Computer Networks Assignment 01

Name : Sarita Sangrez

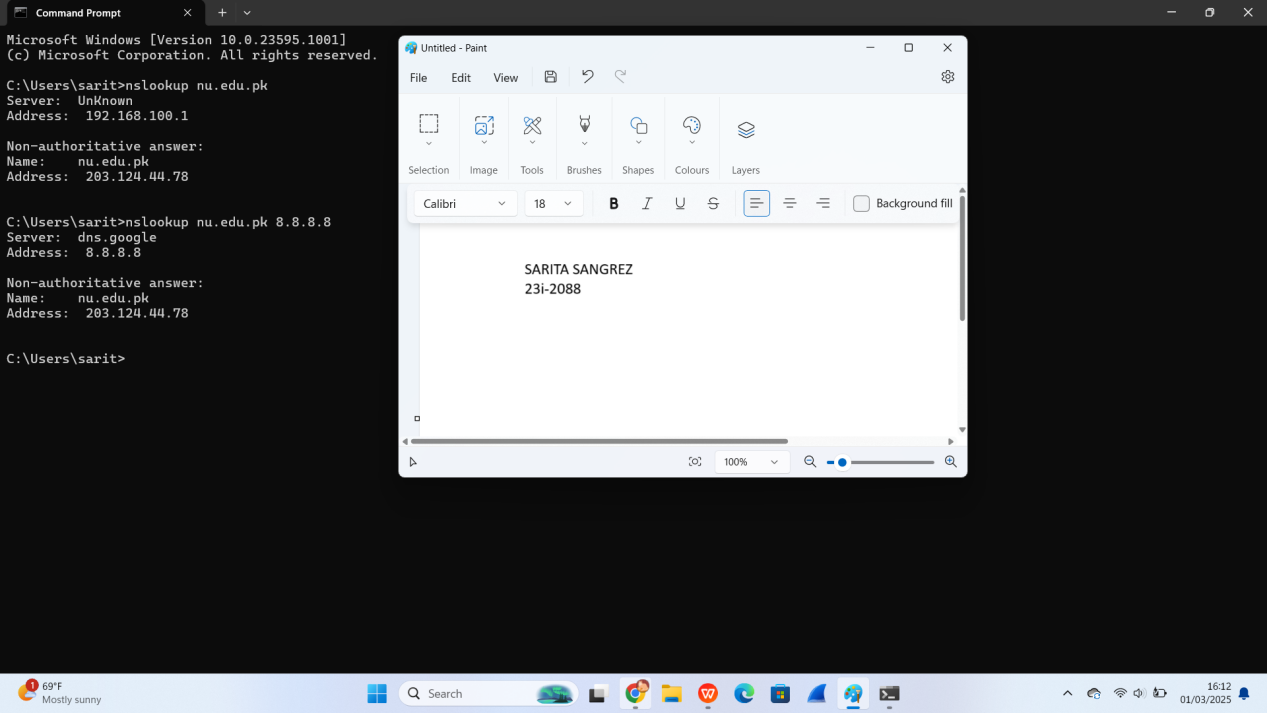
Section : CY-A

Roll No. 23i-2088

Date : 1st March 2025

**QUESTION #1 Answers**

1. 203.124.44.78



1. 149.40.228.116



1. 192.168.100.1

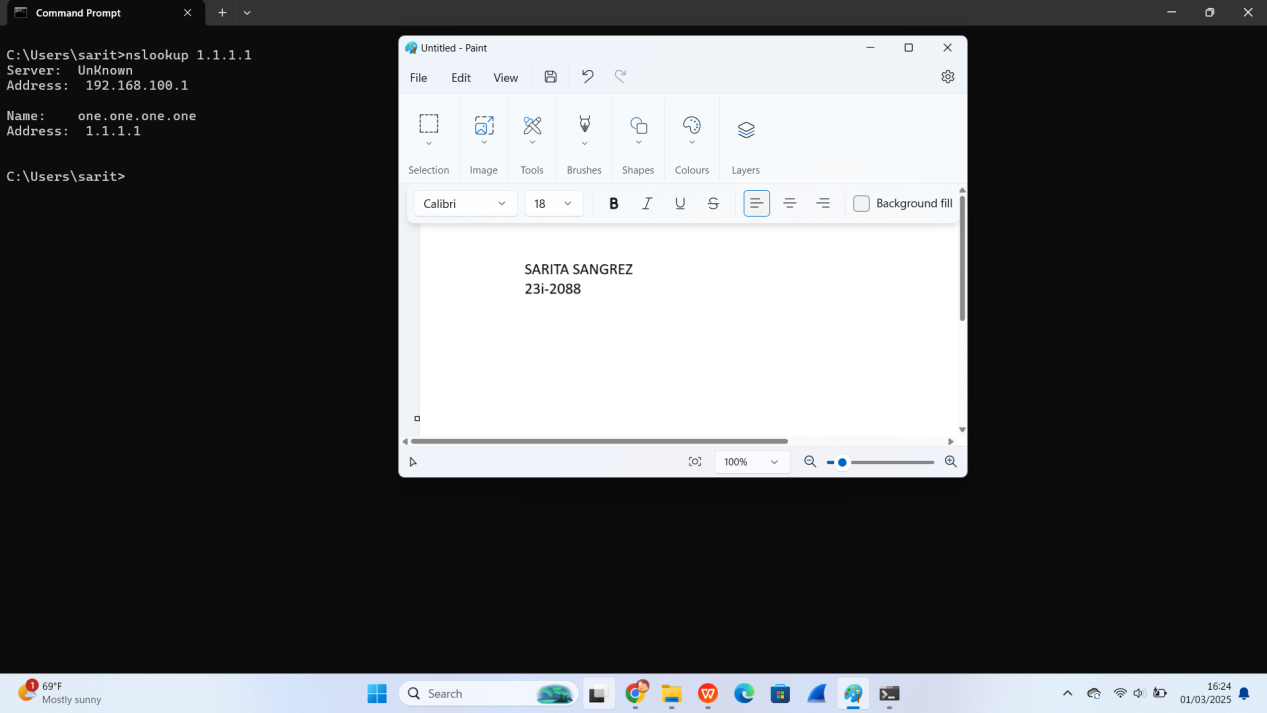


1. Non authoritative answer as mentioned :



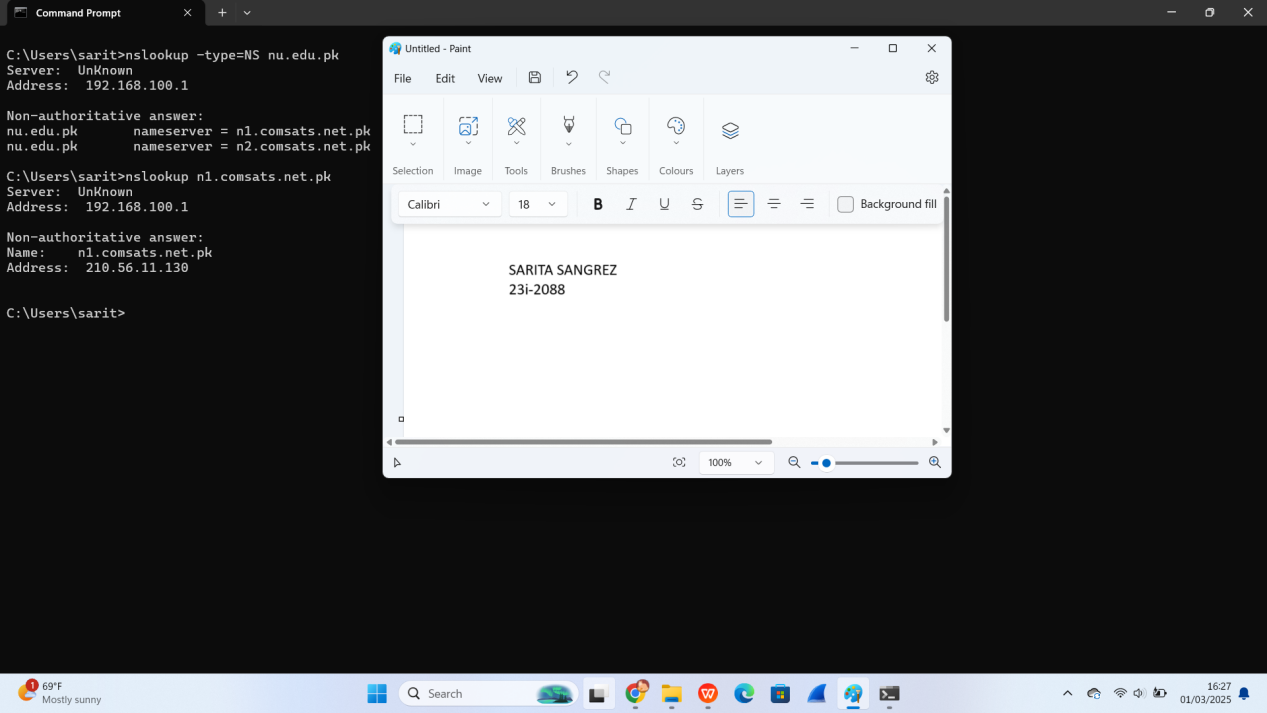
1. Command used : nslookup 1.1.1.1

hostname is one.one.one.one



1. Command used : nslookup -type=NS nu.edu.pk

Name of one of the authoritative servers is n1.comsats.net.pk with the IP address 210.56.11.130



