COEN 366 - LAB 3

Antoine Gaubil 40115052

WireShark 2

1. **Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?**

   I ran the command on the Asian Institute of maritime studies.

```
C:\Users\Antoine>nslookup www.aims.edu.ph
Server:  dns2.videotron.ca
Address:  24.201.245.77

Non-authoritative answer:
Name:    www.aims.edu.ph
Address:  124.107.130.204
```

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

   I ran the command on the ecole polytechnique of paris. The answer is “non-authoritative,” meaning that this answer came from the cache of some server rather than from an authoritative DNS server. The authoritative DNS server for polytechnique is milou.polytechnique.fr.

```
C:\Users\Antoine>nslookup -type=NS www.polytechnique.edu
Server:  dns2.videotron.ca
Address:  24.201.245.77

Non-authoritative answer:
www.polytechnique.edu   canonical name = drupal.polytechnique.fr

polytechnique.fr
        primary name server = milou.polytechnique.fr
        responsible mail addr = hostmaster.polytechnique.fr
        serial  = 2023110615
        refresh = 7200 (2 hours)
        retry   = 3600 (1 hour)
        expire  = 1209600 (14 days)
        default TTL = 3600 (1 hour)
```

3. **Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?**

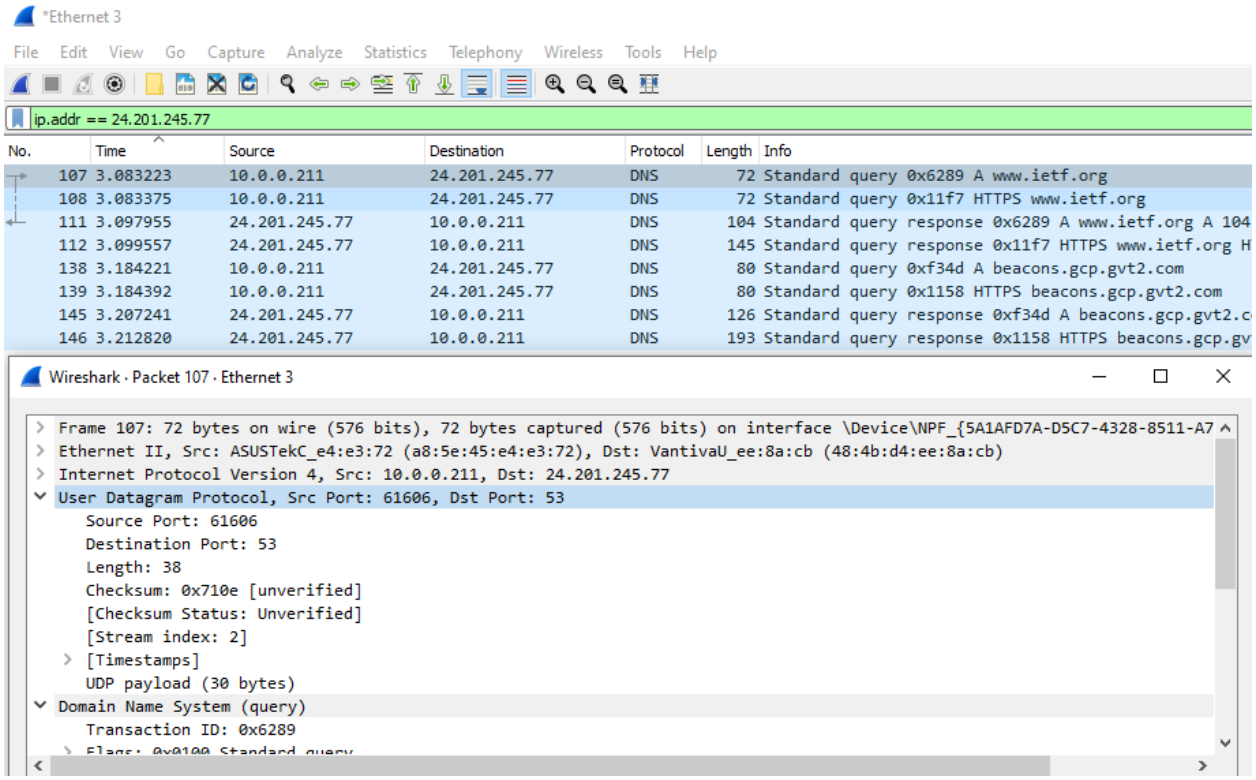
   The IP address is 66.218.84.44

```
C:\Users\Antoine>nslookup milou.polytechnique.fr mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  66.218.84.44

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

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

   The query and response messages are sent over User Datagram Protocol (UDP):



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

   Destination port of the query message is port 53. The source port of the DNS response message is port 61606.

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**?

   The DNS query message is sent to IP address 24.201.245.77 with a source of 10.0.0.211 which is the ethernet IPv4 address. Using ipconfig to determine the IP address of my local DNS server: we can see that the value of the DNS is 24.201.245.77. They match!

