CPTS 455 : Computer Networks and Security

Name : Mahesh Kumar Srinivas

WSU ID - 011845961

Assignment 1

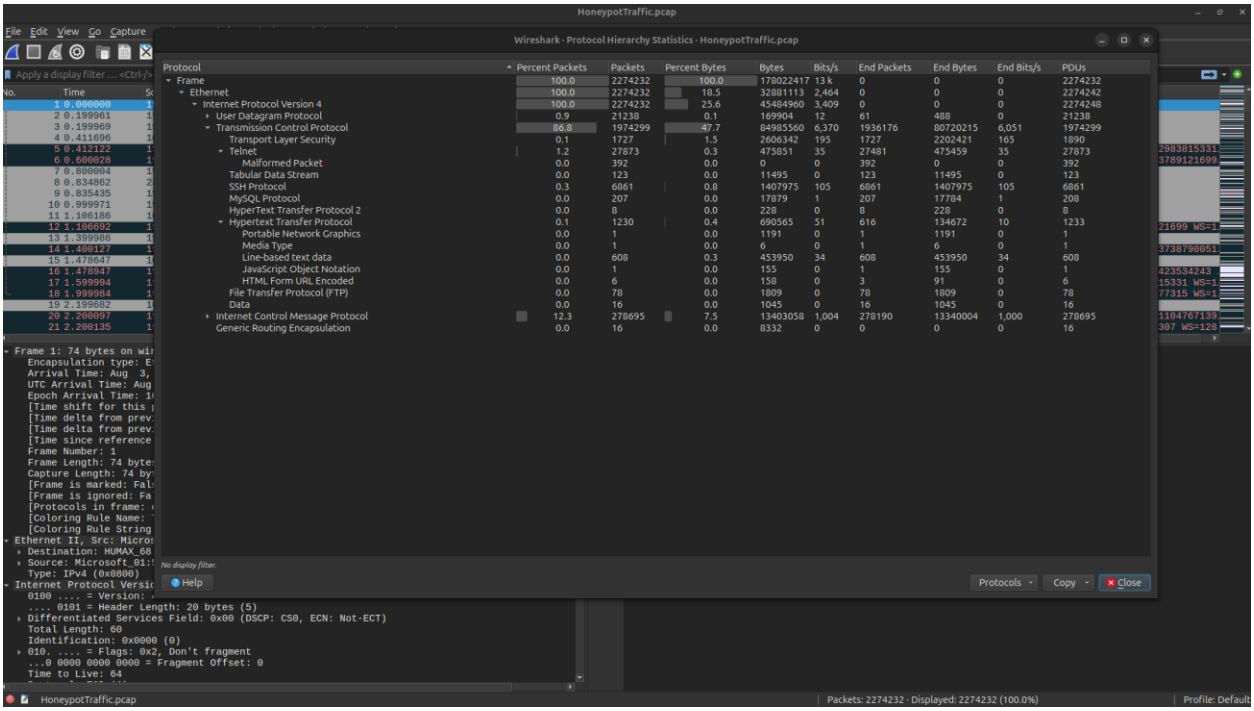

Figure 1: Statistics of pcap file

The above image shows the statistics of the pcap file. We can see how the packet capture is distributed among the different protocols. All the protocols are communicating using IPv4, and around 86.8% of the communication is over the TCP protocol.

