浙江大学

本科实验报告

课程名称：　计算机网络

实验名称：　网络协议分析

姓　　名：　徐文祥

学　　院：　计算机学院

系：　软件工程

专　　业：　软件工程

学　　号：　3140101005

指导教师：　黄正谦

2018 年 11 月 2 日

浙江大学实验报告

一、 实验目的

- 学习使用 Wireshark 抓包工具。
- 观察和理解常见网络协议的交互过程
- 理解数据包分层结构和格式。

二、 实验内容

- Wireshark 是 PC 上使用最广泛的免费抓包工具，可以分析大多数常见的协议数据包。有 Windows 版本和 Mac 版本，可以免费从网上下载。
- 掌握网络协议分析软件 Wireshark 的使用，学会配置过滤器
- 观察所在网络出现的各类网络协议，了解其种类和分层结构
- 观察捕获到的数据包格式，理解各字段含义
- 根据要求配置 Wireshark，捕获某一类协议的数据包，并分析解读

三、 主要仪器设备

- 联网的 PC 机、Windows、Linux 或 Mac 操作系统、浏览器软件
- WireShark 协议分析软件

四、 操作方法与实验步骤

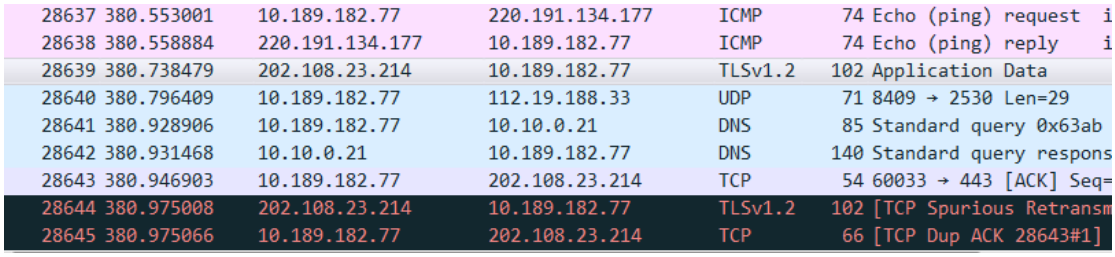
- 安装网络包捕获软件 Wireshark
- 配置网络包捕获软件，捕获所有机器的数据包
- 观察捕获到的数据包，并对照解析结果和原始数据包
- 配置网络包捕获软件，只捕获特定 IP 或特定类型的包
- 抓取以下通信协议数据包，观察通信过程和数据包格式
  - ✓ PING：测试一个目标地址是否可达
  - ✓ TRACE ROUTE：跟踪一个目标地址的途经路由
  - ✓ NSLOOKUP：查询一个域名
  - ✓ HTTP：访问一个网页

五、 实验数据记录和处理

✧ Part One

1. **运行 Wireshark 软件，开始捕获数据包，列出你看到的协议名字（至少 5 个）。**

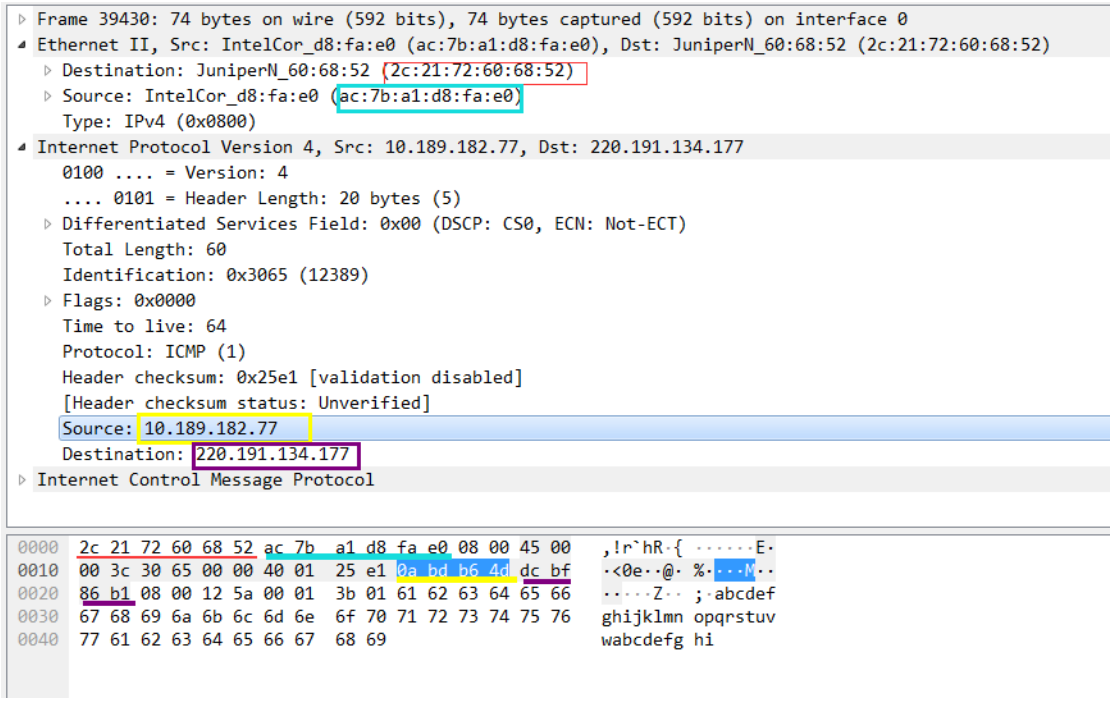
   协议名：UDP，TCP，ICMP，TLSv1.2，DNS



2. **找一个包含 IP 的数据包，这个数据包有 3 层？最高层协议是 IPv4，ICMP ，从 Ethernet 开始往上，各层协议的名字分别为： IPv4，ICMP 。**

   展开 IP 层协议，标出源 IP 地址、目标 IP 地址及其在数据包中的具体位置，展开 Ethernet 层，标出源 MAC 地址和目标 MAC 地址及其在数据包中的具体位置。

