TTM4100 - Lab 1

Sander Lindberg

1 Question 1

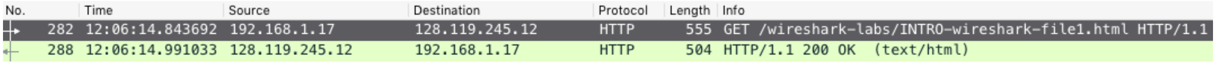
> *"List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.*

Answer: TCP, DNS, HTTP

2 Question 2

> *"How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)"*

Answer:



No.	Time	Source	Destination	Protocol	Length	Info
282	12:06:14.843692	192.168.1.17	128.119.245.12	HTTP	555	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
288	12:06:14.991033	128.119.245.12	192.168.1.17	HTTP	504	HTTP/1.1 200 OK (text/html)

Figur 1: Snippet of Wireshark trace

The GET message was sent **12:06:14.843692** and the OK message was recieved **12:06:14.991033**, so it took about **0.147341** seconds.

3 Question 3

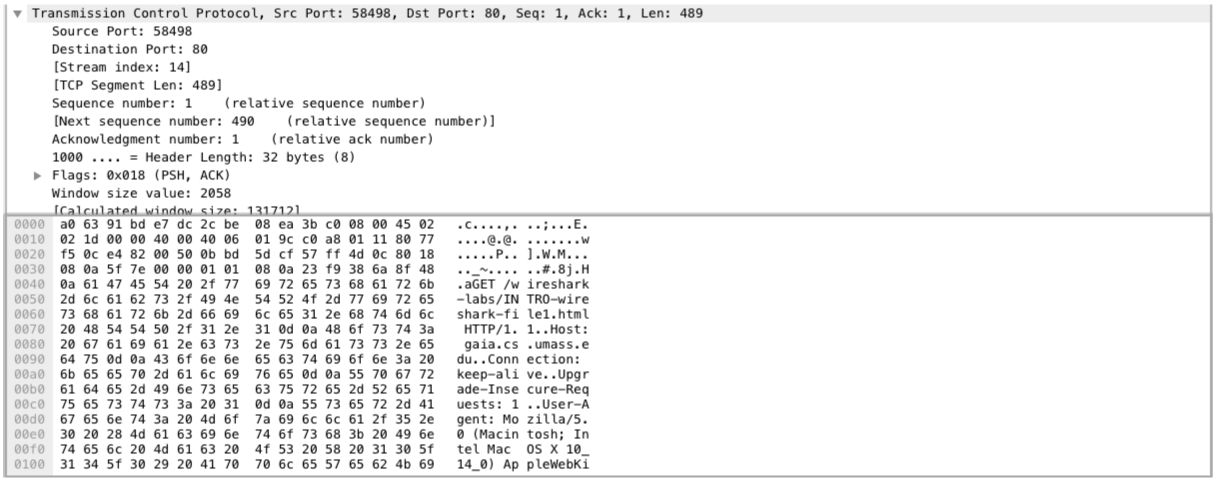
> *"What is the Internet address of the gaia.cs.umass.edu (also known as www.net.cs.umass.edu)? What is the Internet address of your computer?"*

Answer: From figure 1, we see that the Internet address of **gaia.cs.umass.edu** is **128.119.245.12** (The destination in the GET message) and the Internet address for my computer is **192.168.1.17** (the source address in the GET message).

4 Question 4

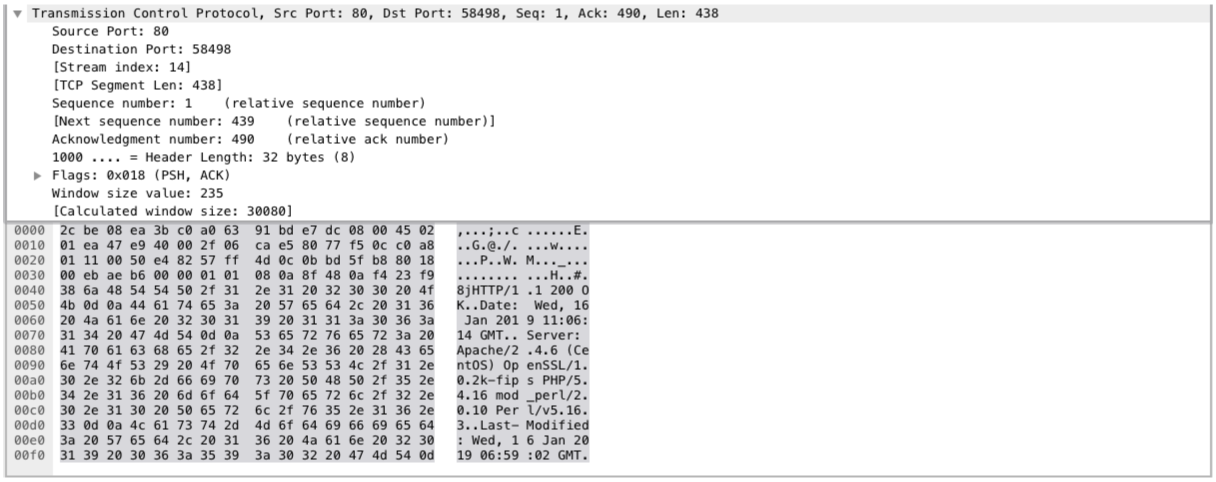
> *"Take screenshots of the two HTTP messages (GET and OK) referred to in question 2 above. The screenshots should include the packet-header window for these messages and the packet list window (see the beginning of this tutorial for the descriptions of the different windows)."*

