

西安科技大学

**计算机网络原理**

**学院：** 计算机科学与技术学院

**专业：** 网络工程系   
 **班级：** 网络工程1801班

**姓名：** 吴斌

**学号：** 18408020129

**日期：** 2020 年 6 月

1）**HTTP工作原理:**

http是一个简单的请求-响应协议，它通常运行在TCP之上。它指定了客户端可能发送给服务器什么样的消息以及得到什么样的响应。请求和响应消息的头以ASCII码形式给出；而消息内容则具有一个类似MIME的格式。这个简单模型是早期Web成功的有功之臣，因为它使得开发和部署是那么的直截了当。

HTTP是基于客户/服务器模式，且面向连接的。典型的HTTP事务处理有如下的过程：

（1）客户与服务器建立连接；

（2）客户向服务器提出请求；

（3）服务器接受请求，并根据请求返回相应的文件作为应答；

（4）客户与服务器关闭连接。

客户与服务器之间的HTTP连接是一种一次性连接，它限制每次连接只处理一个请求，当服务器返回本次请求的应答后便立即关闭连接，下次请求再重新建立连接。这种一次性连接主要考虑到WWW服务器面向的是Internet中成干上万个用户，且只能提供有限个连接，故服务器不会让一个连接处于等待状态，及时地释放连接可以大大提高服务器的执行效率。

HTTP是一种无状态协议，即服务器不保留与客户交易时的任何状态。这就大大减轻了服务器记忆负担，从而保持较快的响应速度。HTTP是一种面向对象的协议。允许传送任意类型的数据对象。它通过数据类型和长度来标识所传送的数据内容和大小，并允许对数据进行压缩传送。当用户在一个html文档中定义了一个超文本链后，浏览器将通过TCP/IP协议与指定的服务器建立连接。

从技术上讲是客户在一个特定的TCP端口（端口号一般为80）上打开一个套接字。如果服务器一直在这个周知的端口上倾听连接，则该连接便会建立起来。然后客户通过该连接发送一个包含请求方法的请求块。

HTTP规范定义了9种请求方法，每种请求方法规定了客户和服务器之间不同的信息交换方式，常用的请求方法是GET和POST。服务器将根据客户请求完成相应操作，并以应答块形式返回给客户，最后关闭连接。

2）**实验设计思路:**

我们有成熟的抓包工具，有要分析的协议名称，知道该协议的工作原理，HTTP协议工作于客户端-服务端架构上。浏览器作为HTTP客户端通过URL向HTTP服务端即WEB服务器发送所有请求。所以我们直接完成操作即可。

3）**实验过程:**

首先关闭所有计算机进程，以防抓的包太多影响观察。然后打开wireshark开始抓包，再然后打开浏览器输入事先复制的网址[**https://www.xust.edu.cn/**](https://www.xust.edu.cn/)，然后观察抓到数据包的变化情况。在这过程中完成了一次HTTP操作。

