



Offline iOS Tracking and Remote Wiping

By:

Mitch Kajzer (St. Joseph County, IN Cyber Crimes Unit)

From the proceedings of

The Digital Forensic Research Conference

DFRWS USA 2022

July 11-14, 2022

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment.

As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

<https://dfrws.org>

iOS Offline Tracking and Wiping



07/11/2022



 **DFRWS2021**
VIRTUAL USA

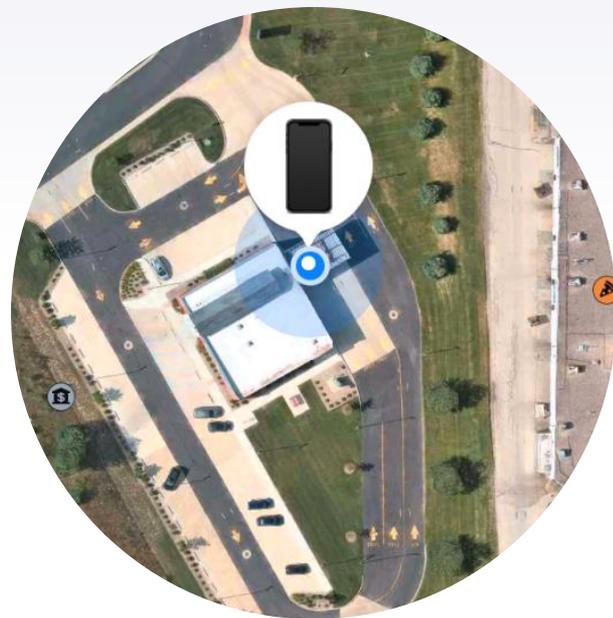
Mitch Kajzer

- ▶ University of Notre Dame. Associate Professor. Center for Research Computing
- ▶ St. Joseph County (IN) Prosecutor. Executive Director of the Cyber Crimes Unit
- ▶ Retired from the South Bend (IN) Police Department
- ▶ 33rd year in law enforcement



Outline

- ▶ Explanation of offline tracking and the U1 chip
- ▶ Implications of the chip
- ▶ Testing setup, procedure, and results
- ▶ Best practices



Offline Tracking

- ▶ Certain powered-down iOS devices may still be trackable
- ▶ Powered off doesn't really mean powered off
- ▶ When powering down a compatible device for the first time, it displays a pop up informing the user that the phone remains findable

iPhone Remains Findable After Power Off

Find My helps you locate this iPhone when it is lost or stolen, even after power off.

The location is visible in Find My on your other devices, and to people in Family Sharing you share location with.

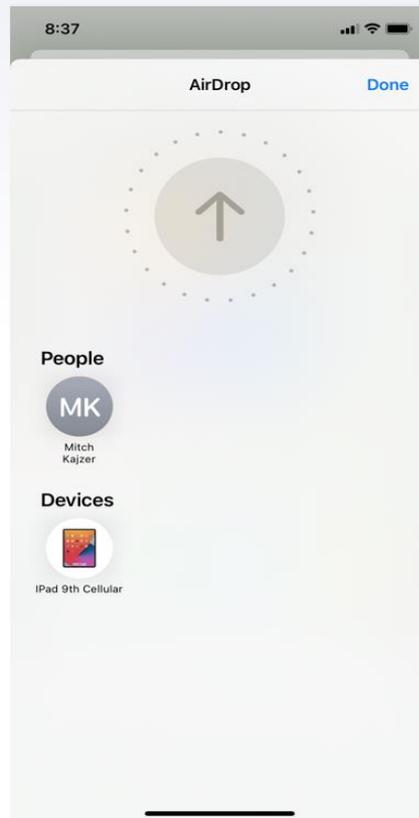
You can change this "Find My network" functionality by going to Find My in Settings.

OK

Cancel

U1 Chip

- ▶ Apple: “Used for spatial awareness. Allows the iPhone to understand its precise location relative to other nearby U1-equipped Apple devices.”



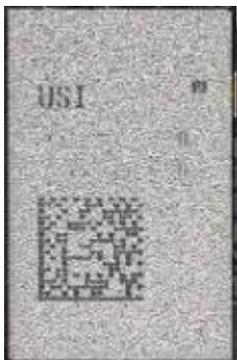
Can you be more precise? Yes.

The new Apple-designed U1 chip uses Ultra Wideband technology for spatial awareness — allowing iPhone 11 Pro to precisely locate other U1-equipped Apple devices. It's like adding another sense to iPhone, and it's going to lead to amazing new capabilities.

With U1 and iOS 13, you can point your iPhone toward someone else's, and AirDrop will prioritize that device so you can share files faster.⁴ And that's just the beginning.

U1 Chip

- ▶ Apple: “Used for spatial awareness. Allows the iPhone to understand its precise location relative to other nearby U1-equipped Apple devices.”

