Project 2

ECE 5565
Network Architecture and Protocols

Ajit Sarkaar
906213662
sarkaar@vt.edu

Date of Submission:
10/30/2018

PART 2.2

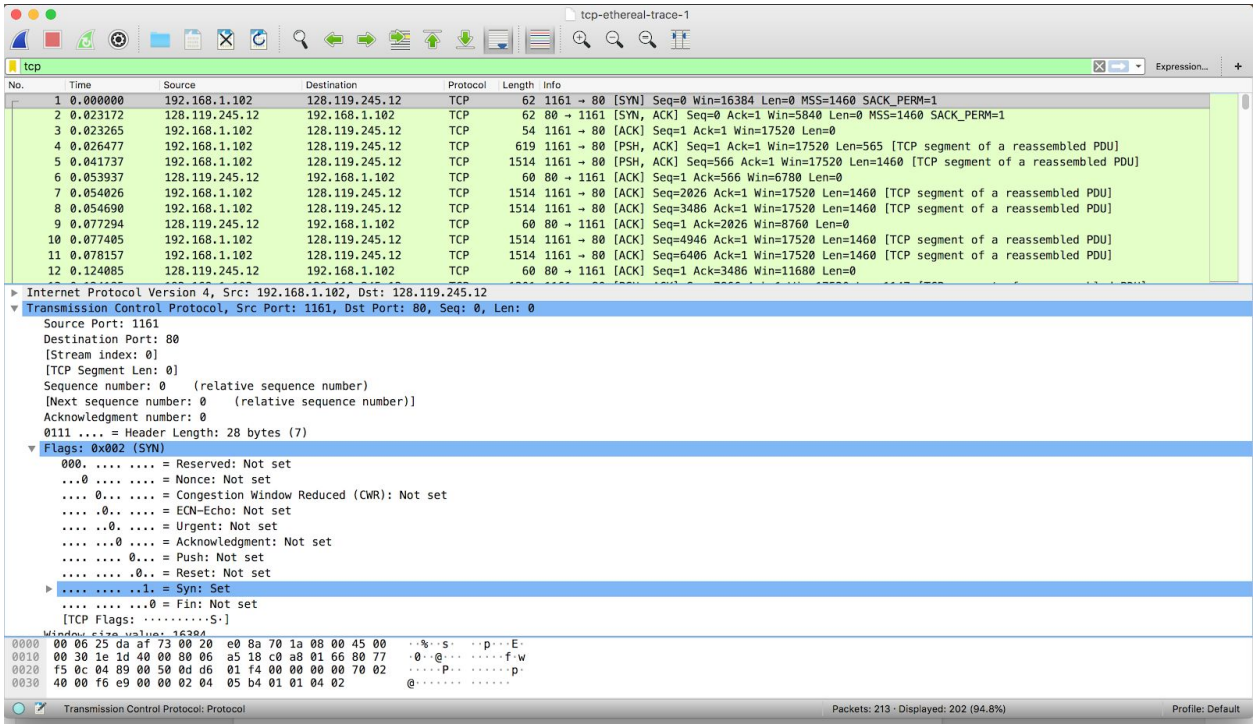
1. Client IP Address: 192.168.1.102
   Client Port Number: 1161
   The IP address of gaia.cs.umass.edu is: 128.119.245.12
   Gaia.cs.umass.edu is sending and receiving TCP segments for this connection on port number: 80.

```
No.     Time           Source                Destination           Protocol Length Info
    199 5.297341       192.168.1.102         128.119.245.12        HTTP     104    POST
/ethereal-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)

Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
Ethernet  II,  Src:  Actionte_8a:70:1a  (00:20:e0:8a:70:1a),  Dst:  LinksysG_da:af:73
(00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len:
50
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 50]
    Sequence number: 164041    (relative sequence number)
    [Next sequence number: 164091    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 17520
    [Calculated window size: 17520]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x9f0f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (50 bytes)
    TCP segment data (50 bytes)
[122 Reassembled TCP Segments (164090 bytes): #4(565), #5(1460), #7(1460), #8(1460),
#10(1460), #11(1460), #13(1147), #18(1460), #19(1460), #20(1460), #21(1460), #22(1460),
#23(892), #30(1460), #31(1460), #32(1460), #33(1460), #34(1460), #3]
Hypertext Transfer Protocol
MIME    Multipart    Media    Encapsulation,    Type:    multipart/form-data,    Boundary:
"---------------------------265001916915724"
```

2. Sequence number of the TCP SYN Segment to initiate the connection: 0
   The SYN bit in the TCP Flag field is set to 1, which identifies the segment as a SYN segment.

```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       192.168.1.102         128.119.245.12        TCP      62     1161
→ 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet  II,  Src:  Actionte_8a:70:1a  (00:20:e0:8a:70:1a),  Dst:  LinksysG_da:af:73
(00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
```

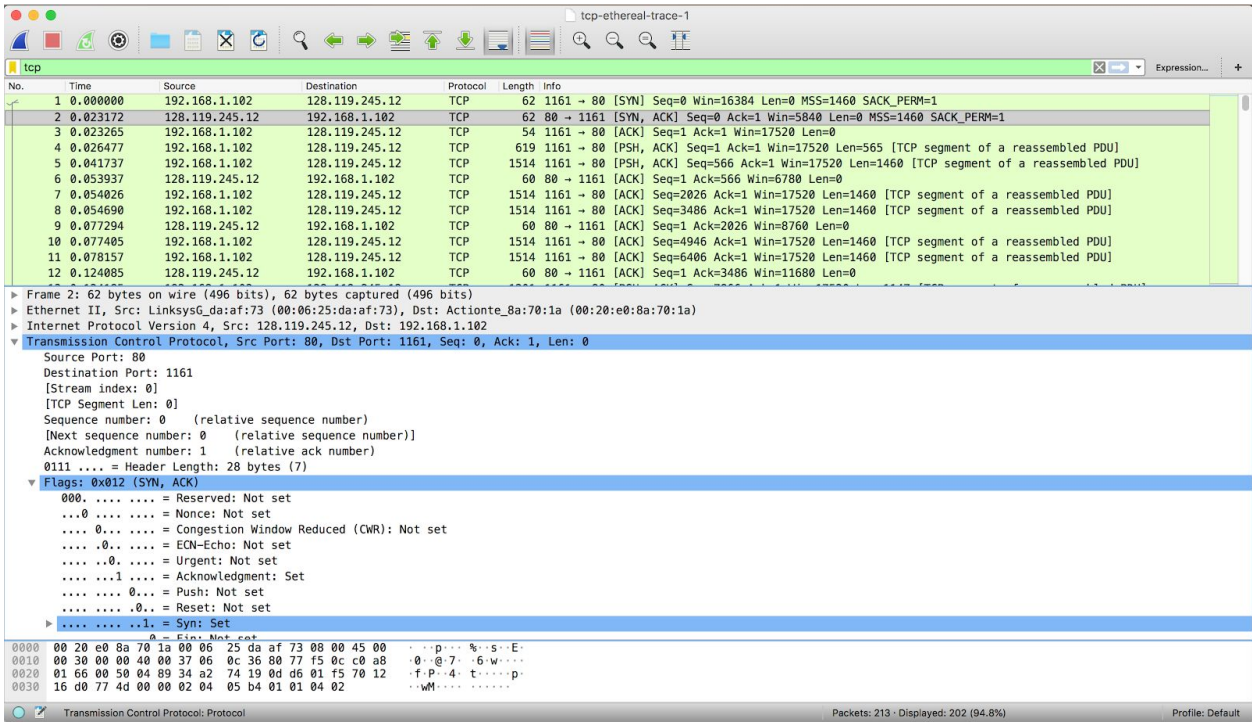
```
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    0111 .... = Header Length: 28 bytes (7)
    Flags: 0x002 (SYN)
    Window size value: 16384
    [Calculated window size: 16384]
    Checksum: 0xf6e9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
     Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP),
SACK permitted
    [Timestamps]
```



3. Sequence number of the [SYN ACK] segment sent from server to client: 0
   Value of the ACK field in the [SYN ACK] segment: 1
   Since this is the 2nd step in the 3-way handshake in TCP, The server, gaia.cs.umass.edu determines this number by incrementing the last received sequence number from the client. The server is telling the client that it is expecting the client to send a segment with this sequence number: 0 + 1 = 1.
   The SYN bit and the ACK bit in the segment are set to 1, which identifies this as a [SYN ACK] segment.

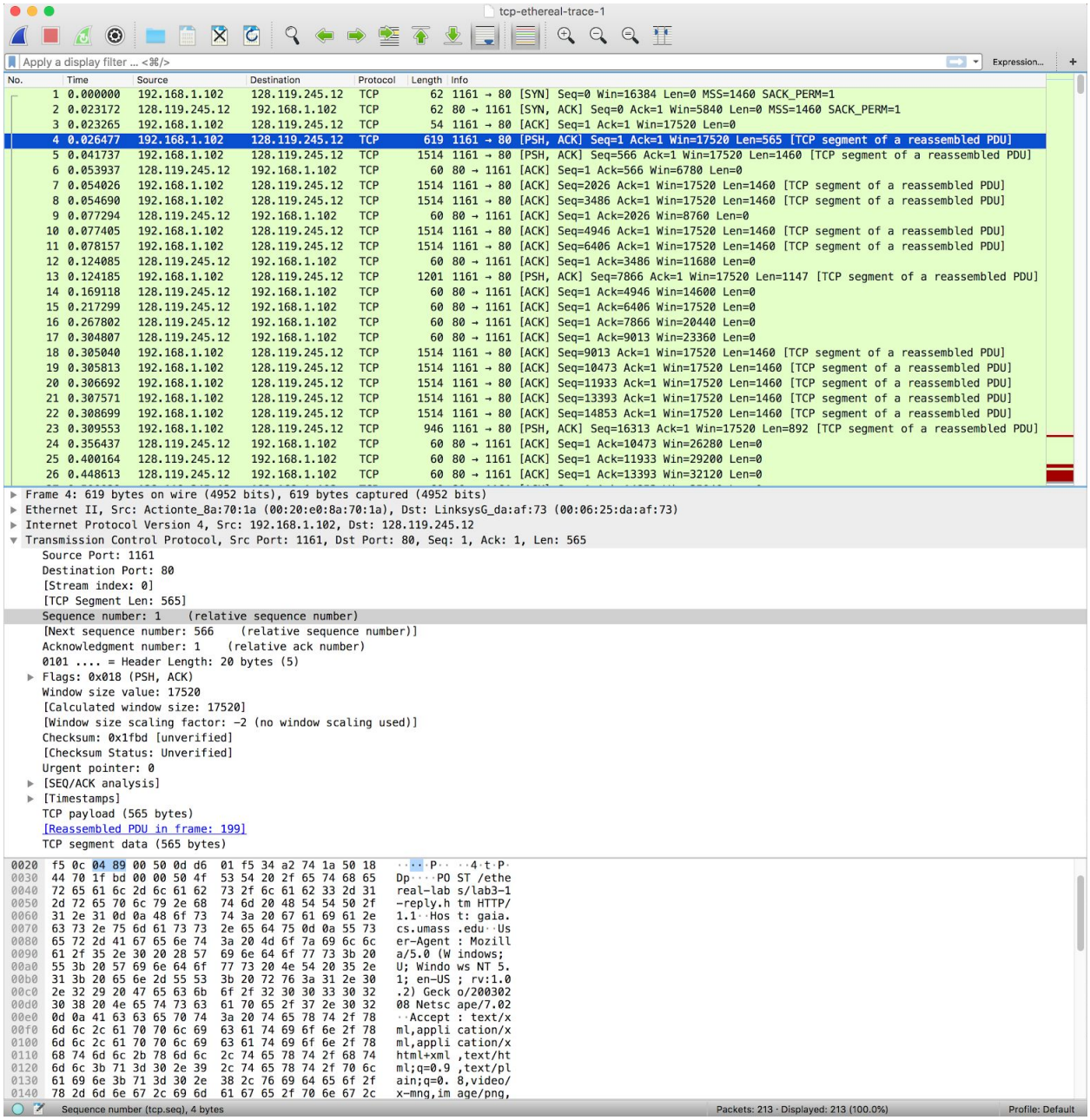
```
No.     Time           Source                Destination           Protocol Length Info
```

```
      2 0.023172       128.119.245.12        192.168.1.102         TCP      62     80 →
1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1

Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet  II,  Src:  LinksysG_da:af:73  (00:06:25:da:af:73),  Dst:  Actionte_8a:70:1a
(00:20:e0:8a:70:1a)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0111 .... = Header Length: 28 bytes (7)
    Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·····A··S·]
    Window size value: 5840
    [Calculated window size: 5840]
    Checksum: 0x774d [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
     Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP),
SACK permitted
    [SEQ/ACK analysis]
    [Timestamps]
```



4. Sequence number of the TCP segment containing the HTTP POST command: 1

```
No.     Time           Source                Destination           Protocol Length Info
      4 0.026477       192.168.1.102         128.119.245.12        TCP      619    1161
→ 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]

Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73
(00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, Ack: 1, Len: 565
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 565]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 566    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 17520
    [Calculated window size: 17520]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x1fbd [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (565 bytes)
    [Reassembled PDU in frame: 199]
    TCP segment data (565 bytes)
```



