

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 <input type="checkbox"/>	较熟练 <input type="checkbox"/>	一般 <input type="checkbox"/>	不熟练 <input type="checkbox"/>			
综合知识应用能力	强 <input type="checkbox"/>	较强 <input type="checkbox"/>	一般 <input type="checkbox"/>	差 <input type="checkbox"/>			
报告内容	完整 <input type="checkbox"/>	较完整 <input type="checkbox"/>	一般 <input type="checkbox"/>	不完整 <input type="checkbox"/>			
报告格式	规范 <input type="checkbox"/>	较规范 <input type="checkbox"/>	一般 <input type="checkbox"/>	不规范 <input type="checkbox"/>			
实验完成状况	好 <input type="checkbox"/>	较好 <input type="checkbox"/>	一般 <input type="checkbox"/>	差 <input type="checkbox"/>			
工作量	饱满 <input type="checkbox"/>	适中 <input type="checkbox"/>	一般 <input type="checkbox"/>	欠缺 <input type="checkbox"/>			
学习、工作态度	好 <input type="checkbox"/>	较好 <input type="checkbox"/>	一般 <input type="checkbox"/>	差 <input type="checkbox"/>			
抄袭现象	无 <input type="checkbox"/>	有 <input type="checkbox"/> 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

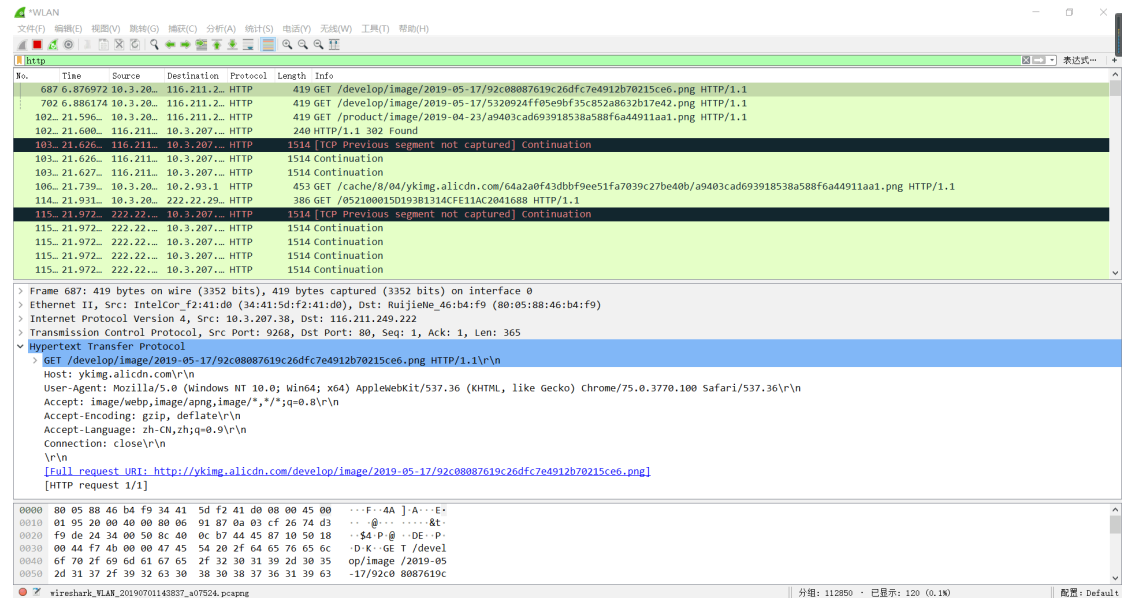
(3) 登录实验管理服务器，提交实验报告电子档。

(4) 提交纸质版实验报告。

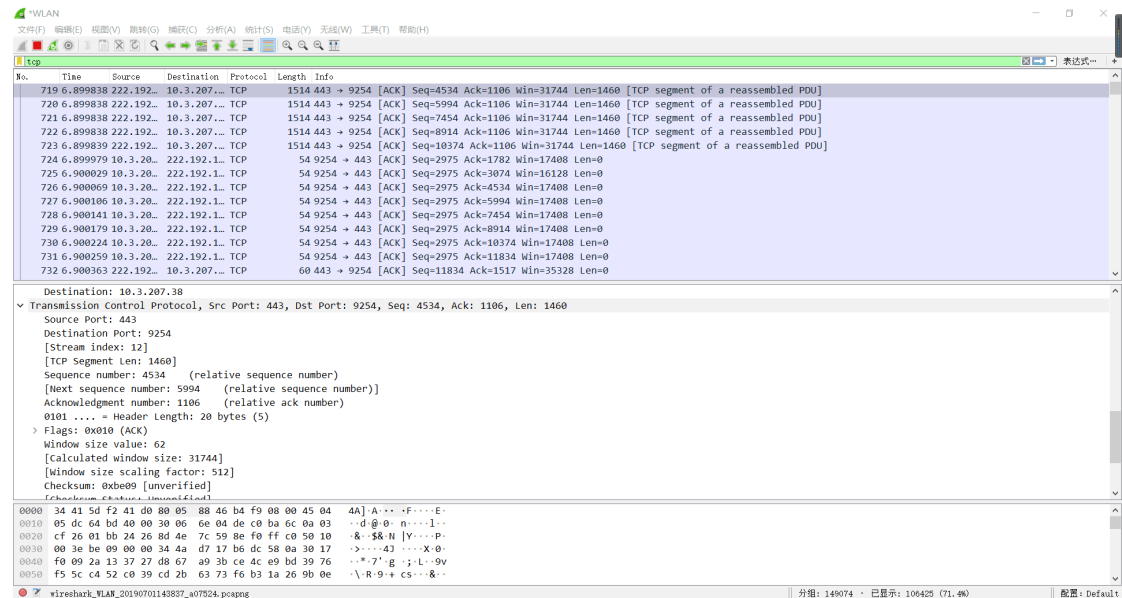
实验报告内容：

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

Wireshark packet capture for UDP traffic. The packet list shows a UDP packet from 10.3.25.1 to 10.3.255.2. The packet details pane shows the UDP header and data. The packet bytes pane shows the raw data in hexadecimal and ASCII.

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	N-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: 1f5: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: u8/3:1f5
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...	OTICQ	121	OTICQ 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 00h...X...E-
0010 01 23 30 9f 00 00 80 11 72 14 0a 03 83 11 0a 03 ..#.....r.....
0020 ff ff d6 83 d6 83 01 0f 70 06 00 44 45 53 4b 54p-DESKT
0030 4f 50 2d 34 48 44 49 4b 31 31 00 b6 1f 67 95 00 OP-4HD1K 11...g...
0040 00 00 00 00 00 00 00 00 00 00 33 27 00 00 00 003'.....
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

Wireshark packet capture for ARP traffic. The packet list shows multiple ARP requests from 191.445.44.1 to 10.3.106.23. The packet details pane shows the ARP request details. The packet bytes pane shows the raw data in hexadecimal and ASCII.

