

# CSE 307 Lab 2

Aditya Balwani, SBU ID : 109353920

## I. WireShark HTTP Lab

### Part 1

1. HTTP 1.1
2. The browser accepts English (US) as mentioned in `Accept-Language: en-US,en;`
3. My IP Address : 10.245.247.201  
gaia IP Address : 128.119.245.12
4. The server returns status code 200 which is HTTP OK
5. Last-Modified: Sat, 19 Sep 2015 05:59:01 GMT
6. 128 Bytes
7. No, all the headers are found in the raw data

The image shows a Wireshark 1.12.7 capture of an HTTP GET request and response. The filter is set to 'http'. The packet list shows a GET request (frame 468) and a 200 OK response (frame 473). The packet details pane shows the structure of the HTTP request, including the Host, Accept, Upgrade-Insecure-Requests, User-Agent, Accept-Encoding, and Accept-Language headers. The raw data pane shows the hexadecimal and ASCII representation of the packet bytes.

No.	Time	Source	Destination	Protocol	Length	Info
316	2015-09-19 13:19:53.482986000	fe80::91c4:4c03:cb4ff02::c	128.119.245.12	SSDP	208	M-SEARCH * HTTP/1.1
468	2015-09-19 13:19:54.940669000	10.245.247.201	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file1.html
473	2015-09-19 13:19:54.951735000	128.119.245.12	10.245.247.201	HTTP	542	HTTP/1.1 200 OK (text/html)
586	2015-09-19 13:19:55.344654000	10.245.247.201	128.119.245.12	HTTP	433	GET /favicon.ico HTTP/1.1
589	2015-09-19 13:19:55.355531000	128.119.245.12	10.245.247.201	HTTP	540	HTTP/1.1 404 Not Found (text/html)

Frame 468: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface 0  
Ethernet II, Src: Elitegro\_76:50:b6 (ec:a8:6b:76:50:b6), Dst: Hewlett-\_63:a3:28 (b8:af:67:63:a3:28)  
Internet Protocol Version 4, Src: 10.245.247.201 (10.245.247.201), Dst: 128.119.245.12 (128.119.245.12)  
Transmission Control Protocol, Src Port: 54210 (54210), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 433  
Hypertext Transfer Protocol  
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36\r\nAccept-Encoding: gzip, deflate, sdch\r\nAccept-Language: en-US,en;q=0.8,ms;q=0.6,es;q=0.4\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]  
[HTTP request 1/2]  
[Response in frame: 473]  
[Next request in frame: 586]

0000 0b af 67 63 a3 28 ec a8 6b 76 50 b6 08 00 45 00 ..gc(.. kVP...E.  
0010 01 d9 60 38 40 00 80 06 00 00 0a f5 f7 c9 80 77 ..8a... ..w  
0020 f5 0c d3 c2 00 50 ba a2 fa 3e e3 d6 44 2d 50 18 ....P...6..p-p.  
0030 01 02 7a 0e 00 00 47 45 54 20 2f 77 69 72 65 73 ..Z...GE T/wires  
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/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.c connectio  
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 41 n: keep-alive.A  
00a0 63 65 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html  
00b0 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 ,applica tion/xht  
00c0 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 ml+xml,a pplicati  
00d0 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 on/xml;q =0.9,ima  
00e0 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 2e ge/webp, /\*;q=0.  
00f0 38 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 8..Upgra de-Insec  
0100 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d ur e-Regu ests: 1.  
0110 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a User-Ag ent: Moz  
0120 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 illa/5.0 (Window  
0130 73 20 4e 54 20 31 30 2e 30 3b 20 57 4f 57 36 34 s NT 10. 0; wow64  
0140 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 ) Applew eokit/53  
0150 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 7.36 (KH TML, lik  
0160 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f e gecko) chrome/  
0170 34 35 2e 30 2e 32 34 35 34 2e 39 33 20 53 61 66 45.0.245 4.93 Saf  
0180 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 ari/537. 36.Acce  
0190 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encod ing: gzi  
01a0 70 2c 20 64 65 66 6c 61 74 65 2c 20 73 64 63 68 p, defla te sdch  
01b0 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 .Accept -Languag  
01c0 65 3a 20 65 6e 2d 55 33 2c 65 6e 3b 71 3d 30 2e e: en-US ,en;q=0.  
01d0 38 2c 6d 73 3b 71 3d 30 2e 36 2c 65 73 3b 71 3d 8,ms;q=0 .6,es;q=  
01e0 30 2e 34 0d 0a 0d 0a 0.4....

