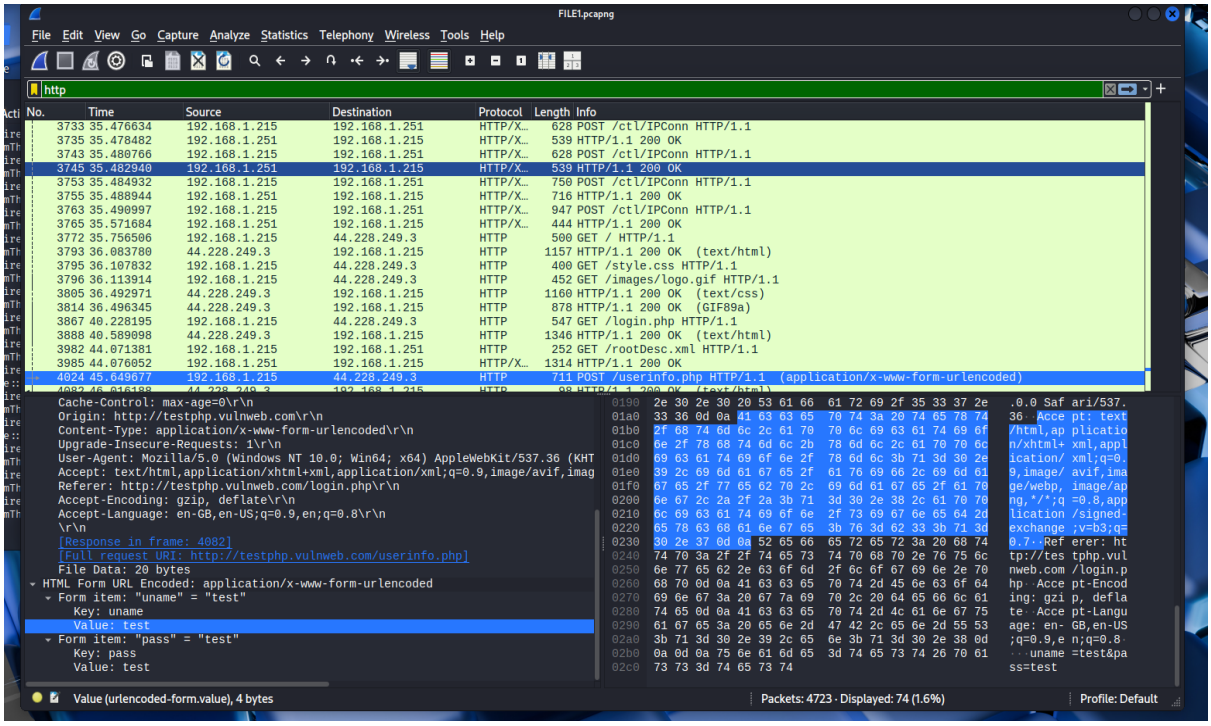
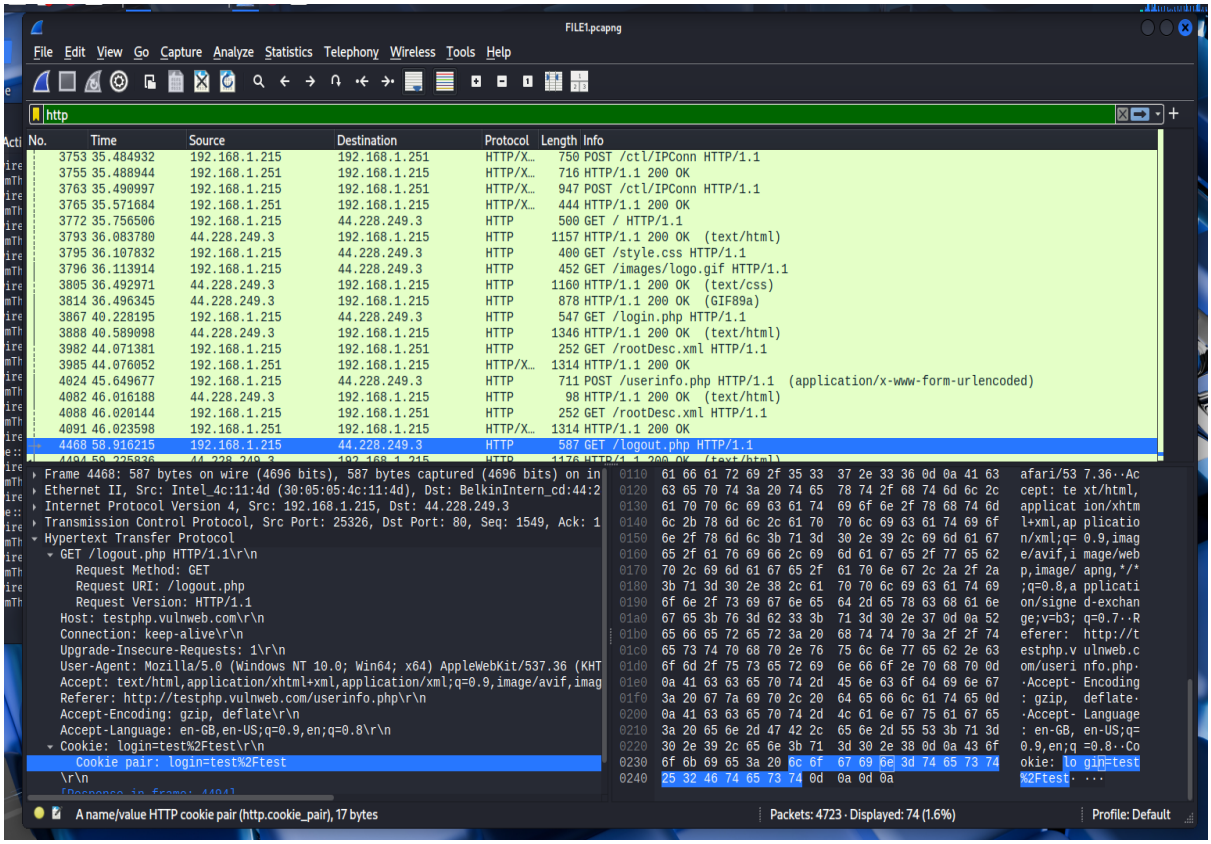
TASK 2