1. nu.edu.pk MX preference = 10, mail exchanger = aspmx5.googlemail.com

nu.edu.pk MX preference = 5, mail exchanger = alt2.aspmx.l.google.com

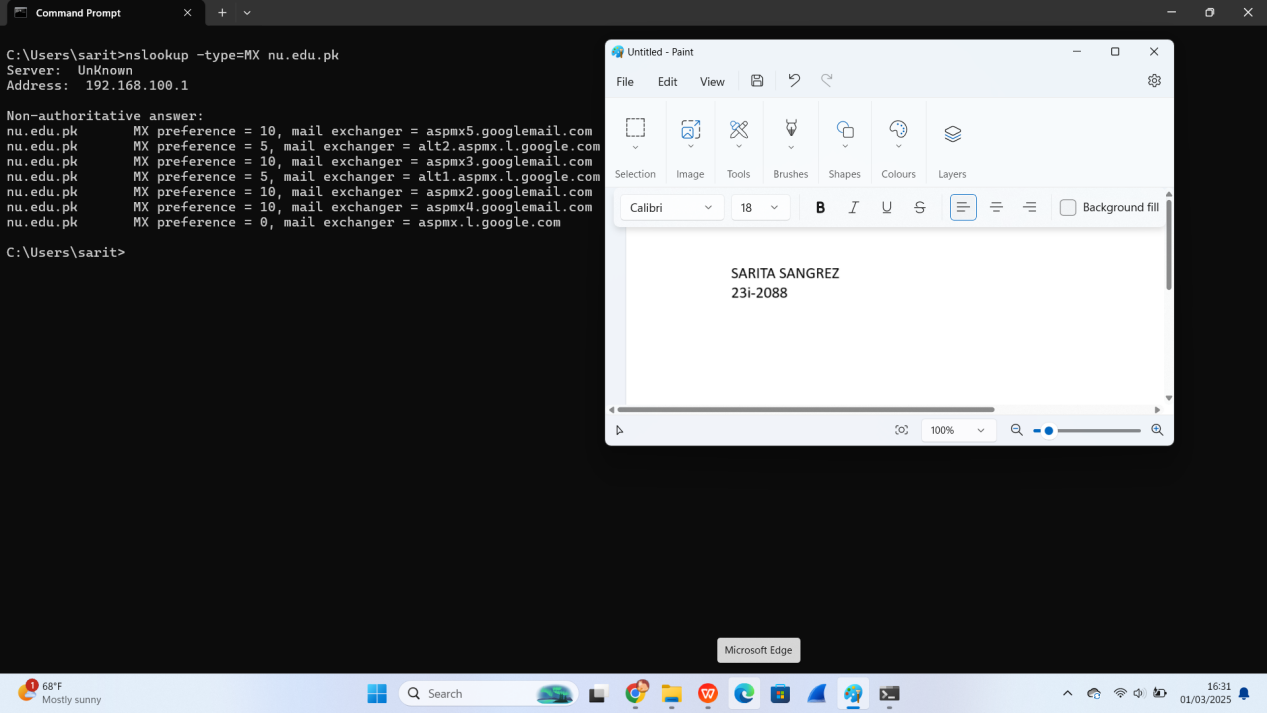
nu.edu.pk MX preference = 10, mail exchanger = aspmx3.googlemail.com

nu.edu.pk MX preference = 5, mail exchanger = alt1.aspmx.l.google.com

nu.edu.pk MX preference = 10, mail exchanger = aspmx2.googlemail.com

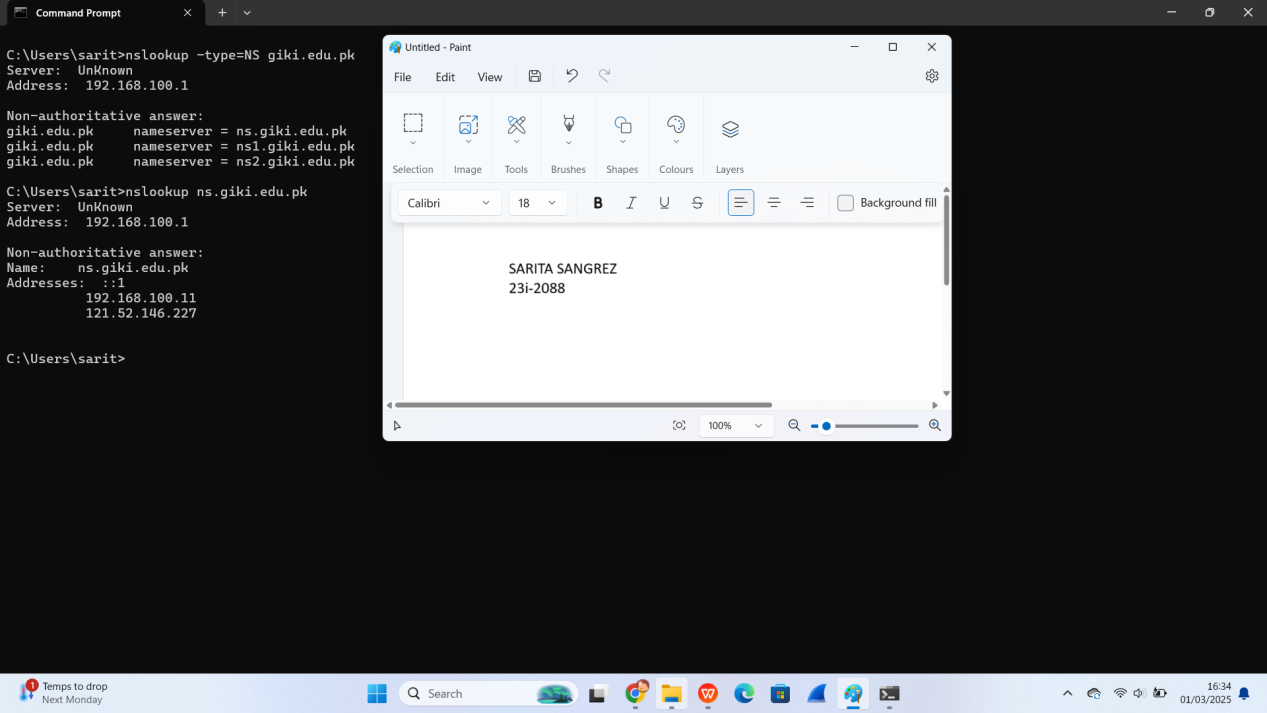
nu.edu.pk MX preference = 10, mail exchanger = aspmx4.googlemail.com

