Escuela Colombiana de ingeniería Julio Garavito

Seguridad y privacidad de TI

Laboratorio 12

Integrantes

Diego Castellanos

Profesor

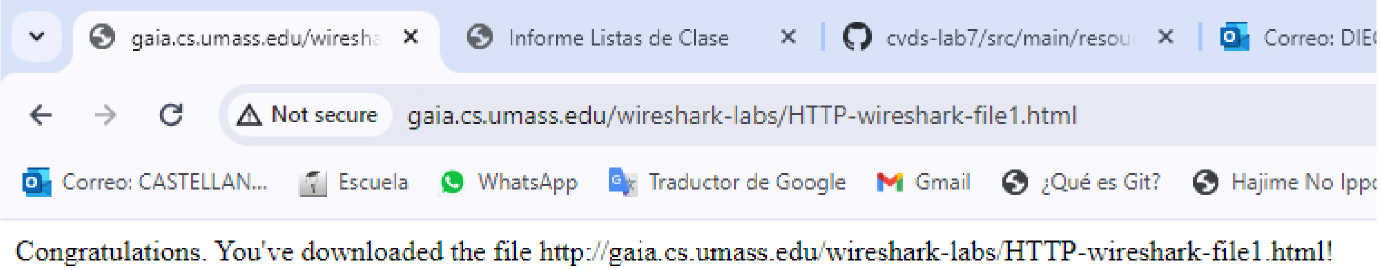
Daniel Esteban Vela López

Bogotá 2024

ESCUELA
COLOMBIANA
DE INGENIERÍA
JULIO GARAVITO

HTTP

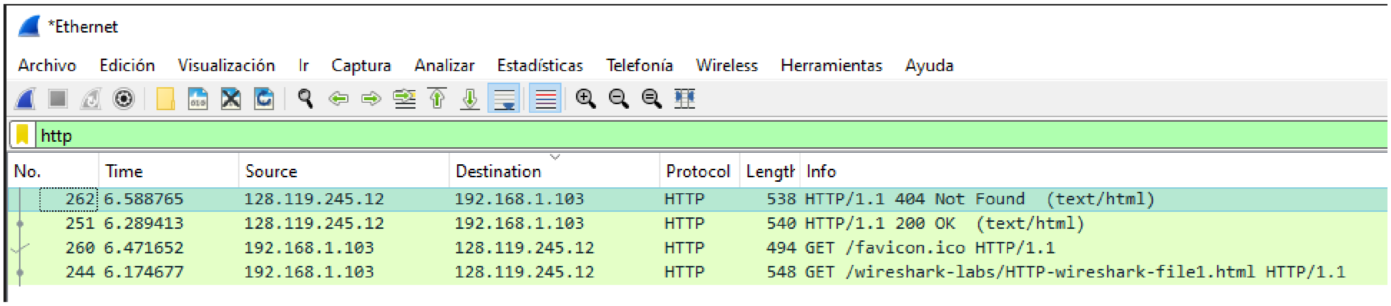
1. The Basic HTTP GET/response interaction



gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

Congratulations. You've downloaded the file http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!

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

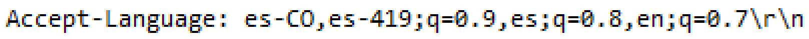


http

```
No.   Time      Source          Destination     Protocol Length Info
  262 6.588765  128.119.245.12  192.168.1.103   HTTP     538 HTTP/1.1 404 Not Found  (text/html)
  251 6.289413  128.119.245.12  192.168.1.103   HTTP     540 HTTP/1.1 200 OK  (text/html)
  260 6.471652  192.168.1.103   128.119.245.12  HTTP     494 GET /favicon.ico HTTP/1.1
  244 6.174677  192.168.1.103   128.119.245.12  HTTP     548 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
```

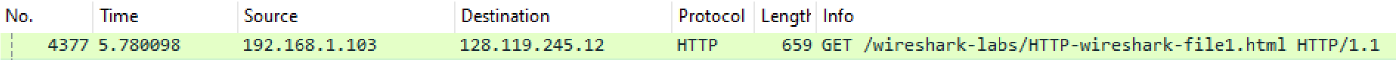
Tanto el browser como el servidor están corriendo la versión 1.1.

2. What languages (if any) does your browser indicate that it can accept to the server?



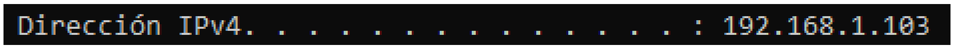
```
Accept-Language: es-CO,es-419;q=0.9,es;q=0.8,en;q=0.7\r\n
```

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



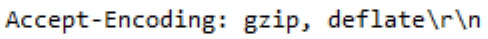
```
No.   Time      Source          Destination     Protocol Length Info
 4377 5.780098  192.168.1.103   128.119.245.12  HTTP     659 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
```

La IP de mi computador es 192.168.1.103, la IP del servidor es 128.119.245.12



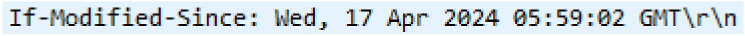
```
Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.103
```

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



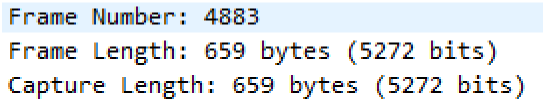
```
Accept-Encoding: gzip, deflate\r\n
```

5. When was the HTML file that you are retrieving last modified at the server?



```
If-Modified-Since: Wed, 17 Apr 2024 05:59:02 GMT\r\n
```

