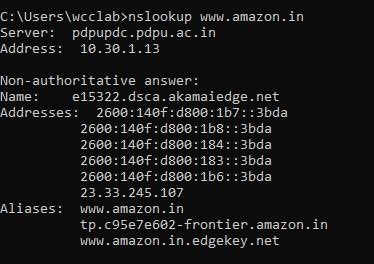
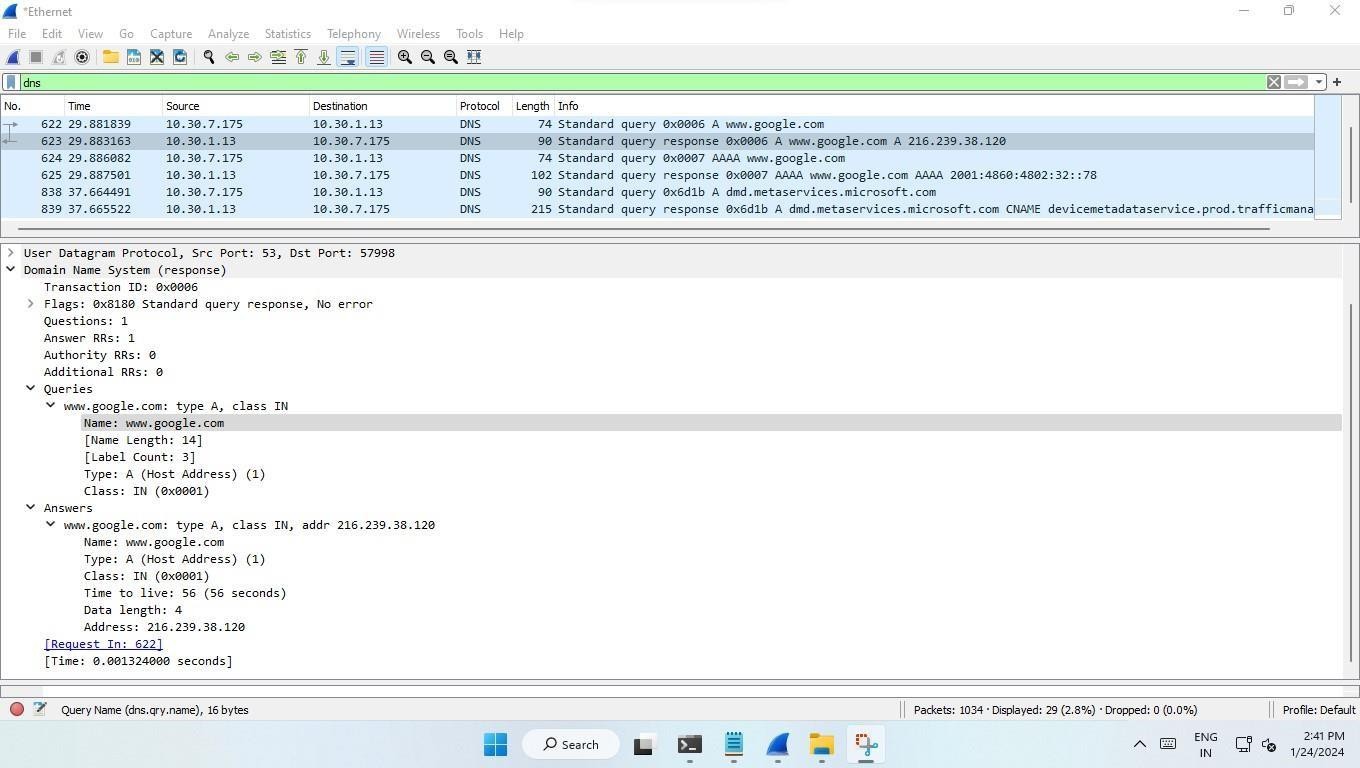
