**北京邮电大学软件学院**

**\_\_2019-2020\_\_学年第\_1\_学期实验报告**

**课程名称： 计算机网络**

**实验名称： 实验一：数据链路层实验**

**实验完成人：**

**姓名：** **刘子豪** **学号：**\_\_**2017211971**\_**成绩：**\_\_\_\_\_\_\_\_

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

**日 期： 2019 年 10 月 23 日**

1. **实验目的**

通过本实验使学生理解协议数据单元（PDU）概念、掌握以太网帧结构字段定义和功能。

1. **实验任务**

搭建实验环境，使用网络抓包软件（如Wireshark软件等）抓取访问互联网所产生的数据包，分析其中的以太网帧结构字段组成，掌握以太网帧结构字段的功能。

1. **实验内容**

1) 在可以访问互联网的主机上下载并安装网络抓包软件Wireshark。

2) 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。

3) 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。

4) 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。

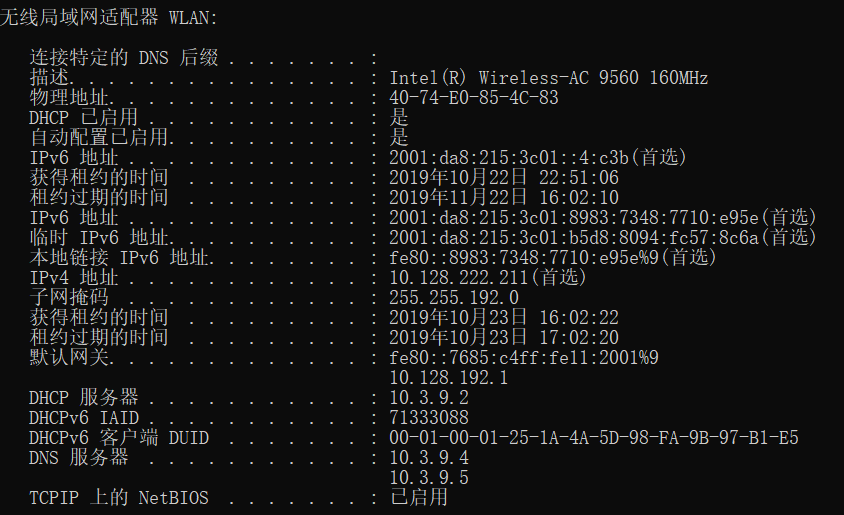
1. **实验环境**

1) Windows系统主机或Linux系统主机；

2) Wireshark软件

1. **实验过程与结果**
2. **查看本机IP地址以及MAC地址**

在Windows系统下，输入命令**ipconfig /all**，结果如下：

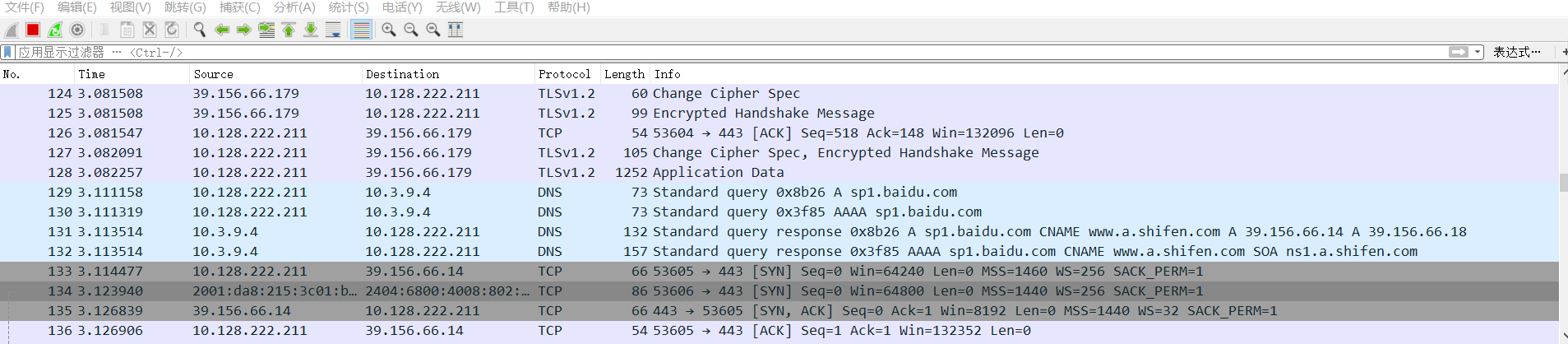


因此，可以得到：

* 本机的IPv4地址：10.128.222.211
* 本机的MAC地址：40-74-E0-85-4C-83
* DNS服务器：10.3.9.4 和 10.3.9.5

1. **访问百度网站，并抓取访问过程中的数据包**

在浏览器中输入网址[www.baidu.com](http://www.baidu.com)，对百度进行访问。当浏览器加载出网页后，抓取到了数据包，如下所示：

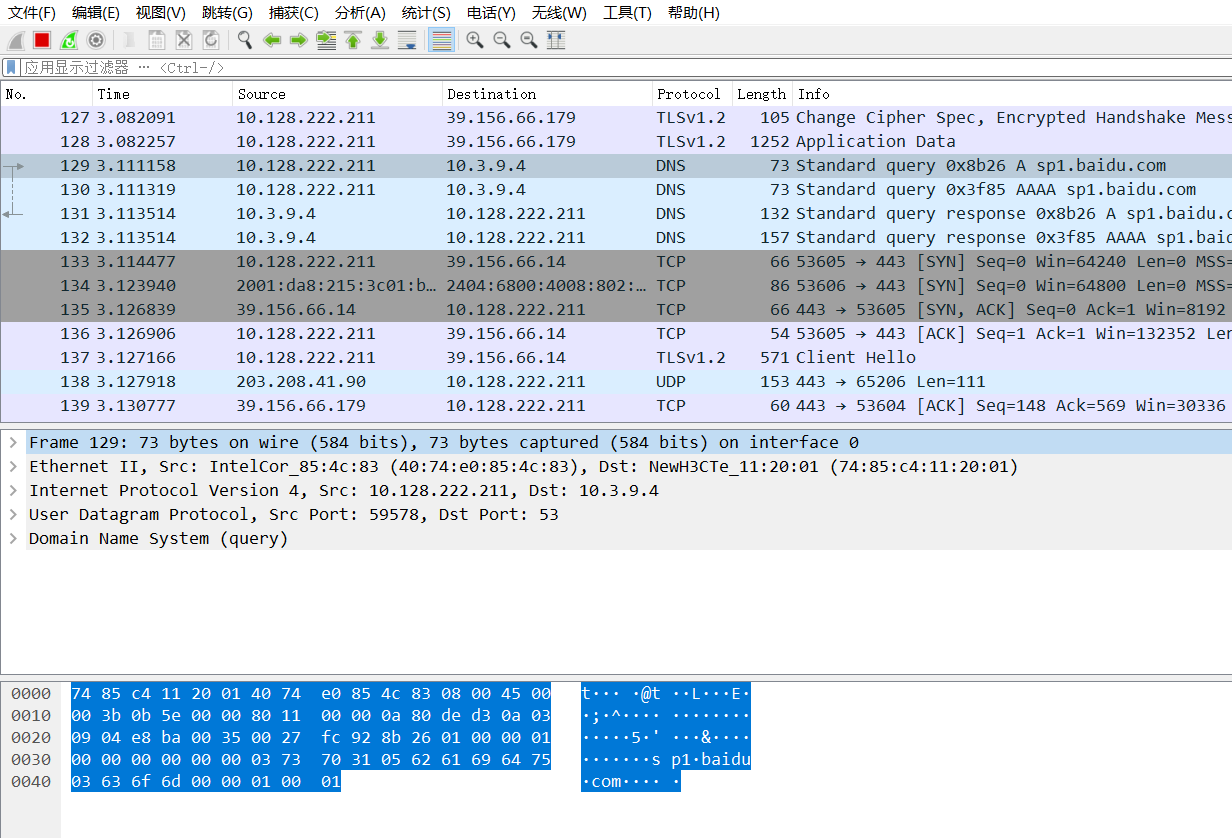


从图中可以看到，编号为129，130的帧的发送方为本机，接收方为DNS服务器（IP地址见ipconfig的查询结果），根据数据帧的Info字段，推断该帧的功能为：**本机向DNS服务器询问www.baidu.com的IP地址**。