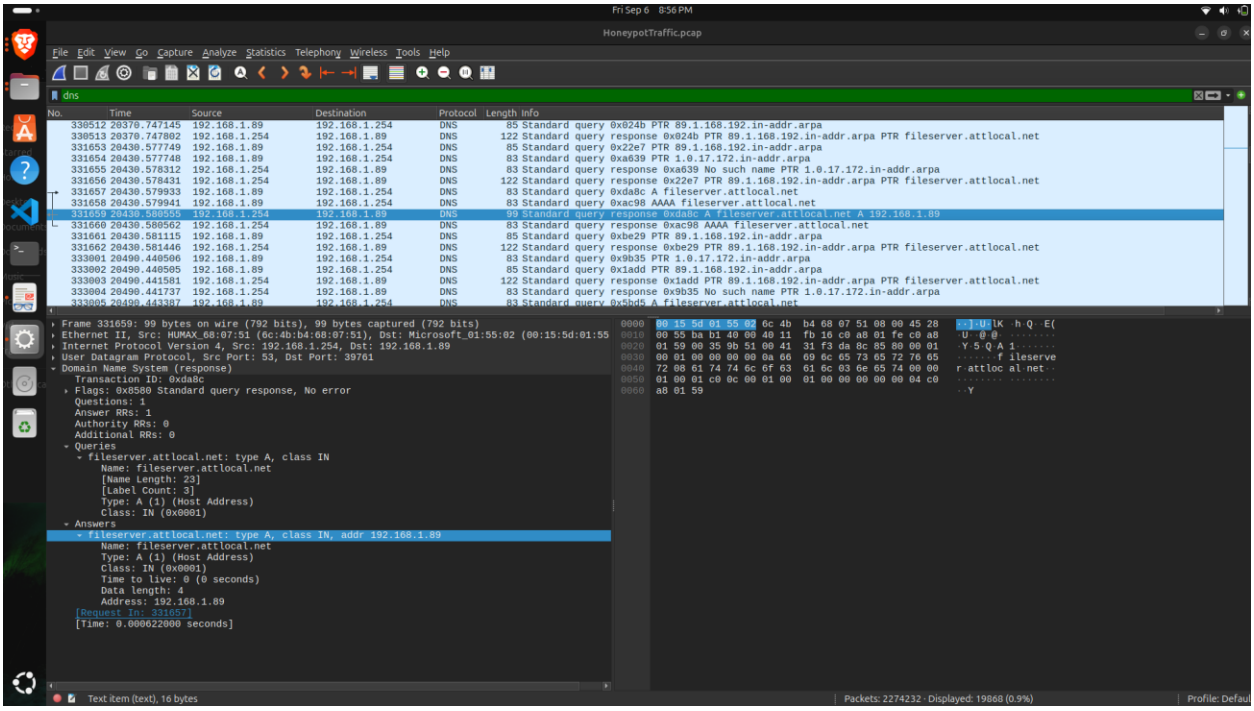

Figure 2: DNS protocol packet

The packet captured above is of the DNS protocol. The DNS information can be seen in the bottom left part of the image, showing the Domain Name System response, queries, and answers for this packet. It also displays the source and destination addresses. Additionally, we can see the User Datagram Protocol (UDP) details, where the entire UDP packet information is visible. In this packet, the DNS has resolved the domain name 'fileserver.attlocal.net' to the IP address '192.168.1.89..

