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	姚舜宇		院系	计算学部		
班级	1903602		学号	1190202107		
任课教师	李全龙		指导教师	李全龙		
实验地点	格物 207		实验时间	2021.11.20		
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：

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。

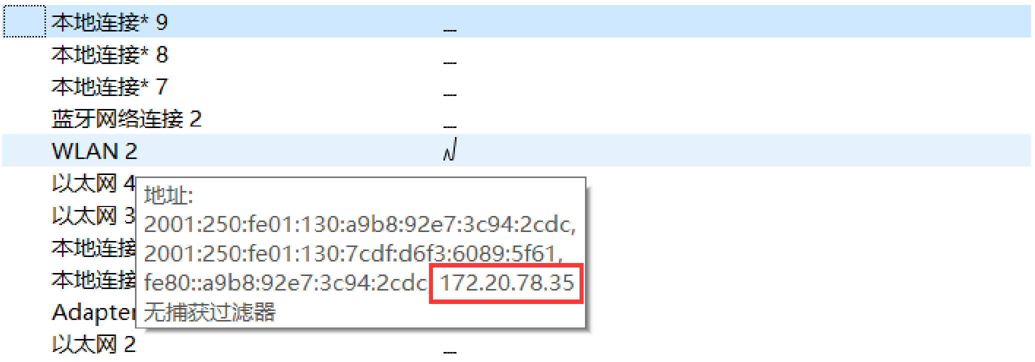
1. 学习wireshark的使用
2. 利用wireshark分析HTTP协议
3. 利用wireshark分析TCP协议
4. 利用wireshark分析IP协议

5. 利用wireshark分析Ethernet数据帧
6. 利用wireshark分析DNS协议
7. 利用wireshark分析UDP协议
8. 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。

首先需要知道本机的IPv4地址。地址：172.20.78.35

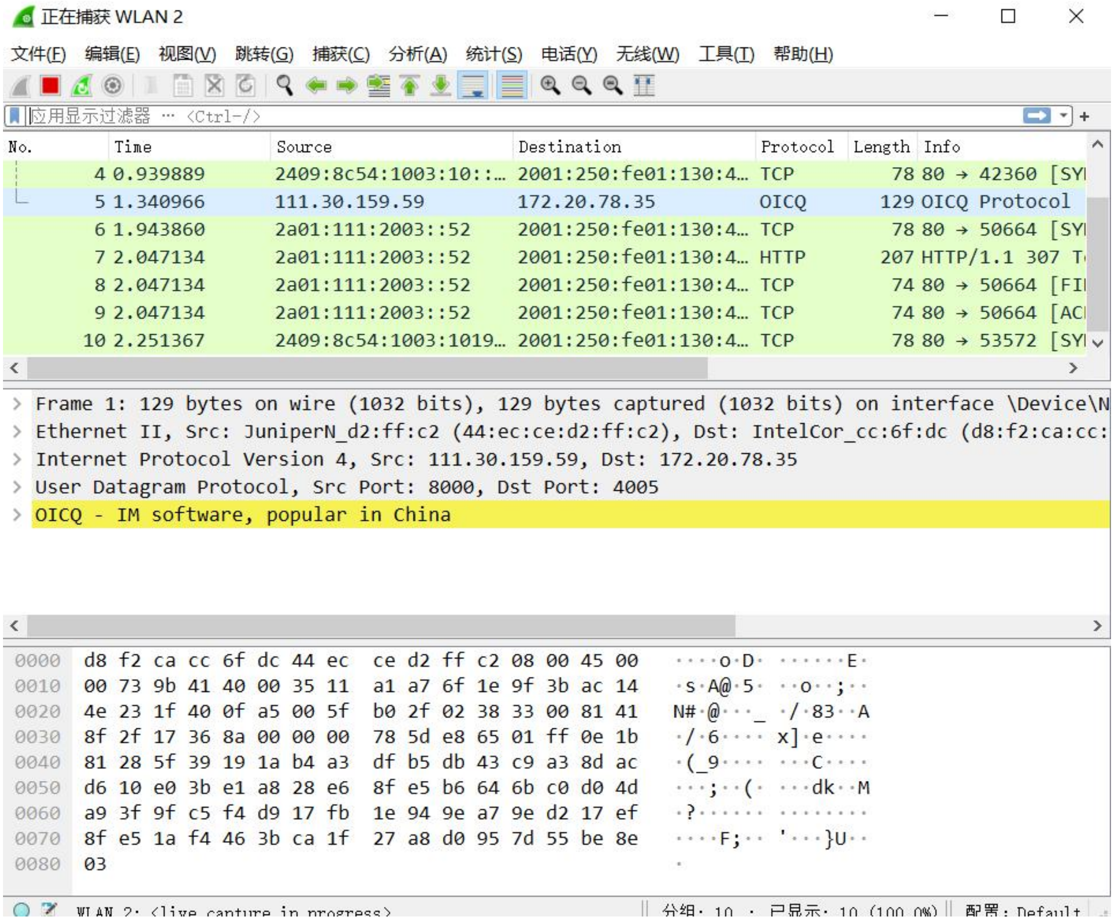


```
本地连接* 9
本地连接* 8
本地连接* 7
蓝牙网络连接 2
WLAN 2
以太网 4
以太网 3
本地连接
本地连接
Adapter
以太网 2
```

地址:
2001:250:fe01:130:a9b8:92e7:3c94:2cdc,
2001:250:fe01:130:7cdf:d6f3:6089:5f61,
fe80::a9b8:92e7:3c94:2cdc, 172.20.78.35
无捕获过滤器

1. wireshark的使用

   双击WLAN2，wireshark就自动开始分组捕获，可以在应用显示过滤器一栏中输入协议进行筛选。可以将捕获记录保存到本地。



正在捕获 WLAN 2
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.  Time      Source                  Destination             Protocol Length Info
   4 0.939889  2409:8c54:1003:10::…   2001:250:fe01:130:4…   TCP          78 80 → 42360 [SY
   5 1.340966  111.30.159.59           172.20.78.35            OICQ        129 OICQ Protocol
   6 1.943860  2a01:111:2003::52       2001:250:fe01:130:4…   TCP          78 80 → 50664 [SY
   7 2.047134  2a01:111:2003::52       2001:250:fe01:130:4…   HTTP        207 HTTP/1.1 307 T
   8 2.047134  2a01:111:2003::52       2001:250:fe01:130:4…   TCP          74 80 → 50664 [FI
   9 2.047134  2a01:111:2003::52       2001:250:fe01:130:4…   TCP          74 80 → 50664 [AC
  10 2.251367  2409:8c54:1003:1019…   2001:250:fe01:130:4…   TCP          78 80 → 53572 [SY
```

```
> Frame 1: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on interface \Device\N
> Ethernet II, Src: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2), Dst: IntelCor_cc:6f:dc (d8:f2:ca:cc:
> Internet Protocol Version 4, Src: 111.30.159.59, Dst: 172.20.78.35
> User Datagram Protocol, Src Port: 8000, Dst Port: 4005
> OICQ - IM software, popular in China
```

```
0000  d8 f2 ca cc 6f dc 44 ec  ce d2 ff c2 08 00 45 00   ····o·D· ······E·
0010  00 73 9b 41 40 00 35 11  a1 a7 6f 1e 9f 3b ac 14   ·s·A@·5· ··o··;··
0020  4e 23 1f 40 0f a5 00 5f  b0 2f 02 38 33 00 81 41   N#·@···_ ·/·83··A
0030  8f 2f 17 36 8a 00 00 00  78 5d e8 65 01 ff 0e 1b   ·/·6···· x]·e····
0040  81 28 5f 39 19 1a b4 a3  df b5 db 43 c9 a3 8d ac   ·(_9···· ···C····
0050  d6 10 e0 3b e1 a8 28 e6  8f e5 b6 64 6b c0 d0 4d   ···;··(· ···dk··M
0060  a9 3f 9f c5 f4 d9 17 fb  1e 94 9e a7 9e d2 17 ef   ·?······ ········
0070  8f e5 1a f4 46 3b ca 1f  27 a8 d0 95 7d 55 be 8e   ····F;·· '···}U··
0080  03                                                 ·
```

WLAN 2: <live capture in progress>
分组: 10 · 已显示: 10 (100.0%)
配置: Default

2. HTTP分析

（1）.HTTP GET/response交互

在应用显示过滤器中输入http进行筛选，然后开始捕获。打开浏览器，访问hitgs.hit.edu.cn，然后停止捕获。将结果保存在http1.pcapng中。

（2）.HTTP 条件GET/response交互

启动浏览器，清楚缓存，在应用显示过滤器中输入http进行筛选，然后开始捕获，访问hitgs.hit.edu.cn，然后刷新网页，停止分组捕获。将结果保存在http2.pcapng中。

3. TCP分析

首先访问http://gaia.cs.umass.edu/wireshark-labs/alice.txt，获得alice.txt文件。然后打开http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html，选择好本地alice.txt文件的 位置。然后启动Wireshark开始分组捕获，在浏览器中点击“Upload alice.txt file”按钮上传文件，在文件上传完毕后停止Wireshark分组捕获。在筛选规则中选择“tcp”部分，进行分析即可，将所有分组保存在文件tcp.pcapng中。

4. IP分析

使用pingplotter进行实验，待发送IP分组的网站为hit.edu.cn，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。将所有分组保存在ip.pcapng中。

5. 抓取ARP数据包

在命令行输入arp –a命令，查看主机上ARP缓存的内容。在命令行模式下输入：ping 192.168.1.82。然后启动Wireshark进行捕获。将所有分组保存在arp.pcapng中。

6. 抓取UDP数据包

先启动Wireshark分组捕获，然后用QQ给好友发送消息，消息发送结束后，停止分组捕获。将所有分组保存在udp.pcapng中。

7. 利用wireshark进行DNS协议分析

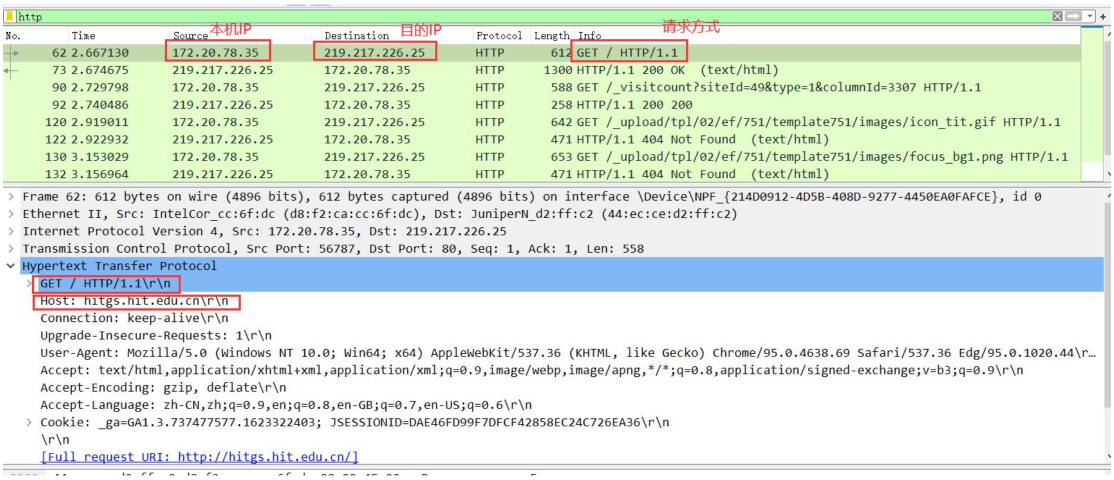
打开浏览器输入www.baidu.com，打开wireshark启动抓包，在控制台回车执行完毕后停止抓包。将所有分组保存在dns.pcapng中。

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。

1. HTTP GET/response交互

打开http1.pcapng，输入http进行分组过滤，点击第一条HTTP报文，信息如下。



```
No.     Time      Source          Destination     Protocol Length Info
   62 2.667130    172.20.78.35    219.217.226.25  HTTP      612 GET / HTTP/1.1
   73 2.674675    219.217.226.25  172.20.78.35    HTTP     1300 HTTP/1.1 200 OK  (text/html)
   90 2.729798    172.20.78.35    219.217.226.25  HTTP      588 GET /_visitcount?siteId=49&type=1&columnId=3307 HTTP/1.1
   92 2.740486    219.217.226.25  172.20.78.35    HTTP      258 HTTP/1.1 200 200
  120 2.919011    172.20.78.35    219.217.226.25  HTTP      642 GET /_upload/tpl/02/ef/751/template751/images/icon_tit.gif HTTP/1.1
  122 2.922932    219.217.226.25  172.20.78.35    HTTP      471 HTTP/1.1 404 Not Found  (text/html)
  130 3.153029    172.20.78.35    219.217.226.25  HTTP      653 GET /_upload/tpl/02/ef/751/template751/images/focus_bg1.png HTTP/1.1
  132 3.156964    219.217.226.25  172.20.78.35    HTTP      471 HTTP/1.1 404 Not Found  (text/html)

