# **Wireshark实验**

# **学号：17363092 姓名：叶茂青**

1. **实验目的**

熟悉并掌握 Wireshark 的基本使用；了解网络协议实体间进行交互以及报文交换的情况；学会使用 Wireshark 分析 IP、ICMP 以及 TCP 协议。

1. **预备知识**

要深入理解网络协议，需要观察它们的工作过程并使用它们，即观察两个协议实体之间交换的报文序列，探究协议操作的细节，使协议实体执行某些动作，观察这些动作及其影响。这种观察可以在仿真环境下或在因特网这样的真实网络环境中完成。观察正在运行的协议实体间交换报文的基本工具被称为分组嗅探器（packet sniffer），又称分组捕获器。顾名思义，分组嗅探器捕获（嗅探）你的计算机发送和接收的报文。图 1 显示了一个分组嗅探器的结构。

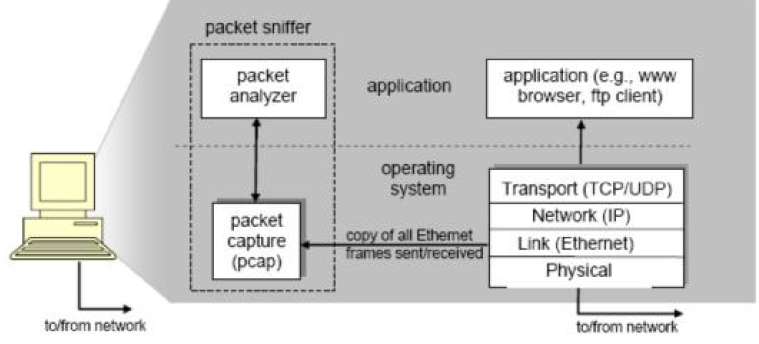


图 1 分组嗅探器结构

图 1 右边是计算机上正常运行的协议和应用程序（如：Web 浏览器和 FTP 客户端）。分组嗅探器（虚线框中的部分）主要有两部分组成：第一是分组捕获器，其功能是捕获计算机发送和接收的每一个链路层帧的拷贝；第二个组成部分是分组分析器，其作用是分析并显示协议报文所有字段的内容（它能识别目前使用的各种网络协议）。

运行 Wireshark 程序时，其图形用户界面如图 2 所示。最初，各窗口中并无数据显示。Wireshark 的界面主要有五个组成部分：

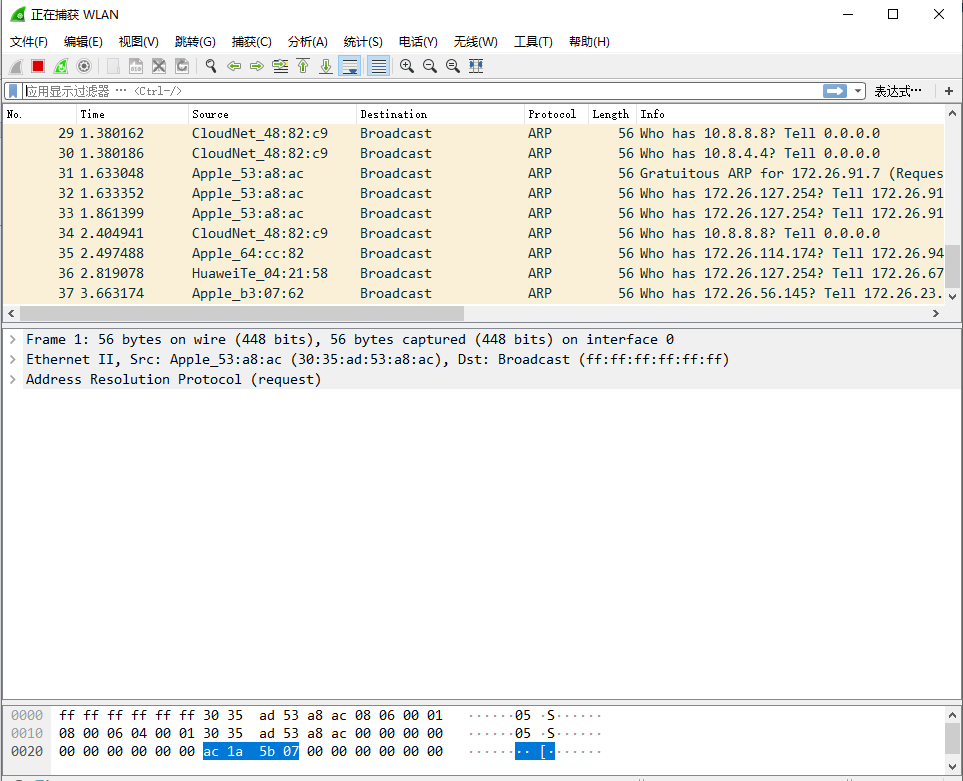
****

图 2 Wireshark 的界面

* + 命令菜单（command menus）：命令菜单位于窗口的最顶部，是标准的下拉式菜单。
  + 协议筛选框（display filter specification ）：在该处填写某种协议的名称，Wireshark 据此对分组列表窗口中的分组进行过滤，只显示你需要的分组。
  + 捕获分组列表（listing of captured packets）：按行显示已被捕获的分组内容，其中包括：分组序号、捕获时间、源地址和目的地址、协议类型、协议信息说明。单击某一列的列名，可以使分组列表按指定列排序。其中，协议类型是发送或接收分组的最高层协议的类型。
  + 分组首部明细（details of selected packet header ）：显示捕获分组列表窗口中被选中分组的首部详细信息。包括该分组的各个层次的首部信息，需要查看哪层信息，双击对应层次或单击该层最前面的“>”即可。
  + 分组内容窗口（packet content ）：分别以十六进制（左）和 ASCII 码（右）两种格式显示被捕获帧的完整内容。

1. **实验内容**
   1. **任务一：分析以太网帧**

IP 地址用于标识因特网上每台主机，而端口号则用于区别在同一台主机上运行的不同网络应用程序。在链路层，有介质访问控制（Media Access Control,MAC）地址。在局域网中，每个网络设备必须有唯一的 MAC 地址。设备监听共享通信介质以获取目标 MAC 地址与自己相匹配的分组。

Wireshark 能把 MAC 地址的组织标识转化为代表生产商的字符串，例如，00:06:5b:e3:4d:1a 也能以 Dell:e3:4d:1a 显示，因为组织唯一标识符 00:06:5b 属于Dell。地址 ff:ff:ff:ff:ff:ff 是一个特殊的 MAC 地址，意味着数据应该广播到局域网的

所有设备。

发送分组到本地网外的主机，需要跨越一组独立的本地网，这些本地网通过称为网关或路由器的中间机器连接。网关有多个网络接口卡，用它们同时连接多个本地网。最初的发送者或源主机直接通过本地网发送数据到本地网关，网关转发数据报到其它网关，直到最后到达目的主机所在的本地网的网关。

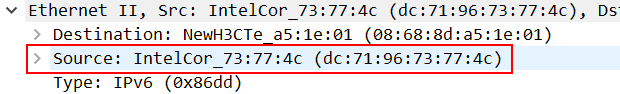
* + 1. 俘获和分析以太网帧

1. 启动Wireshark 分组嗅探器，在过滤显示窗口（filter display window）中输入http，开始Wireshark 分组俘获。
2. 在浏览器地址栏中输入要访问的网址，如www.sysu.edu.cn
3. 停止分组俘获。在俘获分组列表中（listing of captured packets ）中找到 HTTP GET 信息和响应信息，如图 3 所示（替换成你的截图）。

