

Joel Benjamin Castillo (jc5383)
 CS6843 - Computer Networking
 Prof. Rafail Portnoy

Wireshark Lab - HTTP

Section 1: The Basic HTTP GET/response Interaction

NOTE: This section of the lab was run on a different virtual machine. I accidentally destroyed my VirtualBox machine while running some updates (using Kali Linux). When I rebuilt the machine I switched over to using a **Bridged Network Adapter** as opposed to the default **Host-Only Adapter** so that I could copy the **pcapng** files from my VM to my Windows host for screenshots and further analysis using SSH. For later sections of the lab my IP address is **192.168.1.49** as opposed to **10.0.2.15**.

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

HTTP v1.1

```
> Frame 8: 454 bytes on wire (3632 bits), 454 bytes captured (3632 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 46278, Dst Port: 80, Seq: 1, Ack: 1, Len: 400
▼ 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; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 10]
```

Server: HTTP v1.1

```
> Frame 10: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0a:94:54 (08:00:27:0a:94:54)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 80, Dst Port: 46278, Seq: 1, Ack: 401, Len: 486
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 27 Sep 2018 23:54:33 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Thu, 27 Sep 2018 05:59:01 GMT\r\n
    ETag: "80-576d4091ba60c"\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
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.010581309 seconds]
    [Request in frame: 8]
```

2. What languages (if any) does your browser indicate that it can accept to the server? Languages: **en-US, en** (In that order)

```
> Frame 8: 454 bytes on wire (3632 bits), 454 bytes captured (3632 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 46278, Dst Port: 80, Seq: 1, Ack: 1, Len: 400
▼ 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; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 10]
```

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server? My Computer: **10.0.2.15**
gaia.cs.umass.edu: **128.119.245.12**

No.	Time	Source	Destination	Protocol	Length	Info
8	0.012433279	10.0.2.15	128.119.245.12	HTTP	454	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
10	0.023014588	128.119.245.12	10.0.2.15	HTTP	540	HTTP/1.1 200 OK (text/html)

```
> Frame 8: 454 bytes on wire (3632 bits), 454 bytes captured (3632 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 46278, Dst Port: 80, Seq: 1, Ack: 1, Len: 400
▼ 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; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 10]
```

4. What is the status code returned from the server to your browser? **200 OK**

```
> Frame 10: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0a:94:54 (08:00:27:0a:94:54)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 80, Dst Port: 46278, Seq: 1, Ack: 401, Len: 486
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 27 Sep 2018 23:54:33 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Thu, 27 Sep 2018 05:59:01 GMT\r\n
    ETag: "80-576d4091ba60c"\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
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.010581309 seconds]
    [Request in frame: 8]
```

5. When was the HTML file that you are retrieving last modified at the server? **Thu, 27 Sep 2018**

05:59:01 GMT

```
> Frame 10: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0a:94:54 (08:00:27:0a:94:54)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 80, Dst Port: 46278, Seq: 1, Ack: 401, Len: 486
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 27 Sep 2018 23:54:33 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Thu, 27 Sep 2018 05:59:01 GMT\r\n
    ETag: "80-576d4091ba60c"\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
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.010581309 seconds]
    [Request in frame: 8]
```

6. How many bytes of content are being returned to your browser? **128 bytes**

```
> Frame 10: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0a:94:54 (08:00:27:0a:94:54)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 80, Dst Port: 46278, Seq: 1, Ack: 401, Len: 486
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 27 Sep 2018 23:54:33 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Thu, 27 Sep 2018 05:59:01 GMT\r\n
    ETag: "80-576d4091ba60c"\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
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.010581309 seconds]
    [Request in frame: 8]
```

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. There are no additional headers shown

in the packet content window.

```
> Frame 10: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0a:94:54 (08:00:27:0a:94:54)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 80, Dst Port: 46278, Seq: 1, Ack: 401, Len: 486
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 27 Sep 2018 23:54:33 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Thu, 27 Sep 2018 05:59:01 GMT\r\n
    ETag: "80-576d4091ba60c"\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
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.010581309 seconds]
    [Request in frame: 8]
    File Data: 128 bytes
  > Line-based text data: text/html (4 lines)
```

