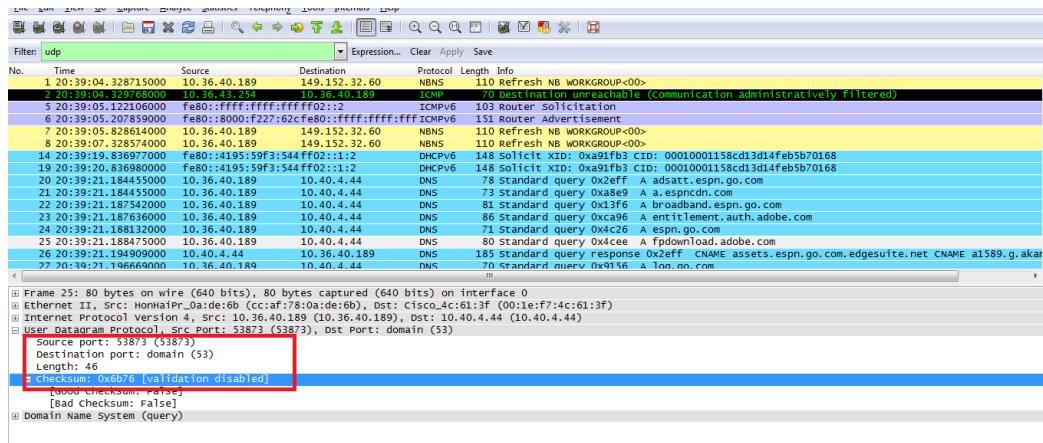




COMPUTER NETWORKS ASSIGNMENT 2

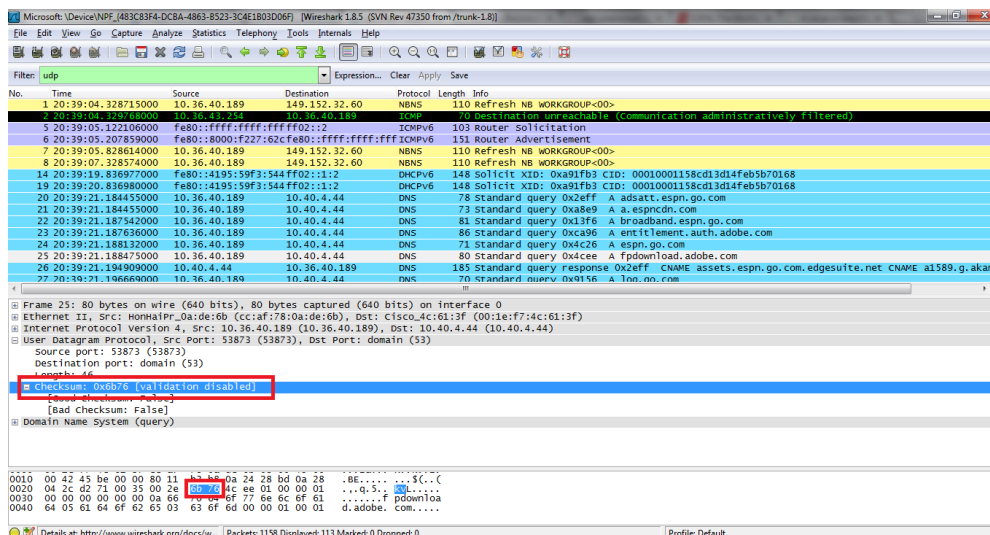
Made By:
Aniket Singh
2101091CS

1) 1. Select one UDP packet from your trace. From this packet, determine 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.) Name these fields.



The header only contains 4 fields: the source port, destination port, length, and checksum.

By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.



Each of the UDP header fields is 2 bytes long

3. 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 value in the length field, in the example below it is 46, is the sum of the 8 header bytes and the remaining data bytes encapsulated in the packet.

4. 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 maximum number of bytes that can be in the payload is 2^{16} - the bytes already being used by the header field (8). Therefore the maximum payload is $65535-8= 65527$ bytes.

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

The largest possible source port number is 2^{16} or 65535.

6. What is the protocol number for UDP? Give your answer in both hexadecimal and 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).

The protocol number for UDP is 17 in decimal notation which in hexadecimal notation is 0x11.

