Description

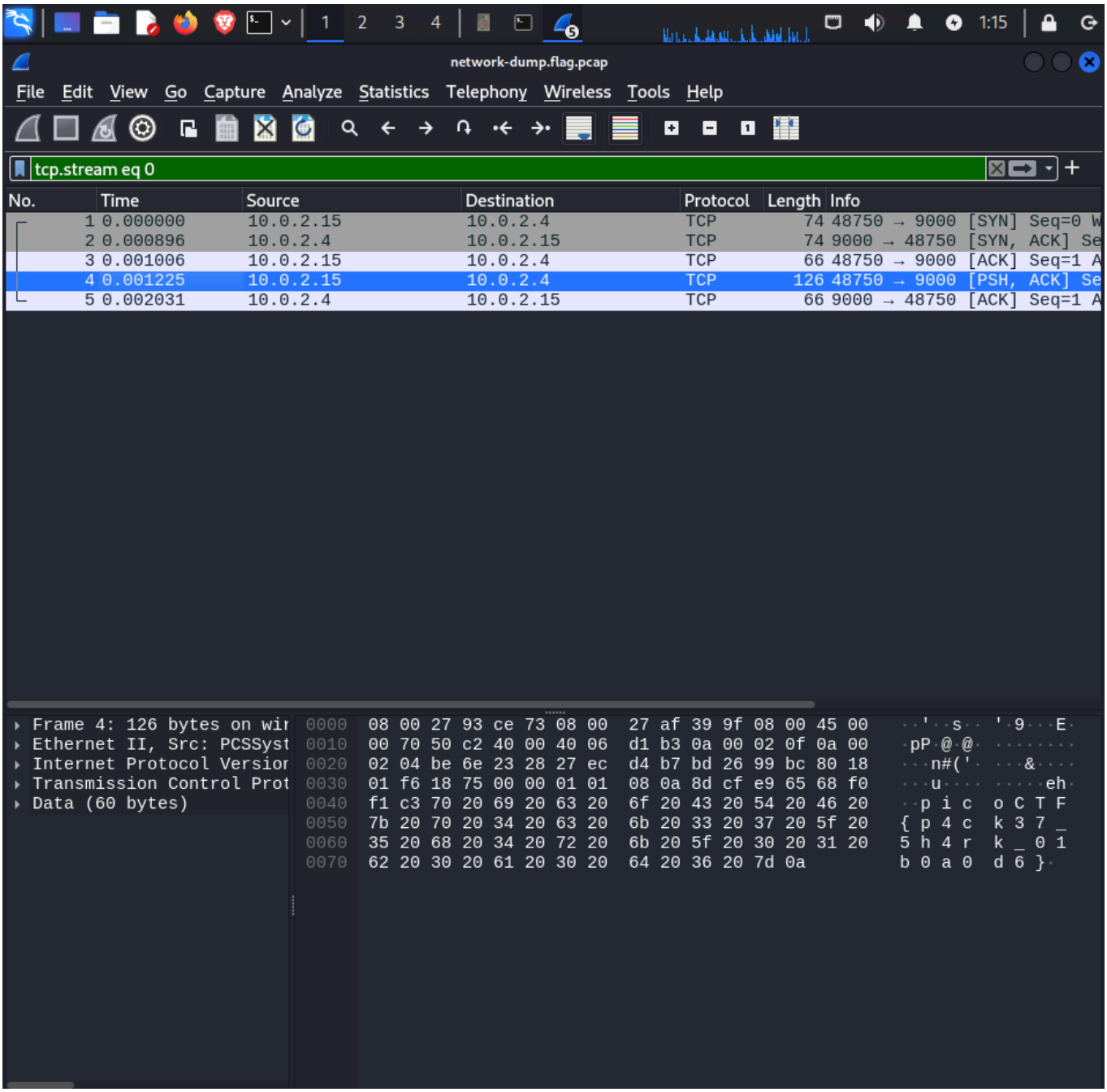
Download the packet capture file and use packet analysis software to find the flag.

