

HAMMAD KHAN MUSAKHEL

21801175

CS472

Wireshark Assignment

1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

MDNS
ARP
LLMNR
UDP
TCP
SSDP
NBNS
IGMPv2
TLSv1...
DNS

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select *Time Display Format*, then select *Time-of-day*.)

16:48:19.791844, request sent

16:48:19.945737, response OK received

It took 0.153893 seconds to receive the HTTP OK reply.

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

Internet Address of gaia.cs.umass.edu: 128.119.245.12

Internet Address of my computer: 139.179.210.130

4. Print the two HTTP messages displayed in step 9 above. To do so, select *Print* from the Wireshark *File* command menu, and select “*Selected Packet Only*” and “*Print as displayed*” and then click OK.

First HTTP Message (using Screenshot as Print was not working on my PC) below:

No.	Time	Source	Destination	Protocol	Length	Info
+ 767	16:48:19.791844	139.179.210.130	128.119.245.12	HTTP	549	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
+ 798	16:48:19.945737	128.119.245.12	139.179.210.130	HTTP	504	HTTP/1.1 200 OK (text/html)

```

> Frame 767: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface en0, id 0
> Ethernet II, Src: Apple_ea:03:4f (64:5a:ed:ea:03:4f), Dst: SuperMic_8e:b3:73 (0c:c4:7a:8e:b3:73)
> Internet Protocol Version 4, Src: 139.179.210.130, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49569, Dst Port: 80, Seq: 1, Ack: 1, Len: 483
< Hypertext Transfer Protocol
  < GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/INTRO-wireshark-file1.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      If-None-Match: "51-5ecc27985be02"\r\n
      Upgrade-Insecure-Requests: 1\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
      If-Modified-Since: Wed, 20 Oct 2021 05:59:01 GMT\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Safari/605.1.15\r\n
      Accept-Language: en-us\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 798]
  
```

Second HTTP Message (using Screenshot as Print was not working on my PC)

No.	Time	Source	Destination	Protocol	Length	Info
+ 767	16:48:19.791844	139.179.210.130	128.119.245.12	HTTP	549	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
+ 798	16:48:19.945737	128.119.245.12	139.179.210.130	HTTP	504	HTTP/1.1 200 OK (text/html)

```

> Ethernet II, Src: SuperMic_8e:b3:73 (0c:c4:7a:8e:b3:73), Dst: Apple_ea:03:4f (64:5a:ed:ea:03:4f)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.210.130
> Transmission Control Protocol, Src Port: 80, Dst Port: 49569, Seq: 1, Ack: 484, Len: 438
< 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
      Date: Thu, 21 Oct 2021 13:48:20 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Thu, 21 Oct 2021 05:59:02 GMT\r\n
      ETag: "51-5ecd697696e58"\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 1/1]
    [Time since request: 0.153893000 seconds]
    [Request in frame: 767]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
  
```

Wireshark Lab: HTTP

1. The Basic HTTP GET/response interaction

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

Browser: 1.1

Server: 1.1

No.	Time	Source	Destination	Protocol	Length	Info
583	17:20:50.336869	139.179.210.130	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
613	17:20:50.488738	128.119.245.12	139.179.210.130	HTTP	552	HTTP/1.1 200 OK (text/html)

```

> Frame 583: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface en0, id 0
> Ethernet II, Src: Apple_ea:03:4f (64:5:a:ed:ea:03:4f), Dst: SuperMic_8e:b3:73 (0:c4:7a:8e:b3:73)
> Internet Protocol Version 4, Src: 139.179.210.130, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49813, Dst Port: 80, Seq: 1, Ack: 1, Len: 397
< 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
    Host: gaia.cs.umass.edu\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Safari/605.1.15\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: Keep-alive\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: 613]
```

Browser HTTP version

No.	Time	Source	Destination	Protocol	Length	Info
583	17:20:50.336869	139.179.210.130	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
613	17:20:50.488738	128.119.245.12	139.179.210.130	HTTP	552	HTTP/1.1 200 OK (text/html)

```

> Frame 613: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
> Ethernet II, Src: SuperMic_8e:b3:73 (0:c4:7a:8e:b3:73), Dst: Apple_ea:03:4f (64:5:a:ed:ea:03:4f)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.210.130
> Transmission Control Protocol, Src Port: 80, Dst Port: 49813, Seq: 1, Ack: 398, Len: 486
< 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
      Date: Thu, 21 Oct 2021 14:20:50 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Thu, 21 Oct 2021 05:59:02 GMT\r\n
      ETag: "80-5ced697699568"\r\n
      Accept-Ranges: bytes\r\n
      Content-Length: 128\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 1/1]
    [Time since request: 0.151869000 seconds]
    [Request in frame: 583]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
```

Server HTTP version

- What languages (if any) does your browser indicate that it can accept to the server?
My browser indicates it can accept en-us (English – United States):

No.	Time	Source	Destination	Protocol	Length	Info
583	17:20:50.336869	139.179.210.130	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
613	17:20:50.488738	128.119.245.12	139.179.210.130	HTTP	552	HTTP/1.1 200 OK (text/html)

```

> Frame 583: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface en0, id 0
> Ethernet II, Src: Apple_ea:03:4f (64:5a:ed:ea:03:4f), Dst: SuperMic_8e:b3:73 (0:c4:7a:8e:b3:73)
> Internet Protocol Version 4, Src: 139.179.210.130, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49813, Dst Port: 80, Seq: 1, Ack: 1, Len: 397
< 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
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Safari/605.1.15\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\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: 613]
```

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

IP Address of gaia.cs.umass.edu: 128.119.245.12

IP Address of my computer: 139.179.210.130

No.	Time	Source	Destination	Protocol	Length	Info
583	17:20:50.336869	139.179.210.130	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
613	17:20:50.488738	128.119.245.12	139.179.210.130	HTTP	552	HTTP/1.1 200 OK (text/html)

```

> Frame 583: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface en0, id 0
> Ethernet II, Src: Apple_ea:03:4f (64:5a:ed:ea:03:4f), Dst: SuperMic_8e:b3:73 (0:c4:7a:8e:b3:73)
> Internet Protocol Version 4, Src: 139.179.210.130, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49813, Dst Port: 80, Seq: 1, Ack: 1, Len: 397
< 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
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Safari/605.1.15\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\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: 613]
```

The light blue line indicates from where the information was received.

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

Status code return: 200

No.	Time	Source	Destination	Protocol	Length	Info
→ 583	17:20:50.336869	139.179.210.130	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
→ 613	17:20:50.488738	128.119.245.12	139.179.210.130	HTTP	552	HTTP/1.1 200 OK (text/html)

```

> Frame 613: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
> Ethernet II, Src: SuperMic_8:e:b3:73 (0:c:c4:7a:8:e:b3:73), Dst: Apple_ea:03:4f (64:5:a:ed:ea:03:4f)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.210.130
> Transmission Control Protocol, Src Port: 80, Dst Port: 49813, Seq: 1, Ack: 398, 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: Thu, 21 Oct 2021 14:20:50 GMT\r\n
        Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
        Last-Modified: Thu, 21 Oct 2021 05:59:02 GMT\r\n
        ETag: "80-5ced697699568"\r\n
        Accept-Ranges: bytes\r\n
        Content-Length: 128\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 1/1]
        └ [Time since request: 0.151869000 seconds]
```

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

The HTMP file retrieved was last modified at 21 October 2021, 05:59:02:

No.	Time	Source	Destination	Protocol	Length	Info
→ 583	17:20:50.336869	139.179.210.130	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
→ 613	17:20:50.488738	128.119.245.12	139.179.210.130	HTTP	552	HTTP/1.1 200 OK (text/html)

```

> Frame 613: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
> Ethernet II, Src: SuperMic_8:e:b3:73 (0:c:c4:7a:8:e:b3:73), Dst: Apple_ea:03:4f (64:5:a:ed:ea:03:4f)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.210.130
> Transmission Control Protocol, Src Port: 80, Dst Port: 49813, Seq: 1, Ack: 398, 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: Thu, 21 Oct 2021 14:20:50 GMT\r\n
        Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
        Last-Modified: Thu, 21 Oct 2021 05:59:02 GMT\r\n
        ETag: "80-5ced697699568"\r\n
        Accept-Ranges: bytes\r\n
        Content-Length: 128\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 1/1]
        └ [Time since request: 0.151869000 seconds]
```

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

Bytes received: 128 bytes

No.	Time	Source	Destination	Protocol	Length	Info
→ 583	17:20:50.336869	139.179.210.130	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
← 613	17:20:50.488738	128.119.245.12	139.179.210.130	HTTP	552	HTTP/1.1 200 OK (text/html)

✓ 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: Thu, 21 Oct 2021 14:20:50 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
 Last-Modified: Thu, 21 Oct 2021 05:59:02 GMT\r\n
 ETag: "80-5ced697699568"\r\n
 Accept-Ranges: bytes\r\n
 > Content-Length: 128\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 1/1]
 [Time since request: 0.151869000 seconds]
 [Request in frame: 583]
 [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)

- 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, all the layers are present in the content window.