An iPhone screen displaying the AirDrop interface. At the top, it says 'AirDrop' with 'Cancel' and 'Done' buttons. Below that is a large circular profile picture of Hugo Verweij, with his name and 'Tap to Share' below it. Underneath is a section titled 'People' with a grid of eight circular profile pictures and names: Hugo Verweij, Candace Salinas, Dean Orlosky, Jackelyn Perra, Kirk von Rohr, Aled Evans, Priyanka Kanse, and Charles Parrish. At the bottom is a section titled 'Other People' with four circular icons and names: Demi's iMac Pro, Matty's iPhone, Fiona's iPhone, and John's iPhone.

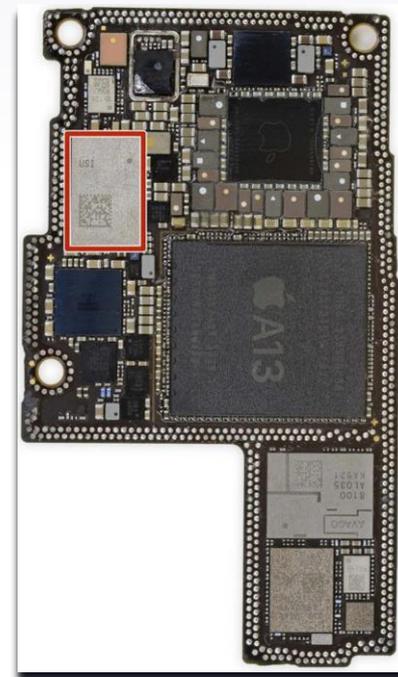
Can you be more precise? Yes.

The new Apple-designed U1 chip uses Ultra Wideband technology for spatial awareness — allowing iPhone 11 Pro to precisely locate other U1-equipped Apple devices. It's like adding another sense to iPhone, and it's going to lead to amazing new capabilities.

With U1 and iOS 13, you can point your iPhone toward someone else's, and AirDrop will prioritize that device so you can share files faster.⁴ And that's just the beginning.