> Frame 62: 612 bytes on wire (4896 bits), 612 bytes captured (4896 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
> Internet Protocol Version 4, Src: 172.20.78.35, Dst: 219.217.226.25
> Transmission Control Protocol, Src Port: 56787, Dst Port: 80, Seq: 1, Ack: 1, Len: 558
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: hitgs.hit.edu.cn\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36 Edg/95.0.1020.44\r…
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
  > Cookie: _ga=GA1.3.737477577.1623322403; JSESSIONID=DAE46FD99F7DFCF42858EC24C726EA36\r\n
    \r\n
    [Full request URI: http://hitgs.hit.edu.cn/]
```

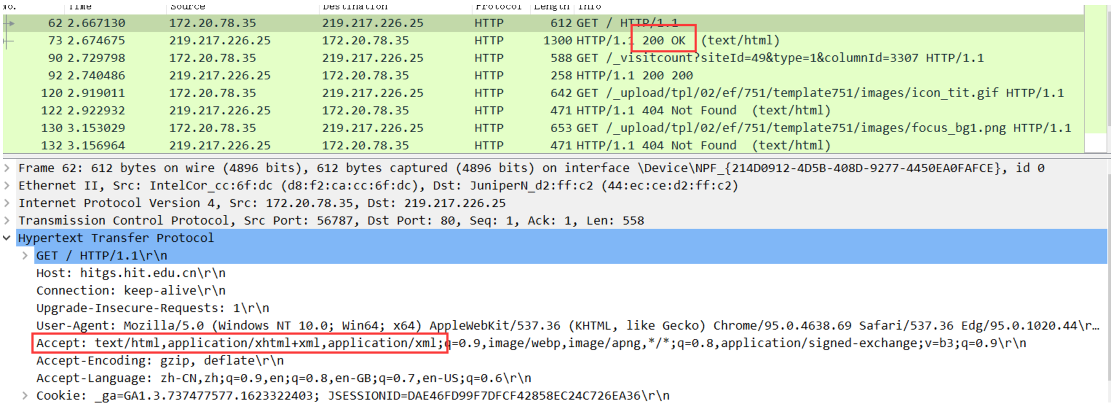
思考题：

(1).浏览器运行的协议为HTTP/1.1，访问的服务器运行的HTTP版本号是HTTP/1.1。

(2).浏览器向服务器指出的接收的语言版本对象为：Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n。

(3).本机IP地址为172.20.78.35，服务器的IP地址为219.217.226.25。

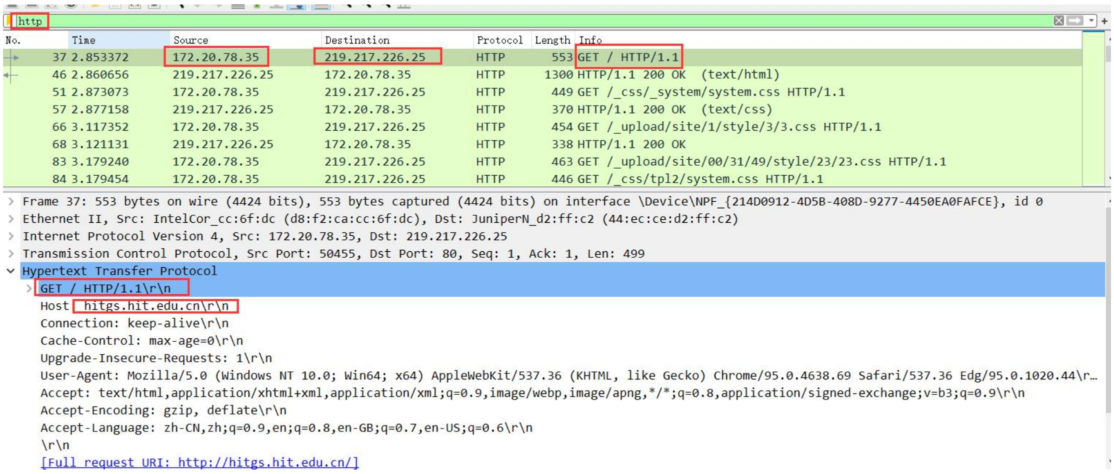
(4).服务器向浏览器返回的状态码为200。



```
No.    Time         Source            Destination       Protocol  Length Info
    62 2.667130     172.20.78.35      219.217.226.25    HTTP       612 GET / HTTP/1.1
    73 2.674675     219.217.226.25    172.20.78.35      HTTP      1300 HTTP/1.1 200 OK  (text/html)
    90 2.729798     172.20.78.35      219.217.226.25    HTTP       588 GET /_visitcount?siteId=49&type=1&columnId=3307 HTTP/1.1
    92 2.740486     219.217.226.25    172.20.78.35      HTTP       258 HTTP/1.1 200 200
   120 2.919011     172.20.78.35      219.217.226.25    HTTP       642 GET /_upload/tpl/02/ef/751/template751/images/icon_tit.gif HTTP/1.1
   122 2.922932     219.217.226.25    172.20.78.35      HTTP       471 HTTP/1.1 404 Not Found  (text/html)
   130 3.153029     172.20.78.35      219.217.226.25    HTTP       653 GET /_upload/tpl/02/ef/751/template751/images/focus_bg1.png HTTP/1.1
   132 3.156964     219.217.226.25    172.20.78.35      HTTP       471 HTTP/1.1 404 Not Found  (text/html)

> Frame 62: 612 bytes on wire (4896 bits), 612 bytes captured (4896 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
> Internet Protocol Version 4, Src: 172.20.78.35, Dst: 219.217.226.25
> Transmission Control Protocol, Src Port: 56787, Dst Port: 80, Seq: 1, Ack: 1, Len: 558
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: hitgs.hit.edu.cn\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36 Edg/95.0.1020.44\r…
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
  > Cookie: _ga=GA1.3.737477577.1623322403; JSESSIONID=DAE46FD99F7DFCF42858EC24C726EA36\r\n
```

2. HTTP 条件GET/response交互

打开http2.pcapng，输入http进行分组过滤，点击第一条HTTP报文，信息如下。

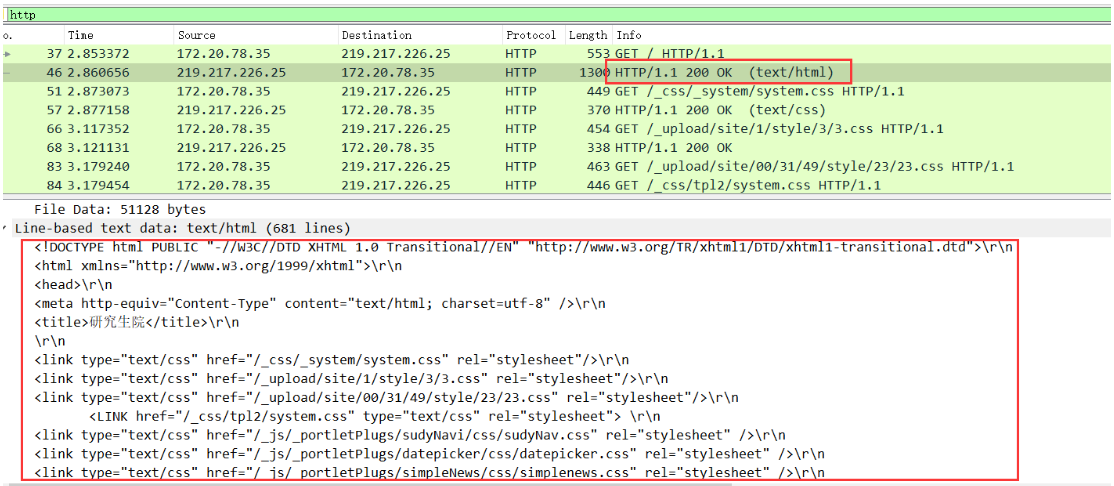


```
http

No.    Time         Source            Destination       Protocol  Length Info
    37 2.853372     172.20.78.35      219.217.226.25    HTTP       553 GET / HTTP/1.1
    46 2.860656     219.217.226.25    172.20.78.35      HTTP      1300 HTTP/1.1 200 OK  (text/html)
    51 2.873073     172.20.78.35      219.217.226.25    HTTP       449 GET /_css/_system/system.css HTTP/1.1
    57 2.877158     219.217.226.25    172.20.78.35      HTTP       370 HTTP/1.1 200 OK  (text/css)
    66 3.117352     172.20.78.35      219.217.226.25    HTTP       454 GET /_upload/site/1/style/3/3.css HTTP/1.1
    68 3.121131     219.217.226.25    172.20.78.35      HTTP       338 HTTP/1.1 200 OK
    83 3.179240     172.20.78.35      219.217.226.25    HTTP       463 GET /_upload/site/00/31/49/style/23/23.css HTTP/1.1
    84 3.179454     172.20.78.35      219.217.226.25    HTTP       446 GET /_css/tpl2/system.css HTTP/1.1

> Frame 37: 553 bytes on wire (4424 bits), 553 bytes captured (4424 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
> Internet Protocol Version 4, Src: 172.20.78.35, Dst: 219.217.226.25
> Transmission Control Protocol, Src Port: 50455, Dst Port: 80, Seq: 1, Ack: 1, Len: 499
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host  hitgs.hit.edu.cn\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36 Edg/95.0.1020.44\r…
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
    \r\n
    [Full request URI: http://hitgs.hit.edu.cn/]
```

思考题：

(1).第一个HTTP GET请求没有IF-MODIFIED-SINCE头部

(2).服务器在第一个GET中返回了文件的内容如下。可以看出服务器返回的文件内容是用来构成主页HTML的其他元素。



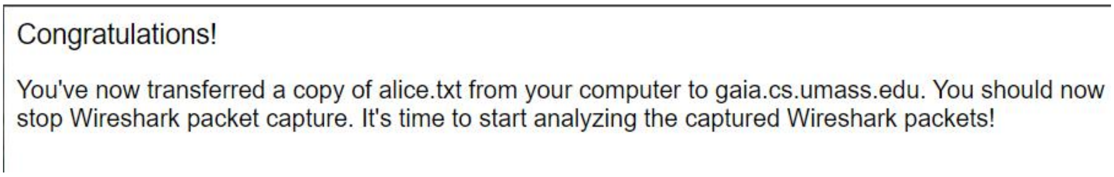
```
http
o.      Time        Source            Destination       Protocol Length Info
   37 2.853372    172.20.78.35      219.217.226.25    HTTP      553 GET / HTTP/1.1
   46 2.860656    219.217.226.25    172.20.78.35      HTTP     1300 HTTP/1.1 200 OK  (text/html)
   51 2.873073    172.20.78.35      219.217.226.25    HTTP      449 GET /_css/_system/system.css HTTP/1.1
   57 2.877158    219.217.226.25    172.20.78.35      HTTP      370 HTTP/1.1 200 OK  (text/css)
   66 3.117352    172.20.78.35      219.217.226.25    HTTP      454 GET /_upload/site/1/style/3/3.css HTTP/1.1
   68 3.121131    219.217.226.25    172.20.78.35      HTTP      338 HTTP/1.1 200 OK
   83 3.179240    172.20.78.35      219.217.226.25    HTTP      463 GET /_upload/site/00/31/49/style/23/23.css HTTP/1.1
   84 3.179454    172.20.78.35      219.217.226.25    HTTP      446 GET /_css/tpl2/system.css HTTP/1.1
    File Data: 51128 bytes
  Line-based text data: text/html (681 lines)
    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">\r\n
    <html xmlns="http://www.w3.org/1999/xhtml">\r\n
    <head>\r\n
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />\r\n
    <title>研究生院</title>\r\n
    \r\n
    <link type="text/css" href="/_css/_system/system.css" rel="stylesheet"/>\r\n
    <link type="text/css" href="/_upload/site/1/style/3/3.css" rel="stylesheet"/>\r\n
    <link type="text/css" href="/_upload/site/00/31/49/style/23/23.css" rel="stylesheet"/>\r\n
          <LINK href="/_css/tpl2/system.css" type="text/css" rel="stylesheet"> \r\n
    <link type="text/css" href="/_js/_portletPlugs/sudyNavi/css/sudyNav.css" rel="stylesheet" />\r\n
    <link type="text/css" href="/_js/_portletPlugs/datepicker/css/datepicker.css" rel="stylesheet" />\r\n
    <link type="text/css" href="/_js/_portletPlugs/simpleNews/css/simplenews.css" rel="stylesheet" />\r\n
```

(3).对于浏览器向服务器发出较晚的HTTP GET请求，报文中有一行IF-MODIFIED-SINCE。在该首部行后跟着的信息是缓存文件上次修改的时间。

(4).服务器对较晚的HTTP GET请求的响应中的HTTP状态代码是304，服务器不会明确返回文件的内容，因为会从浏览器中读取内容。

3. TCP分析

下载alice.txt之后，进入网站上传。

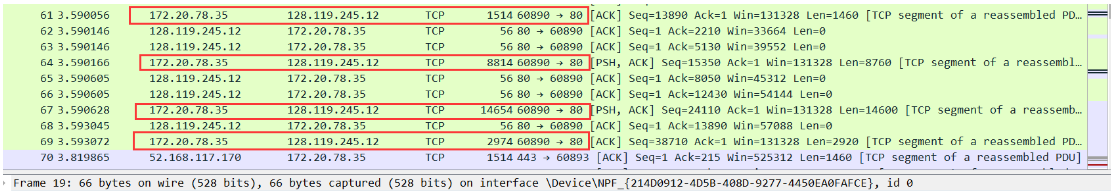


Congratulations!

You've now transferred a copy of alice.txt from your computer to gaia.cs.umass.edu. You should now stop Wireshark packet capture. It's time to start analyzing the captured Wireshark packets!

思考题：

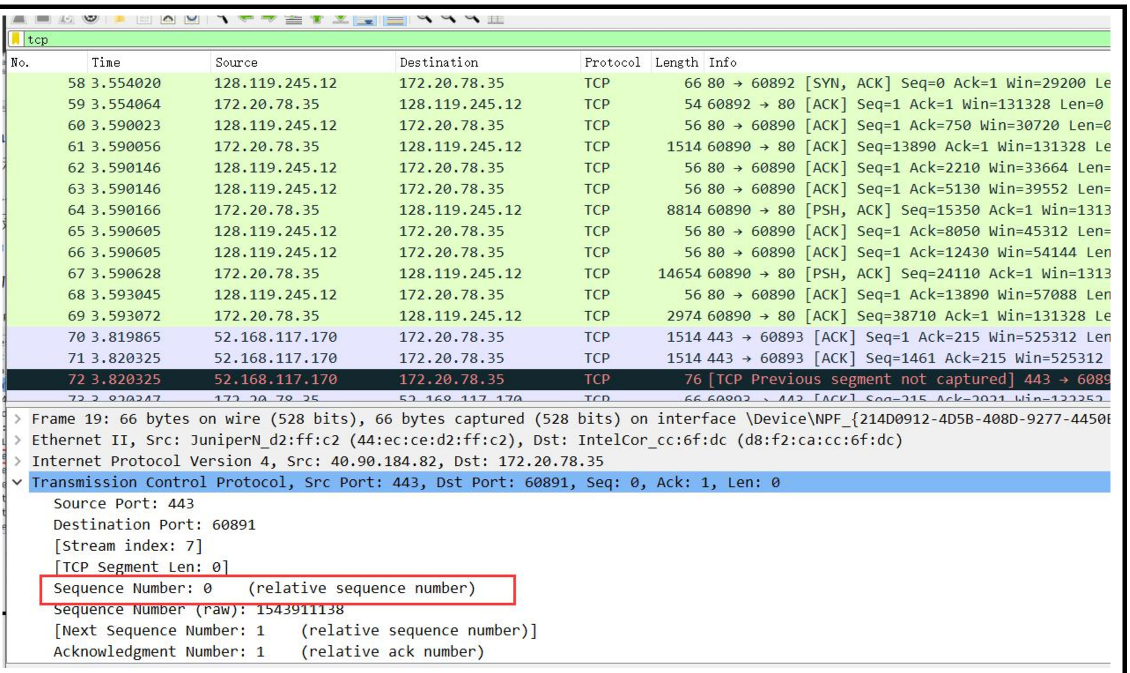
(1). 客户端主机的IP地址和TCP端口号分别为172.20.78.35和60891。



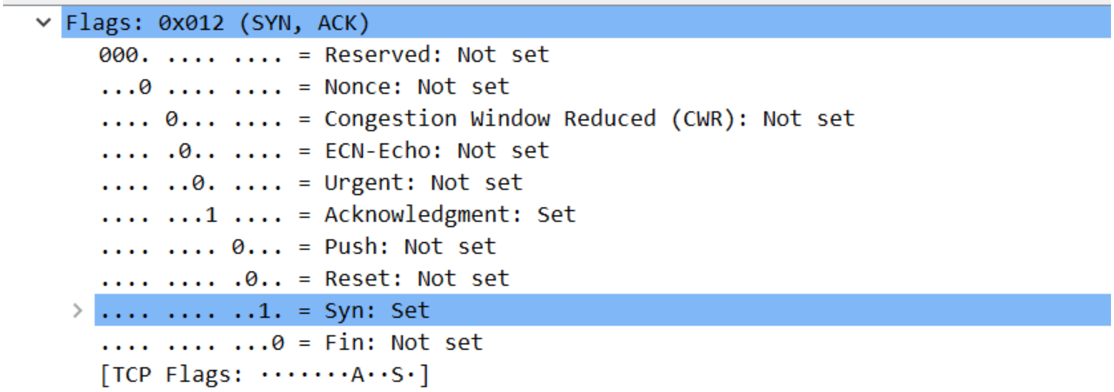
```
   61 3.590056    172.20.78.35     128.119.245.12   TCP    1514 60890 → 80 [ACK] Seq=13890 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PD…
   62 3.590146    128.119.245.12   172.20.78.35     TCP      56 80 → 60890 [ACK] Seq=1 Ack=2210 Win=33664 Len=0
   63 3.590146    128.119.245.12   172.20.78.35     TCP      56 80 → 60890 [ACK] Seq=1 Ack=5130 Win=39552 Len=0
   64 3.590166    172.20.78.35     128.119.245.12   TCP    8814 60890 → 80 [PSH, ACK] Seq=15350 Ack=1 Win=131328 Len=8760 [TCP segment of a reassembl…
   65 3.590605    128.119.245.12   172.20.78.35     TCP      56 80 → 60890 [ACK] Seq=1 Ack=8050 Win=45312 Len=0
   66 3.590605    128.119.245.12   172.20.78.35     TCP      56 80 → 60890 [ACK] Seq=1 Ack=12430 Win=54144 Len=0
   67 3.590628    172.20.78.35     128.119.245.12   TCP   14654 60890 → 80 [PSH, ACK] Seq=24110 Ack=1 Win=131328 Len=14600 [TCP segment of a reassemb…
   68 3.593045    128.119.245.12   172.20.78.35     TCP      56 80 → 60890 [ACK] Seq=1 Ack=13890 Win=57088 Len=0
   69 3.593072    172.20.78.35     128.119.245.12   TCP    2974 60890 → 80 [ACK] Seq=38710 Ack=1 Win=131328 Len=2920 [TCP segment of a reassembled PD…
   70 3.819865    52.168.117.170   172.20.78.35     TCP    1514 443 → 60893 [ACK] Seq=1 Ack=215 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
 Frame 19: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
```

(2). 服务器IP地址为128. 119. 245. 12，它用来发送和接收TCP报文的端口号是80。

(3). 客户服务器之间用于初始化TCP 连接的TCP SYN报文段的序号是0。在该报文段中将SYN置为1，表示该报文段用于tcp建立连接。

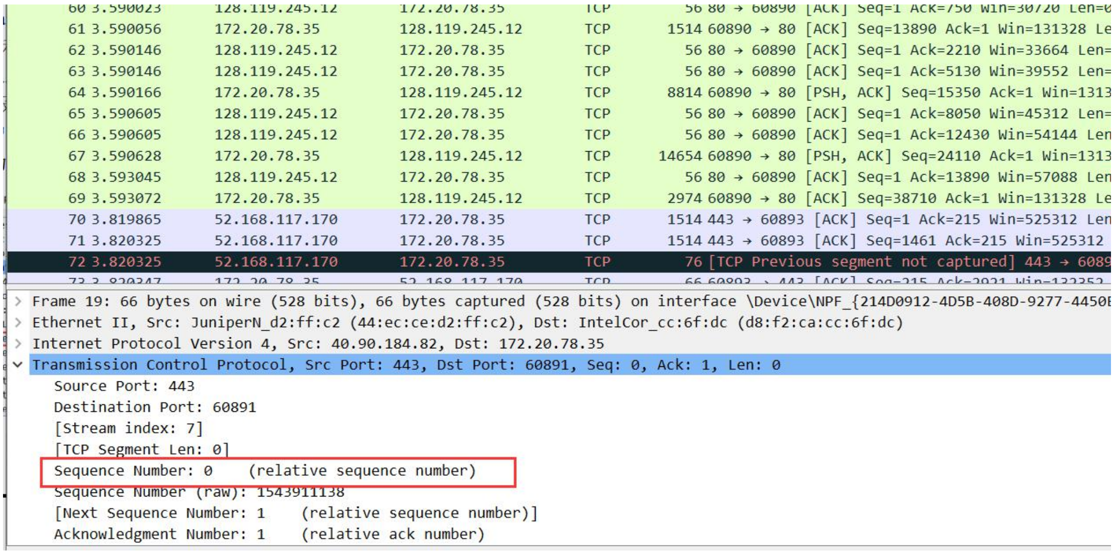


