

# Wireshark Lab: UDP

## Questions:

1. There are four fields in the UDP header:

Source Port

Destination Port

Length

Checksum

The image shows a Wireshark capture of a UDP packet. The packet list at the top shows a DNS query from 192.168.1.101 to 68.87.71.226. The packet details pane shows the UDP header fields: Source Port: 4372, Destination Port: 53, Length: 51, and Checksum: 0x77d4. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
2	0.012481	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston.comcast.net
3	0.014232	192.168.1.101	68.87.71.226	DNS	91	Standard query 0x0002 A www.mit.edu.hsd1.ma.comcast.net
4	0.042641	68.87.71.226	192.168.1.101	DNS	171	Standard query response 0x0002 No such name A www.mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
5	0.044178	192.168.1.101	68.87.71.226	DNS	86	Standard query 0x0003 A www.mit.edu.ma.comcast.net
6	0.058934	68.87.71.226	192.168.1.101	DNS	86	Standard query response 0x0003 Server failure A www.mit.edu.ma.comcast.net
7	0.060268	192.168.1.101	68.87.71.226	DNS	71	Standard query 0x0004 A www.mit.edu
8	0.074984	68.87.71.226	192.168.1.101	DNS	87	Standard query response 0x0004 A www.mit.edu A 18.7.22.83
28	39.781959	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
29	39.794838	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston.comcast.net
30	39.796777	192.168.1.101	68.87.71.226	DNS	87	Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
31	39.823784	68.87.71.226	192.168.1.101	DNS	167	Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
32	39.825175	192.168.1.101	68.87.71.226	DNS	82	Standard query 0x0003 NS mit.edu.ma.comcast.net
33	39.838373	68.87.71.226	192.168.1.101	DNS	82	Standard query response 0x0003 Server failure NS mit.edu.ma.comcast.net
34	39.839799	192.168.1.101	68.87.71.226	DNS	67	Standard query 0x0004 NS mit.edu

Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0  
 Ethernet II, Src: Dell (08:00:07:4f:36:23), Dst: Cisco-L1 (00:16:b6:f4:eb:a8)  
 Internet Protocol Version 4, Src: 192.168.1.101, Dst: 68.87.71.226  
 User Datagram Protocol, Src Port: 4372, Dst Port: 53  
 Source Port: 4372  
 Destination Port: 53  
 Length: 51  
 Checksum: 0x77d4 [unverified]  
 [Checksum Status: Unverified]  
 [Stream index: 0]  
 Domain Name System (query)

0000 00 16 b6 f4 eb a8 00 08 74 4f 36 23 08 00 45 00 ..... t06#..E.  
 0010 00 47 3c f9 00 00 11 af 66 c0 a8 01 65 44 57 .G.....f..eDW  
 0020 47 e2 11 14 00 35 00 33 77 d4 00 01 01 00 00 01 G...S.3w.....  
 0030 00 00 00 00 00 00 03 32 32 36 02 37 31 02 38 37 .....2 26.71.87  
 0040 02 36 38 07 69 6e 2d 61 64 64 72 04 61 72 70 61 .68.in-a ddr arpa  
 0050 00 00 0c 00 01 .....  
 Destination Port (udp.dstport), 2 bytes

Packets: 37 · Displayed: 16 (43.2%) Profile: Default

2. Each of these fields are 2 bytes long, for a total udp header length of 8 bytes

Applications [Mozilla Firefox] 404 Not Found - Mozilla ... udp-wireshark-trace.pcap [Pictures - File Manager] Downloads - File Manager 23:23 root

udp-wireshark-trace.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
2	0.012481	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston.comcast.net
3	0.014232	192.168.1.101	68.87.71.226	DNS	91	Standard query 0x0002 A www.mit.edu.hsd1.ma.comcast.net
4	0.042641	68.87.71.226	192.168.1.101	DNS	171	Standard query response 0x0002 No such name A www.mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
5	0.044178	192.168.1.101	68.87.71.226	DNS	86	Standard query 0x0003 A www.mit.edu.ma.comcast.net
6	0.058934	68.87.71.226	192.168.1.101	DNS	86	Standard query response 0x0003 Server failure A www.mit.edu.ma.comcast.net
7	0.060268	192.168.1.101	68.87.71.226	DNS	71	Standard query 0x0004 A www.mit.edu
8	0.074984	68.87.71.226	192.168.1.101	DNS	87	Standard query response 0x0004 A www.mit.edu A 18.7.22.83
28	39.781959	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
29	39.794838	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston.comcast.net
30	39.796777	192.168.1.101	68.87.71.226	DNS	87	Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
31	39.823784	68.87.71.226	192.168.1.101	DNS	167	Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
32	39.825175	192.168.1.101	68.87.71.226	DNS	82	Standard query 0x0003 NS mit.edu.ma.comcast.net
33	39.838373	68.87.71.226	192.168.1.101	DNS	82	Standard query response 0x0003 Server failure NS mit.edu.ma.comcast.net
34	39.839799	192.168.1.101	68.87.71.226	DNS	67	Standard query 0x0004 NS mit.edu

Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits)  
Ethernet II, Src: Dell\_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco-Li\_f4:eb:a8 (00:16:b6:f4:eb:a8)  
Internet Protocol Version 4, Src: 192.168.1.101, Dst: 68.87.71.226  
User Datagram Protocol, Src Port: 4372, Dst Port: 53  
Source Port: 4372  
Destination Port: 53  
Length: 51  
Checksum: 0x77d4 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 0]  
Domain Name System (query)

0000 00 16 b6 f4 eb a8 00 00 74 4f 36 23 08 00 45 00 ... 06#.: E  
0010 00 47 3c f9 00 00 00 11 af 60 00 a8 01 65 44 57 ... G<...f...OW  
0020 47 3c f9 00 00 00 11 af 60 00 a8 01 65 44 57 ... G<...f...OW  
0030 00 00 00 00 00 00 03 32 32 36 32 37 31 02 38 37 ... ..2 26 74 87  
0040 02 36 36 37 69 6e 2d 61 64 64 72 04 61 72 70 61 ... 68 in-a ddr arpa  
0050 00 00 0c 00 01 .....

User Datagram Protocol (udp), 8 bytes

Packets: 37 · Displayed: 16 (43.2%) Profile: Default

3. The length field is the number of header bytes, 8, plus the number of udp data bytes, in this case, 42.

4.  $2^{16} - 1 = 65535$  bytes possible minus the header = 65527 bytes

5. Largest source port number would be 65535

6. The UDP protocol number is 17 or 0x11 in hex.

The image shows a Wireshark packet capture of a DNS query and response. The packet list shows a query from 192.168.1.101 to 68.87.71.226. The packet details show the query structure with fields like Version, Header Length, Total Length, Identification, Flags, Time to Live, Protocol (UDP 17), Header checksum, Source, Destination, and User Datagram Protocol. The packet bytes show the raw data in hexadecimal and ASCII.

Applications [Mozilla Firefox] 404 Not Found - Mozilla ... udp-wireshark-trace.pcap [Pictures - File Manager] Downloads - File Manager 23:31 root

udp-wireshark-trace.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
2	0.012481	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston.comcast.net
3	0.014232	192.168.1.101	68.87.71.226	DNS	91	Standard query 0x0002 A www.mit.edu.hsd1.ma.comcast.net
4	0.042641	68.87.71.226	192.168.1.101	DNS	171	Standard query response 0x0002 No such name A www.mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
5	0.044178	192.168.1.101	68.87.71.226	DNS	86	Standard query 0x0003 A www.mit.edu.ma.comcast.net
6	0.058934	68.87.71.226	192.168.1.101	DNS	86	Standard query response 0x0003 Server failure A www.mit.edu.ma.comcast.net
7	0.060268	192.168.1.101	68.87.71.226	DNS	71	Standard query 0x0004 A www.mit.edu
8	0.074984	68.87.71.226	192.168.1.101	DNS	87	Standard query response 0x0004 A www.mit.edu A 18.7.22.83
28	39.781959	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
29	39.794838	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston.comcast.net
30	39.796777	192.168.1.101	68.87.71.226	DNS	87	Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
31	39.823784	68.87.71.226	192.168.1.101	DNS	167	Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
32	39.825175	192.168.1.101	68.87.71.226	DNS	82	Standard query 0x0003 NS mit.edu.ma.comcast.net
33	39.838373	68.87.71.226	192.168.1.101	DNS	82	Standard query response 0x0003 Server failure NS mit.edu.ma.comcast.net
34	39.839799	192.168.1.101	68.87.71.226	DNS	67	Standard query 0x0004 NS mit.edu

Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on Ethernet II, Src: Dell 4f:36:23 (00:08:74:4f:36:23), Dst: Cisco-Li f4:eb:a8 (00:16:b6:f4:eb:a8)

Internet Protocol Version 4, Src: 192.168.1.101, Dst: 68.87.71.226

0100 .... = Version: 4  
... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 71  
Identification: 0x3cf9 (15609)  
Flags: 0x0000  
Time to live: 128  
Protocol: UDP (17)  
Header checksum: 0xaf66 [validation disabled]  
[Header checksum status: Unverified]  
Source: 192.168.1.101  
Destination: 68.87.71.226

User Datagram Protocol, Src Port: 4372, Dst Port: 53

Source Port: 4372  
Destination Port: 53  
Length: 51  
Checksum: 0x77d4 [unverified]

0000 00 16 b6 f4 eb a8 00 08 74 4f 36 23 08 00 45 00 ..... t06#..E  
0010 00 47 3c f9 00 00 00 11 af 66 c9 a8 01 65 44 57 .G<.....f...eDw  
0020 47 e2 11 14 00 35 00 33 77 d4 00 01 01 00 00 01 G...5.3 w.....  
0030 00 00 00 00 00 00 03 32 32 36 02 37 31 02 38 37 .....2 26 71 87  
0040 02 36 38 07 09 6e 2d 61 64 64 72 04 61 72 70 61 -68-in-a ddr.arpa  
0050 00 00 0c 00 01 .....

Internet Protocol Version 4 (ip), 20 bytes

Packets: 37 · Displayed: 16 (43.2%)

Profile: Default

7. UDP sent by the host has source port as 4732 and destination as 53. UDP reply to the host has these values reversed, showing that the same ports are being used.

The screenshot shows a Wireshark packet capture of a DNS query and response. The packet list shows a query from 192.168.1.101 to 68.87.71.226 on port 4732 to port 53. The response is from 68.87.71.226 to 192.168.1.101 on port 53 to port 4732. The response contains a PTR record for 226.71.87.68.in-addr.arpa.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
2	0.012481	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfordc2.ma.boston.comcast.net
3	0.014232	192.168.1.101	68.87.71.226	DNS	91	Standard query 0x0002 A www.mit.edu.hsd1.ma.comcast.net
4	0.042641	68.87.71.226	192.168.1.101	DNS	171	Standard query response 0x0002 No such name A www.mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
5	0.044178	192.168.1.101	68.87.71.226	DNS	86	Standard query 0x0003 A www.mit.edu.ma.comcast.net
6	0.058934	68.87.71.226	192.168.1.101	DNS	86	Standard query response 0x0003 Server failure A www.mit.edu.ma.comcast.net
7	0.060268	192.168.1.101	68.87.71.226	DNS	71	Standard query 0x0004 A www.mit.edu
8	0.074984	68.87.71.226	192.168.1.101	DNS	87	Standard query response 0x0004 A www.mit.edu A 18.7.22.83
28	39.781959	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
29	39.794838	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfordc2.ma.boston.comcast.net
30	39.796777	192.168.1.101	68.87.71.226	DNS	87	Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
31	39.823784	68.87.71.226	192.168.1.101	DNS	167	Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
32	39.825175	192.168.1.101	68.87.71.226	DNS	82	Standard query 0x0003 NS mit.edu.ma.comcast.net
33	39.838373	68.87.71.226	192.168.1.101	DNS	82	Standard query response 0x0003 Server failure NS mit.edu.ma.comcast.net
34	39.839799	192.168.1.101	68.87.71.226	DNS	67	Standard query 0x0004 NS mit.edu

Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on Ethernet II, Src: Dell 4f:36:23 (00:08:74:4f:36:23), Dst: Cisco-Li f4:eb:a8 (00:16:b6:f4:eb:a8)

Internet Protocol Version 4, Src: 192.168.1.101, Dst: 68.87.71.226

User Datagram Protocol, Src Port: 4372, Dst Port: 53

Source Port: 4372  
Destination Port: 53  
Length: 51  
Checksum: 0x704 [Unverified]  
[Checksum Status: Unverified]  
[Stream index: 0]

Domain Name System (query)

0000 00 16 b6 f4 eb a8 00 08 74 4f 36 23 08 00 45 00 .....t06#-E  
0010 00 47 3c f9 00 00 00 11 af 66 c0 a8 01 65 44 57 .G<.....f...eDw  
0020 47 e2 11 14 00 35 00 33 77 d4 00 01 01 00 00 01 G...5.3 w.....  
0030 00 00 00 00 00 00 03 32 32 36 02 37 31 02 38 37 .....2 26 71 87  
0040 02 36 38 07 69 6e 2d 61 64 64 72 04 61 72 70 61 -68-in-a ddr arpa  
0050 00 00 0c 00 01 .....