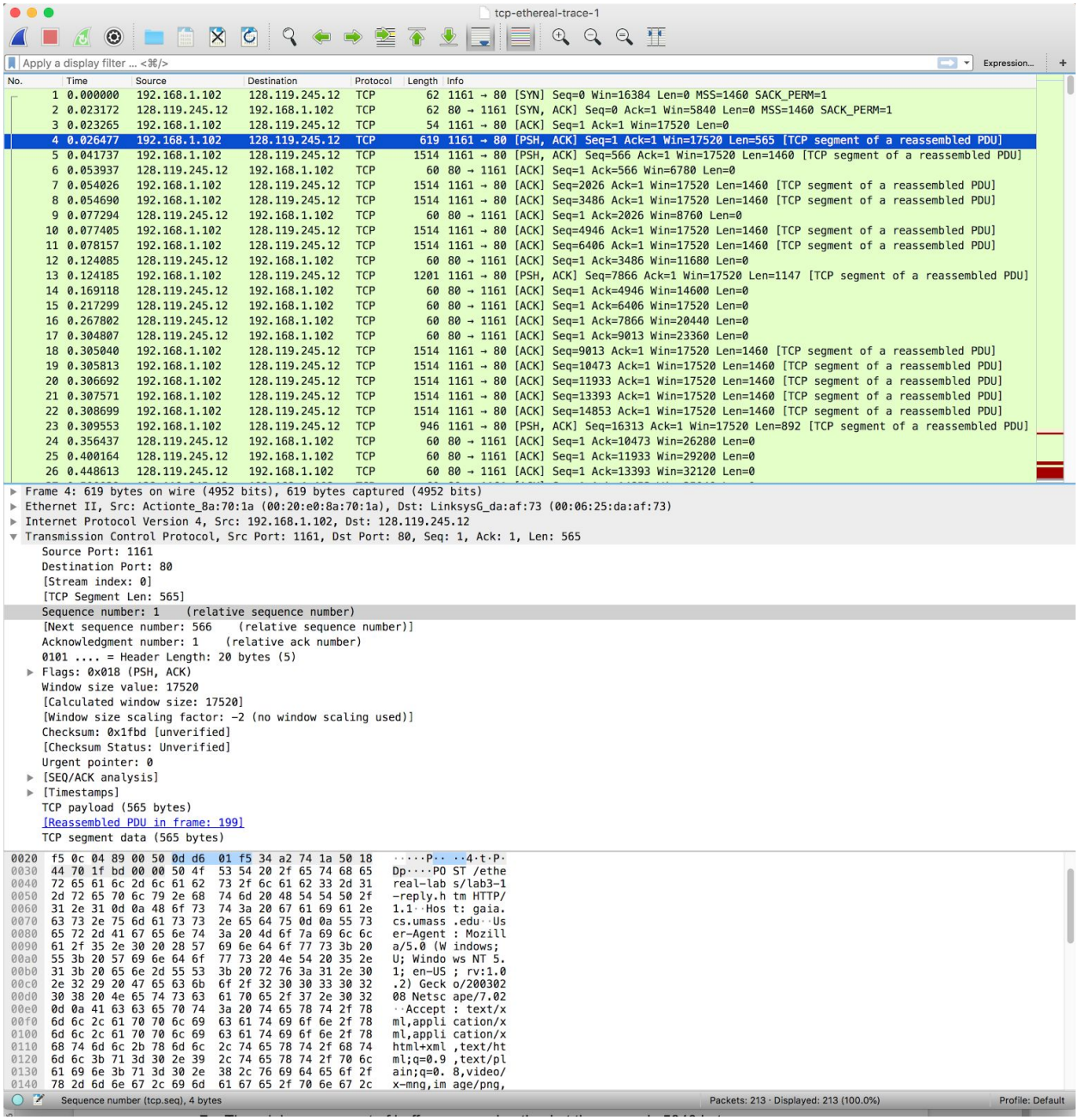
5. The HTTP POST segment is the 1st segment of the group. Segments 1 to 6 are segment numbers 4, 5, 7, 8, 10 and 11 in this trace respectively. Their sequence numbers are:
   1 -> 1, 2 -> 566, 3 -> 2026, 4 -> 3486, 5 -> 4946 and 6 -> 6406.

The timings of the 6 segments are:

Segment #	Sent Time(Sec)	ACK Received(Sec)	RTT(Sec)
Segment 1	0.026477	0.053937	0.027460
Segment 2	0.041737	0.077294	0.035557
Segment 3	0.054026	0.124085	0.070059
Segment 4	0.054690	0.169118	0.114430
Segment 5	0.077405	0.218299	0.139890
Segment 6	0.078157	0.267802	0.189640

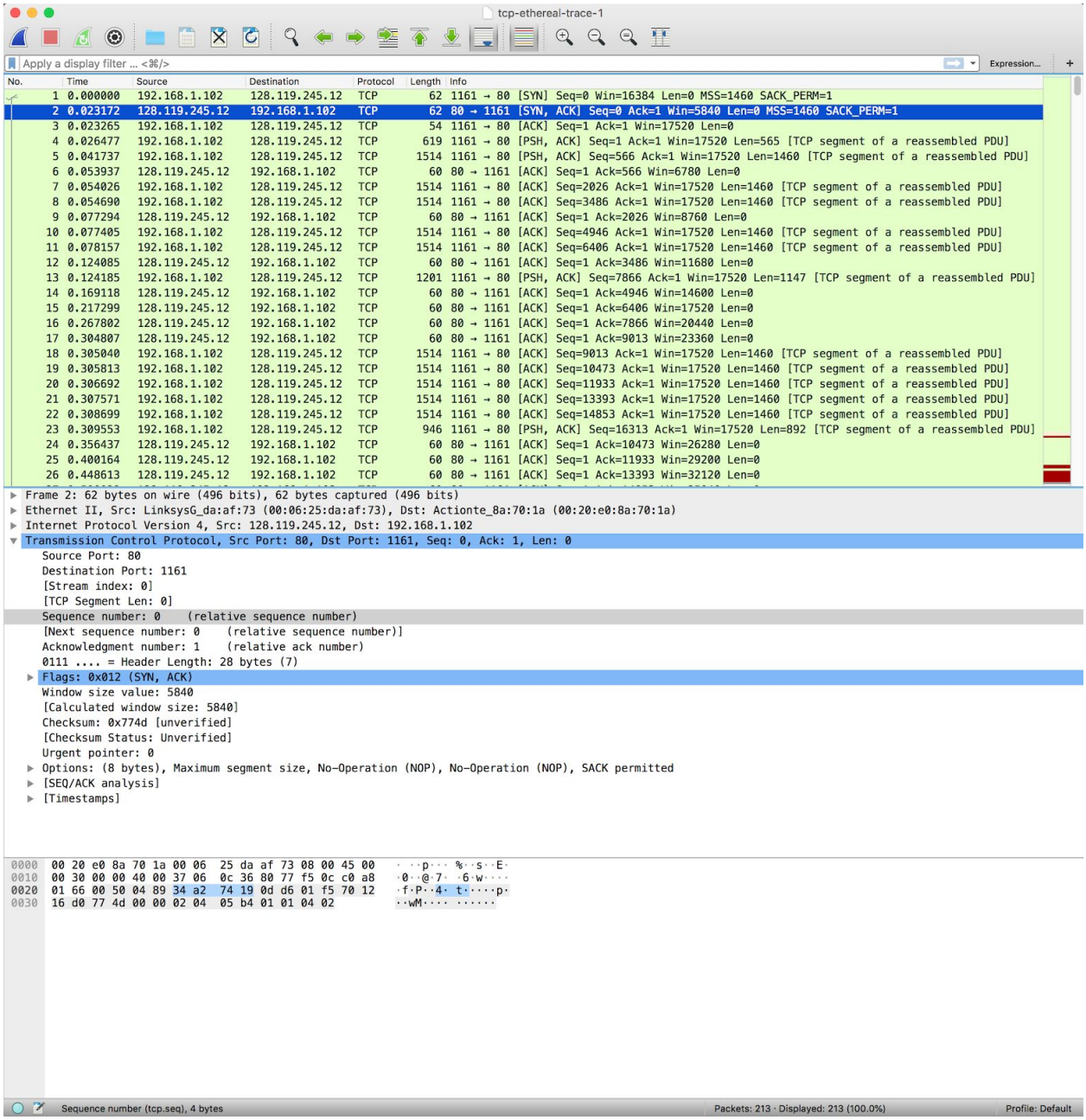
Estimated RTT calculation for segments:

1. Estimated RTT_1 remains the same as RTT for 1st segment = 0.02746s
2. Estimated RTT_2 = 0.875 * 0.02746 + 0.125 * 0.035557 = 0.0285s.
3. Estimated RTT_3 = 0.875 * 0.0285 + 0.125 * 0.070059 = 0.0337s.
4. Estimated RTT_4 = 0.875 * 0.0337 + 0.125 * 0.114430 = 0.0438s.
5. Estimated RTT_5 = 0.875 * 0.0438 + 0.125 * 0.139890 = 0.0558s.
6. Estimated RTT_6 = 0.875 * 0.0558 + 0.125 * 0.189640 = 0.0725s.



6. Length of the first 6 segments:
   1 -> 565 bytes
   2 -> 1460 bytes
   3 -> 1460 bytes
   4 -> 1460 bytes
   5 -> 1460 bytes
   6 -> 1460 bytes
7. The minimum amount of buffer space advertised at the server is 5840 bytes, as seen from the first ACK from the server. The receiver window grows until a maximum receiver

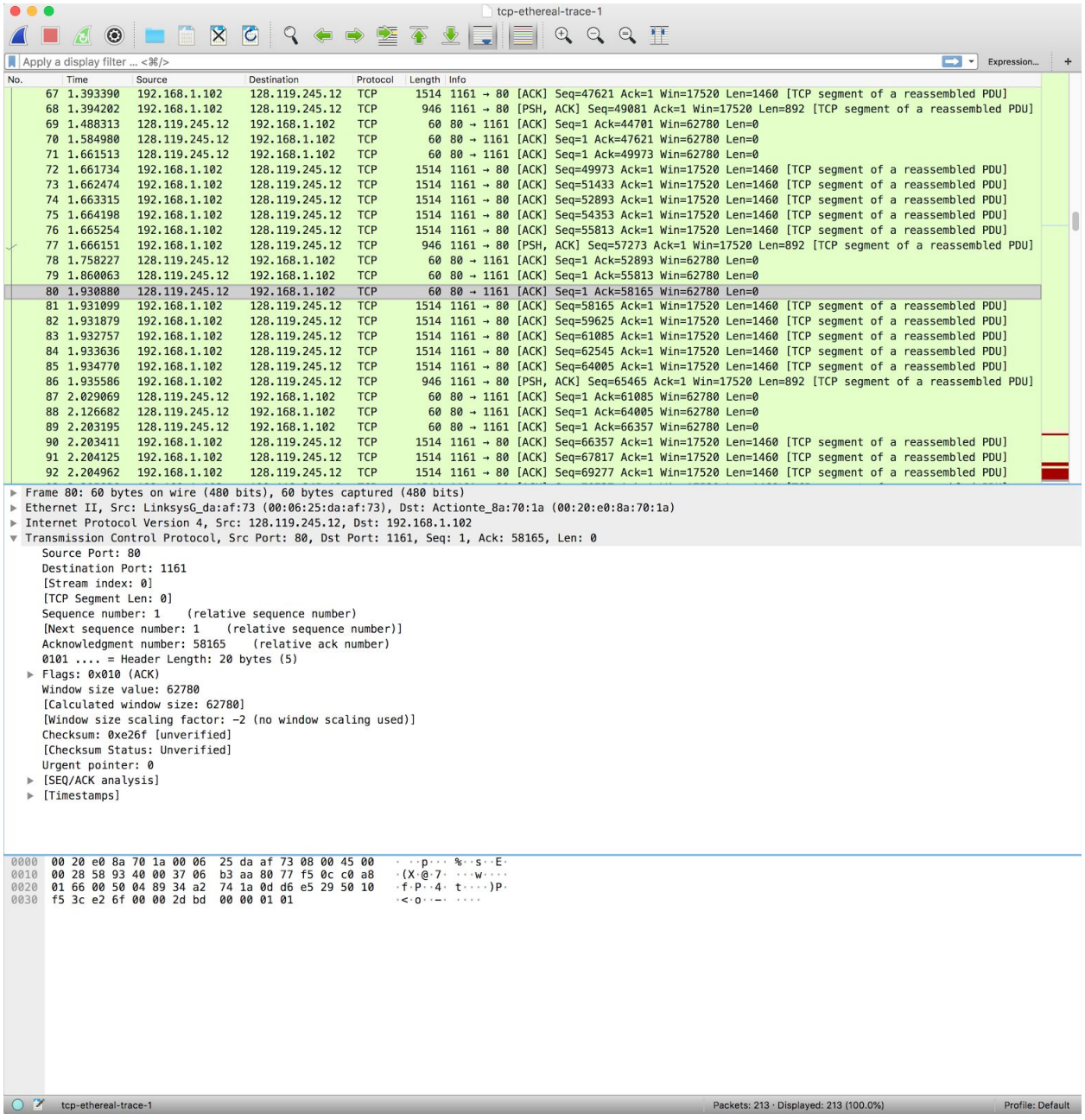
buffer size of 62780 bytes. The sender is never throttled due to lack of receiver buffer space.



8. There are no retransmitted segments in this trace file. We can check for retransmitted segments by checking the sequence numbers of TCP segments in the file. As observed, all sequence numbers increase uniformly with time. If a retransmission had occurred, a sequence number would be out of order, that is, smaller than its neighbouring segments.
9. The difference between the acknowledged sequence numbers of two consecutive ACKs gives the amount of data received by the server between these two ACKs. The acknowledged sequence numbers and their amount is given below:

ACK	ACK Sequence Number	ACK Data
ACK 1	566	566
ACK 2	2026	1460
ACK 3	3486	1460
ACK 4	4946	1460
ACK 5	6406	1460
ACK 6	7866	1460
ACK 7	9013	1147
ACK 8	10473	1460
ACK 9	11933	1460
ACK 10	13393	1460
ACK 11	14853	1460
ACK 12	16313	1460

Segment 80 acknowledged data of 2920 bytes which indicates that the receiver has ACKed every other segment since the receiver usually ACKs data of 1460 bytes.

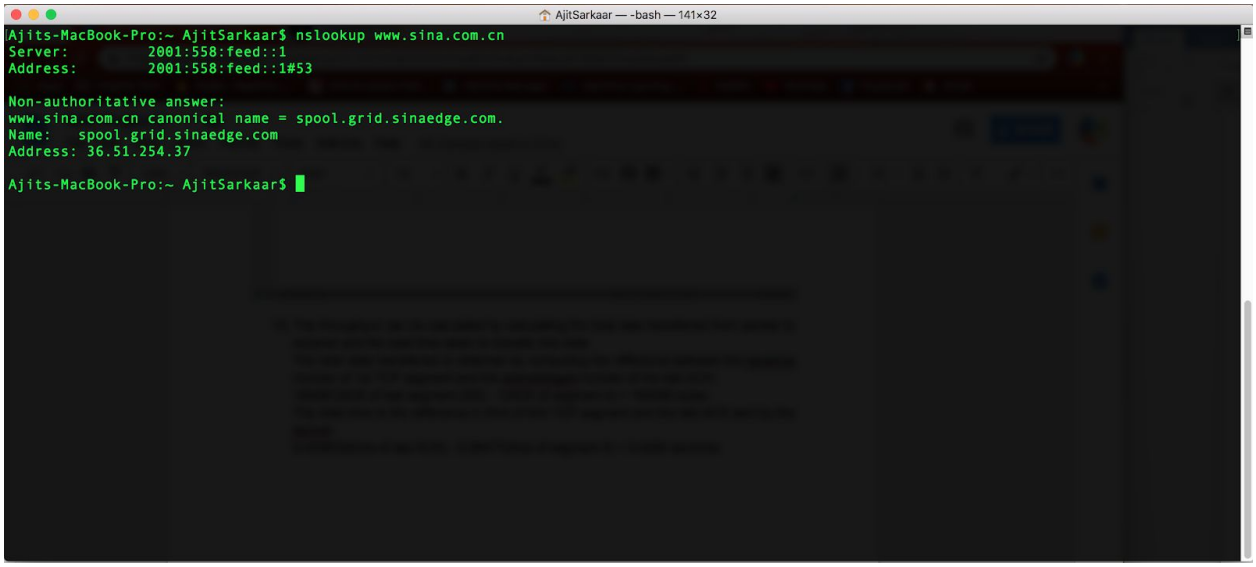


10. The throughput can be calculated by calculating the total data transferred from sender to receiver and the total time taken to transfer this data.
    The total data transferred is obtained by computing the difference between the sequence number of 1st TCP segment and the acknowledged number of the last ACK:
    164091(ACK of last segment 202) - 1(ACK of segment 4) = 164090 bytes.
    The total time is the difference in time of first TCP segment and the last ACK sent by the receiver:
    5.455830(time of last ACK) - 0.26477(time of segment 4) = 5.4292 seconds.

