

BlueSleuth Bluetooth Locator

User Manual Version 1.3



Table of Contents

Introduction.....	2
Bluetooth Basics.....	2
What's a Skimmer?.....	2
Bluetooth Skimmers.....	3
Detecting Bluetooth Skimmers.....	4
Bluetooth Skimmer Software.....	4
Unboxing.....	5
Powering On/Off Your Unit.....	5
Charging Your Unit.....	6
Main Measurement Screen.....	7
BT Direction Finding Screen.....	9
BLE Signal Strength Screen.....	10
Options Menu Screen.....	11
Battery Calibration Screen.....	12
Product Info Screen	13

Introduction

BlueSleuth Bluetooth locator is a handheld unit that constantly scans for all nearby BT (Bluetooth) and BLE (Bluetooth Low Energy) devices. These devices include smartphones, smartwatches, IoT (Internet of Things) devices, wireless headphones and earbuds and many other types of wireless devices. All BT and BLE devices communicate on a specific set of RF bands. BlueSleuth can receive these signals up to 75 feet away and also communicate with some of these devices by pairing with them. Once paired, BlueSleuth's (DF) Direction Finding antenna allows users to hunt down BT or BLE devices including ones hidden inside ATMs, gas pumps and more in the form of skimmers. BlueSleuth measures RSSI (Realtime Signal Strength Indicator) in dBm allowing BT and BLE devices to be located based upon their proximity to the BlueSleuth receiver.

Bluetooth Basics

Each device has a small radio transmitter/receiver component that allows a computing device like a laptop, tablet, or smartphone to transmit data to different peripheral devices including Bluetooth speakers, headphones and other wireless devices.

Bluetooth transmitters send and receive radio waves at frequencies between 2.402 and 2.4835 GHz with 79 different channels. Bluetooth frequencies and the 2.4 GHz band are set apart from mobile phones, radio, and television. Bluetooth transmitters use low power and are designed for short-range transmissions.

When Bluetooth is turned on, devices can be configured to detect and connect automatically. Up to 8 different devices can use Bluetooth connectivity to communicate at once – one being the *master*, while the rest are connected as *slaves*. Each pair of devices uses one of the 79 available channels so that they don't interfere with each other.



What's a Skimmer?

Credit card skimmers steal people's credit card numbers and details by intercepting a person's credit card number, PIN, and details so that the thief either clones the credit card and uses it or sells it on the Dark Web. Learn more about the cost of skimming and cybercriminals and how to keep your facility secure by downloading our e-paper at link:

<https://www.bvsystems.com/wp-content/uploads/2019/06/SkimmersScammers-e-paper.pdf>

There are many different types of credit card skimmers. Chip-enabled credit cards were created to help eliminate skimming but they don't prevent a technique cybercriminals use called shimming.

Skimming – a thief places the card on a card reader – it intercepts the magnetic stripe information when a customer slides their card through the skimmer.

Shims or shimming – this is when a device is attached directly to a card reader. It is connected to the part of the terminal where the card has already been decrypted to defeat the protection provided by "chip and pin" technology. So, in essence, it sits between the chip on the card and the chip reader. It is then able to read and copy the information from the credit card stripe when the card is swiped



through the shim; just like skimming. Sometimes these devices are paper-thin and simply inserted into the card slot.

Deep insert skimmer or shim – these devices are positioned deep inside the card reader. They can reside hidden for days or weeks, harvesting information from the magnetic stripe before being detected and removed.



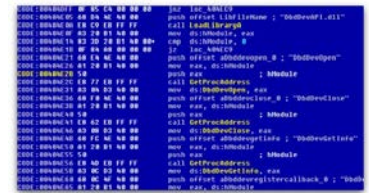
Keyboard overlays – these are simply devices placed over the pin pad that intercept the input as a person types in their PIN.



Video overlays – similar to the keyboard overlay, these are tiny, pinhole cameras that record a victim's PIN codes on the keypad. Sometimes they use audio to record the sounds as someone enters their PIN.



Network sniffers – these devices are on the same physical network as the target device. Instead of stealing data from the magnetic stripe, they're designed to steal information as it's transmitted across the network.