2. The HTTP CONDITIONAL GET/response interaction

- 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. I can't figure out where it is. I have assessed the entire content of the request sent from my browser and there's no “IF-MODIFIED-SINCE.”

No.	Time	Source	Destination	Protocol	Length	Info
→ 311	18:50:26.113147	139.179.210.130	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
← 322	18:50:26.261172	128.119.245.12	139.179.210.130	HTTP	796	HTTP/1.1 200 OK (text/html)
322	18:50:26.434193	139.179.210.130	128.119.245.12	HTTP	420	GET /favicon.ico HTTP/1.1
350	18:50:26.586033	128.119.245.12	139.179.210.130	HTTP	551	HTTP/1.1 404 Not Found (text/html)
387	18:50:29.431898	139.179.210.130	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
673	18:50:29.580864	128.119.245.12	139.179.210.130	HTTP	796	HTTP/1.1 200 OK (text/html)

> Frame 311: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface en0, id 0
 > Ethernet II, Src: Apple_ea03:4f (64:5:ae:03:4f), Dst: SuperMic_8eb3:73 (0:c4:7a:8:eb:3:73)
 > Internet Protocol Version 4, Src: 139.179.210.130, Dst: 128.119.245.12
 > Transmission Control Protocol, Src Port: 50642, Dst Port: 80, Seq: 1, Ack: 1, Len: 397
 ✓ 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 URL: /wireshark-labs/HTTP-wireshark-file2.html
 Protocol Version: HTTP/1.1
 Host: gaia.cs.umass.edu\r\n
 Upgrade-Insecure-Requests: 1\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Safari/605.1.15\r\n
 Accept-Language: en-us\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: keep-alive\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: 322]

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

Yes, the status is 200 OK from the server and there was no significant delay:

```
No. | Time | Source | Destination | Protocol | Length | Info
+-+ 311 18:50:26.113147 139.179.210.130 128.119.245.12 HTTP 463 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
+-+ 322 18:50:26.261172 128.119.245.12 139.179.210.130 HTTP 796 HTTP/1.1 200 OK (text/html)
+-+ 350 18:50:26.434193 139.179.210.130 128.119.245.12 HTTP 420 GET /favicon.ico HTTP/1.1
+-+ 387 18:50:26.586033 128.119.245.12 139.179.210.130 HTTP 551 HTTP/1.1 404 Not Found (text/html)
+-+ 673 18:50:29.431898 139.179.210.130 128.119.245.12 HTTP 463 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
+-+ 718 18:50:29.580684 128.119.245.12 139.179.210.130 HTTP 796 HTTP/1.1 200 OK (text/html)

> Frame 322: 796 bytes on wire (6368 bits), 796 bytes captured (6368 bits) on interface en0, id 0
> Ethernet II, Src: SuperMic_8e:03:73 (0c:c4:7a:8e:b3:73), Dst: Apple_ea:03:4f (64:5a:ed:ea:03:4f)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.210.130
> Transmission Control Protocol, Src Port: 80, Dst Port: 50642, Seq: 1, Ack: 398, Len: 730
< 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: Thu, 21 Oct 2021 15:50:26 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 21 Oct 2021 05:59:02 GMT\r\n
    ETag: "173-5ced6976989b0"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\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 1/1]
  [Time since request: 0.148025000 seconds]
  [Request in frame: 311]
  [Request URI: http://galia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [Request Headers: Host: r3.o.lencr.org\r\nAccept: */*\r\nUser-Agent: com.apple.trustd/2.1\r\nAccept-Language: en-us\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\n]
  [Response Headers: Host: r3.o.lencr.org\r\nX-Apple-Request-UUID: E6A315B1-93CC-4A82-B483-393731503DF\r\nIf-None-Match: "0326188597BDF69547B8BB0674E817BC878DAAF126BA408C9B733ACA980DD03"\r\nAccept: */*\r\nIf-Modified-Since: Thu, 21 Oct 2021 07:00:00 GMT\r\nUser-Agent: com.apple.trustd/2.1\r\nAccept-Language: en-us\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\n]
  [Full request URI: http://r3.o.lencr.org/MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFEjayaD7K9MtT%2FDeaNL1Z7c1%2BbPEBBQULrMxt1hWye...]
  [HTTP request 1/1]
  [Response in frame: 1291]

0000 64 5a ed ea 03 4f 0c c4 7a 8e b3 73 08 00 45 02 d2 00 z...s-E...
```

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 can seem to have the “IF-MODIFIED-SINCE:” header in my second GET request. This is to make sure we don’t fetch the same contents already downloaded if not modified:

```
No. | Time | Source | Destination | Protocol | Length | Info
+-+ 1288 19:14:22.305516 139.179.210.130 193.140.13.82 HTTP 554 GET /MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFEjayaD7K9MtT%2FDeaNL1Z7c1%2BbPEBBQULrMxt1hWye... HTTP/1.1
+-+ 1291 19:14:22.319994 193.140.13.82 139.179.210.130 HTTP 426 HTTP/1.1 304 Not Modified

> Frame 1288: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface en0, id 0
> Ethernet II, Src: Apple_ea:03:4f (64:5a:ed:ea:03:4f), Dst: SuperMic_8e:b3:73 (0c:c4:7a:8e:b3:73)
> Internet Protocol Version 4, Src: 139.179.210.130, Dst: 193.140.13.82
> Transmission Control Protocol, Src Port: 50600, Dst Port: 80, Seq: 1, Ack: 1, Len: 488
< 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: Thu, 21 Oct 2021 15:50:26 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 21 Oct 2021 05:59:02 GMT\r\n
    ETag: "173-5ced6976989b0"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\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 1/1]
  [Time since request: 0.148025000 seconds]
  [Request in frame: 1288]
  [Request URI: http://r3.o.lencr.org/MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFEjayaD7K9MtT%2FDeaNL1Z7c1%2BbPEBBQULrMxt1hWye...]
  [Request Headers: Host: r3.o.lencr.org\r\nAccept: */*\r\nUser-Agent: com.apple.trustd/2.1\r\nAccept-Language: en-us\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\n]
  [Response Headers: Host: r3.o.lencr.org\r\nX-Apple-Request-UUID: E6A315B1-93CC-4A82-B483-393731503DF\r\nIf-None-Match: "0326188597BDF69547B8BB0674E817BC878DAAF126BA408C9B733ACA980DD03"\r\nAccept: */*\r\nIf-Modified-Since: Thu, 21 Oct 2021 07:00:00 GMT\r\nUser-Agent: com.apple.trustd/2.1\r\nAccept-Language: en-us\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\n]
  [Full request URI: http://r3.o.lencr.org/MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFEjayaD7K9MtT%2FDeaNL1Z7c1%2BbPEBBQULrMxt1hWye...]
  [HTTP request 1/1]
  [Response in frame: 1291]

0000 0d 0a 48 6f 73 74 3a 20 72 33 2e 6f 2e 6c 65 6e ... Host: r3.o.lencr.org
```

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?

