

help trying to reverse engineer CRC algorithm

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2008-07/msg00025.html>

- *From:* mramirez <manologab@xxxxxxxxxx>
 - *Date:* Fri, 4 Jul 2008 13:16:27 -0700 (PDT)
-

Hi,

This a protocol I'm trying to implement but I can't figure out what's the CRC algorithm used (assuming that it's indeed a CRC).

Here are some captures, I included those that I consider more helpful.

This packages are all 136 bytes long, all the are filled with 0x00, each line is a diferent packet except the last one.

```
26 00 00 00 .... 00 AD D2 7E
26 05 00 00 .... 00 2A 24 7E
26 04 00 00 .... 00 0B BA 7E
26 20 00 00 .... 00 AE 8F 7E
26 21 00 00 .... 00 8F 11 7E
26 22 00 00 .... 00 FD BB 7E
26 23 00 00 .... 00 DC 25 7E
26 24 00 00 .... 00 08 E7 7E
26 28 00 00 .... 00 E2 5E 7E
26 02 01 00 .... 00 C4 1E 7E
27 43 02 15 38 30 39 33 30 37 36 35 35 30 40 61 6C 6C 74 65 6C 2E 6E
65\
74 00 .... 00 16 07 7E
```

There are other packages of different lengths also.

```
41 30 30 30 30 30 30 DF 8A 7E
41 01 70 41 7E
29 01 00 31 40 7E
```

I tried to apply the method described here:

<http://www.derkeiler.com/Newsgroups/sci.crypt/2006-05/msg01205.html>

with the 26 2x packets, but I got an strange result:

```
26 00 = ADD2
26 20 = AE8F
26 21 = 8F11
```

help trying to reverse engineer CRC algorithm

26 22 = FDBB

26 24 = 08E7

26 28 = E25E

$AE8F^{*2}8F11=219E$

$AE8F^{*2}FDBB=5334$

$AE8F^{*2}08E7=A668$

$AE8F^{*2}E25E=4CD1$

$219E^{*2} \wedge 5334 = 1008$

$5334^{*2} \wedge A668 = 0$

$A668^{*2} \wedge 4CD1 = 10001$

It feels like I'm almost there but I must be missing something obvious.

Any ideas?

Thanks in advance.

Manolo Ramirez T.

.