6. How many bytes of content are being returned to your browser?

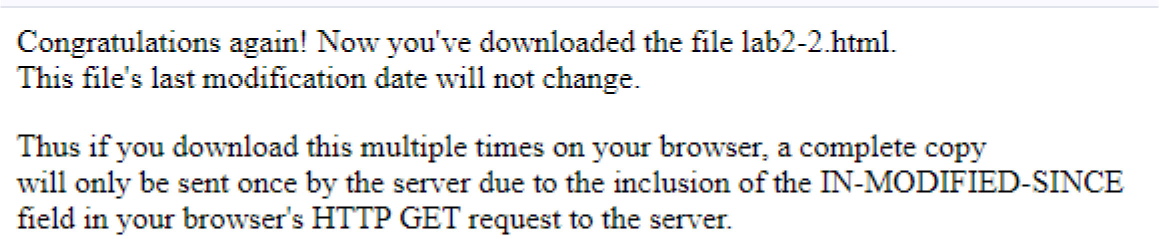


```
Frame Number: 4883
Frame Length: 659 bytes (5272 bits)
Capture Length: 659 bytes (5272 bits)
```

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.

Ninguno.

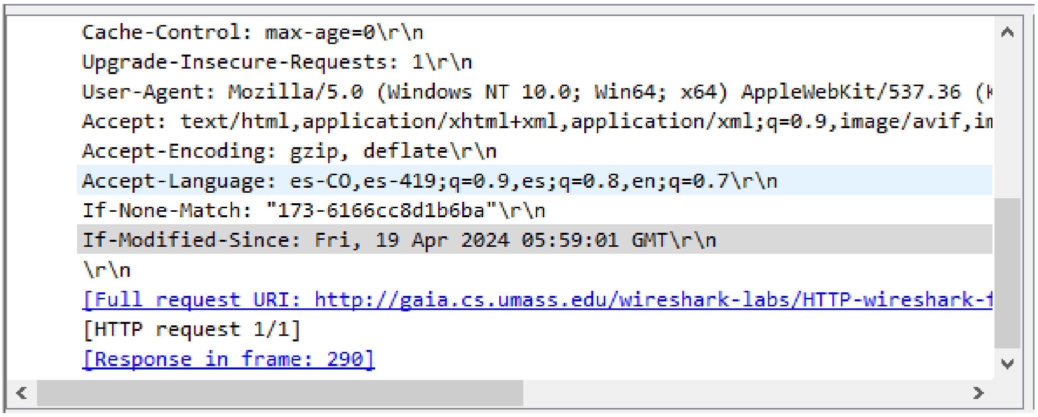
2. The HTTP CONDITIONAL GET/response interaction



Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE field in your browser's HTTP GET request to the server.

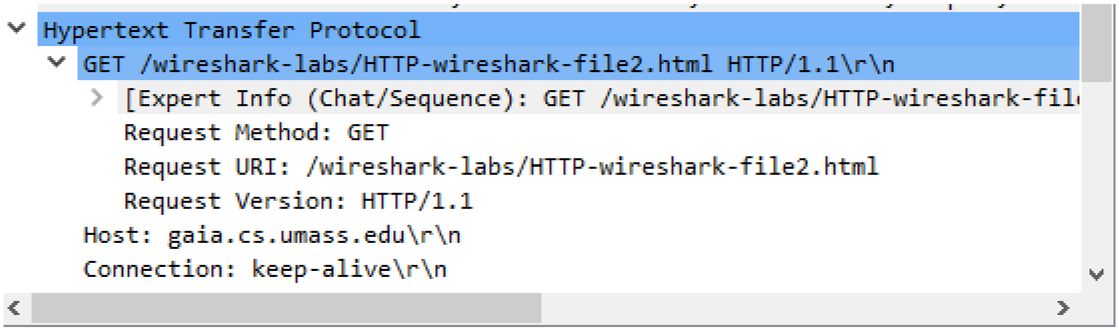
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?



```
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 (K
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Encoding: gzip, deflate\r\n
Accept-Language: es-CO,es-419;q=0.9,es;q=0.8,en;q=0.7\r\n
If-None-Match: "173-6166cc8d1b6ba"\r\n
If-Modified-Since: Fri, 19 Apr 2024 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-f
[HTTP request 1/1]
[Response in frame: 290]
```

Si se aprecia el "IF-MODIFIED-SINCE"

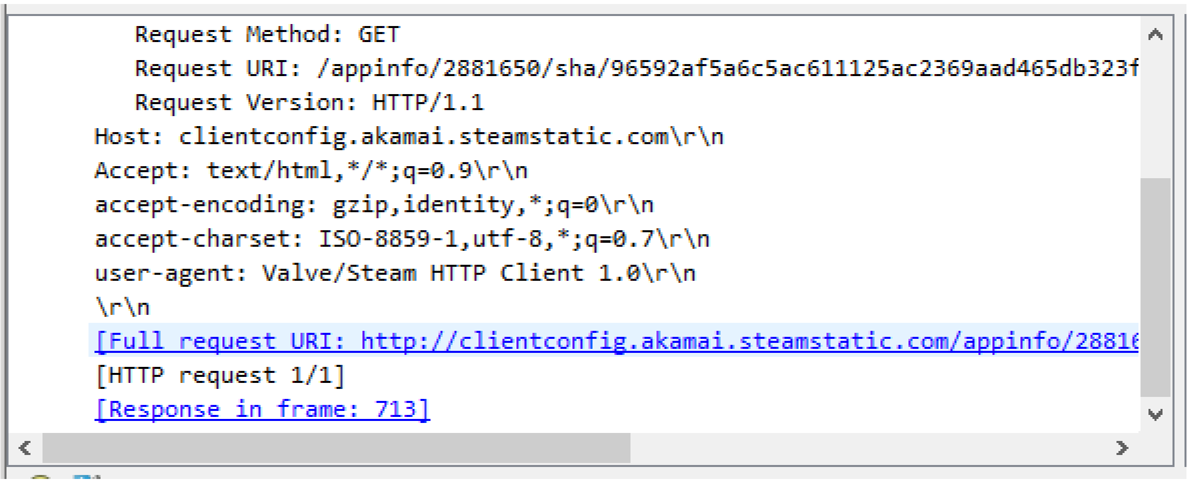
9.Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?



```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-fil
    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
```