Card reader interceptor – these are devices that look like the front of a card reader but they're not. Like a skimmer or shim device, they read the information off of the magnetic stripe. Unlike a shim, they're not able to defeat chip and PIN technology.



Bluetooth Skimmers

There are multiple ways for a shim or skimmer to store information. They can use on-chip storage retrieved via a serial communications port, a USB key drive, or a Bluetooth adapter.

The “old fashioned” way of retrieving card data from the skimmers might be to remove the device from a gas pump, ATM, or Point-of-Sales device and either connect to it through the serial port or remove the USB storage device. Physical retrieval isn't difficult but impacts the ability of a criminal to safely scale a card harvesting operation.

Using Bluetooth saves a criminal time and that adds up when they've got multiple card skimmers in operation. Using Bluetooth technology, they can sit in a car and remotely pull card data off the skimmer.

Bluetooth chips are cheap because they're mass-produced and can sell for less than \$10. Manufacturing a custom PCB or board design is inexpensive so adding a Bluetooth radio to a card skimmer device is cheap and relatively easy. Due to range and cost, most US credit card skimmers are using Bluetooth Classic and not the newer Bluetooth Low Energy standard. BlueSleuth scans for both of these standards.

Detecting Bluetooth Skimmers

There are three major pieces of information that can be used to detect Bluetooth enabled credit card skimmers: Class-of-Device, Device Name, and MAC Address.

Class-Of-Device

According to [Bluetooth.com](https://www.bluetooth.com), "the Major Device Class segment is the highest level of granularity for defining a Bluetooth device. A device's main function determines its Major Class assignment. There are 32 major classes". See our definitions: [here](#).

Class-of-device is what's used by the Bluetooth protocol to identify if it's communicating via a Bluetooth speaker, Bluetooth headset, a car infotainment system, a network, or a peripheral device. Class-of-Device tells the Bluetooth transmitter what profile it needs to load in order to successfully communicate with a device. Profiles are analogous to a device Category.

Many Bluetooth enabled credit card skimmers use an uncategorized Class-of-Device. Meaning that the Bluetooth protocol doesn't load a particular profile to enable communications.

Mobile device operating systems and most apps are designed not to attempt to pair to a device when the Class-of-Device is 'uncategorized'. This means that 'uncategorized' Class-of-Device won't even show up in your "available devices" list.

Device Name

In some cases, Bluetooth skimmers use radios that default to the Device Name "HC-05", "HC-06", "HC-08", or "FREE2MOVE". The problem is that there are many other devices that use the same Bluetooth modules and they aren't card skimming devices.

There are also skimmers that have a custom name that would look normal at first glance. So, we can't only rely on Device Name alone to identify card skimmers. A crafty criminal can rename the device to broadcast what would otherwise be a commonly found name, like Sync or Beats. Using only the Device Name could result in false positives that would likely cause people to misidentify skimmers.

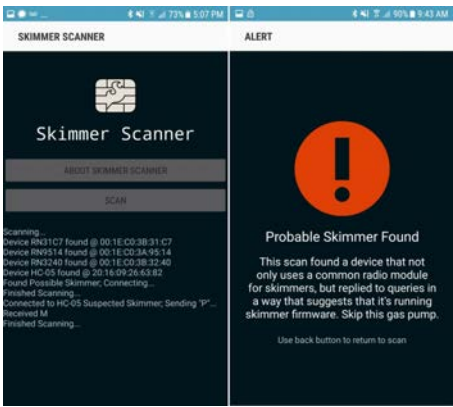
MAC Address

Lastly, because criminals are using commercial-off-the-shelf Bluetooth chips, law enforcement and researchers have narrowed down the list of chips to a specific set of manufacturers.

As previously discussed, these chipsets are widely available. Meaning that a scan of a gas station is just as likely to detect a legitimate device as it is a credit card skimmer. That being said, some of the skimming devices recovered by law enforcement use a fictitious MAC address that looks like a date. For example, 20:18:11.

