How To Search Your Environment For Bluetooth Tracking Devices

Maggie Delano, mdelano1@swarthmore.edu

Purpose of this Guide

This guide is for anyone who is concerned about Bluetooth devices like Apple AirTags tracking you or someone you care about without their consent. It will discuss how these trackers can be misused and what you can do about it.

Disclaimers

This guide will provide options for searching for and disabling Bluetooth tracker devices. You should always prioritize your own safety, as disabling or destroying devices could alert the person tracking you, and they could escalate their abusive behavior. You should also consider the importance of documenting what is happening, especially if the legal system is involved in some way. Trust your instincts on what is right for you. You can contact a national helpline to be connected with resources in your area.

Bluetooth Devices for Location Tracking

Bluetooth trackers like Tiles and AirTags have become increasingly popular to help people keep track of their possessions such as car keys and wallets. They may also be used to keep track of kids or pets. However, these trackers can also be used to track another person's location without their consent. When someone places a Tile or AirTag in another person's car, purse, or on their person, that person's location can be updated whenever that tracker connects to another device on the network. These trackers are small and can be hard to detect. While Apple has implemented some security features to prevent stalking, notifications are limited to iOS devices, and can take several hours to trigger. There are no such features for the Tile device (though it is in the works). You have a right to privacy. If you are concerned someone may be tracking you, you can use Bluetooth scanning to help search your surroundings and identify potential trackers that are being used without your consent.

Signs Someone Might Be Using a Bluetooth Tracker

The most important thing you can do is trust your instincts. If a person seems to run into you frequently, or seems to know where you have been, there is a chance they may be tracking your location using a Bluetooth tracker or other method. If you suspect someone might be tracking your location, you can use this guide to search for Bluetooth trackers. However, Bluetooth trackers are just one way of tracking location. This Location Tracking guide has information on other methods of location tracking.

How To: Manually Searching For Bluetooth Trackers

This section will be divided based on your phone operating system (Android or iOS). Instructions will be given to search for both a Tile tracker and for an Apple AirTag.

iOS

Steps:

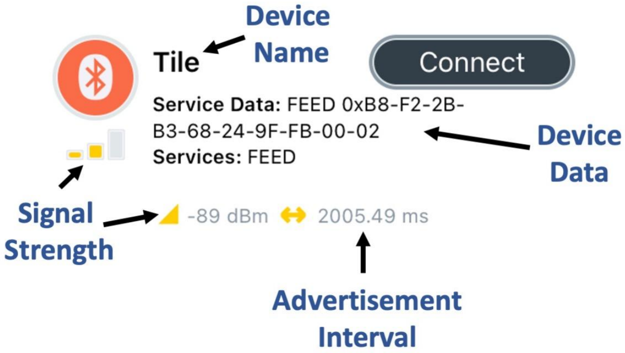
1. Download a free bluetooth scanning application
2. Use the scanning application to search for and identify particular Bluetooth trackers
3. (Optional) repeat the scan in different locations and at different times to confirm the tracker is travelling with you
4. (Optional) search your surroundings for the tracker
5. (Optional) once detected, disable the tracker

Downloading a free bluetooth scanning application

To actively search for a Tile or an Apple AirTag, you can download a bluetooth scanning app. While there are many options available on the App Store, the nRF connect app is recommended as it has features that make the AirTags easier to identify.

Searching for and Identifying Bluetooth Tracking Devices

After you download and open the nRF connect app, the app should automatically begin scanning for Bluetooth devices nearby. Depending on the location, there could be a handful to over 100 devices. This in itself is not necessarily a cause for alarm; Bluetooth is used by many smart devices such as TVs, speakers, phones and laptops. The goal here will be to look specifically for devices that are likely used for tracking location. After the app scans for nearby Bluetooth devices, a list of devices should display on the screen. Each device will have different information displayed in the list, as shown in the Figure below. The device name (if present) will show up at the top of the entry, device data will show up in the middle, and signal strength and the Bluetooth advertisement interval will be displayed to the side and to the bottom of each entry.



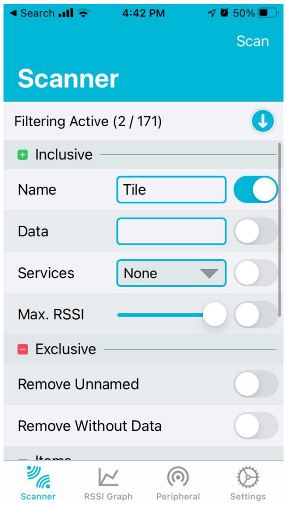
Tile

Service Data: FEED 0xB8-F2-2B-B3-68-24-9F-FB-00-02
Services: FEED

-89 dBm 2005.49 ms

Figure 1: Example Bluetooth device shown in the nRF connect app.

