**北京邮电大学软件学院**

**2017－2018学年第一学期实验报告**

**课程名称： 计算机网络**

**项目名称： 数据链路层实验**

**项目完成人：**

**姓名：\_\_\_黄莹\_\_\_\_\_学号：\_2017211953\_\_\_\_\_\_\_**

**指导教师：\_\_\_\_\_王文东\_\_\_雷友珣 \_\_\_\_\_\_\_\_\_**

**日 期： 2019年 10月 27日**

1. **实验目的**

通过本实验使学生理解数据链路层协议数据单元（PDU）的定义和数据链路层功能。

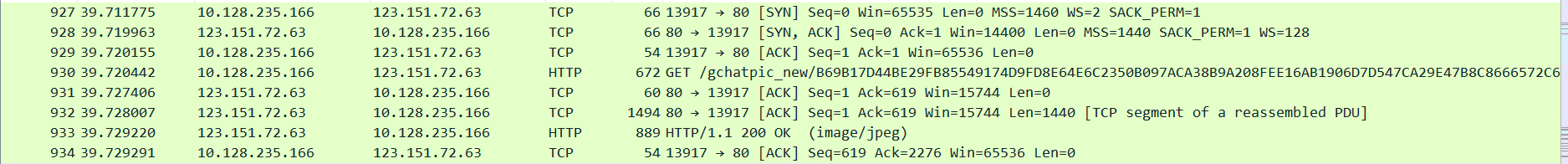
1. **实验内容**
2. 在可以访问互联网的主机上下载并安装网络抓包软件Wireshark。
3. 运行Wireshark软件，启动Wireshark软件的抓包功能抓取本主机访问互联网中某网站过程中发送和接收的数据包。
4. 对所抓取的数据包进行分析，分析所发送和接收的数据包的以太网帧结构中的源MAC地址、目的MAC地址和类型（type）字段的使用方法；理解各字段的含义和功能。
5. 选做部分：分析所抓取的数据包中的DNS（Domain Name System）消息、TCP报文、IP分组、HTTP协议消息的字段组成及作用。
6. **实验环境**
7. Windows系统主机或Linux系统主机；
8. Wireshark软件，软件下载网址：https://www.wireshark.org/
9. **实验过程及结果**
   1. 启动Wireshark程序。
   2. 点击Wireshark程序主窗口的“Capture ”菜单项，选中该下拉菜单中的“Options”菜单项，通过出现的“Capture Options”窗口中的“Interface”选择框设置需要抓取哪个网卡发送/接收的数据包。
   3. 可通过“Capture Options”窗口中的“Capture Filter”选择框设置需要抓取的数据包的类型，比如选择“IP only”。
   4. 点击“Capture Options”窗口中的“start”按钮，启动抓包工作。此时可看见Wireshark程序出现了一个新的窗口：“Capturing”窗口。
   5. 启动本计算机中的浏览器程序（IE浏览器或Firefox浏览器），在浏览器的地址栏中输入所要访问的网站的网址（例如北京邮电大学的网址<http://www.bupt.edu.cn>）后按回车键，可看到浏览器中出现该网站的主页。

打开网址<http://www.bupt.edu.cn>对传输的数据包分析



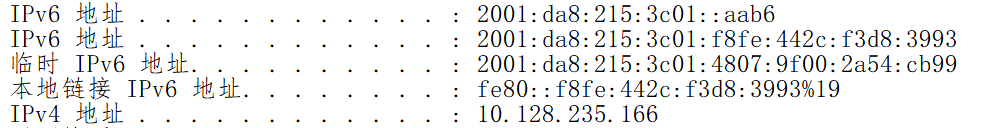
* 1. 在Wireshark程序的“Capturing”窗口中观察Wireshark程序抓取的数据包；该窗口中的每一条记录为本机发送或接收到的一个数据包；

观察从本机发往北邮官网网址的数据包，协议为TCP,HTTP等。



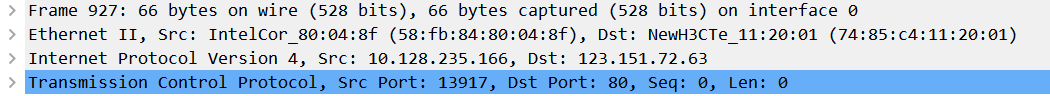
* 1. 用ipconfig命令查看本机ip地址与MAC地址

本机ip地址如下：



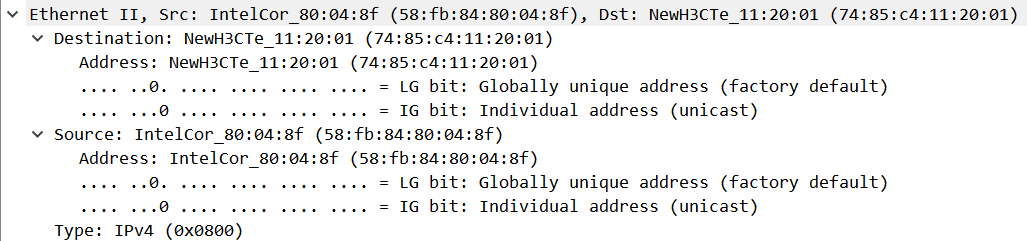
* 1. 鼠标双击“Capturing”窗口中的一条记录，出现展示该数据包详细信息的窗口。在该窗口下面部分的子窗口中有该数据包（数据链路层帧）的二进制数据表示；在该窗口上面部分的子窗口中有Wireshark程序对该帧的分析，详细列出了该帧的字段组成以及各字段的取值。观察该帧的“Destination”字段、“Source”字段、“Type”字段的取值，以及该帧携带的数据。在实验报告中分析数据链路层帧的字段组成和作用。