Frame (frame), 487 bytes Packets: 1541 · Displayed: 8 (0.5%) · Load time: 0:00.035 Profile: Default

Capture.pcapng [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
316	2015-09-19 13:19:53.482986000	fe80::91c4:4c03:cb4ff02::c	128.119.245.12	SSDP	208	M-SEARCH * HTTP/1.1
468	2015-09-19 13:19:54.940669000	10.245.247.201	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file1.html
473	2015-09-19 13:19:54.951735000	128.119.245.12	10.245.247.201	HTTP	542	HTTP/1.1 200 OK (text/html)
586	2015-09-19 13:19:55.344654000	10.245.247.201	128.119.245.12	HTTP	433	GET /favicon.ico HTTP/1.1
589	2015-09-19 13:19:55.355531000	128.119.245.12	10.245.247.201	HTTP	540	HTTP/1.1 404 Not Found (text/html)

Frame 473: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0

Ethernet II, Src: Hewlett\_63:a3:28 (b8:af:67:63:a3:28), Dst: Elitegro\_76:50:b6 (ec:a8:6b:76:50:b6)

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.245.247.201 (10.245.247.201)

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 54210 (54210), Seq: 1, Ack: 434, Len: 488

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sat, 19 Sep 2015 17:19:57 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: Sat, 19 Sep 2015 05:59:01 GMT\r\n

ETag: "80-520135849b2db"\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 1/2]

[Time since request: 0.011066000 seconds]

0000 ec a8 6b 76 50 b6 b8 af 67 63 a3 28 08 00 45 00 ...kvP... gc.(.E.

0010 02 10 85 f2 40 00 36 06 44 b3 80 77 f5 0c 0a f5 ...@.6. D.w...

0020 f7 c9 00 50 d3 c2 e5 d6 44 2d ba a2 fb e7 50 18 ...P... D...P.

0030 00 7b 78 2a 00 00 48 54 54 50 2f 31 2e 31 20 32 ...{x\*..HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 00 OK..D ate: Sat

0050 2c 20 31 39 20 53 65 70 20 32 30 31 35 20 31 37 :19 Sep 2015 17

0060 3a 31 39 3a 35 37 20 47 4d 54 0d 0a 53 65 72 76 :19:57 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 31 65 2d 66 69 70 73 20 50 48 L/1.0.1e -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 39 64 65 76 20 50 65 72 6c 2f l/2.0.9d ev Perl/

00c0 76 35 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f v5.16.3. .Last-Mo

00d0 64 69 66 69 65 64 3a 20 53 61 74 2c 20 31 39 20 dified: Sat, 19

00e0 53 65 70 20 32 30 31 35 20 30 35 3a 35 39 3a 30 Sep 2015 05:59:0

00f0 31 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 1 GMT..E Tag: "80

0100 2d 35 32 30 31 33 35 38 34 39 62 32 64 62 22 0d -5201358 49b2db".

0110 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 .Accept- Ranges:

0120 62 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c bytes..C ontent-L

0130 65 6e 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 length: 1 28..Keep

0140 2d 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d -Alive: timeout=

0150 35 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 5, max=1 00..Conn

0160 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 ection: Keep-Ali

0170 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 ve..Cont ent-Type

0180 3a 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 : text/h tml; cha

0190 72 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 rset=UTF -8....<h

01a0 74 6d 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 tml>.Con gratulat

01b0 69 6f 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f ions. Y ou've do

01c0 77 6e 6c 6f 61 64 65 64 20 74 68 65 20 66 69 6c wnloaded the fil

01d0 65 20 0a 68 74 74 70 3a 2f 2f 67 61 69 61 2e 63 e .http: //gaia.c

01e0 73 2e 75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 s.umass. edu/wire

01f0 73 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d shark-la bs/HTTP-

File: "C:\Users\Aditya\Dropbox\Notes\CSE3..." Packets: 1541 · Displayed: 8 (0.5%) · Load time: 0:00.035 Profile: Default

## Part 2

1. No, the first one does not have IF-MODIFIED-SINCE
2. Yes the server explicitly returns the content of the file, since its there in the raw data
3. Yes, the second HTTP GET Request contains an IF-MODIFIED-SINCE header, and it contains the date and time of when the page was last modified
4. The server return a 304 NOT MODIFIED, and it did not explicitly return the contents of the file.

Capture 2.pcapng [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
870	2015-09-19 14:10:20.603540000	fe80::91c4:4c03:cb4ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
901	2015-09-19 14:10:20.900918000	10.245.247.201	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file2.html HT
906	2015-09-19 14:10:20.913502000	128.119.245.12	HTTP	786	HTTP/1.1 200 OK (text/html)

< >

Frame 901: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface 0

- Ethernet II, Src: Elitegro\_76:50:b6 (ec:a8:6b:76:50:b6), Dst: Hewlett-\_63:a3:28 (b8:af:67:63:a3:28)
- Internet Protocol Version 4, Src: 10.245.247.201 (10.245.247.201), Dst: 128.119.245.12 (128.119.245.12)
- Transmission Control Protocol, Src Port: 55891 (55891), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 476
- Hypertext Transfer Protocol
  - GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  - Host: gaia.cs.umass.edu\r\n
  - Connection: keep-alive\r\n
  - Pragma: no-cache\r\n
  - Cache-Control: no-cache\r\n
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n
  - Upgrade-Insecure-Requests: 1\r\n
  - User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36\r\n
  - Accept-Encoding: gzip, deflate, sdch\r\n
  - Accept-Language: en-US,en;q=0.8,ms;q=0.6,es;q=0.4\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: 906]
  - [Next request in frame: 951]