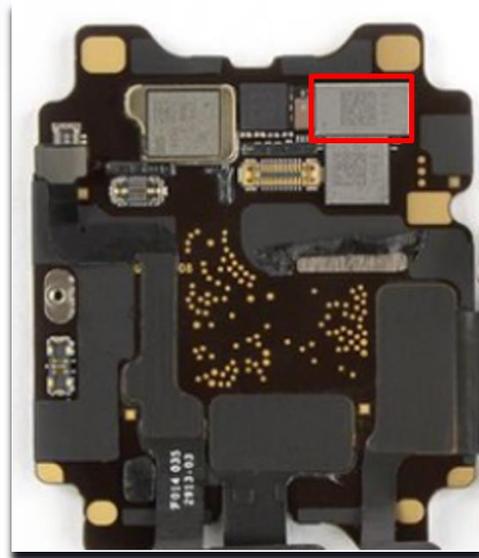
U1 Chip

- ▶ Compatible Devices
- ▶ iPhone 11



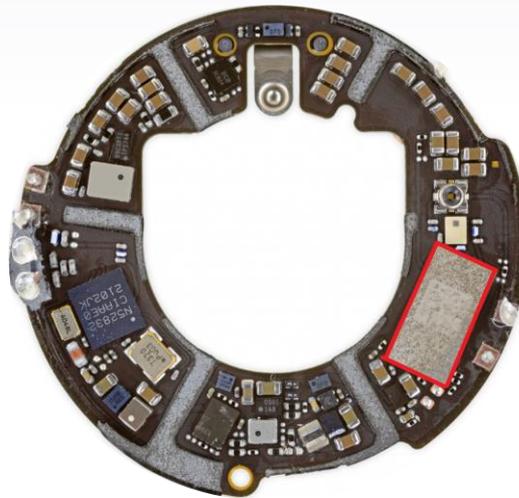
U1 Chip

- ▶ Compatible Devices
- ▶ Apple Watch 6



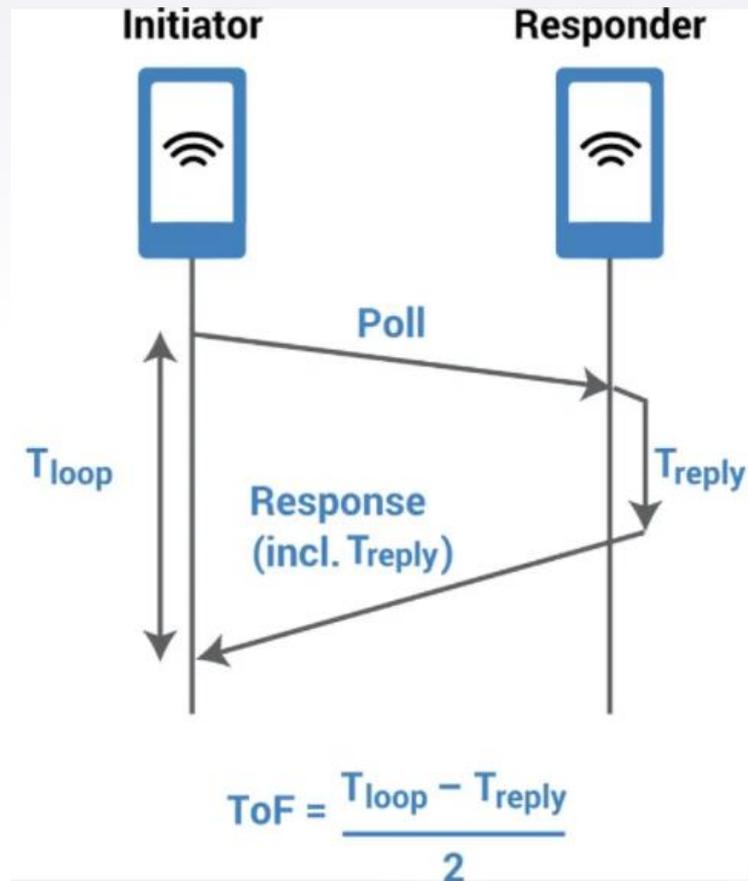
U1 Chip

- ▶ Compatible Devices
- ▶ AirTag



Ultra-Wideband

- ▶ Short-range wireless communications protocol
- ▶ Very low energy usage
- ▶ “Continuously scanning radar that can precisely lock onto an object, discover it’s location, and communicate with it.”
- ▶ Uses high-frequency, low-range pulse radio signals. Much more accurate than GPS or Classic Bluetooth



Capabilities of the Chip

- ▶ Very precise spatial and directional data
- ▶ It knows what other chips are around it and how far away they are.
- ▶ Accuracy of less than four inches
- ▶ Line of sight range is over 600feet
- ▶ Apple in promotional literature: "Think of it as GPS at the scale of your living room."

Offline Tracking

- ▶ Offline tracking is essentially crowdsourcing using Ultra-Wideband
- ▶ To track an offline device, you must either be logged into the iCloud account of the device or using an iOS device configured with the same iCloud account
- ▶ Uses asymmetric encryption



Offline Tracking

- ▶ Offline Device
 - ▶ Using Ultra-Wideband, the offline device continuously sends out pulses.
 - ▶ These pulses include the Public Key of the offline device.
- ▶ Devices in the Area
 - ▶ Picks up the Public Key from the offline device.
 - ▶ Records the location and encrypts it using the Public Key from the offline device.
 - ▶ The encrypted location, along with a hash of the Public Key, is transmitted to Apple.

Offline Tracking

- ▶ Tracking Device or iCloud
 - ▶ When you click on FindMy, the hash of the Public Key is sent to Apple. They search their database for any matches.
 - ▶ When a match is found, it sends the encrypted location data that it received from the snitch device to the tracking device.
 - ▶ FindMy on the tracking device decrypts it using the Private Key.
- ▶ What can Apple see and what records do they keep?
 - ▶ Nothing. Since they do not know the Private Key, they cannot decrypt any location data. There is no historical data kept.

Implications and Questions

- ▶ Remote Wiping
 - ▶ The wipe command uses crypto-shredding and erases all encryption keys.
 - ▶ Data is left encrypted and inaccessible.
 - ▶ Can a device be wiped remotely using Ultra-Wideband?



Testing Materials and Setup

Target Device

Apple iPhone 11

iOS 15.0.2

Chip: A13 Bionic and U1

Cellular and WiFi

Name: iPhone 11 Cellular

Cy [REDACTED] s.org

Friendly Device

Apple iPad 9th Generation

iOS 15.1

Chip: A12 Bionic 64 bit

Cellular and WiFi

Name: iPad 9th Cellular

Cy [REDACTED] s.org

Unknown (snitch) Devices

iPhone XR

iPhone 8

iPhone 13 Pro

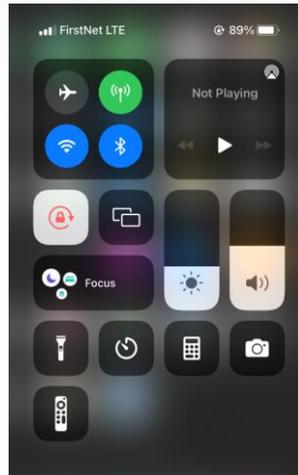
iPad 6th Generation



▶ Radio Terminology

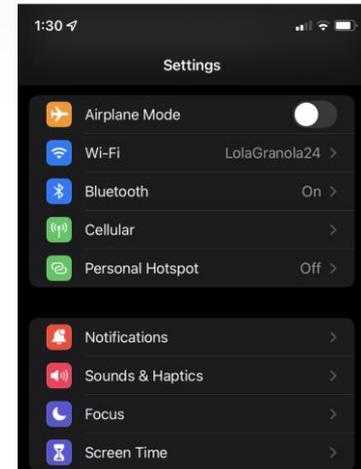
Disabled

- ▶ Via the Control Center.
- ▶ Typically for 24 hours. Then automatically reenabled.



