中国矿业大学计算机学院

2017 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 袁孝健 学 号 06172151

专业班级 信息安全 2017-01 班

学 院 计算机科学与技术学院

任课教师 顾军

课程基础理论掌握程度	熟练 □	较熟练 □	一般 □	不熟练 □
综合知识应用能力	强 □	较强 □	一般 □	差 □
报告内容	完整 □	较完整 □	一般 □	不完整 □
报告格式	规范 □	较规范 □	一般 □	不规范 □
实验完成状况	好 □	较好 □	一般 □	差 □
工作量	饱满 □	适中 □	一般 □	欠缺 □
学习、工作态度	好 □	较好 □	一般 □	差 □
抄袭现象	无 □	有 □ 姓名:		
存在问题				
总体评价				

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）运用抓包工具，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）运用抓包工具，连续获取面向连接的互联网访问情形下的本机网卡数据包；对连续获取的数据包找到执行面向连接过程的报文，给出实现面向连接过程（TCP 三次握手）的详细分析。

（3）分别对不同互联网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；要求分别获取 WWW 服务、Email 服务、QQ 通信和迅雷文件下载四种不同网络服务过程中的数据包。

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。

（3）透过 Web 服务访问，分析 HTTP 协议工作过程，总结 HTTP 协议特点；透过 HTTP 工作过程分析，获取 TCP 协议的工作过程，验证连接建立的三次握手过程，以及滑动窗口工作机制。

