哈爾濱工業大學
Harbin Institute of Technology

计算机网络
课程实验报告

实验名称	利用 Wireshark 进行协议分析					
姓名	李劲光		院系	计算机学与技术学院		
班级	1903201		学号	L190202102		
任课教师	聂兰顺		指导教师	聂兰顺		
实验地点			实验时间			
实验课表现	出勤、表现得分(10)		实验报告得分(40)		实验总分	
	操作结果得分(50)					
教师评语						

计算机科学与技术学院 SINCE 1956...
School of Computer Science and Technology

实验目的：

（注：实验报告模板中的各项内容仅供参考，可依照实际实验情况进行修改。）
本次实验的主要目的。

熟悉并掌握 Wireshark 的基本操作，了解网络协议实体间进行交互以及报文交换的情况。

实验内容：

概述本次实验的主要内容，包含的实验项等。

1) 学习 Wireshark 的使用
2) 利用 Wireshark 分析 HTTP 协议
3) 利用 Wireshark 分析 TCP 协议
4) 利用 Wireshark 分析 IP 协议
5) 利用 Wireshark 分析 Ethernet 数据帧

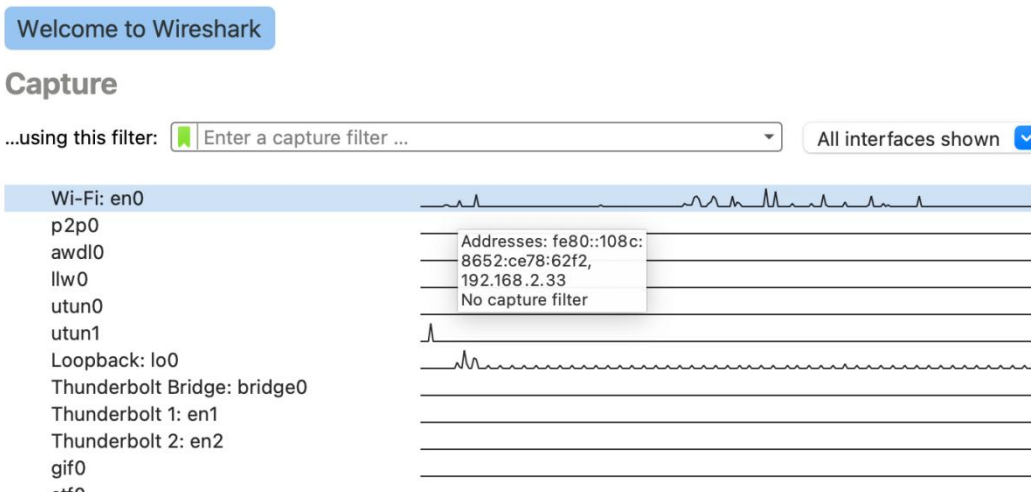
选做内容：

a) 利用 Wireshark 分析 DNS 协议
b) 利用 Wireshark 分析 UDP 协议
c) 利用 Wireshark 分析 ARP 协议

实验过程：

以文字描述、实验结果截图等形式阐述实验过程，必要时可附相应的代码截图或以附件形式提交。

在本次实验中，IP地址分别是：192.168.2.33，172.20.10.3， MacOS 主机。



（一）Wireshark 的使用

在 Wireshark 的使用环节，然后访问 http://www.hit.edu.cn。在完整的页面加载完成后，结束分组捕获。在这一段时间 Wireshark 捕获了本机所有利用该无线网卡与其他网络实体进行交换的报文。

（二）HTTP 分析

1）HTTP GET/response 交互

-启动 Web browser，然后启动 Wireshark 分组嗅探器。在窗口的显

-示过滤说明处输入“http”，分组列表子窗口中将只显示所俘获到的 HTTP 报文。

-开始 Wireshark 分组俘获。

-在打开的 Web browser 窗口中输入一下地址：http://hitgs.hit.edu.cn/news

-停止分组俘获。

2）HTTP 条件 GET/response 交互

-启动浏览器，清空浏览器的缓存（在浏览器中，选择“工具”菜单中的“Internet 选项”命令，在出现的对话框中，选择“删除文件”）。

-启动 Wireshark 分组俘获器。开始 Wireshark 分组俘获。

-在浏览器的地址栏中输入以下 URL: http://hitgs.hit.edu.cn/news,在你的浏览器中重新输入相同的 URL 或单击浏览器中的“刷新”按钮。

-停止 Wireshark 分组俘获，在显示过滤筛选说明处输入“http”,分组列表子窗口中将只显示所俘获到的 HTTP 报文。

（三）TCP 分析

A. 俘获大量的由本地主机到远程服务器的 TCP 分组

（1） 启动浏览器，打开 http://gaia.cs.umass.edu/Wireshark-labs/alice.txt 网页，得到 ALICE'S ADVENTURES IN WONDERLAND 文本，将该文件保存到你的主机上。

