电子科技大学信息与软件工程学院

**实 验 报 告**

学 号 2016220304031

姓 名 邓巧

（实验） 课程名称 计算机网络

理论教师 傅翀

实验教师 傅翀

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：邓巧 学号：2016220304031 指导教师：傅翀**

**实验时间：2015年5月21日**

1. **实验名称：使用Wireshark抓取各类协议网络数据包**
2. **实验目的：**

使用WireShark分别抓取HTTP协议通信的网络数据和DNS通信的网络数据，分析对应的HTTP、TCP、IP协议和DNS、UDP、IP协议。

1. **实验原理：**

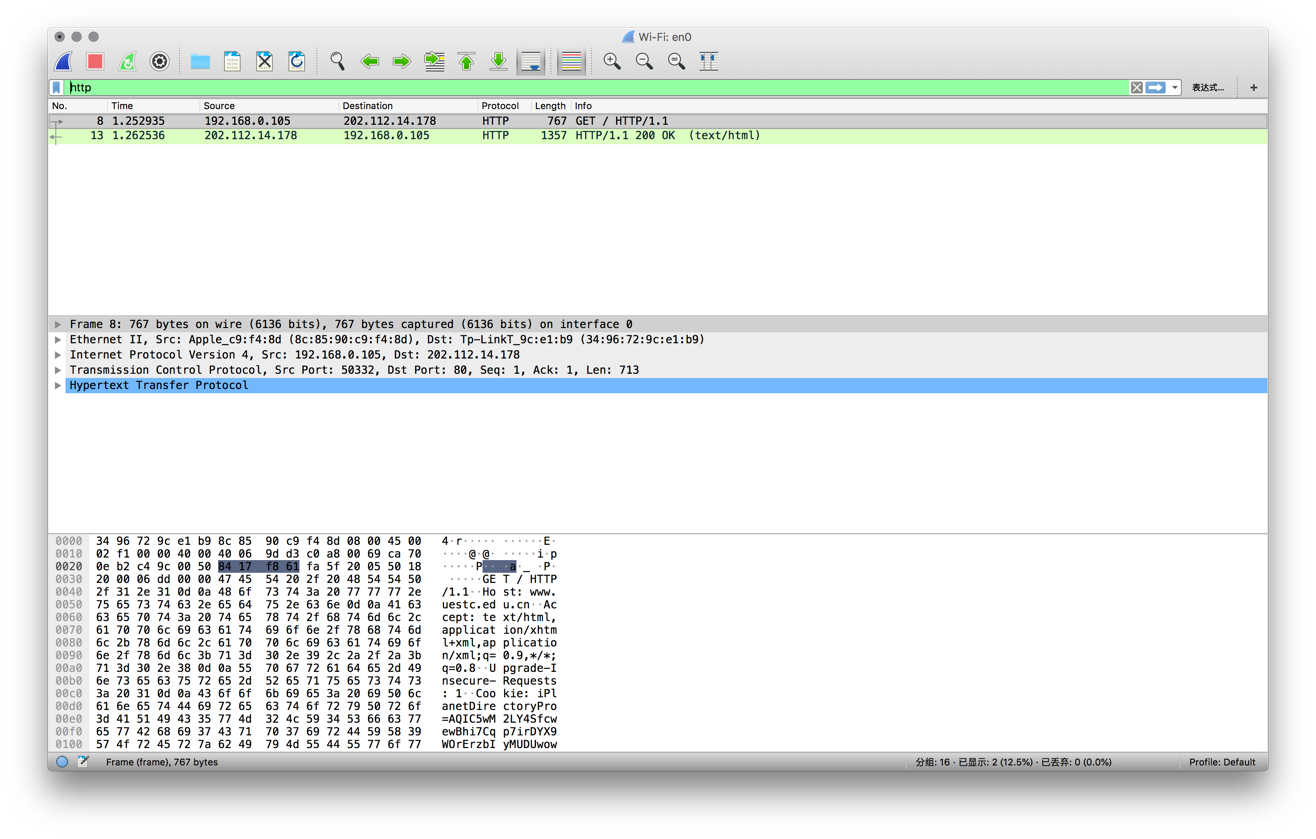
通过使用Wireshark对网络数据包进行抓取，分析。达到了解各类网络协议，和各个网络软件的工作原理的目的。

