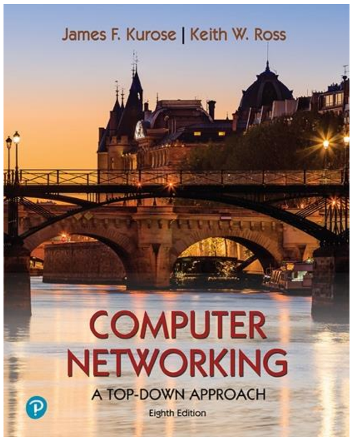
2151013087

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-inside-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, 8h 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*.

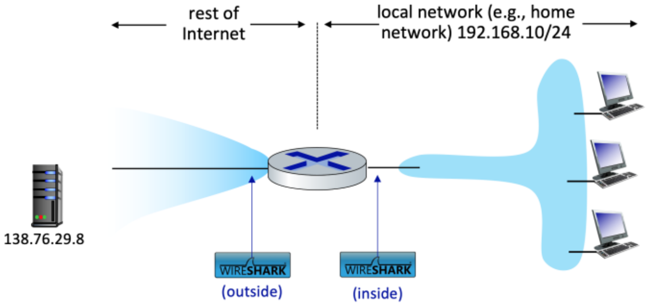


Figure 1: NAT packet capture scenario

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.

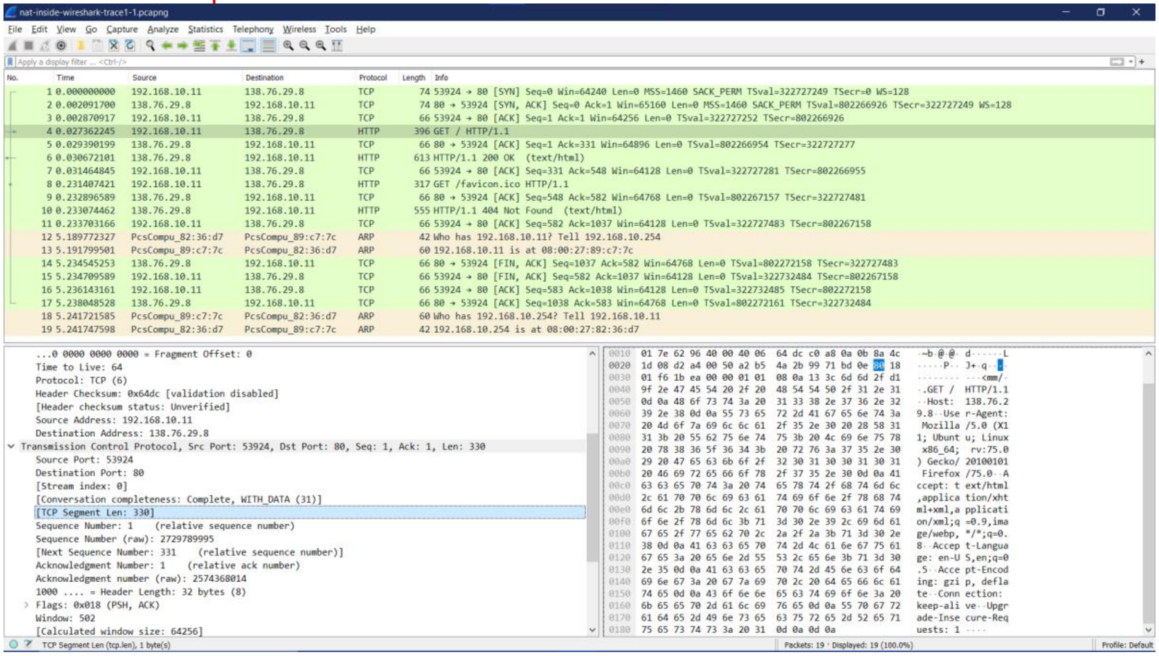
Answer the following questions[3].

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

[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

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?

- The IP address: 192.168.10.11
- The source port number: 53924
- Destination IP address: 138.76.249.8
- The destination port number: 80



