Wireshark Wonders

Diving into the Shark Tank

About Me

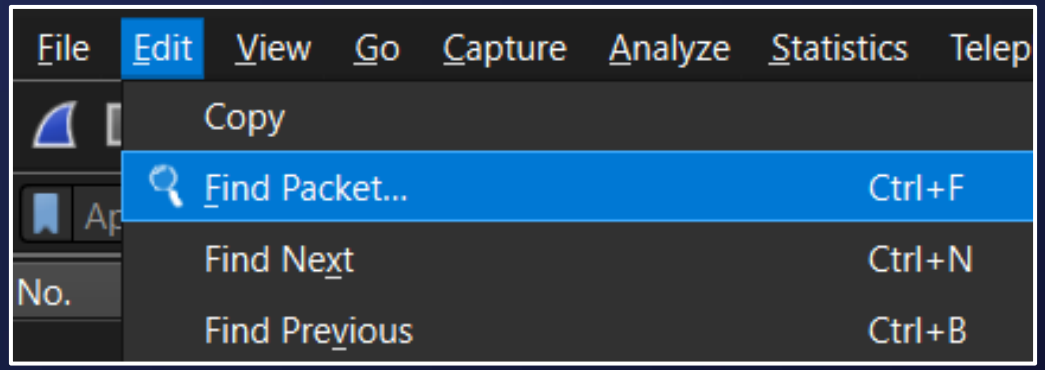
- Jia Qi
- Degree Y2 Cybersecurity student
- MCC alumni & crew, GCC alumni
- President @ FSEC-SS APU

01 Wireshark Basics

My “muscle memory”

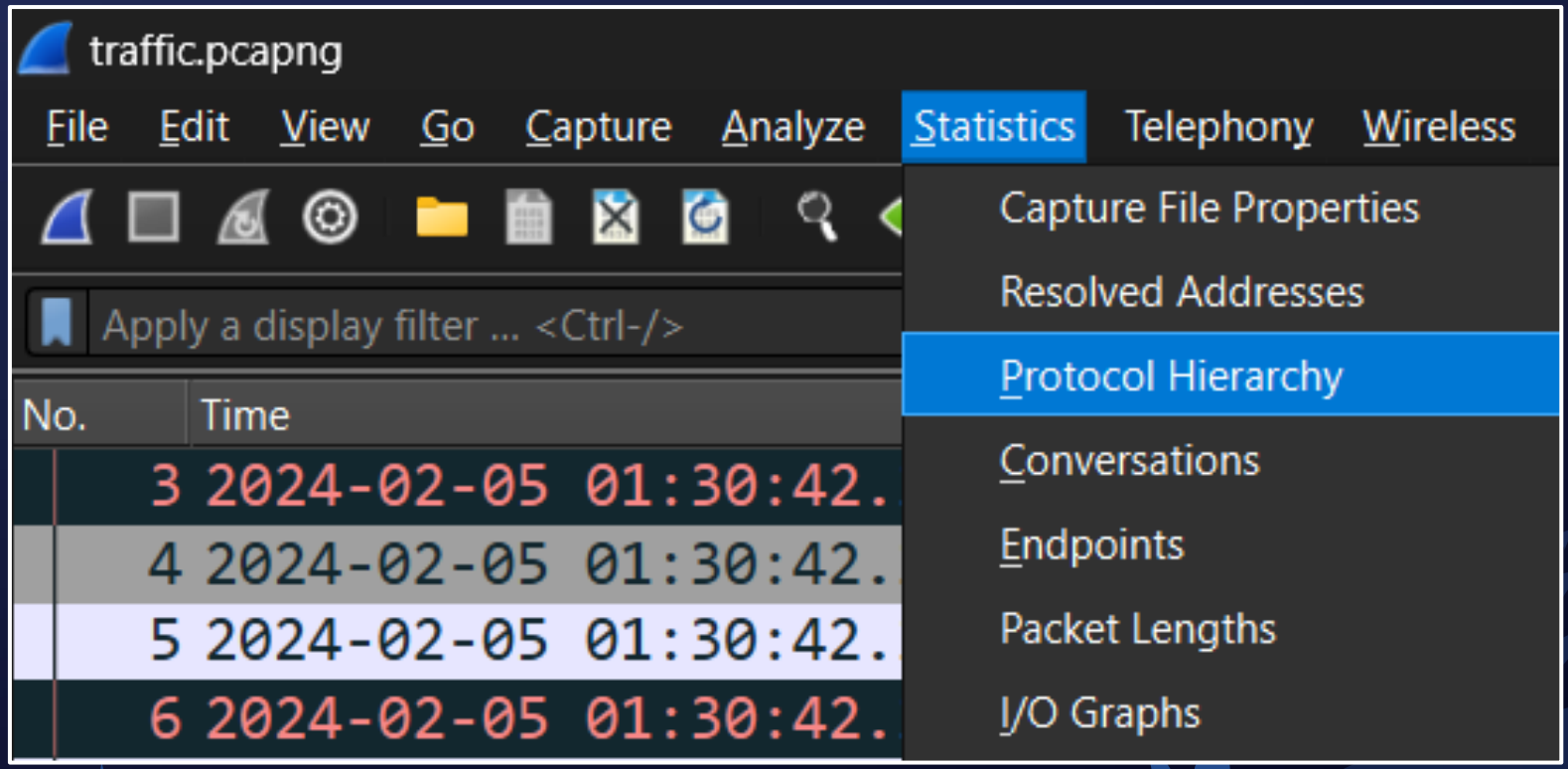
Zip password: **wireshark**

Find String

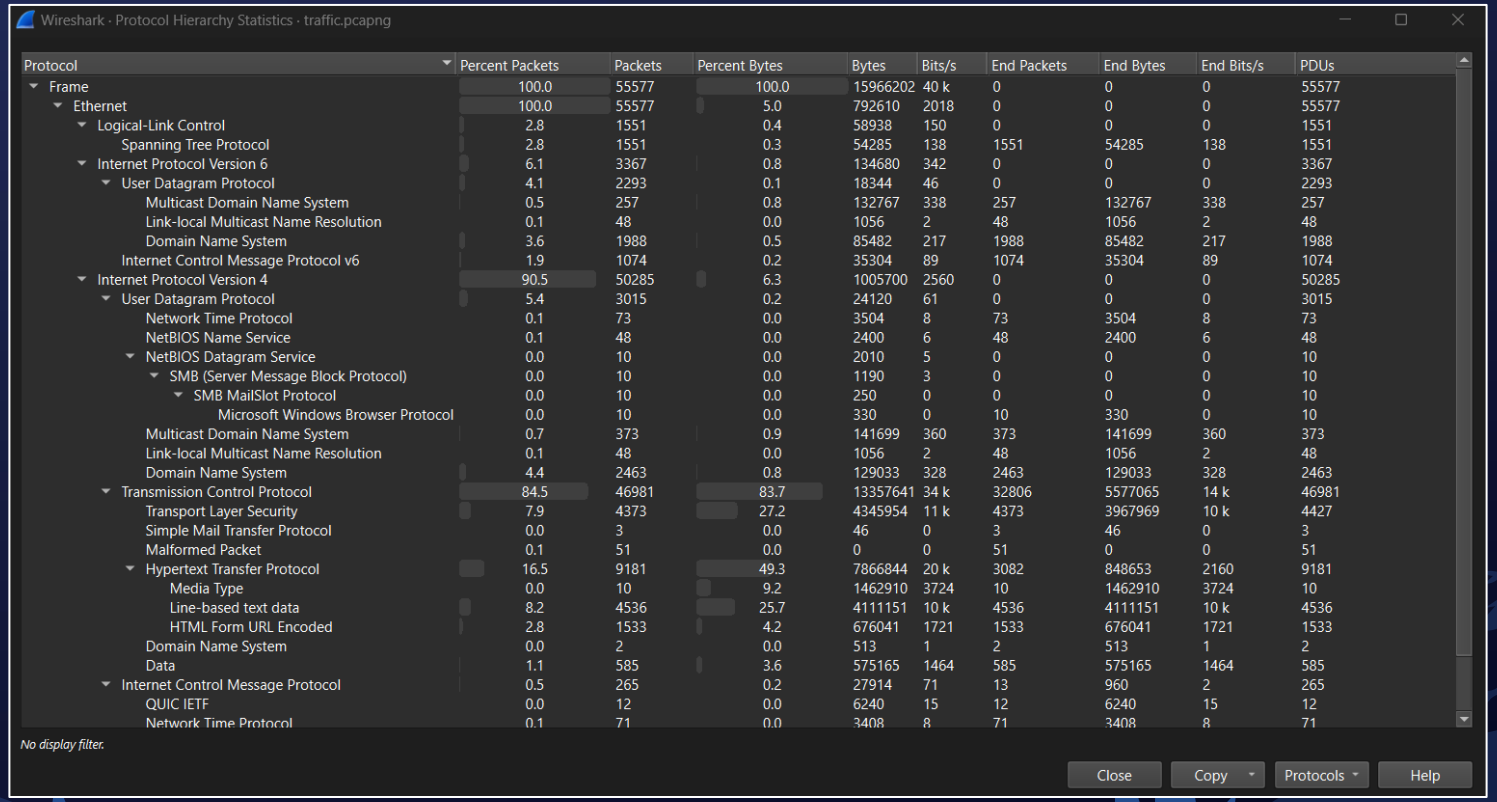

File
Edit
View
Go
Capture
Analyze
Statistics
Telep
Copy
Find Packet...
Ctrl+F
Find Next
Ctrl+N
Find Previous
Ctrl+B
No.