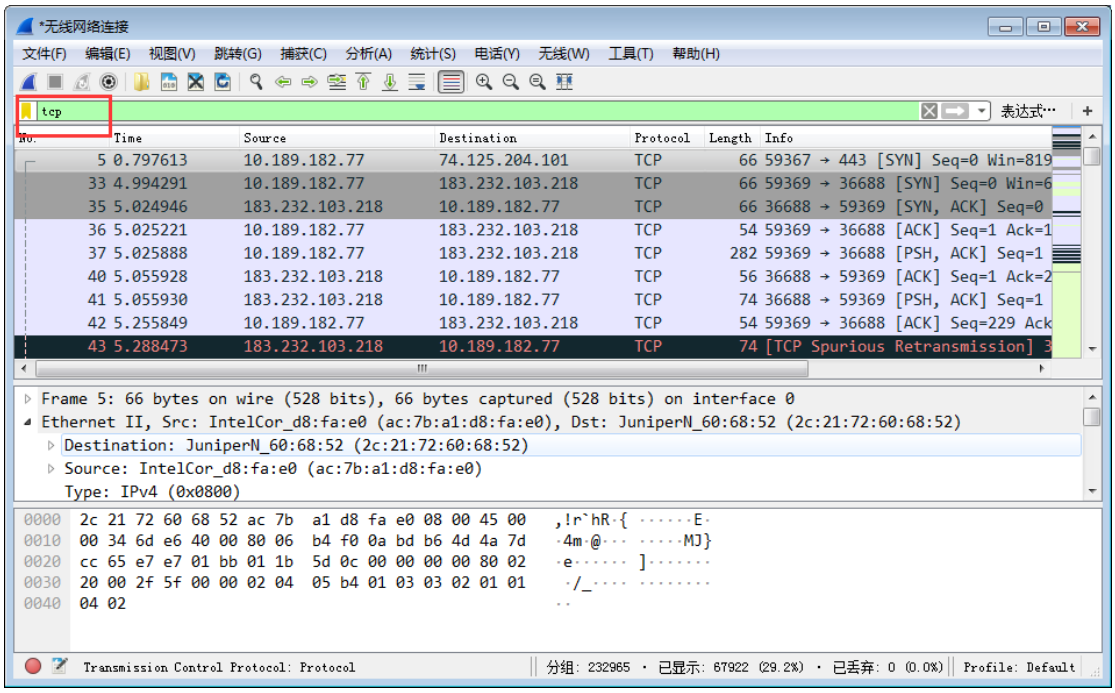
   截图：



3. **配置应用显示过滤器，让界面只显示某一协议类型的数据包（输入协议名称）。**

   使用的过滤器： 显示过滤器 ，希望显示的协议类型： TCP 。

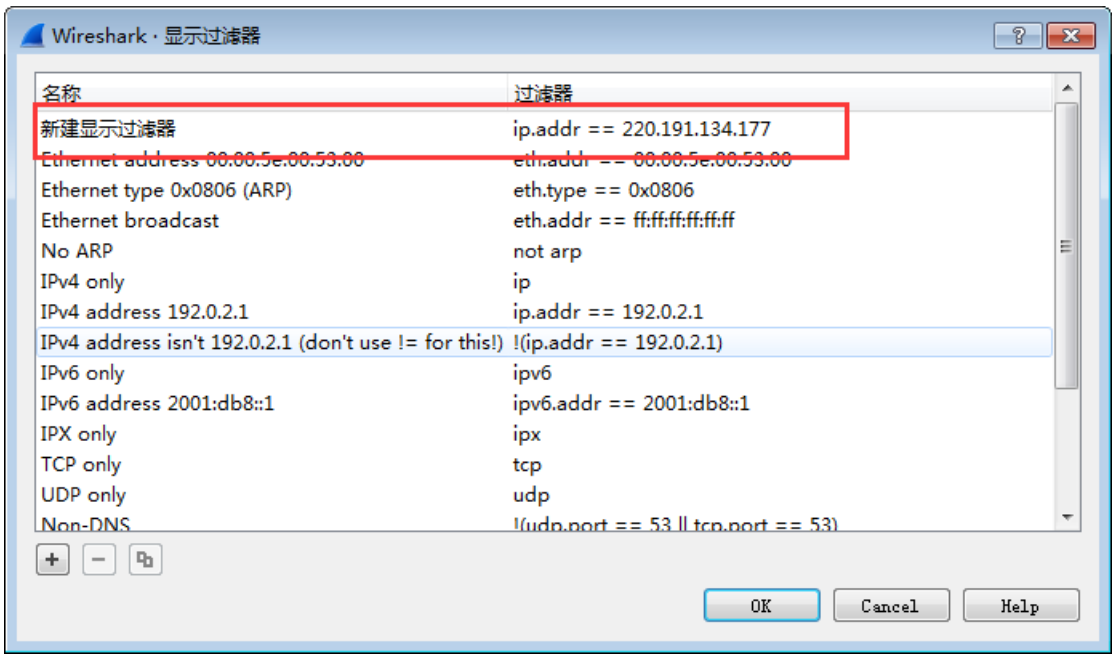
   截图：

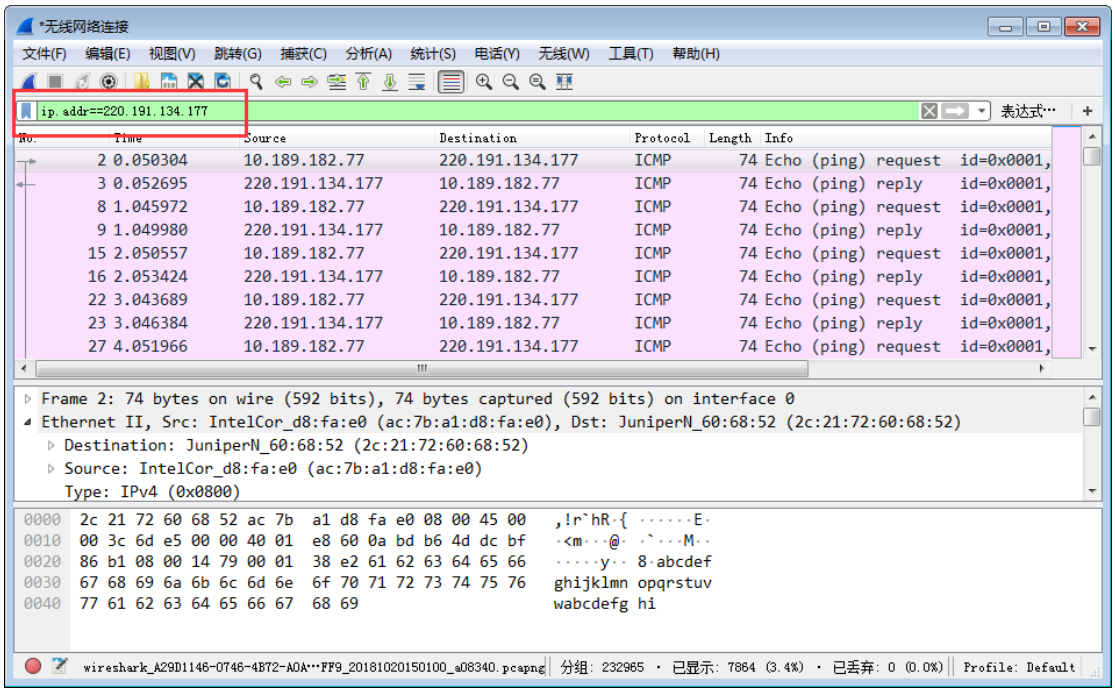


4. 配置应用显示过滤器，让界面只显示某个 IP 地址的数据包（ip.addr==x.x.x.x）。

使用的过滤器：显示过滤器 ，希望显示的 IP 地址：220.191.134.177 。

截图：

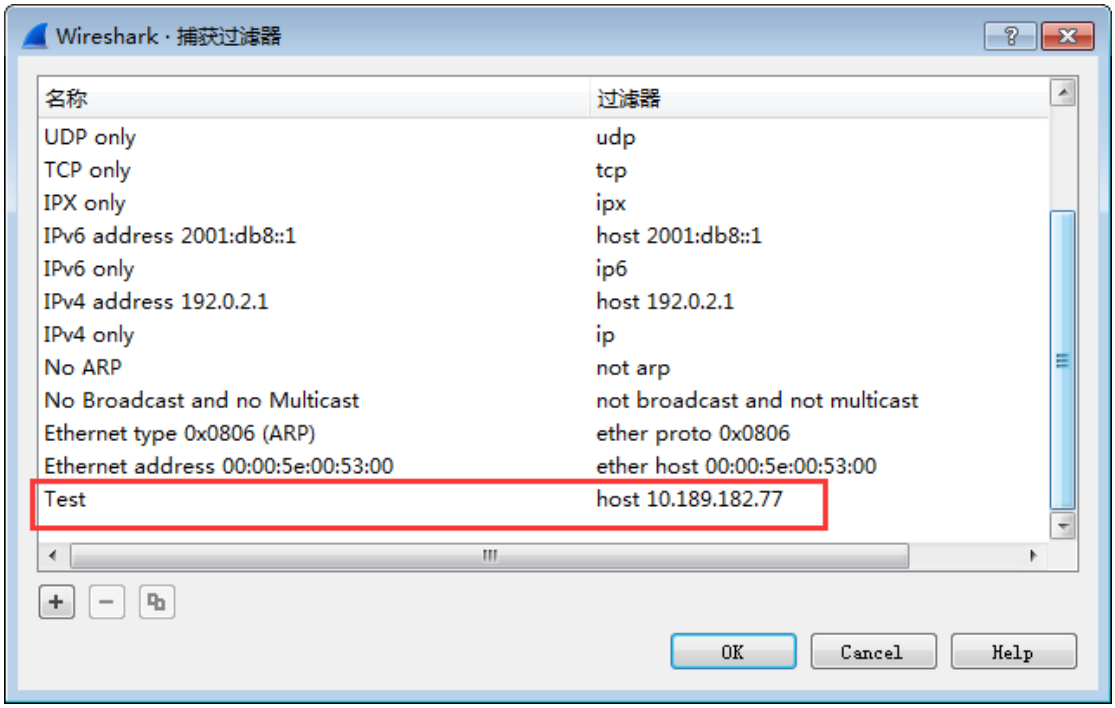


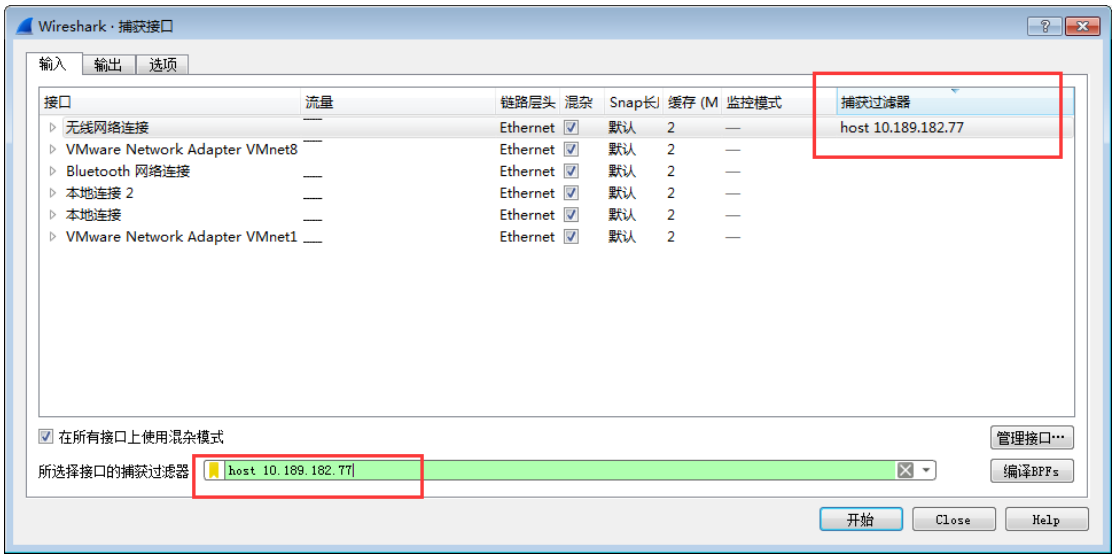


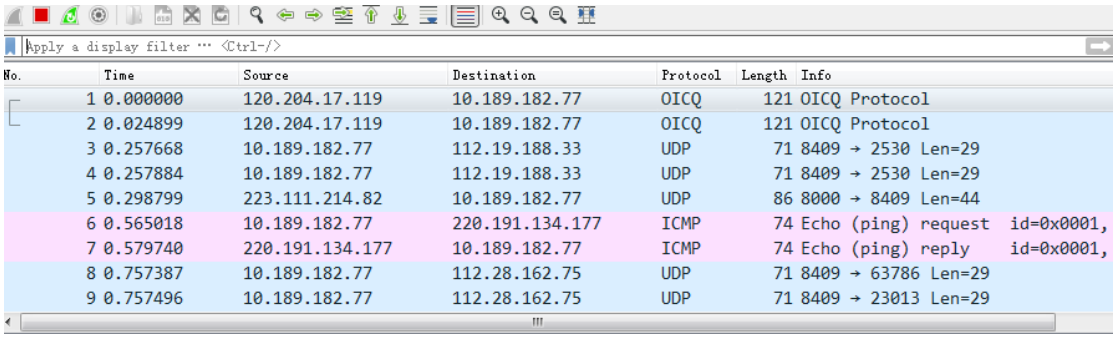