Bluetooth Skimmer Software

There are several Bluetooth skimmer detection apps available for smartphones and laptops but these software-based solutions can only partially address the issue of Bluetooth skimmers. Software-based apps rely on consumer grade antennas and receivers found in smartphones and other wireless devices. Bluetooth apps do not effectively locate skimmers. Smartphone apps will occasionally display a suspicious or unknown Bluetooth device, but it cannot lock onto or locate it through wireless directional antenna technology. Gas pumps and ATMs are usually grouped together making it virtually impossible to distinguish which kiosk in a grouping contains a skimmer without opening up each one to inspect and verify.



Unboxing

Unpack and completely charge up your BlueSleuth using the supplied power transformer and charging dock. Be sure that the unit is seated firmly in the charging dock so that the metal contacts on the bottom are connecting for a constant charge. The mini-USB port located on the side is for firmware updates via any Windows PC. Check with BVS support to make sure you have the latest firmware and updating instructions. Be sure to only use the provided omni-directional antenna and directional antenna authorized by BVS support. This will ensure that your unit properly scans all Bluetooth and BLE signals at maximum sensitivity.



Powering Up/Down Your Unit

Power up BlueSleuth by pressing the white button below the touchscreen. This same button is the only physical button on the unit and also powers down the unit by holding it in for a few seconds. Before powering up, connect the antenna. This ensures that the unit will immediately begin scanning all nearby BT and BLE

Operation

BlueSleuth contains 2 independent modules constantly scanning for all nearby bluetooth and bluetooth low energy devices. When BlueSleuth pairs to a BT device, the unit may begin to perform true direction finding of that device. For BLE devices that do not allow for full connection or pairing, BlueSleuth allows for basic signal strength measurement. When first scanning an area for all nearby bluetooth devices, the included omni-directional antenna is recommended. Once all nearby bluetooth devices have been detected, direction finding can be performed by replacing the omni-directional antenna with the directional antenna. For more information on typical detection ranges and environments, see included BlueSleuth data sheet or consult your BVS sales engineer.

<div><div></div><div></div><div></div><div></div></div>	
MAC / ID	RSSI (dBm)
18:65:90:0E:1B:23 FREE2MOVE	-43
C0:CE:CD:E6:00:26 APPLE WATCH	-69
18:00:DB:0D:A1:17 FITBIT FLEX	-78
00:16:AD:8E:71:15 BT-100 HEADPHONE	-100
<div><div>BT ONLY</div><div>BLE ONLY</div><div>BT & BLE</div><div>PAGE</div></div>	

Upon startup, BlueSleuth automatically scans all nearby BT and BLE devices. BlueSleuth contains 2 independent modules constantly scanning for all nearby BT and BLE devices. When BlueSleuth pairs (not all devices will automatically pair) to a BT device, the unit may begin to perform true direction finding of that device. For BLE devices that do not allow for full connection or pairing, BlueSleuth allows for basic signal strength measurement. Use the included omni-directional antenna to first sweep the entire area of interest to discover all devices. BlueSleuth lists all devices found by signal strength with the highest RSSI at the top of the list. Use the page button to scroll the entire list of devices or sort the list by BT, BLE or both using the buttons along the bottom of the screen. All devices that fit the profile of a skimmer (using a variety of data points) appear in red on the list. A red alert icon also appears on top of the screen in case the suspected skimmer is not visible on the current page of device shown. Friendly or known devices can be removed from the list to make this process easier in areas containing many BT or BLE devices. Users can also navigate to the main settings screen to change other settings. Once a suspected skimmer is identified, users should swap the omni-directional antenna for the direction finding antenna in order to locate the suspected skimmer. See all features detailed further in this user manual.











Charging Your Unit

BlueSleuth ships with an AC powered charging dock. Place unit in charging dock and be sure the red LED on top of unit is ON. If red LED is not ON, BlueSleuth is not being charged. Try adjusting BlueSleuth in dock until red LED is ON. Charging takes approximately 4 hours. You may also use the mini-USB port on the side to slowly trickle charge your unit overnight if you do not have access to the charging dock. BlueSleuth runs approximately 10 hours from a full charge. BlueSleuth has smart trickle charging circuitry that is always calibrating the battery but if your battery runtime is noticeably short after a full charge, you may need to manually calibrate the battery. Go to BATTERY under MAIN MENU for more details and consult BVS support if you have any questions or concerns.



