

Wireshark Lab

lukas_borges

Part I

Capturing <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> packet

No.	Time	Source	Destination	Protocol	Length	Info
3035	05:24:47.437959	10.0.0.9	239.255.255.250	SSDP	136	M-SEARCH * HTTP/1.1
3354	05:25:10.377427	10.0.0.1	239.255.255.250	SSDP	379	NOTIFY * HTTP/1.1
3355	05:25:10.380698	10.0.0.1	239.255.255.250	SSDP	324	NOTIFY * HTTP/1.1
3356	05:25:10.383841	10.0.0.1	239.255.255.250	SSDP	315	NOTIFY * HTTP/1.1
3357	05:25:10.387756	10.0.0.1	239.255.255.250	SSDP	389	NOTIFY * HTTP/1.1
3363	05:25:11.501173	10.0.0.13	128.119.245.12	HTTP	408	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3365	05:25:11.554508	128.119.245.12	10.0.0.13	HTTP	506	HTTP/1.1 200 OK (text/html)
3395	05:25:17.441307	10.0.0.9	239.255.255.250	SSDP	136	M-SEARCH * HTTP/1.1

▶	Frame 3363: 408 bytes on wire (3264 bits), 408 bytes captured (3264 bits) on interface 0
▶	Ethernet II, Src: Apple_ef:3c:a0 (78:31:c1:ef:3c:a0), Dst: Technico_57:1e:73 (44:32:c8:57:1e:73)
▶	Internet Protocol Version 4, Src: 10.0.0.13, Dst: 128.119.245.12
▶	Transmission Control Protocol, Src Port: 51199 (51199), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 342
▼	Hypertext Transfer Protocol
▼	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
▶	[Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
▶	Request Method: GET
▶	Request URI: /wireshark-labs/INTRO-wireshark-file1.html
▶	Request Version: HTTP/1.1
▶	Host: gaia.cs.umass.edu\r\n
▶	User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:44.0) Gecko/20100101 Firefox/44.0\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
▶	\r\n
▶	[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
▶	[HTTP request 1/1]
▶	[Response in frame: 3365]

0000	44 32 c8 57 1e 73 78 31	c1 ef 3c a0 08 00 45 00	D2.W.sx1 ...<...E.
0010	01 8a d1 40 40 00 40 06	e8 9c 9a 00 00 0d 80 77	...@.W
0020	f5 0c c7 ff 00 50 b6 22	16 46 b8 c4 f4 33 80 18P." .F...3..
0030	10 15 db 9a 00 00 01 01	08 0a 3a 9b 14 01 a3 f9:.....
0040	41 d2 47 45 54 20 2f 77	69 72 65 73 68 61 72 6b	A.GET /w ireshark
0050	2d 6c 61 62 73 2f 49 4e	54 52 4f 2d 77 69 72 65	-labs/IN TR0-wire
0060	73 68 61 72 6b 2d 66 69	6c 65 31 2e 68 74 6d 6c	shark-fi le1.html
0070	20 48 54 54 50 2f 31 2e	31 0d 0a 48 6f 73 74 3a	HTTP/1. 1..Host:
0080	20 67 61 69 61 2e 63 73	2e 75 6d 61 73 73 2e 65	gaia.cs .umass.e
0090	64 75 0d 0a 55 73 65 72	2d 41 67 65 6e 74 3a 20	du..User -Agent:
00a0	4d 6f 7a 69 6c 6c 61 2f	35 2e 30 20 28 4d 61 63	Mozilla/ 5.0 (Mac

1. 3 protocols: Hyper Text Transfer Protocol (HTTP), Online Certificate Status Protocol (OCSP) and Simple Service Discovery Protocol (SSDP)
2. $.554508 - .501173 = .53335$ seconds
3. gaia.cs.umass.edu IP: 128.119.245.12
my IP: 10.0.0.13

Part II

1. The basic HTTP GET/response interaction

1. HTTP 1.1
2. No language specification (Accept-language or 'en') on header

3. My browser: 10.0.0.3
Gaia: 128.119.245.12
4. 200 OK
5. Last-Modified: Sun, 28 Feb 2016 06:59:01 GMT
6. Content-length: 128 bytes
7. No extra headers

Content-Length:

No.	Time	Source	Destination	Protocol	Length	Info
11	05:50:47.414267	10.0.0.1	239.255.255.250	SSDP	379	NOTIFY * HTTP/1.1
12	05:50:47.417524	10.0.0.1	239.255.255.250	SSDP	324	NOTIFY * HTTP/1.1
13	05:50:47.420746	10.0.0.1	239.255.255.250	SSDP	315	NOTIFY * HTTP/1.1
14	05:50:47.424542	10.0.0.1	239.255.255.250	SSDP	389	NOTIFY * HTTP/1.1
15	05:50:47.426197	10.0.0.9	239.255.255.250	SSDP	136	M-SEARCH * HTTP/1.1
19	05:50:48.333188	10.0.0.13	128.119.245.12	HTTP	407	GET /wireshark-labs/HTTP-wireshark-f
21	05:50:48.391685	128.119.245.12	10.0.0.13	HTTP	554	HTTP/1.1 200 OK (text/html)

▶ Frame 21: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
▶ Ethernet II, Src: Technico_57:1e:73 (44:32:c8:57:1e:73), Dst: Apple_ef:3c:a0 (78:31:c1:ef:3c:a0)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.13
▶ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 51343 (51343), Seq: 1, Ack: 342, Len: 488
▼ Hypertext Transfer Protocol
▶ HTTP/1.1 200 OK\r\n
Date: Sun, 28 Feb 2016 10:50:48 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
Last-Modified: Sun, 28 Feb 2016 06:59:01 GMT\r\n
ETag: "80-52ccf11323a6c"\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: 0.058497000 seconds]
[\[Request in frame: 19\]](#)
▶ Line-based text data: text/html

Last-modified:

11	05:50:47.414267	10.0.0.1	239.255.255.250	SSDP	379	NOTIFY * HTTP/1.1
12	05:50:47.417524	10.0.0.1	239.255.255.250	SSDP	324	NOTIFY * HTTP/1.1
13	05:50:47.420746	10.0.0.1	239.255.255.250	SSDP	315	NOTIFY * HTTP/1.1
14	05:50:47.424542	10.0.0.1	239.255.255.250	SSDP	389	NOTIFY * HTTP/1.1
15	05:50:47.426197	10.0.0.9	239.255.255.250	SSDP	136	M-SEARCH * HTTP/1.1
19	05:50:48.333188	10.0.0.13	128.119.245.12	HTTP	407	GET /wireshark-labs/HTTP-wireshark-f
21	05:50:48.391685	128.119.245.12	10.0.0.13	HTTP	554	HTTP/1.1 200 OK (text/html)

▶	Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.13
▶	Transmission Control Protocol, Src Port: 80 (80), Dst Port: 51343 (51343), Seq: 1, Ack: 342, Len: 488
▼	Hypertext Transfer Protocol
▶	HTTP/1.1 200 OK\r\n
	Date: Sun, 28 Feb 2016 10:50:48 GMT\r\n
	Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
	Last-Modified: Sun, 28 Feb 2016 06:59:01 GMT\r\n
	ETag: "80-52ccf11323a6c"\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: 0.058497000 seconds]
	Request in frame: 19
▶	Line-based text data: text/html

0060	20 46 65 62 20 32 30 31 36 20 31 30 3a 35 30 3a	Feb 201 6 10:50:
0070	34 38 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20	48 GMT.. Server:
0080	41 70 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65	Apache/2 .4.6 (Ce
0090	6e 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e	ntOS) Op enSSL/1.
00a0	30 2e 31 65 2d 66 69 70 73 20 50 48 50 2f 35 2e	0.1e-fip s PHP/5.
00b0	34 2e 31 36 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e	4.16 mod _perl/2.
00c0	30 2e 39 64 65 76 20 50 65 72 6c 2f 76 35 2e 31	0.9dev P erl/v5.1
00d0	36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69	6.3..Las t-Modifi
00e0	65 64 3a 20 53 75 6e 2c 20 32 38 20 46 65 62 20	ed: Sun, 28 Feb
00f0	32 30 31 36 20 30 36 3a 35 39 3a 30 31 20 47 4d	2016 06: 59:01 GM
0100	54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 35 32 63	T..ETag: "80-52c
0110	63 66 31 31 33 32 33 61 36 63 22 0d 0a 41 63 63	cf11323a 6c"..Acc
0120	65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65	ept-Rang es: byte
0130	73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74	s..Conte nt-Lengt
0140	68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 6c 69	h: 128.. Keep-Ali

