**Networking - M1 international - Lab: Web and DNS**

**-Submitted by** Cyril Naves & Gabriel Pires

**1. WEB Part1:** <http://www.i3s.unice.fr/~raparicio/teaching/intr2netw/labs/Part1/index.html>

1. In the above URL, which part corresponds to the server and which part corresponds to the path of the object

on the server?

**Ans:**

Server: <http://www.i3s.unice.fr/>

Path of Object: [~raparicio/teaching/intr2netw/labs/Part1/index.html](http://www.i3s.unice.fr/~raparicio/teaching/intr2netw/labs/Part1/index.html)

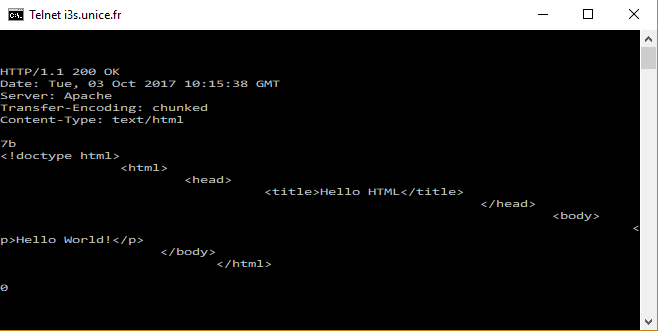
1. Connect using telnet on the server. Once the TCP channel is established, enter a GET command so as to retrieve the URL with non persistent HTTP connection. You must have a GET and a host line so that the server answers correctly.

**Ans:**

Command:

GET /~raparicio/teaching/intr2netw/labs/Part1/index.html HTTP/1.1

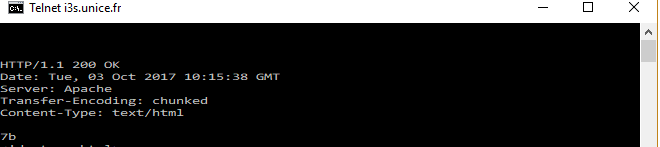
Host:i3s.unice.fr



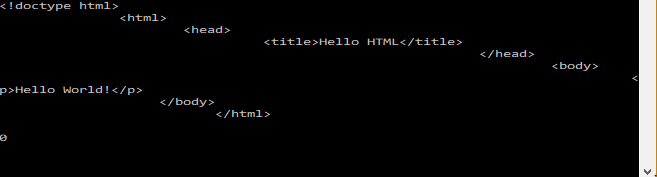
3.Which part of the answer corresponds to the control information and which part corresponds to the data?

**Ans:**

Control Information:



Data:



4.What is the response status and what does it means?

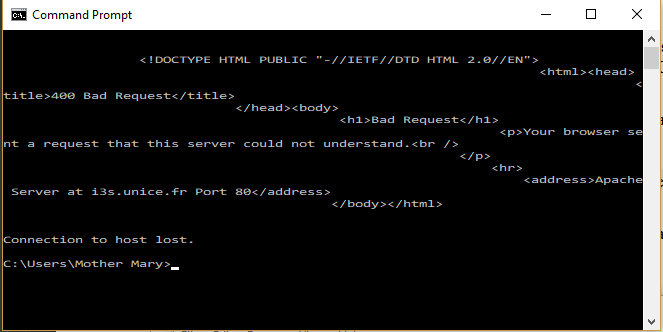
**Ans:**

Response Status: 200

Request succeeded, Requested Object later in the message

5.Create a HTTP request without indicating the method, that is, a request that is not syntactically correct. What is the response status and what does it mean?

**Ans:**



**Command:** ( Without using GET method)

/~raparicio/teaching/intr2netw/labs/Part1/index.html HTTP/1.1

Host:i3s.unice.fr

Response Status: 400

The HTTP 400 Bad Request response status code indicates that the server could not understand the request due to invalid syntax

6.Create a GET request that is syntactically correct but it asks for a non available object. What is the response status given by the server and what does it mean?

**Ans:**

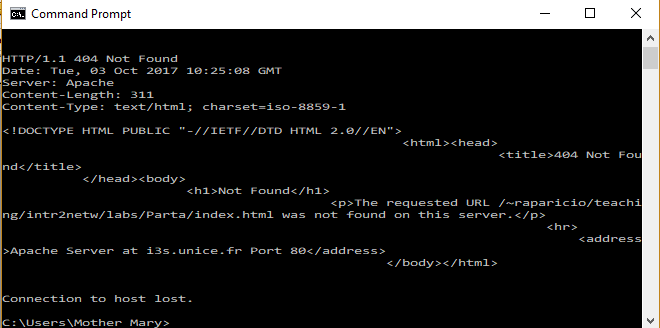
Command:

GET /~raparicio/teaching/intr2netw/labs/Parta/index.html HTTP/1.1

Host:i3s.unice.fr

Here GET request Object Path is changed to Parta instead of Part1

Response:

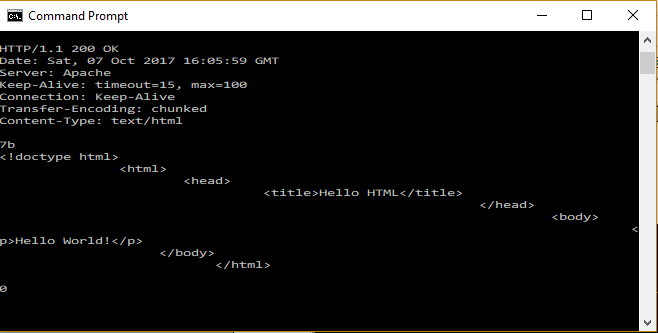


Status Code: 404 NOT FOUND

Request document not found on this server

7.Create a correct request (correct syntax and an existing object) in HTTP/1.1 and add the following line to the header after the host option :Connection: Keep-Alive

What are the changes in the returned HTTP header and in the TCP connection?

**Ans:**

Command:

GET /~raparicio/teaching/intr2netw/labs/Part1/index.html HTTP/1.1

Host:i3s.unice.fr

Connection:Keep-Alive

Returned HTTP Header contains the following values which are added

1. Keep-alive with timeout and max
2. Connection : keep-alive

**Part 2:**

http://www.i3s.unice.fr/~raparicio/teaching/intr2netw/labs/Part2/index.html

1.Go to Firefox-> Developer Tools-> Network Tab, and type the url http://www.i3s.unice.fr/~rapari-cio/teaching/intr2netw/labs/Part2/index.html

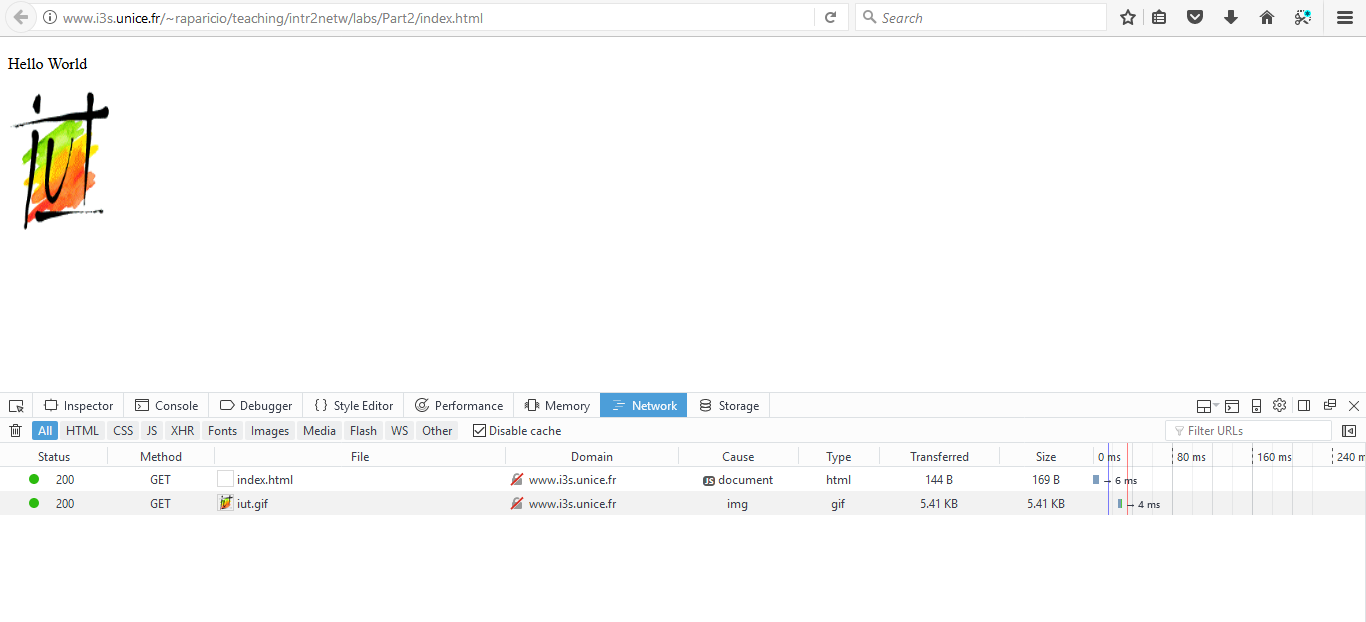
in the browser. On the Network tab, which type of HTTP requests are displayed and how many? Why? (You probably will need to clear navigation history he first time and after several connections)

**Ans:**

GET Requests totalling to no 2 were displayed in the network tools which were of status 200

Because each GET Request corresponds to the fetching of the following from the server:

1. HTML ,Javascript files( to render the webpage components)
2. CSS Files( To get the design file css components required for the webpage)
3. png and jpeg files to get the image components



2.If you refresh the same url with the button beside the address bar(without clearing the navigation history this time), do they display the same HTTP requests as before?