Si, gracias al la transferencia del protocolo.

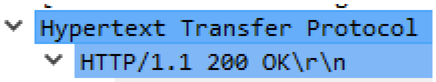
10.Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?



```
    Request Method: GET
    Request URI: /appinfo/2881650/sha/96592af5a6c5ac611125ac2369aad465db323f
    Request Version: HTTP/1.1
  Host: clientconfig.akamai.steamstatic.com\r\n
  Accept: text/html,*/*;q=0.9\r\n
  accept-encoding: gzip,identity,*;q=0\r\n
  accept-charset: ISO-8859-1,utf-8,*;q=0.7\r\n
  user-agent: Valve/Steam HTTP Client 1.0\r\n
  \r\n
  [Full request URI: http://clientconfig.akamai.steamstatic.com/appinfo/28816
  [HTTP request 1/1]
  [Response in frame: 713]
```

No se aprecia el “IF-MODIFIED-SINCE”

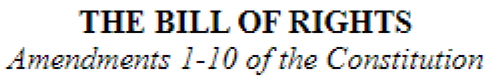
11.What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
```

No devuelve el contenido del archivo.

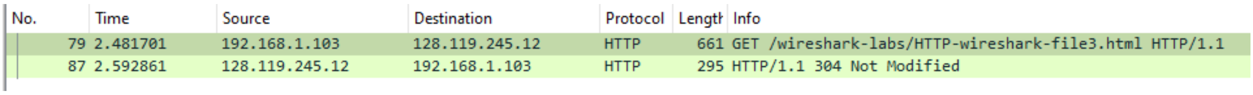
3. Retrieving Long Documents



THE BILL OF RIGHTS

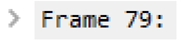
Amendments 1-10 of the Constitution

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?



No.	Time	Source	Destination	Protocol	Length	Info
79	2.481701	192.168.1.103	128.119.245.12	HTTP	661	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
87	2.592861	128.119.245.12	192.168.1.103	HTTP	295	HTTP/1.1 304 Not Modified

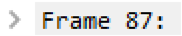
Solo mandó uno.



```
Frame 79:
```

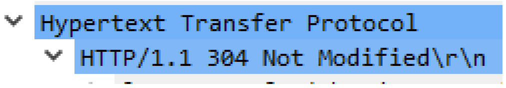
El número dle paquete es 79.

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



```
Frame 87:
```

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

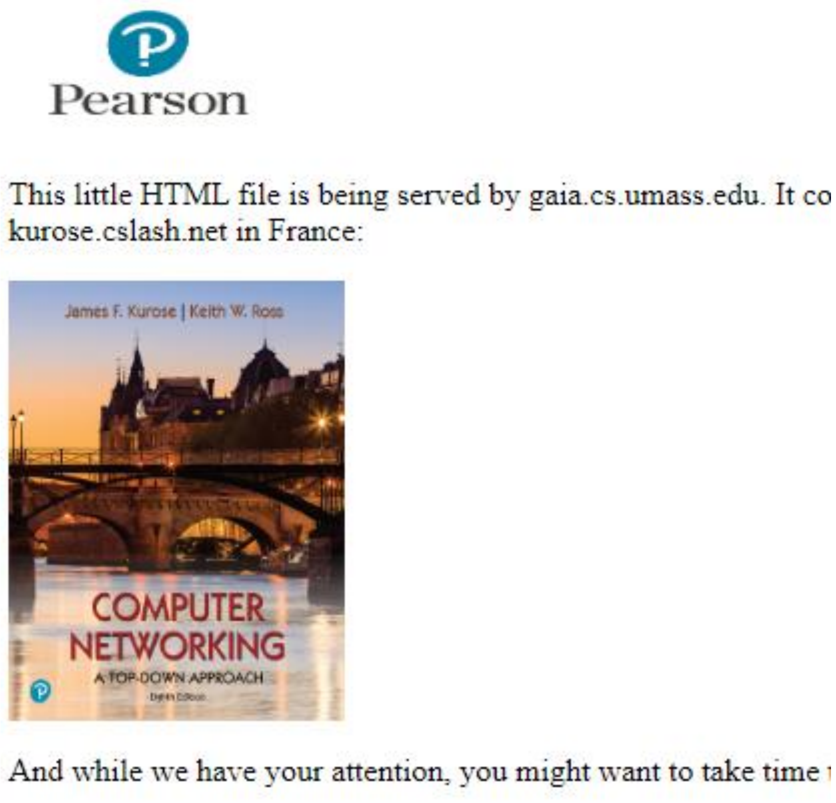


