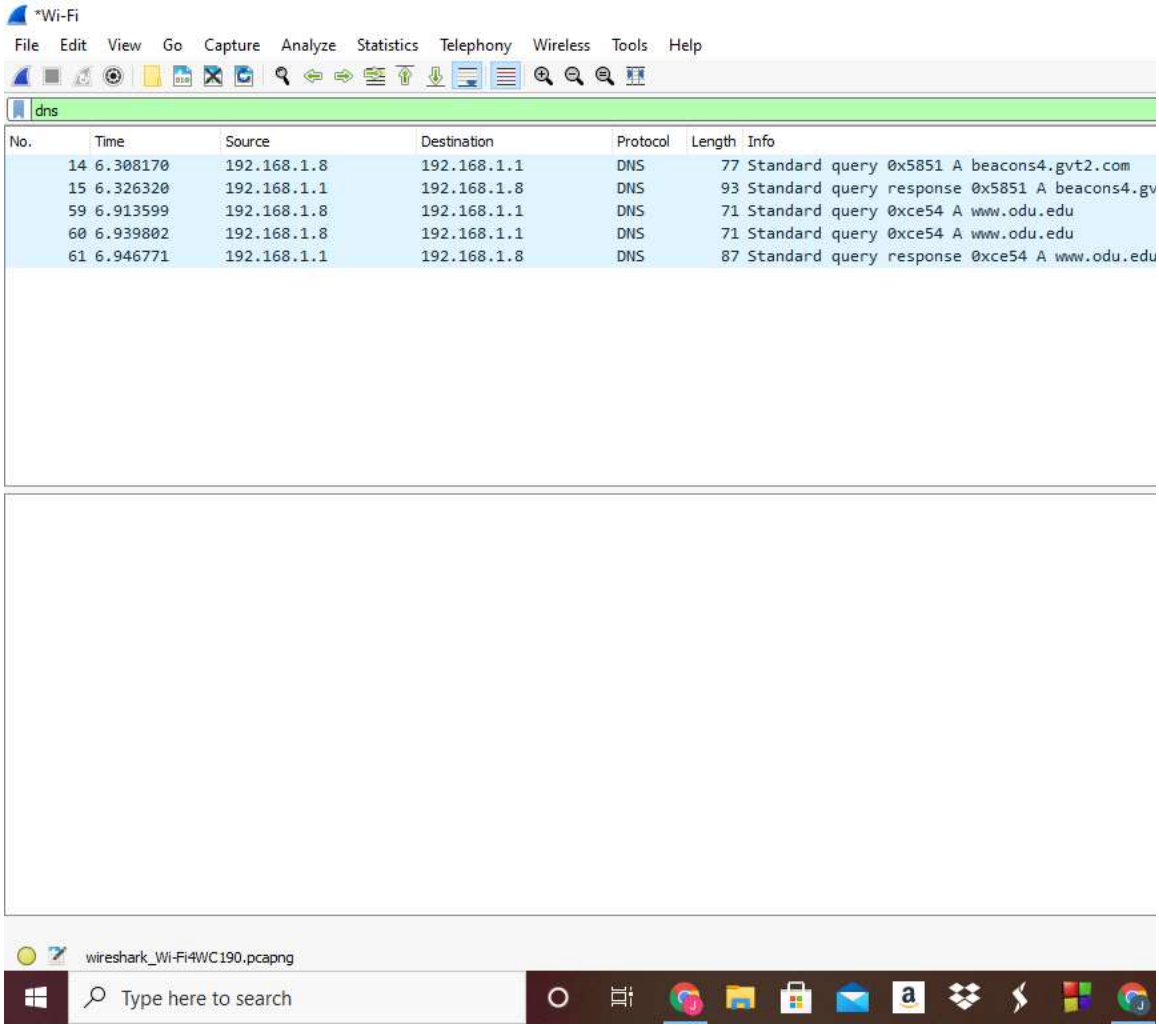
Old Dominion University

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment 1.2: Basic Wireshark Practice

Jordan Sustarsic

- Use Wireshark to capture and save ALL related packets when you ping the URL "www.odu.edu".
    - Locate the DNS queries and responses in the traffic.