nat-inside-wireshark-trace1-1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time         Source             Destination        Protocol  Length Info
  1 0.000000000  192.168.10.11      138.76.29.8        TCP         74 53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=322727249 TSecr=0 WS=128
  2 0.002091700  138.76.29.8        192.168.10.11      TCP         74 80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=802266926 TSecr=322727249 WS=128
  3 0.002870917  192.168.10.11      138.76.29.8        TCP         66 53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=802266926
  4 0.027362245  192.168.10.11      138.76.29.8        HTTP       396 GET / HTTP/1.1
  5 0.029390199  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 0.030672101  138.76.29.8        192.168.10.11      HTTP       613 HTTP/1.1 200 OK  (text/html)
  7 0.031464845  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 0.231407421  192.168.10.11      138.76.29.8        HTTP       317 GET /favicon.ico HTTP/1.1
  9 0.232896589  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 0.233074462  138.76.29.8        192.168.10.11      HTTP       555 HTTP/1.1 404 Not Found  (text/html)
 11 0.233703166  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 5.189772327  PcsCompu_82:36:d7  PcsCompu_89:c7:7c  ARP         42 Who has 192.168.10.11? Tell 192.168.10.254
 13 5.191799501  PcsCompu_89:c7:7c  PcsCompu_82:36:d7  ARP         60 192.168.10.11 is at 08:00:27:89:c7:7c
 14 5.234545253  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 5.234709589  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 5.236143161  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 5.238048528  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 5.241721585  PcsCompu_89:c7:7c  PcsCompu_82:36:d7  ARP         60 Who has 192.168.10.254? Tell 192.168.10.11
 19 5.241747598  PcsCompu_82:36:d7  PcsCompu_89:c7:7c  ARP         42 192.168.10.254 is at 08:00:27:82:36:d7
```

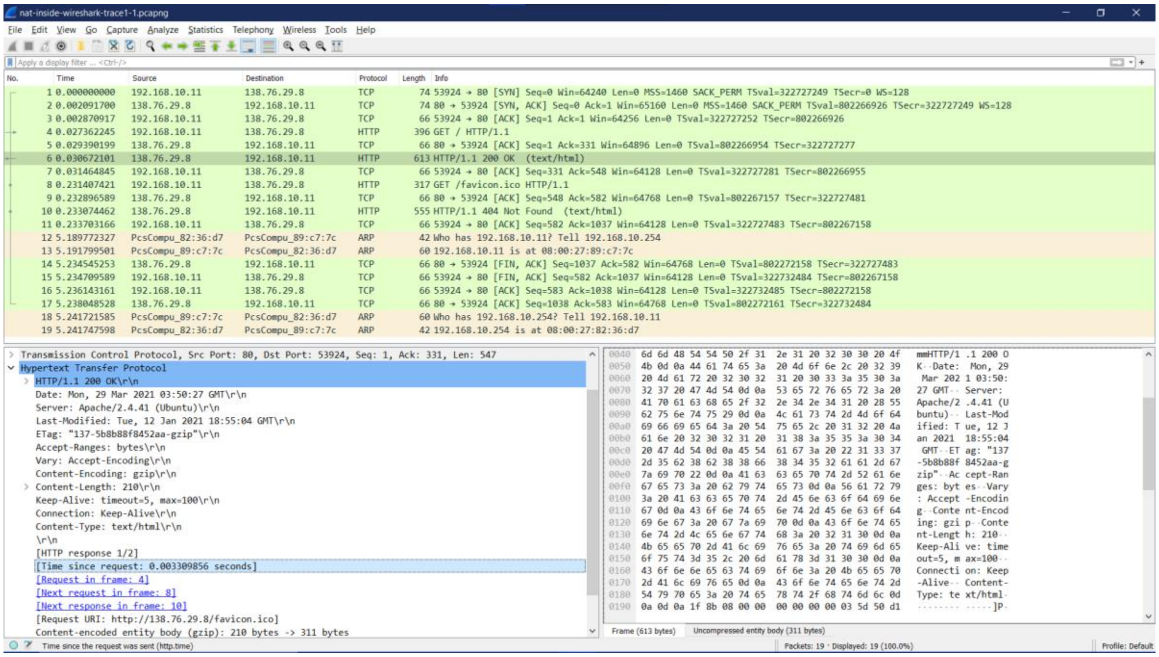
```
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x64dc [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.10.11
    Destination Address: 138.76.29.8
v Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
    Source Port: 53924
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 330]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2729789995
    [Next Sequence Number: 331    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2574368014
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 502
    [Calculated window size: 64256]
```

```
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 80 18   ·····P·· J+·q····
0030  01 f6 1b ea 00 00 01 01  08 0a 13 3c 6d 6d 2f d1   ········ ···<mm/·
0040  9f 2e 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ·.GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  31 33 38 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  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 58 31    Mozilla /5.0 (X1
0080  31 3b 20 55 62 75 6e 74  75 3b 20 4c 69 6e 75 78   1; Ubunt u; Linux
0090  20 78 38 36 5f 36 34 3b  20 72 76 3a 37 35 2e 30    x86_64;  rv:75.0
00a0  29 20 47 65 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 35 2e 30 0d 0a 41    Firefox /75.0··A
00c0  63 63 65 70 74 3a 20 74  65 78 74 2f 68 74 6d 6c   ccept: t ext/html
00d0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74   ,applica tion/xht
00e0  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63 61 74 69   ml+xml,a pplicati
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 4c 61 6e 67 75 61   8··Accep t-Langua
0120  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b 71 3d 30   ge: en-U S,en;q=0
0130  2e 35 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   .5··Acce pt-Encod
0140  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
0150  74 65 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   te··Conn ection: 
0160  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 55 70 67 72   keep-ali ve··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 ····
```

TCP Segment Len (tcp.len), 1 byte(s) | Packets: 19 · Displayed: 19 (100.0%) | Profile: Default

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?

- 0.003309856



nat-inside-wireshark-trace1-1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time         Source             Destination        Protocol  Length Info
  1 0.000000000  192.168.10.11      138.76.29.8        TCP         74 53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=322727249 TSecr=0 WS=128
  2 0.002091700  138.76.29.8        192.168.10.11      TCP         74 80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=802266926 TSecr=322727249 WS=128
  3 0.002870917  192.168.10.11      138.76.29.8        TCP         66 53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=802266926
  4 0.027362245  192.168.10.11      138.76.29.8        HTTP       396 GET / HTTP/1.1
  5 0.029390199  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 0.030672101  138.76.29.8        192.168.10.11      HTTP       613 HTTP/1.1 200 OK  (text/html)
  7 0.031464845  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 0.231407421  192.168.10.11      138.76.29.8        HTTP       317 GET /favicon.ico HTTP/1.1
  9 0.232896589  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 0.233074462  138.76.29.8        192.168.10.11      HTTP       555 HTTP/1.1 404 Not Found  (text/html)
 11 0.233703166  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 5.189772327  PcsCompu_82:36:d7  PcsCompu_89:c7:7c  ARP         42 Who has 192.168.10.11? Tell 192.168.10.254
 13 5.191799501  PcsCompu_89:c7:7c  PcsCompu_82:36:d7  ARP         60 192.168.10.11 is at 08:00:27:89:c7:7c
 14 5.234545253  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 5.234709589  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 5.236143161  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 5.238048528  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 5.241721585  PcsCompu_89:c7:7c  PcsCompu_82:36:d7  ARP         60 Who has 192.168.10.254? Tell 192.168.10.11
 19 5.241747598  PcsCompu_82:36:d7  PcsCompu_89:c7:7c  ARP         42 192.168.10.254 is at 08:00:27:82:36:d7
```