Apply a display filter ... <Ctrl-/>
Packet details
Narrow (UTF-8 / ASCII)
Case sensitive
String
flag

Protocol Hierarchy

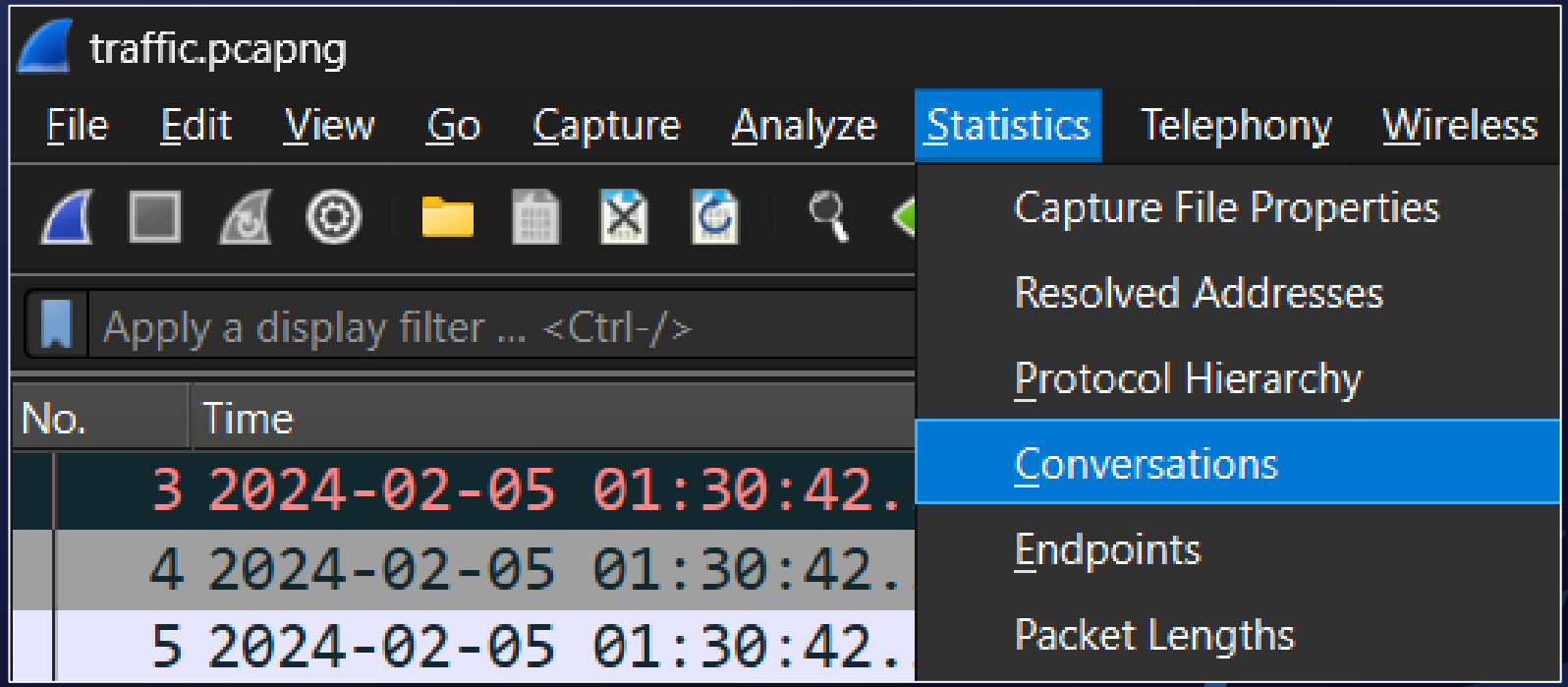


Protocol Hierarchy

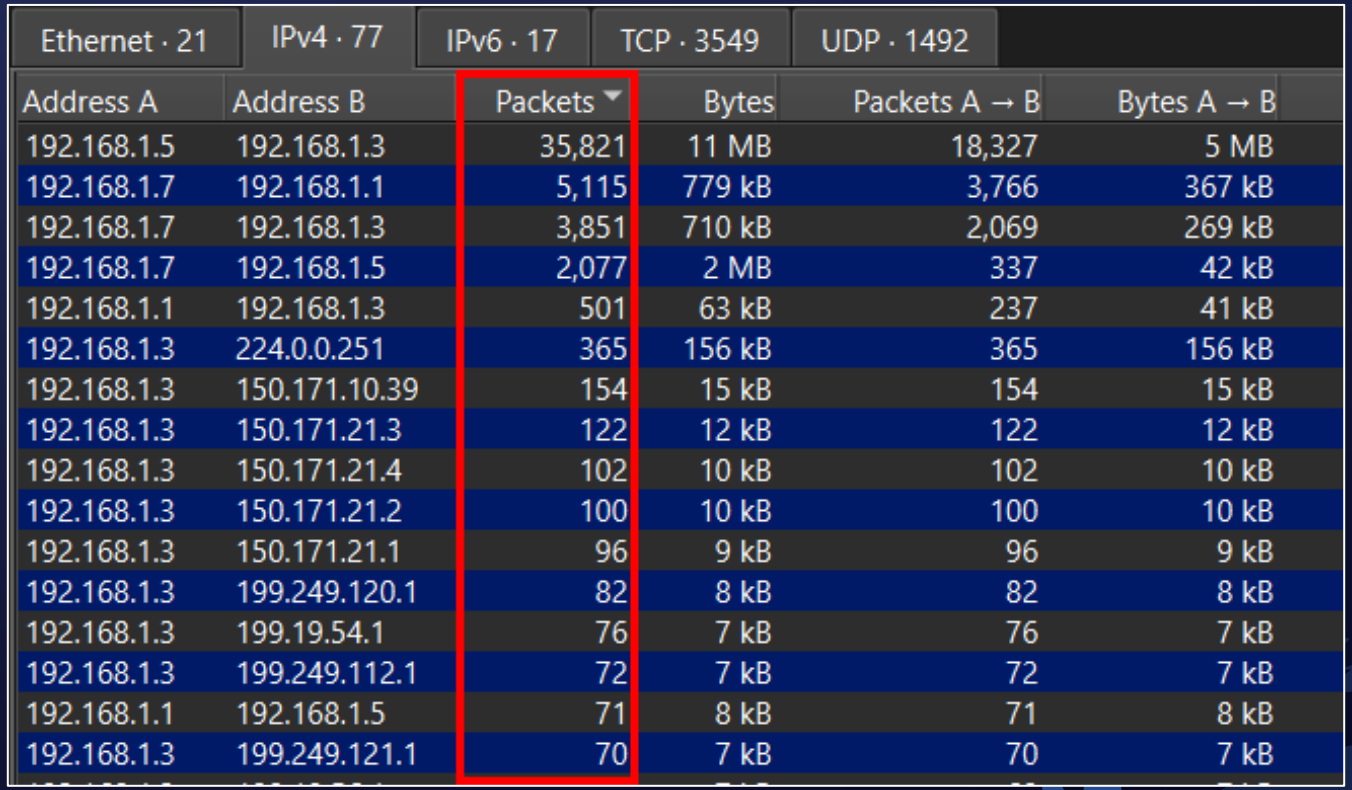


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	55577	100.0	15966202	40 k	0	0	0	55577
Ethernet	100.0	55577	5.0	792610	2018	0	0	0	55577
Logical-Link Control	2.8	1551	0.4	58938	150	0	0	0	1551
Spanning Tree Protocol	2.8	1551	0.3	54285	138	1551	54285	138	1551
Internet Protocol Version 6	6.1	3367	0.8	134680	342	0	0	0	3367
User Datagram Protocol	4.1	2293	0.1	18344	46	0	0	0	2293
Multicast Domain Name System	0.5	257	0.8	132767	338	257	132767	338	257
Link-local Multicast Name Resolution	0.1	48	0.0	1056	2	48	1056	2	48
Domain Name System	3.6	1988	0.5	85482	217	1988	85482	217	1988
Internet Control Message Protocol v6	1.9	1074	0.2	35304	89	1074	35304	89	1074
Internet Protocol Version 4	90.5	50285	6.3	1005700	2560	0	0	0	50285
User Datagram Protocol	5.4	3015	0.2	24120	61	0	0	0	3015
Network Time Protocol	0.1	73	0.0	3504	8	73	3504	8	73
NetBIOS Name Service	0.1	48	0.0	2400	6	48	2400	6	48
NetBIOS Datagram Service	0.0	10	0.0	2010	5	0	0	0	10
SMB (Server Message Block Protocol)	0.0	10	0.0	1190	3	0	0	0	10
SMB MailSlot Protocol	0.0	10	0.0	250	0	0	0	0	10
