

Home work 10

Apply a display filter ... <Ctrl>

No.	Time	Source	Destination	Protocol	Length	Info
3	0.055972145	192.168.1.1	192.168.1.4	DNS	126	Standard query response 0x28d8 AAAA akamai.com AAAA 2a02:26f0:1700:598::b63 AAAA 2a02:26f0:1700:584::b63
4	0.056400973	192.168.1.1	192.168.1.4	DNS	86	Standard query response 0x3485 A akamai.com A 84.53.158.92
21	0.058827976	192.168.1.1	192.168.1.4	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
23	0.067747747	192.168.1.1	192.168.1.4	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
24	0.067748092	192.168.1.1	192.168.1.4	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
32	0.083860612	192.168.1.1	192.168.1.4	DNS	84	Standard query response 0xc077 No such name PTR 1.1.1.108.192.in-addr.arpa
41	0.099339216	192.168.1.1	192.168.1.4	DNS	86	Standard query response 0x5175 No such name PTR 1.100.168.192.in-addr.arpa
55	0.134788983	192.168.1.1	192.168.1.4	DNS	152	Standard query response 0xb950 No such name PTR 56.133.226.87.in-addr.arpa SOA dns1.msk.ip.rostelecom.ru
58	0.155715956	192.168.1.1	192.168.1.4	DNS	126	Standard query response 0xafdc PTR 46.129.155.213.in-addr.arpa PTR s-b9-link.ip.twelve99.net
60	0.171844548	192.168.1.1	192.168.1.4	DNS	127	Standard query response 0xcf0a PTR 180.139.115.62.in-addr.arpa PTR s-bb1-link.ip.twelve99.net
86	0.233965777	192.168.1.1	192.168.1.4	DNS	128	Standard query response 0x9e27 PTR 94.134.115.62.in-addr.arpa PTR hbq-bb3-link.ip.twelve99.net
97	0.338167249	192.168.1.1	192.168.1.4	DNS	127	Standard query response 0xdac4 PTR 19.249.91.80.in-addr.arpa PTR ldn-bb1-link.ip.twelve99.net
99	0.417266233	192.168.1.1	192.168.1.4	DNS	127	Standard query response 0x8e20 PTR 75.120.115.62.in-addr.arpa PTR ldn-b3-link.ip.twelve99.net
101	0.451614734	192.168.1.1	192.168.1.4	DNS	144	Standard query response 0xd6df PTR 185.169.115.62.in-addr.arpa PTR akamai-1c350070-ldn-b3.ip.twelve99-cust.net
112	0.510175394	192.168.1.1	192.168.1.4	DNS	133	Standard query response 0x5ec6 PTR 205.48.210.23.in-addr.arpa PTR ae4.linx-lon12.netarch.akamai.com
123	0.868910230	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0xd79e PTR 92.158.53.84.in-addr.arpa PTR a84-53-158-92.deploy.static.akamaitechnologies.com
1	0.000000000	192.168.1.4	192.168.1.1	DNS	70	Standard query 0x3485 A akamai.com
2	0.000221781	192.168.1.4	192.168.1.1	DNS	70	Standard query 0x28d8 AAAA akamai.com
5	0.057110769	192.168.1.4	84.53.158.92	ICMP	70	Echo (ping) request id=0x0002, seq=1/256, ttl=1 (no response found!)
6	0.057145034	192.168.1.4	84.53.158.92	ICMP	70	Echo (ping) request id=0x0002, seq=2/512, ttl=1 (no response found!)
7	0.057155770	192.168.1.4	84.53.158.92	ICMP	70	Echo (ping) request id=0x0002, seq=3/768, ttl=1 (no response found!)
8	0.057882475	192.168.1.4	84.53.158.92	ICMP	70	Echo (ping) request id=0x0002, seq=4/1024, ttl=1 (no response found!)

