

**Kirollous Ramzy Assad**  
**Lab 8**

# Question 1

Wireshark screenshot showing network traffic. The top pane displays a list of captured HTTP requests:

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027362245	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030672101	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231407421	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.2338074462	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)

The bottom pane shows the detailed view of the selected packet (No. 8), which is a GET request for 'favicon.ico':

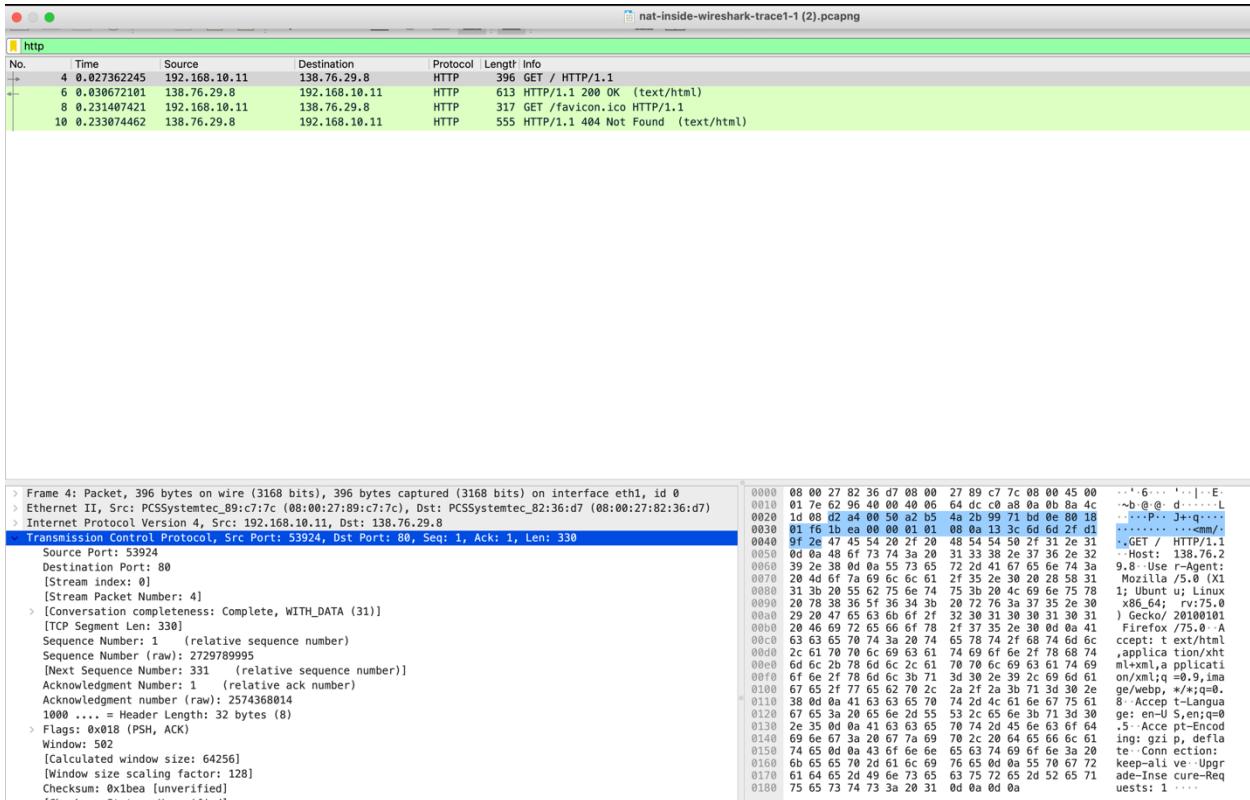
```
> Frame 8: Packet, 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth1, id 0
> Ethernet II, Src: PCSSystemtec_89:c7:7c (08:00:27:89:c7:7c), Dst: PCSSystemtec_82:36:d7 (08:00:27:82:36:d7)
< Internet Protocol Version 4, Src: 192.168.10.11, Dst: 138.76.29.8
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 382
    Identification: 0x6296 (25238)
  > 010. .... = Flags: 0x2, Don't fragment
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x64dc [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.10.11
  Destination Address: 138.76.29.8
  [Stream index: 0]
  > Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
  > Hypertext Transfer Protocol
```

