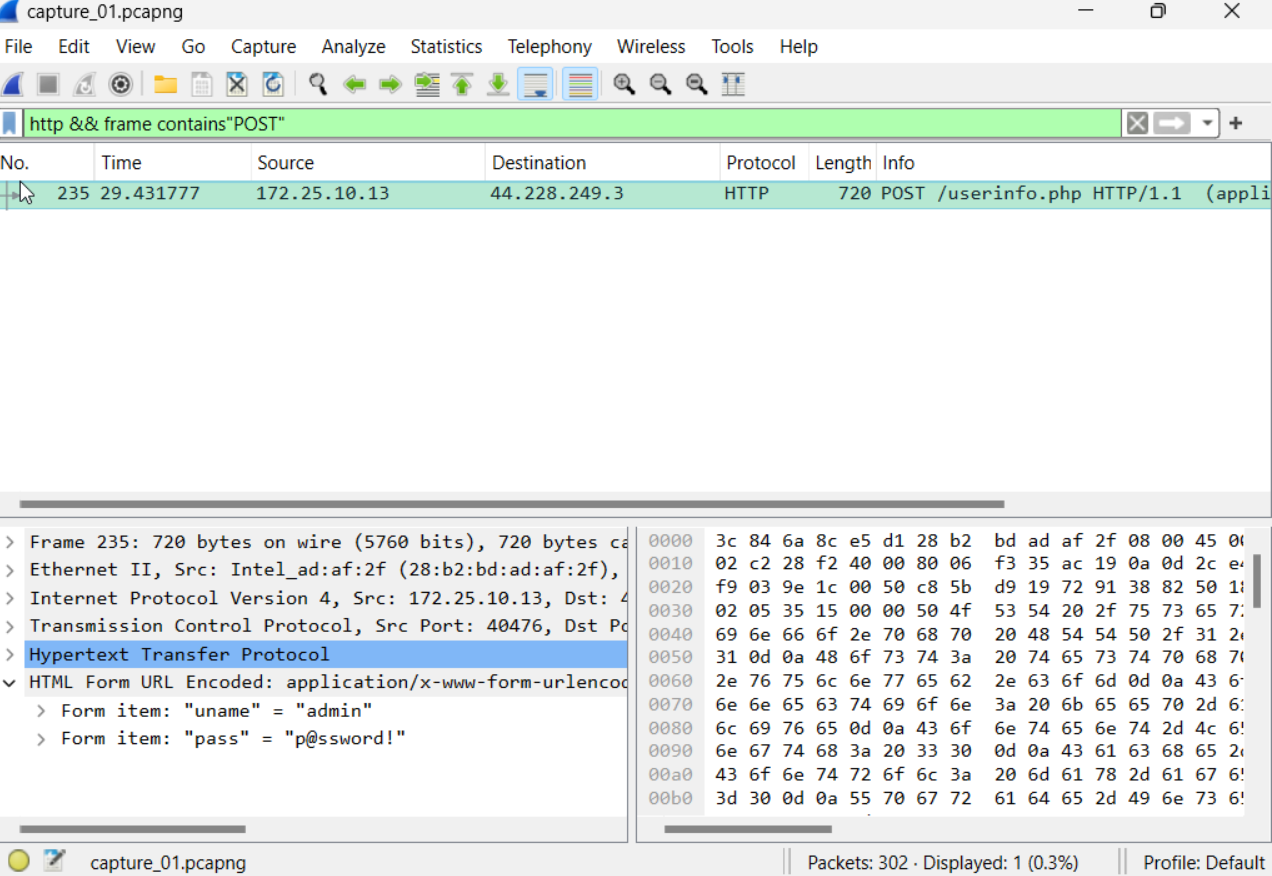
# Wireshark Packet Analysis Project Report