Turned Off

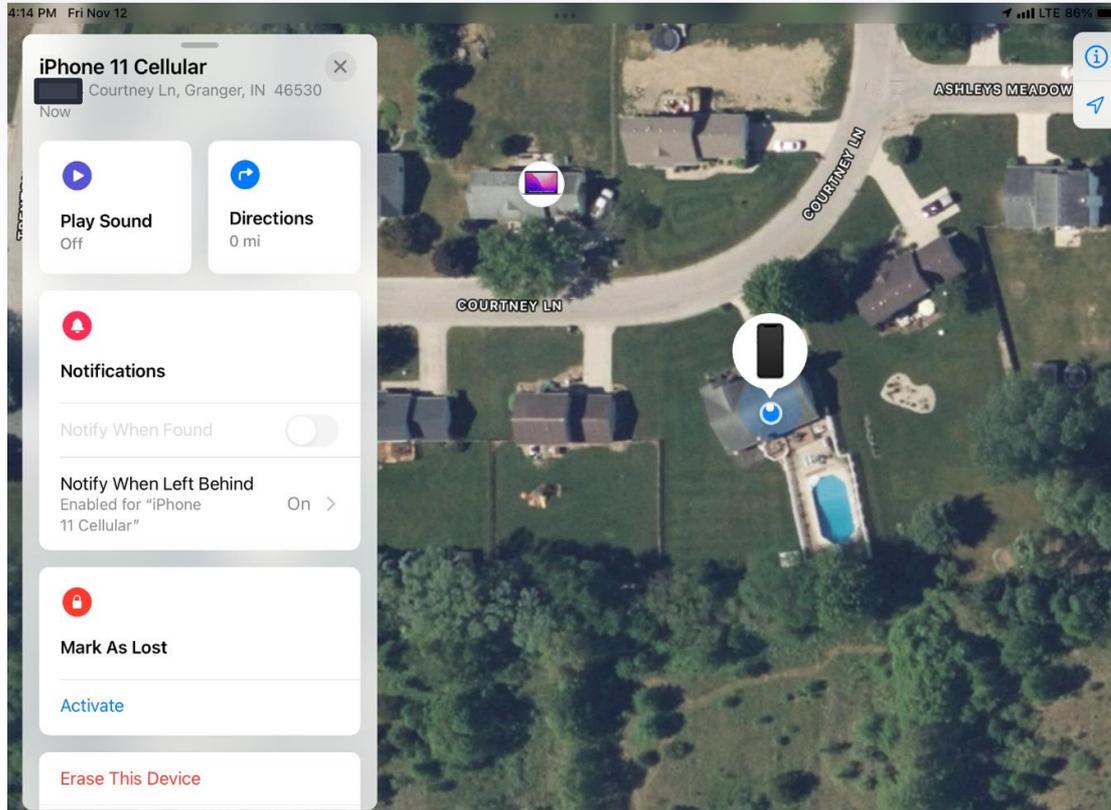
- ▶ Via Settings.
- ▶ Remains off until turned on again by the user.



▶ Tracking Scenario 1

- ▶ All radios left on
- ▶ Phone powered down at Notre Dame.
- ▶ Drove to Granger, IN
- ▶ Friendly Device and Snitch Devices in the car

