**电子科技大学**

**实**

**验**

**报**

**告**

学生姓名：李昊霖

学号：2019270102007

课程名称：计算机网络基础

指导教师：杨宁

日期： 2021 年 4 月 1 日

实验项目名称： 4-2 wireshark-NAT实验

报告评分： 教师签字：

**一、实验概要**

**实验目的:**

研究 NAT 协议内容，学会分析NAT设备的抓包文件。

**实验内容**：

用在家庭网络的一个客户端PC发送到 www.google.com 简单HTTP请求并且捕获它，在该客户端 PC 进行抓包并存为 NAT\_home\_side文件，将位于 NAT 路由连 ISP 网络的 Wireshark 的抓包结果称为 NAT\_ISP\_side。

**二、实验步骤、数据及分析结果**

**实验步骤:**

下载作者的抓包文件并进行分析，回答指导书相关问题。

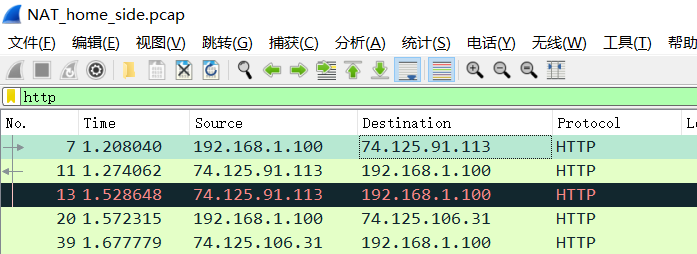
**实验数据及分析:**

回答指导书问题**：**

问题1-5：

1. What is the IP address of the client?

答:192.168.1.100,如图。



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

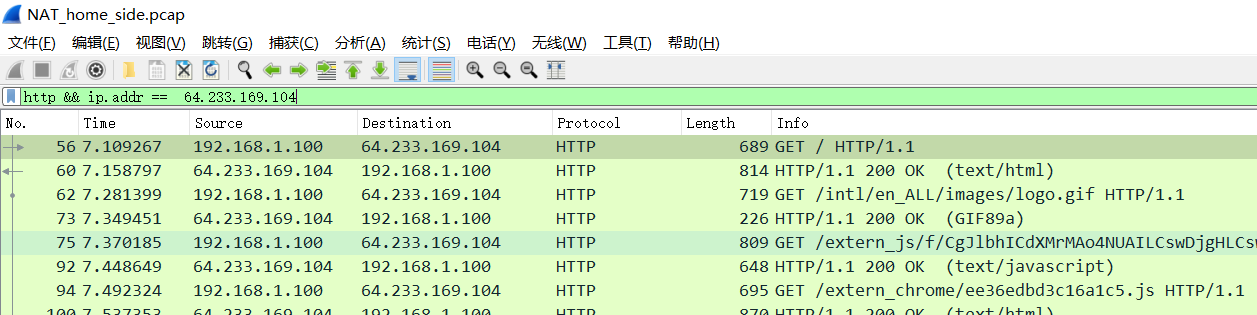
main Google server that will serve up the main Google web page has IP address

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：如图。



3. Consider now the HTTP GET sent from the client to the Google server (whose IP

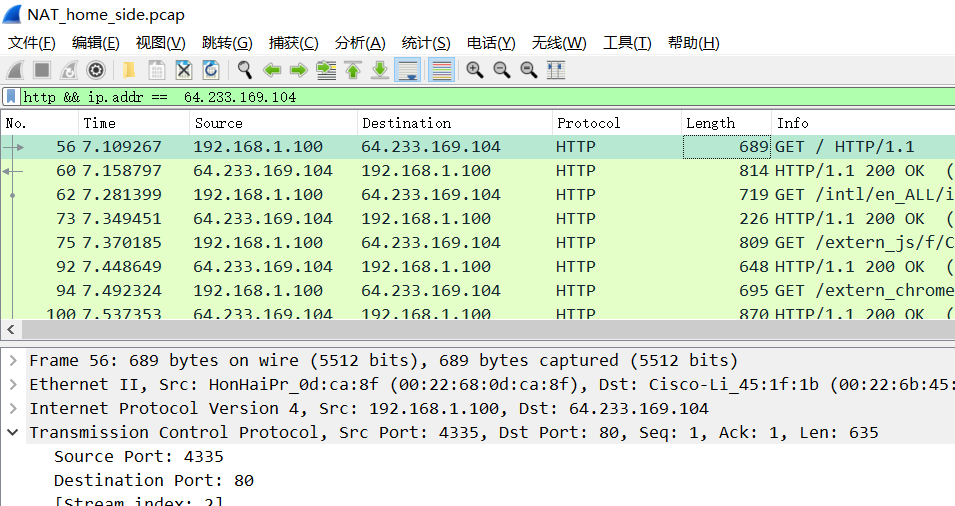
address is IP address 64.233.169.104) at time 7.109267. What are the source and

