电子科技大学信息与软件工程学院

**实 验 报 告**

学 号 2017221302009

姓 名 陆圣珩

（实验） 课程名称 计算机网络

理论教师 刘梦娟

实验教师 刘梦娟

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：陆圣珩 学号：2017221302009 指导教师：刘梦娟**

**实验地点：信软楼西303 实验时间：2019.4**

**一、实验名称：应用层协议验证实验**

**二、实验学时：2学时**

**三、实验目的：**

掌握Wireshark工具的基本用法；

掌握HTTP协议的各种报文格式、报文的发送顺序，以及各种规定动作；

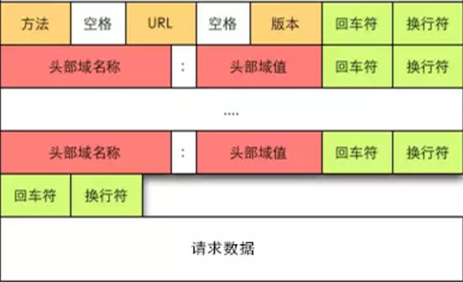
熟悉nslookup工具的基本用法；

理解DNS协议的运行过程。

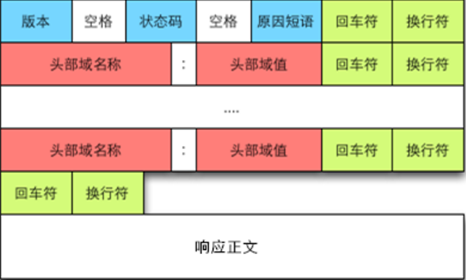
**四、实验原理：**

**HTTP协议的报文格式**

下图为http请求的报文结构



下图为http响应报文结构



**HTTP协议的基本发送/响应顺序**

1) 建立连接：客户端与服务器建立TCP连接

2) 发送请求：打开一个连接后，客户端把请求信息发送到服务器的相应端口上，完成请求动作提交。

3) 发送响应：服务器在处理完客户端请求之后，要向客户端发送响应消息。

4) 关闭连接：客户端和服务器端都可以关闭套接字来结束TCP/IP对话。

**HTTP协议的持续连接和非持续连接的区别**

http的持续连接是指请求多个对象可以使用同一个tcp连接，而非持续连接指的是每请求一个对象都需要建立一个新的tcp连接，比如在一个HTML页面中嵌有多个图像时，采用持续连接时对这些图像的请求可以使用同一个tcp连接，而非持续连接时每个图像都需要建立一个新的tcp连接。持续连接相对于非持续连接来说，传输效率更高，而采用流水线机制的持续连接效率更高。

**DNS协议的基本工作过程**

下面以域名为m.xyz.com的主机欲通过另一个主机的域名y.abc.com的IP地址为例，简述DNS协议过程。

主机m.xyz.com先向其本地服务器dns.xyz.com进行递归查询。

本地域名服务器先查询高速缓存，如果不久前已经查询过域名y.abc.com的IP，那么本地域名服务器就不必向根域名服务器查询，而是直接把高速缓存中存放的上次查询的结果（即y.abc.com的IP地址）告诉用户。

本地域名服务器采用迭代查询。他先向一个根域名服务器查询。

根域名服务器告诉本地域名服务器，下一次应查询的顶级域名服务器dns.com的IP地址。

本地域名服务器向顶级域名服务器dns.com进行查询。

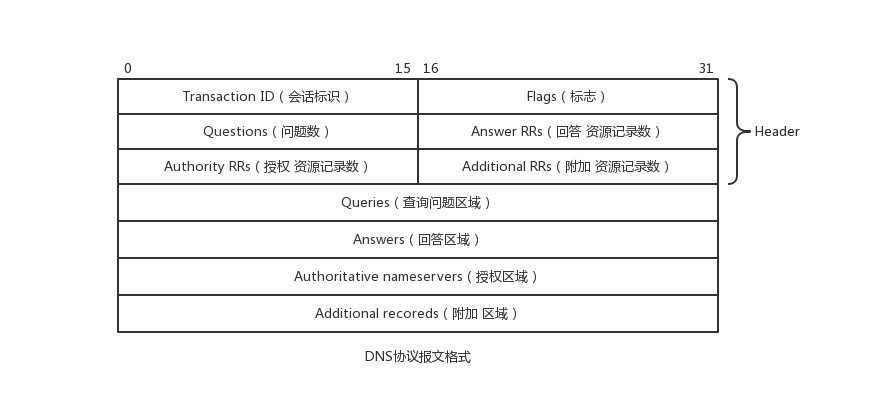
顶级域名服务器dns.com告诉本地域名服务器，下一次应查询的权限域名服务器dns.abc.com的IP地址。

本地域名服务器向权限域名服务器dns.abc.com进行查询。

权限域名服务器dns.abc.com告诉本地域名服务器，所查询的主机的ip地址。

本地域名服务器最后把查询的结果告诉主机m.xyz.com。

**DNS协议的报文格式和发送/响应顺序**



**五、实验内容：**

实验内容主要包括两个部分：第一个部分是关于HTTP协议的验证实验，第二个部分是DNS协议的验证实验。

在HTTP部分，实验包括：

(1)基本的HTTP GET/response交互；

(2) HTTP 条件GET/response交互；

(3) 检索一个大文件；

(4) 请求一个包含多个嵌入对象的文件，观察交互过程。

在DNS部分，主要完成捕获DNS查询包和响应包：

(1) 在浏览器中访问一个网站的，DNS查询包和响应包，分析主要字段的含义；

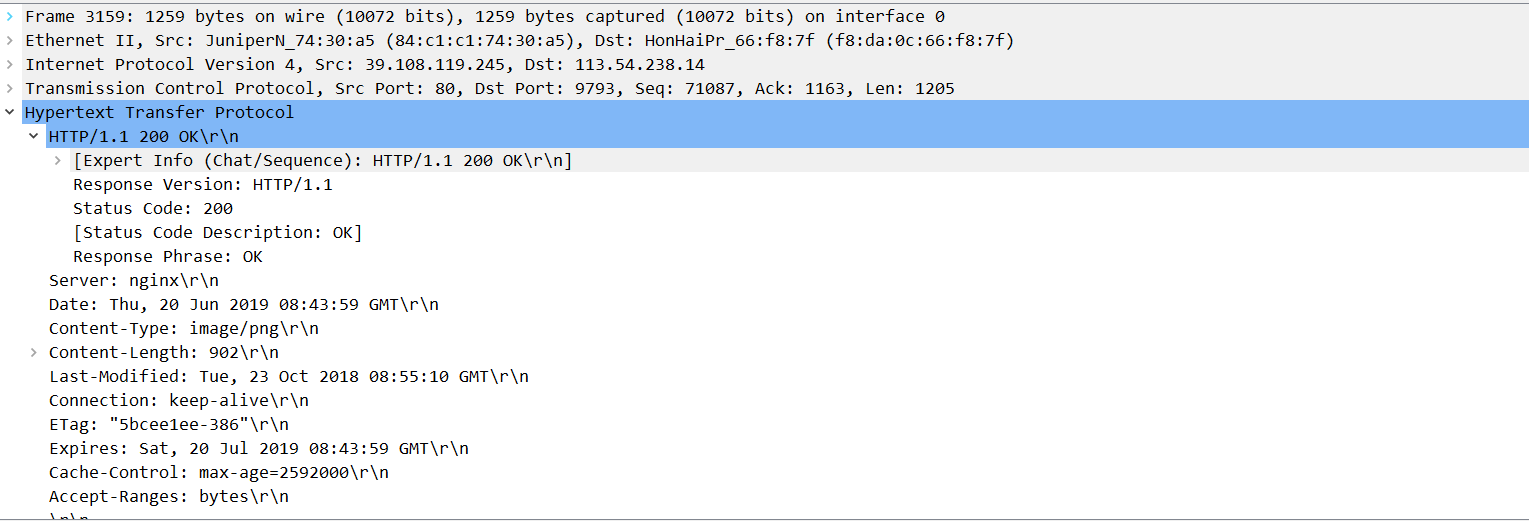
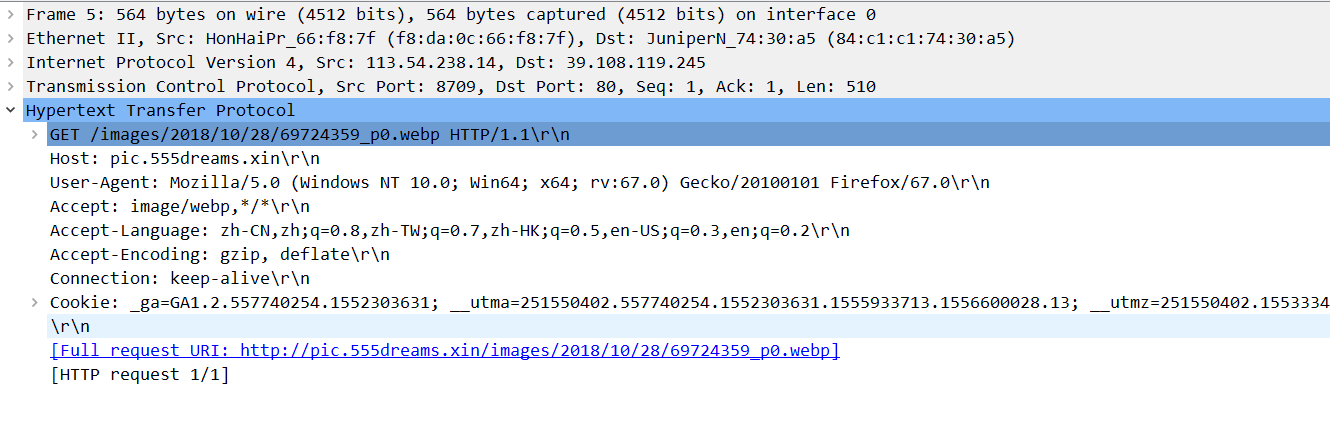
(2) 利用nslookup工具查询DNS地址，捕获DNS查询包和响应包，分析主要字段的含义。

