CSC3511 Security and Network - Week 4 Homework

Topic: DNS
(You may find it helpful to consult the DNS specifications, RFC 1034 and RFC 1035)

DNS Query Tools: nslookup vs dig

nslookup

Pros: - Available on Windows, macOS, and Linux by default
- Simple syntax; interactive mode available

Cons: - Limited output formatting
- Some consider it deprecated (though still widely used)
- Less flexible than dig

dig (Domain Information Groper)

Pros: - More detailed output
- Better for scripting
- More flexible query options
- Preferred by network professionals

Cons: - Not installed by default on Windows
- Slightly more complex syntax

> For this homework, we'll use **nslookup**, but you are encouraged to explore **dig** as well.

Basic DNS Lookup

Open a command prompt and type:

```
nslookup www.google.com
```

Notes:

1. `nslookup` is used to query DNS servers for domain names and IP addresses.
2. Running it without arguments enters *interactive mode*. Type `exit` to leave.

Questions

1. How many IP addresses do you see?
    - 3 IP addresses:
        - One DNS server `10.200.0.29`

    - One IPv4 `142.250.190.132`
    - One IPv6 ‘2607:f8b0:4009:814::2004

2. What similarities and differences do you notice between them?
    - The IPv4 and IPv6 addresses are for the same URI `www.google.com`.
    - The IP address `10.200.0.29` is for MSOE’s local DNS server.
3. What server services your reply (first line of the response)? Why might this be?
    - MSOE’s DNS server services the reply, as it has a cache of Google’s server address.
4. Does your response say *“Non-authoritative answer”*? Why might this occur?
    - Yes, it does. It means that the response is not from an authoritative server, but rather the DNS server’s cache.

Wireshark Network Analysis

Follow the steps below and answer Questions **5.1 – 5.3.**

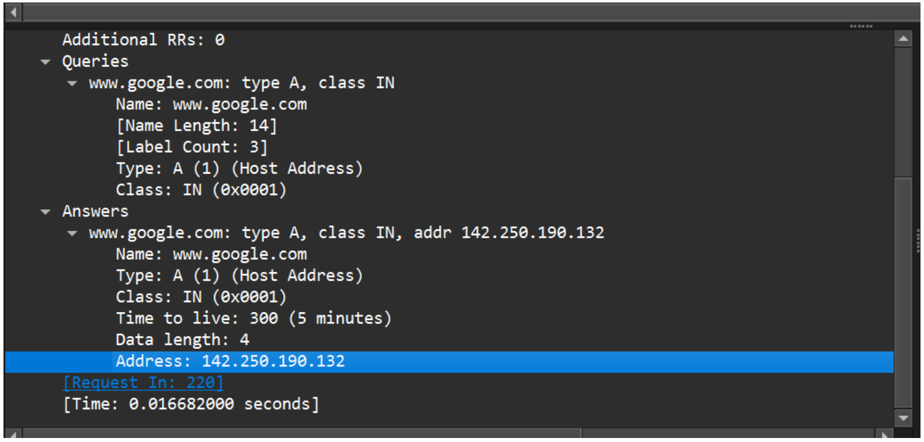
Step-by-Step Instructions

1. **Install and Launch Wireshark**
    - Download Wireshark
    - Run as administrator (Windows)
2. **Select Network Interface**
    - Choose your active network (usually WiFi) and start capture
3. **Apply DNS Filter**
    - Enter `dns` in the filter bar and press Enter
4. **Capture DNS Traffic**
    - With Wireshark running, run:

      ```
      nslookup www.google.com
      ```

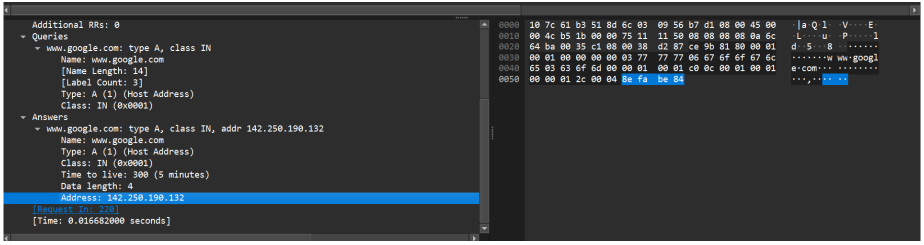
    - Stop capture after a few seconds
5. **Analyze DNS Packets**
    - Expand **Domain Name System (query)** and **(response)** sections ### Questions

5.1. Can you find the IP addresses in the response packets? - Yes, there are 2 response packets (one for IPv4 and one for IPv6). For each response packet, the IP is located within the Answers section.



```
   Additional RRs: 0
 ▾ Queries
   ▾ www.google.com: type A, class IN
       Name: www.google.com
       [Name Length: 14]
       [Label Count: 3]
       Type: A (1) (Host Address)
       Class: IN (0x0001)
 ▾ Answers
   ▾ www.google.com: type A, class IN, addr 142.250.190.132
       Name: www.google.com
       Type: A (1) (Host Address)
       Class: IN (0x0001)
       Time to live: 300 (5 minutes)
       Data length: 4
       Address: 142.250.190.132
   [Request In: 220]
   [Time: 0.016682000 seconds]
```