No, we have the content in the cache thus we receive the 304 Not Modified status code; the server didn't return files explicitly:

```
No. | Time | Source | Destination | Protocol | Length | Info
+- 1288 19:14:22.305516 139.179.210.130 193.140.13.82 HTTP 554 GET /MFgwVqADAgEAMEBwTTBLMAkGBSs0AwIaBQAEFEjayaD7K9MtT%2FDeaNL1Z7c1%2BbPEBBQULrMxt1hwY...
+- 1291 19:14:22.319994 193.140.13.82 139.179.210.130 HTTP 426 HTTP/1.1 304 Not Modified

> Frame 1291: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits) on interface en0, id 0
> Ethernet II, Src: SuperMic_8eb:b3:73 (0:c4:7a:8e:b3:73), Dst: Apple_ea:03:4f (64:5a:ed:ea:03:4f)
> Internet Protocol Version 4, Src: 193.140.13.82, Dst: 139.179.210.130
> Transmission Control Protocol, Src Port: 80, Dst Port: 50900, Seq: 1, Ack: 489, Len: 360
  Hypertext Transfer Protocol
    > HTTP/1.1 304 Not Modified\r\n
      Content-Type: application/ocsp-response\r\n
      Last-Modified: Thu, 21 Oct 2021 07:00:00 UTC\r\n
      ETag: "022618859780F6F69547888BD674E8178C878DAAF126BA408C9B733ACA980DD3"\r\n
      Cache-Control: public, no-transform, must-revalidate, max-age=16404\r\n
      Expires: Thu, 21 Oct 2021 20:47:46 GMT\r\n
      Date: Thu, 21 Oct 2021 16:14:22 GMT\r\n
      Connection: keep-alive\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.014478000 seconds]
      [Request in frame: 1288]
      [Request URI: http://r3.o.lencr.org/MFgwVqADAgEAMEBwTTBLMAkGBSs0AwIaBQAEFEjayaD7K9MtT%2FDeaNL1Z7c1%2BbPEBBQULrMxt1hwY65QCUdH6%2BdixTCxgISA92Lb%2BjeDPsPqIgSNwfqijZq]

0000 64 Sa ed ea 03 4f 0c c4 7a 8e b3 73 08 00 45 02 dZ--0-- z--s--E-
```

3. Retrieving Long Documents

```
No. | Time | Source | Destination | Protocol | Length | Info
+- 762 21:26:27.339998 139.179.210.130 128.119.245.12 HTTP 463 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
+- 772 21:26:27.492113 128.119.245.12 139.179.210.130 HTTP 583 HTTP/1.1 200 OK (text/html)

> Frame 772: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en0, id 0
> Ethernet II, Src: SuperMic_8eb:b3:73 (0:c4:7a:8e:b3:73), Dst: Apple_ea:03:4f (64:5a:ed:ea:03:4f)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 139.179.210.130
> Transmission Control Protocol, Src Port: 80, Dst Port: 51530, Seq: 4345, Ack: 398, Len: 517
  [4. Reassembled TCP Segments (4861 bytes): #769(1448), #770(1448), #771(1448), #772(517)]
  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: Thu, 21 Oct 2021 18:26:27 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Thu, 21 Oct 2021 05:59:02 GMT\r\n
      ETag: "1194-5ced697853b0"\r\n
      Accept-Ranges: bytes\r\n
      Content-Length: 4500\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 1/1]
      [Time since request: 0.152123000 seconds]
      [Request in frame: 762]
      [Request URI: http://galia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
      File Data: 4500 bytes
    > Line-based text data: text/html (98 lines)
```

4. How many HTTP GET request messages were sent by your browser?

There is only one GET message request sent from my browser to the server

5. How many data-containing TCP segments were needed to carry the single HTTP response?

Only one data segment needed to carry out the HTTP response with 4500 bytes carried in file data. Ironically, I expected there to be more as suggested in the problem set, but I received only one response from the HTTP server. The attached screenshot above shows that only one data containing TCP segment is received.

6. What is the status code and phrase associated with the response to the HTTP GET request?

status code: 200, status response: OK

7. Are there any HTTP status lines in the transmitted data associated with a TCP- induced “Continuation”?

No.

4. HTML Documents with Embedded Objects

The screenshot shows a Wireshark capture window. The packet list pane shows multiple HTTP requests and responses. The details pane shows the full request and response for the file 'HTTP-wireshark-file4.html'. The bytes pane shows the raw binary data of the file. The status bar at the bottom indicates the byte range from 0000 to 0c47a8e73645a.

```
> Frame 235: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface en0, id 0
> Ethernet II, Src: Apple_ea:03:4f (64:5a:ed:ea:03:4f), Dst: SuperMic_8e:b3:73 (0:c4:7a:8e:b3:73)
> Internet Protocol Version 4, Src: 139.179.210.130, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51568, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
> Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file4.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 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 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: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
[HTTP request 1/2]
[Response in frame: 247]
[Next request in frame: 252]
```

5. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?

As one can see from the above screenshot attached, there are in total GET requests sent to the following Internet Addresses:

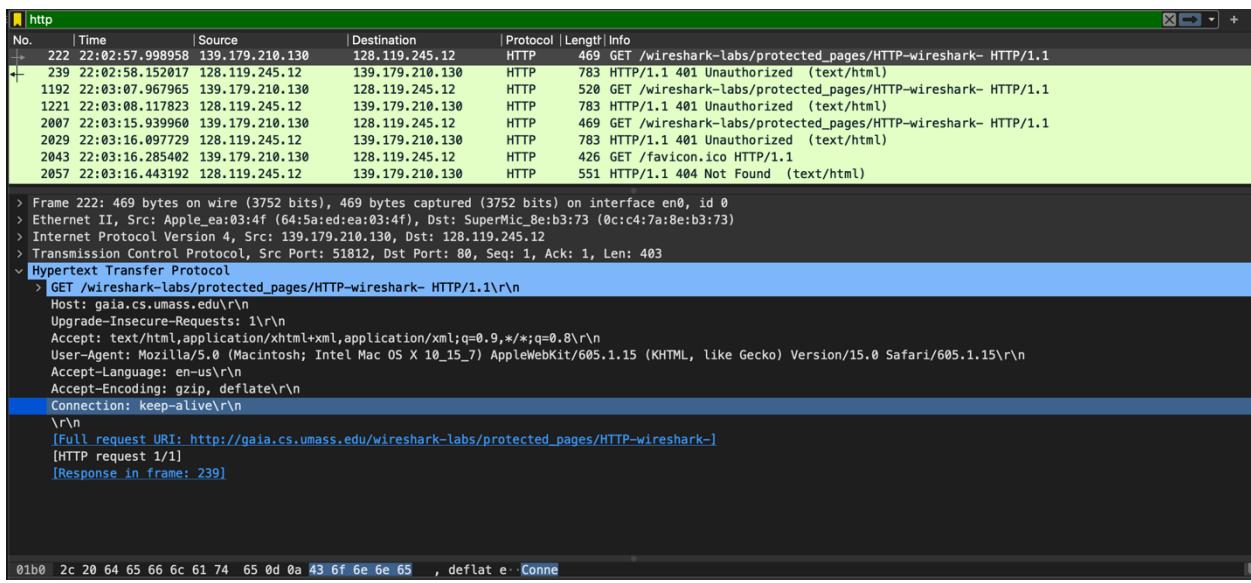
128.119.245.12 (2 requests sent to this address)

178.79.137.164
193.140.13.81

6. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

By checking the TCP ports, we can see if the files were downloaded serially or in parallel. In this case the 2 images were transmitted over 2 TCP connections as depicted in the screenshot above, therefore, they were downloaded serially. Two separate connections were made to retrieve these images separately. We can also see that a status code of 301 is received when a GET is requested for cover_small.jpg; this results in a redirection to retrieve the resource. Thus, more than 2 TCP connections to retrieve the images, hence, serially.

5. HTTP Authentication



The screenshot shows a Wireshark capture of network traffic. The packet list pane shows several HTTP requests and responses. The details pane shows the full request URI: `http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-`. The bytes pane at the bottom shows the raw hex and ASCII data of the captured packets.

```
> Frame 222: 469 bytes on wire (3752 bits), 469 bytes captured (3752 bits) on interface en0, id 0
> Ethernet II, Src: Apple_ea:03:4f (64:5a:ed:ea:03:4f), Dst: SuperMic_8e:b3:73 (0:c4:7a:8e:b3:73)
> Internet Protocol Version 4, Src: 139.179.210.130, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51812, Dst Port: 80, Seq: 1, Ack: 1, Len: 403
< Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Safari/605.1.15\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-]
  [HTTP request 1/1]
  [Response in frame: 239]
```

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

As we can see above, the status code in response to the initial GET request is 401 with phrase 'Unauthorized.'

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

No.	Time	Source	Destination	Protocol	Length	Info
222	22:02:57.998958	139.179.210.130	128.119.245.12	HTTP	469	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
239	22:02:58.152017	128.119.245.12	139.179.210.130	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
+ 1192	22:03:07.967965	139.179.210.130	128.119.245.12	HTTP	520	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
+ 1221	22:03:08.117823	128.119.245.12	139.179.210.130	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
2007	22:03:15.939966	139.179.210.130	128.119.245.12	HTTP	469	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
2029	22:03:16.097729	128.119.245.12	139.179.210.130	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
2043	22:03:16.285402	139.179.210.130	128.119.245.12	HTTP	426	GET /favicon.ico HTTP/1.1
2057	22:03:16.443192	128.119.245.12	139.179.210.130	HTTP	551	HTTP/1.1 404 Not Found (text/html)

```

> Frame 1192: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface en0, id 0
> Ethernet II, Src: Apple_ea:03:4f (64:5:a:ed:ea:03:4f), Dst: SuperMic_8:e:b3:73 (0:c:c4:7:a:8:e:b3:73)
> Internet Protocol Version 4, Src: 139.179.210.130, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51811, Dst Port: 80, Seq: 1, Ack: 1, Len: 454
< 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
      Upgrade-Insecure-Requests: 1\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Safari/605.1.15\r\n
      Accept-Language: en-us\r\n
      Accept-Encoding: gzip, deflate\r\n
    > Authorization: Basic aGFtbWFkLm1hY2hvOmhbW1hZA==\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-]
      [HTTP request 1/1]
      ....
01d0 65 0d 0a 41 75 74 68 6f 72 69 7a 61 74 69 6f 6e  e·Authorization

```

The new field included is Authorization as seen in the screenshot above. I have highlighted the new field. It contains the encoded form of the username and password.

