

MSSV: 21520683

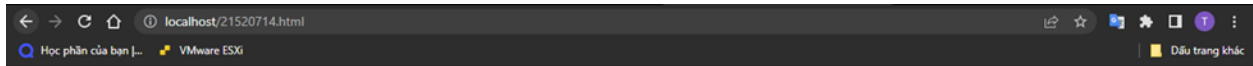
Tên: Nguyễn Thành Đăng

# NHẬP MÔN MẠNG MÁY TÍNH

## Buổi 2. Phân tích gói tin HTTP với WIRESHARK

### I. Tạo website cơ bản với Localhost





**MSSV: 21520714**

**Họ và tên: Trinh Tan Dat**

## II. HTTP GET/response có điều kiện

Máy em và bạn không thể kết nối với nhau nên kết quả Wireshark sẽ dùng số liệu của bạn khác  
Nên em dùng link: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

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

```
> [SEQ/ACK analysis]
TCP payload (584 bytes)
▼ Hypertext Transfer Protocol
> GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\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/106.0.0.0 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
If-None-Match: "51-5ea434600e715"\r\n
If-Modified-Since: Wed, 05 Oct 2022 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 2/2]
[Prev request in frame: 3081]
[Response in frame: 4208]
```

Server đang sử dụng HTTP 1.1

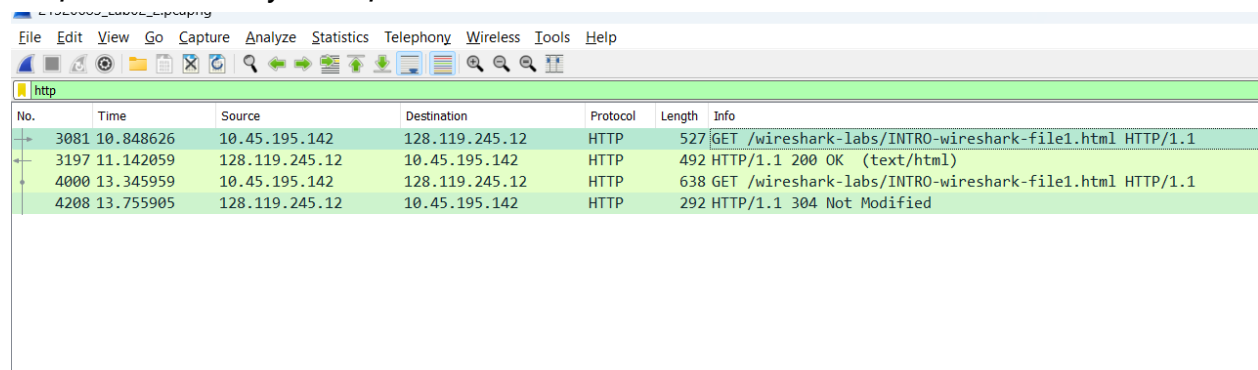
```

    TCP payload (438 bytes)
  / Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
      Date: Thu, 06 Oct 2022 02:07:18 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Wed, 05 Oct 2022 05:59:01 GMT\r\n
      ETag: "51-5ea434600e715"\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 1/2]
    [Time since request: 0.293433000 seconds]
    [Request in frame: 3081]
    [Next request in frame: 4000]

```

Trình duyệt đang sử dụng HTTP 1.1

## 2. Địa chỉ IP của máy tính bạn là bao nhiêu? Của web server là bao nhiêu?



| No.  | Time      | Source         | Destination    | Protocol | Length | Info  |
|------|-----------|----------------|----------------|----------|--------|---|
| 3081 | 10.848626 | 10.45.195.142  | 128.119.245.12 | HTTP     | 527    | GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |
| 3197 | 11.142059 | 128.119.245.12 | 10.45.195.142  | HTTP     | 492    | HTTP/1.1 200 OK (text/html)                             |
| 4000 | 13.345959 | 10.45.195.142  | 128.119.245.12 | HTTP     | 638    | GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |
| 4208 | 13.755905 | 128.119.245.12 | 10.45.195.142  | HTTP     | 292    | HTTP/1.1 304 Not Modified                               |