destination IP addresses and TCP source and destination ports on the IP datagram

carrying this HTTP GET?

答：源 IP 192.168.1.100 端口 4335

目的 IP 64.233.169.104 端口 80



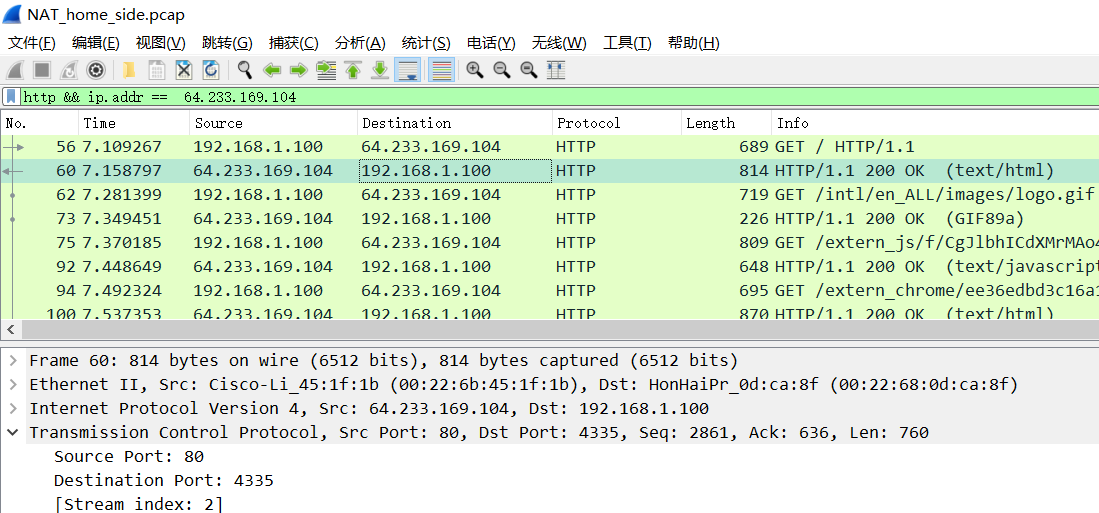
4. At what time is the corresponding 200 OK HTTP message received from the

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?

答：时间 7.158797 s，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

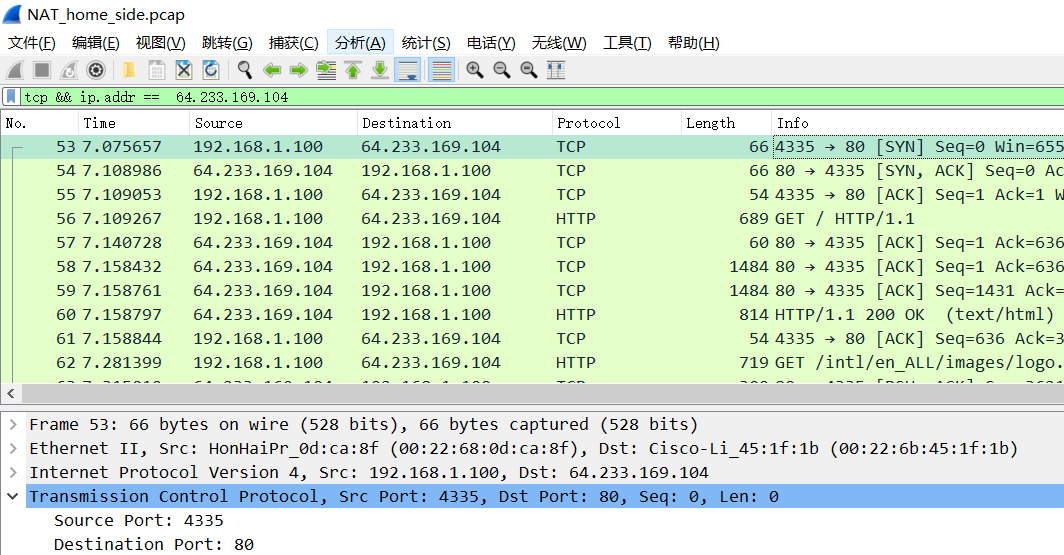
response to the SYN. At what time is this ACK received at the client? (Note: to