DNS

- Run *nslookup* to obtain the IP address of a Web server in Asia.

For this part, I queried the webpage of AIT based in Thailand. The IP address for that server was 203.159.12.3

```

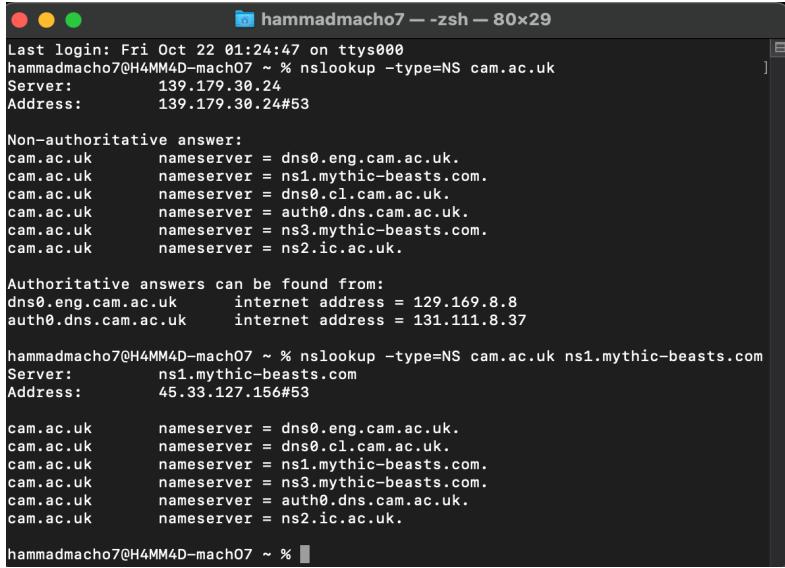
hammadmacho7 -- zsh -- 80x24
Last login: Thu Oct 21 23:28:05 on ttys000
hammadmacho7@H4MM4D-mach07 ~ % nslookup www.asdu.ait.ac.th
Server:        139.179.30.24
Address:       139.179.30.24#53

Non-authoritative answer:
www.asdu.ait.ac.th canonical name = www.misu.ait.ac.th.
Name:   www.misu.ait.ac.th
Address: 203.159.12.3

hammadmacho7@H4MM4D-mach07 ~ %

```

- Run *nslookup* to determine the authoritative DNS servers for a university in Europe.



```
Last login: Fri Oct 22 01:24:47 on ttys000
hammadmacho7@H4MM4D-mach07 ~ % nslookup -type=NS cam.ac.uk
Server:      139.179.30.24
Address:     139.179.30.24#53

Non-authoritative answer:
cam.ac.uk      nameserver = dns0.eng.cam.ac.uk.
cam.ac.uk      nameserver = ns1.mythic-beasts.com.
cam.ac.uk      nameserver = dns0.cl.cam.ac.uk.
cam.ac.uk      nameserver = auth0.dns.cam.ac.uk.
cam.ac.uk      nameserver = ns3.mythic-beasts.com.
cam.ac.uk      nameserver = ns2.ic.ac.uk.

Authoritative answers can be found from:
dns0.eng.cam.ac.uk    internet address = 129.169.8.8
auth0.dns.cam.ac.uk   internet address = 131.111.8.37

hammadmacho7@H4MM4D-mach07 ~ % nslookup -type=NS cam.ac.uk ns1.mythic-beasts.com
Server:      ns1.mythic-beasts.com
Address:     45.33.127.156#53

cam.ac.uk      nameserver = dns0.eng.cam.ac.uk.
cam.ac.uk      nameserver = dns0.cl.cam.ac.uk.
cam.ac.uk      nameserver = ns1.mythic-beasts.com.
cam.ac.uk      nameserver = ns3.mythic-beasts.com.
cam.ac.uk      nameserver = auth0.dns.cam.ac.uk.
cam.ac.uk      nameserver = ns2.ic.ac.uk.

hammadmacho7@H4MM4D-mach07 ~ %
```

The query I sent for this part was for www.cam.ac.uk (Cambridge University) in England. One of the primary/authoritative servers is:
ns1.mythic-beasts.com.

- Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail.



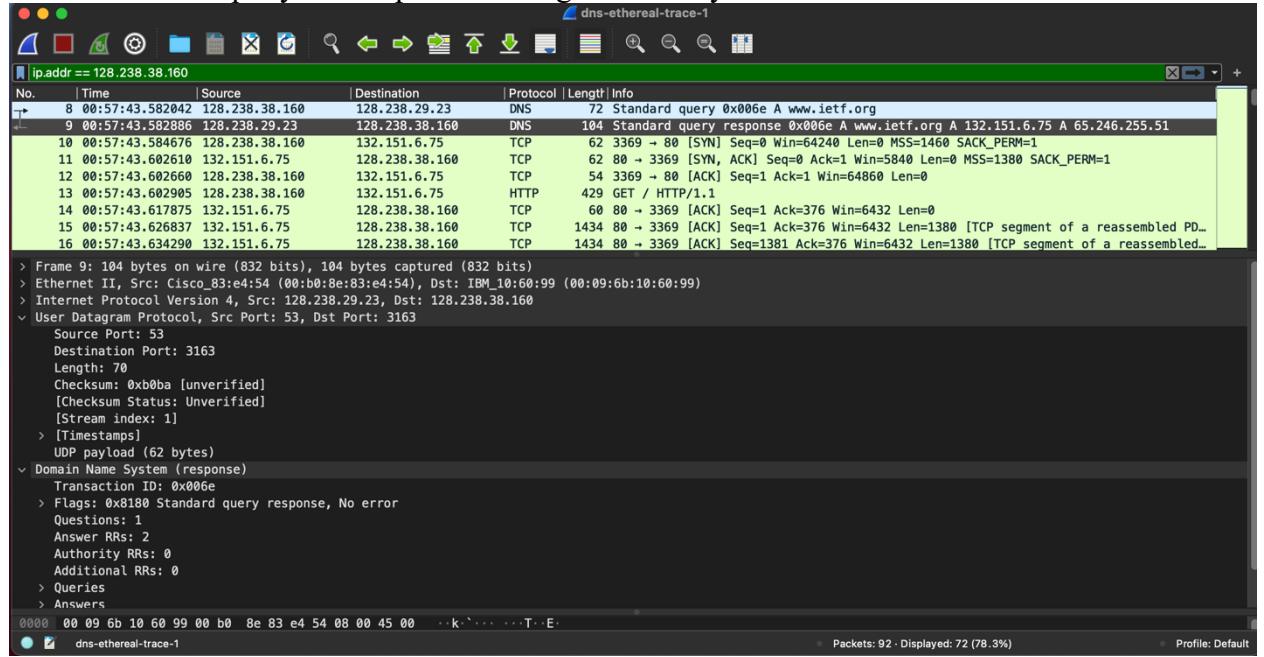
```
[hammadmacho7@H4MM4D-mach07 ~ % nslookup ox.ac.uk ns1.mythic-beasts.com
Server:      ns1.mythic-beasts.com
Address:     45.33.127.156#53

Name:  ox.ac.uk
Address: 151.101.130.216
Name:  ox.ac.uk
Address: 151.101.66.216
Name:  ox.ac.uk
Address: 151.101.2.216
Name:  ox.ac.uk
Address: 151.101.194.216

hammadmacho7@H4MM4D-mach07 ~ %
```

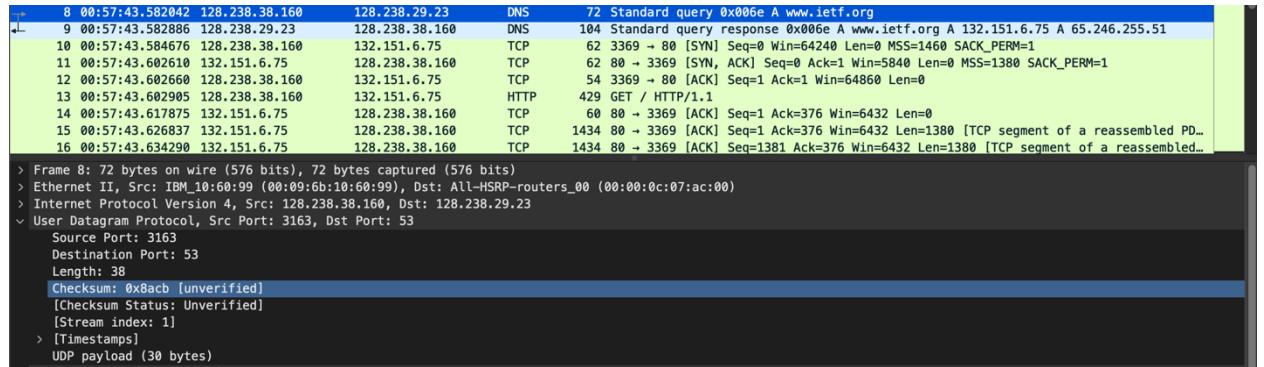
I couldn't find the servers for yahoo mail thus I queried another British university Oxford university using **ns1.mythic-beasts.com**.