5. 配置捕获过滤器，只捕获某个 IP 地址的数据包（host x.x.x.x）。

使用的过滤器：捕获过滤器 ，希望捕获的 IP 地址：10.189.182.77 。

截图：



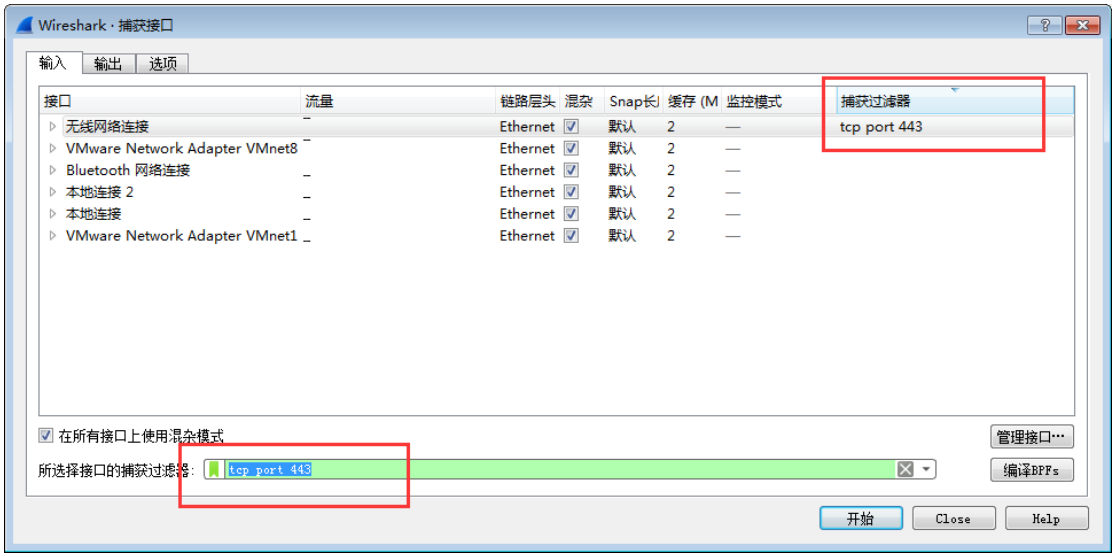


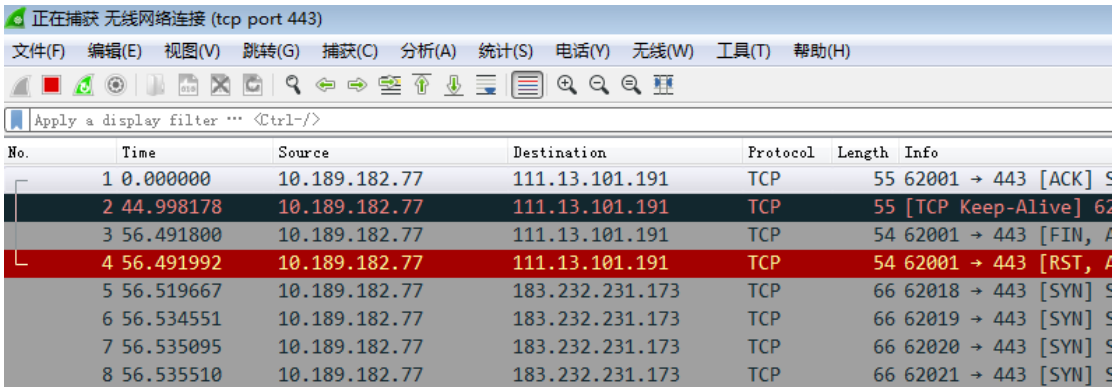


6. 配置捕获过滤器，只捕获某类协议的数据包（tcp port xx 或者 udp port xx）。

使用的过滤器：捕获过滤器 ，希望捕获的协议类型：TCP(tcp port 443) 。

截图：





✧ Part Two

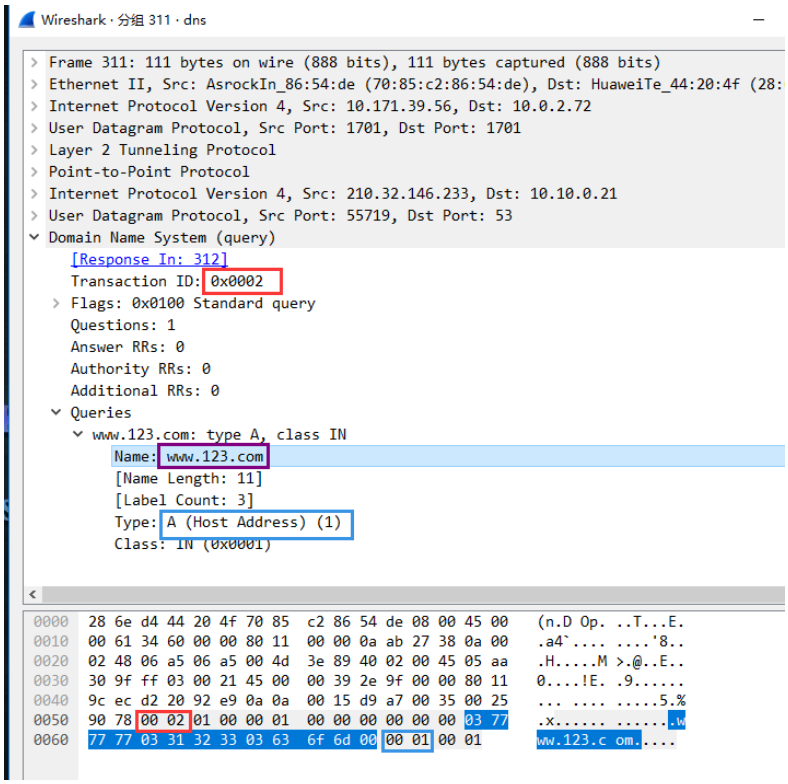
任务 1：使用 nslookup 命令，查询某个域名，并捕获这次的数据包。DNS 数据包由哪几层协议构成？ IPv4，UDP，L2TP，PPP，DNS 。使用的服务方端口是： 53 。

