中国矿业大学计算机学院

2019 级本科生计算机网络实验报告

实验内容 协议报文分析

学生姓名 许万鹏 学 号 05191643

专业班级 信息安全 19-01 班

学 院 计算机科学与技术学院

任课教师 顾 军

评语	

综合成绩: 任课教师签字:

年 月 日

实验编号：03

实验名称：协议报文分析

实验内容：

（1）分别获取不同互联网访问情形下的本机网卡数据包；过滤捕获和过滤显示不同条件的数据包。

（2）获取 ARP 协议数据单元，进行报文格式解析。

（3）获取 ping、tracert、nslookup 命令对应的交互数据，进行报文格式解析。

（4）针对不同互联网应用的执行过程进行抓包，对 DNS 服务、WWW 服务、Email 服务、QQ 通信、微信、迅雷文件下载等六种不同网络应用服务访问情形下的数据包进行逐层分析，给出各层协议的主要参数及意义。

实验要求：

（1）运用抓包工具，实时抓包，记录包状态变化；

（2）给出不同应用情境下的不同层次数据包的分析结果，对每种应用服务的协议数据需要从应用层、运输层、网络层、数据链路层四个层次对相关协议格式、字段取值进行解析。

（3）对基于 TCP 的应用层协议，需要获取 TCP 协议的工作过程，验证连接建立的三次握手过程、四次挥手过程以及滑动窗口工作机制。

（4）验证 IP 数据包、TCP 报文段和 UDP 数据报的**校验和**。

（5）验证数据链路层的 CRC **冗余校验**。

预习要求：

提前通过互联网或在实验室开始实验前登录实验管理服务器，点击预习链接，阅览或下载实验指导书——预习\网络协议\进阶-IP 分组基本报文分析。

操作与观察：

正确按照实验指导书步骤操作，观察记录下操作结果。

实验报告要求：

（1） 按照实验要求，完成全部实验内容

（2） 在标准实验报告书上填写全部实验操作记录和观察结果

（3） 登录实验管理服务器，提交实验报告电子档。

（4） 提交纸质版实验报告。

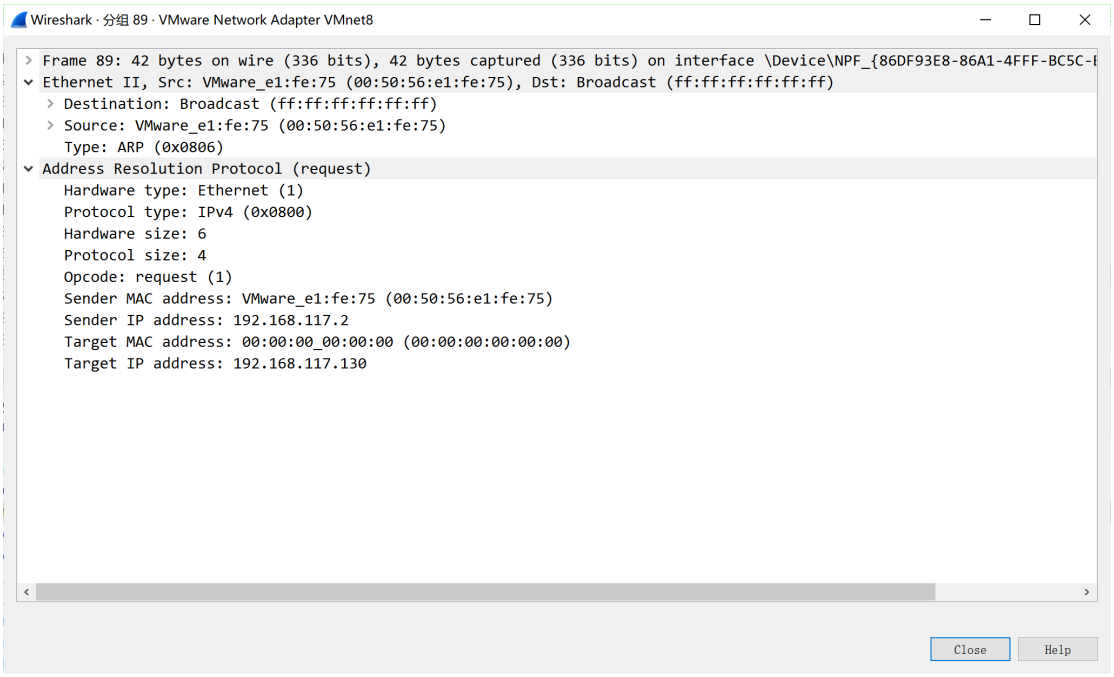
实验报告内容：

一、分别获取不同互联网访问情形下的本机网卡数据包；过滤捕获和过滤显示不同条件的数据包

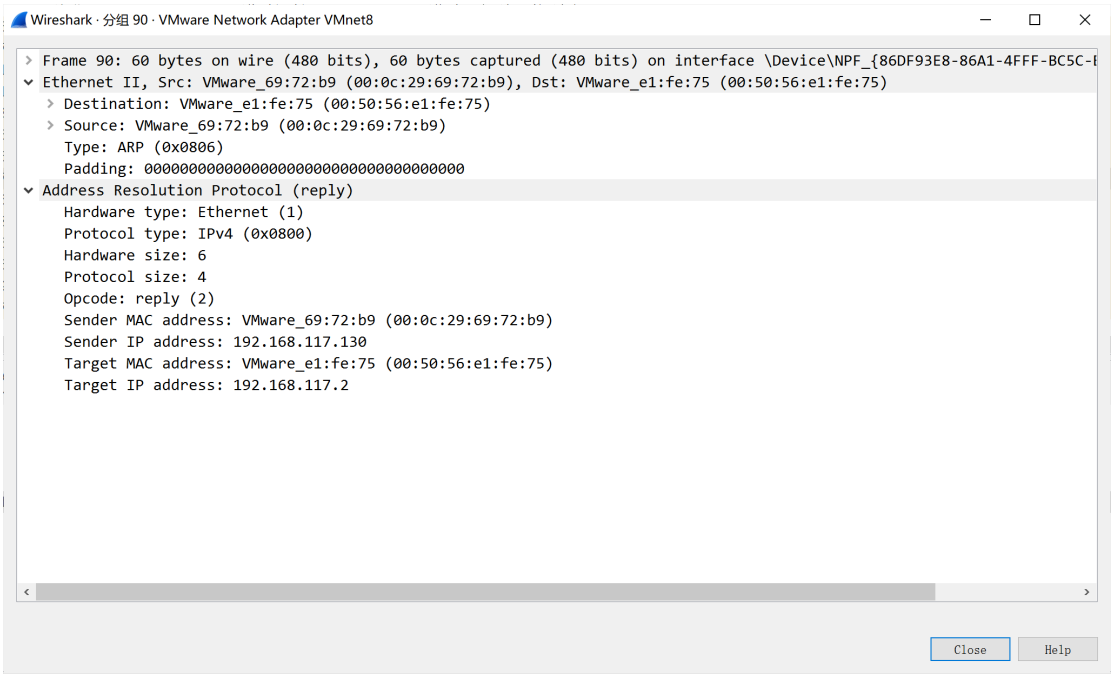
详见以下内容。

二、获取 ARP 协议数据单元，进行报文格式解析。

Request



Reply



Ethernet II 数据帧的格式：

Frame	物理层的数据帧概况
Ethernet II	数据链路层以太网帧头部信息
Destination	表示目的地址，此处为广播
Source	表示源地址
Type	表示上层时 ARP 协议

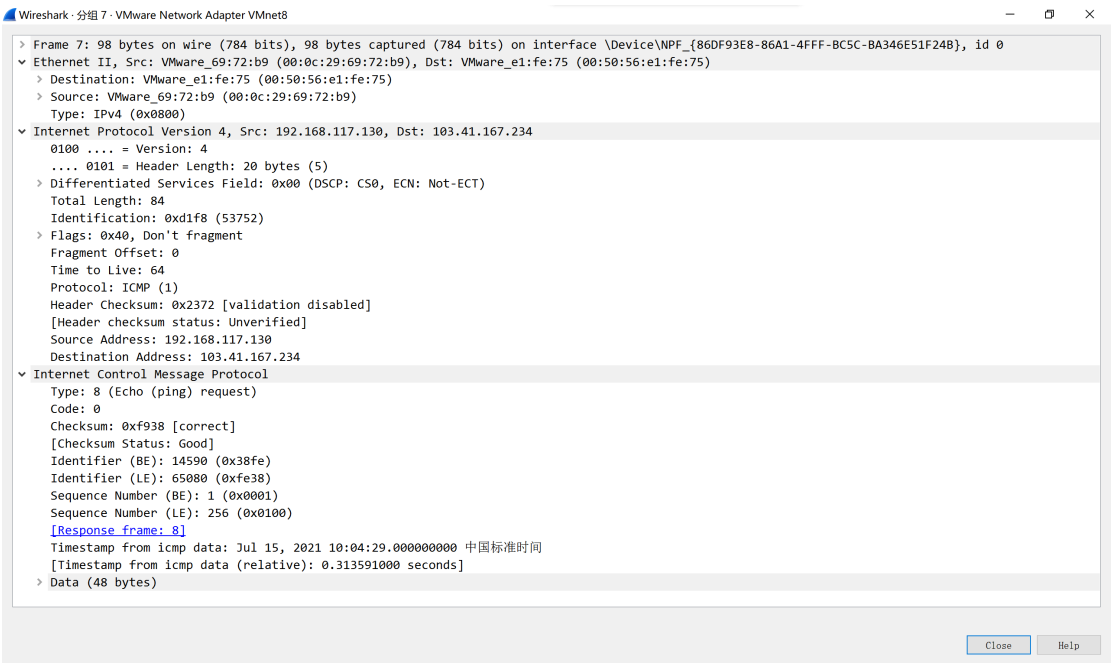
ARP Request/Reply

Hardware type	硬件类型，此处为 1 表示以太网
Protocol type	协议类型，此处为 IPv4
Hardware size	硬件地址长度
Protocol size	协议长度
Opcode	操作码
Sender MAC address	发送主机的 MAC 地址
Sender IP address	发送主机的 IP 地址
Target MAC address	目标主机的 MAC 地
Target IP address	目标主机的 IP 地址