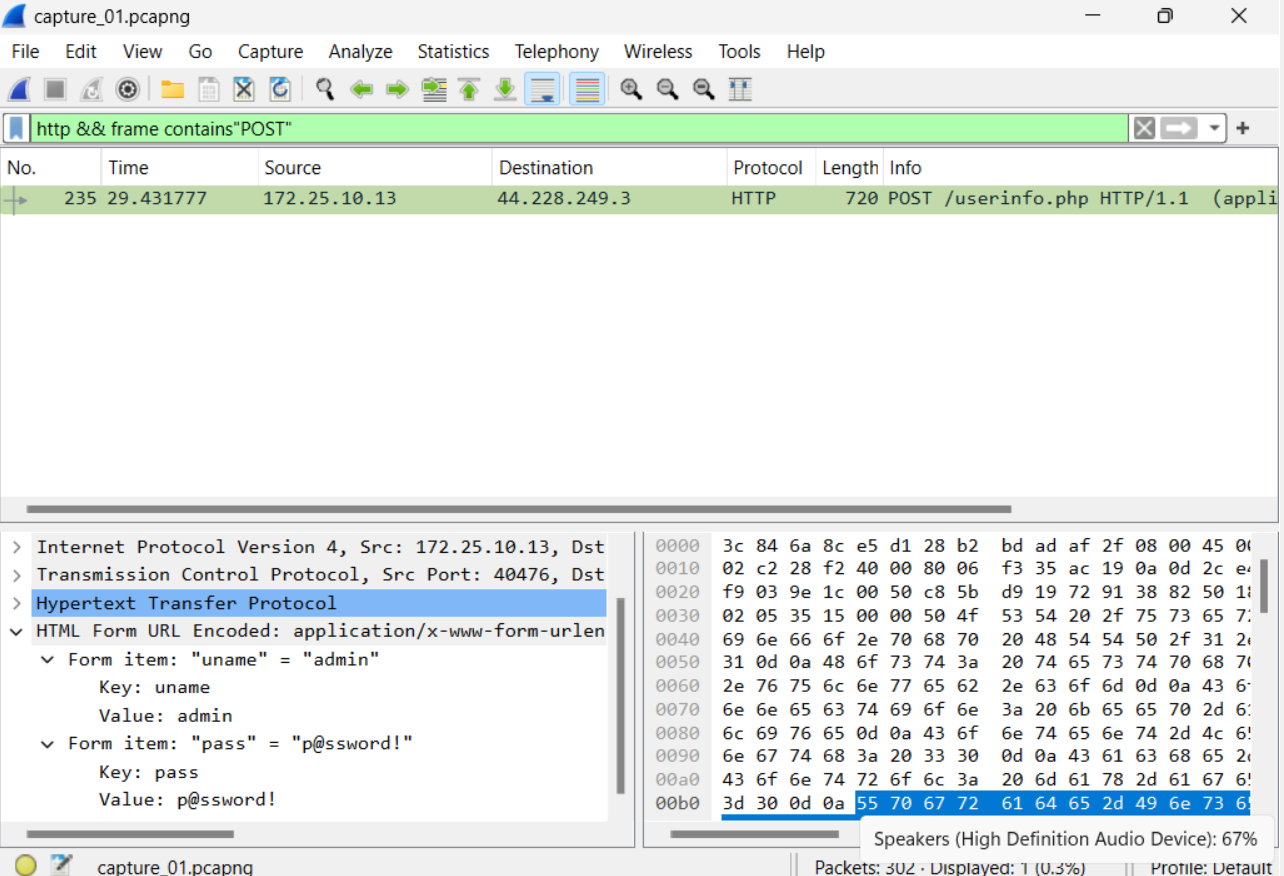
Task 1: (10 points)

