Lab 04_NAT

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 of the client that sends the HTTP GET (Source Address):
192.168.10.11

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

Source port : 53924

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

the destination IP address: 138.76.29.8

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

Destination port: 80

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

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

Source port : 80

Destination IP address: 192.168.10.11

Destination port: 53924

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

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 IP Address: 10.0.1.254
Source port : 53924
Destination IP address: 138.76.29.8
Destination port: 80

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

Source IP address

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?

Version: NO

Header Length: No

Flags: No

Checksum: Yes

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	10:50:27.744	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	10:50:27.746	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=322
3	10:50:27.746	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	10:50:27.771	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	10:50:27.773	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	10:50:27.774	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
7	10:50:27.775	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	10:50:27.975	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	10:50:27.976	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	10:50:27.977	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	10:50:27.977	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	10:50:32.933	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	Who has 10.0.1.253? Tell 10.0.1.254
13	10:50:32.935	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	10.0.1.253 is at 08:00:27:22:fd:74
14	10:50:32.975	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	Who has 10.0.1.254? Tell 10.0.1.253
15	10:50:32.975	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	10.0.1.254 is at 08:00:27:43:65:cd
16	10:50:32.978	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	10:50:32.978	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	10:50:32.980	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	10:50:32.982	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
> 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
    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
∨ Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
    Source Port: 53924
    Destination Port: 80

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

---

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	10:50:27.744	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	10:50:27.746	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=322727
3	10:50:27.746	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	10:50:27.771	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	10:50:27.773	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	10:50:27.774	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
7	10:50:27.775	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	10:50:27.975	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	10:50:27.976	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	10:50:27.977	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	10:50:27.977	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	10:50:32.933	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	Who has 10.0.1.253? Tell 10.0.1.254
13	10:50:32.935	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	10.0.1.253 is at 08:00:27:22:fd:74
14	10:50:32.975	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	Who has 10.0.1.254? Tell 10.0.1.253
15	10:50:32.975	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	10.0.1.254 is at 08:00:27:43:65:cd
16	10:50:32.978	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	10:50:32.978	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	10:50:32.980	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	10:50:32.982	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 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
    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
∨ Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
    Source Port: 80
    Destination Port: 53924

```
0000  08 00 27 43 65 cd 08 00  27 22 fd
0010  02 57 6c 7c 40 00 3f 06  19 d3 8a
0020  01 fe 00 50 d2 a4 99 71  bd 0e a2
0030  01 fb eb 0d 00 00 01 01  08 0a 2f
0040  6d 6d 48 54 54 50 2f 31  2e 31 20
0050  4b 0d 0a 44 61 74 65 3a  20 4d 6f
0060  20 4d 61 72 20 32 30 32  31 20 30
0070  32 37 20 47 4d 54 0d 0a  53 65 72
0080  41 70 61 63 68 65 2f 32  2e 34 2e
0090  62 75 6e 74 75 29 0d 0a  4c 61 73
00a0  69 66 69 65 64 3a 20 54  75 65 2c
00b0  61 6e 20 32 30 32 31 20  31 38 3a
00c0  20 47 4d 54 0d 0a 41 63  63 65 70
00d0  2d 35 62 32 38 62 38 66  38 34 35
00e0  7a 69 70 22 0d 0a 41 63  63 65 70
00f0  67 65 73 3a 20 62 79 74  65 73 0d
0100  3a 20 41 63 63 65 70 74  2d 45 6e
0110  67 0d 0a 43 6f 6e 74 65  6e 74 2d
```