Địa chỉ IP của máy : 10.45.195.142

Địa chỉ IP của web server: 128.119.245.12

## 3. Mã trạng thái (status code) trả về từ server là gì?

GET lần thứ nhất

Trạng thái : 200 OK\r\n

```

    TCP payload (438 bytes)
  / Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
      Date: Thu, 06 Oct 2022 02:07:18 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Wed, 05 Oct 2022 05:59:01 GMT\r\n
      ETag: "51-5ea434600e715"\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 1/2]
    [Time since request: 0.293433000 seconds]
    [Request in frame: 3081]
    [Next request in frame: 4000]
    [Next response in frame: 4208]

```

Ý nghĩa: Website được chấp nhận, nhận được gói tin từ server

#### 4. Server đã trả về cho trình duyệt bao nhiêu bytes nội dung?

```
> HTTP/1.1 200 OK\r\n
Date: Thu, 06 Oct 2022 02:07:18 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Wed, 05 Oct 2022 05:59:01 GMT\r\n
ETag: "51-5ea434600e715"\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 1/2]
[Time since request: 0.293433000 seconds]
[Request in frame: 3081]
[Next request in frame: 4000]
[Next response in frame: 4208]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
File Data: 81 bytes
> Line-based text data: text/html (3 lines)
0170 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 .Content -Type: t
0180 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 ext/html ; charse
```

Server đã trả về 81 bytes

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

GET đầu xuất hiện

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

```
\r\n
[HTTP response 1/2]
[Time since request: 0.293433000 seconds]
[Request in frame: 3081]
[Next request in frame: 4000]
[Next response in frame: 4208]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
File Data: 81 bytes
> Line-based text data: text/html (3 lines)
<html>\n
Congratulations! You've downloaded the first Wireshark lab file!\n
</html>\n
0170 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 .Content -Type: t
0180 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 ext/html ; charse
```

Có, vì ta đã truy cập vào được trang web

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

```
request received. URI
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
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/106.0.0.0 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
If-None-Match: "51-5ea434600e715"\r\n
If-Modified-Since: Wed, 05 Oct 2022 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 2/2]
[Prev request in frame: 3081]
[Response in frame: 4208]
```

Có, giá trị là Wed

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 thực sự gửi về nội dung của file hay không? Giải thích.

|   |      |           |                |                |      |     |   |
|---|------|-----------|----------------|----------------|------|-----|---|
| ✓ | 4000 | 13.345959 | 10.45.195.142  | 128.119.245.12 | HTTP | 638 | GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |
|   | 4208 | 13.755905 | 128.119.245.12 | 10.45.195.142  | HTTP | 292 | HTTP/1.1 304 Not Modified                               |

Mã trạng thái là 304 Not Modified

Ý nghĩa: Là không có sự thay đổi trong gói tin nhận được so với lần truy cập trước

Server không thực sự gửi về nội dung của file

|   |   |
|---|---|
| ▼ | Hypertext Transfer Protocol   |
| ▼ | HTTP/1.1 304 Not Modified\r\n   |
| > | [Expert Info (Chat/Sequence): 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   |
|   | Date: Thu, 06 Oct 2022 02:07:21 GMT\r\n   |
|   | Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n |
|   | Connection: Keep-Alive\r\n  |
|   | Keep-Alive: timeout=5, max=99\r\n   |
|   | ETag: "51-5ea434600e715"\r\n  |
|   | \r\n  |
|   | [HTTP response 2/2]   |
|   | [Time since request: 0.409946000 seconds]   |
|   | <a href="#">[Prev request in frame: 3081]</a>   |
|   | <a href="#">[Prev response in frame: 3197]</a>  |
|   | <a href="#">[Request in frame: 4000]</a>  |
|   | [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]             |

Vì không có gói tin mới nhận được.

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

| No. | Time | Source    | Destination    | Protocol       | Length | Info  |
|-----|------|-----------|----------------|----------------|--------|---|
| +   | 3081 | 10.848626 | 10.45.195.142  | 128.119.245.12 | HTTP   | 527 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |
| +   | 3197 | 11.142059 | 128.119.245.12 | 10.45.195.142  | HTTP   | 492 HTTP/1.1 200 OK (text/html)                             |
| +   | 4000 | 13.345959 | 10.45.195.142  | 128.119.245.12 | HTTP   | 638 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |
| +   | 4208 | 13.755905 | 128.119.245.12 | 10.45.195.142  | HTTP   | 292 HTTP/1.1 304 Not Modified                               |

Gửi 2 đến cùng một địa chỉ IP ( Trong hình )