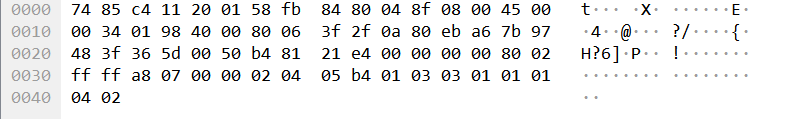
本机发送的数据包



**第一行：说明这是927号帧，线路66字节，实际捕获66字节。**

**第二行：包含了源MAC地址字段、目的MAC地址字段、类型字段的取值。**





数据链路层帧头的14Bytes由目的地址（6Byte)、源地址（6Byte）和类型（2Byte）组成，前六个Bytes（74:85:c4:11:20:01)为目的地址，后六个Bytes（58:fb:84:80:04:8f）为源地址，最后两个Bytes（0x0800）表示ipv4协议。（0806 ARP协议，08dd ipv6协议）。

**第三行：包含了互联网协议IPv4，具体分析见后面IP分组字段组成分析；**

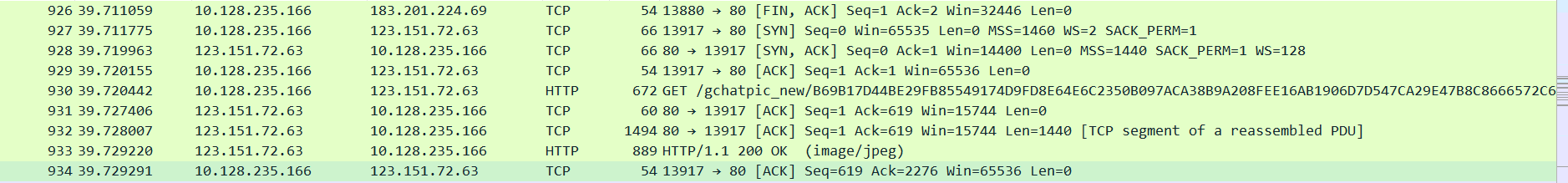
**第四行：包含了TCP文字报，具体分析见后面TCP报文字段组成分析。**

* 1. 观察“Capturing”窗口显示的所抓取的数据包，分析哪些数据包是发送出去的数据包，哪些数据包是接收到的数据包。

本机ip地址为10.128.235.166

927、929、930、934均为本机**发送**的数据包；

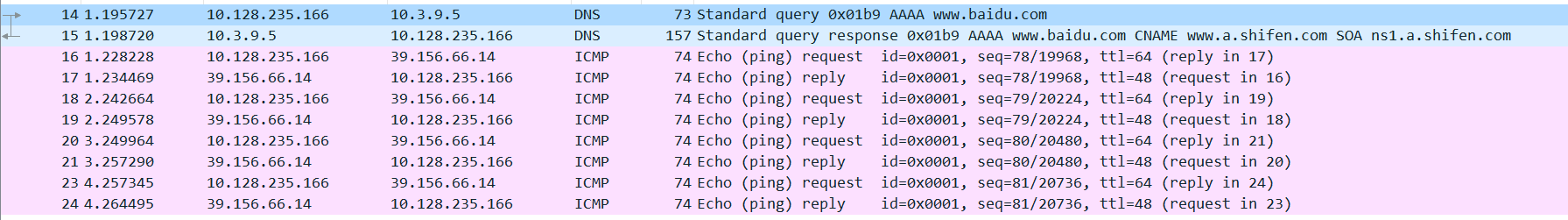
928、931、932、933均为本机**接收**的数据包；



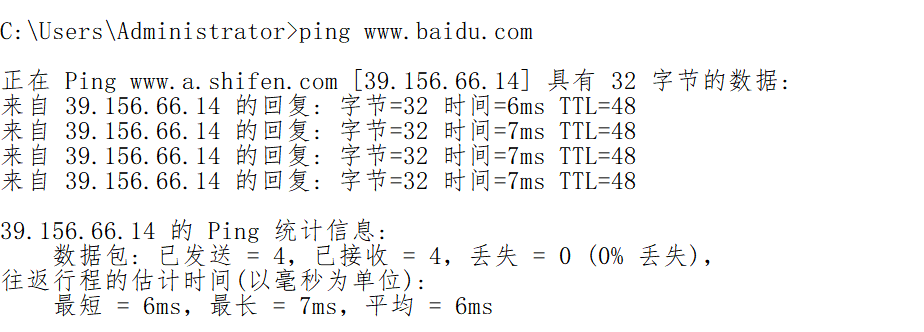
在抓取的数据中，source为123.151.72.63的为接收到的数据包，destination为123.151.72.63的为发送出去的数据包。

* 1. 分析访问互联网网站的协议过程，包括DNS域名解析过程、TCP连接建立过程、HTTP协议过程；分析DNS协议消息、IP协议消息、TCP协议消息、HTTP协议消息格式。

1. **DNS域名解析过程**



这是ping www.baidu.com抓取到的数据包



总体来看有两个DNS包(一次域名解析),和8个ICMP包(四次ping)

