

1 - Selecione o primeiro segmento UDP em seu rastreamento. Qual é o packet number deste segmento no arquivo de rastreamento? Que tipo de carga útil da camada de aplicação ou mensagem de protocolo está sendo transportada neste segmento UDP? Veja os detalhes deste pacote no Wireshark. Quantos campos existem no cabeçalho UDP? (Você não deve procurar no livro didático! Responda a essas perguntas diretamente do que você observa no rastreamento de pacotes.) Quais são os nomes desses campos?

No.	Time	Source	Destination	Protocol	Length	Request line	User Datagram Protocol	Info
8651	0.000000	99.181.80.16	192.168.0.6	TLSv1.2	766			Application Data, Application Data, Application Data
8652	0.000088	192.168.0.6	99.181.80.16	TCP	54			60520 → 443 [ACK] Seq=14446 Ack=4742878 Win=2053 Len=0
8653	0.002760	192.168.0.6	66.22.200.45	UDP	1167		✓	55720 → 50004 Len=1125
8654	0.000050	192.168.0.6	66.22.200.45	UDP	1168		✓	55720 → 50004 Len=1126
8655	0.000013	192.168.0.6	66.22.200.45	UDP	1168		✓	55720 → 50004 Len=1126
8656	0.000022	192.168.0.6	66.22.200.45	UDP	1168		✓	55720 → 50004 Len=1126
8657	0.000022	192.168.0.6	66.22.200.45	UDP	1168		✓	55720 → 50004 Len=1126
8658	0.015012	66.22.200.45	192.168.0.6	UDP	122		✓	50004 → 55720 Len=0
8659	0.000024	192.168.0.6	66.22.200.45	UDP	1159		✓	55720 → 50004 Len=1117
8660	0.000041	192.168.0.6	66.22.200.45	UDP	1159		✓	55720 → 50004 Len=1117
8661	0.000017	192.168.0.6	66.22.200.45	UDP	1160		✓	55720 → 50004 Len=1118
8662	0.000014	192.168.0.6	66.22.200.45	UDP	1160		✓	55720 → 50004 Len=1118
8663	0.000017	192.168.0.6	66.22.200.45	UDP	1160		✓	55720 → 50004 Len=1118
8664	0.021923	192.168.0.6	66.22.200.45	UDP	1158		✓	55720 → 50004 Len=1116
8665	0.000040	192.168.0.6	66.22.200.45	UDP	1158		✓	55720 → 50004 Len=1116
8666	0.000017	192.168.0.6	66.22.200.45	UDP	1158		✓	55720 → 50004 Len=1116
8667	0.000016	192.168.0.6	66.22.200.45	UDP	1158		✓	55720 → 50004 Len=1116
8668	0.000021	192.168.0.6	66.22.200.45	UDP	1159		✓	55720 → 50004 Len=1117
8669	0.010608	99.181.80.16	192.168.0.6	TLSv1.2	82			Application Data
8670	0.000000	99.181.80.16	192.168.0.6	TCP	1516			60520 → 443 [ACK] Seq=14446 Win=377 Len=1460 (TCP segment of a nonestablished connection)

