



Lab 2

BÁO CÁO BÀI THỰC HÀNH SỐ [2]

Phân tích gói tin HTTP với Wireshark

Sniffing HTTP Traffic with Wireshark

Môn học: NHẬP MÔN MẠNG MÁY TÍNH

Sinh viên thực hiện	Nguyễn Dương Đại (23520217)
Thời gian thực hiện	1/10/2024 – 07/10/2024
Số câu đã hoàn thành	13/13

TRẢ LỜI CÁC CÂU HỎI

Câu 1: Trình duyệt đang sử dụng phiên bản HTTP 1.0 hay 1.1? Phiên bản HTTP server đang sử dụng là bao nhiêu?

Trả lời:

No.	Time	Source	Destination	Protocol	Length	Info
137	3.986012	10.0.136.178	10.0.144.145	HTTP	560	GET /23521489.html HTTP/1.1
139	3.995528	10.0.144.145	10.0.136.178	HTTP	653	HTTP/1.1 200 OK (text/html)

- Trình duyệt đang sử dụng phiên bản HTTP 1.1

- Phiên bản HTTP sever đang sử dụng là: HTTP 1.1

Câu 2: Địa chỉ IP của máy tính bạn là bao nhiêu? Của web server là bao nhiêu?

Trả lời:

No.	Time	Source	Destination	Protocol	Length	Info
137	3.986012	10.0.136.178	10.0.144.145	HTTP	560	GET /23521489.html HTTP/1.1
139	3.995528	10.0.144.145	10.0.136.178	HTTP	653	HTTP/1.1 200 OK (text/html)

Khi gửi request từ máy ta đến server thì Source chính là máy ta và Destination chính là máy chủ. Do đó, có thể thấy, IP của máy ta là **10.0.136.178** và IP của server là **10.0.144.145**

Câu 3: Mã trạng thái (status code) trả về từ server là gì?

Trả lời:

611	8.540102	10.0.136.178	10.0.144.145	HTTP	501	GET /favicon.ico HTTP/1.1
139	3.995528	10.0.144.145	10.0.136.178	HTTP	653	HTTP/1.1 200 OK (text/html)
624	0.033518	10.0.144.145	10.0.136.178	HTTP	103	HTTP/1.1 204 Not Modified

Mã trạng thái trả về từ server là 200 OK.

- 200 OK: Truy cập thành công đến server.

Câu 4: Server đã trả về cho trình duyệt bao nhiêu bytes nội dung?

Trả lời:

No.	Time	Source	Destination	Protocol	Length	Info
137	3.986012	10.0.136.178	10.0.144.145	HTTP	560	GET /23521489.html HTTP/1.1
139	3.995528	10.0.144.145	10.0.136.178	HTTP	653	HTTP/1.1 200 OK (text/html)

```

▶ Frame 139: 653 bytes on wire (5224 bits), 653 bytes captured (5224 bits) on interface \Device\NPF_{73D50
▶ Ethernet II, Src: LiteonTechno_af:64:37 (e0:0a:f6:af:64:37), Dst: AzureWaveTec_b4:80:c1 (f8:54:f6:b4:80:
▶ Internet Protocol Version 4, Src: 10.0.144.145, Dst: 10.0.136.178
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 53562, Seq: 1, Ack: 507, Len: 599
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Content-Type: text/html\r\n
    Last-Modified: Sun, 06 Oct 2024 07:35:15 GMT\r\n
    Accept-Ranges: bytes\r\n
    ETag: "e88f3749c217db1:0"\r\n
    Server: Microsoft-IIS/10.0\r\n
    Date: Sun, 06 Oct 2024 07:44:30 GMT\r\n
  ▶ Content-Length: 374\r\n
    \r\n
    [Request in frame: 137]
    [Time since request: 0.009516000 seconds]
    [Request URI: /23521489.html]
    [Full request URI: http://10.0.144.145/23521489.html]
    File Data: 374 bytes
  ▶ Line-based text data: text/html (12 lines)

```

Mình chứng ở câu 3 trả về cho ta 1 gói tin: text.

