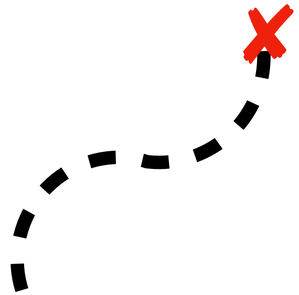
Unraveling Time

Understanding Time Formats in iOS sysdiagnose for Security Forensics

Lina Wilske

Importance of time in sysdiagnose

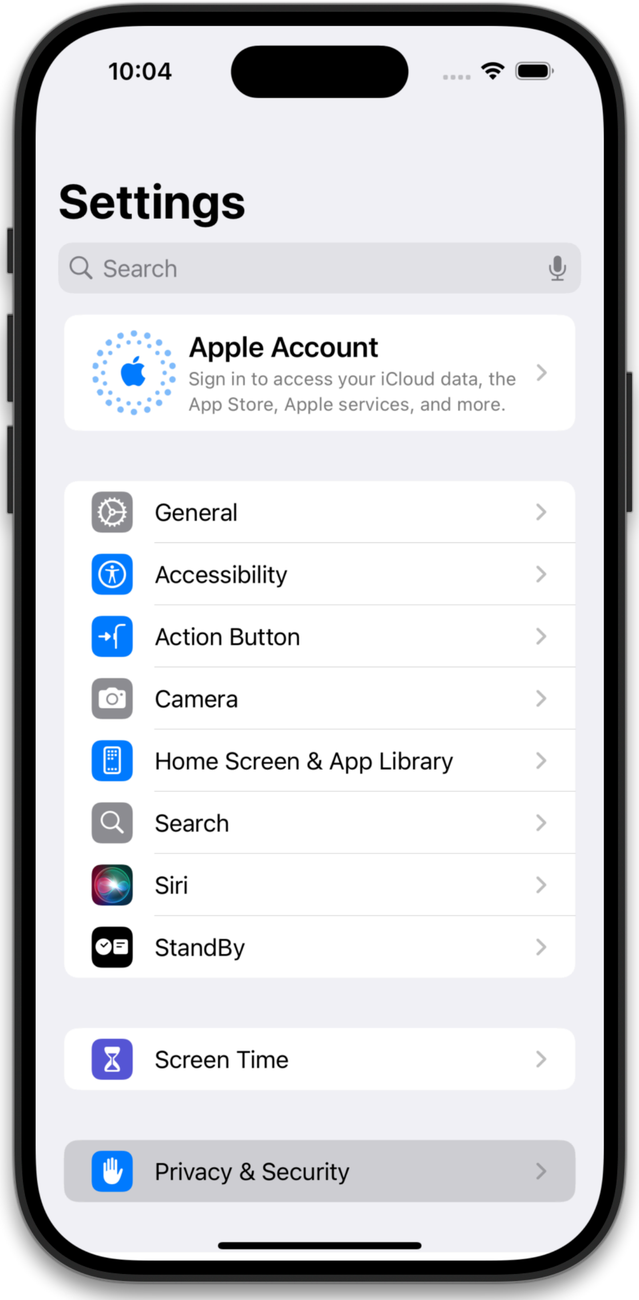
Investigate incidents

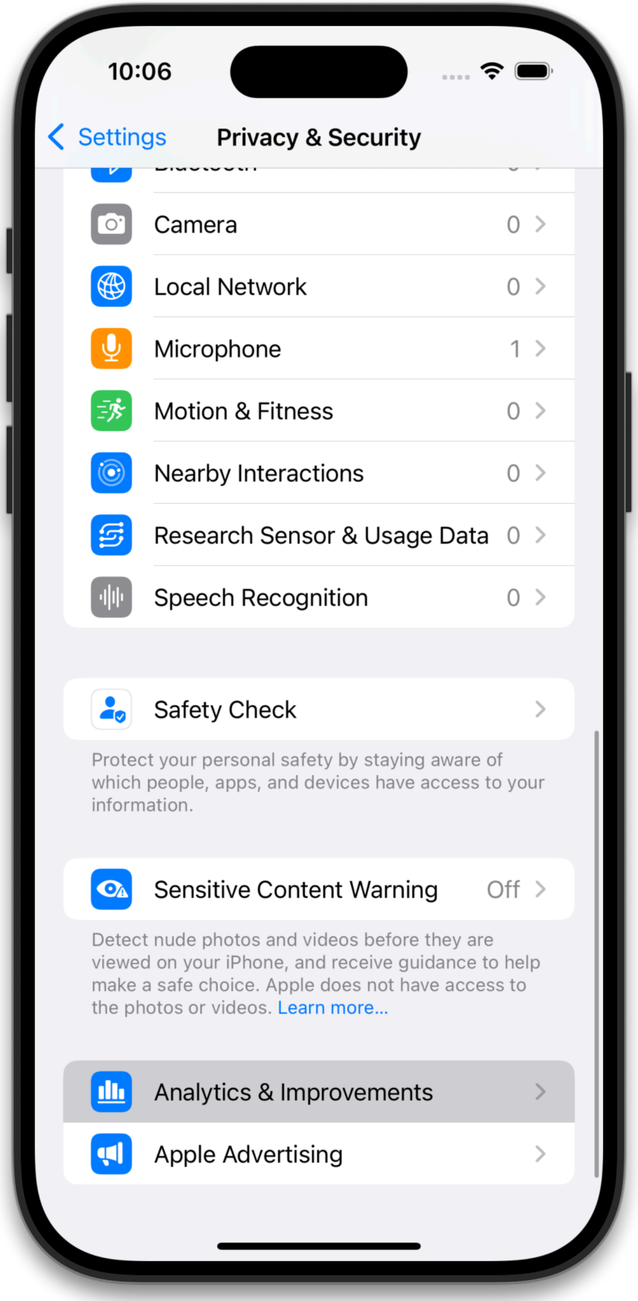


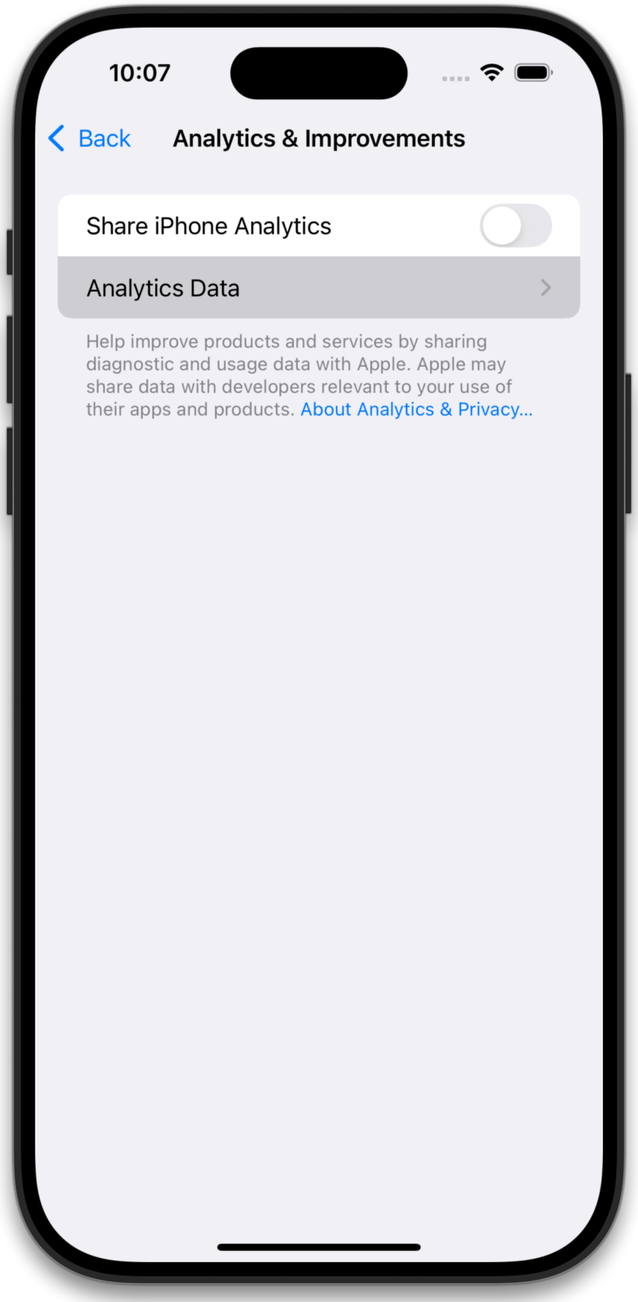
Trace changes of files

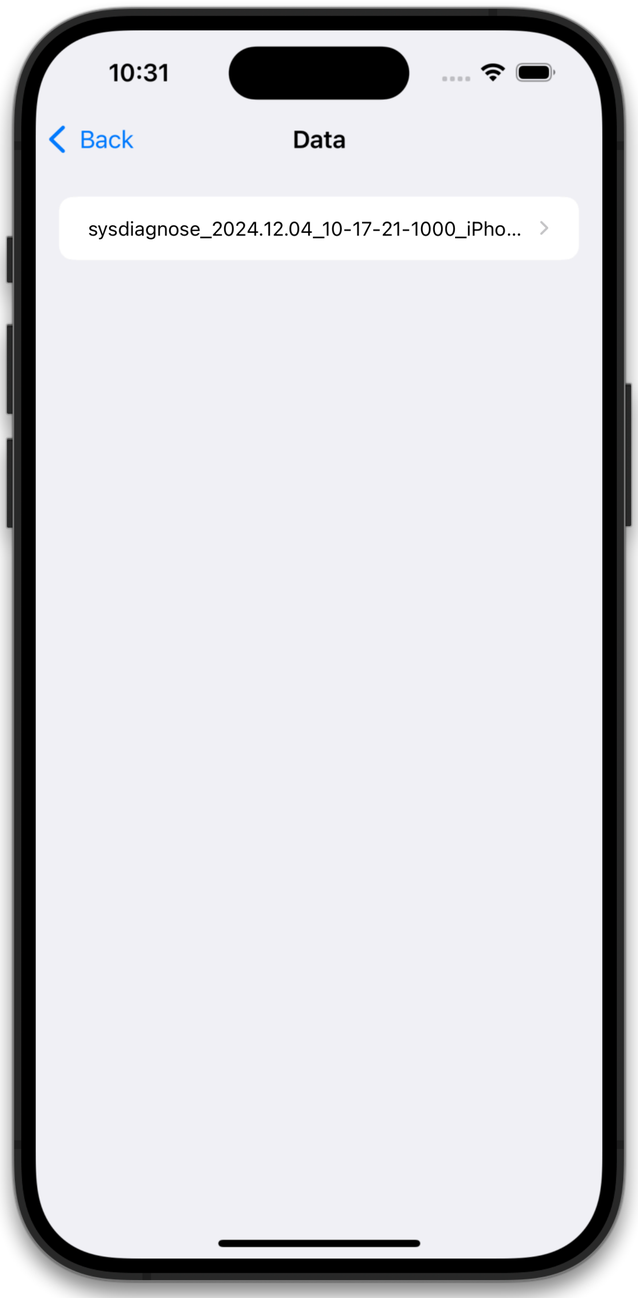
Understand how compromise happened


