

EXPERIMENT10**ANALYZING DOMAIN NAME SYSTEM (DNS) PROTOCOL IN WIRE-SHARK****OBJECTIVE:**

- Understand the Domain Name System Protocol

THEORY:

Domain Name System (DNS) translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we'll take a closer look at the client side of DNS. Recall that the client's role in the DNS is relatively simple – a client sends a *query* to its local DNS server, and receives a *response* back. Much can go on “under the covers,” invisible to the DNS clients, as the hierarchical DNS servers communicate with each other to either recursively or iteratively resolve the client's DNS query. From the DNS client's standpoint, however, the protocol is quite simple – a query is formulated to the local DNS server and a response is received from that server. Before beginning this lab, you'll probably want to review DNS by reading Section 2.5 of the text. In particular, you may want to review the material on **local DNS servers**, **DNS caching**, **DNS records and messages**, and the **TYPE** field in the DNS record.

1. nslookup

In this lab, we'll make extensive use of the *nslookup* tool, which is available in most Linux/Unix and Microsoft platforms today. To run *nslookup* in Linux/Unix, you just type the *nslookup* command on the command line. To run it in Windows, open the Command Prompt and run *nslookup* on the command line.

In its most basic operation, *nslookup* tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a toplevel-domain DNS server, an authoritative DNS server, or an intermediate DNS server (see the textbook for definitions of these terms). To accomplish this task, *nslookup* sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

```
C:\>nslookup www.mit.edu
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Name:    www.mit.edu
Address:  18.7.22.83

C:\>nslookup -type=NS mit.edu
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Non-authoritative answer:
mit.edu nameserver = bitsy.mit.edu
mit.edu nameserver = strawb.mit.edu
mit.edu nameserver = w20ns.mit.edu

bitsy.mit.edu    internet address = 18.72.0.3
strawb.mit.edu   internet address = 18.71.0.151
w20ns.mit.edu    internet address = 18.70.0.160

C:\>nslookup www.aiit.or.kr bitsy.mit.edu
Server:  BITSY.MIT.EDU
Address:  18.72.0.3

Non-authoritative answer:
Name:    www.aiit.or.kr
Address:  218.36.94.200
```

Figure 10.1 shows the results of three independent *nslookup* commands (displayed in the Windows Command Prompt). In this example, the client host is located on the campus of Polytechnic University in Brooklyn, where the default local DNS server is *dns-prime.poly.edu*. When running *nslookup*, if no DNS server is specified, then *nslookup* sends the query to the default DNS server, which in this case is *dns-prime.poly.edu*.

Details of each command:

- ***nslookup www.mit.edu***

In words, this command is saying “*Please send me the IP address for the host www.mit.edu.*” As shown in the screenshot, the response from this command provides two pieces of information: (1) the name and IP address of the DNS server that provides the answer; and (2) the answer itself, which is the host name and IP address of *www.mit.edu*. Although the response came from the local DNS server at Polytechnic University, it is quite possible that this local DNS server iteratively contacted several other DNS servers to get the answer, as described in Section 2.5 of the textbook.

- ***nslookup -type=NS mit.edu***

In this example, we have provided the option “-type=NS” and the domain “mit.edu”. This causes *nslookup* to send a query for a type-NS record to the default local DNS server. In words, the query is saying, “*Please send me the host names of the authoritative DNS for mit.edu.*” (When the -type option is not used, *nslookup* uses the default, which is to query for type A records; see Section 2.5.3 in the text.) The answer, displayed in the above screenshot, first indicates the DNS server that is providing the answer (which is the default local DNS server) along with three MIT name servers. Each of these servers is indeed an authoritative DNS server for the hosts on the MIT campus.

However, *nslookup* also indicates that the answer is “non-authoritative,” meaning that this answer came from the cache of some server rather than from an authoritative MIT DNS server. Finally, the answer also includes the IP addresses of the authoritative DNS servers at MIT. (Even though the type-NS query generated by *nslookup* did not explicitly ask for the IP addresses, the local DNS server returned these “for free” and *nslookup* displays the result.)

- ***nslookup www.aiit.or.kr bitsy.mit.edu***

In this example, we indicate that we want the query sent to the DNS server *bitsy.mit.edu* rather than to the default DNS server (*dns-prime.poly.edu*). Thus, the query and reply transaction takes place directly between our querying host and *bitsy.mit.edu*. In this example, the DNS server *bitsy.mit.edu* provides the IP address of the host *www.aiit.or.kr*, which is a web server at the Advanced Institute of Information Technology (in Korea).

Do the following (and write down the results)

1. Run *nslookup* to obtain the IP address of a Web server in Asia, e.g. www.lums.edu.pk.
Paste screenshot of your result here:

```
C:\Users\l236006>nslookup www.lums.edu.pk
Server:  MAINDC.fastlhr.nu.edu.pk
Address: 172.16.99.2

Non-authoritative answer:
Name:    lums.edu.pk
Addresses: 111.68.103.174
          110.93.234.24
          203.135.62.24
Aliases: www.lums.edu.pk

C:\Users\l236006>
```

2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe (e.g., cam.ac.uk)

```
C:\Users\l236006>nslookup -type=NS cam.ac.uk
Server:  MAINDC.fastlhr.nu.edu.pk
Address: 172.16.99.2

Non-authoritative answer:
cam.ac.uk      nameserver = ns1.mythic-beasts.com
cam.ac.uk      nameserver = auth0.dns.cam.ac.uk
cam.ac.uk      nameserver = dns0.cl.cam.ac.uk
cam.ac.uk      nameserver = ns2.ic.ac.uk
cam.ac.uk      nameserver = ns3.mythic-beasts.com
cam.ac.uk      nameserver = dns0.eng.cam.ac.uk

ns1.mythic-beasts.com  internet address = 45.33.127.156
ns1.mythic-beasts.com  AAAA IPv6 address = 2600:3c00:e000:19::1
auth0.dns.cam.ac.uk    internet address = 131.111.8.37
auth0.dns.cam.ac.uk    AAAA IPv6 address = 2001:630:212:8::d:a0
dns0.cl.cam.ac.uk      internet address = 128.232.0.19
dns0.cl.cam.ac.uk      AAAA IPv6 address = 2a05:b400:110::d:a0
ns2.ic.ac.uk           internet address = 155.198.142.82
ns2.ic.ac.uk           AAAA IPv6 address = 2a0c:5bc0:4:1::82
ns3.mythic-beasts.com  internet address = 185.24.221.32
ns3.mythic-beasts.com  AAAA IPv6 address = 2a02:2770:11:0:21a:4aff:febe:759b
dns0.eng.cam.ac.uk     internet address = 129.169.8.8

C:\Users\l236006>
```