**DNS域名解析的过程可分为下面六个过程：**

1.先向本地dns缓存查看有没有该域名对应的ip地址，有直接跳出，没有接着往下

2.向根dns服务器询问域名对应的ip地址(根dns服务器会让他去查询顶级dns服务器)

3.向顶级dns服务器询问域名对应的ip地址(顶级dns服务器会让他去查询权威dns服务器)

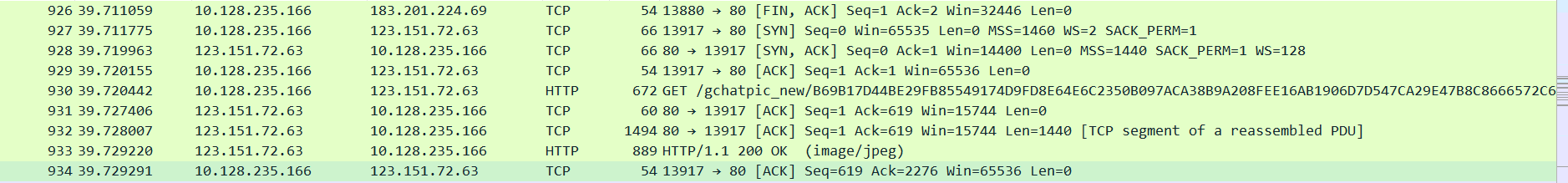
4.向权威dns服务器询问域名对应的ip地址(权威dns服务器会让他去查询二级dns服务器)

5.向二级dns服务器询问域名对应的ip地址(二级dns服务器会返回对应的ip地址)

