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	马旭		院系	计算科学与技术学院	
班级	1603106		学号	1160300601	
任课教师	聂兰顺		指导教师	聂兰顺	
实验地点	格物楼 207		实验时间	2018.11.14	
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

目录

1.实验目的

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。

2.实验内容

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

3.实验过程

3.1.Wireshark 的使用

1. 启动主机上的 web 浏览器。

2. 启动 Wireshark。你会看到如图 6-2 所示的窗口，只是窗口中没有任何分组列表。

3. 开始分组俘获：选择“capture”下拉菜单中的“Capture Options”命令，会出现如图 6-3 所示的“Wireshark: Capture Options”窗口，可以设置分组俘获的选项。

4. 在实验中，可以使用窗口中显示的默认值。在“Wireshark: CaptureOptions”的最上面有一个“Interface List”下拉菜单，其中显示计算机所具有的网络接口（即网卡）。当计算机具有多个活动网卡时，需要选择其中一个用来发送或接收分组的网络接口（如某个有线接口）。随后，单击“Start”开始进行分组俘获，所有由选定网卡发送和接收的分组都将被俘获。

5. 开始分组俘获后，会出现一个窗口。该窗口统计显示各类已俘获数据包。在该窗口的工具栏中有一个“stop”按钮，可以停止分组的俘获。但此时你最好不要停止俘获分组。

6. 在运行分组俘获的同时，在浏览器地址栏中输入某网页的 URL，如：http://www.hit.edu.cn。为显示该网页，浏览器需要连接 www.hit.edu.cn 的服务器，并与之交换 HTTP 消息，以下载该网页。包含这些 HTTP 报文的以太网帧将被

Wireshark 俘获。

7. 当完整的页面下载完成后，单击 Wireshark 菜单栏中的 stop 按钮，停止分组俘获。Wireshark 主窗口显示已俘获的你的计算机与其他网络实体交换的所有协议报文，其中一部分就是与 www.hit.edu.cn 服务器交换的 HTTP 报文。此时主窗口与图 6-3 相似。

8. 在显示筛选规则中输入“http”，单击“回车”，分组列表窗口将只显示 HTTP 协议报文。

9. 选择分组列表窗口中的第一条 http 报文。它应该是你的计算机发向 www.hit.edu.cn 服务器的 HTTP GET 报文。当你选择该报文后，以太网帧、IP 数据报、TCP 报文段、以及 HTTP 报文首部信息都将显示在分组首部子窗口中。单击分组首部详细信息子窗口中向右和向下箭头，可以最小化帧、以太网、IP、TCP 信息显示量，可以最大化 HTTP 协议相关信息的显示量。

3.2.HTTP 分析

1). HTTP GET/response 交互

1. 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。
2. 开始 Wireshark 分组俘获。
3. 在打开的 Web browser 窗口中输入一下地址：http://hitgs.hit.edu.cn/news
4. 停止分组俘获。

2). HTTP 条件 GET/response 交互

1. 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”）。
2. 启动 Wireshark 分组俘获器。开始 Wireshark 分组俘获。
3. 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。
4. 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。

3.3．TCP 分析

1. 俘获大量的由本地主机到远程服务器的 TCP 分组

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。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 INWONDERLAND 的全名（含路径），此时不要按“Uploadalice.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。
（6） 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。

3.4.IP 分析

通过分析执行 traceroute 程序发送和接收到的 IP 数据包，我们将研究 IP 数据包的各个字段，并详细研究 IP 分片。

A. 通过执行 traceroute 执行捕获数据包

为了产生一系列 IP 数据报，我们利用 traceroute 程序发送具有不同大小的数据包给目的主机 X。回顾之前 ICMP 实验中使用的 traceroute 程序，源主机发送的第一个数据包的 TTL 设位 1，第二个为 2，第三个为 3，等等。每当路由器收到一个包，都会将其 TTL 值减 1。这样，当第 n 个数据包到达了第 n 个路由器时，第 n 个路由器发现该数据包的 TTL 已经过期了。根据 IP 协议的规则，路由器将该数据包丢弃并将一个 ICMP 警告消息送回源主机。

在 Windows 自带的 tracert 命令不允许用户改变由 tracert 命令发送的 ICMP echo 请求消息（ping 消息）的大小。一个更优秀的 traceroute 程序是 pingplotter，下载并安装 pingplotter。ICMP echo 请求消息的大小可以通过下面方法在 pingplotter 中进行设置。Edit->Options->Packet，然后填写 Packet Size(in bytes，default=56)域。实验步骤：

（1） 启动 Wireshark 并开始数据包捕获

（2） 启动 pingplotter 并“Address to Trace Window”域中输入目的地址。

在“# of times to Trace”域中输入“3”，这样就不过采集过多的数据。Edit->Options->Packet，将 Packet Size(in bytes,default=56)域设为 56，这样将发送一系列大小为 56 字节的包。然后按下“Trace”按钮。得到的 pingplotter 窗口。

（1） Edit->Options->Packet，然后将 Packet Size(in bytes,default=56)域改为 2000，这样将发送一系列大小为 2000 字节的包。然后按下“Resume”按钮。

（2） 最后，将 Packet Size(in bytes,default=56)域改为 3500，发送一系列大小为 3500 字节的包。然后按下“Resume”按钮。

（3） 停止 Wireshark 的分组捕获。

B. 对捕获的数据包进行分析

（1）在你的捕获窗口中，应该能看到由你的主机发出的一系列 ICMPEcho Request 包和中间路由器返回的一系列 ICMP TTL-exceeded 消息。选择第一个你的主机发出的 ICMP Echo Request 消息，在 packet details 窗口展开数据包的 Internet Protocol 部分。

（2）单击 Source 列按钮，这样将对捕获的数据包按源 IP 地址排序。选择第一个你的主机发出的 ICMP Echo Request 消息，在 packet details 窗口展开数据包的 Internet Protocol 部分。在“listing of captured packets”窗口，你会看到许多后

续的 ICMP 消息（或许还有你主机上运行的其他协议的数据包）

（3）找到由最近的路由器（第一跳）返回给你主机的 ICMP Time-to-live exceeded 消息。

（4）单击 Time 列按钮，这样将对捕获的数据包按时间排序。找到在将包大小改为 2000 字节后你的主机发送的第一个 ICMP Echo Request 消息。

