**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 胡钧耀 学 号 06192081

专业班级 计科2019-4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。

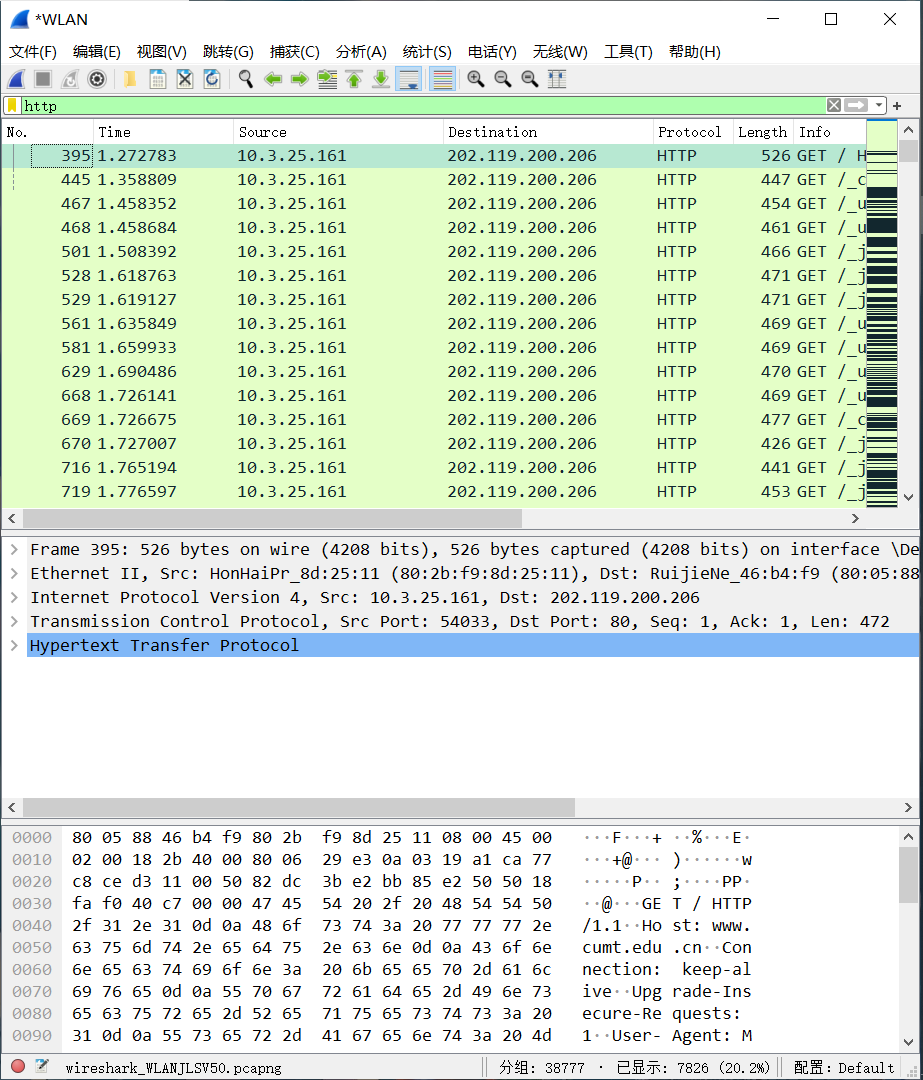
**实验报告要求：**

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。

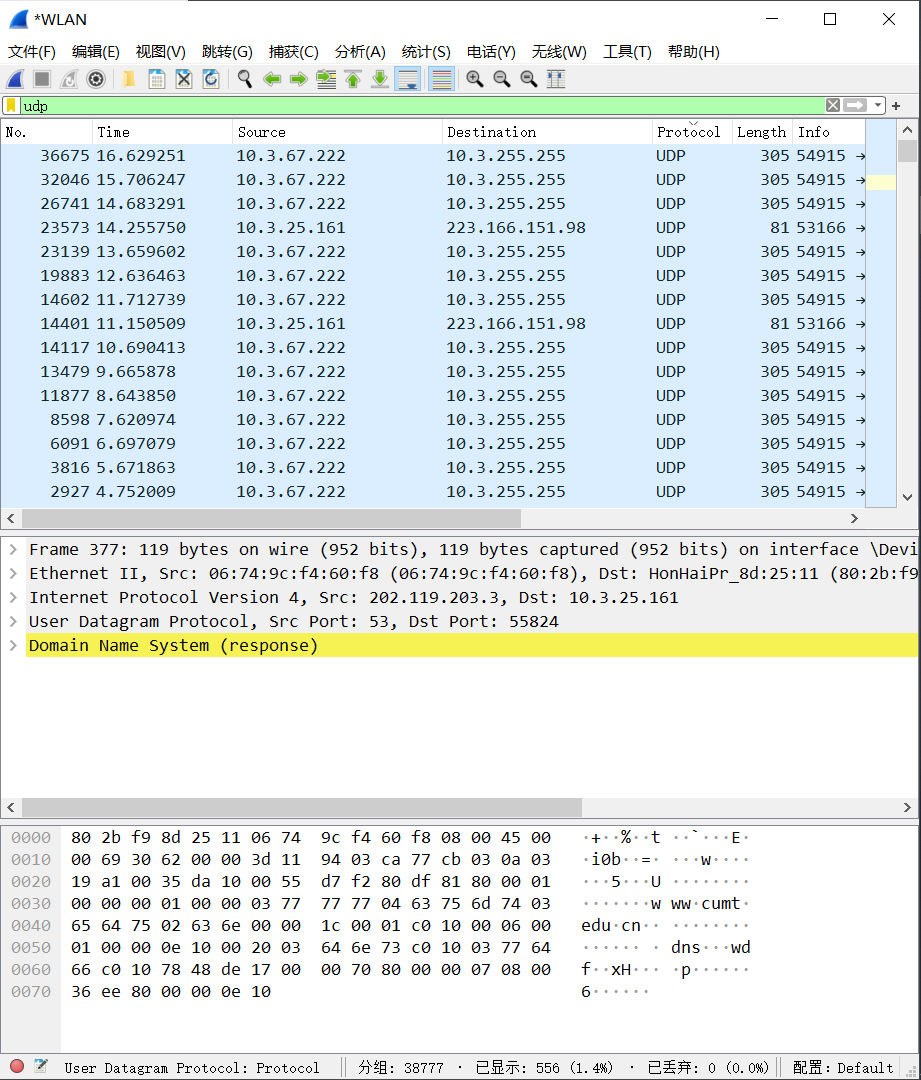
**实验报告内容：**

**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**

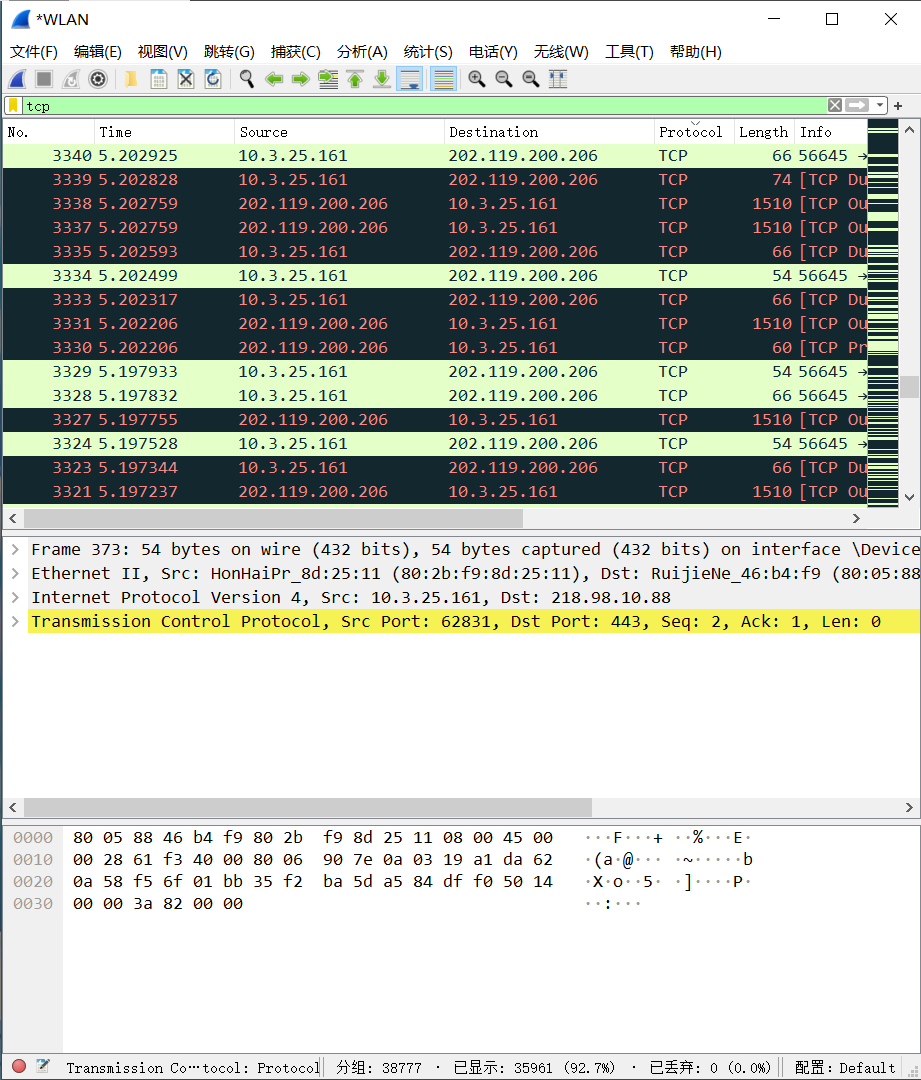
**HTTP**



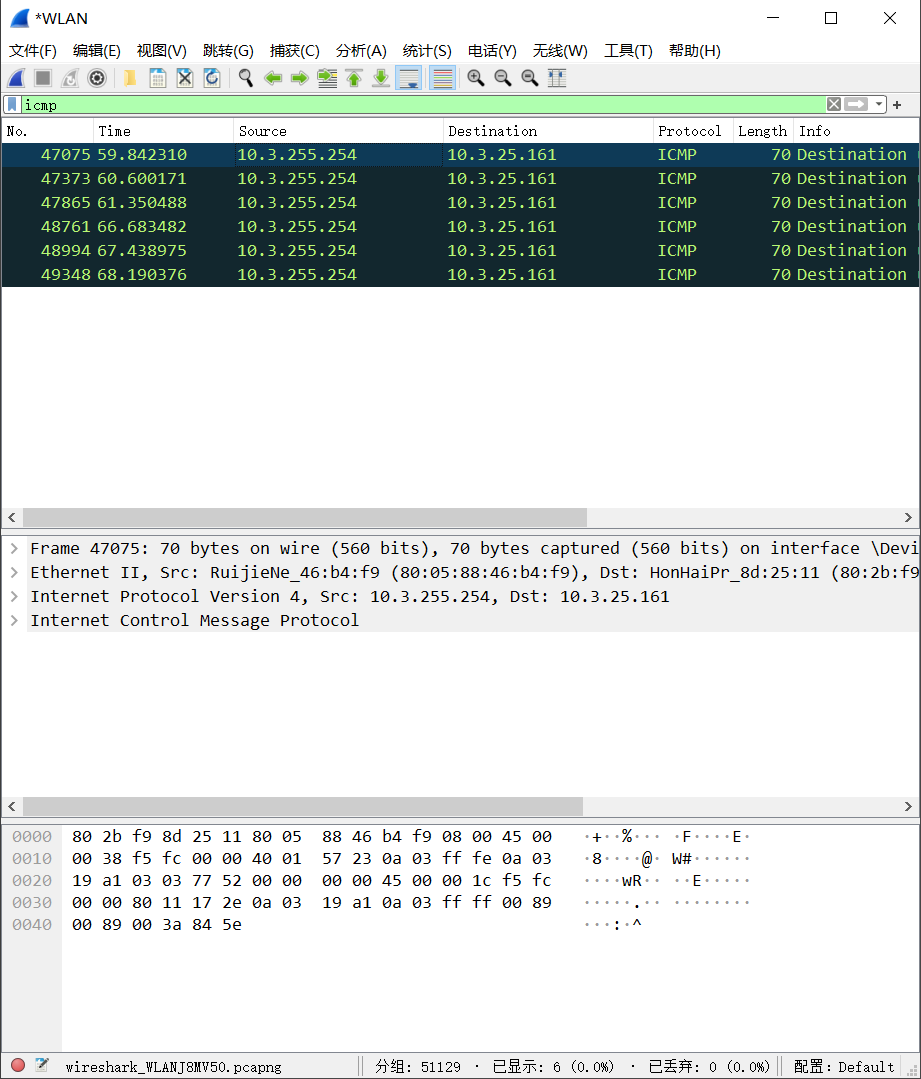
**UDP**



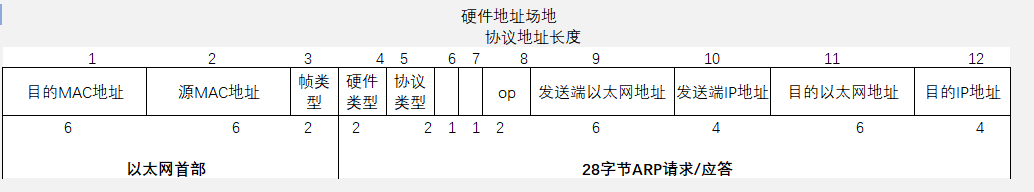
**TCP**



**ICMP**



**2. 获取ARP协议数据单元，进行报文格式解析**



字段1：ARP请求的目的以太网地址，全1时，代表广播地址。

字段2：发送ARP请求的以太网地址。

字段3：以太网帧类型表示后面的数据类型，ARP请求和ARP应答此字段为：0x0806。

字段4：硬件地址类型，硬件地址不止以太网一种，是以太网类型时，值为1。

字段5：表示要映射的协议地址的类型，要对IPv4地址进行映射，此值为0x0800。

字段6和7：表示硬件地址长度和协议地址长度，MAC地址占6字节，IP地址占4字节。

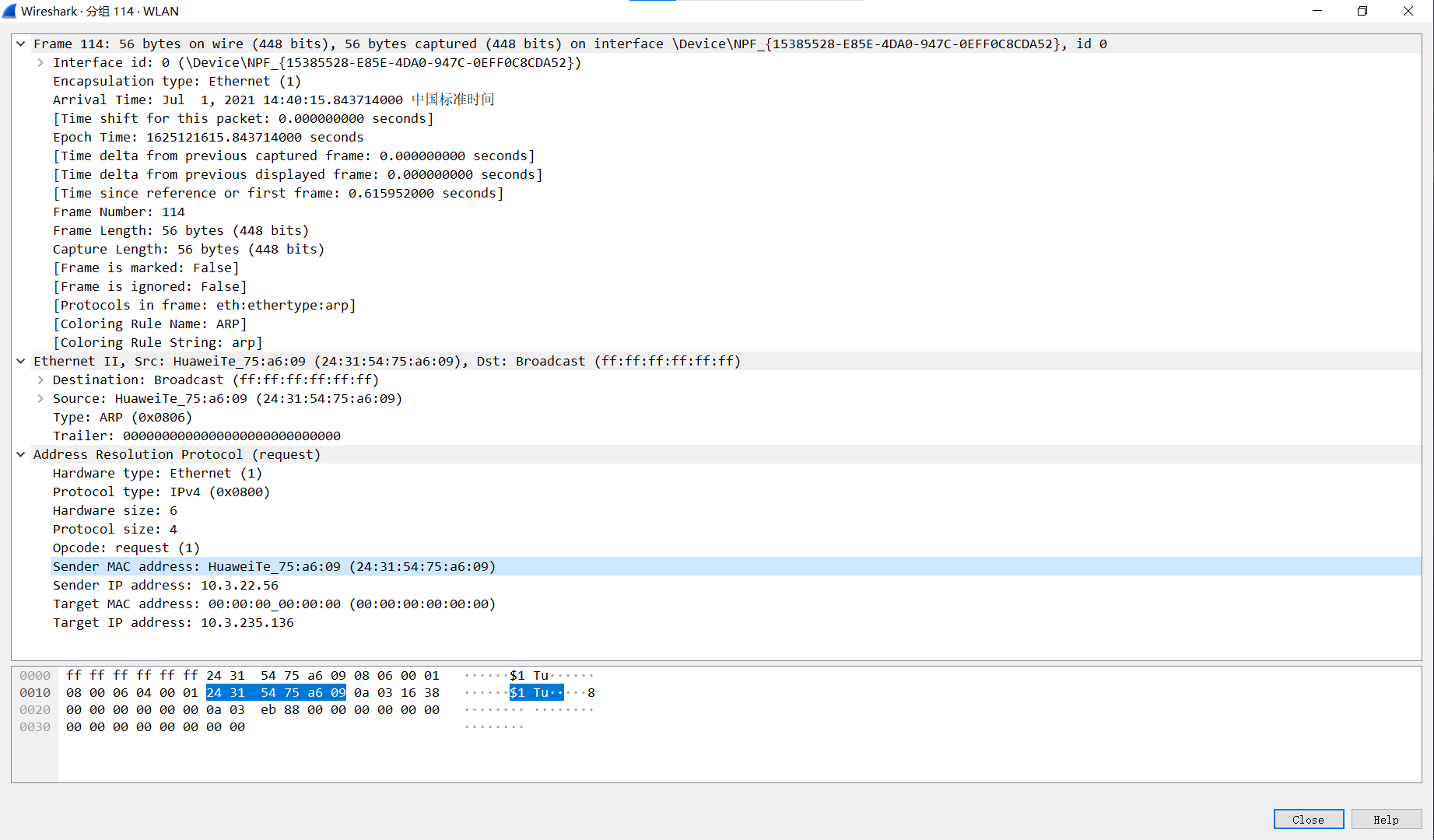
字段8：是操作类型字段，值为1，表示进行ARP请求；值为2，表示进行ARP应答；值为3，表示进行RARP请求；值为4，表示进行RARP应答。

字段9：是发送端ARP请求或应答的硬件地址，这里是以太网地址，和字段2相同。

字段10：是发送ARP请求或应答的IP地址。

字段11和12：是目的端的硬件地址和IP地址。

**（1）请求报文**



0000 ff ff ff ff ff ff 24 31 54 75 a6 09 08 06 00 01 ......$1Tu......