3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. If server does not respond, just type the command you used.

```
C:\Users\l236006>nslookup -type=MX yahoo.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
yahoo.com      MX preference = 1, mail exchanger = mta7.am0.yahoodns.net
yahoo.com      MX preference = 1, mail exchanger = mta6.am0.yahoodns.net
yahoo.com      MX preference = 1, mail exchanger = mta5.am0.yahoodns.net

C:\Users\l236006>nslookup -type=MX yahoo.com dns0.cl.cam.ac.uk
Server:  dns0.cl.cam.ac.uk
Address:  128.232.0.19

*** dns0.cl.cam.ac.uk can't find yahoo.com: Query refused

C:\Users\l236006>
```

Query refused

2. ipconfig

ipconfig (for Windows) and *ifconfig* (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues. Here we'll only describe *ipconfig*, although the Linux/Unix *ifconfig* is very similar. *ipconfig* can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on. For example, if you want to see all this information about your host, simply enter: *ipconfig/all* into the Command Prompt, as shown in figure 10.2.

type

ipconfig/all

```

C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : USG11631-ZMWQA6
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : poly.edu
    Description . . . . . : Intel(R) PRO/100 VE Network Connecti
on
    Physical Address. . . . . : 00-09-6B-10-60-99
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 128.238.38.160
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 128.238.38.1
    DHCP Server . . . . . : 128.238.29.25
    DNS Servers . . . . . : 128.238.29.22
                           128.238.29.23
                           128.238.2.38
                           128.238.32.22
    Primary WINS Server . . . . . : 128.238.29.23
    Secondary WINS Server . . . . . : 128.238.29.22
    Lease Obtained. . . . . : Monday, August 30, 2004 1:30:50 PM
    Lease Expires . . . . . : Monday, August 30, 2004 7:30:50 PM

```

Figure

10.2

ipconfig is also very useful for managing the DNS information stored in your host. We learned that a host can cache DNS records it recently obtained.

To see these cached records, after the prompt C:\> provide the following command:

```
ipconfig /displaydns
```

Each entry shows the remaining Time to Live (TTL) in seconds.

To clear the cache, enter `ipconfig /flushdns`

Flushing the DNS cache clears all entries and reloads the entries from the host's file.

3. Tracing DNS with Wireshark

Let's first capture the DNS packets that are generated by ordinary Web surfing activity.

- Use *ipconfig* to empty the DNS cache in your host.
- Open your browser and empty your browser cache. (With Internet Explorer, go to Tools menu and select Internet Options; then in the General tab select Delete Files.)
- Start packet capture in Wireshark.
- With your browser, visit the Web page: <http://www.ietf.org>
- Stop packet capture.

Answer the following questions:

4. **Locate the DNS query and response messages. Are they sent over UDP or TCP?**

They are sent over UDP

Lab Manual of ‘Data Communication and Networks’

242	2.439957	10.102.110.7	172.16.99.2	DNS	97 Standard query 0x0b2c A array817.prod.do.dsp.mp.microsoft.com
243	2.440834	172.16.99.2	10.102.110.7	DNS	113 Standard query response 0xb02c A array817.prod.do.dsp.mp.microsoft.com A 72.154.7.110
290	2.771022	10.102.110.7	172.16.99.2	DNS	87 Standard query 0xd85d A lab1-pc01.fastlhr.nu.edu.pk
291	2.771595	172.16.99.2	10.102.110.7	DNS	158 Standard query response 0xd85d No such name A lab1-pc01.fastlhr.nu.edu.pk SOA maindc.fastlhr.nu.edu.pk
415	3.805239	10.102.110.7	172.16.99.2	DNS	94 Standard query 0x6479 A kv801.prod.do.dsp.mp.microsoft.com
416	3.806287	172.16.99.2	10.102.110.7	DNS	204 Standard query response 0x6479 A kv801.prod.do.dsp.mp.microsoft.com CNAME kv801.prod.do.dsp.mp.microsoft.com.edgekey.net CNAME e12437.d.akamaiedge.net A 104.73.164.75
504	4.212817	10.102.110.7	172.16.99.2	DNS	72 Standard query 0x0992 Unknown (65) www.ietf.org
506	4.213626	172.16.99.2	10.102.110.7	DNS	145 Standard query response 0x0992 Unknown (65) www.ietf.org Unknown (65)
507	4.213793	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xe290 A www.ietf.org
509	4.214731	172.16.99.2	10.102.110.7	DNS	104 Standard query response 0xe290 A www.ietf.org A 104.16.44.99 A 104.16.45.99
512	4.215520	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xd969 A www.ietf.org
515	4.216150	172.16.99.2	10.102.110.7	DNS	104 Standard query response 0xd969 A www.ietf.org A 104.16.45.99 A 104.16.44.99
516	4.216384	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xca15 AAAA www.ietf.org
521	4.216961	172.16.99.2	10.102.110.7	DNS	128 Standard query response 0xca15 AAAA www.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63
654	5.014784	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x6691 Unknown (65) static.ietf.org
655	5.014926	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x160c A static.ietf.org
656	5.016836	172.16.99.2	10.102.110.7	DNS	140 Standard query response 0x6691 Unknown (65) static.ietf.org Unknown (65)
657	5.016837	172.16.99.2	10.102.110.7	DNS	107 Standard query response 0x160c A static.ietf.org A 104.16.44.99 A 104.16.45.99
658	5.017331	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x65fd A static.ietf.org
661	5.018129	172.16.99.2	10.102.110.7	DNS	107 Standard query response 0x65fd A static.ietf.org A 104.16.45.99 A 104.16.44.99
> Frame 504: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{84902142-B15D-4A67-B278-D3543EF562ED}, id 0					
> Ethernet II, Src: e8:cf:83:42:53:c4 (e8:cf:83:42:53:c4), Dst: Cisco_0c:10:ff (00:1f:9e:0c:10:ff)					
> Internet Protocol Version 4, Src: 10.102.110.7, Dst: 172.16.99.2					
User Datagram Protocol, Src Port: 62565, Dst Port: 53					
Source Port: 62565					
Destination Port: 53					
Length: 38					
Checksum: 0x87b7 [unverified]					
[Checksum Status: Unverified]					
[Stream index: 8]					
> [Timestamps]					
> Domain Name System (query)					

