STEP 1: : Capture and Analyze Network Traffic Using Wireshark.

NOW GO ON YOUR PC AND OPEN WIRESHARK IF IT IS THERE OTHERWISE INSTALL FROM BROWSER.

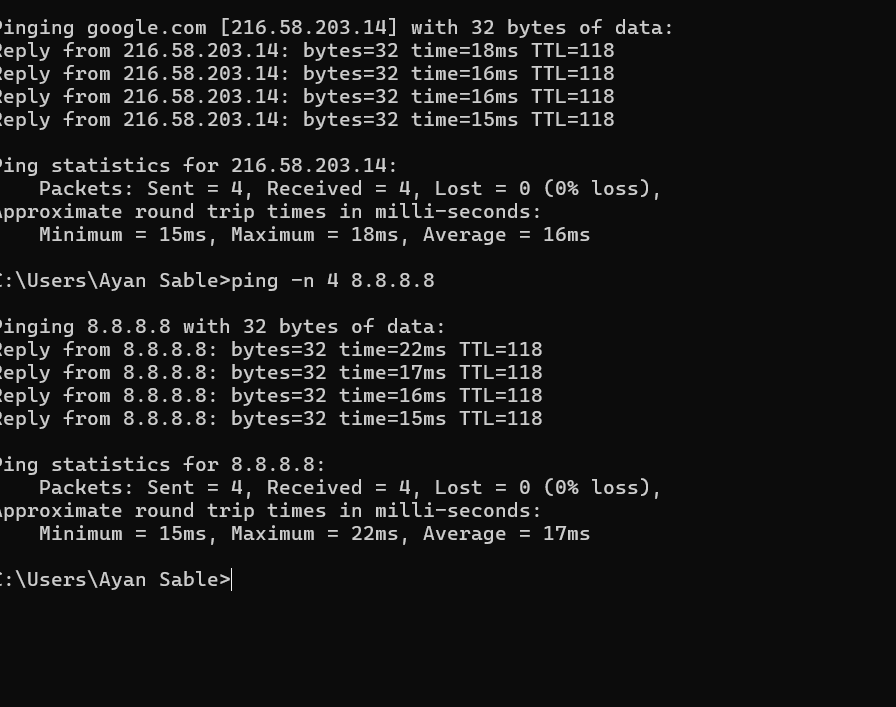
STEP 2: Start capturing on your active network interface.

A screenshot of a computer screen

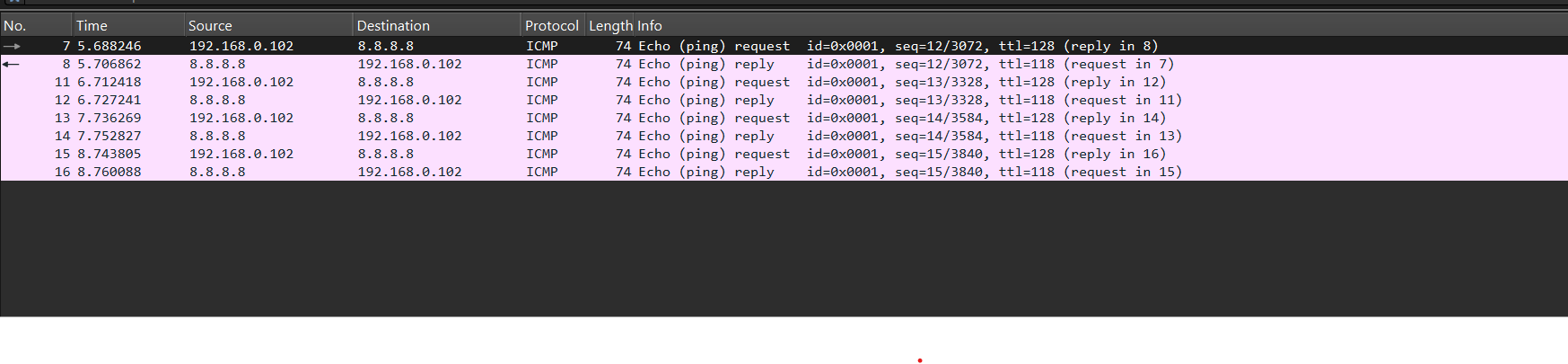
AI-generated content may be incorrect.

THIS IS THE CURRENT ANALYSIS OF MY PC NOW WE HAVE CHECK NETWORK TRAFFIC.

