Forensic Investigation iPhone (based on NFI Data) - Panama Case Kris & Lisanne

	Date	Time	Activity / Comment	Passcode	SIM PIN	Battery	Est. Temp	Signal-Log	Display
Session 1	**31.03.2014**	13:13	**Power On** - Boot-Time 1:47	Yes	Yes				
		14:00	WhatsApp (maybe WA to Kris friend "going hiking")			70%			
		16:42	Wi-Fi SbtR | 16:59 WhatsApp | last activity 19:07						
	01.04.2014	04:13	System						
		11:05	First Use 1.4.			51%	23.4 °C	**-82 dBm, 5 Bars**	●●●●●
		11:20						**-85 dBm, 4 Bars**	●●●●○
		11:49						Dead Zone - Freeze -82 dBm, 1 Bars	**No Service**
		12:33						**-82 dBm, 1 Bars**	●○○○○
		13:15	4 Photos likely Mirador, Last: IMG_2128.JPG					**-87 dBm, 3 Bars**	●●●○○
		13:16						**-89 dBm, 4 Bars**	●●●●○
		13:38	*~800 Powerlogs by 16:39 - likely sporadic activity*					Dead Zone - Freeze -94 dBm, 1 Bars	**No Service**
		16:39	**Emergency Call 112**			42%	24.2 °C	Dead Zone - Freeze -94 dBm, 1 Bars	**No Service**
	Powerlogs	16:40						Dead Zone - Freeze -94 dBm, 1 Bars	**No Service**
	Count: ~5800	17:52	**Power Off** - No More File System Activity						
Session 2	**02.04.2014**	08:12	**Power On** - Boot-Time 1:38	Yes	Yes				
		08:13	Settings 2G/3G and **Snapshot** Control Center (8:14)						
	Powerlogs	08:14	**Emergency Call 112**			43%	19.3 °C	Dead Zone - Dummy -113 dBm, 1 Bars	**No Service**
	Count: ~120	08:14	**Power Off** - No More File System Activity						
Session 3, 4, 5	**03.04.2014**	09:31	**Power On** - Boot-Time n/a because of NFI Error	Yes	Yes				
		09:33	**Emergency Call 911 (twice in 4 sec.)**			42%	19 °C	Dead Zone - Dummy -113 dBm, 1 Bars	**No Service**
		09:33	**Snapshot** Dialer-App						
		09:33	Baseband-Log: kNoNetworkService (typical)						
		09:33	**Power Off** - No More File System Activity						
		11:45	**Power On** - User-initiated shutdown during startup	**Likely**	Yes	Powerlog process (battery, signal, apps, etc.) not started			**Searching ...**
		11:46	**Power Off** - No More File System Activity						(may be No Service)
		15:58	**Power On** - Boot-Time 1:52	Yes	Yes				
	Powerlogs	16:02	**Snapshot** Contact "Mytiam"			39%	24.1 °C	Dead Zone - Dummy -113 dBm, 1 Bars	**No Service**
	Count: ~250	16:02	**Power Off** - No More File System Activity						

The file CurrentPowerlog.powerlog has not been archived since April 4th. This means that there have been no Powerlogs since April 4th, not even on DVD.

Session 6, 7	**04.04.2014**	10:16	**Power On** - User-initiated shutdown during startup	**Likely**	**Yes**	Powerlog process (battery, signal, apps, etc.) not started	**Searching …**
		10:17	**Power Off** - No More File System Activity			est. 38%	(may be No Service)
		13:41	**Power On** - User-initiated shutdown during startup	**Likely**	**Yes**	Powerlog process (battery, signal, apps, etc.) not started	**Searching …**
		13:42	**Power Off** - No More File System Activity			est. 37%	(may be No Service)
Session 8, 9	**05.04.2014**	10:50	**Power On** - User-initiated shutdown during startup	**Likely**	**Yes**	Powerlog process (battery, signal, apps, etc.) not started	**Searching …**
		10:51	**Power Off** - No More File System Activity			est 36%	(may be No Service)
		13:37	**Power On** - User-initiated shutdown during startup	**Likely**	**No**	Powerlog process (battery, signal, apps, etc.) not started	**Locked SIM**
		13:38	**Power Off** - No More File System Activity			est. 35%	
Session 10, 11	**06.04.2014**	10:26	**Power On** - User-initiated shutdown during startup	**Yes**	**No**	Powerlog process (battery, signal, apps, etc.) not started	**Locked SIM**
		10:27	**Snapshot** Worldclock-App via home screen				
		10:27	**Power Off** - No More File System Activity			est. 34%	
		14:34	**Power On** - User-initiated shutdown during startup	**Likely**	**No**	Powerlog process (battery, signal, apps, etc.) not started	**Locked SIM**
		14:35	**Power Off** - No More File System Activity			est. 33%	
	07.04.2014		No Activity			est. 32%	
	08.04.2014		No Activity			est. 32%	
	09.04.2014		No Activity			est. 31%	
	10.04.2014		No Activity			est. 31%	
Session 12	**11.04.2014**	10:50	**Power On** - Boot-Time n/a because no Powerlogs **18 Files created / changed 10:50 - 11:56** **No Crash-Report / LowBatteryLog** The NFI examined whether the device stayed on until the battery drained; result: negative	**No**	**No**	Powerlogs generated in RAM not persistently stored because phone not initially unlocked - RAM/NAND "bug" May be manipulated via SSH-Ramdisk (DFU-Mode) May be used by third party	**Locked SIM** **iPhone locked**
		11:56	**Power Off** - No More File System Activity			est. 5-30%	