（2） 打开 http://gaia.cs.umass.edu/Wireshark-labs/TCP-Wireshark-file1.html， 如图 6-6 所示，窗口如下图所示。在 Browse 按钮旁的文本框中输入保存在你的主机上的文件 ALICE'S ADVENTURES IN WONDERLAND 的全 名（含路径），此时不要按 “Upload alice.txt file”按钮。

（3） 启动 Wireshark，开始分组俘获。

（4） 在浏览器中，单击“Upload alice.txt file”按钮，将文件上传到 gaia.cs.umass.edu 服务器，一旦文件上传完毕，一个简短的贺词信息将显示在你的浏览器窗口中。

（5） 停止俘获。

B. 浏览追踪信息，在显示筛选规则中输入“tcp”,可以看到在本地主机和服务器之间

传输的一系列 tcp 和 http 报文，你应该能看到包含 SYN 报文的三次握手。也可以看到有主机向服务器发送的一个 HTTP POST 报文和一系列的“http continuation”报文。

C. TCP 基础

（四）IP 分析

1. 使用 pingplotter 进行实验，启动 Wireshark 开始分组捕获，首先发送一系列 56 字节的包；再发送一系列 2000 字节的包；再发送一系列 3500 字节的包，然后停止 Wireshark 捕获。

2. 在这段时间捕获的数据包见文件，具体结果分析见实验结果部分。

（五）抓取 ARP 数据包

1. 利用 arp 查看本机的 ARP 缓存表

2. 开始 Wireshark 分组捕获，在命令行中输入：ping <IP>

3. ping 通之后利用停止 Wireshark 捕获，这段时间捕获的分组。

（六）抓取 UDP 数据包

启动 Wireshark 分组捕获，利用 QQ 给好友发送消息，消息发送结束后，停止分组捕获；这段时间捕获的报文分组见，具体结果分析见实验结果部分。

（七）利用 Wireshark 进行 DNS 协议分析

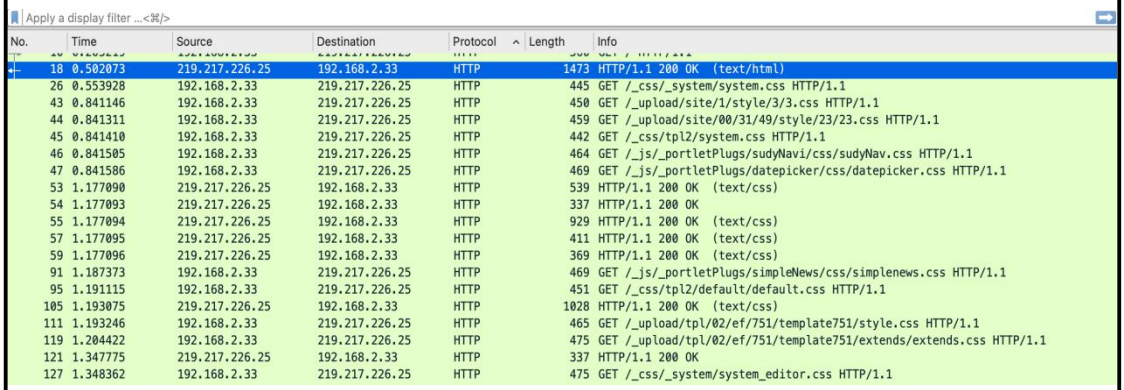
首先清空 dns 缓存，在浏览器中访问 http://www.google.com.hk/，进行 Wireshark 抓包，这段时间抓取的分组见，具体的结果分析见实验结果部分。