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

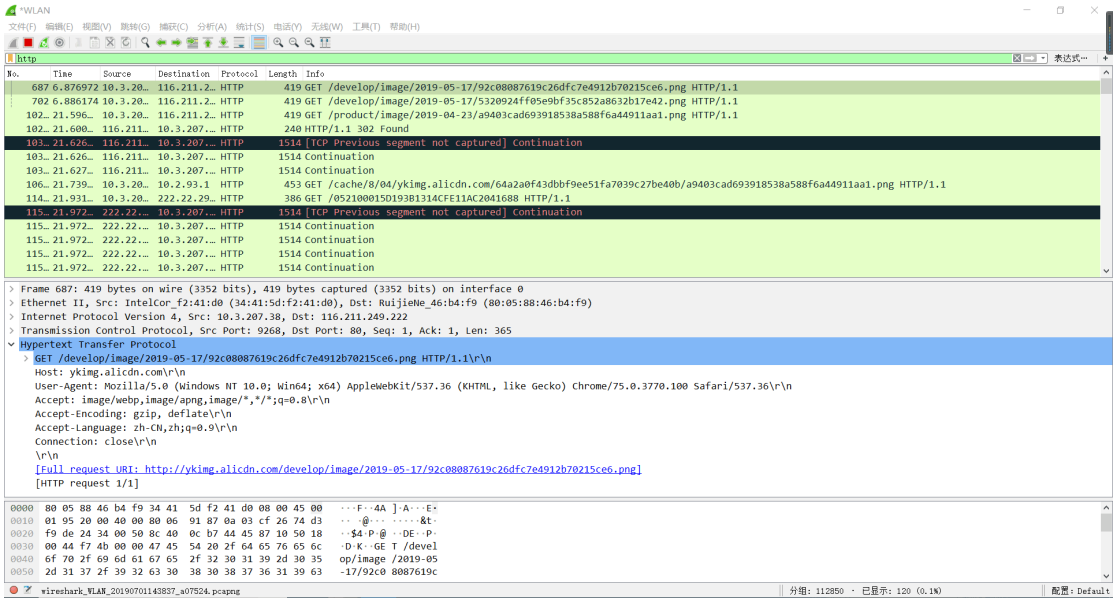
（3） 登录实验管理服务器，提交实验报告电子档。

（4） 提交纸质版实验报告。

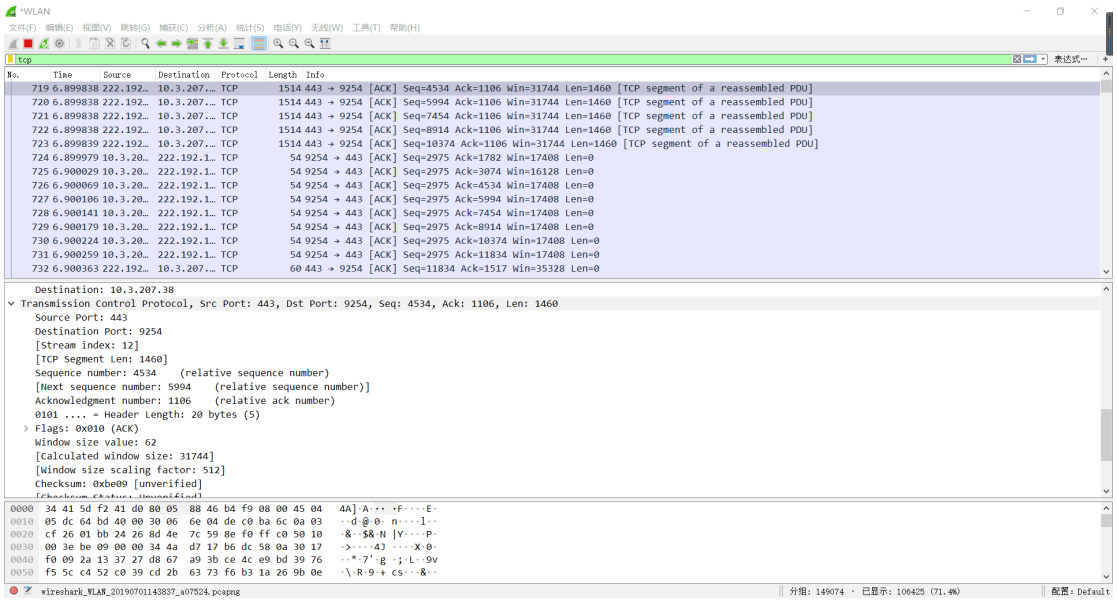
实验报告内容：

1. 运用抓包工具，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。

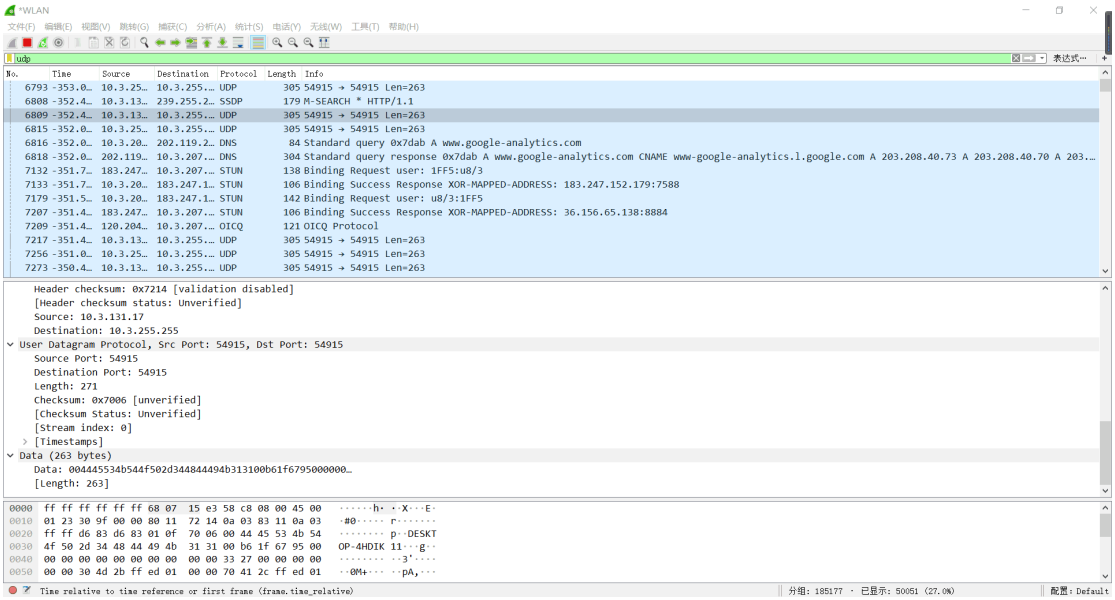
（1）HTTP



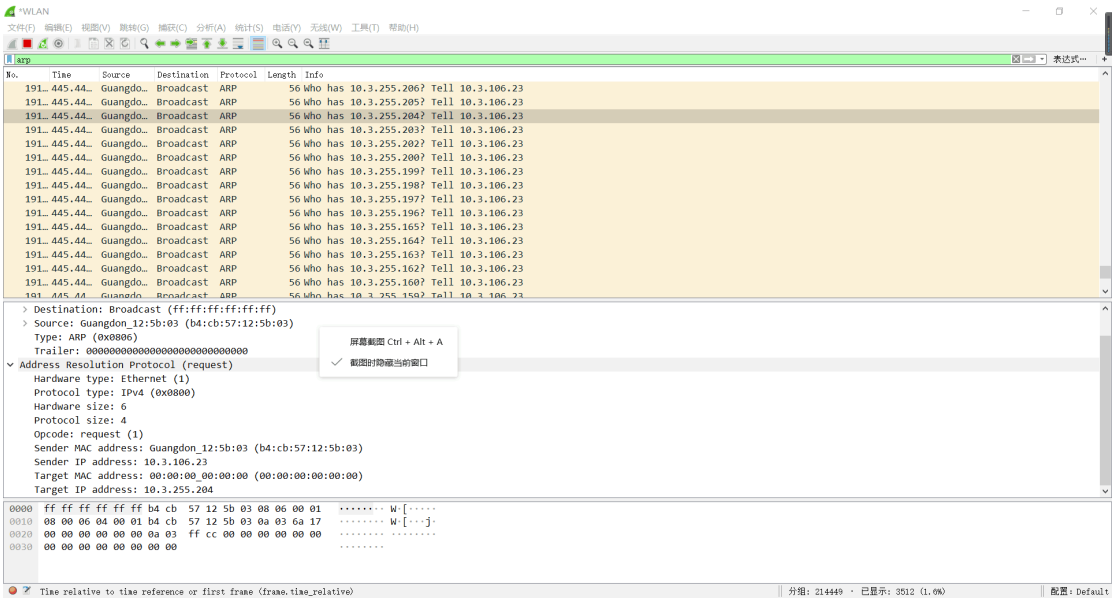
（2）TCP



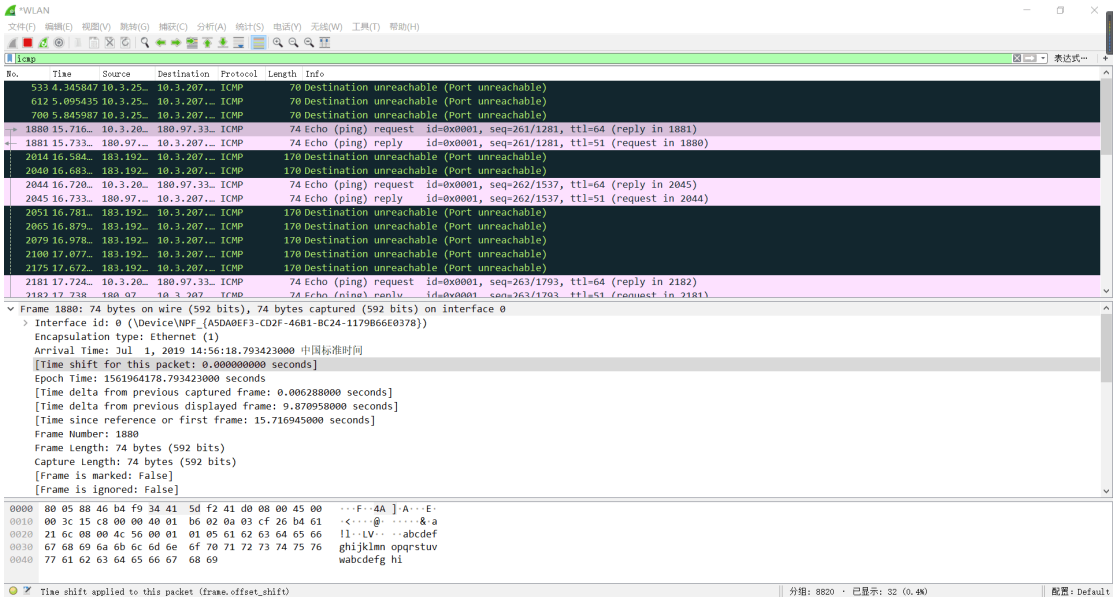
（3）UDP


*WLAN
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
表达式…
No. Time Source Destination Protocol Length Info
6793 -353.0… 10.3.25… 10.3.255.… UDP 305 54915 → 54915 Len=263
6808 -352.4… 10.3.13… 239.255.2… SSDP 179 M-SEARCH * HTTP/1.1
6809 -352.4… 10.3.13… 10.3.255.… UDP 305 54915 → 54915 Len=263
6815 -352.0… 10.3.25… 10.3.255.… UDP 305 54915 → 54915 Len=263
6816 -352.0… 10.3.20… 202.119.2… DNS 84 Standard query 0x7dab A www.google-analytics.com
6818 -352.0… 202.119… 10.3.207.… DNS 304 Standard query response 0x7dab A www.google-analytics.com CNAME www-google-analytics.l.google.com A 203.208.40.73 A 203.208.40.70 A 203.…
7132 -351.7… 183.247… 10.3.207.… STUN 138 Binding Request user: 1FF5:u8/3
7133 -351.7… 10.3.20… 183.247.1… STUN 106 Binding Success Response XOR-MAPPED-ADDRESS: 183.247.152.179:7588
7179 -351.5… 10.3.20… 183.247.1… STUN 142 Binding Request user: u8/3:1FF5
7207 -351.4… 183.247… 10.3.207.… STUN 106 Binding Success Response XOR-MAPPED-ADDRESS: 36.156.65.138:8884
7209 -351.4… 120.204… 10.3.207.… OICQ 121 OICQ Protocol
7217 -351.4… 10.3.13… 10.3.255.… UDP 305 54915 → 54915 Len=263
7256 -351.0… 10.3.25… 10.3.255.… UDP 305 54915 → 54915 Len=263
7273 -350.4… 10.3.13… 10.3.255.… UDP 305 54915 → 54915 Len=263
Header checksum: 0x7214 [validation disabled]
[Header checksum status: Unverified]
Source: 10.3.131.17
Destination: 10.3.255.255
User Datagram Protocol, Src Port: 54915, Dst Port: 54915
Source Port: 54915
Destination Port: 54915
Length: 271
Checksum: 0x7006 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
Data (263 bytes)
Data: 004445534b544f502d344844494b313100b61f6795000000…
[Length: 263]
0000 ff ff ff ff ff ff 68 07 15 e3 58 c8 08 00 45 00 ·····h· ··X···E·
0010 01 23 30 9f 00 00 80 11 72 14 0a 03 83 11 0a 03 ·#0····· r·····
0020 ff ff d6 83 d6 83 01 0f 70 06 00 44 45 53 4b 54 ·····p··DESKT
0030 4f 50 2d 34 48 44 49 4b 31 31 00 b6 1f 67 95 00 OP-4HDIK 11···g··
0040 00 00 00 00 00 00 00 00 00 00 33 27 00 00 00 00 ·····3'····
0050 00 00 30 4d 2b ff ed 01 00 00 70 41 2c ff ed 01 ··0M+··· ··pA,···
Time relative to time reference or first frame (frame.time_relative)
分组: 185177 · 已显示: 50051 (27.0%)
配置: Default