分别选择一个请求包和一个响应包，展开最高层协议的详细内容，标出交易 ID、查询类型、查询的域名内容以及查询结果。

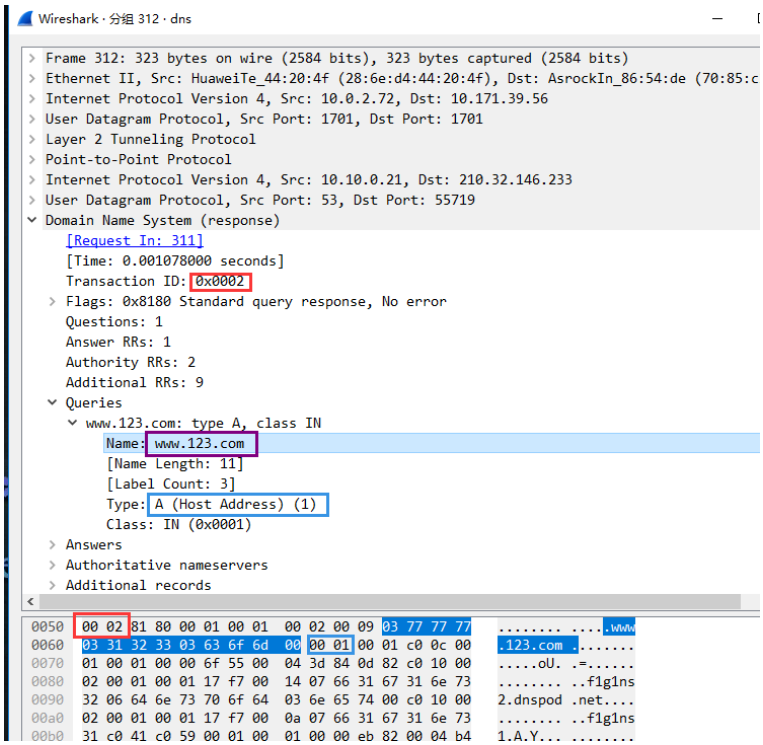
截图：

测试网址：

请求包：



响应包：



任务 2：使用 Ping 命令，分别测试某个 IP 地址和某个域名的连通性，并捕获数据包。捕获到了哪些相关协议数据包？

Ping IP 地址时：ICMP，OICQ

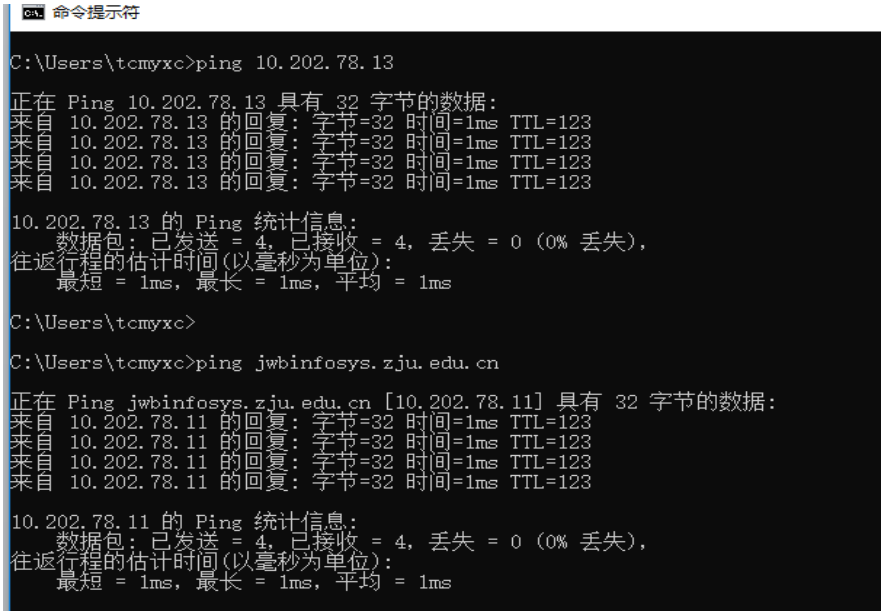
Ping 域名时：ICMP，OICQ，UDP

ICMP 数据包分别由哪几层协议构成？ICMP，IPv4，PPP，L2TP，UDP

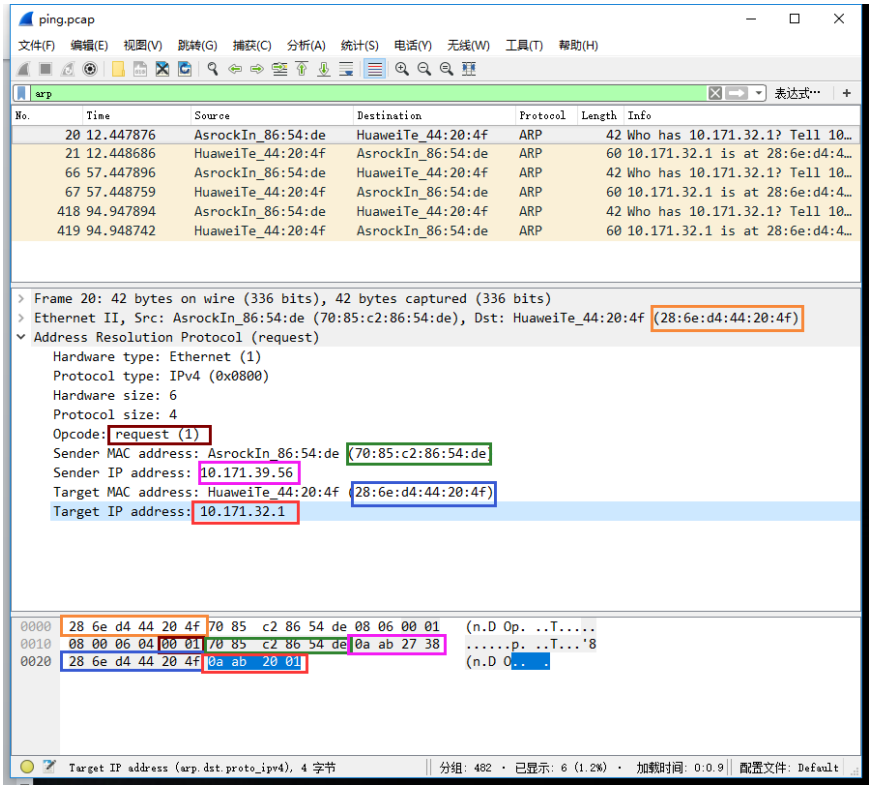
分别选择一个 ARP 请求和响应数据包，展开最高层协议的详细内容，标出操作码、发送者 IP 地址、发送者 MAC 地址、查询的目标 IP 地址、Ethernet 层的目标 MAC 地址以及查询结果。

