Network Traffic Analysis & Incident Investigation Using PCAP

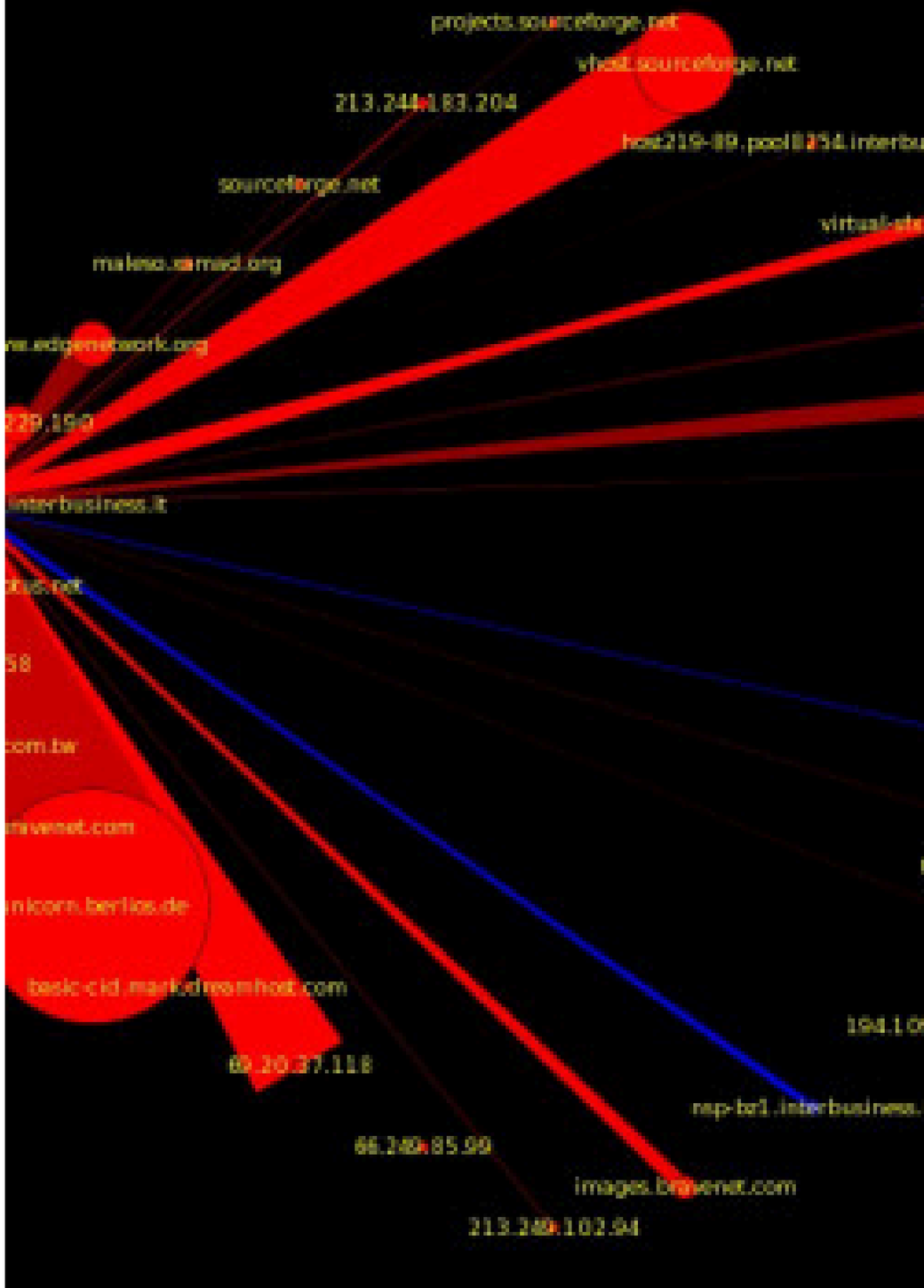
(SOC Analyst Simulation)

PRESENTED BY

SADHANA KUSHWAHA

ERP: 6606118

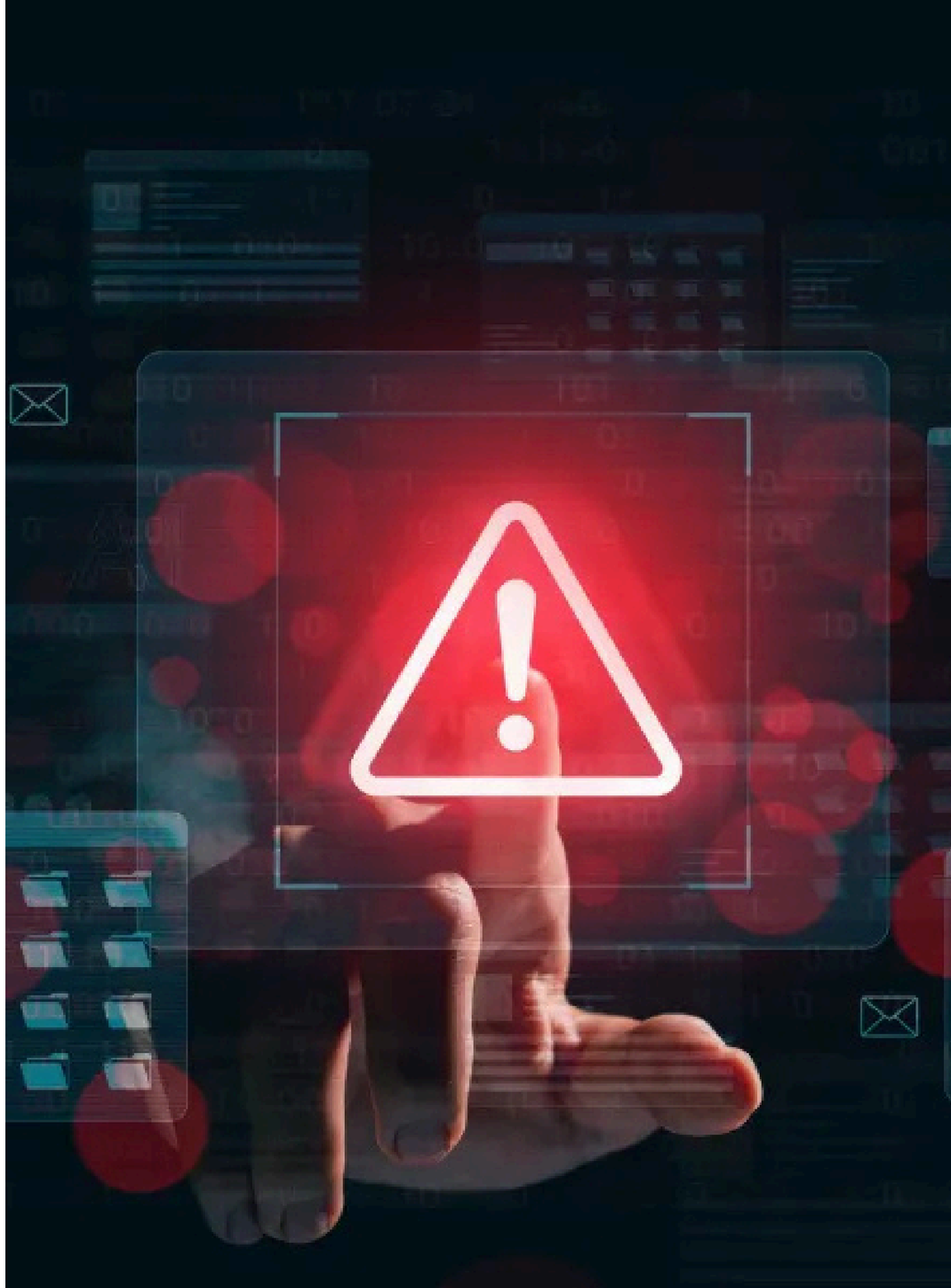
TABLE OF CONTENTS



PROJECT OVERVIEW

This project focuses on analyzing network traffic using PCAP files, simulating the role of a SOC Analyst.

The goal is to identify malicious activity, detect reconnaissance behavior, analyze HTTP traffic, and extract files from unencrypted network communication using Wireshark.

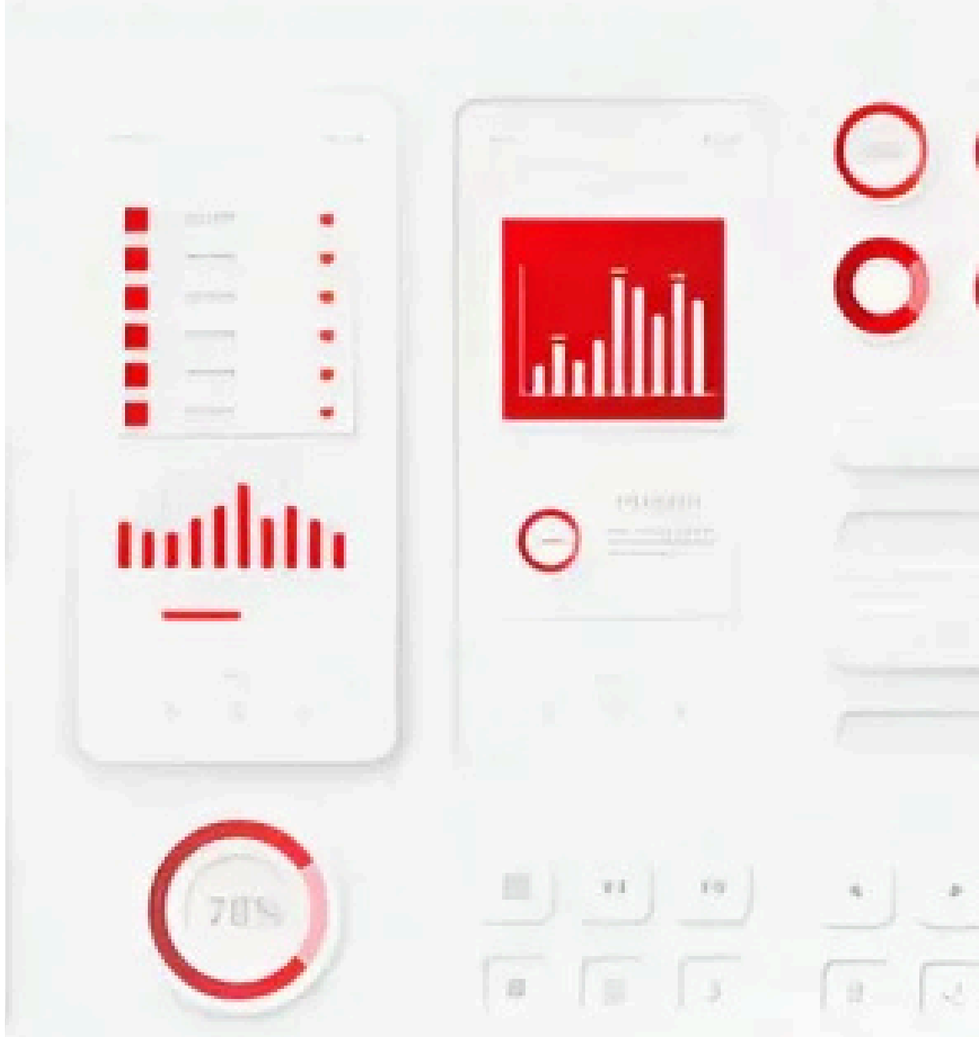


PROJECT OBJECTIVES

- Analyze PCAP files like a SOC Analyst.
- Identify attacker and victim IP addresses.
- Detect reconnaissance activity such as Nmap port scanning.
- Analyze HTTP traffic.
- Extract files from unencrypted network traffic.

TOOLS USED

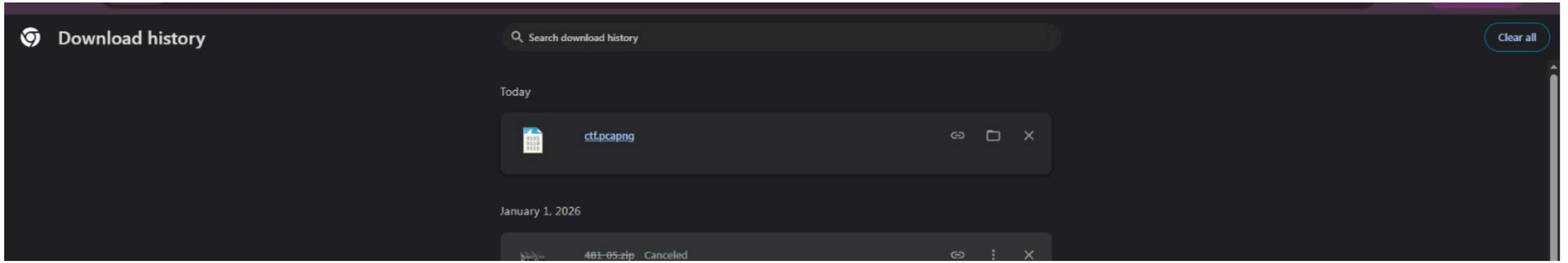
- **Wireshark:** Used to analyze PCAP files, identify attacker and victim IPs, detect port scanning, analyze HTTP traffic, and extract files.
- **Windows OS:** Host operating system used for performing the analysis.
- **PCAP File:** Network traffic capture provided for investigation.
- **ZIP Extraction Tool:** Used to extract the downloaded ZIP file and retrieve the flag.