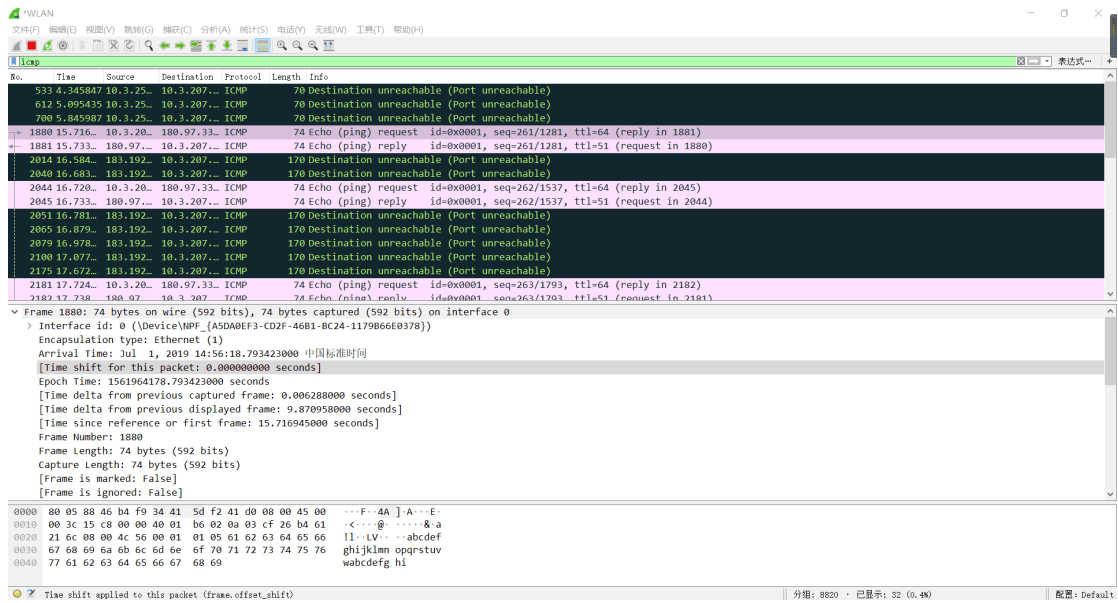
No.	Time	Source	Destination	Protocol	Length	Info
191	.445.44...	Guangdo...	Broadcast	ARP	56	who has 10.3.255.206? Tell 10.3.106.23
191	.445.44...	Guangdo...	Broadcast	ARP	56	who has 10.3.255.205? Tell 10.3.106.23
191	.445.44...	Guangdo...	Broadcast	ARP	56	who has 10.3.255.204? Tell 10.3.106.23
191	.445.44...	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 10.3.255.150? 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

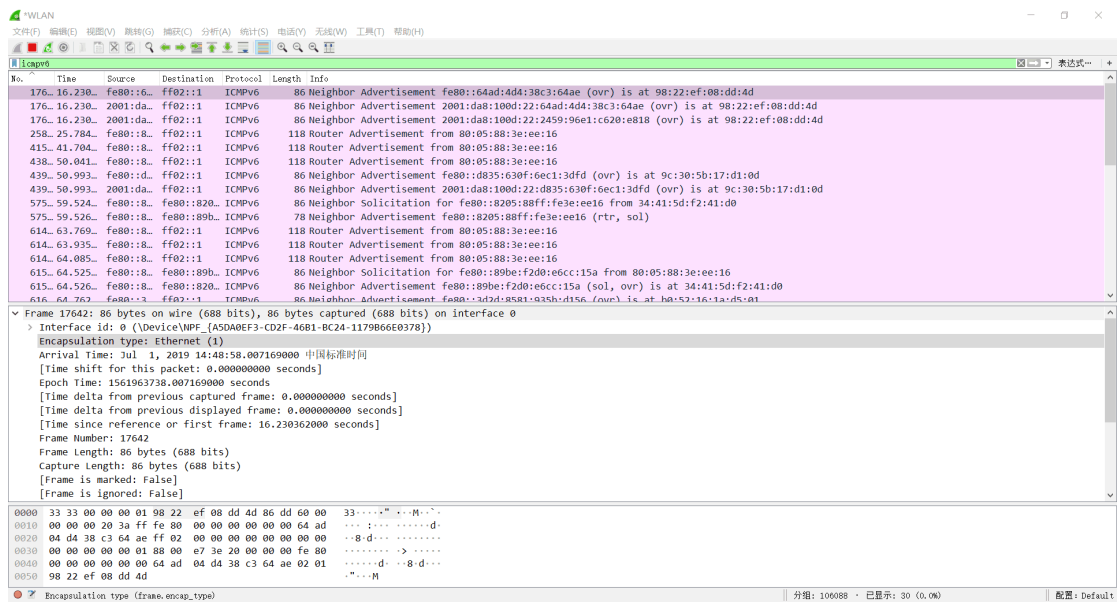
0000 ff ff ff ff ff ff b4 cb 57 12 5b 03 00 06 00 01W[.....
0010 00 00 06 04 00 01 b4 cb 57 12 5b 03 0a 03 6a 17W[.....
0020 00 00 00 00 00 00 0a 03 ff cc 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00

Time relative to time reference or first frame (frame.time_relative) 分组: 214449 · 已显示: 3512 (1.0%) 配置: Default

