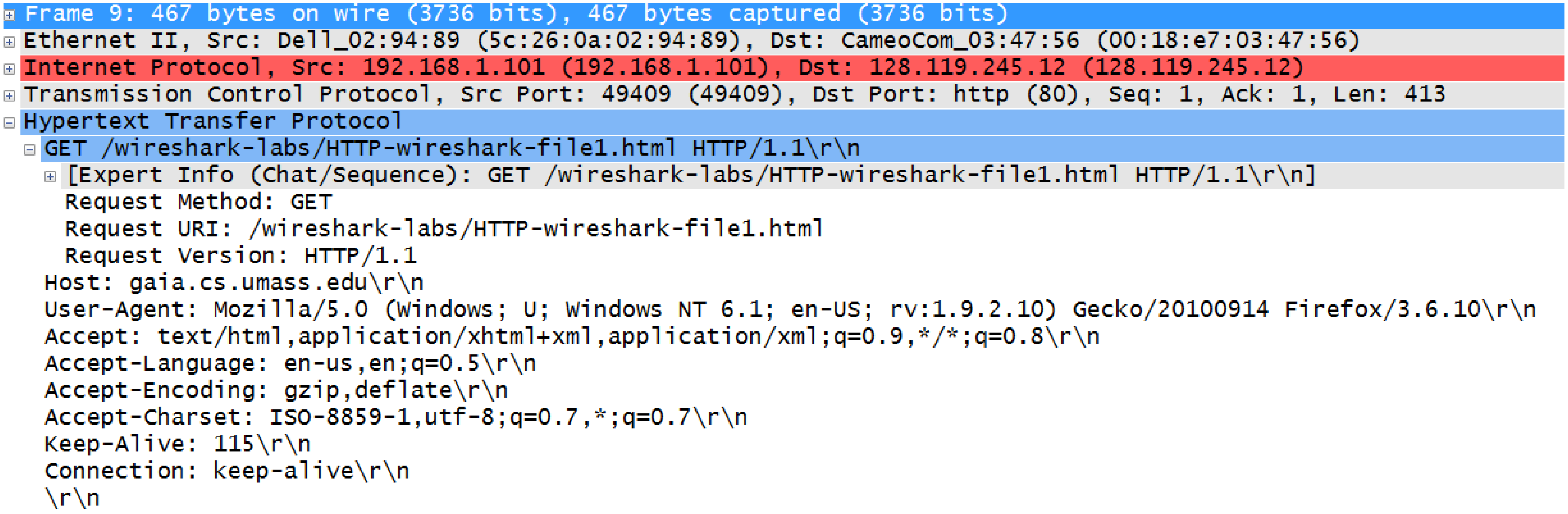
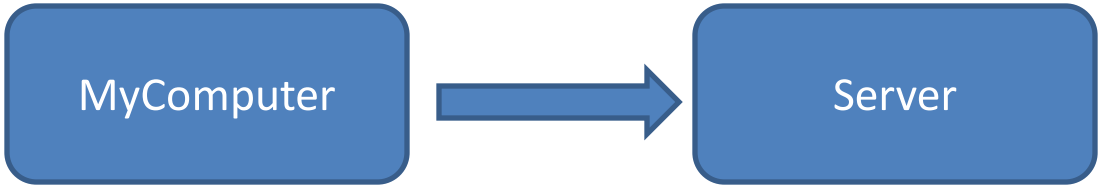
HTTP Protocols

Wireshark Lab

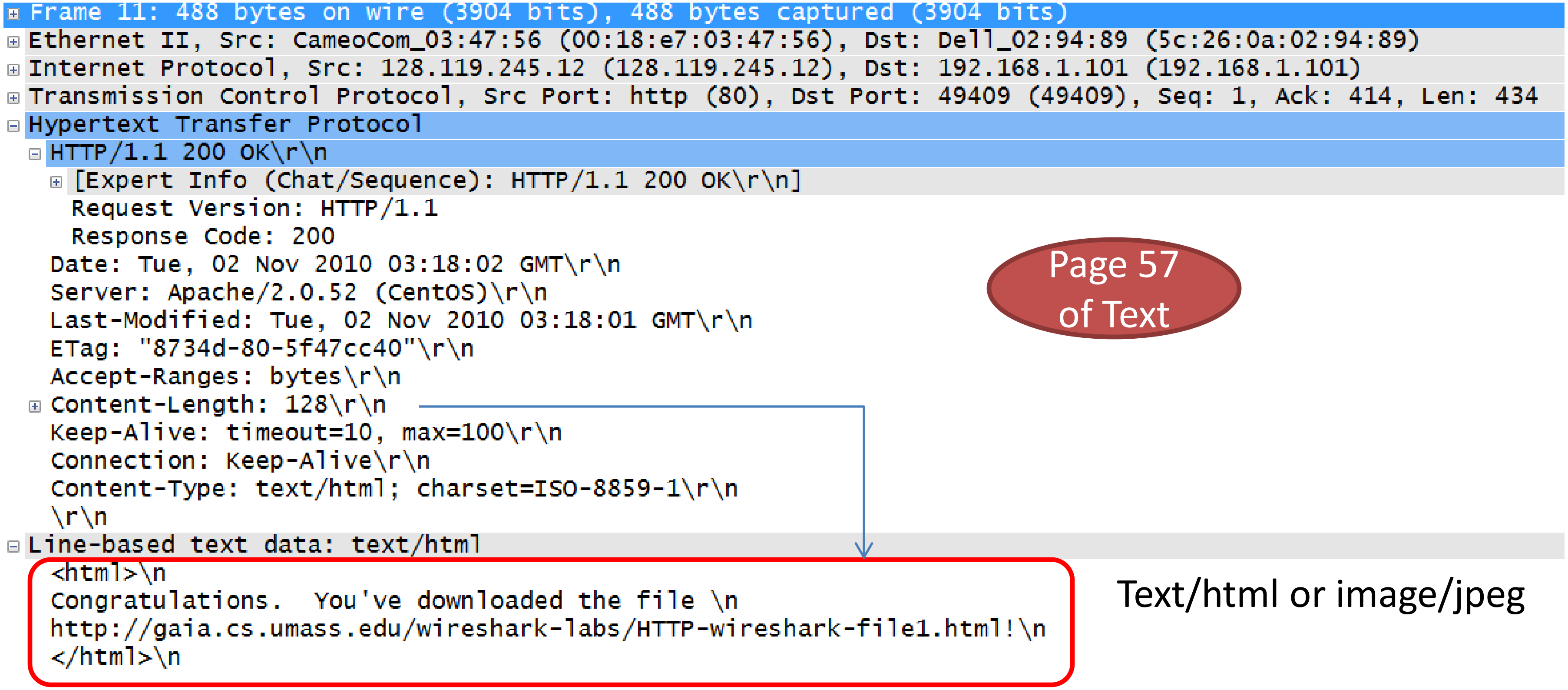
Request: GET



```
⊞ Frame 9: 467 bytes on wire (3736 bits), 467 bytes captured (3736 bits)
⊞ Ethernet II, Src: Dell_02:94:89 (5c:26:0a:02:94:89), Dst: CameoCom_03:47:56 (00:18:e7:03:47:56)
⊞ Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 49409 (49409), Dst Port: http (80), Seq: 1, Ack: 1, Len: 413
⊟ Hypertext Transfer Protocol
  ⊟ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.10) Gecko/20100914 Firefox/3.6.10\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
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    \r\n
```



