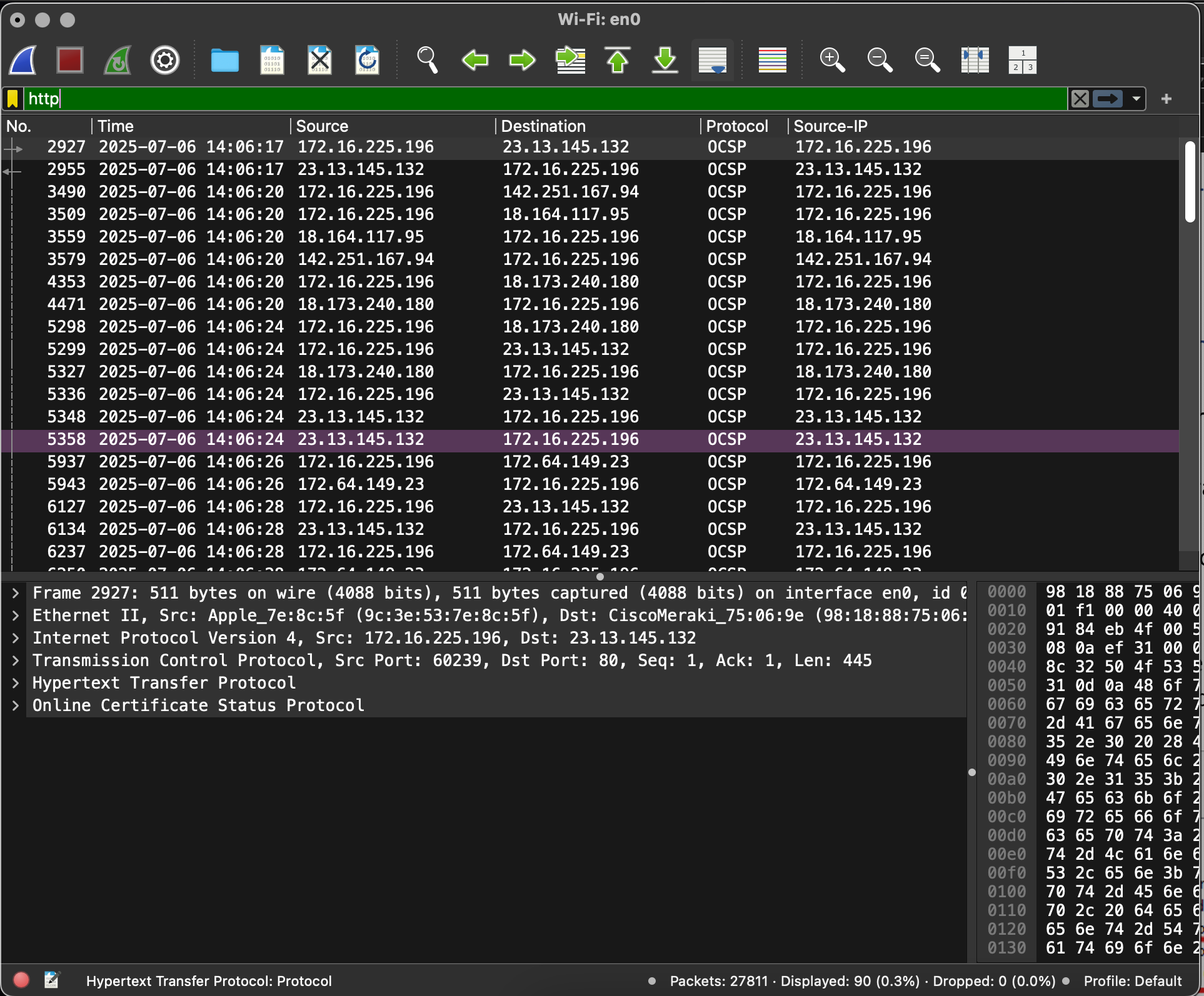
William Fan

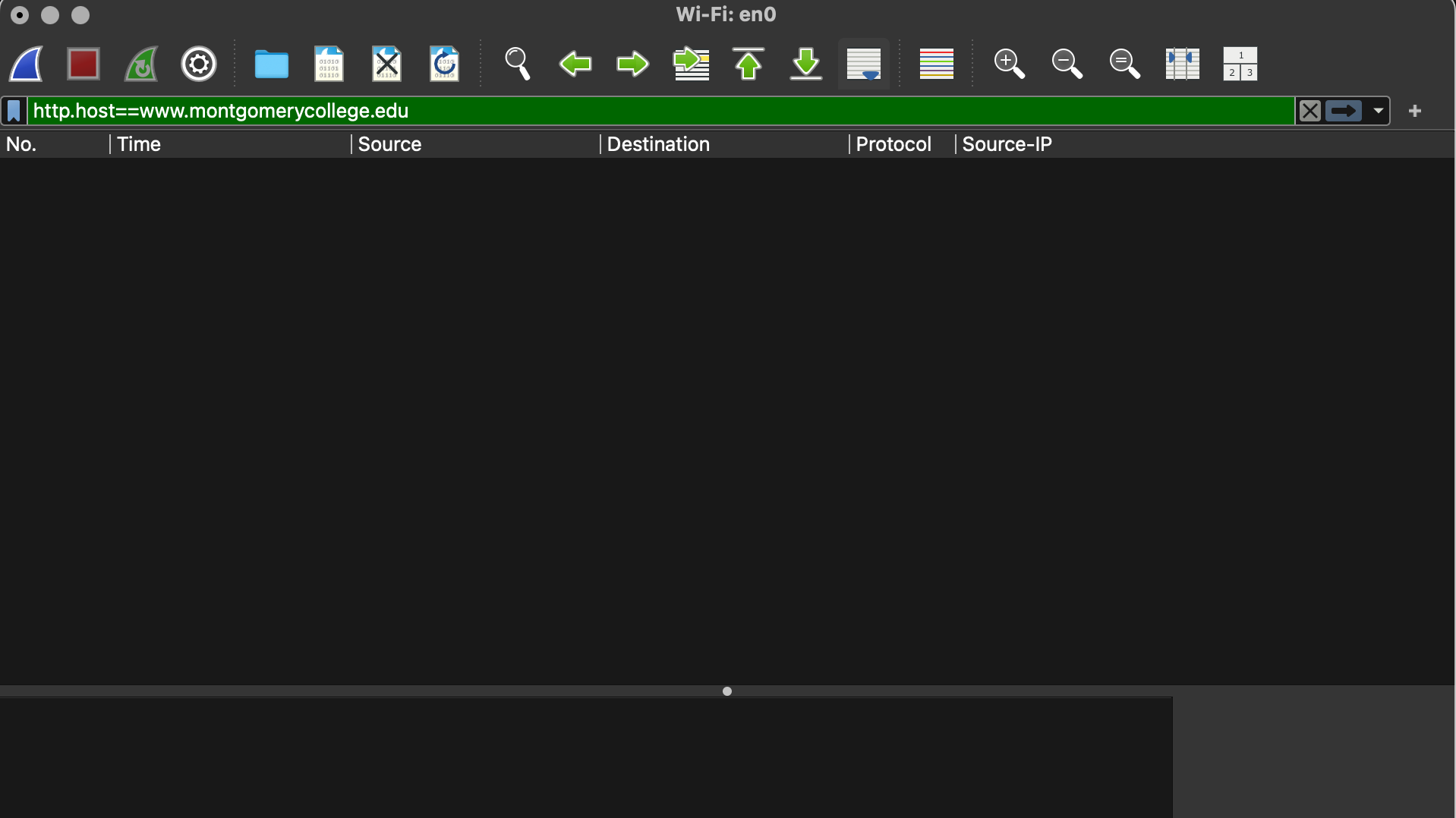
Jul 6th 2025

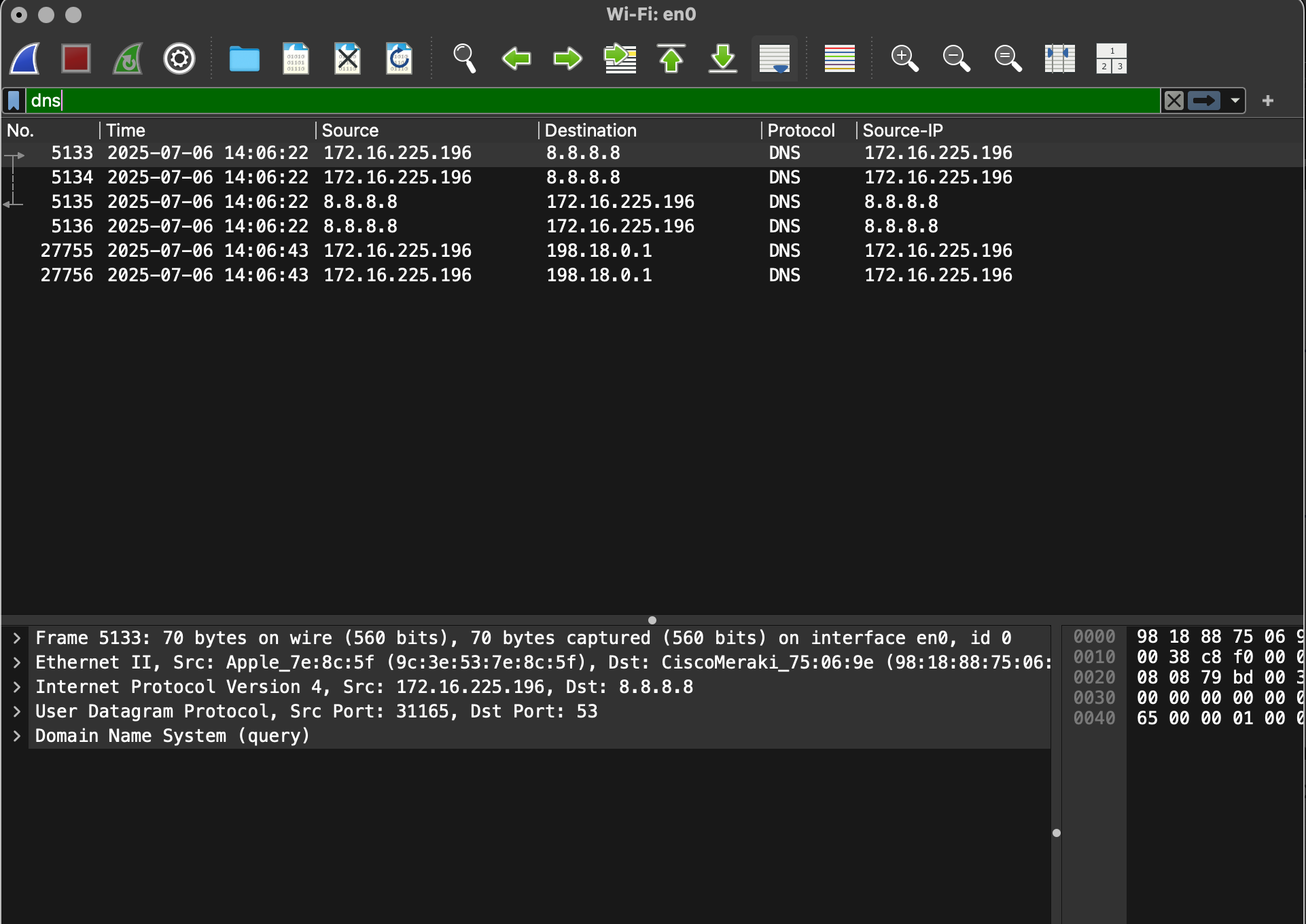
NWIT 245

