Lab7 Wireshark_NAT

- 学号:1813075
- 姓名:刘茵

1. What is the IP address of the client?

```
No.     Time           Source                Destination           Protocol Length Info
      7 1.208040       192.168.1.100         74.125.91.113         HTTP     1035   POST /safebrowsing/downloads?
```

答：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 .

答:

http && ip.addr == 64.233.169.104

	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswI
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16a1c5.js HT
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefin
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1
124	7.737783	64.233.169.104	192.168.1.100	HTTP	269	HTTP/1.1 204 No Content
127	7.763501	64.233.169.104	192.168.1.100	HTTP	1204	HTTP/1.1 200 OK (image/x-icon)

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?

```
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
Hypertext Transfer Protocol
```

答：源IP：192.168.1.100 端口：4335

目的IP：64.233.169.104 端口：80

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?

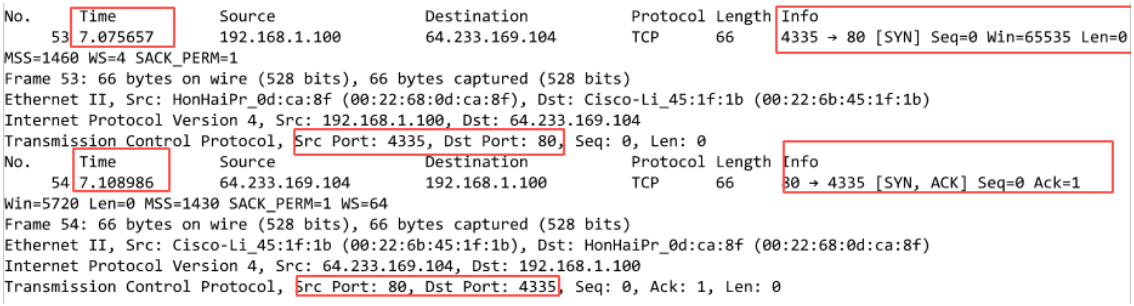
```
No.     Time           Source                Destination           Protocol Length Info
     60 7.158797       64.233.169.104        192.168.1.100         HTTP     814    HTTP/1.1 200 OK  (text/html)
Frame 60: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)
Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
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, Ack: 636, Len: 760
[3 Reassembled TCP Segments (3620 bytes): #58(1430), #59(1430), #60(760)]
Hypertext Transfer Protocol
Line-based text data: text/html (12 lines)
```

答：时间：7.158797

源IP：64.233.169.104 端口：80

目的IP：192.168.1.100 端口：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 7.109267? 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? (Note: to find these segments you will need to clear the Filter expression you entered above in step 2. If you enter the filter “tcp”, only TCP segments will be displayed by Wireshark).



