

HTTP 实验

陈鸿绪 PB21000224 2023. 10. 3

第一部分：

1. 您浏览器运行的是 HTTP 1.0 还是 1.1 版本？服务器运行的是什么版本的 HTTP？

9471	2023-10-02	21:28:52.635780	100.64.130.89	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
9501	2023-10-02	21:28:52.911331	128.119.245.12	100.64.130.89	HTTP	540	HTTP/1.1 200 OK (text/html)

均为 1.1 版本。

2. 您的浏览器向服务器表明它可以接受什么语言（如果有）？

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/av
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n

由上可知为汉语。

3. 您计算机的 IP 地址是什么？ gaia.cs.umass.edu 服务器的 IP 地址是什么？

Source	Destination
100.64.130.89	128.119.245.12
128.119.245.12	100.64.130.89

4. 从服务器返回给浏览器的状态代码是什么？

Status Code: 200
[Status Code Description: OK]
Response Phrase: OK

5. 您正在检索的 HTML 文件在服务器上最后一次修改的时间是什么时候？

Last-Modified: Mon, 02 Oct 2023 05:59:01 GMT\r\n

注意以上显示的为 GMT 时间（格林威治标准时间）。

6. 有多少字节的内容被返回给您的浏览器？

Content-Length: 128\r\n
[Content length: 128]

由上可知为 128 字节。

7. 通过检查数据包内容窗口中的原始数据，您是否看到数据包列表窗口中未显示的数据中有任何头信息？如果有，请指出一个。

```

HTTP/1.1 200 OK\r\n
> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
  Date: Mon, 02 Oct 2023 13:28:52 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Mon, 02 Oct 2023 05:59:01 GMT\r\n
  ETag: "80-606b5788db7c4"\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

```

Last-Modified 的数据在列表窗口未显示。

第一部分：

187	2023-10-02	23:42:20.520129	100.64.130.89	128.119.245.12	HTTP	678	GET	/wireshark-labs/HTTP-wireshark-file2.html	HTTP/1.1
22	2023-10-02	23:42:31.361458	100.64.130.89	106.75.98.17	HTTP	1163	GET	/dspreport/dsp/rp?data=CAESIGMxZGJlYzZiYzNhMGFmNGIwY2EwZ	
22	2023-10-02	23:42:31.394960	106.75.98.17	100.64.130.89	HTTP	230	HTTP/1.1	200 (image/webp)	
22	2023-10-02	23:42:31.420476	100.64.130.89	180.163.247.237	HTTP	1429	GET	/s?type=1&r=20&tid=NTM2MDA2NzQ0MjgwNzE1MjcwNTAwMjI&finfc	
22	2023-10-02	23:42:31.431769	180.163.247.237	100.64.130.89	HTTP	510	HTTP/1.1	200 OK (GIF89a)	
26	2023-10-02	23:42:32.736178	100.64.130.89	128.119.245.12	HTTP	566	GET	/wireshark-labs/HTTP-wireshark-file2.html	HTTP/1.1
26	2023-10-02	23:42:33.014087	128.119.245.12	100.64.130.89	HTTP	784	HTTP/1.1	200 OK (text/html)	
60	2023-10-02	23:50:52.015961	100.64.130.89	128.119.245.12	HTTP	678	GET	/wireshark-labs/HTTP-wireshark-file2.html	HTTP/1.1
60	2023-10-02	23:50:52.291157	128.119.245.12	100.64.130.89	HTTP	294	HTTP/1.1	304 Not Modified	
61	2023-10-02	23:50:57.287254	100.64.130.89	128.119.245.12	HTTP	678	GET	/wireshark-labs/HTTP-wireshark-file2.html	HTTP/1.1
61	2023-10-02	23:50:57.335364	100.64.130.89	128.119.245.12	HTTP	678	GET	/wireshark-labs/HTTP-wireshark-file2.html	HTTP/1.1
62	2023-10-02	23:50:57.616707	128.119.245.12	100.64.130.89	HTTP	294	HTTP/1.1	304 Not Modified	

- 检查从您的浏览器到服务器的第一个 HTTP GET 请求的内容。您在 HTTP GET 中看到 “IF-MODIFIED-SINCE” ？

```

If-None-Match: "173-606b5788dac0c"\r\n
If-Modified-Since: Mon, 02 Oct 2023 05:59:01 GMT\r\n

```

如上可见存在。

- 检查服务器响应的内容。服务器是否明确返回了文件的内容？你怎么知道的？

```

> Hypertext Transfer Protocol
> Line-based text data: text/html (10 lines)

```

由上可见明确返回了文件的内容。展开即可看见完全内容。

- 现在检查从您的浏览器到服务器的第二个 HTTP GET 请求的内容。您在 HTTP GET 中看到 “IF-MODIFIED-SINCE:”，如果有，那么 “IF-MODIFIED-SINCE:” 头后面跟着什么信息？

经过检查，第二个没有 “IF-MODIFIED-SINCE:” 。

11. 服务器响应这个第二个 HTTP GET 返回的 HTTP 状态码和短语是什么？服务器是否明确返回了文件的内容？解释原因。

Status Code: 304

[Status Code Description: Not Modified]