Volume up
+ down
Power
09:49
Kaanapali
Maps
WEDNESDAY
4
No events today
Calendar
WED
4
Calendar
Photos
Reminders
News
Maps
Health
Wallet
Settings
Search

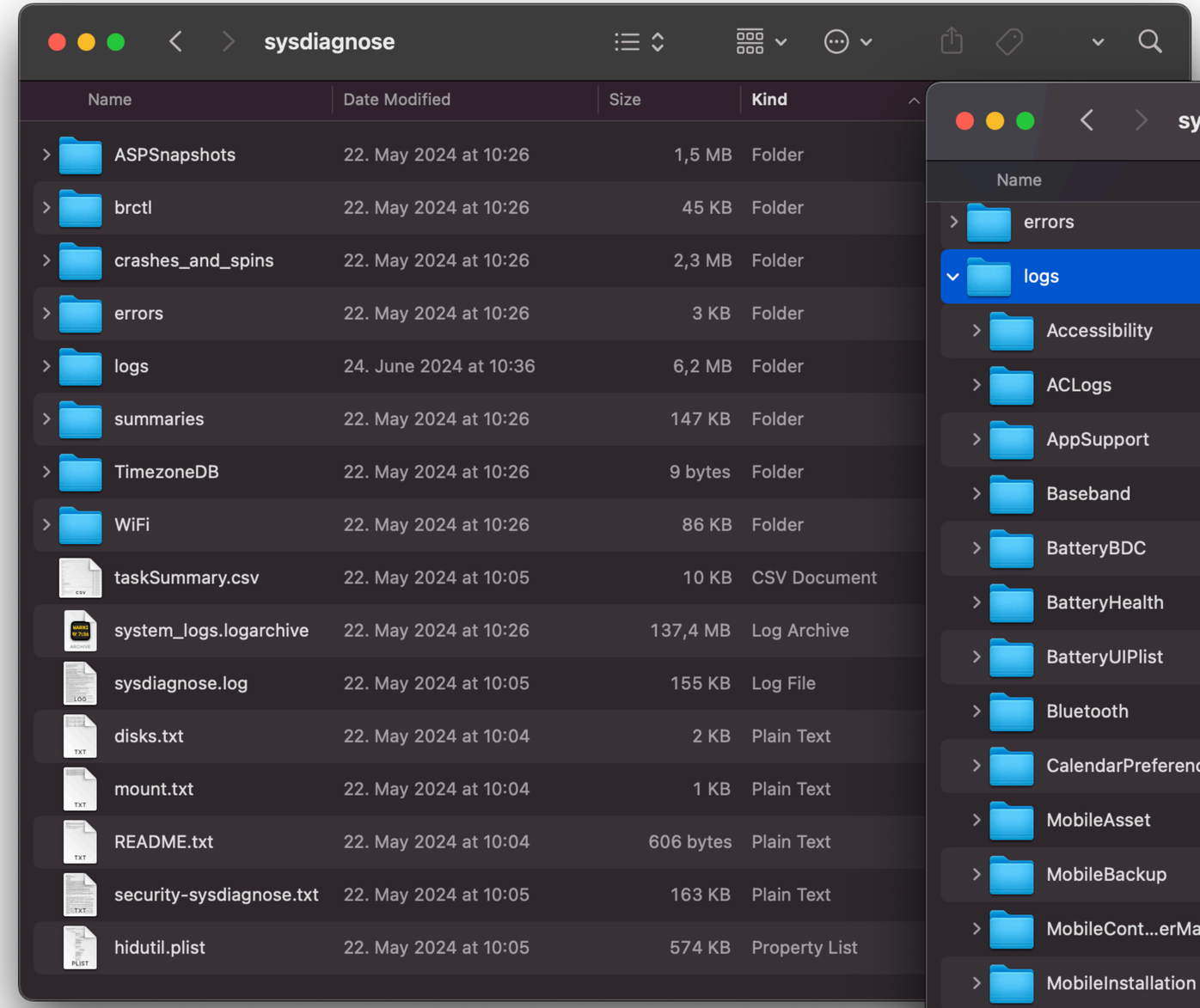

10:04
Settings
Search
Apple Account
Sign in to access your iCloud data, the App Store, Apple services, and more.
General
Accessibility
Action Button
Camera
Home Screen & App Library
Search
Siri
StandBy
Screen Time
Privacy & Security

