

## Lab 5: NAT

University of Windsor  
Department of Electrical and Computer Engineering  
ELEC 8560 – Computer Networks  
Semester: Fall 2023

**Student Name:** Amey Mahendra Thakur

**Student number:** 110107589

### Answers:

1. Client IP Address sending HTTP GET request: **192.168.10.11**  
Source Port Number of TCP segment for HTTP GET request: **53924**  
Destination IP Address for HTTP GET request: **138.76.29.8**  
Destination Port Number of TCP segment for HTTP GET request: **80**

The image shows a Wireshark packet capture analysis of a network trace. The main packet list on the left shows a series of packets. Packet 4, at time 0.02, is an HTTP GET request from source 192.168.10.11 to destination 138.76.29.8. Red arrows point to the source and destination IP addresses in this packet. The packet details pane on the right shows the structure of this packet. The Ethernet II section shows the source MAC as PcsCompu\_89:c7:7c and the destination MAC as PcsCompu\_82:36:d7. The Internet Protocol section shows the source IP as 192.168.10.11 and the destination IP as 138.76.29.8. The Transmission Control Protocol section shows the source port as 53924, the destination port as 80, and the sequence number as 1. The Hypertext Transfer Protocol section shows the request line as GET / HTTP/1.1. The packet bytes pane at the bottom shows the raw data of the packet, with the first few bytes corresponding to the Ethernet II header.

**AMEY MAHENDRA THAKUR**  
**110107589**

- The NAT router forwards the HTTP 200 OK message from the webserver to the client on the router's LAN side at approximately **0.030672101 seconds** into the trace, measured from the first captured packet.

Wireshark - Packet 6: nat-inside-wireshark-trace1-1.pcapng

Section number: 1

Interface id: 0 (eth1)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 28, 2021 23:50:27.774683377 Eastern Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1616989827.774683377 seconds

[Time delta from previous captured frame: 0.001281902 seconds]

[Time delta from previous displayed frame: 0.001281902 seconds]

**[Time since reference or first frame: 0.030672101 seconds]**

Frame Number: 6

Frame Length: 613 bytes (4904 bits)

Capture Length: 613 bytes (4904 bits)

[Frame is marked: False]

[Protocols in Frame: eth:ethertype:ip:tcp:http:data-text-lines]

[Coloring Rule Name: HTTP]

0000 08 00 27 89 c7 7c 08 00 27 82 36 d7 08 00 45 00 ...:|@-> \.L....  
 0010 02 57 6c 7c 40 00 3e 06 5c 1d 8a 4c 1d 08 c0 a8 ...P...q...Ku...  
 0020 0a 0b 00 50 d2 a4 99 71 bd 0e a2 b5 4b 75 80 18 ...X...-/-K<...  
 0030 01 fb 2c 58 00 00 01 01 08 0a 2f d1 9f 4b 13 3c ...mHTT/P.1.1 200 0  
 0040 6d 6d 4d 54 50 2f 31 2e 31 20 32 30 38 20 4f ...K-Date: Mon, 29  
 0050 4b 0d 0a 4d 61 74 65 3a 20 4d 6f 6e 2c 20 32 39 ...Mar 2021 03:50:  
 0060 2d 40 61 72 20 32 30 32 31 20 30 33 3a 35 30 3a ...27 GMT- Server:  
 0070 32 37 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 ...Apache/2.4.41 (U  
 0080 41 70 61 63 68 65 2f 32 2e 3a 2e 3a 31 20 28 55 ...buntu)- Last-Mod  
 0090 62 75 6e 74 75 29 0d 0a 4c 61 73 74 2d 4d 6f 64 ...ified: Tue, 12 J  
 00a0 69 66 69 65 64 3a 20 54 75 65 2c 20 31 32 20 4a ...an 2021 18:55:04  
 00b0 61 6e 20 32 30 32 31 20 31 38 3a 35 35 3a 30 3a ...GMT-ET ag: "137  
 00c0 20 47 4d 54 0d 0a 54 54 61 67 3a 20 22 31 33 37 ...-5b0b88f 8452aa-g  
 00d0 2d 35 62 38 62 38 38 66 38 34 35 32 61 61 2d 67 ...zip"-Ac cept-Ran  
 00e0 7a 69 70 22 0d 0a 41 63 63 65 70 74 2d 52 61 61 6e ...ges: byt es-Vary  
 00f0 67 65 73 3a 20 62 79 74 65 73 0d 0a 56 61 72 79 ...: Accept -Encodin  
 0100 3a 20 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e ...g-Conte nt-Encod  
 0110 67 0d 0a 43 6f 6e 74 65 6e 74 2d 45 6e 63 6f 64 ...ing: gzi p-Conte  
 0120 69 6e 67 3a 20 67 7a 69 70 0d 0a 43 6f 6e 74 65