FILE 1

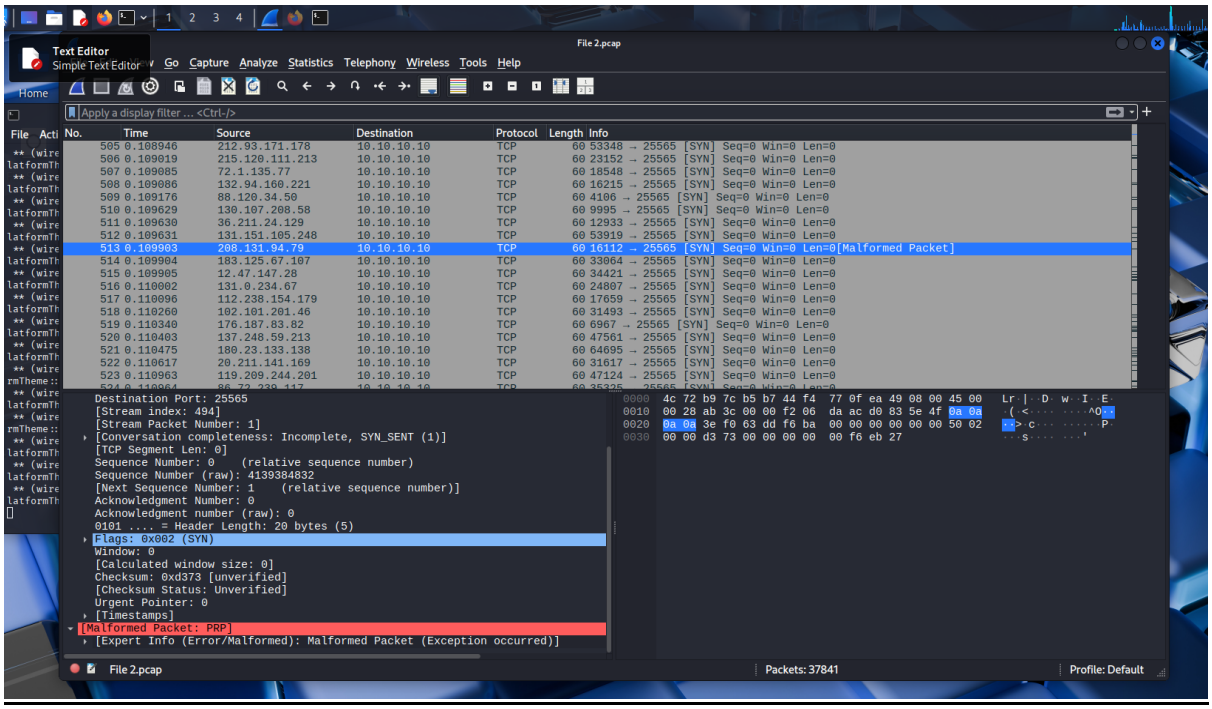
I was browsing unsecured website while my wireshark was active. Analyse the PCAP file and find out a credential present in the network logs.

