

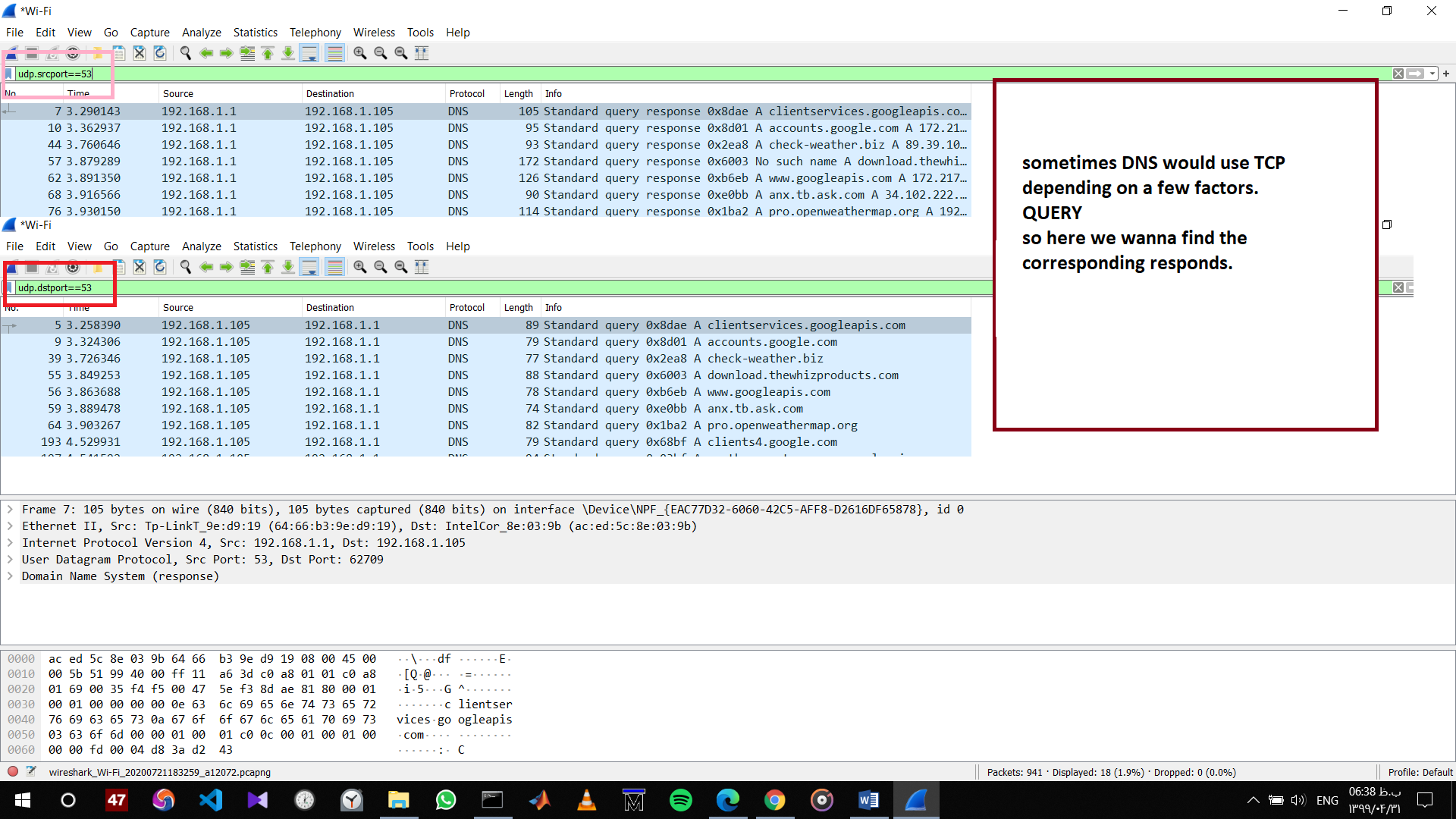
|  |
| --- |
|  |
|  |
| Wireshark \_ LAB 2 |