Microsoft Windows Browser Protocol	0.0	10	0.0	330	0	10	330	0	10
Multicast Domain Name System	0.7	373	0.9	141699	360	373	141699	360	373
Link-local Multicast Name Resolution	0.1	48	0.0	1056	2	48	1056	2	48
Domain Name System	4.4	2463	0.8	129033	328	2463	129033	328	2463
Transmission Control Protocol	84.5	46981	83.7	13357641	34 k	32806	5577065	14 k	46981
Transport Layer Security	7.9	4373	27.2	4345954	11 k	4373	3967969	10 k	4427
Simple Mail Transfer Protocol	0.0	3	0.0	46	0	3	46	0	3
Malformed Packet	0.1	51	0.0	0	0	51	0	0	51
Hypertext Transfer Protocol	16.5	9181	49.3	7866844	20 k	3082	848653	2160	9181
Media Type	0.0	10	9.2	1462910	3724	10	1462910	3724	10
Line-based text data	8.2	4536	25.7	4111151	10 k	4536	4111151	10 k	4536
HTML Form URL Encoded	2.8	1533	4.2	676041	1721	1533	676041	1721	1533
Domain Name System	0.0	2	0.0	513	1	2	513	1	2
Data	1.1	585	3.6	575165	1464	585	575165	1464	585
Internet Control Message Protocol	0.5	265	0.2	27914	71	13	960	2	265
QUIC IETF	0.0	12	0.0	6240	15	12	6240	15	12
Network Time Protocol	0.1	71	0.0	3408	8	71	3408	8	71

Conversations



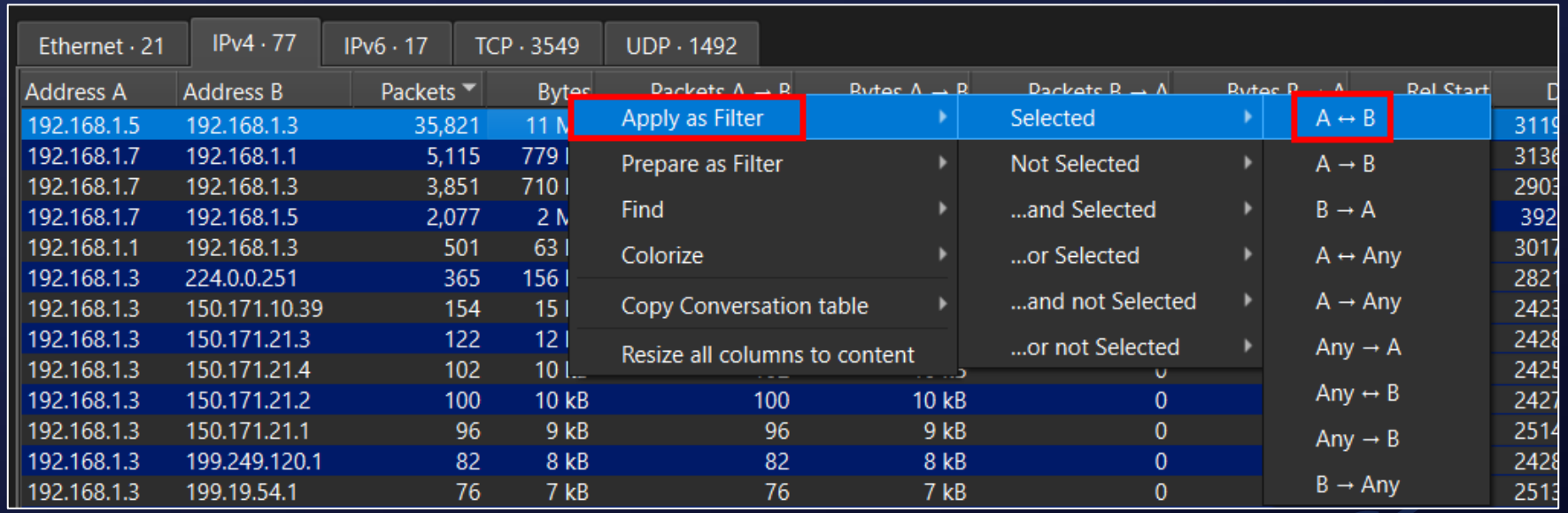
Conversations



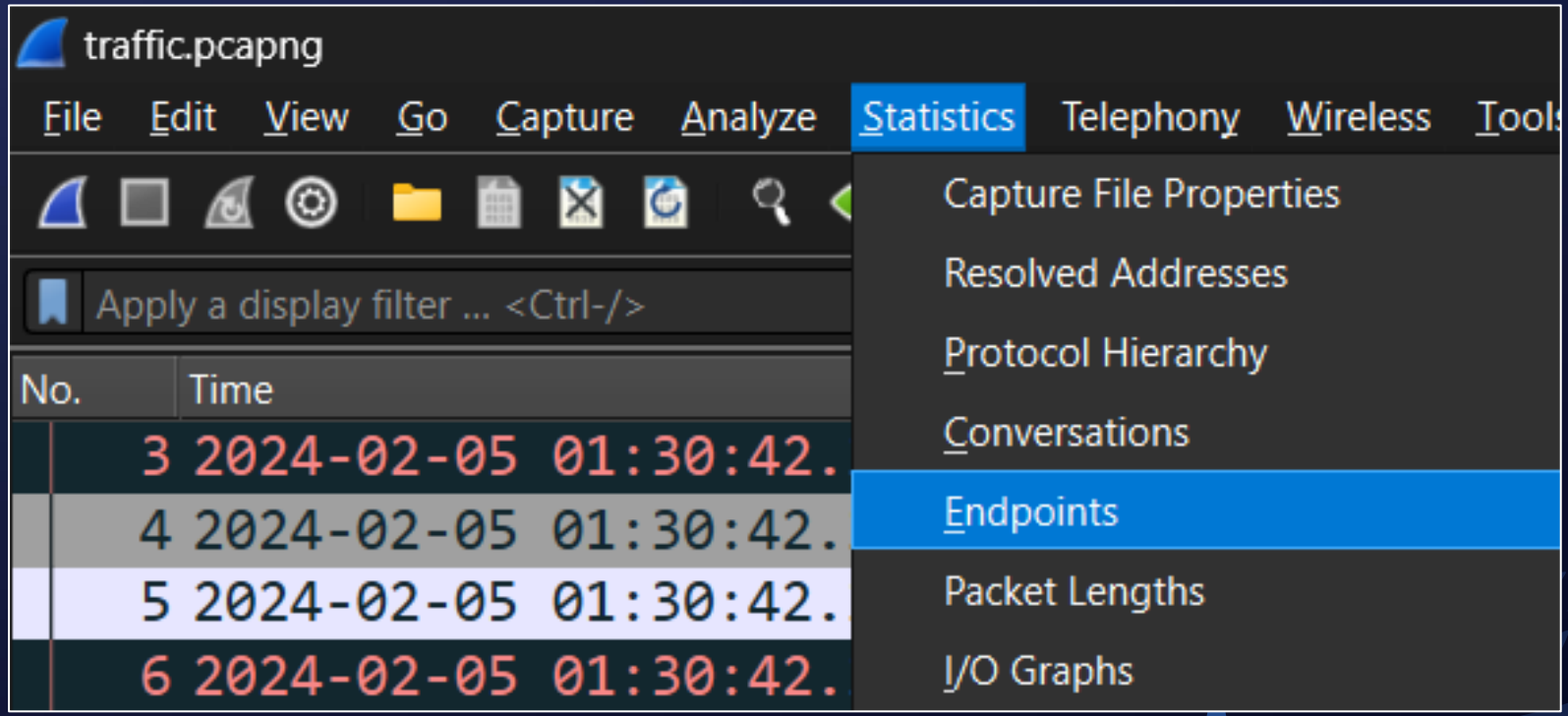
Ethernet · 21 | IPv4 · 77 | IPv6 · 17 | TCP · 3549 | UDP · 1492