Once you have begun scanning, you can start looking for devices that might be Bluetooth trackers. The two most common devices are the Tile devices and the Apple AirTag. Tile devices are very easy to scan for. If there are only a few devices, you can scroll through the list manually and look for devices that have the name “Tile” (see image above). If there are many devices, scroll to the top of the list and click the arrow on the right to bring down the filter option. There you can enter the name “Tile” and click the slider to the right to search for only devices with the name “Tile.” Click the window again to close the filter panel.



Filtering Active (2 / 171)

Inclusive

Name: Tile ●

Data: ○

Services: None ○

Max. RSSI ○

Exclusive

Remove Unnamed ○

Remove Without Data ○

Figure 2: Example of how to use the filter screen to search for Tile devices.

AirTags are harder to scan for as they don’t have a name the way the Tile does; instead the name shows up as “N/A” (see Figure 3). Instead, you will have to look for an AirTag based on its advertisement interval, which is the number to the right of the signal strength. An AirTag should show no name (N/A) but have an advertisement interval of approximately 2000 ms. (Note: because the AirTag has no name (N/A), there is a chance for “false positives” where the device is actually something else. You can verify by following similar instructions using an Android device). After you have completed your first scan, jump to the section on what you should do after you complete your first scan.

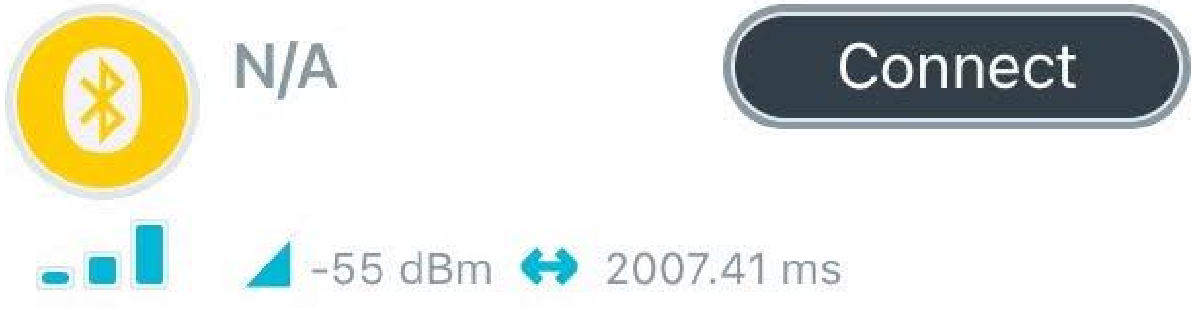


FIgure 3: Example AirTag. Note that the AirTag does not have a name (N/A), but it can be identified based on the signal strength (three bars, suggesting close proximity) and the advertisement interval (about 2000 ms).

Android

Steps:

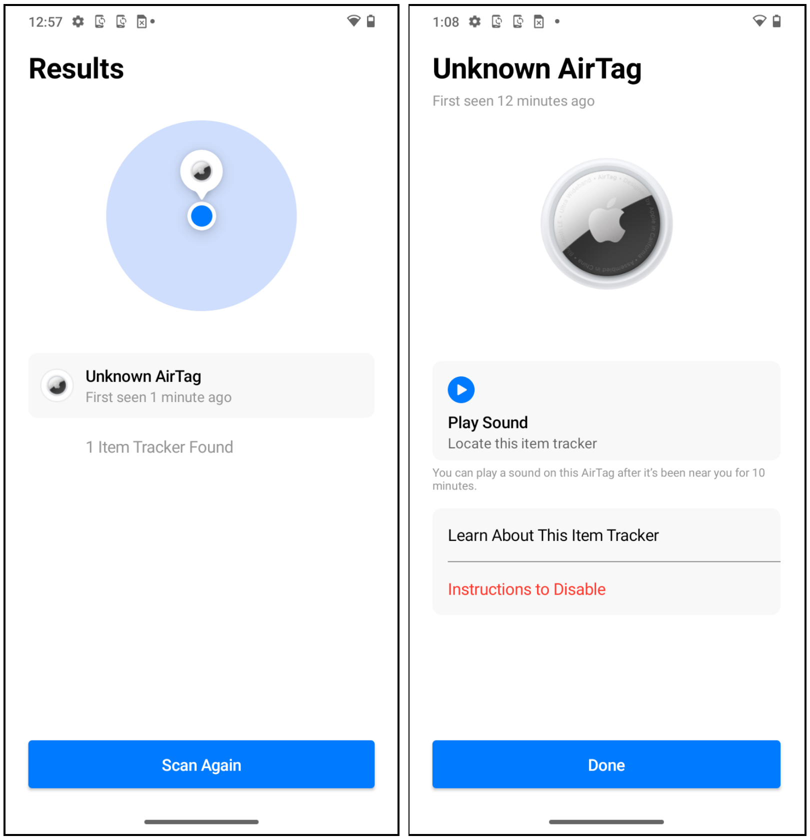
1. Download a free bluetooth scanning application
2. Use the scanning application to search for and identify particular Bluetooth trackers
3. (Optional) repeat the scan in different locations and at different times to confirm the tracker is travelling with you
4. (Optional) search your surroundings for the tracker
5. (Optional) once detected, disable the tracker

