

### Challenge Name: Alpha Do You Copy

**Category: PCAP/MISC**

**Flag:** STMCTF{morse\_is\_morse}

Given PCAP file contains unusual traffic packets and SYN/ACK flag flows definitely does not fit with normal traffic standards.

No.	Time	Source	Destination	Protocol	Length	Info
44	2.853420000	58.79.105.23	58.79.105.23	TCP	54	[TCP Window Update] 2082 + 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
45	2.910540000	58.79.105.23	58.79.105.23	TCP	54	[TCP Window Update] 64140 + 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
46	2.989134000	58.79.105.23	58.79.105.23	TCP	54	[TCP Window Update] 34546 + 80 [None] Seq=1 Win=8192 Len=0
47	3.061378000	58.79.105.23	58.79.105.23	TCP	54	2824 + 80 [SYN] Seq=0 Win=8192 Len=0
48	3.126212000	58.79.105.23	58.79.105.23	TCP	54	[TCP Window Update] 23490 + 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
49	3.213793000	58.79.105.23	58.79.105.23	TCP	54	25770 + 80 [SYN] Seq=0 Win=8192 Len=0
50	3.268160000	58.79.105.23	58.79.105.23	TCP	54	[TCP Window Update] 32888 + 80 [None] Seq=1 Win=8192 Len=0
51	3.338499000	58.79.105.23	58.79.105.23	TCP	54	9510 + 80 [SYN] Seq=0 Win=8192 Len=0
52	3.406635000	58.79.105.23	58.79.105.23	TCP	54	9530 + 80 [SYN] Seq=0 Win=8192 Len=0
53	3.485330000	58.79.105.23	58.79.105.23	TCP	54	11278 + 80 [SYN] Seq=0 Win=8192 Len=0
54	3.554360000	58.79.105.23	58.79.105.23	TCP	54	[TCP Window Update] 11995 + 80 [None] Seq=1 Win=8192 Len=0
55	3.618310000	58.79.105.23	58.79.105.23	TCP	54	20704 + 80 [SYN] Seq=0 Win=8192 Len=0
56	3.676833000	58.79.105.23	58.79.105.23	TCP	54	[TCP Window Update] 42872 + 80 [None] Seq=1 Win=8192 Len=0
57	3.750274000	58.79.105.23	58.79.105.23	TCP	54	[TCP Window Update] 31844 + 80 [None] Seq=1 Win=8192 Len=0
58	3.813216000	58.79.105.23	58.79.105.23	TCP	54	[TCP Window Update] 11692 + 80 [None] Seq=1 Win=8192 Len=0
59	3.880405000	58.79.105.23	58.79.105.23	TCP	54	[TCP Window Update] 37734 + 80 [None] Seq=1 Win=8192 Len=0
60	3.970461000	58.79.105.23	58.79.105.23	TCP	54	[TCP Window Update] 802 + 80 [None] Seq=1 Win=8192 Len=0
61	0.474515000	58.79.105.23	58.79.105.23	TCP	54	[TCP Window Update] 21469 + 80 [None] Seq=1 Win=8192 Len=0
62	4.305649000	192.168.0.1	192.168.0.255	TCP	61	[TCP Retransmission] 0 + 0 [None] Seq=1 Win=65532 Len=0

```

> Frame 62: 61 bytes on wire (488 bits), 61 bytes captured (488 bits)
on Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.255
> Transmission Control Protocol, Src Port: 0, Dst Port: 0, Seq: 1, Len: 6
> VSS Monitoring Ethernet trailer, Source Port: 125

```

0000	00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00	.....E-
0010	00 2e 00 00 00 40 00 40 06 b8 79 c0 a8 00 01 c0 a8	...@...y.....
0020	00 ff 00 00 00 00 00 00 00 00 00 00 00 00 50 00	.....P.....
0030	ff fc 2d 91 00 00 00 00 00 00 00 00 00 7d	.....}

Since these flags are definitely in incorrect order, these may be used to send a message in different syntax. Converting TCP flags to the signals could work for morse like signal based communication.

Traffic contains only SYN, ACK and "NONE" flags.

Translating “ACK to -”, “SYN to .” and “No flags to ‘space’ ” gives following morse string;

----- . . . . .

Converting the output to ASCII provides the flag;

[illegible]