0000	08 00 27 0a 94 54 52 54	00 12 35 02 08 00 45 00	..'.TRT ..5...E..
0010	02 0e 63 41 00 00 40 06	94 16 80 77 f5 0c 0a 00	..cA...@...w....
0020	02 0f 00 50 b4 c6 08 fa	d4 02 98 3d 61 cd 50 18	...P.... ...=a.P.
0030	ff ff 04 42 00 00 48 54	54 50 2f 31 2e 31 20 32	...B...HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 54 68 75	00 OK..D ate: Thu
0050	2c 20 32 37 20 53 65 70	20 32 30 31 38 20 32 33	, 27 Sep 2018 23
0060	3a 35 34 3a 33 33 20 47	4d 54 0d 0a 53 65 72 76	:54:33 G MT..Serv
0070	65 72 3a 20 41 70 61 63	68 65 2f 32 2e 34 2e 36	er: Apac he/2.4.6
0080	20 28 43 65 6e 74 4f 53	29 20 4f 70 65 6e 53 53	(CentOS) OpenSS
0090	4c 2f 31 2e 30 2e 32 6b	2d 66 69 70 73 20 50 48	L/1.0.2k -fips PH
00a0	50 2f 35 2e 34 2e 31 36	20 6d 6f 64 5f 70 65 72	P/5.4.16 mod_per
00b0	6c 2f 32 2e 30 2e 31 30	20 50 65 72 6c 2f 76 35	l/2.0.10 Perl/v5
00c0	2e 31 36 2e 33 0d 0a 4c	61 73 74 2d 4d 6f 64 69	.16.3..L ast-Modi
00d0	66 69 65 64 3a 20 54 68	75 2c 20 32 37 20 53 65	fied: Th u, 27 Se
00e0	70 20 32 30 31 38 20 30	35 3a 35 39 3a 30 31 20	p 2018 0 5:59:01
00f0	47 4d 54 0d 0a 45 54 61	67 3a 20 22 38 30 2d 35	GMT..ETa g: "80-5
0100	37 36 64 34 30 39 31 62	61 36 30 63 22 0d 0a 41	76d4091b a60c"..A
0110	63 63 65 70 74 2d 52 61	6e 67 65 73 3a 20 62 79	ccept-Ra nges: by
0120	74 65 73 0d 0a 43 6f 6e	74 65 6e 74 2d 4c 65 6e	tes..Con tent-Len
0130	67 74 68 3a 20 31 32 38	0d 0a 4b 65 65 70 2d 41	gth: 128 ..Keep-A
0140	6c 69 76 65 3a 20 74 69	6d 65 6f 75 74 3d 35 2c	live: ti meout=5,
0150	20 6d 61 78 3d 31 30 30	0d 0a 43 6f 6e 6e 65 63	max=100 ..Connec
0160	74 69 6f 6e 3a 20 4b 65	65 70 2d 41 6c 69 76 65	tion: Ke ep-Alive
0170	0d 0a 43 6f 6e 74 65 6e	74 2d 54 79 70 65 3a 20	..Conten t-Type:
0180	74 65 78 74 2f 68 74 6d	6c 3b 20 63 68 61 72 73	text/htm l; chars
0190	65 74 3d 55 54 46 2d 38	0d 0a 0d 0a 3c 68 74 6d	et=UTF-8<htm
01a0	6c 3e 0a 43 6f 6e 67 72	61 74 75 6c 61 74 69 6f	l>..Congr atulatio
01b0	6e 73 2e 20 20 59 6f 75	27 76 65 20 64 6f 77 6e	ns. You 've down
01c0	6c 6f 61 64 65 64 20 74	68 65 20 66 69 6c 65 20	loaded t he file
01d0	0a 68 74 74 70 3a 2f 2f	67 61 69 61 2e 63 73 2e	..http:// gaia.cs.
01e0	75 6d 61 73 73 2e 65 64	75 2f 77 69 72 65 73 68	umass.ed u/wiresh
01f0	61 72 6b 2d 6c 61 62 73	2f 48 54 54 50 2d 77 69	ark-labs /HTTP-wi
0200	72 65 73 68 61 72 6b 2d	66 69 6c 65 31 2e 68 74	reshark- file1.ht
0210	6d 6c 21 0a 3c 2f 68 74	6d 6c 3e 0a	ml!</ht ml>..

