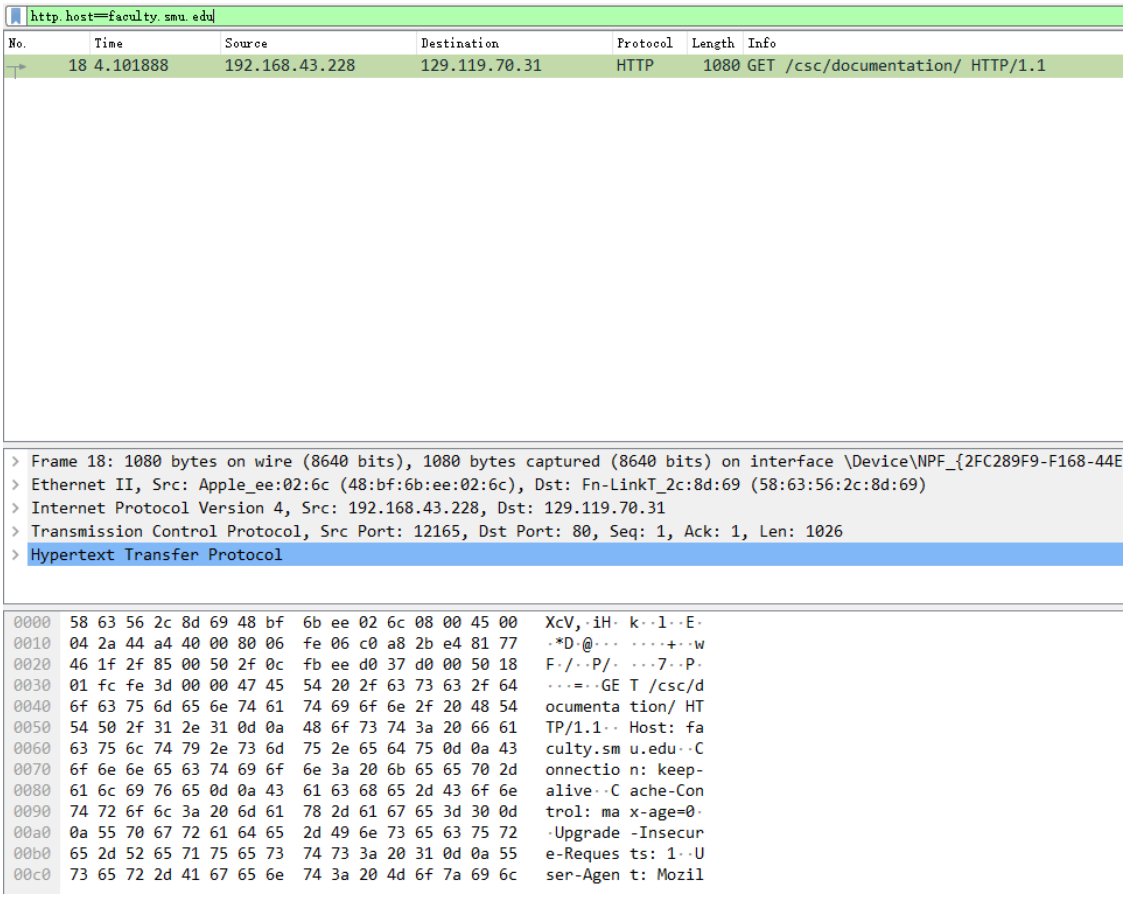
Xuan(James) Zhai

CS3339 Lab

March 19th, 2021

CS 3339 - Lab 5 - Lab Report

1: Carefully read the lab instructions and finish all tasks above. Attach screenshots to your report for steps 7, 8 and 10.