C. 找到在将包大小改为 3500 字节后你的主机发送的第一个 ICMP Echo Request 消息。

3.5.抓取 ARP 数据包

1）利用 MS-DOS 命令：arp 或 c:\windows\system32\arp 查看主机上 ARP 缓存的内容。

（2）在命令行模式下输入：ping 192.168.1.82（或其他 IP 地址）

（3）启动 Wireshark，开始分组俘获。

3.6.抓取 UDP 数据包

（1）启动 Wireshark，开始分组捕获；

（2）发送 QQ 消息给你的好友；

（3）停止 Wireshark 组捕获；

（4）在显示筛选规则中输入“udp”并展开数据包的细节。

3.7.利用 WireShark 进行 DNS 协议分析

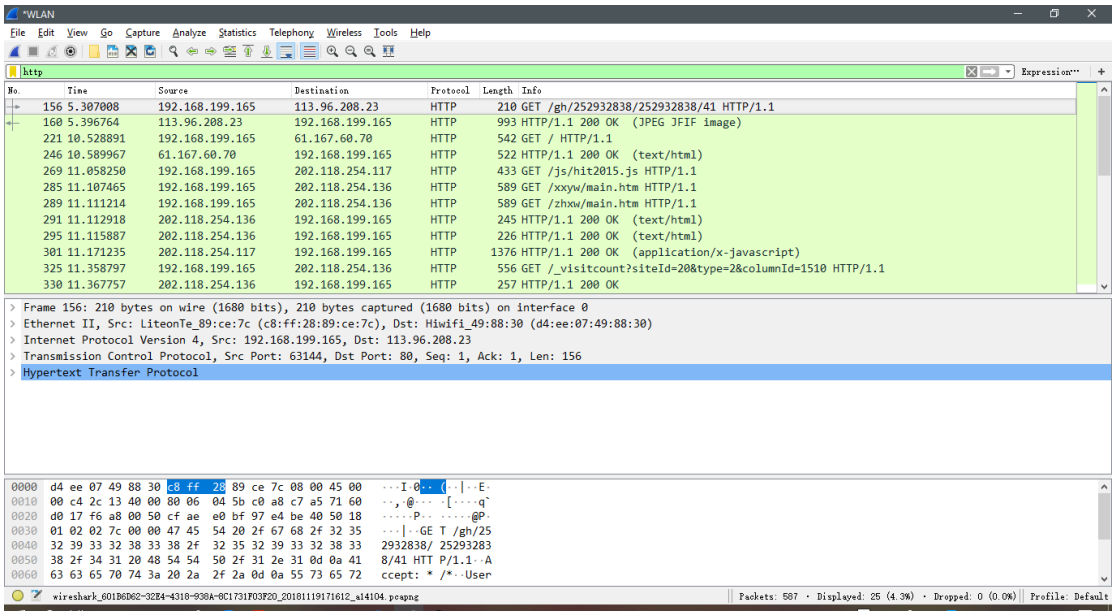
（1）打开浏览器键入:www.baidu.com

（2）打开 Wireshark,启动抓包.

（3）在控制台回车执行完毕后停止抓包.

4.实验结果

4.1 Wireshark 的使用



4.2. HTTP 分析

(1).HTTP GET/response 响应

1). 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？

答：我的浏览器是 HTTP1.1，我所访问的服务器所运行的 HTTP 协议版本号 HTTP/1.1

2). 你的浏览器向服务器指出它能接收何种语言版本的对象？

答：

```
Content-Type: text/html\r\n
```

3). 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？

答：我的 IP:192.168.199.165，服务器的：219.217.227.25

4). 从服务器向你的浏览器返回的状态代码是多少？

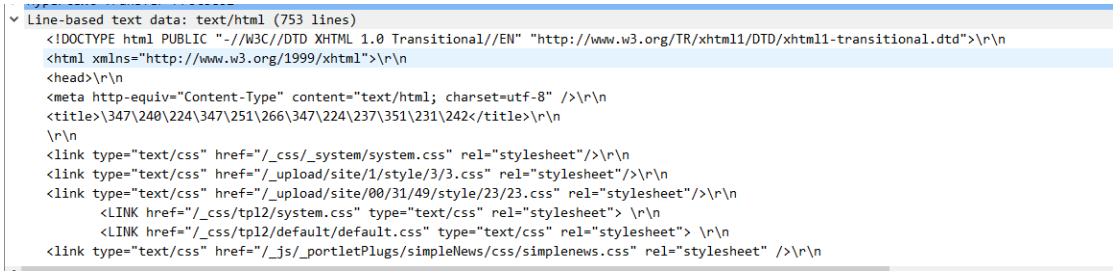
答：状态码：200

2). HTTP 条件 GET/response 交互

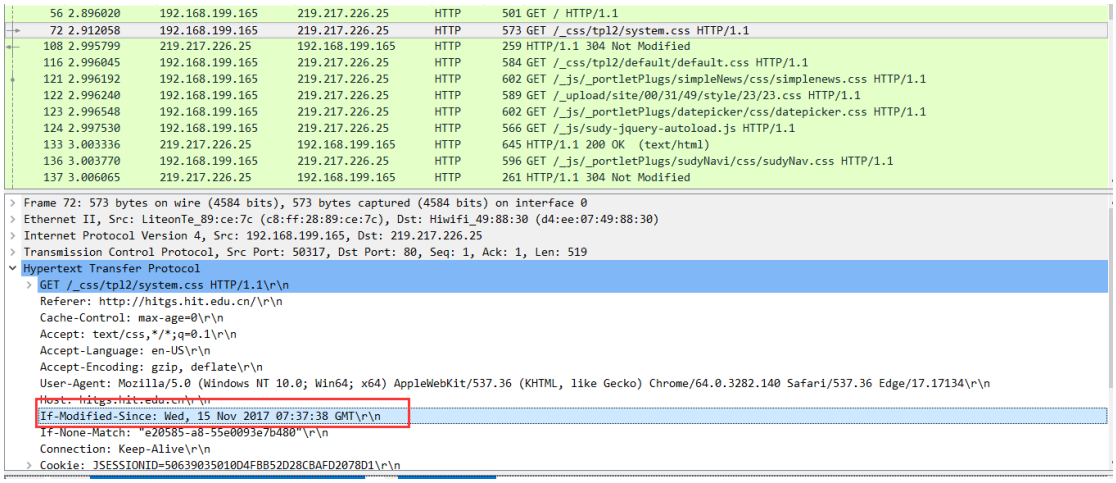
1) 分析你的浏览器向服务器发出的第一个 HTTP GET 请求的内容，在该请求

报文中，是否有一行是：IF-MODIFIED-SINCE？
答：没有

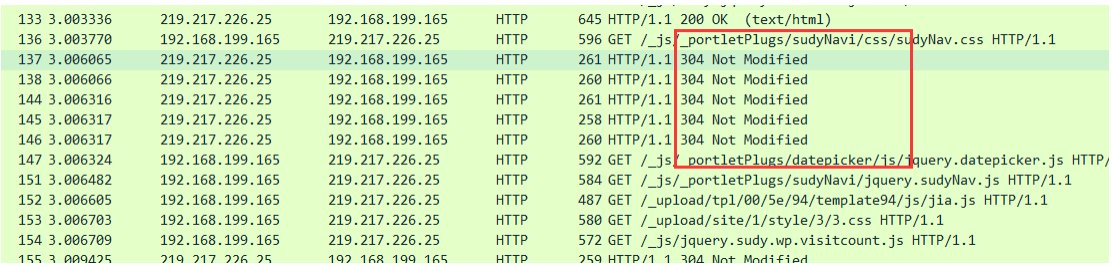
2) 分析服务器响应报文的内容，服务器是否明确返回了文件的内容？如何获知？
答：服务器明确了文件返回的内容，可以通过 wireshark 查看，如下图：



