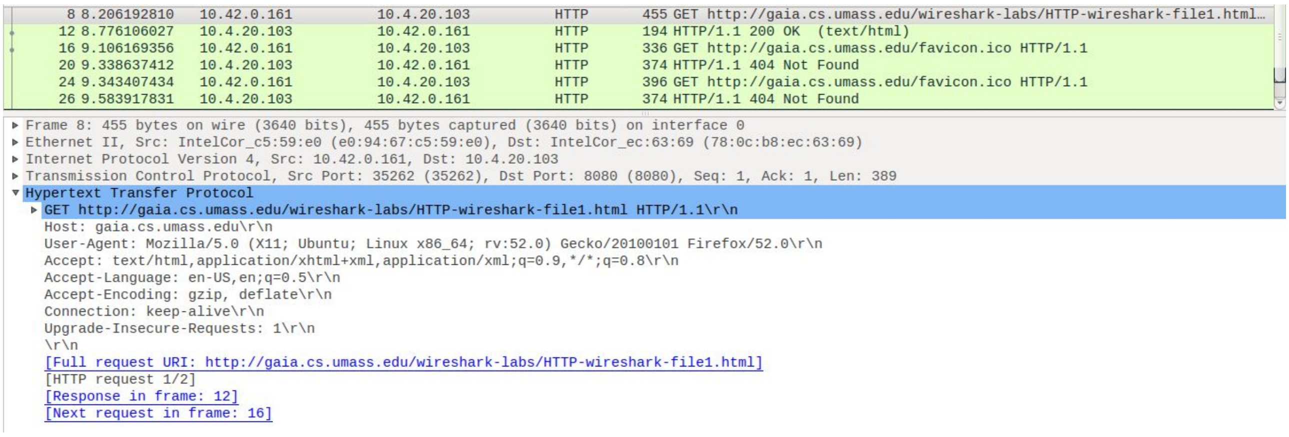
Computer networks Assgn -2

Nikhil Rayaprolu
201501090
CSE

PART-1: WIRESHARK HTTP

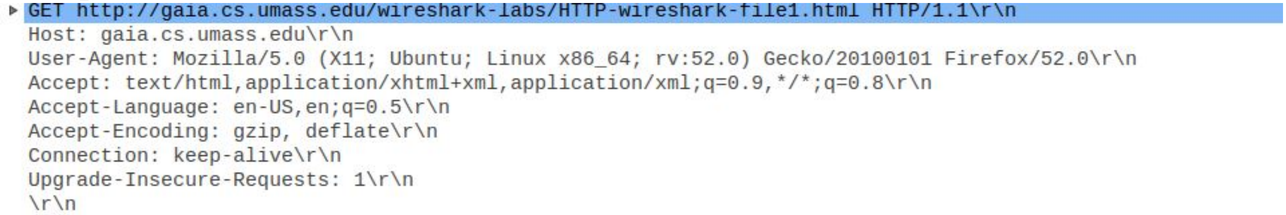
A. THE BASIC HTTP GET/Response interaction



```
  8 8.206192810   10.42.0.161       10.4.20.103       HTTP     455 GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html…
 12 8.776106027   10.4.20.103       10.42.0.161       HTTP     194 HTTP/1.1 200 OK  (text/html)
 16 9.106169356   10.42.0.161       10.4.20.103       HTTP     336 GET http://gaia.cs.umass.edu/favicon.ico HTTP/1.1
 20 9.338637412   10.4.20.103       10.42.0.161       HTTP     374 HTTP/1.1 404 Not Found
 24 9.343407434   10.42.0.161       10.4.20.103       HTTP     396 GET http://gaia.cs.umass.edu/favicon.ico HTTP/1.1
 26 9.583917831   10.4.20.103       10.42.0.161       HTTP     374 HTTP/1.1 404 Not Found
```

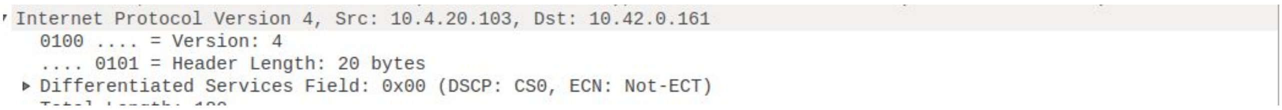
```
▸ Frame 8: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface 0
▸ Ethernet II, Src: IntelCor_c5:59:e0 (e0:94:67:c5:59:e0), Dst: IntelCor_ec:63:69 (78:0c:b8:ec:63:69)
▸ Internet Protocol Version 4, Src: 10.42.0.161, Dst: 10.4.20.103
▸ Transmission Control Protocol, Src Port: 35262 (35262), Dst Port: 8080 (8080), Seq: 1, Ack: 1, Len: 389
▾ Hypertext Transfer Protocol
  ▸ GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 12]
    [Next request in frame: 16]
```

1)My browser is running HTTP vesion 1.1 . The server is also running HTTP version 1.1 . The languages that browser indicates so that it can accept the server are en-US,en.



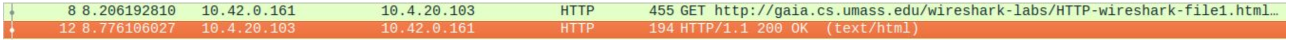
```
▸ GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
```

2)The IP address of my computer is 10.42.0.161 . The IP address of the gaia.cs.umass.edu server is unknown here, since I am inside a proxy network and the address of the proxy I used is 10.4.20.103.