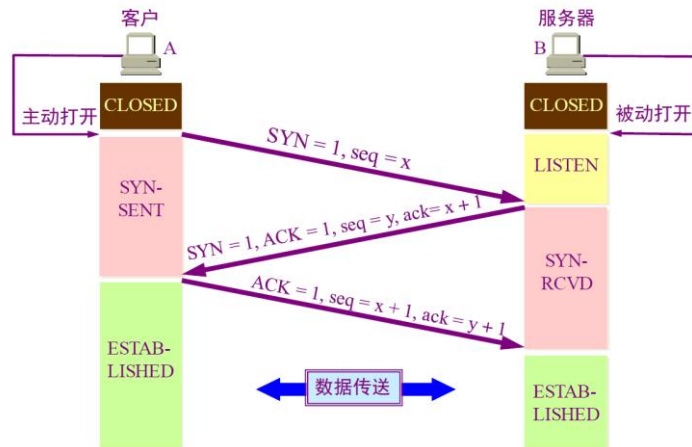
(5) ICMP



(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：

No.	Time	Source	Destination	Protocol	Length	Info
21	1.838975	10.3.207.38	47.240.7.79	TCP	54	15647 → 31178 [ACK] Seq=192 Ack=338 Win=65 Len=0
22	1.839283	10.3.207.38	47.240.7.79	TCP	93	15647 → 31178 [PSH, ACK] Seq=192 Ack=338 Win=65 Len=39
24	1.941449	47.240.7.79	10.3.207.38	TCP	60	31178 → 15647 [ACK] Seq=338 Ack=231 Win=284 Len=0
59	4.475044	10.3.207.38	47.102.49.49	TCP	66	15664 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
60	4.495491	47.102.49.49	10.3.207.38	TCP	62	80 → 15664 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 WS=128
61	4.495604	10.3.207.38	47.102.49.49	TCP	54	15664 → 80 [ACK] Seq=1 Ack=1 Win=17408 Len=0
62	4.495810	10.3.207.38	47.102.49.49	HTTP	463	GET / HTTP/1.1
63	4.517505	47.102.49.49	10.3.207.38	TCP	60	80 → 15664 [ACK] Seq=1 Ack=410 Win=30336 Len=0
64	4.517505	47.102.49.49	10.3.207.38	TCP	60	80 → 15664 [PSH, ACK] Seq=1 Ack=410 Win=30336 Len=4 [TCP segment of a reassembled PDU]
65	4.517505	47.102.49.49	10.3.207.38	TCP	60	80 → 15664 [RST, ACK] Seq=5 Ack=410 Win=30336 Len=0
66	4.517586	10.3.207.38	47.102.49.49	TCP	54	[TCP Dup ACK 61#1] 15664 → 80 [ACK] Seq=410 Ack=1 Win=17408 Len=0
67	4.558338	10.3.207.38	47.102.49.49	TCP	54	15664 → 80 [ACK] Seq=410 Ack=5 Win=17408 Len=0
69	4.667074	10.3.207.38	47.102.49.49	TCP	54	15654 → 80 [FIN, ACK] Seq=1 Ack=1 Win=17516 Len=0
72	4.867197	10.3.207.38	47.102.49.49	TCP	54	[TCP Retransmission] 15654 → 80 [FIN, ACK] Seq=1 Ack=1 Win=17516 Len=0
74	5.437534	10.3.207.38	47.102.49.49	TCP	54	15595 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	5.562505	10.3.207.38	47.102.49.49	TCP	54	[TCP Retransmission] 15654 → 80 [FIN, ACK] Seq=1 Ack=1 Win=17516 Len=0

(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：

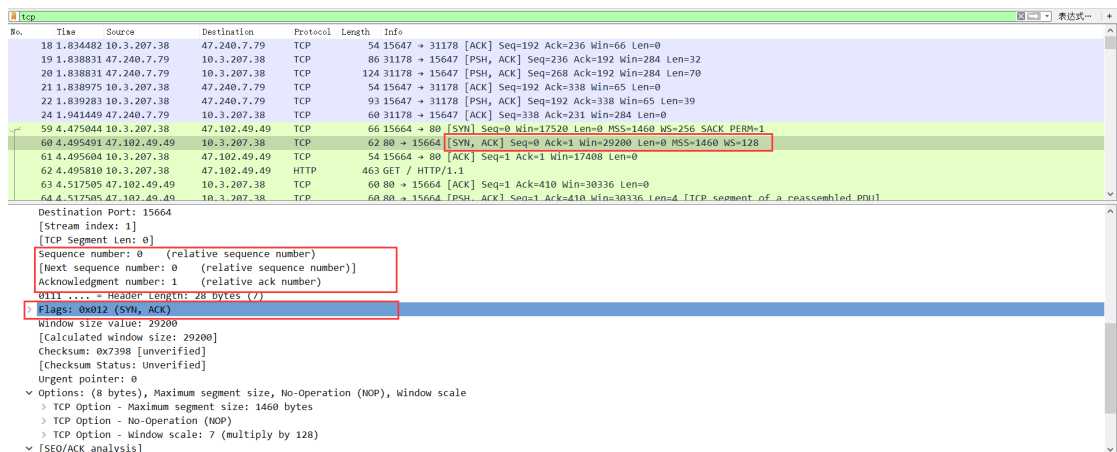
① 第一次握手：

No.	Time	Source	Destination	Protocol	Length	Info
18	1.834482	10.3.207.38	47.240.7.79	TCP	54	15647 → 31178 [ACK] Seq=192 Ack=236 Win=66 Len=0
19	1.838831	47.240.7.79	10.3.207.38	TCP	86	31178 → 15647 [PSH, ACK] Seq=236 Ack=192 Win=284 Len=32
20	1.838831	47.240.7.79	10.3.207.38	TCP	124	31178 → 15647 [PSH, ACK] Seq=268 Ack=192 Win=284 Len=70
21	1.838975	10.3.207.38	47.240.7.79	TCP	54	15647 → 31178 [ACK] Seq=192 Ack=338 Win=65 Len=0
22	1.839283	10.3.207.38	47.240.7.79	TCP	93	15647 → 31178 [PSH, ACK] Seq=192 Ack=338 Win=65 Len=39
24	1.941449	47.240.7.79	10.3.207.38	TCP	60	31178 → 15647 [ACK] Seq=338 Ack=231 Win=284 Len=0
59	4.475044	10.3.207.38	47.102.49.49	TCP	66	15664 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
60	4.495491	47.102.49.49	10.3.207.38	TCP	62	80 → 15664 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 WS=128
61	4.495604	10.3.207.38	47.102.49.49	TCP	54	15664 → 80 [ACK] Seq=1 Ack=1 Win=17408 Len=0
62	4.495810	10.3.207.38	47.102.49.49	HTTP	463	GET / HTTP/1.1
63	4.517505	47.102.49.49	10.3.207.38	TCP	60	80 → 15664 [ACK] Seq=1 Ack=410 Win=30336 Len=0
64	4.517505	47.102.49.49	10.3.207.38	TCP	60	80 → 15664 [PSH, ACK] Seq=1 Ack=410 Win=30336 Len=4 [TCP segment of a reassembled PDU]

Destination Port: 80
[Stream index: 1]
[TCP segment of a reassembled PDU]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
1000 = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window size value: 17520
[Calculated window size: 17520]
Checksum: 0x3df5 [Unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
> TCP Option - Maximum segment size: 1460 bytes
> TCP Option - No-Operation (NOP)
> TCP Option - Window scale: 8 (multiply by 256)
> TCP Option - No-Operation (NOP)

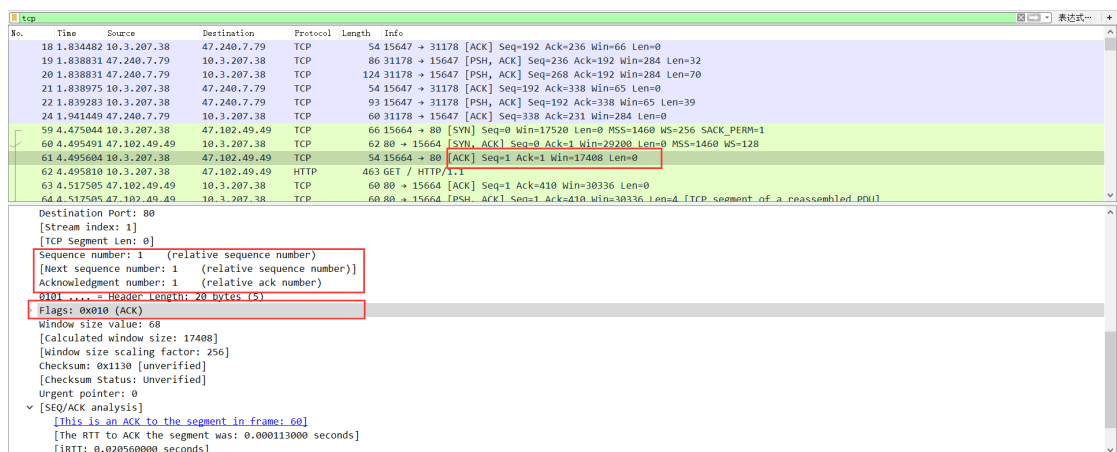
本机 (10.3.207.38) 向目的主机 (47.102.49.49) 请求建立连接，发送请求报文段，设置首部中 SYN=1，同时选择一个初始序列号 seq=0。TCP 规定 SYN 报文段不能携带数据，但是消耗掉一个序号，此时 TCP 客户进程进入 SYN-SENT 状态。

