

# Hollong BLE Sniffer VTH201A Software Introduction v1.0



### History:

Version	Date	Note
v1.0	2017-06-17	Initial



# ViewTool loT Technology

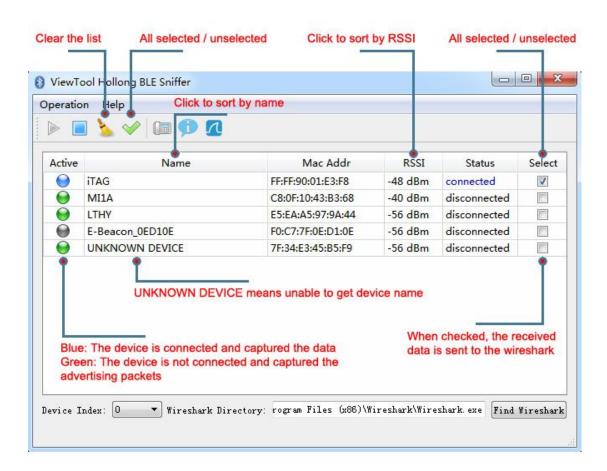
1. Software Functionality Description	3 -
1.1 Software Introduction	3 -
1.2 One click to start BLE Sniffer	4 -
1.3 Select Device To Be Monitored	5 -
1.4 Device Active Status Indicator	6 -
1.5 Device Sorting	7 -
2. Wireshark Functionality Brief	8 -
2.1 BLE Data Display	8 -
2.2 Protocol Filtering	9 -
2.3 BLE Protocol Interpret	10 -
2.4 Capturing Encrypted Data	11 -
2.5 Other Features	12 -
3 Technical Support And Services	- 13 -



# 1. Software Functionality Description

### 1.1 Software Introduction

Hollong BLE Sniffer Software include two major parts, One is for data capturing, device management, and sorting, filtering, Another one is for data display, data interpret, The window for first part is showing below:



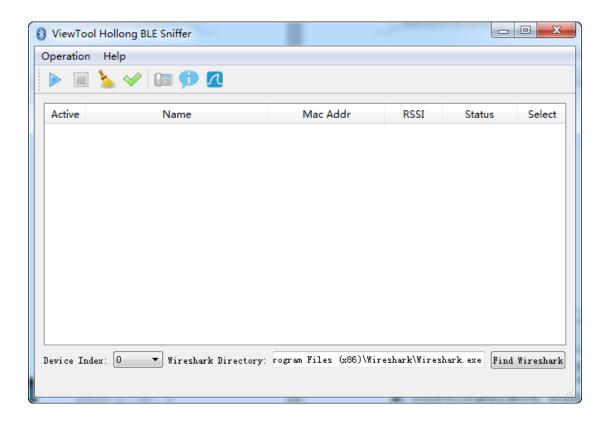
### Software functionlities::

- 1.One click to start, no setting required, after BLE Sniffer started, it will start to scan all BLE devices around, then list all discovered devices into list table, and kick off Wireshark application.
- 2.Select individual device or do multiple devices selection, Hollong provides the easiest way to do device selection to choose the device to be monitored, extremely saving time on device selection, data filtering and display.

### **ViewTool IoT Technology**

- 3.Device sorting, There are two ways to sort device: by device name or by device RF signal strength (RSSI), It will be much easier to find desired device in bunch of devices.
- 4.Device active status indicator, If on green, presents received advertising data in specific time (now set to 5 seconds but may be changed), If not receiving data in certain time, it will turn to grey., Changing to blue means current device has been connected.

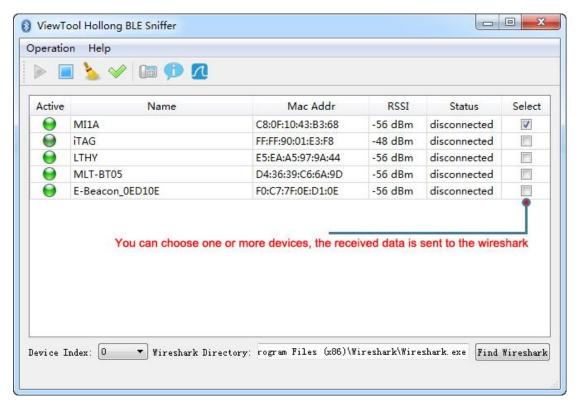
### 1.2 One click to start BLE Sniffer



One click the start button (blue triangle) will start BLE Sniffer capturing, After BLE Sniffer capturing started, all discovered BLE device will be put into list table, kicking off Wireshark immediately, no setting required on Wireshark to watch captured BLE data as well as protocol interpreted data in detail.