```
tcp
No.   Time        Source           Destination      Protocol  Length Info
   58 3.554020    128.119.245.12   172.20.78.35     TCP         66 80 → 60892 [SYN, ACK] Seq=0 Ack=1 Win=29200 Le
   59 3.554064    172.20.78.35     128.119.245.12   TCP         54 60892 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   60 3.590023    128.119.245.12   172.20.78.35     TCP         56 80 → 60890 [ACK] Seq=1 Ack=750 Win=30720 Len=0
   61 3.590056    172.20.78.35     128.119.245.12   TCP       1514 60890 → 80 [ACK] Seq=13890 Ack=1 Win=131328 Le
   62 3.590146    128.119.245.12   172.20.78.35     TCP         56 80 → 60890 [ACK] Seq=1 Ack=2210 Win=33664 Len=
   63 3.590146    128.119.245.12   172.20.78.35     TCP         56 80 → 60890 [ACK] Seq=1 Ack=5130 Win=39552 Len=
   64 3.590166    172.20.78.35     128.119.245.12   TCP       8814 60890 → 80 [PSH, ACK] Seq=15350 Ack=1 Win=1313
   65 3.590605    128.119.245.12   172.20.78.35     TCP         56 80 → 60890 [ACK] Seq=1 Ack=8050 Win=45312 Len=
   66 3.590605    128.119.245.12   172.20.78.35     TCP         56 80 → 60890 [ACK] Seq=1 Ack=12430 Win=54144 Len
   67 3.590628    172.20.78.35     128.119.245.12   TCP      14654 60890 → 80 [PSH, ACK] Seq=24110 Ack=1 Win=1313
   68 3.593045    128.119.245.12   172.20.78.35     TCP         56 80 → 60890 [ACK] Seq=1 Ack=13890 Win=57088 Len
   69 3.593072    172.20.78.35     128.119.245.12   TCP       2974 60890 → 80 [ACK] Seq=38710 Ack=1 Win=131328 Le
   70 3.819865    52.168.117.170   172.20.78.35     TCP       1514 443 → 60893 [ACK] Seq=1 Ack=215 Win=525312 Len
   71 3.820325    52.168.117.170   172.20.78.35     TCP       1514 443 → 60893 [ACK] Seq=1461 Ack=215 Win=525312
   72 3.820325    52.168.117.170   172.20.78.35     TCP         76 [TCP Previous segment not captured] 443 → 6089
   73 3.820347    172.20.78.35     52.168.117.170   TCP         66 60893 → 443 [ACK] Seq=215 Ack=2921 Win=132352

> Frame 19: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450E
> Ethernet II, Src: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2), Dst: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc)
> Internet Protocol Version 4, Src: 40.90.184.82, Dst: 172.20.78.35
v Transmission Control Protocol, Src Port: 443, Dst Port: 60891, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 60891
    [Stream index: 7]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1543911138
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
```



```
v 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
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······A··S·]
```

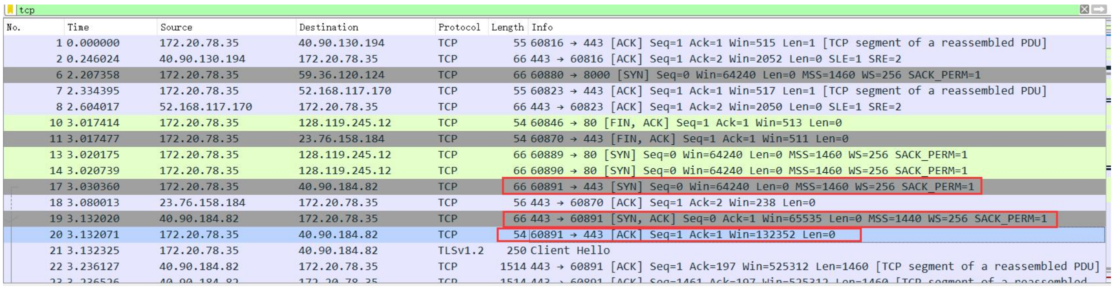
(4). 服务器向客户端发送的SYNACK报文段序号为0。该报文段中Acknowledgement字段的值是1。Gaia.cs.umass.edu服务器通过SYN请求报文段的seq序号加1来决定此值。在该报文段中，是使用flag部分的ack以及SYN标记为1来标示该报文段是SYNACK报文段的。



```
   60 3.590023    128.119.245.12   172.20.78.35     TCP         56 80 → 60890 [ACK] Seq=1 Ack=750 Win=30720 Len=0
   61 3.590056    172.20.78.35     128.119.245.12   TCP       1514 60890 → 80 [ACK] Seq=13890 Ack=1 Win=131328 Le
   62 3.590146    128.119.245.12   172.20.78.35     TCP         56 80 → 60890 [ACK] Seq=1 Ack=2210 Win=33664 Len=
   63 3.590146    128.119.245.12   172.20.78.35     TCP         56 80 → 60890 [ACK] Seq=1 Ack=5130 Win=39552 Len=
   64 3.590166    172.20.78.35     128.119.245.12   TCP       8814 60890 → 80 [PSH, ACK] Seq=15350 Ack=1 Win=1313
   65 3.590605    128.119.245.12   172.20.78.35     TCP         56 80 → 60890 [ACK] Seq=1 Ack=8050 Win=45312 Len=
   66 3.590605    128.119.245.12   172.20.78.35     TCP         56 80 → 60890 [ACK] Seq=1 Ack=12430 Win=54144 Len
   67 3.590628    172.20.78.35     128.119.245.12   TCP      14654 60890 → 80 [PSH, ACK] Seq=24110 Ack=1 Win=1313
   68 3.593045    128.119.245.12   172.20.78.35     TCP         56 80 → 60890 [ACK] Seq=1 Ack=13890 Win=57088 Len
   69 3.593072    172.20.78.35     128.119.245.12   TCP       2974 60890 → 80 [ACK] Seq=38710 Ack=1 Win=131328 Le
   70 3.819865    52.168.117.170   172.20.78.35     TCP       1514 443 → 60893 [ACK] Seq=1 Ack=215 Win=525312 Len
   71 3.820325    52.168.117.170   172.20.78.35     TCP       1514 443 → 60893 [ACK] Seq=1461 Ack=215 Win=525312
   72 3.820325    52.168.117.170   172.20.78.35     TCP         76 [TCP Previous segment not captured] 443 → 6089
   73 3.820347    172.20.78.35     52.168.117.170   TCP         66 60893 → 443 [ACK] Seq=215 Ack=2921 Win=132352

