Mark Lam
Wireshark Lab: HTTP
17 September 2019

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

My browser is running HTTP/1.1

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

My browser accepts en-US, en.

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

My Ip address is: 10.18.98.174.
gaia.cs.umass.edu is 128.119.245.12

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

I get a 200 OK status code.

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

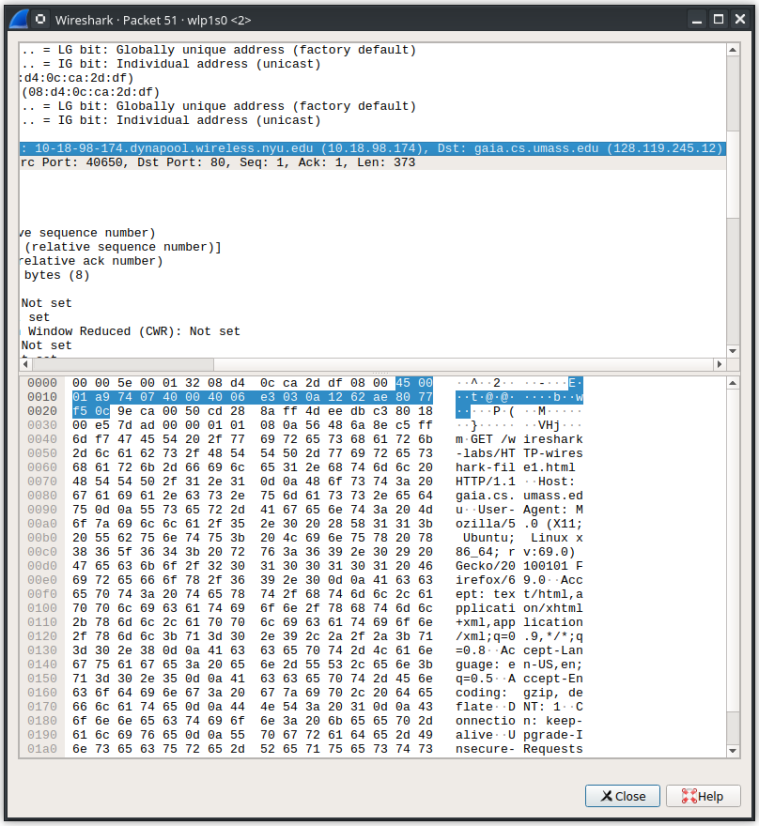
It was last modified Tue, 17 Sep 2019

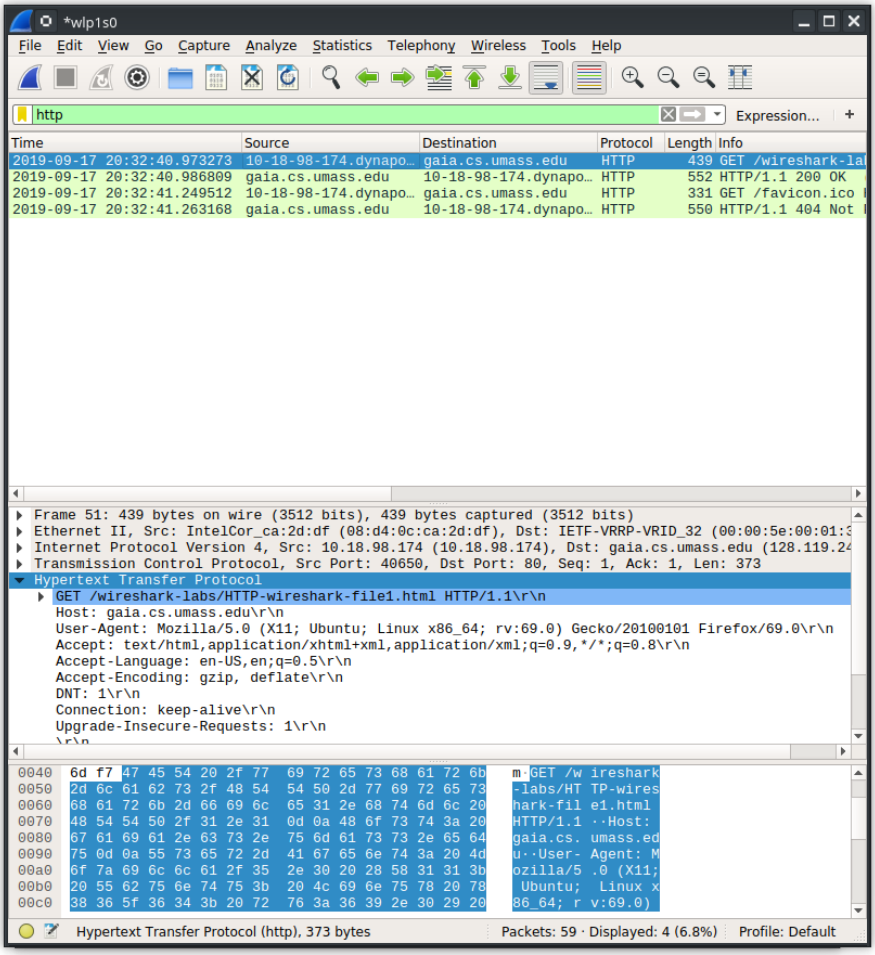
6.How many bytes of content are being returned to your browser?

