Project Manual

DNS Monitor

Khodarevskyi Dmytro

Faculty of Information Technology
Brno University of Technology
Czech Republic
November 8, 2024

Contents

1 Introduction **3**
- 1.1 Background / Theory . . . 3
  - 1.1.1 What is DNS? . . . 3
  - 1.1.2 DNS - A Record . . . 3
  - 1.1.3 DNS - AAAA Record . . . 3
  - 1.1.4 DNS - NS Record . . . 4
  - 1.1.5 DNS - MX Record . . . 4
  - 1.1.6 DNS - SOA Record . . . 4
  - 1.1.7 DNS - CNAME Record . . . 4
  - 1.1.8 DNS - SRV Record . . . 4
- 1.2 Objectives . . . 4

2 Methodology **5**
- 2.1 Approach . . . 5
- 2.2 Tools and Technologies . . . 5

3 Implementation **6**
- 3.1 System Design . . . 6
- 3.2 Structure . . . 6
- 3.3 Program Flowchart . . . 7
- 3.4 Implementation Details . . . 7
  - 3.4.1 Compressed names . . . 7
  - 3.4.2 Unsupported types . . . 8
  - 3.4.3 Types verbose output . . . 8
- 3.5 Program Guide . . . 10

4 Results **11**
- 4.1 Testing . . . 11
  - 4.1.1 Test 1 (List active interfaces) . . . 11
  - 4.1.2 Test 2 (Non verbose mode, Interface mode) . . . 12
  - 4.1.3 Test 3 (Non verbose mode, File mode) . . . 13

4.1.4 Test 4 (Verbose mode, File mode, A Record) 14
4.1.5 Test 5 (Verbose mode, File mode, AAAA Record) . . . 16
4.1.6 Test 6 (Verbose mode, File mode, NS Record) 18
4.1.7 Test 7 (Verbose mode, File mode, MX Record) 20
4.1.8 Test 8 (Verbose mode, File mode, SOA Record) 22
4.1.9 Test 9 (Verbose mode, File mode, CNAME Record) . . 24
4.1.10 Test 10 (Verbose mode, File mode, SRV Record) 26
4.2 Testing Summary 28

Chapter 1

Introduction

1.1 Background / Theory

1.1.1 What is DNS?

The Domain Name System (DNS) is a hierarchical and distributed name service that provides a naming system for computers, services, and other resources on the Internet or other Internet Protocol (IP) networks. It associates various information with domain names (identification strings) assigned to each of the associated entities. Most prominently, it translates readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. The Domain Name System has been an essential component of the functionality of the Internet since 1985. [1]

1.1.2 DNS - A Record

The "A" record stands for "Address" and is used to map a domain name to the IP address (IPv4) of the computer hosting the domain. When a computer looks up a domain name, it will find the corresponding IP address in the DNS record and connect to the correct server. [2]

1.1.3 DNS - AAAA Record

The "AAAA" record is an IPv6 address record that maps a hostname to a 128-bit IPv6 address. [2]

1.1.4 DNS - NS Record

The "NS" record stands for "Name Server" and indicates which DNS server is authoritative for that domain (which server contains the actual DNS records). [2]

1.1.5 DNS - MX Record

The "MX" record stands for "Mail Exchange" and directs email to a mail server. This record type is used to specify the mail server responsible for receiving email on behalf of a domain. [2]

1.1.6 DNS - SOA Record

The "SOA" record stands for "Start of Authority" and provides authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and timers relating to refreshing the zone. [2]

1.1.7 DNS - CNAME Record

The "CNAME" record stands for "Canonical Name" and is used to alias one name to another. When a DNS client requests a record that contains a CNAME, which points to another name, the DNS resolution process is repeated with the new name. [2]

1.1.8 DNS - SRV Record

The "SRV" record is a generalized service location record used when DNS queries are made for a non-existent domain. It is used to define the location of servers for specified services, such as LDAP, SIP, and XMPP. [2]

1.2 Objectives

This project aims to create a DNS monitoring tool to help monitor DNS names and corresponding IP addresses, which the program can save to files. Also, it can read information from files or specified interfaces and show it in the console to the standard output (in 2 different modes).

Chapter 2

Methodology

2.1 Approach

The approach was to use C++ to implement the project and Libpcap [4] for network packet capture. Various sources were reviewed to understand the DNS protocol and how to capture DNS packets. The project was divided into several parts: DNS parsing command line arguments, packet capturing, packet parsing, and outputting the information in the console. The project was developed using the Visual Studio Code IDE and the CMake build system.

