Problem Set 1: Internetworking

SOLUTION:

A. INITIAL STEPS –

List of IP addresses in this whole process:

- *Laptop IP address – 192.168.77.128*
- *Default Gateway IP address – 192.168.77.2*
- *northeastern.edu – 104.96.198.146*

```
sbhatia@ubuntu:~$ ifconfig ens33
ens33     Link encap:Ethernet  HWaddr 00:0c:29:39:d9:5f
          inet addr:192.168.77.128  Bcast:192.168.77.255  Mask:255.255.255.0     ← Laptop IP address
          inet6 addr: fe80::a215:8683:9f45:e425/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:175466 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44722 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:204219655 (204.2 MB)  TX bytes:18046227 (18.0 MB)

sbhatia@ubuntu:~$ netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.77.2    0.0.0.0         UG        0 0          0 ens33   ← Gateway IP address
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 ens33
192.168.77.0    0.0.0.0         255.255.255.0   U         0 0          0 ens33
```

Clearing ARP cache for the default gateway of the network:

```
sbhatia@ubuntu:~$ arp -n                                                       ← List ARP table
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.77.254           ether   00:50:56:eb:27:10   C                     ens33
192.168.77.2             ether   00:50:56:ea:55:15   C                     ens33
sbhatia@ubuntu:~$ sudo arp -d 192.168.77.2                                     ← Clear MAC for gateway
sbhatia@ubuntu:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.77.254           ether   00:50:56:eb:27:10   C                     ens33
192.168.77.2                     (incomplete)                              ens33 ← MAC Cleared
```

Assumption:

We are assuming here that the laptop already has an IP address and knows the default gateway router in its network. In short, DHCP process has already occurred and the laptop is already connected to the Internet.

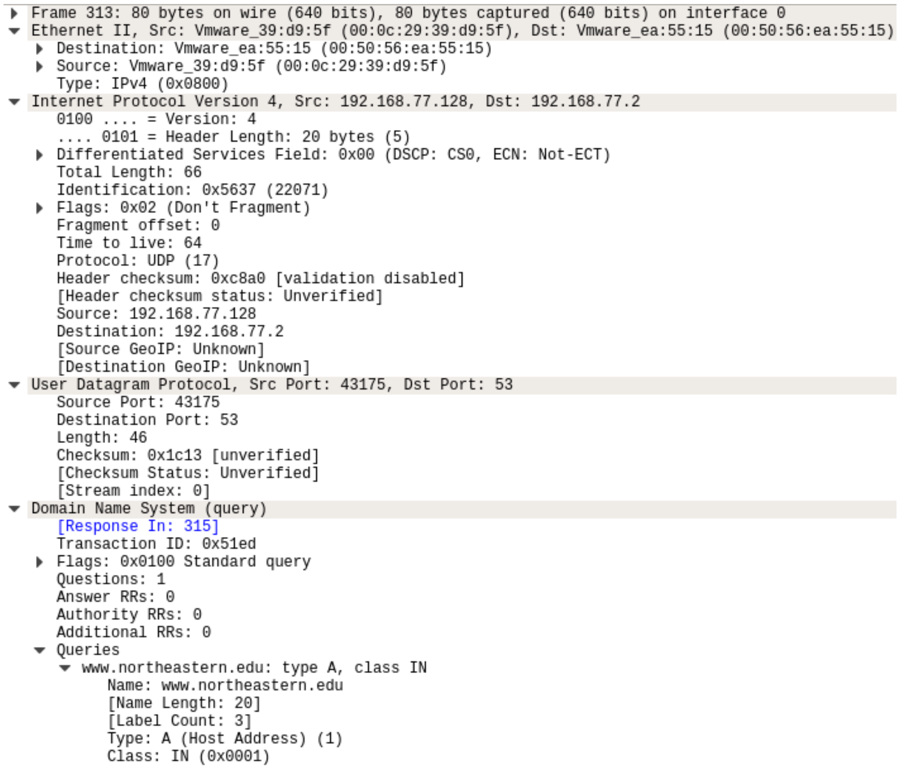
When we click a URL on the internet browser, the process begins by opening a TCP socket that will be used to send the HTTP Request message to http://www.northeastern.edu/ to retrieve the web page.

For creation of the socket, we need to know the IP address of the web page. For this, DNS protocol is used to get the name-IP address translation.