3) 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，代表浏览器有缓存，后面代表时间，即服务器在这个事件之后是否有更新。图示如下：



4) 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：使用的状态码是 304，不会返回明确文件，使用没有过期的缓存文件。



4.3．TCP 分析

1. 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：IP：192.168.199.165　Port：63848，如下图：

16	1.312138	192.168.199.165	128.119.245.12	TCP	66 63848 → 80 [
19	1.718753	128.119.245.12	192.168.199.165	TCP	66 80 → 63848 [

3. 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：IP：128.119.245.12　Port：80，如下图：

16	1.312138	192.168.199.165	128.119.245.12	TCP	66 63848 → 80 [
19	1.718753	128.119.245.12	192.168.199.165	TCP	66 80 → 63848 [

4. 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：用于初始化 TCP 连接的 TCP SYN 报文段的序号：0，在该报文段中，是用 SYN 位设置为 1 来标示该报文是 SYN 报文段的。如下图：

16	1.312138	192.168.199.165	128.119.245.12	TCP	66 63848 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
19	1.718753	128.119.245.12	192.168.199.165	TCP	66 80 → 63848 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
21	1.718868	192.168.199.165	128.119.245.12	TCP	54 63848 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
22	1.719322	192.168.199.165	128.119.245.12	TCP	735 63848 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=681 [TCP segment of a reassembled PD…

```
Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..1. = Syn: Set
    [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80]
        [Connection establish request (SYN): server port 80]
        [Severity level: Chat]
        [Group: Sequence]
    .... .... ...0 = Fin: Not set
    [TCP Flags: ··········S·]
```

5. 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：报文序号是：0，Acknowledgement 是：1，服务器通过将客户端的 seq+1 得到该值，该报文端中是使用将 syn 标记为 1 来表示是 SYNACK 报文段的。

如下图所示：

16	1.312138	192.168.199.165	128.119.245.12	TCP	66 63848 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
19	1.718753	128.119.245.12	192.168.199.165	TCP	66 80 → 63848 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
21	1.718868	192.168.199.165	128.119.245.12	TCP	54 63848 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
22	1.719322	192.168.199.165	128.119.245.12	TCP	735 63848 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=681 [TCP segment of a reassembled PD…

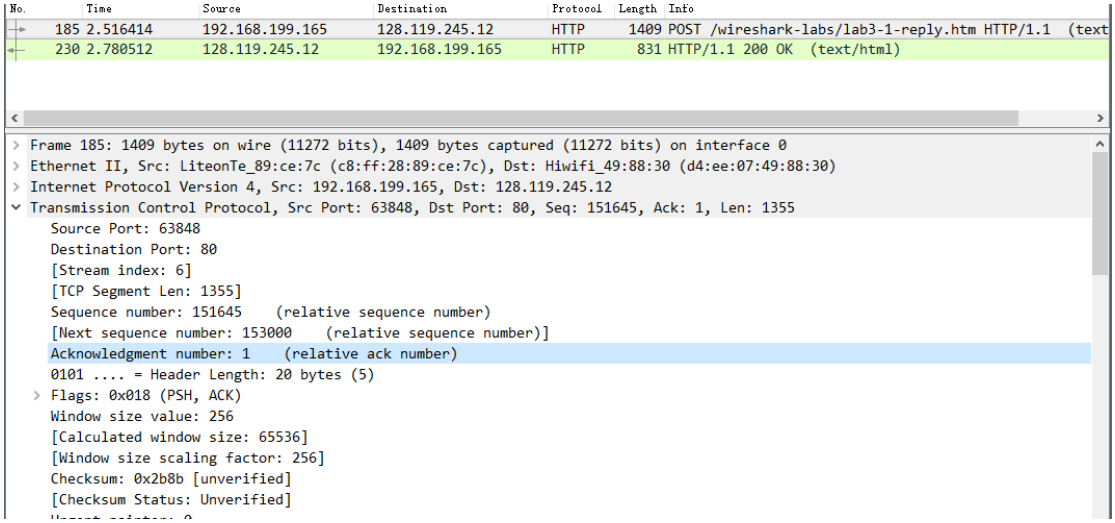
```
Flags: 0x012 (SYN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
    v [Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 80]
        [Connection establish acknowledge (SYN+ACK): server port 80]
        [Severity level: Chat]
        [Group: Sequence]
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·····A··S·]
```

6. 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端发送一个 syn 报文，其中 seq=0，然后服务端收到后发送一个 ack=1,seq=0 的 syn 报文，然后客户端回复一个 seq=1,ack=1 的 syn=0 的报文。

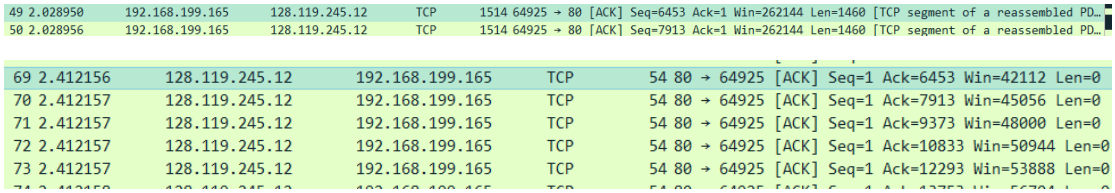
7. 包含 HTTP POST 命令的 TCP 报文段的序号是多少？

答：包含 HTTP POST 命令的 TCP 报文段序号是：1，如下图：



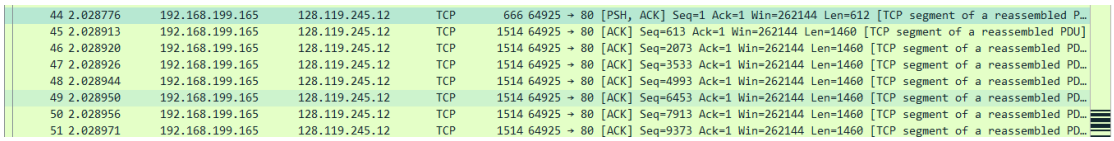
8. 如果将包含 HTTP POST 命令的 TCP 报文段看作是 TCP 连接上的第一个报文段，那么该 TCP 连接上的第六个报文段的序号是多少？是何时发送的？该报文段所对应的 ACK 是何时接收的？

答：第六个报文段 seq 是 6453，在 http post 发送之前，tcp 连接建立之后发送



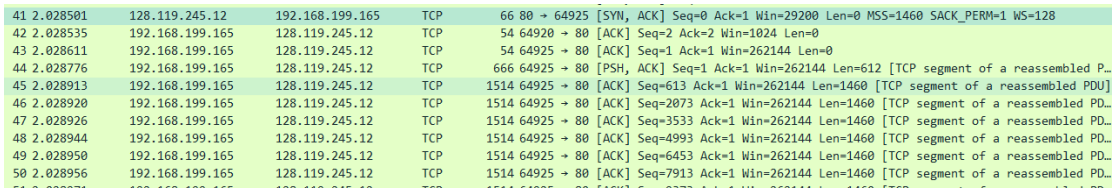
上图中对应的 ack 即为第六个 ack。

9. 前六个 TCP 报文段的长度各是多少？



10. 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：接收端公示的最小可用缓存空间是 29200，限制发送端的传输后，接收端的缓存够用，因为该缓存空间一直在增大。如下图所示：

