7 *Things Every Examiner* SHOULD DO *When Collecting Mobile Devices*

GRAYSHIFT

www.grayshift.com

Collecting mobile devices as evidence can be challenging.

We have compiled a short list of 7 things you should do when collecting mobile evidence. Bear in mind this is not a complete list, nor should it be considered policy; and ALL methods should be tested and verified independently prior to deploying them in the field.

- ☐ **Get the device off the network**
- ☐ **Get power to the device**
- ☐ **If the device is open and awake, keep it that way**
- ☐ **Attempt to get the passcode**
- ☐ **Legal process**
- ☐ **Collect external storage media and additional devices**
- ☐ **Investigate all potentially paired devices**

1

Get the device off the network

There are a couple of reasons why this step is listed in the #1 position, and device isolation should not be overlooked.

Most smartphones have the ability to receive remote wipe commands from users. This feature is designed to provide an additional layer of security in case the device becomes lost or stolen, or if users want to protect their personal data.

While this is a great feature for the average user, it is a terrible feature for law enforcement investigators, as it can be utilized by suspects to destroy potentially incriminating evidence.

This happens more than you might think. Imagine sitting in your lab, looking down at the device, and seeing the dreaded “erasing” progress bar…the device has started a remote wipe sequence, and it’s too late to continue in most cases. There are very few worse feelings, and we know personally this has happened to many forensic examiners.

Taking a mobile device off the network will help prevent the remote wipe command from reaching the evidence.

Another reason for device isolation may be up for debate, but we prefer to act on the side of caution: EVIDENCE ADDITIONS/ CHANGING.

At first glance some members of law enforcement may think this is a good thing. It may be for investigations, but not for court orders. Let's explain.

When you collect the device, it is law enforcement's responsibility to protect the integrity of the data. Now imagine the device sitting in the lab for hours, maybe days, and it is still receiving messages, emails, and other incoming data. At some point, this may become a "wiretap" opposed to a simple search of a mobile device. This of course is a court decision. We suggest reaching out to your local prosecutor to determine best next steps after a device has been lawfully seized.

Even worse, misleading or false information may be sent to the device to throw investigators off course.

Best advice…**GET IT OFF THE NETWORK.**

This can be done in several ways.

One way is to place the device into Airplane Mode**.** On most devices, this can be done with the default settings even when the device has a handset lock in place. While there are multiple methods to achieve this, most devices allow for network isolation with a swipe from the top of the screen downward.

Please research the specific device you are dealing with, as users can change this option and outcomes may vary.

For court orders, reach out to your local prosecutor to determine best next steps after lawfully seizing a device.

Faraday Technology, or write blocking material, is another option to prevent a device from sending or receiving signals from a wireless network. This does include most radio frequencies.

Here are a few options for using Faraday materials.

Faraday Bag: small pouch designed to fit mobile phones.

Faraday Box: larger, heavy box with connections to the device that have been tested to ensure a signal neutral environment.

Aluminum Foil: Yes, this does work and requires multiple layers. It is an inexpensive alternative if budgets do not allow for Faraday containers.

SIM/UICC removal: This method will remove the device from the cellular network, but does not protect against Wi-Fi, Bluetooth, NFC, or other radio hardware within the device. SIM removal may also impact biometric unlock capabilities.

Power Off: This method should only be used as a LAST RESORT, as it will affect device state and your ability to obtain access to key evidence.