```
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
```

15.How many data-containing TCP segments were needed tocarry the single HTTP response and the text of theBill of Rights?

2

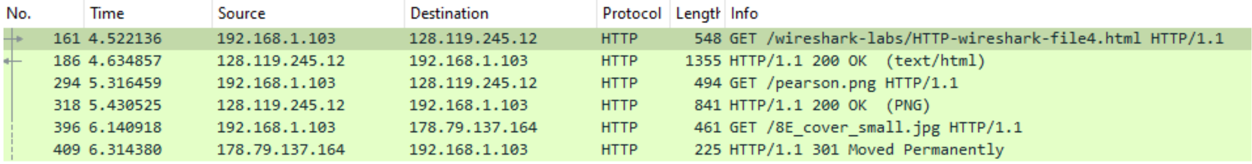
4. HTML Documents with Embedded Objects



This little HTML file is being served by gaia.cs.umass.edu. It co
kurose.cslash.net in France:

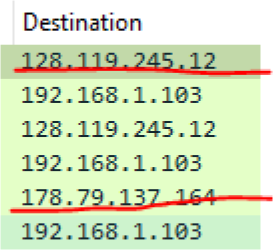
And while we have your attention, you might want to take time

16.How many HTTP GET request messagesdid your browser send? To which Internet addresses were these GET requests sent?



No.	Time	Source	Destination	Protocol	Length	Info
161	4.522136	192.168.1.103	128.119.245.12	HTTP	548	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
186	4.634857	128.119.245.12	192.168.1.103	HTTP	1355	HTTP/1.1 200 OK (text/html)
294	5.316459	192.168.1.103	128.119.245.12	HTTP	494	GET /pearson.png HTTP/1.1
318	5.430525	128.119.245.12	192.168.1.103	HTTP	841	HTTP/1.1 200 OK (PNG)
396	6.140918	192.168.1.103	178.79.137.164	HTTP	461	GET /8E_cover_small.jpg HTTP/1.1
409	6.314380	178.79.137.164	192.168.1.103	HTTP	225	HTTP/1.1 301 Moved Permanently

Pidió 3 HTTP GET a dos IP diferentes.

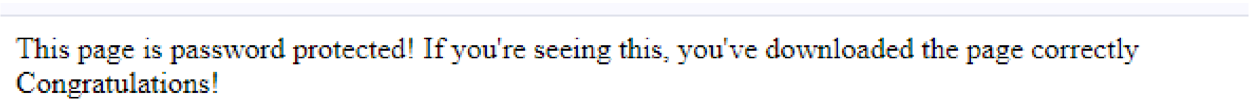


Destination
128.119.245.12
192.168.1.103
128.119.245.12
192.168.1.103
178.79.137.164
192.168.1.103

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.

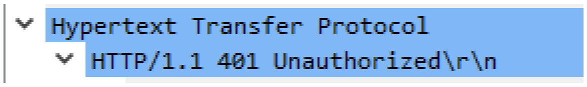
Fueron descargadas en serie, pues se necesitó dos GET para su descarga.

5 HTTP Authentication



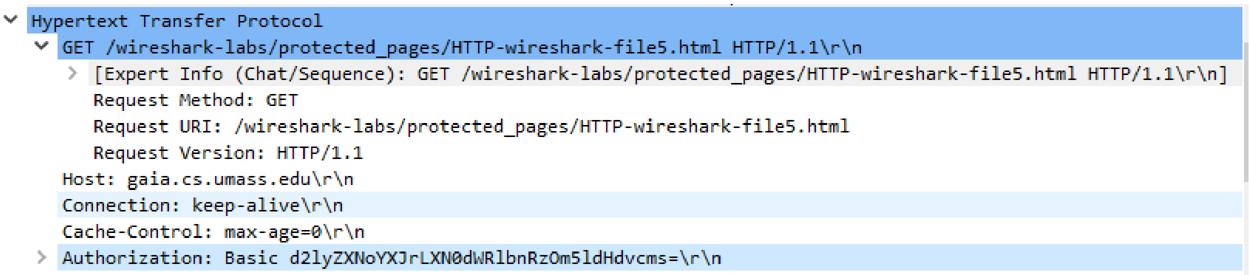
This page is password protected! If you're seeing this, you've downloaded the page correctly
Congratulations!

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



```
v Hypertext Transfer Protocol
  v HTTP/1.1 401 Unauthorized\r\n
```

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



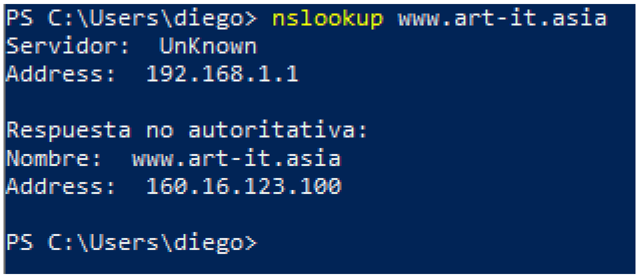
```
v Hypertext Transfer Protocol
  v GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
```

El nuevo campo que se agregó fue el de Authorization.

DNS

1. nslookup

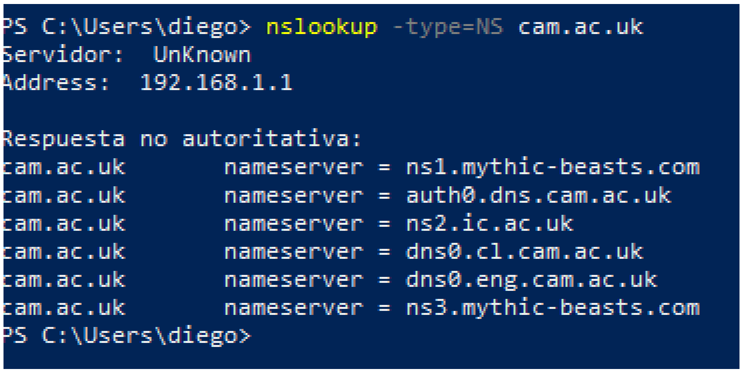
1. Run nslookupto obtain the IP address of a Web server in Asia. What is the IP address of that server?