Startup process | Boot-Time: This refers to the time after powering on the device that iOS needs to initialize all daemons and processes, especially the PowerLog process. It does *not* refer to the time until the lock screen or home screen appears. Typically, this takes about 1:10 to 1:20 minutes after power-on. On Kris's iPhone, however, it takes 1:40 to 1:50 minutes.The cause is unknown - possible reasons include a jailbreak, spy app, numerous boot-time processes, or low free storage space. The NFI did not provide shutdown times with second-level accuracy, even though this would have been possible (via FSEvents). As a result, for sessions with very short uptime and an entered SIM PIN, it cannot be determined precisely whether the iPhone was shut down during the signal search ("Searching") or just a few seconds afterward. A signal check only begins after the passcode and SIM PIN have been entered (at the earliest 1:05 after power-on). The display repeatedly switches between "Searching" and "No Service" when the iPhone is attempting retries in a signal dead zone.

Q&A

Was the iPhone partially unusable due to water or moisture damage? Did the touchscreen have a partial defect? Did the backlight fail? Or the hardware buttons?

Most likely not. While the iPhone isn't waterproof, it is rated for operation in up to 95% humidity. All input elements (swipes, buttons, dial pads, keyboard) were functioning quickly and without errors. With a ghost touch issue, however, entering an 8-digit code and SIM PIN (Passcode last entered on April 6) or using the device smoothly would be virtually impossible.

Moreover, the keyboard can be repositioned to three different areas of the screen by rotating the phone into landscape mode. There are also a variety of accessibility features, such as Zoom and AssistiveTouch, which allow for alternative operation of the device or for relocating and enlarging input elements anywhere on the screen - including those required for entering the SIM PIN. In the event of a backlight failure, VoiceOver can be used in dark environments. Every system setting can be scrolled to any part of the screen. Emergency calls can be made via two different dial pad layouts. Calls can also be initiated through the voice assistant (basic Siri), which is enabled by default.

It's not about needing to know all these functions. It's about, if you have an issue, trying to solve the problem through the settings. And that there are forensic traces of these attempts.

In June, a moderately bloated battery was discovered. But were there already battery issues or voltage drops back in April that could have caused the iPhone to shut down unexpectedly - for example, on days when it had very short uptime?

Most likely not. Kris was using a relatively new iPhone 4 Rev. A, a model that was released years after the original launch. The main issue with a partially defective battery would typically be a voltage drop under load - for instance, when launching an app. The iPhone might still show 40% battery, but the voltage could already have dropped below the minimum. Some insights into the battery's health can also be gained from the battery logs, which help determine whether it was still in good condition or already showed signs of wear or failure.

Kris's iPhone (April 3, 4 PM):

- Capacity: 89% - good, estimated to be around 1 year old (~250 cycles)
- Voltage: 3.75 V - consistent with 39% charge, technically coherent

The battery was in relatively good condition. No abnormalities. No signs of cell damage or voltage drops. The battery was functioning normally and not defective. In fact, these values were significantly better than those of my two iPhone 4 batteries. There are also system crash reports such as Low Voltage, Power Failure, and Kernel Panic. These are triggered by sudden shutdowns and typically generated during the next reboot, while controlled, automatic shutdowns (e.g., Low Battery) allow iOS to log the event immediately.