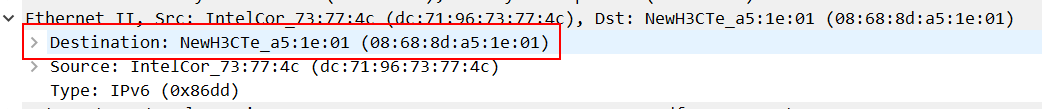
HTTP GET 信息被封装在 TCP 分组中，TCP 分组又被封装在 IP 数据报中，IP 数据报又被封装在以太网帧中）。在分组明细窗口中展开 Ethernet II 信息（packet details window）。

回答下面的问题：

* 1. 你所在的主机 48-bit Ethernet 地址是多少？



* 1. Ethernet 帧中目的地址是多少？这个目的地址是www.sysu.edu.cn 的Ethernet 地址吗？



不是，这只是无线路由器的mac地址

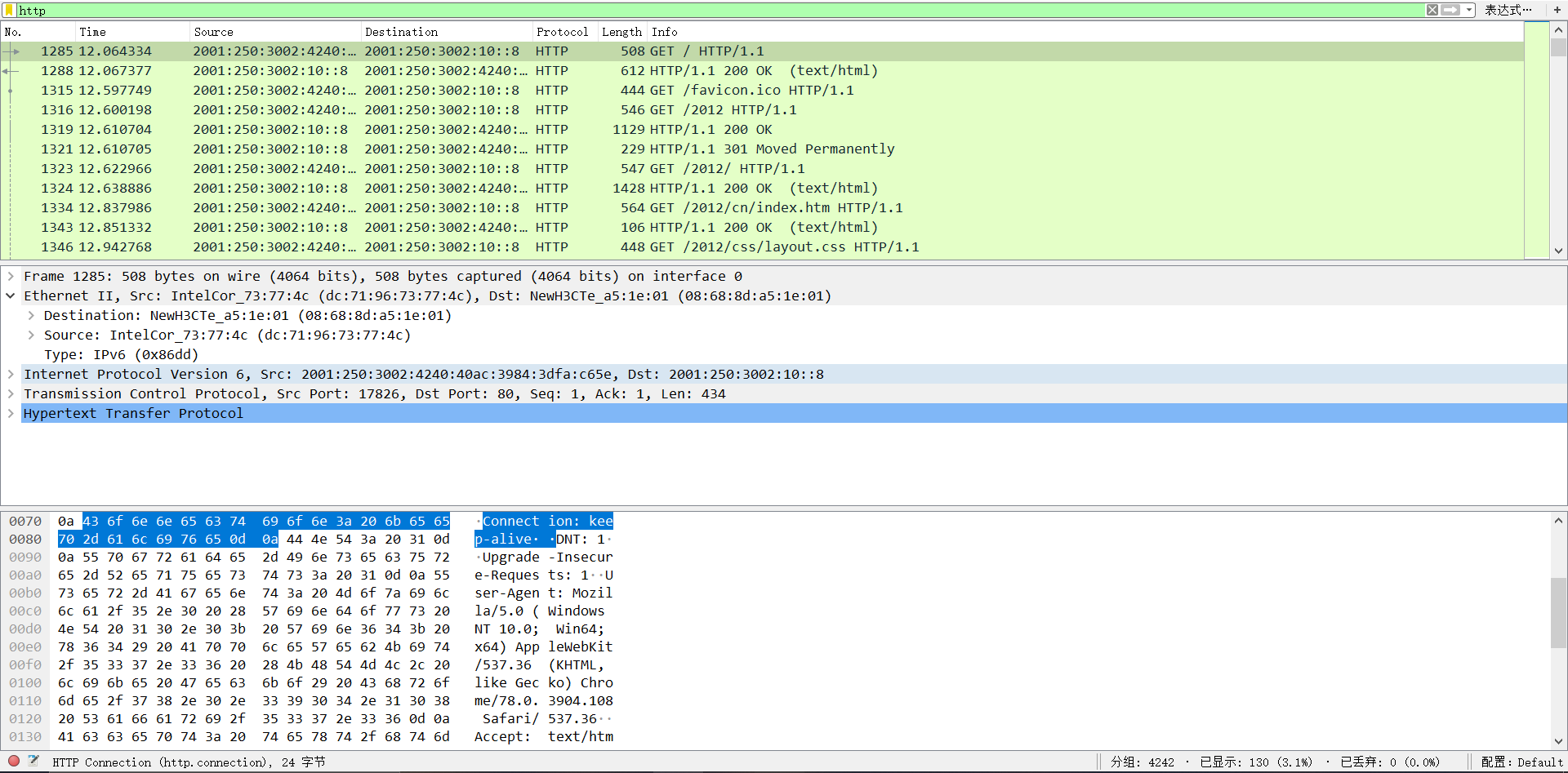


图 3 HTTP GET信息和响应信息

* 1. **任务二：分析 ICMP 协议**

Ping 和 traceroute 命令都依赖于 ICMP。ICMP 可以看作是 IP 协议的伴随协议。

ICMP 报文被封装在 IP 数据报发送。

1. ping 和 ICMP

利用 Ping 程序产生 ICMP 分组。Ping 向因特网中的某个特定主机发送特殊的探测报文并等待表明主机在线的回复。具体做法：

1. 打开 Windows 命令提示符窗口（Windows Command Prompt）。
2. 启动Wireshark 分组嗅探器，在过滤显示窗口（filter display window）中输入icmp，开始Wireshark 分组俘获。
3. 输入“*ping –n 10 ise.sysu.edu.cn*” 。其中*“-n 10*”指明应返回10条ping信息。
4. 当ping程序终止时，停止Wireshark 分组俘获。实验结束后会出现如图 5所示的命令窗口：