实验结果：

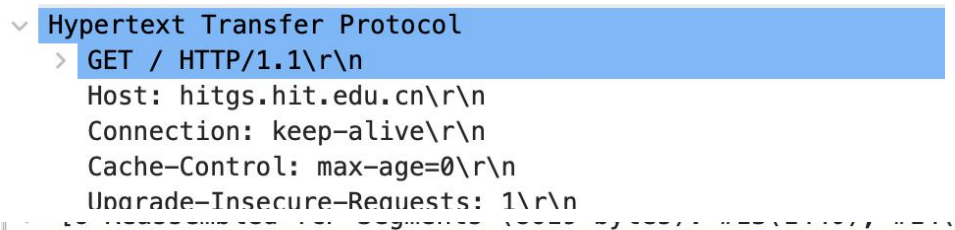
采用演示截图、文字说明等方式，给出本次实验的实验结果。

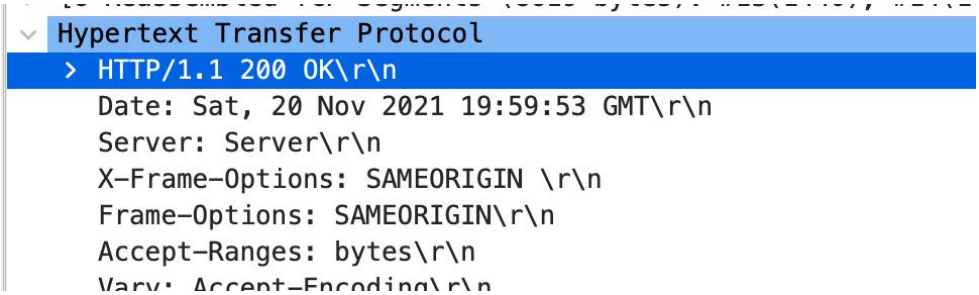
（二）HTTP 分析

1）HTTPGET/response 交互，启动浏览器，然后启动 Wireshark 分组嗅探器。浏览器窗口中输入访问以下地址：http://hitgs.hit.edu.cn 停止分组俘获捕获分组的截图如下。

