Order of Volatilty in Modern Smartphone Forensics

SANS DFIR SUMMIT, 22 JULY 2021

MATTIA EPIFANI

WHO AM I

- I live and work in Italy

- Master's Degree in IT in 2002 @ UNIGE

- Founder and CEO @ REALITY NET
- Digital Forensics Analyst

- Contract professor in Digital Forensics @ UNIGE
- SANS Institute Certified Instructor FOR585/FOR500

- Researcher at IGSG – CNR (Italian National Council of Research)

ORDER OF VOLATILTY

https://datatracker.ietf.org/doc/html/rfc3227#section-2.1

- RFC 3227 – February 2002
- *When collecting evidence* ***you should proceed from the volatile to the less volatile***
- *Here is an example order of volatility for a typical system.*
  - *registers, cache*
  - *routing table, arp cache, process table, kernel statistics, memory*
  - *temporary file systems*
  - *disk*
  - *remote logging and monitoring data that is relevant to the system in question*
  - *physical configuration, network topology*
  - *archival media*

ORDER OF VOLATILTY ON MOBILE DEVICES

- **Key and general questions**
- Is the device turned on or off?
- If it's turned on, is it locked or unlocked?
- If it's turned on and locked, can you access (code or biometric or other)?

TURNED OFF DEVICES

- Do you know the **exact model**?
- Is there any method that can be used to create a **physical image** (typically on FDE devices) or a **full file system** (typically on FBE devices)?
- Is this method working at a low-level, so that it doesn’t need to boot the OS?
- Examples:
  - Checkm8 on iOS devices
  - Bootloader-based acquisition on Android devices
  - EDL mode on Android devices with Qualcomm chipsets
  - Qualcomm/MTK Live

WHAT’S THE CORRECT ORDER?

- **It depends! ☺**

- If you can create a physical/full file system without booting the OS and you trust the method, go for it

- But if you need to:
  - turn on the device (or the device is turned on)
  - interact with it (i.e. activate USB debugging)
  - pair it with your forensic workstation
- In this case, **you should approach in a way that acquires the data from the most volatile to the less volatile**

ANDROID DEVICES

- When no solution is available to create a physical/full file system image, we typically rely on:
  - **Agent installation**
    - Android agent to extract data from content providers and screenshots
  - **Backup features**
    - Native (ADB)
    - Vendor based (Huawei HiSuite, Samsung SmartSwitch, LG)
  - **Application downgrade**

- Can we get more?
- What’s the correct order?

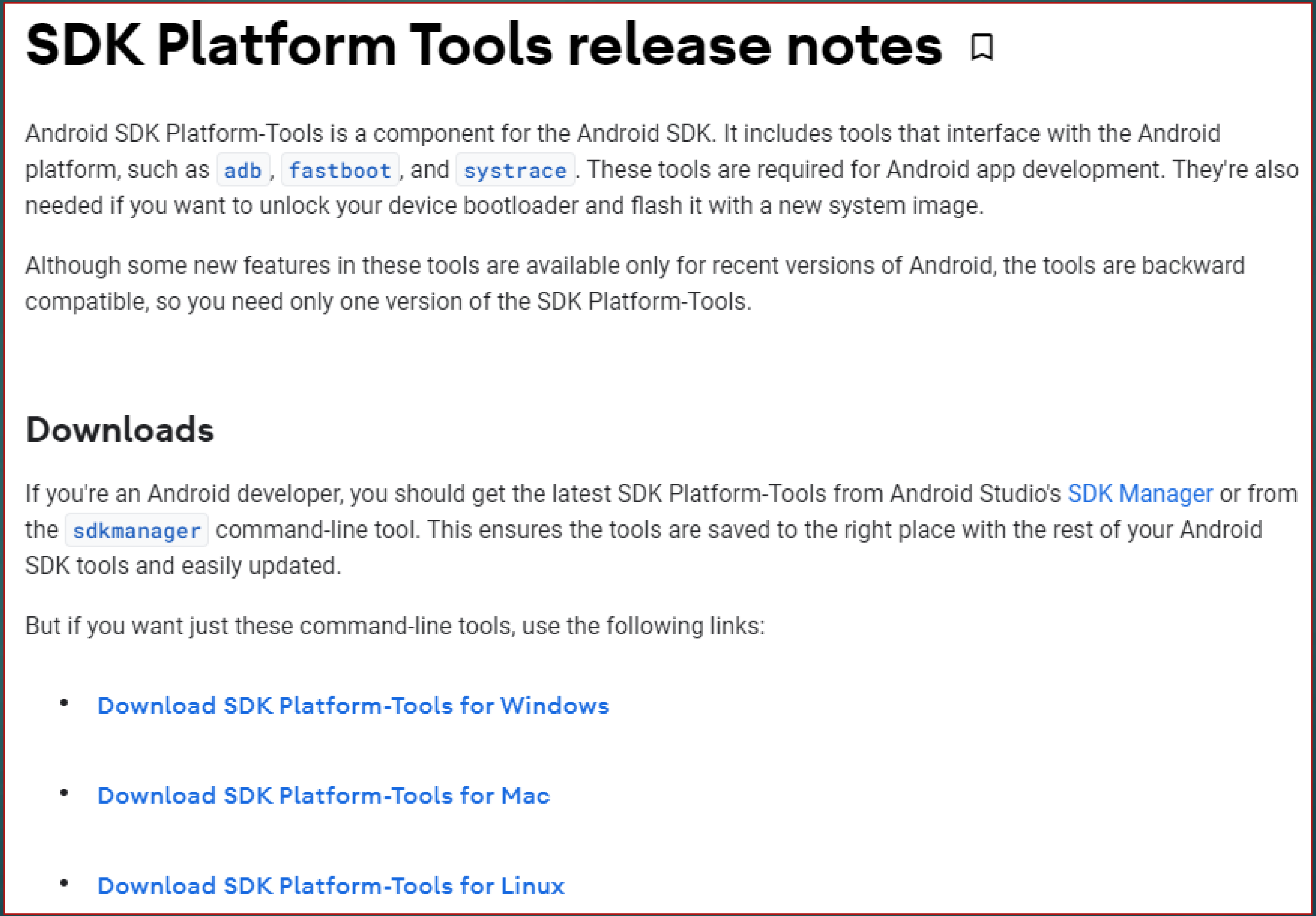
ADB

https://developer.android.com/studio/command-line/adb

- ***Android Debug Bridge*** *(adb) is a versatile command-line tool that lets you* ***communicate with a device***
- *To use adb with a device connected over USB, you* ***must enable USB debugging in the device system settings****, under* ***Developer*** *options*
- *On Android 4.2 and higher, the Developer options screen is hidden by default. To make it visible, go to* ***Settings > About phone and tap Build number seven times****. Return to the previous screen to find Developer options at the bottom*
- *On some devices, the Developer options screen might be located or named differently.*

ADB

https://developer.android.com/studio/releases/platform-tools



SDK Platform Tools release notes

Android SDK Platform-Tools is a component for the Android SDK. It includes tools that interface with the Android platform, such as `adb`, `fastboot`, and `systrace`. These tools are required for Android app development. They're also needed if you want to unlock your device bootloader and flash it with a new system image.

Although some new features in these tools are available only for recent versions of Android, the tools are backward compatible, so you need only one version of the SDK Platform-Tools.

Downloads

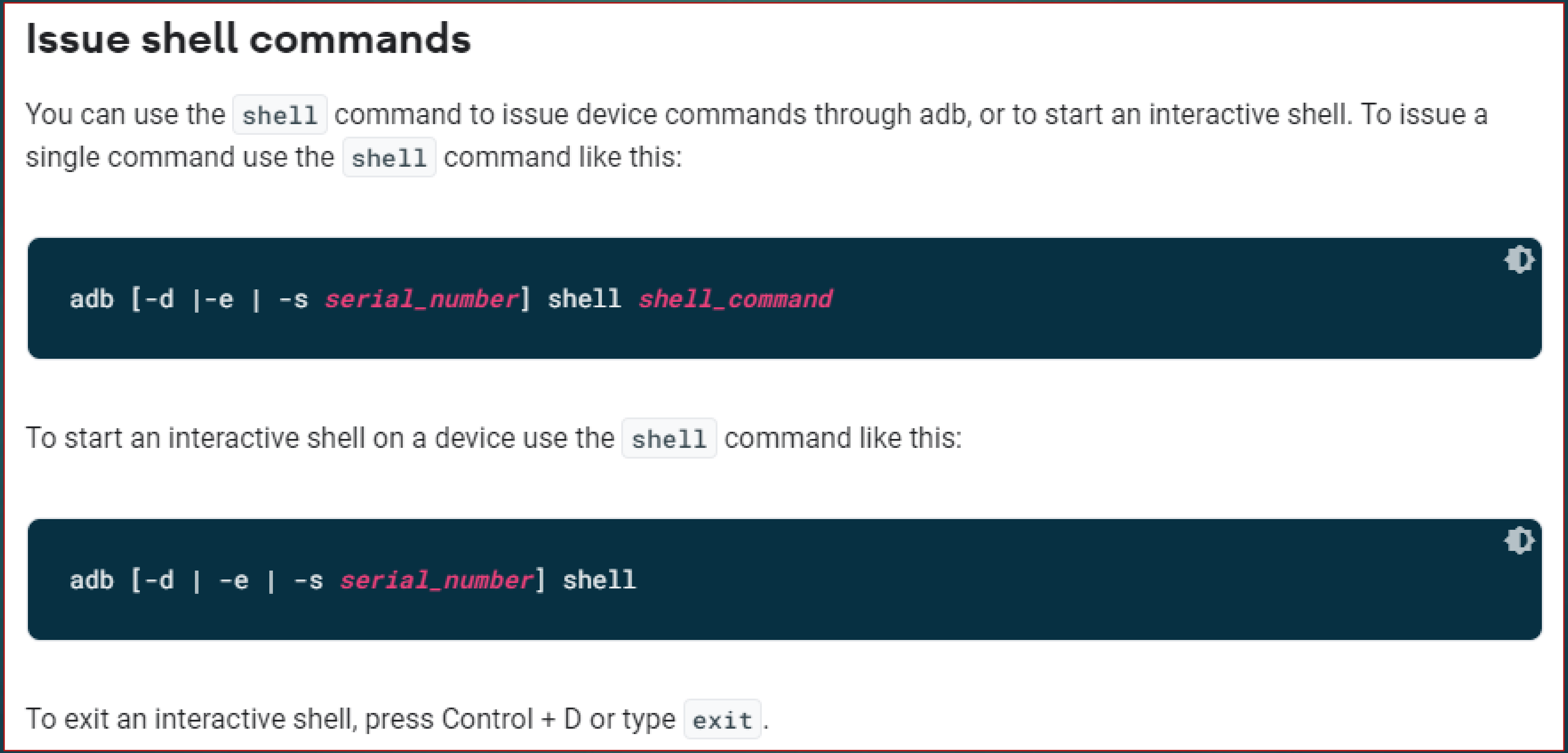
If you're an Android developer, you should get the latest SDK Platform-Tools from Android Studio's SDK Manager or from the `sdkmanager` command-line tool. This ensures the tools are saved to the right place with the rest of your Android SDK tools and easily updated.

But if you want just these command-line tools, use the following links:

- Download SDK Platform-Tools for Windows
- Download SDK Platform-Tools for Mac
- Download SDK Platform-Tools for Linux

ADB SHELL

https://developer.android.com/studio/command-line/adb



Issue shell commands

You can use the `shell` command to issue device commands through adb, or to start an interactive shell. To issue a single command use the `shell` command like this:

```
adb [-d |-e | -s serial_number] shell shell_command
```

To start an interactive shell on a device use the `shell` command like this:

```
adb [-d | -e | -s serial_number] shell
```

To exit an interactive shell, press Control + D or type `exit`.

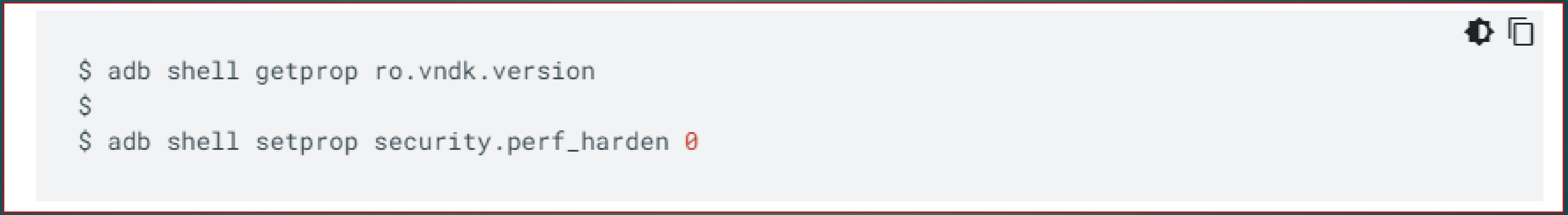
COMMAND TYPES

- Getprop
- Linux
- Dumpsys
- Package Manager
- Backup
- Pull
  - Partial file system
  - APKs

GETPROP

https://source.android.com/devices/architecture/configuration/add-system-properties#shell-commands

- *The **getprop** command can be used to read device properties*



```
$ adb shell getprop ro.vndk.version
$
$ adb shell setprop security.perf_harden 0
```

Getprop

getprop ro.product.model	Device model
getprop ro.product.manufacturer	Device manufacturer
getprop ro.serialno	Device serial number
getprop ro.build.fingerprint	Android fingerprint
getprop ro.build.version.release	Android version
getprop ro.build.date	Build date
getprop ro.build.id	Build ID
getprop ro.boot.bootloader	Bootloader info
getprop ro.build.version.security_patch	Security Patch
getprop persist.sys.timezone	Timezone

Getprop

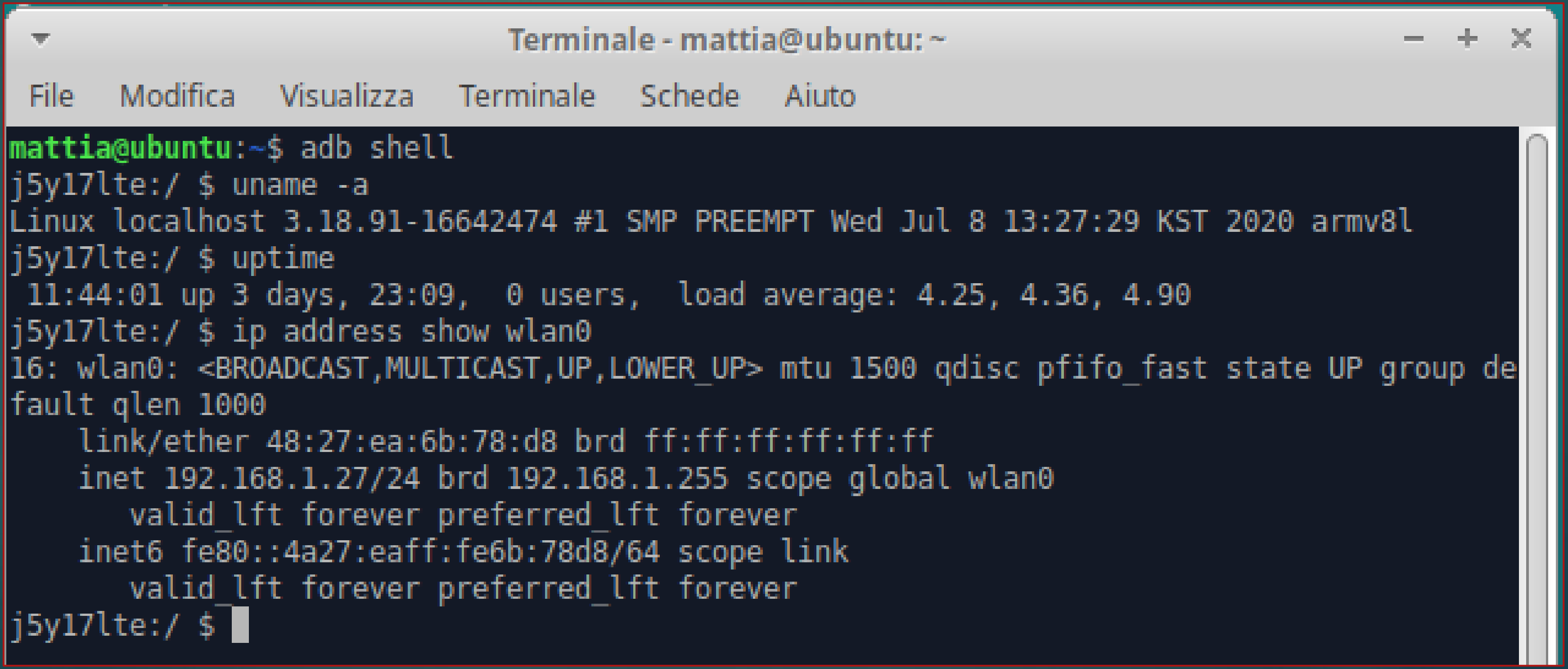
getprop ro.product.device	Product device
getprop ro.product.name	Product name
getprop ro.product.code	Product code
getprop ro.chipname	Chipname
getprop ril.serialnumber	Device Serial Number
getprop gsm.version.baseband	Baseband version
getprop ro.csc.country_code	Country Code
getprop persist.sys.usb.config	USB Configuration
getprop storage.mmc.size	Storage size
getprop ro.crypto.state	Encryption state

Linux commands

- id
- uname -a
- cat /proc/version
- uptime
- printenv
- cat /proc/partitions
- cat /proc/cpuinfo
- cat /proc/diskstats
- df
- df -ah
- mount
- ip address show wlan0
- ifconfig -a
- netstat -an
- lsof
- ps -ef
- top -n 1
- cat /proc/sched_debug
- vmstat
- sysctl -a
- ime list
- service list
- logcat -S -b all
- logcat -d -b all V:*

Linux commands

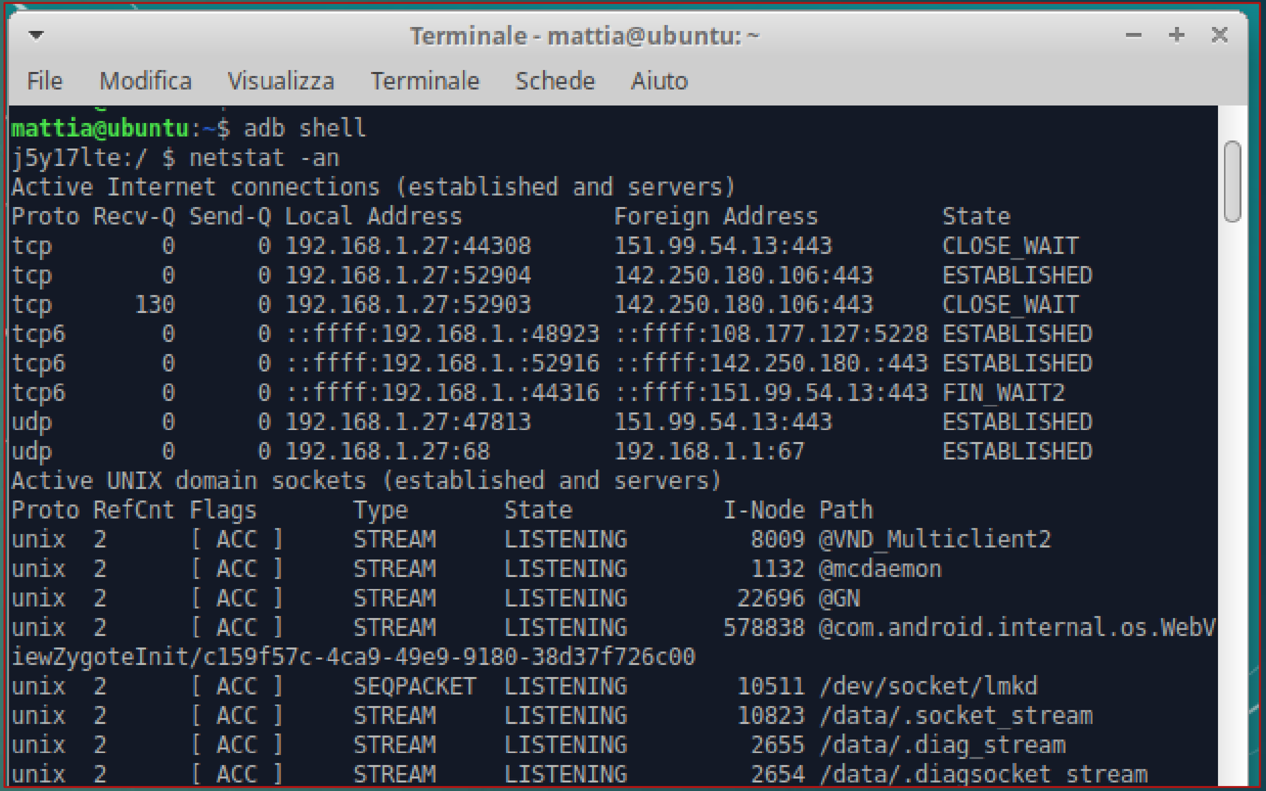
- Linux version
- System time and uptime
- IP Address on WiFi



```
mattia@ubuntu:~$ adb shell
j5y17lte:/ $ uname -a
Linux localhost 3.18.91-16642474 #1 SMP PREEMPT Wed Jul 8 13:27:29 KST 2020 armv8l
j5y17lte:/ $ uptime
 11:44:01 up 3 days, 23:09,  0 users,  load average: 4.25, 4.36, 4.90
j5y17lte:/ $ ip address show wlan0
16: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group de
fault qlen 1000
    link/ether 48:27:ea:6b:78:d8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.27/24 brd 192.168.1.255 scope global wlan0
       valid_lft forever preferred_lft forever
    inet6 fe80::4a27:eaff:fe6b:78d8/64 scope link
       valid_lft forever preferred_lft forever
j5y17lte:/ $ 
```

netstat -an

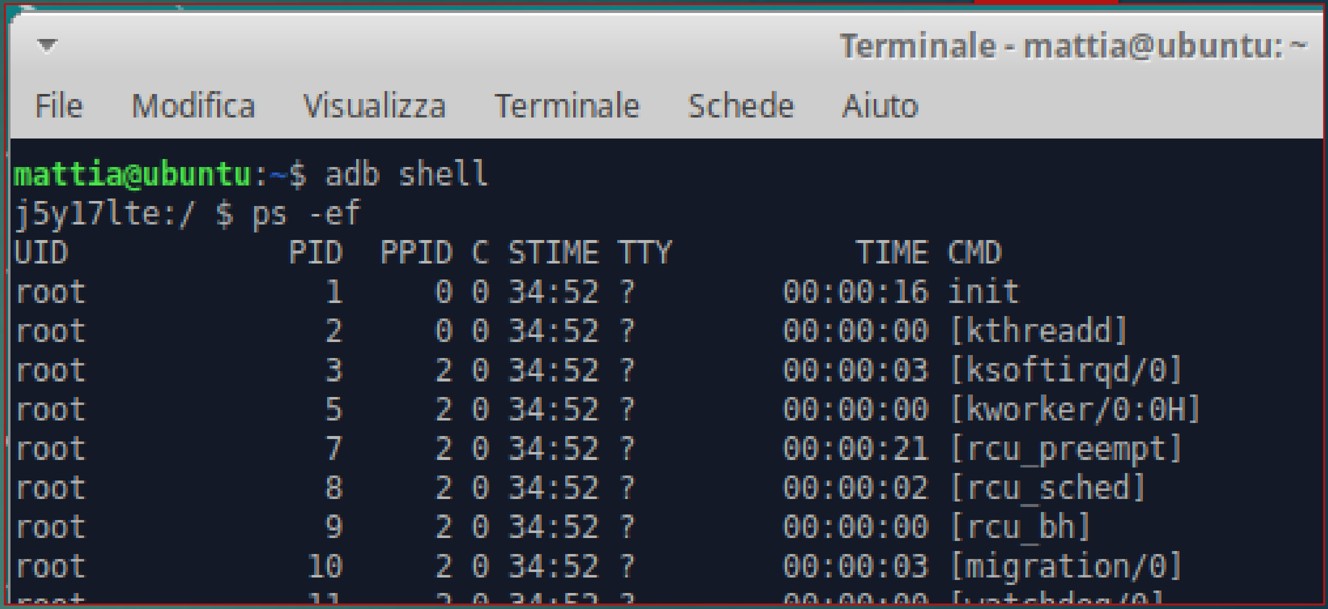
- Network connections
- All sockets (-a)
- Don’t resolve names (-n)



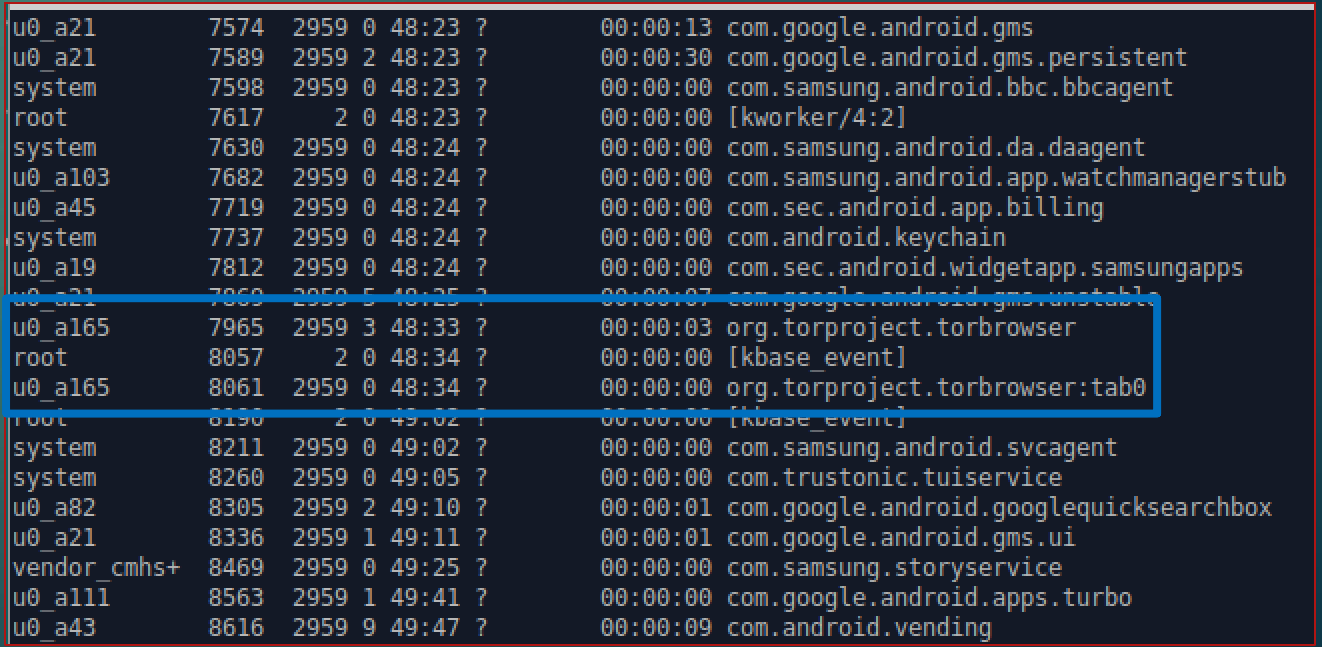
```
mattia@ubuntu:~$ adb shell
j5y17lte:/ $ netstat -an
Active Internet connections (established and servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.1.27:44308      151.99.54.13:443        CLOSE_WAIT
tcp        0      0 192.168.1.27:52904      142.250.180.106:443     ESTABLISHED
tcp      130      0 192.168.1.27:52903      142.250.180.106:443     CLOSE_WAIT
tcp6       0      0 ::ffff:192.168.1.:48923 ::ffff:108.177.127:5228 ESTABLISHED
tcp6       0      0 ::ffff:192.168.1.:52916 ::ffff:142.250.180.:443 ESTABLISHED
tcp6       0      0 ::ffff:192.168.1.:44316 ::ffff:151.99.54.13:443 FIN_WAIT2
udp        0      0 192.168.1.27:47813      151.99.54.13:443        ESTABLISHED
udp        0      0 192.168.1.27:68         192.168.1.1:67          ESTABLISHED
Active UNIX domain sockets (established and servers)
Proto RefCnt Flags       Type       State           I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING         8009 @VND_Multiclient2
unix  2      [ ACC ]     STREAM     LISTENING         1132 @mcdaemon
unix  2      [ ACC ]     STREAM     LISTENING        22696 @GN
unix  2      [ ACC ]     STREAM     LISTENING       578838 @com.android.internal.os.WebV
iewZygoteInit/c159f57c-4ca9-49e9-9180-38d37f726c00
unix  2      [ ACC ]     SEQPACKET  LISTENING        10511 /dev/socket/lmkd
unix  2      [ ACC ]     STREAM     LISTENING        10823 /data/.socket_stream
unix  2      [ ACC ]     STREAM     LISTENING         2655 /data/.diag_stream
unix  2      [ ACC ]     STREAM     LISTENING         2654 /data/.diagsocket_stream
```

ps -ef

- Running processes
- Every process (-e)
- Full-format listing (-f)



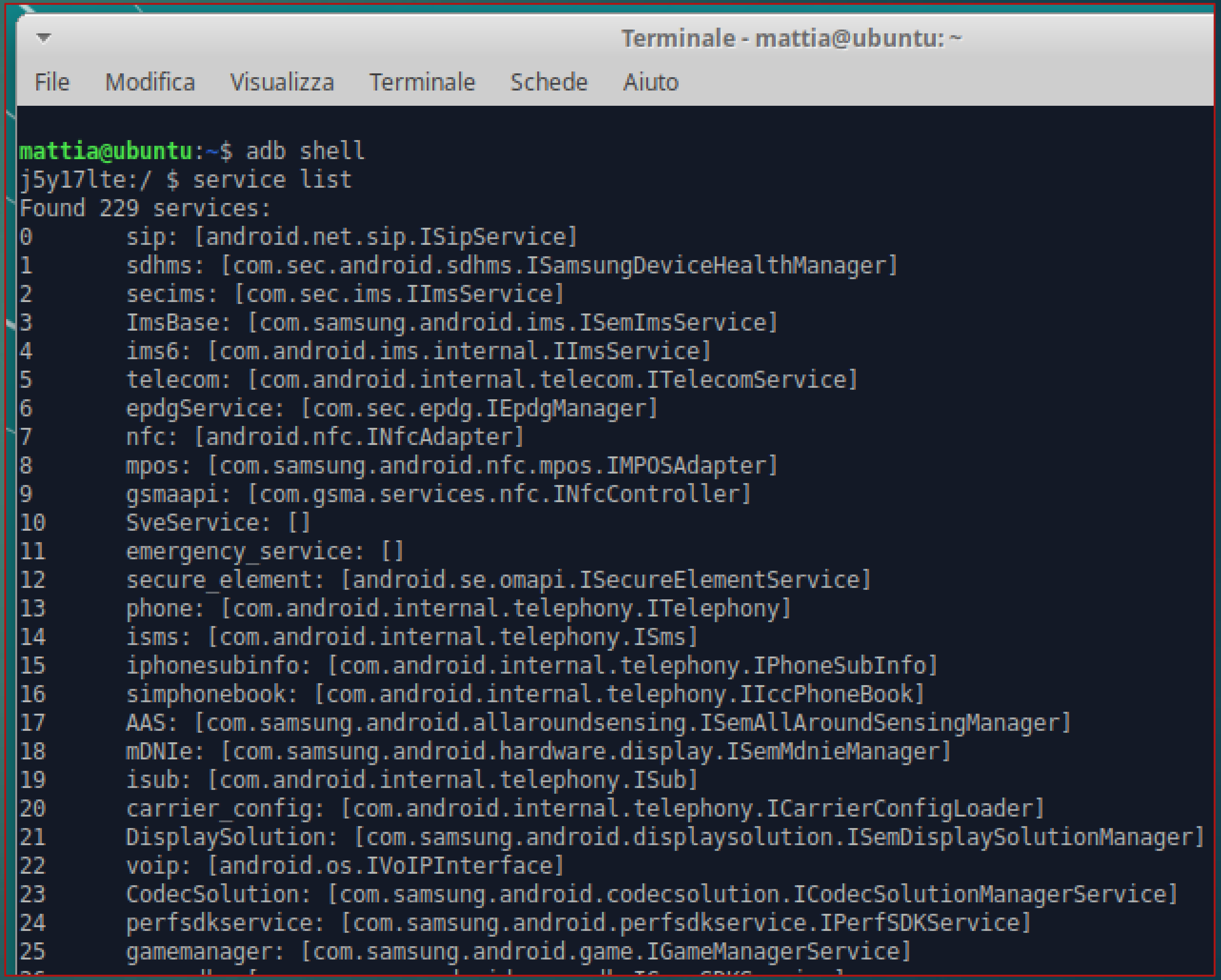
```
mattia@ubuntu:~$ adb shell
j5y17lte:/ $ ps -ef
UID            PID  PPID C STIME TTY          TIME CMD
root             1     0 0 34:52 ?        00:00:16 init
root             2     0 0 34:52 ?        00:00:00 [kthreadd]
root             3     2 0 34:52 ?        00:00:03 [ksoftirqd/0]
root             5     2 0 34:52 ?        00:00:00 [kworker/0:0H]
root             7     2 0 34:52 ?        00:00:21 [rcu_preempt]
root             8     2 0 34:52 ?        00:00:02 [rcu_sched]
root             9     2 0 34:52 ?        00:00:00 [rcu_bh]
root            10     2 0 34:52 ?        00:00:03 [migration/0]
root            11     2 0 34:52 ?        00:00:00 [watchdog/0]
```



```
u0_a21        7574  2959 0 48:23 ?        00:00:13 com.google.android.gms
u0_a21        7589  2959 2 48:23 ?        00:00:30 com.google.android.gms.persistent
system        7598  2959 0 48:23 ?        00:00:00 com.samsung.android.bbc.bbcagent
root          7617     2 0 48:23 ?        00:00:00 [kworker/4:2]
system        7630  2959 0 48:24 ?        00:00:00 com.samsung.android.da.daagent
u0_a103       7682  2959 0 48:24 ?        00:00:00 com.samsung.android.app.watchmanagerstub
u0_a45        7719  2959 0 48:24 ?        00:00:00 com.sec.android.app.billing
system        7737  2959 0 48:24 ?        00:00:00 com.android.keychain
u0_a19        7812  2959 0 48:24 ?        00:00:00 com.sec.android.widgetapp.samsungapps
u0_a21        7869  2959 5 48:25 ?        00:00:07 com.google.android.gms.unstable
u0_a165       7965  2959 3 48:33 ?        00:00:03 org.torproject.torbrowser
root          8057     2 0 48:34 ?        00:00:00 [kbase_event]
u0_a165       8061  2959 0 48:34 ?        00:00:00 org.torproject.torbrowser:tab0
root          8190     2 0 49:02 ?        00:00:00 [kbase_event]
system        8211  2959 0 49:02 ?        00:00:00 com.samsung.android.svcagent
system        8260  2959 0 49:05 ?        00:00:00 com.trustonic.tuiservice
u0_a82        8305  2959 2 49:10 ?        00:00:01 com.google.android.googlequicksearchbox
u0_a21        8336  2959 1 49:11 ?        00:00:01 com.google.android.gms.ui
vendor_cmhs+  8469  2959 0 49:25 ?        00:00:00 com.samsung.storyservice
u0_a111       8563  2959 1 49:41 ?        00:00:00 com.google.android.apps.turbo
u0_a43        8616  2959 9 49:47 ?        00:00:09 com.android.vending
```

service list

- Running services



```
mattia@ubuntu:~$ adb shell
j5y17lte:/ $ service list
Found 229 services:
0       sip: [android.net.sip.ISipService]
1       sdhms: [com.sec.android.sdhms.ISamsungDeviceHealthManager]
2       secims: [com.sec.ims.IImsService]
3       ImsBase: [com.samsung.android.ims.ISemImsService]
4       ims6: [com.android.ims.internal.IImsService]
5       telecom: [com.android.internal.telecom.ITelecomService]
6       epdgService: [com.sec.epdg.IEpdgManager]
7       nfc: [android.nfc.INfcAdapter]
8       mpos: [com.samsung.android.nfc.mpos.IMPOSAdapter]
9       gsmaapi: [com.gsma.services.nfc.INfcController]
10      SveService: []
11      emergency_service: []
12      secure_element: [android.se.omapi.ISecureElementService]
13      phone: [com.android.internal.telephony.ITelephony]
14      isms: [com.android.internal.telephony.ISms]
15      iphonesubinfo: [com.android.internal.telephony.IPhoneSubInfo]
16      simphonebook: [com.android.internal.telephony.IIccPhoneBook]
17      AAS: [com.samsung.android.allaroundsensing.ISemAllAroundSensingManager]
18      mDNIe: [com.samsung.android.hardware.display.ISemMdnieManager]
19      isub: [com.android.internal.telephony.ISub]
20      carrier_config: [com.android.internal.telephony.ICarrierConfigLoader]
21      DisplaySolution: [com.samsung.android.displaysolution.ISemDisplaySolutionManager]
22      voip: [android.os.IVoIPInterface]
23      CodecSolution: [com.samsung.android.codecsolution.ICodecSolutionManagerService]
24      perfsdkservice: [com.samsung.android.perfsdkservice.IPerfSDKService]
25      gamemanager: [com.samsung.android.game.IGameManagerService]
```