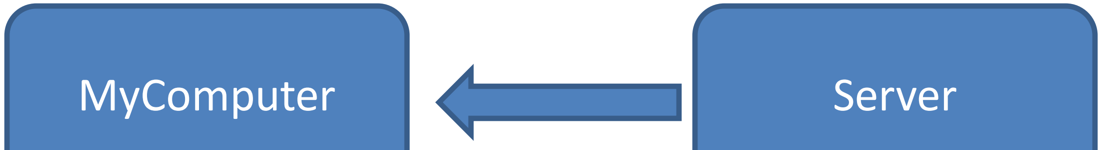
Respond: OK 200 / 400 Bad Req. / 404 Not Found

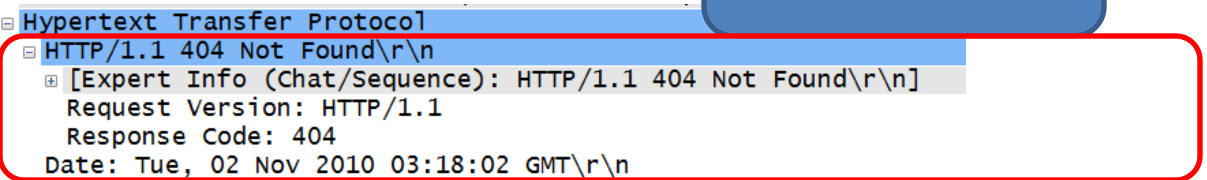


```
⊞ Frame 11: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits)
⊞ Ethernet II, Src: CameoCom_03:47:56 (00:18:e7:03:47:56), Dst: Dell_02:94:89 (5c:26:0a:02:94:89)
⊞ Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.101 (192.168.1.101)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 49409 (49409), Seq: 1, Ack: 414, Len: 434
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊞ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Response Code: 200
    Date: Tue, 02 Nov 2010 03:18:02 GMT\r\n
    Server: Apache/2.0.52 (CentOS)\r\n
    Last-Modified: Tue, 02 Nov 2010 03:18:01 GMT\r\n
    ETag: "8734d-80-5f47cc40"\r\n
    Accept-Ranges: bytes\r\n
  ⊞ Content-Length: 128\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
⊟ Line-based text data: text/html
    <html>\n
    Congratulations.  You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n
```