Downloading a free bluetooth scanning application

To actively search for a Tile or an Apple AirTag, you can download a bluetooth scanning app. The nRF connect app or similar bluetooth scanning apps can scan for devices of all types, but are harder to use. There are also AirTag specific apps you can download, including the Tracker Detect app that is made by Apple.

Searching for AirTags And Other Devices Using Apple's Tracker Detect App

Apple has written a Tracker Detect app specifically for AirTags and other trackers that use Apple's Find My network. To get started, hit the scan button on the app. If there are any AirTags near you they will show up on the screen:



12:57

Results

Unknown AirTag
First seen 1 minute ago

1 Item Tracker Found

1:08

Unknown AirTag
First seen 12 minutes ago

Play Sound
Locate this item tracker

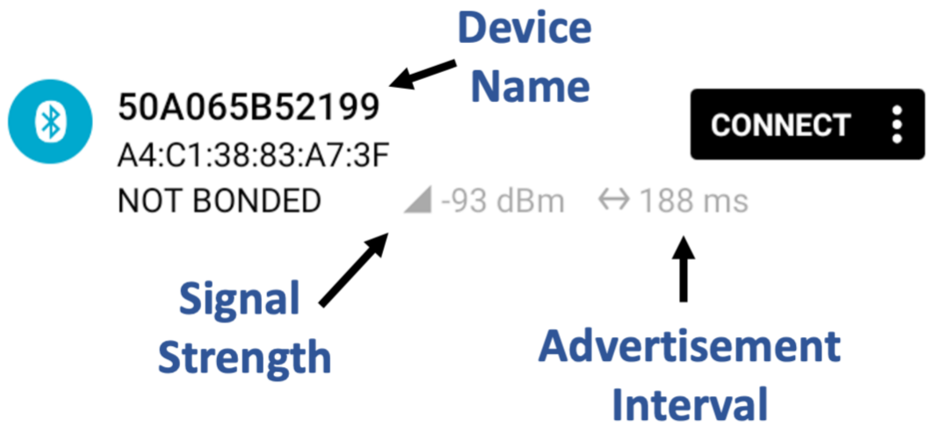
You can play a sound on this AirTag after it's been near you for 10 minutes.

Figure 4: An unknown AirTag showing up on Apple's Tracker Detector App for Android. The ability to locate a tracker shows up after the tracker has been in range for 10 minutes. Click the blue play button to trigger a sound.

Once an AirTag has been detected, you have to wait 10 minutes before you can activate a sound on the device. (This is to prevent activating a sound on a nearby device that is passing by but does not stay in range). When the activate sound button turns blue, you can press it and a short, 3 second sound will trigger on the AirTag. You can repeat this process as needed to try to locate the AirTag around you. Proceed to Searching Your Surroundings for A Location Tracker.

Searching for and Identifying Bluetooth Tracking Devices Using the nRF Connect App

