CS 352 Project 2 - DNS Analysis Report

Students:

- Christopher Doss (cad407)
- Brian Zhang (bz271)

Part A: Wireshark Answers

Part A Questions and Answers

Question 1: What is the value of domain name found in the question section of the dns query? (For each query in the test suite)

Query 1: ilab1.cs.rutgers.edu (A record)

Hexadecimal Representation:

```
05 69 6c 61 62 31 02 63 73 07 72 75 74 67 65 72 73 03 65 64 75 00
```

Query 2: ilab1.cs.rutgers.edu (AAAA record)

Hexadecimal Representation:

```
05 69 6c 61 62 31 02 63 73 07 72 75 74 67 65 72 73 03 65 64 75 00
```

Query 3: whale.stanford.edu (AAAA)

Hexadecimal Representation:

```
05 77 68 61 6c 65 08 73 74 61 6e 66 6f 72 64 03 65 64 75 00
```

Explanation: Full domain name encoding: (5)whale(8)stanford(3)edu(0)

Query 4: www.princeton.edu (A)

Hexadecimal Representation:

```
03 77 77 77 09 70 72 69 6e 63 65 74 6f 6e 03 65 64 75 00
```

Explanation: Full domain name encoding: (3)www(9)princeton(3)edu(0)

Question 2: What is the value of domain name found in the answer section of dns response? Explain (For each query)

Query 1 & 2: ilab1.cs.rutgers.edu (both A and AAAA)

Hexadecimal Representation:

```
c0 0c
```

Explanation: DNS pointer compression - points to byte offset 12 where the name is stored in question section

Query 3: whale.stanford.edu (AAAA)

Hexadecimal Representation:

```
c0 12
```

Explanation: DNS pointer compression - points to byte offset 0x12 where "stanford.edu" is stored. This is the Name field of the resource record in the answer section.

Query 4: www.princeton.edu (A)

Hexadecimal Representation:

```
c0 0c
```

Explanation: DNS pointer compression - points to byte offset 0x0c (12) where the query domain is stored in the question section

---

Question 3: What is the value of the rdlength field in the dns response message? (For each query)

Query 1: ilab1.cs.rutgers.edu (A record response)

RDLENGTH: `00 04`

Query 2: ilab1.cs.rutgers.edu (AAAA record response)

RDLENGTH: `00 10`

Query 3: whale.stanford.edu (AAAA record response)

RDLENGTH: `00 29`

Query 4: www.princeton.edu (A record response)

RDLENGTH: `00 04`

Question 4: What is the value of the address received in the dns response message? (For each query)

Query 1: ilab1.cs.rutgers.edu (A record)

Answer IP: `128.6.13.2` **Hexadecimal:** `80 06 0d 02`

Query 2: ilab1.cs.rutgers.edu (AAAA record)

Answer IP: `2620:0:d60:ac0d::2` **Hexadecimal:** `26 20 00 00 0d 60 ac 0d 00 00 00 00 00 00 00 02`

Query 3: whale.stanford.edu (AAAA record)

Answer: No AAAA record found - SOA response only **Result:** NXDOMAIN for AAAA type

Query 4: www.princeton.edu (A record)

Answer IPs (CNAME chain):

- `104.18.5.101` → Hex: `68 12 05 65`
- `104.18.4.101` → Hex: `68 12 04 65` **Note:** Response includes CNAME www.princeton.edu.cdn.cloudflare.net before A records

---

Part B: NS Records Queries

Part B Questions and Answers

Question 5: What is the value of QDCOUNT, ANCOUNT, NSCOUNT, ARCOUNT in the dns response message? (For each query)

Query 1: rutgers.edu (NS)

```
QDCOUNT: 00 01
ANCOUNT: 00 05
NSCOUNT: 00 00
ARCOUNT: 00 00
```

Query 2: rutgers.edu (NS)

```
QDCOUNT: 00 01
ANCOUNT: 00 05
NSCOUNT: 00 00
ARCOUNT: 00 00
```

Query 3: stanford.edu (NS)

```
QDCOUNT: 00 01
ANCOUNT: 00 06
NSCOUNT: 00 00
ARCOUNT: 00 00
```

Query 4: princeton.edu (NS)

```
QDCOUNT: 00 01
ANCOUNT: 00 09
NSCOUNT: 00 00
ARCOUNT: 00 00
```

Question 6: What is the value of the rdlength field in the dns response message? (For each resource record in each response)

Query 1 & 2: rutgers.edu NS Records

Nameserver	RDLENGTH (hex)
ns1.rutgers.edu	00 06
runs2.rutgers.edu	00 08
ns6.dnsmadeeasy.com	00 15
ns5.dnsmadeeasy.com	00 06
ns7.dnsmadeeasy.com	00 06

Query 3: stanford.edu NS Records

Nameserver	RDLENGTH (hex)
atalante.stanford.edu	00 0b
argus.stanford.edu	00 08

Nameserver	RDLENGTH (hex)
avallone.stanford.edu	00 0b
ns6.dnsmadeeasy.com	00 15
ns7.dnsmadeeasy.com	00 06
ns5.dnsmadeeasy.com	00 06