2.2 Tools and Technologies

- `C++` - Programming language used for the implementation of the project.
- `Libpcap` - Library used for network packet capturing. [4]

Chapter 3

Implementation

3.1 System Design

The project was created using OOP with two classes, one responsible for command line arguments parsing and the other for packet capturing and parsing.

3.2 Structure

- `main.cpp` - Main file of the project.
- `ParseArgs.cpp` - Implementation of command line argument parsing.
- `ParseArgs.hpp` - Header file for ParseArgs class.
- `Monitor.cpp` - Implementation of packet capturing and DNS packets parsing.
- `Monitor.hpp` - Header file for Monitor class.
- `makefile` - Makefile for building the project.

3.3 Program Flowchart

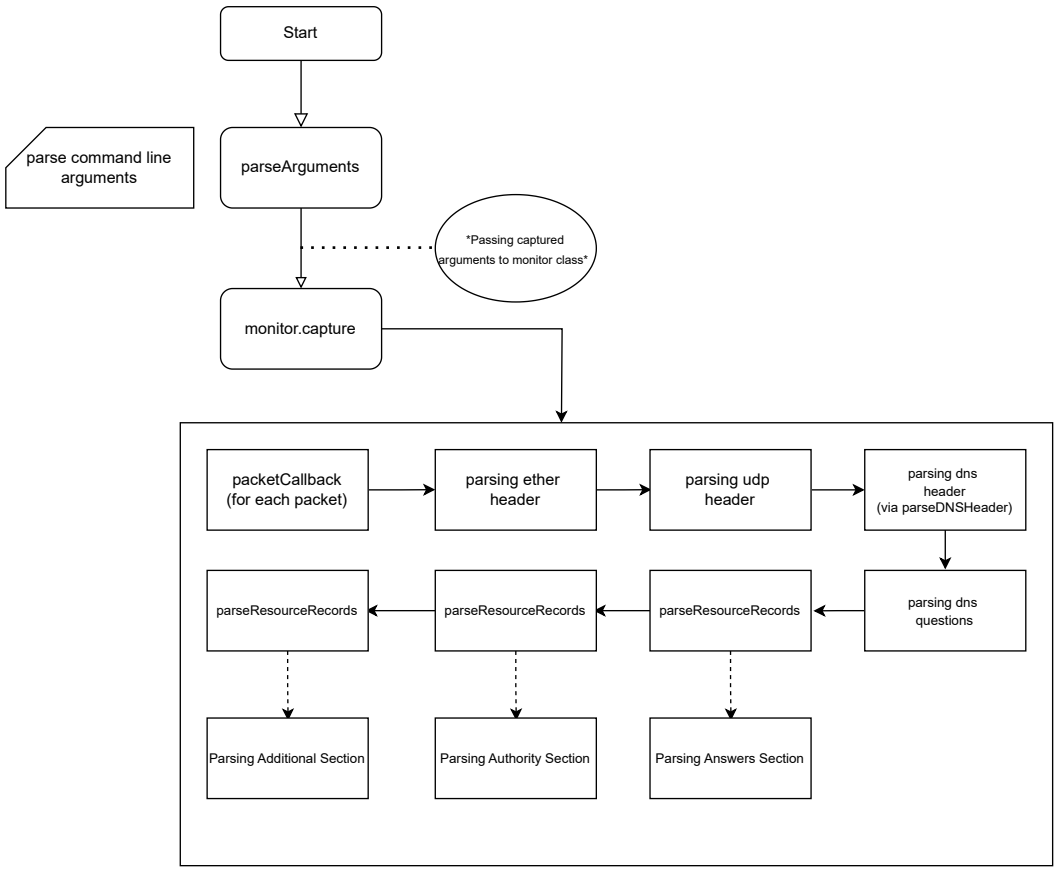

Figure 3.1: Program Flowchart

3.4 Implementation Details

3.4.1 Compressed names

In DNS records that contain domain names, the domain names are often compressed to save space. [3] This is done by replacing the domain name with a pointer to the domain name elsewhere in the packet. The pointer consists of two octets. The first two bits are set to 1, and the remaining 14 bits are the offset from the start of the packet to the domain name. This

allows for domain names to be repeated in the packet without taking up extra space.