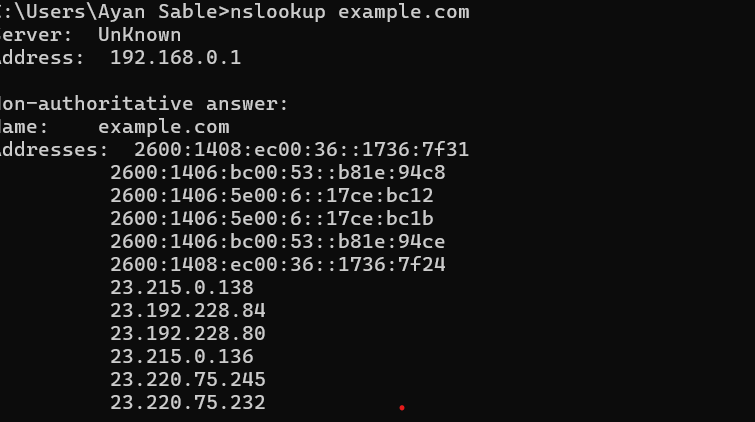
STEP 3:NOW TO BROWSER AND VISIT ANY WEBSITE AND GRNTLY GO ON COMMAND AND RUN COMMAND EG (PING GOOGLE.COM)



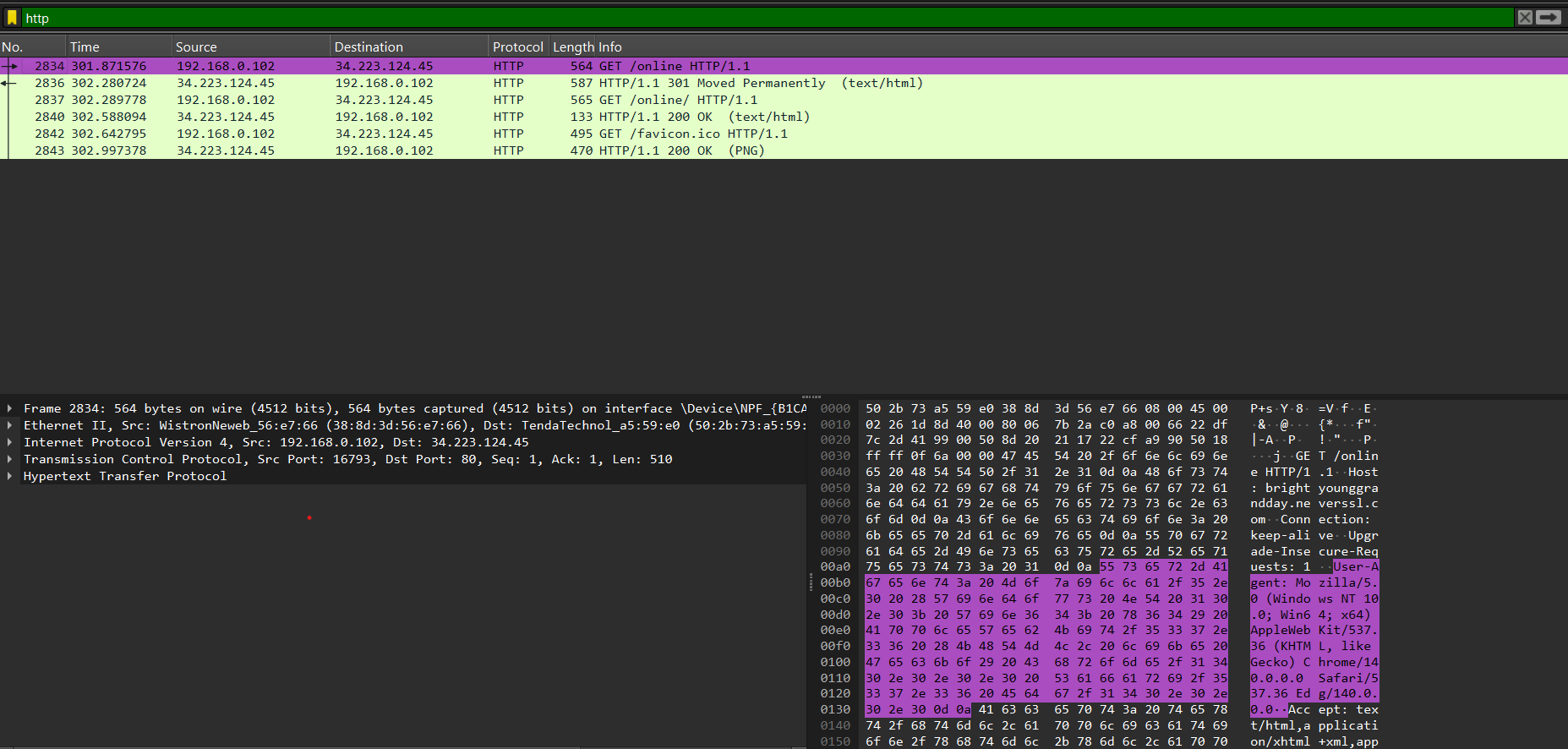
##NOW GO ON WIRESHARK AND SEE ICMP PACKET ON WIRESHARK.

