

Forum:[Hack Forums](#)

Thread: [EXPLOITATION OF SEIZED IPHONES: Investigators' tools are advancing, and quickly.](#)

Th3HulK - October 15, 2026, 7:22 pm

Cellebrite and GrayKey, the two main players in law-enforcement extraction software, have both unveiled new capabilities in recent months.

In March 2026, Cellebrite announced new methods for accessing iPhone 11 through 16 running iOS 26 or later — even when locked, provided the device is in AFU state. The company also announced support for the iPhone 17, without guaranteeing the same extraction capabilities.

Then in early October, a 404 Media investigation revealed that GrayKey would be able to preserve AFU-associated extraction capabilities even after an iPhone restart.

Quick Reminder: AFU vs. BFU

When an iPhone has just booted, it's in BFU (Before First Unlock). Until the owner enters the passcode, much of the encryption key material is unavailable, making data particularly hard to extract.

As soon as it's unlocked once, it switches to AFU (After First Unlock). Even when the screen locks again, certain cryptographic keys stay accessible to the system so apps and services keep working.

That's what interests investigators. By exploiting specific vulnerabilities, their tools can potentially reach data that would be inaccessible in BFU: messages, histories, files, app databases, and so on. Temporary data matters too — caches, location info, activity traces, anything sitting in RAM. It can be forensically valuable, but some of it disappears or becomes unreachable after a restart.

Apple Saw This Coming

Since iOS 18.1, an iPhone can automatically restart after roughly 72 hours without unlocking. The goal is partly to return it to BFU and make certain data much harder to extract.

Picture an iPhone seized during a search: locked, passcode unknown, but still in AFU. If it restarts, certain extraction possibilities vanish. That's exactly the limitation GrayKey and Cellebrite now claim to bypass.

GrayKey: Preserving AFU Across a Restart

According to an internal training video revealed by 404 Media, Magnet Forensics developed two features: GrayKey Preserve and Evidence Preservation Mode. The manufacturer claims it can preserve AFU-associated extraction capabilities even after a restart or power loss, and retain certain temporary data — cached locations, recently deleted photos, and iMessage-related elements.

Cellebrite: Same Objective

In spring 2026, Cellebrite introduced Safeguard Mode, designed to preserve an iPhone's exploitation possibilities despite automatic restarts. It also claims new capabilities for accessing locked devices running iOS 26.

What This Means for Seized Phones

Quite a lot, and it changes the game. Until now, investigators risked losing their exploitation window when an iPhone restarted and reverted to BFU. Now they could seize a phone in AFU, preserve the favorable conditions for extraction, and exploit it days or weeks later — which makes it far easier to transfer devices to specialized labs and preserve digital elements at risk of disappearing.

That said, caution is warranted. The technical mechanisms remain secret, and their effectiveness across all recent iPhones hasn't been publicly demonstrated. These announcements don't mean every iPhone is unlockable without a passcode. But they show that forensic vendors are no longer just chasing access to data — they're now trying to sustainably preserve the conditions that make extraction possible.

Bastille - *October 15, 2026, 10:05 pm*

This is a really interesting topic, i've made a thread about smartphones who were accessible through those technologies and which ones were safe in 2025 :

<https://hackforums.net/showthread.php?tid=6296678>

GraphenOS was the best at the time I've made the thread, I guess they're still the best, but they've recently shared that they're not planning to make it available on Pixel 11, maybe due to some components that weren't in the previous phones

ssuzuki53 - *October 16, 2026, 4:33 pm*

Thank for sharing dude..very information.

Th3HulK - *October 17, 2026, 4:02 am*

(Oct 15, 2026 10:05 PM)Bastille Wrote: [\[CITE\]](#) This is a really interesting topic, i've made a thread about smartphones who were accessible through those technologies and which ones were safe in 2025 : <https://hackforums.net/showthread.php?tid=6296678>

GraphenOS was the best at the time I've made the thread, I guess they're still the best, but they've recently shared that they're not planning to make it available on Pixel 11, maybe due to some components that weren't in the previous phones

Yea, went through your thread too, you did a great job, those guy are getting better at it everyday