# Wireshark Lab: NAT v8.1

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.,* J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

In this lab, we'll investigate the behavior of a NAT router. This lab will be different from our other Wireshark labs, where we've captured a trace file at a single Wireshark measurement point. Because we're interested in capturing packets at *both* the input and output sides of the NAT device, we'll need to capture packets at *two* locations. Also, because many students don't have easy access to a NAT device or to two computers on which to take Wireshark measurements, this isn't a lab that is easily done "live" by a student. So, in this lab, you'll use Wireshark trace files that we've captured for you. This should be a relatively short and easy lab since the concepts behind NAT aren't difficult, but it'll be good nonetheless to observe NAT in action. Before beginning this lab, you'll probably want to review the material on NAT in section 4.3.3 in the text[1].

NAT Measurement Scenario

In this lab, we'll capture packets containing a simple HTTP GET request message from a client inside a home network to a remote server, and the corresponding HTTP response from that server. Within the home network, the home network router provides a NAT service, as discussed in Chapter 4. Figure 1 shows our Wireshark trace-collection scenario. We'll capture packets in *two* locations, and thus this lab has *two* trace files:

- We'll capture packets being received at the local area network (LAN) side of the NAT router. All devices in this LAN have addresses in 192.168.10/24. This file is named *nat-<u>inside</u>-wireshark-trace1-1.pcapng* [2].

---

[1] References to figures and sections are for the 8th edition of our text, *Computer Networks, A Top-down Approach, 8th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2020.* Our website for this book is http://gaia.cs.umass.edu/kurose_ross You'll find lots of interesting open material there.

[2] You can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip and extract the trace file *nat-inside-wireshark-trace1-1.pcapng*. These trace files can be used to answer these Wireshark lab questions without actually capturing packets on your own. Each trace was made using Wireshark running on one of the author's computers, while performing the steps indicated in the Wireshark lab. Once you've downloaded a trace file, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the trace file name.

- Because we're also interested in analyzing packets being forwarded (and received) by the NAT router on its Internet-facing side, we'll collect a second trace file on the Internet side of the router, as shown in Figure 1. Packets captured by Wireshark at this point that were sent from a host on the right to the server on the left will have undergone NAT translation by the time they reach this second measurement point. This file is named *nat-outside-wireshark-trace1-1.pcapng*.
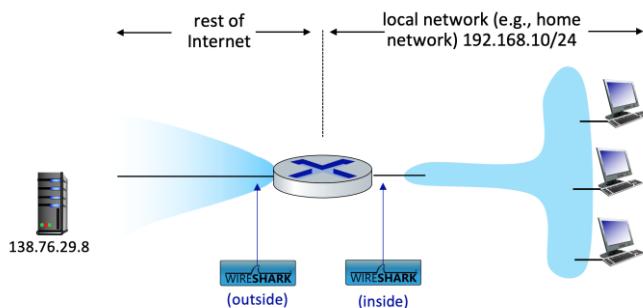

Figure 1: NAT packet capture scenario

In the scenario shown in Figure 1, one of the hosts within the LAN will send an HTTP GET request to the web server at IP address 138.76.29.8, which will respond back to the requesting host. Of course, we're not really interested in the HTTP GET request itself, but rather how the NAT router changes the IP addresses and port numbers of the datagram containing the GET request on the LAN side (inside) to addresses and port numbers in the fowarded outgoing datagram on the Internet side (outside) of the NAT router.

Let's first take a look at what's happening on the LAN side of the NAT router. Open the *nat-inside-wireshark-trace1-1.pcapng* trace file. In this file, you should see an HTTP GET request addressed to the external web server at IP address 138.76.29.8, as well as the subsequent HTTP response message ("200 OK"). Both of these messages in the trace file were captured on the LAN side of the router.

Answer the following questions[3].