5.2. How are they encoded in the DNS packet structure? - IP addresses are encoded in bytes (hexadecimal digits) in the response data



```
   Additional RRs: 0
 ▾ Queries
   ▾ www.google.com: type A, class IN
       Name: www.google.com
       [Name Length: 14]
       [Label Count: 3]
       Type: A (1) (Host Address)
       Class: IN (0x0001)
 ▾ Answers
   ▾ www.google.com: type A, class IN, addr 142.250.190.132
       Name: www.google.com
       Type: A (1) (Host Address)
       Class: IN (0x0001)
       Time to live: 300 (5 minutes)
       Data length: 4
       Address: 142.250.190.132
   [Request In: 220]
   [Time: 0.016682000 seconds]
```

```
0000  10 7c 61 b3 51 8d 6c 03  09 56 b7 d1 08 00 45 00   ·|a·Q·l· ·V····E·
0010  00 4c b5 1b 00 00 75 11  11 50 08 08 08 08 0a 6c   ·L····u· ·P·····l
0020  64 ba 00 35 c1 08 00 38  d2 87 ce 9b 81 80 00 01   d··5···8 ········
0030  00 01 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 01  00 01 c0 0c 00 01 00 01   e·com··· ········
0050  00 00 01 2c 00 04 8e fa  be 84                     ···,···· ··
```

5.3. What other information do you see in the DNS packets? - We can also see information like the DNS record type, class, tile to live, length of data (in bytes) and additional flags.

> **Privacy Note:** Only capture traffic on networks you own or have permission to monitor.

Mail Query

DNS Record Types

Record Type	Description
A	Maps a domain name to an IPv4 address
MX	Mail Exchange record; specifies mail servers + priority
CNAME	Alias from one domain name to another
PTR	Used for reverse DNS lookups (IP → domain name)

MX Query Exercise

Run:

```
nslookup -q=MX mit.edu
```

Example output:

```
mit.edu mail exchanger = 10 mail.mit.edu
mit.edu mail exchanger = 20 backup-mail.mit.edu
```

Questions

6. What is the name of the mail server with the lowest priority number?

- `mail.mit.edu`

7. What server services your reply?
    - The cache of MSOE'S DNS server `10.200.0.29`
8. Does your response say *"Non-authoritative answer"*? Why might this occur?
    - Yes. This occurs as MSOE'S DNS server has a cache of the record.

Hierarchical Authoritative Lookup

Run:

```
nslookup www.msoe.edu a.root-servers.net
```

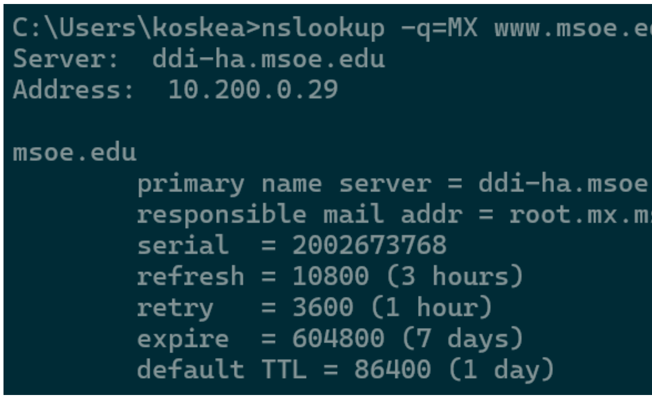
You should see:

```
Name: <domain>
Served by:
- d.gtld-servers.net
  192.31.80.30
  net
```

Questions

9. What domain name do you get while looking up the mail server?

    - Primary Name Server: `ddi-ha.msoe.edu`



```
C:\Users\koskea>nslookup -q=MX www.msoe.e
Server:  ddi-ha.msoe.edu
Address:  10.200.0.29

msoe.edu
        primary name server = ddi-ha.msoe
        responsible mail addr = root.mx.m
        serial  = 2002673768
        refresh = 10800 (3 hours)
        retry   = 3600 (1 hour)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
```

- Responsible Mail Addr: `root.mx.msoe.edu`

10. Fill in the table as you move through the DNS hierarchy:

Domain Name Server Doma	in Served IP	Address
a.root-servers.net (roo	t) 19	8.41.0.4
a.edu-servers.net edu	19	2.5.6.30
1-05.azure-dns.com msoe	.edu 13.	107.236.5

11. Explain why the root server doesn't directly return the IP for www.msoe.edu.
    - The root server doesn't return the IP for www.msoe.edu because it doesn't store specific domain records.