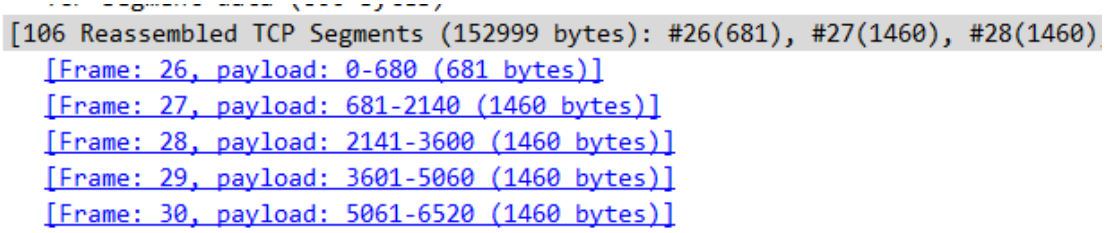


11. 在跟踪文件中是否有重传的报文段？进行判断的依据是什么？

答：没有发生重传了。因为在 wireshark 中没有出现重传的记录。

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

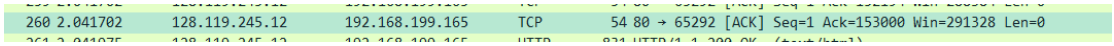
答：



由上图可知，数据总长度为 152999B

时间计算：

结束时间：



开始时间：

可得时间为：2.041702s-0.399032s = 1.64267s

传输速率：152999B/1.64267s = 93.140 byte/s

4.4. IP 分析

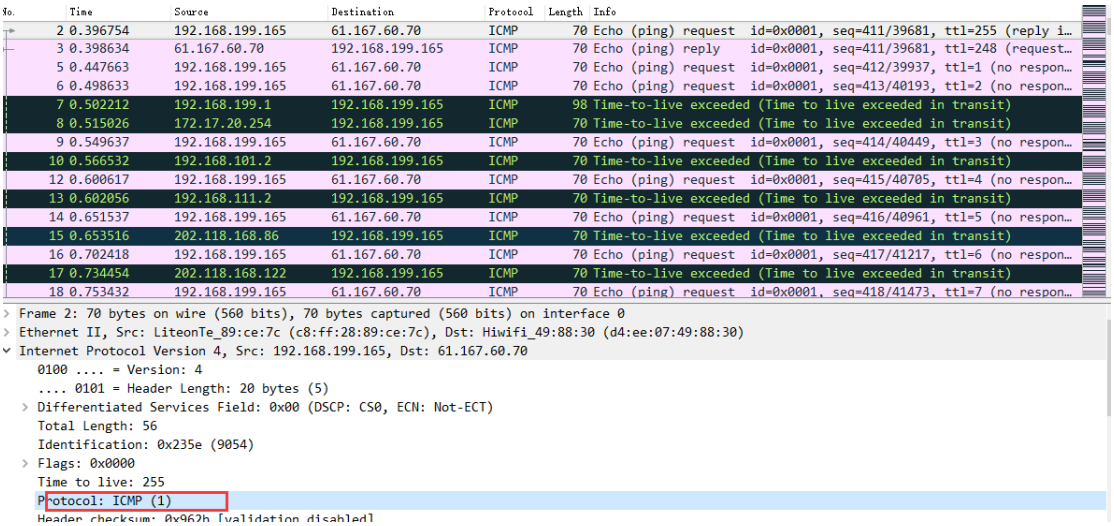
1.

(1). 你主机的 IP 地址是什么：

答：192.168.199.165

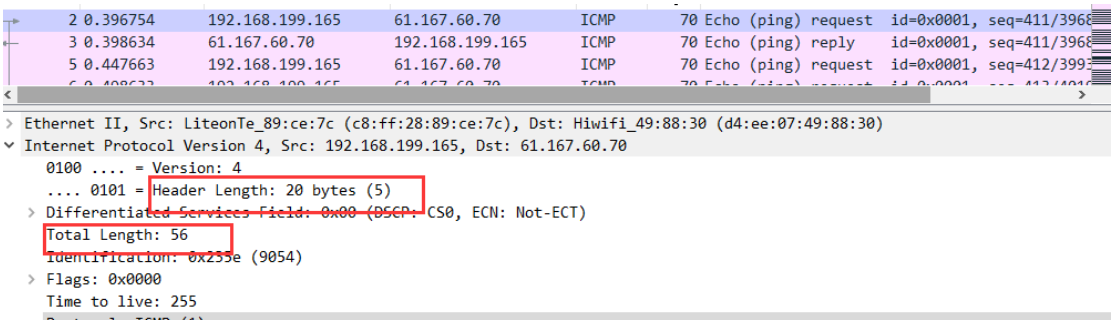
(2). 在 IP 数据包头中，上层协议（upper layer）字段的值是什么？

答：是 1



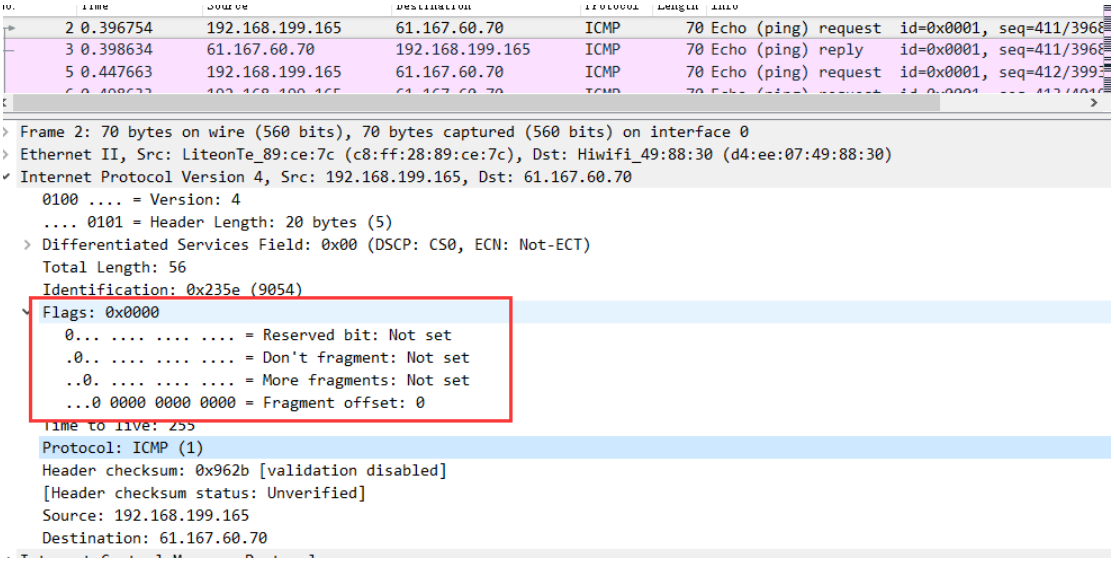
(3). IP 头有多少字节？该 IP 数据包的净载为多少字节？并解释你是怎样确定？该 IP 数据包的净载大小的？