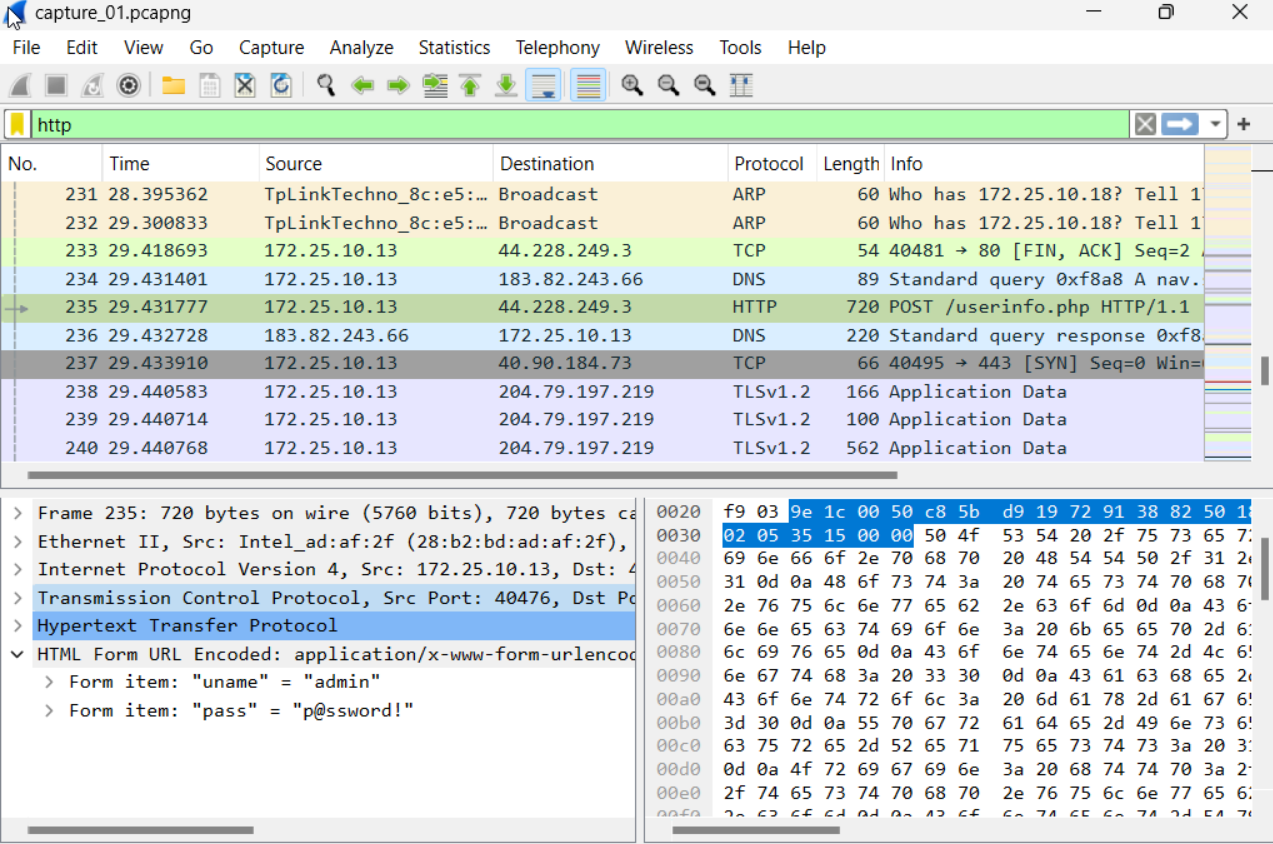
1. Screenshot of the packet that contains the username and password details:

[Please make sure that the Frame No., Username and Password are clearly visible on the screenshot]