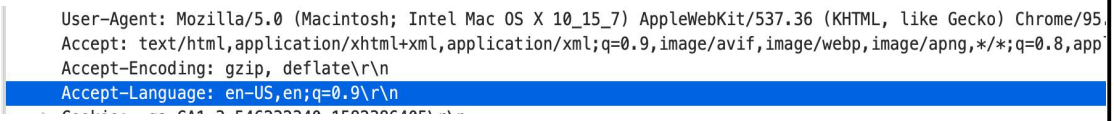


✧你的浏览器运行的是 HTTP1.0，还是 HTTP1.1？你所访问的服务器所运行 HTTP 协议的版本号是多少？

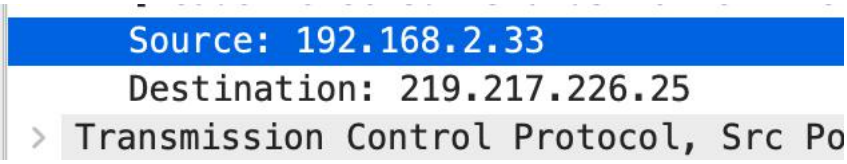




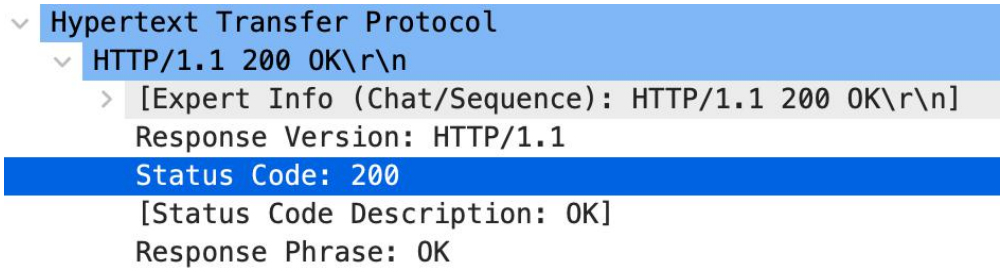
✧你的浏览器向服务器指出它能接收何种语言版本的对象？



✧你的计算机的 IP 地址是多少？服务器 http://hitgs.hit.edu.cn/news 的 IP 地址是多少？



✧从服务器向你的浏览器返回的状态代码是多少？



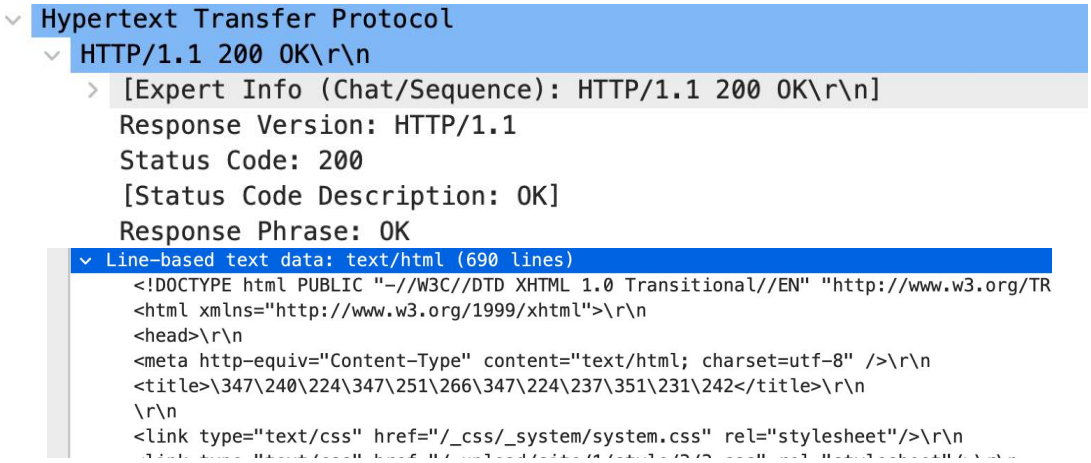
2) HTTP条件GET/response交互

✧分析你的浏览器向服务器发出的第一个 HTTP GET 请求的内容，在该请求报文中，是否有一行是：IF-MODIFIED-SINCE?

答：没有 IF-MODIFIED-SINCE 请求行。

✧分析服务器响应报文的内容，服务器是否明确返回了文件的内容？如何获知?

答：Status code 为 200OK 表示明确返回了，返回的数据如下图。



✧分析你的浏览器向服务器发出的较晚的“HTTP GET”请求，在该请求报文中是否有一行是：IF-MODIFIED-SINCE？如果有，在该首部行后面跟着的信息是什么?

答：有，这字段后面代表的是时间，即咨询服务器在这个时候之后是否更新。

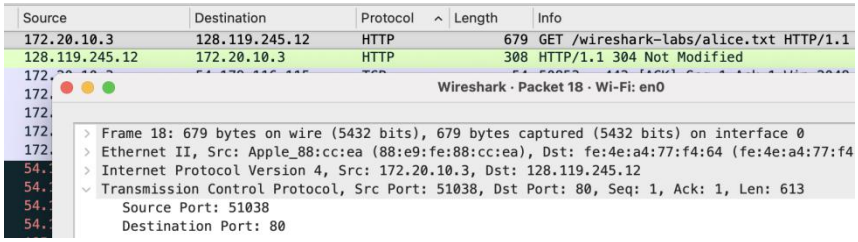
✧服务器对较晚的 HTTP GET 请求的响应中的 HTTP 状态代码是多少？服务器是否明确返回了文件的内容？请解释。

答：请求响应中 HTTP Status code 为 304，根据之前 HTTP GET 中的 IF-MODIFIED-SINCE 字段内的时间服务器判断为 Not Modified，于是客户端可以使用本地这个，没有过期的缓存文件，这不会明确返回文件。

（三）TCP 分析

➢向 gaia.cs.umass.edu 服务器传送文件的客户端主机的 IP 地址和 TCP 端口号是多少?

答：172.20.10.3 : 51038

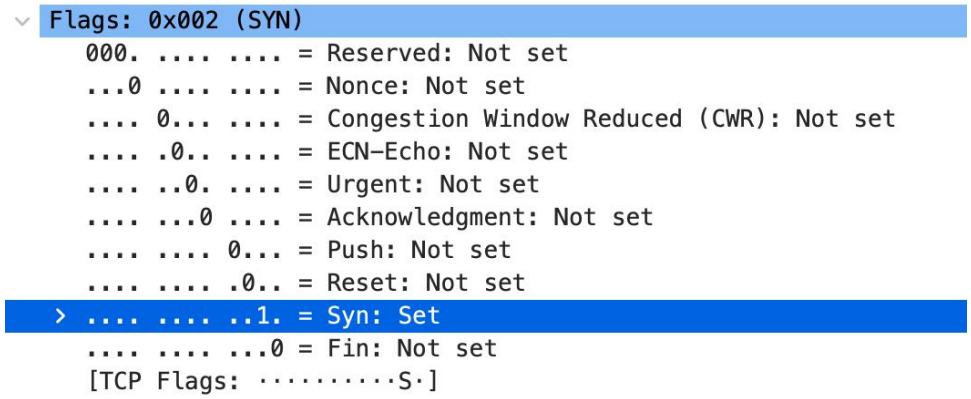


➢Gaia.cs.umass.edu 服务器的 IP 地址是多少？对这一连接，它用来发送和接收 TCP 报文的端口号是多少？

答：服务器的 IP 地址是 128.119.245.12，TCP 报文的端口号是 80。

➢客户服务器之间用于初始化 TCP 连接的 TCP SYN 报文段的序号（sequence number）是多少？在该报文段中，是用什么来标示该报文段是 SYN 报文段的？