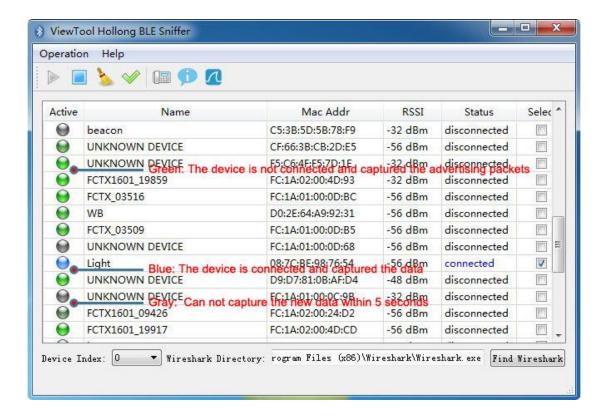
### 1.3 Select Device To Be Monitored



In the case of bunch of BLE devices presents, it's tough to watch right device's data on demand because there are too many unrelated data displayed in Wireshark, The desired data will be hidden into tremendous data, Hollong BLE Sniffer supply a easiest way to select device to be monitored, user could quickly select the device in shortest time.



### 1.4 Device Active Status Indicator

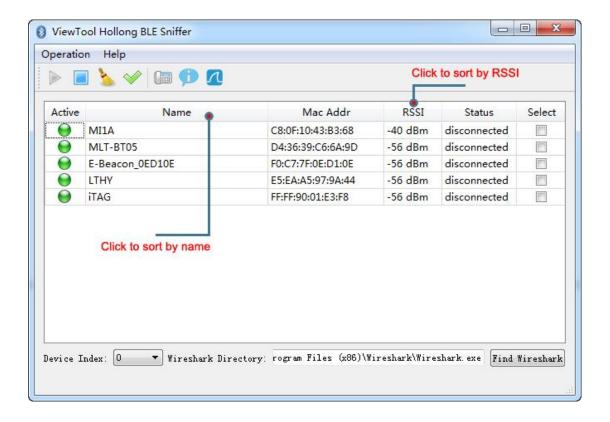


Except to watch and analyze the data on Wireshark, Hollong BLE Sniffer supply another easy way to monitor device status, There is device status indicator to show device status.

If indicator is green, presents advertising data has been received, If turn to blue, presents current device is connecte and received data after connection built, If turn to greay, presents device is not active (no advertising data or connection data received in designated time).



# 1.5 Device Sorting



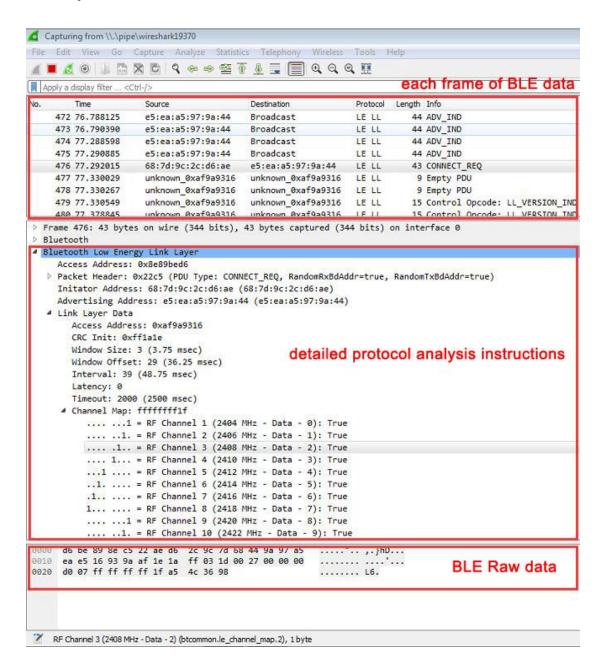
In case of bunch of devices presents or same name on different devices, it's hard to find right one, With device sorting feature, by click "Name" or "RSSI" to sort device on demand. Click once to sort device on one direction and double click on reversed direction.