Internet Protocol Version 4 (ip), 20 bytes

Packets: 37 · Displayed: 16 (43.2%)

Profile: Default

## And the response:

The image shows a Wireshark packet capture of a DNS response. The top pane displays a list of 34 packets, all of which are DNS messages. The selected packet (No. 34) is a Standard query response from 192.168.1.101 to 68.87.71.226. The middle pane shows the details of this packet, including the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header. The destination port 4372 is circled in red. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Applications [Mozilla Firefox] 404 Not Found - Mozilla ... udp-wireshark-trace.pcap [Pictures - File Manager] Downloads - File Manager 23:35 root

udp-wireshark-trace.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
2	0.012481	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston.comcast.net
3	0.014232	192.168.1.101	68.87.71.226	DNS	91	Standard query 0x0002 A www.mit.edu.hsd1.ma.comcast.net
4	0.042641	68.87.71.226	192.168.1.101	DNS	171	Standard query response 0x0002 No such name A www.mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
5	0.044178	192.168.1.101	68.87.71.226	DNS	86	Standard query 0x0003 A www.mit.edu.ma.comcast.net
6	0.058934	68.87.71.226	192.168.1.101	DNS	86	Standard query response 0x0003 Server failure A www.mit.edu.ma.comcast.net
7	0.060268	192.168.1.101	68.87.71.226	DNS	71	Standard query 0x0004 A www.mit.edu
8	0.074984	68.87.71.226	192.168.1.101	DNS	87	Standard query response 0x0004 A www.mit.edu A 18.7.22.83
28	39.781959	192.168.1.101	68.87.71.226	DNS	85	Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
29	39.794838	68.87.71.226	192.168.1.101	DNS	137	Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston.comcast.net
30	39.796777	192.168.1.101	68.87.71.226	DNS	87	Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
31	39.823784	68.87.71.226	192.168.1.101	DNS	167	Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
32	39.825175	192.168.1.101	68.87.71.226	DNS	82	Standard query 0x0003 NS mit.edu.ma.comcast.net
33	39.838373	68.87.71.226	192.168.1.101	DNS	82	Standard query response 0x0003 Server failure NS mit.edu.ma.comcast.net
34	39.839799	192.168.1.101	68.87.71.226	DNS	67	Standard query 0x0004 NS mit.edu

Frame 2: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0  
Ethernet II, Src: Cisco-Li\_f4:eb:a8 (00:16:b6:f4:eb:a8), Dst: Dell\_4f:36:23 (00:08:74:4f:36:23)  
Internet Protocol Version 4, Src: 68.87.71.226, Dst: 192.168.1.101  
User Datagram Protocol, Src Port: 53, Dst Port: 4372  
Source Port: 53  
Destination Port: 4372  
Length: 103  
Checksum: 0x13c [unverified]  
[Checksum Status: Unverified]  
[Stream index: 0]  
Domain Name System (response)

0000 00 08 74 4f 36 23 00 16 b6 f4 eb a8 08 00 45 00 ..t06#.....E.  
0010 00 7b 01 cd 40 00 32 11 f8 5e 44 57 47 e2 c0 a8 .{. @.2. ^DWG..  
0020 01 65 00 35 11 14 00 67 c7 3c 00 01 81 80 00 01 .e 5...g <.....  
0030 00 01 00 00 00 00 03 32 32 36 02 37 31 02 38 37 .....2 26 71 87  
0040 02 36 38 07 69 6e 2d 61 64 64 72 04 61 72 70 61 -68 in-a ddr.arpa  
0050 00 00 0c 00 01 c0 0c 00 0c 00 01 00 00 de 45 00 .....E..  
0060 28 03 63 6e 73 0c 63 68 65 6c 6d 73 66 64 72 64 (. cns ch elmsfdrd  
0070 63 32 02 6d 61 06 62 6f 73 74 6f 6e 07 63 6f 6d c2-ma bo ston-com

Internet Protocol Version 4 (ip), 20 bytes

Packets: 37 · Displayed: 16 (43.2%) Profile: Default