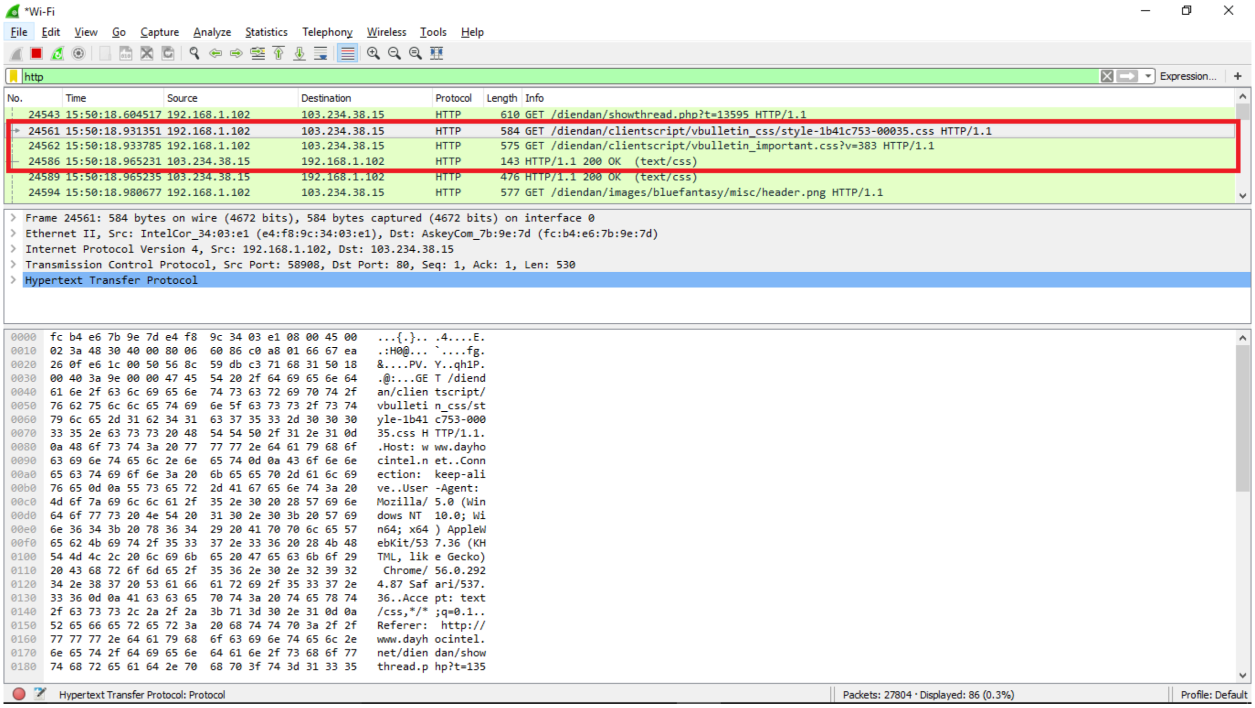
Họ Và Tên: Phạm Thị Hồng Hạnh
Mã SV: 15022830

1. List the different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
   Answer:
   - QUIC
   - TLS
   - ARP
   - UDP
   - TCP
   - HTTP
   - SSDP
   - IGMP
   - DNS
   - MDNS
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 packetlisting 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:
   - The HTTP was sent at 18.931351 and the reply was received at 18.965231. The delay was 0.03388.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

http

```
No.   Time            Source          Destination     Protocol Length Info
24543 15:50:18.604517 192.168.1.102   103.234.38.15   HTTP     610 GET /diendan/showthread.php?t=13595 HTTP/1.1
24561 15:50:18.931351 192.168.1.102   103.234.38.15   HTTP     584 GET /diendan/clientscript/vbulletin_css/style-1b41c753-00035.css HTTP/1.1
24562 15:50:18.933785 192.168.1.102   103.234.38.15   HTTP     575 GET /diendan/clientscript/vbulletin_important.css?v=383 HTTP/1.1
24586 15:50:18.965231 103.234.38.15   192.168.1.102   HTTP     143 HTTP/1.1 200 OK  (text/css)
24589 15:50:18.965235 103.234.38.15   192.168.1.102   HTTP     476 HTTP/1.1 200 OK  (text/css)
24594 15:50:18.980677 192.168.1.102   103.234.38.15   HTTP     577 GET /diendan/images/bluefantasy/misc/header.png HTTP/1.1
```

```
> Frame 24561: 584 bytes on wire (4672 bits), 584 bytes captured (4672 bits) on interface 0
> Ethernet II, Src: IntelCor_34:03:e1 (e4:f8:9c:34:03:e1), Dst: AskeyCom_7b:9e:7d (fc:b4:e6:7b:9e:7d)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 103.234.38.15
> Transmission Control Protocol, Src Port: 58908, Dst Port: 80, Seq: 1, Ack: 1, Len: 530
> Hypertext Transfer Protocol
```

```
0000  fc b4 e6 7b 9e 7d e4 f8  9c 34 03 e1 08 00 45 00   ...{.}.. .4....E.
0010  02 3a 48 30 40 00 80 06  60 86 c0 a8 01 66 67 ea   .:H0@... `....fg.
0020  26 0f e6 1c 00 50 56 8c  59 db c3 71 68 31 50 18   &....PV. Y..qh1P.
0030  00 40 3a 9e 00 00 47 45  54 20 2f 64 69 65 6e 64   .@:...GE T /diend
0040  61 6e 2f 63 6c 69 65 6e  74 73 63 72 69 70 74 2f   an/clien tscript/
0050  76 62 75 6c 6c 65 74 69  6e 5f 63 73 73 2f 73 74   vbulleti n_css/st
0060  79 6c 65 2d 31 62 34 31  63 37 35 33 2d 30 30 30   yle-1b41 c753-000
0070  33 35 2e 63 73 73 20 48  54 54 50 2f 31 2e 31 0d   35.css H TTP/1.1.
0080  0a 48 6f 73 74 3a 20 77  77 77 2e 64 61 79 68 6f   .Host: w ww.dayho
0090  63 69 6e 74 65 6c 2e 6e  65 74 0d 0a 43 6f 6e 6e   cintel.n et..Conn
00a0  65 63 74 69 6f 6e 3a 20  6b 65 65 70 2d 61 6c 69   ection:  keep-ali
00b0  76 65 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   ve..User -Agent: 
00c0  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
00d0  64 6f 77 73 20 4e 54 20  31 30 2e 30 3b 20 57 69   dows NT  10.0; Wi
00e0  6e 36 34 3b 20 78 36 34  29 20 41 70 70 6c 65 57   n64; x64 ) AppleW
00f0  65 62 4b 69 74 2f 35 33  37 2e 33 36 20 28 4b 48   ebKit/53 7.36 (KH
0100  54 4d 4c 2c 20 6c 69 6b  65 20 47 65 63 6b 6f 29   TML, lik e Gecko)
0110  20 43 68 72 6f 6d 65 2f  35 36 2e 30 2e 32 39 32    Chrome/ 56.0.292
0120  34 2e 38 37 20 53 61 66  61 72 69 2f 35 33 37 2e   4.87 Saf ari/537.
0130  33 36 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   36..Acce pt: text
0140  2f 63 73 73 2c 2a 2f 2a  3b 71 3d 30 2e 31 0d 0a   /css,*/* ;q=0.1..
0150  52 65 66 65 72 65 72 3a  20 68 74 74 70 3a 2f 2f   Referer:  http://
0160  77 77 77 2e 64 61 79 68  6f 63 69 6e 74 65 6c 2e   www.dayh ocintel.
0170  6e 65 74 2f 64 69 65 6e  64 61 6e 2f 73 68 6f 77   net/dien dan/show
0180  74 68 72 65 61 64 2e 70  68 70 3f 74 3d 31 33 35   thread.p hp?t=135
```

Hypertext Transfer Protocol: Protocol | Packets: 27804 · Displayed: 86 (0.3%) | Profile: Default

3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?
   Answer:
   Internet address gaia.cs.umass.edu: 125.235.4.59
   Internet address my computer: 192.168.1.102

