



### 3. Source: 192.168.1.100,4335 Destination: 64.233.169.104,80

The image shows a Wireshark packet capture of an HTTP GET request. The packet list shows a single packet (No. 56) at time 2009-09-21 03:43:07.378402, from source 192.168.1.100 to destination 64.233.169.104, protocol HTTP, length 689, info GET / HTTP/1.1. The packet details pane shows the HTTP structure: GET / HTTP/1.1 (text/html), Host: 64.233.169.104, User-Agent: Mozilla/5.0 (Windows; U; MSIE 6.0; en-US; Windows NT 5.1) AppleWebKit/525.13 (KHTML, like Gecko) Chrome/16.0.912.76 Safari/525.13, Accept: \*/\*, Accept-Language: en-US, Accept-Encoding: gzip, deflate, Content-Type: application/javascript, Content-Length: 648, Cache-Control: no-cache, Pragma: no-cache, Expires: -1, Connection: close. The packet bytes pane shows the raw data: 0000 00 22 68 0d ca 8f 00 22 6b 45 1f 1b 00 00 45 20 ... h... KE... E

No.	Time	Source	Destination	Protocol	Length	Info
56	2009-09-21 03:43:07.378402	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1

Time to Live: 50  
Protocol: TCP (6)  
Header Checksum: 0xe3b3 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 64.233.169.104  
Destination Address: 192.168.1.100  
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760  
Source Port: 80  
Destination Port: 4335  
[Stream index: 2]  
[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): 416404056  
0101 .... = Header Length: 20 bytes (5)

0000 00 22 68 0d ca 8f 00 22 6b 45 1f 1b 00 00 45 20 ... h... KE... E  
0010 03 20 f6 1e 00 00 32 06 e3 3b 40 e9 a9 68 c0 a8 ... 2... h...  
0020 01 64 00 50 10 ef e9 4f 43 c1 f8 32 39 60 50 18 ... d P... C... P...  
0030 00 6e 52 55 00 00 b6 ca 78 05 b6 ec 90 f0 06 4f ... nRU... x... O...

### 4. Source: 64.233.169.104, 4335 Destination: 192.168.1.100,4335, Time: 7.427932

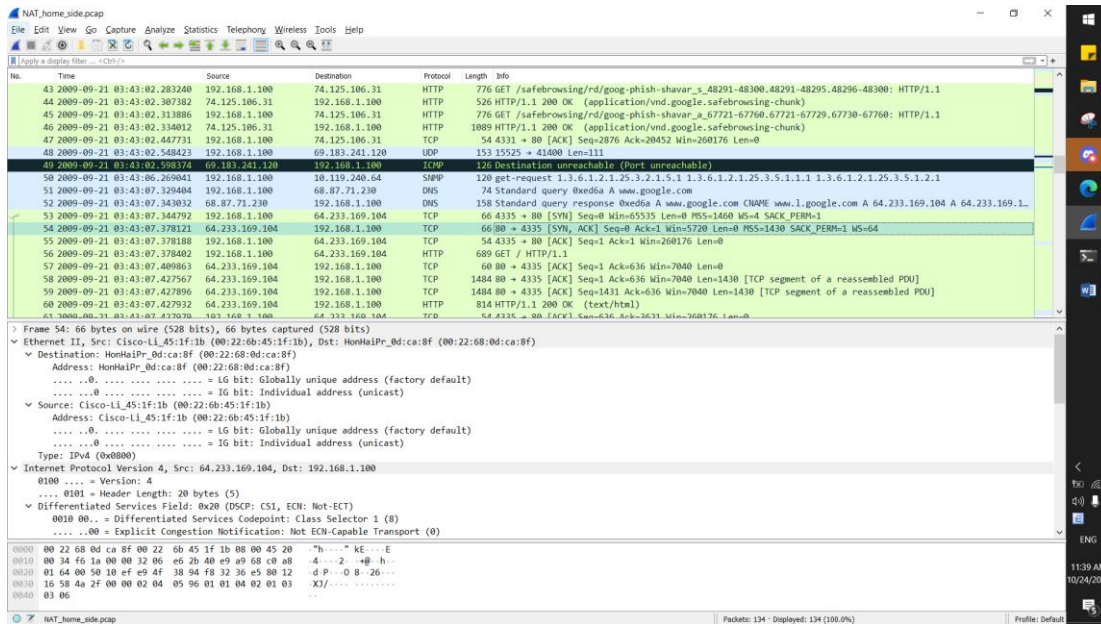
The image shows a Wireshark packet capture of an HTTP response. The packet list shows a single packet (No. 43) at time 2009-09-21 03:43:07.283248, from source 64.233.169.104 to destination 192.168.1.100, protocol HTTP, length 776, info GET / HTTP/1.1. The packet details pane shows the HTTP structure: 200 OK (application/vnd.google.safebrowsing-chunk), Content-Type: application/vnd.google.safebrowsing-chunk, Content-Length: 776, Cache-Control: no-cache, Pragma: no-cache, Expires: -1, Connection: close. The packet bytes pane shows the raw data: 0000 00 22 6b 45 1f 1b 00 22 68 0d ca 8f 00 00 45 00 ... KE... h... E