1. **实验内容：**
2. 抓取并分析HTTP协议，以及应用层之下的TCP、IP协议。
3. 抓取并分析DNS协议，以及应用层之下的UDP、IP协议。
4. **实验器材（设备、元器件）：**

Wireshark、PC机一台

1. **实验步骤：**
2. 打开Wireshark
3. 使用浏览器访问网页
4. 使用Wireshark中的过滤器进行筛选
5. 查看数据包，分析内容
6. **实验结果与分析（含重要数据结果分析或核心代码流程分析）**
7. 打开wireshark，点击开始
8. 打开浏览器，输入网址<http://www.uestc.edu.cn>.
9. 在过滤器中选择http过滤。

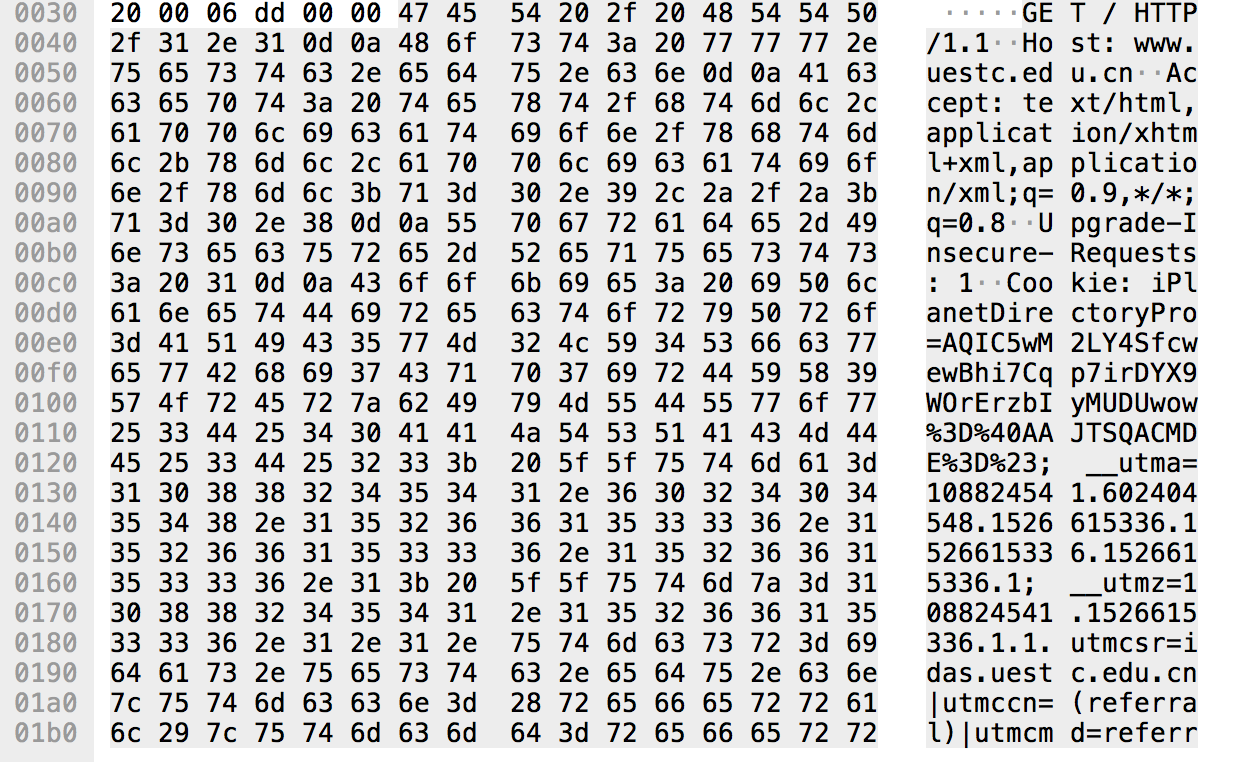
得到一组http请求和响应报文。



1. http请求报文：







* 其中，请求头中包含
* 请求方法：这里使用的GET
* 请求的资源定位符，此处为根目录。
* 请求头使用的协议，即HTTP/1.1
* 请求头后跟随\r\n，其后的host代表主机名。对于访问的<http://uestc.edu.cn>来说，主机名为[www.uestc.edu.cn](http://www.uestc.edu.cn)。
* Accept表示浏览器可接受的MIME类型。此处为：