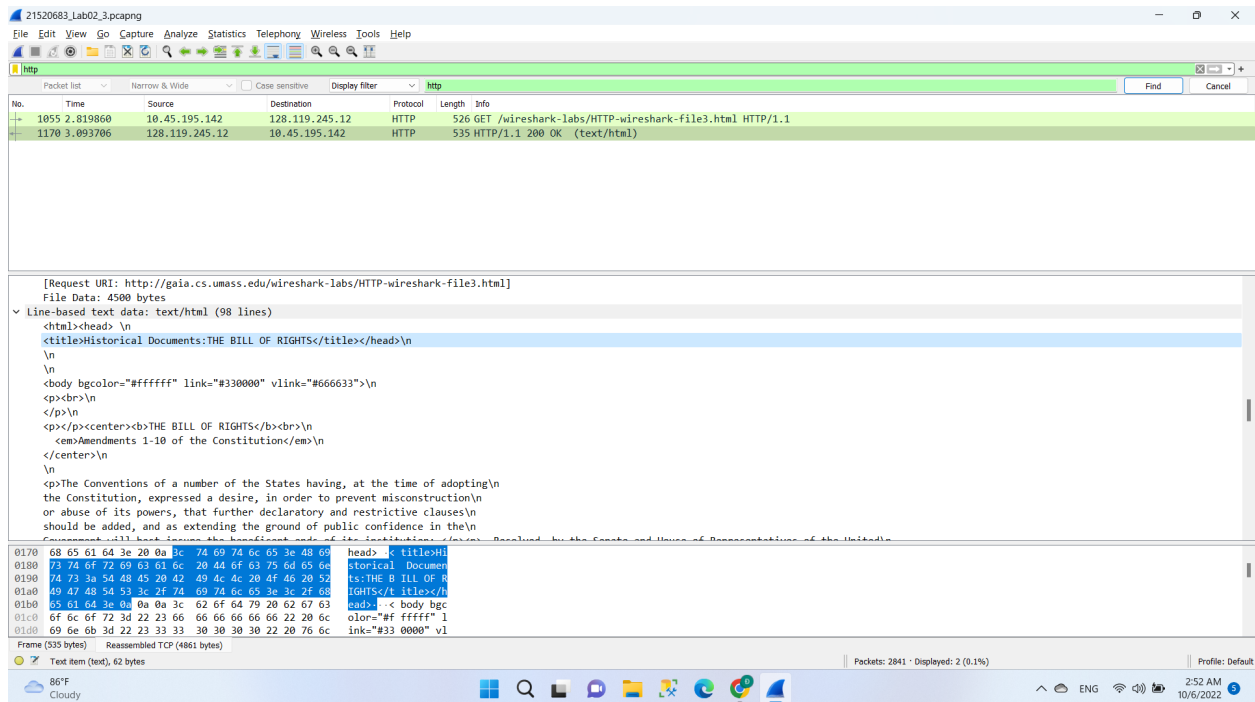
### III. Truy cập các trang HTTP dài

Link bắt gói tin: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

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

| 21520683_Lab02_3.pcapng  |      |          |                |                |        |  |
|--|------|----------|----------------|----------------|--------|--|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help |      |          |                |                |        |  |
| http   |      |          |                |                |        |  |
| No.  | Time | Source   | Destination    | Protocol       | Length | Info   |
| +  | 1055 | 2.819860 | 10.45.195.142  | 128.119.245.12 | HTTP   | 526 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 |
| +  | 1170 | 3.093706 | 128.119.245.12 | 10.45.195.142  | HTTP   | 535 HTTP/1.1 200 OK (text/html)                            |

Trình duyệt gửi 1 HTTP GET



Phản hồi trong gói tin đầu tiên

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

- > [SEQ/ACK analysis]
  - TCP payload (481 bytes)
  - TCP segment data (481 bytes)
- ✓ [3 Reassembled TCP Segments (4861 bytes): #1167(1460), #1169(2920), #1170(481)]
  - [Frame: 1167, payload: 0-1459 (1460 bytes)]
  - [Frame: 1169, payload: 1460-4379 (2920 bytes)]
  - [Frame: 1170, payload: 4380-4860 (481 bytes)]
  - [Segment count: 3]
  - [Reassembled TCP length: 4861]
  - [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205468752c203036204f63742032...]
- > Hypertext Transfer Protocol
- > Line-based text data: text/html (98 lines)