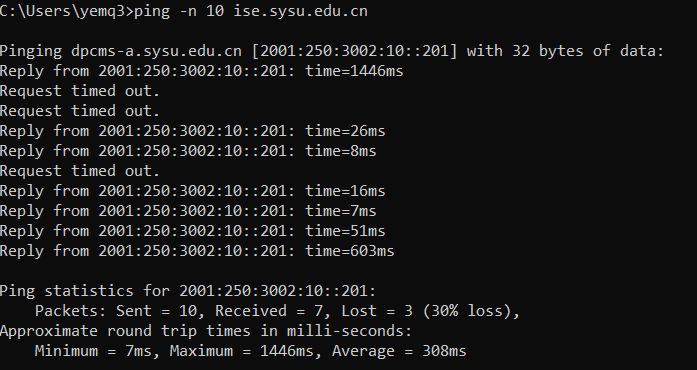


图 4 命令窗口

停止分组俘获后，会出现如图 5所示的界面：

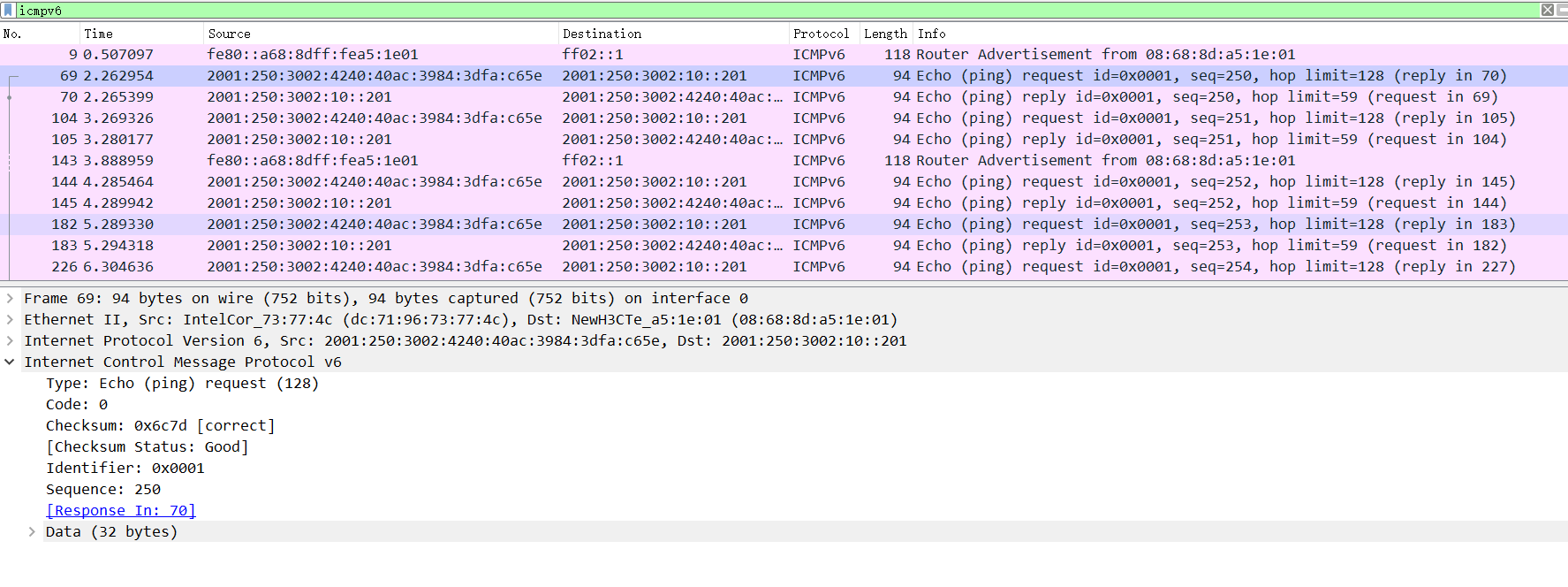


图 5 停止分组俘获后Wireshark的界面

图 6是在分组内容窗口中显示了ICMP协议的详细信息。观察这个ICMP分组， 可以看出，此ICMP分组的Type 1 2 8 and Code 0 即所谓的ICMP “echo request” 分组。

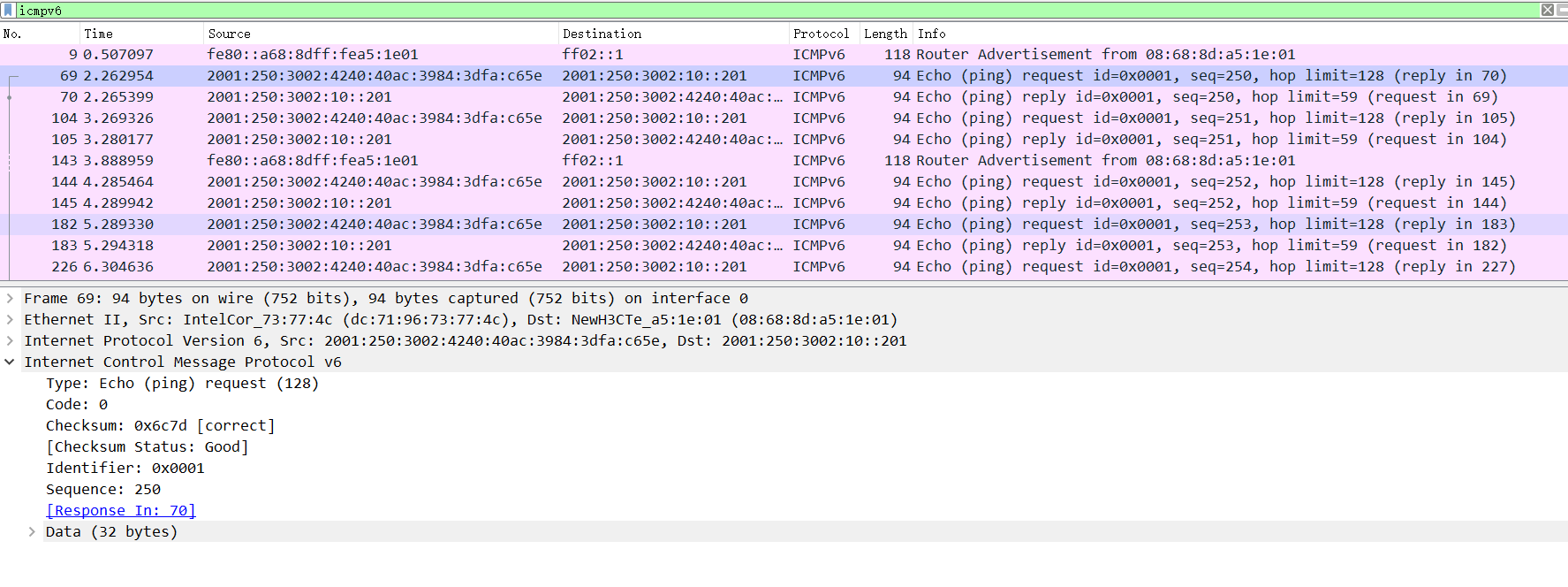
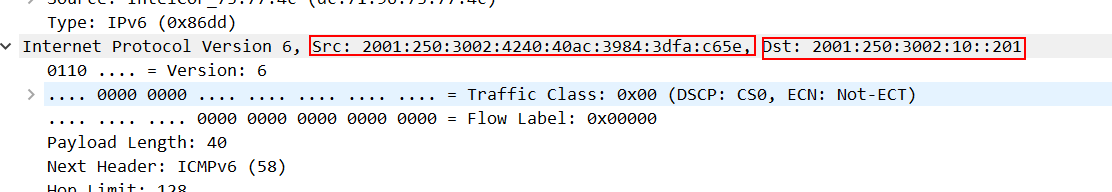