Hex and ASCII dump of the selected packet:

0000	08 00 27 82 36 d7 08 00	27 89 c7 7c 08 00 45 00	...`-6...`.. ..E-
0010	01 7e 62 96 40 00 40 06	64 dc c0 a8 0a 0b 8a 4c	~-b-@.d+...L
0020	1d 08 d2 a4 00 50 a2 b5	4a 2b 99 71 bd 0e 00 18	...-P..J+-q...-
0030	01 f6 1b ea 00 00 01 01	08 0a 13 3c 6d 6d 2f d1	...-...`-...`-...`-.
0040	00 00 00 00 00 00 00 00	54 54 54 54 54 54 54 54	...-GET / favicon.ico
0050	0d 0a 48 6f 73 74 3a 20	31 74 58 2e 37 36 2e 32	...-Host: 138.76.2
0060	39 2e 38 0d 0a 55 73 65	72 2d 41 67 65 6e 74 3a	9.8 -Use r-Agent:
0070	29 4d 6f 7a 69 6c 6c 61	2f 35 2a 30 28 28 58 31	Mozilla /5.0 (X1
0080	31 3b 20 55 62 75 6c 74	75 3b 20 4c 69 66 75 78	Ubuntu u; Linus
0090	20 78 38 36 5f 36 34 3b	20 72 70 3a 37 35 2e 30	x86_64; rv:75.0
00a0	29 28 47 63 63 6b 6f 2f	32 30 31 30 30 31 30 31	) Gecko/20100101
00b0	20 46 69 72 65 66 6f 78	2f 37 32 2e 30 0d 41	Firefox /75.0 A
00c0	63 63 63 63 63 63 63 63	64 64 64 64 64 64 64 64	ccent/1.0 ext/html
00d0	00 00 00 00 00 00 00 00	74 69 6f 5e 78 68 74	application/x-javascript
00e0	6d 6c 2b 78 6d 6c 2c 61	70 78 6c 69 63 61 74 69	ml+xml,a applicati
00f0	6f 6e 2f 78 6d 6c 3b 71	3d 30 2e 39 2c 69 6d 61	on/xml;q=0.9,ima
0100	67 65 2f 77 65 62 70 2c	2a 2f 2a 3b 71 3d 30 2e	ge/webp, */*;q=0.
0110	38 0d 0a 41 63 63 65 70	74 2d 4e 61 6e 67 75 61	8 -Acces t-Langua
0120	67 65 3a 20 65 6e 2d 55	53 2c 65 6e 3b 71 3d 30	ge: en-US,en;q=0
0130	2d 35 0d 0a 63 63 65 70	70 74 25 45 6e 60 64	.., Acces pt-Cod
0140	69 65 0d 0a 20 65 6e 69	70 74 25 45 6e 60 64	ing: en-US,defaul
0150	74 65 0d 0a 43 6f 6e 66	65 63 74 69 6e 3a 20	te - Conn ection:
0160	6b 65 65 70 2d 61 6c 69	76 65 0d 0a 55 70 67 72	keep-alive -Upgr
0170	61 64 65 2d 49 6e 73 65	63 75 72 65 2d 52 65 71	ade-Inse cure-Req
0180	75 65 73 74 73 3a 20 31	0d 0a 0d 0a	uests: 1 ...