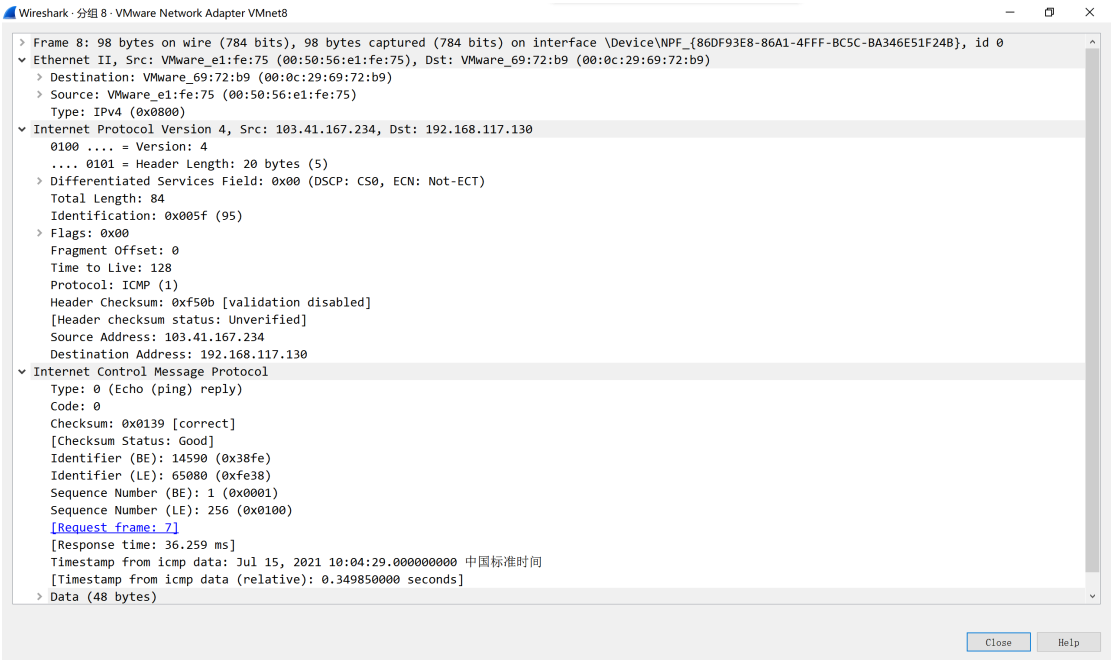
三、获取 ping、tracert、nslookup 命令对应的交互数据，进行报文格式解析。

3.1 PING

REQUSET



REPLY



Ethernet II 数据帧的格式：

Frame	物理层的数据帧概况
Ethernet II	数据链路层以太网帧头部信息
Destination	表示目的地址，此处为广播
Source	表示源地址
Type	表示上层时 ARP 协议

IP 数据包的信息：

Version	表示版本
Header Length:	表示 n 个以 32 bit 为单位的 word，即 4n 字节。
Time to live:	生存时间
Protocol:	1，表示 ICMP
Source	源 IP 地址
Destination	目的 IP 地址

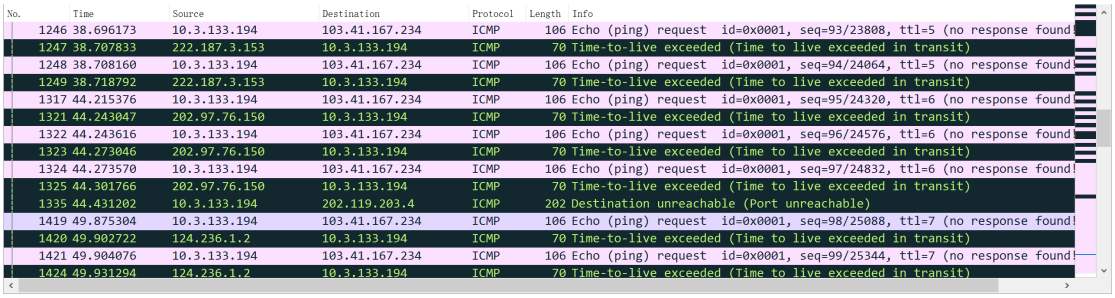
ICMP 数据包的格式如下：

Type↵	Code↵	Checksum↵
Identifier↵		Seq Num↵
Data ↵		

Type:	1 字节，表示特定类型的 ICMP 报文
Code	1 字节，进一步细分 ICMP 的类型
Checksum	2 字节，表示校验和
Identifier	2 字节，匹配 Request/Reply 的标识符
Seq Num	2 字节，匹配 Request/Reply 的序列号
Data	数据部分

3.2 TRACERT

格式:

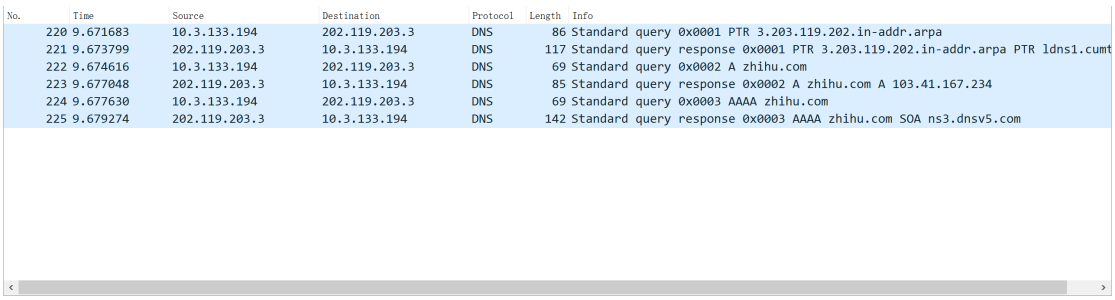


No.	Time	Source	Destination	Protocol	Length	Info
1246	38.696173	10.3.133.194	103.41.167.234	ICMP	106	Echo (ping) request id=0x0001, seq=93/23808, ttl=5 (no response found!
1247	38.707833	222.187.3.153	10.3.133.194	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1248	38.708160	10.3.133.194	103.41.167.234	ICMP	106	Echo (ping) request id=0x0001, seq=94/24064, ttl=5 (no response found!
1249	38.718792	222.187.3.153	10.3.133.194	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1317	44.215376	10.3.133.194	103.41.167.234	ICMP	106	Echo (ping) request id=0x0001, seq=95/24320, ttl=6 (no response found!
1321	44.243047	202.97.76.150	10.3.133.194	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1322	44.243616	10.3.133.194	103.41.167.234	ICMP	106	Echo (ping) request id=0x0001, seq=96/24576, ttl=6 (no response found!
1323	44.273046	202.97.76.150	10.3.133.194	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1324	44.273570	10.3.133.194	103.41.167.234	ICMP	106	Echo (ping) request id=0x0001, seq=97/24832, ttl=6 (no response found!
1325	44.301766	202.97.76.150	10.3.133.194	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1335	44.431202	10.3.133.194	202.119.203.4	ICMP	202	Destination unreachable (Port unreachable)
1419	49.875304	10.3.133.194	103.41.167.234	ICMP	106	Echo (ping) request id=0x0001, seq=98/25088, ttl=7 (no response found!
1420	49.902722	124.236.1.2	10.3.133.194	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1421	49.904076	10.3.133.194	103.41.167.234	ICMP	106	Echo (ping) request id=0x0001, seq=99/25344, ttl=7 (no response found!
1424	49.931294	124.236.1.2	10.3.133.194	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

由于 tracrt 命令的底层协议与 ping 的底层协议相同（都是 ICMP）,故不做具体分析。

3.3 nslookup

格式:



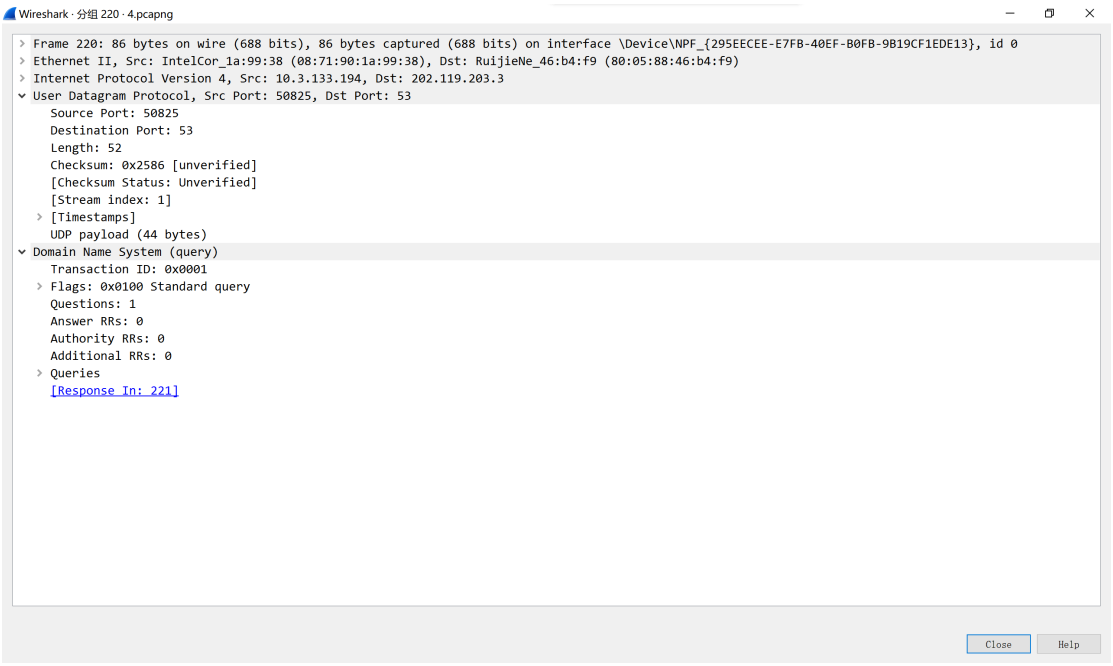
No.	Time	Source	Destination	Protocol	Length	Info
220	9.671683	10.3.133.194	202.119.203.3	DNS	86	Standard query 0x0001 PTR 3.203.119.202.in-addr.arpa
221	9.673799	202.119.203.3	10.3.133.194	DNS	117	Standard query response 0x0001 PTR 3.203.119.202.in-addr.arpa PTR ldns1.cumt
222	9.674616	10.3.133.194	202.119.203.3	DNS	69	Standard query 0x0002 A zhihu.com
223	9.677048	202.119.203.3	10.3.133.194	DNS	85	Standard query response 0x0002 A zhihu.com A 103.41.167.234
224	9.677630	10.3.133.194	202.119.203.3	DNS	69	Standard query 0x0003 AAAA zhihu.com
225	9.679274	202.119.203.3	10.3.133.194	DNS	142	Standard query response 0x0003 AAAA zhihu.com SOA ns3.dnsv5.com

其中,

第二次 DNS 请求查询 www.zhihu.com 域名对应的 IP4 地址（A 代表 IP4）;

第三次 DNS 请求查询 www.zhihu.com 域名对应的 IP6 地址（AAAA 代表 IP6）；

Query：



Response：

UDP 数据帧分析

Source Port	源端口号
Destination Port	目的端口号
Length	长度字段
Checksum	校验和

DNS 报文分析

Transacti ID	标识字段
Flags	标志字段
Question	问题数
Answer RRs	回答资源记录数
Authority RRs	授权资源记录数
Additional RRs	附加资源记录数

四、针对不同互联网应用的执行过程进行抓包

4.1 DNS 服务

操作及 PacketList:同 3.3

现给出第二次查询过程分析

```
> Frame 222: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{295EECEE-E7FB-40EF-B0FB-9B19CF1EDE13}, id 0
> Ethernet II, Src: IntelCor_1a:99:38 (08:71:90:1a:99:38), Dst: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
> Internet Protocol Version 4, Src: 10.3.133.194, Dst: 202.119.203.3
> User Datagram Protocol, Src Port: 50826, Dst Port: 53
> Domain Name System (query)
```