图 6 ICMP协议详细信息

在实验报告中回答下面问题：

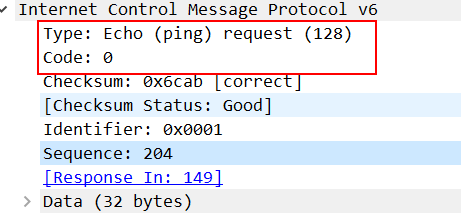
1. 你所在主机的IP地址是多少？目的主机的IP地址是多少？



本机地址： 2001:250:3002:4240:40ac:3984:3dfa:c65e

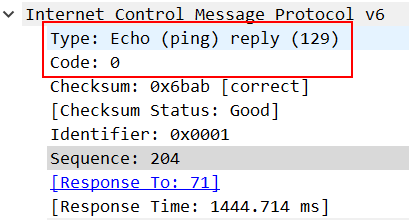
目的主机地址：2001:250:3002:10::201

1. 查看ping请求分组，ICMP的type 和code是多少？



Type:128 Code:0

1. 查看相应得ICMP响应信息，ICMP的type 和code又是多少？



Type:129 Code:0

1. ICMP和Traceroute

在Wireshark 下，用Traceroute程序俘获ICMP分组。Traceroute能够映射出通

往特定的因特网主机途径的所有中间主机。

源端发送一串ICMP分组到目的端。发送的第一个分组时，TTL=1；发送第二个分组时，TTL=2，依次类推。路由器把经过它的每一个分组TTL字段值减1。当一个 分组到达了路由器时的TTL字段为1时，路由器会发送一个ICMP错误分组（ICMP error packet）给源端。

1. 启动Window 命令提示符窗口
2. 启动Wireshark分组嗅探器，开始分组俘获。
3. Tracert命令在c:\windows\system32 下，所以在MS-DOS 命令提示行或者输

入“*tracert ise.sysu.edu.cn* ” or “*c:\windows\system32\tracert hostname* ” (注意在Windows 下, 命令是 “*tracert* ” 而不是“*traceroute*”。)如图 7所示：