METHODOLOGY & STEPS :

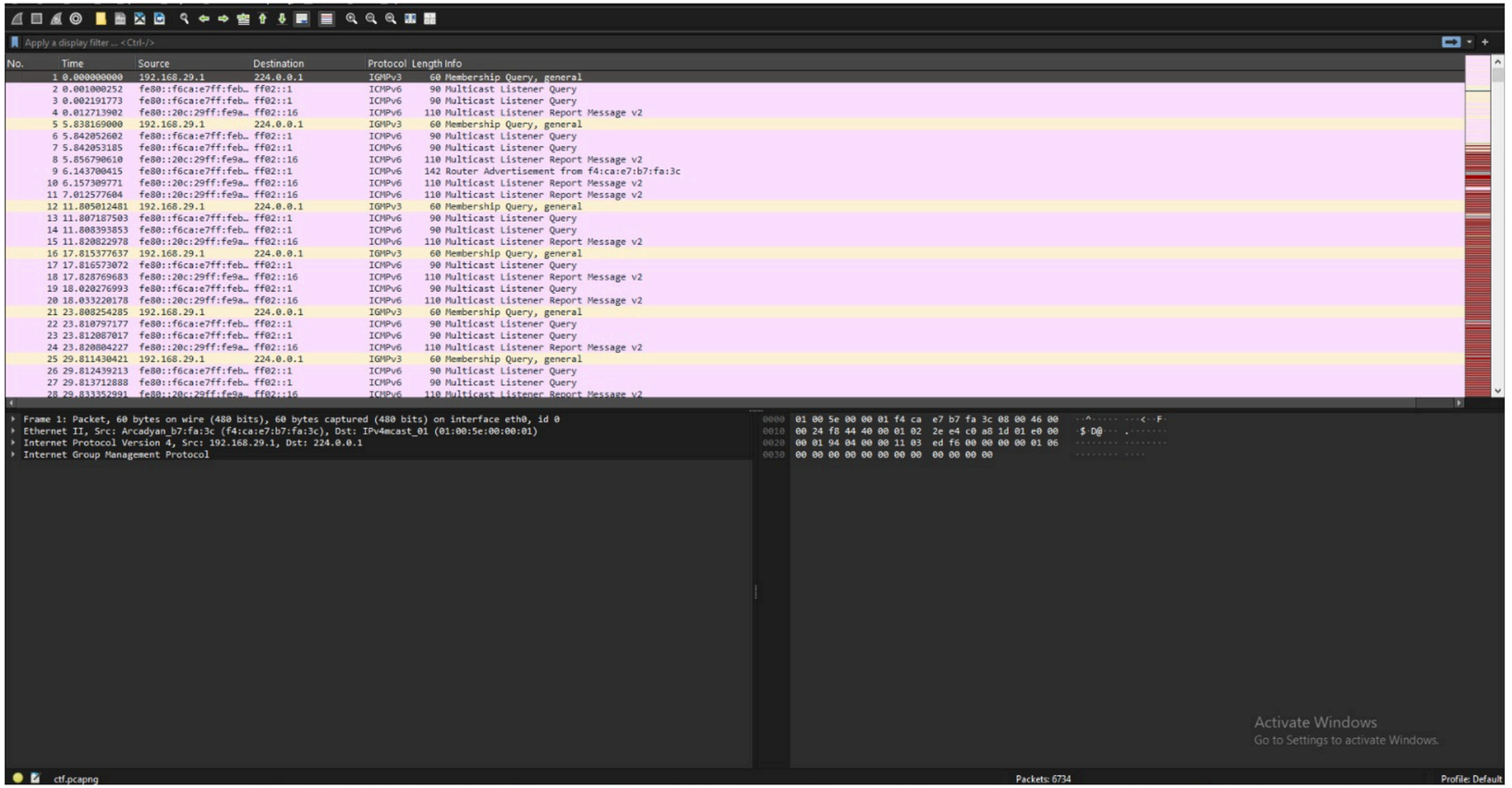
Step 1 : Download PCAP File

- Obtain the PCAP file provided for analysis.



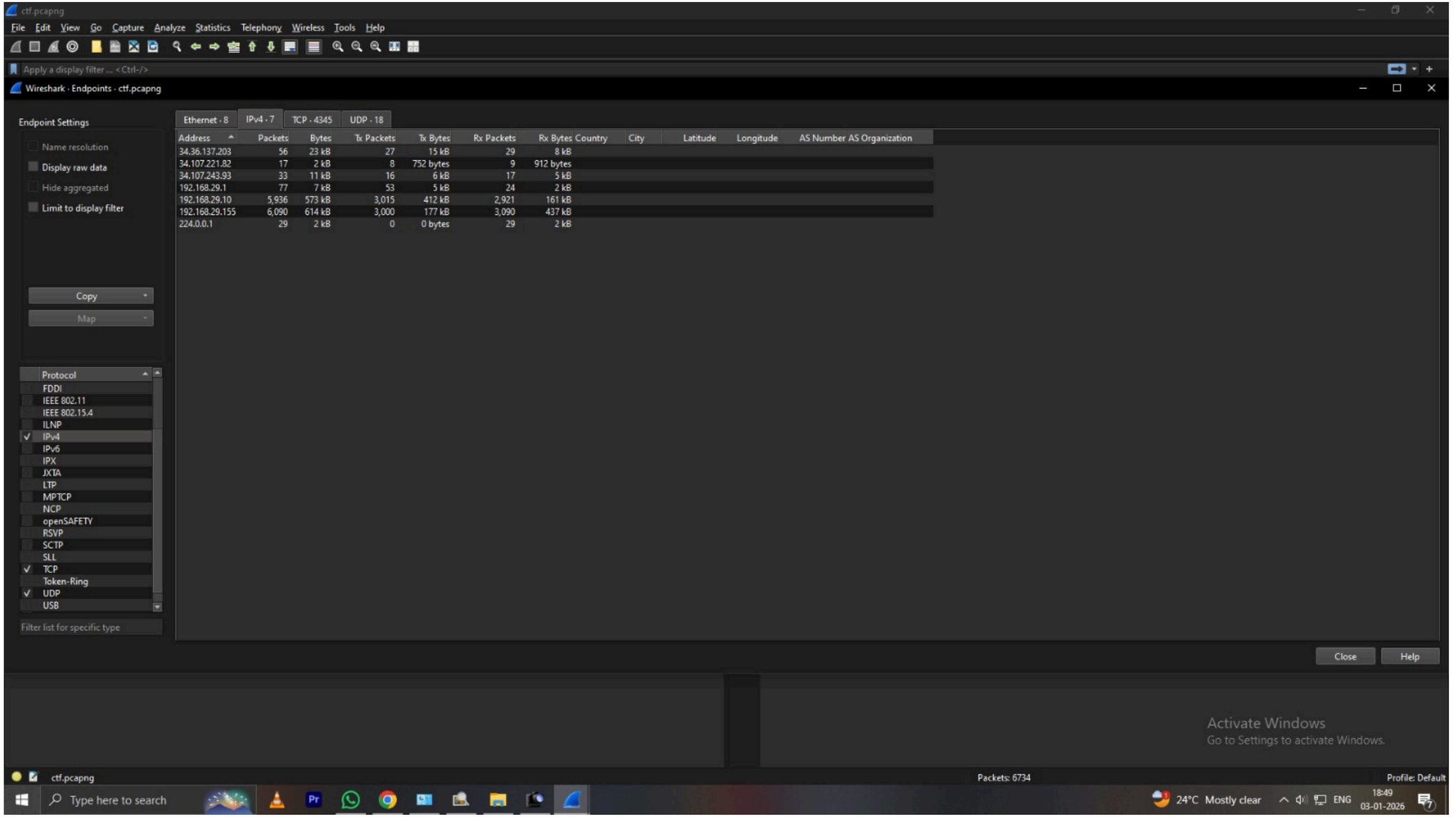
Step 2 : Open PCAP in Wireshark

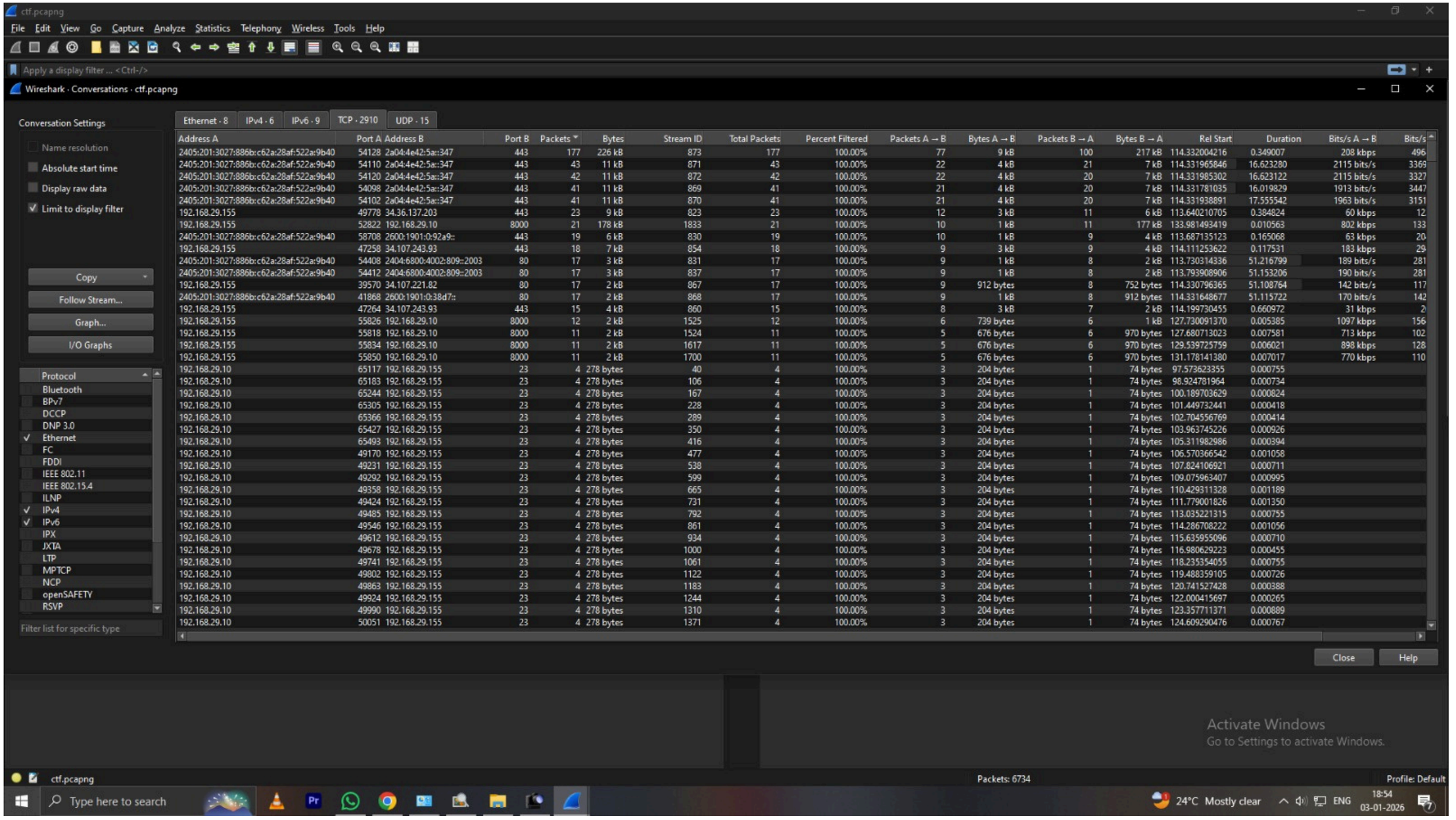
- Launch Wireshark
- Open the downloaded PCAP file