Tracking Scenario 1

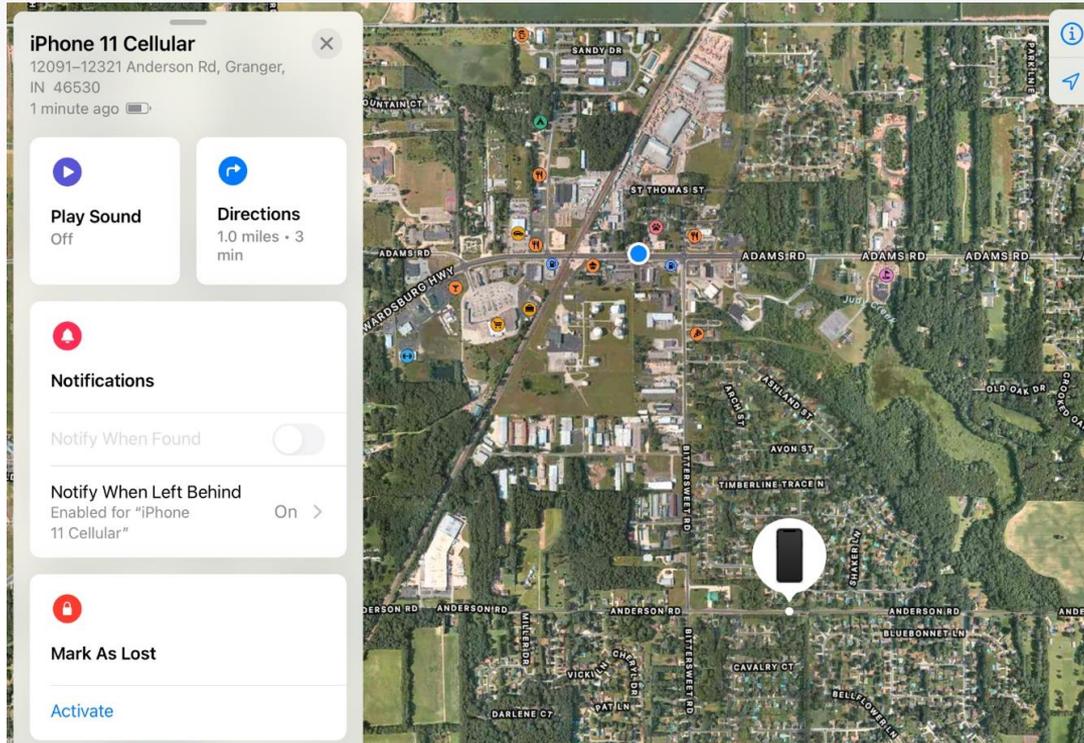


▶ Tracking Scenario 2

- ▶ All radios left on
- ▶ Phone powered down at home in Granger
- ▶ Taken for a drive
- ▶ One Friendly Device and three Snitch Devices in the car

