

10th Homework

Ogloblin Ivan

8 июня 2022 г.

1

Source: 192.168.1.4

```
3 0.955972145 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 0.956400973 192.168.1.1 192.168.1.4 DNS 86 Standard query response 0x3485 A akamai.com A 84.53.158.92
21 0.958827976 192.168.1.1 192.168.1.4 ICMP 98 Time-to-live exceeded (Time to live exceeded in transit)
23 0.967747747 192.168.1.1 192.168.1.4 ICMP 98 Time-to-live exceeded (Time to live exceeded in transit)
24 0.967748992 192.168.1.1 192.168.1.4 ICMP 98 Time-to-live exceeded (Time to live exceeded in transit)
32 0.983660612 192.168.1.1 192.168.1.4 DNS 84 Standard query response 0xcd77 No such name PTR 1.1.168.192.in-addr.arpa
41 0.999339216 192.168.1.1 192.168.1.4 DNS 86 Standard query response 0x5175 No such name PTR 1.180.168.192.in-addr.arpa
55 0.134788983 192.168.1.1 192.168.1.4 DNS 152 Standard query response 0xb059 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-b6-link.ip.twelve99.net
69 0.171844548 192.168.1.1 192.168.1.4 DNS 127 Standard query response 0xcf8a 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 hbg-bb3-link.ip.twelve99.net
97 0.338167249 192.168.1.1 192.168.1.4 DNS 127 Standard query response 0xdac4 PTR 10.249.91.88.in-addr.arpa PTR ldn-bb1-link.ip.twelve99.net
99 0.417286233 192.168.1.1 192.168.1.4 DNS 127 Standard query response 0x8e29 PTR 75.129.115.62.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 0x06fd 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 205.48.219.23.in-addr.arpa PTR ae4.linx-lon12.netarch.akamai.com
123 0.868910239 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 0.908080699 192.168.1.4 192.168.1.1 DNS 70 Standard query 0x3485 A akamai.com
2 0.908221781 192.168.1.4 192.168.1.1 DNS 70 Standard query 0x28d8 AAAA akamai.com
5 0.957110769 192.168.1.4 84.53.158.92 ICMP 70 Echo (ping) request id=0x0002, seq=1/256, ttl=1 (no response found)
6 0.957145834 192.168.1.4 84.53.158.92 ICMP 70 Echo (ping) request id=0x0002, seq=2/512, ttl=1 (no response found)
7 0.957159770 192.168.1.4 84.53.158.92 ICMP 70 Echo (ping) request id=0x0002, seq=3/768, ttl=1 (no response found)
8 0.957166475 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 wi01, id 0
* Ethernet II, Src: 84:6e:e0:a2:6f:89 (84:6e:e0:a2:6f:89), Dst: Netgear_0a:c2:48 (c4:64:15:0a: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)
0000 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 00 00 .....Hdn...0...
0010 00 38 1e 00 00 00 01 01 e7 07 c0 a8 01 04 54 35 ..8.....75
0020 9e 5c 08 00 4d 44 00 02 00 01 48 49 4a 4b 4c 4d ..\ MD - HIJKLM
0030 4e 4f 58 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d NOPQRSTU VWXYZ[\
0040 5e 5f 60 61 62 63 ^_ abc
```

2

Protocol: ICMP (1)