```
Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller #2
   Physical Address. . . . . . . . . : A8-5E-45-E4-E3-72
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.0.0.211(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : November 10, 2023 12:53:06 PM
   Lease Expires . . . . . . . . . . : November 12, 2023 12:53:02 PM
   Default Gateway . . . . . . . . . : 10.0.0.1
   DHCP Server . . . . . . . . . . . : 10.0.0.1
   DNS Servers . . . . . . . . . . . : 24.201.245.77
                                       24.200.243.189
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

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

   The DNS query message shows the following : Flags: 0x0100 Standard query as well as Answer RRs: 0. The DNS query message is a standard query (Type A) with no answers.

8. **Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?**

   The response message contains 1 answer, the address of the website requested:

```
▼ Answers
  ▼ www.ietf.org: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 185 (3 minutes, 5 seconds)
      Data length: 4
      Address: 104.16.45.99
```

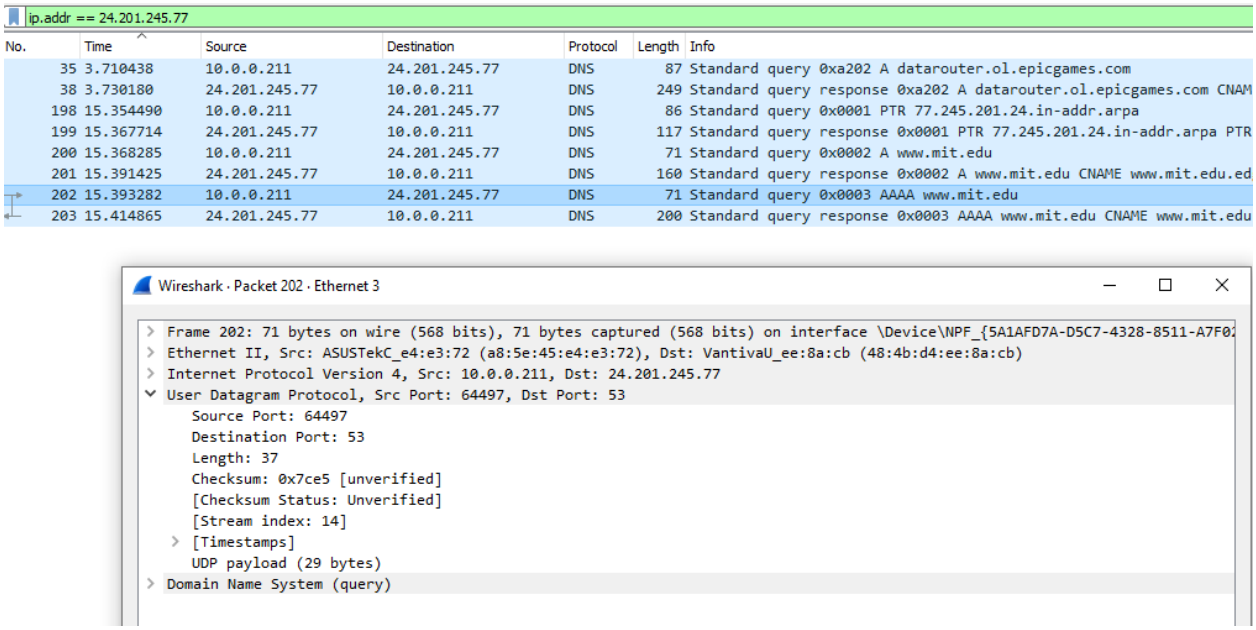
9. **Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?**

   The destination IP address is the same as the previous response message answer : 104.16.45.99.

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

    For each image, the host issues a new DNS query.