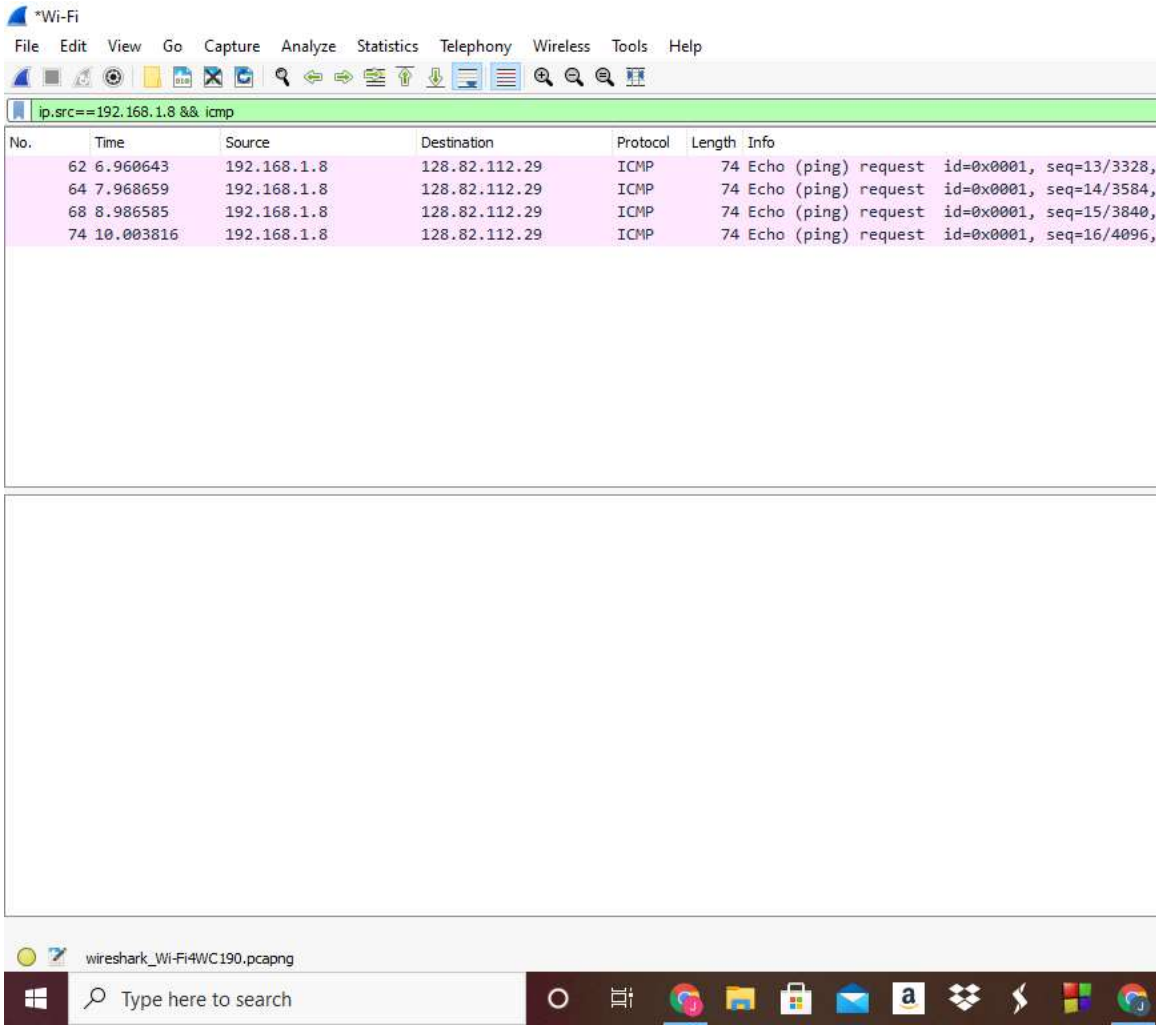
- What is the IP address of the DNS server?