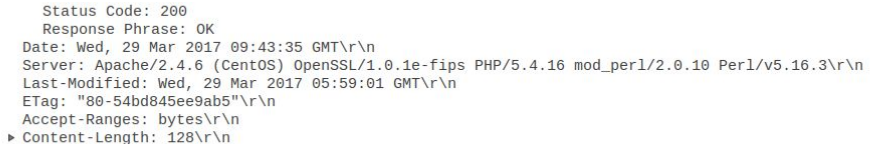
```
▾ Internet Protocol Version 4, Src: 10.4.20.103, Dst: 10.42.0.161
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
```

3)The status code returned from the server to my browser is 200 .



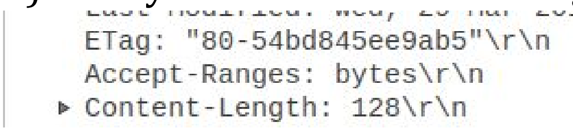
```
  8 8.206192810   10.42.0.161       10.4.20.103       HTTP     455 GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html…
 12 8.776106027   10.4.20.103       10.42.0.161       HTTP     194 HTTP/1.1 200 OK  (text/html)
```

4)4)The HTML file that i am retrieving is last modified at the server at Wed, 29 Mar 2017 05:59:01 GMT.



```
  Status Code: 200
  Response Phrase: OK
Date: Wed, 29 Mar 2017 09:43:35 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Last-Modified: Wed, 29 Mar 2017 05:59:01 GMT\r\n
ETag: "80-54bd845ee9ab5"\r\n
Accept-Ranges: bytes\r\n
▸ Content-Length: 128\r\n
```

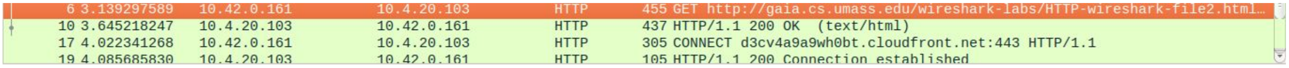
5)128 bytes of content are being returned to my browser.



```
  ETag: "80-54bd845ee9ab5"\r\n
  Accept-Ranges: bytes\r\n
▸ Content-Length: 128\r\n
```

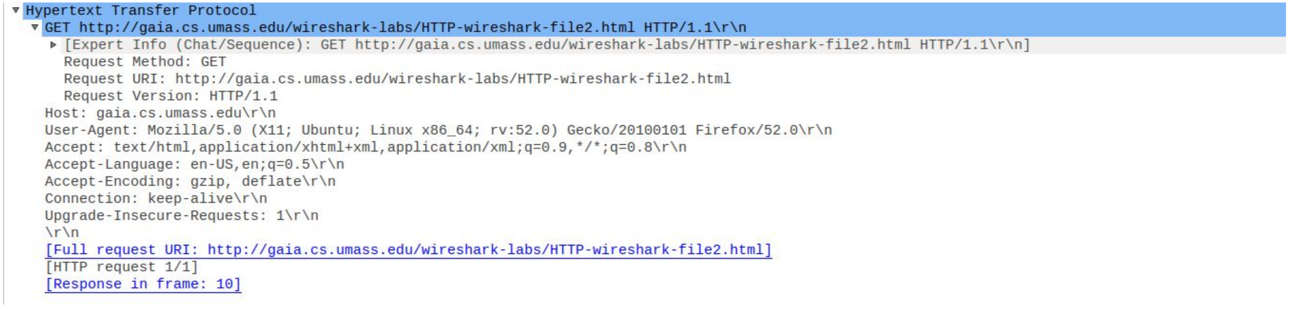
6)No, I dont see any in the HTTP message below.

B. THE HTTP CONDITIONAL GET/response interaction



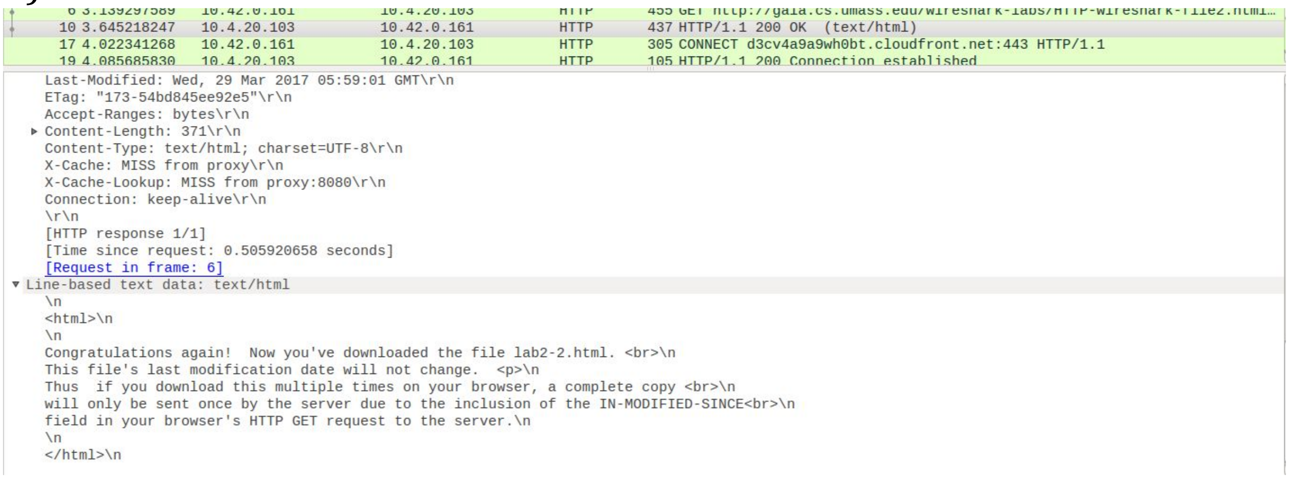
```
    6 3.139297589   10.42.0.161     10.4.20.103     HTTP    455 GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html…
   10 3.645218247   10.4.20.103     10.42.0.161     HTTP    437 HTTP/1.1 200 OK  (text/html)
   17 4.022341268   10.42.0.161     10.4.20.103     HTTP    305 CONNECT d3cv4a9a9wh0bt.cloudfront.net:443 HTTP/1.1
   19 4.085685830   10.4.20.103     10.42.0.161     HTTP    105 HTTP/1.1 200 Connection established
```