4. Locate the DNS query and response messages. Are they sent over UDP or TCP?



As seen in the Screenshot, it is sent over UDP (User Datagram Protocol).

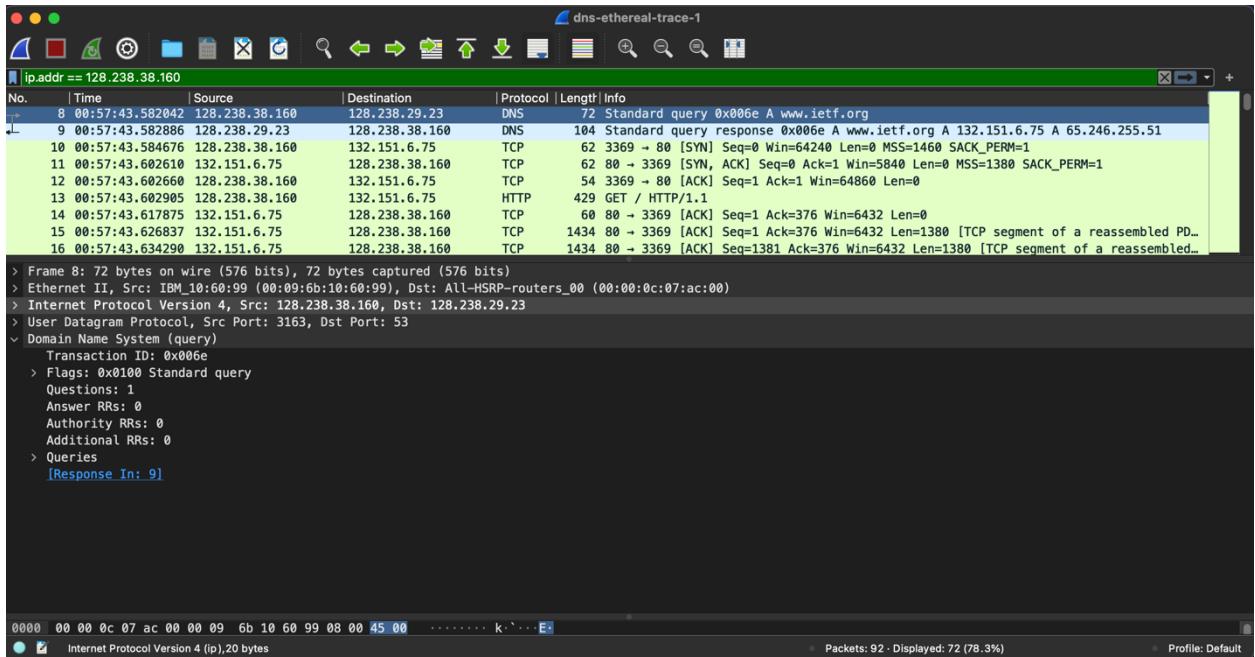
5. What is the destination port for the DNS query message? What is the source port of DNS response message?



Source port: 3163

Destination Port: 53

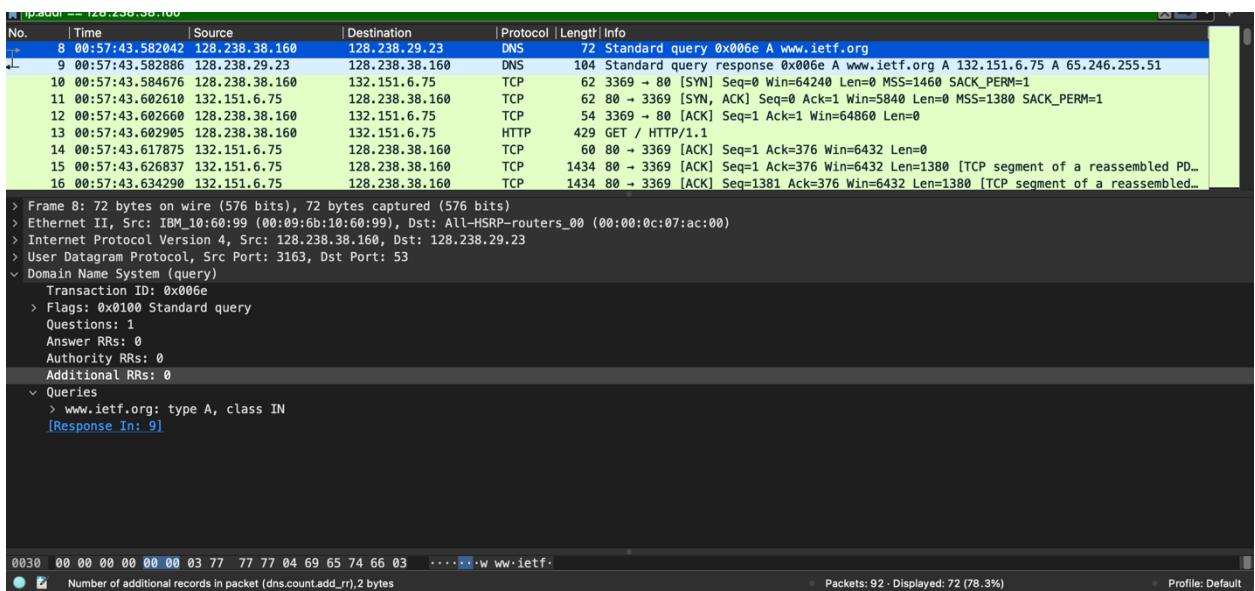
6. To what IP address is the DNS query message sent? Use `ipconfig` to determine the IP address of your local DNS server. Are these two IP addresses the same?



DNS message sent to IP Address: 128.238.29.23

Yes, it must be the local DNS server and be same. I have used the packet lists provided in the assignment PDF. I have resorted to using the packets provided as I have a MacOS which uses Unix CLI. The commands are very different from the ones provided, thus, for uniformity purposes, I am using packets.

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



The query type is A, and as the screenshot above displays, it doesn't contain any answers.

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

```

No. | Time | Source | Destination | Protocol | Length | Info
8  00:57:43.582842 128.238.38.160 128.238.29.23  DNS   72 Standard query 0x006e A www.ietf.org
9  00:57:43.582886 128.238.29.23 128.238.38.160  DNS   104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
10 00:57:43.584676 128.238.38.160 132.151.6.75  TCP    62 3369 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
11 00:57:43.602610 132.151.6.75 128.238.38.160  TCP    62 80 - 3369 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
12 00:57:43.602660 128.238.38.160 132.151.6.75  TCP    54 3369 -> 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
13 00:57:43.602985 128.238.38.160 132.151.6.75  HTTP   429 GET / HTTP/1.1
14 00:57:43.617875 132.151.6.75 128.238.38.160  TCP    60 80 - 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=0
15 00:57:43.626837 132.151.6.75 128.238.38.160  TCP    1434 80 - 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PD...
16 00:57:43.634290 132.151.6.75 128.238.38.160  TCP    1434 80 - 3369 [ACK] Seq=1381 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled...

> Frame 9: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
> Ethernet II, Src: Cisco_83:e4:54 (00:b0:8e:83:e4:54), Dst: IBM_10:60:99 (00:09:6b:10:60:99)
> Internet Protocol Version 4, Src: 128.238.29.23, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3163
< Domain Name System (response)
  Transaction ID: 0x006e
  Flags: 0x8100 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
< Queries
  > www.ietf.org: type A, class IN
< Answers
  > www.ietf.org: type A, class IN, addr 132.151.6.75
  > www.ietf.org: type A, class IN, addr 65.246.255.51
  [Request In: 8]
  [Time: 0.000844000 seconds]

0030 00 02 00 00 00 03 77 77 04 69 65 74 66 03  ... w www.ietf...
  Number of additional records in packet (dns.count.add_rr),2 bytes
  Packets: 92 - Displayed: 72 (78.3%)  Profile: Default

```

Two answers are provided;
each answer contains name, type, class, time to live, data length, and address of the queried webpage.