② 第二次握手



目的主机 (47.102.49.49) 收到请求报文后, 同意建立连接, 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



本机 (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 的数据段头部信息

Hypertext Transfer Protocol: 应用层的信息

(1) WWW 服务 (http 协议)

1533	21.317..	10.3.207.38	121.14.32.168	HTTP	1305 GET /slide 2 786 219724.html HTTP/1.1
2433	96.447..	121.14.32.168	10.3.207.38	HTTP	1514 [TCP Previous segment not captured] continuation
2436	96.447..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2437	96.447..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2438	96.447..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2439	96.447..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2440	96.447..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2441	96.447..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2442	96.447..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2452	96.488..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2453	96.488..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2454	96.488..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2455	96.488..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2456	96.488..	121.14.32.168	10.3.207.38	HTTP	1514 [TCP Previous segment not captured] continuation
2461	96.489..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2463	96.489..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2464	96.489..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2475	96.532..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation
2476	96.532..	121.14.32.168	10.3.207.38	HTTP	1514 Continuation

> Frame 1533: 1305 bytes on wire (10440 bits), 1305 bytes captured (10440 bits) on interface 0
 > Ethernet II, Src: IntelCor_f2:41:d0 (34:41:5d:f2:41:d0), Dst: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
 > Internet Protocol Version 4, Src: 10.3.207.38, Dst: 121.14.32.168
 > Transmission Control Protocol, Src Port: 16356, Dst Port: 80, Seq: 1, Ack: 1, Len: 1251
 > Hypertext Transfer Protocol

① 数据链路层

Wireshark - 分组 1533 - WLAN	
> Frame 1533: 1305 bytes on wire (10440 bits), 1305 bytes captured (10440 bits) on interface 0	
> Ethernet II, Src: IntelCor_f2:41:d0 (34:41:5d:f2:41:d0), Dst: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9) <ul style="list-style-type: none"> Destination: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9) <ul style="list-style-type: none"> Address: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9) <ul style="list-style-type: none">0. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast) Source: IntelCor_f2:41:d0 (34:41:5d:f2:41:d0) <ul style="list-style-type: none"> Address: IntelCor_f2:41:d0 (34:41:5d:f2:41:d0) <ul style="list-style-type: none">0. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast) 	
Type: IPv4 (0x0800)	
> Internet Protocol Version 4, Src: 10.3.207.38, Dst: 121.14.32.168	
> Transmission Control Protocol, Src Port: 16356, Dst Port: 80, Seq: 1, Ack: 1, Len: 1251	
> Hypertext Transfer Protocol	

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。

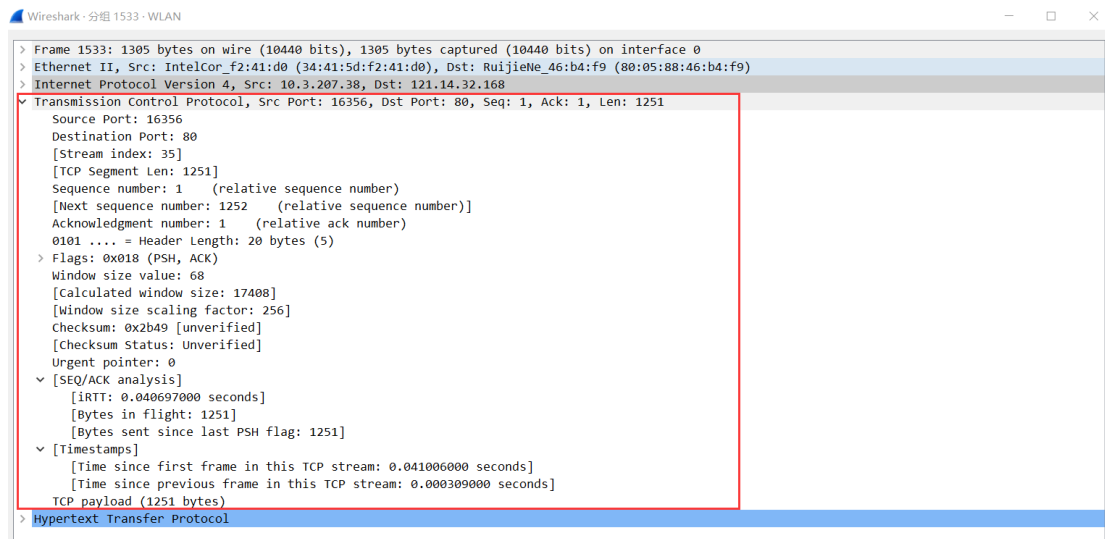
② 网络层

Wireshark - 分组 1533 - WLAN	
> Frame 1533: 1305 bytes on wire (10440 bits), 1305 bytes captured (10440 bits) on interface 0	
> Ethernet II, Src: IntelCor_f2:41:d0 (34:41:5d:f2:41:d0), Dst: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9) <ul style="list-style-type: none"> Internet Protocol Version 4, Src: 10.3.207.38, Dst: 121.14.32.168 <ul style="list-style-type: none"> 0100 = Version: 4 ... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) <ul style="list-style-type: none"> 0000 00.. = Differentiated Services Codepoint: Default (0)00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) Total Length: 1291 Identification: 0x13f0 (5104) Flags: 0x4000, Don't fragment <ul style="list-style-type: none"> 0... = Reserved bit: Not set .1.. = Don't fragment: Set ..0. = More fragments: Not set ...0 0000 0000 0000 = Fragment offset: 0 Time to live: 128 Protocol: TCP (6) Header checksum: 0x6f1d [validation disabled] [Header checksum status: Unverified] Source: 10.3.207.38 Destination: 121.14.32.168 	
> Transmission Control Protocol, Src Port: 16356, Dst Port: 80, Seq: 1, Ack: 1, Len: 1251	
> Hypertext Transfer Protocol	

