Wireshark Lab: DNS

PART 1

1.Run *nslookup* to obtain the IP address of a Web server in Asia.
I performed nslookup for www.rediff.com

```
C:\Documents and Settings>nslookup www.rediff.com
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Name:    www.rediff.com
Address:  208.184.138.70
```

Screenshot taken after question 1

2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.
I performed nslookup for a European University in Ioannina Greece

```
C:\Documents and Settings\andromahe>cd..

C:\Documents and Settings>nslookup -type=NS uoi.gr
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Non-authoritative answer:
uoi.gr  nameserver = kouzina.noc.uoi.gr
uoi.gr  nameserver = marina.noc.uoi.gr
uoi.gr  nameserver = nic.grnet.gr

kouzina.noc.uoi.gr      internet address = 195.130.120.110
marina.noc.uoi.gr       internet address = 195.130.120.120
nic.grnet.gr    internet address = 194.177.210.210

C:\Documents and Settings>
```

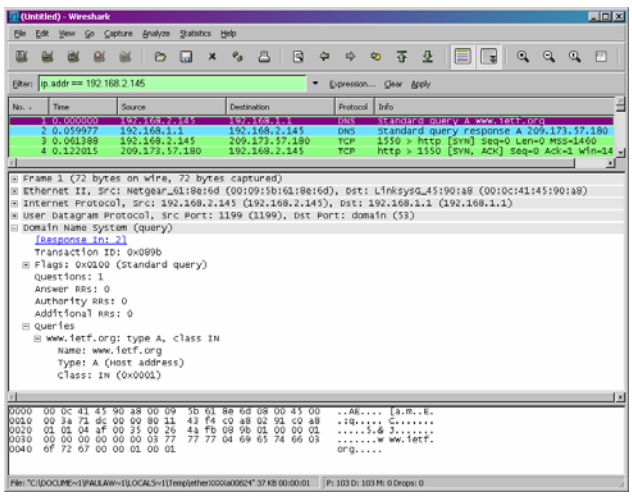
Screenshot taken after question 2

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

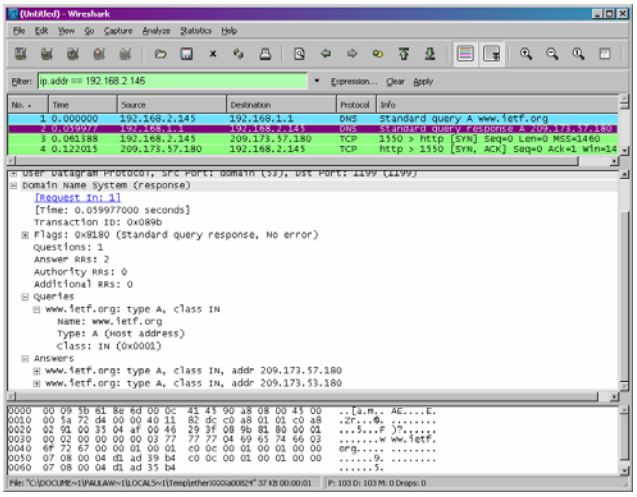
```
C:\Documents and Settings>nslookup mail.yahoo.com bitsy.mit.edu
Server:  BITSY.MIT.EDU
Address:  18.72.0.3

Non-authoritative answer:
Name:    login.yahoo.akadns.net
Address:  216.109.127.60
Aliases:  mail.yahoo.com, login.yahoo.com


C:\Documents and Settings>
```