Qua hình trên, ở **File Data** số bytes nội dung của ta là **374 bytes**.

Câu 5: Xem xét nội dung của HTTP GET đầu tiên. Bạn có thấy dòng “IF-MODIFIED-SINCE” hay không?

Trả lời:

No.	Time	Source	Destination	Protocol	Length	Info
137	3.986012	10.0.136.178	10.0.144.145	HTTP	560	GET /23521489.html HTTP/1.1
139	3.995528	10.0.144.145	10.0.136.178	HTTP	653	HTTP/1.1 200 OK (text/html)

```

▶ Frame 137: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface \Device\NPF_{73D50
▶ Ethernet II, Src: AzureWaveTec_b4:80:c1 (f8:54:f6:b4:80:c1), Dst: LiteonTechno_af:64:37 (e0:0a:f6:af:64:
▶ Internet Protocol Version 4, Src: 10.0.136.178, Dst: 10.0.144.145
▶ Transmission Control Protocol, Src Port: 53562, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
▼ Hypertext Transfer Protocol
  ▶ GET /23521489.html HTTP/1.1\r\n
    Host: 10.0.144.145\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\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/1
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: vi,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Response in frame: 139]
    [Full request URI: http://10.0.144.145/23521489.html]

```

Trong nội dung của HTTP GET đầu tiên, không tồn tại dòng “IF – MODIFIED SINCE”.

Câu 6: Xem xét nội dung phản hồi từ server. Server có thật sự trả về nội dung của file HTML hay không? Tại sao?

Trả lời:

```

> Frame 139: 653 bytes on wire (5224 bits), 653 bytes captured (5224 bits) on interface \Device\NPF_{73D50
> Ethernet II, Src: LiteonTechno_af:64:37 (e0:0a:f6:af:64:37), Dst: AzureWaveTec_b4:80:c1 (f8:54:f6:b4:80:
> Internet Protocol Version 4, Src: 10.0.144.145, Dst: 10.0.136.178
> Transmission Control Protocol, Src Port: 80, Dst Port: 53562, Seq: 1, Ack: 507, Len: 599
> Hypertext Transfer Protocol
  Line-based text data: text/html (12 lines)
    <!DOCTYPE html>\r\n
    <html>\r\n
    <head>\r\n
    <title>Thực hành nhập môn mạng máy tính - 2024</title>\r\n
    <meta charset="utf-8">\r\n
    </head>\r\n
    <body>\r\n
    <center></c
    <center><h1>MSSV: 23521489</h1></center>\r\n
    <center><h2> Họ và tên: Võ Lưu Chí Thiện</h2></center>\r\n
    </body>\r\n
    </html>\r\n

```

Sau khi xem nội dung phản hồi của server, ta thấy rằng server đã thật sự trả về nội dung của file HTML.

Giải thích: Vì ban đầu trước khi bắt gói tin, ta đã xóa cache rồi. Do đó, khi người dùng gửi request lên server, server sẽ kiểm tra xem trong cache có nội dung đó chưa. Nếu chưa thì server sẽ trả về nội dung của file đó cho người dùng. Ngược lại thì không. Vì trước khi bắt gói tin, ta đã xóa bộ nhớ cache rồi, nên server sẽ không tìm thấy file đó. Do đó, nội dung của file đó sẽ được trả về cho người dùng.

Câu 7: Xem xét nội dung của HTTP GET thứ 2. Bạn có thấy dòng “IF-MODIFIED-SINCE” hay không? Nếu có, giá trị của IF-MODIFIED-SINCE là gì?