Source Address: 192.168.10.11

Destination Address: 138.76.29.8

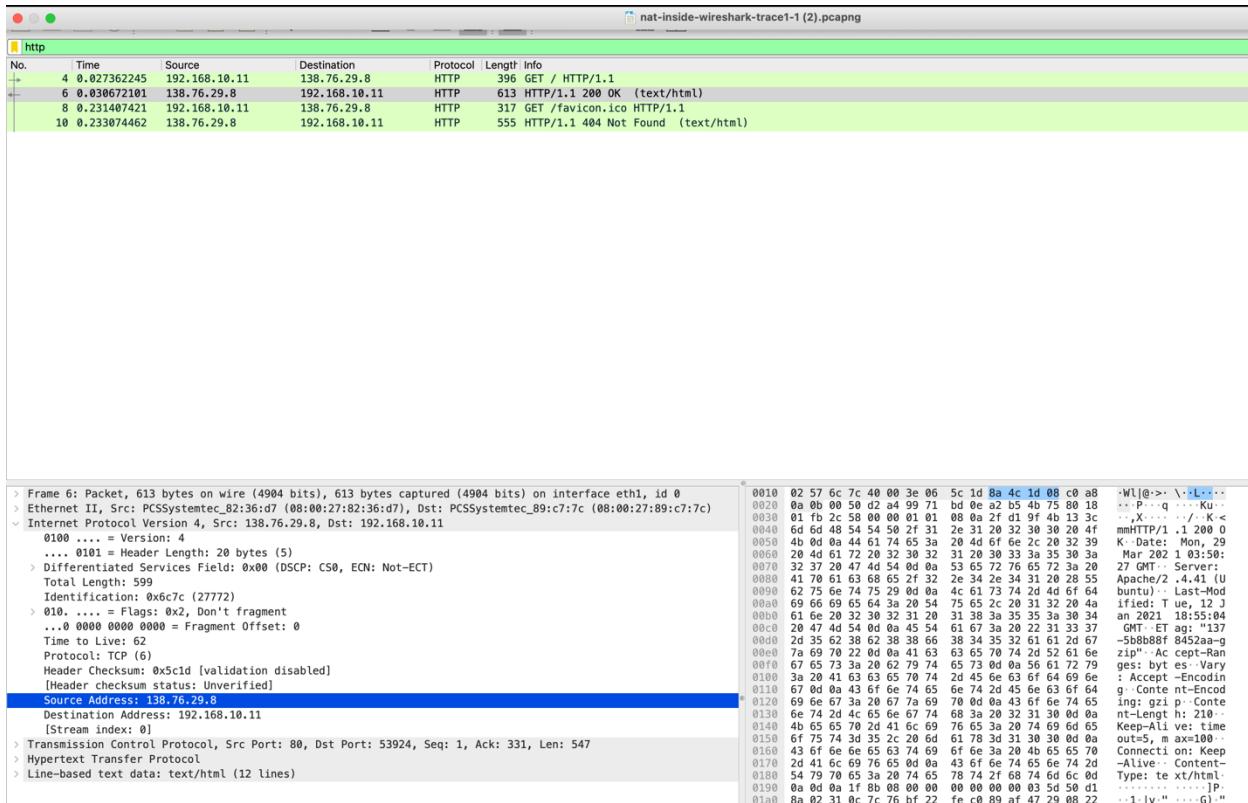


Source Port: 53924  
 Destination Port: 80

## **Question 2**

Time = 0.27362245

## **QUESTION 3**



Source Address: 138.76.29.8

Destination Address: 192.168.10.11

nat-inside-wireshark-trace1-1 (2).pcapng

http

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027362245	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030672101	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231407421	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233074462	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)

Frame 0: PACKET, 163 bytes on wire (14994 bits), 163 bytes captured (14994 bits) on interface en0, link layer type Ethernet II (0x0800), source PCSsystemtec\_82:36:d7 (08:00:27:82:36:d7), destination PCSsystemtec\_89:c7:c (08:00:27:89:c7:c)  
> Ethernet II, Src: PCSsystemtec\_82:36:d7 (08:00:27:82:36:d7), Dst: PCSsystemtec\_89:c7:c (08:00:27:89:c7:c) [ethertype IPv4 (0x0800), src 138.76.29.8, dst 192.168.10.11]  
> Internet Protocol Version 4, Src: 138.76.29.8, Dst: 192.168.10.11 [iph\_length: 56 / ihl: 5] [ttl: 64 / tos: 0x0]  
> Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547  
Source Port: 80  
Destination Port: 53924  
[Stream index: 0]  
[Stream Packet Number: 6]  
> [Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 547]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 2574368014  
[Next Sequence Number: 548 (relative sequence number)]  
Acknowledgment Number: 331 (relative ack number)  
Acknowledgment number (raw): 2729790325  
1000 .... = Header Length: 32 bytes (8)  
> Flags: 0x018 (PSH, ACK)  
Window: 507  
[Calculated window size: 64896]  
[Window size scaling factor: 128]  
Checksum: 0x2c58 [unverified]  
[Checksum Status: Unverified]