Section 2: The HTTP Conditional GET/response Interaction

- 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? No

```
> Frame 8: 454 bytes on wire (3632 bits), 454 bytes captured (3632 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 46446, Dst Port: 80, Seq: 1, Ack: 1, Len: 400
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/2]
    [Response in frame: 10]
    [Next request in frame: 14]
```

-
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell? Yes - The content is available in the packet contents window. The total size returned by the

server is 371 bytes, in 3 frames (highlighted below.)

```
> Frame 10: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface 0
> Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0a:94:54 (08:00:27:0a:94:54)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 80, Dst Port: 46446, Seq: 1, Ack: 401, Len: 730
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 29 Sep 2018 02:24:18 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Fri, 28 Sep 2018 05:59:02 GMT\r\n
    ETag: "173-576e826fdabcc"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 371\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.022995985 seconds]
  [Request in frame: 8]
  [Next request in frame: 14]
  [Next response in frame: 16]
```

```
00b0 6c 2f 32 2e 30 2e 31 30 20 50 65 72 6c 2f 76 35 1/2.0.10 Perl/v5
00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..L ast-Modi
00d0 66 69 65 64 3a 20 46 72 69 2c 20 32 38 20 53 65 fied: Fr i, 28 Se
00e0 70 20 32 30 31 38 20 30 35 3a 35 39 3a 30 32 20 p 2018 0 5:59:02
00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 31 37 33 2d GMT..ETa g: "173-
0100 35 37 36 65 38 32 36 66 64 61 62 63 63 22 0d 0a 576e826f dabcc"..
0110 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 Accept-R anges: b
0120 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 ytes..Co ntent-Le
0130 6e 67 74 68 3a 20 33 37 31 0d 0a 4b 65 65 70 2d ngth: 37 1..Keep-
0140 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 Alive: t imeout=5
0150 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 , max=10 0..Conne
0160 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 ction: K eep-Aliv
0170 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a e..Conte nt-Type:
0180 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 text/ht ml; char
0190 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 0a 3c 68 set=UTF- 8.....<h
01a0 74 6d 6c 3e 0a 0a 43 6f 6e 67 72 61 74 75 6c 61 tml>..Co ngratula
01b0 74 69 6f 6e 73 20 61 67 61 69 6e 21 20 20 4e 6f tions ag ain! No
01c0 77 20 79 6f 75 27 76 65 20 64 6f 77 6e 6c 6f 61 w you've downloa
01d0 64 65 64 20 74 68 65 20 66 69 6c 65 20 6c 61 62 ded the file lab
01e0 32 2d 32 2e 68 74 6d 6c 2e 20 3c 62 72 3e 0a 54 2-2.html . <br>..T
01f0 68 69 73 20 66 69 6c 65 27 73 20 6c 61 73 74 20 his file 's last
0200 6d 6f 64 69 66 69 63 61 74 69 6f 6e 20 64 61 74 modifica tion dat
0210 65 20 77 69 6c 6c 20 6e 6f 74 20 63 68 61 6e 67 e will n ot chang
0220 65 2e 20 30 3c 70 3e 0a 54 68 75 73 20 20 69 66 e. <p>..Thus if
0230 20 79 6f 75 20 64 6f 77 6e 6c 6f 61 64 20 74 68 you dow nload th
0240 69 73 20 6d 75 6c 74 69 70 6c 65 20 74 69 6d 65 is multi ple time
0250 73 20 6f 6e 20 79 6f 75 72 20 62 72 6f 77 73 65 s on you r browse
0260 72 2c 20 61 20 63 6f 6d 70 6c 65 74 65 20 63 6f r, a com plete co
0270 70 79 20 3c 62 72 3e 0a 77 69 6c 6c 20 6f 6e 6c py <br>..will onl
0280 79 20 62 65 20 73 65 6e 74 20 6f 6e 63 65 20 62 y be sen t once b
0290 79 20 74 68 65 20 73 65 72 76 65 72 20 64 75 65 y the se rver due
02a0 20 74 6f 20 74 68 65 20 69 6e 63 6c 75 73 69 6f to the inclusio
02b0 6e 20 6f 66 20 74 68 65 20 49 4e 2d 4d 4f 44 49 n of the IN-MODI
02c0 46 49 45 44 2d 53 49 4e 43 45 3c 62 72 3e 0a 66 FIED-SIN CE<br>..f
02d0 69 65 6c 64 20 69 6e 20 79 6f 75 72 20 62 72 6f ield in your bro
02e0 77 73 65 72 27 73 20 48 54 54 50 20 47 45 54 20 wser's H TTP GET
02f0 72 65 71 75 65 73 74 20 74 6f 20 74 68 65 20 73 request to the s
0300 65 72 76 65 72 2e 0a 0a 3c 2f 68 74 6d 6c 3e 0a erver...</html>..
```