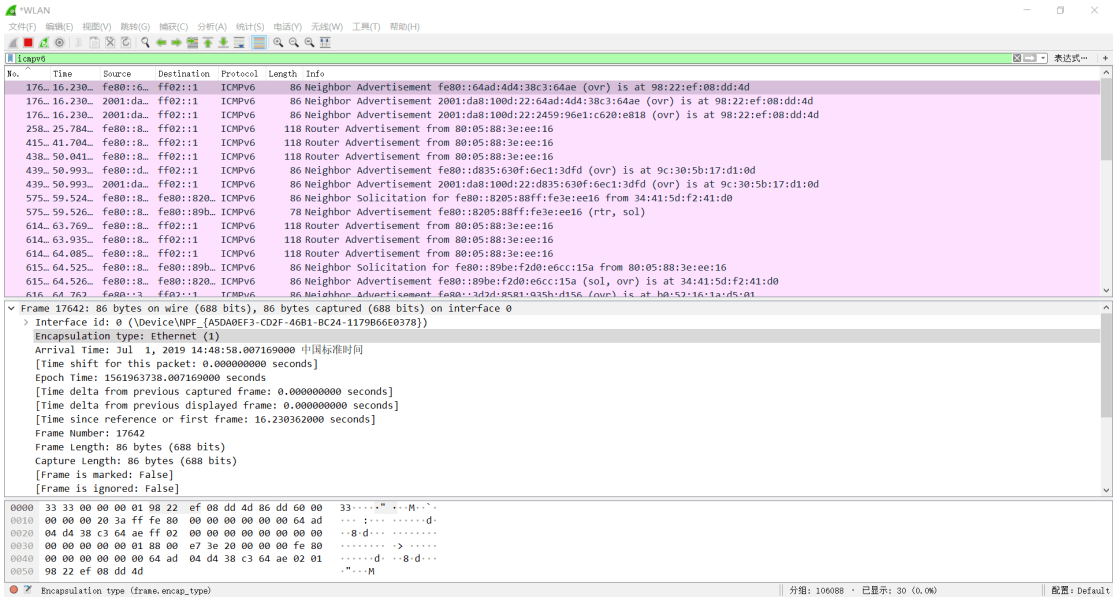
（4）ARP


*WLAN
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
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.206? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.205? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.204? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.203? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.202? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.200? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.199? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.198? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.197? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.196? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.165? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.164? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.163? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.162? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.160? Tell 10.3.106.23
191… 445.44… Guangdo… Broadcast ARP 56 Who has 10.3.255.159? Tell 10.3.106.23
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: Guangdon_12:5b:03 (b4:cb:57:12:5b:03)
Type: ARP (0x0806)
Trailer: 00000000000000000000000000000000
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: Guangdon_12:5b:03 (b4:cb:57:12:5b:03)
Sender IP address: 10.3.106.23
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 10.3.255.204
屏幕截图 Ctrl + Alt + A
截图时隐藏当前窗口
0000 ff ff ff ff ff ff b4 cb 57 12 5b 03 08 06 00 01 ·····W·[·····
0010 08 00 06 04 00 01 b4 cb 57 12 5b 03 0a 03 6a 17 ·····W·[···j·
0020 00 00 00 00 00 00 0a 03 ff cc 00 00 00 00 00 00 ·····
0030 00 00 00 00 00 00 00 00 ·····
Time relative to time reference or first frame (frame.time_relative)
分组: 214449 · 已显示: 3512 (1.6%)
配置: Default

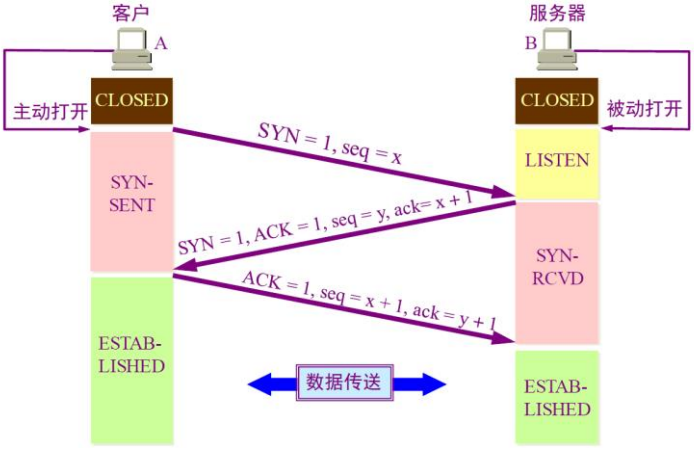
（5）ICMP



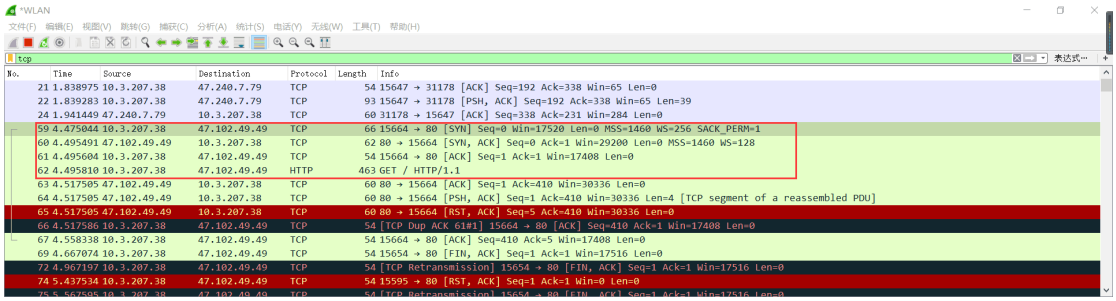
（6）ICMPv6



2. 运用抓包工具，连续获取面向连接的互联网访问情形下的本机网卡数据包；对连续获取的数据包找到执行面向连接过程的报文，给出实现面向连接过程（TCP 三次握手）的详细分析。

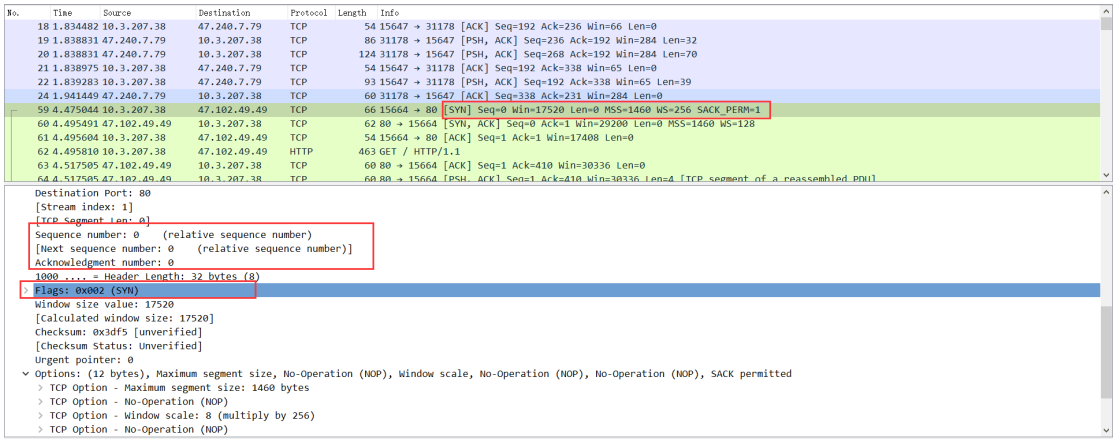


(1)访问优酷（47.102.49.49），观察 TCP 的三次握手流程，在 Wireshark 中追踪 TCP 流入下:



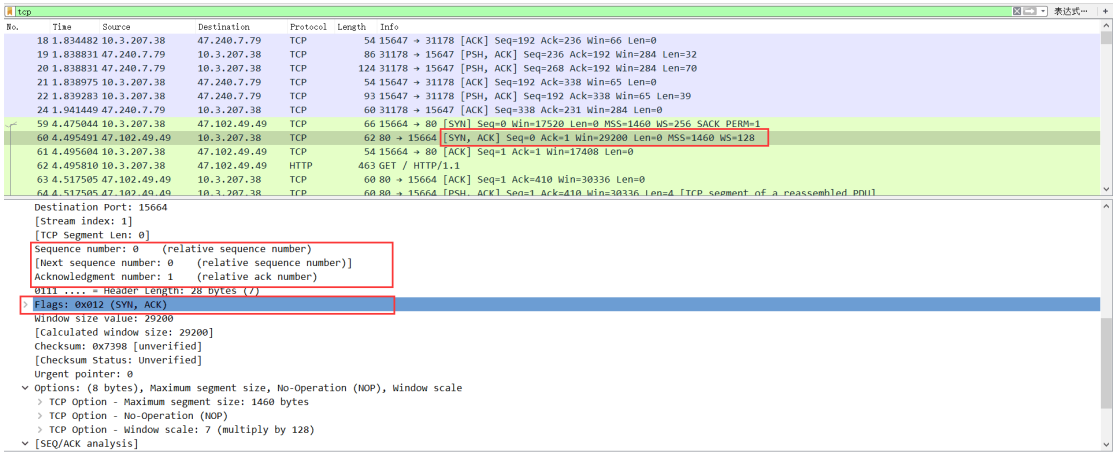
（2）上述框选部分即为三握手流程，下面对三握手流程进行分析:

① 第一次握手:



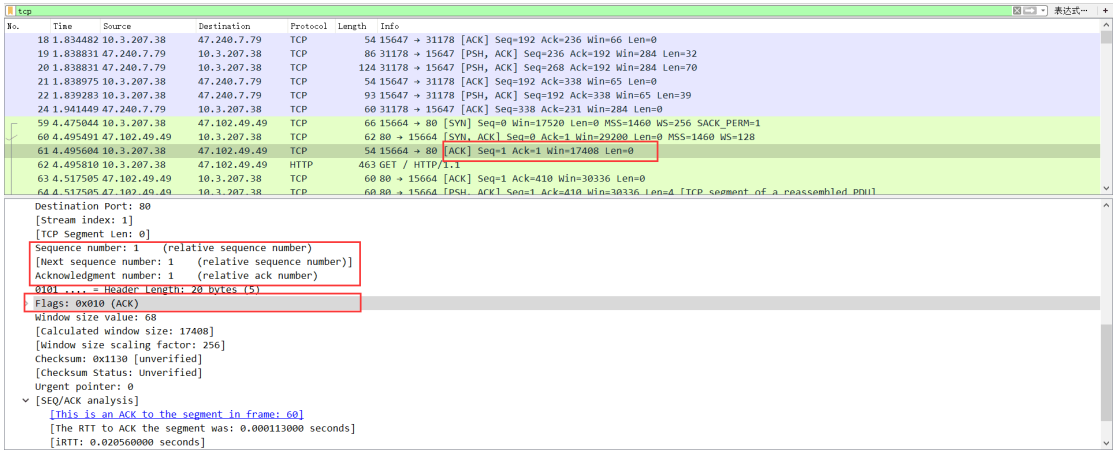
本机（10.3.207.38）向目的主机（47.102.49.49）请求建立连接，发送请求报文段，设置首部中 SYN=1，同时选择一个初始序列号 seq=0。TCP 规定 SYN 报文段不能现代数据，但是消耗掉一个序号，此时 TCP 客户进程进入 SYN-SENT 状态。

② 第二次握手



目的主机（47.102.49.49）收到请求报文后，同意建立练级，并发送确认。在报文段中将 ACK 和 SYN 均设为 1，并将确认序号(Acknowledgement Number)加 1，同时也为自己选择一个初始序号。

③ 第三次握手

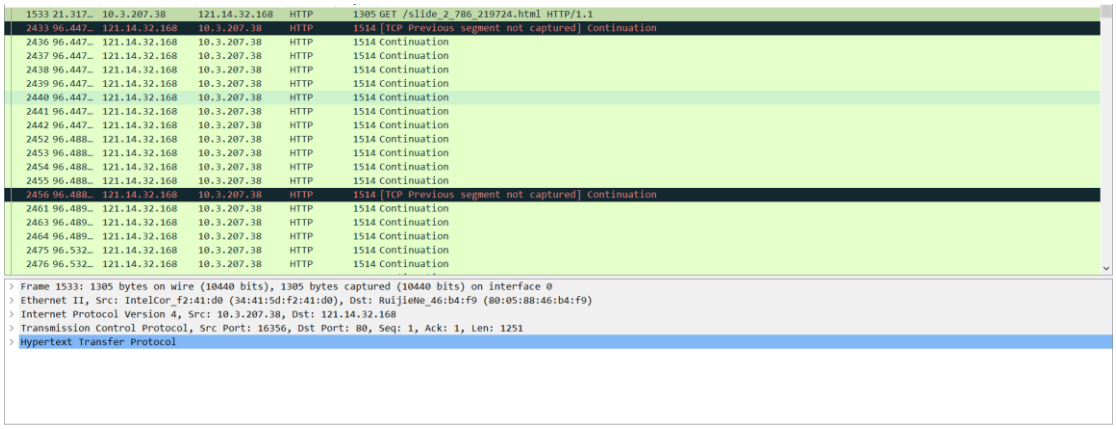


本记（10.3.207.38）收到确认后，还要再给出确认。确认报文段的 ACK 设置为 1，确认号等于目的主机的确认号加 1，自己的序号为 0+1=1。

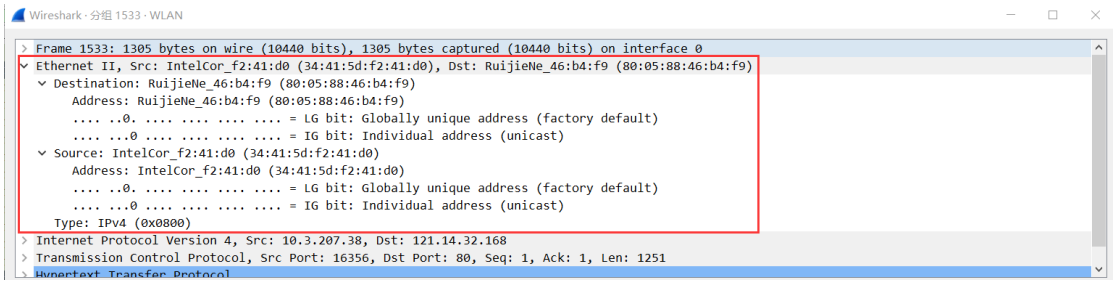
3. 分别对不同互联网访问情形下的数据包进行逐层分析，给出各层协议的主要参数及意义；要求分别获取 WWW 服务、Email 服务、QQ 通信和迅雷文件下载四种不同网络服务过程中的数据包。

Frame：物理层的数据帧概况(这是最底层的，一般以比特流传送)
Ethernet II：数据链路层以太网帧头部信息，
Internet Protocol Version 4：网络层 IP 包头部信息
Transmission Control Protocol：传输层 T 的数据段头部信
Hypertext Transfer Protocol：应用层的信息