Sno. 235





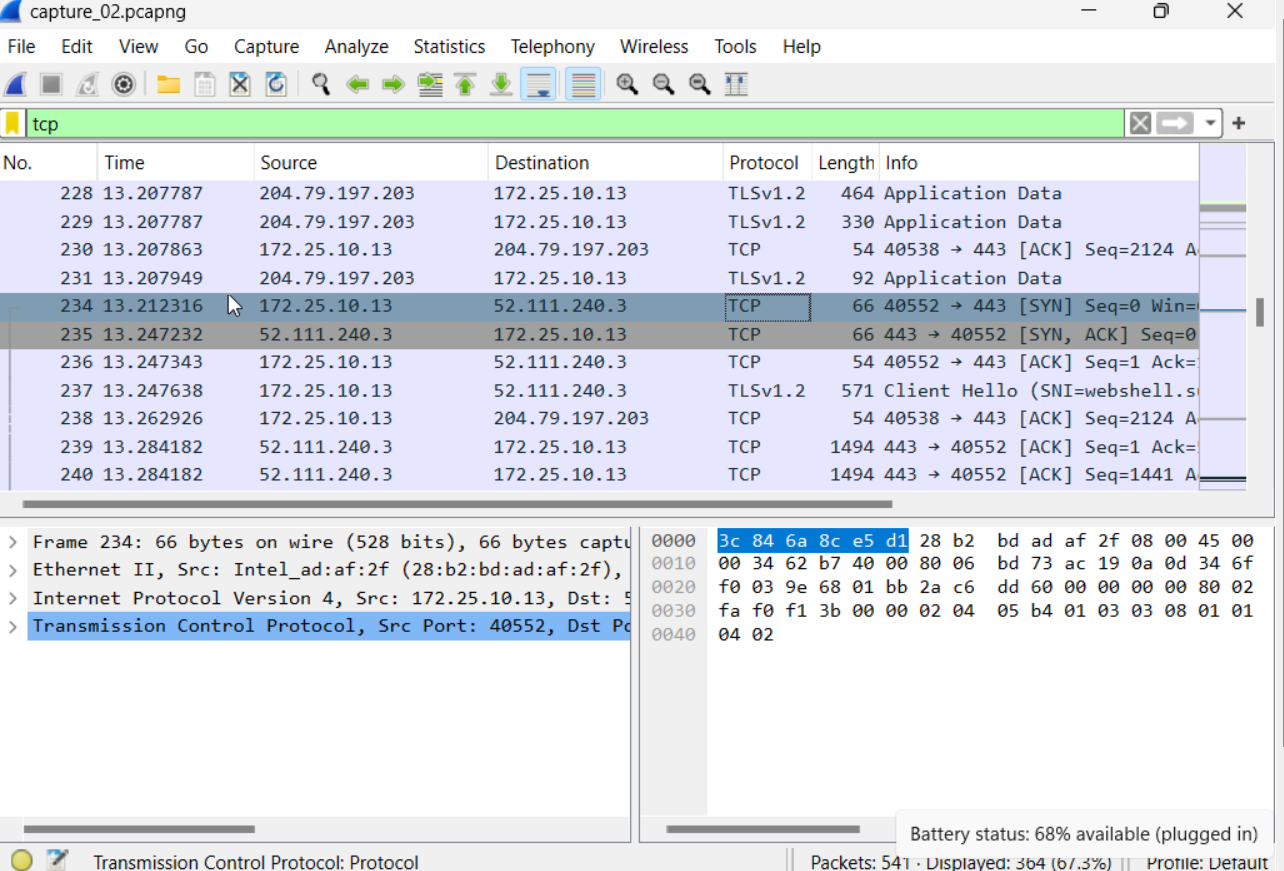


Task 2: (15 points)

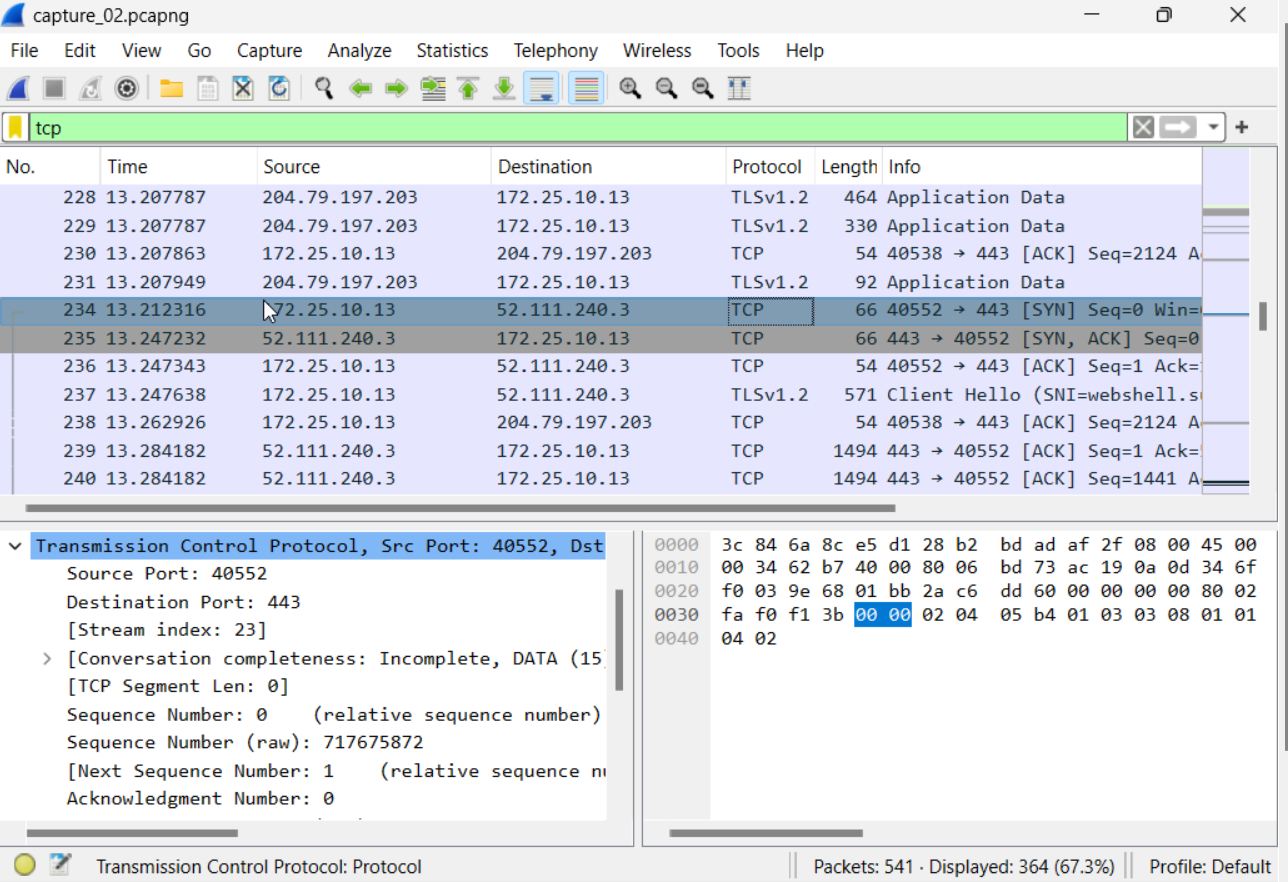
1. Screenshot (of the packet list pane) for the 3-way TCP handshake:

[Please ensure that the Frame No., Time, Source, Destination, Protocol, Length and Info details are visible in the screenshot].