5. What is the destination port for the DNS query message? What is the source port of DNS response message?

Query message Source port =53 see destination port

243	2.440834	172.16.99.2	10.102.110.7	DNS	113 Standard query response 0xb02c A array817.prod.do.dsp.mp.microsoft.com A 72.154.7.110
290	2.771022	10.102.110.7	172.16.99.2	DNS	87 Standard query 0xd85d A lab1-pc01.fastlhr.nu.edu.pk
291	2.771595	172.16.99.2	10.102.110.7	DNS	158 Standard query response 0xd85d No such name A lab1-pc01.fastlhr.nu.edu.pk SOA maindc.fastlhr.nu.edu.pk
415	3.805239	10.102.110.7	172.16.99.2	DNS	94 Standard query 0x6479 A kv801.prod.do.dsp.mp.microsoft.com
416	3.806287	172.16.99.2	10.102.110.7	DNS	204 Standard query response 0x6479 A kv801.prod.do.dsp.mp.microsoft.com CNAME kv801.prod.do.dsp.mp.microsoft.com.edgekey.net CNAME e12437.d.akamaiedge.net A 104.73.164.75
504	4.212817	10.102.110.7	172.16.99.2	DNS	72 Standard query 0x0992 Unknown (65) www.ietf.org
506	4.213626	172.16.99.2	10.102.110.7	DNS	145 Standard query response 0x0992 Unknown (65) www.ietf.org Unknown (65)
507	4.213793	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xe290 A www.ietf.org
509	4.214731	172.16.99.2	10.102.110.7	DNS	104 Standard query response 0xe290 A www.ietf.org A 104.16.44.99 A 104.16.45.99
512	4.215520	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xd969 A www.ietf.org
515	4.216150	172.16.99.2	10.102.110.7	DNS	104 Standard query response 0xd969 A www.ietf.org A 104.16.45.99 A 104.16.44.99
516	4.216384	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xca15 AAAA www.ietf.org
521	4.216961	172.16.99.2	10.102.110.7	DNS	128 Standard query response 0xca15 AAAA www.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63
654	5.014784	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x6691 Unknown (65) static.ietf.org
655	5.014926	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x160c A static.ietf.org
656	5.016836	172.16.99.2	10.102.110.7	DNS	140 Standard query response 0x6691 Unknown (65) static.ietf.org Unknown (65)
657	5.016837	172.16.99.2	10.102.110.7	DNS	107 Standard query response 0x160c A static.ietf.org A 104.16.44.99 A 104.16.45.99
658	5.017331	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x65fd A static.ietf.org
661	5.018129	172.16.99.2	10.102.110.7	DNS	107 Standard query response 0x65fd A static.ietf.org A 104.16.45.99 A 104.16.44.99
> Frame 504: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{84902142-B15D-4A67-B278-D3543EF562ED}, id 0					
> Ethernet II, Src: e8:cf:83:42:53:c4 (e8:cf:83:42:53:c4), Dst: Cisco_0c:10:ff (00:1f:9e:0c:10:ff)					
> Internet Protocol Version 4, Src: 10.102.110.7, Dst: 172.16.99.2					
User Datagram Protocol, Src Port: 62565, Dst Port: 53					
Source Port: 62565					
Destination Port: 53					
Length: 38					
Checksum: 0x87b7 [unverified]					
[Checksum Status: Unverified]					
[Stream index: 8]					
> [Timestamps]					
> Domain Name System (query)					

Message port = 53 (response)

290	2.771022	10.102.110.7	172.16.99.2	DNS	87 Standard query 0xd85d A lab1-pc01.fastlhr.nu.edu.pk
291	2.771595	172.16.99.2	10.102.110.7	DNS	158 Standard query response 0xd85d No such name A lab1-pc01.fastlhr.nu.edu.pk SOA maindc.fastlhr.nu.edu.pk
415	3.805239	10.102.110.7	172.16.99.2	DNS	94 Standard query 0x6479 A kv801.prod.do.dsp.mp.microsoft.com
416	3.806287	172.16.99.2	10.102.110.7	DNS	204 Standard query response 0x6479 A kv801.prod.do.dsp.mp.microsoft.com CNAME kv801.prod.do.dsp.mp.microsoft.com.edgekey.net CNAME e12437.d.akamaiedge.net A 104.73.164.75
504	4.212817	10.102.110.7	172.16.99.2	DNS	72 Standard query 0x0992 Unknown (65) www.ietf.org
506	4.213626	172.16.99.2	10.102.110.7	DNS	145 Standard query response 0x0992 Unknown (65) www.ietf.org Unknown (65)
507	4.213793	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xe290 A www.ietf.org
509	4.214731	172.16.99.2	10.102.110.7	DNS	104 Standard query response 0xe290 A www.ietf.org A 104.16.44.99 A 104.16.45.99
512	4.215520	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xd969 A www.ietf.org
515	4.216150	172.16.99.2	10.102.110.7	DNS	104 Standard query response 0xd969 A www.ietf.org A 104.16.45.99 A 104.16.44.99
516	4.216384	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xca15 AAAA www.ietf.org
521	4.216961	172.16.99.2	10.102.110.7	DNS	128 Standard query response 0xca15 AAAA www.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63
654	5.014784	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x6691 Unknown (65) static.ietf.org
655	5.014926	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x160c A static.ietf.org
656	5.016836	172.16.99.2	10.102.110.7	DNS	140 Standard query response 0x6691 Unknown (65) static.ietf.org Unknown (65)
657	5.016837	172.16.99.2	10.102.110.7	DNS	107 Standard query response 0x160c A static.ietf.org A 104.16.44.99 A 104.16.45.99
658	5.017331	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x65fd A static.ietf.org
661	5.018129	172.16.99.2	10.102.110.7	DNS	107 Standard query response 0x65fd A static.ietf.org A 104.16.45.99 A 104.16.44.99
> Frame 506: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{84902142-B15D-4A67-B278-D3543EF562ED}, id 0					
> Ethernet II, Src: Cisco_0c:10:ff (00:1f:9e:0c:10:ff), Dst: e8:cf:83:42:53:c4 (e8:cf:83:42:53:c4)					
> Internet Protocol Version 4, Src: 172.16.99.2, Dst: 10.102.110.7					
User Datagram Protocol, Src Port: 53, Dst Port: 62565					
Source Port: 53					
Destination Port: 62565					
Length: 111					
Checksum: 0x6400 [unverified]					
[Checksum Status: Unverified]					
[Stream index: 8]					
> [Timestamps]					
> Domain Name System (response)					

6. To what IP address is the DNS query message sent? Use *ipconfig* to determine the IP address of your local DNS server. Are these two IP addresses the same?