Screenshot taken after question 3

PART 3a



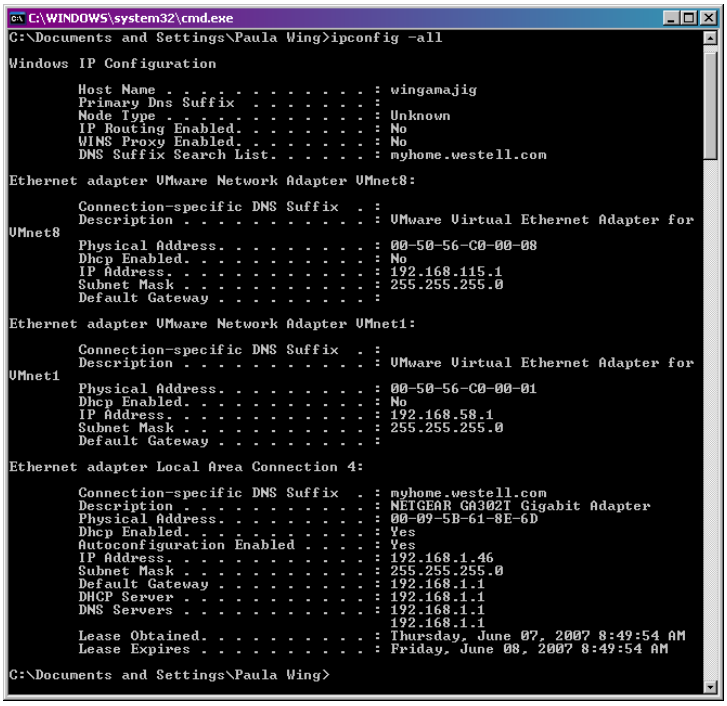
Screenshot for DNS query



Screenshot for DNS response

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

5. What is the destination port for the DNS query message? What is the source port of DNS response message?
The destination port for the DNS query is 53 and the source port of the DNS response is 53.



Screenshot for ipconfig –all

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?
It's sent to 192.168.1.1 which is the IP address of one of my local DNS servers.

7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
It's a type A Standard Query and it doesn't contain any answers.

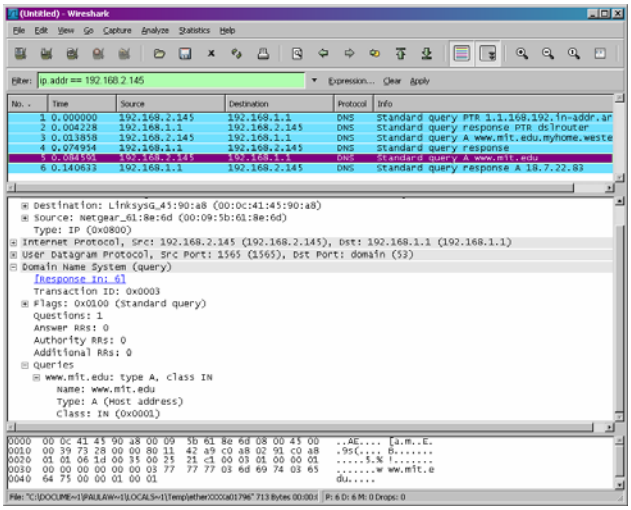
8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
There were 2 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address.

```
Answers
www.ietf.org: type A, class IN, addr 209.173.57.180
    Name: www.ietf.org
    Type: A (Host address)
    Class: IN (0x0001)
    Time to live: 30 minutes
    Data length: 4
    Addr: 209.173.57.180
www.ietf.org: type A, class IN, addr 209.173.53.180
    Name: www.ietf.org
    Type: A (Host address)
    Class: IN (0x0001)
    Time to live: 30 minutes
    Data length: 4
    Addr: 209.173.53.180
```

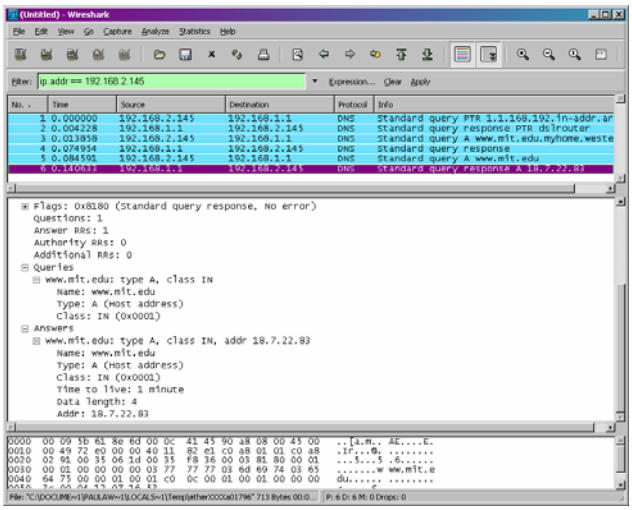
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
The first SYN packet was sent to 209.173.57.180 which corresponds to the first IP address provided in the DNS response message.