Total Length: 1153	0020 c8 2d 8b a8 c3 54 04 6d 4f 7e 9b 65 dd 49 59 20 ...:T...Q...+...Y...
Identification: 0x0982 (55682)	0030 bb f9 00 0d 7b 44 be de 00 03 50 bb c2 63 99 52 ...:D...P...c...R...
Flags: 0x0	0040 35 00 c4 5b 7b 62 81 ec 36 6c 82 2a cd bc a5 32 5 ...:[b...61...*...2...
Fragment Offset: 0	0050 b1 41 fe 5e 4e 82 d3 7f 4b d3 89 12 19 8d fd 47 ...:A...N...K...+...G...
Time to Live: 128	0060 dc 91 a9 64 a2 13 e2 9c 98 89 9c b3 64 92 97 30 ...:d...d...+...d...0...
Protocol: UDP (17)	0070 bb 87 37 2a c9 6e 1b 96 ed aa c3 71 8b a1 55 5a ...:7...n...+...q...U...Z...
Header Checksum: 0x91f7 [validation disabled]	0080 da 04 b3 5e da d2 a5 9f 06 76 89 bf dd 5c 6b 57 ...:A...+...v...+...W...
[Header checksum status: Unverified]	0090 cb 9c 72 82 f2 4f 92 a4 e8 bd 5c 7c 4c 01 8c 90 ...:p...0...+...+...[...L...+...
Source Address: 192.168.0.6	00a0 44 c1 02 de 95 3d 51 37 d1 6d 05 c8 af fb c2 b9 ...:D...+...Q...7...+...m...+...+...
Destination Address: 66.22.200.45	00b0 a7 62 43 34 74 0f 57 17 80 5a b8 14 a3 78 7d 9c ...:bC4t...W...+...Z...+...x...+...+...
User Datagram Protocol, Src Port: 55720, Dst Port: 50004	00c0 47 d2 48 f1 59 fe 51 3e 8c 19 32 c8 7a 8d d9 58 ...:G...H...Y...Q...+...2...+...z...+...X...
Source Port: 55720	00d0 f7 86 9f 77 d8 fd 8e bf f7 ec f3 a5 40 3b 0f aa ...:w...+...+...+...+...+...+...+...+...+...
Destination Port: 50004	00e0 a6 85 3d 81 09 e0 a6 6b 6a ff c0 22 cc 2f 6a 2a ...:e...+...k...j...+...+...+...+...+...+...
Length: 1133	00f0 95 6c e9 46 03 dc d5 e5 81 6c 65 e0 88 d8 14 ...:e...+...F...+...+...+...+...+...+...+...+...
Checksum: 0x4f75 [unverified]	0100 f5 d5 85 ba 14 65 86 7c 35 c7 37 79 93 95 b9 d5 ...:e...+...+...+...+...+...+...+...+...+...+...
[Checksum status: Unverified]	0110 ca 3a 49 0b cd 6d b4 9f e6 fb 36 c7 97 3c 26 40 ...:i...+...+...+...+...+...+...+...+...+...+...
[Stream index: 0]	0120 b1 ac 28 a0 f3 18 cc b3 c6 a7 14 c4 4b a1 3f c5 ...:e...+...+...+...+...+...+...+...+...+...+...
[Timestamps]	0130 36 4f 16 2b 0a 52 fd 8b 7f c7 f7 7f d1 72 b6 1d ...:6...+...+...+...+...+...+...+...+...+...+...
[Time since first frame: 0.477079000 seconds]	0140 9c c6 c6 30 a9 56 3c 00 f7 0b 2f aa 1a 31 ba 21 ...:0...+...V...+...+...+...+...+...+...+...+...
[Time since previous frame: 0.015974000 seconds]	0150 8d 33 6a a5 ce 87 e8 a6 a5 6a 9a 98 43 05 e6 ad ...:3...+...+...+...+...+...+...+...+...+...+...
UDP payload (1125 bytes)	0160 af 08 f9 b3 cc 87 55 73 c7 74 ed 4f 4d 0b c1 74 ...:e...+...+...+...+...+...+...+...+...+...+...
Data: 9065dd495920b9f9000d7b44bede000350bdc6399523500c45b7b6281ec366c822acdbcc...	0170 65 c6 d8 d7 ed 98 fe 90 0c a2 e5 53 84 4e b3 51 ...:e...+...+...+...+...+...+...+...+...+...+...
[Length: 1125]	0180 ec a6 d7 1c b2 a5 92 89 ec 16 c2 cc 27 a0 a6 b5 ...:e...+...+...+...+...+...+...+...+...+...+...

2 - Consultando as informações exibidas no campo de conteúdo do pacote do Wireshark para este pacote (ou consultando o livro), qual é o comprimento (em bytes) de cada um dos campos do cabeçalho UDP?

Os campos do cabeçalho UDP possuem 8 bytes de comprimento.

Fonte: <http://www.cs.toronto.edu/~ahchinaei/teaching/2016jan/csc358/Assignment3wSol.pdf> (página 2).

3 - O valor no campo "Length" é o comprimento de quê? (Você pode consultar o texto para esta resposta). Verifique sua reivindicação com seu pacote UDP capturado.

É o comprimento total do cabeçalho conjuntamente com o do pacote enviado.

4 - Qual é o número máximo de bytes que podem ser incluídos em uma carga UDP? (Dica: a resposta a esta pergunta pode ser determinada pela sua resposta à questão 2 acima.)

Limite teórico: 65.535 bytes (8 bytes do header + 65.527 bytes do conteúdo).

Fonte: https://en.wikipedia.org/wiki/User_Datagram_Protocol#:~:text=The%20field%20size%20sets%20a.data%20for%20a%20UDP%20datagram.

O maior número de portas é 47823.