nu.edu.pk MX preference = 0, mail exchanger = aspmx.l.google.com



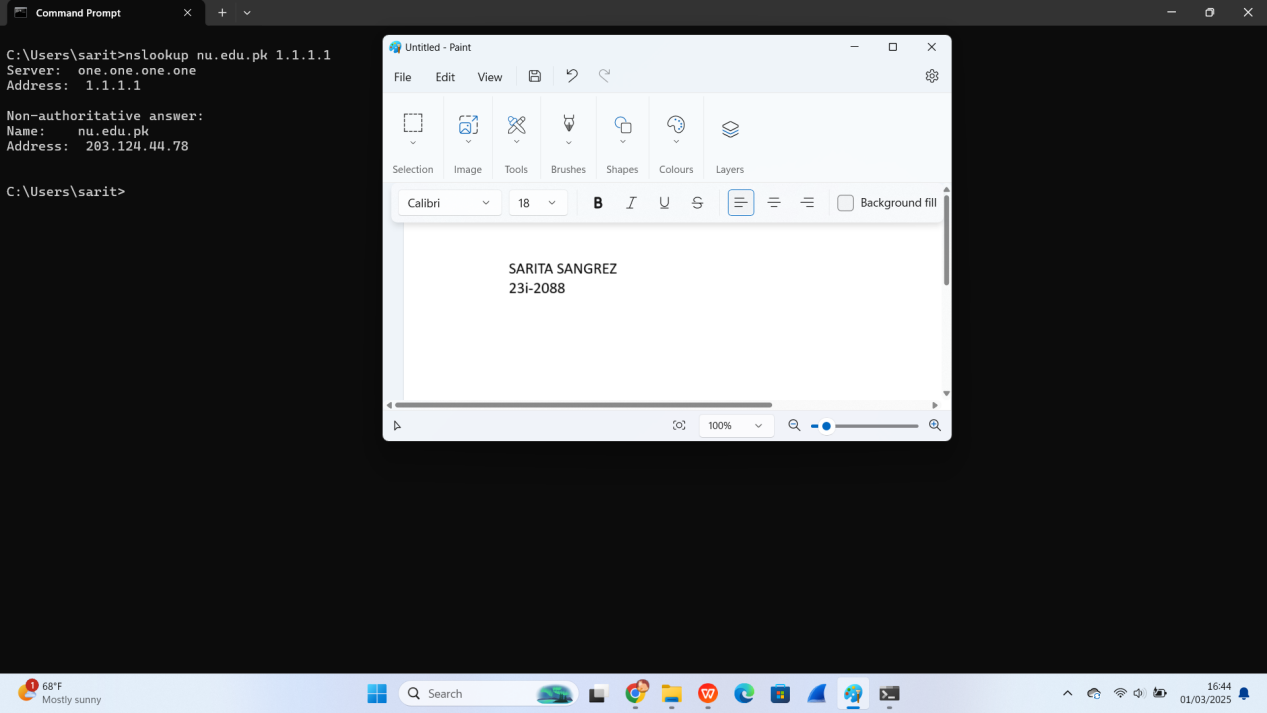
1. The name of the first authoritative nameserver is ns.giki.edu.pk.

To find the IP address of this nameservere, I would use the command “nslookup authoritative\_server\_name” that is ns.giki.edu.pk in this case.



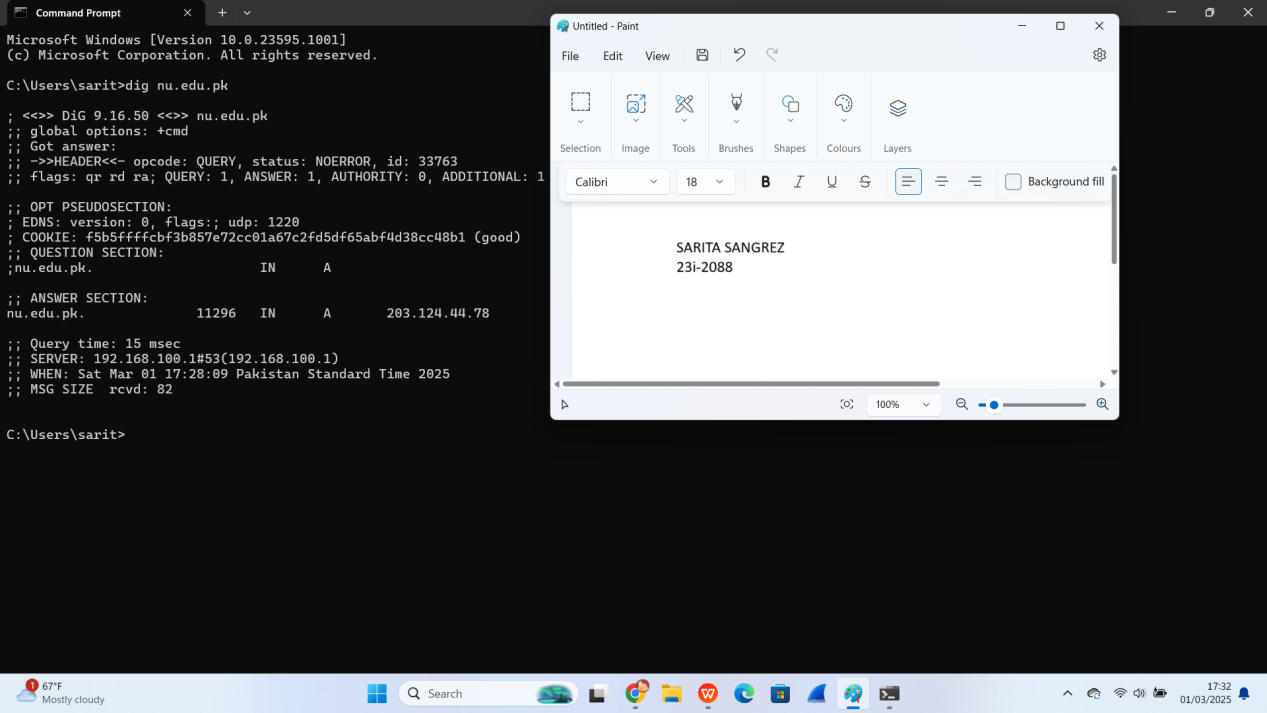
1. I will use CloudFare/1.1.1.1.