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B
192.168.1.5	192.168.1.3	35,821	11 MB	18,327	5 MB
192.168.1.7	192.168.1.1	5,115	779 kB	3,766	367 kB
192.168.1.7	192.168.1.3	3,851	710 kB	2,069	269 kB
192.168.1.7	192.168.1.5	2,077	2 MB	337	42 kB
192.168.1.1	192.168.1.3	501	63 kB	237	41 kB
192.168.1.3	224.0.0.251	365	156 kB	365	156 kB
192.168.1.3	150.171.10.39	154	15 kB	154	15 kB
192.168.1.3	150.171.21.3	122	12 kB	122	12 kB
192.168.1.3	150.171.21.4	102	10 kB	102	10 kB
192.168.1.3	150.171.21.2	100	10 kB	100	10 kB
192.168.1.3	150.171.21.1	96	9 kB	96	9 kB
192.168.1.3	199.249.120.1	82	8 kB	82	8 kB
192.168.1.3	199.19.54.1	76	7 kB	76	7 kB
192.168.1.3	199.249.112.1	72	7 kB	72	7 kB
192.168.1.1	192.168.1.5	71	8 kB	71	8 kB
192.168.1.3	199.249.121.1	70	7 kB	70	7 kB

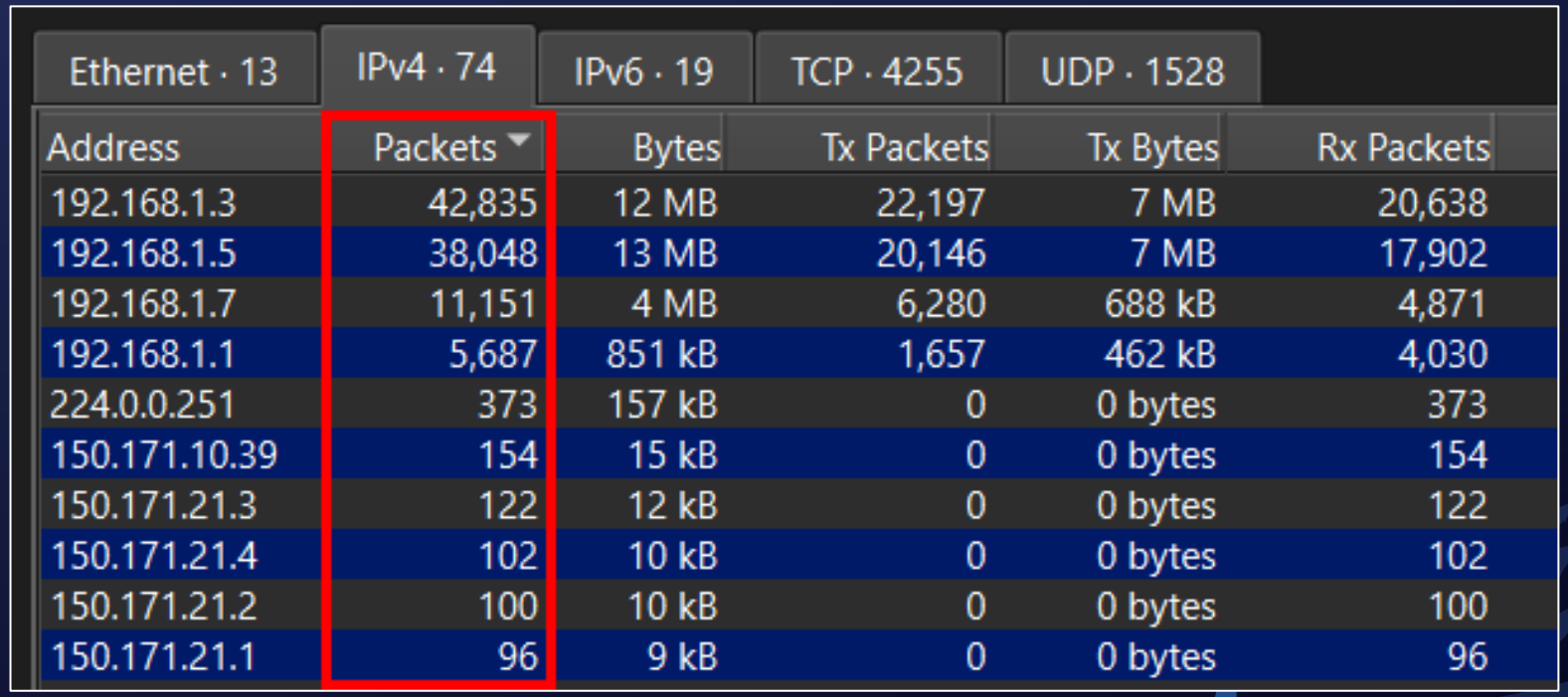
Conversations



Endpoints


traffic.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools
Apply a display filter ... <Ctrl-/>
No. Time
3 2024-02-05 01:30:42.
4 2024-02-05 01:30:42.
5 2024-02-05 01:30:42.
6 2024-02-05 01:30:42.
Capture File Properties
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs

Endpoints



Ethernet · 13 | IPv4 · 74 | IPv6 · 19 | TCP · 4255 | UDP · 1528

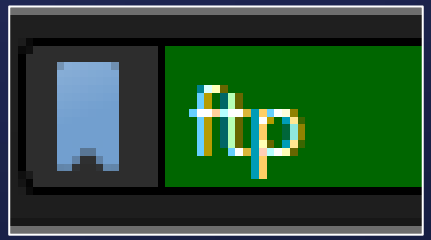
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets
192.168.1.3	42,835	12 MB	22,197	7 MB	20,638
192.168.1.5	38,048	13 MB	20,146	7 MB	17,902
192.168.1.7	11,151	4 MB	6,280	688 kB	4,871
192.168.1.1	5,687	851 kB	1,657	462 kB	4,030
224.0.0.251	373	157 kB	0	0 bytes	373
150.171.10.39	154	15 kB	0	0 bytes	154
150.171.21.3	122	12 kB	0	0 bytes	122
150.171.21.4	102	10 kB	0	0 bytes	102
150.171.21.2	100	10 kB	0	0 bytes	100
150.171.21.1	96	9 kB	0	0 bytes	96

02 Filtering

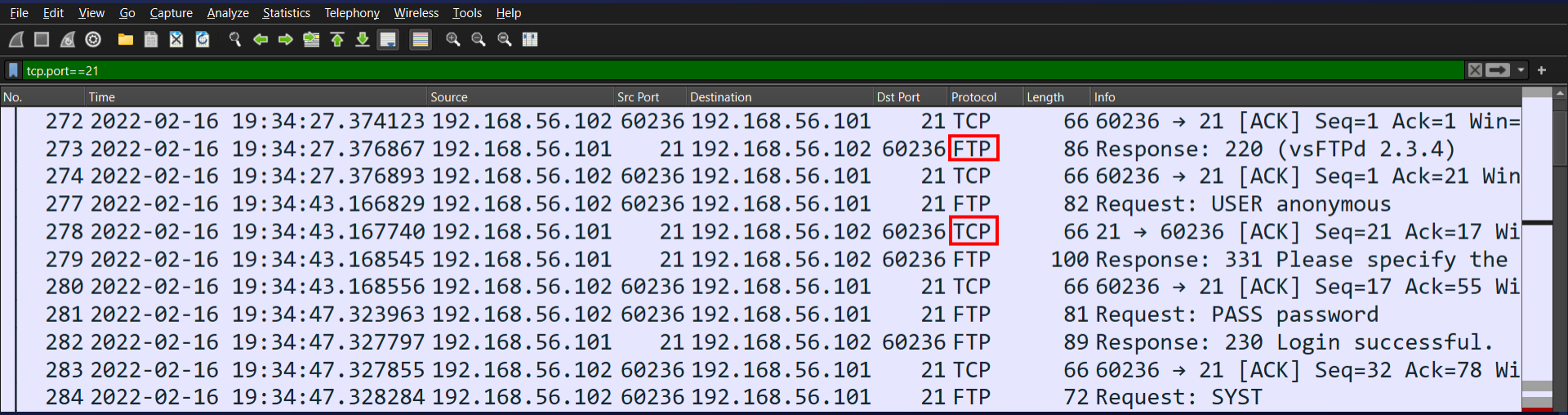
Just like how you filter your selfie pic