Trả lời:

No.	Time	Source	Destination	Protocol	Length Info
137	3.986012	10.0.136.178	10.0.144.145	HTTP	560 GET /23521489.html HTTP/1.1
139	3.995528	10.0.144.145	10.0.136.178	HTTP	653 HTTP/1.1 200 OK (text/html)
611	8.540102	10.0.136.178	10.0.144.145	HTTP	501 GET /favicon.ico HTTP/1.1
613	8.593256	10.0.144.145	10.0.136.178	HTTP	1437 HTTP/1.1 404 Not Found (text/html)
623	9.806503	10.0.136.178	10.0.144.145	HTTP	629 GET /23521489.html HTTP/1.1
624	9.933518	10.0.144.145	10.0.136.178	HTTP	197 HTTP/1.1 304 Not Modified
▶ Frame 623: 629 bytes on wire (5032 bits), 629 bytes captured (5032 bits) on interface \Device\NPF_{73D50 ▶ Ethernet II, Src: AzureWaveTec_b4:80:c1 (f8:54:f6:b4:80:c1), Dst: LiteonTechno_af:64:37 (e0:0a:f6:af:64:37) ▶ Internet Protocol Version 4, Src: 10.0.136.178, Dst: 10.0.144.145 ▶ Transmission Control Protocol, Src Port: 53562, Dst Port: 80, Seq: 954, Ack: 1983, Len: 575 ▶ Hypertext Transfer Protocol GET /23521489.html HTTP/1.1\r\n Host: 10.0.144.145\r\n Connection: keep-alive\r\n Cache-Control: max-age=0\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/114.0.5884.51 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\r\n Accept-Encoding: gzip, deflate\r\n Accept-Language: vi,en-US;q=0.9,en;q=0.8\r\n If-None-Match: "e88f3749c217db1:0"\r\n If-Modified-Since: Sun, 06 Oct 2024 07:35:15 GMT\r\n \r\n [Response in frame: 624] [Full request URI: http://10.0.144.145/23521489.html]					

Trong hình trên, ở dòng được bôi đậm, ta thấy có xuất hiện “IF-MODIFIED-SINCE” với giá trị là: *Sun, 06 Oct 2024 07:35:15 GMT*

Câu 8: Mã trạng thái HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là gì? Ý nghĩa nó là gì? Server có thật sự gửi về nội dung của file hay không? Giải thích.

Trả lời:

623	9.806503	10.0.136.178	10.0.144.145	HTTP	629 GET /23521489.html HTTP/1.1
624	9.933518	10.0.144.145	10.0.136.178	HTTP	197 HTTP/1.1 304 Not Modified

```
▶ Frame 624: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits) on interface \Device\NPF_{73D56...}
▶ Ethernet II, Src: LiteonTechno_af:64:37 (e0:0a:f6:af:64:37), Dst: AzureWaveTec_b4:80:c1 (f8:54:f6:b4:80:c1)
▶ Internet Protocol Version 4, Src: 10.0.144.145, Dst: 10.0.136.178
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 53562, Seq: 1983, Ack: 1529, Len: 143
▼ Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
    Accept-Ranges: bytes\r\n
    ETag: "e88f3749c217db1:0"\r\n
    Server: Microsoft-IIS/10.0\r\n
    Date: Sun, 06 Oct 2024 07:44:36 GMT\r\n
    \r\n
    [Request in frame: 623]
    [Time since request: 0.127015000 seconds]
    [Request URI: /23521489.html]
    [Full request URI: http://10.0.144.145/23521489.html]
```

Trong hình trên, ta thấy phần thông tin của gói tin đó không có chỗ nào hiển thị cho ta về nội dung của trang web như lần GET đầu tiên.

Giải thích: Vì lúc này, trong bộ nhớ cache của ta đã có nội dung của file đó ở lần gửi request đầu tiên (được minh chứng thông qua trạng thái **304 NOT MODIFIED** được trả về), do đó, lúc này, server sẽ không gửi lại nội dung đó cho người dùng nữa.

Câu 9: Trình duyệt đã gửi bao nhiêu HTTP GET? Đến những địa chỉ IP nào?

