# University of Tehran

## School of Electrical and Computer Engineering

## Computer Networks

# Wireshark Lab 2

| **Student Name** | **Student ID** |
|---|---|
| Alireza Javid | 810198375 |

**Instructor:**

Dr. Shahmansouri

# Contents

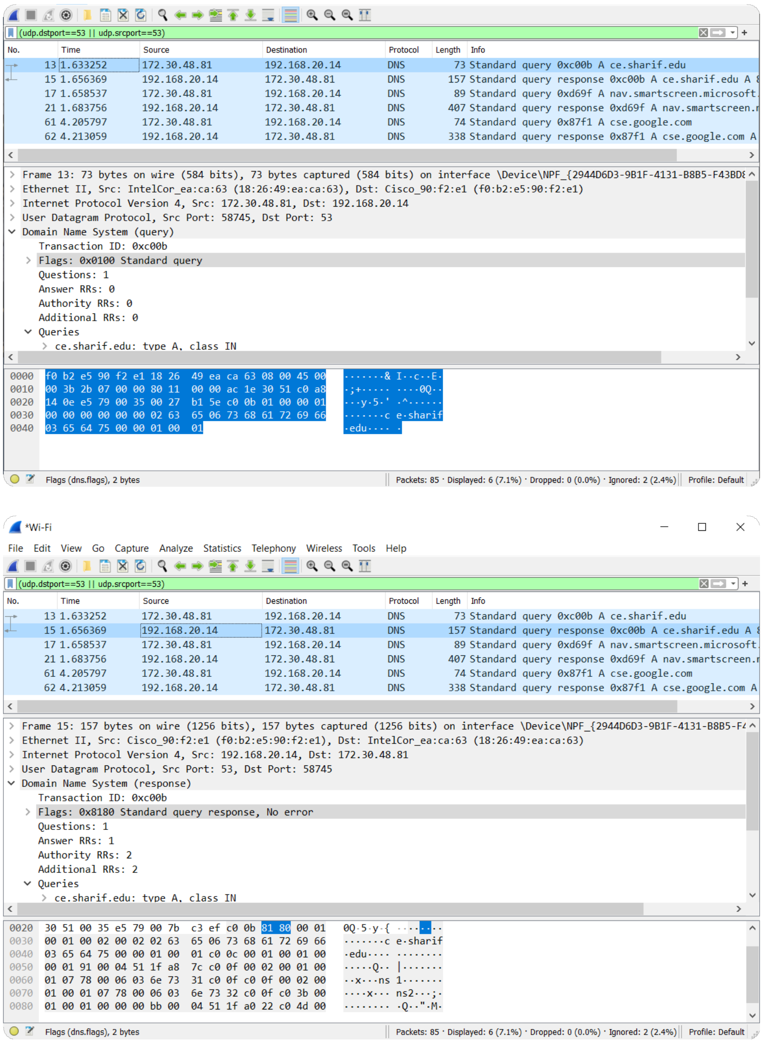
1 DNS 2

2 HTTP 9

# 1 DNS

Our random website must be a http protocle. we use http://ce.sharif.edu as our random website.
With *ipconfig /flushdns* command, we flush DNS in our computer. DNS flushing is the mechanism which the user can manually make all the entries in the cache invalid, so the host's computer re-fetches new pairs from now on, whenever it needs and stores it in the local cache.
Now back to Lab's questions:

1. In figure 1 we can see these packets contain requests to the DNS servers for translating a host name to an IP address First DNS is quary and second DNS is a response massage to quary. other DNS massages is for Google and Microsoft servers which we talk about them later.



```
(udp.dstport==53 || udp.srcport==53)

No.   Time      Source          Destination     Protocol Length Info
   13 1.633252  172.30.48.81    192.168.20.14   DNS         73 Standard query 0xc00b A ce.sharif.edu
   15 1.656369  192.168.20.14   172.30.48.81    DNS        157 Standard query response 0xc00b A ce.sharif.edu A 8
   17 1.658537  172.30.48.81    192.168.20.14   DNS         89 Standard query 0xd69f A nav.smartscreen.microsoft.
   21 1.683756  192.168.20.14   172.30.48.81    DNS        407 Standard query response 0xd69f A nav.smartscreen.r
   61 4.205797  172.30.48.81    192.168.20.14   DNS         74 Standard query 0x87f1 A cse.google.com
   62 4.213059  192.168.20.14   172.30.48.81    DNS        338 Standard query response 0x87f1 A cse.google.com A
```

```
> Frame 13: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{2944D6D3-9B1F-4131-B8B5-F43BD8
> Ethernet II, Src: IntelCor_ea:ca:63 (18:26:49:ea:ca:63), Dst: Cisco_90:f2:e1 (f0:b2:e5:90:f2:e1)
> Internet Protocol Version 4, Src: 172.30.48.81, Dst: 192.168.20.14
> User Datagram Protocol, Src Port: 58745, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xc00b
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > ce.sharif.edu: type A, class IN
```

```
0000  f0 b2 e5 90 f2 e1 18 26  49 ea ca 63 08 00 45 00   ·······& I··c··E·
0010  00 3b 2b 07 00 00 80 11  00 00 ac 1e 30 51 c0 a8   ·;+····· ····0Q··
0020  14 0e e5 79 00 35 00 27  b1 5e c0 0b 01 00 00 01   ···y·5·' ·^······
0030  00 00 00 00 00 00 02 63  65 06 73 68 61 72 69 66   ·······c e·sharif
0040  03 65 64 75 00 00 01 00  01                        ·edu···· ·
```

Flags (dns.flags), 2 bytes | Packets: 85 · Displayed: 6 (7.1%) · Dropped: 0 (0.0%) · Ignored: 2 (2.4%) | Profile: Default

```
(udp.dstport==53 || udp.srcport==53)

No.   Time      Source          Destination     Protocol Length Info
   13 1.633252  172.30.48.81    192.168.20.14   DNS         73 Standard query 0xc00b A ce.sharif.edu
   15 1.656369  192.168.20.14   172.30.48.81    DNS        157 Standard query response 0xc00b A ce.sharif.edu A 8
   17 1.658537  172.30.48.81    192.168.20.14   DNS         89 Standard query 0xd69f A nav.smartscreen.microsoft.
   21 1.683756  192.168.20.14   172.30.48.81    DNS        407 Standard query response 0xd69f A nav.smartscreen.r
   61 4.205797  172.30.48.81    192.168.20.14   DNS         74 Standard query 0x87f1 A cse.google.com
   62 4.213059  192.168.20.14   172.30.48.81    DNS        338 Standard query response 0x87f1 A cse.google.com A
```