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 29 Mar 2021 03:50:27 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Last-Modified: Tue, 12 Jan 2021 18:55:04 GMT\r\n
    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]
    [Request URI: http://138.76.29.8/favicon.ico]
    Content-encoded entity body (gzip): 210 bytes -> 311 bytes
```

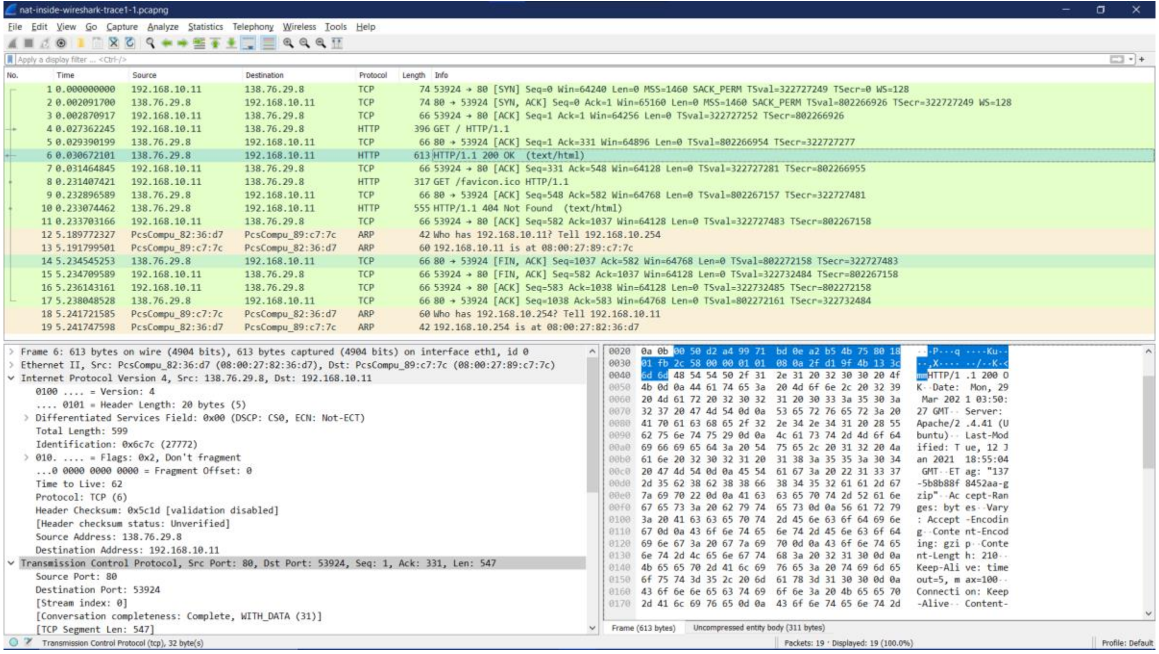
```
0040  6d 6d 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   mmHTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 4d 6f 6e 2c 20 32 39   K··Date:  Mon, 29
0060  20 4d 61 72 20 32 30 32  31 20 30 33 3a 35 30 3a    Mar 202 1 03:50:
0070  32 37 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   27 GMT·· Server: 
0080  41 70 61 63 68 65 2f 32  2e 34 2e 34 31 20 28 55   Apache/2 .4.41 (U
0090  62 75 6e 74 75 29 0d 0a  4c 61 73 74 2d 4d 6f 64   buntu)·· Last-Mod
00a0  69 66 69 65 64 3a 20 54  75 65 2c 20 31 32 20 4a   ified: T ue, 12 J
00b0  61 6e 20 32 30 32 31 20  31 38 3a 35 35 3a 30 34   an 2021  18:55:04
00c0  20 47 4d 54 0d 0a 45 54  61 67 3a 20 22 31 33 37    GMT··ET ag: "137
00d0  2d 35 62 38 62 38 38 66  38 34 35 32 61 61 2d 67   -5b8b88f 8452aa-g
00e0  7a 69 70 22 0d 0a 41 63  63 65 70 74 2d 52 61 6e   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 6e 63 6f 64 69 6e   : Accept -Encodin
0110  67 0d 0a 43 6f 6e 74 65  6e 74 2d 45 6e 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: gzi p··Conte
0130  6e 74 2d 4c 65 6e 67 74  68 3a 20 32 31 30 0d 0a   nt-Lengt h: 210··
0140  4b 65 65 70 2d 41 6c 69  76 65 3a 20 74 69 6d 65   Keep-Ali ve: time
0150  6f 75 74 3d 35 2c 20 6d  61 78 3d 31 30 30 0d 0a   out=5, m ax=100··
0160  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 4b 65 65 70   Connecti on: 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 xt/html·
0190  0a 0d 0a 1f 8b 08 00 00  00 00 00 00 03 5d 50 d1   ········ ·····]P·
```

Frame (613 bytes) | Uncompressed entity body (311 bytes)

Time since the request was sent (http.time) | Packets: 19 · Displayed: 19 (100.0%) | Profile: Default

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

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:138.76.29.8, 53924 Destination:192.168.10.11, 80



nat-inside-wireshark-trace1-1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time         Source             Destination        Protocol Length Info
   1 0.000000000  192.168.10.11      138.76.29.8        TCP      74 53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=322727249 TSecr=0 WS=128
   2 0.002091700  138.76.29.8        192.168.10.11      TCP      74 80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=802266926 TSecr=322727249 WS=128
   3 0.002870917  192.168.10.11      138.76.29.8        TCP      66 53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=802266926
   4 0.027362245  192.168.10.11      138.76.29.8        HTTP    396 GET / HTTP/1.1
   5 0.029390199  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 0.030672101  138.76.29.8        192.168.10.11      HTTP    613 HTTP/1.1 200 OK  (text/html)
   7 0.031464845  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 0.231407421  192.168.10.11      138.76.29.8        HTTP    317 GET /favicon.ico HTTP/1.1
   9 0.232896589  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 0.233074462  138.76.29.8        192.168.10.11      HTTP    555 HTTP/1.1 404 Not Found  (text/html)
  11 0.233703166  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 5.189772327  PcsCompu_82:36:d7  PcsCompu_89:c7:7c  ARP      42 Who has 192.168.10.11? Tell 192.168.10.254
  13 5.191799501  PcsCompu_89:c7:7c  PcsCompu_82:36:d7  ARP      60 192.168.10.11 is at 08:00:27:89:c7:7c
  14 5.234545253  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 5.234709589  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 5.236143161  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 5.238048528  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 5.241721585  PcsCompu_89:c7:7c  PcsCompu_82:36:d7  ARP      60 Who has 192.168.10.254? Tell 192.168.10.11
  19 5.241747598  PcsCompu_82:36:d7  PcsCompu_89:c7:7c  ARP      42 192.168.10.254 is at 08:00:27:82:36:d7
```

```
> 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)
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
v Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
    Source Port: 80
    Destination Port: 53924
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 547]
```

```
0020  0a 0b 00 50 d2 a4 99 71  bd 0e a2 b5 4b 75 80 18   ···P···q ····Ku··
0030  01 fb 2c 58 00 00 01 01  08 0a 2f d1 9f 4b 13 3c   ··,X···· ··/··K·<
0040  6d 6d 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   mmHTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 4d 6f 6e 2c 20 32 39   K··Date:  Mon, 29
0060  20 4d 61 72 20 32 30 32  31 20 30 33 3a 35 30 3a    Mar 202 1 03:50:
0070  32 37 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   27 GMT··  Server:
0080  41 70 61 63 68 65 2f 32  2e 34 2e 34 31 20 28 55   Apache/2 .4.41 (U
0090  62 75 6e 74 75 29 0d 0a  4c 61 73 74 2d 4d 6f 64   buntu)··  Last-Mod
00a0  69 66 69 65 64 3a 20 54  75 65 2c 20 31 32 20 4a   ified: T ue, 12 J
00b0  61 6e 20 32 30 32 31 20  31 38 3a 35 35 3a 30 34   an 2021  18:55:04
00c0  20 47 4d 54 0d 0a 45 54  61 67 3a 20 22 31 33 37    GMT··ET ag: "137
00d0  2d 35 62 38 62 38 38 66  38 34 35 32 61 61 2d 67   -5b8b88f 8452aa-g
00e0  7a 69 70 22 0d 0a 41 63  63 65 70 74 2d 52 61 6e   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 6e 63 6f 64 69 6e   : Accept -Encodin
0110  67 0d 0a 43 6f 6e 74 65  6e 74 2d 45 6e 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: gzi p··Conte
0130  6e 74 2d 4c 65 6e 67 74  68 3a 20 32 31 30 0d 0a   nt-Lengt h: 210··
0140  4b 65 65 70 2d 41 6c 69  76 65 3a 20 74 69 6d 65   Keep-Ali ve: time
0150  6f 75 74 3d 35 2c 20 6d  61 78 3d 31 30 30 0d 0a   out=5, m ax=100··
0160  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 4b 65 65 70   Connecti on: Keep
0170  2d 41 6c 69 76 65 0d 0a  43 6f 6e 74 65 6e 74 2d   -Alive·· Content-
```