0020 0a 0b 00 50 d2 a4 99 71 bd 0e a2 b5 4b 75 80 18 ..P...q ...K..  
0030 00 00 00 00 00 00 00 00 08 0a 21 97 4b 00 3c 00 ..K..  
0040 6d 6d 0a 24 54 6f 2f 31 20 4d 66 2c 20 32 30 4f mHTTP/1.1 200 0  
0050 4b 0d 0a 24 61 74 65 3a 20 4d 6f 6e 2c 20 32 30 K..Date: Mon, 29  
0060 20 4d 61 72 20 32 30 32 31 20 30 33 3a 35 30 3a Mar 2021 03:50:  
0070 32 37 20 47 4d 54 00 0a 53 65 72 76 65 72 3a 20 27 GMT- Server:  
0080 41 70 61 63 68 65 2f 32 2e 34 22 34 31 20 28 55 Apache/2.4.41 (U  
0090 62 75 6e 73 75 29 00 0a 4c 61 73 74 2d 4d 6f 64 buntu).. Last-Mod  
00a0 69 66 69 65 64 3a 20 54 75 65 20 31 32 20 4a ified: Tue, 12 J  
00b0 61 6e 28 37 32 30 54 31 38 30 35 35 3a 20 30 4a ari 2021 18:55:46  
00c0 69 6e 28 37 32 30 54 31 38 30 35 35 3a 20 30 4a GMT- ET 2021-137  
00d0 2d 35 62 38 62 38 38 66 38 34 35 32 61 61 2d 67 -5bb8b81 8452aa-g  
00e0 78 69 70 22 0d 0a 41 63 63 65 70 74 2d 52 61 66 zip": Ac cept-Ran  
00f0 67 65 73 3a 20 62 79 74 65 73 0d 0a 56 61 72 79 ges: byt es- Vary  
0100 3a 20 41 63 63 65 70 74 2d 45 6d 63 6f 64 69 66 : Accept- Encodin  
0110 67 0d 0a 43 6f 6e 74 65 6e 74 2d 45 6d 63 6f 64 g- Conte nt-Encod  
0120 69 6e 67 3a 20 67 7a 69 70 0d 0a 43 6f 6e 74 65 ing: gzip p- Conte  
0130 6e 74 2d 4c 65 6e 6a 69 68 3a 20 32 31 30 0d 0a nt-Length: 216  
0140 6f 75 74 3d 35 2c 20 6d 61 78 3d 31 30 30 0d 0a Content- Encoding: gzip  
0150 6f 75 74 3d 35 2c 20 6d 61 78 3d 31 30 30 0d 0a out=5, # ax=100  
0160 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 Connection: Keep  
0170 2d 41 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d -Alive: Content-  
0180 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 0d Type: te/htlm-  
0190 0a 0d 0a 1f 8b 08 00 00 00 00 00 00 03 5d 50 d1 .....P  
01a0 8a 02 31 0c 7c 76 bf 22 fe c0 89 af 47 29 08 22 ..-1- lv" ....G)"

