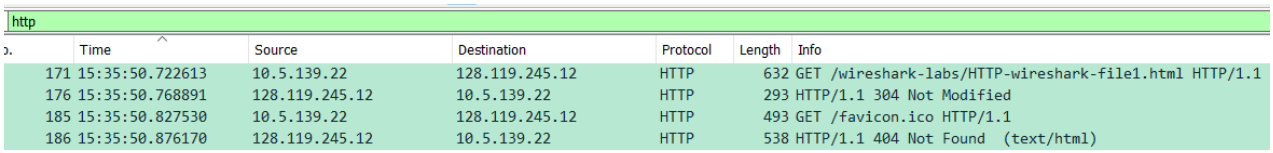
ENGR 3321 - Lab 2: Wireshark HTTP
September 29th 2022
Nathan Cauwet
873271826

1. The Basic HTTP GET/response interaction:



http

No.	Time	Source	Destination	Protocol	Length	Info
171	15:35:50.722613	10.5.139.22	128.119.245.12	HTTP	632	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
176	15:35:50.768891	128.119.245.12	10.5.139.22	HTTP	293	HTTP/1.1 304 Not Modified
185	15:35:50.827530	10.5.139.22	128.119.245.12	HTTP	493	GET /favicon.ico HTTP/1.1
186	15:35:50.876170	128.119.245.12	10.5.139.22	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Prefer: safe
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.42
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: "80-5e951dfebb45b"
If-Modified-Since: Fri, 23 Sep 2022 05:59:01 GMT
```

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

HTTP version 1.1 is running on both

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

HTML

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

My IP: 10.5.139.22

Gaia.cs.umass.edu IP: 128.199.245.12

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

The server replies to the 1st GET with “304 Not Modified”. For the 2nd GET it returns “404 Not Found”

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

Fri, 23 Sep 2022 05:59:01 GMT

```
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Prefer: safe\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) A
Accept: text/html,application/xhtml+xml,application/xml
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "80-5e951dfebb45b"\r\n
If-Modified-Since: Fri, 23 Sep 2022 05:59:01 GMT\r\n
\r\n
```

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

From server: 293 + 538 = 831 bytes

Sent to server : 632 + 493 = 1125 bytes

1.7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

I assume there is one but I can't find it. I thought I saw php in there, however I am now unable to find it.

2. The HTTP CONDITIONAL GET/response interaction:

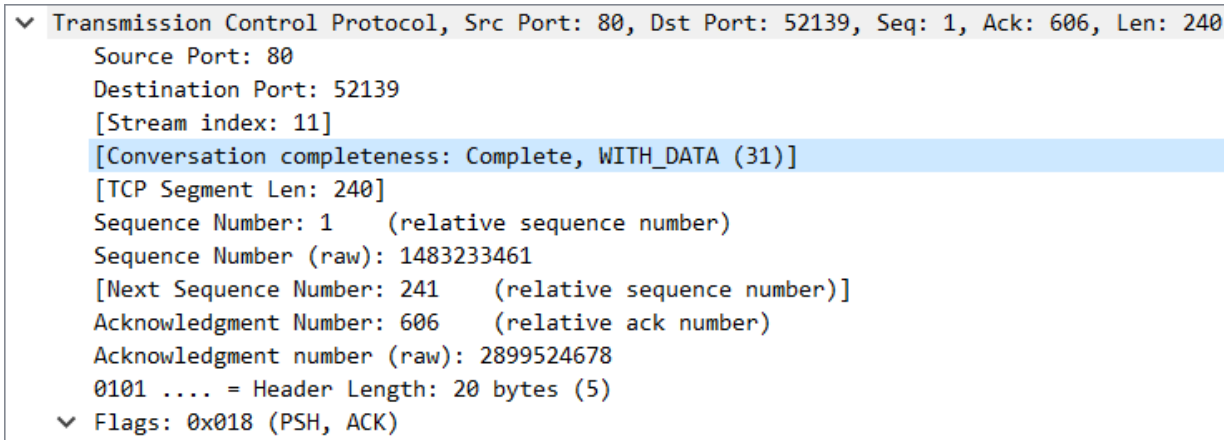
Q8) Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

Yes, highlighted in green here:

```
GET /wireshark-labs/HTTP-wireshark-file2.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
Prefer: safe\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/105.0.0.0 Safari/537.36 Edg/105.0.1343.42\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: en-US,en;q=0.9\r\n
If-None-Match: "173-5e951dfebac8b"\r\n
If-Modified-Since: Fri, 23 Sep 2022 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 54]
```

Q9) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Yes, the TCP response analysis states that the conversation is complete. It is notable that it only shows as complete if the cache is empty in the browser before loading the page.



Q10) 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?

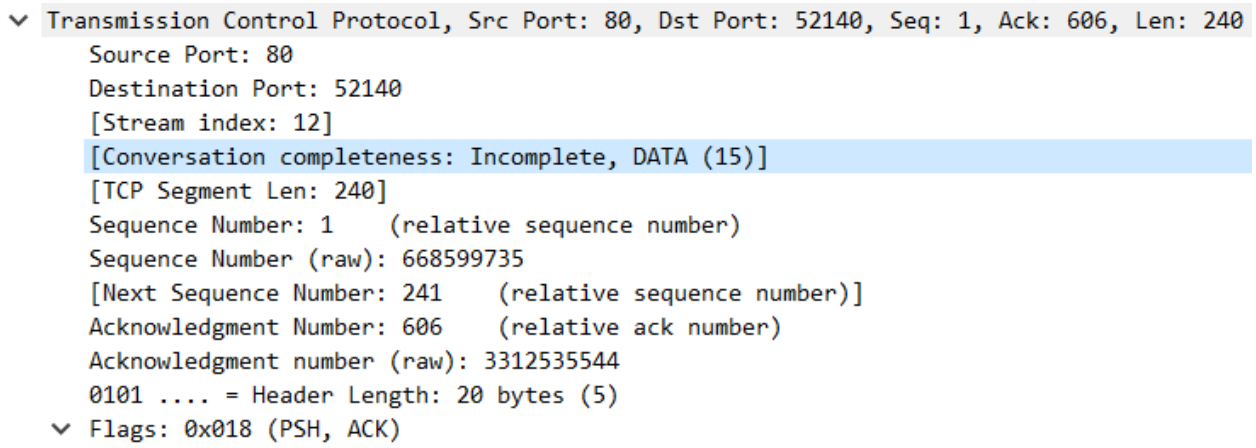
Yes. It shows the following:

If-Modified-Since: Fri, 23 Sep 2022 05:59:01 GMT\r\n

\r\n

Q11) 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? Explain.

The HTTP status code returned is "304 Not Modified". The server did not explicitly return the contents, it appears to have updated the contents (based on the cached data):



3. Retrieving Long Documents:

Q12) How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?

No.	Time	Source	Destination	Protocol	Length	Info
232	10:27:21.222086	10.5.139.22	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
245	10:27:21.282464	128.119.245.12	10.5.139.22	HTTP	757	HTTP/1.1 200 OK (text/html)
257	10:27:21.366654	10.5.139.22	128.119.245.12	HTTP	493	GET /favicon.ico HTTP/1.1
260	10:27:21.412463	128.119.245.12	10.5.139.22	HTTP	538	HTTP/1.1 404 Not Found (text/html)

My browser sent **2** HTTP GET request messages. The packet number of the trace containing the GET for the Bill of Rights was 232 (the first one).

Q13) Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

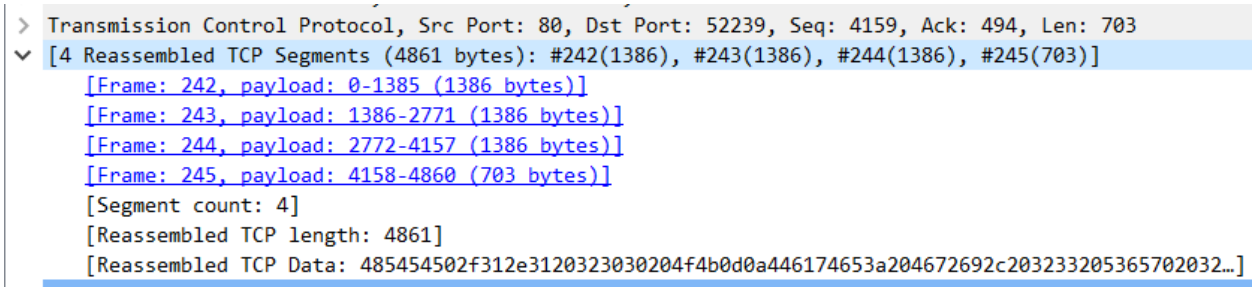
Packet number 245 contains the response and the status code.

Q14) What is the status code and phrase in the response?

The status code is 200 and the phrase is "OK".

Q15) How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Four TCP segments were returned containing data for the HTTP response and the Bill of Rights text.



4. HTML Documents with Embedded Objects:

Q16) How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Three total HTTP GET requests were sent.

The first two went to gaia.cs.umass.edu (ip: 128.119.245.12) and the third went to kurose.cslash.net (ip: 178.79.137.164)

Q17) Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

Wireshark is able to make a flow diagram from your data (shown below). According to this flow diagram the first GETs were parallel, however, the first and second image were not downloaded in parallel because they are from two different hosts. The time is also slightly different.

5. HTTP Authentication:

No.	Time	Source	Destination	Protocol	Length	Info
59	10:45:17.644217	10.5.139.22	128.119.245.12	HTTP	563	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
66	10:45:17.692151	128.119.245.12	10.5.139.22	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
10847	10:45:38.224262	10.5.139.22	128.119.245.12	HTTP	648	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
10854	10:45:38.271155	128.119.245.12	10.5.139.22	HTTP	544	HTTP/1.1 200 OK (text/html)

Q18) What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

The server's response to the initial GET message is status code 401 "Unauthorized".