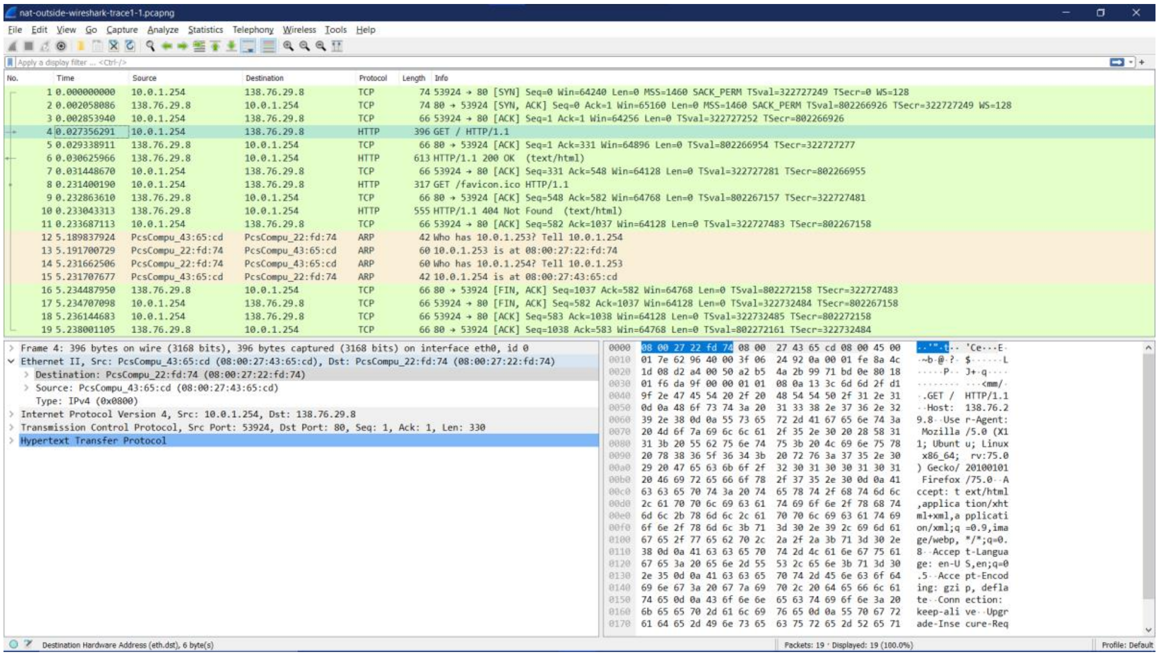
Frame (613 bytes)
Uncompressed entity body (311 bytes)
Transmission Control Protocol (tcp), 32 byte(s)
Packets: 19 · Displayed: 19 (100.0%)
Profile: Default