Lab 2- Traffic Signature Analysis with Wireshark Lab Report

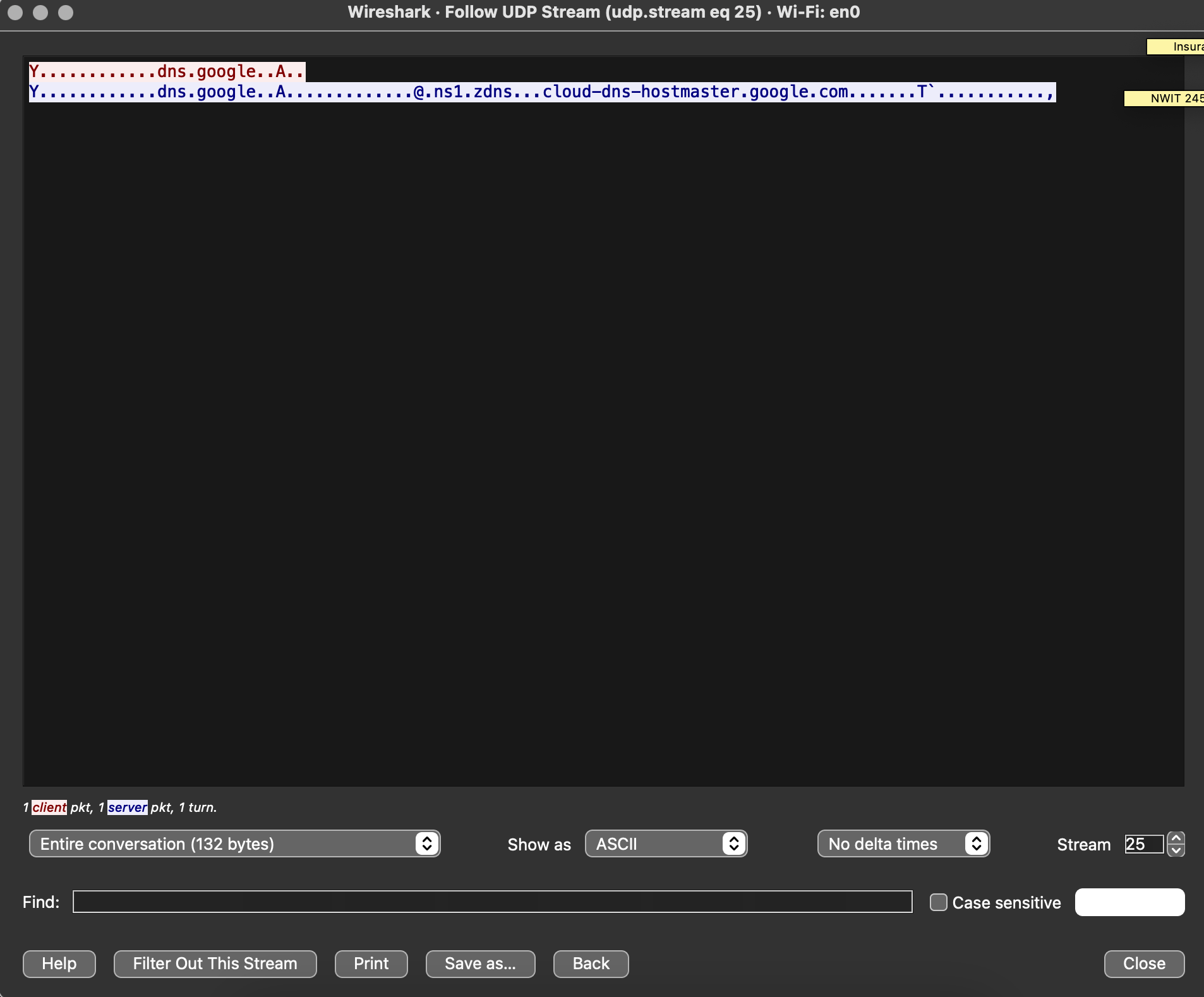
Screenshot 1: Displays network traffic filtered by http.request, which lists only outgoing HTTP requests. This confirms that the HTTP filter is working correctly.

Screenshot 2: It displays the packet details pane showing HTTP host information, uses of http.host == www.montgomerycollege.edu filter. This tests whether specific traffic can be isolated and viewed.