分析：

版本：4，首部长度的：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

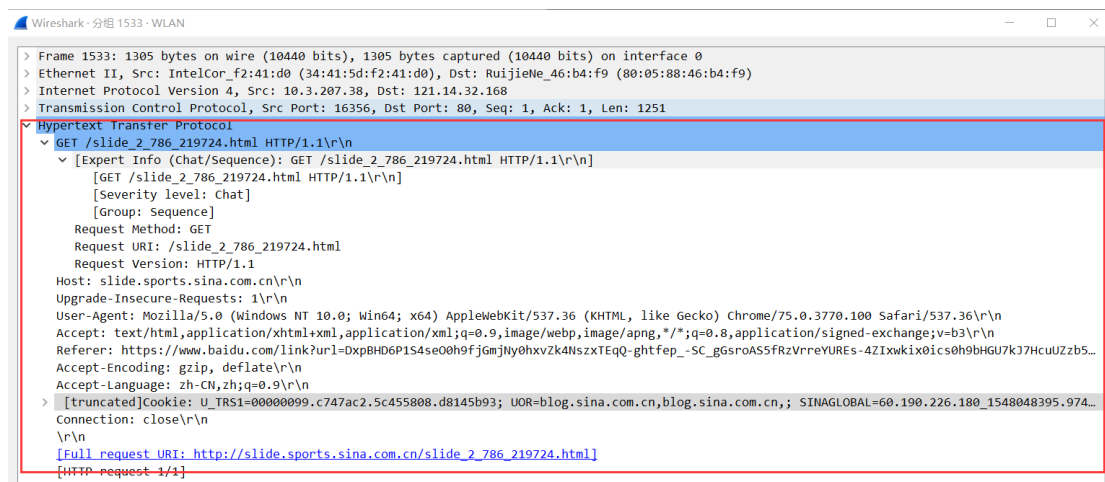
③ 运输层



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)

No.	Time	Source	Destination	Protocol	Length	Info
294..223.94..	74.208.5.15	192.168.169.11	74.208.5.15	SMTP	108 S:	220 gm-x.com (mrpxus001) Nemesis SMTP Service ready
294..223.95..	192.168.169.11	74.208.5.15	74.208.5.15	SMTP	76 C:	EHLO DESKTOP-I00TGPE
295..224.97..	74.208.5.15	192.168.169.11	74.208.5.15	SMTP	176 S:	250-gm-x.com Hello DESKTOP-I00TGPE [58.218.185.148] 250-8BITIME 250-AUTH LOGIN PLAIN 250-SIZE 141557760 250-S
295..224.97..	192.168.169.11	74.208.5.15	74.208.5.15	SMTP	66 C:	AUTH LOGIN
295..225.23..	74.208.5.15	192.168.169.11	74.208.5.15	SMTP	72 S:	334 VXXlcm5hbbu6
295..225.23..	192.168.169.11	74.208.5.15	74.208.5.15	SMTP	80 C:	User: aXhsb2ira69uQgiHawWV29t
295..225.48..	74.208.5.15	192.168.169.11	74.208.5.15	SMTP	72 S:	334 UGFzc3dvcMq6
295..225.48..	192.168.169.11	74.208.5.15	74.208.5.15	SMTP	72 C:	Pass: aXhsb2ira69uWjJay
295..225.77..	74.208.5.15	192.168.169.11	74.208.5.15	SMTP	84 S:	235 Authentication succeeded
295..225.84..	192.168.169.11	74.208.5.15	74.208.5.15	SMTP	97 C:	MAIL FROM: <islomkhon@mail.com> SIZE=1378
296..227.47..	192.168.169.11	74.208.5.15	74.208.5.15	SMTP	84 C:	RCPT TO: <islomkhon@126.com>
296..227.87..	74.208.5.15	192.168.169.11	74.208.5.15	SMTP	62 S:	250 OK
296..227.87..	192.168.169.11	74.208.5.15	74.208.5.15	SMTP	84 C:	RCPT TO: <islomkhon@163.com>
296..228.38..	74.208.5.15	192.168.169.11	74.208.5.15	SMTP	62 S:	250 OK
296..228.38..	192.168.169.11	74.208.5.15	74.208.5.15	SMTP	60 C:	DATA
297..228.63..	74.208.5.15	192.168.169.11	74.208.5.15	SMTP	100 S:	354 Start mail input; end with <CRLF>.<CRLF>
297..228.63..	192.168.169.11	74.208.5.15	74.208.5.15	SMTP	495 C:	DATA fragment, 441 bytes
297..228.93..	192.168.169.11	74.208.5.15	74.208.5.15	SMTP/L..	996 from:	"islomkhon@mail.com" <islomkhon@mail.com>, subject: fddfd, (text/plain) (text/html)
297..229.20..	74.208.5.15	192.168.169.11	74.208.5.15	SMTP	126 S:	250 Requested mail action okay, completed: id=0MGjPS-1hk2Bq1bXh-0004zu

> Frame 29479: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface 0
 > Ethernet II, Src: NewH3CTe_c1:80:01 (1c:ab:34:c1:80:01), Dst: CompalIn_a1:f0:12 (f8:a9:63:a1:f0:12)
 > Internet Protocol Version 4, Src: 74.208.5.15, Dst: 192.168.169.11
 > Transmission Control Protocol, Src Port: 25, Dst Port: 54825, Seq: 1, Ack: 1, Len: 54
 > Simple Mail Transfer Protocol

① 数据链路层

Wireshark · 分组 29670 · smtp.pcapng	
> Frame 29670: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0 > Ethernet II, Src: NewH3CTe_c1:80:01 (1c:ab:34:c1:80:01), Dst: CompalIn_a1:f0:12 (f8:a9:63:a1:f0:12) Destination: CompalIn_a1:f0:12 (f8:a9:63:a1:f0:12) Address: CompalIn_a1:f0:12 (f8:a9:63:a1:f0:12)0. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast) Source: NewH3CTe_c1:80:01 (1c:ab:34:c1:80:01) Address: NewH3CTe_c1:80:01 (1c:ab:34:c1:80:01)0. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast) Type: IPv4 (0x0800) > Internet Protocol Version 4, Src: 74.208.5.15, Dst: 192.168.169.11 > Transmission Control Protocol, Src Port: 25, Dst Port: 54825, Seq: 286, Ack: 152, Len: 8 > Simple Mail Transfer Protocol	