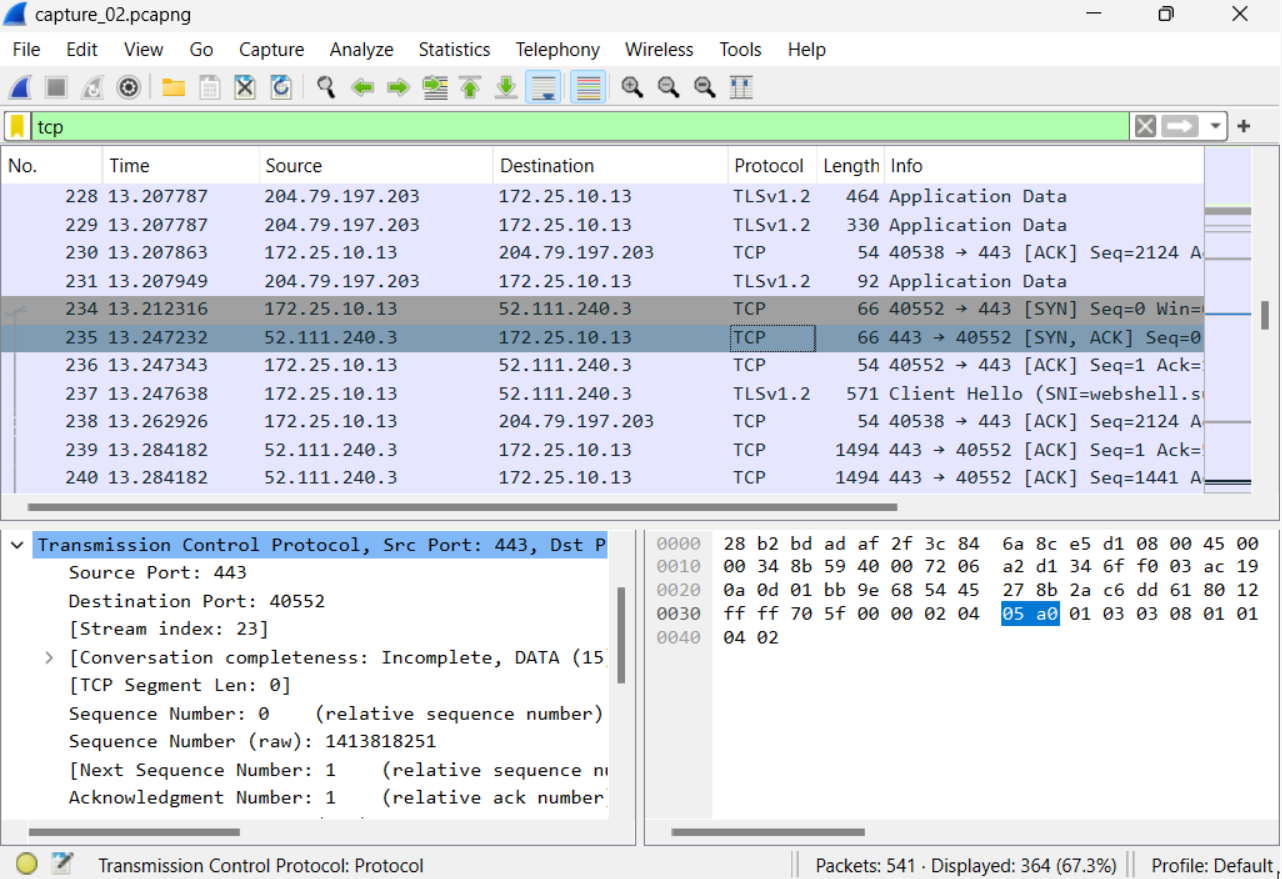
Sno. 234,235,236



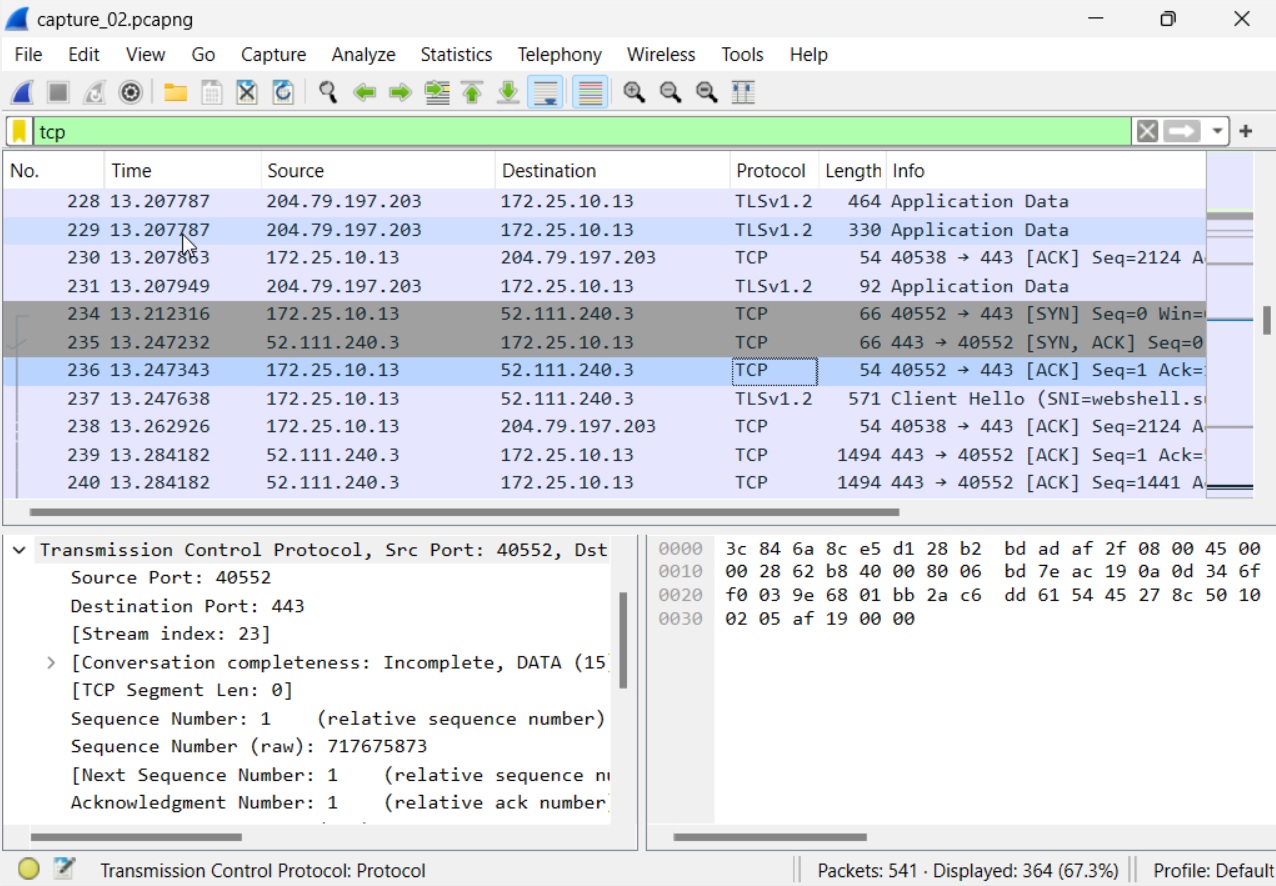
SYN packet



SYN-ACK packet



ACK packet



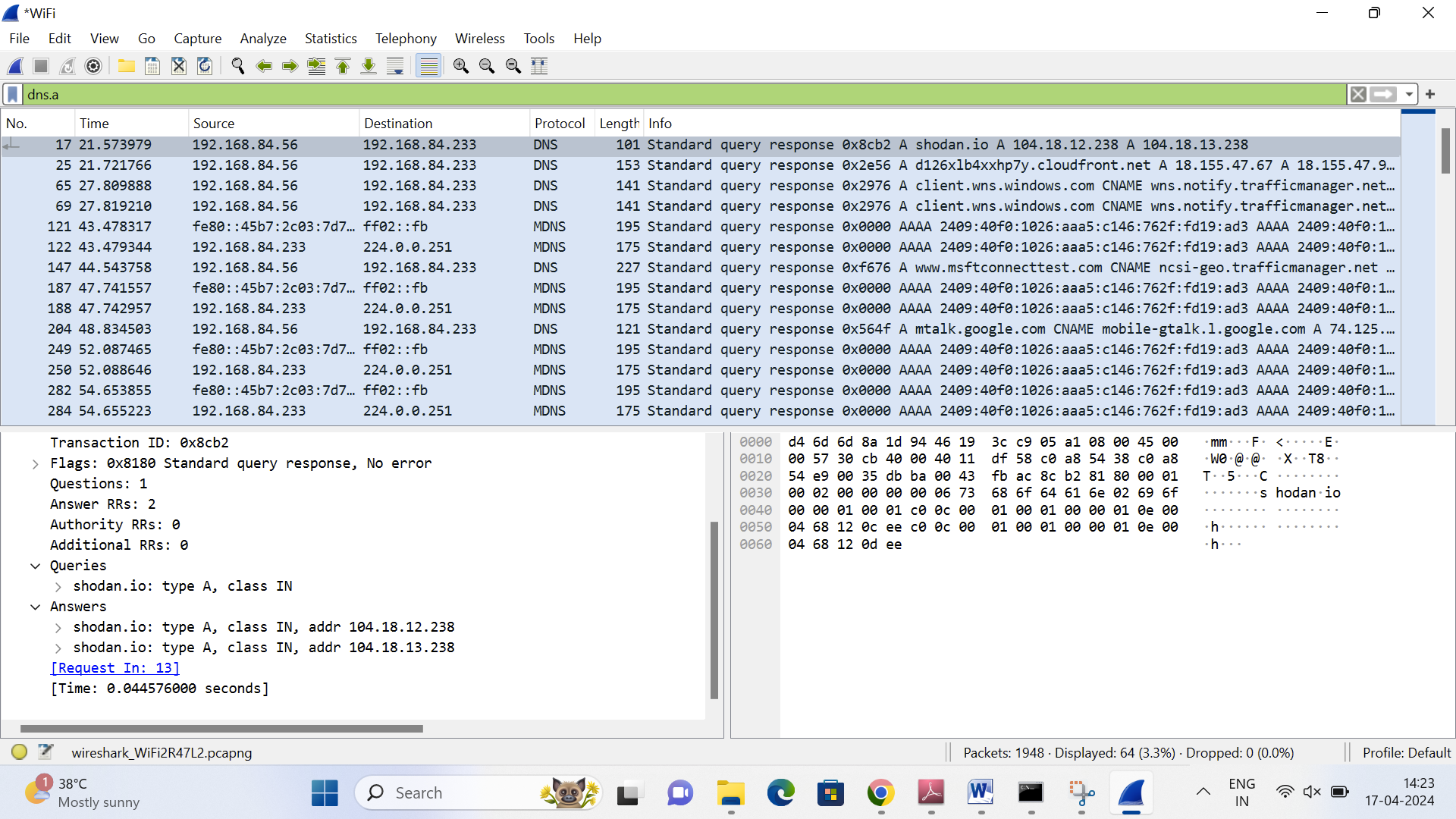