**六、实验器材（设备、元器件）：**

台式机，软件Wireshark

**七、实验步骤：**

**步骤1：完成基本的HTTP GET/response交互实验（访问一个网页）**



贴截图并简单说明

* 你的浏览器运行的是HTTP1.0还是1.1？服务器运行的HTTP协议的版本是哪个版本？

**回答：HTTP 1.1**

* 你的浏览器向服务器指示它能接受的语言是什么？

**回答：**

**zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2**

* 你的主机的IP地址是多少？你访问的服务器的IP地址是多少？

**回答：主机：113.54.238.14 服务器：39.108.119.245**

* 服务器返回给你的浏览器的状态码是多少？表示什么含义？

**回答：200 请求成功**

* 你获取的HTML文件的最近更新时间是多少？

**回答：Tue, 23 Oct 2018 08:55:10 GMT**

* 返回给你的浏览器的内容有多少字节？

**回答：902 bytes**

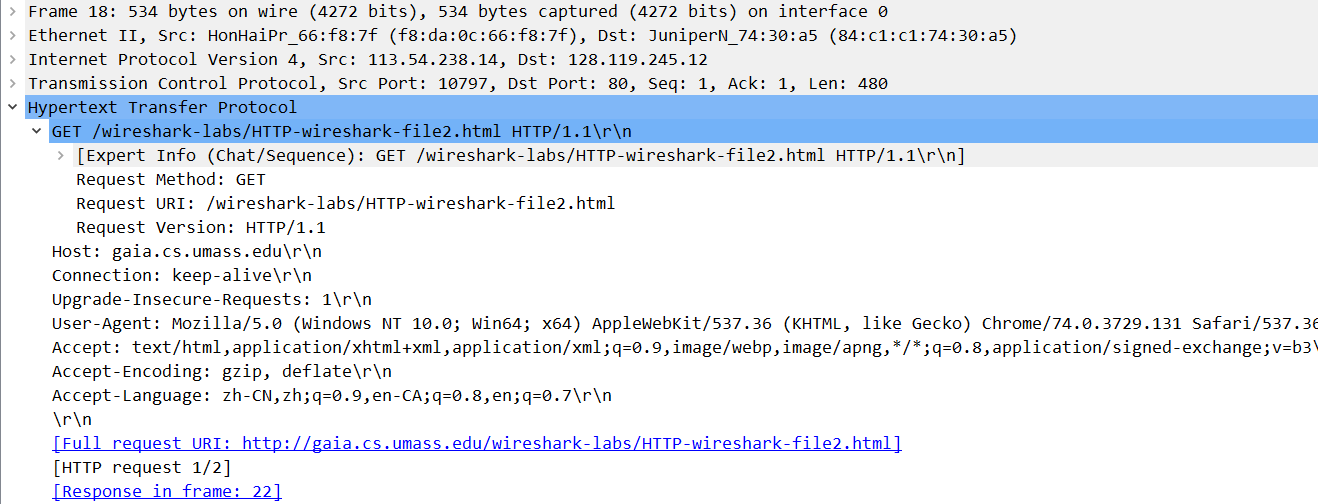
* 通过检查分组内容窗口中的原始数据，可以看到任何数据的头部信息吗？

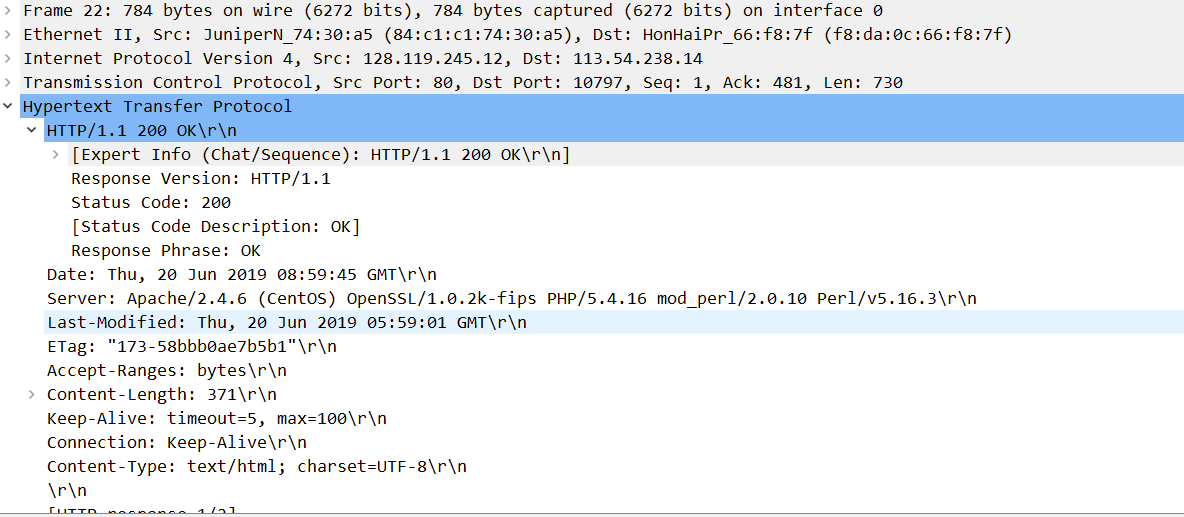
**回答：**

**步骤2：完成HTTP 条件GET/response交互实验**

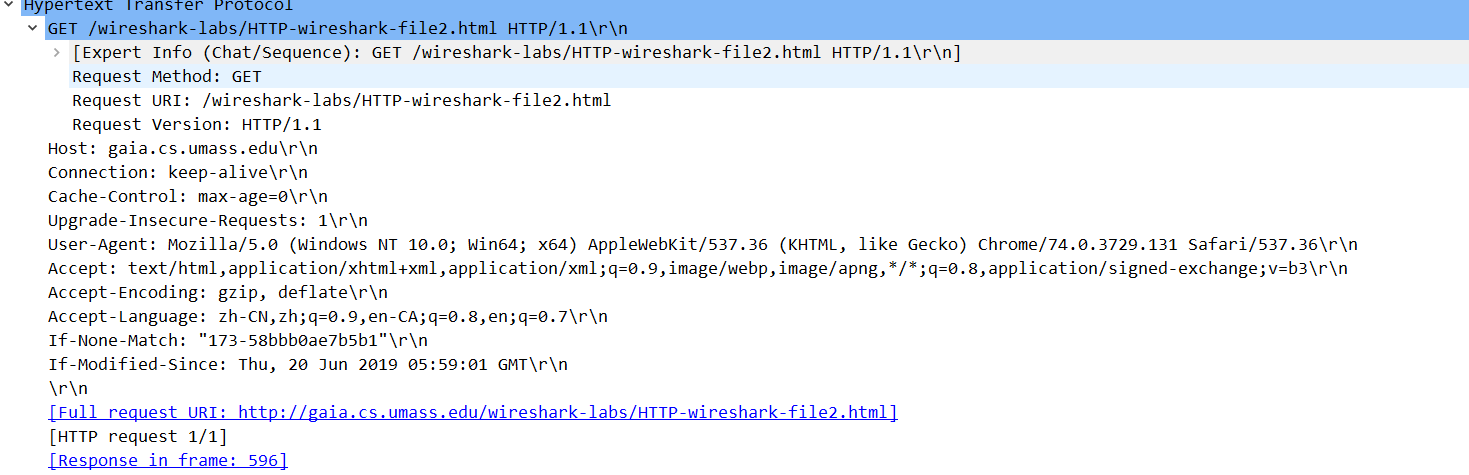
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