一次HTTP操作称为一个事务，其工作过程可分为四步：

1.首先客户机与服务器需要建立连接。只要单击某个超级链接，HTTP的工作开始。

2.建立连接后，客户机发送一个请求给服务器，请求方式的格式为：统一资源标识符（URL），协议版本号，后边是MIME信息包括请求修饰符，客户机信息和可能的内容。

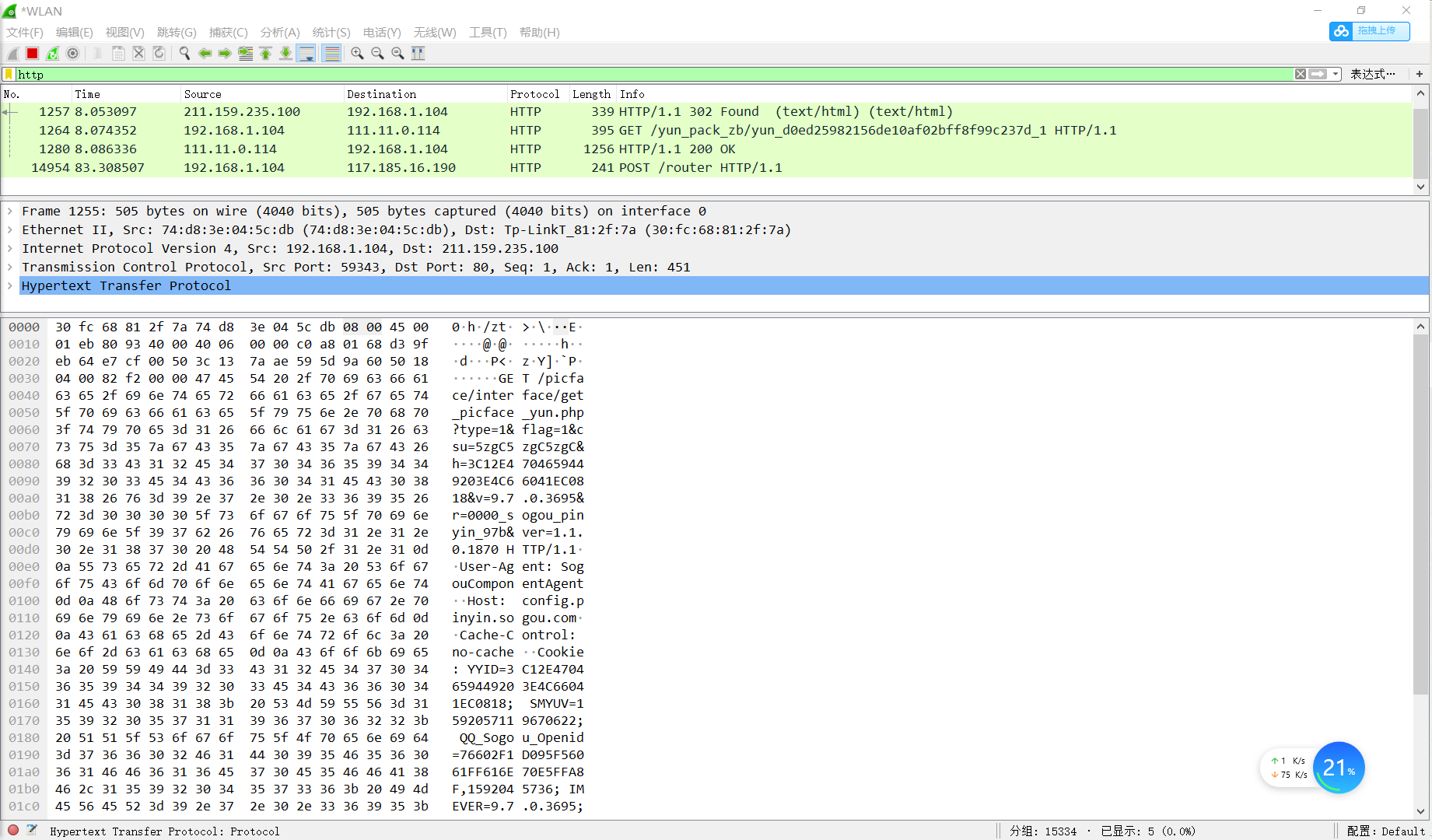
3.服务器接到请求后，给予相应的响应信息，其格式为一个状态行，包括信息的协议版本号，一个成功或错误的代码，后边是MIME信息包括服务器信息，实体信息和可能的内容。

4.客户端接收服务器所返回的信息通过浏览器显示在用户的显示屏上，然后客户机与服务器断开连接。

**然后就我们抓到的报文开始分析。**

4）**实验结果展示及分析:**

**先分析http协议**



**Hypertext Transfer Protocol**：**（请求信息）**  
GET / HTTP/1.1\r\n #请求行信息#  
**[Expert Info (Chat/Sequence):** GET / HTTP/1.1\r\n] #专家信息#  
**Request Method:** GET #请求的方法#  
**Request URI:** / #请求的URI#  
**Request Version:** HTTP/1.1 #请求的版本#  
**Host:** www.boomgg.cn\r\n #请求主机#  
**Connection:** keep-alive\r\n #使用持久链接#  
**Upgrade-Insecure-Requests:** 1\r\n #升级不安全请求#  
**User-Agent:** Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36\r\n #浏览器类型#  
**Accept-Encoding:** gzip, deflate, sdch\r\n #请求的编码格式#  
**Accept:**text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n #请求的类型#  
**Accept-Language:** zh-CN,zh;q=0.8\r\n #请求语言#  
**Cookie:**CNZZDATA155540=cnzz\_eid%3D20937234201483596271-%26ntime%3D1483596271\r\n #Cookie信息#Cookie **pair:**CNZZDATA155540=cnzz\_eid%3D20937234201483596271-%26ntime%3D1483596271\r\n #Cookie对#