- IP Datagram for HTTP 200 OK Message:

- Source IP/Port: **138.76.29.8 / 80**
- Destination IP/Port: **192.168.10.11 / 53924**

Wireshark - Packet 6: nat-inside-wireshark-trace1-1.pcapng

Frame 6: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth1, id 0

Ethernet II, Src: PcsCompu\_82:36:d7 (08:00:27:82:36:d7), Dst: PcsCompu\_89:c7:7c (08:00:27:89:c7:7c)

Internet Protocol Version 4, Src: 138.76.29.8, Dst: 192.168.10.11

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

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

Total Length: 599

Identification: 0x6c7c (27772)

010. .... = Flags: 0x2, Don't fragment

... 0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 62

Protocol: TCP (6)

Header Checksum: 0x5c1d [validation disabled]

[Header checksum status: Unverified]

Source Address: 138.76.29.8

Destination Address: 192.168.10.11

Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547

Source Port: 80

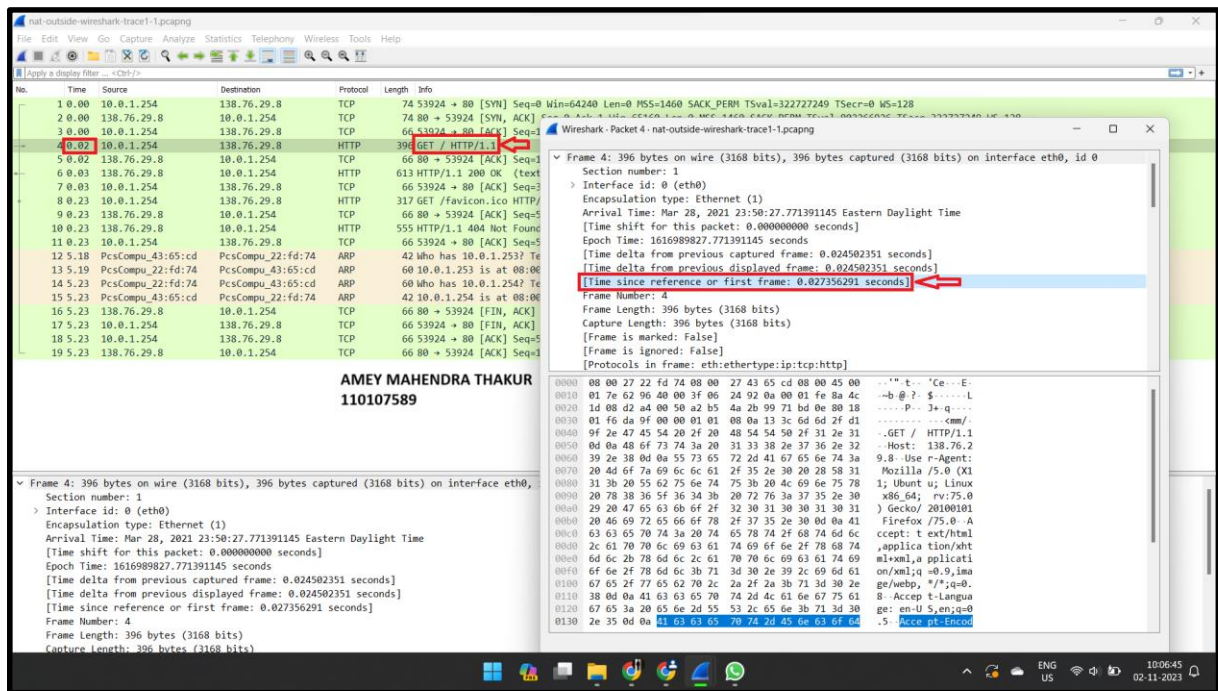
Destination Port: 53924

(Stream index: 0)