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。

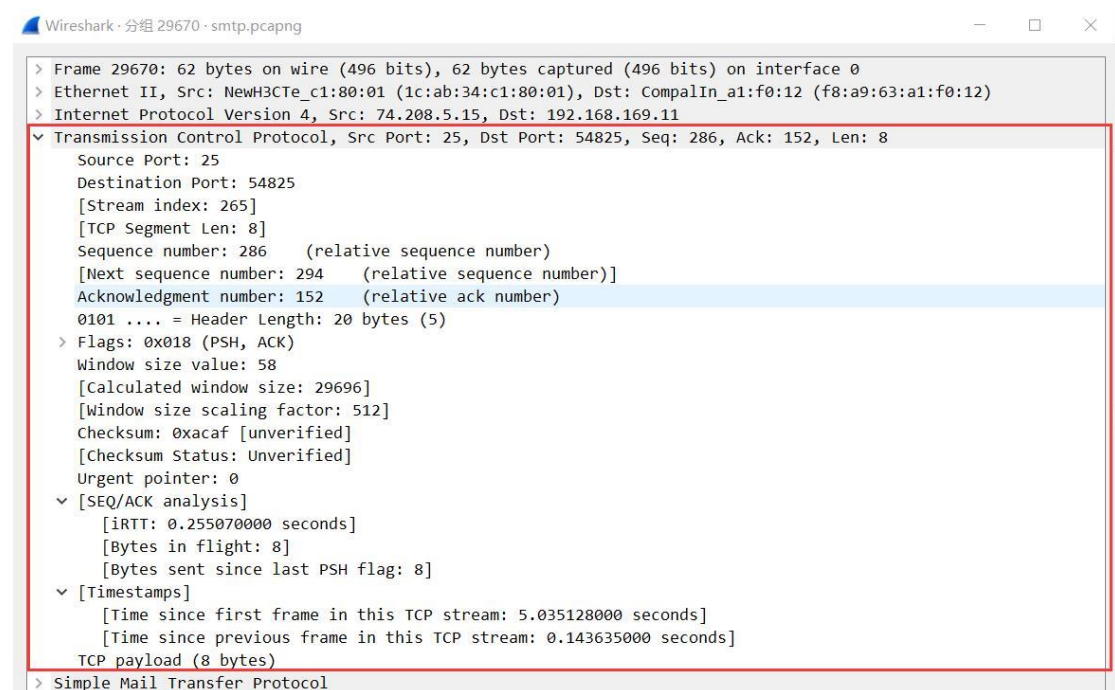
② 网络层

Wireshark · 分组 29670 · smtp.pcapng	
> Frame 29670: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0 > Ethernet II, Src: NewH3CTe_c1:80:01 (1c:ab:34:c1:80:01), Dst: CompalIn_a1:f0:12 (f8:a9:63:a1:f0:12) > Internet Protocol Version 4, Src: 74.208.5.15, Dst: 192.168.169.11 0100 = Version: 4 ... 0101 = Header Length: 20 bytes (5) Differntiated 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: 48 Identification: 0x9089 (37001) Flags: 0x4000, Don't fragment 0... .. = Reserved bit: Not set .1.. .. = Don't fragment: Set ..0. = More fragments: Not set ...0 0000 0000 0000 = Fragment offset: 0 Time to live: 48 Protocol: TCP (6) Header checksum: 0x00ac [validation disabled] [Header checksum status: Unverified] Source: 74.208.5.15 Destination: 192.168.169.11 > Transmission Control Protocol, Src Port: 25, Dst Port: 54825, Seq: 286, Ack: 152, Len: 8 > Simple Mail Transfer Protocol	

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。

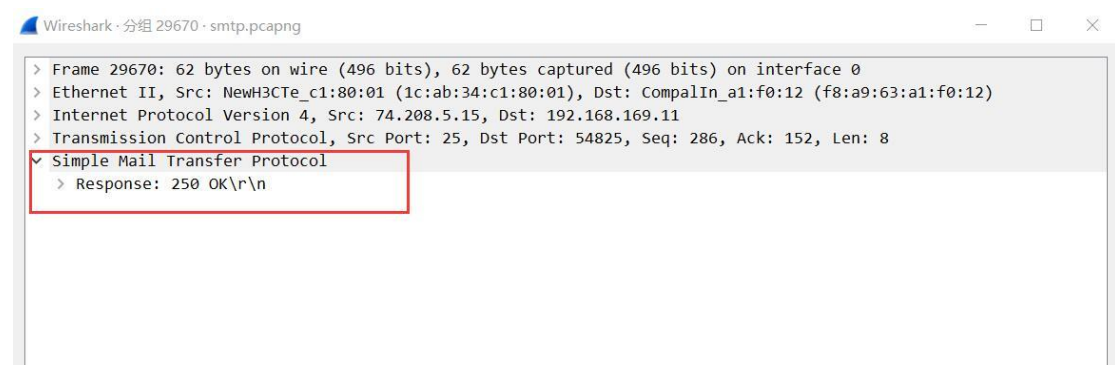
③ 运输层



分析:

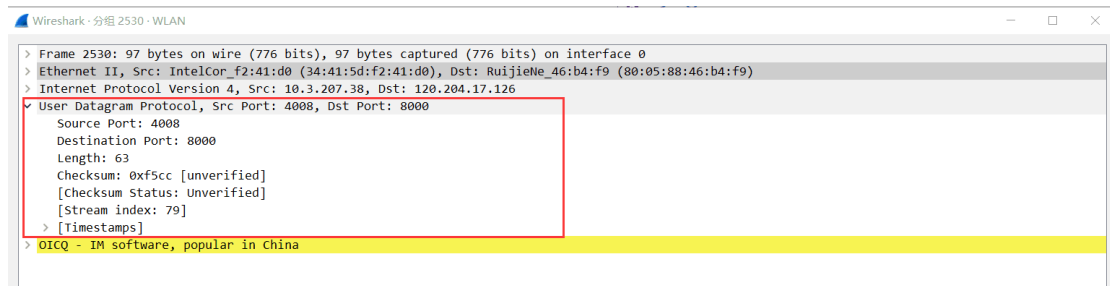
源端口号为 25，目的端口号为 54825，seq=286，ack=152，接收窗口大小为 58 字节。

④ 应用层



分析：采用 SMTP 协议，250 OK 表示要求的邮件操作完成。

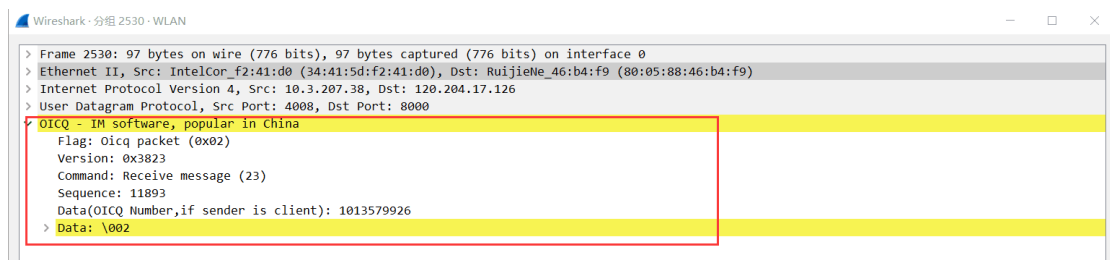
③ 运输层



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

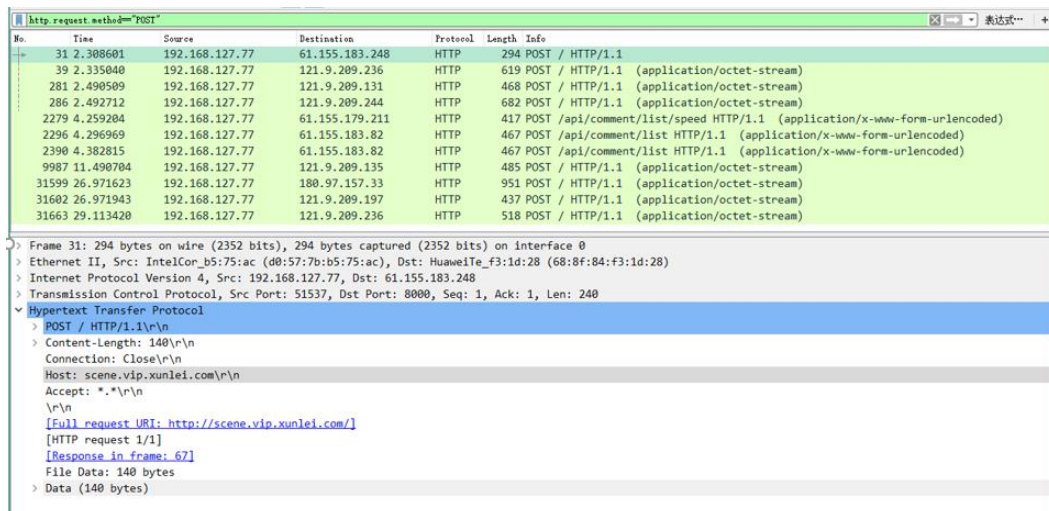


分析:

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词：

No.	Time	Source	Destination	Protocol	Length	Info
31	2.308601	192.168.12...	61.155.183...	HTTP	294	POST / HTTP/1.1
34	2.310611	192.168.12...	180.97.85...	HTTP	455	GET /cinemas/download_recommend?nonce=21246987&sig=PKPPr_n1_tU0Qo0h87ag22glicU=&page=0&accesskey=pc.xunlei&clientv=10.0.1.28&position=pc_download_tab&download...
39	2.315040	192.168.12...	121.9.209...	HTTP	619	POST / HTTP/1.1 (application/octet-stream)
63	2.365041	180.97.85...	192.168.12...	HTTP	151	HTTP/1.1 200 OK (application/json)
67	2.386344	61.155.183...	192.168.12...	HTTP	944	HTTP/1.1 200 OK (text/plain)
108	2.422559	121.9.209...	192.168.12...	HTTP	748	HTTP/1.1 200 OK (text/plain)
129	2.442562	192.168.12...	192.168.12...	HTTP	127	[TCP Previous segment not captured] Continuation
151	2.443030	192.168.12...	61.147.81.6	HTTP	54	GET /f2b4f40b00b17618964ad37b7593487imageview/1/a/500/h/180/interlace/1/format/jpg HTTP/1.1
164	2.445869	61.147.81.6	192.168.12...	HTTP	1514	Continuation
165	2.445870	61.147.81.6	192.168.12...	HTTP	1514	Continuation
172	2.449599	61.147.81.6	192.168.12...	HTTP	1514	Continuation
173	2.449600	61.147.81.6	192.168.12...	HTTP	1514	Continuation
200	2.458326	192.168.12...	180.101.56...	HTTP	54	GET /usrimg/135626991/default/1506349469/300x300 HTTP/1.1
216	2.471441	61.147.81.6	192.168.12...	HTTP	209	[TCP Previous segment not captured] Continuation
240	2.474564	61.147.81.6	192.168.12...	HTTP	127	[TCP Previous segment not captured] Continuation
240	2.474565	61.147.81.6	192.168.12...	HTTP	127	[TCP Previous segment not captured] Continuation

Frame 34: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface 0
Ethernet II, Src: IntelCor_b5:75:ac (d0:57:7b:b5:75:ac), Dst: HuaweiTe_f3:1d:28 (68:8f:84:f3:1d:28)
Internet Protocol Version 4, Src: 192.168.127.77, Dst: 180.97.85.236
Transmission Control Protocol, Src Port: 51539, Dst Port: 80, Seq: 1, Ack: 1, Len: 401
Hypertext Transfer Protocol
[Truncated]GET /cinemas/download_recommend?nonce=21246987&sig=PKPPr_n1_tU0Qo0h87ag22glicU=&page=0&accesskey=pc.xunlei&clientv=10.0.1.28&position=pc_download_tab&downloadtext=360yun_setup_2.1.0.1147.exe×tamp=1531812962&appid=144...
Host: api.shoulei-sai.xunlei.com\r\n
Account-Id: 0\r\n
Chat-Version: 2\r\n
Peer-Id: C8D3F239482000Q\r\n
User-Id: 0\r\n
Session-Id: \r\n
Connection: close\r\n
App-Type: pc_xunlei\r\n
\r\n
[Full request URI: http://api.shoulei-sai.xunlei.com/cinemas/download_recommend?nonce=21246987&sig=PKPPr_n1_tU0Qo0h87ag22glicU=&page=0&accesskey=pc.xunlei&clientv=10.0.1.28&position=pc_download_tab&downloadtext=360yun_setup_2.1.0.1147.exe×tamp=1531812962&appid=144...]
[HTTP request 1/1]
[Response in frame: 63]

③ 追踪迅雷下载的 TCP 流：

>	Frame 31: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface 0
>	Ethernet II, Src: IntelCor_b5:75:ac (d0:57:7b:b5:75:ac), Dst: HuaweiTe_f3:1d:28 (68:8f:84:f3:1d:28)
>	Internet Protocol Version 4, Src: 192.168.127.77, Dst: 61.155.183.248
>	Transmission Control Protocol, Src Port: 51537, Dst Port: 8000, Seq: 1, Ack: 1, Len: 240
>	Hypertext Transfer Protocol
>	POST / HTTP/1.1\r\n
>	Content-Length: 140\r\n
>	Connection: Close\r\n
>	Host: scene.vip.xunlei.com\r\n
>	Accept: */*\r\n
>	\r\n
>	[Full request URI: http://scene.vip.xunlei.com/]
>	[HTTP request 1/1]
>	[Response in frame: 67]
>	File Data: 140 bytes
>	Data (140 bytes)

>	Frame 39: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface 0
>	Ethernet II, Src: IntelCor_b5:75:ac (d0:57:7b:b5:75:ac), Dst: HuaweiTe_f3:1d:28 (68:8f:84:f3:1d:28)
>	Internet Protocol Version 4, Src: 192.168.127.77, Dst: 121.9.209.236
>	Transmission Control Protocol, Src Port: 51538, Dst Port: 80, Seq: 1, Ack: 1, Len: 565
>	Hypertext Transfer Protocol
>	POST / HTTP/1.1\r\n
>	Host: hub5idx.shub.sandai.net:80\r\n
>	Content-type: application/octet-stream\r\n
>	Content-Length: 432\r\n
>	Connection: Close\r\n
>	\r\n
>	[Full request URI: http://hub5idx.shub.sandai.net:80/]
>	[HTTP request 1/1]
>	[Response in frame: 108]
>	File Data: 432 bytes
>	Media Type


```
Wireshark · 追踪 TCP 流 (tcp.stream eq 2) · Thunder

POST / HTTP/1.1
Host: hub5idx.shub.sandai.net:80
Content-type: application/octet-stream
Content-Length: 432
Connection: Close

.X.&.'.....NT0.4W
S..?0y\.._a[.:i~. ^..D8}.....,r`..0...^U...1.Kr...s.C""...9...v....(d;jX..
..6.M.W\..
..i;[.y.....X.....P3... ..|.i.<!=Lt.U.J...I.y=?...V.J.....#Z..J.....h.X.G.K.
933.....g.r...o.....Av.$Q.a(...7...w.o...!...r1:.....@5!..y.r.hJm...z;.)A.. B.
5U..H#...G43.6C=[..T...%:.G.M81Y....1
.....H..on..."<..K...X..Z4j....|.....g.....c..la.1..o..u.
{.....U.....bP.C..j.....HTTP/1.1 200 OK
Server: openresty/1.9.3.2
Date: Sun, 08 Jul 2018 01:22:43 GMT
Content-Type: text/plain
Connection: close
Content-Length: 2004

.....61vx.w.5..
...J...I.y=?...V.J.....#Z..J.....h.X.G.K.933.....+u..FFZ...9%.....=<uE.s\...0B...-(...VI.eE...
...>m..`....[)....qI.....#.'+e...q.....|.mb6.{...{C..YF.i./
\.....fh.mX...k=s.k..d...xb.....K.....+...2'.C..W.Q.gL,b...^H..9....}.Nr.F....4,...B.v..d/[.
6T5m]..qF....-a.e_....om..&u .. .....i9..oc..An.i..E&?.....h...
3...f4e..<cl..k...R..#.....3.#(.u...{..U...Z....>..6.v..T.L.....
...*.R.aO.E..tP2.R...L..#...!..1..a..i...b.9.rk)..$. ....1\6. ....=...3d...B.U.
%.Xog...h....q0vt.x.t...]y.O....0..&m.s.>A.....+...=Sr..M2*..Y..~..H...H....K....}.V.*..^..!
C.OC...G.VG...s....81..&."wr"=..m....0...-T\...nA%.....
.(.....]6.v.f.Y.%3..z
```