Response Phrase: Not Modified

没有明确返回文件的内容,原因在于浏览器在刚浏览过该页面后具有该页面缓存。

12. 浏览器发送了多少个 HTTP GET 请求消息？跟踪中的哪个数据包号包含获取权利法案的 GET 消息？

703	2023-10-02 23:56:48.780306	100.64.130.89	128.119.245.12	HTTP	566 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
708	2023-10-02 23:56:49.058241	128.119.245.12	100.64.130.89	HTTP	535 HTTP/1.1 200 OK (text/html)

发送了 1 个 HTTP GET 请求，第 703 号包含了权利法案的 GET 消息。

13. 跟踪中的哪个数据包号包含与 HTTP GET 请求响应相关的状态码和短语？由上一题的图可见，第 708 号包含了相关状态码和短语。

- #### 14. 响应中的状态码和短语是什么？

200, OK

15. 需要多少个包含数据的 TCP 段来承载单个 HTTP 响应和权利法案的文本？

```
[4 Reassembled TCP Segments (4861 bytes): #705(1460), #706(1460), #707(1460), #708(481)]
```

[Frame: 705, payload: 0-1459 (1460 bytes)]

[Frame: 706, payload: 1460-2919 (1460 bytes)]

[Frame: 707, payload: 2920-4379 (1460 bytes)]

```
[Frame: 708, payload: 4380-4860 (481 bytes)]
```

```
[Segment count: 4]
```

```
[Reassembled TCP length: 4861]
```

```
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d6f6e2c203032204f6
```

可以看见需要四个 TCP 段来承载单个 HTTP 响应和权利法案的文本。

16. 您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 Internet 地址？

No.	Time	Source	Destination	Protocol	Length	Info
26.	2023-10-03 00:50:31.802248	100.64.130.89	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
26.	2023-10-03 00:50:32.079827	128.119.245.12	100.64.130.89	HTTP	1355	HTTP/1.1 200 OK (text/html)
26.	2023-10-03 00:50:32.085105	100.64.130.89	128.119.245.12	HTTP	512	GET /pearson.png HTTP/1.1
27.	2023-10-03 00:50:32.22245	100.64.130.89	206.0.192	HTTP/JSON	239	POST /api/browser/edge/navigate/ HTTP/1.1, JavaScript Object
27.	2023-10-03 00:50:32.362541	128.119.245.12	100.64.130.89	HTTP	745	HTTP/1.1 200 OK (PNG)
27.	2023-10-03 00:50:32.456801	206.0.192	100.64.130.89	HTTP/JSON	85	HTTP/1.1 200 OK, JavaScript Object Notation (application/json)
28.	2023-10-03 00:50:33.270391	100.64.130.89	178.79.137.164	HTTP	479	GET /8E_cover_small.jpg HTTP/1.1
28.	2023-10-03 00:50:33.619630	178.79.137.164	100.64.130.89	HTTP	625	HTTP/1.1 301 Moved Permanently
28.	2023-10-03 00:50:34.451516	2001:da8:d800:a...a	2001:da8:d800:91ff::	HTTP	208	GET /8E_cover_small.jpg HTTP/1.1
34..	2023-10-03 00:50:36.760964	2a01:7e00::f03c...	2001:da8:d800:a715:58...	HTTP	765	HTTP/1.1 200 OK (JPEG JFIF image)

发送了四个 HTTP GET 请求消息，有：128.119.245.12 以及 178.79.137.164 以及 2a01:7e00::f03c:91ff:fe70:4c18 (ipv6)

17. 您能否判断您的浏览器是串行下载两个图像，还是从两个网站并行下载？请解释。

Date: Mon, 02 Oct 2023 16:50:35 GMT\r\n

Date: Mon, 02 Oct 2023 16:50:32 GMT\r\n

由上可见两张图片是串行下载，因为时间不同。

18. 服务器对浏览器初始 HTTP GET 消息的响应（状态码和短语）是什么？

No.	Time	Source	Destination	Protocol	Length	Info
229	2023-10-03 01:01:28.869123	100.64.130.89	128.119.245.12	HTTP	582	GET /wireshark-labs/protected_pages/HTTP-w
258	2023-10-03 01:01:29.144612	128.119.245.12	100.64.130.89	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
630	2023-10-03 01:01:55.290098	100.64.130.89	128.119.245.12	HTTP	667	GET /wireshark-labs/protected_pages/HTTP-w
652	2023-10-03 01:01:55.569044	128.119.245.12	100.64.130.89	HTTP	544	HTTP/1.1 200 OK (text/html)

由上图片可见状态码为 401 短语为 Unauthorized。

19. 当您的浏览器第二次发送 HTTP GET 消息时，HTTP GET 消息中包含了什么新字段？

▼ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5l\r\n
Credentials: wireshark-students:network

HTTP GET 消息中包含了“Authorization”头部字段，该字段包含了输入的用户名（wireshark-students）和密码（network）。