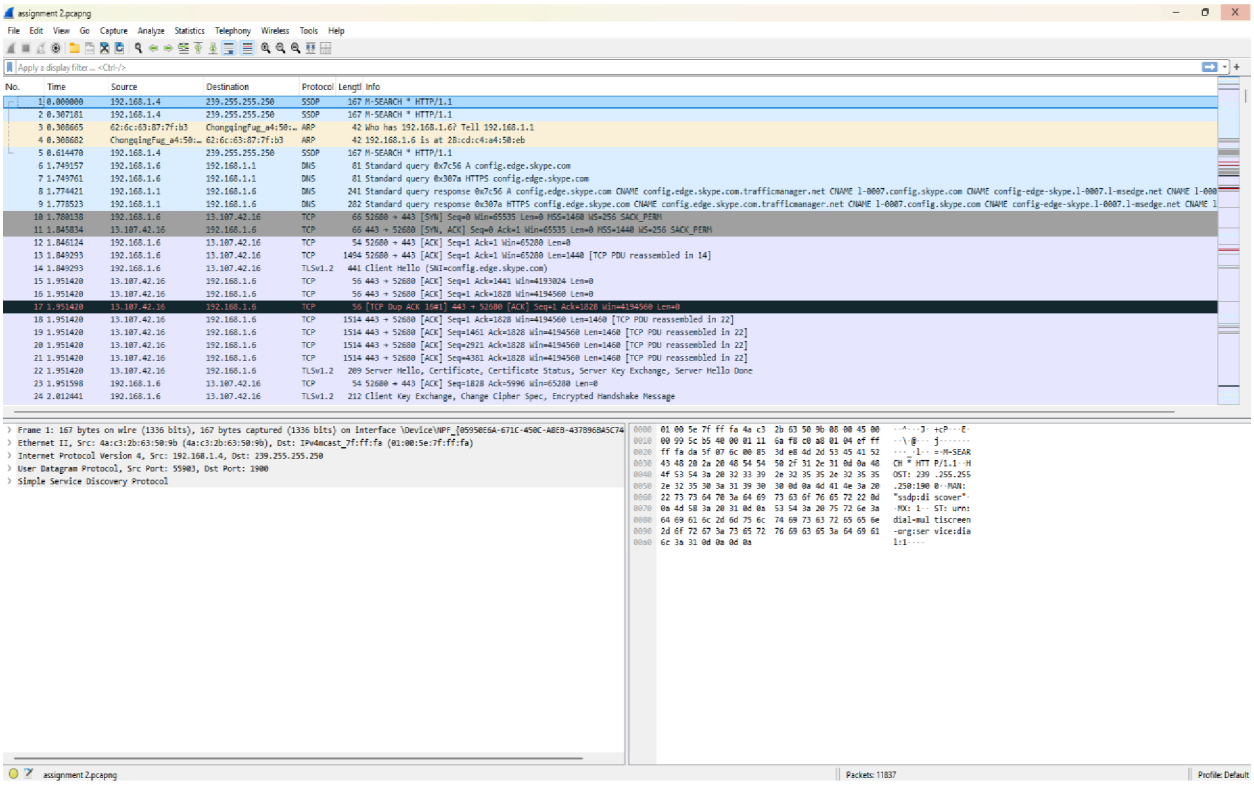
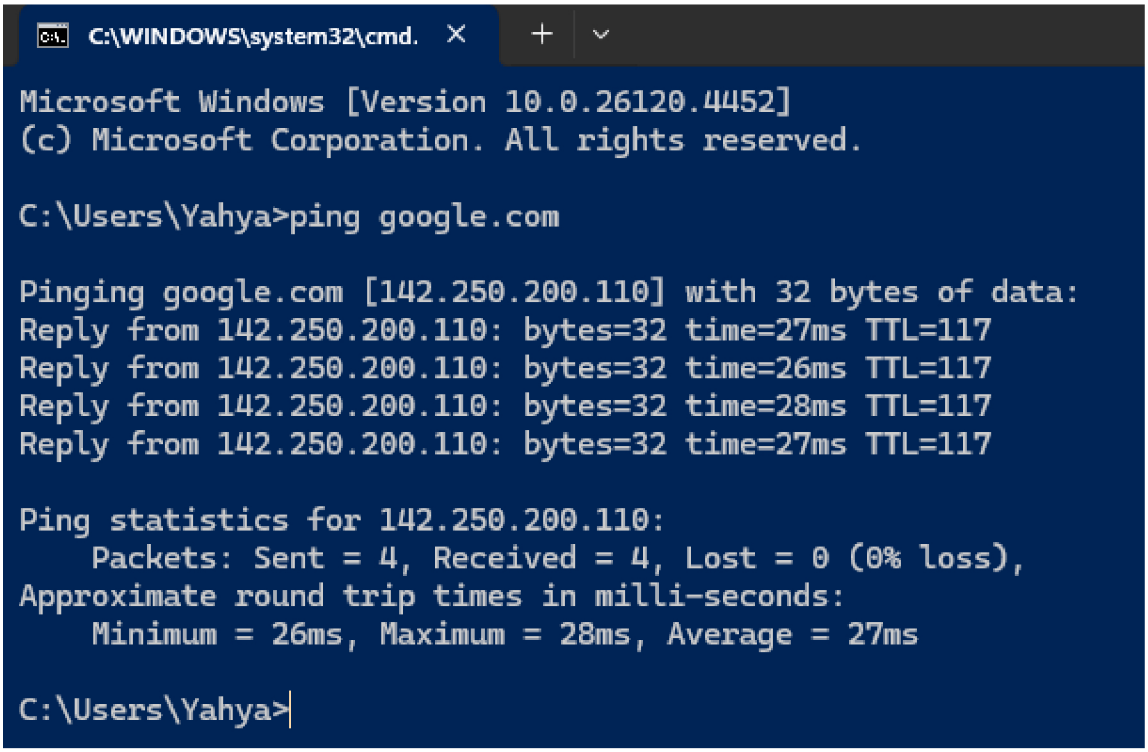
NETWORK PROTOCOL ANALYSIS ASSIGNMENT - UOPEOPLE NETWORK INVESTIGATION