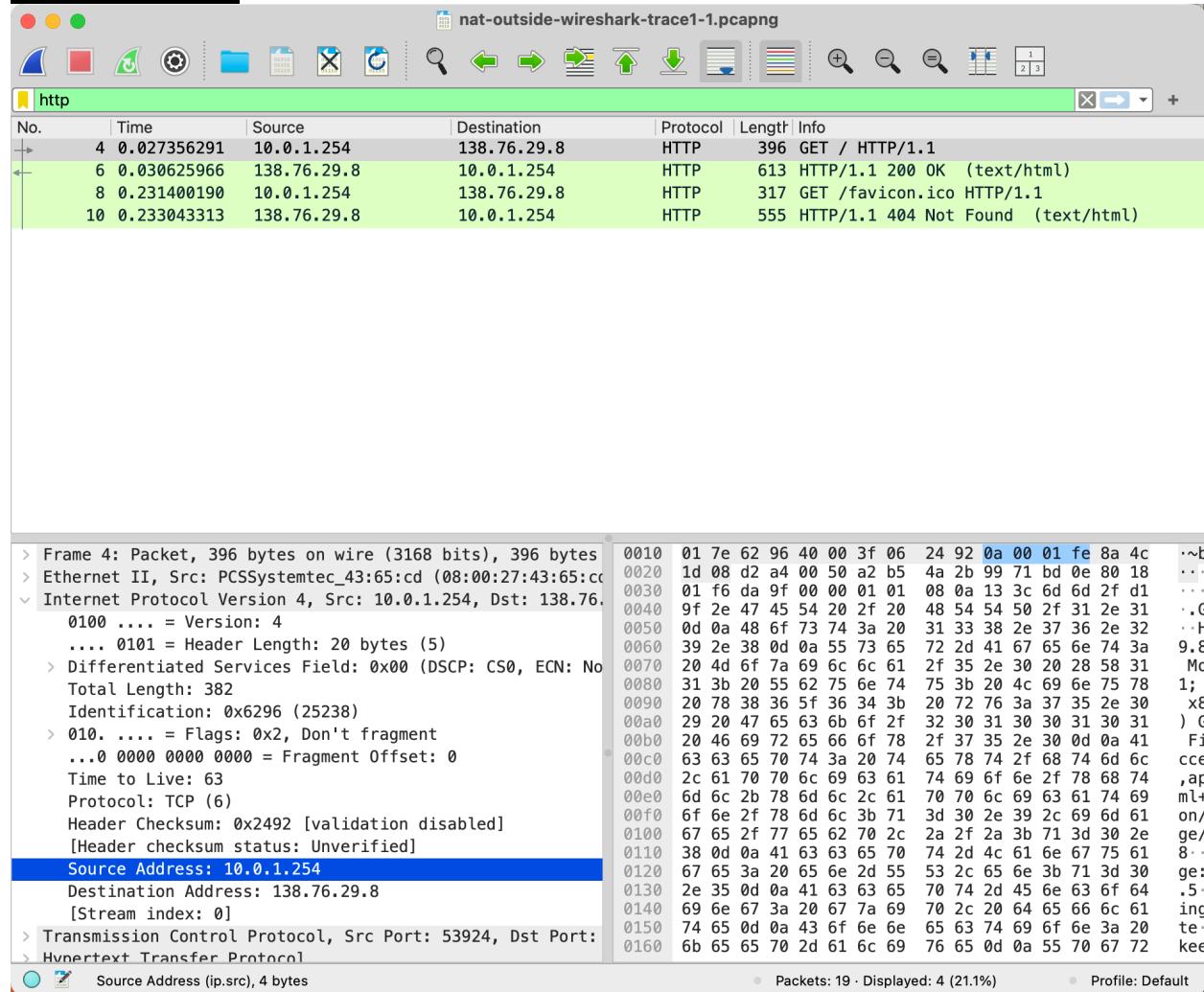
Source Port: 80  
Destination Port: 53924