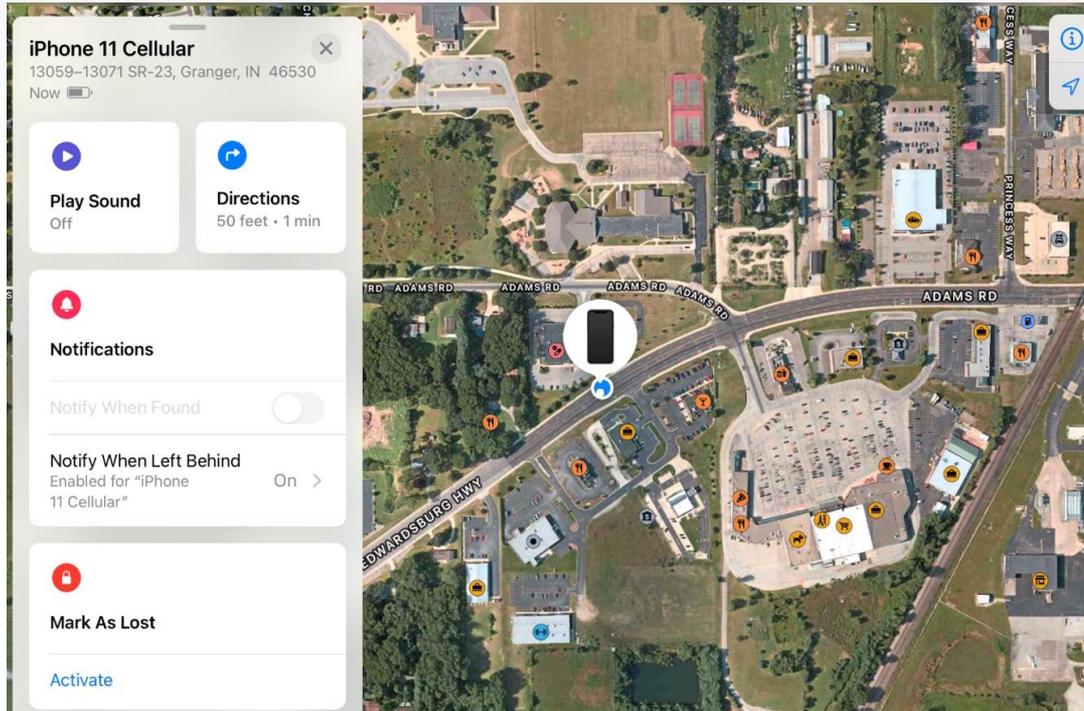
Tracking Scenario 2

- ▶ Initial tracking delay of about one-minute

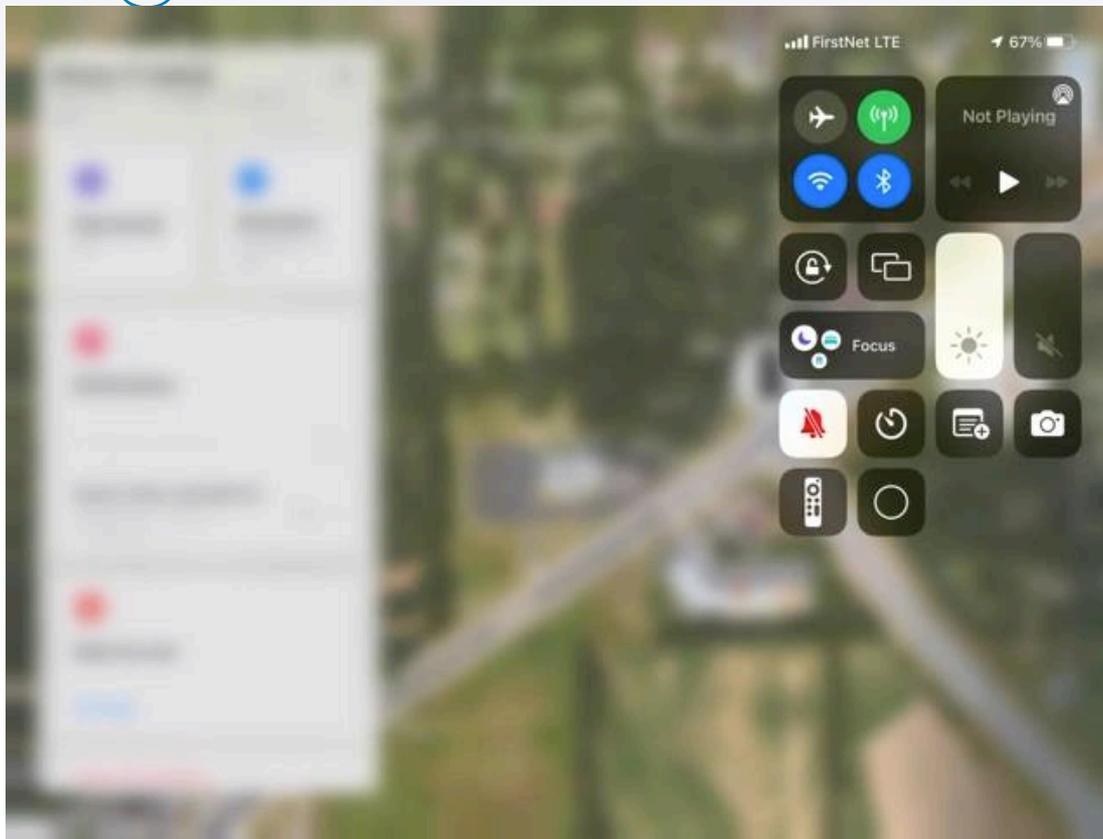


Tracking Scenario 2

- ▶ After about one minute, Ultra-Wideband locked on to the offline device



▶ Tracking Scenario 2



Powered Off Tracking



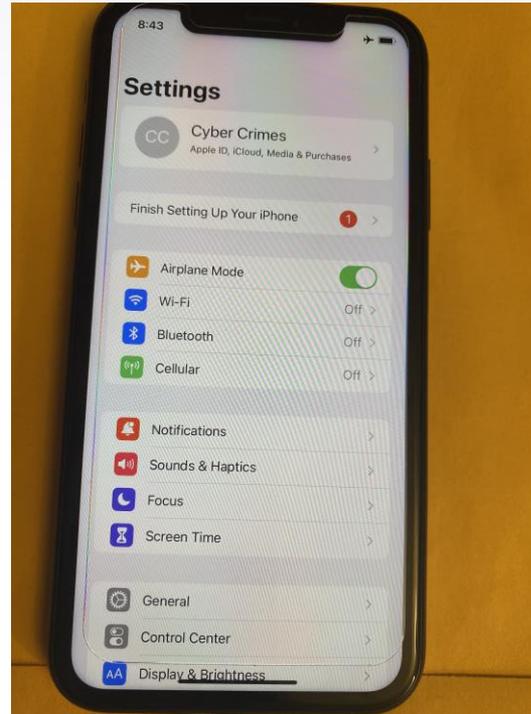
| Powered-off State | Tracked? |
|-------------------------------------|------------|
| All radios left on | Yes |
| Airplane Mode | Yes |
| Bluetooth disabled (Control Center) | Yes |
| Bluetooth turned off (Settings) | No |
| All radios turned off | No |

