

Trabalho Wireshark

Luiza Ávila

Introdução

01) HTTP & TCP

02) 0,181172 segundos

03) IP do site gaia.cs.umass.edu : 128.119.245.12

Meu IP : 192.168.0.10

04)

| | | | | | |
|------|-----------------|----------------|----------------|------|---|
| 1412 | 17:48:50,670147 | 192.168.0.10 | 128.119.245.12 | HTTP | 560 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |
| 1426 | 17:48:50,851319 | 128.119.245.12 | 192.168.0.10 | HTTP | 491 HTTP/1.1 200 OK (text/html) |
| 1428 | 17:48:51,229177 | 192.168.0.10 | 128.119.245.12 | HTTP | 492 GET /favicon.ico HTTP/1.1 |
| 1429 | 17:48:51,407278 | 128.119.245.12 | 192.168.0.10 | HTTP | 537 HTTP/1.1 404 Not Found (text/html) |

<

> Frame 1412: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface \Device\NPF_{09C6D243-6621-487A-838B-D0B36146E086}, id 0

> Ethernet II, Src: IntelCor_0c:52:15 (5c:cd:5b:0c:52:15), Dst: ARRISGro_0d:54:c2 (5c:e3:0e:0d:54:c2)

> Internet Protocol Version 4, Src: 192.168.0.10, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 49494, Dst Port: 80, Seq: 1, Ack: 1, Len: 506

✓ 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

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 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: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7,es;q=0.6\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

[HTTP request 1/2]

[Response in frame: 1426]

[Next request in frame: 1428]

0010 02 22 de f0 40 00 80 06 e3 ae c0 a8 00 0a 80 77 ..-@... ..w

0020 f5 0c c1 56 00 50 c8 96 a8 e6 a3 12 a6 47 50 18 ...V.P... ..GP.

0030 01 00 ec bc 00 00 47 45 54 20 2f 77 69 72 65 73GE T/wires

0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-

0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.

Time to live (p.ttl), 1 byte(s)

Packets: 6762 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%)

DNS

01) site: gadgets.in

IP: 164.52.194.7

```
C:\Users\luiza>nslookup www.gadgets.in
Servidor:  UnKnown
Address:  2804:14d:1:0:181:213:132:2

Não é resposta autoritativa:
Nome:      www.gadgets.in
Address:   164.52.194.7
```

02) Universidade de Sorbonne

```
C:\Users\luiza>nslookup -type=ns sorbonne-universite.fr
Servidor:  UnKnown
Address:  2804:14d:1:0:181:213:132:2

Não é resposta autoritativa:
sorbonne-universite.fr  nameserver = shiva.jussieu.fr
sorbonne-universite.fr  nameserver = soleil.uvsq.fr
sorbonne-universite.fr  nameserver = ganesh.upmc.fr
```

03)

```
C:\Users\luiza>nslookup portal.office365.com shiva.jussieu.fr
Servidor:  shiva.jussieu.fr
Address:  134.157.0.129

*** shiva.jussieu.fr não encontrou portal.office365.com: Query refused
```

04) Usa UDP

| | | | | | |
|------|-----------------|---------------|---------------|-----|--|
| 59 | 19:28:31,791742 | 192.168.0.10 | 181.213.132.3 | DNS | 72 Standard query 0x8a18 A www.ietf.org |
| 63 | 19:28:31,812475 | 181.213.132.3 | 192.168.0.10 | DNS | 165 Standard query response 0x8a18 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net |
| 1227 | 19:28:34,001714 | 192.168.0.10 | 181.213.132.3 | DNS | 78 Standard query 0xba22 AAAA analytics.ietf.org |
| 1233 | 19:28:35,010778 | 192.168.0.10 | 181.213.132.2 | DNS | 78 Standard query 0xba22 AAAA analytics.ietf.org |
| 1235 | 19:28:35,429477 | 181.213.132.3 | 192.168.0.10 | DNS | 120 Standard query response 0xba22 AAAA analytics.ietf.org CNAME ietf.org AAAA 2001:0db8:0000:0000:0000:0000:0000:0000 |
| 1237 | 19:28:35,429620 | 181.213.132.2 | 192.168.0.10 | DNS | 120 Standard query response 0xba22 AAAA analytics.ietf.org CNAME ietf.org AAAA 2001:0db8:0000:0000:0000:0000:0000:0000 |