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?
    - Time: 0.027356291


nat-outside-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

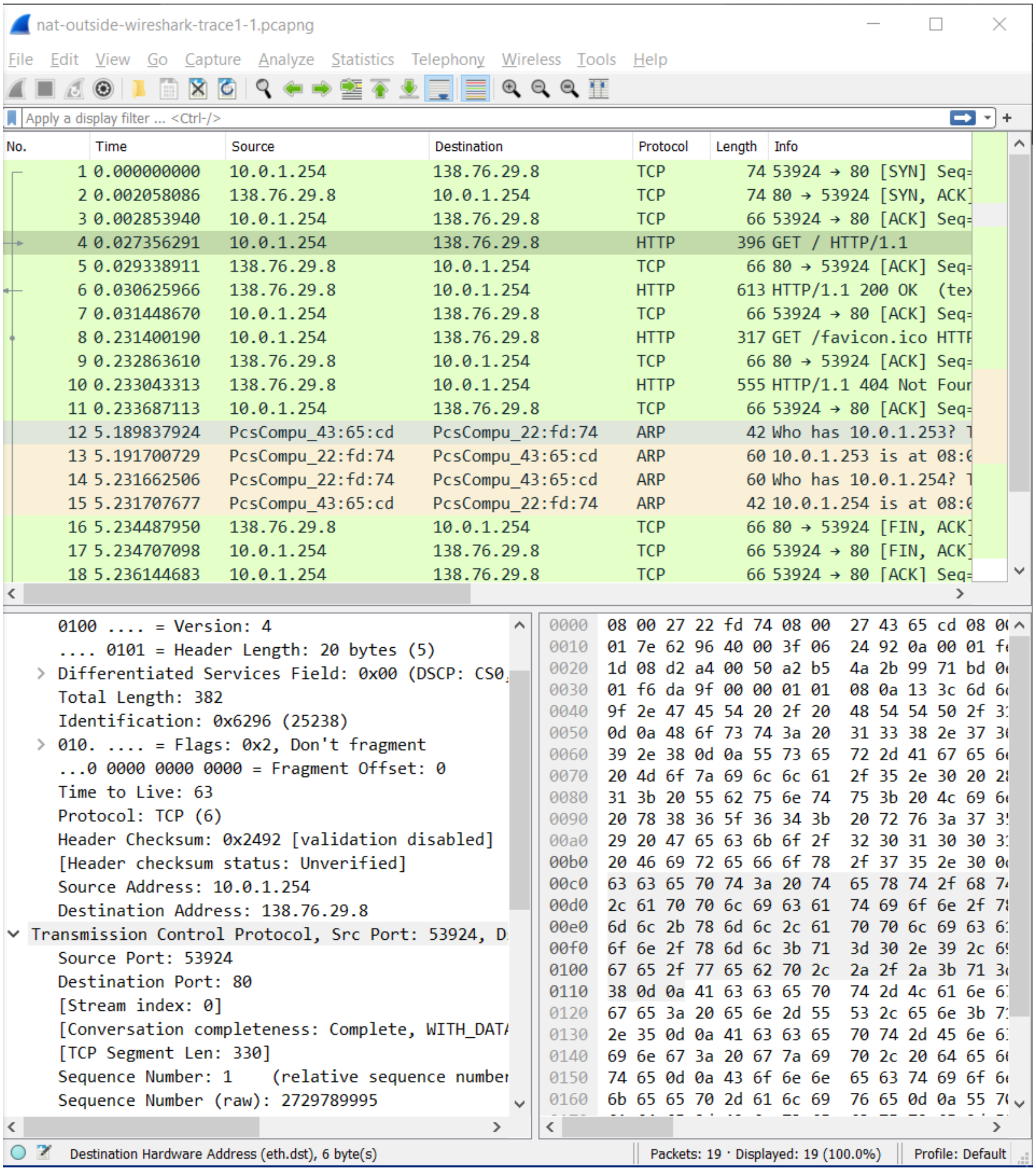
```
No.  Time         Source             Destination        Protocol Length Info
   1 0.000000000  10.0.1.254         138.76.29.8        TCP       74 53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=322727249 TSecr=0 WS=128
   2 0.002058086  138.76.29.8        10.0.1.254         TCP       74 80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=802266926 TSecr=322727249 WS=128
   3 0.002853940  10.0.1.254         138.76.29.8        TCP       66 53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=802266926
   4 0.027356291  10.0.1.254         138.76.29.8        HTTP     396 GET / HTTP/1.1
   5 0.029338911  138.76.29.8        10.0.1.254         TCP       66 80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277
   6 0.030625966  138.76.29.8        10.0.1.254         HTTP     613 HTTP/1.1 200 OK  (text/html)
   7 0.031448670  10.0.1.254         138.76.29.8        TCP       66 53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955
   8 0.231400190  10.0.1.254         138.76.29.8        HTTP     317 GET /favicon.ico HTTP/1.1
   9 0.232863610  138.76.29.8        10.0.1.254         TCP       66 80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481
  10 0.233043313  138.76.29.8        10.0.1.254         HTTP     555 HTTP/1.1 404 Not Found  (text/html)
  11 0.233687113  10.0.1.254         138.76.29.8        TCP       66 53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158
  12 5.189837924  PcsCompu_43:65:cd  PcsCompu_22:fd:74  ARP       42 Who has 10.0.1.253? Tell 10.0.1.254
  13 5.191700729  PcsCompu_22:fd:74  PcsCompu_43:65:cd  ARP       60 10.0.1.253 is at 08:00:27:22:fd:74
  14 5.231662506  PcsCompu_22:fd:74  PcsCompu_43:65:cd  ARP       60 Who has 10.0.1.254? Tell 10.0.1.253
  15 5.231707677  PcsCompu_43:65:cd  PcsCompu_22:fd:74  ARP       42 10.0.1.254 is at 08:00:27:43:65:cd
  16 5.234487950  138.76.29.8        10.0.1.254         TCP       66 80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TSval=802272158 TSecr=322727483
  17 5.234707098  10.0.1.254         138.76.29.8        TCP       66 53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322732484 TSecr=802267158
  18 5.236144683  10.0.1.254         138.76.29.8        TCP       66 53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TSval=322732485 TSecr=802272158
  19 5.238001105  138.76.29.8        10.0.1.254         TCP       66 80 → 53924 [ACK] Seq=1038 Ack=583 Win=64768 Len=0 TSval=802272161 TSecr=322732484
```

```
> Frame 4: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth0, id 0
v Ethernet II, Src: PcsCompu_43:65:cd (08:00:27:43:65:cd), Dst: PcsCompu_22:fd:74 (08:00:27:22:fd:74)
  > Destination: PcsCompu_22:fd:74 (08:00:27:22:fd:74)
  > Source: PcsCompu_43:65:cd (08:00:27:43:65:cd)
    Type: IPv4 (0x0800)
> 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
```

```
0000  08 00 27 22 fd 74 08 00  27 43 65 cd 08 00 45 00   ..'".t.. 'Ce...E.
0010  01 7e 62 96 40 00 3f 06  24 92 0a 00 01 fe 8a 4c   .~b.@.?. $......L
0020  1d 08 d2 a4 00 50 a2 b5  4a 2b 99 71 bd 0e 80 18   .....P.. J+.q....
0030  01 f6 da 9f 00 00 01 01  08 0a 13 3c 6d 6d 2f d1   ........ ...<mm/.
0040  9f 2e 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ..GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  31 33 38 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  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 58 31    Mozilla /5.0 (X1
0080  31 3b 20 55 62 75 6e 74  75 3b 20 4c 69 6e 75 78   1; Ubunt u; Linux
0090  20 78 38 36 5f 36 34 3b  20 72 76 3a 37 35 2e 30    x86_64;  rv:75.0
00a0  29 20 47 65 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 35 2e 30 0d 0a 41    Firefox /75.0..A
00c0  63 63 65 70 74 3a 20 74  65 78 74 2f 68 74 6d 6c   ccept: t ext/html
00d0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74   ,applica tion/xht
00e0  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63 61 74 69   ml+xml,a pplicati
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 4c 61 6e 67 75 61   8..Accep t-Langua
0120  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b 71 3d 30   ge: en-U S,en;q=0
0130  2e 35 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   .5..Acce pt-Encod
0140  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
0150  74 65 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   te..Conn ection: 
0160  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 55 70 67 72   keep-ali ve..Upgr
0170  61 64 65 2d 49 6e 73 65  63 75 72 65 2d 52 65 71   ade-Inse cure-Req
```