Main Measurement Screen

   	
MAC / ID	RSSI (dBm)
18:65:90:0E:1B:23 FREE2MOVE	-43
C0:CE:CD:E6:00:26 APPLE WATCH	-69
18:00:DB:0D:A1:17 FITBIT FLEX	-78
00:16:AD:8E:71:15 BT-100 HEADPHONE	-100
   	

MAC / ID	RSSI (dBm)
18:65:90:0E:1B:23 FREE2MOVE	-43

A suspected BT skimmer has been detected. These fields display the device ID/ MAC address and the RSSI in dBm. Touch this area to monitor only this device in order to survey it or locate it in the direction finding screen.

C0:CE:CD:E6:00:26 APPLE WATCH	-69
----------------------------------	-----

The detected device is BLE (indicated by light blue color or device name) Touch this area to monitor only this device in order to survey it or locate it in the direction finding screen.



Touch this icon to navigate to the OPTIONS settings menu screen.



This button (garbage can) is used to add a device to the whitelist of friendly or known devices that you know are not skimmers. Begin by touching this button. Next, choose the device(s) that you wish to move to the whitelist. To exit this mode, press this button once again.



This alert only appears when a suspected skimmer has been detected. All MAC/Device IDs listed in red are suspected skimmers.



This battery icon indicates roughly how much power is left. Visit the BATTERY button in the OPTIONS menu for more details on battery power and battery calibration procedures.



Touch this button to only view nearby BT devices. BlueSleuth is always scanning for all BT and BLE devices so this button is only acting as a filter for viewing. Skimmer alerts will appear regardless of which devices you are currently viewing.



Touch this button to only view nearby BLE devices. BlueSleuth is always scanning for all BT and BLE devices so this button is only acting as a filter for viewing. Skimmer alerts will appear regardless of which devices you are currently viewing.

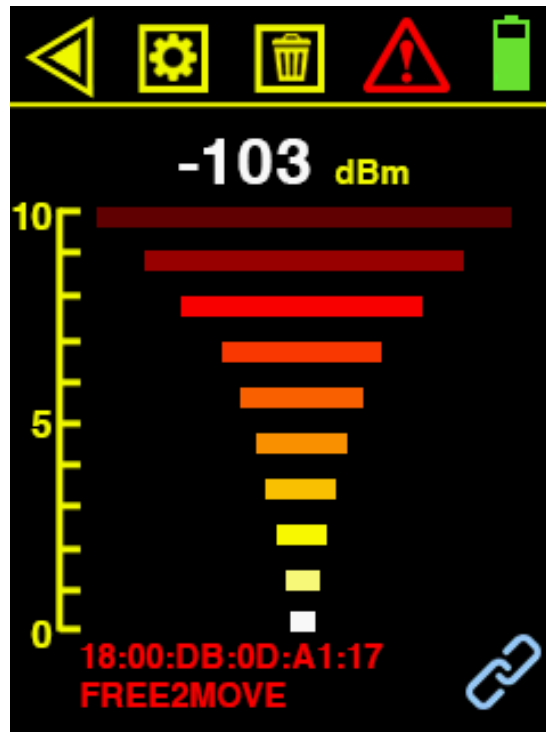


Touch this button to view all nearby BT and BLE devices. BlueSleuth is always scanning for all BT and BLE devices so this button is only acting as a filter for viewing. Skimmer alerts will appear regardless of which devices you are currently viewing.



Touch the down arrow to view next page of devices below. Touch the up arrow to view the previous page of devices.

BT Direction Finding Screen



Once paired with a nearby active BT device, this screen allows for true direction finding of hidden devices with range up to 125 feet. Vibration and audible beeping alerts increase with signal strength. Pairing chain icon (lower right) blinks to indicate pairing in process. Audible beeps only occur when there is a change in measurement. Chain link icon stops blinking once pairing is successful enabling fast RSSI measurements for true direction finding. Be sure to only use included direction finding antenna while in this screen.