① 数据链路层

```
Ethernet II, Src: IntelCor_1a:99:38 (08:71:90:1a:99:38), Dst: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
  Destination: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
      Address: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: IntelCor_1a:99:38 (08:71:90:1a:99:38)
      Address: IntelCor_1a:99:38 (08:71:90:1a:99:38)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

目的地址	80:05:88:46:b4:f9
源地址	08:71:90:1a:99:38
上层协议	IPv4

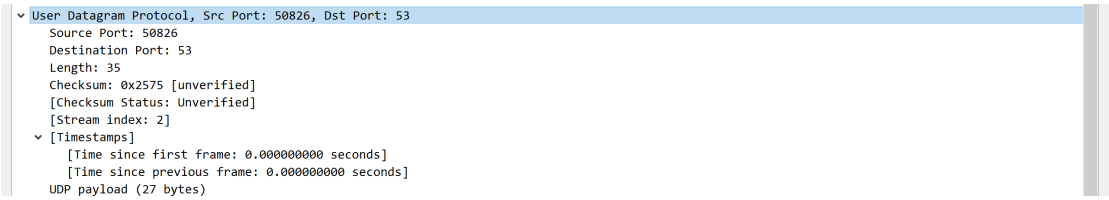
② 网络层

```
Internet Protocol Version 4, Src: 10.3.133.194, Dst: 202.119.203.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 55
    Identification: 0xb37b (45947)
  Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.3.133.194
    Destination Address: 202.119.203.3
```

版本	4
首部长度	20 字节

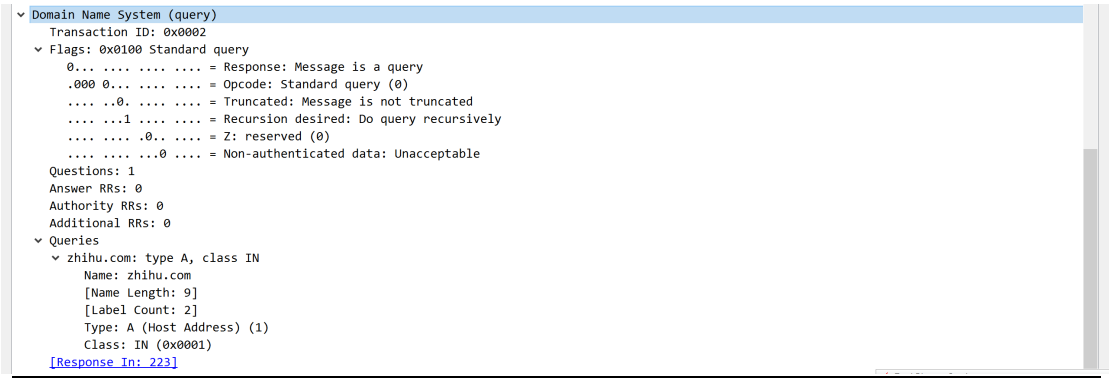
总长度	55 字节
标识	0Xb37B
分片否?	不分片
生存时间	128 跳
协议	UDP
源 IP 地址	10.0.133.194
目的 IP 地址	202.119.203.3

③ 运输层



源端口号	50826
目的端口号	53
长度	35
检验和	0x2575

④ 应用层

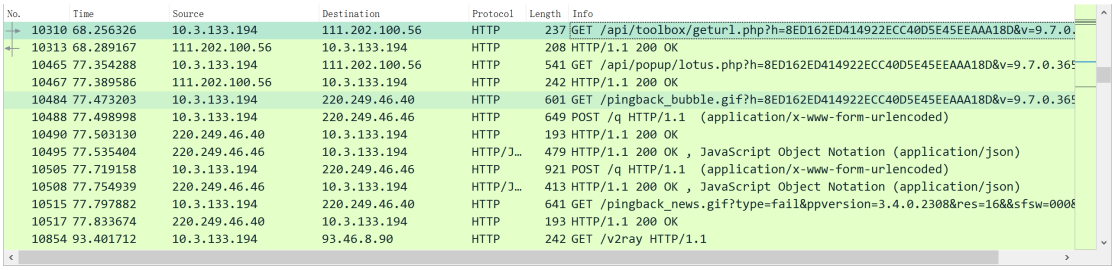


标识字段	0x0002
标志字段	0x0100
问题数	1
回答资源记录数	0
授权资源记录数	0

附加资源记录数	0

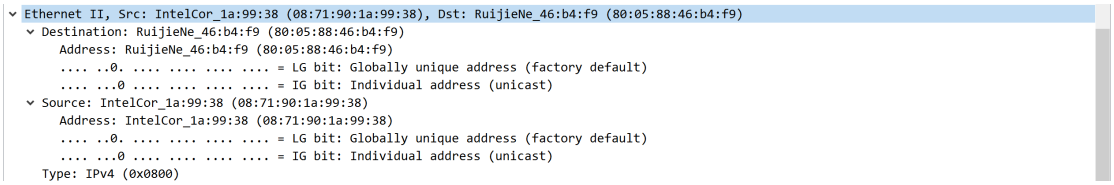
4.2 WWW 服务

PacketList:



No.	Time	Source	Destination	Protocol	Length	Info
10310	68.256326	10.3.133.194	111.202.100.56	HTTP	237	GET /api/toolbox/geturl.php?h=8ED162ED414922ECC40D5E45EEAAA18D&v=9.7.0.
10313	68.289167	111.202.100.56	10.3.133.194	HTTP	208	HTTP/1.1 200 OK
10465	77.354288	10.3.133.194	111.202.100.56	HTTP	541	GET /api/popup/lotus.php?h=8ED162ED414922ECC40D5E45EEAAA18D&v=9.7.0.365
10467	77.389586	111.202.100.56	10.3.133.194	HTTP	242	HTTP/1.1 200 OK
10484	77.473203	10.3.133.194	220.249.46.40	HTTP	601	GET /pingback_bubble.gif?h=8ED162ED414922ECC40D5E45EEAAA18D&v=9.7.0.365
10488	77.498998	10.3.133.194	220.249.46.46	HTTP	649	POST /q HTTP/1.1 (application/x-www-form-urlencoded)
10490	77.503130	220.249.46.40	10.3.133.194	HTTP	193	HTTP/1.1 200 OK
10495	77.535404	220.249.46.46	10.3.133.194	HTTP/J…	479	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
10505	77.719158	10.3.133.194	220.249.46.46	HTTP	921	POST /q HTTP/1.1 (application/x-www-form-urlencoded)
10508	77.754939	220.249.46.46	10.3.133.194	HTTP/J…	413	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
10515	77.797882	10.3.133.194	220.249.46.40	HTTP	641	GET /pingback_news.gif?type=fail&ppversion=3.4.0.2308&res=16&&sfsw=0008
10517	77.833674	220.249.46.40	10.3.133.194	HTTP	193	HTTP/1.1 200 OK
10854	93.401712	10.3.133.194	93.46.8.90	HTTP	242	GET /v2ray HTTP/1.1

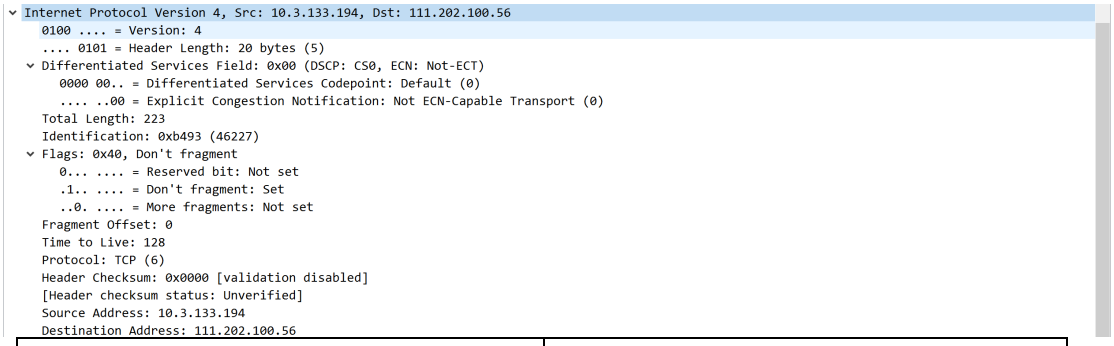
① 数据链路层



```
Ethernet II, Src: IntelCor_1a:99:38 (08:71:90:1a:99:38), Dst: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
  Destination: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
      Address: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: IntelCor_1a:99:38 (08:71:90:1a:99:38)
      Address: IntelCor_1a:99:38 (08:71:90:1a:99:38)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

目的地址	80:05:88:46:b4:f9
源地址	08:71:90:1a:99:38
上层协议	IPv4

② 网络层

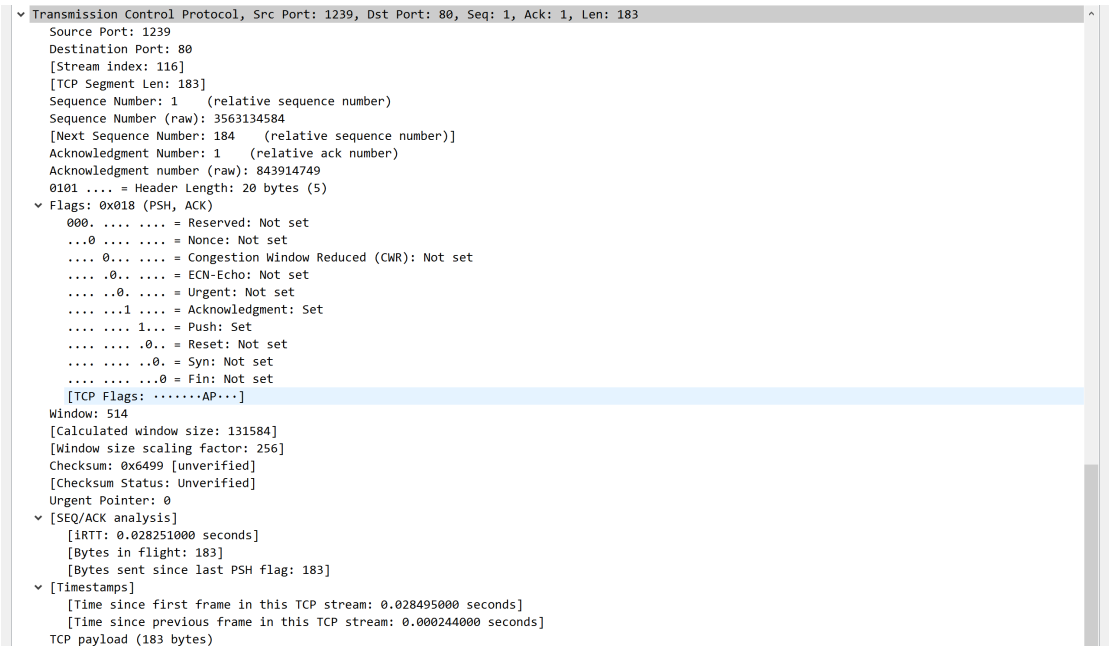


```
Internet Protocol Version 4, Src: 10.3.133.194, Dst: 111.202.100.56
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 223
    Identification: 0xb493 (46227)
  Flags: 0x40, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.3.133.194
    Destination Address: 111.202.100.56
```