（1）WWW 服务（http 协议）

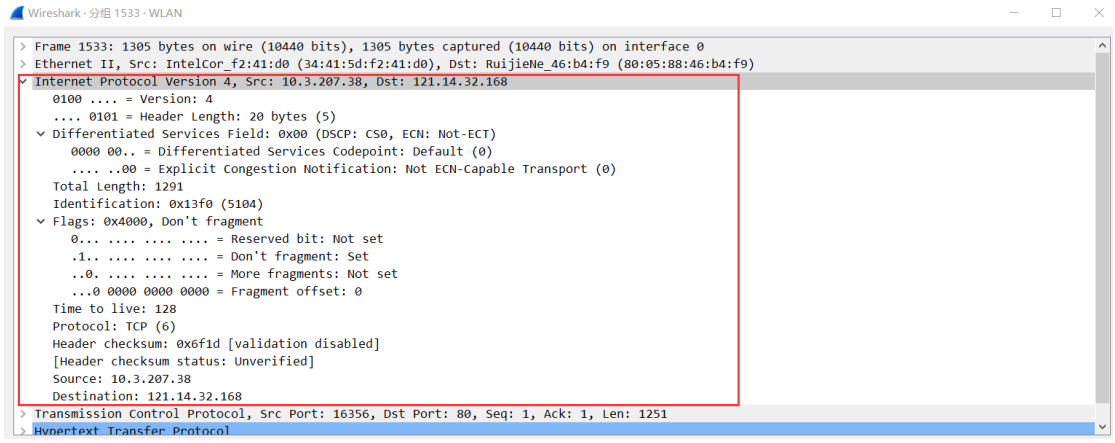


① 数据链路层



目的地址为 80:05:88:46:b4:f9，源地址为 34:41:5d:f2:41:d0，上层协议采用 IPv4 协议。

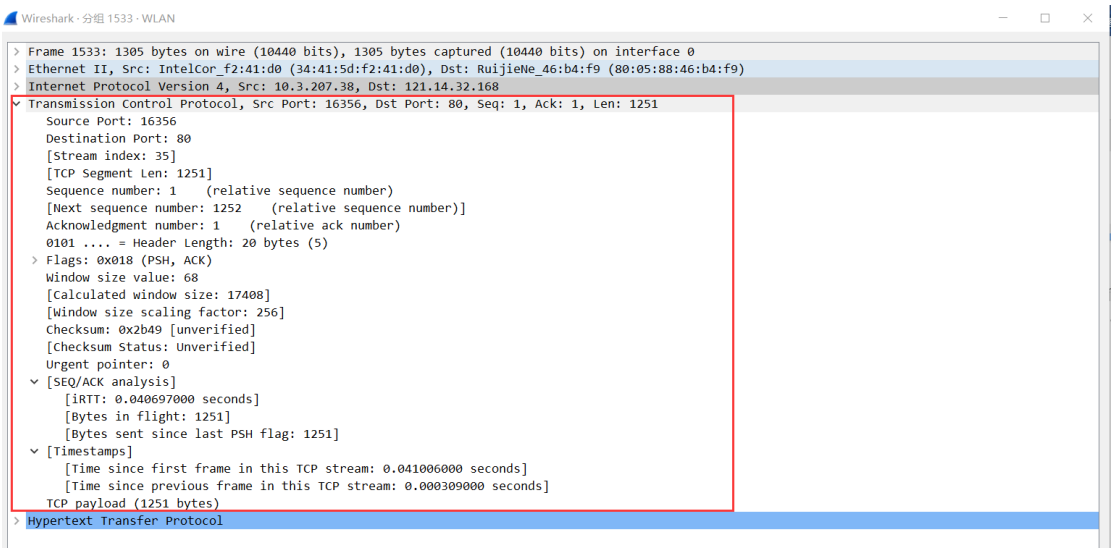
② 网络层



分析：

版本：4，首部长度：20 字节，总长度：1291 字节，标识：0x13f0，不能分片，生存时间：128 跳，协议为：TCP，首部检验和：0x6f1d，源 IP 地址：10.3.207.38，目的 IP 地址：121.14.32.168

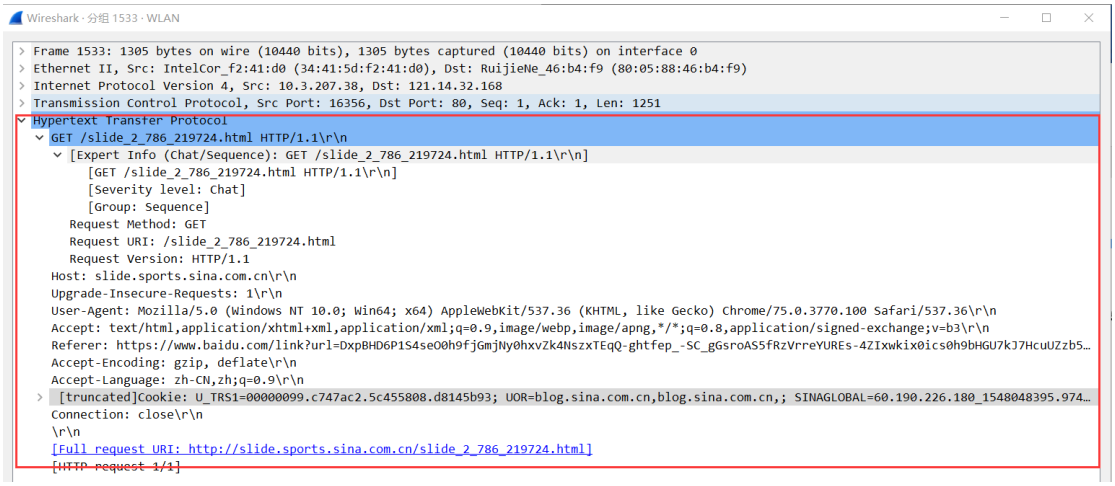
③ 运输层



分析：

源端口：16356，目的端口：80，序号：1，确认号：1，PSH=1,ACK=1,窗口大小：256，检验和：0x2b49，紧急指针：0

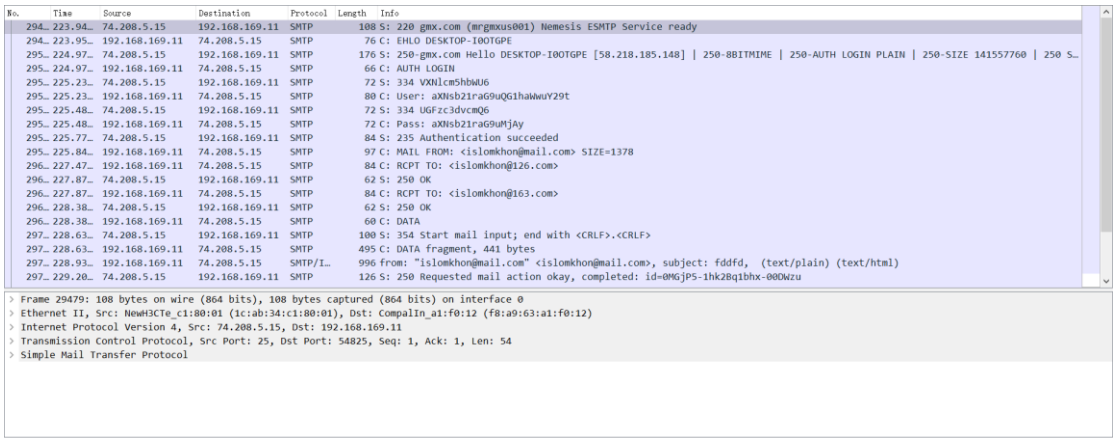
④ 应用层



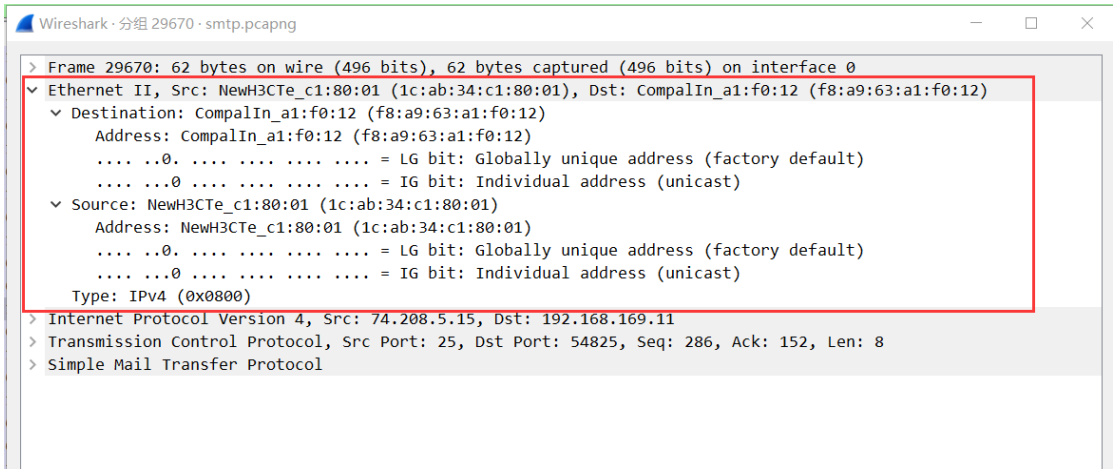
分析：

方法为 GET，URL 为/slide_2_786_219724.html，版本为 HTTP/1.1，\r\n 为回车换行，之后为各首部字段名以及相应的值，在该报文段中还是设置了 Cookie。

