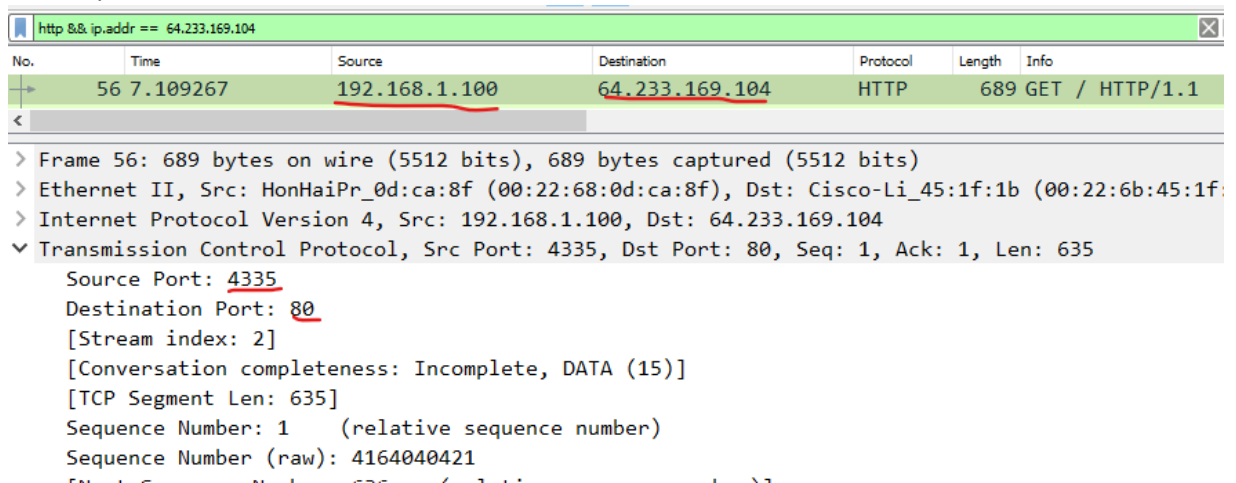


# COMP 3203 Wireshark 8

Name: Nirmith Victor D’Almeida

Number: 101160124

1. The IP address of client is 192.168.1.100.
2. The client actually communicates with several different Google servers in order to implement “safe browsing.” (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression “http && ip.addr == 64.233.169.104” (without quotes) into the Filter: field in Wireshark .
3. Destination IP : 64.233.169.104  
Destination port: 80  
Source IP : 192.168.1.100  
Source port: 4335



The screenshot shows the Wireshark interface with a packet capture filter applied: `http && ip.addr == 64.233.169.104`. The packet list shows a single packet (No. 56) at time 7.109267, from source 192.168.1.100 to destination 64.233.169.104, protocol HTTP, length 689, info GET / HTTP/1.1. The details pane for packet 56 shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1

> Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)  
> Ethernet II, Src: HonHaiPr\_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li\_45:1f:1b (00:22:6b:45:1f:1b)  
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104  
▼ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635  
    Source Port: 4335  
    Destination Port: 80  
    [Stream index: 2]  
    [Conversation completeness: Incomplete, DATA (15)]  
    [TCP Segment Len: 635]  
    Sequence Number: 1 (relative sequence number)  
    Sequence Number (raw): 4164040421

4. Time for the 200 OK HTTP Message is 7.158797

Source IP: 64.233.169.104

Source port: 80

Destination IP: 192.168.1.100

Destination Port: 4335

60	7.158797	64.233.169.104	192.168.1.100	HTTP
60	7.381700	192.168.1.100	64.233.169.104	HTTP

> Frame 60: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)  
> Ethernet II, Src: Cisco-Li\_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr\_  
> Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100  
✓ Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861,  
Source Port: 80  
Destination Port: 4335  
[Stream index: 2]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 760]  
Sequence Number: 2861 (relative sequence number)

- 5.

- a. 7.075657

- b. Destination IP : 64.233.169.104

Destination port: 80

Source IP : 192.168.1.100

Source port: 4335

53	7.075657	192.168.1.100	64.233.169.104	TCP	66 4335 → 80 [SYN] S
----	----------	---------------	----------------	-----	----------------------

> Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
> Ethernet II, Src: HonHaiPr\_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li\_45:1f:1b (00:22:6b:45:1f:1b)  
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104  
✓ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0  
Source Port: ~~4335~~  
Destination Port: 80  
[Stream index: 2]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)

- c. Source IP: 64.233.169.104

Source port: 80

Destination IP: 192.168.1.100

Destination Port: 4335

54	7.108986	64.233.169.104	192.168.1.100	TCP	66	80 → 4335
55	7.108987	192.168.1.100	64.233.169.104	TCP	54	4335 → 80

Frame 54: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
 Ethernet II, Src: Cisco-Li\_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr\_0d:ca:8f (00:22:6b:45:1f:1b)  
 Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100  
 Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0  
 Source Port: 80  
 Destination Port: 4335  
 [Stream index: 2]  
 [Conversation completeness: Incomplete, DATA (15)]

d. 7.108986

6.

a. 6.069168

b. Source IP: 71.192.34.104

Source port: 4335

Destination IP: 64.233.169.104

Destination Port: 80

85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
86	6.117570	64.233.169.104	71.192.34.104	HTTP	614	HTTP/1.1 200 OK

Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)  
 Ethernet II, Src: Dell\_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco\_bf:6c:01 (00:0e:d6:bf:6c:01)  
 Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104  
 Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635  
 Source Port: 4335  
 Destination Port: 80  
 [Stream index: 2]

c. Source IP address has changed

7.

a. No change

b. Checksum has changed

c. Since source IP address has changed for the ISP side. The checksum value has changed since they contain the value of the source IP address.

8.

a. 6.117570

b.

90	6.117570	64.233.169.104	71.192.34.104	HTTP	814 HTTP/1.1 200 OK (text/html)
<p>&gt; Frame 90: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)</p> <p>&gt; Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)</p> <p>&gt; Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104</p> <p>▼ Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760</p> <p>Source Port: <u>80</u></p> <p>Destination Port: <u>4335</u></p> <p>[Stream index: 2]</p> <p>[Conversation completeness: Incomplete, DATA (15)]</p> <p>[TCP Segment Len: 760]</p>					

c. Destination IP address has changed

9.

a. 6.035475

b. For the SYN

82	6.035475	71.192.34.104	64.233.169.104	TCP	66 4335 → 80 [SYN] Seq: 2861
<p>Frame 82: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)</p> <p>Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)</p> <p>Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104</p> <p>Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0</p> <p>Source Port: <u>4335</u></p> <p>Destination Port: <u>80</u></p> <p>[Stream index: 2]</p> <p>[Conversation completeness: Incomplete, DATA (15)]</p> <p>[TCP Segment Len: 0]</p>					

For The ACK

83	6.067775	64.233.169.104	71.192.34.104	TCP	66 80 → 4335 [SYN, ACK] Seq: 2861
84	6.068754	71.192.34.104	64.233.169.104	TCP	60 4335 → 80 [ACK] Seq: 2861
<p>Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)</p> <p>Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)</p> <p>Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104</p> <p>Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0</p> <p>Source Port: <u>80</u></p> <p>Destination Port: <u>4335</u></p> <p>[Stream index: 2]</p> <p>[Conversation completeness: Incomplete, DATA (15)]</p> <p>[TCP Segment Len: 0]</p>					

c. For Syn and ACK the Source and destination address has changed respectively.

10.

NAT translation table	
WAN side	LAN side
71.192.34.104, 4335	192.168.1.100, 4335