截图：

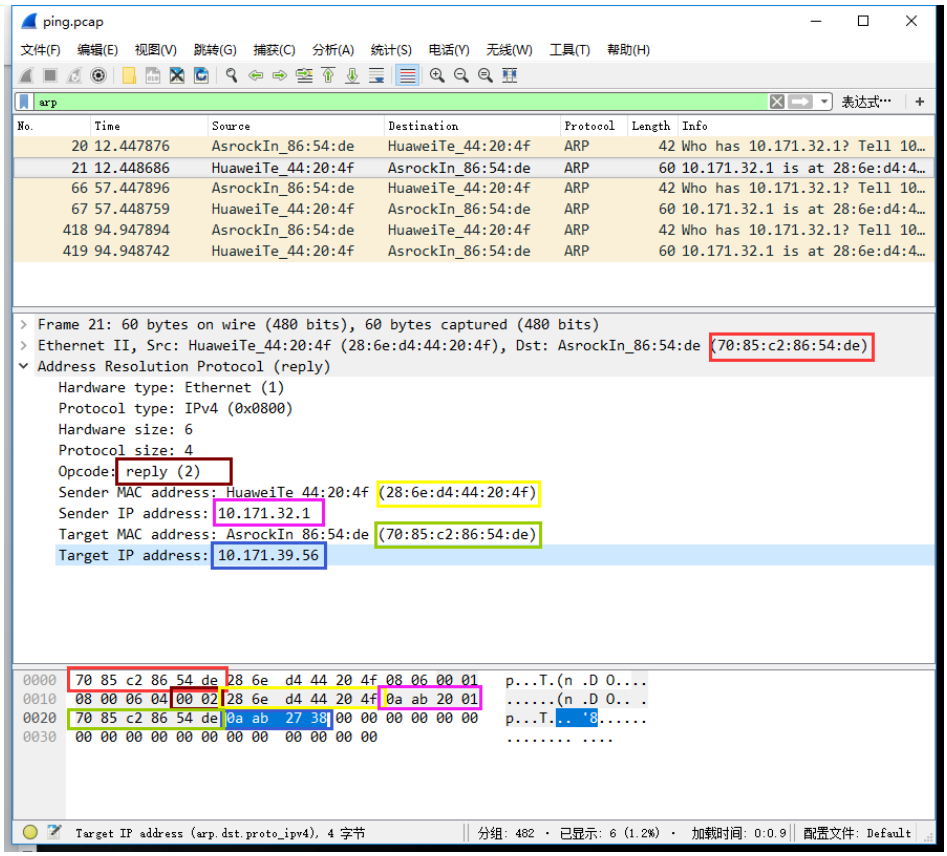
测试网址：



请求包：


ping.pcap
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)
arp
表达式…
No. Time Source Destination Protocol Length Info
20 12.447876 AsrockIn_86:54:de HuaweiTe_44:20:4f ARP 42 Who has 10.171.32.1? Tell 10…
21 12.448686 HuaweiTe_44:20:4f AsrockIn_86:54:de ARP 60 10.171.32.1 is at 28:6e:d4:4…
66 57.447896 AsrockIn_86:54:de HuaweiTe_44:20:4f ARP 42 Who has 10.171.32.1? Tell 10…
67 57.448759 HuaweiTe_44:20:4f AsrockIn_86:54:de ARP 60 10.171.32.1 is at 28:6e:d4:4…
418 94.947894 AsrockIn_86:54:de HuaweiTe_44:20:4f ARP 42 Who has 10.171.32.1? Tell 10…
419 94.948742 HuaweiTe_44:20:4f AsrockIn_86:54:de ARP 60 10.171.32.1 is at 28:6e:d4:4…
Frame 20: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: AsrockIn_86:54:de (70:85:c2:86:54:de), Dst: HuaweiTe_44:20:4f (28:6e:d4:44:20:4f)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: AsrockIn_86:54:de (70:85:c2:86:54:de)
Sender IP address: 10.171.39.56
Target MAC address: HuaweiTe_44:20:4f (28:6e:d4:44:20:4f)
Target IP address: 10.171.32.1
0000 28 6e d4 44 20 4f 70 85 c2 86 54 de 08 06 00 01 (n.D Op. ..T.....
0010 08 00 06 04 00 01 70 85 c2 86 54 de 0a ab 27 38 ......p. ..T...'8
0020 28 6e d4 44 20 4f 0a ab 20 01 (n.D O.. .
Target IP address (arp.dst.proto_ipv4), 4 字节
分组: 482 · 已显示: 6 (1.2%) · 加载时间: 0:0.9
配置文件: Default

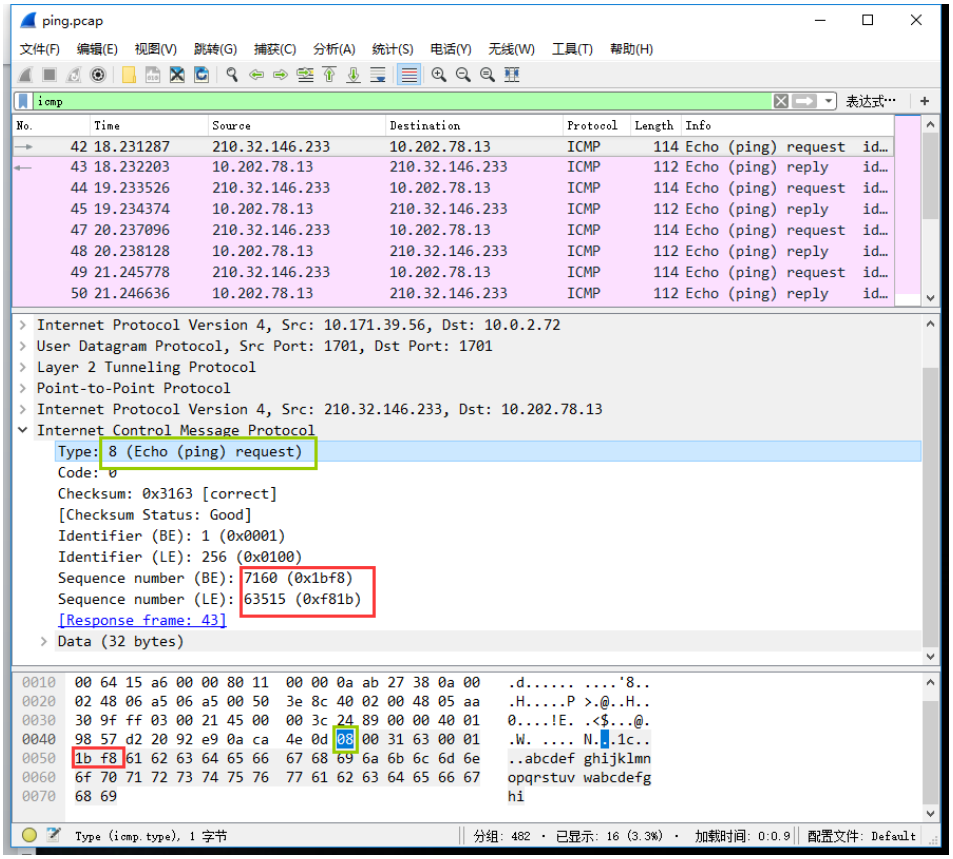
响应包：


ping.pcap
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)
arp
表达式…
No. Time Source Destination Protocol Length Info
20 12.447876 AsrockIn_86:54:de HuaweiTe_44:20:4f ARP 42 Who has 10.171.32.1? Tell 10…
21 12.448686 HuaweiTe_44:20:4f AsrockIn_86:54:de ARP 60 10.171.32.1 is at 28:6e:d4:4…
66 57.447896 AsrockIn_86:54:de HuaweiTe_44:20:4f ARP 42 Who has 10.171.32.1? Tell 10…
67 57.448759 HuaweiTe_44:20:4f AsrockIn_86:54:de ARP 60 10.171.32.1 is at 28:6e:d4:4…
418 94.947894 AsrockIn_86:54:de HuaweiTe_44:20:4f ARP 42 Who has 10.171.32.1? Tell 10…
419 94.948742 HuaweiTe_44:20:4f AsrockIn_86:54:de ARP 60 10.171.32.1 is at 28:6e:d4:4…
Frame 21: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: HuaweiTe_44:20:4f (28:6e:d4:44:20:4f), Dst: AsrockIn_86:54:de (70:85:c2:86:54:de)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HuaweiTe_44:20:4f (28:6e:d4:44:20:4f)
Sender IP address: 10.171.32.1
Target MAC address: AsrockIn_86:54:de (70:85:c2:86:54:de)
Target IP address: 10.171.39.56
0000 70 85 c2 86 54 de 28 6e d4 44 20 4f 08 06 00 01 p...T.(n .D O....
0010 08 00 06 04 00 02 28 6e d4 44 20 4f 0a ab 20 01 ......(n .D O.. .
0020 70 85 c2 86 54 de 0a ab 27 38 00 00 00 00 00 00 p...T... '8......
0030 00 00 00 00 00 00 00 00 00 00 00 00 ....
Target IP address (arp.dst.proto_ipv4), 4 字节
分组: 482 · 已显示: 6 (1.2%) · 加载时间: 0:0.9
配置文件: Default

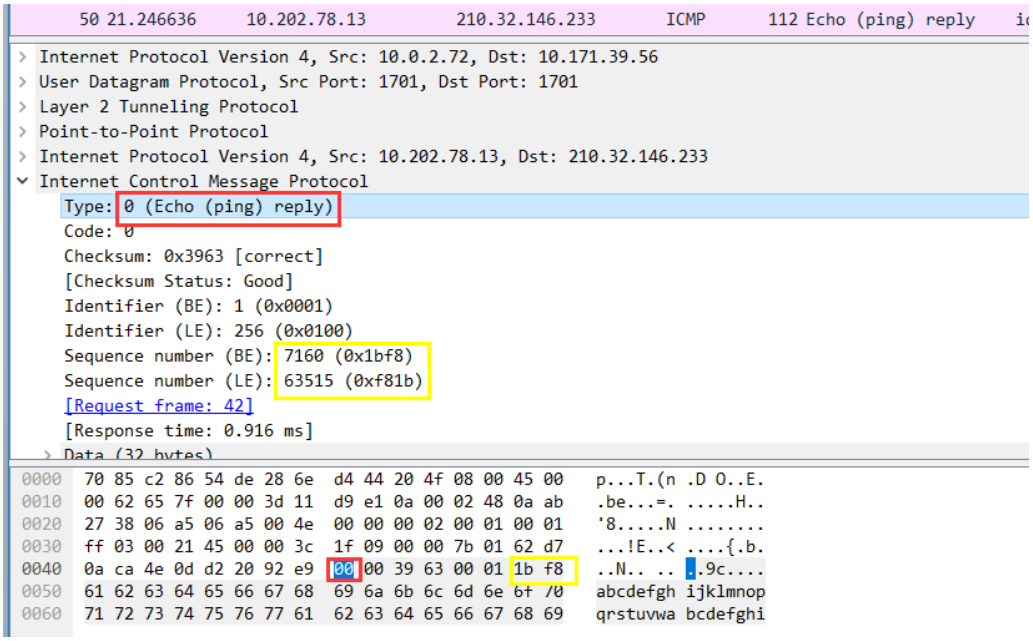
分别选择一个 ICMP 请求和响应数据包，展开最高层协议的详细内容，标出类型、序号。