版本	4
首部长度	20 字节
总长度	223 字节
标识	0XB493
分片否?	不分片
生存时间	128 跳
协议	TCP

源 IP 地址	10.3.133.194
目的 IP 地址	111.202.100.56

③ 运输层



源端口号	1239
目的端口号	80
seq	1
ack	1
rwnd	514

④ 应用层

方法	GET
URL	如图
版本	HTTP/1.1

4.3 Email 服务

PacketList:

No.	Time	Source	Destination	Protocol	Length	Info
1331	40.244491	123.126.97.5	10.3.133.194	SMTP	119	S: 220 163.com Anti-spam GT for Coremail System (163com[20141201])
1936	53.638225	10.3.133.194	123.126.97.5	SMTP	58	C: DATA fragment, 4 bytes
1942	53.672527	123.126.97.5	10.3.133.194	SMTP	90	S: 502 Error: command not implemented
2059	58.725483	10.3.133.194	123.126.97.5	SMTP	65	C: helo lalal
2060	58.759749	123.126.97.5	10.3.133.194	SMTP	62	S: 250 OK
2259	67.538352	10.3.133.194	123.126.97.5	SMTP	65	C: auth login
2261	67.572295	123.126.97.5	10.3.133.194	SMTP	72	S: 334 dXNlcm5hbWU6
5061	124.502637	10.3.133.194	123.126.97.5	SMTP	83	C: User: [redacted]M5OUAxNjMuY29t
5062	124.539591	123.126.97.5	10.3.133.194	SMTP	72	S: 334 UGFzc3dvcmQ6
6108	142.911861	10.3.133.194	123.126.97.5	SMTP	79	C: Pass: [redacted]UVlaUFRUSg==
6110	142.963975	123.126.97.5	10.3.133.194	SMTP	85	S: 235 Authentication successful
7237	194.760338	10.3.133.194	123.126.97.5	SMTP	89	C: mail from: <xuwanpeng4399@163.com>
7238	194.800124	123.126.97.5	10.3.133.194	SMTP	67	S: 250 Mail OK
10427	289.171589	10.3.133.194	123.126.97.5	SMTP	81	C: rcpt to: <xwp@cumt.edu.cn>
10430	289.208333	123.126.97.5	10.3.133.194	SMTP	67	S: 250 Mail OK
10499	291.371708	10.3.133.194	123.126.97.5	SMTP	59	C: data
10500	291.406445	123.126.97.5	10.3.133.194	SMTP	91	S: 354 End data with <CR><LF>.<CR><LF>
12242	313.471195	10.3.133.194	123.126.97.5	SMTP	75	C: DATA fragment, 21 bytes
13187	325.385996	10.3.133.194	123.126.97.5	SMTP	83	C: DATA fragment, 29 bytes
13428	337.657696	10.3.133.194	123.126.97.5	SMTP	67	C: DATA fragment, 13 bytes
14244	351.360067	10.3.133.194	123.126.97.5	SMTP	55	C: DATA fragment, 1 byte
14462	362.433086	10.3.133.194	123.126.97.5	SMTP	64	C: DATA fragment, 10 bytes
14648	370.983067	10.3.133.194	123.126.97.5	SMTP	62	C: DATA fragment, 8 bytes
14807	379.383156	10.3.133.194	123.126.97.5	SMTP	67	C: DATA fragment, 13 bytes
14892	384.809202	10.3.133.194	123.126.97.5	SMTP	56	C: DATA fragment, 2 bytes
14899	384.857094	123.126.97.5	10.3.133.194	SMTP	221	S: 554 DT:SPM 163 smtp5,HdxpCgC3s6JUhd1gSG1LCA--.44286S2 1625130669,please s
19517	453.383760	10.3.133.194	123.126.97.5	SMTP	55	C: DATA fragment, 1 byte
19518	453.421382	123.126.97.5	10.3.133.194	SMTP	88	S: 421 closing transmission channel

① 数据链路层

```
Ethernet II, Src: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9), Dst: IntelCor_1a:99:38 (08:71:90:1a:99:38)
  Destination: IntelCor_1a:99:38 (08:71:90:1a:99:38)
      Address: IntelCor_1a:99:38 (08:71:90:1a:99:38)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
      Address: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

目的地址	08:71:90:1a:99:38
源地址	80:05:88:46:b4:f9
上层协议	IPv4

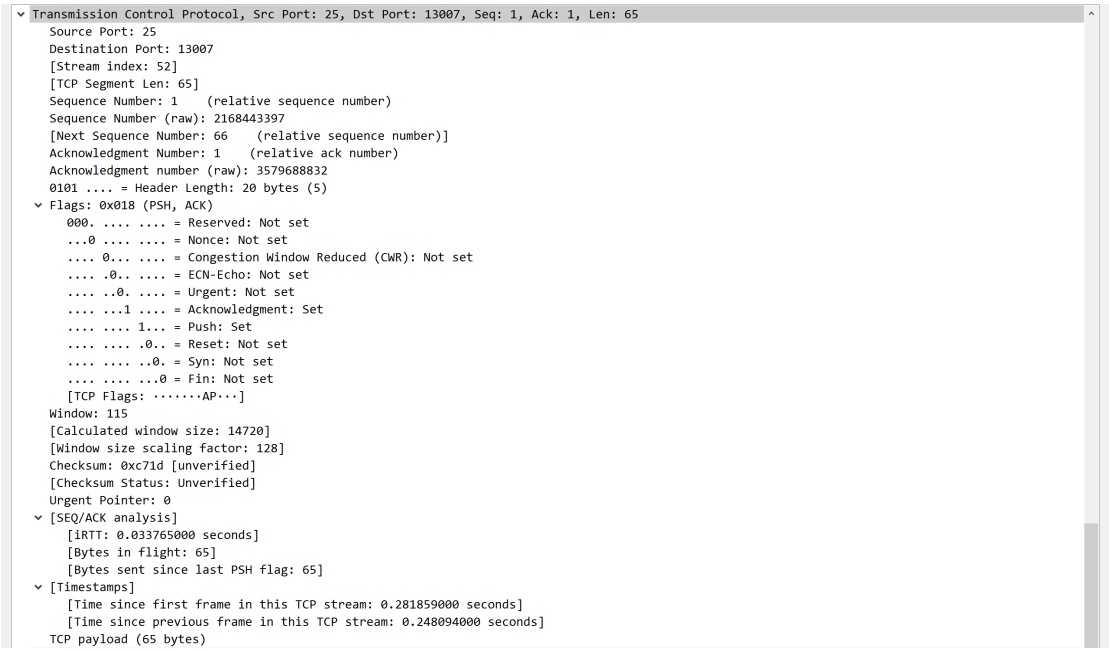
② 网络层

```
Internet Protocol Version 4, Src: 123.126.97.5, Dst: 10.3.133.194
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 105
    Identification: 0x2ead (11949)
  Flags: 0x40, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 51
    Protocol: TCP (6)
    Header Checksum: 0xac99 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 123.126.97.5
    Destination Address: 10.3.133.194
```

版本	4
首部长度	20 字节

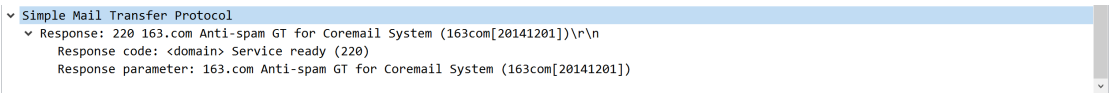
总长度	105
标识	0x2EAD
分片否?	不分片
生存时间	51 跳
协议	TCP
源 IP 地址	123.126.97.5
目的 IP 地址	10.3.133.194

③ 运输层



源端口号	25
目的端口号	13007
seq	1
ack	1
rwnd	115

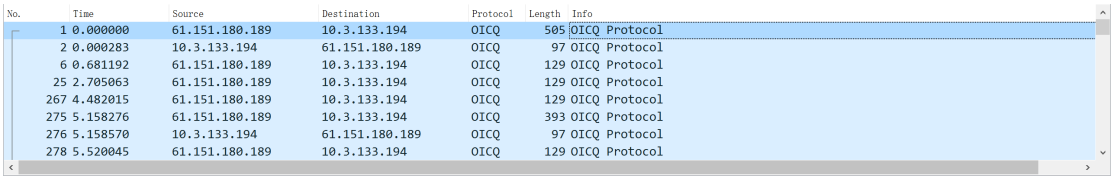
④ 应用层



响应字段	220 (Authentication failed)

4.4 QQ 通信

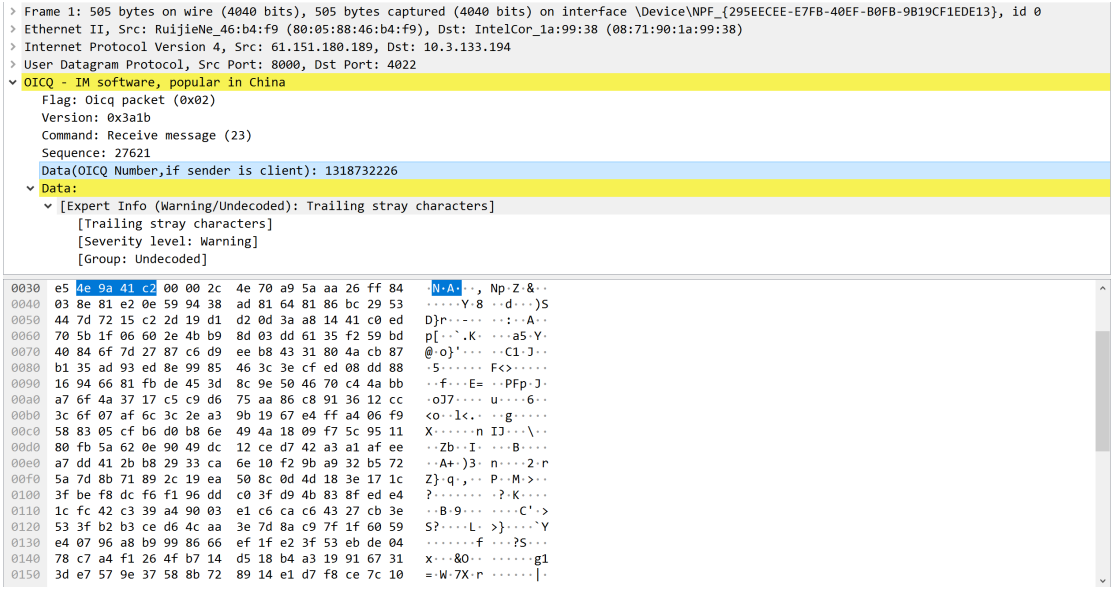
PacketList:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	61.151.180.189	10.3.133.194	OICQ	505	OICQ Protocol
2	0.000283	10.3.133.194	61.151.180.189	OICQ	97	OICQ Protocol
6	0.681192	61.151.180.189	10.3.133.194	OICQ	129	OICQ Protocol
25	2.705063	61.151.180.189	10.3.133.194	OICQ	129	OICQ Protocol
267	4.482015	61.151.180.189	10.3.133.194	OICQ	129	OICQ Protocol
275	5.158276	61.151.180.189	10.3.133.194	OICQ	393	OICQ Protocol
276	5.158570	10.3.133.194	61.151.180.189	OICQ	97	OICQ Protocol
278	5.520045	61.151.180.189	10.3.133.194	OICQ	129	OICQ Protocol

前四层略

应用层:

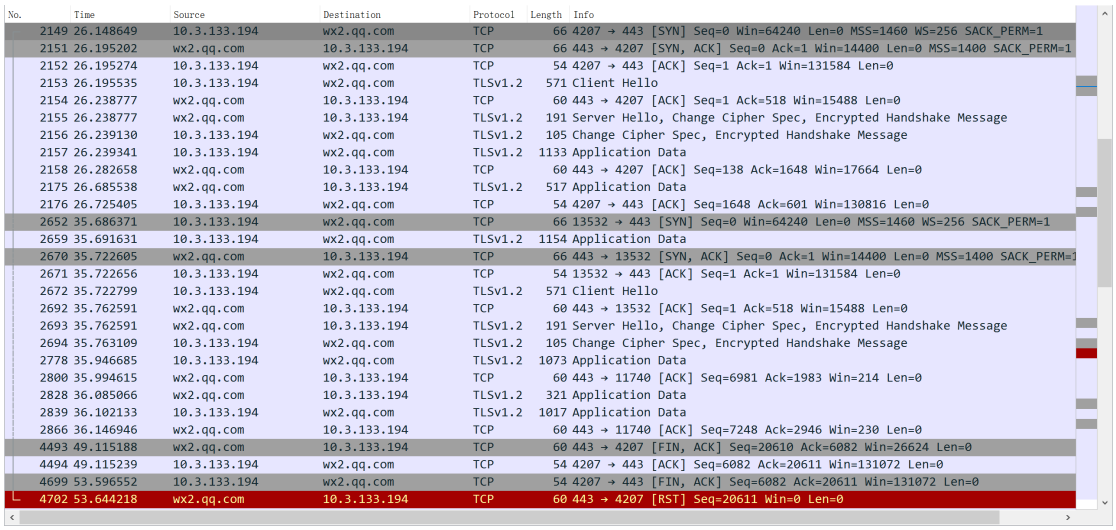