0000 08 00 27 89 c7 7c 08 00 27 82 36 d7 08 00 45 00 ...:|@-> \.L....  
 0010 02 57 6c 7c 40 00 3e 06 5c 1d 8a 4c 1d 08 c0 a8 ...P...q...Ku...  
 0020 0a 0b 00 50 d2 a4 99 71 bd 0e a2 b5 4b 75 80 18 ...X...-/-K<...  
 0030 01 fb 2c 58 00 00 01 01 08 0a 2f d1 9f 4b 13 3c ...mHTT/P.1.1 200 0  
 0040 6d 6d 4d 54 50 2f 31 2e 31 20 32 30 38 20 4f ...K-Date: Mon, 29  
 0050 4b 0d 0a 4d 61 74 65 3a 20 4d 6f 6e 2c 20 32 39 ...Mar 2021 03:50:  
 0060 2d 40 61 72 20 32 30 32 31 20 30 33 3a 35 30 3a ...27 GMT- Server:  
 0070 32 37 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 ...Apache/2.4.41 (U  
 0080 41 70 61 63 68 65 2f 32 2e 3a 2e 3a 31 20 28 55 ...buntu)- Last-Mod  
 0090 62 75 6e 74 75 29 0d 0a 4c 61 73 74 2d 4d 6f 64 ...ified: Tue, 12 J  
 00a0 69 66 69 65 64 3a 20 54 75 65 2c 20 31 32 20 4a ...an 2021 18:55:04  
 00b0 61 6e 20 32 30 32 31 20 31 38 3a 35 35 3a 30 3a ...GMT-ET ag: "137  
 00c0 20 47 4d 54 0d 0a 54 54 61 67 3a 20 22 31 33 37 ...-5b0b88f 8452aa-g  
 00d0 2d 35 62 38 62 38 38 66 38 34 35 32 61 61 2d 67 ...zip"-Ac cept-Ran