1. What is the IP address of the client that sends the HTTP GET request in the *nat-inside-wireshark-trace1-1.pcapng* trace?
   The IP address is 192.168.10.11

---

[3] For the author's class, when answering the following questions with hand-in assignments, students sometimes need to print out specific packets (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the packet they've found the information that answers a question. They do this by marking paper copies with a pen or annotating electronic copies with text in a colored font. There are also learning management system (LMS) modules for teachers that allow students to answer these questions online and have answers auto-graded for these Wireshark labs at http://gaia.cs.umass.edu/kurose_ross/lms.htm

```
 4 10:50:27.7713…  192.168.10.11       138.76.29.8        HTTP   396 GET / HTTP/1.1
 5 10:50:27.7734…  138.76.29.8         192.168.10.11      TCP     66 80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277
 6 10:50:27.7746…  138.76.29.8         192.168.10.11      HTTP   613 HTTP/1.1 200 OK  (text/html)
 7 10:50:27.7754…  192.168.10.11       138.76.29.8        TCP     66 53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955
 8 10:50:27.9754…  192.168.10.11       138.76.29.8        HTTP   317 GET /favicon.ico HTTP/1.1
 9 10:50:27.9769…  138.76.29.8         192.168.10.11      TCP     66 80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481
10 10:50:27.9770…  138.76.29.8         192.168.10.11      HTTP   555 HTTP/1.1 404 Not Found  (text/html)
11 10:50:27.9777…  192.168.10.11       138.76.29.8        TCP     66 53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158
12 10:50:32.9337…  PcsCompu_82:36:d7   PcsCompu_89:c7:7c  ARP     42 Who has 192.168.10.11? Tell 192.168.10.254
13 10:50:32.9358…  PcsCompu_89:c7:7c   PcsCompu_82:36:d7  ARP     60 192.168.10.11 is at 08:00:27:89:c7:7c
14 10:50:32.9785…  138.76.29.8         192.168.10.11      TCP     66 80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TSval=802272158 TSecr=322727483
15 10:50:32.9787…  192.168.10.11       138.76.29.8        TCP     66 53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322732484 TSecr=802267158
16 10:50:32.9801…  192.168.10.11       138.76.29.8        TCP     66 53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TSval=322732485 TSecr=802272158
17 10:50:32.9820…  138.76.29.8         192.168.10.11      TCP     66 80 → 53924 [ACK] Seq=1038 Ack=583 Win=64768 Len=0 TSval=802272161 TSecr=322732484
18 10:50:32.9857…  PcsCompu_89:c7:7c   PcsCompu_82:36:d7  ARP     60 Who has 192.168.10.254? Tell 192.168.10.11
19 10:50:32.9857…  PcsCompu_82:36:d7   PcsCompu_89:c7:7c  ARP     42 192.168.10.254 is at 08:00:27:82:36:d7
```

 What is the source port number of the TCP segment in this datagram containing the HTTP GET request?