第一次：





第二次：



* 检查从浏览器到服务器的第一个HTTP获取请求的内容。你是否看到HTTP GET请求报文中的 “IF-MODIFIED-SINCE”？

**回答： 无**

* 检查服务器响应的内容。服务器是否显式返回文件的内容？你怎么知道？

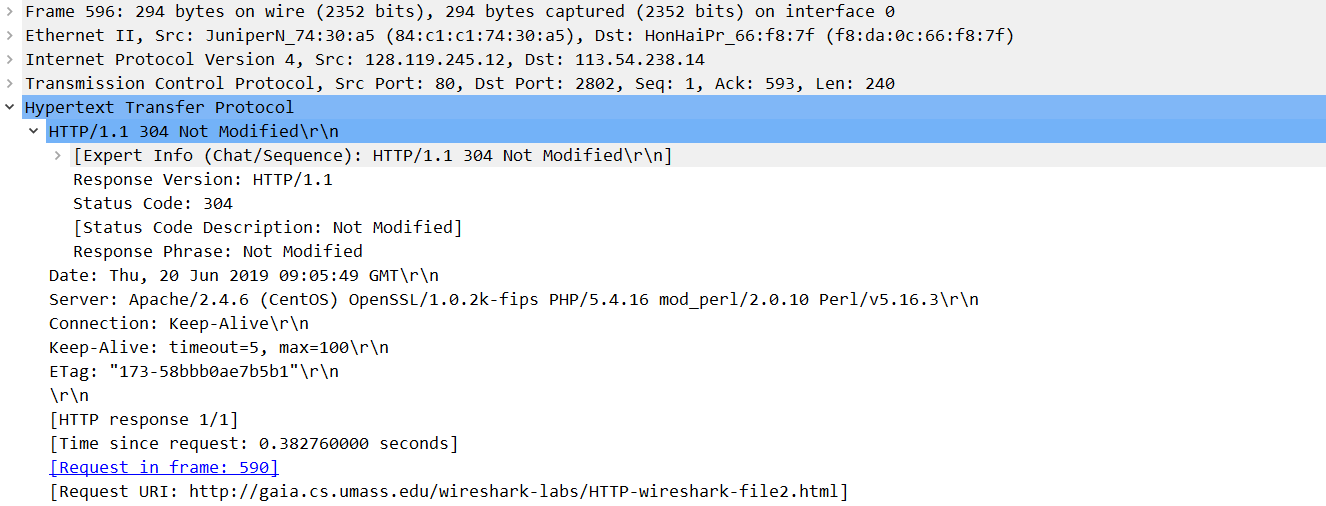
**回答：服务器返回了文件的内容，数据字段有371字节**

* 现在检查从浏览器到服务器的第二个HTTP获取请求的内容。你是否看到了HTTP GET请求报文中的“IF-MODIFIED-SINCE”?如果是，那么“IF-MODIFIED-SINCE”代表了什么？

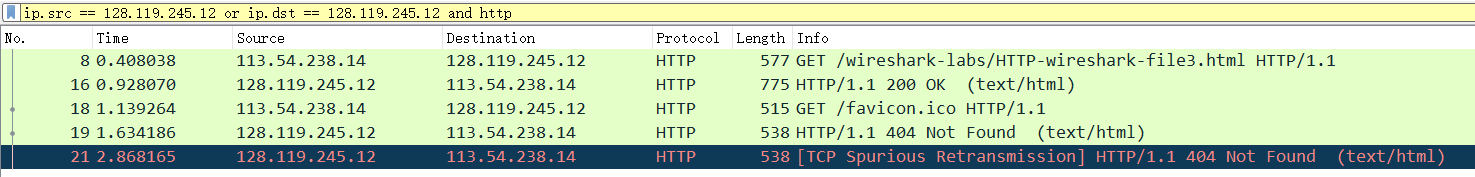
**回答：** **看到了。IF-MODIFIED-SINCE代表最后修改时间，服务器会把这个时间与服务器上实际文件的最后修改时间进行比较，一致则返回304，不一致，返回HTTP状态码200和新的文件内容。**

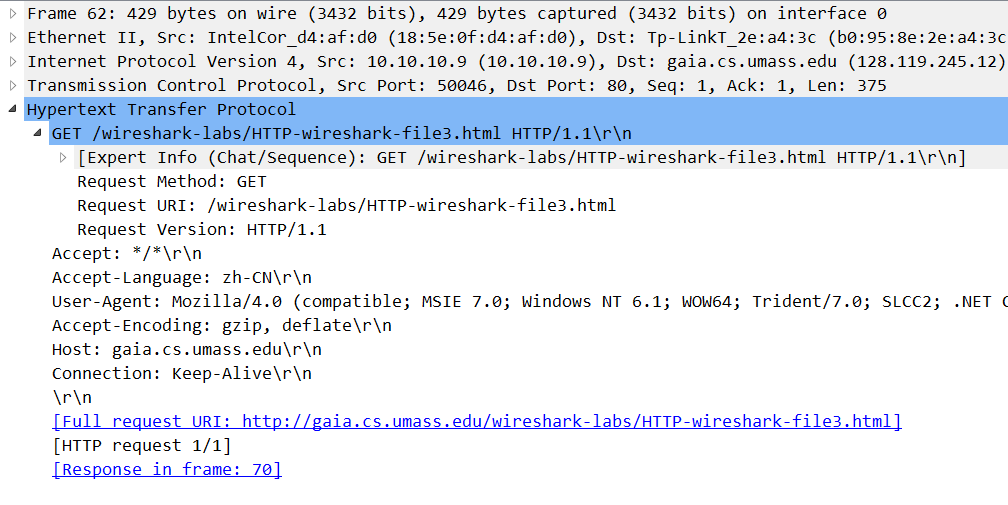
* 响应第二个http请求时从服务器返回的http状态代码和短语是什么？服务器是否显式返回文件的内容？解释。

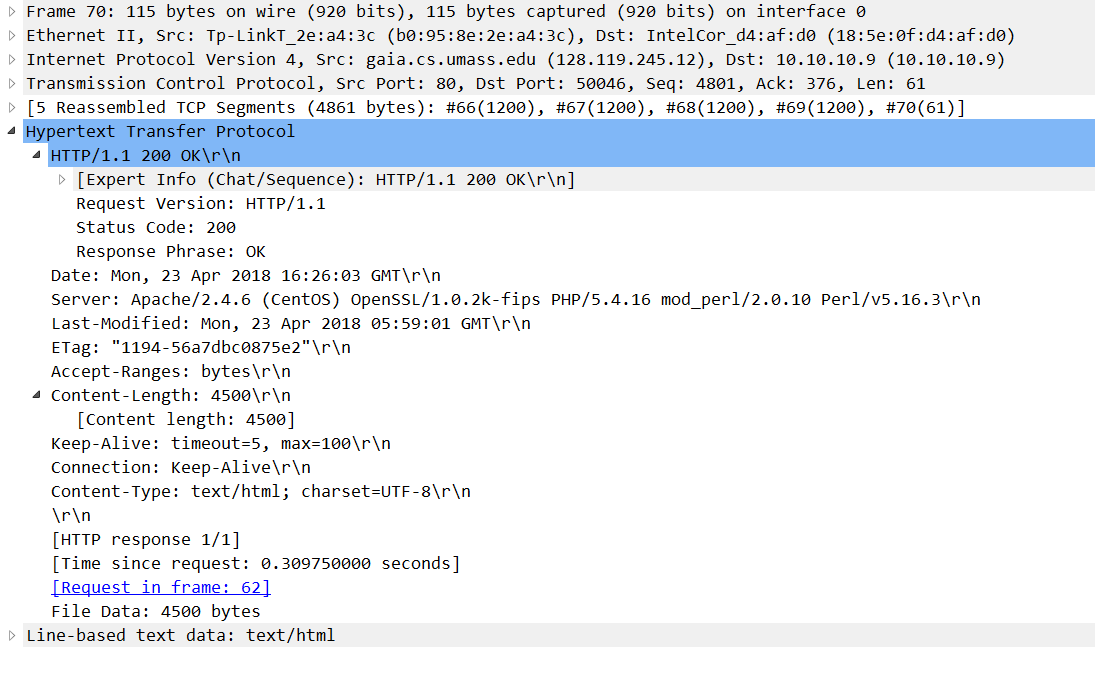
**回答： 304 服务器不返回文件内容，客户端接到之后，就直接把本地缓存文件显示到浏览器中**



