Lab4 NAT

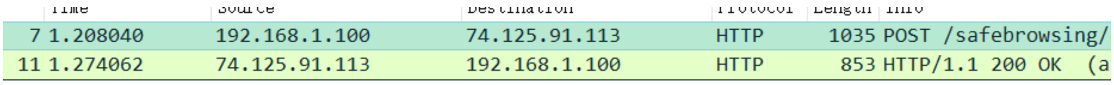
宁晨然 17307130178

一、实验目的

了解网络抓包中的信息。

二、实验过程

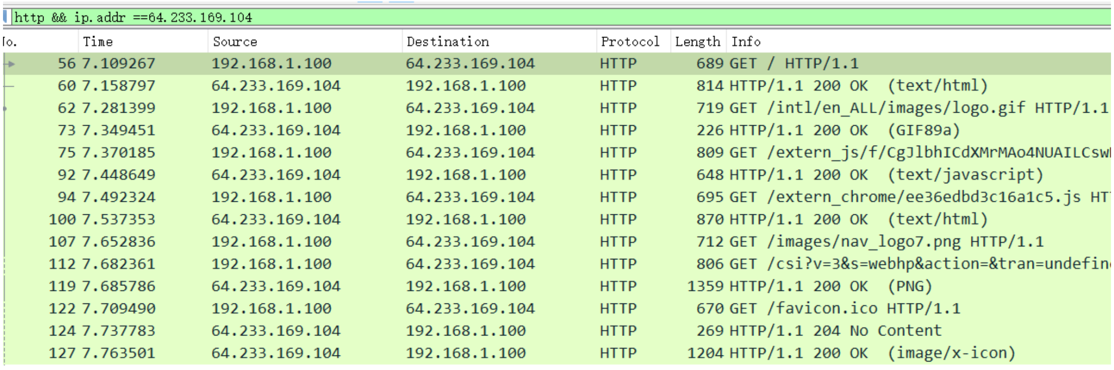
1. What is the IP address of the client?



	Time	Source	Destination	Protocol	Length	Info
7	1.208040	192.168.1.100	74.125.91.113	HTTP	1035	POST /safebrowsing/
11	1.274062	74.125.91.113	192.168.1.100	HTTP	853	HTTP/1.1 200 OK (a

IP 地址是 192.168.1.100

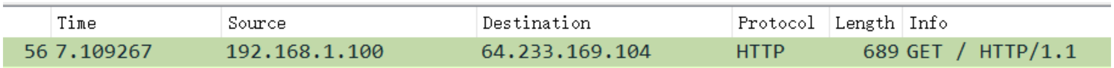
2. The client actually communicates with several different Google servers in order to implement “safe browsing.” (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing 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 .



```
http && ip.addr ==64.233.169.104
```

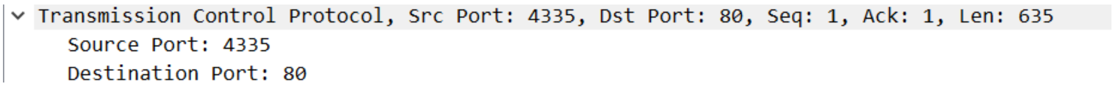
lo.	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	7.349451	64.233.169.104	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/CgJlbhICdXMrMAo4NUAILCswl
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?



	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1

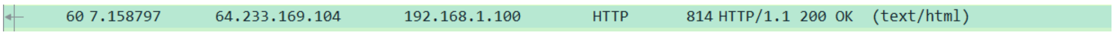
IP source address = 192.178.1.100/ IP destination address = 64.233.169.104



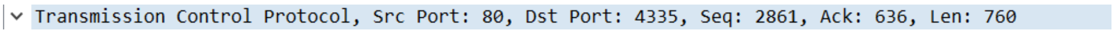
```
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
    Source Port: 4335
    Destination Port: 80
```

TCP source port = 4335 ; TCP destination port = 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?



60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)

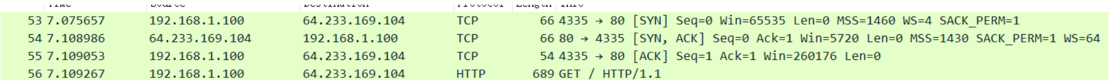


```
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
```

IP source = 64.233.169.104 ; destination = 192.168.1.100

TCP source port = 80 ; 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 7.109267? 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).