0010 08 00 06 04 00 01 24 31 54 75 a6 09 0a 03 16 38 ......$1Tu.....8

0020 00 00 00 00 00 00 0a 03 eb 88 00 00 00 00 00 00 ................

0030 00 00 00 00 00 00 00 00 ........

ff ff ff ff ff ff ---- 目的MAC地址，全1为广播地址（Broadcast）

24 31 54 75 a6 09 ---- 本机MAC地址（HuaweiTe）

08 06 ---------------- 数据帧类型0806，代表是ARP报文

00 01 ---------------- 硬件类型（Ethernet，以太网）

08 00 ---------------- 协议类型（IPv4）

06 ------------------- 硬件地址长度为6

04 ------------------- 协议地址长度为4

00 01 ---------------- 操作码为1，表示请求

24 31 54 75 a6 09 ---- 发送端ARP请求的硬件地址，以太网地址

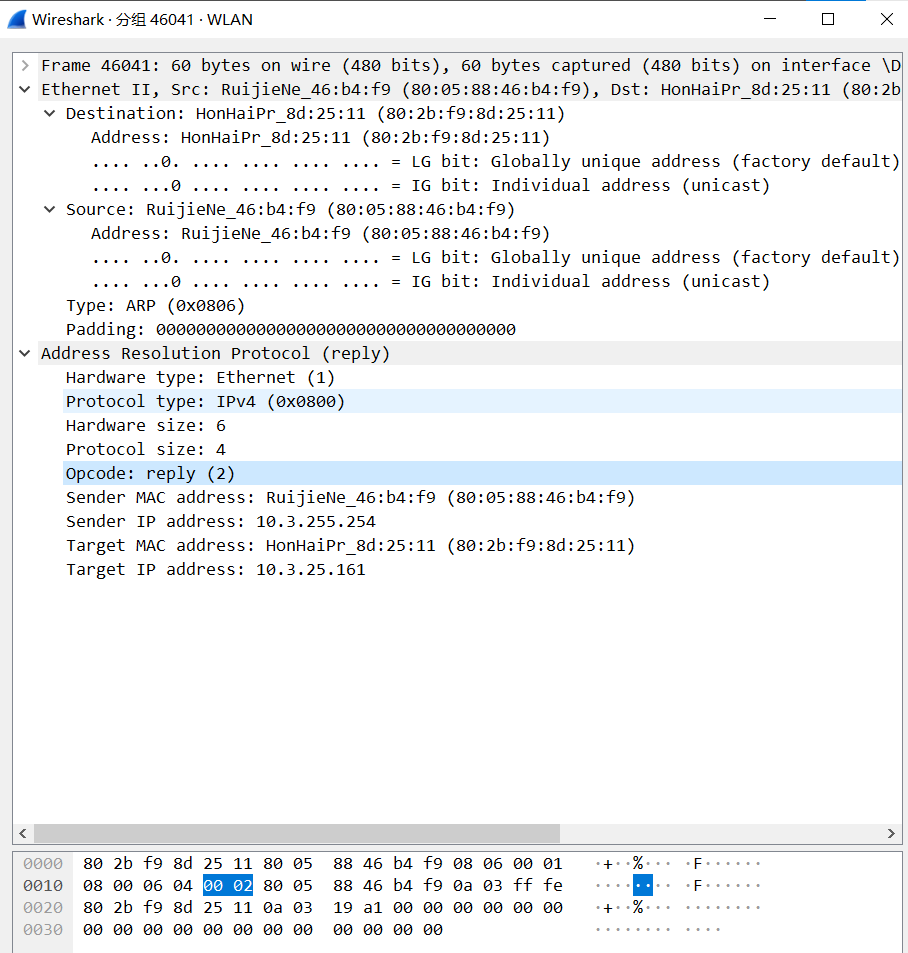
0a 03 16 38 ---------- 发送端IP地址

00 00 00 00 00 00 ---- 目的以太网地址

0a 03 eb 88 ---------- 目的IP地址

00 00 00 00 00 00 00 00 00 00 00 00 00 00 – 超额（Trailer）保证56个字节

**（2）应答报文**



0000 80 2b f9 8d 25 11 80 05 88 46 b4 f9 08 06 00 01 .+..%....F......

0010 08 00 06 04 00 02 80 05 88 46 b4 f9 0a 03 ff fe .........F......

0020 80 2b f9 8d 25 11 0a 03 19 a1 00 00 00 00 00 00 .+..%...........

0030 00 00 00 00 00 00 00 00 00 00 00 00 ............