**[Full request URI:** <https://www.xust.edu.cn/>] #请求的URI全称#

**[HTTP request 1/3]** #HTTP请求进度#

**[Response in frame: 12]** #响应帧#

**[Next request in frame: 15]** #下一个请求帧#

**Hypertext Transfer Protocol**：**（响应信息）**

HTTP/1.1 200 OK\r\n #响应行信息#

**[Expert Info (Chat/Sequence):** HTTP/1.1 200 OK\r\n] #专家信息#

**Request Version:** HTTP/1.1 #请求版本#

**Status Code:** 200 #状态码#

**Response Phrase:** OK #响应短语#

**Date:** Tue, 31 Jan 2017 07:34:36 GMT\r\n #响应时间#

**Server:** Apache/2.4.6 (CentOS) PHP/5.4.16\r\n #服务器信息#

**Last-Modified:** Tue, 17 Jun 2014 16:00:47 GMT\r\n #上一次修改#

**ETag:** "4b8d-4fc0a3f32a9c0"\r\n #上一次修改标识#

**Accept-Ranges:** bytes\r\n #接收范围#

**Content-Length:** 19341\r\n #内容长度#

**Keep-Alive:** timeout=5, max=99\r\n #保持响应时间,以及最大值#

**Connection:** Keep-Alive\r\n #使用持久链接#

**Content-Type:** text/css\r\n #响应的内容类型#

[HTTP response 2/3] #HTTP响应#

[**Time since request:** 0.423110000 seconds] #响应使用时长#

[**Prev request in frame**: 5] #上一个请求的帧#

[**Prev response in frame:** 12] #上一个响应的帧#