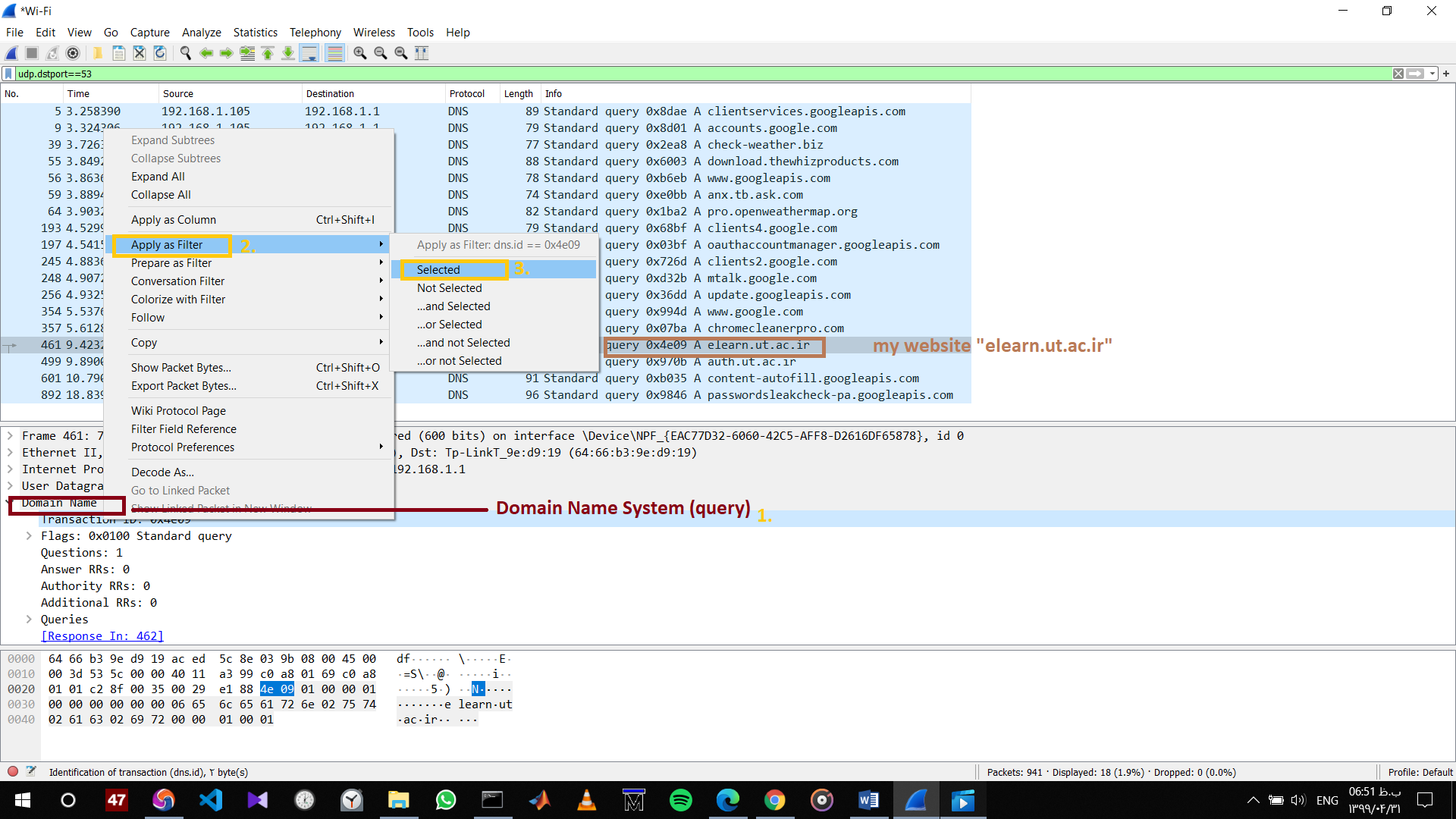
# DNS

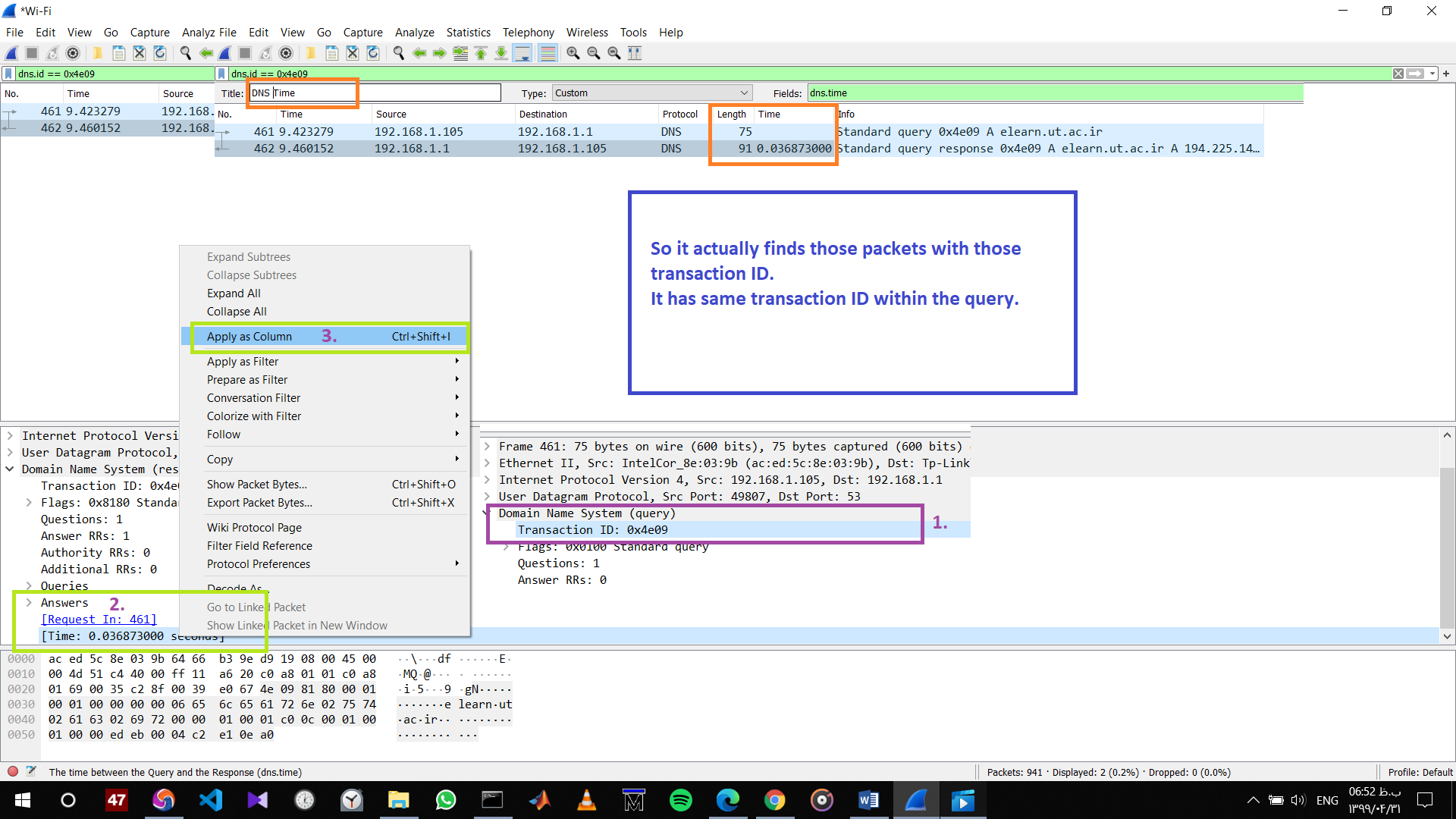
Part 1.