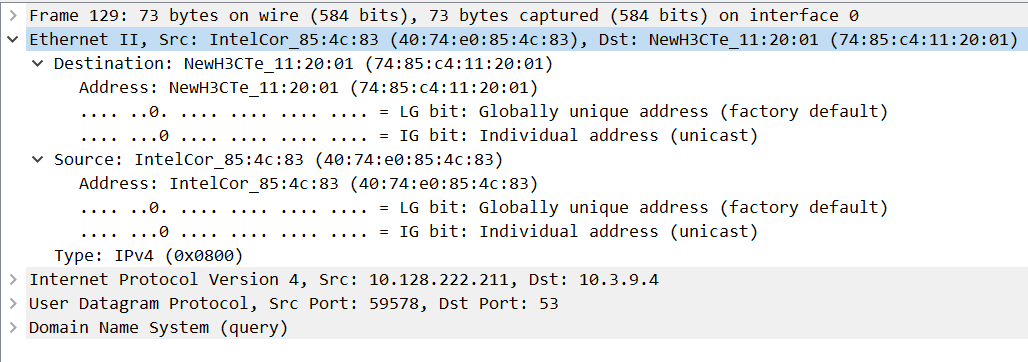
编号为131，132的帧的发送方为DNS服务器，接收方为本机，根据数据帧的Info字段，推断该帧的功能为：**DNS服务器将IP地址返回到本机**。

1. **对一个数据包的数据帧进行分析**

下面对之前抓取的DNS数据包进行分析（以编号为129的数据包为例）：



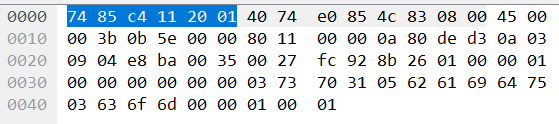
在数据包解析窗口中，第二行（Ethernet II…）对应数据包的数据链路层帧头部分，因此对这一部分进行详细分析：