I created a separate function called `parseDomainName`, which takes the current position in the packet, the beginning of the packet, and the string for storing the domain name and the domain's file name.

IF: first two bits are set to 1, then it is a pointer to the domain name.

THEN: Go to the offset from the start of the packet to the domain name.

IF: the first two bits are not set to 1, then it is a domain name.

THEN: Read the length of the domain name and read the domain name itself.

IF: the length of the domain name is 0, then it is the end of the domain name.

THEN: Return the domain name.

3.4.2 Unsupported types

Unsuported types are outputted with type number that was captured in the DNS packet, including the domain name, time to live, class, and mark `(unhandled type)`.

For example:

```
itojun.org. IN 255 (unhandled type)
```

3.4.3 Types verbose output

Each type has a verbose output. Format for every supported type is the following:

A Record

```
<DNS name> <TTL> <Class> A <IPv4 address>
```

For example:

```
itojun.org. 3600 IN A 210.160.95.97
```

AAAA Record

<DNS name> <TTL> <Class> AAAA <IPv6>

For example:

itojun.org. 3600 IN AAAA 2001:200:0:8002:203:47ff:fea5:3085

NS Record

<DNS name> <TTL> <Class> NS <name server>

For example:

itojun.org. 3600 IN NS coconut.itojun.org.

SOA Record

<DNS name> <TTL> <Class> SOA <primary NS> <responsible email>

<serial> <refresh> <retry> <expire> <minimum>

For example:

itojun.org. 3600 IN SOA itojun.org. root.itojun.org.

199903080 3600 300 3600000 3600

CNAME Record

<DNS name> <TTL> <Class> CNAME <canonical name>

For example:

www.wide.ad.jp. 3600 IN CNAME endo.wide.ad.jp.

SRV Record

<DNS name> <TTL> <Class> SRV <priority> <weight> <port> <target>

For example:

sip.wide.ad.jp. 3600 IN SRV 0 0 5060 sip.wide.ad.jp.

3.5 Program Guide

The program can be run with the following command line arguments:

```
./dns-monitor (-i <interface> | -p <pcapfile>) [-v] [-m] [-d <domainsfile>]
[-t <translationsfile>]
```

Parameters:

- `-i <interface>` - the name of the interface on which the program will listen, or
- `-p <pcapfile>` - the name of the PCAP file that the program will process
- `-v` - "verbose" mode: complete listing of DNS message details (optional)
- `-m` - list active interfaces (optional)
- `-d <domainsfile>` - name of the domain name file (optional), if the file does not exist, the program will create it
- `-t <translationsfile>` - name of the file with the translation of domain names to IP (optional), if the file does not exist, the program will create it

Chapter 4

Results

4.1 Testing

DISCLAIMER:

- The following results were compared with the WireShark tool, all outputs specified below are correct according to WireShark.
- Specified files was used during the testing.
  - `v6(1).pcap` - file with A, AAAA, MX, NS, SOA, CNAME packets.
  - `dns_srv.pcap` - file with SRV packets.
  - `dns-mx.pcap` - file with MX packets.
  - `SOA_text.pcap` - file with SOA packets.
  - `dns.pcap` - file with CNAME packets.

4.1.1 Test 1 (List active interfaces)

Terminal command:

```
./dns-monitor -m
```

Terminal output:

```
eth0
any
lo
docker0
bluetooth-monitor
```

```
nflog
nfqueue
dbus-system
dbus-session
```

All interfaces are listed correctly.

Output is correct. ✓

4.1.2 Test 2 (Non verbose mode, Interface mode)

Terminal 1 command:

```
sudo ./dns-monitor -i eth0
```

Terminal 2 command:

```
dig @8.8.8.8 example.com
```

Terminal 1 output:

```
2024-10-21 23:54:01 172.28.112.41 -> 8.8.8.8 (Q 1/0/0/1)
2024-10-21 23:54:01 8.8.8.8 -> 172.28.112.41 (R 1/1/0/1)
```

Terminal 2 output:

```
; <<>> DiG 9.18.24-0ubuntu0.22.04.1-Ubuntu <<>> @8.8.8.8
   example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32513
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
   ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;example.com.                    IN      A

;; ANSWER SECTION:
example.com.            2975    IN      A       93.184.215.14

;; Query time: 0 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Oct 21 23:54:01 CEST 2024
;; MSG SIZE  rcvd: 56
```

In both outputs, the IP address, count of Q., Ans., Auth., Add. are the same.