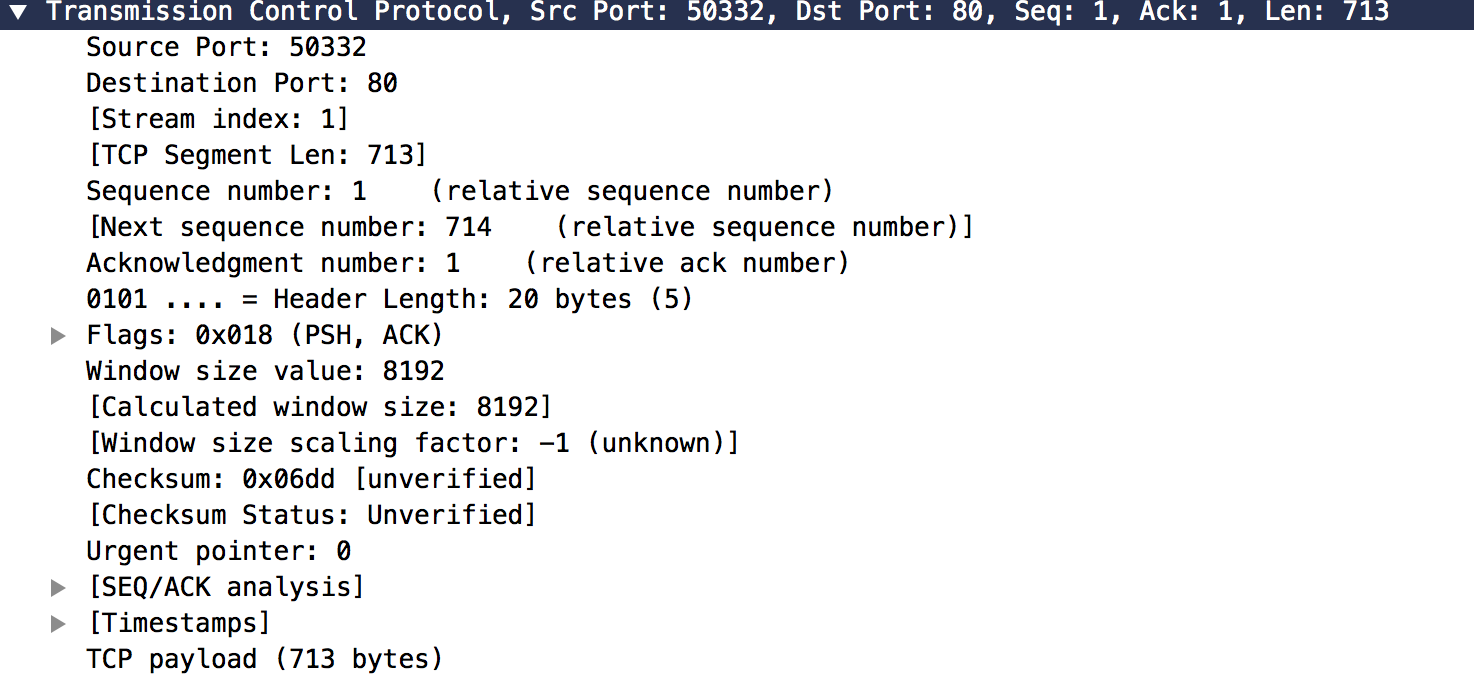


* 表示接收单一精确的MIME类型：text/html, application/xhtml+xml, application/xml，且权重为0.9.也接受其他类型\*/\*，权重为0.8。
* Upgrade-insecure-requests用于让浏览器自动升级请求从http到https,用于大量包含http资源的http网页直接升级到https而不会报错。如：