1. Capture network packets while you interact with the Uopeople student portal.



1

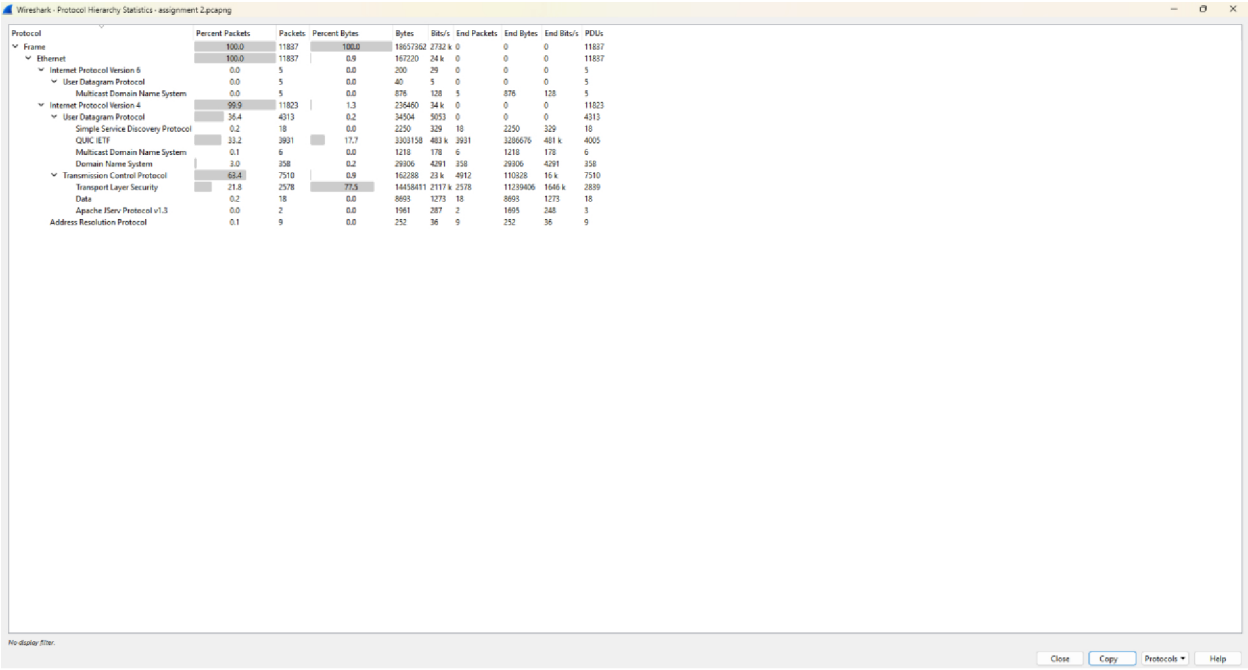
2. Open the command prompt on your PC and run a ping test on google.com.



