

Lab 1: Packet analysis at application layer using Wireshark
SCSR1213 Network Communications
Universiti Teknologi Malaysia

Name : MADINA SURAYA BINTI ZHARIN

Matric No : A20EC0203

Section : 02

Objective:

1. Understanding of network protocols by observing the sequence of messages exchanged between two protocol entities, delving down into the details of protocol operation, and causing protocols to perform certain actions and then observing these actions and their consequences.
2. To introduce student with Wireshark software tool for packet analyzer.
3. To analyze protocol used in application layer such as http and dns.

Reference material: Computer Networking: A Top-Down Approach, 7th ed., J.F. Kurose and K.W. Ross.



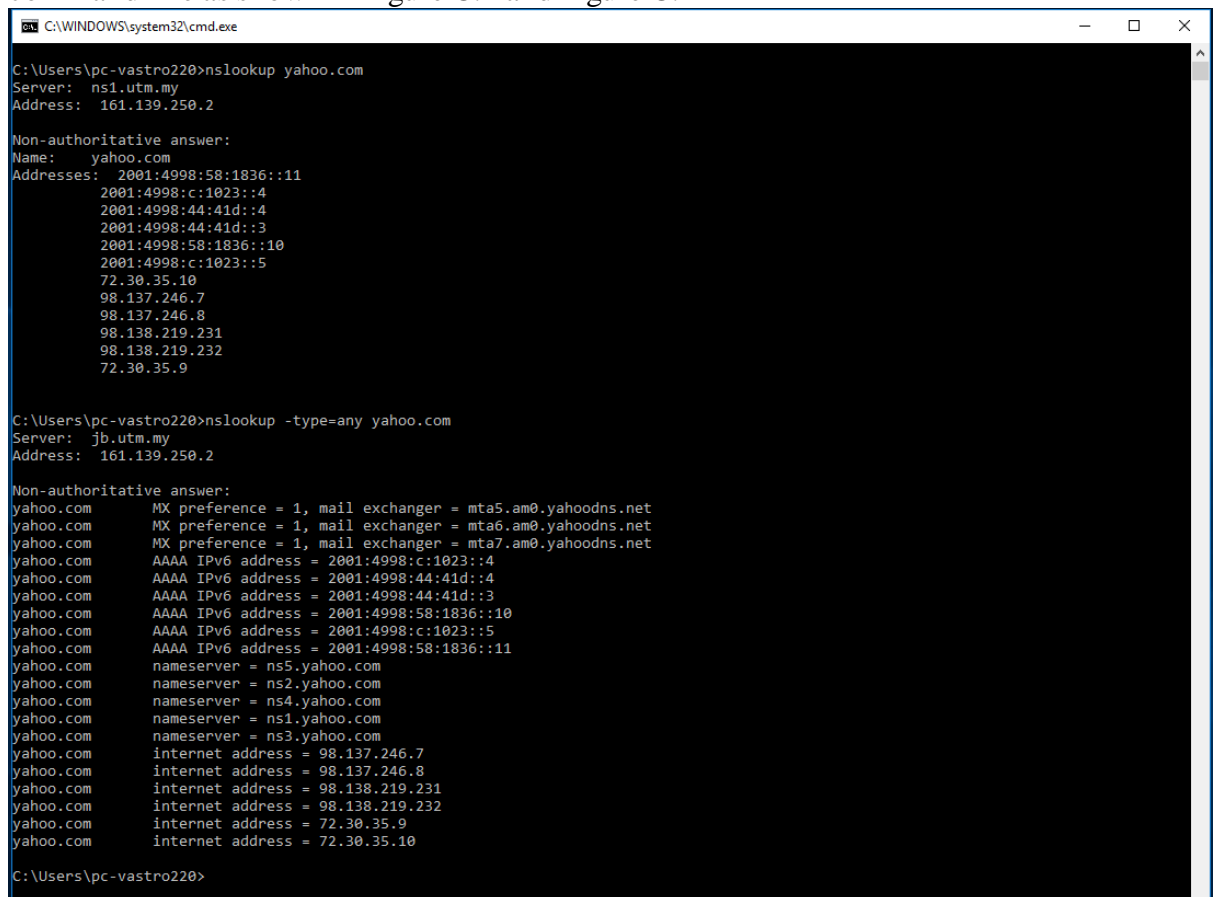
Mark

PART C: DNS Trace

1.0 nslookup

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 top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server. 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.

