Wireshark Lab: DNS (Modified)

1. Nslookup

1. Run nslookup to obtain the IP address of a Web server in Asia

```
C:\Windows\system32>nslookup www.u-tokyo.ac.jp
Server:  dns49.turktelekom.com.tr
Address:  195.175.39.49

Non-authoritative answer:
Name:    www.u-tokyo.ac.jp
Address:  210.152.243.234
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe

```
C:\Windows\system32>nslookup -type=NS www.boun.edu.tr
Server:  dns49.turktelekom.com.tr
Address:  195.175.39.49

Non-authoritative answer:
www.boun.edu.tr canonical name = lir.cc.boun.edu.tr

cc.boun.edu.tr
        primary name server = simurg.cc.boun.edu.tr
        responsible mail addr = hostmaster.boun.edu.tr
        serial  = 2019092702
        refresh = 10800 (3 hours)
        retry   = 3600 (1 hour)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
```

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! Mail.

```
C:\Windows\system32>nslookup www.boun.edu.tr mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  87.248.118.23

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
^C
```

The IP addreess for the DNS server if queried for the Yahoo! mail server is 87.248.118.23

2. ipconfig

3. Tracing DNS with Wireshark

4. DNS query and response messages are sent over UDP

```
User Datagram Protocol, Src Port: 49593, Dst Port: 53
```

5. Destination port is 53 and source port is 49593

```
User Datagram Protocol, Src Port: 49593, Dst Port: 53
```

6. IP address which is the DNS query message sent is 195.175.39.50

```
11 3.592814      192.168.1.39      195.175.39.50      DNS      72 Standard query 0xab86 A www.ietf.org
```

This IP addresses are the same

```
DNS Servers . . . . . . . . . . . . : 195.175.39.49
                                      195.175.39.50
```

7. Type of DNS query is A and it does not contain any “answers”.

```
Queries
  www.ietf.org: type A, class IN
      Name: www.ietf.org
      [Name Length: 12]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

8. 3 answers is provided. These answers contain:

```
Answers
  www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
```

9. Yes, the destination IP address of the SYN packet corresponds to the IP addresses provided in the DNS response message.

```
Internet Protocol Version 4, Src: 192.168.1.39, Dst: 104.20.0.85
> www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
```

10. No, the images are all loaded from www.ietf.org, so additional DNS queries are not necessary (the host uses a cached address).

11. Destination port is 53.

```
User Datagram Protocol, Src Port: 60737, Dst Port: 53
```

12. The DNS query messageis sent to:

```
Destination: 195.175.39.49
```

Yes, it is the IP address of my default local DNS server

```
Server:  dns49.turktelekom.com.tr
Address:  195.175.39.49
```

13. Type of DNS query is AAAA and it does not contain any “answers”.

```
▼ Queries
  ▼ www.mit.edu: type AAAA, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
```

14. 4 answers are provided. 2 of them corresponds to CNAME and the others A.

```
▼ Answers
  > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:9c00:1a4::255e
  > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:9c00:193::255e
```

15. Screenshot:

ip.addr == 192.168.1.39 — Expression…

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.39	195.175.39.49	DNS	86	Standard query 0x0001 PTR 49.39.175.195.in-addr.arpa
2	0.008755	195.175.39.49	192.168.1.39	DNS	124	Standard query response 0x0001 PTR 49.39.175.195.in-addr.
3	0.010643	192.168.1.39	195.175.39.49	DNS	71	Standard query 0x0002 A www.mit.edu
4	0.095555	195.175.39.49	192.168.1.39	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mi
5	0.099197	192.168.1.39	195.175.39.49	DNS	71	Standard query 0x0003 AAAA www.mit.edu
6	0.118953	195.175.39.49	192.168.1.39	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME ww

```
> Frame 6: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface 0
> Ethernet II, Src: ZyxelCom_a1:0f:b6 (04:bf:6d:a1:0f:b6), Dst: AsustekC_2b:24:06 (2c:4d:54:2b:24:06)
> Internet Protocol Version 4, Src: 195.175.39.49, Dst: 192.168.1.39
> User Datagram Protocol, Src Port: 53, Dst Port: 60737
▼ Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  ▼ Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:9c00:1a4::255e
    > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:9c00:193::255e
    [Request In: 5]
    [Time: 0.019756000 seconds]
```

16. IP address is the DNS query message sent is:

```
> Internet Protocol Version 4, Src: 192.168.1.39, Dst: 195.175.39.49
```

Yes, it is the IP address of my local DNS server

```
Server:  dns49.turktelekom.com.tr
Address:  195.175.39.49
```