7)There is no IF-MODIFIED-SINCE in the first GET.



```
▾ Hypertext Transfer Protocol
  ▾ GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\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: 10]
```

8)Yes the server returned the contents of the file

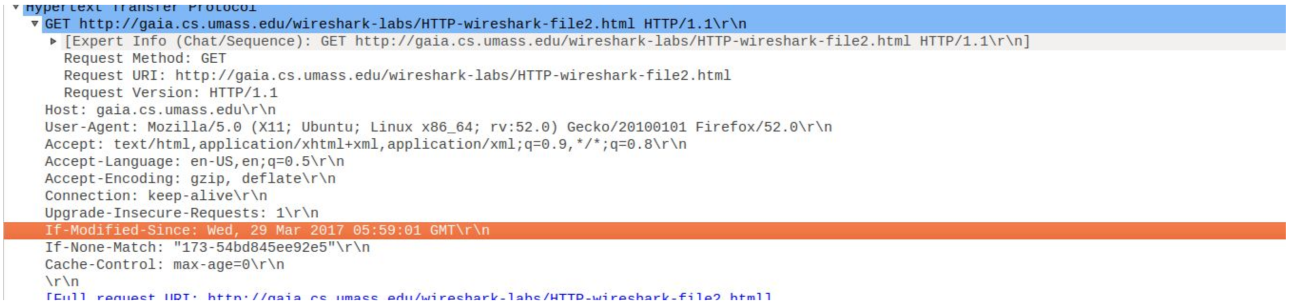


```
    6 3.139297589   10.42.0.161     10.4.20.103     HTTP    455 GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html…
   10 3.645218247   10.4.20.103     10.42.0.161     HTTP    437 HTTP/1.1 200 OK  (text/html)
   17 4.022341268   10.42.0.161     10.4.20.103     HTTP    305 CONNECT d3cv4a9a9wh0bt.cloudfront.net:443 HTTP/1.1
   19 4.085685830   10.4.20.103     10.42.0.161     HTTP    105 HTTP/1.1 200 Connection established

    Last-Modified: Wed, 29 Mar 2017 05:59:01 GMT\r\n
    ETag: "173-54bd845ee92e5"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 371\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    X-Cache: MISS from proxy\r\n
    X-Cache-Lookup: MISS from proxy:8080\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.505920658 seconds]
    [Request in frame: 6]
▾ Line-based text data: text/html
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

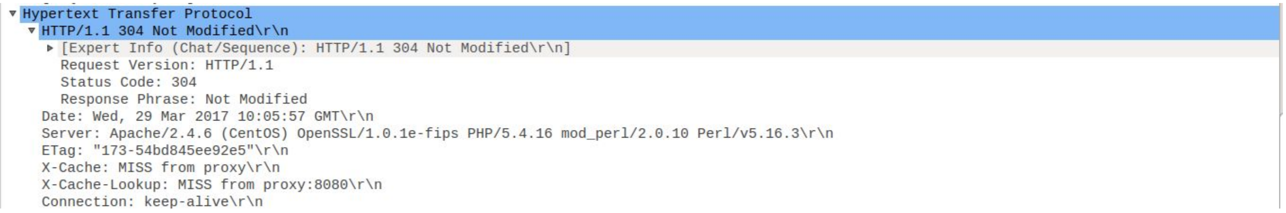
9)Yes we can see an “IF_MODIFIED_SINCE:” in the second HTTP GET. The information that follows IF_MODIFIED-SINCE header is

Wed, 29 Mar 2017 05:59:01 GMT i.e the browser is asking the server whether the file it has had been modified since that time.



```
▾ Hypertext Transfer Protocol
  ▾ GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Wed, 29 Mar 2017 05:59:01 GMT\r\n
    If-None-Match: "173-54bd845ee92e5"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

10)The file has not been modified.So the contents of the file is not returned in the HTTP message. The HTTP status code returned is 304 and the phrase returned is Not Modified.

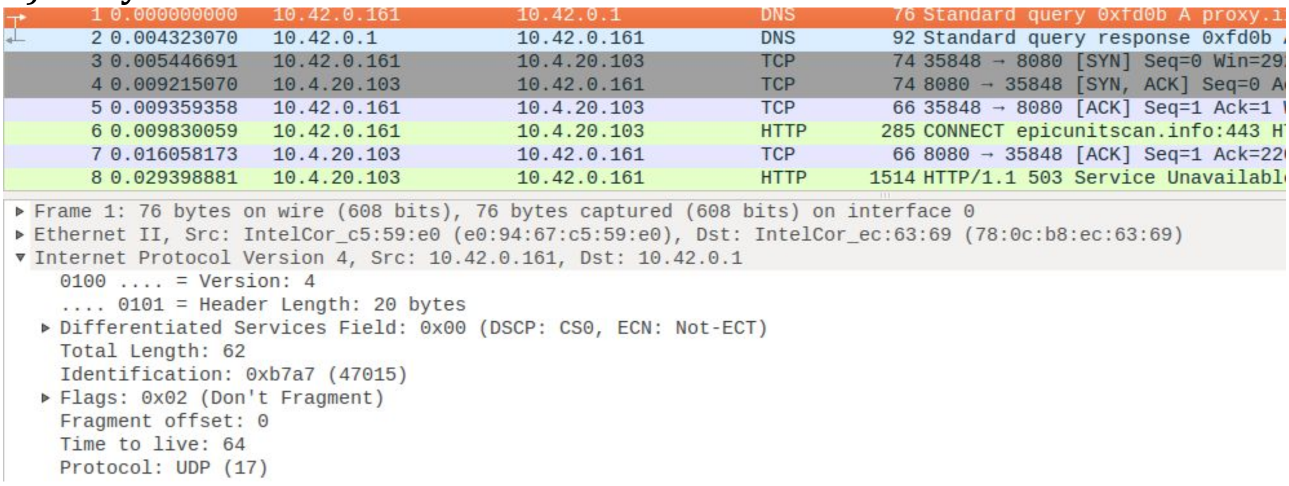


```
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 304 Not Modified\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Request Version: HTTP/1.1
      Status Code: 304
      Response Phrase: Not Modified
    Date: Wed, 29 Mar 2017 10:05:57 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    ETag: "173-54bd845ee92e5"\r\n
    X-Cache: MISS from proxy\r\n
    X-Cache-Lookup: MISS from proxy:8080\r\n
    Connection: keep-alive\r\n
```