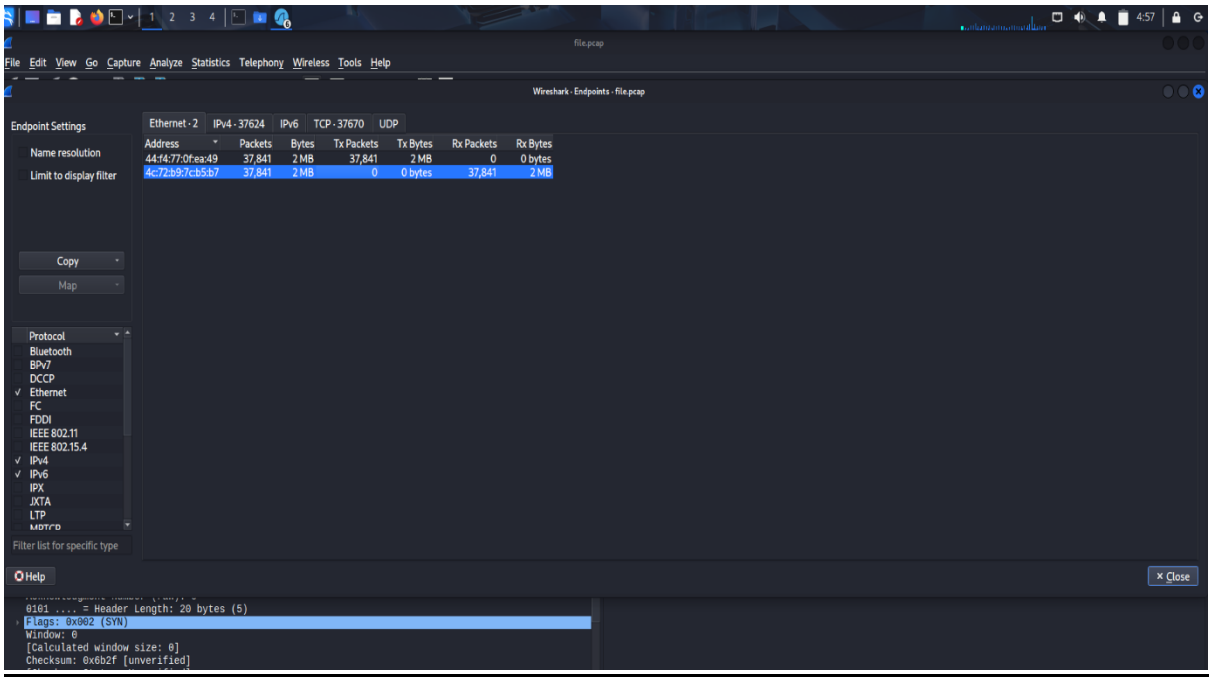


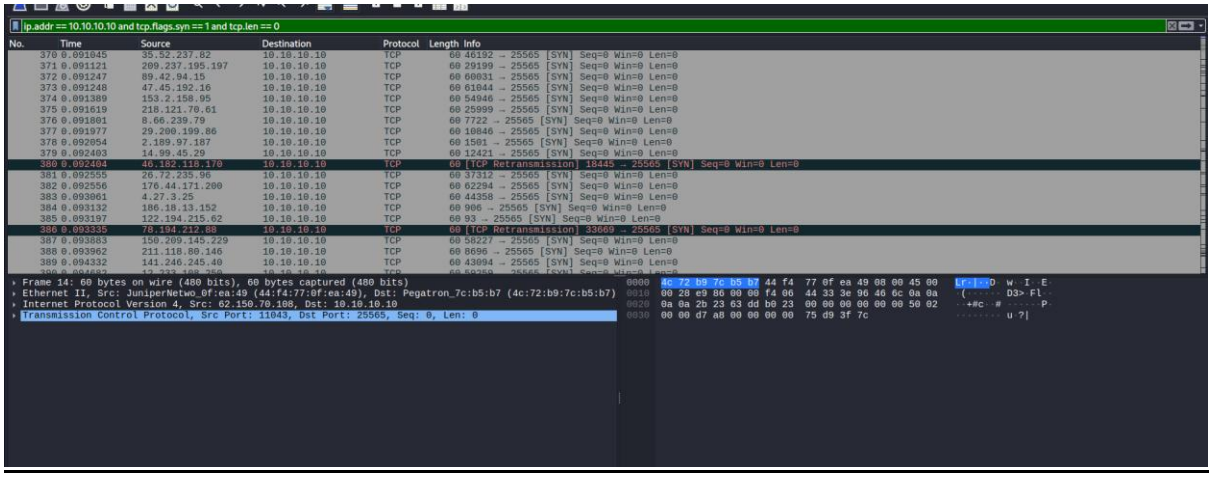


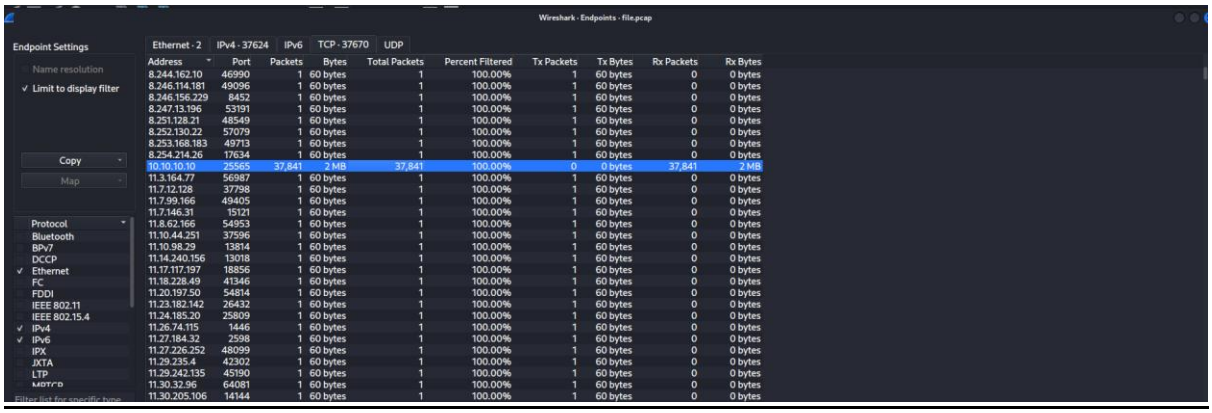