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



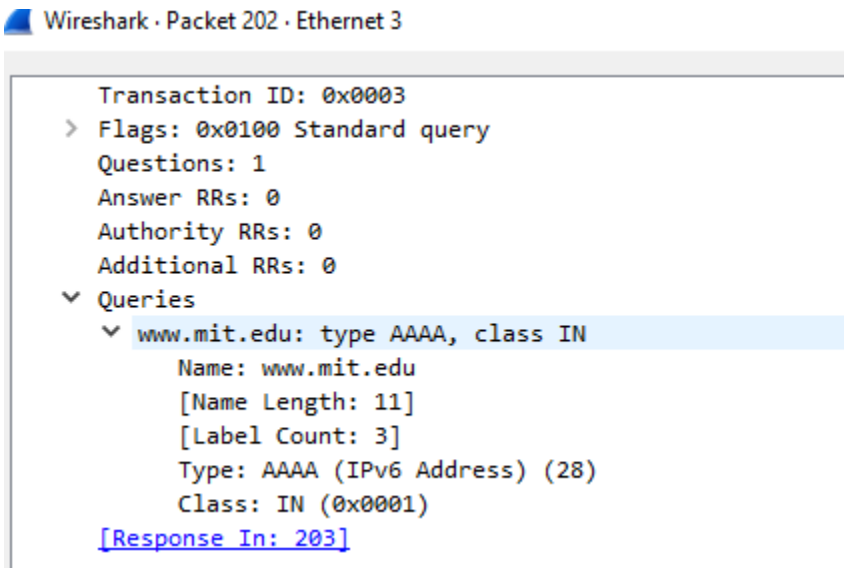
   The source port is 64497 and the destination port is 53.

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

    The query message is sent to the following IP address : 24.201.245.77 which is the same as the local DNS.

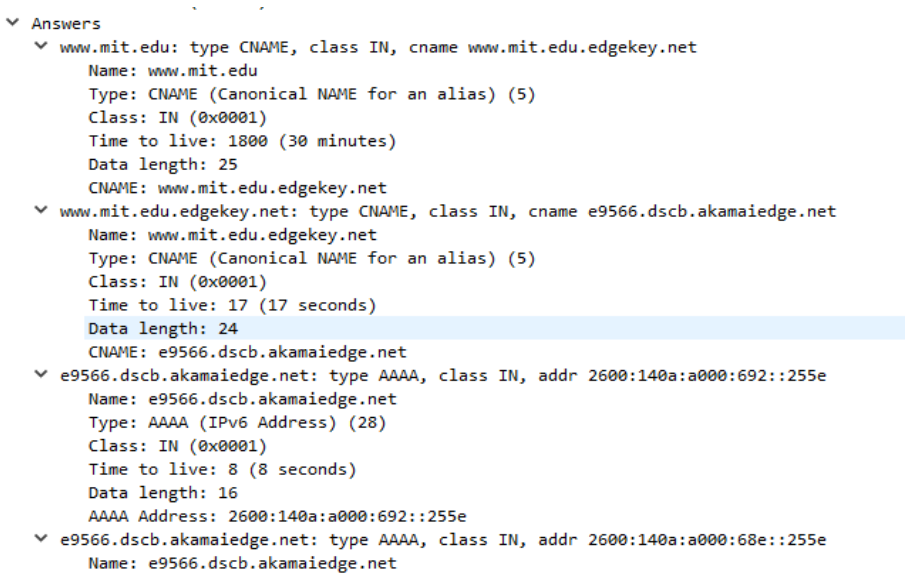
13. **Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?**

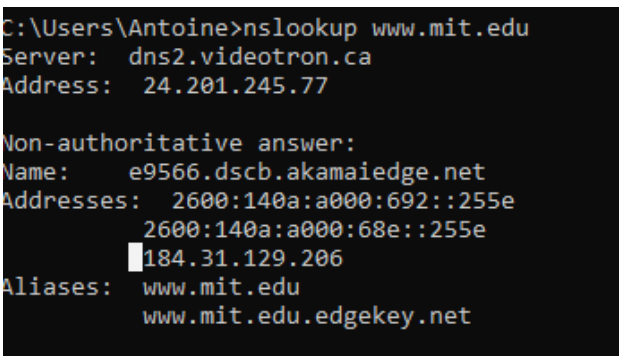
    It is a Type AAAA query with no answers :



14. **Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?**

    There are 4 answers which contain the server authoritative names and aliases of the nslookup query which match the answer on the command prompt :





15. See Above

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

The query message is sent to the following IP address : 24.201.245.77 which is the same as the local DNS.

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

It is a type NS query with no answers. Which is normal because we force -type=NS.

```
Transaction ID: 0x0002
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
v Queries
  v mit.edu: type NS, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
```

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

```
v Answers
  > mit.edu: type NS, class IN, ns eur5.akam.net
  > mit.edu: type NS, class IN, ns ns1-37.akam.net
  > mit.edu: type NS, class IN, ns asia2.akam.net
  > mit.edu: type NS, class IN, ns ns1-173.akam.net
  > mit.edu: type NS, class IN, ns usw2.akam.net
  > mit.edu: type NS, class IN, ns use2.akam.net
  > mit.edu: type NS, class IN, ns use5.akam.net
  > mit.edu: type NS, class IN, ns asia1.akam.net
```

```
C:\Users\Antoine>nslookup -type=NS mit.edu
Server:  dns2.videotron.ca
Address:  24.201.245.77

Non-authoritative answer:
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia1.akam.net
```

The response message provides 8 total answers with the MIT nameservers in different regions. The message does not include the IP addresses :

19. See Above

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?