> Frame 19: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450E
> Ethernet II, Src: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2), Dst: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc)
> Internet Protocol Version 4, Src: 40.90.184.82, Dst: 172.20.78.35
v Transmission Control Protocol, Src Port: 443, Dst Port: 60891, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 60891
    [Stream index: 7]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1543911138
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
```

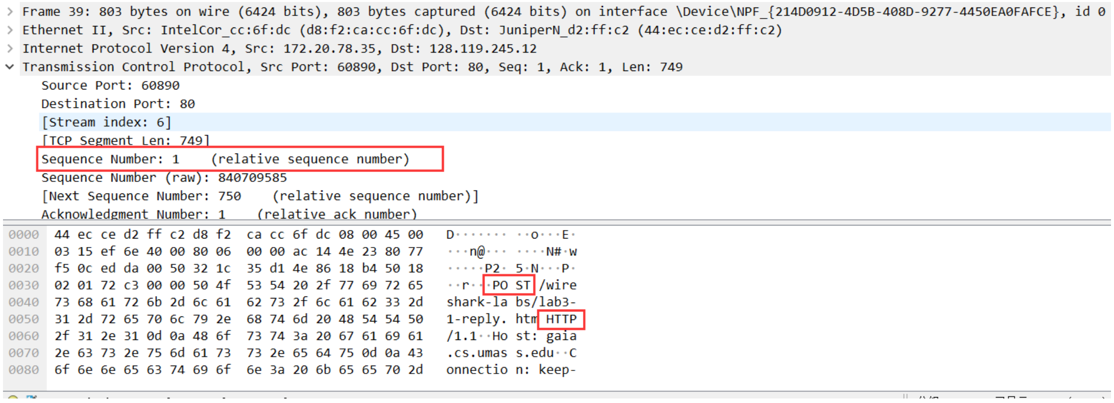
(5).分析TCP三次握手过程

第一次握手，客户端向服务器发送SYN请求报文，第二次握手，服务器向客户端回复SYNACK报文，然后第三次握手就是客户端向服务器回复ack报文段，此时回复的ack报文段中，ack的内容为为1（为SYNACK报文段序号加1），说明是第三次握手。



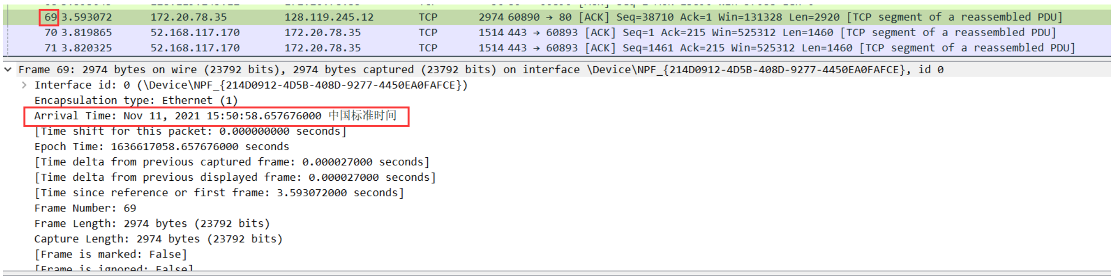
```
tcp
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  172.20.78.35    40.90.130.194   TCP        55 60816 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reassembled PDU]
   2 0.246024  40.90.130.194   172.20.78.35    TCP        66 443 → 60816 [ACK] Seq=1 Ack=2 Win=2052 Len=0 SLE=1 SRE=2
   6 2.207358  172.20.78.35    59.36.120.124   TCP        66 60880 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   7 2.334395  172.20.78.35    52.168.117.170  TCP        55 60823 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reassembled PDU]
   8 2.604017  52.168.117.170  172.20.78.35    TCP        66 443 → 60823 [ACK] Seq=1 Ack=2 Win=2050 Len=0 SLE=1 SRE=2
  10 3.017414  172.20.78.35    128.119.245.12  TCP        54 60846 → 80 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
  11 3.017477  172.20.78.35    23.76.158.184   TCP        54 60870 → 443 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0
  13 3.020175  172.20.78.35    128.119.245.12  TCP        66 60889 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  14 3.020739  172.20.78.35    128.119.245.12  TCP        66 60890 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  17 3.030360  172.20.78.35    40.90.184.82    TCP        66 60891 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  18 3.080013  23.76.158.184   172.20.78.35    TCP        56 443 → 60870 [ACK] Seq=1 Ack=2 Win=238 Len=0
  19 3.132020  40.90.184.82    172.20.78.35    TCP        66 443 → 60891 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
  20 3.132071  172.20.78.35    40.90.184.82    TCP        54 60891 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  21 3.132325  172.20.78.35    40.90.184.82    TLSv1.2   250 Client Hello
  22 3.236127  40.90.184.82    172.20.78.35    TCP      1514 443 → 60891 [ACK] Seq=1 Ack=197 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
  23 3.236526  40.90.184.82    172.20.78.35    TCP      1514 443 → 60891 [ACK] Seq=1461 Ack=197 Win=525312 Len=1460 [TCP segment of a reassembled
```

(6).包含HTTP POST命令的TCP报文段的序号是1。



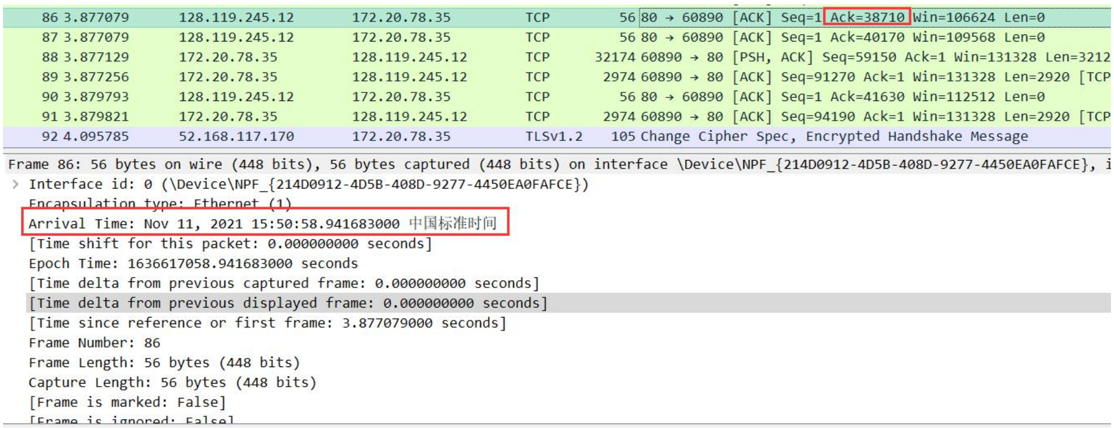
```
> Frame 39: 803 bytes on wire (6424 bits), 803 bytes captured (6424 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
> Internet Protocol Version 4, Src: 172.20.78.35, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 60890, Dst Port: 80, Seq: 1, Ack: 1, Len: 749
    Source Port: 60890
    Destination Port: 80
    [Stream index: 6]
    [TCP Segment Len: 749]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 840709585
    [Next Sequence Number: 750    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)

0000  44 ec ce d2 ff c2 d8 f2  ca cc 6f dc 08 00 45 00   D·······  ··o···E·
0010  03 15 ef 6e 40 00 80 06  00 00 ac 14 4e 23 80 77   ···n@···  ····N#·w
0020  f5 0c ed da 00 50 32 1c  35 d1 4e 86 18 b4 50 18   ·····P2·  5·N···P·
0030  02 01 72 c3 00 00 50 4f  53 54 20 2f 77 69 72 65   ··r···PO  ST /wire
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la  bs/lab3-
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply.  htm HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 67 61 69 61   /1.1··Ho  st: gaia
0070  2e 63 73 2e 75 6d 61 73  73 2e 65 64 75 0d 0a 43   .cs.umas  s.edu··C
0080  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio  n: keep-
```

(7).向下查询到第六个报文段信息如下：



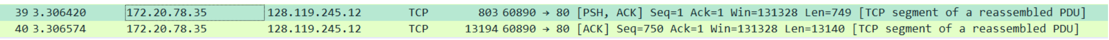
```
  69 3.593072  172.20.78.35    128.119.245.12  TCP   2974 60890 → 80 [ACK] Seq=38710 Ack=1 Win=131328 Len=2920 [TCP segment of a reassembled PDU]
  70 3.819865  52.168.117.170  172.20.78.35    TCP   1514 443 → 60893 [ACK] Seq=1 Ack=215 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
  71 3.820325  52.168.117.170  172.20.78.35    TCP   1514 443 → 60893 [ACK] Seq=1461 Ack=215 Win=525312 Len=1460 [TCP segment of a reassembled PDU]

v Frame 69: 2974 bytes on wire (23792 bits), 2974 bytes captured (23792 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
  > Interface id: 0 (\Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 11, 2021 15:50:58.657676000 中国标准时间
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1636617058.657676000 seconds
    [Time delta from previous captured frame: 0.000027000 seconds]
    [Time delta from previous displayed frame: 0.000027000 seconds]
    [Time since reference or first frame: 3.593072000 seconds]
    Frame Number: 69
    Frame Length: 2974 bytes (23792 bits)
    Capture Length: 2974 bytes (23792 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
```

是在第一帧发送后3.593秒之后发送的报文段。该报文段对应的ACK报文接收如下：

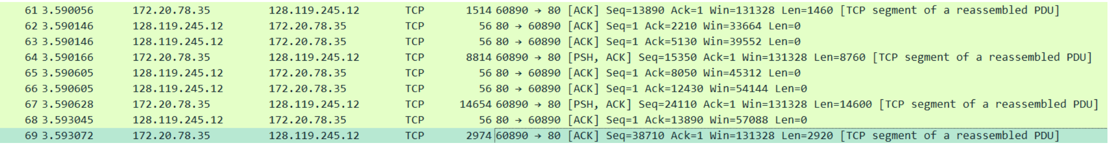


```
  86 3.877079  128.119.245.12  172.20.78.35    TCP      56 80 → 60890 [ACK] Seq=1 Ack=38710 Win=106624 Len=0
  87 3.877079  128.119.245.12  172.20.78.35    TCP      56 80 → 60890 [ACK] Seq=1 Ack=40170 Win=109568 Len=0
  88 3.877129  172.20.78.35    128.119.245.12  TCP   32174 60890 → 80 [PSH, ACK] Seq=59150 Ack=1 Win=131328 Len=3212
  89 3.877256  172.20.78.35    128.119.245.12  TCP    2974 60890 → 80 [ACK] Seq=91270 Ack=1 Win=131328 Len=2920 [TCP
  90 3.879793  128.119.245.12  172.20.78.35    TCP      56 80 → 60890 [ACK] Seq=1 Ack=41630 Win=112512 Len=0
  91 3.879821  172.20.78.35    128.119.245.12  TCP    2974 60890 → 80 [ACK] Seq=94190 Ack=1 Win=131328 Len=2920 [TCP
  92 4.095785  52.168.117.170  172.20.78.35    TLSv1.2  105 Change Cipher Spec, Encrypted Handshake Message

Frame 86: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, i
  > Interface id: 0 (\Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 11, 2021 15:50:58.941683000 中国标准时间
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1636617058.941683000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 3.877079000 seconds]
    Frame Number: 86
    Frame Length: 56 bytes (448 bits)
    Capture Length: 56 bytes (448 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
```

(8).



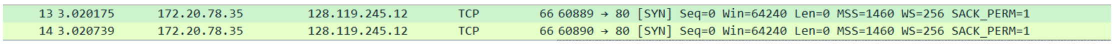
```
 39 3.306420   172.20.78.35     128.119.245.12    TCP     803 60890 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=749 [TCP segment of a reassembled PDU]
 40 3.306574   172.20.78.35     128.119.245.12    TCP   13194 60890 → 80 [ACK] Seq=750 Ack=1 Win=131328 Len=13140 [TCP segment of a reassembled PDU]
```



```
 61 3.590056   172.20.78.35     128.119.245.12    TCP    1514 60890 → 80 [ACK] Seq=13890 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
 62 3.590146   128.119.245.12   172.20.78.35      TCP      56 80 → 60890 [ACK] Seq=1 Ack=2210 Win=33664 Len=0
 63 3.590146   128.119.245.12   172.20.78.35      TCP      56 80 → 60890 [ACK] Seq=1 Ack=5130 Win=39552 Len=0
 64 3.590166   172.20.78.35     128.119.245.12    TCP    8814 60890 → 80 [PSH, ACK] Seq=15350 Ack=1 Win=131328 Len=8760 [TCP segment of a reassembled PDU]
 65 3.590605   128.119.245.12   172.20.78.35      TCP      56 80 → 60890 [ACK] Seq=1 Ack=8050 Win=45312 Len=0
 66 3.590605   128.119.245.12   172.20.78.35      TCP      56 80 → 60890 [ACK] Seq=1 Ack=12430 Win=54144 Len=0
 67 3.590628   172.20.78.35     128.119.245.12    TCP   14654 60890 → 80 [PSH, ACK] Seq=24110 Ack=1 Win=131328 Len=14600 [TCP segment of a reassembled PDU]
 68 3.593045   128.119.245.12   172.20.78.35      TCP      56 80 → 60890 [ACK] Seq=1 Ack=13890 Win=57088 Len=0
 69 3.593072   172.20.78.35     128.119.245.12    TCP    2974 60890 → 80 [ACK] Seq=38710 Ack=1 Win=131328 Len=2920 [TCP segment of a reassembled PDU]
```

长度分别为：749，13140，1460，8760，14600，2920字节。

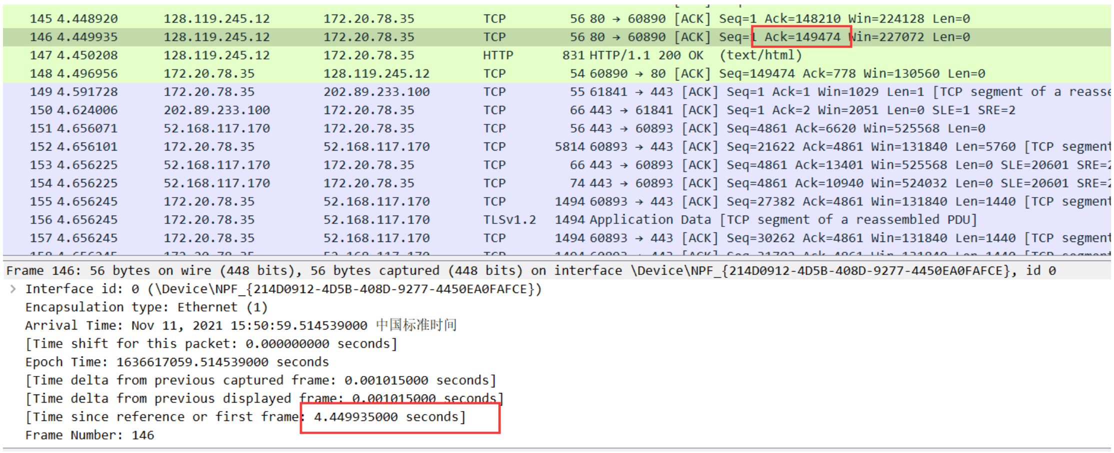
(9).接收端公示的最小的可用缓存空间为64240字节。在整个过程中接收端并没有对发送端的传输进行限制



```
 13 3.020175   172.20.78.35     128.119.245.12    TCP      66 60889 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 14 3.020739   172.20.78.35     128.119.245.12    TCP      66 60890 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

(10).得到序列号随时间的变化，可以看出整个过程中序列号随时间一直增长，为1，750，13890，15350，24110，38710。而若有重传的报文段会出现序列号变小的情况。说明没有发生重传。

