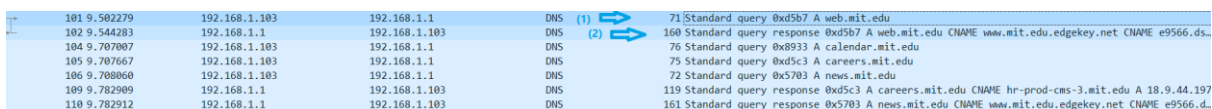


Part 1.

1. Because the DNS Resolver Cache is flushed, the IP address of the host name will be found by sending a query to DNS local server. (1) shows the query for the webpage that I chose. As shown in Figure 1 this request is sent from my computer to the DNS service source (which is my router).

In response to that query the IP address is distinguished, response is sent from the router to my computer. (2)



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|--|
| 101 | 9.502279 | 192.168.1.103 | 192.168.1.1 | DNS | 71 | Standard query 0xd5b7 A web.mit.edu |
| 102 | 9.544283 | 192.168.1.1 | 192.168.1.103 | DNS | 160 | Standard query response 0xd5b7 A web.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.ds... |
| 104 | 9.707007 | 192.168.1.103 | 192.168.1.1 | DNS | 76 | Standard query 0x8933 A calendar.mit.edu |
| 105 | 9.707667 | 192.168.1.103 | 192.168.1.1 | DNS | 75 | Standard query 0xd5c3 A careers.mit.edu |
| 106 | 9.708060 | 192.168.1.103 | 192.168.1.1 | DNS | 72 | Standard query 0x5703 A news.mit.edu |
| 109 | 9.782909 | 192.168.1.1 | 192.168.1.103 | DNS | 119 | Standard query response 0xd5c3 A careers.mit.edu CNAME hr-prod-cms-3.mit.edu A 18.9.44.197 |
| 110 | 9.782912 | 192.168.1.1 | 192.168.1.103 | DNS | 161 | Standard query response 0x5703 A news.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.d... |

Figure 1

2. In Figure 2 "Transaction ID" is the identification that it is the same as Transaction ID of response. The first parameter of "Flags" shows that this message is query and its value is 0 (the first bit). "Opcode" identifies the type of query that is standard (4 bits). 8th bit shows that recursion is desired.

Questions: the value provides the number of requests that are sent in the DNS query segment.

We can see that Answer RRs is zero because it is a query message.

In Queries we can see the content of the question, the host name (web.mit.edu) and type (A, that is IPv4) of the query and the class (IN) and as we know from Questions there is 1 request.

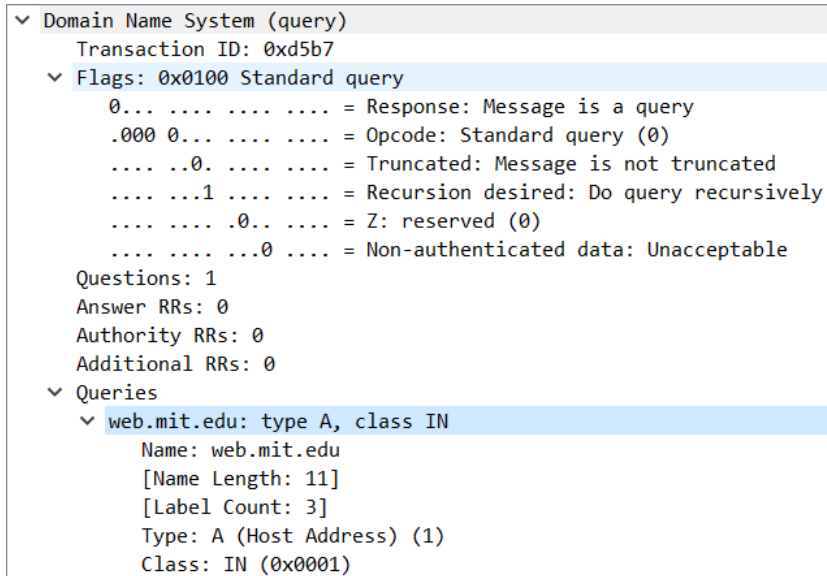


Figure 2

3. In Figure 3 we can see that "Transaction ID" is the identification that is the same as query. The first parameter of "Flags" shows that this is the response and its value is 1 (first bit). "Answer authenticated"/"Authoritative" says that the server that has responded is not the owner of the host name. Recursion is desired and available.

Answer RRs: Shows the number of responses that is 3.

Authority RRs: Shows the number of responses from authoritative servers, as we know is 0.