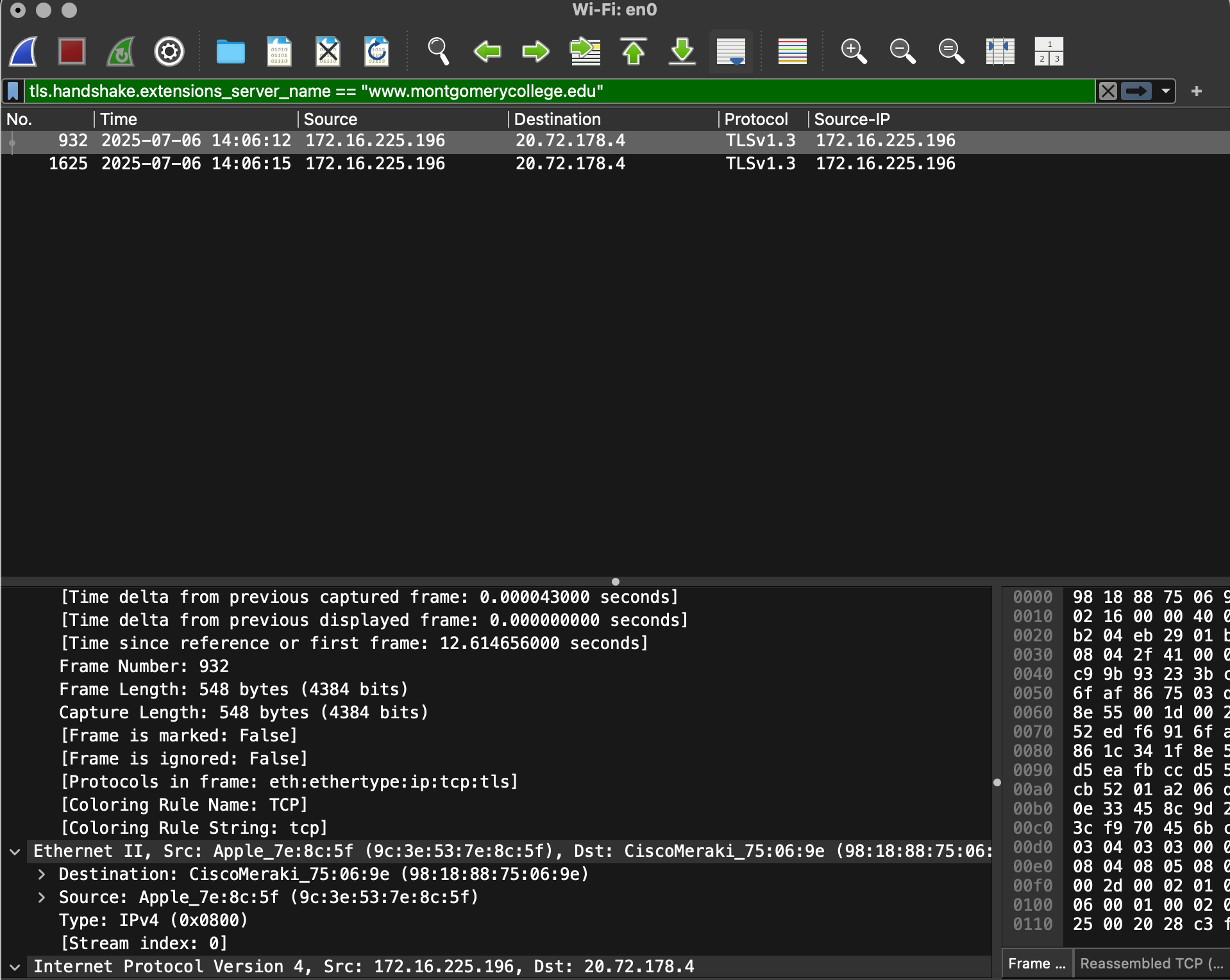


Screenshot 3: Demonstrates DNS traffic capture.

