**Wireshark分析-HTTP协议实验过程**

## 实验一：基本的 HTTP GET/Response 操作

### （1）实验步骤：

①打开浏览器；

②开启 Wireshark，但不开始数据包捕获。在 Wireshark 主窗口顶部的 Filter中输入“ http”，因此只有捕获的 HTTP 消息稍后会显示在数据包列表窗口中；

③等待大约一分钟，然后开始 Wireshark 数据报捕获；

④在浏览器中输入如下地址： **http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html** 浏览器将会显示一个很简单的且只有一行的 HTML 文件；

⑤停止 Wireshark 的数据报捕获。

### （2）回答问题：

Q1.你的浏览器运行的 HTTP 是 1.0 版本还是 1.1 版本？服务器运行 HTTP 是哪个版本？H1.我的浏览器运行的是1.1版本，服务器运行的也是1.1版本。

Q2.你的浏览器能接受服务器的哪些语言？H2.我的浏览器能接受zh-cn和zh等语言。

Q3.你的电脑的 IP 地址是多少？ gaia.cs.umass.edu服务器的 IP 地址是多少？H3.我的IP地址是172.31.192.70，服务器的IP地址是128.119.245.12

Q4.从服务器返回到你的浏览器的状态码是什么？H4.状态码是200.

Q5.什么时候在服务器端得到最后修正的 HTML 文件？H5.2016.7.13 05:59:01

Q6.多少字节的内容已经返回到你的浏览器？H6.Content-Length：128字节。

Q7.除以上已回答过的字段外，头部还有哪些字段？在数据包内容窗口中检查原始数据，是否有未在数据包列表中显示的头部？

H7.HTTP请求报文中还有Host字段、connection字段、Accept字段、User-agent字段、Accept-Encoding字段等。

HTTP响应报文中还有server字段、connection字段等。

截图1：

## 实验二：HTTP GET/Response 有条件的相互作用

### （1）实验步骤：

在开始前先确信你的浏览器缓存是空的，对于 IE 浏览器选择工具-Internet 选项-删除文件，钩选“删除全部文件”从你的浏览器中移除缓存的文件，然后点击确定按钮。现在按以下步骤做：

①打开 Wireshark，开始数据包捕获。

②在你的浏览器中输入如下的 URL 地址： <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

浏览器将会显示一个很简单的 5 行的 HTML 文件；

③快速地在你的浏览器中再次输入相同的 URL（或者点一下刷新）；

④停止 Wireshark 数据包捕获，在在 Wireshark 主窗口顶部的 Filter 中输入“ http”，因此只有捕获的 HTTP 消息稍后将会显示在数据包列表窗口中。

得到如下数据报：

红框中的数据正是我们要获取的,即两次HTTP的请求和响应。

截图:2

### （2）回答问题：

Q8.从你的浏览器到服务器得到的请求中检查第一个 HTTP GET 的内容。在 HTTP GET中你有没有看到一行“ IF-MODIFIED-SINCE” ?为什么？H8.没有这行，因为这是浏览器首次获取该页面。

Q9.检查服务器回应内容，服务器明确地返回了文件的内容吗？你怎样断定？H9.明确返回了。从line-based text data中的数据可以看出。

Q10.现在从你的浏览器到服务器得到的请求中检查第二个 HTTP GET 的内容。 在 HTTP GET 中你有没有看到一行“ IF-MODIFIED-SINCE” ?如果有，在“ IF-MODIFIED-SINCE”头部有什么信息？H10.有这行字段。信息为上次访问该网址的时间。

Q11.第二次 HTTP 返回的状态码是多少？从服务器返回的响应第二个 HTTP GET 的短语是什么？服务器明确地返回了文件的内容吗？为什么？

H11.状态码是304，短语是Not Modified，并没有明确返回文件内容，因为该网页内容在上次访问之后未被修改过，且本浏览器中有上次访问的缓存。

## 实验三：得到较长的文档

### （1）实验步骤：

在前面实验得到的文档是简单和短小的 HTML 文件， 让我们来看看下载一个长的 HTML文件时会出现什么。按以下要求做：

①打开你的浏览器，确信你的浏览器缓存是空的，就如上面讨论的；

②打开 Wireshark，开始数据包捕获；

③在你的浏览器中输入如下的 URL 地址： **http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html** 你的浏览器将会显示相当长的美国权利法案；

④停止 Wireshark 数据包捕获，在 Filter 栏输入“ http”，因此只有捕获的 HTTP 消息稍后将会显示在数据包列表窗口中。

### （2）回答问题：

Q12.你的浏览器发送了多少个HTTP GET请求消息？H12.1个。

Q13．传输这一个HTTP响应需要多少个TCP数据段？

H13.4个TCP数据段。

Q14.响应HTTP GET请求的相关的状态码和短语是什么？H14.200 OK.

Q15．在TCP“Continuation”附加关联的传输数据中有没有HTTP状态码和短语？H15.？截图3：

## 实验四：带有内嵌对象的HTML文档

### （1）实验步骤：

①打开浏览器，确信你的浏览器缓存是空的，就如上面讨论的；

②打开 Wireshark Network Analyzer，开始数据包捕获；

③在你的浏览器中输入如下的 URL 地址： **http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html**

④停止 Wireshark 数据包捕获，在 Filter 窗口中输入“ http”，因此只有捕获的 HTTP 消息稍后将会显示在数据包列表窗口中。

### （2）回答问题：

Q16. 你的浏览器发送了多少个HTTP GET请求消息？这些GET请求发送到哪些IP地址？

H16. 截图:4

Q17．你的浏览器是否同时下载这两张图片（并发的从两个网站上下载图片）？你是如何判断的？

H17.不是并发下载的，是先后请求先后到达的。

## 实验五：HTTP认证

### （1）实验步骤：

①确信你的浏览器缓存是空的，就如上面讨论的。关闭你的浏览器，然后再打开；

②打开 Wireshark Network Analyzer，开始数据包捕获；

③在你的浏览器中输入如下的 URL 地址： **http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html** 在出现的对话框中输入用户名和密码，用户名是“wireshark-students”，密码是“network”；

④停止Wireshark 数据包捕获，在Filter窗口中输入“ http”，因此只有捕获的HTTP消息稍后将会显示在数据包列表窗口中。

### （2）回答问题：

Q18．服务器对起初的HTTP GET消息的响应（状态码和短语）是什么？与前一部分实验相比，在这个响应消息中出现了什么新的字段？H18. 401 Authorization Required，出现了www-Authenticate字段。

Q19．当你的浏览器第二次发送HTTP GET消息时，有什么新的字段被包含在HTTP GET消息中？对应的服务器响应有没有新的字段出现？H19. GET消息中出现了新的Authorization字段。服务器响应出现了ETag字段。

Q20．当你的浏览器第三次发送HTTP GET消息时， 有什么新的字段被包含在HTTP GET消息中？当你输入正确的用户名和密码后，服务器给出的响应是什么？H20. HTTP request字段。响应页面截图：5