6.接收到ip地址后，会先把ip和域名对应关系保存到本地dns缓存，以便下次方便访问

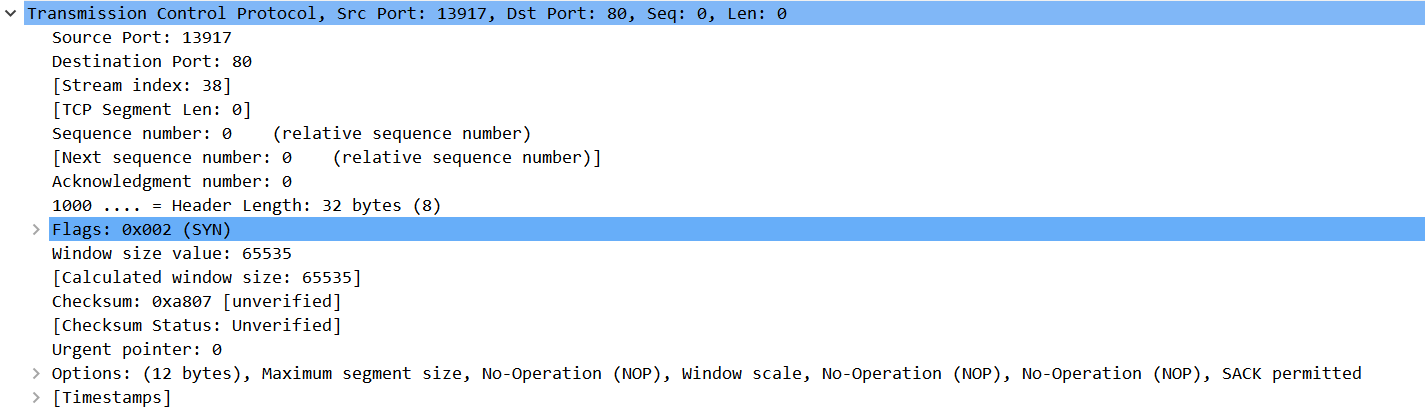
1. **TCP建立连接过程（三次握手）**

如图红框部分为TCP建立连接的过程。

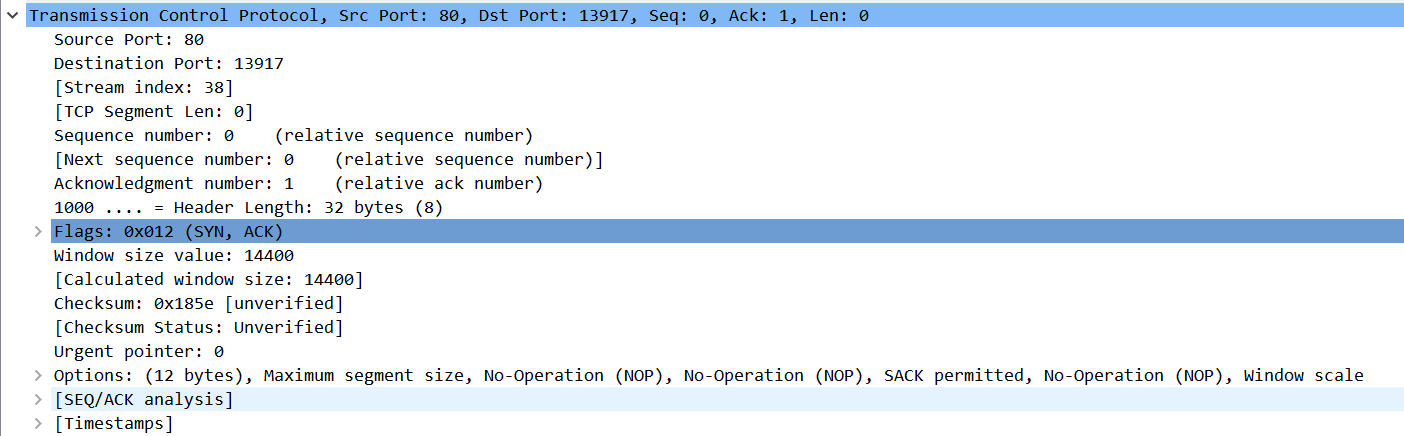


HTTP开始之前先**三次握手**：

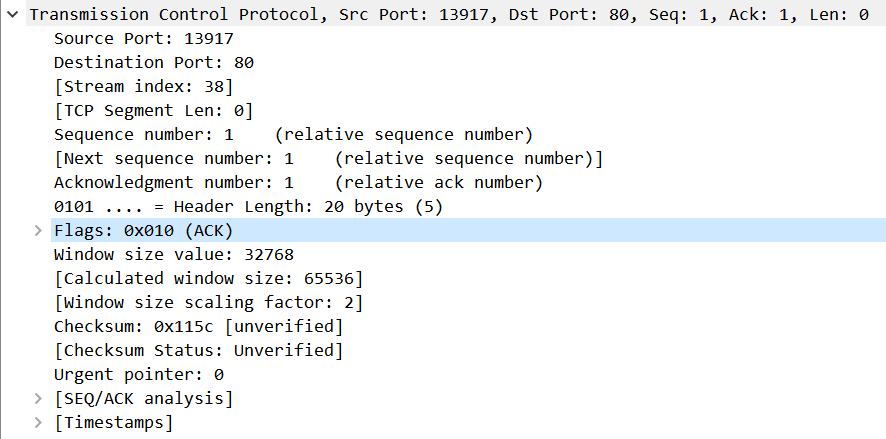
**第一阶段**就是客户向服务器发送同步请求(第927行)，Seq=0，标志位SYN；



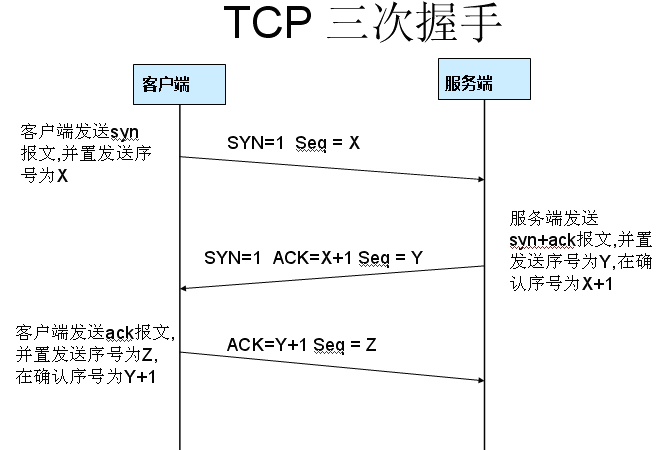
**第二阶段**就是服务器向客户回复一个ACK包（第928行），ACK=X+1，X=0，所以ACK=1，seq=Y=0；标志位为SYN，ACK;



**第三阶段**是客户向服务器发送ACK（第929行），其中Seq=1，ACK=1，标志位为ACK。



至此，TCP的三次握手结束。

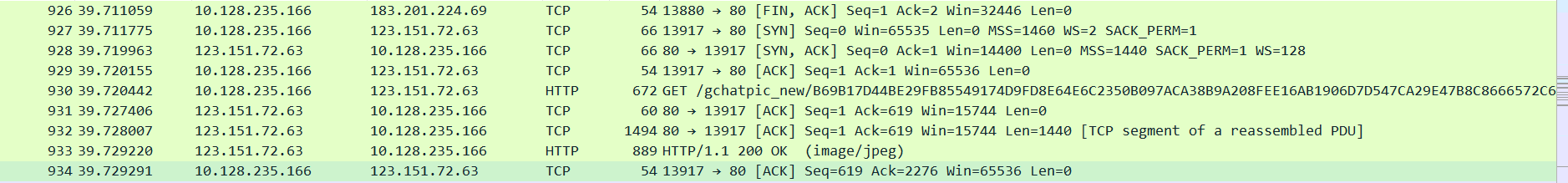


**SYN报文**：图中显示从客户端发送至服务器端的SYN报文，此报文用于与服务器建立同步，确保客户端和服务器端的通信按次序传输。SYN报文的头部有一个32 bit序列号。底端对话框显示了报文一些有用信息如报文类型，序列号。

**SYN/ACK报文**：服务器的响应。一旦服务器接收到客户端的SYN报文，就读取报文的序列号并且使用此编号作为响应，也就是说它告知客户机，服务器接收到了SYN报文，通过对原SYN报文序列号加一并且作为响应编号来实现，之后客户端就知道服务器能够接收通信。