Hence, the throughput for the TCP connection is:
164090/5.4292 = 30.333KBytes/seconds.

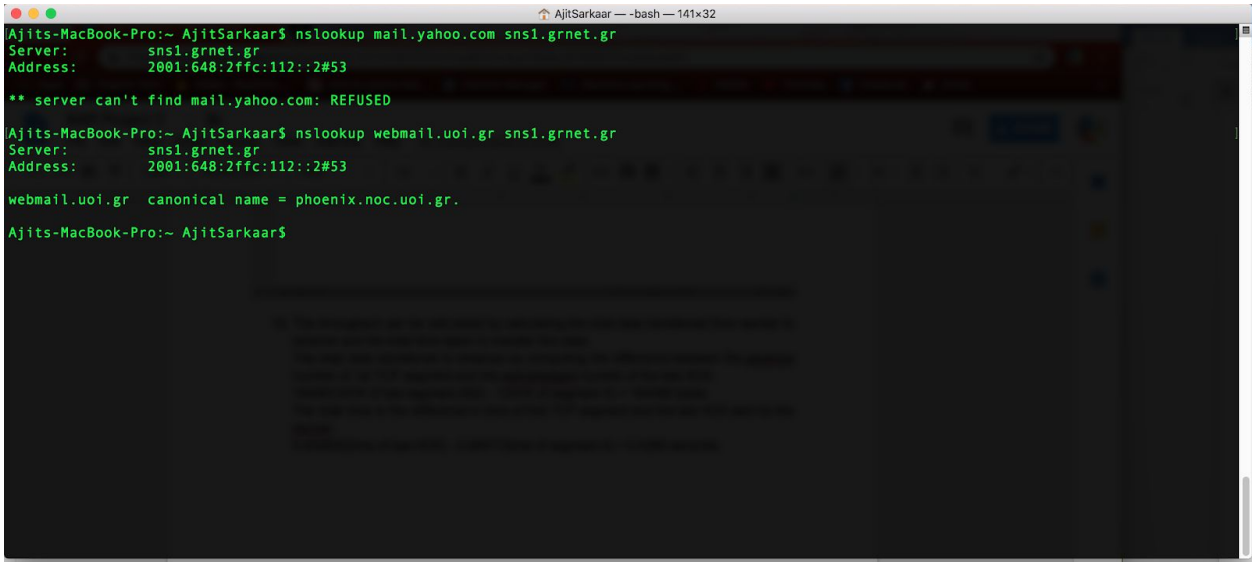
PART 2.3

1. After running the command nslookup www.sina.com.cn, the IP address of the web server www.sina.com.cn is: 36.51.254.37

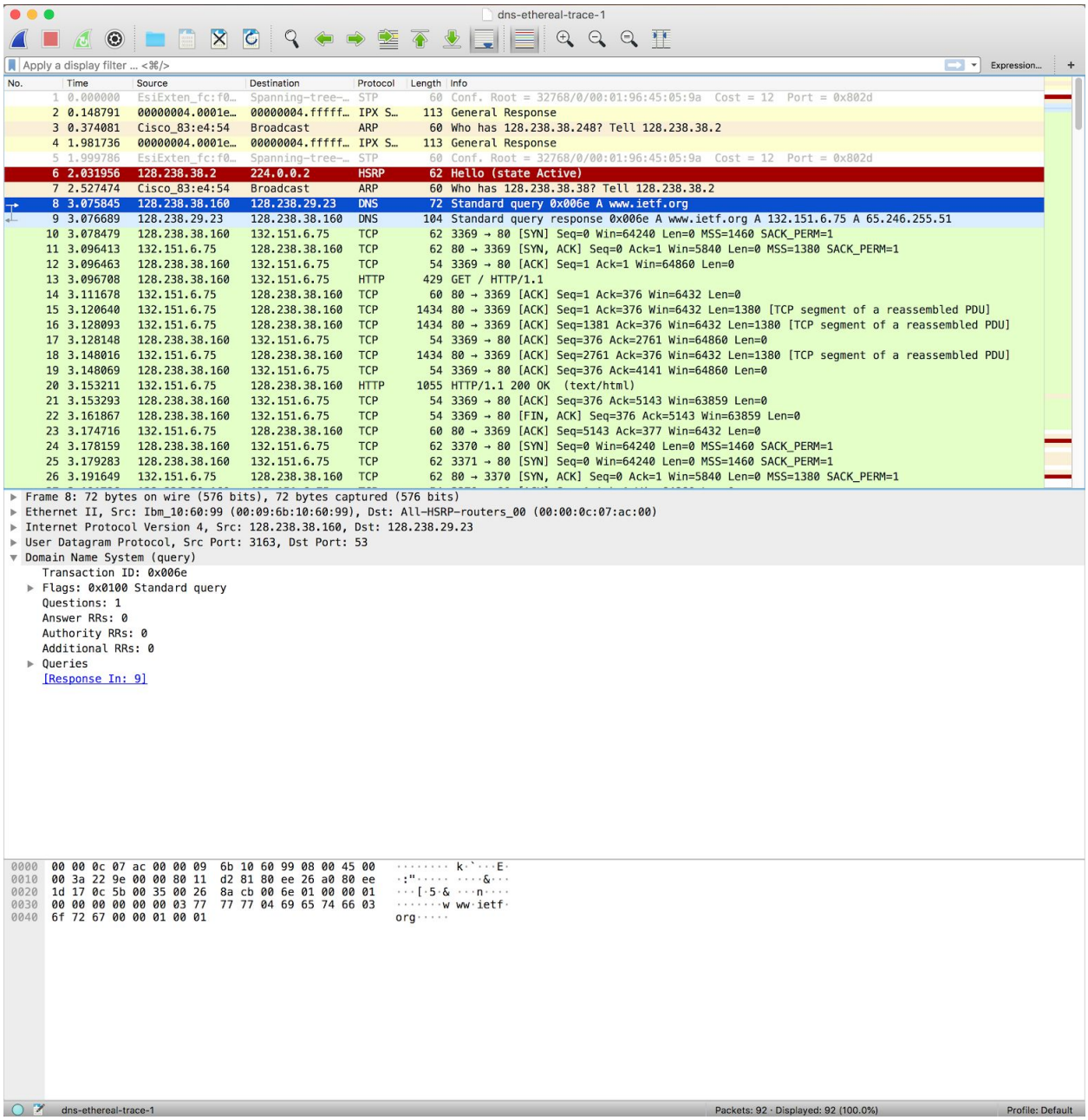


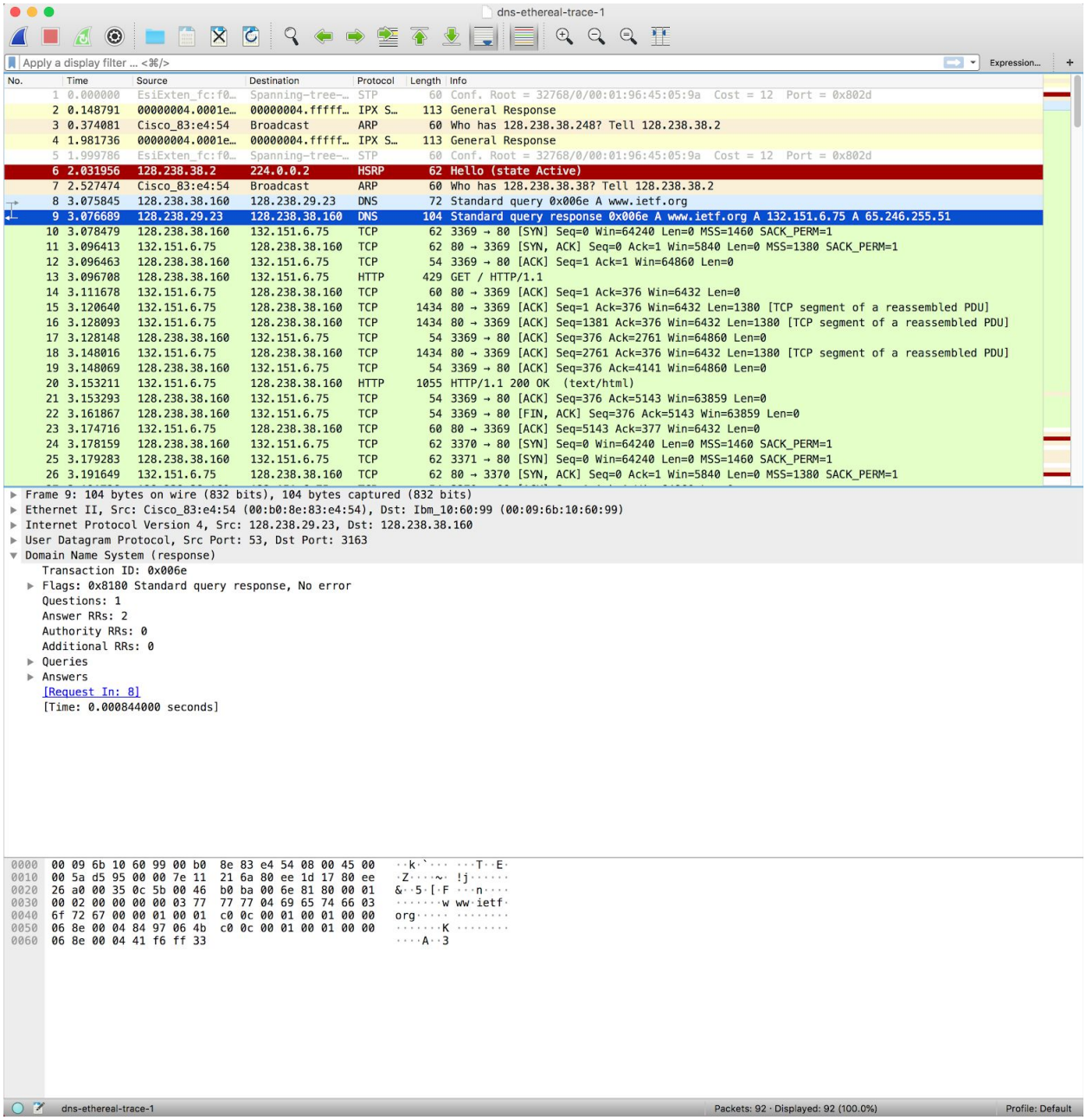
2. After running the command nslookup -type=NS uoi.gr, the authoritative DNS servers for University of Ioannina in Greece are given below: sns1.grnet.gr 83.212.5.22

3. Running the command nslookup mail.yahoo.com sns1.grnet.gr, the server cant find the address of the mail server due to security rules, and refuses the connection as shown below. After trying to query the authoritative DNS servers of uoi.gr, of the domain name webmail.uoi.gr, the canonical name for the mail server is returned as shown below:

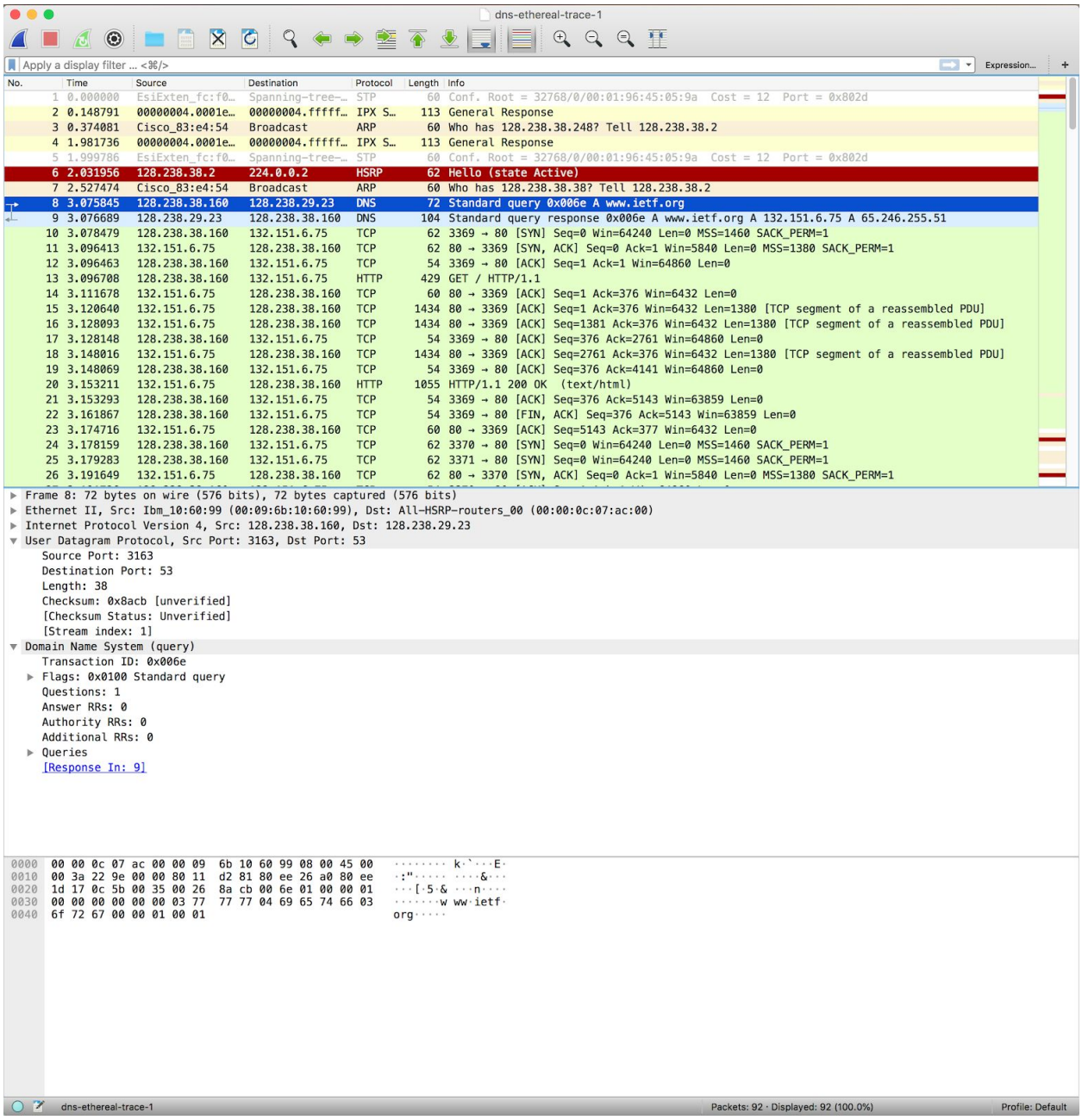


4. They are sent over UDP.

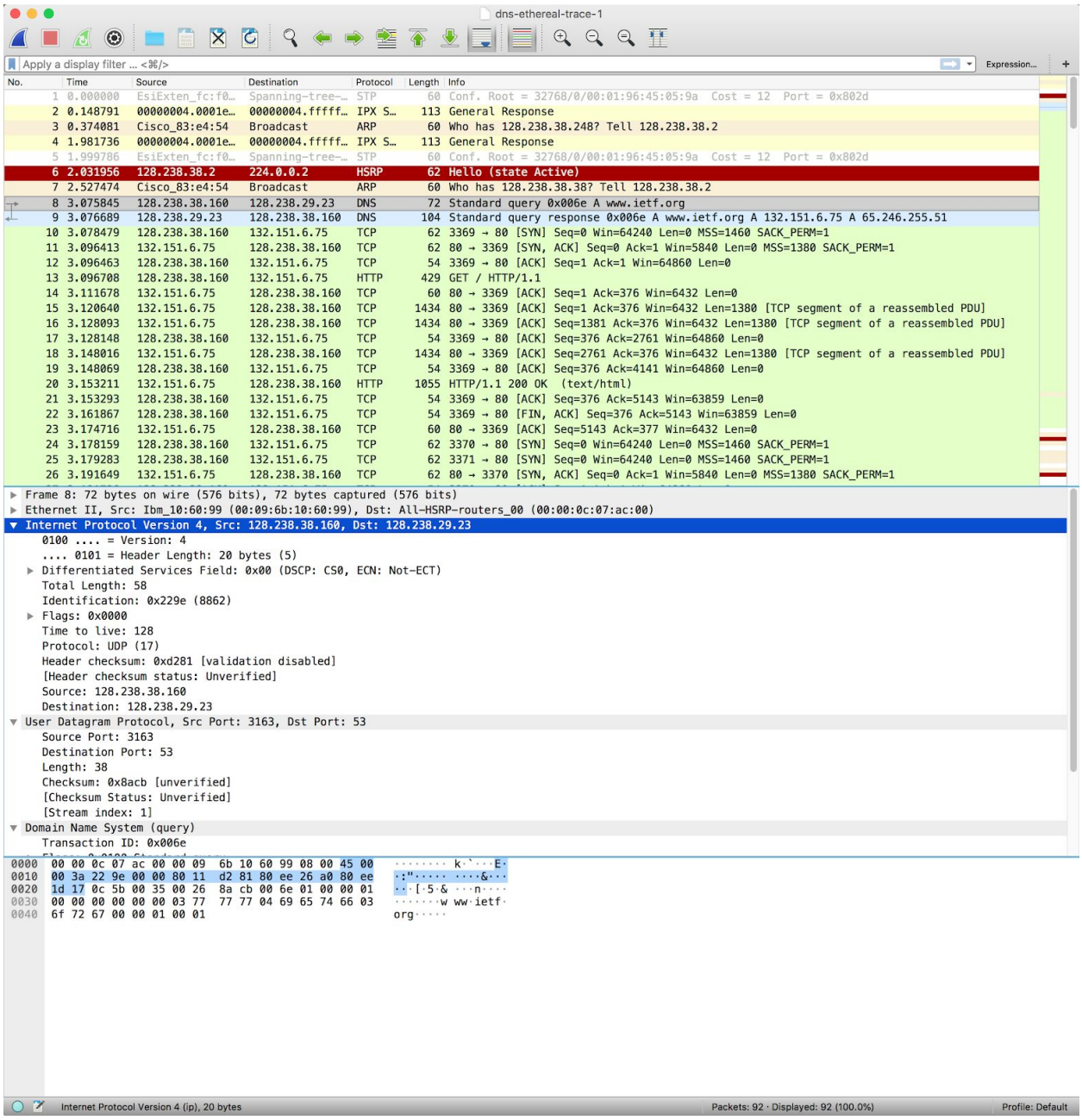

dns-ethereal-trace-1
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 EsiExten_fc:f0… Spanning-tree-… STP 60 Conf. Root = 32768/0/00:01:96:45:05:9a Cost = 12 Port = 0x802d
2 0.148791 00000004.0001e… 00000004.fffff… IPX S… 113 General Response
3 0.374081 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.248? Tell 128.238.38.2
4 1.981736 00000004.0001e… 00000004.fffff… IPX S… 113 General Response
5 1.999786 EsiExten_fc:f0… Spanning-tree-… STP 60 Conf. Root = 32768/0/00:01:96:45:05:9a Cost = 12 Port = 0x802d
6 2.031956 128.238.38.2 224.0.0.2 HSRP 62 Hello (state Active)
7 2.527474 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.38? Tell 128.238.38.2
8 3.075845 128.238.38.160 128.238.29.23 DNS 72 Standard query 0x006e A www.ietf.org
9 3.076689 128.238.29.23 128.238.38.160 DNS 104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
10 3.078479 128.238.38.160 132.151.6.75 TCP 62 3369 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
11 3.096413 132.151.6.75 128.238.38.160 TCP 62 80 → 3369 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
12 3.096463 128.238.38.160 132.151.6.75 TCP 54 3369 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
13 3.096708 128.238.38.160 132.151.6.75 HTTP 429 GET / HTTP/1.1
14 3.111678 132.151.6.75 128.238.38.160 TCP 60 80 → 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=0
15 3.120640 132.151.6.75 128.238.38.160 TCP 1434 80 → 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
16 3.128093 132.151.6.75 128.238.38.160 TCP 1434 80 → 3369 [ACK] Seq=1381 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
17 3.128148 128.238.38.160 132.151.6.75 TCP 54 3369 → 80 [ACK] Seq=376 Ack=2761 Win=64860 Len=0
18 3.148016 132.151.6.75 128.238.38.160 TCP 1434 80 → 3369 [ACK] Seq=2761 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PDU]
19 3.148069 128.238.38.160 132.151.6.75 TCP 54 3369 → 80 [ACK] Seq=376 Ack=4141 Win=64860 Len=0
20 3.153211 132.151.6.75 128.238.38.160 HTTP 1055 HTTP/1.1 200 OK (text/html)
21 3.153293 128.238.38.160 132.151.6.75 TCP 54 3369 → 80 [ACK] Seq=376 Ack=5143 Win=63859 Len=0
22 3.161867 128.238.38.160 132.151.6.75 TCP 54 3369 → 80 [FIN, ACK] Seq=376 Ack=5143 Win=63859 Len=0
23 3.174716 132.151.6.75 128.238.38.160 TCP 60 80 → 3369 [ACK] Seq=5143 Ack=377 Win=6432 Len=0
24 3.178159 128.238.38.160 132.151.6.75 TCP 62 3370 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
25 3.179283 128.238.38.160 132.151.6.75 TCP 62 3371 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
26 3.191649 132.151.6.75 128.238.38.160 TCP 62 80 → 3370 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
User Datagram Protocol, Src Port: 3163, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x006e
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 9]
0000 00 00 0c 07 ac 00 00 09 6b 10 60 99 08 00 45 00 .... k.`...E.
0010 00 3a 22 9e 00 00 80 11 d2 81 80 ee 26 a0 80 ee .:"..... ....&...
0020 1d 17 0c 5b 00 35 00 26 8a cb 00 6e 01 00 00 01 ...[.5.& ...n....
0030 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03 ....w ww.ietf.
0040 6f 72 67 00 00 01 00 01 org.....
dns-ethereal-trace-1
Packets: 92 · Displayed: 92 (100.0%)
Profile: Default



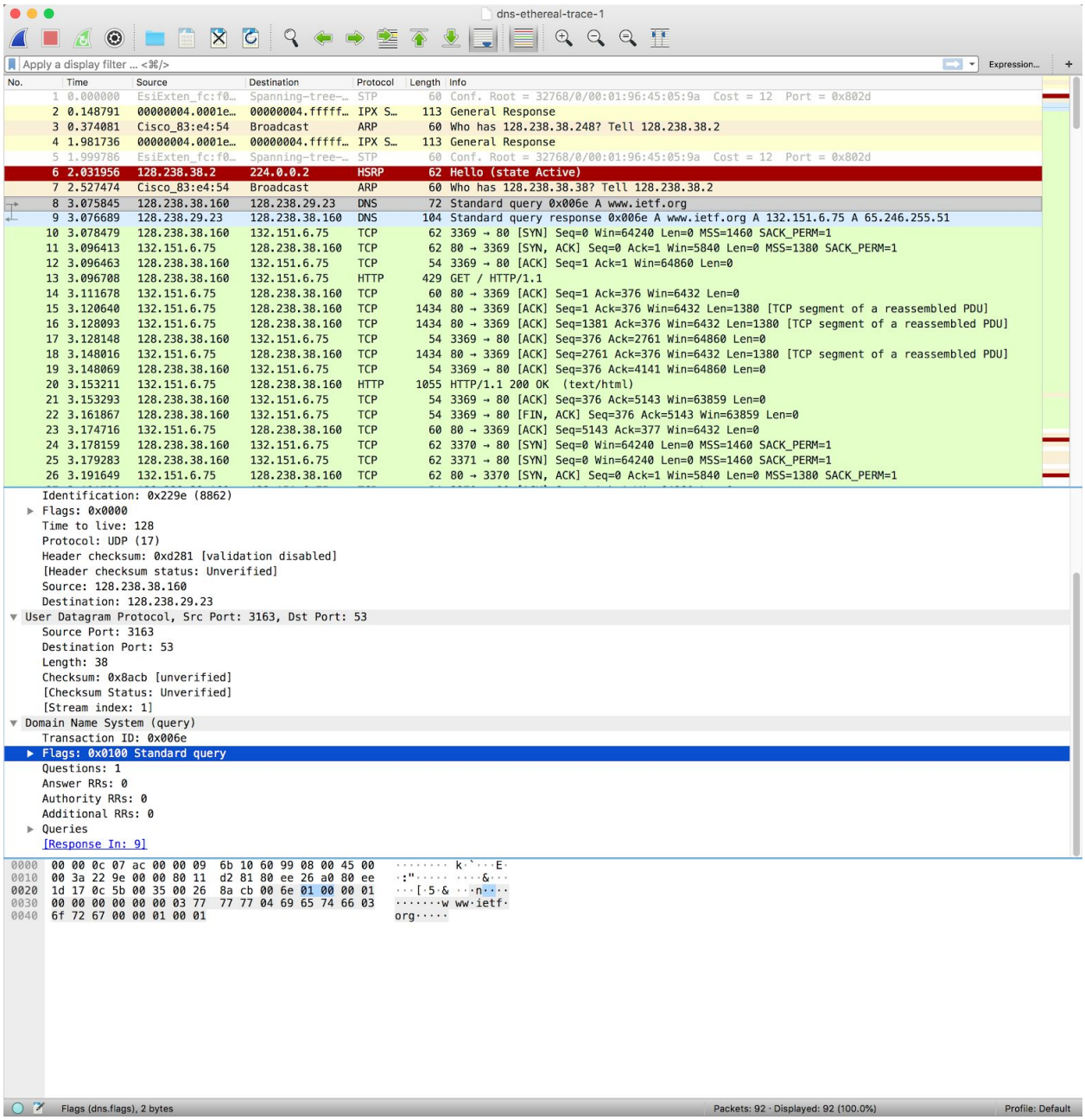
5. The destination port for the DNS query is 53 and the source port of the DNS response is 53.



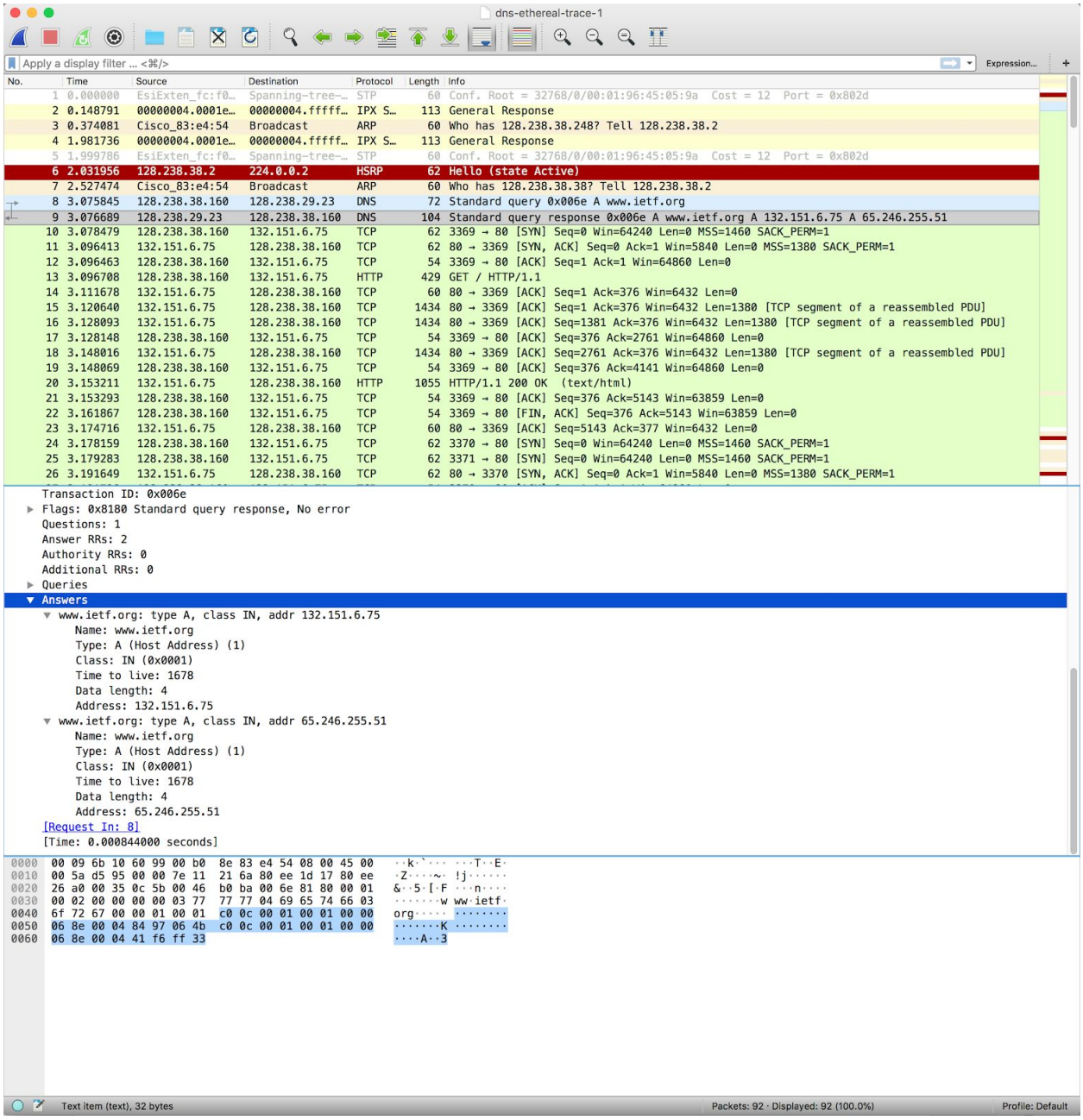
6. The DNS query message is sent to the IP address: 128.238.29.23
   The IP address of the DNS server of the local host is: 128.238.29.23