- To run it in Windows, open the Command Prompt (cmd) and run nslookup on the command line as shown in Figure C.1 and Figure C.2



```
C:\WINDOWS\system32\cmd.exe

C:\Users\pc-vastro220>nslookup yahoo.com
Server: ns1.utm.my
Address: 161.139.250.2

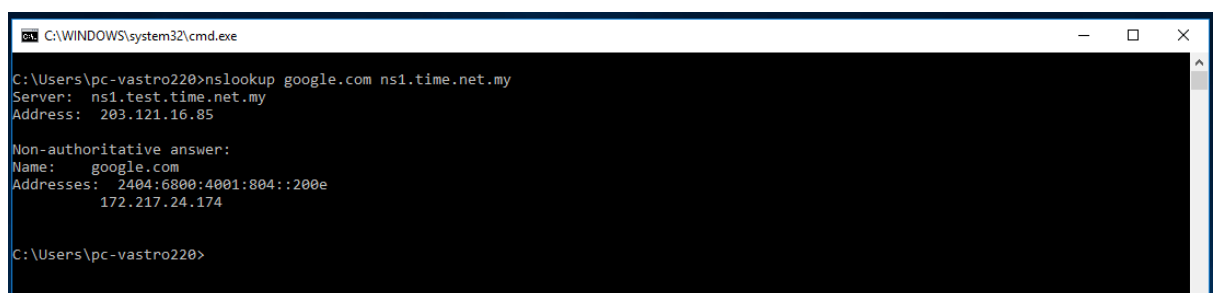
Non-authoritative answer:
Name: yahoo.com
Addresses: 2001:4998:58:1836::11
           2001:4998:c:1023::4
           2001:4998:44:41d::4
           2001:4998:44:41d::3
           2001:4998:58:1836::10
           2001:4998:c:1023::5
           72.30.35.10
           98.137.246.7
           98.137.246.8
           98.138.219.231
           98.138.219.232
           72.30.35.9

C:\Users\pc-vastro220>nslookup -type=any yahoo.com
Server: jb.utm.my
Address: 161.139.250.2

Non-authoritative answer:
yahoo.com      MX preference = 1, mail exchanger = mta5.am0.yahoodns.net
yahoo.com      MX preference = 1, mail exchanger = mta6.am0.yahoodns.net
yahoo.com      MX preference = 1, mail exchanger = mta7.am0.yahoodns.net
yahoo.com      AAAA IPv6 address = 2001:4998:c:1023::4
yahoo.com      AAAA IPv6 address = 2001:4998:44:41d::4
yahoo.com      AAAA IPv6 address = 2001:4998:44:41d::3
yahoo.com      AAAA IPv6 address = 2001:4998:58:1836::10
yahoo.com      AAAA IPv6 address = 2001:4998:c:1023::5
yahoo.com      AAAA IPv6 address = 2001:4998:58:1836::11
yahoo.com      nameserver = ns5.yahoo.com
yahoo.com      nameserver = ns2.yahoo.com
yahoo.com      nameserver = ns4.yahoo.com
yahoo.com      nameserver = ns1.yahoo.com
yahoo.com      nameserver = ns3.yahoo.com
yahoo.com      internet address = 98.137.246.7
yahoo.com      internet address = 98.137.246.8
yahoo.com      internet address = 98.138.219.231
yahoo.com      internet address = 98.138.219.232
yahoo.com      internet address = 72.30.35.9
yahoo.com      internet address = 72.30.35.10

C:\Users\pc-vastro220>
```

Figure C.1: nslookup result



```
C:\WINDOWS\system32\cmd.exe

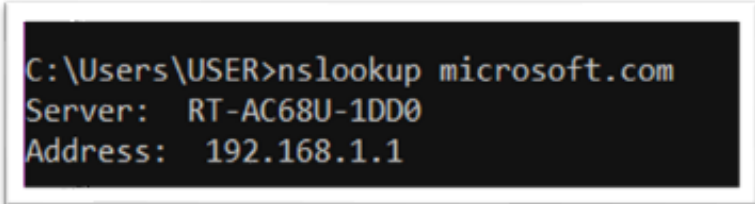
C:\Users\pc-vastro220>nslookup google.com ns1.time.net.my
Server: ns1.test.time.net.my
Address: 203.121.16.85

Non-authoritative answer:
Name: google.com
Addresses: 2404:6800:4001:804::200e
           172.217.24.174

C:\Users\pc-vastro220>
```