0000	b8 af 67 63 a3 28 ec a8 6b 76 50 b6 08 00 45 00	..gc(.. kVp...E..
0010	02 04 60 5f 40 00 80 06 00 00 0a f5 f7 c9 80 77	.. @... ..w
0020	f5 0c da 53 00 50 10 8f 0d 82 99 83 ae 35 50 18	..S.P... ..5p
0030	01 02 7a 39 00 00 47 45 54 20 2f 77 69 72 65 73	..29..GE T /wires
0040	68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77	hark-lab s/HTTP-w
0050	69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68	reshark -file2.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..C connectio
0090	6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 50	n: keep-alive..P
00a0	72 61 67 6d 61 3a 20 6e 6f 2d 63 61 63 68 65 0d	ragma: n o-cache.
00b0	0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20	.Cache-C ontrol:
00c0	6e 6f 2d 63 61 63 68 65 0d 0a 41 63 63 65 70 74	no-cache ..Accept
00d0	3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c	: text/h tml,appl
00e0	69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d	ication/ xhtml+xml
00f0	6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d	l,applic ation/xml
0100	6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65	l;q=0.9, image/we
0110	62 70 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 55 70	bp,*/*;q =0.8..up
0120	67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52	grade-In secure-R
0130	65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72	quests: 1..User
0140	2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f	-Agent: Mozilla/
0150	35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20	5.0 (Win dows NT
0160	31 30 2e 30 3b 20 57 4f 57 36 34 29 20 41 70 70	10.0; wo w64) App
0170	6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20	lewebkit /537.36
0180	28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63	(KHTML, like Gec
0190	6b 6f 29 20 43 68 72 6f 6d 65 2f 34 35 2e 30 2e	ko) Chro me/45.0.
01a0	32 34 35 34 2e 39 33 20 53 61 66 61 72 69 2f 35	2454.93 Safari/5
01b0	33 37 2e 33 36 0d 0a 41 63 63 63 70 74 2d 45 6e	37.36..A ccept-En
01c0	63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65	coding: gzip, de
01d0	66 6c 61 74 65 2c 20 73 64 63 68 0d 0a 41 63 63	flate, s dch..Acc
01e0	65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e	pt-Lang uage: en

Frame (frame), 530 bytes Packets: 2666 · Displayed: 17 (0.6%) · Load time: 0:00.039 Profile: Default

Capture 2.pcapng [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
870	2015-09-19 14:10:20.603540000	fe80::91c4:4c03:cb4ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
901	2015-09-19 14:10:20.900918000	10.245.247.201	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
906	2015-09-19 14:10:20.913502000	128.119.245.12	HTTP	786	HTTP/1.1 200 OK (text/html)

< >

Frame 906: 786 bytes on wire (6288 bits), 786 bytes captured (6288 bits) on interface 0

- Ethernet II, Src: Hewlett\_63:a3:28 (b8:af:67:63:a3:28), Dst: Elitegro\_76:50:b6 (ec:a8:6b:76:50:b6)
- Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.245.247.201 (10.245.247.201)
- Transmission Control Protocol, Src Port: 80 (80), Dst Port: 55891 (55891), Seq: 1, Ack: 477, Len: 732
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
    - Date: Sat, 19 Sep 2015 18:10:23 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: Sat, 19 Sep 2015 05:59:01 GMT\r\n
    - Etag: "173-520135849a723"\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: 0.012584000 seconds]
    - [\[Request in frame: 901\]](#)
    - [\[Next request in frame: 951\]](#)
    - [\[Next response in frame: 955\]](#)
  - Line-based text data: text/html
    - \n
    - <html>\n
    - \n
    - Congratulations again! Now you've downloaded the file lab2-2.html. <br>\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 <br>\n
    - will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    - field in your browser's HTTP GET request to the server.\n
    - \n
    - </html>\n

0130 4c 65 6e 67 74 68 3a 20 33 37 31 0d 0a 4b 65 65 Length: 371..Keep-Alive: timeout=5, max=100..Connection: Keep-Alive..Content-Type: text/html; charset=UTF-8....<html>... Congratulations again! Now you've downloaded the file lab2-2.html. <br> This file's last modification date will not change. <p> Thus if you download this multiple times on your browser, a complete copy <br> will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE field in your browser's HTTP GET request to the server. </html>

Response line (http.response.line), 32 bytes Packets: 2666 · Displayed: 17 (0.6%) · Load time: 0:00.039 Profile: Default

Capture 2.pcapng [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
1924	2015-09-19 14:10:26.603472000	fe80::91c4:4c03:cb4ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
2024	2015-09-19 14:10:27.809123000	10.245.247.178	SSDP	175	M-SEARCH * HTTP/1.1
2041	2015-09-19 14:10:28.084373000	10.245.247.201	HTTP	599	GET /wireshark-labs/HTTP-wireshark-file2.html HT
2043	2015-09-19 14:10:28.097166000	128.119.245.12	HTTP	296	HTTP/1.1 304 Not Modified