答：初始化连接的 TCP SYN 报文段的序号为 0，该报文段将 SYN 标志位置为 1，表示该报文段是 SYN 段用来于 TCP 建立连接。

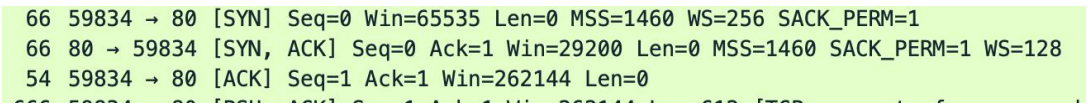


➢服务器向客户端发送的 SYNACK 报文段序号是多少？该报文段中，Acknowledgement 字段的值是多少？Gaia.cs.umass.edu 服务器是如何决定此值的？在该报文段中，是用什么来标示该报文段是 SYNACK 报文段的？

答：SYNACK 报文段序号为 0，acknowledgement 为 1，服务器通过 SYN 请求报文段的 seq 序号加 1 确定 acknowledgement，在该报文段使用 FLAGS ack 和 SYN 标志位置为 1 表示，该报文段为 SYNACK 报文段。

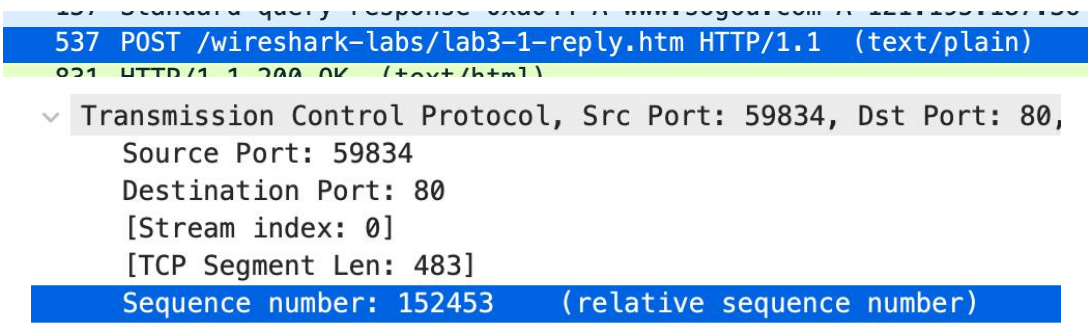
➢你能从捕获的数据包中分析出 tcp 三次握手过程吗？

答：首先客户端向服务器发送 seq=0 建立连接请求 然后向客户端返回 seq=0,ack=1。



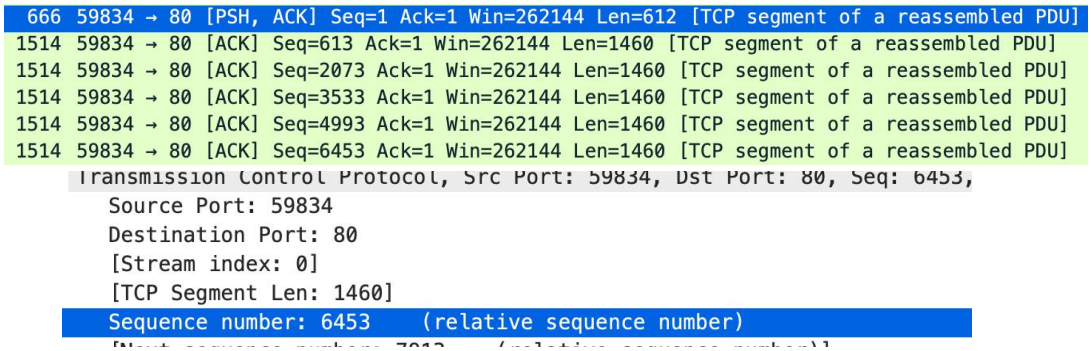
➢包含 HTTP POST 命令的 TCP 报文段的序号是多少？

答：152453



➢如果将包含 HTTP POST 命令的 TCP 报文段看作是 TCP 连接上的第一个报文段，那么该 TCP 连接上的第六个报文段的序号是多少？是何时发送的？该报文段所对应的 ACK 是何时接收的？