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

PART 3b



Screenshot for DNS query



Screenshot for DNS response

11. What is the destination port for the DNS query message? What is the source port of DNS response message?
The destination port of the DNS query is 53 and the source port of the DNS response is 53.

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
It's sent to 192.168.1.1 which as we can see from the ipconfig –all screenshot, is the default local DNS server.

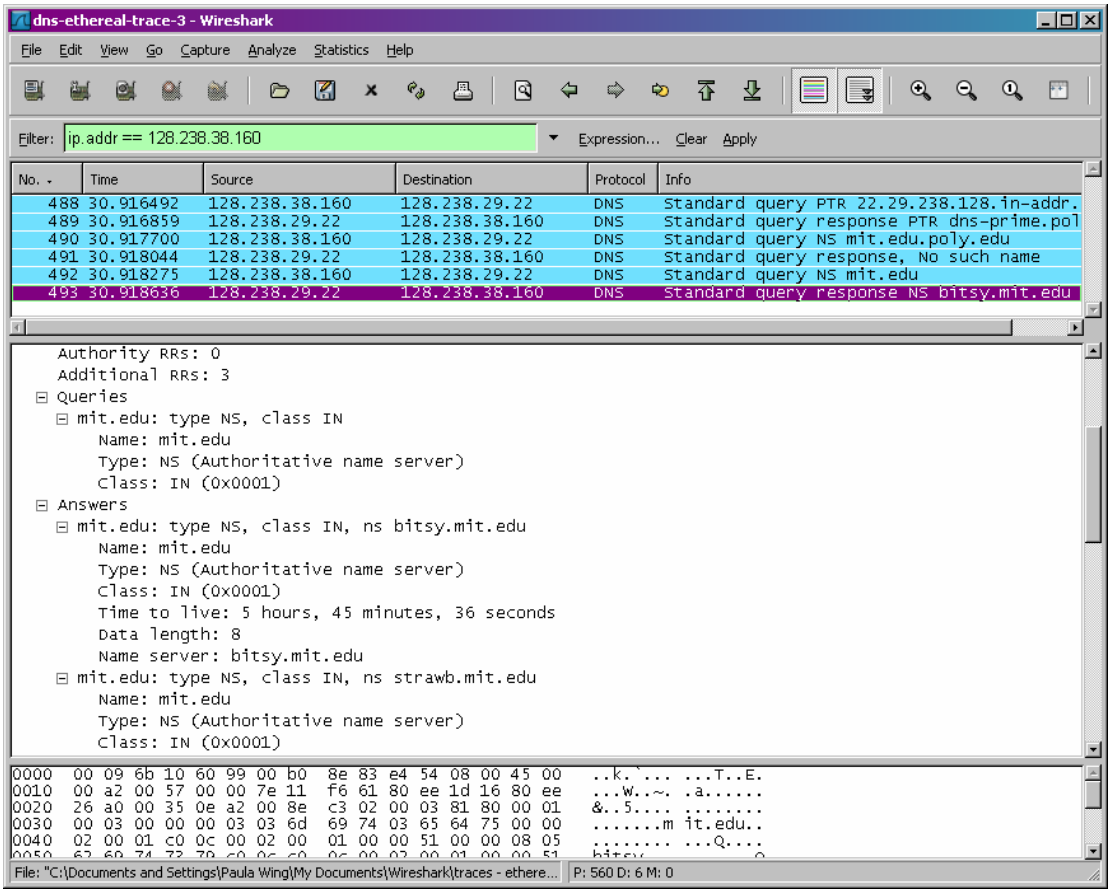
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
The query is of type A and it doesn't contain any answers.

14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
The response DNS message contains one answer containing the name of the host, the type of address, the class, and the IP address.

```
Answers
   www.mit.edu: type A, class IN, addr 18.7.22.83
       Name: www.mit.edu
       Type: A (Host address)
       Class: IN (0x0001)
       Time to live: 1 minute
       Data length: 4
       Addr: 18.7.22.83
```

15. Provide a screenshot.

PART 3c



Screenshot for DNS response

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
It was sent to 128.238.29.22 which is my default DNS server.