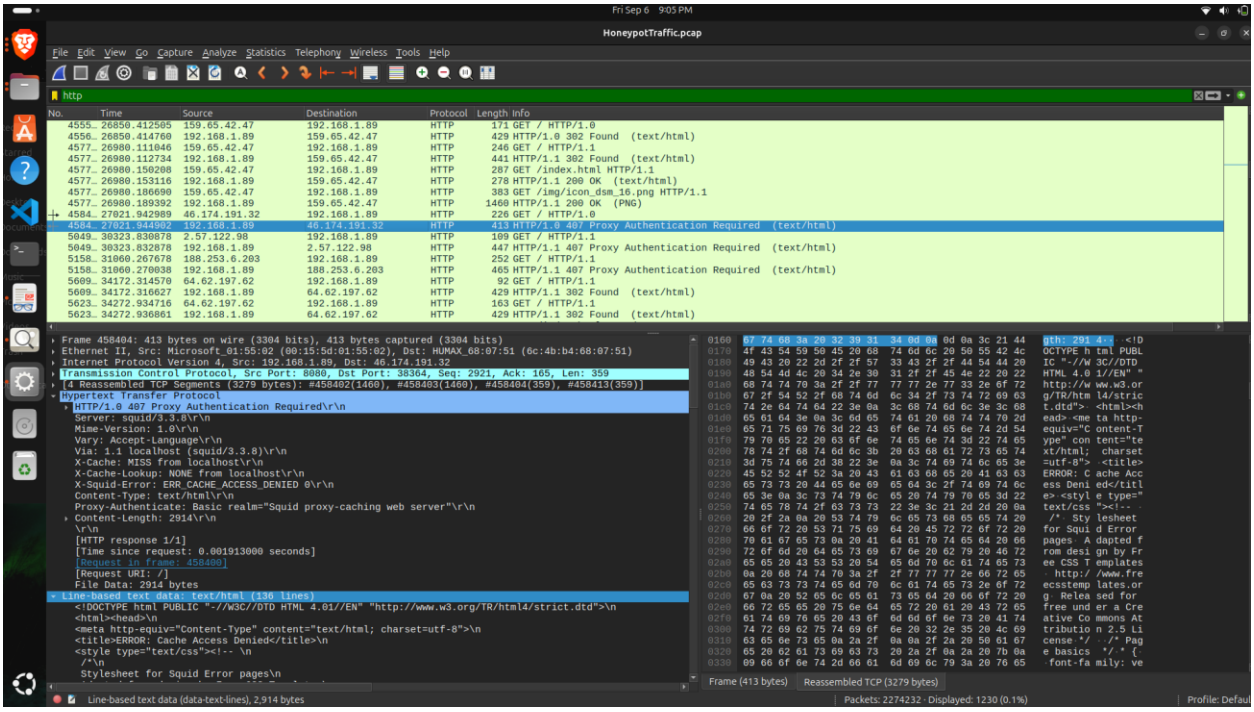

Figure 3: HTTP protocol packet

The screenshot above shows a packet capture of an HTTP request. After applying a filter to view all captured HTTP packets, I saw this one. It shows a GET request that receives a '407 Proxy Authentication Required' response, indicating that proper authentication is missing to access the webpage. The packet details are visible in the bottom left corner, including source and destination ports and the text/html content. Additionally, we can see that TCP segment reassembly is also performed in this packet. From filtering the HTTP packets, I noticed that many of the requests resulted in '404 Not Found' or authentication failures. This leads me to conclude that the user is attempting to access the website without proper authorization.

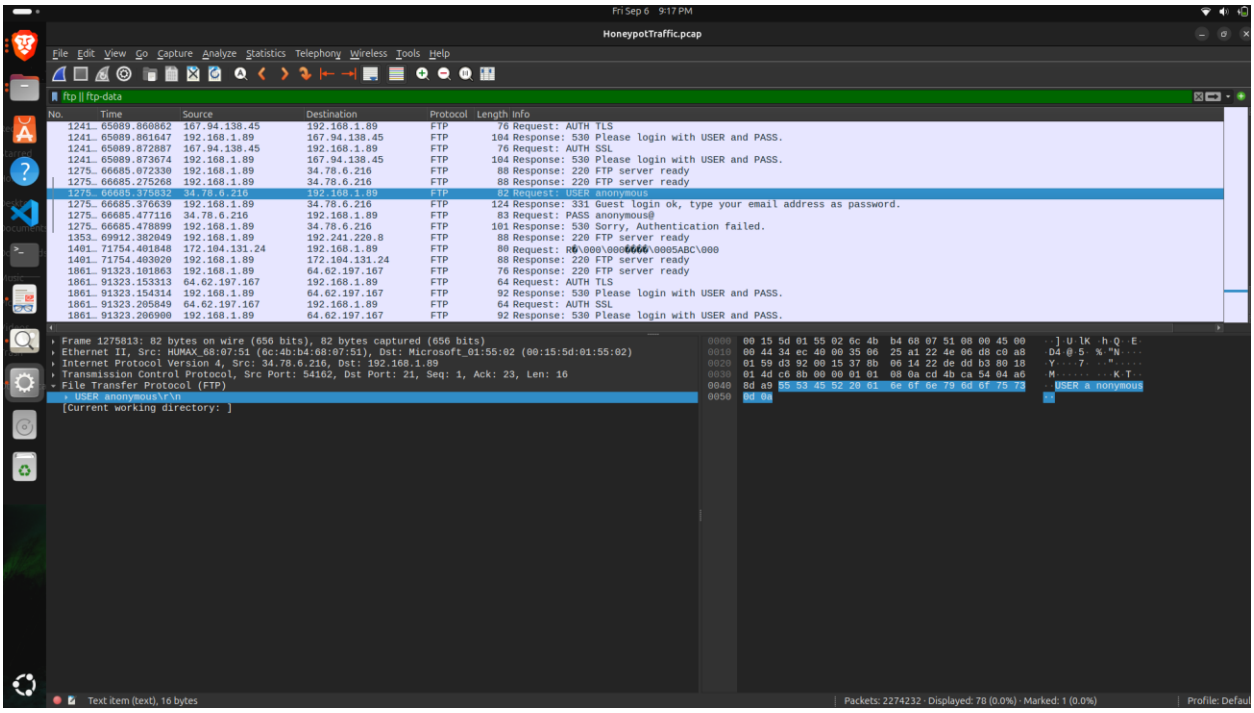

Figure 4.1: DNS protocol packet

In the above capture, I have captured an FTP packet. The request shows the user providing the name 'anonymous.