Frame 2041: 599 bytes on wire (4792 bits), 599 bytes captured (4792 bits) on interface 0

Ethernet II, Src: Elitegro\_76:50:b6 (ec:a8:6b:76:50:b6), Dst: Hewlett-\_63:a3:28 (b8:af:67:63:a3:28)

Internet Protocol Version 4, Src: 10.245.247.201 (10.245.247.201), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 55904 (55904), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 545

Hypertext Transfer Protocol

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

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36\r\n

Accept-Encoding: gzip, deflate, sdch\r\n

Accept-Language: en-US,en;q=0.8,ms;q=0.6,es;q=0.4\r\n

If-None-Match: "173-520135849a723"\r\n

If-Modified-Since: Sat, 19 Sep 2015 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: 2043]

0000 b8 af 67 63 a3 28 ec a8 6b 76 50 b6 08 00 45 00 ..gc.(...kvp...E.

0010 02 49 60 67 40 00 80 06 00 00 0a f5 f7 c9 80 77 .I g@... ..w

0020 f5 0c da 60 00 50 e3 b0 4b c5 84 fc 07 5a 50 18 ...P...K...ZP.

0030 01 02 7a 7e 00 00 47 45 54 20 2f 77 69 72 65 73 ..Z...GE T /wires

0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w

0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68 ireshark -file2.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..C onnectio

0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 n: keep- alive..C

00a0 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 ache-con trol: ma

00b0 78 2d 61 67 65 3d 30 0d 0a 41 63 63 65 70 74 3a x-age=0. .Accept:

00c0 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 text/ht ml,appli

00d0 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c cation/x tml+xml

00e0 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c ,applica tion/xml

00f0 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65 62 ;q=0.9,i mage/web

0100 70 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 55 70 67 p,\*/\*;q= 0.8..Upg

0110 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 rade-Ins ecore-Re

0120 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d quests: 1..user-

0130 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: M ozilla/5

0140 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 .0 (wind ows NT 1

0150 30 2e 30 3b 20 57 4f 57 36 34 29 20 41 70 70 6c 0.0; WOW 64) Appl

0160 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 ewebKit/ 537.36 (

0170 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b KHTML, l ike Geck

0180 6f 29 20 43 68 72 6f 6d 65 2f 34 35 2e 30 2e 32 o) Chrom e/45.0.2

0190 34 35 34 2e 39 33 20 53 61 66 61 72 69 2f 35 33 454.93 s afari/53

01a0 37 2e 33 36 0d 0a 41 63 63 65 70 74 2d 45 6e 63 7.36..Ac cept-Enc

01b0 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 oding: g zip, def

01c0 6c 61 74 65 2c 20 73 64 63 68 0d 0a 41 63 63 65 late, sd ch..Acce

01d0 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d nt-l anguage: en-

File: "C:\Users\Aditya\Dropbox\Notes\CSE3..." Packets: 2666 · Displayed: 17 (0.6%) · Load time: 0:00.039 Profile: Default



Capture 2.pcapng [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **http** Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
1924	2015-09-19 14:10:26.003472000	10.245.247.201	SSDP	208	M-SEARCH * HTTP/1.1
2024	2015-09-19 14:10:27.809123000	10.245.247.178	SSDP	175	M-SEARCH * HTTP/1.1
2041	2015-09-19 14:10:28.084373000	10.245.247.201	HTTP	599	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2043	2015-09-19 14:10:28.097166000	128.119.245.12	HTTP	296	HTTP/1.1 304 Not Modified

< >

Frame 2043: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface 0

Ethernet II, Src: Hewlett\_63:a3:28 (b8:af:67:63:a3:28), Dst: Elitegro\_76:50:b6 (ec:a8:6b:76:50:b6)

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.245.247.201 (10.245.247.201)

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 55904 (55904), Seq: 1, Ack: 546, Len: 242

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

Date: Sat, 19 Sep 2015 18:10:31 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=100\r\n

ETag: "173-520135849a723"\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.012793000 seconds]