Page 57 of Text

Text/html or image/jpeg





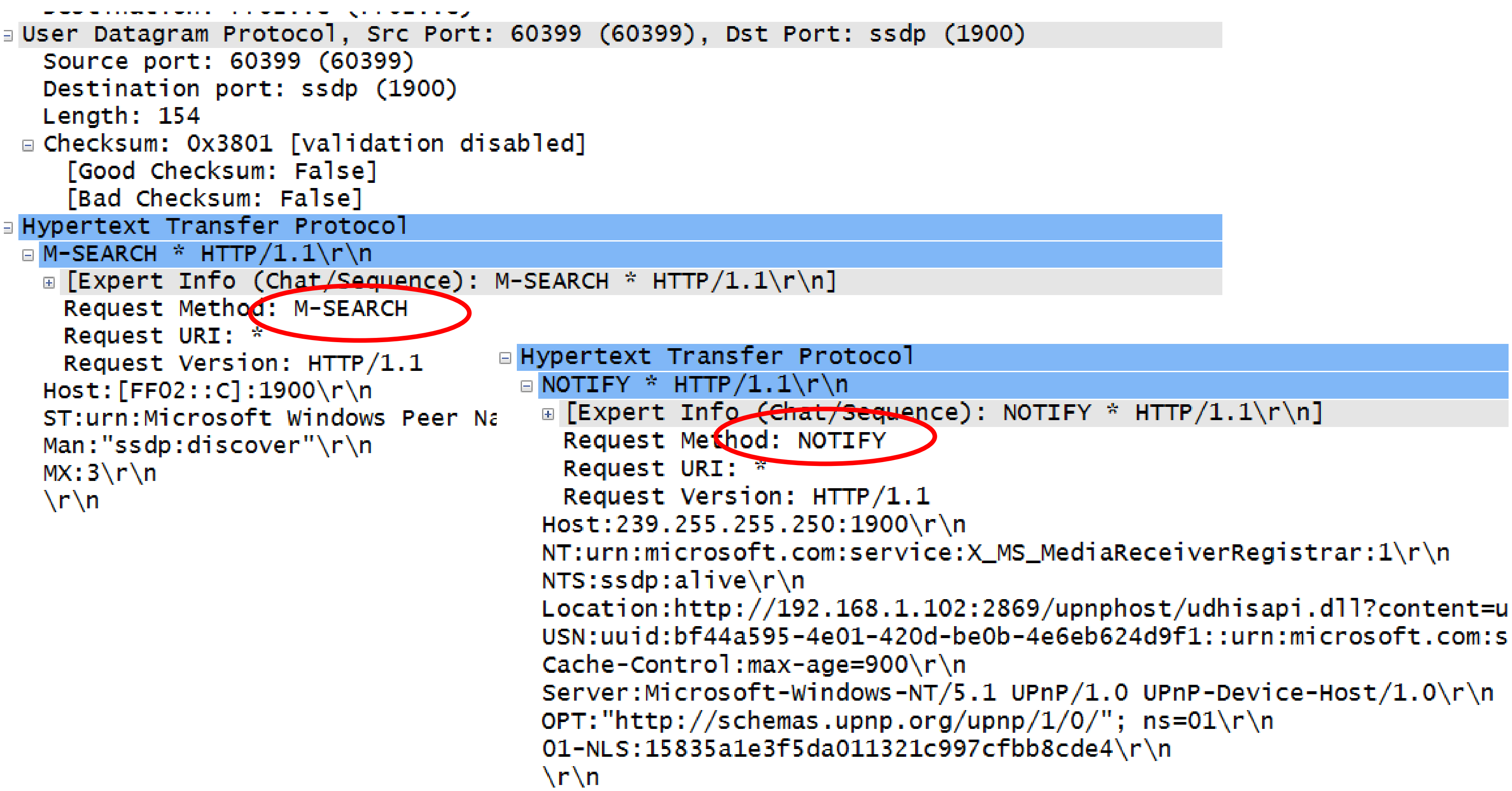
```
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 404 Not Found\r\n
    ⊞ [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      Request Version: HTTP/1.1
      Response Code: 404
    Date: Tue, 02 Nov 2010 03:18:02 GMT\r\n
```

SSDP: **Simple Service Discovery Protocol (SSDP)**

- SSDP is a text-based protocol based on the Hypertext Transfer Protocol
  - SSDP uses UDP transport protocol on port 1900
  - multicast adress (239.255.255.250)
- This protocol allows you to discover and configure devices using uPnP (Universal Plug and Play) automatically, this process is referred to as SSDP Discover
  - No need for Dynamic Host Configuration Protocol (DHCP) or the Domain Name System (DNS) – name server is available
  - supported by Microsoft Windows operating systems
  - Allows automatically joining a network without having DHCP (useful for wireless)
- A client that wishes to discover available services on a network, uses the M-SEARCH method
  - Responses to such search requests are sent via unicast addressing to the originating address and port number of the multicast request
- such search requests are sent via unicast addressing to the originating address and port number of the multicast request

Use the following to eliminate showing these messages: *not udp.dstport == 1900*

SSDP: Search and Notify



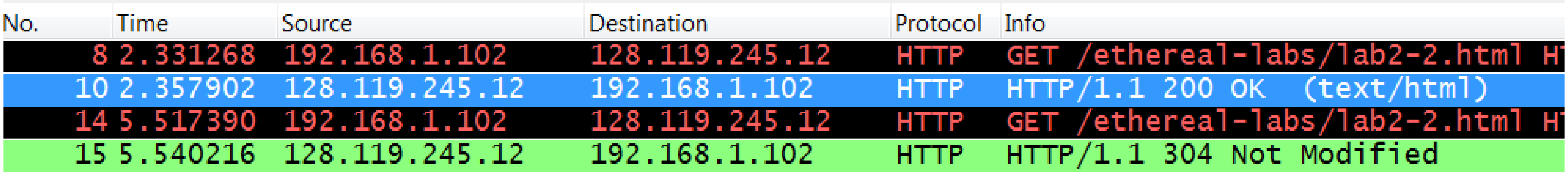
```
  Destination: ff02::c (ff02::c)
⊟ User Datagram Protocol, Src Port: 60399 (60399), Dst Port: ssdp (1900)
    Source port: 60399 (60399)
    Destination port: ssdp (1900)
    Length: 154
  ⊟ Checksum: 0x3801 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
⊟ Hypertext Transfer Protocol
  ⊟ M-SEARCH * HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): M-SEARCH * HTTP/1.1\r\n]
      Request Method: M-SEARCH
      Request URI: *
      Request Version: HTTP/1.1
    Host:[FF02::C]:1900\r\n
    ST:urn:Microsoft Windows Peer Na
    Man:"ssdp:discover"\r\n
    MX:3\r\n
    \r\n
```

```
⊟ Hypertext Transfer Protocol
  ⊟ NOTIFY * HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): NOTIFY * HTTP/1.1\r\n]
      Request Method: NOTIFY
      Request URI: *
      Request Version: HTTP/1.1
    Host:239.255.255.250:1900\r\n
    NT:urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1\r\n
    NTS:ssdp:alive\r\n
    Location:http://192.168.1.102:2869/upnphost/udhisapi.dll?content=u
    USN:uuid:bf44a595-4e01-420d-be0b-4e6eb624d9f1::urn:microsoft.com:s
    Cache-Control:max-age=900\r\n
    Server:Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0\r\n
    OPT:"http://schemas.upnp.org/upnp/1/0/"; ns=01\r\n
    01-NLS:15835a1e3f5da011321c997cfbb8cde4\r\n
    \r\n
```