**ACK报文**：客户端对服务器发送的确认报文，告诉服务器客户端接收到了SYN/ACK报文，并且与前一步一样客户端也将序列号加一，此包发送完毕，客户端和服务器进入ESTABLISHED状态，完成三次握手。

1. **HTTP协议过程:**



TCP三次握手建立连接（927-929行）；

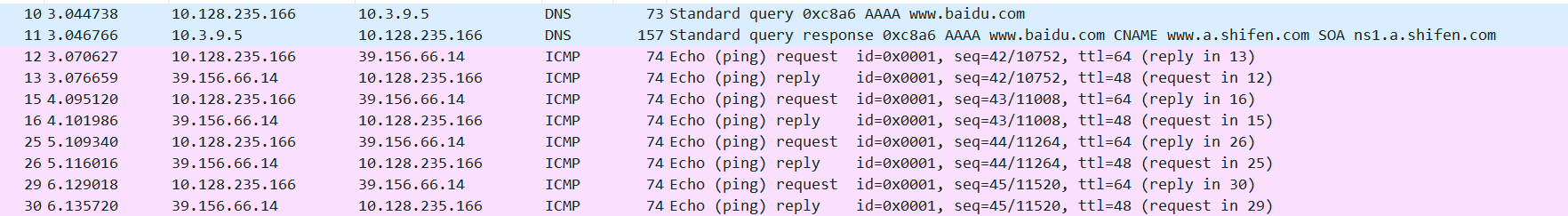
TCP三次握手结束之后就是HTTP请求(第930行)；

客户发出HTTP请求之后，服务器收到请求发送ACK（第931行）；

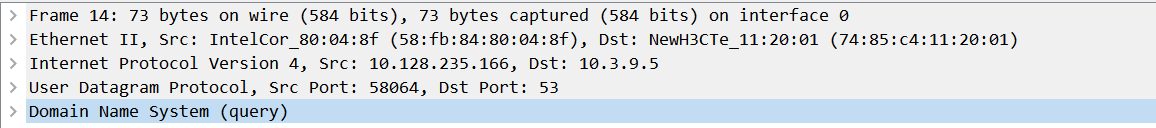
服务器发送报文（第933行）；

客户收到保文后发送应答报文（第934行）

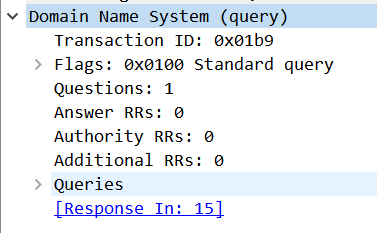
1. **DNS协议消息分析**



**打开第一个DNS，如下图所示：**

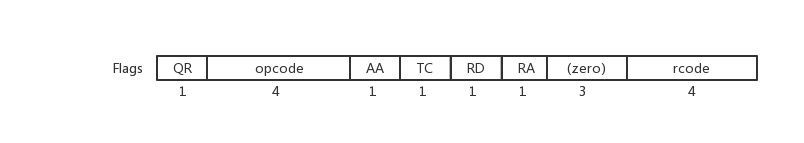


DNS为应用层，下层传输层采用UDP，再下层网络层为IPv4，然后是数据链路层以太网帧，需要关注的应用层实现也是DNS本身，UDP中目的端口为53，Ip协议中目的地址为10.3.9.5，**第一个包是请求包。**



第二行：会话标识（2字节）0x01b9，是DNS报文的ID标识，对于请求报文和其对应的应答报文，这个字段是相同的，通过它可以区分DNS应答报文是哪个请求的响应。

第三行：标志（2字节），含义如下：



QR（1bit）：查询/响应标志，0为查询，1为响应

opcode（4bit）：0表示标准查询，1表示反向查询，2表示服务器状态请求

AA（1bit）：表示授权回答

TC（1bit）：表示可截断的

RD（1bit）：表示期望递归

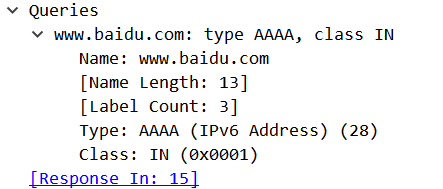
RA（1bit）：表示可用递归

rcode（4bit）：表示返回码，0表示没有差错，3表示名字差错，2表示服务器错误（Server Failure）

也就是说，当前是一个请求标志，标准查询，不授权回答，不可截断，期望递归，不可用递归，没有差错。

第四行、第五行、第六行、第七行：数量字段（总共8字节）：Questions、Answer RRs、Authority RRs、Additional RRs 各自表示后面的四个区域的数目。Questions表示查询问题区域节的数量，Answers表示回答区域的数量，Authoritative namesversers表示授权区域的数量，Additional recoreds表示附加区域的数量。

**查询区正文：**



第三行：查询名www.baidu.com，长度不固定，且不使用填充字节，一般该字段表示的就是需要查询的域名（如果是反向查询，则为IP，反向查询即由IP地址反查域名）