80 2b f9 8d 25 11 ---- 目的MAC地址（HonHaiPr）

80 05 88 46 b4 f9 ---- 本机MAC地址（RuijieNe）

08 06 ---------------- 数据帧类型0806，代表是ARP报文

00 01 ---------------- 硬件类型（Ethernet，以太网）

08 00 ---------------- 协议类型（IPv4）

06 ------------------- 硬件地址长度为6

04 ------------------- 协议地址长度为4

00 01 ---------------- 操作码为2，表示响应

24 31 54 75 a6 09 ---- 发送端ARP请求的硬件地址，以太网地址

0a 03 ff fe ---------- 发送端IP地址

80 2b f9 8d 25 11 ---- 目的以太网地址

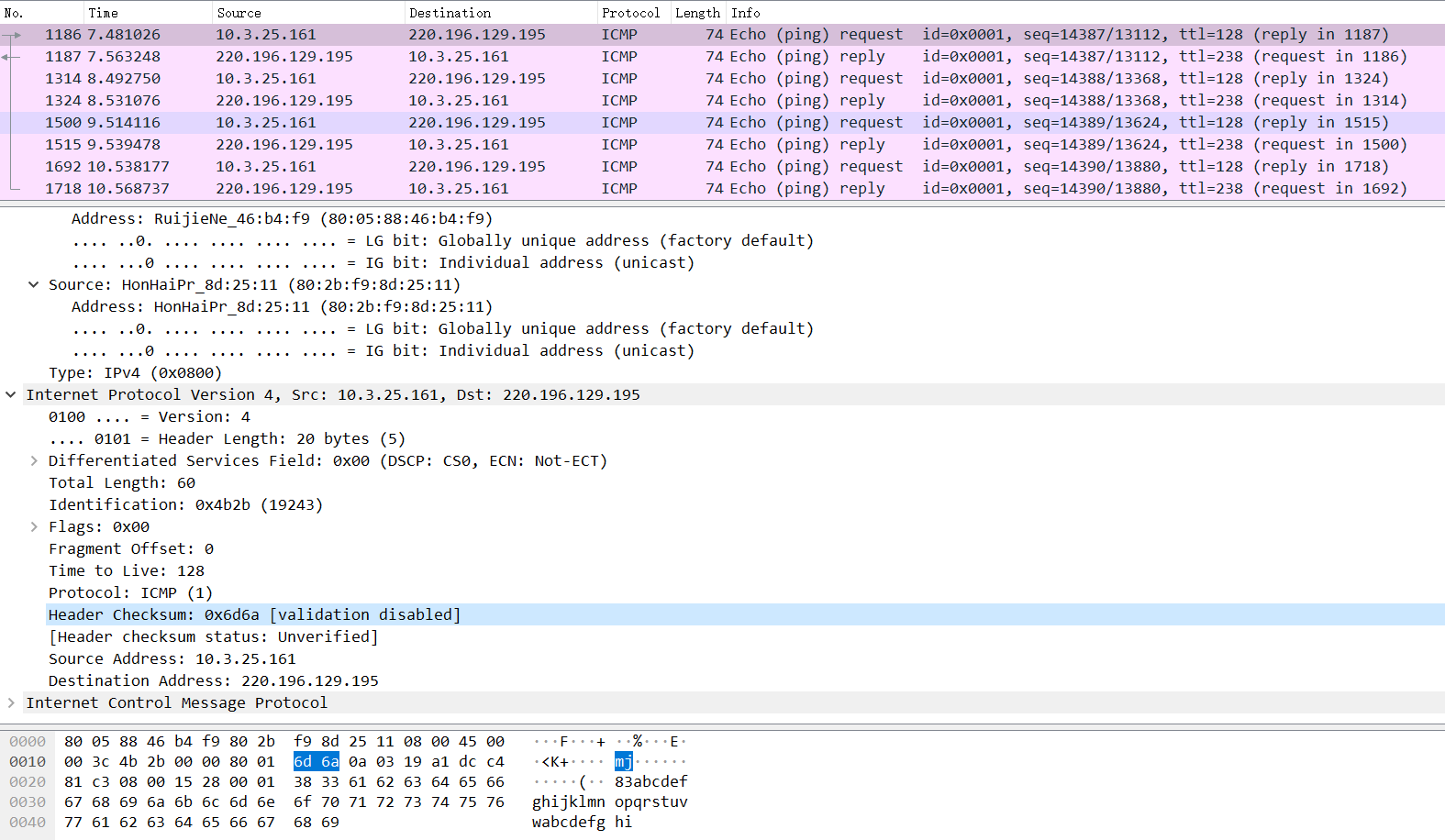
0a 03 19 a1 ---------- 目的IP地址

00 00 00 00 00 00 00 00 00 00 00 00 00 00 – 填充（Padding）保证56个字节

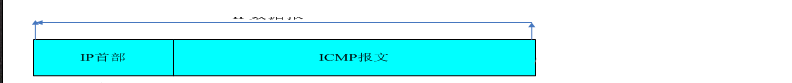
**3.获取ping、tracert、nslookup命令对应的交互数据，进行报文格式解析**

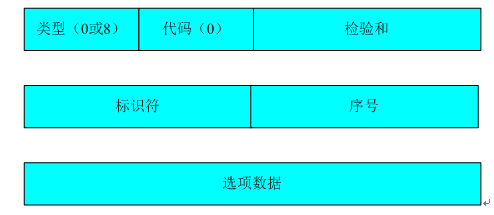
**ping**





可以看到windows下ping默认执行4次ping程序，wireshark抓到8个ICMP查询报文，具体看一次请求和应答过程。一个包由报文由IP首部和ICMP报文组成。





0000 80 05 88 46 b4 f9 80 2b f9 8d 25 11 08 00 45 00 ...F...+..%...E.

0010 00 3c 4b 2b 00 00 80 01 6d 6a 0a 03 19 a1 dc c4 .<K+....mj......

0020 81 c3 08 00 15 28 00 01 38 33 61 62 63 64 65 66 .....(..83abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmnopqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabcdefghi

80 05 88 46 b4 f9 ----- 目的MAC地址（RuijieNe）

2b f9 8d 25 11 08 ----- 本机MAC地址（HonHaiPr）

08 00 ---------------- 协议类型（IPv4）

45 ------------------- 协议版本（4），头长度（20字节）（5）

00 ------------------- 忽略显式拥塞

00 3c ---------------- 总长度60

4b 2b ---------------- 识别码19243

00 00 ---------------- 偏移量

80 ------------------- TTL时间 128

01 ------------------- 协议为ICMP（1）

6d 6a ---------------- 头部检验和（未经验证）

0a 03 19 a1 ---------- 源地址

dc c4 81 c3 ---------- 目标地址

08 ------------------- 类型为8，ping请求

00 ------------------- 代码0

15 28 ---------------- 检验和（正确）

00 01 ---------------- 标识符（windows为LE，0x0100，256）

38 33 ---------------- 序列号（windows为LE，0x3338，13112）

61 62 63 . . . 69 ---- 发送的数据（abc..i）

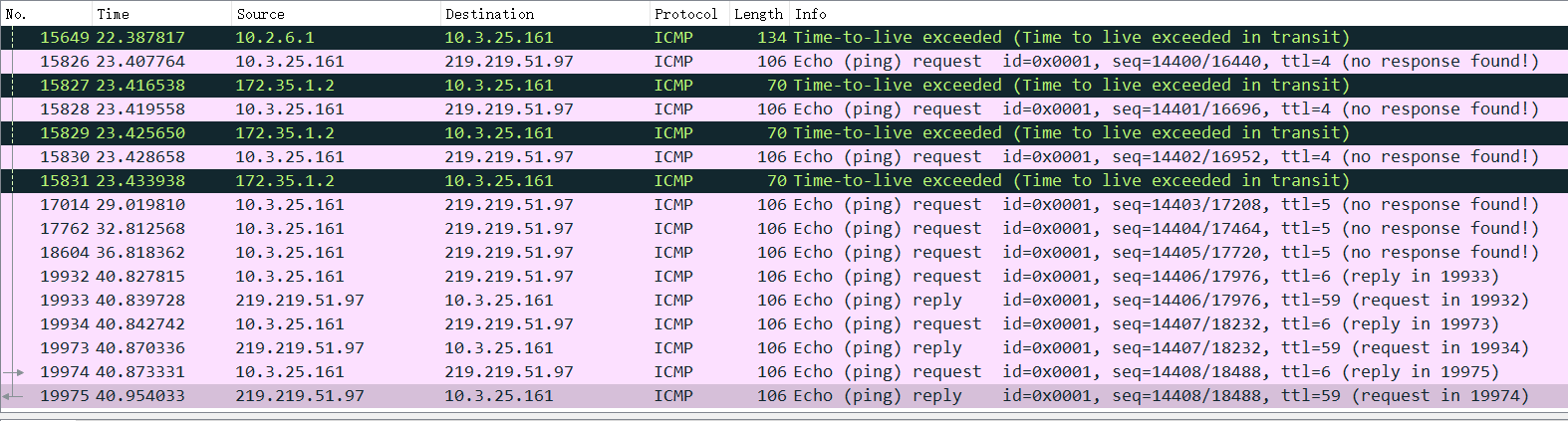
通过查询ICMP报文类型可知，Type为8的包为回射请求（Ping请求）

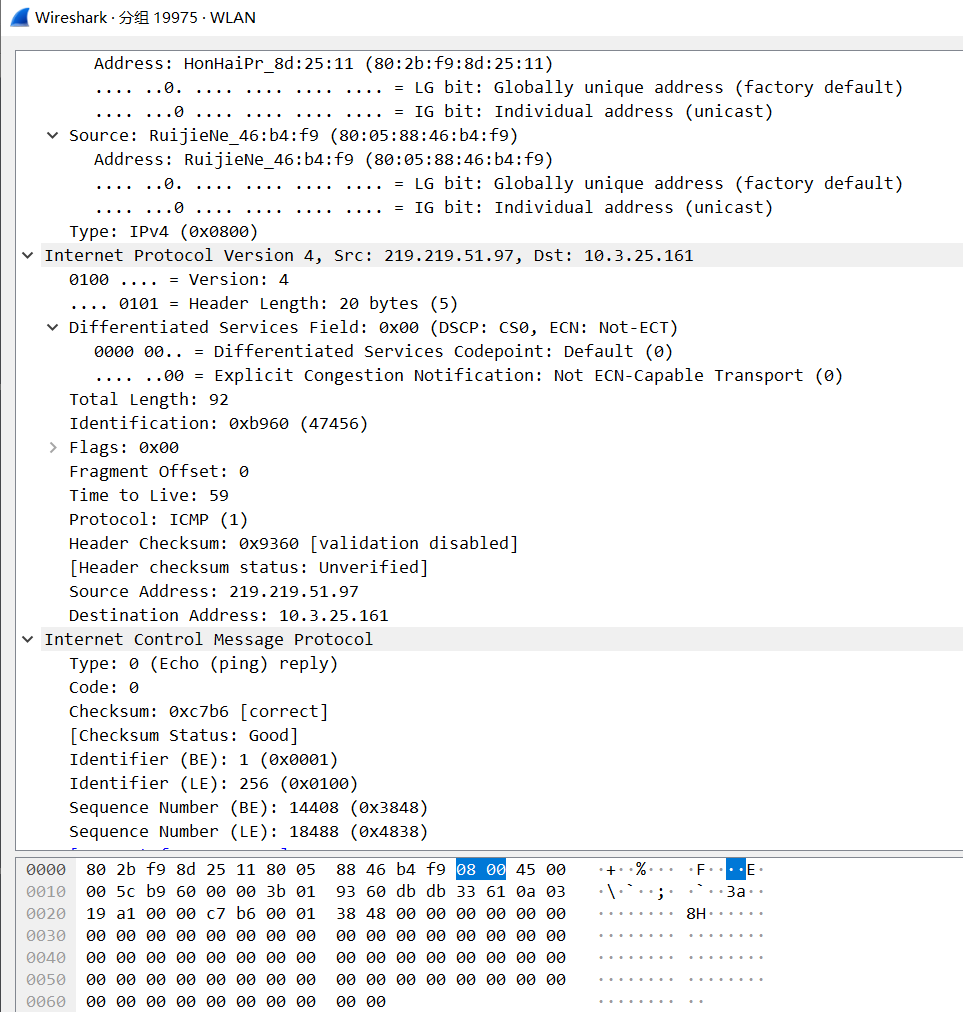
使用相同的方法，查看Echo (ping) reply包，得到type类型为0

通过查询ICMP报文类型可知，Type为0的包为回射应答（ping应答）

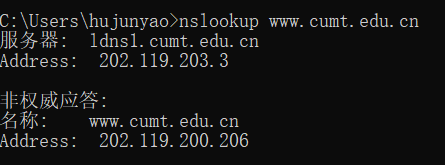
**tracert**

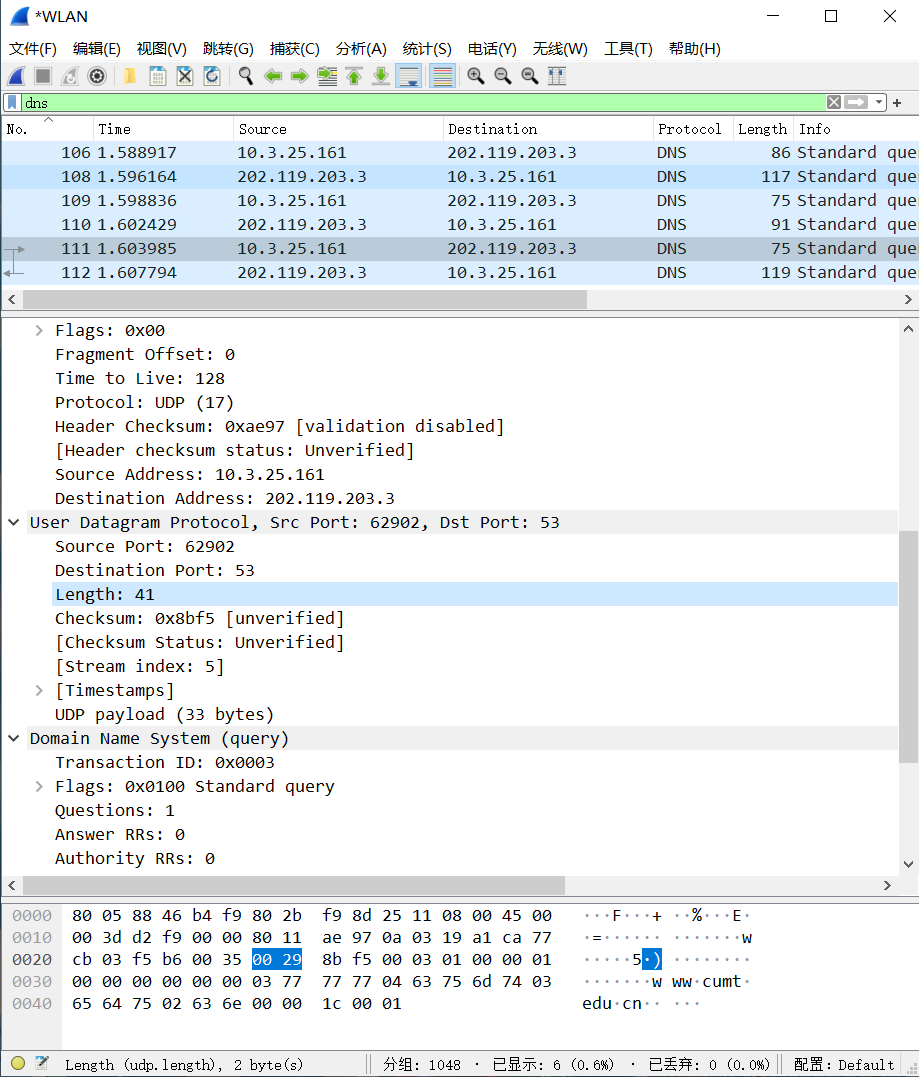






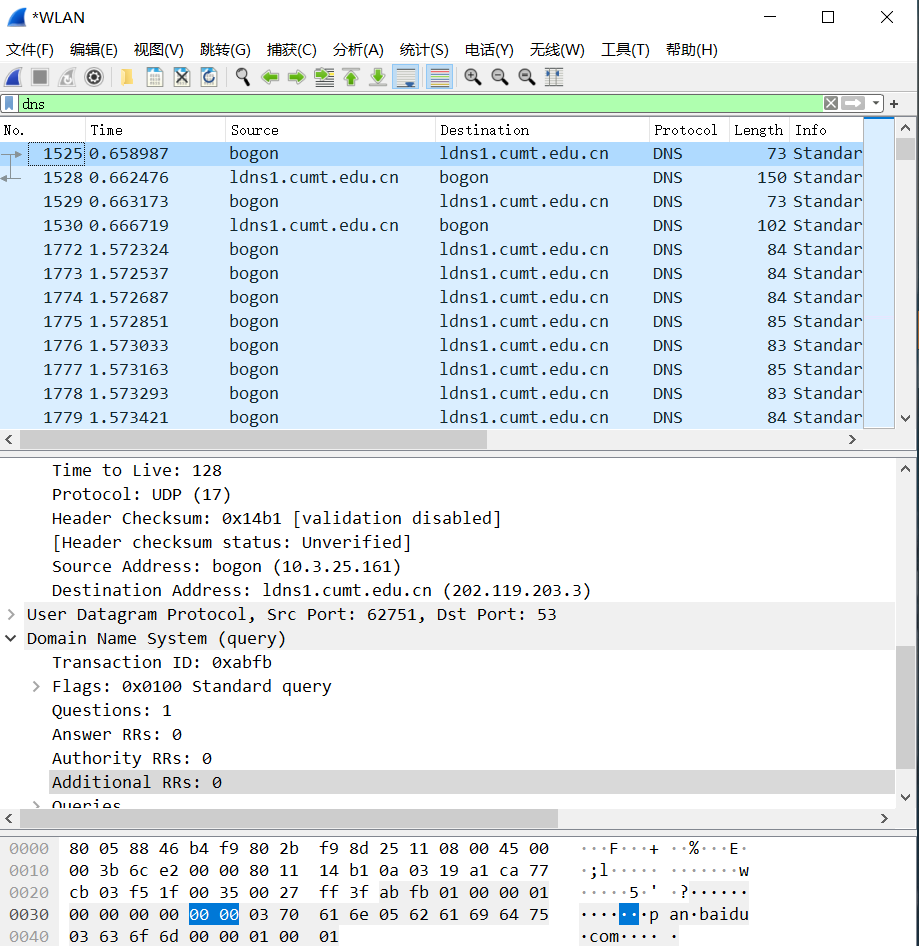
**nslookup**



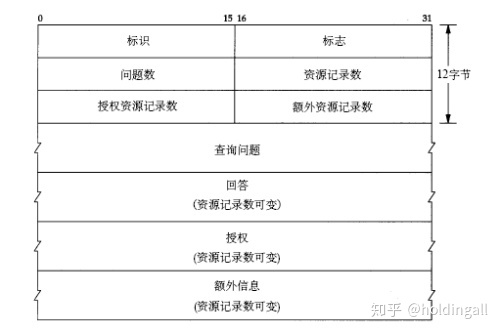


**4.针对不同互联网应用的执行过程进行抓包，对DNS服务、WWW服务、Email服务、QQ通信、微信、迅雷文件下载等六种不同网络应用服务访问情形下的数据包进行逐层分析，给出各层协议的主要参数及意义。**

**DNS服务**



DNS有两种报文：查询报文和回答报文。两者格式相同。



0000 80 2b f9 8d 25 11 80 05 88 46 b4 f9 08 00 **45 00** .+..%....F....E.

0010 **00 58 39 ce 00 00 3d 11 8a a8 ca 77 cb 03 0a 03 .X9...=....w....**

0020 **19 a1** 00 35 ff 02 00 44 82 45 **f8 54 81 80 00 01 ..**.5...D.E**.T....**

0030 **00 01 00 00 00 00 03 70 61 6e 05 62 61 69 64 75 .......pan.baidu**

0040 **03 63 6f 6d 00 00 1c 00 01 c0 0c 00 05 00 01 00 .com............**

0050 **00 02 96 00 11 05 79 69 79 75 6e 01 6e 06 73 68 ......yiyun.n.sh**

0060 **69 66 65 6e c0 16 ifen..**

**DNS服务：**应用层DNS（F8 54 … … c0 16）

f8 54 ---- Transaction ID: 由客户端指定的标识数据，DNS server会将这个字段原样返回，client端可以用来区分不同的 DNS 请求

81 80 ---- Flags:1000 0001 1000 0000 标志，16位

1 ---- Response:0 表示查询，1 表示响应，这里是响应报文

0000 – Opcode: 查询类型，0是普通查询

0 ---- Authoritative: 服务器不是权威认证域服务器（响应包用）

0 ---- Truncated: 报文没有被截断（收发包都用）

1 ---- Recursion desired: 需要递归（收发包都用）（客户端最好置 1，要不然 DNS 不执行递归查询，将有很多数据没能查到）

1 ---- Recursion available: 服务器有能力递归查询（响应包用）

0 ---- Z: 保留位0

0 ---- Answer authenticated: 数据没有被服务器鉴定过

0 ---- Non-authenticated data: 未鉴定数据不被允许

0000 - Reply code: 响应状态码，0为正确（此外还有1查询个数错误2服务器内部错误，3名字不存在等状态）

00 01 ---- Questions: 询问数为1

00 01 ---- Answer RRs: 响应数为1

00 00 ---- Authority RRs: 权威认证机构数目为0

00 00 ---- Additional RRs：附加信息数目为0

03 70 … … 00 01 --------------------------- Queries: 请求数据

03 70 61 6e 05 62 61 69 64 75 03 63 6f 6d 00

----------------- 资源域名 pan.baidu.com

00 1c ----------- 查询类型为AAAA（IPv6地址）（1c=>28）

00 01 ----------- Class: 0x0001代表IN

c0 0c … … c0 16 --------------------------- Answer: 响应数据正文

c0 0c ----------- Name: pan.baidu.com

00 05 ----------- 类型为CNAME（规范名）

00 01 ----------- Class: 0x0001代表IN

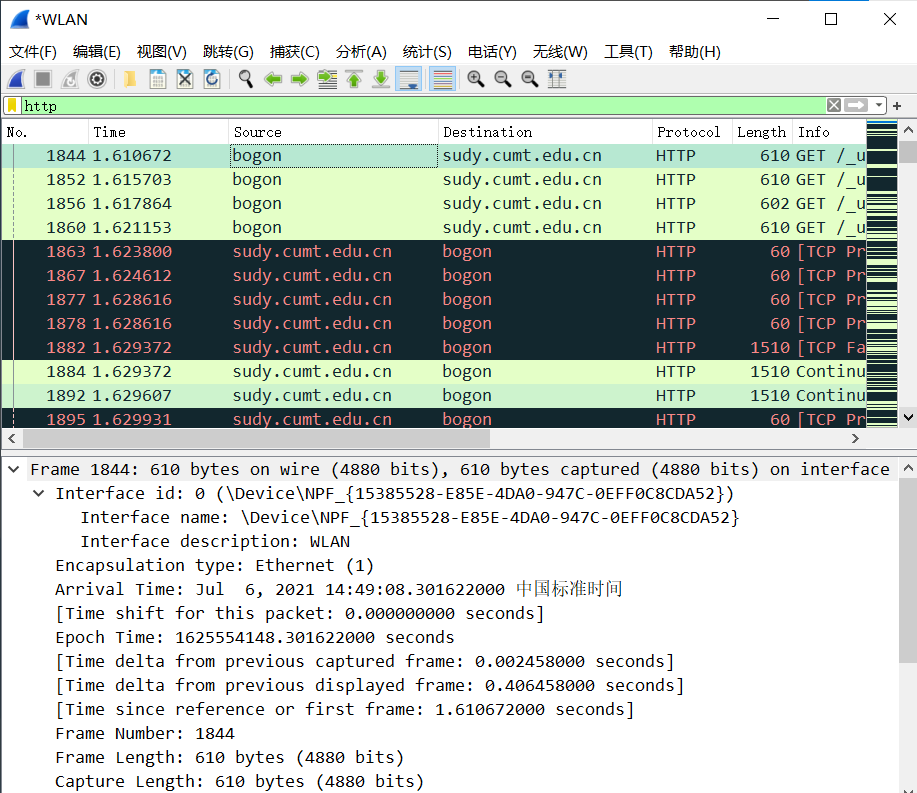
00 00 02 96 ----- TTL时间：662s

00 11 ----------- 数据长度为17

05 79 69 79 75 6e 01 6e 06 73 68 69 66 65 6e c0 16

----------------- CNAME(规范名): yiyun.n.shifen.com

**WWW服务**



HTTP报文有两种：请求报文（左侧），响应报文（右侧）**。**





0000 80 05 88 46 b4 f9 80 2b f9 8d 25 11 08 00 45 00 ...F...+..%...E.

0010 02 54 fa 85 40 00 80 06 47 34 0a 03 19 a1 ca 77 .T..@...G4.....w

0020 c8 ce c1 ed 00 50 e7 11 18 9d 5e 48 e3 7b 50 18 .....P....^H.{P.