答：第六个报文段的序号是 6453，在 HTTP POST 发送之前，TCP 连接建立后发送，对应的 ack 即为服务器返回的第六个 ack。

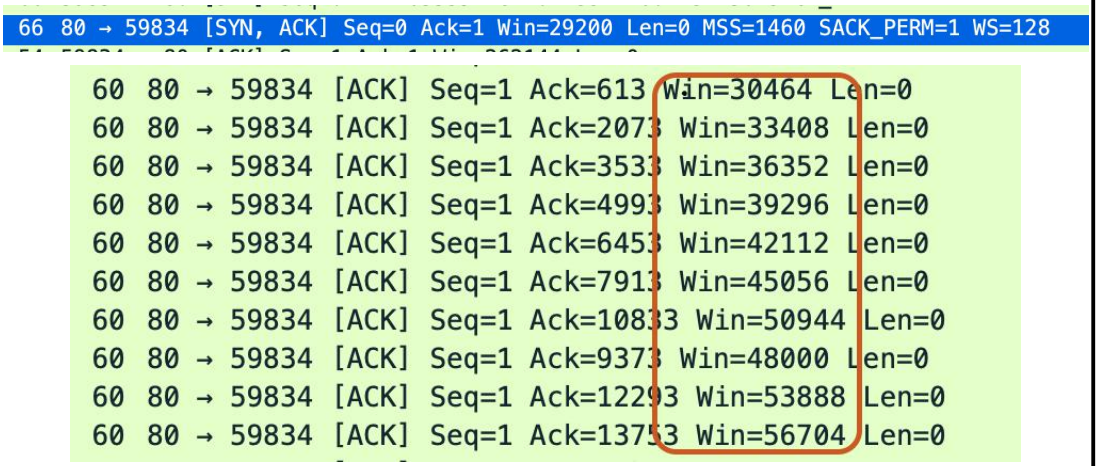


➢前六个 TCP 报文段的长度各是多少？

答：666、1514、1514、1514、1514、1514。

➢在整个跟踪过程中，接收端公示的最小的可用缓存空间是多少？限制发送端的传输以后，接收端的缓存是否仍然不够用？

答：接收端公示的最小的可用缓存空间是 29200，该窗口大小会一直增加， 所以不会出现接收端的缓存是否仍然不够用的情况。



➢在跟踪文件中是否有重传的报文段？进行判断的依据是什么？

答：列号一直在增长，从未出现重复就可以断定无重传报文段。

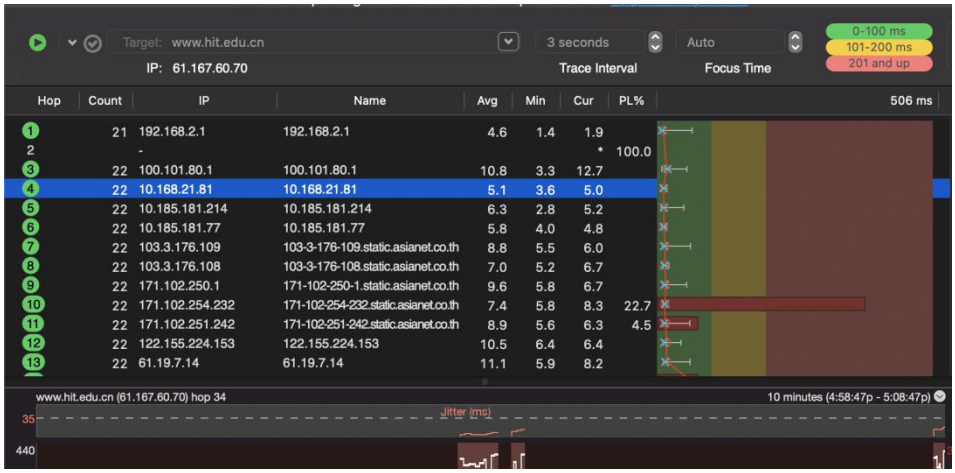
➢TCP 连接的 throughput (bytes transferred per unit time)是多少？请写出你的计算过程。

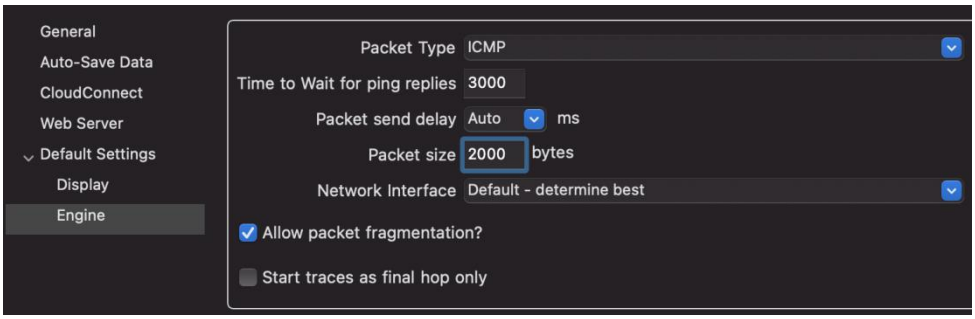
答：总的长度为 152871B+109*54B=158757B

发送时间间隔为 1.673847s

吞吐量为 158757B/1.673847s=94845.59bps

（四）IP 分析





➢你主机的 IP 地址是什么？

答：192.168.2.33

Source	Destination	Protocol
192.168.2.33	61.167.60.70	ICMP
192.168.2.33	61.167.60.70	ICMP

➢在 IP 数据包头中，上层协议（upper layer）字段的值是什么？

答：01

➢IP 头有多少字节？该 IP 数据包的净载为多少字节？并解释你是怎样确定

答：IP 头有 20 字节。因为 IP 数据包的净载为 36 字节，36B+20B=56B。

```
Internet Protocol Version 4, Src: 192.168.2.33, Dst: 61.167.60.70
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
```

➢该 IP 数据包的净载大小的?