Answers: The first answer shows host name (web.mit.edu), type (CNAM), class (IN) and value (that is another host name (www.mit.edu.edgekey.net) that we are redirected to).

The second answer is the same as previous one.

The last one: type (A → IPv4), class (IN) and value (IP address of the host name).

```

Transaction ID: 0xd5b7
✓ 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
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
> Queries
✓ Answers
  ✓ web.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    Name: web.mit.edu
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 506 (8 minutes, 26 seconds)
    Data length: 25
    CNAME: www.mit.edu.edgekey.net
  ✓ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    Name: www.mit.edu.edgekey.net
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 221 (3 minutes, 41 seconds)
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  ✓ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.66.82.6
    Name: e9566.dscb.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 221 (3 minutes, 41 seconds) 4
    Data length: 4
    Address: 104.66.82.6

```

Figure 3

4. Every time that we ask a server the IP of a host name, the mapping is saved in a cache for a time (TTL) during this time we do not need to contact the server. Time to live indicates how stable the entry is in terms of seconds (needed for caching). After that time in order to load that host name we have to contact the server to find the IP address. It is found in reply packet and in this case is shown in Figure 3 and we can see that every answer has its own TTL.

5. These DNS queries are for links of the websites in this page, for example at the bottom of the page there are links for Instagram, twitter, Facebook and YouTube. And some other MIT related websites that has link in this webpage.

| | | | | |
|--------------|---------------|-------------|-----|--|
| 111 9.784772 | 192.168.1.103 | 192.168.1.1 | DNS | 73 Standard query 0xc20c A space.mit.edu |
| 112 0.784772 | 192.168.1.103 | 192.168.1.1 | DNS | 82 Standard query 0xc20c A space.mit.edu |

Figure 4

| | | | | |
|---------------|---------------|---------------|-----|--|
| 152 10.653018 | 192.168.1.103 | 192.168.1.1 | DNS | 77 Standard query 0x0a9d A www.instagram.com |
| 154 10.655540 | 192.168.1.1 | 192.168.1.103 | DNS | 92 Standard query response 0x5f2c A www.facebook.com A 10.10.34.35 |
| 158 10.658140 | 192.168.1.103 | 192.168.1.1 | DNS | 75 Standard query 0x665e A www.youtube.com |
| 159 10.658904 | 192.168.1.103 | 192.168.1.1 | DNS | 83 Standard query 0x6686 A stats.g.doubleclick.net |
| 160 10.704290 | 192.168.1.1 | 192.168.1.103 | DNS | 90 Standard query response 0x0485 A www.google.com A 172.217.169.228 |
| 161 10.707041 | 192.168.1.1 | 192.168.1.103 | DNS | 137 Standard query response 0x0a9d A www.instagram.com CNAME z-p42-instagram.c10r.facebook.co... |