[**Request in frame: 15**] #请求的帧#

[**Next request in frame: 47**] #下一个请求的帧#

**[Next response in frame: 59]** #下一个响应的帧#

**File Data:** 19341 bytes #文件数据大小#

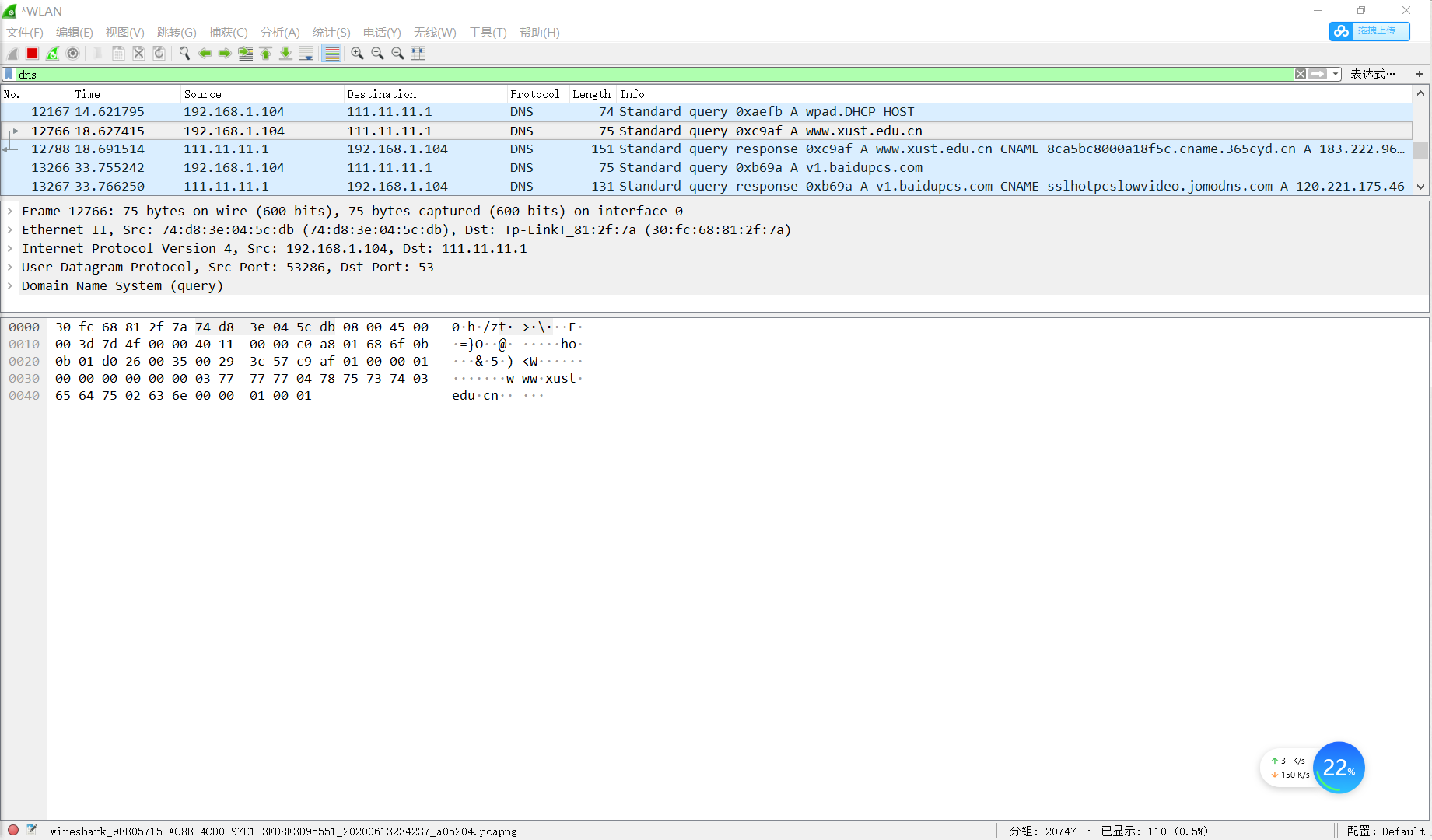
**Line-based text data:** text/css #数据#

**Form item:** "UserID" = "Kemin" #这里可以看到发送的用户名

**Form item:** "UserPass" = "Fang" #这里可以看到发送的密码

**Form item:** "Log" = "Login"

**接下来分析tcp协议**



Source Port: http (80)                                //源端口号

Destination Port: 60575 (60575)                //目的端口号

Sequence22number:2262436122(relative22sequence22number)                //32位序列号

Acknowledgment22number:22122(relative22ack22number)                         //32位确认序列号，即发送端希望收到的序列号

010122....22= 22Header22Length:222022bytes22(5)                                              //4位首部长度

Flags: 0x010 (ACK)                              //标志位  ACK置1

Window size value: 240          //16位窗口大小（用于接收方的流量控制）Checksum: 0xacb5 [unverified]                                  //16位检验和