（2）Email 服务（SMTP 协议）



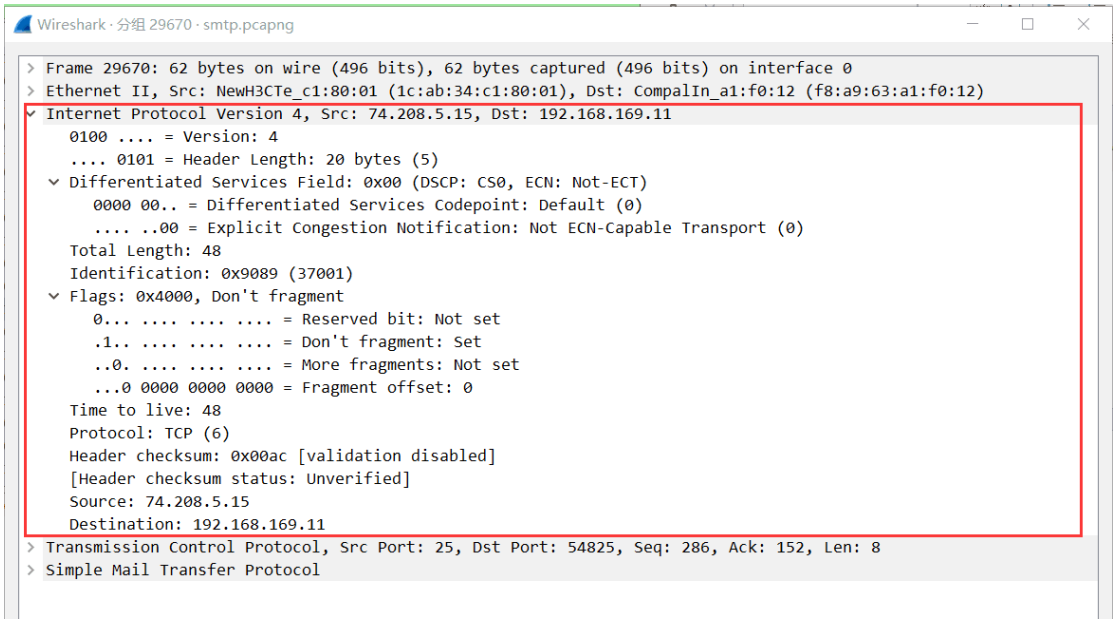
① 数据链路层



分析：

目的地址为 f8:a9:63:a1:f0:12，源地址为 1c:ab:34:c1:80:01，上层协议是 IPv4。

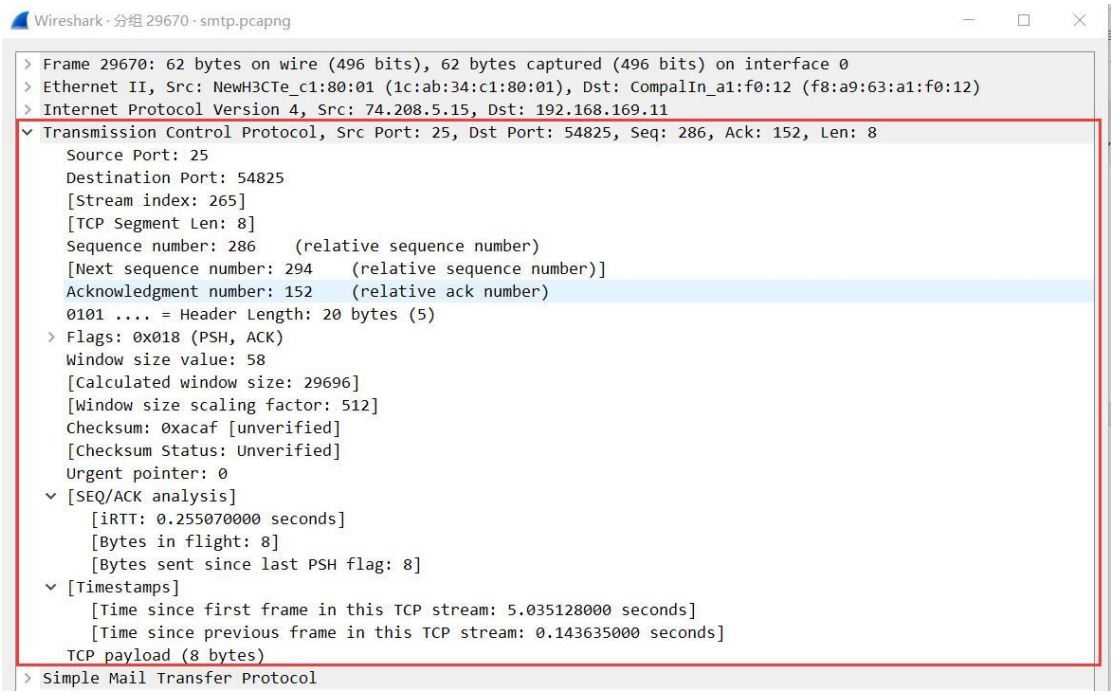
② 网络层



分析：

版本为 IPv4，源地址为 74.200.5.15，目的地址为 192.168.169.11，首部长度为 48，标识为 0x9089，不分片，存活时间为 48 跳，传输层协议为 TCP。

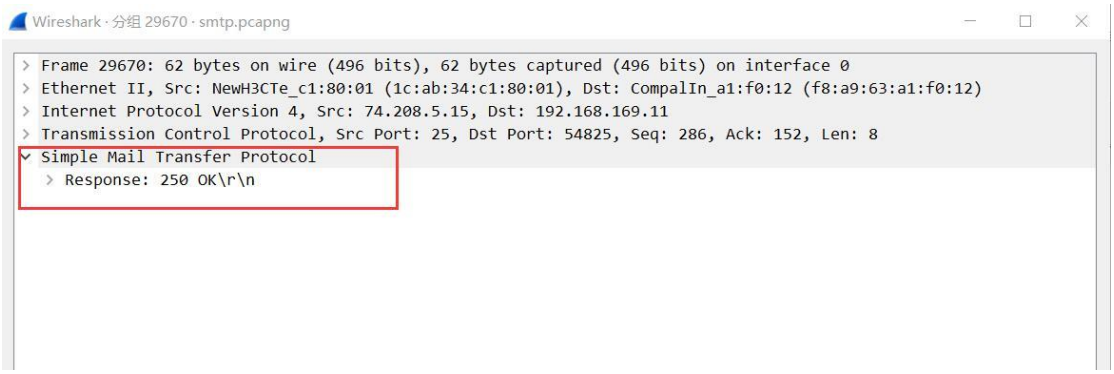
③ 运输层



分析：

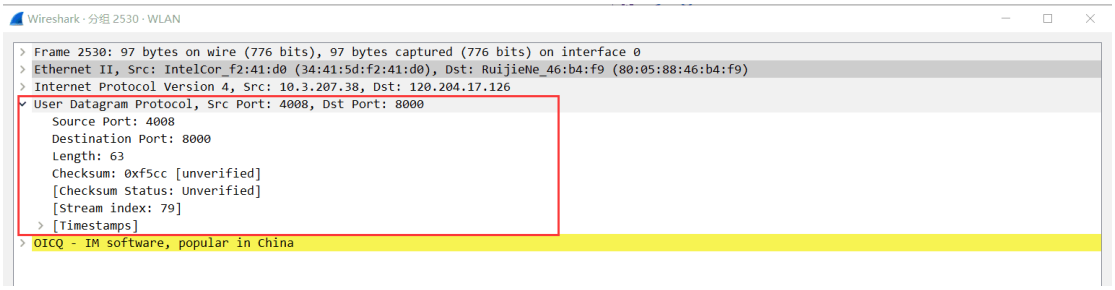
源端口号为 25，目的端口号为 54825，seq=286，ack=152，接收窗口大小为 58 字节。