Services

- account
- activity
- alarm
- appops
- audio
- autofill
- backup
- battery
- batteryproperties
- batterystats
- bluetooth_manager
- carrier_config
- clipboard
- connectivity
- content
- cpuinfo
- dbinfo -v
- device_policy
- devicestoragemonitor
- diskstats

Services

- display
- dropbox
- gfxinfo
- iphonesubinfo
- jobscheduler
- location
- -t 60 meminfo -a
- mount
- netpolicy
- netstats
- network_management
- network_score
- notification --noredact
- package
- password_policy
- permission
- phone
- power
- procstats --full-details
- restriction_policy

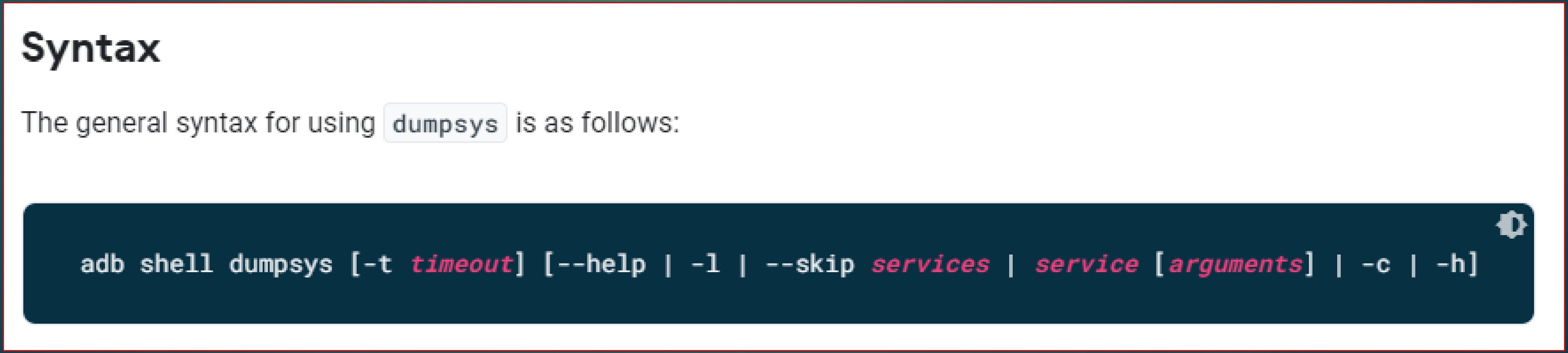
Services

- sdhms
- sec_location
- secims
- search
- sensorservice
- settings
- shortcut
- stats
- statusbar
- storaged
- telecom
- usagestats
- user
- usb
- vibrator
- wallpaper
- wifi
- window

DUMPSYS

https://developer.android.com/studio/command-line/dumpsys

- *dumpsys is a tool that runs on Android devices and* ***provides information about system services****.*
- *You can call dumpsys from the command line using the Android Debug Bridge (ADB) to get* ***diagnostic output for all system services running on a connected device***



Syntax

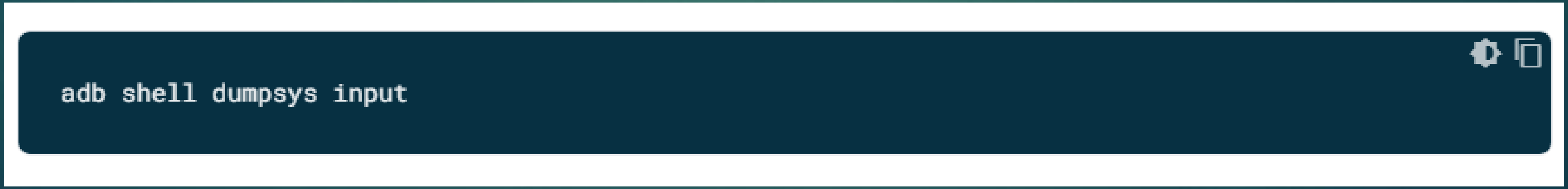
The general syntax for using `dumpsys` is as follows:

```
adb shell dumpsys [-t timeout] [--help | -l | --skip services | service [arguments] | -c | -h]
```

DUMPSYS

https://developer.android.com/studio/command-line/dumpsys

- *To get a diagnostic output for all system services for your connected device, simply run **adb shell dumpsys***
- *However, this outputs far more information than you would typically want*
- *For more manageable output, **specify the service you want to examine by including it in the command***
- *For example, the command below provides system data for input components, such as touchscreens or built-in keyboards*

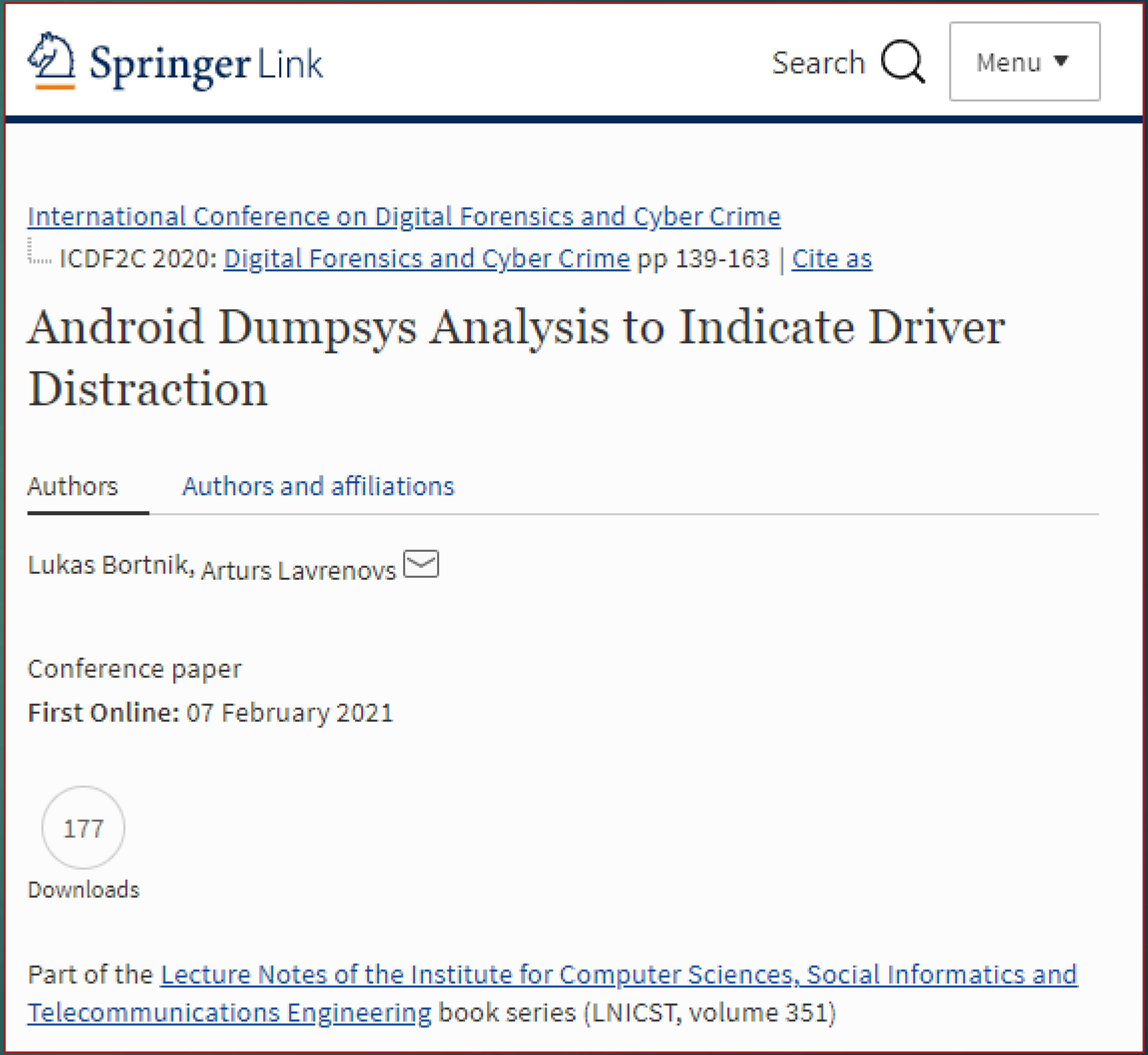


```
adb shell dumpsys input
```

Android Dumpsys Analysis to Indicate Driver Distraction

https://ccdcoe.org/uploads/2021/03/Android-Dumpsys-Analysis-to-Indicate-Driver-Distraction.pdf

- *This paper introduces a non-intrusive analysis method which will extend the range of known techniques to determine a possible cause of driver distraction*
- *All Android dumpsys services are examined to identify the scope of evidence providers which can assist investigators in identifying the driver's intentional interaction with the smartphone*
- *The study demonstrates that it is possible to identify a driver's activities without access to their personal content*



International Conference on Digital Forensics and Cyber Crime

ICDF2C 2020: Digital Forensics and Cyber Crime pp 139-163 | Cite as

Android Dumpsys Analysis to Indicate Driver Distraction

Authors | Authors and affiliations

Lukas Bortnik, Arturs Lavrenovs

Conference paper

First Online: 07 February 2021

177

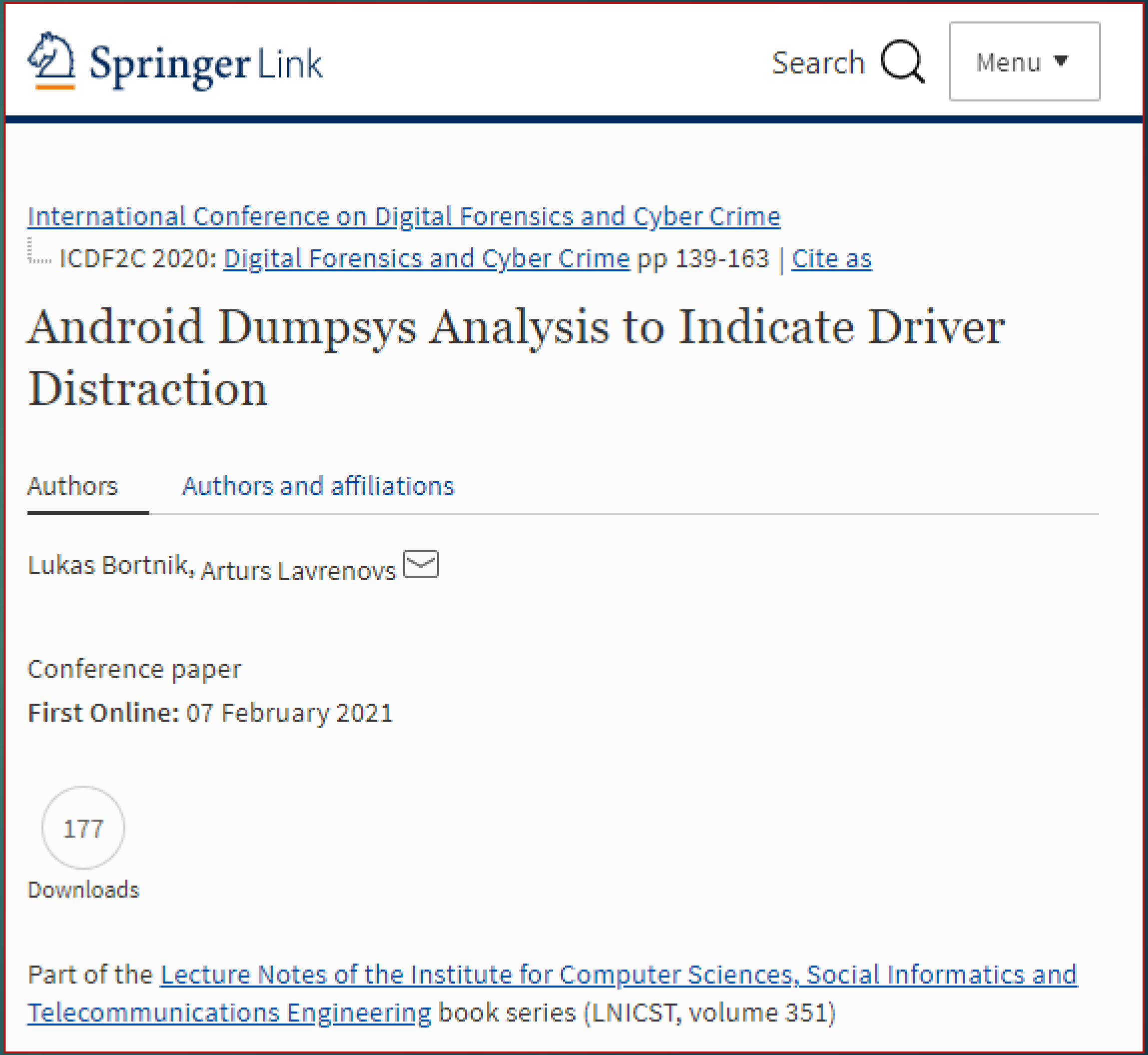
Downloads

Part of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering book series (LNICST, volume 351)

Android Dumpsys Analysis to Indicate Driver Distraction

https://ccdcoe.org/uploads/2021/03/Android-Dumpsys-Analysis-to-Indicate-Driver-Distraction.pdf

- *As with any other operating system, much of the analytical data generated by system services, installed applications or telemetry functions is **not designed for digital forensic purposes***
- *The primary drawback is that **only a limited number of subject-relevant system events are time-stamped***
- *Moreover, **system services do not necessarily generate diagnostic events with a unified timestamp format.***
- *Even if some diagnostic data does survive a system reboot, **particular content was shown to be eventually overwritten, either due to user interaction or just after regular system runtime***



International Conference on Digital Forensics and Cyber Crime

ICDF2C 2020: Digital Forensics and Cyber Crime pp 139-163 | Cite as

Android Dumpsys Analysis to Indicate Driver Distraction

Lukas Bortnik, Arturs Lavrenovs

Conference paper

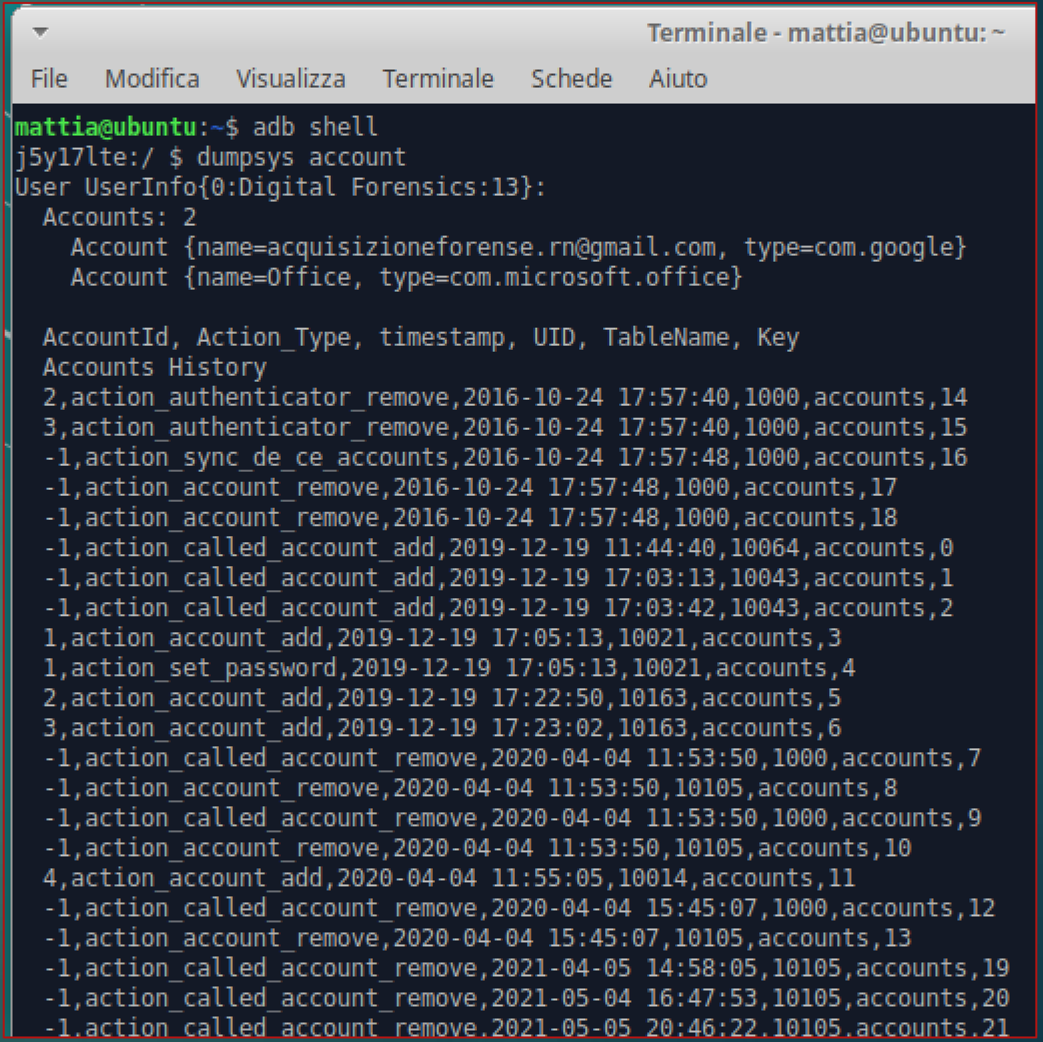
First Online: 07 February 2021

177
Downloads

Part of the Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering book series (LNICST, volume 351)

dumpsys **account**

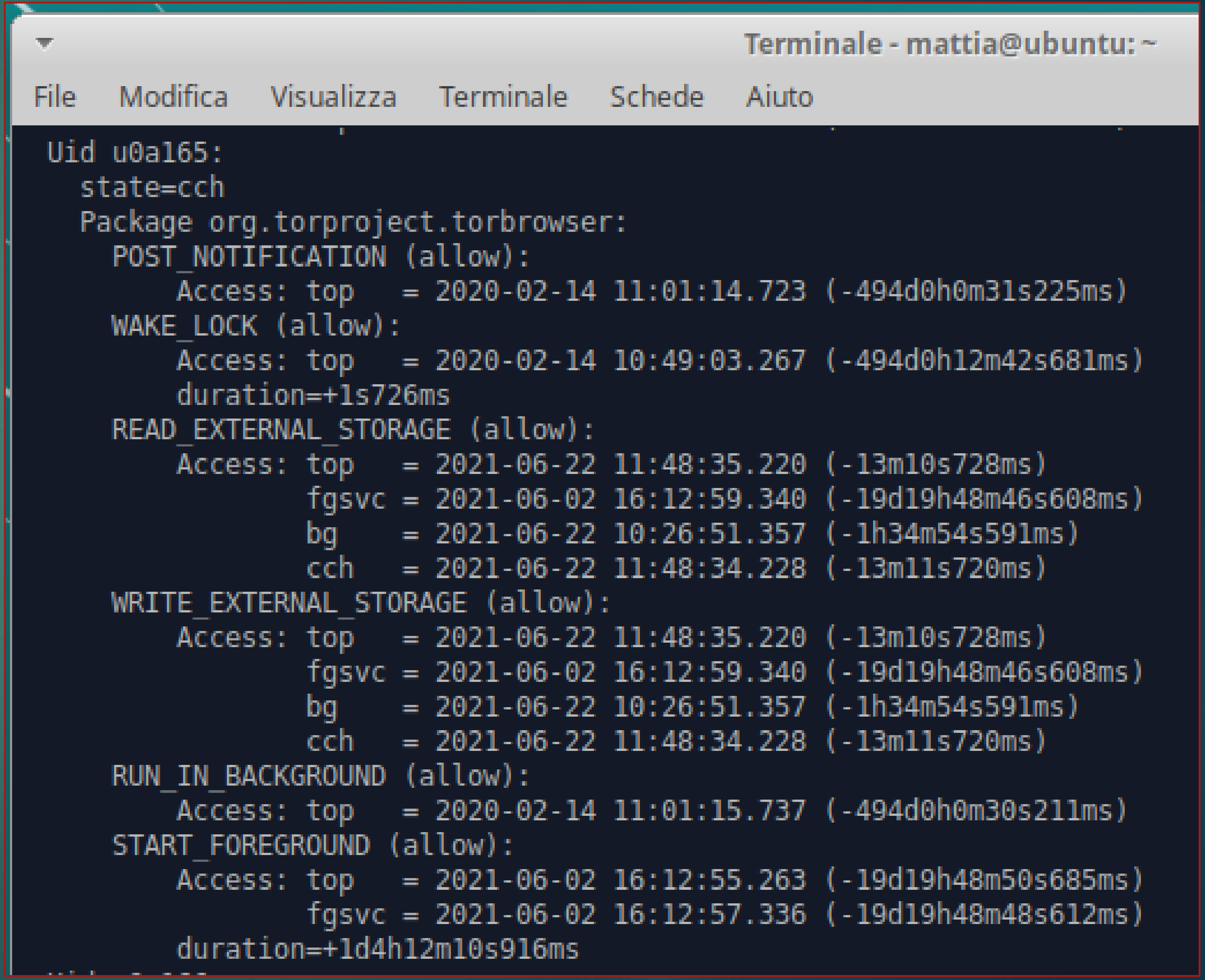
- Account information



```
mattia@ubuntu:~$ adb shell
j5y17lte:/ $ dumpsys account
User UserInfo{0:Digital Forensics:13}:
  Accounts: 2
    Account {name=acquisizioneforense.rn@gmail.com, type=com.google}
    Account {name=Office, type=com.microsoft.office}

  AccountId, Action_Type, timestamp, UID, TableName, Key
  Accounts History
  2,action_authenticator_remove,2016-10-24 17:57:40,1000,accounts,14
  3,action_authenticator_remove,2016-10-24 17:57:40,1000,accounts,15
  -1,action_sync_de_ce_accounts,2016-10-24 17:57:48,1000,accounts,16
  -1,action_account_remove,2016-10-24 17:57:48,1000,accounts,17
  -1,action_account_remove,2016-10-24 17:57:48,1000,accounts,18
  -1,action_called_account_add,2019-12-19 11:44:40,10064,accounts,0
  -1,action_called_account_add,2019-12-19 17:03:13,10043,accounts,1
  -1,action_called_account_add,2019-12-19 17:03:42,10043,accounts,2
  1,action_account_add,2019-12-19 17:05:13,10021,accounts,3
  1,action_set_password,2019-12-19 17:05:13,10021,accounts,4
  2,action_account_add,2019-12-19 17:22:50,10163,accounts,5
  3,action_account_add,2019-12-19 17:23:02,10163,accounts,6
  -1,action_called_account_remove,2020-04-04 11:53:50,1000,accounts,7
  -1,action_account_remove,2020-04-04 11:53:50,10105,accounts,8
  -1,action_called_account_remove,2020-04-04 11:53:50,1000,accounts,9
  -1,action_account_remove,2020-04-04 11:53:50,10105,accounts,10
  4,action_account_add,2020-04-04 11:55:05,10014,accounts,11
  -1,action_called_account_remove,2020-04-04 15:45:07,1000,accounts,12
  -1,action_account_remove,2020-04-04 15:45:07,10105,accounts,13
  -1,action_called_account_remove,2021-04-05 14:58:05,10105,accounts,19
  -1,action_called_account_remove,2021-05-04 16:47:53,10105,accounts,20
  -1,action_called_account_remove,2021-05-05 20:46:22,10105,accounts,21
```

dumpsys **appops**

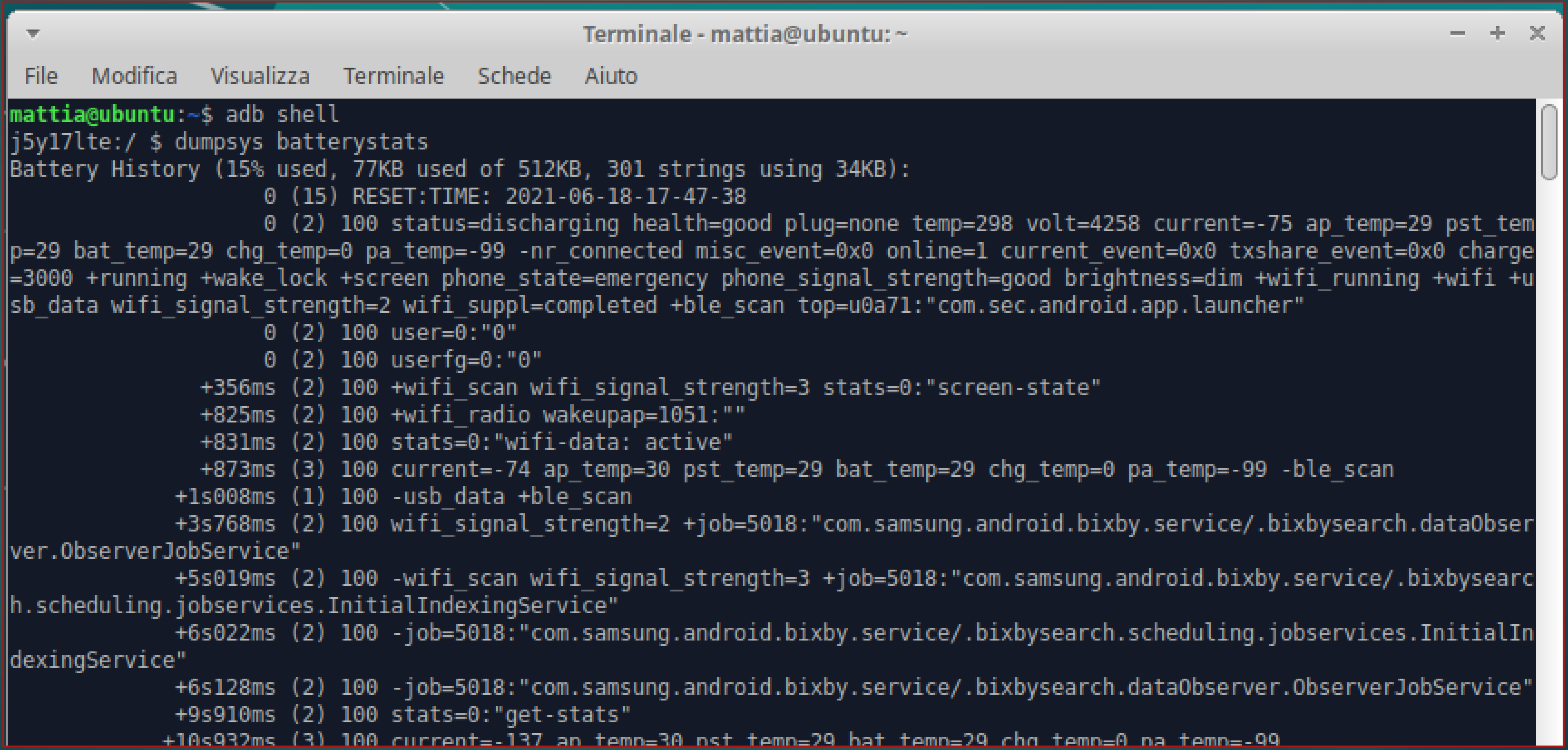
- App-ops are used for two purposes: **Access control** and **tracking**
- App-ops cover a wide variety of functionality from helping with runtime permissions to battery consumption tracking
- https://android.googlesource.com/platform/frameworks/base/+/master/core/java/android/app/AppOps.md



```
Uid u0a165:
  state=cch
  Package org.torproject.torbrowser:
    POST_NOTIFICATION (allow):
        Access: top   = 2020-02-14 11:01:14.723 (-494d0h0m31s225ms)
    WAKE_LOCK (allow):
        Access: top   = 2020-02-14 10:49:03.267 (-494d0h12m42s681ms)
        duration=+1s726ms
    READ_EXTERNAL_STORAGE (allow):
        Access: top   = 2021-06-22 11:48:35.220 (-13m10s728ms)
                fgsvc = 2021-06-02 16:12:59.340 (-19d19h48m46s608ms)
                bg    = 2021-06-22 10:26:51.357 (-1h34m54s591ms)
                cch   = 2021-06-22 11:48:34.228 (-13m11s720ms)
    WRITE_EXTERNAL_STORAGE (allow):
        Access: top   = 2021-06-22 11:48:35.220 (-13m10s728ms)
                fgsvc = 2021-06-02 16:12:59.340 (-19d19h48m46s608ms)
                bg    = 2021-06-22 10:26:51.357 (-1h34m54s591ms)
                cch   = 2021-06-22 11:48:34.228 (-13m11s720ms)
    RUN_IN_BACKGROUND (allow):
        Access: top   = 2020-02-14 11:01:15.737 (-494d0h0m30s211ms)
    START_FOREGROUND (allow):
        Access: top   = 2021-06-02 16:12:55.263 (-19d19h48m50s685ms)
                fgsvc = 2021-06-02 16:12:57.336 (-19d19h48m48s612ms)
        duration=+1d4h12m10s916ms
```

dumpsys **batterystats**

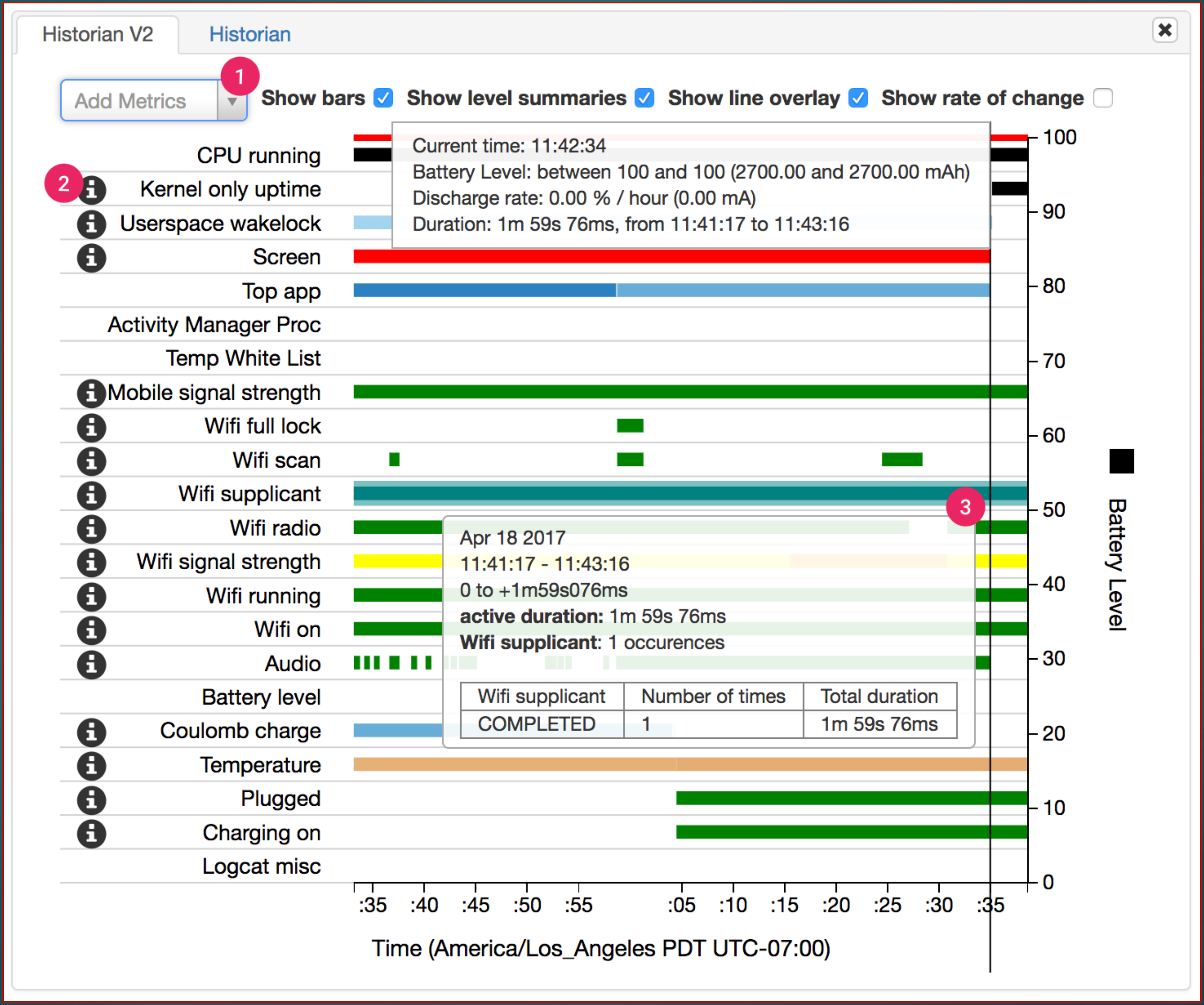
- Batterystats is a tool included in the Android framework that collects battery data on a device



```
mattia@ubuntu:~$ adb shell
j5y17lte:/ $ dumpsys batterystats
Battery History (15% used, 77KB used of 512KB, 301 strings using 34KB):
                    0 (15) RESET:TIME: 2021-06-18-17-47-38
                    0 (2) 100 status=discharging health=good plug=none temp=298 volt=4258 current=-75 ap_temp=29 pst_tem
p=29 bat_temp=29 chg_temp=0 pa_temp=-99 -nr_connected misc_event=0x0 online=1 current_event=0x0 txshare_event=0x0 charge
=3000 +running +wake_lock +screen phone_state=emergency phone_signal_strength=good brightness=dim +wifi_running +wifi +u
sb_data wifi_signal_strength=2 wifi_suppl=completed +ble_scan top=u0a71:"com.sec.android.app.launcher"
                    0 (2) 100 user=0:"0"
                    0 (2) 100 userfg=0:"0"
               +356ms (2) 100 +wifi_scan wifi_signal_strength=3 stats=0:"screen-state"
               +825ms (2) 100 +wifi_radio wakeupap=1051:""
               +831ms (2) 100 stats=0:"wifi-data: active"
               +873ms (3) 100 current=-74 ap_temp=30 pst_temp=29 bat_temp=29 chg_temp=0 pa_temp=-99 -ble_scan
             +1s008ms (1) 100 -usb_data +ble_scan
             +3s768ms (2) 100 wifi_signal_strength=2 +job=5018:"com.samsung.android.bixby.service/.bixbysearch.dataObser
ver.ObserverJobService"
             +5s019ms (2) 100 -wifi_scan wifi_signal_strength=3 +job=5018:"com.samsung.android.bixby.service/.bixbysearc
h.scheduling.jobservices.InitialIndexingService"
             +6s022ms (2) 100 -job=5018:"com.samsung.android.bixby.service/.bixbysearch.scheduling.jobservices.InitialIn
dexingService"
             +6s128ms (2) 100 -job=5018:"com.samsung.android.bixby.service/.bixbysearch.dataObserver.ObserverJobService"
             +9s910ms (2) 100 stats=0:"get-stats"
            +10s932ms (3) 100 current=-137 ap_temp=30 pst_temp=29 bat_temp=29 chg_temp=0 pa_temp=-99
```

Profile battery usage with Batterystats and Battery Historian

https://developer.android.com/topic/performance/power/setup-battery-historian



Show bars ☑ Show level summaries ☑ Show line overlay ☑ Show rate of change ☐

Current time: 11:42:34
Battery Level: between 100 and 100 (2700.00 and 2700.00 mAh)
Discharge rate: 0.00 % / hour (0.00 mA)
Duration: 1m 59s 76ms, from 11:41:17 to 11:43:16

