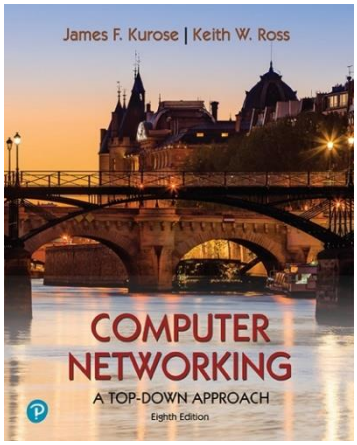
Wireshark Lab: HTTP v8.1

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.*, J.F. Kurose and K.W. Ross

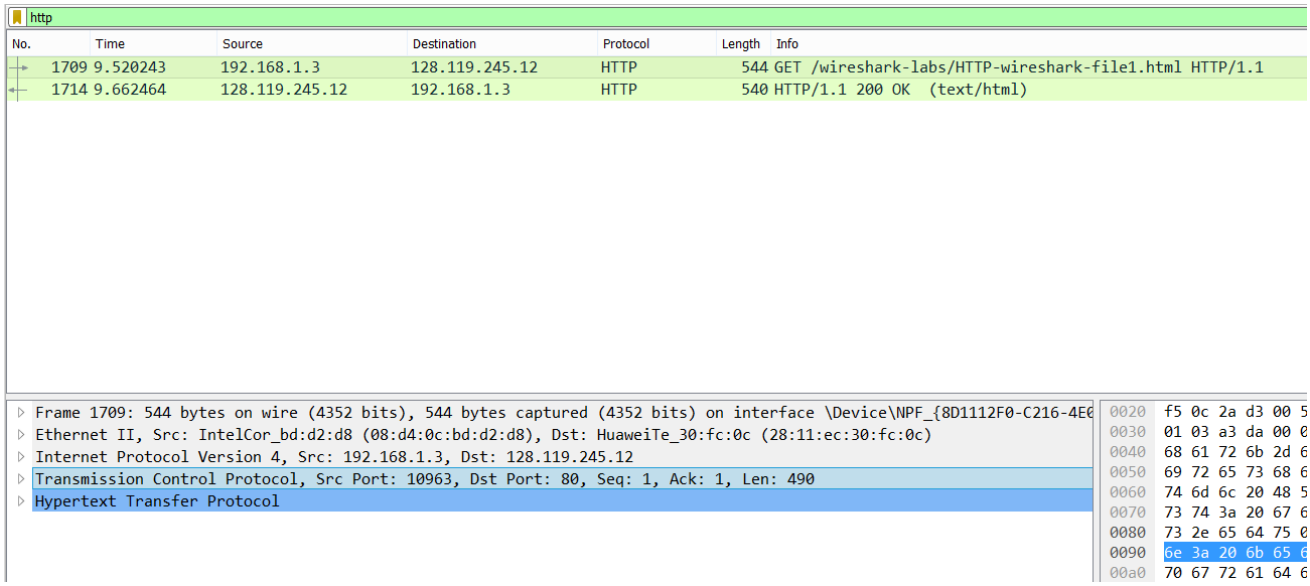


"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

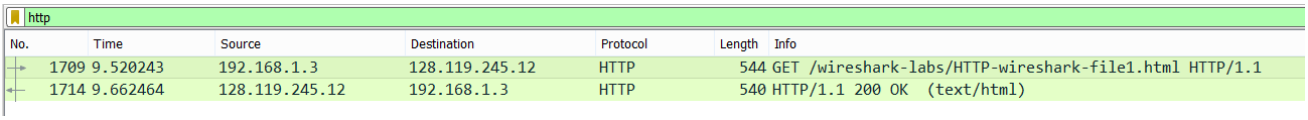
Contents

Basic HTTP GET/response interaction

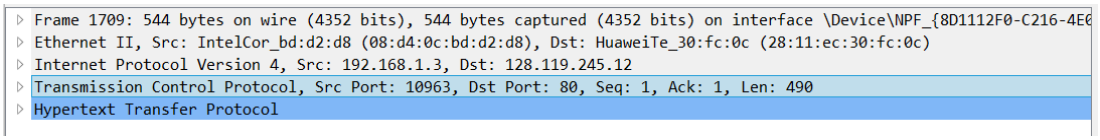
1. Start up your web browser.
2. Start up the Wireshark packet sniffer.
3. Enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.
4. Wait a bit more than one minute, and then begin Wireshark packet capture.
5. Enter the following to your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
6. Your browser should display the very simple, one-line HTML file.
7. Stop Wireshark packet capture.
8. Your Wireshark should be like this:



a. The packet-listing window that **two HTTP messages were captured**: the GET message (from your browser to the gaia.cs.umass.edu web server) and the response message from the server to your browser.



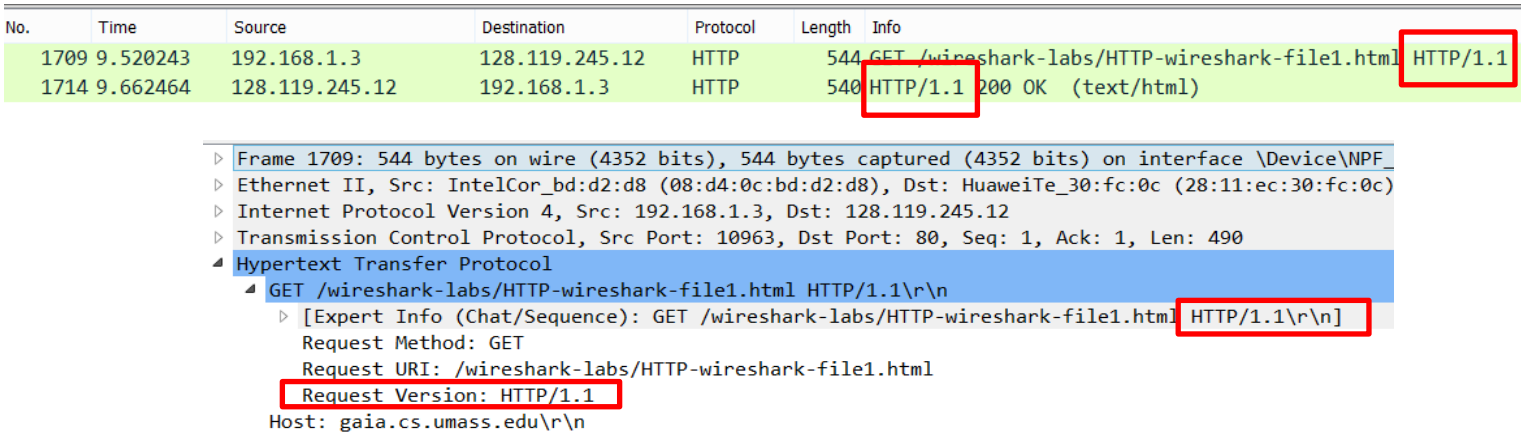
b. Wireshark displays the Frame, Ethernet, IP, and TCP packet information as well.



(*Note:* You should ignore any HTTP GET and response for favicon.ico. If you see a reference to this file, it is your browser automatically asking the server if it (the server) has a small icon file that should be displayed next to the displayed URL in your browser. We'll ignore references to this pesky file in this lab.).

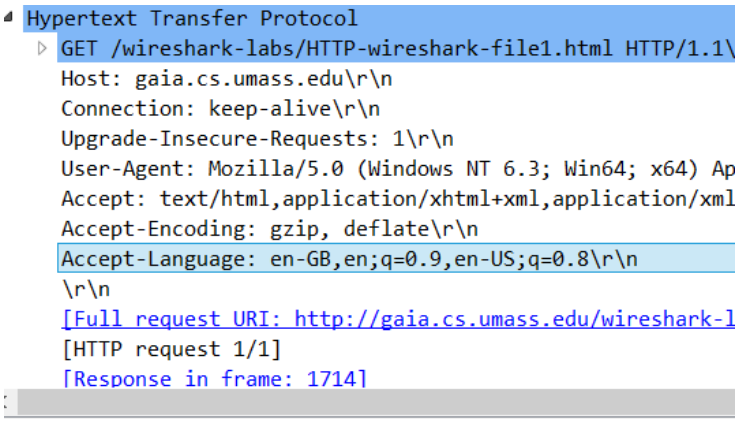
Exercise

1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?