Ethernet adapter Ethernet 4:

```

Connection-specific DNS Suffix  . : fastlhr.nu.edu.pk
Description . . . . . : Intel(R) Ethernet Connection (17) I219-LM #3
Physical Address. . . . . : E8-CF-83-42-53-C4
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::64c3:a16c:fd12:2beb%11(Preferred)
IPv4 Address. . . . . : 10.102.110.7(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, November 10, 2025 11:20:38 AM
Lease Expires . . . . . : Tuesday, November 11, 2025 11:20:37 AM
Default Gateway . . . . . : 10.102.110.1
DHCP Server . . . . . : 172.16.99.6
DHCPv6 IAID . . . . . : 468242307
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-9D-42-F2-6C-3C-8C-50-5A-3C
DNS Servers . . . . . : 172.16.99.2
                        172.16.99.10
                        172.16.99.5
NetBIOS over Tcpi. . . . . : Enabled
    
```

Both ip address are same

172.16.99.2

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Type A , IPv4 . answers Zero

290 2.771802	10.102.110.7	172.16.99.2	DNS	87 Standard query 0xd85d A lab1-pc01.fastlhr.nu.edu.pk
291 2.771595	172.16.99.2	10.102.110.7	DNS	158 Standard query response 0xd85d No such name A lab1-pc01.fastlhr.nu.edu.pk SOA maindc.fastlhr.nu.edu.pk
415 3.805239	10.102.110.7	172.16.99.2	DNS	94 Standard query 0x6479 A kv001.prod.do.dsp.mp.microsoft.com
416 3.806287	172.16.99.2	10.102.110.7	DNS	204 Standard query response 0x6479 A kv001.prod.do.dsp.mp.microsoft.com CNAME kv001.prod.do.dsp.mp.microsoft.com.edgekey.net CNAME e12437.d.akamaiedge.net A 104.
504 4.212817	10.102.110.7	172.16.99.2	DNS	72 Standard query 0x0992 Unknown (65) www.ietf.org
506 4.213626	172.16.99.2	10.102.110.7	DNS	145 Standard query response 0x0992 Unknown (65) www.ietf.org Unknown (65)
507 4.213793	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xe290 A www.ietf.org
509 4.214731	172.16.99.2	10.102.110.7	DNS	104 Standard query response 0xe290 A www.ietf.org A 104.16.44.99 A 104.16.45.99
512 4.215520	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xd969 A www.ietf.org
515 4.216150	172.16.99.2	10.102.110.7	DNS	104 Standard query response 0xd969 A www.ietf.org A 104.16.45.99 A 104.16.44.99
516 4.216384	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xca15 AAAA www.ietf.org
521 4.216961	172.16.99.2	10.102.110.7	DNS	128 Standard query response 0xca15 AAAA www.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63
654 5.014784	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x6691 Unknown (65) static.ietf.org
655 5.014926	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x160c A static.ietf.org
656 5.016836	172.16.99.2	10.102.110.7	DNS	148 Standard query response 0x6691 Unknown (65) static.ietf.org Unknown (65)
657 5.016837	172.16.99.2	10.102.110.7	DNS	107 Standard query response 0x160c A static.ietf.org A 104.16.44.99 A 104.16.45.99
658 5.017391	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x65fd A static.ietf.org
661 5.018129	172.16.99.2	10.102.110.7	DNS	107 Standard query response 0x65fd A static.ietf.org A 104.16.45.99 A 104.16.44.99
> Frame 507: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF{B4902142-B15D-4A67-B27B-D3543EF562E0}, id 0 > Ethernet II, Src: e8:cf:83:42:53:c4 (e8:cf:83:42:53:c4), Dst: Cisco_0c:10:ff (00:1f:9e:0c:10:ff) > Destination: Cisco_0c:10:ff (00:1f:9e:0c:10:ff) > Source: e8:cf:83:42:53:c4 (e8:cf:83:42:53:c4) > Type: IPv4 (0x0800) > Internet Protocol Version 4, Src: 10.102.110.7, Dst: 172.16.99.2 > User Datagram Protocol, Src Port: 62565, Dst Port: 53 > Source Port: 62565 > Destination Port: 53 > Length: 38 > Checksum: 0x87b7 [unverified] > [Checksum Status: Unverified] > [Stream index: 8] > [Timestamps] > Domain Name System (query)				

Lab Manual of ‘Data Communication and Networks’

```
> Frame 507: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{84902142-815D-4A67-B278-D3543EF562ED}, id 0
▼ Ethernet II, Src: e8:cf:83:42:53:c4 (e8:cf:83:42:53:c4), Dst: Cisco_0c:10:ff (00:1f:9e:0c:10:ff)
  > Destination: Cisco_0c:10:ff (00:1f:9e:0c:10:ff)
  > Source: e8:cf:83:42:53:c4 (e8:cf:83:42:53:c4)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.102.110.7, Dst: 172.16.99.2
▼ User Datagram Protocol, Src Port: 62565, Dst Port: 53
  Source Port: 62565
  Destination Port: 53
  Length: 38
  Checksum: 0x87b7 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 8]
  > [Timestamps]
▼ Domain Name System (query)
  Transaction ID: 0xe290
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    [Response In: 509]
```

8. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

```
415 3.805239 10.102.110.7 172.16.99.2 DNS 94 Standard query 0x6479 A kv801.prod.do.dsp.mp.microsoft.com
416 3.806287 172.16.99.2 10.102.110.7 DNS 204 Standard query response 0x6479 A kv801.prod.do.dsp.mp.microsoft.com CNAME kv801.prod.do.dsp.mp.microsoft.com.edgekey.net CNAME e12437.d.akama
504 4.212817 10.102.110.7 172.16.99.2 DNS 72 Standard query 0x0992 Unknown (65) www.ietf.org
506 4.213626 172.16.99.2 10.102.110.7 DNS 145 Standard query response 0x0992 Unknown (65) www.ietf.org Unknown (65)
507 4.213793 10.102.110.7 172.16.99.2 DNS 72 Standard query 0xe290 A www.ietf.org
509 4.214731 172.16.99.2 10.102.110.7 DNS 104 Standard query response 0xe290 A www.ietf.org A 104.16.44.99 A 104.16.45.99
512 4.215520 10.102.110.7 172.16.99.2 DNS 72 Standard query 0xd969 A www.ietf.org
515 4.216150 172.16.99.2 10.102.110.7 DNS 104 Standard query response 0xd969 A www.ietf.org A 104.16.45.99 A 104.16.44.99
516 4.216384 10.102.110.7 172.16.99.2 DNS 72 Standard query 0xca15 AAAA www.ietf.org
521 4.216961 172.16.99.2 10.102.110.7 DNS 128 Standard query response 0xca15 AAAA www.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63
654 5.014784 10.102.110.7 172.16.99.2 DNS 75 Standard query 0x6691 Unknown (65) static.ietf.org
655 5.014926 10.102.110.7 172.16.99.2 DNS 75 Standard query 0x160c A static.ietf.org
656 5.016836 172.16.99.2 10.102.110.7 DNS 148 Standard query response 0x6691 Unknown (65) static.ietf.org Unknown (65)
657 5.016837 172.16.99.2 10.102.110.7 DNS 107 Standard query response 0x160c A static.ietf.org A 104.16.44.99 A 104.16.45.99
658 5.017331 10.102.110.7 172.16.99.2 DNS 75 Standard query 0x65fd A static.ietf.org
661 5.018129 172.16.99.2 10.102.110.7 DNS 107 Standard query response 0x65fd A static.ietf.org A 104.16.45.99 A 104.16.44.99

> Frame 509: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{84902142-815D-4A67-B278-D3543EF562ED}, id 0
▼ Ethernet II, Src: Cisco_0c:10:ff (00:1f:9e:0c:10:ff), Dst: e8:cf:83:42:53:c4 (e8:cf:83:42:53:c4)
  > Destination: e8:cf:83:42:53:c4 (e8:cf:83:42:53:c4)
  > Source: Cisco_0c:10:ff (00:1f:9e:0c:10:ff)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.16.99.2, Dst: 10.102.110.7
▼ User Datagram Protocol, Src Port: 53, Dst Port: 62565
  Source Port: 53
  Destination Port: 62565
  Length: 70
  Checksum: 0x51da [unverified]
  [Checksum Status: Unverified]
  [Stream index: 8]
  > [Timestamps]
▼ Domain Name System (response)
  Transaction ID: 0xe290
  > Flags: 0x0100 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  > Answers
    [Request In: 507]
    [Time: 0.000938000 seconds]
```

Answer 2

9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Filter tcp, go at last, see first tcp seq = 0

No.	Time	Source	Destination	Protocol	Length	Info
2948	6.709514	104.16.45.99	10.102.110.7	TCP	66	[TCP Retransmission] 443 → 41198 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=0192
2950	6.730476	104.16.45.99	10.102.110.7	TCP	60	443 → 41200 [ACK] Seq=1897 Ack=3286 Win=131072 Len=0
2951	6.838957	104.16.45.99	10.102.110.7	TLSv1.3	309	Application Data
2952	6.880777	10.102.110.7	104.16.45.99	TCP	54	41200 → 443 [ACK] Seq=3286 Ack=2152 Win=262912 Len=0
2970	7.107016	172.217.169.234	10.102.110.7	TLSv1.2	1466	Application Data
2971	7.107913	172.217.169.234	10.102.110.7	TLSv1.2	183	Application Data
2972	7.107949	10.102.110.7	172.217.169.234	TCP	54	41183 → 443 [ACK] Seq=1 Ack=1542 Win=1025 Len=0
2976	7.296810	10.102.110.24	10.102.110.7	TCP	66	59536 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2977	7.297085	10.102.110.7	10.102.110.24	TCP	66	7680 → 59536 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
2978	7.297676	10.102.110.24	10.102.110.7	TCP	60	59536 → 7680 [ACK] Seq=1 Ack=1 Win=262656 Len=0
2979	7.297912	10.102.110.24	10.102.110.7	TCP	129	59536 → 7680 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=75
2980	7.298379	10.102.110.7	10.102.110.24	TCP	129	7680 → 59536 [PSH, ACK] Seq=1 Ack=76 Win=2097920 Len=75
2981	7.299207	10.102.110.24	10.102.110.7	TCP	70	59536 → 7680 [PSH, ACK] Seq=76 Ack=76 Win=262656 Len=16
2982	7.299383	10.102.110.7	10.102.110.24	TCP	70	7680 → 59536 [PSH, ACK] Seq=76 Ack=92 Win=2097920 Len=16
2983	7.299624	10.102.110.7	10.102.110.24	TCP	54	7680 → 59536 [FIN, ACK] Seq=92 Ack=92 Win=2097920 Len=0
2984	7.300286	10.102.110.24	10.102.110.7	TCP	60	59536 → 7680 [ACK] Seq=92 Ack=93 Win=262656 Len=0
2985	7.300286	10.102.110.24	10.102.110.7	TCP	60	59536 → 7680 [FIN, ACK] Seq=92 Ack=93 Win=262656 Len=0
2986	7.300349	10.102.110.7	10.102.110.24	TCP	54	7680 → 59536 [ACK] Seq=93 Ack=93 Win=2097920 Len=0
3026	7.750960	10.102.110.7	172.217.169.238	TCP	55	8007 → 443 [ACK] Seq=1 Ack=1 Win=1025 Len=1 [TCP segment of a reassembled PDU]
3027	7.756898	142.250.187.14	10.102.110.7	TLSv1.2	185	Application Data
3028	7.756899	142.250.187.14	10.102.110.7	TLSv1.2	85	Application Data
3029	7.756899	142.250.187.14	10.102.110.7	TLSv1.2	93	Application Data
3030	7.756996	10.102.110.7	142.250.187.14	TCP	54	4225 → 443 [ACK] Seq=1 Ack=202 Win=8195 Len=0
3031	7.758737	10.102.110.7	142.250.187.14	TLSv1.2	89	Application Data
3032	7.758824	10.102.110.7	142.250.187.14	TLSv1.2	93	Application Data
3033	7.758879	10.102.110.7	142.250.187.14	TLSv1.2	89	Application Data

> Frame 2977: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF{B4902142-B150-4A67-B278-D3543EF562ED}, id 0
 > Ethernet II, Src: e8fcf83:42:53:c4 (e8fcf83:42:53:c4), Dst: e8fcf83:41:0e:e6 (e8fcf83:41:0e:e6)
 > Destination: e8fcf83:41:0e:e6 (e8fcf83:41:0e:e6)
 > Source: e8fcf83:42:53:c4 (e8fcf83:42:53:c4)
 > Type: IPv4 (0x0800)
 > Internet Protocol Version 4, Src: 10.102.110.7, Dst: 10.102.110.24
 > Transmission Control Protocol, Src Port: 7680, Dst Port: 59536, Seq: 0, Ack: 1, Len: 0