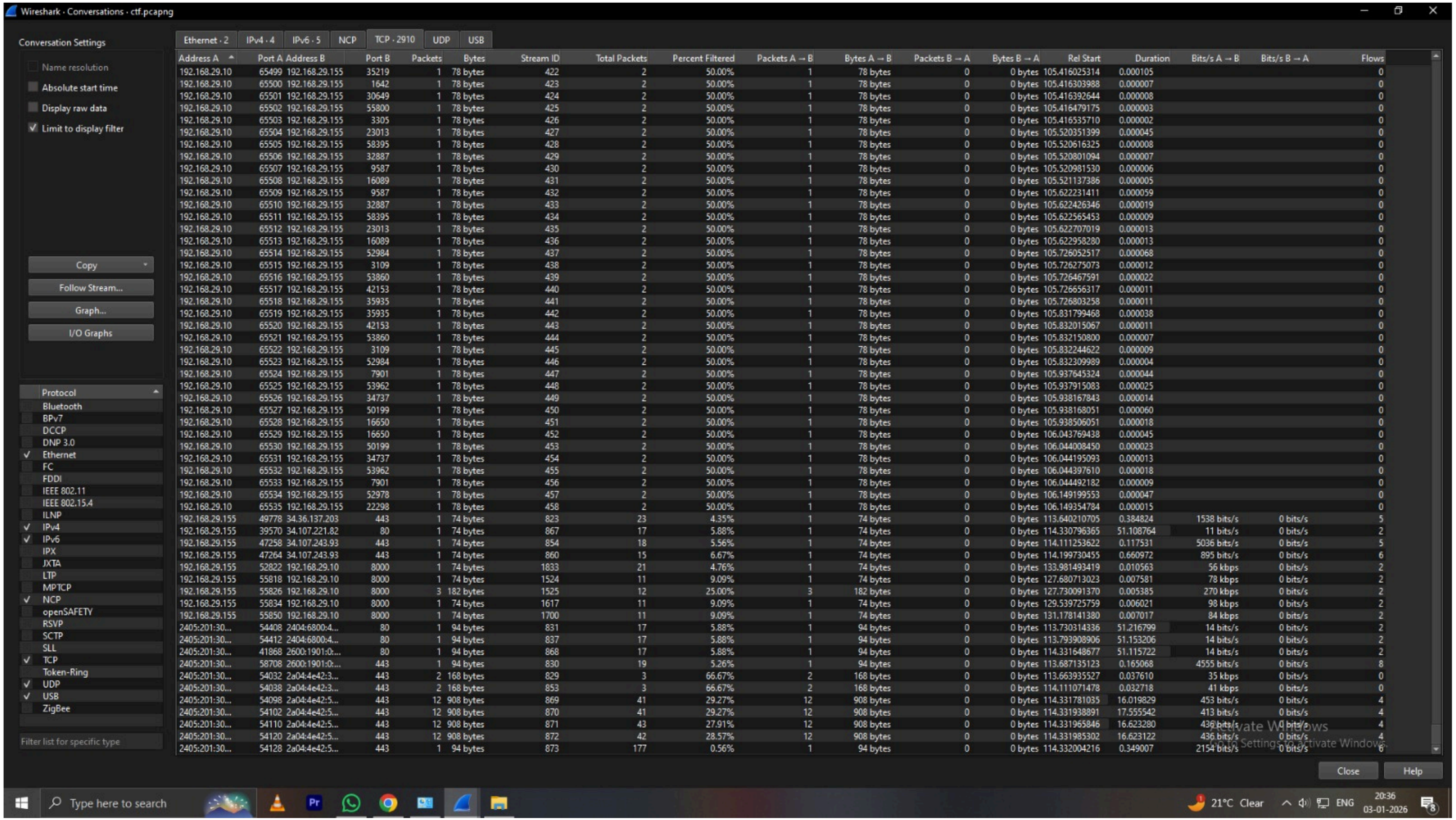


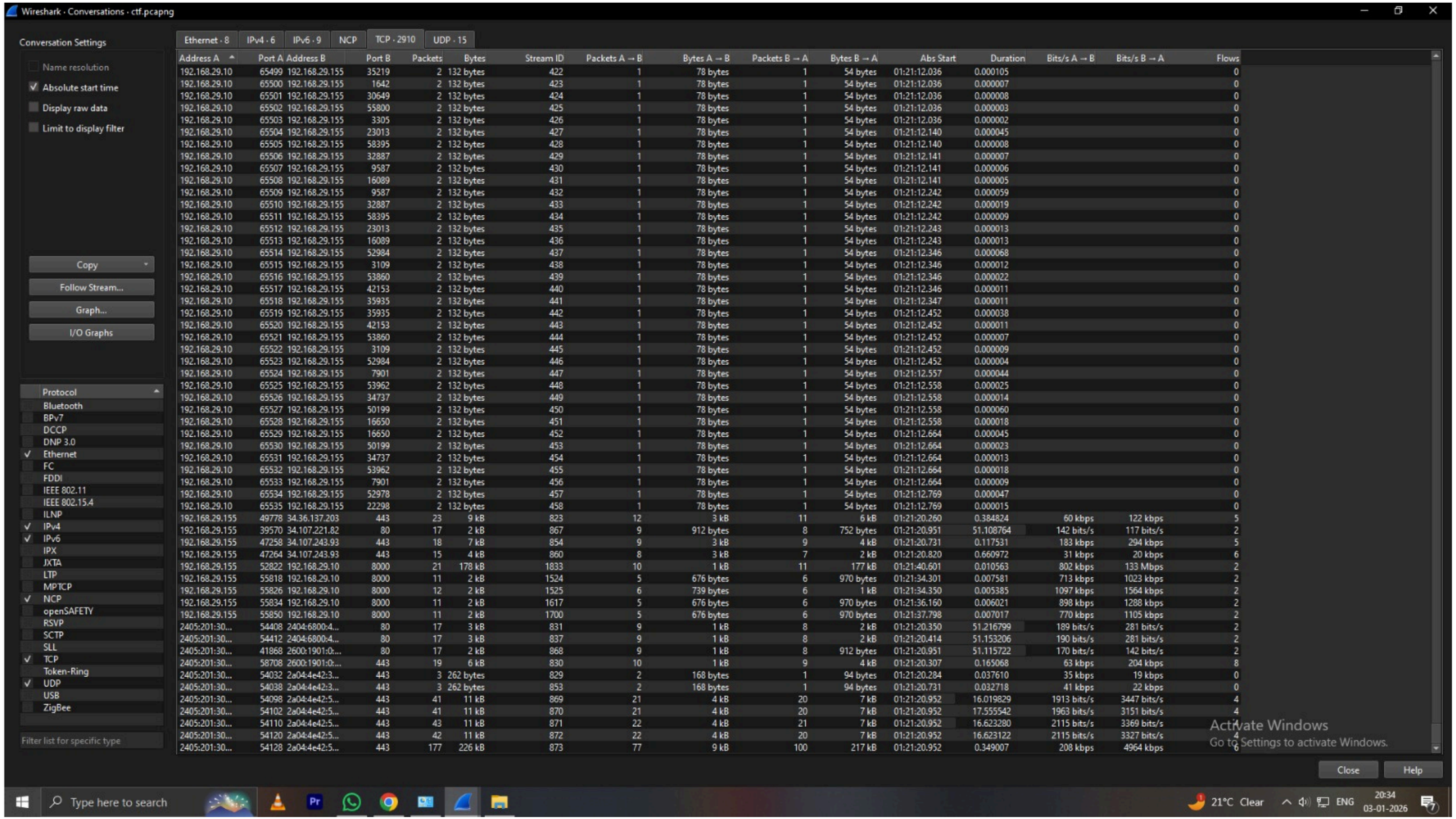
Step 3 : Analyze Traffic Pattern

- Use Statistics Conversations
- Identify high packet flow between source and destination
- Determine attacker and victim IP addresses


ctf.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Endpoints · ctf.pcapng
Endpoint Settings
Name resolution
Display raw data
Hide aggregated
Limit to display filter
Copy
Map
Protocol
FDDI
IEEE 802.11
IEEE 802.15.4
ILNP
IPv4
IPv6
IPX
JXTA
LTP
MPTCP
NCP
openSAFETY
RSVP
SCTP
SLL
TCP
Token-Ring
UDP
USB
Filter list for specific type
Ethernet · 8
IPv4 · 7
TCP · 4345
UDP · 18
Address Packets Bytes Tx Packets Tx Bytes Rx Packets Rx Bytes Country City Latitude Longitude AS Number AS Organization
34.36.137.203 56 23 kB 27 15 kB 29 8 kB
34.107.221.82 17 2 kB 8 752 bytes 9 912 bytes
34.107.243.93 33 11 kB 16 6 kB 17 5 kB
192.168.29.1 77 7 kB 53 5 kB 24 2 kB
192.168.29.10 5,936 573 kB 3,015 412 kB 2,921 161 kB
192.168.29.155 6,090 614 kB 3,000 177 kB 3,090 437 kB
224.0.0.1 29 2 kB 0 0 bytes 29 2 kB
Close
Help
Activate Windows
Go to Settings to activate Windows.
ctf.pcapng
Packets: 6734
Profile: Default
Type here to search
24°C Mostly clear
ENG
18:49
03-01-2026