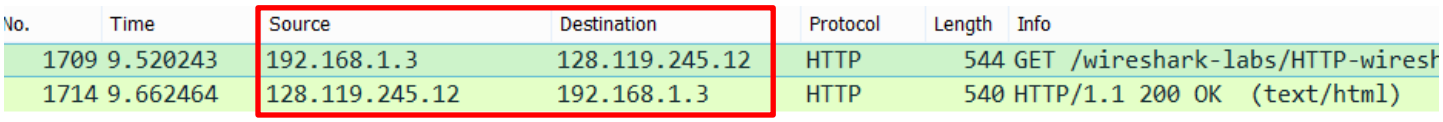
Select the "GET" packet.
In the "Hypertext Transfer Protocol", you notice that HTTP version is 1.1
Select the response packet, you notice that the server is running HTTP version 1.1

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



Select the "GET" packet.
Expand the "Hypertext Transfer Protocol", notice the field "Accept-Language" indicating that the browser accepts English.

3. What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server?

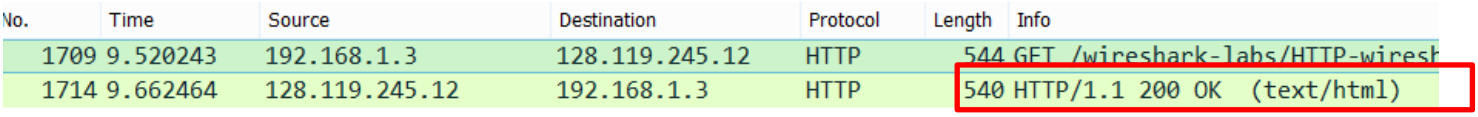


No.	Time	Source	Destination	Protocol	Length	Info
1709	9.520243	192.168.1.3	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wiresh
1714	9.662464	128.119.245.12	192.168.1.3	HTTP	540	HTTP/1.1 200 OK (text/html)

My IP address is 192.16.1.3

The server's IP address is 128.119.245.12

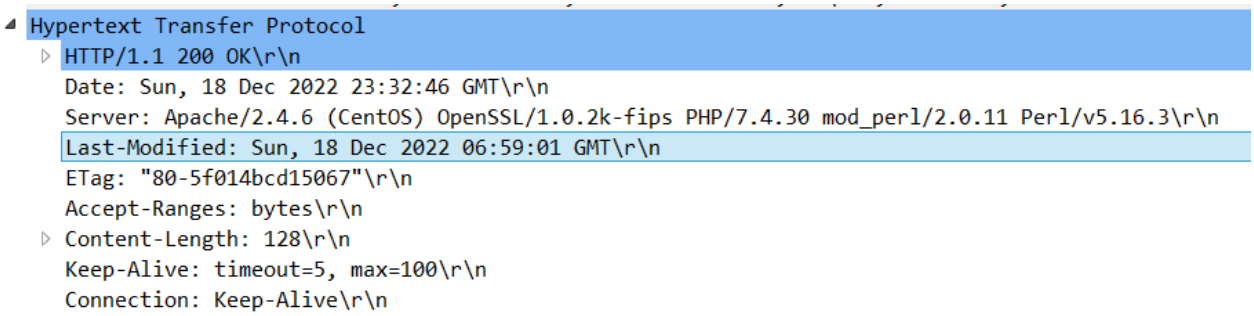
4. What is the status code returned from the server to your browser?