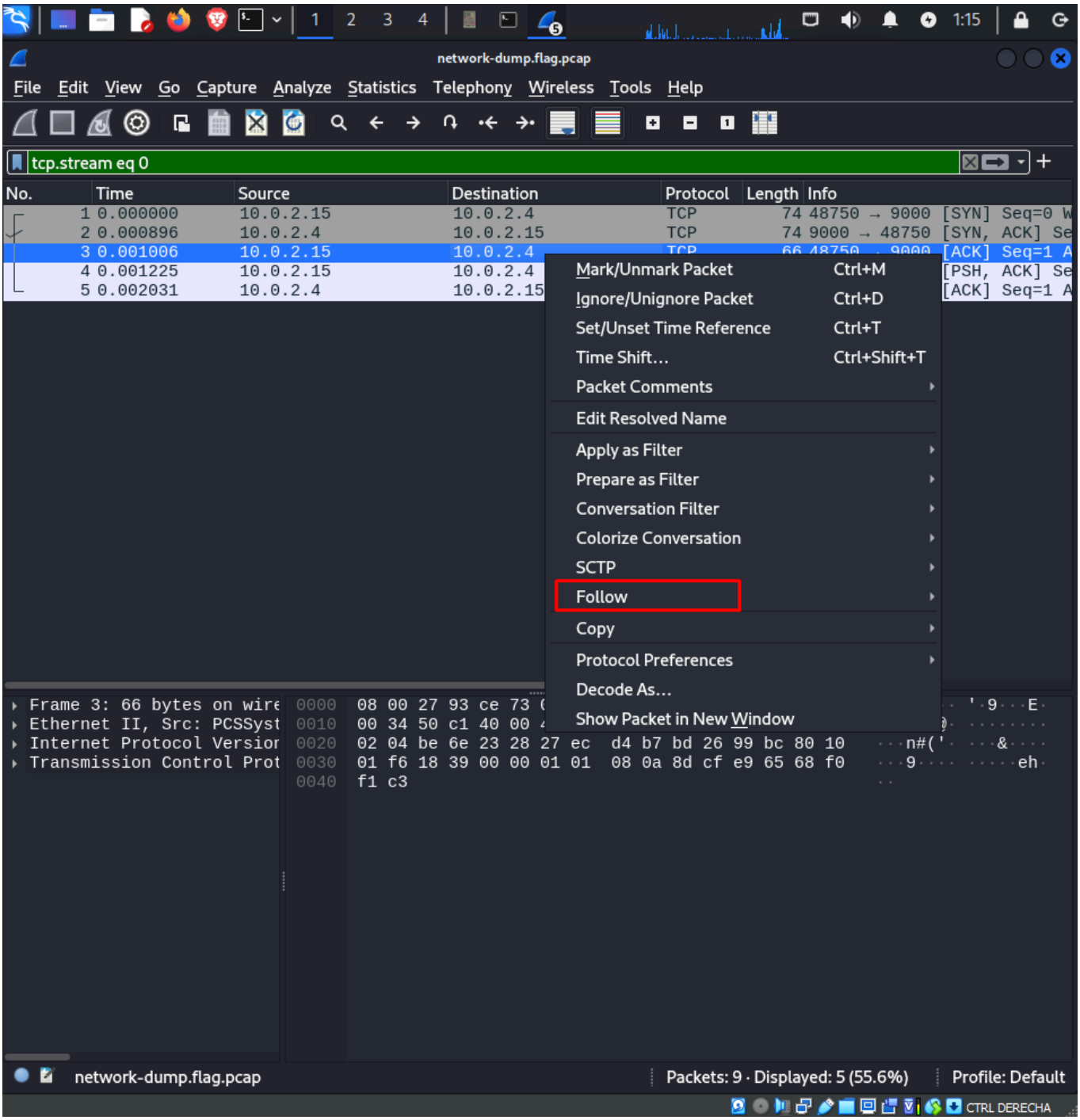
- Download packet capture

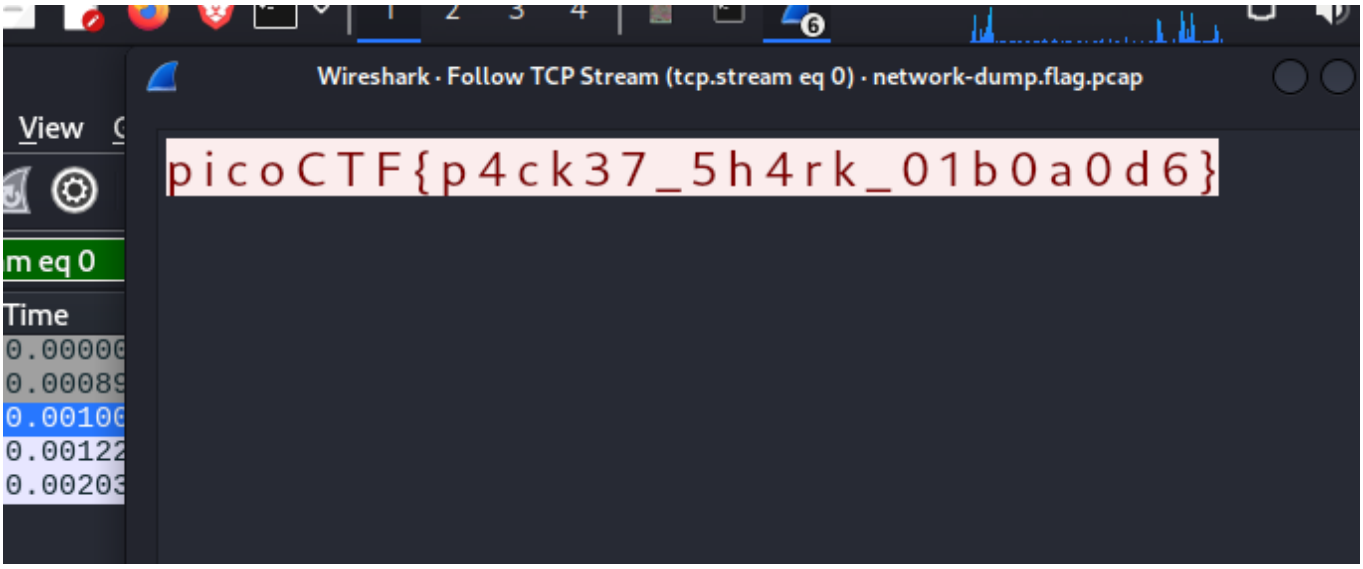
Hints

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

Solución


network-dump.flag.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
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 W
2 0.000896 10.0.2.4 10.0.2.15 TCP 74 9000 → 48750 [SYN, ACK] Se
3 0.001006 10.0.2.15 10.0.2.4 TCP 66 48750 → 9000 [ACK] Seq=1 A
4 0.001225 10.0.2.15 10.0.2.4 TCP 126 48750 → 9000 [PSH, ACK] Se
5 0.002031 10.0.2.4 10.0.2.15 TCP 66 9000 → 48750 [ACK] Seq=1 A
Frame 4: 126 bytes on wir
Ethernet II, Src: PCSSyst
Internet Protocol Versior
Transmission Control Prot
Data (60 bytes)
0000 08 00 27 93 ce 73 08 00 27 af 39 9f 08 00 45 00
0010 00 70 50 c2 40 00 40 06 d1 b3 0a 00 02 0f 0a 00
0020 02 04 be 6e 23 28 27 ec d4 b7 bd 26 99 bc 80 18
0030 01 f6 18 75 00 00 01 01 08 0a 8d cf e9 65 68 f0
0040 f1 c3 70 20 69 20 63 20 6f 20 43 20 54 20 46 20
0050 7b 20 70 20 34 20 63 20 6b 20 33 20 37 20 5f 20
0060 35 20 68 20 34 20 72 20 6b 20 5f 20 30 20 31 20
0070 62 20 30 20 61 20 30 20 64 20 36 20 7d 0a


network-dump.flag.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
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 W
2 0.000896 10.0.2.4 10.0.2.15 TCP 74 9000 → 48750 [SYN, ACK] Se
3 0.001006 10.0.2.15 10.0.2.4 [ACK] Seq=1 A
4 0.001225 10.0.2.15 10.0.2.4 [PSH, ACK] Se
5 0.002031 10.0.2.4 10.0.2.15 [ACK] Seq=1 A