What happened between the two times you typed the url?

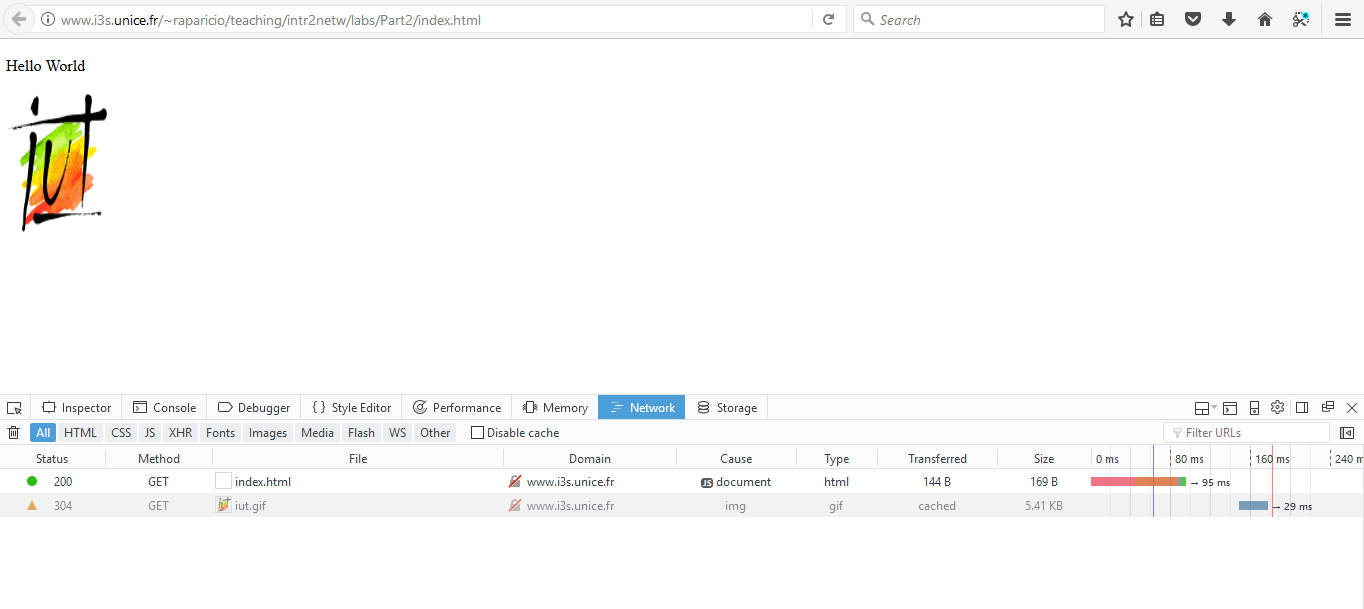
**Ans:**If the same page is refreshed as before the same HTTP request totalling to 2 are displayed with getting the following components:

1) HTML ,Javascript files( to render the webpage components)

2) CSS Files( To get the design file css components required for the webpage)

3) png and jpeg files to get the image components

But the status of the **HTTP requests were of status 304** with no content modified as there was an implicit redirection to get the cached resources in the browser.



**Part 3:**

Uploading data to the server

Using the Network Tab at the Developer Tools of Firefox, compare the upload operations performed for the following URLs:

http://www.i3s.unice.fr/~raparicio/teaching/intr2netw/labs/Part3/index.html

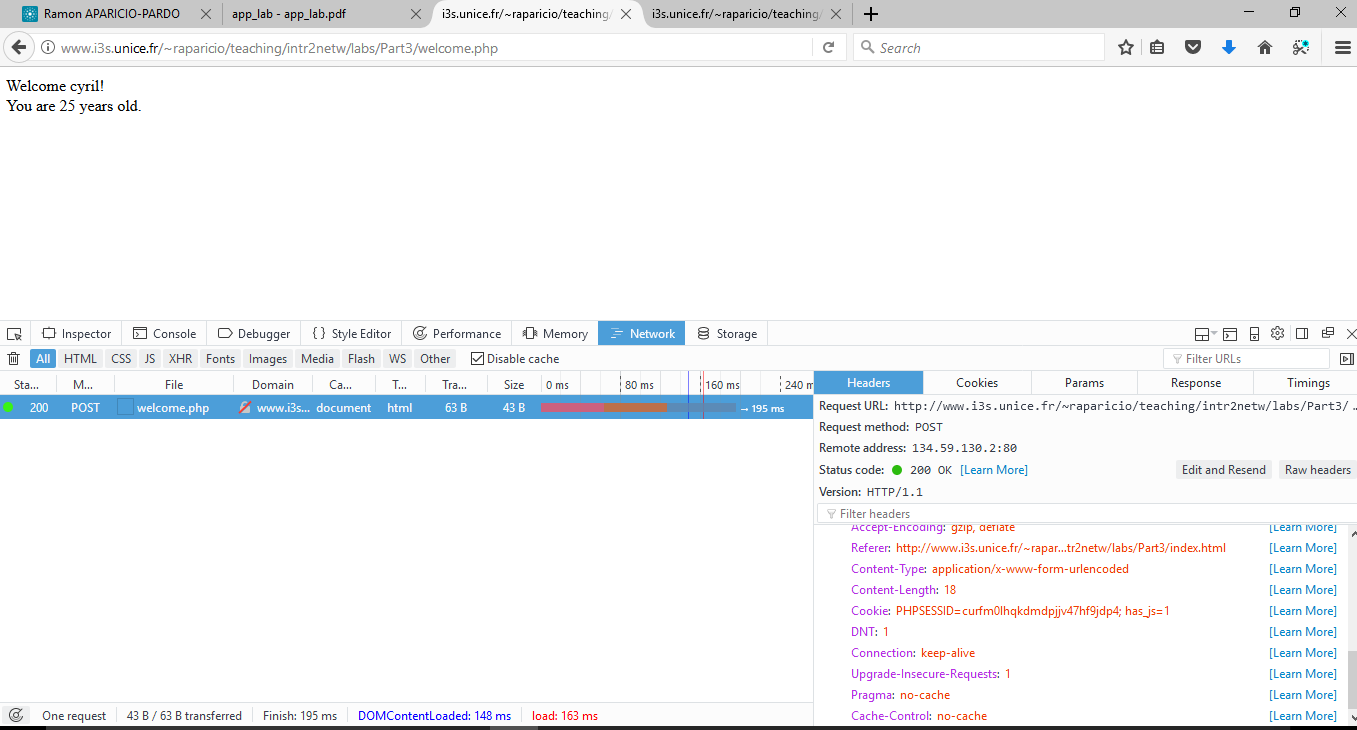
, and http://www.i3s.unice.fr/~raparicio/teaching/intr2netw/labs/Part3/index2.html

Hint: empty the network tab once the page has been downloaded so as to see only the operation performed when you click on Submit

**Ans:**

1)Request <http://www.i3s.unice.fr/~raparicio/teaching/intr2netw/labs/Part3/index.html> redirected to <http://www.i3s.unice.fr/~raparicio/teaching/intr2netw/labs/Part3/welcome.php>

Here the HTTP Request was a POST Operation with the request parameters embedded in the header of the HTTP Request