在该部分中，包括Destination, Source, Type三个字段：

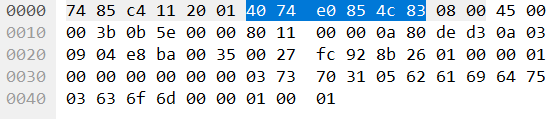
* **Destination: 74:85:c4:11:20:01**

接收方的MAC地址，在该数据包中代表的是DNS服务器的MAC地址。



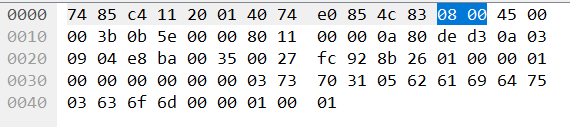
* **Source: 40:74:e0:85:4c:83**

发送方的MAC地址，在该数据包中代表的是本机的MAC地址，这与之前通过ipconfig命令查看的MAC地址相符合。



* **Type: IPv4(0x0800)**

使用的IP协议，可以知道该数据包中网络层使用的是IPv4协议。

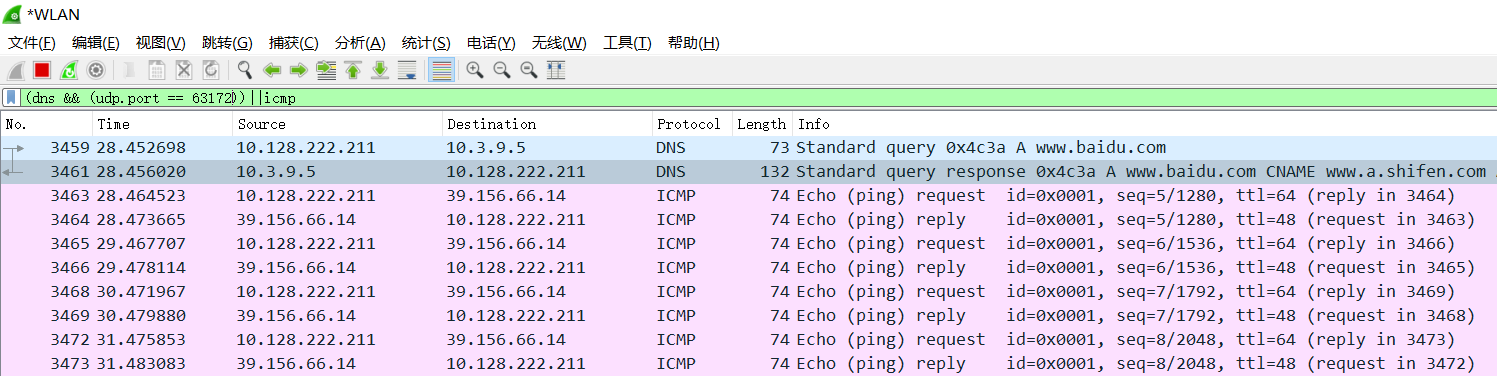


1. **（选做部分）分析实验中抓取的DNS（Domain Name System）消息、HTTP消息、TCP报文和IP分组，分析TCP报文字段组成及含义，分析IP分组的字段组成及含义。**
2. **DNS协议过程分析**

以ping命令访问www.baidu.com，通过该事例进行说明：



数据包抓取情况如下:



在该过程中，产生了2个DNS数据包以及8个ICMP数据包。

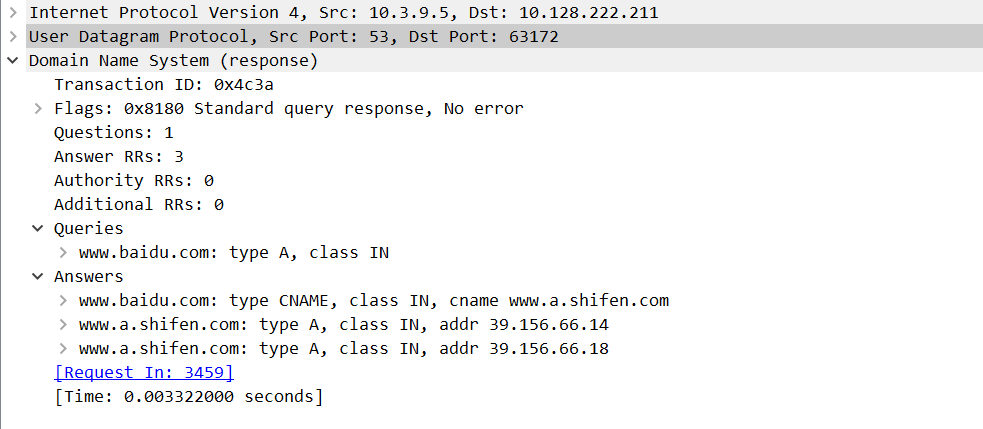
其中，DNS数据包的作用是向域名服务器请求某域名（www.baidu.com）对应的IP地址，ICMP包的作用是执行ping命令的发送、应答过程（因为一共有4次ping，因此总共有8个ICMP数据包）。

DNS域名解析过程如下：

* 客户端向DNS服务器发送查询信息，查询www.baidu.com的IP地址（第3459行）。
* DNS服务器收到查询请求，并发送应答消息，包中包含该域名对应的IP地址（第3461行）。

