天 津 商 业 大 学 学 生 实 验 报 告

开课实验室：现代信息交流中心 403　　开课时间：2014 年 12 月 16 日　　实验报告：2014 年 12 月 16 日

学院名称	信息工程学院	年级、专业、班	软件工程 1201	学号	20125041	姓名	王靖伟	同组姓名	无
课程名称	Computer Networks and Internets	实验项目名称	应用层协议实验			指导教师		尉斌	
实验类型	验证 ■	综合 □	设计 □	创新 □				成绩	
教师评语	教师签名： 年　月　日								

实验报告内容一般包括以下几个内容：1、目的要求　2、仪器用具及材料（仪器名称及主要规格、用具名称）　3、实验内容及原理（简单但要抓住要点，写出依据原理）　4、操作方法与实验步骤　5、数据图表格（照片）　6、实验过程原始记录　7 数据处理及结果（按实验要求处理数据、结论）　8、作业题　9、讨论（对实验中存在的问题、进一步的想法等进行讨论）

实验报告内容：

1）实验目的：①熟悉应用层协议的内容和功能；

②掌握应用层协议的使用方法

2）实验要求：①掌握 HTTP 的功能和使用方法

②掌握与该协议相关的工具操作方法

3）实验设备：协议服务器（利用已有的网络服务器）；协议客户端软件

4）实验过程：

① 应用协议的功能

② 客户端软件的配置与操作

③ 回答课后问题（需详细阐述，注明题号和问题）

5）实验心得

注 1.每个实验项目一份实验报告。2.实验报告第一页学生必须使用规定的实验报告纸书写，附页用实验报告附页纸或 A4 纸书写，字迹工整，曲线要画在坐标纸上，线路图要整齐、清楚（不得徒手画）。3. 实验教师必须对每份实验报告进行批改，用红笔指出实验报告中的错、漏之处，并给出评语、成绩，签全名、注明日期。 4.待实验课程结束以后，要求学生把实验报告整理好，交给实验指导教师，加上实验课学生考勤及成绩登记表（见附件 2）、目录和学院统一的封面（见附件 3）后，统一装订成册存档。

天津商业大学学生实验报告附页

开课实验室：现代信息交流中心 403　　开课时间：2014 年 12 月 16 日　　实验报告：2014 年 12 月 16 日

根据文件 httpWebBrowsing.cap 回答下列问题。

（1）跟踪我们的 Web 浏览器和 www.google.com Web 服务器之间的 TCP 数据流，分离出浏览器发出的请求，并将文本复制下来。

```
GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.5) Gecko/20031007
Accept:text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q
=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PREF=ID=2922596a77b005c7:TM=1073520455:LM=1073520455:S=Ycw7Yx3HeW-XOndK
```

```
GET /images/logo.gif HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.5) Gecko/20031007
Accept: image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.google.com/
Cookie: PREF=ID=2922596a77b005c7:TM=1073520455:LM=1073520455:S=Ycw7Yx3HeW-XOndK
```

（2）跟踪我们的 Web 浏览器和 www.gnu.org Web 服务器之间的第一个 TCP 数据流，用你喜欢的编辑器将服务器第一次响应的 HTML 源代码复制出来，保存为 foo.html，并用 Web 浏览器打开它，如图 1 所示。用什么方法使它看起来像 www.gnu.org 的主页？遗漏了什么？为什么？