截图：

请求包：



响应包：



任务 3：使用 Tracert 命令（Mac 下使用 Traceroute 命令），跟踪某个外部 IP 地址的路由，并捕获这次的数据包。跟踪路由使用的数据包协议类型是：__ICMP__，数据包由几层协议构成？__ICMP，IPV4，PPP，L2TP，UDP__。

观察并记录请求包中 IP 协议层的 TTL 字段变化规律，第一个请求的 TTL 等于__1__，同样 TTL 的请求连续发送了__3__个，然后每次 TTL 增加了__1__，最后一个请求的 TTL 等于__11__。附上截图：

截图：

追踪网址：

软件截图：

117 31.135413	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7172/1052, ttl=1 (no response found!)
118 31.136654	10.0.2.72	210.32.146.233	ICMP	108	Time-to-live exceeded (Time to live exceeded in transit)
119 31.137259	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7173/1308, ttl=1 (no response found!)
120 31.138032	10.0.2.72	210.32.146.233	ICMP	108	Time-to-live exceeded (Time to live exceeded in transit)
121 31.138817	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7174/1564, ttl=1 (no response found!)
122 31.139608	10.0.2.72	210.32.146.233	ICMP	108	Time-to-live exceeded (Time to live exceeded in transit)
125 32.145500	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7175/1820, ttl=2 (no response found!)
126 32.146442	10.3.7.70	210.32.146.233	ICMP	108	Time-to-live exceeded (Time to live exceeded in transit)
127 32.149735	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7176/2076, ttl=2 (no response found!)
128 32.150568	10.3.7.70	210.32.146.233	ICMP	108	Time-to-live exceeded (Time to live exceeded in transit)
129 32.154542	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7177/2332, ttl=2 (no response found!)
130 32.155398	10.3.7.70	210.32.146.233	ICMP	108	Time-to-live exceeded (Time to live exceeded in transit)
135 33.990662	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7178/2588, ttl=3 (no response found!)
136 33.991716	10.3.7.213	210.32.146.233	ICMP	108	Time-to-live exceeded (Time to live exceeded in transit)
137 33.992773	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7179/2844, ttl=3 (no response found!)
138 33.993849	10.3.7.213	210.32.146.233	ICMP	108	Time-to-live exceeded (Time to live exceeded in transit)
139 33.994481	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7180/3100, ttl=3 (no response found!)
146 38.387561	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7181/3356, ttl=4 (no response found!)
147 38.390320	39.174.130.17	210.32.146.233	ICMP	108	Time-to-live exceeded (Time to live exceeded in transit)
148 38.391442	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7182/3612, ttl=4 (no response found!)

177 43.953930	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7190/5660, ttl=7 (no response found!)
179 47.561359	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7191/5916, ttl=7 (no response found!)
181 51.561295	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7192/6172, ttl=7 (no response found!)
186 55.563965	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7193/6428, ttl=8 (no response found!)
187 55.593413	120.241.49.238	210.32.146.233	ICMP	108	Time-to-live exceeded (Time to live exceeded in transit)
188 55.595037	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7194/6684, ttl=8 (no response found!)
189 55.624432	120.241.49.238	210.32.146.233	ICMP	108	Time-to-live exceeded (Time to live exceeded in transit)
190 55.628604	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7195/6940, ttl=8 (no response found!)
191 55.658006	120.241.49.238	210.32.146.233	ICMP	108	Time-to-live exceeded (Time to live exceeded in transit)
204 65.887999	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7196/7196, ttl=9 (no response found!)
205 69.561473	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7197/7452, ttl=9 (no response found!)
208 73.559382	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7198/7708, ttl=9 (no response found!)
215 77.562201	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7199/7964, ttl=10 (no response found!)
217 81.561415	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7200/8220, ttl=10 (no response found!)
250 85.558636	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7201/8476, ttl=10 (no response found!)
282 89.564128	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7202/8732, ttl=11 (reply in 283)
283 89.593055	183.232.231.172	210.32.146.233	ICMP	144	Echo (ping) reply id=0x0001, seq=7202/8732, ttl=54 (request in 282)
284 89.594543	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7203/8988, ttl=11 (reply in 285)
285 89.623619	183.232.231.172	210.32.146.233	ICMP	144	Echo (ping) reply id=0x0001, seq=7203/8988, ttl=54 (request in 284)
286 89.625081	210.32.146.233	183.232.231.172	ICMP	146	Echo (ping) request id=0x0001, seq=7204/9244, ttl=11 (reply in 287)
287 89.654100	183.232.231.172	210.32.146.233	ICMP	144	Echo (ping) reply id=0x0001, seq=7204/9244, ttl=54 (request in 286)

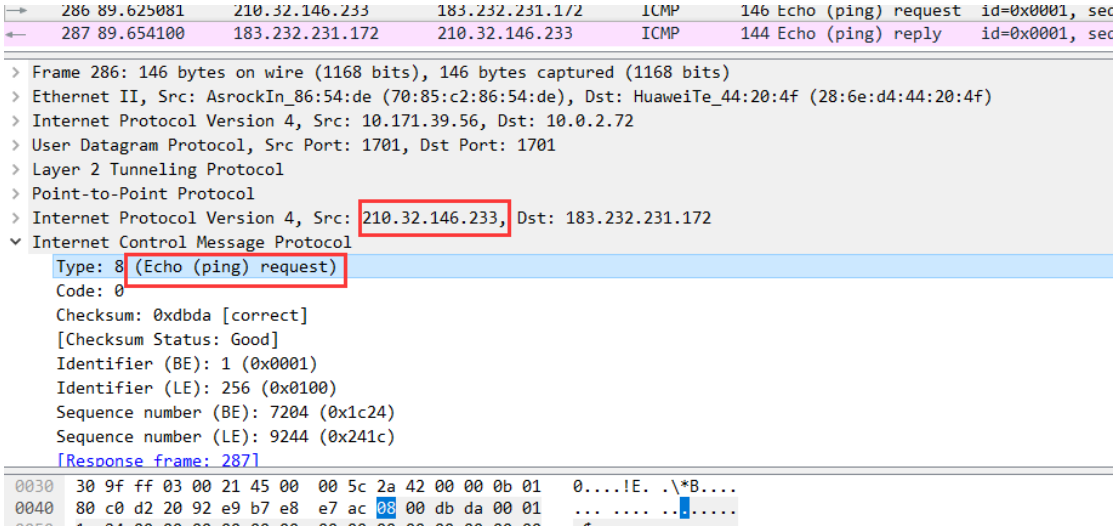
观察并记录响应包的信息，第一组响应包的发送者 IP 是：__10.0.2.72__，标记 ICMP 层的类型字段。最后一组响应包的发送者 IP 是：__210.32.146.233__，标记 ICMP 层的类型字段。附上截图：

截图：

第一组：

```
126 32.146442    10.3.7.70          210.32.146.233     ICMP    108 Time-to-live exceeded (Time to live exceeded
> Frame 118: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
> Ethernet II, Src: HuaweiTe_44:20:4f (28:6e:d4:44:20:4f), Dst: AsrockIn_86:54:de (70:85:c2:86:54:de)
> Internet Protocol Version 4, Src: 10.0.2.72, Dst: 10.171.39.56
> User Datagram Protocol, Src Port: 1701, Dst Port: 1701
> Layer 2 Tunneling Protocol
> Point-to-Point Protocol
> Internet Protocol Version 4, Src: 10.0.2.72, Dst: 210.32.146.233
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
  > Internet Protocol Version 4, Src: 210.32.146.233, Dst: 183.232.231.172
  v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xdbfa [unverified] [in ICMP error packet]
0000  70 85 c2 86 54 de 28 6e  d4 44 20 4f 08 00 45 00   p...T.(n .D O..E.
```

最后一组：



✧ Part Three

1. **运行 ipconfig /flushdns 命令清空 DNS 缓存，然后打开浏览器，访问 www.zju.edu.cn，并使用捕获过滤器只捕获访问该网站的数据（过滤器设置：tcp port 80 or udp port 53），网页完全打开后，停止捕获。**