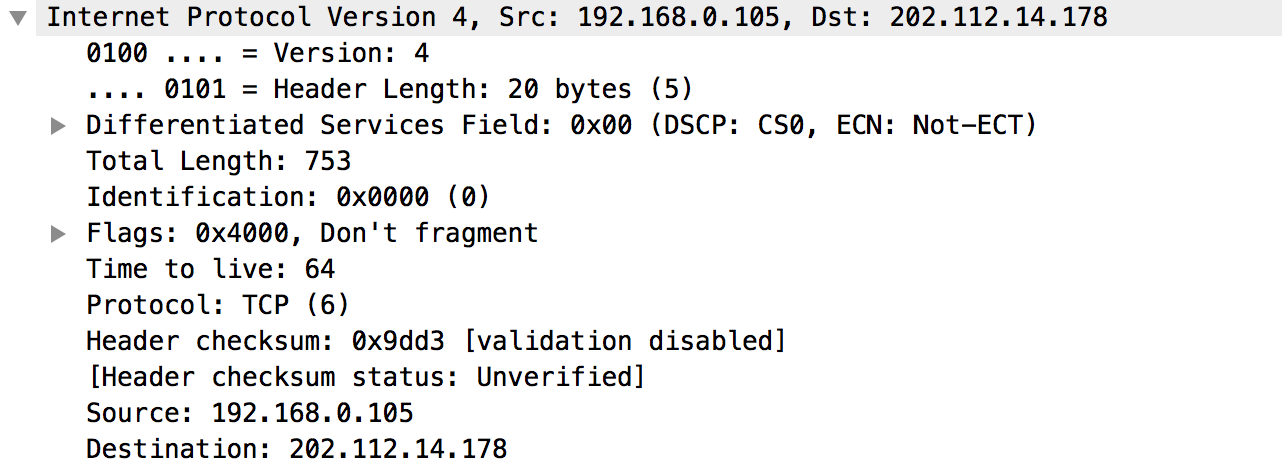
* Cookie:包含浏览器的cookie信息。
* User-agent告诉服务器，创建请求的浏览器和用户代理名称等信息。
* 此处表示，用户浏览器为基于mozilla的safari。
* Accept-Language: 告知服务器，我们能够处理的自然语言。
* Accept-encoding：告知服务器，我们能接受的内容编码，通常是某种压缩算法。
* Connection:表示采用持久连接或非持久连接，确定在当前事务完成后是否会保持连接。

1. tcp报文内容为



* 其中source Port 和Destination Port分别表示源端口和目的端口。此次源端口为50332，而目的端口为80.
* 序列号为1
* 确认号为1
* 报头长度20 bytes
* 3bits保留字段
* 标志符，其中PSH和ACK有效，PSH表示尽快接收。
* Window size value:接收窗口长度8192
* Checksum：校验和。此处为0x06dd
* Urgent pointer:紧急指针。

3.IP协议的报文内容：



· version:4 版本,此处版本为ipv4.

· header length:头部长度，此处为20 bytes

· differentiated services field:区分服务字段，在早期就是表示IP协议的服务类型，但在现在的以太网中已经被淘汰了，不再用了，把最后一位规定为零。

· total length:表示IP数据报文的总长度，也就是说这个IP数据报文的数据总共有多少个字节，其中包括了IP数据报文的首部和数据部分。总长度占16位（即16-31位），指的是首部部分和数据部分的长度，单位为字节。

· identification: 它是一个计数器，用来对产生的数据报进行标识，每传输一个数据报都要计数一次，用于标识分片的唯一性。

· flags: 标志,占用3位（即16 - 18），这三位分别是：R，D，M三位，第一位是保留位，没有被使用，目前只有后两个比特有意义。

D：标志字段中间的一位是 DF (Don’t fragment)，表示传输的数据不允许分片。一般DF = 1的话，表示数据一次性传输过去，不允许分片。

M：标志字段的最低位是 MF (More fragment)。代表数据是否分片，如果MF位值为1，表示后面还有数据，还没有传输完毕，相当于数据分片，分批次传输，如果MF = 0表示最后一个分片或者只有一个分片。