Type dns

No.	Time	Source	Destination	Protocol	Length	Info
416	3.806287	172.16.99.2	10.102.110.7	DNS	284	Standard query response 0x6479 A kv801.prod.do.dsp.mp.microsoft.com CNAME kv801.prod.do.dsp.mp.microsoft.com.edgekey.net CNAME e12437.d.akam
504	4.212817	10.102.110.7	172.16.99.2	DNS	72	Standard query 0x0992 Unknown (65) www.ietf.org
506	4.213626	172.16.99.2	10.102.110.7	DNS	145	Standard query response 0x0992 Unknown (65) www.ietf.org Unknown (65)
507	4.213793	10.102.110.7	172.16.99.2	DNS	72	Standard query 0xe290 A www.ietf.org
509	4.214731	172.16.99.2	10.102.110.7	DNS	104	Standard query response 0xe290 A www.ietf.org A 104.16.44.99 A 104.16.45.99
512	4.215520	10.102.110.7	172.16.99.2	DNS	72	Standard query 0xd969 A www.ietf.org
515	4.216150	172.16.99.2	10.102.110.7	DNS	104	Standard query response 0xd969 A www.ietf.org A 104.16.45.99 A 104.16.44.99
516	4.216384	10.102.110.7	172.16.99.2	DNS	72	Standard query 0xca15 AAAA www.ietf.org
521	4.216961	172.16.99.2	10.102.110.7	DNS	128	Standard query response 0xca15 AAAA www.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63

Both addresses are same 10.102.110.7

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Yes as two static requests are seen for the two images.

Lab Manual of 'Data Communication and Networks'

515	4.216150	172.16.99.2	10.102.110.7	DNS	104 Standard query response 0xd969 A www.ietf.org A 104.16.45.99 A 104.16.44.99
516	4.216384	10.102.110.7	172.16.99.2	DNS	72 Standard query 0xca15 AAAA www.ietf.org
521	4.216961	172.16.99.2	10.102.110.7	DNS	128 Standard query response 0xca15 AAAA www.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63
654	5.014784	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x6691 Unknown (65) static.ietf.org
655	5.014926	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x160c A static.ietf.org
656	5.016836	172.16.99.2	10.102.110.7	DNS	148 Standard query response 0x6691 Unknown (65) static.ietf.org Unknown (65)
657	5.016837	172.16.99.2	10.102.110.7	DNS	107 Standard query response 0x160c A static.ietf.org A 104.16.44.99 A 104.16.45.99
658	5.017331	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x65fd A static.ietf.org
661	5.018129	172.16.99.2	10.102.110.7	DNS	107 Standard query response 0x65fd A static.ietf.org A 104.16.45.99 A 104.16.44.99
662	5.018237	10.102.110.7	172.16.99.2	DNS	75 Standard query 0x8704 AAAA static.ietf.org
663	5.018756	172.16.99.2	10.102.110.7	DNS	131 Standard query response 0x8704 AAAA static.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63
1368	5.556708	10.102.110.7	172.16.99.2	DNS	78 Standard query 0x5d2c A analytics.ietf.org
1369	5.556709	10.102.110.7	172.16.99.2	DNS	78 Standard query 0x14d2 Unknown (65) analytics.ietf.org
1370	5.557505	172.16.99.2	10.102.110.7	DNS	151 Standard query response 0x14d2 Unknown (65) analytics.ietf.org Unknown (65)
1371	5.557505	172.16.99.2	10.102.110.7	DNS	110 Standard query response 0x5d2c A analytics.ietf.org A 104.16.45.99 A 104.16.44.99
1372	5.557870	10.102.110.7	172.16.99.2	DNS	78 Standard query 0x7e58 A analytics.ietf.org
1374	5.558634	172.16.99.2	10.102.110.7	DNS	110 Standard query response 0x7e58 A analytics.ietf.org A 104.16.44.99 A 104.16.45.99
1377	5.558872	10.102.110.7	172.16.99.2	DNS	78 Standard query 0x9e9e AAAA analytics.ietf.org

> Frame 658: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{B4902142-B15D-4A67-B278-D3543EF562ED}, id 0

Important Note

For questions 11 and onwards, if you are unable get results from nslookup commands, you may use the trace files given in a zipped folder at the following link.

<http://gaia.cs.umass.edu/wiresharklabs/wireshark-traces.zip>

• Using a trace file



Download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract files. The traces in this zip file were collected by Wireshark running on one of the author's computers, while performing the steps indicated in the Wireshark lab. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting any trace file.

Now let's use nslookup and capture its packets.

- Start packet capture.
- Do an nslookup on www.mit.edu
- Stop packet capture.

(For Questions 11-15, dns-ethereal-trace-2 can be used only if you are unable get results from nslookup)

▼ today

 dns-ethereal-trace-2.pcap	11/10/2025 1:11 PM	Wireshark capture...	4 KB
 wireshark-traces.zip	11/10/2025 1:07 PM	Compressed (zip)...	514 KB

Open the first file

11. What is the destination port for the DNS query message? What is the source port of DNS response message?

Destination port:53

Source port: 3741

No.	Time	Source	Destination	Protocol	Length	Info
15	4.951232	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
16	4.951638	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
17	4.952571	128.238.38.160	128.238.29.22	DNS	80	Standard query 0x0002 A www.mit.edu.poly.edu
18	4.952953	128.238.29.22	128.238.38.160	DNS	139	Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
19	4.953172	128.238.38.160	128.238.29.22	DNS	71	Standard query 0x0003 A www.mit.edu
20	4.969929	128.238.29.22	128.238.38.160	DNS	196	Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu NS W20NS.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160

> Frame 17: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
 > Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
 > Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
 > User Datagram Protocol, Src Port: 3741, Dst Port: 53
 Source Port: 3741
 Destination Port: 53
 Length: 46
 Checksum: 0x9339 [unverified]
 [Checksum Status: Unverified]
 [Stream Index: 2]
 > [Timestamps]
 > Domain Name System (query)

Response

No.	Time	Source	Destination	Protocol	Length	Info
15	4.951232	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
16	4.951638	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
17	4.952571	128.238.38.160	128.238.29.22	DNS	80	Standard query 0x0002 A www.mit.edu.poly.edu
18	4.952953	128.238.29.22	128.238.38.160	DNS	139	Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
19	4.953172	128.238.38.160	128.238.29.22	DNS	71	Standard query 0x0003 A www.mit.edu
20	4.969929	128.238.29.22	128.238.38.160	DNS	196	Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu NS W20NS.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160