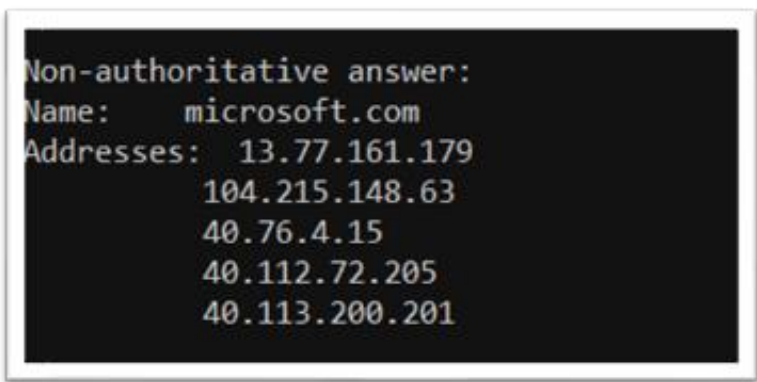
Figure C.2: nslookup result

1. Run nslookup to obtain the IP address of a www.microsoft.com server. What is the IP address of that server? Add screenshot to your answer.



```
C:\Users\USER>nslookup microsoft.com
Server: RT-AC68U-1DD0
Address: 192.168.1.1
```

2. Run nslookup to determine the non-authoritative DNS servers for domain microsoft.com. Add screenshot to your answer.

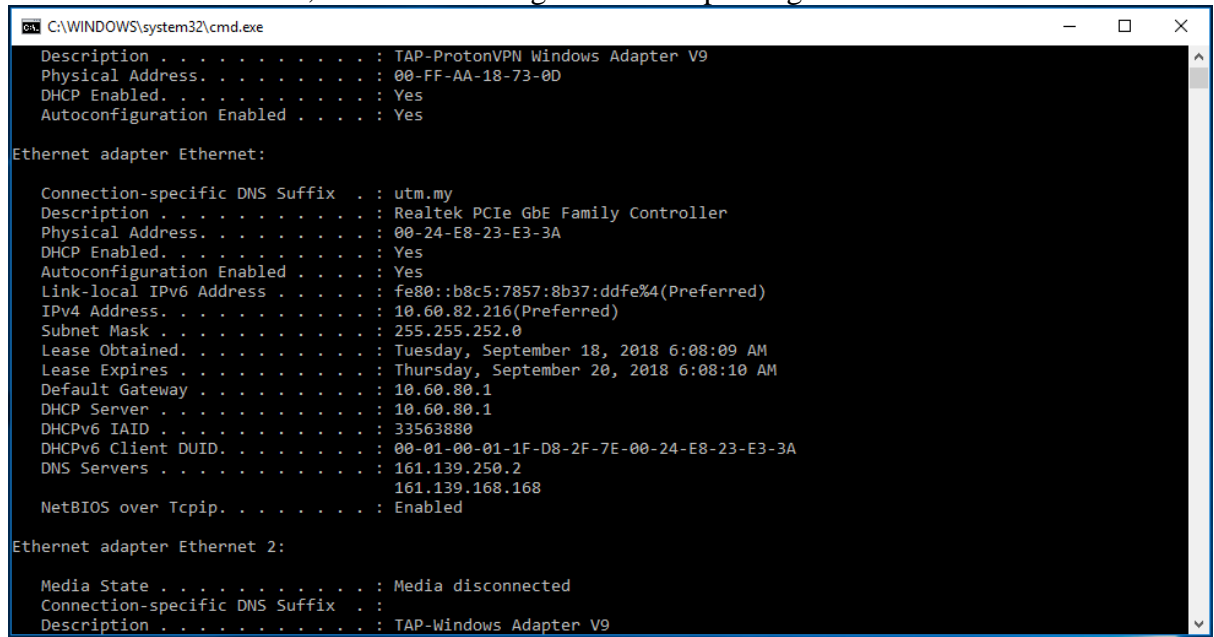


```
Non-authoritative answer:
Name: microsoft.com
Addresses: 13.77.161.179
          104.215.148.63
          40.76.4.15
          40.112.72.205
          40.113.200.201
```

2.0 ipconfig

ipconfig can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on.