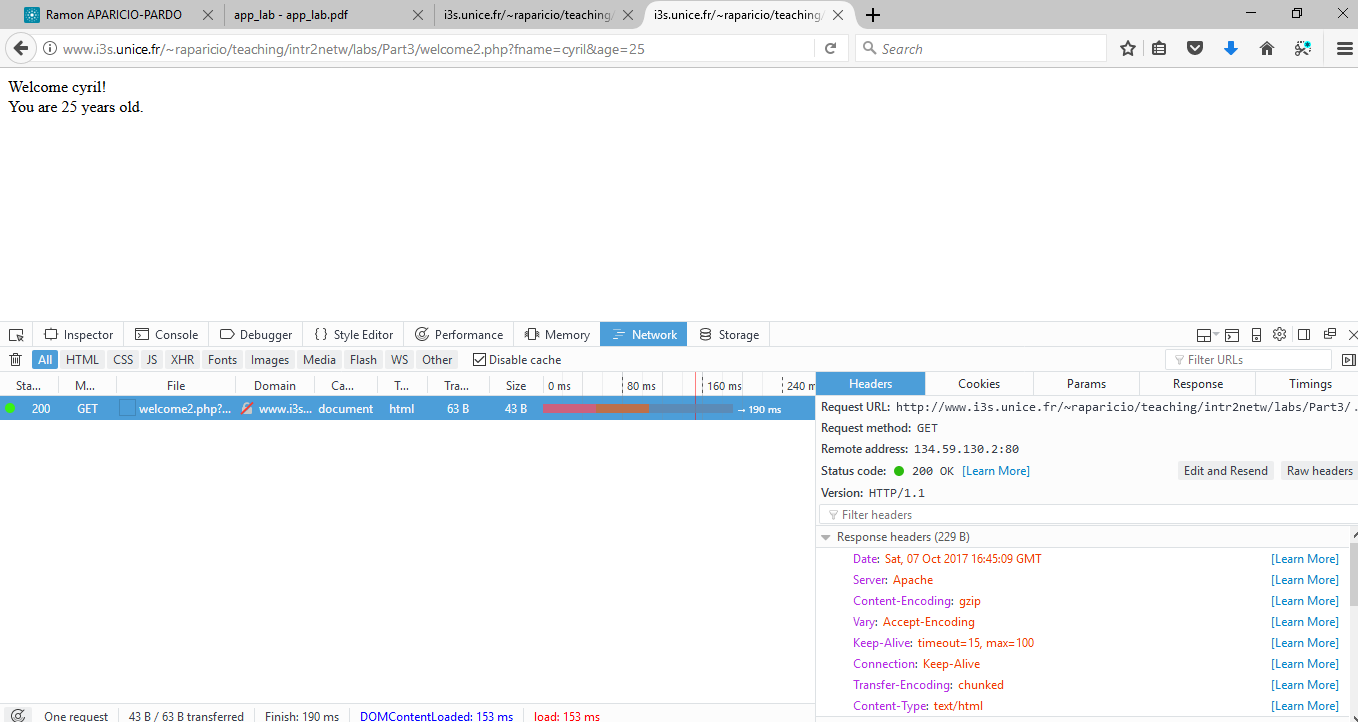


1. Request <http://www.i3s.unice.fr/~raparicio/teaching/intr2netw/labs/Part3/index2.html> redirected to <http://www.i3s.unice.fr/~raparicio/teaching/intr2netw/labs/Part3/welcome2.php?fname=cyril&age=25>

Here the HTTP Request was a GET Operation with the request parameters passed not in the header of the HTTP Request but in the URL as a parameter:

**fname=cyril**

**age=25**



**2. DNS**

**Preliminary: typical RTT in an IP network**

The objective of this first exercise is to figure out the typical distances in

IP networks. Here is a set of domains in the Internet that are organized based on their geographical distance with respect to our local position (Sophia - Antipolis).

1.For each site, use nslookup (see appendix) to find one mail exchanger and one dns server for this domain.

Report in a table their names/IPs

a)Local domain: unice.fr

b)European domain: aalto.fi

c)US domain: bu.edu

d)Australia domain: sydney.edu.au

**Ans:**

Command:

nslookup -type=MX unice.fr -----> for finding mail exchange server

nslookup -type=ns unice.fr -------> for finding naming server

|  |  |  |
| --- | --- | --- |
|  | **MAIL EXCHANGER** | **DNS SERVER** |
| Local domain: unice.fr | ip-nice06.unice.fr | Taloa.nice.fr |
| European domain: aalto.fi | mx.aalto.fi | ns02.aalto.fi |
| US domain: bu.edu | relay-mx4.bu.edu | edns01.bu.edu |
| Australia domain: sydney.edu.au | au-smtp-inbound-2.mimecast.com | extro.ucc.usyd.edu.au |

2.Report the average RTT obtained using ping towards the web server of each domain (obtained by adding www to the domain name).

**Ans:**

Command: ping www.unice.fr

|  |  |
| --- | --- |
| **Domain** | **RTT( millisecs)** |
| Local domain: unice.fr | Minimum: 57ms Maximum: 64ms Average: 58ms |
| European domain: aalto.fi | Minimum:46ms Maximum:77ms Average:56ms |
| US domain: bu.edu | Minimum: Maximum: Average: **Request Timed Out** |
| Australia domain: sydney.edu.au | Minimum:343 Maximum:346 Average:344 |

Simple queries

1.Open a terminal window and type nslookup www.unice.fr. What is the IP of the server that responded?

**Ans:**

IP of server: [www.unice.fr](http://www.unice.fr/) 134.59.204.9

2.Let us now ask for a more verbose response:nslookup -debug www.unice.fr

Explain the different parts of the response

**Ans:**

C:\Users\Mother Mary>nslookup -debug www.google.fr

------------

Got answer:

HEADER:

opcode = QUERY, id = 1, rcode = NOERROR

header flags: response, auth. answer, want recursion, recursion avail.

questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:

253.127.154.10.in-addr.arpa, type = PTR, class = IN

ANSWERS:

-> 253.127.154.10.in-addr.arpa

name = t154.wifi.unice.fr

ttl = 0 (0 secs)

------------

Server: t154.wifi.unice.fr

Address: 10.154.127.253

*Explanation 1: 1st Got Answer is used to get the hostname of server from which nslookup is performed for unice.fr*

------------

Got answer:

HEADER:

opcode = QUERY, id = 2, rcode = NXDOMAIN

header flags: response, auth. answer, want recursion, recursion avail.

questions = 1, answers = 0, authority records = 1, additional = 0

QUESTIONS:

www.google.fr.wifi.unice.fr, type = A, class = IN

AUTHORITY RECORDS:

-> unice.fr

ttl = 86400 (1 day)

primary name server = taloa.unice.fr

responsible mail addr = hostmaster.unice.fr

serial = 2017101709

refresh = 21600 (6 hours)

retry = 3600 (1 hour)

expire = 864000 (10 days)

default TTL = 86400 (1 day)

------------

------------

Got answer:

HEADER:

opcode = QUERY, id = 3, rcode = NXDOMAIN

header flags: response, auth. answer, want recursion, recursion avail.

questions = 1, answers = 0, authority records = 1, additional = 0

QUESTIONS:

www.google.fr.wifi.unice.fr, type = AAAA, class = IN

AUTHORITY RECORDS:

-> unice.fr

ttl = 86400 (1 day)

primary name server = taloa.unice.fr

responsible mail addr = hostmaster.unice.fr

serial = 2017101709

refresh = 21600 (6 hours)

retry = 3600 (1 hour)

expire = 864000 (10 days)

default TTL = 86400 (1 day)

------------

------------

Got answer:

HEADER:

opcode = QUERY, id = 4, rcode = NXDOMAIN

header flags: response, auth. answer, want recursion, recursion avail.

questions = 1, answers = 0, authority records = 1, additional = 0

QUESTIONS:

www.google.fr.unice.fr, type = A, class = IN

AUTHORITY RECORDS:

-> unice.fr

ttl = 86400 (1 day)

primary name server = taloa.unice.fr

responsible mail addr = hostmaster.unice.fr

serial = 2017101709

refresh = 21600 (6 hours)

retry = 3600 (1 hour)

expire = 864000 (10 days)

default TTL = 86400 (1 day)

------------

------------

Got answer:

HEADER:

opcode = QUERY, id = 5, rcode = NXDOMAIN

header flags: response, auth. answer, want recursion, recursion avail.

questions = 1, answers = 0, authority records = 1, additional = 0

QUESTIONS:

www.google.fr.unice.fr, type = AAAA, class = IN

AUTHORITY RECORDS:

-> unice.fr

ttl = 86400 (1 day)

primary name server = taloa.unice.fr

responsible mail addr = hostmaster.unice.fr

serial = 2017101709

refresh = 21600 (6 hours)

retry = 3600 (1 hour)

expire = 864000 (10 days)

default TTL = 86400 (1 day)

------------

------------

Got answer:

HEADER:

opcode = QUERY, id = 6, rcode = NOERROR

header flags: response, want recursion, recursion avail.

questions = 1, answers = 1, authority records = 4, additional = 4

QUESTIONS:

www.google.fr, type = A, class = IN

ANSWERS:

-> www.google.fr

internet address = 216.58.213.131

ttl = 157 (2 mins 37 secs)

AUTHORITY RECORDS:

-> google.fr

nameserver = ns1.google.com

ttl = 106092 (1 day 5 hours 28 mins 12 secs)

-> google.fr

nameserver = ns3.google.com

ttl = 106092 (1 day 5 hours 28 mins 12 secs)

-> google.fr

nameserver = ns4.google.com

ttl = 106092 (1 day 5 hours 28 mins 12 secs)

-> google.fr

nameserver = ns2.google.com

ttl = 106092 (1 day 5 hours 28 mins 12 secs)

ADDITIONAL RECORDS:

-> ns1.google.com

internet address = 216.239.32.10

ttl = 2189 (36 mins 29 secs)

-> ns2.google.com

internet address = 216.239.34.10

ttl = 2189 (36 mins 29 secs)

-> ns4.google.com

internet address = 216.239.38.10

ttl = 2189 (36 mins 29 secs)

-> ns3.google.com

internet address = 216.239.36.10

ttl = 2189 (36 mins 29 secs)

***Explanation 2:*** *5th Got Answer related to the actual request for nslookup*

*Header Section: Contains details about the request and its non- ERROR*

*Questions Section: Shows request was for AAAA records for* [www.unice.fr](http://www.unice.fr)

*Answers Section: Displays google.fr with an IP address* 216.58.213.131 and ttl = 157 (2 mins 37 secs)

Authority Records: specifies the name servers that correspond to the domain ..like ns3.google.com