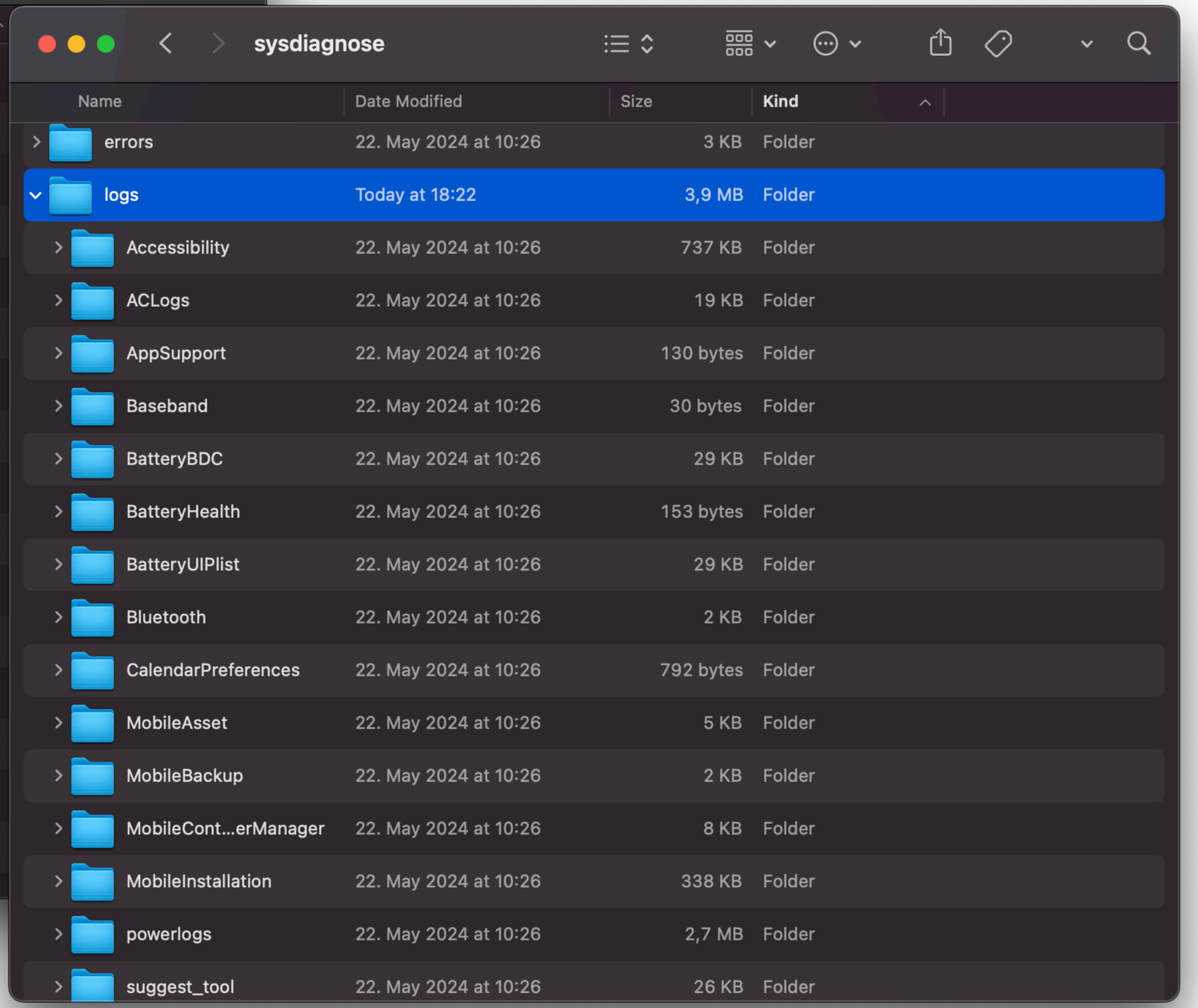

10:06
Settings
Privacy & Security
Camera 0
Local Network 0
Microphone 1
Motion & Fitness 0
Nearby Interactions 0
Research Sensor & Usage Data 0
Speech Recognition 0
Safety Check
Protect your personal safety by staying aware of which people, apps, and devices have access to your information.
Sensitive Content Warning Off
Detect nude photos and videos before they are viewed on your iPhone, and receive guidance to help make a safe choice. Apple does not have access to the photos or videos. Learn more...
Analytics & Improvements
Apple Advertising


10:07
Back
Analytics & Improvements
Share iPhone Analytics
Analytics Data
Help improve products and services by sharing diagnostic and usage data with Apple. Apple may share data with developers relevant to your use of their apps and products. About Analytics & Privacy...


10:31
Back
Data
sysdiagnose_2024.12.04_10-17-21-1000_iPho...

simplified


sysdiagnose
Name
Date Modified
Size
Kind
ASPSnapshots 22. May 2024 at 10:26 1,5 MB Folder
brctl 22. May 2024 at 10:26 45 KB Folder
crashes_and_spins 22. May 2024 at 10:26 2,3 MB Folder
errors 22. May 2024 at 10:26 3 KB Folder
logs 24. June 2024 at 10:36 6,2 MB Folder
summaries 22. May 2024 at 10:26 147 KB Folder
TimezoneDB 22. May 2024 at 10:26 9 bytes Folder
WiFi 22. May 2024 at 10:26 86 KB Folder
taskSummary.csv 22. May 2024 at 10:05 10 KB CSV Document
system_logs.logarchive 22. May 2024 at 10:26 137,4 MB Log Archive
sysdiagnose.log 22. May 2024 at 10:05 155 KB Log File
disks.txt 22. May 2024 at 10:04 2 KB Plain Text
mount.txt 22. May 2024 at 10:04 1 KB Plain Text
README.txt 22. May 2024 at 10:04 606 bytes Plain Text
security-sysdiagnose.txt 22. May 2024 at 10:05 163 KB Plain Text
hidutil.plist 22. May 2024 at 10:05 574 KB Property List


sysdiagnose
Name
Date Modified
Size
Kind
errors 22. May 2024 at 10:26 3 KB Folder
logs Today at 18:22 3,9 MB Folder
Accessibility 22. May 2024 at 10:26 737 KB Folder
ACLogs 22. May 2024 at 10:26 19 KB Folder
AppSupport 22. May 2024 at 10:26 130 bytes Folder
Baseband 22. May 2024 at 10:26 30 bytes Folder
BatteryBDC 22. May 2024 at 10:26 29 KB Folder
BatteryHealth 22. May 2024 at 10:26 153 bytes Folder
BatteryUIPlist 22. May 2024 at 10:26 29 KB Folder
Bluetooth 22. May 2024 at 10:26 2 KB Folder
CalendarPreferences 22. May 2024 at 10:26 792 bytes Folder
MobileAsset 22. May 2024 at 10:26 5 KB Folder
MobileBackup 22. May 2024 at 10:26 2 KB Folder
MobileCont...erManager 22. May 2024 at 10:26 8 KB Folder
MobileInstallation 22. May 2024 at 10:26 338 KB Folder
powerlogs 22. May 2024 at 10:26 2,7 MB Folder
suggest_tool 22. May 2024 at 10:26 26 KB Folder