B. ACTUAL TRANSACTION –

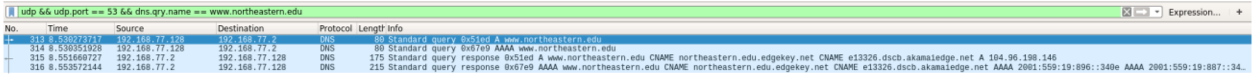
Step 1: DNS Query Message

a. The OS of the laptop/device creates a DNS query message with the URL in the question section of the message.
b. The DNS message is placed in a UDP segment with the destination port as 53 which is default for DNS protocol.
c. The UDP segment is placed in an IP packet with the source address of the device and destination address of the DNS server which was received in the DHCP ACK.
d. This IP packet is then placed in an Ethernet frame and addressed to the gateway router of the same network.
e. However, we do not know the MAC address of the router. Before sending this DNS query, we need to find out the MAC address.



```
▸ Frame 313: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
▾ Ethernet II, Src: Vmware_39:d9:5f (00:0c:29:39:d9:5f), Dst: Vmware_ea:55:15 (00:50:56:ea:55:15)
  ▸ Destination: Vmware_ea:55:15 (00:50:56:ea:55:15)
  ▸ Source: Vmware_39:d9:5f (00:0c:29:39:d9:5f)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.168.77.128, Dst: 192.168.77.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 66
    Identification: 0x5637 (22071)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0xc8a0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.77.128
    Destination: 192.168.77.2
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▾ User Datagram Protocol, Src Port: 43175, Dst Port: 53
    Source Port: 43175
    Destination Port: 53
    Length: 46
    Checksum: 0x1c13 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▾ Domain Name System (query)
    [Response In: 315]
    Transaction ID: 0x51ed
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.northeastern.edu: type A, class IN
        Name: www.northeastern.edu
        [Name Length: 20]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

DNS query and responses

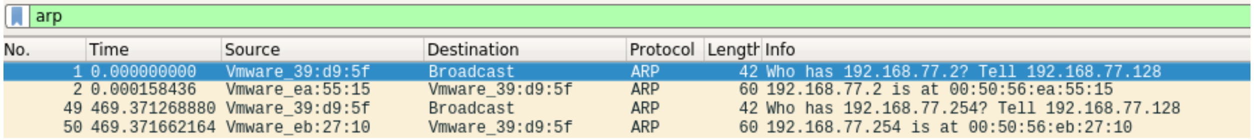


```
udp && udp.port == 53 && dns.qry.name == www.northeastern.edu
No.  Time         Source          Destination     Protocol Length Info
 313 8.530273717  192.168.77.128  192.168.77.2    DNS       80 Standard query 0x51ed A www.northeastern.edu
 314 8.530351928  192.168.77.128  192.168.77.2    DNS       80 Standard query 0x67e9 AAAA www.northeastern.edu
 315 8.551660727  192.168.77.2    192.168.77.128  DNS      175 Standard query response 0x51ed A www.northeastern.edu CNAME northeastern.edu.edgekey.net CNAME e13326.dscb.akamaiedge.net A 104.96.198.146
 316 8.553572144  192.168.77.2    192.168.77.128  DNS      215 Standard query response 0x67e9 AAAA www.northeastern.edu CNAME northeastern.edu.edgekey.net CNAME e13326.dscb.akamaiedge.net AAAA 2001:559:19:896::340e AAAA 2001:559:19:887::34…
```

Step 2: ARP for MAC address of default gateway router

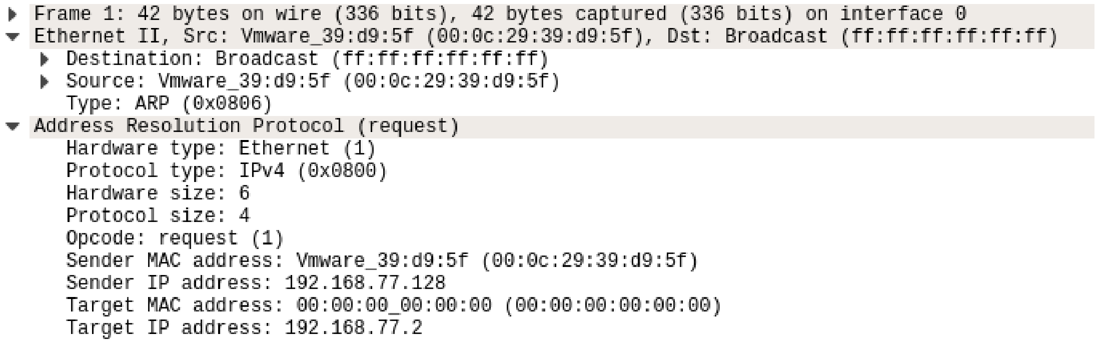
a. At present, we know the IP address of the gateway router but not the MAC address. To obtain this translation, ARP protocol is used.
b. The OS creates an ARP query message for IP address of the gateway router and broadcasts the message i.e. with a MAC address of FF: FF: FF: FF: FF: FF through the Ethernet switch.
c. When the frame reaches the gateway router, it identifies it's IP address in query and creates an ARP reply which is sent back to the laptop.
d. On receiving the ARP reply, my laptop will extract the MAC address of the gateway router and forward the Ethernet frame containing the IP packet which holds the UDP segment for the DNS query.

ARP Packets



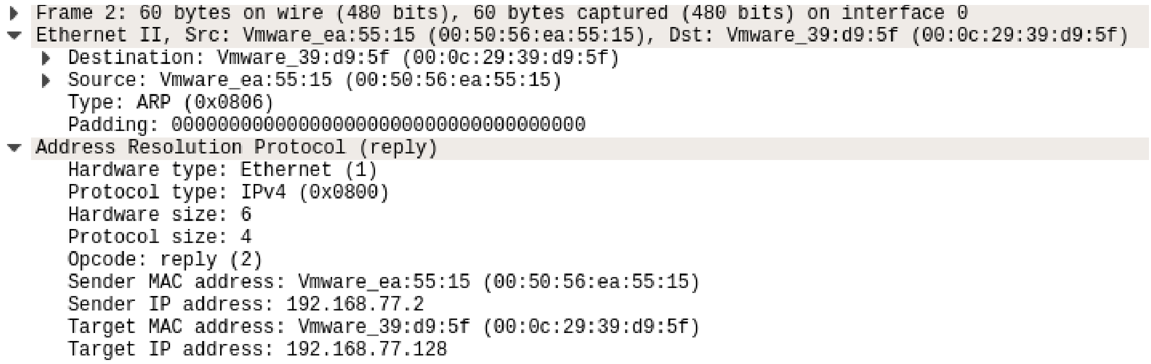
```
arp
No.     Time          Source           Destination      Protocol  Length Info
      1 0.000000000   Vmware_39:d9:5f  Broadcast        ARP       42 Who has 192.168.77.2? Tell 192.168.77.128
      2 0.000158436   Vmware_ea:55:15  Vmware_39:d9:5f  ARP       60 192.168.77.2 is at 00:50:56:ea:55:15
     49 469.371268880 Vmware_39:d9:5f  Broadcast        ARP       42 Who has 192.168.77.254? Tell 192.168.77.128
     50 469.371662164 Vmware_eb:27:10  Vmware_39:d9:5f  ARP       60 192.168.77.254 is at 00:50:56:eb:27:10
```

ARP Request