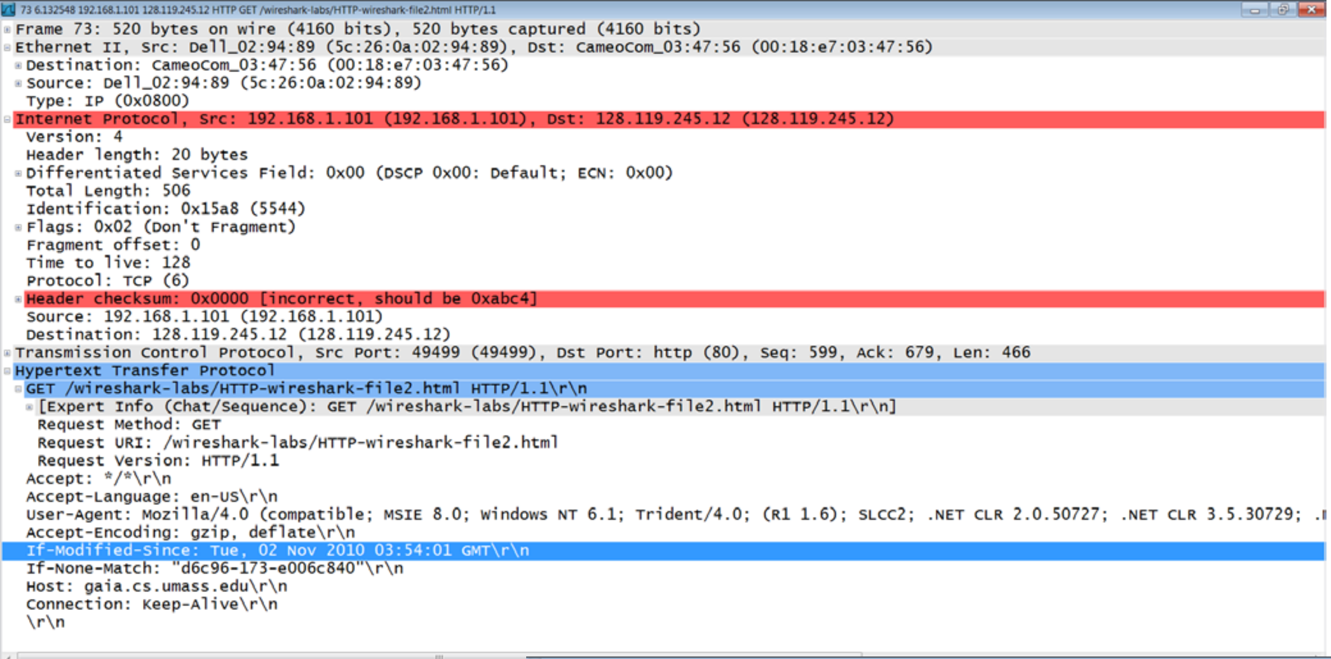
http://www.mudynamics.com/resources/collaterals/SSDP-ProtocolBrief.pdf

Using Cache

- Before the request it check the browser checks the cache
- If it is there checks to see if there is any change in the file using IF-MODIFIED-SINCE
- If the file is not modified then NO MODIFIED response will be returned