  The IP address of the server is: 192.168.1.1

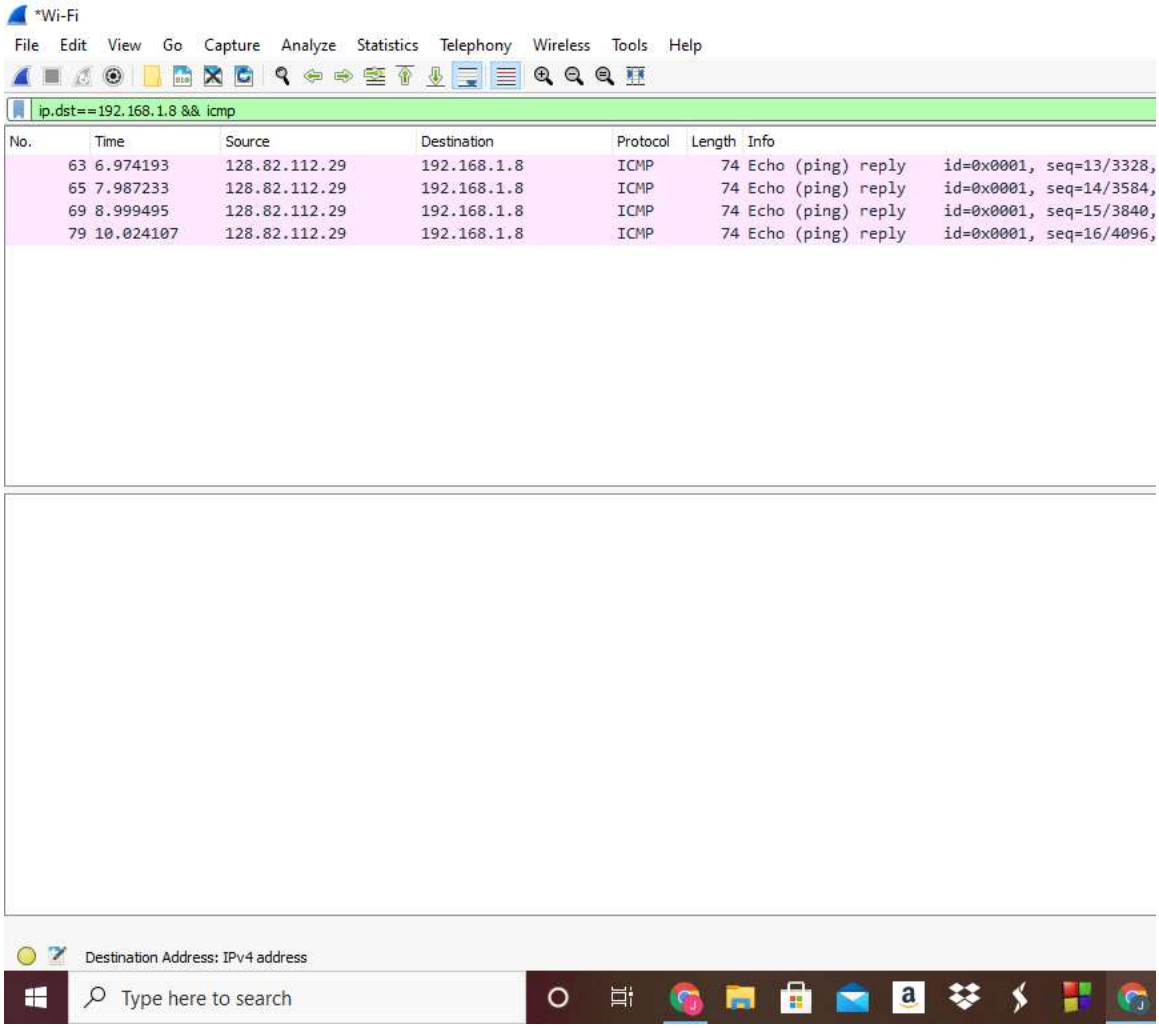
- What information is answered from the DNS server?