BDC_Daily_version2.0_2024-04-07_19:18:24.csv

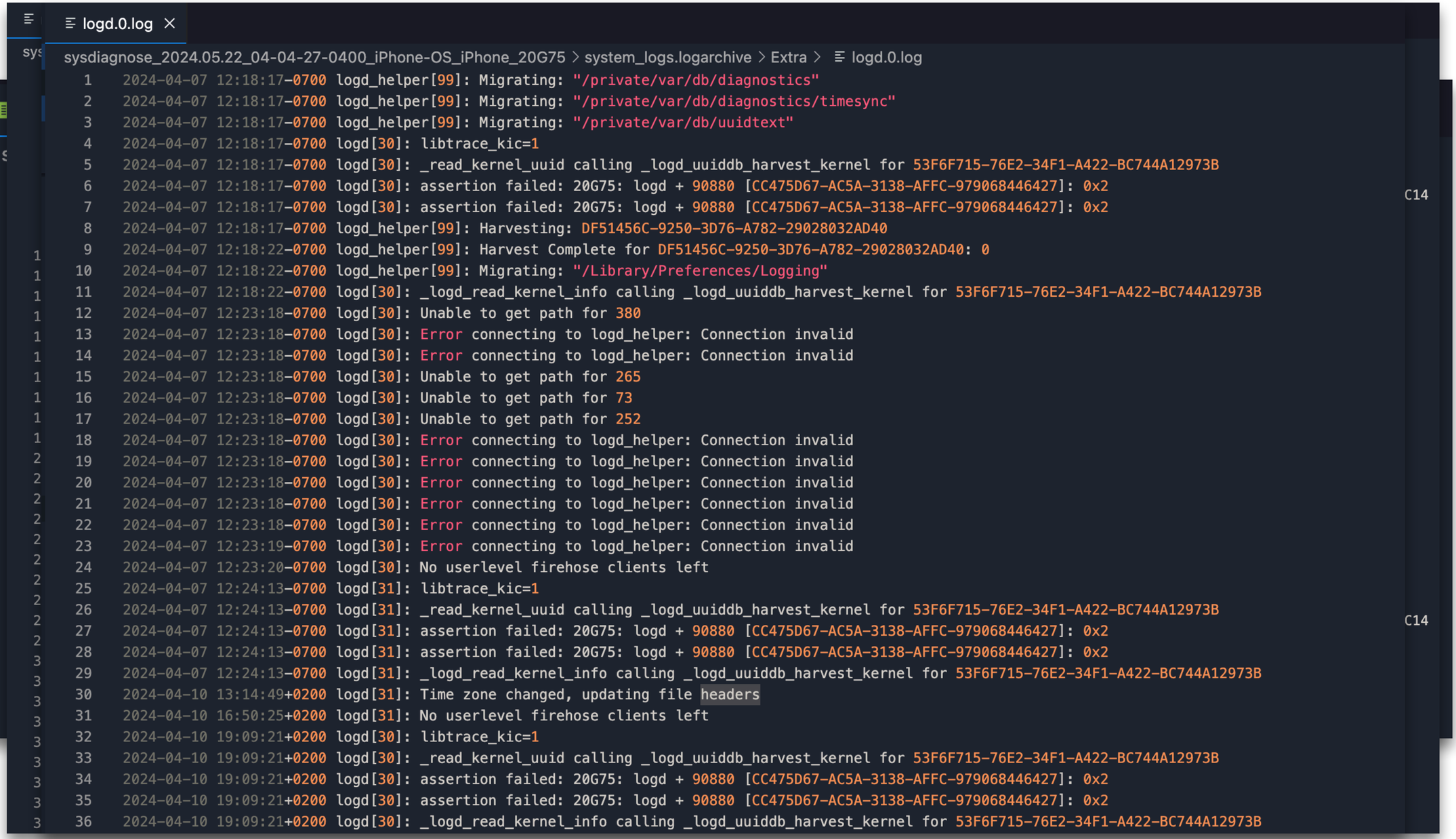
sysdiagnose_2024.05.22_04-04-27-0400_iPhone-OS_iPhone_20G75 > logs > BatteryBDC > BDC_Daily_version2.0_2024-04-07_19:18:24.csv > data

```
1   TimeStamp,WeightedRa,Qmax0,CycleCount,NominalChargeCapacity,TimeAtHighSoc,ChargingVoltage,BHServiceFlags,BHCalibrationFlags
2   2024-04-07 19:18:24,393,1765,204,1629,f428000000000000000000000000000,4185,34078723,0
3   2024-04-08 07:18:24,393,1765,204,1629,f428000000000000000000000000000,4334,3,0
4   2024-04-08 19:21:48,393,1765,204,1629,fa28000000000000000000000000000,4334,3,0
5   2024-04-09 07:34:01,393,1765,204,1629,fa28000000000000000000000000000,4334,3,0
6   2024-04-09 19:22:57,393,1765,204,1629,002900000000000000000000000000,4334,3,0
7   2024-04-10 07:20:07,393,1765,205,1629,002900000000000000000000000000,4334,3,0
8   2024-04-10 19:44:09,372,1765,206,1645,052900000000000000000000000000,4325,3,0
9   2024-04-11 07:26:43,372,1765,206,1645,052900000000000000000000000000,4325,3,0
10  2024-04-11 19:23:06,372,1765,206,1645,0b2900000000000000000000000000,4334,3,0
11  2024-04-12 07:23:22,372,1765,206,1645,0b2900000000000000000000000000,4334,3,0
12  2024-04-12 19:21:58,372,1765,206,1645,112900000000000000000000000000,4334,3,0
13  2024-04-13 07:20:48,372,1765,207,1645,112900000000000000000000000000,4334,3,0
14  2024-04-13 19:23:15,372,1765,207,1645,172900000000000000000000000000,4334,3,0
15  2024-04-14 07:25:57,372,1765,207,1645,172900000000000000000000000000,4334,3,0
16  2024-04-27 08:08:09,372,1765,207,1645,412900000000000000000000000000,4156,34078723,0
17  2024-04-27 20:36:43,372,1765,207,1645,412900000000000000000000000000,4325,3,0
18  2024-04-28 08:12:26,372,1765,207,1645,412900000000000000000000000000,4325,3,0
19  2024-04-28 20:16:19,372,1765,208,1645,472900000000000000000000000000,4325,3,0
20  2024-04-29 08:08:23,372,1765,208,1645,472900000000000000000000000000,4325,3,0
21  2024-04-29 20:11:02,372,1765,208,1645,4d2900000000000000000000000000,4325,3,0
```

mobileactivationd.log.0

sysdiagnose_flight-lon-ber-plus1h-after-datechange_2024.05.26_22-28-38+0200_iPhone-OS_iPhone_20B110 > logs > MobileActivation > mobileactivationd.log.0

```
Fri May 17 17:17:40 2024 [140] <debug> (0x16aed7000) MA: main: ____________________ Mobile Activation Startup ____________________
Fri May 17 17:17:40 2024 [140] <debug> (0x16aed7000) MA: main: build_version: 20B110
Fri May 17 17:17:40 2024 [140] <debug> (0x16aed7000) MA: main: internal_build: false
Fri May 17 17:17:40 2024 [140] <debug> (0x16aed7000) MA: main: uid: 501
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: user_name: mobile
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: system_container_path: /private/var/containers/Data/System/7EE92AA7-D804-43EF-8CD3-1B2377C98761
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: regulatory_images_path: /private/var/containers/Shared/SystemGroup/401FA6CF-ECE1-4E64-BE58-53FA5A91CC14
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: hardware_model: D27AP
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: product_type: iPhone14,7
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: device_class: iPhone
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: has_baseband: true
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: should_hactivate: false
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: is_fpga: false
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: is_devfused_undemoted: false
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: is_prodfused_demoted: false
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: soc_generation: H14
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: ____________________________________________________________
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: dealwith_activation: Activation State: Activated
Fri May 17 17:17:46 2024 [140] <notice> (0x16afef000) MA: -[MobileActivationDaemon unbrickDeviceWithCompletionBlock:]: Unbrick requested by CommCenter
Fri May 17 17:17:46 2024 [140] <notice> (0x16afef000) MA: -[MobileActivationDaemon unbrickDeviceWithCompletionBlock:]: Unbrick requested by CommCenter
Fri May 17 17:17:46 2024 [140] <notice> (0x16b107000) MA: -[MobileActivationDaemon unbrickDeviceWithCompletionBlock:]: Unbrick requested by CommCenter
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: ____________________ Mobile Activation Startup ____________________
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: build_version: 20B110
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: internal_build: false
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: uid: 501
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: user_name: mobile
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: system_container_path: /private/var/containers/Data/System/7EE92AA7-D804-43EF-8CD3-1B2377C98761
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: regulatory_images_path: /private/var/containers/Shared/SystemGroup/401FA6CF-ECE1-4E64-BE58-53FA5A91CC14
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: hardware_model: D27AP
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: product_type: iPhone14,7
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: device_class: iPhone
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: has_baseband: true
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: should_hactivate: false
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: is_fpga: false
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: is_devfused_undemoted: false
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: is_prodfused_demoted: false
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: soc_generation: H14
Fri May 17 17:19:32 2024 [141] <debug> (0x16f13b000) MA: main: ____________________________________________________________
```