④ 应用层



分析：采用 SMTP 协议，250 OK 表示要求的邮件操作完成。

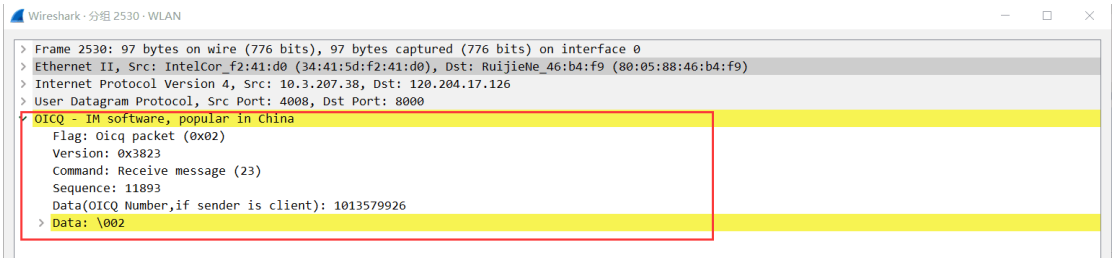
③ 运输层



分析：

源端口：4008，目的端口：8000，长度：63，检验和：0xf5cc（未经证实的）

④ 应用层

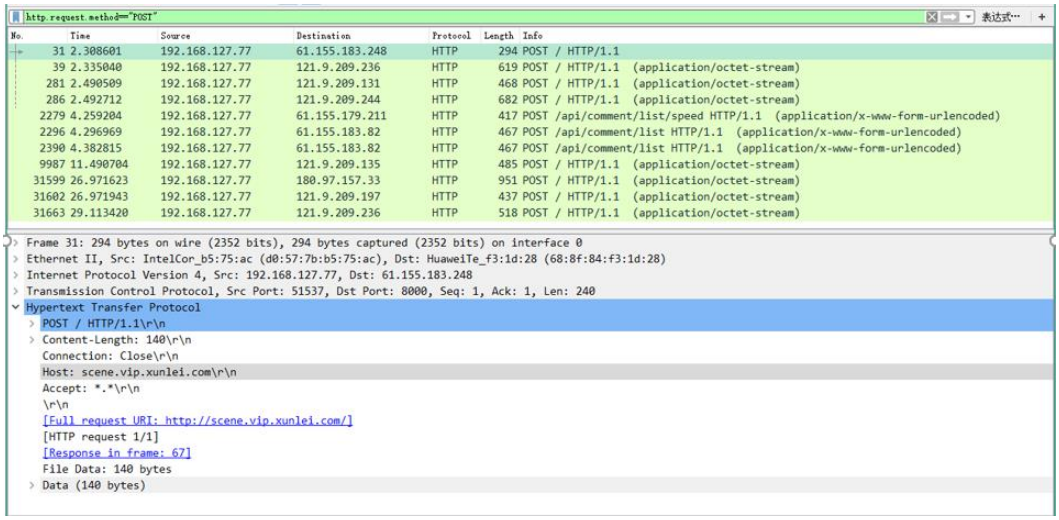


分析:

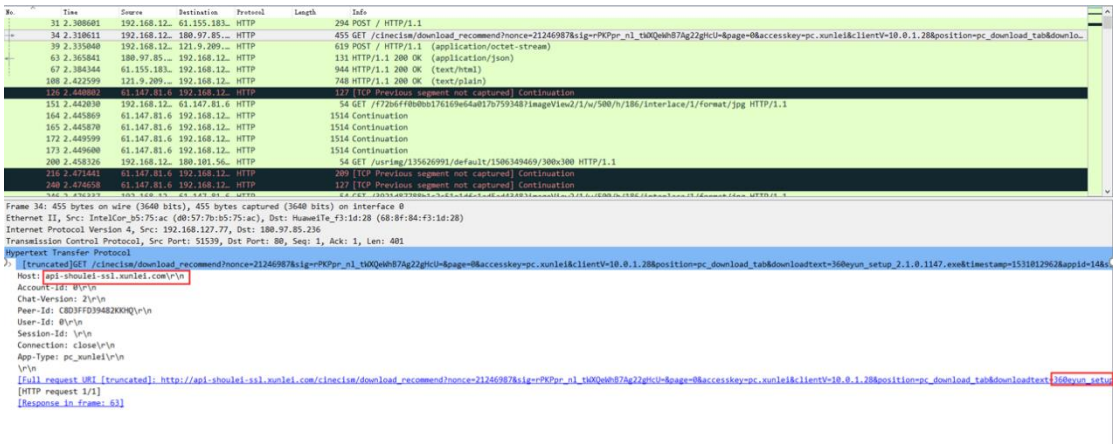
标志位 Oicq packet，版本号位 0x3823，命令是收到信息，序号位 11893，Data 这里是我的 QQ 号。

（3）迅雷文件下载

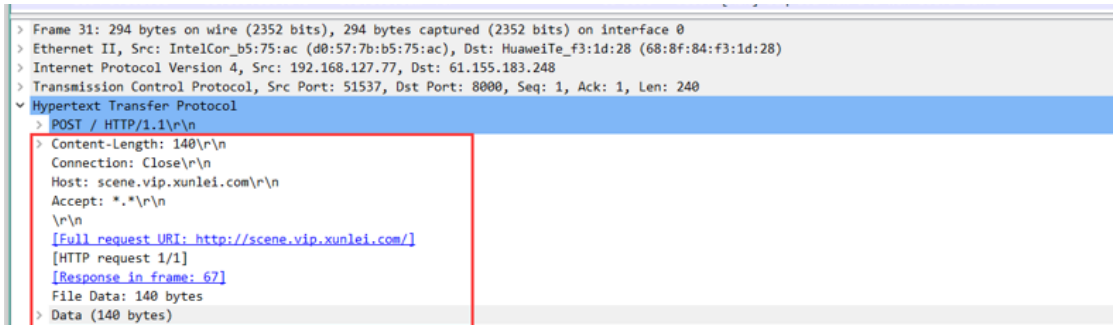
① 抓包如下:

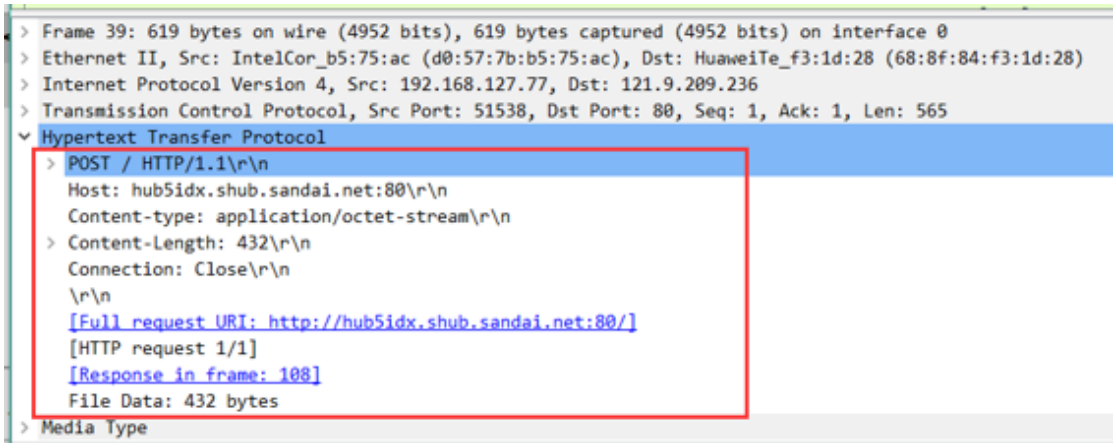


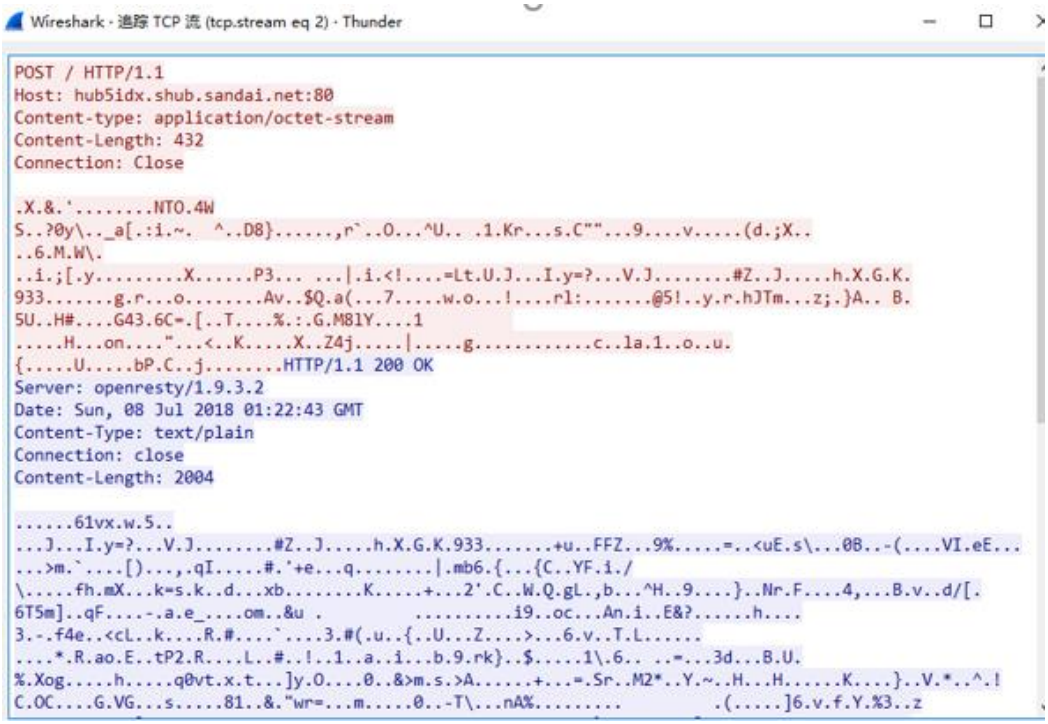
② 选取其中一帧进行分析，在 POST 中发现和下载相关的关键字:



③ 追踪迅雷下载的 TCP 流：

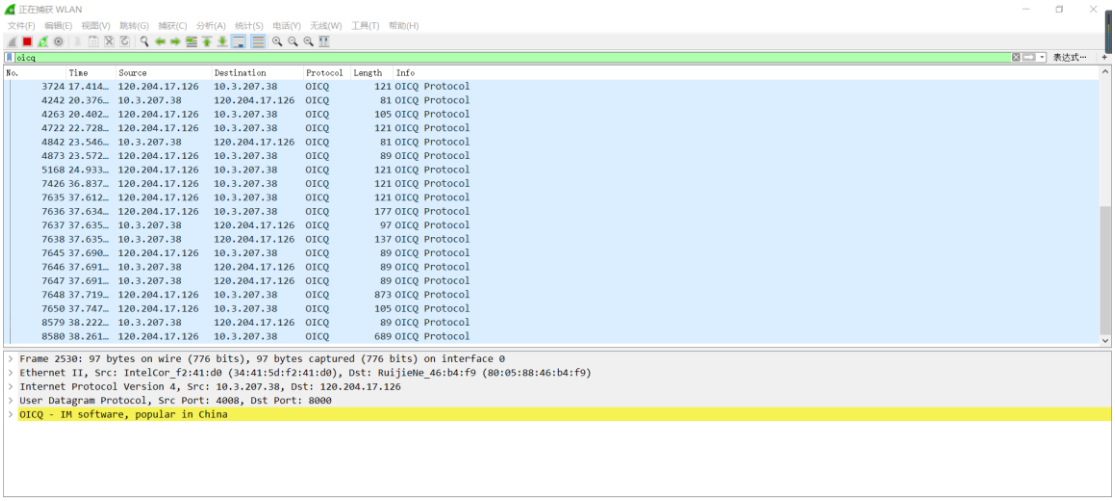




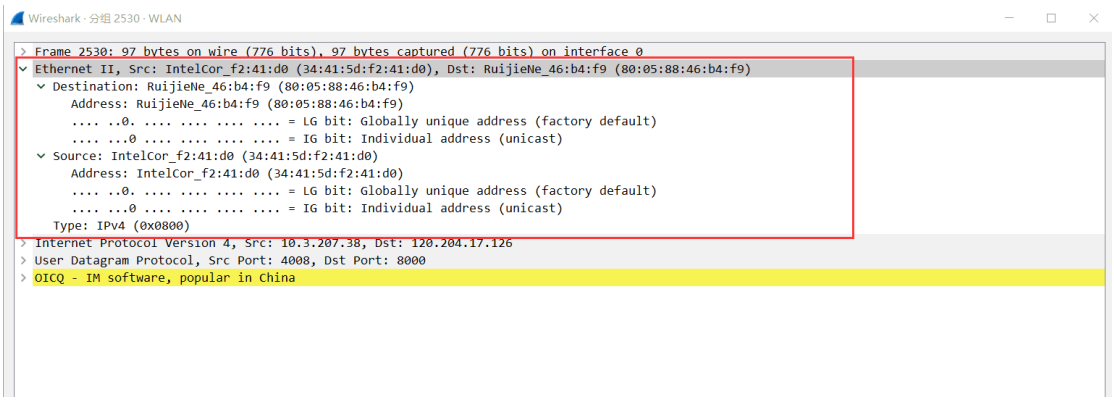


发现迅雷下载不是从同一个服务进行下载，而是同步的从多个服务器进行下载，以提高下载的速度。

（4）QQ 通信（即 OICQ）



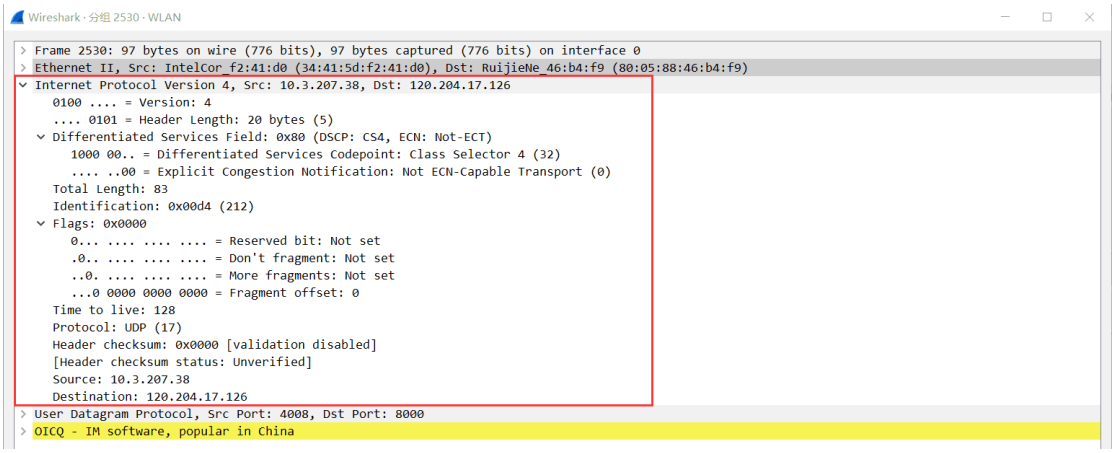
① 数据链路层



分析：

源地址：34:41:5d:f2:41:d0，目的地址：80:05:88:46:b4:f9

② 网络层



分析：

版本：4，首部长度：20 字节，总长度：83 字节，标识：0x00d4，能分片，生存时间：128 跳，协议为：UDP，首部检验和：0x0000，源 IP 地址：10.3.207.38，目的 IP 地址：120.204.17.126

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，其功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料，Wireshark 使用 WinPCAP 作为接口，直接与网卡进行数据报文交换。在实验过程通过对抓取各类报文 WWW 服务、Email 服务、QQ 通信和迅雷文件下载，不仅掌握了对 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，可以说是理论指导实验，实验促进了理论的学习！