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? Yes IF-MODIFIED-SINCE: Fri, 28 Sep 2018 05:59:02 GMT

```
> Frame 14: 523 bytes on wire (4184 bits), 523 bytes captured (4184 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 46446, Dst Port: 80, Seq: 401, Ack: 731, Len: 469
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Fri, 28 Sep 2018 05:59:02 GMT\r\n
    If-None-Match: "173-576e826fdabcc"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 8]
    [Response in frame: 16]
```

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 is **304 Not Modified** No - The contents of the file were not returned (they are not shown in the packet contents window). Since the file was not modified since the last HTTP request, the contents of the file are just

loaded from the browser cache.

```
> Frame 16: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0
> Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0a:94:54 (08:00:27:0a:94:54)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 80, Dst Port: 46446, Seq: 731, Ack: 870, Len: 239
▼ Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Sat, 29 Sep 2018 02:24:20 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-576e826fdabcc"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.023234527 seconds]
    [Prev request in frame: 8]
    [Prev response in frame: 10]
    [Request in frame: 14]
```

```
0000 08 00 27 0a 94 54 52 54 00 12 35 02 08 00 45 00 ..'.TRT..5...E.
0010 01 17 90 c2 00 00 40 06 67 8c 80 77 f5 0c 0a 00 .....@.g.w....
0020 02 0f 00 50 b5 6e 25 a0 d2 dc fd d9 96 28 50 18 ...P.n%.....(P.
0030 ff ff cd 40 00 00 48 54 54 50 2f 31 2e 31 20 33 ...@..HT TP/1.1 3
0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04 Not M odified.
0050 0a 44 61 74 65 3a 20 53 61 74 2c 20 32 39 20 53 .Date: S at, 29 S
0060 65 70 20 32 30 31 38 20 30 32 3a 32 34 3a 32 30 ep 2018 02:24:20
0070 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT..Se rver: 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) Open SSL/1.0.
00a0 32 6b 2d 66 69 70 73 20 50 48 50 2f 35 2e 34 2e 2k-fips PHP/5.4.
00b0 31 36 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 16 mod_p erl/2.0.
00c0 31 30 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 10 Perl/ v5.16.3.
00d0 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 .Connect ion: Kee
00e0 70 2d 41 6c 69 76 65 0d 0a 4b 65 65 70 2d 41 6d p-Alive: .Keep-Al
00f0 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 ive: tim eout=5,
0100 6d 61 78 3d 39 39 0d 0a 45 54 61 67 3a 20 22 31 max=99.. ETag: "1
0110 37 33 2d 35 37 36 65 38 32 36 66 64 61 62 63 63 73-576e8 26fdabcc
0120 22 0d 0a 0d 0a .....
```

Section 3: Retrieving Long Documents

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 were two **HTTP GET** requests sent by my browser. No. 49 and No. 59

No.	Time	Source	Destination	Protocol	Length	Info
49	2018-09-29 08:48:54.895692423	192.168.1.49	128.119.245.12	HTTP	423	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
57	2018-09-29 08:48:54.917970099	128.119.245.12	192.168.1.49	HTTP	583	HTTP/1.1 200 OK (text/html)
59	2018-09-29 08:48:55.032486951	192.168.1.49	128.119.245.12	HTTP	364	GET /favicon.ico HTTP/1.1
60	2018-09-29 08:48:55.062334659	128.119.245.12	192.168.1.49	HTTP	550	HTTP/1.1 404 Not Found (text/html)