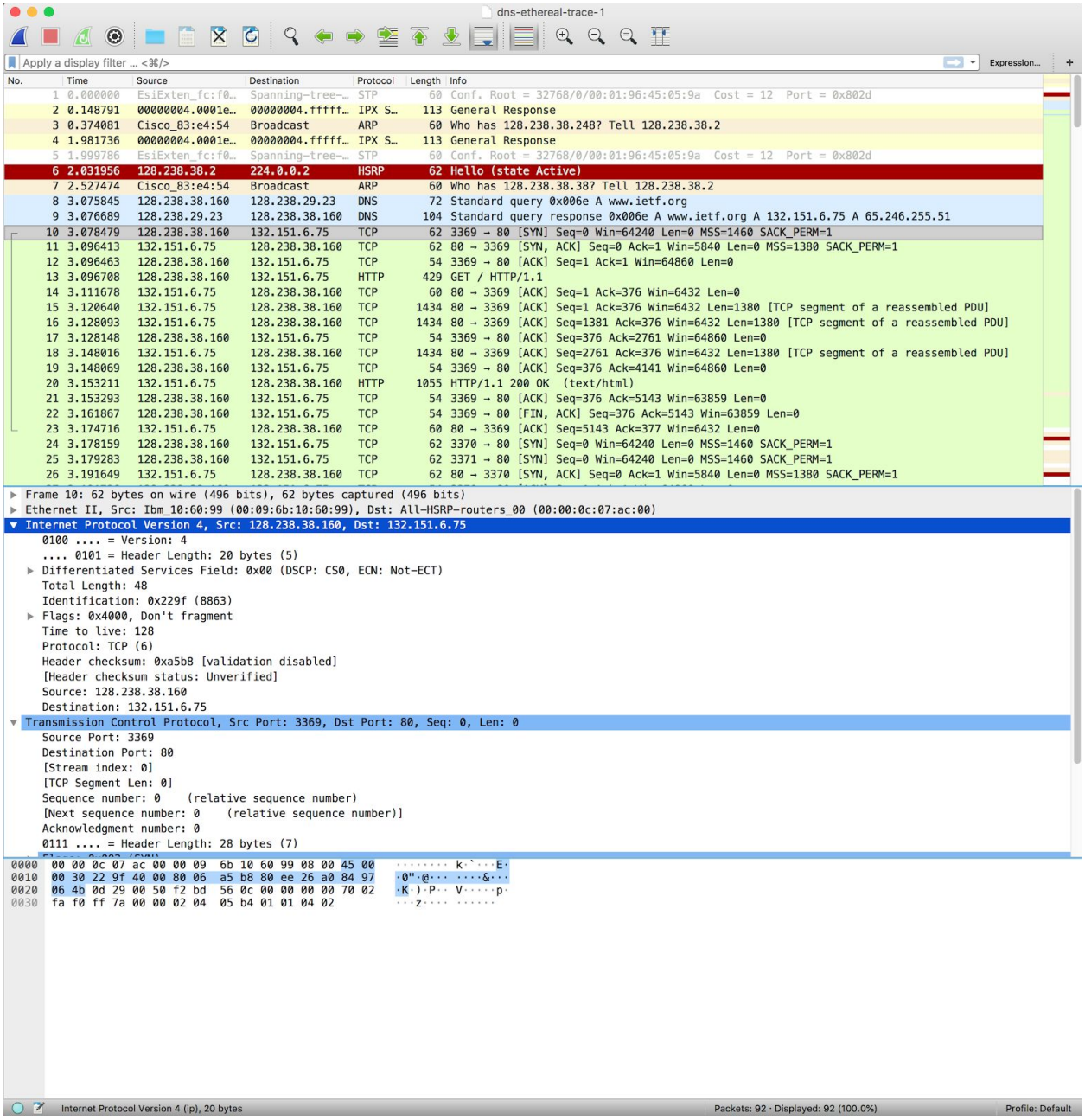
7. The query is a Standard type A query. The query message does not contain any answers.



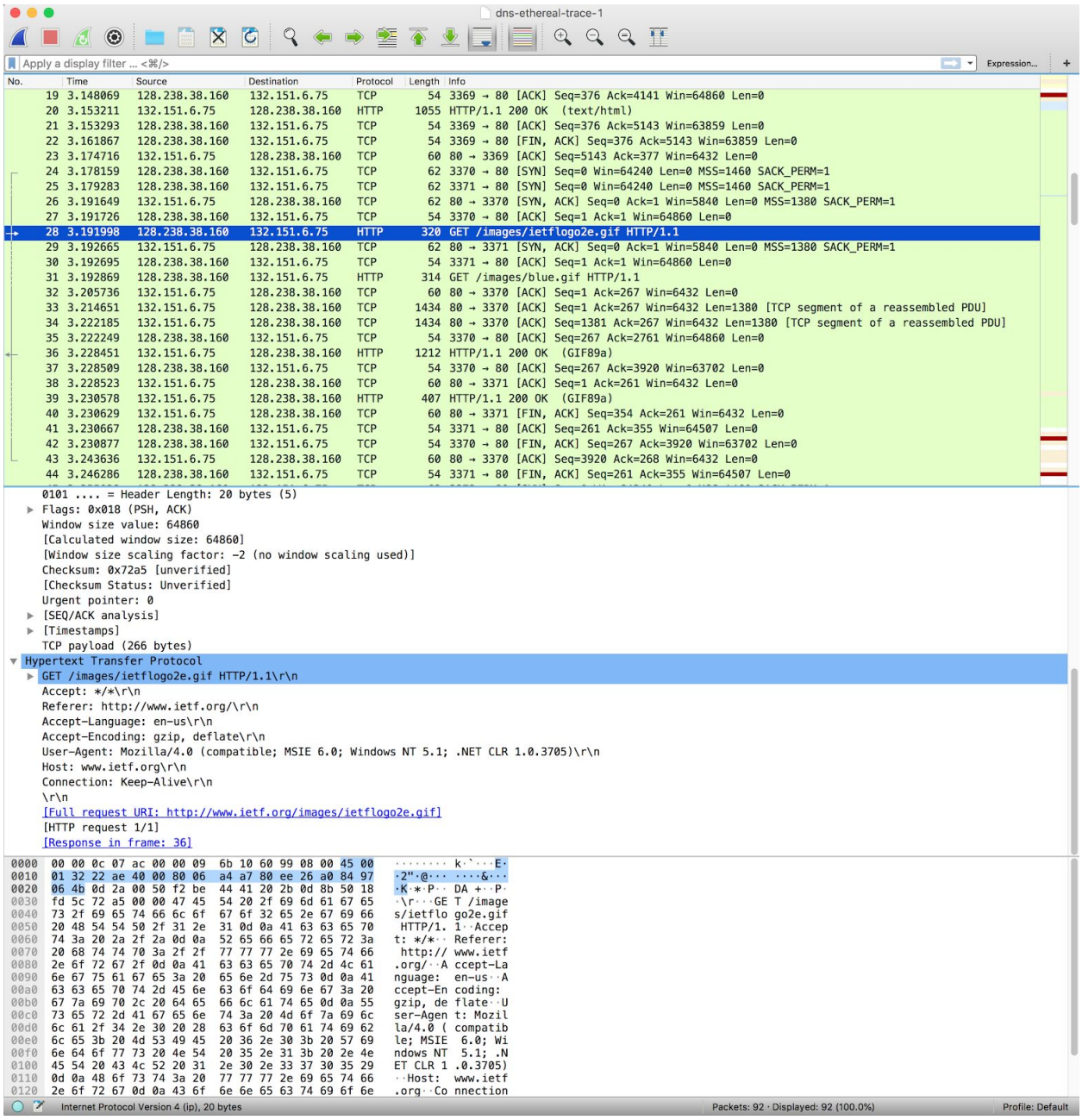
8. There are 2 answers provided. The answers contain information about the name of host, type of address, the class, the TTL, data length and the IP address.



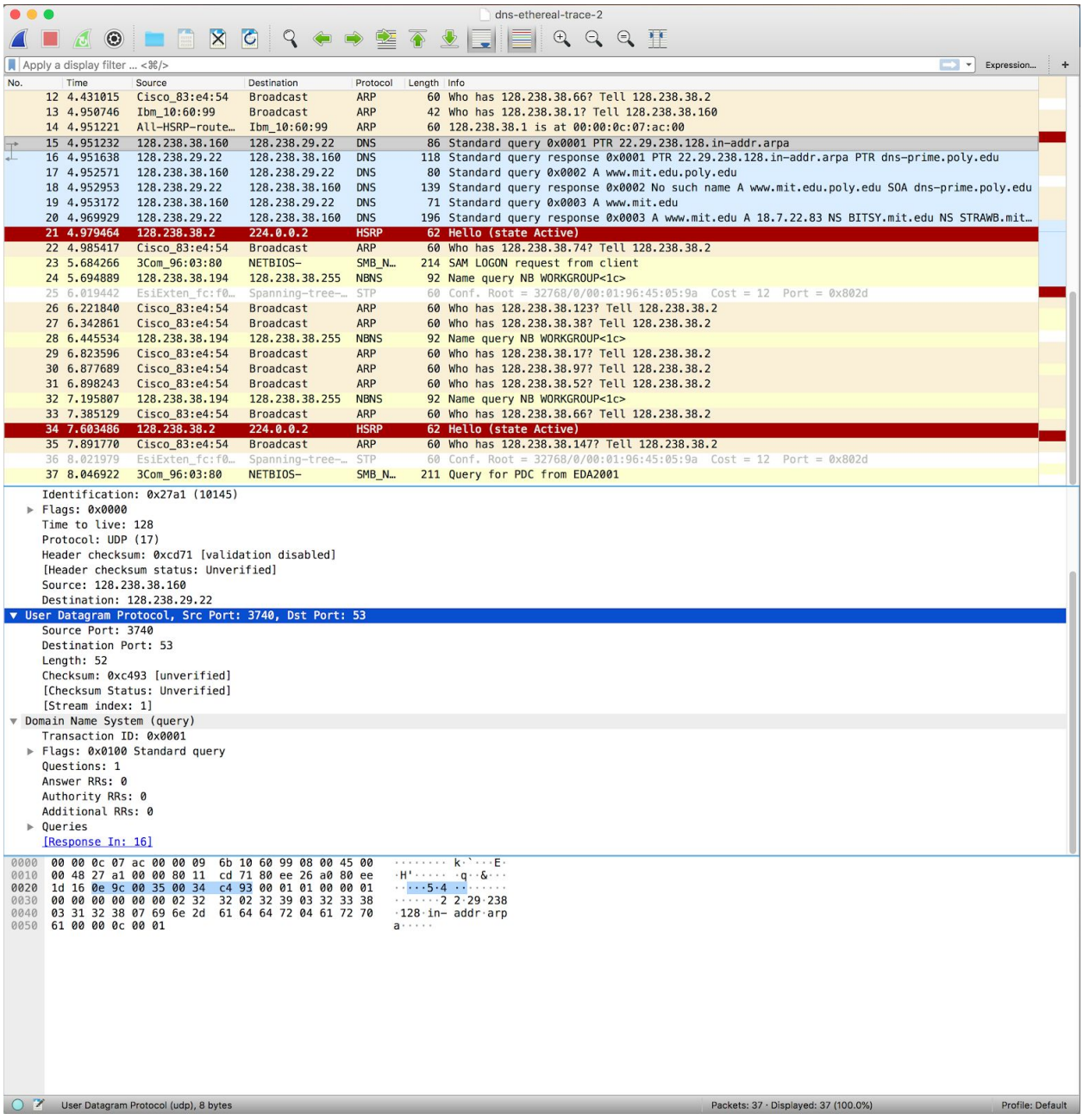
9. The first SYN packet is sent to 132.151.6.75 which corresponds to the first IP address provided in the DNS response message.