Answer:



```
▼ Transmission Control Protocol, Src Port: 58498, Dst Port: 80, Seq: 1, Ack: 1, Len: 489
    Source Port: 58498
    Destination Port: 80
    [Stream index: 14]
    [TCP Segment Len: 489]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 490    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  ▶ Flags: 0x018 (PSH, ACK)
    Window size value: 2058
    [Calculated window size: 131712]
0000  a0 63 91 bd e7 dc 2c be  08 ea 3b c0 08 00 45 02   .c....,. ..;...E.
0010  02 1d 00 00 40 00 40 06  01 9c c0 a8 01 11 80 77   ....@.@. .......w
0020  f5 0c e4 82 00 50 0b bd  5d cf 57 ff 4d 0c 80 18   .....P.. ].W.M...
0030  08 0a 5f 7e 00 00 01 01  08 0a 23 f9 38 6a 8f 48   .._~.... ..#.8j.H
0040  0a 61 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   .aGET /w ireshark
0050  2d 6c 61 62 73 2f 49 4e  54 52 4f 2d 77 69 72 65   -labs/IN TRO-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 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   du..Conn ection: 
00a0  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 55 70 67 72   keep-ali ve..Upgr
00b0  61 64 65 2d 49 6e 73 65  63 75 72 65 2d 52 65 71   ade-Inse cure-Req
00c0  75 65 73 74 73 3a 20 31  0d 0a 55 73 65 72 2d 41   uests: 1 ..User-A
00d0  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
00e0  30 20 28 4d 61 63 69 6e  74 6f 73 68 3b 20 49 6e   0 (Macin tosh; In
00f0  74 65 6c 20 4d 61 63 20  4f 53 20 58 20 31 30 5f   tel Mac  OS X 10_
0100  31 34 5f 30 29 20 41 70  70 6c 65 57 65 62 4b 69   14_0) Ap pleWebKi
```

Figur 2: Get message



```
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 58498, Seq: 1, Ack: 490, Len: 438
    Source Port: 80
    Destination Port: 58498
    [Stream index: 14]
    [TCP Segment Len: 438]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 439    (relative sequence number)]
    Acknowledgment number: 490    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  ▶ Flags: 0x018 (PSH, ACK)
    Window size value: 235
    [Calculated window size: 30080]
0000  2c be 08 ea 3b c0 a0 63  91 bd e7 dc 08 00 45 02   ,...;..c ......E.
0010  01 ea 47 e9 40 00 2f 06  ca e5 80 77 f5 0c c0 a8   ..G.@./. ...w....
0020  01 11 00 50 e4 82 57 ff  4d 0c 0b bd 5f b8 80 18   ...P..W. M..._...
0030  00 eb ae b6 00 00 01 01  08 0a 8f 48 0a f4 23 f9   ........ ...H..#.
0040  38 6a 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   8jHTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 57 65 64 2c 20 31 36   K..Date:  Wed, 16
0060  20 4a 61 6e 20 32 30 31  39 20 31 31 3a 30 36 3a    Jan 201 9 11:06:
0070  31 34 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   14 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 32 6b 2d 66 69 70  73 20 50 48 50 2f 35 2e   0.2k-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 31 30 20 50 65 72  6c 2f 76 35 2e 31 36 2e   0.10 Per l/v5.16.
00d0  33 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   3..Last- Modified
00e0  3a 20 57 65 64 2c 20 31  36 20 4a 61 6e 20 32 30   : Wed, 1 6 Jan 20
00f0  31 39 20 30 36 3a 35 39  3a 30 32 20 47 4d 54 0d   19 06:59 :02 GMT.
```

Figur 3: OK message