Command used : nslookup nu.edu.pk 1.1.1.1

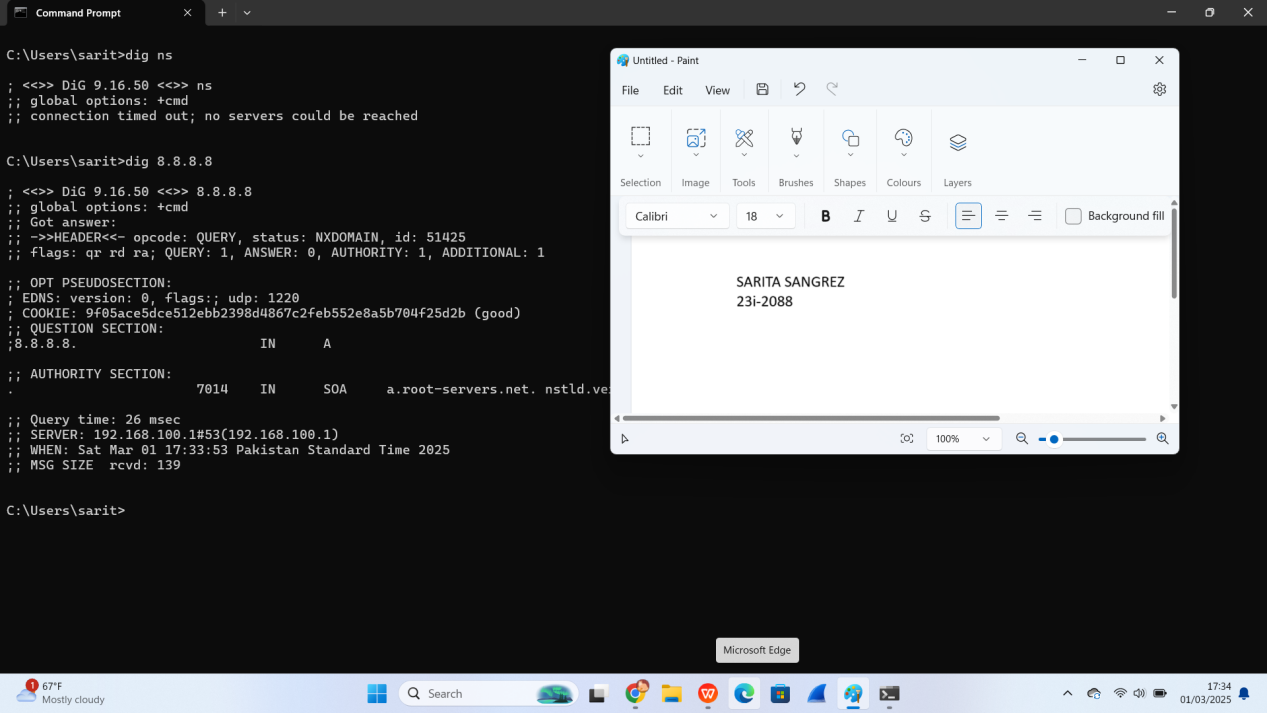


**QUESTION #2 Answers**

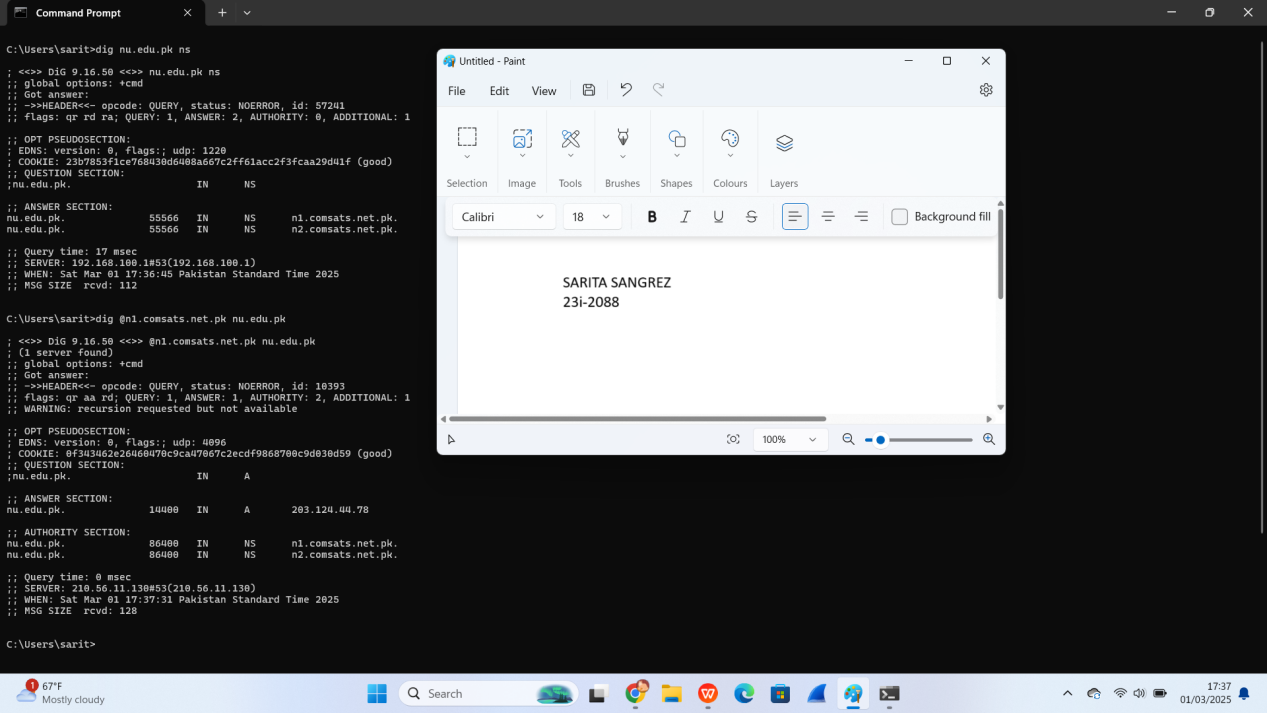
1. The query section shows what was requested and answer section contains response from the DNS server.



