# HACETTEPE UNIVERSITY DEPARTMENT OF COMPUTER ENGINEERING BBM 453 LAB EXPERIMENT



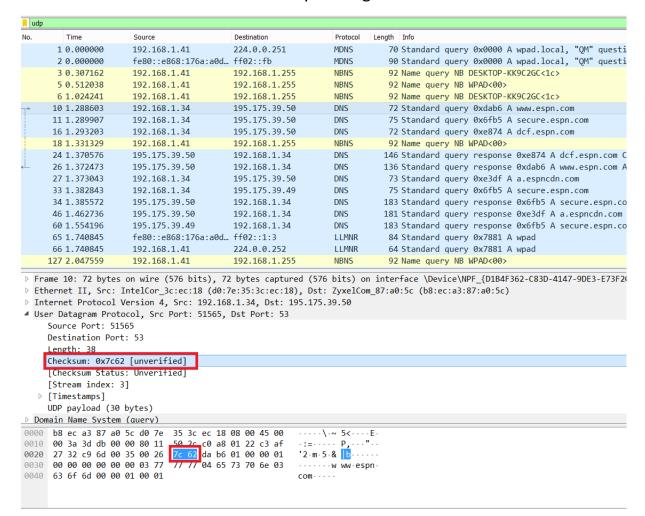
Mehmet Taha USTA – 21527472 Çağlar USLU – 21808388 1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

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

1									
	1 0.000000	192.168.1.41	224.0.0.251	MDNS	70 Standard query 0x0000 A wpad.local, "QM" question				
	2 0.000000	fe80::e868:176a:a0d	ff02::fb	MDNS	90 Standard query 0x0000 A wpad.local, "QM" question				
	3 0.307162	192.168.1.41	192.168.1.255	NBNS	92 Name query NB DESKTOP-KK9C2GC<1c>				
	5 0.512038	192.168.1.41	192.168.1.255	NBNS	92 Name query NB WPAD<00>				
	6 1.024241	192.168.1.41	192.168.1.255	NBNS	92 Name query NB DESKTOP-KK9C2GC<1c>				
	10 1.288603	192.168.1.34	195.175.39.50	DNS	72 Standard query 0xdab6 A www.espn.com				
	11 1.289907	192.168.1.34	195.175.39.50	DNS	75 Standard query 0x6fb5 A secure.espn.com				
	16 1.293203	192.168.1.34	195.175.39.50	DNS	72 Standard query 0xe874 A dcf.espn.com				
	18 1.331329	192.168.1.41	192.168.1.255	NBNS	92 Name query NB WPAD<00>				
	24 1.370576	195.175.39.50	192.168.1.34	DNS	146 Standard query response 0xe874 A dcf.espn.com CNAME				
4	26 1.372473	195.175.39.50	192.168.1.34	DNS	136 Standard query response 0xdab6 A www.espn.com A 54.1				
	27 1.373043	192.168.1.34	195.175.39.50	DNS	73 Standard query 0xe3df A a.espncdn.com				
	33 1.382843	192.168.1.34	195.175.39.49	DNS	75 Standard query 0x6fb5 A secure.espn.com				
	34 1.385572	195.175.39.50	192.168.1.34	DNS	183 Standard query response 0x6fb5 A secure.espn.com CNA				
	46 1.462736	195.175.39.50	192.168.1.34	DNS	181 Standard query response 0xe3df A a.espncdn.com CNAME				
	60 1.554196	195.175.39.49	192.168.1.34	DNS	183 Standard query response 0x6fb5 A secure.espn.com CNA				
	65 1.740845	fe80::e868:176a:a0d	ff02::1:3	LLMNR	84 Standard query 0x7881 A wpad				
	66 1.740845	192.168.1.41	224.0.0.252	LLMNR	64 Standard query 0x7881 A wpad				
	127 2.047559	192.168.1.41	192.168.1.255	NBNS	92 Name query NB WPAD<00>				
<pre></pre>									
⊿	✓ User Datagram Protocol, Src Port: 51565, Dst Port: 53 Source Port: 51565								
П									
	Destination Port:	53							
	Length: 38								
L	Checksum: 0x7c62								
	[Checksum Status:	-							
	[Stream index: 3]								
	▷ [Timestamps]								
	UDP payload (30 bytes)								
$\triangleright$	Domain Name System (query)								

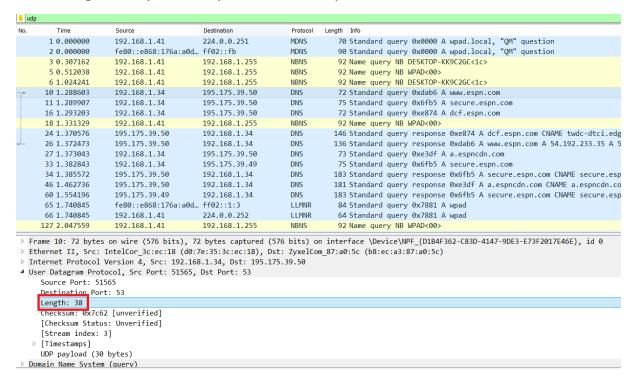
#### 2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

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 is 38, 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.