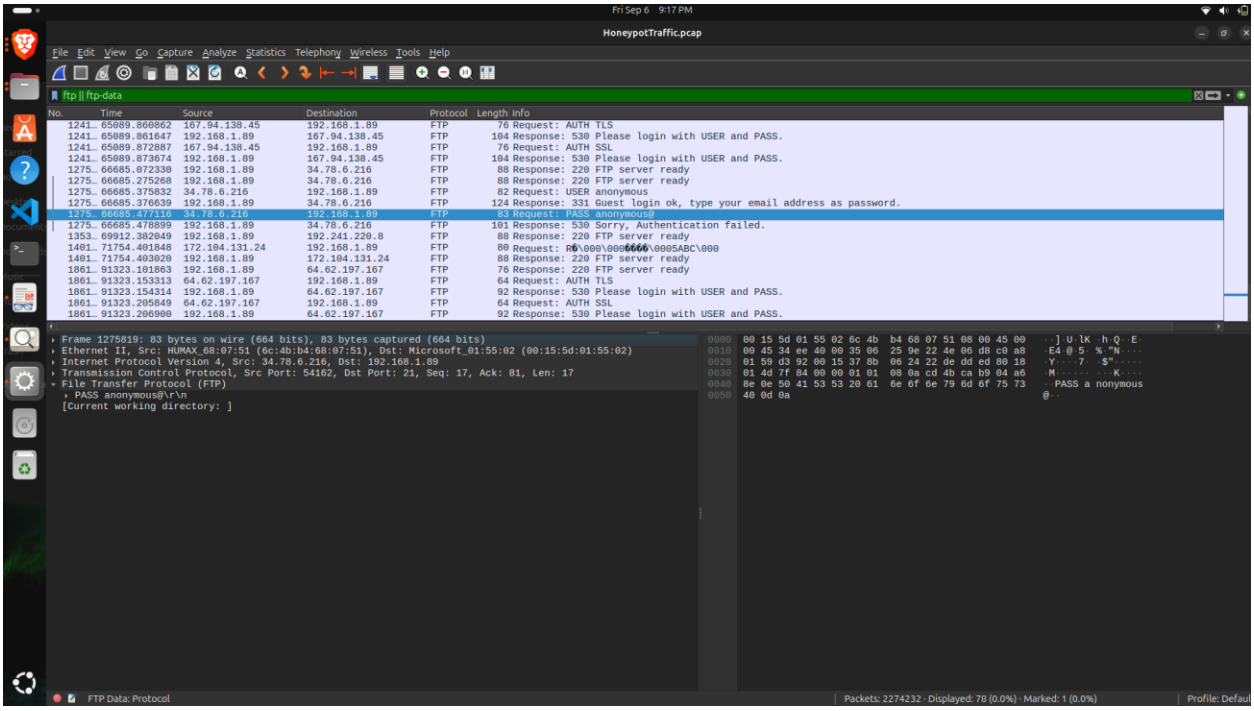

Figure 4.2: DNS protocol packet

We can see that it says 'guest login ok' and asks for an email address as the password. The user enters 'anonymous@' as the password, but the authentication fails. From filtering the FTP packets, I observed that the user attempted to access the server multiple times using various usernames and passwords, but authentication failed each time. However, the guest login was successfully checked. Since FTP is not secure, we were able to view the details in an unencrypted form.