Additional Records: Lists A records for the name servers listed in authority records section

Non-authoritative answer:

------------

Got answer:

HEADER:

opcode = QUERY, id = 7, rcode = NOERROR

header flags: response, want recursion, recursion avail.

questions = 1, answers = 1, authority records = 4, additional = 4

QUESTIONS:

www.google.fr, type = AAAA, class = IN

ANSWERS:

-> www.google.fr

AAAA IPv6 address = 2a00:1450:4007:810::2003

ttl = 163 (2 mins 43 secs)

AUTHORITY RECORDS:

-> google.fr

nameserver = ns4.google.com

ttl = 106092 (1 day 5 hours 28 mins 12 secs)

-> google.fr

nameserver = ns2.google.com

ttl = 106092 (1 day 5 hours 28 mins 12 secs)

-> google.fr

nameserver = ns3.google.com

ttl = 106092 (1 day 5 hours 28 mins 12 secs)

-> google.fr

nameserver = ns1.google.com

ttl = 106092 (1 day 5 hours 28 mins 12 secs)

ADDITIONAL RECORDS:

-> ns1.google.com

internet address = 216.239.32.10

ttl = 2189 (36 mins 29 secs)

-> ns2.google.com

internet address = 216.239.34.10

ttl = 2189 (36 mins 29 secs)

-> ns4.google.com

internet address = 216.239.38.10

ttl = 2189 (36 mins 29 secs)

-> ns3.google.com

internet address = 216.239.36.10

ttl = 2189 (36 mins 29 secs)

Name: www.google.fr

Addresses: 2a00:1450:4007:810::2003

216.58.213.131

*Here nslookup debug command tries to check from university connection server (* t154.wifi.unice.fr*) and then checks for the site* [*www.unice.fr*](http://www.unice.fr/) *recursively until it gets the canonical name of the site* [*www.unice.fr*](http://www.unice.fr/)

3.Run many times nslookup -debug [www.google.fr](http://www.google.fr/) commands. Which field in the answer varies and why?

**Ans:**

Here TTL of the packet varies,it signifies the time when a packet can be kept alive or can be discarded as it hops from one router to another

**Command Response:**

**1st Iteration:**

C:\Users\Mother Mary>nslookup -debug www.google.fr

------------

Got answer:

HEADER:

opcode = QUERY, id = 1, rcode = NOERROR

header flags: response, auth. answer, want recursion, recursion avail.

questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:

1.200.168.192.in-addr.arpa, type = PTR, class = IN

ANSWERS:

-> 1.200.168.192.in-addr.arpa

name = wifi.civfrance.com

ttl = 1 (1 sec)

------------

Server: wifi.civfrance.com

Address: 192.168.200.1

------------

Got answer:

HEADER:

opcode = QUERY, id = 2, rcode = NXDOMAIN

header flags: response, want recursion, recursion avail.

questions = 1, answers = 0, authority records = 0, additional = 0

QUESTIONS:

www.google.fr.civfrance.com, type = A, class = IN

------------

------------

Got answer:

HEADER:

opcode = QUERY, id = 3, rcode = NXDOMAIN

header flags: response, want recursion, recursion avail.

questions = 1, answers = 0, authority records = 1, additional = 0

QUESTIONS:

www.google.fr.civfrance.com, type = AAAA, class = IN

AUTHORITY RECORDS:

-> civfrance.com

ttl = 1544 (25 mins 44 secs)

primary name server = ns1.tasfrance.com

responsible mail addr = wm.atsat.com

serial = 2008082542

refresh = 28800 (8 hours)

retry = 7200 (2 hours)

expire = 604800 (7 days)

default TTL = 86400 (1 day)

------------

------------

Got answer:

HEADER:

opcode = QUERY, id = 4, rcode = NOERROR

header flags: response, want recursion, recursion avail.

questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:

www.google.fr, type = A, class = IN

ANSWERS:

-> www.google.fr

internet address = 172.217.17.131

ttl = 204 (3 mins 24 secs)

------------

Non-authoritative answer:

------------

Got answer:

HEADER:

opcode = QUERY, id = 5, rcode = NOERROR

header flags: response, want recursion, recursion avail.

questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:

www.google.fr, type = AAAA, class = IN

ANSWERS:

-> www.google.fr

AAAA IPv6 address = 2a00:1450:400e:807::2003

ttl = 2 (2 secs)

------------

Name: www.google.fr

Addresses: 2a00:1450:400e:807::2003

172.217.17.131

**2nd Interation:**

C:\Users\Mother Mary>nslookup -debug www.google.fr

------------

Got answer:

HEADER:

opcode = QUERY, id = 1, rcode = NOERROR

header flags: response, auth. answer, want recursion, recursion avail.

questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:

1.200.168.192.in-addr.arpa, type = PTR, class = IN

ANSWERS:

-> 1.200.168.192.in-addr.arpa

name = wifi.civfrance.com

ttl = 1 (1 sec)

------------

Server: wifi.civfrance.com

Address: 192.168.200.1

------------

Got answer:

HEADER:

opcode = QUERY, id = 2, rcode = NXDOMAIN

header flags: response, want recursion, recursion avail.

questions = 1, answers = 0, authority records = 0, additional = 0

QUESTIONS:

www.google.fr.civfrance.com, type = A, class = IN

------------

------------

Got answer:

HEADER:

opcode = QUERY, id = 3, rcode = NXDOMAIN

header flags: response, want recursion, recursion avail.

questions = 1, answers = 0, authority records = 0, additional = 0

QUESTIONS:

www.google.fr.civfrance.com, type = AAAA, class = IN

------------

------------

Got answer:

HEADER:

opcode = QUERY, id = 4, rcode = NOERROR

header flags: response, want recursion, recursion avail.

questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:

www.google.fr, type = A, class = IN

ANSWERS:

-> www.google.fr

internet address = 172.217.17.131

ttl = 195 (3 mins 15 secs)

------------

Non-authoritative answer:

------------

Got answer:

HEADER:

opcode = QUERY, id = 5, rcode = NOERROR

header flags: response, want recursion, recursion avail.

questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:

www.google.fr, type = AAAA, class = IN

ANSWERS:

-> www.google.fr

AAAA IPv6 address = 2a00:1450:400e:807::2003

ttl = 297 (4 mins 57 secs)

------------

Name: www.google.fr

Addresses: 2a00:1450:400e:807::2003

172.217.17.131

**3rd Iteration:**

C:\Users\Mother Mary>nslookup -debug www.google.fr

------------

Got answer:

HEADER:

opcode = QUERY, id = 1, rcode = NOERROR

header flags: response, auth. answer, want recursion, recursion avail.

questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:

1.200.168.192.in-addr.arpa, type = PTR, class = IN

ANSWERS:

-> 1.200.168.192.in-addr.arpa

name = wifi.civfrance.com

ttl = 1 (1 sec)

------------

Server: wifi.civfrance.com

Address: 192.168.200.1

------------

Got answer:

HEADER:

opcode = QUERY, id = 2, rcode = NXDOMAIN

header flags: response, want recursion, recursion avail.

questions = 1, answers = 0, authority records = 0, additional = 0

QUESTIONS:

www.google.fr.civfrance.com, type = A, class = IN

------------

------------

Got answer:

HEADER:

opcode = QUERY, id = 3, rcode = NXDOMAIN

header flags: response, want recursion, recursion avail.

questions = 1, answers = 0, authority records = 0, additional = 0

QUESTIONS:

www.google.fr.civfrance.com, type = AAAA, class = IN

------------

------------

Got answer:

HEADER:

opcode = QUERY, id = 4, rcode = NOERROR

header flags: response, want recursion, recursion avail.

questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:

www.google.fr, type = A, class = IN

ANSWERS:

-> www.google.fr

internet address = 172.217.17.131

ttl = 119 (1 min 59 secs)

------------

Non-authoritative answer:

------------

Got answer:

HEADER:

opcode = QUERY, id = 5, rcode = NOERROR

header flags: response, want recursion, recursion avail.

questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:

www.google.fr, type = AAAA, class = IN

ANSWERS:

-> www.google.fr

AAAA IPv6 address = 2a00:1450:400e:807::2003

ttl = 221 (3 mins 41 secs)

------------

Name: www.google.fr

Addresses: 2a00:1450:400e:807::2003

172.217.17.131

***Authoritative vs. Non authoritative responses***

1.Open a terminal window and type nslookup www.google.fr. Why is the answer flagged as “non authoritative”?

**Ans:**

When nslookup is performed for [www.google.fr](http://www.google.fr/) it is termed as non-authoritative because the response from the naming server does not contain the official records of google domain instead it just the ISP provided naming server which just relies on the cached data about [www.google.fr](http://www.google.fr/) and provides the IP and naming server.

2.We are now going to travel through the hierarchy of DNS servers starting from one of the root servers (list in appendix). You want to resolve [www.google.fr](http://www.google.fr) but you are only allowed considering authoritative answers. Use the Web site [http://www.digwebinterface.com](http://www.digwebinterface.com/) to request A type RRs to the name server that you specify by using the Specify myself option. Detail the different steps, listing the number of DNS servers you crossed and the ones you queried.