[\[Request in frame: 2041\]](#)

```

0000  ec a8 6b 76 50 b6 b8 af 67 63 a3 28 08 00 45 00  ..kvP... gc(...E.
0010  01 1a b0 a8 40 00 36 06 1a f3 80 77 f5 0c 0a f5  ...@.6. ...w...
0020  f7 c9 00 50 da 60 84 fc 07 5a e3 b0 4d e6 50 18  ...P... .Z..M.P.
0030  00 7b bc 6e 00 00 48 54 54 50 2f 31 2e 31 20 33  ...n..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 31 39 20 53  .Date: s at, 19 s
0060  65 70 20 32 30 31 35 20 31 38 3a 31 30 3a 33 31  ep 2015 18:10:31
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  31 65 2d 66 69 70 73 20 50 48 50 2f 35 2e 34 2e  1e-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  39 64 65 76 20 50 65 72 6c 2f 76 35 2e 31 36 2e  9dev Per l/v5.16.
00d0  33 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b  3..Conne ction: K
00e0  65 65 70 2d 41 6c 69 76 65 0d 0a 4b 65 65 70 2d  eep-Aliv e..Keep-
00f0  41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35  Alive: t imeout=5
0100  2c 20 6d 61 78 3d 31 30 30 0d 0a 45 54 61 67 3a  , max=10 0 .ETag:
0110  20 22 31 37 33 2d 35 32 30 31 33 35 38 34 39 61  "173-52 0135849a
0120  37 32 33 22 0d 0a 0d 0a 723"....

```

File: "C:\Users\Aditya\Dropbox\Notes\CSE3..." Packets: 2666 · Displayed: 17 (0.6%) · Load time: 0:00.039 Profile: Default

## Part 3

1. The Browser sent 1 HTTP GET request which is packet number 1945
2. Packet number 1953 in the trace contains the status code and phrase associated with the response to the HTTP GET request.
3. Status Code 200, Phrase : HTTP OK
4. 4 TCP Segments

Capture 3.pcapng [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
1458	2015-09-19 14:27:14.137776000	10.245.247.178	239.255.255.250	SSDP	169 M-SEARCH * HTTP/1.1
1564	2015-09-19 14:27:15.345386000	10.245.247.179	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
1614	2015-09-19 14:27:16.651033000	fe80::91c4:4c03:cb4ff02::c		SSDP	208 M-SEARCH * HTTP/1.1
1945	2015-09-19 14:27:19.864705000	10.245.247.201	128.119.245.12	HTTP	487 GET /wireshark-labs/HTTP-wireshark-file3.html HT
1953	2015-09-19 14:27:19.875960000	128.119.245.12	10.245.247.201	HTTP	777 HTTP/1.1 200 OK (text/html)
2302	2015-09-19 14:27:20.651197000	fe80::91c4:4c03:cb4ff02::c		SSDP	208 M-SEARCH * HTTP/1.1
2694	2015-09-19 14:27:23.651246000	fe80::91c4:4c03:cb4ff02::c		SSDP	208 M-SEARCH * HTTP/1.1

< >

Frame 1945: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface 0

Ethernet II, Src: Elitegro\_76:50:b6 (ec:a8:6b:76:50:b6), Dst: Hewlett-\_63:a3:28 (b8:af:67:63:a3:28)

Internet Protocol Version 4, Src: 10.245.247.201 (10.245.247.201), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 56536 (56536), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 433

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36\r\n

Accept-Encoding: gzip, deflate, sdch\r\n

Accept-Language: en-US,en;q=0.8,ms;q=0.6,es;q=0.4\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]

[HTTP request 1/1]

[Response in frame: 1953]

Offset	Hex	ASCII
0000	b8 af 67 63 a3 28 ec a8 6b 76 50 b6 08 00 45 00	..gc.(. kVp...E.
0010	01 d9 60 75 40 00 80 06 00 00 0a f5 f7 c9 80 77	..u@... ..w
0020	f5 0c dc d8 00 50 c1 f4 7b 87 bb 6e 52 b6 50 18	....P.. {..r.P.
0030	01 02 7a 0e 00 00 47 45 54 20 2f 77 69 72 65 73	..Z...GE T /wires
0040	68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77	hark-lab s/HTTP-w
0050	69 72 65 73 68 61 72 6b 2d 66 69 6c 65 33 2e 68	hreshark -file3.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..C onnectio
0090	6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 41	n: keep-alive..A
00a0	63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c	ccept: t ext/html
00b0	2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74	, applica tion/xht
00c0	6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69	ml+xml,a pplicati
00d0	6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61	on/xml;q =0.9,ima
00e0	67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 2e	ge/webp, /*;q=0.
00f0	38 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63	8..Upgra de-Insec
0100	75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d	ure-Requ ests: 1.
0110	0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a	.User-Ag ent: Moz
0120	69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77	illa/5.0 (window
0130	73 20 4e 54 20 31 30 2e 30 3b 20 57 4f 57 36 34	s NT 10. 0; WOW64
0140	29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33	) Applew ebkit/53
0150	37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b	7.36 (KH TML, lik
0160	55 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f	e Gecko) Chrome/
0170	34 35 2e 30 2e 32 34 35 34 2e 39 33 20 53 61 66	45.0.245 4.93 Saf
0180	61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65	ari/537. 36..Acce
0190	70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69	pt-Encod ing: gzi
01a0	70 2c 20 64 65 66 6c 61 74 65 2c 20 73 64 63 68	p, defla te, sdch
01b0	0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67	..Accept -Languag
01c0	65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e	e: en-US ,en;q=0.
01d0	38 7c 6d 73 3b 71 3d 30 2e 65 73 3b 71 3d	8 ms-n-n & ac-n