logd.0.log
sysdiagnose_2024.05.22_04-04-27-0400_iPhone-OS_iPhone_20G75 > system_logs.logarchive > Extra > logd.0.log
1 2024-04-07 12:18:17-0700 logd_helper[99]: Migrating: "/private/var/db/diagnostics"
2 2024-04-07 12:18:17-0700 logd_helper[99]: Migrating: "/private/var/db/diagnostics/timesync"
3 2024-04-07 12:18:17-0700 logd_helper[99]: Migrating: "/private/var/db/uuidtext"
4 2024-04-07 12:18:17-0700 logd[30]: libtrace_kic=1
5 2024-04-07 12:18:17-0700 logd[30]: _read_kernel_uuid calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
6 2024-04-07 12:18:17-0700 logd[30]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
7 2024-04-07 12:18:17-0700 logd[30]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
8 2024-04-07 12:18:17-0700 logd_helper[99]: Harvesting: DF51456C-9250-3D76-A782-29028032AD40
9 2024-04-07 12:18:22-0700 logd_helper[99]: Harvest Complete for DF51456C-9250-3D76-A782-29028032AD40: 0
10 2024-04-07 12:18:22-0700 logd_helper[99]: Migrating: "/Library/Preferences/Logging"
11 2024-04-07 12:18:22-0700 logd[30]: _logd_read_kernel_info calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
12 2024-04-07 12:23:18-0700 logd[30]: Unable to get path for 380
13 2024-04-07 12:23:18-0700 logd[30]: Error connecting to logd_helper: Connection invalid
14 2024-04-07 12:23:18-0700 logd[30]: Error connecting to logd_helper: Connection invalid
15 2024-04-07 12:23:18-0700 logd[30]: Unable to get path for 265
16 2024-04-07 12:23:18-0700 logd[30]: Unable to get path for 73
17 2024-04-07 12:23:18-0700 logd[30]: Unable to get path for 252
18 2024-04-07 12:23:18-0700 logd[30]: Error connecting to logd_helper: Connection invalid
19 2024-04-07 12:23:18-0700 logd[30]: Error connecting to logd_helper: Connection invalid
20 2024-04-07 12:23:18-0700 logd[30]: Error connecting to logd_helper: Connection invalid
21 2024-04-07 12:23:18-0700 logd[30]: Error connecting to logd_helper: Connection invalid
22 2024-04-07 12:23:18-0700 logd[30]: Error connecting to logd_helper: Connection invalid
23 2024-04-07 12:23:19-0700 logd[30]: Error connecting to logd_helper: Connection invalid
24 2024-04-07 12:23:20-0700 logd[30]: No userlevel firehose clients left
25 2024-04-07 12:24:13-0700 logd[31]: libtrace_kic=1
26 2024-04-07 12:24:13-0700 logd[31]: _read_kernel_uuid calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
27 2024-04-07 12:24:13-0700 logd[31]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
28 2024-04-07 12:24:13-0700 logd[31]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
29 2024-04-07 12:24:13-0700 logd[31]: _logd_read_kernel_info calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
30 2024-04-10 13:14:49+0200 logd[31]: Time zone changed, updating file headers
31 2024-04-10 16:50:25+0200 logd[31]: No userlevel firehose clients left
32 2024-04-10 19:09:21+0200 logd[30]: libtrace_kic=1
33 2024-04-10 19:09:21+0200 logd[30]: _read_kernel_uuid calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
34 2024-04-10 19:09:21+0200 logd[30]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
35 2024-04-10 19:09:21+0200 logd[30]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
36 2024-04-10 19:09:21+0200 logd[30]: _logd_read_kernel_info calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B


logd.0.log
sysdiagnose_2024.05.22_04-04-27-0400_iPhone-OS_iPhone_20G75 > system_logs.logarchive > Extra > logd.0.log
1 2024-04-07 12:18:17-0700 logd_helper[99]: Migrating: "/private/var/db/diagnostics"
2 2024-04-07 12:18:17-0700 logd_helper[99]: Migrating: "/private/var/db/diagnostics/timesync"
3 2024-04-07 12:18:17-0700 logd_helper[99]: Migrating: "/private/var/db/uuidtext"
4 2024-04-07 12:18:17-0700 logd[30]: libtrace_kic=1
5 2024-04-07 12:18:17-0700 logd[30]: _read_kernel_uuid calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
6 2024-04-07 12:18:17-0700 logd[30]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
7 2024-04-07 12:18:17-0700 logd[30]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
8 2024-04-07 12:18:17-0700 logd_helper[99]: Harvesting: DF51456C-9250-3D76-A782-29028032AD40
9 2024-04-07 12:18:22-0700 logd_helper[99]: Harvest Complete for DF51456C-9250-3D76-A782-29028032AD40: 0
10 2024-04-07 12:18:22-0700 logd_helper[99]: Migrating: "/Library/Preferences/Logging"
11 2024-04-07 12:18:22-0700 logd[30]: _logd_read_kernel_info calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
12 2024-04-07 12:23:18-0700 logd[30]: Unable to get path for 380
Files have no common format 😕
21 2024-04-07 12:23:18-0700 logd[30]: Error connecting to logd_helper: Connection invalid
22 2024-04-07 12:23:18-0700 logd[30]: Error connecting to logd_helper: Connection invalid
23 2024-04-07 12:23:19-0700 logd[30]: Error connecting to logd_helper: Connection invalid
24 2024-04-07 12:23:20-0700 logd[30]: No userlevel firehose clients left
25 2024-04-07 12:24:13-0700 logd[31]: libtrace_kic=1
26 2024-04-07 12:24:13-0700 logd[31]: _read_kernel_uuid calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
27 2024-04-07 12:24:13-0700 logd[31]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
28 2024-04-07 12:24:13-0700 logd[31]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
29 2024-04-07 12:24:13-0700 logd[31]: _logd_read_kernel_info calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
30 2024-04-10 13:14:49+0200 logd[31]: Time zone changed, updating file headers
31 2024-04-10 16:50:25+0200 logd[31]: No userlevel firehose clients left
32 2024-04-10 19:09:21+0200 logd[30]: libtrace_kic=1
33 2024-04-10 19:09:21+0200 logd[30]: _read_kernel_uuid calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
34 2024-04-10 19:09:21+0200 logd[30]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
35 2024-04-10 19:09:21+0200 logd[30]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
36 2024-04-10 19:09:21+0200 logd[30]: _logd_read_kernel_info calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B


logd.0.log
sysdiagnose_2024.05.22_04-04-27-0400_iPhone-OS_iPhone_20G75 > system_logs.logarchive > Extra > logd.0.log
1 2024-04-07 12:18:17-0700 logd_helper[99]: Migrating: "/private/var/db/diagnostics"
2 2024-04-07 12:18:17-0700 logd_helper[99]: Migrating: "/private/var/db/diagnostics/timesync"
3 2024-04-07 12:18:17-0700 logd_helper[99]: Migrating: "/private/var/db/uuidtext"
4 2024-04-07 12:18:17-0700 logd[30]: libtrace_kic=1
5 2024-04-07 12:18:17-0700 logd[30]: _read_kernel_uuid calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
6 2024-04-07 12:18:17-0700 logd[30]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
7 2024-04-07 12:18:17-0700 logd[30]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
8 2024-04-07 12:18:17-0700 logd_helper[99]: Harvesting: DF51456C-9250-3D76-A782-29028032AD40
9 2024-04-07 12:18:22-0700 logd_helper[99]: Harvest Complete for DF51456C-9250-3D76-A782-29028032AD40: 0
10 2024-04-07 12:18:22-0700 logd_helper[99]: Migrating: "/Library/Preferences/Logging"
11 2024-04-07 12:18:22-0700 logd[30]: _logd_read_kernel_info calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
12 2024-04-07 12:23:18-0700 logd[30]: Unable to get path for 380
But, how about the time formats?
21 2024-04-07 12:23:18-0700 logd[30]: Error connecting to logd_helper: Connection invalid
22 2024-04-07 12:23:18-0700 logd[30]: Error connecting to logd_helper: Connection invalid
23 2024-04-07 12:23:19-0700 logd[30]: Error connecting to logd_helper: Connection invalid
24 2024-04-07 12:23:20-0700 logd[30]: No userlevel firehose clients left
25 2024-04-07 12:24:13-0700 logd[31]: libtrace_kic=1
26 2024-04-07 12:24:13-0700 logd[31]: _read_kernel_uuid calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
27 2024-04-07 12:24:13-0700 logd[31]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
28 2024-04-07 12:24:13-0700 logd[31]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
29 2024-04-07 12:24:13-0700 logd[31]: _logd_read_kernel_info calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
30 2024-04-10 13:14:49+0200 logd[31]: Time zone changed, updating file headers
31 2024-04-10 16:50:25+0200 logd[31]: No userlevel firehose clients left
32 2024-04-10 19:09:21+0200 logd[30]: libtrace_kic=1
33 2024-04-10 19:09:21+0200 logd[30]: _read_kernel_uuid calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B
34 2024-04-10 19:09:21+0200 logd[30]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
35 2024-04-10 19:09:21+0200 logd[30]: assertion failed: 20G75: logd + 90880 [CC475D67-AC5A-3138-AFFC-979068446427]: 0x2
36 2024-04-10 19:09:21+0200 logd[30]: _logd_read_kernel_info calling _logd_uuiddb_harvest_kernel for 53F6F715-76E2-34F1-A422-BC744A12973B