The request for the Bill of Rights ([HTTP-wireshark-file3.html](http://wireshark-file3.html)) was No. 49

```
> Frame 49: 423 bytes on wire (3384 bits), 423 bytes captured (3384 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46)
> Internet Protocol Version 4, Src: 192.168.1.49, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 34960, Dst Port: 80, Seq: 1, Ack: 1, Len: 357
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    [HTTP request 1/2]
    [Response in frame: 57]
    [Next request in frame: 59]
```

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request? No. 57 contains the Response

No.	Time	Source	Destination	Protocol	Length	Info
49	2018-09-29 08:48:54.895692423	192.168.1.49	128.119.245.12	HTTP	423	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
57	2018-09-29 08:48:54.917970099	128.119.245.12	192.168.1.49	HTTP	583	HTTP/1.1 200 OK (text/html)
59	2018-09-29 08:48:55.032486951	192.168.1.49	128.119.245.12	HTTP	364	GET /favicon.ico HTTP/1.1
60	2018-09-29 08:48:55.062334659	128.119.245.12	192.168.1.49	HTTP	550	HTTP/1.1 404 Not Found (text/html)


```
> Frame 57: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0
> Ethernet II, Src: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46), Dst: PcsCompu_0a:94:54 (08:00:27:0a:94:54)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.49
> Transmission Control Protocol, Src Port: 80, Dst Port: 34960, Seq: 4345, Ack: 358, Len: 517
> [4 Reassembled TCP Segments (4861 bytes): #51(1448), #53(1448), #55(1448), #57(517)]
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 29 Sep 2018 12:48:54 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sat, 29 Sep 2018 05:59:01 GMT\r\n
    ETag: "1194-576fc44cf8a94"\r\n
    Accept-Ranges: bytes\r\n
    > Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.022277676 seconds]
```

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

No.	Time	Source	Destination	Protocol	Length	Info
49	2018-09-29 08:48:54.895692423	192.168.1.49	128.119.245.12	HTTP	423	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
57	2018-09-29 08:48:54.917970099	128.119.245.12	192.168.1.49	HTTP	583	HTTP/1.1 200 OK (text/html)
59	2018-09-29 08:48:55.032486951	192.168.1.49	128.119.245.12	HTTP	364	GET /favicon.ico HTTP/1.1
60	2018-09-29 08:48:55.062334659	128.119.245.12	192.168.1.49	HTTP	550	HTTP/1.1 404 Not Found (text/html)


```

> Frame 57: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0
> Ethernet II, Src: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46), Dst: PcsCompu_0a:94:54 (08:00:27:0a:94:54)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.49
> Transmission Control Protocol, Src Port: 80, Dst Port: 34960, Seq: 4345, Ack: 358, Len: 517
> [4 Reassembled TCP Segments (4861 bytes): #51(1448), #53(1448), #55(1448), #57(517)]
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 29 Sep 2018 12:48:54 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sat, 29 Sep 2018 05:59:01 GMT\r\n
    ETag: "1194-576fc44cf8a94"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.022277676 seconds]

```

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights? 4 TCP Segments

```

> Frame 57: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0
> Ethernet II, Src: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46), Dst: PcsCompu_0a:94:54 (08:00:27:0a:94:54)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.49
> Transmission Control Protocol, Src Port: 80, Dst Port: 34960, Seq: 4345, Ack: 358, Len: 517
> [4 Reassembled TCP Segments (4861 bytes): #51(1448), #53(1448), #55(1448), #57(517)]
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 29 Sep 2018 12:48:54 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sat, 29 Sep 2018 05:59:01 GMT\r\n
    ETag: "1194-576fc44cf8a94"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.022277676 seconds]

```

Section 4: HTML Documents with Embedded Objects

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent? 3 HTTP GET requests were sent

- No. 21 was to 128.119.245.12 - /wireshark-labs/HTTP-wireshark-file4.html
- No. 28 was to 128.119.245.12 - pearson.png