No.	Time	Source	Destination	Protocol	Length	Info
1709	9.520243	192.168.1.3	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wiresh
1714	9.662464	128.119.245.12	192.168.1.3	HTTP	540	HTTP/1.1 200 OK (text/html)

200 OK

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



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Sun, 18 Dec 2022 23:32:46 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Sun, 18 Dec 2022 06:59:01 GMT\r\n
  ETag: "80-5f014bcd15067"\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
```

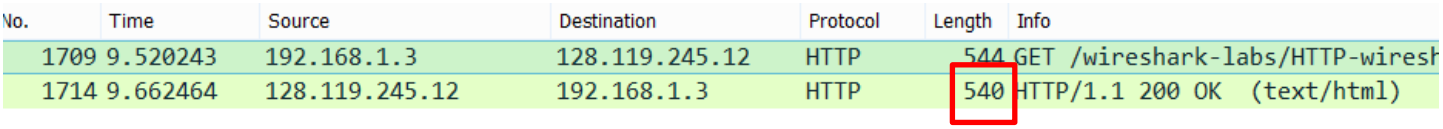
Select the response packet.

Expand the "Hypertext Transfer Protocol" section

Lookup the "Last-Modified" field.

The page is last modified in 18 Dec 2022 at 6:59

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

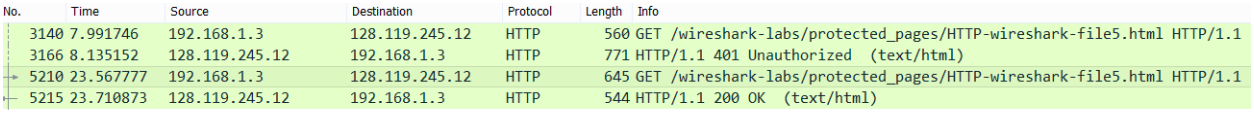


No.	Time	Source	Destination	Protocol	Length	Info
1709	9.520243	192.168.1.3	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wiresh
1714	9.662464	128.119.245.12	192.168.1.3	HTTP	540	HTTP/1.1 200 OK (text/html)

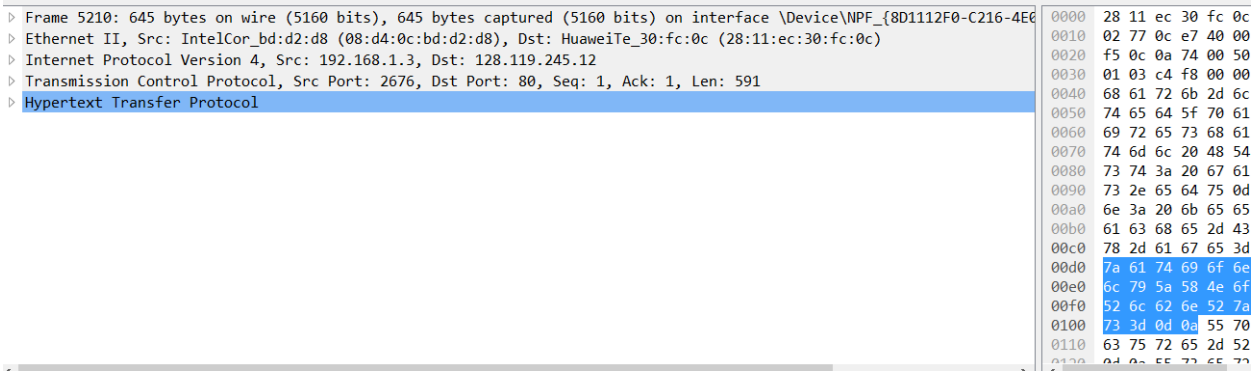
540 bytes

HTTP Authentication

1. Make sure your browser's cache is cleared.
2. Start up the Wireshark packet sniffer
3. Enter the following URL into your browser
   http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html
4. Enter the username "wireshark-students" and password "network".
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.
6. We get the following



No.	Time	Source	Destination	Protocol	Length	Info
3140	7.991746	192.168.1.3	128.119.245.12	HTTP	560	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
3166	8.135152	128.119.245.12	192.168.1.3	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
5210	23.567777	192.168.1.3	128.119.245.12	HTTP	645	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
5215	23.710873	128.119.245.12	192.168.1.3	HTTP	544	HTTP/1.1 200 OK (text/html)