  It gives us the host name's associated IP address

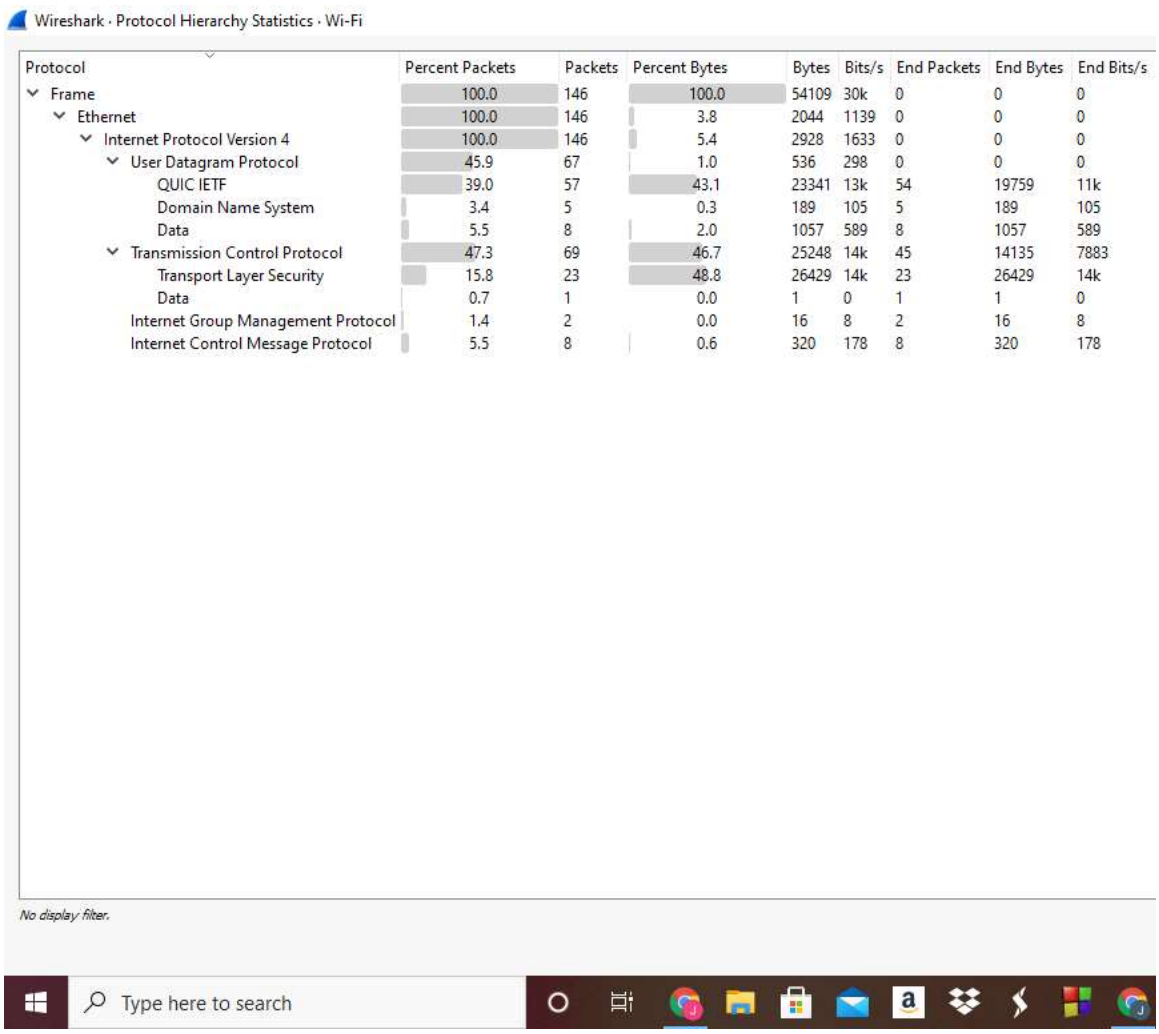
- Apply the proper display filter in Wireshark to show ICMP requests.