Common time formats for logging

`YYYY-MM-DD HH:MM+HH:MM`

`YYYY-MM-DD HH:MM:SS.MMM UTC+HH:MM`

Offset to UTC zone

`YYYY-MM-DD HH:MM:SS(Z)`

ISO 8601

`SSSSSSSSSS`

UNIX epoch

`YYYY-MM-DD HH:MM:SS.MMM GMT`

Timezone abbreviation

`YYYY-MM-DDTHH:MM:SS.MMM(Z)`

`YYYY-MM-DDTHH:MM:SS.MMMMMM`

RFC 3339

https://docs.dynatrace.com/docs/observe-and-explore/log-monitoring/log-monitoring-configuration/timestamp-data-format

Common time formats for logging

2024-12-05 17:26-10:00
2024-12-05 17:26:14.286 UTC-10:00
Offset to UTC zone

2024-12-06 03:26:14
ISO 8601

1733491574
UNIX epoch

2024-12-05 17:26:14.286 HST
Timezone abbreviation

2024-12-06T03:26:14.286Z
2024-12-06T03:26:14.286957
RFC 3339

Offset to UTC in sysdiagnose

logd_helper.0.log

```
2023-10-31 16:13:52+0100 logd_helper[103]: Started logd_helper
2023-10-31 16:13:53+0100 logd_helper[103]: Harvesting: EE5D91CF-6012-3F2A-A8B7-DF68B4AF2E83
2023-10-31 16:14:00+0100 logd_helper[103]: Harvest Complete for EE5D91CF-6012-3F2A-A8B7-DF68B4AF2E83: 0
2023-10-31 16:14:01+0100 logd_helper[103]: Harvesting from memory succeded: 902827CC-E6E8-31C5-820F-3E17E1E8EB67
2023-10-31 16:14:01+0100 logd_helper[103]: OSLog segment memory free failed(returned: 0xe00002c7, role: AOP)
2023-10-31 16:14:01+0100 logd_helper[103]: Harvesting from memory succeded: 902827CC-E6E8-31C5-820F-3E17E1E8EB67
2023-10-31 16:14:01+0100 logd_helper[103]: Harvesting from memory succeded: 2BCA9804-5DA0-3218-AA20-117392997FD9
2023-10-31 16:14:01+0100 logd_helper[103]: Harvesting from memory succeded: 24943E38-2E1F-3E02-9A49-58579ACF45B7
2023-10-31 16:14:01+0100 logd_helper[103]: OSLog segment memory free failed(returned: 0xe00002c7, role: MTP)
2023-10-31 16:14:01+0100 logd_helper[103]: Harvesting from memory succeded: 2494338-2E1F-3E02-9A49-58579ACF45B7
2023-10-31 16:14:01+0100 logd_helper[103]: Harvesting from memory succeded: 2BCA9804-5DA0-3218-AA20-117392997FDA
```

ISO 8601 in sysdiagnose

MAAutoAsset_Locker_History_00.log

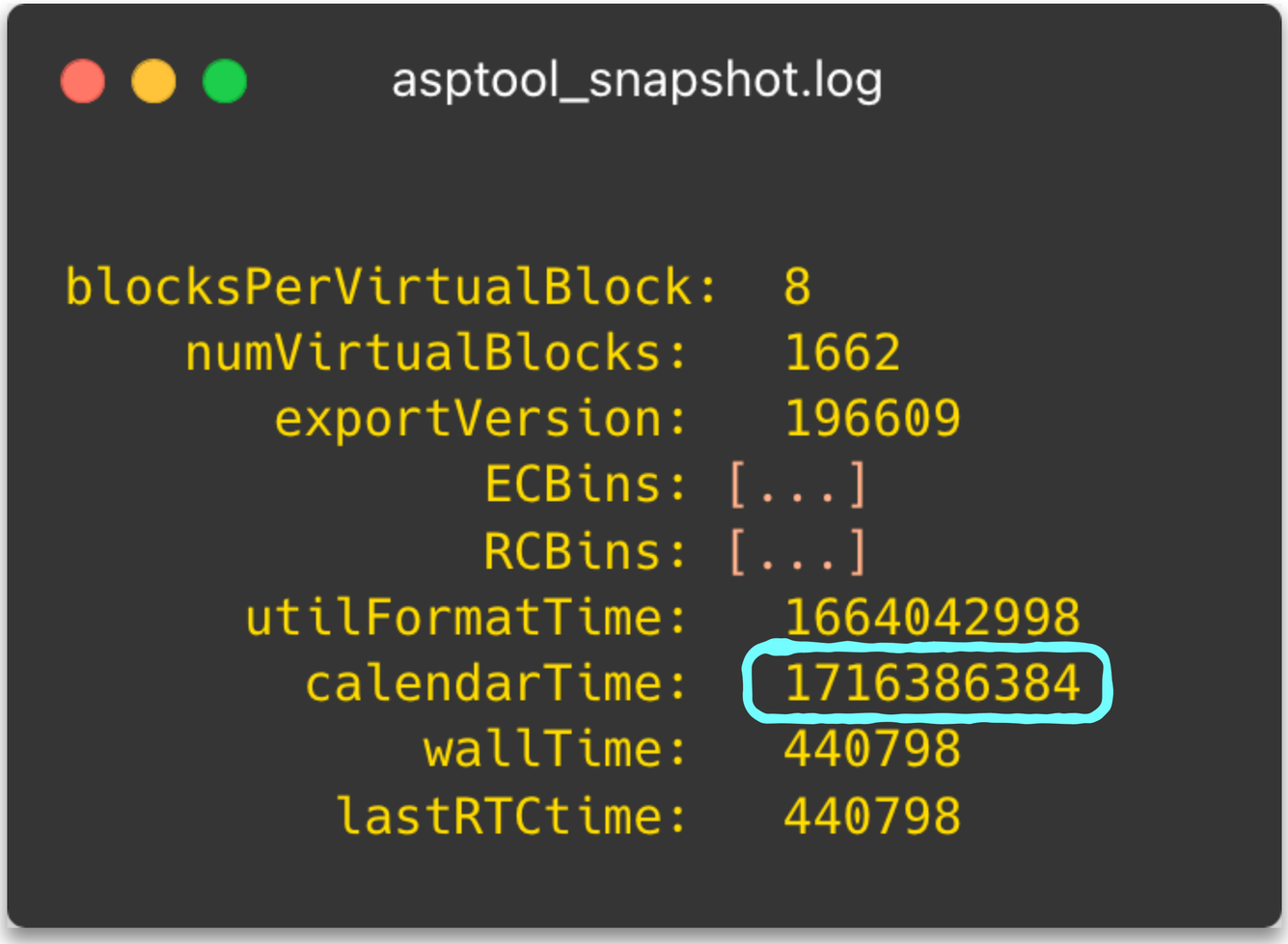
```
time=2024-05-23_16:49:28 op=NEW
time=2024-05-23_16:49:28 op=DEL_CLIENT_UNLOCK          client=com.apple.DataDeliverySe ...
time=2024-05-23_16:50:01 op=MOD_CLIENT_LOCK            client=eligibilityd:lockContent ...
time=2024-05-23_16:50:02 op=MOD_CLIENT_LOCK            client=eligibilityd:lockContent ...
time=2024-05-23_16:50:15 op=ADD_CLIENT_LOCK            client=com.apple.DataDeliverySe ...
time=2024-05-23_16:50:15 op=DEL_CLIENT_UNLOCK          client=com.apple.DataDeliverySe ...
time=2024-05-23_16:50:57 op=ADD_CLIENT_LOCK            client=com.apple.DataDeliverySe ...
time=2024-05-23_16:50:57 op=DEL_CLIENT_UNLOCK          client=com.apple.DataDeliverySe ...
time=2024-05-23_16:50:57 op=ADD_CLIENT_LOCK            client=com.apple.DataDeliverySe ...
time=2024-05-23_16:50:57 op=DEL_CLIENT_UNLOCK          client=com.apple.DataDeliverySe ...
```

RFC 3339 in sysdiagnose

unified_asset_manager.log


```
...
  "atomicInstance" : "5329FB46-DAFC-4D07-98C9-3316DE2A63F3",
  "autoAssetSet" : {
    "assetSetIdentifier" : "com.apple.siri.understanding.nl.overrides"
  },
  "UAFHistoryMetadata" : {
    "reason" : "locked",
    "timestamp" : "2024-06-29T11:29:45.762Z"
  }
},
"filename" : "com.apple.siri.understanding.nl.overrides-uafLockedLog.prev.json",
"history" : "prev"
},
{
"assetSetInfo" : {
  "autoAssetSet" : {
    "assetSetIdentifier" : "com.apple.siri.understanding.nl.overrides"
  },
  "UAFHistoryMetadata" : {
    "reason" : "altered",
    "timestamp" : "2024-07-06T09:01:47.426Z"
  }
},
...
```

UNIX epoch in sysdiagnose



There are even more!