```
> Frame 1: 505 bytes on wire (4040 bits), 505 bytes captured (4040 bits) on interface \Device\NPF_{295EECEE-E7FB-40EF-B0FB-9B19CF1EDE13}, id 0
> Ethernet II, Src: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9), Dst: IntelCor_1a:99:38 (08:71:90:1a:99:38)
> Internet Protocol Version 4, Src: 61.151.180.189, Dst: 10.3.133.194
> User Datagram Protocol, Src Port: 8000, Dst Port: 4022
v OICQ - IM software, popular in China
    Flag: Oicq packet (0x02)
    Version: 0x3a1b
    Command: Receive message (23)
    Sequence: 27621
    Data(OICQ Number,if sender is client): 1318732226
  v Data:
    v [Expert Info (Warning/Undecoded): Trailing stray characters]
        [Trailing stray characters]
        [Severity level: Warning]
        [Group: Undecoded]
```

```
0030  e5 4e 9a 41 c2 00 00 2c  4e 70 a9 5a aa 26 ff 84   ·N·A···, Np·Z·&··
0040  03 8e 81 e2 0e 59 94 38  ad 81 64 81 86 bc 29 53   ·····Y·8 ··d···)S
0050  44 7d 72 15 c2 2d 19 d1  d2 0d 3a a8 14 41 c0 ed   D}r··-·· ··:··A··
0060  70 5b 1f 06 60 2e 4b b9  8d 03 dd 61 35 f2 59 bd   p[··`.K· ···a5·Y·
0070  40 84 6f 7d 27 87 c6 d9  ee b8 43 31 80 4a cb 87   @·o}'··· ··C1·J··
0080  b1 35 ad 93 ed 8e 99 85  46 3c 3e cf ed 08 dd 88   ·5····· F<>·····
0090  16 94 66 81 fb de 45 3d  8c 9e 50 46 70 c4 4a bb   ··f···E= ··PFp·J·
00a0  a7 6f 4a 37 17 c5 c9 d6  75 aa 86 c8 91 36 12 cc   ·oJ7···· u····6··
00b0  3c 6f 07 af 6c 3c 2e a3  9b 19 67 e4 ff a4 06 f9   <o··l<.· ··g·····
00c0  58 83 05 cf b6 d0 b8 6e  49 4a 18 09 f7 5c 95 11   X·····n IJ···\··
00d0  80 fb 5a 62 0e 90 49 dc  12 ce d7 42 a3 a1 af ee   ··Zb··I· ···B····
00e0  a7 dd 41 2b b8 29 33 ca  6e 10 f2 9b a9 32 b5 72   ··A+·)3· n····2·r
00f0  5a 7d 8b 71 89 2c 19 ea  50 8c 0d 4d 18 3e 17 1c   Z}·q·,·· P··M·>··
0100  3f be f8 dc f6 f1 96 dd  c0 3f d9 4b 83 8f ed e4   ?····· ·?·K····
0110  1c fc 42 c3 39 a4 90 03  e1 c6 ca c6 43 27 cb 3e   ··B·9··· ····C'·>
0120  53 3f b2 b3 ce d6 4c aa  3e 7d 8a c9 7f 1f 60 59   S?····L· >}····`Y
0130  e4 07 96 a8 b9 99 86 66  ef 1f e2 3f 53 eb de 04   ·····f ···?S···
0140  78 c7 a4 f1 26 4f b7 14  d5 18 b4 a3 19 91 67 31   x···&O·· ·····g1
0150  3d e7 57 9e 37 58 8b 72  89 14 e1 d7 f8 ce 7c 10   =·W·7X·r ·····|·
```

标志位	Oicq packet
版本号	0x31b
命令	接受信息
序号	27621
数据	1318732226（本人 QQ 号）

4.5 微信



No.	Time	Source	Destination	Protocol	Length	Info
2149	26.148649	10.3.133.194	wx2.qq.com	TCP	66	4207 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2151	26.195202	wx2.qq.com	10.3.133.194	TCP	66	443 → 4207 [SYN, ACK] Seq=0 Ack=1 Win=14400 Len=0 MSS=1400 SACK_PERM=1
2152	26.195274	10.3.133.194	wx2.qq.com	TCP	54	4207 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
2153	26.195535	10.3.133.194	wx2.qq.com	TLSv1.2	571	Client Hello
2154	26.238777	wx2.qq.com	10.3.133.194	TCP	60	443 → 4207 [ACK] Seq=1 Ack=518 Win=15488 Len=0
2155	26.238777	wx2.qq.com	10.3.133.194	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
2156	26.239130	10.3.133.194	wx2.qq.com	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
2157	26.239341	10.3.133.194	wx2.qq.com	TLSv1.2	1133	Application Data
2158	26.282658	wx2.qq.com	10.3.133.194	TCP	60	443 → 4207 [ACK] Seq=138 Ack=1648 Win=17664 Len=0
2175	26.685538	wx2.qq.com	10.3.133.194	TLSv1.2	517	Application Data
2176	26.725405	10.3.133.194	wx2.qq.com	TCP	54	4207 → 443 [ACK] Seq=1648 Ack=601 Win=130816 Len=0
2652	35.686371	10.3.133.194	wx2.qq.com	TCP	66	13532 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2659	35.691631	10.3.133.194	wx2.qq.com	TLSv1.2	1154	Application Data
2670	35.722605	wx2.qq.com	10.3.133.194	TCP	66	443 → 13532 [SYN, ACK] Seq=0 Ack=1 Win=14400 Len=0 MSS=1400 SACK_PERM=1
2671	35.722656	10.3.133.194	wx2.qq.com	TCP	54	13532 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
2672	35.722799	10.3.133.194	wx2.qq.com	TLSv1.2	571	Client Hello
2692	35.762591	wx2.qq.com	10.3.133.194	TCP	60	443 → 13532 [ACK] Seq=1 Ack=518 Win=15488 Len=0
2693	35.762591	wx2.qq.com	10.3.133.194	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
2694	35.763109	10.3.133.194	wx2.qq.com	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
2778	35.946685	10.3.133.194	wx2.qq.com	TLSv1.2	1073	Application Data
2800	35.994615	wx2.qq.com	10.3.133.194	TCP	60	443 → 11740 [ACK] Seq=6981 Ack=1983 Win=214 Len=0
2828	36.085066	wx2.qq.com	10.3.133.194	TLSv1.2	321	Application Data
2839	36.102133	10.3.133.194	wx2.qq.com	TLSv1.2	1017	Application Data
2866	36.146946	wx2.qq.com	10.3.133.194	TCP	60	443 → 11740 [ACK] Seq=7248 Ack=2946 Win=230 Len=0
4493	49.115188	wx2.qq.com	10.3.133.194	TCP	60	443 → 4207 [FIN, ACK] Seq=20610 Ack=6082 Win=26624 Len=0
4494	49.115239	10.3.133.194	wx2.qq.com	TCP	54	4207 → 443 [ACK] Seq=6082 Ack=20611 Win=131072 Len=0
4699	53.596552	10.3.133.194	wx2.qq.com	TCP	54	4207 → 443 [FIN, ACK] Seq=6082 Ack=20611 Win=131072 Len=0
4702	53.644218	wx2.qq.com	10.3.133.194	TCP	60	443 → 4207 [RST] Seq=20611 Win=0 Len=0

使用过滤条件：ip.addr == wx2.qq.com，可以捕获到完整的三报文握手和一次非典型的四报文挥手过程。

这里的非典型在于客户收到服务器发送的「RST」后，主动断开连接。。

下面以三报文握手的第一次报文握手给出分析。

① 数据链路层

```
Ethernet II, Src: LAPTOP-UDSDOI2Q.local (08:71:90:1a:99:38), Dst: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
  Destination: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
      Address: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: LAPTOP-UDSDOI2Q.local (08:71:90:1a:99:38)
      Address: LAPTOP-UDSDOI2Q.local (08:71:90:1a:99:38)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