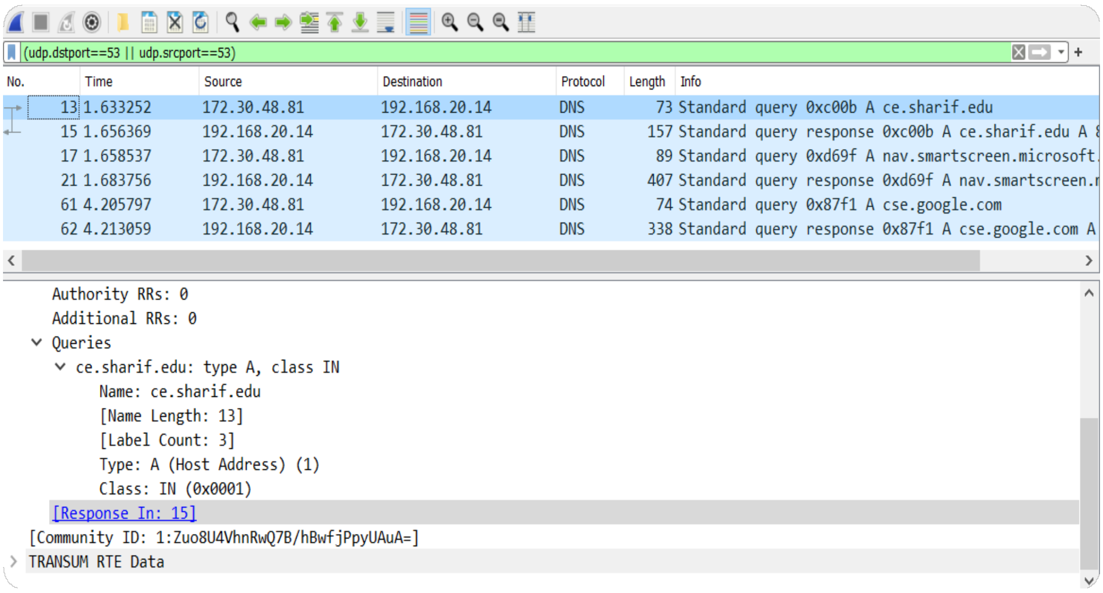
```
> Frame 15: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface \Device\NPF_{2944D6D3-9B1F-4131-B8B5-F4
> Ethernet II, Src: Cisco_90:f2:e1 (f0:b2:e5:90:f2:e1), Dst: IntelCor_ea:ca:63 (18:26:49:ea:ca:63)
> Internet Protocol Version 4, Src: 192.168.20.14, Dst: 172.30.48.81
> User Datagram Protocol, Src Port: 53, Dst Port: 58745
v Domain Name System (response)
    Transaction ID: 0xc00b
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  v Queries
    > ce.sharif.edu: type A, class IN
```

```
0020  30 51 00 35 e5 79 00 7b  c3 ef c0 0b 81 80 00 01   0Q·5·y·{ ········
0030  00 01 00 02 00 02 02 63  65 06 73 68 61 72 69 66   ·······c e·sharif
0040  03 65 64 75 00 00 01 00  01 c0 0c 00 01 00 01 00   ·edu···· ········
0050  00 01 91 00 04 51 1f a8  7c c0 0f 00 02 00 01 00   ·····Q·· |·······
0060  01 07 78 00 06 03 6e 73  31 c0 0f c0 0f 00 02 00   ··x···ns 1·······
0070  01 00 01 07 78 00 06 03  6e 73 32 c0 0f c0 3b 00   ····x··· ns2···;·
0080  01 00 01 00 00 00 bb 00  04 51 1f a0 22 c0 4d 00   ········ ·Q··"·M·
```

Flags (dns.flags), 2 bytes | Packets: 85 · Displayed: 6 (7.1%) · Dropped: 0 (0.0%) · Ignored: 2 (2.4%) | Profile: Default

Figure 1: DNS sequence in Wireshark

2. Again we display quary massage content more precisely.



```
(udp.dstport==53 || udp.srcport==53)
```

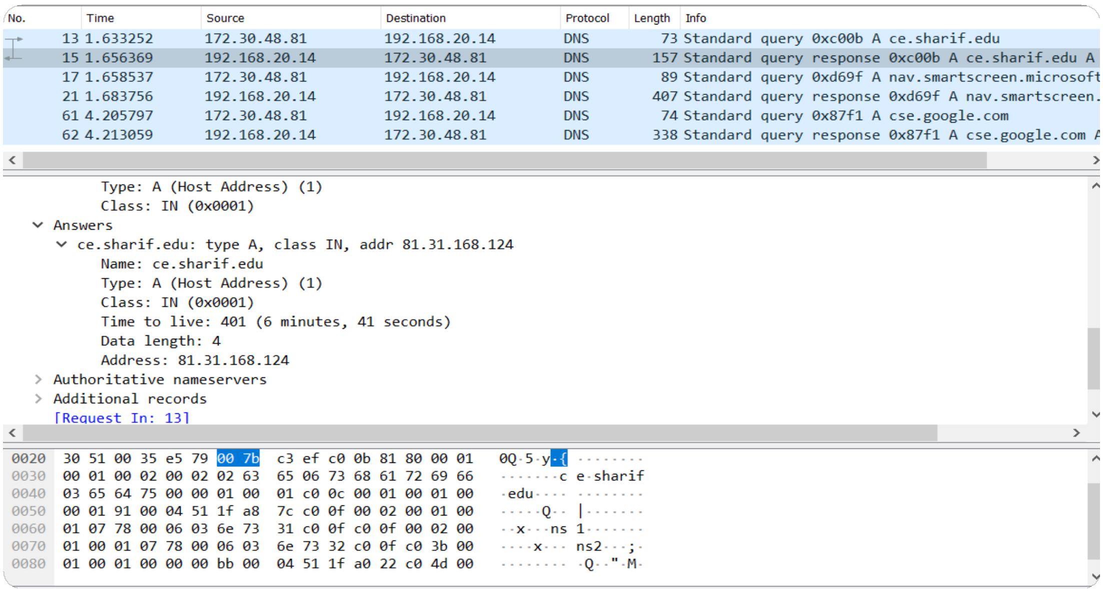
```
No.   Time      Source          Destination     Protocol  Length  Info
   13 1.633252  172.30.48.81    192.168.20.14   DNS           73  Standard query 0xc00b A ce.sharif.edu
   15 1.656369  192.168.20.14   172.30.48.81    DNS          157  Standard query response 0xc00b A ce.sharif.edu A 8
   17 1.658537  172.30.48.81    192.168.20.14   DNS           89  Standard query 0xd69f A nav.smartscreen.microsoft.
   21 1.683756  192.168.20.14   172.30.48.81    DNS          407  Standard query response 0xd69f A nav.smartscreen.r
   61 4.205797  172.30.48.81    192.168.20.14   DNS           74  Standard query 0x87f1 A cse.google.com
   62 4.213059  192.168.20.14   172.30.48.81    DNS          338  Standard query response 0x87f1 A cse.google.com A
```

```
    Authority RRs: 0
    Additional RRs: 0
  v Queries
      v ce.sharif.edu: type A, class IN
          Name: ce.sharif.edu
          [Name Length: 13]
          [Label Count: 3]
          Type: A (Host Address) (1)
          Class: IN (0x0001)
    [Response In: 15]
  [Community ID: 1:Zuo8U4VhnRwQ7B/hBwfjPpyUAuA=]
> TRANSUM RTE Data
```