0030 fa f0 ba 99 00 00 **47** **45 54 20 2f 5f 75 70 6c 6f** ......**GET /\_uplo**

0040 **61 64 2f 61 72 74 69 63 6c 65 2f 69 6d 61 67 65 ad/article/image**

0050 **73 2f 65 64 2f 63 31 2f 65 64 35 32 31 66 61 32 s/ed/c1/ed521fa2**

0060 **34 66 37 38 39 39 65 30 34 30 35 66 33 65 37 39 4f7899e0405f3e79**

0070 **63 61 32 35 2f 36 38 66 30 34 37 38 38 2d 63 61 ca25/68f04788-ca**

0080 **33 65 2d 34 65 31 36 2d 39 33 64 37 2d 34 64 33 3e-4e16-93d7-4d3**

0090 **61 61 33 30 64 32 36 32 39 2e 6a 70 67 20 48 54 aa30d2629.jpg HT**

00a0 **54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 TP/1.1..Host: ww**

00b0 **77 2e 63 75 6d 74 2e 65 64 75 2e 63 6e 0d 0a 43 w.cumt.edu.cn..C**

00c0 **6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d onnection: keep-**

00d0 **61 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e alive..User-Agen**

00e0 **74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozilla/5.0 (**

00f0 **57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;**

0100 **20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70 Win64; x64) App**

0110 **6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 leWebKit/537.36**

0120 **28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 (KHTML, like Gec**

0130 **6b 6f 29 20 43 68 72 6f 6d 65 2f 39 31 2e 30 2e ko) Chrome/91.0.**

0140 **34 34 37 32 2e 31 32 34 20 53 61 66 61 72 69 2f 4472.124 Safari/**

0150 **35 33 37 2e 33 36 20 45 64 67 2f 39 31 2e 30 2e 537.36 Edg/91.0.**

0160 **38 36 34 2e 36 34 0d 0a 41 63 63 65 70 74 3a 20 864.64..Accept:**

0170 **69 6d 61 67 65 2f 77 65 62 70 2c 69 6d 61 67 65 image/webp,image**

0180 **2f 61 70 6e 67 2c 69 6d 61 67 65 2f 73 76 67 2b /apng,image/svg+**

0190 **78 6d 6c 2c 69 6d 61 67 65 2f 2a 2c 2a 2f 2a 3b xml,image/\*,\*/\*;**

01a0 **71 3d 30 2e 38 0d 0a 52 65 66 65 72 65 72 3a 20 q=0.8..Referer:**

01b0 **68 74 74 70 3a 2f 2f 77 77 77 2e 63 75 6d 74 2e http://www.cumt.**

01c0 **65 64 75 2e 63 6e 2f 0d 0a 41 63 63 65 70 74 2d edu.cn/..Accept-**

01d0 **45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 Encoding: gzip,**

01e0 **64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d deflate..Accept-**

01f0 **4c 61 6e 67 75 61 67 65 3a 20 7a 68 2d 43 4e 2c Language: zh-CN,**

0200 **7a 68 3b 71 3d 30 2e 39 2c 65 6e 3b 71 3d 30 2e zh;q=0.9,en;q=0.**

0210 **38 2c 65 6e 2d 47 42 3b 71 3d 30 2e 37 2c 65 6e 8,en-GB;q=0.7,en**

0220 **2d 55 53 3b 71 3d 30 2e 36 0d 0a 43 6f 6f 6b 69 -US;q=0.6..Cooki**

0230 **65 3a 20 4a 53 45 53 53 49 4f 4e 49 44 3d 35 46 e: JSESSIONID=5F**

0240 **44 34 46 33 32 38 43 35 46 35 36 34 30 39 39 45 D4F328C5F564099E**

0250 **33 31 32 41 33 33 33 43 38 31 41 36 42 30 0d 0a 312A333C81A6B0..**

0260 **0d 0a ..**

**WWW服务：**应用层HTTP（47 45 … … 0d 0a）（即粗体部分）

第一部分：请求行

47 45 54 20------------------ 请求（前三位GET，20是空格）

2f 69 … … 70 67 20----------- 请求Request URI: /\_upload/article/images/ed/c1/

ed521fa24f7899e0405f3e79ca25/68f04788-ca3e-4e16-93d7-4d3aa30d2629.jpg

（最后一个20 是空格）

48 54 54 50 2f 31 2e 31 ----- 请求版本 HTTP/1.1

0d 0a ----------------------- 回车符与换行符

第二部分：请求头部

48 6f 73 74 3a 20 77 77 77 2e 63 75 6d 74 2e 65 64 75 2e 63 6e 0d 0a

---------------------- Host: www.cumt.edu.cn \r\n(回车换行)

43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a

---------------------- 连接：keep-alive \r\n(回车换行)

55 73 … … 36 34 0d 0a -------- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 Edg/91.0.864.64 \r\n(回车换行)

41 63 … … 2e 38 0d 0a--------- 接受：image/webp,image/apng,image/svg+xml,

image/\*,\*/\*;q=0.8 \r\n(回车换行)

52 65 … … 6e 2f 0d 0a -------- Referer: http://www.cumt.edu.cn/ \r\n

41 63 … … 74 65 0d 0a -------- 压缩算法可接收解码方式: gzip, deflate \r\n

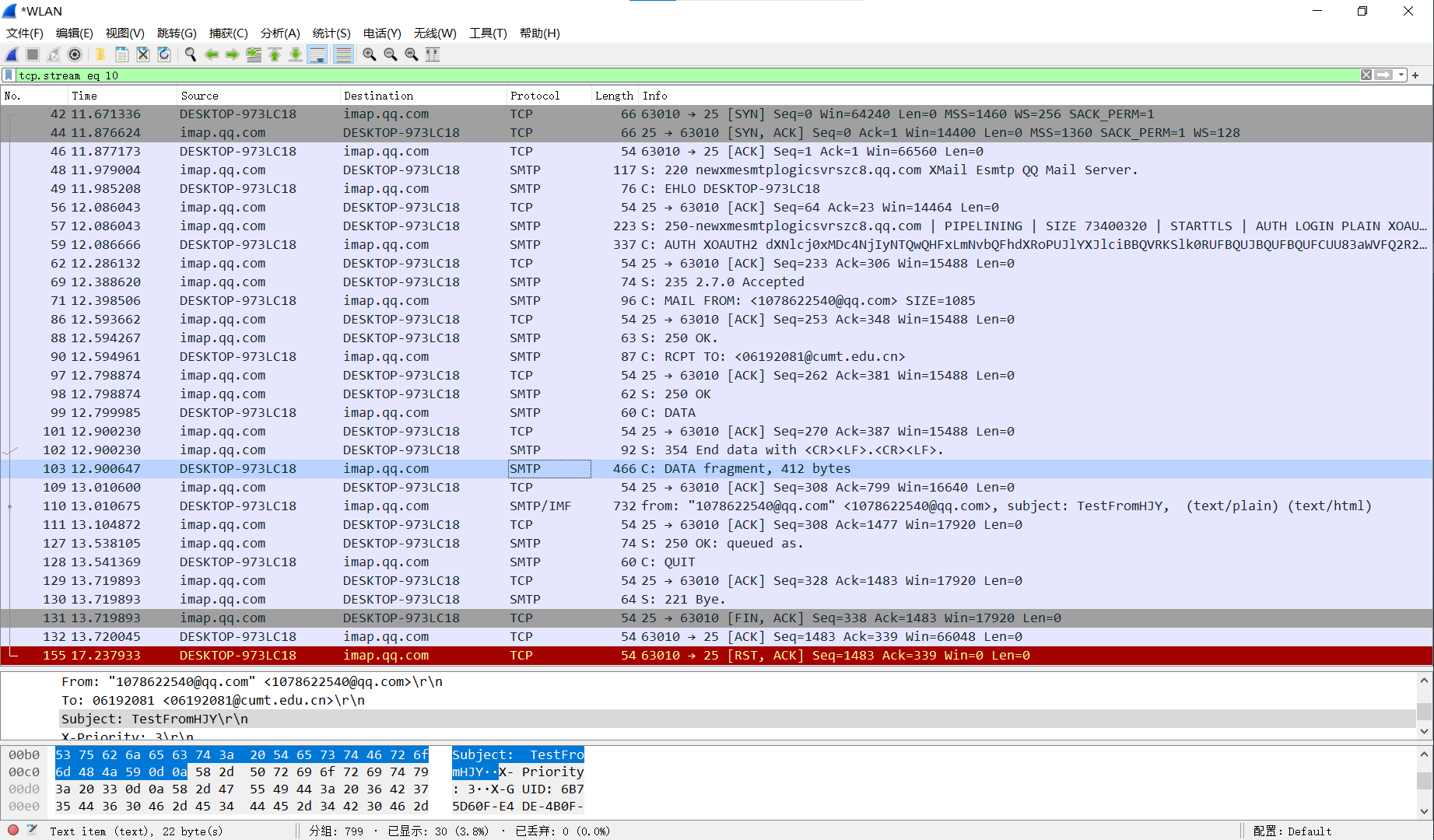
41 63 … … 2e 36 0d 0a -------- 可接收语言: zh-CN,zh;q=0.9,en;

q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n

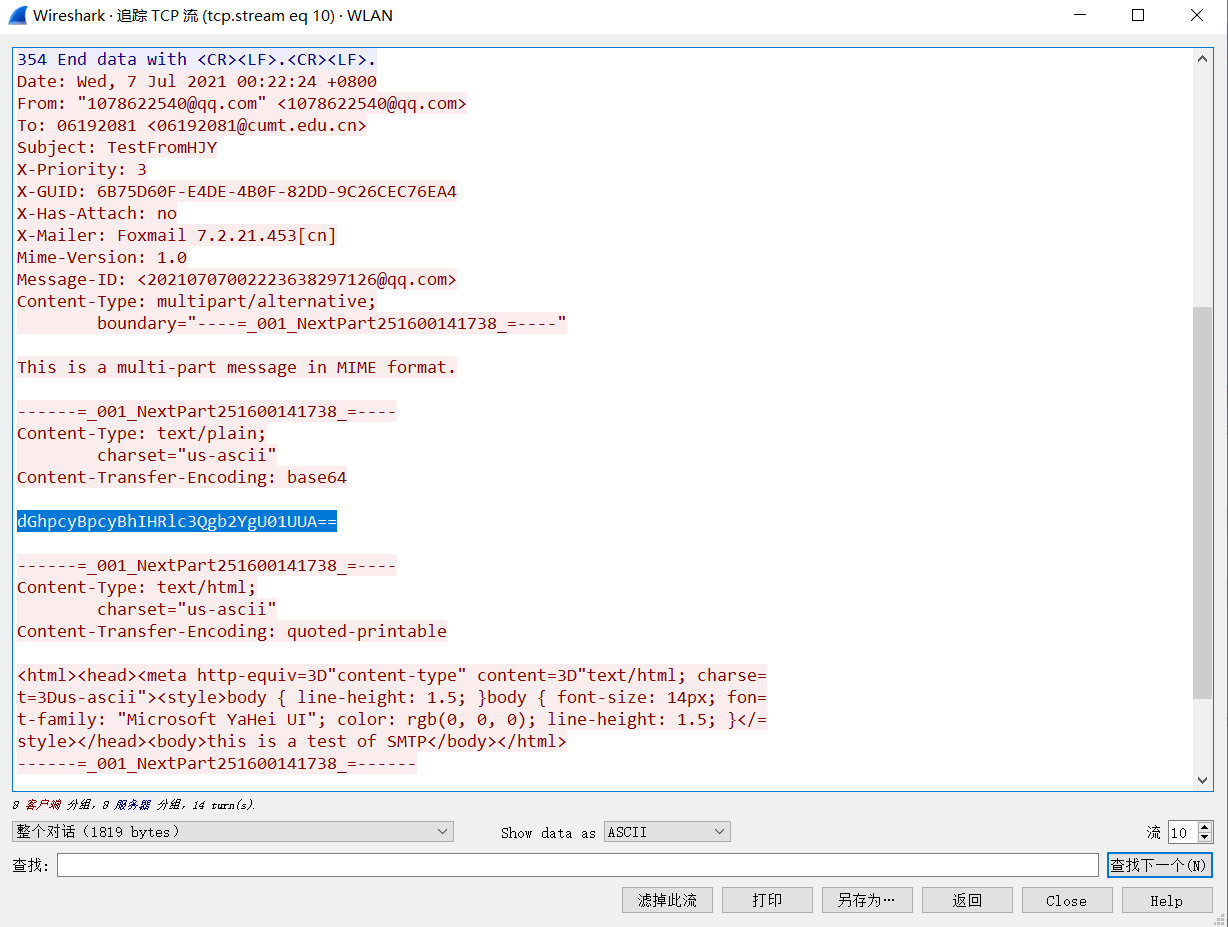
43 6f … … 42 30 0d 0a -------- Cookie: JSESSIONID=

5FD4F328C5F564099E312A333C81A6B0\r\n 当用户A浏览某个使用Cookie的网站时，该网站的服务器就为A产生一个唯一的识别码。

**Email服务**



追踪TCP流，看了一下发现SMTP接受密文，格式应该是目前非常简单的base64加密，所以尝试抓取内容后解密内容



0000 **80 2b f9 8d 25 11 84 76 37 c5 95 13 08 00** 45 68 .+..%..v7.....Eh

0010 00 30 c2 8c 40 00 32 06 01 63 b7 03 e1 2a c0 a8 .0..@.2..c...\*..

0020 2b 9a **00 19 f6 22 8c dd b3 b1 c6 cb e8 0e 50 18** +...."........P.

0030 **00 79 86 8a 00 00** 32 35 30 20 4f 4b 0d 0a .y....250 OK..