3

.... 0101 = Header Length: 20 bytes (5), полезная 56 - 20

4

4.1

меняются TTL, Identification, Header checksum

4.2

все остальные поля не меняются и не должны, поля выше должны меняться

4.3

инкрементирование

5

Identification: 0x1e80 (7808), Time to live: 1

6

Her

7

Identification: 0x359a (13722), Time to live: 63

110	0.452321495	192.168.1.4	84.53.158.92	ICMP	78 Echo (ping) request id=0x0002, seq=49/12544, ttl=17 (reply in 122)
111	0.452858283	192.168.1.4	192.168.1.1	DNS	86 Standard query 0x5ec PTR 205.48.210.23.in-addr.arpa
119	0.511227142	192.168.1.4	192.168.1.1	DNS	85 Standard query 0xd79e PTR 92.158.53.84.in-addr.arpa
124	1.641796676	192.168.1.4	3.68.63.139	TLSv1.2	120 Application Data
125	1.646688940	192.168.1.4	35.232.111.17	TCP	74 45536 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1540782228 TSecr=0 WS=128
128	1.684390510	192.168.1.4	3.68.63.139	TCP	66 43958 → 443 [ACK] Seq=55 Ack=57 Win=783 Len=0 TSval=3593233389 TSecr=4187908050
130	1.889593084	192.168.1.4	35.232.111.17	TCP	66 45536 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1540782471 TSecr=2272394901
131	1.889744437	192.168.1.4	35.232.111.17	HTTP	153 GET / HTTP/1.1
133	2.094760786	192.168.1.4	35.232.111.17	TCP	66 45536 → 80 [ACK] Seq=88 Ack=149 Win=64128 Len=0 TSval=1540782676 TSecr=2272395181
134	2.094930995	192.168.1.4	35.232.111.17	TCP	66 45536 → 80 [FIN, ACK] Seq=88 Ack=149 Win=64128 Len=0 TSval=1540782676 TSecr=2272395181
136	2.095097698	192.168.1.4	35.232.111.17	TCP	66 [TCP Dup ACK 133#1] 45536 → 80 [ACK] Seq=89 Ack=149 win=64128 Len=0 TSval=1540782677 TSecr=2272395181
138	2.095122252	192.168.1.4	35.232.111.17	TCP	66 45536 → 80 [ACK] Seq=89 Ack=150 Win=64128 Len=0 TSval=1540782677 TSecr=2272395181
140	2.402208413	192.168.1.4	213.180.193.2	TCP	66 51472 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=569345610 TSecr=3507665429
25	0.071655262	192.168.100.1	192.168.1.4	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
26	0.071667715	192.168.100.1	192.168.1.4	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
27	0.071779204	192.168.100.1	192.168.1.4	ICMP	98 Time-to-live exceeded (Time to live exceeded in transit)
31	0.083309338	212.48.204.104	192.168.1.4	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
33	0.083709558	212.48.204.104	192.168.1.4	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
34	0.083709652	212.48.204.104	192.168.1.4	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
37	0.090292748	213.155.129.46	192.168.1.4	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
42	0.090916882	213.155.129.46	192.168.1.4	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
43	0.090916882	213.155.129.46	192.168.1.4	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
Frame 25: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0					
Ethernet II, Src: Netgear_9a:c2:48 (c4:84:15:9a: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					
[Raw data: 64 bytes]					
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					
[Raw data: 98 bytes]					
0000	64 6e e0 a2 6f 89 c4 04	15 9a c2 48 00 00 45 c0	dn o ... H E		
0010	00 54 35 9a 00 00 01 01	5e f9 c0 a8 64 01 c0 a8	TS... A...d...		
0020	01 04 00 00 cc 25 00 00	00 00 45 00 00 38 1e 83	...S... E...8...		
0030	00 00 01 01 e7 04 c0 a8	01 64 54 35 9e 5c 08 00 TS...		
0040	76 1b 00 02 09 64 48 49	4a 4b 4c 4d 4e 4f 50 51	v... HI JKL MN OPQ		
0050	52 53 54 55 56 57 58 59	5a 5b 5c 5d 5e 5f 60 61	RSTU VWXY Z[\]^_`a		
0060	62 63		bc		

8

8.1

да, 5

checksum, flags, total length, fragment offset

```

117 0.126895531 80.81.195.147 192.168.1.4 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
118 0.133787965 192.168.1.1 192.168.1.4 DNS 148 Standard query response 0x1a1f No such name PIR 253.148.140.185.in-addr.arpa SOA pri.authdns.ripe.net
119 0.144084332 80.81.195.147 192.168.1.4 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
124 0.146855296 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 0.147370656 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 0x5bfe PIR 147.195.81.0.in-addr.arpa PIR ae10-1.fra30.core-backbone.com
128 0.151524525 192.168.1.4 192.168.1.4 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 184.107.218.43 192.168.1.4 IPv4 1506 Fragmented IP protocol (proto:ICMP 1, off=0, ID=336f) [Reassembled in #145]
142 0.166325638 184.107.218.43 192.168.1.4 IPv4 42 Fragmented IP protocol (proto:ICMP 1, off=1472, ID=336f) [Reassembled in #145]
143 0.166325236 184.107.218.43 192.168.1.4 IPv4 1506 Fragmented IP protocol (proto:ICMP 1, off=1480, ID=336f) [Reassembled in #145]
144 0.166325335 184.107.218.43 192.168.1.4 IPv4 42 Fragmented IP protocol (proto:ICMP 1, off=2952, ID=336f) [Reassembled in #145]
145 0.166325404 184.107.218.43 192.168.1.4 ICMP 54 Echo (ping) reply id=0x0003, seq=26/6056, ttl=57 (request in #142)
146 0.166325476 184.107.218.43 192.168.1.4 IPv4 1506 Fragmented IP protocol (proto:ICMP 1, off=0, ID=3370) [Reassembled in #150]
147 0.166325544 184.107.218.43 192.168.1.4 IPv4 42 Fragmented IP protocol (proto:ICMP 1, off=1472, ID=3370) [Reassembled in #150]
148 0.166325618 184.107.218.43 192.168.1.4 IPv4 1506 Fragmented IP protocol (proto:ICMP 1, off=1480, ID=3370) [Reassembled in #150]
149 0.166325687 184.107.218.43 192.168.1.4 IPv4 42 Fragmented IP protocol (proto:ICMP 1, off=2952, ID=3370) [Reassembled in #150]
150 0.166388435 184.107.218.43 192.168.1.4 ICMP 54 Echo (ping) reply id=0x0003, seq=26/6056, ttl=57 (request in #152)
151 0.167119533 184.107.218.43 192.168.1.4 IPv4 1506 Fragmented IP protocol (proto:ICMP 1, off=0, ID=3371) [Reassembled in #155]
152 0.167119593 184.107.218.43 192.168.1.4 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
+ [Length: 5]
  Protocol: ICMP (1)
  Header checksum: 0x46bd [validation disabled]
  [Header checksum status: Unverified]
  Source: 184.107.218.43
  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: 0000badd0003001940494a4b4c4d4e4f5051525354555657..]
+ Internet Control Message Protocol
0010 02 1c 33 6f 01 72 81 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 WXYZ[\]
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 WXYZ[\]
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 WXYZ[\]
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)