Computer Network 1

LAB 4c

Wireshark lab NAT

Student Name: Alexandre Rousseau

Student ID: 1952001

1. What is the IP address of the client?

IP Address is 192.168.1.100

1. The client communicates with several different Google servers 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. 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.

Http doesn’t return any result but ip.addr == 64.233.169.104 returns result.

1. Une image contenant table

   Description générée automatiquement Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

Source IP Address: 192.168.1.199, Port: 4335

Destination IP Address: 64.233.169.104, Port: 80

1. 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?

Time the corresponding 200 OK HTTP: 7.158432000 seconds

Source IP Address: 64.233.169.104, Port: 80

Destination IP Address: 192.168.1.100, Port: 4335

1. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN.? At what time is this ACK received at the client?

SYN Time: 7.075657000 seconds

SYN Source IP Address: 192.168.1.100, Port: 4335

SYN Destination IP Address: 64.233.169.104, Port: 80

ACK Time: 7.108986000 seconds

ACK Source IP Address: 64.233.169.104, Port: 80

ACK Destination IP Address: 192.168.1.100, Port 4335

1. In the NAT\_ISP\_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT\_home\_side trace file). At what time does this message appear in the NAT\_ISP\_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT\_ISP\_side trace file)? Which of these fields are the same, and which are different, than in your answer to question 3 above?

Time: 6.069168000 seconds

Source IP Address: 71.192.34.104, Port: 4335

Destination IP Address: 64.233.169.104, Port: 80

Destination IP, source IP and ports are different.

1. Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum? If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

GET Message has not changed.

Version is the same.

Source IP changed from 192.168.1.100 to 71.192.34.104 but port is the same.

Header checksum changed from (Home) 0xa94a to (ISP) 0x022f

Header checksum changed because IP Address changed from 192.168.1.100 to 71.192.34.104

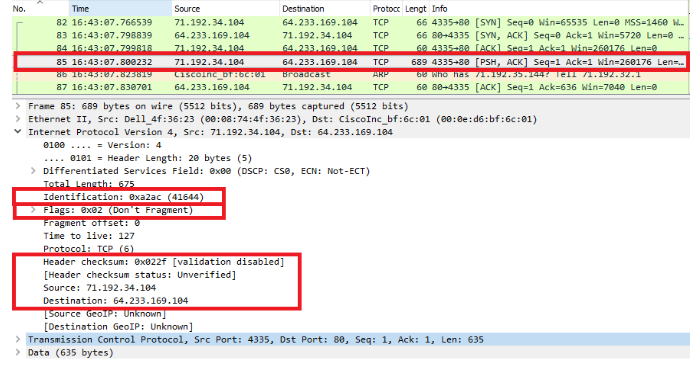


Figure 1: ISP

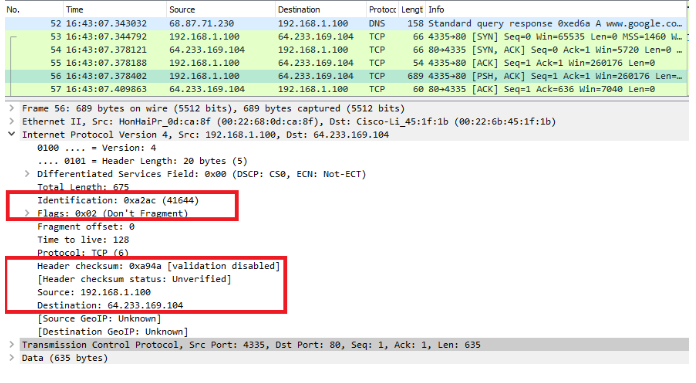


Figure 2: Home

1. 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?

HTTP 200 OK message first time: 6.117078000 seconds.

HTTP 200 OK message Source IP : 64.233.169.104, Port : 80

HTTP 200 OK message Destination IP : 71.192.34.104, Port : 4335

Version is the same, Flag does not change.