2. HTTP Conditional GET/response interaction:

8. No if-modified-since :

No.	Time	Source	Destination	Protocol	Length	Info
32	06:12:36.709232	10.0.0.13	128.119.245.12	HTTP	407	GET /wireshark-labs/HTTP-wireshark...
34	06:12:36.767663	128.119.245.12	10.0.0.13	HTTP	798	HTTP/1.1 200 OK (text/html)
44	06:12:40.647128	10.0.0.13	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark...
45	06:12:40.702288	128.119.245.12	10.0.0.13	HTTP	307	HTTP/1.1 304 Not Modified

▶	Frame 32: 407 bytes on wire (3256 bits), 407 bytes captured (3256 bits) on interface 0
▶	Ethernet II, Src: Apple_ef:3c:a0 (78:31:c1:ef:3c:a0), Dst: Technico_57:1e:73 (44:32:c8:57:1e:73)
▶	Internet Protocol Version 4, Src: 10.0.0.13, Dst: 128.119.245.12
▶	Transmission Control Protocol, Src Port: 51379 (51379), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 341
▼	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 (Macintosh; Intel Mac OS X 10.10; rv:44.0) Gecko/20100101 Firefox/44.0\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

0000	44 32 c8 57 1e 73 78 31	c1 ef 3c a0 08 00 45 00	D2.W.sx1 ..<...E.
0010	01 89 2c f7 40 00 40 06	8c e7 0a 00 00 0d 80 77	...@.w
0020	f5 0c c8 b3 00 50 92 dc	a4 99 d1 73 ad 64 80 18P.. ...s.d..
0030	10 15 78 e7 00 00 01 01	08 0a 3a c6 78 15 a4 24	..x..... ..:X..\$
0040	ac 1c 47 45 54 20 2f 77	69 72 65 73 68 61 72 6b	..GET /w ireshark
0050	2d 6c 61 62 73 2f 48 54	54 50 2d 77 69 72 65 73	-labs/HT TP-wires
0060	68 61 72 6b 2d 66 69 6c	65 32 2e 68 74 6d 6c 20	hark-fil e2.html
0070	48 54 54 50 2f 31 2e 31	0d 0a 48 6f 73 74 3a 20	HTTP/1.1 ..Host:
0080	67 61 69 61 2e 63 73 2e	75 6d 61 73 73 2e 65 64	gaia.cs. umass.ed
0090	75 0d 0a 55 73 65 72 2d	41 67 65 6e 74 3a 20 4d	u..User- Agent: M
00a0	6f 7a 69 6c 6c 61 2f 35	2e 30 20 28 4d 61 63 69	ozilla/5 .0 (Maci
00b0	6e 74 6f 73 68 3b 20 49	6e 74 65 6c 20 4d 61 63	ntosh; I ntel Mac
00c0	20 4f 53 20 58 20 31 30	2e 31 30 3b 20 72 76 3a	OS X 10 .10; rv:
00d0	34 34 2e 30 29 20 47 65	63 6b 6f 2f 32 30 31 30	44.0) Ge cko/2010
00e0	30 31 30 31 20 46 69 72	65 66 6f 78 2f 34 34 2e	0101 Fir efox/44.
00f0	30 0d 0a 41 63 63 65 70	74 3a 20 74 65 78 74 2f	0..Accep t: text/
0100	68 74 6d 6c 2c 61 70 70	6c 69 63 61 74 69 6f 6e	html,app lication
0110	2f 78 68 74 6d 6c 2b 78	6d 6c 2c 61 70 70 6c 69	/xhtml+x ml,appli
0120	63 61 74 69 6f 6e 2f 78	6d 6c 3b 71 3d 30 2e 39	cation/x ml;q=0.9
0130	2c 2a 2f 2a 3b 71 3d 30	2e 38 0d 0a 41 63 63 65	,/*;q=0 .8..Acce
0140	70 74 2d 4c 61 6e 67 75	61 67 65 3a 20 65 6e 2d	pt-Langu age: en-
0150	55 53 2c 65 6e 3b 71 3d	30 2e 35 0d 0a 41 63 63	US,en;q= 0.5..Acc
0160	65 70 74 2d 45 6e 63 6f	64 69 6e 67 3a 20 67 7a	ept-Enco ding: gz
0170	69 70 2c 20 64 65 66 6c	61 74 65 0d 0a 43 6f 6e	ip, defl ate..Con
0180	6e 65 63 74 69 6f 6e 3a	20 6b 65 65 70 2d 61 6c	nection: keep-al