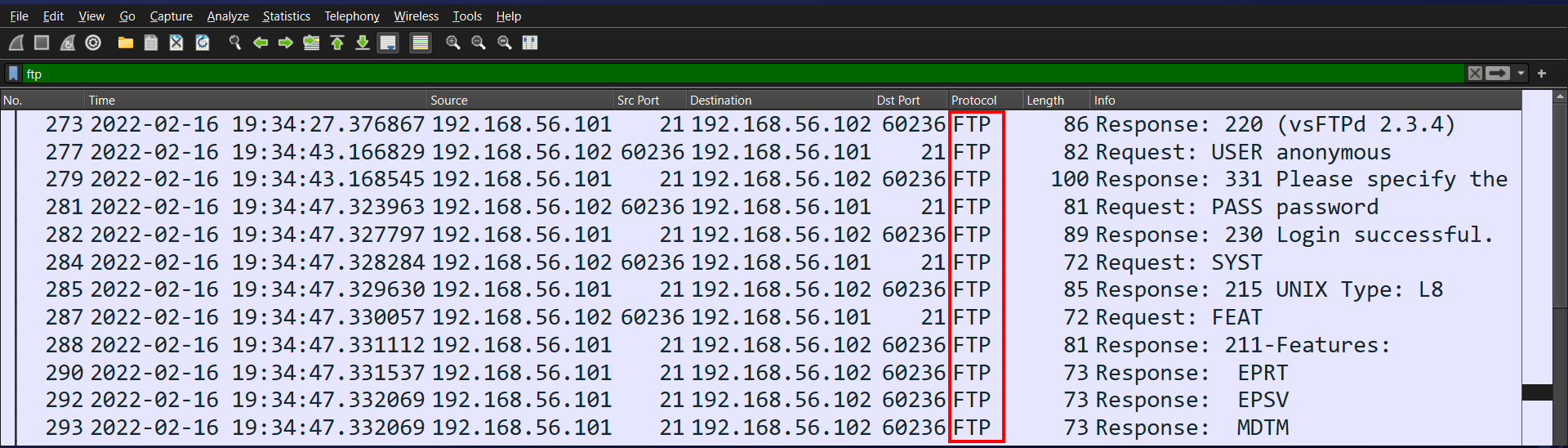
Common Useful Filters

Filter	Function
ip.addr / ip.src / ip.dst	For filtering IP addresses
tcp.port	For filtering port numbers
tcp.port in {80, 10..25}	Filter port 80 & 10-25
contains	Find strings (case sensitive)
matches	Find strings (case insensitive)



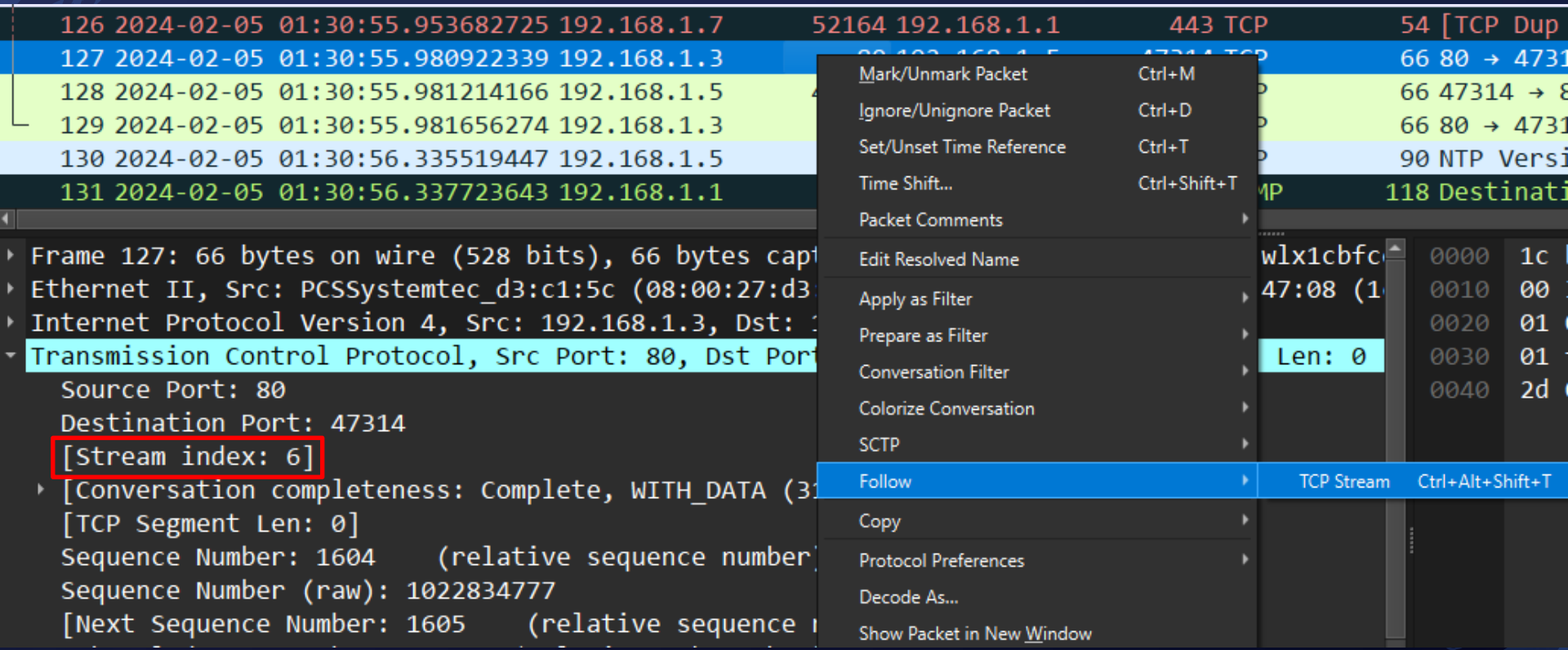
vs


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port==21
No. Time Source Src Port Destination Dst Port Protocol Length Info
272 2022-02-16 19:34:27.374123 192.168.56.102 60236 192.168.56.101 21 TCP 66 60236 → 21 [ACK] Seq=1 Ack=1 Win=
273 2022-02-16 19:34:27.376867 192.168.56.101 21 192.168.56.102 60236 FTP 86 Response: 220 (vsFTPd 2.3.4)
274 2022-02-16 19:34:27.376893 192.168.56.102 60236 192.168.56.101 21 TCP 66 60236 → 21 [ACK] Seq=1 Ack=21 Win
277 2022-02-16 19:34:43.166829 192.168.56.102 60236 192.168.56.101 21 FTP 82 Request: USER anonymous
278 2022-02-16 19:34:43.167740 192.168.56.101 21 192.168.56.102 60236 TCP 66 21 → 60236 [ACK] Seq=21 Ack=17 Wi
279 2022-02-16 19:34:43.168545 192.168.56.101 21 192.168.56.102 60236 FTP 100 Response: 331 Please specify the
280 2022-02-16 19:34:43.168556 192.168.56.102 60236 192.168.56.101 21 TCP 66 60236 → 21 [ACK] Seq=17 Ack=55 Wi
281 2022-02-16 19:34:47.323963 192.168.56.102 60236 192.168.56.101 21 FTP 81 Request: PASS password
282 2022-02-16 19:34:47.327797 192.168.56.101 21 192.168.56.102 60236 FTP 89 Response: 230 Login successful.
283 2022-02-16 19:34:47.327855 192.168.56.102 60236 192.168.56.101 21 TCP 66 60236 → 21 [ACK] Seq=32 Ack=78 Wi
284 2022-02-16 19:34:47.328284 192.168.56.102 60236 192.168.56.101 21 FTP 72 Request: SYST