In the meantime, I've conducted some battery tests - specifically disconnecting the fixed and screwed-in battery from the system, both while the iPhone was powered off and while in standby or active mode. Disconnecting it for just one second is enough. In every case, the iPhone rebooted showing the date January 1, 1970, 1:00 AM. The time shows as 1 AM because the time zone information is retained in NAND, and January 1 is within standard time (not daylight saving time). This also confirms that the iPhone couldn't have shut down suddenly due to a defective battery or voltage drop - because in such cases, this kind of reset would have occurred.

Was the iPhone in June so damaged by water, corrosion, etc., that the NAND memory could only be read using a chip-off procedure?

No. The iPhone 4 uses hardware encryption similar in concept to BitLocker on Windows. You can physically remove the NAND chip and read its raw contents, but without the functioning original device, you cannot decrypt the data - the UID key is fused into the A4 SoC and is not extractable, so the NAND contents are essentially unreadable on their own.

Technical Reference

The findings of this investigation are based on **NFI data** and on **field tests** conducted with my two iPhone 4 devices, which have the **same hardware and firmware as Kris's iPhone**.

Kris's iPhone 4

Model A1332 Rev. A (3,2) - A4 SoC - 8 GB - Firmware iOS 7.0.6

The iPhone 4 was equipped with a compass, a three-axis gyroscope, and an accelerometer. However, motion data could only be recorded and logged in the background with the introduction of power-efficient motion coprocessors, which were first included starting with the iPhone 5.

Kris's iPhone was set to Dutch time, which is Panama time plus 6 hours. Automatic time zone adjustment based on detected location (via Wi-Fi, location services, or GPS) did not work - neither on her phone nor on my test devices. However, the automatic switch to Dutch daylight saving time on March 29 at 8:00 p.m. local time worked correctly. From that point on, the time offset became Panama time plus 7 hours. The iPhone was protected with a 4-digit passcode and a 4-digit SIM PIN.

Relevant Cell Towers near Pianista in 2014

(Distances: Trail 2–4 km, Mirador 5 km)

ASEP Panama

Digicel coverage map (archived)

Roaming partners for the Netherlands: T-Mobile (Kris) / Vodafone

Alto/Bajo Lino, 1200 m elevation, Digicel, 60 m tower
https://maps.app.goo.gl/tWXhD1TU5PsK3A1K9

Jaramillo, 1200 m elevation, SBA Torres, 80 m tower
https://maps.app.goo.gl/eV5zxHPpdMNhPoNi8

Alto Quiel, 1400 m elevation, Digicel, 60 m tower
https://maps.app.goo.gl/RxNnxKyLgse7xm8g8

According to SliP, both Kris (T-Mobile) and Lisanne (KPN NL) were able to use voice calls and SMS in Panama. A formal roaming contract is typically not required for this - it's usually enough for the providers to have a basic roaming agreement in place, even though using the service can be expensive.

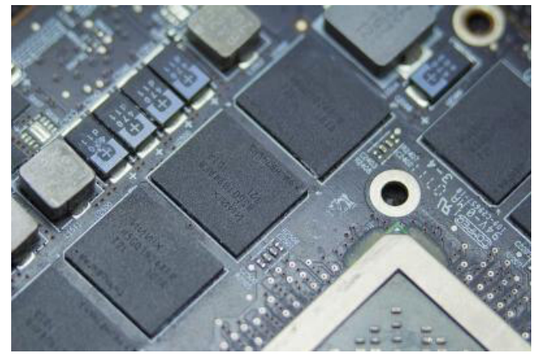
Freeze Logs | Dummy Logs

These logs do not contain real-time measured values. Instead they record either a previously measured value (a *freeze*), or a placeholder value (a *dummy*).

Example scenario: You could wrap an iPhone in aluminum foil at the Mirador, fly it by helicopter to Amsterdam, and then remove it from the foil while inside a cellular dead zone. The device would continue to log the last actually measured value from the Mirador (a *freeze log* showing the freeze dBm & 1 Bars). If you then reboot the phone while still in a dead zone in Amsterdam, it would log the "placeholder value" **-113 dBm, 1 Bars** (a *dummy log*). The iPhone 4S can measure and log signal values below -113 dBm, while the iPhone 4 cannot.

iOS 7 RAM / NAND Flash "bug" (iOS Data Protection)

About a minute or slightly more after powering on the iPhone, the Powerlog process begins recording logs (such as signal strength, battery levels, app usage, etc.). After an hour of use, for instance, several hundred real-time logs are generated. In iOS 7, these logs are stored in volatile RAM until the phone is unlocked for the first time. When the iPhone is unlocked by entering the passcode, the Powerlogs are written to NAND flash memory, even retroactively, with new logs being saved directly to NAND in real time. However, if the iPhone is turned off before being unlocked, the logs are lost, meaning no Powerlogs are available, despite an hour of use.