- Information about host, use the following command: `ipconfig /all`



```
C:\WINDOWS\system32\cmd.exe
Description . . . . . : TAP-ProtonVPN Windows Adapter V9
Physical Address. . . . . : 00-FF-AA-18-73-0D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter Ethernet:

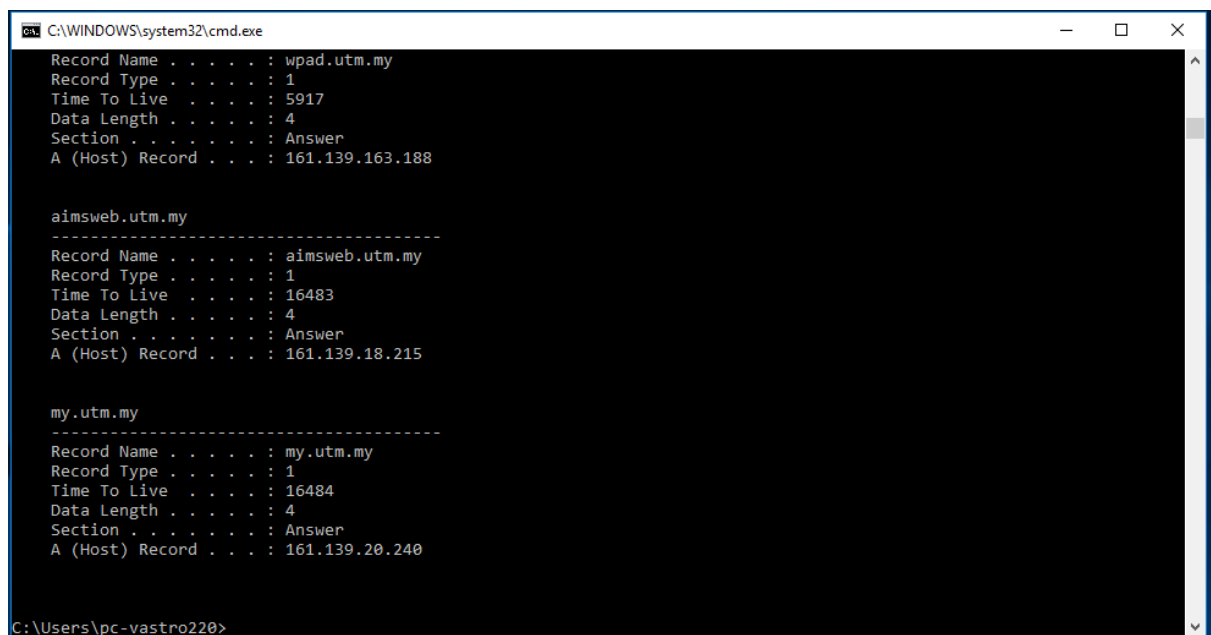
    Connection-specific DNS Suffix  . : utm.my
    Description . . . . . : Realtek PCIe GbE Family Controller
    Physical Address. . . . . : 00-24-E8-23-E3-3A
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::b8c5:7857:8b37:ddfe%4(Preferred)
    IPv4 Address. . . . . : 10.60.82.216(Preferred)
    Subnet Mask . . . . . : 255.255.252.0
    Lease Obtained. . . . . : Tuesday, September 18, 2018 6:08:09 AM
    Lease Expires . . . . . : Thursday, September 20, 2018 6:08:10 AM
    Default Gateway . . . . . : 10.60.80.1
    DHCP Server . . . . . : 10.60.80.1
    DHCPv6 IAID . . . . . : 33563880
    DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-D8-2F-7E-00-24-E8-23-E3-3A
    DNS Servers . . . . . : 161.139.250.2
                           161.139.168.168
    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
    Description . . . . . : TAP-Windows Adapter V9
```

Figure C.3: ipconfig /all result

- ipconfig is also very useful for managing the DNS information stored in your host. Each entry shows the remaining Time to Live (TTL) in seconds. Command: `ipconfig /displaydns`



```
C:\WINDOWS\system32\cmd.exe
Record Name . . . . . : wpad.utm.my
Record Type . . . . . : 1
Time To Live . . . . . : 5917
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 161.139.163.188

-----
aimsweb.utm.my
Record Name . . . . . : aimsweb.utm.my
Record Type . . . . . : 1
Time To Live . . . . . : 16483
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 161.139.18.215

-----
my.utm.my
Record Name . . . . . : my.utm.my
Record Type . . . . . : 1
Time To Live . . . . . : 16484
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 161.139.20.240

C:\Users\pc-vastro220>
```

Figure C.4: ipconfig /displaydns result

- Flushing the DNS cache clears all entries and reloads the entries from the hosts file.