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).

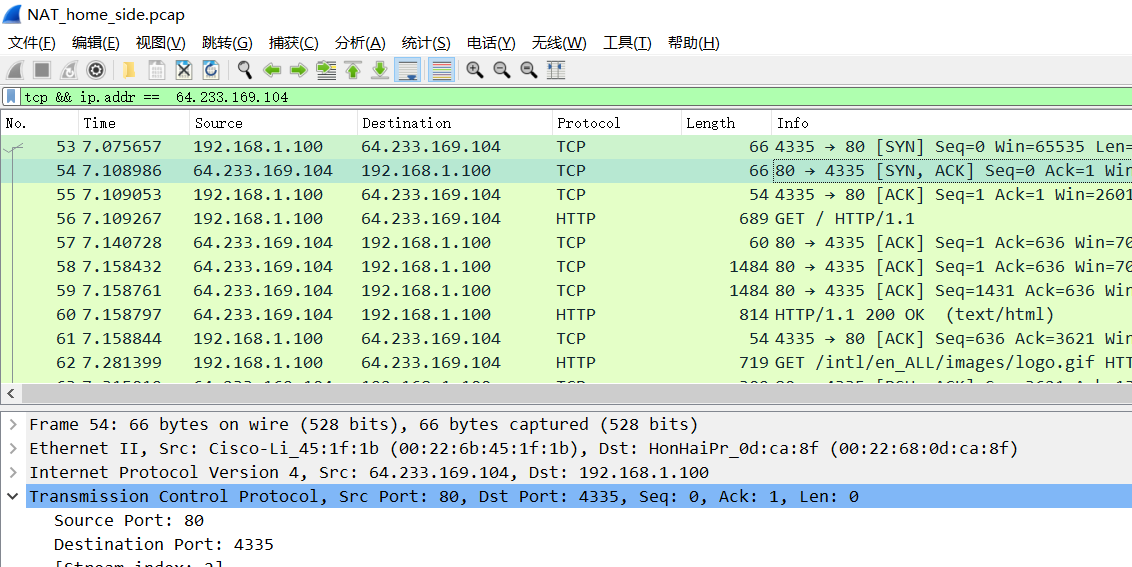
答：7.075657 s发送TCP-SYN报文，信息如下：

源 IP 192.168.1.100 端口 4335 目的 IP 64.233.169.104 端口 80



7.108986 s收到SYN,ACK报文，信息如下：

源 IP 64.233.169.104 端口 80 目的 IP 192.168.1.100 端口 4335



问题6-10：

6. In the NAT\_ISP\_side trace file, find the HTTP GET message was sent from the

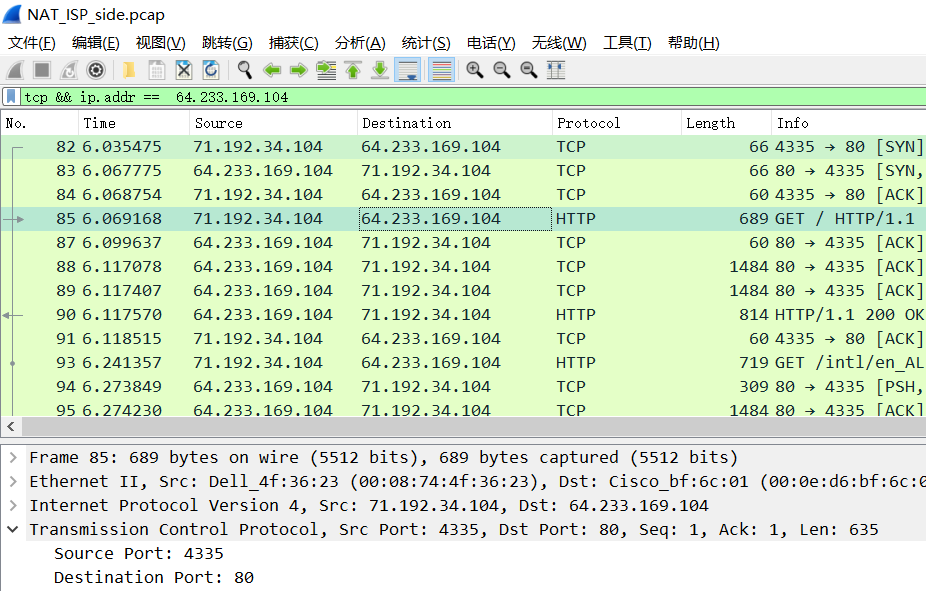
client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT\_home\_side trace file). At what time does this message appear in the NAT\_ISP\_side trace file? What are the source and destination IP addresses and TCP source and destination ports on 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：6.069168 s

