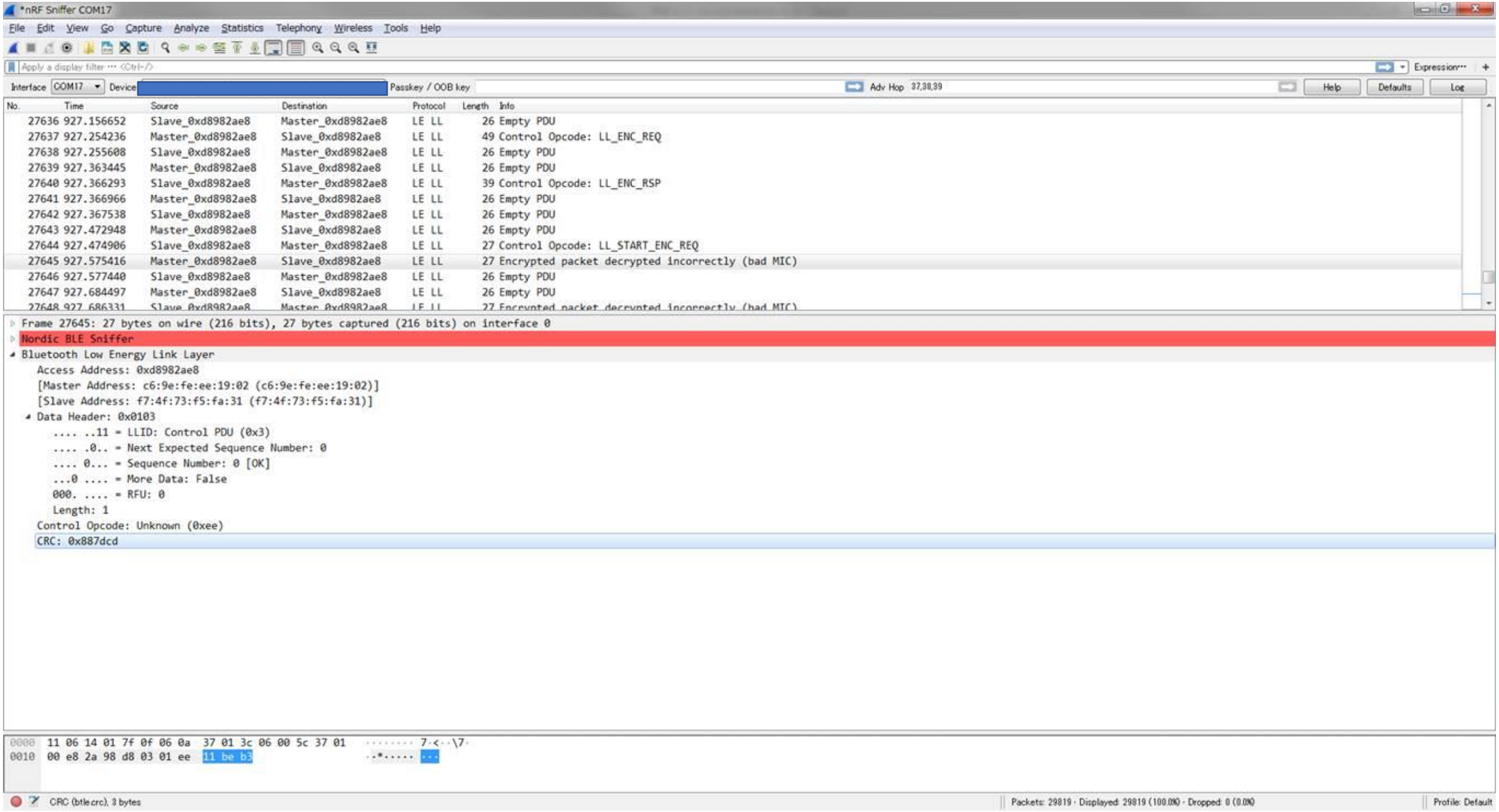
5.5 Sniffing a connection between devices that are already paired

The Sniffer needs to have sniffed the pairing procedure if the devices are already paired. If the sniffer board is reset, stored pairing information will be lost.

To sniff a connection encrypted with passkey:

1. Start the Sniffer if not already running.
2. In the Sniffer, choose the device from the Device drop-down list.
3. Initiate pairing between the devices if it does not happen automatically. A passkey will be displayed on either the Central or the Peripheral device.
4. Type the 6 digit passkey from the passkey text field in Wireshark.
5. Press **Enter**.
6. Enter the passkey into the other device after entering it into the Sniffer.


*nRF Sniffer COM17
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>
Expression···
Interface COM17 Device [redacted] Passkey / OOB key Adv Hop 37,38,39 Help Defaults Log
No. Time Source Destination Protocol Length Info
27636 927.156652 Slave_0xd8982ae8 Master_0xd8982ae8 LE LL 26 Empty PDU
27637 927.254236 Master_0xd8982ae8 Slave_0xd8982ae8 LE LL 49 Control Opcode: LL_ENC_REQ
27638 927.255608 Slave_0xd8982ae8 Master_0xd8982ae8 LE LL 26 Empty PDU
27639 927.363445 Master_0xd8982ae8 Slave_0xd8982ae8 LE LL 26 Empty PDU
27640 927.366293 Slave_0xd8982ae8 Master_0xd8982ae8 LE LL 39 Control Opcode: LL_ENC_RSP
27641 927.366966 Master_0xd8982ae8 Slave_0xd8982ae8 LE LL 26 Empty PDU
27642 927.367538 Slave_0xd8982ae8 Master_0xd8982ae8 LE LL 26 Empty PDU
27643 927.472948 Master_0xd8982ae8 Slave_0xd8982ae8 LE LL 26 Empty PDU
27644 927.474906 Slave_0xd8982ae8 Master_0xd8982ae8 LE LL 27 Control Opcode: LL_START_ENC_REQ
27645 927.575416 Master_0xd8982ae8 Slave_0xd8982ae8 LE LL 27 Encrypted packet decrypted incorrectly (bad MIC)
27646 927.577440 Slave_0xd8982ae8 Master_0xd8982ae8 LE LL 26 Empty PDU
27647 927.684497 Master_0xd8982ae8 Slave_0xd8982ae8 LE LL 26 Empty PDU
27648 927.686331 Slave_0xd8982ae8 Master_0xd8982ae8 LE LL 27 Encrypted packet decrypted incorrectly (bad MIC)
Frame 27645: 27 bytes on wire (216 bits), 27 bytes captured (216 bits) on interface 0
Nordic BLE Sniffer
Bluetooth Low Energy Link Layer
Access Address: 0xd8982ae8
[Master Address: c6:9e:fe:ee:19:02 (c6:9e:fe:ee:19:02)]
[Slave Address: f7:4f:73:f5:fa:31 (f7:4f:73:f5:fa:31)]
Data Header: 0x0103
.... ..11 = LLID: Control PDU (0x3)
.... .0.. = Next Expected Sequence Number: 0
.... 0... = Sequence Number: 0 [OK]
...0 .... = More Data: False
000. .... = RFU: 0
Length: 1
Control Opcode: Unknown (0xee)
CRC: 0x887dcd
0000 11 06 14 01 7f 0f 06 0a 37 01 3c 06 00 5c 37 01 .... 7·<··\7·
0010 00 e8 2a 98 d8 03 01 ee 11 be b3 ··*..... ···
CRC (btle.crc), 3 bytes
Packets: 29819 · Displayed: 29819 (100.0%) · Dropped: 0 (0.0%)
Profile: Default