Command: ipconfig /flushdns

```
C:\WINDOWS\system32\cmd.exe
C:\Users\pc-vastro220>ipconfig /flushdns

Windows IP Configuration

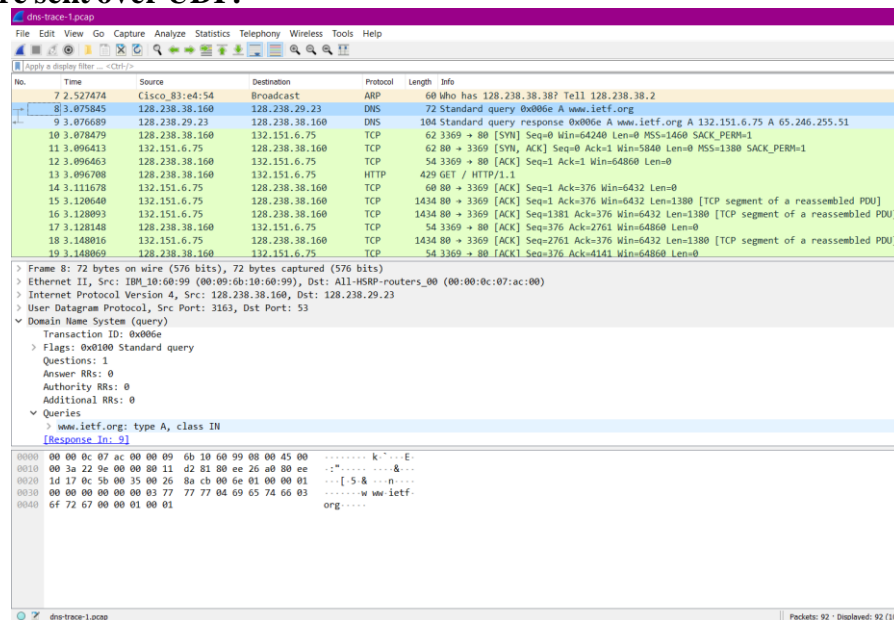
Successfully flushed the DNS Resolver Cache.

C:\Users\pc-vastro220>
```

Figure C.5: ipconfig /flushdns result

3.0 Tracing DNS with Wireshark

- Open packet trace file dns-trace-1. Answer the following questions.
1. Locate the DNS query and response messages. Are then sent over UDP or TCP? Add screenshots in your answer.
They are sent over UDP.



No.	Time	Source	Destination	Protocol	Length	Info
7	2.527474	Cisco_83:e4:54	Broadcast	ARP	60	Who has 128.238.38.38? Tell 128.238.38.2
8	3.075845	128.238.38.160	128.238.29.23	DNS	72	Standard query 0x000e A www.ietf.org
9	3.076689	128.238.29.23	128.238.38.160	DNS	104	Standard query response 0x000e A www.ietf.org A 132.151.6.75 A 65.246.255.51
10	3.078479	128.238.38.160	132.151.6.75	TCP	62	3369 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
11	3.096413	132.151.6.75	128.238.38.160	TCP	62	80 → 3369 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
12	3.096463	128.238.38.160	132.151.6.75	TCP	54	3369 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
13	3.096780	128.238.38.160	132.151.6.75	HTTP	429	GET / HTTP/1.1
14	3.111678	132.151.6.75	128.238.38.160	TCP	60	80 → 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=0
15	3.120640	132.151.6.75	128.238.38.160	TCP	1434	80 → 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
16	3.128093	132.151.6.75	128.238.38.160	TCP	1434	80 → 3369 [ACK] Seq=1381 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
17	3.128148	128.238.38.160	132.151.6.75	TCP	54	3369 → 80 [ACK] Seq=376 Ack=2761 Win=64860 Len=0
18	3.148016	132.151.6.75	128.238.38.160	TCP	1434	80 → 3369 [ACK] Seq=2761 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
19	3.148069	128.238.38.160	132.151.6.75	TCP	54	3369 → 80 [ACK] Seq=376 Ack=4141 Win=64860 Len=0