**步骤3：完成长文件检索实验**







* How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

**回答：发出1个GET请求 编号8**

* 检查捕获结果，哪个数据包编号包含与HTPP获取请求的响应管理的状态代码和短语？

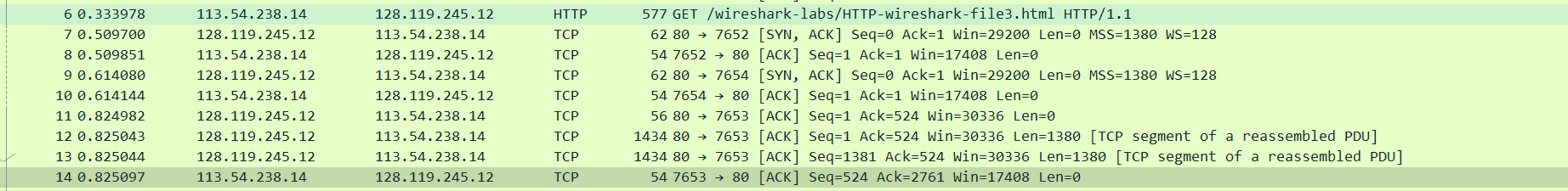
**回答： 编号8**

* 响应中的状态代码和短语是什么？

**回答： Code 200 Phrase OK**

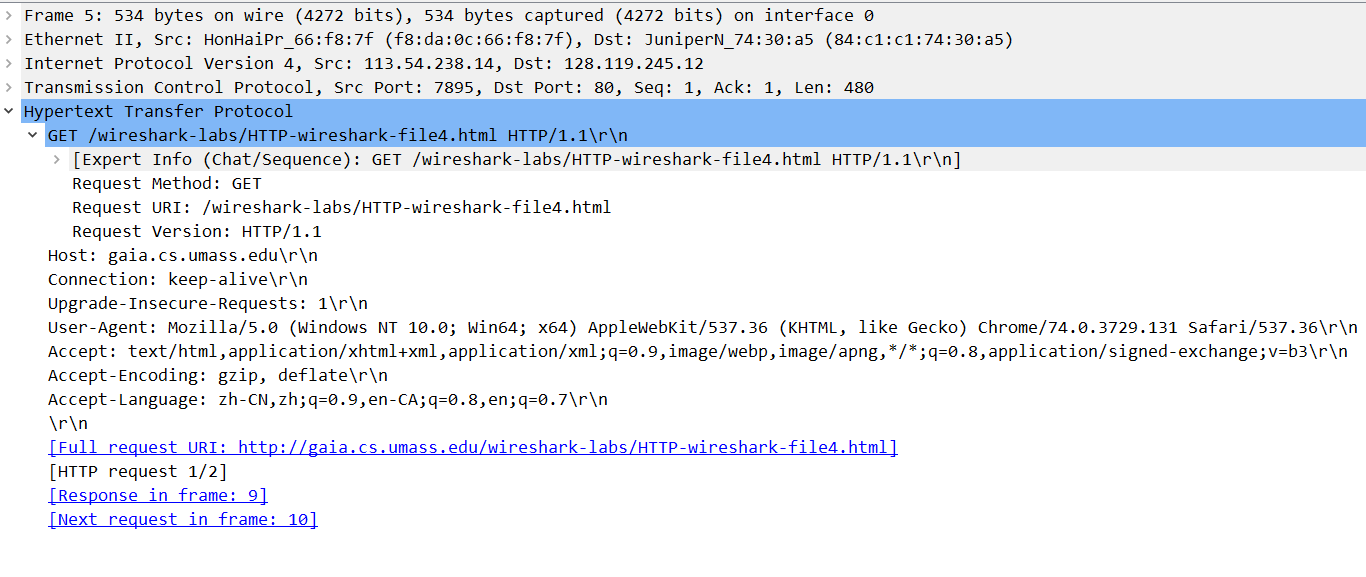
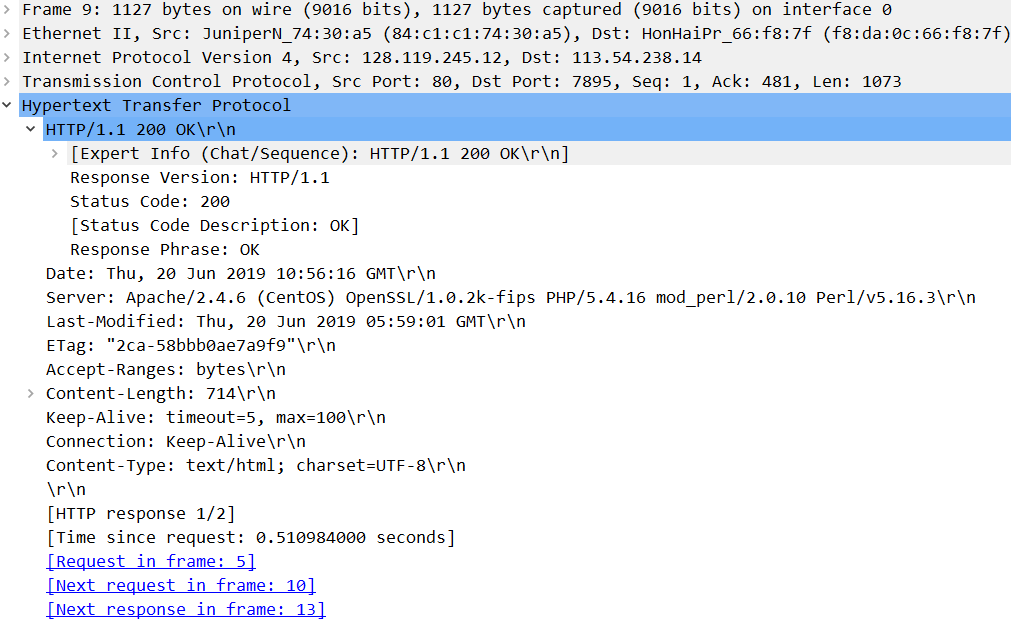
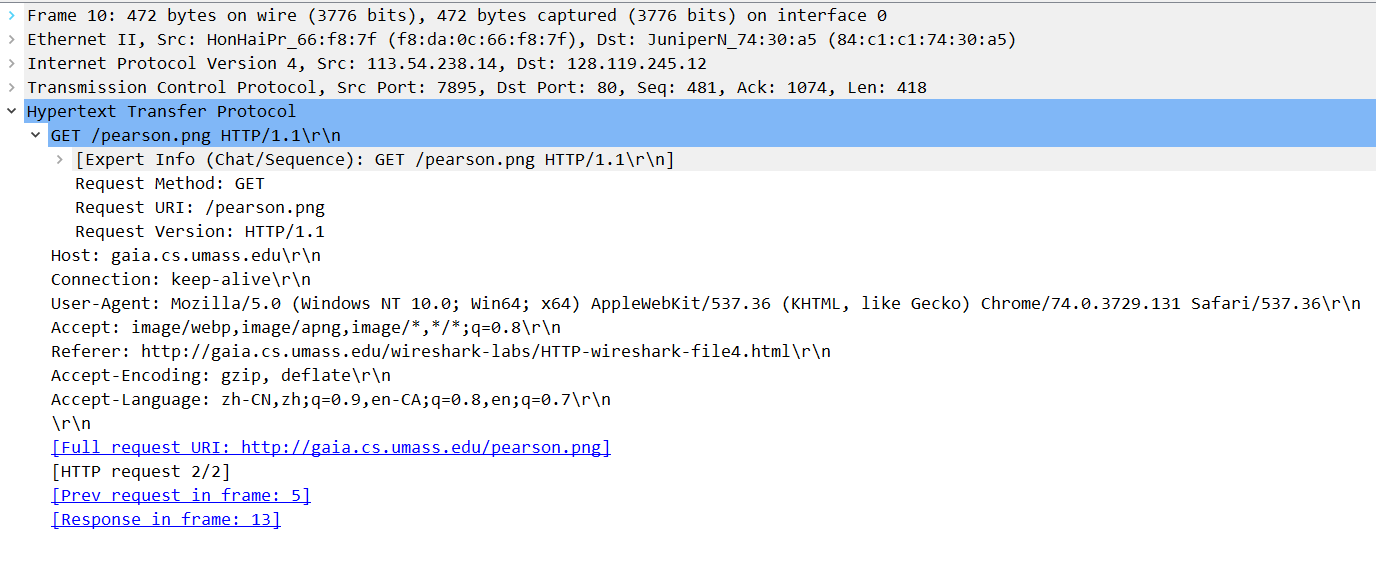
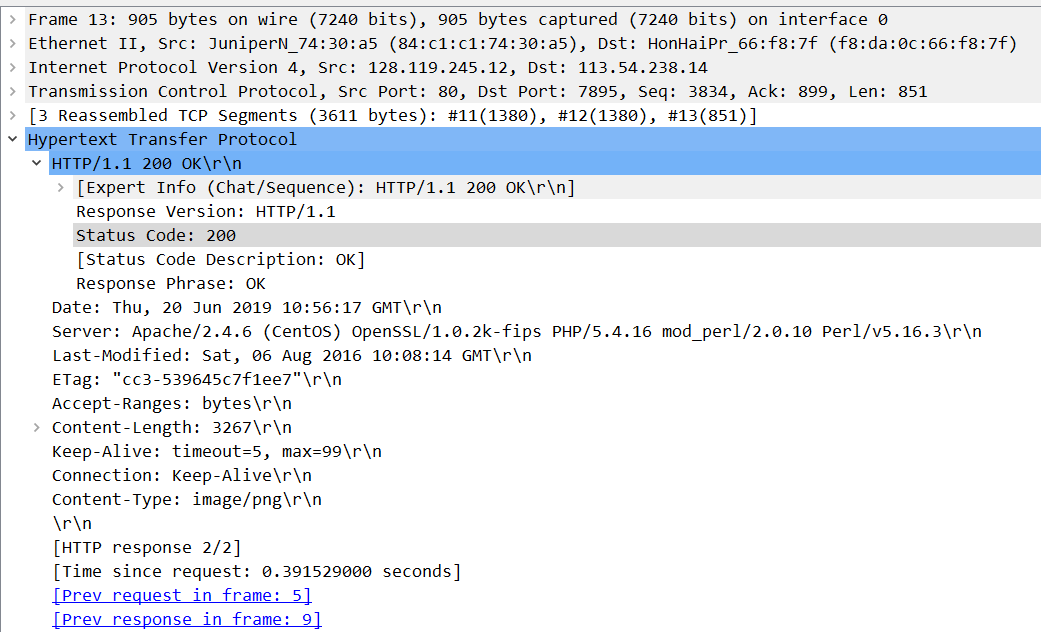
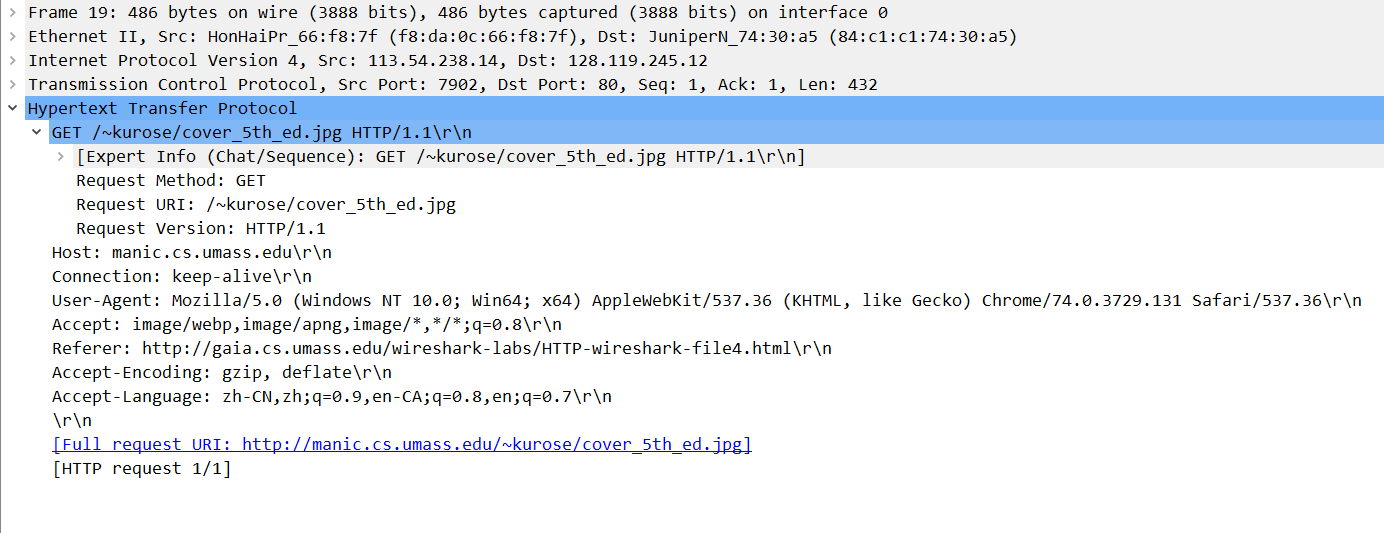
* How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