1. Used dig 8.8.8.8 as for” dig ns” no servers could be reached.

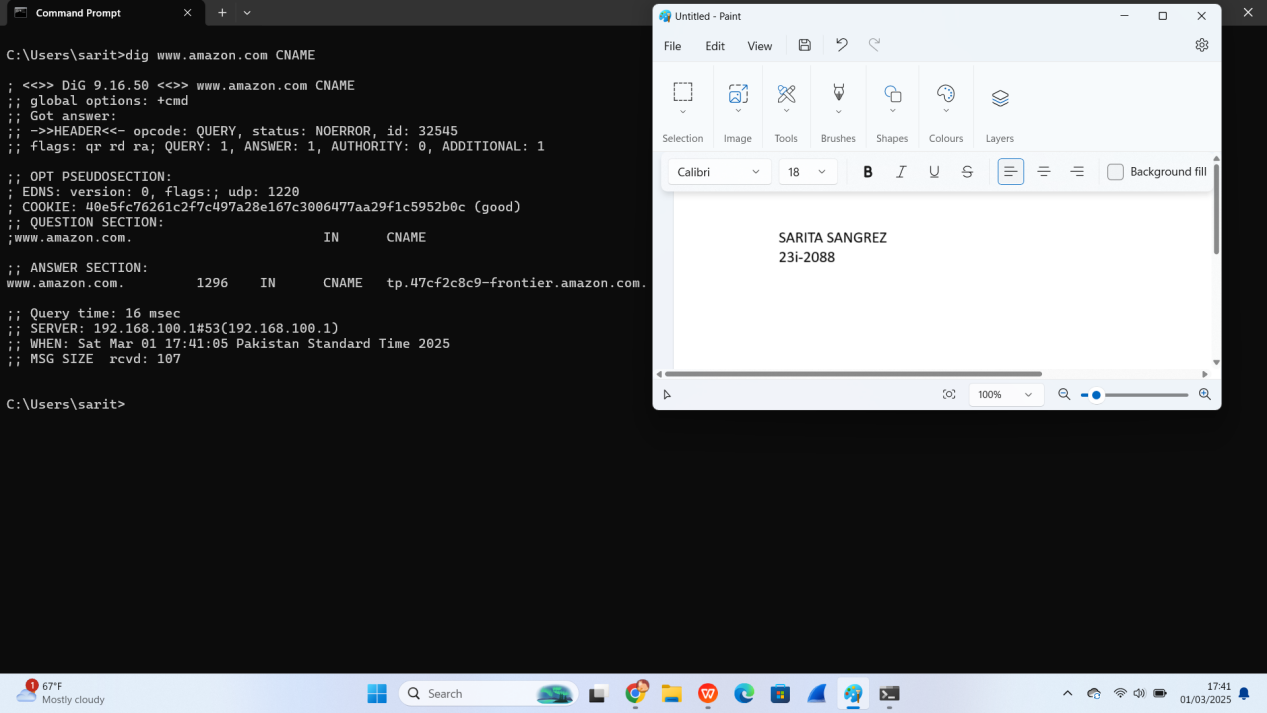


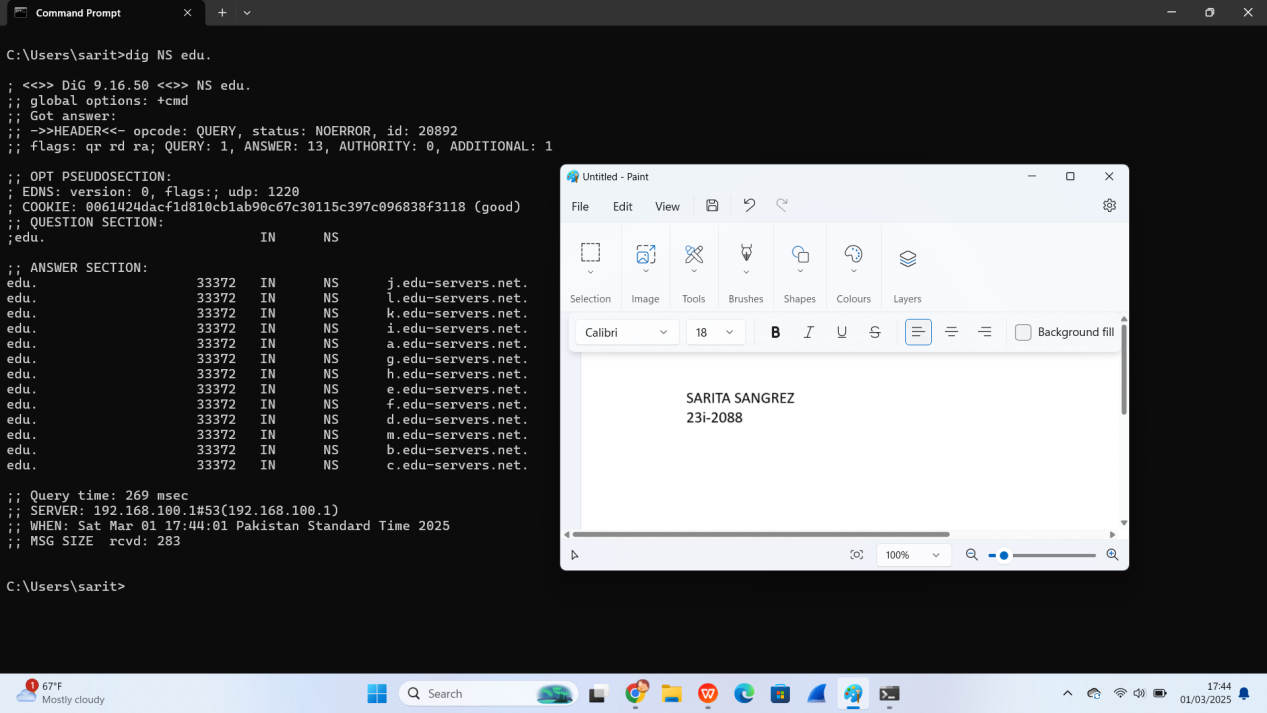
1. I first used command “dig nu.edu.pk ns” and then used dig @n1.comsats.net.pk nu.edu.pk.

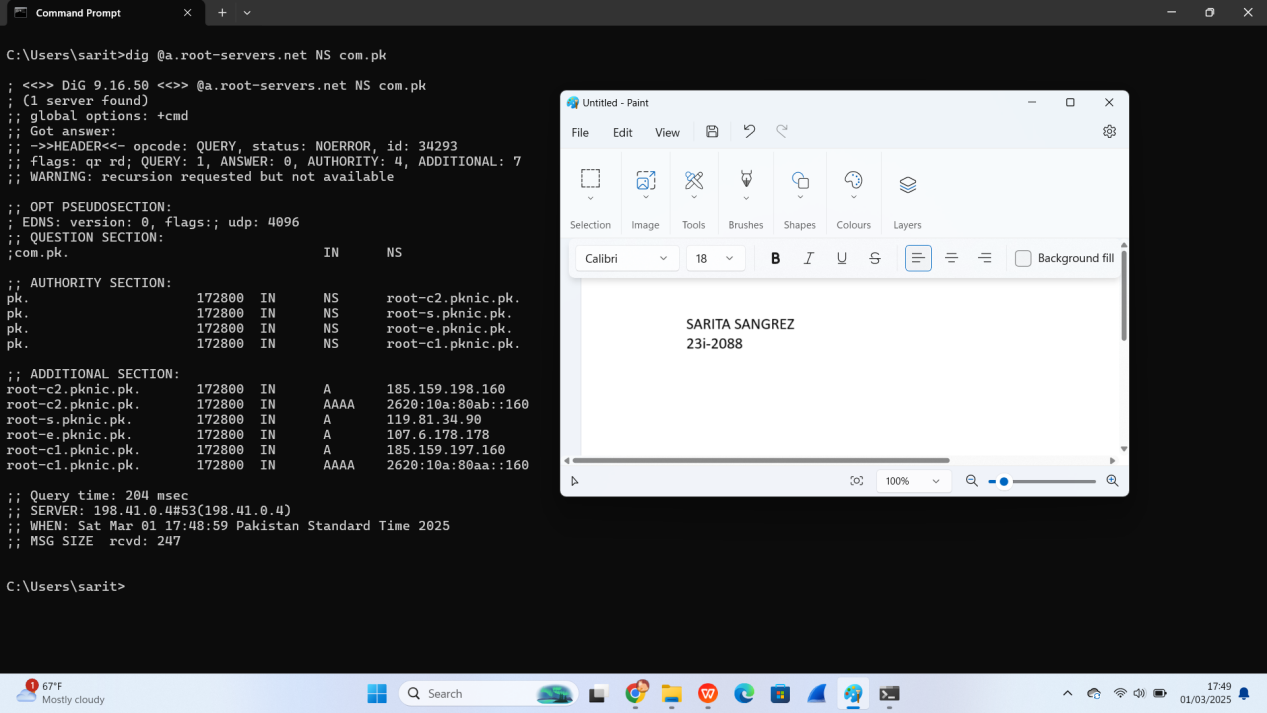


1. Command used : dig www.amazon.com CNAME.

The canonical name is tp.47cf2c8c9-frontier.amazon.com.

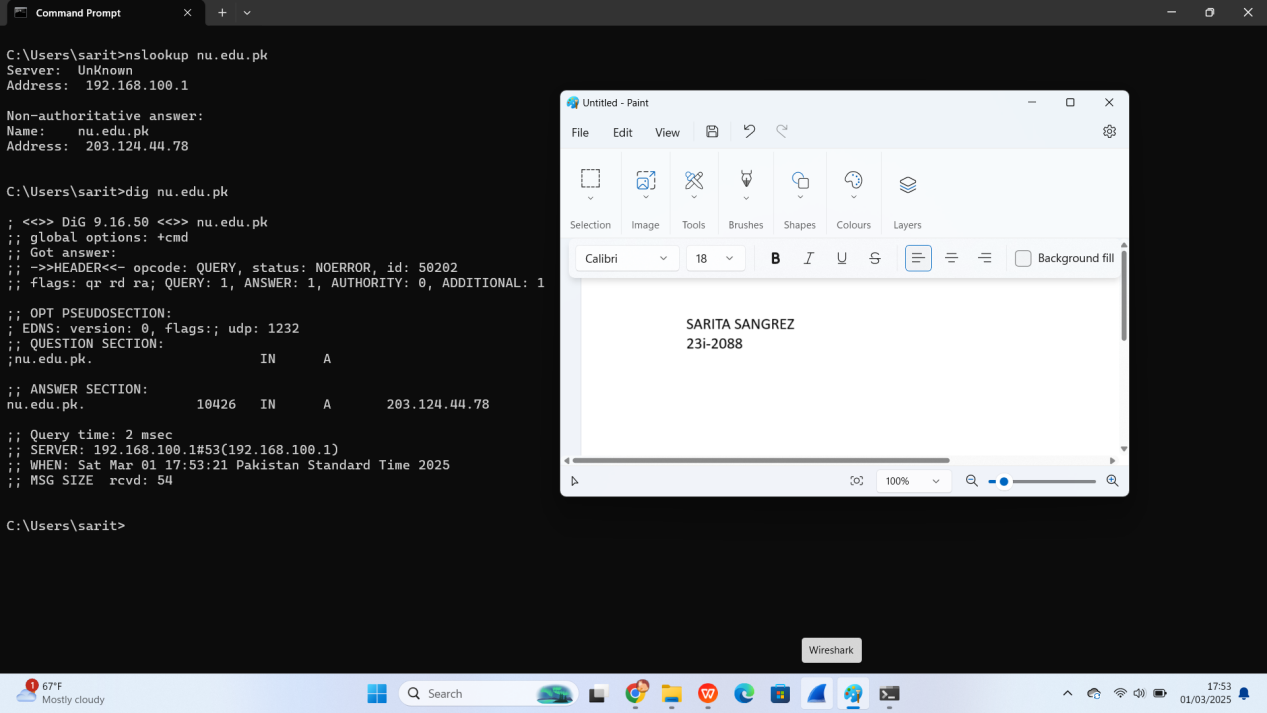


1. 