## **Part B**

### **Question 4**

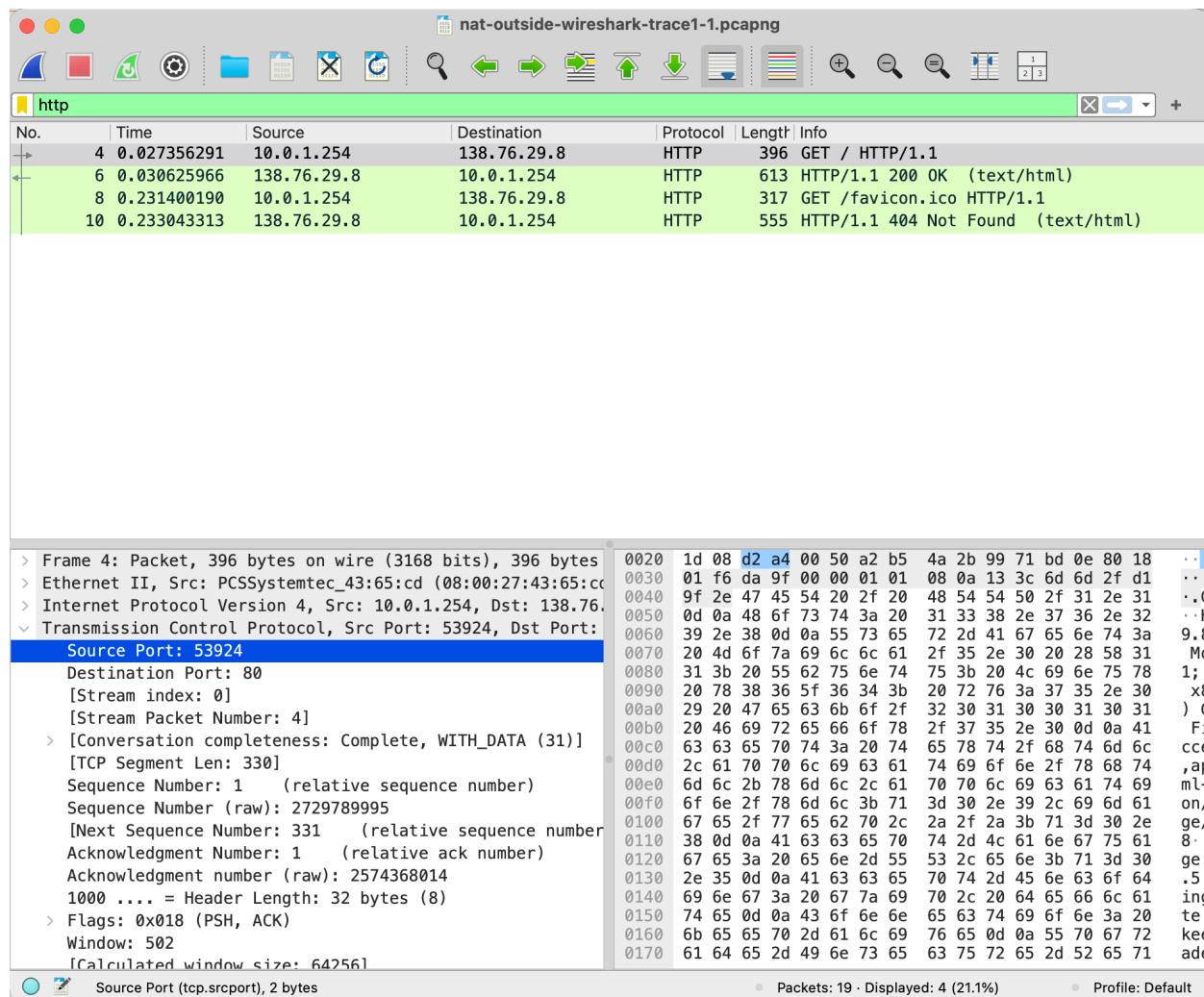
Time =0.027356291

## Question 5



Source Address: 10.0.1.254

Destination Address: 138.76.29.8



Source Port: 53924

Destination Port: 80

## Question 6

- Source IP changed
- Source port did NOT change
- Destination IP unchanged
- Destination port unchange

## Question 7

NAT does **not** modify HTTP payload data.