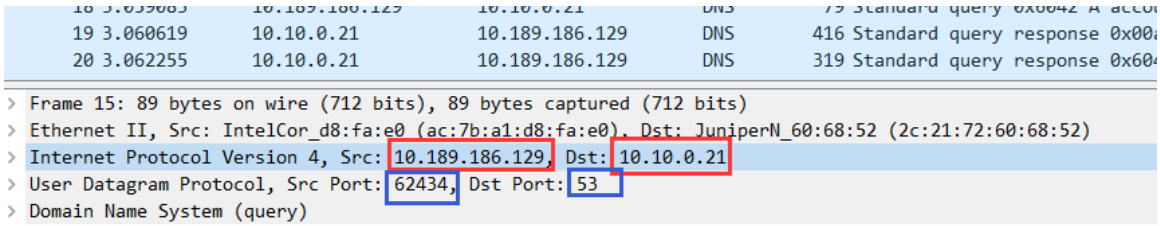
   捕获到的这些最高层的协议数据包分别由哪几层协议构成？

   DNS： IPv4，UDP，DNS

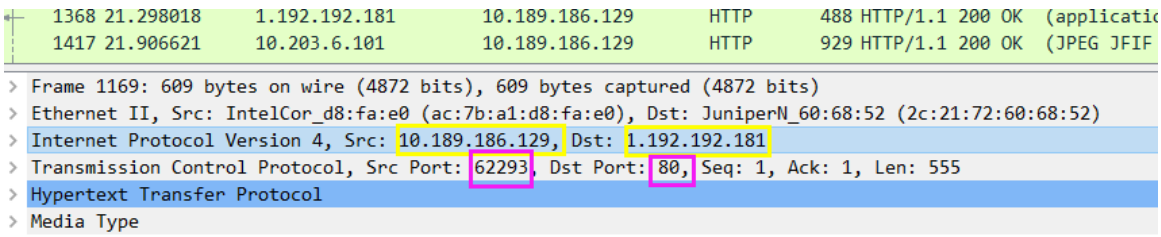
   HTTP: IPv4，TCP，HTTP

   每种协议选取一个代表展开后截图，并标出源和目标 IP 地址、源和目标端口）

DNS 协议：



HTTP 协议：



2. **为了打开网页，浏览器查询了哪些相关的域名？**

域名列表： ns1.msft.net， dns1.zju.edu.cn， ns1.e.shifen.com， dns1.zju.edu.cn， f.root-servers.net， googleapis.l.google.com， dns1.zju.edu.cn， i.root-servers.net， d.gtld-servers.net，g.gtld-servers.net，dns1.zju.edu.cn，zuaa.zju.edu.cn，l.gtld-servers.net，l.gtld-servers.net，h.root-servers.net，h.root-servers.net，ns2.msft.net，ns2.msft.net，clientservices.googleapis.com，f1g1ns2.dnspod.net，www.zju.edu.cn

3. **使用显示过滤器 tcp.stream eq X，让 X 从 0 开始变化，直到没有数据。分析浏览器为了获取网页数据，总共建立了几个连接？（一个 TCP 流对应一个 TCP 连接）**

TCP 连接数： 20

4. **右键点击某个 HTTP 数据包，选择跟踪 TCP 流，可以看到 HTTP 会话的数据。分析浏览器与 WEB 服务器之间进行了几次 HTTP 会话（一对 HTTP 请求和响应对应一次 HTTP 会话）？注意：一个 TCP 流上可能存在多个 HTTP 会话。**

HTTP 会话数： 11

5. **选择一个 HTTP 的 TCP 流进行截图，标出请求和响应部分（最好有多个 HTTP 会话的）：**

截图：

会话 1：

```
GET / HTTP/1.1
Host: www.zju.edu.cn
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.67 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
Hm_lvt_fe30bbc1ee45421ec1679d1b8d8f8453=1540035806,1540035906,1540035961,15
40036067; _pk_id.3.331d=14cff805b92dd47a.
1540035808.1.1540036068.1540035808.;
Hm_lvt_39dcd5bd05965dcfa70b1d2457c6dcae=1540035808,1540035907,1540035961,15
40036068

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 09:09:27 GMT
Server: Apache/2.2.31 (Unix) DAV/2 mod_jk/1.2.23
Accept-Ranges: bytes
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
```

会话 2：

```
GET /_js/_portletPlugs/datepicker/css/datepicker.css HTTP/1.1
Host: www.zju.edu.cn
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.67 Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://www.zju.edu.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
Hm_lvt_fe30bbc1ee45421ec1679d1b8d8f8453=1540035806,1540035906,1540035961,15
40036067; _pk_id.3.331d=14cff805b92dd47a.
1540035808.1.1540036068.1540035808.;
Hm_lvt_39dcd5bd05965dcfa70b1d2457c6dcae=1540035808,1540035907,1540035961,15
40036068

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 09:09:28 GMT
Server: Apache/2.2.31 (Unix) DAV/2 mod_jk/1.2.23
Last-Modified: Mon, 21 Mar 2016 05:58:10 GMT
ETag: "2c11c6-15e0-52e88c808c080"
Accept-Ranges: bytes
Content-Length: 5600
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/css
```

会话 3：

```
}GET /_css/_system/system_editor.css HTTP/1.1
Host: www.zju.edu.cn
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.67 Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://www.zju.edu.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
Hm_lvt_fe30bbc1ee45421ec1679d1b8d8f8453=1540035806,1540035906,1540035961,15
40036067; _pk_id.3.331d=14cff805b92dd47a.
1540035808.1.1540036068.1540035808.;
Hm_lvt_39dcd5bd05965dcfa70b1d2457c6dcae=1540035808,1540035907,1540035961,15
40036068

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 09:09:28 GMT
Server: Apache/2.2.31 (Unix) DAV/2 mod_jk/1.2.23
Last-Modified: Mon, 21 Aug 2017 03:22:50 GMT
ETag: "2c0b00-f071-5573afe511680"
Accept-Ranges: bytes
Content-Length: 61553
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/css
```

会话 4：

```
GET /_upload/article/images/1f/d4/7bd7a2ab45d8be779ad0d7625aaa/
3a90a4d0-045f-4818-b0c5-bd20c43e06a6.jpg HTTP/1.1
Host: www.zju.edu.cn
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.67 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://www.zju.edu.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
Hm_lvt_fe30bbc1ee45421ec1679d1b8d8f8453=1540035806,1540035906,1540035961,15
40036067; _pk_id.3.331d=14cff805b92dd47a.
1540035808.1.1540036068.1540035808.;
Hm_lvt_39dcd5bd05965dcfa70b1d2457c6dcae=1540035808,1540035907,1540035961,15
40036068

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 09:09:29 GMT
Server: Apache/2.2.31 (Unix) DAV/2 mod_jk/1.2.23
Last-Modified: Wed, 31 Oct 2018 09:31:31 GMT
ETag: "3e2d0d-4f0f4-57982f7a442c0"
Accept-Ranges: bytes
Content-Length: 323828
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: image/jpeg
```

会话 5：

```
r..hEg?-Y.c}.."7.h....L....i..>..cC.....N..E...Ih..GET /_upload/tpl/
00/14/20/template20/images/xss.jpg HTTP/1.1
Host: www.zju.edu.cn
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.67 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://www.zju.edu.cn/_upload/tpl/00/14/20/template20/style/
common.css
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
Hm_lvt_fe30bbc1ee45421ec1679d1b8d8f8453=1540035806,1540035906,1540035961,15
40036067; _pk_id.3.331d=14cff805b92dd47a.
1540035808.1.1540036068.1540035808.;
Hm_lvt_39dcd5bd05965dcfa70b1d2457c6dcae=1540035808,1540035907,1540035961,15
40036068

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 09:09:36 GMT
Server: Apache/2.2.31 (Unix) DAV/2 mod_jk/1.2.23
Last-Modified: Wed, 18 Oct 2017 02:14:29 GMT
ETag: "302b6a-a86-55bc8ccac8b40"
Accept-Ranges: bytes
Content-Length: 2694
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: image/jpeg
```

会话 6：

```
..&.y..-.W@..O...L0.s.mn.S.u..&....y|..V...zy<|<...GET /_upload/tpl/
00/14/20/template20/images/li1.gif HTTP/1.1
Host: www.zju.edu.cn
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.67 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://www.zju.edu.cn/_upload/tpl/00/14/20/template20/style/
common.css
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
Hm_lvt_fe30bbc1ee45421ec1679d1b8d8f8453=1540035806,1540035906,1540035961,15
40036067; _pk_id.3.331d=14cff805b92dd47a.
1540035808.1.1540036068.1540035808.;
Hm_lvt_39dcd5bd05965dcfa70b1d2457c6dcae=1540035808,1540035907,1540035961,15
40036068

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 09:09:36 GMT
Server: Apache/2.2.31 (Unix) DAV/2 mod_jk/1.2.23
Last-Modified: Fri, 23 Jun 2017 07:03:22 GMT
ETag: "3010f9-476-5529b325e4280"
Accept-Ranges: bytes
Content-Length: 1142
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: image/gif
```