Note: the site [http://www.digwebinterface.com](http://www.digwebinterface.com/) provides an interface to make use of the UNIX command "dig. If you are using a LINUX or a MAC machine, you can simply tape the command dig with the right options.

You can find an online manual about command dig in <https://linux.die.net/man/1/dig>

**Ans:**

**Authoritative Answers:**

**www.google.fr@ns1.google.com.:**

[www.google.fr.](javascript:addhost('www.google.fr.')) 300 IN [A](http://www.ietf.org/rfc/rfc1035.txt) [216.58.192.195](javascript:addhost('216.58.192.195'))

**www.google.fr@ns2.google.com.:**

[www.google.fr.](javascript:addhost('www.google.fr.')) 300 IN [A](http://www.ietf.org/rfc/rfc1035.txt) [216.58.192.195](javascript:addhost('216.58.192.195'))

**www.google.fr@ns3.google.com.:**

[www.google.fr.](javascript:addhost('www.google.fr.')) 300 IN [A](http://www.ietf.org/rfc/rfc1035.txt) [216.58.192.195](javascript:addhost('216.58.192.195'))

**www.google.fr@ns4.google.com.:**

[www.google.fr.](javascript:addhost('www.google.fr.')) 300 IN [A](http://www.ietf.org/rfc/rfc1035.txt) [216.58.192.195](javascript:addhost('216.58.192.195'))

**www.google.fr@a.root-servers.net:**

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [e.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [f.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [g.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.ext.nic.fr.](about:blank)

**www.google.fr@b.root-servers.net:**

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [g.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [e.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [f.ext.nic.fr.](about:blank)

**www.google.fr@c.root-servers.net:**

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [g.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [f.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [e.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.nic.fr.](about:blank)

**www.google.fr@d.root-servers.net:**

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [f.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [g.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [e.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.ext.nic.fr.](about:blank)

**www.google.fr@e.root-servers.net:**

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [e.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [f.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [g.ext.nic.fr.](about:blank)

3.If we apply the same procedure as above to the case of

www.unice.fr, why is the first answer (returned by the root server) similar for both

[www.google.fr](http://www.google.fr/) and [www.unice.fr](http://www.unice.fr/) ?

Ans:

First Answer returned by the root server: e.root-servers.net are same since both [www.google.fr](http://www.google.fr/) and [www.unice.fr](http://www.unice.fr/) are starting with the same root domain “.**fr**”

**www.google.fr@e.root-servers.net:**

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [e.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [f.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [g.ext.nic.fr.](about:blank)

**www.unice.fr@e.root-servers.net:**

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.ext.nic.fr.](about:blank)

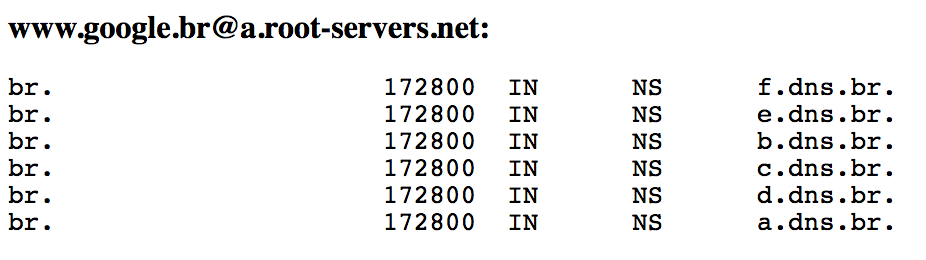
[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [d.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [e.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [f.ext.nic.fr.](about:blank)

[fr.](about:blank) 172800 IN [NS](http://www.ietf.org/rfc/rfc1035.txt) [g.ext.nic.fr.](about:blank)

If we try to run the dig command with a domain from other country then we get a different answer:



**3. ANALYSIS OF A TRACE FROM A WEB BROWSING SESSION**

Open the trace

http\_espn.pcap. (You also can find it in http://www.i3s.unice.fr/~raparicio/teaching/intr2netw) with

Wireshark. It records the loading of a single Web page.

1.What are the transport level protocols that you have observe in the trace. Use a

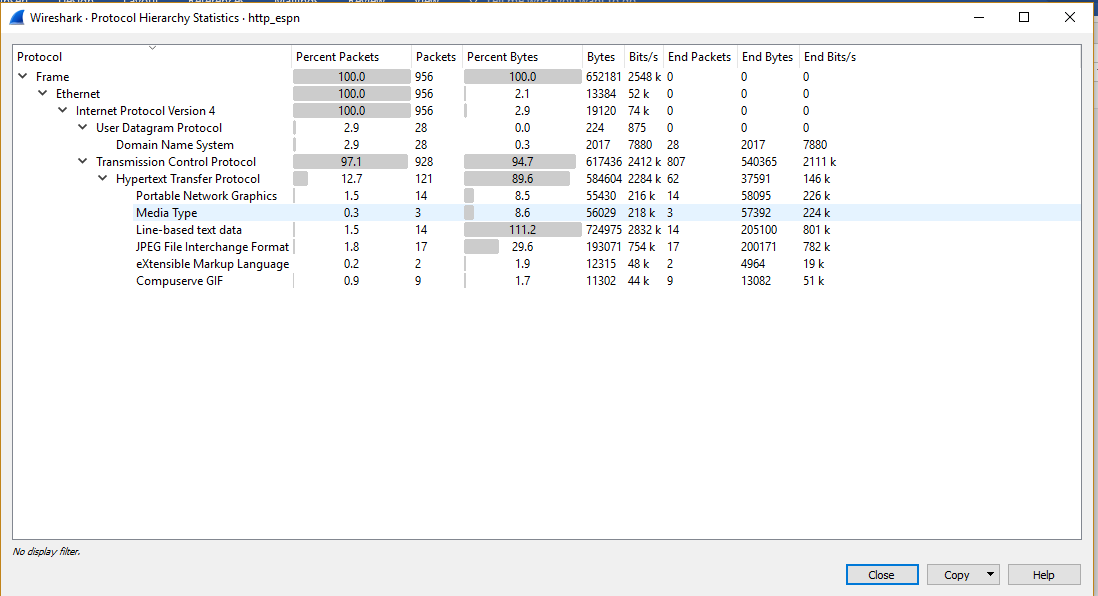
protocol hierarchy function of the statistics menu.

**Ans:**

IPV4 Internet Protocol Version 4

Transport Level Protocols observed:

1. User Datagram Protocol
2. Transmission Control Protocol
3. Hyper Text Transfer Protocol



2.How many conversations do you have at the IP, TCP and UDP protocols in the trace? Use the conversations function of the statistics menu.

**Ans:**

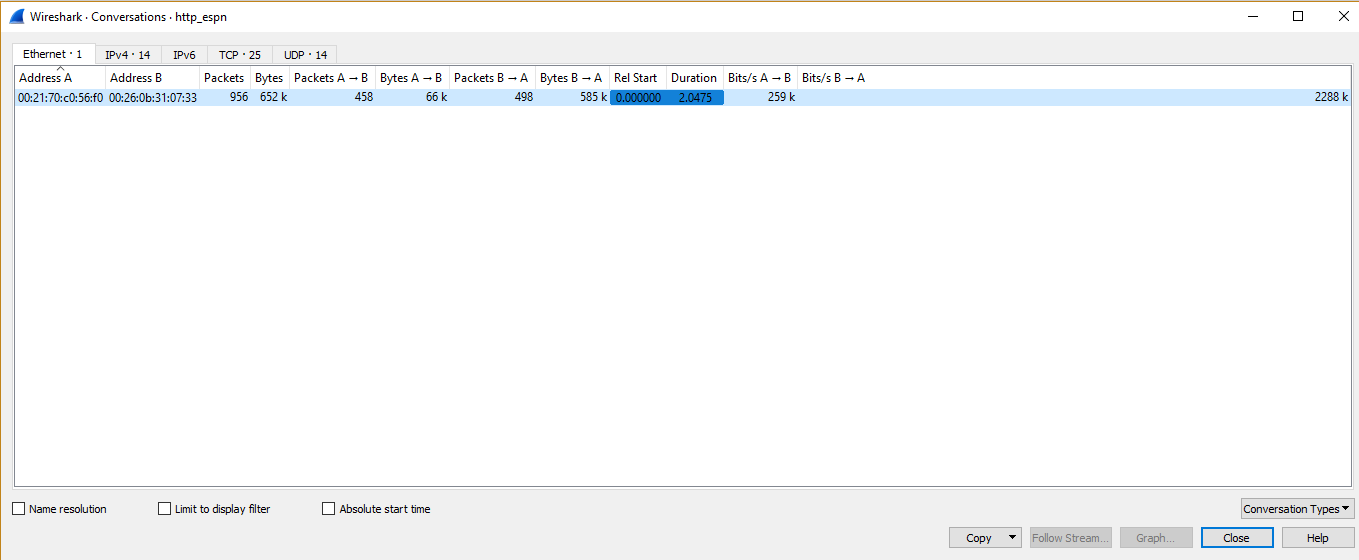
There are following conservations:

1. Ethernet- 1 nos
2. IPv4 – 14 nos
3. Ipv6 – 0 nos
4. TCP- 25 nos
5. UDP- 14 nos

3.What does the Ethernet level information of the conversations function of the

Statistics menu indicates?