· time to live:存活时间，此处表示该包还有64跳存活时间。

· protocol: 上层协议，此处表示上层协议为TCP

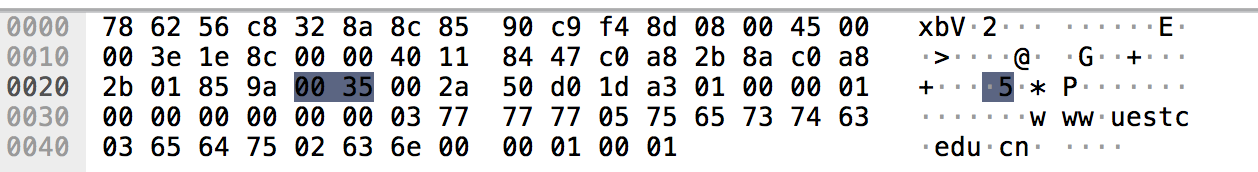
· header checksum status: 首部校验和，此处为0x9dd3

· source和destinagtion分别为源IP和目的IP地址。

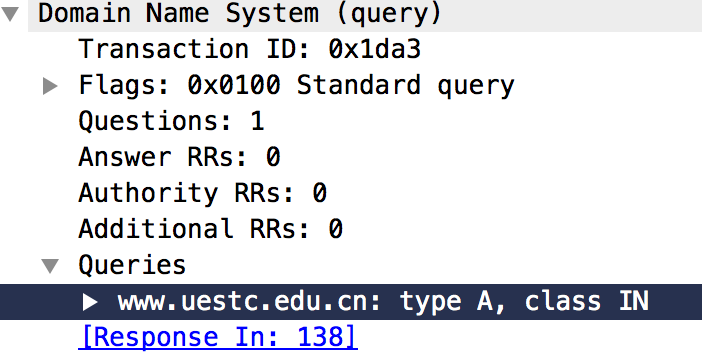
4.DNS报文：



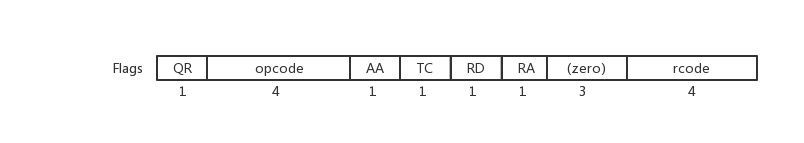
请求内容：



其中，报文内容为：



· Transaction ID:会话标识，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

· 标识：

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。

此处为0x0100.

· 数量字段：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。

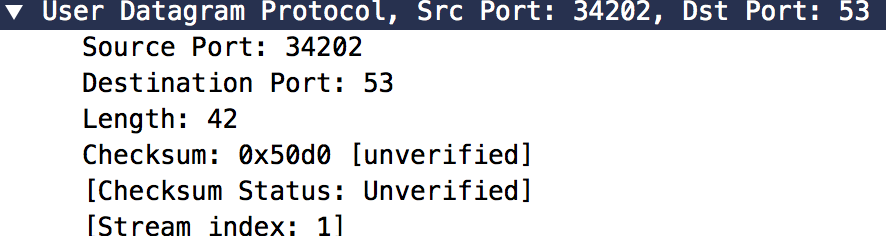
· 查询类型：



此处表示由域名www.uestc.edu.cn获得IPv4地址。

· 查询类：对于internet来说，总为IN

5.UDP报文内容：



· 源端口目的端口：分别为34202，和53.

· 报文长度：53

· 校验和：0x50d0

上层使用的IP内容格式与之前所分析的一致（仅协议一栏不同），不再赘述。

1. **总结及心得体会：**
2. 应该多上手练习，才能增强理解和记忆。
3. 网络的各层次在不同协议中都有体现
4. 应该读多利用过滤器。

**九、对本实验过程及方法、手段的改进建议：**

1. 可以让学生自己实现一个协议。

**报告评分：**

**指导教师签字：**