EV3 Basic:

There are two files in the compressed file, including a .jpg and .pklg.

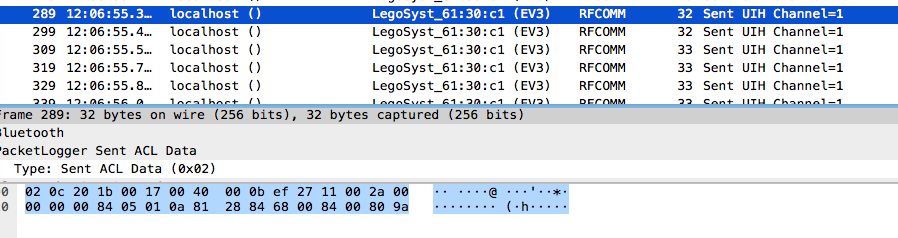
For my mac, the default application to open .pklg file is wireshark, although I haven’t seen this file extension before. The .jpg is shown what the EV3 looks like.

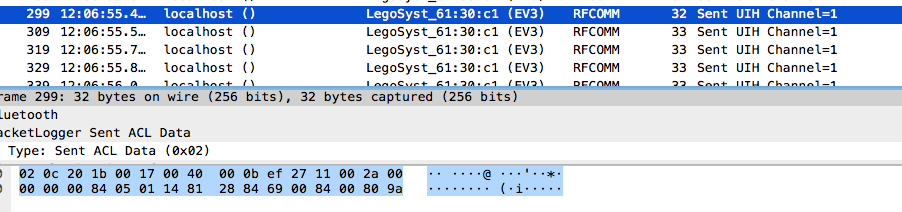
After taking a look, the .pklg file format is similar to pcap or pcapng. In the file, there are timestamp, source/destination (which are characterized as either controller or host), protocol (PKTLOG, HCI\*, L2CAP…), length and info sections.

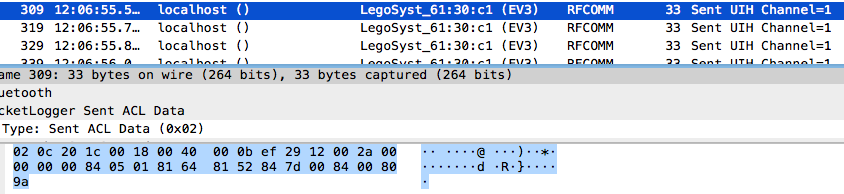
I sorted the source/destination, protocols, and info sections sequentially.

Find out that, with sorting by source, in localhost section:

No. 289, 299, 309…etc showing something interested: hi}







This looks like the beginning and ending of the flag: hixxxxxxxxxxxx}

But, that didn’t make any sense to me since there were bunches of letters missing in the session.

At first, I just noticed that I should take two parameters into consideration for a packet rather than one character. That is: (h, (I, R) etc.

So the result would be:

( 🡪h I { 1 n c d o t …

R 🡪} …

D 🡪 e …

6 🡪 a

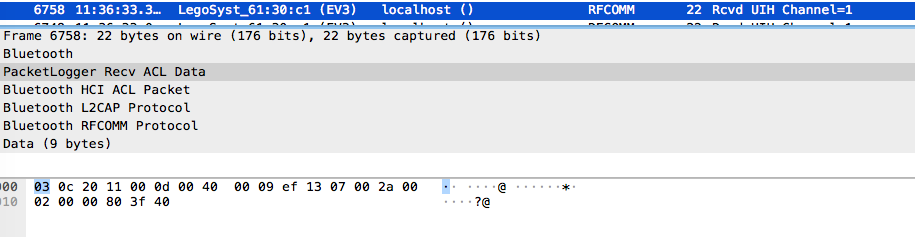
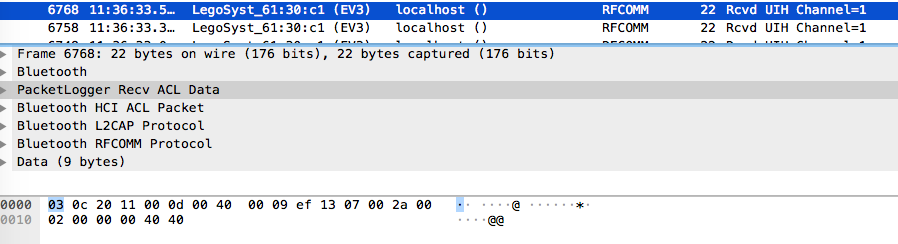
However, that’s still not make sense to me. Based on this order, I cannot get a flag. So I study the packet again and draw, comparing the changing things in different but related packets:

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Parameter1  (might be group) | Parameter2  (might be flag) | Changing bit  (hex=decimal) |
| 289 | ( | H | 0a = 10 |
| 299 | ( | i | 14 = 20 |
| 309 | R | } |  |
| 319 | ( | { | 46 = 70 |
| 329 | ( | 1 | 5a = 90 |
| 339 | ( | n | 3c = 60 |
| 349 | D | e |  |
| 359 | ( | c | 28 = 40 |
| 389 | ( | t | 1e = 30 |
| Keep filling the form | | | |
| Compose: (use the changing bit number as the order from small to big)  Ex:  10-h  20-hi  30-hit  40-hitc  then I get the flag: hitcon{m1nd5t0rm\_communication\_and\_firmware\_developer\_kit} | | | |

EV3 scanner

I sorted source/destination, protocol, length and info separately.

Then, I found that when info section is “Rcvd UIH Channel=1”, the data section looks almost the same for each packet, beside of some are “00 40”, some are “80 3f”. Seeing that it's a scanner on the white paper with black strokes, I deduced that’s the signal when scanning white and black. Moreover, it’s kinds of a car to scan, when meeting the end, the car reversed.(like S track)



|  |
| --- |
| #different line  flagl0 = ""  flagl1 = ""  flagl2 = ""  ...  for i in range(0, len(data)):  temp = "".join(data[i]["\_source"]["layers"]["data"]["data.data"].split(":"))  #turn  if turn == 0:  flagl0 += " "  elif turn == 1:  flagl1 += " "  ....    #put on mark  if detect == '80' and detect == '00':  if turn == 0:  flag10 += "#"  elif turn == 1:  flag11 += "#"  ....  print (flag10)  print (flat11)  ... |