```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▾ Ethernet II, Src: Vmware_39:d9:5f (00:0c:29:39:d9:5f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
   ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   ▸ Source: Vmware_39:d9:5f (00:0c:29:39:d9:5f)
     Type: ARP (0x0806)
▾ Address Resolution Protocol (request)
     Hardware type: Ethernet (1)
     Protocol type: IPv4 (0x0800)
     Hardware size: 6
     Protocol size: 4
     Opcode: request (1)
     Sender MAC address: Vmware_39:d9:5f (00:0c:29:39:d9:5f)
     Sender IP address: 192.168.77.128
     Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
     Target IP address: 192.168.77.2
```

ARP Response



```
▸ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▾ Ethernet II, Src: Vmware_ea:55:15 (00:50:56:ea:55:15), Dst: Vmware_39:d9:5f (00:0c:29:39:d9:5f)
   ▸ Destination: Vmware_39:d9:5f (00:0c:29:39:d9:5f)
   ▸ Source: Vmware_ea:55:15 (00:50:56:ea:55:15)
     Type: ARP (0x0806)
     Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (reply)
     Hardware type: Ethernet (1)
     Protocol type: IPv4 (0x0800)
     Hardware size: 6
     Protocol size: 4
     Opcode: reply (2)
     Sender MAC address: Vmware_ea:55:15 (00:50:56:ea:55:15)
     Sender IP address: 192.168.77.2
     Target MAC address: Vmware_39:d9:5f (00:0c:29:39:d9:5f)
     Target IP address: 192.168.77.128
```

Step 3: Routing DNS Query message to DNS Server

a. The gateway router extracts the DNS query on receiving the frame and looks up in its forwarding table where the packet is to be sent.

b. On getting the appropriate IP interface, it forwards the packet which eventually reaches the DNS server through intra-domain routing (RIP, OSPF or IS-IS) and inter-domain routing (BGP).

Step 4: DNS resolution and reply

a. The DNS server extracts the DNS query message from the packet and looks up the name http://www.northeastern.edu/ in its database.

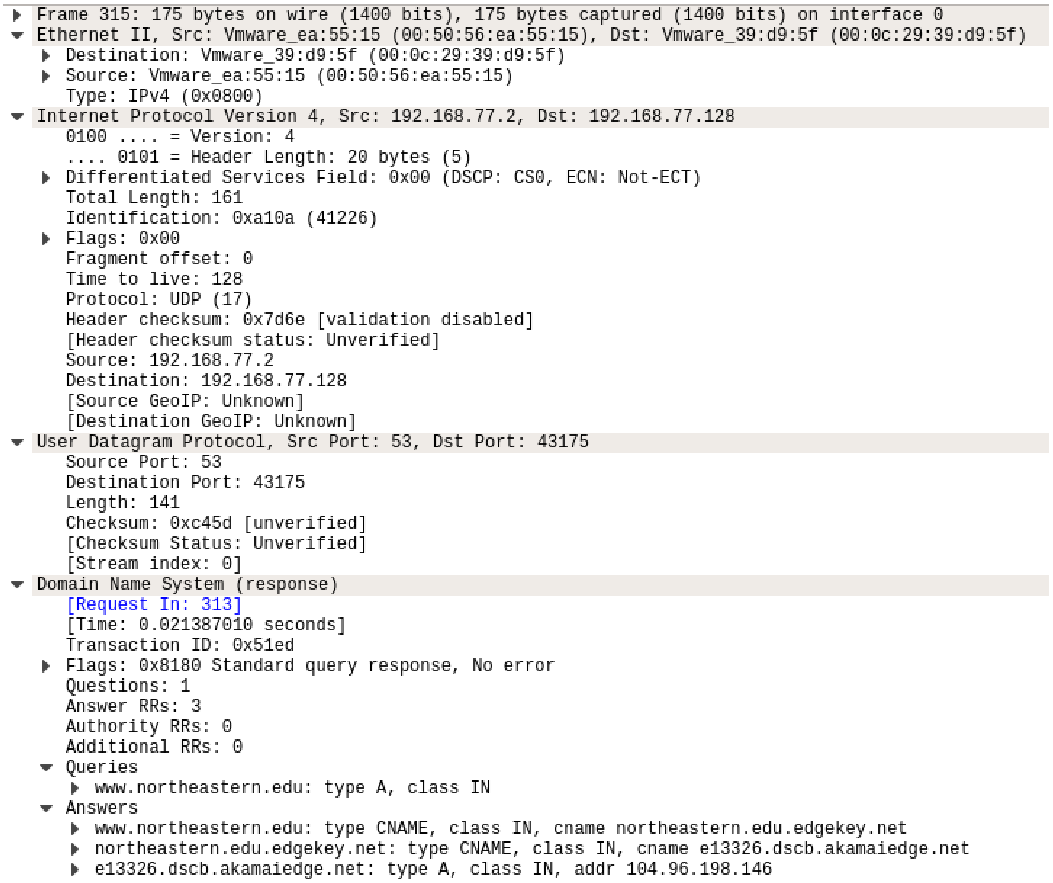
b. It extracts a DNS resource record (RR) that contains an IP address for the requested URL. (Assumption – the RR is already cached in the DNS server)

c. If it is not cached, then the DNS query is forwarded to the Authoritative DNS Server for http://www.northeastern.edu/.

d. Next, the DNS server creates a DNS reply message with the hostname-IP address translation and places in a UDP segment.

e. This UDP segment in an IP packet is addressed sent back to my laptop IP address. Finally, my OS knows the IP address of http://www.northeastern.edu/ and is ready to contact it.

DNS Response

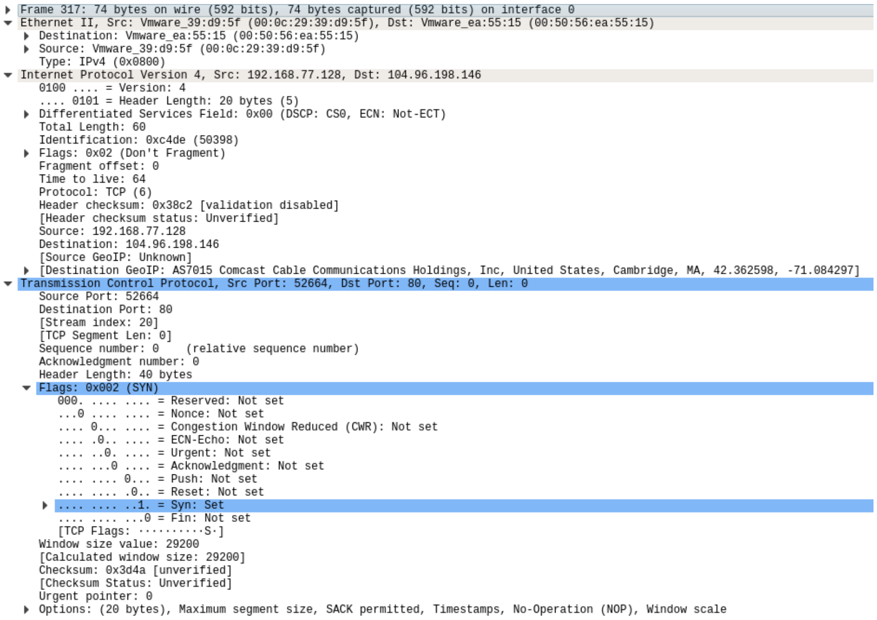