Output is correct. ✓

4.1.3 Test 3 (Non verbose mode, File mode)

Terminal command:

```
./dns-monitor -p v6\(1\).pcap
```

Output (first 4 lines):

```
1999-03-11 14:45:02 3ffe:507:0:1:200:86ff:fe05:80da -> 3ffe
   :501:4819::42 (Q 1/0/0/0)
1999-03-11 14:45:02 3ffe:501:4819::42 -> 3ffe:507:0:1:200:86
   ff:fe05:80da (R 1/6/2/5)
1999-03-11 14:45:08 3ffe:507:0:1:200:86ff:fe05:80da -> 3ffe
   :501:4819::42 (Q 1/0/0/0)
1999-03-11 14:45:08 3ffe:501:4819::42 -> 3ffe:507:0:1:200:86
   ff:fe05:80da (R 1/1/4/5)
```

In the file, the IP address, count of Q., Ans., Auth., Add. are the same.

Output is correct. ✓

4.1.4 Test 4 (Verbose mode, File mode, A Record)

Terminal command:

```
./dns-monitor -p v6\(1\).pcap -v
```

Output (A record):

```
Timestamp: 1999-03-11 14:45:08
SrcIP: 3ffe:501:4819::42
DstIP: 3ffe:507:0:1:200:86ff:fe05:80da
SrcPort: UDP/53
DstPort: UDP/2397
Identifier: 0x6
Flags: QR=1, OPCODE=0, AA=0, TC=0, RD=1, RA=1, AD=0, CD=0,
   RCODE=0

[Question Section]
www.yahoo.com. IN MX

[Answer Section]
www.yahoo.com. 796 IN MX 0 mr1.yahoo.com.

[Authority Section]
yahoo.com. 172696 IN NS ns1.yahoo.com.
yahoo.com. 172696 IN NS ns2.dca.yahoo.com.
yahoo.com. 172696 IN NS ns.europe.yahoo.com.
yahoo.com. 172696 IN NS ns5.dcx.yahoo.com.
```

```
[Additional Section]
mr1.yahoo.com. 796 IN A 206.251.17.77
ns5.dcx.yahoo.com. 172695 IN A 216.32.74.10
ns.europe.yahoo.com. 172695 IN A 195.67.49.25
ns2.dca.yahoo.com. 172695 IN A 209.143.200.34
ns1.yahoo.com. 172695 IN A 204.71.200.33
====================
```

File (A record):

```
Frame 8: 358 bytes on wire (2864 bits), 358 bytes captured
   (2864 bits)
Ethernet II, Src: 3Com_07:69:ea (00:60:97:07:69:ea), Dst:
   Megahertz_05:80:da (00:00:86:05:80:da)
Internet Protocol Version 6, Src: 3ffe:501:4819::42, Dst: 3
   ffe:507:0:1:200:86ff:fe05:80da
User Datagram Protocol, Src Port: 53, Dst Port: 2397
Domain Name System (response)
        Transaction ID: 0x0006
        Flags: 0x8180 Standard query response, No error
        Questions: 1
        Answer RRs: 1
        Authority RRs: 4
        Additional RRs: 5
        Queries
        Answers
        Authoritative nameservers
        Additional records
                mr1.yahoo.com: type A, class IN, addr
                   206.251.17.77
                ns5.dcx.yahoo.com: type A, class IN, addr
                   216.32.74.10
                ns.europe.yahoo.com: type A, class IN, addr
                   195.67.49.25
                ns2.dca.yahoo.com: type A, class IN, addr
                   209.143.200.34
                ns1.yahoo.com: type A, class IN, addr
                   204.71.200.33
        [Request In: 7]
        [Time: 0.135013000 seconds]
```

According to the same packet in WireShark, the output is correct.

