CS494 – Project 2 (Wireshark)

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

1. **What is the IP address of the client?**
   The address of the 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. 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 7.102967. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?**

3. **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?**
   Answer:
   - Source: 192.168.1.100, 4335
   - Destination: 64.233.169.104, 80)

4. **At what time 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:
   - The time at which the corresponding 200 OK HTTP message received from the Google server is 7.158798
   - Source IP : 64.233.169.104
   - Source port : 80
   - Destination IP : 192.168.1.100
   - Destination port : 4335

5. **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 7.102967?**

   Answer:
   The time is: 7.075657

   What are the source and destination IP addresses and source and destination ports for the TCP SYN segment?

   Answer:
   - Source: 192.168.1.100, 4335
   - Destination: 64.233.169.104, 80

   What are the sources and destination IP addresses and source and destination ports of the ACK sent in response to the SYN?

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

Answer:
- Source: 64.233.169.104, 80
- Destination: 192.168.1.100, 4335

At what time is this ACK received at the client?

Answer:
ACK is received at the client at second 7.108986

6. **In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.102967 (where t=7.102967 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?**

Answer:
HTTP GET message appear in NAT_ISP_side trace file at second 6.069168

What are the sources 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)?

Answer:
- Source: 71.192.34.104, 4335
- Destination: 64.233.169.104, 80

Which of these fields are the same, and which are different, than in your answer to question 3 above?

Answer:
Only the source IP address has changed.

7. **Are any fields in the HTTP GET message changed?**

Answer:
There is no field 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 or Checksum?

Answer:
Version, Header length, flags are not changed.
Checksum is changed.

If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

Answer:
The IP source address has changed and the checksum includes the value of the source IP address
- The checksum has changed.

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

8. In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server?

Answer:

The first 200 OK HTTP message received from the Google server is at second 6.308118

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: 64.233.169.104, 80
- Destination: 71.192.34.104, 4335

Which of these fields are the same, and which are different than your answer to question 4 above?

Answer:

Only the destination IP address has changed.

9. 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?

Answer:

The client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured at 6.035475, and 6.067775, respectively.

What are the source and destination IP addresses and source and destination ports for these two segments?

Answer:

SYN:

- Source: 71.192.34.104, 4335
- Destination: 64.233.169.104, 80

ACK:

- Source: 64.233.169.104, 80
- Destination: 71.192.34.104, 4335

Which of these fields are the same, and which are different than your answer to question 5 above?

Answer:

SYN:

The source IP address has changed

ACK:

The destination IP address has changed.
The port numbers are unchanged.

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

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

Answer:

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