遗漏了图片,因为复制出来的源代码只有文本信息，没有图片，所以显示不出来。

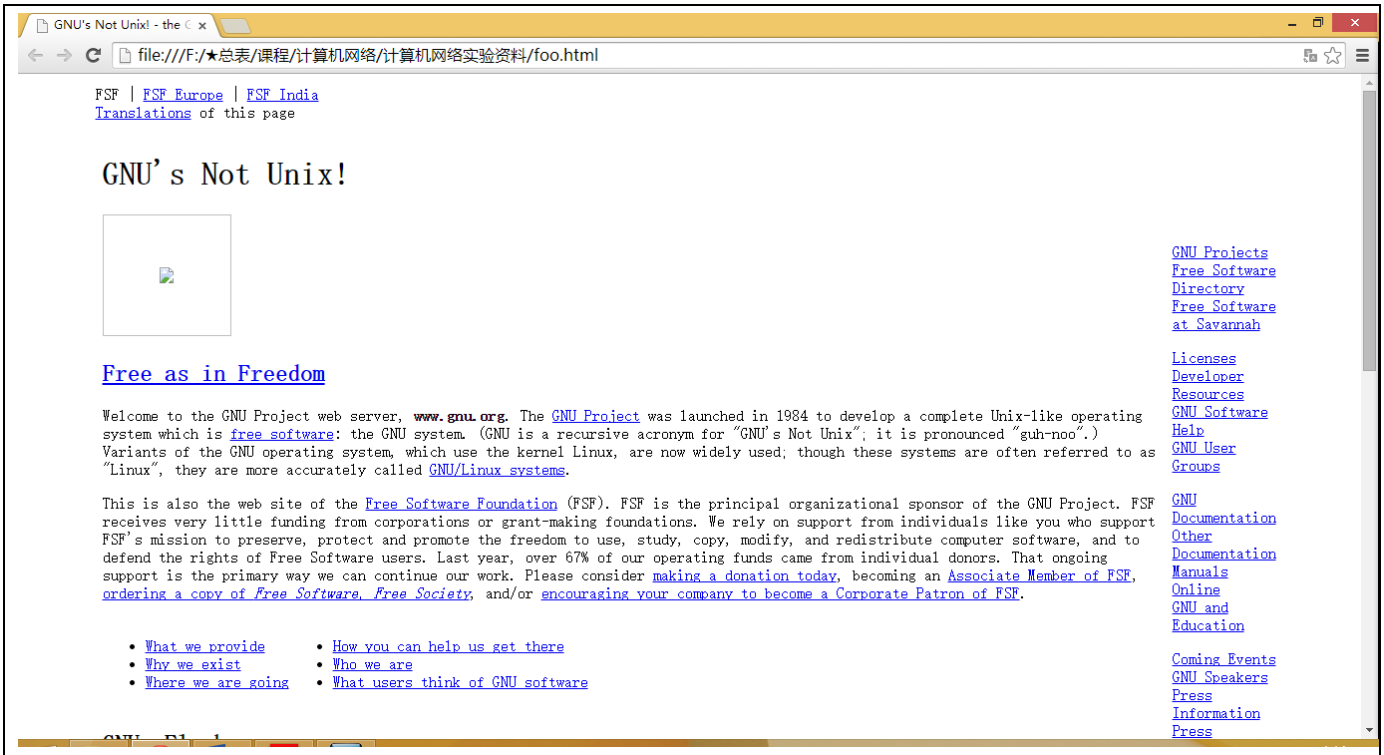


图 1. 用浏览器打开 foo.html

(3)分别写出突出显示跟踪记录中全部 HTTP 请求和只突出显示 HTTP 响应的颜色过滤器，每个过滤器使用什么字符串？

显示跟踪记录中全部 HTTP 请求颜色过滤器，如图 2 所示。过滤结果如图 3 所示。

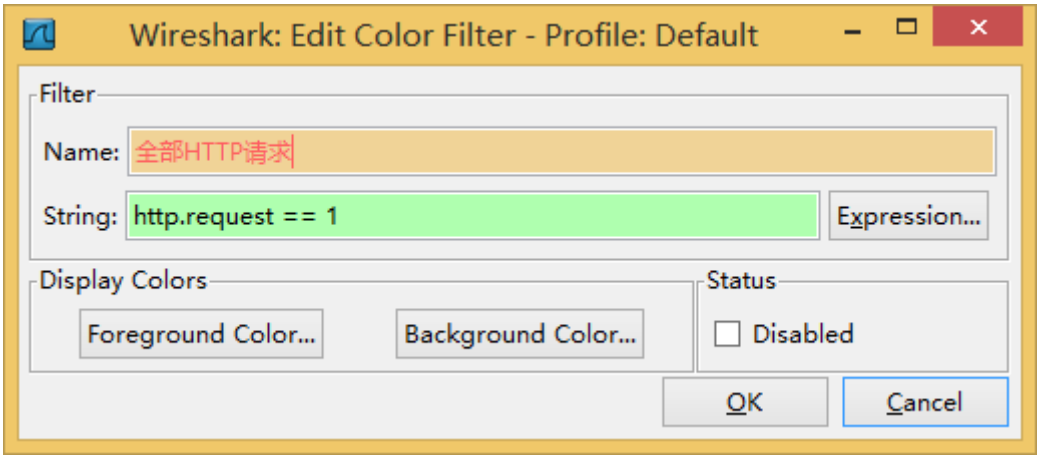


图 2. 显示跟踪记录中全部 HTTP 请求颜色过滤器

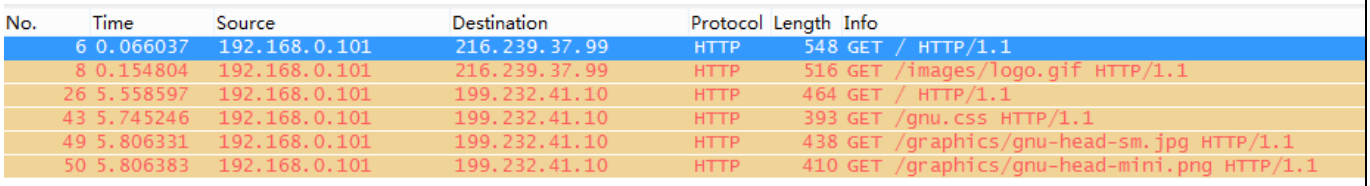


图 3. 全部 HTTP 请求结果

只突出显示 HTTP 响应的颜色过滤器，如图 4 所示。过滤结果如图 5 所示。

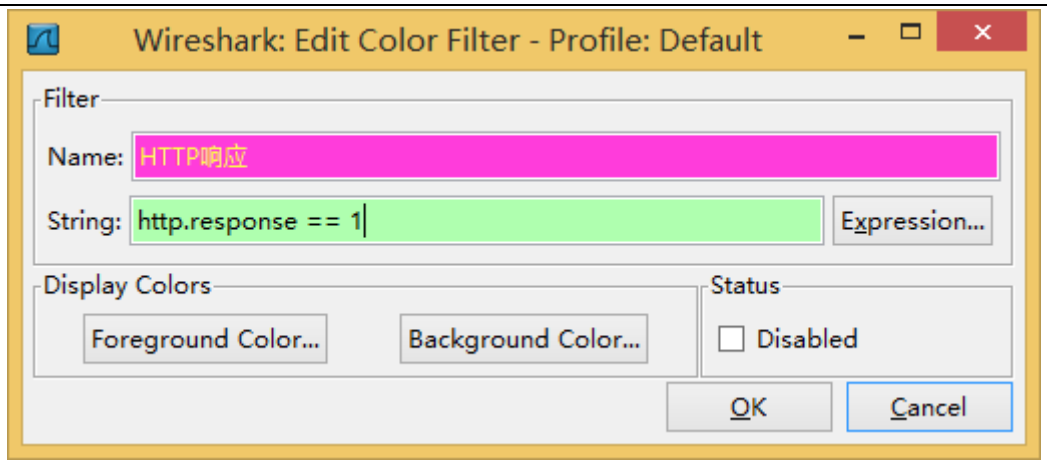


图 4. 只突出显示 HTTP 响应的颜色过滤器

No.	Time	Source	Destination	Protocol	Length	Info
7	0.110624	216.239.37.99	192.168.0.101	HTTP	1438	HTTP/1.1 200 OK (text/html)
19	0.231138	216.239.37.99	192.168.0.101	HTTP	218	HTTP/1.1 200 OK (GIF89a)
44	5.752849	199.232.41.10	192.168.0.101	HTTP	1381	HTTP/1.1 200 OK (text/html)
47	5.791381	199.232.41.10	192.168.0.101	HTTP	197	HTTP/1.1 200 OK (text/css)
55	5.855740	199.232.41.10	192.168.0.101	HTTP	825	HTTP/1.1 200 OK (PNG)
56	5.895037	199.232.41.10	192.168.0.101	HTTP	1296	HTTP/1.1 200 OK (JPEG JFIF image)