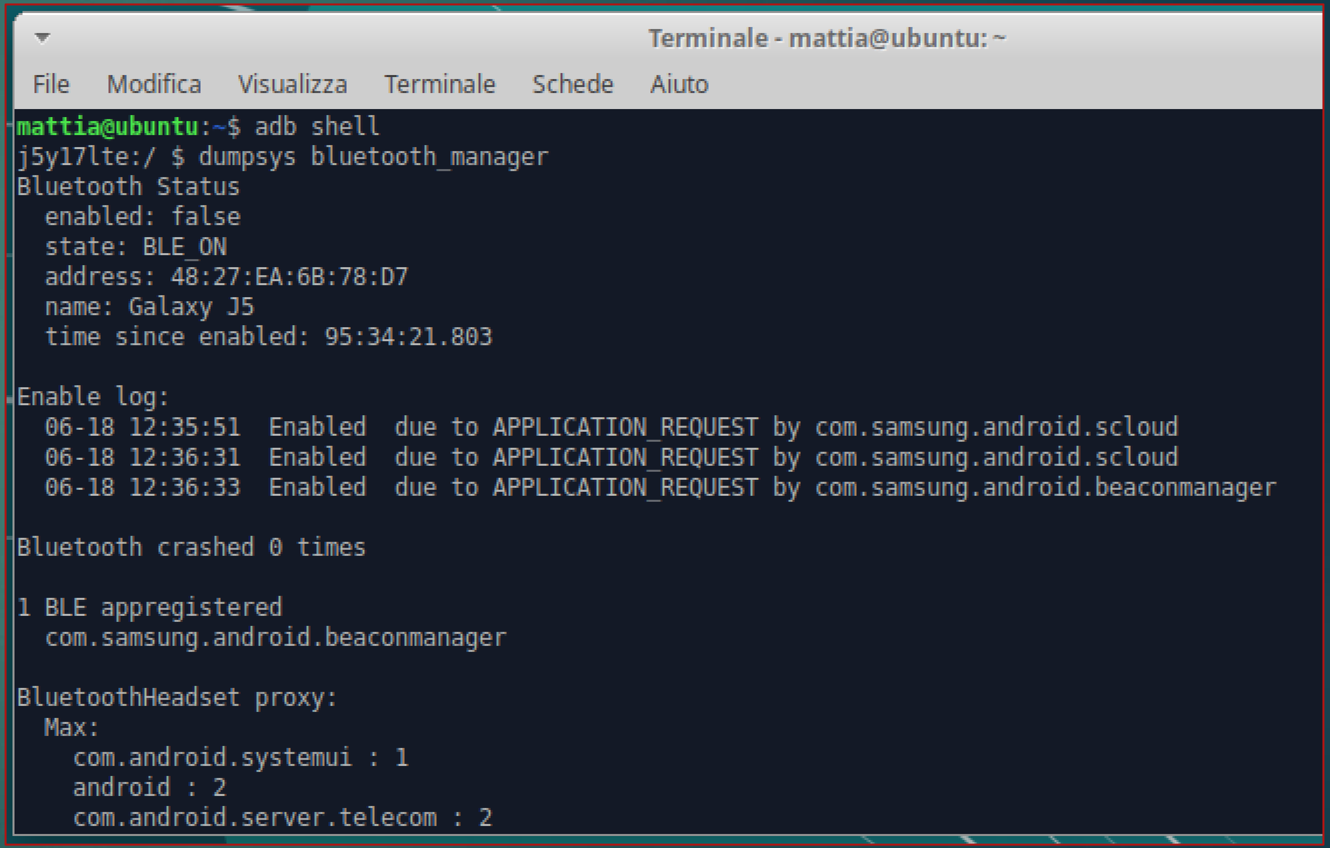
Apr 18 2017
11:41:17 - 11:43:16
0 to +1m59s076ms
active duration: 1m 59s 76ms
Wifi supplicant: 1 occurences

Wifi supplicant	Number of times	Total duration
COMPLETED	1	1m 59s 76ms

dumpsys **bluetooth_manager**

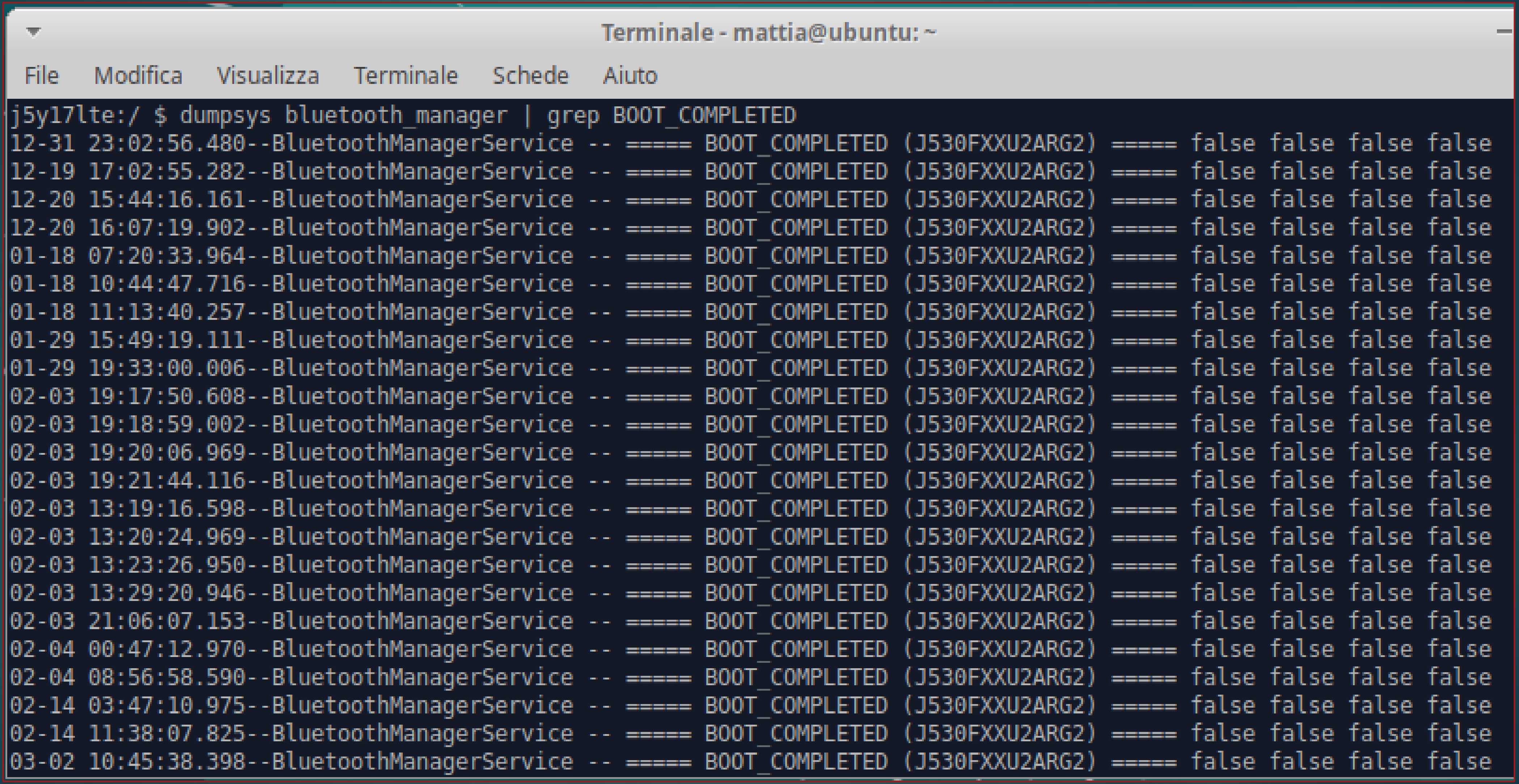
- Bluetooth properties

- https://stackoverflow.com/questions/57299411/interpreting-dumpsys-bluetoothmanager-result



```
mattia@ubuntu:~$ adb shell
j5y17lte:/ $ dumpsys bluetooth_manager
Bluetooth Status
  enabled: false
  state: BLE_ON
  address: 48:27:EA:6B:78:D7
  name: Galaxy J5
  time since enabled: 95:34:21.803

Enable log:
  06-18 12:35:51  Enabled  due to APPLICATION_REQUEST by com.samsung.android.scloud
  06-18 12:36:31  Enabled  due to APPLICATION_REQUEST by com.samsung.android.scloud
  06-18 12:36:33  Enabled  due to APPLICATION_REQUEST by com.samsung.android.beaconmanager

Bluetooth crashed 0 times

1 BLE appregistered
  com.samsung.android.beaconmanager

BluetoothHeadset proxy:
  Max:
    com.android.systemui : 1
    android : 2
    com.android.server.telecom : 2
```

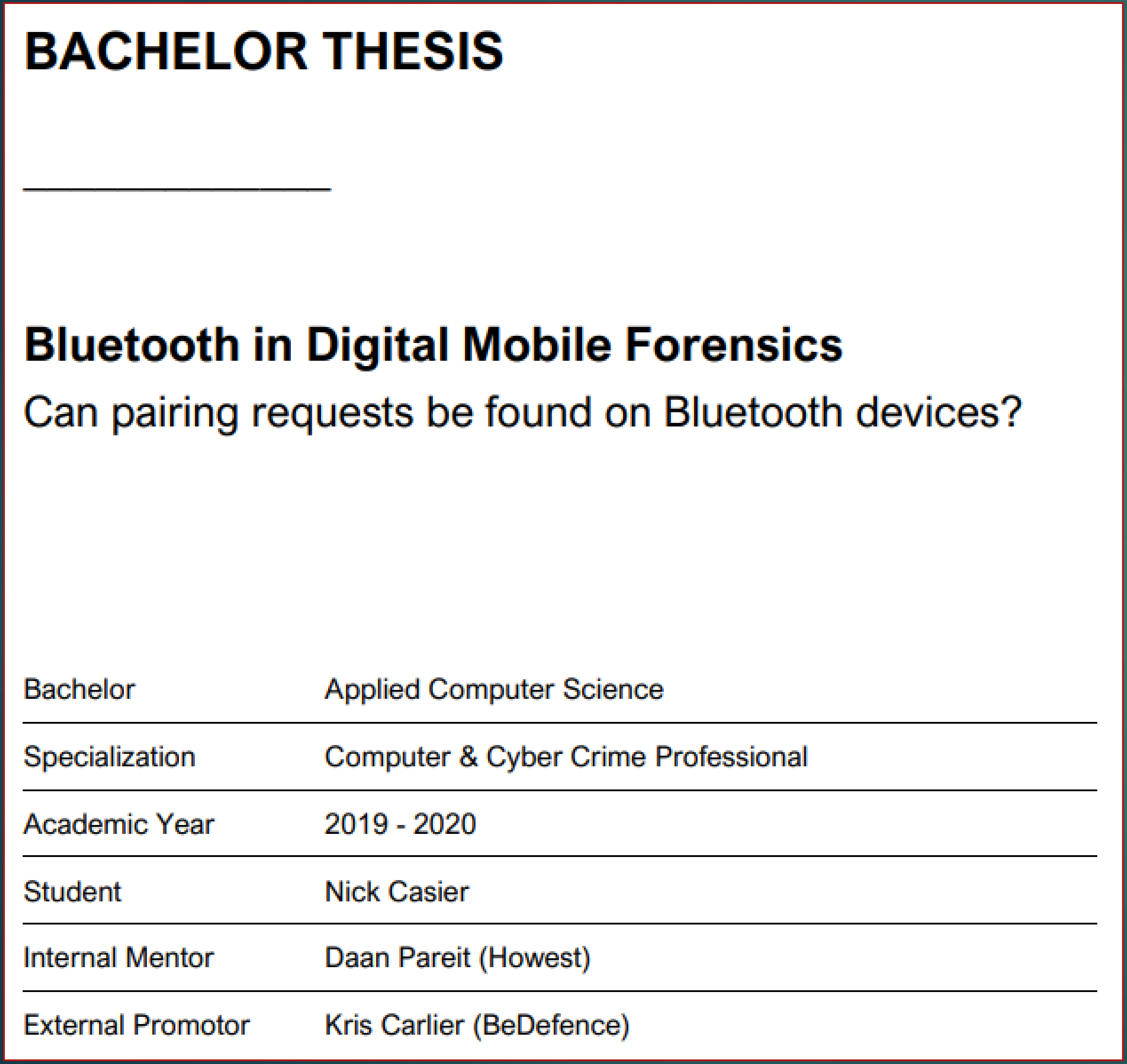
dumpsys **bluetooth_manager | grep BOOT_COMPLETED**



```
j5y17lte:/ $ dumpsys bluetooth_manager | grep BOOT_COMPLETED
12-31 23:02:56.480--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
12-19 17:02:55.282--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
12-20 15:44:16.161--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
12-20 16:07:19.902--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
01-18 07:20:33.964--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
01-18 10:44:47.716--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
01-18 11:13:40.257--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
01-29 15:49:19.111--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
01-29 19:33:00.006--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-03 19:17:50.608--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-03 19:18:59.002--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-03 19:20:06.969--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-03 19:21:44.116--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-03 13:19:16.598--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-03 13:20:24.969--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-03 13:23:26.950--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-03 13:29:20.946--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-03 21:06:07.153--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-04 00:47:12.970--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-04 08:56:58.590--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-14 03:47:10.975--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
02-14 11:38:07.825--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
03-02 10:45:38.398--BluetoothManagerService -- ===== BOOT_COMPLETED (J530FXXU2ARG2) ===== false false false false
```

Bluetooth in Digital Mobile Forensics

https://www.scriptiebank.be/sites/default/files/thesis/2020-08/BaP_NickCasier_BluetoothInDigitalMobileForensics-CanPairingRequestBeFoundOnBluetoothDevices.pdf

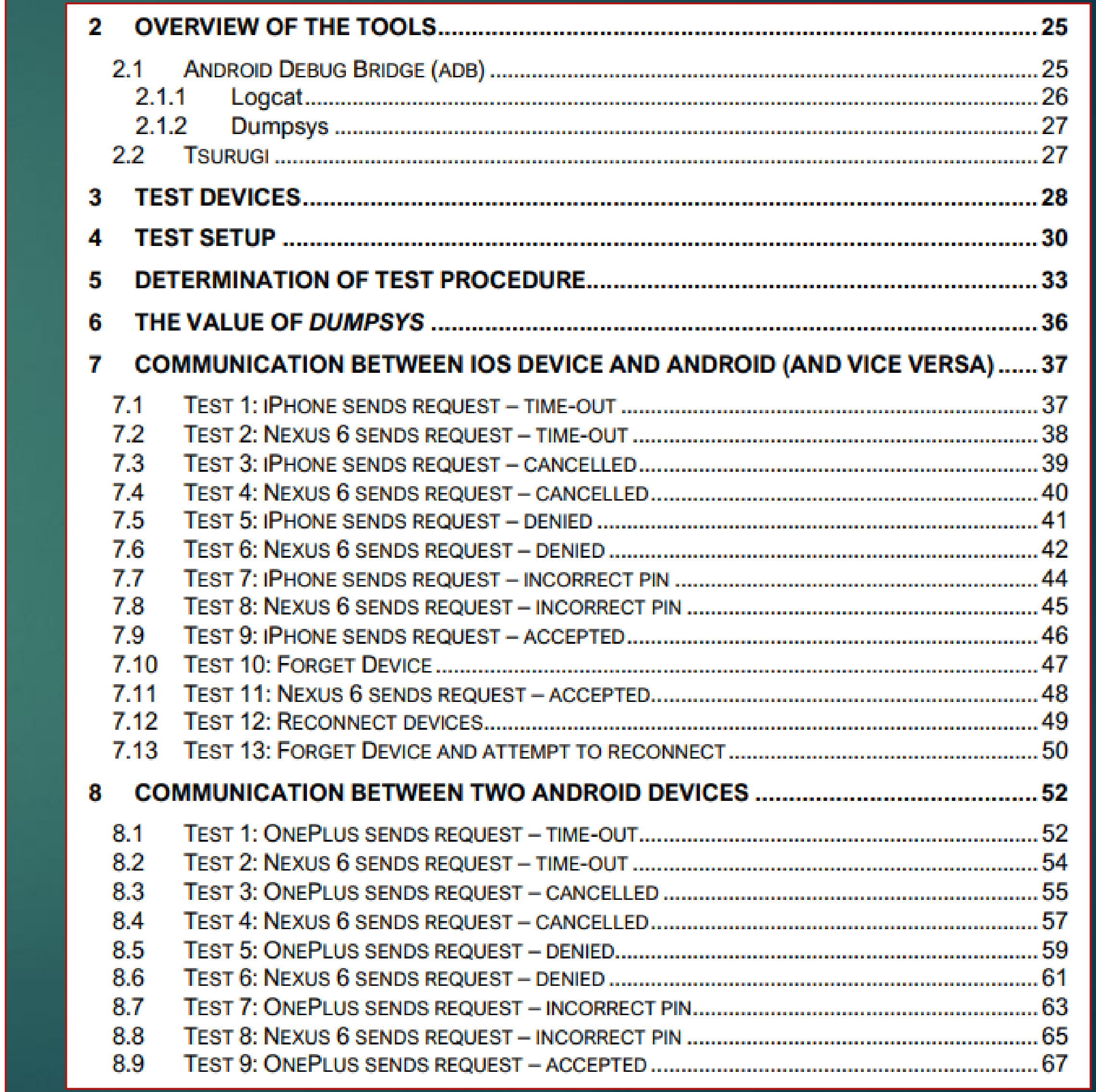


BACHELOR THESIS

Bluetooth in Digital Mobile Forensics

Can pairing requests be found on Bluetooth devices?

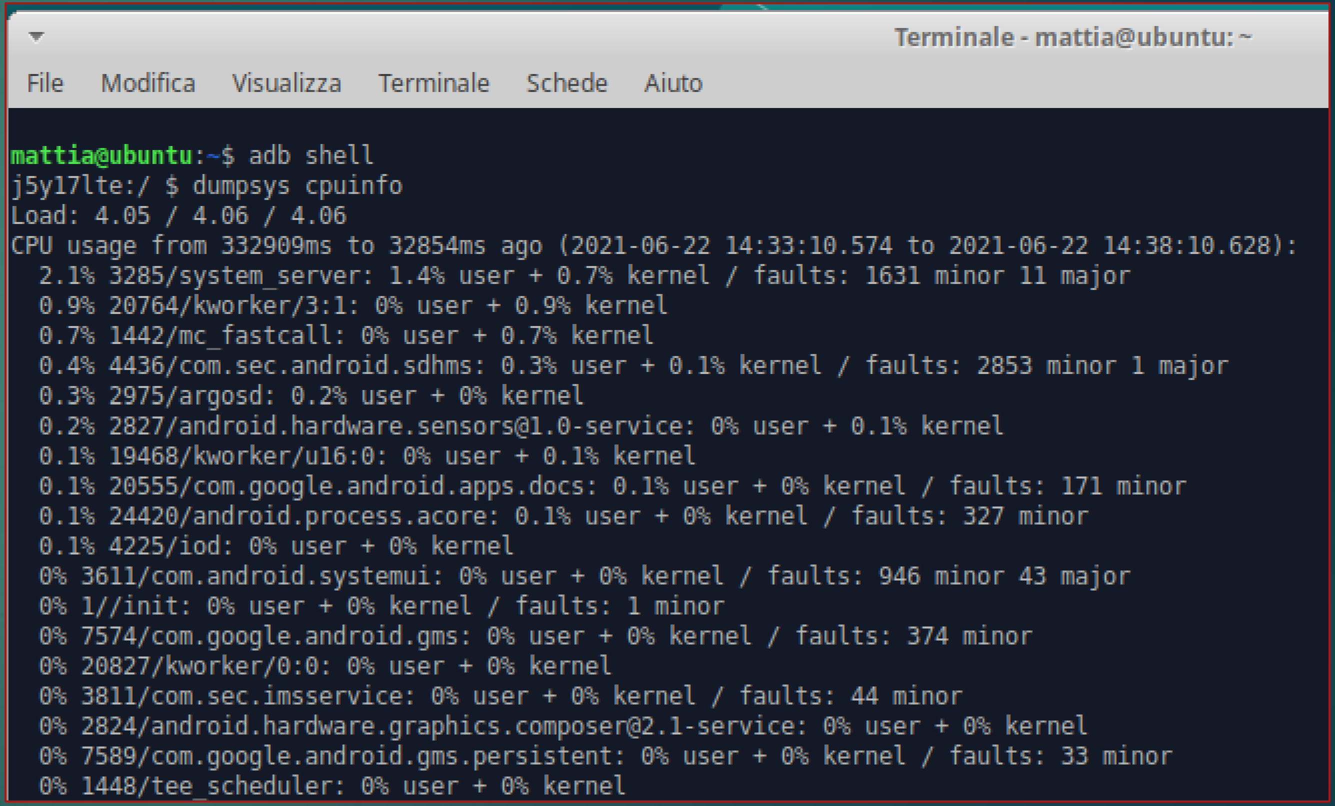
Bachelor	Applied Computer Science
Specialization	Computer & Cyber Crime Professional
Academic Year	2019 - 2020
Student	Nick Casier
Internal Mentor	Daan Pareit (Howest)
External Promotor	Kris Carlier (BeDefence)



dumpsys **cpuinfo**

- Display CPU information

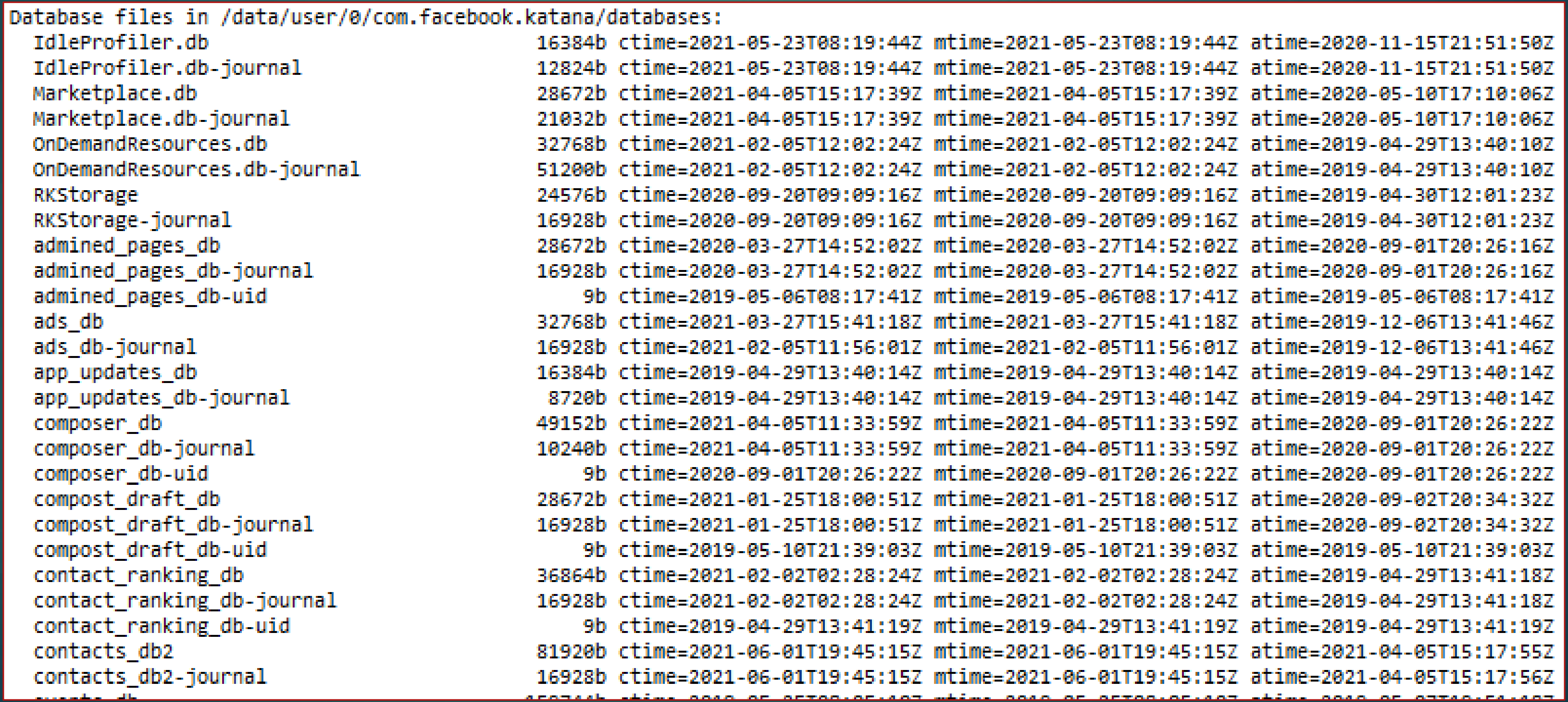
- https://stackoverflow.com/questions/24612982/interpreting-dumpsys-cpuinfo
- https://stackoverflow.com/questions/40186347/dumpsys-cpuinfo-in-android-interpreting-the-results-of-this-command



```
mattia@ubuntu:~$ adb shell
j5y17lte:/ $ dumpsys cpuinfo
Load: 4.05 / 4.06 / 4.06
CPU usage from 332909ms to 32854ms ago (2021-06-22 14:33:10.574 to 2021-06-22 14:38:10.628):
  2.1% 3285/system_server: 1.4% user + 0.7% kernel / faults: 1631 minor 11 major
  0.9% 20764/kworker/3:1: 0% user + 0.9% kernel
  0.7% 1442/mc_fastcall: 0% user + 0.7% kernel
  0.4% 4436/com.sec.android.sdhms: 0.3% user + 0.1% kernel / faults: 2853 minor 1 major
  0.3% 2975/argosd: 0.2% user + 0% kernel
  0.2% 2827/android.hardware.sensors@1.0-service: 0% user + 0.1% kernel
  0.1% 19468/kworker/u16:0: 0% user + 0.1% kernel
  0.1% 20555/com.google.android.apps.docs: 0.1% user + 0% kernel / faults: 171 minor
  0.1% 24420/android.process.acore: 0.1% user + 0% kernel / faults: 327 minor
  0.1% 4225/iod: 0% user + 0% kernel
  0% 3611/com.android.systemui: 0% user + 0% kernel / faults: 946 minor 43 major
  0% 1//init: 0% user + 0% kernel / faults: 1 minor
  0% 7574/com.google.android.gms: 0% user + 0% kernel / faults: 374 minor
  0% 20827/kworker/0:0: 0% user + 0% kernel
  0% 3811/com.sec.imsservice: 0% user + 0% kernel / faults: 44 minor
  0% 2824/android.hardware.graphics.composer@2.1-service: 0% user + 0% kernel
  0% 7589/com.google.android.gms.persistent: 0% user + 0% kernel / faults: 33 minor
  0% 1448/tee_scheduler: 0% user + 0% kernel
```

dumpsys **dbinfo -v**

- List all databases for each package

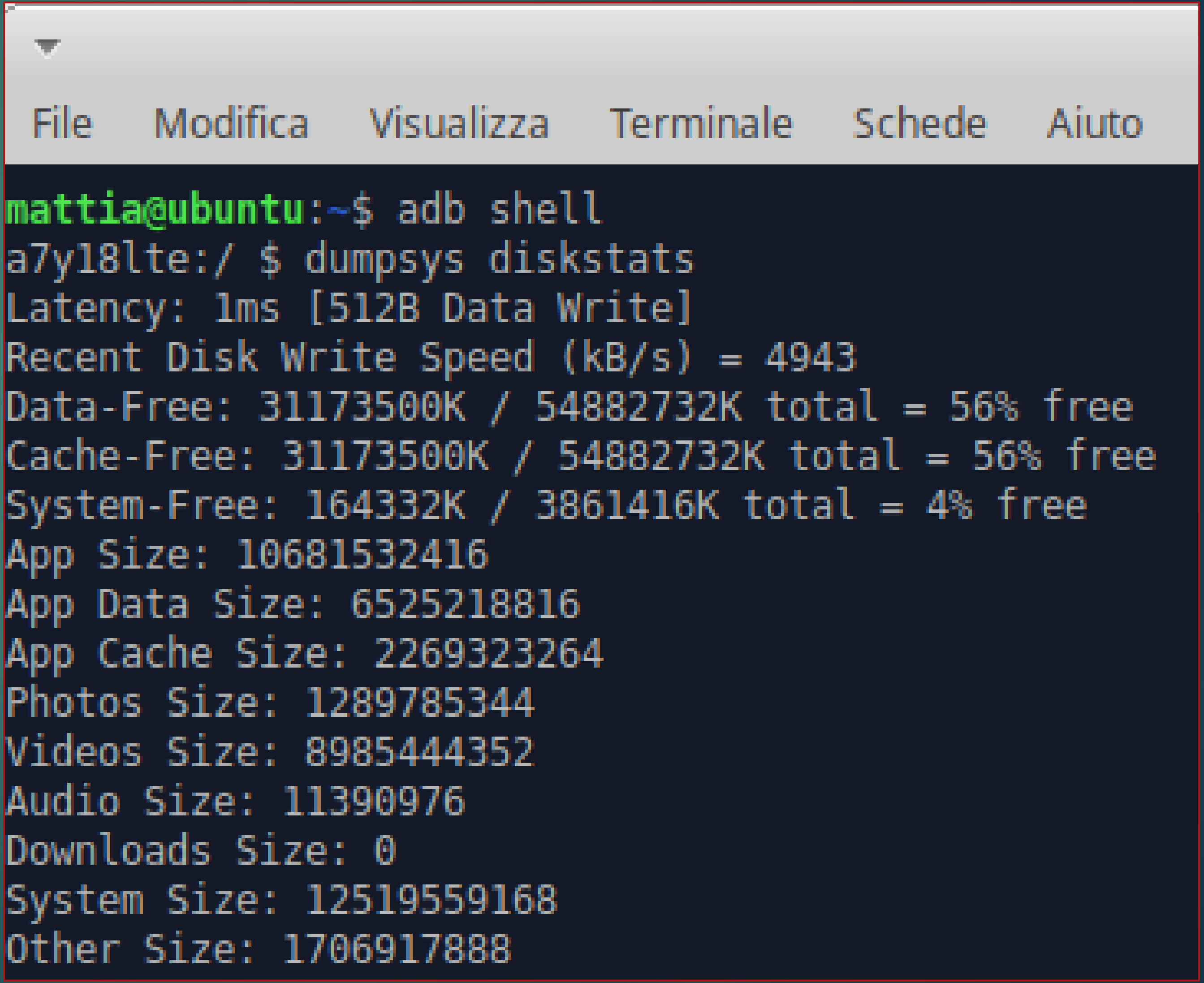


```
Database files in /data/user/0/com.facebook.katana/databases:
  IdleProfiler.db                            16384b ctime=2021-05-23T08:19:44Z mtime=2021-05-23T08:19:44Z atime=2020-11-15T21:51:50Z
  IdleProfiler.db-journal                    12824b ctime=2021-05-23T08:19:44Z mtime=2021-05-23T08:19:44Z atime=2020-11-15T21:51:50Z
  Marketplace.db                             28672b ctime=2021-04-05T15:17:39Z mtime=2021-04-05T15:17:39Z atime=2020-05-10T17:10:06Z
  Marketplace.db-journal                     21032b ctime=2021-04-05T15:17:39Z mtime=2021-04-05T15:17:39Z atime=2020-05-10T17:10:06Z
  OnDemandResources.db                       32768b ctime=2021-02-05T12:02:24Z mtime=2021-02-05T12:02:24Z atime=2019-04-29T13:40:10Z
  OnDemandResources.db-journal               51200b ctime=2021-02-05T12:02:24Z mtime=2021-02-05T12:02:24Z atime=2019-04-29T13:40:10Z
  RKStorage                                  24576b ctime=2020-09-20T09:09:16Z mtime=2020-09-20T09:09:16Z atime=2019-04-30T12:01:23Z
  RKStorage-journal                          16928b ctime=2020-09-20T09:09:16Z mtime=2020-09-20T09:09:16Z atime=2019-04-30T12:01:23Z
  admined_pages_db                           28672b ctime=2020-03-27T14:52:02Z mtime=2020-03-27T14:52:02Z atime=2020-09-01T20:26:16Z
  admined_pages_db-journal                   16928b ctime=2020-03-27T14:52:02Z mtime=2020-03-27T14:52:02Z atime=2020-09-01T20:26:16Z
  admined_pages_db-uid                           9b ctime=2019-05-06T08:17:41Z mtime=2019-05-06T08:17:41Z atime=2019-05-06T08:17:41Z
  ads_db                                     32768b ctime=2021-03-27T15:41:18Z mtime=2021-03-27T15:41:18Z atime=2019-12-06T13:41:46Z
  ads_db-journal                             16928b ctime=2021-02-05T11:56:01Z mtime=2021-02-05T11:56:01Z atime=2019-12-06T13:41:46Z
  app_updates_db                             16384b ctime=2019-04-29T13:40:14Z mtime=2019-04-29T13:40:14Z atime=2019-04-29T13:40:14Z
  app_updates_db-journal                      8720b ctime=2019-04-29T13:40:14Z mtime=2019-04-29T13:40:14Z atime=2019-04-29T13:40:14Z
  composer_db                                49152b ctime=2021-04-05T11:33:59Z mtime=2021-04-05T11:33:59Z atime=2020-09-01T20:26:22Z
  composer_db-journal                        10240b ctime=2021-04-05T11:33:59Z mtime=2021-04-05T11:33:59Z atime=2020-09-01T20:26:22Z
  composer_db-uid                                9b ctime=2020-09-01T20:26:22Z mtime=2020-09-01T20:26:22Z atime=2020-09-01T20:26:22Z
  compost_draft_db                           28672b ctime=2021-01-25T18:00:51Z mtime=2021-01-25T18:00:51Z atime=2020-09-02T20:34:32Z
  compost_draft_db-journal                   16928b ctime=2021-01-25T18:00:51Z mtime=2021-01-25T18:00:51Z atime=2020-09-02T20:34:32Z
  compost_draft_db-uid                           9b ctime=2019-05-10T21:39:03Z mtime=2019-05-10T21:39:03Z atime=2019-05-10T21:39:03Z
  contact_ranking_db                         36864b ctime=2021-02-02T02:28:24Z mtime=2021-02-02T02:28:24Z atime=2019-04-29T13:41:18Z
  contact_ranking_db-journal                 16928b ctime=2021-02-02T02:28:24Z mtime=2021-02-02T02:28:24Z atime=2019-04-29T13:41:18Z
  contact_ranking_db-uid                         9b ctime=2019-04-29T13:41:19Z mtime=2019-04-29T13:41:19Z atime=2019-04-29T13:41:19Z
  contacts_db2                               81920b ctime=2021-06-01T19:45:15Z mtime=2021-06-01T19:45:15Z atime=2021-04-05T15:17:55Z
  contacts_db2-journal                       16928b ctime=2021-06-01T19:45:15Z mtime=2021-06-01T19:45:15Z atime=2021-04-05T15:17:56Z
```

dumpsys **diskstats**

- Disk usage stats

- System, Cache and Data
- App size (Data and Cache)
- Photos
- Videos
- Audio
- Download

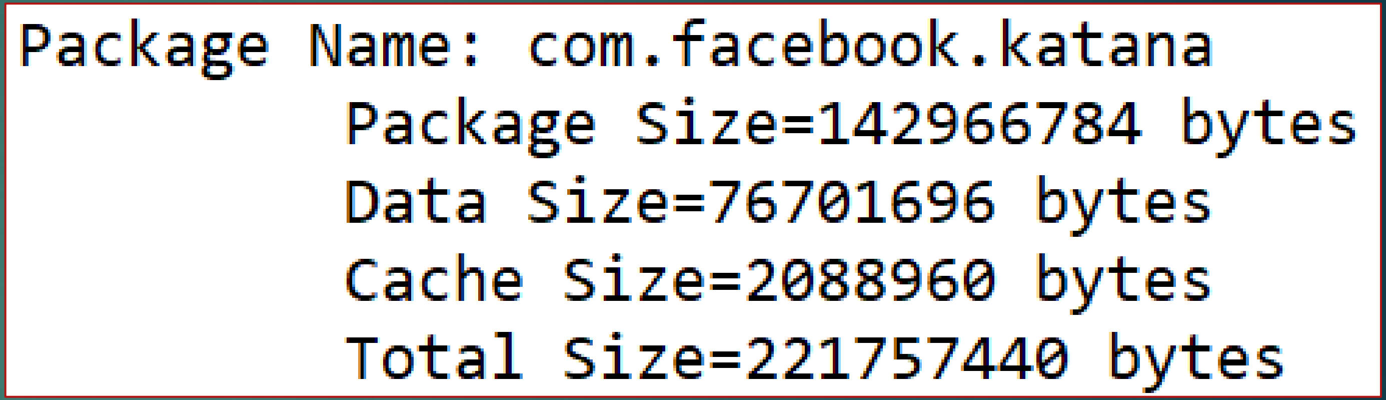


```
mattia@ubuntu:~$ adb shell
a7y18lte:/ $ dumpsys diskstats
Latency: 1ms [512B Data Write]
Recent Disk Write Speed (kB/s) = 4943
Data-Free: 31173500K / 54882732K total = 56% free
Cache-Free: 31173500K / 54882732K total = 56% free
System-Free: 164332K / 3861416K total = 4% free
App Size: 10681532416
App Data Size: 6525218816
App Cache Size: 2269323264
Photos Size: 1289785344
Videos Size: 8985444352
Audio Size: 11390976
Downloads Size: 0
System Size: 12519559168
Other Size: 1706917888
```