会话 7：

```
..
          .........!.......,.......... 0...YD.U".;GET /_upload/tpl/
00/14/20/template20/images/news_top_bg.png HTTP/1.1
Host: www.zju.edu.cn
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.67 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://www.zju.edu.cn/_upload/tpl/00/14/20/template20/style/
default.css
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
Hm_lvt_fe30bbc1ee45421ec1679d1b8d8f8453=1540035806,1540035906,1540035961,15
40036067; _pk_id.3.331d=14cff805b92dd47a.
1540035808.1.1540036068.1540035808.;
Hm_lvt_39dcd5bd05965dcfa70b1d2457c6dcae=1540035808,1540035907,1540035961,15
40036068

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 09:09:36 GMT
Server: Apache/2.2.31 (Unix) DAV/2 mod_jk/1.2.23
Last-Modified: Fri, 23 Jun 2017 07:03:22 GMT
ETag: "3010ad-563-5529b325e4280"
Accept-Ranges: bytes
Content-Length: 1379
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: image/png
```

会话 8：

```
9w....)....IEND.B`.GET /_upload/article/images/ba/bb/
4b302c8b4c3c941e6c670f47b191/51f659a4-0a12-4ccc-99ca-a0a5dee7df6e_s.jpg
HTTP/1.1
Host: www.zju.edu.cn
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.67 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://www.zju.edu.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
Hm_lvt_fe30bbc1ee45421ec1679d1b8d8f8453=1540035806,1540035906,1540035961,15
40036067; _pk_id.3.331d=14cff805b92dd47a.
1540035808.1.1540036068.1540035808.;
Hm_lvt_39dcd5bd05965dcfa70b1d2457c6dcae=1540035808,1540035907,1540035961,15
40036068

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 09:09:36 GMT
Server: Apache/2.2.31 (Unix) DAV/2 mod_jk/1.2.23
Last-Modified: Sat, 27 Oct 2018 14:54:47 GMT
ETag: "a833ac-197a8-57937045e3bc0"
Accept-Ranges: bytes
Content-Length: 104360
Keep-Alive: timeout=5, max=93
Connection: Keep-Alive
Content-Type: image/jpeg
```

会话 9：

```
(.Qv.g.......P.d.kX...*....z.g..GET /_upload/article/images/8d/
d0/7bb02113480abb29ea2f3a4dd99c/dc162eea-d4d2-41c4-a2b9-cf0f04765bb3.jpg
HTTP/1.1
Host: www.zju.edu.cn
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.67 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://www.zju.edu.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
Hm_lvt_39dcd5bd05965dcfa70b1d2457c6dcae=1540035808,1540035907,1540035961,15
40036068;
Hm_lvt_fe30bbc1ee45421ec1679d1b8d8f8453=1540035906,1540035961,1540036067,15
41063373; Hm_lpvt_fe30bbc1ee45421ec1679d1b8d8f8453=1541063373; _pk_id.
3.331d=14cff805b92dd47a.1540035808.2.1541063375.1541063375.; _pk_ses.
3.331d=*

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 09:09:38 GMT
Server: Apache/2.2.31 (Unix) DAV/2 mod_jk/1.2.23
Last-Modified: Thu, 04 Oct 2018 08:59:52 GMT
ETag: "583956-2c4af-5776360bcb200"
Accept-Ranges: bytes
Content-Length: 181423
Keep-Alive: timeout=5, max=92
Connection: Keep-Alive
Content-Type: image/jpeg
```

会话 10：

```
..d`..|...g........j.i.0>E...$....yk.z`zP..Z19U<.....GET /_upload/article/
images/e1/71/c3e52150469b8361d6883b138359/2e04b5fa-
cf72-4f51-9f0d-5d33032aa4ca.jpg HTTP/1.1
Host: www.zju.edu.cn
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.67 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://www.zju.edu.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
Hm_lvt_39dcd5bd05965dcfa70b1d2457c6dcae=1540035808,1540035907,1540035961,15
40036068;
Hm_lvt_fe30bbc1ee45421ec1679d1b8d8f8453=1540035906,1540035961,1540036067,15
41063373; Hm_lpvt_fe30bbc1ee45421ec1679d1b8d8f8453=1541063373; _pk_id.
3.331d=14cff805b92dd47a.1540035808.2.1541063375.1541063375.; _pk_ses.
3.331d=*

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 09:09:41 GMT
Server: Apache/2.2.31 (Unix) DAV/2 mod_jk/1.2.23
Last-Modified: Mon, 17 Sep 2018 08:18:49 GMT
ETag: "e04037-2312d-5760cd2a0ec40"
Accept-Ranges: bytes
Content-Length: 143661
Keep-Alive: timeout=5, max=91
Connection: Keep-Alive
Content-Type: image/jpeg
```

会话 11：

```
y..8....u.....c.@.<......4.9M.-..4.
          .H....=(.ha.3R1.....Re.SHL\...k..P&...GET /_upload/article/
images/da/e1/f0e4b05b4febad93541f91f4958f/a9fb6e2b-
a6dd-43fa-9c14-62de3f18cd31_s.jpg HTTP/1.1
Host: www.zju.edu.cn
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.67 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://www.zju.edu.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
Hm_lvt_39dcd5bd05965dcfa70b1d2457c6dcae=1540035808,1540035907,1540035961,15
40036068;
Hm_lvt_fe30bbc1ee45421ec1679d1b8d8f8453=1540035906,1540035961,1540036067,15
41063373; Hm_lpvt_fe30bbc1ee45421ec1679d1b8d8f8453=1541063373; _pk_id.
3.331d=14cff805b92dd47a.1540035808.2.1541063375.1541063375.; _pk_ses.
3.331d=*

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 09:09:42 GMT
Server: Apache/2.2.31 (Unix) DAV/2 mod_jk/1.2.23
Last-Modified: Sat, 29 Sep 2018 05:43:08 GMT
ETag: "1ce4786-18b6c-576fc0bf51300"
Accept-Ranges: bytes
Content-Length: 101228
Keep-Alive: timeout=5, max=90
Connection: Keep-Alive
Content-Type: image/jpeg
```

六、 实验结果分析与思考

- 如果只想捕获某个特定 WEB 服务器 IP 地址相关的 HTTP 数据包，捕获过滤器应该怎么写？

  host x.x.x.x and port 80 and http

- Ping 发送的是什么类型的协议数据包？什么情况下会出现 ARP 数据包？ Ping 一个域名和 Ping 一个 IP 地址出现的数据包有什么不同？

  （1）ICMP 协议

  （2）Ping 域名时会出现 ARP 数据包

  （3）Ping 域名时会出现 ARP 数据包，Ping 一个 IP 地址时不会出现 ARP 包

- Tracert/Traceroute 发送的是什么类型的协议数据包，整个路由跟踪过程是如何进行的？

  （1）ICMP 协议

  （2）路由追踪过程直接是用 ping 来实现的，但是这个 ping 的 TTL 值在 3 个包后

增大 1，不可达或者超时后返回星号，继续下一个 TTL 的包的发送，一直到达默认设置的 30 跳

- 如何理解 TCP 连接和 HTTP 会话？他们之间存在什么关系？

TCP 连接：为实现数据的可靠传输，TCP 要在应用进程间建立传输连接。它是在两个传输用户之间建立一种逻辑联系，使得通信双方都确认对方为自己的传输连接端点。

HTTP 会话：HTTP 是一个简单的请求-响应协议，它指定了客户端可能发送给服务器什么样的消息以及得到什么样的响应。

HTTP 会话运行在 TCP 之上，只有当 TCP 连接释放之后 HTTP 会话才关闭。

- DNS 为什么选择使用 UDP 协议进行传输？而 HTTP 为什么选择使用 TCP 协议？

UDP 协议并不提供数据传送的保证机制，将安全和排序等功能移交给上层应用来完成，极大降低了执行时间，使速度得到了保证，使用 udp 传输，不用经过 TCP 三次握手，这样 DNS 服务器负载更低，响应更快；TCP 协议中包含了专门的传递保证机制，当数据接收方收到发送方传来的信息时，会自动向发送方发出确认消息；发送方只有在接收到该确认消息之后才继续传送其它信息，否则将一直等待直到收到确认信息为止，具有较高的可靠性。HTTP 需要较高的可靠性，UDP 符合 HTTP 的要求。

七、 讨论、心得

在完成本实验后，你可能会有很多待解答的问题，你可以把它们记在这里，接下来的学习中，你也许会逐渐得到答案的，同时也可以让老师了解到你有哪些困惑，老师在课堂可以安排针对性地解惑。等到课程结束后，你再回头看看这些问题时你或许会有不同的见解：

在台式机上面抓包的时候，PART3 抓不到包，也不知道原因出在了那里，总体来说，实验还是比较简单的，按照实验报告的说明完全可以做下来，但是因为是第一次做，做的比较慢。

在实验过程中你可能会遇到的困难，并得到了宝贵的经验教训，请把它们记录下来，提供给其他人参考吧：

建议安装低版本的软件，抓的包小一点

你对本实验安排有哪些更好的建议呢？欢迎献计献策：

无