图 5. 全部 HTTP 响应结果

（4）发送到 www.gnu.org 的 HTTP 请求有几次，每次请求的是哪些对象，每个对象有多大？你是怎么知道的？

发送到 www.gnu.org 的 HTTP 请求有 4 次，如图 6 所示。

26	5.558597	192.168.0.101	199.232.41.10	HTTP	464 GET / HTTP/1.1
43	5.745246	192.168.0.101	199.232.41.10	HTTP	393 GET /gnu.css HTTP/1.1
49	5.806331	192.168.0.101	199.232.41.10	HTTP	438 GET /graphics/gnu-head-sm.jpg HTTP/1.1
50	5.806383	192.168.0.101	199.232.41.10	HTTP	410 GET /graphics/gnu-head-mini.png HTTP/1.1

图 6. 发送到 www.gnu.org 的 HTTP 请求

第一次请求 Web 页面，第二次请求/gnu.css，第三次请求/graphics/gnu-head-sm.jpg，第四次请求/graphics/gnu-head-mini.png。

我是通过过滤器过滤，然后查看报文得知。

（5）这些请求中哪些是来自于端口 3841 的连接，有几个是来自于端口 3842 的连接？

通过编写过滤器发现，分组 26、分组 50 是来自端口 3841 的请求连接，如图 7 所示。

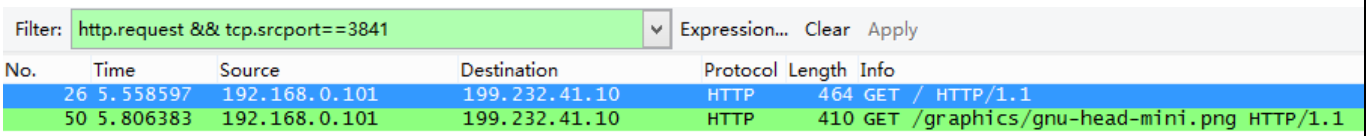


图 7. 来自端口 3841 的请求连接

通过编写过滤器发现，分组 43、分组 49 是来自端口 3842 的请求连接，如图 8 所示。

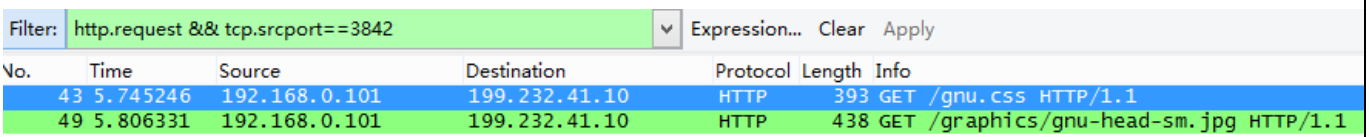


图 8. 来自端口 3842 的请求连接

（6）我们看到的所有被传送对象是否都是 HTML 页？Web 浏览器是如何知道一个数据应该被解释为 HTML 或是其它类型的文件。

我们看到的所有被传送对象是不一定都是 HTML 页，也有像图片.jpg、.png、.gif 这样的类型文件。

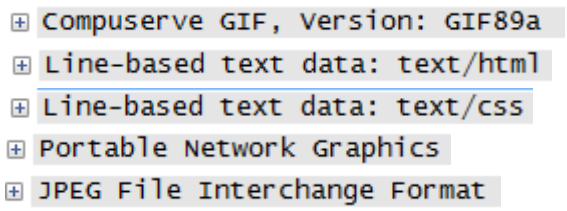
请求后应答的报文会回复类型，“ontent-Type: image/gif”这就是解释为 gif 图片，“Content-Type: text/html”这就被解释为 HTML 页。