PART 2: WIRESHARK DNS

A.Tracing DNS with Wireshark

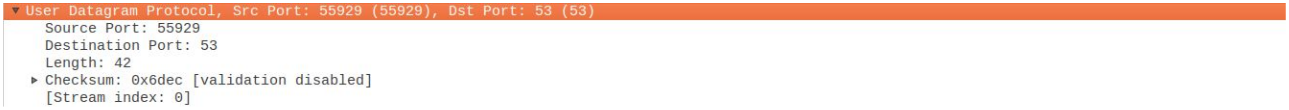
1) They are sent over UDP.



```
      1 0.000000000   10.42.0.161     10.42.0.1       DNS      76 Standard query 0xfd0b A proxy.i
      2 0.004323070   10.42.0.1       10.42.0.161     DNS      92 Standard query response 0xfd0b
      3 0.005446691   10.42.0.161     10.4.20.103     TCP      74 35848 → 8080 [SYN] Seq=0 Win=29
      4 0.009215070   10.4.20.103     10.42.0.161     TCP      74 8080 → 35848 [SYN, ACK] Seq=0 A
      5 0.009359358   10.42.0.161     10.4.20.103     TCP      66 35848 → 8080 [ACK] Seq=1 Ack=1
      6 0.009830059   10.42.0.161     10.4.20.103     HTTP    285 CONNECT epicunitscan.info:443 H
      7 0.016058173   10.4.20.103     10.42.0.161     TCP      66 8080 → 35848 [ACK] Seq=1 Ack=22
      8 0.029398881   10.4.20.103     10.42.0.161     HTTP   1514 HTTP/1.1 503 Service Unavailabl

▸ Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
▸ Ethernet II, Src: IntelCor_c5:59:e0 (e0:94:67:c5:59:e0), Dst: IntelCor_ec:63:69 (78:0c:b8:ec:63:69)
▾ Internet Protocol Version 4, Src: 10.42.0.161, Dst: 10.42.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 62
    Identification: 0xb7a7 (47015)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
```

2)The destination port for DNS query message is 53.

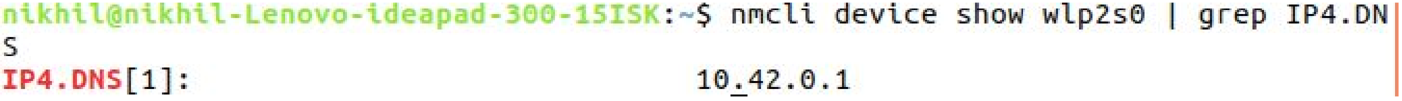


```
▾ User Datagram Protocol, Src Port: 55929 (55929), Dst Port: 53 (53)
    Source Port: 55929
    Destination Port: 53
    Length: 42
  ▸ Checksum: 0x6dec [validation disabled]
    [Stream index: 0]
```

The source port of DNS response message is 53.

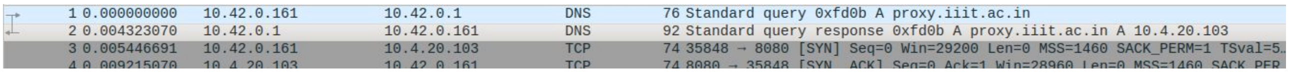
3)Yes the two IP addresses are same.

Command to check local DNS addresses in Linux is
nmcli device show wlp2s0 | grep IP4.DNS



```
nikhil@nikhil-Lenovo-ideapad-300-15ISK:~$ nmcli device show wlp2s0 | grep IP4.DN
S
IP4.DNS[1]:                             10.42.0.1
```

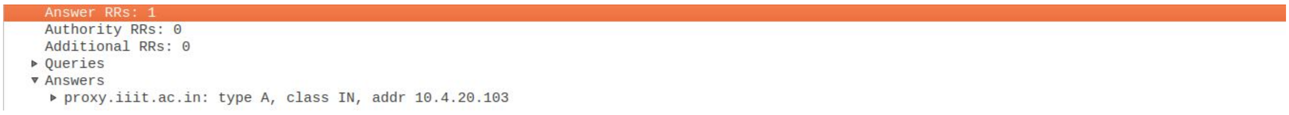
and the destination for the DNS servers in wireshark is 10.42.0.1



```
1 0.000000000   10.42.0.161    10.42.0.1      DNS    76 Standard query 0xfd0b A proxy.iiit.ac.in
2 0.004323070   10.42.0.1      10.42.0.161    DNS    92 Standard query response 0xfd0b A proxy.iiit.ac.in A 10.4.20.103
3 0.005446691   10.42.0.161    10.4.20.103    TCP    74 35848 → 8080 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=5…
4 0.009215070   10.4.20.103    10.42.0.161    TCP    74 8080 → 35848 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PER
```

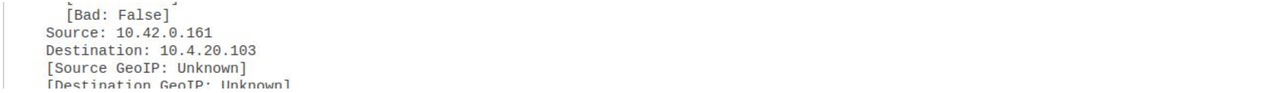
4)1 answer is given.