MEANS IN ICMP PACKET A COMPUTER SEND REQUEST AND SERVER WILL RESPONCE AND ITS DONE SUCCESSFULLY RESPONSE FROM SERVER.

STEP 4:GO TO ANY INSECURE WEBSITE ANY AND GO IN WIRESHARK AND WRITE CMD(http) IT WILL SHOW THAT THE SERVER IS UNKNOWN AND ALSO SHOW HOW IT IS TEXTED MEANS HTML OR ANY OTHER SCRIPT.



AND IN WIRESHARK THE ANALYSIS



STEP 5:NOW VISIT ANY SECURE WEBSITE FROM YOUR BROWSER ANY

A screenshot of a computer

AI-generated content may be incorrect.

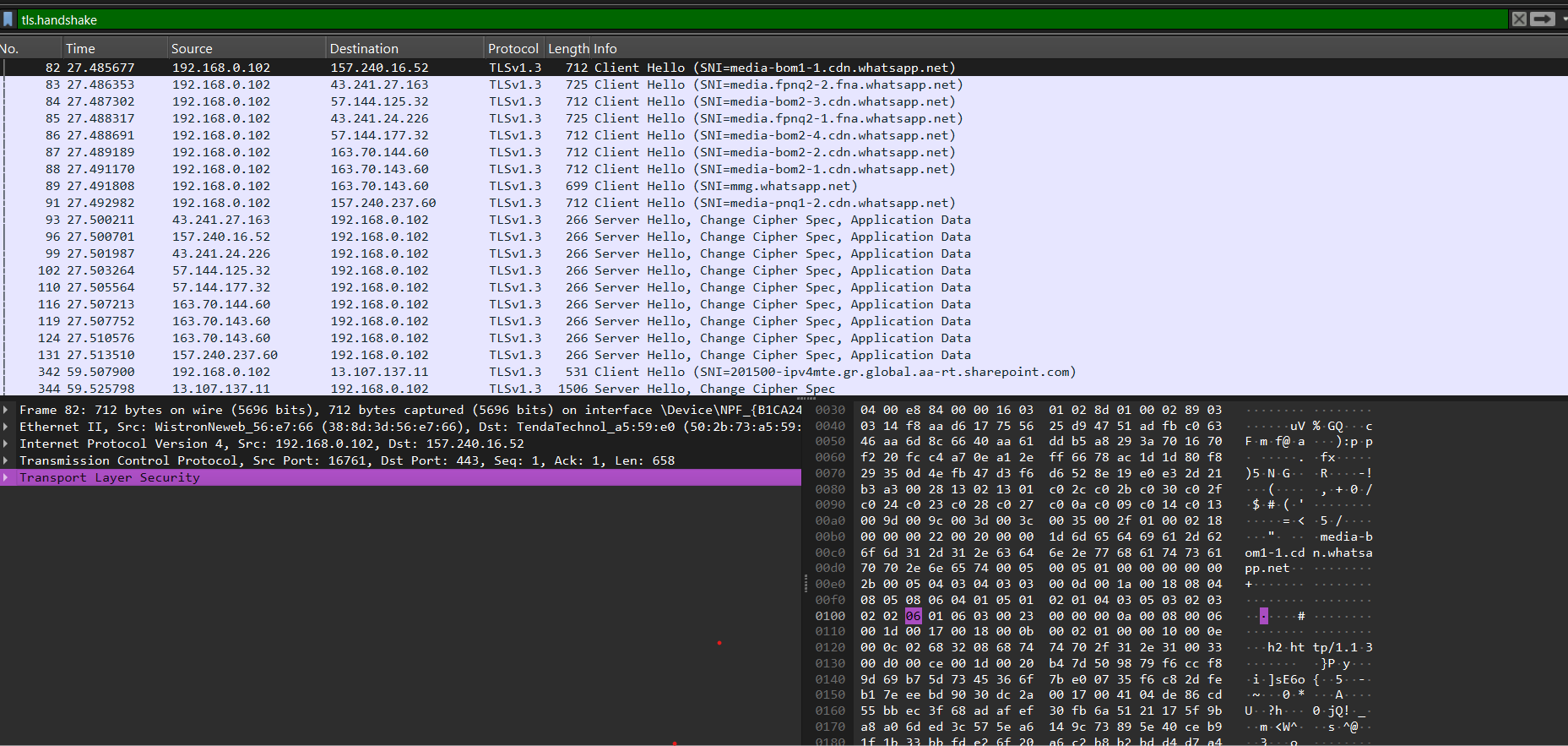
YOU WILL SEE THE OUTPUT ON ANALYSIS

STEP 6:NOW GO TO STATISTIC AND SEE THE CAPTURE AND IDENTIFY TRAFFIC IN (ICMP , DNS ,HTTP,TLS)