```
▶ Frame 315: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface 0
▼ Ethernet II, Src: Vmware_ea:55:15 (00:50:56:ea:55:15), Dst: Vmware_39:d9:5f (00:0c:29:39:d9:5f)
  ▶ Destination: Vmware_39:d9:5f (00:0c:29:39:d9:5f)
  ▶ Source: Vmware_ea:55:15 (00:50:56:ea:55:15)
    Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.77.2, Dst: 192.168.77.128
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 161
    Identification: 0xa10a (41226)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x7d6e [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.77.2
    Destination: 192.168.77.128
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ User Datagram Protocol, Src Port: 53, Dst Port: 43175
    Source Port: 53
    Destination Port: 43175
    Length: 141
    Checksum: 0xc45d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▼ Domain Name System (response)
    [Request In: 313]
    [Time: 0.021387010 seconds]
    Transaction ID: 0x51ed
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ www.northeastern.edu: type A, class IN
  ▼ Answers
    ▶ www.northeastern.edu: type CNAME, class IN, cname northeastern.edu.edgekey.net
    ▶ northeastern.edu.edgekey.net: type CNAME, class IN, cname e13326.dscb.akamaiedge.net
    ▶ e13326.dscb.akamaiedge.net: type A, class IN, addr 104.96.198.146
```

Step 5: TCP three-way handshake

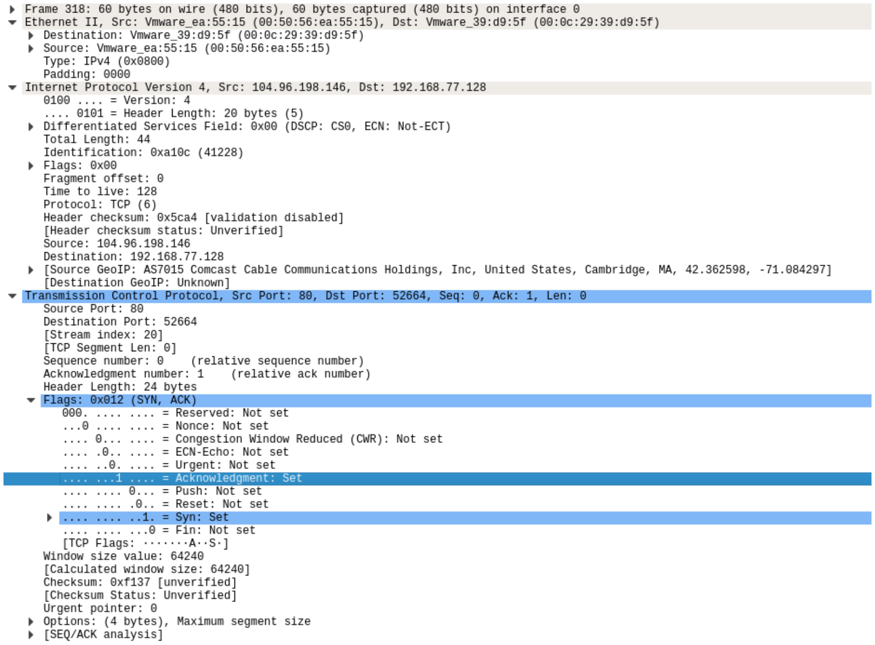
a. Once we know the destination IP, we can create a TCP socket for end-to-end communication.
b. For such communication, a TCP three-way handshake is performed with the destination. First a TCP SYN with destination port 80 (HTTP) is sent.
c. The destination server on receiving this message opens a socket and replies with a TCP SYNACK.
d. The TCP socket on my laptop demultiplexes the datagram sends an ACK and now is ready to transmit actual data to the destination.

TCP SYN