答：Ip 头有 20 字节，该 ip 数据包的净载为 56-20=36 字节，因为该 ip 数据包的总长为 56 字节，总长减去头部即为净载。验证结果示意图如下：



(4). 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？

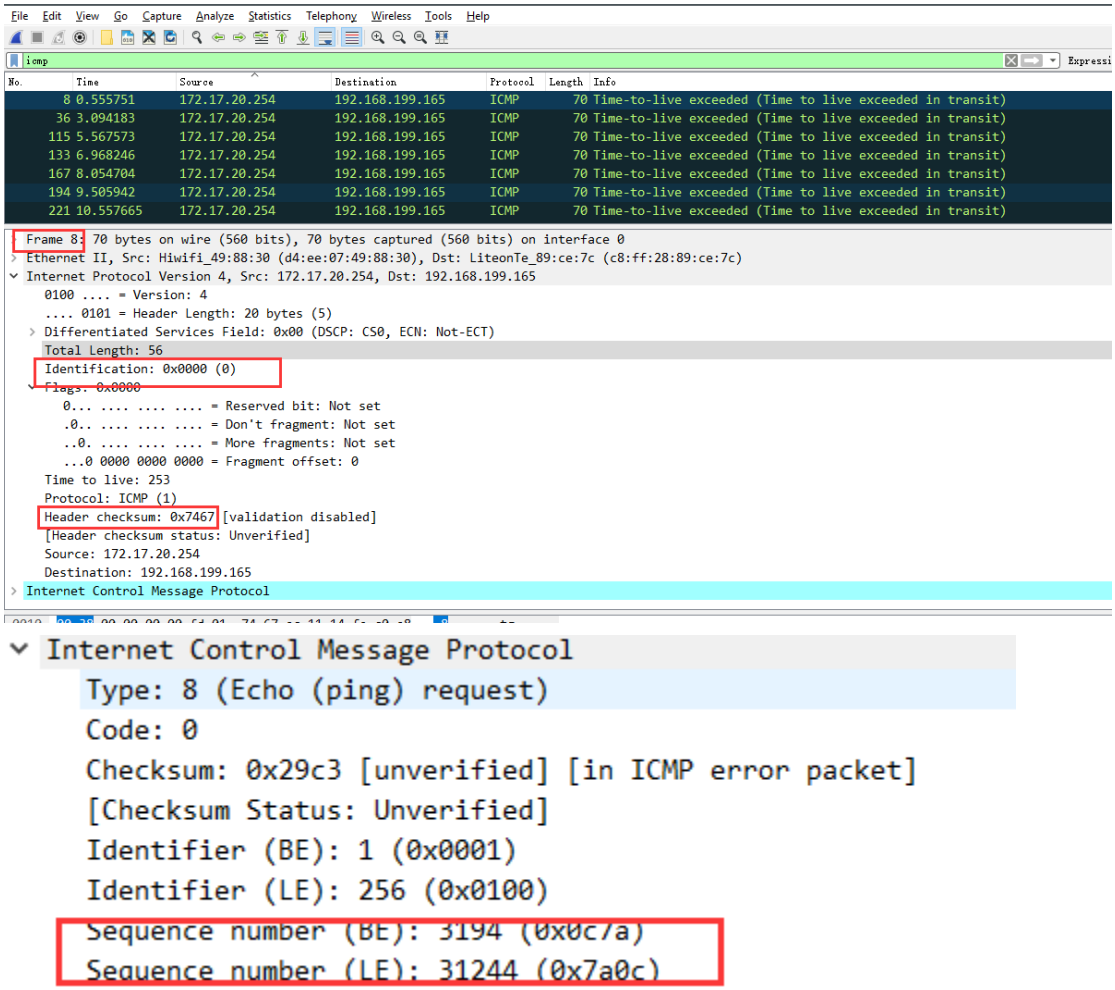
答：没有进行分片，因为 flags 设置为 0x0000。



2.

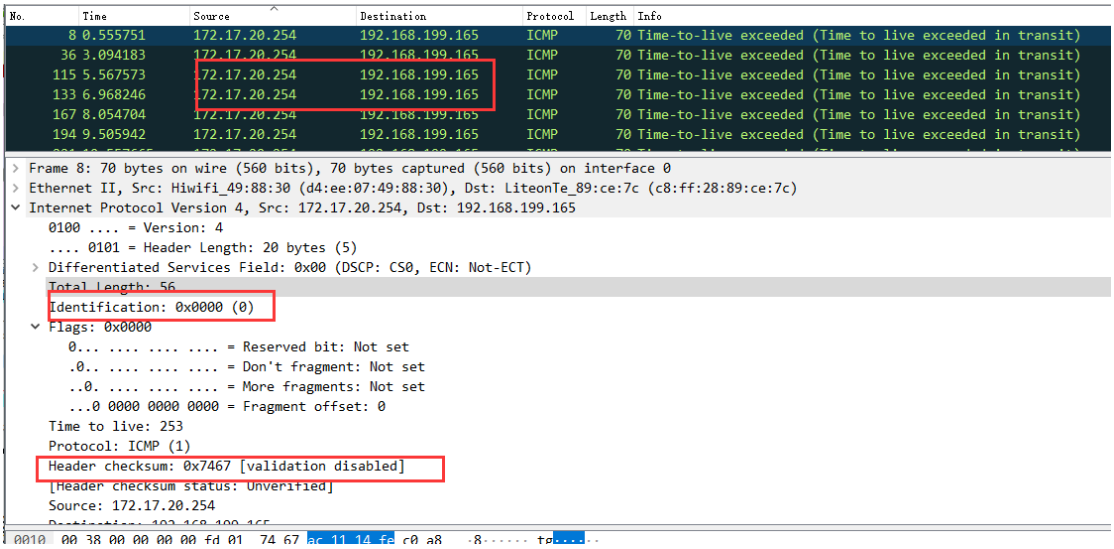
(1). 你主机发出的一系列 ICMP 消息中 IP 数据报中哪些字段总是发生改变？