Trả lời:

No.	Time	Source	Destination	Protocol	Length Info
137	3.986012	10.0.136.178	10.0.144.145	HTTP	560 GET /23521489.html HTTP/1.1
623	9.806503	10.0.136.178	10.0.144.145	HTTP	629 GET /23521489.html HTTP/1.1
92	3.620823	10.0.136.178	23.202.34.233	HTTP	165 GET /connecttest.txt HTTP/1.1
611	8.540102	10.0.136.178	10.0.144.145	HTTP	501 GET /favicon.ico HTTP/1.1
215	4.342986	10.0.136.178	45.122.249.78	HTTP	534 GET /sites/default/files/photos/large/202110/kimg0816.jpg HTTP/1.1

Trình duyệt đã gửi **5 HTTP GET**. Đến các địa chỉ IP: 10.0.144.145, 23.202.34.233, 45.122.249.78.

Câu 10: Trình duyệt đã gửi bao nhiêu HTTP GET? Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ mấy?

Trả lời:

No.	Time	Source	Destination	Protocol	Length	Info
19	1.710847	10.0.136.176	128.119.245.12	HTTP	592	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
30	2.008776	128.119.245.12	10.0.136.176	HTTP	595	HTTP/1.1 200 OK (text/html)
32	2.037633	10.0.136.176	128.119.245.12	HTTP	538	GET /favicon.ico HTTP/1.1
47	2.334419	128.119.245.12	10.0.136.176	HTTP	538	HTTP/1.1 404 Not Found (text/html)
84	2.598798	10.0.136.176	128.119.245.12	HTTP	662	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
815	2.894784	128.119.245.12	10.0.136.176	HTTP	294	HTTP/1.1 304 Not Modified

Trình duyệt gửi 3 HTTP GET. Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ nhất.

No.	Time	Source	Destination	Protocol	Length	Info
19	1.710847	10.0.136.176	128.119.245.12	HTTP	592	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
30	2.008776	128.119.245.12	10.0.136.176	HTTP	595	HTTP/1.1 200 OK (text/html)
32	2.037633	10.0.136.176	128.119.245.12	HTTP	538	GET /favicon.ico HTTP/1.1

```
▶ Frame 30: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface \Device\NPF_{2740...}
▶ Ethernet II, Src: HewlettPacka 50:38:0c (14:58:d0:50:38:0c), Dst: ASUSTekCOMPU_93:be:18 (e8:9c:25:93:b...)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.136.176
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 59003, Seq: 4321, Ack: 539, Len: 541
▶ [3 Reassembled TCP Segments (4861 bytes): #27(2880), #29(1440), #30(541)]
▶ Hypertext Transfer Protocol
▼ 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
  on abuse of its powers, that further declaratory and restrictive clauses\n
```

Câu 11: Cần bao nhiêu TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights?

Trả lời: Cần 3 TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights.

```

▶ Frame 996: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface \Device\NPF_{27409
▶ Ethernet II, Src: HewlettPacka_50:38:0c (14:58:d0:50:38:0c), Dst: ASUSTekCOMPU_93:be:18 (e8:9c:25:93:be:
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.136.176
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 59095, Seq: 4321, Ack: 516, Len: 541
▼ [3 Reassembled TCP Segments (4861 bytes): #993(2880), #995(1440), #996(541)]
  [Frame: 993, payload: 0-2879 (2880 bytes)]
  [Frame: 995, payload: 2880-4319 (1440 bytes)]
  [Frame: 996, payload: 4320-4860 (541 bytes)]
  [Segment count: 3]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data [...]: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c203036204f6374203230
▶ Hypertext Transfer Protocol
▶ Line-based text data: text/html (98 lines)

```

Câu 12: Mã trạng thái và ý nghĩa HTTP response tương ứng với HTTP GET đầu tiên là gì?

No.	Time	Source	Destination	Protocol	Length	Info
953	4.821872	10.0.136.176	128.119.245.12	HTTP	555	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
969	5.125350	128.119.245.12	10.0.136.176	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

Trả lời: Ta thấy HTTP response tương ứng với HTTP GET đầu tiên là **401**

Unauthorized.

Mã trạng thái 401 Unauthorized cho ta biết trang web đó yêu cầu thông tin đăng nhập của người dùng. Do đó, response trên trả về 401 Unauthorized vì ban đầu ta chưa nhập username và password tương ứng.