```
PS C:\Users\diego> nslookup www.art-it.asia
Servidor:  UnKnown
Address:  192.168.1.1

Respuesta no autoritativa:
Nombre:  www.art-it.asia
Address:  160.16.123.100

PS C:\Users\diego>
```

La IP es 160.16.123.100

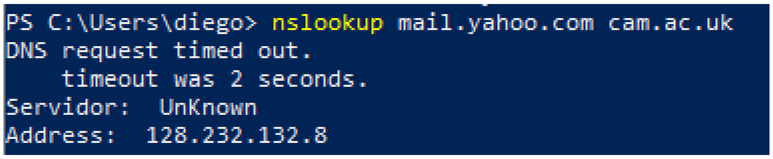
2.Run nslookupto determine the authoritative DNS servers for a university in Europe.



```
PS C:\Users\diego> nslookup -type=NS cam.ac.uk
Servidor:  UnKnown
Address:  192.168.1.1

Respuesta no autoritativa:
cam.ac.uk       nameserver = ns1.mythic-beasts.com
cam.ac.uk       nameserver = auth0.dns.cam.ac.uk
cam.ac.uk       nameserver = ns2.ic.ac.uk
cam.ac.uk       nameserver = dns0.cl.cam.ac.uk
cam.ac.uk       nameserver = dns0.eng.cam.ac.uk
cam.ac.uk       nameserver = ns3.mythic-beasts.com
PS C:\Users\diego>
```

Servidores DNS de cambridge.

3.Run nslookup that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

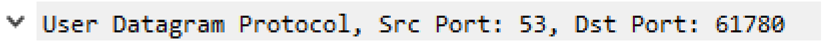


```
PS C:\Users\diego> nslookup mail.yahoo.com cam.ac.uk
DNS request timed out.
    timeout was 2 seconds.
Servidor:  UnKnown
Address:  128.232.132.8
```

La IP es 128.232.132.8

3. Tracing DNS with Wireshark

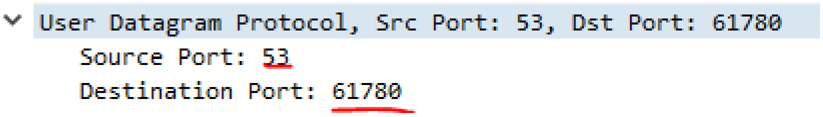
4.Locate the DNS query and response messages. Are thensent over UDP or TCP?+



```
User Datagram Protocol, Src Port: 53, Dst Port: 61780
```

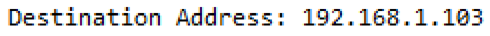
Usa UDP.

5.What is the destination port for the DNS query message? What is the source port of DNS response message?

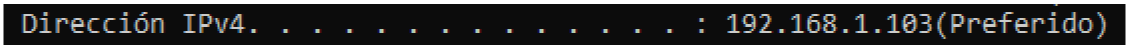


```
User Datagram Protocol, Src Port: 53, Dst Port: 61780
    Source Port: 53
    Destination Port: 61780
```

6.To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?



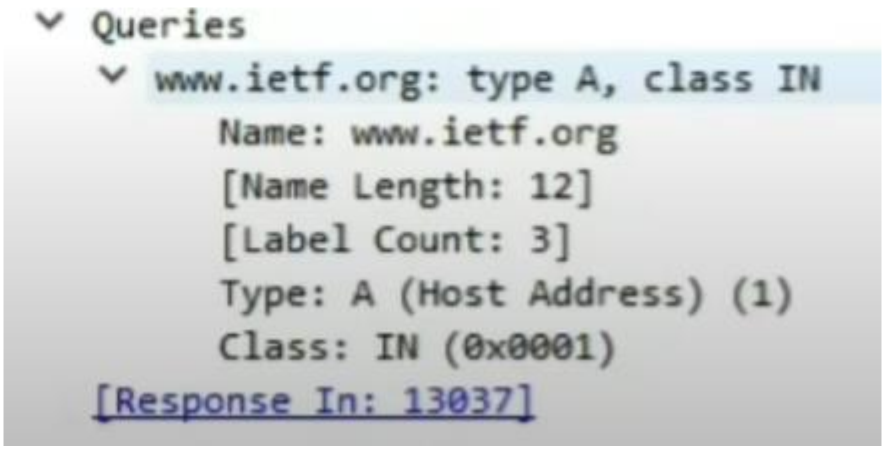
```
Destination Address: 192.168.1.103
```



```
Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.103(Preferido)
```

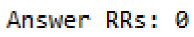
Son la misma.

7.Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



```
Queries
    www.ietf.org: type A, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 13037]
```

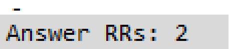
Es de tipo A.