1. 当Traceroute 程序终止时，停止分组俘获。

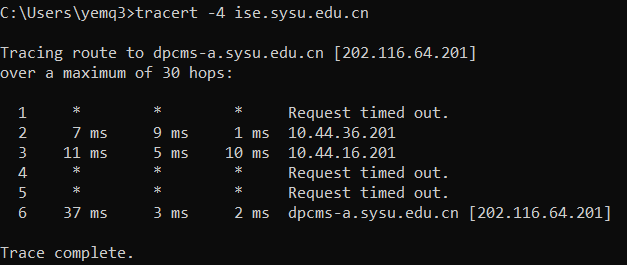


图 7 命令提示窗口显示Traceroute程序结果

图 8显示的是一个路由器返回的ICMP错误分组（ICMP error packet）。

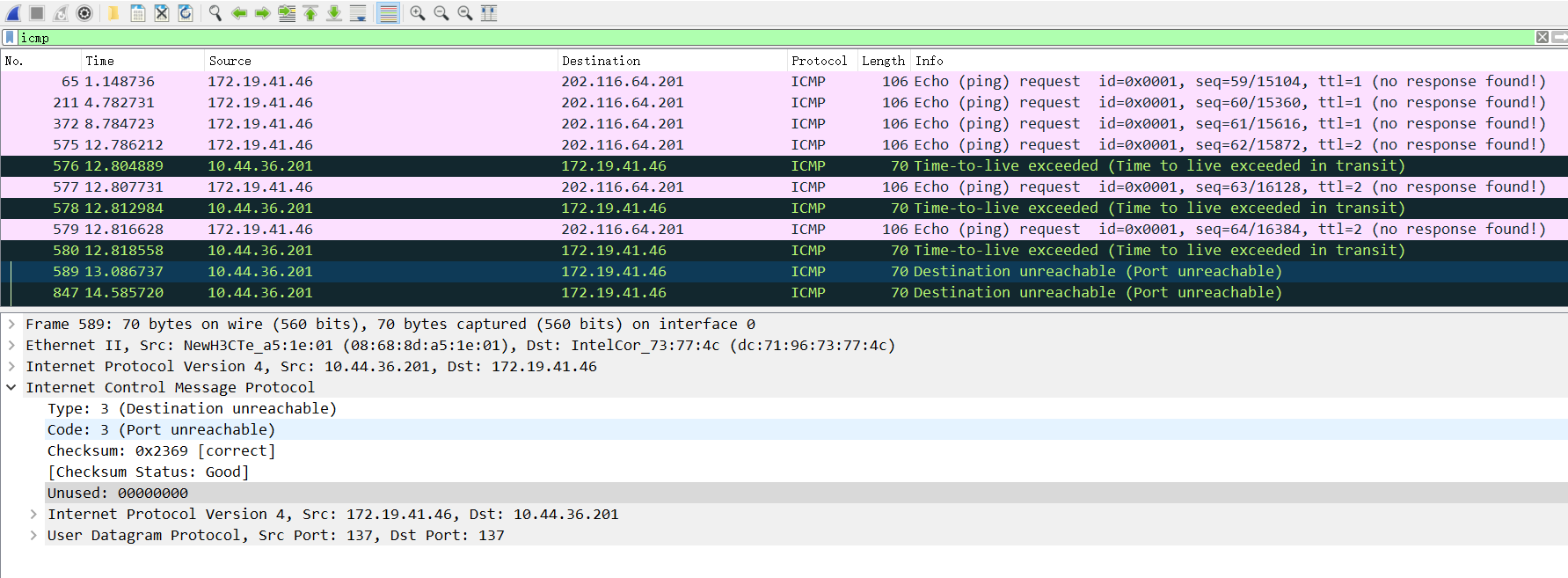


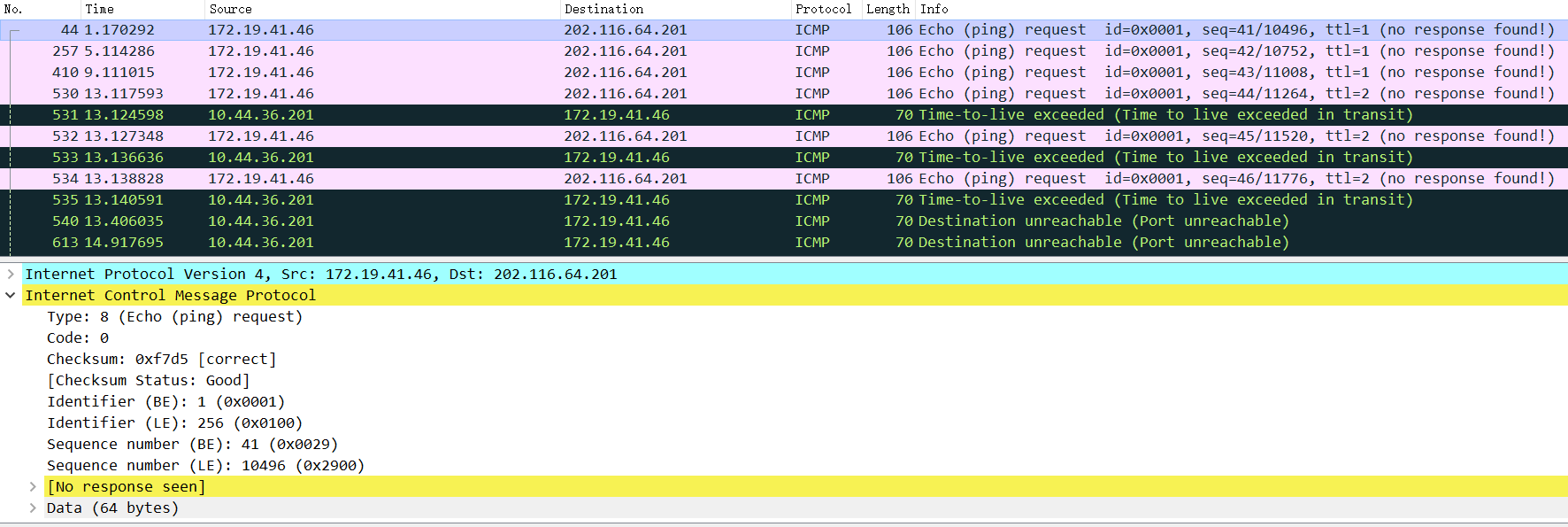
图 8 一个扩展ICMP错误分组信息的Wireshark窗口

在实验报告中回答下面问题：

1. 查看ICMP echo分组，是否这个分组和前面使用 ping命令的ICMP echo一

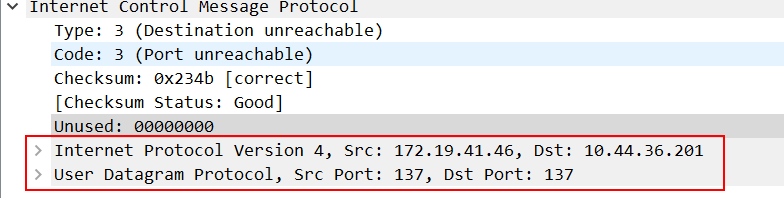
样？

不一样



1. 查看ICMP错误分组，它比ICMP echo 分组包括的信息多。ICMP错误分组比

ICMP echo 分组多包含的信息有哪些？



以上为多包含的内容（User Datagram Protocol在某些错误中不一定有）

* 1. **任务三：分析 TCP 协议**

访问学校主页服务器，通过 Wireshark 捕获通信内容，分析 TCP 连接建立的三

次握手过程。TCP 报文首部格式如图 10 所示：



图 9 TCP报文首部格式

抓取数据包如图 10所示（请将自己的截图替换图 10）：

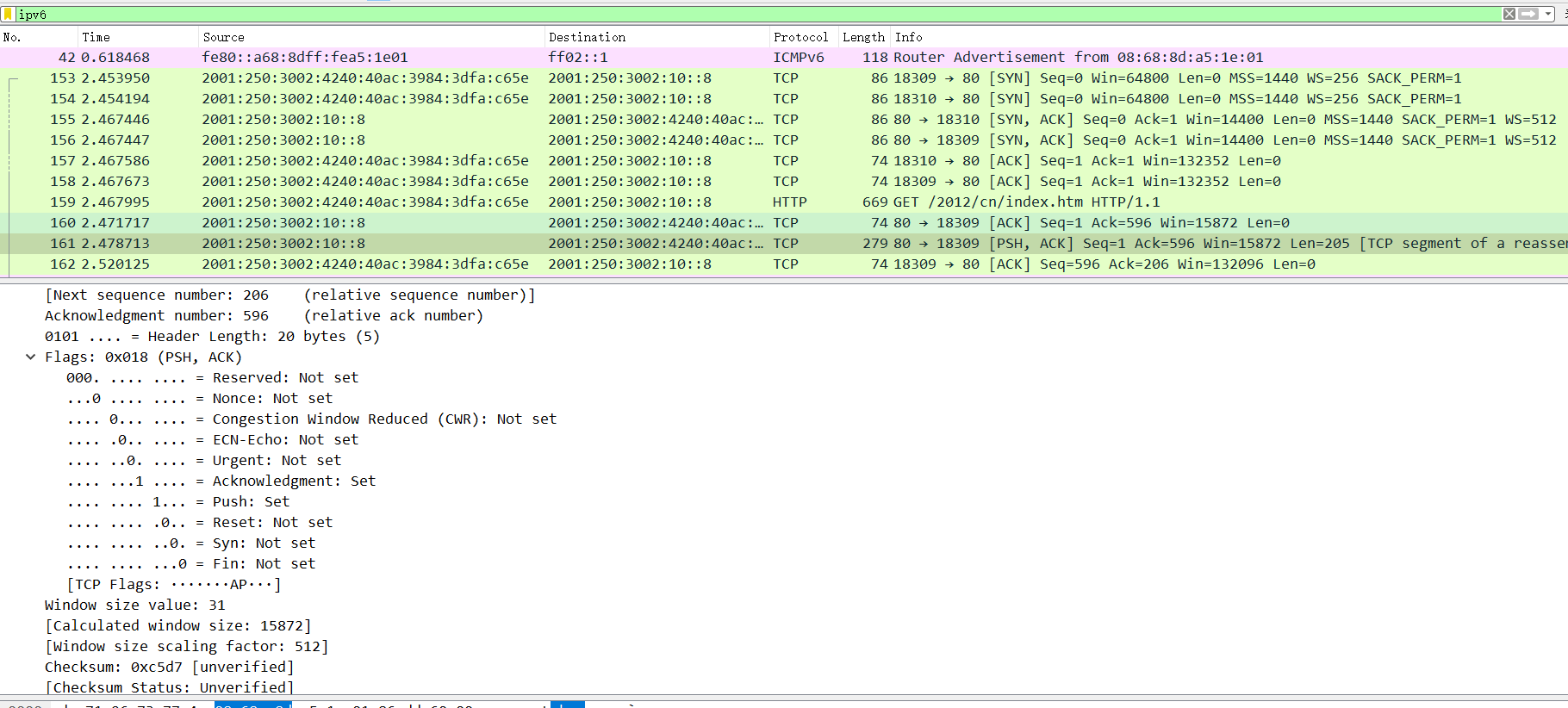


图 10 TCP报文

1. 若只显示第一次握手的数据包，则显示过滤器的规则为 tcp.flags.syn == 1 and tcp.flags.ack == 0 （显示包含 TCP SYN 并且不包含 ACK 标志的数据包）。找