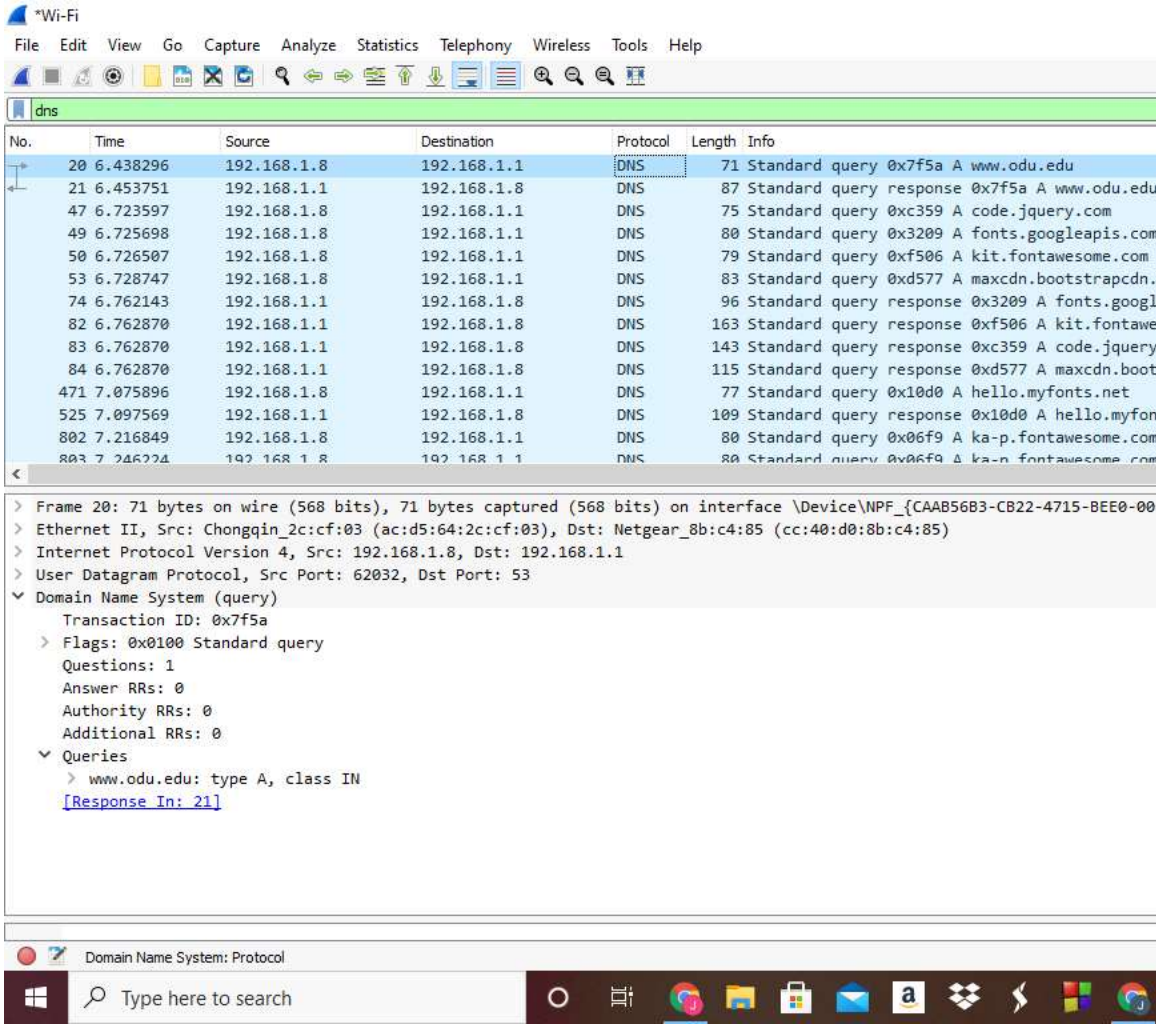
- Apply the proper display filter in Wireshark to show ICMP responses.



- Show the Protocol Hierarchy Statistics of the traffic.


Wireshark · Protocol Hierarchy Statistics · Wi-Fi
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
End Bytes
End Bits/s
Frame 100.0 146 100.0 54109 30k 0 0 0
Ethernet 100.0 146 3.8 2044 1139 0 0 0
Internet Protocol Version 4 100.0 146 5.4 2928 1633 0 0 0
User Datagram Protocol 45.9 67 1.0 536 298 0 0 0
QUIC IETF 39.0 57 43.1 23341 13k 54 19759 11k
Domain Name System 3.4 5 0.3 189 105 5 189 105
Data 5.5 8 2.0 1057 589 8 1057 589
Transmission Control Protocol 47.3 69 46.7 25248 14k 45 14135 7883
Transport Layer Security 15.8 23 48.8 26429 14k 23 26429 14k
Data 0.7 1 0.0 1 0 1 1 0
Internet Group Management Protocol 1.4 2 0.0 16 8 2 16 8
Internet Control Message Protocol 5.5 8 0.6 320 178 8 320 178
No display filter.
Type here to search

- Use Wireshark to capture and save ALL related packets when you visit the URL www.odu.edu in a new Incognito window. Stop capturing after the ODU website is fully loaded.
    - Locate all DNS queries and responses after you open the website and highlight the DNS query for the ODU website.



