Bluetooth Low Energy

# Sniffing, Scanning, Injecting Commands

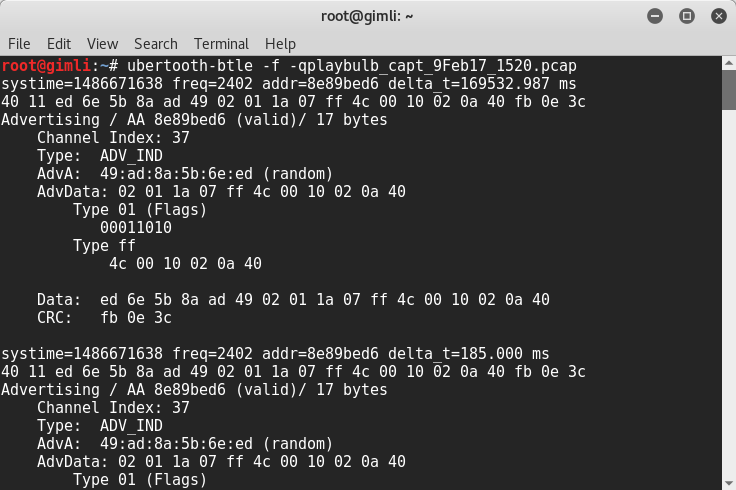
## Tools required:

1. ubertooth and associated libraries (libbtbb and ubertooth tools)
2. bluez (bluez; bluez-tools; bluetooth; bluez-firmware; rfkill)
3. hcitool
4. gattool

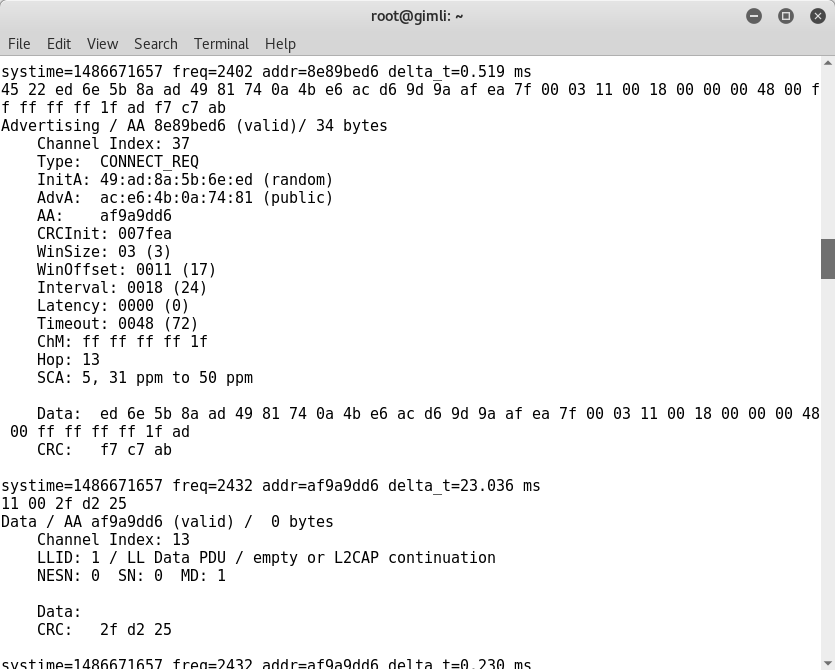
## Sniffing:

1. Make sure ubertooth is plugged in and operating
2. Make sure Bluetooth devices are off
3. Run ubertooth Bluetooth low energy tool with options to follow connections and pipe output into a PCAP file

# ubertooth-btle -f -qplaybulb\_capt\_9Feb17\_1520.pcap



1. Turn on master and slave devices. Connect master to slave; observe the scrolling addr change from “addr=8e89bed6” (advertisement) to something else. When this happens we know a connection has been made and ubertooth is following it. Send commands from slave to master while sniffing.