32754	Unofficial			A backdoor found on certain Linksys, Netgear and other wireless DSL, modems/combo routers ^[394]
32887	Unofficial			Ace of Spades, a multiplayer FPS video game ^[citation needed]
32976	Unofficial			LogMeIn Hamachi, a VPN application; also TCP port 12975 and SSL (TCP 443) ^[395]
33434	Yes	Yes		traceroute
33848		Unofficial		Jenkins, a continuous integration (CI) tool ^{[396][397]}
34000		Unofficial		Infestation: Survivor Stories (formerly known as The War Z), a multiplayer zombie video game ^[verification needed]
34197	No	Unofficial		Factorio, a multiplayer survival and factory-building game ^[398]
35357	Yes			OpenStack Identity (Keystone) administration ^{[399][self-published source?]}
36330	Unofficial			Folding@home Control Port
37008		Unofficial		TZSP intrusion detection ^[citation needed]
40000	Yes	Yes		SafetyNET p – a real-time Industrial Ethernet protocol
41121	Yes	Yes		Tentacle Server ^[400] - Pandora FMS
41794	Yes	Yes		Crestron Control Port ^[401] - Crestron Electronics
41795	Yes	Yes		Crestron Terminal Port ^[402] - Crestron Electronics
41796	Yes	No		Crestron Secure Control Port ^[403] - Crestron Electronics
41797	Yes	No		Crestron Secure Terminal Port ^[404] - Crestron Electronics
42081-42090	Yes	Yes		Zippin - Zippin Stores [?]
42590-42595	Yes	Yes		Glue - MakePro Xt [?]
42806				Discord ^[405]
43110	Unofficial			ZeroNet web UI default port ^[406]
43594–43595		Unofficial		RuneScape ^[407]
44405	Unofficial			Mu Online Connect Server ^[citation needed]
44818	Yes	Yes		EtherNet/IP explicit messaging
47808–47823	Yes	Yes		BACnet Building Automation and Control Networks (47808 ₁₀ = BAC0 ₁₆ to 47823 ₁₀ = BACF ₁₆)
49151	Reserved	Reserved		Reserved ^[2]

Fonte:

[https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers#:~:text=BACnet%20Building%20Automation%20and%20Control%20Networks%20\(4780810%20%3D%20BAC016%20to%204782310%20%3D%20BACF16\)](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers#:~:text=BACnet%20Building%20Automation%20and%20Control%20Networks%20(4780810%20%3D%20BAC016%20to%204782310%20%3D%20BACF16))

6 - Qual é o número do protocolo para UDP? Para responder a essa pergunta, você precisará examinar o campo Protocolo do datagrama IP que contém esse segmento UDP (vide discussão dos campos de cabeçalho IP).

No.	Time	Source	Destination	Protocol	Length	Request line	User Datagram Protocol	Info
8551	0.000000	192.168.0.6	192.168.0.6	TLSv1	766			Application Data, Application Data, Application Data
8552	0.000088	192.168.0.6	99.181.88.16	TCP	54			66520 -> 443 [ACK] Seq=14446 Ack=4742878 Win=2035 Len=0
8553	0.002760	192.168.0.6	66.22.200.45	UDP	1167		✓	55720 -> 50004 Len=1125
8554	0.000050	192.168.0.6	66.22.200.45	UDP	1168		✓	55720 -> 50004 Len=1126
8555	0.000023	192.168.0.6	66.22.200.45	UDP	1168		✓	55720 -> 50004 Len=1126
8556	0.000022	192.168.0.6	66.22.200.45	UDP	1168		✓	55720 -> 50004 Len=1126
8557	0.000022	192.168.0.6	66.22.200.45	UDP	1168		✓	55720 -> 50004 Len=1126
8558	0.015012	66.22.200.45	192.168.0.6	UDP	122		✓	50004 -> 55720 Len=80
8559	0.000024	192.168.0.6	66.22.200.45	UDP	1159		✓	55720 -> 50004 Len=1117
8560	0.000041	192.168.0.6	66.22.200.45	UDP	1159		✓	55720 -> 50004 Len=1117
8561	0.000017	192.168.0.6	66.22.200.45	UDP	1160		✓	55720 -> 50004 Len=1118
8562	0.000014	192.168.0.6	66.22.200.45	UDP	1160		✓	55720 -> 50004 Len=1118
8563	0.000017	192.168.0.6	66.22.200.45	UDP	1160		✓	55720 -> 50004 Len=1118
8564	0.021923	192.168.0.6	66.22.200.45	UDP	1158		✓	55720 -> 50004 Len=1116
8565	0.000040	192.168.0.6	66.22.200.45	UDP	1158		✓	55720 -> 50004 Len=1116
8566	0.000017	192.168.0.6	66.22.200.45	UDP	1158		✓	55720 -> 50004 Len=1116
8567	0.000016	192.168.0.6	66.22.200.45	UDP	1158		✓	55720 -> 50004 Len=1116
8568	0.000021	192.168.0.6	66.22.200.45	UDP	1159		✓	55720 -> 50004 Len=1117
8569	0.010600	99.181.88.16	192.168.0.6	TLSv1.2	82			Application Data
8570	0.000000	99.181.88.16	192.168.0.6	TCP	54			6651 -> 60530 [RST] Seq=4743006 Rst=16666 Win=1771 len=1460 TCP segment of a sequence that doesn't exist