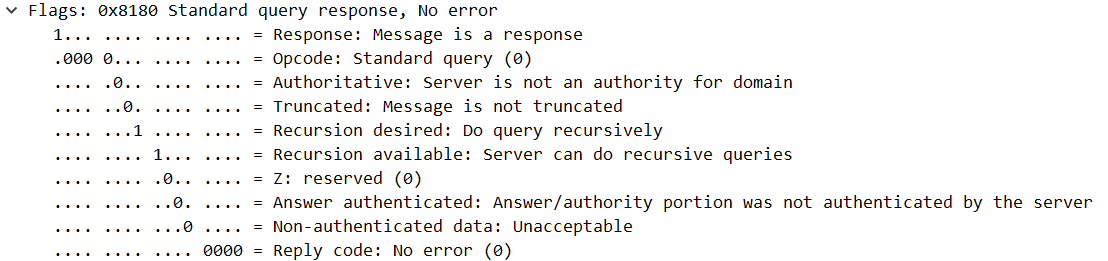
1. **DNS字段组成分析**

第二个DNS包的详细结构如下：



下面对该数据包的DNS部分进行详细分析：

* Transaction ID字段记录了本次事务的ID，**两个DNS数据包的Transaction ID字段的值是相同的**。
* Flags字段的详细信息如下所示：

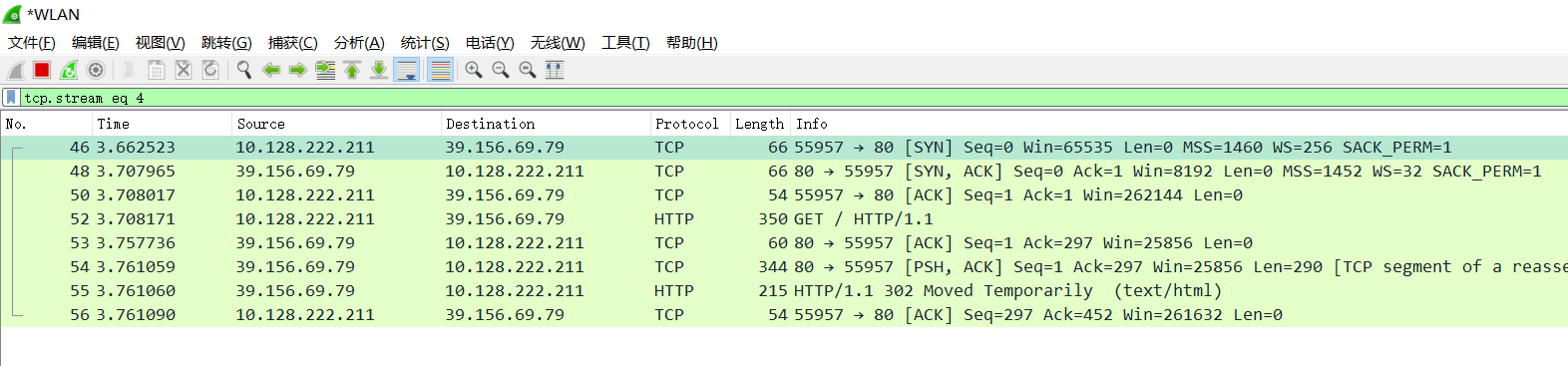


该字段记录了该数据包的很多信息，比如该消息的类型是query还是response， 包中是否产生错误等等。

* Questions字段表示问题计数，由于本次查询的问题只有一个（查询[www.baidu.com的IP](http://www.baidu.com的IP)地址），因此该字段的值为1。
* Answer RR 字段表示应答消息计数，可以知道该数据包中包含3个应答消息。
* Queries字段记录了详细的问题，而查询的是[www.baidu.com的IP](http://www.baidu.com的IP)地址。
* Queries字段记录了详细的应答消息
  + 回答1类型为cname，代表别名，别名为www.a.shifen.com
  + 回答2和回答3均为主机地址，IP地址为39.156.66.14和39.156.66.18