```
Answer RRs: 0
```

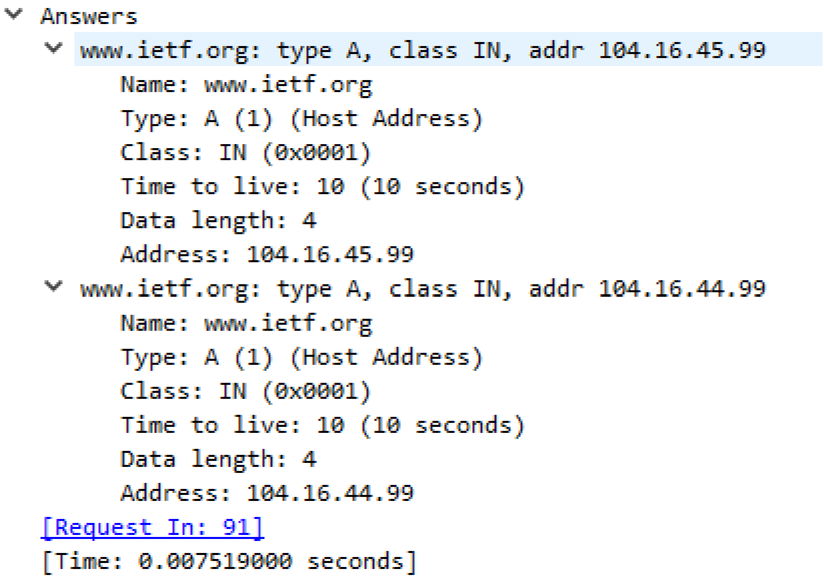
No tiene respuestas.

8.Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?



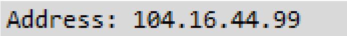
```
Answer RRs: 2
```

Tiene dos respuestas.



```
Answers
  www.ietf.org: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 10 (10 seconds)
      Data length: 4
      Address: 104.16.45.99
  www.ietf.org: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 10 (10 seconds)
      Data length: 4
      Address: 104.16.44.99
  [Request In: 91]
  [Time: 0.007519000 seconds]
```

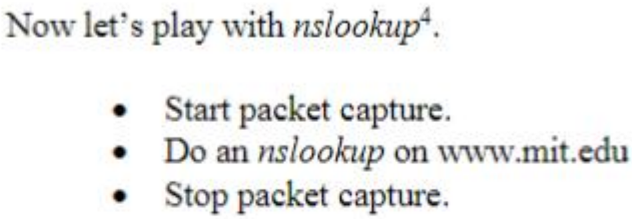
9.Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?



```
Address: 104.16.44.99
```

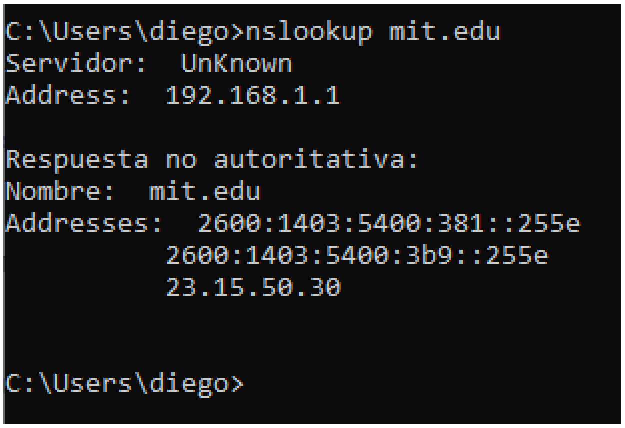
10.This web page contains images. Before retrieving each image, does your host issue newDNS queries?

No.



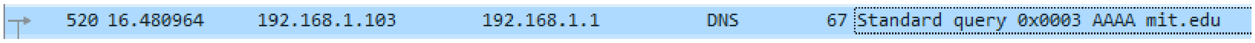
Now let's play with *nslookup*[4].

- Start packet capture.
- Do an *nslookup* on www.mit.edu
- Stop packet capture.

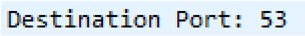


```
C:\Users\diego>nslookup mit.edu
Servidor:  UnKnown
Address:  192.168.1.1

Respuesta no autoritativa:
Nombre:  mit.edu
Addresses:  2600:1403:5400:381::255e
          2600:1403:5400:3b9::255e
          23.15.50.30


C:\Users\diego>
```

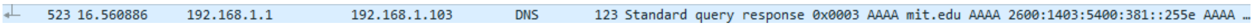
11.What is the destination port for the DNS query message? What is the source port of DNS response message?



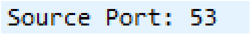
```
520 16.480964    192.168.1.103    192.168.1.1    DNS    67 Standard query 0x0003 AAAA mit.edu
```



```
Destination Port: 53
```

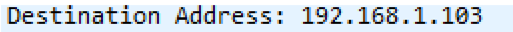


```
523 16.560886    192.168.1.1    192.168.1.103    DNS    123 Standard query response 0x0003 AAAA mit.edu AAAA 2600:1403:5400:381::255e AAAA …
```



```
Source Port: 53
```

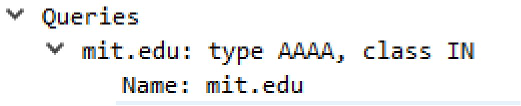
12.To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



```
Destination Address: 192.168.1.103
```

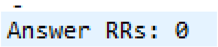
Si.

13.Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



```
⌄ Queries
  ⌄ mit.edu: type AAAA, class IN
      Name: mit.edu
```

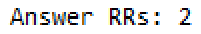
Es de tipo AAAA.