（7）列出你在所有请求中找到的不同首部。是否看到了我们在实验中未看到的一些首部类型？如果有，是哪些？

有一个 HTTP 首部就再没有发现其他的不同的首部了。

（8）列出你在所有响应中找到的不同首部类型。你是否看到了我们在实验中未看到的一些首部类型？如果有，是哪些？

发现如下的不同首部类型：



（9）计算 www.google.com 和 www.gnu.org 的平均响应时间。哪个服务器响应时间最短？请描述你是如何计算的。

计算方法为：Σ（响应时间-请求时间）/次数

如图 9 所示，计算 google.com 的平均响应时间。

6	0.066037	192.168.0.101	216.239.37.99	HTTP	548 GET / HTTP/1.1
7	0.110624	216.239.37.99	192.168.0.101	HTTP	1438 HTTP/1.1 200 OK (text/html)
8	0.154804	192.168.0.101	216.239.37.99	HTTP	516 GET /images/logo.gif HTTP/1.1
19	0.231138	216.239.37.99	192.168.0.101	HTTP	218 HTTP/1.1 200 OK (GIF89a)

图 9.google.com 请求响应报文

计算为[（0.110624-0.066037）+（0.231138-0.154804）]/2=0.06046s

如图 10 所示，计算 gun.org 的平均响应时间。

26	5.558597	192.168.0.101	199.232.41.10	HTTP	464 GET / HTTP/1.1
43	5.745246	192.168.0.101	199.232.41.10	HTTP	393 GET /gnu.css HTTP/1.1
44	5.752849	199.232.41.10	192.168.0.101	HTTP	1381 HTTP/1.1 200 OK (text/html)
47	5.791381	199.232.41.10	192.168.0.101	HTTP	197 HTTP/1.1 200 OK (text/css)
49	5.806331	192.168.0.101	199.232.41.10	HTTP	438 GET /graphics/gnu-head-sm.jpg HTTP/1.1
50	5.806383	192.168.0.101	199.232.41.10	HTTP	410 GET /graphics/gnu-head-mini.png HTTP/1.1
55	5.855740	199.232.41.10	192.168.0.101	HTTP	825 HTTP/1.1 200 OK (PNG)
56	5.895037	199.232.41.10	192.168.0.101	HTTP	1296 HTTP/1.1 200 OK (JPEG JFIF image)

图 10.gun.org 请求响应报文

计算为[（5.752849-5.558597）+（5.791381-5.745246）+（5.855740-5.806383）+（5.895037-5.806331）]/4=（0.240387+0.138063）/4=0.0946125s

结果为 www.google.com 服务器响应时间最短。

（10）哪个分组包含翻译 www.gnu.org 的 DNS 请求和应答？www.gnu.org 的 IP 地址是多少？

分组 21 和分组 22 包含翻译 www.gnu.org 的 DNS 请求和应答，如图 11 所示。

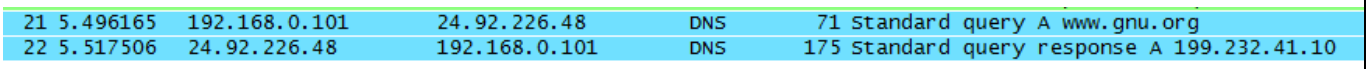


图 10. www.gnu.org 的 DNS 请求和应答

从上面分组 22 的 DNS 报文信息可知，www.gnu.org 的 IP 地址是 199.232.41.10。

实验心得

通过这次实验使我学会了很多实战上的知识。在课堂上学习理论，在实验课上实践，使我对于应用层协议的基础知识更加了解。通过实验，使我更加能熟练使用 Wireshark 工具抓取网络报文、查看已有报文信息并能对报文加以分析。

这次实验使我学会跟踪 Web 浏览器和 Web 服务器之间的 TCP 数据流，并离出浏览器发出的请求的方法。熟练掌握了颜色过滤器的写法和用法。对于 HTTP 的 GET 请求和 HTTP 响应有了更深层次的认识。并且使我对于多重 TCP 流有了一个新的认识。

通过这次实验，也使我更加熟练地掌握使用过滤器过滤出需要的报文。我详细阅读每行报文，掌握了 HTTP 数据报格式以及内容，并且复习了以前的数据报首部，在以后的学习中还应该加强对于报文的阅读理解的能力。