答：IP 数据包的净载为 56B-20B=36B。

➢该 IP 数据包分片了吗？解释你是如何确定该 P 数据包是否进行了分片

答：没有其余的帧并且帧的偏移为 0，推断出没有分片。

```
Flags: 0x0000
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..0. .... .... .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255
Protocol: ICMP (1)
```

➢你主机发出的一系列 ICMP 消息中 IP 数据报中哪些字段总发生改变?

答：ID、TTL、Header Checksum 这三个字段总是变化。

➢哪些字段必须保持常量？哪些字段必须改变？为什么?

答:

必须改变： ID 鉴别，用于区分不同的数据包，TTL 来自于 traceroute 要求， 用于测试路径上的路由的信息，Header Checksum 首部校验和前面的字段改变，这些值也必须跟着改变；

必须保持常量： 除了 ID,TTL,Header Checksum 之外字段保持常量。

➢描述你看到的 IP 数据包 Identification 字段值的形式。

答：每报文 16b 的数值，在线性递增，不断+1

➢Identification 字段和 TTL 字段的值是什么?

答：identification 段变化，为了区分不同的 ICMP TTL 消息，但 TTL 保持不变。

➢最近的路由器（第一跳）返回给你主机的 ICMP Time-to-live exceeded 消息中这些值是否保持不变？为什么?

答：没有变化，IP 没有连接到服务，同一个标识是为了分段然后组装成同一个段，ICMP 返回同一个主机，标识不代表序列号，TTL 报文是一样的，所以 标识保持不变； 因为对于第一跳路由器发回的数据报，TTL 是最大值减 1，始终等于 254。

➢该消息是否被分解成不止一个 IP 数据报?

答：改为 2000B 后，分为了 2 片

➢观察第一个 IP 分片，IP 头部的哪些信息表明数据包被进行了分片？IP 头部的哪些信息表明数据包是第一个而不是最后一个分片？该分片的长度是多少 ？

答: More Fragments=1 表示分片了，不是最后一片，该分片的长度是 1500B。

➢原始数据包被分成了多少片?

答：改为 3500B 后，分为了 3 片

➢这些分片中 IP 数据报头部哪些字段发生了变化?

答：第一个和第二个标志位 More Fragments=1 表示后面还有分片，第一个分片的片偏移为 0，第二个为 185，第三个为 370。

（五）抓取 ARP 数据包

```
PS C:\Windows\system32> arp -a

Interface: 192.168.6.1 --- 0x9
  Internet Address      Physical Address      Type
  192.168.6.254         00-50-56-e1-65-79     dynamic
  192.168.6.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.2.33 --- 0xa
  Internet Address      Physical Address      Type
  192.168.2.1           04-4f-17-05-47-bc     dynamic
  192.168.2.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.8.1 --- 0xc
  Internet Address      Physical Address      Type
  192.168.8.254         00-50-56-ff-7e-7d     dynamic
  192.168.8.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0x11
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
PS C:\Windows\system32> S
```

在 window 主机使用命令 arp -a。

（1）利用 MS-DOS 命令：arp 或 c:\windows\system32\arp 查看主机上 ARP 缓存的内容。说明 ARP 缓存中每一列的含义是什么?

答：输入 apr –a 查看主机上 ARP 缓存的内容。

➢ARP 数据包的格式是怎样的？由几部分构成，各个部分所占的字节数是多少?

答：ARP 由于 9 部分构成，硬件类型 2byte，协议类型 2byte，硬件地址长度 1byte，协议地址长度 1byte，OP 2byte，发送端 MAC 地址 6byte，发送端 IP 地址 4byte，目的 MAC 地址 6byte，目的 IP 地址 4byte。

No.	Time	Source	Destination	Protocol	Length	Info
343	5.581270	Humax_05:47:bc	Apple_88:cc:ea	ARP	42	Who has 192.168.2.38? Tell 192.168.2.1
345	5.581320	Humax_05:47:bc	Apple_88:cc:ea	ARP	42	Who has 192.168.2.38? Tell 192.168.2.1
346	5.581329	Apple_88:cc:ea	Humax_05:47:bc	ARP	42	192.168.2.38 is at 88:e9:fe:88:cc:ea
347	5.581380	Apple_88:cc:ea	Humax_05:47:bc	ARP	42	192.168.2.38 is at 88:e9:fe:88:cc:ea