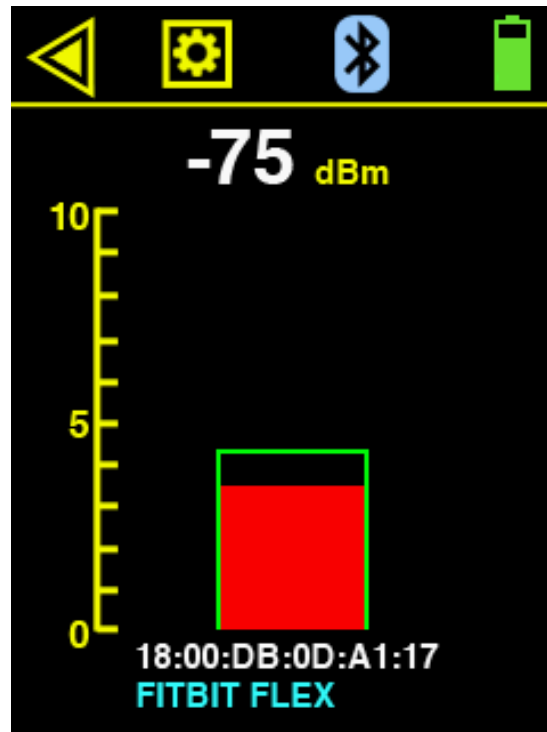


Touch this button to navigate back to the previous screen.



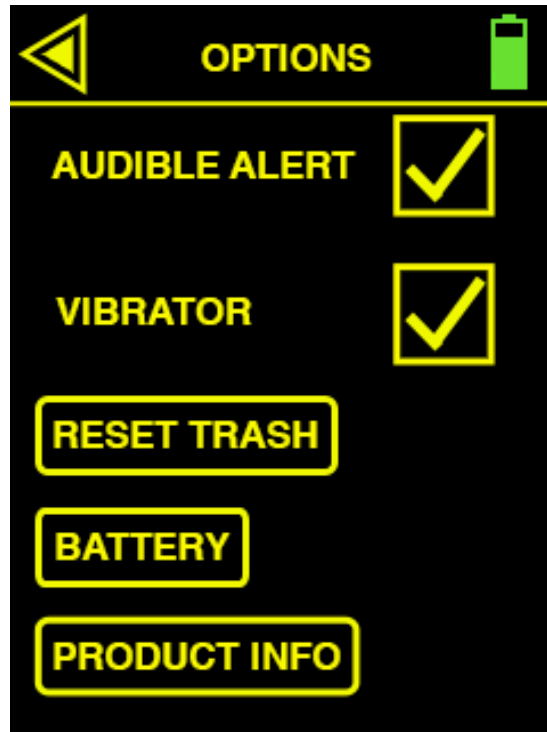
This icon indicates pairing in process (blinking) or that the device has been paired (not blinking) to BlueSleuth. Be sure to wait until device has fully paired to your BlueSleuth in order to direction find it most effectively.

BLE Signal Strength Screen



This screen indicates signal strength of nearby BLE devices to verify activity and approximate location of device. Vibration and audible beeping alerts increase with signal strength. The green watermark outline indicates the peak RSSI reached during the scan. Touch it at anytime to reset the watermark. Since this screen only indicates BLE measurement, it is not truly paired to BLE device making true direction finding more challenging but not impossible.

Options Menu Screen



This screen allows user control of options and unit information.



Press the checkbox to toggle an audible alert on or off. This is handy for users who want some audible feedback during scans and direction finding of BT and BLE devices.



Press the checkbox to toggle the vibrating alert on or off. This is handy for users who want some tactile feedback during scans and direction finding of BT and BLE devices.



Touch this button to reset the whitelist of known or friendly devices already scanned. This is useful if you are entering a new area to scan or have doubts about a device you may have whitelisted by accident.