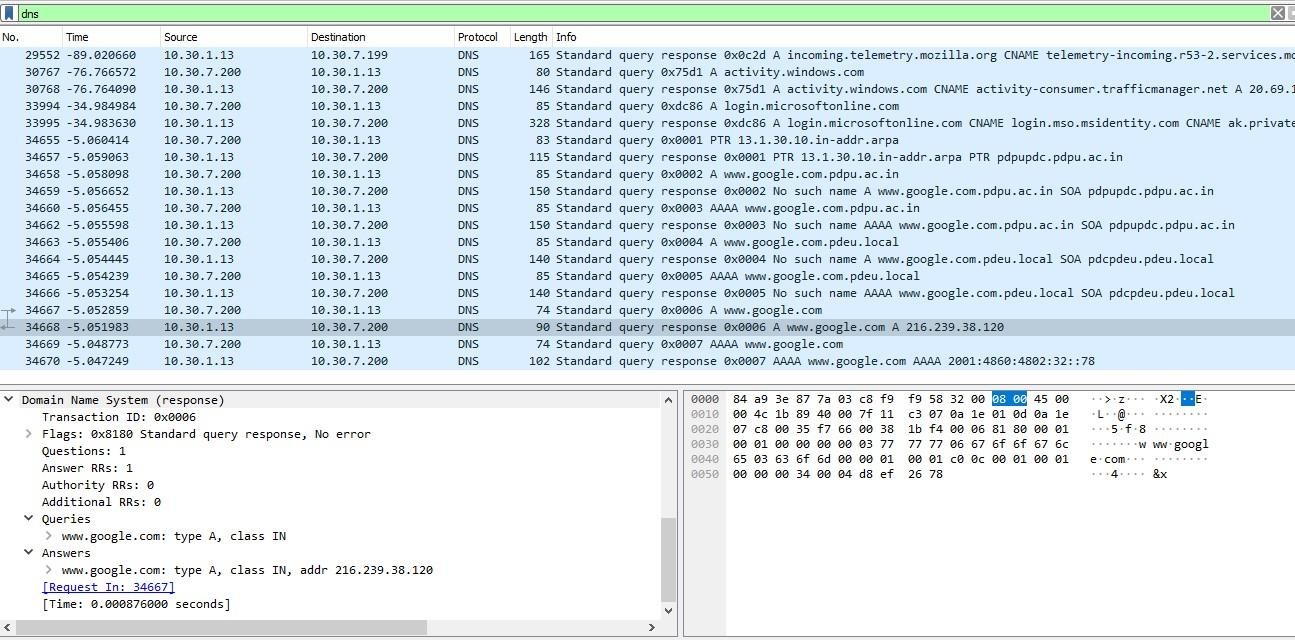
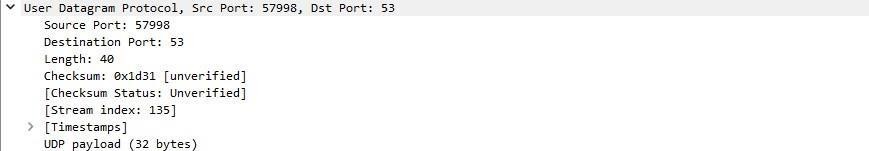
Wireshark

