

Assignment #003:

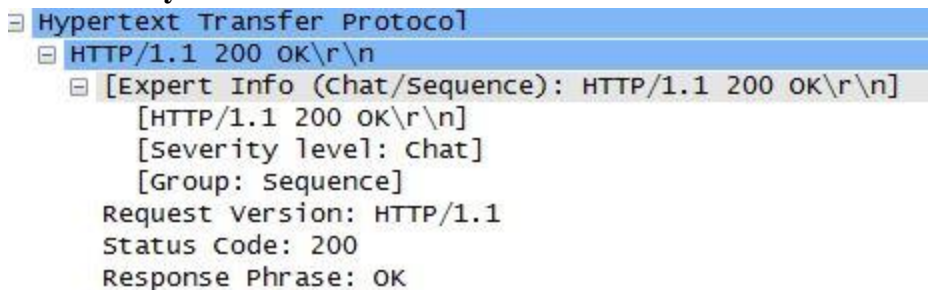
Use Wireshark to study HTTP. You'll explore several aspects of the HTTP protocol: the basic GET/response interaction, HTTP message formats, retrieving HTML files with embedded objects, and HTTP authentication and security.

1. HTTP GET/response interaction

Begin your exploration of HTTP by downloading a very simple HTML file - one that is very short, and contains embedded objects. Please show your screen shots, answer the following questions and circle the answers on your screen shots:

- (1) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

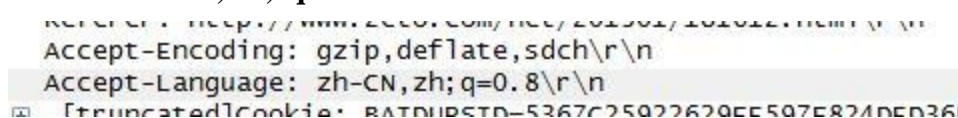
Answer: My browser runs HTTP 1.1 and the server runs HTTP 1.1 too.



```
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
[HTTP/1.1 200 OK\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Version: HTTP/1.1
Status Code: 200
Response Phrase: OK
```

- (2) What languages does your browser indicate that it can accept to the server?

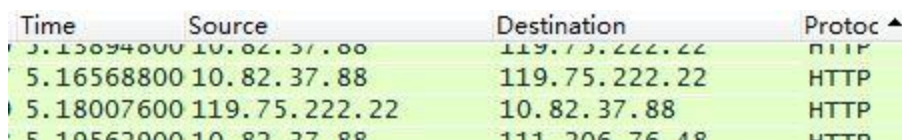
Answer: zh-CN, zh; q=0.8



```
Accept-Encoding: gzip,deflate,sdch\r\n
Accept-Language: zh-CN,zh;q=0.8\r\n
[Truncated]Cookie: BATNIBSTN=5367C25Q22629EE5Q7E824DED36
```

- (3) What is the IP address of your computer and of the server?

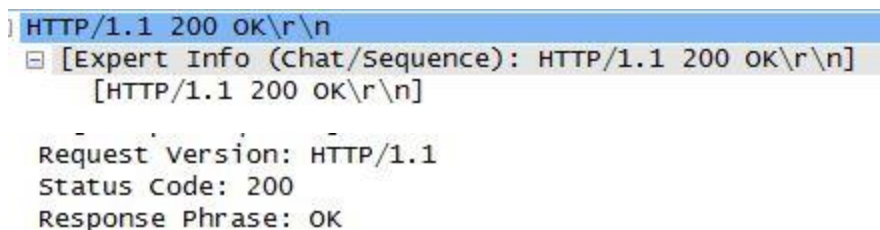
Answer: The IP address of my computer is '10.82.37.88' and the IP address of the server is '119.75.222.22'.



Time	Source	Destination	Protocol
5.15894800	10.82.37.88	119.75.222.22	HTTP
5.16568800	10.82.37.88	119.75.222.22	HTTP
5.18007600	119.75.222.22	10.82.37.88	HTTP
5.18562000	10.82.37.88	119.75.222.22	HTTP

- (4) What is the status code returned from the server to your browser?

Answer: 200 OK



```
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
[HTTP/1.1 200 OK\r\n]
Request Version: HTTP/1.1
Status Code: 200
Response Phrase: OK
```

(5) When was the HTML file that you are retrieving last modified at the server?

Answer: Fri Apr 10 19:39:22 2015

```
Last-Modified: Fri Apr 10 19:39:22 2015\r\n
```

(6) How many bytes of content are being returned to your browser?