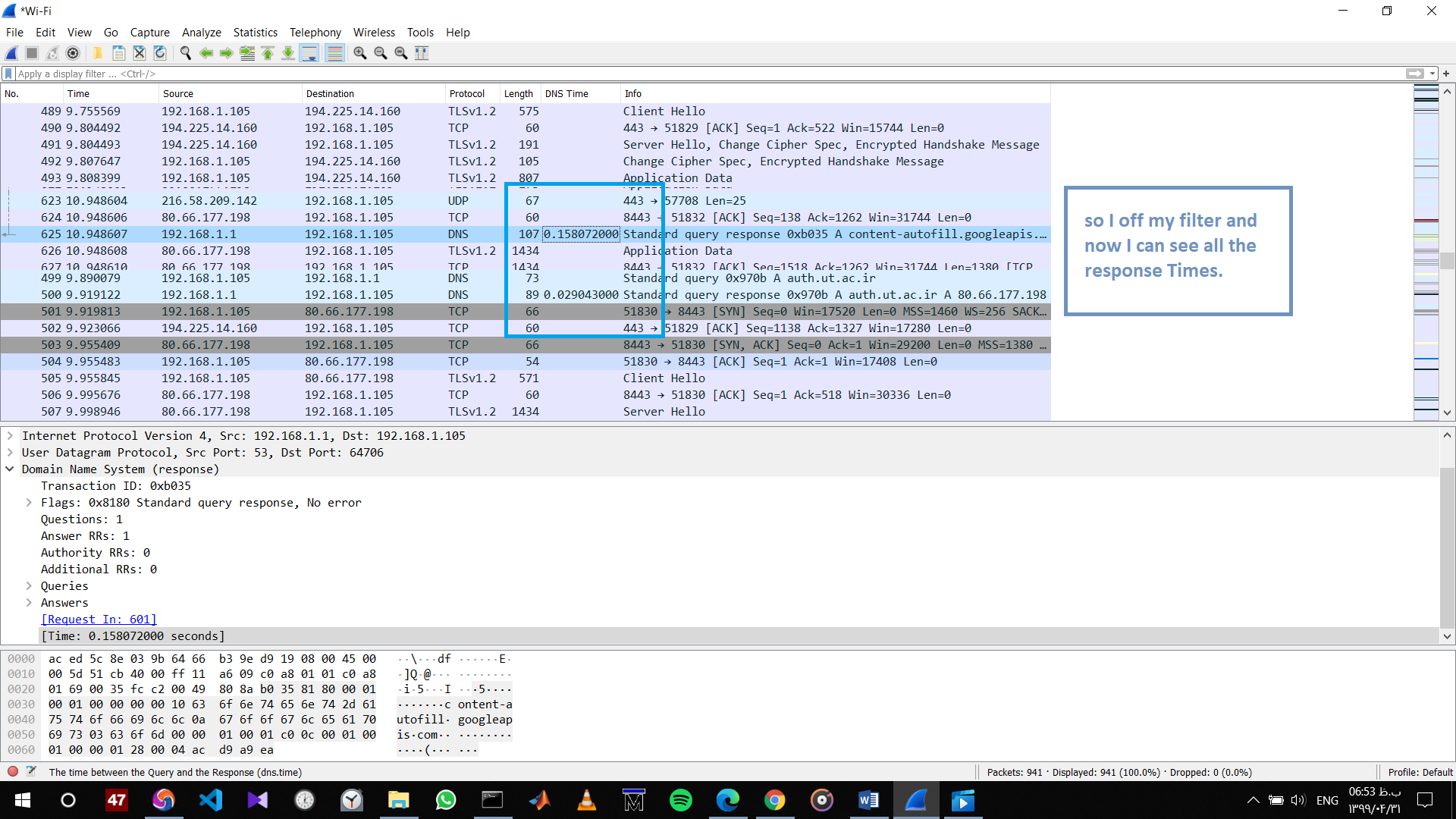
Questions:

Q1.