Other formats in sysdiagnose

mobileactivationd.log.0

```
Fri May 17 17:17:40 2024 [140] <debug> (0x16aed7000) MA: main: _____________________ Mobile Activation Startup _____________________
Fri May 17 17:17:40 2024 [140] <debug> (0x16aed7000) MA: main: build_version: 20B110
Fri May 17 17:17:40 2024 [140] <debug> (0x16aed7000) MA: main: internal_build: false
Fri May 17 17:17:40 2024 [140] <debug> (0x16aed7000) MA: main: uid: 501
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: user_name: mobile
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: system_container_path: /private/var/containers/Data/System/7EE92AA7-
D804-43EF-8CD3-1B2377C98761
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: regulatory_images_path: /private/var/containers/Shared/SystemGroup/401FA6CF-
ECE1-4E64-BE58-53FA5A91CC14
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: hardware_model: D27AP
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: product_type: iPhone14,7
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: device_class: iPhone
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: has_baseband: true
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: should_hactivate: false
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: is_fpga: false
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: is_devfused_undemoted: false
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: is_prodfused_demoted: false
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: soc_generation: H14
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: main: ____________________________________________________________________
Fri May 17 17:17:41 2024 [140] <debug> (0x16aed7000) MA: dealwith_activation: Activation State: Activated
```

Multiple formats in files

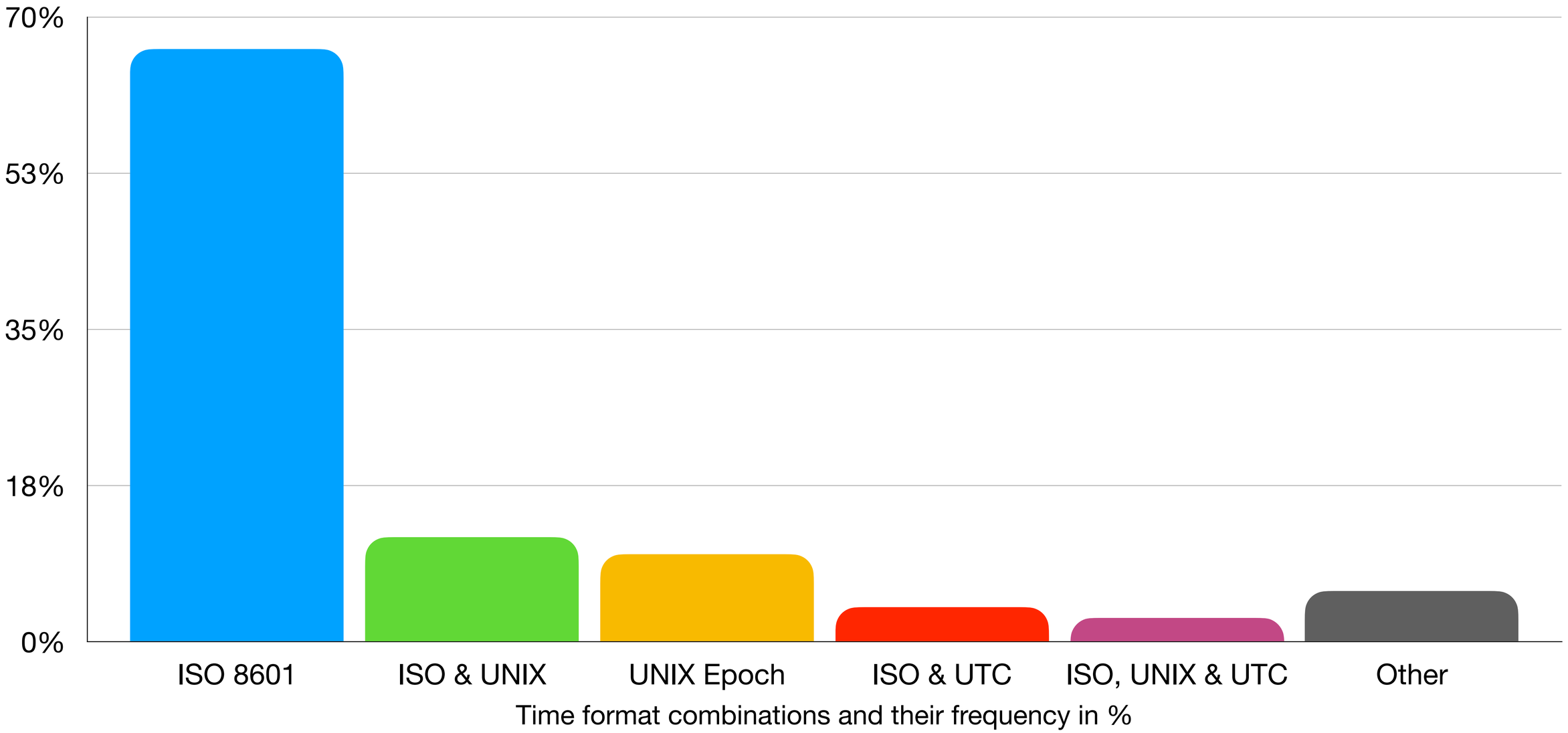
stacks-2024-07-07-132400.ips


```
{"bug_type":"288","timestamp":"2024-07-07 13:24:00.00 +0100","os_version":"iPhone OS 18.0
(22A5297f)","roots_installed":0,"incident_id":"0285B18D-C2AC-4D84-A00C-E32D582A7AEF"}
{
  "build" : "iPhone OS 18.0 (22A5297f)",
  "product" : "iPhone16,1",
  "kernel" : "Darwin Kernel Version 24.0.0: Sun Jun 16 20:49:29 PDT 2024; root:xnu-11215.0.115.502.1~1\/
RELEASE_ARM64_T8122",
  "tuning" : {
  },
...
```