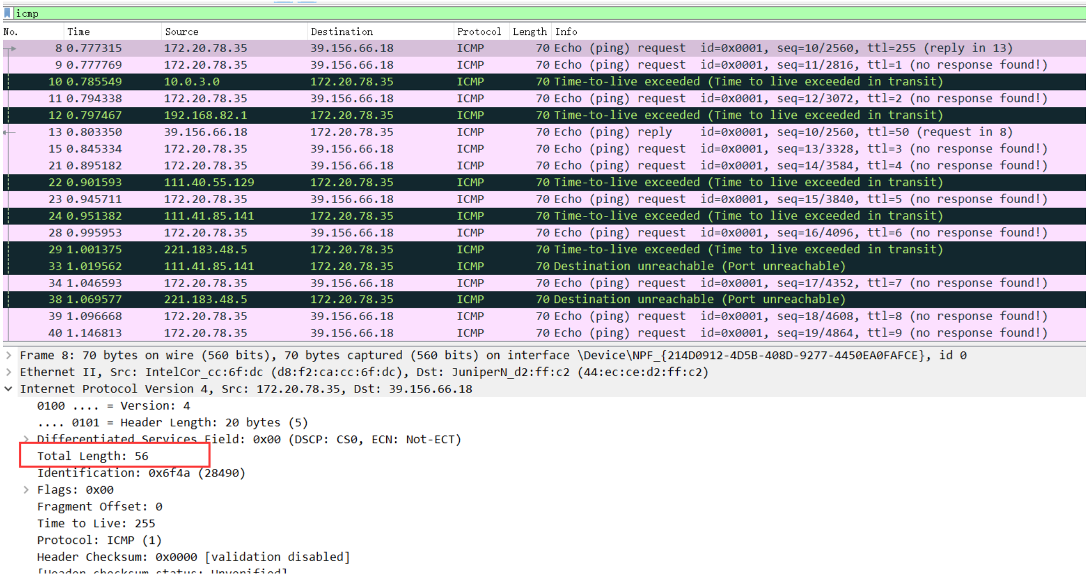
(11).总共传输的字节数为149474-1=149473字节，所用时间为4.449935-3.03036（第一次握手）=1.419575秒。吞吐量throughput=149473字节/1.419575秒=1.053MB/s。



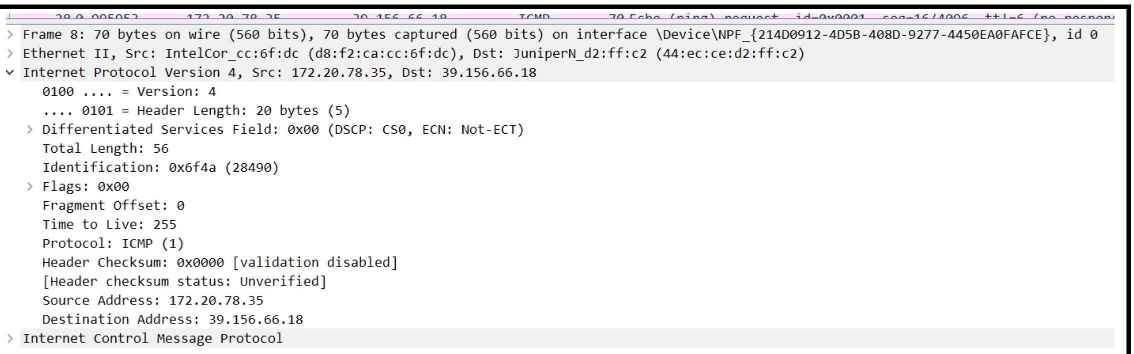
```
145 4.448920   128.119.245.12   172.20.78.35      TCP       56 80 → 60890 [ACK] Seq=1 Ack=148210 Win=224128 Len=0
146 4.449935   128.119.245.12   172.20.78.35      TCP       56 80 → 60890 [ACK] Seq=1 Ack=149474 Win=227072 Len=0
147 4.450208   128.119.245.12   172.20.78.35      HTTP     831 HTTP/1.1 200 OK  (text/html)
148 4.496956   172.20.78.35     128.119.245.12    TCP       54 60890 → 80 [ACK] Seq=149474 Ack=778 Win=130560 Len=0
149 4.591728   172.20.78.35     202.89.233.100    TCP       55 61841 → 443 [ACK] Seq=1 Ack=1 Win=1029 Len=1 [TCP segment of a reasse
150 4.624006   202.89.233.100   172.20.78.35      TCP       66 443 → 61841 [ACK] Seq=1 Ack=2 Win=2051 Len=0 SLE=1 SRE=2
151 4.656071   52.168.117.170   172.20.78.35      TCP       56 443 → 60893 [ACK] Seq=4861 Ack=6620 Win=525568 Len=0
152 4.656101   172.20.78.35     52.168.117.170    TCP     5814 60893 → 443 [ACK] Seq=21622 Ack=4861 Win=131840 Len=5760 [TCP segment
153 4.656225   52.168.117.170   172.20.78.35      TCP       66 443 → 60893 [ACK] Seq=4861 Ack=13401 Win=525568 Len=0 SLE=20601 SRE=
154 4.656225   52.168.117.170   172.20.78.35      TCP       74 443 → 60893 [ACK] Seq=4861 Ack=10940 Win=524032 Len=0 SLE=20601 SRE=
155 4.656245   172.20.78.35     52.168.117.170    TCP     1494 60893 → 443 [ACK] Seq=27382 Ack=4861 Win=131840 Len=1440 [TCP segment
156 4.656245   172.20.78.35     52.168.117.170    TLSv1.2 1494 Application Data [TCP segment of a reassembled PDU]
157 4.656245   172.20.78.35     52.168.117.170    TCP     1494 60893 → 443 [ACK] Seq=30262 Ack=4861 Win=131840 Len=1440 [TCP segment

Frame 146: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
 > Interface id: 0 (\Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE})
   Encapsulation type: Ethernet (1)
   Arrival Time: Nov 11, 2021 15:50:59.514539000 中国标准时间
   [Time shift for this packet: 0.000000000 seconds]
   Epoch Time: 1636617059.514539000 seconds
   [Time delta from previous captured frame: 0.001015000 seconds]
   [Time delta from previous displayed frame: 0.001015000 seconds]
   [Time since reference or first frame: 4.449935000 seconds]
   Frame Number: 146
```

4. IP分析

使用pingplotter向hit.edu.cn发送一系列大小为56字节，2000字节和3500字节的IP分组，然后用Wireshark进行捕获结果如下。



```
icmp
No.  Time       Source           Destination      Protocol Length Info
  8 0.777315   172.20.78.35     39.156.66.18     ICMP       70 Echo (ping) request  id=0x0001, seq=10/2560, ttl=255 (reply in 13)
  9 0.777769   172.20.78.35     39.156.66.18     ICMP       70 Echo (ping) request  id=0x0001, seq=11/2816, ttl=1 (no response found!)
 10 0.785549   10.0.3.0         172.20.78.35     ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 11 0.794338   172.20.78.35     39.156.66.18     ICMP       70 Echo (ping) request  id=0x0001, seq=12/3072, ttl=2 (no response found!)
 12 0.797467   192.168.82.1     172.20.78.35     ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 13 0.803350   39.156.66.18     172.20.78.35     ICMP       70 Echo (ping) reply    id=0x0001, seq=10/2560, ttl=50 (request in 8)
 15 0.845334   172.20.78.35     39.156.66.18     ICMP       70 Echo (ping) request  id=0x0001, seq=13/3328, ttl=3 (no response found!)
 21 0.895182   172.20.78.35     39.156.66.18     ICMP       70 Echo (ping) request  id=0x0001, seq=14/3584, ttl=4 (no response found!)
 22 0.901593   111.40.55.129    172.20.78.35     ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 23 0.945711   172.20.78.35     39.156.66.18     ICMP       70 Echo (ping) request  id=0x0001, seq=15/3840, ttl=5 (no response found!)
 24 0.951382   111.41.85.141    172.20.78.35     ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 28 0.995953   172.20.78.35     39.156.66.18     ICMP       70 Echo (ping) request  id=0x0001, seq=16/4096, ttl=6 (no response found!)
 29 1.001375   221.183.48.5     172.20.78.35     ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 33 1.019562   111.41.85.141    172.20.78.35     ICMP       70 Destination unreachable (Port unreachable)
 34 1.046593   172.20.78.35     39.156.66.18     ICMP       70 Echo (ping) request  id=0x0001, seq=17/4352, ttl=7 (no response found!)
 38 1.069577   221.183.48.5     172.20.78.35     ICMP       70 Destination unreachable (Port unreachable)
 39 1.096668   172.20.78.35     39.156.66.18     ICMP       70 Echo (ping) request  id=0x0001, seq=18/4608, ttl=8 (no response found!)
 40 1.146813   172.20.78.35     39.156.66.18     ICMP       70 Echo (ping) request  id=0x0001, seq=19/4864, ttl=9 (no response found!)

> Frame 8: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
v Internet Protocol Version 4, Src: 172.20.78.35, Dst: 39.156.66.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x6f4a (28490)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
```



```
    28 0.995953      172.20.78.35       39.156.66.18        ICMP       70 Echo (ping) request  id=0x0001, seq=16/4096, ttl=6 (no respon
> Frame 8: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
v Internet Protocol Version 4, Src: 172.20.78.35, Dst: 39.156.66.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x6f4a (28490)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.20.78.35
    Destination Address: 39.156.66.18
> Internet Control Message Protocol
```

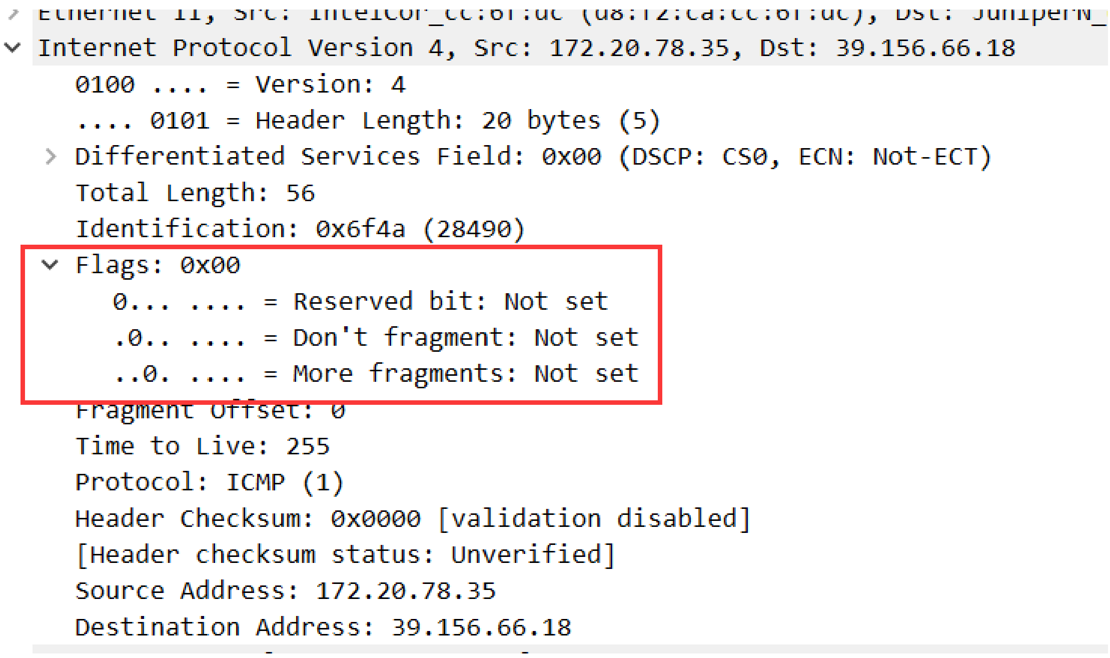
思考题：

(1).我的主机IP地址为172.20.78.35。

(2).对主机第一个发送的ICMP报文进行查看，IP数据包头中，上层协议为ICMP（1）。

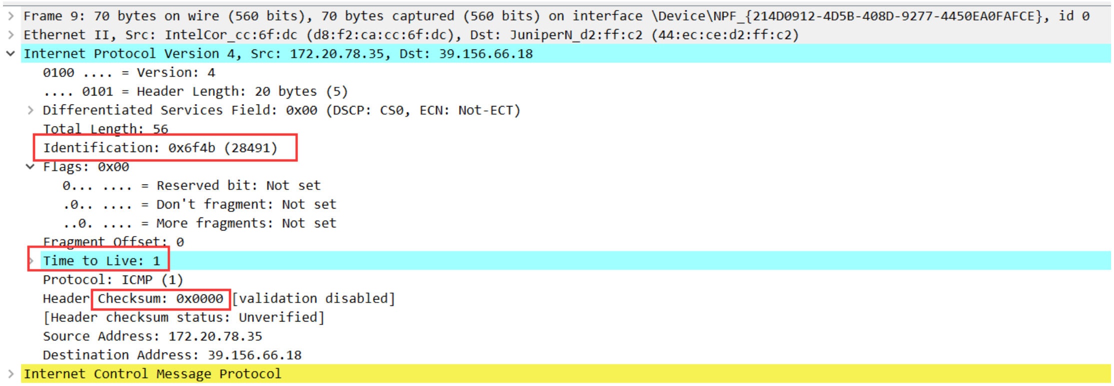
(3).IP头为20字节，该IP数据包的净载为36字节（IP数据包总大小为56字节，头部有20字节，所以净载为56-20=36字节）。