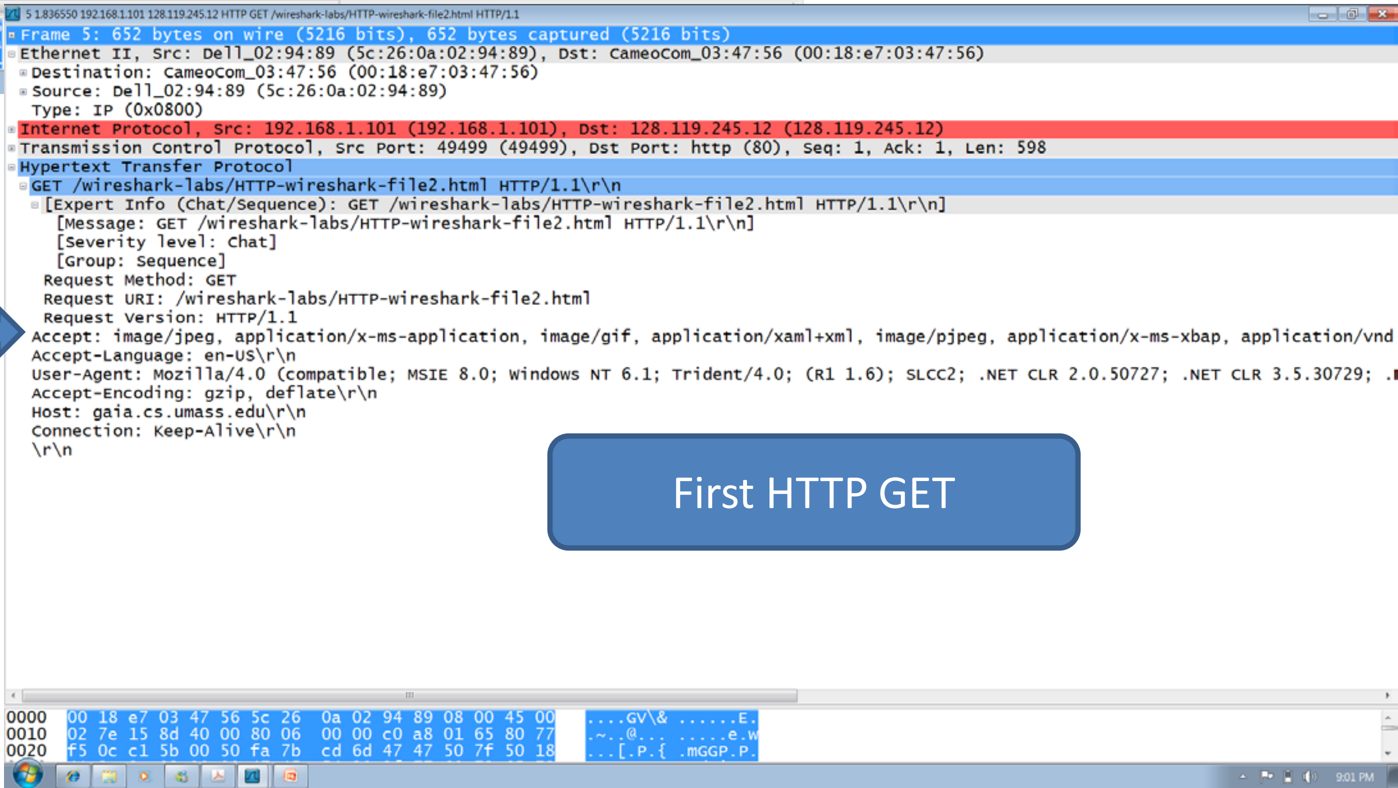
No.	Time	Source	Destination	Protocol	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	GET /ethereal-labs/lab2-2.html H
10	2.357902	128.119.245.12	192.168.1.102	HTTP	HTTP/1.1 200 OK (text/html)
14	5.517390	192.168.1.102	128.119.245.12	HTTP	GET /ethereal-labs/lab2-2.html H
15	5.540216	128.119.245.12	192.168.1.102	HTTP	HTTP/1.1 304 Not Modified



```
73 6.132548 192.168.1.101 128.119.245.12 HTTP GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
⊞ Frame 73: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits)
⊟ Ethernet II, Src: Dell_02:94:89 (5c:26:0a:02:94:89), Dst: CameoCom_03:47:56 (00:18:e7:03:47:56)
  ⊞ Destination: CameoCom_03:47:56 (00:18:e7:03:47:56)
  ⊞ Source: Dell_02:94:89 (5c:26:0a:02:94:89)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 128.119.245.12 (128.119.245.12)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 506
    Identification: 0x15a8 (5544)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ⊞ Header checksum: 0x0000 [incorrect, should be 0xabc4]
    Source: 192.168.1.101 (192.168.1.101)
    Destination: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 49499 (49499), Dst Port: http (80), Seq: 599, Ack: 679, Len: 466
⊟ Hypertext Transfer Protocol
  ⊟ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Accept: */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; (R1 1.6); SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .
    Accept-Encoding: gzip, deflate\r\n
    If-Modified-Since: Tue, 02 Nov 2010 03:54:01 GMT\r\n
    If-None-Match: "d6c96-173-e006c840"\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    \r\n

0170  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 49 66
0180  2d 4d 6f 64 69 66 69 65  64 2d 53 69 6e 63 65 3a
0190  20 54 75 65 2c 20 30 32  20 4e 6f 76 20 32 30 31
```