Pig 1: http.host==faculty.smu.edu

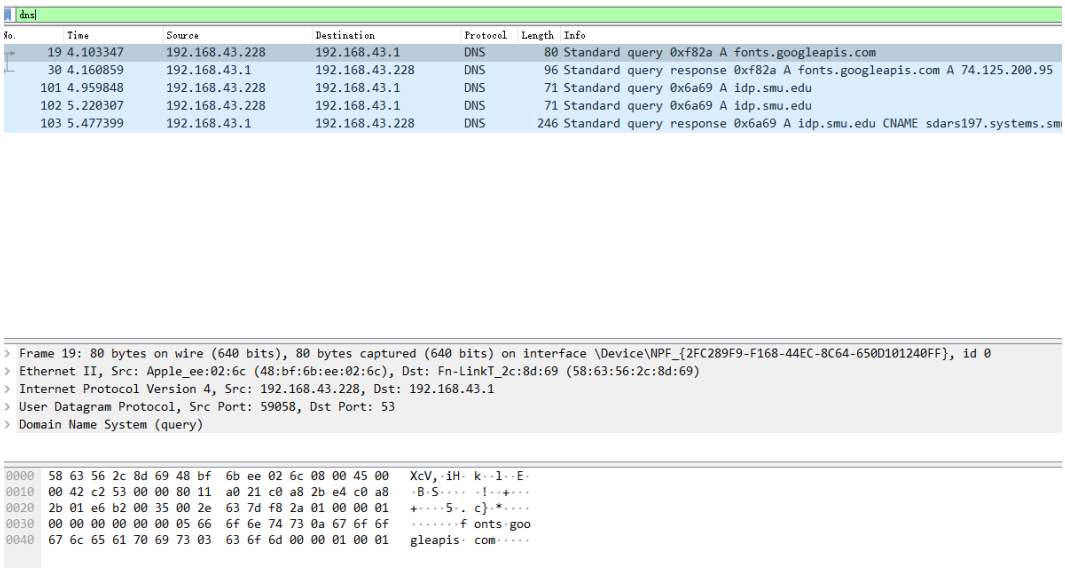


Fig 2: DNS

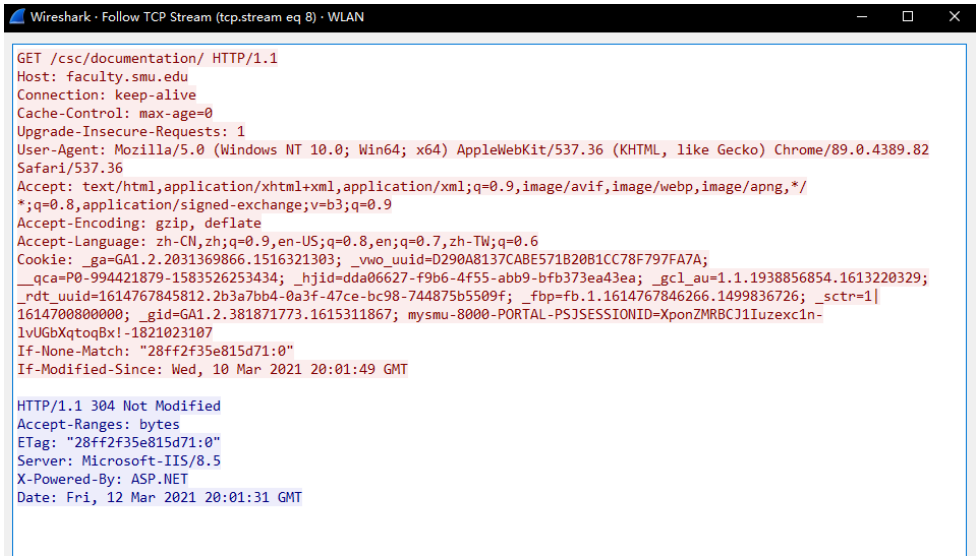


Fig 3: TCP Stream

2: If a packet is highlighted by black, what does it mean for the packet?

If a packet is highlighted by black, it means that the TCP packets may have some problem. For example, they could have been delivered out of order.

3: What is the filter command for listing all outgoing http traffic?

Only type “http”.

4: Why does DNS use Follow UDP Stream while HTTP use Follow TCP Stream?

Compared to TCP Stream, UDP Stream is much faster. Also, DNS requests are generally very small, and they fit well within UDP segments. For HTTP requests, it requires reliable delivery, so it needs TCP Stream which has a three-way handshake and the re-transmission of lost packets.

5: Using Wireshark to capture the FTP password. Explain how you found the password and attach a screenshot of the password packet. How could we have prevented sending the FTP login credentials in plain text over the network?

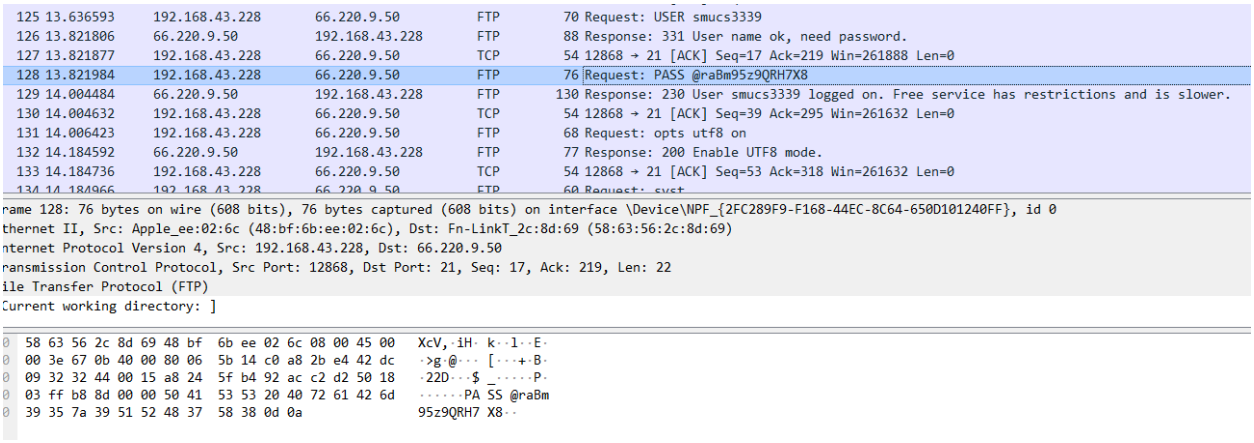


Fig 4: FTP Password

From the graph about we can find out that Wireshark captured the FTP request and response with server name, username, and password. To prevent a potential password leak, we could hash the password with salt to make it be unable to interpret, we could even hash the username to make more confusion.