COMP2322 Computer Networking

Lab 3 Report: DNS

Author
Wang Yuqi
[redacted]

Lecturer
Dr. LOU Wei

BsC in Computer Science
Academic year: 2024/2025 Sem 2

Tracefiles

Answer:

The trace files for this lab report are:

File Name	Parts	Questions
`./q4-q8.pcapng`	browser visit www.ietf.org	4, 6, 8
`./q12-q14.pcapng`	`nslookup` www.mit.edu	12, 14
`./q18.pcapng`	`nslookup -type=NS` mit.edu	18

DISCLAIMER To protect my **personal privacy**, only a selected subset of the original trace file is included. This partial trace retains lab-relevant traffic while scrubbing other sensitive data.

Sensitive Info The full trace contained these info that I do not wish to disclose:

- Public IPs of my private GPU compute nodes
- Public IPs of my private VPN network
- TLS handshake and key exchange messages
- Network activity that reveals my software usage and browsing habits

Questions

Question 2

Q: Run *nslookup* to find authoritative DNS servers for a university in Europe.

- Choice: University of Oxford
- Domain: `ox.ac.uk`

Step 1: query local DNS server

1. Run Command: `nslookup -type=ns ox.ac.uk`
2. Obtain Output:

```
Server:     [redacted]
Address:    [redacted]

Non-authoritative answer:
ox.ac.uk    nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk    nameserver = dns2.ox.ac.uk.
ox.ac.uk    nameserver = dns0.ox.ac.uk.
ox.ac.uk    nameserver = auth4.dns.ox.ac.uk.
ox.ac.uk    nameserver = dns1.ox.ac.uk.
ox.ac.uk    nameserver = auth5.dns.ox.ac.uk.

Authoritative answers can be found from:
auth6.dns.ox.ac.uk  internet address = 185.24.221.32
auth6.dns.ox.ac.uk  has AAAA address 2a02:2770:11:0:21a:4aff:febe:759b
[dns2.ox.ac.uk  internet address = 163.1.2.190
dns0.ox.ac.uk   internet address = 129.67.1.190
auth4.dns.ox.ac.uk  internet address = 45.33.127.156
auth4.dns.ox.ac.uk  has AAAA address 2600:3c00:e000:19::1
dns1.ox.ac.uk   internet address = 129.67.1.191
auth5.dns.ox.ac.uk  internet address = 93.93.128.67
auth5.dns.ox.ac.uk  has AAAA address 2a00:1098:0:80:1000::10]
```

Step 2: Obtain authoritative answers

1. Run Command: `nslookup -type=ns ox.ac.uk 185.24.221.32`
2. Obtain Output:

```
Server:     185.24.221.32
Address:    185.24.221.32#53

ox.ac.uk    nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk    nameserver = auth5.dns.ox.ac.uk.
ox.ac.uk    nameserver = auth4.dns.ox.ac.uk.
ox.ac.uk    nameserver = dns0.ox.ac.uk.
ox.ac.uk    nameserver = dns2.ox.ac.uk.
ox.ac.uk    nameserver = dns1.ox.ac.uk.
```

Answer: The authoritative DNS servers for the University of Oxford are:

```
auth6.dns.ox.ac.uk
auth5.dns.ox.ac.uk
auth4.dns.ox.ac.uk
dns0.ox.ac.uk
dns2.ox.ac.uk
dns1.ox.ac.uk
```

Question 4

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

Answer:

Both DNS query and response messages are sent over **UDP**.
***Note**: Captured DNS query and response packets are attached in the **Appendix**.*

Question 6

Q: 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?