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。

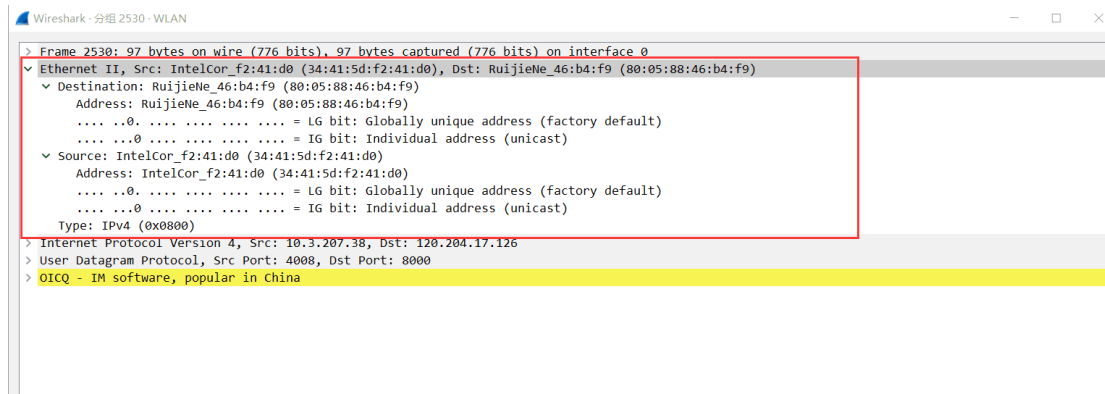
(4) QQ 通信 (即 OICQ)

正在捕获 WLAN

No.	Time	Source	Destination	Protocol	Length	Info
3728	17.414..	120.204.17.126	10.3.207.38	OICQ	121	OICQ Protocol
4242	20.376..	10.3.207.38	120.204.17.126	OICQ	81	OICQ Protocol
4263	20.402..	120.204.17.126	10.3.207.38	OICQ	105	OICQ Protocol
4722	22.728..	120.204.17.126	10.3.207.38	OICQ	121	OICQ Protocol
4842	23.546..	10.3.207.38	120.204.17.126	OICQ	81	OICQ Protocol
4873	23.572..	120.204.17.126	10.3.207.38	OICQ	89	OICQ Protocol
5168	24.933..	120.204.17.126	10.3.207.38	OICQ	121	OICQ Protocol
7426	36.837..	120.204.17.126	10.3.207.38	OICQ	121	OICQ Protocol
7635	37.612..	120.204.17.126	10.3.207.38	OICQ	121	OICQ Protocol
7636	37.634..	120.204.17.126	10.3.207.38	OICQ	177	OICQ Protocol
7637	37.635..	10.3.207.38	120.204.17.126	OICQ	97	OICQ Protocol
7638	37.635..	10.3.207.38	120.204.17.126	OICQ	137	OICQ Protocol
7645	37.690..	120.204.17.126	10.3.207.38	OICQ	89	OICQ Protocol
7646	37.691..	10.3.207.38	120.204.17.126	OICQ	89	OICQ Protocol
7647	37.691..	10.3.207.38	120.204.17.126	OICQ	89	OICQ Protocol
7648	37.719..	120.204.17.126	10.3.207.38	OICQ	873	OICQ Protocol
7658	37.747..	120.204.17.126	10.3.207.38	OICQ	105	OICQ Protocol
8579	38.222..	10.3.207.38	120.204.17.126	OICQ	80	OICQ Protocol
8580	38.261..	120.204.17.126	10.3.207.38	OICQ	689	OICQ Protocol

> Frame 2530: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0
> Ethernet II, Src: IntelCor_F2:41:d0 (34:41:5d:f2:41:d0), Dst: RuijieNe_46:b4:f9 (80:05:88:46:b4:f9)
> Internet Protocol Version 4, Src: 10.3.207.38, Dst: 120.204.17.126
> User Datagram Protocol, Src Port: 4008, Dst Port: 8000
> OICQ - IM software, popular in China

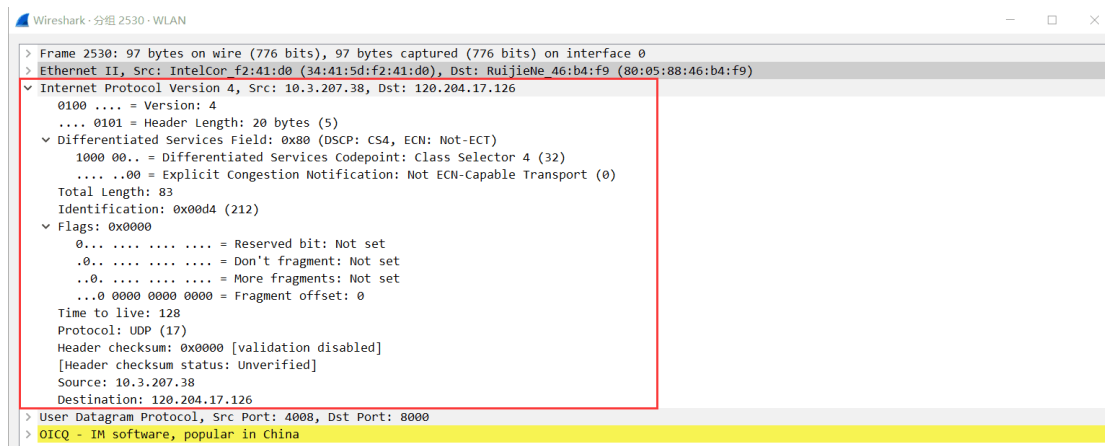
① 数据链路层



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, 其功能是能撷取网络封包, 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!