

Computing and Data Science

Computer network

Assignment no. 4(NAT PCAP File Tracing)

3rd Year

ID: 20221449583

Name: Ali Mohamed Sayed Ahmed

Eng.Mohamed Hatem

Dr. Emad Rauf

1.



NAT_home_side.pcap

This question is related to previous question 3

4. At what time⁴ is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

Answer:

Source IP addresses	64.233.169.104
Destination IP addresses	192.168.1.100
Source port	80
Destination port	4335

2.



NAT_ISP_side.pcap

8. In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?

Answer:

Source IP addresses	64.233.169.104
Destination IP addresses	71.192.34.104
Source port	80
Destination port	4335

- **The time of first 200 OK HTTP Message** = 6.117570
- **Header length:** same = 814
- **Version:** same = 1.1
- **Flags:** same = 0x018
- **Checksum:** it is change because the Destination IP addresses has changed

Screen from Wireshark:

For home side:

ip.src == 64.233.169.104 && http.response.code == 200

No.	Time	Source	Destination	Protocol	Length	Info
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)
127	7.763501	64.233.169.104	192.168.1.100	HTTP	1204	HTTP/1.1 200 OK (image/x-icon)

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 814

Source Port: 80
Destination Port: 4335
[Stream index: 2]
▶ [Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 760]
Sequence Number: 2861 (relative sequence number)
Sequence Number (raw): 3914286017
[Next Sequence Number: 3621 (relative sequence number)]
Acknowledgment Number: 636 (relative ack number)
Acknowledgment number (raw): 4164041056
0101 = Header Length: 20 bytes (5)
▶ Flags: 0x018 (PSH, ACK)
Window: 110
[Calculated window size: 7040]
[Window size scaling factor: 64]
Checksum: 0x5255 [unverified]

0020 01 64 00 50 10 ef e9 4f 43 c1 f8 32 39 60 50 18
0030 00 6e 52 55 00 00 b6 ca 78 d5 b6 ec 90 f0 06 4f
0040 e3 f0 a2 aa e3 94 1b 70 70 50 51 ab b5 96 fb 0c
0050 94 b4 16 21 25 59 3c 02 a7 bd 90 9c a7 55 34 18
0060 1c 57 44 ed 14 89 e5 f8 0e 0a 53 c9 dd 91 b8 3f
0070 4b 37 2c 3b 8a a1 32 42 a7 de 4a f5 86 ab 37 5a
0080 c4 79 49 5f 6c b5 a5 c5 f5 1a 71 b2 8e ca 24 84
0090 88 8c 2b c1 a2 a1 00 ed 2a b9 bf 16 3c 86 4b 9b
00a0 8a 4f 9b 8d 90 06 e1 f7 86 41 3c 83 41 af 47 c0
00b0 4f 85 d0 4e b0 2a 8b b1 fd 1e f7 7c 16 1f b2 04
00c0 1b 3f 56 c1 5c f8 ae 2d 22 66 bd e4 7c d5 10 01
00d0 cf 27 6e bf db 7d b9 16 32 2f d8 0d 09 26 15 e8
00e0 57 d5 5a 52 61 be 46 53 73 8d a9 4b ef 4a 45 4d
00f0 9b 6e 18 4b 9f 8a b4 56 ab ae 2f 9a f8 be 5a 4b
0100 d3 b0 98 e6 ce e6 5f 75 7a e7 de 34 08 9c b3 73
0110 2b e0 ce 59 bb bc 36 b6 ad 36 06 40 f8 51 e6 81

Frame (814 bytes) Reassembled TCP (3620 bytes) Uncompressed

For isp side:

ip.src == 64.233.169.104 && http.response.code == 200

No.	Time	Source	Destination	Protocol	Length	Info
90	6.117570	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK (text/html)
103	6.308118	64.233.169.104	71.192.34.104	HTTP	226	HTTP/1.1 200 OK (GIF89a)
121	6.407366	64.233.169.104	71.192.34.104	HTTP	648	HTTP/1.1 200 OK (text/javascript)
131	6.496234	64.233.169.104	71.192.34.104	HTTP	870	HTTP/1.1 200 OK (text/html)
149	6.644609	64.233.169.104	71.192.34.104	HTTP	1359	HTTP/1.1 200 OK (PNG)
160	6.722203	64.233.169.104	71.192.34.104	HTTP	1204	HTTP/1.1 200 OK (image/x-icon)

▶ Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 814

Source Port: 80
Destination Port: 4335
[Stream index: 2]
▶ [Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 760]
Sequence Number: 2861 (relative sequence number)
Sequence Number (raw): 3914286017
[Next Sequence Number: 3621 (relative sequence number)]
Acknowledgment Number: 636 (relative ack number)
Acknowledgment number (raw): 4164041056
0101 = Header Length: 20 bytes (5)
▶ Flags: 0x018 (PSH, ACK)
Window: 110
[Calculated window size: 7040]
[Window size scaling factor: 64]

0000 00 08 74 4f 36 23 00 0e d6 bf 6c 01 08 00 45 20
0010 03 20 f6 1e 00 00 33 06 3a 20 40 e9 a9 68 47 c0
0020 22 68 00 50 10 ef e9 4f 43 c1 f8 32 39 60 50 18
0030 00 6e aa 39 00 00 b6 ca 78 d5 b6 ec 90 f0 06 4f
0040 e3 f0 a2 aa e3 94 1b 70 70 50 51 ab b5 96 fb 0c
0050 94 b4 16 21 25 59 3c 02 a7 bd 90 9c a7 55 34 18
0060 1c 57 44 ed 14 89 e5 f8 0e 0a 53 c9 dd 91 b8 3f
0070 4b 37 2c 3b 8a a1 32 42 a7 de 4a f5 86 ab 37 5a
0080 c4 79 49 5f 6c b5 a5 c5 f5 1a 71 b2 8e ca 24 84
0090 88 8c 2b c1 a2 a1 00 ed 2a b9 bf 16 3c 86 4b 9b
00a0 8a 4f 9b 8d 90 06 e1 f7 86 41 3c 83 41 af 47 c0
00b0 4f 85 d0 4e b0 2a 8b b1 fd 1e f7 7c 16 1f b2 04
00c0 1b 3f 56 c1 5c f8 ae 2d 22 66 bd e4 7c d5 10 01
00d0 cf 27 6e bf db 7d b9 16 32 2f d8 0d 09 26 15 e8
00e0 57 d5 5a 52 61 be 46 53 73 8d a9 4b ef 4a 45 4d
00f0 9b 6e 18 4b 9f 8a b4 56 ab ae 2f 9a f8 be 5a 4b

Frame (814 bytes) Reassembled TCP (3620 bytes) Uncompressed