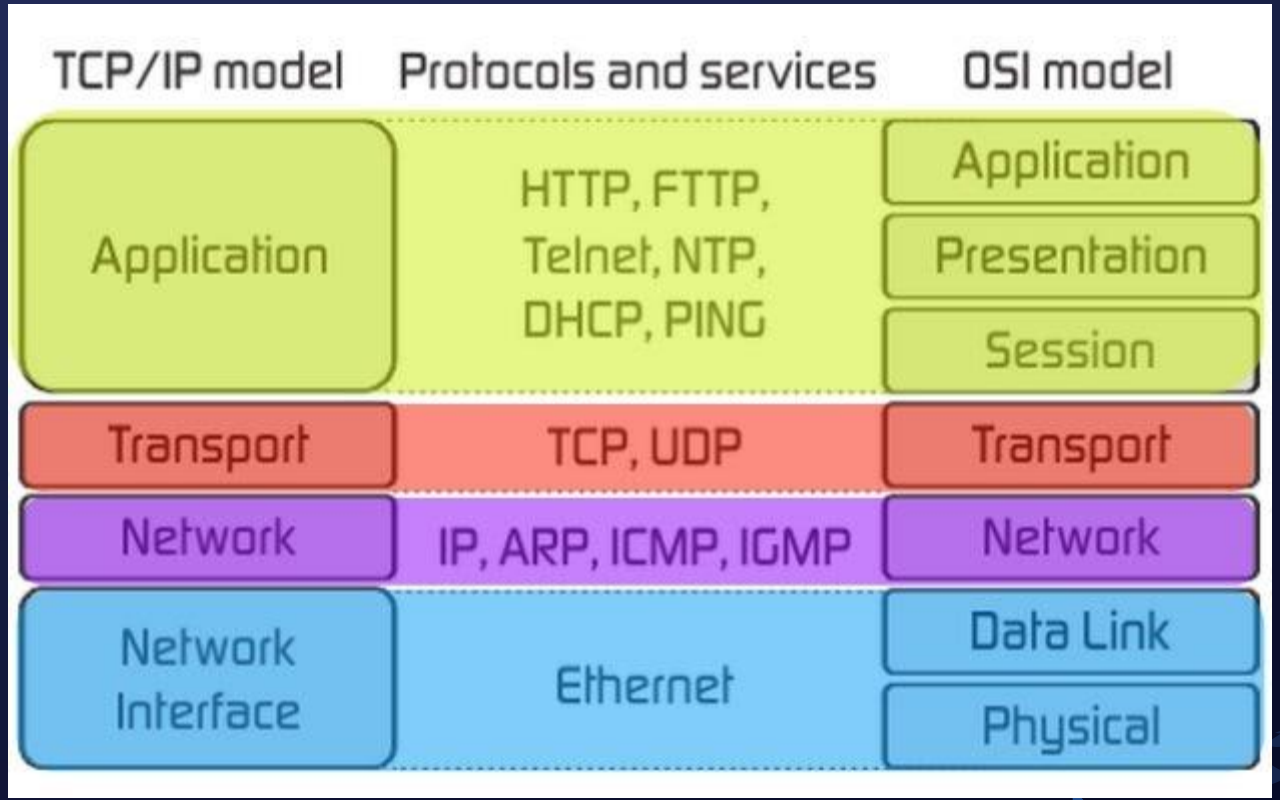
No.	Time	Source	Src Port	Destination	Dst Port	Protocol	Length	Info
273	2022-02-16 19:34:27.376867	192.168.56.101	21	192.168.56.102	60236	FTP	86	Response: 220 (vsFTPd 2.3.4)
277	2022-02-16 19:34:43.166829	192.168.56.102	60236	192.168.56.101	21	FTP	82	Request: USER anonymous
279	2022-02-16 19:34:43.168545	192.168.56.101	21	192.168.56.102	60236	FTP	100	Response: 331 Please specify the
281	2022-02-16 19:34:47.323963	192.168.56.102	60236	192.168.56.101	21	FTP	81	Request: PASS password
282	2022-02-16 19:34:47.327797	192.168.56.101	21	192.168.56.102	60236	FTP	89	Response: 230 Login successful.
284	2022-02-16 19:34:47.328284	192.168.56.102	60236	192.168.56.101	21	FTP	72	Request: SYST
285	2022-02-16 19:34:47.329630	192.168.56.101	21	192.168.56.102	60236	FTP	85	Response: 215 UNIX Type: L8
287	2022-02-16 19:34:47.330057	192.168.56.102	60236	192.168.56.101	21	FTP	72	Request: FEAT
288	2022-02-16 19:34:47.331112	192.168.56.101	21	192.168.56.102	60236	FTP	81	Response: 211-Features:
290	2022-02-16 19:34:47.331537	192.168.56.101	21	192.168.56.102	60236	FTP	73	Response: EPRT
292	2022-02-16 19:34:47.332069	192.168.56.101	21	192.168.56.102	60236	FTP	73	Response: EPSV
293	2022-02-16 19:34:47.332069	192.168.56.101	21	192.168.56.102	60236	FTP	73	Response: MDTM