Time to live change

Une image contenant texte

Description générée automatiquementHeader checksum changed

1. In the NAT\_ISP\_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?

SYN:

Time: 6.035475000 seconds

Source IP Address: 71.192.34.104

Destination IP Address: 64.233.169.104

Une image contenant texte

Description générée automatiquementTime to live changed

ACK:

Time: 6.067775000 seconds

Source IP Address: 64.233.169.104

Destination IP Address: 71.192.34.104

Une image contenant texte

Description générée automatiquementIdentification, Time to live, Flags, Source and Destination IP changed

1. Using your answers to 1-8 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-8 above.

In the WAN, the outside world can see only one client IP address which is the NAT router’s IP – 71.192.34.104. Internal LAN IP Address of the client is 192.168.1.100. The rooter will use the port number after its IP, 71.192.34.104:4335 to forward the packets to the actual client IP – 192.168.1.100:4335.

|  |  |  |  |
| --- | --- | --- | --- |
| WAN (Outside) | | LAN (Local) | |
| IP | Port | IP | Port |
| 71.192.34.104 | 4335 | 192.168.1.100 | 4335 |

**Extra Credit**: The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200 OK request/response studied above. For example, in the NAT\_home\_side trace file, consider the client-to-server GET at time 1.572315, and the GET at time 7.573305. Research the use of these two HTTP messages and write a half page explanation of the purpose of each of these messages.

Before answering the question about google safe browsing, I visited the official website and read about detailed information on Google safe browsing. Based on the description, the Google safe browsing protects clients from malware or unwanted software. When a client clocks on a link from Google’s search results, safe browsing automatically checks the website for the client through Google’s latest update list of unsafe website list. If client visit an unsafe website that contains suspicious software or malware, client gets a warning page. The HTTP request and response in the NAT\_home\_side trace file shows safe browsing in work.

1. In HTTP GET at frame 20 at time 1.572315 the header includes the request URL “safebrowsing cache.google.com/safebrowsing/rd/googlemalware-shaver\_s\_15361-15365.15661-15365”.
2. In HTTP GET at frame 104 at time 7.573305 the header includes the request URL “google.com/generate\_204”

The first URL directs the client to the safebrowsing cache site, while the second URL directs the client to the target website, which means that the website is safe to visit. After looking at the two HTTP GET messages, I found some interesting results. The Destination IP changed from 74.125.106.31 in frame 20 to 74.125.91.113 in frame 104. Additionally, the identification in the header changed because each one is a uniquely assigned number, and the Header checksums changed because the destination address changed. Between frame 20 and 104, the source IP transition twice – once at frame 52 from 74.125.106.31 (safebrowsing cache.google.com) to 64.233.169.104 (www.google.com) and again at frame 96 from 64.233.169.104 (www.google.com) to 74.125.106.31 (clients1.google.com). Both times, there are DNS queries and query answer. Maybe we can guess that there was a Google Search query at frame 96. I tried safebrowsing in real like using Wireshark to capture activities while visiting a website through Google search engine. However, I could not find safebrowsing frame at all. Instead of that, I found TLSv1.2 protocol with handshakes and encrypted DNS protocol.

