Eli KatzF25 ECE 333

[Ekatz9@uic.edu](mailto:Ekatz9@uic.edu)Computer Connection Networks 1

653212753Professor Dr. Loay Abusalah

**Lab 05**

**UDP**

**Executing nslookup** [**www.nyu.edu**](http://www.nyu.edu) **results in figure 1 below**

|  |
| --- |
| **Microsoft Windows [Version 10.0.26100.6584]**  **(c) Microsoft Corporation. All rights reserved.**  **C:\Users\elikw>nslookup www.nyu.edu**  **Server: uic-dns3.uic.edu**  **Address: 128.248.171.50**  **Aliases: 50.171.248.128.in-addr.arpa**  **Non-authoritative answer:**  **Name: d1q5ku5vnwkd2k.cloudfront.net**  **Addresses: 2600:9000:233d:4000:1:f7e2:cb00:93a1**  **2600:9000:233d:3600:1:f7e2:cb00:93a1**  **2600:9000:233d:d400:1:f7e2:cb00:93a1**  **2600:9000:233d:d000:1:f7e2:cb00:93a1**  **2600:9000:233d:2600:1:f7e2:cb00:93a1**  **2600:9000:233d:a600:1:f7e2:cb00:93a1**  **2600:9000:233d:9000:1:f7e2:cb00:93a1**  **2600:9000:233d:dc00:1:f7e2:cb00:93a1**  **108.159.227.127**  **108.159.227.93**  **108.159.227.17**  **108.159.227.49**  **Aliases: www.nyu.edu** |

**While nslookup is executed wireshark captures figure 2 below**

|  |
| --- |
| **634 33.164844 10.13.211.202 142.250.191.106 UDP 71 64132 → 443 Len=29**  **635 33.169197 142.250.191.106 10.13.211.202 UDP 67 443 → 64132 Len=25**  **638 36.099123 10.13.211.202 128.248.171.50 DNS 87 Standard query 0x0001 PTR 50.171.248.128.in-addr.arpa**  **639 36.124383 128.248.171.50 10.13.211.202 DNS 164 Standard query response 0x0001 PTR 50.171.248.128.in-addr.arpa CNAME 50.48-29.171.248.128.in-addr.arpa PTR uic-dns3.uic.edu**  **640 36.130005 10.13.211.202 128.248.171.50 DNS 95 Standard query 0x0002 A www.nyu.edu.client.wireless.uic.edu**  **641 36.193496 128.248.171.50 10.13.211.202 DNS 178 Standard query response 0x0002 No such name A www.nyu.edu.client.wireless.uic.edu SOA uic-dns1.uic.edu**  **642 36.194336 10.13.211.202 128.248.171.50 DNS 95 Standard query 0x0003 AAAA www.nyu.edu.client.wireless.uic.edu**  **643 36.260791 128.248.171.50 10.13.211.202 DNS 178 Standard query response 0x0003 No such name AAAA www.nyu.edu.client.wireless.uic.edu SOA uic-dns1.uic.edu**  **644 36.261922 10.13.211.202 128.248.171.50 DNS 88 Standard query 0x0004 A www.nyu.edu.wireless.uic.edu**  **645 36.428934 128.248.171.50 10.13.211.202 DNS 157 Standard query response 0x0004 No such name A www.nyu.edu.wireless.uic.edu SOA uic-dns1.uic.edu**  **646 36.429851 10.13.211.202 128.248.171.50 DNS 88 Standard query 0x0005 AAAA www.nyu.edu.wireless.uic.edu**  **647 36.637596 128.248.171.50 10.13.211.202 DNS 157 Standard query response 0x0005 No such name AAAA www.nyu.edu.wireless.uic.edu SOA uic-dns1.uic.edu**  **648 36.638221 10.13.211.202 128.248.171.50 DNS 79 Standard query 0x0006 A www.nyu.edu.uic.edu**  **649 36.656623 128.248.171.50 10.13.211.202 DNS 139 Standard query response 0x0006 No such name A www.nyu.edu.uic.edu SOA uic-dns1.uic.edu**  **650 36.657264 10.13.211.202 128.248.171.50 DNS 79 Standard query 0x0007 AAAA www.nyu.edu.uic.edu**  **651 36.664835 128.248.171.50 10.13.211.202 DNS 139 Standard query response 0x0007 No such name AAAA www.nyu.edu.uic.edu SOA uic-dns1.uic.edu**  **652 36.665823 10.13.211.202 128.248.171.50 DNS 71 Standard query 0x0008 A www.nyu.edu**  **653 36.753316 128.248.171.50 10.13.211.202 DNS 178 Standard query response 0x0008 A www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net A 108.159.227.127 A 108.159.227.93 A 108.159.227.17 A 108.159.227.49**  **654 36.763270 10.13.211.202 128.248.171.50 DNS 71 Standard query 0x0009 AAAA www.nyu.edu**  **655 36.790911 128.248.171.50 10.13.211.202 DNS 338 Standard query response 0x0009 AAAA www.nyu.edu CNAME d1q5ku5vnwkd2k.cloudfront.net AAAA 2600:9000:233d:4000:1:f7e2:cb00:93a1 AAAA 2600:9000:233d:3600:1:f7e2:cb00:93a1 AAAA 2600:9000:233d:d400:1:f7e2:cb00:93a1 AAAA 2600:9000:233d:d000:1:f7e2:cb00:93a1 AAAA 2600:9000:233d:2600:1:f7e2:cb00:93a1 AAAA 2600:9000:233d:a600:1:f7e2:cb00:93a1 AAAA 2600:9000:233d:9000:1:f7e2:cb00:93a1 AAAA 2600:9000:233d:dc00:1:f7e2:cb00:93a1**  **656 39.667105 142.250.191.106 10.13.211.202 UDP 120 443 → 64132 Len=78**  **657 39.671937 10.13.211.202 142.250.191.106 UDP 75 64132 → 443 Len=33**  **658 39.878036 10.13.211.202 142.250.191.106 UDP 71 64132 → 443 Len=29** |