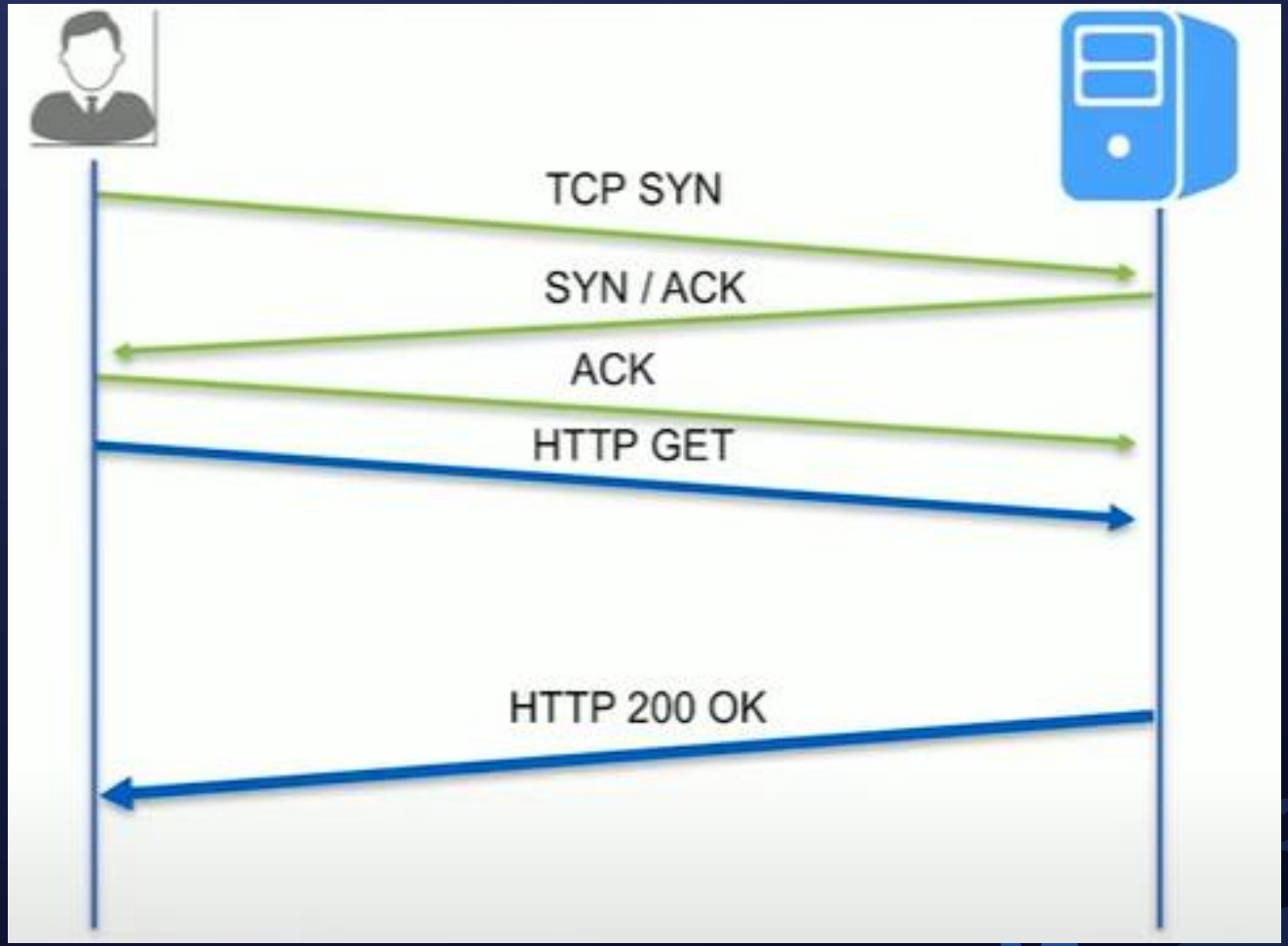
Stream Index



03 Port Scanning

Where you need networking knowledge

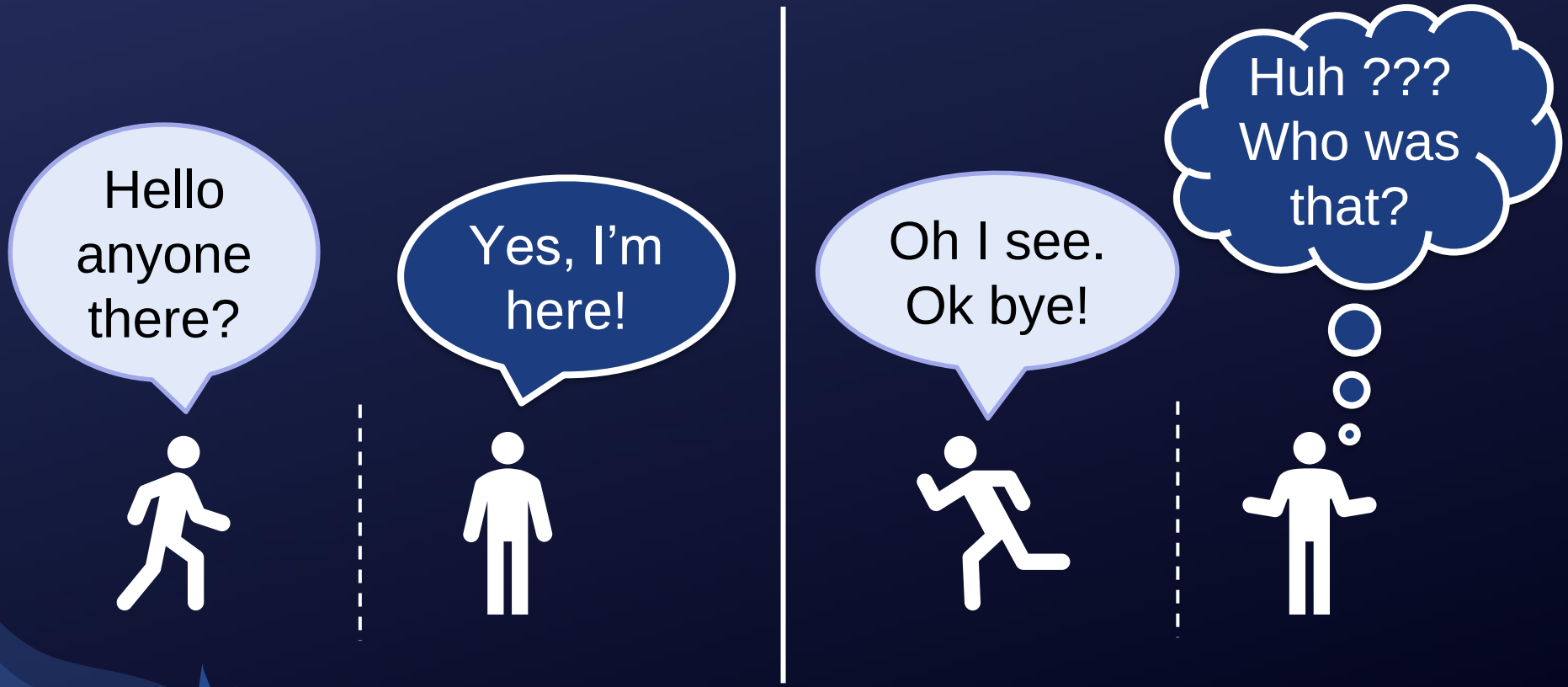

TCP/IP model
Protocols and services
OSI model
Application
HTTP, FTTP, Telnet, NTP, DHCP, PING
Application
Presentation
Session
Transport
TCP, UDP
Transport
Network
IP, ARP, ICMP, IGMP
Network
Network Interface
Ethernet
Data Link
Physical


TCP SYN
SYN / ACK
ACK
HTTP GET
HTTP 200 OK

Common Nmap Scans

- Stealth scan (half-open scan / SYN scan)
- Connect scan (full scan)

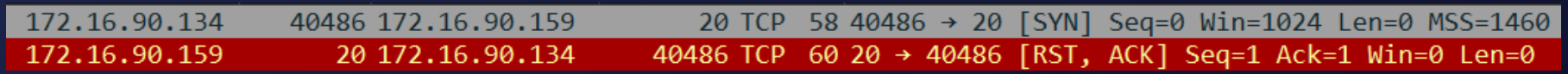
Stealth Scan (-sS) – Open Port



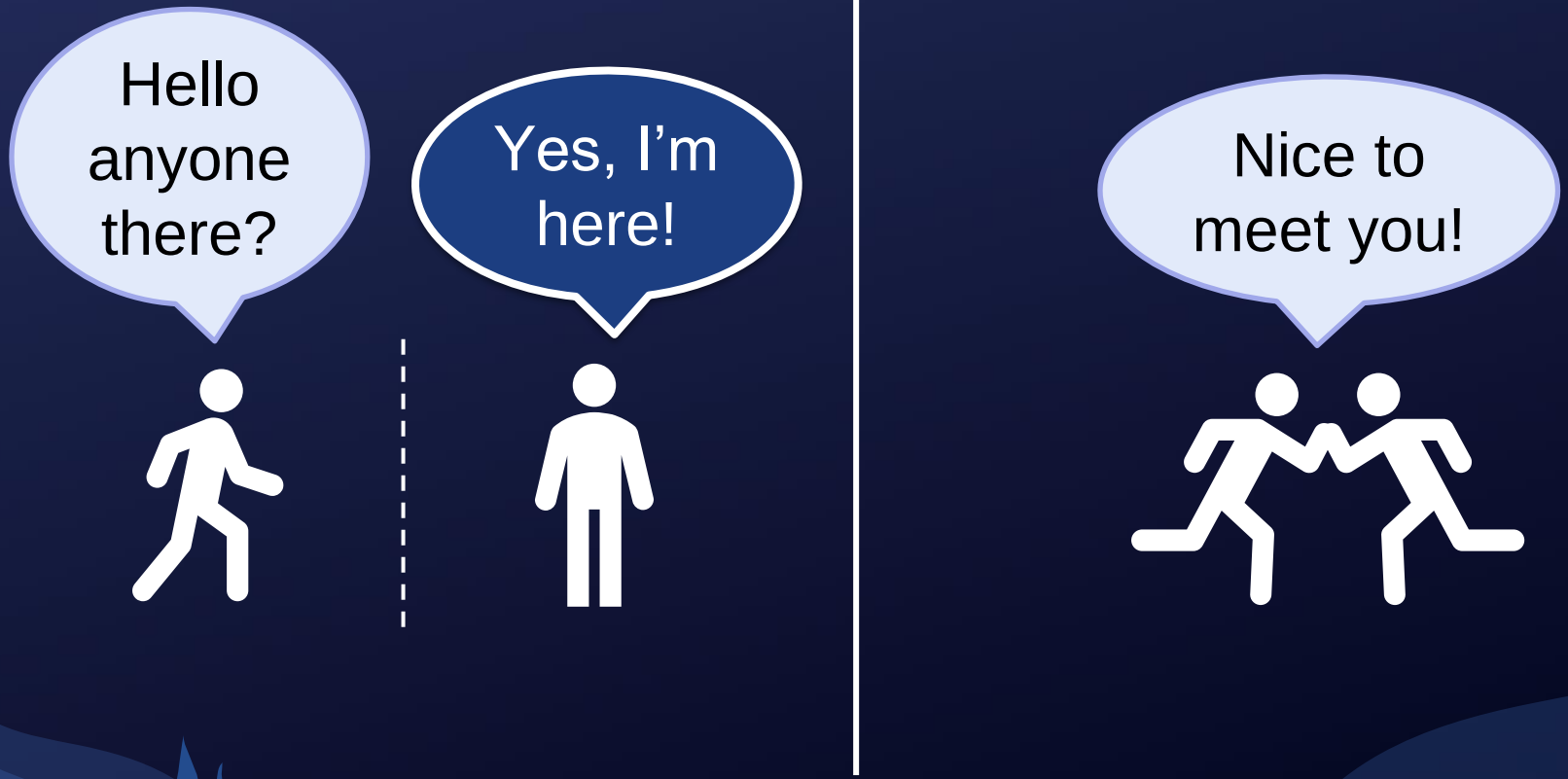
Stealth Scan (Opened Port)