```
Frame 317: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Vmware_39:d9:5f (00:0c:29:39:d9:5f), Dst: Vmware_ea:55:15 (00:50:56:ea:55:15)
   Destination: Vmware_ea:55:15 (00:50:56:ea:55:15)
   Source: Vmware_39:d9:5f (00:0c:29:39:d9:5f)
   Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.77.128, Dst: 104.96.198.146
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 60
   Identification: 0xc4de (50398)
   Flags: 0x02 (Don't Fragment)
   Fragment offset: 0
   Time to live: 64
   Protocol: TCP (6)
   Header checksum: 0x38c2 [validation disabled]
   [Header checksum status: Unverified]
   Source: 192.168.77.128
   Destination: 104.96.198.146
   [Source GeoIP: Unknown]
   [Destination GeoIP: AS7015 Comcast Cable Communications Holdings, Inc, United States, Cambridge, MA, 42.362598, -71.084297]
Transmission Control Protocol, Src Port: 52664, Dst Port: 80, Seq: 0, Len: 0
   Source Port: 52664
   Destination Port: 80
   [Stream index: 20]
   [TCP Segment Len: 0]
   Sequence number: 0    (relative sequence number)
   Acknowledgment number: 0
   Header Length: 40 bytes
   Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]
   Window size value: 29200
   [Calculated window size: 29200]
   Checksum: 0x3d4a [unverified]
   [Checksum Status: Unverified]
   Urgent pointer: 0
   Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
```

TCP SYNACK



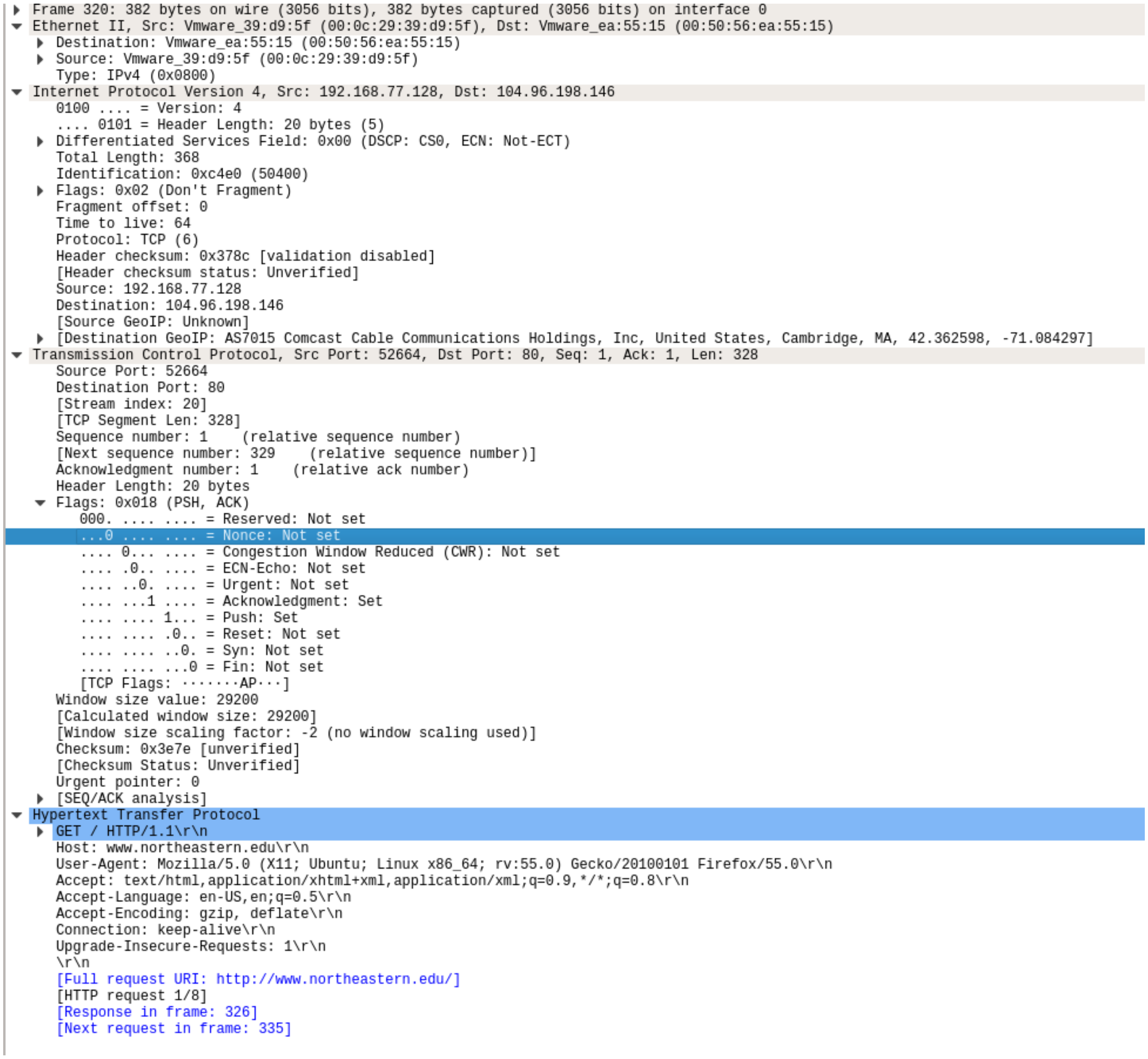
```
Frame 318: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Vmware_ea:55:15 (00:50:56:ea:55:15), Dst: Vmware_39:d9:5f (00:0c:29:39:d9:5f)
   Destination: Vmware_39:d9:5f (00:0c:29:39:d9:5f)
   Source: Vmware_ea:55:15 (00:50:56:ea:55:15)
   Type: IPv4 (0x0800)
   Padding: 0000
Internet Protocol Version 4, Src: 104.96.198.146, Dst: 192.168.77.128
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 44
   Identification: 0xa10c (41228)
   Flags: 0x00
   Fragment offset: 0
   Time to live: 128
   Protocol: TCP (6)
   Header checksum: 0x5ca4 [validation disabled]
   [Header checksum status: Unverified]
   Source: 104.96.198.146
   Destination: 192.168.77.128
   [Source GeoIP: AS7015 Comcast Cable Communications Holdings, Inc, United States, Cambridge, MA, 42.362598, -71.084297]
   [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80, Dst Port: 52664, Seq: 0, Ack: 1, Len: 0
   Source Port: 80
   Destination Port: 52664
   [Stream index: 20]
   [TCP Segment Len: 0]
   Sequence number: 0    (relative sequence number)
   Acknowledgment number: 1    (relative ack number)
   Header Length: 24 bytes
   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: 64240