1. Complete the following table:

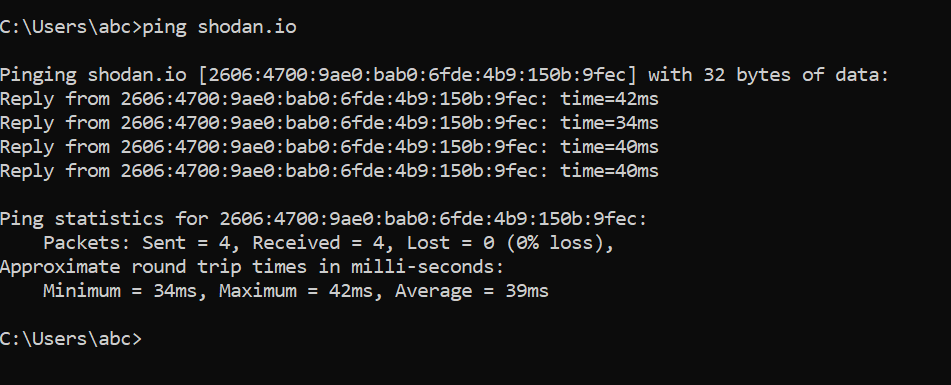
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Frame No. | Source IP address | Source port number | Destination IP address | Destination port |
| SYN Packet | 234 | 172.25.10.13 | 40552 | 52.111.240.3 | 443 |
| SYN-ACK Packet | 235 | 52.111.240.3 | 443 | 172.25.10.13 | 40552 |
| ACK-Packet | 236 | 172.25.10.13 | 40552 | 52.111.240.3 | 443 |