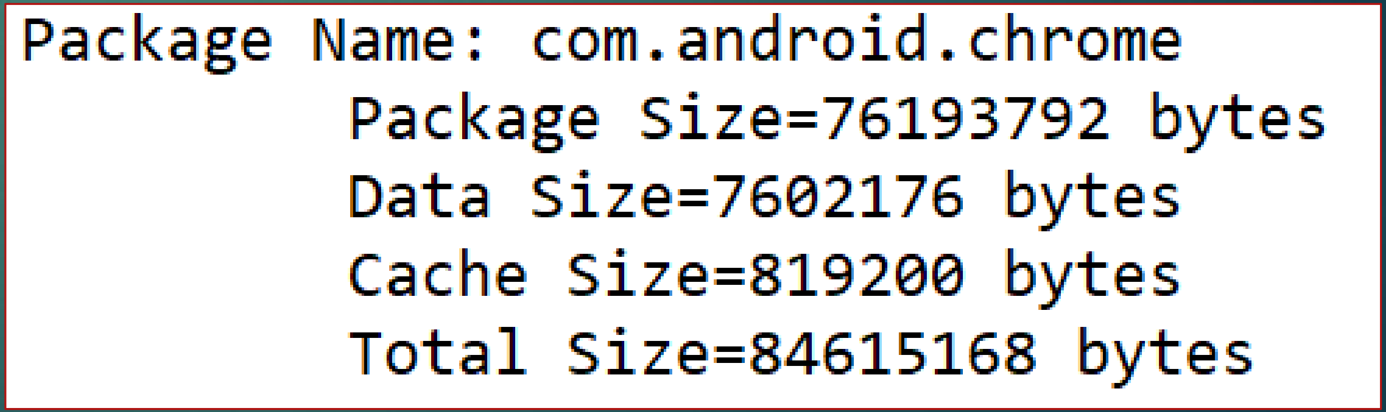
dumpsys **diskstats**

- Per-package stats

- Package size
- Data size
- Cache size
- Total size

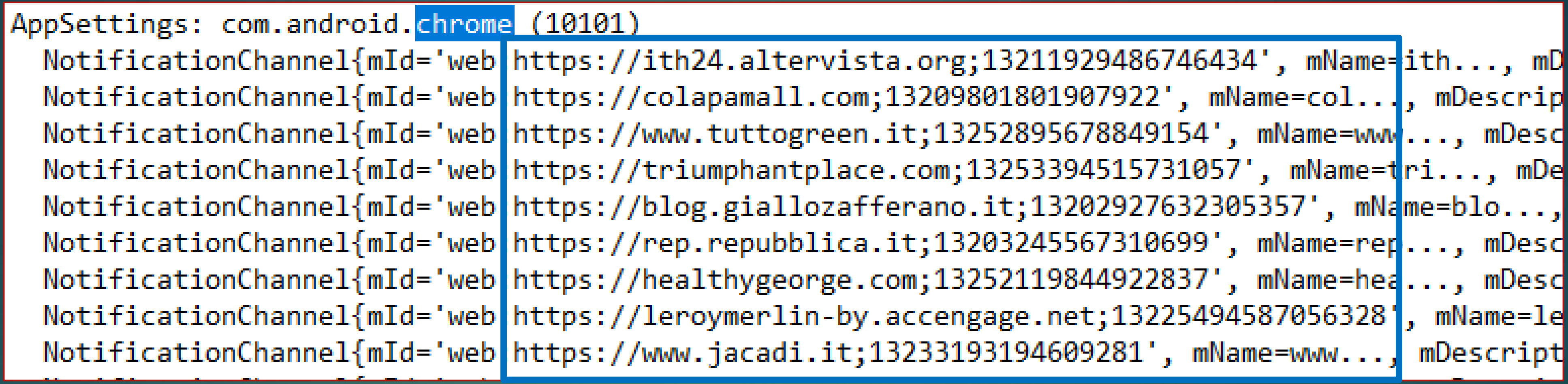


```
Package Name: com.facebook.katana
         Package Size=142966784 bytes
         Data Size=76701696 bytes
         Cache Size=2088960 bytes
         Total Size=221757440 bytes
```

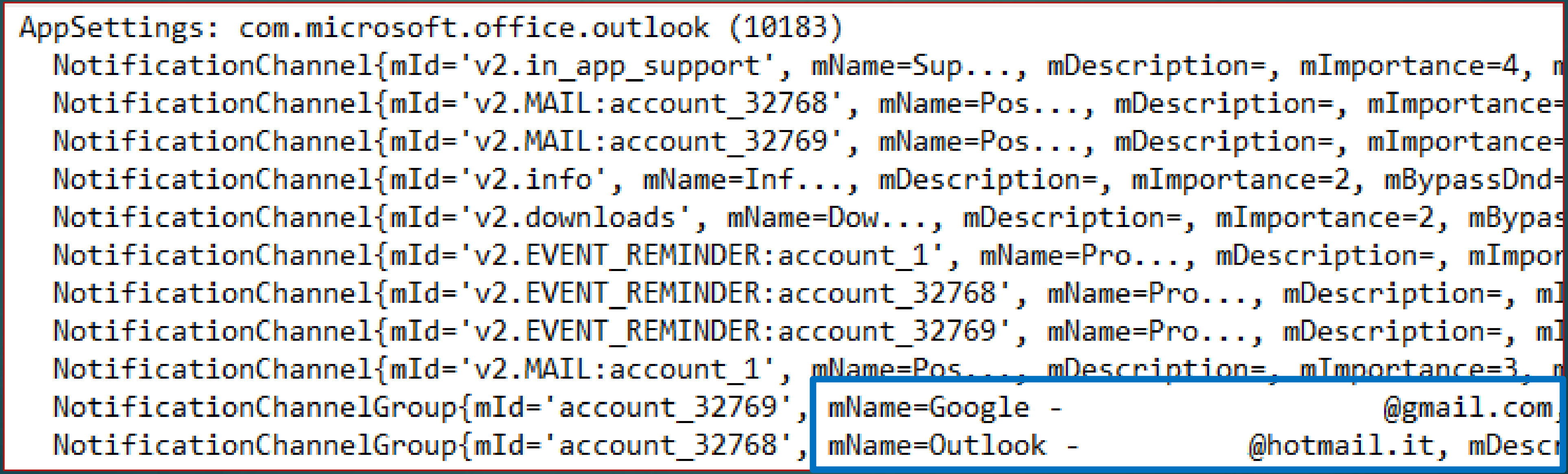


```
Package Name: com.android.chrome
         Package Size=76193792 bytes
         Data Size=7602176 bytes
         Cache Size=819200 bytes
         Total Size=84615168 bytes
```

dumpsys **notification**

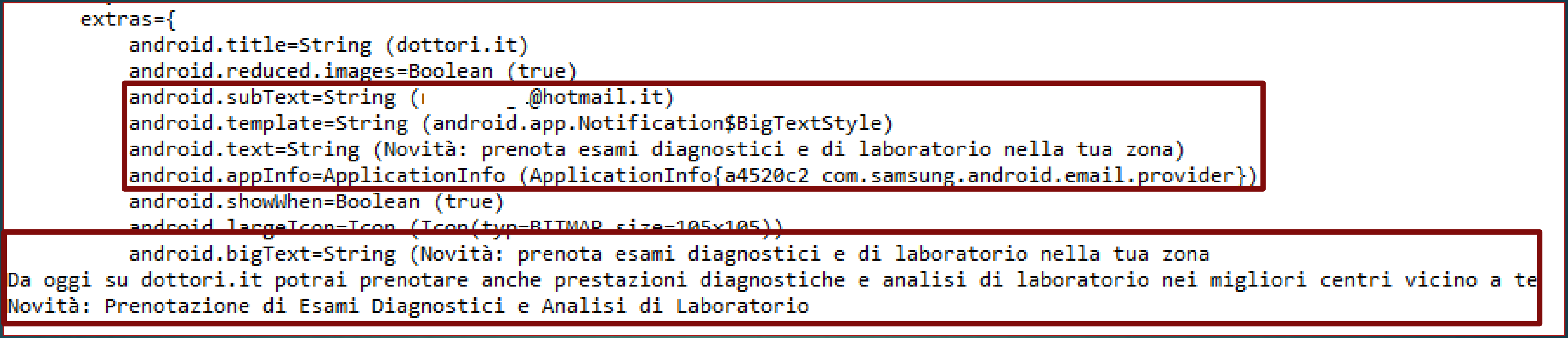


```
AppSettings: com.android.chrome (10101)
  NotificationChannel{mId='web https://ith24.altervista.org;13211929486746434', mName=ith..., mD
  NotificationChannel{mId='web https://colapamall.com;13209801801907922', mName=col..., mDescrip
  NotificationChannel{mId='web https://www.tuttogreen.it;13252895678849154', mName=www..., mDesc
  NotificationChannel{mId='web https://triumphantplace.com;13253394515731057', mName=tri..., mDe
  NotificationChannel{mId='web https://blog.giallozafferano.it;13202927632305357', mName=blo...,
  NotificationChannel{mId='web https://rep.repubblica.it;13203245567310699', mName=rep..., mDesc
  NotificationChannel{mId='web https://healthygeorge.com;13252119844922837', mName=hea..., mDesc
  NotificationChannel{mId='web https://leroymerlin-by.accengage.net;13225494587056328', mName=le
  NotificationChannel{mId='web https://www.jacadi.it;13233193194609281', mName=www..., mDescript
```

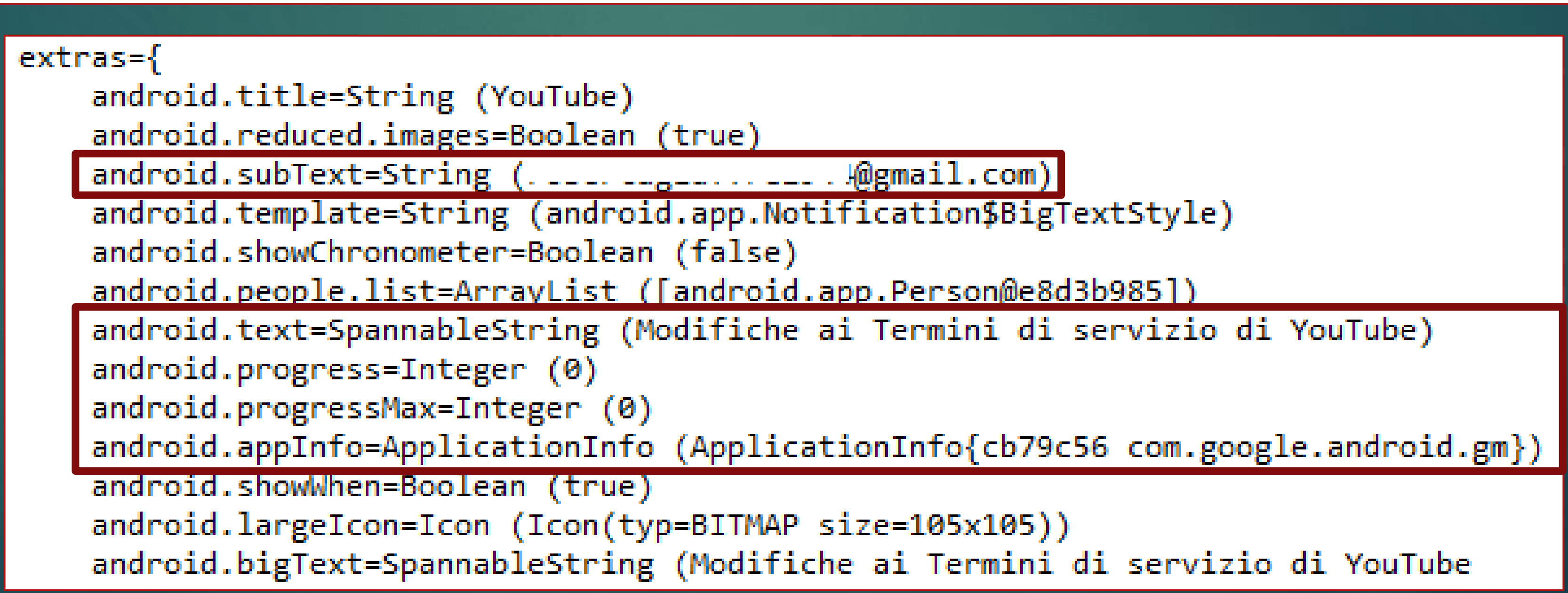


```
AppSettings: com.microsoft.office.outlook (10183)
  NotificationChannel{mId='v2.in_app_support', mName=Sup..., mDescription=, mImportance=4, m
  NotificationChannel{mId='v2.MAIL:account_32768', mName=Pos..., mDescription=, mImportance=
  NotificationChannel{mId='v2.MAIL:account_32769', mName=Pos..., mDescription=, mImportance=
  NotificationChannel{mId='v2.info', mName=Inf..., mDescription=, mImportance=2, mBypassDnd=
  NotificationChannel{mId='v2.downloads', mName=Dow..., mDescription=, mImportance=2, mBypas
  NotificationChannel{mId='v2.EVENT_REMINDER:account_1', mName=Pro..., mDescription=, mImpor
  NotificationChannel{mId='v2.EVENT_REMINDER:account_32768', mName=Pro..., mDescription=, mI
  NotificationChannel{mId='v2.EVENT_REMINDER:account_32769', mName=Pro..., mDescription=, mI
  NotificationChannel{mId='v2.MAIL:account_1', mName=Pos..., mDescription=, mImportance=3, m
  NotificationChannelGroup{mId='account_32769', mName=Google -                @gmail.com,
  NotificationChannelGroup{mId='account_32768', mName=Outlook -         @hotmail.it, mDescr
```

dumpsys **notification --noredact**

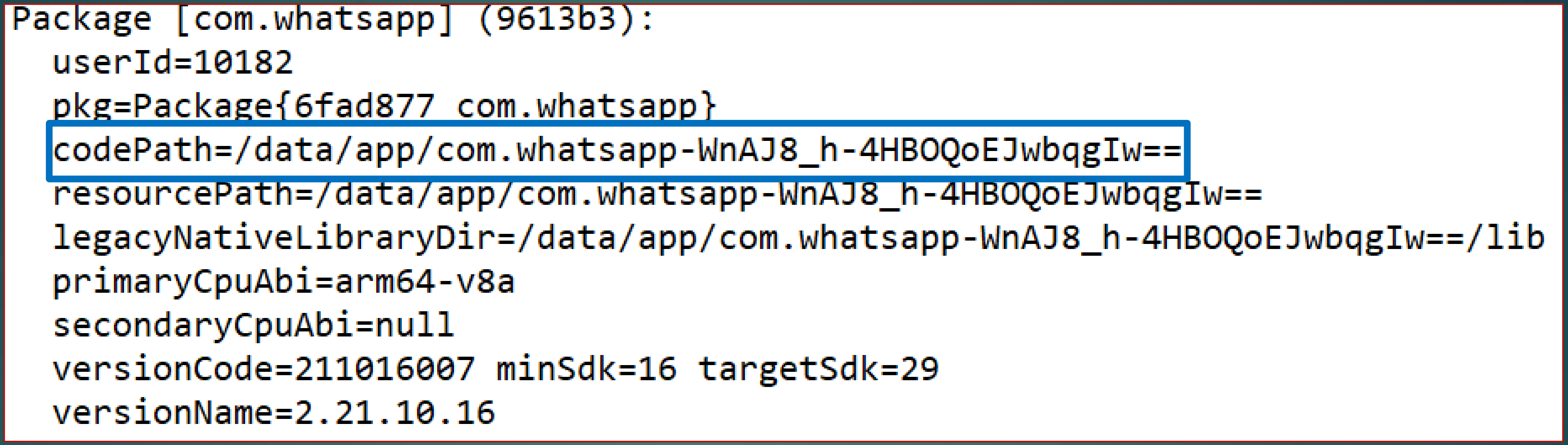


```
      extras={
          android.title=String (dottori.it)
          android.reduced.images=Boolean (true)
          android.subText=String ([redacted]@hotmail.it)
          android.template=String (android.app.Notification$BigTextStyle)
          android.text=String (Novità: prenota esami diagnostici e di laboratorio nella tua zona)
          android.appInfo=ApplicationInfo (ApplicationInfo{a4520c2 com.samsung.android.email.provider})
          android.showWhen=Boolean (true)
          android.largeIcon=Icon (Icon(typ=BITMAP size=105x105))
          android.bigText=String (Novità: prenota esami diagnostici e di laboratorio nella tua zona
Da oggi su dottori.it potrai prenotare anche prestazioni diagnostiche e analisi di laboratorio nei migliori centri vicino a te
Novità: Prenotazione di Esami Diagnostici e Analisi di Laboratorio
```

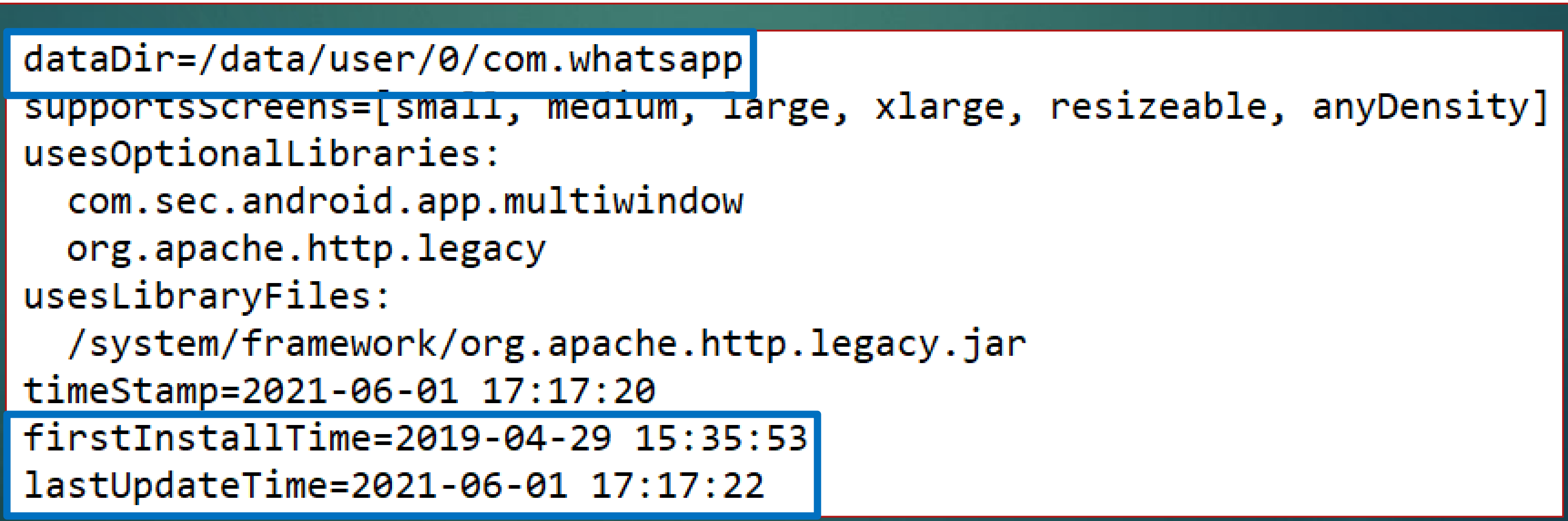


```
extras={
    android.title=String (YouTube)
    android.reduced.images=Boolean (true)
    android.subText=String ([redacted]@gmail.com)
    android.template=String (android.app.Notification$BigTextStyle)
    android.showChronometer=Boolean (false)
    android.people.list=ArrayList ([android.app.Person@e8d3b985])
    android.text=SpannableString (Modifiche ai Termini di servizio di YouTube)
    android.progress=Integer (0)
    android.progressMax=Integer (0)
    android.appInfo=ApplicationInfo (ApplicationInfo{cb79c56 com.google.android.gm})
    android.showWhen=Boolean (true)
    android.largeIcon=Icon (Icon(typ=BITMAP size=105x105))
    android.bigText=SpannableString (Modifiche ai Termini di servizio di YouTube
```

dumpsys **package**

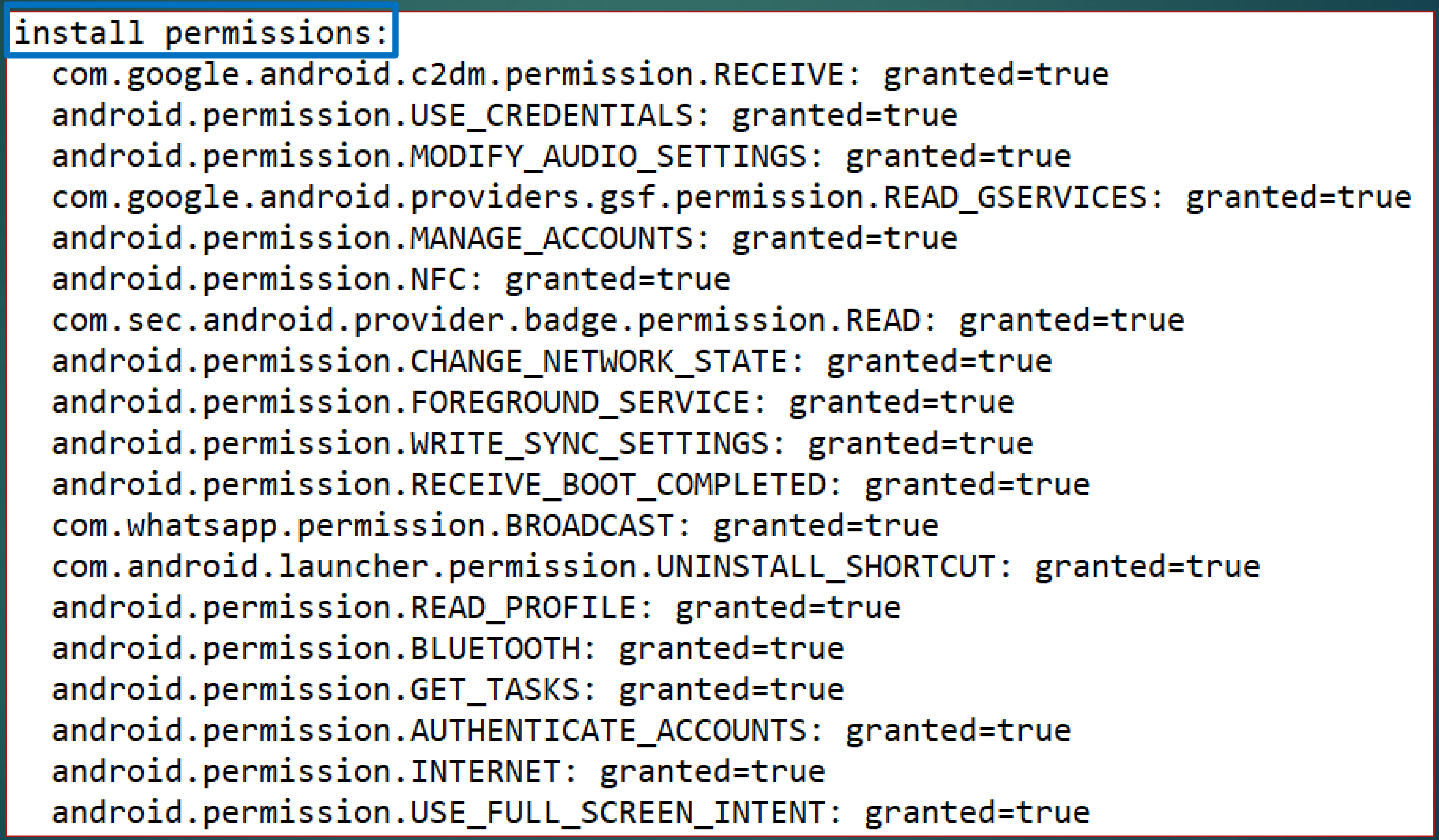


```
Package [com.whatsapp] (9613b3):
  userId=10182
  pkg=Package{6fad877 com.whatsapp}
  codePath=/data/app/com.whatsapp-WnAJ8_h-4HBOQoEJwbqgIw==
  resourcePath=/data/app/com.whatsapp-WnAJ8_h-4HBOQoEJwbqgIw==
  legacyNativeLibraryDir=/data/app/com.whatsapp-WnAJ8_h-4HBOQoEJwbqgIw==/lib
  primaryCpuAbi=arm64-v8a
  secondaryCpuAbi=null
  versionCode=211016007 minSdk=16 targetSdk=29
  versionName=2.21.10.16
```



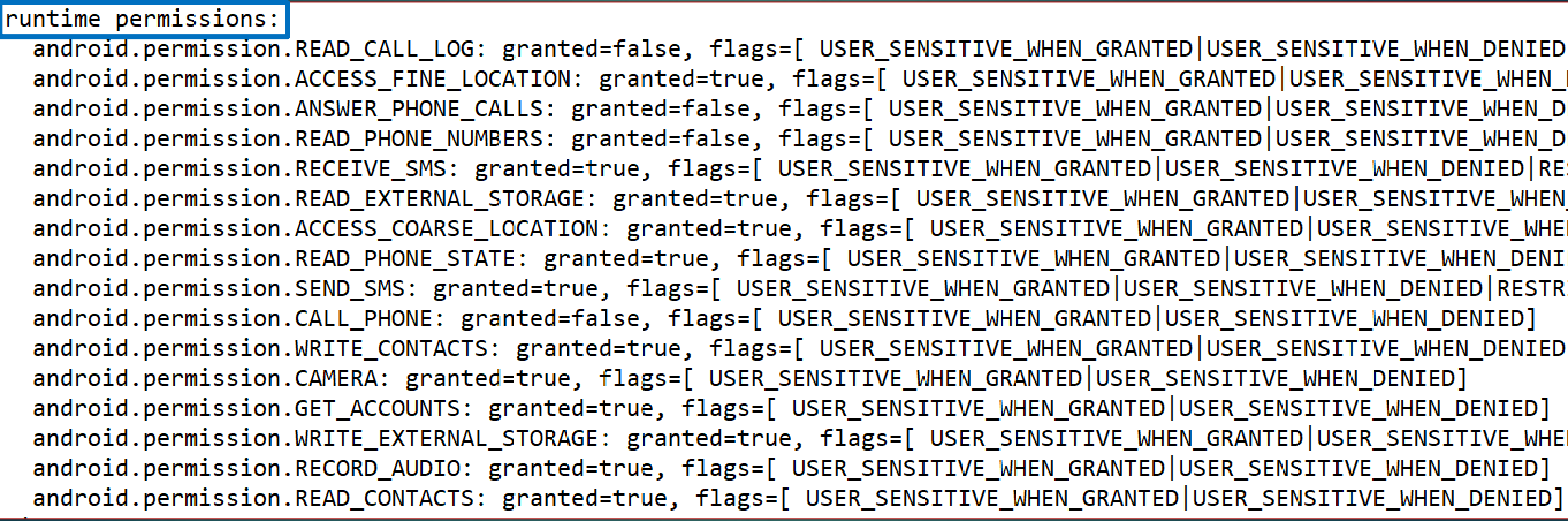
```
dataDir=/data/user/0/com.whatsapp
supportsScreens=[small, medium, large, xlarge, resizeable, anyDensity]
usesOptionalLibraries:
  com.sec.android.app.multiwindow
  org.apache.http.legacy
usesLibraryFiles:
  /system/framework/org.apache.http.legacy.jar
timeStamp=2021-06-01 17:17:20
firstInstallTime=2019-04-29 15:35:53
lastUpdateTime=2021-06-01 17:17:22
```

dumpsys **package**



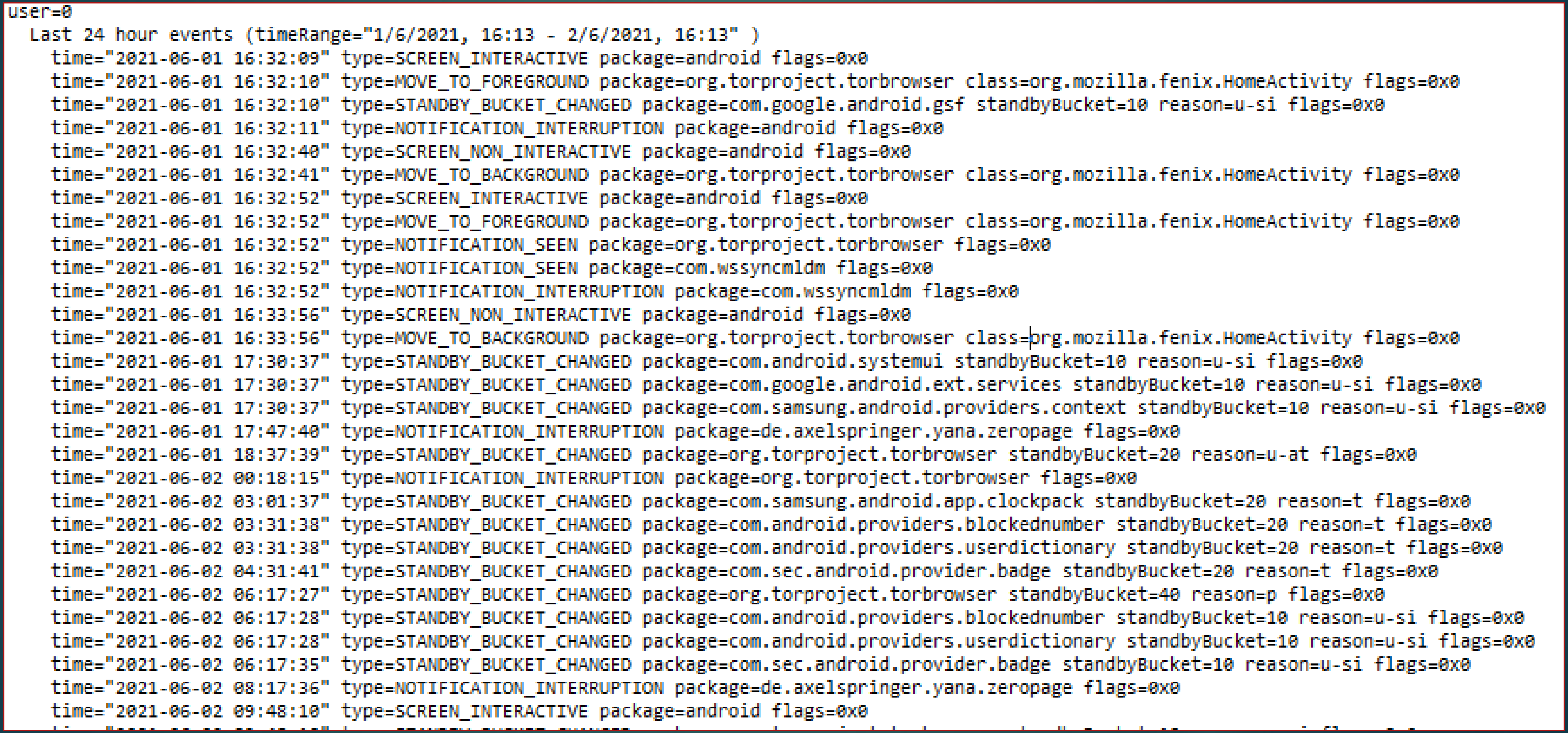
```
install permissions:
  com.google.android.c2dm.permission.RECEIVE: granted=true
  android.permission.USE_CREDENTIALS: granted=true
  android.permission.MODIFY_AUDIO_SETTINGS: granted=true
  com.google.android.providers.gsf.permission.READ_GSERVICES: granted=true
  android.permission.MANAGE_ACCOUNTS: granted=true
  android.permission.NFC: granted=true
  com.sec.android.provider.badge.permission.READ: granted=true
  android.permission.CHANGE_NETWORK_STATE: granted=true
  android.permission.FOREGROUND_SERVICE: granted=true
  android.permission.WRITE_SYNC_SETTINGS: granted=true
  android.permission.RECEIVE_BOOT_COMPLETED: granted=true
  com.whatsapp.permission.BROADCAST: granted=true
  com.android.launcher.permission.UNINSTALL_SHORTCUT: granted=true
  android.permission.READ_PROFILE: granted=true
  android.permission.BLUETOOTH: granted=true
  android.permission.GET_TASKS: granted=true
  android.permission.AUTHENTICATE_ACCOUNTS: granted=true
  android.permission.INTERNET: granted=true
  android.permission.USE_FULL_SCREEN_INTENT: granted=true
```

dumpsys **package**



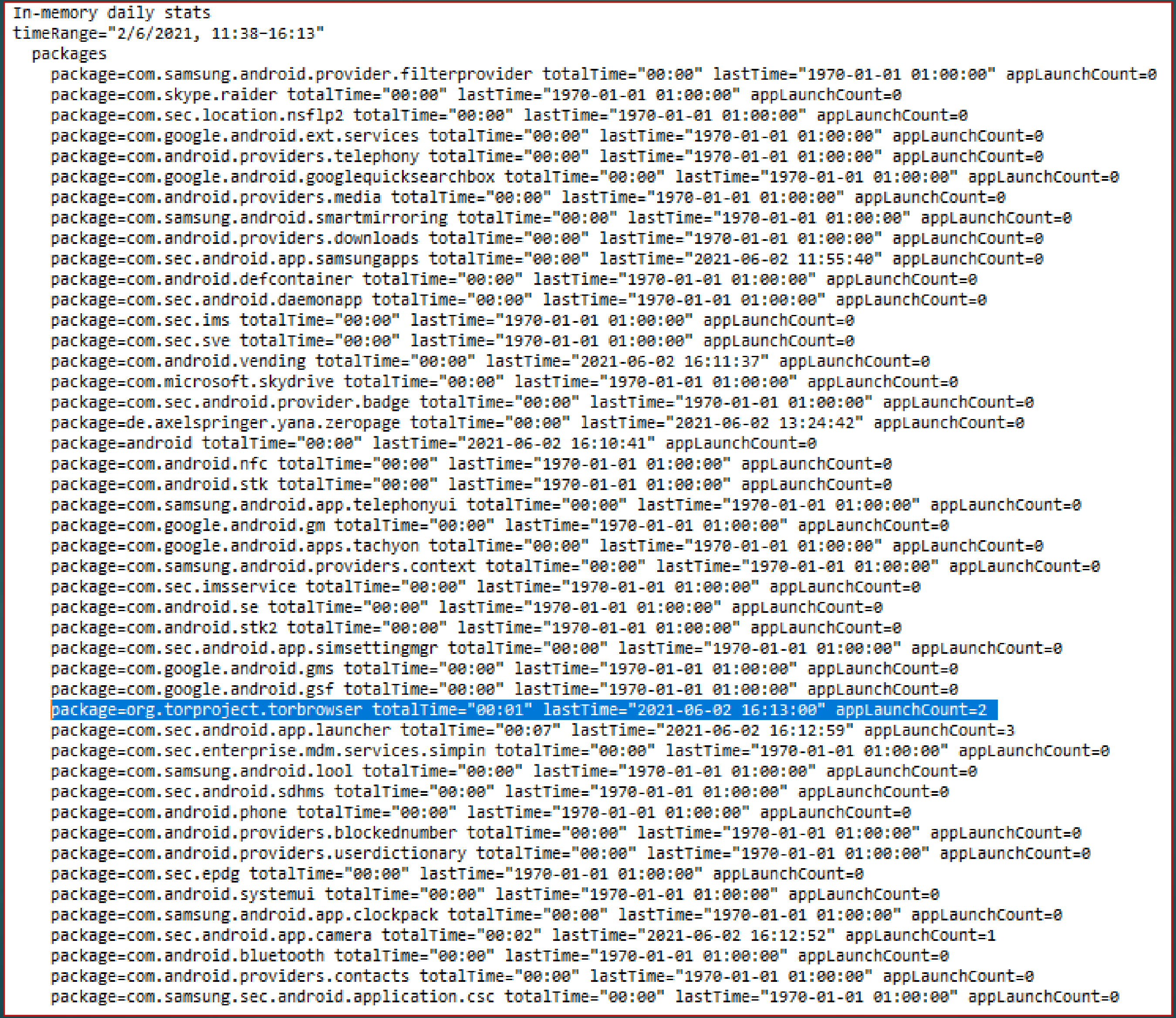
```
runtime permissions:
  android.permission.READ_CALL_LOG: granted=false, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED
  android.permission.ACCESS_FINE_LOCATION: granted=true, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_
  android.permission.ANSWER_PHONE_CALLS: granted=false, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_D
  android.permission.READ_PHONE_NUMBERS: granted=false, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_D
  android.permission.RECEIVE_SMS: granted=true, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RE
  android.permission.READ_EXTERNAL_STORAGE: granted=true, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN
  android.permission.ACCESS_COARSE_LOCATION: granted=true, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHE
  android.permission.READ_PHONE_STATE: granted=true, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENI
  android.permission.SEND_SMS: granted=true, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED|RESTR
  android.permission.CALL_PHONE: granted=false, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
  android.permission.WRITE_CONTACTS: granted=true, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED
  android.permission.CAMERA: granted=true, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
  android.permission.GET_ACCOUNTS: granted=true, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
  android.permission.WRITE_EXTERNAL_STORAGE: granted=true, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHE
  android.permission.RECORD_AUDIO: granted=true, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
  android.permission.READ_CONTACTS: granted=true, flags=[ USER_SENSITIVE_WHEN_GRANTED|USER_SENSITIVE_WHEN_DENIED]
```