Figure 2: DNS query packet

It is a type A (IPV4 translation) massage. Prefix ”A” indicates a (Hostname – IPV4) translation record and we can see it’s response is number 15 packet.

3. As we can see in figure 3, It is a type A (IPV4 translation) and it’s Class is IN (Internet Network)



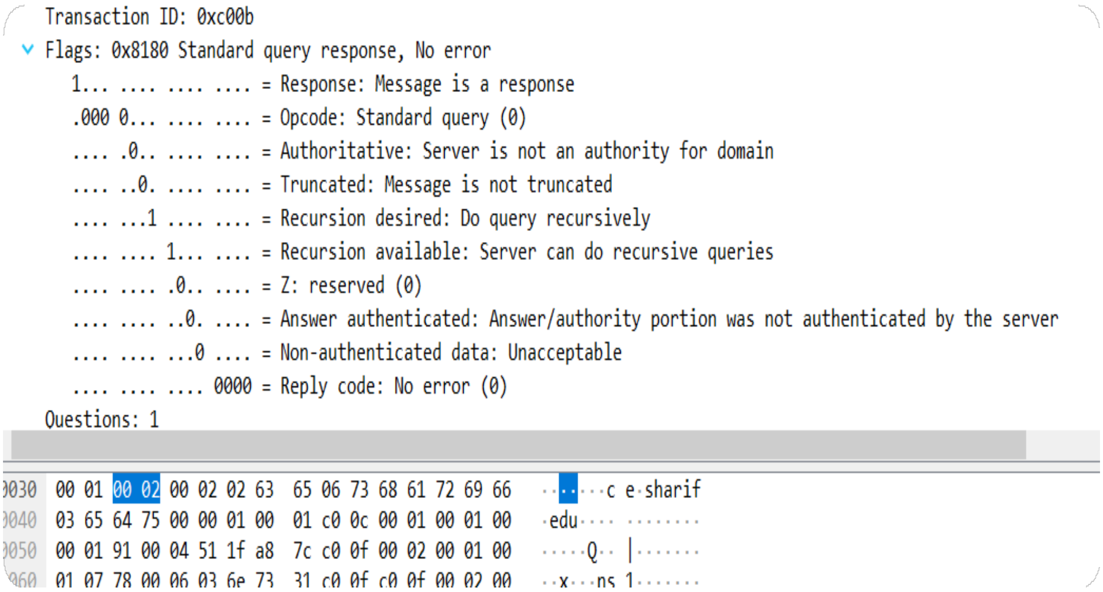
```
No.   Time       Source          Destination     Protocol  Length  Info
   13 1.633252   172.30.48.81    192.168.20.14   DNS          73   Standard query 0xc00b A ce.sharif.edu
   15 1.656369   192.168.20.14   172.30.48.81    DNS         157   Standard query response 0xc00b A ce.sharif.edu A
   17 1.658537   172.30.48.81    192.168.20.14   DNS          89   Standard query 0xd69f A nav.smartscreen.microsoft
   21 1.683756   192.168.20.14   172.30.48.81    DNS         407   Standard query response 0xd69f A nav.smartscreen.
   61 4.205797   172.30.48.81    192.168.20.14   DNS          74   Standard query 0x87f1 A cse.google.com
   62 4.213059   192.168.20.14   172.30.48.81    DNS         338   Standard query response 0x87f1 A cse.google.com A
```

```
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    ⌄ Answers
      ⌄ ce.sharif.edu: type A, class IN, addr 81.31.168.124
            Name: ce.sharif.edu
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 401 (6 minutes, 41 seconds)
            Data length: 4
            Address: 81.31.168.124
    › Authoritative nameservers
    › Additional records
      [Request In: 13]
```

```
0020  30 51 00 35 e5 79 00 7b  c3 ef c0 0b 81 80 00 01   0Q·5·y·{ ········
0030  00 01 00 02 00 02 02 63  65 06 73 68 61 72 69 66   ·······c e·sharif
0040  03 65 64 75 00 00 01 00  01 c0 0c 00 01 00 01 00   ·edu···· ········
0050  00 01 91 00 04 51 1f a8  7c c0 0f 00 02 00 01 00   ·····Q·· |·······
0060  01 07 78 00 06 03 6e 73  31 c0 0f c0 0f 00 02 00   ··x···ns 1·······
0070  01 00 01 07 78 00 06 03  6e 73 32 c0 0f c0 3b 00   ····x··· ns2···;·
0080  01 00 01 00 00 00 bb 00  04 51 1f a0 22 c0 4d 00   ········ ·Q··"·M·
```

Figure 3: response of the DNS packet

Now we look at flags in figure 4:



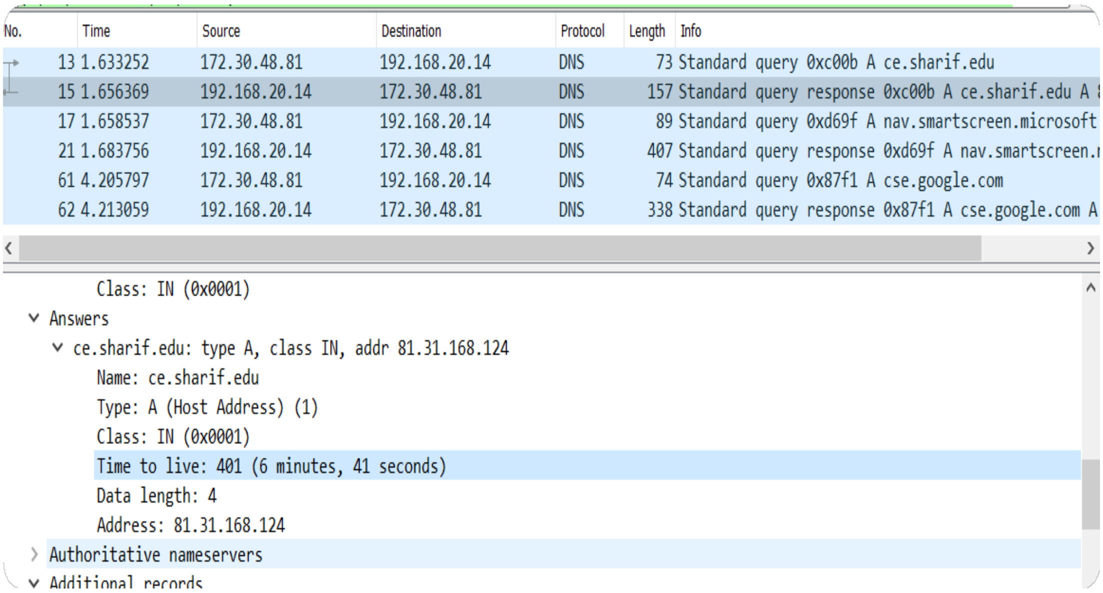
```
  Transaction ID: 0xc00b
⌄ Flags: 0x8180 Standard query response, No error
    1... .... .... .... = Response: Message is a response
    .000 0... .... .... = Opcode: Standard query (0)
    .... .0.. .... .... = Authoritative: Server is not an authority for domain
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... 1... .... = Recursion available: Server can do recursive queries
    .... .... .0.. .... = Z: reserved (0)
    .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
```

```
030  00 01 00 02 00 02 02 63  65 06 73 68 61 72 69 66   ·······c e·sharif
040  03 65 64 75 00 00 01 00  01 c0 0c 00 01 00 01 00   ·edu···· ········
050  00 01 91 00 04 51 1f a8  7c c0 0f 00 02 00 01 00   ·····Q·· |·······
060  01 07 78 00 06 03 6e 73  31 c0 0f c0 0f 00 02 00   ··x···ns 1·······
```

Figure 4: flags of DNS response

- The flag's first bit indicates that it's a response message.
- The Opcode identifies the request type: In our case it's a standard query (0).
- As we know DNS server is an Authoritative DNS for the domain and involves a copy of its domain's information. This information can be passed to the DNS server by an administrator or the upper DNS server. in this example server is not an authority for domain.
- Truncations happens when the message is longer than the standard limit issued for the Transport Layer protocol. TCP messages are length-unlimited but UDP messages have a maximum size of 512 bytes and messages longer than this size should be truncated. as we can see in figure 4 in this example message is not truncated.
- A recursive DNS lookup is where one DNS server communicates with several other DNS servers to hunt down an IP address and return it to the client. This is in contrast to an iterative DNS query, where the client communicates directly with each DNS server involved in the lookup. The Client request a Recursion Method using the "Recursion Desired bit" and the Server replies whether it supports the method by the "Recursion Available bit" or not. in this example we use recursive DNS.
- Z bit: reserved for future use
- Answer Authentication: Indicates whether the answer/authority is authenticated by the DNS server or not. in this example it is not authenticated by the server
- Data authentication is the process of confirming the origin and integrity of data. Data authentication has two elements: authenticating that you're getting data from the correct entity and validating the integrity of that data. in this example we use Non-authenticated data.
- Reply codes play a main role in troubleshooting DNS problems. In this example we have "reply code: no error" which means, DNS query successfully completed.

4. Time-to-live (TTL) is a value for the period of time that a packet, or data, should exist on a computer or network before being discarded. it prevent slow cache access and high load. After the expiration of a record's TTL, it should be discarded or refreshed.
   TTL can be found in the Answers part of a Response message.
   As we see in figure 5 TTL for this example is 401 (6 minutes, 41 seconds).



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 13 | 1.633252 | 172.30.48.81 | 192.168.20.14 | DNS | 73 | Standard query 0xc00b A ce.sharif.edu |
| 15 | 1.656369 | 192.168.20.14 | 172.30.48.81 | DNS | 157 | Standard query response 0xc00b A ce.sharif.edu A |
| 17 | 1.658537 | 172.30.48.81 | 192.168.20.14 | DNS | 89 | Standard query 0xd69f A nav.smartscreen.microsoft |
| 21 | 1.683756 | 192.168.20.14 | 172.30.48.81 | DNS | 407 | Standard query response 0xd69f A nav.smartscreen. |
| 61 | 4.205797 | 172.30.48.81 | 192.168.20.14 | DNS | 74 | Standard query 0x87f1 A cse.google.com |
| 62 | 4.213059 | 192.168.20.14 | 172.30.48.81 | DNS | 338 | Standard query response 0x87f1 A cse.google.com A |

```
        Class: IN (0x0001)
  ⌄ Answers
    ⌄ ce.sharif.edu: type A, class IN, addr 81.31.168.124
        Name: ce.sharif.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 401 (6 minutes, 41 seconds)
        Data length: 4
        Address: 81.31.168.124
  › Authoritative nameservers
  ⌄ Additional records
```

Figure 5: TTL for his example

5. These websites are actually the DNS servers placed in the path of our queries. as we know 3 types of queries are used in DNS messages:

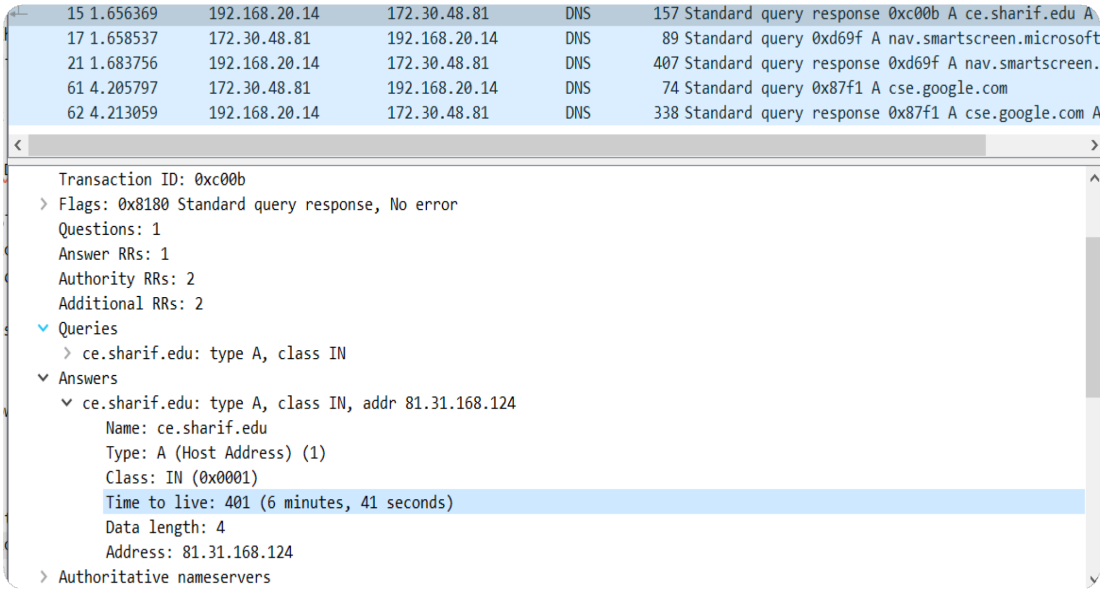
   (a) Recursive

   (b) Iterative

   (c) Non-Recursive

   In this example we use Recursive Queries. this query is initiated by the DNS resolver checking the DNS local cache for finding the corresponding IP address to the hostname the client has requested. If the pair isn't found in the local cache, The DNS resolver starts a recursive process, contacting the local DNS, TLD's Root DNS and vice versa in the destination side until it finds the Authoritative Name Server holding the corresponding IP address for the destination and returns it to the client. The procedure ends up by storing the recent accessed pair in the clients local DNS cache.
   Also if we try to access These websites, we got error.

6. As we can see in figure below we have only one answer This answers contains:



```
15 1.656369   192.168.20.14   172.30.48.81    DNS   157 Standard query response 0xc00b A ce.sharif.edu A
17 1.658537   172.30.48.81    192.168.20.14   DNS    89 Standard query 0xd69f A nav.smartscreen.microsoft
21 1.683756   192.168.20.14   172.30.48.81    DNS   407 Standard query response 0xd69f A nav.smartscreen.
61 4.205797   172.30.48.81    192.168.20.14   DNS    74 Standard query 0x87f1 A cse.google.com
62 4.213059   192.168.20.14   172.30.48.81    DNS   338 Standard query response 0x87f1 A cse.google.com A
```

```
  Transaction ID: 0xc00b
> Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 2
  Additional RRs: 2
v Queries
  > ce.sharif.edu: type A, class IN
v Answers
  v ce.sharif.edu: type A, class IN, addr 81.31.168.124
      Name: ce.sharif.edu
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 401 (6 minutes, 41 seconds)
      Data length: 4
      Address: 81.31.168.124
> Authoritative nameservers
```

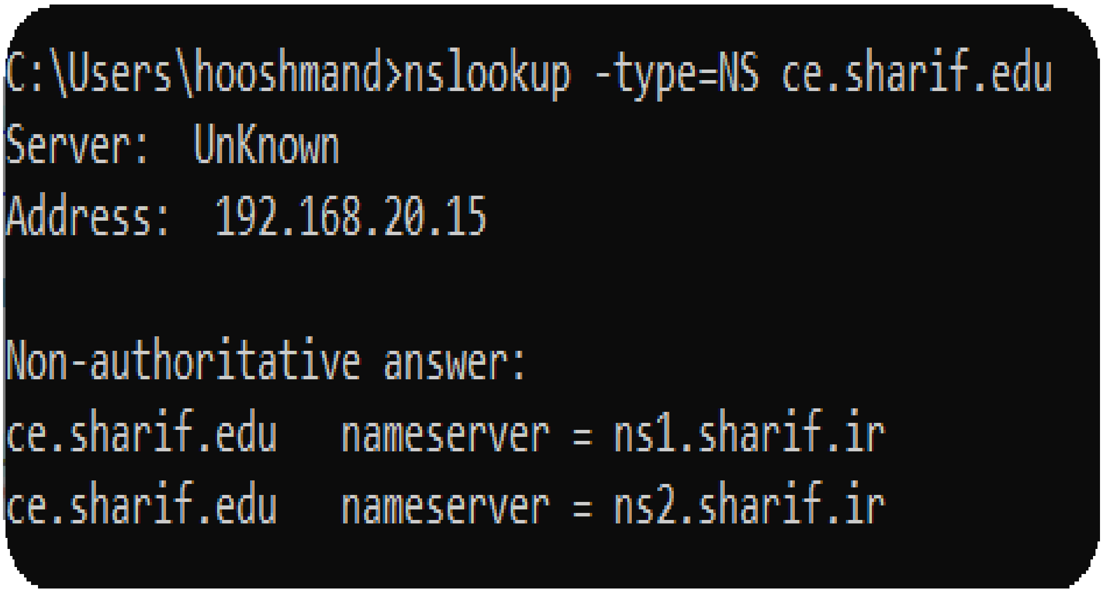
Figure 6: Answer to quary

7. *nslookup -type=NS* is used for the following cases:

   (a) Find the IP address of a host.

   (b) Find the domain name of an IP address.