The source port number is 53924

```
 4 10:50:27.7713…  192.168.10.11       138.76.29.8        HTTP   396 GET / HTTP/1.1
 5 10:50:27.7734…  138.76.29.8         192.168.10.11      TCP     66 80 → 53924 [ACK] Seq=1 Ack
 6 10:50:27.7746…  138.76.29.8         192.168.10.11      HTTP   613 HTTP/1.1 200 OK  (text/htm
 7 10:50:27.7754…  192.168.10.11       138.76.29.8        TCP     66 53924 → 80 [ACK] Seq=331 A
 8 10:50:27.9754…  192.168.10.11       138.76.29.8        HTTP   317 GET /favicon.ico HTTP/1.1
 9 10:50:27.9769…  138.76.29.8         192.168.10.11      TCP     66 80 → 53924 [ACK] Seq=548 A
10 10:50:27.9770…  138.76.29.8         192.168.10.11      HTTP   555 HTTP/1.1 404 Not Found  (t
11 10:50:27.9777…  192.168.10.11       138.76.29.8        TCP     66 53924 → 80 [ACK] Seq=582 A
12 10:50:32.9337…  PcsCompu_82:36:d7   PcsCompu_89:c7:7c  ARP     42 Who has 192.168.10.11? Tel
13 10:50:32.9358…  PcsCompu_89:c7:7c   PcsCompu_82:36:d7  ARP     60 192.168.10.11 is at 08:00:
14 10:50:32.9785…  138.76.29.8         192.168.10.11      TCP     66 80 → 53924 [FIN, ACK] Seq=
15 10:50:32.9787…  192.168.10.11       138.76.29.8        TCP     66 53924 → 80 [FIN, ACK] Seq=
16 10:50:32.9801…  192.168.10.11       138.76.29.8        TCP     66 53924 → 80 [ACK] Seq=583 A
17 10:50:32.9820…  138.76.29.8         192.168.10.11      TCP     66 80 → 53924 [ACK] Seq=1038
18 10:50:32.9857…  PcsCompu_89:c7:7c   PcsCompu_82:36:d7  ARP     60 Who has 192.168.10.254? Te
19 10:50:32.9857…  PcsCompu_82:36:d7   PcsCompu_89:c7:7c  ARP     42 192.168.10.254 is at 08:00
```

```
> Frame 4: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth1, id 0
> Ethernet II, Src: PcsCompu_89:c7:7c (08:00:27:89:c7:7c), Dst: PcsCompu_82:36:d7 (08:00:27:82:36:d7)
> Internet Protocol Version 4, Src: 192.168.10.11, Dst: 138.76.29.8
> Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
> Hypertext Transfer Protocol
```

 What is the destination IP address of this HTTP GET request?

The destination IP address is 138.76.29.8

 What is the destination port number of the TCP segment in this datagram containing the HTTP GET request?

The destination IP port is 80

2. At what time[4] is the corresponding HTTP 200 OK message from the webserver forwarded by the NAT router to the client on the router's LAN side?

   GET time: 10:50:27,774683377
   200 OK time: 10:50:27,771373521
   ➔ **It receives after 0,003309856s**

---

[4] Specify time using the time since the beginning of the trace (rather than absolute, wall-clock time).

```
 6 10:50:27.7746… 138.76.29.8      192.168.10.11     HTTP    613 HTTP/1.1 200 OK  (text/html)
 7 10:50:27.7754… 192.168.10.11    138.76.29.8       TCP      66 53924 → 80 [ACK] Seq=331 Ack=54{
 8 10:50:27.9754… 192.168.10.11    138.76.29.8       HTTP    317 GET /favicon.ico HTTP/1.1
 9 10:50:27.9769… 138.76.29.8      192.168.10.11     TCP      66 80 → 53924 [ACK] Seq=548 Ack=58.
10 10:50:27.9770… 138.76.29.8      192.168.10.11     HTTP    555 HTTP/1.1 404 Not Found  (text/h
11 10:50:27.9777… 192.168.10.11    138.76.29.8       TCP      66 53924 → 80 [ACK] Seq=582 Ack=10:
12 10:50:32.9337… PcsCompu_82:36:d7 PcsCompu_89:c7:7c ARP     42 Who has 192.168.10.11? Tell 192
13 10:50:32.9358… PcsCompu_89:c7:7c PcsCompu_82:36:d7 ARP     60 192.168.10.11 is at 08:00:27:89
14 10:50:32.9785… 138.76.29.8      192.168.10.11     TCP      66 80 → 53924 [FIN, ACK] Seq=1037 /
15 10:50:32.9787… 192.168.10.11    138.76.29.8       TCP      66 53924 → 80 [FIN, ACK] Seq=582 A
16 10:50:32.9801… 192.168.10.11    138.76.29.8       TCP      66 53924 → 80 [ACK] Seq=583 Ack=10:
17 10:50:32.9820… 138.76.29.8      192.168.10.11     TCP      66 80 → 53924 [ACK] Seq=1038 Ack=5{
18 10:50:32.9857… PcsCompu_89:c7:7c PcsCompu_82:36:d7 ARP     60 Who has 192.168.10.254? Tell 19:
19 10:50:32.9857… PcsCompu_82:36:d7 PcsCompu_89:c7:7c ARP     42 192.168.10.254 is at 08:00:27:8:
```

```
  ETag: "137-5b8b88f8452aa-gzip"\r\n
  Accept-Ranges: bytes\r\n
  Vary: Accept-Encoding\r\n
  Content-Encoding: gzip\r\n
> Content-Length: 210\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.003309856 seconds]
  [Request in frame: 4]
  [Next request in frame: 8]
  [Next response in frame: 10]
```