答：SYN 报文：

发送时间：7.075657 s

源IP: 192.168.1.100 端口: 4335

目的IP：64.233.169.104 端口:80

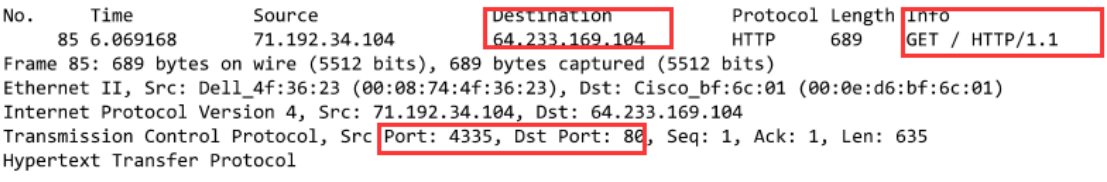
SYN ACK 报文：

收到时间：7.108986 s

源IP：64.233.169.104 端口：80

目的IP：192.168.1.100 端口：4335

6. In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (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?



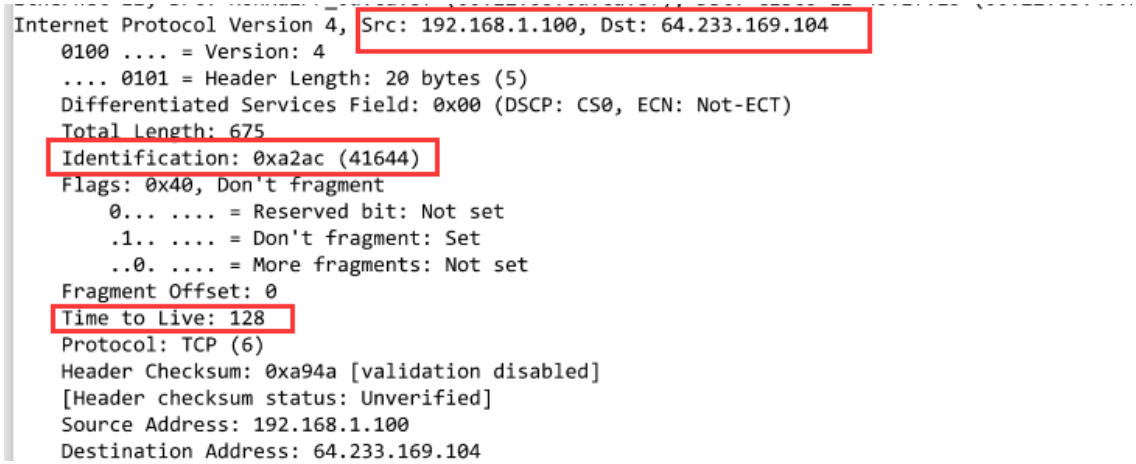
答：出现时间：6.069168 s

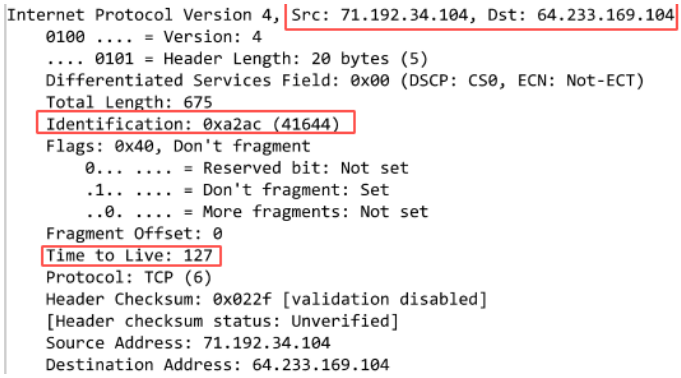
源IP：71.192.34.104 端口：4335

目的IP：64.233.169.104 端口：80

目的地址和端口相同，源地址不同。

7. 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.

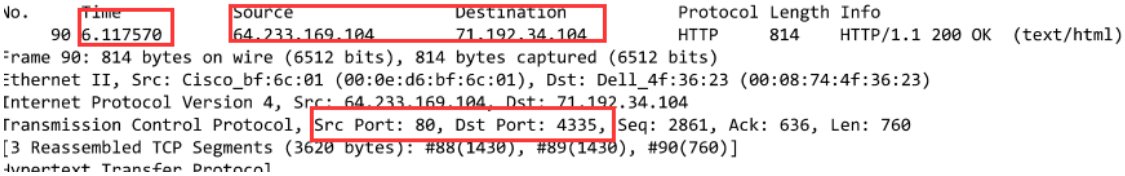




答：HTTP消息没有更改。

IP数据报中的源IP地址、校验和、TTL发生改变。

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?



答：时间：6.117570

源IP：64.233.169.104 端口：80

目的IP：71.192.34.104 端口：4335

源地址和端口相同，目的地址不同。

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? 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?

```
No.     Time           Source                Destination           Protocol Length Info
     82 6.035475       71.192.34.104         64.233.169.104        TCP      66     4335 → 80 [SYN] Seq=0 Win=65535 Len=0
MSS=1460 WS=4 SACK_PERM=1
Frame 82: 66 bytes on wire (528 bits), 66 bytes captured (528 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
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xa2aa (41642)
    Flags: 0x40, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 127
    Protocol: TCP (6)
    Header Checksum: 0x04a0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 71.192.34.104
    Destination Address: 64.233.169.104
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
No.     Time           Source                Destination           Protocol Length Info
     83 6.067775       64.233.169.104        71.192.34.104         TCP      66     80 → 4335 [SYN, ACK] Seq=0 Ack=1
Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64
Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xf61a (63002)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 51
    Protocol: TCP (6)
    Header Checksum: 0x3d10 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 64.233.169.104
    Destination Address: 71.192.34.104
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0
```

答：SYN 报文：

发送时间：6.035475 s

源IP: 71.192.34.104 端口: 4335

目的IP：64.233.169.104 端口:80

SYN ACK 报文：

收到时间：6.06775 s

源IP：64.233.169.104 端口：80

目的IP：71.192.34.104 端口：4335

SYN的源目的IP不同，SYN ACK的目的IP不同。

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

答：

	WAN side	**LAN side**
IP	71.192.34.104	192.168.1.100
PORT	4355	4355