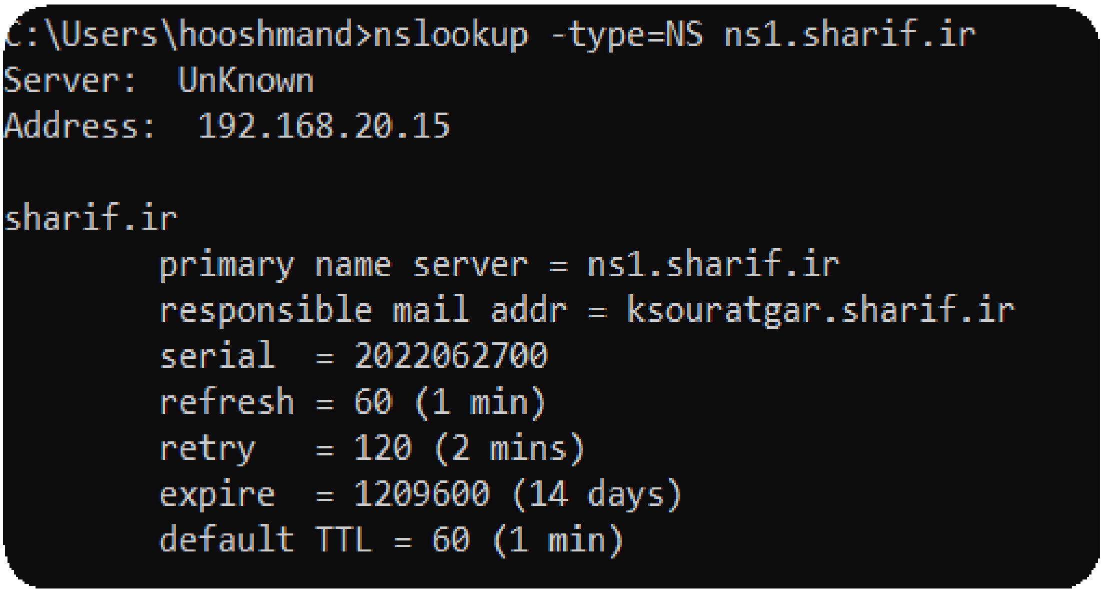
   (c) Find mail servers for a domain.



```
C:\Users\hooshmand>nslookup -type=NS ce.sharif.edu
Server:  UnKnown
Address:  192.168.20.15

Non-authoritative answer:
ce.sharif.edu   nameserver = ns1.sharif.ir
ce.sharif.edu   nameserver = ns2.sharif.ir
```

Figure 7: results of given commend for *ce.sharif.ir*

A Non-authoritative answer, shows that the resolver didn't fetch the answer from an authoritative DNS server, and got it from a cache record stored in some DNS server along the path. As we can see in figure above, we found the IP address of a domain name and we have 2 non-authoritative answer. if we try same commend for *ns1.sharif.ir* we get below result:

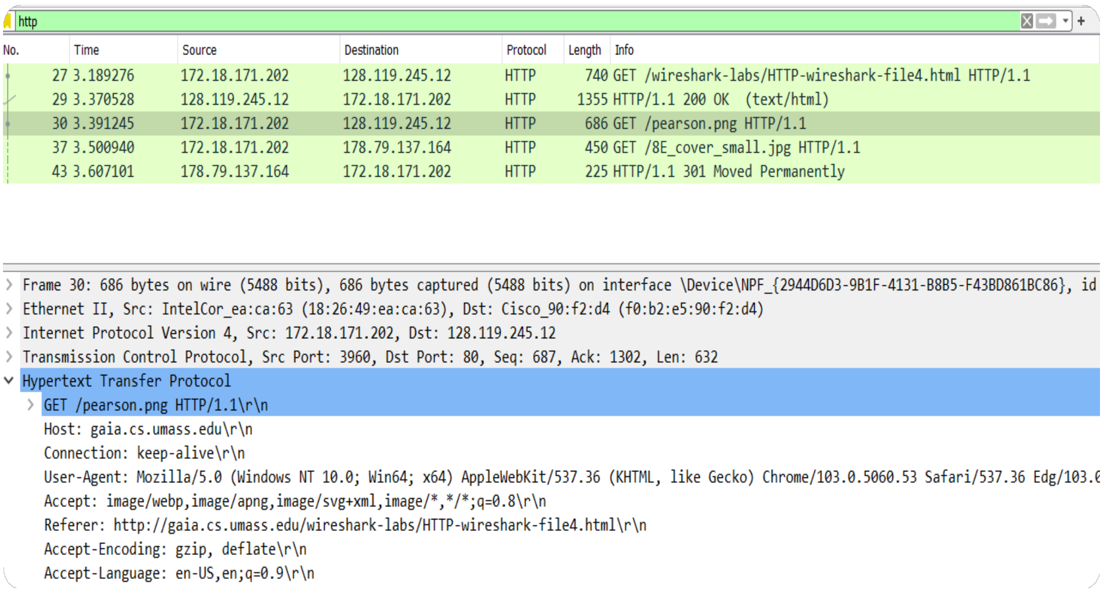


```
:\Users\hooshmand>nslookup -type=NS ns1.sharif.ir
Server:  UnKnown
Address:  192.168.20.15

sharif.ir
        primary name server = ns1.sharif.ir
        responsible mail addr = ksouratgar.sharif.ir
        serial  = 2022062700
        refresh = 60 (1 min)
        retry   = 120 (2 mins)
        expire  = 1209600 (14 days)
        default TTL = 60 (1 min)
```

Figure 8: results of given commend for *ns1.sharif.ir*

This will return the primary name server, responsible mail addresses, default ttl and more. we can see more details in figure 8.

# 2 HTTP



```
http
No.       Time        Source            Destination       Protocol  Length  Info
     27 3.189276     172.18.171.202    128.119.245.12    HTTP       740 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
     29 3.370528     128.119.245.12    172.18.171.202    HTTP      1355 HTTP/1.1 200 OK  (text/html)
     30 3.391245     172.18.171.202    128.119.245.12    HTTP       686 GET /pearson.png HTTP/1.1
     37 3.500940     172.18.171.202    178.79.137.164    HTTP       450 GET /8E_cover_small.jpg HTTP/1.1
     43 3.607101     178.79.137.164    172.18.171.202    HTTP       225 HTTP/1.1 301 Moved Permanently

> Frame 30: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits) on interface \Device\NPF_{2944D6D3-9B1F-4131-B8B5-F43BD861BC86}, id
> Ethernet II, Src: IntelCor_ea:ca:63 (18:26:49:ea:ca:63), Dst: Cisco_90:f2:d4 (f0:b2:e5:90:f2:d4)
> Internet Protocol Version 4, Src: 172.18.171.202, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 3960, Dst Port: 80, Seq: 687, Ack: 1302, Len: 632
v Hypertext Transfer Protocol
  > GET /pearson.png HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36 Edg/103.0
    Accept: image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
```

Figure 9: results of Wireshark with http filter

1. As we can see in figure above, The browser has sent 3 GET messages corresponding to the 3 data files it has accessed( html file and 2 images).