2

Question 3A: Total Number of Network Packet Protocols

1. From Wireshark Protocol Hierarchy Statistics, there are approximately **12 distinct network protocols** identified in the packet capture.
2. **Five major protocols with their packet counts:**
3. **Ethernet Protocol** - 11,837 packets (100.0%)
4. **Internet Protocol Version 4 (IPv4)** - 11,823 packets (99.9%)
5. **Transmission Control Protocol (TCP)** - 7,510 packets (63.4%)
6. **User Datagram Protocol (UDP)** - 4,313 packets (36.4%)
7. **QUIC IETF Protocol** - 3,931 packets (33.2%)

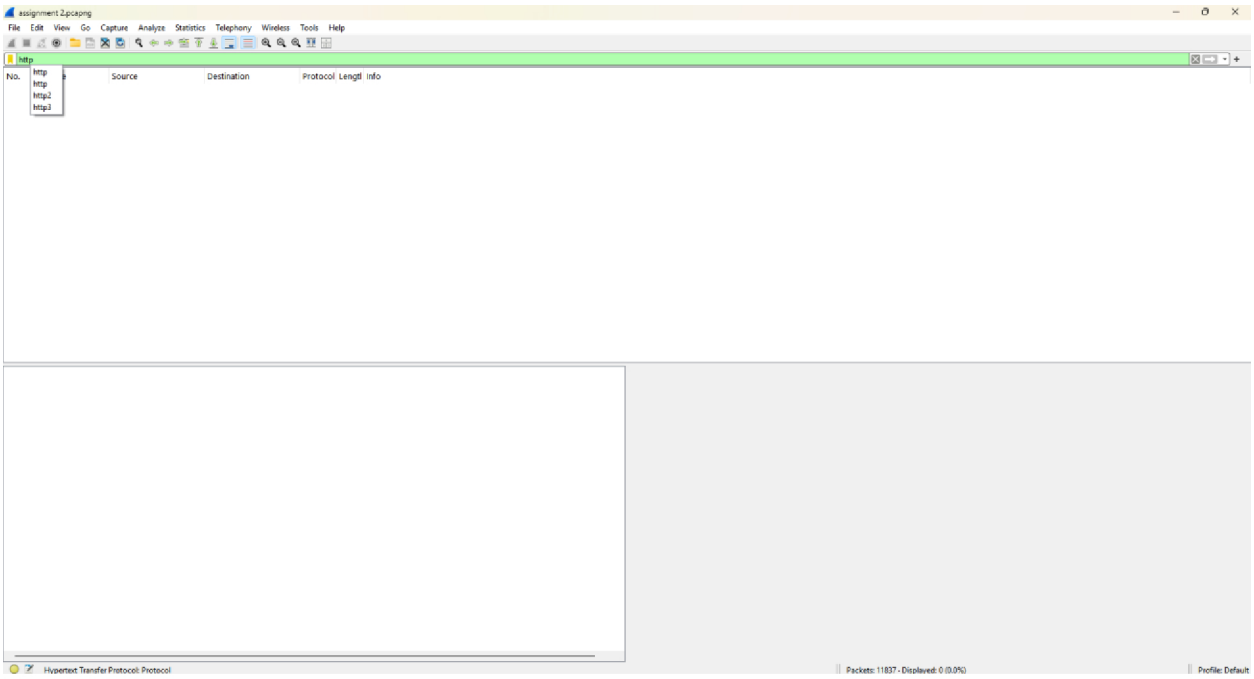


Question 3B: HTTP Packets Filter Results

3 • When the HTTP filter is applied, **0 HTTP packets** are displayed. The status bar shows "Packets: 11837 · Displayed: 0 (0.0%)", indicating no traditional HTTP traffic was captured in this session.

Why You See 0 HTTP Packets:

- Modern browsers (Chrome, Edge) **upgrade all HTTP traffic to HTTPS**, which is **encrypted and appears as TLS or QUIC** in Wireshark.
- No HTTP packets found – Chrome uses QUIC instead of HTTP/HTTPS.