答：他们的 seq、ttl、Frame、Identification、校验和总是在发生改变。验证结果示意图如下：



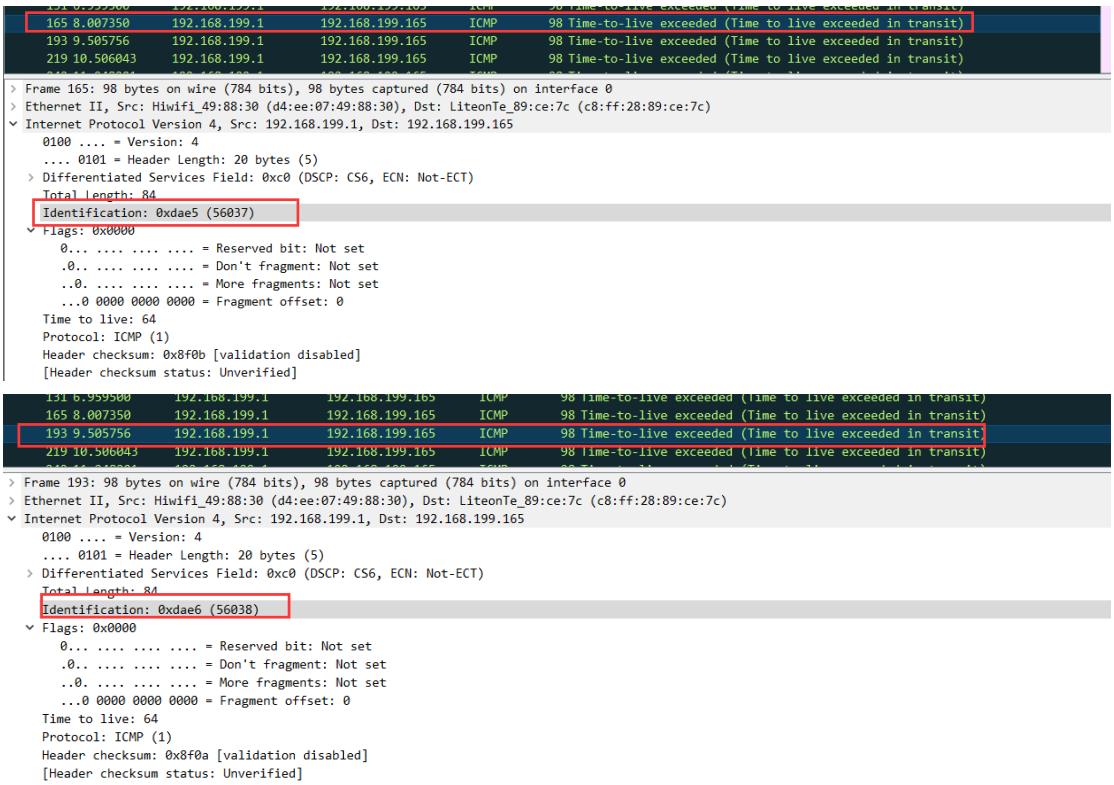
(2). 哪些字段必须保持常量？哪些字段必须改变？为什么？

答：以下字段必须保持常量：Version, Source IP, Destination IP。 以下字段必须改变：identification, Header checksum。 源 ip 地址和目的 ip 地址是不能变的，要不就不是该 ip 数据包了。标识字段唯一地标识主机发送的每一份数据报，而校验和是根据前面的数据进行计算，当然会改变。验证结果示意图如下：



(3).描述你看到的 IP 数据包 Identification 字段值的形式。

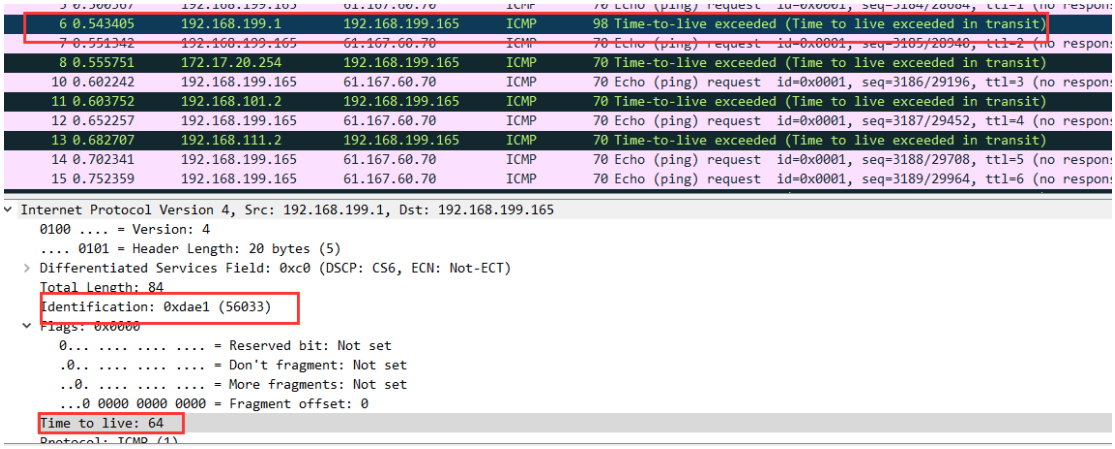
答：每一个 ip 数据包的标志位均不一样，且相邻的 ip 数据包标志位差 1。验证结果示意图如下：



3.

(1). Identification 字段和 TTL 字段的值是什么？

答：是 0xdae1 和 64，如下图所示：



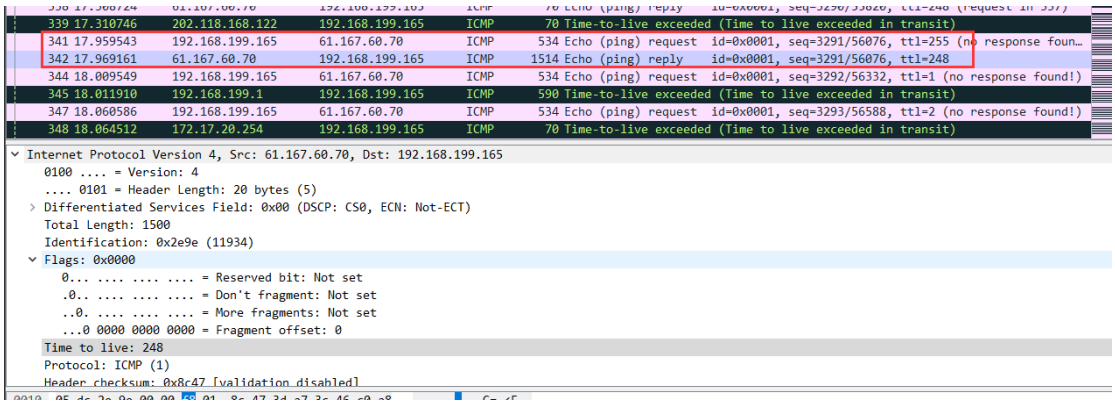
(2). 最近的路由器（第一跳）返回给你主机的 ICMP Time-to-live exceeded 消息中这些值是否保持不变？为什么？

答：保持不变，均为 64，因为线路固定路由器固定，自然捕获的相关 ip 数据包 ttl 也固定。

4.