FILE 2

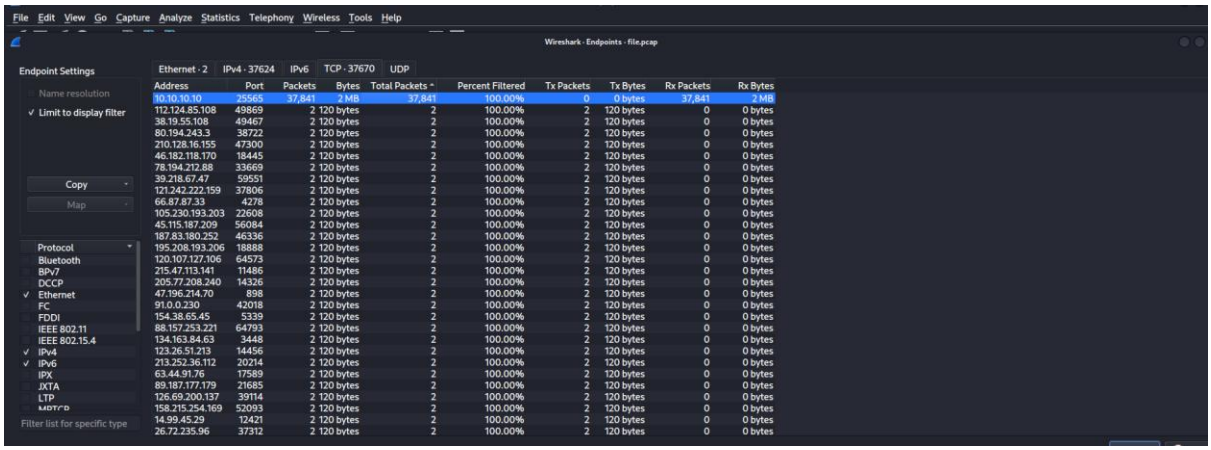
Analyse the file and tell me what's wrong with the network data