File: "C:\Users\Aditya\Dropbox\Notes\CSE3... Packets: 2794 · Displayed: 9 (0.3%) · Load time: 0:00.063 Profile: Default

Capture 3.pcapng [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **http** Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
1458	2015-09-19 14:27:14.137776000	10.245.247.178	SSDP	169	M-SEARCH * HTTP/1.1
1564	2015-09-19 14:27:15.345386000	10.245.247.179	SSDP	175	M-SEARCH * HTTP/1.1
1614	2015-09-19 14:27:16.651033000	fe80::91c4:4c03:cb4ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
1945	2015-09-19 14:27:19.864705000	10.245.247.201	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file3.html HT
1953	2015-09-19 14:27:19.875960000	128.119.245.12	HTTP	777	HTTP/1.1 200 OK (text/html)
2302	2015-09-19 14:27:20.651197000	fe80::91c4:4c03:cb4ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
2694	2015-09-19 14:27:23.651246000	fe80::91c4:4c03:cb4ff02::c	SSDP	208	M-SEARCH * HTTP/1.1

< >

Frame 1953: 777 bytes on wire (6216 bits), 777 bytes captured (6216 bits) on interface 0

- Ethernet II, Src: Hewlett\_63:a3:28 (b8:af:67:63:a3:28), Dst: Elitegro\_76:50:b6 (ec:a8:6b:76:50:b6)
- Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.245.247.201 (10.245.247.201)
- Transmission Control Protocol, Src Port: 80 (80), Dst Port: 56536 (56536), Seq: 4141, Ack: 434, Len: 723
- [4 Reassembled TCP Segments (4863 bytes): #1949(1380), #1950(1380), #1952(1380), #1953(723)]
- [Frame: 1949, payload: 0-1379 (1380 bytes)]
- [Frame: 1950, payload: 1380-2759 (1380 bytes)]
- [Frame: 1952, payload: 2760-4139 (1380 bytes)]
- [Frame: 1953, payload: 4140-4862 (723 bytes)]
- [Segment count: 4]
- [Reassembled TCP length: 4863]
- [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053...]
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
    - Date: Sat, 19 Sep 2015 18:27:22 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: Sat, 19 Sep 2015 05:58:01 GMT\r\n

< >

0000	ec a8 6b 76 50 b6 b8 af	67 63 a3 28 08 00 45 00	..kvp... gc.(.E.
0010	02 fb ee b4 40 00 36 06	db 05 80 77 f5 0c 0a f5	....@.6. ....w....
0020	f7 c9 00 50 dc d8 bb 6e	62 e2 c1 f4 7d 38 50 18	...P...n b...}8P.
0030	00 7b fc 14 00 00 72 74	20 6f 66 20 74 68 65 20	{.....rt of the
0040	55 6e 69 74 65 64 20 53	74 61 74 65 73 2c 20 74	United s tates, t
0050	68 61 6e 20 61 63 63 6f	72 64 69 6e 67 0a 74 6f	han acco rding.to
0060	20 74 68 65 20 72 73 6c	65 73 20 6f 66 20 74 68	the rul es of th
0070	65 20 63 6f 6d 6d 6f 6e	20 6c 61 77 2e 0a 0a 3c	e common law...<
0080	2f 70 3e 3c 70 3e 3c 61	20 6e 61 6d 65 3d 22 38	/p><p><a name='8
0090	22 3e 3c 73 74 72 6f 6e	67 3e 3c 68 33 3e 41 6d	/><strong g><h3>Am
00a0	65 6e 64 6d 65 6e 74 20	56 49 49 49 3c 2f 68 33	endment VIII</h3>
00b0	3e 3c 2f 73 74 72 6f 6e	67 3e 3c 2f 61 3e 0a 0a	<</strong g></a>...
00c0	3c 70 3e 3c 2f 70 3e 3c	70 3e 45 78 63 65 73 73	<p></p>< p>Excess
00d0	69 76 65 20 62 61 69 6c	20 73 68 61 6c 6c 20 6e	ive bail shall n
00e0	6f 74 20 62 65 20 72 65	71 75 69 72 65 64 2c 20	ot be re quired fi
00f0	6e 6f 72 20 65 78 63 65	73 73 69 76 65 20 66 69	nor exce ssive fi
0100	6e 65 73 0a 69 6d 70 6f	73 65 64 2c 20 6e 6f 72	nes.impo sed, nor
0110	20 63 72 75 65 6c 20 61	6e 64 20 75 6e 75 73 75	cruel a nd unusu
0120	61 6c 20 70 75 6e 69 73	68 6d 65 6e 74 73 20 69	al punis hments i
0130	6e 66 6c 69 63 74 65 64	2e 0a 0a 3c 2f 70 3e 3c	nflicted ...</p><
0140	70 3e 3c 61 20 6e 61 6d	65 3d 22 39 22 3e 3c 73	p><a nam e='9"><s
0150	74 72 6f 6e 67 3e 3c 68	33 3e 41 6d 65 6e 64 6d	trong><h 3>Amendm
0160	65 6e 74 20 49 58 3c 2f	68 33 3e 3c 2f 73 74 72	ent IX</ h3></str
0170	6f 6e 67 3e 3c 2f 61 3e	0a 0a 3c 70 3e 3c 2f 70	ong></a> ...<p></p
0180	3e 3c 70 3e 54 68 65 20	65 6e 75 6d 65 72 61 74	><p>The enumerat
0190	69 6f 6e 20 69 6e 20 74	68 65 20 43 6f 6e 73 74	ion in t he Const
01a0	69 74 75 74 69 6f 6e 2c	20 6f 66 20 63 65 72 74	itution, of cert