源 IP 71.192.34.104 端口 4335 目的 IP 64.233.169.104 端口 80

源端口，目的IP地址、端口与问题3相同

发送时间，源IP地址与问题3不同

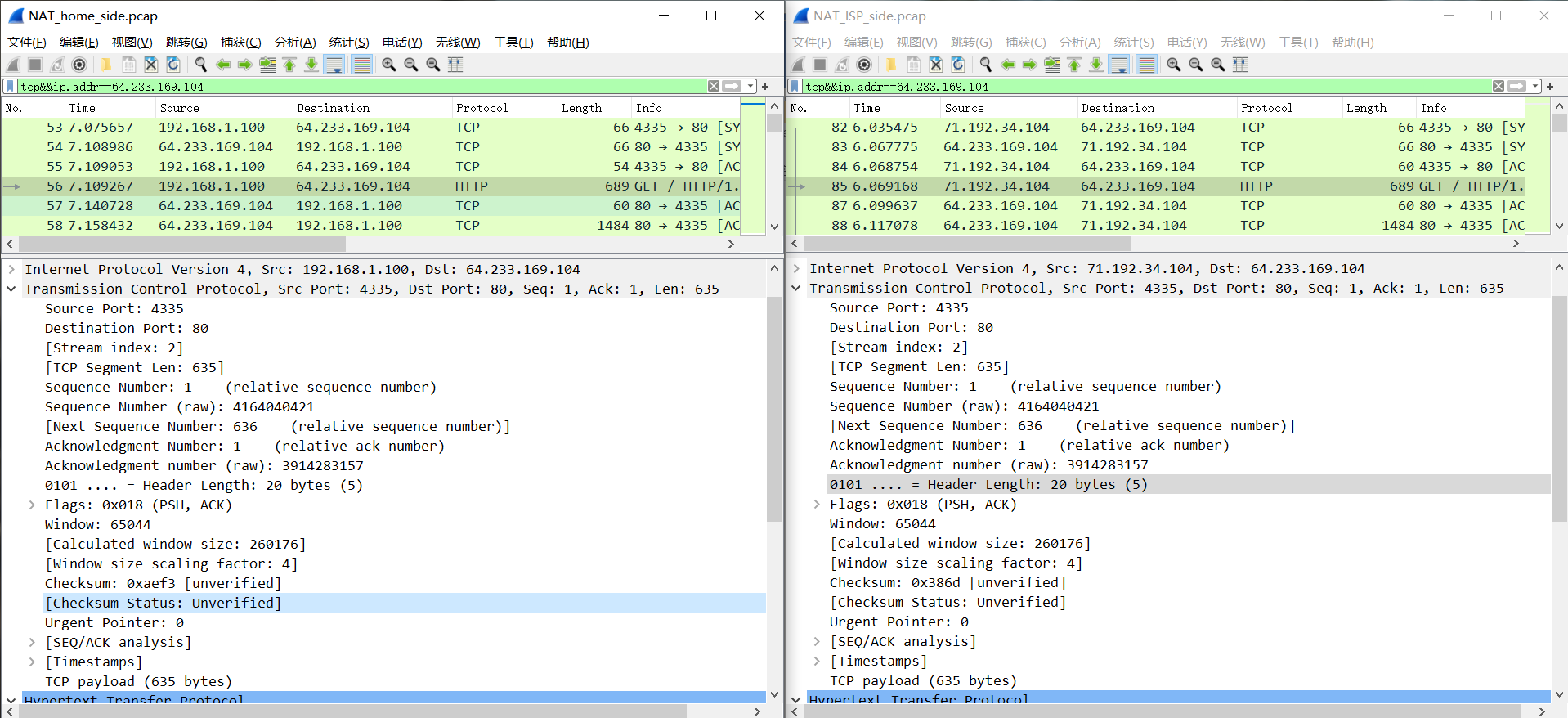