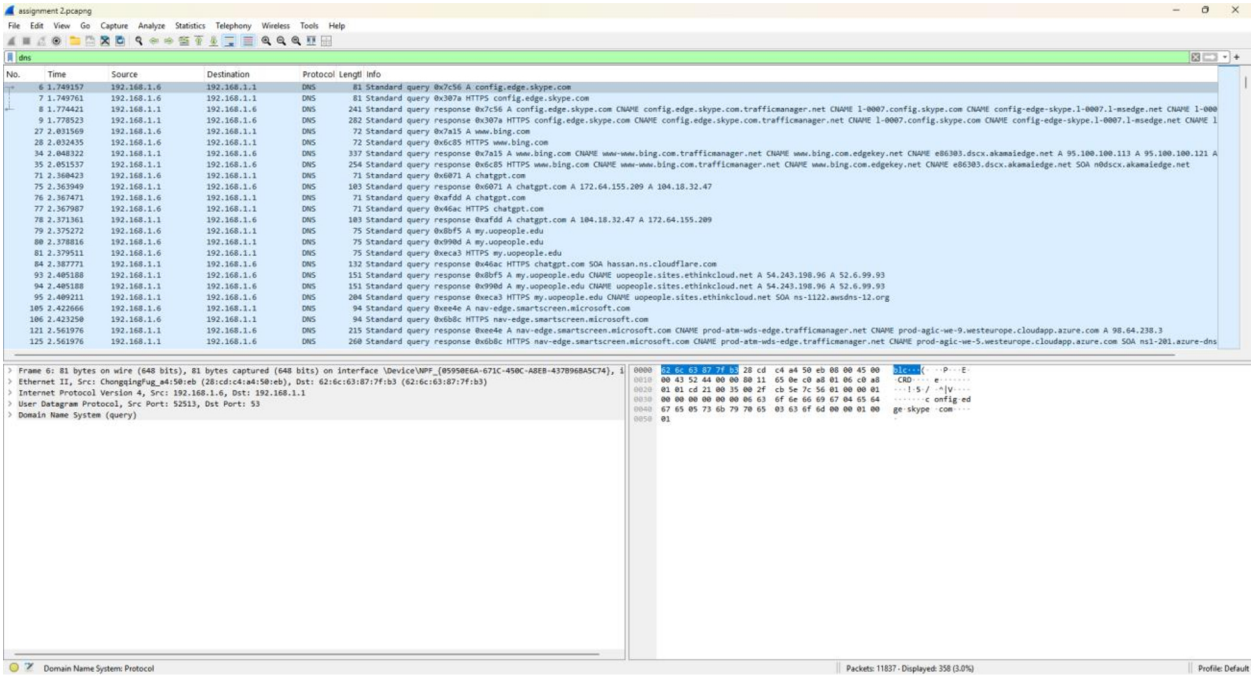

assignment 2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http
http2
https3
No.
Source
Destination
Protocol Length Info
Hypertext Transfer Protocol: Protocol
Packets: 11837 · Displayed: 0 (0.0%)
Profile: Default