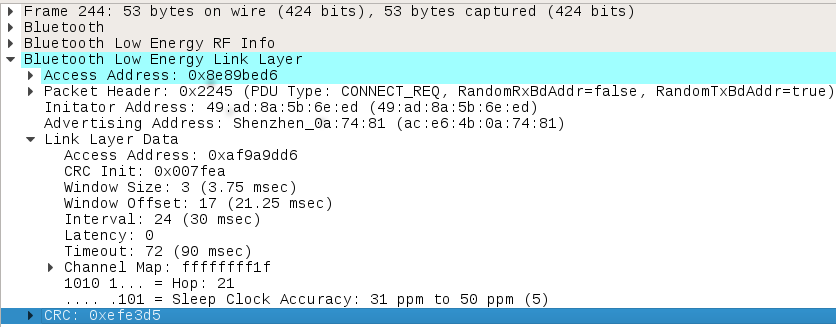
1. Open capture in wireshark.

# wireshark playbulb\_capt\_9Feb17\_1520.pcap

1. Scroll through capture in wireshark until you find an advertsiment followed immediately by a connection request (ADV\_IND then CONNECT\_REQ).



1. In a CONNECT\_REQ packet the master will inform the slave of the new access address that will be used for the connection. This address is found within the “Bluetooth Low Energy Link Layer”, in “Link Layer Data”, and in the field “Access Address” (not to be confused with the “Access Address field within the top level “Bluetooth Low Energy Link Layer”).

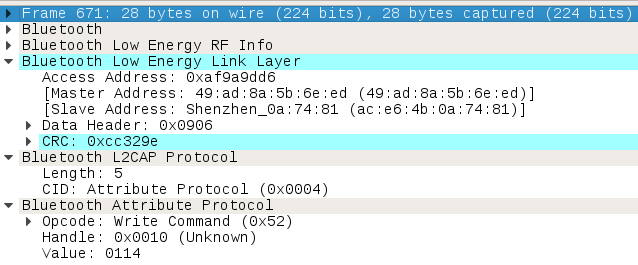


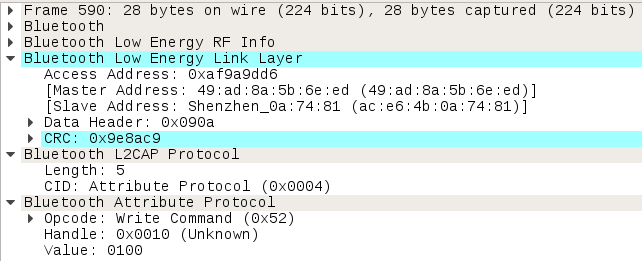
1. This new address for the connection can be used to filter the rest of the connection within wireshark by using the display filter “btle.access\_address” and the new address (use the shortcut “ctrl+shift+V” while highliting the “Access Address” to copy the value).



1. After filtering, scroll through the list of packets until a “Write Command” is found. Take note of any and all write commands as these are what the master potentially sends to the slave as an action. Observe the “Slave Address”, “Handle”, and “Value” fields for this command (within “Bluetooth Low Energy Link Layer” and “Bluetooth Attribute Protocol”). These are the values that will be used to repeat







## Scanning:

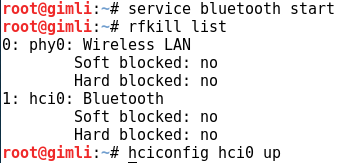
1. Next, make sure a dongle is connected, start the bluetooth service, check to make sure the dongle is on and not blocked, and bring up the device.

# service bluetooth start

# rfkill list

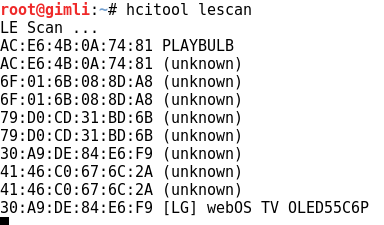
# rfkill unblock bluetooth //if blocked

# hciconfig hci0 up



1. Scan for bluetooth low energy devices utilizing hcitool and look for the device with the slave address

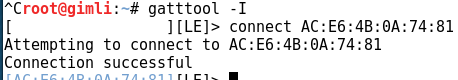
# hcitool lescan



## Inserting commands:

1. Using GATT tool’s command shell, connect to the device using its address:

# gatttool -I

[LE]>

1. Utilizing values found above, write a command to the device.

# char-write-cmd 0x0010 0100

# char-write-cmd 0x0010 0114