Query 4: princeton.edu NS Records

Nameserver	RDLENGTH (hex)
a7-65.akam.net	00 08
a1-158.akam.net	00 11
a20-65.akam.net	00 09
a3-67.akam.net	00 08
a6-64.akam.net	00 08
a24-66.akam.net	00 09
ns5.dnsmadeeasy.com	00 06
ns6.dnsmadeeasy.com	00 06
ns7.dnsmadeeasy.com	00 15

Question 7: What are the name server names received in the response? (For each query)

Query 1 & 2: rutgers.edu Nameservers

```
1. ns1.rutgers.edu
2. runs2.rutgers.edu
3. ns6.dnsmadeeasy.com
4. ns5.dnsmadeeasy.com
5. ns7.dnsmadeeasy.com
```

Query 3: stanford.edu Nameservers

```
1. atalante.stanford.edu
2. argus.stanford.edu
3. avallone.stanford.edu
4. ns6.dnsmadeeasy.com
5. ns7.dnsmadeeasy.com
6. ns5.dnsmadeeasy.com
```

Query 4: princeton.edu Nameservers

```
1. a7-65.akam.net
2. a1-158.akam.net
3. a20-65.akam.net
4. a3-67.akam.net
5. a6-64.akam.net
6. a24-66.akam.net
7. ns5.dnsmadeeasy.com
8. ns6.dnsmadeeasy.com
9. ns7.dnsmadeeasy.com
```

Part C: Iterative Resolver

Part C Questions and Answers

Question 8: What is the value of the type field in the first dns query among the iterative messages? (For each query in test suite)

Query 1: ilab1.cs.rutgers.edu (A record) - Packet 1

Type field: `00 02`

Query 2: ilab1.cs.rutgers.edu (AAAA record) - Packet 17

Type field: `00 02` (AAAA record, IPv6 address)

Query 3: whale.stanford.edu (AAAA record) - Packet 33

Type field: `00 02` (AAAA record, IPv6 address)

Query 4: www.princeton.edu (A record) - Packet 49

Type field: `00 02` (A record, IPv4 address)

Question 9: What is the value of the type field value in resource records in first dns response message among the iterative messages? (For each query)

Query 1: ilab1.cs.rutgers.edu - First Response from Root (Packet 2)

Section	Type	Hex Value	Count	Record Examples
Authority	NS	`00 02`	13	d.edu-servers.net, b.edu-servers.net, etc.
Additional	A	`00 01`	6	192.31.80.30, 192.33.14.30, etc.

Section	Type	Hex Value	Count	Record Examples
Additional	AAAA	`00 1c`	5	2001:500:856e::30, 2001:503:231d::2:30, etc.

Query 2: ilab1.cs.rutgers.edu (AAAA) - First Response from Root (Packet 18)

Section	Type	Hex Value	Count	Record Examples
Authority	NS	`00 02`	13	Same 13 edu-servers
Additional	A	`00 01`	6	Same A records for edu servers
Additional	AAAA	`00 1c`	5	Same AAAA records for edu servers

Query 3: whale.stanford.edu - First Response from Root (Packet 34)

Section	Type	Hex Value	Count	Record Examples
Authority	NS	`00 02`	13	Same 13 edu-servers
Additional	A	`00 01`	6	Same A records for edu servers
Additional	AAAA	`00 1c`	5	Same AAAA records for edu servers

Query 4: www.princeton.edu - First Response from Root (Packet 50)

Section	Type	Hex Value	Count	Record Examples
Authority	NS	`00 02`	13	Same 13 edu-servers
Additional	A	`00 01`	6	Same A records for edu servers
Additional	AAAA	`00 1c`	5	Same AAAA records for edu servers

Question 10: What is the destination IP of second dns query sent? Where is this ip found from? (For each query)

Query 1: ilab1.cs.rutgers.edu (A) - Second Query (Packet 3)

Destination IP: `192.31.80.30` **Hexadecimal:** `c0 1f 50 1e`

Where found: From glue record (A record) for `d.edu-servers.net` in Additional section of first root response (Packet 2)

Query 2: ilab1.cs.rutgers.edu (AAAA) - Second Query (Packet 19)

Destination IP: `192.31.80.30` (same as Query 1) **Hexadecimal:** `c0 1f 50 1e`

Where found: Same glue record from root response for d.edu-servers.net

Query 3: whale.stanford.edu (AAAA) - Second Query (Packet 35)

Destination IP: `192.31.80.30` (same as Queries 1 & 2) **Hexadecimal:** `c0 1f 50 1e`

Where found: Same glue record from root response for d.edu-servers.net

Query 4: www.princeton.edu (A) - Second Query (Packet 51)

Destination IP: `192.31.80.30` (same as Queries 1, 2, & 3) **Hexadecimal:** `c0 1f 50 1e`

Where found: Same glue record from root response for d.edu-servers.net

---