Second HTTP GET

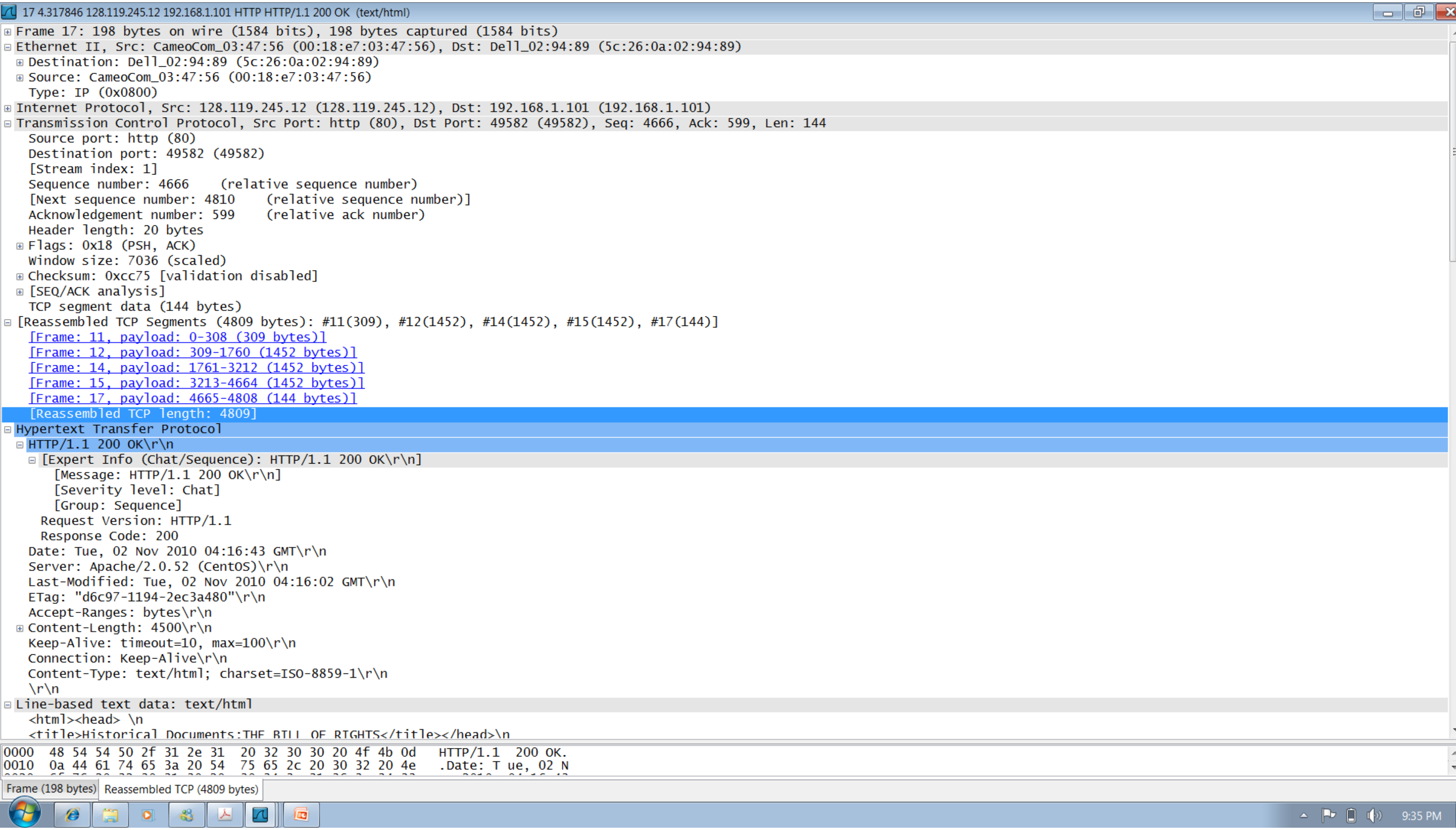


```
5 1.836550 192.168.1.101 128.119.245.12 HTTP GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
⊞ Frame 5: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits)
⊟ Ethernet II, Src: Dell_02:94:89 (5c:26:0a:02:94:89), Dst: CameoCom_03:47:56 (00:18:e7:03:47:56)
  ⊞ Destination: CameoCom_03:47:56 (00:18:e7:03:47:56)
  ⊞ Source: Dell_02:94:89 (5c:26:0a:02:94:89)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 49499 (49499), Dst Port: http (80), Seq: 1, Ack: 1, Len: 598
⊟ Hypertext Transfer Protocol
  ⊟ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    ⊟ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [Message: GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, application/vnd
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; (R1 1.6); SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    \r\n

0000  00 18 e7 03 47 56 5c 26  0a 02 94 89 08 00 45 00   ....GV\& ......E.
0010  02 7e 15 8d 40 00 80 06  00 00 c0 a8 01 65 80 77   .~..@... .....e.w
0020  f5 0c c1 5b 00 50 fa 7b  cd 6d 47 47 50 7f 50 18   ...[.P.{ .mGGP.P.
```