- What does it return instead?
    - The root server instead returns a list of .edu TLD name servers that will have the records for .edu domains.
- Why is DNS designed this way?
    - To distribute load and allow scalability
- What are the advantages of this hierarchical approach?
    -

      Scalability, reduced load, and allow for faster query times

Wireshark Sniffing

Run:

`nslookup www.nytimes.com`

Question: Roughly how many query packets do you see (not counting responses)? - There are 7 query packets

Then run:

```
nslookup -nosearch -q=A www.nytimes.com
```

12. How many query packets do you see now?
    - There are 2 query packets

- The `-nosearch` and `-q=A` options should reduce the number of packets sent.

Time To Live (TTL)

Run:

```
nslookup -d2 -nosearch -q=a www.msoe.edu
```

If that doesn't work, try:

```
nslookup -debug www.msoe.edu
```

13. What is the TTL for the message?
    - 86400 (24 hours)

- How does it change between runs?
  - It decreases as time passes between runs until the record expires and must be refreshed from the authoritative server.
- What units are used?
  - Seconds

Now query the authoritative server:

```
nslookup -d2 -nosearch -q=a www.msoe.edu <authoritative-name-server>
```

14. What is the TTL for this message?
    - 86400 seconds (24 hours)
    - How does it change between runs?
      - It does not decrease as it reports the original TTL value since it is the source of truth for the record.
    - Why does the authoritative server behave differently?
      -

        # The authoritative server returns the full TTL because its the original source of the DNS record, not a cached copy on the MSOE DNS server.

PTR Lookup

15. Use:

```
nslookup -q=PTR 64.182.211.4
```

- What is the domain name for this IP?

  - `www.northpole.com`
- Where is the company located?
  -

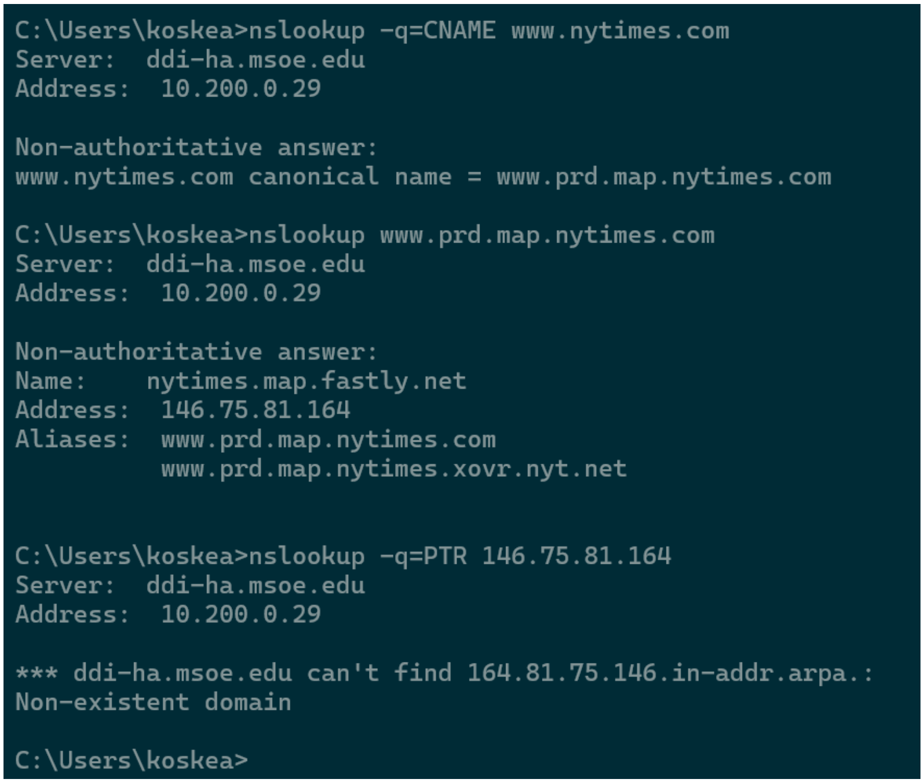
The website is hosted in a data center in Dallas, Texas (Gotten from here. Not sure what else you were asking for.)

CNAME Lookup

16. Use:

```
nslookup -q=CNAME www.nytimes.com
```

17. Then, perform a PTR lookup on the resulting IP address.



```
C:\Users\koskea>nslookup -q=CNAME www.nytimes.com
Server:  ddi-ha.msoe.edu
Address:  10.200.0.29

Non-authoritative answer:
www.nytimes.com canonical name = www.prd.map.nytimes.com

C:\Users\koskea>nslookup www.prd.map.nytimes.com
Server:  ddi-ha.msoe.edu
Address:  10.200.0.29

Non-authoritative answer:
Name:    nytimes.map.fastly.net
Address:  146.75.81.164
Aliases:  www.prd.map.nytimes.com
          www.prd.map.nytimes.xovr.nyt.net


C:\Users\koskea>nslookup -q=PTR 146.75.81.164
Server:  ddi-ha.msoe.edu
Address:  10.200.0.29

*** ddi-ha.msoe.edu can't find 164.81.75.146.in-addr.arpa.:
Non-existent domain

C:\Users\koskea>
```

Figure 1: image

- Why is the result not the same domain?
  - There is no resultant PTR record for the IP returned by the nslookup of nytimes's CNAME address.