9. Yes, the HTML code displayed on browser is present:

No.	Time	Source	Destination	Protocol	Length	Info
32	06:12:36.709232	10.0.0.13	128.119.245.12	HTTP	407	GET /wireshark-labs/HTTP-wireshark...
34	06:12:36.767663	128.119.245.12	10.0.0.13	HTTP	798	HTTP/1.1 200 OK (text/html)
44	06:12:40.647128	10.0.0.13	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark...
45	06:12:40.702288	128.119.245.12	10.0.0.13	HTTP	307	HTTP/1.1 304 Not Modified

[\[Request in frame: 32\]](#)
[\[Next request in frame: 44\]](#)
[\[Next response in frame: 45\]](#)

▼ Line-based text data: text/html
\n
<html>\n
\n
Congratulations again! Now you've downloaded the file lab2-2.html.
\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy
\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n

0190	65 78 74 2f 68 74 6d 6c	3b 20 63 68 61 72 73 65	ext/html ; charse
01a0	74 3d 55 54 46 2d 38 0d	0a 0d 0a 0a 3c 68 74 6d	t=UTF-8.<htm
01b0	6c 3e 0a 0a 43 6f 6e 67	72 61 74 75 6c 61 74 69	l>..Cong ratulati
01c0	6f 6e 73 20 61 67 61 69	6e 21 20 20 4e 6f 77 20	ons agai n! Now
01d0	79 6f 75 27 76 65 20 64	6f 77 6e 6c 6f 61 64 65	you've d ownloade
01e0	64 20 74 68 65 20 66 69	6c 65 20 6c 61 62 32 2d	d the fi le lab2-
01f0	32 2e 68 74 6d 6c 2e 20	3c 62 72 3e 0a 54 68 69	2.html. .Thi
0200	73 20 66 69 6c 65 27 73	20 6c 61 73 74 20 6d 6f	s file's last mo
0210	64 69 66 69 63 61 74 69	6f 6e 20 64 61 74 65 20	dificati on date
0220	77 69 6c 6c 20 6e 6f 74	20 63 68 61 6e 67 65 2e	will not change.
0230	20 20 3c 70 3e 0a 54 68	75 73 20 20 69 66 20 79	<p>.Th us if y
0240	6f 75 20 64 6f 77 6e 6c	6f 61 64 20 74 68 69 73	ou downl oad this
0250	20 6d 75 6c 74 69 70 6c	65 20 74 69 6d 65 73 20	multipl e times
0260	6f 6e 20 79 6f 75 72 20	62 72 6f 77 73 65 72 2c	on your browser,
0270	20 61 20 63 6f 6d 70 6c	65 74 65 20 63 6f 70 79	a compl ete copy
0280	20 3c 62 72 3e 0a 77 69	6c 6c 20 6f 6e 6c 79 20	 .wi ll only
0290	62 65 20 73 65 6e 74 20	6f 6e 63 65 20 62 79 20	be sent once by
02a0	74 68 65 20 73 65 72 76	65 72 20 64 75 65 20 74	the serv er due t
02b0	6f 20 74 68 65 20 69 6e	63 6c 75 73 69 6f 6e 20	o the in clusion
02c0	6f 66 20 74 68 65 20 49	4e 2d 4d 4f 44 49 46 49	of the I N-MODIFI

10. Yes: Sun, 28 Feb 2016 06:59:01 GMT

No.	Time	Source	Destination	Protocol	Length	Info
32	06:12:36.709232	10.0.0.13	128.119.245.12	HTTP	407	GET /wireshark-labs/HTTP-wireshark...
34	06:12:36.767663	128.119.245.12	10.0.0.13	HTTP	798	HTTP/1.1 200 OK (text/html)
44	06:12:40.647128	10.0.0.13	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark...
45	06:12:40.702288	128.119.245.12	10.0.0.13	HTTP	307	HTTP/1.1 304 Not Modified

Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:44.0) Gecko/20100101 Firefox/44.0\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
If-Modified-Since: Sun, 28 Feb 2016 06:59:01 GMT\r\n
If-None-Match: "173-52ccf1132329c"\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: 32]
[Response in frame: 45]

00d0	34 34 2e 30 29 20 47 65	63 6b 6f 2f 32 30 31 30	44.0) Gecko/2010
00e0	30 31 30 31 20 46 69 72	65 66 6f 78 2f 34 34 2e	0101 Firefox/44.
00f0	30 0d 0a 41 63 63 65 70	74 3a 20 74 65 78 74 2f	0..Accept: text/
0100	68 74 6d 6c 2c 61 70 70	6c 69 63 61 74 69 6f 6e	html,application
0110	2f 78 68 74 6d 6c 2b 78	6d 6c 2c 61 70 70 6c 69	/xhtml+xml,appli
0120	63 61 74 69 6f 6e 2f 78	6d 6c 3b 71 3d 30 2e 39	cation/x ml;q=0.9
0130	2c 2a 2f 2a 3b 71 3d 30	2e 38 0d 0a 41 63 63 65	,/*;q=0 .8..Acce
0140	70 74 2d 4c 61 6e 67 75	61 67 65 3a 20 65 6e 2d	pt-Language: en-
0150	55 53 2c 65 6e 3b 71 3d	30 2e 35 0d 0a 41 63 63	US,en;q= 0.5..Acc
0160	65 70 74 2d 45 6e 63 6f	64 69 6e 67 3a 20 67 7a	ept-Encoding: gz
0170	69 70 2c 20 64 65 66 6c	61 74 65 0d 0a 43 6f 6e	ip, deflate..Con
0180	6e 65 63 74 69 6f 6e 3a	20 6b 65 65 70 2d 61 6c	nection: keep-al
0190	69 76 65 0d 0a 49 66 2d	4d 6f 64 69 66 69 65 64	ive..If- Modified
01a0	2d 53 69 6e 63 65 3a 20	53 75 6e 2c 20 32 38 20	-Since: Sun, 28
01b0	46 65 62 20 32 30 31 36	20 30 36 3a 35 39 3a 30	Feb 2016 06:59:0
01c0	31 20 47 4d 54 0d 0a 49	66 2d 4e 6f 6e 65 2d 4d	1 GMT..I f-None-M
01d0	61 74 63 68 3a 20 22 31	37 33 2d 35 32 63 63 66	atch: "1 73-52ccf
01e0	31 31 33 32 33 32 3f 63	22 0d 0a 43 61 63 68 65	1132329c"..Cache
01f0	2d 43 6f 6e 74 72 6f 6c	3a 20 6d 61 78 2d 61 67	-Control : max-ag
0200	65 3d 30 0d 0a 0d 0a		e=0....

11. The response was a 304 Not Modified

No.	Time	Source	Destination	Protocol	Length	Info
32	06:12:36.709232	10.0.0.13	128.119.245.12	HTTP	407	GET /wireshark-labs/HTTP-wireshark...
34	06:12:36.767663	128.119.245.12	10.0.0.13	HTTP	798	HTTP/1.1 200 OK (text/html)
44	06:12:40.647128	10.0.0.13	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark...
45	06:12:40.702288	128.119.245.12	10.0.0.13	HTTP	307	HTTP/1.1 304 Not Modified

- ▶ Frame 45: 307 bytes on wire (2456 bits), 307 bytes captured (2456 bits) on interface 0
- ▶ Ethernet II, Src: Technico_57:1e:73 (44:32:c8:57:1e:73), Dst: Apple_ef:3c:a0 (78:31:c1:ef:3c:a0)
- ▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.13
- ▶ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 51379 (51379), Seq: 733, Ack: 795, Len: 241

▼ Hypertext Transfer Protocol

- ▶ HTTP/1.1 304 Not Modified\r\n

Date: Sun, 28 Feb 2016 11:12:40 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n

Connection: Keep-Alive\r\n

Keep-Alive: timeout=5, max=99\r\n

ETag: "173-52ccf1132329c"\r\n

\r\n

[HTTP response 2/2]