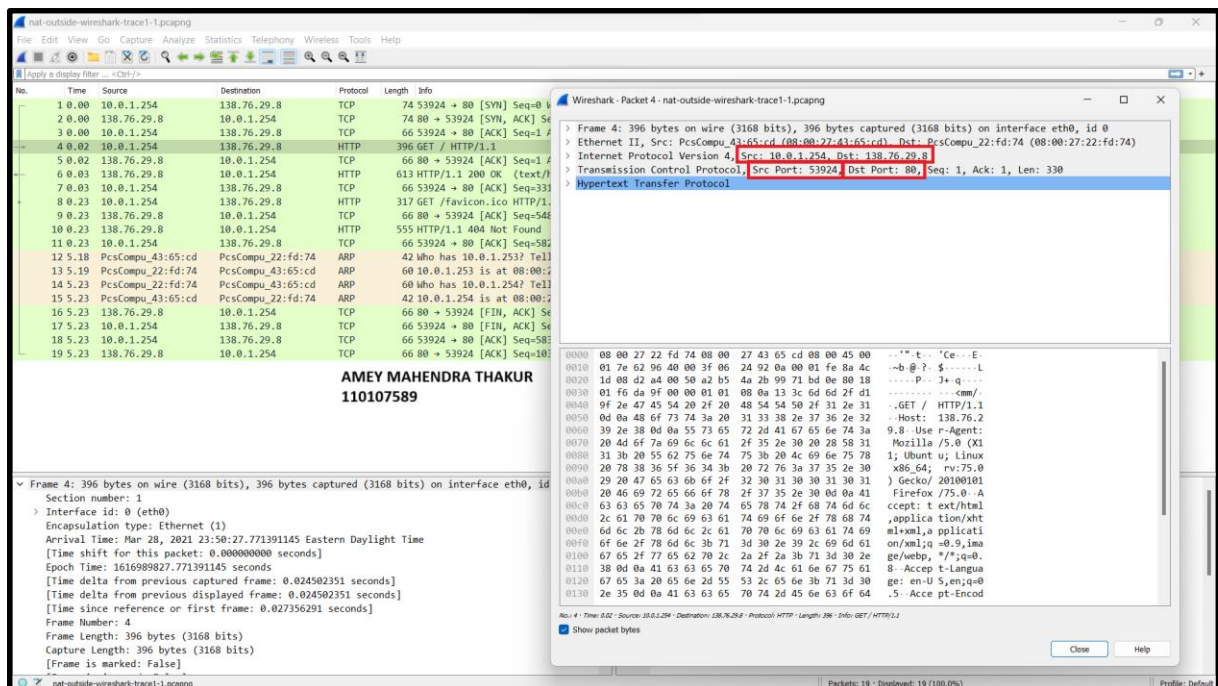


4. Time of Appearance of HTTP GET Message: The HTTP GET message appeared in the nat-outside-wireshark-trace1-1.pcapng trace file at around **0.027356291** seconds.