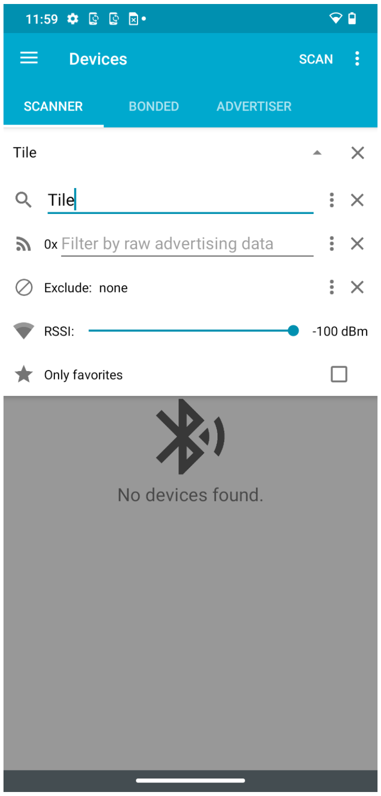
After you download and open the nRF connect app, the app should automatically begin scanning for Bluetooth devices nearby. Depending on the location, there could be a handful to over 100 devices. This in itself is not necessarily a cause for alarm; Bluetooth is used by many smart devices such as TVs, speakers, phones and laptops. The goal here will be to look specifically for devices that are likely used for tracking location. After the app scans for nearby Bluetooth devices, a list of devices should display on the screen. Each device will have different information displayed in the list, as shown in the figure below. The device name (if present) will show up at the top of the entry, device data will show up to the left, and signal strength and the Bluetooth advertisement interval will be displayed on the bottom. Signal strength is represented using a unit called dBm (decibel-milliwatts). Values that are less negative correspond to higher signal strength. So something that is -30 dBm has a higher signal strength than something -90 dBm. This does not exactly correspond to the distance to the device, but is a good proxy.



50A065B52199
A4:C1:38:83:A7:3F
NOT BONDED -93 dBm ↔ 188 ms

Figure 6: Example Bluetooth device shown in the nRF connect app on Android.

Once you have begun scanning, you can start looking for devices that might be Bluetooth trackers. The two most common devices are the Tile devices and the Apple AirTag. Tile devices are very easy to scan for. If there are only a few devices, you can scroll through the list manually and look for devices that have the name “Tile.” If there are many devices, click the arrow on the top right to bring down the filter option. There you can enter the name “Tile.” Click the arrow again to close the filter panel.



Tile

Tile

0x Filter by raw advertising data

Exclude: none

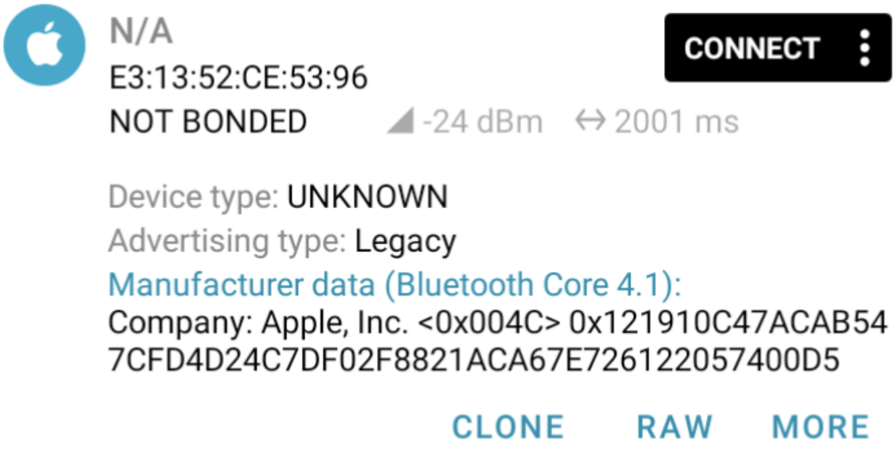
RSSI: -100 dBm

Only favorites □

No devices found.

Figure 7: Example of how to use the filter screen to search for Tile devices.

AirTags are harder to scan for as they don't have a name the way the Tile does; instead the name shows up as "N/A" (see Figure 8). Instead, you will have to look for an AirTag based on its advertisement interval, which is the number to the right of the signal strength. An AirTag should show no name (N/A) but have an advertisement interval of approximately 2000 ms.



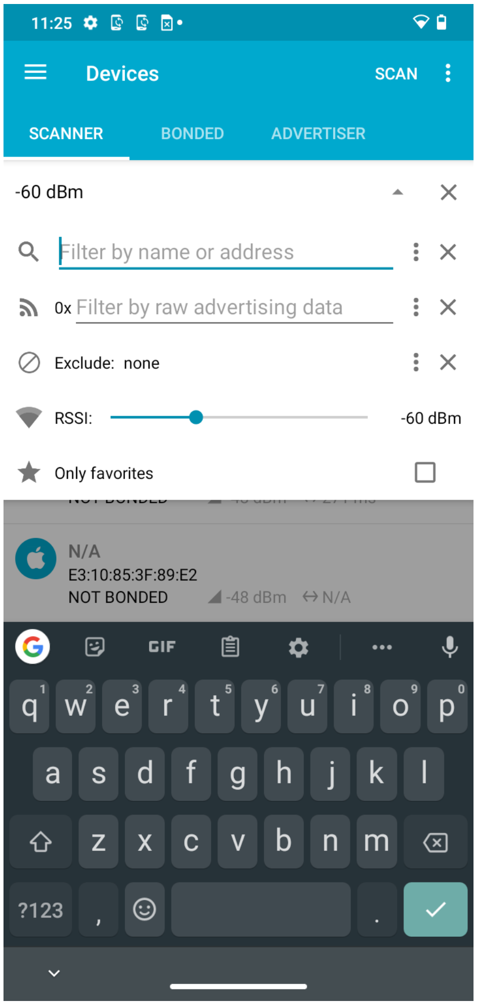
N/A
E3:13:52:CE:53:96
NOT BONDED -24 dBm ↔ 2001 ms