1. **Select the first UDP segment in your trace. What is the packet number of this segment in the trace file?**

The first UDP Segment (frame 638) is shown:

|  |
| --- |
| **Frame 638: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF\_{5355D3DE-8C6A-4534-9378-0167D2AF8433}, id 0**  **Ethernet II, Src: Intel\_89:73:3a (84:5c:f3:89:73:3a), Dst: PaloAltoNetw\_ed:80:15 (b4:0c:25:ed:80:15)**  **Internet Protocol Version 4, Src: 10.13.211.202, Dst: 128.248.171.50**  **User Datagram Protocol, Src Port: 51101, Dst Port: 53**  Source Port: 51101  Destination Port: 53  Length: 53  Checksum: 0x0a49 [unverified]  [Checksum Status: Unverified]  [Stream index: 9]  [Stream Packet Number: 1]  [Timestamps]  UDP payload (45 bytes)  **Domain Name System (query)**  Transaction ID: 0x0001  Flags: 0x0100 Standard query  Questions: 1  Answer RRs: 0  Authority RRs: 0  Additional RRs: 0  Queries  **[Response In: 639]** |

The Packet is Number 1 in the stream

**What type of application-layer payload or protocol message is being carried in this UDP segment?**

The Payload of this UDP Segment is DNS Protocol, Query Message

**Look at the details of this packet in Wireshark. How many fields there are in the UDP header?**

**(You shouldn’t look in the textbook! Answer these questions directly from what you observe in the packet trace.)**

There are 4 Fields in the UDP Header: Source Port, Destination Port, Length, & Checksum

**What are the names of these fields?**

Source Port, Destination Port, Length, & Checksum

1. **By consulting the displayed information in Wireshark’s packet content field for this packet (or by consulting the textbook), what is the length (in bytes) of each of the UDP header fields?**