```
Answer RRs: 0
```

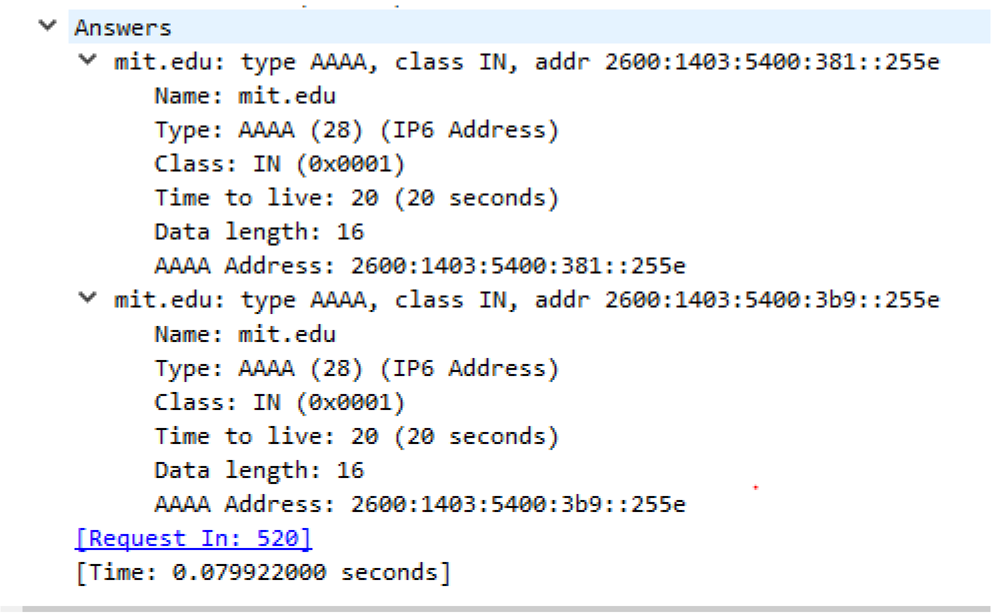
No tiene respuestas.

14.Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

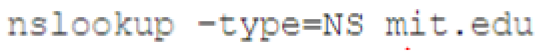


```
Answer RRs: 2
```

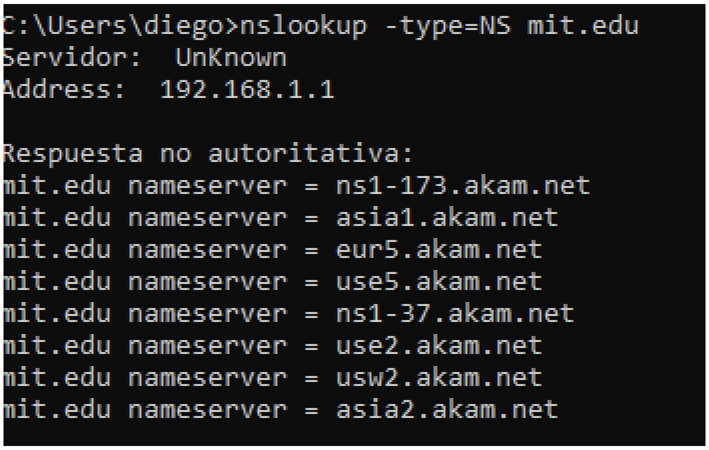
Tiene dos respuestas.



```
v Answers
    v mit.edu: type AAAA, class IN, addr 2600:1403:5400:381::255e
          Name: mit.edu
          Type: AAAA (28) (IP6 Address)
          Class: IN (0x0001)
          Time to live: 20 (20 seconds)
          Data length: 16
          AAAA Address: 2600:1403:5400:381::255e
    v mit.edu: type AAAA, class IN, addr 2600:1403:5400:3b9::255e
          Name: mit.edu
          Type: AAAA (28) (IP6 Address)
          Class: IN (0x0001)
          Time to live: 20 (20 seconds)
          Data length: 16
          AAAA Address: 2600:1403:5400:3b9::255e
  [Request In: 520]
  [Time: 0.079922000 seconds]
```

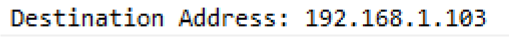


```
nslookup -type=NS mit.edu
```



```
C:\Users\diego>nslookup -type=NS mit.edu
Servidor:  UnKnown
Address:  192.168.1.1

Respuesta no autoritativa:
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia2.akam.net
```

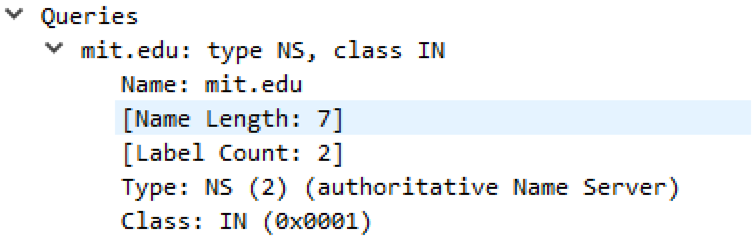
16.To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



```
Destination Address: 192.168.1.103
```

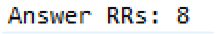
Si.

17.Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