Frame 59: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{09C6D243-6621-487A-838B-D0B36146E086}, id 0
Ethernet II, Src: IntelCor_0c:52:15 (5c:cd:5b:0c:52:15), Dst: ARRTSGro_0d:54:c2 (5c:e3:0e:0d:54:c2)
Internet Protocol Version 4, Src: 192.168.0.10, Dst: 181.213.132.3
User Datagram Protocol, Src Port: 63366, Dst Port: 53
Domain Name System (query)

05) Porta de destino da consulta: 53

Porta de origem da resposta: 53

06) A mensagem é enviada para o endereço 192.168.0.10. O endereço de IP do DNS é o mesmo.

07) Type: A (Host Address)

Não possui nenhum campo de resposta (“answer”)

08) Existem 4 campos. Em comum, as quatro possuem: “Name”; “Type”; “Class”; “Time to live”; “Data length”. Três delas possuem “Address” e uma possui “CNAME”.

```
Answers
  www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    Name: www.ietf.org
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 33
    CNAME: www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.111.6
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 104.20.111.6
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 172.67.33.249
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 172.67.33.249
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.110.6
    Name: www.ietf.org.cdn.cloudflare.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300 (5 minutes)
    Data length: 4
    Address: 104.20.110.6
[Request In: 59]
[Time: 0.020733000 seconds]
```

09) O meu wireshark não capturou nenhum SYN enviado pelo meu servidor. Ele recebeu um ACK de outro IP que eu estou assumindo é CNAME.

| | | | | | |
|------|-----------------|---------------|--------------|-----|---|
| 1306 | 19:28:39,716850 | 18.229.78.240 | 192.168.0.10 | TCP | 60 443 → 49675 [ACK] Seq=1 Ack=80 Win=204 Len=0 |
|------|-----------------|---------------|--------------|-----|---|

10) Não, as informações são enviadas diretamente pelas consultas DNS.

11) Porta de destino da consulta: 53

Porta de origem da resposta: 53

12) Estou usando wifi, meu endereço IP não aparece no wireshark. O destino da mensagem resposta é 2804:14c:5b70:8501:99cf:d090:ba38:8d58 ; que é um dos meus DNS locais.

13) Type: A (Host Address)

Não possui nenhum campo de resposta (“answer”)

14) Existem 3 campos. Em comum, as três possuem: “Name”; “Type”; “Class”; “Time to live”; “Data length”. Uma delas possui “Address” e duas possuem “CNAME”.

| | |
|--|--|
| Answers | |
| www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net | |
| Name: www.mit.edu | |
| Type: CNAME (Canonical NAME for an alias) (5) | |
| Class: IN (0x0001) | |
| Time to live: 1800 (30 minutes) | |
| Data length: 25 | |
| CNAME: www.mit.edu.edgekey.net | |
| www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net | |
| Name: www.mit.edu.edgekey.net | |
| Type: CNAME (Canonical NAME for an alias) (5) | |
| Class: IN (0x0001) | |
| Time to live: 60 (1 minute) | |
| Data length: 24 | |
| CNAME: e9566.dscb.akamaiedge.net | |
| e9566.dscb.akamaiedge.net: type A, class IN, addr 23.77.110.137 | |
| Name: e9566.dscb.akamaiedge.net | |
| Type: A (Host Address) (1) | |
| Class: IN (0x0001) | |
| Time to live: 20 (20 seconds) | |
| Data length: 4 | |
| Address: 23.77.110.137 | |
| [Request In: 13] | |
| [Time: 0.077118000 seconds] | |