Email服务：应用层SMTP

(32 35 30 20 4f 4b 0d 0a)

32 35 30 ----- 响应码为250，表示接受邮件行为已经完成

20 ----------- 空格

4f 4b -------- 响应参数为OK

0d 0a -------- \r\n

Email服务：传输层TCP

(00 19 f6 22 8c dd b3 b1 c6 cb e8 0e 50 18 00 79 86 8a 00 00)

00 19 -------- 发出端口为25

f6 22 -------- 目标端口为63010

8c dd b3 b1 -- 序列号Sequence Number (raw): 2363339697

Sequence Number: 262 (relative sequence number)

c6 cb e8 0e -- 确认号Acknowledgment number (raw): 3335251982

Acknowledgment Number: 381(relative ack number)

50 18 -------- 01010000 00011000

0101 ----------- 首部长度为20

Flags: 0x018 (PSH, ACK) PSH与ACK为1

000. .... .... = 保留字Reserved未设置

...0 .... .... = 随机数Nonce未设置

.... 0... .... = 拥塞窗口减少Congestion Window Reduced未设置

.... .0.. .... = ECN-Echo: Not set

.... ..0. .... = Urgent: Not set

.... ...1 .... = 确认信号置1，Acknowledgment: Set

.... .... 1... = 通知接收方应尽快将报文段交付应用层Push: Set

.... .... .0.. = Reset: Not set

.... .... ..0. = Syn: Not set

.... .... ...0 = Fin: Not set

00 79 --------- 窗口大小为121

86 8a --------- 检验和0x868a

00 00 --------- 紧急指针为0

Email服务：网络层IP

(45 68 00 30 c2 8c 40 00 32 06 01 63 b7 03 e1 2a c0 a8 2b 9a)

45 -- 0100 0101 ------- 版本为4，首部长度为20字节（5）

68 -- 服务类型 Differentiated Services Field: 0x68 (DSCP: AF31, ECN: Not-ECT)

0110 10 --------- DSCP 差分服务代码点：保证转发31 (26)

00 -------------- ECN显式拥塞通知：不支持ECN的运输(0)

00 30 ----------------- 总长度为48

c2 8c ----------------- 识别码0xc28c（49804）

40 00 –- 0100前三位 –-- 未设置保留字，不分段，不设置更多的段，段偏移量为0

32 -------------------- TTL时间50

06 -------------------- 协议为TCP（6）

01 63 ----------------- 头部检验和为0x0163

b7 03 e1 2a ----------- 源地址为imap.qq.com(183.3.225.42)

c0 a5 2b 9a ----------- 目的为我自己的电脑(DESTOP-973LC18,192.168.43.154)

Email服务：链路层MAC（DIXEthernetV2标准）

(80 2b f9 8d 25 11 84 76 37 c5 95 13 08 00)

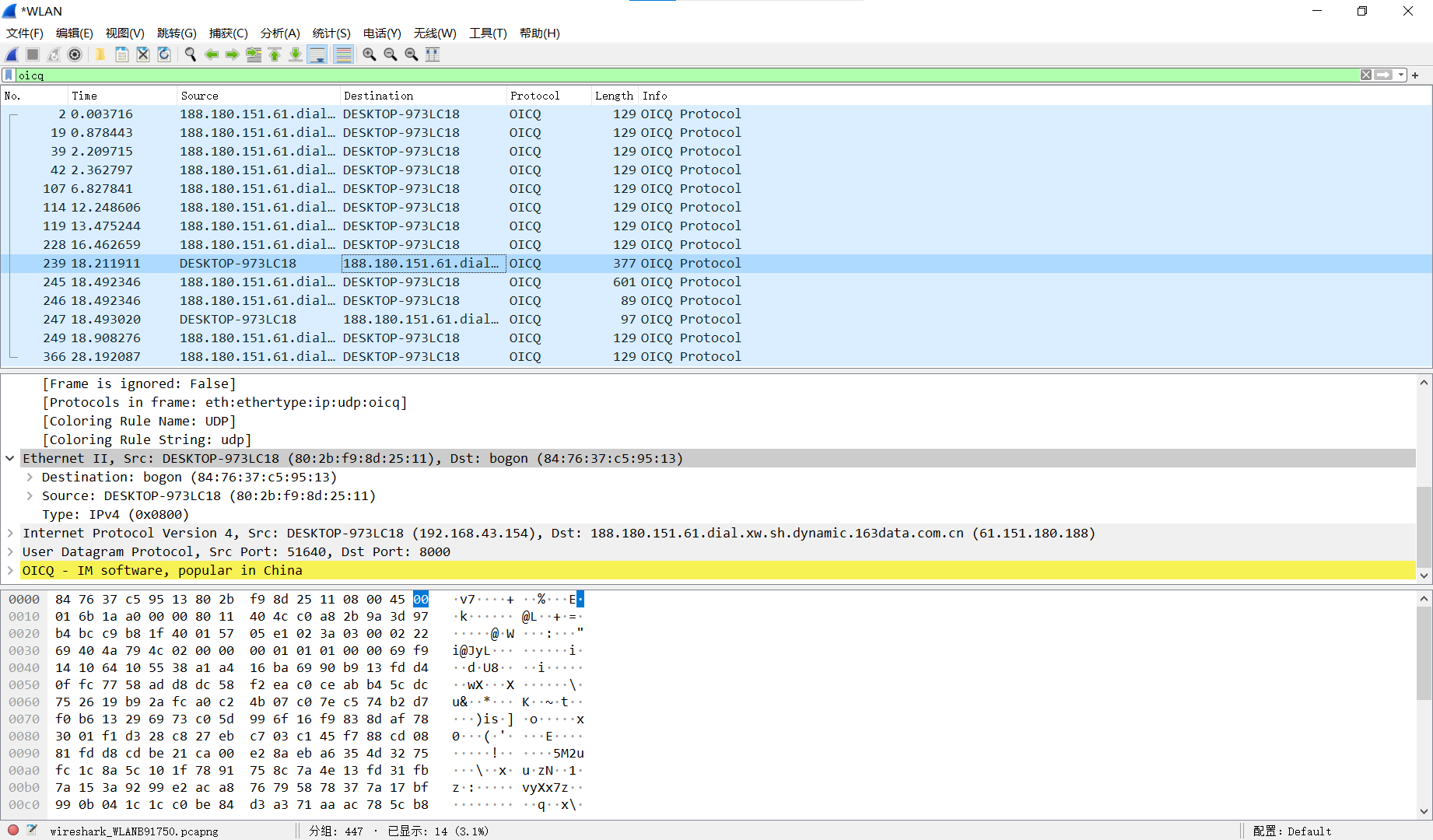
Ethernet II

80 2b f9 8d 25 11 –- Destination: DESKTOP-973LC18 (80:2b:f9:8d:25:11)

84 76 37 c5 95 13 –- 源地址Source: bogon (84:76:37:c5:95:13)

08 00 -------------- 类型Type: IPv4 (0x0800)

**QQ通信**

****

0000 80 2b f9 8d 25 11 84 76 37 c5 95 13 08 00 45 00 .+..%..v7.....E.

0010 00 4b 42 35 40 00 33 11 26 d7 3d 97 b4 bc c0 a8 .KB5@.3.&.=.....

0020 2b 9a **1f 40 c9 b8 00 37 79 cd** 02 3a 03 00 02 22 +..@...7y..:..."

0030 69 40 4a 79 4c 00 00 00 31 f1 92 c7 e8 10 dc a2 i@JyL...1.......

0040 01 3c eb bd 08 4a 7c 91 6b 4d c0 5f d3 7f 10 9f .<...J|.kM.\_....

0050 c8 b3 16 8a c5 47 04 7a 03 .....G.z.

QQ通信：应用层OICQ

02 -------------------- 标志02，是oicq packet

3a 03 ----------------- 版本是0x3a03

00 02 ----------------- 命令字是2，heart message

22 69 ----------------- 序列号是8809

40 4a 79 4c ------ Data (OICQ Number, if sender is client): 1078622540

00 00 00 … … 7a 03 ---- qq加密信息

QQ通信：传输层UDP

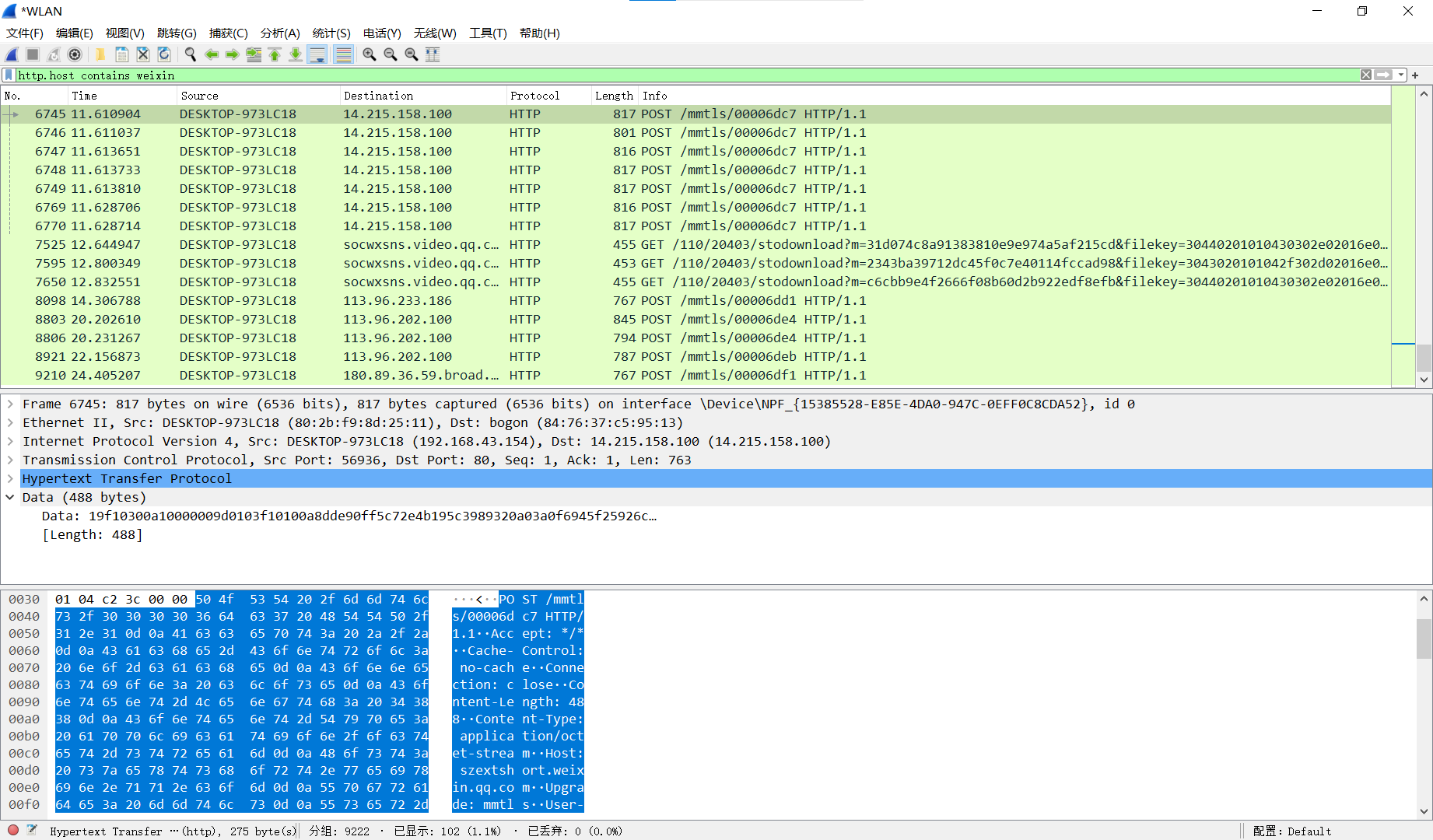
1f 40 ----------------- 源端口 8000

c9 b8 ----------------- 目的端口 51640

00 37 ----------------- 长度 55

79 cd ----------------- 检验和为0x793d

**微信**



0000 84 76 37 c5 95 13 80 2b f9 8d 25 11 08 00 45 00 .v7....+..%...E.

0010 03 23 31 1a 40 00 80 06 2d 3d c0 a8 2b 9a 0e d7 .#1.@...-=..+...

0020 9e 64 de 68 00 50 ae 0d a4 07 90 bc 16 c4 50 18 .d.h.P........P.