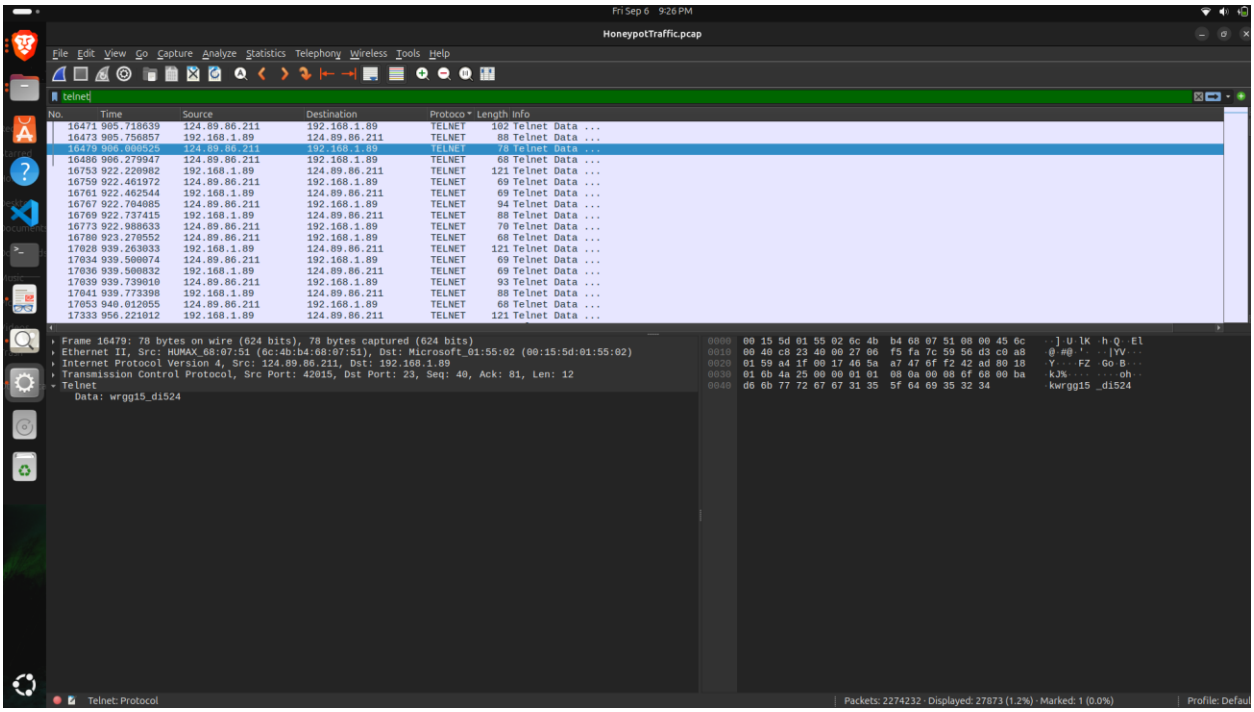

Figure 5: Telnet protocol packet

The screenshot above shows a TELNET packet capture. The actions taken and their outputs can be seen in the TELNET section. This packet capture appears immediately after the previous packet, which requested a password. Therefore, we can conclude that this packet likely contains the password entered by the user.