   [Calculated window size: 64240]
   Checksum: 0xf137 [unverified]
   [Checksum Status: Unverified]
   Urgent pointer: 0
   Options: (4 bytes), Maximum segment size
   [SEQ/ACK analysis]
```

Step 6: HTTP GET request

a. My browser now creates a HTTP GET message containing the URL http://www.northeastern.edu/ to be fetched.

b. This message is added in the payload of the TCP segment, which is placed in an IP datagram and forwarded to the HTTP server.

HTTP GET



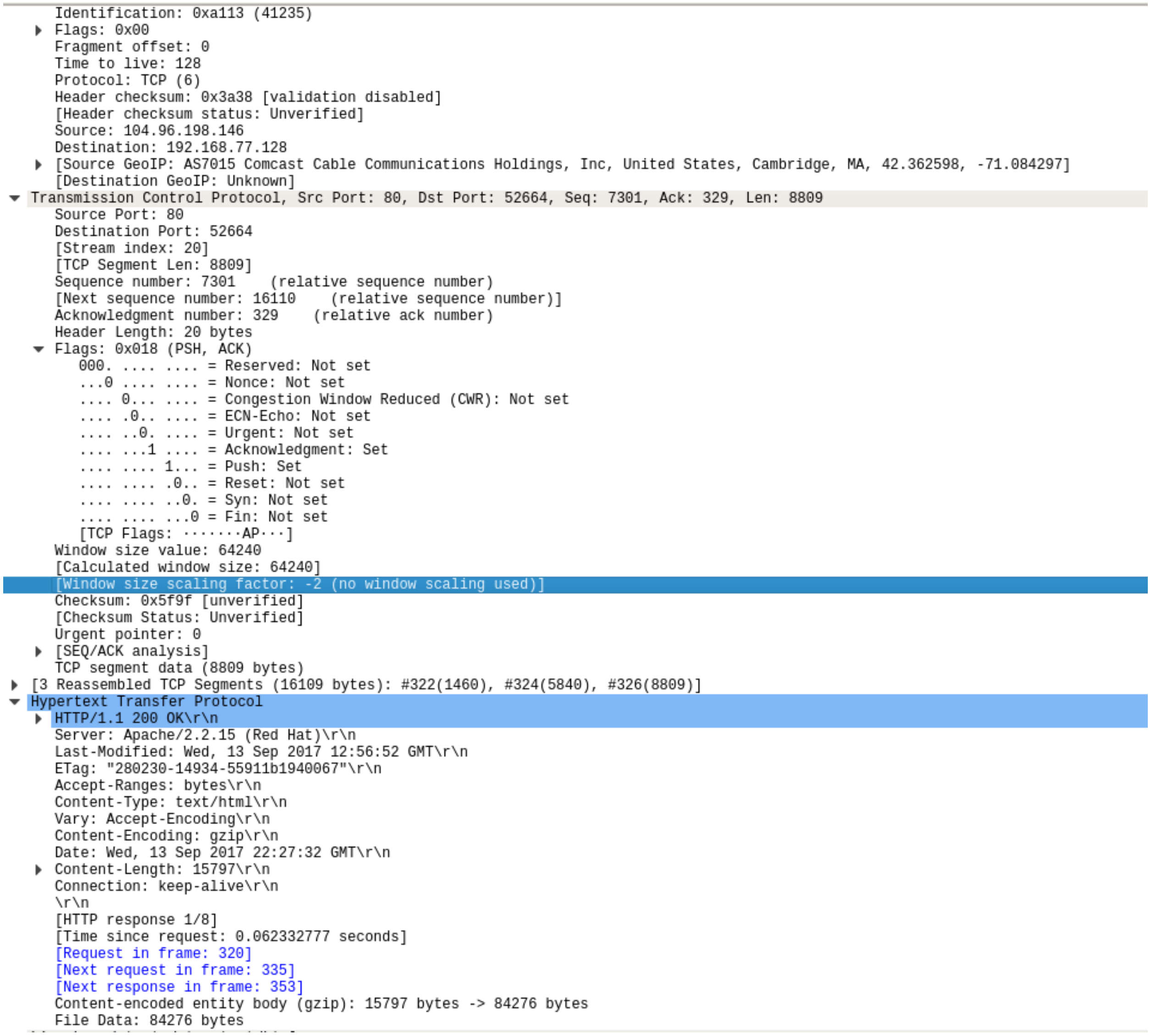
```
▶ Frame 320: 382 bytes on wire (3056 bits), 382 bytes captured (3056 bits) on interface 0
▼ Ethernet II, Src: Vmware_39:d9:5f (00:0c:29:39:d9:5f), Dst: Vmware_ea:55:15 (00:50:56:ea:55:15)
  ▶ Destination: Vmware_ea:55:15 (00:50:56:ea:55:15)
  ▶ Source: Vmware_39:d9:5f (00:0c:29:39:d9:5f)
    Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.77.128, Dst: 104.96.198.146
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 368
    Identification: 0xc4e0 (50400)
  ▶ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x378c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.77.128
    Destination: 104.96.198.146
    [Source GeoIP: Unknown]
  ▶ [Destination GeoIP: AS7015 Comcast Cable Communications Holdings, Inc, United States, Cambridge, MA, 42.362598, -71.084297]
▼ Transmission Control Protocol, Src Port: 52664, Dst Port: 80, Seq: 1, Ack: 1, Len: 328
    Source Port: 52664
    Destination Port: 80
    [Stream index: 20]
    [TCP Segment Len: 328]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 329    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header Length: 20 bytes
  ▼ Flags: 0x018 (PSH, 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
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······AP···]
    Window size value: 29200
    [Calculated window size: 29200]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x3e7e [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▶ [SEQ/ACK analysis]
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: www.northeastern.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://www.northeastern.edu/]
    [HTTP request 1/8]
    [Response in frame: 326]
    [Next request in frame: 335]
```

Step 7: HTTP response and displayed

a. The HTTP server receives the GET request and fetches the content and places it in a HTTP response message and sends it via the TCP socket.

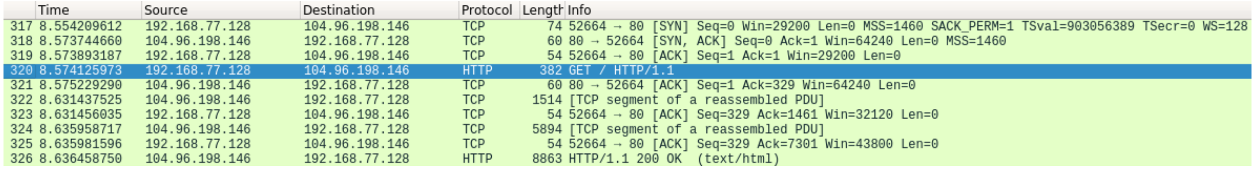
b. The datagram containing the reply is extracted, and demultiplexed at the TCP socket to get the actual HTML page for http://www.northeastern.edu/ which is then finally displayed on my browser.

HTTP 200 OK