- How many other DNS queries have been captured after the ODU website is

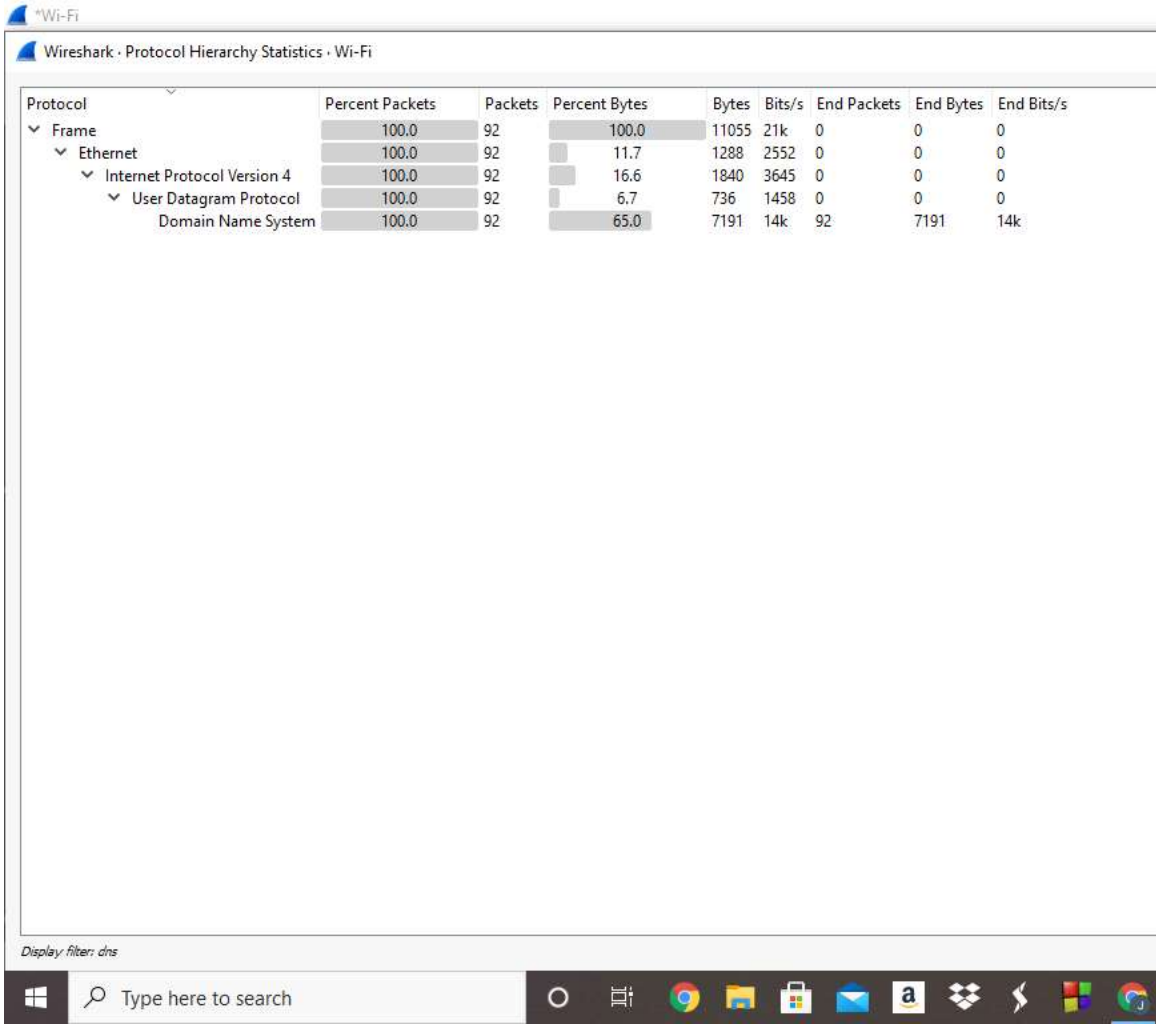
loaded? Can you explain why this happens?

Too many other packets have been captured to count. I believe this happens due to all the other stuff linked to the odu site: ads, widgets, external links, etc….

- Combine what you have observed in the previous questions. Can you identify the widgets (external links) loaded on the ODU website?

  Any of the social media capture would be since there are links to them on the main website: facebook, twitter, youtube, etc…

- Show the Protocol Hierarchy Statistics of the traffic.



- Study two Protocol Hierarchy Statistics in Task 1. f and Task 2.d, respectively. Explain the main differences between the two types of traffic.

  When we pinged www.odu.edu there were less packets in the "User Datagram Protocol" than when we visited the site, so the DNS server was being used more when we visited the site due to all the external links connected to the website.

  Also when we pinged the site in part 1, there was use of the "Transmission Control Protocol" as opposed to part two which did not include that at all. This means when we pinged the website we were trying to communicate with it and send messages over the network.