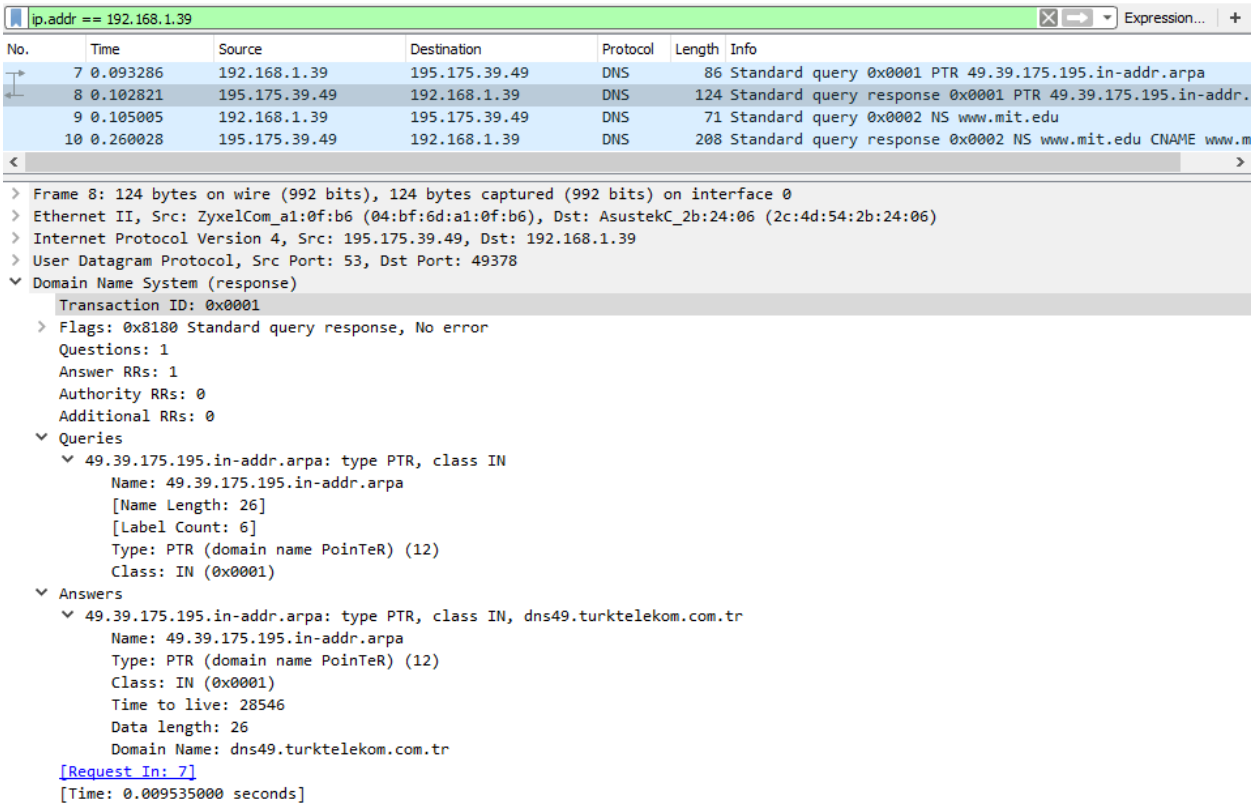
17. Type is PTR(domain name PoinTeR) and it does not contain any “answers”

```
v Queries
  > 49.39.175.195.in-addr.arpa: type PTR, class IN
```

18. Nameserver is 49.39.175.195.in-addr.arpa

```
v Answers
  v 49.39.175.195.in-addr.arpa: type PTR, class IN, dns49.turktelekom.com.tr
      Name: 49.39.175.195.in-addr.arpa
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)
      Time to live: 28546
      Data length: 26
      Domain Name: dns49.turktelekom.com.tr
```

19. Screenshot



NOTE: When I run the "`nslookup www.kaist.edu use2.akam.net`" command, I get refused answer:

```
C:\Windows\system32>nslookup www.kaist.edu use2.akam.net
Server:  UnKnown
Address:  96.7.49.64

*** UnKnown can't find www.kaist.edu: Query refused
```

Thus, I used the trace file dns-ethereal-trace-4 in the zip file "http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip"

20. The query is sent to 18.72.0.3.

    ```
    > Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
    ```

    It corresponds to bitsy.mit.edu.