```
      Identification: 0xa113 (41235)
    ▸ Flags: 0x00
      Fragment offset: 0
      Time to live: 128
      Protocol: TCP (6)
      Header checksum: 0x3a38 [validation disabled]
      [Header checksum status: Unverified]
      Source: 104.96.198.146
      Destination: 192.168.77.128
    ▸ [Source GeoIP: AS7015 Comcast Cable Communications Holdings, Inc, United States, Cambridge, MA, 42.362598, -71.084297]
      [Destination GeoIP: Unknown]
  ▾ Transmission Control Protocol, Src Port: 80, Dst Port: 52664, Seq: 7301, Ack: 329, Len: 8809
      Source Port: 80
      Destination Port: 52664
      [Stream index: 20]
      [TCP Segment Len: 8809]
      Sequence number: 7301    (relative sequence number)
      [Next sequence number: 16110    (relative sequence number)]
      Acknowledgment number: 329    (relative ack number)
      Header Length: 20 bytes
    ▾ Flags: 0x018 (PSH, 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
         .... .... 1... = Push: Set
         .... .... .0.. = Reset: Not set
         .... .... ..0. = Syn: Not set
         .... .... ...0 = Fin: Not set
         [TCP Flags: ·······AP···]
      Window size value: 64240
      [Calculated window size: 64240]
      [Window size scaling factor: -2 (no window scaling used)]
      Checksum: 0x5f9f [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
    ▸ [SEQ/ACK analysis]
      TCP segment data (8809 bytes)
  ▸ [3 Reassembled TCP Segments (16109 bytes): #322(1460), #324(5840), #326(8809)]
  ▾ Hypertext Transfer Protocol
    ▸ HTTP/1.1 200 OK\r\n
      Server: Apache/2.2.15 (Red Hat)\r\n
      Last-Modified: Wed, 13 Sep 2017 12:56:52 GMT\r\n
      ETag: "280230-14934-55911b1940067"\r\n
      Accept-Ranges: bytes\r\n
      Content-Type: text/html\r\n
      Vary: Accept-Encoding\r\n
      Content-Encoding: gzip\r\n
      Date: Wed, 13 Sep 2017 22:27:32 GMT\r\n
    ▸ Content-Length: 15797\r\n
      Connection: keep-alive\r\n
      \r\n
      [HTTP response 1/8]
      [Time since request: 0.062332777 seconds]
      [Request in frame: 320]
      [Next request in frame: 335]
      [Next response in frame: 353]
      Content-encoded entity body (gzip): 15797 bytes -> 84276 bytes
      File Data: 84276 bytes
```

TCP stream for full transaction