Answer: 320 bytes

```
Content-Length: 320\r\n[Content length: 320]
```

(7) Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Answer: No.

```
Hypertext Transfer Protocol
+ [truncated]GET /ecom?di=745777&dcb=BAIDU_DUP_define&dtm=BAIDU_DUP
Host: cb.baidu.com\r\n
Connection: keep-alive\r\n
Accept: */*\r\n
User-Agent: Mozilla/5.0 (windows NT 6.1) AppleWebKit/537.36 (KHTML
Referer: http://www.2cto.com/net/201301/181612.html\r\n
Accept-Encoding: gzip,deflate, sdch\r\n
Accept-Language: zh-CN,zh;q=0.8\r\n
+ [truncated]Cookie: BAIDUSID=5367C25922629FE597F824DED36DE19C; lo
Cookie pair: BAIDUSID=5367C25922629FE597F824DED36DE19C
Cookie pair: locale=zh
Cookie pair [truncated]: __xsptplus188=188.16.1423470260.1423470
Cookie pair: ATS_PASS=1
```

(8) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer: No.

```
Line-based text data: text/javascript
[truncated]BAIDU_DUP_define('request!745777_0',[],{deps:['c1b/fixed7o'],data:{'id': '745777','_stype': 0,'_w': 200,'_h': 200,'_type': 'json_html','_htm

[HTTP response 1/6]
[Time since request: 0.012308000 seconds]
[Request in frame: 238]
[Next request in frame: 255]
[Next response in frame: 258]
```

(9) Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Answer: No.

```

Hypertext Transfer Protocol
[truncated]GET /ecom?di=298612&dcb=BAIDU_DUP_define&dtm=BAIDU_DUP2_SET3SONADSL0T&dbv=2&dci=0&dri=0&dis=0&dai=2&dds=&drs=1&dvi=1421289014&ltu=http%3A%2F%2F
Host: cb.baidu.com\r\n
Connection: keep-alive\r\n
Accept: */*\r\n
User-Agent: Mozilla/5.0 (windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.153 Safari/537.36 SE 2.X MetaSr 1.0\r\n
Referer: http://www.2cto.com/net/201301/181612.html\r\n
Accept-Encoding: gzip,deflate,sdch\r\n
Accept-Language: zh-CN,zh;q=0.8\r\n
[truncated]Cookie: BAIDUID=5367C25922629FE597F824DED36DE19C; locale=zh; __xstptlus188=188.16.1423470260.1423470582.2%232%7Cwww.sogou.com%7C%7C%25E8%2F%2F
\r\n
[Full request URI [truncated]: http://cb.baidu.com/ecom?di=298612&dcb=BAIDU_DUP_define&dtm=BAIDU_DUP2_SET3SONADSL0T&dbv=2&dci=0&dri=0&dis=0&dai=2&dds=&drs=
[HTTP request 2/6]
[Prev request in frame: 238]
[Prev response in frame: 241]
[Request in frame: 255]
[Next request in frame: 260]
[Next response in frame: 263]

```

(10) What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file?

Answer: 200 OK

```

[HTTP response 2/6]
[Time since request: 0.011516000 seconds]
[Prev request in frame: 238]
[Prev response in frame: 241]
[Request in frame: 255]
[Next request in frame: 260]
[Next response in frame: 263]
Line-based text data: text/javascript
[truncated]BAIDU_DUP_define('request!298612_0',[],{deps:['c1b/fixed7o'],data:{'id': '298612','_stype': 0,'_w': 980,'_h': 60,'_type': 'json_html','_ht

```

2. HTTP Authentication

Please try visiting a web site that is password-protected and examine the sequence of HTTP message exchanged for such a site. Do the following:

(1) Make sure your browser's cache is cleared, as discussed above, and close down your browser.

Then, start up your browser

(2) Start up the Wireshark packet sniffer

(3) Enter the URL into your browser

(4) Type the requested user name and password into the pop up box.

(5) Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

(**Note:** You might want to first read up on HTTP authentication by reviewing the Wikipedia entry at http://en.wikipedia.org/wiki/Basic_access_authentication.)

Please show your screen shots, answer the following questions and circle the answers on your screen shots:

(1) What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Answer: 302 Found

```
HTTP/1.1 302 Found\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 302 Found\r\n]
[HTTP/1.1 302 Found\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Version: HTTP/1.1
Status Code: 302
Response Phrase: Found
Server: nginx/1.4.3\r\n
Date: Fri, 10 Apr 2015 13:13:40 GMT\r\n
Content-Type: text/html\r\n
```

(2) When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answer: The new field is 'index.php/main'.

The First Time:

```
GET / HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
[GET / HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /
Request Version: HTTP/1.1
Host: bbs.nankai.edu.cn\r\n
Connection: keep-alive\r\n
```

The Second Time:

```
GET /index.php/main HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /index.php/main HTTP/1.1\r\n]
[GET /index.php/main HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /index.php/main
Request Version: HTTP/1.1
Host: bbs.nankai.edu.cn\r\n
Connection: keep-alive\r\n
```

学号: 1210565

2015 年 4 月 10 日星期五