The loss of logs is essentially a side effect of the underlying security and Data Protection policies, even though, for example, battery levels do not involve private data.

Technical background (NSFileProtectionCompleteUntilFirstUserAuthentication):

Apple Security Guide: https://support.apple.com/de-de/guide/security/secb010e978a/web

Technical blog: https://blog.angelovillegas.com/ios-data-protection/

In-depth article (German): https://www.heise.de/hintergrund/iOS-Verschluesselung-durchleuchtet-2066500.html

FSEvents

File System Events (FSEvents) are a type of file system journal that contains a wealth of forensic information - information that was likely not analyzed by the NFI or their forensic tools. Among other things, every use of the iPhone (excluding DFU mode) leaves behind two hidden files in two hidden directories, with timestamps accurate to the second that clearly indicate the exact time the device was powered off. **The NFI reviewed the file system activity, so they checked the timestamps of the FSEvent files.**

Further details:

Archived article: Apple FSEevents-Forensics - Nicole Ibrahim

Blog: https://www.hexordia.com/blog/mac-forensics-analysis

```
/$  find . -daystart -mtime 105 -type f -printf "%p %TY-%Tm-%Td %TH:%T
./.fseventsd/000000000004f95f 2024-06-03 00:07:06 +0200
./private/var/.fseventsd/000000000004fba8 2024-06-03 00:07:06 +0200
```

Emergency Calls | CallHistory.db

Using this **SQLite database**, all calls and call attempts can be traced - including details such as **timestamp, phone number, network connection**, and **call duration**. Similar data is also logged in the P**owerlogs**, though without recording the phone number.

Emergency calls can be made **without entering a passcode or SIM PIN** via the emergency call feature on the lock screen. While the **RAM/NAND flash "bug"** prevents **persistent storage of Powerlogs** when the iPhone is powered off without first being unlocked, it **does not prevent emergency call attempts from being logged** in the call history database. **No emergency call attempts were made after the morning of April 3** - otherwise, they would have been recorded in the call history.

Emergency calls are possible on **any available network**. This means they can still be placed even when the phone shows **"No Service"** or **"Locked SIM".**

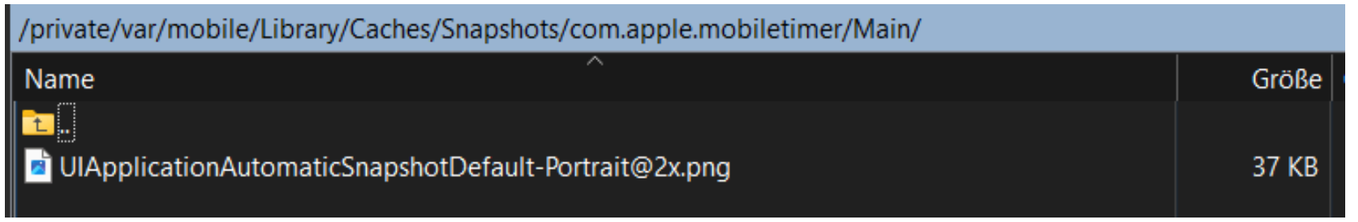
Snapshots

When using apps on iOS 7, the system automatically creates *"last state"* snapshots - essentially screenshots - of the user's last activity within each app. These snapshots can capture anything from a drafted SMS message, to a settings change or check (as seen in the Control Center on April 2), or even the Phone app → Dialer (as on April 3 at 9:33 a.m.).

Both the Dialer screen on April 3 at 9:33 a.m. (time of the last emergency calls) and the contact "Mytiam" at 4:02 p.m. the same day were accessed via the Phone app. The fact that *both* activities have individual "last state" snapshots is due to the Dialer having its **own separate snapshot**.

Each time an app is used again, its previous "last state" snapshot is overwritten. The purpose of these snapshots is to provide a real-time image for the **fade-out animation** when closing an app, and to display in the **App Switcher** (accessed via double-pressing the Home button).