dumpsys **usagestats**



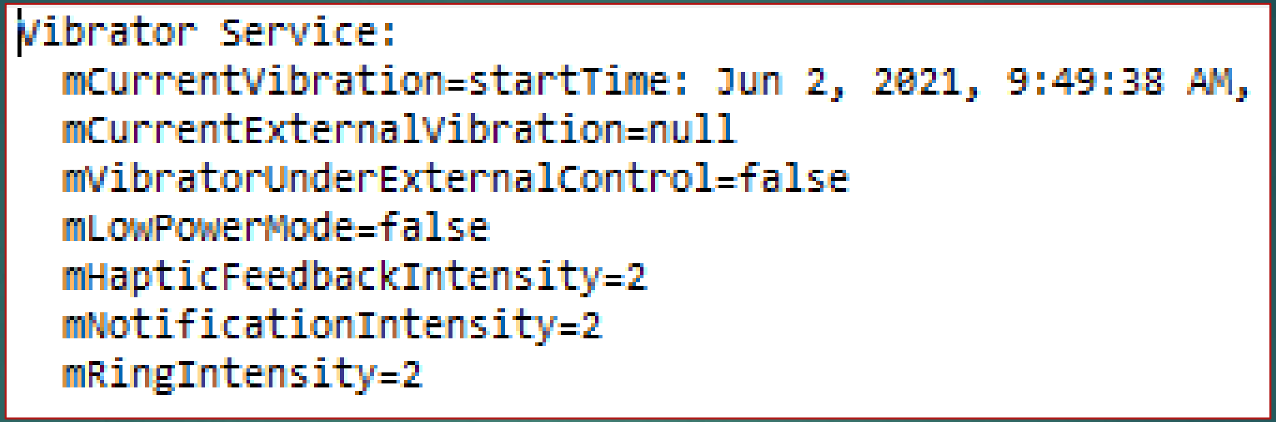
```
user=0
  Last 24 hour events (timeRange="1/6/2021, 16:13 - 2/6/2021, 16:13" )
    time="2021-06-01 16:32:09" type=SCREEN_INTERACTIVE package=android flags=0x0
    time="2021-06-01 16:32:10" type=MOVE_TO_FOREGROUND package=org.torproject.torbrowser class=org.mozilla.fenix.HomeActivity flags=0x0
    time="2021-06-01 16:32:10" type=STANDBY_BUCKET_CHANGED package=com.google.android.gsf standbyBucket=10 reason=u-si flags=0x0
    time="2021-06-01 16:32:11" type=NOTIFICATION_INTERRUPTION package=android flags=0x0
    time="2021-06-01 16:32:40" type=SCREEN_NON_INTERACTIVE package=android flags=0x0
    time="2021-06-01 16:32:41" type=MOVE_TO_BACKGROUND package=org.torproject.torbrowser class=org.mozilla.fenix.HomeActivity flags=0x0
    time="2021-06-01 16:32:52" type=SCREEN_INTERACTIVE package=android flags=0x0
    time="2021-06-01 16:32:52" type=MOVE_TO_FOREGROUND package=org.torproject.torbrowser class=org.mozilla.fenix.HomeActivity flags=0x0
    time="2021-06-01 16:32:52" type=NOTIFICATION_SEEN package=org.torproject.torbrowser flags=0x0
    time="2021-06-01 16:32:52" type=NOTIFICATION_SEEN package=com.wssyncmldm flags=0x0
    time="2021-06-01 16:32:52" type=NOTIFICATION_INTERRUPTION package=com.wssyncmldm flags=0x0
    time="2021-06-01 16:33:56" type=SCREEN_NON_INTERACTIVE package=android flags=0x0
    time="2021-06-01 16:33:56" type=MOVE_TO_BACKGROUND package=org.torproject.torbrowser class=org.mozilla.fenix.HomeActivity flags=0x0
    time="2021-06-01 17:30:37" type=STANDBY_BUCKET_CHANGED package=com.android.systemui standbyBucket=10 reason=u-si flags=0x0
    time="2021-06-01 17:30:37" type=STANDBY_BUCKET_CHANGED package=com.google.android.ext.services standbyBucket=10 reason=u-si flags=0x0
    time="2021-06-01 17:30:37" type=STANDBY_BUCKET_CHANGED package=com.samsung.android.providers.context standbyBucket=10 reason=u-si flags=0x0
    time="2021-06-01 17:47:40" type=NOTIFICATION_INTERRUPTION package=de.axelspringer.yana.zeropage flags=0x0
    time="2021-06-01 18:37:39" type=STANDBY_BUCKET_CHANGED package=org.torproject.torbrowser standbyBucket=20 reason=u-at flags=0x0
    time="2021-06-02 00:18:15" type=NOTIFICATION_INTERRUPTION package=org.torproject.torbrowser flags=0x0
    time="2021-06-02 03:01:37" type=STANDBY_BUCKET_CHANGED package=com.samsung.android.app.clockpack standbyBucket=20 reason=t flags=0x0
    time="2021-06-02 03:31:38" type=STANDBY_BUCKET_CHANGED package=com.android.providers.blockednumber standbyBucket=20 reason=t flags=0x0
    time="2021-06-02 03:31:38" type=STANDBY_BUCKET_CHANGED package=com.android.providers.userdictionary standbyBucket=20 reason=t flags=0x0
    time="2021-06-02 04:31:41" type=STANDBY_BUCKET_CHANGED package=com.sec.android.provider.badge standbyBucket=20 reason=t flags=0x0
    time="2021-06-02 06:17:27" type=STANDBY_BUCKET_CHANGED package=org.torproject.torbrowser standbyBucket=40 reason=p flags=0x0
    time="2021-06-02 06:17:28" type=STANDBY_BUCKET_CHANGED package=com.android.providers.blockednumber standbyBucket=10 reason=u-si flags=0x0
    time="2021-06-02 06:17:28" type=STANDBY_BUCKET_CHANGED package=com.android.providers.userdictionary standbyBucket=10 reason=u-si flags=0x0
    time="2021-06-02 06:17:35" type=STANDBY_BUCKET_CHANGED package=com.sec.android.provider.badge standbyBucket=10 reason=u-si flags=0x0
    time="2021-06-02 08:17:36" type=NOTIFICATION_INTERRUPTION package=de.axelspringer.yana.zeropage flags=0x0
    time="2021-06-02 09:48:10" type=SCREEN_INTERACTIVE package=android flags=0x0
```

dumpsys **usagestats**

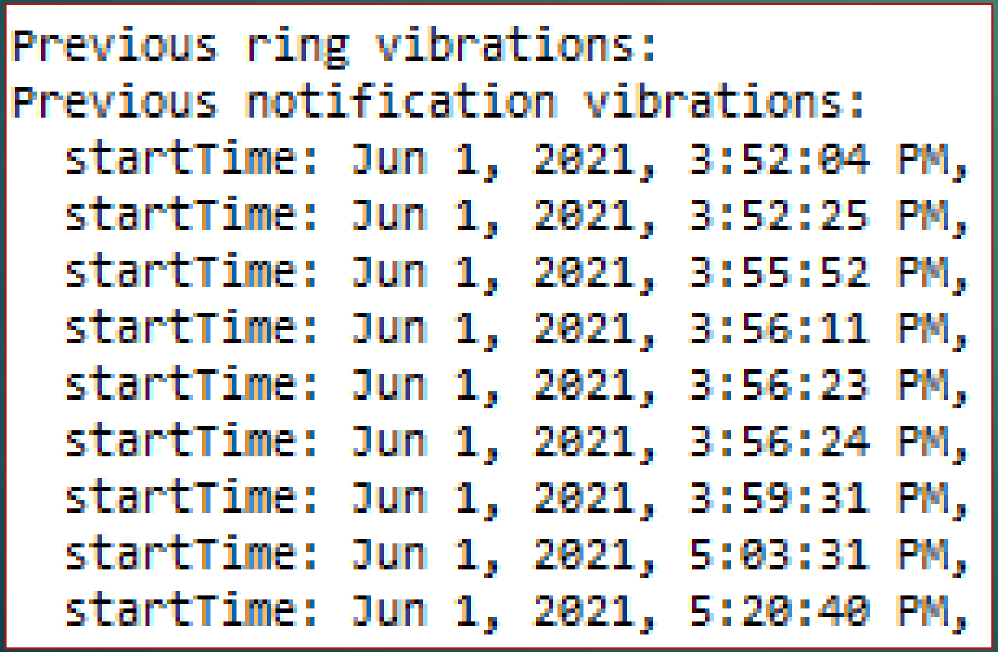


```
In-memory daily stats
timeRange="2/6/2021, 11:38-16:13"
  packages
    package=com.samsung.android.provider.filterprovider totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.skype.raider totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.sec.location.nsflp2 totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.google.android.ext.services totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.android.providers.telephony totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.google.android.googlequicksearchbox totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.android.providers.media totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.samsung.android.smartmirroring totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.android.providers.downloads totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.sec.android.app.samsungapps totalTime="00:00" lastTime="2021-06-02 11:55:40" appLaunchCount=0
    package=com.android.defcontainer totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.sec.android.daemonapp totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.sec.ims totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.sec.sve totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.android.vending totalTime="00:00" lastTime="2021-06-02 16:11:37" appLaunchCount=0
    package=com.microsoft.skydrive totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.sec.android.provider.badge totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=de.axelspringer.yana.zeropage totalTime="00:00" lastTime="2021-06-02 13:24:42" appLaunchCount=0
    package=android totalTime="00:00" lastTime="2021-06-02 16:10:41" appLaunchCount=0
    package=com.android.nfc totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.android.stk totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.samsung.android.app.telephonyui totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.google.android.gm totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.google.android.apps.tachyon totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.samsung.android.providers.context totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.sec.imsservice totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.android.se totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.android.stk2 totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.sec.android.app.simsettingmgr totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.google.android.gms totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.google.android.gsf totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=org.torproject.torbrowser totalTime="00:01" lastTime="2021-06-02 16:13:00" appLaunchCount=2
    package=com.sec.android.app.launcher totalTime="00:07" lastTime="2021-06-02 16:12:59" appLaunchCount=3
    package=com.sec.enterprise.mdm.services.simpin totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.samsung.android.lool totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.sec.android.sdhms totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.android.phone totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.android.providers.blockednumber totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.android.providers.userdictionary totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.sec.epdg totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.android.systemui totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.samsung.android.app.clockpack totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.sec.android.app.camera totalTime="00:02" lastTime="2021-06-02 16:12:52" appLaunchCount=1
    package=com.android.bluetooth totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.android.providers.contacts totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
    package=com.samsung.sec.android.application.csc totalTime="00:00" lastTime="1970-01-01 01:00:00" appLaunchCount=0
```

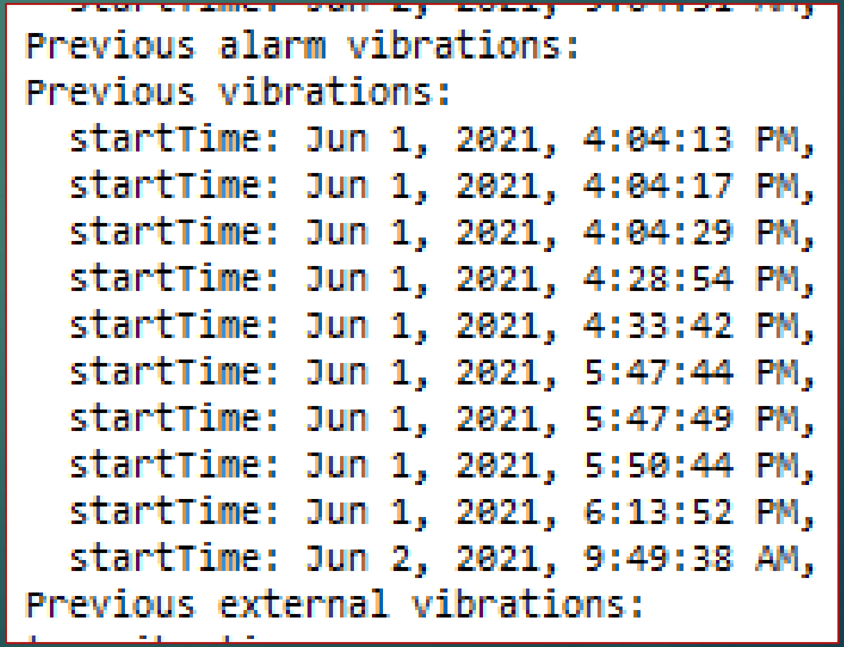
dumpsys **vibrator**



```
Vibrator Service:
  mCurrentVibration=startTime: Jun 2, 2021, 9:49:38 AM,
  mCurrentExternalVibration=null
  mVibratorUnderExternalControl=false
  mLowPowerMode=false
  mHapticFeedbackIntensity=2
  mNotificationIntensity=2
  mRingIntensity=2
```

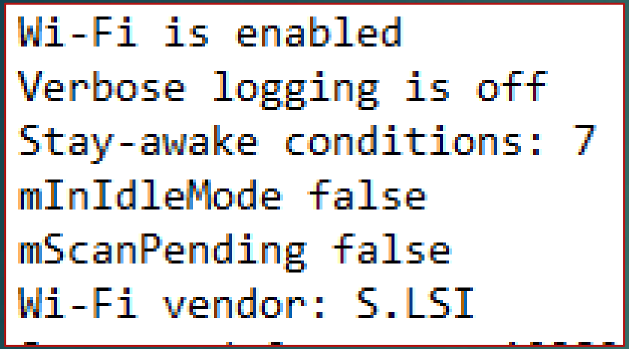


```
Previous ring vibrations:
Previous notification vibrations:
  startTime: Jun 1, 2021, 3:52:04 PM,
  startTime: Jun 1, 2021, 3:52:25 PM,
  startTime: Jun 1, 2021, 3:55:52 PM,
  startTime: Jun 1, 2021, 3:56:11 PM,
  startTime: Jun 1, 2021, 3:56:23 PM,
  startTime: Jun 1, 2021, 3:56:24 PM,
  startTime: Jun 1, 2021, 3:59:31 PM,
  startTime: Jun 1, 2021, 5:03:31 PM,
  startTime: Jun 1, 2021, 5:20:40 PM,
```

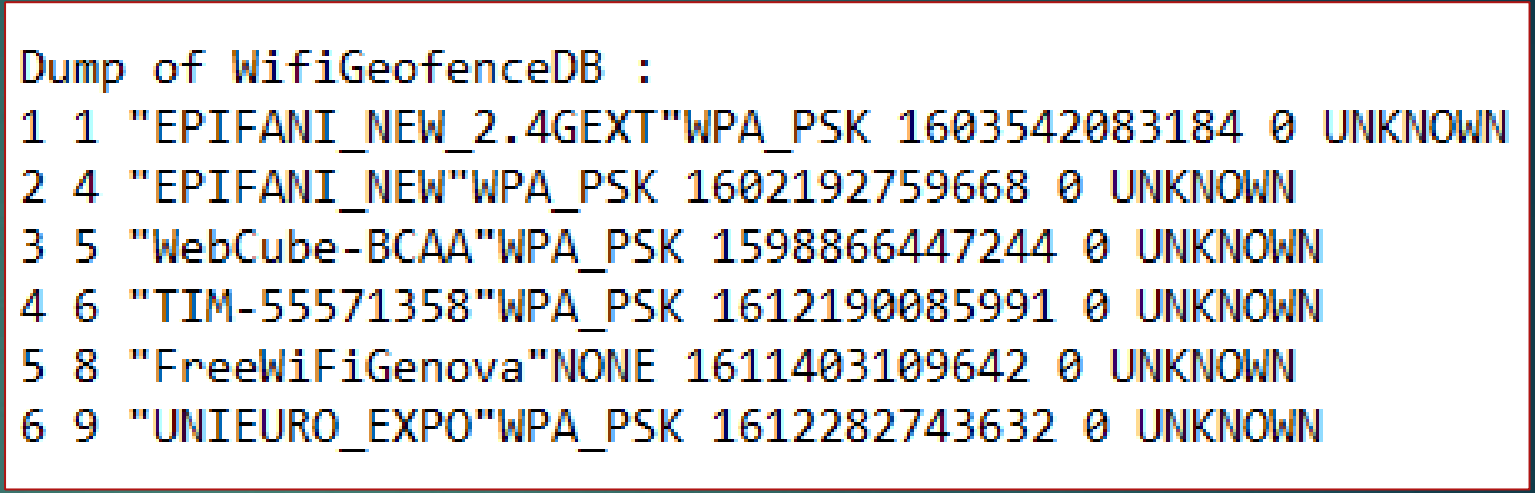


```
Previous alarm vibrations:
Previous vibrations:
  startTime: Jun 1, 2021, 4:04:13 PM,
  startTime: Jun 1, 2021, 4:04:17 PM,
  startTime: Jun 1, 2021, 4:04:29 PM,
  startTime: Jun 1, 2021, 4:28:54 PM,
  startTime: Jun 1, 2021, 4:33:42 PM,
  startTime: Jun 1, 2021, 5:47:44 PM,
  startTime: Jun 1, 2021, 5:47:49 PM,
  startTime: Jun 1, 2021, 5:50:44 PM,
  startTime: Jun 1, 2021, 6:13:52 PM,
  startTime: Jun 2, 2021, 9:49:38 AM,
Previous external vibrations:
```

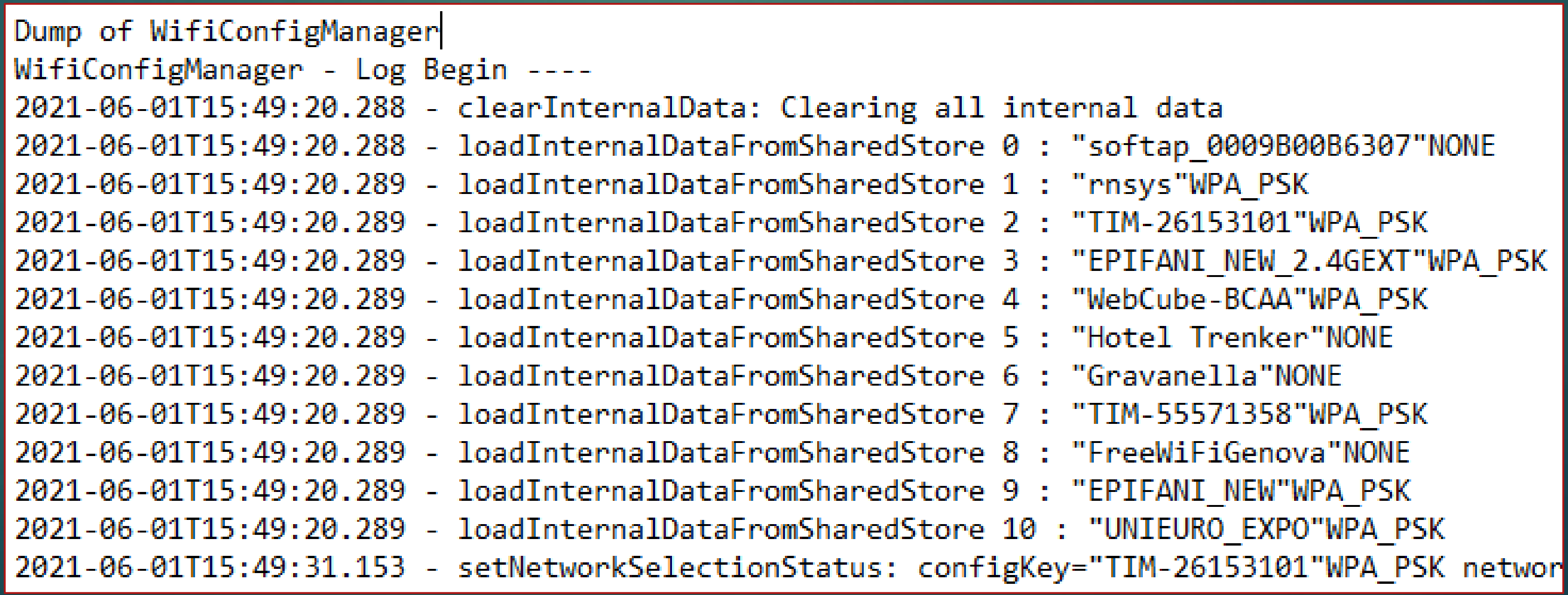
dumpsys **wifi**



```
Wi-Fi is enabled
Verbose logging is off
Stay-awake conditions: 7
mInIdleMode false
mScanPending false
Wi-Fi vendor: S.LSI
```

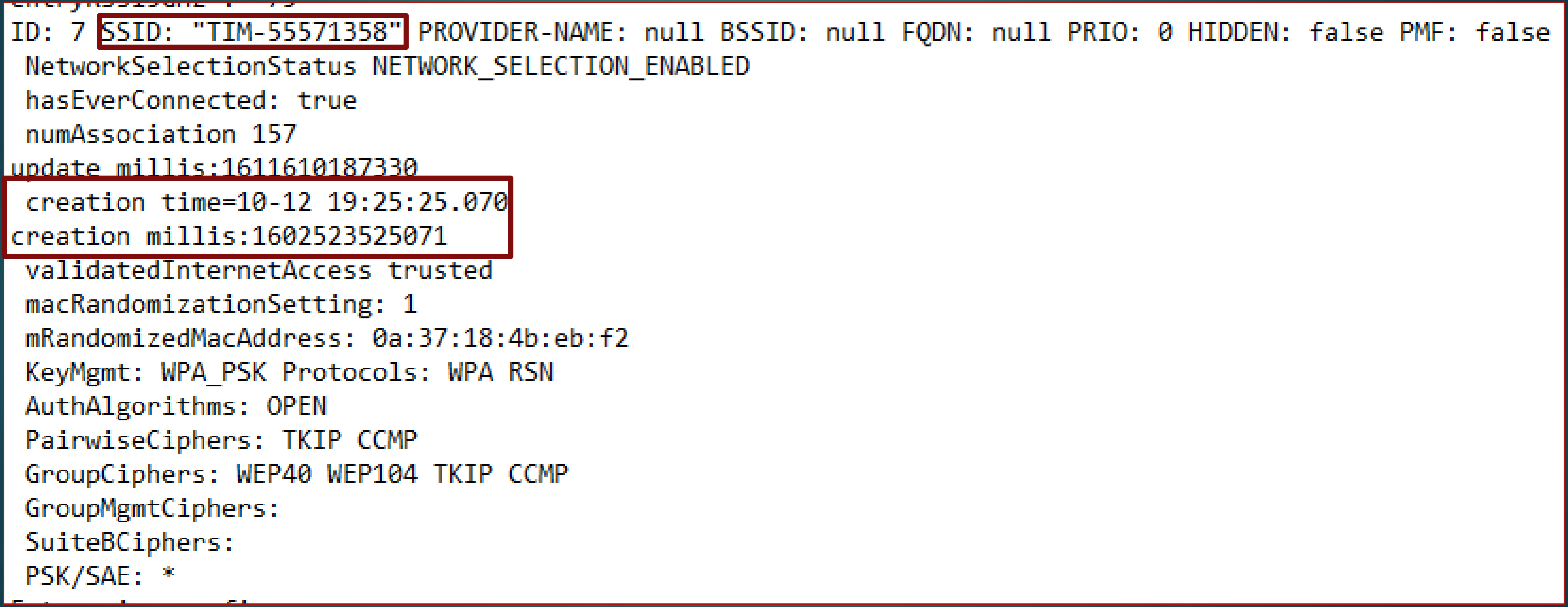


```
Dump of WifiGeofenceDB :
1 1 "EPIFANI_NEW_2.4GEXT"WPA_PSK 1603542083184 0 UNKNOWN
2 4 "EPIFANI_NEW"WPA_PSK 1602192759668 0 UNKNOWN
3 5 "WebCube-BCAA"WPA_PSK 1598866447244 0 UNKNOWN
4 6 "TIM-55571358"WPA_PSK 1612190085991 0 UNKNOWN
5 8 "FreeWiFiGenova"NONE 1611403109642 0 UNKNOWN
6 9 "UNIEURO_EXPO"WPA_PSK 1612282743632 0 UNKNOWN
```



```
Dump of WifiConfigManager
WifiConfigManager - Log Begin ----
2021-06-01T15:49:20.288 - clearInternalData: Clearing all internal data
2021-06-01T15:49:20.288 - loadInternalDataFromSharedStore 0 : "softap_0009B00B6307"NONE
2021-06-01T15:49:20.289 - loadInternalDataFromSharedStore 1 : "rnsys"WPA_PSK
2021-06-01T15:49:20.289 - loadInternalDataFromSharedStore 2 : "TIM-26153101"WPA_PSK
2021-06-01T15:49:20.289 - loadInternalDataFromSharedStore 3 : "EPIFANI_NEW_2.4GEXT"WPA_PSK
2021-06-01T15:49:20.289 - loadInternalDataFromSharedStore 4 : "WebCube-BCAA"WPA_PSK
2021-06-01T15:49:20.289 - loadInternalDataFromSharedStore 5 : "Hotel Trenker"NONE
2021-06-01T15:49:20.289 - loadInternalDataFromSharedStore 6 : "Gravanella"NONE
2021-06-01T15:49:20.289 - loadInternalDataFromSharedStore 7 : "TIM-55571358"WPA_PSK
2021-06-01T15:49:20.289 - loadInternalDataFromSharedStore 8 : "FreeWiFiGenova"NONE
2021-06-01T15:49:20.289 - loadInternalDataFromSharedStore 9 : "EPIFANI_NEW"WPA_PSK
2021-06-01T15:49:20.289 - loadInternalDataFromSharedStore 10 : "UNIEURO_EXPO"WPA_PSK
2021-06-01T15:49:31.153 - setNetworkSelectionStatus: configKey="TIM-26153101"WPA_PSK networ
```

dumpsys **wifi**

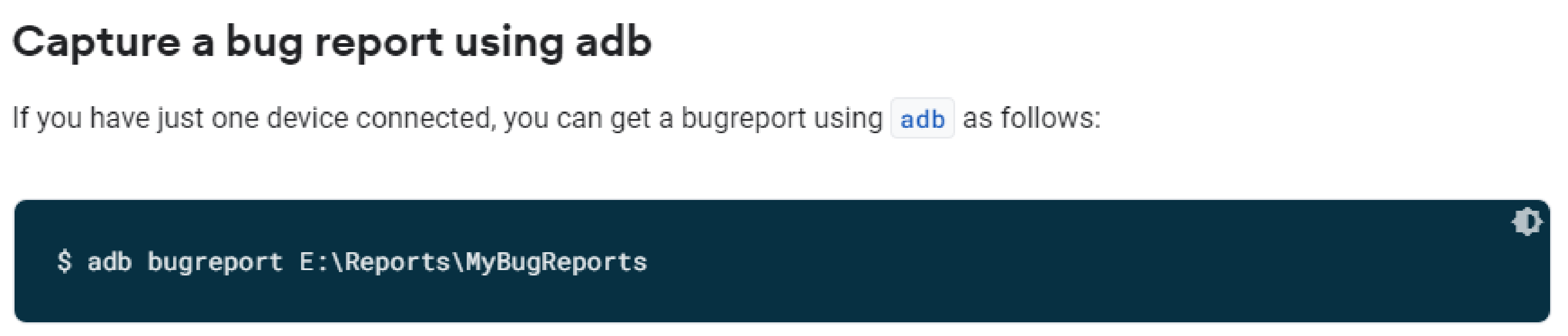


```
ID: 7 SSID: "TIM-55571358" PROVIDER-NAME: null BSSID: null FQDN: null PRIO: 0 HIDDEN: false PMF: false
 NetworkSelectionStatus NETWORK_SELECTION_ENABLED
 hasEverConnected: true
 numAssociation 157
update millis:1611610187330
 creation time=10-12 19:25:25.070
creation millis:1602523525071
 validatedInternetAccess trusted
 macRandomizationSetting: 1
 mRandomizedMacAddress: 0a:37:18:4b:eb:f2
 KeyMgmt: WPA_PSK Protocols: WPA RSN
 AuthAlgorithms: OPEN
 PairwiseCiphers: TKIP CCMP
 GroupCiphers: WEP40 WEP104 TKIP CCMP
 GroupMgmtCiphers:
 SuiteBCiphers:
 PSK/SAE: *
```

BUGREPORT

https://developer.android.com/studio/debug/bug-report#bugreportadb

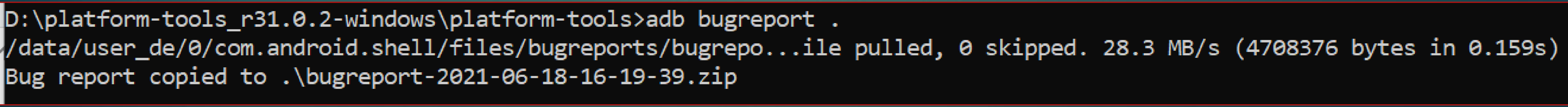
- A bug report contains device logs, stack traces, and other diagnostic information



Capture a bug report using adb

If you have just one device connected, you can get a bugreport using `adb` as follows:

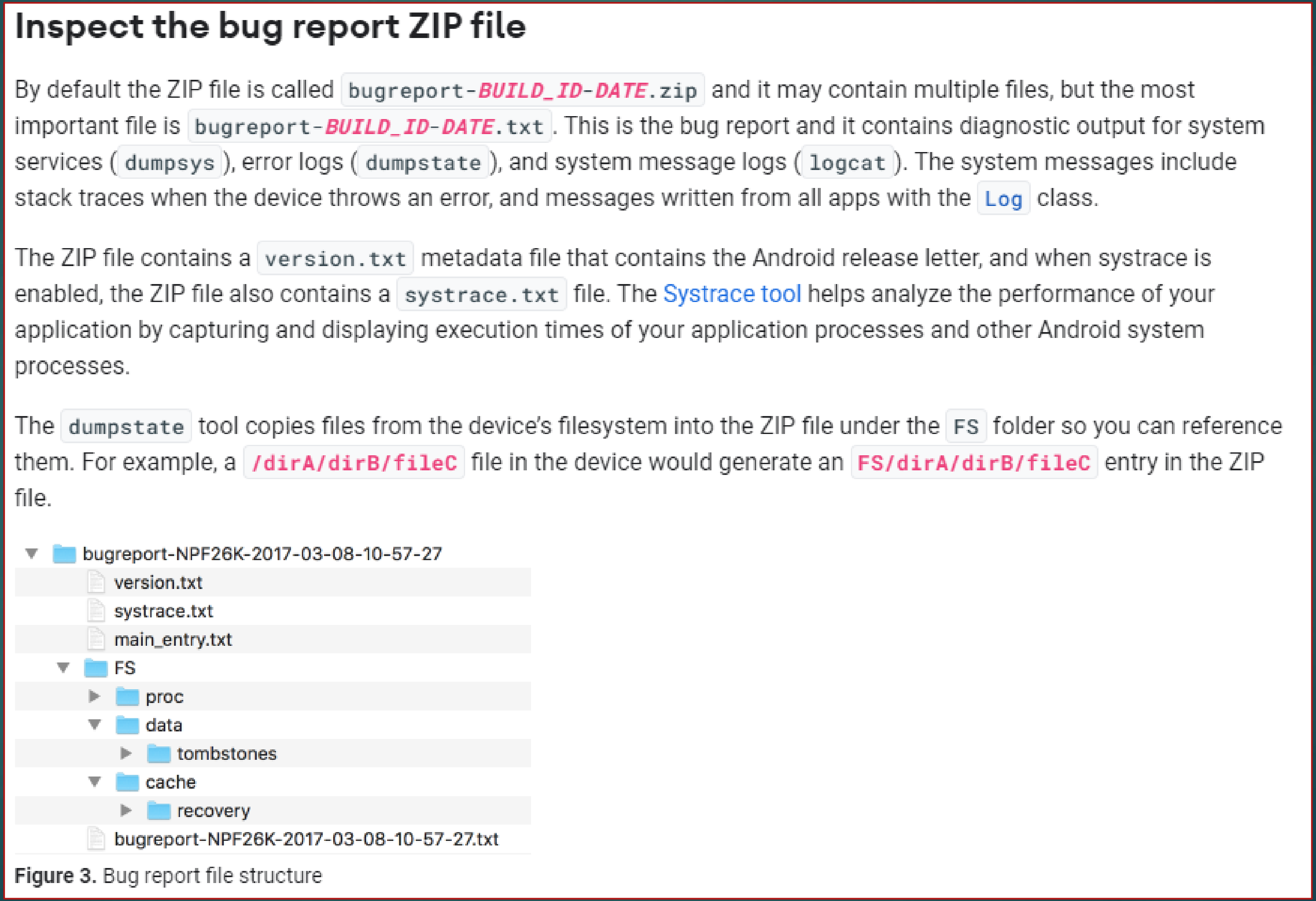
```
$ adb bugreport E:\Reports\MyBugReports
```



```
D:\platform-tools_r31.0.2-windows\platform-tools>adb bugreport .
/data/user_de/0/com.android.shell/files/bugreports/bugrepo...ile pulled, 0 skipped. 28.3 MB/s (4708376 bytes in 0.159s)
Bug report copied to .\bugreport-2021-06-18-16-19-39.zip
```

BUGREPORT

https://developer.android.com/studio/debug/bug-report#bugreport



Inspect the bug report ZIP file

By default the ZIP file is called `bugreport-BUILD_ID-DATE.zip` and it may contain multiple files, but the most important file is `bugreport-BUILD_ID-DATE.txt`. This is the bug report and it contains diagnostic output for system services (`dumpsys`), error logs (`dumpstate`), and system message logs (`logcat`). The system messages include stack traces when the device throws an error, and messages written from all apps with the `Log` class.

The ZIP file contains a `version.txt` metadata file that contains the Android release letter, and when systrace is enabled, the ZIP file also contains a `systrace.txt` file. The Systrace tool helps analyze the performance of your application by capturing and displaying execution times of your application processes and other Android system processes.

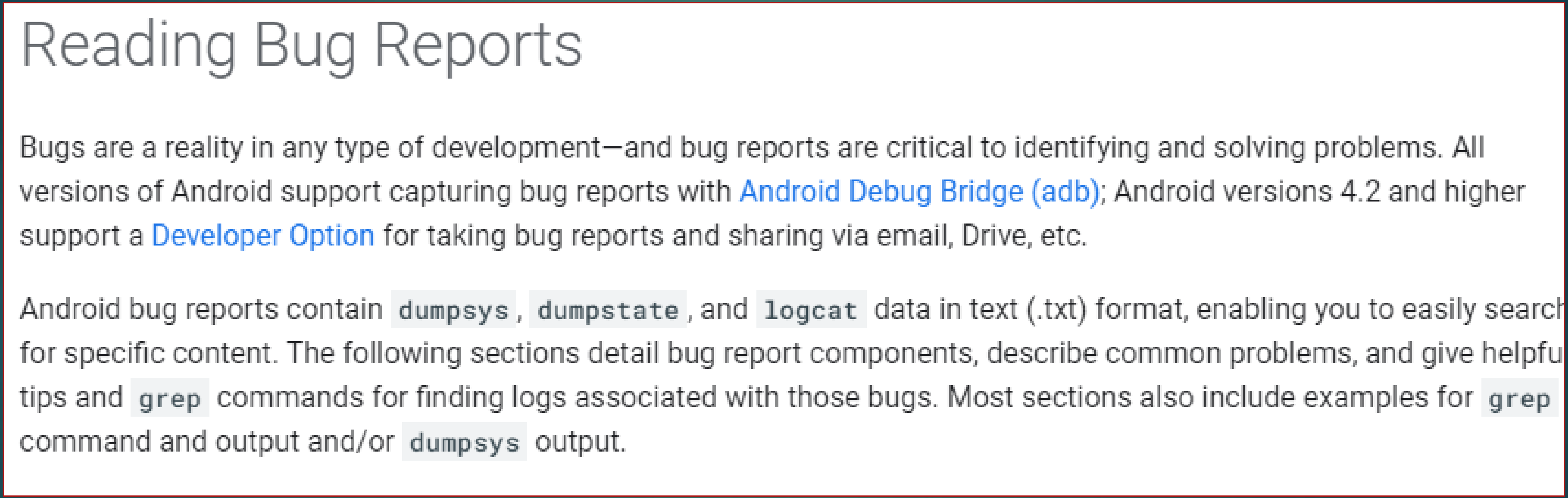
The `dumpstate` tool copies files from the device's filesystem into the ZIP file under the `FS` folder so you can reference them. For example, a `/dirA/dirB/fileC` file in the device would generate an `FS/dirA/dirB/fileC` entry in the ZIP file.

```
▼ bugreport-NPF26K-2017-03-08-10-57-27
      version.txt
      systrace.txt
      main_entry.txt
    ▼ FS
        ▶ proc
        ▼ data
            ▶ tombstones
        ▼ cache
            ▶ recovery
      bugreport-NPF26K-2017-03-08-10-57-27.txt
```

Figure 3. Bug report file structure

BUGREPORT

https://source.android.com/setup/contribute/read-bug-reports



Reading Bug Reports

Bugs are a reality in any type of development—and bug reports are critical to identifying and solving problems. All versions of Android support capturing bug reports with Android Debug Bridge (adb); Android versions 4.2 and higher support a Developer Option for taking bug reports and sharing via email, Drive, etc.

Android bug reports contain `dumpsys`, `dumpstate`, and `logcat` data in text (.txt) format, enabling you to easily search for specific content. The following sections detail bug report components, describe common problems, and give helpfu tips and `grep` commands for finding logs associated with those bugs. Most sections also include examples for `grep` command and output and/or `dumpsys` output.