出第一次握手的数据包并截取对该数据包的展开图，根据截图填写下面字段的内容。

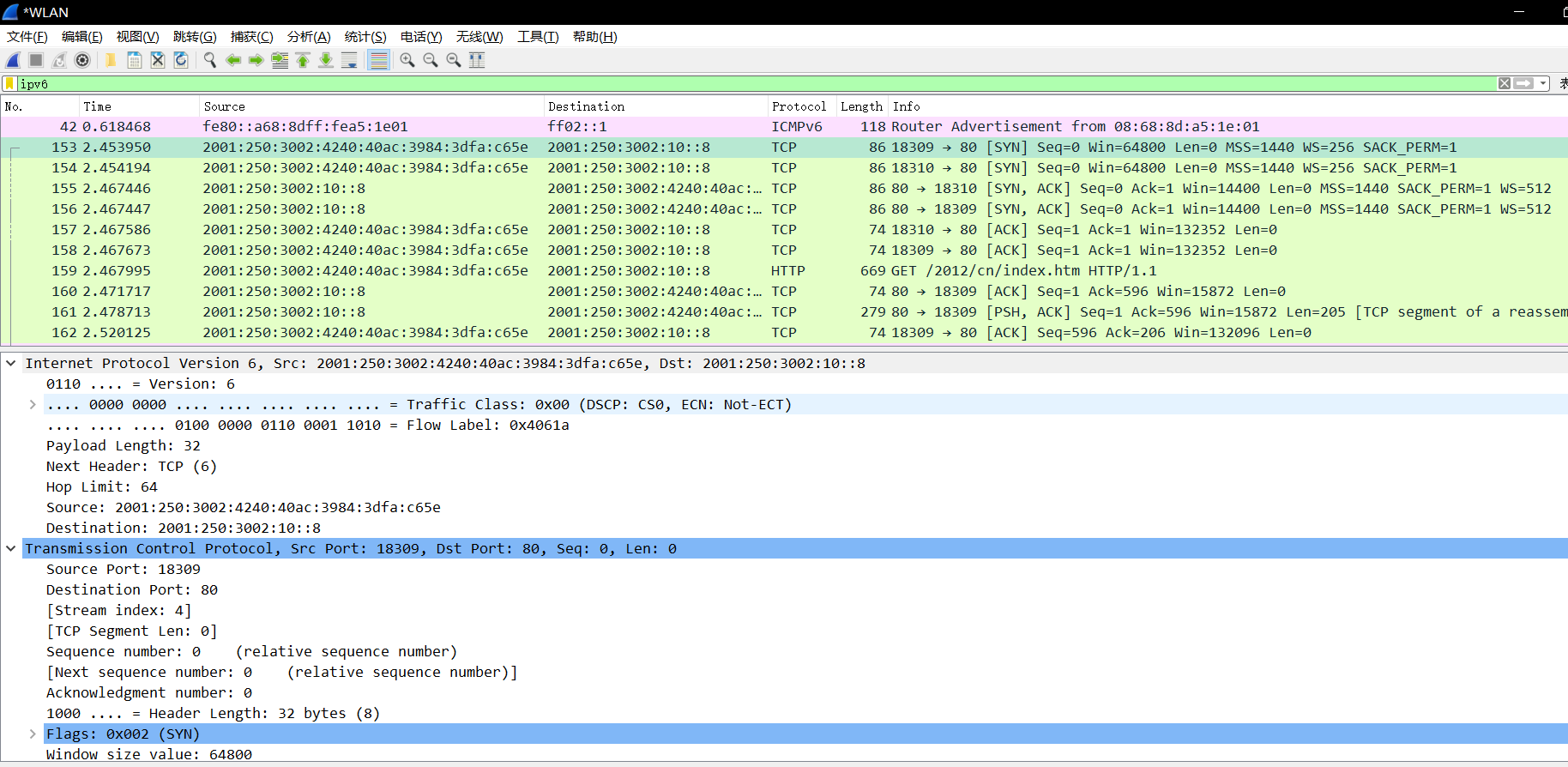


表 1 第一次握手

|  |  |
| --- | --- |
| 源地址 | 2001:250:3002:4240:40ac:3984:3dfa:c65e |
| 目的地址 | 2001:250:3002:10::8 |
| 序号 | 0 |
| 确认号 | 0 |
| 数据偏移 | 32 |
| URG | 0 |
| ACK | 0 |
| PSH | 0 |
| RST | 0 |
| SYN | 1 |
| FIN | 0 |
| 窗口 | 64800 |

1. 若只显示第二次握手的数据包，则显示过滤器的规则为 tcp.flags.syn == 1 and tcp.flags.ack == 1 ，找出第二次握手的数据包并截取对该数据包的展开图， 根据截图填写下面字段的内容。

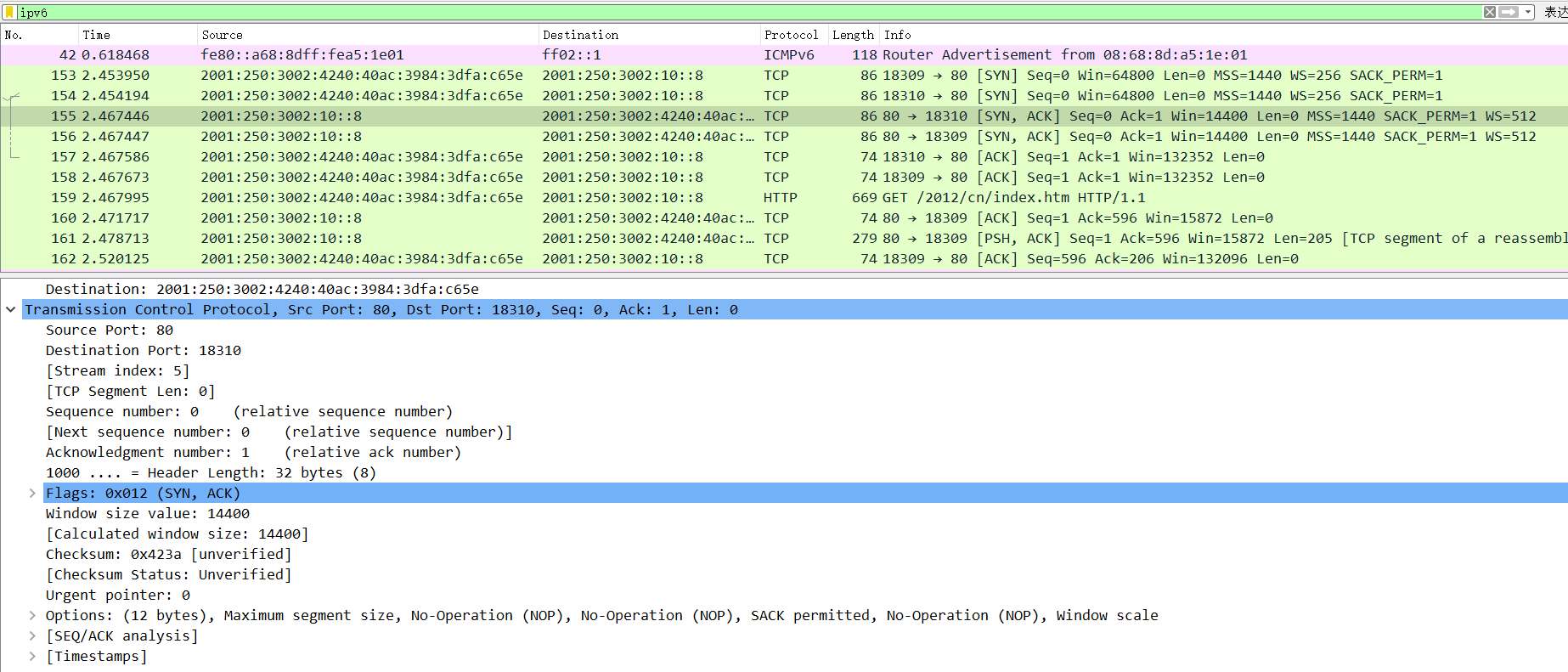


表 2 第二次握手

|  |  |
| --- | --- |
| 源地址 | 2001:250:3002:10::8 |
| 目的地址 | 2001:250:3002:4240:40ac:3984:3dfa:c65e |
| 序号 | 0 |
| 确认号 | 1 |
| 数据偏移 | 32 |
| URG | 0 |
| ACK | 1 |
| PSH | 0 |
| RST | 0 |
| SYN | 1 |
| FIN | 01 |
| 窗口 | 14400 |

1. 若只显示第三次握手的数据包，则显示过滤器的规则为 tcp.flags.syn == 0 and tcp.flags.ack == 1，找出第三次握手的数据包并截取对该数据包的展开图，根据截图填写下面字段的内容。