1. **TCP连接建立过程——三次握手**

通过浏览器访问[www.baidu.com](http://www.baidu.com)，并在wireshark中进行数据包抓取，过滤出TCP和ipv4的数据包之后，对TCP数据流进行追踪，得到的结果如下：

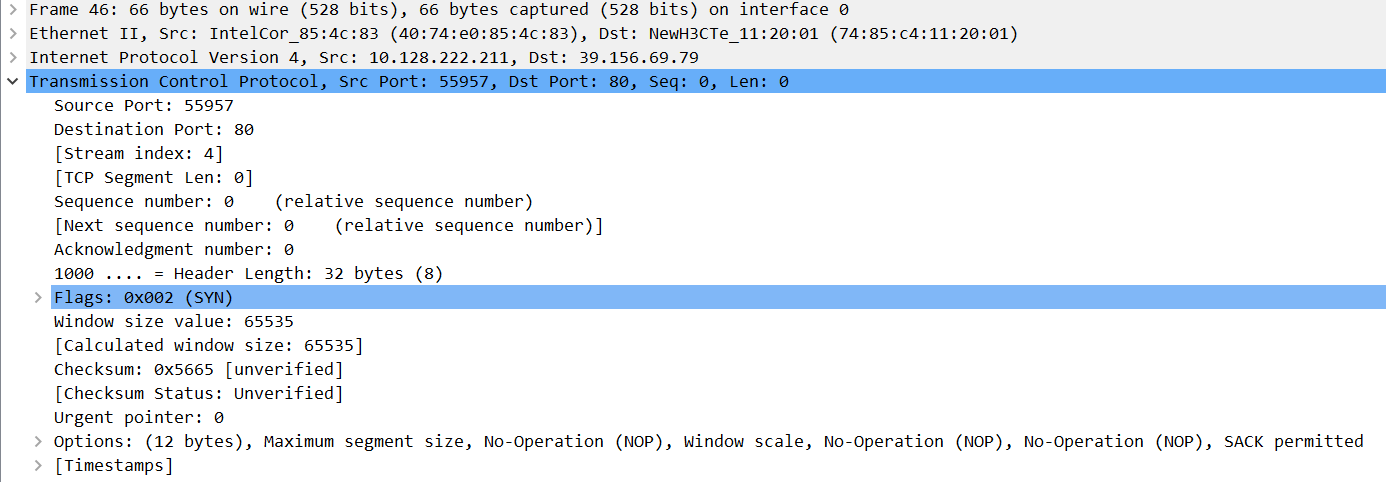


前三个TCP数据包即为TCP建立连接所用的三个数据包，使用了三次握手的方法，下面对这三个数据包的功能进行分析，从而对三次握手的整个过程进行描述：

* [SYN]: 客户端首先向服务端发送syn=1的包（第46行），该包用于与服务器建立同步，发送之后，客户端等待服务器的响应。
* [SYN, ACK]: 服务器的响应（第48行）。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]: 客户端对服务器发送的确认报文（第50行），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。