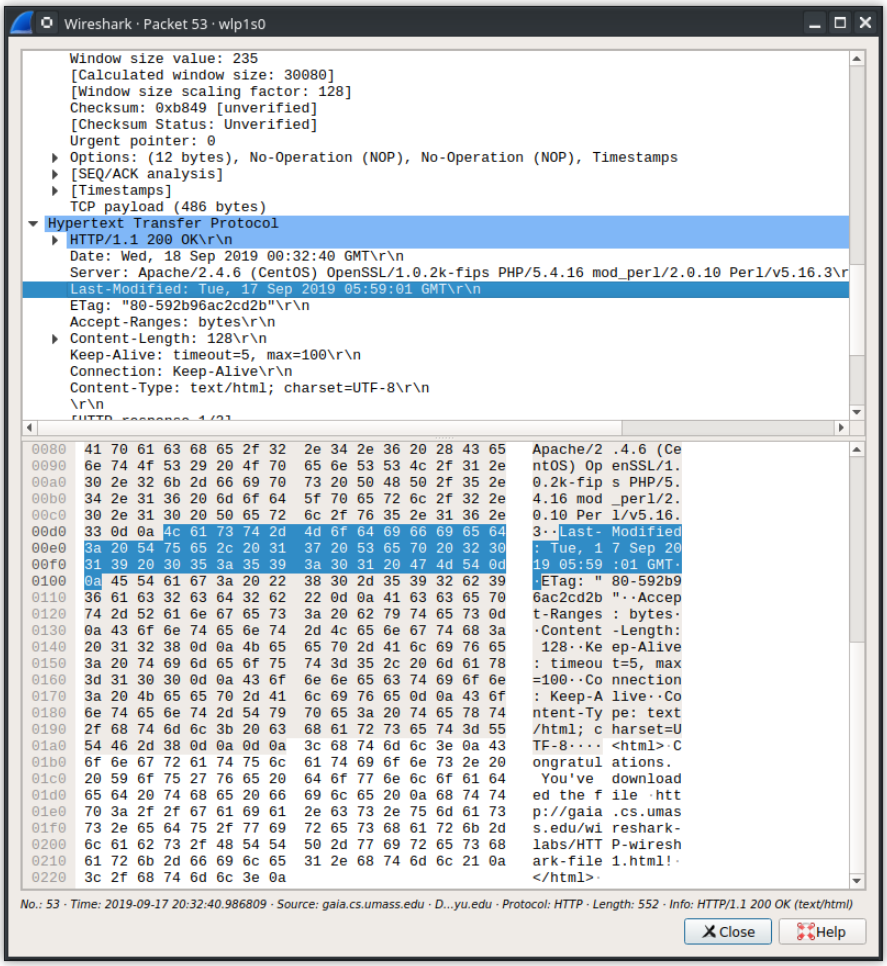
The file data size is 128 bytes.

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

All of the headers can be displayed in the raw data.


Wireshark · Packet 51 · wlp1s0 <2>
.. = LG bit: Globally unique address (factory default)
.. = IG bit: Individual address (unicast)
:d4:0c:ca:2d:df)
(08:d4:0c:ca:2d:df)
.. = LG bit: Globally unique address (factory default)
.. = IG bit: Individual address (unicast)
: 10-18-98-174.dynapool.wireless.nyu.edu (10.18.98.174), Dst: gaia.cs.umass.edu (128.119.245.12)
rc Port: 40650, Dst Port: 80, Seq: 1, Ack: 1, Len: 373
ve sequence number)
(relative sequence number)]
relative ack number)
bytes (8)
Not set
set
Window Reduced (CWR): Not set
Not set
0000 00 00 5e 00 01 32 08 d4 0c ca 2d df 08 00 45 00
0010 01 a9 74 07 40 00 40 06 e3 03 0a 12 62 ae 80 77
0020 f5 0c 9e ca 00 50 cd 28 8a ff 4d ee db c3 80 18
0030 00 e5 7d ad 00 00 01 01 08 0a 56 48 6a 8e c5 ff
0040 6d f7 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b
0050 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 72 65 73
0060 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 6d 6c 20
0070 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20
0080 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64
0090 75 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d
00a0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b
00b0 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 20 78
00c0 38 36 5f 36 34 3b 20 72 76 3a 36 39 2e 30 29 20
00d0 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46
00e0 69 72 65 66 6f 78 2f 36 39 2e 30 0d 0a 41 63 63
00f0 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61
0100 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c
0110 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e
0120 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71
0130 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e
0140 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b
0150 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e
0160 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65
0170 66 6c 61 74 65 0d 0a 44 4e 54 3a 20 31 0d 0a 43
0180 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d
0190 61 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49
01a0 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73
Close
Help