(4).没有分片。通过观察flag区域可以推断得出。可以看到没有其余的帧且帧的偏移为0，MF=0，则说明该IP数据包没有分片。

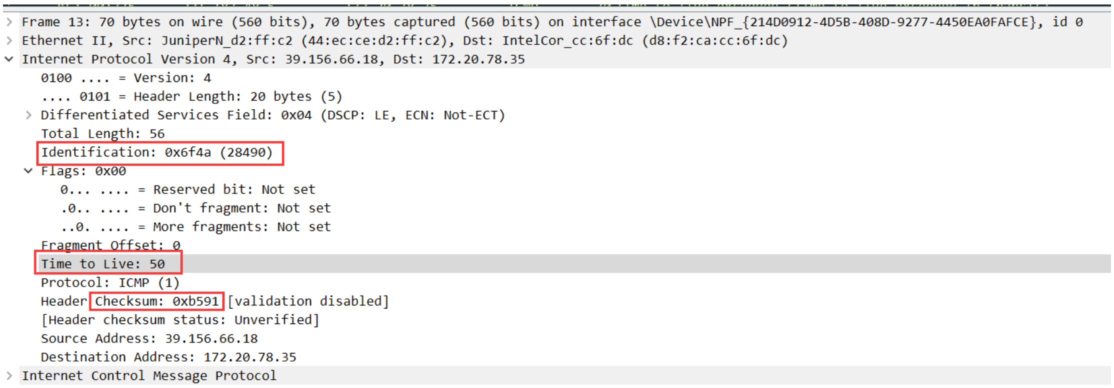


```
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_
v Internet Protocol Version 4, Src: 172.20.78.35, Dst: 39.156.66.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x6f4a (28490)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.20.78.35
    Destination Address: 39.156.66.18
```

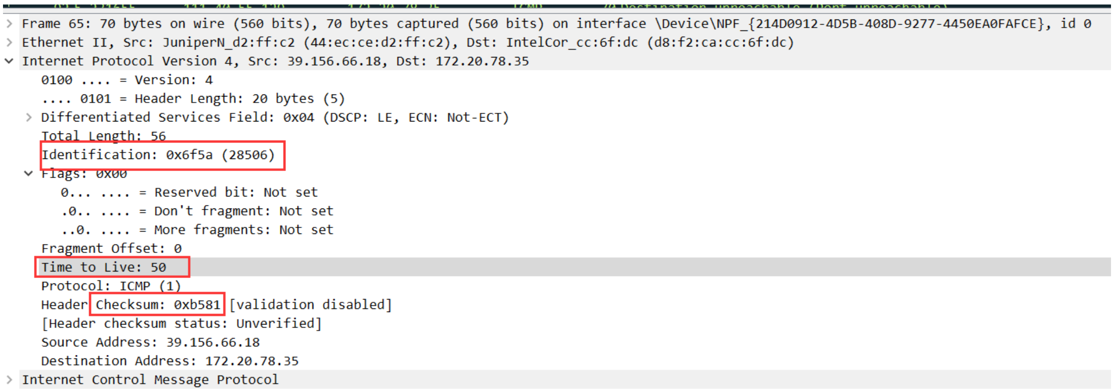
(5).通过比较几个分组可以发现，这些IP数据包的Identification、TTL和checknum字段总是发生改变。



```
> Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
v Internet Protocol Version 4, Src: 172.20.78.35, Dst: 39.156.66.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x6f4b (28491)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.20.78.35
    Destination Address: 39.156.66.18
> Internet Control Message Protocol
```



```
> Frame 13: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2), Dst: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc)
v Internet Protocol Version 4, Src: 39.156.66.18, Dst: 172.20.78.35
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x04 (DSCP: LE, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x6f4a (28490)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 50
    Protocol: ICMP (1)
    Header Checksum: 0xb591 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 39.156.66.18
    Destination Address: 172.20.78.35
> Internet Control Message Protocol
```

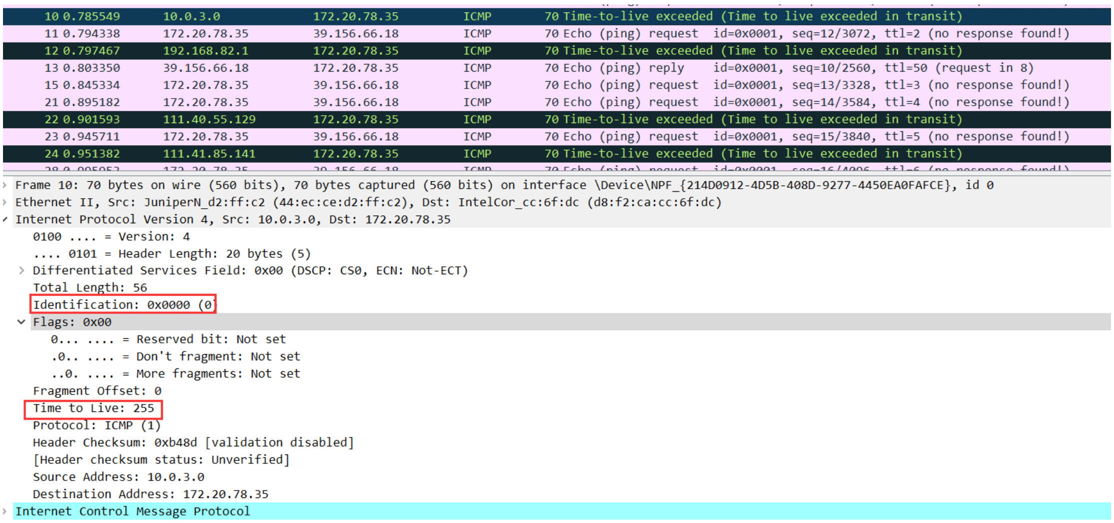


```
> Frame 65: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2), Dst: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc)
v Internet Protocol Version 4, Src: 39.156.66.18, Dst: 172.20.78.35
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x04 (DSCP: LE, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x6f5a (28506)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 50
    Protocol: ICMP (1)
    Header Checksum: 0xb581 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 39.156.66.18
    Destination Address: 172.20.78.35
> Internet Control Message Protocol
```

(6).保持常量的字段有：版本号、上层协议、源IP地址和目的IP地址。因为要使该数据包成功发送到目的地址，这些字段必须保持该值。必须改变的字段有：Identification，TTL，checknum。Identification是IP数据包的序号，每个包的序号都不同。且根据traceroute的工作原理，每次主机发送的IP数据包的TTL都加一。校验和为头部数据求和得出，这两者的变化都会使校验和发生改变。

(7).Idenfification字段由两个字节组成，每次加1。

(8).找到最近的路由器返回给主机的ICMP Time-to-lice exceeded消息。查看该报文如下：

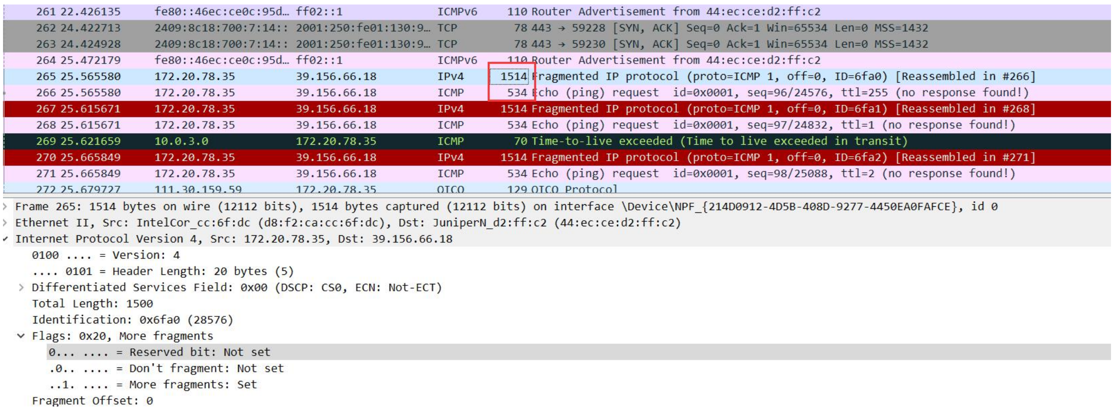


```
10 0.785549   10.0.3.0       172.20.78.35   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
11 0.794338   172.20.78.35   39.156.66.18   ICMP   70 Echo (ping) request  id=0x0001, seq=12/3072, ttl=2 (no response found!)
12 0.797467   192.168.82.1   172.20.78.35   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
13 0.803350   39.156.66.18   172.20.78.35   ICMP   70 Echo (ping) reply    id=0x0001, seq=10/2560, ttl=50 (request in 8)
15 0.845334   172.20.78.35   39.156.66.18   ICMP   70 Echo (ping) request  id=0x0001, seq=13/3328, ttl=3 (no response found!)
21 0.895182   172.20.78.35   39.156.66.18   ICMP   70 Echo (ping) request  id=0x0001, seq=14/3584, ttl=4 (no response found!)
22 0.901593   111.40.55.129  172.20.78.35   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)
23 0.945711   172.20.78.35   39.156.66.18   ICMP   70 Echo (ping) request  id=0x0001, seq=15/3840, ttl=5 (no response found!)
24 0.951382   111.41.85.141  172.20.78.35   ICMP   70 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 10: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2), Dst: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc)
✓ Internet Protocol Version 4, Src: 10.0.3.0, Dst: 172.20.78.35
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x0000 (0)
  ˅ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0xb48d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.3.0
    Destination Address: 172.20.78.35
> Internet Control Message Protocol
```

Identification字段为0x0000，TTL字段为255。

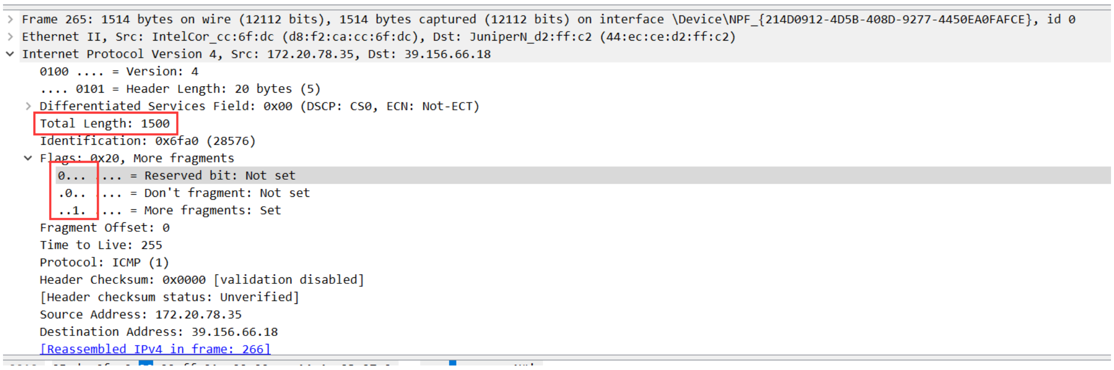
(9). Identification会改变，TTL不变。因为在同一跳，Identification用于区分不同的IP数据包，TTL字段相同。

(10). 可以发现包大小改为2000字节后我的主机发送的第一个ICMP Echo Request消息被分成了两片，分别为1514字节和534字节。



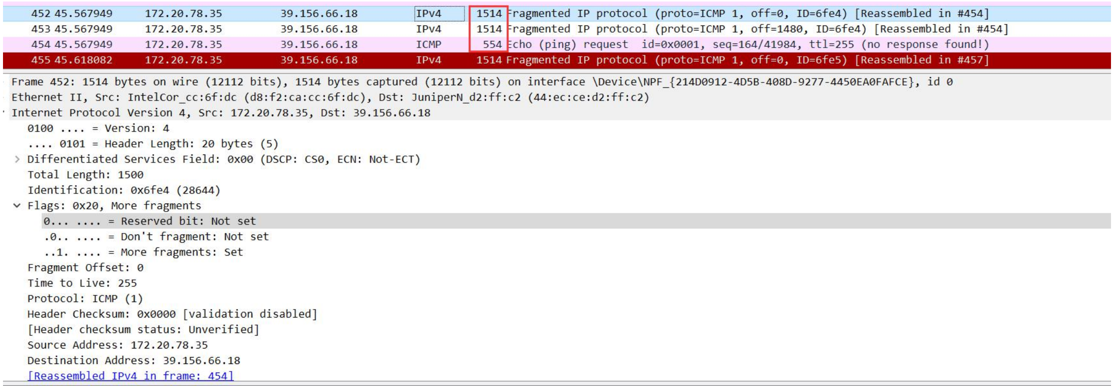
```
261 22.426135  fe80::46ec:ce0c:95d…  ff02::1               ICMPv6  110 Router Advertisement from 44:ec:ce:d2:ff:c2
262 24.422713  2409:8c18:700:7:14::  2001:250:fe01:130:9…  TCP      78 443 → 59228 [SYN, ACK] Seq=0 Ack=1 Win=65534 Len=0 MSS=1432
263 24.424928  2409:8c18:700:7:14::  2001:250:fe01:130:9…  TCP      78 443 → 59230 [SYN, ACK] Seq=0 Ack=1 Win=65534 Len=0 MSS=1432
264 25.472179  fe80::46ec:ce0c:95d…  ff02::1               ICMPv6  110 Router Advertisement from 44:ec:ce:d2:ff:c2
265 25.565580  172.20.78.35          39.156.66.18          IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6fa0) [Reassembled in #266]
266 25.565580  172.20.78.35          39.156.66.18          ICMP    534 Echo (ping) request  id=0x0001, seq=96/24576, ttl=255 (no response found!)
267 25.615671  172.20.78.35          39.156.66.18          IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6fa1) [Reassembled in #268]
268 25.615671  172.20.78.35          39.156.66.18          ICMP    534 Echo (ping) request  id=0x0001, seq=97/24832, ttl=1 (no response found!)
269 25.621659  10.0.3.0              172.20.78.35          ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
270 25.665849  172.20.78.35          39.156.66.18          IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6fa2) [Reassembled in #271]
271 25.665849  172.20.78.35          39.156.66.18          ICMP    534 Echo (ping) request  id=0x0001, seq=98/25088, ttl=2 (no response found!)
272 25.679727  111.30.159.59         172.20.78.35          OICQ    129 OICQ Protocol

> Frame 265: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
✓ Internet Protocol Version 4, Src: 172.20.78.35, Dst: 39.156.66.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x6fa0 (28576)
  ˅ Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment Offset: 0
```

(11). 观察第一个报文段，此时DF=0，MF=1，说明了该数据包进行了分片，并且不是最后一个分片。并且该数据包的片偏移为0，说明该包是第一个数据包。该分片的长度为1500字节