Exp 3 : To understand the working of DNS by using wire shark and packet trace

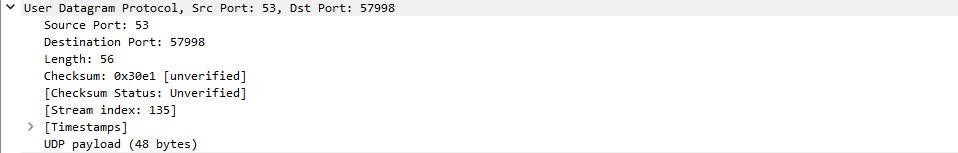
1. Name server lookup (nslookup) query and response for www.google.com:
2. 



It uses the user datagram protocol (UDP).

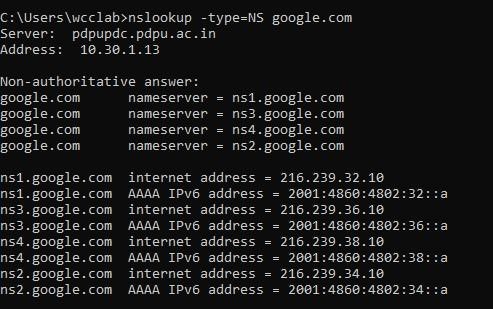
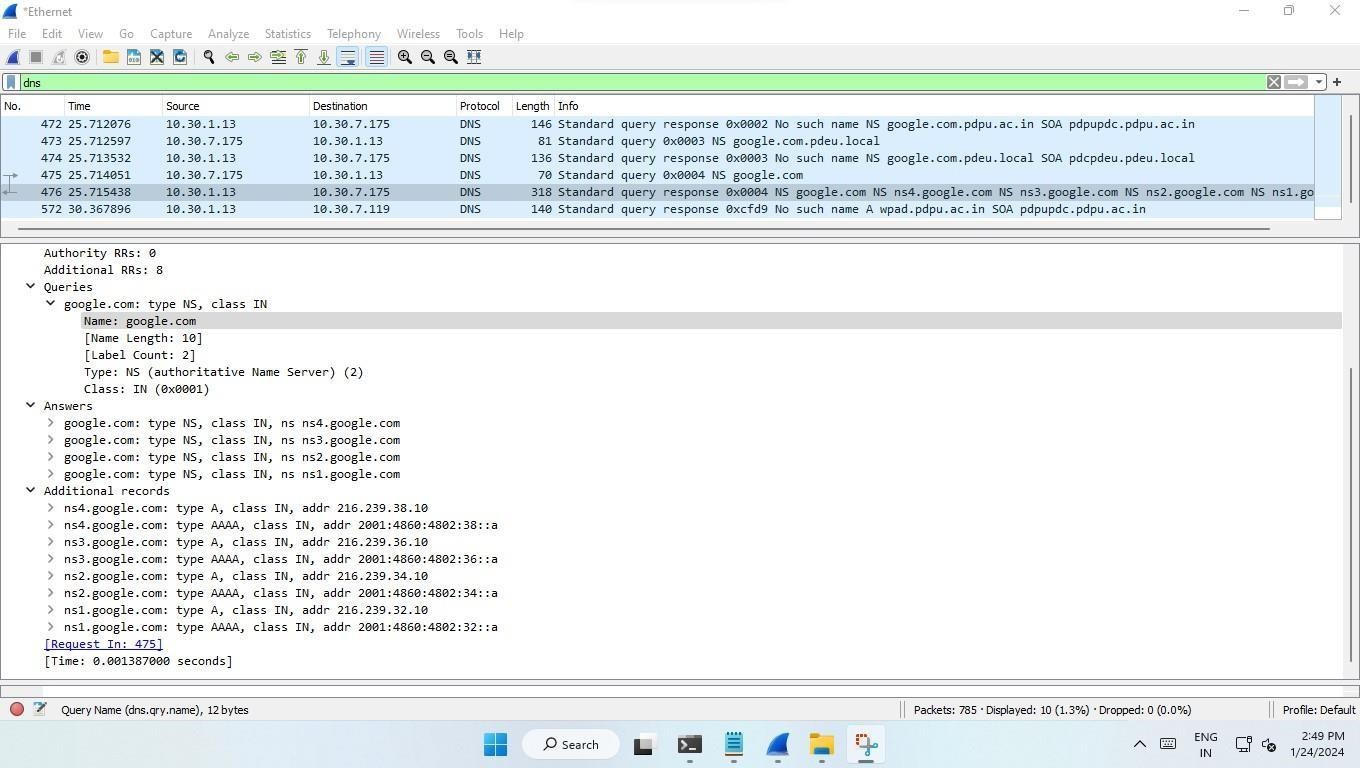


This are the configuration of the request sent. Where source port and destination port are mentioned.

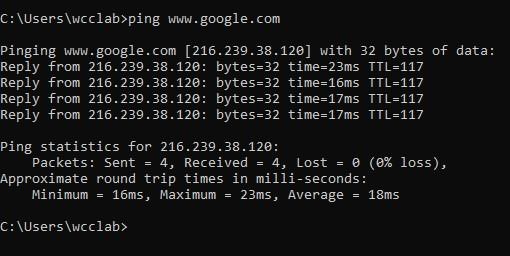


This are the configuration of the response received. Where source port and destination port are mentioned. And we can observe that ports are exact opposite of the request.