PACKAGE MANAGER

https://developer.android.com/studio/command-line/adb#pm

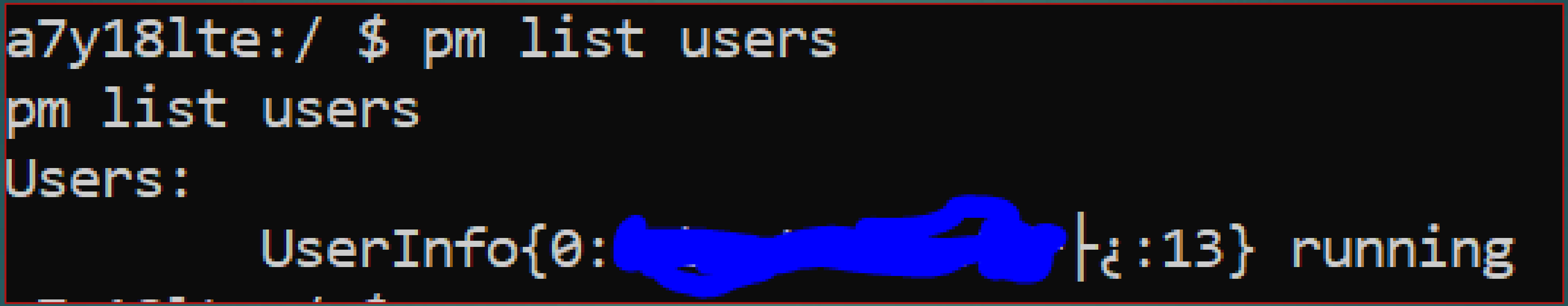
- *Within an adb shell, you* ***can issue commands with the package manager (pm) tool*** *to perform actions and queries on app packages installed on the device*

- While in the shell, the syntax is:

```
pm command
```

pm list users

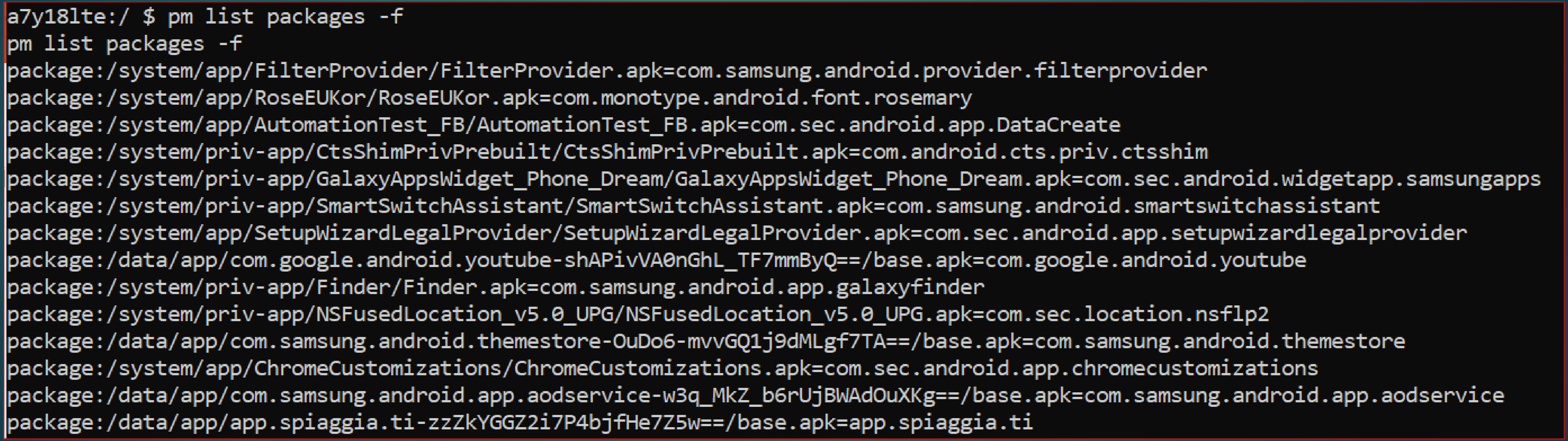
- Prints all users on the system



```
a7y18lte:/ $ pm list users
pm list users
Users:
        UserInfo{0:[redacted]├¿:13} running
```

pm list packages -f

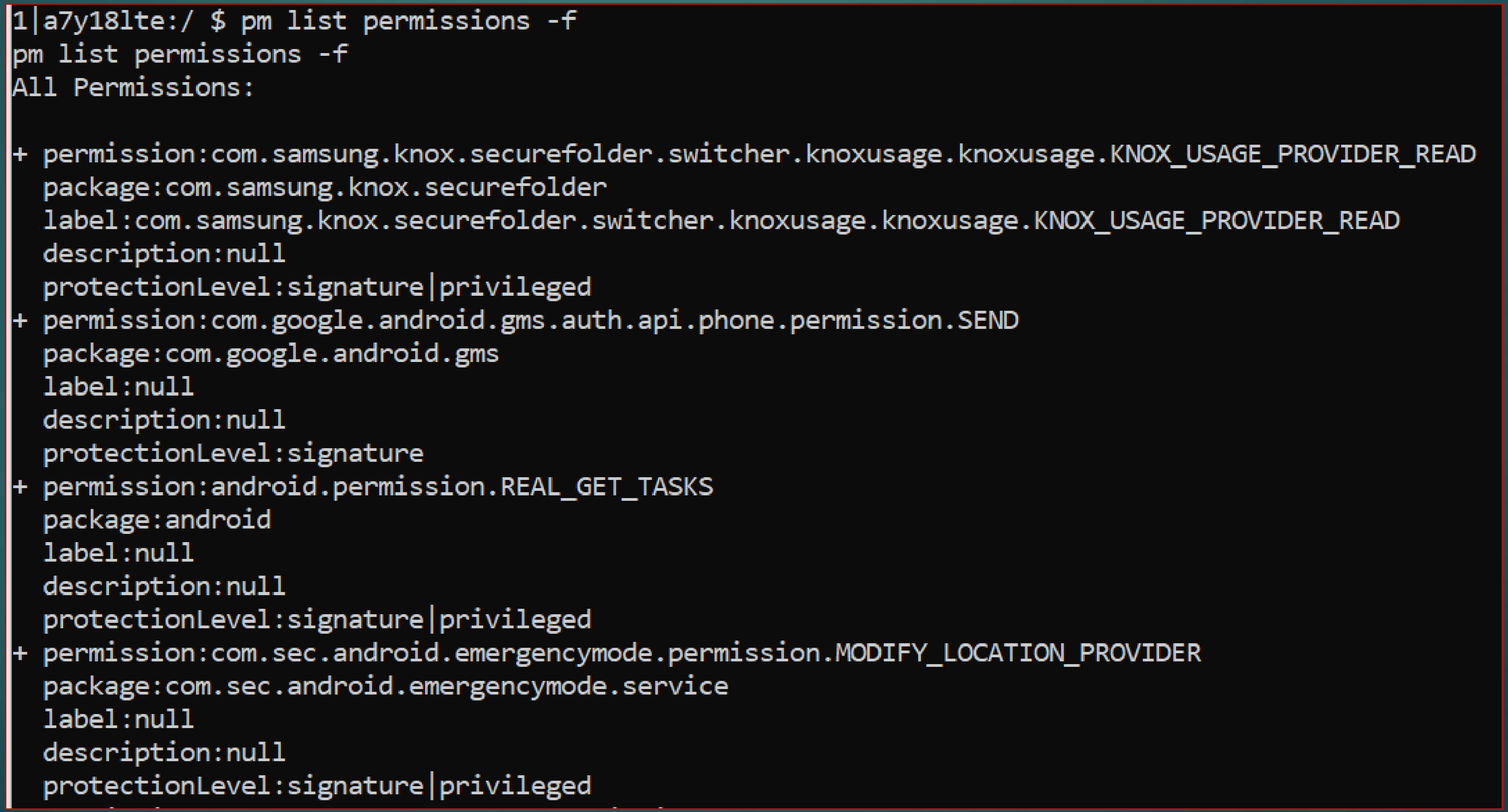
- Prints all packages, including their associated APKs (-f)



```
a7y18lte:/ $ pm list packages -f
pm list packages -f
package:/system/app/FilterProvider/FilterProvider.apk=com.samsung.android.provider.filterprovider
package:/system/app/RoseEUKor/RoseEUKor.apk=com.monotype.android.font.rosemary
package:/system/app/AutomationTest_FB/AutomationTest_FB.apk=com.sec.android.app.DataCreate
package:/system/priv-app/CtsShimPrivPrebuilt/CtsShimPrivPrebuilt.apk=com.android.cts.priv.ctsshim
package:/system/priv-app/GalaxyAppsWidget_Phone_Dream/GalaxyAppsWidget_Phone_Dream.apk=com.sec.android.widgetapp.samsungapps
package:/system/priv-app/SmartSwitchAssistant/SmartSwitchAssistant.apk=com.samsung.android.smartswitchassistant
package:/system/app/SetupWizardLegalProvider/SetupWizardLegalProvider.apk=com.sec.android.app.setupwizardlegalprovider
package:/data/app/com.google.android.youtube-shAPivVA0nGhL_TF7mmByQ==/base.apk=com.google.android.youtube
package:/system/priv-app/Finder/Finder.apk=com.samsung.android.app.galaxyfinder
package:/system/priv-app/NSFusedLocation_v5.0_UPG/NSFusedLocation_v5.0_UPG.apk=com.sec.location.nsflp2
package:/data/app/com.samsung.android.themestore-OuDo6-mvvGQ1j9dMLgf7TA==/base.apk=com.samsung.android.themestore
package:/system/app/ChromeCustomizations/ChromeCustomizations.apk=com.sec.android.app.chromecustomizations
package:/data/app/com.samsung.android.app.aodservice-w3q_MkZ_b6rUjBWAdOuXKg==/base.apk=com.samsung.android.app.aodservice
package:/data/app/app.spiaggia.ti-zzZkYGGZ2i7P4bjfHe7Z5w==/base.apk=app.spiaggia.ti
```

pm list permissions -f

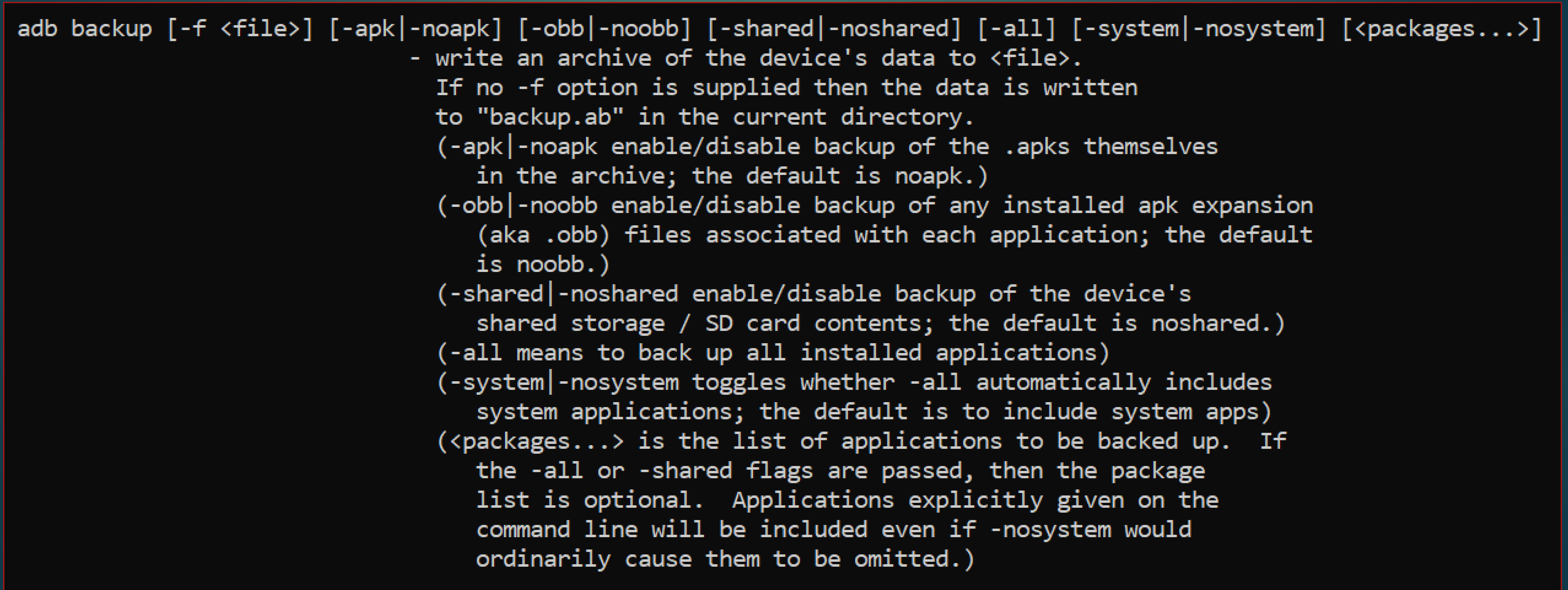
- Prints all known permissions, including all related information (-f)



```
1|a7y18lte:/ $ pm list permissions -f
pm list permissions -f
All Permissions:

+ permission:com.samsung.knox.securefolder.switcher.knoxusage.knoxusage.KNOX_USAGE_PROVIDER_READ
  package:com.samsung.knox.securefolder
  label:com.samsung.knox.securefolder.switcher.knoxusage.knoxusage.KNOX_USAGE_PROVIDER_READ
  description:null
  protectionLevel:signature|privileged
+ permission:com.google.android.gms.auth.api.phone.permission.SEND
  package:com.google.android.gms
  label:null
  description:null
  protectionLevel:signature
+ permission:android.permission.REAL_GET_TASKS
  package:android
  label:null
  description:null
  protectionLevel:signature|privileged
+ permission:com.sec.android.emergencymode.permission.MODIFY_LOCATION_PROVIDER
  package:com.sec.android.emergencymode.service
  label:null
  description:null
  protectionLevel:signature|privileged
```

ANDROID BACKUP

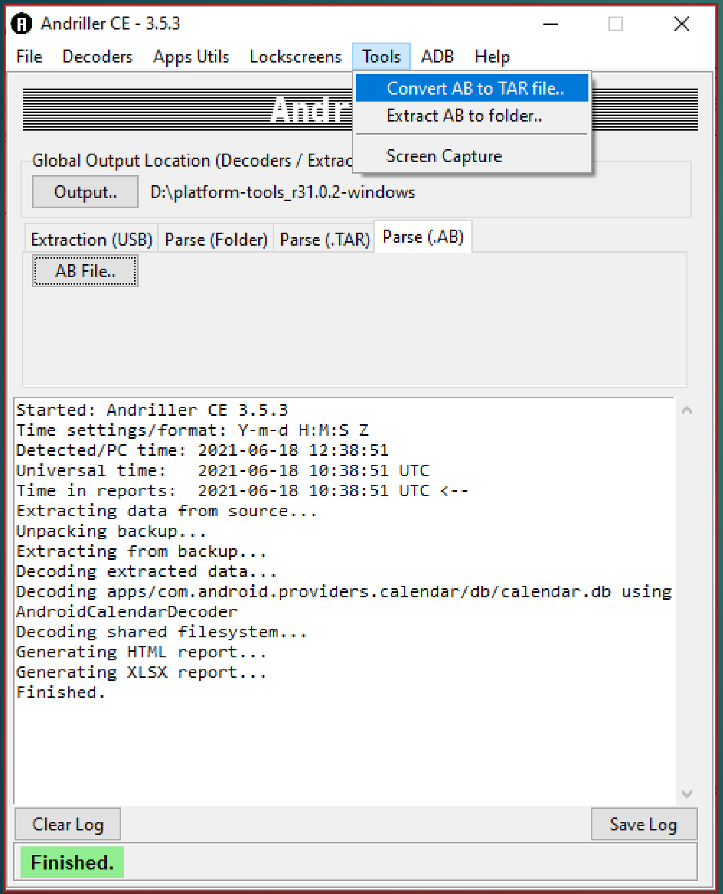
- Now deprecated, but still working with latest ADB release



```
adb backup [-f <file>] [-apk|-noapk] [-obb|-noobb] [-shared|-noshared] [-all] [-system|-nosystem] [<packages...>]
                             - write an archive of the device's data to <file>.
                               If no -f option is supplied then the data is written
                               to "backup.ab" in the current directory.
                               (-apk|-noapk enable/disable backup of the .apks themselves
                                  in the archive; the default is noapk.)
                               (-obb|-noobb enable/disable backup of any installed apk expansion
                                  (aka .obb) files associated with each application; the default
                                  is noobb.)
                               (-shared|-noshared enable/disable backup of the device's
                                  shared storage / SD card contents; the default is noshared.)
                               (-all means to back up all installed applications)
                               (-system|-nosystem toggles whether -all automatically includes
                                  system applications; the default is to include system apps)
                               (<packages...> is the list of applications to be backed up.  If
                                  the -all or -shared flags are passed, then the package
                                  list is optional.  Applications explicitly given on the
                                  command line will be included even if -nosystem would
                                  ordinarily cause them to be omitted.)
```

ANDROID BACKUP

adb backup -all -shared -system -keyvalue -apk -f backup.ab

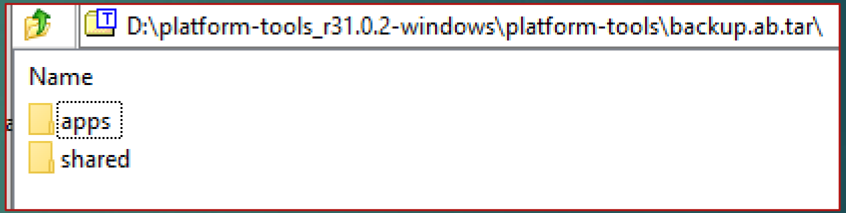


Global Output Location (Decoders / Extrac

Output.. D:\platform-tools_r31.0.2-windows

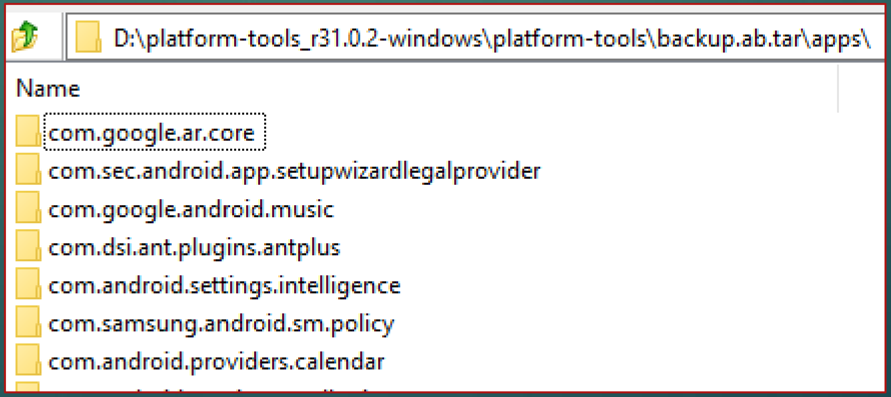
```
Started: Andriller CE 3.5.3
Time settings/format: Y-m-d H:M:S Z
Detected/PC time: 2021-06-18 12:38:51
Universal time:   2021-06-18 10:38:51 UTC
Time in reports:  2021-06-18 10:38:51 UTC <--
Extracting data from source...
Unpacking backup...
Extracting from backup...
Decoding extracted data...
Decoding apps/com.android.providers.calendar/db/calendar.db using
AndroidCalendarDecoder
Decoding shared filesystem...
Generating HTML report...
Generating XLSX report...
Finished.
```

Finished.



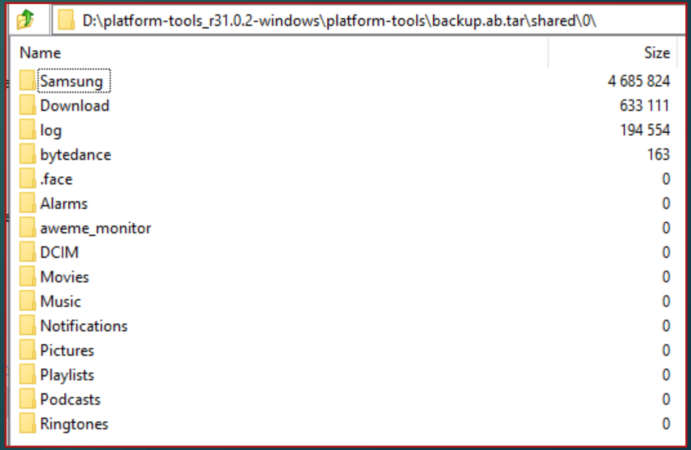
D:\platform-tools_r31.0.2-windows\platform-tools\backup.ab.tar\

Name
- apps
- shared



D:\platform-tools_r31.0.2-windows\platform-tools\backup.ab.tar\apps\

Name
- com.google.ar.core
- com.sec.android.app.setupwizardlegalprovider
- com.google.android.music
- com.dsi.ant.plugins.antplus
- com.android.settings.intelligence
- com.samsung.android.sm.policy
- com.android.providers.calendar



D:\platform-tools_r31.0.2-windows\platform-tools\backup.ab.tar\shared\0\

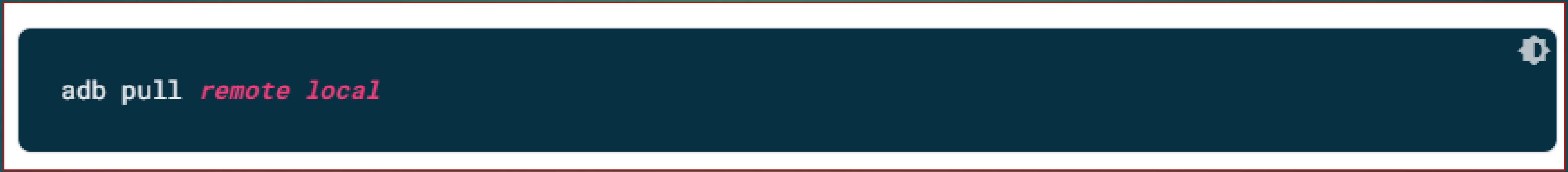
Name	Size
Samsung	4 685 824
Download	633 111
log	194 554
bytedance	163
.face	0
Alarms	0
aweme_monitor	0
DCIM	0
Movies	0
Music	0
Notifications	0
Pictures	0
Playlists	0
Podcasts	0
Ringtones	0

PULL

https://developer.android.com/studio/command-line/adb#copyfiles

- *Use the pull and push commands to copy files to and from a device*

- To copy a file or directory and its sub-directories from the device



```
adb pull remote local
```

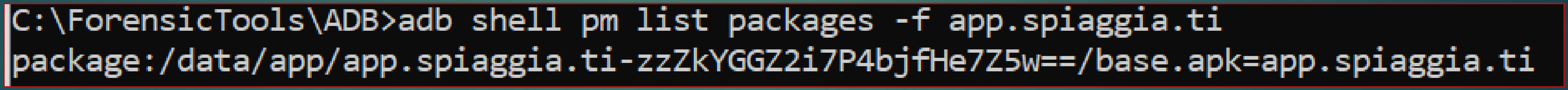
Partial File System

- We can pull
  - **/system** folder, that contains the OS
  - **/sdcard** folder, that points to the emulated storage folder and contains media and other files

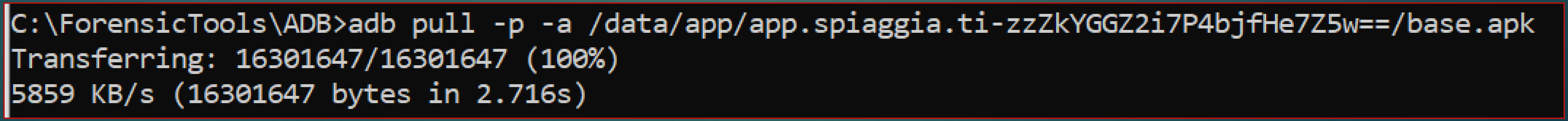
- The **/data** folder requires root access, but some files are always accessible
  - **APKs in /data/app/<package_name>**
  - **/data/system/uiderrors.txt**

APKs

- We can pull system and user-installed APKs
- Run **pm list packages –f <package_name>** to obtain the path
- Run **adb pull <path_to_APK>** to extract the file



```
C:\ForensicTools\ADB>adb shell pm list packages -f app.spiaggia.ti
package:/data/app/app.spiaggia.ti-zzZkYGGZ2i7P4bjfHe7Z5w==/base.apk=app.spiaggia.ti
```

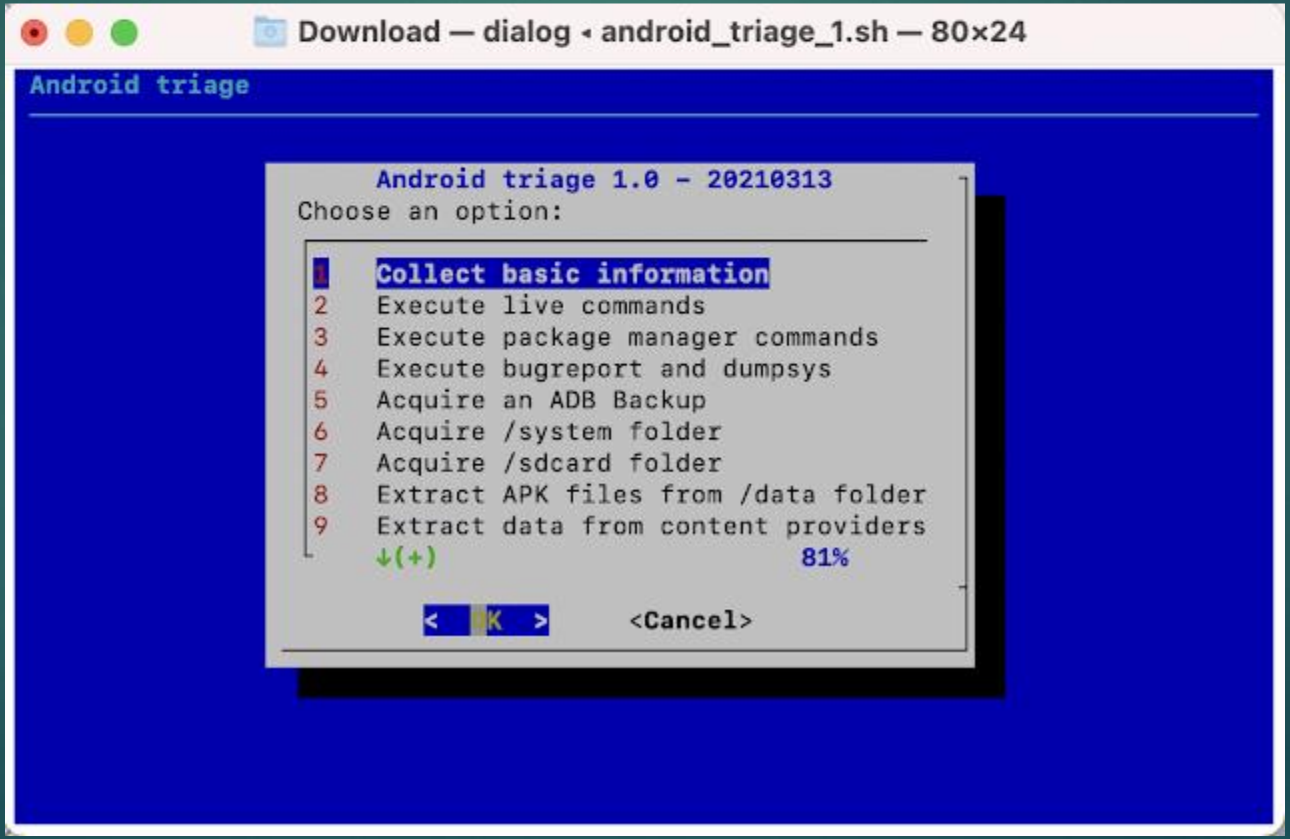


```
C:\ForensicTools\ADB>adb pull -p -a /data/app/app.spiaggia.ti-zzZkYGGZ2i7P4bjfHe7Z5w==/base.apk
Transferring: 16301647/16301647 (100%)
5859 KB/s (16301647 bytes in 2.716s)
```

Android Triage

https://blog.digital-forensics.it/2021/03/triaging-modern-android-devices-aka.html

- Bash script to extract data from an Android device



```
Android triage

              Android triage 1.0 - 20210313
          Choose an option:

           1    Collect basic information
           2    Execute live commands
           3    Execute package manager commands
           4    Execute bugreport and dumpsys
           5    Acquire an ADB Backup
           6    Acquire /system folder
           7    Acquire /sdcard folder
           8    Extract APK files from /data folder
           9    Extract data from content providers
                ↓(+)                              81%

                   <  OK  >         <Cancel>
```

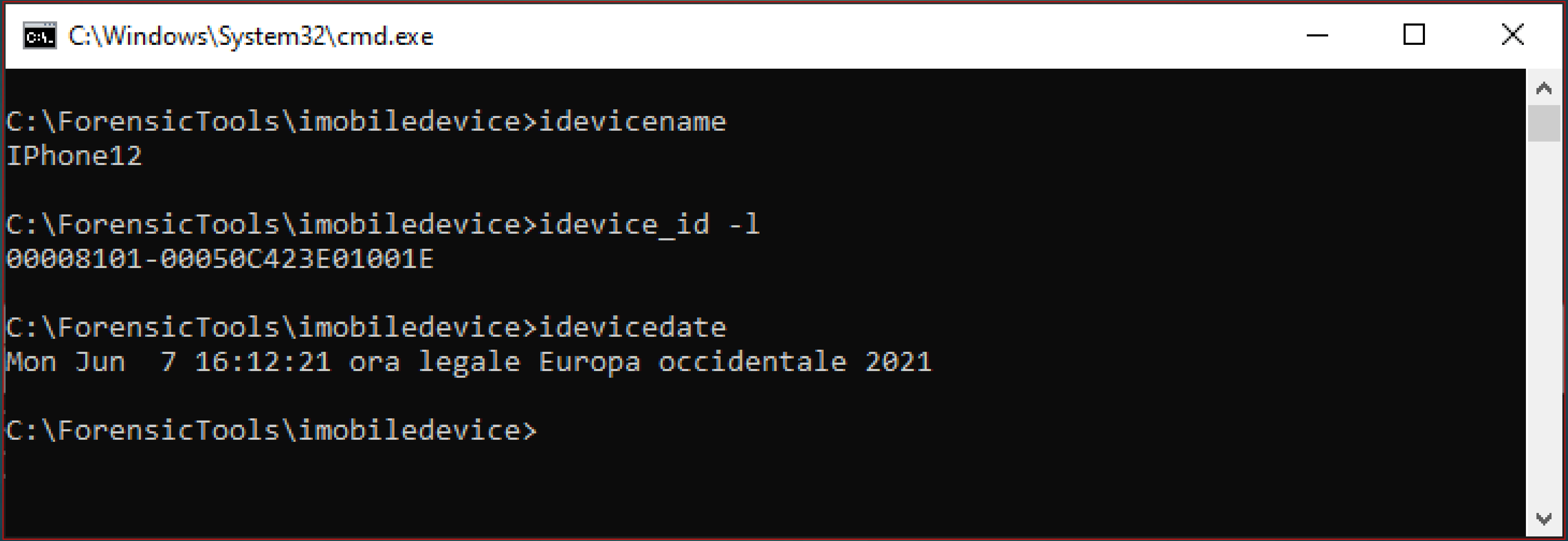
Android Triage

- Download android_triage.sh from https://github.com/RealityNet/android_triage
- Run **sudo apt-get install dialog**
- Run **sudo apt-get install android-tools-adb**
- Run **chmod +x android_triage.sh**
- **Activate ADB** on the Android Device
- **Connect and pair** the Android Device and the host
- Run **./android_triage.sh**

iOS

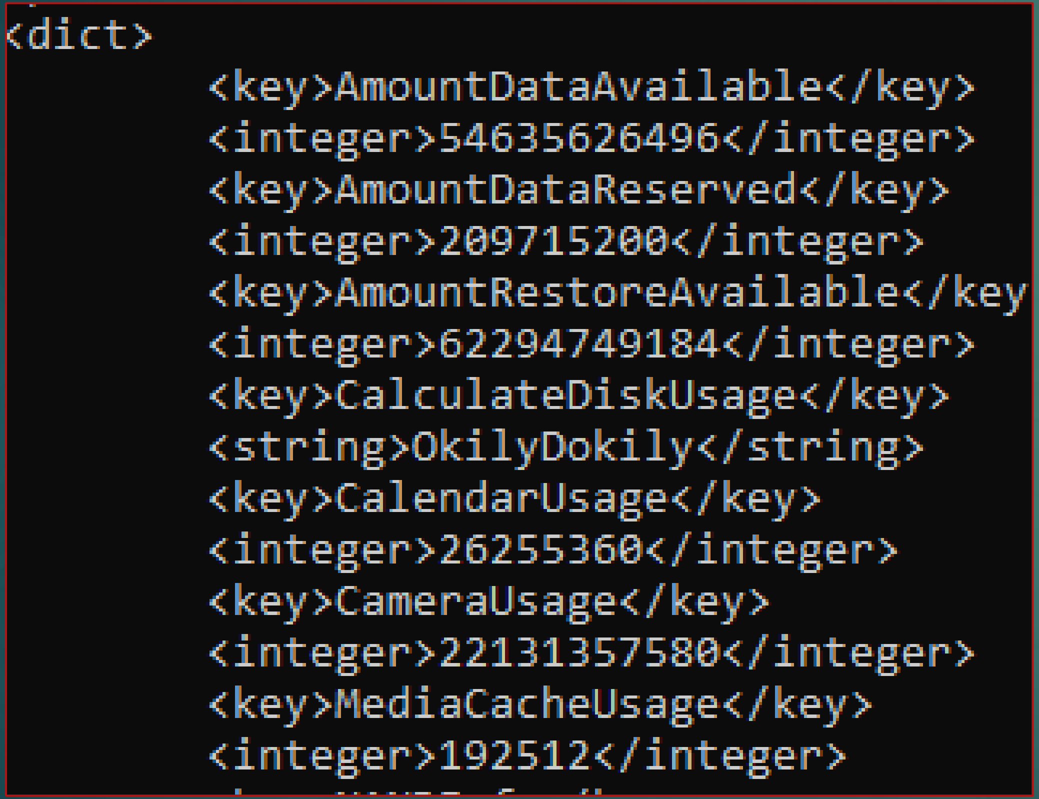
- On iOS devices there are **no native methods to interact with a "shell"**
- The best suite of tools to interact at a low-level is **Libimobiledevice**
- It includes various command line utilities that can be used to extract:
  - Device information
  - Disk usage
  - Battery information
  - Installed applications
  - Crash logs and sysdiagnose

idevicename
idevice_id –l
idevicedate

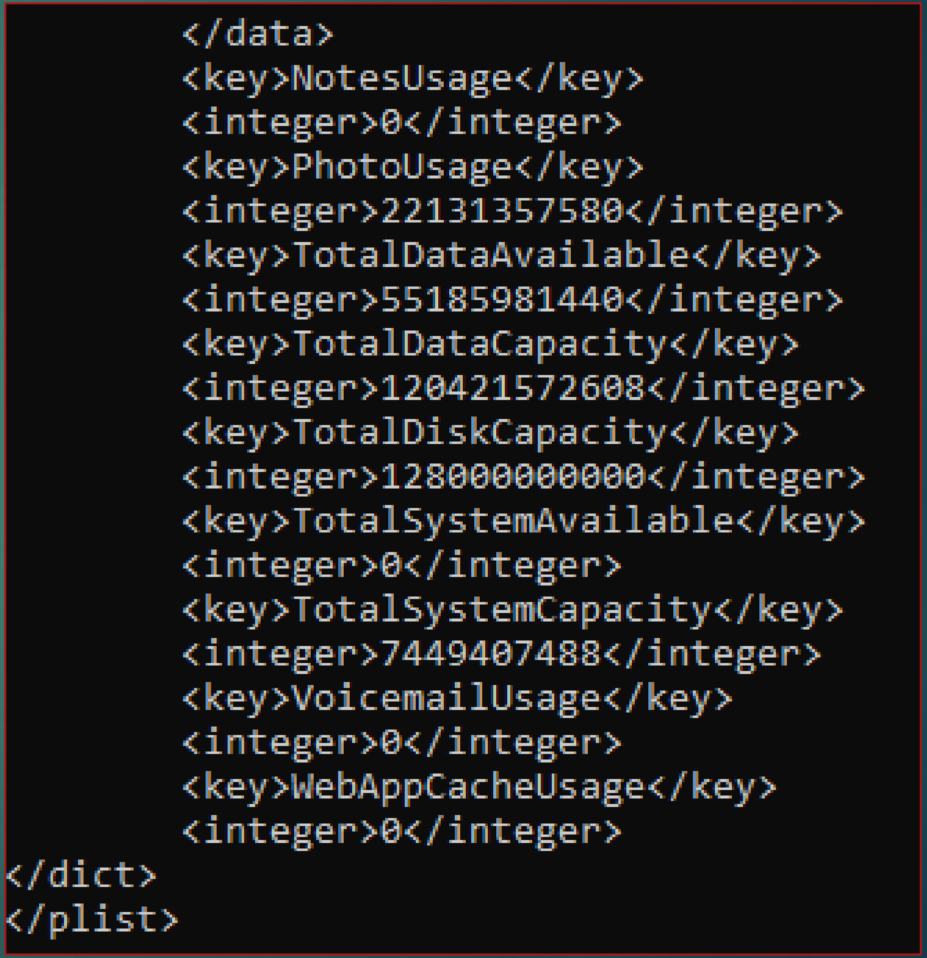


```
C:\ForensicTools\imobiledevice>idevicename
IPhone12

C:\ForensicTools\imobiledevice>idevice_id -l
00008101-00050C423E01001E

C:\ForensicTools\imobiledevice>idevicedate
Mon Jun  7 16:12:21 ora legale Europa occidentale 2021

C:\ForensicTools\imobiledevice>
```

ideviceinfo -q com.apple.disk_usage.factory -x

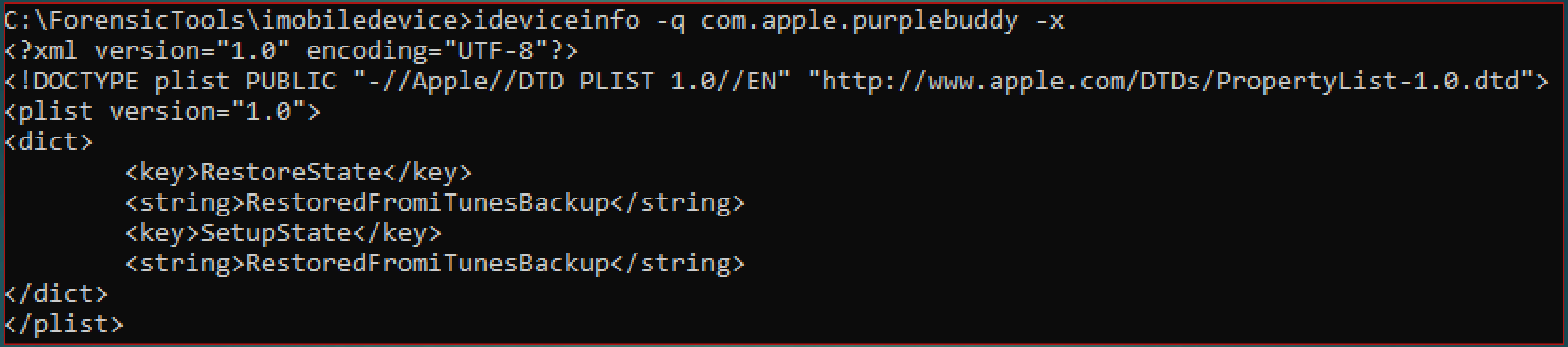


```
<dict>
        <key>AmountDataAvailable</key>
        <integer>54635626496</integer>
        <key>AmountDataReserved</key>
        <integer>209715200</integer>
        <key>AmountRestoreAvailable</key
        <integer>62294749184</integer>
        <key>CalculateDiskUsage</key>
        <string>OkilyDokily</string>
        <key>CalendarUsage</key>
        <integer>26255360</integer>
        <key>CameraUsage</key>
        <integer>22131357580</integer>
        <key>MediaCacheUsage</key>
        <integer>192512</integer>
```