Cần 3 TCP segments

#### IV. Chứng thực HTTP

Link truy cập bắt lần 1:

[http://gaia.cs.umass.edu/wireshark-labs/protected\\_pages/HTTP-wireshark-file5.html](http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html)

Link truy cập bắt lần 2:

[http://gaia.cs.umass.edu/wireshark-labs/protected\\_pages/HTTP-wireshark-](http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-)

12. Mã trạng thái và ý nghĩa nó trong HTTP response tương ứng với HTTP GET đầu tiên là gì?

| No.  | Time      | Source         | Destination    | Protocol | Length | Info   |
|------|-----------|----------------|----------------|----------|--------|--|
| 1517 | 4.425028  | 10.45.195.142  | 128.119.245.12 | HTTP     | 542    | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 1768 | 5.360754  | 128.119.245.12 | 10.45.195.142  | HTTP     | 771    | HTTP/1.1 401 Unauthorized (text/html)                                  |
| 2531 | 8.226301  | 10.45.195.142  | 128.119.245.12 | HTTP     | 532    | GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1           |
| 2932 | 9.675445  | 128.119.245.12 | 10.45.195.142  | HTTP     | 770    | HTTP/1.1 401 Unauthorized (text/html)                                  |
| 6051 | 21.945003 | 10.45.195.142  | 128.119.245.12 | HTTP     | 617    | GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1           |

Trạng thái: 401 Unauthorized

Ý nghĩa: Cố gắng truy cập nhưng không thể được tải cho đến khi đăng nhập bằng một ID

**13. Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu nào mới nào xuất hiện trong HTTP GET?**

|      |           |                |                |      |     |  |
|------|-----------|----------------|----------------|------|-----|--|
| 1517 | 4.425028  | 10.45.195.142  | 128.119.245.12 | HTTP | 542 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 1768 | 5.360754  | 128.119.245.12 | 10.45.195.142  | HTTP | 771 | HTTP/1.1 401 Unauthorized (text/html)                                  |
| 2531 | 8.226301  | 10.45.195.142  | 128.119.245.12 | HTTP | 532 | GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1           |
| 2932 | 9.675445  | 128.119.245.12 | 10.45.195.142  | HTTP | 770 | HTTP/1.1 401 Unauthorized (text/html)                                  |
| 6051 | 21.945003 | 10.45.195.142  | 128.119.245.12 | HTTP | 617 | GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1           |
| 6733 | 23.571325 | 128.119.245.12 | 10.45.195.142  | HTTP | 574 | HTTP/1.1 404 Not Found (text/html)                                     |

|   |  |
|---|--|
| Checksum: 0x458d [unverified]   |  |
| [Checksum Status: Unverified]   |  |
| Urgent Pointer: 0   |  |
| > [Timestamps]  |  |
| > [SEQ/ACK analysis]  |  |
| TCP payload (563 bytes)   |  |
| ▼ Hypertext Transfer Protocol   |  |
| GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1\r\n  |  |
| > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1\r\n]   |  |
| Request Method: GET   |  |
| Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-  |  |
| Request Version: HTTP/1.1   |  |
| Host: gaia.cs.umass.edu\r\n   |  |
| Connection: keep-alive\r\n  |  |
| Cache-Control: max-age=0\r\n  |  |
| > Authorization: Basic d2lyZXNoYXJrLXN0dWU1bnRzOm5ldHdvcm5=\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/106.0.0.0 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 |  |
| 00b0  | 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d 0a 41 ol: max-age=0-\r\n |
| 00c0  | 75 74 68 6f 72 69 7a 61 74 69 6f 6e 3a 20 42 61 uthoriza tion: Ba  |
| 00d0  | 73 69 63 20 64 32 6c 79 5a 58 4e 6f 59 58 4a 72 sic d2ly ZXNoYXJr  |
| 00e0  | 4c 58 4e 30 64 57 52 6c 62 6e 52 7a 4f 6d 35 6d LXN0dWU1 bnRzOm5l  |
| 00f0  | 64 03 64 76 63 6d 73 2d 0a 0a 55 70 67 72 61 64 dvcm5= Upgrad      |
| 0100  | 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 e-Insecu re-Reque  |
| 0110  | 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 sts: 1 - User-Age  |
| 0120  | 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 nt: Mozi lla/5.0   |

Authorization