Urgent pointer: 0                                               //16位紧急指针

**标志位解释：**

**URG：** 紧急指针（ urgent pointer）有效。

**ACK**： 确认序号有效。

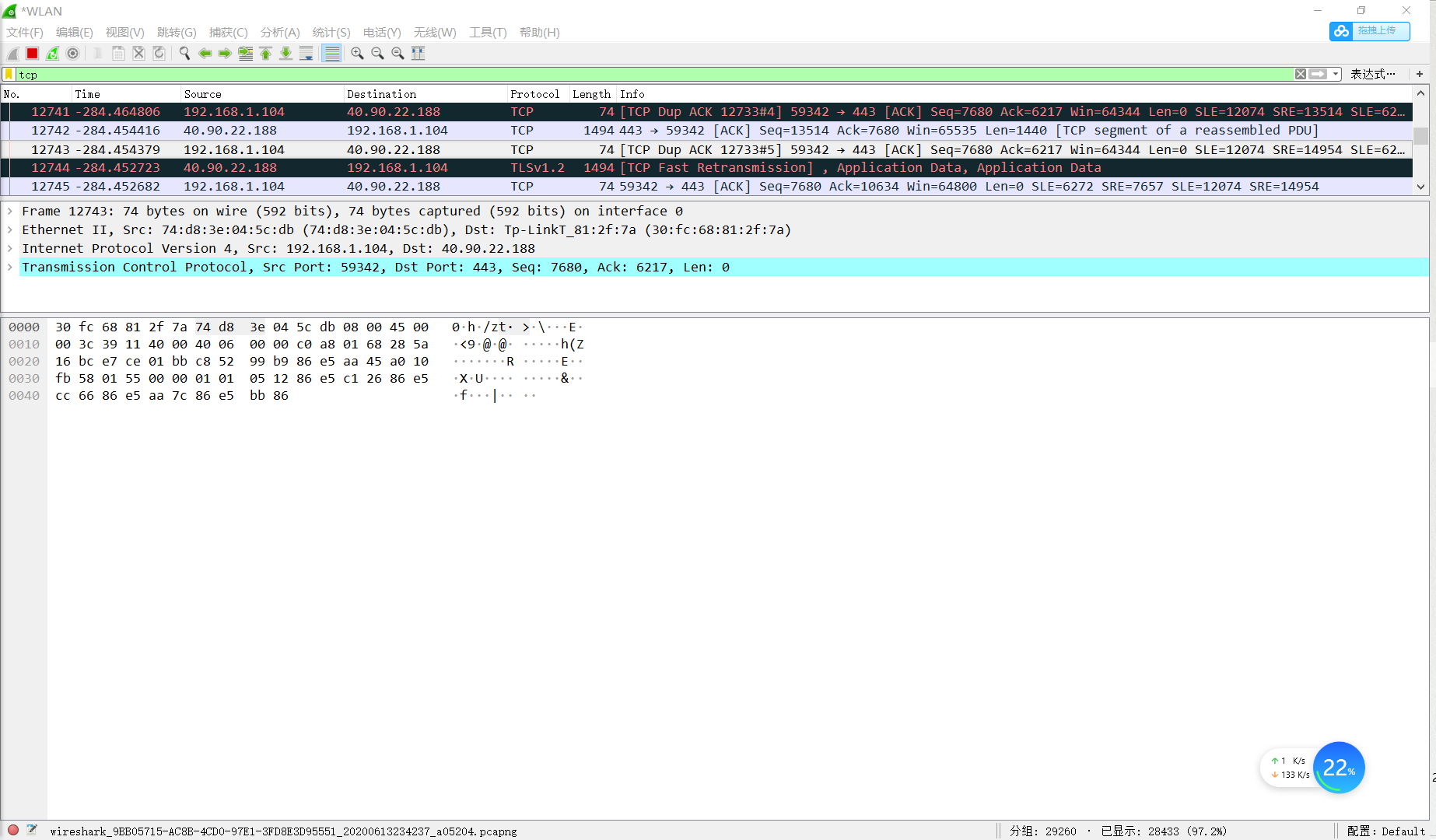
**PSH**： 接收方应该尽快将这个报文段交给应用层。

**RST**： 重建连接。

**SYN：** 同步序号用来发起一个连接。

**FIN**： 发端完成发送任务。

**最后是dns协议：**



**Transaction ID：**DNS 报文的 ID 标识。对于请求报文和其对应的应答报文，该字段的值是相同的。通过它可以区分 DNS 应答报文是对哪个请求进行响应的。

**flags：**DNS 报文中的标志字段。

**questions：**DNS 查询请求的数目。

**Answers RRs：**DNS 响应的数目。

**Authority RRs：**权威名称服务器的数目。

**Additional RRs：**额外的记录数目（权威名称服务器对应 IP 地址的数目）。

Domain Name System (query)

Transaction ID: 0x9ad0 #事务ID

Flags: 0x0000 Standard query #报文中的标志字段

0... .... .... .... = Response: Message is a query

#QR字段, 值为0, 因为是一个请求包

.000 0... .... .... = Opcode: Standard query (0)

#Opcode字段, 值为0, 因为是标准查询

.... ..0. .... .... = Truncated: Message is not truncated

#TC字段

.... ...0 .... .... = Recursion desired: Don't do query recursively

#RD字段

.... .... .0.. .... = Z: reserved (0) #保留字段, 值为0

.... .... ...0 .... = Non-authenticated data: Unacceptable

#保留字段, 值为0

Questions: 1 #问题计数, 这里有1个问题

Answer RRs: 0 #回答资源记录数

Authority RRs: 0 #权威名称服务器计数

Additional RRs: 0 #附加资源记录数

Domain Name System (query) #查询请求

Queries #问题部分

baidu.com: type A, class IN

Name: baidu.com #查询名字段, 这里请求域名baidu.com

[Name Length: 9]

