Name : Ramzy Izza Wardhana
NIM : 21/472698/PA/20322
Class : IUP CS B

# Activity 5.3 – Computer System and Networking Lab

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

DNS Query Message:

| | | | | | |
|---|---|---|---|---|---|
| 62 8.473690 | 192.168.1.236 | 192.168.1.1 | DNS | 76 Standard query 0x0003 AAAA www.cs.umass.edu |
| 64 8.789411 | 192.168.1.1 | 192.168.1.236 | DNS | 76 Standard query response 0x0003 AAAA www.cs.uma |
| 107 11.668816 | 192.168.1.158 | 224.0.0.251 | IGMPv2 | 46 Membership Report group 224.0.0.251 |
| 1 0.000000 | 192.168.1.81 | 224.0.0.251 | MDNS | 632 Standard query 0x0000 PTR lb._dns-sd._udp.loca |

```
> Frame 62: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{3F648750-3E67-4449-8F22-9B7E
> Ethernet II, Src: IntelCor_17:c8:c5 (8c:c6:81:17:c8:c5), Dst: Routerbo_2a:0f:23 (08:55:31:2a:0f:23)
> Internet Protocol Version 4, Src: 192.168.1.236, Dst: 192.168.1.1
v User Datagram Protocol, Src Port: 63719, Dst Port: 53
    Source Port: 63719
    Destination Port: 53
    Length: 42
```

DNS Response Message:

| | | | | | |
|---|---|---|---|---|---|
| 62 8.473690 | 192.168.1.236 | 192.168.1.1 | DNS | 76 Standard query 0x0003 AAAA www.cs.umass.edu |
| 64 8.789411 | 192.168.1.1 | 192.168.1.236 | DNS | 76 Standard query response 0x0003 AAAA www.cs.umass.edu |
| 107 11.668816 | 192.168.1.158 | 224.0.0.251 | IGMPv2 | 46 Membership Report group 224.0.0.251 |
| 1 0.000000 | 192.168.1.81 | 224.0.0.251 | MDNS | 632 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" ques |

```
> Frame 64: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{3F648750-3E67-4449-8F22-9B7E3921CDE5}, i
> Ethernet II, Src: Routerbo_2a:0f:23 (08:55:31:2a:0f:23), Dst: IntelCor_17:c8:c5 (8c:c6:81:17:c8:c5)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.236
v User Datagram Protocol, Src Port: 53, Dst Port: 63719
    Source Port: 53
    Destination Port: 63719
    Length: 42
```

*Answer:*

Destination Port: 53 [DNS Query Message] | Source Port : 53 [DNS Response Message]

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

| | | | | | |
|---|---|---|---|---|---|
| 59 8.460789 | 192.168.1.1 | 192.168.1.236 | DNS | 84 Standard query response 0x0001 No such name |
| 60 8.463188 | 192.168.1.236 | 192.168.1.1 | DNS | 76 Standard query 0x0002 A www.cs.umass.edu |

```
C:\Users\themi>nslookup
Default Server:  UnKnown
Address:  192.168.1.1
```

*Answer:*

The DNS query message was sent to 192.168.1.1 which is the IP address of my default local DNS proven by doing nslookup on CMD.

13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

```
v Queries                                      v Domain Name System (query)
    v www.cs.umass.edu: type A, class IN           Transaction ID: 0x0002
        Name: www.cs.umass.edu                   > Flags: 0x0100 Standard query
        [Name Length: 16]                          Questions: 1
        [Label Count: 4]                           Answer RRs: 0
        Type: A (Host Address) (1)                 Authority RRs: 0
        Class: IN (0x0001)                         Additional RRs: 0
    [Response In: 61]                            v Queries
```

*Answer:* Type: A (Host Address) (1) | Answers: 0 (no answer)

14. Examine the DNS response message to the query message. How many "questions" does this DNS response message contain? How many "answers"?

```
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
```

*Answer:* Question: 1 and Answer:1

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

```
618 25.362419      192.168.1.1        192 168 1 236      DNS      84 Standard query response 0x0001 No su
619 25.366962      192.168.1.236      192.168.1.1        DNS      69 Standard query 0x0002 NS umass.edu
620 25.375178      192.168.1.1        192.168.1.236      DNS      165 Standard query response 0x0002 NS um
```

```
C:\Users\themi>nslookup -type=NS umass.edu
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
umass.edu       nameserver = ns1.umass.edu
umass.edu       nameserver = ns2.umass.edu
umass.edu       nameserver = ns3.umass.edu

umass.edu       nameserver = ns2.umass.edu
umass.edu       nameserver = ns3.umass.edu
umass.edu       nameserver = ns1.umass.edu
```

*Answer:* The DNS Query message was sent to 192.168.1.1 which is my IP address of default local DNS server.

16. Examine the DNS query message. How many questions does the query have? Does the query message contain any "answers"?

```
∨ Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

*Answer :* The DNS query message has 1 question and 0 answer.

17. Examine the DNS response message. How many answers does the response have? What information is contained in the answers? How many additional resource records are returned? What additional information is included in these additional resource records?

*Answer:*

It got 3 Answers from the response message

```
    UDP payload (123 bytes)
∨ Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 3
    Additional RRs: 0
```

Content of each answer are given below:

Additional Resources: 0

```
    Class: IN (0x0001)
∨ Answers
  ∨ umass.edu: type NS, class IN, ns ns1.umass.edu
      Name: umass.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 3582 (59 minutes, 42 seconds)
      Data length: 6
      Name Server: ns1.umass.edu
  ∨ umass.edu: type NS, class IN, ns ns2.umass.edu
      Name: umass.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 3582 (59 minutes, 42 seconds)
      Data length: 6
      Name Server: ns2.umass.edu
  ∨ umass.edu: type NS, class IN, ns ns3.umass.edu
      Name: umass.edu
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 3582 (59 minutes, 42 seconds)
      Data length: 6
      Name Server: ns3.umass.edu
```

```
    UDP payload (123 bytes)
∨ Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query respo
    Questions: 1
    Answer RRs: 3
    Authority RRs: 3
    Additional RRs: 0
  ∨ Queries
```