[Protocols in frame: ethertype:ip:udp:data]
[Coloring Rule Name: udp]
[Coloring Rule String: udp]

Ethernet II, Src: Micro-St-27:f0:f1 (30:9c:23:27:f0:f1), Dst: T-LinkT_3b:a2:84 (28:ee:52:3b:a2:84)
Destination: T-LinkT_3b:a2:84 (28:ee:52:3b:a2:84)
Source: Micro-St-27:f0:f1 (30:9c:23:27:f0:f1)
Type: IPv4 (0x0008)

Internet Protocol Version 4, Src: 192.168.0.6, Dst: 66.22.200.45
0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differeniated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1153
Identification: 0xd982 (55682)
0000 = Flags: 0x0
... 0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x9177 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.6
Destination Address: 66.22.200.45

User Datagram Protocol, Src Port: 55720, Dst Port: 50004
Source Port: 55720
Destination Port: 50004

O número do protocolo UDP é 17.

7 - Examine o par de pacotes UDP em que seu host envia o primeiro pacote UDP e o segundo pacote UDP é uma resposta a este primeiro pacote UDP. (Dica: para que um segundo pacote seja enviado em resposta a um primeiro pacote, o remetente do primeiro pacote deve ser o destino do segundo pacote). Qual é o packet number do primeiro desses dois segmentos UDP no arquivo de rastreamento? Qual é o packet number do segundo desses dois segmentos UDP no arquivo de rastreamento? Descreva a relação entre os números de porta nos dois pacotes.

A relação é que os números da porta de envio e destino são semelhantes.

No.	Time	Source	Destination	Protocol	Length	Info
1468	2.767633	192.168.0.1	192.168.0.104	DNS	145	Standard query response 0x0004 No such name A kabi
1469	2.768217	192.168.0.104	192.168.0.1	DNS	90	Standard query 0x0005 AAAA kabum.com.br.svc.accen
1470	2.771333	66.22.200.45	192.168.0.104	UDP	1100	50004 → 59844 Len=1058
1471	2.772288	192.168.0.1	192.168.0.104	DNS	145	Standard query response 0x0005 No such name AAAA
1472	2.772986	192.168.0.104	192.168.0.1	DNS	86	Standard query 0x0006 A kabum.com.br.accenture.co
1473	2.774504	192.168.0.104	66.22.200.48	UDP	165	59843 → 50001 Len=123
1474	2.783088	66.22.200.45	192.168.0.104	UDP	1116	50004 → 59844 Len=1074
1475	2.783088	66.22.200.45	192.168.0.104	UDP	1116	50004 → 59844 Len=1074
1476	2.783088	66.22.200.45	192.168.0.104	UDP	1116	50004 → 59844 Len=1074
1477	2.783088	66.22.200.45	192.168.0.104	UDP	1116	50004 → 59844 Len=1074

User Datagram Protocol, Src Port: 52579, Dst Port: 53

Source Port: 52579
Destination Port: 53
Length: 56
Checksum: 0x36f5 [unverified]
[Checksum Status: Unverified]
[Stream index: 7]
[Timestamp:]

0000 38 6b 1c 16 ae 55 cc f9 e4 82 08 75 08 00 45 00 8k...U...U...E-

UDP enviado.

2288	192.168.0.1	192.168.0.104	DNS	145	Standard query response 0x0005 No such name AAAA kabum.com.br...
2986	192.168.0.104	192.168.0.1	DNS	86	Standard query 0x0006 A kabum.com.br.accenture.com
4504	192.168.0.104	66.22.200.48	UDP	165	59843 → 50001 Len=123
3088	66.22.200.45	192.168.0.104	UDP	1116	50004 → 59844 Len=1074
3088	66.22.200.45	192.168.0.104	UDP	1116	50004 → 59844 Len=1074
3088	66.22.200.45	192.168.0.104	UDP	1116	50004 → 59844 Len=1074
3088	66.22.200.45	192.168.0.104	UDP	1116	50004 → 59844 Len=1074

User Datagram Protocol, Src Port: 53, Dst Port: 52579

Source Port: 53
Destination Port: 52579
Length: 111
Checksum: 0xc3a6 [unverified]
[Checksum Status: Unverified]
[Stream index: 7]
[Timestamp:]

0000 66 f0 e4 82 08 75 08 fb 16 16 00 55 08 00 45 00 00k...U...E-

Resposta.