This is what it looked like, for example, when the Clock app was opened on **April 6 at 10:27 a.m.**:



Bootlogs

20:28:11 **Power On**

Tue Sep 3 20:28:36 2024 main: Starting Up [NFI Startup Time]
Tue Sep 3 20:28:46 2024 dealwith_activation: Looking up the record for **ICCID** 228672635330891650
Tue Sep 3 20:29:16 2024 SIM status: kCTSIMSupport**SIMStatusReady**

The boot logs (lockdownd) record, among other things, the ICCID (Integrated Circuit Card Identifier) and the correct entry of the SIM PIN. They also log the startup time in a "Starting Up" log, which occurs approximately 25 seconds after "Power On". On all days, a "Starting Up" log is present in every session.

Powerlogs

09/03/24 20:29:18 [Log] state=booting; loggingMode=Lite; binary=aggregated;
09/03/24 20:29:18 [Display] active=yes; brightness=79.0%;
user_brightness=<unknown>; als=disabled; mie=off; slider=51777; mNits=0;
09/03/24 20:29:18 [SpringBoard-screens] Screens=lockscreen;
09/03/24 20:29:18 [WiFi Module]
09/03/24 20:29:18 [Telephony] current_rat=Dual; preferred_rat=UMTS;
camped_rat=Unknown; call_status=Inactive; airplane_mode=off; signal=-113
dBm; bars=1;
09/03/24 20:29:18 [Baseband State Durations]
09/03/24 20:29:18 [WiFi] status=off;
09/03/24 20:29:18 [SpringBoard-states] screen_state=unblanked;
lock_state=locked;
09/03/24 20:29:18 [LoggedWake] reason=hold;
09/03/24 20:29:19 [Battery] level=58.32%; voltage=3842 mV; current=-4 mA;
current_capacity=589 mAh; raw_max_capacity=1010 mAh;
charging_state=Inactive; charging_current=0 mA; battery_temp=27.70 C;
adapter_info=0; connected_status=0;
09/03/24 20:29:24 [SpringBoard-states] screen_state=unblanked;
lock_state=unlocked;
09/03/24 20:29:24 [SpringBoard-screens] Screens=homescreen;

The iPhone stores daily Powerlogs (battery, signal, app usage, etc.) in a file called **\Logs\CurrentPowerlog.powerlog** (for the *current* day)

Before a new log is created, the CurrentPowerlog.powerlog file from the previous day (or the day of last usage) is **archived** under: **\Logs\PLArchive**

There is one separate Powerlog file per day.

March 31:	\Logs\PLArchive\PL_2014-03-31-Blabla.powerlog.gz
April 1:	\Logs\PLArchive\PL_2014-04-01-Blabla.powerlog.gz
April 2:	\Logs\PLArchive\PL_2014-04-02-Blabla.powerlog.gz
April 3:	\Logs\CurrentPowerlog.powerlog

The log for **April 3 was never archived**, because **no further Powerlogs** were created after that date.

Why?

April 4–6: Power-on times were too short to trigger logging.
April 11: Possibly due to the RAM/NAND "bug" or manual interference via DFU mode.

DFU Mode | SSH Ramdisk

Example video: https://www.youtube.com/watch?v=1dh5loiX1dU

In low-level DFU mode, it is possible to access an iPhone without leaving obvious traces - even without a jailbreak or passcode - using an SSH ramdisk. This kind of access allows actions such as deleting, modifying, or creating photos, among other things. When in DFU (Device Firmware Update) mode, the iPhone behaves as if the battery were dead: the display stays off, and the device cannot be powered on normally. If the battery is physically replaced or fully depleted, DFU mode is automatically exited. Notably, if the battery drains completely while in DFU mode, no Low Battery Report is generated.

DFU mode is ideal for covert access and manipulation, as the full iOS system - including the logging system (such as Powerlogs) - does not get loaded at all. However, entering DFU mode is timing-sensitive and prone to errors; a slight misstep can cause the phone to boot up normally, which may then generate an unintended startup log.

Wi-Fi | Locations | Accounts

Some email service providers have provided records containing timestamps and IP addresses that indicate user activity or syncs (e.g., email, ActiveSync, POP). These are most likely session logs. In other words, no data was requested from Google or similar services - instead, investigators appear to have directly accessed the K+L email accounts as early as April 2014 and analyzed their activity logs. The women's accounts were analyzed in the Netherlands - Kris's on April 4 and Lisanne's on April 9. Another finding was that Lisanne searched for "Pipeline Trail" and finally for "Pianista Trail" on April 1 around 10:00 AM.