```
Hypertext Transfer Protocol
  HTTP/1.1 401 Unauthorized\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
    Response Version: HTTP/1.1
    Status Code: 401
    [Status Code Description: Unauthorized]
    Response Phrase: Unauthorized
  Date: Fri, 23 Sep 2022 16:45:17 GMT\r\n
```

Q19) When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

The second time two new fields are included: Cache-Control and Authorization.

```
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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
  Prefer: safe\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/105.0.0.0 Safari/537.36 Edg/105.0.1343.50\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: en-US,en;q=0.9\r\n
  \r\n
```

The username and password are encoded in Base64.

Using this online tool https://www.motobit.com/util/base64-decoder-encoder.asp one can see that d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms= in base64 is equal to wireshark-students:network in regular text.

```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Prefer: safe
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.42
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: "80-5e951dfebb45b"
If-Modified-Since: Fri, 23 Sep 2022 05:59:01 GMT

HTTP/1.1 304 Not Modified
Date: Fri, 23 Sep 2022 15:35:51 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/
v5.16.3
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
ETag: "80-5e951dfebb45b"

GET /favicon.ico HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.42
Prefer: safe
Accept: image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 404 Not Found
Date: Fri, 23 Sep 2022 15:35:51 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/
v5.16.3
Content-Length: 209
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /favicon.ico was not found on this server.</p>
</body></html>
```

C:\Users\ncauw\Documents\lab2.pcapng 193 total packets, 4 shown