第四行：查询名长度

第六行：查询类型，各类型如下，图中为域名获得的IPv6地址。

1 A 由域名获得IPv4地址

2 NS 查询域名服务器

5 CNAME 查询规范名称

6 SOA 开始授权

11 WKS 熟知服务

12 PTR 把IP地址转换成域名

13 HINFO 主机信息

15 MX 邮件交换

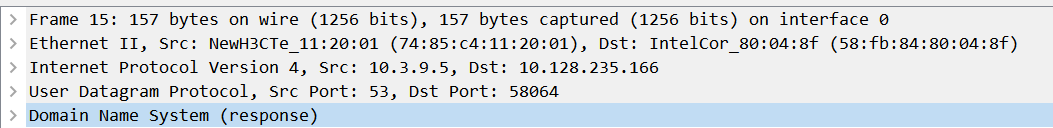
28 AAAA 由域名获得IPv6地址

252 AXFR 传送整个区的请求

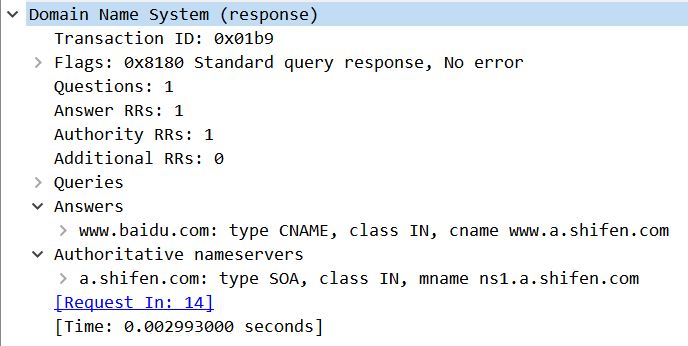
255 ANY 对所有记录的请求

第七行：查询类，通常为1，表明是Internet数据

**打开第二个DNS包，该包为响应包**



UDP中目的端口为58064，Ip协议中目的地址为10.128.235.166。



第二行：会话标识（2字节）0x01b9，DNS报文的ID标识，与它的请求包相同。

第三行：标志，含义是：响应，标准查询，非授权回答，不可截断，期望递归，可用递归，没有差错。

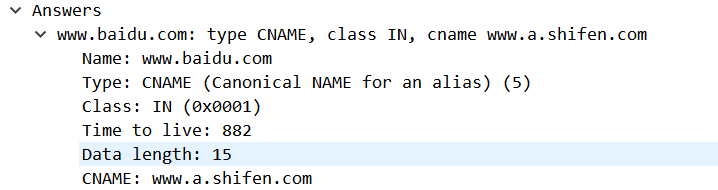
第四行、第五行、第六行、第七行：查询问题区域节的数量为1，回答区域的数量为1，授权区域的数量为1，附加区域的数量为0。

第八行：查询区域，已经分析过。

第九行：回答区域；

第十行：授权区域。

**回答区域正文：**



第二行：域名（2字节或不定长）：它的格式和Queries区域的查询名字字段是一样的。有一点不同就是，当报文中域名重复出现的时候，该字段使用2个字节的偏移指针来表示。比如，在资源记录中，域名通常是查询问题部分的域名的重复，因此用2字节的指针来表示，具体格式是最前面的两个高位是 11，用于识别指针。其余的14位从DNS报文的开始处计数（从0开始），指出该报文中的相应字节数。

第三行：查询类型，表示资源记录的类型，CNAME为查询规范名称。

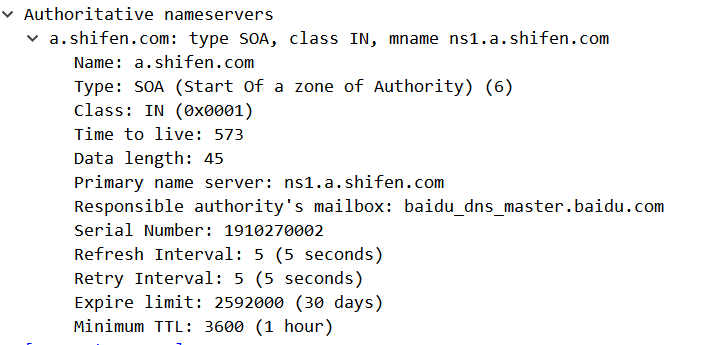
第四行：查询类：对于Internet信息，总是IN

第五行：生存时间（TTL）：以秒为单位，表示的是资源记录的生命周期，一般用于当地址解析程序取出资源记录后决定保存及使用缓存数据的时间，它同时也可以表明该资源记录的稳定程度，极为稳定的信息会被分配一个很大的值（比如86400，这是一天的秒数）。

第六行：资源数据长度

第七行：资源数据：该字段是一个可变长字段，表示按照查询段的要求返回的相关资源记录的数据。可以是Address（表明查询报文想要的回应是一个IP地址）或者CNAME（表明查询报文想要的回应是一个规范主机名）等。

