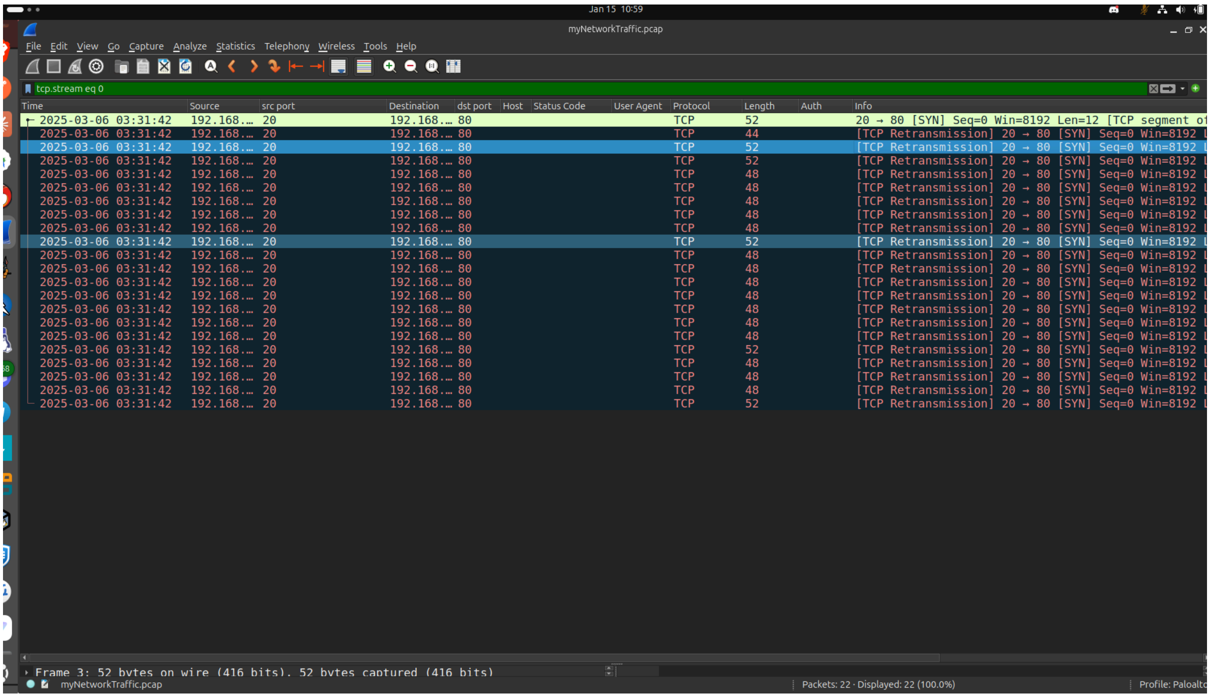
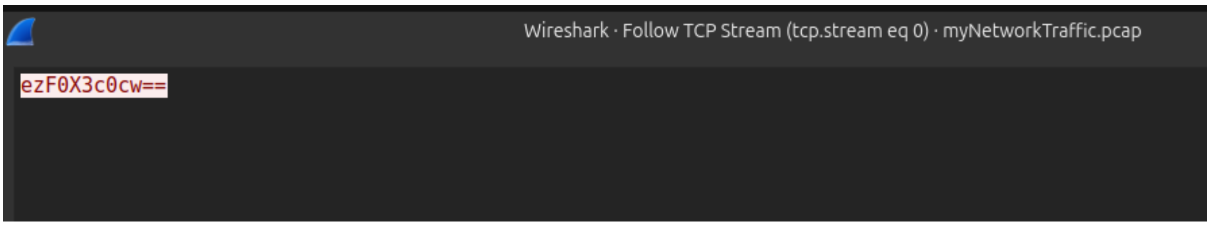
Ph4nt0m 1ntrud3r

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

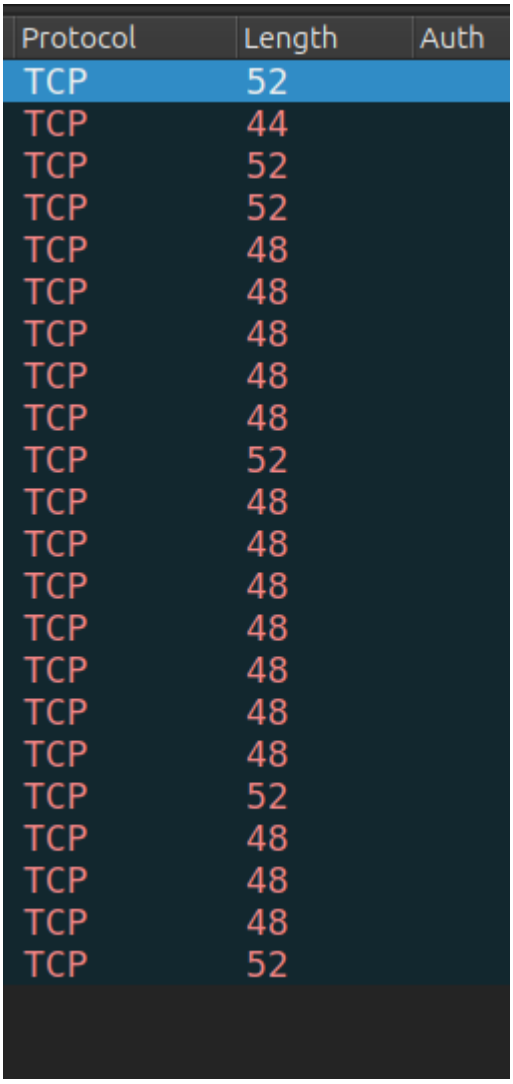


Source	src port	Destination
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2
192.168.0.2	20	192.168.1.2

melakukan analisa dengan mengikuti tcp request

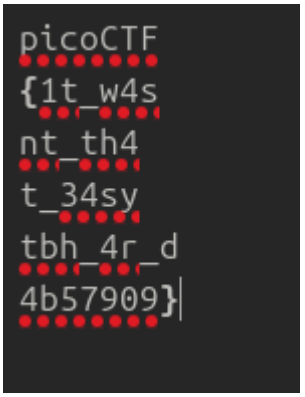


kami mendapatkan sebuah string base64 yang dimana kami bisa melakukan decoding pada string tersebut, kami menemukan potongan potongan flag di dalamnya.



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	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



susun sesuai dengan perkata

picoCTF{1t_w4snt_th4t_34sy_tbh_4r_d4b57909}