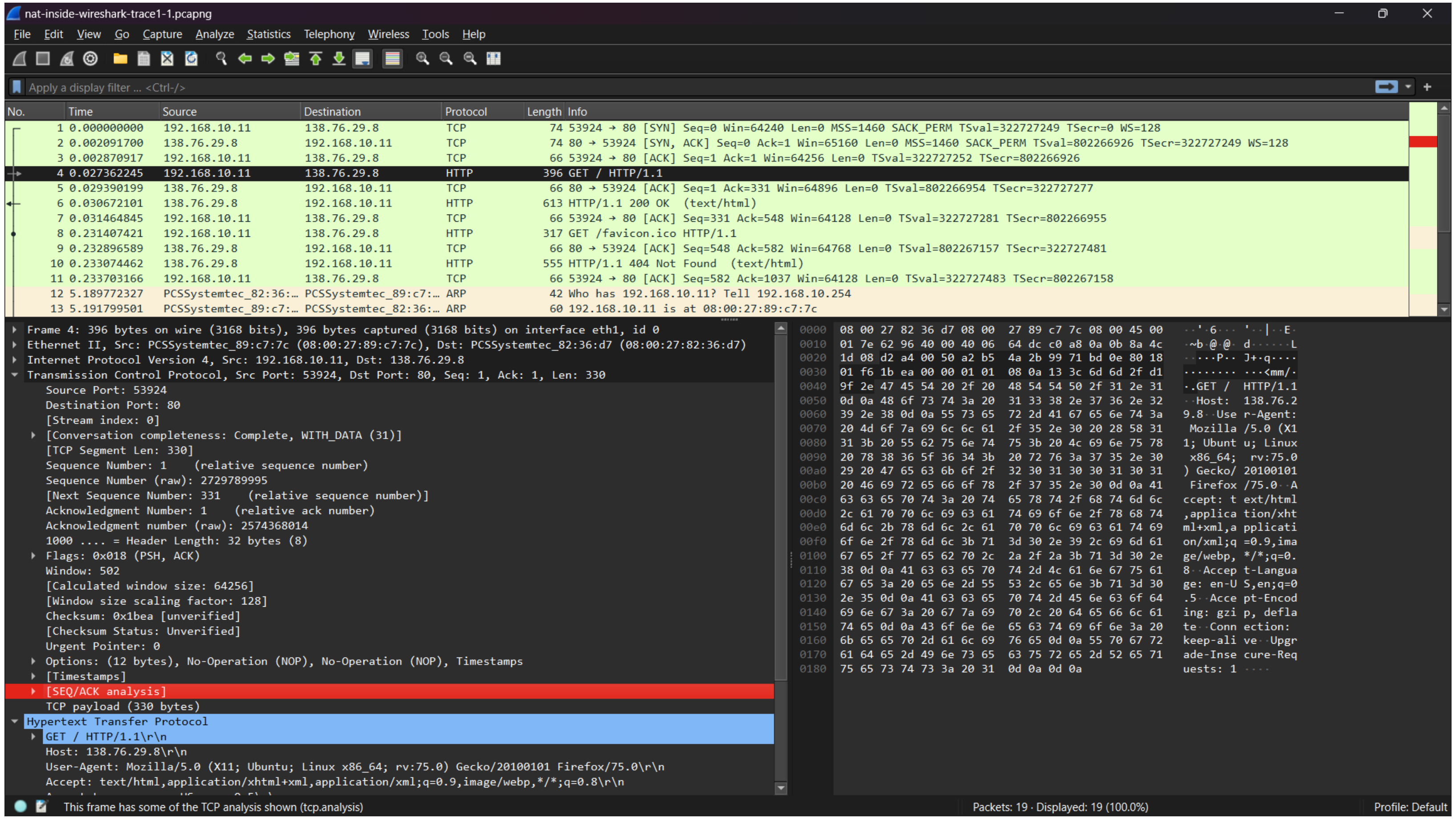
NAT

Yogesh P
201EE138

NAT inside


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  PCSSystemtec_82:36:… PCSSystemtec_89:c7:… ARP        42 Who has 192.168.10.11? Tell 192.168.10.254
   13 5.191799501  PCSSystemtec_89:c7:… PCSSystemtec_82:36:… ARP        60 192.168.10.11 is at 08:00:27:89:c7:7c
```

```
▸ Frame 4: 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
▾ 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]
    [Window size scaling factor: 128]
    Checksum: 0x1bea [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (330 bytes)
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: 138.76.29.8\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
```