By Observing the Raw Data of frame 638, we find the UDP header to be;

C7 9B 00 35 00 35 0A 49

32 bits, 8 for each header field or

8 bytes, 2 for each header field

1. **The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.**

The Length field represents the length of the UDP Segment in Bytes. Referring back to frame 638, where the length field is 53 and the raw Hex Data is:

b40c 25ed 8015 845c f389 733a 0800 4500

0049 9c83 0000 8011 0000 0a0d d3ca 80f8

ab32 c79d 0035 0035 0a49 0001 0100 0001

0000 0000 0000 0235 3003 3137 3103 3234

3803 3132 3807 696e 2d61 6464 7204 6172

7061 0000 0c00 01

or 54 hexadecimal values

1. **What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)**

The Length field is 8 bits such that the maximum segment length is . This includes the 8-byte header; therefore the maximum payload is 248 bytes.

1. **What is the largest possible source port number? (Hint: see the hint in 4.)**

The Source Port field is 8 bits; therefore, the largest possible source port number is 256

1. **What is the protocol number for UDP? Give your answer in decimal notation. To answer this question, you’ll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).**

Referring again to frame 638, the associated IP Datagram is shown as

|  |
| --- |
| **Internet Protocol Version 4, Src: 10.13.211.202, Dst: 128.248.171.50**  0100 .... = Version: 4  .... 0101 = Header Length: 20 bytes (5)  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  Total Length: 73  Identification: 0x9c83 (40067)  000. .... = Flags: 0x0  ...0 0000 0000 0000 = Fragment Offset: 0  Time to Live: 128  Protocol: UDP (17)  Header Checksum: 0x0000 [validation disabled]  [Header checksum status: Unverified]  Source Address: 10.13.211.202  Destination Address: 128.248.171.50  [Stream index: 11] |

UDP is provided as protocol 17.

1. **Examine the pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). What is the packet number of the first of these two UDP segments in the trace file?**

The Response for frame 638 is recorded in frame 639 as shown below

|  |
| --- |
| **Frame 639: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface \Device\NPF\_{5355D3DE-8C6A-4534-9378-0167D2AF8433}, id 0**  **Ethernet II, Src: PaloAltoNetw\_ed:80:15 (b4:0c:25:ed:80:15), Dst: Intel\_89:73:3a (84:5c:f3:89:73:3a)**  **Internet Protocol Version 4, Src: 128.248.171.50, Dst: 10.13.211.202**  **User Datagram Protocol, Src Port: 53, Dst Port: 51101**  Source Port: 53  Destination Port: 51101  Length: 130  Checksum: 0xd7ee [unverified]  [Checksum Status: Unverified]  [Stream index: 9]  [Stream Packet Number: 2]  [Timestamps]  UDP payload (122 bytes)  **Domain Name System (response)**  Transaction ID: 0x0001  Flags: 0x8580 Standard query response, No error  Questions: 1  Answer RRs: 2  Authority RRs: 0  Additional RRs: 0  Queries  50.171.248.128.in-addr.arpa: type PTR, class IN  Name: 50.171.248.128.in-addr.arpa  [Name Length: 27]  [Label Count: 6]  Type: PTR (12) (domain name PoinTeR)  Class: IN (0x0001)  Answers  [Request In: 638]  **[Time: 0.025260000 seconds]** |

**What is the value in the source port field in this UDP segment?**

Frame 638 Source Port: 51101

**What is the value in the destination port field in this UDP segment?**

Frame 638 Destination Port: 53

**What is the packet number of the second of these two UDP segments in the trace file?**

Frame 639 Stream Packet Number: 2

**What is the value in the source port field in this second UDP segment?**

Frame 639 Source Port: 53

**What is the value in the destination port field in this second UDP segment? Describe the relationship between the port numbers in the two packets.**

Frame 639 Destination Port: 51101

The Response Segment has the source and destination ports swapped relative to the Query Segment.