Figure 5

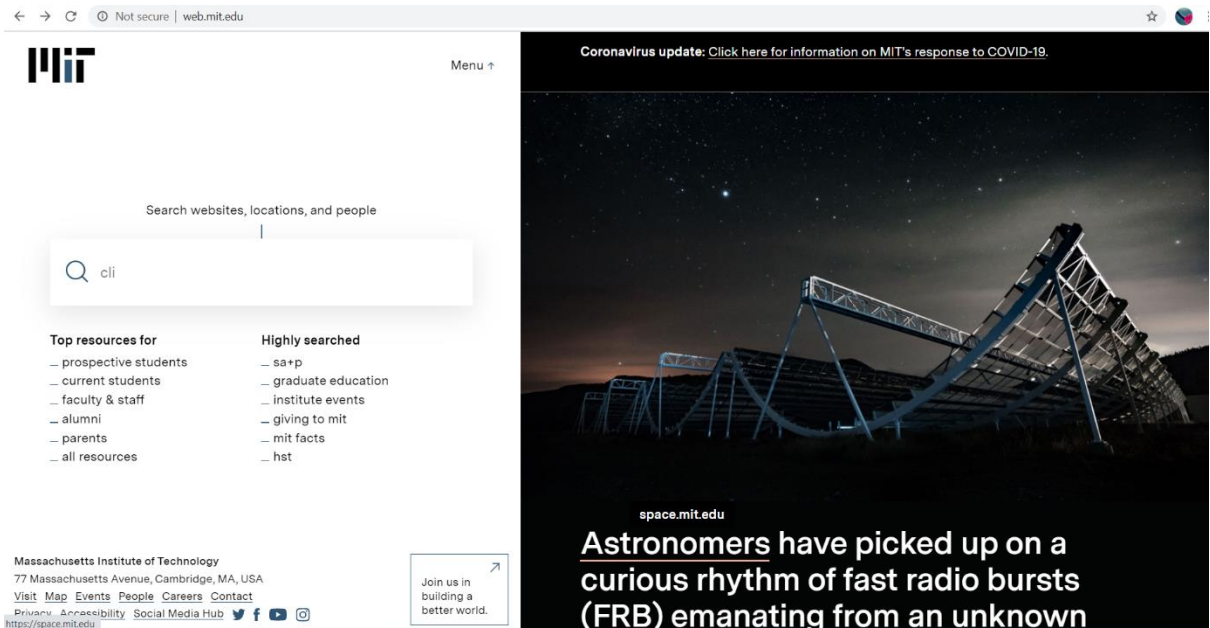


Figure 6

Figure 4 and 5 show the DNS queries for some links and in Figure 6 we can see the webpage that is opened.

There is a query for "google-analytics.com." Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. In Figure 7 we can see the contents of the packet.

```

Domain Name System (query)
Transaction ID: 0x0b0a
Flags: 0x0100 Standard query
 0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
... ..0. .... = Truncated: Message is not truncated
... ..1 .... = Recursion desired: Do query recursively
... ..0... .. = Z: reserved (0)
... ..0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  www.google-analytics.com: type A, class IN
    Name: www.google-analytics.com
    [Name Length: 24]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)

```

Figure 7

6. I chose a random DNS response packet because it wasn't mentioned in the question.

As we can see in the figure below this packet contains 2 answers. The first one redirect to another DNS and the second one contains the IP address.

```

▼ Domain Name System (response)
  Transaction ID: 0x8933
  ▼ 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
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    > calendar.mit.edu: type A, class IN
  ▼ Answers
    ▼ calendar.mit.edu: type CNAME, class IN, cname mit.enterprise.localist.com
      Name: calendar.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 508 (8 minutes, 28 seconds)
      Data length: 29
      CNAME: mit.enterprise.localist.com
    ▼ mit.enterprise.localist.com: type A, class IN, addr 13.92.255.122
      Name: mit.enterprise.localist.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 77 (1 minute, 17 seconds)
      Data length: 4
      Address: 13.92.255.122

```

7. The first two lines of output specify the server to which the request was directed. This server is the default server that my system uses for DNS name resolution.

Non-authoritative answer means that this answer came from the cache of some server rather than from an authoritative MIT DNS server that has the source files.

```
C:\WINDOWS\system32>nslookup -type=NS mit.edu
Server:    UnKnown
Address:   192.168.1.1

Non-authoritative answer:
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia1.akam.net
```

Figure 8

Part2.

1. 4 requests

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--|
| 50 | 9.903877 | 192.168.1.103 | 128.119.245.12 | HTTP | 534 | GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| 65 | 10.307646 | 128.119.245.12 | 192.168.1.103 | HTTP | 1102 | HTTP/1.1 200 OK (text/html) |
| 66 | 10.323830 | 192.168.1.103 | 128.119.245.12 | HTTP | 466 | GET /pearson.png HTTP/1.1 |
| 73 | 10.407377 | 192.168.1.103 | 128.119.245.12 | HTTP | 480 | GET /~kurose/cover_5th_ed.jpg HTTP/1.1 |
| 86 | 10.719325 | 128.119.245.12 | 192.168.1.103 | HTTP | 841 | HTTP/1.1 200 OK (PNG) |
| 196 | 11.114337 | 128.119.245.12 | 192.168.1.103 | HTTP | 1027 | HTTP/1.1 200 OK (JPEG JFIF image) |
| 197 | 11.131134 | 192.168.1.103 | 128.119.245.12 | HTTP | 466 | GET /favicon.ico HTTP/1.1 |
| 201 | 11.521673 | 128.119.245.12 | 192.168.1.103 | HTTP | 263 | HTTP/1.1 404 Not Found (text/html) |

Figure 9

2. The first Get request is to get an html file (Figure 10), the second one is for getting a png image (the upper image in page) (Figure 11), the third one is to get a jpg image (the one that is the cover of a book) (Figure 12) and the last one is for getting an ico image (Figure 13)!

```
▼ 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 (Windows NT 10.0; Win64; x64) AppleWebKit/
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,imag
    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-wi
    [HTTP request 1/3]
```

Figure 10

```
▼ 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
    Accept: image/webp,image/apng,image/*,
    Referer: http://gaia.cs.umass.edu/wire
    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
    [HTTP request 2/3]
```

Figure 11

▼ Hypertext Transfer Protocol

> GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n ←

Host: manic.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/69.0.3496.102 Safari/537.36\r\n

Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n

Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark.html\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9\r\n

\r\n

[Full request URI: http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg]

[HTTP request 1/1]

Figure 12

▼ Hypertext Transfer Protocol

> GET /favicon.ico 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/69.0.3496.102 Safari/537.36\r\n

Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n

Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark.html\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/favicon.ico>]

[HTTP request 3/3]

Figure 13

In all of request in the first line we can see the method that is Get and then we see path name (object). In the next line we have host name and because http 1.1 (persistent) is used so Connection is keep-alive.