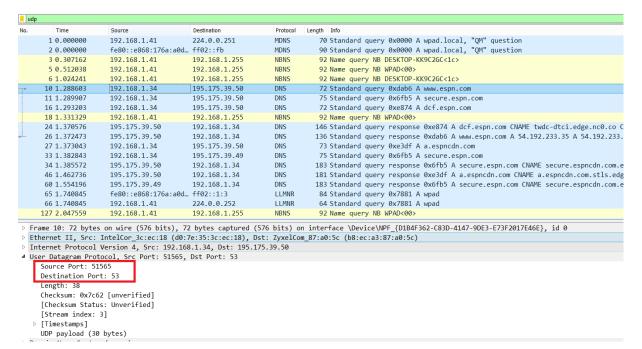
6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

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

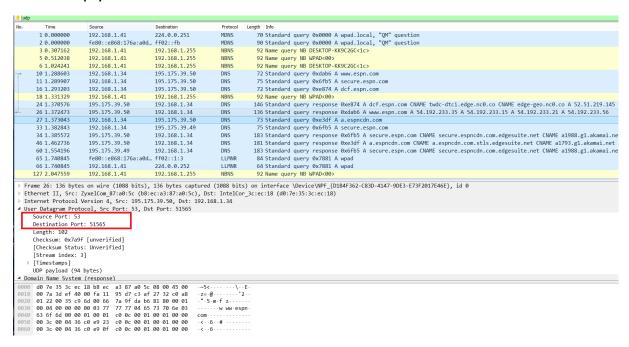
, ud	р									
No.	Time	Source	Destination		Protocol	Length Info				
	1 0.000000	192.168.1.41	224.0.0.251		MDNS	70 Standard query 0x0000 A wpad.local, "QM" ques				
	2 0.000000	fe80::e868:176a:a0d	ff02::fb		MDNS	90 Standard query 0x0000 A wpad.local, "QM" ques				
	3 0.307162	192.168.1.41	192.168.1.255	;	NBNS	92 Name query NB DESKTOP-KK9C2GC<1c>				
	5 0.512038	192.168.1.41	192.168.1.255	5	NBNS	92 Name query NB WPAD<00>				
	6 1.024241	192.168.1.41	192.168.1.255	5	NBNS	92 Name query NB DESKTOP-KK9C2GC<1c>				
	10 1.288603	192.168.1.34	195.175.39.50	)	DNS	72 Standard query 0xdab6 A www.espn.com				
	11 1.289907	192.168.1.34	195.175.39.50	)	DNS	75 Standard query 0x6fb5 A secure.espn.com				
	16 1.293203	192.168.1.34	195.175.39.50	)	DNS	72 Standard query 0xe874 A dcf.espn.com				
	18 1.331329	192.168.1.41	192.168.1.255	j	NBNS	92 Name query NB WPAD<00>				
	24 1.370576	195.175.39.50	192.168.1.34		DNS	146 Standard query response 0xe874 A dcf.espn.com				
4	26 1.372473	195.175.39.50	192.168.1.34		DNS	136 Standard query response Oxdab6 A www.espn.com				
	27 1.373043	192.168.1.34	195.175.39.50	)	DNS	73 Standard query 0xe3df A a.espncdn.com				
	33 1.382843	192.168.1.34	195.175.39.49	)	DNS	75 Standard query 0x6fb5 A secure.espn.com				
	34 1.385572	195.175.39.50	192.168.1.34		DNS	183 Standard query response 0x6fb5 A secure.espn.				
	46 1.462736	195.175.39.50	192.168.1.34		DNS	181 Standard query response 0xe3df A a.espncdn.co				
	60 1.554196	195.175.39.49	192.168.1.34		DNS	183 Standard query response 0x6fb5 A secure.espn.				
	65 1.740845	fe80::e868:176a:a0d	ff02::1:3		LLMNR	84 Standard query 0x7881 A wpad				
	66 1.740845	192.168.1.41	224.0.0.252		LLMNR	64 Standard query 0x7881 A wpad				
	127 2.047559	192.168.1.41	192.168.1.255	j	NBNS	92 Name query NB WPAD<00>				
Total Length: 58 Identification: 0x3ddb (15835)  Flags: 0x00  0 = Reserved bit: Not set  .0 = Don't fragment: Not set  .0 = More fragments: Not set  Fragment Offset: 0  Time to Live: 128  Protocol: UDP (17)  Header Checksum: 0x502c [validation disabled]  [Header checksum status: Unverified]  Source Address: 192.168.1.34  Destination Address: 195.175.39.50										
000	0 b8 ec a3 87 a0	5c d0 7e 35 3c ec 18	08 00 45 00	\	5<	E.				
001		00 80 11 50 2c c0 a8		-:=						
002		35 00 26 7c 62 da b6			k  b					
003		00 03 77 77 77 04 65	73 70 6e 03		ww-espi	n·				
004	0 63 6f 6d 00 00	01 00 01		com						

7. Examine a 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). Describe the relationship between the port numbers in the two packets.

UDP Sent by my host



#### **UDP** Reply to Host



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.