*wlp1s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
Time Source Destination Protocol Length Info
2019-09-17 20:32:40.973273 10-18-98-174.dynapo… gaia.cs.umass.edu HTTP 439 GET /wireshark-la
2019-09-17 20:32:40.986809 gaia.cs.umass.edu 10-18-98-174.dynapo… HTTP 552 HTTP/1.1 200 OK
2019-09-17 20:32:41.249512 10-18-98-174.dynapo… gaia.cs.umass.edu HTTP 331 GET /favicon.ico
2019-09-17 20:32:41.263168 gaia.cs.umass.edu 10-18-98-174.dynapo… HTTP 550 HTTP/1.1 404 Not
Frame 51: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)
Ethernet II, Src: IntelCor_ca:2d:df (08:d4:0c:ca:2d:df), Dst: IETF-VRRP-VRID_32 (00:00:5e:00:01:3
Internet Protocol Version 4, Src: 10.18.98.174 (10.18.98.174), Dst: gaia.cs.umass.edu (128.119.24
Transmission Control Protocol, Src Port: 40650, Dst Port: 80, Seq: 1, Ack: 1, Len: 373
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
DNT: 1\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
0040 6d f7 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b
0050 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 72 65 73
0060 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 6d 6c 20
0070 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20
0080 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64
0090 75 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d
00a0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b
00b0 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 20 78
00c0 38 36 5f 36 34 3b 20 72 76 3a 36 39 2e 30 29 20
m·GET /w ireshark
-labs/HT TP-wires
hark-fil e1.html
HTTP/1.1 ··Host:
gaia.cs. umass.ed
u··User- Agent: M
ozilla/5 .0 (X11;
Ubuntu; Linux x
86_64; r v:69.0)
Hypertext Transfer Protocol (http), 373 bytes
Packets: 59 · Displayed: 4 (6.8%)
Profile: Default



8.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?

If-Modified-since line does not appear in the capture.

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

The content is displayed in line-based text data field.

10.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?

