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 2-A:

WIRESHARK HTTP

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. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   My browser running HTTP version: 1.1
   Version of HTTP: 1.1

2. What languages (if any) does your browser indicate that it can accept to the server?
   Accept-Language: vi-VN,vi;q=0.9

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   IP address of my computer: 192.168.1.92
   IP address of gaia.cs.umass.edu: 128.119.245.12

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

5. When was the HTML file that you are retrieving last modified at the server?
   Last-Modified: Wed, 29 Sep 2021 05:59:01 GMT

6. How many bytes of content are being returned to your browser?
   Content-Length: 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.
   No, I don't see any in the HTTP Message below

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?
   No, I don't see an "IF-MODIFIED-SINCE" line in the HTTP GET

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   Yes

```
Line-based text data: text/html (4 lines)
    <html>\n
    Congratulations.  You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n
```

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 GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?
    Yes, I see

```
If-None-Match: "80-5cd1c06dd90cb"\r\n
If-Modified-Since: Wed, 29 Sep 2021 05:59:01 GMT\r\n
\r\n
```

```
No.     Time           Source                Destination           Protocol Length Info
    196 3.294680       192.168.1.92          128.119.245.12        HTTP     529    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/
1.1
Frame 196: 529 bytes on wire (4232 bits), 529 bytes captured (4232 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: 63790, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
            [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-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/93.0.4577.82 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: vi-VN,vi;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 218]
No.     Time           Source                Destination           Protocol Length Info
    218 3.547288       128.119.245.12        192.168.1.92          HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 218: 540 bytes on wire (4320 bits), 540 bytes captured (4320 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: 63790, Seq: 1, Ack: 476, Len: 486
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]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Wed, 29 Sep 2021 08:39:58 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: "80-5cd1c06dd90cb"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
        [Content length: 128]
    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: 0.252608000 seconds]
    [Request in frame: 196]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
    <html>\n
    Congratulations.  You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n
No.     Time           Source                Destination           Protocol Length Info
    705 9.714931       192.168.1.92          128.119.245.12        HTTP     640    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/
1.1
Frame 705: 640 bytes on wire (5120 bits), 640 bytes captured (5120 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: 60385, Dst Port: 80, Seq: 1, Ack: 1, Len: 586
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
            [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
            [Severity level: Chat]
```

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.
    304 Not Modified
    The file has not been modified! So the text of the file is NOT returned in the HTTP message

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
    HTTP GET request messages: 1
    Packet number in the trace contains the GET message for the Bill or Rights: 1067

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    1118

14. What is the status code and phrase in the response?
    200 OK

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
    1118, 1233, 1234

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
There were three HTTP GET messages sent

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain
The downloads occurred in parallel. Note that the two GET messages for the images are in packets 1131 and 1134. The 200OK reply containing the images sow up as packets 1132, and 1165. Thus the request for the second image file (packet 1134) was made BEFORE packet 1132, the first image file was received