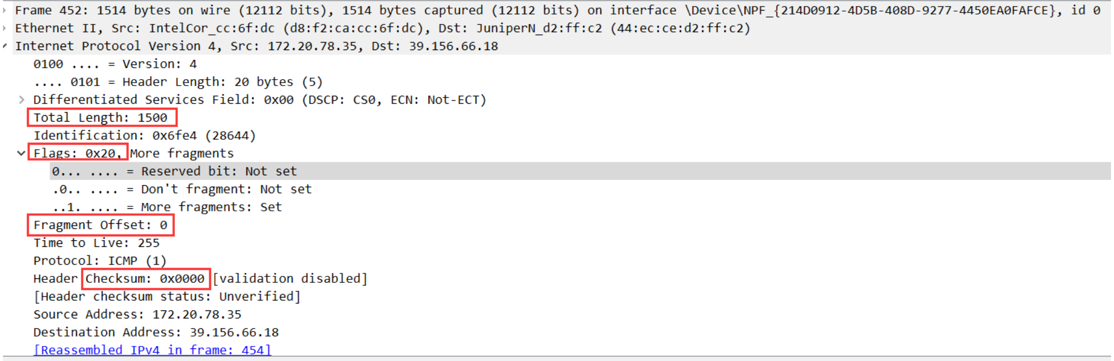
```
> Frame 265: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
˅ Internet Protocol Version 4, Src: 172.20.78.35, Dst: 39.156.66.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x6fa0 (28576)
  ˅ Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.20.78.35
    Destination Address: 39.156.66.18
    [Reassembled IPv4 in frame: 266]
```

(12). 从下图中可以看到将包大小改为3500字节后，第一个ICMP Echo Request消息被分成了三片，分别为1514字节，1514字节和534字节。

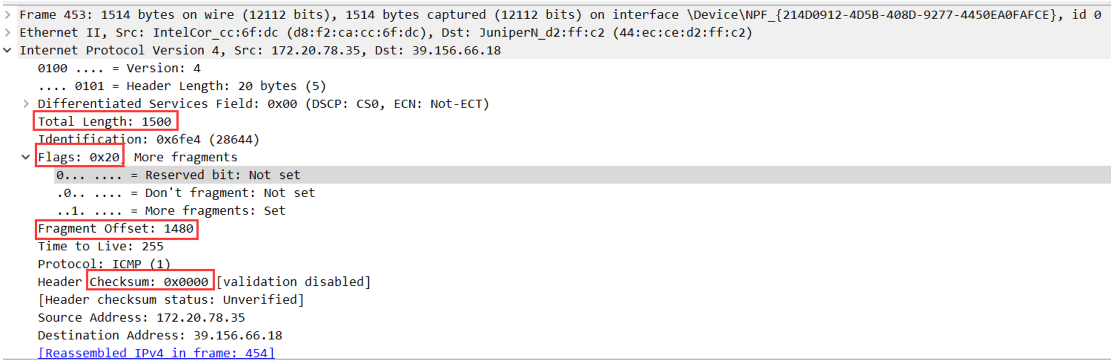


```
452 45.567949   172.20.78.35   39.156.66.18   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6fe4) [Reassembled in #454]
453 45.567949   172.20.78.35   39.156.66.18   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=6fe4) [Reassembled in #454]
454 45.567949   172.20.78.35   39.156.66.18   ICMP    554 Echo (ping) request  id=0x0001, seq=164/41984, ttl=255 (no response found!)
455 45.618082   172.20.78.35   39.156.66.18   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6fe5) [Reassembled in #457]
Frame 452: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
Internet Protocol Version 4, Src: 172.20.78.35, Dst: 39.156.66.18
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 1500
  Identification: 0x6fe4 (28644)
v Flags: 0x20, More fragments
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
  Fragment Offset: 0
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.20.78.35
  Destination Address: 39.156.66.18
  [Reassembled IPv4 in frame: 454]
```

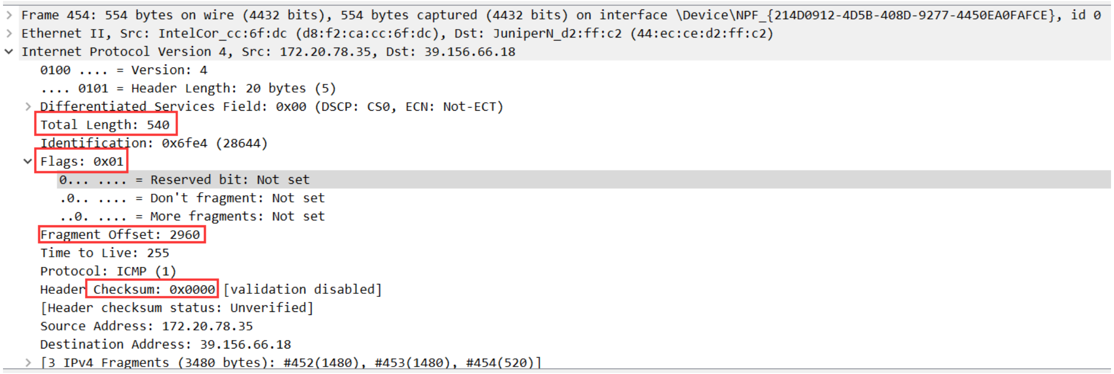
(13). 这三个IP分片的数据头部Total length，片偏移量，标志位，checksum字段发生了变化。如下图所示。



```
> Frame 452: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
v Internet Protocol Version 4, Src: 172.20.78.35, Dst: 39.156.66.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x6fe4 (28644)
  v Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.20.78.35
    Destination Address: 39.156.66.18
    [Reassembled IPv4 in frame: 454]
```

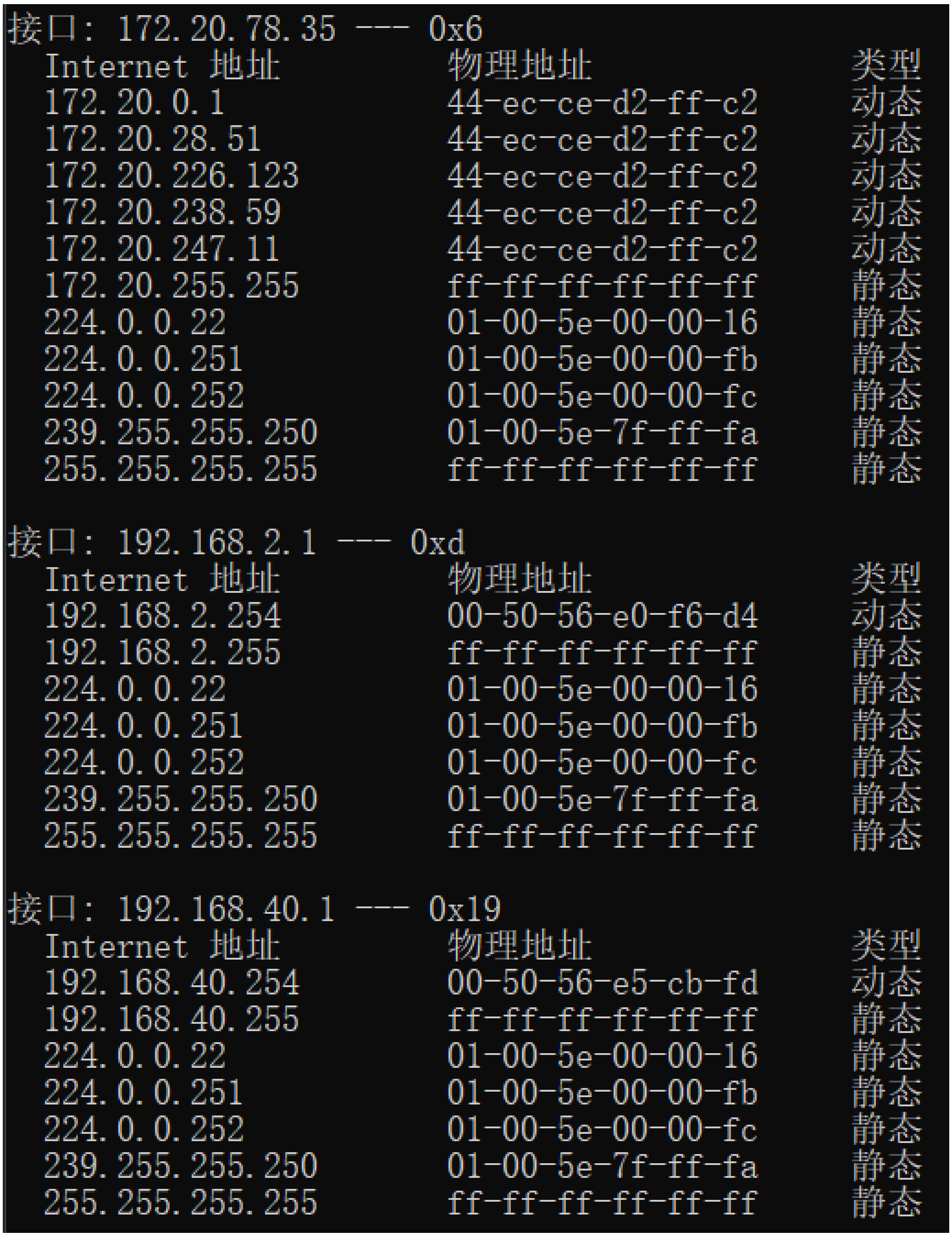


```
> Frame 453: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
v Internet Protocol Version 4, Src: 172.20.78.35, Dst: 39.156.66.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x6fe4 (28644)
  v Flags: 0x20  More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment Offset: 1480
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.20.78.35
    Destination Address: 39.156.66.18
    [Reassembled IPv4 in frame: 454]
```



```
> Frame 454: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
v Internet Protocol Version 4, Src: 172.20.78.35, Dst: 39.156.66.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 540
    Identification: 0x6fe4 (28644)
  v Flags: 0x01
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 2960
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.20.78.35
    Destination Address: 39.156.66.18
  > [3 IPv4 Fragments (3480 bytes): #452(1480), #453(1480), #454(520)]
```

5. 抓取ARP数据包

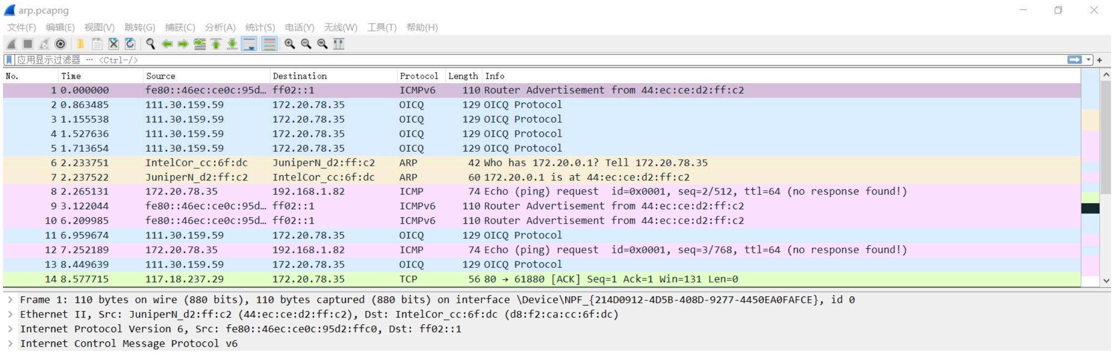


```
接口: 172.20.78.35 --- 0x6
  Internet 地址         物理地址              类型
  172.20.0.1            44-ec-ce-d2-ff-c2     动态
  172.20.28.51          44-ec-ce-d2-ff-c2     动态
  172.20.226.123        44-ec-ce-d2-ff-c2     动态
  172.20.238.59         44-ec-ce-d2-ff-c2     动态
  172.20.247.11         44-ec-ce-d2-ff-c2     动态
  172.20.255.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 192.168.2.1 --- 0xd
  Internet 地址         物理地址              类型
  192.168.2.254         00-50-56-e0-f6-d4     动态
  192.168.2.255         ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 192.168.40.1 --- 0x19
  Internet 地址         物理地址              类型
  192.168.40.254        00-50-56-e5-cb-fd     动态
  192.168.40.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

思考题：

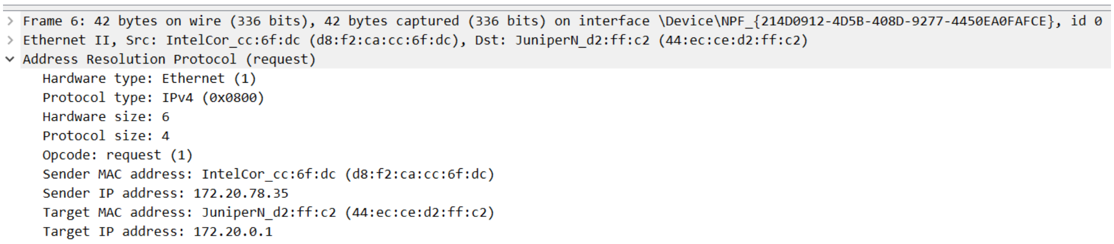
(1).ARP缓存中第一列为借口的IP地址，第二列为借口的MAC地址，第三列为地址的类型，包括静态和动态。

(2).清除主机ARP缓存的内容，抓取ping命令时的数据包，如下图：


arp.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.   Time        Source                   Destination        Protocol  Length Info
    1 0.000000    fe80::46ec:ce0c:95d…     ff02::1            ICMPv6     110 Router Advertisement from 44:ec:ce:d2:ff:c2
    2 0.863485    111.30.159.59            172.20.78.35       OICQ       129 OICQ Protocol
    3 1.155538    111.30.159.59            172.20.78.35       OICQ       129 OICQ Protocol
    4 1.527636    111.30.159.59            172.20.78.35       OICQ       129 OICQ Protocol
    5 1.713654    111.30.159.59            172.20.78.35       OICQ       129 OICQ Protocol
    6 2.233751    IntelCor_cc:6f:dc        JuniperN_d2:ff:c2  ARP         42 Who has 172.20.0.1? Tell 172.20.78.35
    7 2.237522    JuniperN_d2:ff:c2        IntelCor_cc:6f:dc  ARP         60 172.20.0.1 is at 44:ec:ce:d2:ff:c2
    8 2.265131    172.20.78.35             192.168.1.82       ICMP        74 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (no response found!)
    9 3.122044    fe80::46ec:ce0c:95d…     ff02::1            ICMPv6     110 Router Advertisement from 44:ec:ce:d2:ff:c2
   10 6.209985    fe80::46ec:ce0c:95d…     ff02::1            ICMPv6     110 Router Advertisement from 44:ec:ce:d2:ff:c2
   11 6.959674    111.30.159.59            172.20.78.35       OICQ       129 OICQ Protocol
   12 7.252189    172.20.78.35             192.168.1.82       ICMP        74 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (no response found!)
   13 8.449639    111.30.159.59            172.20.78.35       OICQ       129 OICQ Protocol
   14 8.577715    117.18.237.29            172.20.78.35       TCP         56 80 → 61880 [ACK] Seq=1 Ack=1 Win=131 Len=0

> Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2), Dst: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc)
> Internet Protocol Version 6, Src: fe80::46ec:ce0c:95d2:ffc0, Dst: ff02::1
> Internet Control Message Protocol v6
```