# 2. Wireshark Functionality Brief

### 2.1 BLE Data Display

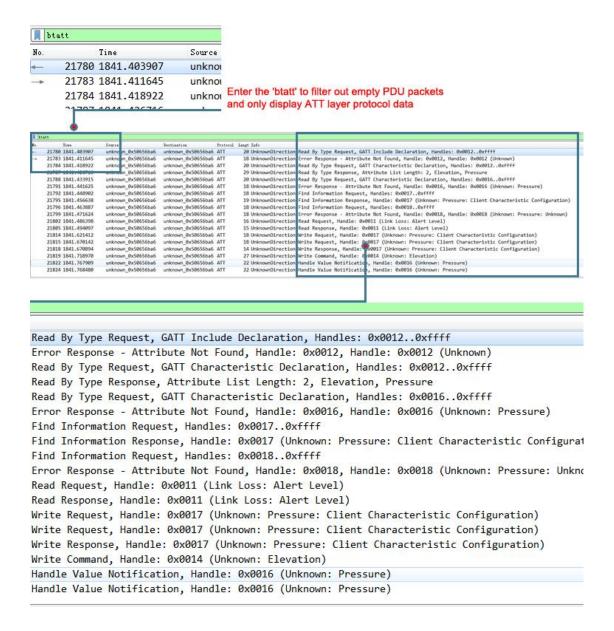
Wireshark is powerful protocol interpret application softwar with tremendous standard protocol supported, Hollong BLE Sniffer adopts its BLE protocol interpret feature  $_{\circ}$ 



One click to start BLE Sniffer, select desired device, no any setting required to watch BLE data on Wireshark $_{\circ}$ 



# 2.2 Protocol Filtering



After BLE device connected, there are many empty packets presents, the desired effected data will be overwhelmed, The protocol filtering feature supplied by Wireshark could help on this issue, For example, in Wireshark filtering expression input box type "btatt" then press enter button on PC, Wireshark will filter off all empty packet and leave only ATT protocol data, take it easy to watch all desired data. If no filtering required, delete "btatt" then press enter again, all data will comes back. Data filtering doesn't lose any captured data.



# 2.3 BLE Protocol Interpret

```
▶ Frame 21822: 22 bytes on wire (176 bits), 22 bytes captured (176 bits) on interface 0

■ Bluetooth

    [Source: unknown_0x50656ba6]
    [Destination: unknown_0x50656ba6]
▲ Bluetooth Low Energy Link Layer
    Access Address: 0x50656ba6
    [Master Address: 58:03:fa:52:6b:6c (58:03:fa:52:6b:6c)]
    [Slave Address: e5:ea:a5:97:9a:44 (e5:ea:a5:97:9a:44)]
  △ Data Header: 0x0d16
      000. .... = RFU: 0
...1 .... = More Data: True
      .... 0... = Sequence Number: 0
      .... .1.. = Next Expected Sequence Number: 1
       .... ..10 = LLID: Start of an L2CAP message or a complete L2CAP message with no fragmentation (0x2)
      000. .... = RFU: 0
       ...0 1101 = Length: 13
  △ CRC: 0xdae33b
     ▲ [Expert Info (Note/Checksum): CRC unchecked, not all data available]
         [CRC unchecked, not all data available]
         [Severity level: Note]
         [Group: Checksum]
▲ Bluetooth L2CAP Protocol
    Length: 9
    CID: Attribute Protocol (0x0004)
△ Bluetooth Attribute Protocol
  ■ Opcode: Handle Value Notification (0x1b)
      0... = Authentication Signature: False
       .0.. .... = Command: False
       ..01 1011 = Method: Handle Value Notification (0x1b)

■ Handle: 0x0016 (Unknown: Pressure)

      [Service UUID: Unknown (0x1950)]
      [UUID: Pressure (0x2a6d)]
    Pressure: 0x280104a1
```

Click to select one frame of captured data on Wireshark, Interpreted BLE data will be displayed, it's great help on analysis of BLE protocol, data transmission in detail, error discovering and debugging,