```
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 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  ····
```

This frame has some of the TCP analysis shown (tcp.analysis)

Packets: 19 · Displayed: 19 (100.0%)

Profile: Default

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?

A:Client IP:192.168.10.11 , sourceport: 53924, destinationIP:138.76.29.8, destport:80

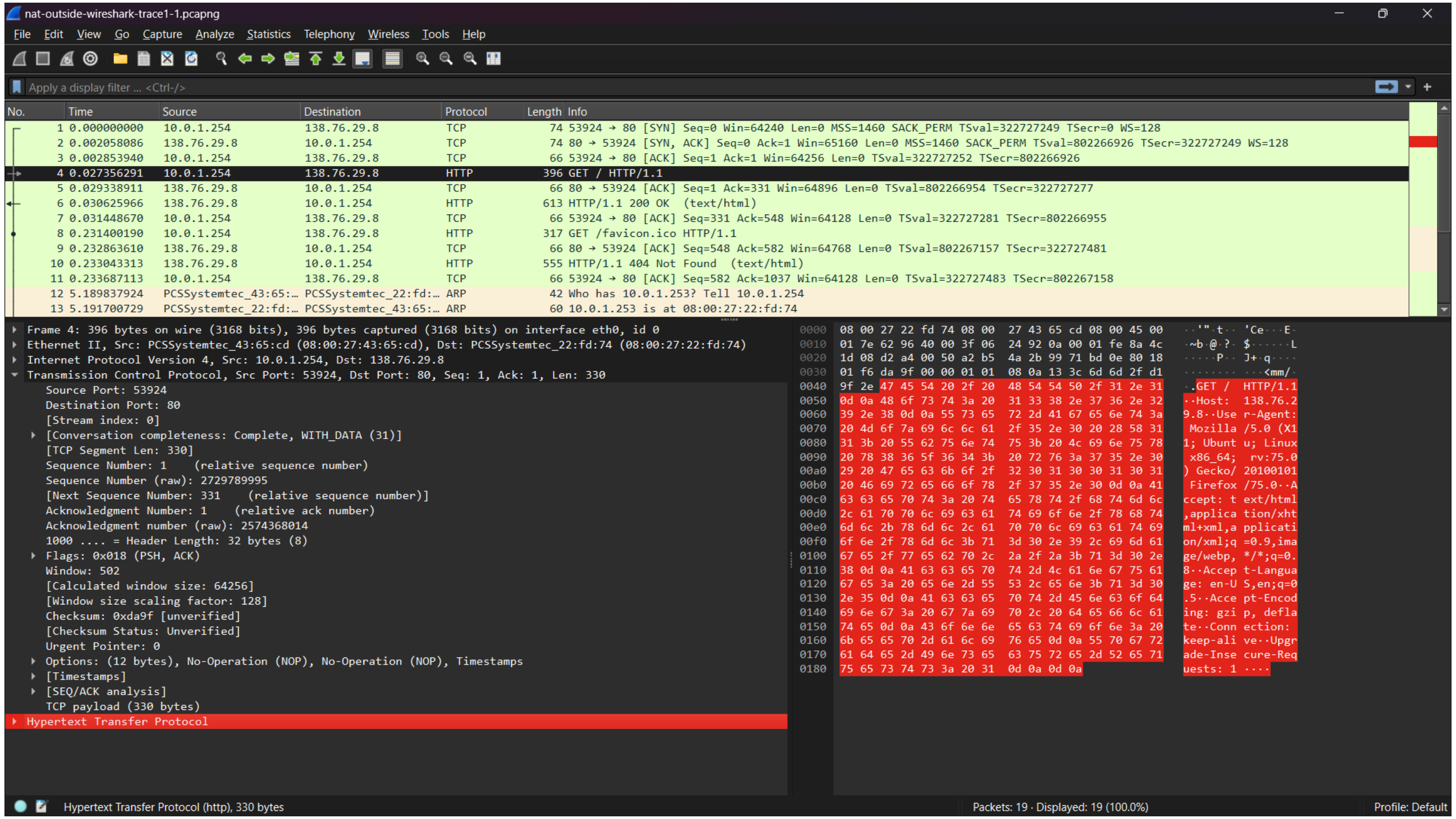
2. At what time is the corresponding HTTP 200 OK message from the webserver forwarded by the NAT router to the client on the router's LAN side?

A:0.30672101

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?

A:sourceip: 138.76.29.8, destip: 192.168.10.11, Src Port: 80, Dst Port: 53924

NAT outside


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  PCSSystemtec_43:65:… PCSSystemtec_22:fd:… ARP      42 Who has 10.0.1.253? Tell 10.0.1.254
   13 5.191700729  PCSSystemtec_22:fd:… PCSSystemtec_43:65:… ARP      60 10.0.1.253 is at 08:00:27:22:fd:74
```

```
› Frame 4: 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)
› 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
     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]
     [Window size scaling factor: 128]
     Checksum: 0xda9f [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   › Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
   › [Timestamps]
   › [SEQ/ACK analysis]
     TCP payload (330 bytes)
› 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
0180  75 65 73 74 73 3a 20 31  0d 0a 0d 0a               uests: 1 ····
```

```
Hypertext Transfer Protocol (http), 330 bytes          Packets: 19 · Displayed: 19 (100.0%)          Profile: Default
```

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

A: 0.027356921

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)?

A: SourceIP:10.0.1.254,DestinationIP: 138.76.29.8, Source Port: 53924, Destination Port: 80

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

A: sourceIP address is different

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

A: sourceIP address

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?

A: checksum is different, others are same

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

A: 0.030625966

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)?

A:Src: 138.76.29.8, Dst: 10.0.1.254, 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?

A: Src: 138.76.29.8, Dst: 192.168.10.11, Source Port: 80 , Destination Port: 53924