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?

```

No. | Time | Source | Destination | Protocol | Length | Info
8  00:57:43.582842 128.238.38.160 128.238.29.23  DNS   72 Standard query 0x006e A www.ietf.org
9  00:57:43.582886 128.238.29.23 128.238.38.160  DNS   104 Standard query response 0x006e A www.ietf.org A 132.151.6.75 A 65.246.255.51
10 00:57:43.584676 128.238.38.160 132.151.6.75  TCP    62 3369 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
11 00:57:43.602610 132.151.6.75 128.238.38.160  TCP    62 80 - 3369 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
12 00:57:43.602660 128.238.38.160 132.151.6.75  TCP    54 3369 -> 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
13 00:57:43.602985 128.238.38.160 132.151.6.75  HTTP   429 GET / HTTP/1.1
14 00:57:43.617875 132.151.6.75 128.238.38.160  TCP    60 80 - 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=0
15 00:57:43.626837 132.151.6.75 128.238.38.160  TCP    1434 80 - 3369 [ACK] Seq=1 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled PD...
16 00:57:43.634290 132.151.6.75 128.238.38.160  TCP    1434 80 - 3369 [ACK] Seq=1381 Ack=376 Win=6432 Len=1380 [TCP segment of a reassembled...

> Frame 10: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:c0:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 132.151.6.75
> Transmission Control Protocol, Src Port: 3369, Dst Port: 80, Seq: 0, Len: 0

0000 00 00 0c 07 ac 00 00 09 6b 10 60 99 08 00 45 00  ..... k. . E.
  dns-ethereal-trace-1
  Packets: 92 - Displayed: 72 (78.3%)  Profile: Default

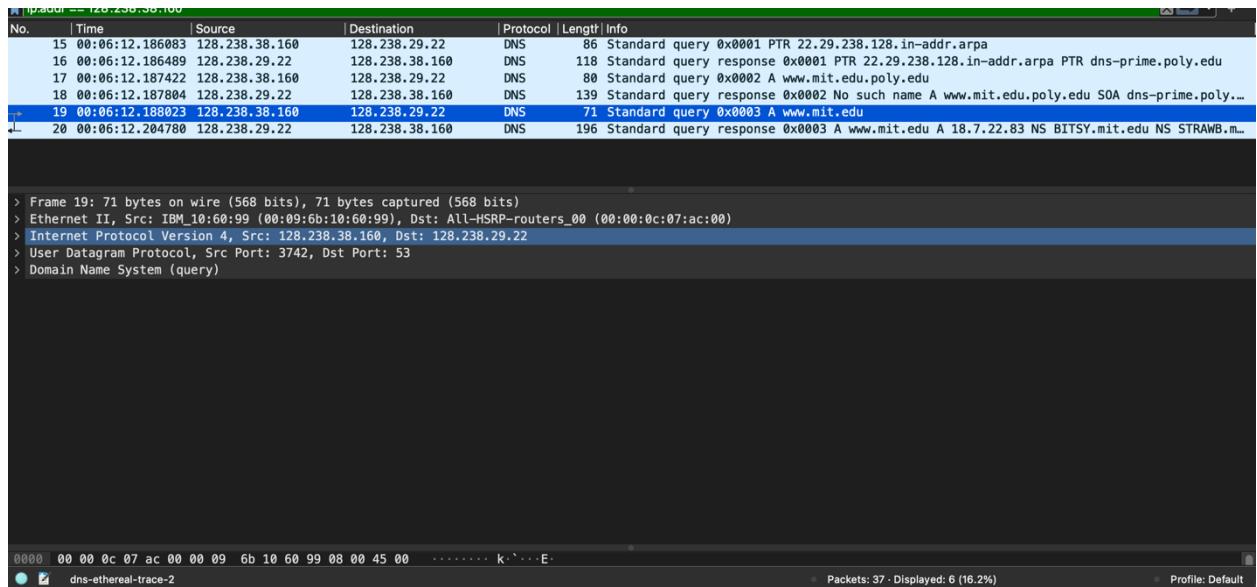
```

Yes, it corresponds to the IP address 132.151.6.75

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

No, there are no further DNS requests sent. The images are loaded from www.ietf.org. We can also see from the screenshots provided above that only one DNS request is sent.

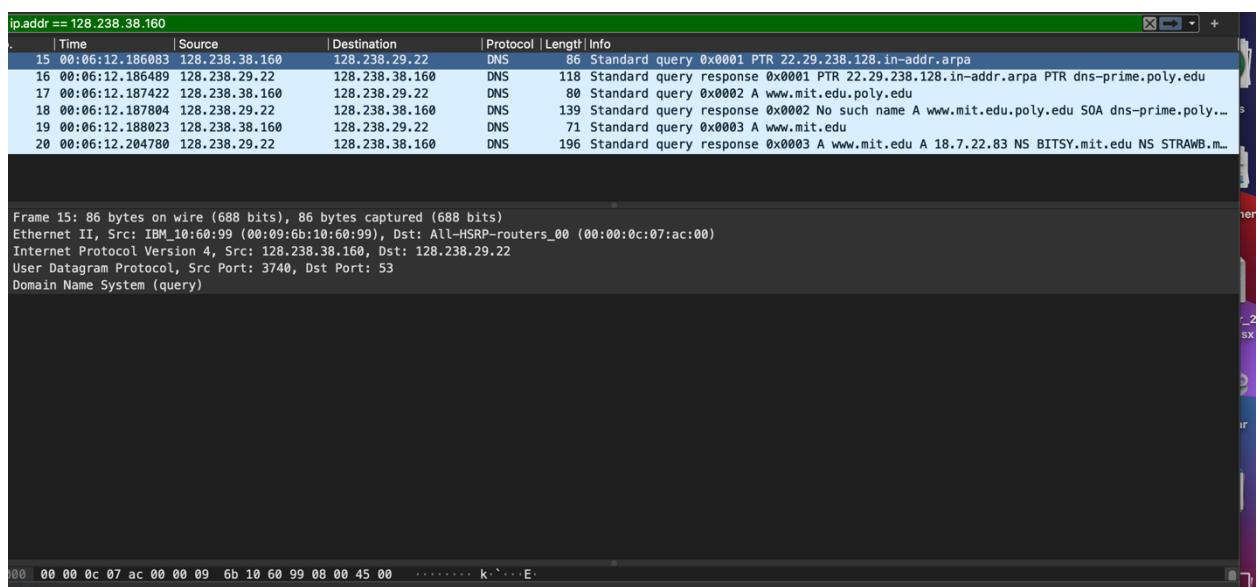
11. What is the destination port for the DNS query message? What is the source port of DNS response message?



Source Port for query: 3742

Source Port for response: 53

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



IP address query message sent: 128.238.29.22, and yes, it is the default local DNS server.

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

No.	Time	Source	Destination	Protocol	Length	Info
15	00:06:12.186083	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
16	00:06:12.186489	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
17	00:06:12.187422	128.238.38.160	128.238.29.22	DNS	80	Standard query 0x0002 A www.mit.edu.poly.edu
18	00:06:12.187804	128.238.29.22	128.238.38.160	DNS	139	Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly...
19	00:06:12.188023	128.238.38.160	128.238.29.22	DNS	71	Standard query 0x0003 A www.mit.edu
20	00:06:12.204780	128.238.29.22	128.238.38.160	DNS	196	Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.m...

> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3742, Dst Port: 53
v Domain Name System (query)
 Transaction ID: 0x0003
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
v Queries
 > www.mit.edu: type A, class IN
 [Response In: 20]
0030 00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65 :rw ww-mit.e
Text item (text),17 bytes Packets: 37 - Displayed: 6 (16.2%) Profile: Default

The type of query sent is A, and no this query doesn't contain any answers.