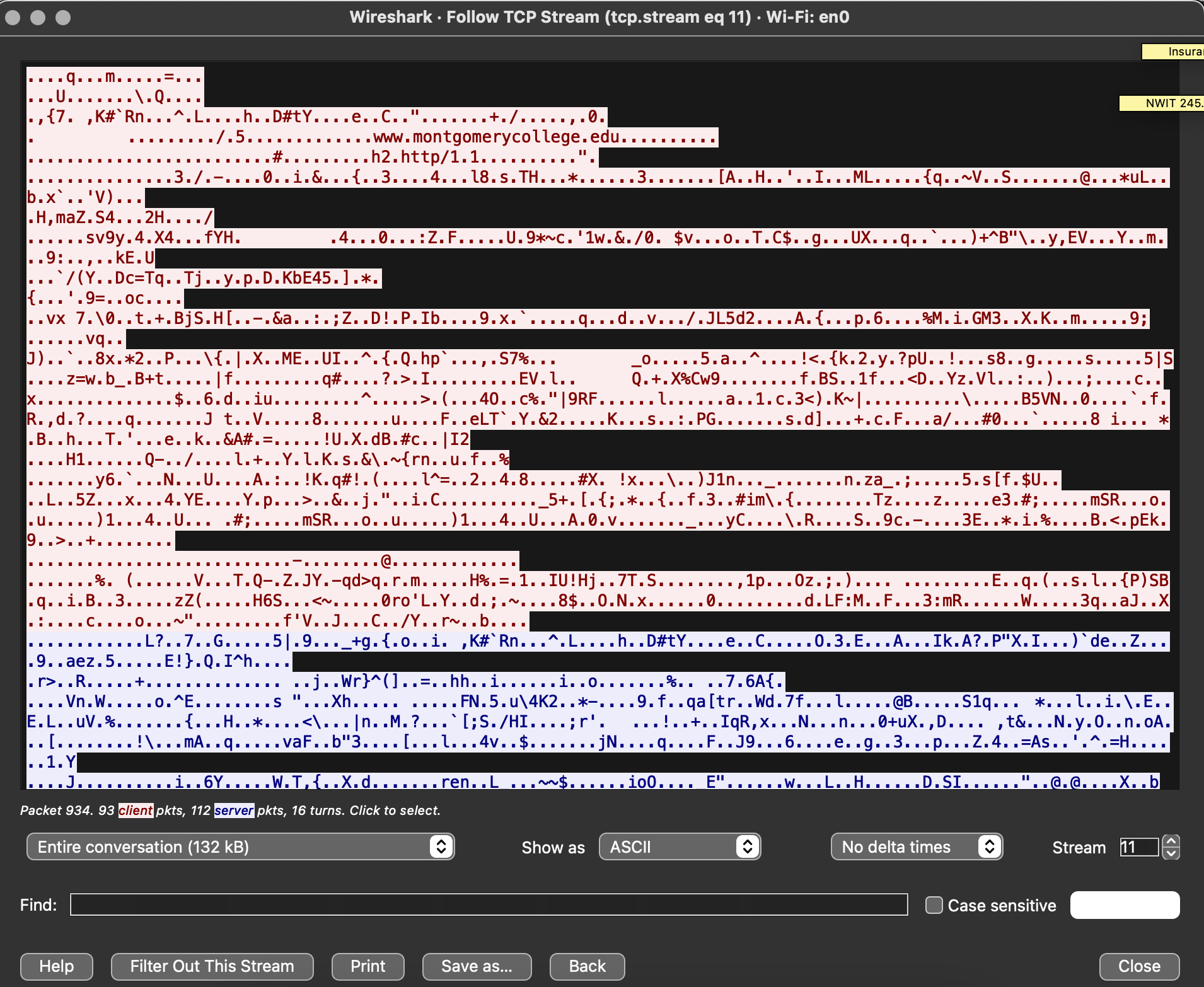
Screenshot 4: This shows the use of “Follow UDP Stream” on a DNS packet, supporting the explanation of why DNS uses UDP.