I am using a macOS device. I do not have access to `ipconfig`

- Run Alternative Command: `scutil --dns`
- Obtained Output:

```
DNS configuration

resolver #1
  nameserver[0] : [redacted]
  nameserver[1] : [redacted]
  nameserver[2] : [redacted]
  if_index : 14 (en0)
  flags    : Request A records
  reach    : 0x00000002 (Reachable)
```

Answer: They are **the same**
The DNS query message is sent to the IP address `10.2.140.142`
The IP address of the local DNS server also contained `10.2.140.142`

***Note**: DNS query destination IP address can be found in **Appendix**.*

Question 8

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

Answer:

- **Two** answers are provided for both `www.ietf.org` and `static.ietf.org`.
- Answers for www.ietf.org:

```
www.ietf.org: type A, class IN, addr 104.16.44.99 \
  Name: www.ietf.org
  Type: A (1) (Host Address)
  Class: IN (0x0001)
  Time to live: 300 (5 minutes)
  Data length: 4
  Address: 104.16.44.99

www.ietf.org: type A, class IN, addr 104.16.45.99
  Name: www.ietf.org Type: A (1) (Host Address)
  Class: IN (0x0001)
  Time to live: 300 (5 minutes)
  Data length: 4
  Address: 104.16.45.99
```

- Answers for static.ietf.org:

```
static.ietf.org: type A, class IN, addr 104.16.44.99
  Name: static.ietf.org Type: A (1) (Host Address)
  Class: IN (0x0001)
  Time to live: 300 (5 minutes)
  Data length: 4
  Address: 104.16.44.99

static.ietf.org: type A, class IN, addr 104.16.45.99
  Name: static.ietf.org Type: A (1) (Host Address)
  Class: IN (0x0001)
  Time to live: 300 (5 minutes)
  Data length: 4
  Address: 104.16.45.99
```

Question 12

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

Answer:

Query message is sent to the IP: [redacted]
Yes, this is the IP address of my default local DNS server (*as in Question 6*)

Question 14

Q: Examine the DNS response message. How many "answers" are provided? What do each of these answers contain? (www.mit.edu)

Answer: There are **three** answers for `www.mit.edu`.

- `CNAME  www.mit.edu.edgekey.net`
- `CNAME  e9566.dscb.akamaiedge.net`
- `A  23.66.151.49`

Question 18

Q: 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?

Answer:
8 MIT nameservers provided, with **4** additional responses (IP addresses):

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

Additional-records
  asia2.akam.net: type A, class IN, addr 95.101.36.64
  asia1.akam.net: type A, class IN, addr 95.100.175.64
  eur5.akam.net: type A, class IN, addr 23.74.25.64
  use2.akam.net: type A, class IN, addr 96.7.49.64
```

Appendix

Query & Response: www.ietf.org

```
No.   Time      Source          Destination   Protocol Length Info
4395  28.74167  [redacted]      [redacted]    DNS      72     Standard query 0xda44 A www.ietf.org
Frame 4395: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0
Ethernet II, [redacted]
Internet Protocol Version 4, [redacted]
User Datagram Protocol, Src Port: 57249, Dst Port: 53
Domain Name System (query)

No.   Time      Source        Destination     Protocol Length Info
4396  28.755966 10.2.140.142  [redacted]      DNS      104    Standard query response 0xda44 A www.
ietf.org A 104.16.44.99 A 104.16.45.99
Frame 4396: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface en0, id 0
Ethernet II, [redacted]
Internet Protocol Version 4, [redacted]
User Datagram Protocol, Src Port: 53, Dst Port: 57249
Domain Name System (response)
  Transaction ID: 0xda44
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
    www.ietf.org: type A, class IN, addr 104.16.44.99 \
      Name: www.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.44.99
    www.ietf.org: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
  [Request In: 1]
  [Time: 0.014288000 seconds]
```

Query & Response: static.ietf.org

```
No.   Time      Source          Destination   Protocol Length Info
4493  28.886355 [redacted]      [redacted]    DNS      75     Standard query 0x857e A static.ietf.org
Frame 4493: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface en0, id 0
Ethernet II, [redacted]
Internet Protocol Version 4, [redacted]
User Datagram Protocol, Src Port: 55090, Dst Port: 53
Domain Name System (query)