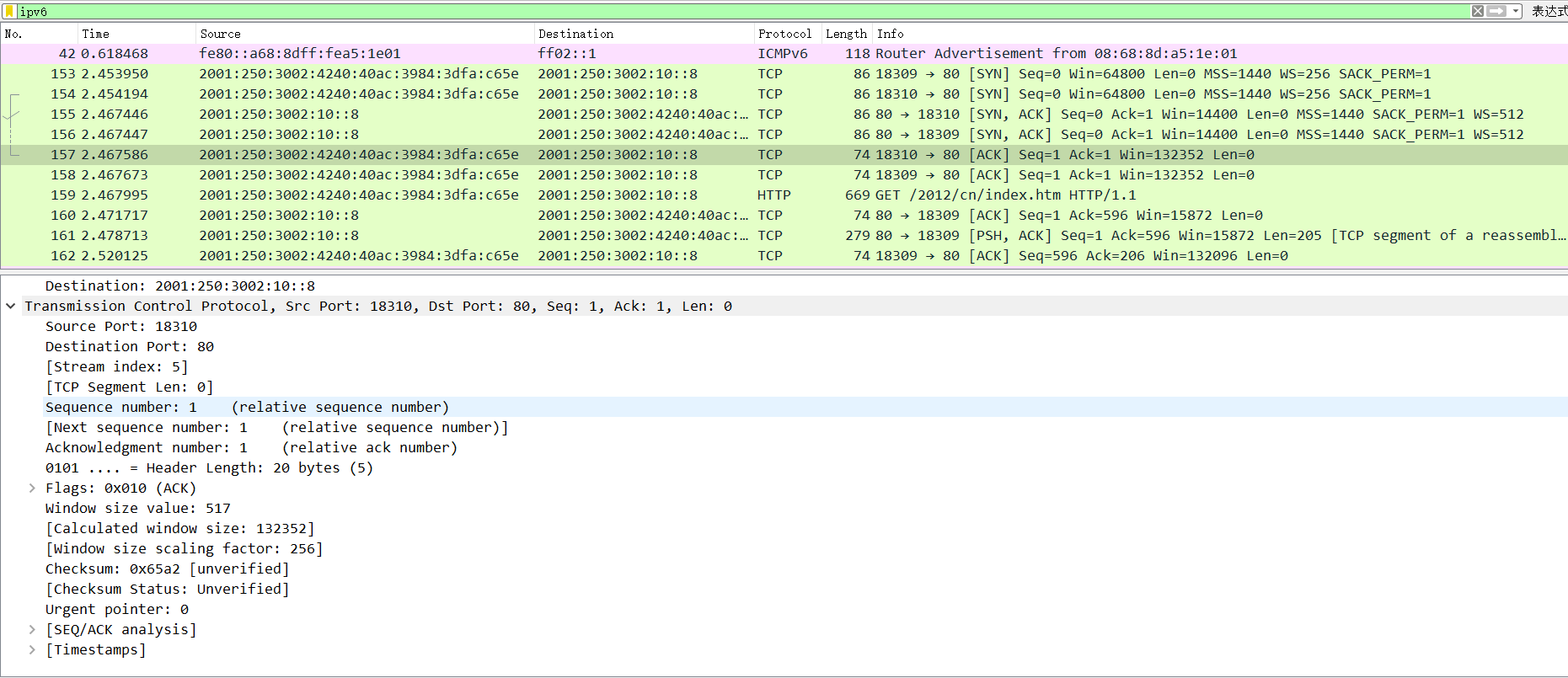


表 3 第三次握手

|  |  |
| --- | --- |
| 源地址 | 2001:250:3002:4240:40ac:3984:3dfa:c65e |
| 目的地址 | 2001:250:3002:10::8 |
| 序号 | 1 |
| 确认号 | 1 |
| 数据偏移 | 20 |
| URG | 0 |
| ACK | 1 |
| PSH | 0 |
| RST | 0 |
| SYN | 0 |
| FIN | 0 |
| 窗口 | 132352（517\*256） |