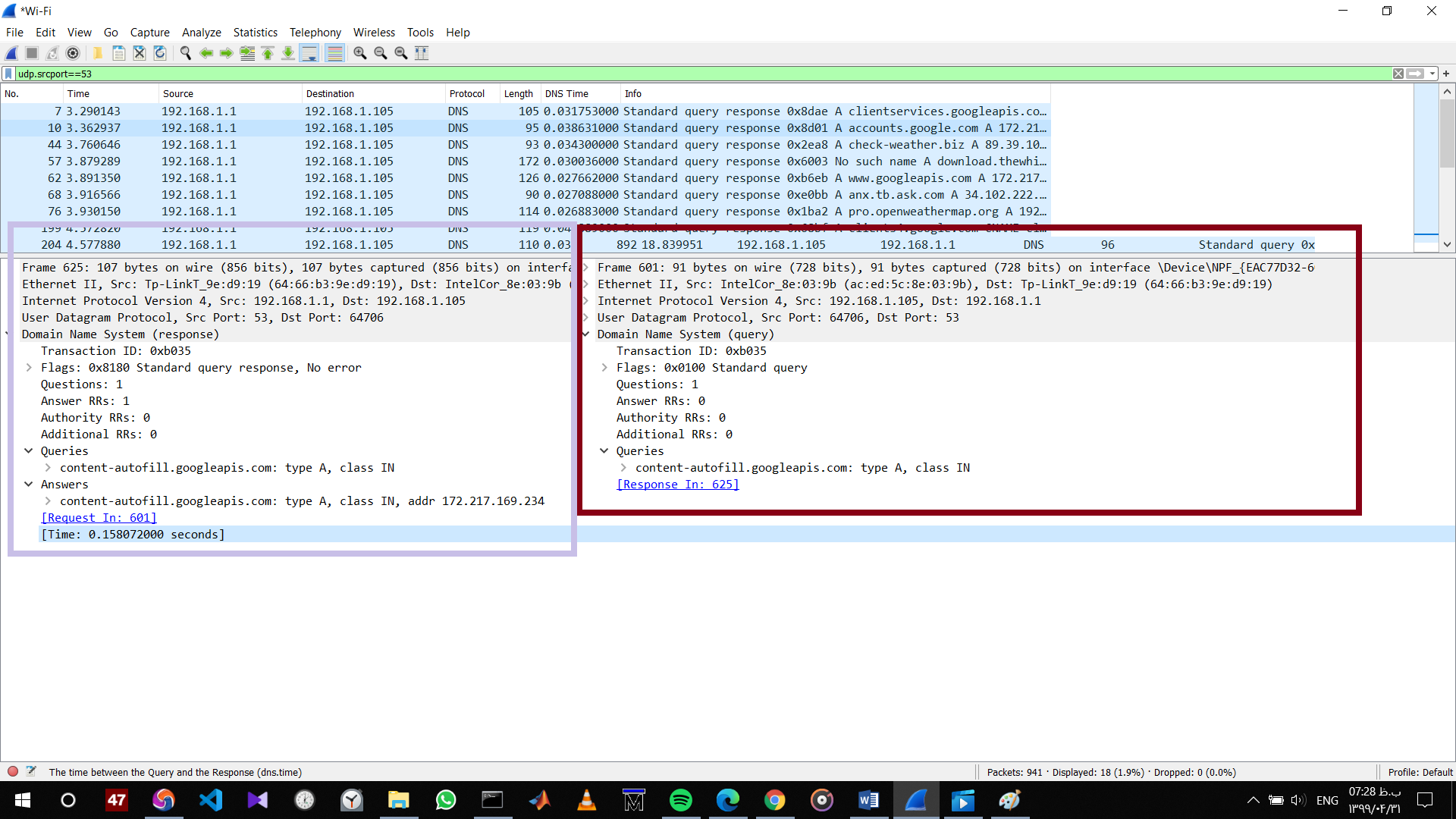




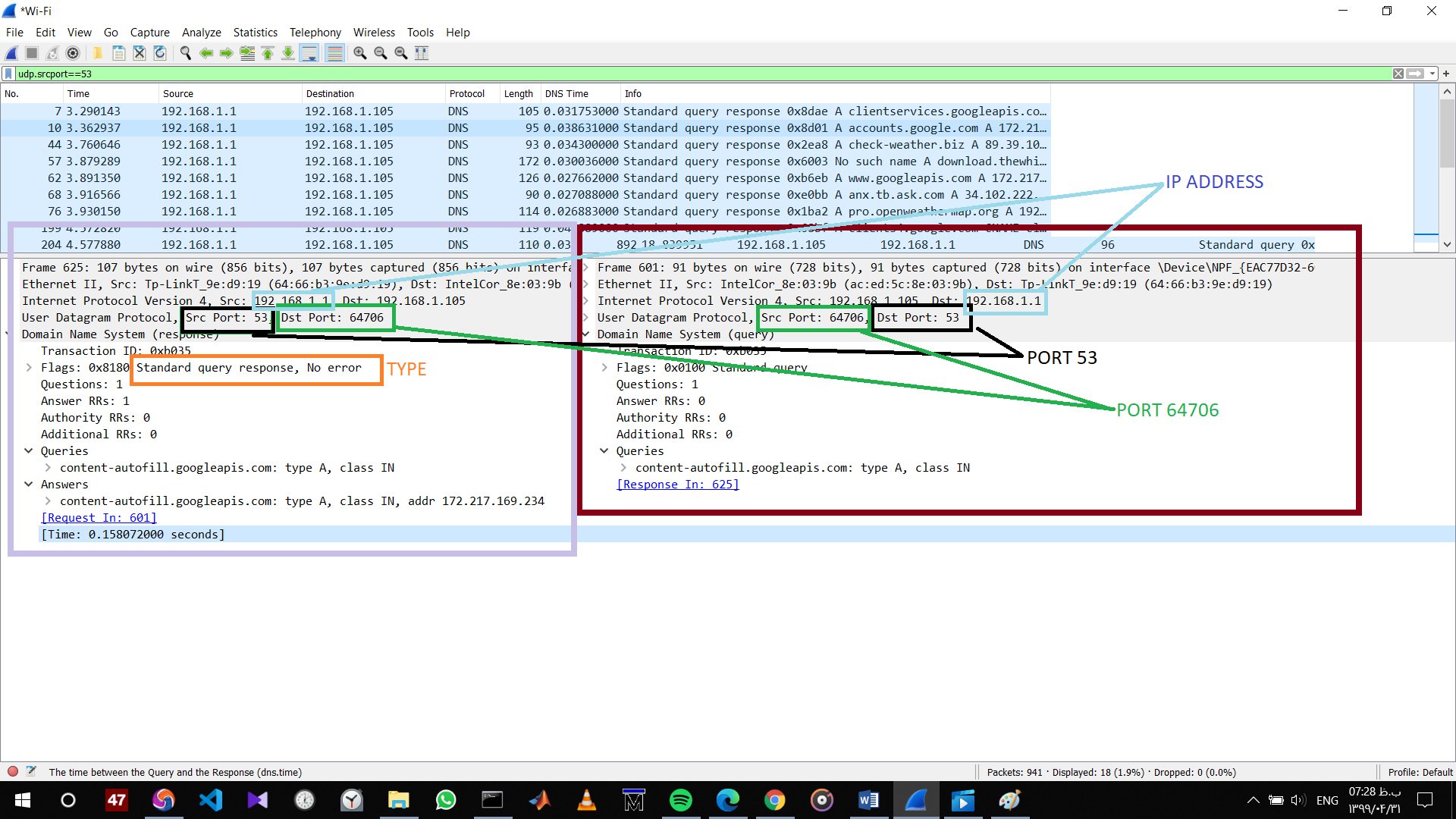


Q2.

*answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address.*

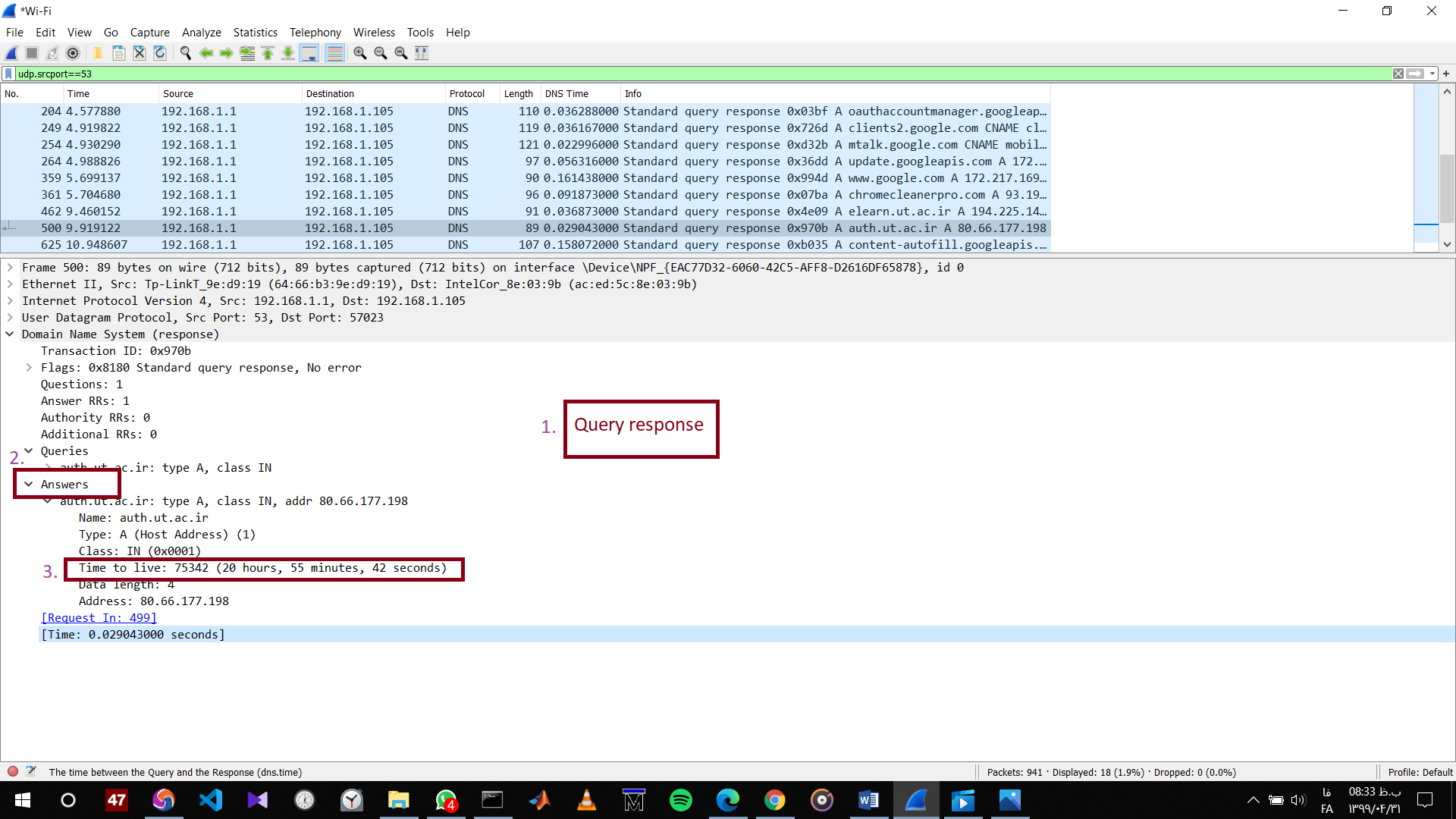
**

Q3.



*They are sent over UDP and the destination port of DNS query is 53 and the source port of the DNS response is 53. the IP address is 192.168.1.1 which is the local DNS server.*

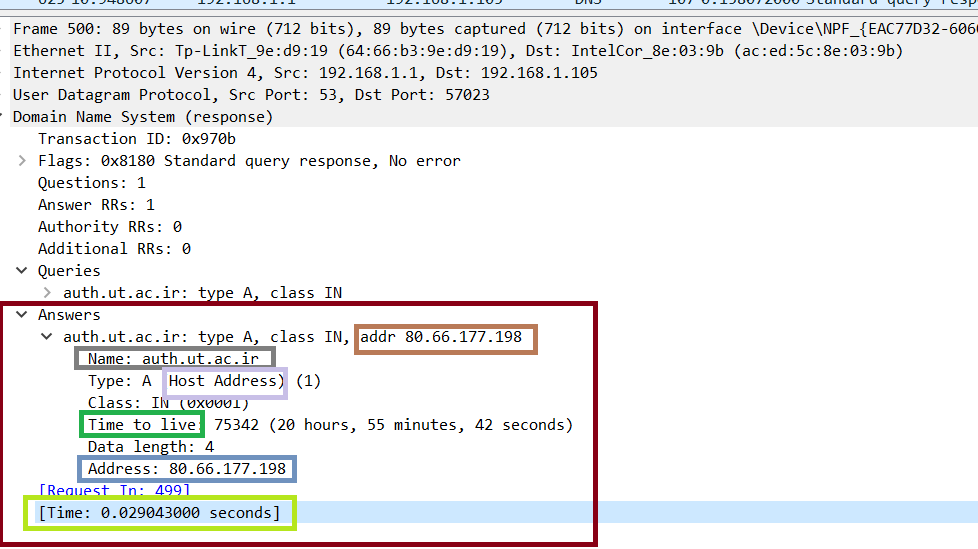
Q4.

