/en/blog