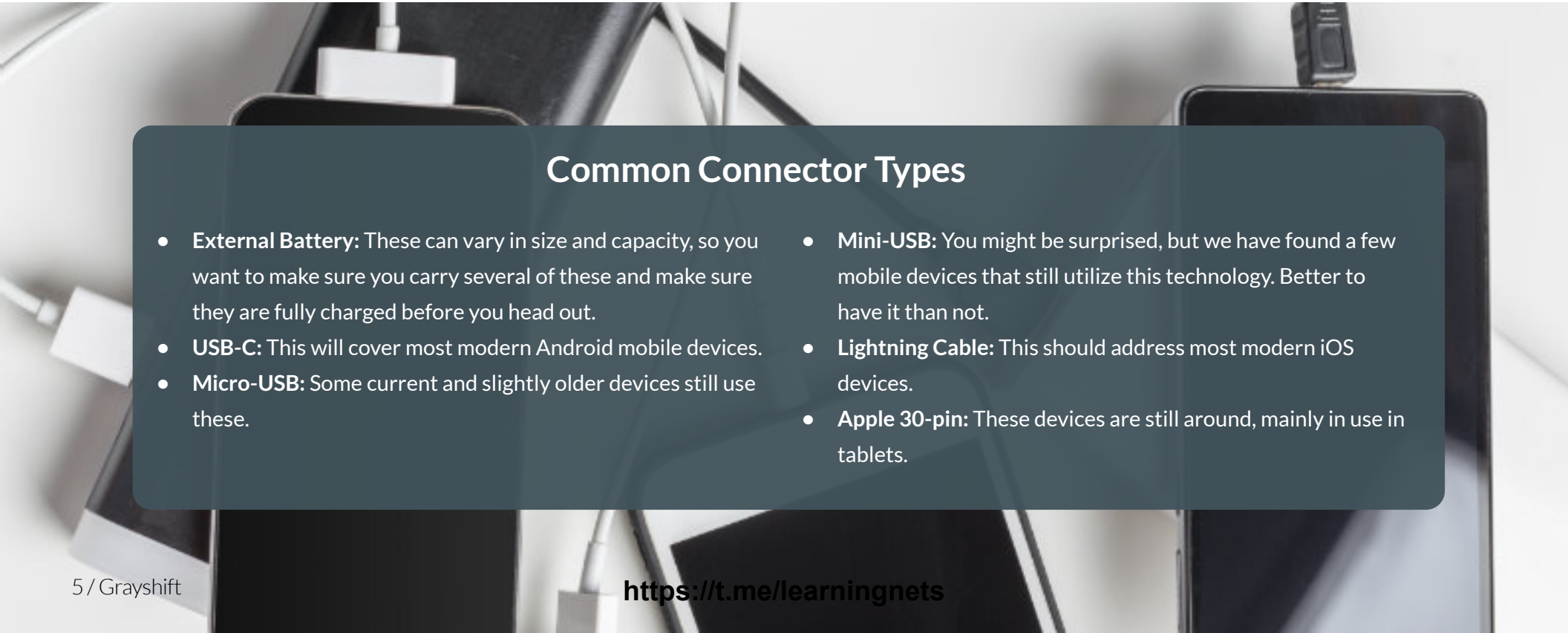
Image Credit: MOS Equipment, mosequipment.com

2

Get power to the device

This step is a priority if the device is currently turned on. If the device is accessible AND an Android device, you may be able to adjust settings available on specific devices that will help prevent the device from automatically being placed in a sleep state when power is attached. If this is the case, we will cover the importance of keeping the device in this stage in another step.

There are a couple of considerations when getting power to a mobile device: connectors. While this is much simpler than the days of flip phones with proprietary connectors for every model, you still need to carry a few items in your evidence bag.



Common Connector Types

- **External Battery:** These can vary in size and capacity, so you want to make sure you carry several of these and make sure they are fully charged before you head out.
- **USB-C:** This will cover most modern Android mobile devices.
- **Micro-USB:** Some current and slightly older devices still use these.
- **Mini-USB:** You might be surprised, but we have found a few mobile devices that still utilize this technology. Better to have it than not.
- **Lightning Cable:** This should address most modern iOS devices.
- **Apple 30-pin:** These devices are still around, mainly in use in tablets.

3

If the device is open and awake, keep it that way

If you locate a device that is unlocked and presenting an “open” screen, try your best to keep it open and available for access.

This is sometimes challenging since there are only a few ways to achieve this outcome. As with anything else, you should test these methods prior to trying them on the scene.