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
Frame 3: 66 bytes on wire
Ethernet II, Src: PCSSyst
Internet Protocol Versior
Transmission Control Prot
0000 08 00 27 93 ce 73
0010 00 34 50 c1 40 00
0020 02 04 be 6e 23 28 27 ec d4 b7 bd 26 99 bc 80 10
0030 01 f6 18 39 00 00 01 01 08 0a 8d cf e9 65 68 f0
0040 f1 c3
network-dump.flag.pcap
Packets: 9 · Displayed: 5 (55.6%)
Profile: Default
CTRL DERECHA




```
┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_03_forensic_01/packets_primer]
└─$ wget https://artifacts.picoctf.net/c/196/network-dump.flag.pcap
--2024-11-06 02:13:48--  https://artifacts.picoctf.net/c/196/network-
dump.flag.pcap
Resolving artifacts.picoctf.net (artifacts.picoctf.net)... 3.161.55.64,
3.161.55.61, 3.161.55.100, ...
Connecting to artifacts.picoctf.net
(artifacts.picoctf.net)|3.161.55.64|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 778 [application/octet-stream]
Saving to: ‘network-dump.flag.pcap’

network-dump.flag.pcap 100%[============================>]     778  --.-KB/s
in 0.001s

2024-11-06 02:13:49 (1.35 MB/s) - ‘network-dump.flag.pcap’ saved [778/778]


┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_03_forensic_01/packets_primer]
└─$ wireshark network-dump.flag.pcap &
[2] 11355
```

Bandera

```
flag: picoCTF{p4ck37_5h4rk_01b0a0d6}
```

Notas Adicionales

Bastó con abrir el archivo `.pcap` en `wireshar` y seguir cualquier stream, ya que la flag se encontraba en todos.

Referencias

-