数据包格式如下：



```
> Frame 6: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc)
    Sender IP address: 172.20.78.35
    Target MAC address: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
    Target IP address: 172.20.0.1
```

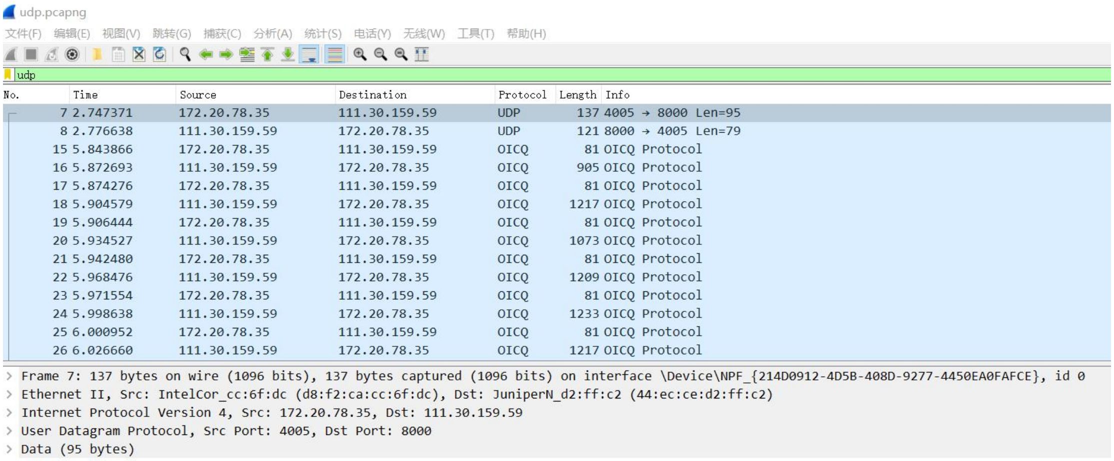
构成部分有：
硬件类型：2字节
协议类型：2字节
硬件地址长度：6字节
协议长度：4字节
操作类型：用来表示这个报文的类型，ARP请求为1，2字节
发送方MAC地址：6字节
发送方IP地址：4字节
目标MAC地址：6字节
目标IP地址：4字节。

(3).可以根据操作类型字段判断。若为1则为请求包，若为2则为应答包。

(4).因为查询MAC时主机不知道目的IP的MAC地址是多少，所以需要在局域网中广播查询。而ARP响应只需要发给提出查询的主机即可，所以ARP查询需要在广播帧中传送，而ARP响应要在一个有明确目的局域网地址的帧中传送。

6. 抓取UDP数据包

启动wireshark开始分组捕获，发送QQ消息，停止捕获。筛选中UDP数据包如下。


udp.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
udp

```
No.      Time        Source          Destination     Protocol  Length Info
      7 2.747371     172.20.78.35    111.30.159.59   UDP          137 4005 → 8000 Len=95
      8 2.776638     111.30.159.59   172.20.78.35    UDP          121 8000 → 4005 Len=79
     15 5.843866     172.20.78.35    111.30.159.59   OICQ          81 OICQ Protocol
     16 5.872693     111.30.159.59   172.20.78.35    OICQ         905 OICQ Protocol
     17 5.874276     172.20.78.35    111.30.159.59   OICQ          81 OICQ Protocol
     18 5.904579     111.30.159.59   172.20.78.35    OICQ        1217 OICQ Protocol
     19 5.906444     172.20.78.35    111.30.159.59   OICQ          81 OICQ Protocol
     20 5.934527     111.30.159.59   172.20.78.35    OICQ        1073 OICQ Protocol
     21 5.942480     172.20.78.35    111.30.159.59   OICQ          81 OICQ Protocol
     22 5.968476     111.30.159.59   172.20.78.35    OICQ        1209 OICQ Protocol
     23 5.971554     172.20.78.35    111.30.159.59   OICQ          81 OICQ Protocol
     24 5.998638     111.30.159.59   172.20.78.35    OICQ        1233 OICQ Protocol
     25 6.000952     172.20.78.35    111.30.159.59   OICQ          81 OICQ Protocol
     26 6.026660     111.30.159.59   172.20.78.35    OICQ        1217 OICQ Protocol

> Frame 7: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
> Internet Protocol Version 4, Src: 172.20.78.35, Dst: 111.30.159.59
> User Datagram Protocol, Src Port: 4005, Dst Port: 8000
> Data (95 bytes)
```

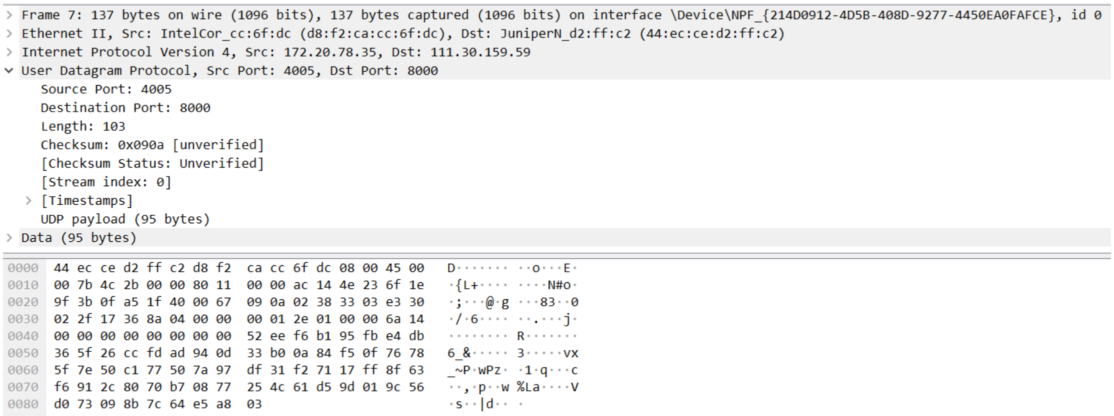
思考题：

(1).消息是基于UDP的。

(2).主机IP地址：172.20.78.35，目的主机的IP地址为111.30.159.59。

(3).主机发送QQ消息的端口号为4005，QQ服务器的端口号为8000。

(4).数据包格式如下。



```
> Frame 7: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
> Internet Protocol Version 4, Src: 172.20.78.35, Dst: 111.30.159.59
v User Datagram Protocol, Src Port: 4005, Dst Port: 8000
    Source Port: 4005
    Destination Port: 8000
    Length: 103
    Checksum: 0x090a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (95 bytes)
> Data (95 bytes)

0000  44 ec ce d2 ff c2 d8 f2  ca cc 6f dc 08 00 45 00   D·······  ··o···E·
0010  00 7b 4c 2b 00 00 80 11  00 00 ac 14 4e 23 6f 1e   ·{L+····  ····N#o·
0020  9f 3b 0f a5 1f 40 00 67  09 0a 02 38 33 03 e3 30   ·;···@·g  ···83··0
0030  02 2f 17 36 8a 04 00 00  00 01 2e 01 00 00 6a 14   ·/·6····  ··.···j·
0040  00 00 00 00 00 00 00 00  52 ee f6 b1 95 fb e4 db   ········  R·······
0050  36 5f 26 cc fd ad 94 0d  33 b0 0a 84 f5 0f 76 78   6_&·····  3·····vx
0060  5f 7e 50 c1 77 50 7a 97  df 31 f2 71 17 ff 8f 63   _~P·wPz·  ·1·q···c
0070  f6 91 2c 80 70 b7 08 77  25 4c 61 d5 9d 01 9c 56   ··,·p··w  %La····V
0080  d0 73 09 8b 7c 64 e5 a8  03                        ·s··|d··  ·
```

字段有：

源端口号：2字节

目的端口号：2字节

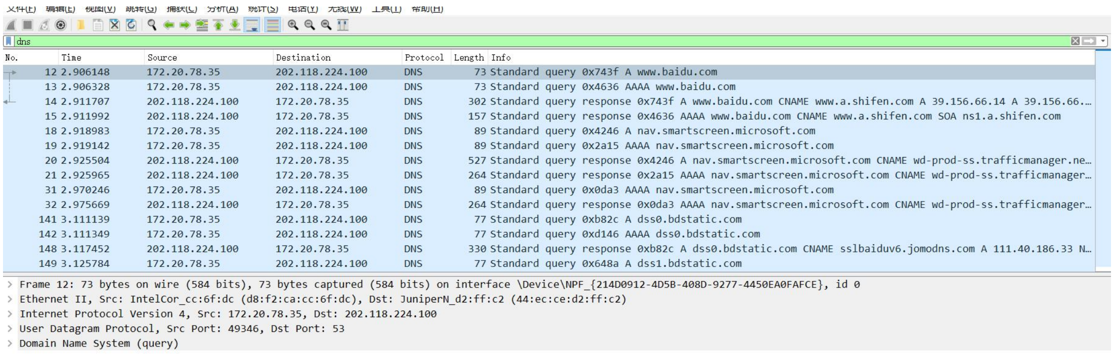
报文长度：2字节

校验和：2字节

(5).由于UDP是不可靠数据传输，所以每次发送一个ICQ数据包后服务器都会返回一个ICQ数据包进行确认。和TCP相比，UDP在发送数据之前没有握手，这里能够推断出UDP是无连接的。

7. 利用wireshark进行DNS协议分析

访问www.baidu.com的抓包结果如下。

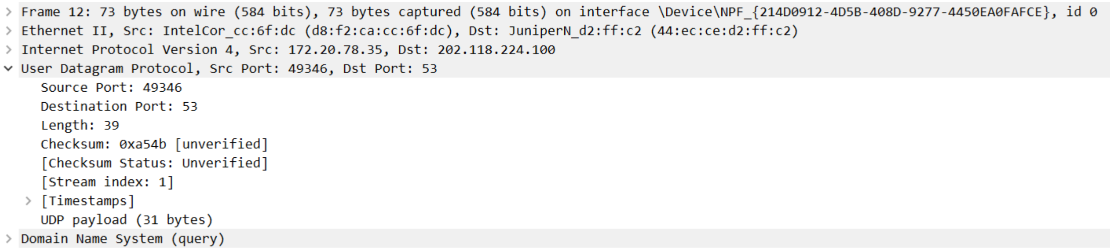

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

dns

```
No.   Time      Source          Destination     Protocol Length Info
   12 2.906148  172.20.78.35    202.118.224.100 DNS       73 Standard query 0x743f A www.baidu.com
   13 2.906328  172.20.78.35    202.118.224.100 DNS       73 Standard query 0x4636 AAAA www.baidu.com
   14 2.911707  202.118.224.100 172.20.78.35    DNS      302 Standard query response 0x743f A www.baidu.com CNAME www.a.shifen.com A 39.156.66.14 A 39.156.66.…
   15 2.911992  202.118.224.100 172.20.78.35    DNS      157 Standard query response 0x4636 AAAA www.baidu.com CNAME www.a.shifen.com SOA ns1.a.shifen.com
   18 2.918983  172.20.78.35    202.118.224.100 DNS       89 Standard query 0x4246 A nav.smartscreen.microsoft.com
   19 2.919142  172.20.78.35    202.118.224.100 DNS       89 Standard query 0x2a15 AAAA nav.smartscreen.microsoft.com
   20 2.925504  202.118.224.100 172.20.78.35    DNS      527 Standard query response 0x4246 A nav.smartscreen.microsoft.com CNAME wd-prod-ss.trafficmanager.ne…
   21 2.925965  202.118.224.100 172.20.78.35    DNS      264 Standard query response 0x2a15 AAAA nav.smartscreen.microsoft.com CNAME wd-prod-ss.trafficmanager…
   31 2.970246  172.20.78.35    202.118.224.100 DNS       89 Standard query 0x0da3 AAAA nav.smartscreen.microsoft.com
   32 2.975669  202.118.224.100 172.20.78.35    DNS      264 Standard query response 0x0da3 AAAA nav.smartscreen.microsoft.com CNAME wd-prod-ss.trafficmanager…
  141 3.111139  172.20.78.35    202.118.224.100 DNS       77 Standard query 0xb82c A dss0.bdstatic.com
  142 3.111349  172.20.78.35    202.118.224.100 DNS       77 Standard query 0xd146 AAAA dss0.bdstatic.com
  148 3.117452  202.118.224.100 172.20.78.35    DNS      330 Standard query response 0xb82c A dss0.bdstatic.com CNAME sslbaiduv6.jomodns.com A 111.40.186.33 N…
  149 3.125784  172.20.78.35    202.118.224.100 DNS       77 Standard query 0x648a A dss1.bdstatic.com
```

```
> Frame 12: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
> Internet Protocol Version 4, Src: 172.20.78.35, Dst: 202.118.224.100
> User Datagram Protocol, Src Port: 49346, Dst Port: 53
> Domain Name System (query)
```

数据包格式如下：



```
> Frame 12: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{214D0912-4D5B-408D-9277-4450EA0FAFCE}, id 0
> Ethernet II, Src: IntelCor_cc:6f:dc (d8:f2:ca:cc:6f:dc), Dst: JuniperN_d2:ff:c2 (44:ec:ce:d2:ff:c2)
> Internet Protocol Version 4, Src: 172.20.78.35, Dst: 202.118.224.100
v User Datagram Protocol, Src Port: 49346, Dst Port: 53
    Source Port: 49346
    Destination Port: 53
    Length: 39
    Checksum: 0xa54b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (31 bytes)
> Domain Name System (query)
```

问题讨论：

在实验结果中已经进行了论述。

心得体会：

1. 学会了使用wireshark进行抓包的操作
2. 通过使用软件进行协议的分析，加深了对各种协议以及数据包格式的理解。