**Ans:**



Ethernet Level conversation display the conversation that took place within time boundary of machine at Address A and Address B:

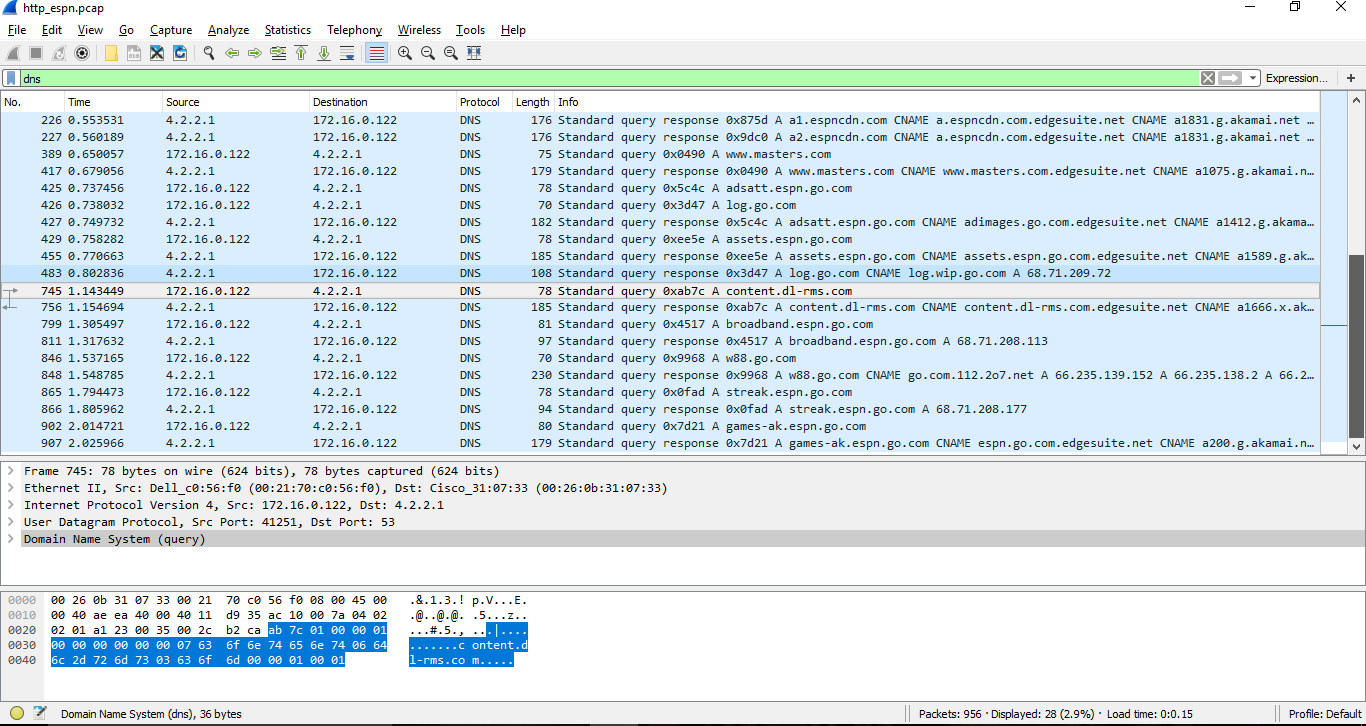
* **Network** — contains the IP or Ethernet addresses of the computer nodes that exchanged messages.

Here ethernet address from machine A: **00:21:70:c0:56:f0** to machine B: **00:26:0b:31:07:33**

* **Packets** — Total no of packets transferred between the two addresses. **956**
* **Bytes** — based on the payloadLength property of any module that defines this field, the values in this column specify the total payload byte volume of all messages (containing this property) that are associated with each Network conversation between Machine A and Machine B **652181**
* **KBs** — provides an indication of the data transmission rate in kilobytes-per-second for the messages in a conversation.
* **Duration** — specifies the delta between the **StartTime** and **EndTime** values. Total Duration of the packet transfer between Machine A and Machine B
* **Packets A ->B: 458 No of Packets Transferred from Machine A to Machine B**
* **Bytes A -> B :66467**
* **Bytes A-> B:** **66467**
* **Packets B ->A: 498**
* **Bytes B -> A 585714**
* **Bits A-> B 259702.40519818978**
* **Bits B->A 2288524.1481976397**

4.Let us now focus on DNS traffic. Create a filter to filter only DNS queries. To do this, position the cursor on the DNS flags in the lower window, then right click to create the filter using the Apply As filter and then the Selected option. How many such DNS requests of RR of type A do you find?

**Ans:**



Total no of **DNS Requests of RR Type A: 14 and Responses are 14**

No. Time Source Destination Protocol Length Info

1 0.000000 172.16.0.122 4.2.2.1 DNS 72 Standard query 0x9a6b A www.espn.com

9 0.144300 172.16.0.122 4.2.2.1 DNS 71 Standard query 0x530a A espn.go.com

21 0.326066 172.16.0.122 4.2.2.1 DNS 73 Standard query 0x49f3 A a.espncdn.com

224 0.542078 172.16.0.122 4.2.2.1 DNS 74 Standard query 0x875d A a1.espncdn.com

225 0.549050 172.16.0.122 4.2.2.1 DNS 74 Standard query 0x9dc0 A a2.espncdn.com

389 0.650057 172.16.0.122 4.2.2.1 DNS 75 Standard query 0x0490 A www.masters.com

425 0.737456 172.16.0.122 4.2.2.1 DNS 78 Standard query 0x5c4c A adsatt.espn.go.com

426 0.738032 172.16.0.122 4.2.2.1 DNS 70 Standard query 0x3d47 A log.go.com

429 0.758282 172.16.0.122 4.2.2.1 DNS 78 Standard query 0xee5e A assets.espn.go.com

745 1.143449 172.16.0.122 4.2.2.1 DNS 78 Standard query 0xab7c A content.dl-rms.com

799 1.305497 172.16.0.122 4.2.2.1 DNS 81 Standard query 0x4517 A broadband.espn.go.com

846 1.537165 172.16.0.122 4.2.2.1 DNS 70 Standard query 0x9968 A w88.go.com

865 1.794473 172.16.0.122 4.2.2.1 DNS 78 Standard query 0x0fad A streak.espn.go.com

902 2.014721 172.16.0.122 4.2.2.1 DNS 80 Standard query 0x7d21 A games-ak.espn.go.com

5.Report the response time of the first two DNS request using the time column.

**Ans:**

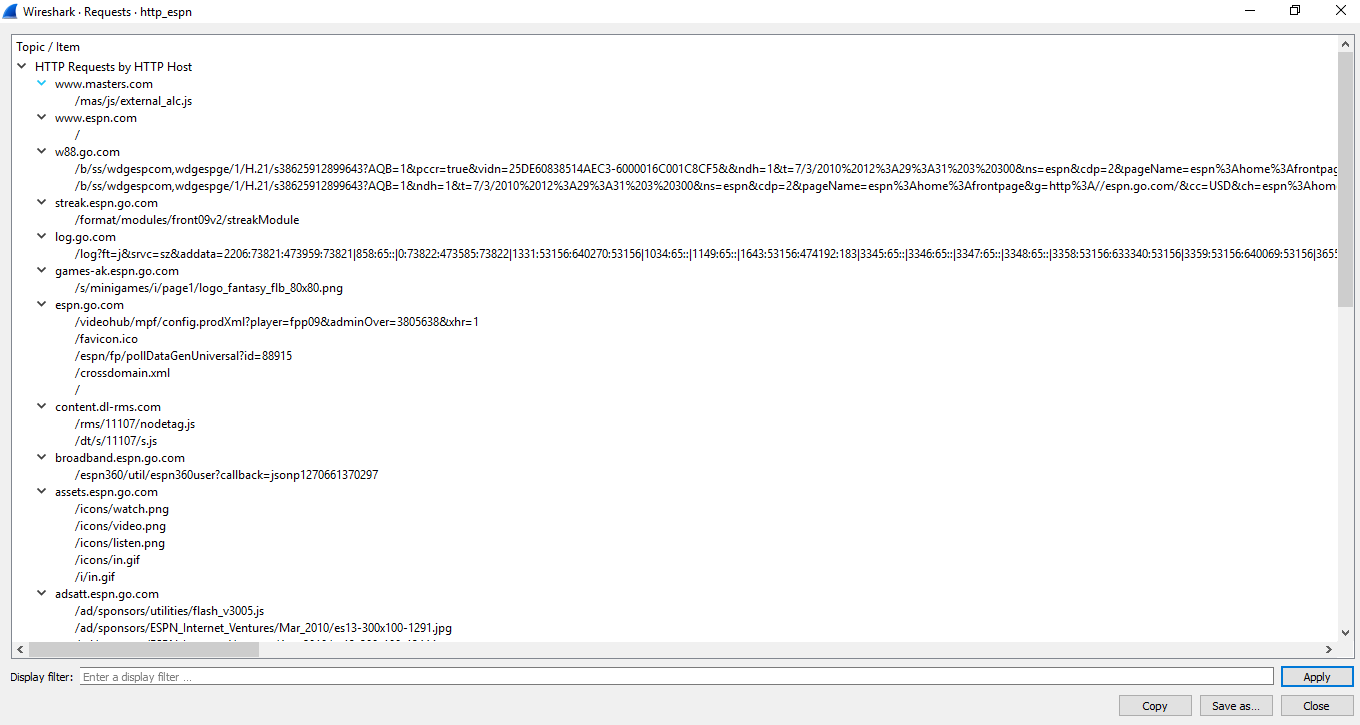
Response Time for Standard query response 0x9a6b A www.espn.com A 199.181.132.250 is **0.011665**

Response Time for Standard query response 0x530a A espn.go.com A 68.71.208.11 is **0.155758**

6.Let us consider HTTP requests. Use the HTTP -Requests option from the

Statistics menu. Interpret the result and show that it is in line with the DNS requests that were performed by the client.