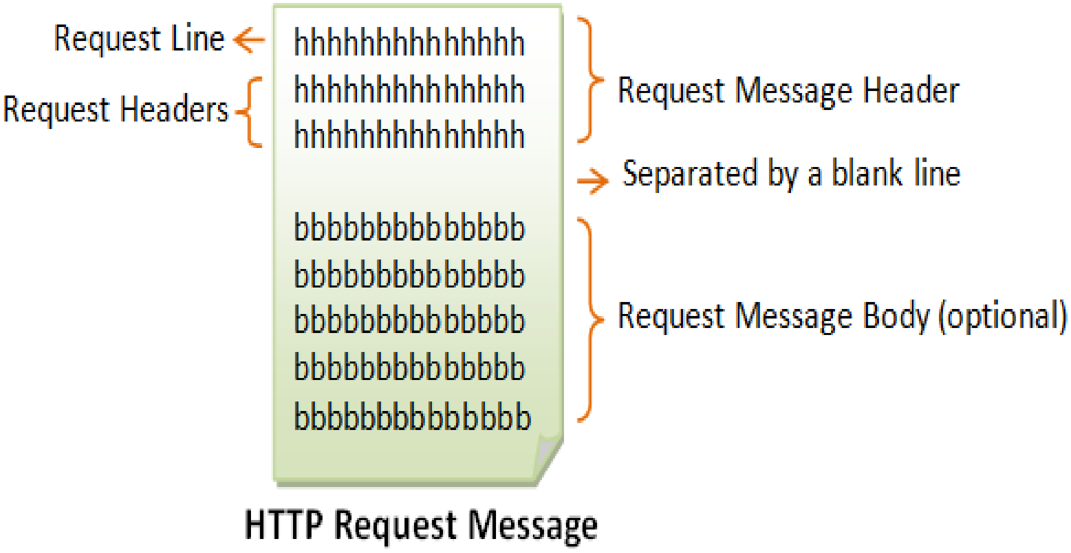


Figure 10: body of http request message

2. GET is an HTTP method for requesting data from the server. Requests using the HTTP GET method should only fetch data, cannot enclose data in the body of a GET message, and should not have any other effect on data on the server.
   In this example we have GET massages corresponding to every file in webpage.

   (a) Main HTML file

   (b) The image of our 8th edition book cover in button of page.

(c) The logo of our publisher, Pearson. in top of page.

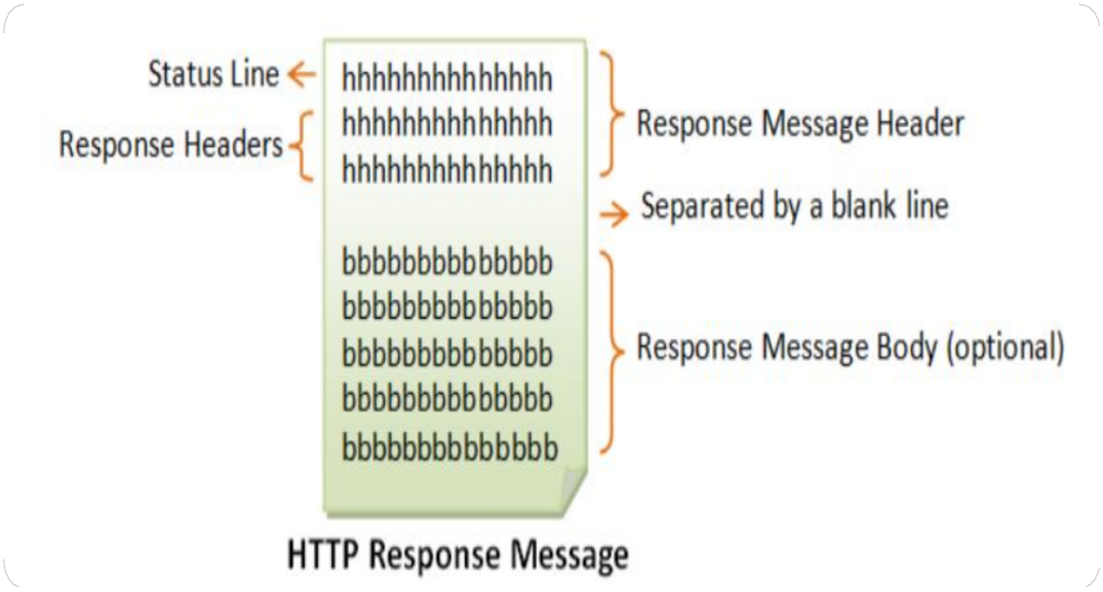
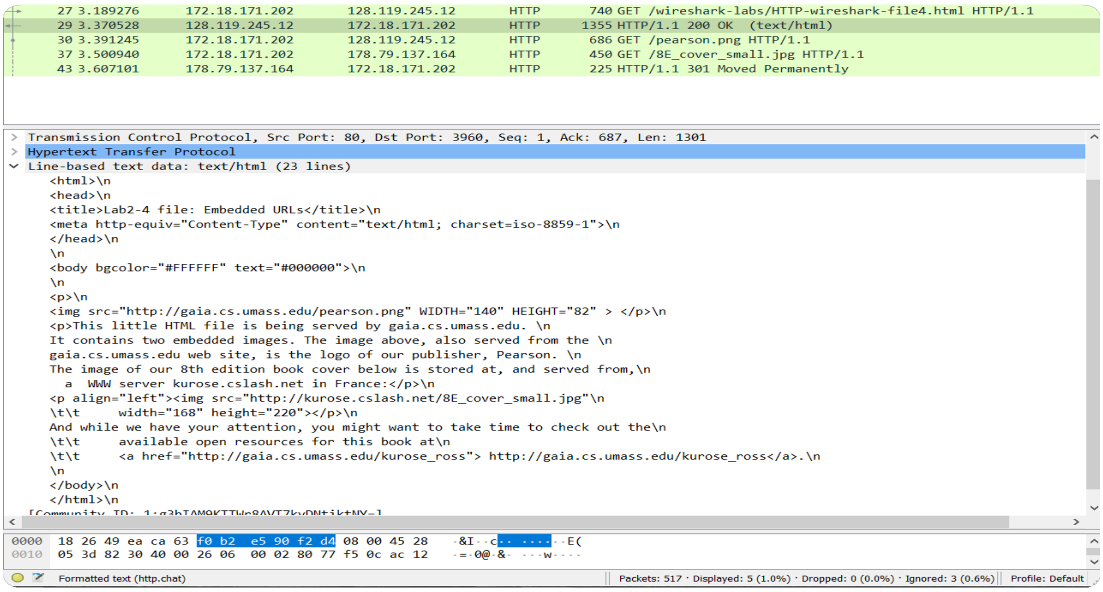


Figure 11: body of http response message

3. The response headers provide the necessary description of the document returned, such as the last modified date, the MIME type (Content-Type), and the length of the document (Content-Length). The response body contains the requested document. The browser will format and display the document according to its media type (e.g., Plain-text, HTML, JPEG, GIF, and etc.) and other information obtained from the response headers. for instance If the requested document is available, the server returns the document with a response status code ”200 OK”. In our problem we have 2 response massages shown below.