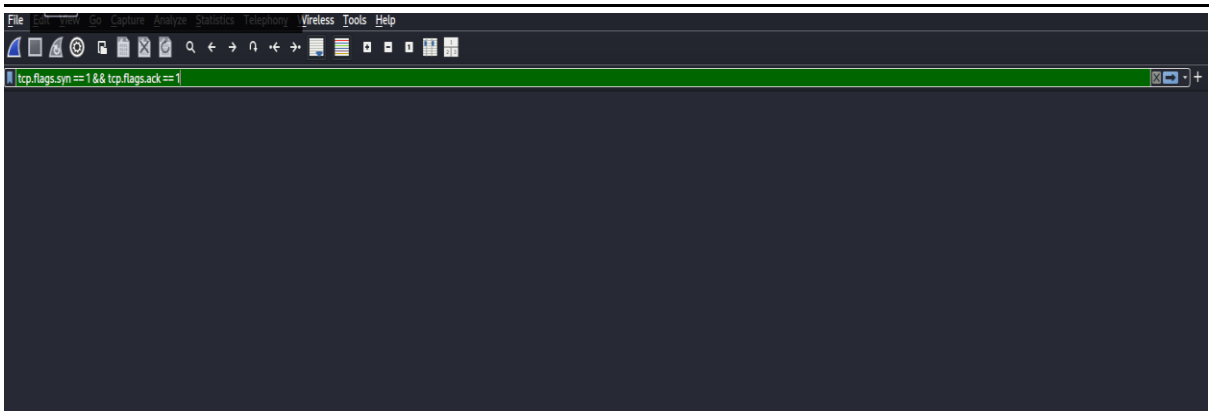


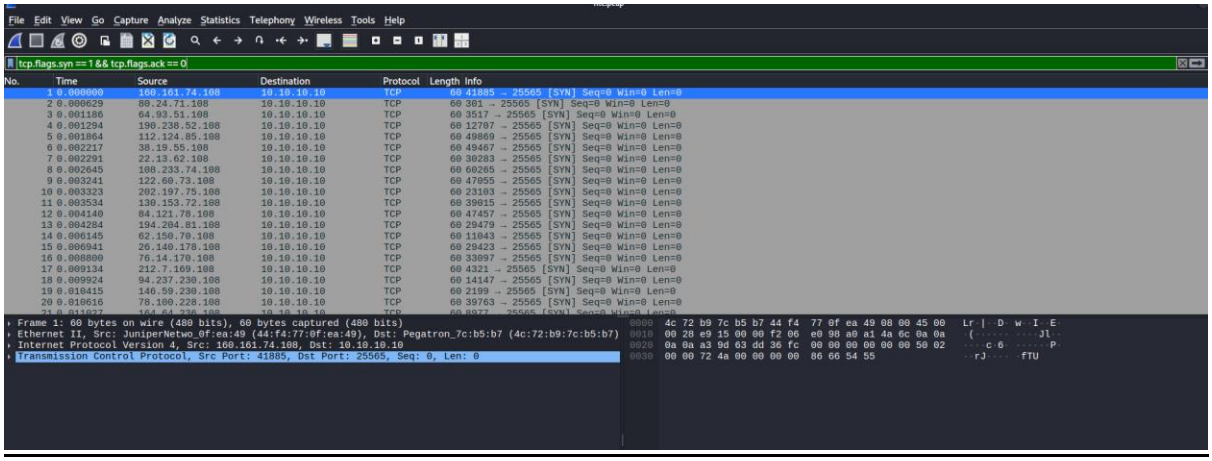



ip.addr == 10.10.10.10 and tcp.flags.syn == 1 and tcp.len == 0
No. Time Source Destination Protocol Length Info
370 0.091045 35.52.237.82 10.10.10.10 TCP 60 46192 → 25565 [SYN] Seq=0 Win=0 Len=0
371 0.091121 209.237.195.197 10.10.10.10 TCP 60 29199 → 25565 [SYN] Seq=0 Win=0 Len=0
372 0.091247 89.42.94.15 10.10.10.10 TCP 60 60031 → 25565 [SYN] Seq=0 Win=0 Len=0
373 0.091248 47.45.192.16 10.10.10.10 TCP 60 61044 → 25565 [SYN] Seq=0 Win=0 Len=0
374 0.091389 153.2.158.95 10.10.10.10 TCP 60 54946 → 25565 [SYN] Seq=0 Win=0 Len=0
375 0.091619 218.121.70.61 10.10.10.10 TCP 60 25999 → 25565 [SYN] Seq=0 Win=0 Len=0
376 0.091801 8.66.239.79 10.10.10.10 TCP 60 7722 → 25565 [SYN] Seq=0 Win=0 Len=0
377 0.091977 29.200.199.86 10.10.10.10 TCP 60 10846 → 25565 [SYN] Seq=0 Win=0 Len=0
378 0.092054 2.189.97.187 10.10.10.10 TCP 60 1501 → 25565 [SYN] Seq=0 Win=0 Len=0
379 0.092403 14.99.45.29 10.10.10.10 TCP 60 12421 → 25565 [SYN] Seq=0 Win=0 Len=0
380 0.092404 46.182.118.170 10.10.10.10 TCP 60 [TCP Retransmission] 18445 → 25565 [SYN] Seq=0 Win=0 Len=0
381 0.092555 26.72.235.96 10.10.10.10 TCP 60 37312 → 25565 [SYN] Seq=0 Win=0 Len=0
382 0.092556 176.44.171.200 10.10.10.10 TCP 60 62294 → 25565 [SYN] Seq=0 Win=0 Len=0
383 0.093061 4.27.3.25 10.10.10.10 TCP 60 44358 → 25565 [SYN] Seq=0 Win=0 Len=0
384 0.093132 186.18.13.152 10.10.10.10 TCP 60 906 → 25565 [SYN] Seq=0 Win=0 Len=0
385 0.093197 122.194.215.62 10.10.10.10 TCP 60 93 → 25565 [SYN] Seq=0 Win=0 Len=0
386 0.093335 78.194.212.88 10.10.10.10 TCP 60 [TCP Retransmission] 33669 → 25565 [SYN] Seq=0 Win=0 Len=0
387 0.093883 150.209.145.229 10.10.10.10 TCP 60 58227 → 25565 [SYN] Seq=0 Win=0 Len=0
388 0.093962 211.118.80.146 10.10.10.10 TCP 60 8696 → 25565 [SYN] Seq=0 Win=0 Len=0