[Time since request: 0.055160000 seconds]

```

0000 78 31 c1 ef 3c a0 44 32 c8 57 1e 73 08 00 45 20 x1..<.D2 .W.s..E
0010 01 25 01 0c 40 00 30 06 c9 16 80 77 f5 0c 0a 00 .%.@.0. ...w....
0020 00 0d 00 50 c8 b3 d1 73 b0 40 92 dc a7 b3 80 18 ...P...s .@.....
0030 00 f3 43 8d 00 00 01 01 08 0a a4 24 bb ce 3a c6 ..C..... ..$.:.
0040 87 71 48 54 54 50 2f 31 2e 31 20 33 30 34 20 4e .qHTTP/1 .1 304 N
0050 6f 74 20 4d 6f 64 69 66 69 65 64 0d 0a 44 61 74 ot Modif ied..Dat
0060 65 3a 20 53 75 6e 2c 20 32 38 20 46 65 62 20 32 e: Sun, 28 Feb 2
0070 30 31 36 20 31 31 3a 31 32 3a 34 30 20 47 4d 54 016 11:1 2:40 GMT
0080 0d 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68 65 ..Server : Apache
0090 2f 32 2e 34 2e 36 20 28 43 65 6e 74 4f 53 29 20 /2.4.6 ( CentOS)
00a0 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e 31 65 2d 66 OpenSSL/ 1.0.1e-f
00b0 69 70 73 20 50 48 50 2f 35 2e 34 2e 31 36 20 6d ips PHP/ 5.4.16 m
00c0 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 39 64 65 76 od_perl/ 2.0.9dev
00d0 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 0a 43 Perl/v5 .16.3..C
00e0 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d onnectio n: Keep-
00f0 41 6c 69 76 65 0d 0a 4b 65 65 70 2d 41 6c 69 76 Alive..K eep-Aliv
0100 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61 e: timeo ut=5, ma
0110 78 3d 39 39 0d 0a 45 54 61 67 3a 20 22 31 37 33 x=99..ET ag: "173
0120 2d 35 32 63 63 66 31 31 33 32 33 32 39 63 22 0d -52ccf11 32329c".
0130 0a 0d 0a ...

```

This happened because the file inside the server remains unchanged in comparison to the file cached. There is no need for of another costly round-trip-time to send me something I already have.

3. Retrieving Long Documents

12. One HTTP GET

13. Packet number 9

No.	Time	Source	Destination	Protocol	Length	Info
6	14:59:05.317063	10.0.0.13	128.119.245.12	HTTP	407	GET /wireshark-labs/HTTP-wireshark...
9	14:59:05.375571	128.119.245.12	10.0.0.13	HTTP	1514	HTTP/1.1 200 OK (text/html)

</p>\n						
<p><p><center>THE BILL OF RIGHTS \n						
Amendments 1-10 of the Constitution\n						
</center>\n						
\n						
<p>The Conventions of a number of the States having, at the time of adopting\n						
the Constitution, expressed a desire, in order to prevent misconstruction\n						
or abuse of its powers, that further declaratory and restrictive clauses\n						
should be added, and as extending the ground of public confidence in the\n						
Government will best insure the beneficent ends of its institution; </p><p> Resolved, by the Senate and House of Repi						
States of America, in Congress assembled, two-thirds of both Houses concurring,\n						
that the following articles be proposed to the Legislatures of the several\n						
States, as amendments to the Constitution of the United States; all or any\n						
of which articles, when ratified by three-fourths of the said Legislatures,\n						