172.16.90.134	40486	172.16.90.159	80	TCP	58 40486 → 80 [SYN] Seq=0 Win=1024 Len=
172.16.90.159	80	172.16.90.134	40486	TCP	60 80 → 40486 [SYN, ACK] Seq=0 Ack=1 Wi
172.16.90.134	40486	172.16.90.159	80	TCP	54 40486 → 80 [RST] Seq=1 Win=0 Len=0

Stealth Scan (Closed Port)



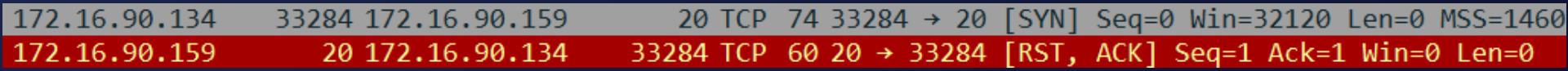
Connect Scan (-sT) – Open Port



Connect Scan (Open Port)

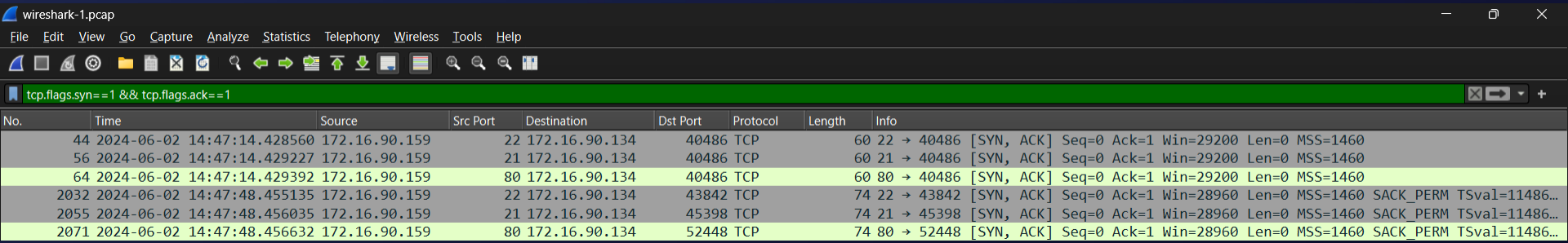
172.16.90.134	52448	172.16.90.159	80	TCP	74 52448 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=146
172.16.90.159	80	172.16.90.134	52448	TCP	74 80 → 52448 [SYN, ACK] Seq=0 Ack=1 Win=28960 Le
172.16.90.134	52448	172.16.90.159	80	TCP	66 52448 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 T
172.16.90.134	52448	172.16.90.159	80	TCP	66 52448 → 80 [RST, ACK] Seq=1 Ack=1 Win=32128 Le

Connect Scan (Closed Port)



How to Filter for Open Port

```
ip.src == <source_ip_add> && ip.dst == <dest_ip_add> &&
tcp.flags.syn==1 && tcp.flags.ack==1
```



TCP Completeness = 39 → Possible Connect Scan

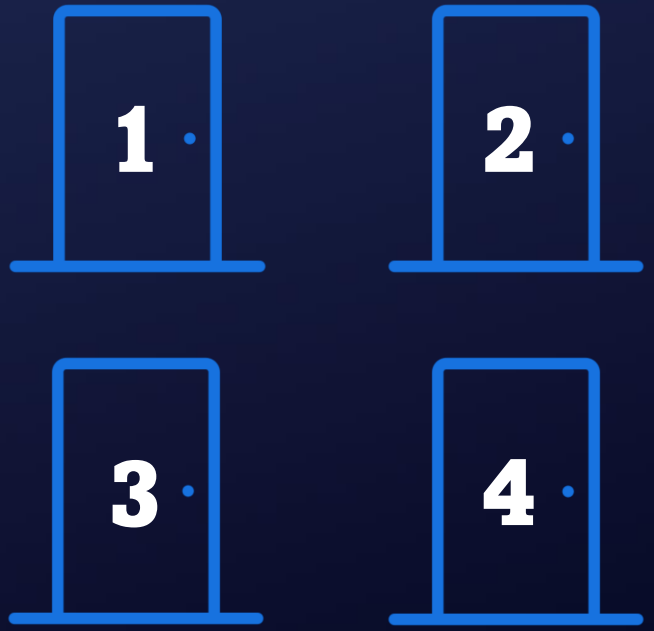
04 Capstone Challenge

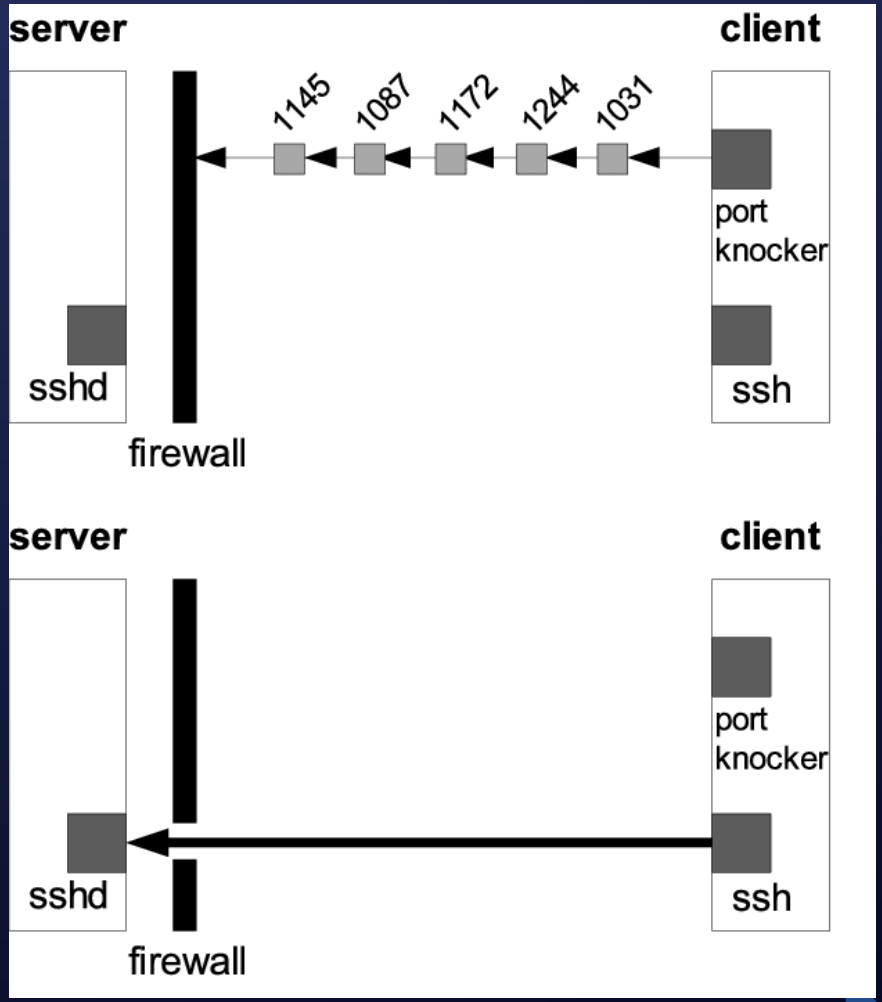
Where you apply your knowledge

Question

- Identify the open port(s)
- Identify the port knocking sequence

Port Knocking




server
client
1145
1087
1172
1244
1031
port
knocker
sshd
ssh
firewall
server
client
port
knocker
sshd
ssh
firewall

Answer

- Port 5000
  - `tcp.flags.syn==1 && tcp.flags.ack==1`
- 17613 22791 20882 51313
  - `tcp.flags.syn==1`

https://tinyurl.com/cslu2-wireshark