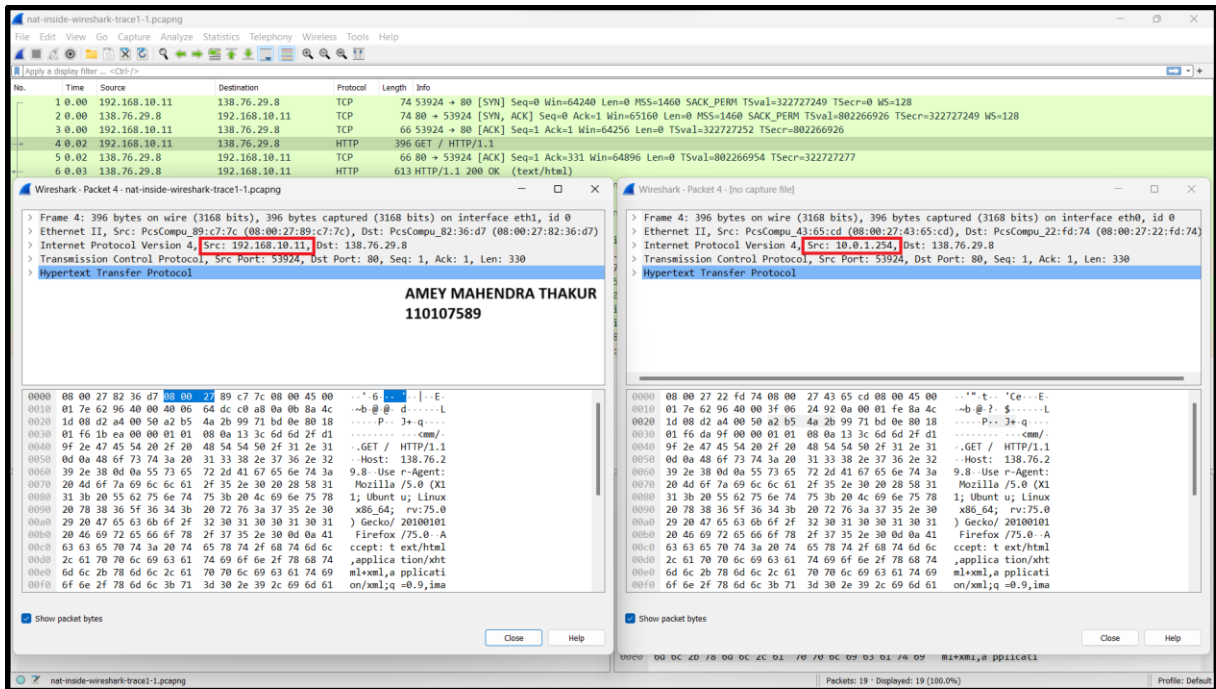


5. IP Datagram for HTTP GET Message in nat-outside-wireshark-trace1-1.pcapng:

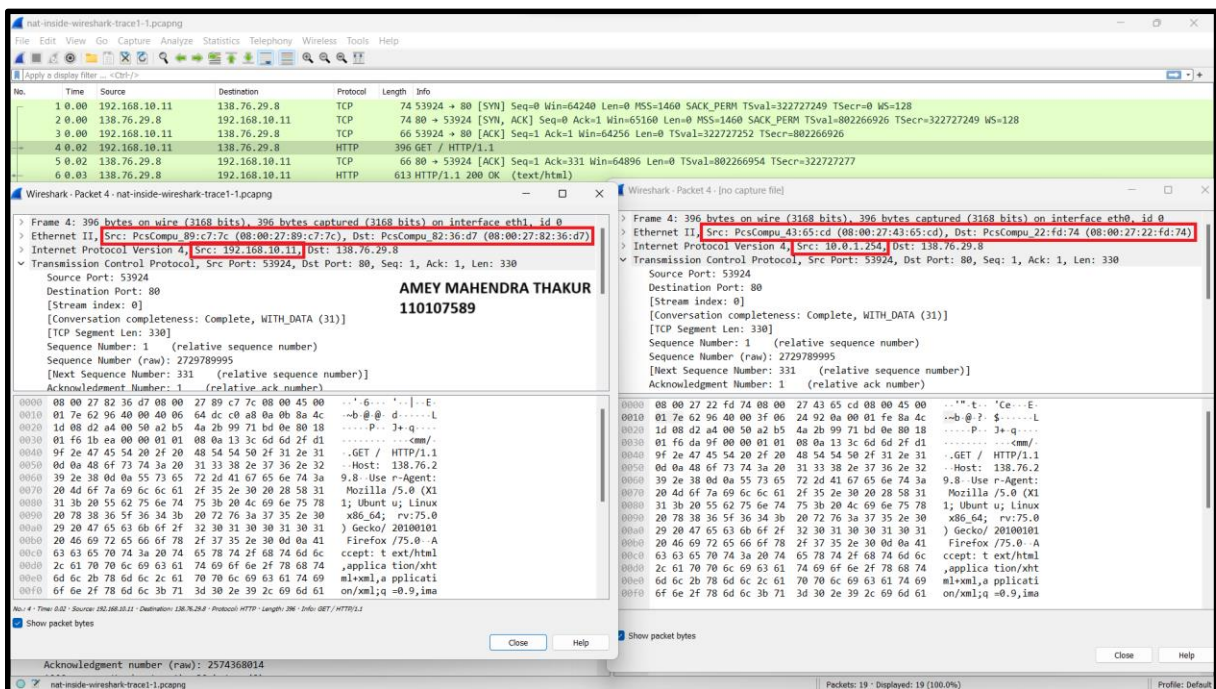
- Source IP/Port: **10.0.1.254 / 53924**
- Destination IP/Port: **138.76.29.8 / 80**



6. When comparing the HTTP GET messages from both files, the only difference I observed among the SRC IP, DST IP, SRC Port, and DST Port fields is that the **SRC IP address is different in both instances.**