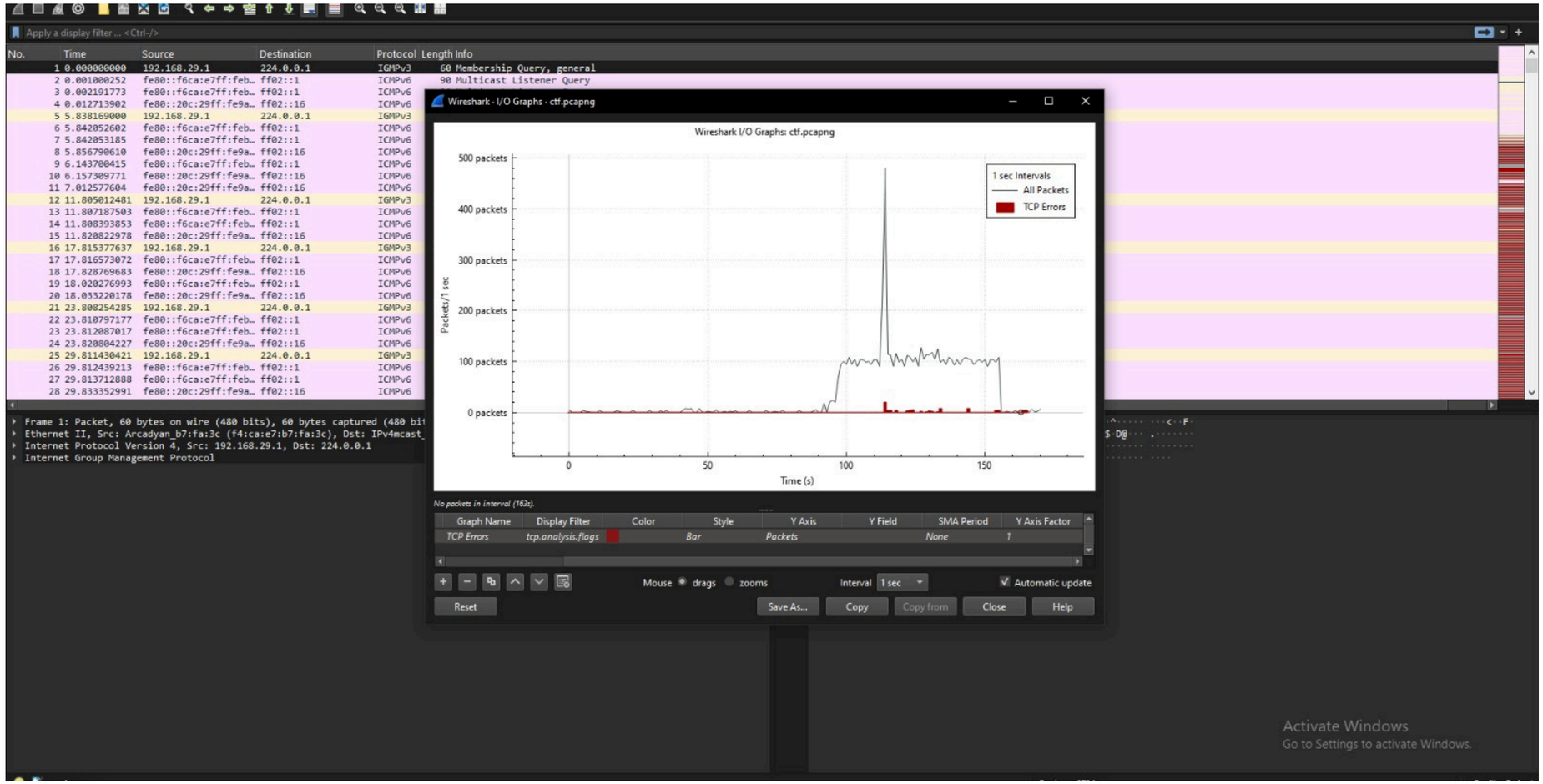

ctf.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Conversations · ctf.pcapng
Conversation Settings
Name resolution
Absolute start time
Display raw data
Limit to display filter
Copy
Follow Stream...
Graph...
I/O Graphs
Protocol
Bluetooth
BPv7
DCCP
DNP 3.0
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
ILNP
IPv4
IPv6
IPX
JXTA
LTP
MPTCP
NCP
openSAFETY
RSVP
Filter list for specific type
Ethernet · 8
IPv4 · 6
IPv6 · 9
TCP · 2910
UDP · 15
Address A Port A Address B Port B Packets Bytes Stream ID Total Packets Percent Filtered Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration Bits/s A → B Bits/s
2405:201:3027:886b:c62a:28af:522a:9b40 54128 2a04:4e42:5a::347 443 177 226 kB 873 177 100.00% 77 9 kB 100 217 kB 114.332004216 0.349007 208 kbps 496
2405:201:3027:886b:c62a:28af:522a:9b40 54110 2a04:4e42:5a::347 443 43 11 kB 871 43 100.00% 22 4 kB 21 7 kB 114.331965846 16.623280 2115 bits/s 3369
2405:201:3027:886b:c62a:28af:522a:9b40 54120 2a04:4e42:5a::347 443 42 11 kB 872 42 100.00% 22 4 kB 20 7 kB 114.331985302 16.623122 2115 bits/s 3327
2405:201:3027:886b:c62a:28af:522a:9b40 54098 2a04:4e42:5a::347 443 41 11 kB 869 41 100.00% 21 4 kB 20 7 kB 114.331781035 16.019829 1913 bits/s 3447
2405:201:3027:886b:c62a:28af:522a:9b40 54102 2a04:4e42:5a::347 443 41 11 kB 870 41 100.00% 21 4 kB 20 7 kB 114.331938891 17.555542 1963 bits/s 3151
192.168.29.155 49778 34.36.137.203 443 23 9 kB 823 23 100.00% 12 3 kB 11 6 kB 113.640210705 0.384824 60 kbps 12
192.168.29.155 52822 192.168.29.10 8000 21 178 kB 1833 21 100.00% 10 1 kB 11 177 kB 133.981493419 0.010563 802 kbps 133
2405:201:3027:886b:c62a:28af:522a:9b40 58708 2600:1901:0:92a9:: 443 19 6 kB 830 19 100.00% 10 1 kB 9 4 kB 113.687135123 0.165068 63 kbps 20
192.168.29.155 47258 34.107.243.93 443 18 7 kB 854 18 100.00% 9 3 kB 9 4 kB 114.111253622 0.117531 183 kbps 29
2405:201:3027:886b:c62a:28af:522a:9b40 54408 2404:6800:4002:809::2003 80 17 3 kB 831 17 100.00% 9 1 kB 8 2 kB 113.730314336 51.216799 189 bits/s 281
2405:201:3027:886b:c62a:28af:522a:9b40 54412 2404:6800:4002:809::2003 80 17 3 kB 837 17 100.00% 9 1 kB 8 2 kB 113.793908906 51.153206 190 bits/s 281
192.168.29.155 39570 34.107.221.82 80 17 2 kB 867 17 100.00% 9 912 bytes 8 752 bytes 114.330796365 51.108764 142 bits/s 117
2405:201:3027:886b:c62a:28af:522a:9b40 41868 2600:1901:0:38d7:: 80 17 2 kB 868 17 100.00% 9 1 kB 8 912 bytes 114.331648677 51.115722 170 bits/s 142
192.168.29.155 47264 34.107.243.93 443 15 4 kB 860 15 100.00% 8 3 kB 7 2 kB 114.199730455 0.660972 31 kbps 2
192.168.29.155 55826 192.168.29.10 8000 12 2 kB 1525 12 100.00% 6 739 bytes 6 1 kB 127.730091370 0.005385 1097 kbps 156
192.168.29.155 55818 192.168.29.10 8000 11 2 kB 1524 11 100.00% 5 676 bytes 6 970 bytes 127.680713023 0.007581 713 kbps 102
192.168.29.155 55834 192.168.29.10 8000 11 2 kB 1617 11 100.00% 5 676 bytes 6 970 bytes 129.539725759 0.006021 898 kbps 128
192.168.29.155 55850 192.168.29.10 8000 11 2 kB 1700 11 100.00% 5 676 bytes 6 970 bytes 131.178141380 0.007017 770 kbps 110
192.168.29.10 65117 192.168.29.155 23 4 278 bytes 40 4 100.00% 3 204 bytes 1 74 bytes 97.573623355 0.000755
192.168.29.10 65183 192.168.29.155 23 4 278 bytes 106 4 100.00% 3 204 bytes 1 74 bytes 98.924781964 0.000734
192.168.29.10 65244 192.168.29.155 23 4 278 bytes 167 4 100.00% 3 204 bytes 1 74 bytes 100.189703629 0.000824
192.168.29.10 65305 192.168.29.155 23 4 278 bytes 228 4 100.00% 3 204 bytes 1 74 bytes 101.449732441 0.000418
192.168.29.10 65366 192.168.29.155 23 4 278 bytes 289 4 100.00% 3 204 bytes 1 74 bytes 102.704556769 0.000414
192.168.29.10 65427 192.168.29.155 23 4 278 bytes 350 4 100.00% 3 204 bytes 1 74 bytes 103.963745226 0.000926
192.168.29.10 65493 192.168.29.155 23 4 278 bytes 416 4 100.00% 3 204 bytes 1 74 bytes 105.311982986 0.000394
192.168.29.10 49170 192.168.29.155 23 4 278 bytes 477 4 100.00% 3 204 bytes 1 74 bytes 106.570366542 0.001058
192.168.29.10 49231 192.168.29.155 23 4 278 bytes 538 4 100.00% 3 204 bytes 1 74 bytes 107.824106921 0.000711
192.168.29.10 49292 192.168.29.155 23 4 278 bytes 599 4 100.00% 3 204 bytes 1 74 bytes 109.075963407 0.000995
192.168.29.10 49358 192.168.29.155 23 4 278 bytes 665 4 100.00% 3 204 bytes 1 74 bytes 110.429311328 0.001189
192.168.29.10 49424 192.168.29.155 23 4 278 bytes 731 4 100.00% 3 204 bytes 1 74 bytes 111.779001826 0.001350
192.168.29.10 49485 192.168.29.155 23 4 278 bytes 792 4 100.00% 3 204 bytes 1 74 bytes 113.035221315 0.000755
192.168.29.10 49546 192.168.29.155 23 4 278 bytes 861 4 100.00% 3 204 bytes 1 74 bytes 114.286708222 0.001056
192.168.29.10 49612 192.168.29.155 23 4 278 bytes 934 4 100.00% 3 204 bytes 1 74 bytes 115.635955096 0.000710
192.168.29.10 49678 192.168.29.155 23 4 278 bytes 1000 4 100.00% 3 204 bytes 1 74 bytes 116.980629223 0.000455
192.168.29.10 49741 192.168.29.155 23 4 278 bytes 1061 4 100.00% 3 204 bytes 1 74 bytes 118.235354055 0.000755
192.168.29.10 49802 192.168.29.155 23 4 278 bytes 1122 4 100.00% 3 204 bytes 1 74 bytes 119.488359105 0.000726
192.168.29.10 49863 192.168.29.155 23 4 278 bytes 1183 4 100.00% 3 204 bytes 1 74 bytes 120.741527428 0.000388
192.168.29.10 49924 192.168.29.155 23 4 278 bytes 1244 4 100.00% 3 204 bytes 1 74 bytes 122.000415697 0.000265
192.168.29.10 49990 192.168.29.155 23 4 278 bytes 1310 4 100.00% 3 204 bytes 1 74 bytes 123.357711371 0.000889
192.168.29.10 50051 192.168.29.155 23 4 278 bytes 1371 4 100.00% 3 204 bytes 1 74 bytes 124.609290476 0.000767
Close
Help
Activate Windows
Go to Settings to activate Windows.
ctf.pcapng
Packets: 6734
Profile: Default
Type here to search
24°C Mostly clear
ENG
18:54
03-01-2026


Wireshark · Conversations · ctf.pcapng
Conversation Settings
Name resolution
Absolute start time
Display raw data
Limit to display filter
Copy
Follow Stream...
Graph...
I/O Graphs
Protocol
Bluetooth
BPv7
DCCP
DNP 3.0
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
ILNP
IPv4
IPv6
IPX
JXTA
LTP
MPTCP
NCP
openSAFETY
RSVP
SCTP
SLL
TCP
Token-Ring
UDP
USB
ZigBee
Filter list for specific type
Ethernet · 2
IPv4 · 4
IPv6 · 5
NCP
TCP · 2910
UDP
USB
Address A Port A Address B Port B Packets Bytes Stream ID Total Packets Percent Filtered Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration Bits/s A → B Bits/s B → A Flows
192.168.29.10 65499 192.168.29.155 35219 1 78 bytes 422 2 50.00% 1 78 bytes 0 0 bytes 105.416025314 0.000105 0
192.168.29.10 65500 192.168.29.155 1642 1 78 bytes 423 2 50.00% 1 78 bytes 0 0 bytes 105.416303988 0.000007 0
192.168.29.10 65501 192.168.29.155 30649 1 78 bytes 424 2 50.00% 1 78 bytes 0 0 bytes 105.416392644 0.000008 0
192.168.29.10 65502 192.168.29.155 55800 1 78 bytes 425 2 50.00% 1 78 bytes 0 0 bytes 105.416479175 0.000003 0
192.168.29.10 65503 192.168.29.155 3305 1 78 bytes 426 2 50.00% 1 78 bytes 0 0 bytes 105.416535710 0.000002 0
192.168.29.10 65504 192.168.29.155 23013 1 78 bytes 427 2 50.00% 1 78 bytes 0 0 bytes 105.520351399 0.000045 0
192.168.29.10 65505 192.168.29.155 58395 1 78 bytes 428 2 50.00% 1 78 bytes 0 0 bytes 105.520616325 0.000008 0
192.168.29.10 65506 192.168.29.155 32887 1 78 bytes 429 2 50.00% 1 78 bytes 0 0 bytes 105.520801094 0.000007 0
192.168.29.10 65507 192.168.29.155 9587 1 78 bytes 430 2 50.00% 1 78 bytes 0 0 bytes 105.520981530 0.000006 0
192.168.29.10 65508 192.168.29.155 16089 1 78 bytes 431 2 50.00% 1 78 bytes 0 0 bytes 105.521137386 0.000005 0
192.168.29.10 65509 192.168.29.155 9587 1 78 bytes 432 2 50.00% 1 78 bytes 0 0 bytes 105.622231411 0.000059 0
192.168.29.10 65510 192.168.29.155 32887 1 78 bytes 433 2 50.00% 1 78 bytes 0 0 bytes 105.622426346 0.000019 0
192.168.29.10 65511 192.168.29.155 58395 1 78 bytes 434 2 50.00% 1 78 bytes 0 0 bytes 105.622565453 0.000009 0
192.168.29.10 65512 192.168.29.155 23013 1 78 bytes 435 2 50.00% 1 78 bytes 0 0 bytes 105.622707019 0.000013 0
192.168.29.10 65513 192.168.29.155 16089 1 78 bytes 436 2 50.00% 1 78 bytes 0 0 bytes 105.622958280 0.000013 0
192.168.29.10 65514 192.168.29.155 52984 1 78 bytes 437 2 50.00% 1 78 bytes 0 0 bytes 105.726052517 0.000068 0
192.168.29.10 65515 192.168.29.155 3109 1 78 bytes 438 2 50.00% 1 78 bytes 0 0 bytes 105.726275073 0.000012 0
192.168.29.10 65516 192.168.29.155 53860 1 78 bytes 439 2 50.00% 1 78 bytes 0 0 bytes 105.726467591 0.000022 0
192.168.29.10 65517 192.168.29.155 42153 1 78 bytes 440 2 50.00% 1 78 bytes 0 0 bytes 105.726656317 0.000011 0
192.168.29.10 65518 192.168.29.155 35935 1 78 bytes 441 2 50.00% 1 78 bytes 0 0 bytes 105.726803258 0.000011 0
192.168.29.10 65519 192.168.29.155 35935 1 78 bytes 442 2 50.00% 1 78 bytes 0 0 bytes 105.831799468 0.000038 0
192.168.29.10 65520 192.168.29.155 42153 1 78 bytes 443 2 50.00% 1 78 bytes 0 0 bytes 105.832015067 0.000011 0
192.168.29.10 65521 192.168.29.155 53860 1 78 bytes 444 2 50.00% 1 78 bytes 0 0 bytes 105.832150800 0.000007 0
192.168.29.10 65522 192.168.29.155 3109 1 78 bytes 445 2 50.00% 1 78 bytes 0 0 bytes 105.832244622 0.000009 0
192.168.29.10 65523 192.168.29.155 52984 1 78 bytes 446 2 50.00% 1 78 bytes 0 0 bytes 105.832309989 0.000004 0
192.168.29.10 65524 192.168.29.155 7901 1 78 bytes 447 2 50.00% 1 78 bytes 0 0 bytes 105.937645324 0.000044 0
192.168.29.10 65525 192.168.29.155 53962 1 78 bytes 448 2 50.00% 1 78 bytes 0 0 bytes 105.937915083 0.000025 0
192.168.29.10 65526 192.168.29.155 34737 1 78 bytes 449 2 50.00% 1 78 bytes 0 0 bytes 105.938167843 0.000014 0
192.168.29.10 65527 192.168.29.155 50199 1 78 bytes 450 2 50.00% 1 78 bytes 0 0 bytes 105.938168051 0.000060 0
192.168.29.10 65528 192.168.29.155 16650 1 78 bytes 451 2 50.00% 1 78 bytes 0 0 bytes 105.938506051 0.000018 0
192.168.29.10 65529 192.168.29.155 16650 1 78 bytes 452 2 50.00% 1 78 bytes 0 0 bytes 106.043769438 0.000045 0
192.168.29.10 65530 192.168.29.155 50199 1 78 bytes 453 2 50.00% 1 78 bytes 0 0 bytes 106.044008450 0.000023 0
192.168.29.10 65531 192.168.29.155 34737 1 78 bytes 454 2 50.00% 1 78 bytes 0 0 bytes 106.044195093 0.000013 0
192.168.29.10 65532 192.168.29.155 53962 1 78 bytes 455 2 50.00% 1 78 bytes 0 0 bytes 106.044397610 0.000018 0
192.168.29.10 65533 192.168.29.155 7901 1 78 bytes 456 2 50.00% 1 78 bytes 0 0 bytes 106.044492182 0.000009 0
192.168.29.10 65534 192.168.29.155 52978 1 78 bytes 457 2 50.00% 1 78 bytes 0 0 bytes 106.149199553 0.000047 0
192.168.29.10 65535 192.168.29.155 22298 1 78 bytes 458 2 50.00% 1 78 bytes 0 0 bytes 106.149354784 0.000015 0
192.168.29.155 49778 34.36.137.203 443 1 74 bytes 823 23 4.35% 1 74 bytes 0 0 bytes 113.640210705 0.384824 1538 bits/s 0 bits/s 5
192.168.29.155 39570 34.107.221.82 80 1 74 bytes 867 17 5.88% 1 74 bytes 0 0 bytes 114.330796365 51.108764 11 bits/s 0 bits/s 2
192.168.29.155 47258 34.107.243.93 443 1 74 bytes 854 18 5.56% 1 74 bytes 0 0 bytes 114.111253622 0.117531 5036 bits/s 0 bits/s 5
192.168.29.155 47264 34.107.243.93 443 1 74 bytes 860 15 6.67% 1 74 bytes 0 0 bytes 114.199730455 0.660972 895 bits/s 0 bits/s 6
192.168.29.155 52822 192.168.29.10 8000 1 74 bytes 1833 21 4.76% 1 74 bytes 0 0 bytes 133.981493419 0.010563 56 kbps 0 bits/s 2
192.168.29.155 55818 192.168.29.10 8000 1 74 bytes 1524 11 9.09% 1 74 bytes 0 0 bytes 127.680713023 0.007581 78 kbps 0 bits/s 2
192.168.29.155 55826 192.168.29.10 8000 3 182 bytes 1525 12 25.00% 3 182 bytes 0 0 bytes 127.730091370 0.005385 270 kbps 0 bits/s 2
192.168.29.155 55834 192.168.29.10 8000 1 74 bytes 1617 11 9.09% 1 74 bytes 0 0 bytes 129.539725759 0.006021 98 kbps 0 bits/s 2
192.168.29.155 55850 192.168.29.10 8000 1 74 bytes 1700 11 9.09% 1 74 bytes 0 0 bytes 131.178141380 0.007017 84 kbps 0 bits/s 2
2405:201:30... 54408 2404:6800:4... 80 1 94 bytes 831 17 5.88% 1 94 bytes 0 0 bytes 113.730314336 51.216799 14 bits/s 0 bits/s 2
2405:201:30... 54412 2404:6800:4... 80 1 94 bytes 837 17 5.88% 1 94 bytes 0 0 bytes 113.793908906 51.153206 14 bits/s 0 bits/s 2
2405:201:30... 41868 2600:1901:0:... 80 1 94 bytes 868 17 5.88% 1 94 bytes 0 0 bytes 114.331648677 51.115722 14 bits/s 0 bits/s 2
2405:201:30... 58708 2600:1901:0:... 443 1 94 bytes 830 19 5.26% 1 94 bytes 0 0 bytes 113.687135123 0.165068 4555 bits/s 0 bits/s 8
2405:201:30... 54032 2a04:4e42:3... 443 2 168 bytes 829 3 66.67% 2 168 bytes 0 0 bytes 113.663935527 0.037610 35 kbps 0 bits/s 0
2405:201:30... 54038 2a04:4e42:3... 443 2 168 bytes 853 3 66.67% 2 168 bytes 0 0 bytes 114.111071478 0.032718 41 kbps 0 bits/s 0
2405:201:30... 54098 2a04:4e42:5... 443 12 908 bytes 869 41 29.27% 12 908 bytes 0 0 bytes 114.331781035 16.019829 453 bits/s 0 bits/s 4
2405:201:30... 54102 2a04:4e42:5... 443 12 908 bytes 870 41 29.27% 12 908 bytes 0 0 bytes 114.331938891 17.555542 413 bits/s 0 bits/s 4
2405:201:30... 54110 2a04:4e42:5... 443 12 908 bytes 871 43 27.91% 12 908 bytes 0 0 bytes 114.331965846 16.623280 436 bits/s 0 bits/s 4
2405:201:30... 54120 2a04:4e42:5... 443 12 908 bytes 872 42 28.57% 12 908 bytes 0 0 bytes 114.331985302 16.623122 436 bits/s 0 bits/s 4
2405:201:30... 54128 2a04:4e42:5... 443 1 94 bytes 873 177 0.56% 1 94 bytes 0 0 bytes 114.332004216 0.349007 2154 bits/s 0 bits/s 6
Close
Help
Type here to search
21°C Clear
ENG
20:36
03-01-2026