```
▷ Frame 5210: 645 bytes on wire (5160 bits), 645 bytes captured (5160 bits) on interface \Device\NPF_{8D1112F0-C216-4E6
▷ Ethernet II, Src: IntelCor_bd:d2:d8 (08:d4:0c:bd:d2:d8), Dst: HuaweiTe_30:fc:0c (28:11:ec:30:fc:0c)
▷ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
▷ Transmission Control Protocol, Src Port: 2676, Dst Port: 80, Seq: 1, Ack: 1, Len: 591
▷ Hypertext Transfer Protocol
```

```
0000  28 11 ec 30 fc 0c
0010  02 77 0c e7 40 00
0020  f5 0c 0a 74 00 50
0030  01 03 c4 f8 00 00
0040  68 61 72 6b 2d 6c
0050  74 65 64 5f 70 61
0060  69 72 65 73 68 61
0070  74 6d 6c 20 48 54
0080  73 74 3a 20 67 61
0090  73 2e 65 64 75 0d
00a0  6e 3a 20 6b 65 65
00b0  61 63 68 65 2d 43
00c0  78 2d 61 67 65 3d
00d0  7a 61 74 69 6f 6e
00e0  6c 79 5a 58 4e 6f
00f0  52 6c 62 6e 52 7a
0100  73 3d 0d 0a 55 70
0110  63 75 72 65 2d 52
```

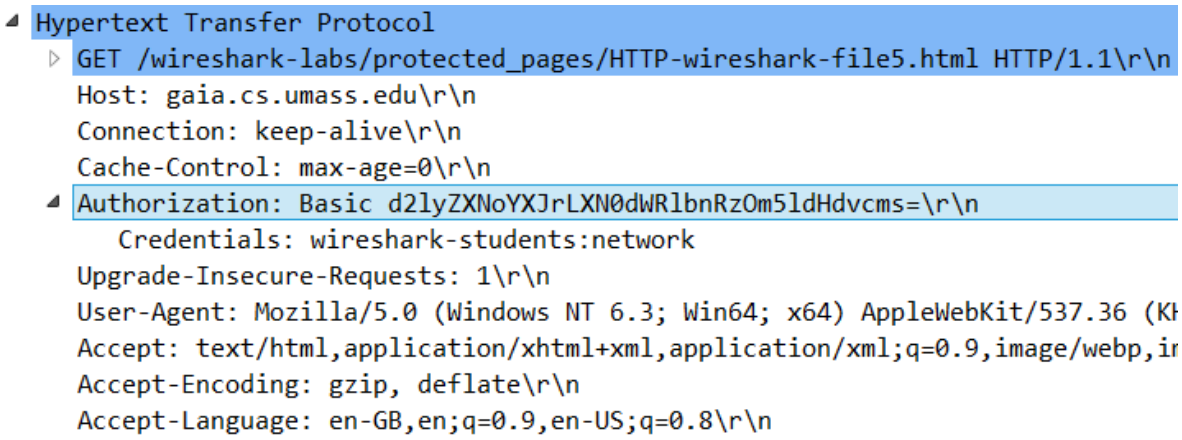
Exercise

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

3140	7.991746	192.168.1.3	128.119.245.12	HTTP	560	GET /wireshark-labs/protected_pages/HTTP-wire
3166	8.135152	128.119.245.12	192.168.1.3	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
5210	23.567777	192.168.1.3	128.119.245.12	HTTP	645	GET /wireshark-labs/protected_pages/HTTP-wire
5215	23.710873	128.119.245.12	192.168.1.3	HTTP	544	HTTP/1.1 200 OK (text/html)

401 Unauthorized

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



Authorization field. It includes the username and password.

The username (wireshark-students) and password (network) that you entered are encoded in the string of characters (d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=). While it may appear that your username and password are encrypted, they are simply encoded in a format known as Base64 format. The username and password are not encrypted! To see this, go to http://www.motobit.com/util/base64-decoder-encoder.asp and enter the base64-encoded string d2lyZXNoYXJrLXN0dWRlbnRz and decode.