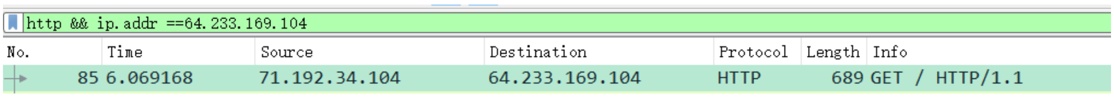
```
   53 7.075657     192.168.1.100      64.233.169.104     TCP       66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
   54 7.108986     64.233.169.104     192.168.1.100      TCP       66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64
   55 7.109053     192.168.1.100      64.233.169.104     TCP       54 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
   56 7.109267     192.168.1.100      64.233.169.104     HTTP     689 GET / HTTP/1.1
```

三次握手如上图，第一次客户-服务器的 SYN 段信息在 7.075657 时间发送的。

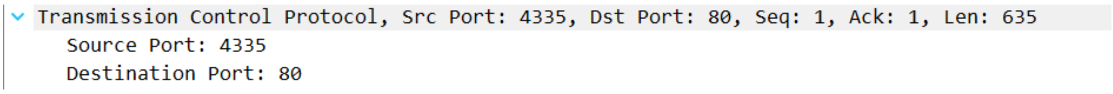
IP source address = 192.168.1.100 ; destination = 64.233.169.104

ACK: IP source = 64.233.169.104 ; destination = 192.168.1.100; 时间 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 7.109267 (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?



```
http && ip.addr ==64.233.169.104
No.      Time          Source             Destination        Protocol  Length  Info
      85 6.069168      71.192.34.104      64.233.169.104     HTTP         689  GET / HTTP/1.1
```



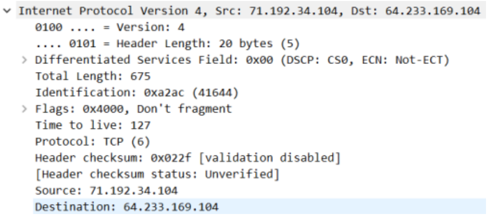
```
v Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
    Source Port: 4335
    Destination Port: 80
```

time = 6.069168； destination IP = 64.233.169.104 ; source IP = 71.192.34.104

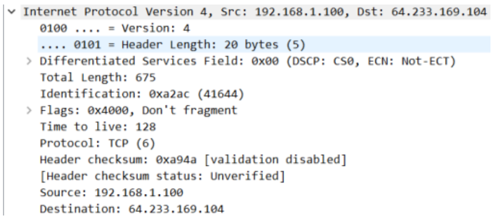
TCP source port = 4335； destination port = 80

时间不同，源地址和目标地址不同，TCP 端口相同。

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.



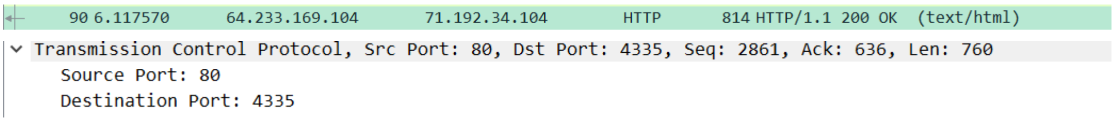
```
v Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 675
    Identification: 0xa2ac (41644)
  > Flags: 0x4000, Don't fragment
    Time to live: 127
    Protocol: TCP (6)
    Header checksum: 0x022f [validation disabled]
    [Header checksum status: Unverified]
    Source: 71.192.34.104
    Destination: 64.233.169.104
```



```
v 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)
    Total Length: 675
    Identification: 0xa2ac (41644)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xa94a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.100
    Destination: 64.233.169.104
```

左图是 ISPside，右图是 homeside。对比发现，除了上一题中提到的 ip src/dst 变化外，time tolive 变化， header checksum 变化。因为 header checksum 是 ip 头部的校验位，所以头部信息变化自然 checksum 也会变化。

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?



```
   90 6.117570    64.233.169.104    71.192.34.104    HTTP    814 HTTP/1.1 200 OK  (text/html)
 Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
    Source Port: 80
    Destination Port: 4335
```

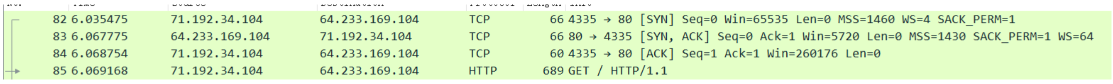
time = 6.117570

ip source = 64.233.169.104 ; dst = 71.192.34.104

TCP source port = 80; dst port = 4335

time 和目的 ip 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?



```
   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
   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
   84 6.068754    71.192.34.104     64.233.169.104    TCP     60 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
   85 6.069168    71.192.34.104     64.233.169.104    HTTP   689 GET / HTTP/1.1
```

client-to-server TCP SYN time = 6.035475;server-to-client TCP ACK time = 6.067775

source ip = 71.192.34.104 -> dst = 64.233.169.104; 第二个反过来

发送 TCP 的源地址 ip 不同，其他都相同。