0200	20 62 67 63 6f 6c 6f 72	3d 22 23 66 66 66 66 66	bgcolor="#ffffff
0210	66 22 20 6c 69 6e 6b 3d	22 23 33 33 30 30 30 30	f" link= "#330000
0220	22 20 76 6c 69 6e 6b 3d	22 23 36 36 36 36 33 33	" vlink= "#666633
0230	22 3e 0a 3c 70 3e 3c 62	72 3e 0a 3c 2f 70 3e 0a	".<p><b r>.</p>.
0240	3c 70 3e 3c 2f 70 3e 3c	63 65 6e 74 65 72 3e 3c	<p></p>< center><
0250	62 3e 54 48 45 20 42 49	4c 4c 20 4f 46 20 52 49	b>THE BI LL OF RI
0260	47 48 54 53 3c 2f 62 3e	3c 62 72 3e 0a 20 20 3c	GHTS . <
0270	65 6d 3e 41 6d 65 6e 64	6d 65 6e 74 73 20 31 2d	em>Amend ments 1-
0280	31 30 20 6f 66 20 74 68	65 20 43 6f 6e 73 74 69	10 of th e Consti
0290	74 75 74 69 6f 6e 3c 2f	65 6d 3e 0a 3c 2f 63 65	tution</ em>.</ce
02a0	6e 74 65 72 3e 0a 0a 3c	70 3e 54 68 65 20 43 6f	nter>.< p>The Co
02b0	6e 76 65 6e 74 69 6f 6e	73 20 6f 66 20 61 20 6e	nvention s of a n
02c0	75 6d 62 65 72 20 6f 66	20 74 68 65 20 53 74 61	umber of the Sta
02d0	74 65 73 20 68 61 76 69	6e 67 2c 20 61 74 20 74	tes havi ng, at t
02e0	68 65 20 74 69 6d 65 20	6f 66 20 61 64 6f 70 74	he time of adopt
02f0	69 6e 67 0a 74 68 65 20	43 6f 6e 73 74 69 74 75	ing.the Constitu
0300	74 69 6f 6e 2c 20 65 78	70 72 65 73 73 65 64 20	tion, ex pressed
0310	61 20 64 65 73 69 72 65	2c 20 69 6e 20 6f 72 64	a desire , in ord
0320	65 72 20 74 6f 20 70 72	65 76 65 6e 74 20 6d 69	er to pr event mi
0330	73 63 6f 6e 73 74 72 75	63 74 69 6f 6e 0a 6f 72	sconstru ction.or

14. HTTP/1.1 200 OK

15. Data is reassembled between packets 9 through 12. 4 TCP segments total.

No.	Time	Source	Destination	Protocol	Length	Info
8	14:59:05.371820	128.119.245.12	10.0.0.13	TCP	66	[TCP Dup ACK 7#1] 80 → 51722 [ACK] Seq=1 Ack=342 Win=30080 Len=0 TSval=2785455572 TSecr=994146381
9	14:59:05.375571	128.119.245.12	10.0.0.13	HTTP	1514	HTTP/1.1 200 OK (text/html)
10	14:59:05.376825	128.119.245.12	10.0.0.13	TCP	1514	80 → 51722 [ACK] Seq=1449 Ack=342 Win=30080 Len=1448 TSval=2785455573 TSecr=994146381
11	14:59:05.376883	128.119.245.12	10.0.0.13	TCP	1514	80 → 51722 [ACK] Seq=2897 Ack=342 Win=30080 Len=1448 TSval=2785455573 TSecr=994146381
12	14:59:05.376885	128.119.245.12	10.0.0.13	TCP	585	80 → 51722 [PSH, ACK] Seq=4345 Ack=342 Win=30080 Len=519 TSval=2785455573 TSecr=994146381
13	14:59:05.376103	10.0.0.13	128.119.245.12	TCP	66	51722 → 80 [ACK] Seq=342 Ack=2897 Win=129600 Len=0 TSval=994146438 TSecr=2785455573
14	14:59:05.376149	10.0.0.13	128.119.245.12	TCP	66	51722 → 80 [ACK] Seq=342 Ack=4864 Win=127648 Len=0 TSval=994146438 TSecr=2785455573
15	14:59:05.376149	10.0.0.13	128.119.245.12	TCP	66	[TCP Window Update] 51722 → 80 [ACK] Seq=342 Ack=4864 Win=131072 Len=0 TSval=994146438 TSecr=2785455573

▶ Frame 9: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
 ▶ Ethernet II, Src: Technico_57:1e:73 (44:32:c8:57:1e:73), Dst: Apple_ef:3c:a0 (78:31:c1:ef:3c:a0)
 ▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.13
 ▶ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 51722 (51722), Seq: 1, Ack: 342, Len: 1448
 ▶ Hypertext Transfer Protocol

▼ Line-based text data: text/html
 <html><head> \n
 <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
 \n
 <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
 <p>
\n
 </p>\n
 <p><p><center>THE BILL OF RIGHTS
\n
 Amendments 1-10 of the Constitution\n
 </center>\n
 \n