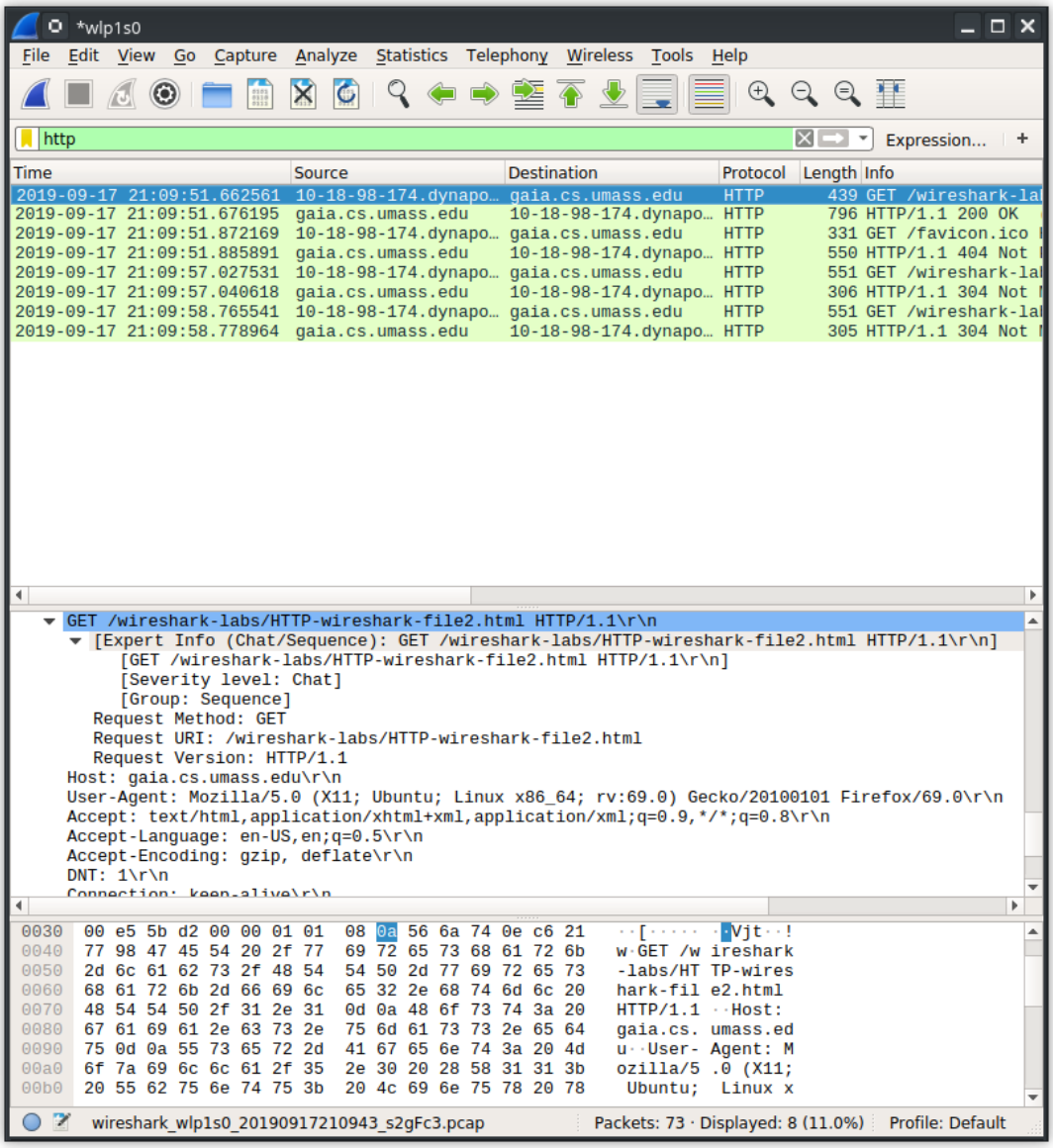
If-Modified-Since: Tue, 17 Sep 2019 05:59:01 GMT\r\n

This is the same as previous captured packet.

11.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 status code of the second response is 304 Not Modified.
The server does not return contents.

8.



12.How many HTTP GET request messages did your browser send?Which packet number in the trace contains the GET message for the Bill or Rights?

There was only one HTTP GET request. It was packet number 98 in my trace.

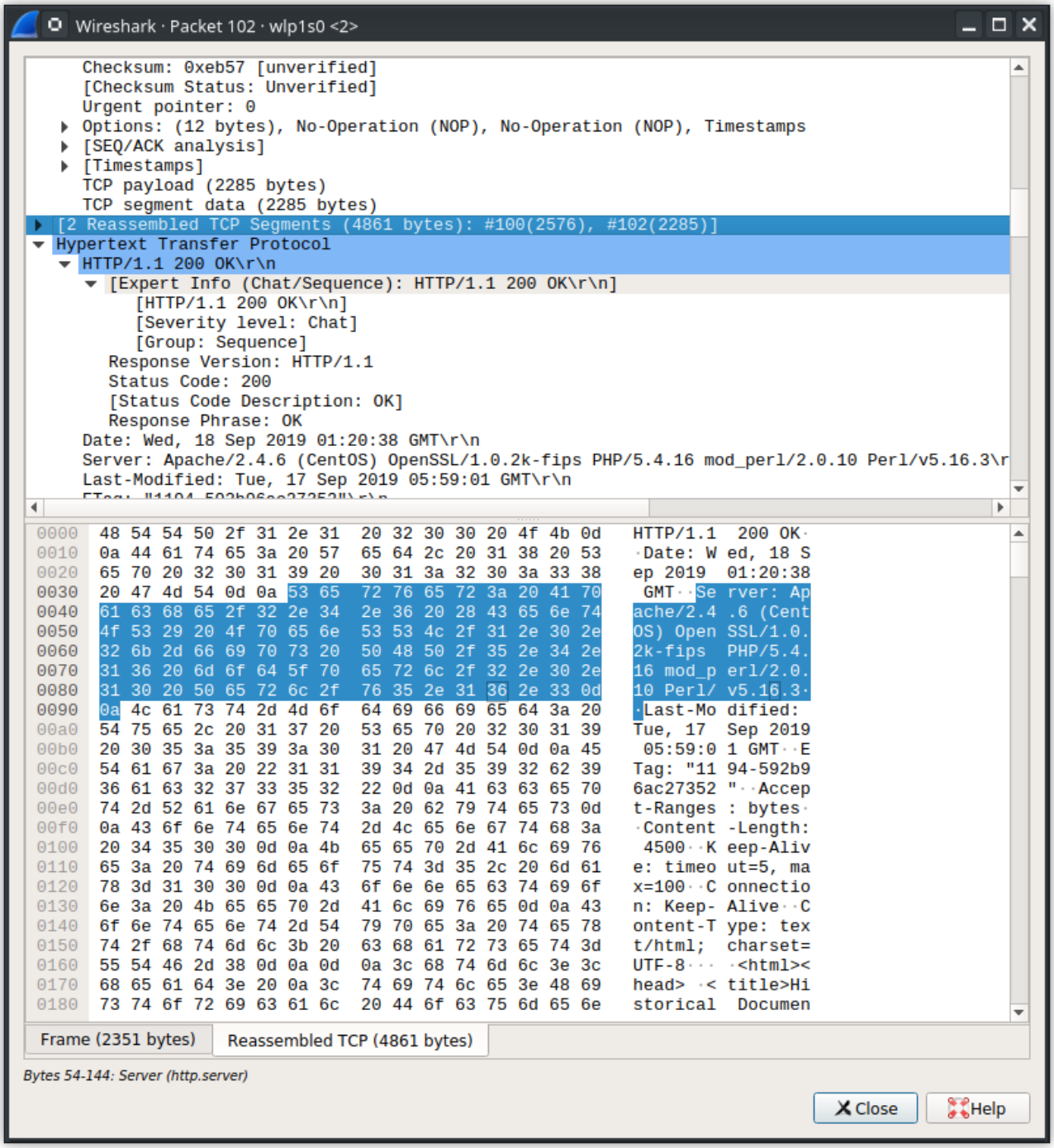
13.Which packet number inthe trace contains the status code and phrase associated with the response to the HTTP GET request?