```
    Time          Source           Destination      Protocol Length Info
317 8.554209612   192.168.77.128   104.96.198.146   TCP        74 52664 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=903056389 TSecr=0 WS=128
318 8.573744660   104.96.198.146   192.168.77.128   TCP        60 80 → 52664 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
319 8.573893187   192.168.77.128   104.96.198.146   TCP        54 52664 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
320 8.574125973   192.168.77.128   104.96.198.146   HTTP      382 GET / HTTP/1.1
321 8.575229290   104.96.198.146   192.168.77.128   TCP        60 80 → 52664 [ACK] Seq=1 Ack=329 Win=64240 Len=0
322 8.631437525   104.96.198.146   192.168.77.128   TCP      1514 [TCP segment of a reassembled PDU]
323 8.631456035   192.168.77.128   104.96.198.146   TCP        54 52664 → 80 [ACK] Seq=329 Ack=1461 Win=32120 Len=0
324 8.635958717   104.96.198.146   192.168.77.128   TCP      5894 [TCP segment of a reassembled PDU]
325 8.635981596   192.168.77.128   104.96.198.146   TCP        54 52664 → 80 [ACK] Seq=329 Ack=7301 Win=43800 Len=0
326 8.636458750   104.96.198.146   192.168.77.128   HTTP     8863 HTTP/1.1 200 OK  (text/html)
```