# 2.4 Capturing Encrypted Data

```
Time
                                                                 Protocol Lengt Info
                         Source
                                              Destination
                                                                           40 L2CAP Fragment
    53498 3569.642429
                          unknown_0x506574a1
                                              unknown_0x506574a1 LE LL
                         unknown_0x506574a1 unknown_0x506574a1 LE LL
    53499 3570.109964
                                                                            9 Empty PDU
                                                                           40 L2CAP Fragment
    53500 3570.110458
                         unknown 0x506574a1 unknown 0x506574a1 LE LL
    53501 3570.110694
                         unknown_0x506574a1
                                              unknown_0x506574a1 LE LL
                                                                           9 Empty PDU
    53502 3570.111159
                         unknown 0x506574a1 unknown 0x506574a1 LE LL
                                                                           40 L2CAP Fragment
                         unknown_0x506574a1 unknown_0x506574a1 LE LL
    53503 3570.111395
                                                                           9 Empty PDU
    53504 3570.578705
                         unknown_0x506574a1 unknown_0x506574a1 LE LL
                                                                            9 Empty PDU
                                                                           40 L2CAP Fragment
                         unknown_0x506574a1 unknown_0x506574a1 LE LL
    53505 3570.579193
    53506 3570.579420
                         unknown_0x506574a1 unknown_0x506574a1 LE LL
                                                                           9 Empty PDU
                         unknown_0x506574a1 unknown_0x506574a1 LE LL unknown_0x506574a1 unknown_0x506574a1 LE LL
    53507 3570.579888
                                                                           40 L2CAP Fragment
    53508 3570.580130
                                                                           9 Empty PDU
    53509 3571.047441
                         unknown_0x506574a1 unknown_0x506574a1 LE LL
                                                                            9 Empty PDU
                                                                           40 L2CAP Fragment
    53510 3571.047930
                         unknown_0x506574a1 unknown_0x506574a1 LE LL
    53511 3571.048156
                         unknown_0x506574a1
                                              unknown_0x506574a1 LE LL
                                                                            9 Empty PDU
    53512 3571.048625
                         unknown_0x506574a1 unknown_0x506574a1 LE LL
                                                                           40 L2CAP Fragment
    53513 3571.048867
                         unknown_0x506574a1 unknown_0x506574a1 LE LL
                                                                            9 Empty PDU
                                              unknown_0x506574a1 LE LL
    53514 3571.516177
                         unknown_0x506574a1
                                                                            9 Empty PDU
    53515 3571.516665
                         unknown_0x506574a1 unknown_0x506574a1 LE LL
                                                                           40 L2CAP Fragment
    53516 3571.516891
                         unknown_0x506574a1 unknown_0x506574a1 LE LL
                                                                            9 Empty PDU
    53517 3571 517350
                          unknown 0v50657/101 unknown 0v50657/101 LF LL
                                                                            AA LOCAD Enom
  △ Data Header: 0x1f1a
      000. .... = RFU: 0
      ...1 .... = More Data: True
      .... 1... = Sequence Number: 1
      .... .0.. = Next Expected Sequence Number: 0
      .... ..10 = LLID: Start of an L2CAP message or a complete L2CAP message with no fragmentation (0x2)
      000. .... = RFU: 0
      ...1 1111 = Length: 31
    L2CAP Fragment
  [Expert Info (Note/Checksum): CRC unchecked, not all data available]
         [CRC unchecked, not all data available]
         [Severity level: Note]
         [Group: Checksum]
     a1 74 65 50 1a 1f 51 88 df 32 d5 82 20 9f 54 76
                                                         .teP..Q. .2.. .Tv
     70 36 ec e0 06 08 b5 87 39 f8 6a 24 2e b6 61 f1
                                                         p6..... 9.j$..a.
0020 bb d0 26 88 98 97 b9 a0
                                                         ......
```

Hollong BLE Sniffer is capable to capture encrypted data (SMP protocol), Wireshark only display captured encrypted raw data instead of decrypted data in this version.

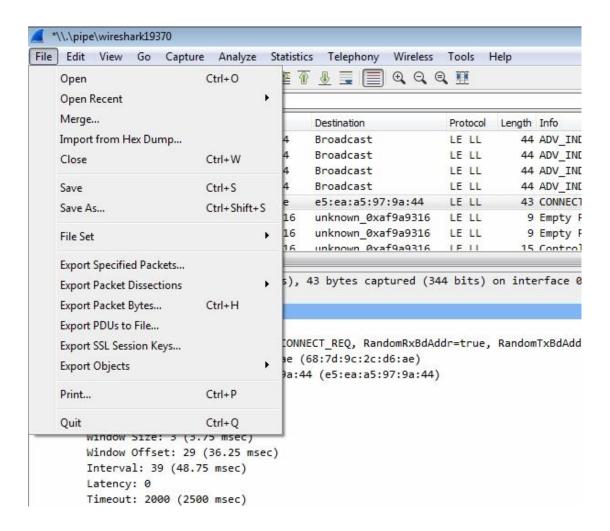


### 2.5 Other Features

```
0000 d6 be 89 8e 00 1b 9d 6a c6 39 36 d4 02 01 06 05 .....j .96.....

0010 02 e0 ff e0 fe 0b ff 8f 49 88 a0 d4 36 39 c6 6a 0020 9d 8d 9b 56 ....V
```

Wireshark could display raw BLE data, It's convenient to compare captured raw data with the data in BLE master and slave device.



Wireshark supply captured data save to file function to ease restore saved file data to display in anytime.



# 3. Technical Support And Services

- Lifetime technical support, one year free repairing or replacement (in case);
- Driver, Software, User Manual, Application source code could be downloaded at:www.viewtool.com;
- BBS: <u>www.viewtool.com/bbs</u>
- Technical support email: <u>fae@viewtool.com</u>
- Sales email: <u>sales@viewtool.com</u>

Company official wechat account:

