Discipline Knowledge Morality

Bangladesh Army University of Science and Technology (BAUST)

Assignment

Topic Name: Wireshark Lab:
HTTP v8.1

Course title: **:** Computer Network

Course code: CSE 3205

Submitted to:

Dr. S. M. Sadakatul Bari
Assistant Professor
Dept. of CSE,
Bangladesh Army University of science and Technology

Submitted by:

MD Asif Hossain
Session: 2018-19

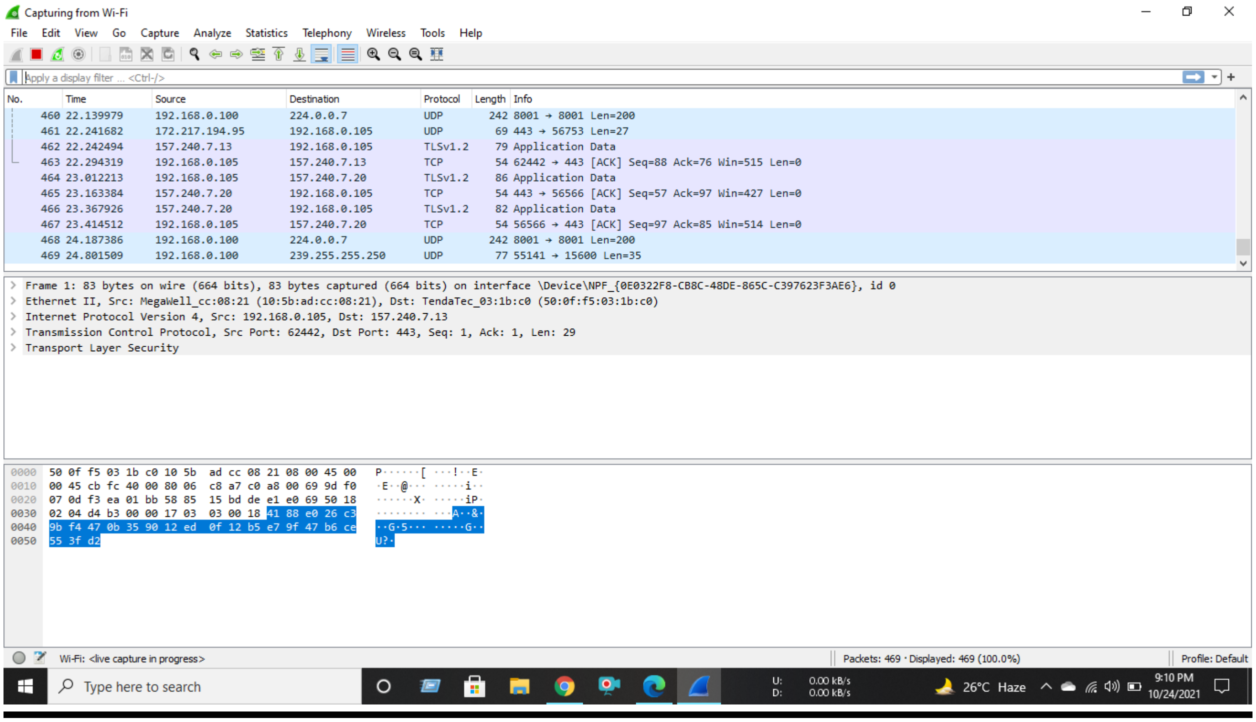
Roll: 180201015

Level-3, Term-II

Sec: A, Dept. of CSE

Date of submission: 24/10/2021

Installing proof:


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
U: 0.00 kB/s
D: 0.00 kB/s
26°C Haze
9:10 PM
10/24/2021

```
No.     Time        Source           Destination       Protocol  Length Info
    460 22.139979   192.168.0.100    224.0.0.7         UDP        242 8001 → 8001 Len=200
    461 22.241682   172.217.194.95   192.168.0.105     UDP         69 443 → 56753 Len=27
    462 22.242494   157.240.7.13     192.168.0.105     TLSv1.2     79 Application Data
    463 22.294319   192.168.0.105    157.240.7.13      TCP         54 62442 → 443 [ACK] Seq=88 Ack=76 Win=515 Len=0
    464 23.012213   192.168.0.105    157.240.7.20      TLSv1.2     86 Application Data
    465 23.163384   157.240.7.20     192.168.0.105     TCP         54 443 → 56566 [ACK] Seq=57 Ack=97 Win=427 Len=0
    466 23.367926   157.240.7.20     192.168.0.105     TLSv1.2     82 Application Data
    467 23.414512   192.168.0.105    157.240.7.20      TCP         54 56566 → 443 [ACK] Seq=97 Ack=85 Win=514 Len=0
    468 24.187386   192.168.0.100    224.0.0.7         UDP        242 8001 → 8001 Len=200
    469 24.801509   192.168.0.100    239.255.255.250   UDP         77 55141 → 15600 Len=35
```

```
> Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{0E0322F8-CB8C-48DE-865C-C397623F3AE6}, id 0
> Ethernet II, Src: MegaWell_cc:08:21 (10:5b:ad:cc:08:21), Dst: TendaTec_03:1b:c0 (50:0f:f5:03:1b:c0)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 157.240.7.13
> Transmission Control Protocol, Src Port: 62442, Dst Port: 443, Seq: 1, Ack: 1, Len: 29
> Transport Layer Security
```

```
0000  50 0f f5 03 1b c0 10 5b  ad cc 08 21 08 00 45 00   P······[ ···!··E·
0010  00 45 cb fc 40 00 80 06  c8 a7 c0 a8 00 69 9d f0   ·E··@··· ·····i··
0020  07 0d f3 ea 01 bb 58 85  15 bd de e1 e0 69 50 18   ······X· ·····iP·
0030  02 04 d4 b3 00 00 17 03  03 00 18 41 88 e0 26 c3   ········ ···A··&·
0040  9b f4 47 0b 35 90 12 ed  0f 12 b5 e7 9f 47 b6 ce   ··G·5··· ·····G··
0050  55 3f d2                                           U?·
```

```
Wi-Fi: <live capture in progress>        Packets: 469 · Displayed: 469 (100.0%)        Profile: Default
```

1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?

Ans: 1.1

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

Ans : en-us

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

Ans : My IP : 128.119.245.12   Destination : 192.168.0.105

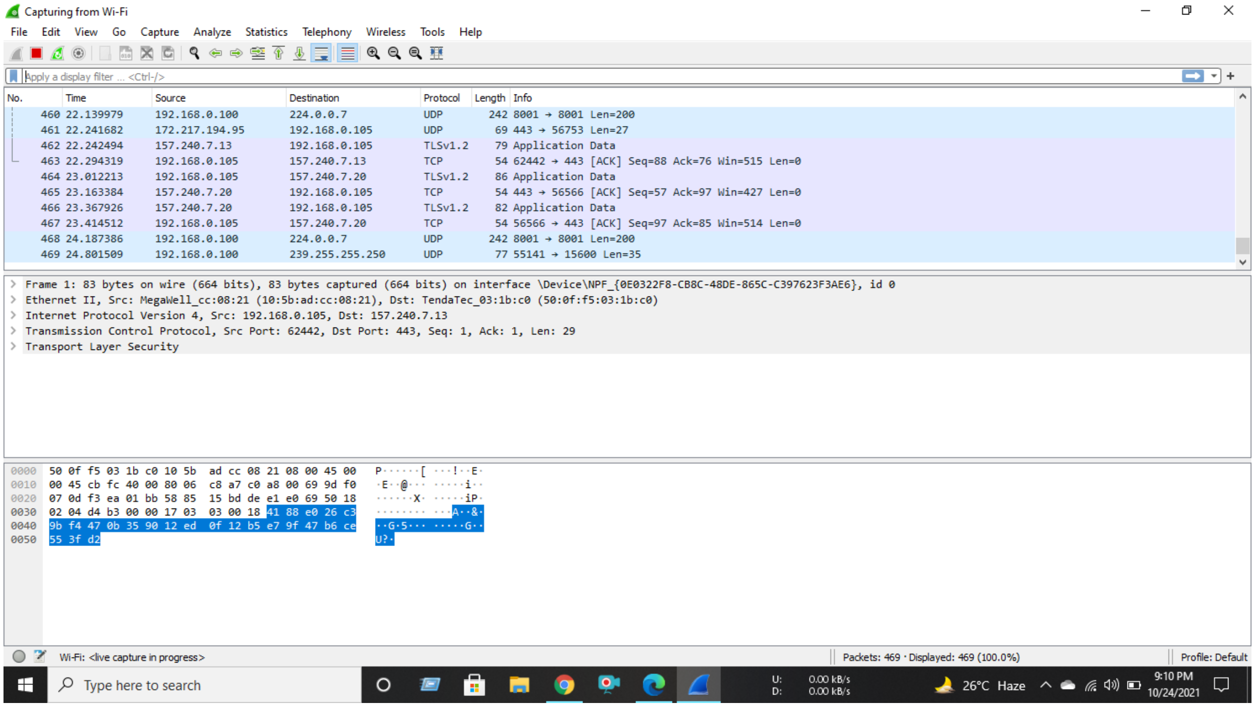
4.What is the status code returned from the server to your browser?

Ans:200 OK

5. When was the HTML file that you are retrieving last modified at the server?
Ans: Last-Modified: Sun, 24 Oct 2021 05:59:01 GMT\r\n

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

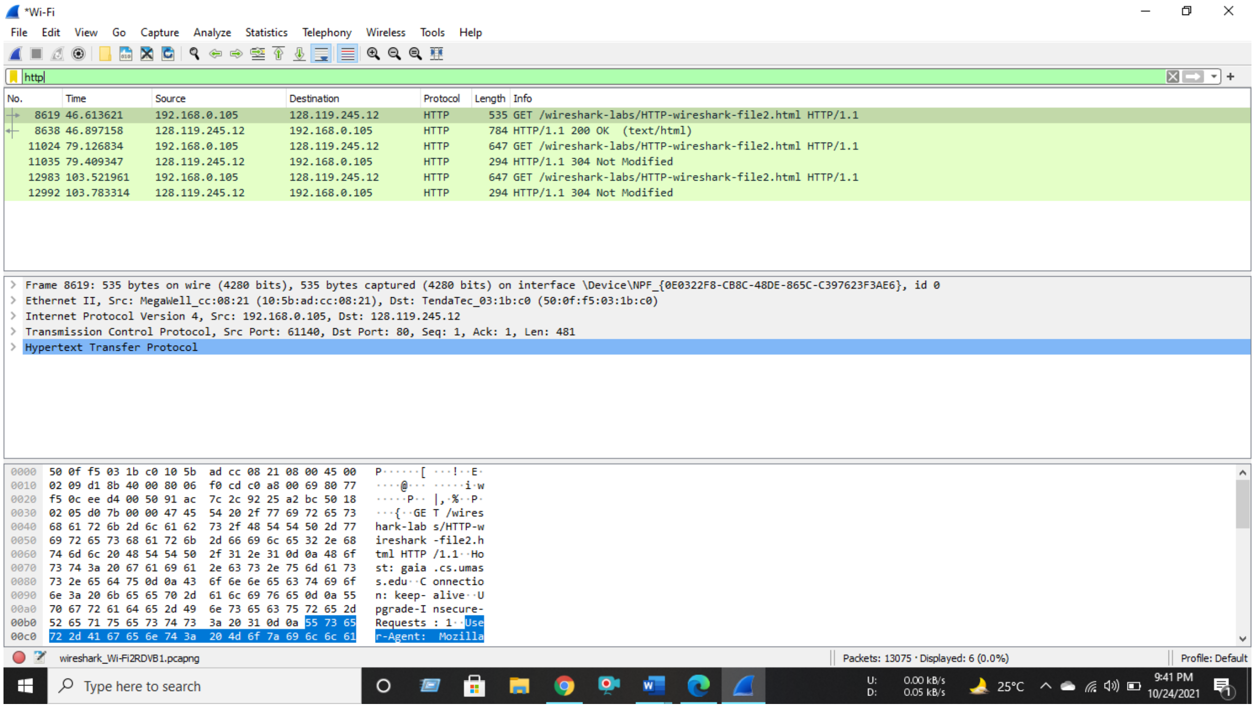
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
Ans: No header found



```
No.     Time        Source           Destination      Protocol  Length Info
    460 22.139979   192.168.0.100    224.0.0.7        UDP       242 8001 → 8001 Len=200
    461 22.241682   172.217.194.95   192.168.0.105    UDP        69 443 → 56753 Len=27
    462 22.242494   157.240.7.13     192.168.0.105    TLSv1.2    79 Application Data
    463 22.294319   192.168.0.105    157.240.7.13     TCP        54 62442 → 443 [ACK] Seq=88 Ack=76 Win=515 Len=0
    464 23.012213   192.168.0.105    157.240.7.20     TLSv1.2    86 Application Data
    465 23.163384   157.240.7.20     192.168.0.105    TCP        54 443 → 56566 [ACK] Seq=57 Ack=97 Win=427 Len=0
    466 23.367926   157.240.7.20     192.168.0.105    TLSv1.2    82 Application Data
    467 23.414512   192.168.0.105    157.240.7.20     TCP        54 56566 → 443 [ACK] Seq=97 Ack=85 Win=514 Len=0
    468 24.187386   192.168.0.100    224.0.0.7        UDP       242 8001 → 8001 Len=200
    469 24.801509   192.168.0.100    239.255.255.250  UDP        77 55141 → 15600 Len=35
```

```
> Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{0E0322F8-CB8C-48DE-865C-C397623F3AE6}, id 0
> Ethernet II, Src: MegaWell_cc:08:21 (10:5b:ad:cc:08:21), Dst: TendaTec_03:1b:c0 (50:0f:f5:03:1b:c0)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 157.240.7.13
> Transmission Control Protocol, Src Port: 62442, Dst Port: 443, Seq: 1, Ack: 1, Len: 29
> Transport Layer Security
```

```
0000  50 0f f5 03 1b c0 10 5b  ad cc 08 21 08 00 45 00   P······[ ···!··E·
0010  00 45 cb fc 40 00 80 06  c8 a7 c0 a8 00 69 9d f0   ·E··@··· ·····i··
0020  07 0d f3 ea 01 bb 58 85  15 bd de e1 e0 69 50 18   ······X· ·····iP·
0030  02 04 d4 b3 00 00 17 03  03 00 18 41 88 e0 26 c3   ········ ···A··&·
0040  9b f4 47 0b 35 90 12 ed  0f 12 b5 e7 9f 47 b6 ce   ··G·5··· ·····G··
0050  55 3f d2                                           U?·
```


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Type here to search
U: 0.00 kB/s
D: 0.05 kB/s
25°C
9:41 PM
10/24/2021

```
No.    Time        Source          Destination     Protocol Length Info
  8619 46.613621   192.168.0.105   128.119.245.12  HTTP      535 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  8638 46.897158   128.119.245.12  192.168.0.105   HTTP      784 HTTP/1.1 200 OK  (text/html)
 11024 79.126834   192.168.0.105   128.119.245.12  HTTP      647 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 11035 79.409347   128.119.245.12  192.168.0.105   HTTP      294 HTTP/1.1 304 Not Modified
 12983 103.521961  192.168.0.105   128.119.245.12  HTTP      647 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 12992 103.783314  128.119.245.12  192.168.0.105   HTTP      294 HTTP/1.1 304 Not Modified
```

```
> Frame 8619: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{0E0322F8-CB8C-48DE-865C-C397623F3AE6}, id 0
> Ethernet II, Src: MegaWell_cc:08:21 (10:5b:ad:cc:08:21), Dst: TendaTec_03:1b:c0 (50:0f:f5:03:1b:c0)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61140, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
> Hypertext Transfer Protocol
```

```
0000  50 0f f5 03 1b c0 10 5b  ad cc 08 21 08 00 45 00   P······[ ···!··E·
0010  02 09 d1 8b 40 00 80 06  f0 cd c0 a8 00 69 80 77   ····@··· ·····i·w
0020  f5 0c ee d4 00 50 91 ac  7c 2c 92 25 a2 bc 50 18   ·····P·· |,·%··P·
0030  02 05 d0 7b 00 00 47 45  54 20 2f 77 69 72 65 73   ···{··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 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
```

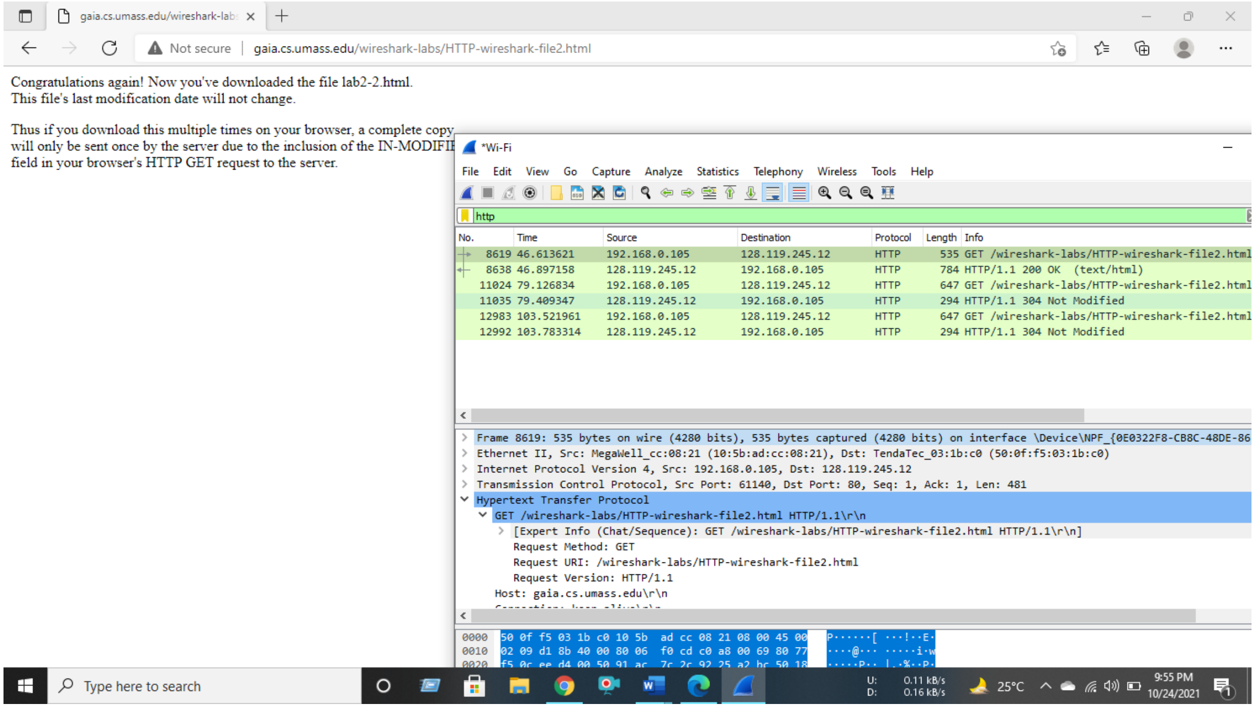
```
wireshark_Wi-Fi2RDVB1.pcapng     Packets: 13075 · Displayed: 6 (0.0%)     Profile: Default
```

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?
Ans: No

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
Ans: Yes. In line-based text data. Wireshark includes a section titled "Line-Based Text Data" Which shows the server sent back to my browser which is specifically what the website showed when I brought it up on my browser

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 ? If so, what information follows the "IF-MODIFIED-SINCE:" header?
Ans: Sun, 24 Oct 2021 05:59:01

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.
Ans: 304 not modified Yes it does in line-based text data


gaia.cs.umass.edu/wireshark-lab
Not secure
gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Type here to search
U: 0.11 kB/s
D: 0.16 kB/s
25°C
9:55 PM
10/24/2021

Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy
will only be sent once by the server due to the inclusion of the IN-MODIFIE
field in your browser's HTTP GET request to the server.

```
No.    Time        Source          Destination     Protocol Length Info
 8619 46.613621   192.168.0.105   128.119.245.12  HTTP      535 GET /wireshark-labs/HTTP-wireshark-file2.html
 8638 46.897158   128.119.245.12  192.168.0.105   HTTP      784 HTTP/1.1 200 OK  (text/html)
11024 79.126834   192.168.0.105   128.119.245.12  HTTP      647 GET /wireshark-labs/HTTP-wireshark-file2.html
11035 79.409347   128.119.245.12  192.168.0.105   HTTP      294 HTTP/1.1 304 Not Modified
12983 103.521961  192.168.0.105   128.119.245.12  HTTP      647 GET /wireshark-labs/HTTP-wireshark-file2.html
12992 103.783314  128.119.245.12  192.168.0.105   HTTP      294 HTTP/1.1 304 Not Modified
```

```
> Frame 8619: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{0E0322F8-CB8C-48DE-86
> Ethernet II, Src: MegaWell_cc:08:21 (10:5b:ad:cc:08:21), Dst: TendaTec_03:1b:c0 (50:0f:f5:03:1b:c0)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61140, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
v Hypertext Transfer Protocol
  v 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
    Host: gaia.cs.umass.edu\r\n
```

```
0000  50 0f f5 03 1b c0 10 5b  ad cc 08 21 08 00 45 00   P······[ ···!··E·
0010  02 09 d1 8b 40 00 80 06  f0 cd c0 a8 00 69 80 77   ····@··· ·····i·w
0020  f5 0c ee d4 00 50 91 ac  7c 2c 92 25 a2 bc 50 18   ·····P·· |,·%··P·
```