**Ans:**



**List of HTTP Requests:**

HTTP/Requests:

Topic / Item Count Average Min val Max val Rate (ms) Percent Burst rate Burst start

HTTP Requests by HTTP Host 61 0.0309 100% 0.2000 0.806

www.masters.com 1 0.0005 1.64% 0.0100 0.690

/mas/js/external\_alc.js 1 0.0005 100.00% 0.0100 0.690

www.espn.com 1 0.0005 1.64% 0.0100 0.000

/ 1 0.0005 100.00% 0.0100 0.000

w88.go.com 2 0.0010 3.28% 0.0200 1.613

/b/ss/wdgespcom,wdgespge/1/H.21/s38625912899643?AQB=1&pccr=true&vidn=25DE60838514AEC3-6000016C001C8CF5&&ndh=1&t=7/3/2010%2012%3A29%3A31%203%20300&ns=espn&cdp=2&pageName=espn%3Ahome%3Afrontpage&g=http%3A//espn.go.com/&cc=USD&ch=espn%3Ahome&server=espn.go.com&events=event3%2Cevent38&products=ads%3Blogin\_cta\_unreg\_reg\_registernow%3B%3B%3Bevent38%3D1%2Cads%3B2009\_insdr\_mod\_front\_xxx\_xxx%3B%3B%3Bevent38%3D1%2Cads%3B3358%3A53156%3A633340%3A53156%3B%3B%3Bevent38%3D1&c1=espn&h1=espn%3Ahome%3Afrontpage&c2=D%3DSWID&c4=index&c5=espn%3Ahome%3Afrontpage&c6=New&v7=%3Aunknown%3Aanonymous%3Aanonymous%3Apremium-no%3A&v9=en&c11=anonymous%3Apremium-no&v11=index%3Aespn%3Ahome&v13=espn%3Ahome%3Afrontpage&c17=en&c21=unknown&c22=unknown&c24=First%20Visit&c29=anonymous&c30=false&s=1280x800&c=24&j=1.7&v=N&k=Y&bw=994&bh=565&p=Shockwave%20Flash%3BVLC%20Multimedia%20Plugin%20%28compatible%20Totem%202.28.2%29%3BWindows%20Media%20Player%20Plug-in%2010%20%28compatible%3B%20Totem%29%3BDivX%AE%20Web%20Player%3BQuickTime%20Plug-in%207.2.0%3B&AQE=1 1 0.0005 50.00% 0.0100 1.708

/b/ss/wdgespcom,wdgespge/1/H.21/s38625912899643?AQB=1&ndh=1&t=7/3/2010%2012%3A29%3A31%203%20300&ns=espn&cdp=2&pageName=espn%3Ahome%3Afrontpage&g=http%3A//espn.go.com/&cc=USD&ch=espn%3Ahome&server=espn.go.com&events=event3%2Cevent38&products=ads%3Blogin\_cta\_unreg\_reg\_registernow%3B%3B%3Bevent38%3D1%2Cads%3B2009\_insdr\_mod\_front\_xxx\_xxx%3B%3B%3Bevent38%3D1%2Cads%3B3358%3A53156%3A633340%3A53156%3B%3B%3Bevent38%3D1&c1=espn&h1=espn%3Ahome%3Afrontpage&c2=D%3DSWID&c4=index&c5=espn%3Ahome%3Afrontpage&c6=New&v7=%3Aunknown%3Aanonymous%3Aanonymous%3Apremium-no%3A&v9=en&c11=anonymous%3Apremium-no&v11=index%3Aespn%3Ahome&v13=espn%3Ahome%3Afrontpage&c17=en&c21=unknown&c22=unknown&c24=First%20Visit&c29=anonymous&c30=false&s=1280x800&c=24&j=1.7&v=N&k=Y&bw=994&bh=565&p=Shockwave%20Flash%3BVLC%20Multimedia%20Plugin%20%28compatible%20Totem%202.28.2%29%3BWindows%20Media%20Player%20Plug-in%2010%20%28compatible%3B%20Totem%29%3BDivX%AE%20Web%20Player%3BQuickTime%20Plug-in%207.2.0%3B&AQE=1 1 0.0005 50.00% 0.0100 1.613

streak.espn.go.com 1 0.0005 1.64% 0.0100 1.884

/format/modules/front09v2/streakModule 1 0.0005 100.00% 0.0100 1.884

log.go.com 1 0.0005 1.64% 0.0100 0.869

/log?ft=j&srvc=sz&addata=2206:73821:473959:73821|858:65::|0:73822:473585:73822|1331:53156:640270:53156|1034:65::|1149:65::|1643:53156:474192:183|3345:65::|3346:65::|3347:65::|3348:65::|3358:53156:633340:53156|3359:53156:640069:53156|3655:65::&method=GET&cap=&svr=espn.go.com&host=espn.go.com&guid=B249644A-DD09-42ED-BD98-1C75B2F98967&sf=cnt\_codes:SZ11 1 0.0005 100.00% 0.0100 0.869

games-ak.espn.go.com 1 0.0005 1.64% 0.0100 2.036

/s/minigames/i/page1/logo\_fantasy\_flb\_80x80.png 1 0.0005 100.00% 0.0100 2.036

espn.go.com 5 0.0025 8.20% 0.0300 1.315

/videohub/mpf/config.prodXml?player=fpp09&adminOver=3805638&xhr=1 1 0.0005 20.00% 0.0100 1.385

/favicon.ico 1 0.0005 20.00% 0.0100 1.806

/espn/fp/pollDataGenUniversal?id=88915 1 0.0005 20.00% 0.0100 1.383

/crossdomain.xml 1 0.0005 20.00% 0.0100 1.315

/ 1 0.0005 20.00% 0.0100 0.219

content.dl-rms.com 2 0.0010 3.28% 0.0100 1.165

/rms/11107/nodetag.js 1 0.0005 50.00% 0.0100 1.165

/dt/s/11107/s.js 1 0.0005 50.00% 0.0100 1.806

broadband.espn.go.com 1 0.0005 1.64% 0.0100 1.385

/espn360/util/espn360user?callback=jsonp1270661370297 1 0.0005 100.00% 0.0100 1.385

assets.espn.go.com 5 0.0025 8.20% 0.0400 0.806

/icons/watch.png 1 0.0005 20.00% 0.0100 0.838

/icons/video.png 1 0.0005 20.00% 0.0100 0.806

/icons/listen.png 1 0.0005 20.00% 0.0100 0.926

/icons/in.gif 1 0.0005 20.00% 0.0100 0.901

/i/in.gif 1 0.0005 20.00% 0.0100 0.901

adsatt.espn.go.com 4 0.0020 6.56% 0.0200 0.901

/ad/sponsors/utilities/flash\_v3005.js 1 0.0005 25.00% 0.0100 0.782

/ad/sponsors/ESPN\_Internet\_Ventures/Mar\_2010/es13-300x100-1291.jpg 1 0.0005 25.00% 0.0100 0.901

/ad/sponsors/ESPN\_Internet\_Ventures/Apr\_2010/es13-300x100-1344.jpg 1 0.0005 25.00% 0.0100 0.926