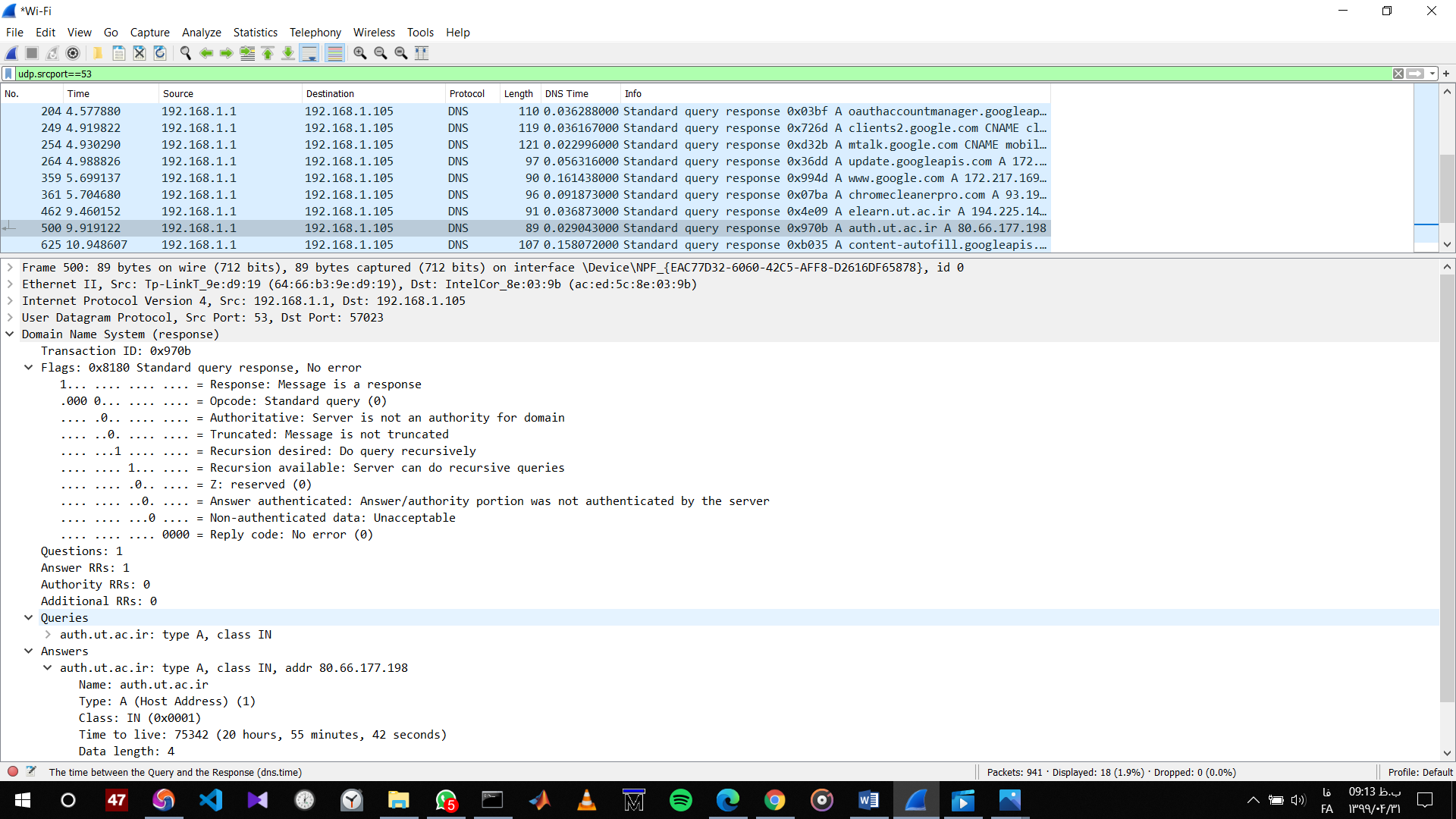


Q5.

*It can be a reference from any website pulling a picture, an advertisement or whatever off from another domains server - that’s why u might see lots of sites you "never visit".*

Q6.

**



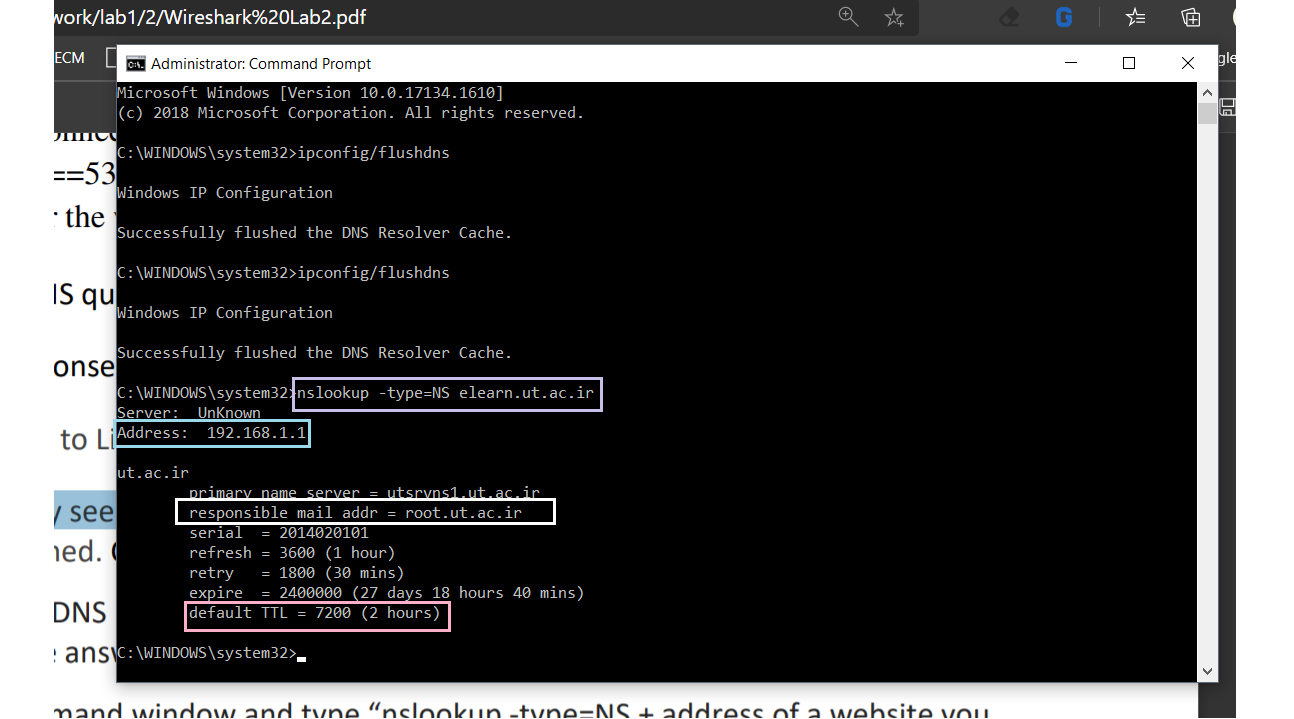
Q7.