```
Queries
  mit.edu: type NS, class IN
    Name: mit.edu
    [Name Length: 7]
    [Label Count: 2]
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
```

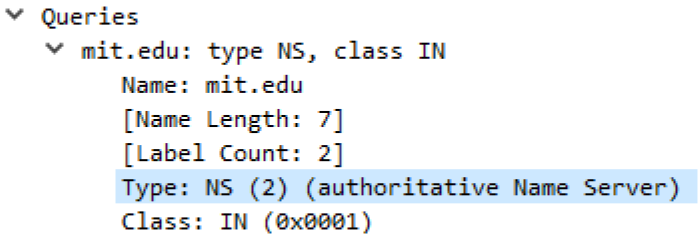
Es de tipo NS.



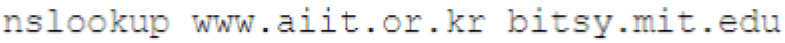
```
Answer RRs: 8
```

Tiene 8 respuestas.

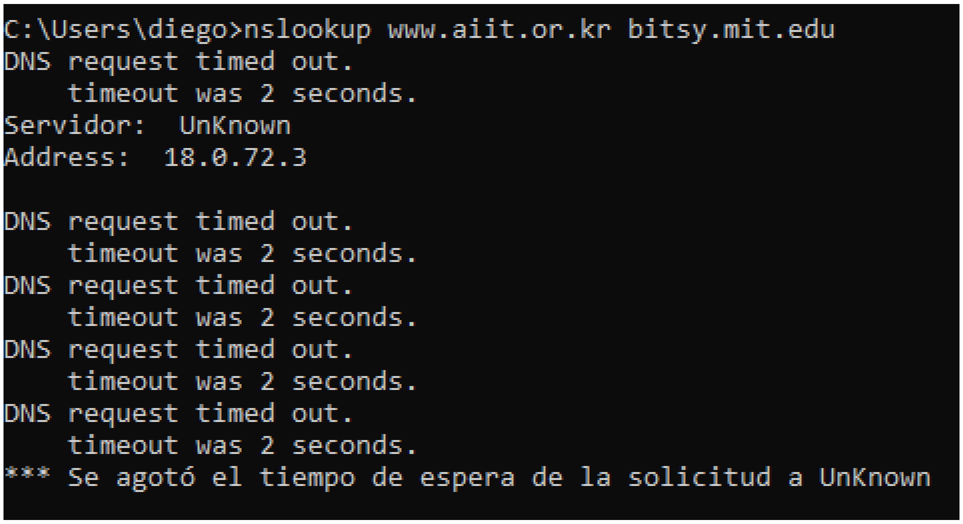
18.Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addressesof the MIT namesers?



```
Queries
  mit.edu: type NS, class IN
    Name: mit.edu
    [Name Length: 7]
    [Label Count: 2]
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
```

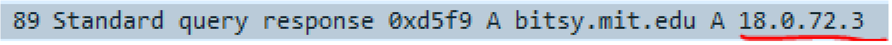


```
nslookup www.aiit.or.kr bitsy.mit.edu
```

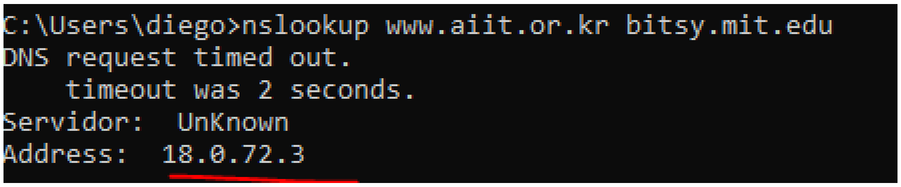


```
C:\Users\diego>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Servidor:  UnKnown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Se agotó el tiempo de espera de la solicitud a UnKnown
```

20.To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

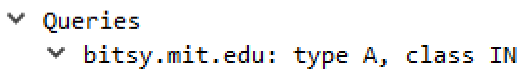


```
89 Standard query response 0xd5f9 A bitsy.mit.edu A 18.0.72.3
```



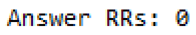
```
C:\Users\diego>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Servidor:  UnKnown
Address:  18.0.72.3
```

21.Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



```
⌄ Queries
  ⌄ bitsy.mit.edu: type A, class IN
```

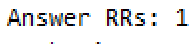
Es de tipo A.



```
Answer RRs: 0
```

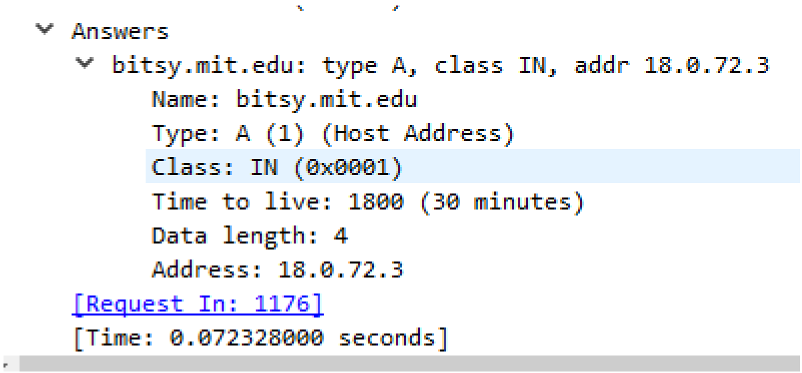
No tiene respuestas.

22.Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?



```
Answer RRs: 1
```

Tiene una respuesta.



```
⌄ Answers
  ⌄ bitsy.mit.edu: type A, class IN, addr 18.0.72.3
      Name: bitsy.mit.edu
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 4
      Address: 18.0.72.3
  [Request In: 1176]
  [Time: 0.072328000 seconds]
```