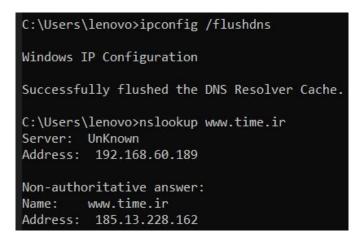
Part 1: DNS

1. Analyzing the answer for the "nslookup" command:



The nslookup command provides information about the DNS (Domain Name System) records for a given website. It returns the IP address associated with the website, along with other details such as the DNS server that provided the response.

No.		Time	Source	Destination	Protocol	Length Info
	427	11.464857	192.168.60.62	192.168.60.189	DNS	87 Standard query 0x0001 PTR 189.60.168.192.in-addr.arpa
4	428	11.468188	192.168.60.189	192.168.60.62	DNS	87 Standard query response 0x0001 No such name PTR 189.60.168.192.in-addr.arpa
	429	11.469290	192.168.60.62	192.168.60.189	DNS	71 Standard query 0x0002 A www.time.ir
	436	11.521422	192.168.60.189	192.168.60.62	DNS	87 Standard query response 0x0002 A www.time.ir A 185.13.228.162
	437	11.524460	192.168.60.62	192.168.60.189	DNS	71 Standard query 0x0003 AAAA www.time.ir
	440	11.552717	192.168.60.189	192.168.60.62	DNS	130 Standard query response 0x0003 AAAA www.time.ir SOA ns2.parsihost.com

2. Analyzing the answer for the "nslookup -type=NS" command:

```
C:\Users\lenovo>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\lenovo>nslookup -type=NS www.time.ir
Server: UnKnown
Address: 192.168.60.189

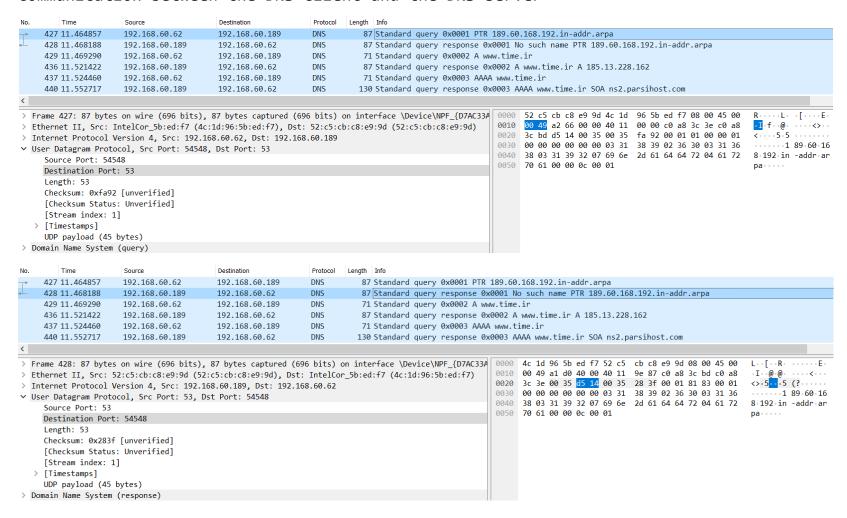
time.ir
    primary name server = ns2.parsihost.com
    responsible mail addr = admin.time.ir
    serial = 1678790598
    refresh = 3600 (1 hour)
    retry = 3600 (1 hour)
    expire = 604800 (7 days)
    default TTL = 10800 (3 hours)
```

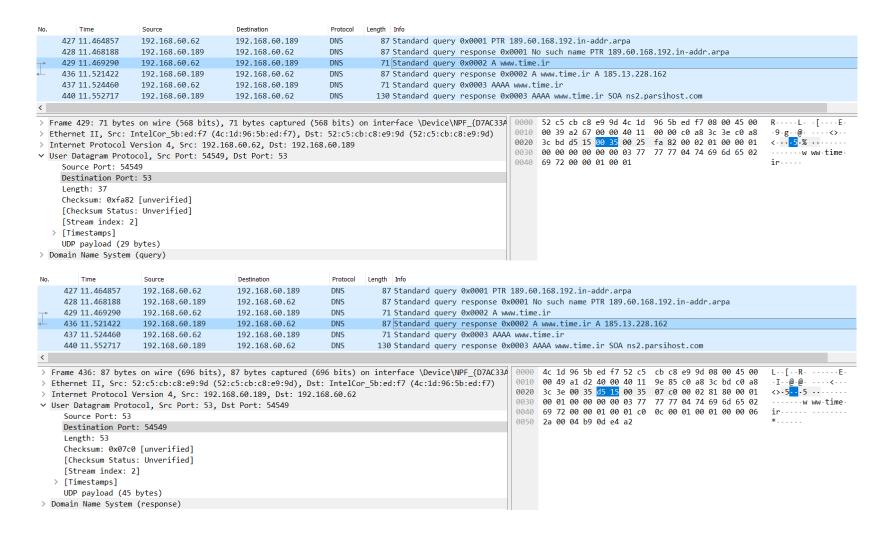
The nslookup command with the "-type=NS" parameter is used to specifically query the DNS server for the authoritative name servers (NS records) of a domain. This command returns the list of name servers responsible for the queried domain.