First HTTP GET

Showing Large Message



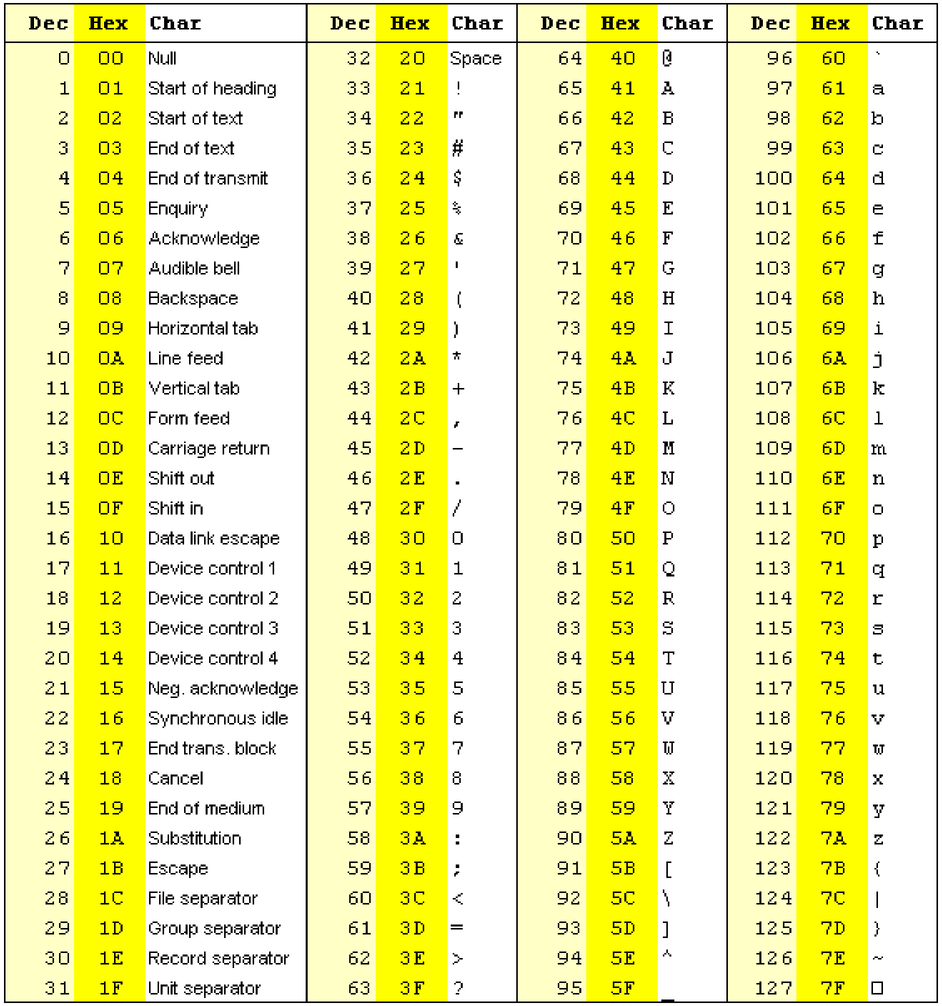
```
17 4.317846 128.119.245.12 192.168.1.101 HTTP HTTP/1.1 200 OK  (text/html)
⊞ Frame 17: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits)
⊟ Ethernet II, Src: CameoCom_03:47:56 (00:18:e7:03:47:56), Dst: Dell_02:94:89 (5c:26:0a:02:94:89)
  ⊞ Destination: Dell_02:94:89 (5c:26:0a:02:94:89)
  ⊞ Source: CameoCom_03:47:56 (00:18:e7:03:47:56)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.101 (192.168.1.101)
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 49582 (49582), Seq: 4666, Ack: 599, Len: 144
    Source port: http (80)
    Destination port: 49582 (49582)
    [Stream index: 1]
    Sequence number: 4666    (relative sequence number)
    [Next sequence number: 4810    (relative sequence number)]
    Acknowledgement number: 599    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size: 7036 (scaled)
  ⊞ Checksum: 0xcc75 [validation disabled]
  ⊞ [SEQ/ACK analysis]
    TCP segment data (144 bytes)
⊟ [Reassembled TCP Segments (4809 bytes): #11(309), #12(1452), #14(1452), #15(1452), #17(144)]
    [Frame: 11, payload: 0-308 (309 bytes)]
    [Frame: 12, payload: 309-1760 (1452 bytes)]
    [Frame: 14, payload: 1761-3212 (1452 bytes)]
    [Frame: 15, payload: 3213-4664 (1452 bytes)]
    [Frame: 17, payload: 4665-4808 (144 bytes)]
    [Reassembled TCP length: 4809]
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊟ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [Message: HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Response Code: 200
    Date: Tue, 02 Nov 2010 04:16:43 GMT\r\n
    Server: Apache/2.0.52 (CentOS)\r\n
    Last-Modified: Tue, 02 Nov 2010 04:16:02 GMT\r\n
    ETag: "d6c97-1194-2ec3a480"\r\n
    Accept-Ranges: bytes\r\n
  ⊞ Content-Length: 4500\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
⊟ Line-based text data: text/html
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n

0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
0010  0a 44 61 74 65 3a 20 54  75 65 2c 20 30 32 20 4e   .Date: T ue, 02 N

Frame (198 bytes)   Reassembled TCP (4809 bytes)
```

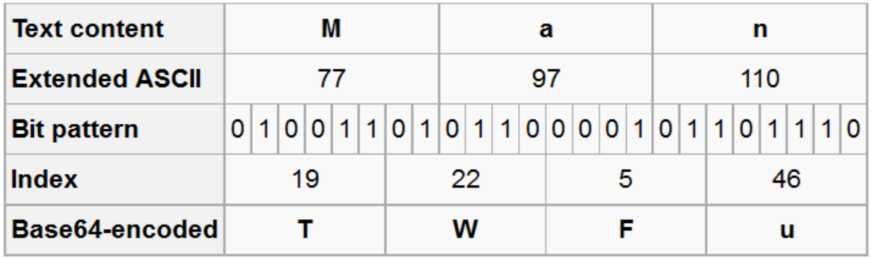
Authentication

ASCII



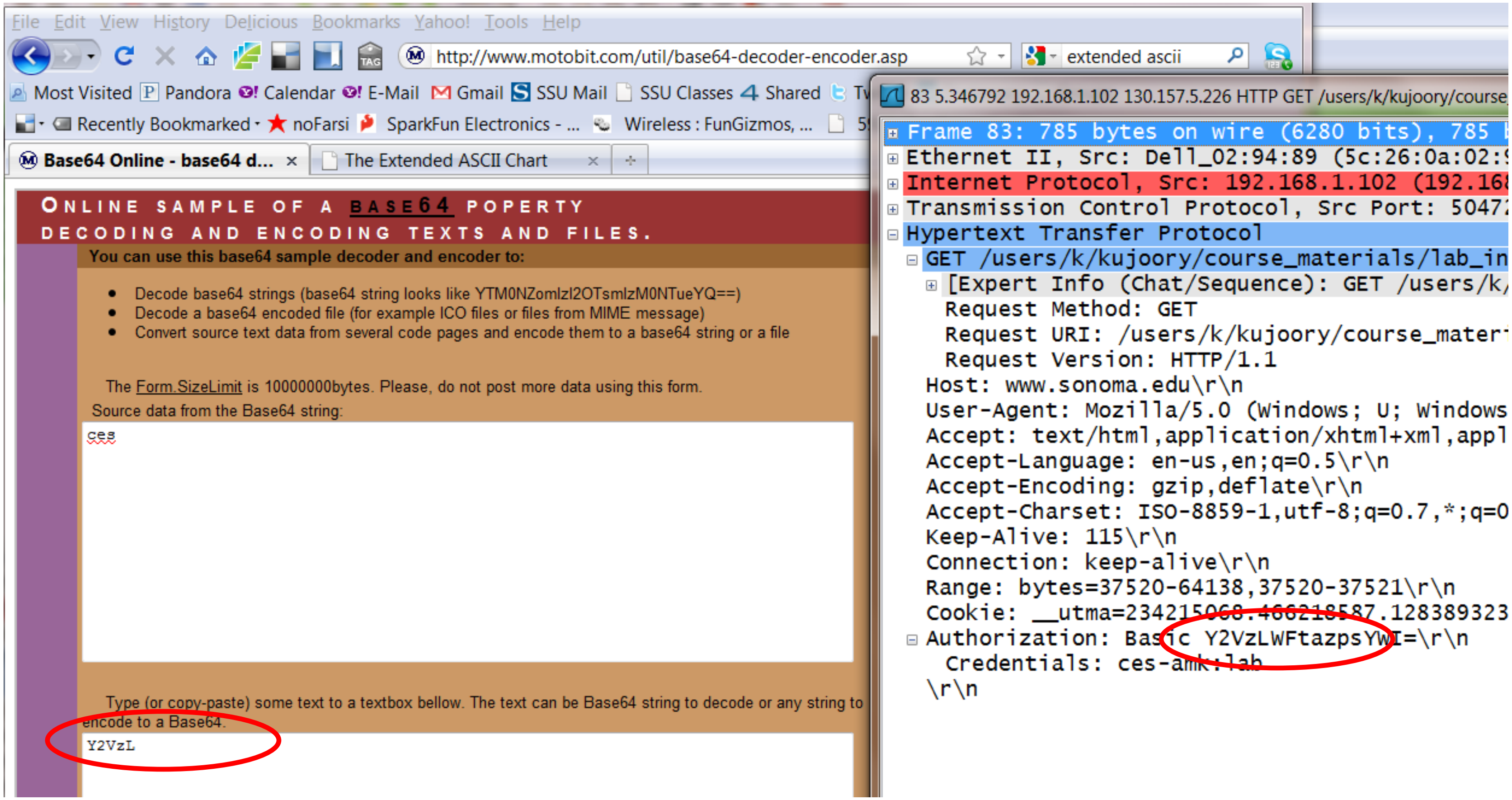
Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(	72	48	H	104	68	h
9	09	Horizontal tab	41	29	)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

- Base64 (2^6)
- Consider an example: Man
- The buffer is 24-bit wide – then we take 6 bit at a time



<table>
<tr><td>Text content</td><td colspan="8">M</td><td colspan="8">a</td><td colspan="8">n</td></tr>
<tr><td>Extended ASCII</td><td colspan="8">77</td><td colspan="8">97</td><td colspan="8">110</td></tr>
<tr><td>Bit pattern</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td></tr>
<tr><td>Index</td><td colspan="6">19</td><td colspan="6">22</td><td colspan="6">5</td><td colspan="6">46</td></tr>
<tr><td>Base64-encoded</td><td colspan="6">T</td><td colspan="6">W</td><td colspan="6">F</td><td colspan="6">u</td></tr>
</table>

Decoding the Base64


File Edit View History Delicious Bookmarks Yahoo! Tools Help
http://www.motobit.com/util/base64-decoder-encoder.asp
extended ascii
Most Visited
Pandora
Calendar
E-Mail
Gmail
SSU Mail
SSU Classes
Shared
Recently Bookmarked
noFarsi
SparkFun Electronics - ...
Wireless : FunGizmos, ...
Base64 Online - base64 d...
The Extended ASCII Chart

ONLINE SAMPLE OF A BASE64 POPERTY DECODING AND ENCODING TEXTS AND FILES.

You can use this base64 sample decoder and encoder to:

- Decode base64 strings (base64 string looks like YTM0NZomIzI2OTsmIzM0NTueYQ==)
- Decode a base64 encoded file (for example ICO files or files from MIME message)
- Convert source text data from several code pages and encode them to a base64 string or a file

The Form.SizeLimit is 10000000bytes. Please, do not post more data using this form.

Source data from the Base64 string:

ces

Type (or copy-paste) some text to a textbox bellow. The text can be Base64 string to decode or any string to encode to a Base64.

Y2VzL

```
83 5.346792 192.168.1.102 130.157.5.226 HTTP GET /users/k/kujoory/course
⊞ Frame 83: 785 bytes on wire (6280 bits), 785
⊞ Ethernet II, Src: Dell_02:94:89 (5c:26:0a:02:
⊞ Internet Protocol, Src: 192.168.1.102 (192.168
⊞ Transmission Control Protocol, Src Port: 5047
⊟ Hypertext Transfer Protocol
  ⊟ GET /users/k/kujoory/course_materials/lab_in
    ⊞ [Expert Info (Chat/Sequence): GET /users/k/
      Request Method: GET
      Request URI: /users/k/kujoory/course_mater
      Request Version: HTTP/1.1
    Host: www.sonoma.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows
    Accept: text/html,application/xhtml+xml,appl
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    Range: bytes=37520-64138,37520-37521\r\n
    Cookie: __utma=234215068.466218587.128389323
  ⊟ Authorization: Basic Y2VzLWFtazpsYWI=\r\n
      Credentials: ces-amk:lab
    \r\n
```