01b0	6d 6c 3e 3c 68 65 61 64	3e 20 0a 3c 74 69 74 6c	ml><head > .<titl
01c0	65 3e 48 69 73 74 6f 72	69 63 61 6c 20 44 6f 63	e>Histor ical Doc
01d0	75 6d 65 6e 74 73 3a 54	48 45 20 42 49 4c 4c 20	uments:T HE BILL
01e0	4f 46 20 52 49 47 48 54	53 3c 2f 74 69 74 6c 65	OF RIGHT S</title
01f0	3e 3c 2f 68 65 61 64 3e	0a 0a 0a 3c 62 6f 64 79	></head> ...<body
0200	20 62 67 63 6f 6c 6f 72	3d 22 23 66 66 66 66 66	bgcolor="#ffffff
0210	66 22 20 6c 69 6e 6b 3d	22 23 33 33 30 30 30 30	f" link= "#330000
0220	22 20 76 6c 69 6e 6b 3d	22 23 36 36 36 36 33 33	" vlink= "#666633
0230	22 3e 0a 3c 70 3e 3c 62	72 3e 0a 3c 2f 70 3e 0a	".<p><b r>.</p>.
0240	3c 70 3e 3c 2f 70 3e 3c	63 65 6e 74 65 72 3e 3c	<p></p>< center><
0250	62 3e 54 48 45 20 42 49	4c 4c 20 4f 46 20 52 49	b>THE BI LL OF RI
0260	47 48 54 53 3c 2f 62 3e	3c 62 72 3e 0a 20 20 3c	GHTS . <
0270	65 6d 3e 41 6d 65 6e 64	6d 65 6e 74 73 20 31 2d	em>Amend ments 1-
0280	31 30 20 6f 66 20 74 68	65 20 43 6f 6e 73 74 69	10 of th e Consti
0290	74 75 74 69 6f 6e 3c 2f	65 6d 3e 0a 3c 2f 63 65	tution</ em>.</ce
02a0	6e 74 65 72 3e 0a 0a 3c	70 3e 54 68 65 20 43 6f	nter>.< p>The Co
02b0	6e 76 65 6e 74 69 6f 6e	73 20 6f 66 20 61 20 6e	nvention s of a n
02c0	75 6d 62 65 72 20 6f 66	20 74 68 65 20 53 74 61	umber of the Sta
02d0	74 65 73 20 68 61 76 69	6e 67 2c 20 61 74 20 74	tes havi ng, at t
02e0	68 65 20 74 69 6d 65 20	6f 66 20 61 64 6f 70 74	he time of adopt
02f0	69 6e 67 0a 74 68 65 20	43 6f 6e 73 74 69 74 75	ing.the Constitu
0300	74 69 6f 6e 2c 20 65 78	70 72 65 73 73 65 64 20	tion, ex pressed

4. HTML Documents with Embedded Objects

16. 4 HTTP GET request messages to:

- wireshark-labs/HTTP-wireshark-file.4html
- /assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif
- /~kurose/cover_5th_ed.jpg
- /~kurose/cover_5th_ed.jpg

19	15:37:32.924970	10.0.0.13	128.119.245.12	HTTP	407	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
21	15:37:32.980119	128.119.245.12	10.0.0.13	HTTP	1168	HTTP/1.1 200 OK (text/html)
27	15:37:33.052290	10.0.0.13	165.193.140.14	HTTP	479	GET /assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif HTTP/1.1
31	15:37:33.058381	10.0.0.13	128.119.240.90	HTTP	438	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
43	15:37:33.119001	165.193.140.14	10.0.0.13	HTTP	332	HTTP/1.1 200 OK
52	15:37:33.178297	10.0.0.13	128.119.240.90	HTTP	438	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
56	15:37:33.229597	128.119.240.90	10.0.0.13	HTTP	1514	HTTP/1.1 200 OK (JPEG JFIF image)[Malformed Packet]

17. Browser behavior gives it away since the top image loaded before the bottom image. There is no GET message requesting two images at the same time. One GET request for each image and they are satisfied serially.

5. HTTP Authentication

No.	Time	Source	Destination	Protocol	Length	Info
9	15:52:47.158902	10.0.0.13	128.119.245.12	HTTP	423	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
11	15:52:47.217153	128.119.245.12	10.0.0.13	HTTP	785	HTTP/1.1 401 Unauthorized (text/html)
35	15:52:53.507558	10.0.0.13	128.119.245.12	HTTP	482	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
37	15:52:53.562960	128.119.245.12	10.0.0.13	HTTP	558	HTTP/1.1 200 OK (text/html)

18. 401 Unauthorized

19. 200 OK