*As a command-line tool, nslookup gives you the ability to find the IP address for a specific host, or vice versa.*

*Having these options is important because if DNS isn’t working correctly, no online functionality is available—you can’t look at websites, use chat services, or send emails.*

*Using nslookup functionality, you can perform several troubleshooting steps:*

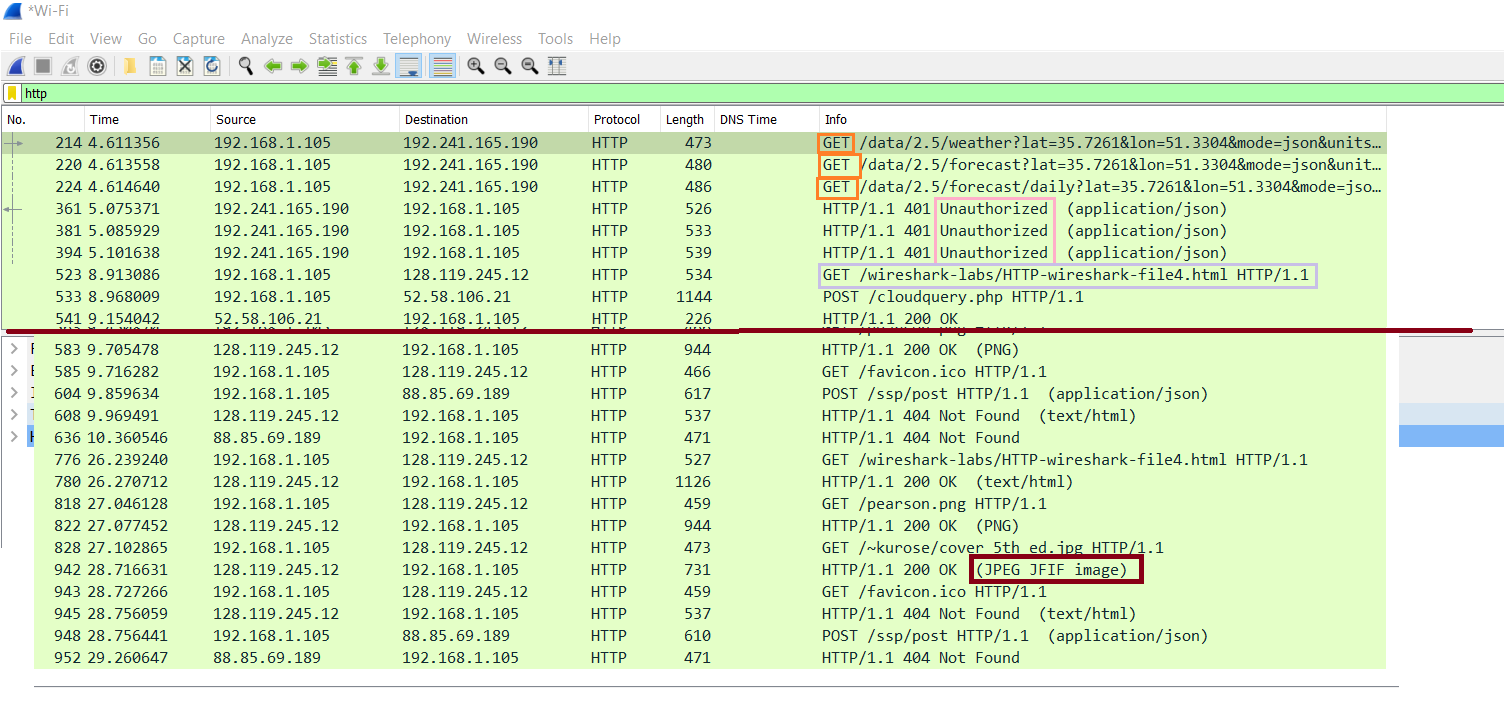
* *Verifying connectivity to the DNS server*
* *Checking other devices or users for name resolution issues*
* *Testing the local server*
* *Scanning for spyware and viruses*
* *Flushing the DNS cache*

