**Unlock your Bluetooth – How to**

**If the system already has all the necessary files installed, the user can skip straight to capturing the packets in Wireshark**

**Install necessary packages:**

sudo apt-get install cmake libusb-1.0-0-dev make gcc g++ libbluetooth-dev pkg-config libpcap-dev python-numpy python-pyside python-qt4

**Install libbtbb**

wget https://github.com/greatscottgadgets/libbtbb/archive/2018-12-R1.tar.gz -O libbtbb-2018-12-R1.tar.gz

tar -xf libbtbb-2018-12-R1.tar.gz

cd libbtbb-2018-12-R1

mkdir build

cd build

cmake ..

make

sudo make install

**Install Bluez**

cd ~

wget http://www.kernel.org/pub/linux/bluetooth/bluez-5.37.tar.xz

tar xvf bluez-5.37.tar.xz

./configure --enable-library

make

sudo make install

systemctl status Bluetooth

sudo systemctl start Bluetooth

sudo systemctl enable bluetooth

**Enable BLE features of Bluez**

sudo nano /lib/systemd/system/bluetooth.service

***Change configuration file line 9 to look like this***

ExecStart=/usr/local/libexec/bluetooth/bluetoothd –experimental

sudo systemctl daemon-reload

sudo systemctl restart bluetooth

**Install Ubertooth Tools**

wget https://github.com/greatscottgadgets/ubertooth/releases/download/2018-12-R1/ubertooth-2018-12-R1.tar.xz

tar xf ubertooth-2018-12-R1.tar.xz

cd ubertooth-2018-12-R1/host

mkdir build

cd build

cmake ..

make

sudo make install

**Update Ubertooth One Firmware**

cd ubertooth-2018-12-R1/ubertooth-one-firmware-bin

ubertooth-dfu -d bluetooth\_rxtx.dfu -r

**Install Ubertooth Plugin for Wireshark**

sudo apt-get install wireshark wireshark-dev libwireshark-dev cmake

cd libbtbb-2018-12-R1/wireshark/plugins/btbb

mkdir build

cd build

cmake -DCMAKE\_INSTALL\_LIBDIR=/usr/lib/x86\_64-linux-gnu/wireshark/libwireshark3/plugins ..

make

sudo make install

sudo apt-get install wireshark wireshark-dev libwireshark-dev cmake

cd libbtbb-2018-12-R1/wireshark/plugins/btbredr

mkdir build

cd build

cmake -DCMAKE\_INSTALL\_LIBDIR=/usr/lib/x86\_64-linux-gnu/wireshark/libwireshark3/plugins ..

make

sudo make install

**To Capture the BLE Packets in Wireshark**

1. In terminal, run command: *mkfifo /tmp/pipe*
2. Run Wireshark software
3. Go to *Capture* and then *Options*
4. Press the *Manage Interfaces* button and then click the *+* button
5. Add the Pipe */tmp/pipe*
6. Save and start the pipe
7. Back in terminal, run the command *ubertooth-btle -f -c /tmp/pipe*

**User Encapsulation not handled error**

1. Go to *Protocols* and then *DLT\_USER* within Wireshark
2. Press the *Edit* button and then the *+* button
3. Choose the option *User 0 (DLT=147)* and *btle* for the Payload Protocol
4. This can then be saved and exited back into Wireshark

**Install Bettercap**

sudo apt-get update

sudo apt-get install bettercap

**Use Bettercap**

sudo Bettercap

***Start BLE discovery***

ble.recon on

***Show all the BLE devices that were discovered***

ble.show

***Connect to specific MAC address of BLE device***

ble.enum MACADDRESS

***Write the hex data to the MAC address entered***

ble.write MACADDRESS UUID HEX\_DATA

**Install Crackle**

Download this file - <http://lacklustre.net/projects/crackle/crackle-0.1.tgz>

***Run the following commands in terminal***

tar -xvzf /path/to/yourfile.tgz

cd /path/to/crackle

make

make install

**Use Crackle**

crackle -i <filename.pcap> -o <output\_filename.pcap>