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

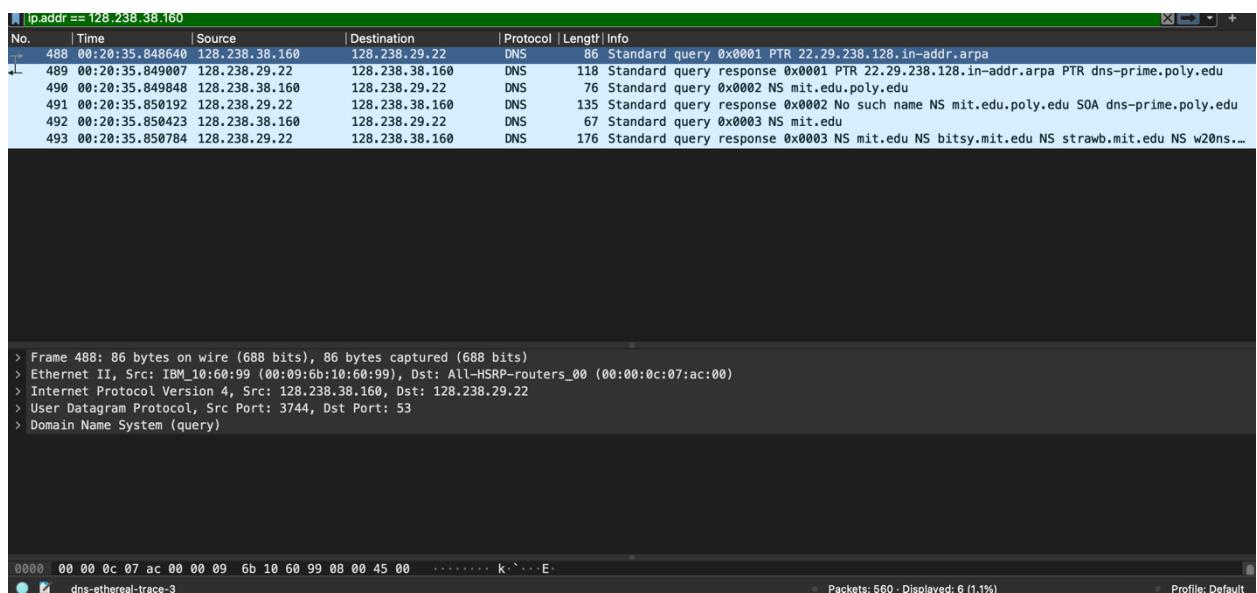
No.	Time	Source	Destination	Protocol	Length	Info
15	00:06:12.186083	128.238.38.160	128.238.29.22	DNS	86	Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
16	00:06:12.186489	128.238.29.22	128.238.38.160	DNS	118	Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
17	00:06:12.187422	128.238.38.160	128.238.29.22	DNS	80	Standard query 0x0002 A www.mit.edu.poly.edu
18	00:06:12.187804	128.238.29.22	128.238.38.160	DNS	139	Standard query response 0x0002 No such name A www.mit.edu.poly.edu SOA dns-prime.poly...
19	00:06:12.188023	128.238.38.160	128.238.29.22	DNS	71	Standard query 0x0003 A www.mit.edu
20	00:06:12.204780	128.238.29.22	128.238.38.160	DNS	196	Standard query response 0x0003 A www.mit.edu A 18.7.22.83 NS BITSY.mit.edu NS STRAWB.m...

Answer RRs: 1
Authority RRs: 3
Additional RRs: 3
v Queries
 > www.mit.edu: type A, class IN
v Answers
 > www.mit.edu: type A, class IN, addr 18.7.22.83
v Authoritative nameservers
 > mit.edu: type NS, class IN, ns BITSY.mit.edu
 > mit.edu: type NS, class IN, ns STRAWB.mit.edu
 > mit.edu: type NS, class IN, ns W20NS.mit.edu
v Additional records
0090 4e 53 c0 10 c0 39 00 01 00 01 00 00 54 60 00 04 NS..:9..:..T`..
Text item (text),48 bytes Packets: 37 - Displayed: 6 (16.2%) Profile: Default

One answer provided and three authority RR's.

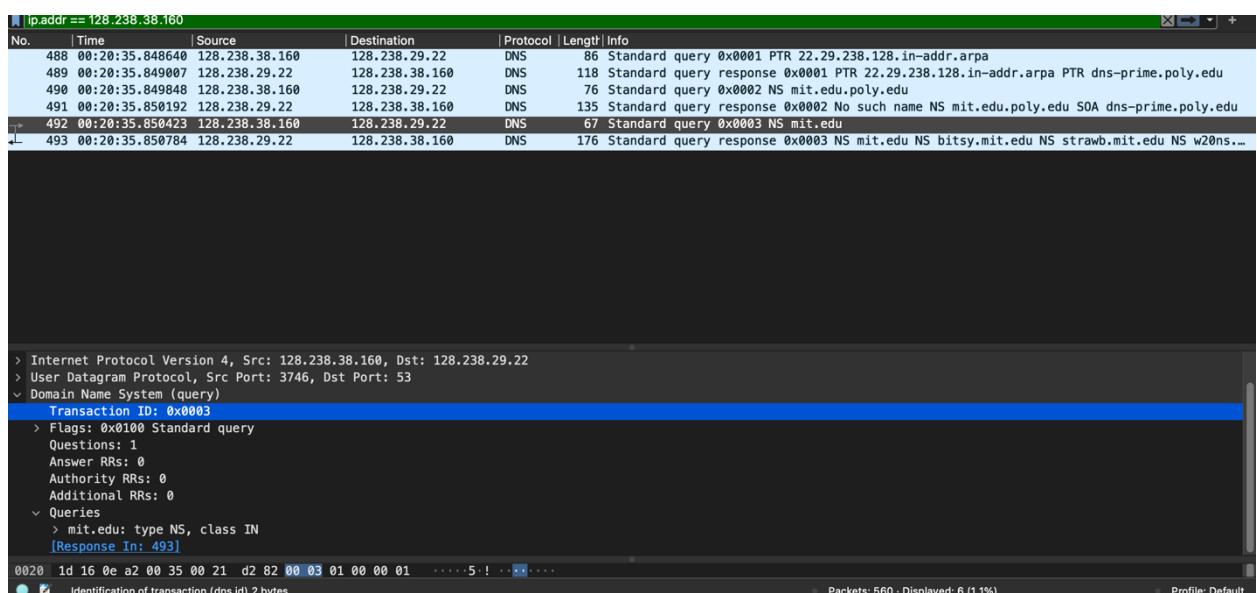
15. Provide a screenshot. (Provided above)

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



The local DNS server query sent to is IP address 128.238.29.22, and yes, this is the local DNS server. We can see that in the above screenshots that it is the same local server queries are sent to.

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



Examining the second last and last queries; the last query request sent is of type NS as seen in the above screenshot.

18. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?

MIT name servers responded with addresses:

bitsy.mit.edu 18.72.0.3

strawb.mit.edu 18.71.0.151

w20ns.mit.edu 18.70.0.160

And no authority RRs.

```
ip.addr == 128.238.38.160
No. | Time | Source | Destination | Protocol | Length | Info
---|---|---|---|---|---|---
488 00:20:35.848640 128.238.38.160 128.238.29.22 DNS 86 Standard query 0x0001 PTR 22.29.238.128.in-addr.arpa
489 00:20:35.849007 128.238.29.22 128.238.38.160 DNS 118 Standard query response 0x0001 PTR 22.29.238.128.in-addr.arpa PTR dns-prime.poly.edu
490 00:20:35.849844 128.238.38.160 128.238.29.22 DNS 76 Standard query 0x0002 NS mit.poly.edu
491 00:20:35.850192 128.238.29.22 128.238.38.160 DNS 135 Standard query response 0x0002 No such name NS mit.edu.poly.edu SOA dns-prime.poly.edu
492 00:20:35.850423 128.238.38.160 128.238.29.22 DNS 67 Standard query 0x0003 NS mit.edu
493 00:20:35.850784 128.238.29.22 128.238.38.160 DNS 176 Standard query response 0x0003 NS mit.edu NS bitsy.mit.edu NS strawb.mit.edu NS w20ns...
Answer RRs: 3
Authority RRs: 0
Additional RRs: 3
Queries
> mit.edu: type NS, class IN
Answers
> mit.edu: type NS, class IN, ns bitsy.mit.edu
> mit.edu: type NS, class IN, ns strawb.mit.edu
> mit.edu: type NS, class IN, ns w20ns.mit.edu
Additional records
[Request In: 492]
[Time: 0.000361000 seconds]

0020 26 a0 00 35 0e a2 00 0e c3 02 00 03 81 80 00 01 & 5----- . . . .
Identification of transaction (dns.id).2 bytes
Packets: 560 - Displayed: 6 (1.1%)
Profile: Default

Queries
> mit.edu: type NS, class IN
Answers
> mit.edu: type NS, class IN, ns bitsy.mit.edu
> mit.edu: type NS, class IN, ns strawb.mit.edu
> mit.edu: type NS, class IN, ns w20ns.mit.edu
Additional records
> bitsy.mit.edu: type A, class IN, addr 18.72.0.3
> strawb.mit.edu: type A, class IN, addr 18.71.0.151
> w20ns.mit.edu: type A, class IN, addr 18.70.0.160
[Request In: 492]
[Time: 0.000361000 seconds]
```

19. Provide a screenshot. (Provided above)

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?