1. “Nslookup” provides a simplified output with only the name and the IP address mentioned.

“dig” gives a detailed output, including query time, TTL, authority records, and additional sections.



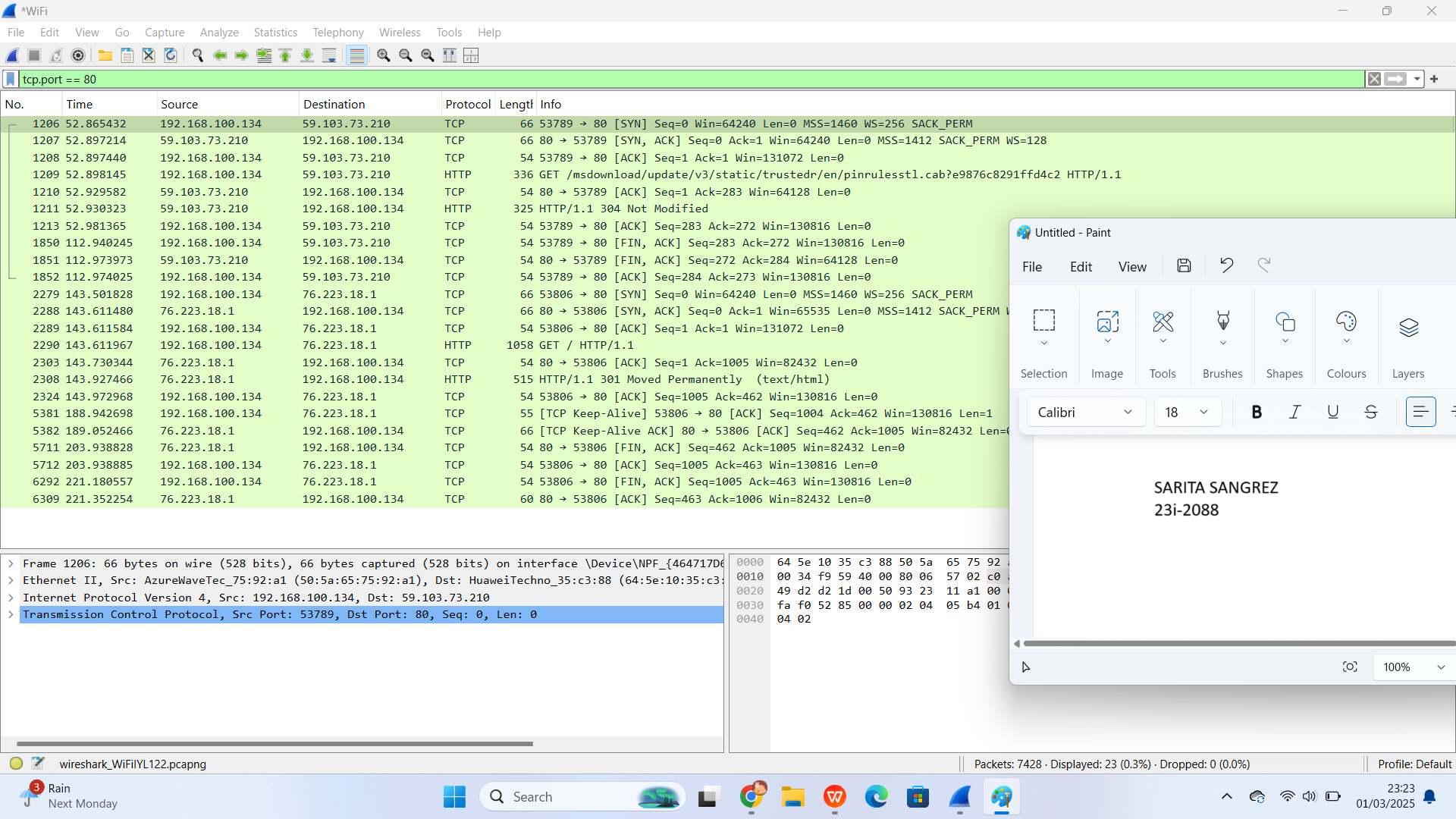
**QUESTION #3 Answers**

**TASK 1**

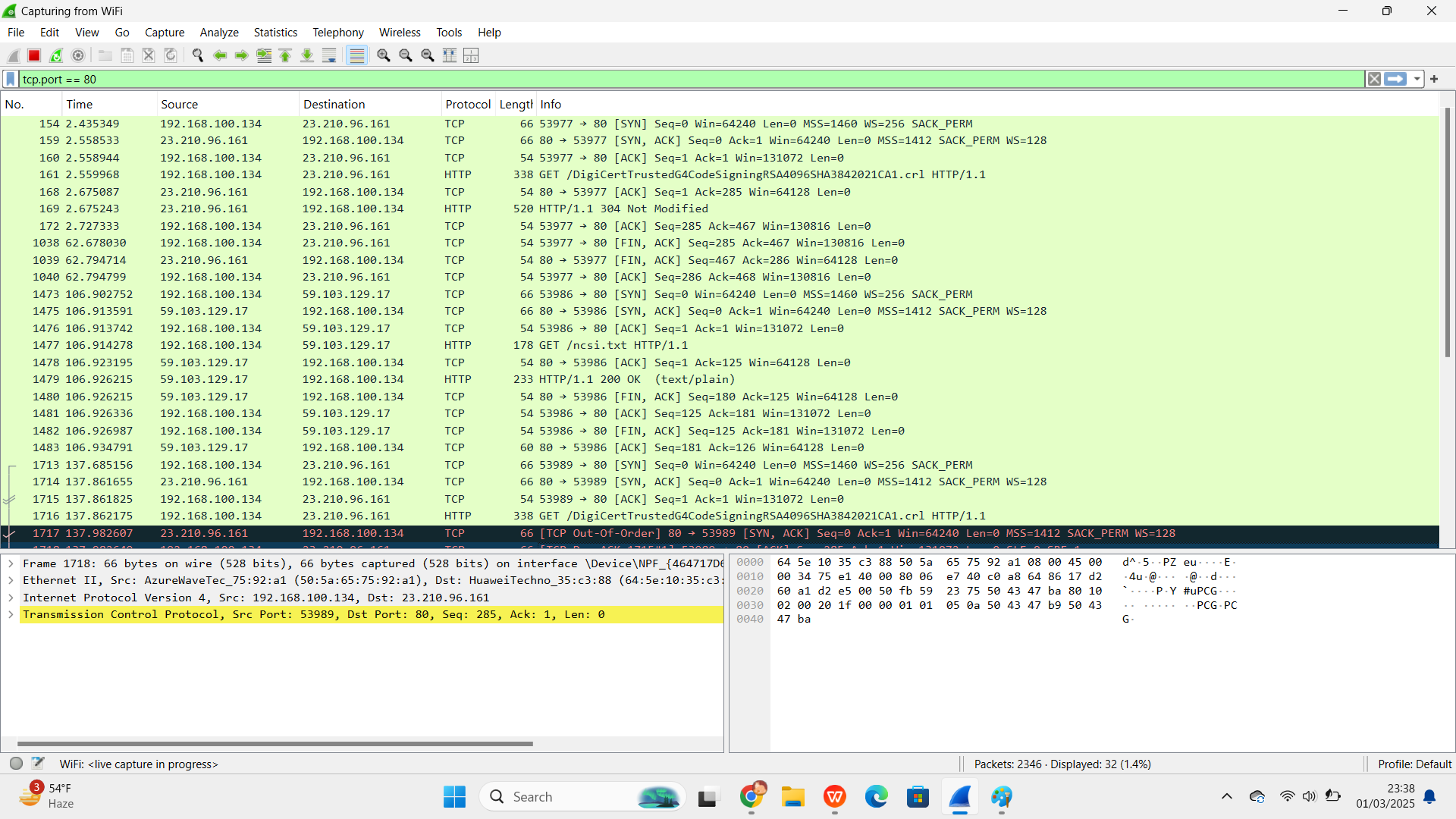
URL1: <http://upload.wikimedia.org/wikipedia/commons/3/3f/JPEG_example_flower.jpg>

URL 2 : <http://go.com/>

1. When I fetched the static image url for the second time, only 3 packets were captured as all other packets were loaded from the local cache.