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

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

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)?
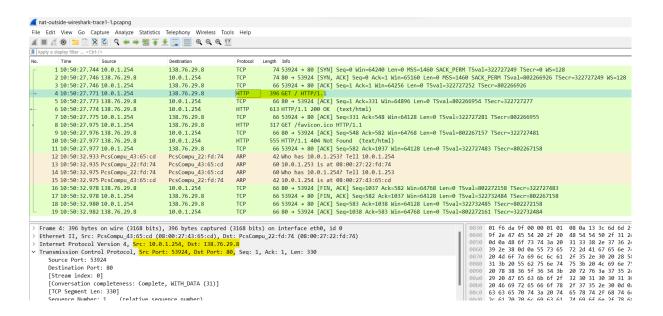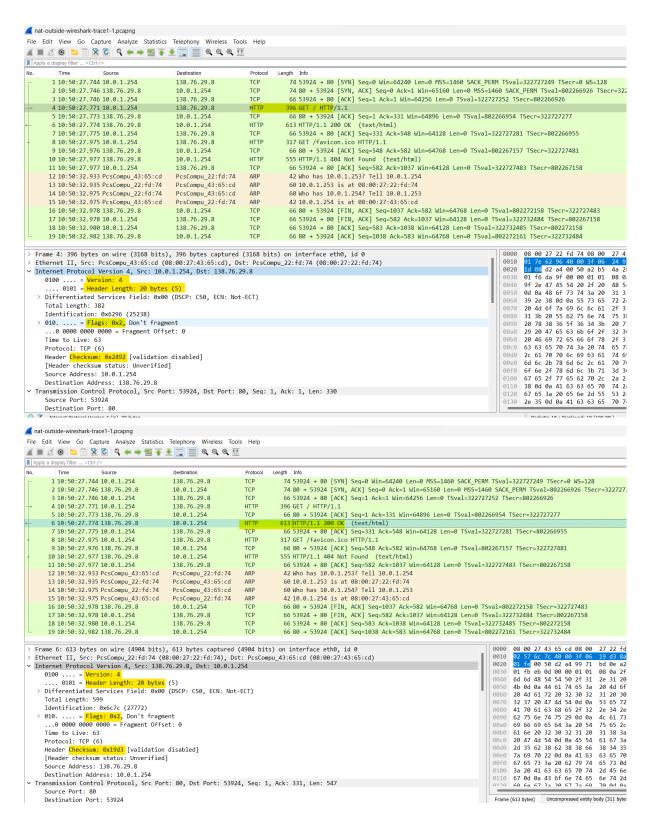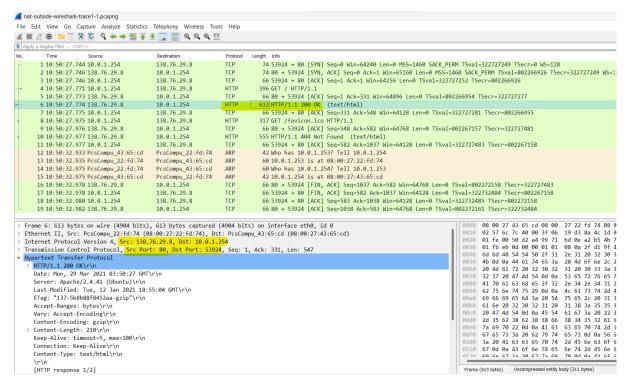
Source IP Address: 138.76.29.8
Source port : 80
Destination IP address: 10.0.1.254
Destination port: 53924

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	10:50:27.744	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	10:50:27.746	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=1:
3	10:50:27.746	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	10:50:27.771	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	10:50:27.773	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	10:50:27.774	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
7	10:50:27.775	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	10:50:27.975	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	10:50:27.976	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	10:50:27.977	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	10:50:27.977	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	10:50:32.933	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	42	Who has 10.0.1.253? Tell 10.0.1.254
13	10:50:32.935	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	60	10.0.1.253 is at 08:00:27:22:fd:74
14	10:50:32.975	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	Who has 10.0.1.254? Tell 10.0.1.253
15	10:50:32.975	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	10.0.1.254 is at 08:00:27:43:65:cd
16	10:50:32.978	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	10:50:32.978	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	10:50:32.980	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	10:50:32.982	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 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
  > 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]

```
0000  08 00 27 43 65 cd 08 00  27 22 fd 74 08 0
0010  02 57 6c 7c 40 00 3f 06  19 d3 8a 4c 1d 0
0020  01 fe 00 50 d2 a4 99 71  bd 0e a2 b5 4b 7
0030  01 fb eb 0d 00 00 01 01  08 0a 2f d1 9f 4
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
```

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

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
Source port : 80
Destination IP address: 192.168.10.11
Destination port: 53924

rest of Internet — local network (e.g., home network) 192.168.10/24

WIRESHARK (outside) WIRESHARK (inside)

138.76.29.8