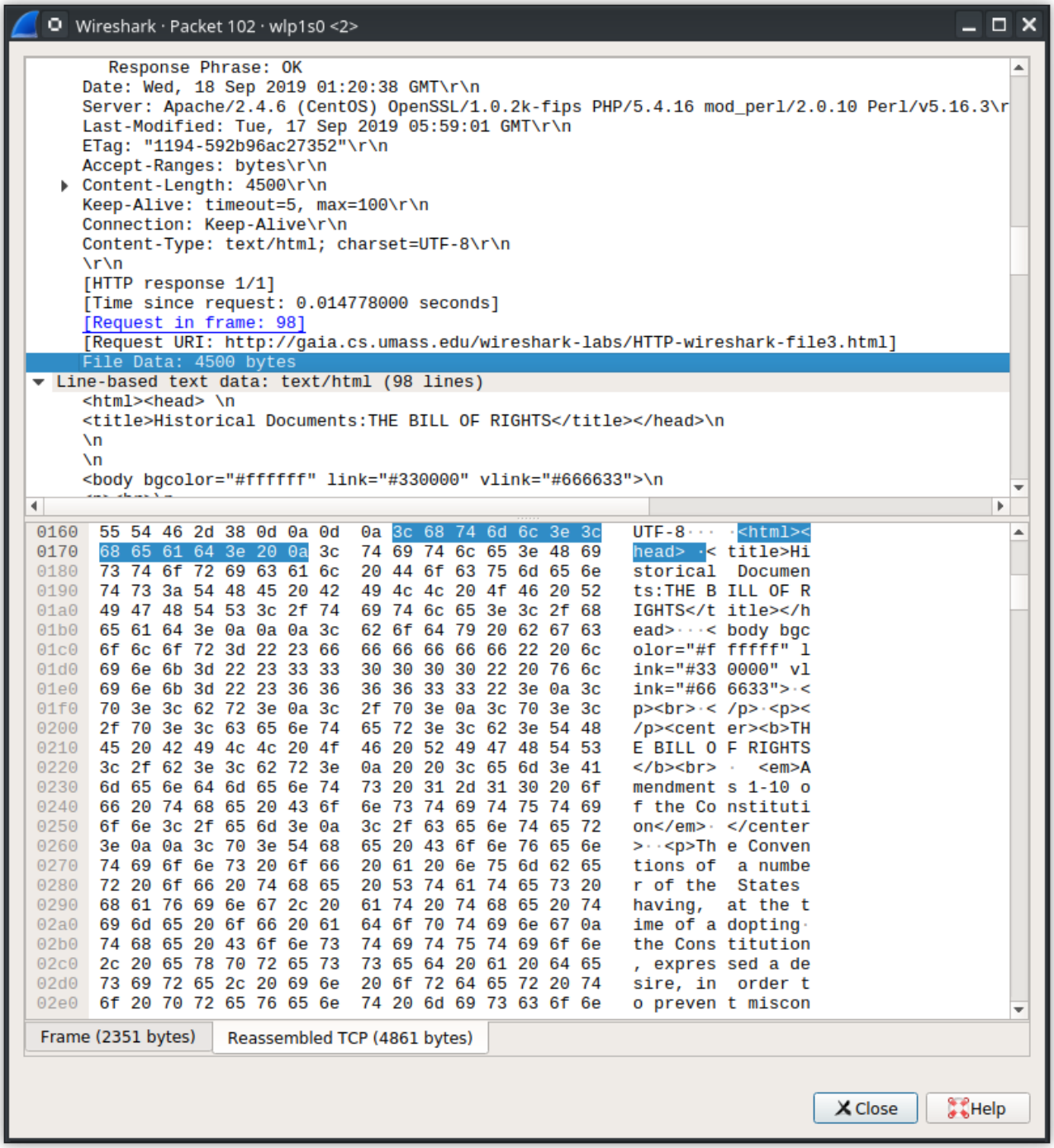
In my trace the response was packet number 102.