The answer contains proxy.iiit.ac.in: type A, class IN , addr 10.4.20.103



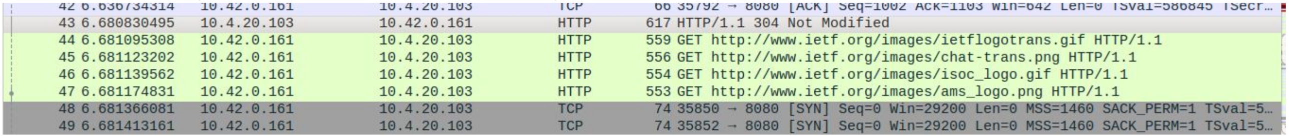
```
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
  ▾ Answers
    ▸ proxy.iiit.ac.in: type A, class IN, addr 10.4.20.103
```

5)Yes it corresponds to the answer given by the DNS response message



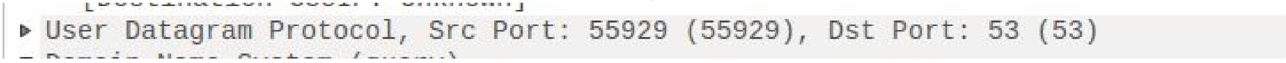
```
    [Bad: False]
    Source: 10.42.0.161
    Destination: 10.4.20.103
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

6)No , it doesn’t issue any new DNS messages. It uses the answers returned by the first DNS query.



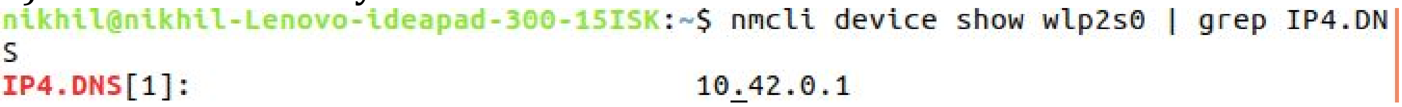
```
42 6.636734314  10.42.0.161    10.4.20.103    TCP     66 35792 → 8080 [ACK] Seq=1002 Ack=1103 Win=642 Len=0 TSval=586845 TSecr…
43 6.680830495  10.4.20.103    10.42.0.161    HTTP   617 HTTP/1.1 304 Not Modified
44 6.681095308  10.42.0.161    10.4.20.103    HTTP   559 GET http://www.ietf.org/images/ietflogotrans.gif HTTP/1.1
45 6.681123202  10.42.0.161    10.4.20.103    HTTP   556 GET http://www.ietf.org/images/chat-trans.png HTTP/1.1
46 6.681139562  10.42.0.161    10.4.20.103    HTTP   554 GET http://www.ietf.org/images/isoc_logo.gif HTTP/1.1
47 6.681174831  10.42.0.161    10.4.20.103    HTTP   553 GET http://www.ietf.org/images/ams_logo.png HTTP/1.1
48 6.681366081  10.42.0.161    10.4.20.103    TCP     74 35850 → 8080 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=5…
49 6.681413161  10.42.0.161    10.4.20.103    TCP     74 35852 → 8080 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=5…
```

7)the destination port for the DNS query message and source port of DNS response message are same that is 53



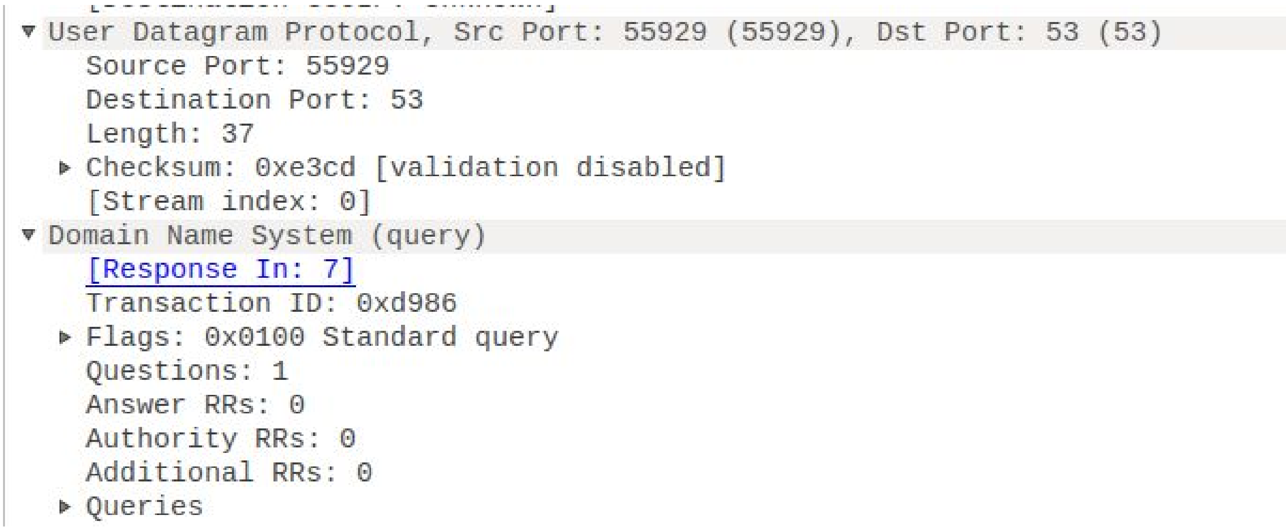
```
▸ User Datagram Protocol, Src Port: 55929 (55929), Dst Port: 53 (53)
```

8)Yes it is sent to my local DNS server.



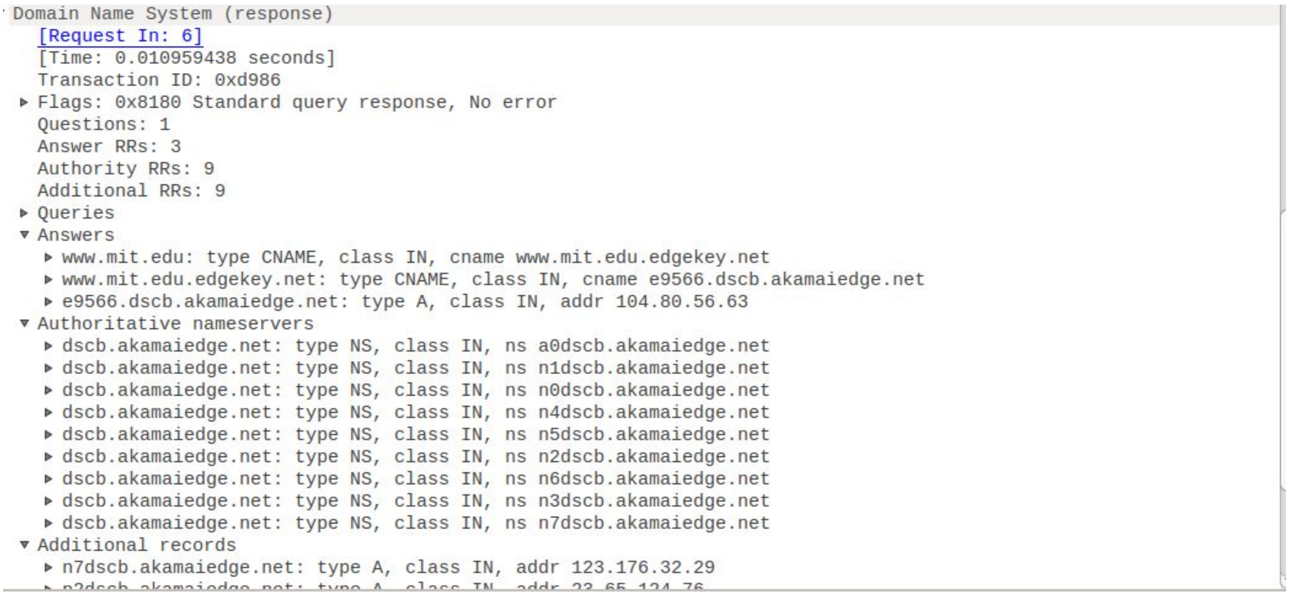
```
nikhil@nikhil-Lenovo-ideapad-300-15ISK:~$ nmcli device show wlp2s0 | grep IP4.DN
S
IP4.DNS[1]:                             10.42.0.1
```

9)type of the DNS query is UDP. It has 0 Answers .



```
▼ User Datagram Protocol, Src Port: 55929 (55929), Dst Port: 53 (53)
    Source Port: 55929
    Destination Port: 53
    Length: 37
  ▶ Checksum: 0xe3cd [validation disabled]
    [Stream index: 0]
▼ Domain Name System (query)
    [Response In: 7]
    Transaction ID: 0xd986
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
```

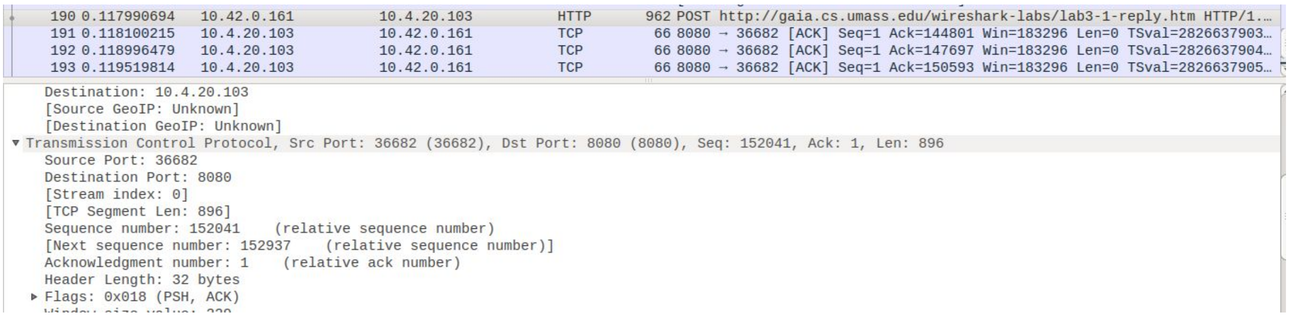
10) it has 3 answers, each contain a DNS datagram of MIT