Powered Off Tracking

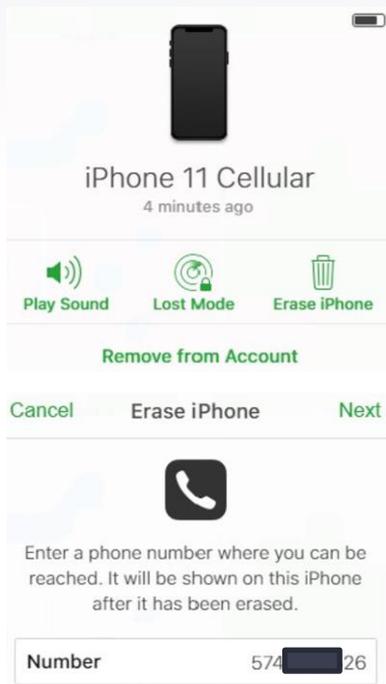
Tracked



Not Tracked



Let's Wipe Some Phones



iPhone 11 Cellular
4 minutes ago

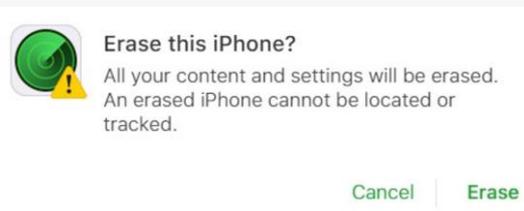
Play Sound Lost Mode Erase iPhone

Remove from Account

Cancel Erase iPhone Next

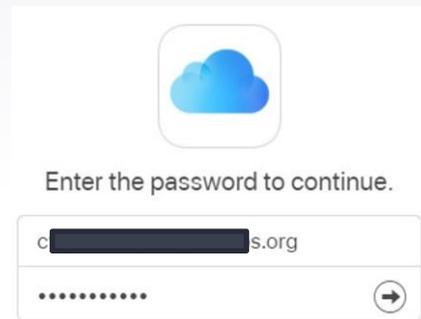
Enter a phone number where you can be reached. It will be shown on this iPhone after it has been erased.

Number 574 [redacted] 26



Erase this iPhone?
All your content and settings will be erased.
An erased iPhone cannot be located or tracked.

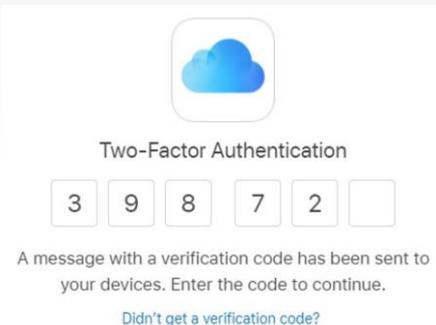
Cancel Erase



Enter the password to continue.

c [redacted] s.org

.....

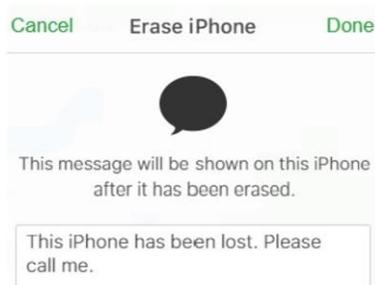


Two-Factor Authentication

3 9 8 7 2

A message with a verification code has been sent to your devices. Enter the code to continue.

[Didn't get a verification code?](#)



Cancel Erase iPhone Done

This message will be shown on this iPhone after it has been erased.

This iPhone has been lost. Please call me.

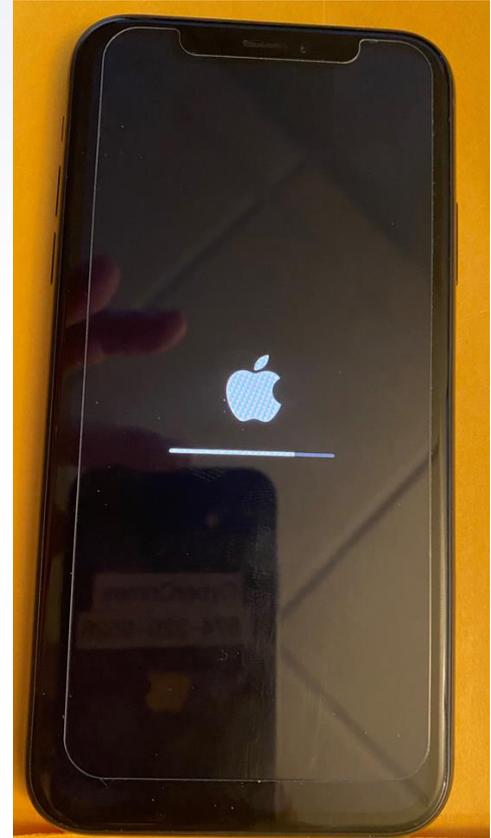


Erase Started
If you recover this iPhone, some services may be temporarily unavailable after it is restored.