14.What is the status code and phrase in the response?
The status code and phrase was 200 OK

15.How many data-containing TCP segments were needed tocarry the single HTTP response and the text of theBill of Rights

There was 2 reassembled tcp segments





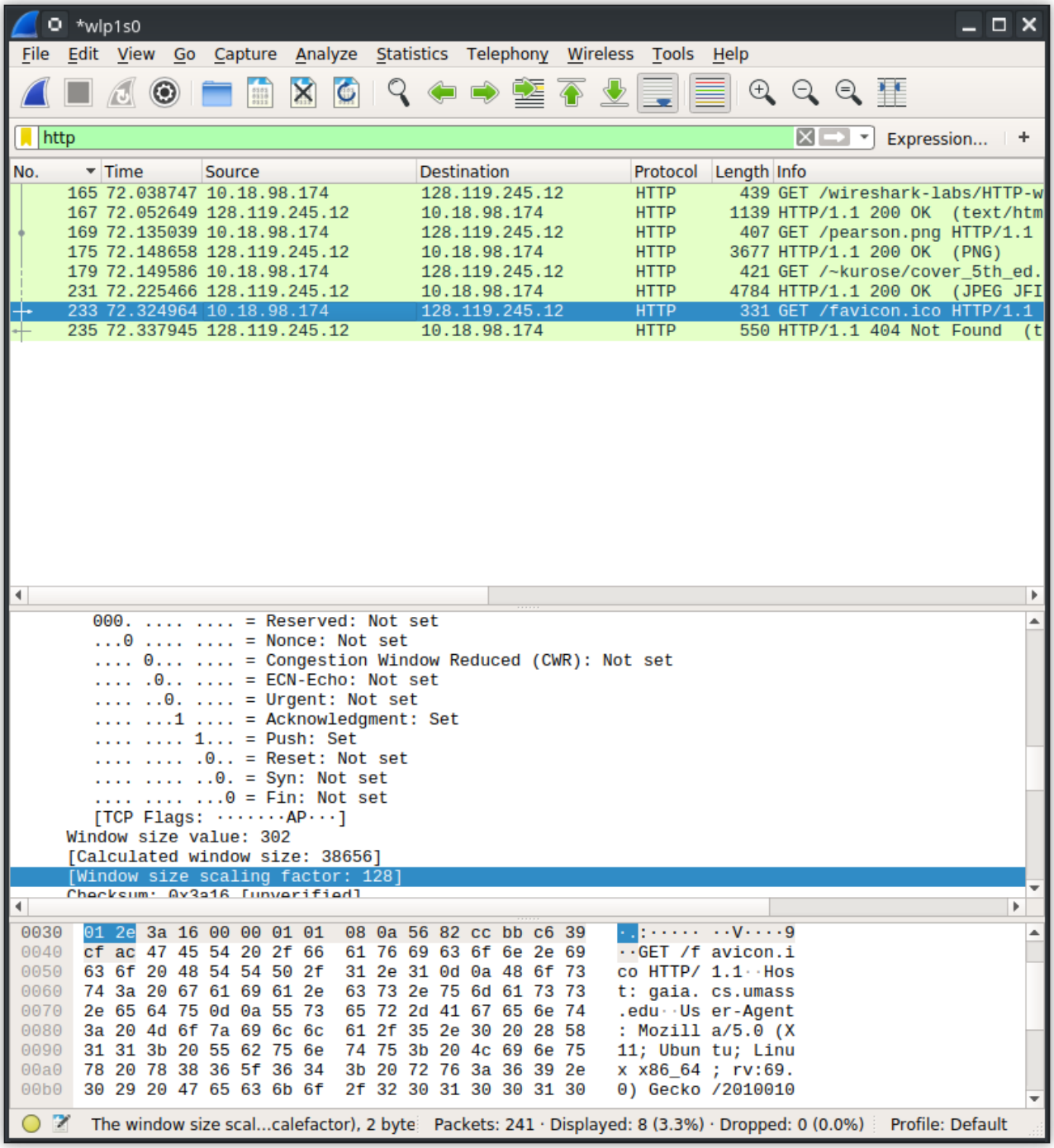
16.How many HTTP GET request messagesdid your browser send? To which Internet addresses were these GET requests sent?