**

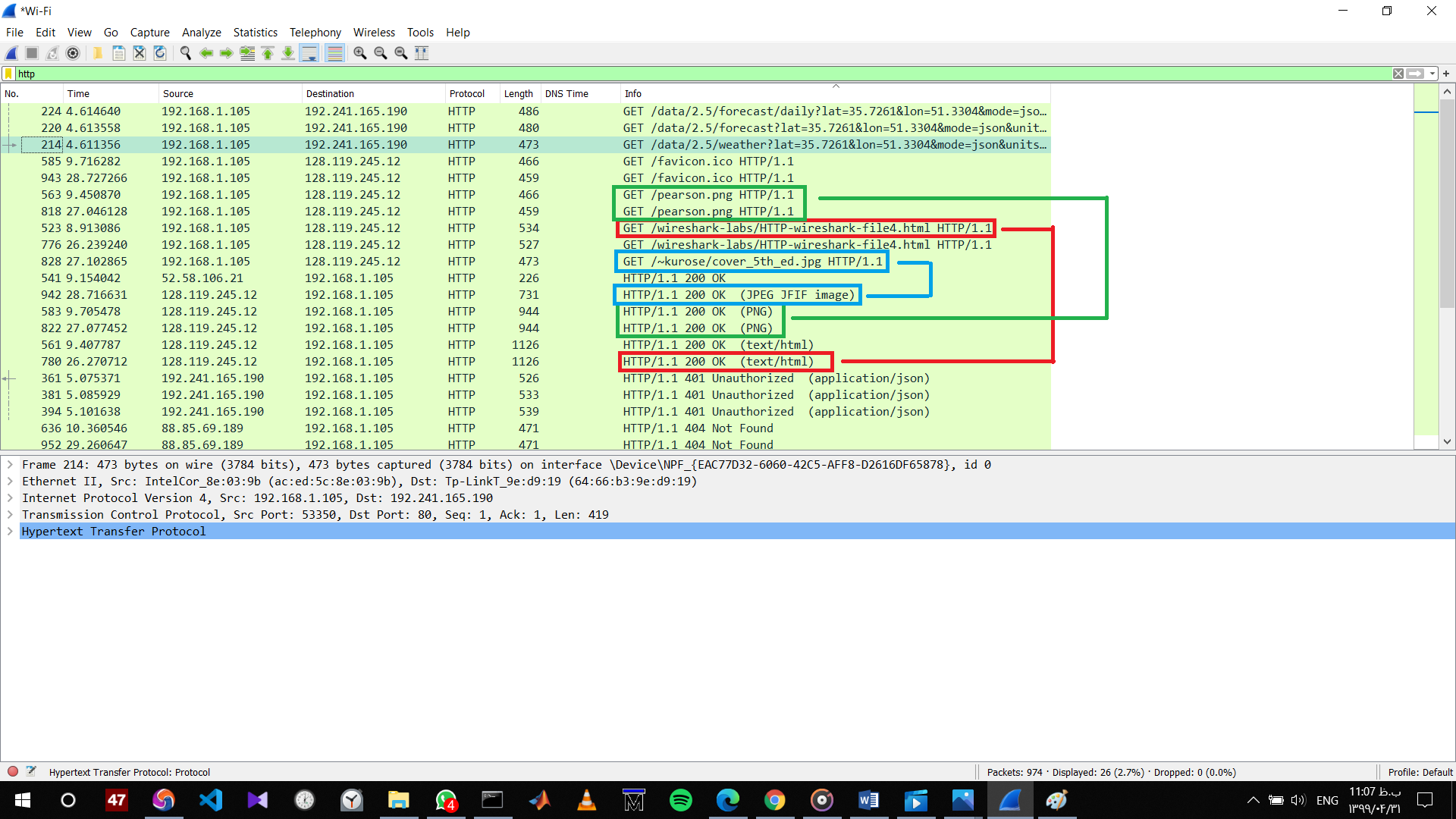
HTTP

Part 2.

Q1.



Q2.

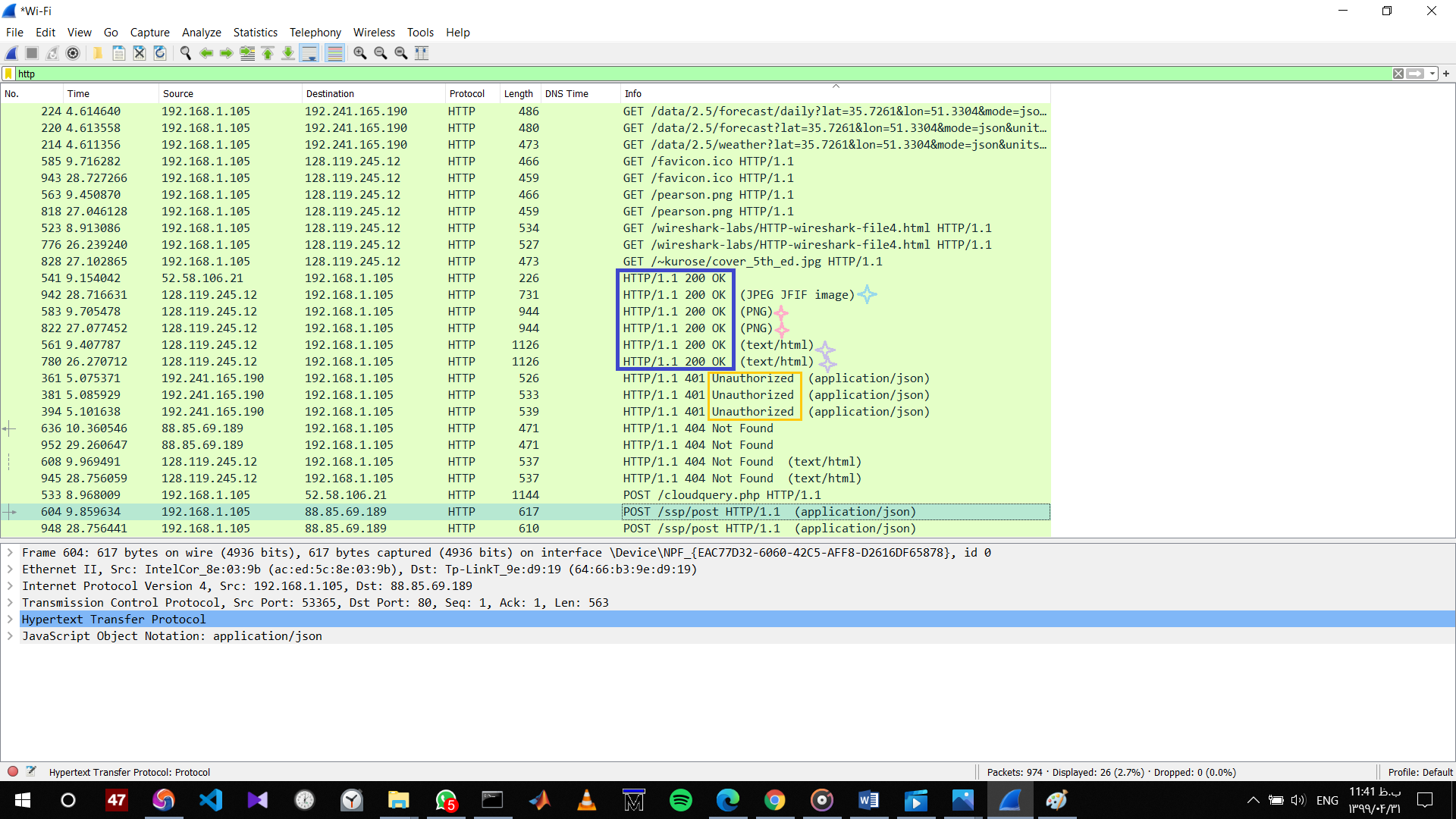


The HTTP messages we send to:

1. To get the base file
2. To get the pearson logo
3. To get the 5th edition textbook cover

And notice that messages were send to different IP address.

Q3.



*The HTTP protocol (*[*RFC 2616*](ftp://ftp.isi.edu/in-notes/rfc2616.txt)*) defines a simple framework for access authentication schemes. The assumption is that a certain group of pages -- usually referred to as a protected realm or just a realm -- should only be accessible to certain people who are able to provide credentials if challenged by the server.*