1. 三次握手之后，客户端要请求服务器传送数据。找出第一次请求的数据包

并截取对该数据包的展开图粘贴在下方，并根据截图填写表 4。

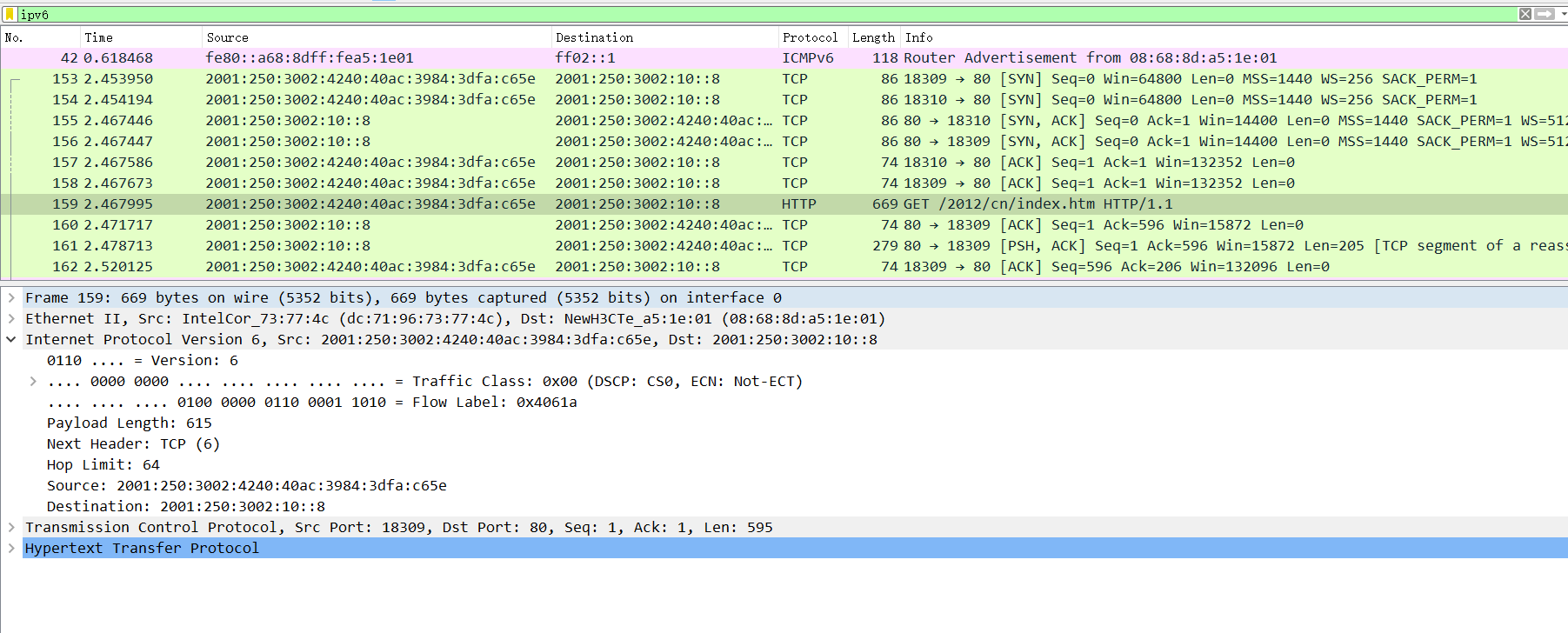


表 4 第一次请求数据

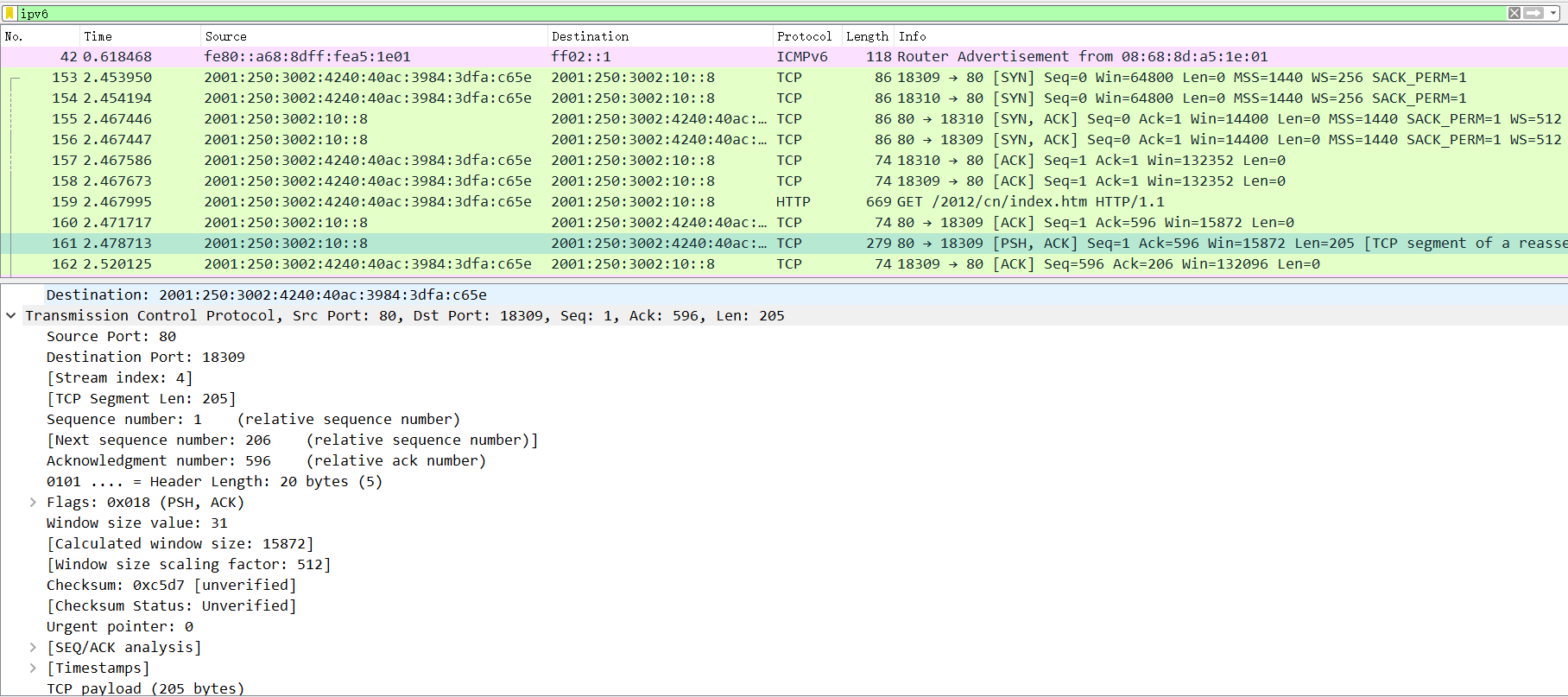
|  |  |
| --- | --- |
| 源地址 | 2001:250:3002:4240:40ac:3984:3dfa:c65e |
| 目的地址 | 2001:250:3002:10::8 |
| 序号 | 1 |
| 确认号 | 1 |
| 数据偏移 | 20 |
| URG | 0 |
| ACK | 1 |
| PSH | 1 |
| RST | 0 |
| SYN | 0 |
| FIN | 0 |
| 窗口 | 132352（517\*256） |

问题：你是如何确定是第一次的请求的数据包？

三次握手后，本机向目的主机发送的第一个tcp包

1. 服务器要传送数据给客户端。找出第一次回复的数据包并截取对该数据包

的展开图粘贴在下方，并根据截图填写表 5。



包含请求内容的数据应该是序号为161的包，前一个包用于告知发送的长度

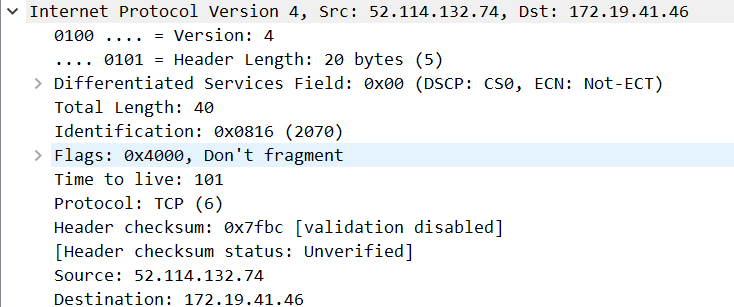
表 5 第一次回复数据

|  |  |
| --- | --- |
| 源地址 | 2001:250:3002:10::8 |
| 目的地址 | 2001:250:3002:4240:40ac:3984:3dfa:c65e |
| 序号 | 1 |
| 确认号 | 596 |
| 数据偏移 | 20 |
| URG | 0 |
| ACK | 1 |
| PSH | 1 |
| RST | 0 |
| SYN | 0 |
| FIN | 0 |
| 窗口 | 15872（31\*512） |

* 1. **任务四 分析IP数据报**

自己设计实验，抓取 IP 数据报，解释 IP 数据报首部各字段的含义并写在下方。

以一个TCP包为例

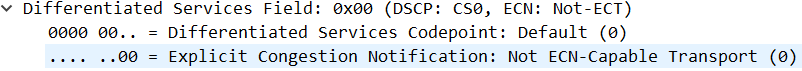


从上到下每一行的含义

版本号：用的网络是ipv4所以版本号为4

头部长度：20

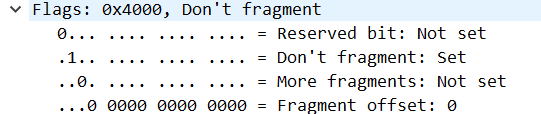
服务类型：



总长度：40

标识位：0x0816

标志位：



TTL：101

协议标识：TCP

校验和：0x7fbc

源地址：52.114.132.74

目的地址：172.19.41.46

1. 实验报告要求
2. 针对以上实验任务，在报告中明确描述对各任务要求的完成情况，报告中同时需提供实验时的 wireshark 运行截图，并进行替换，回答问题并给出分析。
3. 实验过程出现的问题（与四个任务有关），并给出自己的解释，要求至少提出一个。
4. 实验报告给的步骤都是基于ipv4的，wireshark的过滤器要设置为icmpv6才能查看到ipv6的ICMP包
5. Ipv6下对ise.sysu.edu.cn的tracerouter中途节点都可以ping通，为了查看icmp不可达的报文，用-4参数强制使用ipv4进行实验
6. 实验为每人独立完成，实验报告以个人为单位独立完成。
7. 实验报告应在**2019年12月12日 7pm**前上交，且上交电子稿即可，发送邮箱**cs\_network@yeah.net**。