0030 01 04 c2 3c 00 00 **50 4f 53 54 20 2f 6d 6d 74 6c** ...<..POST /mmtl

0040 **73 2f 30 30 30 30 36 64 63 37 20 48 54 54 50 2f** s/00006dc7 HTTP/

0050 **31 2e 31 0d 0a** 41 63 63 65 70 74 3a 20 2a 2f 2a 1.1..Accept: \*/\*

0060 0d 0a **43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a** ..Cache-Control:

0070 **20 6e 6f 2d 63 61 63 68 65 0d 0a** 43 6f 6e 6e 65 no-cache..Conne

0080 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a **43 6f** ction: close..Co

0090 **6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 34 38** ntent-Length: 48

00a0 **38 0d 0a** 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 8..Content-Type:

00b0 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6f 63 74 application/oct

00c0 65 74 2d 73 74 72 65 61 6d 0d 0a **48 6f 73 74 3a** et-stream..Host:

00d0 **20 73 7a 65 78 74 73 68 6f 72 74 2e 77 65 69 78** szextshort.weix

00e0 **69 6e 2e 71 71 2e 63 6f 6d 0d 0a** 55 70 67 72 61 in.qq.com..Upgra

00f0 64 65 3a 20 6d 6d 74 6c 73 0d 0a **55 73 65 72 2d** de: mmtls..User-

0100 **41 67 65 6e 74 3a 20 4d 69 63 72 6f 4d 65 73 73** Agent: MicroMess

0110 **65 6e 67 65 72 20 43 6c 69 65 6e 74 0d 0a** 58 2d enger Client..X-

0120 4f 6e 6c 69 6e 65 2d 48 6f 73 74 3a 20 73 7a 65 Online-Host: sze

0130 78 74 73 68 6f 72 74 2e 77 65 69 78 69 6e 2e 71 xtshort.weixin.q

0140 71 2e 63 6f 6d 0d 0a **0d 0a** 19 f1 03 00 a1 00 00 q.com...........

… … …

0330 b8 .

微信：应用层HTTP

50 4f 53 54 20------------------ 请求（前四位POST，20是空格）

2f 6d … … 63 37 20----------- 请求Request URI: /mmtls/00006dc7（20 是空格）

48 54 54 50 2f 31 2e 31 ----- 请求版本 HTTP/1.1

0d 0a ----------------------- 回车符与换行符

41 63 63 65 70 74 3a 20 2a 2f 2a ---- Accept: \*/\*\r\n

43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a

---- Cache-Control: no-cache\r\n

43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a

---- Connection: close\r\n

43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 34 38 38 0d 0a

---- Content-Length: 488\r\n

43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 61 6d 0d 0a

----Content-Type: application/octet-stream\r\n

48 6f 73 74 3a 20 73 7a 65 78 74 73 68 6f 72 74 2e 77 65 69 78 69 6e 2e 71 71 2e 63 6f 6d 0d 0a

----Host: szextshort.weixin.qq.com\r\n

55 70 67 72 61 64 65 3a 20 6d 6d 74 6c 73 0d 0a

---- Upgrade: mmtls\r\n

55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 4d 65 73 73 65 6e 67 65 72 20 43 6c 69 65 6e 74 0d 0a

---- User-Agent: MicroMessenger Client\r\n

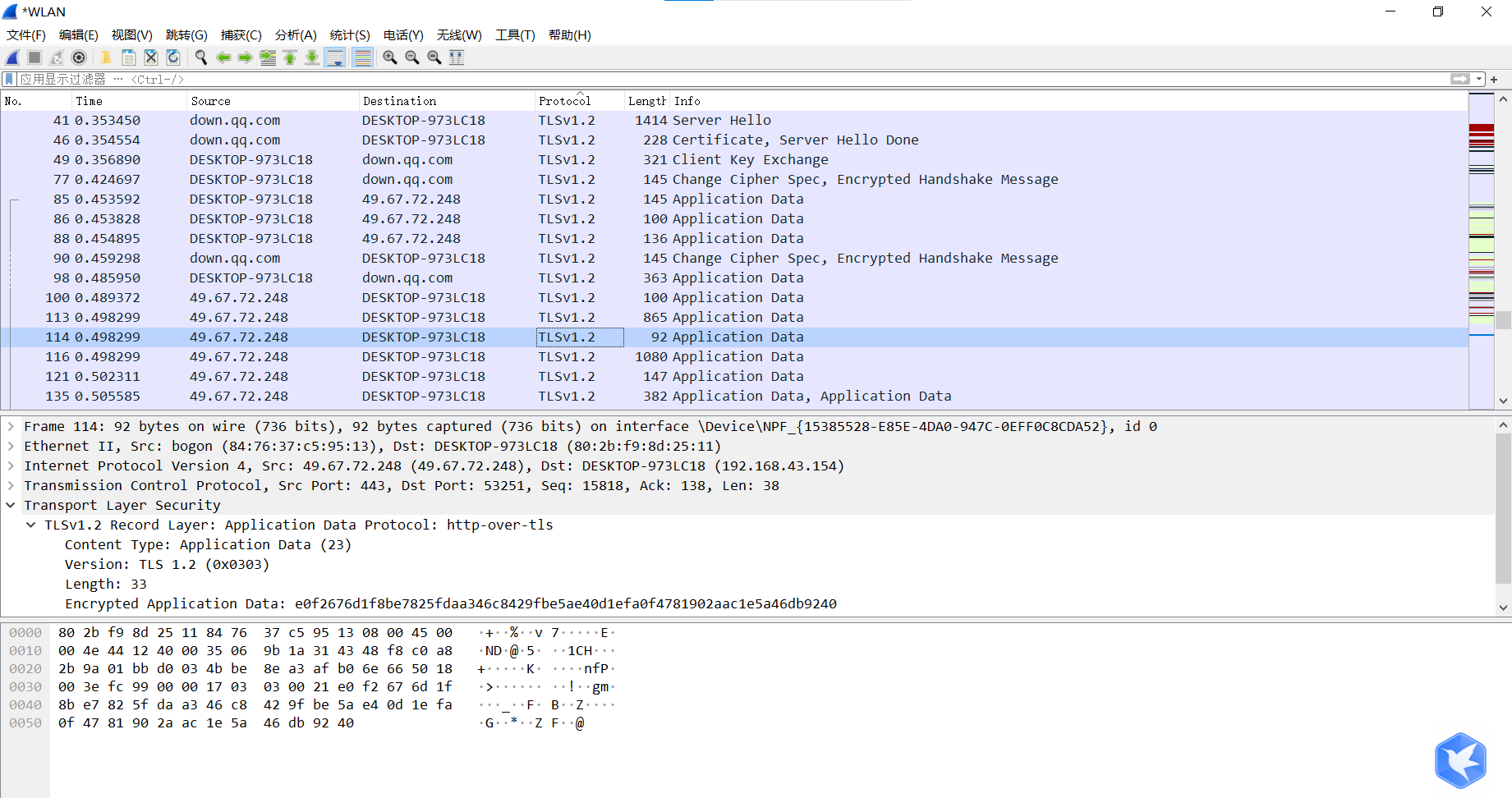
58 2d 4f 6e 6c 69 6e 65 2d 48 6f 73 74 3a 20 73 7a 65 78 74 73 68 6f 72 74 2e 77 65 69 78 69 6e 2e 71 71 2e 63 6f 6d 0d 0a

---- X-Online-Host: szextshort.weixin.qq.com\r\n

0d 0a ---------- /r/n

19 f1 03 00 a1 00 00 … … b8 ------- File Data: 488 bytes

**迅雷文件下载**



0000 80 2b f9 8d 25 11 84 76 37 c5 95 13 08 00 45 00 .+..%..v7.....E.

0010 00 4e 44 12 40 00 35 06 9b 1a 31 43 48 f8 c0 a8 .ND.@.5...1CH...

0020 2b 9a 01 bb d0 03 4b be 8e a3 af b0 6e 66 50 18 +.....K.....nfP.

0030 00 3e fc 99 00 00 17 03 03 00 21 e0 f2 67 6d 1f .>........!..gm.

0040 8b e7 82 5f da a3 46 c8 42 9f be 5a e4 0d 1e fa ...\_..F.B..Z....

0050 0f 47 81 90 2a ac 1e 5a 46 db 92 40 .G..\*..ZF..@

迅雷：应用层TLSv1.2

17 ------- 内容类型 Content Type: 应用数据Application Data (23)

03 03 ---- 版本Version: TLS 1.2 (0x0303)

00 21 ---- 长度Length: 33

e0 f2 67 6d 1f … … 46 db 92 40 --- 加密应用数据Encrypted Application Data:

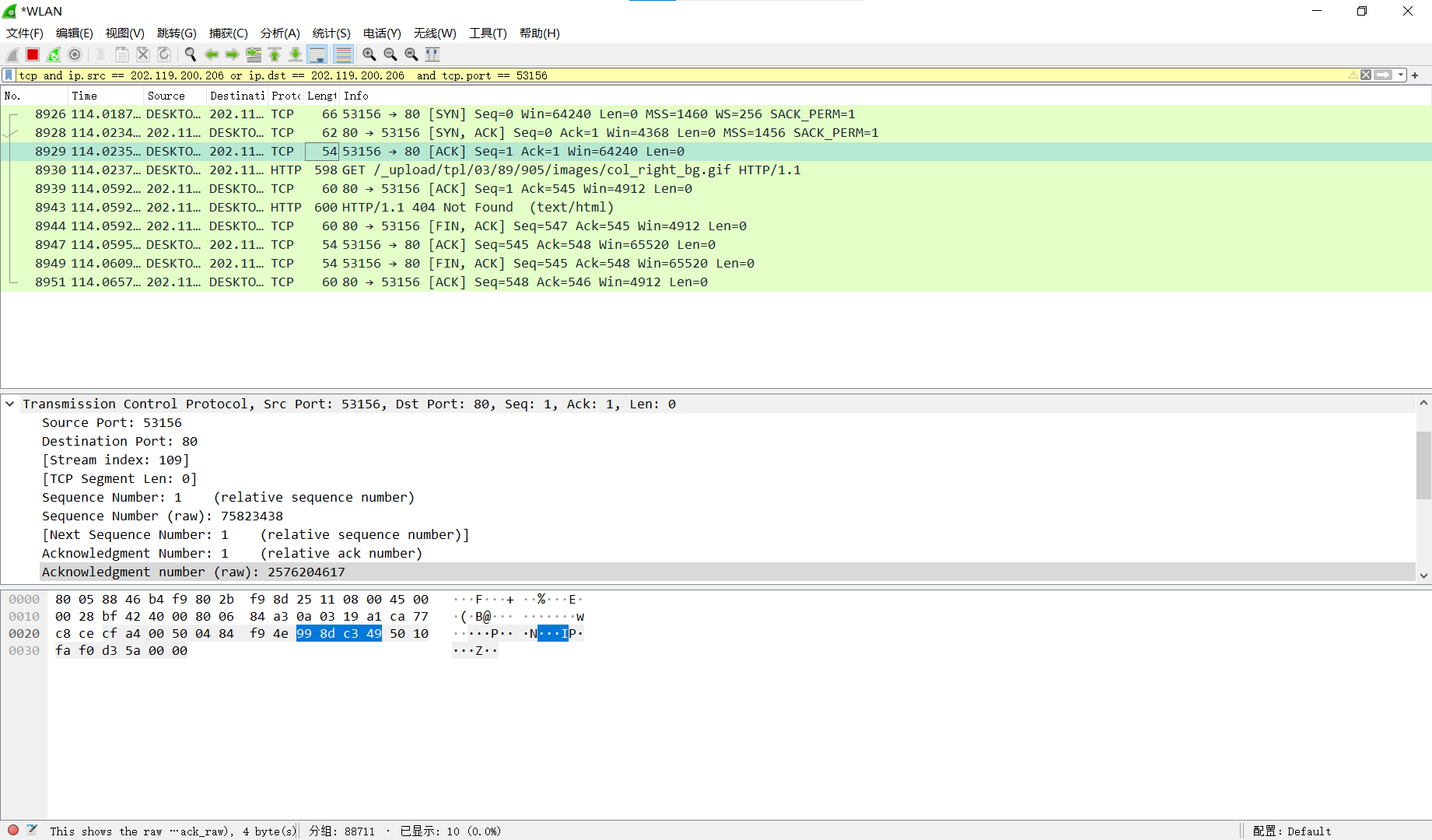
e0f2676d1f8be7825fdaa346c8429fbe5ae40d1efa0f4781902aac1e5a46db9240

**5.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。**

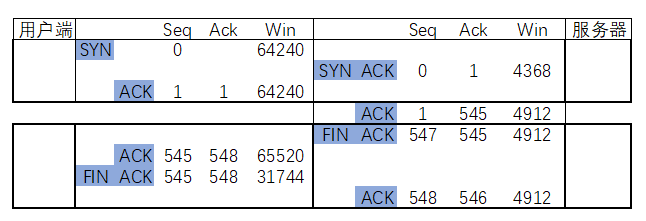
设置过滤条件为tcp and ip.src == 202.119.200.206 or ip.dst ==