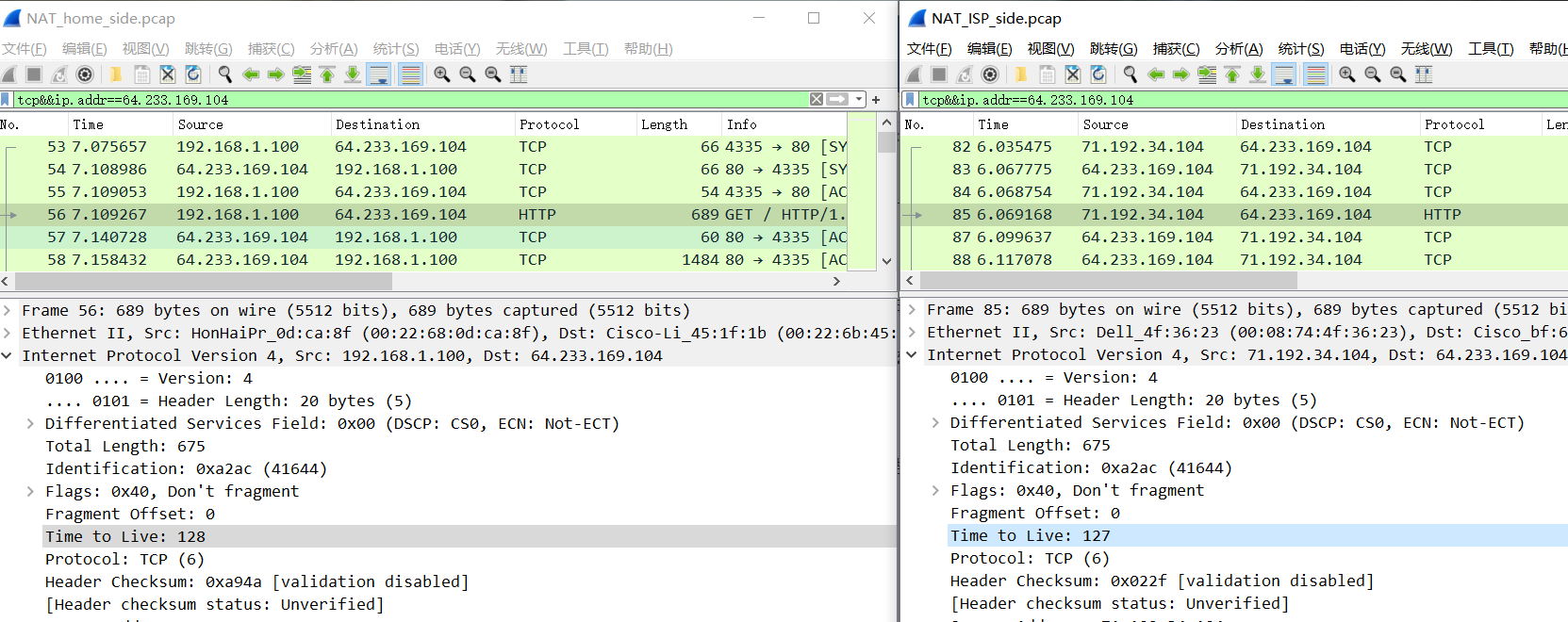
7. Are any fields in the HTTP GET message changed? Which of the following fields