**回答： 9**



**步骤4：完成有嵌入对象的HTML文件的请求实验**

你的浏览器将展示一个短的HTML文件（这个文件具有2个图片）。在这个基础的HTML文件中引用了2个图片。这就意味着图片本身并不包含在HTML中；在下载的HTML文件中包含了这2个图片的URLs。正如在本书中讨论的，你的浏览器将能够从指定的站定下载这两个图片。发行商的logo将能够从[www.aw-bc.com](http://www.aw-bc.com)站定检索到。第五版的封面是从manic.cs.umass.edu服务器上获取的。

贴截图并简单说明

* 浏览器发送了多少个HTTP GET请求信息? 这些GET请求发送到哪些Internet地址?

**回答：浏览器发送了3个GET请求消息，分别发送到：**

**128.119.245.12（基本的HTML文件）**

**128.119.245.12（公司logo）**

**128.119.240.90（第五版的封面）**

* 你能否回答你的浏览器是否连续下载了两个图像，或者它们是否是从两个web站点并行下载的？说明。

**回答：是先后下载的，不是并行；**

**[待补充，这个包的分析，可能与TCP的各种片段有关]**

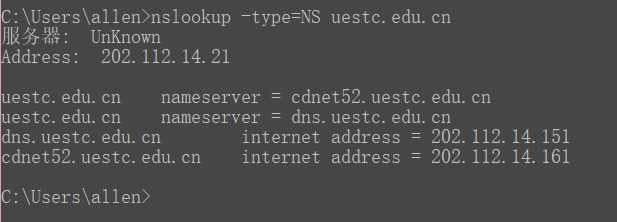
**步骤5：学习nslookup工具，完成以下工作：**

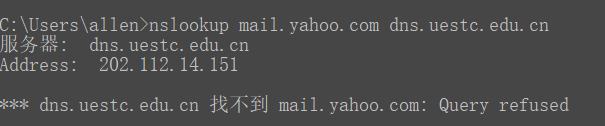
1. 运行nslookup获取亚洲Web服务器的IP地址。该服务器的IP地址是什么?**www.baidu.com的IP地址是119.75.216.20。**

2. 运行nslookup确定中国大学的权威DNS服务器

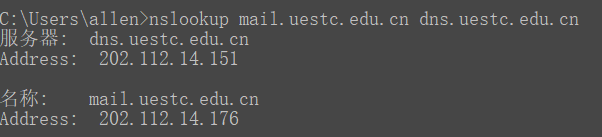
3. 运行nslookup以便为在问题2中获得的DNS服务器的之一来获取雅虎邮件的邮件服务器。它的IP地址是什么？







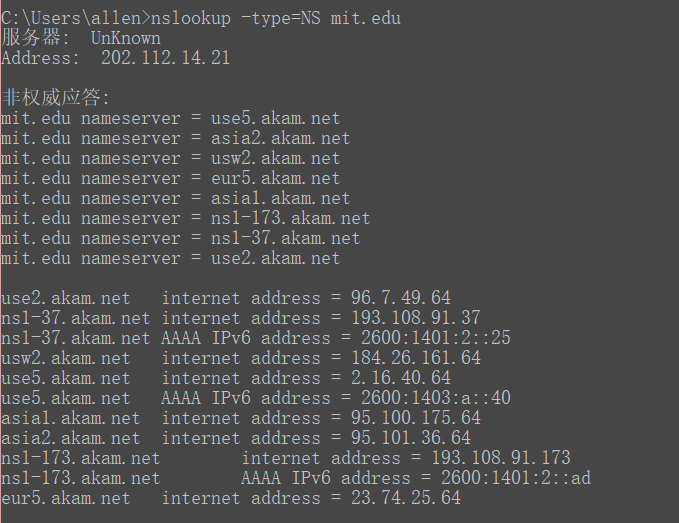
IP地址是209.73.190.12

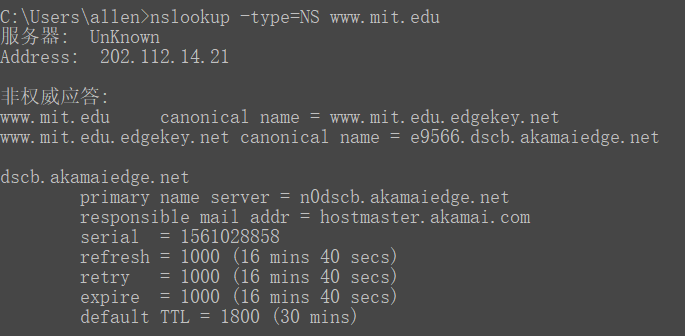


电子科大邮箱的IP地址

参数：–type=NS

含义：查询这个域对应的权威DNS服务器



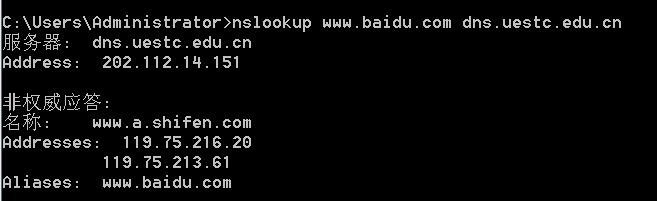


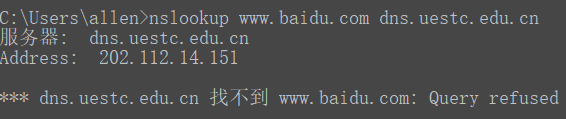
含义是请把主机名为mit.edu的权威DNS发送给我。（当-type选项没有使用时，将查询默认的type A records）

Each of these servers is indeed an authoritative DNS server for the hosts on the MIT campus. However, *nslookup* also indicates that the answer is “non-authoritative,” meaning that this answer came from the cache of some server rather than from an authoritative MIT DNS server. Finally, the answer also includes the IP addresses of the authoritative DNS servers at MIT. (Even though the type-NS query generated by *nslookup* did not explicitly ask for the IP addresses, the local DNS server returned these “for free” and *nslookup* displays the result.)