```
Domain Name System (response)
  [Request In: 6]
  [Time: 0.010959438 seconds]
  Transaction ID: 0xd986
▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 9
  Additional RRs: 9
▶ Queries
▼ Answers
  ▶ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  ▶ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  ▶ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.80.56.63
▼ Authoritative nameservers
  ▶ dscb.akamaiedge.net: type NS, class IN, ns a0dscb.akamaiedge.net
  ▶ dscb.akamaiedge.net: type NS, class IN, ns n1dscb.akamaiedge.net
  ▶ dscb.akamaiedge.net: type NS, class IN, ns n0dscb.akamaiedge.net
  ▶ dscb.akamaiedge.net: type NS, class IN, ns n4dscb.akamaiedge.net
  ▶ dscb.akamaiedge.net: type NS, class IN, ns n5dscb.akamaiedge.net
  ▶ dscb.akamaiedge.net: type NS, class IN, ns n2dscb.akamaiedge.net
  ▶ dscb.akamaiedge.net: type NS, class IN, ns n6dscb.akamaiedge.net
  ▶ dscb.akamaiedge.net: type NS, class IN, ns n3dscb.akamaiedge.net
  ▶ dscb.akamaiedge.net: type NS, class IN, ns n7dscb.akamaiedge.net
▼ Additional records
  ▶ n7dscb.akamaiedge.net: type A, class IN, addr 123.176.32.29
  ▶ n2dscb.akamaiedge.net: type A, class IN, addr 23.65.124.76
```

Part 3 : Wireshark TCP

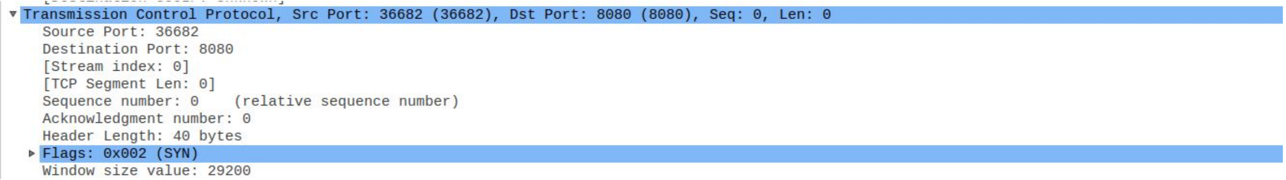
1.The client IP address is 10.42.0.161, TCP port number is 36682



```
190 0.117990694   10.42.0.161    10.4.20.103    HTTP    962 POST http://gaia.cs.umass.edu/wireshark-labs/lab3-1-reply.htm HTTP/1.…
191 0.118100215   10.4.20.103    10.42.0.161    TCP      66 8080 → 36682 [ACK] Seq=1 Ack=144801 Win=183296 Len=0 TSval=2826637903…
192 0.118996479   10.4.20.103    10.42.0.161    TCP      66 8080 → 36682 [ACK] Seq=1 Ack=147697 Win=183296 Len=0 TSval=2826637904…
193 0.119519814   10.4.20.103    10.42.0.161    TCP      66 8080 → 36682 [ACK] Seq=1 Ack=150593 Win=183296 Len=0 TSval=2826637905…
```

```
    Destination: 10.4.20.103
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ Transmission Control Protocol, Src Port: 36682 (36682), Dst Port: 8080 (8080), Seq: 152041, Ack: 1, Len: 896
    Source Port: 36682
    Destination Port: 8080
    [Stream index: 0]
    [TCP Segment Len: 896]
    Sequence number: 152041    (relative sequence number)
    [Next sequence number: 152937    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header Length: 32 bytes
  ▸ Flags: 0x018 (PSH, ACK)
```

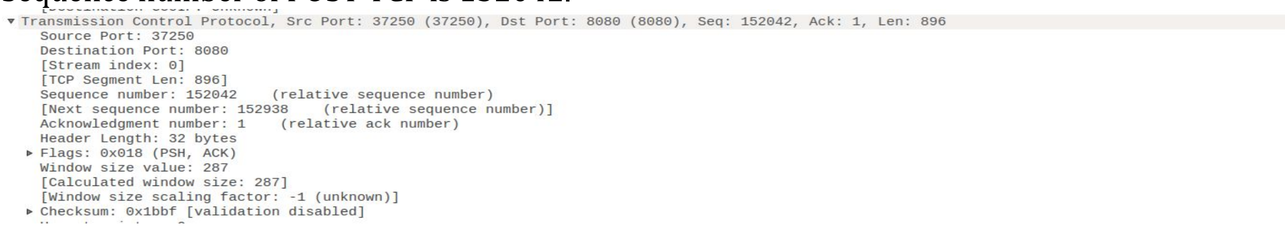
2.the host IP address is (proxy server) is 10.4.20.103 , TCP PORT number is 8080.
3.The client IP address is 10.42.0.161, TCP port number is 36682
4.the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu is 0 , the flag of TCP shows it as SYN.



```
▼ Transmission Control Protocol, Src Port: 36682 (36682), Dst Port: 8080 (8080), Seq: 0, Len: 0
    Source Port: 36682
    Destination Port: 8080
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 40 bytes
  ▸ Flags: 0x002 (SYN)
    Window size value: 29200
```

5.

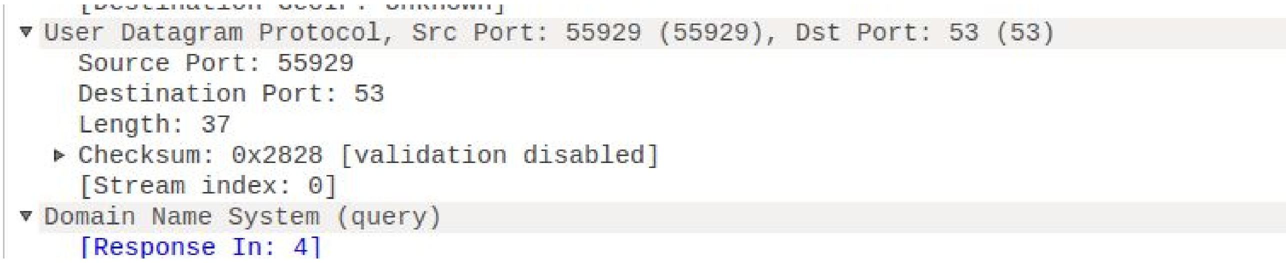
Sequence number of POST TCP is 152042.