    ```
    > BITSY.MIT.EDU: type A, class IN, addr 18.72.0.3
    ```

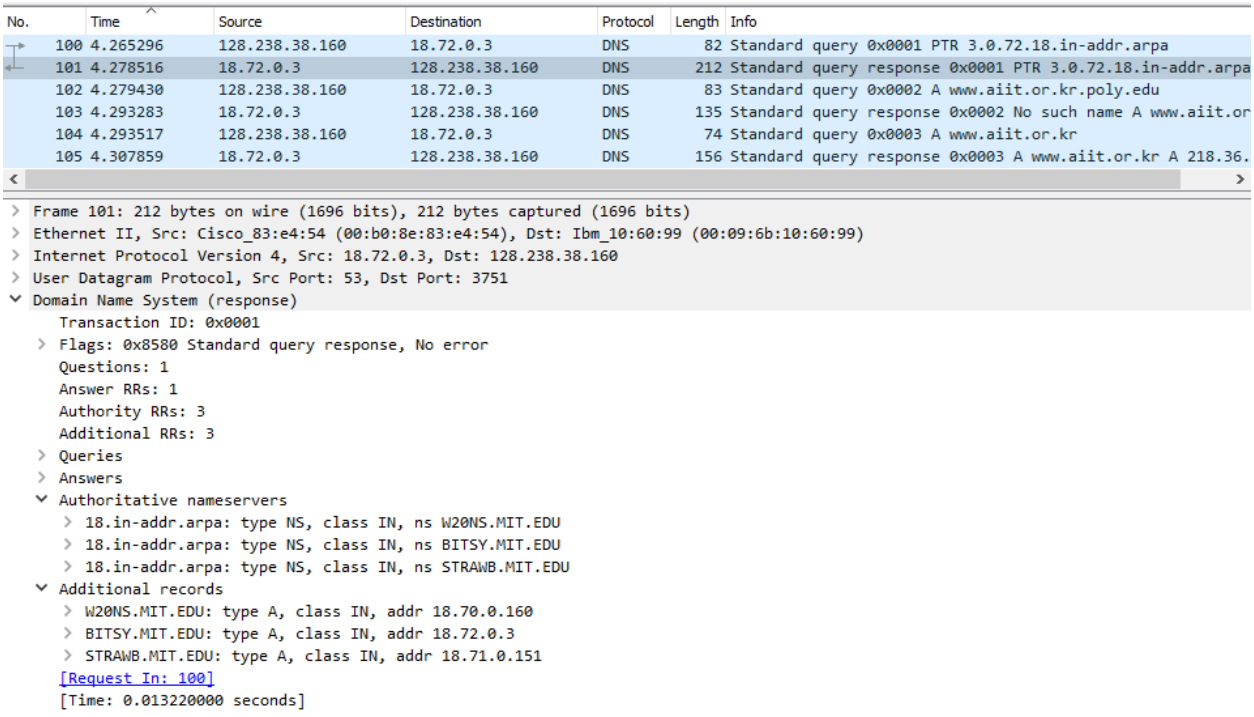
21. It's a PTR type query that doesn't contain any answers.

    ```
    ▼ Queries
      ▼ 3.0.72.18.in-addr.arpa: type PTR, class IN
          Name: 3.0.72.18.in-addr.arpa
          [Name Length: 22]
          [Label Count: 6]
          Type: PTR (domain name PoinTeR) (12)
          Class: IN (0x0001)
    ```

22. One answer is provided in the DNS response message. It contains the following:

    ```
    ▼ Answers
      ▼ 3.0.72.18.in-addr.arpa: type PTR, class IN, BITSY.MIT.EDU
          Name: 3.0.72.18.in-addr.arpa
          Type: PTR (domain name PoinTeR) (12)
          Class: IN (0x0001)
          Time to live: 21600
          Data length: 15
          Domain Name: BITSY.MIT.EDU
    ```

23. Screenshot:



No.	Time	Source	Destination	Protocol	Length	Info
100	4.265296	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101	4.278516	18.72.0.3	128.238.38.160	DNS	212	Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa
102	4.279430	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.aiit.or.kr.poly.edu
103	4.293283	18.72.0.3	128.238.38.160	DNS	135	Standard query response 0x0002 No such name A www.aiit.or
104	4.293517	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.aiit.or.kr
105	4.307859	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A www.aiit.or.kr A 218.36.

```
> Frame 101: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: Ibm_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 18.72.0.3, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3751
v Domain Name System (response)
    Transaction ID: 0x0001
  > Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 3
  > Queries
  > Answers
  v Authoritative nameservers
    > 18.in-addr.arpa: type NS, class IN, ns W20NS.MIT.EDU
    > 18.in-addr.arpa: type NS, class IN, ns BITSY.MIT.EDU
    > 18.in-addr.arpa: type NS, class IN, ns STRAWB.MIT.EDU
  v Additional records
    > W20NS.MIT.EDU: type A, class IN, addr 18.70.0.160
    > BITSY.MIT.EDU: type A, class IN, addr 18.72.0.3
    > STRAWB.MIT.EDU: type A, class IN, addr 18.71.0.151
    [Request In: 100]
    [Time: 0.013220000 seconds]
```