3. In Figure 14 we can see the Get response of the first request.

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Last-Modified: Tue, 16 Jun 2020 05:59:04 GMT\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 714\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Date: Tue, 16 Jun 2020 14:59:18 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.7 mod_perl/2.0.11 Perl/v5.16.3\r\n
    ETag: "2ca-5a82d3d9b4de9"\r\n
    Age: 0\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/3]
    [Time since request: 0.403769000 seconds]
    [Request in frame: 50]
    [Next request in frame: 66]
    [Next response in frame: 86]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 714 bytes
  > Line-based text data: text/html (17 lines)
```




Figure 14

```
▼ Line-based text data: text/html (17 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
   </p>\n
  <p>This little HTML file is being served by gaia.cs.umass.edu. \n
  It contains two embedded images. <br> The image above, also served from the \n
  gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. <br>\n
  The image of our 5th edition book cover below is stored at, and served from, the www server caite.cs.umass.edu:</p>\n
  <p align="left"></p>\n
  </body>\n
  </html>\n
```

Figure 15

Since the type of the object in this message is html, we can see the data in Figure 15 that is html code of the page.

In Figure 16 we can see response of the second Get request.

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Last-Modified: Sat, 06 Aug 2016 10:08:14 GMT\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 3267\r\n
    Content-Type: image/png\r\n
    Date: Tue, 16 Jun 2020 14:59:19 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.7 mod_perl/2.0.11 Perl/v5.16.3\r\n
    ETag: "cc3-539645c7f1ee7"\r\n
    Age: 0\r\n
    Connection: keep-alive\r\n
  \r\n
  [HTTP response 2/3]
  [Time since request: 0.395495000 seconds]
  [Prev request in frame: 50]
  [Prev response in frame: 65]
  [Request in frame: 66]
  [Next request in frame: 197]
  [Next response in frame: 201]
  [Request URI: http://gaia.cs.umass.edu/favicon.ico]
  File Data: 3267 bytes
> Portable Network Graphics
```

Figure 16

```
▼ Portable Network Graphics
  PNG Signature: 89504e470d0a1a0a
  > Image Header (IHDR)
  > Palette (PLTE)
  > Image data chunk (IDAT)
  > Image Trailer (IEND)
```

Figure 17

As we know the object of this message is png and we can see the content in Figure 17.

In Figure 18 we can see response of the third Get request and we can see that the format of the object is JPEG.

```

▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Last-Modified: Tue, 15 Sep 2009 18:23:27 GMT\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 100968\r\n
    Content-Type: image/jpeg\r\n
    Date: Tue, 16 Jun 2020 14:59:19 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.7 mod_perl/2.0.11 Perl/v5.16.3\r\n
    ETag: "18a68-473a1e0e6e5c0"\r\n
    Age: 0\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.706960000 seconds]
    \[Request in frame: 73\]
    [Request URI: http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg]
    File Data: 100968 bytes
  > JPEG File Interchange Format

```

Figure 18

```

▼ Hypertext Transfer Protocol
  > HTTP/1.1 404 Not Found\r\n
    Date: Tue, 16 Jun 2020 14:59:20 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.7 mod_perl/2.0.11 Perl/v5.16.3\r\n
  > Content-Length: 209\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    Connection: close\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.390539000 seconds]
    \[Prev request in frame: 66\]
    \[Prev response in frame: 86\]
    \[Request in frame: 197\]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 209 bytes
▼ Line-based text data: text/html (7 lines)
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <html><head>\n
  <title>404 Not Found</title>\n
  </head><body>\n
  <h1>Not Found</h1>\n
  <p>The requested URL /favicon.ico was not found on this server.</p>\n
  </body></html>\n

```

Figure 19

Figure 19 shows the response of the last Get request. We can see that the status code of this response is "Not found" and it means that the requested document was not on the server and connection is closed. But in previous responses status was "ok" and connection was keep-alive.

Date shows the time that server has respond to the request. And Server indicates the sever that respond.

We can also find the format of the object from connection-type in response massages.