No.	Time	Source	Destination	Protocol	Length	Info
43	2009-09-21 03:43:07.283248	64.233.169.104	192.168.1.100	HTTP	776	GET / HTTP/1.1

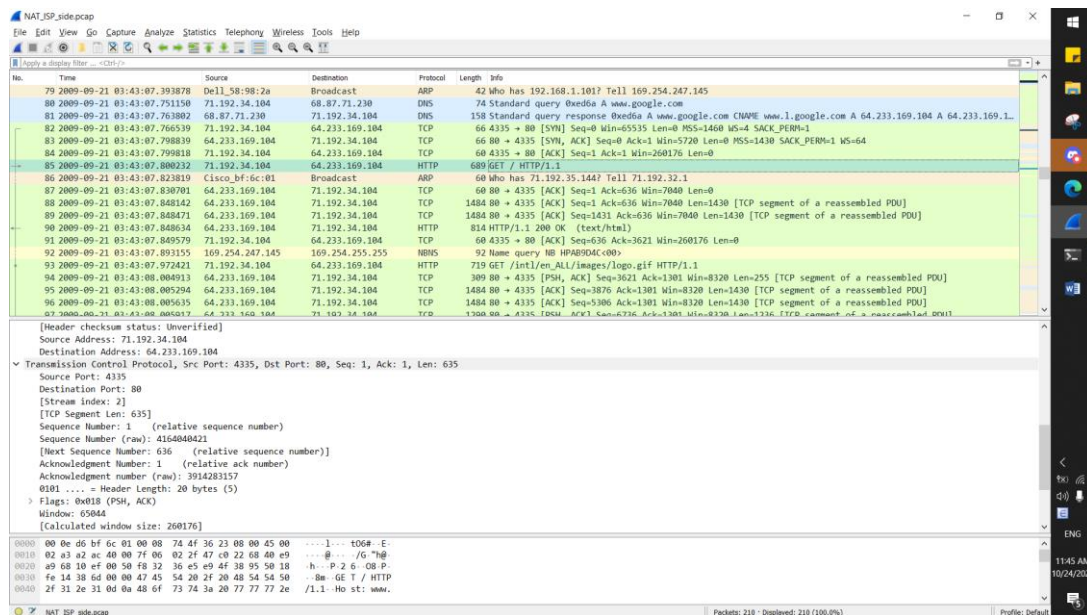
Source: HostIP: 0dca:8f (00:22:68:0d:ca:8f)  
Address: HostIP: 0dca:8f (00:22:68:0d:ca:8f)  
Type: IPv4 (0x0000)  
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104  
0100 .... = Version: 4  
0101 .... = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
0000 00 .. = Differentiated Services Codepoint: Default (0)  
0000 00 .. = Explicit Congestion Notification: Not ECN-Capable Transport (0)  
Total Length: 52  
Identification: 0xa2aa (41642)  
Flags: 0x00, Don't Fragment  
Fragment Offset: 0  
Time to Live: 128  
Protocol: TCP (6)

0000 00 22 6b 45 1f 1b 00 22 68 0d ca 8f 00 00 45 00 ... KE... h... E  
0010 00 34 a2 aa 00 00 00 ab bb c0 a8 01 64 40 e9 ... 4...  
0020 a9 68 10 ef 00 50 f0 32 36 04 00 00 00 30 02 ... h... P... G...  
0030 ff ff 82 62 00 00 02 04 05 b4 01 03 03 02 01 01 ... b...  
0040 04 02 ...