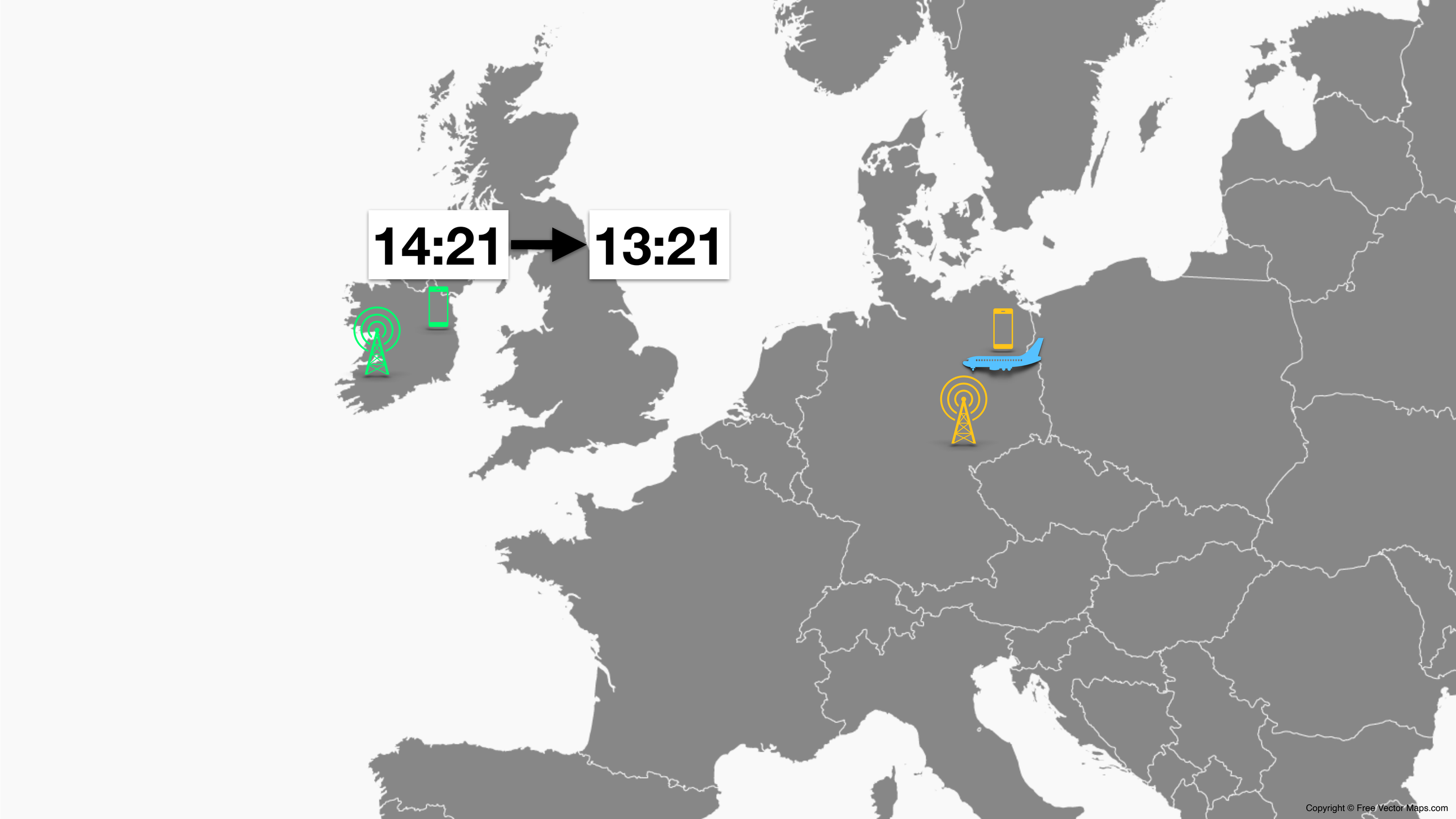
Multiple formats in files

hidutil.plist

```
<key>ActivityLog</key>
<array>
    <dict>
        ..
        <key>ActivityTime</key>
        <string>2024-07-07 12:13:46.289649</string>
    </dict>
...
    <dict>
        <key>Generation Stats</key>
        <array>
            <dict>
                ...
                <key>startTime</key>
                <string>2024-07-07 13:13:10 +0200</string>
                <key>start...Epoch</key>
                <integer>1720350790</integer>
                ...
            </dict>
            ...
            <dict>
                ...
                <key>set_time</key>
                <string>07.07.24, 11:42:26 Central European Summer Time</string>
                ...
            </dict>
```


70%
53%
35%
18%
0%
ISO 8601
ISO & UNIX
UNIX Epoch
ISO & UTC
ISO, UNIX & UTC
Other
Time format combinations and their frequency in %

But how does time change?



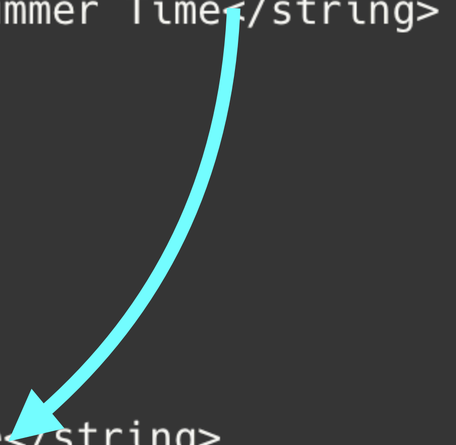
Event triggering time change

logd.0.log

```
2024-03-06 10:22:33+0000 logd[32]: Received a Purgeable Request from CacheDelete on volume: /private/var
2024-03-06 10:22:33+0000 logd[32]: Reporting 1714576944/234122680 bytes as purgeable
2024-03-06 12:18:17+0100 logd[32]: Time zone changed, updating file headers
2024-03-06 13:14:09+0100 logd[32]: flush for power button
```

hidutil.plist

```
<dict>
    <key>key</key>
    <string>PreserveTimestamp</string>
    <key>set time</key>
    <string>07.07.24, 14:21:41 Central European Summer Time</string>
    <key>value</key>
    <true/>
</dict>
<dict>
    <key>key</key>
    <string>HostStateNotification</string>
    <key>set time</key>
    <string>07.07.24, 13:24:08 Irish Standard Time</string>
    <key>value</key>
    <dict>
        <key>PocketTouchesExpected</key>
        <true/>
        <key>ScreenOn</key>
        <true/>
    </dict>
</dict>
```



AppConduit.lol.0

```
Wed May 22 16:34:49 2024 [186] <notice> (0x16db73000) -[ACXDeviceConnectionClient
applicationIsInstalledOnDeviceWithPairingID:withBundleID:completion:]: [...]
Wed May 22 15:36:24 2024 [186] <notice> (0x16db73000) -[ACXDeviceConnectionClient enableObservers]_block_invoke: [...]
```

logdata.statistics.0.txt

```
--- !logd statistics record
type  : Memory Rollover
time  : 2024-05-22 16:31:27+0200
total : 19804552
procs :
    - ...

--- !logd statistics record
type  : Memory Rollover
time  : 2024-05-22 15:32:26+0100
total : 19500920
procs :
    - ...
```

logd_helper.0.log

```
2024-05-22 16:30:36+0200 logd_helper[110]: IOP connect to subrole uuid
06C9CFD7-7822-39D6-9875-4F54A717BCA9

2024-05-22 16:30:36+0200 logd_helper[110]: attach to firmware role
using uuid returned 0xE00002C2

2024-05-22 16:30:36+0200 logd_helper[110]: Harvesting from memory
succeded: 06C9CFD7-7822-39D6-9875-4F54A717BCA9
2024-05-22 15:38:12+0100 logd_helper[110]: IOP connect to coproc DCP

2024-05-22 15:38:12+0100 logd_helper[110]: IOP connect to coproc AOP
```


hidutil.plist
<dict>
<key>Digitizer</key>
<integer>101</integer>
<key>VendorDefined</key>
<integer>49</integer>
<key>startTime</key>
<string>2024-07-07 14:21:52 +0200</string>
<key>startTimeSinceEpoch</key>
<integer>1720354912</integer>
<key>totalCount</key>
<integer>49</integer>
</dict>
<dict>
<key>Digitizer</key>
<integer>94</integer>
<key>VendorDefined</key>
<integer>47</integer>
<key>startTime</key>
<string>2024-07-07 13:22:02 +0100</string>
<key>startTimeSinceEpoch</key>
<integer>1720354922</integer>
<key>totalCount</key>
<integer>47</integer>
</dict>

--more-precision?

log-bb-2024-05-26-.../info.txt

```
Starting From: 2024-05-26-21-28-06
Size (Bytes): 1016320
File: 0x0001DC8C.bin
Starting From: 2024-05-26-21-28-06
Size (Bytes): 1025024
File: 0x0001DC8D.bin
Starting From: 2024-05-26-22-28-07
Size (Bytes): 1041792
File: 0x0001DC8E.bin
Starting From: 2024-05-26-22-28-07
Size (Bytes): 1015936
File: 0x0001DC8F.bin
```

How could one detect changes

- most precise
  - baseband logs (if possible)
- most info (if gathered)
  - hidutil.plist
  - system_logs.logarchive, especially logd.0.log and logdata.statistics.0.txt
  - AppConduit and MobileActivation logs

Mahalo!

M.Sc. Computer Science student

Hasso Plattner Insititute

research@linawilske.dev

Objective by the Sea
version 7.0