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?
   The source and destination IP addresses: 138.76.29.8 & 192.168.10.11
   The TCP source and destination ports: 80 & 53924

```
 3 2021-03-29 10:50:27.746882193 192.168.10.11    138.76.29.8      TCP      66 53924 → 80 [ACK] Seq=1 Ack=1 Wii
 4 2021-03-29 10:50:27.771373521 192.168.10.11    138.76.29.8      HTTP    396 GET / HTTP/1.1
 5 2021-03-29 10:50:27.773401475 138.76.29.8      192.168.10.11    TCP      66 80 → 53924 [ACK] Seq=1 Ack=331 |
 6 2021-03-29 10:50:27.774683377 138.76.29.8      192.168.10.11    HTTP    613 HTTP/1.1 200 OK  (text/html)
 7 2021-03-29 10:50:27.775476121 192.168.10.11    138.76.29.8      TCP      66 53924 → 80 [ACK] Seq=331 Ack=54{
 8 2021-03-29 10:50:27.975418697 192.168.10.11    138.76.29.8      HTTP    317 GET /favicon.ico HTTP/1.1
 9 2021-03-29 10:50:27.976907865 138.76.29.8      192.168.10.11    TCP      66 80 → 53924 [ACK] Seq=548 Ack=58.
10 2021-03-29 10:50:27.977085738 138.76.29.8      192.168.10.11    HTTP    555 HTTP/1.1 404 Not Found  (text/h
```

```
> 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
> Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
> Hypertext Transfer Protocol
> Line-based text data: text/html (12 lines)
```

In the following we'll focus on these two HTTP messages (GET and 200 OK). Our goal below will be to locate these two HTTP messages in the trace file *nat-outside-wireshark-trace1-1.pcapng*, captured on the Internet-side link between the router and the ISP. Because the captured packets heading towards the server will have already been forwarded through the NAT router, some of the IP address and port numbers will have been changed as a result of NAT translation.

Open the trace file *nat-outside-wireshark-trace1-1.pcapng.* Note that the time stamps in this file and the *nat-inside-wireshark-trace1-1.pcapng* file are not necessarily synchronized.

In the *nat-outside-wireshark-trace1-1.pcapng* trace file, find the HTTP GET message that corresponds to the HTTP GET message that was sent from the client to the 138.76.29.8 server at time *t*=0.27362245, where *t*=0.27362245 is the time at which this message was sent, as recorded in the *nat-inside-wireshark-trace1-1.pcapng* trace file.

4. At what time does this HTTP GET message appear in the *nat-outside-wireshark-trace1-1.pcapng* trace file?
   10:50:27,771391145

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 *nat-outside-wireshark-trace1-1.pcapng* trace file)?
   The source and destination IP addresses: 10.0.1.254 & 138.76.29.8
   The TCP source and destination ports: 53924 & 80