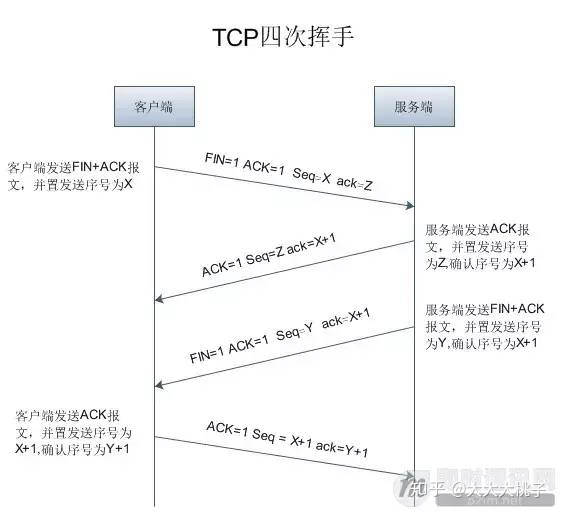
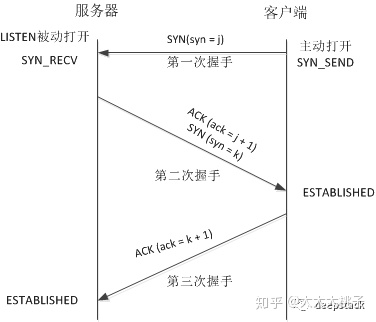
202.119.200.206 and tcp.port == 53156

抓包本机（DESKTOP-973LC18.local）与矿大教务部（202.119.200.206）之间的TCP传输，53156是本机端口，80是服务器端口。



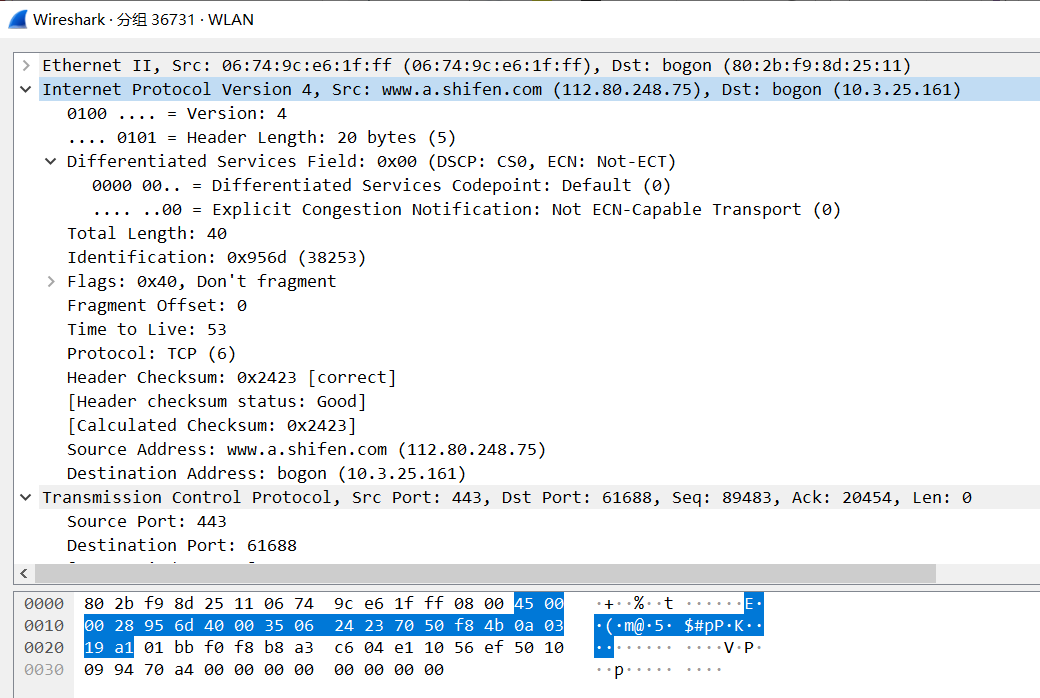
三次握手、四次挥手过程





**6.验证IP数据包、TCP报文段和UDP数据报的校验和。**

**IP数据包检验和正确**



4500 + 0028 IP首部，checksum置零

+ 956d + 4000

+ 3506 +[0000]

+ 7050 + f84b

+ 0a03 + 19a1

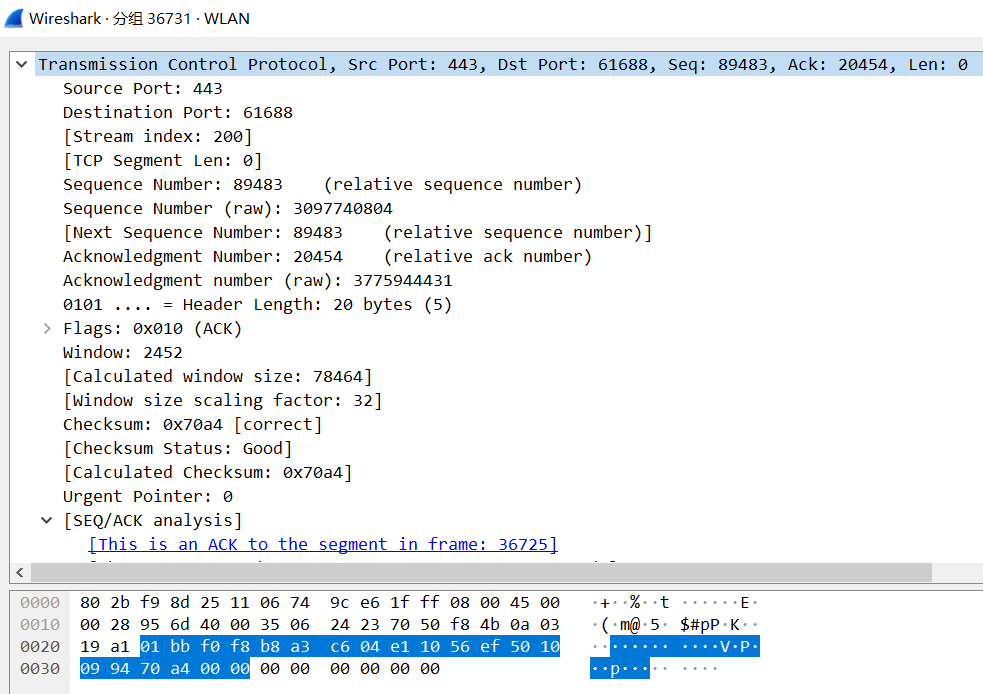
= 2dbda ------>

dbdc = 1101101111011100

-----> 0010010000100011 = 2423 = header checksum

验证成功

**TCP报文段检验和正确**



7050 + f84b 源地址

+ 0a03 + 19a1 目的地址

+ 0006 + 001a 前三行伪首部 保留0，协议字，TCP长度20字节

+ 01bb + f0f8 TCP首部，checksum置零

+ b8a3 + c604

+ e110 + 56ef

+ 5010 + 0994

+[0000]+ 0000

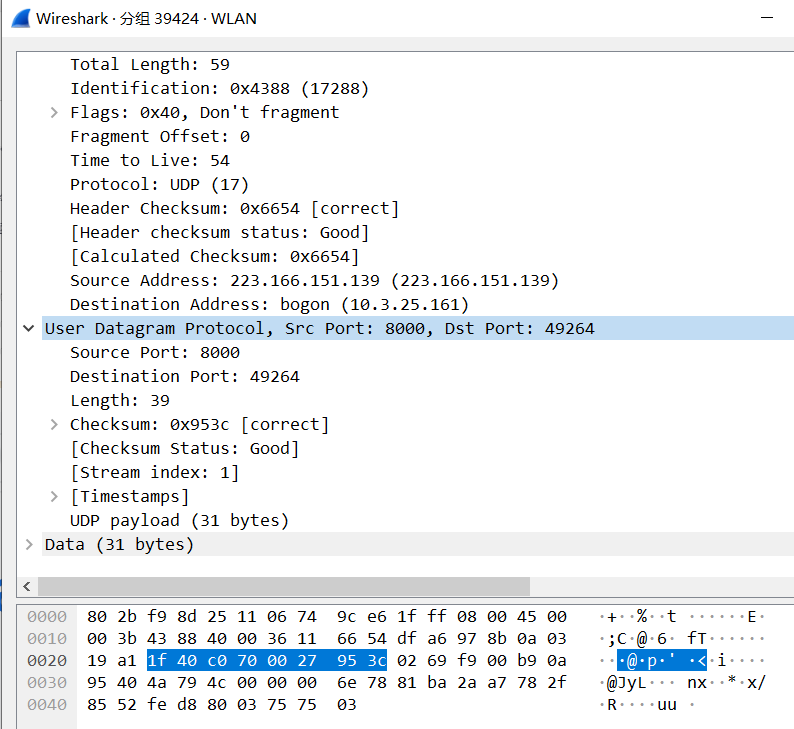
= 58f56 ------>

8f5b = 1000111101011011

-----> 0111000010100100 = 70a4

验证成功

**UDP数据报检验和正确**



dfa6 + 978b 下面三行伪首部，本行源地址

+ 0a03 + 19a1 目的地址

+ 0011 + 0027 保留0，11代表UDP协议（17），27是UDP长度为39

+ 1f40 + c070 下面两行UDP首部，checksum置零

+ 0027 +[0000]

+ 0269 + f900 + b90a + 9540 + 4a79 + 4c00 + 0000 + 6e78

+ 81ba + 2aa7 + 782f + 8552 + fed8 + 8003 + 7575 + 0300

= 96aba ------>

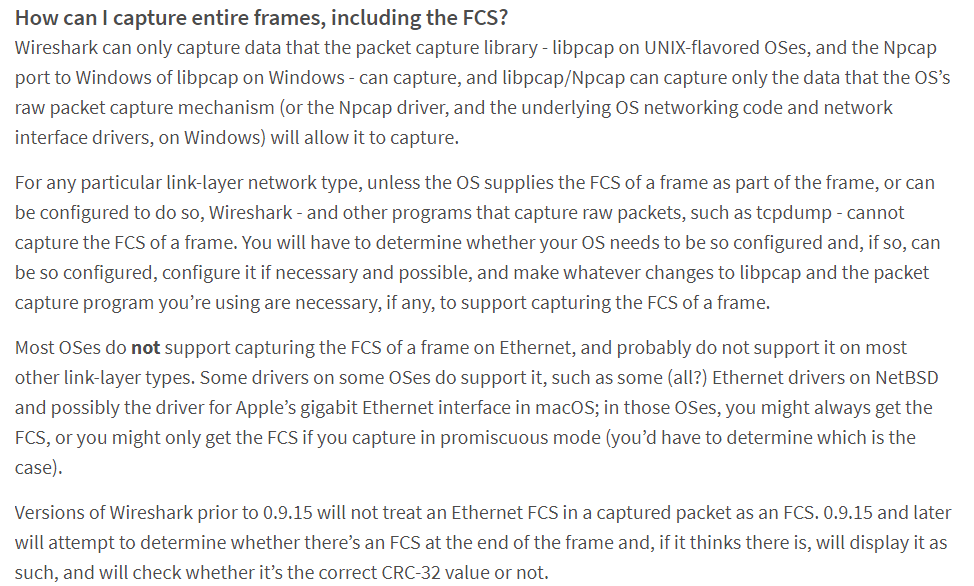
6ac3 = 0110101011000011

-----> 1001010100111100 = 953c

验证成功

**7.验证数据链路层的CRC冗余校验。**

但是物理网卡会去掉一头的前同步码8个字节，去掉一尾的CRC4个字节，暂无验证方法，下附官网解释：



**实验体会：**

通过本次实验，我对 Wireshark 软件的基本操作、过滤器填写、追踪流有了更深入的了解；对 IP、 UDP、TCP、HTTP 等协议的首部有了更好的掌握；对 TCP 协议连接建立、数据传送、连接释放过程有了直观的了解。

通过 Wireshark，结合网络上的资料，我对 TCP 协议的三次握手与四次挥手过程有了更直观的认识。在抓包过程中，我遇到了很多问题，例如包的真正到达时间不是严格和 seq 顺序一致，还和网络环境等复杂因素有关系，由此有课本上的“超时重传”、“确认丢失”、“确认迟到”等问题。

Wireshark 真的是一款非常强大的抓包工具，其功能是撷取网络封包，并尽可显示出最为详细的资料 Wireshark 使用 WinPCAP 作为接口，直与网卡进行数据报文交换。它的很多功能我在本次实验中还没有用到，在将来，我会更深入地去学习和了解这些网络分析用的工具软件，提高网络分析、网络安全的能力。