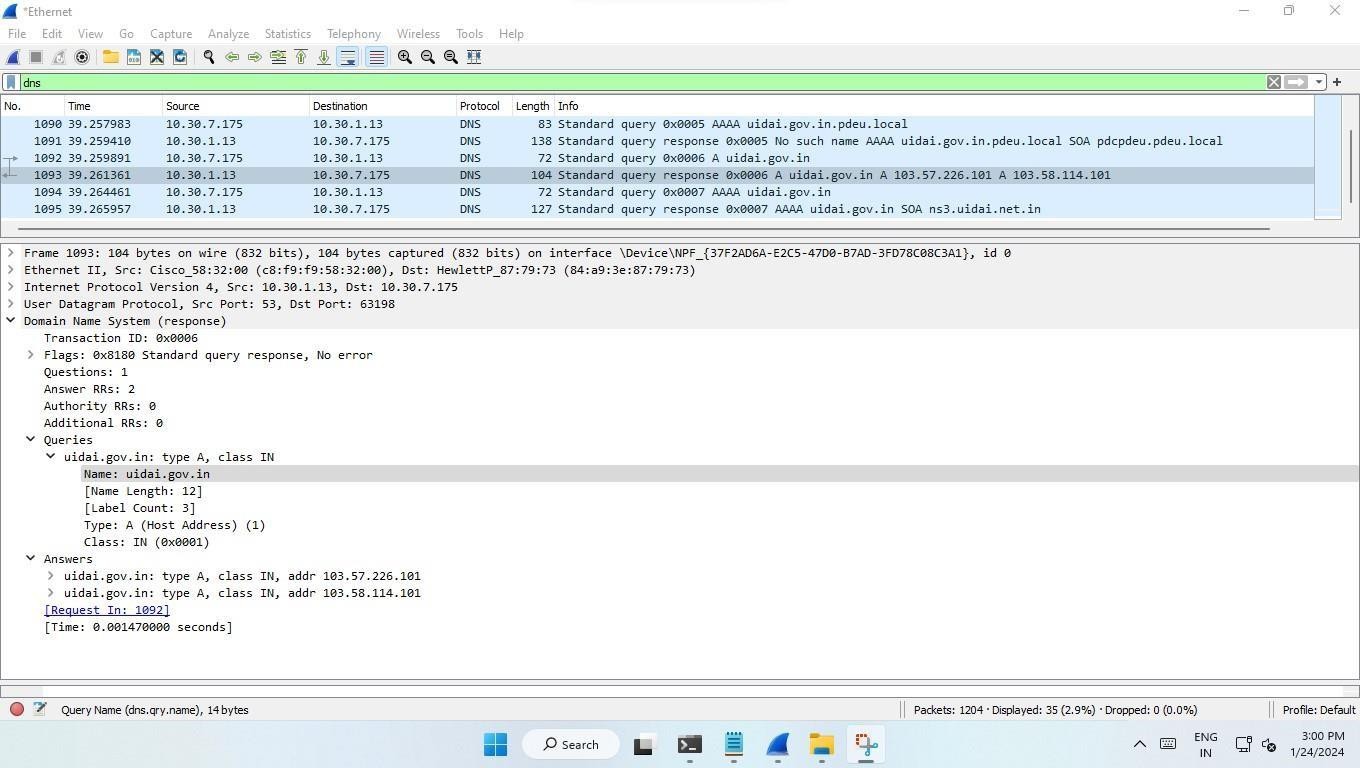
1. Name server lookup (nslookup) query and response for google.com:

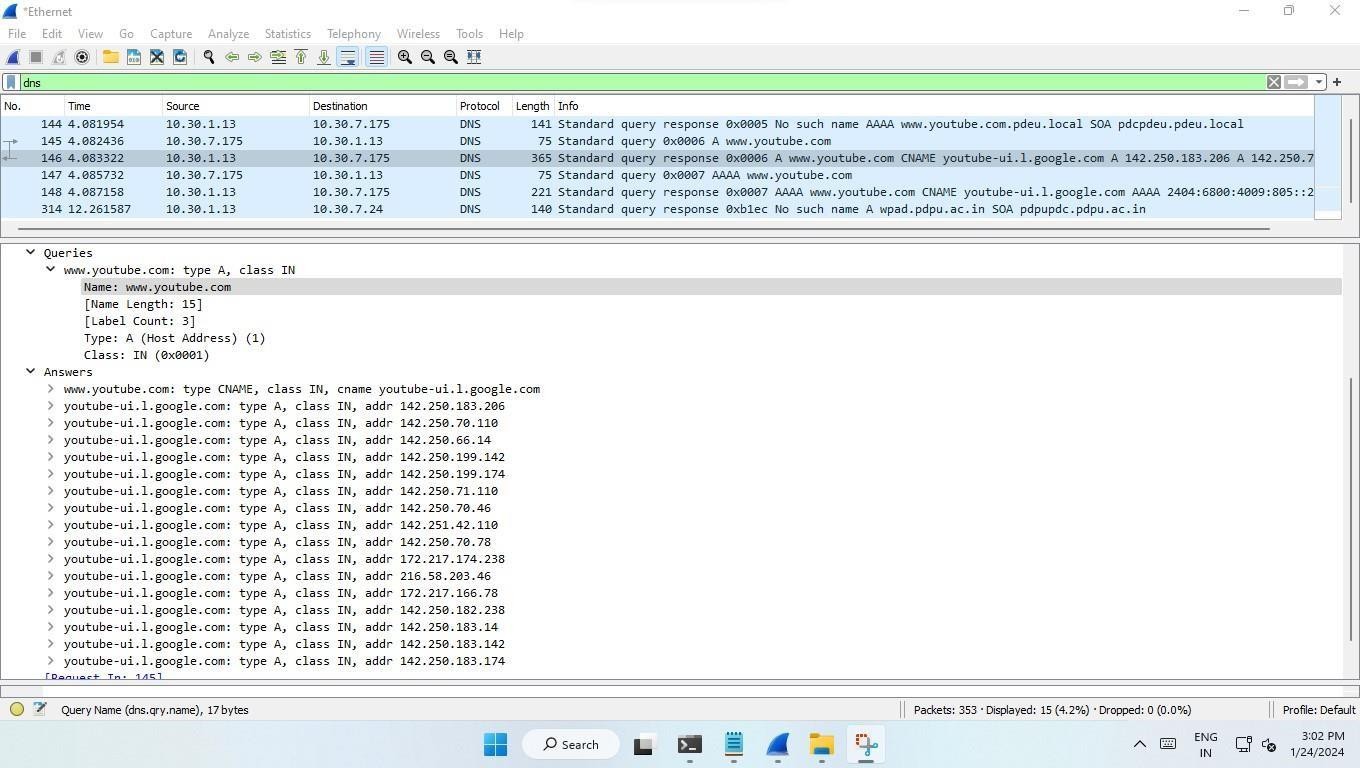


Using Ping to check reliability and connectivity of our network:



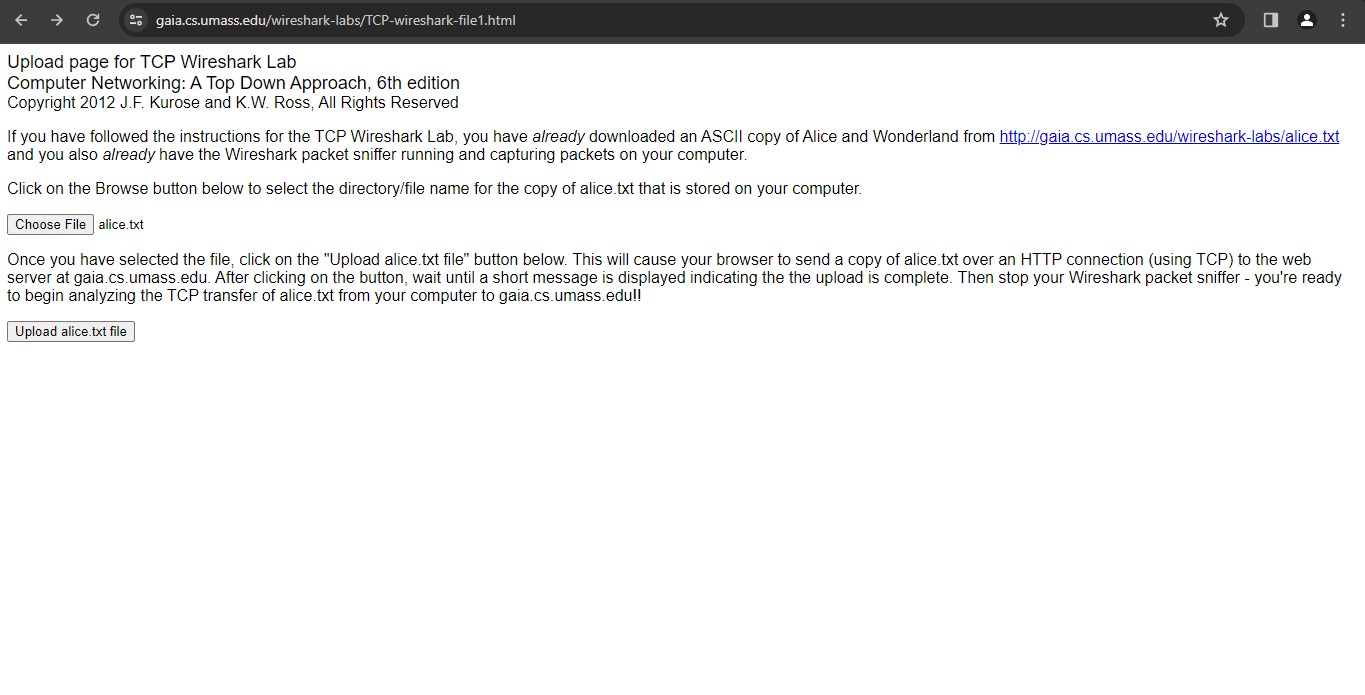
1. Name server lookup (nslookup) query and response for uidai.gov.in and [www.youtube.com](http://www.youtube.com/) (multiple-IP-address servers):



