ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

MÔN HỌC

Bài báo cáo LAB 1-B:

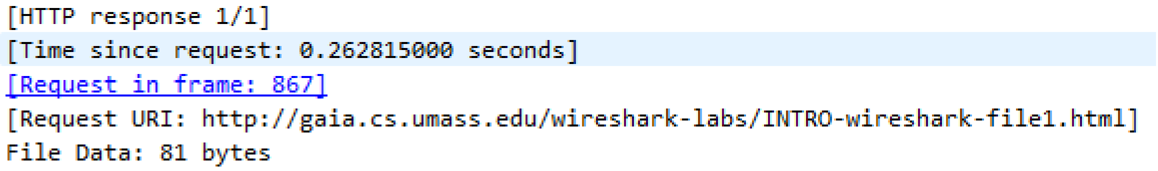
WIRESHARK INTRODUCTION

Giảng viên hướng dẫn:	Nguyễn Tấn Đạt.
Lớp:	L10.
Sinh viên thực hiện:	Đinh Như Tân
Mã số sinh viên:	1915040

HỒ CHÍ MINH, THÁNG 09 NĂM 2021

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
   Trả lời: UDP, DNS, TCP

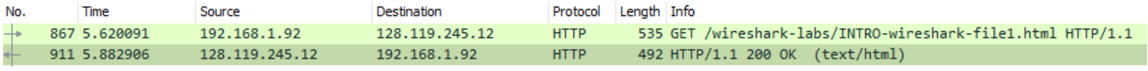
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)
   Trả lời: 0.262815000 seconds



```
[HTTP response 1/1]
[Time since request: 0.262815000 seconds]
[Request in frame: 867]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
File Data: 81 bytes
```

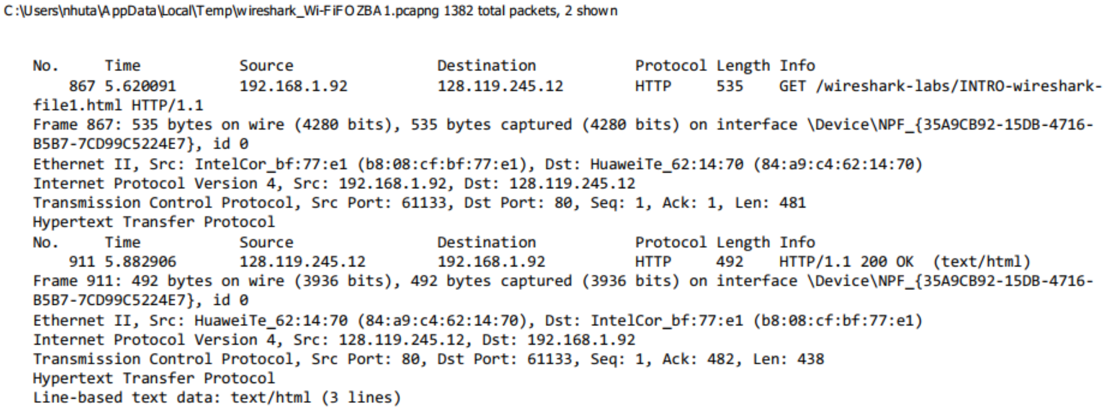
3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer? ***Trả lời:***

   - Internet address of the gaia.cs.umass.edu: 128.119.245.12
   - Internet address of my computer: 192.168.1.92



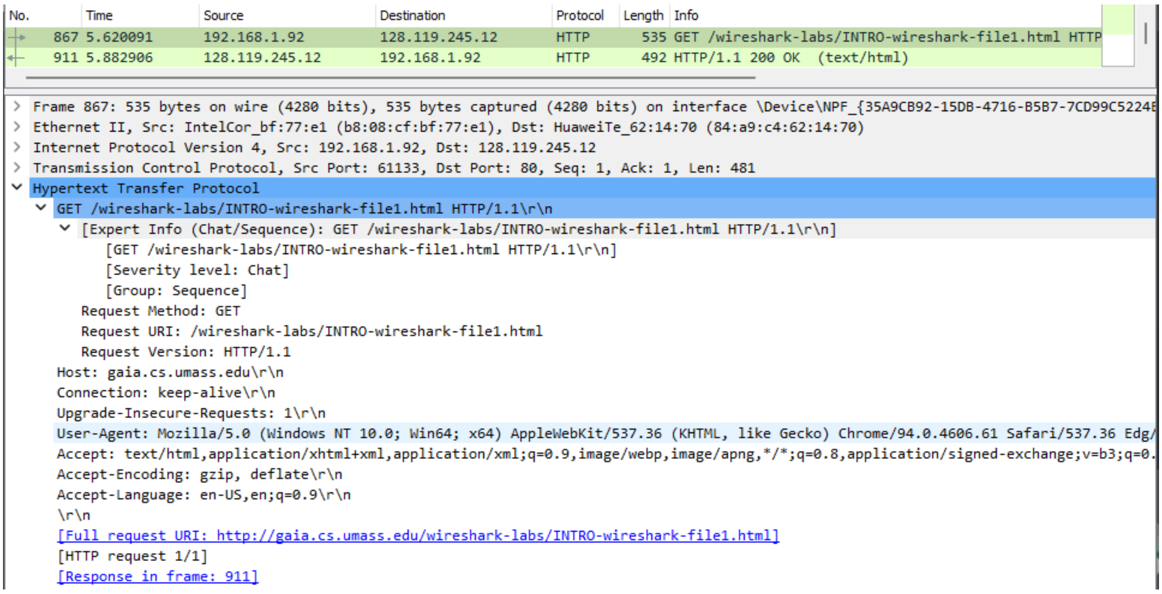
```
No.     Time        Source          Destination     Protocol  Length  Info
867  5.620091    192.168.1.92    128.119.245.12  HTTP      535  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
911  5.882906    128.119.245.12  192.168.1.92    HTTP      492  HTTP/1.1 200 OK  (text/html)
```

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.