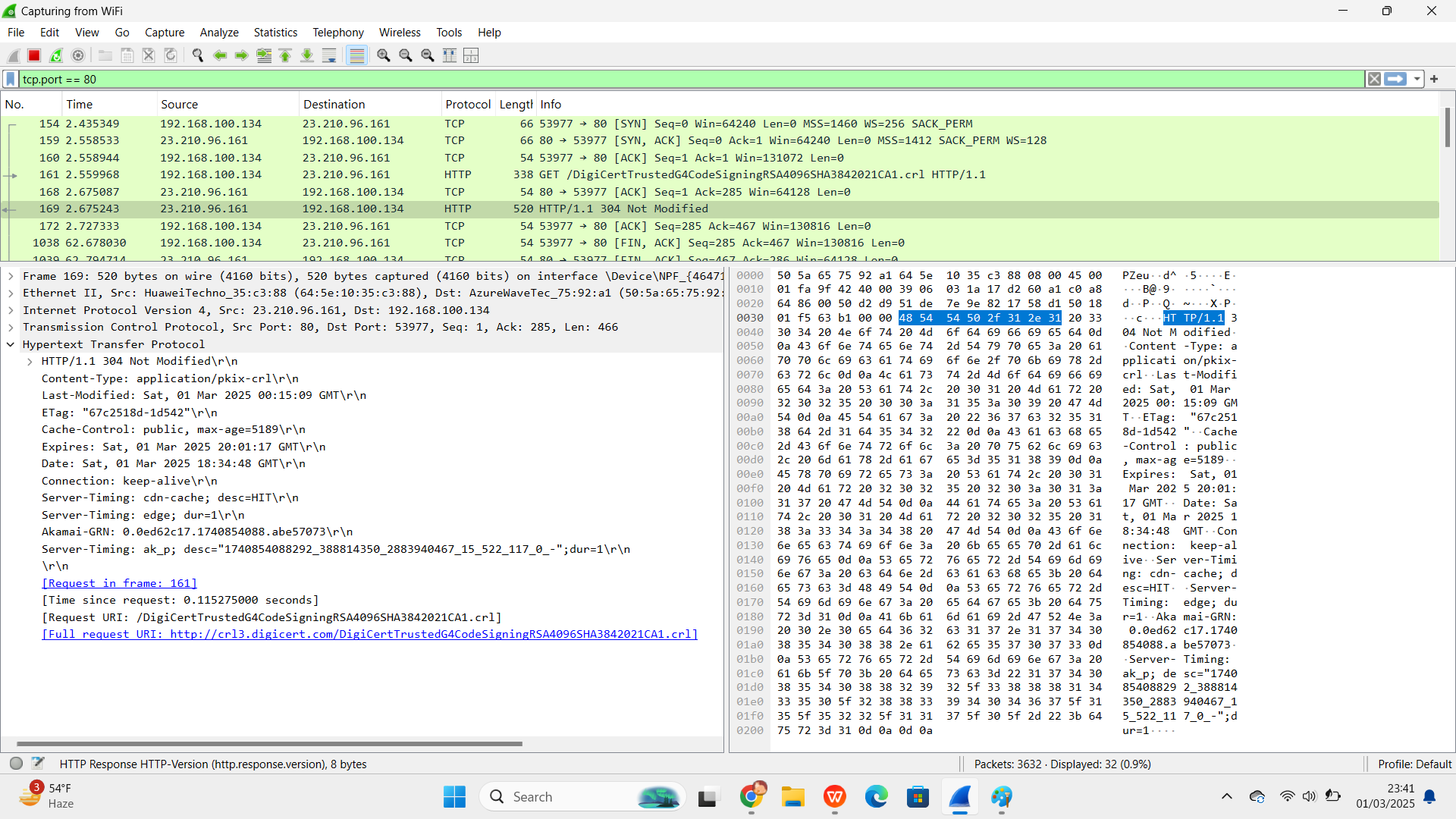


1. One HTTP request was made.

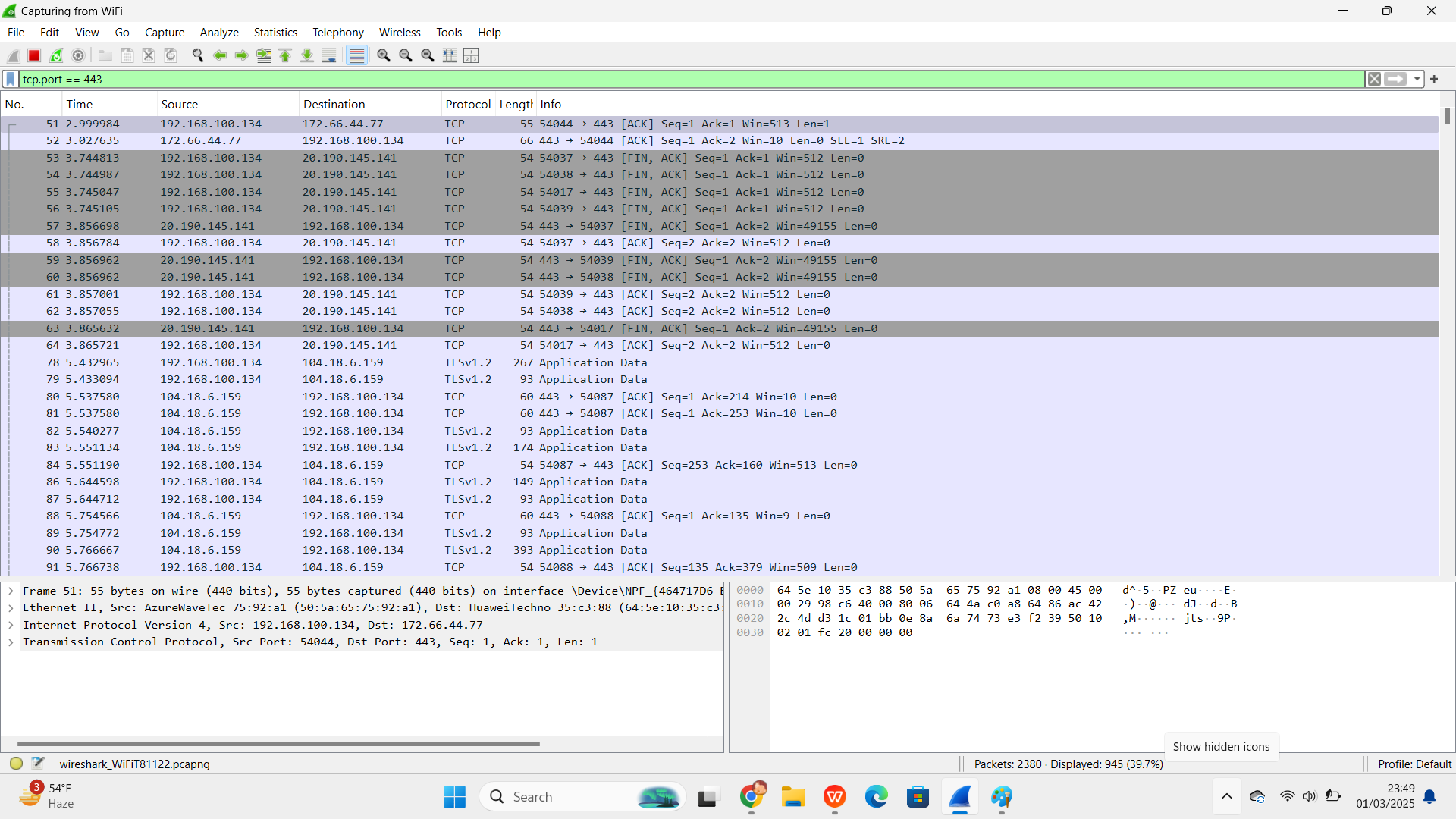


1. 200 Ok, 304 Not Modified etc.
2. Headers present are :

Content-Type, Last-Modified, ETag, Cache-Control, Expires, Date, Connection and so on.