Destination Hardware Address (eth.dst), 6 byte(s)
Packets: 19 · Displayed: 19 (100.0%)
Profile: Default

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)?
   - Source: 10.0.1.254, 53
   - Destination: 138.76.29.8
   - Source port: 53924
   - Destination port: 80


nat-outside-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.1.254	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=
2	0.002058086	138.76.29.8	10.0.1.254	TCP	74	80 → 53924 [SYN, ACK]
3	0.002853940	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.029338911	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (te
7	0.031448670	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTT
9	0.232863610	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Fou
11	0.233687113	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=
12	5.189837924	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	Who has 10.0.1.253?
13	5.191700729	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	10.0.1.253 is at 08:
14	5.231662506	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	Who has 10.0.1.254?
15	5.231707677	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	10.0.1.254 is at 08:
16	5.234487950	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [FIN, ACK]
17	5.234707098	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [FIN, ACK]
18	5.236144683	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0,
    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
v Transmission Control Protocol, Src Port: 53924, D
    Source Port: 53924
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DAT
    [TCP Segment Len: 330]
    Sequence Number: 1    (relative sequence number
    Sequence Number (raw): 2729789995
```

```
0000  08 00 27 22 fd 74 08 00  27 43 65 cd 08
0010  01 7e 62 96 40 00 3f 06  24 92 0a 00 01
0020  1d 08 d2 a4 00 50 a2 b5  4a 2b 99 71 bd
0030  01 f6 da 9f 00 00 01 01  08 0a 13 3c 6d
0040  9f 2e 47 45 54 20 2f 20  48 54 54 50 2f
0050  0d 0a 48 6f 73 74 3a 20  31 33 38 2e 37
0060  39 2e 38 0d 0a 55 73 65  72 2d 41 67 65
0070  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20
0080  31 3b 20 55 62 75 6e 74  75 3b 20 4c 69
0090  20 78 38 36 5f 36 34 3b  20 72 76 3a 37
00a0  29 20 47 65 63 6b 6f 2f  32 30 31 30 30
00b0  20 46 69 72 65 66 6f 78  2f 37 35 2e 30
00c0  63 63 65 70 74 3a 20 74  65 78 74 2f 68
00d0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f
00e0  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63
00f0  6f 6e 2f 78 6d 6c 3b 71  3d 30 2e 39 2c
0100  67 65 2f 77 65 62 70 2c  2a 2f 2a 3b 71
