中国科学技术大学计算机学院

计算机网络实验报告

实验二

利用 Wireshark 观察 http 报文

学　　号：PB18081616

姓　　名：谭园

专　　业：计算机科学与技术

指导老师：张信明

中国科学技术大学计算机学院

2020 年 11 月 14 日

一、 实验目的

1. 熟悉并掌握 Wireshark 网络分析工具。

2. 捕获观察并分析 HTTP 报文结构。

3. 回答第二次实验 PDF 文件中的问题。

4. 分析 HTTP 中 get 和 post 请求方式的区别

二、 实验原理

HTTP 协议

三、 实验条件

1、 硬件条件：一台 PC 机

2、 软件条件：wireshark，注意配置软件的环境条件

四、 实验过程

1、 wireshark 的安装

2、 基本 HTTP GET/response 交互

3、 HTTP 条件 GET/response 交互

4、 检索长文件

5、 带有图片的 HTML 文档

6、 HTTP 认证

7、 问题回答

五、 结果分析

1.实验图像

四.2


http
No. Time Source Destination Protocol Length Info
2261 52.475790 114.214.228.122 128.119.245.12 HTTP 572 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2274 52.725030 128.119.245.12 114.214.228.122 HTTP 540 HTTP/1.1 200 OK (text/html)
2281 52.794691 114.214.228.122 128.119.245.12 HTTP 504 GET /favicon.ico HTTP/1.1
2292 53.040080 128.119.245.12 114.214.228.122 HTTP 538 HTTP/1.1 404 Not Found (text/html)
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6,ja;q=0.5\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 2274]
[Next request in frame: 2281]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sat, 14 Nov 2020 05:30:30 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Fri, 13 Nov 2020 06:58:01 GMT\r\n
ETag: "80-5b3f78ca15457"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.249240000 seconds]
[Request in frame: 2261]
[Next request in frame: 2281]
[Next response in frame: 2292]
[Request URI: http://gaia.cs.umass.edu/favicon.ico]
File Data: 128 bytes
Hypertext Transfer Protocol
GET /favicon.ico HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36\r\n
Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8\r\n
Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6,ja;q=0.5\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/favicon.ico]
[HTTP request 2/2]
[Prev request in frame: 2261]
[Response in frame: 2292]

```
Hypertext Transfer Protocol
  > HTTP/1.1 404 Not Found\r\n
    Date: Sat, 14 Nov 2020 05:30:30 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
  > Content-Length: 209\r\n
    Keep-Alive: timeout=5, max=99\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.245389000 seconds]
    [Prev request in frame: 2261]
    [Prev response in frame: 2274]
    [Request in frame: 2281]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 209 bytes
> Line-based text data: text/html (7 lines)
```

四.3

```
Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Sat, 14 Nov 2020 05:38:11 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-5b3f78ca1489f"\r\n
    \r\n
    [HTTP response 2/3]
    [Time since request: 0.246704000 seconds]
    [Prev request in frame: 325]
    [Prev response in frame: 389]
    [Request in frame: 431]
    [Next request in frame: 484]
    [Next response in frame: 496]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

```
Hypertext Transfer Protocol
  > GET /favicon.ico HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36\r\n
    Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6,ja;q=0.5\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/favicon.ico]
    [HTTP request 3/3]
    [Prev request in frame: 431]
    [Response in frame: 496]
```

```
Hypertext Transfer Protocol
  > HTTP/1.1 404 Not Found\r\n
    Date: Sat, 14 Nov 2020 05:38:12 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
  > Content-Length: 209\r\n
    Keep-Alive: timeout=5, max=98\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.245635000 seconds]
    [Prev request in frame: 431]
    [Prev response in frame: 482]
    [Request in frame: 484]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 209 bytes
  > Line-based text data: text/html (7 lines)
```

四.5

```
Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6,ja;q=0.5\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    [HTTP request 1/1]
    [Response in frame: 222]
```

```
Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 14 Nov 2020 05:43:59 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Fri, 13 Nov 2020 06:58:01 GMT\r\n
    ETag: "1194-5b3f78ca0f697"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.249340000 seconds]
    [Request in frame: 165]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
```

四.6

```
Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6,ja;q=0.5\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame: 359]
```

```
Hypertext Transfer Protocol
  > HTTP/1.1 401 Unauthorized\r\n
    Date: Sat, 14 Nov 2020 06:01:23 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  > Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.241709000 seconds]
    [Request in frame: 239]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    File Data: 381 bytes
```

```
Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  > Authorization: Basic d2lyZXNoYWstc3R1ZGVudHM6bmV0d29yaw==\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6,ja;q=0.5\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame: 1693]
```

```
Hypertext Transfer Protocol
  > HTTP/1.1 401 Unauthorized\r\n
    Date: Sat, 14 Nov 2020 06:01:41 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  > Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.242597000 seconds]
    [Request in frame: 1683]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    File Data: 381 bytes
  > Line-based text data: text/html (12 lines)
```

2 回答问题

1. 浏览器和服务器都运行 HTTP/1.1

2.接受语言：zh-CN，zh-TW，en-US 应该就是简体字和繁体字，英语。

3.计算机：114.214.228.122

Gaia.cs.umass.edu：128.119.245.12

4.200 OK

5.Fri，13 Nov 2020 06:58:01 GMT

6.128 bytes

7.没有看到

8.没有看到 IF-MODIFIED-SINCE

9.反回了文件内容，在实体部分可以看到

10. 看到了，IF-MODIFIED-SINCE：Fri，13 Nov 2020 06:58:01 GMT

11.304 Not Modified，服务器没有明确返回文件内容，因为文件后来没有被修改

12.只发送了一个

13.4 个

14.200 OK

15.没有，并没有查找到 continuation

16.3 个，一个网页，两个图片

17.串行，因为 Connection：Keep-Alive

18.401 Unauthorized

19.Authoorization:Basic

d2lyZXNoYWstc3R1ZGVudHM6bmV0d29yaw==\r\n

3 回答 HTTP 中 get 和 post 请求方式的区别

a) GET 请求的数据会附在 URL 之后（就是把数据放置在 HTTP 协议头中）,而与之对应的，POST 把提交的数据放置在 HTTP 包的包体中.

b) POST 的安全性更高，通过 GET 提交数据，用户名和密码将明文出现在 URL 上