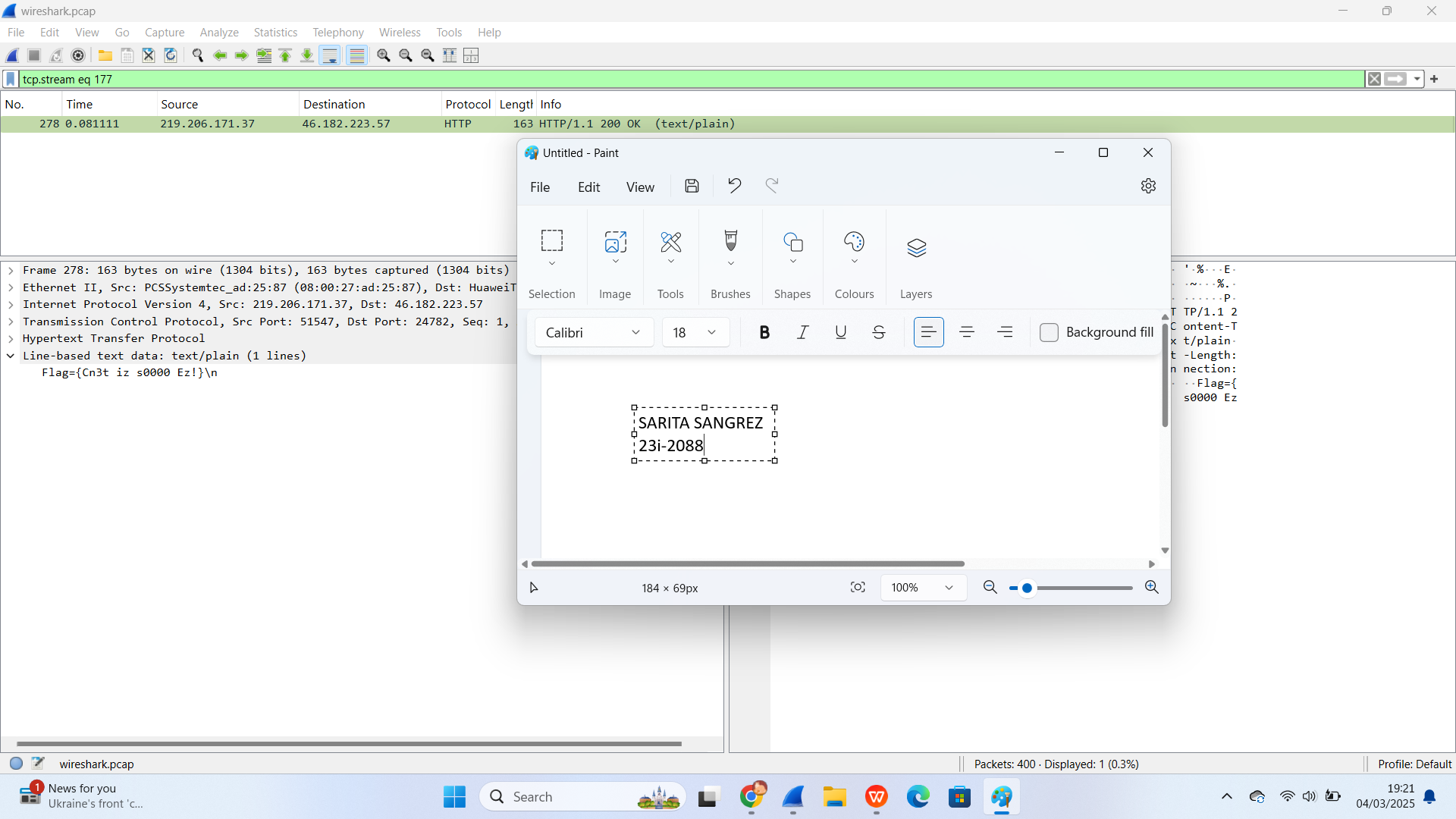
1. When I captured HTTPS using the URL <https://www.isc.org/bind/> and the filter tcp.port == 443, I saw the TSL handshake that enables encrypted communication between the client and the server.



**TASK 02**

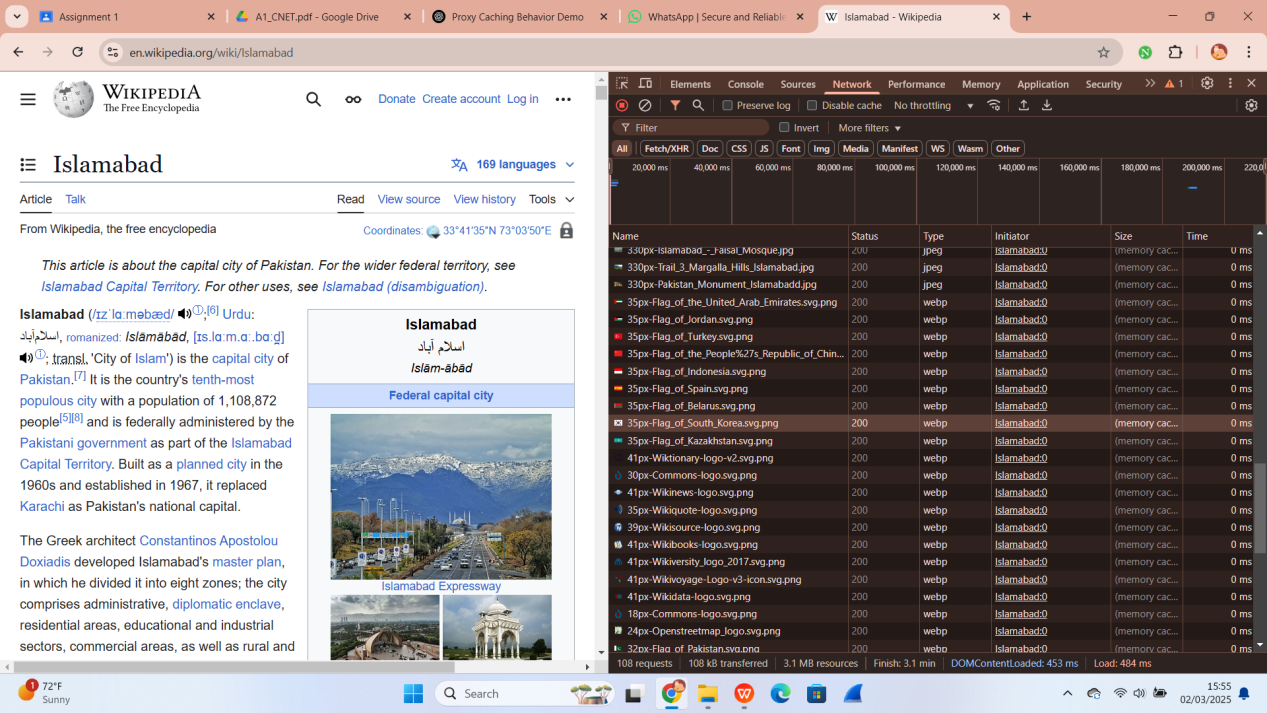
The flag is embedded in wireshark.pcap.

Flag={Cn3t iz s0000 Ez!}



**TASK 3**

When I perform a normal reload, content is retrieved from the cache. This can be seen under the size column where “memory cache” is written. We will also be able to see “last-modified” details under HTTP response headers and 304 status code once we click on one packet.

****

When I perform a force reload, browser bypasses the cache and requests fresh content. Hence, status code 200 ok is seen under Status column.