0110  38 0d 0a 41 63 63 65 70  74 2d 4c 61 6e
0120  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b
0130  2e 35 0d 0a 41 63 63 65  70 74 2d 45 6e
0140  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65
0150  74 65 0d 0a 43 6f 6e 6e  65 63 74 69 6f
0160  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 55
```

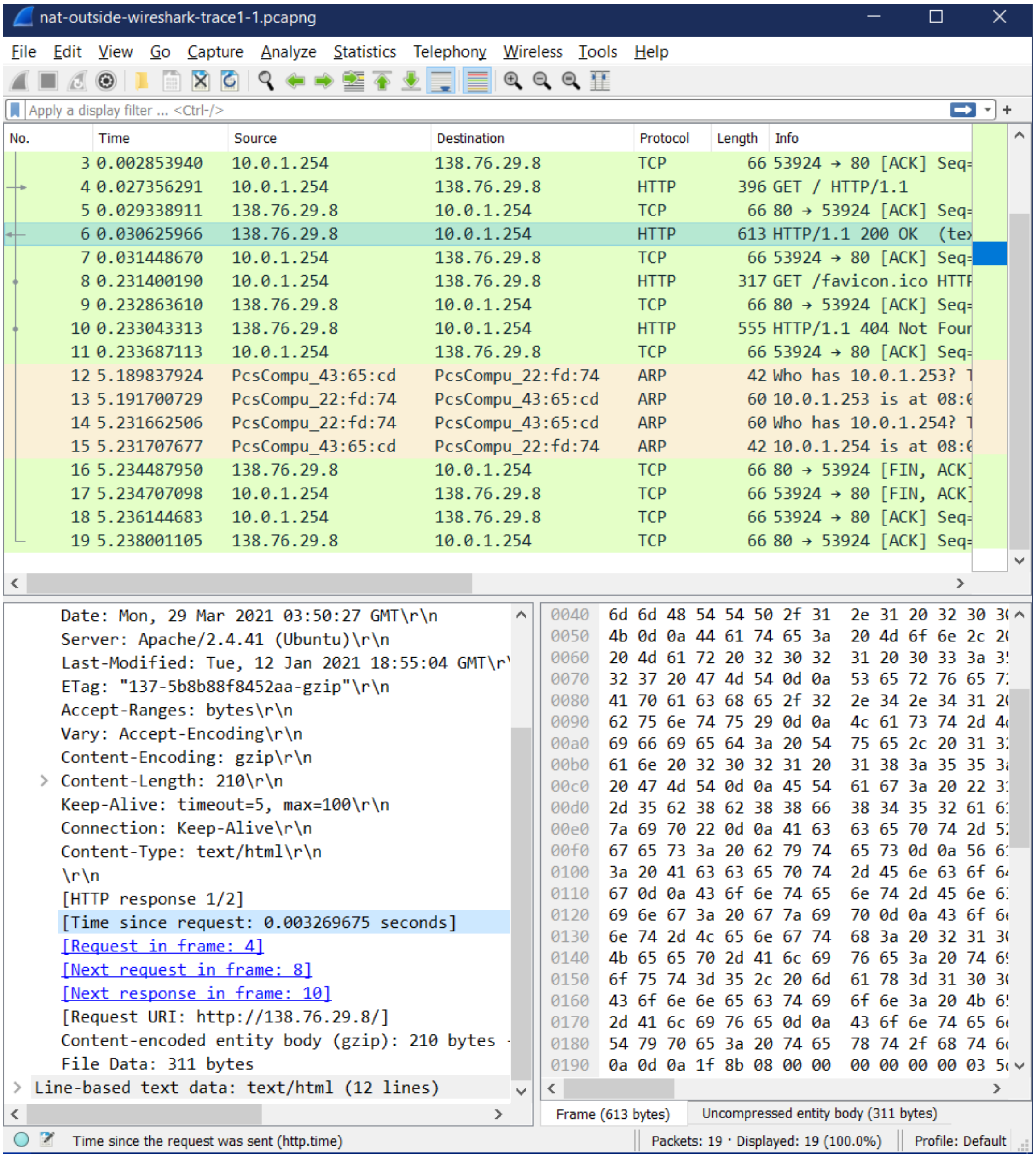
Destination Hardware Address (eth.dst), 6 byte(s) | Packets: 19 · Displayed: 19 (100.0%) | Profile: Default

6. Which of these four fields are different than in your answer to question 1 above?
   - Inside: Source : 192.168.10.11, 53924 Destination: 138.76.249.8, 80
   - Outside: Source : 10.0.1.254, 53924 Destination: 138.76.29.8, 80
7. Are any fields in the HTTP GET message changed?
   - None
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-<u>outside</u>-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-<u>outside</u>-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



nat-outside-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time         Source           Destination      Protocol  Length Info
  3 0.002853940  10.0.1.254       138.76.29.8      TCP        66 53924 → 80 [ACK] Seq=
  4 0.027356291  10.0.1.254       138.76.29.8      HTTP      396 GET / HTTP/1.1
  5 0.029338911  138.76.29.8      10.0.1.254       TCP        66 80 → 53924 [ACK] Seq=
  6 0.030625966  138.76.29.8      10.0.1.254       HTTP      613 HTTP/1.1 200 OK  (tex
  7 0.031448670  10.0.1.254       138.76.29.8      TCP        66 53924 → 80 [ACK] Seq=
  8 0.231400190  10.0.1.254       138.76.29.8      HTTP      317 GET /favicon.ico HTTP
  9 0.232863610  138.76.29.8      10.0.1.254       TCP        66 80 → 53924 [ACK] Seq=
 10 0.233043313  138.76.29.8      10.0.1.254       HTTP      555 HTTP/1.1 404 Not Four
 11 0.233687113  10.0.1.254       138.76.29.8      TCP        66 53924 → 80 [ACK] Seq=
 12 5.189837924  PcsCompu_43:65:cd PcsCompu_22:fd:74 ARP      42 Who has 10.0.1.253? T
 13 5.191700729  PcsCompu_22:fd:74 PcsCompu_43:65:cd ARP      60 10.0.1.253 is at 08:0
 14 5.231662506  PcsCompu_22:fd:74 PcsCompu_43:65:cd ARP      60 Who has 10.0.1.254? T
 15 5.231707677  PcsCompu_43:65:cd PcsCompu_22:fd:74 ARP      42 10.0.1.254 is at 08:0
 16 5.234487950  138.76.29.8      10.0.1.254       TCP        66 80 → 53924 [FIN, ACK]
 17 5.234707098  10.0.1.254       138.76.29.8      TCP        66 53924 → 80 [FIN, ACK]
 18 5.236144683  10.0.1.254       138.76.29.8      TCP        66 53924 → 80 [ACK] Seq=
 19 5.238001105  138.76.29.8      10.0.1.254       TCP        66 80 → 53924 [ACK] Seq=
```