目的地址	80:05:88:46:b4:f9
源地址	08:71:90:1a:99:38
上层协议	IPv4

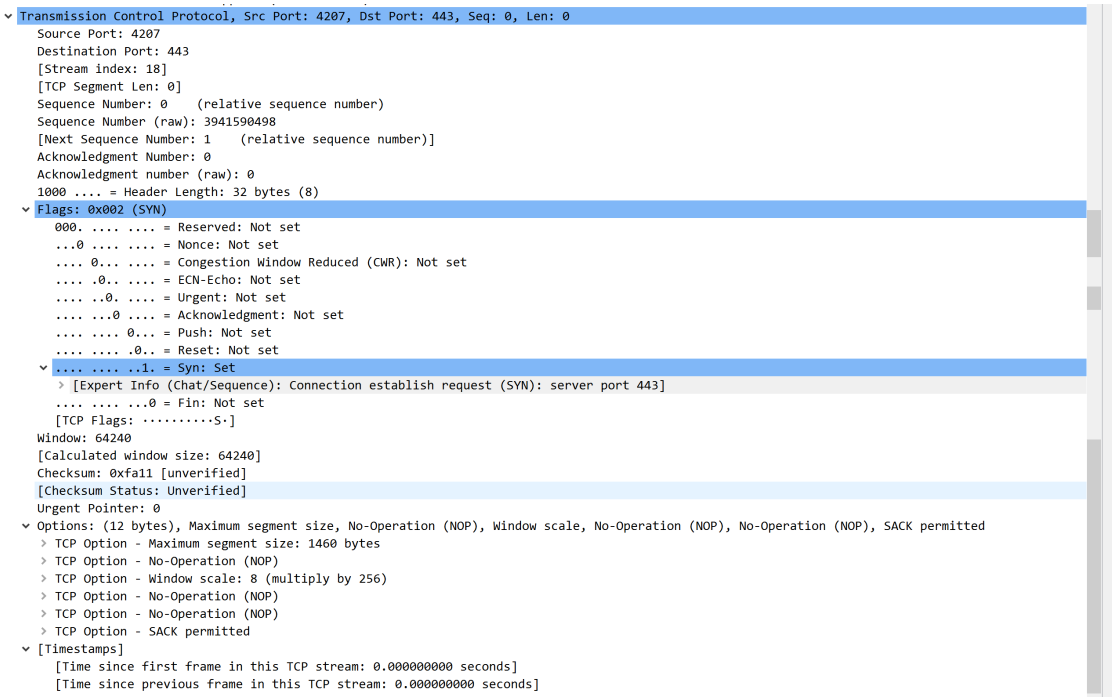
② 网络层

```
Internet Protocol Version 4, Src: 10.3.133.194 (10.3.133.194), Dst: wx2.qq.com (61.241.44.53)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 52
    Identification: 0x6dd8 (28120)
  Flags: 0x40, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.3.133.194 (10.3.133.194)
    Destination Address: wx2.qq.com (61.241.44.53)
```

版本	4
首部长度	20 字节

总长度	52
标识	0x6DD8
分片否?	不分片
生存时间	128 跳
协议	TCP
源 IP 地址	10.3.133.194
目的 IP 地址	wx2.qq.com

③ 运输层

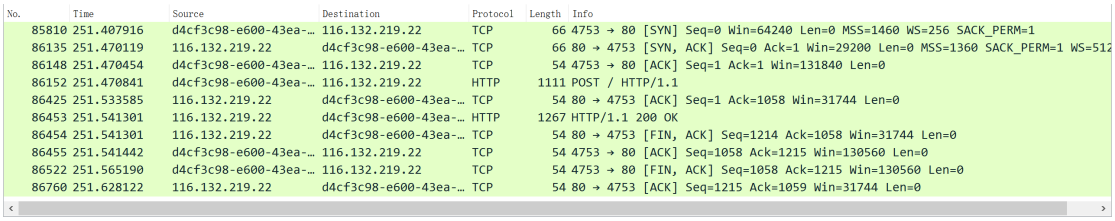


源端口号	4207
目的端口号	443
seq	0
ack	0
rwnd	64240

4.6 迅雷下载

使用过滤条件：http.request.method == "POST"，可以捕获大量迅雷下载相关帧

PacketList:



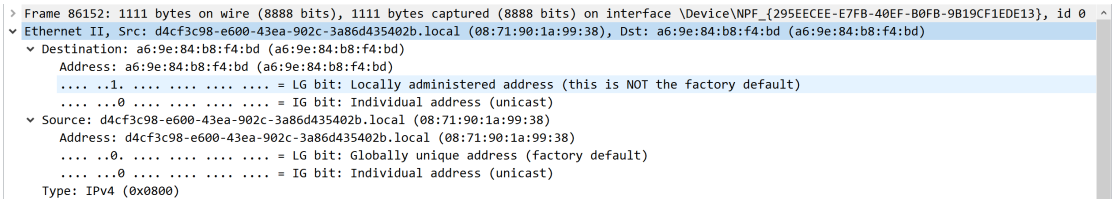
No.	Time	Source	Destination	Protocol	Length	Info
85810	251.407916	d4cf3c98-e600-43ea-…	116.132.219.22	TCP	66	4753 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
86135	251.470119	116.132.219.22	d4cf3c98-e600-43ea-…	TCP	66	80 → 4753 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM=1 WS=512
86148	251.470454	d4cf3c98-e600-43ea-…	116.132.219.22	TCP	54	4753 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
86152	251.470841	d4cf3c98-e600-43ea-…	116.132.219.22	HTTP	1111	POST / HTTP/1.1
86425	251.533585	116.132.219.22	d4cf3c98-e600-43ea-…	TCP	54	80 → 4753 [ACK] Seq=1 Ack=1058 Win=31744 Len=0
86453	251.541301	116.132.219.22	d4cf3c98-e600-43ea-…	HTTP	1267	HTTP/1.1 200 OK
86454	251.541301	116.132.219.22	d4cf3c98-e600-43ea-…	TCP	54	80 → 4753 [FIN, ACK] Seq=1214 Ack=1058 Win=31744 Len=0
86455	251.541442	d4cf3c98-e600-43ea-…	116.132.219.22	TCP	54	4753 → 80 [ACK] Seq=1058 Ack=1215 Win=130560 Len=0
86522	251.565190	d4cf3c98-e600-43ea-…	116.132.219.22	TCP	54	4753 → 80 [FIN, ACK] Seq=1058 Ack=1215 Win=130560 Len=0
86760	251.628122	116.132.219.22	d4cf3c98-e600-43ea-…	TCP	54	80 → 4753 [ACK] Seq=1215 Ack=1059 Win=31744 Len=0

观察过滤帧，发现大量 URL 除包含域名“xunlei”外，还包含域名“sandai”。

这里其实涉及到迅雷的历史。“迅雷”立足于为全球互联网提供最好的多媒体下载服务，由邹胜龙及程浩先生于 2002 年底在美国硅谷创立。2003 年 1 月底，他们回国正式成立深圳市三代科技开发有限公司“三代”，2005 年 5 月正式更名为深圳市迅雷网络技术有限公司（简称“迅雷”）暨“迅雷”在大中华区的研发中心和运营中心。因此兼有 sandai.net 和 xunlei.com 两个域名。

选取 POST 报文进行分析

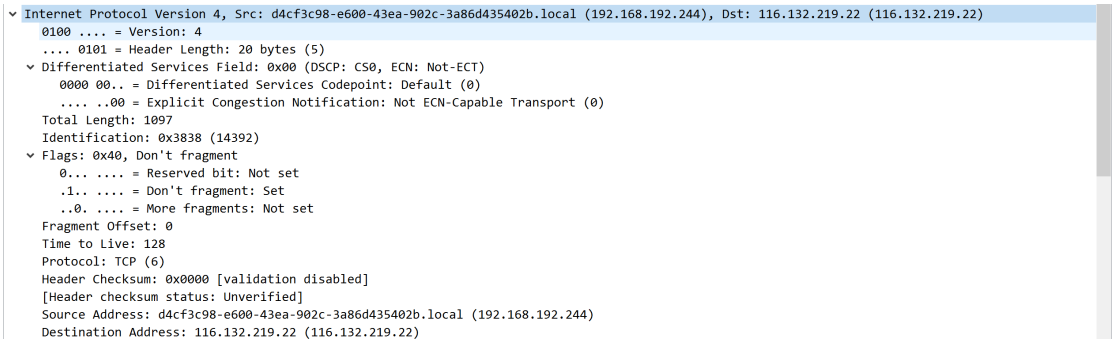
① 数据链路层



```
Frame 86152: 1111 bytes on wire (8888 bits), 1111 bytes captured (8888 bits) on interface \Device\NPF_{295EECEE-E7FB-40EF-B0FB-9B19CF1EDE13}, id 0
Ethernet II, Src: d4cf3c98-e600-43ea-902c-3a86d435402b.local (08:71:90:1a:99:38), Dst: a6:9e:84:b8:f4:bd (a6:9e:84:b8:f4:bd)
  Destination: a6:9e:84:b8:f4:bd (a6:9e:84:b8:f4:bd)
      Address: a6:9e:84:b8:f4:bd (a6:9e:84:b8:f4:bd)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: d4cf3c98-e600-43ea-902c-3a86d435402b.local (08:71:90:1a:99:38)
      Address: d4cf3c98-e600-43ea-902c-3a86d435402b.local (08:71:90:1a:99:38)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

目的地址	a6:9e:84:b8:f4:bd
源地址	08:71:90:1a:99:38
上层协议	IPv4

② 网络层

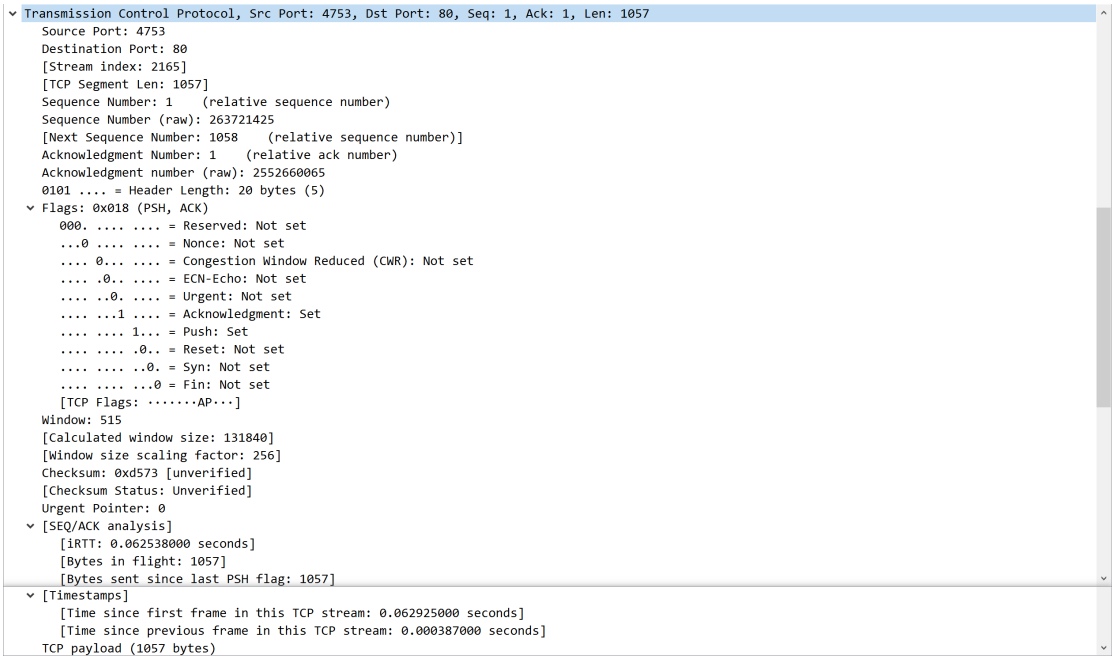