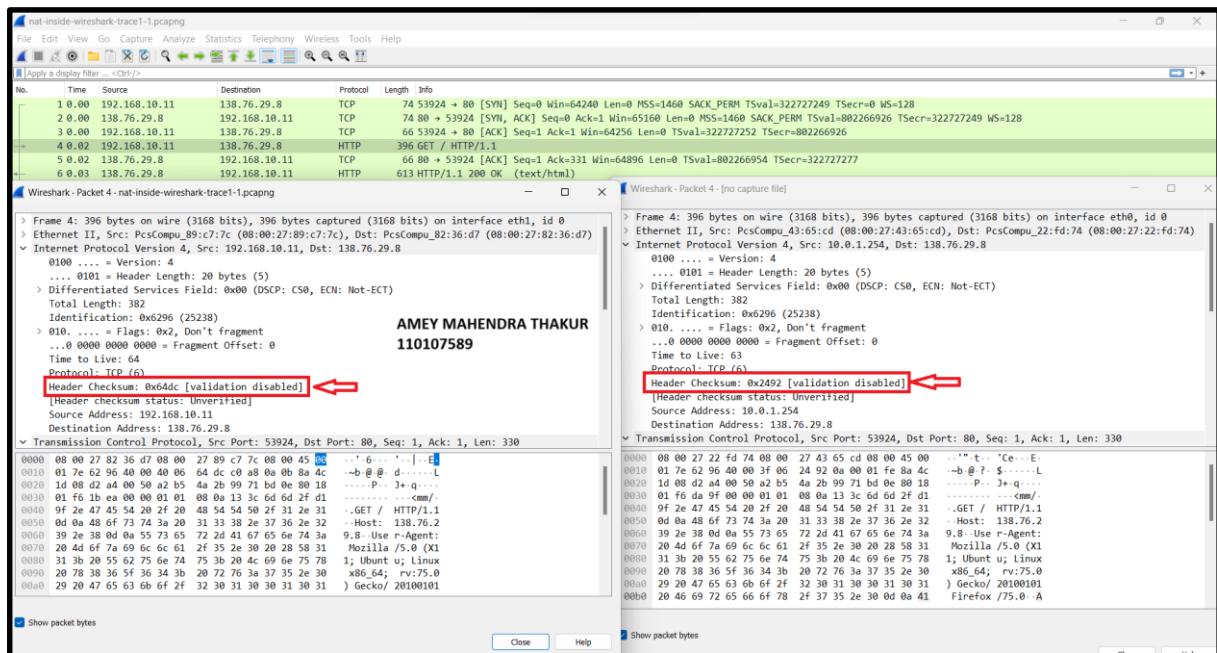
7. In addition to the previously mentioned change in the source IP address, there is also a modification in both the **source and destination MAC addresses** within the Ethernet datagram.



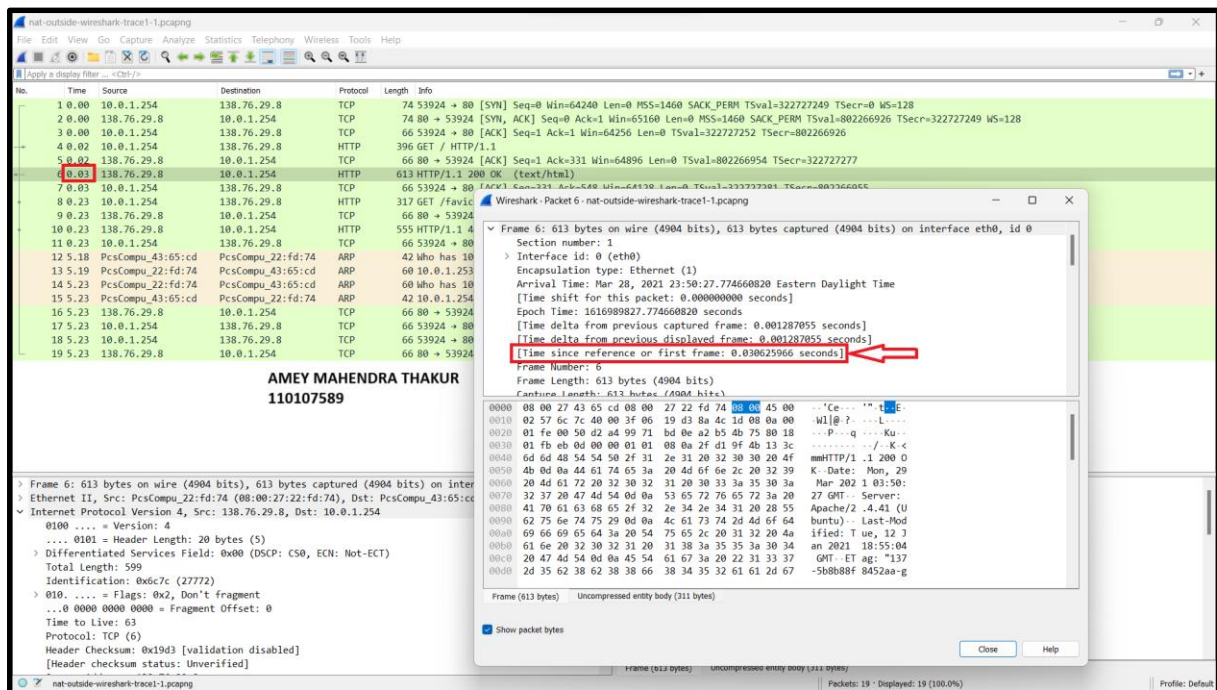
8. In the IP datagram carrying the HTTP GET, the Version, Header Length, and Flags fields remain consistent when comparing the datagram received on the local area network (inside) to