Here's an excerpt:

- **Kris -** Mar 29, 3:22 PM, IP 1 (ISP A) | Mar 30, 10:02 PM, IP 2 (ISP A) | Mar 31, 6:15 PM, IP 2 (ISP A)
- **Lisanne -** Mar 30, 11:08 PM, IP 2 (ISP A) | Mar 31, 8:36 PM, IP 3 (ISP B)

These times are likely in Dutch local time (NLT). If that's the case, Kris would have used public Wi-Fi on the ferry on March 29 at 9:22 AM. By comparing IP addresses, it could have been determined that K+L were using a public Wi-Fi network on March 31 between 1 and 2 PM. That scenario would require Kris to have shut down and restarted the iPhone between 11:15 AM and 1:13 PM on March 31. Overall, this timeline makes more sense.

It's possible that the logged IPs don't belong to the public Wi-Fi routers used in Bocas or Boquete, but rather to proxy servers or CGNAT gateways. These servers are part of the provider's network infrastructure and are typically centralized or located at only a few sites. This would mean that the logged IP addresses could not be directly used to determine the exact location or endpoint - such as a specific public Wi-Fi hotspot. Btw: The iPhone saves all connected Wi-Fi networks in a "List of Known Networks", including the timestamp of last use and the SSID of the Wi-Fi router.

Lisanne's location history was retrieved from her Google account and analyzed. The last recorded location was on **April 1 at 9:57 AM, a few hundred meters north of SbtR** in Alto Boquete. The location may have been determined via GPS, Wi-Fi databases, or mobile networks - all of which affect accuracy (ranging from about 5 meters to several hundred meters). To conserve battery, location isn't logged continuously but based on events - such as movement, Wi-Fi changes, or the use of apps like Google Maps. When the phone is in standby mode, logging may stop altogether.