Frame (777 bytes) Reassembled TCP (4863 bytes)

Frame (frame), 777 bytes Packets: 2794 · Displayed: 9 (0.3%) · Load time: 0:00.063 Profile: Default

## Part 4

- The browser sent 4 HTTP GET Requests
  - 1 to 128.119.245.12 for the Wireshark lab webpage
  - 1 to 165.193.140.14 for the Pearson Logo
  - 2 to 128.119.240.90 for the cover of the 5th Edition of Computer Networking
- We can tell whether the browser downloaded the images serially or in parallel by looking at the time of the requests. Since the GET for the second request is sent after the first image is already received, we can say that the images were downloaded serially



Capture 4.pcapng [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
386	2015-09-19 14:42:18.829375000	10.245.247.201	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file4.html
388	2015-09-19 14:42:18.840521000	128.119.245.12	10.245.247.201	HTTP	1156	HTTP/1.1 200 OK (text/html)
412	2015-09-19 14:42:19.059761000	10.245.247.201	165.193.140.14	HTTP	513	GET /assets/hip/us/hip_us_pearsonhighered/ima
423	2015-09-19 14:42:19.092455000	165.193.140.14	10.245.247.201	HTTP	998	HTTP/1.1 200 OK (GIF89a)
578	2015-09-19 14:42:19.891401000	10.245.247.201	128.119.240.90	HTTP	472	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
582	2015-09-19 14:42:19.902344000	128.119.240.90	10.245.247.201	HTTP	510	HTTP/1.1 302 Found (text/html)
600	2015-09-19 14:42:19.966634000	10.245.247.201	128.119.240.90	HTTP	472	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
695	2015-09-19 14:42:20.025836000	128.119.240.90	10.245.247.201	HTTP	526	HTTP/1.1 200 OK (JPEG JFIF image)

Frame 386: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface 0

Ethernet II, Src: Elitegro\_76:50:b6 (ec:a8:6b:76:50:b6), Dst: Hewlett-\_63:a3:28 (b8:af:67:63:a3:28)

Internet Protocol Version 4, Src: 10.245.247.201 (10.245.247.201), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 57041 (57041), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 433

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36\r\n

Accept-Encoding: gzip, deflate, sdch\r\n

Accept-Language: en-US,en;q=0.8,ms;q=0.6,es;q=0.4\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]

[HTTP request 1/1]

[Response in frame: 388]

0000 b8 af 67 63 a3 28 ec a8 6b 76 50 b6 08 00 45 00 ..gc.(.. kVP...E.

0010 01 d9 60 80 40 00 80 06 00 00 0a f5 f7 c9 80 77 ..@... .....

0020 f5 0c de d1 00 50 b5 1b 4a 3f f4 f1 00 78 50 18 ....P... j?...xP.

0030 01 02 7a 0e 00 00 47 45 54 20 2f 77 69 72 65 73 ..Z...GE T /wires

0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w

0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 34 2e 68 ireshark -file4.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..C onnectio

0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 41 n: keep- alive..A

00a0 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html

00b0 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 ,applica tion/xht

00c0 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 ml+xml,a pplicati

00d0 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 on/xml;q =0.9,ima

00e0 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 2e ge/webp, /\*;q=0.

00f0 38 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 8..Upgra de-Insec

0100 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d ure-Requ ests: 1.

0110 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a .User-Ag ent: Moz

0120 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 illa/5.0 (window

0130 73 20 4e 54 20 31 30 2e 30 3b 20 57 4f 57 36 34 s NT 10. 0; wow64

0140 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 ) Applew ebkit/53

File: "C:\Users\Aditya\Dropbox\Notes\CSE3..." Packets: 1072 · Displayed: 12 (1.1%) · Load time: 0:00.039 Profile: Default