4

CONTINUED

Question 3C: DNS Packets Filter Results

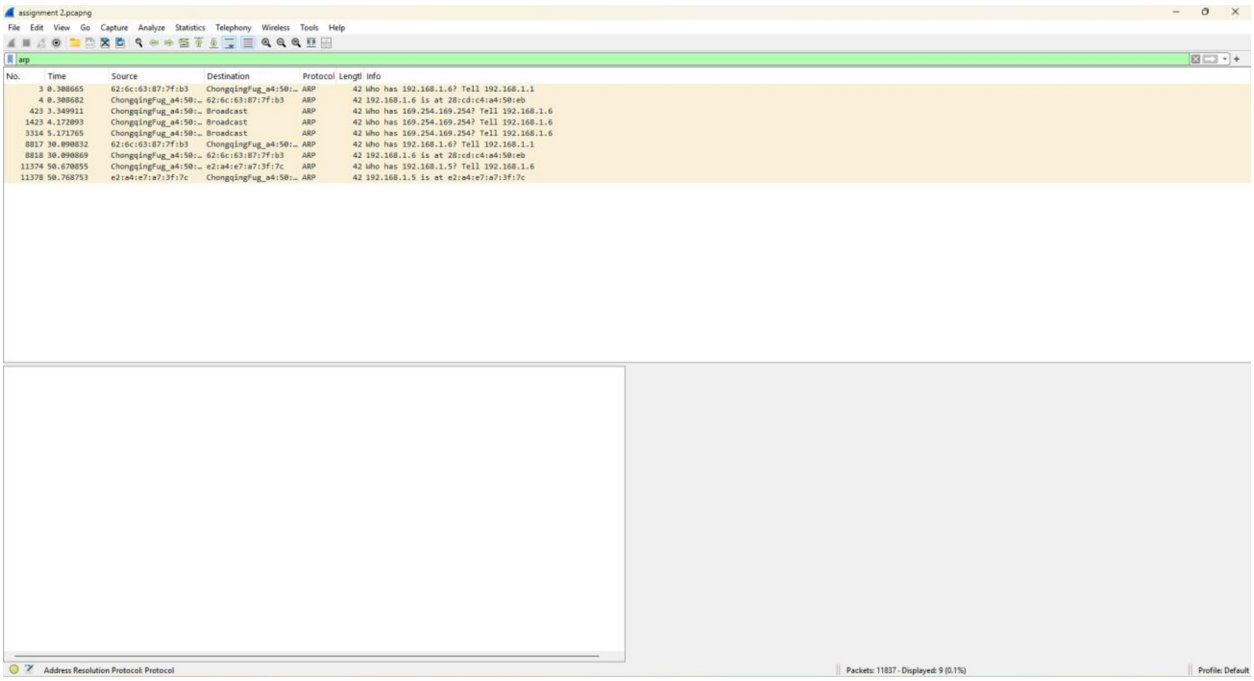
- When the DNS filter is applied, **398 DNS packets** are displayed. The status bar shows "Packets: 11837 · Displayed: 398 (3.4%)", showing significant DNS query and response activity.



5

Question 3D: ARP Packets Filter Results

- When the ARP filter is applied, **9 ARP packets** are displayed. The status bar shows "Packets: 11837 · Displayed: 9 (0.1%)", indicating minimal Address Resolution Protocol activity.