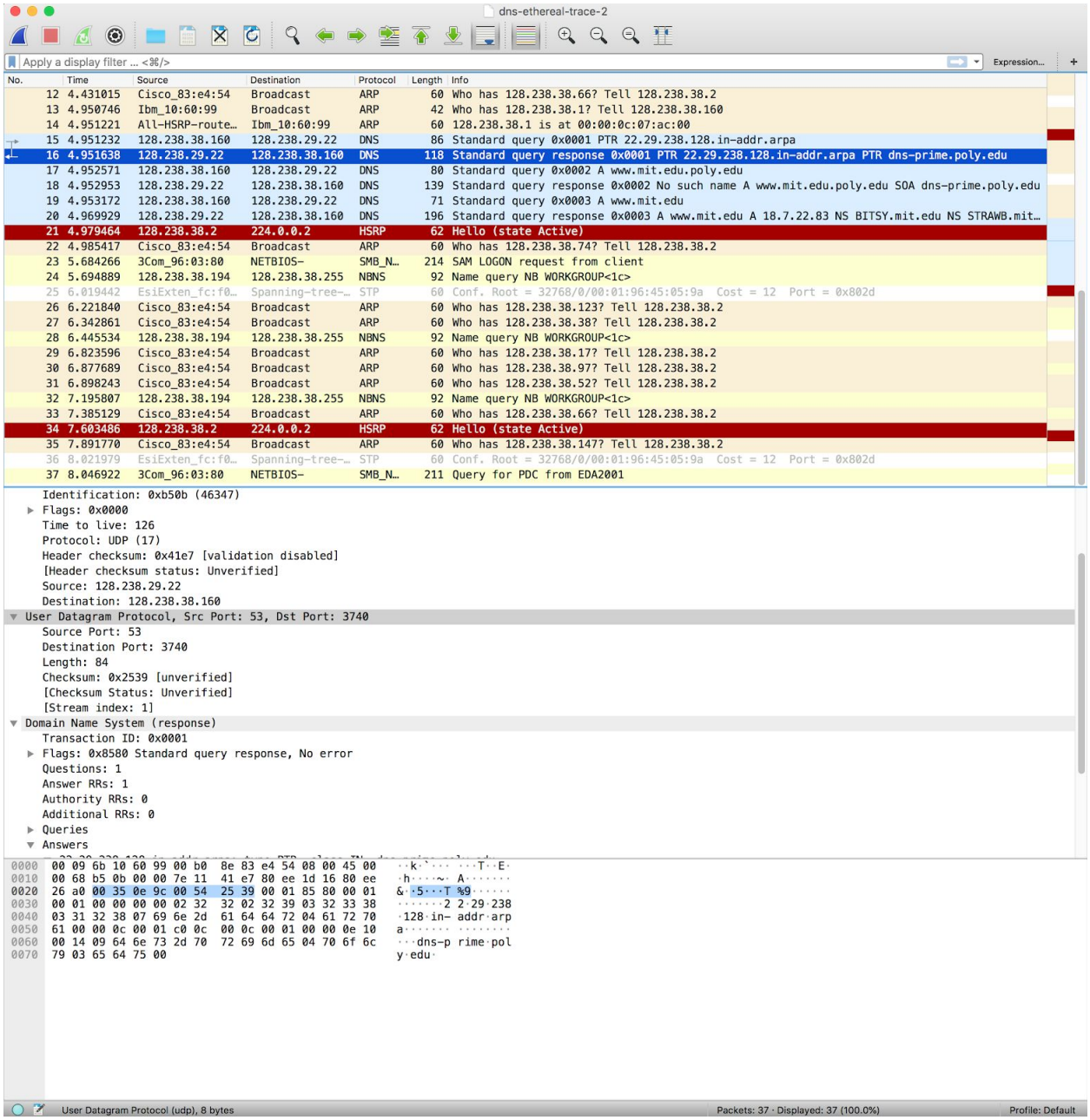


10. No, new DNS queries are not issued before retrieving each image.

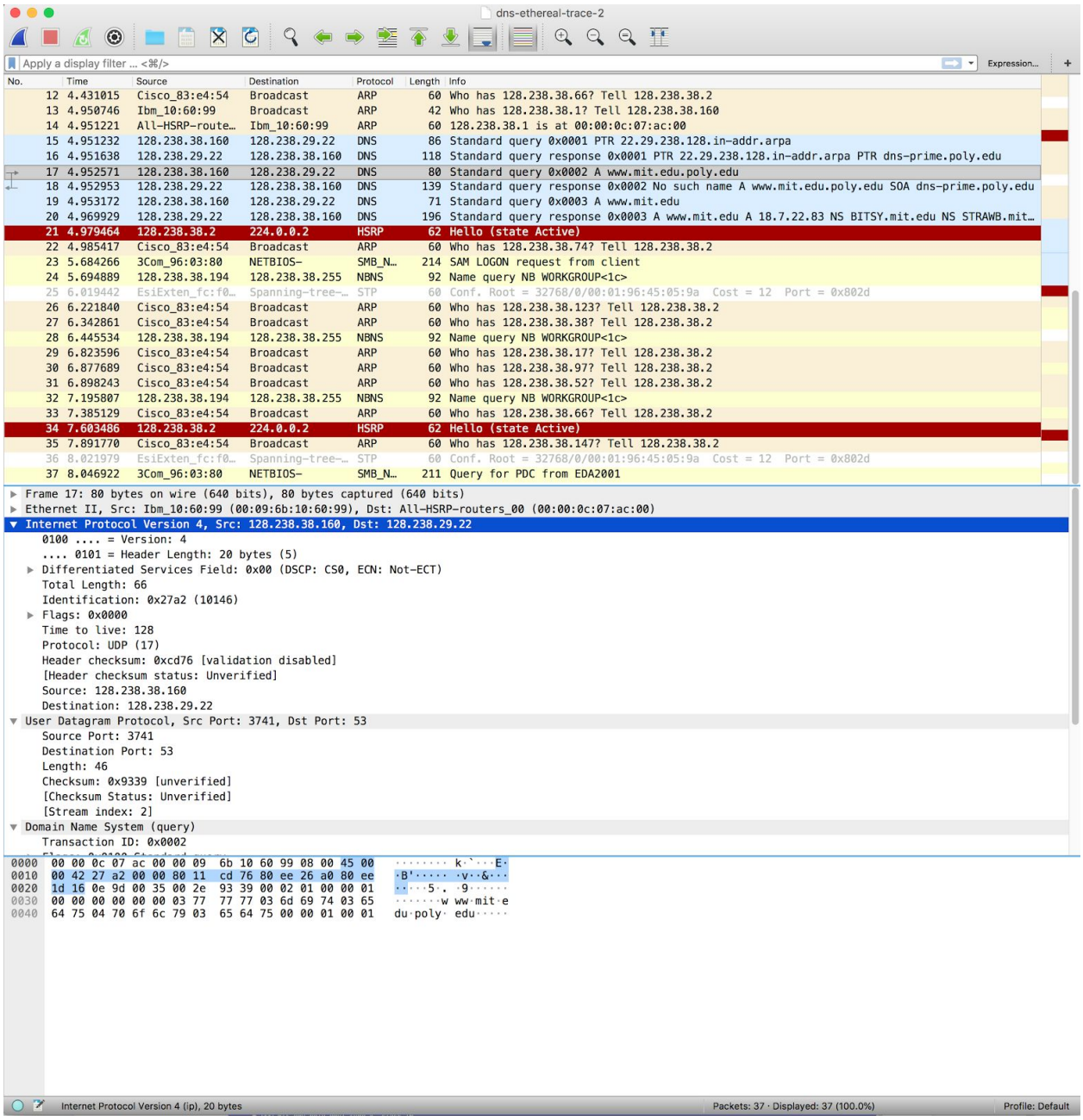


11. The destination port of the DNS query is 53 and the source port of the response is 53.

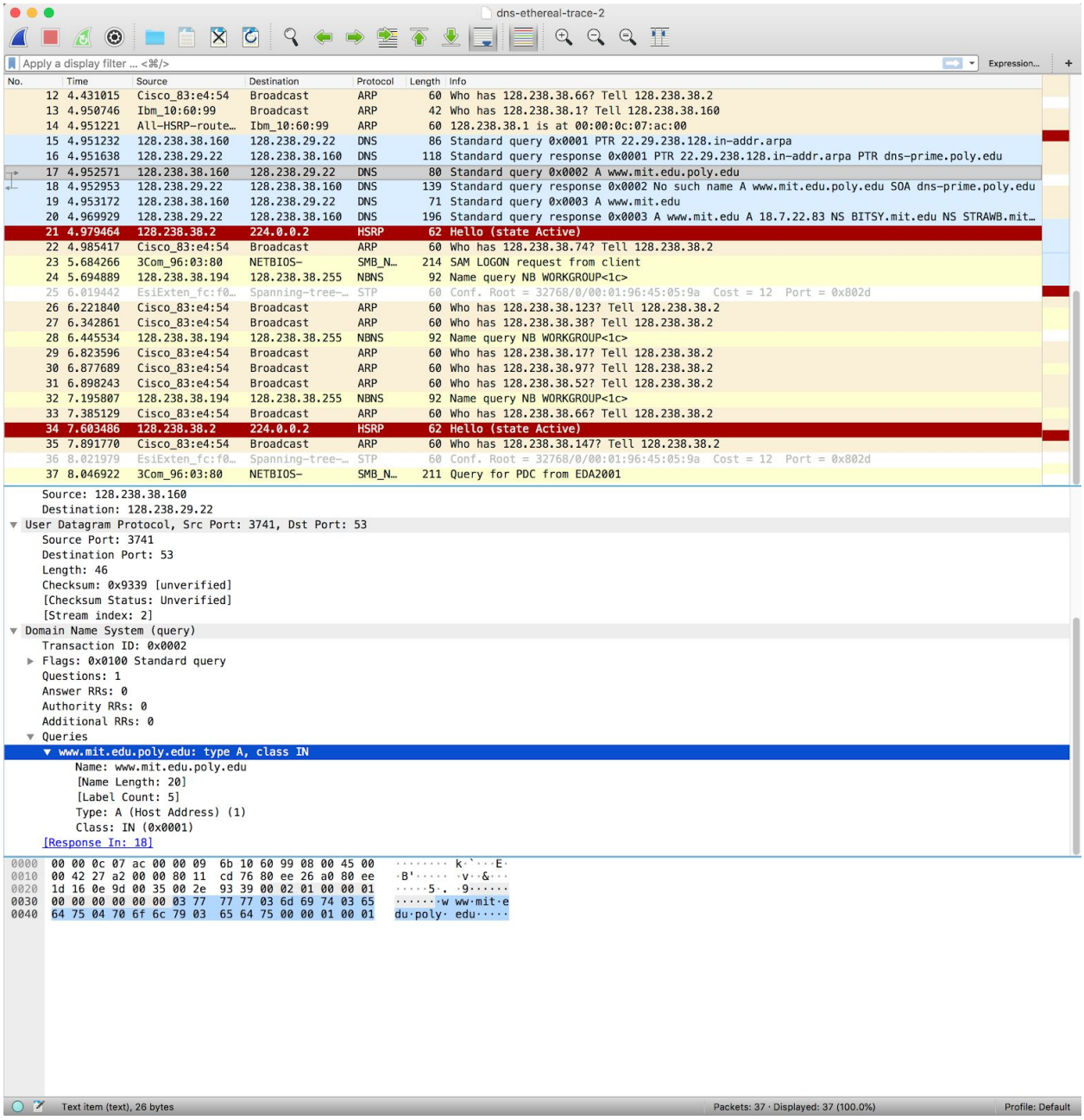

dns-ethereal-trace-2
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
12 4.431015 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.66? Tell 128.238.38.2
13 4.950746 Ibm_10:60:99 Broadcast ARP 42 Who has 128.238.38.1? Tell 128.238.38.160
14 4.951221 All-HSRP-route… Ibm_10:60:99 ARP 60 128.238.38.1 is at 00:00:0c:07:ac:00
15 4.951232 128.238.38.160 128.238.29.22 DNS 86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
16 4.951638 128.238.29.22 128.238.38.160 DNS 118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
17 4.952571 128.238.38.160 128.238.29.22 DNS 80 Standard query 0x0002 A www.mit.edu.poly.edu
18 4.952953 128.238.29.22 128.238.38.160 DNS 139 Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly.edu
19 4.953172 128.238.38.160 128.238.29.22 DNS 71 Standard query 0x0003 A www.mit.edu
20 4.969929 128.238.29.22 128.238.38.160 DNS 196 Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.mit…
21 4.979464 128.238.38.2 224.0.0.2 HSRP 62 Hello (state Active)
22 4.985417 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.74? Tell 128.238.38.2
23 5.684266 3Com_96:03:80 NETBIOS- SMB_N… 214 SAM LOGON request from client
24 5.694889 128.238.38.194 128.238.38.255 NBNS 92 Name query NB WORKGROUP<1c>
25 6.019442 EsiExten_fc:f0… Spanning-tree-… STP 60 Conf. Root = 32768/0/00:01:96:45:05:9a Cost = 12 Port = 0x802d
26 6.221840 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.123? Tell 128.238.38.2
27 6.342861 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.38? Tell 128.238.38.2
28 6.445534 128.238.38.194 128.238.38.255 NBNS 92 Name query NB WORKGROUP<1c>
29 6.823596 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.17? Tell 128.238.38.2
30 6.877689 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.97? Tell 128.238.38.2
31 6.898243 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.52? Tell 128.238.38.2
32 7.195807 128.238.38.194 128.238.38.255 NBNS 92 Name query NB WORKGROUP<1c>
33 7.385129 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.66? Tell 128.238.38.2
34 7.603486 128.238.38.2 224.0.0.2 HSRP 62 Hello (state Active)
35 7.891770 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.147? Tell 128.238.38.2
36 8.021979 EsiExten_fc:f0… Spanning-tree-… STP 60 Conf. Root = 32768/0/00:01:96:45:05:9a Cost = 12 Port = 0x802d
37 8.046922 3Com_96:03:80 NETBIOS- SMB_N… 211 Query for PDC from EDA2001
Identification: 0x27a1 (10145)
Flags: 0x0000
Time to live: 128
Protocol: UDP (17)
Header checksum: 0xcd71 [validation disabled]
[Header checksum status: Unverified]
Source: 128.238.38.160
Destination: 128.238.29.22
User Datagram Protocol, Src Port: 3740, Dst Port: 53
Source Port: 3740
Destination Port: 53
Length: 52
Checksum: 0xc493 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
Domain Name System (query)
Transaction ID: 0x0001
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 16]
0000 00 00 0c 07 ac 00 00 09 6b 10 60 99 08 00 45 00 .... k.`...E.
0010 00 48 27 a1 00 00 80 11 cd 71 80 ee 26 a0 80 ee .H'..... .q..&...
0020 1d 16 0e 9c 00 35 00 34 c4 93 00 01 01 00 00 01 .....5.4 ....
0030 00 00 00 00 00 00 02 32 32 02 32 39 03 32 33 38 ....2 2.29.238
0040 03 31 32 38 07 69 6e 2d 61 64 64 72 04 61 72 70 .128.in- addr.arp
0050 61 00 00 0c 00 01 a.....
User Datagram Protocol (udp), 8 bytes
Packets: 37 · Displayed: 37 (100.0%)
Profile: Default



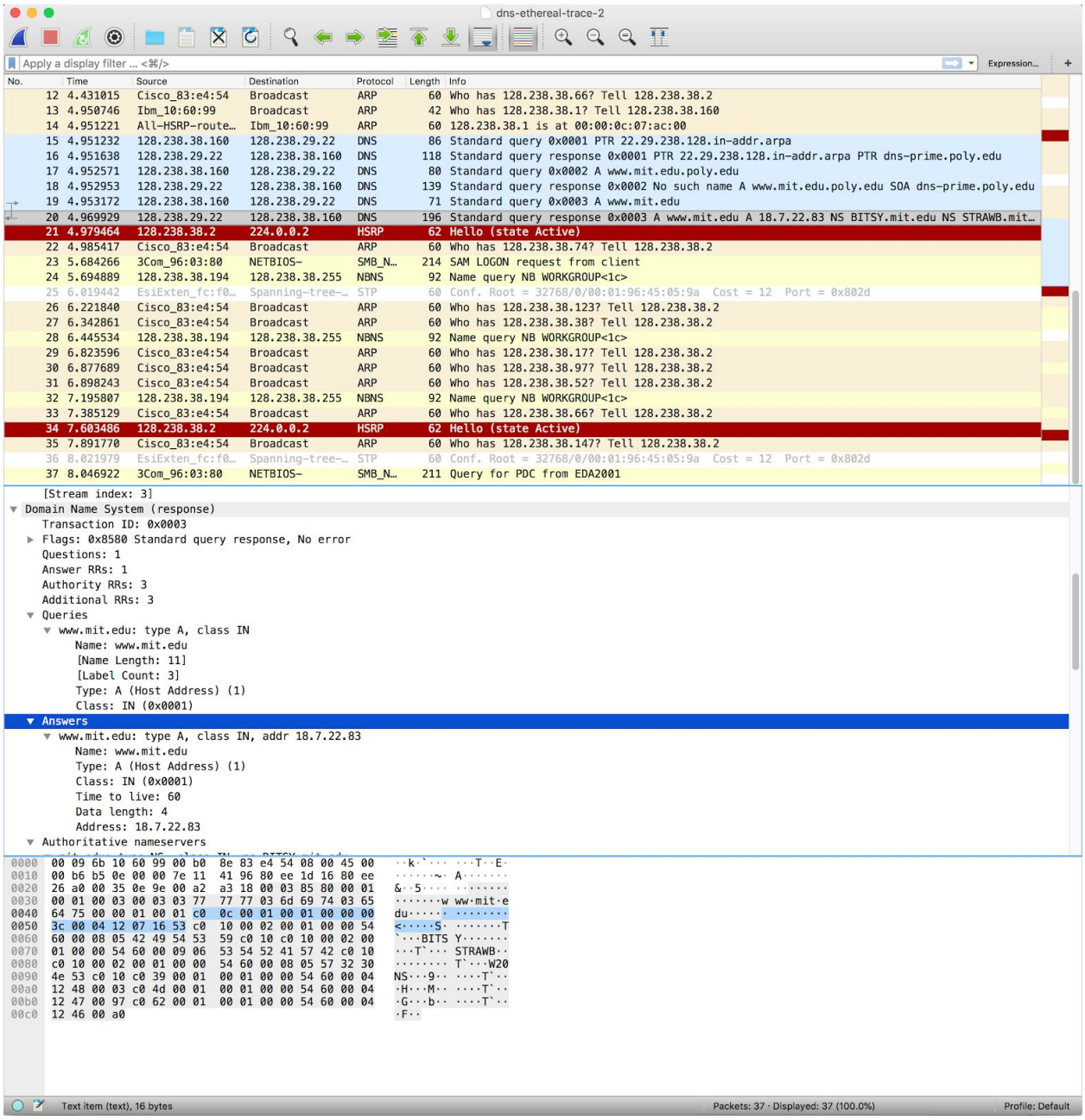
12. The DNS query message is sent to IP address: 128.238.29.22. This is the IP address of the local default DNS server.