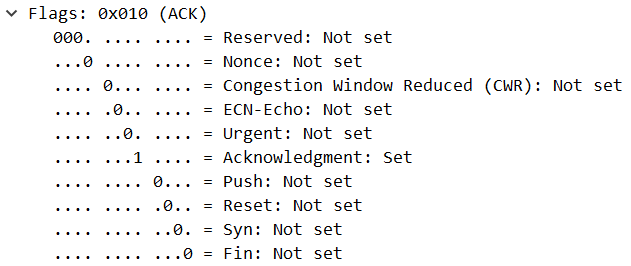
1. **TCP报文字段组成**

下图为TCP部分的全部内容：



一些字段的具体作用：

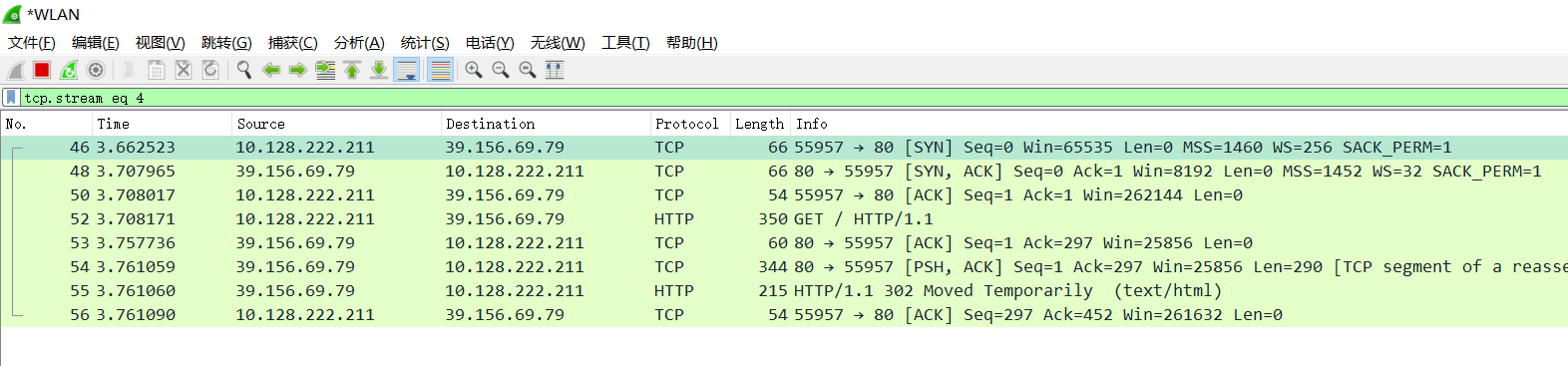
* Source Port: 发送方的端口号
* Destination Port: 接收方的端口号
* Sequence number: 报文的序列号（相对序列号）
* Acknowledgment number: 确认序列号，用来表示报文是否包含ACK信息。
* Header length: 报文头部长度。
* **Flags**: 标记字段，记录了报文的性质，比如ACK，SYN，RST，FIN等等，下图为该字段的详细内容。



* Window size value: 流量控制的窗口大小，**通过控制该字段，防止发送方发送消息速度过快，从而淹没接收方**。
* Checknum: 数据段的校验和。

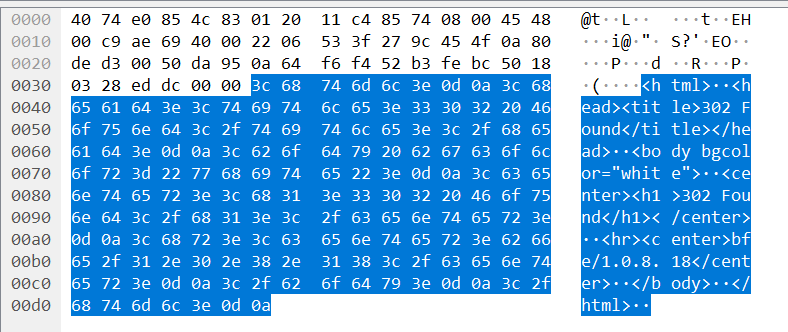
1. **HTTP协议过程**

仍然以使用浏览器访问[www.baidu.com](http://www.baidu.com)为例：



HTTP协议过程如下：

* 当客户端和服务端通过三次握手建立TCP连接（第46，48，50行，详细过程见2）中的分析）。
* 客户端发送HTTP请求，请求获得服务端中的网页信息（第52行）。在图中，客户端发送了GET请求，协议版本为HTTP/1.1。
* 服务器收到GET请求之后，发送ACK消息（第53行）。
* 服务器发送HTTP消息，里面包含具体的网页信息（第55行）。**查看该数据包的数据字段，可以发现是一个完整的HTTP网页代码**：