Wireshark · Conversations · ctf.pcapng
Conversation Settings
Name resolution
Absolute start time
Display raw data
Limit to display filter
Copy
Follow Stream...
Graph...
I/O Graphs
Protocol
Bluetooth
BPv7
DCCP
DNP 3.0
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
ILNP
IPv4
IPv6
IPX
JXTA
LTP
MPTCP
NCP
openSAFETY
RSVP
SCTP
SLL
TCP
Token-Ring
UDP
USB
ZigBee
Filter list for specific type
Ethernet · 8
IPv4 · 6
IPv6 · 9
NCP
TCP · 2910
UDP · 15
Address A Port A Address B Port B Packets Bytes Stream ID Packets A → B Bytes A → B Packets B → A Bytes B → A Abs Start Duration Bits/s A → B Bits/s B → A Flows
192.168.29.10 65499 192.168.29.155 35219 2 132 bytes 422 1 78 bytes 1 54 bytes 01:21:12.036 0.000105 0
192.168.29.10 65500 192.168.29.155 1642 2 132 bytes 423 1 78 bytes 1 54 bytes 01:21:12.036 0.000007 0
192.168.29.10 65501 192.168.29.155 30649 2 132 bytes 424 1 78 bytes 1 54 bytes 01:21:12.036 0.000008 0
192.168.29.10 65502 192.168.29.155 55800 2 132 bytes 425 1 78 bytes 1 54 bytes 01:21:12.036 0.000003 0
192.168.29.10 65503 192.168.29.155 3305 2 132 bytes 426 1 78 bytes 1 54 bytes 01:21:12.036 0.000002 0
192.168.29.10 65504 192.168.29.155 23013 2 132 bytes 427 1 78 bytes 1 54 bytes 01:21:12.140 0.000045 0
192.168.29.10 65505 192.168.29.155 58395 2 132 bytes 428 1 78 bytes 1 54 bytes 01:21:12.140 0.000008 0
192.168.29.10 65506 192.168.29.155 32887 2 132 bytes 429 1 78 bytes 1 54 bytes 01:21:12.141 0.000007 0
192.168.29.10 65507 192.168.29.155 9587 2 132 bytes 430 1 78 bytes 1 54 bytes 01:21:12.141 0.000006 0
192.168.29.10 65508 192.168.29.155 16089 2 132 bytes 431 1 78 bytes 1 54 bytes 01:21:12.141 0.000005 0
192.168.29.10 65509 192.168.29.155 9587 2 132 bytes 432 1 78 bytes 1 54 bytes 01:21:12.242 0.000059 0
192.168.29.10 65510 192.168.29.155 32887 2 132 bytes 433 1 78 bytes 1 54 bytes 01:21:12.242 0.000019 0
192.168.29.10 65511 192.168.29.155 58395 2 132 bytes 434 1 78 bytes 1 54 bytes 01:21:12.242 0.000009 0
192.168.29.10 65512 192.168.29.155 23013 2 132 bytes 435 1 78 bytes 1 54 bytes 01:21:12.243 0.000013 0
192.168.29.10 65513 192.168.29.155 16089 2 132 bytes 436 1 78 bytes 1 54 bytes 01:21:12.243 0.000013 0
192.168.29.10 65514 192.168.29.155 52984 2 132 bytes 437 1 78 bytes 1 54 bytes 01:21:12.346 0.000068 0
192.168.29.10 65515 192.168.29.155 3109 2 132 bytes 438 1 78 bytes 1 54 bytes 01:21:12.346 0.000012 0
192.168.29.10 65516 192.168.29.155 53860 2 132 bytes 439 1 78 bytes 1 54 bytes 01:21:12.346 0.000022 0
192.168.29.10 65517 192.168.29.155 42153 2 132 bytes 440 1 78 bytes 1 54 bytes 01:21:12.346 0.000011 0
192.168.29.10 65518 192.168.29.155 35935 2 132 bytes 441 1 78 bytes 1 54 bytes 01:21:12.347 0.000011 0
192.168.29.10 65519 192.168.29.155 35935 2 132 bytes 442 1 78 bytes 1 54 bytes 01:21:12.452 0.000038 0
192.168.29.10 65520 192.168.29.155 42153 2 132 bytes 443 1 78 bytes 1 54 bytes 01:21:12.452 0.000011 0
192.168.29.10 65521 192.168.29.155 53860 2 132 bytes 444 1 78 bytes 1 54 bytes 01:21:12.452 0.000007 0
192.168.29.10 65522 192.168.29.155 3109 2 132 bytes 445 1 78 bytes 1 54 bytes 01:21:12.452 0.000009 0
192.168.29.10 65523 192.168.29.155 52984 2 132 bytes 446 1 78 bytes 1 54 bytes 01:21:12.452 0.000004 0
192.168.29.10 65524 192.168.29.155 7901 2 132 bytes 447 1 78 bytes 1 54 bytes 01:21:12.557 0.000044 0
192.168.29.10 65525 192.168.29.155 53962 2 132 bytes 448 1 78 bytes 1 54 bytes 01:21:12.558 0.000025 0
192.168.29.10 65526 192.168.29.155 34737 2 132 bytes 449 1 78 bytes 1 54 bytes 01:21:12.558 0.000014 0
192.168.29.10 65527 192.168.29.155 50199 2 132 bytes 450 1 78 bytes 1 54 bytes 01:21:12.558 0.000060 0
192.168.29.10 65528 192.168.29.155 16650 2 132 bytes 451 1 78 bytes 1 54 bytes 01:21:12.558 0.000018 0
192.168.29.10 65529 192.168.29.155 16650 2 132 bytes 452 1 78 bytes 1 54 bytes 01:21:12.664 0.000045 0
192.168.29.10 65530 192.168.29.155 50199 2 132 bytes 453 1 78 bytes 1 54 bytes 01:21:12.664 0.000023 0
192.168.29.10 65531 192.168.29.155 34737 2 132 bytes 454 1 78 bytes 1 54 bytes 01:21:12.664 0.000013 0
192.168.29.10 65532 192.168.29.155 53962 2 132 bytes 455 1 78 bytes 1 54 bytes 01:21:12.664 0.000018 0
192.168.29.10 65533 192.168.29.155 7901 2 132 bytes 456 1 78 bytes 1 54 bytes 01:21:12.664 0.000009 0
192.168.29.10 65534 192.168.29.155 52978 2 132 bytes 457 1 78 bytes 1 54 bytes 01:21:12.769 0.000047 0
192.168.29.10 65535 192.168.29.155 22298 2 132 bytes 458 1 78 bytes 1 54 bytes 01:21:12.769 0.000015 0
192.168.29.155 49778 34.36.137.203 443 23 9 kB 823 12 3 kB 11 6 kB 01:21:20.260 0.384824 60 kbps 122 kbps 5
192.168.29.155 39570 34.107.221.82 80 17 2 kB 867 9 912 bytes 8 752 bytes 01:21:20.951 51.108764 142 bits/s 117 bits/s 2
192.168.29.155 47258 34.107.243.93 443 18 7 kB 854 9 3 kB 9 4 kB 01:21:20.731 0.117531 183 kbps 294 kbps 5
192.168.29.155 47264 34.107.243.93 443 15 4 kB 860 8 3 kB 7 2 kB 01:21:20.820 0.660972 31 kbps 20 kbps 6
192.168.29.155 52822 192.168.29.10 8000 21 178 kB 1833 10 1 kB 11 177 kB 01:21:40.601 0.010563 802 kbps 133 Mbps 2
192.168.29.155 55818 192.168.29.10 8000 11 2 kB 1524 5 676 bytes 6 970 bytes 01:21:34.301 0.007581 713 kbps 1023 kbps 2
192.168.29.155 55826 192.168.29.10 8000 12 2 kB 1525 6 739 bytes 6 1 kB 01:21:34.350 0.005385 1097 kbps 1564 kbps 2
192.168.29.155 55834 192.168.29.10 8000 11 2 kB 1617 5 676 bytes 6 970 bytes 01:21:36.160 0.006021 898 kbps 1288 kbps 2
192.168.29.155 55850 192.168.29.10 8000 11 2 kB 1700 5 676 bytes 6 970 bytes 01:21:37.798 0.007017 770 kbps 1105 kbps 2
2405:201:30... 54408 2404:6800:4... 80 17 3 kB 831 9 1 kB 8 2 kB 01:21:20.350 51.216799 189 bits/s 281 bits/s 2
2405:201:30... 54412 2404:6800:4... 80 17 3 kB 837 9 1 kB 8 2 kB 01:21:20.414 51.153206 190 bits/s 281 bits/s 2
2405:201:30... 41868 2600:1901:0:... 80 17 2 kB 868 9 1 kB 8 912 bytes 01:21:20.951 51.115722 170 bits/s 142 bits/s 2
2405:201:30... 58708 2600:1901:0:... 443 19 6 kB 830 10 1 kB 9 4 kB 01:21:20.307 0.165068 63 kbps 204 kbps 8
2405:201:30... 54032 2a04:4e42:3... 443 3 262 bytes 829 2 168 bytes 1 94 bytes 01:21:20.284 0.037610 35 kbps 19 kbps 0
2405:201:30... 54038 2a04:4e42:3... 443 3 262 bytes 853 2 168 bytes 1 94 bytes 01:21:20.731 0.032718 41 kbps 22 kbps 0
2405:201:30... 54098 2a04:4e42:5... 443 41 11 kB 869 21 4 kB 20 7 kB 01:21:20.952 16.019829 1913 bits/s 3447 bits/s 4
2405:201:30... 54102 2a04:4e42:5... 443 41 11 kB 870 21 4 kB 20 7 kB 01:21:20.952 17.555542 1963 bits/s 3151 bits/s 4
2405:201:30... 54110 2a04:4e42:5... 443 43 11 kB 871 22 4 kB 21 7 kB 01:21:20.952 16.623280 2115 bits/s 3369 bits/s 4
2405:201:30... 54120 2a04:4e42:5... 443 42 11 kB 872 22 4 kB 20 7 kB 01:21:20.952 16.623122 2115 bits/s 3327 bits/s 4
2405:201:30... 54128 2a04:4e42:5... 443 177 226 kB 873 77 9 kB 100 217 kB 01:21:20.952 0.349007 208 kbps 4964 kbps 6
Activate Windows
Go to Settings to activate Windows.
Close
Help
Type here to search
21°C Clear
ENG
20:34
03-01-2026