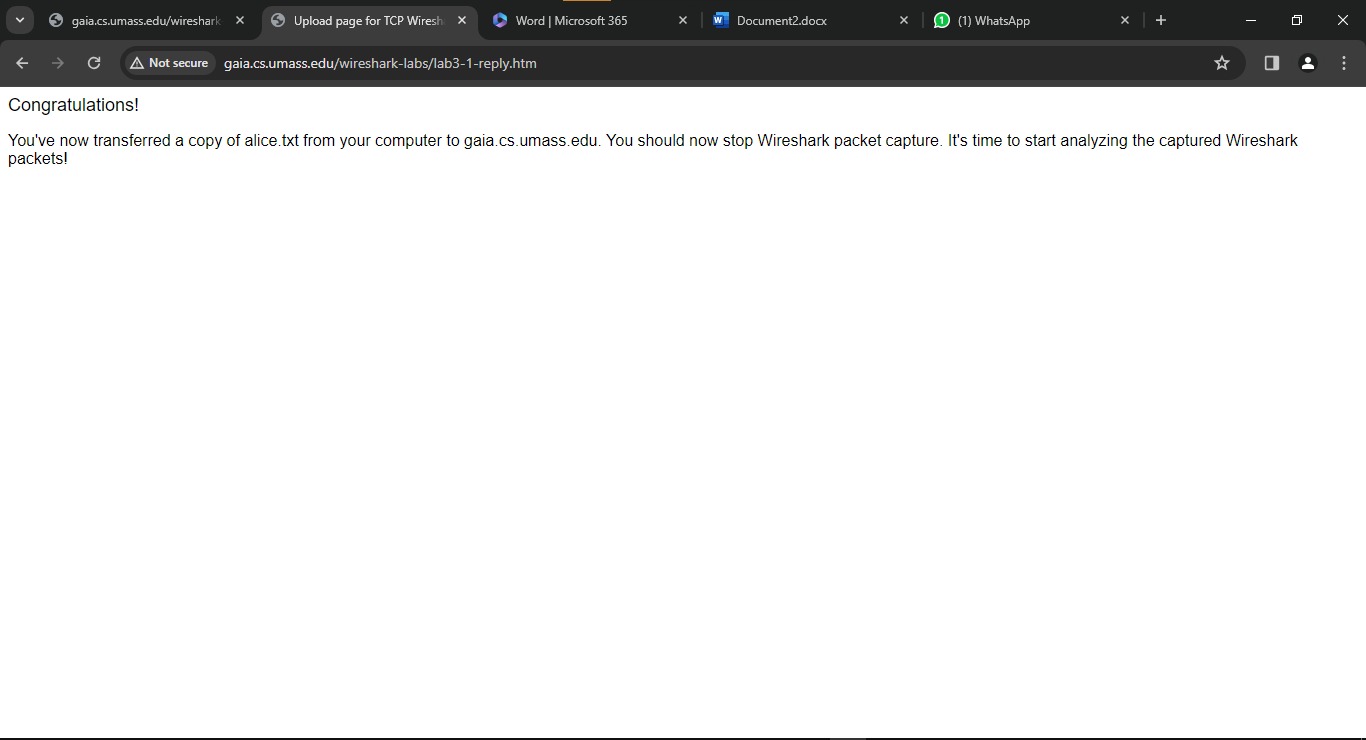


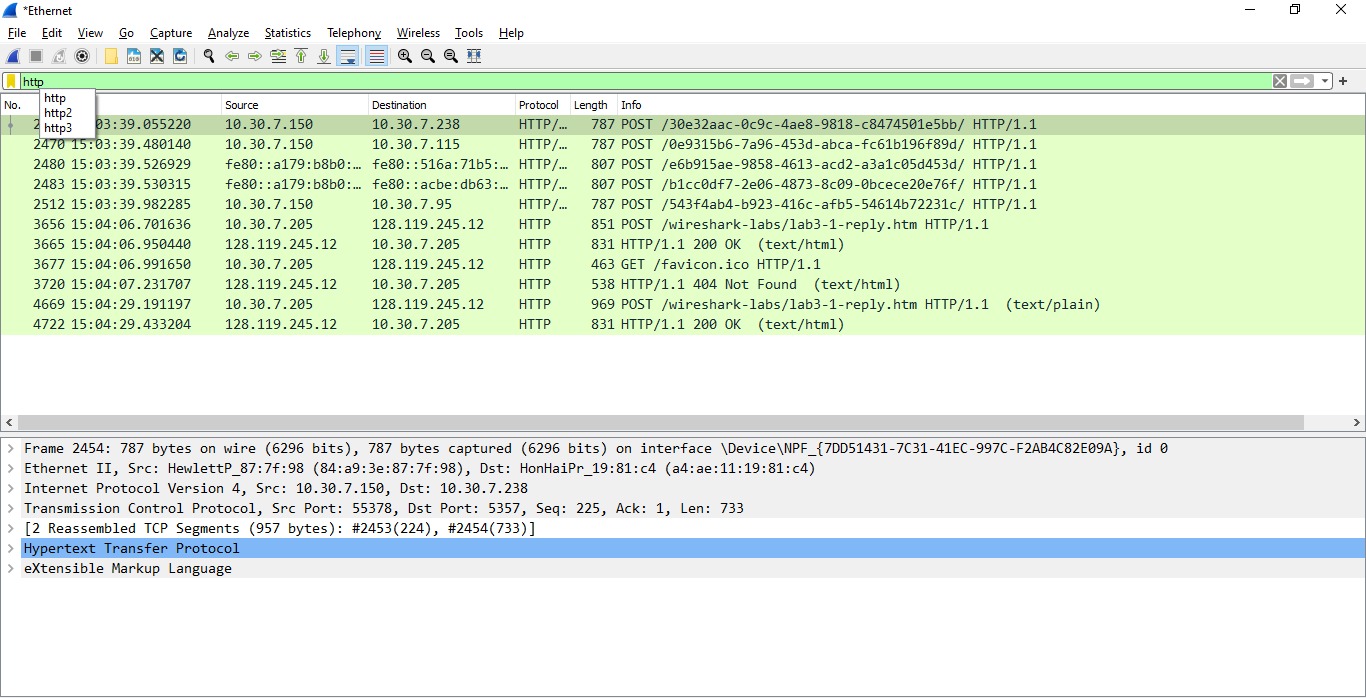
In both cases we are getting all the IP-addresses in response.