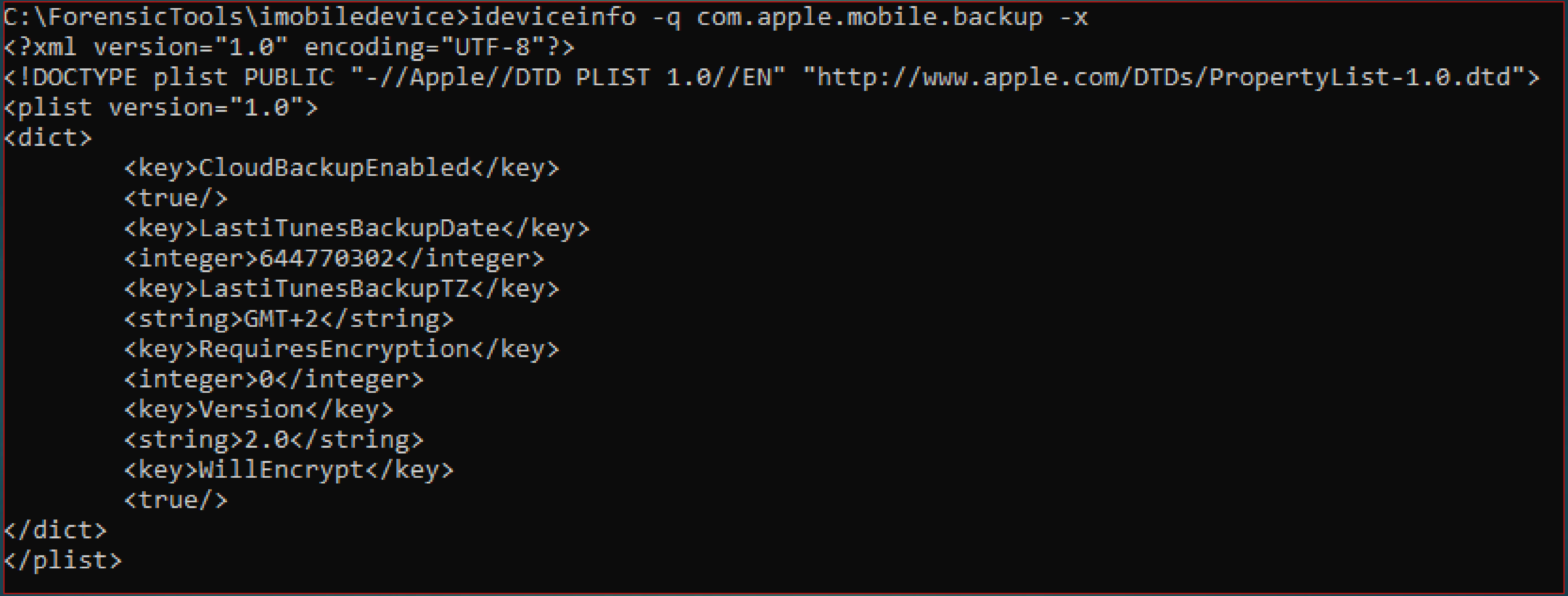
```
        </data>
        <key>NotesUsage</key>
        <integer>0</integer>
        <key>PhotoUsage</key>
        <integer>22131357580</integer>
        <key>TotalDataAvailable</key>
        <integer>55185981440</integer>
        <key>TotalDataCapacity</key>
        <integer>120421572608</integer>
        <key>TotalDiskCapacity</key>
        <integer>128000000000</integer>
        <key>TotalSystemAvailable</key>
        <integer>0</integer>
        <key>TotalSystemCapacity</key>
        <integer>7449407488</integer>
        <key>VoicemailUsage</key>
        <integer>0</integer>
        <key>WebAppCacheUsage</key>
        <integer>0</integer>
</dict>
</plist>
```

ideviceinfo -q com.apple.purplebuddy -x



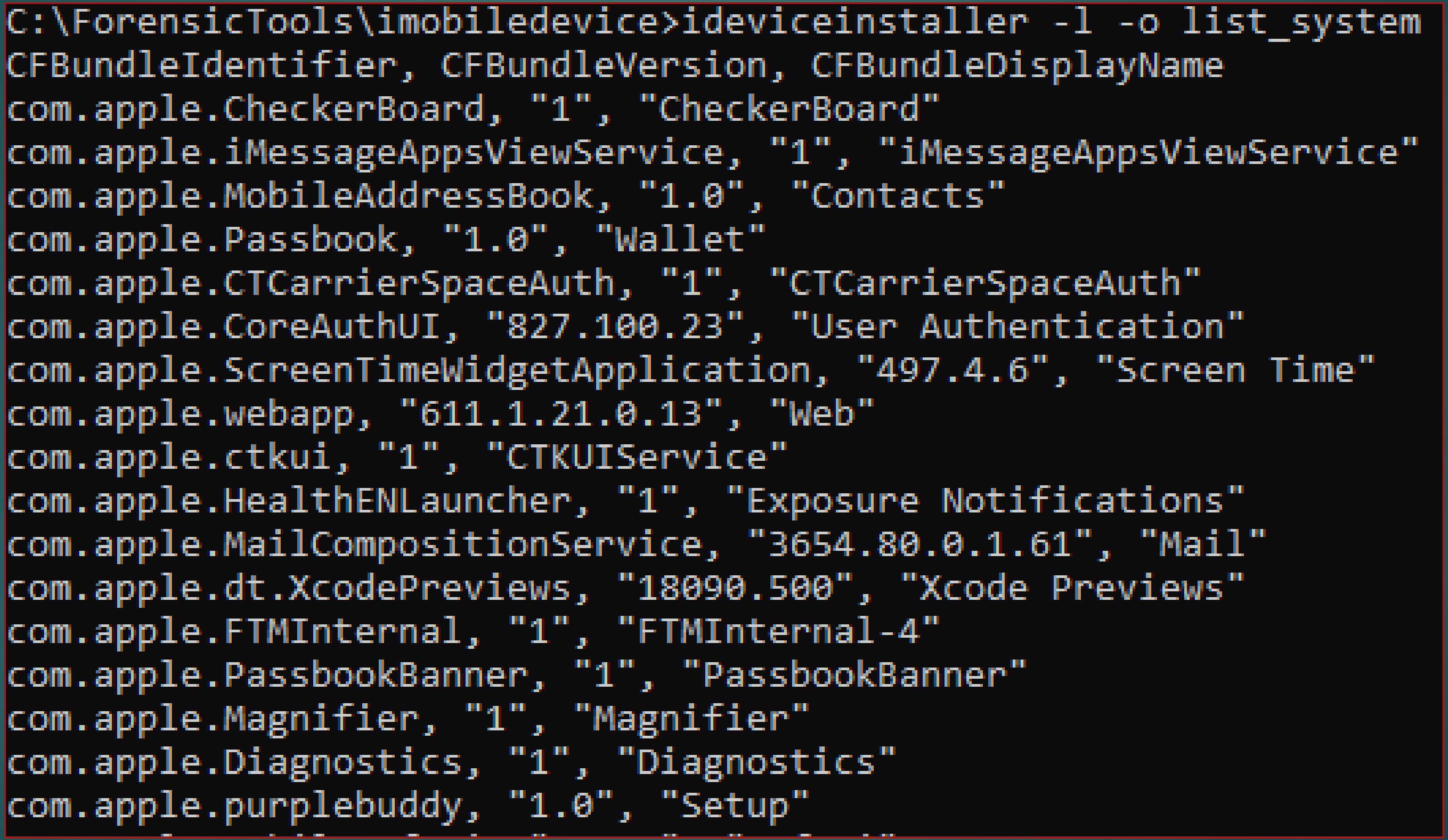
```
C:\ForensicTools\imobiledevice>ideviceinfo -q com.apple.purplebuddy -x
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>RestoreState</key>
        <string>RestoredFromiTunesBackup</string>
        <key>SetupState</key>
        <string>RestoredFromiTunesBackup</string>
</dict>
</plist>
```

ideviceinfo -q com.apple.mobile.backup -x



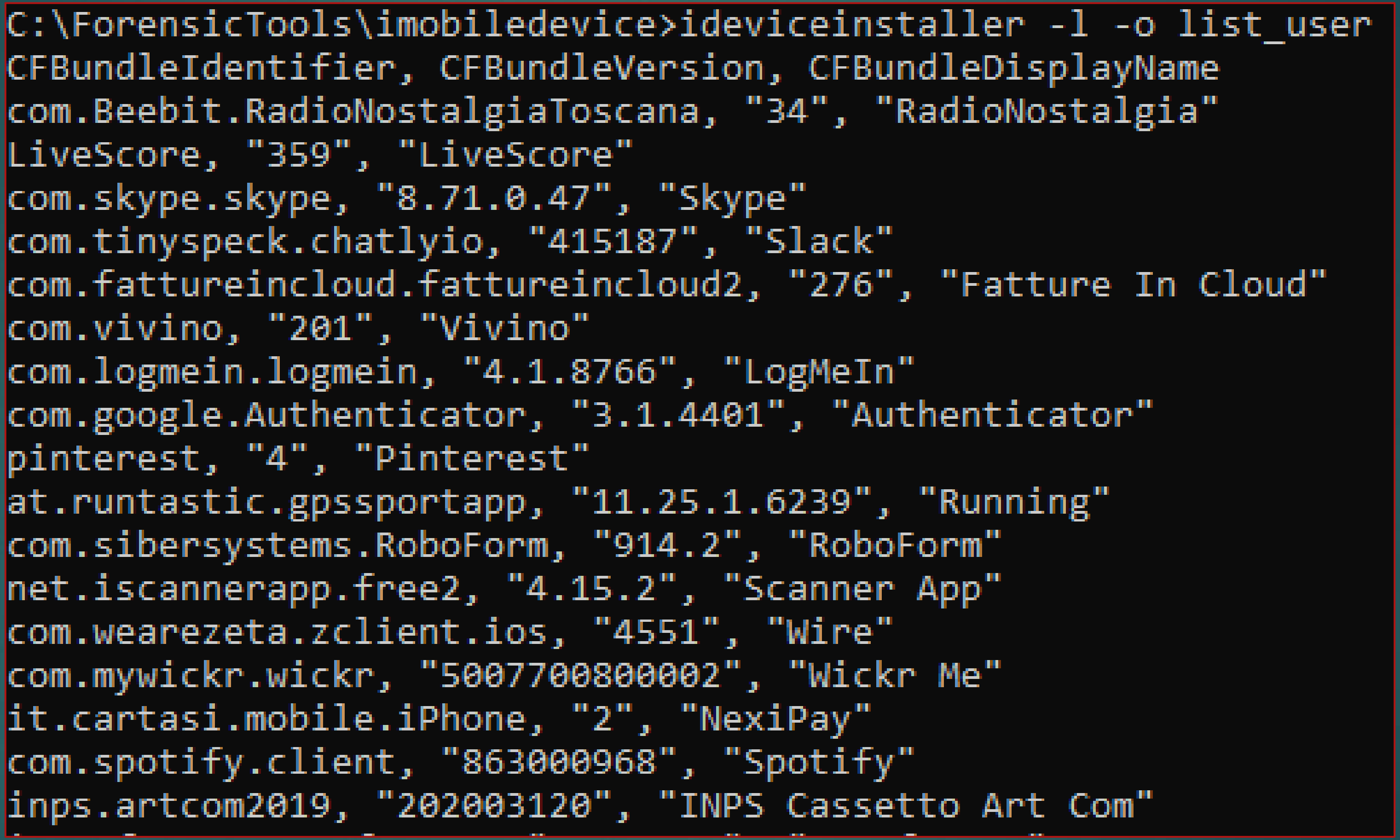
```
C:\ForensicTools\imobiledevice>ideviceinfo -q com.apple.mobile.backup -x
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>CloudBackupEnabled</key>
        <true/>
        <key>LastiTunesBackupDate</key>
        <integer>644770302</integer>
        <key>LastiTunesBackupTZ</key>
        <string>GMT+2</string>
        <key>RequiresEncryption</key>
        <integer>0</integer>
        <key>Version</key>
        <string>2.0</string>
        <key>WillEncrypt</key>
        <true/>
</dict>
</plist>
```

ideviceinstaller -l -o list_system



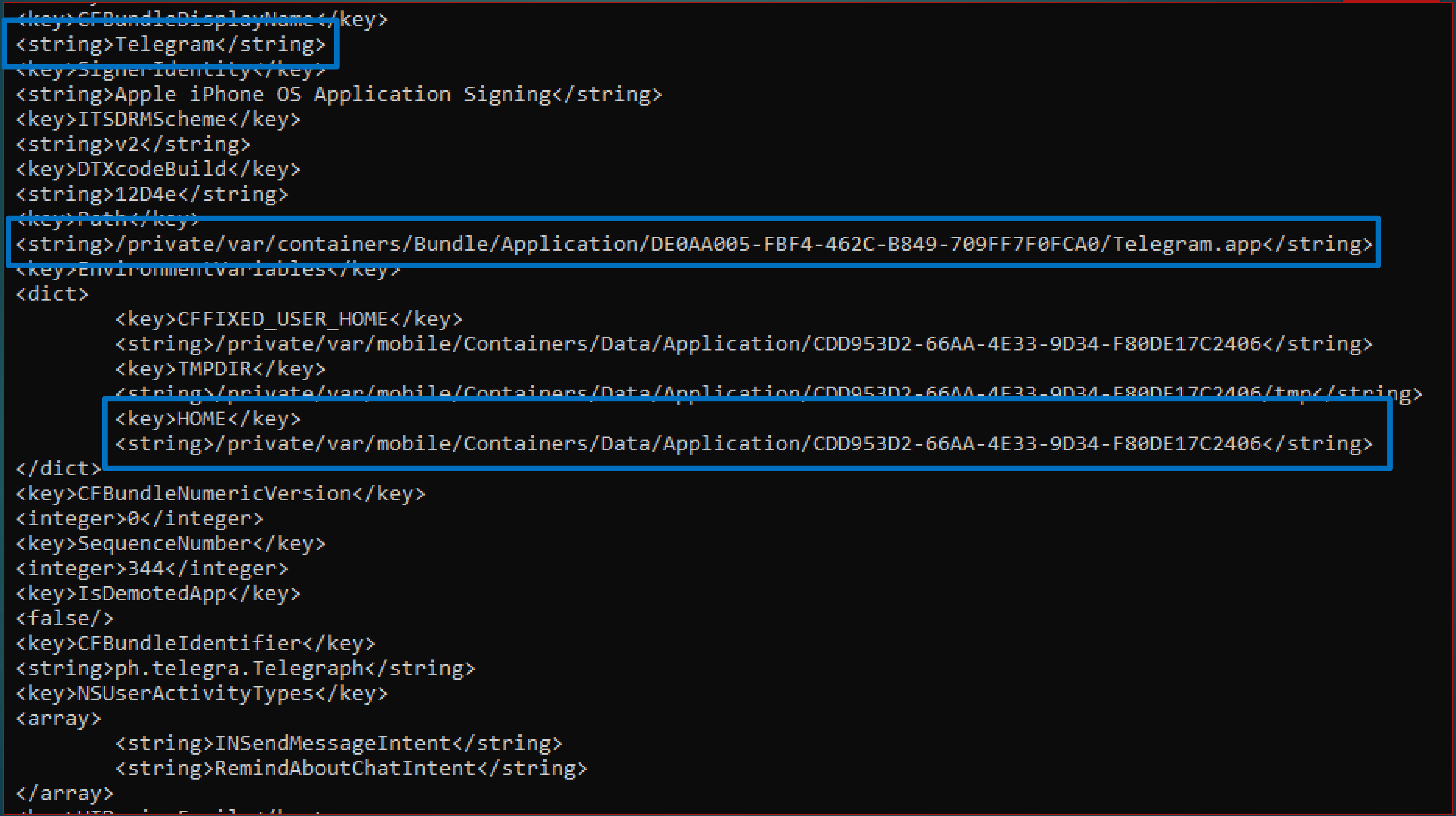
```
C:\ForensicTools\imobiledevice>ideviceinstaller -l -o list_system
CFBundleIdentifier, CFBundleVersion, CFBundleDisplayName
com.apple.CheckerBoard, "1", "CheckerBoard"
com.apple.iMessageAppsViewService, "1", "iMessageAppsViewService"
com.apple.MobileAddressBook, "1.0", "Contacts"
com.apple.Passbook, "1.0", "Wallet"
com.apple.CTCarrierSpaceAuth, "1", "CTCarrierSpaceAuth"
com.apple.CoreAuthUI, "827.100.23", "User Authentication"
com.apple.ScreenTimeWidgetApplication, "497.4.6", "Screen Time"
com.apple.webapp, "611.1.21.0.13", "Web"
com.apple.ctkui, "1", "CTKUIService"
com.apple.HealthENLauncher, "1", "Exposure Notifications"
com.apple.MailCompositionService, "3654.80.0.1.61", "Mail"
com.apple.dt.XcodePreviews, "18090.500", "Xcode Previews"
com.apple.FTMInternal, "1", "FTMInternal-4"
com.apple.PassbookBanner, "1", "PassbookBanner"
com.apple.Magnifier, "1", "Magnifier"
com.apple.Diagnostics, "1", "Diagnostics"
com.apple.purplebuddy, "1.0", "Setup"
```

ideviceinstaller -l -o list_user



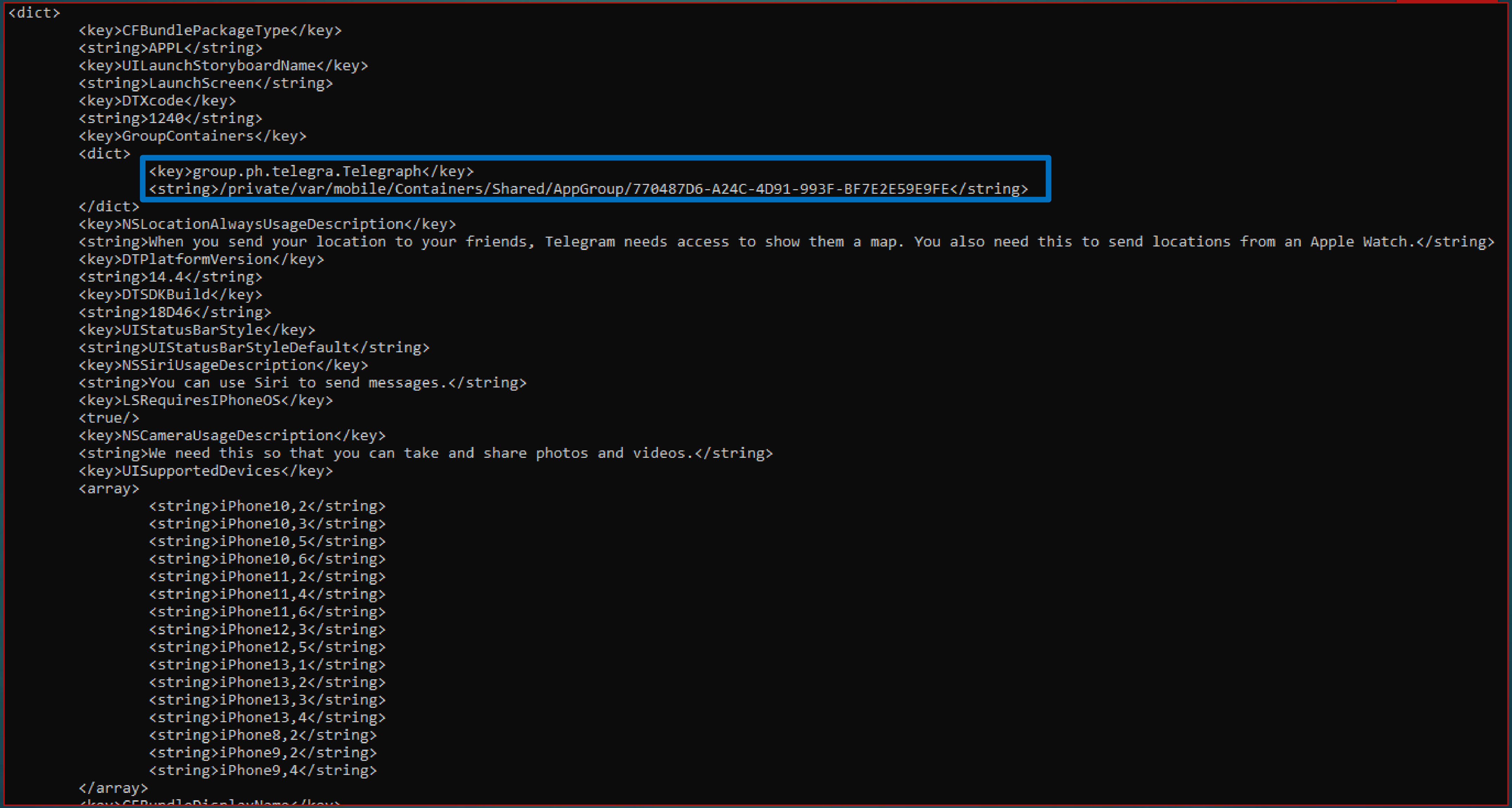
```
C:\ForensicTools\imobiledevice>ideviceinstaller -l -o list_user
CFBundleIdentifier, CFBundleVersion, CFBundleDisplayName
com.Beebit.RadioNostalgiaToscana, "34", "RadioNostalgia"
LiveScore, "359", "LiveScore"
com.skype.skype, "8.71.0.47", "Skype"
com.tinyspeck.chatlyio, "415187", "Slack"
com.fattureincloud.fattureincloud2, "276", "Fatture In Cloud"
com.vivino, "201", "Vivino"
com.logmein.logmein, "4.1.8766", "LogMeIn"
com.google.Authenticator, "3.1.4401", "Authenticator"
pinterest, "4", "Pinterest"
at.runtastic.gpssportapp, "11.25.1.6239", "Running"
com.sibersystems.RoboForm, "914.2", "RoboForm"
net.iscannerapp.free2, "4.15.2", "Scanner App"
com.wearezeta.zclient.ios, "4551", "Wire"
com.mywickr.wickr, "5007700800002", "Wickr Me"
it.cartasi.mobile.iPhone, "2", "NexiPay"
com.spotify.client, "863000968", "Spotify"
inps.artcom2019, "202003120", "INPS Cassetto Art Com"
```

ideviceinstaller -l -o xml



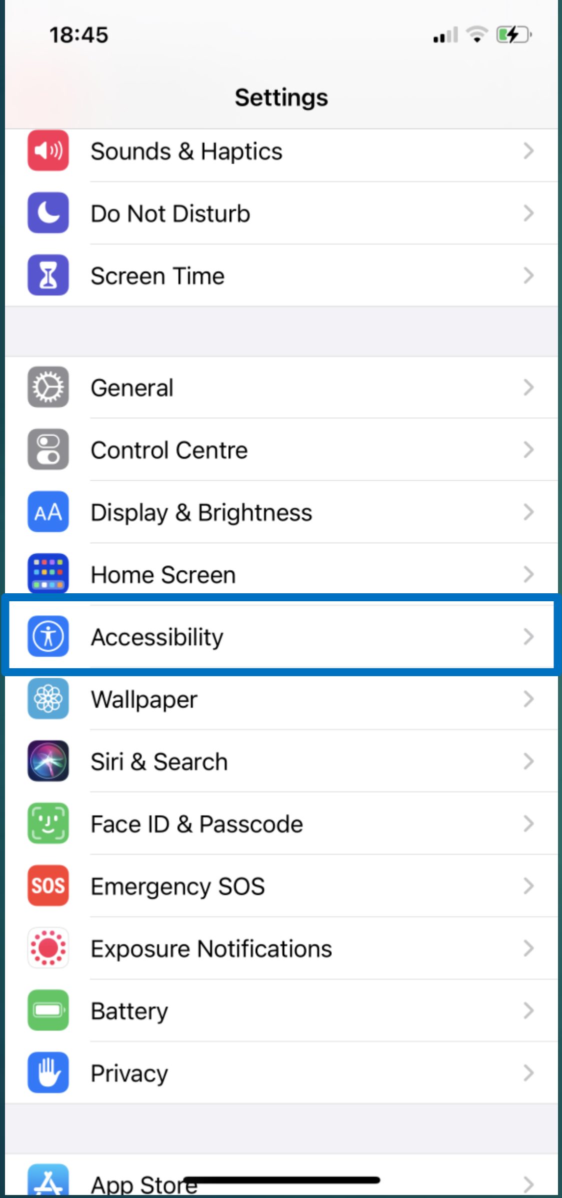
```
<key>CFBundleDisplayName</key>
<string>Telegram</string>
<key>SignerIdentity</key>
<string>Apple iPhone OS Application Signing</string>
<key>ITSDRMScheme</key>
<string>v2</string>
<key>DTXcodeBuild</key>
<string>12D4e</string>
<key>Path</key>
<string>/private/var/containers/Bundle/Application/DE0AA005-FBF4-462C-B849-709FF7F0FCA0/Telegram.app</string>
<key>EnvironmentVariables</key>
<dict>
        <key>CFFIXED_USER_HOME</key>
        <string>/private/var/mobile/Containers/Data/Application/CDD953D2-66AA-4E33-9D34-F80DE17C2406</string>
        <key>TMPDIR</key>
        <string>/private/var/mobile/Containers/Data/Application/CDD953D2-66AA-4E33-9D34-F80DE17C2406/tmp</string>
        <key>HOME</key>
        <string>/private/var/mobile/Containers/Data/Application/CDD953D2-66AA-4E33-9D34-F80DE17C2406</string>
</dict>
<key>CFBundleNumericVersion</key>
<integer>0</integer>
<key>SequenceNumber</key>
<integer>344</integer>
<key>IsDemotedApp</key>
<false/>
<key>CFBundleIdentifier</key>
<string>ph.telegra.Telegraph</string>
<key>NSUserActivityTypes</key>
<array>
        <string>INSendMessageIntent</string>
        <string>RemindAboutChatIntent</string>
</array>
```

ideviceinstaller -l -o xml



```
<dict>
        <key>CFBundlePackageType</key>
        <string>APPL</string>
        <key>UILaunchStoryboardName</key>
        <string>LaunchScreen</string>
        <key>DTXcode</key>
        <string>1240</string>
        <key>GroupContainers</key>
        <dict>
                <key>group.ph.telegra.Telegraph</key>
                <string>/private/var/mobile/Containers/Shared/AppGroup/770487D6-A24C-4D91-993F-BF7E2E59E9FE</string>
        </dict>
        <key>NSLocationAlwaysUsageDescription</key>
        <string>When you send your location to your friends, Telegram needs access to show them a map. You also need this to send locations from an Apple Watch.</string>
        <key>DTPlatformVersion</key>
        <string>14.4</string>
        <key>DTSDKBuild</key>
        <string>18D46</string>
        <key>UIStatusBarStyle</key>
        <string>UIStatusBarStyleDefault</string>
        <key>NSSiriUsageDescription</key>
        <string>You can use Siri to send messages.</string>
        <key>LSRequiresIPhoneOS</key>
        <true/>
        <key>NSCameraUsageDescription</key>
        <string>We need this so that you can take and share photos and videos.</string>
        <key>UISupportedDevices</key>
        <array>
                <string>iPhone10,2</string>
                <string>iPhone10,3</string>
                <string>iPhone10,5</string>
                <string>iPhone10,6</string>
                <string>iPhone11,2</string>
                <string>iPhone11,4</string>
                <string>iPhone11,6</string>
                <string>iPhone12,3</string>
                <string>iPhone12,5</string>
                <string>iPhone13,1</string>
                <string>iPhone13,2</string>
                <string>iPhone13,3</string>
                <string>iPhone13,4</string>
                <string>iPhone8,2</string>
                <string>iPhone9,2</string>
                <string>iPhone9,4</string>
        </array>
        <key>CFBundleDisplayName</key>
```

Generate a sysdiagnose



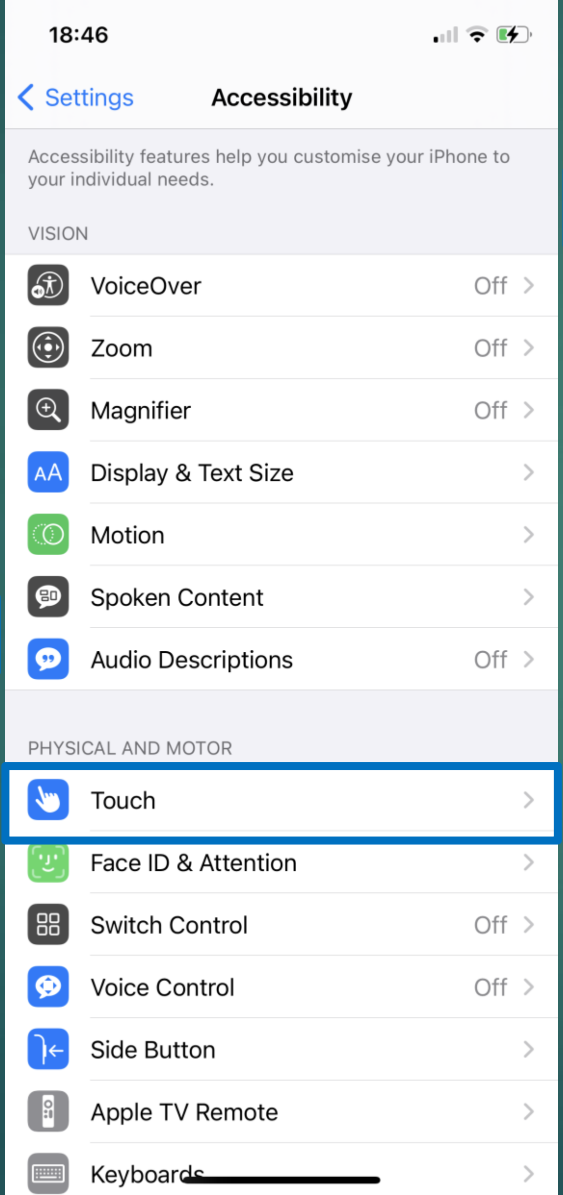
18:45

Settings

- Sounds & Haptics
- Do Not Disturb
- Screen Time

- General
- Control Centre
- Display & Brightness
- Home Screen
- Accessibility
- Wallpaper
- Siri & Search
- Face ID & Passcode
- Emergency SOS
- Exposure Notifications
- Battery
- Privacy

- App Store



18:46

< Settings **Accessibility**

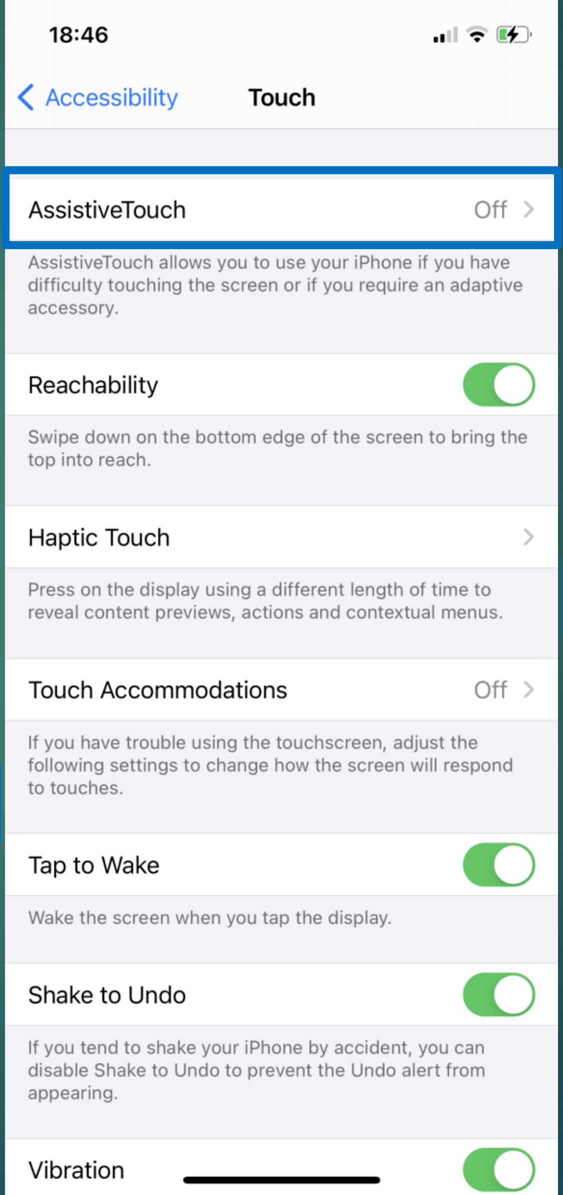
Accessibility features help you customise your iPhone to your individual needs.

VISION

- VoiceOver Off
- Zoom Off
- Magnifier Off
- Display & Text Size
- Motion
- Spoken Content
- Audio Descriptions Off

PHYSICAL AND MOTOR

- Touch
- Face ID & Attention
- Switch Control Off
- Voice Control Off
- Side Button
- Apple TV Remote
- Keyboards



18:46

< Accessibility **Touch**

AssistiveTouch Off

AssistiveTouch allows you to use your iPhone if you have difficulty touching the screen or if you require an adaptive accessory.

Reachability

Swipe down on the bottom edge of the screen to bring the top into reach.

Haptic Touch

Press on the display using a different length of time to reveal content previews, actions and contextual menus.

Touch Accommodations Off

If you have trouble using the touchscreen, adjust the following settings to change how the screen will respond to touches.

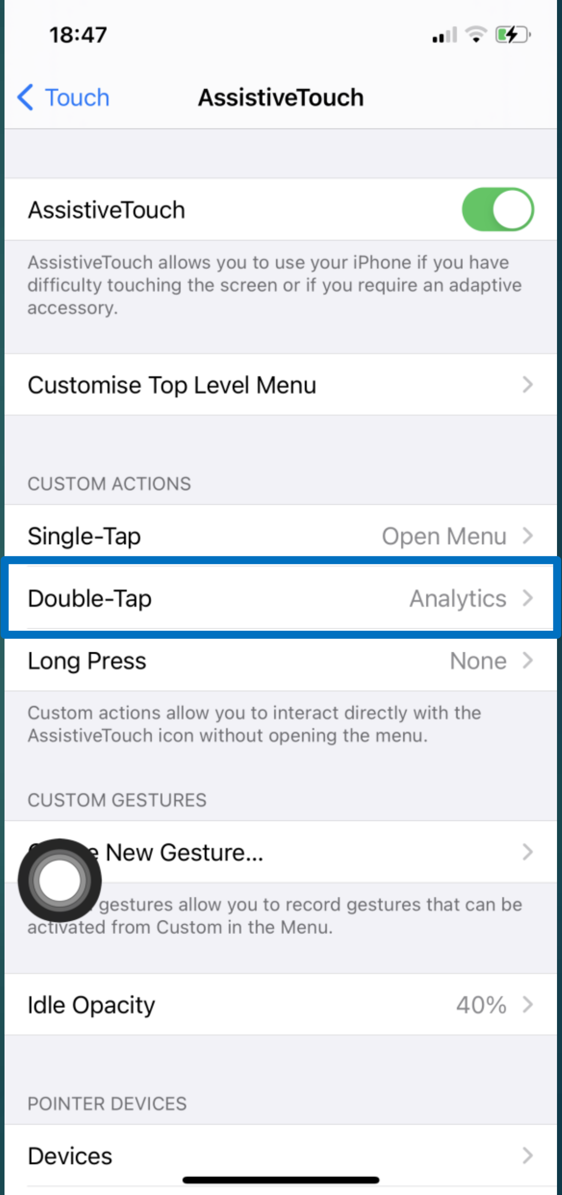
Tap to Wake

Wake the screen when you tap the display.