389 0.094332 141.246.245.40 10.10.10.10 TCP 60 43094 → 25565 [SYN] Seq=0 Win=0 Len=0
Frame 14: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: JuniperNetwo_0f:ea:49 (44:f4:77:0f:ea:49), Dst: Pegatron_7c:b5:b7 (4c:72:b9:7c:b5:b7)
Internet Protocol Version 4, Src: 62.150.70.108, Dst: 10.10.10.10
Transmission Control Protocol, Src Port: 11043, Dst Port: 25565, Seq: 0, Len: 0
0000 4c 72 b9 7c b5 b7 44 f4 77 0f ea 49 08 00 45 00
0010 00 28 e9 86 00 00 f4 06 44 33 3e 96 46 6c 0a 0a
0020 0a 0a 2b 23 63 dd b0 23 00 00 00 00 00 00 50 02
0030 00 00 d7 a8 00 00 00 00 75 d9 3f 7c


Wireshark · Endpoints · file.pcap
Endpoint Settings
Ethernet · 2 IPv4 · 37624 IPv6 TCP · 37670 UDP
Address Port Packets Bytes Total Packets Percent Filtered Tx Packets Tx Bytes Rx Packets Rx Bytes
10.10.10.10 25565 37,841 2 MB 37,841 100.00% 0 0 bytes 37,841 2 MB


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Endpoints · file.pcap
Endpoint Settings
Ethernet · 2 IPv4 · 37624 IPv6 TCP · 37670 UDP
Address Port Packets Bytes Total Packets Percent Filtered Tx Packets Tx Bytes Rx Packets Rx Bytes
10.10.10.10 25565 37,841 2 MB 37,841 100.00% 0 0 bytes 37,841 2 MB


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1 && tcp.flags.ack == 1



Note: Per review found there is only SYN and no ACK, SYN = 1 and ACK = 0

So as a conclusion the type of attacks are SYN flood (A **SYN flood** is a form of denial-of-service attack on data communications in which an attacker rapidly initiates a connection to a server without finalizing the connection. The server has to spend resources waiting for half-opened connections, which can consume enough resources to make the system unresponsive to legitimate traffic.).

Also, as my assumption found port scanning too. port scanning itself is not inherently an attack, it is a common technique used in malicious attacks .