Frame 5: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface wlo1, id 0

Ethernet II, Src: 64:6e:e0:a2:6f:89 (64:6e:e0:a2:6f:89), Dst: Netgear_0a:c2:48 (c4:04:15:0a:c2:48)

Internet Protocol Version 4, Src: 192.168.1.4, Dst: 84.53.158.92

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0800 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 56

Identification: 0x1e80 (7808)

Flags: 0x0000

0... .. = Reserved bit: Not set

.0... .. = Don't fragment: Not set

..0... .. = More fragments: Not set

Fragment offset: 0

Time to live: 1

[Expert Info (Note/Sequence): "Time To Live" only 1]

[Time To Live" only 1]

[Severity level: Note]

[Group: Sequence]

Protocol: ICMP (1)

Header checksum: 0xe707 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.4

Destination: 84.53.158.92

Internet Control Message Protocol

0000 c4 04 15 0a c2 48 64 6e e0 a2 6f 89 08 00 45 00Hdn..o...H..E..

0010 00 54 35 9a 00 01 01 5e f9 c0 a8 64 01 c0 a8 ..T5...A...d...T5...A...d...

0020 01 04 0b 00 cc 25 00 00 00 00 45 00 38 1e 83%...E..8...

0030 00 00 01 01 e7 04 c0 a8 01 04 54 35 9e 5c 08 00T5\...

0040 76 1b 00 02 00 04 48 49 4a 4b 4c 4d 4e 4f 50 51 v.....HI JKLMNOPQ

0050 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 RSTUVWXY Z[\]^_`a

0060 62 63 bc

Header Length (ip_hdr_len), 1 byte

Packets: 140 · Displayed: 140 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

1. Source: 192.168.1.4
2. Protocol: ICMP (1)
3. 0101 = Header Length: 20 bytes (5), полезная 56 - 20
- 4а. меняются TTL, Identification, Header checksum
- 4б. все остальные поля не меняются и не должны, поля выше должны меняться
- 4с. инкрементирование
5. Identification: 0x1e80 (7808), Time to live: 1
6. Нет
7. Identification: 0x359a (13722), Time to live: 63

Frame 25: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0

Ethernet II, Src: Netgear_0a:c2:48 (c4:04:15:0a:c2:48), Dst: 64:6e:e0:a2:6f:89 (64:6e:e0:a2:6f:89)

Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.1.4

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)

1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 84

Identification: 0x359a (13722)

Flags: 0x0000

0... .. = Reserved bit: Not set

.0... .. = Don't fragment: Not set

..0... .. = More fragments: Not set

Fragment offset: 0

Time to live: 63

Protocol: ICMP (1)

Header checksum: 0x5ef9 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.100.1

Destination: 192.168.1.4

Internet Control Message Protocol

0000 64 6e e0 a2 6f 89 c4 04 15 0a c2 48 08 00 45 c0 dn..o...H..E..

0010 00 54 35 9a 00 01 01 5e f9 c0 a8 64 01 c0 a8 ..T5...A...d...T5...A...d...

0020 01 04 0b 00 cc 25 00 00 00 00 45 00 38 1e 83%...E..8...

0030 00 00 01 01 e7 04 c0 a8 01 04 54 35 9e 5c 08 00T5\...

0040 76 1b 00 02 00 04 48 49 4a 4b 4c 4d 4e 4f 50 51 v.....HI JKLMNOPQ

0050 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 RSTUVWXY Z[\]^_`a

0060 62 63 bc

8. а. да, 5; б. checksum, flags, total length, fragment offset

io. Time Source Destination Protocol Length Info

117 0.126885531 80.81.195.147 192.168.1.4 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

118 0.133787365 192.168.1.1 192.168.1.4 DNS 148 Standard query response 0x1a1f No such name PTR 253.148.148.185.in-addr.arpa SOA pri.authdns.ripe.net

123 0.146852962 80.81.195.147 192.168.1.4 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

124 0.146852962 80.255.14.58 192.168.1.4 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

125 0.147370677 80.255.14.58 192.168.1.4 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

126 0.147370856 80.255.14.58 192.168.1.4 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

127 0.151142144 192.168.1.1 192.168.1.4 DNS 130 Standard query response 0x86f6 PTR 147.195.81.80.in-addr.arpa PTR ae10-1.fra30.core-backbone.com