[Label Count: 2]

Type: A (Host Address) (1) #查询类型字段, 这里为A类型

Class: IN (0x0001) #查询类字段, 这里为互联网地址

Answers #“回答问题区域”字段

baidu.com: type A, class IN, addr 220.181.57.216 #资源记录部分

Name: baidu.com #域名字段, 这里请求的域名为baidu.com

Type: A (Host Address) (1) #类型字段, 这里为A类型

Class: IN (0x0001) #类字段

Time to live: 5 #生存时间

Data length: 4 #数据长度

Address: 40.90.22.188 #资源数据, 这里为IP地址

baidu.com: type A, class IN, addr 123.125.115.110 #资源记录部分

Name: baidu.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 5

Data length: 4

Address: 123.125.115.110

Authoritative nameservers #“权威名称服务器区域”字段

baidu.com: type NS, class IN, ns ns7.baidu.com #资源记录部分

Name: baidu.com

Type: NS (authoritative Name Server) (2) #类型字段, 这里为NS类型

Class: IN (0x0001)

Time to live: 5

Data length: 6

Name Server: ns7.baidu.com #权威名称服务器

baidu.com: type NS, class IN, ns dns.baidu.com #资源记录部分

Name: baidu.com

Type: NS (authoritative Name Server) (2) #类型字段, 这里为NS类型

Class: IN (0x0001)

Time to live: 5

Data length: 6

Name Server: dns.baidu.com #权威名称服务器

baidu.com: type NS, class IN, ns ns3.baidu.com #资源记录部分

Name: baidu.com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 5

Data length: 6

Name Server: ns3.baidu.com #权威名称服务器

baidu.com: type NS, class IN, ns ns4.baidu.com #资源记录部分

Name: baidu.com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 5

Data length: 6

Name Server: ns4.baidu.com #权威名称服务器

baidu.com: type NS, class IN, ns ns2.baidu.com #资源记录部分

Name: baidu.com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 5

Data length: 6

Name Server: ns2.baidu.com #权威名称服务器

Additional records #“附加信息区域”字段

dns.baidu.com: type A, class IN, addr 202.108.22.220 #资源记录部分

Name: dns.baidu.com #“权威名称服务器”名称

Type: A (Host Address) (1) #类型字段, 这里为A类型

Class: IN (0x0001)

Time to live: 5

Data length: 4

Address: 202.108.22.220 #“权威名称服务器”的IP地址

ns2.baidu.com: type A, class IN, addr 61.135.165.235 #资源记录部分

Name: ns2.baidu.com #“权威名称服务器”名称

Type: A (Host Address) (1) #类型字段, 这里为A类型

Class: IN (0x0001)

Time to live: 5

Data length: 4

Address: 61.135.165.235 #“权威名称服务器”的IP地址

ns3.baidu.com: type A, class IN, addr 220.181.37.10 #资源记录部分

Name: ns3.baidu.com #“权威名称服务器”名称

Type: A (Host Address) (1) #类型字段, 这里为A类型

Class: IN (0x0001)

Time to live: 5

Data length: 4

Address: 220.181.37.10 #“权威名称服务器”的IP地址

ns4.baidu.com: type A, class IN, addr 220.181.38.10 #资源记录部分

Name: ns4.baidu.com #“权威名称服务器”名称

Type: A (Host Address) (1) #类型字段, 这里为A类型

Class: IN (0x0001)

Time to live: 5

Data length: 4

Address: 220.181.38.10 #“权威名称服务器”的IP地址

ns7.baidu.com: type A, class IN, addr 180.76.76.92 #资源记录部分

Name: ns7.baidu.com #“权威名称服务器”名称

Type: A (Host Address) (1) #类型字段, 这里为A类型

Class: IN (0x0001)

Time to live: 5

Data length: 4

Address: 180.76.76.92 #“权威名称服务器”的IP地址

**附做本次实验本机的网络信息:**

述完。