```
Internet Protocol Version 4, Src: d4cf3c98-e600-43ea-902c-3a86d435402b.local (192.168.192.244), Dst: 116.132.219.22 (116.132.219.22)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1097
    Identification: 0x3838 (14392)
  Flags: 0x40, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: d4cf3c98-e600-43ea-902c-3a86d435402b.local (192.168.192.244)
    Destination Address: 116.132.219.22 (116.132.219.22)
```

版本	4
首部长度	20 字节
总长度	1097
标识	0x3838

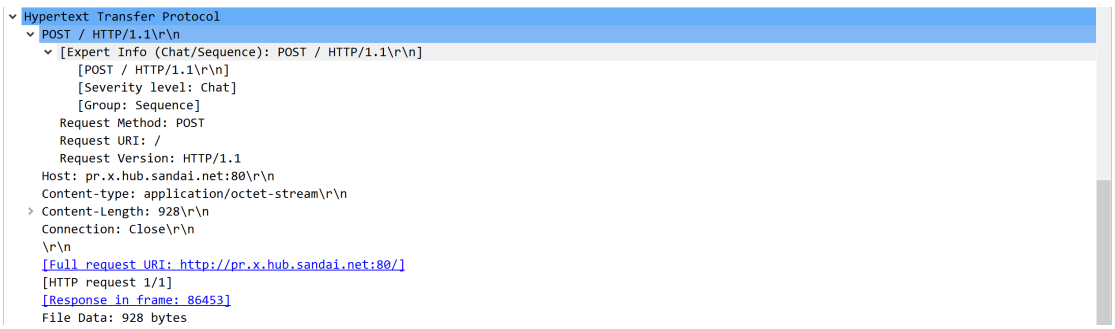
分片否?	不分片
生存时间	128 跳
协议	TCP
源 IP 地址	192.168.192.244
目的 IP 地址	116.132.219.22

③ 运输层



源端口号	4753
目的端口号	80
seq	1
ack	1
rwnd	515

④ 应用层

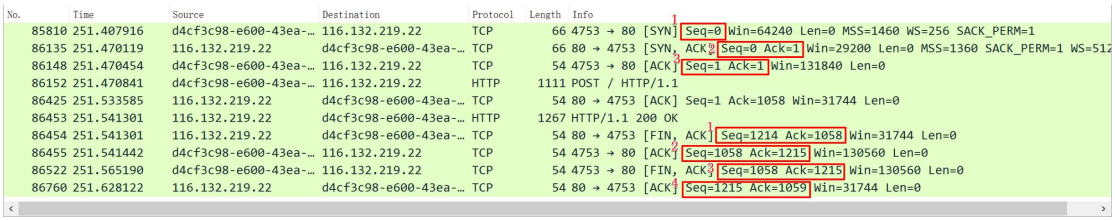


方法	POST
版本	HTTP/1.1
主机	pr.x.hub.sandai.net

五、验证三报文握手及四报文挥手

以刚刚的迅雷下载为例，分析完整的三报文握手和四报文挥手。

PacketList:



No.	Time	Source	Destination	Protocol	Length	Info
85810	251.407916	d4cf3c98-e600-43ea-…	116.132.219.22	TCP	66	4753 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
86135	251.470119	116.132.219.22	d4cf3c98-e600-43ea-…	TCP	66	80 → 4753 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM=1 WS=512
86148	251.470454	d4cf3c98-e600-43ea-…	116.132.219.22	TCP	54	4753 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
86152	251.470841	d4cf3c98-e600-43ea-…	116.132.219.22	HTTP	1111	POST / HTTP/1.1
86425	251.533585	116.132.219.22	d4cf3c98-e600-43ea-…	TCP	54	80 → 4753 [ACK] Seq=1 Ack=1058 Win=31744 Len=0
86453	251.541301	116.132.219.22	d4cf3c98-e600-43ea-…	HTTP	1267	HTTP/1.1 200 OK
86454	251.541301	116.132.219.22	d4cf3c98-e600-43ea-…	TCP	54	80 → 4753 [FIN, ACK] Seq=1214 Ack=1058 Win=31744 Len=0
86455	251.541442	d4cf3c98-e600-43ea-…	116.132.219.22	TCP	54	4753 → 80 [ACK] Seq=1058 Ack=1215 Win=130560 Len=0
86522	251.565190	d4cf3c98-e600-43ea-…	116.132.219.22	TCP	54	4753 → 80 [FIN, ACK] Seq=1058 Ack=1215 Win=130560 Len=0
86760	251.628122	116.132.219.22	d4cf3c98-e600-43ea-…	TCP	54	80 → 4753 [ACK] Seq=1215 Ack=1059 Win=31744 Len=0

说明：方括号[ ]中代表为 1 的标志

三报文握手：

1. **SYN=1**, seq=0

2. **SYN=1, ACK=1**, seq=0, ack=1

3. **ACK=1**, seq=1, ack=1

四报文挥手：

1. **FIN=1**, seq=1214（确认部分忽略）

2. **ACK=1**, seq=1058, ack=1215

3. **FIN=1, ACK=1**, seq=1058, ack=1215

4. **ACK=1**, seq=1215, ack=1059

由此可见，实验结果与预期过程相同。

六、验证 IP 数据包、TCP 报文段和 UDP 数据报的校验和

注：本实验中由于本人主机的网卡自带检验和计算，导致 wireshark 捕捉到的 IP 报文中的 request 报文中的 checksum 字段均为 0。但这也方便了对 reply 报文的 checksum 检验结果的观察，即为 0 代表与预期相同。

6.1 IP 数据报

Requset

```
Header Checksum: 0x0000 incorrect, should be 0x7e86(may be caused by "IP checksum offload"?)
  [Expert Info (Error/Checksum): Bad checksum [should be 0x7e86]]
      [Bad checksum [should be 0x7e86]]
      [Severity level: Error]
      [Group: Checksum]
  [Header checksum status: Bad]
  [Calculated Checksum: 0x7e86]
  Source Address: 192.168.192.244 (192.168.192.244)
  Destination Address: 103.41.167.234 (103.41.167.234)
```

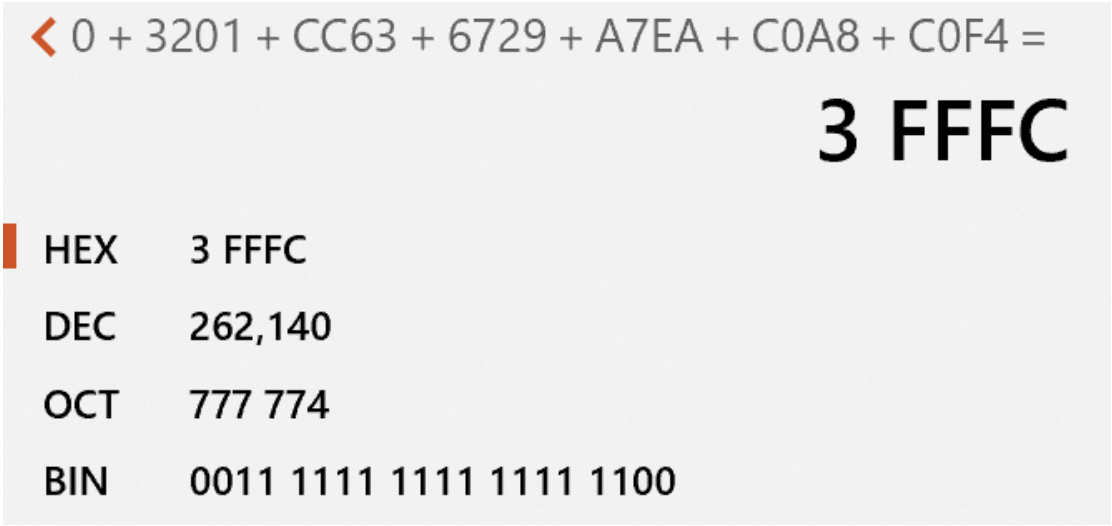
```
0000  a6 9e 84 b8 f4 bd 08 71  90 1a 99 38 08 00 45 00   ·······q ···8··E·
0010  00 3c 2b 8a 00 00 80 01  00 00 c0 a8 c0 f4 67 29   ·<+····· ······g)
0020  a7 ea 08 00 4c a9 00 01  00 b2 61 62 63 64 65 66   ····L··· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

Reply

```
Internet Protocol Version 4, Src: 103.41.167.234 (103.41.167.234), Dst: 192.168.192.244 (192.168.192.244)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)
    0010 10.. = Differentiated Services Codepoint: Assured Forwarding 11 (10)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 60
  Identification: 0x2b8a (11146)
  Flags: 0x00
```

```
0000  08 71 90 1a 99 38 a6 9e  84 b8 f4 bd 08 00 45 28   ·q···8·· ·····E(
0010  00 3c 2b 8a 00 00 32 01  cc 5e 67 29 a7 ea c0 a8   ·<+···2· ·^g)····
0020  c0 f4 00 00 54 a9 00 01  00 b2 61 62 63 64 65 66   ····T··· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

对后者进行计算



由循环反码算数运算有：$[FFFC+3]_{反}=0000$

与预期一致

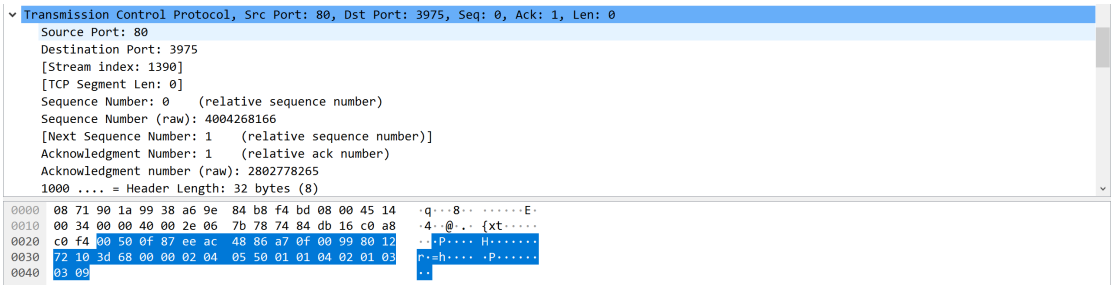
6.2 TCP 数据报

Request