Câu 13: Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu nào mới nào xuất hiện trong HTTP GET? Hãy giải thích ý nghĩa và các vấn đề liên quan của trường mới này.

Trả lời: Gói HTTP GET đầu tiên:

No.	Time	Source	Destination	Protocol	Length	Info
953	4.821872	10.0.136.176	128.119.245.12	HTTP	555	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
969	5.125350	128.119.245.12	10.0.136.176	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
3550	21.696308	10.0.136.176	128.119.245.12	HTTP	640	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
3566	21.968692	128.119.245.12	10.0.136.176	HTTP	574	HTTP/1.1 404 Not Found (text/html)

```

▶ Internet Protocol Version 4, Src: 10.0.136.176, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 59280, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
▼ Hypertext Transfer Protocol
  ▶ GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1\r\n
    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/1
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: vi,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Response in frame: 969]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-]

```


Gói HTTP GET thứ 2:

http					
No.	Time	Source	Destination	Protocol	Length Info
953	4.821872	10.0.136.176	128.119.245.12	HTTP	555 GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
969	5.125350	128.119.245.12	10.0.136.176	HTTP	771 HTTP/1.1 401 Unauthorized (text/html)
3550	21.696308	10.0.136.176	128.119.245.12	HTTP	640 GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
3566	21.968692	128.119.245.12	10.0.136.176	HTTP	574 HTTP/1.1 404 Not Found (text/html)
▶ Frame 3550: 640 bytes on wire (5120 bits), 640 bytes captured (5120 bits) on interface \Device\NPF_{2740...}					
▶ Ethernet II, Src: ASUSTekCOMPU_93:be:18 (e8:9c:25:93:be:18), Dst: HewlettPacka_50:38:0c (14:58:d0:50:38:0c)					
▶ Internet Protocol Version 4, Src: 10.0.136.176, Dst: 128.119.245.12					
▶ Transmission Control Protocol, Src Port: 59285, Dst Port: 80, Seq: 1, Ack: 1, Len: 586					
▼ Hypertext Transfer Protocol					
▶ GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1\r\n					
Host: gaia.cs.umass.edu\r\n					
Connection: keep-alive\r\n					
Cache-Control: max-age=0\r\n					
▼ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcmcs=\r\n					
Credentials: wireshark-students:network					
Upgrade-Insecure-Requests: 1\r\n					
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36					
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8					
Accept-Encoding: gzip, deflate\r\n					
Accept-Language: vi,en-US;q=0.9,en;q=0.8\r\n					
\r\n					
[Response in frame: 3566]					
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-]					

Khi so sánh giữa nội dung gói tin HTTP GET lần thứ 1 và lần thứ 2, ta thấy rằng, trong nội dung của HTTP GET lần thứ 2 xuất hiện trường dữ liệu mới: **Authorization**. Trong trường dữ liệu mới đó, ta thấy nội dung **Credentials** nó lưu giữ thông tin **username** và **password** mà ta phải nhập vào nếu muốn truy cập vào trang web.

Ý nghĩa và các vấn đề liên quan **Authorization**:

Trường **Authorization** xác định quyền truy cập của người dùng hoặc hệ thống đến tài nguyên trong ứng dụng. Ý nghĩa chính gồm:

1. **Kiểm soát truy cập**: Chỉ cho phép những người dùng có quyền thực hiện các hành động nhất định.
2. **Bảo mật**: Ngăn chặn truy cập trái phép và bảo vệ hệ thống.

Vấn đề liên quan:

- **Quá tải quyền hạn**: Cấp quyền quá nhiều gây rủi ro bảo mật.
- **Xác thực kém**: Authentication yếu làm giảm hiệu quả Authorization.
- **Phân quyền sai sót**: Lỗi hổng trong việc quản lý quyền có thể bị khai thác.
- **Quản lý phức tạp**: Đặc biệt trong hệ thống lớn với nhiều người dùng.

Các mô hình phổ biến: **RBAC** (theo vai trò) và **ABAC** (theo thuộc tính).