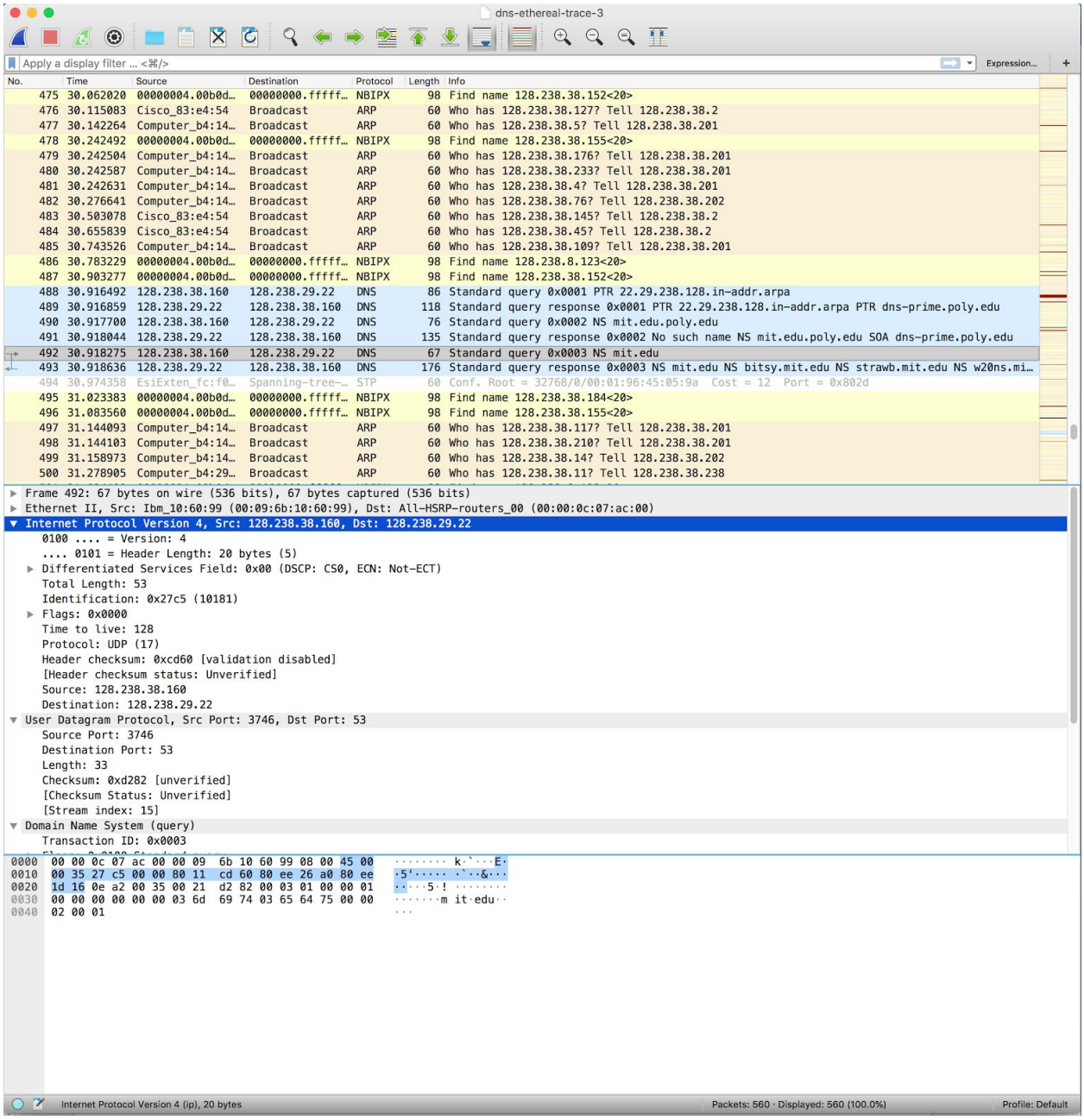
13. The query is of type A. It does not contain any answers.



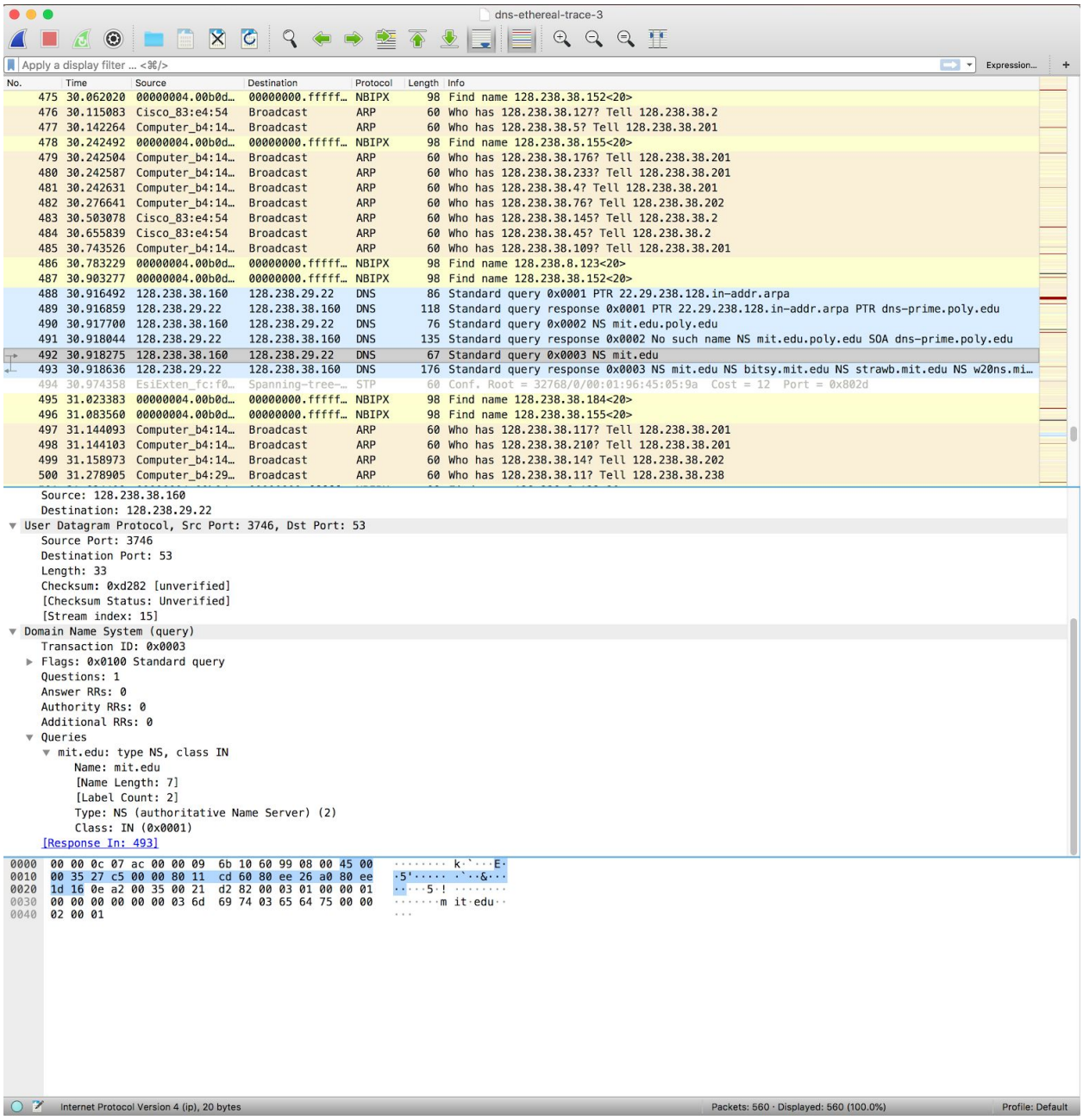
14. There is only 1 answer provided. The answer contains information about the name of host, type of address, the class, the TTL, data length and the IP address.



15. The DNS query message is sent to the IP address: 128.238.29.22 This is the IP address of the local default DNS server.



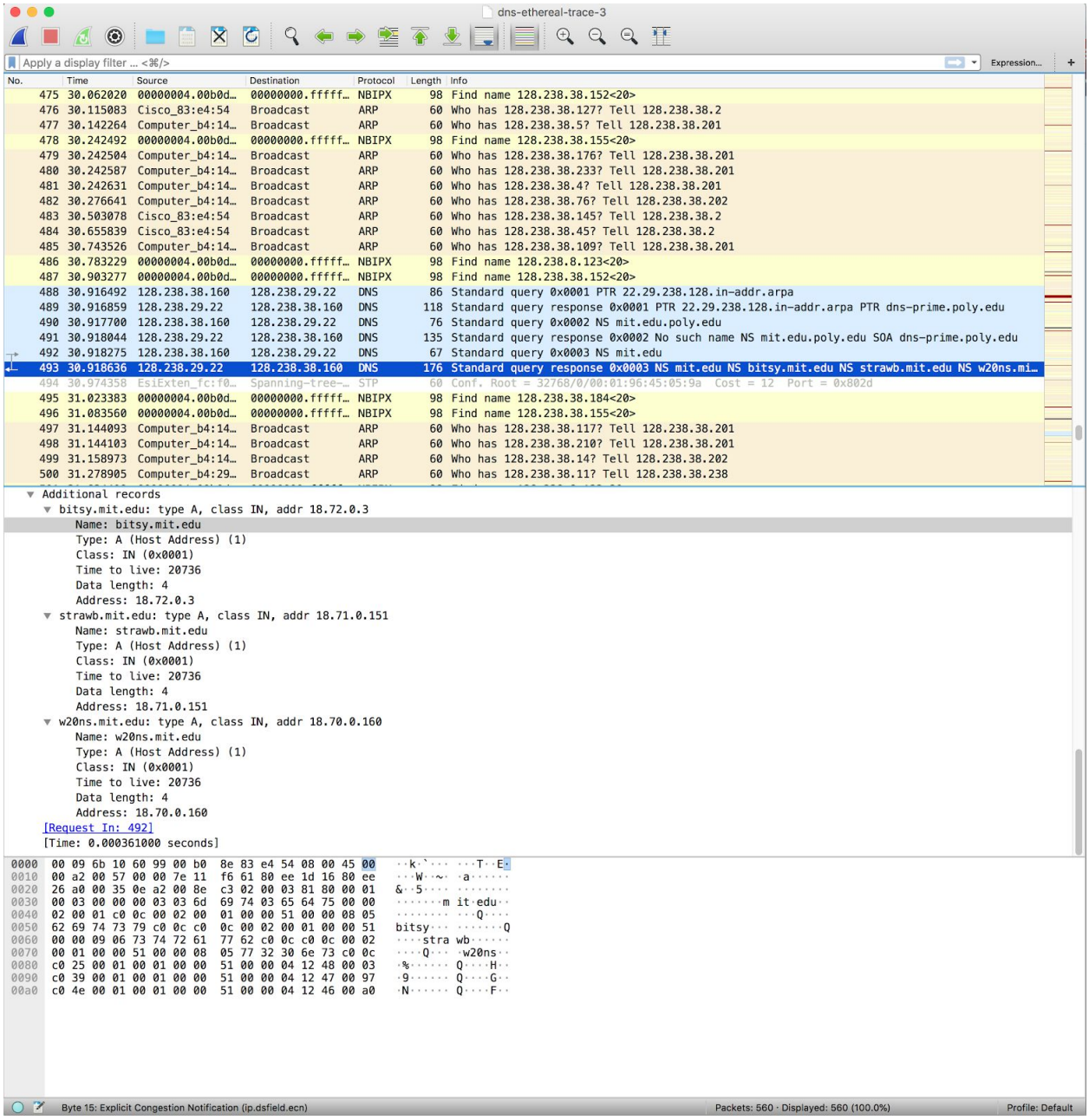
16. It's a type NS DNS query that doesn't contain any answers.



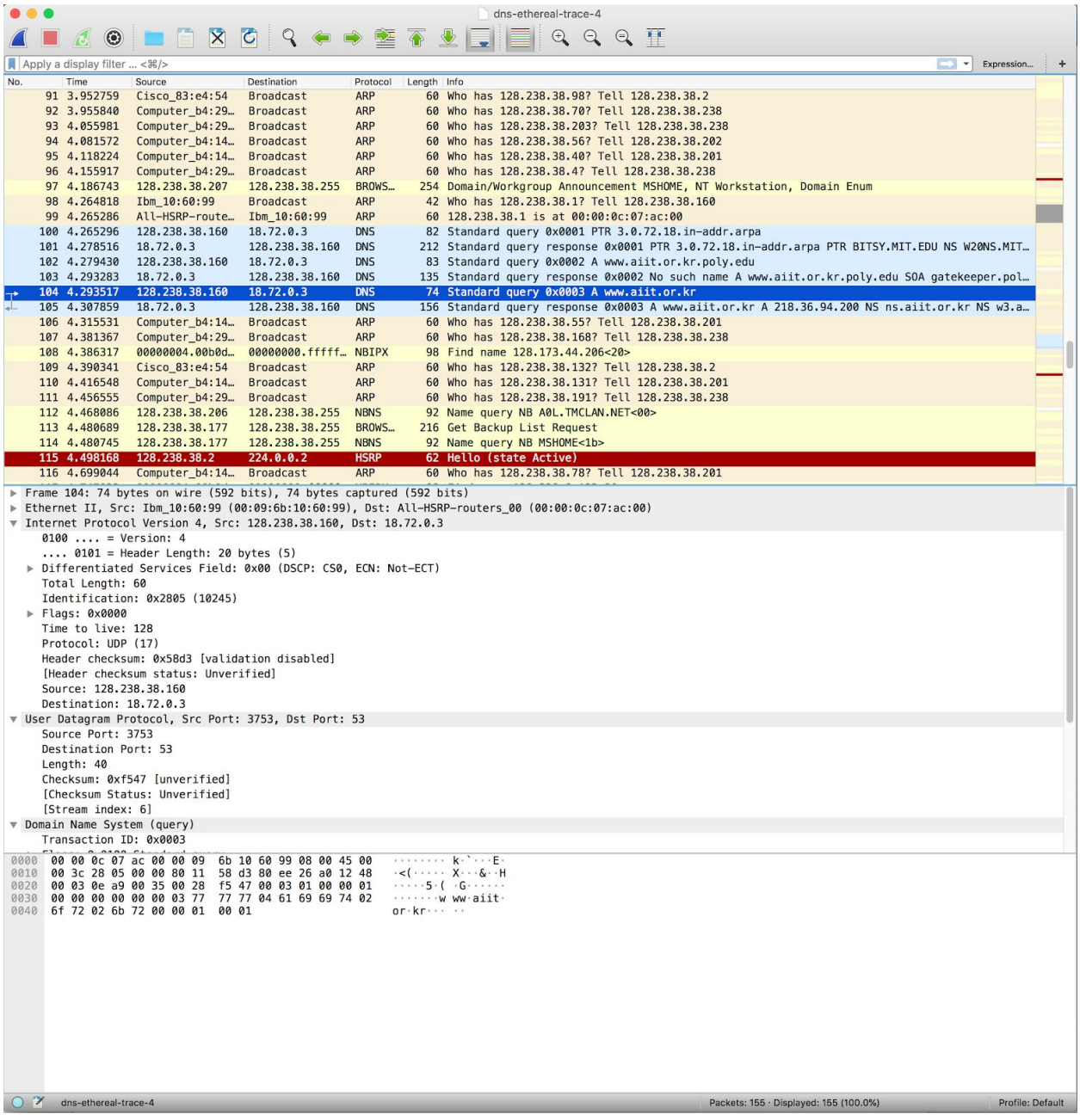
17. The response message provides the MIT nameservers bitsy.mit.edu, strawb.mit.edu and w20ns.mit.edu. The IP address are available in the additional records field of Wireshark as given below:

```
Additional records
        bitsy.mit.edu: type A, class IN, addr 18.72.0.3
            Name: bitsy.mit.edu
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 20736
            Data length: 4
            Address: 18.72.0.3
        strawb.mit.edu: type A, class IN, addr 18.71.0.151
```