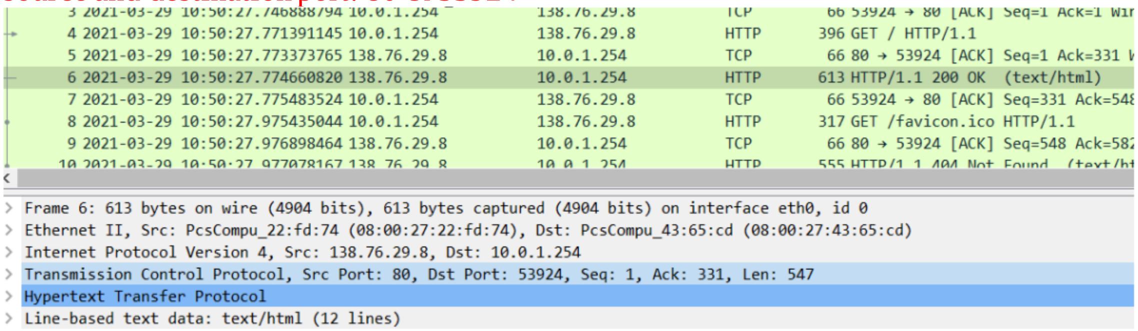
```
    Date: Mon, 29 Mar 2021 03:50:27 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Last-Modified: Tue, 12 Jan 2021 18:55:04 GMT\r
    ETag: "137-5b8b88f8452aa-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  > Content-Length: 210\r\n
    Keep-Alive: 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: 0.003269675 seconds]
    [Request in frame: 4]
    [Next request in frame: 8]
    [Next response in frame: 10]
    [Request URI: http://138.76.29.8/]
    Content-encoded entity body (gzip): 210 bytes
    File Data: 311 bytes
> Line-based text data: text/html (12 lines)
```

```
0040  6d 6d 48 54 54 50 2f 31  2e 31 20 32 30 3
0050  4b 0d 0a 44 61 74 65 3a  20 4d 6f 6e 2c 2
0060  20 4d 61 72 20 32 30 32  31 20 30 33 3a 3
0070  32 37 20 47 4d 54 0d 0a  53 65 72 76 65 7
0080  41 70 61 63 68 65 2f 32  2e 34 2e 34 31 2
0090  62 75 6e 74 75 29 0d 0a  4c 61 73 74 2d 4
00a0  69 66 69 65 64 3a 20 54  75 65 2c 20 31 3
00b0  61 6e 20 32 30 32 31 20  31 38 3a 35 35 3
00c0  20 47 4d 54 0d 0a 45 54  61 67 3a 20 22 3
00d0  2d 35 62 38 62 38 38 66  38 34 35 32 61 6
00e0  7a 69 70 22 0d 0a 41 63  63 65 70 74 2d 5
00f0  67 65 73 3a 20 62 79 74  65 73 0d 0a 56 6
0100  3a 20 41 63 63 65 70 74  2d 45 6e 63 6f 6
0110  67 0d 0a 43 6f 6e 74 65  6e 74 2d 45 6e 6
0120  69 6e 67 3a 20 67 7a 69  70 0d 0a 43 6f 6
0130  6e 74 2d 4c 65 6e 67 74  68 3a 20 32 31 3
0140  4b 65 65 70 2d 41 6c 69  76 65 3a 20 74 6
0150  6f 75 74 3d 35 2c 20 6d  61 78 3d 31 30 3
0160  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 4b 6
0170  2d 41 6c 69 76 65 0d 0a  43 6f 6e 74 65 6
0180  54 79 70 65 3a 20 74 65  78 74 2f 68 74 6
0190  0a 0d 0a 1f 8b 08 00 00  00 00 00 00 03 5
```

Frame (613 bytes)
Uncompressed entity body (311 bytes)
Time since the request was sent (http.time)
Packets: 19 · Displayed: 19 (100.0%)
Profile: Default

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-<u>outside</u>-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 Wir
 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!