OK

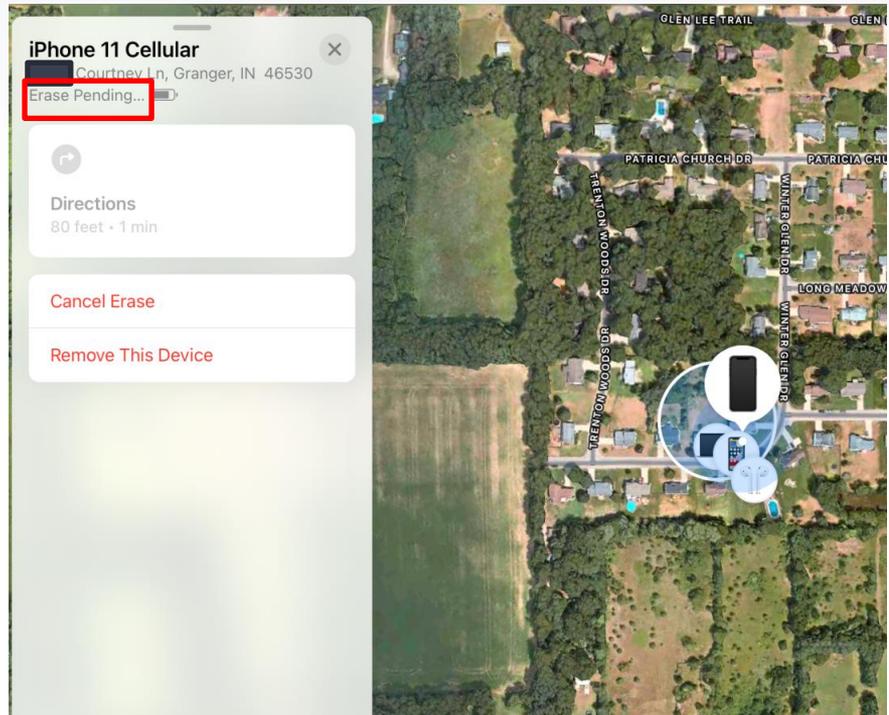
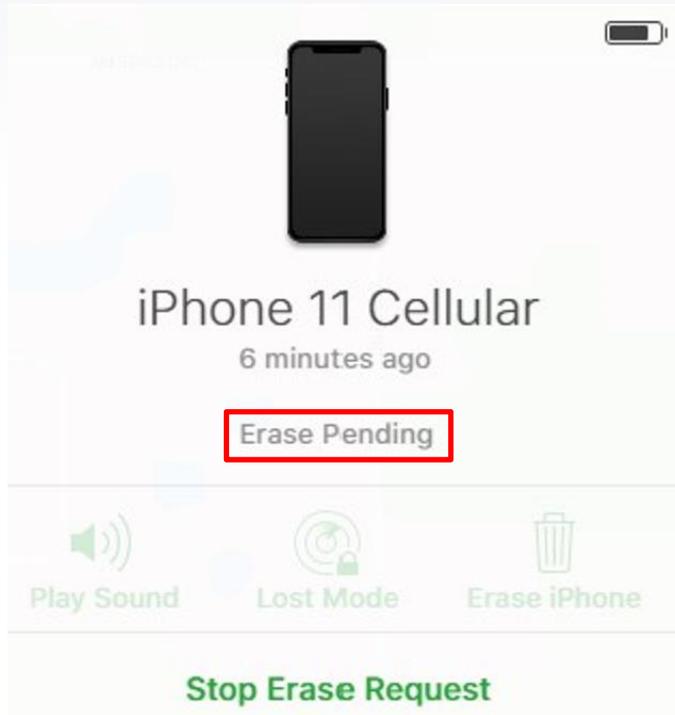
Wiping Scenario

- ▶ Phone powered on with all radios enabled



Wiping Scenario

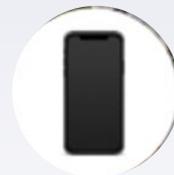
- ▶ Phone powered off with all radios turned off



▶ Wiping Scenario

- ▶ With the wipe command pending, the phone was then powered on.
- ▶ (Reminder. When the phone was powered off, all radios were off).
- ▶ The phone was not wiped when it powered on

Powered Off Wiping



| Powered-off State | Wiped when Powered on? |
|-------------------------------------|------------------------|
| All radios left on | Yes |
| Airplane Mode | No |
| Bluetooth disabled (Control Center) | No |
| Bluetooth turned off (Settings) | No |
| All radios turned off | No |

Summary: Tracking and Wiping

| Powered-on and Powered-off Devices | Tracked? | Wiped? |
|-------------------------------------|------------|------------|
| All radios active | Yes | Yes |
| Airplane Mode | Yes | No |
| Bluetooth disabled (Control Center) | Yes | No |
| Bluetooth turned off (Settings) | No | No |
| All radios turned off | No | No |
| Faraday bag | No | No |

Summary

- ▶ The device remains trackable unless Bluetooth is turned off from settings. Disabling it from the Control Center only disables Classic Bluetooth, not Ultra-Wideband.
- ▶ If a wipe command is sent to the device, it will not wipe unless it successfully connects to a cellular or Wi-Fi network.
- ▶ The wipe command is not executed on the device via Ultra-Wideband.
- ▶ Is the wipe command delivered via Ultra-Wideband?

Best Practices

- ▶ If you have the passcode, enter Settings and turn off all radios. This is the ideal situation as the phone will not be trackable and cannot be sent the wipe command.
- ▶ If you do not have the passcode, place the phone into Airplane Mode. The phone will still be trackable, but it will not accept the wipe command.
- ▶ If you cannot get the phone into Airplane Mode, place into a Faraday Bag/Box.
- ▶ When GrayKey accesses the phone, it turns off all radios.

Best Practices

- ▶ Currently, devices will not execute the wipe command through Ultra-Wideband.
- ▶ What if that changes?



Best Practices

- ▶ Place GrayKey into a Faraday Box



Best Practices

- ▶ Place GrayKey into a Faraday Box



THANK YOU!

▶ mkajzer@stjoepros.org