Output is correct. ✓

4.1.5 Test 5 (Verbose mode, File mode, AAAA Record)

Terminal command:

```
./dns-monitor -p v6\(1\).pcap -v
```

Output (AAAA record):

```
Timestamp: 1999-03-11 14:45:18
SrcIP: 3ffe:501:4819::42
DstIP: 3ffe:507:0:1:200:86ff:fe05:80da
SrcPort: UDP/53
DstPort: UDP/2398
Identifier: 0x2C72
Flags: QR=1, OPCODE=0, AA=0, TC=0, RD=1, RA=1, AD=0, CD=0,
    RCODE=0

[Question Section]
kiwi.itojun.org. IN AAAA

[Answer Section]
kiwi.itojun.org. 3425 IN AAAA 3ffe:501:410:0:2c0:dfff:fe47:33
    e
kiwi.itojun.org. 3425 IN AAAA 3ffe:501:410:100:5254:ff:feda
    :48bf

[Authority Section]
itojun.org. 3474 IN NS coconut.itojun.org.
itojun.org. 3474 IN NS tiger.hiroo.oshokuji.org.

[Additional Section]
tiger.hiroo.oshokuji.org. 3425 IN A 210.145.33.242
coconut.itojun.org. 3425 IN A 210.160.95.97
```

```
[Additional Section]
mr1.yahoo.com. 796 IN A 206.251.17.77
ns5.dcx.yahoo.com. 172695 IN A 216.32.74.10
ns.europe.yahoo.com. 172695 IN A 195.67.49.25
ns2.dca.yahoo.com. 172695 IN A 209.143.200.34
ns1.yahoo.com. 172695 IN A 204.71.200.33
====================
```

File (AAAA record):

```
Frame 15: 282 bytes on wire (2256 bits), 282 bytes captured
   (2256 bits)
Ethernet II, Src: 3Com_07:69:ea (00:60:97:07:69:ea), Dst:
   Megahertz_05:80:da (00:00:86:05:80:da)
Internet Protocol Version 6, Src: 3ffe:501:4819::42, Dst: 3
   ffe:507:0:1:200:86ff:fe05:80da
User Datagram Protocol, Src Port: 53, Dst Port: 2398
Domain Name System (response)
        Transaction ID: 0x2c72
        Flags: 0x8180 Standard query response, No error
        Questions: 1
        Answer RRs: 2
        Authority RRs: 2
        Additional RRs: 2
        Queries
                kiwi.itojun.org: type AAAA, class IN
        Answers
                kiwi.itojun.org: type AAAA, class IN, addr 3
                   ffe:501:410:0:2c0:dfff:fe47:33e
                kiwi.itojun.org: type AAAA, class IN, addr 3
                   ffe:501:410:100:5254:ff:feda:48bf
        Authoritative nameservers
        Additional records
        [Request In: 14]
        [Time: 0.012374000 seconds]
```

4.1.6 Test 6 (Verbose mode, File mode, NS Record)

Terminal command:

```
./dns-monitor -p v6\(1\).pcap -v
```

Output (NS record):

```
Timestamp: 1999-03-11 14:45:37
SrcIP: 3ffe:501:4819::42
DstIP: 3ffe:507:0:1:200:86ff:fe05:80da
SrcPort: UDP/53
DstPort: UDP/2405
Identifier: 0xB362
Flags: QR=1, OPCODE=0, AA=1, TC=0, RD=1, RA=1, AD=0, CD=0,
    RCODE=0

[Question Section]
www.wide.ad.jp. IN AAAA

[Answer Section]
www.wide.ad.jp. 3600 IN CNAME endo.wide.ad.jp.
endo.wide.ad.jp. 3600 IN AAAA 3ffe:501:0:1001::2

[Authority Section]
wide.ad.jp. 3600 IN NS ns.wide.ad.jp.
wide.ad.jp. 3600 IN NS ns.tokyo.wide.ad.jp.
wide.ad.jp. 3600 IN NS ns.rcac.tdi.co.jp.

[Additional Section]
ns.wide.ad.jp. 3600 IN A 203.178.136.63
ns.tokyo.wide.ad.jp. 3600 IN A 203.178.136.61
ns.rcac.tdi.co.jp. 86400 IN A 202.249.17.17
====================
```