Step 4 : Identify Attack Start Time

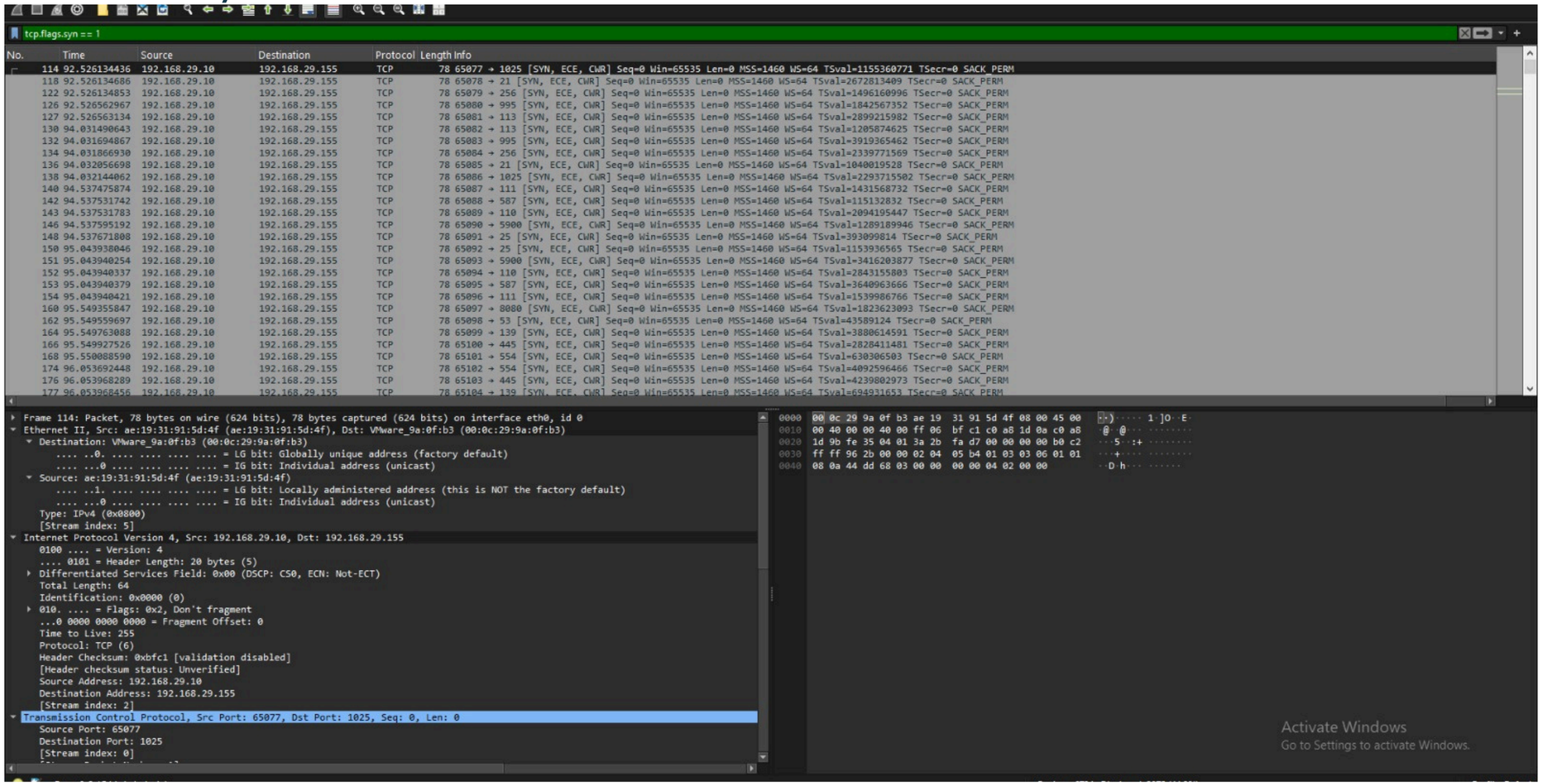
- Use Statistics → I/O Graph
- Analyze timestamps to find sudden spikes in traffic

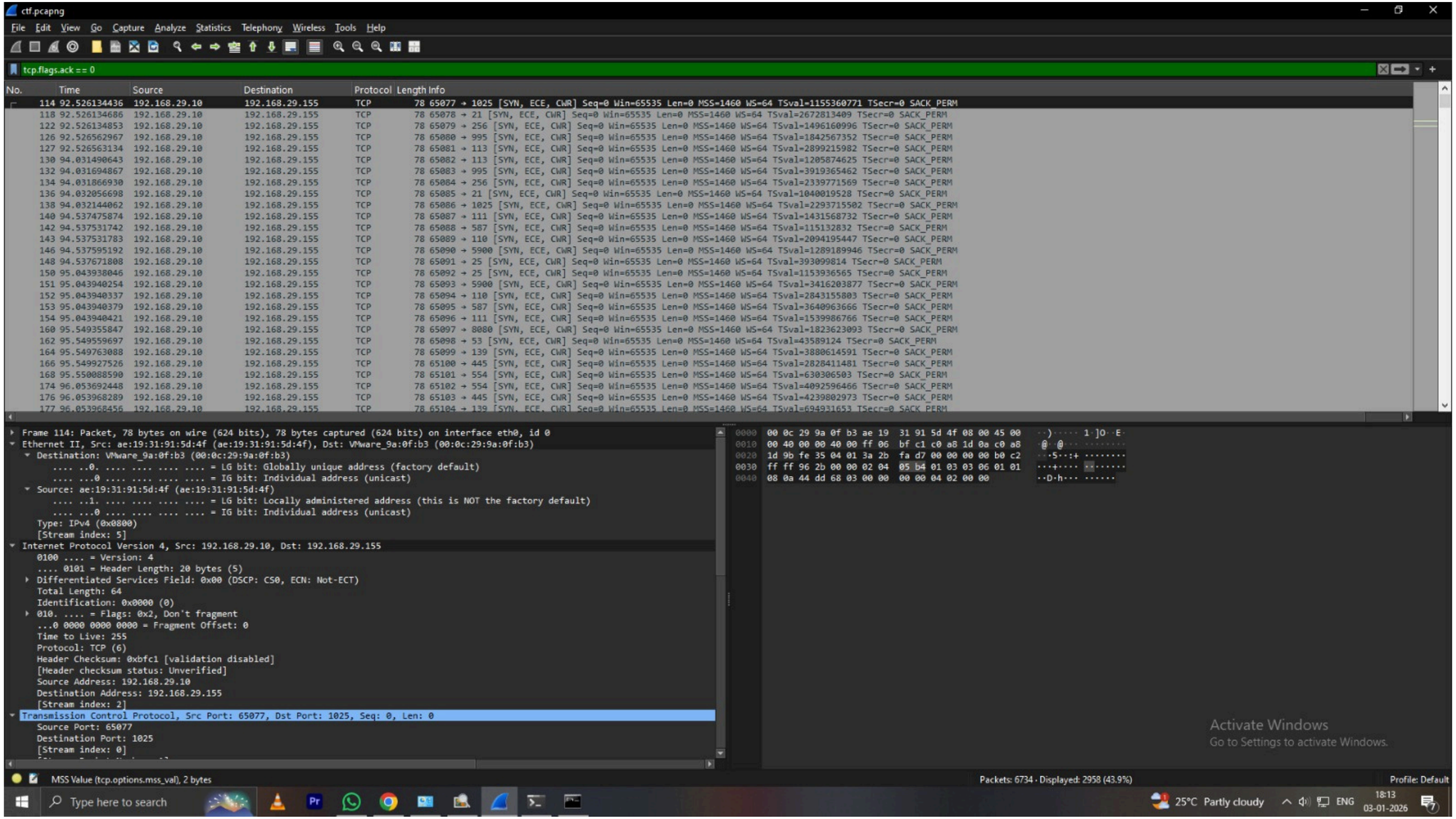


Step 5 : Detect Reconnaissance Activity (Port Scanning)

Apply the following Wireshark filter: tcp.flags.syn == 1 && tcp.flags.ack == 0

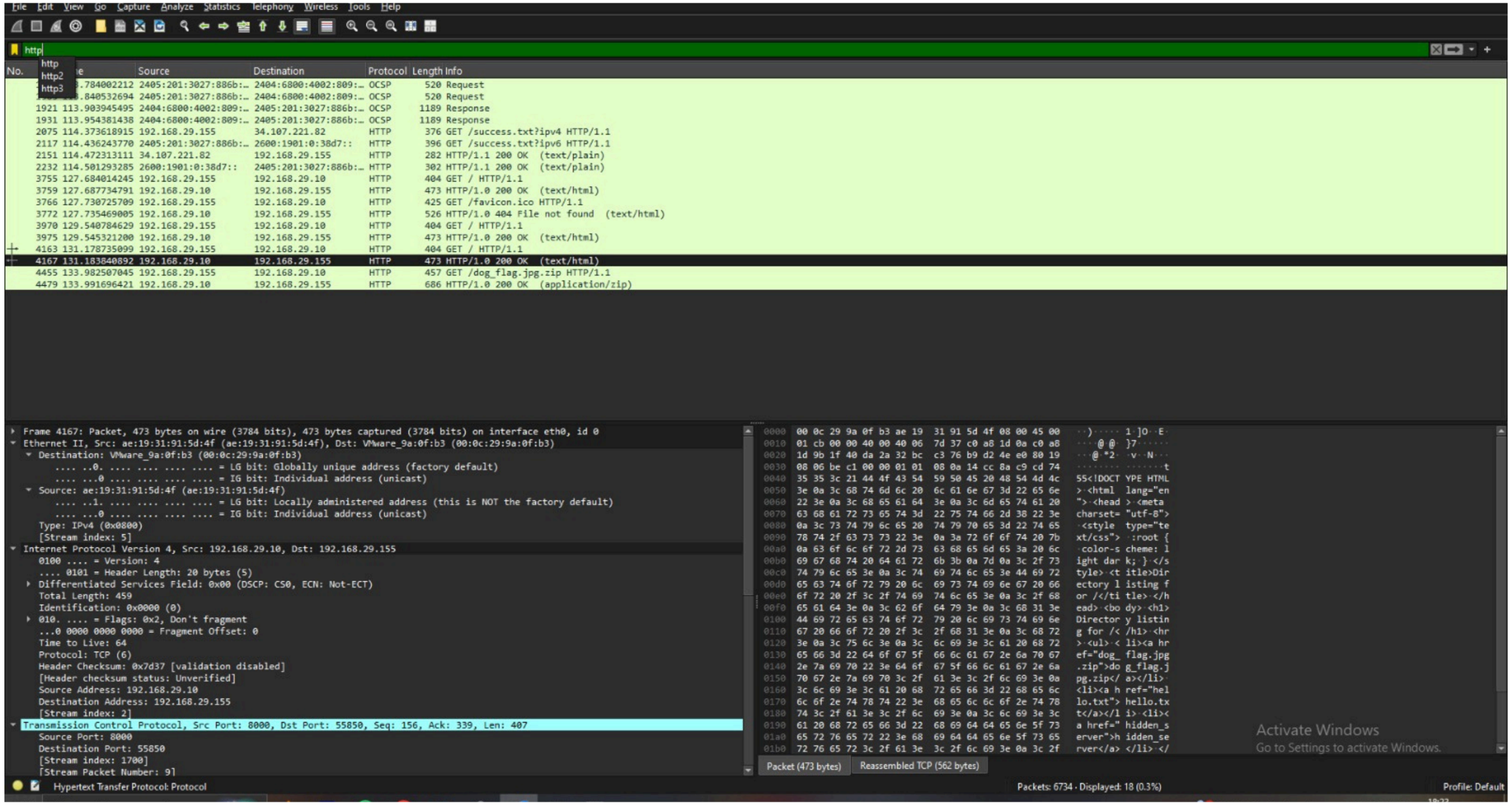
- Large number of SYN packets sent to multiple ports confirms scanning activity