## Part 5

1. After the initial request, the server responds with a 401 Unauthorized
2. The second request now contains the "Authorization" field

capture 5.pcapng [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **http** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
155	2015-09-19 15:09:50.740709000	fe80::91c4:4c03:cb4ff02::c	128.119.245.12	SSDP	208	M-SEARCH * HTTP/1.1
285	2015-09-19 15:09:52.395884000	10.245.247.201	128.119.245.12	HTTP	502	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
289	2015-09-19 15:09:52.407441000	128.119.245.12	10.245.247.201	HTTP	773	HTTP/1.1 401 Unauthorized (text/html)
373	2015-09-19 15:09:53.740595000	fe80::91c4:4c03:cb4ff02::c	128.119.245.12	SSDP	208	M-SEARCH * HTTP/1.1
543	2015-09-19 15:09:56.740785000	fe80::91c4:4c03:cb4ff02::c	128.119.245.12	SSDP	208	M-SEARCH * HTTP/1.1
627	2015-09-19 15:09:59.022934000	10.245.247.201	128.119.245.12	HTTP	561	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
629	2015-09-19 15:09:59.034508000	128.119.245.12	10.245.247.201	HTTP	585	HTTP/1.1 404 Not Found (text/html)
724	2015-09-19 15:10:00.740974000	fe80::91c4:4c03:cb4ff02::c	128.119.245.12	SSDP	208	M-SEARCH * HTTP/1.1

Frame 627: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface 0

Ethernet II, Src: Elitegro\_76:50:b6 (ec:a8:6b:76:50:b6), Dst: Hewlett-63:a3:28 (b8:af:67:63:a3:28)

Internet Protocol Version 4, Src: 10.245.247.201 (10.245.247.201), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 58018 (58018), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 507

Hypertext Transfer Protocol

GET /wireshark-labs/protected\_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzom5ldHdvcm0=\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36\r\n

Accept-Encoding: gzip, deflate, sdch\r\n

Accept-Language: en-US,en;q=0.8,ms;q=0.6,es;q=0.4\r\n

\r\n

[Full request URI: [http://gaia.cs.umass.edu/wireshark-labs/protected\\_pages/HTTP-wiresharkfile5.html](http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html)]

[HTTP request 1/1]

[Response in frame: 629]

0000 b8 af 67 63 a3 28 ec a8 6b 76 50 b6 08 00 45 00 ..gc(.. kvP...E.  
0010 02 23 61 6a 40 00 80 06 00 00 0a f5 f7 c9 80 77 .#aj@... ..w  
0020 f5 0c e2 a2 00 50 ec e9 8b 97 19 2b 82 44 50 18 ....P...+.DP.  
0030 01 02 7a 58 00 00 47 45 54 20 2f 77 69 72 65 73 ..zx..GE T/wires  
0040 68 61 72 6b 2d 6c 61 62 73 2f 70 72 6f 74 65 63 hark-lab s/protec  
0050 74 65 64 5f 70 61 67 65 73 2f 48 54 54 50 2d 77 ted\_page s/HTTP-w  
0060 69 72 65 73 68 61 72 6b 66 69 6c 65 35 2e 68 74 ireshark file5.ht  
0070 6d 6c 20 48 54 50 2f 31 2e 31 0d 0a 48 6f 73 ml HTTP/ 1.1..Hos  
0080 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 t: gaia. cs.umass  
0090 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e .edu..Co nnection  
00a0 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 41 75 : keep-a live..Au  
00b0 74 68 6f 72 69 7a 61 74 69 6f 6e 3a 20 42 61 73 thorizat ion: Bas  
00c0 69 63 20 64 32 6c 79 5a 58 4e 6f 59 58 4a 72 4c ic d2lyz XNoYXJrL  
00d0 58 4e 30 64 57 52 6c 62 6e 52 7a 4f 6d 35 6c 64 XN0dWR1b nRzom5ld  
00e0 48 64 76 63 6d 73 3d 0d 0a 41 63 63 65 70 74 3a Hdvcms=. .Accept:  
00f0 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 text/ht ml,appli  
0100 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c cation/x tml+xml  
0110 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c ,applica tion/xml  
0120 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65 62 ;q=0.9,i mage/web  
0130 70 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 55 70 67 p,\*/\*;q= 0.8..Upg  
0140 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 rade-Ins ecur e-Re

File: "C:\Users\Aditya\Dropbox\Notes\CSE310\Lab 2" Packets: 860 · Displayed: 9 (1.0%) · Load time: 0:00.037 Profile: Default

## II. Python client and server

### Server

```
adi@adi-Inspiron-5537: ~/Dropbox/Notes/CSE310/Lab 2
adi@adi-Inspiron-5537:~/Dropbox/Notes/CSE310/Lab 2$ python TCPServer.py

The server is ready to receive
```

### Test Cases

```
adi@adi-Inspiron-5537: ~/Dropbox/Notes/CSE310/Lab 2
adi@adi-Inspiron-5537:~/Dropbox/Notes/CSE310/Lab 2$ python TCPClient.py
Input lowercase sentence:hello
From Server: HELLO
adi@adi-Inspiron-5537:~/Dropbox/Notes/CSE310/Lab 2$ python TCPClient.py
Input lowercase sentence:SOMETHING SOMETHING
From Server: SOMETHING SOMETHING
adi@adi-Inspiron-5537:~/Dropbox/Notes/CSE310/Lab 2$
```