15)

| | | | | | |
|---|-----------------|--|--|-----|---|
| 7 | 20:44:19,225993 | 2804:14c:5b70:8501:99cf:d090:ba38:8d58 | 2804:14d:1:0:181:213:132:2 | DNS | 152 Standard query 0x0001 PTR 2.0.0.0.2.3.1.0.3.1.2.0.1.8.1.0.0.0.0.1.0.0.0.d.4.1.0.4.0. |
| 12 | 20:44:19,247632 | 2804:14d:1:0:181:213:132:2 | 2804:14c:5b70:8501:99cf:d090:ba38:8d58 | DNS | 212 Standard query response 0x0001 No such name PTR 2.0.0.0.2.3.1.0.3.1.2.0.1.8.1.0.0.0.0. |
| 13 | 20:44:19,253070 | 2804:14c:5b70:8501:99cf:d090:ba38:8d58 | 2804:14d:1:0:181:213:132:2 | DNS | 91 Standard query 0x0002 A www.mit.edu |
| 14 | 20:44:19,330188 | 2804:14d:1:0:181:213:132:2 | 2804:14c:5b70:8501:99cf:d090:ba38:8d58 | DNS | 180 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566 |
| 15 | 20:44:19,340231 | 2804:14c:5b70:8501:99cf:d090:ba38:8d58 | 2804:14d:1:0:181:213:132:2 | DNS | 91 Standard query 0x0003 AAAA www.mit.edu |
| 16 | 20:44:19,357657 | 2804:14d:1:0:181:213:132:2 | 2804:14c:5b70:8501:99cf:d090:ba38:8d58 | DNS | 220 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566 |
| < | | | | | |
| > | | | | | |
| > Frame 14: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface \Device\NPF_{09C6D243-6621-487A-83BB-D0B36146E086}, id 0 | | | | | |
| > Ethernet II, Src: ARRISGro_0d:54:c2 (5c:e3:0e:0d:54:c2), Dst: IntelCor_0c:52:15 (5c:cd:5b:0c:52:15) | | | | | |
| > Internet Protocol Version 6, Src: 2804:14d:1:0:181:213:132:2, Dst: 2804:14c:5b70:8501:99cf:d090:ba38:8d58 | | | | | |
| > User Datagram Protocol, Src Port: 53, Dst Port: 64299 | | | | | |
| > Domain Name System (response) | | | | | |

16) Estou usando wifi, meu endereço IP não aparece no wireshark. O destino da mensagem resposta é 2804:14c:5b70:8501:99cf:d090:ba38:8d58 ; que é um dos meus DNS locais.

17) Type: NS (Authoritative name server)

23)

HTTP

01) O navegador executa HTTP 1.1, assim como o servidor.

```

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]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file1.html
    Request Version: HTTP/1.1

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK

```

02) Aceita pt-BR, pt, en, es, en-US

```

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/85.0.4183.83 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: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7,es;q=0.6\r\n

```

03) Meu IP: 192.168.0.10

IP de gaia.cs.umass.edu: 128.119.245.12

| Time | Source | Destination | Protocol | Length | Info |
|-----------------|--------------|----------------|----------|--------|--|
| 14:02:22,357840 | 192.168.0.10 | 128.119.245.12 | HTTP | 559 | GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 |

04) Status code: 200

```

HTTP/1.1 200 OK\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK

```

05) Última vez que foi modificado: Sábado, 5 de setembro de 2020 05:59 GMT

```

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sat, 05 Sep 2020 05:59:03 GMT\r\n
ETag: "80-5ae8aaeb91097"\r\n
Accept-Ranges: bytes\r\n

```

06) 128 bytes

```
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.164679000 seconds]
[Request in frame: 336]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
```

07) Todos os cabeçalhos estão na listagem.

08) Não vejo a linha “IF-MODIFIED-SINCE”.

```
✓ Hypertext Transfer Protocol
  ✓ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    ✓ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.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/85.0.4183.83 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: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7,es;q=0.6\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
      [HTTP request 1/1]
      [Response in frame: 2975]
```

09) Sim, todo o arquivo html está exibido em line-based text data

```
✓ Line-based text data: text/html (10 lines)
  \n
  <html>\n
  \n
  Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
  This file's last modification date will not change. <p>\n
  Thus if you download this multiple times on your browser, a complete copy <br>\n
  will only be sent once by the server due to the inclusion of the IF-MODIFIED-SINCE<br>\n
  field in your browser's HTTP GET request to the server.\n
  \n
  </html>\n
```

10) Sim, eu vejo a linha. O que segue é a data de hoje com a hora de acesso no fuso GMT.

```
If-Modified-Since: Sat, 05 Sep 2020 05:59:03 GMT\r\n
```