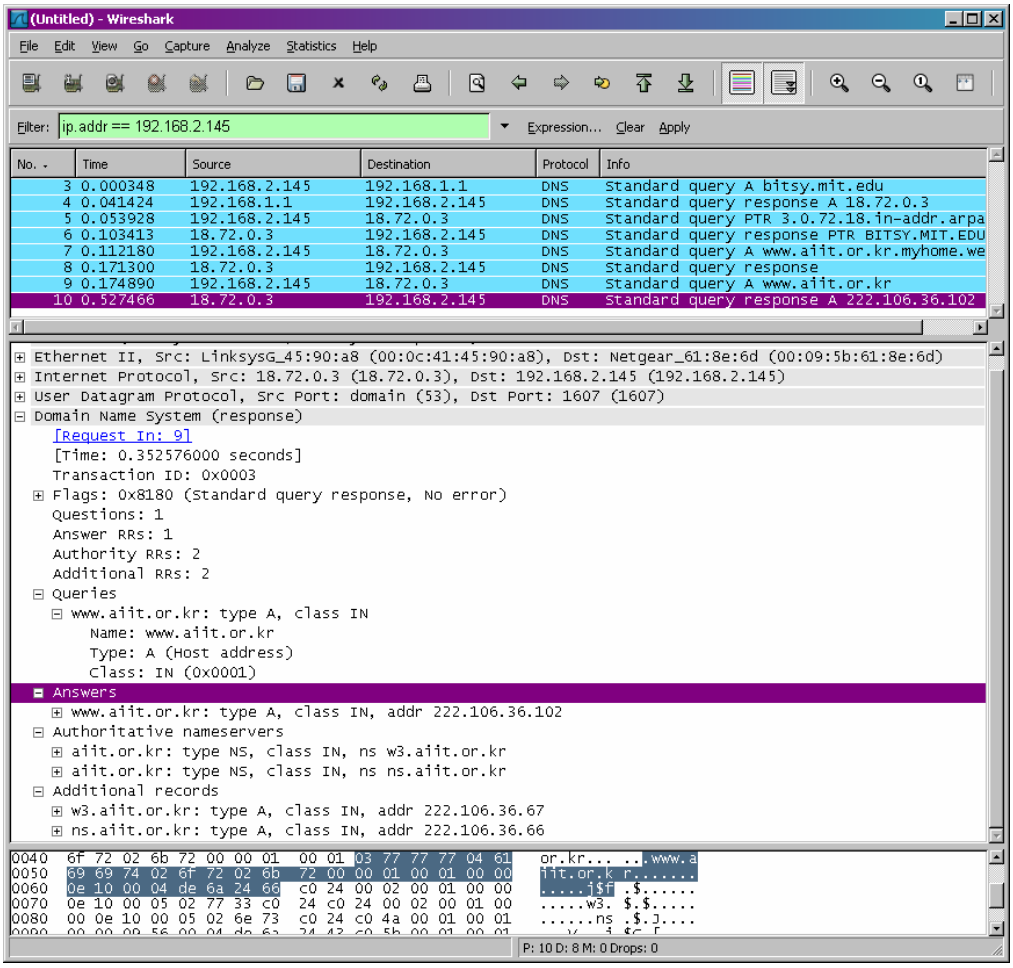
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
It's a type NS DNS query that doesn't contain any answers.

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 nameservers?
The nameservers are bitsy, strawb and w20ns. We can find their IP addresses if we expand the Additional records field in Wireshark as seen below.

```
Answers
        mit.edu: type NS, class inet, ns bitsy.mit.edu
        mit.edu: type NS, class inet, ns strawb.mit.edu
        mit.edu: type NS, class inet, ns w20ns.mit.edu
    Additional records
        bitsy.mit.edu: type A, class inet, addr 18.72.0.3
        strawb.mit.edu: type A, class inet, addr 18.71.0.151
        w20ns.mit.edu: type A, class inet, addr 18.70.0.160
```

19. Provide a screenshot.

PART 3d



Screenshot for DNS response

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 query is sent to 18.72.0.3 which corresponds to bitsy.mit.edu.

21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
It's a standard type A query that doesn't contain any answers.

22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
One answeri s provided in the DNS response message. It contains the following:

```
Answers
        www.aiit.or.kr: type A, class inet, addr 222.106.36.102
            Name: www.aiit.or.kr
            Type: Host address
            Class: inet
            Time to live: 1 hour
            Data length: 4
            Addr: 222.106.36.102
```

23. Provide a screenshot.