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Apple_88:cc:ea (88:e9:fe:88:cc:ea)
    Sender IP address: 192.168.2.38
    Target MAC address: Humax_05:47:bc (04:4f:17:05:47:bc)
    Target IP address: 192.168.2.1
```

（在 MacOS 主机抓取 ARP 数据包。）

➢如何判断一个 ARP 数据是请求包还是应答包?

答：当 OP 字段为 0x0001 是请求包，当 OP 字段为 0x0002 是应答包。

➢为什么 ARP 查询要在广播帧中传送，而 ARP 响应要在一个有着明确目的局域网地址的帧中传送?

答：进行 ARP 查询时，不知道目的 IP 地址对应的 MAC 地址，所以需要广播查询， 并且 ARP 响应报文知道查询主机的 MAC 地址，局域网内的其他主机不需要这个查询的结果。 ARP 响应必须在它在具有明确目标 LAN 地址的帧中传输。

（六）抓取 UDP 数据包

➢消息是基于 UDP 的还是 TCP 的?

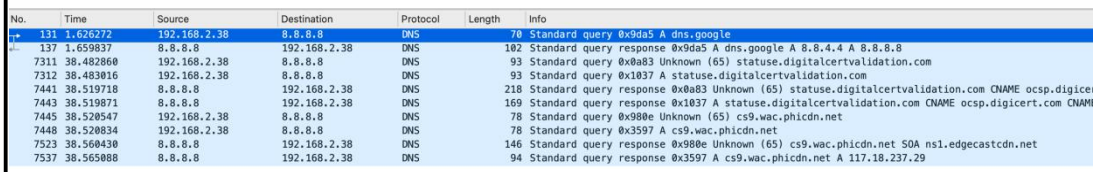
答：UDP

➢数据报的格式是什么样的？都包含哪些字段，分别占多少字节?

答：UDP 数据报格式有两部分，报头和数据。 头部很简单，一共 8byte。包括源端口号 2byte。

（七）利用 WireShark 进行 DNS 协议分析

（1）打开浏览器键入:www.baidu.com，www.google.com。我的 IP 地址：192.168.2.38，本地域名服务器 IP 地址：8.8.8.8.



No.	Time	Source	Destination	Protocol	Length	Info
131	1.626272	192.168.2.38	8.8.8.8	DNS	70	Standard query 0x9da5 A dns.google
137	1.659837	8.8.8.8	192.168.2.38	DNS	102	Standard query response 0x9da5 A dns.google A 8.8.4.4 A 8.8.8.8
7311	38.482860	192.168.2.38	8.8.8.8	DNS	93	Standard query 0x0a83 Unknown (65) statuse.digitalcertvalidation.com
7312	38.483016	192.168.2.38	8.8.8.8	DNS	93	Standard query 0x1037 A statuse.digitalcertvalidation.com
7441	38.519718	8.8.8.8	192.168.2.38	DNS	218	Standard query response 0x0a83 Unknown (65) statuse.digitalcertvalidation.com CNAME ocsp.digice
7443	38.519871	8.8.8.8	192.168.2.38	DNS	169	Standard query response 0x1037 A statuse.digitalcertvalidation.com CNAME ocsp.digicert.com CNAM
7445	38.520547	192.168.2.38	8.8.8.8	DNS	78	Standard query 0x980e Unknown (65) cs9.wac.phicdn.net
7448	38.520834	192.168.2.38	8.8.8.8	DNS	78	Standard query 0x3597 A cs9.wac.phicdn.net
7523	38.560430	8.8.8.8	192.168.2.38	DNS	146	Standard query response 0x980e Unknown (65) cs9.wac.phicdn.net SOA ns1.edgecastcdn.net
7537	38.565088	8.8.8.8	192.168.2.38	DNS	94	Standard query response 0x3597 A cs9.wac.phicdn.net A 117.18.237.29

```
[Header checksum status: Unverified]
Source: 192.168.2.38
Destination: 8.8.8.8
```

```
User Datagram Protocol, Src Port: 19098, Dst Port: 53
    Source Port: 19098
    Destination Port: 53
    Length: 36
    Checksum: 0x8f35 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
```

问题讨论： 对实验过程中的思考问题进行讨论或回答。 对互联网的5层协议有系统的了解。应用层：支持各种网络应用，如FTP、SMTP、HTTP。传输层的进程间的数据传输的TCP、UDP，网络层的数据包从源主机到目的主机的路由和转发，链路层的主机、交换机、路由器等的数据传输。
心得体会： 结合实验过程和结果给出实验的体会和收获。 通过本次实验我掌握了如何使用 Wireshark 工具抓包的方法，理解网络协议实体之间的交互和消息交换。