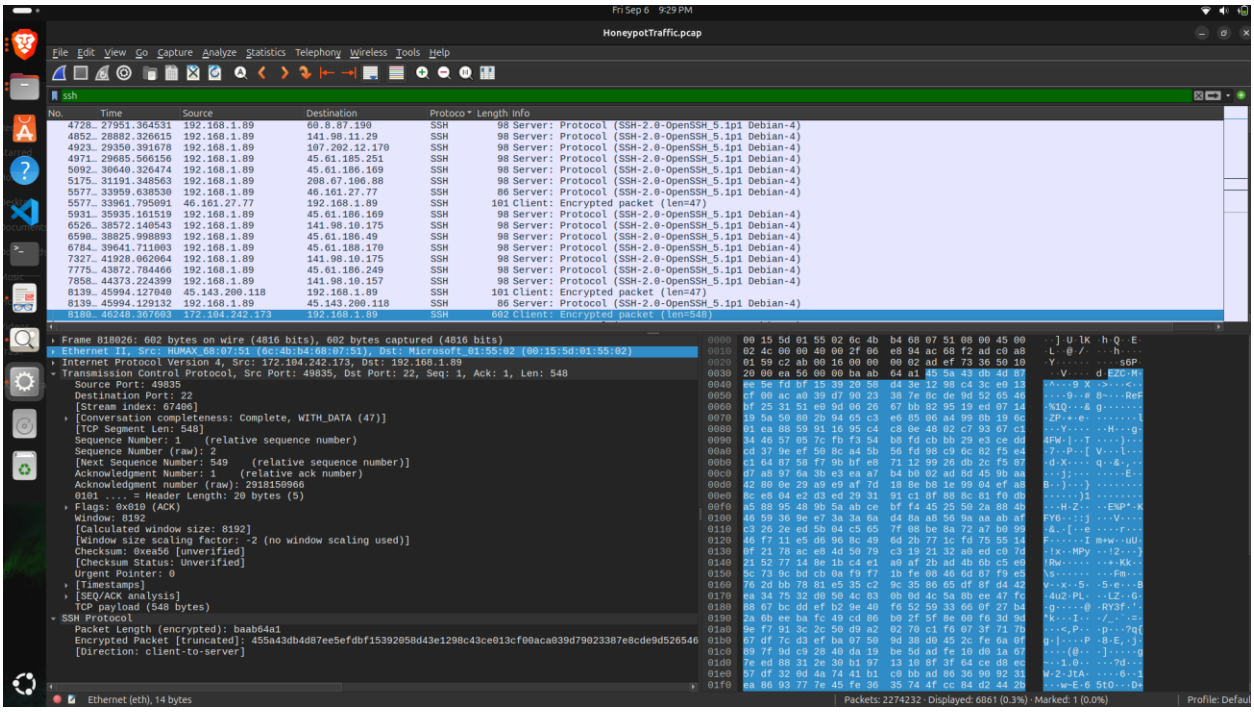

Figure 6.1: SSH protocol packet

The packet capture above is for SSH. We can see that the protocol used by the client involves encrypted packets, indicating that this protocol is secure.

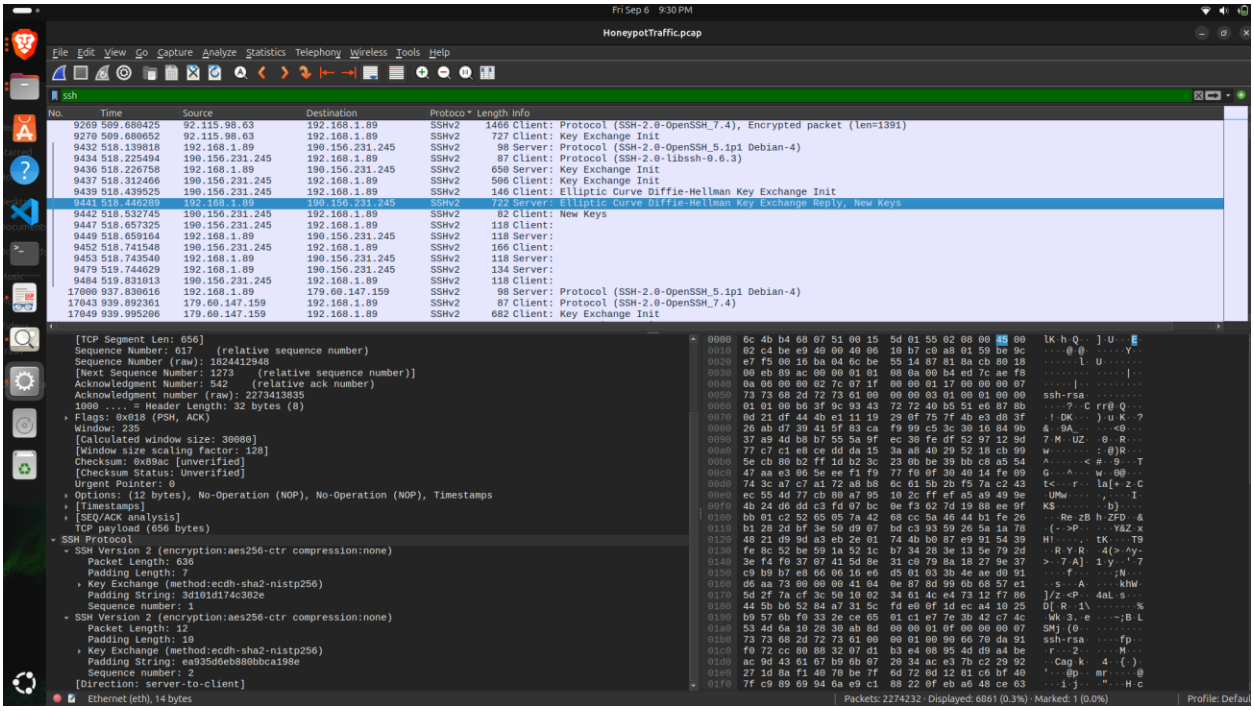

Figure 6.2: SSH protocol packet

The packet above is also for SSH, specifically using SSHv2. In the screenshot, I can observe that the Diffie-Hellman key exchange is being used to secure the channel by establishing a shared secret key. We can see the exchange initialization taking place and new keys being generated.