3 2021-03-29 10:50:27.746888794	10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK]
4 2021-03-29 10:50:27.771391145	10.0.1.254	138.76.29.8	HTTP	396 GET / HTTP/1.1
5 2021-03-29 10:50:27.773373765	138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [ACK]
6 2021-03-29 10:50:27.774660820	138.76.29.8	10.0.1.254	HTTP	613 HTTP/1.1 200 OK
7 2021-03-29 10:50:27.775483524	10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK]
8 2021-03-29 10:50:27.975435044	10.0.1.254	138.76.29.8	HTTP	317 GET /favicon.ico
9 2021-03-29 10:50:27.976898464	138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [ACK]
10 2021-03-29 10:50:27.977078167	138.76.29.8	10.0.1.254	HTTP	555 HTTP/1.1 404 Not

```
▸ Frame 4: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_43:65:cd (08:00:27:43:65:cd), Dst: PcsCompu_22:fd:74 (08:00:27:22:fd:74)
▸ Internet Protocol Version 4, Src: 10.0.1.254, Dst: 138.76.29.8
▸ Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
▸ Hypertext Transfer Protocol
```
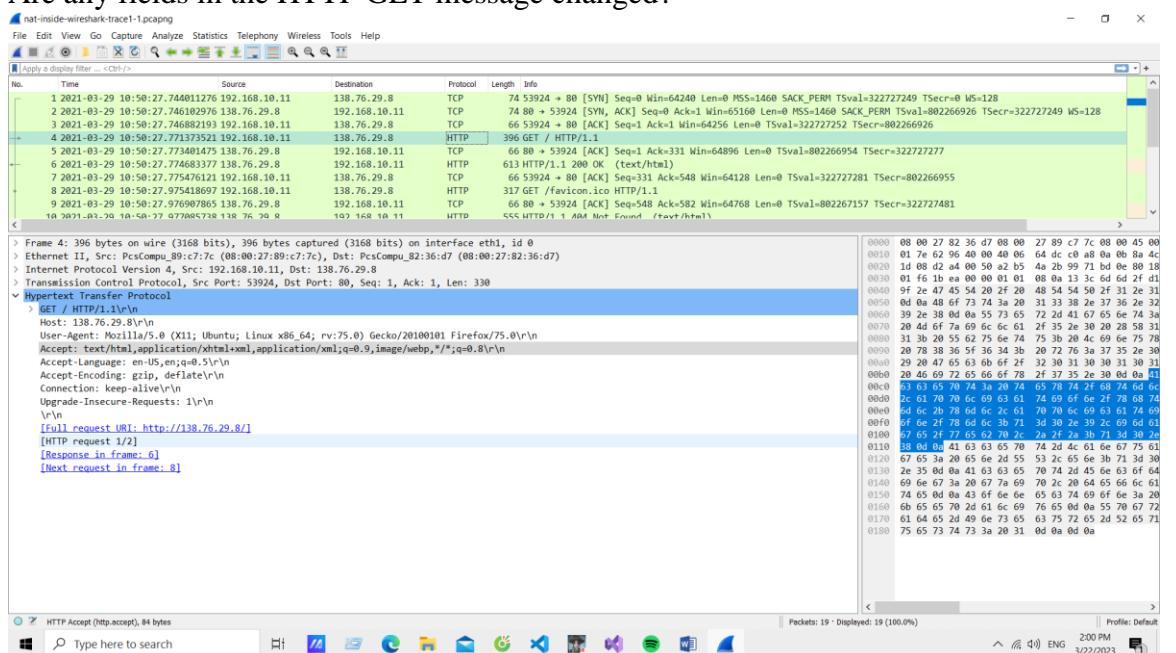
6. Which of these four fields are different than in your answer to question 1 above?
   The source and destination IP addresses
   inside: 192.168.10.11 & 138.76.29.8
   outside: 10.0.1.254 & 138.76.29.8
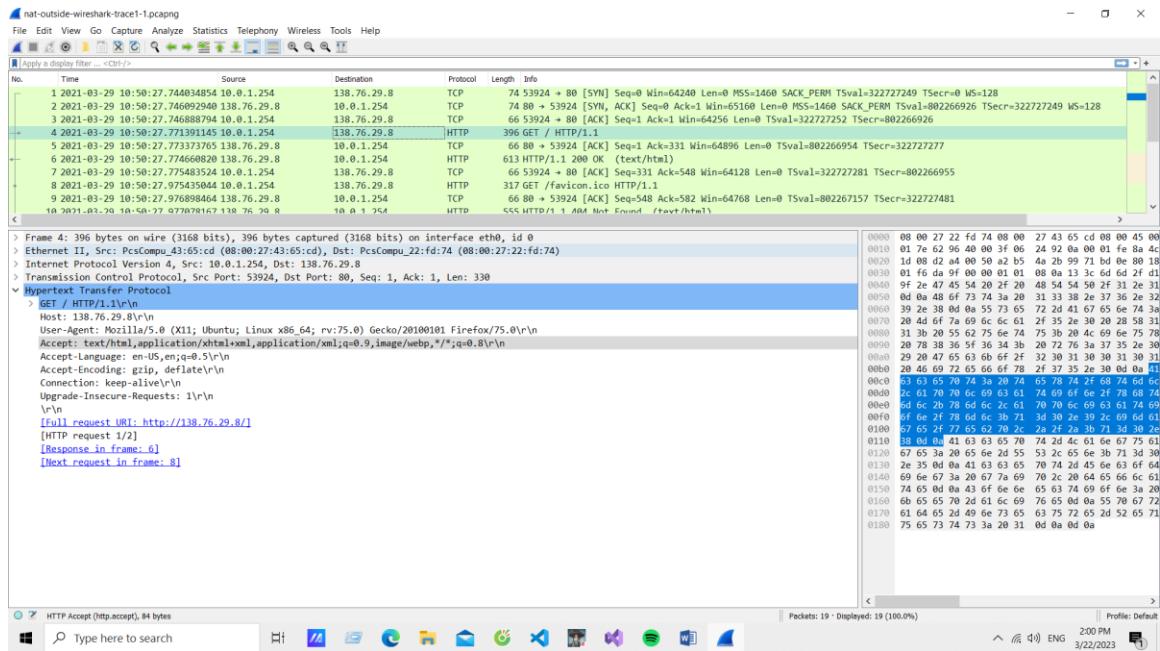
7. Are any fields in the HTTP GET message changed?