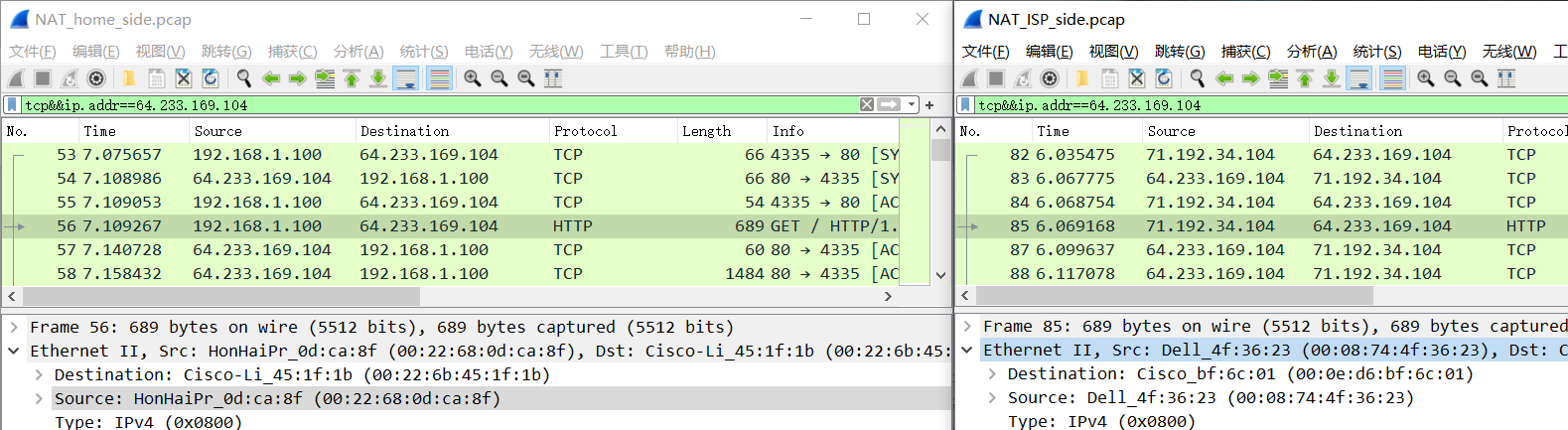
in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