Task 3: (15 points)

1. Screenshot of the DNS response containing the IPv4 address:

[Please make sure that the Frame No. and the IPv4 address are clearly visible on the screenshot

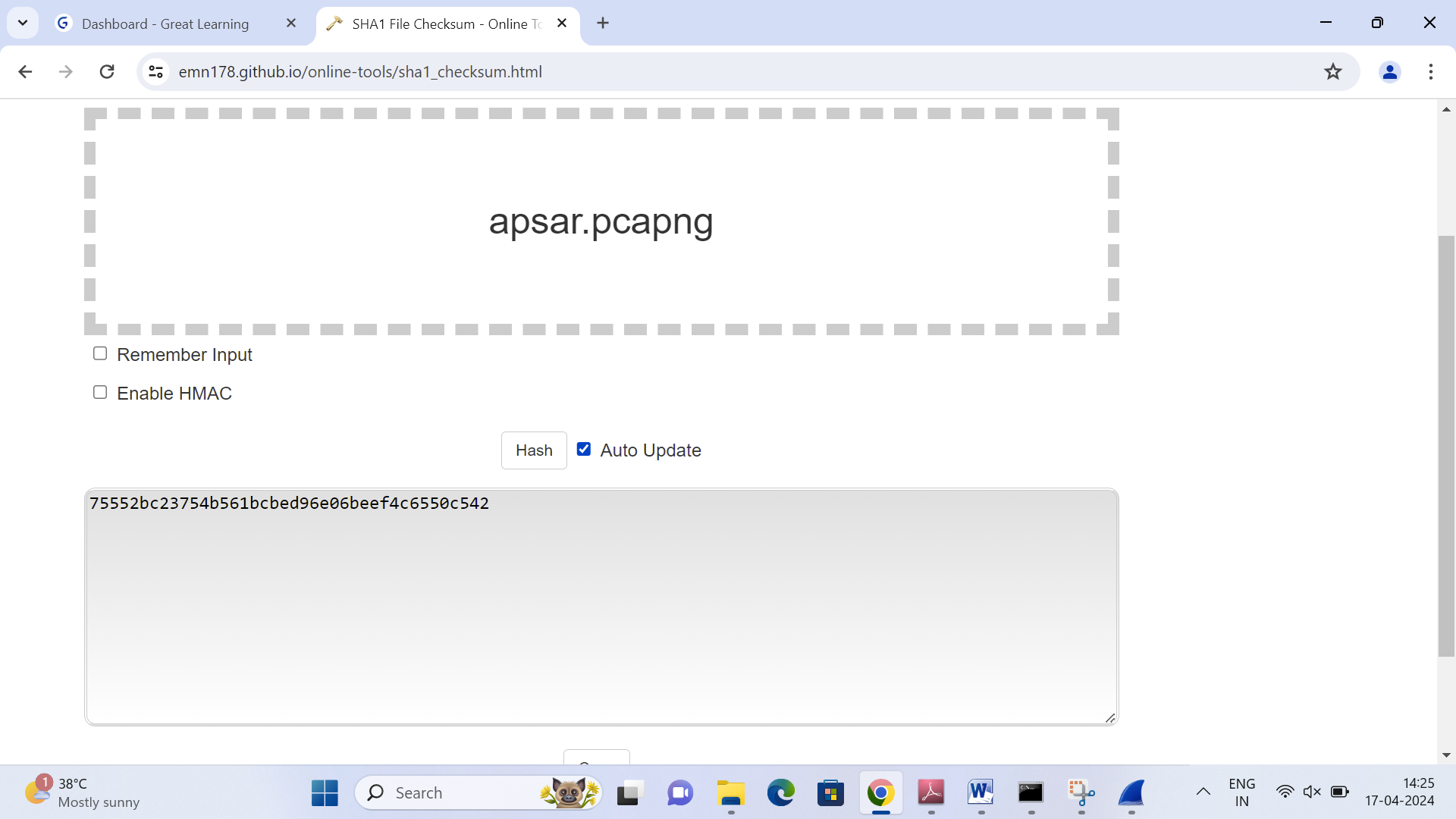




1. SHA-1 hash of the .pcap file that you saved:

**75552bc23754b561bcbed96e06beef4c6550c542**

[Use the tool - [https://emn178.github.io/online-tools/sha1\_checksum.html](https://emn178.github.io/online-tools/sha1_checksum.html%20) to get the SHA-1 hash]



1. Upload the .pcap file on Olympus along with this Word document.