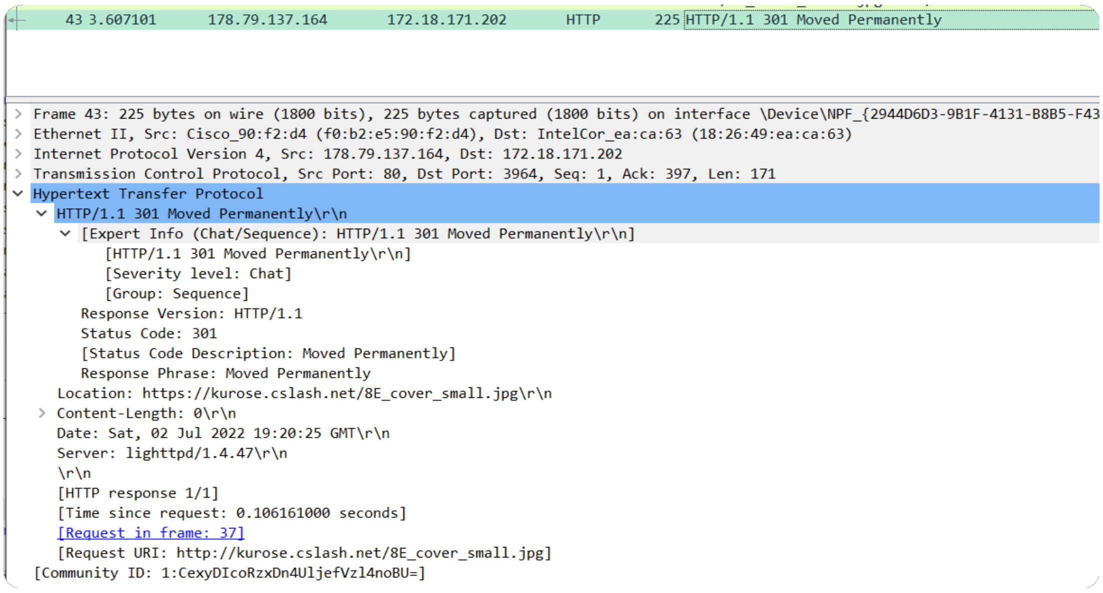
    (a) Main HTML file and links of 2 image in it. This response has status code 200, which means no problem has occurred.



```
 27 3.189276     172.18.171.202     128.119.245.12     HTTP      740 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 29 3.370528     128.119.245.12     172.18.171.202     HTTP     1355 HTTP/1.1 200 OK  (text/html)
 30 3.391245     172.18.171.202     128.119.245.12     HTTP      686 GET /pearson.png HTTP/1.1
 37 3.500940     172.18.171.202     178.79.137.164     HTTP      450 GET /8E_cover_small.jpg HTTP/1.1
 43 3.607101     178.79.137.164     172.18.171.202     HTTP      225 HTTP/1.1 301 Moved Permanently

> Transmission Control Protocol, Src Port: 80, Dst Port: 3960, Seq: 1, Ack: 687, Len: 1301
> Hypertext Transfer Protocol
v Line-based text data: text/html (23 lines)
    <html>\n
    <head>\n
    <title>Lab2-4 file: Embedded URLs</title>\n
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">\n
    </head>\n
    \n
    <body bgcolor="#FFFFFF" text="#000000">\n
    \n
    <p>\n
    <img src="http://gaia.cs.umass.edu/pearson.png" WIDTH="140" HEIGHT="82" > </p>\n
    <p>This little HTML file is being served by gaia.cs.umass.edu. \n
    It contains two embedded images. The image above, also served from the \n
    gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. \n
    The image of our 8th edition book cover below is stored at, and served from,\n
      a  WWW server kurose.cslash.net in France:</p>\n
    <p align="left"><img src="http://kurose.cslash.net/8E_cover_small.jpg"\n
    \t\t     width="168" height="220"></p>\n
    And while we have your attention, you might want to take time to check out the\n
    \t\t     available open resources for this book at\n
    \t\t     <a href="http://gaia.cs.umass.edu/kurose_ross"> http://gaia.cs.umass.edu/kurose_ross</a>.\n
    \n
    </body>\n
    </html>\n
 [Community ID: 1:g3hIAMQKTTWr8AVTZkvDNtiktNY=]

0000  18 26 49 ea ca 63 f0 b2  e5 90 f2 d4 08 00 45 28   ·&I··c·· ······E(
0010  05 3d 82 30 40 00 26 06  00 02 80 77 f5 0c ac 12   ·=·0@·&· ···w····

Formatted text (http.chat)    Packets: 517 · Displayed: 5 (1.0%) · Dropped: 0 (0.0%) · Ignored: 3 (0.6%)    Profile: Default
```

Figure 12: html file response message

    (b) The image of our 8th edition book cover in button of page. Main HTML file and links of 2 image in it. This response has status code



```
     43 3.607101        178.79.137.164        172.18.171.202        HTTP        225 HTTP/1.1 301 Moved Permanently

> Frame 43: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface \Device\NPF_{2944D6D3-9B1F-4131-B8B5-F43
> Ethernet II, Src: Cisco_90:f2:d4 (f0:b2:e5:90:f2:d4), Dst: IntelCor_ea:ca:63 (18:26:49:ea:ca:63)
> Internet Protocol Version 4, Src: 178.79.137.164, Dst: 172.18.171.202
> Transmission Control Protocol, Src Port: 80, Dst Port: 3964, Seq: 1, Ack: 397, Len: 171
v Hypertext Transfer Protocol
  v HTTP/1.1 301 Moved Permanently\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
        [HTTP/1.1 301 Moved Permanently\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 301
      [Status Code Description: Moved Permanently]
      Response Phrase: Moved Permanently
    Location: https://kurose.cslash.net/8E_cover_small.jpg\r\n
  > Content-Length: 0\r\n
    Date: Sat, 02 Jul 2022 19:20:25 GMT\r\n
    Server: lighttpd/1.4.47\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.106161000 seconds]
    [Request in frame: 37]
    [Request URI: http://kurose.cslash.net/8E_cover_small.jpg]
  [Community ID: 1:CexyDIcoRzxDn4UljefVzl4noBU=]
```

Figure 13: image response message

301, which means requested resource has been moved to the URL given by the location header.

We have no individual response for Pearson logo.