下面的命令是通过制定的DNS服务器来查询域名对应的IP地址：

nslookup www.baidu.com dns.uestc.edu.cn

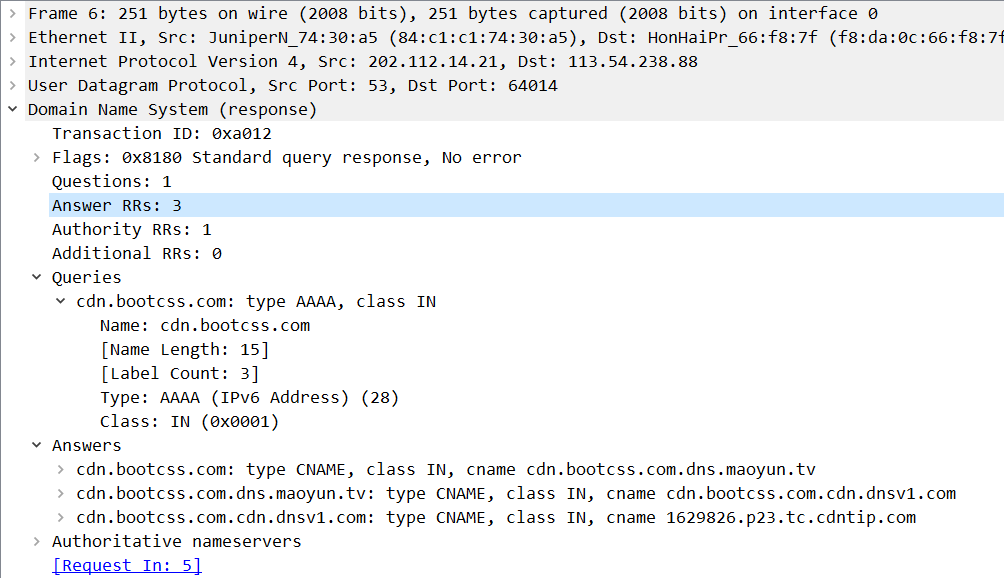
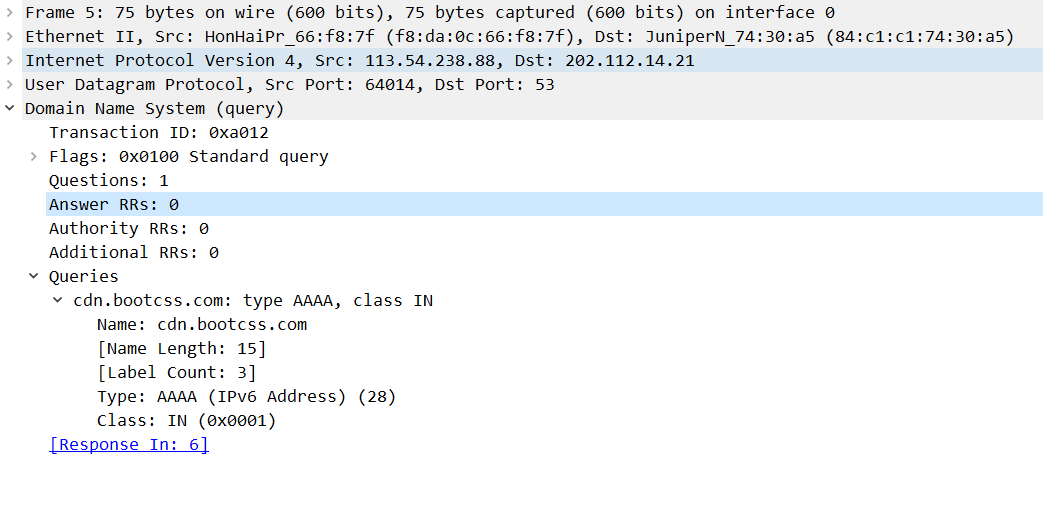




上面的命令是指定使用（电子科技大学的权威域名服务器）来查询百度域名对应的IP地址；

**nslookup –option1 –option2 host-to-find dns-server**

**步骤6：完成通过浏览器访问一个网页的DNS查询/响应包的捕获**



* 找到DNS查询和响应消息。然后找出它是通过UDP或TCP发送的？

**回答： UDP**



* DNS查询消息的目标端口是什么？DNS响应消息的源端口是什么？

**回答：53**



* DNS查询消息是发送到哪个IP地址？使用ipconfig确定本地DNS服务器的IP地址。这两个IP地址是否相同？

**回答： 113.54.238.99 相同**

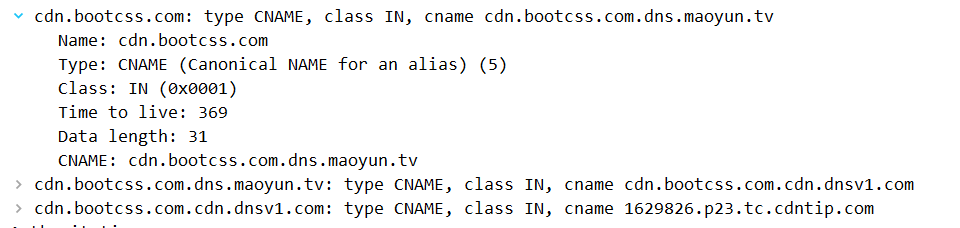


* 检查DNS查询消息。DNS查询的“type”是什么？查询消息是否包含“Answers”？

**回答： AAAA 不包含**

* 检查DNS响应消息。提供了多少“Answers”？每一个“Answer”包含了什么？

**回答：提供了三个Answers，每个Answer包含了**



* 思考由你的主机发送的后续TCP SYN数据包。SYN数据包的目标ip地址是否与DNS响应消息中提供的任何IP地址相对应？

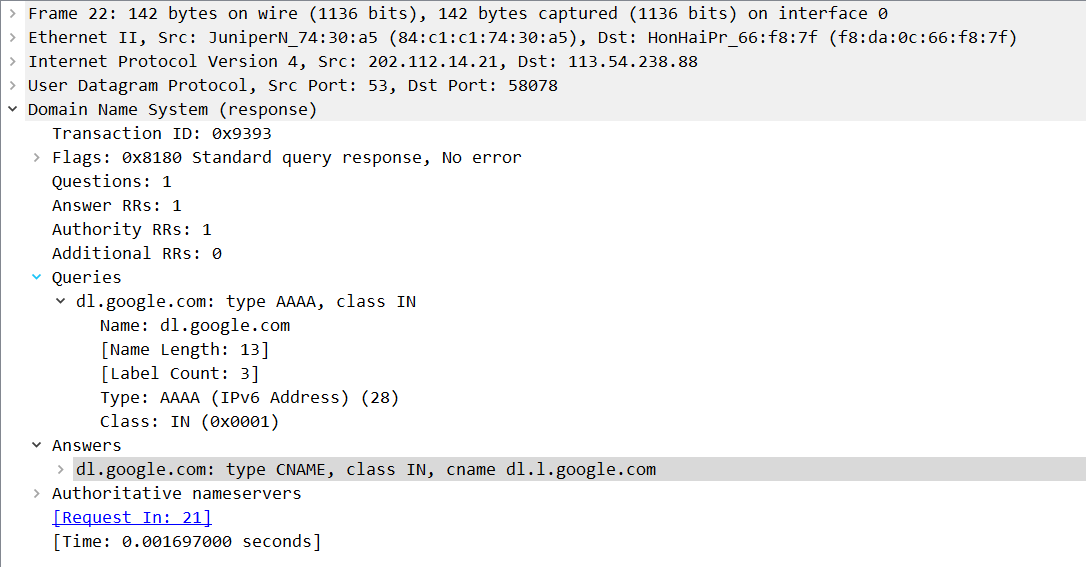
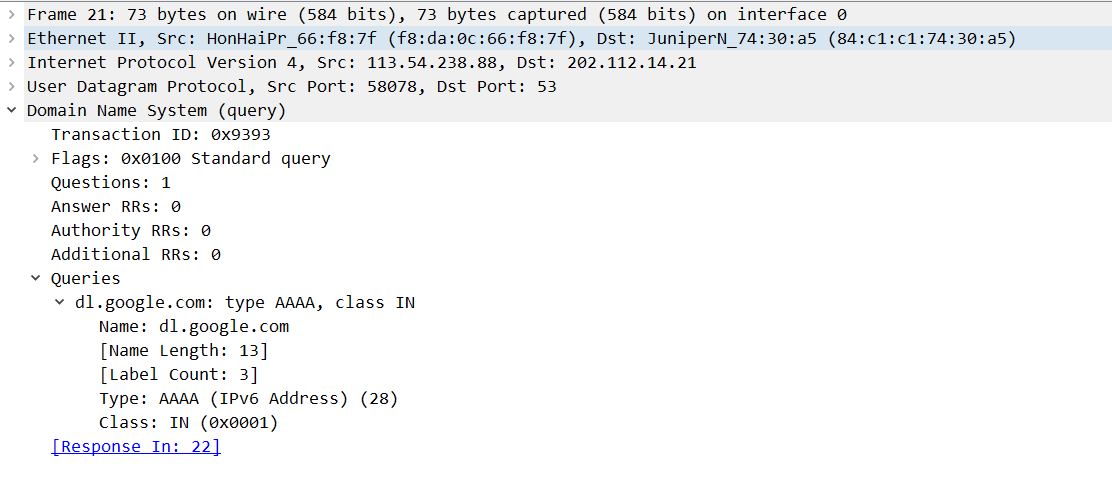
**回答：相对应**