### 5. Time: 7.344792- Source: 192.168.1.100, 4335 – Destination: 64.233.169.104, 80.



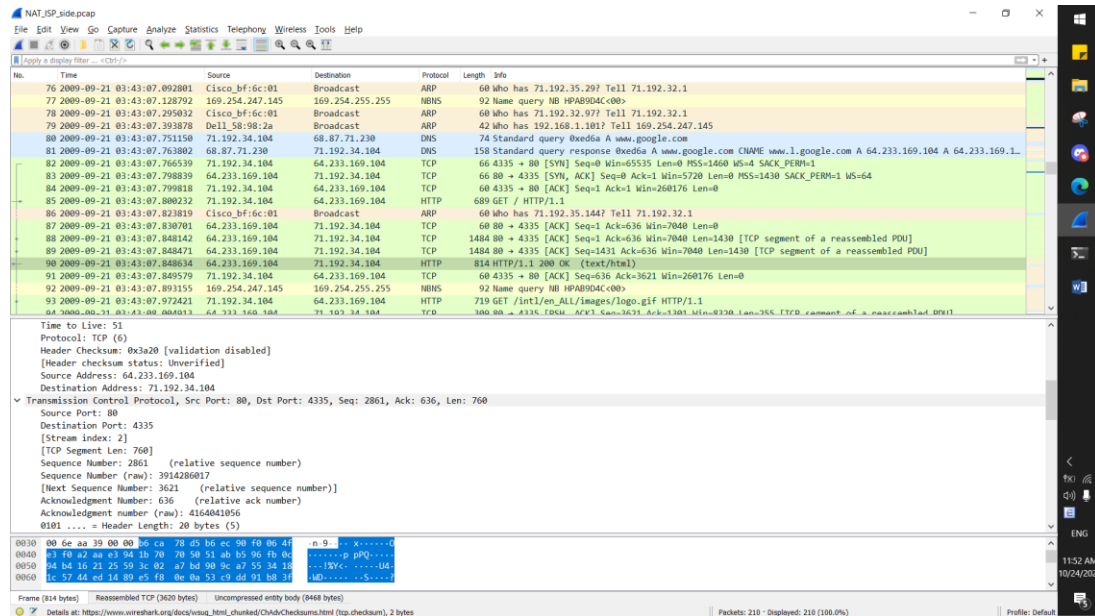
Time: 7.378121 - Source: 64.233.169.104, 80 – Destination: 192.168.1.100, 4335



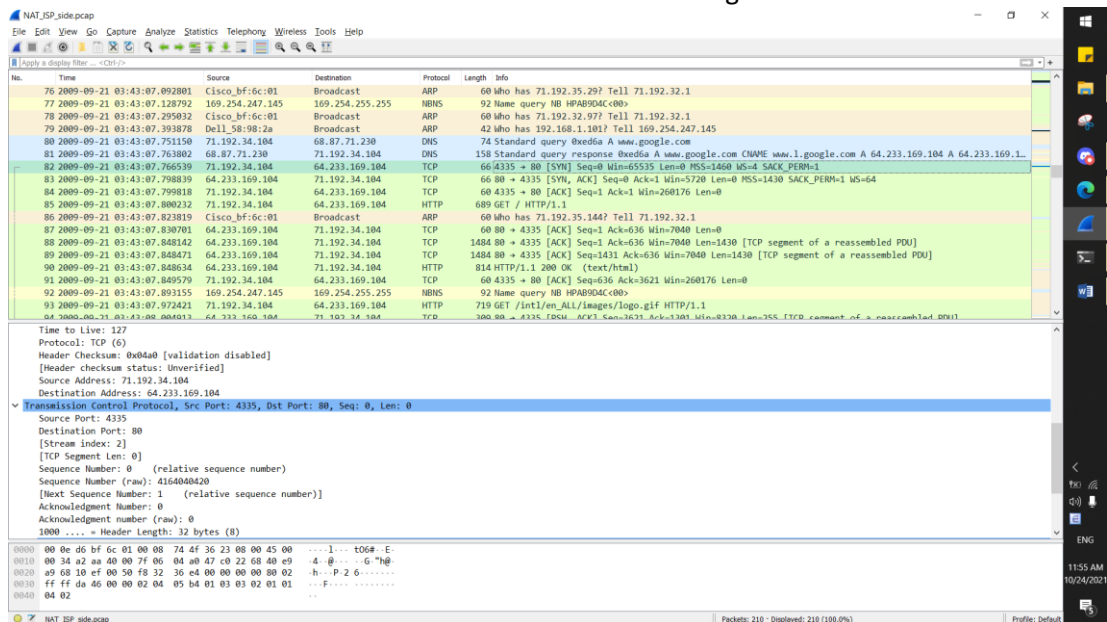
6. Time: 7.800232 – Source : 71.192.31.104, 4335 – Destination: 64.233.169.104, 80

Only the source IP address has changed

7. Are any fields in the HTTP GET message changed? (Answer: No) Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version (Answer: No), Header Length (Answer: No), Flags (Answer: No), Checksum (Answer: Yes). If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change. (Answer: Since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed).



8. Time: 7.848634 – Source: 64.233.169.104, 80 – Destination: 71.192.34.104, 4335. Only the destination IP address has changed



9. SYN: Time: 7.766539 – Source: 71.192.34.104, 4335 Dest: 64.233.169.104, 80

ACK: time: 7.798839 – Source: 64.233.169.104, 80 – Dest: 71.192.34.104, 4335

For the SYN, the source IP address has changed, for the ACK, the destination IP address has changed . The port numbers are unchanged.

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