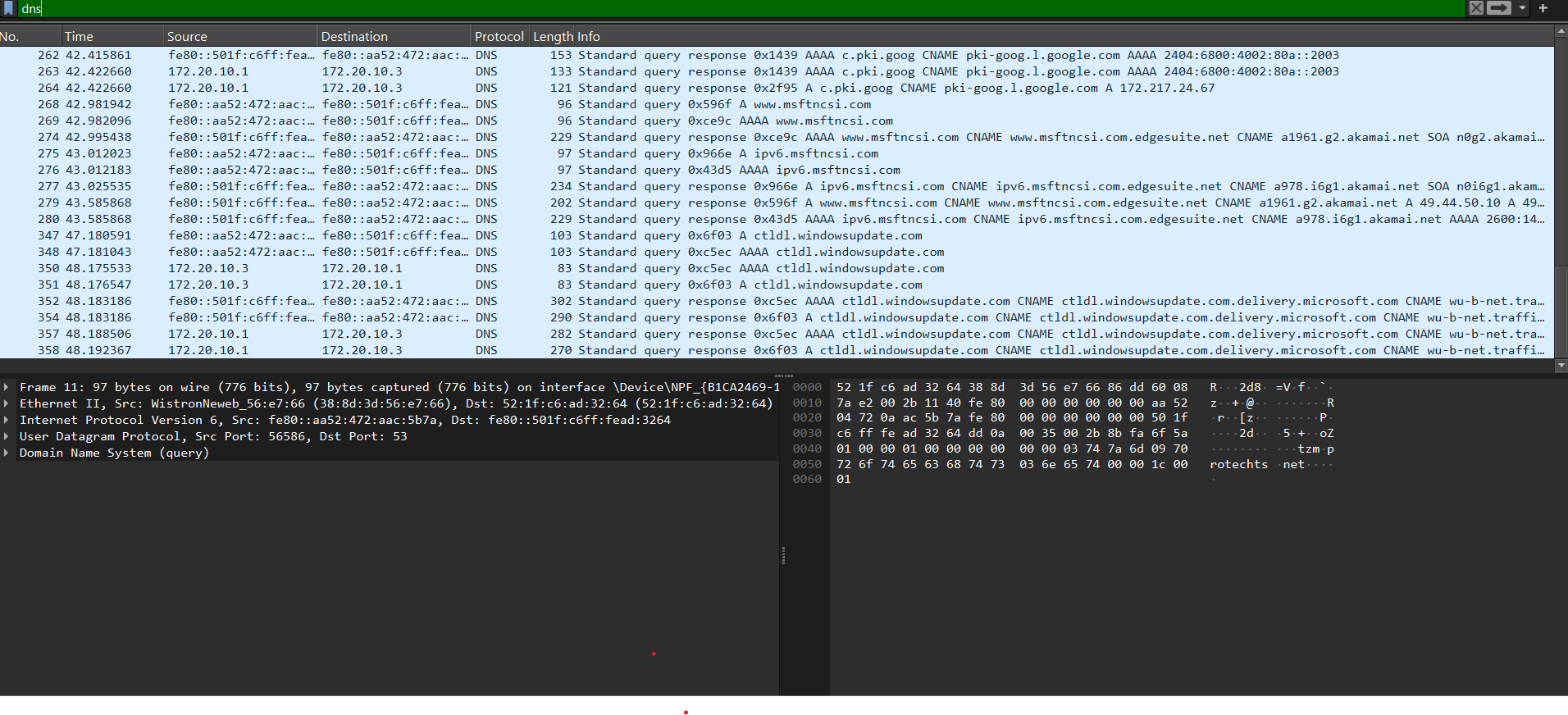
A screenshot of a computer

AI-generated content may be incorrect.

##NOW GO AND SEE HTTPS HANDSHAKE MEANS CLIENT HELLO AND SERVER HELLO’



DNS QUERY



##Observations

ICMP shows ping works correctly

DNS queries are resolving domain names

HTTP/TLS shows web browsing traffic

ARP shows local network activity