No.	Time	Source	Destination	Protocol	Length	Info
51	00:36:47.779514	128.238.38.201	128.238.38.160	TCP	62	1597 → 3127 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
52	00:36:47.779539	128.238.38.201	128.238.38.160	TCP	62	1596 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
53	00:36:47.779549	128.238.38.201	128.238.38.160	TCP	62	1600 → 130 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
54	00:36:47.779592	128.238.38.201	128.238.38.160	TCP	62	1595 → 1025 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
55	00:36:47.779691	128.238.38.201	128.238.38.160	TCP	62	1598 → 6129 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
56	00:36:47.779778	128.238.38.201	128.238.38.160	TCP	62	1593 → 135 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
57	00:36:47.779785	128.238.38.201	128.238.38.160	TCP	62	1592 → 2745 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
100	00:36:49.831431	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101	00:36:49.844651	18.72.0.3	128.238.38.160	DNS	212	Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY/MIT.EDU NS W20NS.M...
102	00:36:49.845565	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.aiit.or.kr.poly.edu
103	00:36:49.859418	18.72.0.3	128.238.38.160	DNS	135	Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.p...
104	00:36:49.859652	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.aiit.or.kr
105	00:36:49.873994	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3...

> Frame 100: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 3751, Dst Port: 53
 `- Domain Name System (query)
 Transaction ID: 0x0001
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 `- Queries
 0030 00 00 00 00 00 00 01 33 01 30 02 37 32 02 31 383 0·72·18
 Text item (text), 28 bytes
 Packets: 155 · Displayed: 13 (8.4%) Profile: Default

The query is sent to IP address 18.72.0.3, which is the IP address of bitsy.mit.edu (the server queried for the query instead of the default local server).

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

No.	Time	Source	Destination	Protocol	Length	Info
51	00:36:47.779514	128.238.38.201	128.238.38.160	TCP	62	1597 → 3127 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
52	00:36:47.779539	128.238.38.201	128.238.38.160	TCP	62	1596 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
53	00:36:47.779549	128.238.38.201	128.238.38.160	TCP	62	1600 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
54	00:36:47.779592	128.238.38.201	128.238.38.160	TCP	62	1595 → 1025 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
55	00:36:47.779691	128.238.38.201	128.238.38.160	TCP	62	1598 → 6129 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
56	00:36:47.779778	128.238.38.201	128.238.38.160	TCP	62	1593 → 135 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
57	00:36:47.779785	128.238.38.201	128.238.38.160	TCP	62	1592 → 2745 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
100	00:36:49.831431	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101	00:36:49.844651	18.72.0.3	128.238.38.160	DNS	212	Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY/MIT.EDU NS W20NS.M...
102	00:36:49.845565	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.aiit.or.kr.poly.edu
103	00:36:49.859418	18.72.0.3	128.238.38.160	DNS	135	Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.p...
104	00:36:49.859652	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.aiit.or.kr
105	00:36:49.873994	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3...

> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 3753, Dst Port: 53
 Domain Name System (query)
 Transaction ID: 0x0003
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 > www.aiit.or.kr: type A, class IN
 [Response In: 105]
 0030 00 00 00 00 00 00 03 77 77 77 04 61 69 69 74 02w ww.aiit.
 Text item (text), 20 bytes

Packets: 155 - Displayed: 13 (8.4%) Profile: Default

Type of query: A
 and the query message doesn't contain any answers.

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

No.	Time	Source	Destination	Protocol	Length	Info
51	00:36:47.779514	128.238.38.201	128.238.38.160	TCP	62	1597 → 3127 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
52	00:36:47.779539	128.238.38.201	128.238.38.160	TCP	62	1596 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
53	00:36:47.779549	128.238.38.201	128.238.38.160	TCP	62	1600 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
54	00:36:47.779592	128.238.38.201	128.238.38.160	TCP	62	1595 → 1025 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
55	00:36:47.779691	128.238.38.201	128.238.38.160	TCP	62	1598 → 6129 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
56	00:36:47.779778	128.238.38.201	128.238.38.160	TCP	62	1593 → 135 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
57	00:36:47.779785	128.238.38.201	128.238.38.160	TCP	62	1592 → 2745 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
100	00:36:49.831431	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101	00:36:49.844651	18.72.0.3	128.238.38.160	DNS	212	Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY/MIT.EDU NS W20NS.M...
102	00:36:49.845565	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.aiit.or.kr.poly.edu
103	00:36:49.859418	18.72.0.3	128.238.38.160	DNS	135	Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.p...
104	00:36:49.859652	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.aiit.or.kr
105	00:36:49.873994	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3...

> Internet Protocol Version 4, Src: 18.72.0.3, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3753
 Domain Name System (response)
 Transaction ID: 0x0003
 Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 1
 Authority RRs: 2
 Additional RRs: 2
 Queries
 > www.aiit.or.kr: type A, class IN
 Answers
 0030 00 01 00 02 00 02 03 77 77 77 04 61 69 69 74 02w ww.aiit.
 Text item (text), 20 bytes

Packets: 155 - Displayed: 13 (8.4%) Profile: Default

There is One answer RRs and Two authority RRs. The answer contains type of query, address of the queried webpage, class, time to live, data length, and address. The below screenshot provides further details of the answer and authority RRs.

```

Additional RRs: 2
  < Queries
    > www.aiit.or.kr: type A, class IN
  < Answers
    < www.aiit.or.kr: type A, class IN, addr 218.36.94.200
      Name: www.aiit.or.kr
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 3338 (55 minutes, 38 seconds)
      Data length: 4
      Address: 218.36.94.200
  < Authoritative nameservers
    < aiit.or.kr: type NS, class IN, ns ns.aiit.or.kr

```

```

  < Queries
    > www.aiit.or.kr: type A, class IN
  < Answers
    < www.aiit.or.kr: type A, class IN, addr 218.36.94.200
  < Authoritative nameservers
    > aiit.or.kr: type NS, class IN, ns ns.aiit.or.kr
    > aiit.or.kr: type NS, class IN, ns w3.aiit.or.kr
  < Additional records
    > ns.aiit.or.kr: type A, class IN, addr 222.106.36.66
    > w3.aiit.or.kr: type A, class IN, addr 222.106.36.67
[Request In: 104]
[Time: 0.014342000 seconds]

```

23. Provide a screenshot.

No.	Time	Source	Destination	Protocol	Length	Info
51	00:36:47.779514	128.238.38.201	128.238.38.160	TCP	62	1597 → 3127 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
52	00:36:47.779539	128.238.38.201	128.238.38.160	TCP	62	1596 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
53	00:36:47.779549	128.238.38.201	128.238.38.160	TCP	62	1600 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
54	00:36:47.779592	128.238.38.201	128.238.38.160	TCP	62	1595 → 1025 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
55	00:36:47.779691	128.238.38.201	128.238.38.160	TCP	62	1598 → 6129 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
56	00:36:47.779778	128.238.38.201	128.238.38.160	TCP	62	1593 → 135 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
57	00:36:47.779785	128.238.38.201	128.238.38.160	TCP	62	1592 → 2745 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
100	00:36:49.831431	128.238.38.160	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
101	00:36:49.844651	18.72.0.3	128.238.38.160	DNS	212	Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY/MIT.EDU NS W20NS.M...
102	00:36:49.845565	128.238.38.160	18.72.0.3	DNS	83	Standard query 0x0002 A www.aiit.or.kr.poly.edu
103	00:36:49.859418	18.72.0.3	128.238.38.160	DNS	135	Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.p...
104	00:36:49.859652	128.238.38.160	18.72.0.3	DNS	74	Standard query 0x0003 A www.aiit.or.kr
105	00:36:49.873994	18.72.0.3	128.238.38.160	DNS	156	Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3...

Questions: 1
Answer RRs: 1
Authority RRs: 2
Additional RRs: 2

- < Queries
 - > www.aiit.or.kr: type A, class IN
- < Answers
 - > www.aiit.or.kr: type A, class IN, addr 218.36.94.200
- < Authoritative nameservers
- < Additional records

[Request In: 104]
[Time: 0.014342000 seconds]

0040 6f 72 02 6b 72 00 00 01 00 01 c0 0c 00 01 00 01 or.kr...
Packets: 155 · Displayed: 13 (8.4%)

Text item (text), 16 bytes Profile: Default