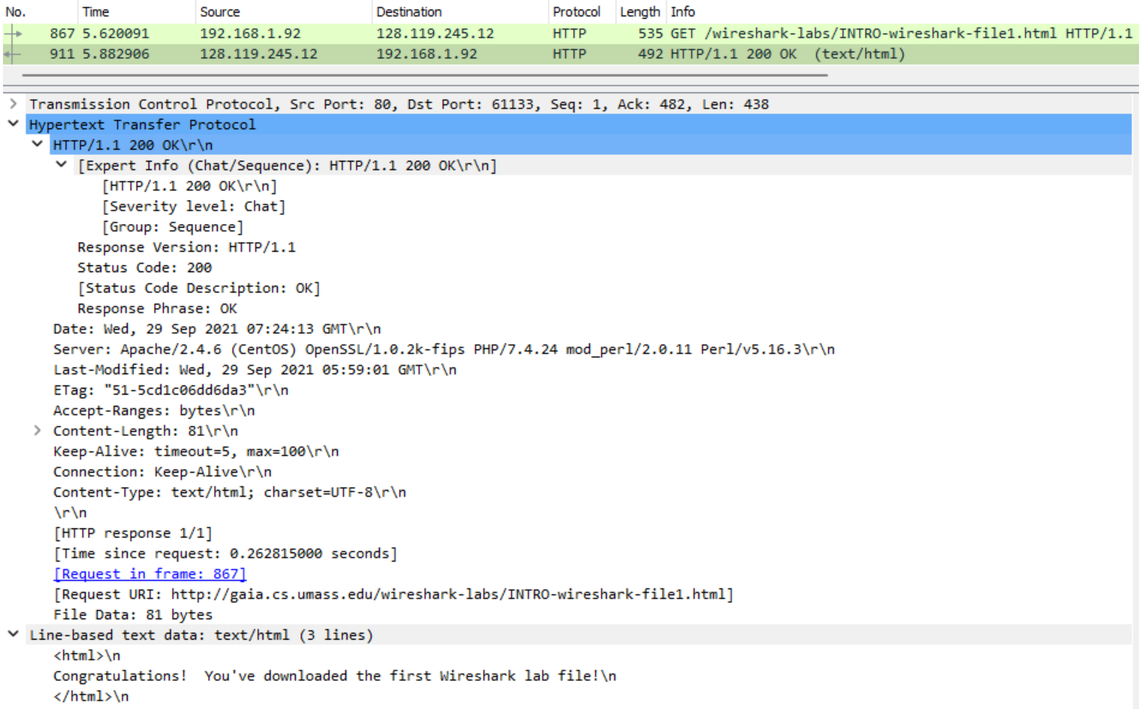
```
C:\Users\nhuta\AppData\Local\Temp\wireshark_Wi-FiFOZBA1.pcapng 1382 total packets, 2 shown


No.     Time           Source                Destination           Protocol Length Info
    867 5.620091       192.168.1.92          128.119.245.12        HTTP     535    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 867: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{35A9CB92-15DB-4716-
B5B7-7CD99C5224E7}, id 0
Ethernet II, Src: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1), Dst: HuaweiTe_62:14:70 (84:a9:c4:62:14:70)
Internet Protocol Version 4, Src: 192.168.1.92, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61133, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    911 5.882906       128.119.245.12        192.168.1.92          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 911: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{35A9CB92-15DB-4716-
B5B7-7CD99C5224E7}, id 0
Ethernet II, Src: HuaweiTe_62:14:70 (84:a9:c4:62:14:70), Dst: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.92
Transmission Control Protocol, Src Port: 80, Dst Port: 61133, Seq: 1, Ack: 482, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```



```
No.     Time        Source          Destination      Protocol  Length  Info
   867 5.620091    192.168.1.92    128.119.245.12   HTTP        535 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP
   911 5.882906    128.119.245.12  192.168.1.92     HTTP        492 HTTP/1.1 200 OK  (text/html)

> Frame 867: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{35A9CB92-15DB-4716-B5B7-7CD99C5224E
> Ethernet II, Src: IntelCor_bf:77:e1 (b8:08:cf:bf:77:e1), Dst: HuaweiTe_62:14:70 (84:a9:c4:62:14:70)
> Internet Protocol Version 4, Src: 192.168.1.92, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61133, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
v Hypertext Transfer Protocol
  v GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    v [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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36 Edg/
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 911]
```



```
No.     Time        Source          Destination      Protocol  Length  Info
   867 5.620091    192.168.1.92    128.119.245.12   HTTP        535 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   911 5.882906    128.119.245.12  192.168.1.92     HTTP        492 HTTP/1.1 200 OK  (text/html)

> Transmission Control Protocol, Src Port: 80, Dst Port: 61133, Seq: 1, Ack: 482, Len: 438
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Wed, 29 Sep 2021 07:24:13 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 29 Sep 2021 05:59:01 GMT\r\n
    ETag: "51-5cd1c06dd6da3"\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 1/1]
    [Time since request: 0.262815000 seconds]
    [Request in frame: 867]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
v Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```