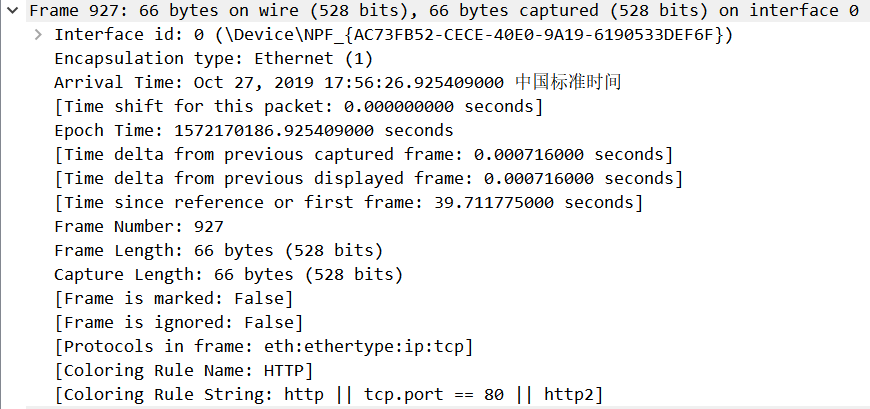
**授权区域正文同回答区域正文格式几乎相同。**



第8-14行：均为资源数据。

1. **TCP协议消息分析**

**1.帧：**



第一行：927号帧，线路66字节，实际捕获66字节；

第二行：接口id为0

第三行：封装类型

第四行：捕获日期和时间：Arrival Time: Oct 27, 2019 17:56:26.925409000 中国标准时间

第六行：信息出现时间：Epoch Time: 1572170186.925409000 seconds

第七行：[Time delta from previous captured frame: 0.141705000 seconds]与前一捕获数据帧时间隔

第八行：[Time delta from previous displayed frame: 0.141705000 seconds]与前一显示帧的时间隔

第九行：[Time since reference or first frame: 28.052351000 seconds]此包与第一帧的时间间隔

第十行：Frame Number: 927 帧的编号

第十一行：Frame Length: 66 bytes (528 bits) 帧的长度

第十二行：Capture Length: 66 bytes (528 bits) 被捕获的帧的长度

第十三行：[Frame is marked: False] 帧被标记：无

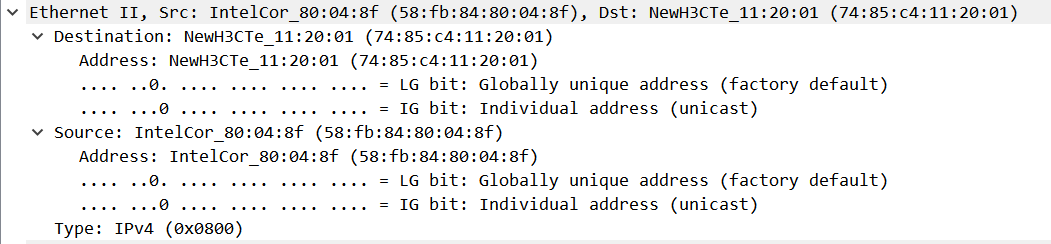
第十四行：[Frame is ignored: False] 帧被忽略：无

第十五行：[Protocols in frame: eth:ethertype:ip:tcp] 帧中的协议以太网、ip、tcp

第十六行：[Coloring Rule Name: HTTP] 色彩规则名称

第十七行：[Coloring Rule String: http || tcp.port == 80 || http2] 色彩规则字符串

**2.Ethernet 协议分析：**

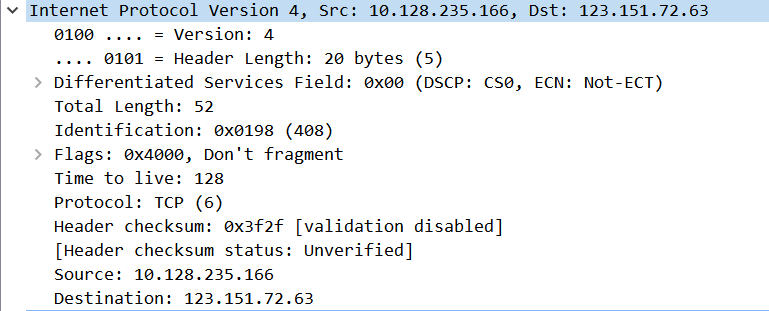


Destination: NewH3CTe\_11:20:01 (74:85:c4:11:20:01)目的mac地址

Source: IntelCor\_80:04:8f (58:fb:84:80:04:8f)源mac地址

Type: IPv4 (0x0800) 类型是ipv4数据包

**3.ipv4协议信息分析**



第一行：Internet Protocol Version 4, Src: 10.128.235.166, Dst: 123.151.72.63 ip版本为4

第二行：互联网协议IPv4

第三行：.... 0101 = Header Length: 20 bytes (5) IP头部长度为20字节

第四行：Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) 差分服务字段

第五行：IP包的总长度为52

第六行：标志字段

第七行：Flags: 0x4000, Don't fragment标记字段，不支持分组

第八行：Time to live: 128 生存期，TTL通常表示包在被丢弃前最多能经过的路由器个数，当数据包传输到一个路由器之后，TTL就自动减1，如果减到0了还没有传送到目标主机，那么就自动丢失。

第九行：此包内封装的上层协议为TCP

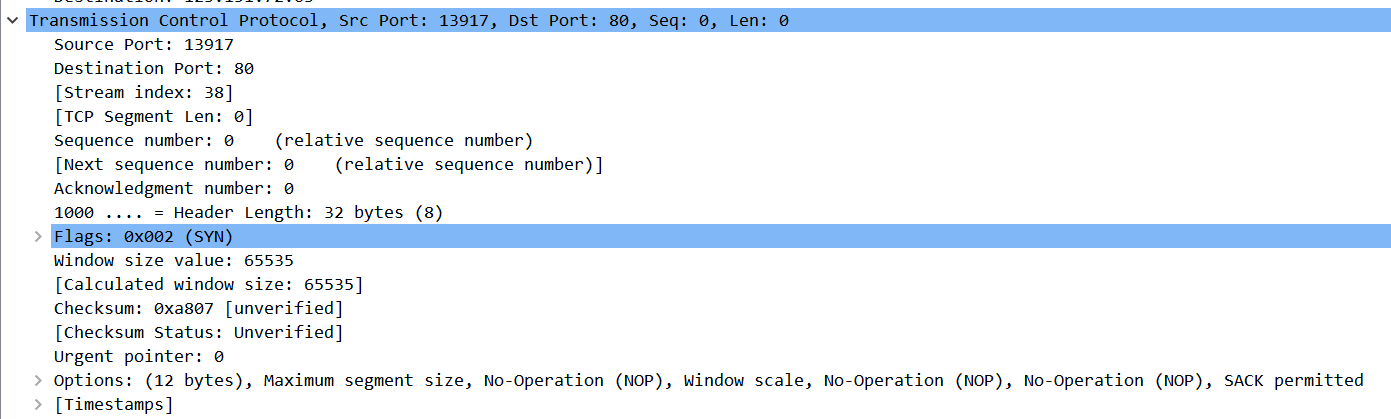
第十行：Header checksum: 0x3f2f [validation disabled] 头部数据的校验和