Internet Protocol Version 4, Src: 128.238.29.23, Dst: 128.238.38.160

User Datagram Protocol, Src Port: 53, Dst Port: 3163

Domain Name System (response)

Transaction ID: 0x000e

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 2

Authority RRs: 0

Additional RRs: 0

Queries

www.ietf.org: type A, class IN

Answers

[Request In: 8]

[Time: 0.000844000 seconds]

```

0000  00 09 6b 10 60 99 00 b0 8e 83 e4 54 08 00 45 00  -k.....T.E
0010  00 5a d5 95 00 00 7e 11 21 6a 80 ee 1d 17 80 ee  -Z.....lj.....
0020  26 a0 00 35 0c 5b 00 46 b0 ba 00 6e 81 80 00 01  -&-5.[F.....
0030  00 02 00 00 00 00 03 77 77 77 04 69 65 74 66 03  -.....w ww.ietf.
0040  6f 72 67 00 00 01 00 01 c0 0c 00 01 00 01 00 00  -org.....K .....
0050  06 8e 00 04 84 97 06 4b c0 0c 00 01 00 01 00 00  -.....A..3
0060  06 8e 00 04 41 f6 ff 33

```

- What is the destination port for the DNS query message? What is the source port of DNS response message? Add screenshots in your answer.

The source port of DNS response message is 53.

User Datagram Protocol, Src Port: 3163, Dst Port: 53

User Datagram Protocol, Src Port: 53, Dst Port: 3163

3. To what IP address is the DNS query message sent? Add screenshots in your answer.
The IP address is 192.168.1.148

```
Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::7c97:78e2:f43f:13f7%7
    IPv4 Address. . . . . : 192.168.1.148
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Ethernet 4:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? Add screenshots in your answer.
Type A and it does not contain any answers.

```
Transaction ID: 0x006e
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
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)
[Response In: 9]
```

```

Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
  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)
  Answers
    [Request In: 8]
    [Time: 0.000844000 seconds]

```

5. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? Add screenshots in your answer.

There are 2 answers which contains the host name, type of address, class, TTL, data length and IP address.