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
The HTTP GET includes the Authorization: Basic: field

```
No.     Time           Source                Destination           Protocol Length Info
    595 3.807341       192.168.1.92          221.133.13.123        HTTP/JSON 937    POST /lib/ajax/service.php?
sesskey=DEf1iIOoOJ&info=core_session_time_remaining&nosessionupdate=true HTTP/1.1 , JavaScript Object Notation (application/json)
Frame 595: 937 bytes on wire (7496 bits), 937 bytes captured (7496 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: 221.133.13.123
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 923
    Identification: 0xcec5 (52933)
    Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x7b92 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.92
    Destination Address: 221.133.13.123
Transmission Control Protocol, Src Port: 55509, Dst Port: 80, Seq: 1, Ack: 1, Len: 883
Hypertext Transfer Protocol
    POST /lib/ajax/service.php?sesskey=DEf1iIOoOJ&info=core_session_time_remaining&nosessionupdate=true HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): POST /lib/ajax/service.php?
sesskey=DEf1iIOoOJ&info=core_session_time_remaining&nosessionupdate=true HTTP/1.1\r\n]
            [POST /lib/ajax/service.php?sesskey=DEf1iIOoOJ&info=core_session_time_remaining&nosessionupdate=true HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: POST
        Request URI: /lib/ajax/service.php?sesskey=DEf1iIOoOJ&info=core_session_time_remaining&nosessionupdate=true
        Request Version: HTTP/1.1
    Host: e-learning.hcmut.edu.vn\r\n
    Connection: keep-alive\r\n
    Content-Length: 66\r\n
        [Content length: 66]
    Accept: application/json, text/javascript, */*; q=0.01\r\n
    X-Requested-With: XMLHttpRequest\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36\r\n
    Content-Type: application/json\r\n
    Origin: http://e-learning.hcmut.edu.vn\r\n
    Referer: http://e-learning.hcmut.edu.vn/user/index.php?id=103289\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5\r\n
    Cookie: _ga_72P80XK126=GS1.1.1632025274.1.1.1632025316.0; _ga=GA1.3.1182204120.1631883404; _gid=GA1.3.1999048524.1632369926;
MoodleSession=sqo1bu2mk6rccnot2mj1768iie\r\n
        Cookie pair: _ga_72P80XK126=GS1.1.1632025274.1.1.1632025316.0
        Cookie pair: _ga=GA1.3.1182204120.1631883404
        Cookie pair: _gid=GA1.3.1999048524.1632369926
        Cookie pair: MoodleSession=sqo1bu2mk6rccnot2mj1768iie
    \r\n
    [Full request URI: http://e-learning.hcmut.edu.vn/lib/ajax/service.php?
sesskey=DEf1iIOoOJ&info=core_session_time_remaining&nosessionupdate=true]
    [HTTP request 1/1]
    [Response in frame: 684]
    File Data: 66 bytes
JavaScript Object Notation: application/json
No.     Time           Source                Destination           Protocol Length Info
    684 4.644428       221.133.13.123        192.168.1.92          HTTP/JSON 468    HTTP/1.1 200 OK , JavaScript Object Notation
(application/json)
Frame 684: 468 bytes on wire (3744 bits), 468 bytes captured (3744 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: 221.133.13.123, Dst: 192.168.1.92
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 454
    Identification: 0xbce7 (48359)
    Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 50
    Protocol: TCP (6)
    Header Checksum: 0xdd45 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 221.133.13.123
    Destination Address: 192.168.1.92
Transmission Control Protocol, Src Port: 80, Dst Port: 55509, Seq: 1, Ack: 884, Len: 414
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]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Wed, 29 Sep 2021 09:11:00 GMT\r\n
    Server: Apache\r\n
    X-Powered-By: PHP/7.2.34\r\n
    Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
    Cache-Control: no-store, no-cache, must-revalidate\r\n
    Pragma: no-cache\r\n
    Keep-Alive: timeout=3, max=500\r\n
    Connection: Keep-Alive\r\n
    Transfer-Encoding: chunked\r\n
    Content-Type: application/json; charset=utf-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.837087000 seconds]
    [Request in frame: 595]
    [Request URI: http://e-learning.hcmut.edu.vn/lib/ajax/service.php?
sesskey=DEf1iIOoOJ&info=core_session_time_remaining&nosessionupdate=true]
    HTTP chunked response
    File Data: 64 bytes
JavaScript Object Notation: application/json
No.     Time           Source                Destination           Protocol Length Info
   1067 7.868894       192.168.1.92          128.119.245.12        HTTP     529    GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/
1.1
Frame 1067: 529 bytes on wire (4232 bits), 529 bytes captured (4232 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
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 515
    Identification: 0x7db2 (32178)
    Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x43ba [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.92
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 61117, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
            [GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file3.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/93.0.4577.82 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: vi-VN,vi;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    [HTTP request 1/1]
    [Response in frame: 1119]
No.     Time           Source                Destination           Protocol Length Info
   1119 8.119299       128.119.245.12        192.168.1.92          HTTP     679    HTTP/1.1 200 OK  (text/html)
Frame 1119: 679 bytes on wire (5432 bits), 679 bytes captured (5432 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
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 665
    Identification: 0x37e9 (14313)
    Flags: 0x40, Don't fragment
```

```
    Fragment Offset: 0
    Time to Live: 39
    Protocol: TCP (6)
    Header Checksum: 0xe1ed [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 192.168.1.92
Transmission Control Protocol, Src Port: 80, Dst Port: 61117, Seq: 4237, Ack: 476, Len: 625
[2 Reassembled TCP Segments (4861 bytes): #1118(4236), #1119(625)]
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]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Wed, 29 Sep 2021 09:11:04 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: "1194-5cd1c06dd5632"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 4500\r\n
        [Content length: 4500]
    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: 0.251205000 seconds]
    [Request in frame: 1067]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
    <p><br>\n
    </p>\n
    <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
      <em>Amendments 1-10 of the Constitution</em>\n
    </center>\n
    \n
    <p>The Conventions of a number of the States having, at the time of adopting\n
    the Constitution, expressed a desire, in order to prevent misconstruction\n
    or abuse of its powers, that further declaratory and restrictive clauses\n
    should be added, and as extending the ground of public confidence in the\n
    Government will best insure the beneficent ends of its institution; </p><p>  Resolved, by the Senate and House of Representatives of
the United\n
    States of America, in Congress assembled, two-thirds of both Houses concurring,\n
    that the following articles be proposed to the Legislatures of the several\n
    States, as amendments to the Constitution of the United States; all or any\n
    of which articles, when ratified by three-fourths of the said Legislatures,\n
    to be valid to all intents and purposes as part of the said Constitution,\n
    namely:    </p><p><a name="1"><strong><h3>Amendment I</h3></strong></a>\n
    \n
    <p></p><p>Congress shall make no law respecting an establishment of\n
    religion, or prohibiting the free exercise thereof; or\n
    abridging the freedom of speech, or of the press; or the\n
    right of the people peaceably to assemble, and to petition\n
    the government for a redress of grievances.\n
    \n
    </p><p><a name="2"><strong><h3>Amendment II</h3></strong></a>\n
    \n
    <p></p><p>A well regulated militia, being necessary to the security\n
    of a free state, the right of the people to keep and bear\n
    arms, shall not be infringed.\n
    \n
    </p><p><a name="3"><strong><h3>Amendment III</h3></strong></a>\n
    \n
    <p></p><p>No soldier shall, in time of peace be quartered in any house,\n
    without the consent of the owner, nor in time of war, but\n
    in a manner to be prescribed by law.\n
    \n
    </p><p><a name="4"><strong><h3>Amendment IV</h3></strong></a>\n
    \n
```