* 此网页包含图像。在检索每一个图像之前，你的主机是否发出新的DNS查询？

**回答：在检索每一个图像之前，如果对象的URL是与前面查询相同的域名，则主机没有发送新的DNS查询，这是因为在本机上有该域名的IP地址缓存；如果对象的URL与前面查询不同的域名，则需要发送新的DNS查询消息。**

**步骤7：利用nslookup工具查询一个域名，捕获DNS查询/响应包**

1. 开始数据包捕获
2. 执行nslookup在 (你自己希望获知的域名)
3. 停止数据包捕获(截图)



* DNS查询消息的目标端口是什么？DNS响应消息的源端口是什么？

**回答：53**

* DNS查询消息是发送给哪个IP地址？这是默认本地DNS服务器的IP地址吗？

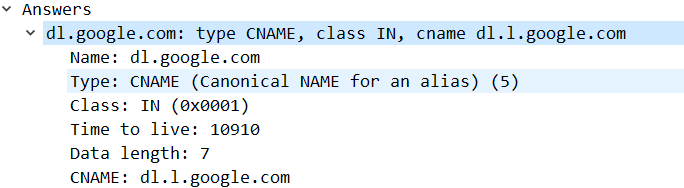
**回答： 113.54.238.99 相同**

* 检查DNS查询消息。DNS查询的“type”是什么？查询消息是否包含“Answers”？

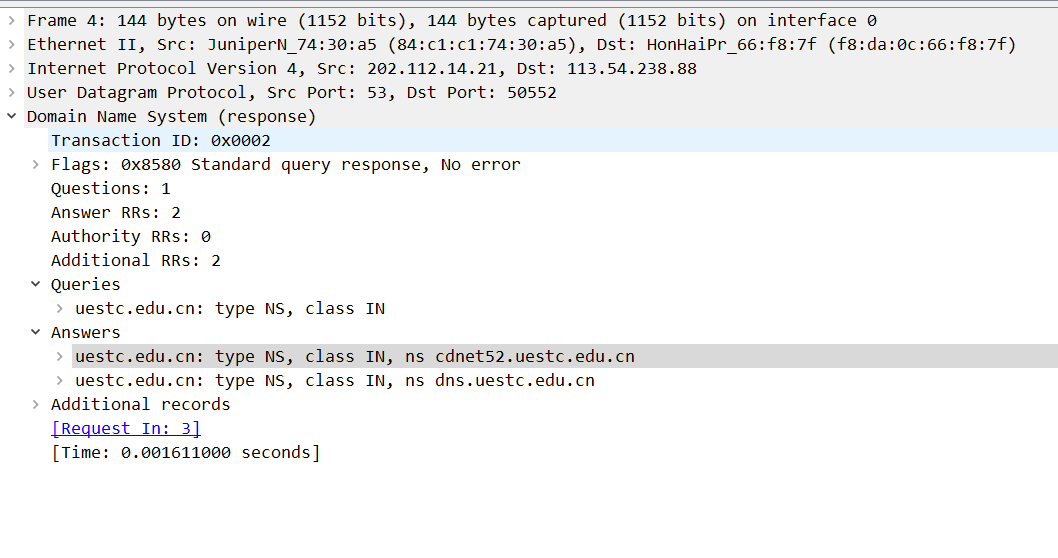
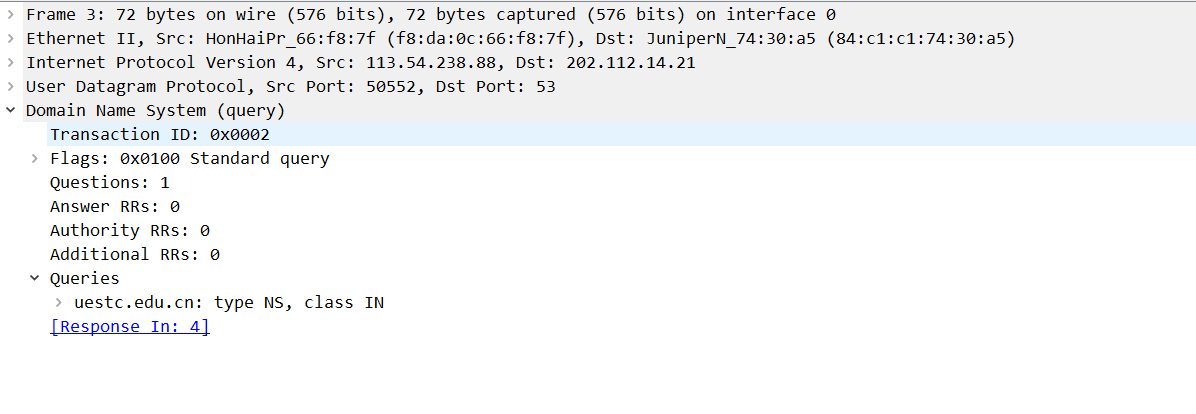
**回答：type是AAAA ，不包含Answers。**