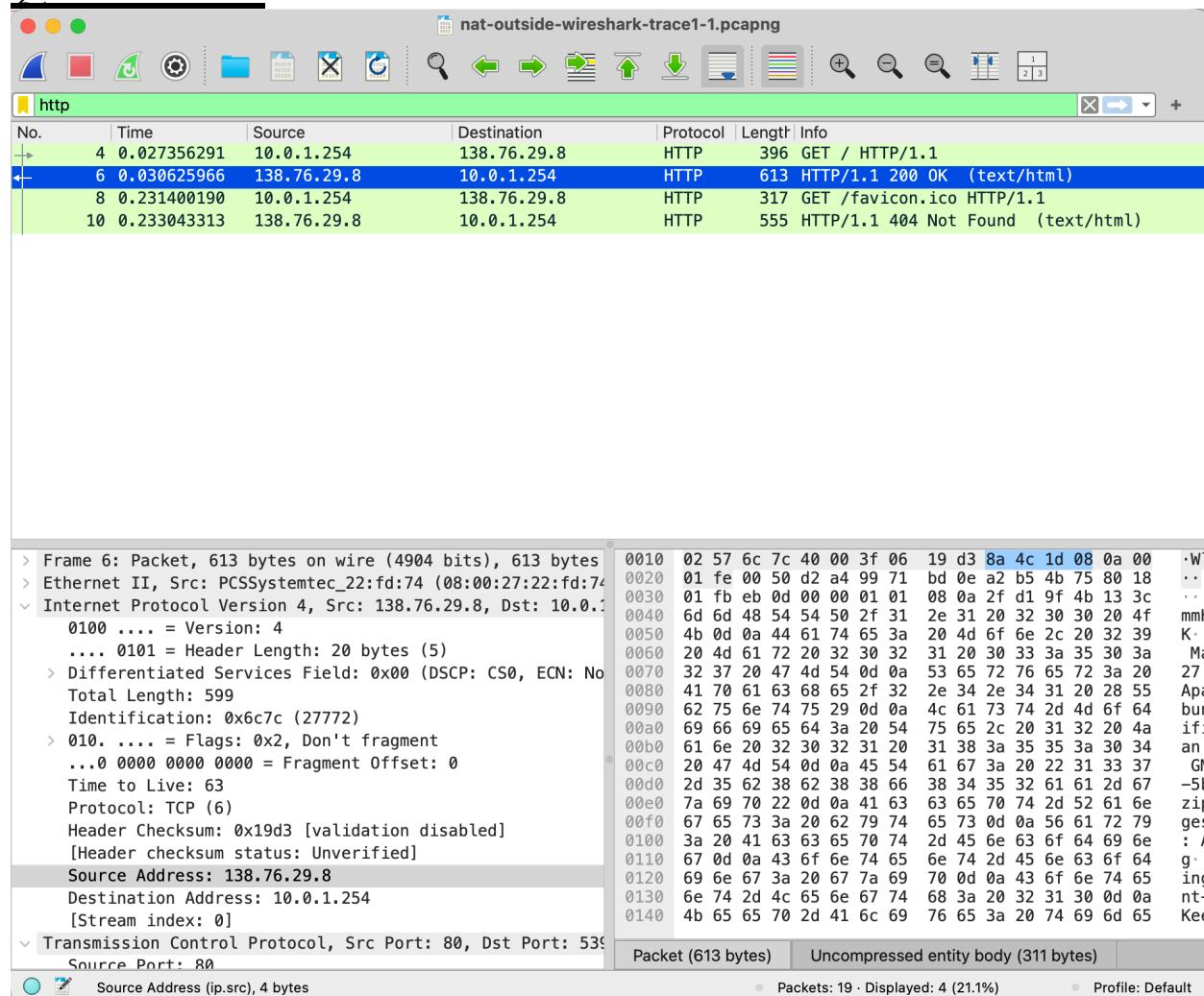
## Question 8

- IP Header Checksum
- TTL may also change (decremented by router)