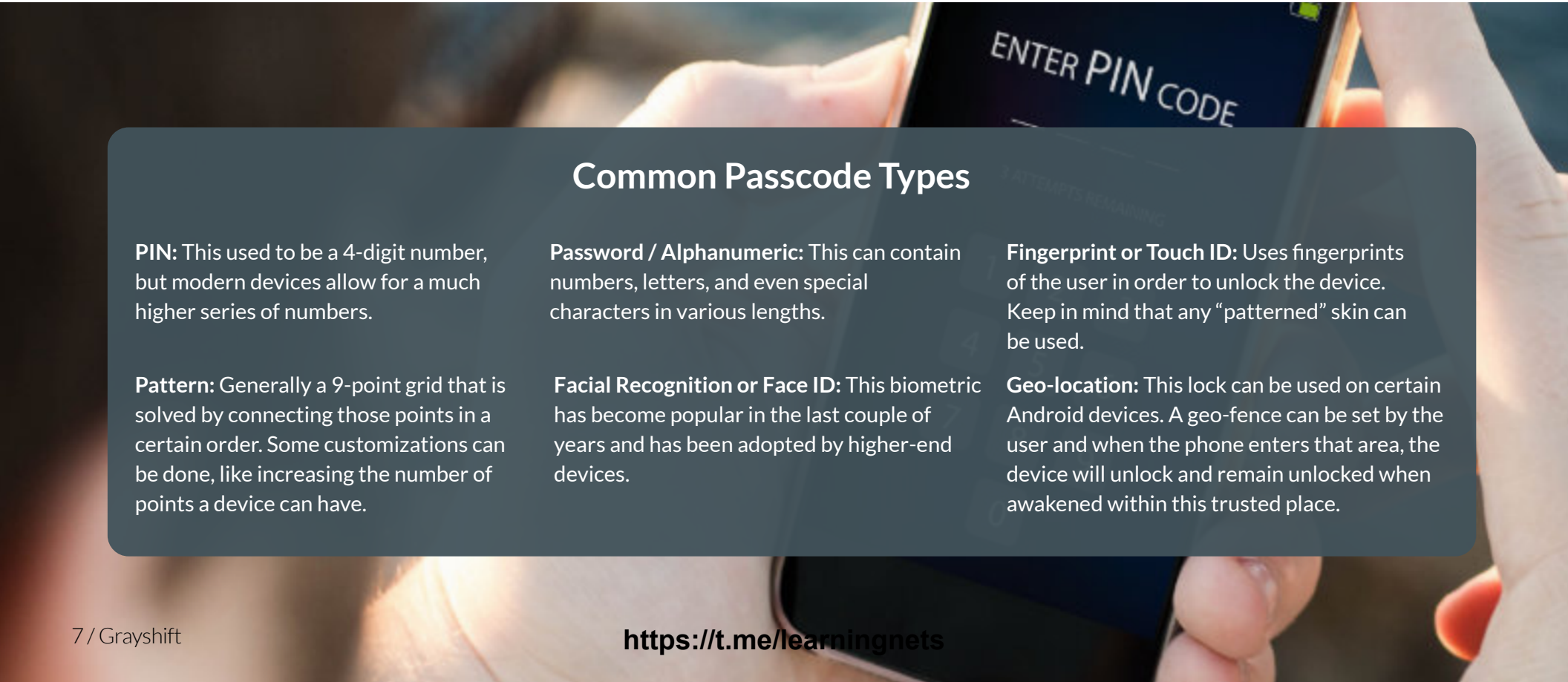
1. **Use a mouse simulator USB on Android:** This will not work on all Android devices, but the principle has been around and used on computer systems. It is a USB device that simulates the moving of a mouse. Very simple. Keep in mind you are plugging a device into the system and you need to articulate all of the steps taken in your reporting.
2. **Finger tap:** Simply finding an area on the device screen without application icons and tapping or sliding your finger to keep the device awake. You MUST be careful not to start any installed applications or processes. If any application or process is started during this process, you should document what occurred.

4

Attempt to get the passcode

The success of getting the passcode for a device will vary dramatically depending on whether you are collecting the device from a victim, witness, or suspect. As always, we recommend using proper legal process and documentation (i.e. consent paper, search warrant, exceptions, etc.).

Let's review the various types of passcodes depending on device make and/or model.