File (NS record):

```
Frame 115: 322 bytes on wire (2576 bits), 322 bytes captured
   (2576 bits)
Ethernet II, Src: 3Com_07:69:ea (00:60:97:07:69:ea), Dst:
   Megahertz_05:80:da (00:00:86:05:80:da)
Internet Protocol Version 6, Src: 3ffe:501:4819::42, Dst: 3
   ffe:507:0:1:200:86ff:fe05:80da
User Datagram Protocol, Src Port: 53, Dst Port: 2405
Domain Name System (response)
    Transaction ID: 0xb362
    Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 3
    Additional RRs: 3
    Queries
    Answers
    Authoritative nameservers
        wide.ad.jp: type NS, class IN, ns ns.wide.ad.jp
            Name: wide.ad.jp
            Type: NS (2) (authoritative Name Server)
            Class: IN (0x0001)
            Time to live: 3600 (1 hour)
            Data length: 15
            Name Server: ns.wide.ad.jp
        wide.ad.jp: type NS, class IN, ns ns.tokyo.wide.ad.jp
            Name: wide.ad.jp
            Type: NS (2) (authoritative Name Server)
            Class: IN (0x0001)
            Time to live: 3600 (1 hour)
            Data length: 21
            Name Server: ns.tokyo.wide.ad.jp
        wide.ad.jp: type NS, class IN, ns ns.rcac.tdi.co.jp
            Name: wide.ad.jp
            Type: NS (2) (authoritative Name Server)
            Class: IN (0x0001)
            Time to live: 3600 (1 hour)
            Data length: 19
            Name Server: ns.rcac.tdi.co.jp
    Additional records
    [Request In: 114]
    [Time: 0.678878000 seconds]
```

According to the same packet in WireShark, the output is correct.

Output is correct. ✓

4.1.7 Test 7 (Verbose mode, File mode, MX Record)

Terminal command:

```
./dns-monitor -p dns-mx.pcap -v
```

Output (MX record):

```
Timestamp: 2013-12-03 22:09:57
SrcIP: 10.2.95.39
DstIP: 10.180.156.185
SrcPort: UDP/53
DstPort: UDP/51427
Identifier: 0x4C17
Flags: QR=1, OPCODE=0, AA=0, TC=0, RD=1, RA=1, AD=0, CD=0,
    RCODE=0

[Question Section]
mx.com. IN MX

[Answer Section]
mx.com. 3600 IN MX 10 cluster5.us.messagelabs.com.
mx.com. 3600 IN MX 20 cluster5a.us.messagelabs.com.

[Authority Section]
mx.com. 3600 IN NS dns2.stabletransit.com.
mx.com. 3600 IN NS dns1.stabletransit.com.

[Additional Section]
dns2.stabletransit.com. 1302 IN A 65.61.188.4
dns1.stabletransit.com. 3559 IN A 69.20.95.4
====================
```

File (MX record):

```
Frame 2: 216 bytes on wire (1728 bits), 216 bytes
   captured (1728 bits)
Ethernet II, Src: Jetcell_d1:76:00 (00:d0:2b:d1
   :76:00), Dst: Apple_ff:51:cb (00:1f:5b:ff:51:cb)
Internet Protocol Version 4, Src: 10.2.95.39, Dst:
   10.180.156.185
User Datagram Protocol, Src Port: 53, Dst Port: 51427
Domain Name System (response)
        Transaction ID: 0x4c17
        Flags: 0x8180 Standard query response, No
           error
        Questions: 1
        Answer RRs: 2
        Authority RRs: 2
        Additional RRs: 2
        Queries
        Answers
                mx.com: type MX, class IN, preference
                    10, mx cluster5.us.messagelabs.
                   com
                        Name: mx.com
                        Type: MX (15) (Mail eXchange)
                        Class: IN (0x0001)
                        Time to live: 3600 (1 hour)
                        Data length: 28
                        Preference: 10
                        Mail Exchange: cluster5.us.
                           messagelabs.com
                mx.com: type MX, class IN, preference
                    20, mx cluster5a.us.messagelabs.
                   com
                        Name: mx.com
                        Type: MX (15) (Mail eXchange)
                        Class: IN (0x0001)
                        Time to live: 3600 (1 hour)
                        Data length: 14
                        Preference: 20
                        Mail Exchange: cluster5a.us.
                           messagelabs.com
        Authoritative nameservers
        Additional records
        [Request In: 1]
        [Time: 0.082653000 seconds]
```

According to the same packet in WireShark, the output is correct.