the corresponding datagram forwarded on the Internet side (outside) of the NAT router. However, there is a difference in the **Header Checksum** value between the two instances.

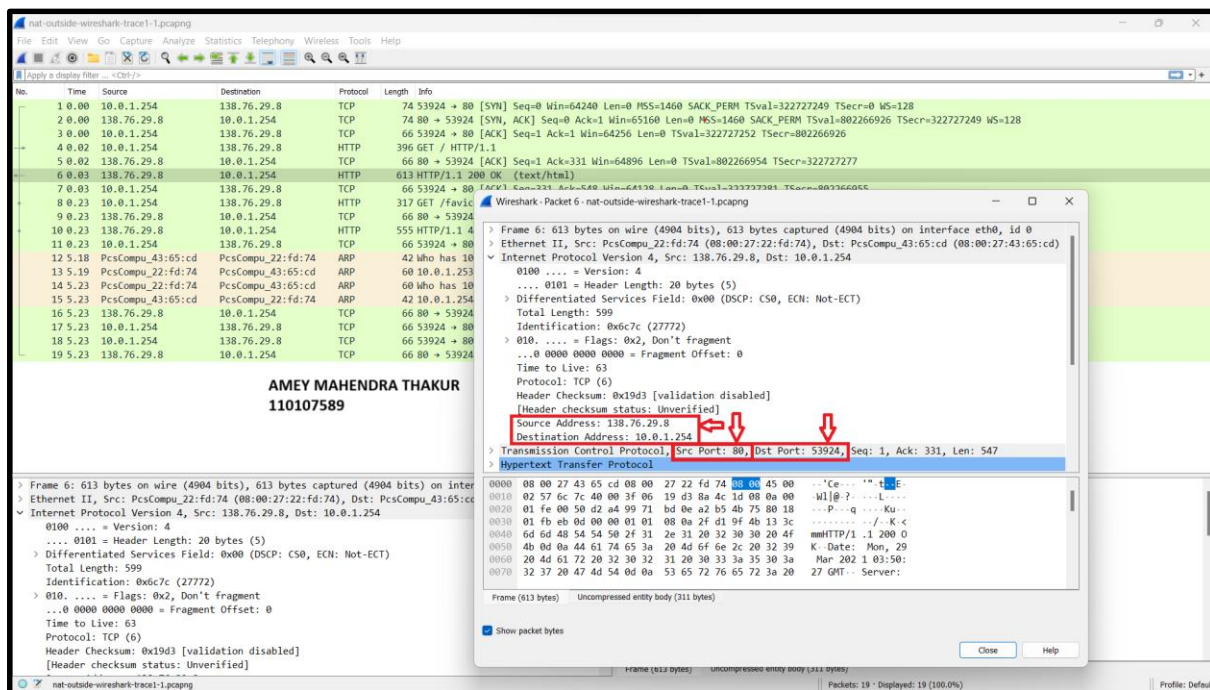


9. Time of Appearance of HTTP OK Message: The HTTP OK message appeared in the nat-outside-wireshark-trace1-1.pcapng trace file at around **0.030625966** seconds.



10. IP Datagram for HTTP Reply ("200 OK") Message in nat-outside-wireshark-trace1-1.pcapng:

- Source IP/Port: **138.76.29.8 / 80**
- Destination IP/Port: **10.0.1.254 / 53924**



## 11. IP Datagram for HTTP Reply ("200 OK") Forwarded to Destination Host:

- Source IP/Port: 138.76.29.8 / 80
- Destination IP/Port: 192.168.10.11 / 53924