* 检查DNS响应消息，提供了多少“Answers”？每一个“Answer”包含了些什么？

**回答： 1**



**步骤8：利用nslookup工具查询一个域名，捕获DNS查询/响应包**

 DNS查询消息发送的目的IP地址是什么？这是默认本地DNS服务器的IP地址吗？

**回答： 202.112.14.21 不是**

* 检查DNS查询消息。DNS查询的“type”是什么？查询消息是否包含“Answers”？

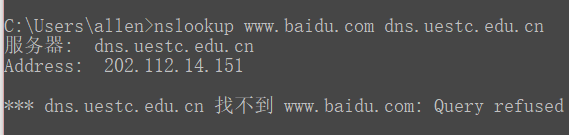
**回答:查询的类型是type为SN，查询消息中不包含Answers；**

* 检查DNS响应消息。响应消息提供了电子科技大学的什么域名？此响应消息是否还提供了电子科技大学域名的IP地址？

**回答：提供了电子科技大学的权威域名服务器，没有提供域名的IP地址。**

步骤7中的第二步改为：nslookup –type=NS uestc.edu.cn

改为：nslookup www.baidu.com dns.uestc.edu.cn



**八、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）**

针对步骤1的结果，回答以下问题：

* 你的浏览器运行的是HTTP1.0还是1.1？服务器运行的HTTP协议的版本是哪个版本？

**回答：HTTP 1.1**

* 你的浏览器向服务器指示它能接受的语言是什么？

**回答：**

**zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2**

* 你的主机的IP地址是多少？你访问的服务器的IP地址是多少？

**回答：主机：113.54.238.14 服务器：39.108.119.245**

* 服务器返回给你的浏览器的状态码是多少？表示什么含义？

**回答：200 请求成功**

* 你获取的HTML文件的最近更新时间是多少？

**回答：Tue, 23 Oct 2018 08:55:10 GMT**

* 返回给你的浏览器的内容有多少字节？

**回答：902 bytes**

* 通过检查分组内容窗口中的原始数据，可以看到任何数据的头部信息吗？

**回答：可以**

针对步骤2的结果，回答以下问题：

* 检查从浏览器到服务器的第一个HTTP获取请求的内容。你是否看到HTTP GET请求报文中的 “IF-MODIFIED-SINCE”？

**回答： 无**

* 检查服务器响应的内容。服务器是否显式返回文件的内容？你怎么知道？

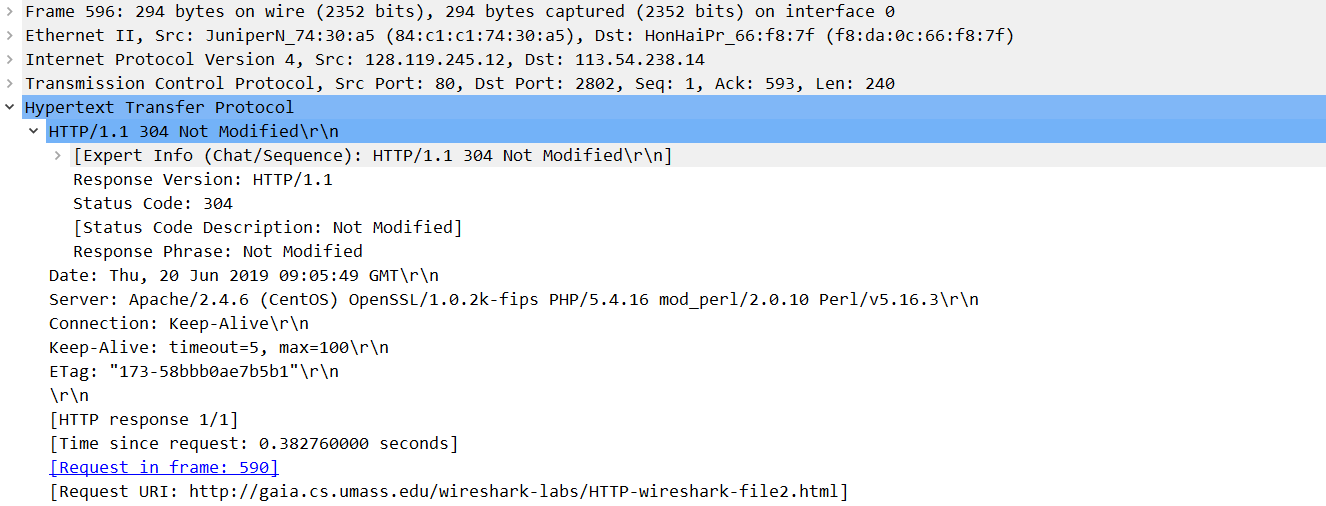
**回答：服务器返回了文件的内容，数据字段有371字节**

* 现在检查从浏览器到服务器的第二个HTTP获取请求的内容。你是否看到了HTTP GET请求报文中的“IF-MODIFIED-SINCE”?如果是，那么“IF-MODIFIED-SINCE”代表了什么？

**回答：** **看到了。IF-MODIFIED-SINCE代表最后修改时间，服务器会把这个时间与服务器上实际文件的最后修改时间进行比较，一致则返回304，不一致，返回HTTP状态码200和新的文件内容。**

* 响应第二个http请求时从服务器返回的http状态代码和短语是什么？服务器是否显式返回文件的内容？解释。

**回答： 304 服务器不返回文件内容，客户端接到之后，就直接把本地缓存文件显示到浏览器中**



针对步骤3的实验结果，回答以下问题：

* How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

**回答：发出1个GET请求 编号8**

* 检查捕获结果，哪个数据包编号包含与HTPP获取请求的响应管理的状态代码和短语？

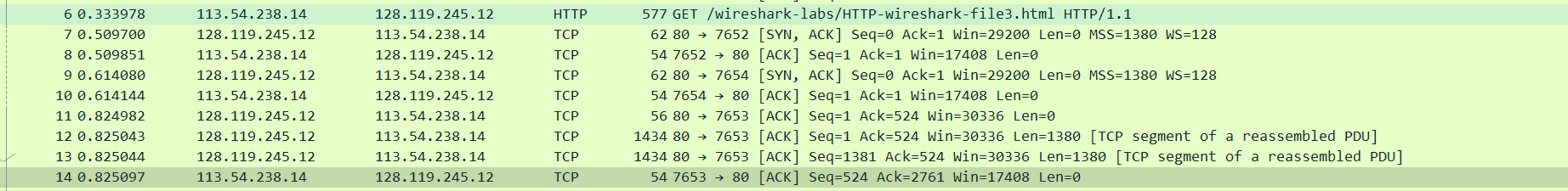
**回答： 编号8**

* 响应中的状态代码和短语是什么？

**回答： Code 200 Phrase OK**

* How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

**回答： 9**



针对步骤4的实验结果，回答以下问题：

* 浏览器发送了多少个HTTP GET请求信息? 这些GET请求发送到哪些Internet地址?

**回答：浏览器发送了3个GET请求消息，分别发送到：**

**128.119.245.12（基本的HTML文件）**

**128.119.245.12（公司logo）**

**128.119.240.90（第五版的封面）**

* 你能否回答你的浏览器是否连续下载了两个图像，或者它们是否是从两个web站点并行下载的？说明。

**回答：是先后下载的，不是并行；**

针对步骤6的实验结果，回答以下问题：

* 找到DNS查询和响应消息。然后找出它是通过UDP或TCP发送的？

**回答： UDP**



* DNS查询消息的目标端口是什么？DNS响应消息的源端口是什么？

**回答：53**



* DNS查询消息是发送到哪个IP地址？使用ipconfig确定本地DNS服务器的IP地址。这两个IP地址是否相同？

**回答： 113.54.238.99 相同**

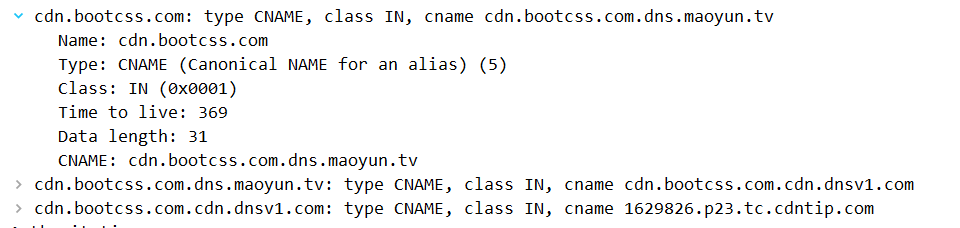


* 检查DNS查询消息。DNS查询的“type”是什么？查询消息是否包含“Answers”？

**回答： AAAA 不包含**

* 检查DNS响应消息。提供了多少“Answers”？每一个“Answer”包含了什么？

**回答：提供了三个Answers，每个Answer包含了**



* 思考由你的主机发送的后续TCP SYN数据包。SYN数据包的目标ip地址是否与DNS响应消息中提供的任何IP地址相对应？

**回答：相对应**

* 此网页包含图像。在检索每一个图像之前，你的主机是否发出新的DNS查询？

**回答：在检索每一个图像之前，如果对象的URL是与前面查询相同的域名，则主机没有发送新的DNS查询，这是因为在本机上有该域名的IP地址缓存；如果对象的URL与前面查询不同的域名，则需要发送新的DNS查询消息。**

针对步骤7的实验结果，回答以下问题：

* DNS查询消息的目标端口是什么？DNS响应消息的源端口是什么？

**回答：53**

* DNS查询消息是发送给哪个IP地址？这是默认本地DNS服务器的IP地址吗？

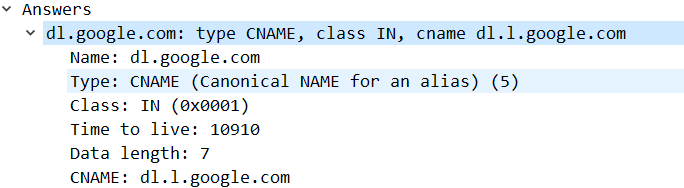
**回答： 113.54.238.99 相同**

* 检查DNS查询消息。DNS查询的“type”是什么？查询消息是否包含“Answers”？

**回答：type是AAAA ，不包含Answers。**

* 检查DNS响应消息，提供了多少“Answers”？每一个“Answer”包含了些什么？

**回答： 1**



针对步骤8的实验结果，回答以下问题：

第一个命令的截图的问题：

**回答： 202.112.14.21 不是**

* 检查DNS查询消息。DNS查询的“type”是什么？查询消息是否包含“Answers”？

**回答:查询的类型是type为SN，查询消息中不包含Answers；**

* 检查DNS响应消息。响应消息提供了电子科技大学的什么域名？此响应消息是否还提供了电子科技大学域名的IP地址？

**回答：提供了电子科技大学的权威域名服务器，没有提供域名的IP地址。**

**九、总结及心得体会：**

本次实验学习了wireshark的基本操作，并通过wireshark回顾并巩固了计算机网络HTTP与DNS的相关知识。在使用wireshark的过程中，可以很直观的参与到真实的计算机网络相关体验，而脱离的单纯的课本学习。实验中也对自己搭设的网站进行了测试，并对HTTP及DNA有了更深的理解。

**十、对本实验过程及方法、手段的改进建议：**

**无**

**报告评分：**

**指导教师签字：**