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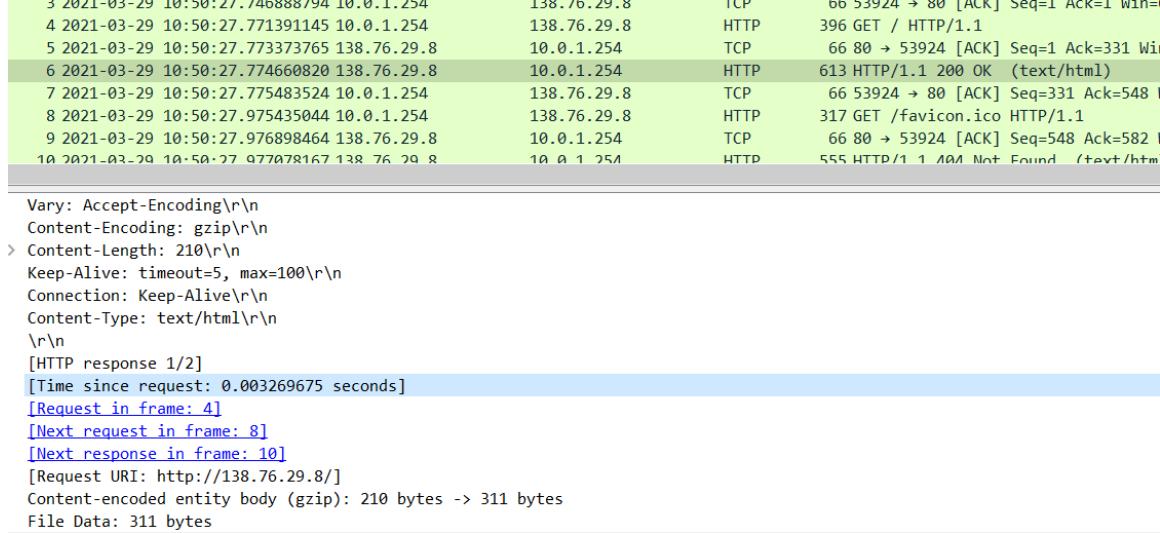
8. Which of the following fields in the IP datagram carrying the HTTP GET are changed from the datagram received on the local area network (inside) to the corresponding datagram forwarded on the Internet side (outside) of the NAT router: Version, Header Length, Flags, Checksum?