Shake to Undo

If you tend to shake your iPhone by accident, you can disable Shake to Undo to prevent the Undo alert from appearing.

Vibration



18:47

< Touch **AssistiveTouch**

AssistiveTouch

AssistiveTouch allows you to use your iPhone if you have difficulty touching the screen or if you require an adaptive accessory.

Customise Top Level Menu

CUSTOM ACTIONS

- Single-Tap Open Menu
- Double-Tap Analytics
- Long Press None

Custom actions allow you to interact directly with the AssistiveTouch icon without opening the menu.

CUSTOM GESTURES

e New Gesture...

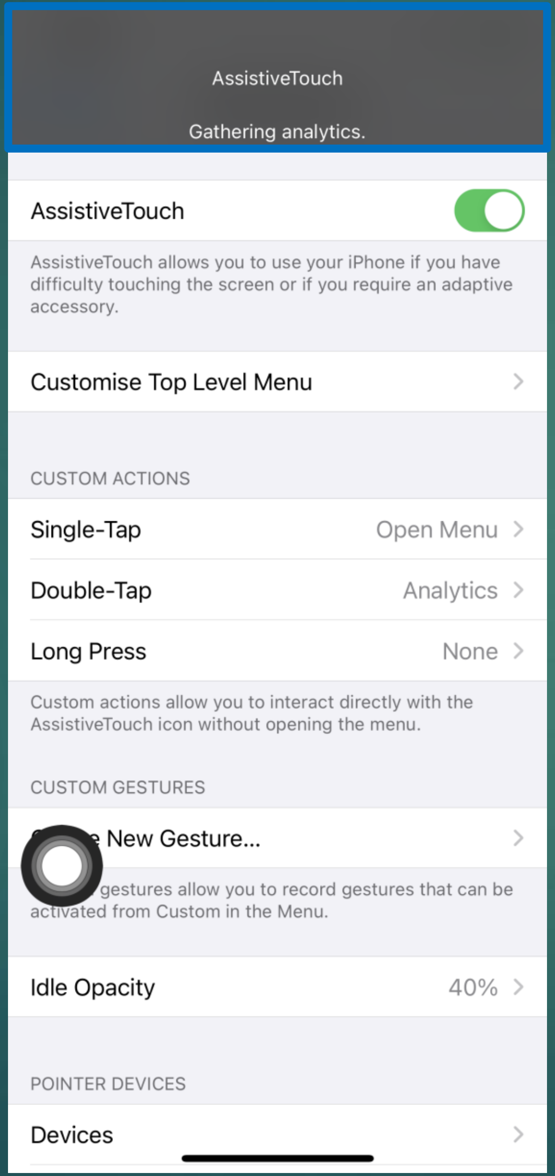
gestures allow you to record gestures that can be activated from Custom in the Menu.

Idle Opacity 40%

POINTER DEVICES

Devices

Generate a sysdiagnose



AssistiveTouch

Gathering analytics.

AssistiveTouch

AssistiveTouch allows you to use your iPhone if you have difficulty touching the screen or if you require an adaptive accessory.

Customise Top Level Menu

CUSTOM ACTIONS

Single-Tap Open Menu

Double-Tap Analytics

Long Press None

Custom actions allow you to interact directly with the AssistiveTouch icon without opening the menu.

CUSTOM GESTURES

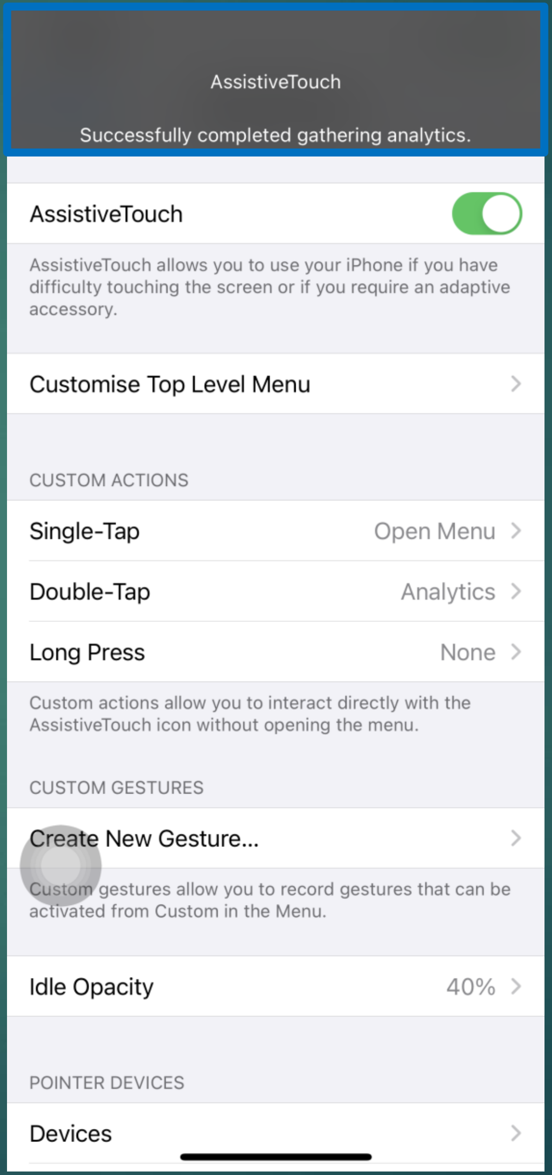
e New Gesture...

gestures allow you to record gestures that can be activated from Custom in the Menu.

Idle Opacity 40%

POINTER DEVICES

Devices



AssistiveTouch

Successfully completed gathering analytics.

AssistiveTouch

AssistiveTouch allows you to use your iPhone if you have difficulty touching the screen or if you require an adaptive accessory.

Customise Top Level Menu

CUSTOM ACTIONS

Single-Tap Open Menu

Double-Tap Analytics

Long Press None

Custom actions allow you to interact directly with the AssistiveTouch icon without opening the menu.

CUSTOM GESTURES

Create New Gesture...

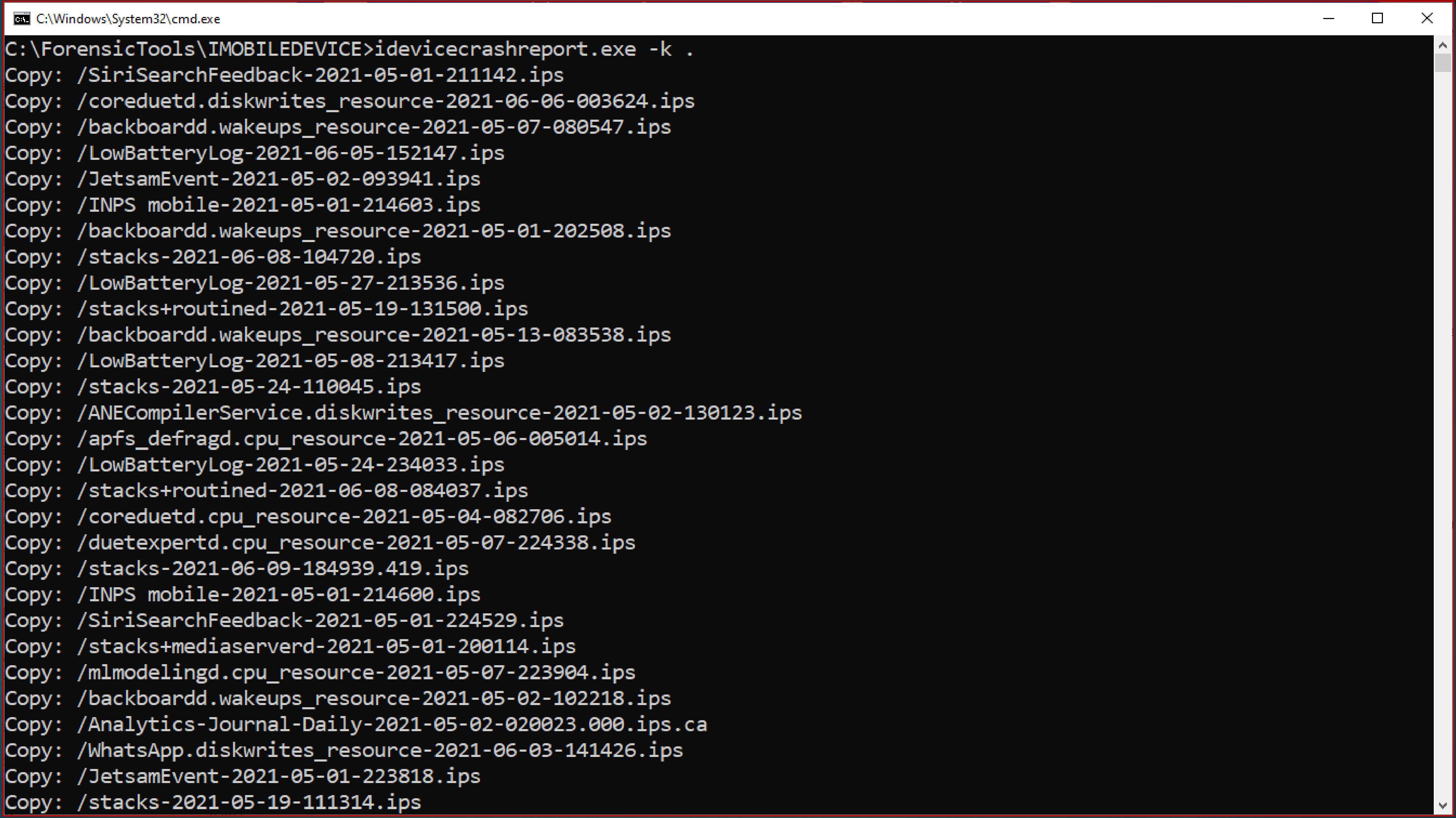
Custom gestures allow you to record gestures that can be activated from Custom in the Menu.

Idle Opacity 40%

POINTER DEVICES

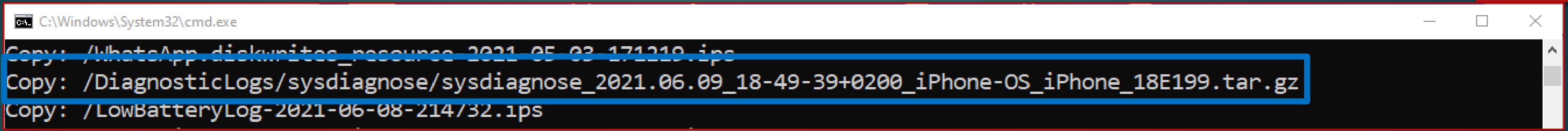
Devices

idevicecrashreport -k

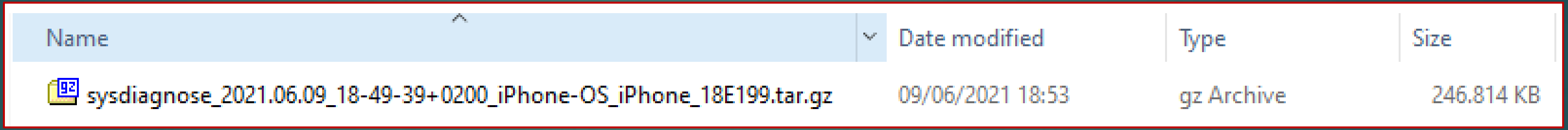


```
C:\ForensicTools\IMOBILEDEVICE>idevicecrashreport.exe -k .
Copy: /SiriSearchFeedback-2021-05-01-211142.ips
Copy: /coreduetd.diskwrites_resource-2021-06-06-003624.ips
Copy: /backboardd.wakeups_resource-2021-05-07-080547.ips
Copy: /LowBatteryLog-2021-06-05-152147.ips
Copy: /JetsamEvent-2021-05-02-093941.ips
Copy: /INPS mobile-2021-05-01-214603.ips
Copy: /backboardd.wakeups_resource-2021-05-01-202508.ips
Copy: /stacks-2021-06-08-104720.ips
Copy: /LowBatteryLog-2021-05-27-213536.ips
Copy: /stacks+routined-2021-05-19-131500.ips
Copy: /backboardd.wakeups_resource-2021-05-13-083538.ips
Copy: /LowBatteryLog-2021-05-08-213417.ips
Copy: /stacks-2021-05-24-110045.ips
Copy: /ANECompilerService.diskwrites_resource-2021-05-02-130123.ips
Copy: /apfs_defragd.cpu_resource-2021-05-06-005014.ips
Copy: /LowBatteryLog-2021-05-24-234033.ips
Copy: /stacks+routined-2021-06-08-084037.ips
Copy: /coreduetd.cpu_resource-2021-05-04-082706.ips
Copy: /duetexpertd.cpu_resource-2021-05-07-224338.ips
Copy: /stacks-2021-06-09-184939.419.ips
Copy: /INPS mobile-2021-05-01-214600.ips
Copy: /SiriSearchFeedback-2021-05-01-224529.ips
Copy: /stacks+mediaserverd-2021-05-01-200114.ips
Copy: /mlmodelingd.cpu_resource-2021-05-07-223904.ips
Copy: /backboardd.wakeups_resource-2021-05-02-102218.ips
Copy: /Analytics-Journal-Daily-2021-05-02-020023.000.ips.ca
Copy: /WhatsApp.diskwrites_resource-2021-06-03-141426.ips
Copy: /JetsamEvent-2021-05-01-223818.ips
Copy: /stacks-2021-05-19-111314.ips
```

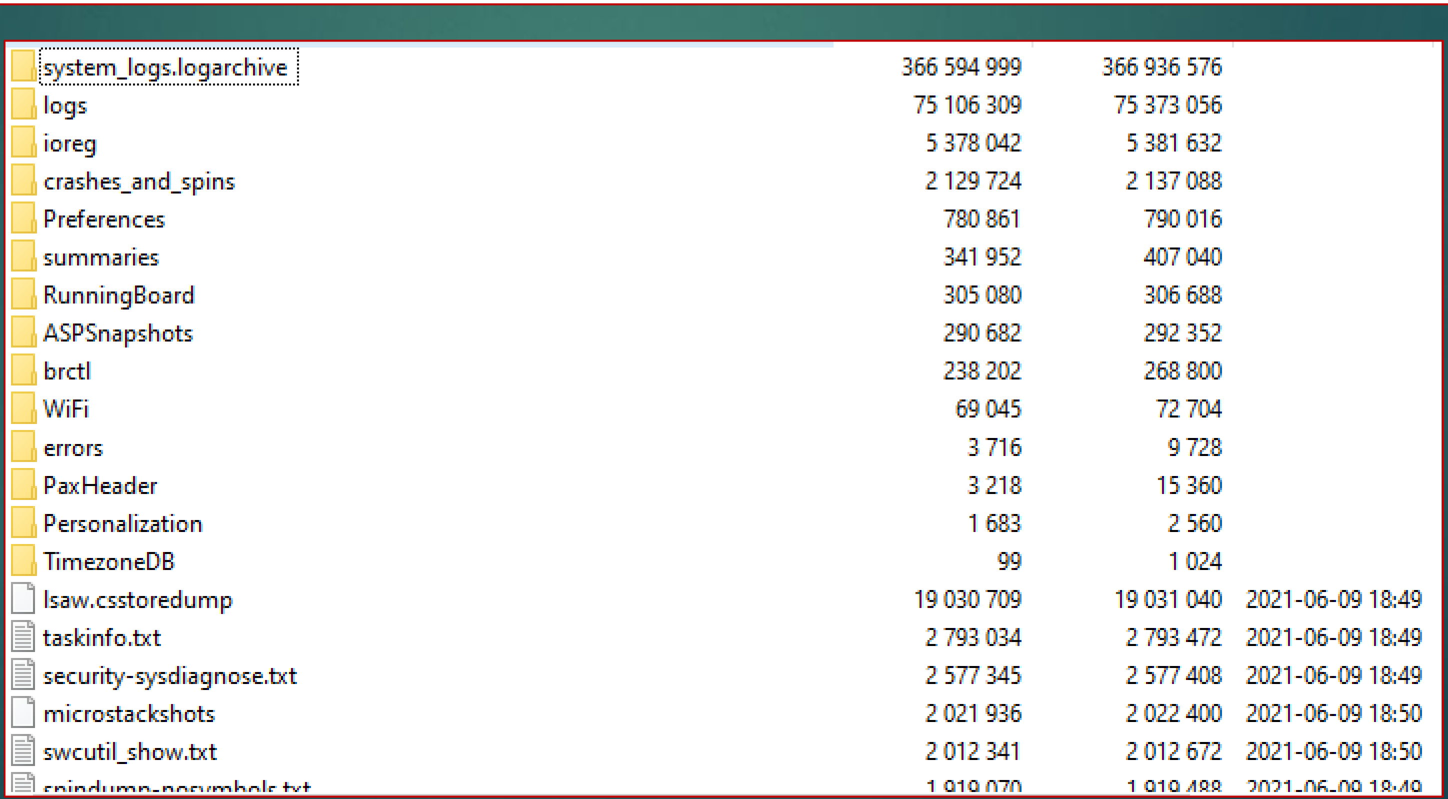
Sysdiagnose



```
Copy: /WhatsApp.diskwrites_resource-2021-05-03-171219.ips
Copy: /DiagnosticLogs/sysdiagnose/sysdiagnose_2021.06.09_18-49-39+0200_iPhone-OS_iPhone_18E199.tar.gz
Copy: /LowBatteryLog-2021-06-08-214732.ips
```



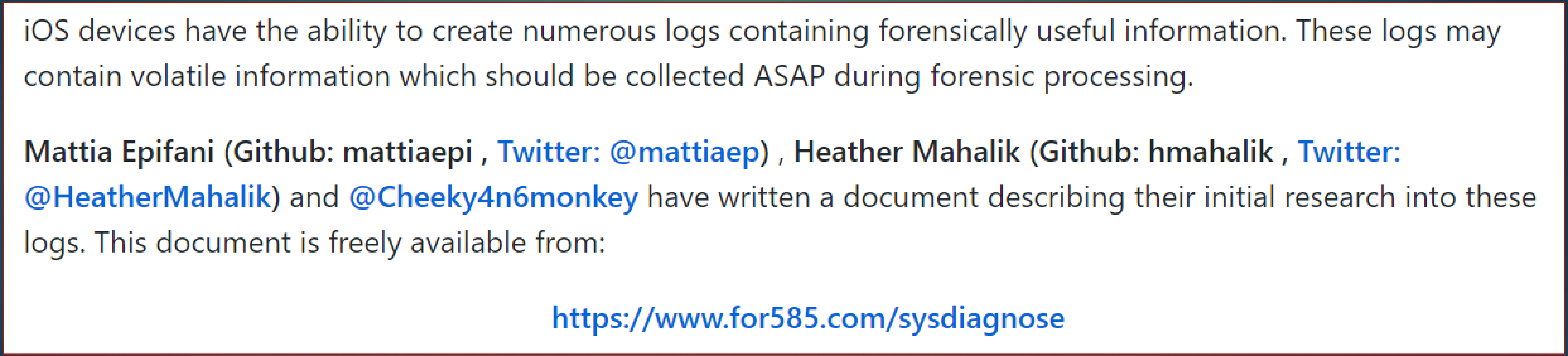
Name	Date modified	Type	Size
sysdiagnose_2021.06.09_18-49-39+0200_iPhone-OS_iPhone_18E199.tar.gz	09/06/2021 18:53	gz Archive	246.814 KB



system_logs.logarchive	366 594 999	366 936 576	
logs	75 106 309	75 373 056	
ioreg	5 378 042	5 381 632	
crashes_and_spins	2 129 724	2 137 088	
Preferences	780 861	790 016	
summaries	341 952	407 040	
RunningBoard	305 080	306 688	
ASPSnapshots	290 682	292 352	
brctl	238 202	268 800	
WiFi	69 045	72 704	
errors	3 716	9 728	
PaxHeader	3 218	15 360	
Personalization	1 683	2 560	
TimezoneDB	99	1 024	
lsaw.csstoredump	19 030 709	19 031 040	2021-06-09 18:49
taskinfo.txt	2 793 034	2 793 472	2021-06-09 18:49
security-sysdiagnose.txt	2 577 345	2 577 408	2021-06-09 18:49
microstackshots	2 021 936	2 022 400	2021-06-09 18:50
swcutil_show.txt	2 012 341	2 012 672	2021-06-09 18:50
spindump-nosymbols.txt	1 919 070	1 919 488	2021-06-09 18:49

iOS Sysdiagnose references

https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts

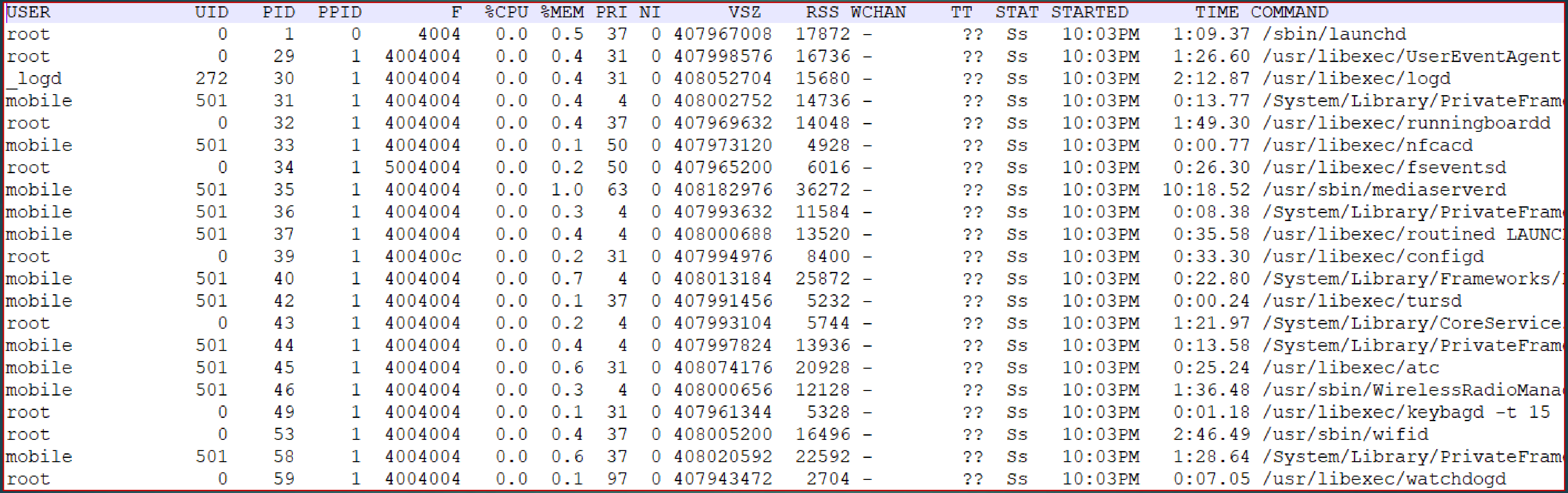


iOS devices have the ability to create numerous logs containing forensically useful information. These logs may contain volatile information which should be collected ASAP during forensic processing.

Mattia Epifani (Github: mattiaepi , Twitter: @mattiaep) , **Heather Mahalik (Github: hmahalik ,** Twitter: @HeatherMahalik) and @Cheeky4n6monkey have written a document describing their initial research into these logs. This document is freely available from:

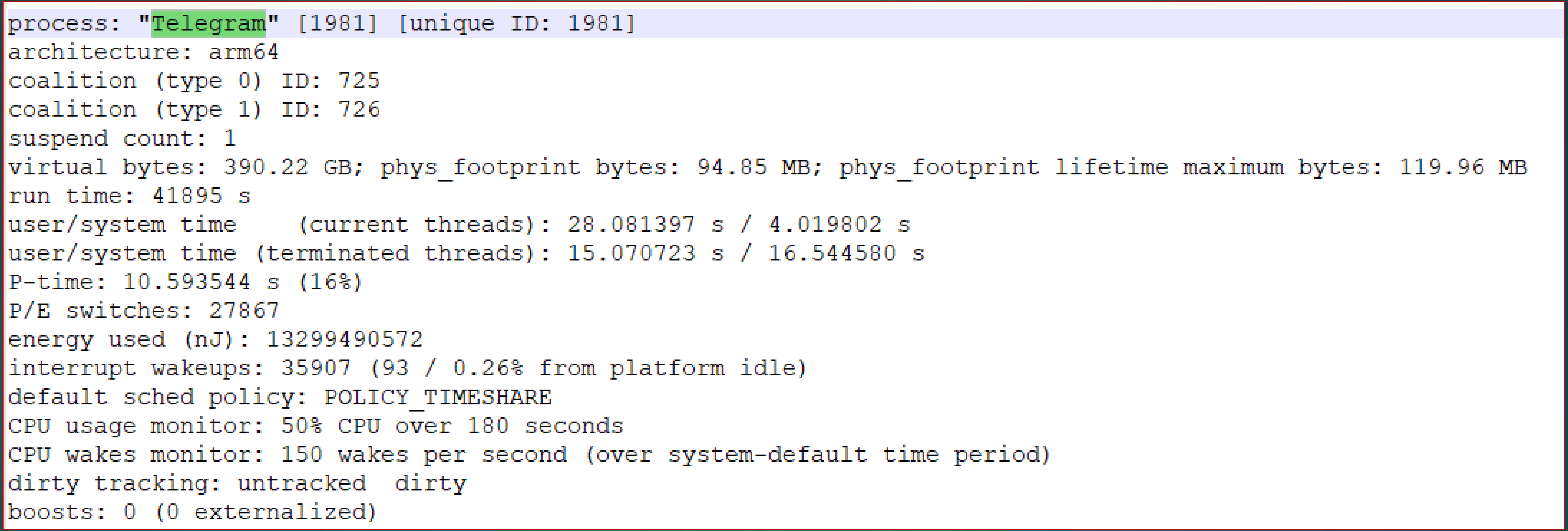
https://www.for585.com/sysdiagnose

ps.txt



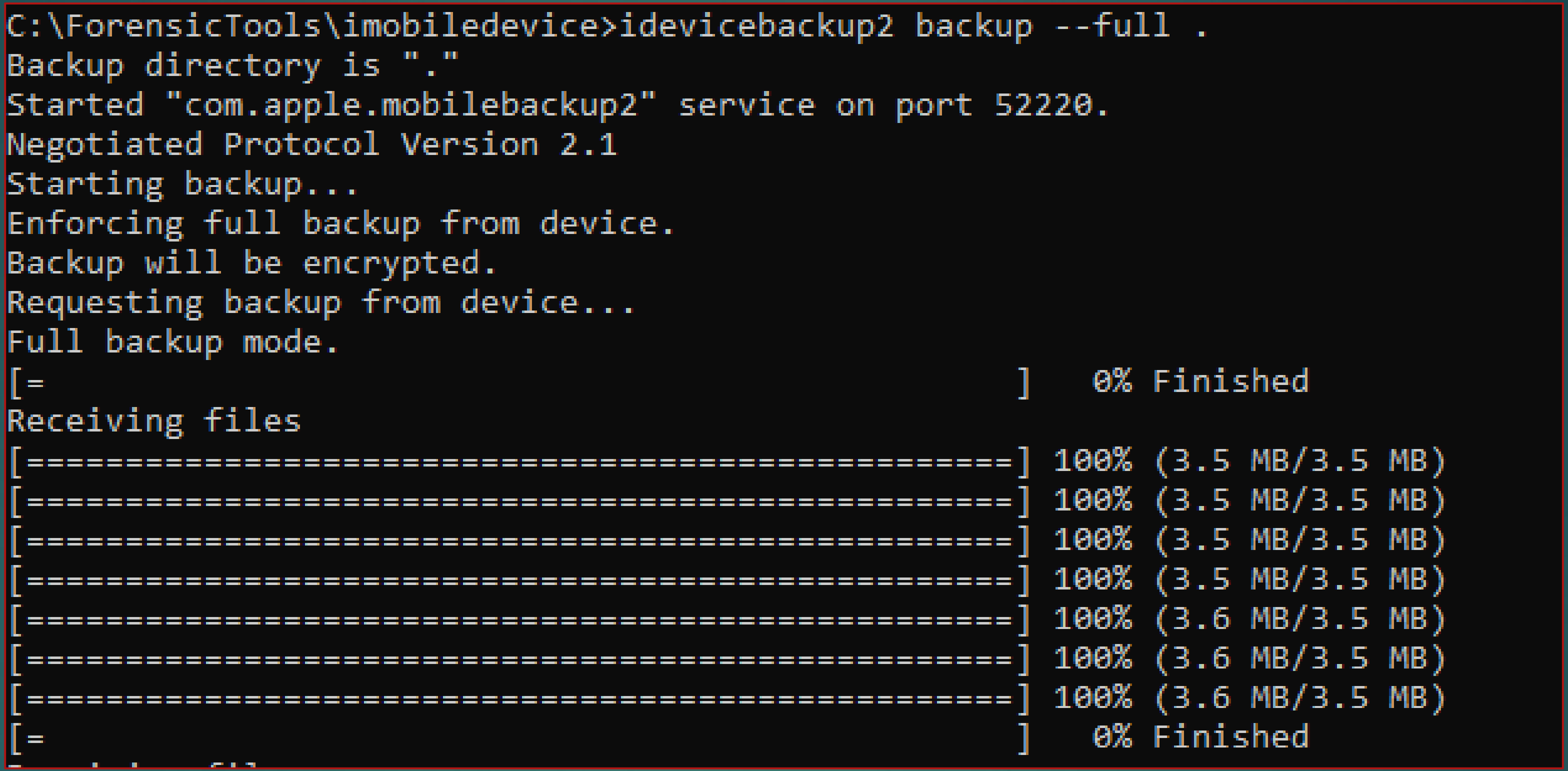
```
USER             UID   PID  PPID         F  %CPU %MEM PRI NI       VSZ    RSS WCHAN     TT  STAT STARTED       TIME COMMAND
root               0     1     0      4004   0.0  0.5  37  0 407967008  17872 -         ??  Ss    10:03PM   1:09.37 /sbin/launchd
root               0    29     1   4004004   0.0  0.4  31  0 407998576  16736 -         ??  Ss    10:03PM   1:26.60 /usr/libexec/UserEventAgent
_logd            272    30     1   4004004   0.0  0.4  31  0 408052704  15680 -         ??  Ss    10:03PM   2:12.87 /usr/libexec/logd
mobile           501    31     1   4004004   0.0  0.4   4  0 408002752  14736 -         ??  Ss    10:03PM   0:13.77 /System/Library/PrivateFram
root               0    32     1   4004004   0.0  0.4  37  0 407969632  14048 -         ??  Ss    10:03PM   1:49.30 /usr/libexec/runningboardd
mobile           501    33     1   4004004   0.0  0.1  50  0 407973120   4928 -         ??  Ss    10:03PM   0:00.77 /usr/libexec/nfcacd
root               0    34     1   5004004   0.0  0.2  50  0 407965200   6016 -         ??  Ss    10:03PM   0:26.30 /usr/libexec/fseventsd
mobile           501    35     1   4004004   0.0  1.0  63  0 408182976  36272 -         ??  Ss    10:03PM  10:18.52 /usr/sbin/mediaserverd
mobile           501    36     1   4004004   0.0  0.3   4  0 407993632  11584 -         ??  Ss    10:03PM   0:08.38 /System/Library/PrivateFram
mobile           501    37     1   4004004   0.0  0.4   4  0 408000688  13520 -         ??  Ss    10:03PM   0:35.58 /usr/libexec/routined LAUNC
root               0    39     1   400400c   0.0  0.2  31  0 407994976   8400 -         ??  Ss    10:03PM   0:33.30 /usr/libexec/configd
mobile           501    40     1   4004004   0.0  0.7   4  0 408013184  25872 -         ??  Ss    10:03PM   0:22.80 /System/Library/Frameworks/
mobile           501    42     1   4004004   0.0  0.1  37  0 407991456   5232 -         ??  Ss    10:03PM   0:00.24 /usr/libexec/tursd
root               0    43     1   4004004   0.0  0.2   4  0 407993104   5744 -         ??  Ss    10:03PM   1:21.97 /System/Library/CoreService
mobile           501    44     1   4004004   0.0  0.4   4  0 407997824  13936 -         ??  Ss    10:03PM   0:13.58 /System/Library/PrivateFram
mobile           501    45     1   4004004   0.0  0.6  31  0 408074176  20928 -         ??  Ss    10:03PM   0:25.24 /usr/libexec/atc
mobile           501    46     1   4004004   0.0  0.3   4  0 408000656  12128 -         ??  Ss    10:03PM   1:36.48 /usr/sbin/WirelessRadioMana
root               0    49     1   4004004   0.0  0.1  31  0 407961344   5328 -         ??  Ss    10:03PM   0:01.18 /usr/libexec/keybagd -t 15
root               0    53     1   4004004   0.0  0.4  37  0 408005200  16496 -         ??  Ss    10:03PM   2:46.49 /usr/sbin/wifid
mobile           501    58     1   4004004   0.0  0.6  37  0 408020592  22592 -         ??  Ss    10:03PM   1:28.64 /System/Library/PrivateFram
root               0    59     1   4004004   0.0  0.1  97  0 407943472   2704 -         ??  Ss    10:03PM   0:07.05 /usr/libexec/watchdogd
```

taskinfo.txt

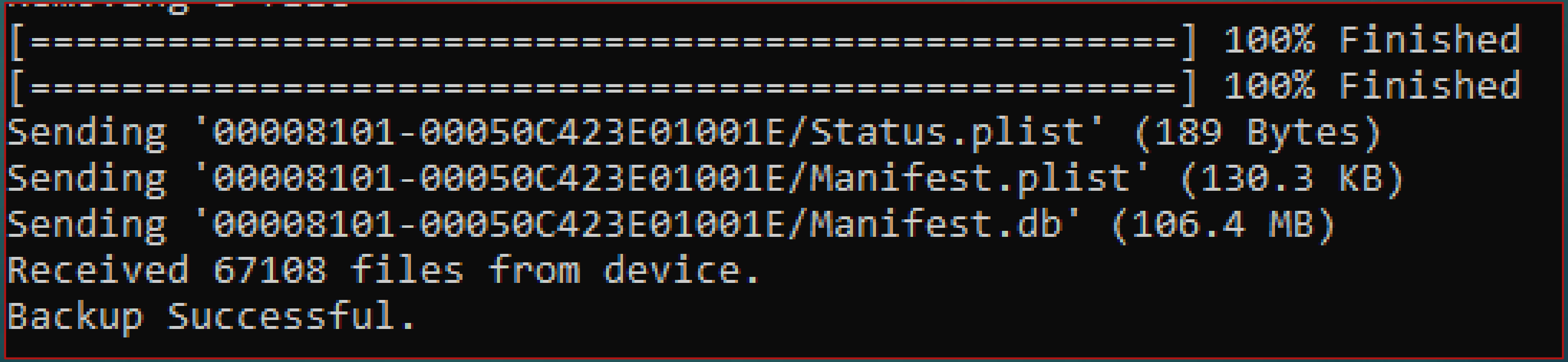


```
process: "Telegram" [1981] [unique ID: 1981]
architecture: arm64
coalition (type 0) ID: 725
coalition (type 1) ID: 726
suspend count: 1
virtual bytes: 390.22 GB; phys_footprint bytes: 94.85 MB; phys_footprint lifetime maximum bytes: 119.96 MB
run time: 41895 s
user/system time    (current threads): 28.081397 s / 4.019802 s
user/system time (terminated threads): 15.070723 s / 16.544580 s
P-time: 10.593544 s (16%)
P/E switches: 27867
energy used (nJ): 13299490572
interrupt wakeups: 35907 (93 / 0.26% from platform idle)
default sched policy: POLICY_TIMESHARE
CPU usage monitor: 50% CPU over 180 seconds
CPU wakes monitor: 150 wakes per second (over system-default time period)
dirty tracking: untracked  dirty
boosts: 0 (0 externalized)
```

idevicebackup2 backup –full .



```
C:\ForensicTools\imobiledevice>idevicebackup2 backup --full .
Backup directory is "."
Started "com.apple.mobilebackup2" service on port 52220.
Negotiated Protocol Version 2.1
Starting backup...
Enforcing full backup from device.
Backup will be encrypted.
Requesting backup from device...
Full backup mode.
[=                                                 ]   0% Finished
Receiving files
[==================================================] 100% (3.5 MB/3.5 MB)
[==================================================] 100% (3.5 MB/3.5 MB)
[==================================================] 100% (3.5 MB/3.5 MB)
[==================================================] 100% (3.5 MB/3.5 MB)
[==================================================] 100% (3.6 MB/3.5 MB)
[==================================================] 100% (3.6 MB/3.5 MB)
[==================================================] 100% (3.6 MB/3.5 MB)
[=                                                 ]   0% Finished
```



```
[==================================================] 100% Finished
[==================================================] 100% Finished
Sending '00008101-00050C423E01001E/Status.plist' (189 Bytes)
Sending '00008101-00050C423E01001E/Manifest.plist' (130.3 KB)
Sending '00008101-00050C423E01001E/Manifest.db' (106.4 MB)
Received 67108 files from device.
Backup Successful.
```

CONTACTS

Mattia Epifani

mattia.epifani@realitynet.it

@mattiaep