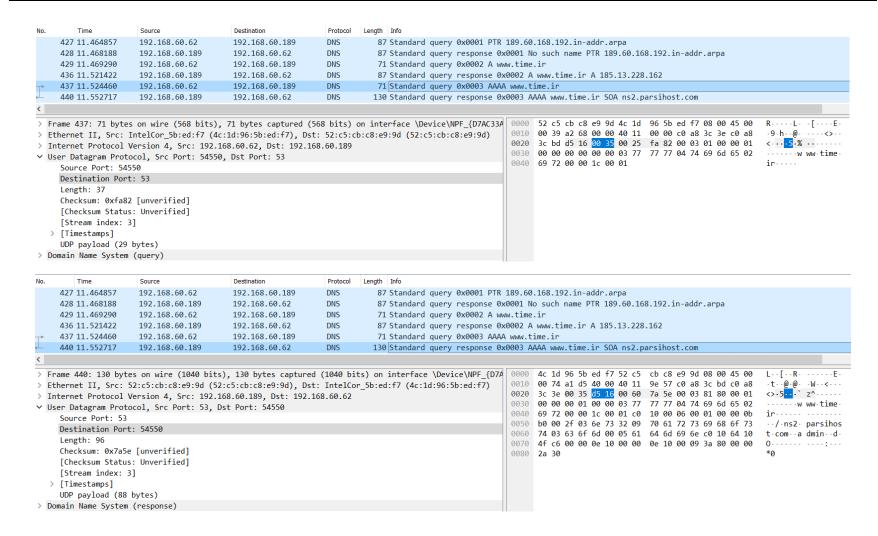
```
43 6.666809
                192.168.60.62
                                     192.168.60.189
                                                          DNS
                                                                     87 Standard query 0x0001 PTR 189.60.168.192.in-addr.arpa
44 6.670189
                192.168.60.189
                                     192.168.60.62
                                                                     87 Standard query response 0x0001 No such name PTR 189.60.168.192.in-addr.arpa
45 6.671376
               192.168.60.62
                                     192.168.60.189
                                                         DNS
                                                                     71 Standard query 0x0002 NS www.time.ir
54 6.834705
                192.168.60.189
                                     192.168.60.62
                                                                    130 Standard query response 0x0002 NS www.time.ir SOA ns2.parsihost.com
                                                         DNS
```

3. Describing the DNS sequences in Wireshark results:

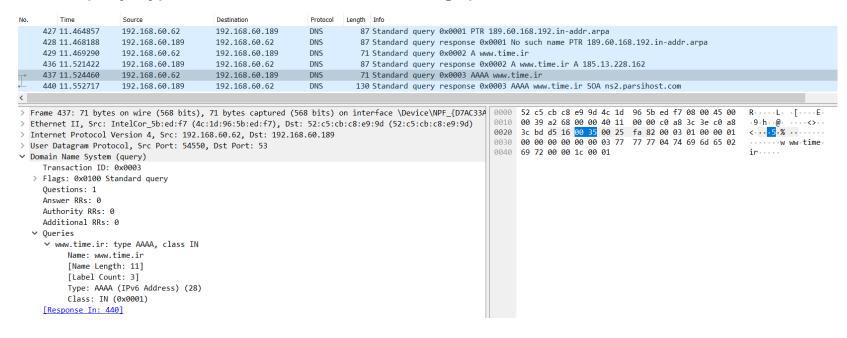
By filtering UDP connections with port number 53 (udp.dstport==53 || udp.srcport==53), we can identify DNS-related traffic in Wireshark. The DNS sequences refer to the series of DNS queries and responses captured in the packet capture. They represent the communication between the DNS client and the DNS server