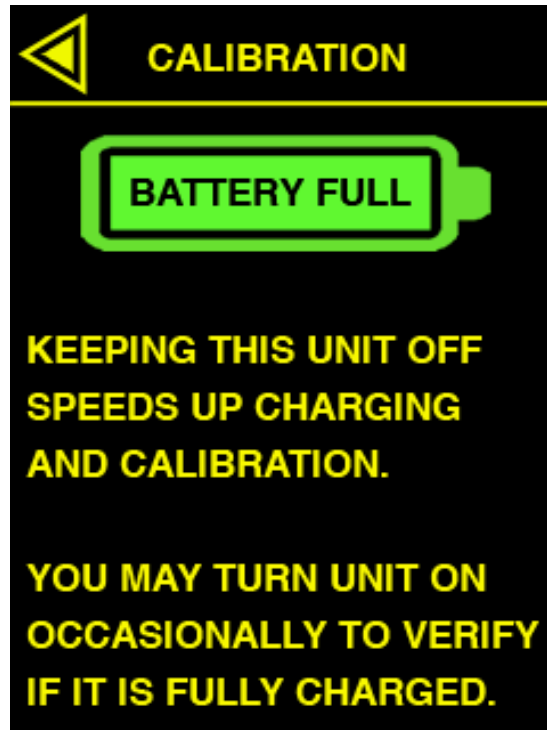


Touch this button to view the battery CALIBRATION screen that includes battery capacity details and charging instructions.



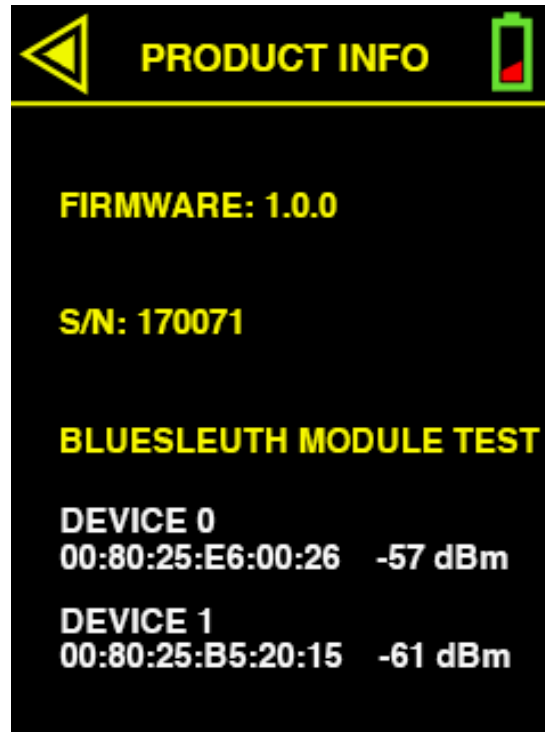
Touch this button to view your unit's firmware, serial number and a BlueSleuth module test to verify the receiver's operation.

Battery Calibration Screen



This screen displays the remaining battery capacity. If you are experiencing noticeably shorter run times for your BlueSleuth, navigate to this screen and follow the instructions. If battery issues persist, contact BVS support at 732-548-3737 or support@bvsystems.com.

Battery Calibration Screen



This screen displays the unit's firmware version, serial number and a module test to verify that the BT and BLE receivers are operating properly if you find yourself in an area with no other active BT or BLE devices besides BlueSleuth itself.

Always have your firmware version and serial number available if you are contacting BVS sales or support with questions.

Check www.bvsystems.com/technical-support for the latest firmware updates for your BlueSleuth unit. Users can update firmware themselves via the included mini-USB cable and port located on the side of the unit and Windows PC. Be sure to watch the BlueSleuth firmware update video on our YouTube for instructions. <https://youtu.be/2Hxss7z3glc>

Thank you for your purchase, we look forward to supporting you and your team.

Customer Support

Berkeley Varitronics Systems, Inc.
Liberty Corporate Park
255 Liberty Street
Metuchen, NJ 08840

8:00 AM to 6:00 PM EST
Toll Free: 888-737-4287
Phone: 732-548-3737
Fax: 732-548-3404

24/7 (expect a reply within one day)
email: support@bvsystems.com
www.bvsystems.com