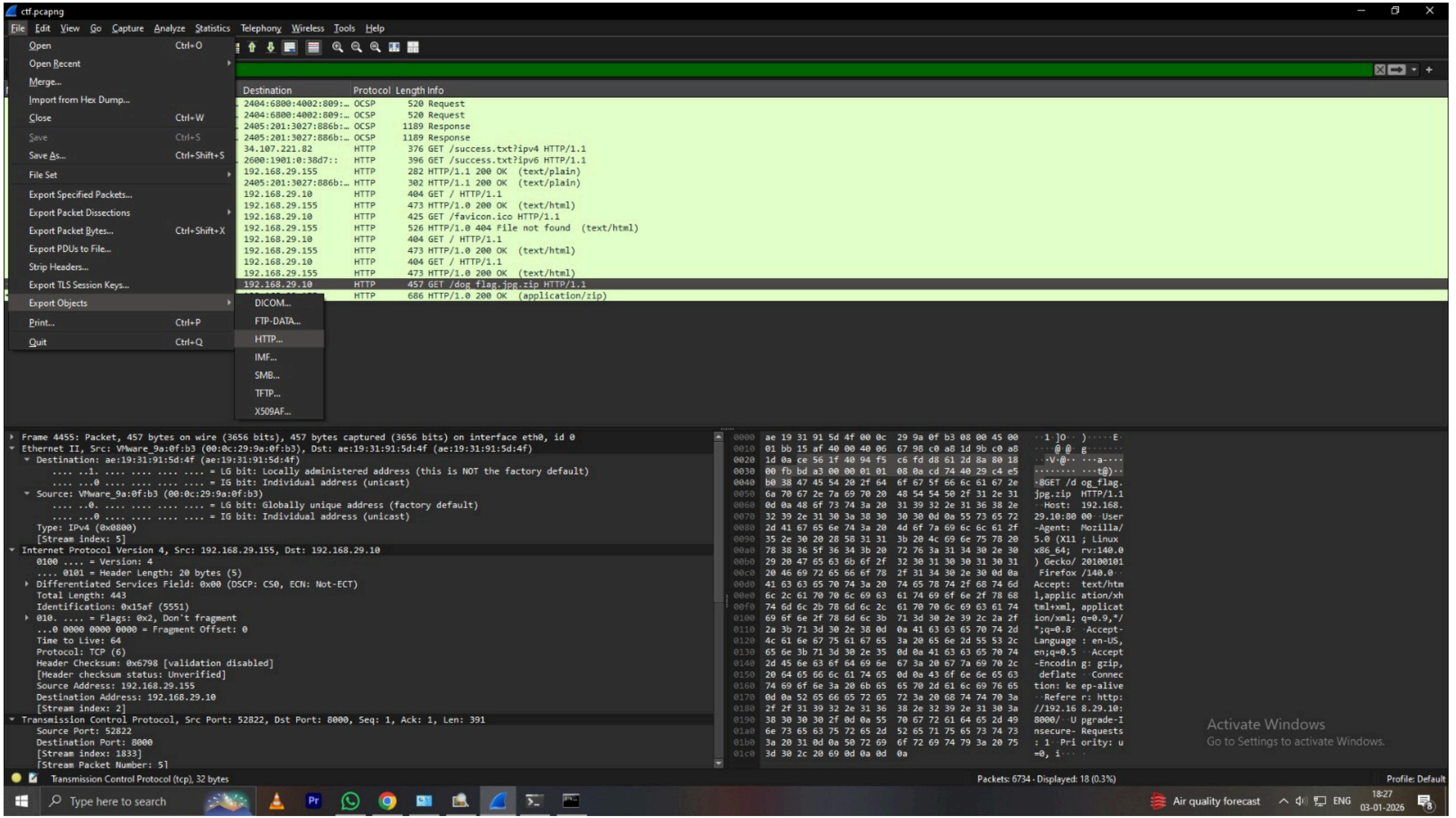


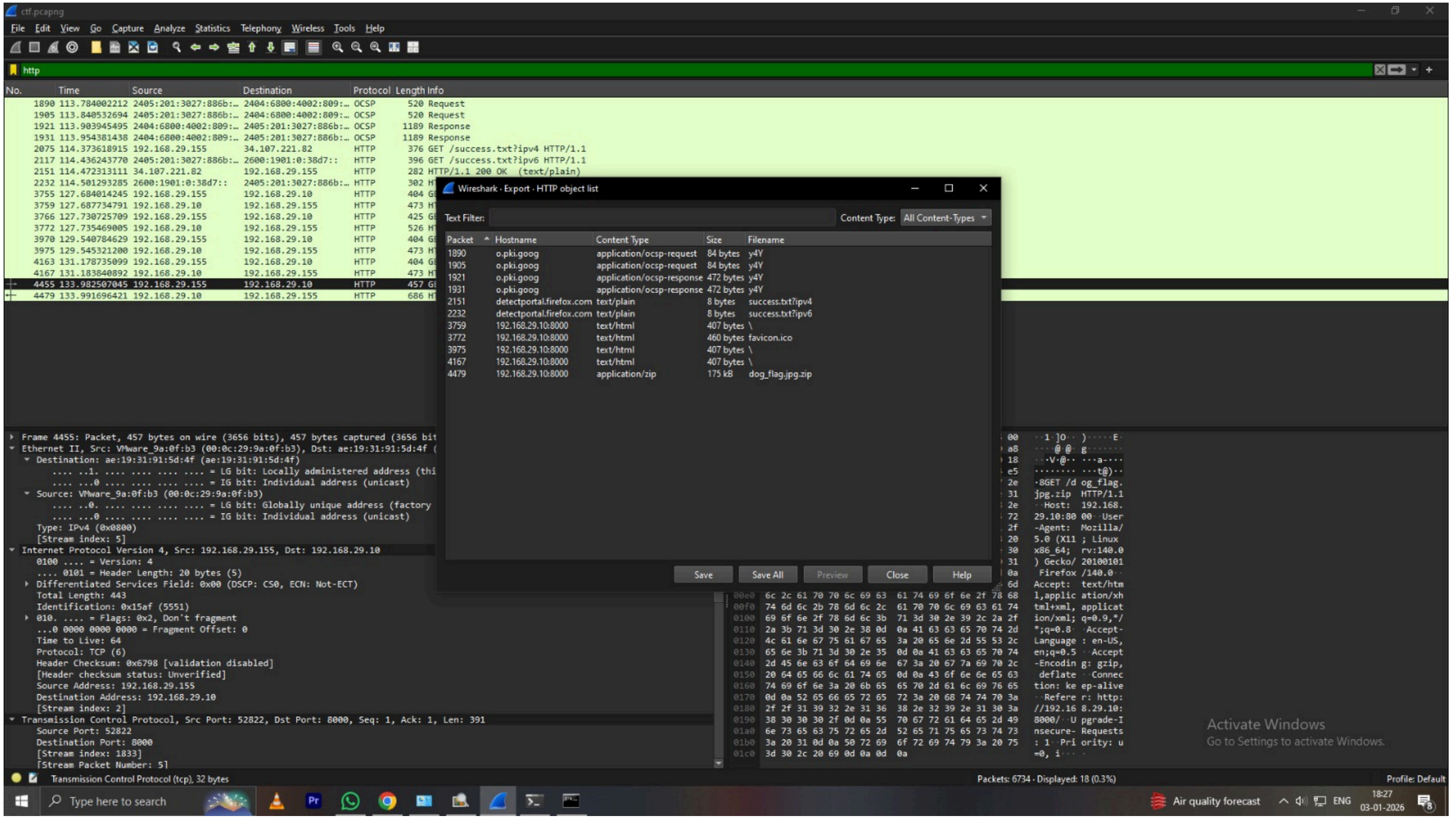

ctf.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.ack == 0
No. Time Source Destination Protocol Length Info
114 92.526134436 192.168.29.10 192.168.29.155 TCP 78 65077 → 1025 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1155360771 TSecr=0 SACK_PERM
118 92.526134686 192.168.29.10 192.168.29.155 TCP 78 65078 → 21 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2672813409 TSecr=0 SACK_PERM
122 92.526134853 192.168.29.10 192.168.29.155 TCP 78 65079 → 256 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1496160996 TSecr=0 SACK_PERM
126 92.526562967 192.168.29.10 192.168.29.155 TCP 78 65080 → 995 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1842567352 TSecr=0 SACK_PERM
127 92.526563134 192.168.29.10 192.168.29.155 TCP 78 65081 → 113 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2899215982 TSecr=0 SACK_PERM
130 94.031490643 192.168.29.10 192.168.29.155 TCP 78 65082 → 113 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1205874625 TSecr=0 SACK_PERM
132 94.031694867 192.168.29.10 192.168.29.155 TCP 78 65083 → 995 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3919365462 TSecr=0 SACK_PERM
134 94.031866930 192.168.29.10 192.168.29.155 TCP 78 65084 → 256 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2339771569 TSecr=0 SACK_PERM
136 94.032056698 192.168.29.10 192.168.29.155 TCP 78 65085 → 21 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1040019528 TSecr=0 SACK_PERM
138 94.032144062 192.168.29.10 192.168.29.155 TCP 78 65086 → 1025 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2293715502 TSecr=0 SACK_PERM
140 94.537475874 192.168.29.10 192.168.29.155 TCP 78 65087 → 111 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1431568732 TSecr=0 SACK_PERM
142 94.537531742 192.168.29.10 192.168.29.155 TCP 78 65088 → 587 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=115132832 TSecr=0 SACK_PERM
143 94.537531783 192.168.29.10 192.168.29.155 TCP 78 65089 → 110 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2094195447 TSecr=0 SACK_PERM
146 94.537595192 192.168.29.10 192.168.29.155 TCP 78 65090 → 5900 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1289189946 TSecr=0 SACK_PERM
148 94.537671808 192.168.29.10 192.168.29.155 TCP 78 65091 → 25 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=393099814 TSecr=0 SACK_PERM
150 95.043938046 192.168.29.10 192.168.29.155 TCP 78 65092 → 25 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1153936565 TSecr=0 SACK_PERM
151 95.043940254 192.168.29.10 192.168.29.155 TCP 78 65093 → 5900 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3416203877 TSecr=0 SACK_PERM
152 95.043940337 192.168.29.10 192.168.29.155 TCP 78 65094 → 110 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2843155803 TSecr=0 SACK_PERM
153 95.043940379 192.168.29.10 192.168.29.155 TCP 78 65095 → 587 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3640963666 TSecr=0 SACK_PERM
154 95.043940421 192.168.29.10 192.168.29.155 TCP 78 65096 → 111 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1539986766 TSecr=0 SACK_PERM
160 95.549355847 192.168.29.10 192.168.29.155 TCP 78 65097 → 8080 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1823623093 TSecr=0 SACK_PERM
162 95.549559697 192.168.29.10 192.168.29.155 TCP 78 65098 → 53 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=43589124 TSecr=0 SACK_PERM
164 95.549763088 192.168.29.10 192.168.29.155 TCP 78 65099 → 139 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3880614591 TSecr=0 SACK_PERM
166 95.549927526 192.168.29.10 192.168.29.155 TCP 78 65100 → 445 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2828411481 TSecr=0 SACK_PERM
168 95.550088590 192.168.29.10 192.168.29.155 TCP 78 65101 → 554 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=630306503 TSecr=0 SACK_PERM
174 96.053692448 192.168.29.10 192.168.29.155 TCP 78 65102 → 554 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4092596466 TSecr=0 SACK_PERM
176 96.053968289 192.168.29.10 192.168.29.155 TCP 78 65103 → 445 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4239802973 TSecr=0 SACK_PERM
177 96.053968456 192.168.29.10 192.168.29.155 TCP 78 65104 → 139 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=694931653 TSecr=0 SACK_PERM
Frame 114: Packet, 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0, id 0
Ethernet II, Src: ae:19:31:91:5d:4f (ae:19:31:91:5d:4f), Dst: VMware_9a:0f:b3 (00:0c:29:9a:0f:b3)
Destination: VMware_9a:0f:b3 (00:0c:29:9a:0f:b3)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: ae:19:31:91:5d:4f (ae:19:31:91:5d:4f)
.... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 5]
Internet Protocol Version 4, Src: 192.168.29.10, Dst: 192.168.29.155
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 64
Identification: 0x0000 (0)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
Protocol: TCP (6)
Header Checksum: 0xbfc1 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.29.10
Destination Address: 192.168.29.155
[Stream index: 2]
Transmission Control Protocol, Src Port: 65077, Dst Port: 1025, Seq: 0, Len: 0
Source Port: 65077
Destination Port: 1025
[Stream index: 0]
0000 00 0c 29 9a 0f b3 ae 19 31 91 5d 4f 08 00 45 00
0010 00 40 00 00 40 00 ff 06 bf c1 c0 a8 1d 0a c0 a8
0020 1d 9b fe 35 04 01 3a 2b fa d7 00 00 00 00 b0 c2
0030 ff ff 96 2b 00 00 02 04 05 b4 01 03 03 06 01 01
0040 08 0a 44 dd 68 03 00 00 00 00 04 02 00 00
Activate Windows
Go to Settings to activate Windows.
MSS Value (tcp.options.mss_val), 2 bytes
Packets: 6734 · Displayed: 2958 (43.9%)
Profile: Default
Type here to search
25°C Partly cloudy
ENG
18:13
03-01-2026

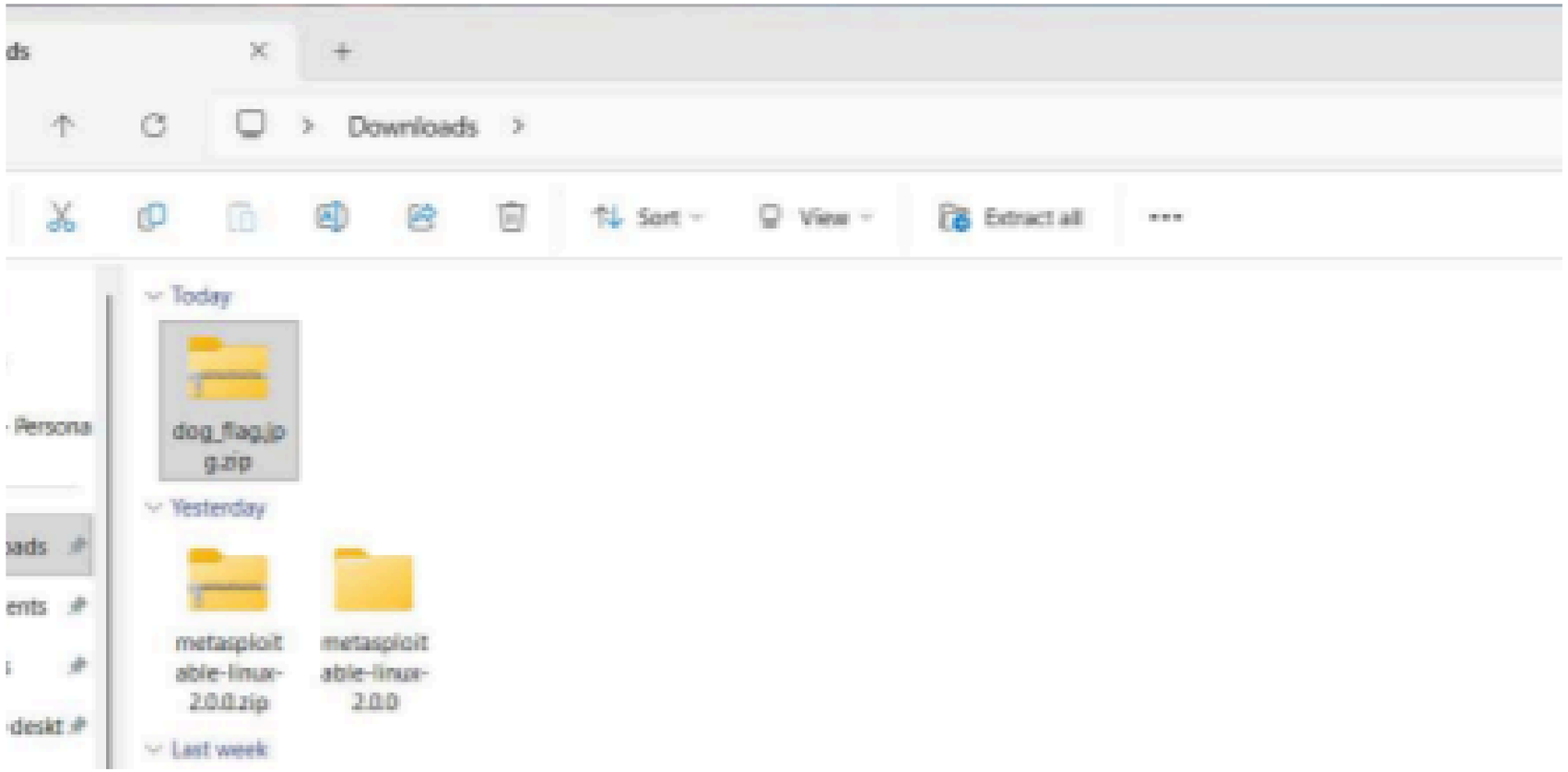
Step 6 : Analyze HTTP Traffic

- Apply HTTP filter: http
- Navigate to File Export Objects HTTP
- Identify and extract the downloaded ZIP file