> Frame 18: 139 bytes on wire (1112 bits), 139 bytes captured (1112 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: 128.238.29.22, Dst: 128.238.38.160
 > User Datagram Protocol, Src Port: 53, Dst Port: 3741
 Source Port: 53
 Destination Port: 3741
 Length: 105
 Checksum: 0xadda [unverified]
 [Checksum Status: Unverified]
 [Stream Index: 2]
 > [Timestamps]
 > Domain Name System (response)

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Destination IP Address 128.238.29.22

Lab Manual of ‘Data Communication and Networks’

No.	Time	Source	Destination	Protocol	Length	Info
15	4.951232	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
16	4.951638	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
17	4.952571	128.238.38.160	128.238.29.22	DNS	80	Standard query 0x0002 A www.mit.edu.poly.edu
18	4.952953	128.238.29.22	128.238.38.160	DNS	139	Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
19	4.953172	128.238.38.160	128.238.29.22	DNS	71	Standard query 0x0003 A www.mit.edu
20	4.969929	128.238.29.22	128.238.38.160	DNS	196	Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu NS W20NS.mit.edu A 18.72.0.3 A 1

```
> Frame 17: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
✓ Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 66
    Identification: 0x27a2 (10146)
    > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xcd76 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.238.38.160
    Destination: 128.238.29.22
✓ User Datagram Protocol, Src Port: 3741, Dst Port: 53
```

13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Type A, ipv4 answers 0

No.	Time	Source	Destination	Protocol	Length	Info
15	4.951232	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
16	4.951638	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
17	4.952571	128.238.38.160	128.238.29.22	DNS	80	Standard query 0x0002 A www.mit.edu.poly.edu
18	4.952953	128.238.29.22	128.238.38.160	DNS	139	Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
19	4.953172	128.238.38.160	128.238.29.22	DNS	71	Standard query 0x0003 A www.mit.edu
20	4.969929	128.238.29.22	128.238.38.160	DNS	196	Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu NS W20NS.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160

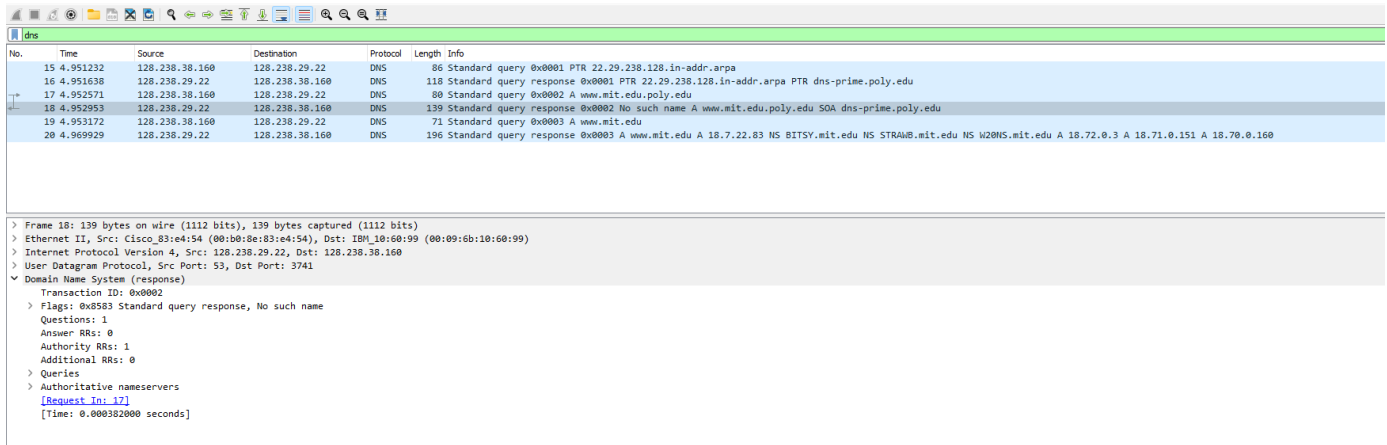
```
> Frame 17: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3741, Dst Port: 53
✓ Domain Name System (query)
    Transaction ID: 0x0002
    > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    > Queries
    [Response in: 18]
```

14. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

The DNS query is of type-A. The query message does not contain any answers.

15. Provide a screenshot

Lab Manual of ‘Data Communication and Networks’



The image shows a Wireshark packet capture of DNS traffic. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the details of the selected packet (No. 18), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (response).

No.	Time	Source	Destination	Protocol	Length	Info
15	4.951232	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
16	4.951638	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
17	4.952571	128.238.38.160	128.238.29.22	DNS	80	Standard query 0x0002 A www.mit.edu.poly.edu
18	4.952953	128.238.29.22	128.238.38.160	DNS	139	Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
19	4.953172	128.238.38.160	128.238.29.22	DNS	71	Standard query 0x0003 A www.mit.edu
20	4.969929	128.238.29.22	128.238.38.160	DNS	196	Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit.edu NS W20NS.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160

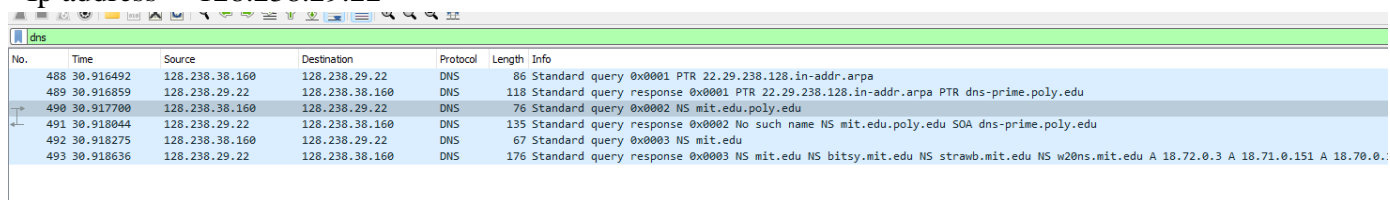
Frame 18: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 128.238.29.22, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3741
▼ Domain Name System (response)
Transaction ID: 0x0002
> Flags: 0x8583 Standard query response, No such name
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
> Queries
> Authoritative nameservers
[Request In: 17]
[Time: 0.000382800 seconds]

Now repeat the previous experiment, but instead issue the command:
nslookup –type=NS mit.edu

(For Questions 16-19, dns-ethereal-trace-3 can be used only if you are unable get results from nslookup)

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ip address 128.238.29.22



The image shows a Wireshark packet capture of DNS traffic. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the details of the selected packet (No. 490), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (response).