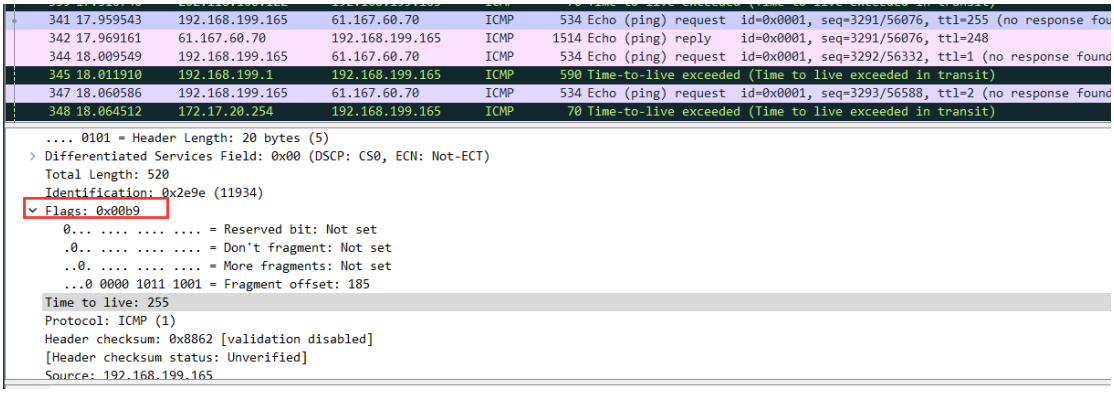
(1). 该消息是否被分解成不止一个 IP 数据报？

答：消息被分解不止一个 IP 数据报



(2). 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

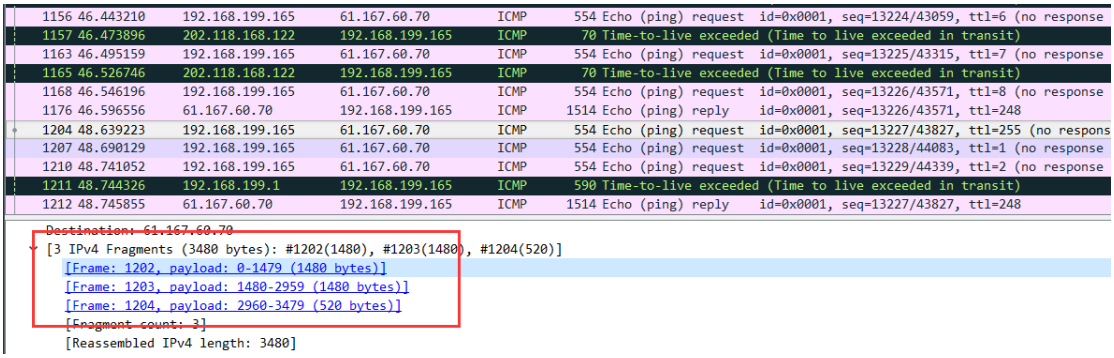
答：flags 被设置为 0x00b6，offset 不为 0，所以不是最后一个分片，该片大小为 534,如下图所示：



5.

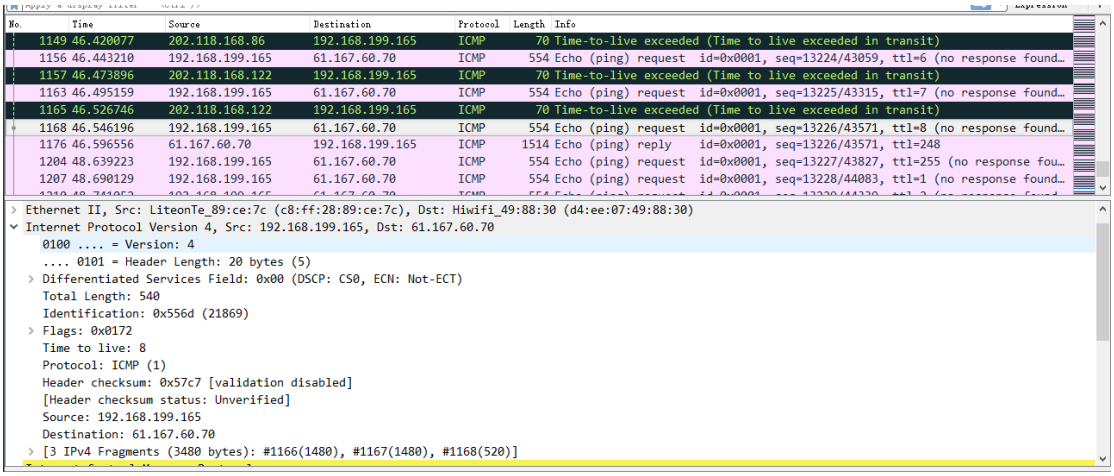
(1). 原始数据包被分成了多少片？

答：原始数据包被分成了 3 片。如下图所示：



(2). 这些分片中 IP 数据报头部哪些字段发生了变化？

答：数据包头部中有如下字段发生了变化：Total Length ，Flags，Fragment offset，Head checksum。结果如下图所示：



4.5.ARP 协议分析

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：使用 arp –a 查看主机上 ARP 缓存的内容，结果如下图所示：

```
C:\Users\MaXU>arp -a

Interface: 192.168.199.165 --- 0xb
  Internet Address      Physical Address      Type
  192.168.199.1         d4-ee-07-49-88-30     dynamic
  192.168.199.113       10-4a-7d-d8-91-a9     dynamic
  192.168.199.179       60-83-34-b7-8b-57     dynamic
  192.168.199.255       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
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.175.1 --- 0xd
  Internet Address      Physical Address      Type
  192.168.175.254       00-50-56-ec-b4-9d     dynamic
  192.168.175.255       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
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.98.1 --- 0xf
  Internet Address      Physical Address      Type
  192.168.98.254        00-50-56-ef-e6-10     dynamic
  192.168.98.255        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
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\MaXU>
```

ARP 缓存中的每一列分别表示 IP 地址所对应的物理地址和类型（动态配置或静态配置）

2. 清除主机上 ARP 缓存的内容,抓取 ping 命令时的数据包。分析数据包,回答下面的问题：
(1).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 数据 bao1 格式如下图所示：

由 9 部分组成，分别是：硬件类型：2bytes，协议类型：2bytes，硬件地址长度：1byte，协议地址长度：1byte，OP：2byte，发送端 MAC 地址：6bytes，发送端 IP 地址：4bytes，目标 MAC 地址：6bytes，目标 IP 地址：4bytes。
截取的一个 ARP 数据报如下：

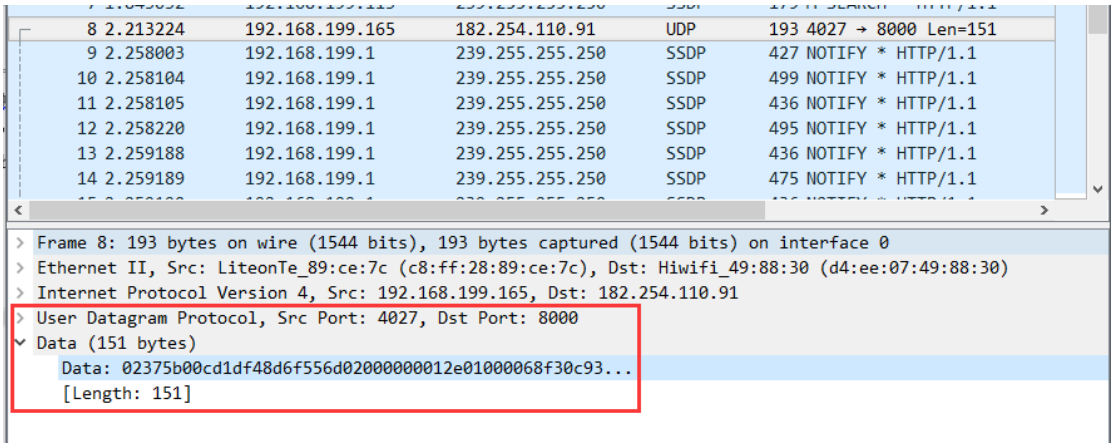
```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LiteonTe_89:ce:7c (c8:ff:28:89:ce:7c)
    Sender IP address: 192.168.199.165
    Target MAC address: Hiwifi_49:88:30 (d4:ee:07:49:88:30)
    Target IP address: 192.168.199.1
```