```
No.     Time               Source                Destination           Protocol Length Info
    171 15:35:50.722613    10.5.139.22           128.119.245.12        HTTP     632    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 171: 632 bytes on wire (5056 bits), 632 bytes captured (5056 bits) on interface \Device\NPF_{3F3DB8EB-1AC0-401B-8543-3316F86ED445}, id 0
Ethernet II, Src: RivetNet_ea:43:59 (9c:b6:d0:ea:43:59), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
Internet Protocol Version 4, Src: 10.5.139.22, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50709, Dst Port: 80, Seq: 1, Ack: 1, Len: 578
Hypertext Transfer Protocol
0000  00 00 0c 07 ac 00 9c b6 d0 ea 43 59 08 00 45 00   ..........CY..E.
0010  02 6a b5 2b 40 00 80 06 38 c3 0a 05 8b 16 80 77   .j.+@...8......w
0020  f5 0c c6 15 00 50 fe 69 f0 82 c2 2d e1 9f 50 18   .....P.i...-..P.
0030  02 02 d1 a7 00 00 47 45 54 20 2f 77 69 72 65 73   ......GET /wires
0040  68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77   hark-labs/HTTP-w
0050  69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68   ireshark-file1.h
0060  74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f   tml HTTP/1.1..Ho
0070  73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73   st: gaia.cs.umas
0080  73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f   s.edu..Connectio
0090  6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 50   n: keep-alive..P
00a0  72 65 66 65 72 3a 20 73 61 66 65 0d 0a 55 70 67   refer: safe..Upg
00b0  72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65   rade-Insecure-Re
00c0  71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d   quests: 1..User-
00d0  41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35   Agent: Mozilla/5
00e0  2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31   .0 (Windows NT 1
00f0  30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29   0.0; Win64; x64)
0100  20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37    AppleWebKit/537
0110  2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65   .36 (KHTML, like
0120  20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31    Gecko) Chrome/1
0130  30 35 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 2f   05.0.0.0 Safari/
0140  35 33 37 2e 33 36 20 45 64 67 2f 31 30 35 2e 30   537.36 Edg/105.0
0150  2e 31 33 34 33 2e 34 32 0d 0a 41 63 63 65 70 74   .1343.42..Accept
0160  3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c   : text/html,appl
0170  69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d   ication/xhtml+xm
0180  6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d   l,application/xm
0190  6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65   l;q=0.9,image/we
01a0  62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f   bp,image/apng,*/
01b0  2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74   *;q=0.8,applicat
01c0  69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61   ion/signed-excha
01d0  6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 39 0d 0a   nge;v=b3;q=0.9..
01e0  41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a   Accept-Encoding:
01f0  20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a    gzip, deflate..
0200  41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a   Accept-Language:
0210  20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 0d    en-US,en;q=0.9.
0220  0a 49 66 2d 4e 6f 6e 65 2d 4d 61 74 63 68 3a 20   .If-None-Match:
0230  22 38 30 2d 35 65 39 35 31 64 66 65 62 62 34 35   "80-5e951dfebb45
0240  62 22 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 64 2d   b"..If-Modified-
0250  53 69 6e 63 65 3a 20 46 72 69 2c 20 32 33 20 53   Since: Fri, 23 S
0260  65 70 20 32 30 32 32 20 30 35 3a 35 39 3a 30 31   ep 2022 05:59:01
0270  20 47 4d 54 0d 0a 0d 0a                            GMT....
```

C:\Users\ncauw\Documents\lab2.pcapng 193 total packets, 4 shown

```
No.     Time               Source                Destination           Protocol Length Info
    176 15:35:50.768891    128.119.245.12        10.5.139.22           HTTP     293    HTTP/1.1 304 Not Modified
Frame 176: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{3F3DB8EB-1AC0-401B-8543-3316F86ED445}, id 0
Ethernet II, Src: Cisco_1c:dc:fb (00:6c:bc:1c:dc:fb), Dst: RivetNet_ea:43:59 (9c:b6:d0:ea:43:59)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.5.139.22
Transmission Control Protocol, Src Port: 80, Dst Port: 50709, Seq: 1, Ack: 579, Len: 239
Hypertext Transfer Protocol
0000  9c b6 d0 ea 43 59 00 6c bc 1c dc fb 08 00 45 00   ....CY.l......E.
0010  01 17 59 f0 40 00 2f 06 e6 51 80 77 f5 0c 0a 05   ..Y.@./..Q.w....
0020  8b 16 00 50 c6 15 c2 2d e1 9f fe 69 f2 c4 50 18   ...P...-...i..P.
0030  00 ee 15 57 00 00 48 54 54 50 2f 31 2e 31 20 33   ...W..HTTP/1.1 3
0040  30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d   04 Not Modified.
0050  0a 44 61 74 65 3a 20 46 72 69 2c 20 32 33 20 53   .Date: Fri, 23 S
0060  65 70 20 32 30 32 32 20 31 35 3a 33 35 3a 35 31   ep 2022 15:35:51
0070  20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70    GMT..Server: Ap
0080  61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74   ache/2.4.6 (Cent
0090  4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e   OS) OpenSSL/1.0.
00a0  32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e   2k-fips PHP/7.4.
00b0  33 30 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e   30 mod_perl/2.0.
00c0  31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d   11 Perl/v5.16.3.
00d0  0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65   .Connection: Kee
00e0  70 2d 41 6c 69 76 65 0d 0a 4b 65 65 70 2d 41 6c   p-Alive..Keep-Al
00f0  69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20   ive: timeout=5,
0100  6d 61 78 3d 31 30 30 0d 0a 45 54 61 67 3a 20 22   max=100..ETag: "
0110  38 30 2d 35 65 39 35 31 64 66 65 62 62 34 35 62   80-5e951dfebb45b
0120  22 0d 0a 0d 0a                                    "....
```

C:\Users\ncauw\Documents\lab2.pcapng 193 total packets, 4 shown