Common Passcode Types

PIN: This used to be a 4-digit number, but modern devices allow for a much higher series of numbers.

Password / Alphanumeric: This can contain numbers, letters, and even special characters in various lengths.

Fingerprint or Touch ID: Uses fingerprints of the user in order to unlock the device. Keep in mind that any "patterned" skin can be used.

Pattern: Generally a 9-point grid that is solved by connecting those points in a certain order. Some customizations can be done, like increasing the number of points a device can have.

Facial Recognition or Face ID: This biometric has become popular in the last couple of years and has been adopted by higher-end devices.

Geo-location: This lock can be used on certain Android devices. A geo-fence can be set by the user and when the phone enters that area, the device will unlock and remain unlocked when awakened within this trusted place.

5

Legal process

We cannot stress the importance of this step enough. It could mean the difference between getting the evidence accepted into court or not. With that, we will say **"You MUST have proper legal authority"** when you collect or search data, if you are law enforcement. If you are a private entity, please consult a legal expert.

In law enforcement, there are a few basic rules that apply to legal authority. Please always check with the prosecutor who has authority over your jurisdiction.

Here is a shortlist of legal processes. This list is not all-inclusive.

1. **Search Warrant**: Order issued by a judge or magistrate making a determination of probable cause to search for evidence. This is always the recommended method for collecting evidence.
2. **Consent**: If you get consent from an individual, get it in writing with their signature. Also, be sure to provide them a clear method to revoke consent at any time.
3. **Do not forget about the exception rules**: There have been a lot of court rulings on these over the years, so please check with your local prosecutor to ensure you are within legal boundaries.

Chain of Custody

There is no better time to start the chain of custody on a device than right when you first see it. Take as many notes as you can about the condition of the device, its location at the time of seizure, the time it was secured, the device state upon collection, who took control of the evidence, and where it was secured every step of the way. This should occur each time the device is moved or touched, and the actions taken on the device should be recorded at each stage.

6

Collect external storage media and additional devices

Investigators sometimes overlook this step because more and more devices store data internally and not on removable media. Always keep in mind that most users are not on the “cutting-edge” of technology and may resort to storing data on external media.