4. Print the two HTTP messages displayed in step 9 above. To do so, select Print from the Wireshark File command menu, and select "Selected Packet Only" and "Print as displayed" and then click OK.
   Answer:
   GET HTTP:
   24561 15:50:18.931351   192.168.1.102   103.234.38.15   HTTP
   584   GET /diendan/clientscript/vbulletin_css/ style-1b41c753-00035.css
   HTTP/1.1 Frame 24561: 584 bytes on wire (4672 bits), 584 bytes captured

```
(4672 bits) on interface 0    Interface id: 0 (\Device\NPF_{88AC6491-510A-
4D87-A6EF-C4ECD466ECD9})    Encapsulation type: Ethernet (1)
Arrival Time: Feb 22, 2017 22:50:18.931351000 SE Asia Standard Time
[Time shift for this packet: 0.000000000 seconds]    Epoch Time:
1487778618.931351000 seconds    [Time delta from previous captured
frame: 0.003497000 seconds]    [Time delta from previous displayed frame:
0.326834000 seconds]    [Time since reference or first frame:
176.855383000 seconds]    Frame Number: 24561    Frame Length: 584
bytes (4672 bits)    Capture Length: 584 bytes (4672 bits)    [Frame is
marked: False]    [Frame is ignored: False]    [Protocols in frame:
eth:ethertype:ip:tcp:http]    [Coloring Rule Name: HTTP]    [Coloring Rule
String: http || tcp.port == 80 || http2] Ethernet II, Src: IntelCor_34:03:e1
(e4:f8:9c:34:03:e1), Dst: AskeyCom_7b:9e:7d (fc:b4:e6:7b:9e:7d)
Destination: AskeyCom_7b:9e:7d (fc:b4:e6:7b:9e:7d)    Source:
IntelCor_34:03:e1 (e4:f8:9c:34:03:e1)    Type: IPv4 (0x0800) Internet
Protocol Version 4, Src: 192.168.1.102, Dst: 103.234.38.15    0100 .... =
Version: 4    .... 0101 = Header Length: 20 bytes (5)    Differentiated
Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)    Total Length: 570
Identification: 0x4830 (18480)    Flags: 0x02 (Don't Fragment)    Fragment
offset: 0    Time to live: 128    Protocol: TCP (6)    Header checksum:
0x6086 [validation disabled]    [Header checksum status: Unverified]
Source: 192.168.1.102    Destination: 103.234.38.15    [Source GeoIP:
Unknown]    [Destination GeoIP: Unknown] Transmission Control Protocol,
Src Port: 58908, Dst Port: 80, Seq: 1, Ack: 1, Len: 530 Hypertext Transfer
Protocol    GET /diendan/clientscript/vbulletin_css/style-1b41c753-
00035.css HTTP/1.1\r\n    Host: www.dayhocintel.net\r\n    Connection:
keep-alive\r\n    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87
Safari/537.36\r\n    Accept: text/css,*/*;q=0.1\r\n    Referer:
http://www.dayhocintel.net/diendan/showthread.php?t=13595\r\n    Accept-
Encoding: gzip, deflate, sdch\r\n    Accept-Language: en-
US,en;q=0.8,vi;q=0.6\r\n    Cookie:
bbsessionhash=948509d0df864740573808420b92bad9;
bblastvisit=1487777344; bblastactivity=0\r\n    \r\n    [Full request URI:
http://www.dayhocintel.net/diendan/clientscript/vbulletin_css/style-
1b41c753-00035.css]    [HTTP request 1/7]    [Response in frame: 24586]
[Next request in frame: 24682]
HTTP OK:
24561 15:50:18.931351    192.168.1.102        103.234.38.15        HTTP
584    GET /diendan/clientscript/vbulletin_css/ style-1b41c753-00035.css
HTTP/1.1 Frame 24561: 584 bytes on wire (4672 bits), 584 bytes captured
(4672 bits) on interface 0    Interface id: 0 (\Device\NPF_{88AC6491-510A-
4D87-A6EF-C4ECD466ECD9})    Encapsulation type: Ethernet (1)
Arrival Time: Feb 22, 2017 22:50:18.931351000 SE Asia Standard Time
[Time shift for this packet: 0.000000000 seconds]    Epoch Time:
1487778618.931351000 seconds    [Time delta from previous captured
frame: 0.003497000 seconds]    [Time delta from previous displayed frame:
0.326834000 seconds]    [Time since reference or first frame:
176.855383000 seconds]    Frame Number: 24561    Frame Length: 584
bytes (4672 bits)    Capture Length: 584 bytes (4672 bits)    [Frame is
marked: False]    [Frame is ignored: False]    [Protocols in frame:
eth:ethertype:ip:tcp:http]    [Coloring Rule Name: HTTP]    [Coloring Rule
String: http || tcp.port == 80 || http2] Ethernet II, Src: IntelCor_34:03:e1
(e4:f8:9c:34:03:e1), Dst: AskeyCom_7b:9e:7d (fc:b4:e6:7b:9e:7d)
Destination: AskeyCom_7b:9e:7d (fc:b4:e6:7b:9e:7d)    Source:
IntelCor_34:03:e1 (e4:f8:9c:34:03:e1)    Type: IPv4 (0x0800) Internet
Protocol Version 4, Src: 192.168.1.102, Dst: 103.234.38.15    0100 .... =
Version: 4    .... 0101 = Header Length: 20 bytes (5)    Differentiated
Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)    Total Length: 570
Identification: 0x4830 (18480)    Flags: 0x02 (Don't Fragment)    Fragment
offset: 0    Time to live: 128    Protocol: TCP (6)    Header checksum:
0x6086 [validation disabled]    [Header checksum status: Unverified]
Source: 192.168.1.102    Destination: 103.234.38.15    [Source GeoIP:
Unknown]    [Destination GeoIP: Unknown] Transmission Control Protocol,
Src Port: 58908, Dst Port: 80, Seq: 1, Ack: 1, Len: 530 Hypertext Transfer
Protocol    GET /diendan/clientscript/vbulletin_css/style-1b41c753-
00035.css HTTP/1.1\r\n    Host: www.dayhocintel.net\r\n    Connection:
keep-alive\r\n    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87
Safari/537.36\r\n    Accept: text/css,*/*;q=0.1\r\n    Referer:
```

http://www.dayhocintel.net/diendan/showthread.php?t=13595\r\n   Accept-Encoding: gzip, deflate, sdch\r\n   Accept-Language: en-US,en;q=0.8,vi;q=0.6\r\n   Cookie: bbsessionhash=948509d0df8647405738084 20b92bad9; bblastvisit=1487777344; bblastactivity=0\r\n   \r\n   [Full request URI: http://www.dayhocintel.net/diendan/clientscript/vbulletin_css/style-1b41c753-00035.css]   [HTTP request 1/7]   [Response in frame: 24586]   [Next request in frame: 24682]