The Source IP has changed resulting in the Checksum changing as this contains the Source IP within it

Let's continue to look at the *nat-outside-wireshark-trace1-1.pcapng* trace file. Find the HTTP reply containing the "200 OK" message that was received in response to the HTTP GET request you just examined in questions 4-8 above.

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

It receive at 10:50:27.774660820 and the GET time is 10:50:27.771391145 -> received after 0.003269675

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)?
The source and destination IP addresses: 138.76.29.8 & 10.0.1.254
The TCP source and destination port: 80 & 53924

```
  3 2021-03-29 10:50:27.746888794 10.0.1.254      138.76.29.8     TCP    66 53924 → 80 [ACK] Seq=1 Ack=1 Win
  4 2021-03-29 10:50:27.771391145 10.0.1.254      138.76.29.8     HTTP   396 GET / HTTP/1.1
  5 2021-03-29 10:50:27.773373765 138.76.29.8     10.0.1.254      TCP    66 80 → 53924 [ACK] Seq=1 Ack=331 W
  6 2021-03-29 10:50:27.774660820 138.76.29.8     10.0.1.254      HTTP   613 HTTP/1.1 200 OK  (text/html)
  7 2021-03-29 10:50:27.775483524 10.0.1.254      138.76.29.8     TCP    66 53924 → 80 [ACK] Seq=331 Ack=548
  8 2021-03-29 10:50:27.975435044 10.0.1.254      138.76.29.8     HTTP   317 GET /favicon.ico HTTP/1.1
  9 2021-03-29 10:50:27.976898464 138.76.29.8     10.0.1.254      TCP    66 80 → 53924 [ACK] Seq=548 Ack=582
 10 2021-03-29 10:50:27.977078167 138.76.29.8     10.0.1.254      HTTP   555 HTTP/1.1 404 Not Found  (text/ht
<
> Frame 6: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth0, id 0
> Ethernet II, Src: PcsCompu_22:fd:74 (08:00:27:22:fd:74), Dst: PcsCompu_43:65:cd (08:00:27:43:65:cd)
> Internet Protocol Version 4, Src: 138.76.29.8, Dst: 10.0.1.254
> Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
> Hypertext Transfer Protocol
> Line-based text data: text/html (12 lines)
```

Lastly, let's consider what happens when the NAT router receives this datagram that you examined in questions 9 and 10, performs NAT translation, and finally forwards that datagram to the destination host on the LAN side. Based on your answers to questions 1 through 10 above and your knowledge of how NAT works, you should be able to answer the following question without actually looking at the *nat-inside-wireshark-trace1-1.pcapng* trace file:

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?
IP address 138.76.29.8 and 192.168.10.24

Just to make sure you understand NAT, you should now use Wireshark to peek into the *nat-inside-wireshark-trace1-1.pcapng* trace file at look at the HTTP reply ("200 OK"). Do your answers to question 11 above match what you see in the *nat-inside-wireshark-trace1-1.pcapng* trace file? [Hopefully, your answer is yes ☺].

That's it! See, we told you this Wireshark NAT lab wasn't going to be hard!