- No. 36 was to 128.119.245.12 - /~kurose/cover_5th_ed.jpg

No.	Time	Source	Destination	Protocol	Length	Info
21	2018-09-29 08:57:22.586186572	192.168.1.49	128.119.245.12	HTTP	466	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
24	2018-09-29 08:57:22.621753252	128.119.245.12	192.168.1.49	HTTP	1139	HTTP/1.1 200 OK (text/html)
28	2018-09-29 08:57:22.701303478	192.168.1.49	128.119.245.12	HTTP	423	GET /pearson.png HTTP/1.1
36	2018-09-29 08:57:22.725883125	192.168.1.49	128.119.245.12	HTTP	437	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
39	2018-09-29 08:57:22.728875714	128.119.245.12	192.168.1.49	HTTP	2229	HTTP/1.1 200 OK (PNG)
154	2018-09-29 08:57:22.843456468	128.119.245.12	192.168.1.49	HTTP	2920	HTTP/1.1 200 OK (JPEG JFIF image)


```

> Frame 21: 466 bytes on wire (3728 bits), 466 bytes captured (3728 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46)
> Internet Protocol Version 4, Src: 192.168.1.49, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 34994, Dst Port: 80, Seq: 1, Ack: 1, Len: 400
< Hypertext Transfer Protocol
  < GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
    [HTTP request 1/2]
    [Response in frame: 241

```

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. The images were downloaded serially because there were multiple TCP requests sent out for the images.

> Frame 36: 437 bytes on wire (3496 bits), 437 bytes captured (3496 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46)
> Internet Protocol Version 4, Src: 192.168.1.49, Dst: 128.119.245.12
< Transmission Control Protocol, Src Port: 34996, Dst Port: 80, Seq: 1, Ack: 1, Len: 371
Source Port: 34996
Destination Port: 80
[Stream index: 2]
[TCP Segment Len: 371]
Sequence number: 1 (relative sequence number)
[Next sequence number: 372 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1000 = Header Length: 32 bytes (8)
> Flags: 0x018 (PSH, ACK)
Window size value: 229
[Calculated window size: 29312]
[Window size scaling factor: 128]
Checksum: 0x38f7 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

> Frame 36: 437 bytes on wire (3496 bits), 437 bytes captured (3496 bits) on interface 0
> Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46)
> Internet Protocol Version 4, Src: 192.168.1.49, Dst: 128.119.245.12
< Transmission Control Protocol, Src Port: 34996, Dst Port: 80, Seq: 1, Ack: 1, Len: 371
Source Port: 34996
Destination Port: 80
[Stream index: 2]
[TCP Segment Len: 371]
Sequence number: 1 (relative sequence number)
[Next sequence number: 372 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1000 = Header Length: 32 bytes (8)
> Flags: 0x018 (PSH, ACK)
Window size value: 229
[Calculated window size: 29312]
[Window size scaling factor: 128]
Checksum: 0x38f7 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

Section 5: HTTP Authentication

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? **401 Unauthorized**

No.	Time	Source	Destination	Protocol	Length	Info
9	2018-09-29 09:00:22.536646168	192.168.1.49	128.119.245.12	HTTP	439	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
12	2018-09-29 09:00:22.560807226	128.119.245.12	192.168.1.49	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
26	2018-09-29 09:00:33.156946469	192.168.1.49	128.119.245.12	HTTP	498	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
28	2018-09-29 09:00:33.190495150	128.119.245.12	192.168.1.49	HTTP	556	HTTP/1.1 200 OK (text/html)

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message? **Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm5l**

>	Frame 26: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0
>	Ethernet II, Src: PcsCompu_0a:94:54 (08:00:27:0a:94:54), Dst: Netgear_8a:c9:46 (c0:ff:d4:8a:c9:46)
>	Internet Protocol Version 4, Src: 192.168.1.49, Dst: 128.119.245.12
>	Transmission Control Protocol, Src Port: 35006, Dst Port: 80, Seq: 1, Ack: 1, Len: 432
▼	Hypertext Transfer Protocol
>	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
	Host: gaia.cs.umass.edu\r\n
	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\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
	Connection: keep-alive\r\n
	Upgrade-Insecure-Requests: 1\r\n
>	Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm5l\r\n\r\n
	[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
	[HTTP request 1/1]
	[Response in frame: 28]