Microsoft [Device\NPF_{483C83F4-DCBA-4863-B523-3C4E1B03D06F}] [Wireshark 1.8.5 [SVN Rev 47350 from /trunk-1.8]]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: udp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
28	20:39:21.197103000	10.40.4.44	10.36.40.189	DNS	176	Standard query response 0xa8e9 CNAME a.espncdn.com.edgesuite.net CNAME a1589.g1.akamai.f
33	20:39:21.204122000	10.36.40.189	10.40.4.44	DNS	77	Standard query 0x5a82 A sp.auth.adobe.com
37	20:39:21.211336000	10.40.4.44	10.36.40.189	DNS	87	Standard query response 0x4c26 A 68.71.212.152
38	20:39:21.211519000	10.40.4.44	10.36.40.189	DNS	175	Standard query response 0xca96 CNAME vsan.scene7.com.edgekey.net CNAME e765.g.akamaiedge
39	20:39:21.213221000	10.36.40.189	10.40.4.44	DNS	78	Standard query 0xb942 A streak.espn.go.com
42	20:39:21.223466000	10.40.4.44	10.36.40.189	DNS	108	Standard query response 0x9156 CNAME log.wip.go.com A 68.71.220.175
61	20:39:21.251836000	10.40.4.44	10.36.40.189	DNS	94	Standard query response 0xb942 A 68.71.212.199
81	20:39:21.296311000	10.40.4.44	10.36.40.189	DNS	203	Standard query response 0x4cee CNAME fpdladobe.wip4.adobe.com CNAME fpdownload.adobe.com
82	20:39:21.296277000	10.40.4.44	10.36.40.189	DNS	202	Standard query response 0x13f6 A 68.71.216.192
83	20:39:21.296356000	10.40.4.44	10.36.40.189	DNS	345	Standard query response 0x5a82 CNAME sp.adobepass.com A 66.235.134.217
249	20:39:22.069132000	10.36.40.189	10.40.4.44	DNS	78	Standard query 0x6017 A ad.doubleclick.net
250	20:39:22.086987000	10.40.4.44	10.36.40.189	DNS	131	Standard query response 0x6017 CNAME dart.l.doubleclick.net A 173.194.43.59 A 173.194.4
405	20:39:22.605050000	10.36.40.189	10.40.4.44	DNS	84	Standard query 0x8c97 A espndeportes.espn.go.com
406	20:39:22.605523000	10.36.40.189	10.40.4.44	DNS	73	Standard query 0x551e A m.espn.go.com
407	20:39:22.606353000	10.36.40.189	10.40.4.44	DNS	72	Standard query 0x02a8 A espnshop.com
409	20:39:22.625006000	10.40.4.44	10.36.40.189	DNS	100	Standard query response 0x8c97 A 68.71.216.161

Fragment offset: 0
Time to live: 126
Protocol: UDP (17)
Header checksum: 0x8d8e [correct]
Source: 10.40.4.44 (10.40.4.44)
Destination: 10.36.40.189 (10.36.40.189)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol (53), Src Port: domain (53), Dst Port: 50037 (50037)
Source port: domain (53)
Destination port: 50037 (50037)
Length: 97
Checksum: 0xe75d [validation disabled]
Domain Name System (response)

0000 cc af 78 0a de 6b 00 1e f7 4c 61 3f 08 00 45 00 . . x . . k La ? . . E .
0010 00 75 2d b5 40 00 7e 11 8d 8e 0a 28 04 2c 0a 24 . u . @ (. . . \$
0020 28 bd 00 35 c3 75 00 61 e7 5d 60 17 81 80 00 01 (. 5 . u . a .)
0030 00 03 00 00 00 00 02 61 64 0b 64 6f 75 62 6c 65 a d . double
0040 63 6c 69 63 6b 03 6e 65 74 00 00 01 00 01 c0 0c click . ne t
0050 00 05 00 01 00 01 20 8c 00 00 04 61 72 74 01
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File: C:\Users\Max\AppData\Local\Temp\w... Packets: 1158 Displayed: 113 Marked: 0 Dropped: 0 Profile: Default

The relationship between port numbers is that the source port on the send message is the destination port of the receive message. The destination port for the send message is also the source port for the receive message.