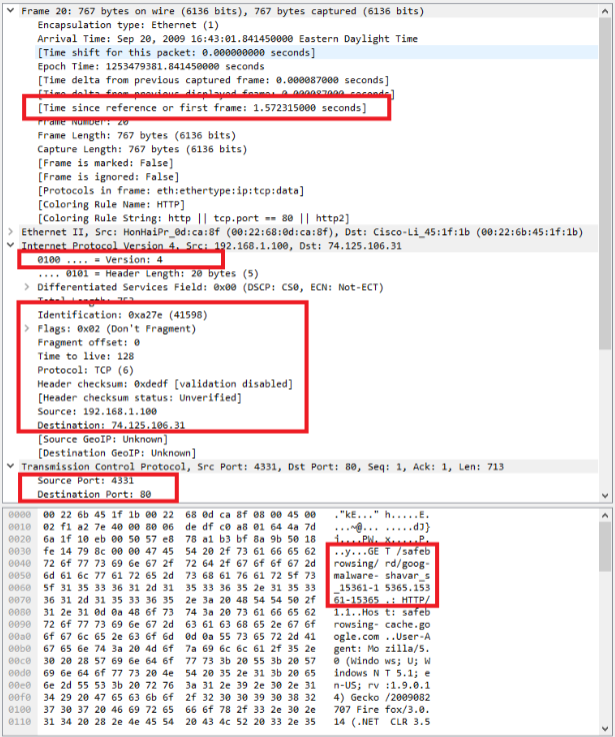


Figure 3: Client to server GET at time 1.572315

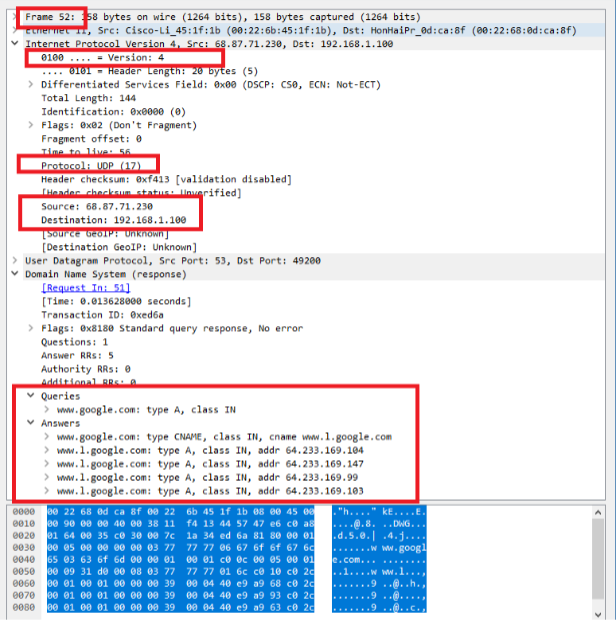


Figure 4: Transition to Source IP: 64.233.169.104, Home\_side\_Frame 52

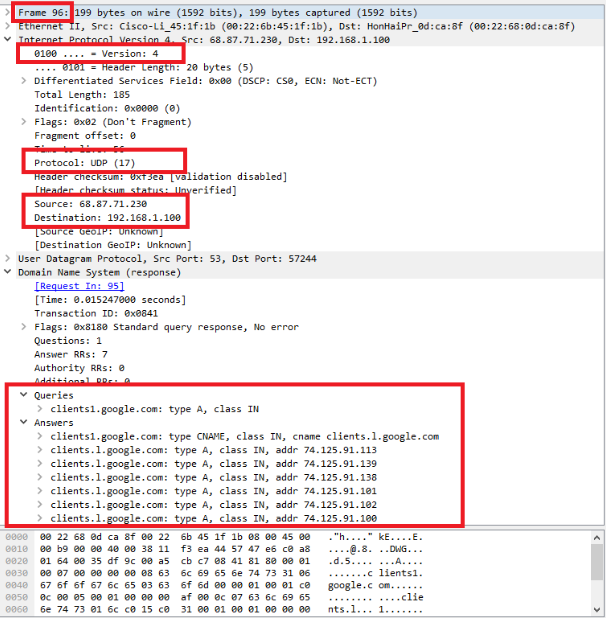


Figure 5: Transition to Source IP Address: 74.125.91.113, Home\_side\_Frame 96

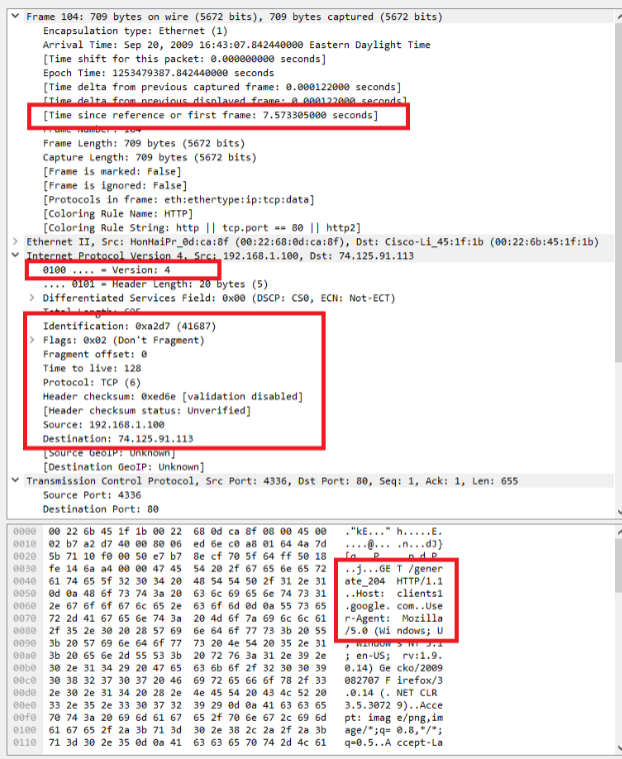


Figure 6: Client to server GET at time 7.573305