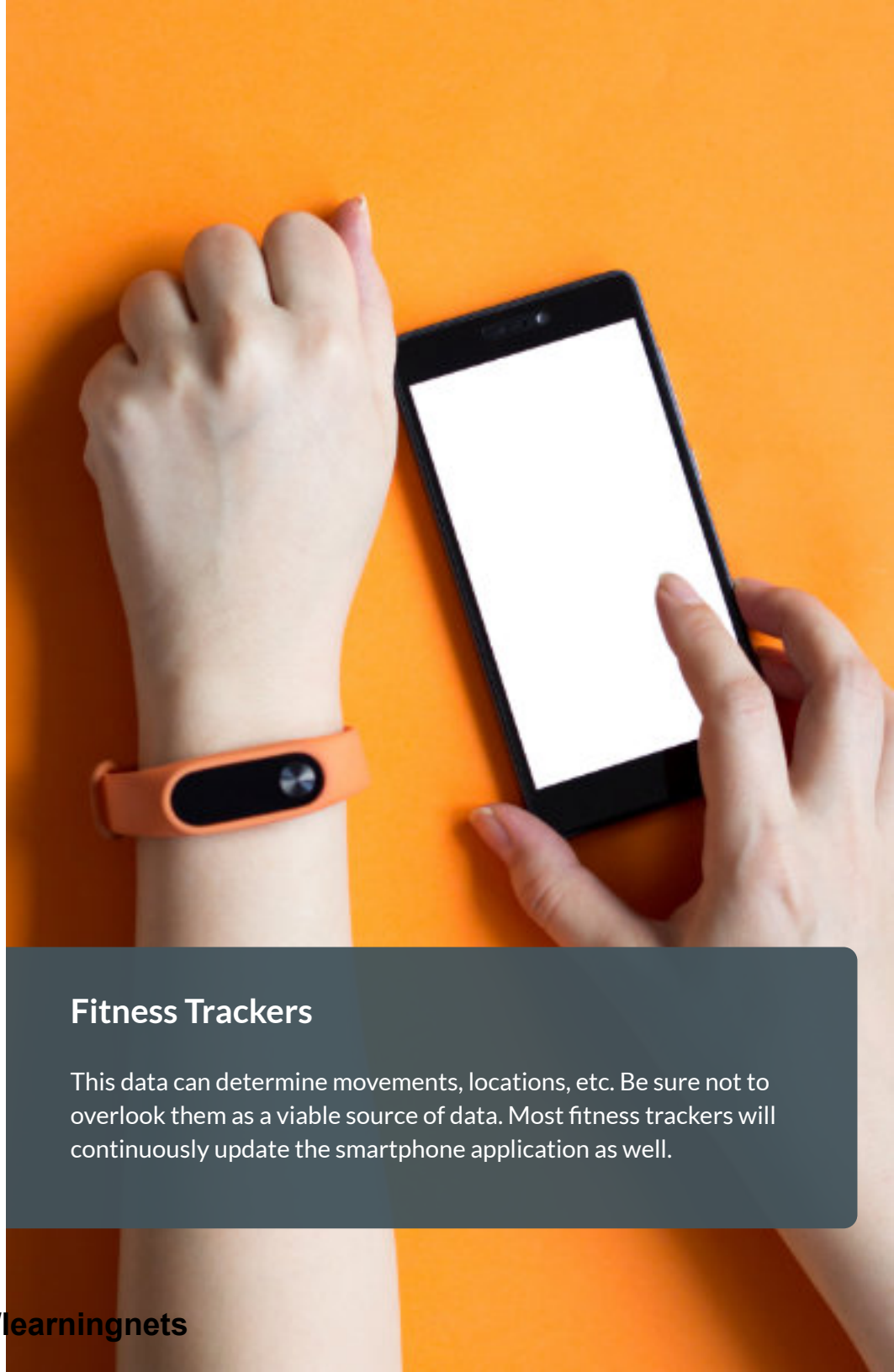
1. **Micro SD Cards:** These are used to store data on some Android devices and drones.
2. **External USB Devices:** These can be used directly in some mobile devices to backup data, including images.
3. **Computers:** Devices can be backed up to internal computer hard drives. When all else fails to get into a locked device, a backup may come in handy in your investigation.

7

Investigate all potentially paired devices

Modern devices can be paired via Bluetooth to other external devices. This step, while the last in our list, can contain endless items when you consider the possibilities.

1. Let's start with one of the most popular paired devices, **a car**. You probably already do this with your own device. It's convenient to have all your contacts, messages, and call history synced up to your phone. This can also leave trace evidence in the memory units onboard the vehicle. This type of forensics is a different topic altogether and should be considered as a viable source of information from a mobile device.
2. One you may not have considered are **wireless hotspots and routers.** These devices contain connectivity information and MAC addresses that you may need to prove a connection.
3. Other **smart devices and hubs.** While this list can be exhausting, it is important to know the types of devices that can be paired with mobile devices and which ones may contain information to aid your investigation.



Fitness Trackers

This data can determine movements, locations, etc. Be sure not to overlook them as a viable source of data. Most fitness trackers will continuously update the smartphone application as well.

Putting These Steps Into Practice

While we know these 7 steps are not an exhaustive list, they serve as foundational steps to help you create a plan for collecting physical evidence on-scene.

Once you've collected the physical evidence, you'll need to figure out a method to lawfully obtain access to the evidence and collect it in a forensically sound way. Using a forensic access tool like GrayKey can help you get important evidence from lawfully seized mobile devices.

Get Started

About Grayshift

Grayshift is a leading provider of mobile device digital forensics, specializing in lawful access and extraction. Grayshift solutions are purpose-built to help law enforcement and government investigative agencies swiftly resolve critical investigations and ensure public safety. The company's innovative GrayKey technology provides same-day access, complete control, and comprehensive data extraction from mobile devices. Designed and assembled in the United States, GrayKey is trusted by 1000 agencies across more than 25 countries globally. For more information, visit www.grayshift.com.

Follow Us