No.   Time      Source        Destination     Protocol Length Info
4497  28.896616 [redacted]    [redacted]      DNS      107    Standard query response 0x857e A
static.ietf.org A 104.16.44.99 A 104.16.45.99
Frame 4497: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface en0, id 0
Ethernet II, Src: [redacted]
Internet Protocol Version 4, [redacted]
User Datagram Protocol, Src Port: 53, Dst Port: 55090
Domain Name System (response)
```

```
  Transaction ID: 0x857e
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
    static.ietf.org: type A, class IN, addr 104.16.44.99
      Name: static.ietf.org Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.44.99
    static.ietf.org: type A, class IN, addr 104.16.45.99
      Name: static.ietf.org Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
[Request In: 3]
[Time: 0.010261000 seconds]
```

Query & Response: www.mit.edu

```
No. Time      Source          Destination   Protocol Length Info
1   0.000000  [redacted]      [redacted]    DNS      71     Standard query 0xf14a A www.mit.edu
Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 0
Ethernet II, [redacted]
Internet Protocol Version 4, [redacted]
User Datagram Protocol, Src Port: 59873, Dst Port: 53
Domain Name System (query)

No. Time      Source        Destination     Protocol Length Info
2   0.082897  [redacted]    [redacted]      DNS      160    Standard query response 0xf14a A www.mit.
edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.66.151.49
Frame 2: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface en0, id 0
Ethernet II, [redacted]
Internet Protocol Version 4, [redacted]
User Datagram Protocol, Src Port: 53, Dst Port: 59873
Domain Name System (response)
```

Query & Response: `-type=NS` mit.edu

```
No.   Time               Source          Destination     Protocol Length Info
1     11:24:19.278675054 [redacted]      [redacted]      DNS      78     Standard query
  0x2df3 NS mit.edu OPT

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface wlo1, id 0
Ethernet II, [redacted]
Internet Protocol Version 4, [redacted]
User Datagram Protocol, Src Port: 36487, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x2df3
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
    Queries
    Additional records
        <Root>: type OPT
    [Response In: 2]
```

```
No.   Time               Source           Destination     Protocol Length Info
2     11:24:19.283395781 [redacted]       [redacted]      DNS      309    Standard query
  response 0x2df3 NS mit.edu NS asia2.akam.net NS asia1.akam.net NS use5.akam.net NS usw2.akam.net NS
  ns1-173.akam.net NS eur5.akam.net NS use2.akam.net NS ns1-37.akam.net A 95.101.36.64 A 95.100.175.64
  A 23.74.25.64 A 96.7.49.64 OPT

Frame 2: 309 bytes on wire (2472 bits), 309 bytes captured (2472 bits) on interface wlo1, id 0
Ethernet II, [redacted]
Internet Protocol Version 4, [redacted]
User Datagram Protocol, Src Port: 53, Dst Port: 36487
Domain Name System (response)
    Transaction ID: 0x2df3
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 5
    Queries
    Answers
        mit.edu: type NS, class IN, ns asia2.akam.net
        mit.edu: type NS, class IN, ns asia1.akam.net
        mit.edu: type NS, class IN, ns use5.akam.net
        mit.edu: type NS, class IN, ns usw2.akam.net
        mit.edu: type NS, class IN, ns ns1-173.akam.net
        mit.edu: type NS, class IN, ns eur5.akam.net
        mit.edu: type NS, class IN, ns use2.akam.net
        mit.edu: type NS, class IN, ns ns1-37.akam.net
    Additional records
        asia2.akam.net: type A, class IN, addr 95.101.36.64
        asia1.akam.net: type A, class IN, addr 95.100.175.64
        eur5.akam.net: type A, class IN, addr 23.74.25.64
        use2.akam.net: type A, class IN, addr 96.7.49.64
        <Root>: type OPT
    [Request In: 1]
    [Time: 0.004720727 seconds]
```