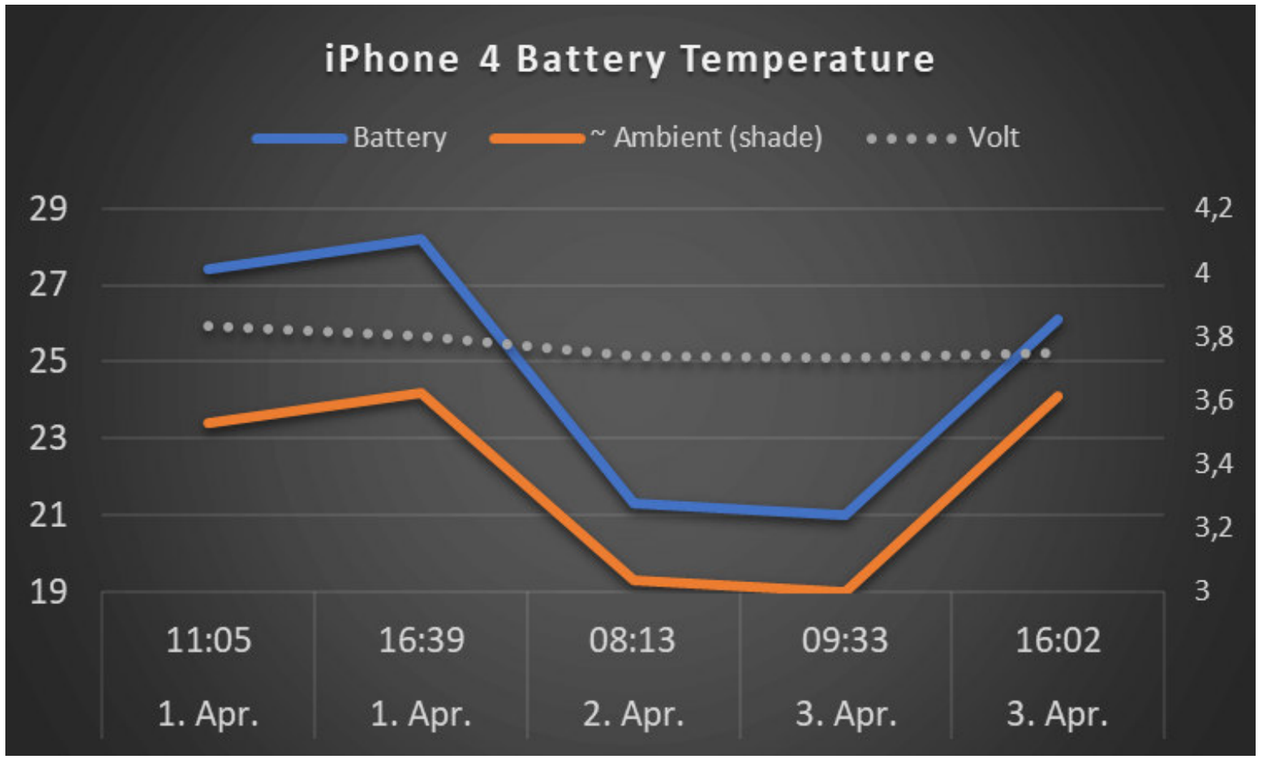
Battery Temperature

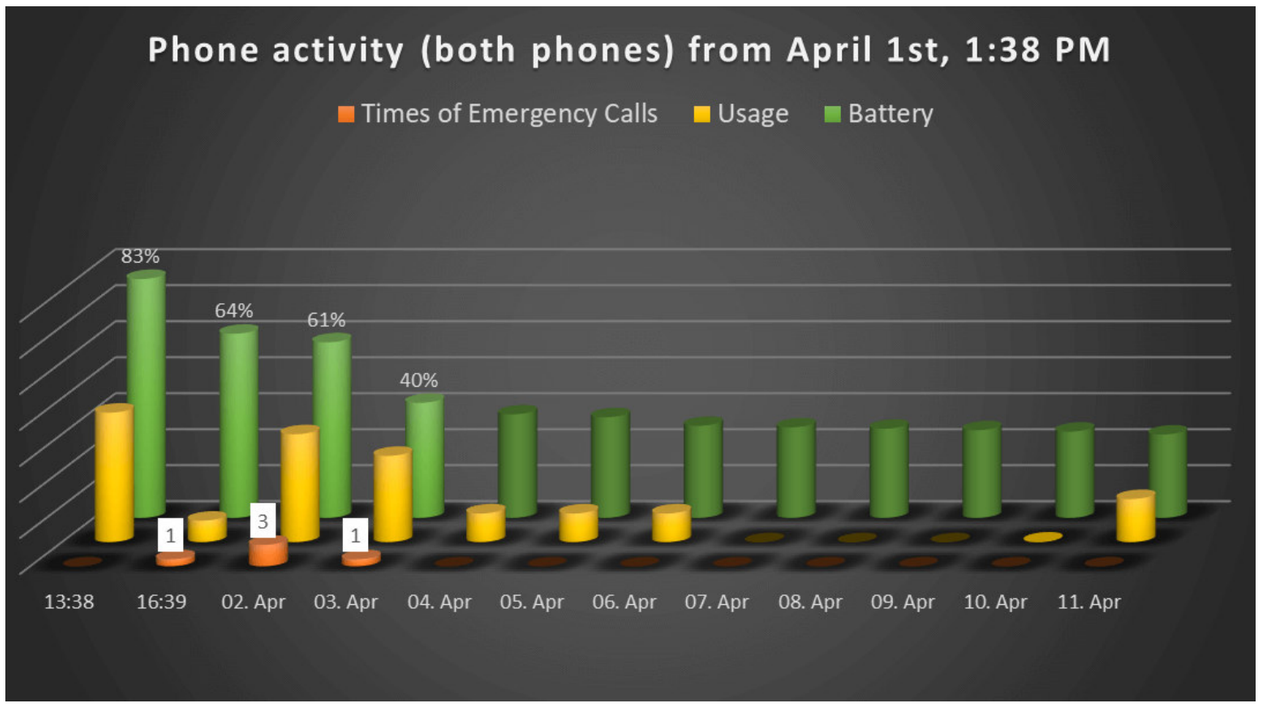
The iPhone 4 logs battery temperature using an internal sensor located near the battery. This is part of the iOS 7's safety features, which can automatically shut down the device and generate a crash report when conditions such as unstable voltage (≤ 3.0 V) or critical temperatures (50–60°C) are detected.

On April 1st, the iPhone was in standby mode and likely spent most of the time inside the backpack, which can lead to some internal heat buildup due to restricted airflow. When the battery temperature is measured just a few seconds after booting up - as was the case on April 2nd and 3rd - there hasn't yet been any significant internal heat buildup. After powering on from a completely shut-down state, the battery temperature is very close to the ambient temperature.

When carried in the pocket of denim shorts, the phone gradually adjusts to body temperature. For instance, if turned off and kept in the pocket for one hour at an ambient temperature of 22 °C, the iPhone can reach approximately 32 °C. However, no such temperature values were recorded in the battery data between April 1st and 3rd.