```
▼ Transmission Control Protocol, Src Port: 37250 (37250), Dst Port: 8080 (8080), Seq: 152042, Ack: 1, Len: 896
    Source Port: 37250
    Destination Port: 8080
    [Stream index: 0]
    [TCP Segment Len: 896]
    Sequence number: 152042    (relative sequence number)
    [Next sequence number: 152938    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header Length: 32 bytes
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 287
    [Calculated window size: 287]
    [Window size scaling factor: -1 (unknown)]
  ▸ Checksum: 0x1bbf [validation disabled]
```

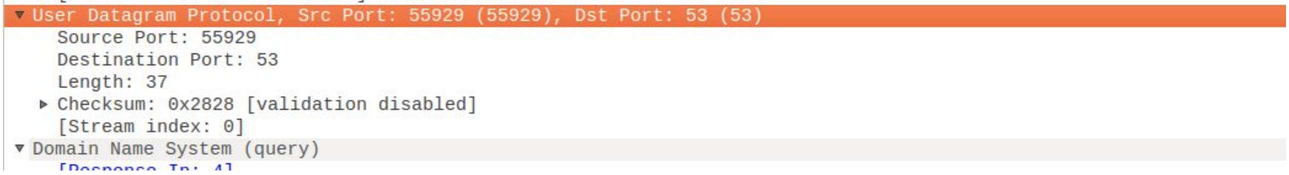
Part 4 : Wireshark UDP

1.4 Fields

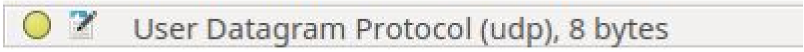


```
▼ User Datagram Protocol, Src Port: 55929 (55929), Dst Port: 53 (53)
    Source Port: 55929
    Destination Port: 53
    Length: 37
  ▸ Checksum: 0x2828 [validation disabled]
    [Stream index: 0]
▼ Domain Name System (query)
    [Response In: 4]
```

2.   8 bytes UDP packet header added with 29 bytes payload from Application Layer equals to the length of 37 bytes.



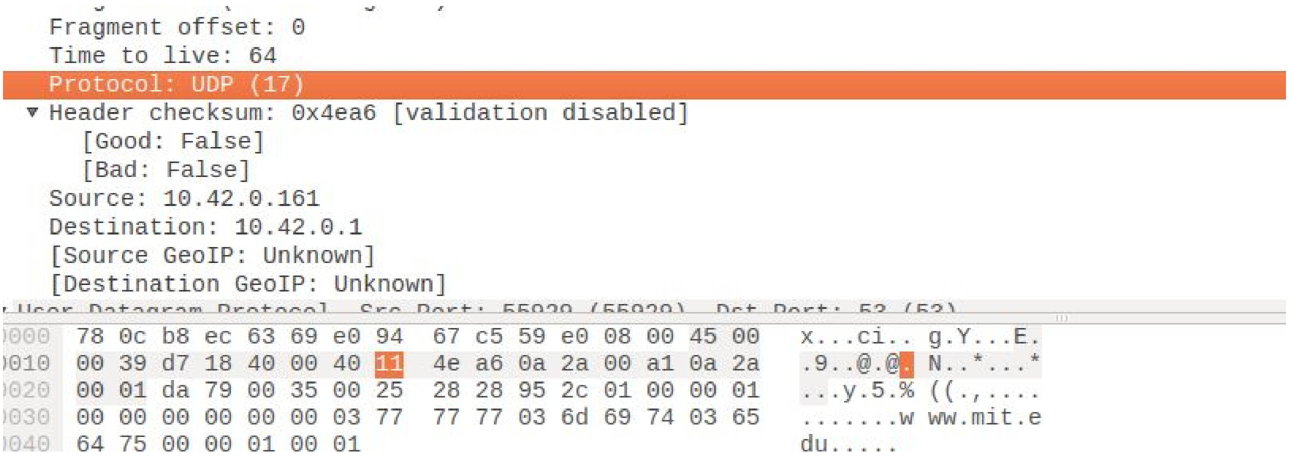
```
▼ User Datagram Protocol, Src Port: 55929 (55929), Dst Port: 53 (53)
    Source Port: 55929
    Destination Port: 53
    Length: 37
  ▸ Checksum: 0x2828 [validation disabled]
    [Stream index: 0]
▼ Domain Name System (query)
```



User Datagram Protocol (udp), 8 bytes

3.The maximum number of bytes that can be in the payload is 2^16- the bytes already being used by the header field (8). Therefore the maximum payload is 65535-8= 65527 bytes.
The largest possible source port number is 2^16 or 65535.

4.Protocol number in decimal is 17.
Protocol number in hexadecimal is 11.



```
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
  ▾ Header checksum: 0x4ea6 [validation disabled]
      [Good: False]
      [Bad: False]
    Source: 10.42.0.161
    Destination: 10.42.0.1
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▸ User Datagram Protocol, Src Port: 55929 (55929), Dst Port: 53 (53)
0000  78 0c b8 ec 63 69 e0 94  67 c5 59 e0 08 00 45 00   x...ci.. g.Y...E.
0010  00 39 d7 18 40 00 40 11  4e a6 0a 2a 00 a1 0a 2a   .9..@.@. N..*...*
0020  00 01 da 79 00 35 00 25  28 28 95 2c 01 00 00 01   ...y.5.% ((.,....
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   .......w ww.mit.e
0040  64 75 00 00 01 00 01                               du.....
```

5)The basic idea is that the **UDP checksum** is a the complement of a 16-bit one's complement sum calculated over an IP "pseudo-header" and the actual **UDP** data. The IP pseudo-header is the source address, destination address, protocol (padded with a zero byte) and **UDP** length.