My browser sent 4 HTTP GET requests.

The requests were sent to gaia.cs.umass.edu (128.119.245.12)

17.Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain

They were sent serially over two ports: 44112 and 44110.



16.

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

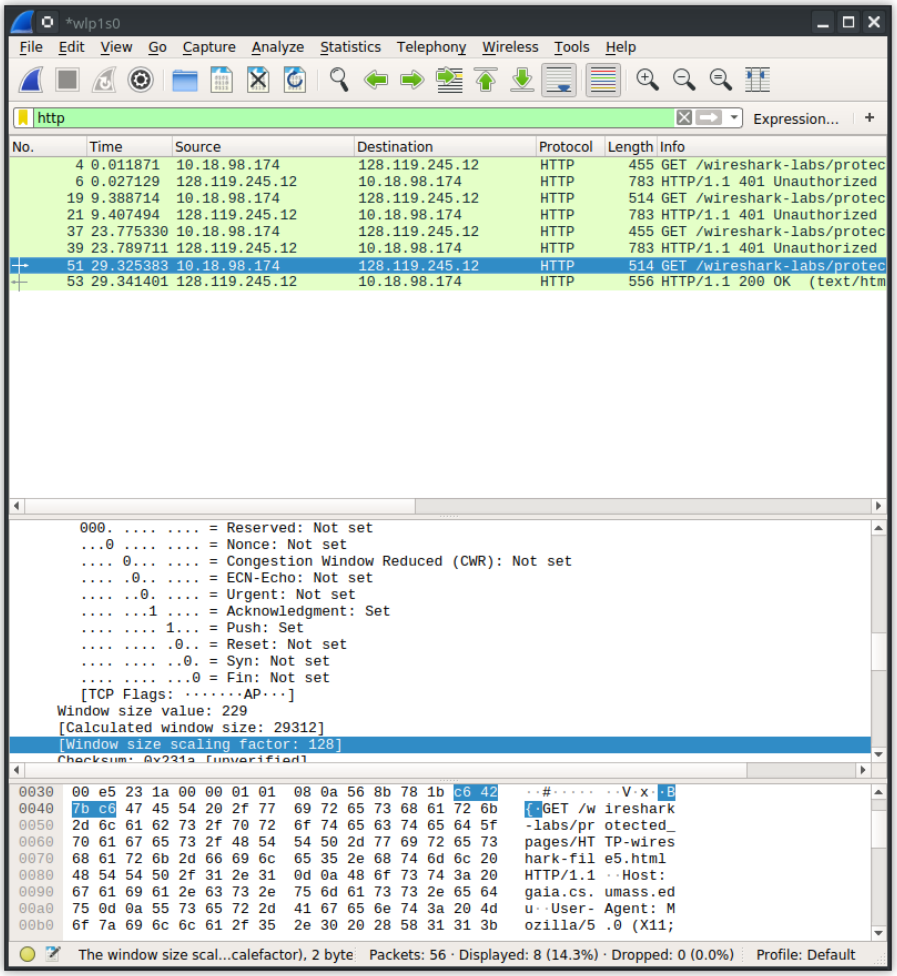
My initial response was 401 unauthorized.