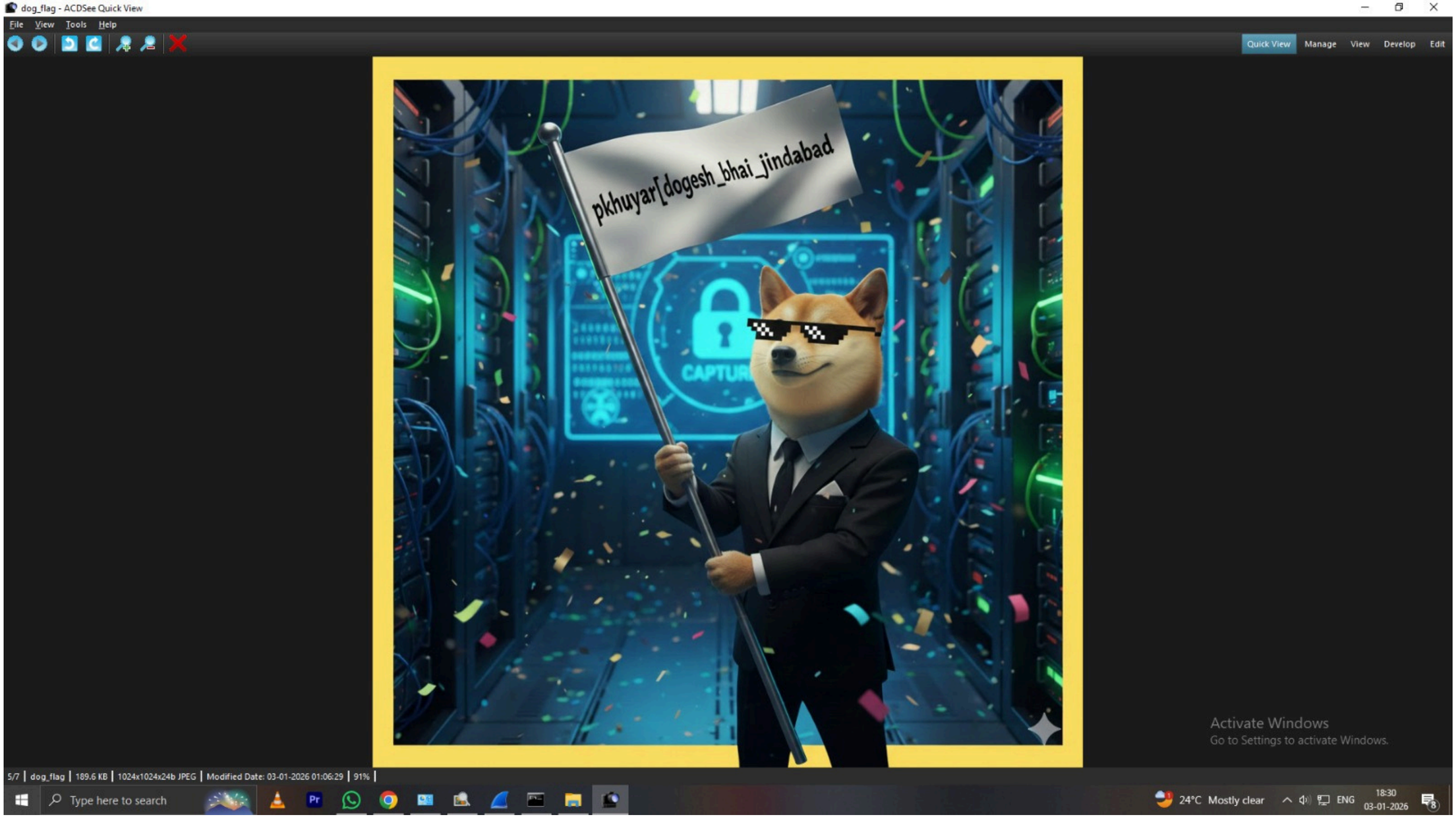

ctf.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Strip Headers...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
FTP-DATA...
HTTP...
IMF...
SMB...
TFTP...
X509AF...
Destination Protocol Length Info
2404:6800:4002:809:... OCSP 520 Request
2404:6800:4002:809:... OCSP 520 Request
2405:201:3027:886b:... OCSP 1189 Response
2405:201:3027:886b:... OCSP 1189 Response
34.107.221.82 HTTP 376 GET /success.txt?ipv4 HTTP/1.1
2600:1901:0:38d7:: HTTP 396 GET /success.txt?ipv6 HTTP/1.1
192.168.29.155 HTTP 282 HTTP/1.1 200 OK (text/plain)
2405:201:3027:886b:... HTTP 302 HTTP/1.1 200 OK (text/plain)
192.168.29.10 HTTP 404 GET / HTTP/1.1
192.168.29.155 HTTP 473 HTTP/1.0 200 OK (text/html)
192.168.29.10 HTTP 425 GET /favicon.ico HTTP/1.1
192.168.29.155 HTTP 526 HTTP/1.0 404 File not found (text/html)
192.168.29.10 HTTP 404 GET / HTTP/1.1
192.168.29.155 HTTP 473 HTTP/1.0 200 OK (text/html)
192.168.29.10 HTTP 404 GET / HTTP/1.1
192.168.29.155 HTTP 473 HTTP/1.0 200 OK (text/html)
192.168.29.10 HTTP 457 GET /dog_flag.jpg.zip HTTP/1.1
HTTP 686 HTTP/1.0 200 OK (application/zip)
Frame 4455: Packet, 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits) on interface eth0, id 0
Ethernet II, Src: VMware_9a:0f:b3 (00:0c:29:9a:0f:b3), Dst: ae:19:31:91:5d:4f (ae:19:31:91:5d:4f)
Destination: ae:19:31:91:5d:4f (ae:19:31:91:5d:4f)
.... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
....0 .... = IG bit: Individual address (unicast)
Source: VMware_9a:0f:b3 (00:0c:29:9a:0f:b3)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 5]
Internet Protocol Version 4, Src: 192.168.29.155, Dst: 192.168.29.10
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 443
Identification: 0x15af (5551)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x6798 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.29.155
Destination Address: 192.168.29.10
[Stream index: 2]
Transmission Control Protocol, Src Port: 52822, Dst Port: 8000, Seq: 1, Ack: 1, Len: 391
Source Port: 52822
Destination Port: 8000
[Stream index: 1833]
[Stream Packet Number: 51
0000 ae 19 31 91 5d 4f 00 0c 29 9a 0f b3 08 00 45 00
0010 01 bb 15 af 40 00 40 06 67 98 c0 a8 1d 9b c0 a8
0020 1d 0a ce 56 1f 40 94 f5 c6 fd d8 61 2d 8a 80 18
0030 00 fb bd a3 00 00 01 01 08 0a cd 74 40 29 c4 e5
0040 b0 38 47 45 54 20 2f 64 6f 67 5f 66 6c 61 67 2e
0050 6a 70 67 2e 7a 69 70 20 48 54 54 50 2f 31 2e 31
0060 0d 0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e
0070 32 39 2e 31 30 3a 38 30 30 30 0d 0a 55 73 65 72
0080 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f
0090 35 2e 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20
00a0 78 38 36 5f 36 34 3b 20 72 76 3a 31 34 30 2e 30
00b0 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31
00c0 20 46 69 72 65 66 6f 78 2f 31 34 30 2e 30 0d 0a
00d0 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d
00e0 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68
00f0 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74
0100 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f
0110 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d
0120 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c
0130 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74
0140 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c
0150 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e 6e 65 63
0160 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65
0170 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a
0180 2f 2f 31 39 32 2e 31 36 38 2e 32 39 2e 31 30 3a
0190 38 30 30 30 2f 0d 0a 55 70 67 72 61 64 65 2d 49
01a0 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73
01b0 3a 20 31 0d 0a 50 72 69 6f 72 69 74 79 3a 20 75
01c0 3d 30 2c 20 69 0d 0a 0d 0a
Transmission Control Protocol (tcp), 32 bytes
Packets: 6734 · Displayed: 18 (0.3%)
Profile: Default
Activate Windows
Go to Settings to activate Windows.
Type here to search
Air quality forecast
ENG
18:27
03-01-2026


ctf.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
1890 113.784002212 2405:201:3027:886b:… 2404:6800:4002:809:… OCSP 520 Request
1905 113.840532694 2405:201:3027:886b:… 2404:6800:4002:809:… OCSP 520 Request
1921 113.903945495 2404:6800:4002:809:… 2405:201:3027:886b:… OCSP 1189 Response
1931 113.954381438 2404:6800:4002:809:… 2405:201:3027:886b:… OCSP 1189 Response
2075 114.373618915 192.168.29.155 34.107.221.82 HTTP 376 GET /success.txt?ipv4 HTTP/1.1
2117 114.436243770 2405:201:3027:886b:… 2600:1901:0:38d7:: HTTP 396 GET /success.txt?ipv6 HTTP/1.1
2151 114.472313111 34.107.221.82 192.168.29.155 HTTP 282 HTTP/1.1 200 OK (text/plain)
2232 114.501293285 2600:1901:0:38d7:: 2405:201:3027:886b:… HTTP 302 H
3755 127.684014245 192.168.29.155 192.168.29.10 HTTP 404 G
3759 127.687734791 192.168.29.10 192.168.29.155 HTTP 473 H
3766 127.730725709 192.168.29.155 192.168.29.10 HTTP 425 G
3772 127.735469005 192.168.29.10 192.168.29.155 HTTP 526 H
3970 129.540784629 192.168.29.155 192.168.29.10 HTTP 404 G
3975 129.545321200 192.168.29.10 192.168.29.155 HTTP 473 H
4163 131.178735099 192.168.29.155 192.168.29.10 HTTP 404 G
4167 131.183840892 192.168.29.10 192.168.29.155 HTTP 473 H
4455 133.982507045 192.168.29.155 192.168.29.10 HTTP 457 G
4479 133.991696421 192.168.29.10 192.168.29.155 HTTP 686 H
Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Packet Hostname Content Type Size Filename
1890 o.pki.goog application/ocsp-request 84 bytes y4Y
1905 o.pki.goog application/ocsp-request 84 bytes y4Y
1921 o.pki.goog application/ocsp-response 472 bytes y4Y
1931 o.pki.goog application/ocsp-response 472 bytes y4Y
2151 detectportal.firefox.com text/plain 8 bytes success.txt?ipv4
2232 detectportal.firefox.com text/plain 8 bytes success.txt?ipv6
3759 192.168.29.10:8000 text/html 407 bytes \
3772 192.168.29.10:8000 text/html 460 bytes favicon.ico
3975 192.168.29.10:8000 text/html 407 bytes \
4167 192.168.29.10:8000 text/html 407 bytes \
4479 192.168.29.10:8000 application/zip 175 kB dog_flag.jpg.zip
Save Save All Preview Close Help
Frame 4455: Packet, 457 bytes on wire (3656 bits), 457 bytes captured (3656 bit
Ethernet II, Src: VMware_9a:0f:b3 (00:0c:29:9a:0f:b3), Dst: ae:19:31:91:5d:4f (
Destination: ae:19:31:91:5d:4f (ae:19:31:91:5d:4f)
.... ..1. .... = LG bit: Locally administered address (thi
....0 .... = IG bit: Individual address (unicast)
Source: VMware_9a:0f:b3 (00:0c:29:9a:0f:b3)
.... ..0. .... = LG bit: Globally unique address (factory
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 5]
Internet Protocol Version 4, Src: 192.168.29.155, Dst: 192.168.29.10
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 443
Identification: 0x15af (5551)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x6798 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.29.155
Destination Address: 192.168.29.10
[Stream index: 2]
Transmission Control Protocol, Src Port: 52822, Dst Port: 8000, Seq: 1, Ack: 1, Len: 391
Source Port: 52822
Destination Port: 8000
[Stream index: 1833]
[Stream Packet Number: 51
00e0 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68
00f0 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74
0100 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f
0110 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d
0120 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c
0130 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74
0140 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c
0150 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e 6e 65 63
0160 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65
0170 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a
0180 2f 2f 31 39 32 2e 31 36 38 2e 32 39 2e 31 30 3a
0190 38 30 30 30 2f 0d 0a 55 70 67 72 61 64 65 2d 49
01a0 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73
01b0 3a 20 31 0d 0a 50 72 69 6f 72 69 74 79 3a 20 75
01c0 3d 30 2c 20 69 0d 0a 0d 0a
Activate Windows
Go to Settings to activate Windows.
Transmission Control Protocol (tcp), 32 bytes
Packets: 6734 · Displayed: 18 (0.3%)
Profile: Default
Type here to search
Air quality forecast
ENG
18:27
03-01-2026



Step 7 : Extract the ZIP File

- Save the ZIP file locally
- Unzip the file to reveal the extracted content and flag


dog_flag - ACDSee Quick View
File View Tools Help
Quick View Manage View Develop Edit
pkhuyar{dogesh_bhai_jindabad
Activate Windows
Go to Settings to activate Windows.
5/7 | dog_flag | 189.6 KB | 1024x1024x24b JPEG | Modified Date: 03-01-2026 01:06:29 | 91% |
Type here to search
24°C Mostly clear
ENG
18:30
03-01-2026

QUESTIONS & ANSWERS

- **What is the attacker IP address?**

  192.168.29.10

- **What is the first packet timestamp related to the attack?**

  Within 1 second (approximately 100 packets)

- **What is the name of the downloaded ZIP file?**

  dog flag.jpg

- **What is the flag obtained after unzipping the file?**

  pkhuyar (dogesh_bhai_jindabad

- **What evidence suggests reconnaissance activity?**

  The attacker sends multiple SYN packets to different port numbers on the victim machine.

RESULT & CONCLUSION

This project demonstrates how PCAP analysis helps in identifying malicious behavior such as port scanning and unauthorized file downloads.

Using Wireshark, we successfully detected reconnaissance activity, identified attacker details, and extracted sensitive files from unencrypted HTTP traffic.

THANK YOU