答：GET报文中传输层仅校验和不同；IP报文中源IP从内网IP改为公网IP，且time to live 字段减一；此外，数据链

路层中MAC地址也不同。





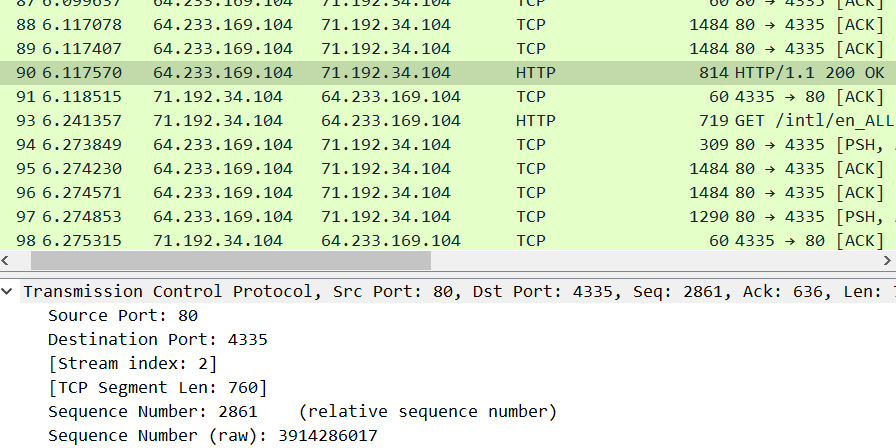


8. In the NAT\_ISP\_side trace file, at what time is the first 200 OK HTTP message

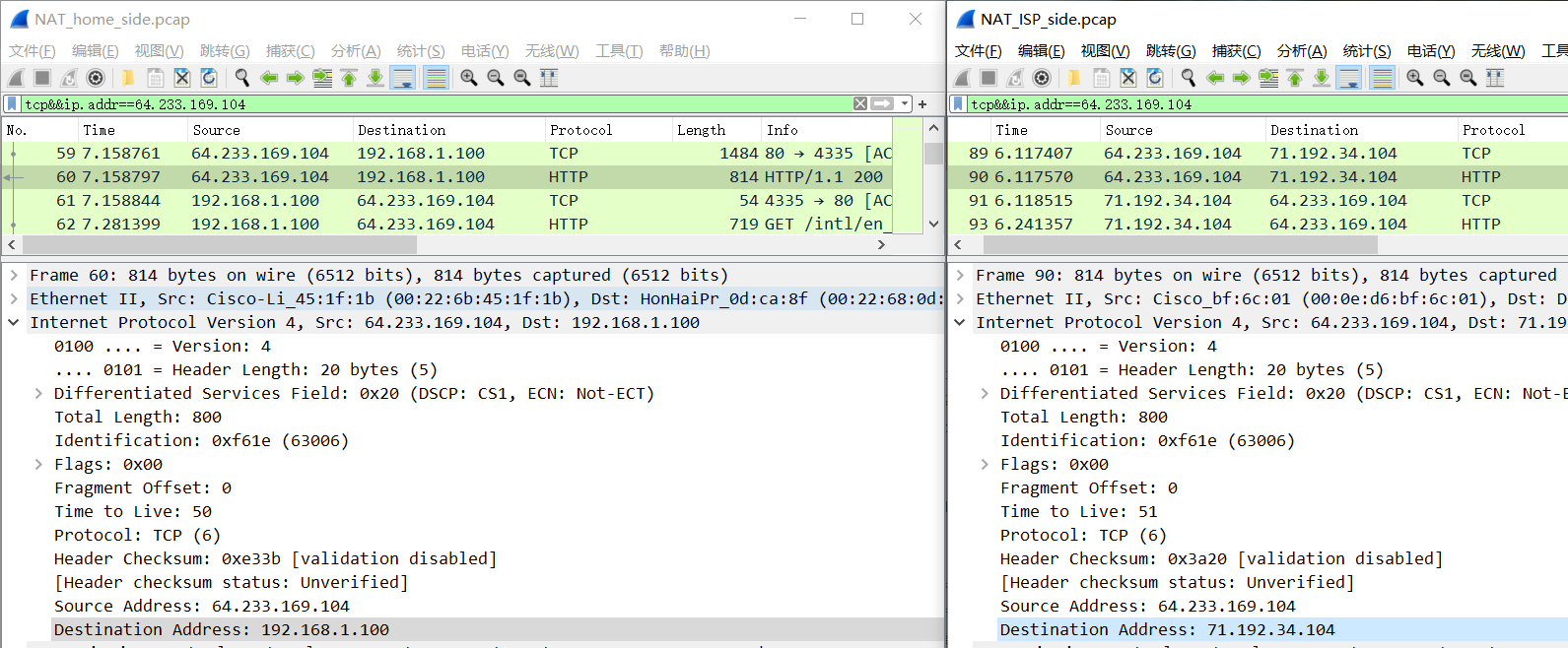
received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?