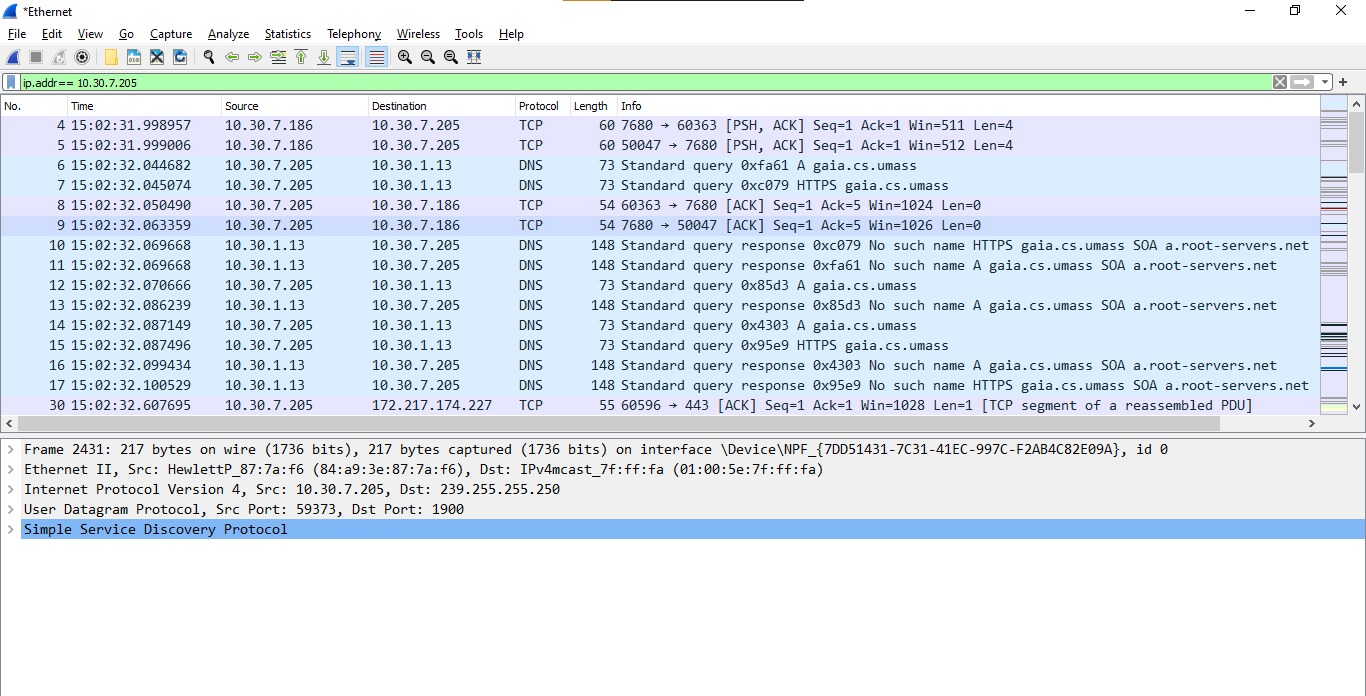
Exp 4: UDP-IP-ICMP PROTOCOL

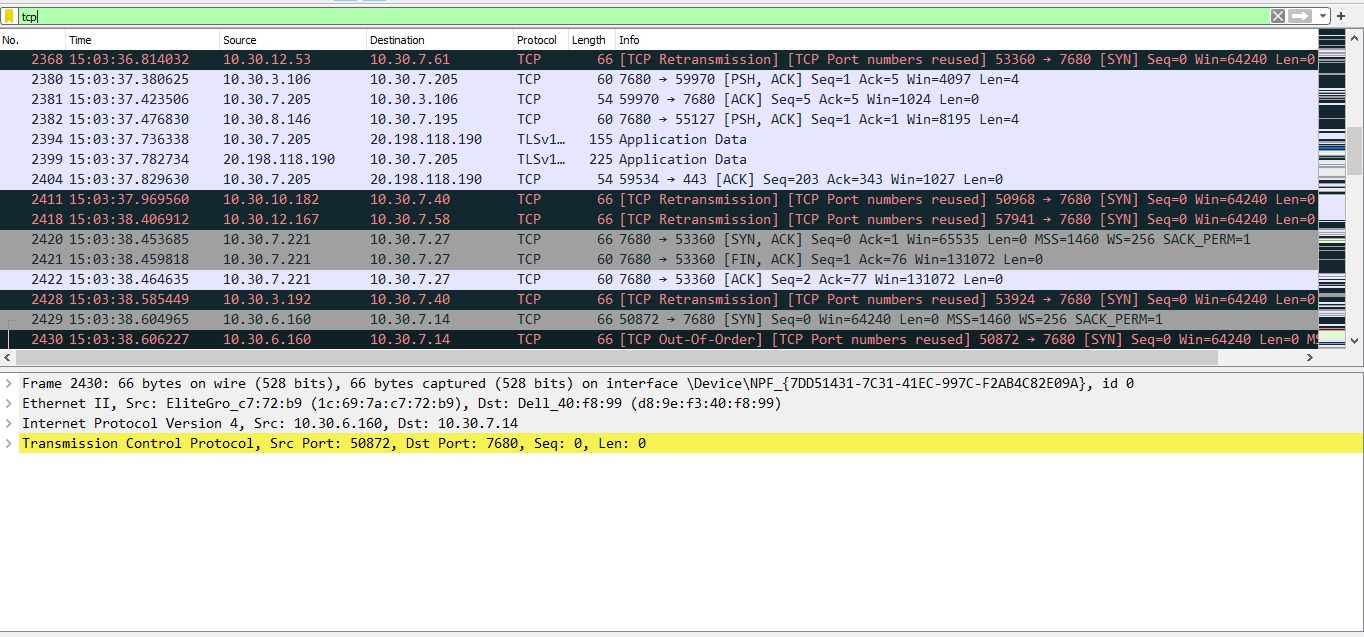


* Use the Browse button in this form to the file on your computer that you just created containing Alice in Wonderland. Don’t press the “Upload alice.txt file” button yet.
* Now start up Wireshark and begin packet capture (see the earlier Wireshark labs if you need a refresher on how to do this).
* Returning to your browser, press the “Upload alice.txt file” button to upload the file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short congratulations message will be displayed in your browser window.
* Stop Wireshark packet capture.









Exp 5 : UDP-IP-ICMP-ARP PROTOCOL