## Question 9

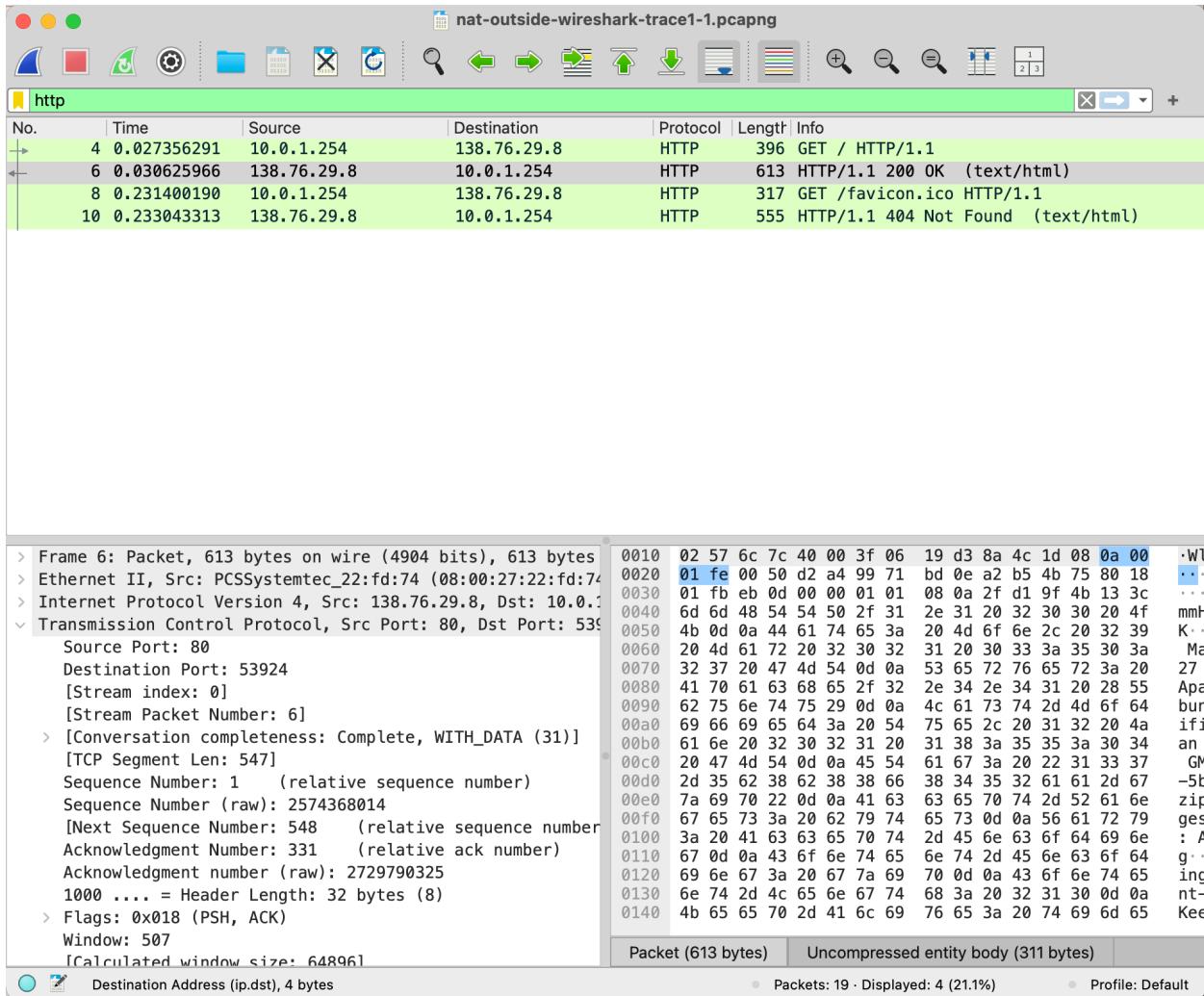
Time = 0.03625966

## Question 10



Source Address: 138.76.29.8

Destination Address: 10.0.1.254



Source Port: 80  
 Destination Port: 53924

## Part C

### Question 11

Source IP = 138.76.29.8  
Destination IP = 192.168.10.11  
Source Port = 80  
Destination Port = 53924