Output is correct. ✓

4.1.8 Test 8 (Verbose mode, File mode, SOA Record)

Terminal command:

```
./dns-monitor -p SOA_test.pcap -v
```

Output (SOA record):

```
Timestamp: 2024-10-13 18:42:34
SrcIP: 147.229.3.200
DstIP: 100.69.162.61
SrcPort: UDP/53
DstPort: UDP/56452
Identifier: 0x5EFE
Flags: QR=1, OPCODE=0, AA=0, TC=0, RD=1, RA=1, AD=0, CD=0,
    RCODE=0

[Question Section]
wikipedia.org. IN SOA

[Answer Section]
wikipedia.org. 3571 IN SOA ns0.wikimedia.org. hostmaster.
    wikimedia.org. 2024072620 43200 7200 1209600 3600

[Authority Section]

[Additional Section]
====================
```

File (SOA record):

```
Frame 7: 137 bytes on wire (1096 bits), 137 bytes captured
   (1096 bits)
Ethernet II, Src: Routerboardc_64:db:82 (48:8f:5a:64:db:82),
   Dst: AzureWaveTec_c5:bc:0b (48:e7:da:c5:bc:0b)
Internet Protocol Version 4, Src: 147.229.3.200, Dst:
   100.69.162.61
User Datagram Protocol, Src Port: 53, Dst Port: 56452
Domain Name System (response)
Transaction ID: 0x5efe
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
        wikipedia.org: type SOA, class IN
Answers
        wikipedia.org: type SOA, class IN, mname ns0.
           wikimedia.org
                Name: wikipedia.org
                Type: SOA (6) (Start Of a zone of Authority)
                Class: IN (0x0001)
                Time to live: 3571 (59 minutes, 31 seconds)
                Data length: 52
                Primary name server: ns0.wikimedia.org
                Responsible authority's mailbox: hostmaster.
                   wikimedia.org
                Serial Number: 2024072620
                Refresh Interval: 43200 (12 hours)
                Retry Interval: 7200 (2 hours)
                Expire limit: 1209600 (14 days)
                Minimum TTL: 3600 (1 hour)
[Request In: 6]
[Time: 0.002694000 seconds]
```

According to the same packet in WireShark, the output is correct.

Output is correct. ✓

4.1.9 Test 9 (Verbose mode, File mode, CNAME Record)

Terminal command:

```
./dns-monitor -p dns.pcap -v
```

Output (CNAME record):

```
Timestamp: 2016-01-08 21:59:15
SrcIP: 4.2.2.1
DstIP: 172.16.16.154
SrcPort: UDP/53
DstPort: UDP/52723
Identifier: 0x5D96
Flags: QR=1, OPCODE=0, AA=0, TC=0, RD=1, RA=1, AD=0, CD=0,
    RCODE=0

[Question Section]
cdn.optimizely.com. IN A

[Answer Section]
cdn.optimizely.com. 11 IN CNAME wac.946A.edgecastcdn.net.
wac.946A.edgecastcdn.net. 1357 IN CNAME gp1.wac.v2cdn.net.
gp1.wac.v2cdn.net. 2664 IN A 72.21.91.8

[Authority Section]

[Additional Section]
====================
```

File (CNAME record):

```
Frame 3: 160 bytes on wire (1280 bits), 160 bytes captured
   (1280 bits) on interface en0, id 0
Ethernet II, Src: CiscoLinksys_17:8c:e8 (c0:c1:c0:17:8c:e8),
   Dst: Apple_cb:b2:56 (78:31:c1:cb:b2:56)
Internet Protocol Version 4, Src: 4.2.2.1, Dst: 172.16.16.154
User Datagram Protocol, Src Port: 53, Dst Port: 52723
Domain Name System (response)
        Transaction ID: 0x5d96
        Flags: 0x8180 Standard query response, No error
        Questions: 1
        Answer RRs: 3
        Authority RRs: 0
        Additional RRs: 0
        Queries
        Answers
                cdn.optimizely.com: type CNAME, class IN,
                   cname wac.946A.edgecastcdn.net
                        Name: cdn.optimizely.com
                        Type: CNAME (5) (Canonical NAME for
                           an alias)
                        Class: IN (0x0001)
                        Time to live: 11 (11 seconds)
                        Data length: 26
                        CNAME: wac.946A.edgecastcdn.net
                wac.946A.edgecastcdn.net: type CNAME, class
                   IN, cname gp1.wac.v2cdn.net
                        Name: wac.946A.edgecastcdn.net
                        Type: CNAME (5) (Canonical NAME for
                           an alias)
                        Class: IN (0x0001)
                        Time to live: 1357 (22 minutes, 37
                           seconds)
                        Data length: 16
                        CNAME: gp1.wac.v2cdn.net
                gp1.wac.v2cdn.net: type A, class IN, addr
                   72.21.91.8
        [Unsolicited: True]
```

According to the same packet in WireShark, the output is correct.