128 0.151623625 81.95.2.78 192.168.1.4 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

130 0.151623808 81.95.2.78 192.168.1.4 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

131 0.151623875 81.95.2.78 192.168.1.4 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)

141 0.162750649 104.107.218.43 192.168.1.4 IPv4 1506 Fragmented IP protocol (proto=ICMP 1, off=0, ID=336f) [Reassembled in #145]

142 0.166325038 104.107.218.43 192.168.1.4 IPv4 42 Fragmented IP protocol (proto=ICMP 1, off=1472, ID=336f) [Reassembled in #145]

143 0.166325236 104.107.218.43 192.168.1.4 IPv4 1506 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=336f) [Reassembled in #145]

144 0.166325335 104.107.218.43 192.168.1.4 IPv4 42 Fragmented IP protocol (proto=ICMP 1, off=2952, ID=336f) [Reassembled in #145]

145 0.166325476 104.107.218.43 192.168.1.4 IPv4 1506 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3370) [Reassembled in #150]

146 0.166325476 104.107.218.43 192.168.1.4 IPv4 1506 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3370) [Reassembled in #150]

147 0.166325544 104.107.218.43 192.168.1.4 IPv4 42 Fragmented IP protocol (proto=ICMP 1, off=1472, ID=3370) [Reassembled in #150]

148 0.166325618 104.107.218.43 192.168.1.4 IPv4 1506 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3370) [Reassembled in #150]

149 0.166325687 104.107.218.43 192.168.1.4 IPv4 42 Fragmented IP protocol (proto=ICMP 1, off=2952, ID=3370) [Reassembled in #150]

150 0.166388435 104.107.218.43 192.168.1.4 ICMP 554 Echo (ping) reply id=0x0003, seq=26/6656, ttl=57 (request in 102)

151 0.167119533 104.107.218.43 192.168.1.4 IPv4 1506 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3371) [Reassembled in #155]

152 0.167119533 104.107.218.43 192.168.1.4 IPv4 42 Fragmented IP protocol (proto=ICMP 1, off=1472, ID=3371) [Reassembled in #155]

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.....00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 540
Identification: 0x336f (13167)
Flags: 0x0172
0... .. = Reserved bit: Not set
.0... .. = Don't fragment: Not set
..0... .. = More fragments: Not set
Fragment offset: 2960
Time to live: 57
Protocol: ICMP (1)
Header checksum: 0x46bd [validation disabled]
[Header checksum status: Unverified]
Source: 104.107.218.43
Destination: 192.168.1.4

[5 IPv4 Fragments (3480 bytes): #141(1472), #142(8), #143(1472), #144(8), #145(520)]
[Frame: 141, payload: 0-1471 (1472 bytes)]
[Frame: 142, payload: 1472-1479 (8 bytes)]
[Frame: 143, payload: 1480-2951 (1472 bytes)]
[Frame: 144, payload: 2952-2959 (8 bytes)]
[Frame: 145, payload: 2960-3479 (520 bytes)]
[Fragment count: 5]
[Reassembled IPv4 length: 3480]
[Reassembled IPv4 data: 0000badd0003001948494a4b4c4d4e4f5051525354555657..]

Internet Control Message Protocol

0010 02 1c 33 6f 01 72 80 01 46 bd 68 6b da 2b c0 a8 ..3o-r0·F-hk·++·
0020 01 04 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d ..PQRSTU VwXYZ[\]
0030 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d ^_abcde fghijklm
0040 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d nopqrstu vwxyz{|}
0050 7e 7f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d ~@ABCDE FGHIJKLM
0060 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d NOPQRSTU VwXYZ[\]
0070 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d ^_abcde fghijklm
0080 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d nopqrstu vwxyz{|}
0090 7e 7f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d ~@ABCDE FGHIJKLM
00a0 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d NOPQRSTU VwXYZ[\]
00b0 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d ^_abcde fghijklm
00c0 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d nopqrstu vwxyz{|}

Frame (554 bytes) Reassembled IPv4 (3480 bytes)

Time to live (ip.ttl), 1 byte

Packets: 210 · Displayed: 210 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Home work 10

2