11) Status 304

```
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: Sat, 05 Sep 2020 18:04:36 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9 mod_perl/2.0.11 Perl/v5.16.3\r\n
```

O servidor não manda novamente o conteúdo pois não houveram modificações, não sendo necessário o reenvio da página. Consigo chegar a essa conclusão pois o cabeçalho de line-based text data não aparece novamente e devido ao status enviado pelo servidor (304-Not modified).

```
7112 15:04:36,690242 128.119.245.12 192.168.0.10 HTTP 293 HTTP/1.1 304 Not Modified
> Frame 7112: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{09C6D243-6621-487A-83BB-D0B36146E086}, id 0
> Ethernet II, Src: ARRISGro_0d:54:c2 (5c:e3:0e:0d:54:c2), Dst: IntelCor_0c:52:15 (5c:cd:5b:0c:52:15)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 58140, Seq: 1, Ack: 618, Len: 239
> Hypertext Transfer Protocol
```

SEM
CABEÇALHO

12) Apenas um HTTP GET foi enviado pelo meu navegador.

```
61 15:45:06,618489 192.168.0.10 128.119.245.12 HTTP 559 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
72 15:45:06,910757 128.119.245.12 192.168.0.10 HTTP 534 HTTP/1.1 200 OK (text/html)
```

13) 4 segmentos de TCP foram necessários para carregar a resposta.

```
> [4 Reassembled TCP Segments (4860 bytes): #69(1460), #70(1460), #71(1460), #72(480)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

14) Status code: 200. Description: OK

```
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
```


15) Não tem nenhuma linha de HTTP nos segmentos TCP.

```
Transmission Control Protocol, Src Port: 80, Dst Port: 58274, Seq: 4301, Ack: 300, Len: 480
[4 Reassembled TCP Segments (4860 bytes): #69(1460), #70(1460), #71(1460), #72(480)]
[Frame: 69, payload: 0-1459 (1460 bytes)]
[Frame: 70, payload: 1460-2919 (1460 bytes)]
[Frame: 71, payload: 2920-4379 (1460 bytes)]
[Frame: 72, payload: 4380-4859 (480 bytes)]
[Segment count: 4]
[Reassembled TCP length: 4860]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a2053...]
```

16) 3 mensagens HTTP GET foram requisitadas para os endereços:

/wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1

/pearson.png HTTP/1.1

/~kurose/cover_5th_ed.jpg HTTP/1.1

| | | |
|------|----------------------|--|
| HTTP | 559 GET | /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| HTTP | 1126 HTTP/1.1 200 OK | (text/html) |
| HTTP | 491 GET | /pearson.png HTTP/1.1 |
| HTTP | 744 HTTP/1.1 200 OK | (PNG) |
| HTTP | 505 GET | /~kurose/cover_5th_ed.jpg HTTP/1.1 |

17) Sequência, pois o servidor esperou uma ser confirmada para requisitar a outra.

18) Código 401 Unauthorized

| | | | | | | |
|----|-----------------|----------------|--------------|------|-------------------------------|-------------|
| 95 | 16:08:02,764525 | 128.119.245.12 | 192.168.0.10 | HTTP | 770 HTTP/1.1 401 Unauthorized | (text/html) |
|----|-----------------|----------------|--------------|------|-------------------------------|-------------|

```
Transmission Control Protocol, Src Port: 80, Dst Port: 58348, Seq: 1, Ack: 522, Len: 716
Hypertext Transfer Protocol
HTTP/1.1 401 Unauthorized\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
[HTTP/1.1 401 Unauthorized\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 401
[Status Code Description: Unauthorized]
Response Phrase: Unauthorized
Date: Sat, 05 Sep 2020 19:08:02 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9 mod_perl/2.0.11 Perl/v5.16.3\r\n
WWW-Authenticate: Basic realm="wireshark-students only"\r\n
Content-Length: 381\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=iso-8859-1\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.230641000 seconds]
[Request in frame: 91]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
File Data: 381 bytes
```

19) O campo “Authorization” com as credentials que eu inseri.

✓ Hypertext Transfer Protocol

> GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.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

✓ Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcms=\r\n

Credentials: wireshark-students:network

Upgrade-Insecure-Requests: 1\r\n