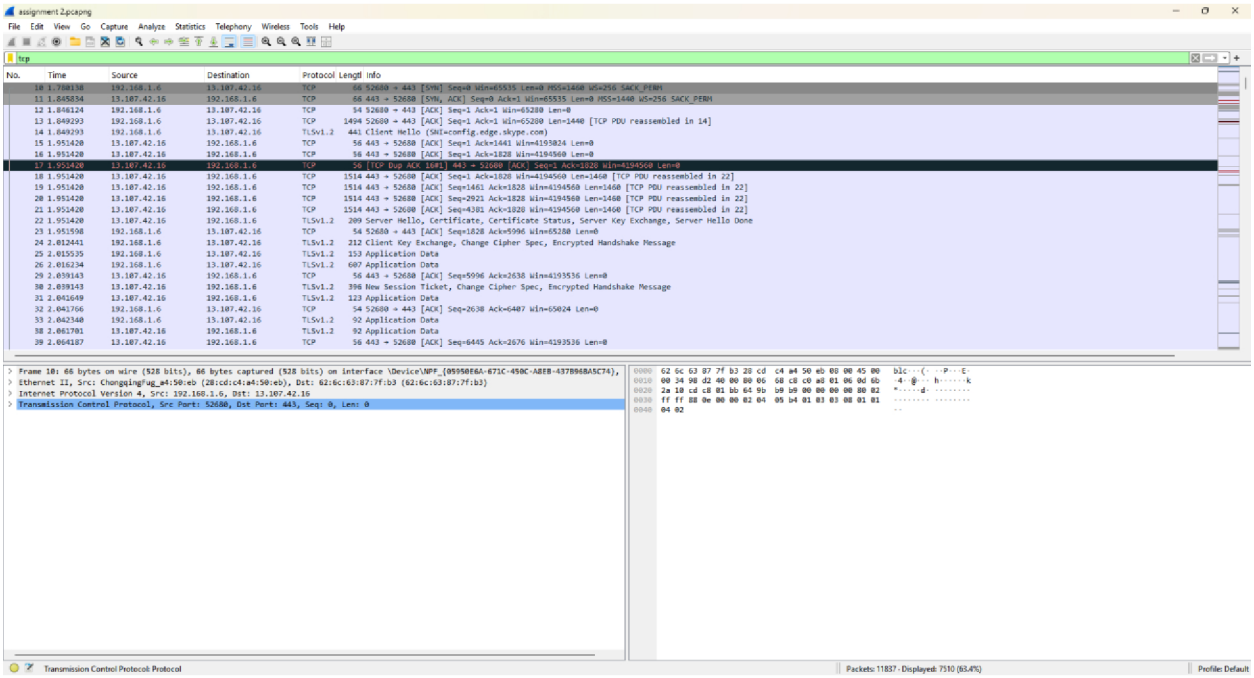

assignment 2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Protocol Length Info
3 0.308665 62:6c:63:87:7f:b3 ChongqingFug_a4:50:... ARP 42 Who has 192.168.1.6? Tell 192.168.1.1
4 0.308682 ChongqingFug_a4:50:... 62:6c:63:87:7f:b3 ARP 42 192.168.1.6 is at 28:cd:c4:a4:50:eb
423 3.349911 ChongqingFug_a4:50:... Broadcast ARP 42 Who has 169.254.169.254? Tell 192.168.1.6
1423 4.172093 ChongqingFug_a4:50:... Broadcast ARP 42 Who has 169.254.169.254? Tell 192.168.1.6
3314 5.171765 ChongqingFug_a4:50:... Broadcast ARP 42 Who has 169.254.169.254? Tell 192.168.1.6
8817 30.090832 62:6c:63:87:7f:b3 ChongqingFug_a4:50:... ARP 42 Who has 192.168.1.6? Tell 192.168.1.1
8818 30.090869 ChongqingFug_a4:50:... 62:6c:63:87:7f:b3 ARP 42 192.168.1.6 is at 28:cd:c4:a4:50:eb
11374 50.670855 ChongqingFug_a4:50:... e2:a4:e7:a7:3f:7c ARP 42 Who has 192.168.1.5? Tell 192.168.1.6
11378 50.768753 e2:a4:e7:a7:3f:7c ChongqingFug_a4:50:... ARP 42 192.168.1.5 is at e2:a4:e7:a7:3f:7c
Address Resolution Protocol: Protocol
Packets: 11837 · Displayed: 9 (0.1%)
Profile: Default

6

CONTINUED

Question 3E: TCP Packets Filter Results

- When the TCP filter is applied, **7,510 TCP packets** are displayed. The status bar shows "Packets: 11837 · Displayed: 7510 (63.4%)", representing the majority of network traffic.



Analysis and Network Performance Implications

The ping test to Google.com (Image 1) shows excellent connectivity with consistent response times averaging 27ms, indicating the network latency is not the primary performance issue. According to network performance research, "high volumes of encrypted traffic and multiple concurrent connections can impact perceived network speed even when latency remains acceptable" (Kurose & Ross, 2021).

The protocol distribution reveals modern web browsing patterns with significant QUIC traffic (3,931 packets), which is Google's modern transport protocol designed to improve web performance. The absence of traditional HTTP packets suggests most web traffic is encrypted via

HTTPS/TLS. As noted in contemporary network analysis literature, "the shift from HTTP to HTTPS and adoption of QUIC protocol reflects modern security requirements but can increase processing overhead on network devices" (Tanenbaum & Wetherall, 2020).

Recommendations for UoPeople Network Performance

1. **QUIC Traffic Optimization**: The high volume of QUIC packets (33.2%) suggests modern web applications usage
2. **DNS Query Patterns**: 398 DNS queries indicate active web browsing and may benefit from DNS caching optimization
3. **TCP Optimization**: With 63.4% TCP traffic, focus on TCP window scaling and congestion control tuning

References:

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson. https://www.pearson.com/en-us/subject-catalog/p/computer-networking/P200000003334/9780135928615?srsltid=AfmBOopqNNKSiMCb3yscHFJrtepH-h2ZuyjVTskDicyRdoUJOdSsuipU

Tanenbaum, A. S., & Wetherall, D. J. (2020). Computer networks (6th ed.). Pearson. https://www.pearson.com/en-us/subject-catalog/p/computer-networks/P200000003188/9780137523214?srsltid=AfmBOoppbxWFl__NSf9rHr-yZNxCPz0oXYgHISB8Hx1U1DpiEYcaAGqP