第十一行：头部校验和状态：未验证

第十二行：Source: 10.128.235.166 源IP地址

第十三行：Destination: 123.151.72.63 目标IP地址

**4.transmission control protocol分析**



第一行：TCP报文主要内容，包括源端口号和目的端口号、Seq和长度。

第二行：源端口号13917，数据传输的16位源端口号和16位目标端口号(用于寻找发端和收端应用进程)；

第三行：目标端口号80。

第四行：Stream index 是一个内部Wireshark映射到：[IP地址A，TCP端口A，IP地址B，TCP端口B] ,相同tcp.stream值的所有数据包对于这些字段都应该具有相同的值

第五行：TCP段长度为0

第六行：相对序列号(此序列号用来确定传送数据的正确位置，且序列号用来侦测丢失的包)；

第七行：下一个序列号

第八行：Acknowledgment number是44位确认序列号，值等于1表示数据包收到，确认有效；

第九行：头部字节长度是32字节；

第十行：Flags，TCP标记字段，含6种标志；ACK：确认序号有效；SYN：同步序号用来发起一个连接；FIN：发端完成发送任务；RST：重新连接；PSH：接收方应该尽快将这个报文段交给应用层；URG：紧急指针(urgentpointer)有效；

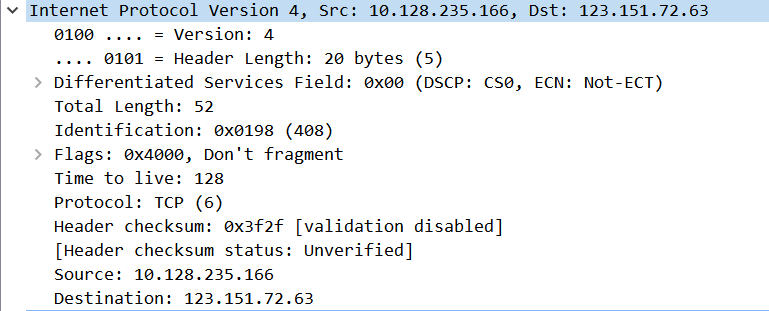
第十一行：window，流量控制的窗口大小，TCP的流量控制由连接的每一端通过声明的窗口大小来提供。窗口大小为字节数，起始于确认序号字段指明的值，这个值是接收端正期望接收的字节。窗口大小是一个16bit字段，因而窗口大小最大为65536字节，上面显示窗口大小为65535字节；

第十三行：Checksum，TCP数据段16位校验和，检验和覆盖了整个的TCP报文段，由发端计算和存储，并由收端进行验证；

第十五行：紧急指针：只有当 URG 标志置 1 时紧急指针才有效。紧急指针是一个正的偏移量，和顺序号字段中的值相加表示紧急数据最后一个字节的序号。 TCP 的紧急方式是发送端向另一端发送紧急数据的一种方式；

第十六行：选项和填充：最常见的可选字段是最长报文大小，又称为MSS（Maximum Segment Size），每个连接方通常都在通信的第一个报文段（为建立连接而设置SYN标志为1的那个段）中指明这个选项，它表示本端所能接受的最大报文段的长度。选项长度不一定是32位的整数倍，所以要加填充位，即在这个字段中加入额外的零，以保证TCP头是32的整数倍。

1. **IP协议消息分析**



第一行：Internet Protocol Version 4, Src: 10.128.235.166, Dst: 123.151.72.63 ip版本为4

第二行：互联网协议IPv4

第三行：.... 0101 = Header Length: 20 bytes (5) IP头部长度为20字节

第四行：Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) 差分服务字段

第五行：IP包的总长度为52

第六行：标志字段

第七行：Flags: 0x4000, Don't fragment标记字段，不支持分组

第八行：Time to live: 128 生存期，TTL通常表示包在被丢弃前最多能经过的路由器个数，当数据包传输到一个路由器之后，TTL就自动减1，如果减到0了还没有传送到目标主机，那么就自动丢失。

第九行：此包内封装的上层协议为TCP

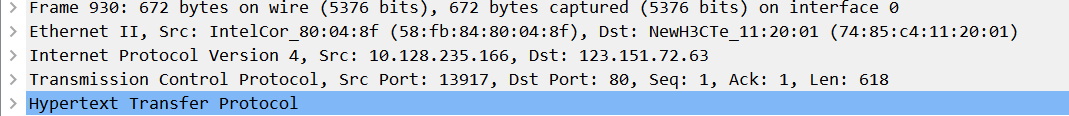
第十行：Header checksum: 0x3f2f [validation disabled] 头部数据的校验和

第十一行：头部校验和状态：未验证

第十二行：Source: 10.128.235.166 源IP地址

第十三行：Destination: 123.151.72.63 目标IP地址

1. **http协议消息格式**



第一行：帧，帧序号为930，传送的字节数为672字节

第二行：以太网，是数据链路层，源mac地址为58:fb:84:80:04:8f，目的mac地址为74:85:c4:11:20:01

第三行：ipv4协议，是网络层，源ip地址为10.128.235.166，目的ip地址为123.151.72.63

第四行：TCP协议，传输控制协议，是传输层，源端口为13917，目标端口为80，此时三次握手已经完成，Seq=1，Ack=1，长度为618

第五行：http协议，超文本传输协议，是应用层。