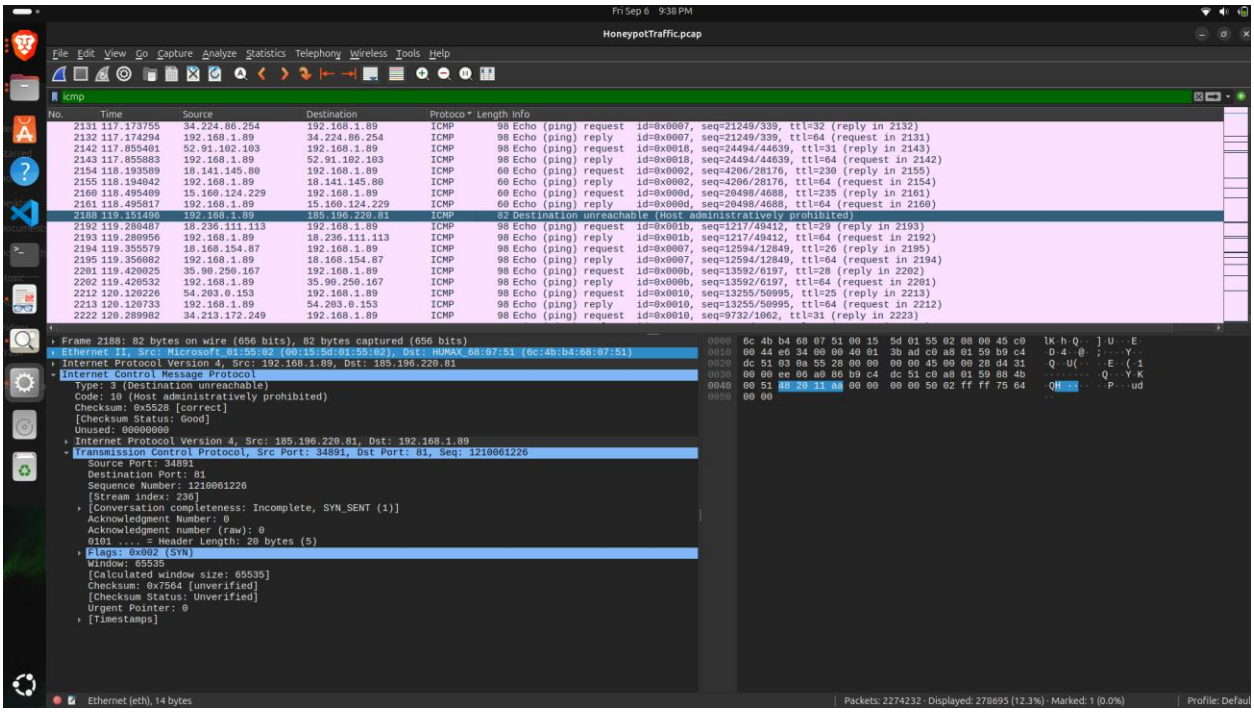

Figure 7: ICMP protocol packet

The screenshot above captures details of the ICMP protocol. As observed, the most frequently seen packets are 'reply,' 'request,' and 'unreachable.' While there are occasional instances where the destination is unreachable, it is mostly reachable. This protocol is used to check the status of network communication.

2.

After investigating the pcap file, I observed multiple general attempts to log in to the website, all of which failed due to authentication issues. This suggests an attempt to breach the system. Additionally, FTP and TELNET are not secure as they transmit usernames and passwords in an unencrypted manner. In contrast, SSH is highly secure, employing encryption to protect data. It also utilizes the Diffie-Hellman key exchange method to establish secure keys.

3.

By doing this exercise, I learned how to install Wireshark on an Ubuntu operating system and use it to investigate network traffic. I became quite familiar with analyzing various protocols and understanding the data being sent and received. I was also able to analyze attack attempts through multiple login attempts and determine which protocols are secure and which are not by examining the packets.