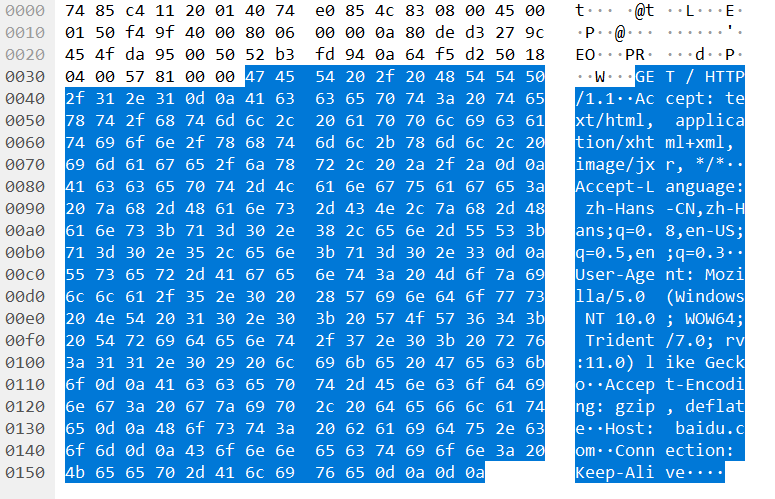
* 客户端收到HTTP消息，返回一个ACK消息（第56行）。

1. **HTTP协议消息格式**

下图为**HTTP请求消息**的详细结构：

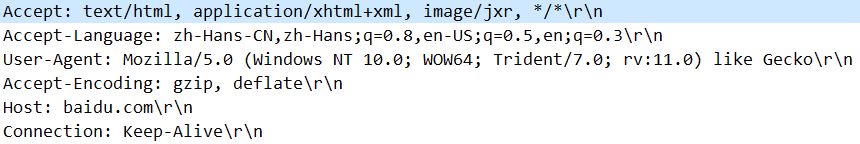


**查看数据包的具体数据内容，可以发现HTTP字段是以ASCII码来传输的：**



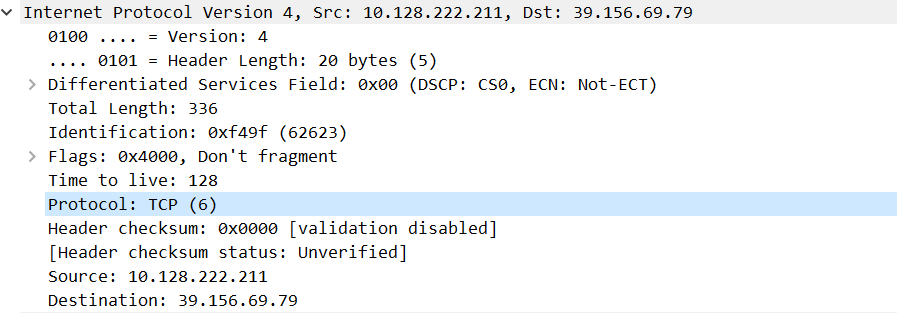
一些重要的字段：

* GET / HTTP/1.1
  + GET: 客户端的请求方法
  + /: 请求的URI
  + HTTP/1.1: 协议的版本
* 请求头：包含许多有关的客户端环境和请求正文的有用信息。例如，请求头可以声明浏览器所用的语言，请求正文的长度等。



1. **IP字段组成**

下图为HTTP请求消息的IP字段：



其中的一些重要字段：

* Version: 版本，**该包使用的是IPv4协议**。
* Header Length: 首部长度，**该包中IP字段的总长度为20字节**。
* Differentiated Services Field: 服务类型。
* Total Length: 数据包长度。
* Flags: 标记字段。
* Protocol：上层协议，该包中IP协议的上层协议为TCP协议。
* Header checksum: 首部校验和，检查IP报头在传输过程中是否损坏。
* Source：10.128.213.85 **发送方的IP地址，该包中为本机。**
* Destination：14.215.177.38  **接收方的IP地址，该包中为HTTP服务器。**

1. **心得体会**

通过使用Wireshark软件对网络数据包进行抓取，对日常生活中的一些网络使用有了更清晰的了解，对各种协议字段组成及含义有了更深的了解，对数据链路层的协议数据单元及功能有了更深的认识。