No.	Time	Source	Destination	Protocol	Length	Info
488	30.916492	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
489	30.916859	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
490	30.917700	128.238.38.160	128.238.29.22	DNS	76	Standard query 0x0002 NS mit.edu.poly.edu
491	30.918044	128.238.29.22	128.238.38.160	DNS	135	Standard query response 0x0002 No such name NS mit.edu.poly.edu SOA dns-prime.poly.edu
492	30.918275	128.238.38.160	128.238.29.22	DNS	67	Standard query 0x0003 NS mit.edu
493	30.918636	128.238.29.22	128.238.38.160	DNS	176	Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160

17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Lab Manual of ‘Data Communication and Networks’

No.	Time	Source	Destination	Protocol	Length	Info
488	30.916492	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
489	30.916859	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
490	30.917700	128.238.38.160	128.238.29.22	DNS	76	Standard query 0x0002 NS mit.edu.poly.edu
491	30.918044	128.238.29.22	128.238.38.160	DNS	135	Standard query response 0x0002 No such name NS mit.edu.poly.edu SOA dns-prime.poly.edu
492	30.918275	128.238.38.160	128.238.29.22	DNS	67	Standard query 0x0003 NS mit.edu
493	30.918636	128.238.29.22	128.238.38.160	DNS	176	Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160

> Frame 493: 176 bytes on wire (1408 bits), 176 bytes captured (1408 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: 128.238.29.22, Dst: 128.238.38.160

> User Datagram Protocol, Src Port: 53, Dst Port: 3746

> Domain Name System (response)

Transaction ID: 0x0003

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 3

> Queries

> Answers

> Additional records

[Request In: 492]

[Time: 0.000361000 seconds]

Type ipv4

18. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?

Yes, the response message contains the IP addresses of the MIT name servers.

19. Provide a screenshot.

No.	Time	Source	Destination	Protocol	Length	Info
488	30.916492	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
489	30.916859	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
490	30.917700	128.238.38.160	128.238.29.22	DNS	76	Standard query 0x0002 NS mit.edu.poly.edu
491	30.918044	128.238.29.22	128.238.38.160	DNS	135	Standard query response 0x0002 No such name NS mit.edu.poly.edu SOA dns-prime.poly.edu
492	30.918275	128.238.38.160	128.238.29.22	DNS	67	Standard query 0x0003 NS mit.edu
493	30.918636	128.238.29.22	128.238.38.160	DNS	176	Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160

> Frame 493: 176 bytes on wire (1408 bits), 176 bytes captured (1408 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: 128.238.29.22, Dst: 128.238.38.160

> User Datagram Protocol, Src Port: 53, Dst Port: 3746

> Domain Name System (response)

Transaction ID: 0x0003

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 3

> Queries

> Answers

> Additional records

> bitsy.mit.edu: type A, class IN, addr 18.72.0.3

> strawb.mit.edu: type A, class IN, addr 18.71.0.151

> w20ns.mit.edu: type A, class IN, addr 18.70.0.160

[Request In: 492]

[Time: 0.000361000 seconds]

Now repeat the previous experiment, but instead issue the command:
nslookup www.aiit.or.kr bitsy.mit.edu

Lab Manual of ‘Data Communication and Networks’
(For Questions 20-23, dns-ethereal-trace-4 can be used only if you are unable get results from nslookup)

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

dns						
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 PTR BITSY.MIT.EDU NS W20NS.MIT.EDU NS BITSY.MIT.EDU NS STRAWB.MIT.EDU A 18.70.0.160 A 18.72.0.3 A 18.71.0.151
102	4.279430	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.aait.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.aait.or.kr.poly.edu SOA gatekeeper.poly.edu
104	4.293517	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.aait.or.kr
105	4.307859	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A www.aait.or.kr A 218.36.94.200 NS ns.aait.or.kr NS w3.aait.or.kr A 222.106.36.66 A 222.106.36.67

> Frame 102: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 3752, Dst Port: 53

Ip address 18.70.0.3, it change from default DNS server.

21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Type: A(IPv4)

dns						
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 PTR BITSY.MIT.EDU NS W20NS.MIT.EDU NS BITSY.MIT.EDU NS STRAWB.MIT.EDU A 18.70.0.160 A 18.72.0.3
102	4.279430	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.aait.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.aait.or.kr.poly.edu SOA gatekeeper.poly.edu
104	4.293517	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.aait.or.kr
105	4.307859	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A www.aait.or.kr A 218.36.94.200 NS ns.aait.or.kr NS w3.aait.or.kr A 222.106.36.66 A 222.106.36.67

> Frame 102: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Destination: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Source: IBM_10:60:99 (00:09:6b:10:60:99)
> Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 3752, Dst Port: 53
> Domain Name System (query)

22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

Answer 1

Lab Manual of 'Data Communication and Networks'

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 PTR BITSY.MIT.EDU NS W20NS.MIT.EDU NS BITSY.MIT.EDU NS STRAW8.MIT.EDU A 18.70.0.160 A 18.72.0.3 A 18.71.0.151
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.kr.poly.edu SOA gatekeeper.poly.edu
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 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36.66 A 222.106.36.67

> Frame 105: 156 bytes on wire (1248 bits), 156 bytes captured (1248 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: 3753
> Domain Name System (response)
Transaction ID: 0x0003
> Flags: 0x0100 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 2
Additional RRs: 2
> Queries
> Answers
> Authoritative nameservers
> Additional records
[Request In: 104]
[Time: 0.014342000 seconds]

Answer the following QUESTIONS:

Q: Why does HTTP and DNS use TCP and UDP respectively?

HTTP and DNS are application layer protocols, and in order to utilize the transport layer services of for example reliable or unreliable (but fast) data transfer we only have two choices in internet: • TCP (Transmission Control Protocol) • UDP (User Datagram Protocol) The application layer encapsulates its data into the segment at the transport layer. DNS usually uses UDP as it does rely much on reliability because of its small segment size.

- If the webpage having 10 reference objects and base html located at different location, then how may HTTP and DNS request will be generated?

A DNS request from the host is sent to the local default gateway DNS server for getting the IP address of the webpage. Now because the webpage has distributed files at different locations in different servers, the DNS will query all the servers (via hierarchical DNS servers) to gather the IP addresses of all the servers at which the webpage data is distributed. Finally, the DNS response will contain the IP addresses of all the servers which contain the required webpage files. The HTTP request now contains the destination IP addresses and therefore forms the segment and then the HTTP request is sent to all those servers (either through TCP or UDP). The DNS query and response usually utilizes UDP.