(2). 如何判断一个 ARP 数据是请求包还是应答包？
答：通过 OP 字段。当 OP 字段值为 0x0001 时是请求包，当 OP 字段值为 0x0002 时是应答包。

(3). 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：因为进行 ARP 查询时并不知道目的 IP 地址对应的 MAC 地址，所以需要广播查询；而 ARP 响应报文知道查询主机的 MAC 地址（通过查询主机发出的查询报文获得），且局域网中的其他主机不需要此次查询的结果，因此 ARP 响应要在一个有着明确目的局域网地址的帧中传送。

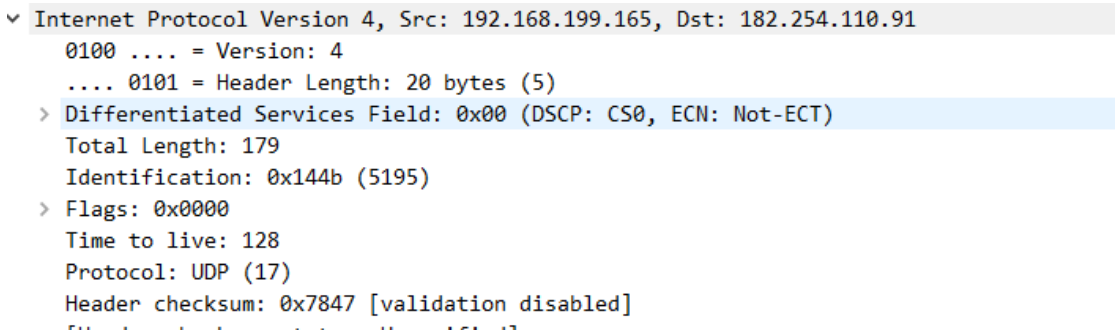
4.6.抓取 UDP 数据包

1. 消息是基于 UDP 的还是 TCP 的？
答：消息基于 UDP 的，如图：



2. 你的主机 ip 地址是什么？目的主机 ip 地址是什么？

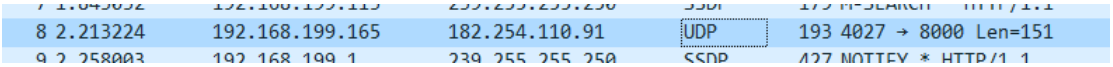
答：我的 IP 地址：192.168.199.165　　目的主机 IP 地址：182.254.110.91



3. 你的主机发送 QQ 消息的端口号和 QQ 服务器的端口号分别是多少？

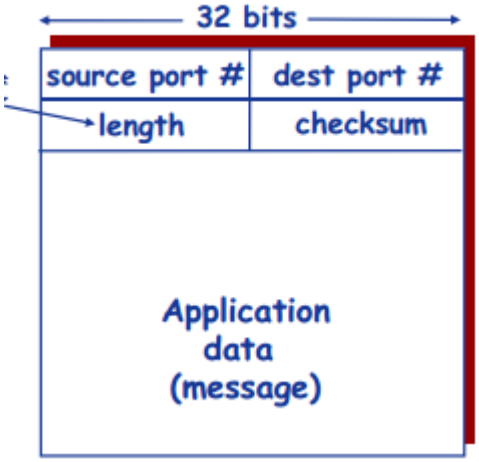
答：发送的端口：4027

接收的端口：8000



4. 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 数据报格式如下图：



由 5 部分构成，分别是源端口号：4 字节，目的端口号：4 字节，长度：4 字节，校验和：4 字节，应用层数据。
抓取的一个 UDP 数据报如下：

```
    Destination: 182.254.116.91
▾ User Datagram Protocol, Src Port: 4027, Dst Port: 8000
    Source Port: 4027
    Destination Port: 8000
    Length: 159
    Checksum: 0xcfac [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
```

为什么你发送一个 ICQ 数据包后，服务器又返回给你的主机一个 ICQ 数据包？这 UDP 的不可靠数据传输有什么联系？对比前面的 TCP 协议分析，你能看出 UDP 是无连接的吗？
答：(1).因为服务器需返回接收的结果给客户端。(2).因为服务器只提供了一次返回的 ACK，所以不保证数据一定送达。(2).UDP 数据包没有序列号，因此不能像 TCP 协议那样先握手再发送数据，因为每次只发送一个数据报，然后等待服务器响应。

4.7.使用 WireShark 进行 DNS 协议分析

抓包如下：

```
542 13.451629   192.168.199.165   192.168.199.1     DNS   73 Standard query 0x9305 A sp0.baidu.com
563 13.500189   192.168.199.1     192.168.199.165   DNS   132 Standard query response 0x9305 A sp0.baidu.com CNAME www.a.shifen.com A 180.97.…
```

```
▾ Domain Name System (response)
    Transaction ID: 0x9305
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ sp0.baidu.com: type A, class IN
        Name: sp0.baidu.com
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Answers
    ▾ sp0.baidu.com: type CNAME, class IN, cname www.a.shifen.com
        Name: sp0.baidu.com
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 36
        Data length: 15
        CNAME: www.a.shifen.com
    ▾ www.a.shifen.com: type A, class IN, addr 180.97.33.107
        Name: www.a.shifen.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 36
        Data length: 4
        Address: 180.97.33.107
```

将 180.97.33.107 输入到浏览器中得到网页如下：

5.问题讨论

1. 在查看抓取 HTTP 时，对于 if-condition，有些文件会发送，有些文件不会发送，所以要多查看几个 GET 请求头，或者直接找 not modified 字前面的 GET。
2. 老师在课上说 QQ 是混合结构，用户间消息的发送是通过 p2p 架构实现的，但是在实际抓包中发现消息是发送到一个服务器上的。
3. 其中有两个地方在抓取时一直得不到正确的情况，第一个是在抓取条件 GET 方法时，按理应该得到 if-condition 字段，但是一直没有，后来通过清空浏览器缓存重新抓取得到；第二个是在抓取 ICMP 协议时，一直找不到分成三段(大小设置为 3500bytes 时)的数据，最后在多次尝试下才找到。

6.心得体会

1. 通过实验，学会了使用 wireshark 抓取 HTTP 协议，TCP 协议，IP 协议，ARP 协议，UDP 协议，DNS 协议。
2. 通过实验，加深了对于各种协议的认识。
3. 在抓取协议时一定要仔细，认真，否则就有可能找不到要找的请求或者响应。