答：时间 6.117570 s

源 IP 64.233.169.104 端口 80 目的 IP 71.192.34.104 端口 4335



TCP报文中仅TCP校验码不同，IP报文中目的地址经过NAT路由器转化为内网IP，且数据链路层MAC地址不同。



9. In the NAT\_ISP\_side trace file, at what time were the client-to-server TCP SYN

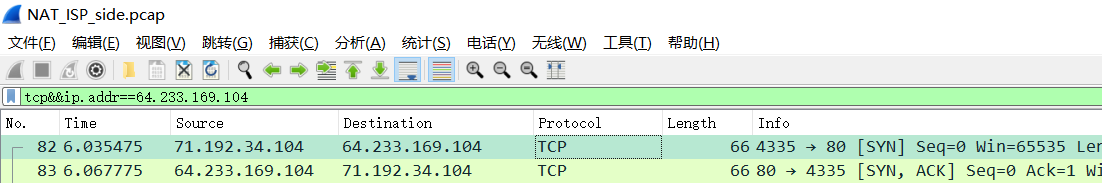
segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?

答：6.035475 s发送TCP-SYN报文，信息如下：

源 IP 71.192.34.104 端口 4335 目的 IP 64.233.169.104 端口 80

6.067775 s收到SYN，ACK报文，信息如下：

源 IP 64.233.169.104 端口 80 目的 IP 71.192.34.104 端口 4335



TCP报文中仅TCP校验码不同，IP报文中源IP地址经过NAT路由器转化为公网IP，且数据链路层MAC地址不同。

Figure 4.25 in the text shows the NAT translation table in the NAT router.

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

HTTP connection considered in questions 1-8 above.

|  |  |
| --- | --- |
| NAT转换表 | |
|
| WAN端 | LAN端 |
| 71.192.34.104，4335 | 192.168.1.100，4335 |

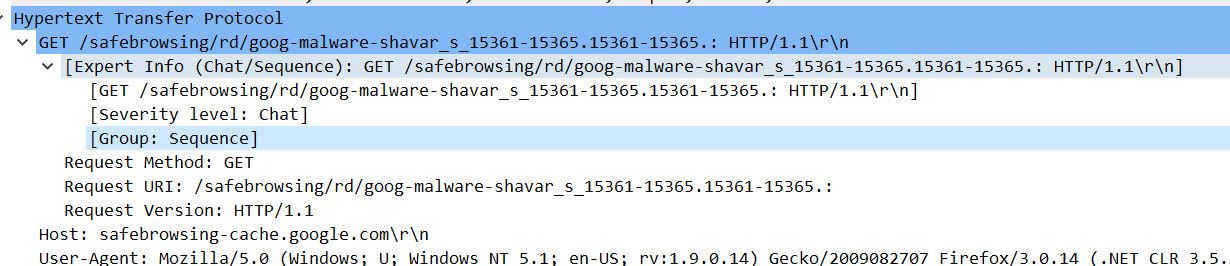
额外问题**：**

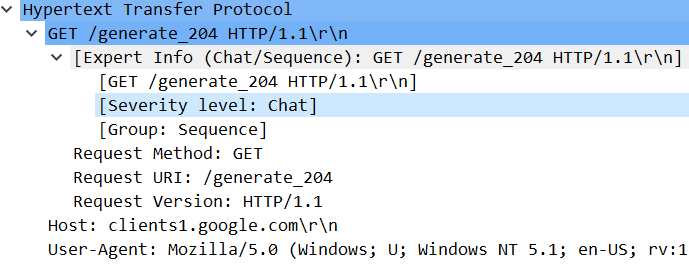
Extra Credit: The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200 OK request/response studied above. For example, in the NAT\_home\_side trace file, consider the client-to-server GET at time 1.572315, and the GET at time 7.573305. Research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

答：两份报文中的特殊字段为：

HTTP 767 GET /safebrowsing/rd/goog-malware-shavar\_s\_15361-15365.15361-15365.: HTTP/1.1

HTTP 709 GET /generate\_204 HTTP/1.1





查阅资料可知这两条报文中的特殊字段应为来自于谷歌为保障安全性所使用的工具，其中[Severity level: Chat]字段指安全级别。

**三、总结及心得体会**

本次实验分析了多组报文经过NAT路由器转化前后的变化，让我深刻理解了NAT在内网和公网之间进行IP地址转化的过程，明白了NAT在解决IP地址不足的问题上起到的重要作用。

**四、对本实验过程及方法、手段的改进建议**

可以学习更多的类似GET /generate\_204 HTTP/1.1的报文，了解前沿的应用方法。