```

  Answers
    www.ietf.org: type A, class IN, addr 132.151.6.75
      Name: www.ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 1678 (27 minutes, 58 seconds)
      Data length: 4
      Address: 132.151.6.75
    www.ietf.org: type A, class IN, addr 65.246.255.51
      Name: www.ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 1678 (27 minutes, 58 seconds)
      Data length: 4
      Address: 65.246.255.51
    [Request In: 8]
    [Time: 0.000844000 seconds]

```


6. 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? Add screenshots in your answer.

Yes. The destination IP address of the SYN correspond to the IP addresses provided in the DNS response message which is 132.151.6.75.

No.	Time	Source	Destination	Protocol	Length	Info
9	1.876480	128.238.29.22	128.238.38.160	DNS	104	Standard query response 0x006c A www.ietf.org A 132.151.6.75 A 65.248.255.32
10	1.876474	128.238.38.160	132.151.6.75	TCP	62	62 3369 → 80 [SYN] Seq=0 Win=64320 Len=0 MSS=1460 SACK_PERM=1
11	1.896411	132.151.6.75	128.238.38.160	TCP	62	80 → 3369 [SYN, ACK] Seq=0 Ack=1 Win=5440 Len=0 MSS=1380 SACK_PERM=1
12	1.896403	128.238.38.160	132.151.6.75	TCP	54	3369 → 80 [ACK] Seq=1 Ack=1 Win=64320 Len=0
13	1.896790	128.238.38.160	132.151.6.75	HTTP	429	GET / HTTP/1.1
14	1.111670	132.151.6.75	128.238.38.160	TCP	60	80 → 3369 [ACK] Seq=1 Ack=176 Win=6432 Len=0
15	1.120640	132.151.6.75	128.238.38.160	TCP	1414	80 → 3369 [ACK] Seq=1 Ack=176 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
16	1.120693	132.151.6.75	128.238.38.160	TCP	1414	80 → 3369 [ACK] Seq=1381 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
17	1.120140	128.238.38.160	132.151.6.75	TCP	54	3369 → 80 [ACK] Seq=176 Ack=2761 Win=64320 Len=0
18	1.140015	132.151.6.75	128.238.38.160	TCP	1414	80 → 3369 [ACK] Seq=2761 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]

7. This web page contains images. Before retrieving each image, does your host issue new DNS queries? **No.**

- Open packet trace file dns-trace-2 for nslookup.
- We see from Wireshark that nslookup actually sent three DNS queries and received three DNS responses. For the purpose of this lab, ignore the first two sets of queries/responses, as they are specific to nslookup and are not normally generated by standard Internet applications. You should instead focus on the last query and response messages.
- Answer the following questions.

8. What is the destination port for the DNS query message? What is the source port of DNS response message? Add screenshots in your answer.

The destination port for the DNS query message is 53 and source port is also 53.

19	4.953172	128.238.38.160	128.238.29.22	DNS	71	Standard query 0:
20	4.969929	128.238.29.22	128.238.38.160	DNS	196	Standard query r
21	4.979464	128.238.38.2	224.0.0.2	HSRP	62	Hello (state Act
22	4.985417	Cisco_83:e4:54	Broadcast	ARP	60	Who has 128.238..
23	5.684266	3Com 96:03:80	NETBIOS-	SMB NE	214	SAM LOGON reques

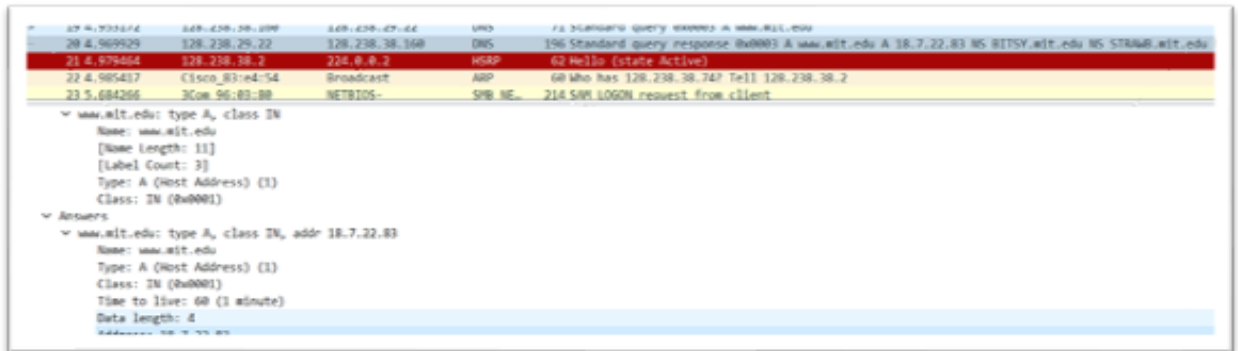
```

> Frame 20: 196 bytes on wire (1568 bits), 196 bytes captured (1568 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: 3742

```

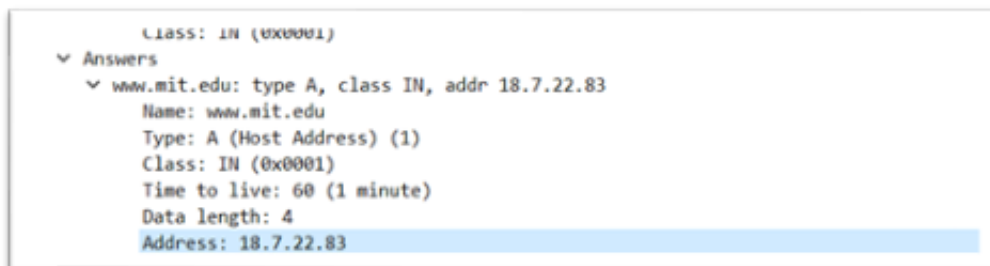
9. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? Add screenshots in your answer.

No. It sent to 187.22.83 which corresponds to mit.edu.



10. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? Add screenshots in your answer.

The DNS query message is type A which contain no answer.



11. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? Add screenshots in your answer.

There is only one answer provided by DNS response message.