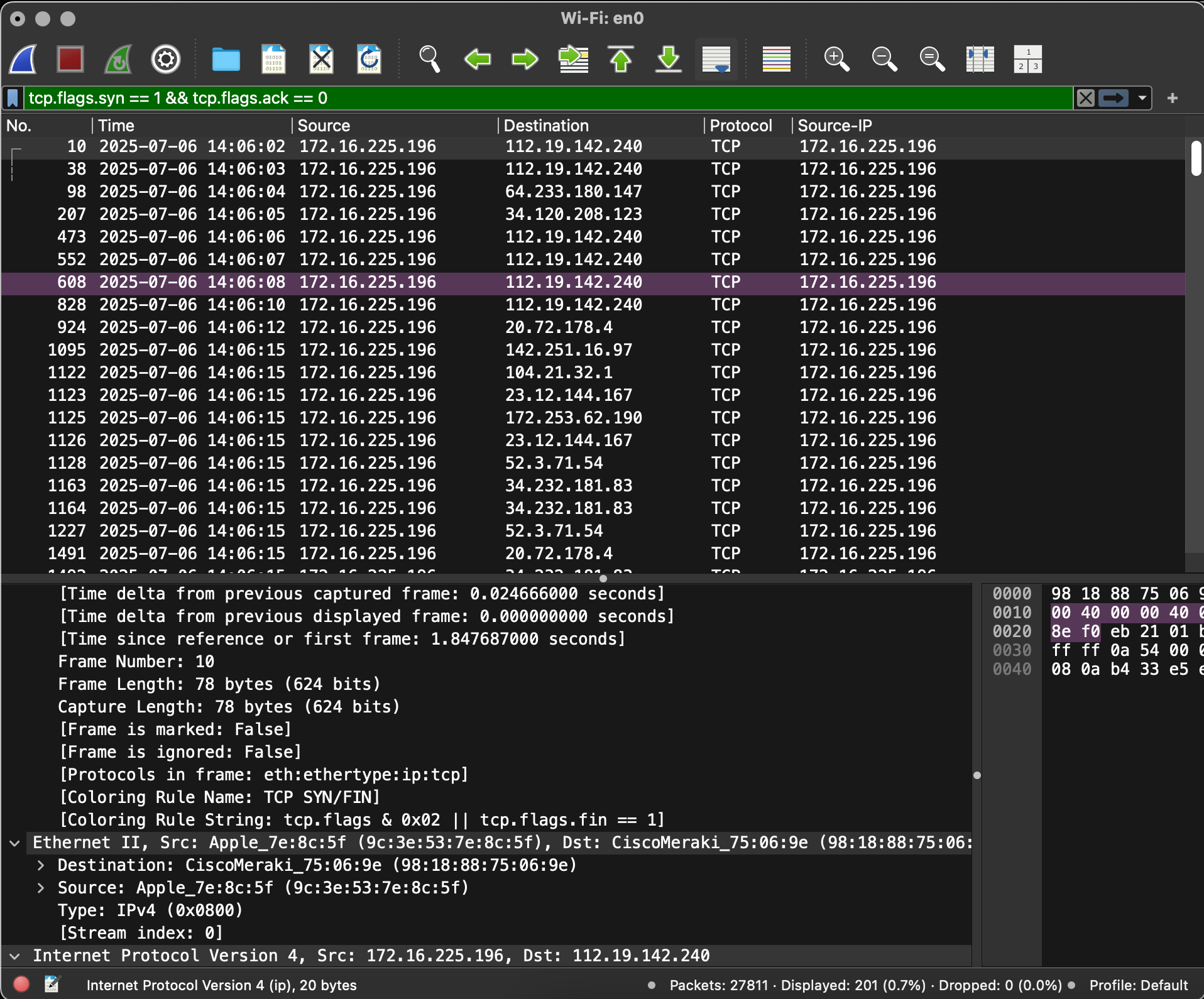
Screenshot 5: This is the closest result I could find using the http.host == www.montgomerycollege.edu filter. Since the website automatically redirects HTTP traffic to HTTPS, no results appeared with the original filter. After researching online, I found a TLS filter command that successfully captured my access to the webpage.



Screenshot 6: This shows what I got from following the TCP stream, and to inspect the full communication content of a specific TCP connection. I had successfully tracked the HTTP/TCP stream of Montgomery College website.



Screenshot 7: This shows the application of the filter tcp.flags.syn == 1 && tcp.flags.ack == 0, which is used to capture only TCP SYN packets (initial connection requests). This helps identify potential scanning or connection initiation behavior.



Lab Questions:

**1. If a packet is highlighted by black (while in default), what does it mean for the packet?**

A packet highlighted in black typically indicates a malformed / potentially harmful packet

**2. What is the filter command for listing all outgoing http traffic?**

http.request

**3. Why does DNS use Follow UDP Stream while HTTP uses Follow TCP Stream?**

DNS (Domain Name System) typically uses the UDP protocol for data transmission because it is faster and suitable for small, simple queries such as name resolution. DNS queries are small and do not require reliable delivery, making UDP a better fit. On the other hand, HTTP uses TCP because web browsing requires reliable and ordered delivery of data. TCP ensures that all packets arrive correctly and in order, which is essential for loading web pages accurately.

**4. Using Wireshark, try to capture the FTP password. Were you successful?**

Yes, if you use ftp.request as a filter.

**5. What are the steps to create a new column for Delta Time Display?**

R-click on Column Name -> Column Preferences -> “Add” + -> Rename

Appropriately -> assign it with “Delta Time Display” from the scroll-down bar

**6. What is the command for filtering to capture only syn requests?**

Tcp.flags.syn == 1 && tcp.flags.ack == 0