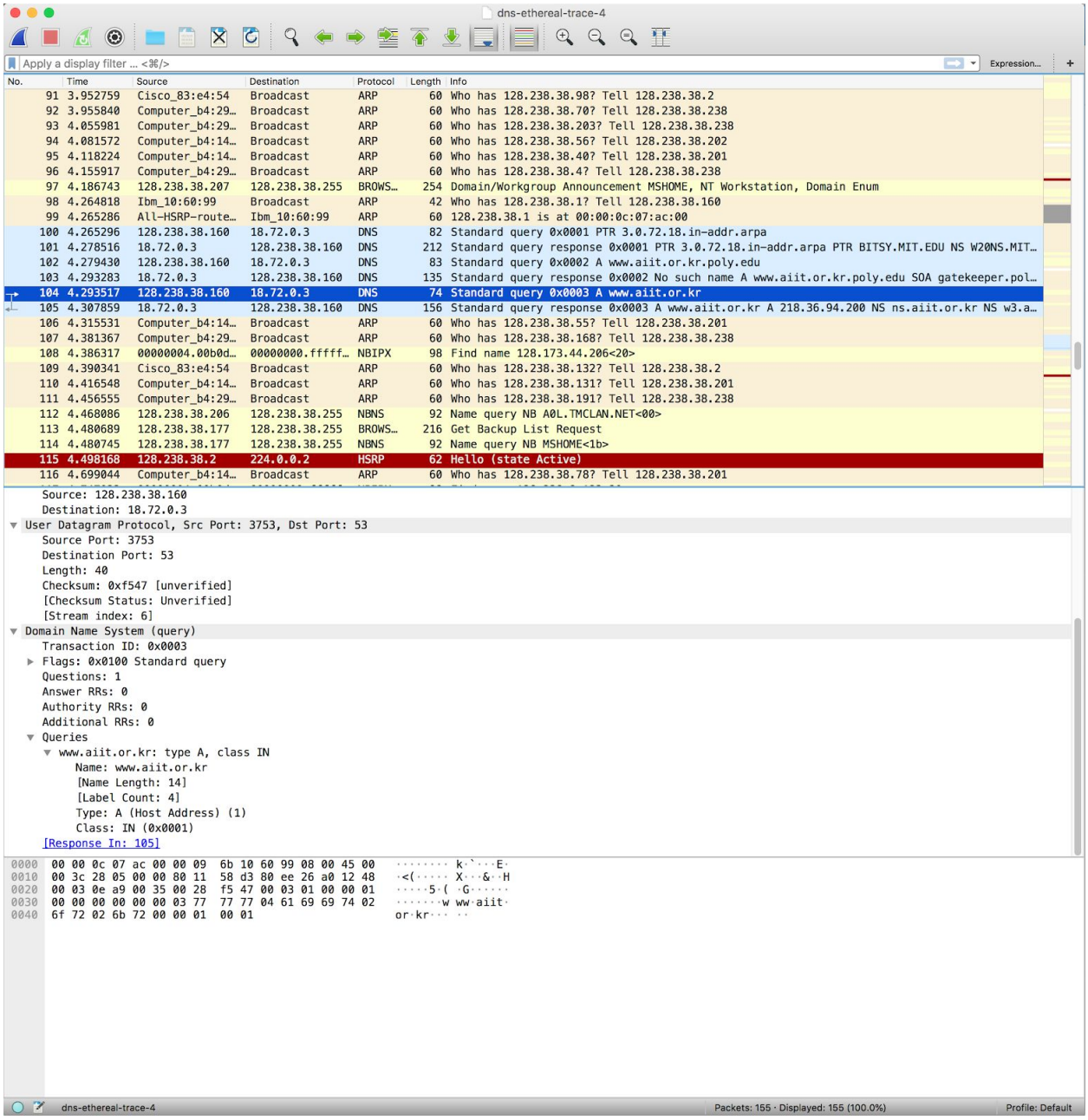
```
        Name: strawb.mit.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20736
        Data length: 4
        Address: 18.71.0.151
    w20ns.mit.edu: type A, class IN, addr 18.70.0.160
        Name: w20ns.mit.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20736
        Data length: 4
        Address: 18.70.0.160
```



18. The DNS query message is sent to the IP address: 18.72.0.3 which is the IP address of bitsy.mit.edu.

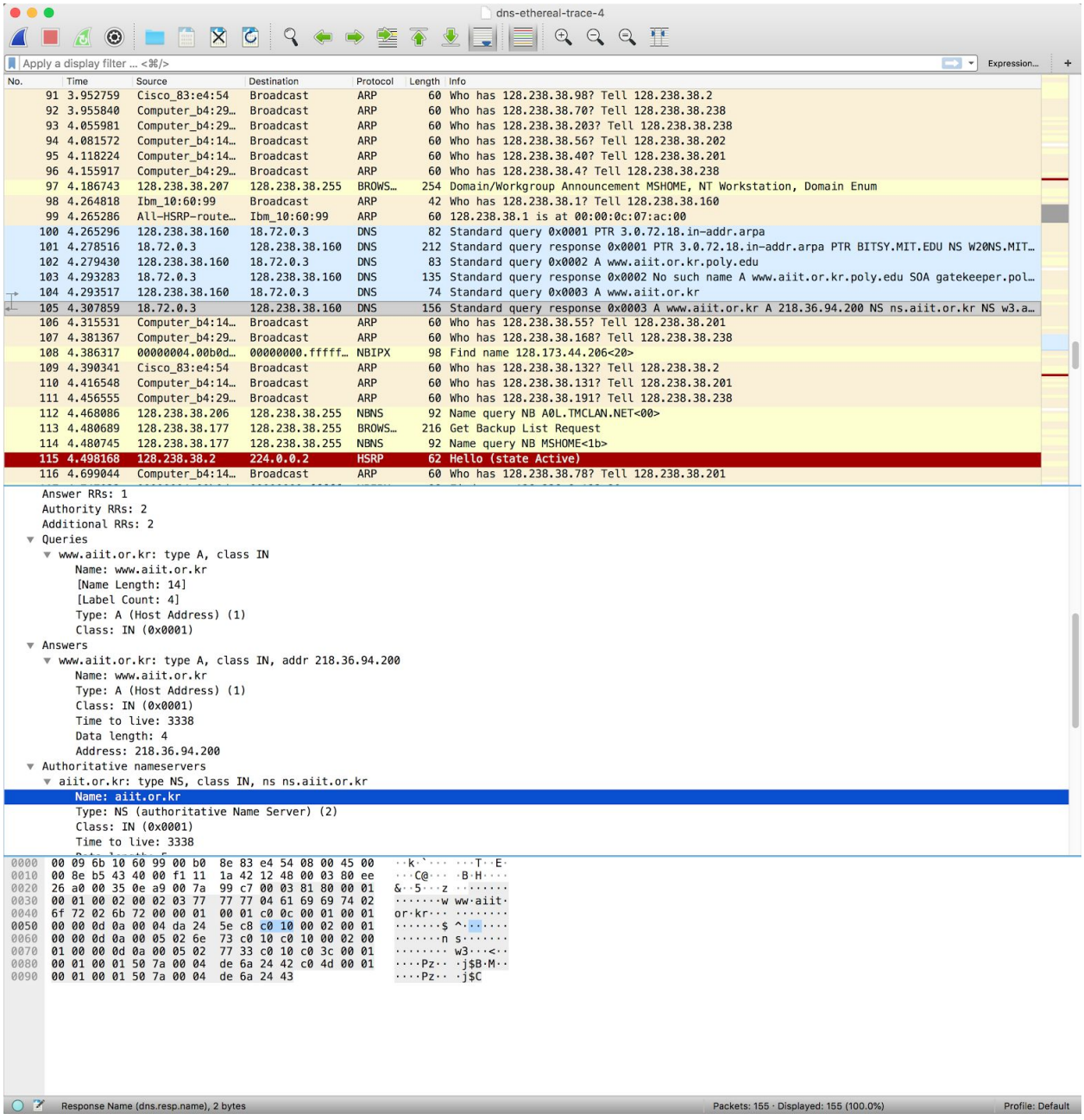


19. The DNS query is a standard Type A query. It does not contain any answers.



20. Only 1 answer is provided in the DNS response message. The answer is shown below:

```
Answers
        www.aiit.or.kr: type A, class IN, addr 218.36.94.200
            Name: www.aiit.or.kr
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 3338
            Data length: 4
            Address: 218.36.94.200
```


dns-ethereal-trace-4
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
91 3.952759 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.98? Tell 128.238.38.2
92 3.955840 Computer_b4:29… Broadcast ARP 60 Who has 128.238.38.70? Tell 128.238.38.238
93 4.055981 Computer_b4:29… Broadcast ARP 60 Who has 128.238.38.203? Tell 128.238.38.238
94 4.081572 Computer_b4:14… Broadcast ARP 60 Who has 128.238.38.56? Tell 128.238.38.202
95 4.118224 Computer_b4:14… Broadcast ARP 60 Who has 128.238.38.40? Tell 128.238.38.201
96 4.155917 Computer_b4:29… Broadcast ARP 60 Who has 128.238.38.4? Tell 128.238.38.238
97 4.186743 128.238.38.207 128.238.38.255 BROWS… 254 Domain/Workgroup Announcement MSHOME, NT Workstation, Domain Enum
98 4.264818 Ibm_10:60:99 Broadcast ARP 42 Who has 128.238.38.1? Tell 128.238.38.160
99 4.265286 All-HSRP-route… Ibm_10:60:99 ARP 60 128.238.38.1 is at 00:00:0c:07:ac:00
100 4.265296 128.238.38.160 18.72.0.3 DNS 82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101 4.278516 18.72.0.3 128.238.38.160 DNS 212 Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY.MIT.EDU NS W20NS.MIT…
102 4.279430 128.238.38.160 18.72.0.3 DNS 83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
103 4.293283 18.72.0.3 128.238.38.160 DNS 135 Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.pol…
104 4.293517 128.238.38.160 18.72.0.3 DNS 74 Standard query 0x0003 A www.aiit.or.kr
105 4.307859 18.72.0.3 128.238.38.160 DNS 156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.a…
106 4.315531 Computer_b4:14… Broadcast ARP 60 Who has 128.238.38.55? Tell 128.238.38.201
107 4.381367 Computer_b4:29… Broadcast ARP 60 Who has 128.238.38.168? Tell 128.238.38.238
108 4.386317 00000004.00b0d… 00000000.fffff… NBIPX 98 Find name 128.173.44.206<20>
109 4.390341 Cisco_83:e4:54 Broadcast ARP 60 Who has 128.238.38.132? Tell 128.238.38.2
110 4.416548 Computer_b4:14… Broadcast ARP 60 Who has 128.238.38.131? Tell 128.238.38.201
111 4.456555 Computer_b4:29… Broadcast ARP 60 Who has 128.238.38.191? Tell 128.238.38.238
112 4.468086 128.238.38.206 128.238.38.255 NBNS 92 Name query NB A0L.TMCLAN.NET<00>
113 4.480689 128.238.38.177 128.238.38.255 BROWS… 216 Get Backup List Request
114 4.480745 128.238.38.177 128.238.38.255 NBNS 92 Name query NB MSHOME<1b>
115 4.498168 128.238.38.2 224.0.0.2 HSRP 62 Hello (state Active)
116 4.699044 Computer_b4:14… Broadcast ARP 60 Who has 128.238.38.78? Tell 128.238.38.201
Answer RRs: 1
Authority RRs: 2
Additional RRs: 2
Queries
www.aiit.or.kr: type A, class IN
Name: www.aiit.or.kr
[Name Length: 14]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.aiit.or.kr: type A, class IN, addr 218.36.94.200
Name: www.aiit.or.kr
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 3338
Data length: 4
Address: 218.36.94.200
Authoritative nameservers
aiit.or.kr: type NS, class IN, ns ns.aiit.or.kr
Name: aiit.or.kr
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 3338
0000 00 09 6b 10 60 99 00 b0 8e 83 e4 54 08 00 45 00 ··k·`··· ···T··E·
0010 00 8e b5 43 40 00 f1 11 1a 42 12 48 00 03 80 ee ···C@··· ·B·H····
0020 26 a0 00 35 0e a9 00 7a 99 c7 00 03 81 80 00 01 &··5···z ········
0030 00 01 00 02 00 02 03 77 77 77 04 61 69 69 74 02 ·······w ww·aiit·
0040 6f 72 02 6b 72 00 00 01 00 01 c0 0c 00 01 00 01 or·kr··· ········
0050 00 00 0d 0a 00 04 da 24 5e c8 c0 10 00 02 00 01 ·······$ ^·······
0060 00 00 0d 0a 00 05 02 6e 73 c0 10 c0 10 00 02 00 ·······n s·······
0070 01 00 00 0d 0a 00 05 02 77 33 c0 10 c0 3c 00 01 ········ w3···<··
0080 00 01 00 01 50 7a 00 04 de 6a 24 42 c0 4d 00 01 ····Pz·· ·j$B·M··
0090 00 01 00 01 50 7a 00 04 de 6a 24 43 ····Pz·· ·j$C
Response Name (dns.resp.name), 2 bytes
Packets: 155 · Displayed: 155 (100.0%)
Profile: Default