Lab Report

CSE351, Computer Networking

Name: Youssef Moustafa Elsayed   ID: 22P0047

Lab No: (8)   Experiment Title: Wireshark Lab: NAT

Date: 18 / 12 /2025

Answering Questions in textbook

1. What is the IP address of the client that sends the HTTP GET request in the natinside-wireshark-trace1-1.pcapng trace? What is the source port number of the TCP segment in this datagram containing the HTTP GET request? What is the destination IP address of this HTTP GET request? What is the destination port number of the TCP segment in this datagram containing the HTTP GET request?

Client IP address: 192.168.10.11

TCP source port: 53924

Destination IP address: 138.76.29.8

TCP destination port: 80

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 4: 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)
v 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]
v Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
    Source Port: 53924
    Destination Port: 80
```

2. At what time is the corresponding HTTP 200 OK message from the webserver forwarded by the NAT router to the client on the router's LAN side?

0.030672101 seconds

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)

3. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

Source IP address: 138.76.29.8

TCP source port: 80

Destination IP address: 192.168.10.11

TCP destination port: 53924

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 6: Packet, 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth1, id 0
> Ethernet II, Src: PCSSystemtec_82:36:d7 (08:00:27:82:36:d7), Dst: PCSSystemtec_89:c7:7c (08:00:27:89:c7:7c)
v Internet Protocol Version 4, Src: 138.76.29.8, Dst: 192.168.10.11
    0100 .... = Version: 4
    .... 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
    [Stream index: 0]
v Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
    Source Port: 80
    Destination Port: 53924
```

4. At what time does this HTTP GET message appear in the nat-outside-wiresharktrace1-1.pcapng trace file?

0.027356291 seconds

No.	Time	Source	Destination	Protocol	Lengtł	Info
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

5. What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying this HTTP GET (as recorded in the natoutside-wireshark-trace1-1.pcapng trace file)?

Source IP address: 10.0.1.254

TCP source port: 53924

Destination IP address: 138.76.29.8

TCP destination port: 80

No.	Time	Source	Destination	Protocol	Lengtł	Info
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

```
> Frame 4: Packet, 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth0, id 0
> Ethernet II, Src: PCSSystemtec_43:65:cd (08:00:27:43:65:cd), Dst: PCSSystemtec_22:fd:74 (08:00:27:22:fd:74)
v Internet Protocol Version 4, Src: 10.0.1.254, 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: 63
    Protocol: TCP (6)
    Header Checksum: 0x2492 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.1.254
    Destination Address: 138.76.29.8
    [Stream index: 0]
v Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
    Source Port: 53924
    Destination Port: 80
```

6. Which of these four fields are different than in your answer to question 1 above?

Only the source IP address is different.

Question 1 source IP address:

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 4: 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)
v 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]
v Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
     Source Port: 53924
     Destination Port: 80
```

Question 5 source IP address:

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

```
> Frame 4: Packet, 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth0, id 0
> Ethernet II, Src: PCSSystemtec_43:65:cd (08:00:27:43:65:cd), Dst: PCSSystemtec_22:fd:74 (08:00:27:22:fd:74)
v Internet Protocol Version 4, Src: 10.0.1.254, 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: 63
     Protocol: TCP (6)
     Header Checksum: 0x2492 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 10.0.1.254
     Destination Address: 138.76.29.8
     [Stream index: 0]
v Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
     Source Port: 53924
     Destination Port: 80
```

7. Are any fields in the HTTP GET message changed?

No. The HTTP GET message is not changed by NAT.

8. Which of the following fields in the IP datagram carrying the HTTP GET are changed from the datagram received on the local area network (inside) to the corresponding datagram forwarded on the Internet side (outside) of the NAT router: Version, Header Length, Flags, Checksum?

Only the IP header checksum is changed.

Nat inside Header Checksum:

Nat outside Header Checksum:

9. At what time does this message appear in the nat-outside-wireshark-trace1- 1.pcapng trace file?

0.030625966 seconds

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

10. What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying this HTTP reply ("200 OK") message (as recorded in the nat-outside-wireshark-trace1-1.pcapng trace file)?

Source IP address: 138.76.29.8

TCP source port: 80

Destination IP address: 10.0.1.254

TCP destination port: 53924

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

```
> Frame 6: Packet, 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth0, id 0
> Ethernet II, Src: PCSSystemtec_22:fd:74 (08:00:27:22:fd:74), Dst: PCSSystemtec_43:65:cd (08:00:27:43:65:cd)
v Internet Protocol Version 4, Src: 138.76.29.8, Dst: 10.0.1.254
    0100 .... = Version: 4
    .... 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: 63
    Protocol: TCP (6)
    Header Checksum: 0x19d3 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 138.76.29.8
    Destination Address: 10.0.1.254
    [Stream index: 0]
v Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
    Source Port: 80
    Destination Port: 53924
```

11. What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying the HTTP reply ("200 OK") that is forwarded from the router to the destination host in the right of Figure 1?

Source IP address: 138.76.29.8

TCP source port: 80

Destination IP address: 192.168.10.11

TCP destination port: 53924