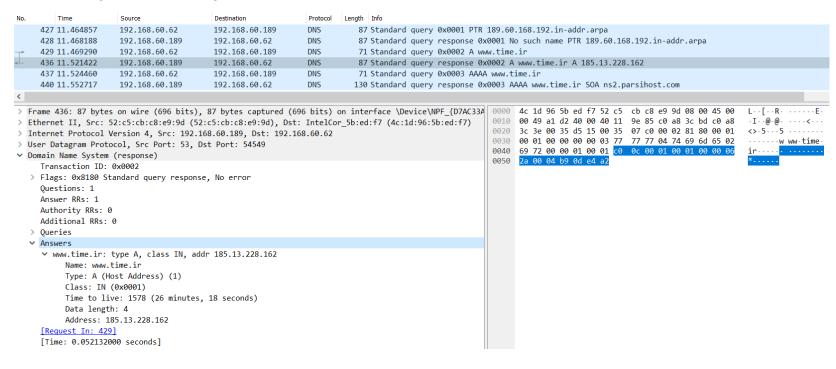


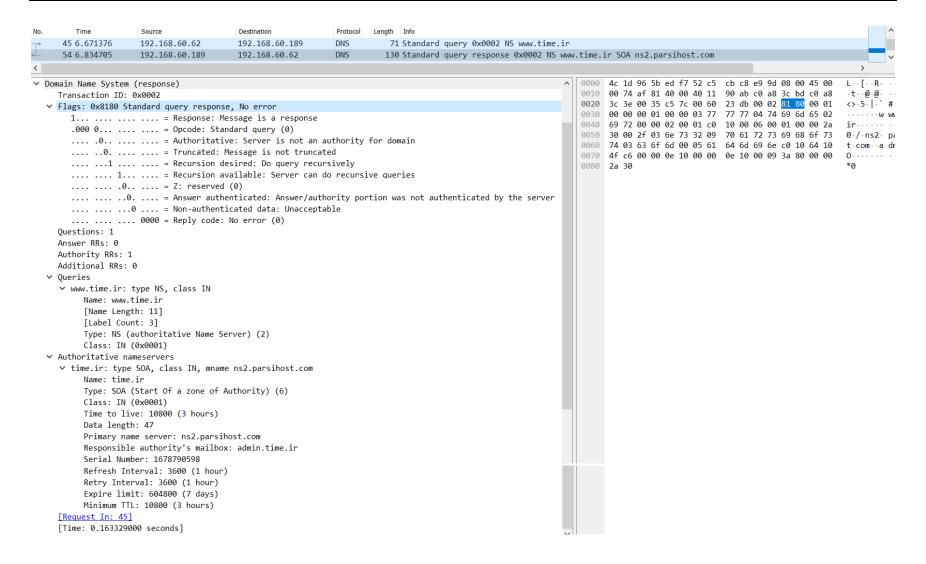
4. The contents of the request, which include the source and destination IP addresses, DNS query types, and the domain names being queried:



5. Describing flags and the answer in the responses of the DNS queries:

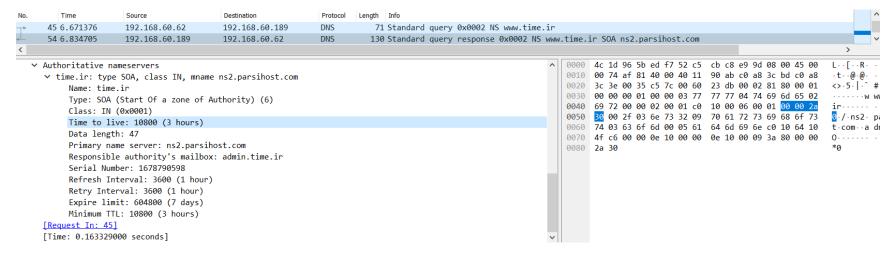
The flags in the DNS response packets indicate various aspects of the response, such as the type of response (e.g., authoritative, non-authoritative), whether it is an answer or a query, and if any errors occurred.





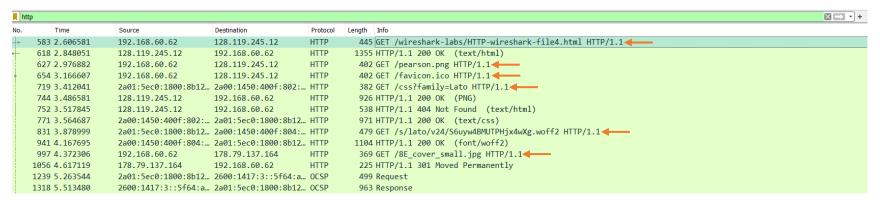
6. Explaining Time to Live (TTL) in DNS protocol:

Time to Live (TTL) is a value specified in DNS records that determines the duration for which a DNS response can be cached by other DNS servers or clients. It indicates how long the information remains valid before it needs to be refreshed. The TTL value can be found in the DNS response packets captured in Wireshark.



Part 1: HTTP

1. The content of the HTTP GET request messages:



2. The content of GET responses:

