CS 372 - Introduction to Computer Networks - Lab 1

Eric Gullufsen

9 April 2016

1 Problems 1 - 6

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
   Answer: In the figure 2 below we can see (among others) the TCP, HTTP, and DNS protocols.

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?
   Answer: As the lab instructions suggest, we switch the Time display format and find (see figure 3 below) that the bit of math we must perform is $0.848417 - 0.73364 = 0.114777$ seconds.

3. What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer?
   Answer: From any of the figures included below, we can see that the IP address of the destination host is 128.119.245.12.

4. Print the two HTTP messages (GET and OK referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the *"Selected Packet Only"* and *"Print as displayed"* radial buttons, and then click OK.
   Answer: It's a bit cumbersome, but I've included the .txt files output by wireshark, instead of printing them to a physical printer. First is the GET request sent from my computer to the umass server, second

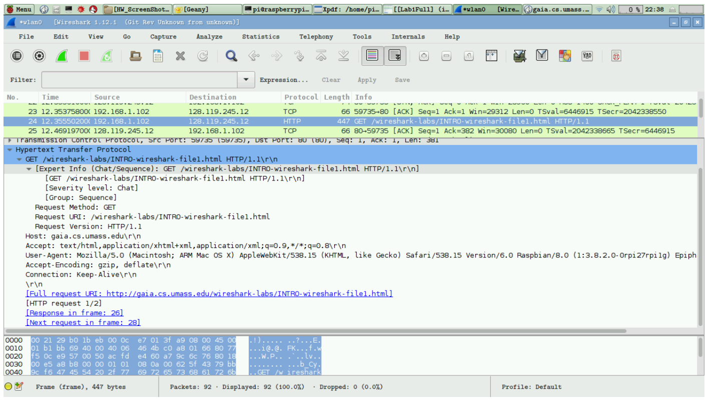
is the reply info.

```
No.     Time               Source                Destination           Protocol Length Info
     24 22:36:35.733640000 192.168.1.102         128.119.245.12        HTTP     447    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 24: 447 bytes on wire (3576 bits), 447 bytes captured (3576 bits) on interface 0
Ethernet II, Src: Mediatek_01:3f:a9 (00:0c:e7:01:3f:a9), Dst: Cisco-Li_b0:1b:eb (00:21:29:b0:1b:eb)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 59735 (59735), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 381
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]
            [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; ARM Mac OS X) AppleWebKit/538.15 (KHTML, like Gecko) Safari/538.15 Version/6.0 Raspbian/8.0 (1:3.8.2.0-0rpi27
    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 1/2]
    [Response in frame: 26]
    [Next request in frame: 28]


No.     Time               Source                Destination           Protocol Length Info
     26 22:36:35.848417000 128.119.245.12        192.168.1.102         HTTP     506    HTTP/1.1 200 OK  (text/html)

Frame 26: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface 0
Ethernet II, Src: Cisco-Li_b0:1b:eb (00:21:29:b0:1b:eb), Dst: Mediatek_01:3f:a9 (00:0c:e7:01:3f:a9)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59735 (59735), Seq: 1, Ack: 382, Len: 440
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Date: Sat, 09 Apr 2016 22:36:35 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, 09 Apr 2016 05:59:01 GMT\r\n
    ETag: "51-530070219d7eb"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\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: 0.114777000 seconds]
    [Request in frame: 24]
    [Next request in frame: 28]
    [Next response in frame: 29]
Line-based text data: text/html
```



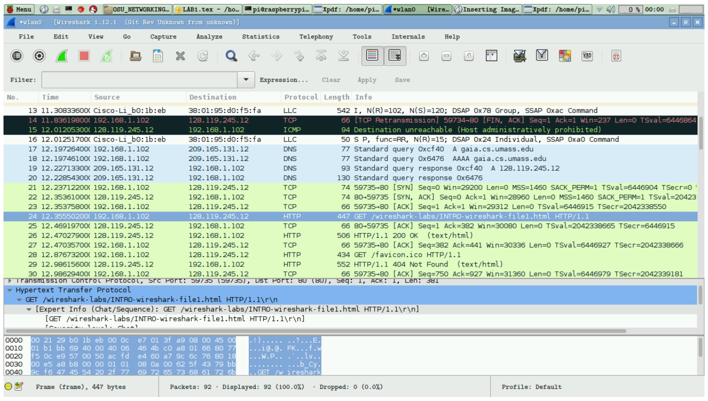
```
No.  Time             Source           Destination      Protocol Length Info
  23 12.35375800( 192.168.1.102    128.119.245.12   TCP          66 59735→80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=6446915 TSecr=2042338550
  24 12.35550200( 192.168.1.102    128.119.245.12   HTTP        447 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  25 12.46919700( 128.119.245.12   192.168.1.102    TCP          66 80→59735 [ACK] Seq=1 Ack=382 Win=30080 Len=0 TSval=2042338665 TSecr=6446915
```

```
▸ Transmission Control Protocol, Src Port: 59735 (59735), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 381
▾ 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]
        [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/INTRO-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; ARM Mac OS X) AppleWebKit/538.15 (KHTML, like Gecko) Safari/538.15 Version/6.0 Raspbian/8.0 (1:3.8.2.0-0rpi27rpi1g) Epiph
    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 1/2]
    [Response in frame: 26]
    [Next request in frame: 28]
```

```
0000  00 21 29 b0 1b eb 00 0c  e7 01 3f a9 08 00 45 00   .!)..... ..?...E.
0010  01 b1 bb 69 40 00 40 06  46 4b c0 a8 01 66 80 77   ...i@.@. FK...f.w
0020  f5 0c e9 57 00 50 ac fd  e4 60 a7 9c 6c 76 80 18   ...W.P.. .`..lv..
0030  00 e5 a8 b8 00 00 01 01  08 0a 00 62 5f 43 79 bb   ........ ...b_Cy.
0040  9c f6 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ..GET /w ireshark
```

```
Frame (frame), 447 bytes    Packets: 92 · Displayed: 92 (100.0%)  · Dropped: 0 (0.0%)    Profile: Default
```

Figure 1: Showing complete HTTP protocol info for request



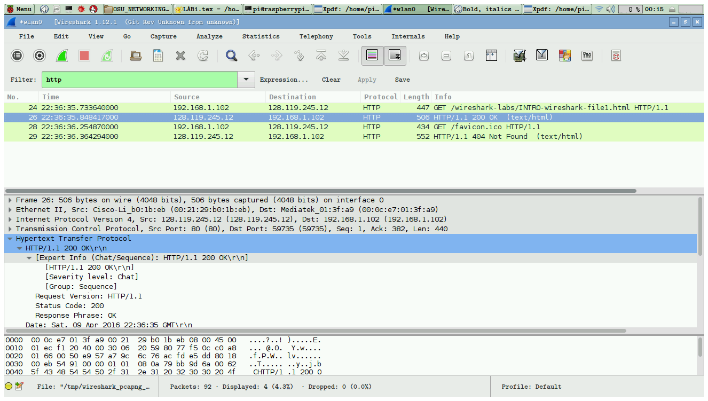
```
No.  Time         Source             Destination        Protocol Length Info
  13 11.30833600( Cisco-Li_b0:1b:eb  38:01:95:d0:f5:fa  LLC         542 I, N(R)=102, N(S)=120; DSAP 0x78 Group, SSAP 0xac Command
  14 11.83619800( 192.168.1.102      128.119.245.12     TCP          66 [TCP Retransmission] 59734→80 [FIN, ACK] Seq=1 Ack=1 Win=237 Len=0 TSval=6446864
  15 12.01205300( 128.119.245.12     192.168.1.102      ICMP         94 Destination unreachable (Host administratively prohibited)
  16 12.01251700( Cisco-Li_b0:1b:eb  38:01:95:d0:f5:fa  LLC          50 S P, func=RR, N(R)=15; DSAP 0x24 Individual, SSAP 0xa0 Command
  17 12.19726400( 192.168.1.102      209.165.131.12     DNS          77 Standard query 0xcf40  A gaia.cs.umass.edu
  18 12.19746100( 192.168.1.102      209.165.131.12     DNS          77 Standard query 0x6476  AAAA gaia.cs.umass.edu
  19 12.22713300( 209.165.131.12     192.168.1.102      DNS          93 Standard query response 0xcf40  A 128.119.245.12
  20 12.22854300( 209.165.131.12     192.168.1.102      DNS         130 Standard query response 0x6476
  21 12.23712200( 192.168.1.102      128.119.245.12     TCP          74 59735→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=6446904 TSecr=0
  22 12.35361000( 128.119.245.12     192.168.1.102      TCP          74 80→59735 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=20423
  23 12.35375800( 192.168.1.102      128.119.245.12     TCP          66 59735→80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=6446915 TSecr=2042338550
  24 12.35550200( 192.168.1.102      128.119.245.12     HTTP        447 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  25 12.46919700( 128.119.245.12     192.168.1.102      TCP          66 80→59735 [ACK] Seq=1 Ack=382 Win=30080 Len=0 TSval=2042338665 TSecr=6446915
  26 12.47027900( 128.119.245.12     192.168.1.102      HTTP        506 HTTP/1.1 200 OK  (text/html)
  27 12.47035700( 192.168.1.102      128.119.245.12     TCP          66 59735→80 [ACK] Seq=382 Ack=441 Win=30336 Len=0 TSval=6446927 TSecr=2042338666
  28 12.87673200( 192.168.1.102      128.119.245.12     HTTP        434 GET /favicon.ico HTTP/1.1
  29 12.98615600( 128.119.245.12     192.168.1.102      HTTP        552 HTTP/1.1 404 Not Found  (text/html)
  30 12.98629400( 192.168.1.102      128.119.245.12     TCP          66 59735→80 [ACK] Seq=750 Ack=927 Win=31360 Len=0 TSval=6446979 TSecr=2042339181
```

```
▸ Transmission Control Protocol, Src Port: 59735 (59735), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 381
▾ 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]
        [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
```

```
0000  00 21 29 b0 1b eb 00 0c  e7 01 3f a9 08 00 45 00   .!)..... ..?...E.
0010  01 b1 bb 69 40 00 40 06  46 4b c0 a8 01 66 80 77   ...i@.@. FK...f.w
0020  f5 0c e9 57 00 50 ac fd  e4 60 a7 9c 6c 76 80 18   ...W.P.. .`..lv..
0030  00 e5 a8 b8 00 00 01 01  08 0a 00 62 5f 43 79 bb   ........ ...b_Cy.
0040  9c f6 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ..GET /w ireshark
```

```
Frame (frame), 447 bytes    Packets: 92 · Displayed: 92 (100.0%)  · Dropped: 0 (0.0%)    Profile: Default
```

Figure 2: Three (plus) different protocols listed



Filter: http

```
No.  Time                Source           Destination      Protocol Length Info
  24 22:36:35.733640000  192.168.1.102    128.119.245.12   HTTP        447 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  26 22:36:35.848417000  128.119.245.12   192.168.1.102    HTTP        506 HTTP/1.1 200 OK  (text/html)
  28 22:36:36.254870000  192.168.1.102    128.119.245.12   HTTP        434 GET /favicon.ico HTTP/1.1
  29 22:36:36.364294000  128.119.245.12   192.168.1.102    HTTP        552 HTTP/1.1 404 Not Found  (text/html)
```

```
▸ Frame 26: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface 0
▸ Ethernet II, Src: Cisco-Li_b0:1b:eb (00:21:29:b0:1b:eb), Dst: Mediatek_01:3f:a9 (00:0c:e7:01:3f:a9)
▸ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
▸ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59735 (59735), Seq: 1, Ack: 382, Len: 440
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    ▾ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Sat, 09 Apr 2016 22:36:35 GMT\r\n
```

```
0000  00 0c e7 01 3f a9 00 21  29 b0 1b eb 08 00 45 00   ....?..! ).....E.
0010  01 ec f1 20 40 00 30 06  20 59 80 77 f5 0c c0 a8   ... @.0.  Y.w....
0020  01 66 00 50 e9 57 a7 9c  6c 76 ac fd e5 dd 80 18   .f.P.W.. lv......
0030  00 eb 54 91 00 00 01 01  08 0a 79 bb 9d 6a 00 62   ..T..... ..y..j.b
0040  5f 43 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f    CHTTP/1 .1 200 O
```

```
File: "/tmp/wireshark_pcapng_…    Packets: 92 · Displayed: 4 (4.3%)  · Dropped: 0 (0.0%)    Profile: Default
```

Figure 3: Time display changed to Time-of-Day for calculation.