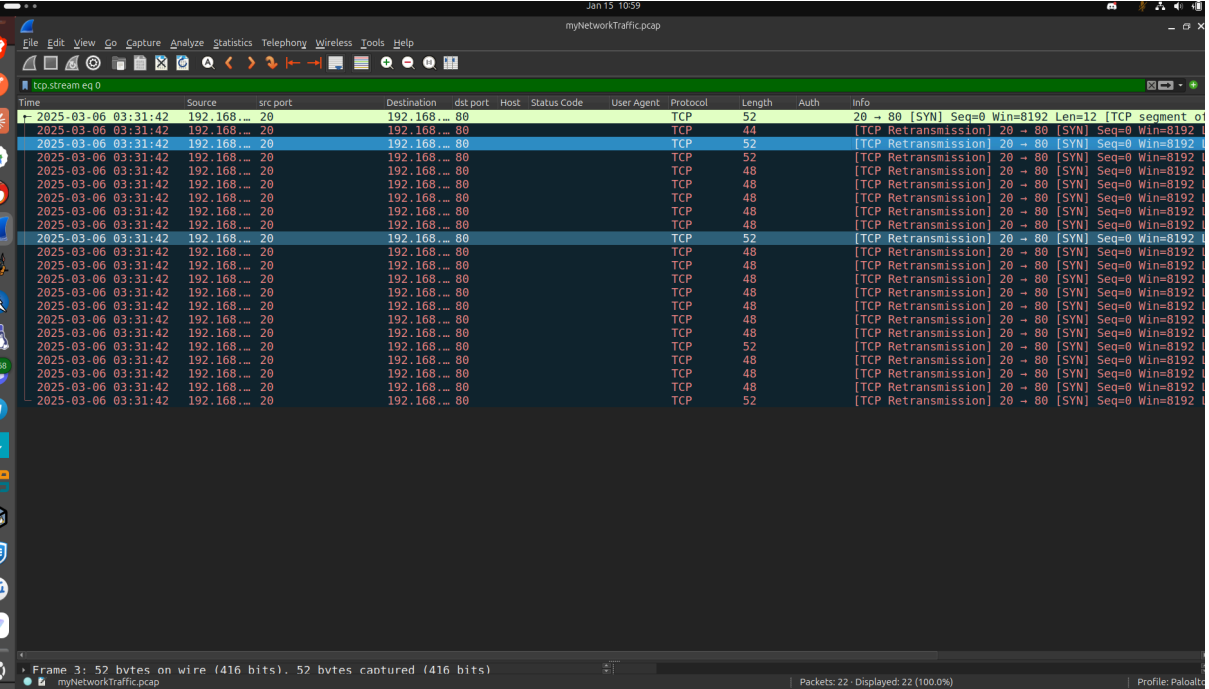


## Ph4nt0m 1ntrud3r

kami mendapatkan sebuah file pcap yang dimana didalamnya berisi sebuah traffic yang mencurigakan



The image shows a Wireshark network traffic capture of a file named 'myNetworkTraffic.pcap'. The capture was taken on Jan 15, 2025, at 10:59. The filter applied is 'tcp.stream eq 0'. The packet list shows a series of TCP segments from source 192.168.1.20 to destination 192.168.1.80. The first packet (Frame 1) is a SYN packet with Seq=0, Win=8192, Len=12. Subsequent packets (Frames 2-22) are retransmissions of this SYN packet, each with Seq=0, Win=8192, and Len=12. The status of these packets is 'Retransmission'. The packet details pane shows the TCP header fields: Seq=0, Win=8192, Len=12, and the info field indicates '[TCP Retransmission]'. The packet bytes pane shows the raw data of the SYN packet.

Time	Source	src port	Destination	dst port	Host	Status Code	User Agent	Protocol	Length	Auth	Info
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	52		20 → 80 [SYN] Seq=0 Win=8192 Len=12 [TCP segment of...
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	44		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	52		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	52		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	48		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192
2025-03-06 03:31:42	192.168.1.20	20	192.168.1.80	80				TCP	52		[TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192

Frame 3: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)

Packets: 22 · Displayed: 22 (100.0%)

Profile: Paloalto



Protocol	Length	Auth
TCP	52	
TCP	44	
TCP	52	
TCP	52	
TCP	48	
TCP	48	
TCP	48	
TCP	48	
TCP	48	
TCP	52	
TCP	48	
TCP	48	
TCP	48	
TCP	48	
TCP	48	
TCP	48	
TCP	48	
TCP	52	
TCP	48	
TCP	48	
TCP	48	
TCP	52	

ikuti request yang memiliki length terbesar yaitu 52 untuk melihat apa encoding yang di simpan didalamnya, ulangi hingga kalian mendapatkan potongan itu secara utuh

```
P · · /% · · NGI1Nzkw
0Q==
```

```
picoCTF
{1t_w4s
nt_th4
t_34sy
tbh_4r_d
4b57909}|
```

susun sesuai dengan perkata

picoCTF{1t\_w4snt\_th4t\_34sy\_tbh\_4r\_d4b57909}

picoCTF{1t\_w4snt\_th4t\_34sy\_tbh\_4r\_d4b57909}