Packets primer

Forensics

Description

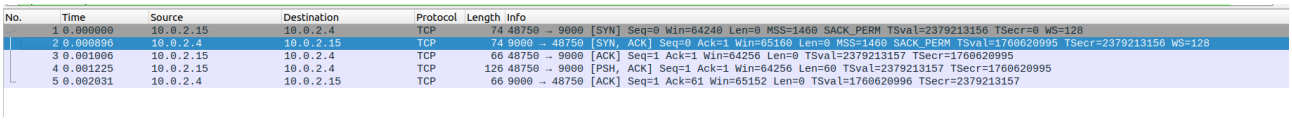
Download the packet capture file and use packet analysis software to find the flag.

Hints:

1) Wireshark, if you can install and use it, is probably the most beginner friendly packet analysis software product.

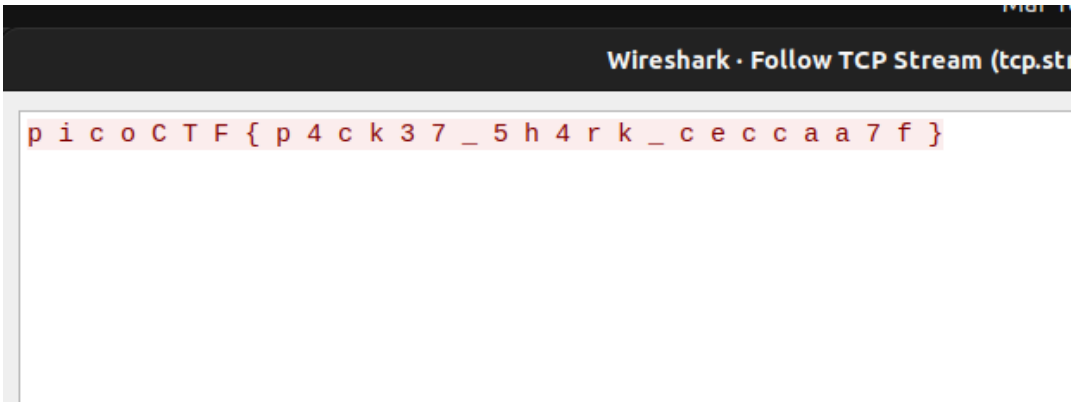
Solution:

1) We see the file type which is a packet capture type so we open it in wireshark.
2) We are interested in UDP and TCP protocols so we need to check them out in this file.
3) Go to the TCP protocols -> follow -> UDP Stream to find the information.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	10.0.2.4	TCP	74	48750 → 9000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2379213156 TSecr=0 WS=128
2	0.000890	10.0.2.4	10.0.2.15	TCP	74	9000 → 48750 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1760620995 TSecr=2379213156 WS=128
3	0.001006	10.0.2.15	10.0.2.4	TCP	66	48750 → 9000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2379213157 TSecr=1760620995
4	0.001225	10.0.2.15	10.0.2.4	TCP	126	48750 → 9000 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=60 TSval=2379213157 TSecr=1760620995
5	0.002031	10.0.2.4	10.0.2.15	TCP	66	9000 → 48750 [ACK] Seq=1 Ack=61 Win=65152 Len=0 TSval=1760620996 TSecr=2379213157

4) We find the flag in the TCP stream but it contains spaces.
5) Omit the spaces to get the final flag.



Flag: picoCTF{p4ck37_5h4rk_ceccaa7f}