Device type: UNKNOWN
Advertising type: Legacy
Manufacturer data (Bluetooth Core 4.1):
Company: Apple, Inc. <0x004C> 0x121910C47ACAB54
7CFD4D24C7DF02F8821ACA67E726122057400D5

Figure 8: Example AirTag as shown on the Android nRF Connect App (when you click on it to see more information). Note that the AirTag does not have a name (N/A), but it can be identified

based on the signal strength (-24 dBm, suggesting close proximity) and the advertisement interval (about 2000 ms).

If there are many devices, you can use the Filter window again to limit based on signal strength (e.g. -60 dBm) by using the slider under the RSSI setting toward the bottom of the filter menu (see Figure 9).



-60 dBm

Exclude: none

RSSI: -60 dBm

N/A
E3:10:85:3F:89:E2
NOT BONDED -48 dBm N/A

Figure 9: How to filter by signal strength in the Android nRF Connect App.

What To Do After Your First Scan

Repeating scans and looking for suspicious trackers

One of the challenges with scanning for Bluetooth devices is that if you are in a crowded area a scan may result in dozens or more Bluetooth devices. Most of these devices will be devices used by other people in the vicinity, and might not be a cause for alarm. However, if you repeat scans and consistently find a Tile or AirTag near you, it could be used to track you, especially if the signal strength has two or three bars (higher than -60 dBm). The ID for a device can change over time even if it is the same physical device. This happens for security reasons, so just because the ID is different doesn't mean it is a different device.

Searching your surroundings for a tracker

If you suspect a tracker might be in your environment, you can try searching for it. A Bluetooth scanner’s signal strength is not a perfectly reliable indicator of distance, but you can use it to get a sense of whether or not you are getting “hotter” or “colder” (closer or farther away from the device). It’s recommended to search anywhere a small device could be hidden on or inside something, such as in bags, purses, gifts, kids toys, inside seat cushions of cars or under the seats, etc.

What to do when you find a tracker

If you do find a tracker on your person or in your vicinity, you can choose whether to stop the device from tracking you or leave it in place. You might leave it in place if you are concerned about alerting the person that is tracking you that you have found the device. You may also want to contact a helpline and/or law enforcement for additional support.

Deactivating and/or destroying the tracker will prevent your location from being tracked, but anyone who placed the tracker will also know that the tracker has been deactivated. If the tracker was able to connect to the tracking networks recently, the owner of the tracker would also know when and where it was deactivated. Devices with removable batteries can be deactivated by removing the battery; other devices will need to be destroyed to prevent them from transmitting, or thrown out in a public area that feels safe. If you do not feel safe deactivating a device for concern about your safety, you can leave the device in place, and keep in mind that your location is being tracked when near the tracker, and seek alternative arrangements when you need to do something without being tracked.

You also have the option of contacting others for help. Trained advocates at helplines can help you consider your options (legal or otherwise) and make plans for your safety. If you feel safe contacting them, law enforcement may be able to investigate your complaint, though it depends on their resources and knowledge about location tracking devices. In such a case it may be a good idea to keep the tracker intact. It may make sense to be in touch with law enforcement if you suspect the tracker was placed by someone who you have a restraining order against and/or are involved in legal proceedings with to preserve potential evidence. You can also consider contacting an attorney or legal aid organization, or contacting the company who manufactures the device directly.

Warning: When Trackers Might Not Show Up On Scans

AirTags and Tiles have different Bluetooth settings depending on whether a person who has registered that device is nearby or not. ***If a person who registered the device is in range of***

that AirTag, it may not advertise over Bluetooth. So, for example, if you scan for an AirTag while other members of your family are home, you may think there are no AirTags present when there actually are. The best place to scan for an AirTag is away from anyone and their devices who you think might be trying to track your location.

Resources and Next Steps

Contact a National Helpline
Location Tracking Guide