```
No.     Time               Source                Destination           Protocol Length Info
    185 15:35:50.827530    10.5.139.22           128.119.245.12        HTTP     493    GET /favicon.ico HTTP/1.1
Frame 185: 493 bytes on wire (3944 bits), 493 bytes captured (3944 bits) on interface \Device\NPF_{3F3DB8EB-1AC0-401B-8543-3316F86ED445}, id 0
Ethernet II, Src: RivetNet_ea:43:59 (9c:b6:d0:ea:43:59), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
Internet Protocol Version 4, Src: 10.5.139.22, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50709, Dst Port: 80, Seq: 579, Ack: 240, Len: 439
Hypertext Transfer Protocol
0000  00 00 0c 07 ac 00 9c b6 d0 ea 43 59 08 00 45 00   ..........CY..E.
0010  01 df b5 2d 40 00 80 06 39 4c 0a 05 8b 16 80 77   ...-@...9L.....w
0020  f5 0c c6 15 00 50 fe 69 f2 c4 c2 2d e2 8e 50 18   .....P.i...-..P.
0030  02 01 65 06 00 00 47 45 54 20 2f 66 61 76 69 63   ..e...GET /favic
0040  6f 6e 2e 69 63 6f 20 48 54 54 50 2f 31 2e 31 0d   on.ico HTTP/1.1.
0050  0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75   .Host: gaia.cs.u
0060  6d 61 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63   mass.edu..Connec
0070  74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65   tion: keep-alive
0080  0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f   ..User-Agent: Mo
0090  7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f   zilla/5.0 (Windo
00a0  77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36   ws NT 10.0; Win6
00b0  34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 62   4; x64) AppleWeb
00c0  4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d   Kit/537.36 (KHTM
00d0  4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43   L, like Gecko) C
00e0  68 72 6f 6d 65 2f 31 30 35 2e 30 2e 30 2e 30 20   hrome/105.0.0.0
00f0  53 61 66 61 72 69 2f 35 33 37 2e 33 36 20 45 64   Safari/537.36 Ed
0100  67 2f 31 30 35 2e 30 2e 31 33 34 33 2e 34 32 0d   g/105.0.1343.42.
0110  0a 50 72 65 66 65 72 3a 20 73 61 66 65 0d 0a 41   .Prefer: safe..A
0120  63 63 65 70 74 3a 20 69 6d 61 67 65 2f 77 65 62   ccept: image/web
0130  70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 69 6d 61   p,image/apng,ima
0140  67 65 2f 73 76 67 2b 78 6d 6c 2c 69 6d 61 67 65   ge/svg+xml,image
0150  2f 2a 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 52 65   /*,*/*;q=0.8..Re
0160  66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 67 61   ferer: http://ga
0170  69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 75 2f   ia.cs.umass.edu/
0180  77 69 72 65 73 68 61 72 6b 2d 6c 61 62 73 2f 48   wireshark-labs/H
0190  54 54 50 2d 77 69 72 65 73 68 61 72 6b 2d 66 69   TTP-wireshark-fi
01a0  6c 65 31 2e 68 74 6d 6c 0d 0a 41 63 63 65 70 74   le1.html..Accept
01b0  2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c   -Encoding: gzip,
01c0  20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74    deflate..Accept
01d0  2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53   -Language: en-US
01e0  2c 65 6e 3b 71 3d 30 2e 39 0d 0a 0d 0a            ,en;q=0.9....
```

C:\Users\ncauw\Documents\lab2.pcapng 193 total packets, 4 shown

```
No.     Time               Source                Destination           Protocol Length Info
    186 15:35:50.876170    128.119.245.12        10.5.139.22           HTTP     538    HTTP/1.1 404 Not Found  (text/html)
Frame 186: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{3F3DB8EB-1AC0-401B-8543-3316F86ED445}, id 0
Ethernet II, Src: Cisco_1c:dc:fb (00:6c:bc:1c:dc:fb), Dst: RivetNet_ea:43:59 (9c:b6:d0:ea:43:59)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.5.139.22
Transmission Control Protocol, Src Port: 80, Dst Port: 50709, Seq: 240, Ack: 1018, Len: 484
Hypertext Transfer Protocol
Line-based text data: text/html (7 lines)
0000  9c b6 d0 ea 43 59 00 6c bc 1c dc fb 08 00 45 00   ....CY.l......E.
0010  02 0c 59 f1 40 00 2f 06 e5 5b 80 77 f5 0c 0a 05   ..Y.@./..[.w....
0020  8b 16 00 50 c6 15 c2 2d e2 8e fe 69 f4 7b 50 18   ...P...-...i.{P.
0030  00 f7 de 9e 00 00 48 54 54 50 2f 31 2e 31 20 34   ......HTTP/1.1 4
0040  30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 44 61   04 Not Found..Da
0050  74 65 3a 20 46 72 69 2c 20 32 33 20 53 65 70 20   te: Fri, 23 Sep
0060  32 30 32 32 20 31 35 3a 33 35 3a 35 31 20 47 4d   2022 15:35:51 GM
0070  54 0d 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68   T..Server: Apach
0080  65 2f 32 2e 34 2e 36 20 28 43 65 6e 74 4f 53 29   e/2.4.6 (CentOS)
0090  20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e 32 6b 2d    OpenSSL/1.0.2k-
00a0  66 69 70 73 20 50 48 50 2f 37 2e 34 2e 33 30 20   fips PHP/7.4.30
00b0  6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 31 31 20   mod_perl/2.0.11
00c0  50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 0a 43 6f   Perl/v5.16.3..Co
00d0  6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 32 30   ntent-Length: 20
00e0  39 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a 20 74   9..Keep-Alive: t
00f0  69 6d 65 6f 75 74 3d 35 2c 20 6d 61 78 3d 39 39   imeout=5, max=99
0100  0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65   ..Connection: Ke
0110  65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e   ep-Alive..Conten
0120  74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d   t-Type: text/htm
0130  6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38   l; charset=iso-8
0140  38 35 39 2d 31 0d 0a 0d 0a 3c 21 44 4f 43 54 59   859-1....<!DOCTY
0150  50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22   PE HTML PUBLIC "
0160  2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d   -//IETF//DTD HTM
0170  4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d   L 2.0//EN">.<htm
0180  6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e   l><head>.<title>
0190  34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74   404 Not Found</t
01a0  69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f   itle>.</head><bo
01b0  64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e   dy>.<h1>Not Foun
01c0  64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65   d</h1>.<p>The re
01d0  71 75 65 73 74 65 64 20 55 52 4c 20 2f 66 61 76   quested URL /fav
01e0  69 63 6f 6e 2e 69 63 6f 20 77 61 73 20 6e 6f 74   icon.ico was not
01f0  20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73    found on this s
0200  65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64   erver.</p>.</bod
0210  79 3e 3c 2f 68 74 6d 6c 3e 0a                     y></html>.
```