```
Checksum: 0xd15e incorrect, should be 0xeb68(maybe caused by "TCP checksum offload"?)
  [Expert Info (Error/Checksum): Bad checksum [should be 0xeb68]]
      [Bad checksum [should be 0xeb68]]
      [Severity level: Error]
      [Group: Checksum]
  [Checksum Status: Bad]
  [Calculated Checksum: 0xeb68]
  Urgent Pointer: 0
```

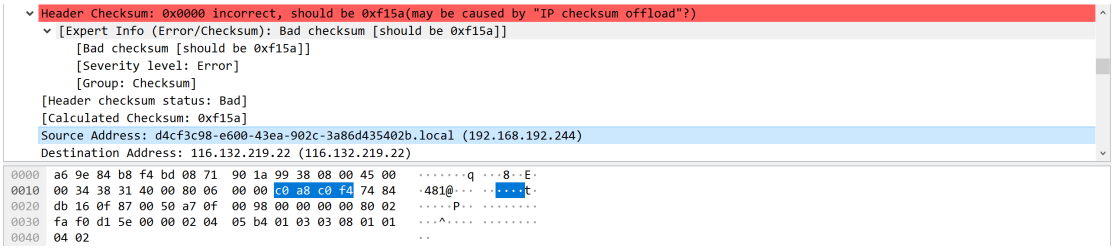
```
0000  a6 9e 84 b8 f4 bd 08 71  90 1a 99 38 08 00 45 00   ·······q ···8··E·
0010  00 34 38 31 40 00 80 06  00 00 c0 a8 c0 f4 74 84   ·481@··· ······t·
0020  db 16 0f 87 00 50 a7 0f  00 98 00 00 00 00 80 02   ·····P·· ········
0030  fa f0 d1 5e 00 00 02 04  05 b4 01 03 03 08 01 01   ···^···· ········
0040  04 02                                             ··
```

Reply

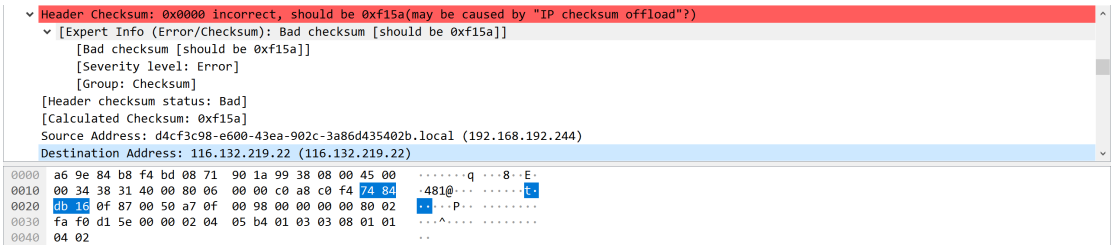


伪首部信息：

字段 1 源地址：



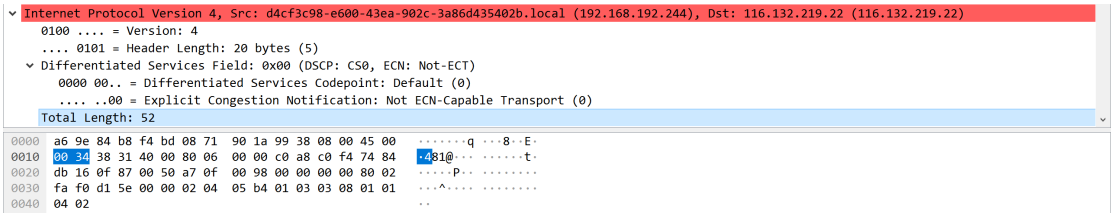
字段 2 目的地址：



字段 3=0

字段 4=6

字段 5 TCP 长度

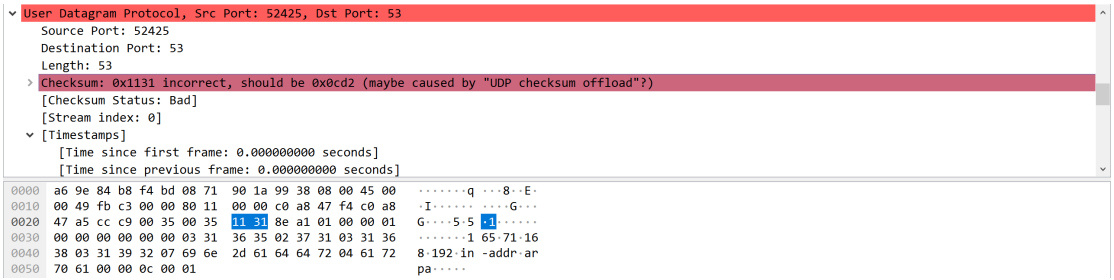


综上，有伪首部=C0A8 C0F4 7484 DB16 0006 0034

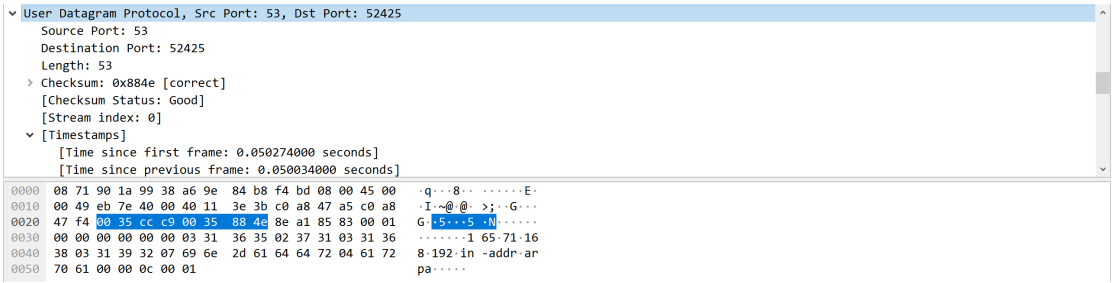
计算结果应得 D15E，与预期相符。

6.3 UDP 数据报

Request

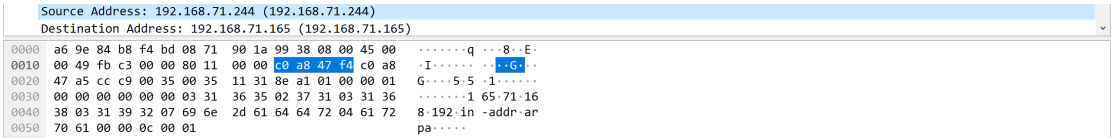


Reply

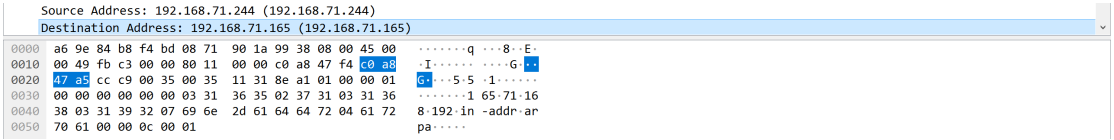


伪首部信息：

字段 1 源 IP 地址：



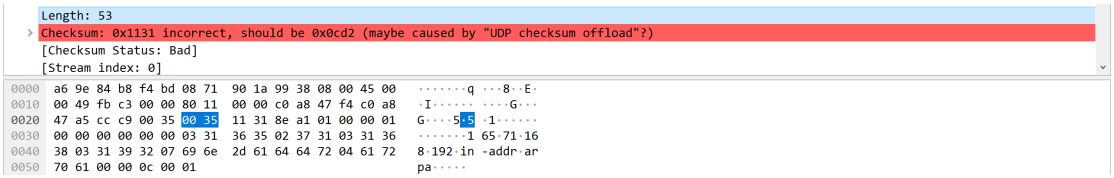
字段 2 目的 IP 地址：



字段 3=0

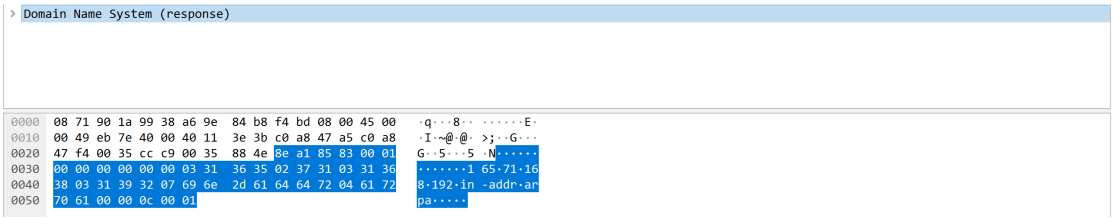
字段 4=17

字段 5 UDP 长度：



即伪首部为 C0A8 47F4 C0A8 47A5 0011 0035

数据部分（这里的数据部分是 DNS 应用）

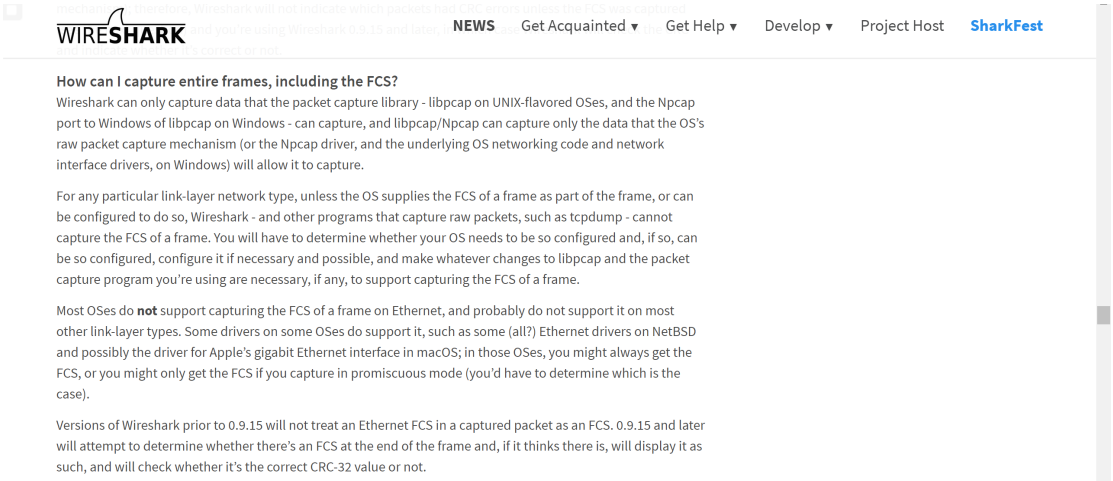


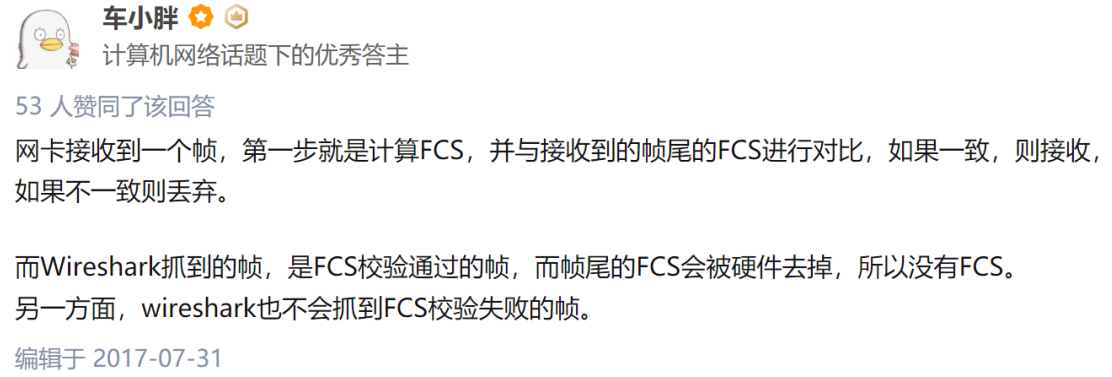
为了对齐，还应在尾部添加 00 00 00

计算结果应得 1131，与预期相符

七、验证数据链路层的 CRC 冗余校验

经查阅官方文档及相关资料，wireshark 无法获取 FCS，也即无法进行 CRC 冗余校验





据资料，omnipeek 软件可以获取 FCS，但受制于期末复习，心有余而力不足，望老师谅解。

实验体会：

此次实验学习了另一个非常强大软件—— Wireshark，这是一个网络封包分析软件，其功能是捕获网络封包，并尽可显示出最为详细的资料，Wireshark 使用 WinPCAP 作为接口，直接与网卡进行数据报文交换。在实验过程通对抓取各类报文及应用层服务，掌握了对 Wireshark 的基本使用方法，也对各类报文的格式有了更加深入的理解，以实践带动了理论学习。