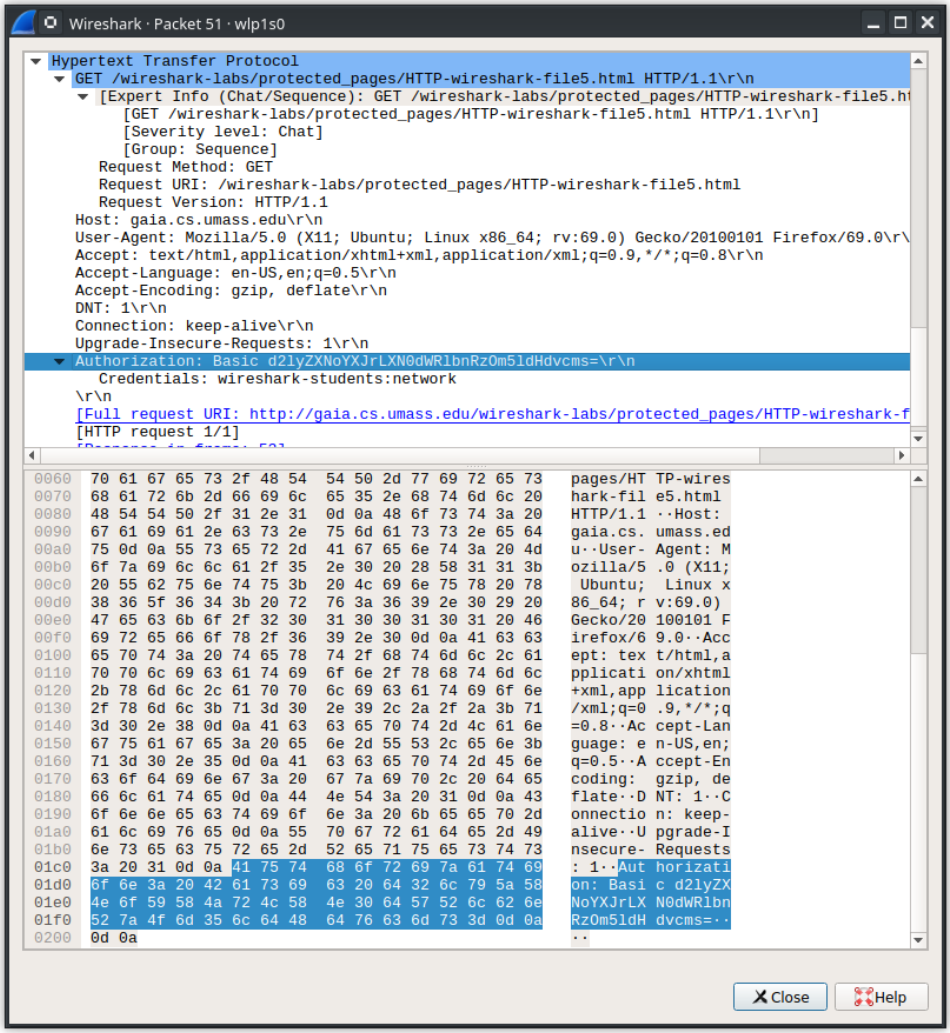
19.When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

The Authorization field dis included in the HTTP GET message. It is decoded in credentials.
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
Credentials: wireshark-students:network

18.

19.




Wireshark · Packet 51 · wlp1s0
Hypertext Transfer Protocol
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.ht
[GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0\r\
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
DNT: 1\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
Credentials: wireshark-students:network
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-f
[HTTP request 1/1]
0060 70 61 67 65 73 2f 48 54 54 50 2d 77 69 72 65 73 pages/HT TP-wires
0070 68 61 72 6b 2d 66 69 6c 65 35 2e 68 74 6d 6c 20 hark-fil e5.html
0080 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ··Host:
0090 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 gaia.cs. umass.ed
00a0 75 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d u··User- Agent: M
00b0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b ozilla/5 .0 (X11;
00c0 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 20 78 Ubuntu; Linux x
00d0 38 36 5f 36 34 3b 20 72 76 3a 36 39 2e 30 29 20 86_64; r v:69.0)
00e0 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 Gecko/20 100101 F
00f0 69 72 65 66 6f 78 2f 36 39 2e 30 0d 0a 41 63 63 irefox/6 9.0··Acc
0100 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 ept: tex t/html,a
0110 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c pplicati on/xhtml
0120 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e +xml,app lication
0130 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 /xml;q=0 .9,*/*;q
0140 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e =0.8··Ac cept-Lan
0150 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b guage: e n-US,en;
0160 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e q=0.5··A ccept-En
0170 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 coding: gzip, de
0180 66 6c 61 74 65 0d 0a 44 4e 54 3a 20 31 0d 0a 43 flate··D NT: 1··C
0190 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d onnectio n: keep-
01a0 61 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 alive··U pgrade-I
01b0 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 nsecure- Requests
01c0 3a 20 31 0d 0a 41 75 74 68 6f 72 69 7a 61 74 69 : 1··Aut horizati
01d0 6f 6e 3a 20 42 61 73 69 63 20 64 32 6c 79 5a 58 on: Basi c d2lyZX
01e0 4e 6f 59 58 4a 72 4c 58 4e 30 64 57 52 6c 62 6e NoYXJrLX N0dWRlbn
01f0 52 7a 4f 6d 35 6c 64 48 64 76 63 6d 73 3d 0d 0a RzOm5ldH dvcms=··
0200 0d 0a ··
Close
Help