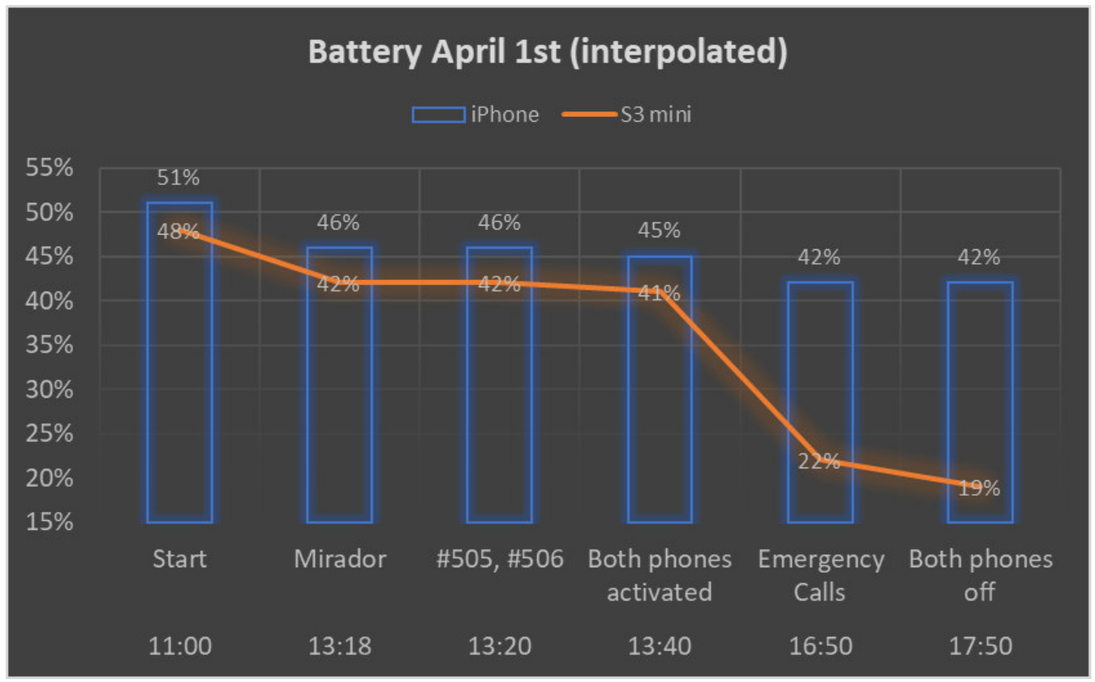
Charts based on phone data





Samsung S3 mini

31.03.2014	13:06	Public Wi-Fi until 13:38	
	13:48	2 photos	
	14:00	Photo gallery open until 15:30	
	16:44	Wi-Fi SbtR until 17:26	
01.04.2014	00:40		64%
	02:12	Received WhatsApp messages from 2:12 to 7:52	
	08:10	Clock app (including alarm function)	
	09:07	First registered Wi-Fi connection	
	09:09	WhatsApp	
	09:32	Facebook	
	09:39	NOS-App NL	
	09:48	First Internet access Android Browser	
	10:10	Last registered Wi-Fi connection	51%
	10:16	Last Internet access Android Browser	
	10:16	**Google Maps active** Cache or Offline Map	
	10:40		49%
	13:14	**Google Maps paused 13:14:10**	
	13:14	Cam App active 13:14:12 - 4 photos likely Mirador	
	13:15	Camera App paused - 1 photo likely Mirador	
	13:40	*19% battery drop by 16:53 - likely longer display use*	41%
	16:51	**Emergency Call 112**	
	16:53		22%
	17:40		19%
	17:52	Power Off	
02.04.2014	06:58	Power On	19%
	06:58	**Emergency Call 112**	
	06:58	Power Off	
	10:52	Power On	
	10:53	**Emergency Call 112 & 911**	19%
	10:53	Power Off	
	13:50	Power On - Power Off	18%
	16:19	Power On	
	16:20		18%
	23:47		6%
03.04.2014	02:21	AccuWeather-App - Activity until 2:47	
	02:51		4%
	07:20		1%
	07:36	Power Off	
04.04.2014	16:50	Power On - Off	1%
	17:00	Power On - Auto Shutdown	0%
05.04.2014	13:14	Startup attempt	
10.04.2014	17:15	Startup attempt	



Sources for Additional or Complementary Analyses of the NFI Report / Phone Data

Book / eBook

[Still Lost in Panama]

Christian Hardinghaus & Annette Nenner

2nd edition 2025 includes findings from this iPhone investigation

- [Imperfect Plan – Forensic Analysis of Phone Data (by Matt)]
- [CamilleG – Official Mobile Phone Data (by Romain C)]