Output is correct. ✓

4.1.10 Test 10 (Verbose mode, File mode, SRV Record)

Terminal command:

```
./dns-monitor -p dns_srv.pcap -v
```

Output (SRV record):

```
Timestamp: 2024-10-16 17:43:07
SrcIP: 147.229.3.100
DstIP: 100.69.167.117
SrcPort: UDP/53
DstPort: UDP/50259
Identifier: 0x209F
Flags: QR=1, OPCODE=0, AA=0, TC=0, RD=1, RA=1, AD=0, CD=0,
   RCODE=0

[Question Section]
_xmpp-client._tcp.jabber.org. IN SRV

[Answer Section]
_xmpp-client._tcp.jabber.org. 60 IN SRV 60 60 60 zeus-v6.
   jabber.org.
_xmpp-client._tcp.jabber.org. 60 IN SRV 30 30 30 zeus.jabber.
   org.

[Authority Section]

[Additional Section]
zeus.jabber.org. 830 IN A 208.68.163.216
zeus-v6.jabber.org. 830 IN AAAA 2605:da00:5222:5269::2:3
        0 (unhandled class) OPT (EDNS)
====================
```

File (SRV record):

```
Frame 79: 216 bytes on wire (1728 bits), 216 bytes captured
   (1728 bits)
Ethernet II, Src: Routerboardc_64:db:82 (48:8f:5a:64:db:82),
   Dst: Intel_4f:63:98 (48:68:4a:4f:63:98)
Internet Protocol Version 4, Src: 147.229.3.100, Dst:
   100.69.167.117
User Datagram Protocol, Src Port: 53, Dst Port: 50259
Domain Name System (response)
        Transaction ID: 0x209f
        Flags: 0x8180 Standard query response, No error
        Questions: 1
        Answer RRs: 2
        Authority RRs: 0
        Additional RRs: 3
        Queries
                _xmpp-client._tcp.jabber.org: type SRV, class
                    IN
                        Name: _xmpp-client._tcp.jabber.org
                        [Name Length: 28]
                        [Label Count: 4]
                        Type: SRV (33) (Server Selection)
                        Class: IN (0x0001)
        Answers
                _xmpp-client._tcp.jabber.org: type SRV, class
                    IN, priority 60, weight 30, port 5222,
                   target zeus-v6.jabber.org
                        Service: _xmpp-client
                        Protocol: _tcp
                        Name: jabber.org
                        Type: SRV (33) (Server Selection)
                        Class: IN (0x0001)
                        Time to live: 60 (1 minute)
                        Data length: 26
                        Priority: 60
                        Weight: 30
                        Port: 5222
                        Target: zeus-v6.jabber.org
                _xmpp-client._tcp.jabber.org: type SRV, class
                    IN, priority 30, weight 30, port 5222,
                   target zeus.jabber.org
                        Service: _xmpp-client
                        Protocol: _tcp
                        Name: jabber.org
                        Type: SRV (33) (Server Selection)
                        Class: IN (0x0001)
                        Time to live: 60 (1 minute)
```

```
                    Data length: 23
                    Priority: 30
                    Weight: 30
                    Port: 5222
                    Target: zeus.jabber.org
Additional records
[Request In: 62]
[Time: 0.044324000 seconds]
```

According to the same packet in WireShark, the output is correct.

Output is correct. ✓

4.2 Testing Summary

All tests above were passed successfully, complete edjecases were not tested. The program is able to parse DNS packets and display them in a human-readable format. The output is correct and matches the output from WireShark. The program is able to parse different types of DNS records, such as A, AAAA, CNAME, MX, NS, SOA, and SRV.

Bibliography

[1] Wikipedia, *Domain Name System*, 2001.

Available at:

https://en.wikipedia.org/wiki/Domain_Name_System.

[2] Wikipedia, *List of DNS record types*, 2007.

Available at:

https://en.wikipedia.org/wiki/List_of_DNS_record_types.

[3] Alan Mislove, *Simple DNS Client*, Fundamentals of Computer Networking, 2011.

Available at:

https://mislove.org/teaching/cs4700/spring11/handouts/project1-primer.pdf.

[4] Tcpdump Group, *Tcpdump & Libpcap*, Latest 2024.

Available at:

https://www.tcpdump.org/index.html#documentation.