The destination of the IP address is 18.0.72.3 which is different to the local DNS address. It belongs to MIT. “It is assigned to the ISP *Massachusetts Institute of Technology*. The address belongs to ASN 3 which is delegated to *MIT-GATEWAYS*.”

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

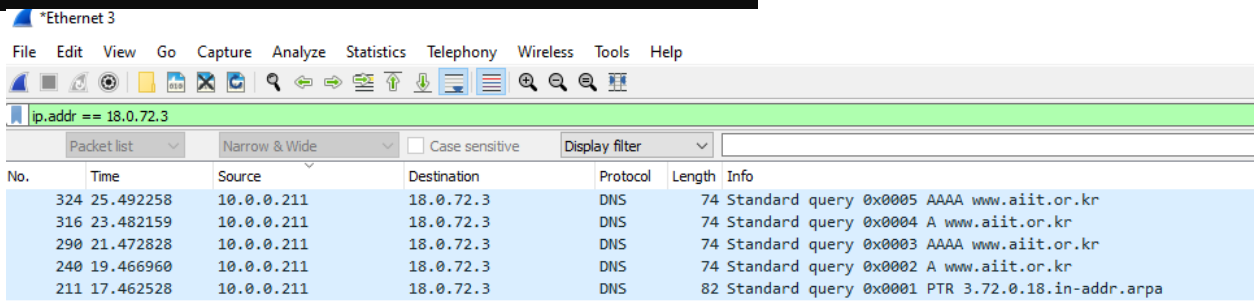
It is a type A query with no answers.

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

```
C:\Users\Antoine>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

There is one answer, which is the server’s IP address.



Mininet 1

1. Give a brief explanation about each topology mentioned above:

   Single : All hosts and switches are connected in a single line with each host connected to a switch which are connected sequentially. It forms a linear topology.

   Reversed : Switches are connected to hosts which form a linear chain; but the order of the connections are a mirror image of the single topology link order.

   Linear : Switches and hosts are connected linearly where each host is connected to à switch and switches are connected in a straight line.

   Tree : Has the structure of a hierarchical tree with a root and branches. The root is the switch and the switches are connected to the branches. The hosts are connected to the leafs (switches) and are good for larger networks because numerous efficient tree searching algorithms have been developed.

2. While trying numerous times and on different settings of the virtualBox, the system would crash every time while downloading packages after the mininet/util/install.sh -a command. I will give the commands but will not be able to provide the screenshots as the mininet did not work.

   Single with 10 hosts: sudo mn --topo single,10 --controller c0
   Reversed with 10 hosts: sudo mn --topo single,10 --controller c0
   Linear with 10 switches : sudo mn --topo linear,10 --controller c0
   Tree with 3 switches and 4 hosts : sudo mn --topo tree,depth=2,fanout=2 --controller c0

3. The python code can be found at the bottom of the assignment.

What I have learned :

In this lab, I have learned nslookup and ipconfig commands in the terminal in order to get information on servers; gather info like the authoritative main server, the different IP addresses and get specific types of requests like ND. The idea of query answers and requests through the wireshark software were useful and interesting to compare the structural response between the command prompt and the wireshark packet sniffer.
The mininet software helped me understand between the idea of virtual networks and how they are built on different topologies.

```
from mininet.net import Mininet
from mininet.node import Controller, OVSSwitch
from
mininet.cli import CLI
from mininet.log import setLogLevel

def ping_hosts(source,
destination):
    source.cmd(f'ping -c1 {destination.IP()}')

if __name__ == '__main__':

 setLogLevel('info')

    network = Mininet(controller=Controller, switch=OVSSwitch)


    controller = network.addController('c0')
    host1, host2, host3 =
network.addHost('h1'), network.addHost('h2'), network.addHost('h3')
    switch1 =
network.addSwitch('s1')

    network.addLink(host1, switch1)
    network.addLink(host2,
switch1)
    network.addLink(host3, switch1)

    network.start()
    CLI(network)


    host1.cmd('wireshark &')
    host2.cmd('wireshark &')
    host3.cmd('wireshark
&')

    ping_hosts(host1, host3)
    ping_hosts(host2, host1)
    ping_hosts(host3,
host2)

    print("Performing pingall...")
    network.pingAll()


network.stop()
```