/ad/sponsors/ESPN\_In\_House\_Marketing/Mar\_2010/espn-300x250-3039.swf 1 0.0005 25.00% 0.0100 1.087

a2.espncdn.com 4 0.0020 6.56% 0.0300 0.590

/prod/assets/sn\_icon\_sprite\_40.png 1 0.0005 25.00% 0.0100 1.129

/prod/assets/master-07092009.png 1 0.0005 25.00% 0.0100 0.590

/prod/assets/gradient\_back.jpg 1 0.0005 25.00% 0.0100 0.636

/prod/assets/bg944-070909.png 1 0.0005 25.00% 0.0100 0.590

a1.espncdn.com 2 0.0010 3.28% 0.0200 0.590

/prod/assets/bg\_v2/bg\_frontpage\_red.jpg 1 0.0005 50.00% 0.0100 0.590

/prod/assets/bg\_v2/bg\_frontpage\_elements.jpg 1 0.0005 50.00% 0.0100 0.590

a.espncdn.com 31 0.0157 50.82% 0.1400 0.806

/webslices/icons/12x12.png 1 0.0005 3.23% 0.0100 0.818

/streak/logo\_sfc\_redesign.gif 1 0.0005 3.23% 0.0100 2.016

/streak/loader\_w.gif 1 0.0005 3.23% 0.0100 2.016

/streak/gradient\_back.jpg 1 0.0005 3.23% 0.0100 1.964

/streak/checks.gif 1 0.0005 3.23% 0.0100 2.019

/streak/SFC09\_playnow.jpg 1 0.0005 3.23% 0.0100 0.869

/prod/assets/totemPoll.swf 1 0.0005 3.23% 0.0100 1.161

/prod/assets/pollBtnActive.png 1 0.0005 3.23% 0.0100 1.542

/prod/assets/pollBtn.png 1 0.0005 3.23% 0.0100 1.468

/prod/assets/main\_search.gif 1 0.0005 3.23% 0.0100 0.817

/prod/assets/clear.png 1 0.0005 3.23% 0.0100 0.901

/prod/assets/carousel\_getflash\_111808.gif 1 0.0005 3.23% 0.0100 0.630

/photo/2010/0407/pga\_g\_furykkids\_576.jpg 1 0.0005 3.23% 0.0100 0.631

/photo/2010/0407/pga\_g\_furykkids\_134.jpg 1 0.0005 3.23% 0.0100 0.759

/photo/2010/0407/nfl\_a\_clausen\_sy\_134.jpg 1 0.0005 3.23% 0.0100 0.760

/photo/2010/0406/ncw\_g\_uconnSC\_134.jpg 1 0.0005 3.23% 0.0100 0.806

/photo/2010/0406/nba\_rookie50ts\_134.jpg 1 0.0005 3.23% 0.0100 0.901

/photo/2010/0405/trv\_detroit\_134.jpg 1 0.0005 3.23% 0.0100 0.902

/media/motion/2010/0407/dm\_100407\_sportscience\_hayward\_thumdnail\_wbig.jpg 1 0.0005 3.23% 0.0100 0.902

/media/motion/2010/0407/dm\_100407\_nfl\_schefter\_haynesworth\_thumdnail\_wbig.jpg 1 0.0005 3.23% 0.0100 0.782

/media/motion/2010/0405/TNR\_Ep2\_Big\_Papi\_APR5\_thumdnail\_wbig.jpg 1 0.0005 3.23% 0.0100 0.902

/insertfiles/javascript/wa/sOmni.js 1 0.0005 3.23% 0.0100 2.017

/icons/watch.png 1 0.0005 3.23% 0.0100 0.902

/icons/listen.png 1 0.0005 3.23% 0.0100 0.860

/icons/in.gif 1 0.0005 3.23% 0.0100 0.819

/i/teamlogos/ncaa/50x50/41.png 1 0.0005 3.23% 0.0100 1.129

/i/columnists/simmons\_bill\_35fp.jpg 1 0.0005 3.23% 0.0100 0.859

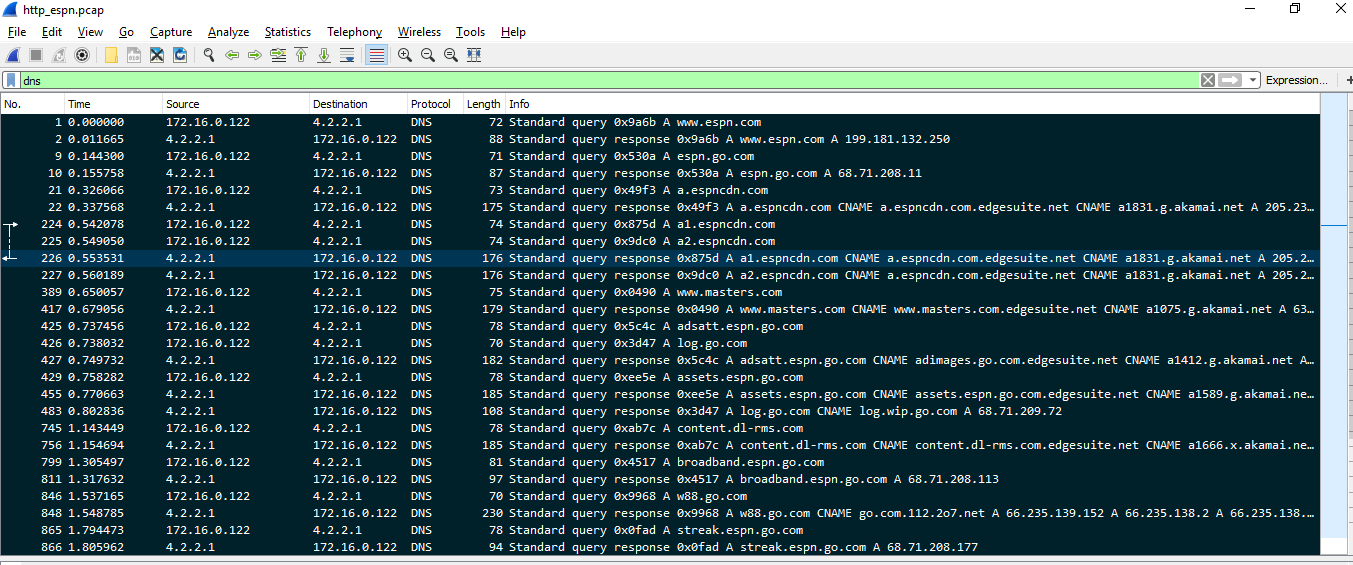
/i/columnists/reilly\_rick\_35fp.jpg 1 0.0005 3.23% 0.0100 0.863

/combiner/c?v=201004021838&js=jquery-1.3.2.js,plugins/json2.js,plugins/teacrypt.js,plugins/jquery.metadata.js,plugins/jquery.bgiframe.js,plugins/jquery.easing.1.3.js,plugins/jquery.hoverIntent.js,plugins/jquery.jcarousel.js,plugins/jquery.tinysort.js,plugins/jquery.pubsub.js,ui/1.7.2/ui.core.js,ui/1.7.2/ui.tabs.js,plugins/ba-debug-0.3.js,espn.l10n.r3.js,swfobject/2.2/swfobject.js,flashObjWrapper.r5.js,espn.core.duo.r24.js,espn.storage.3.js,espn.p13n.r5.js,espn.video.r14.js,espn.insider.r3.js,espn.espn360.stub.r6.js,espn.myHeadlines.stub.r4.js,espn.myfaves.stub.r3.js,%2Fespn%2Fespn%2Fjavascript%2Ffrontpage\_scoreboard,registration/myEspn.201003231022.js,registration%2FstaticLogin.201004011014.js&debug=false 1 0.0005 3.23% 0.0100 0.358

/combiner/c?v=201003241632&css=base.201003241632.css,modules.201003241633.css,modules/insider\_enhanced.200910131831.css,modules/mem\_espn360.200910131831.css,sn\_icon\_sprite.200907150955.css,master\_sprite.200907231718.css,/espn/espn/styles/frontpage\_scoreboard 1 0.0005 3.23% 0.0100 0.358

/combiner/c?js=analytics/sOmni.js,analytics/analytics.js&xhr=1 1 0.0005 3.23% 0.0100 1.306

**List of DNS Requests:**



The HTTP requests coincide with the DNS Requests made

For Eg:

1. DNS Query [www.masters.com](http://www.masters.com) Resources downloaded by HTTP : /mas/js/external\_alc.js
2. DNS Query games-ak.espn.go.com Resources downloaded /s/minigames/i/page1/logo\_fantasy\_flb\_80x80.png

7.Analyze the first three HTTP packets (use an http filter) and explain what happened?

**Ans:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HTTP Requests by HTTP Host | Count | Rate (ms) | Percent | Burst rate | Burst start |
| www.masters.com | 1 | 0.0005 | 1.64% | 0.01 | 0.69 |
| /mas/js/external\_alc.js | 1 | 0.0005 | 100.00% | 0.01 | 0.69 |
| streak.espn.go.com | 1 | 0.0005 | 1.64% | 0.01 | 0 |
| /format/modules/front09v2/streakModule | 1 | 0.0005 | 100.00% | 0.01 | 0 |
| games-ak.espn.go.com | 1 | 0.0005 | 1.64% | 0.01 | 2.036 |
| /s/minigames/i/page1/logo\_fantasy\_flb\_80x80.png | 1 | 0.0005 | 100.00% | 0.01 | 2.036 |

**Count:** Refers to the no of requests

**Rate:** Refers to the Rate at which is responded

**Burst Rate:** Refers to the maximum no of packets sent per interval of time

**Burst Start:** Refers to the time when the maximum packets transferred occurred

8.Go back to the conversations feature in the Statistics menu. Using only the information provided by this function, identify:

**Ans:**

1. the MAC and IP addresses of the local machine where the trace was captured

**MAC: 00:21:70:c0:56:f0**

**IP Address: 172.16.0.122**

b. the IP address of the local dns server: 4.2.2.1

c. the addresses IP of web servers

[www.espn.com](http://www.espn.com) -→199.181.132.250

[www.espn.go.com](http://www.espn.go.com) →68.71.208.11

[www.a.espncdn.com](http://www.a.espncdn.com) → redirected to Akamai.net 63.85.36.8

[www.masters.com](http://www.masters.com) → redirected to Akamai.net 63.85.36.49

[www.assets.espn.go.com.edgesuite.net](http://www.assets.espn.go.com.edgesuite.net) → redirected to Akamai.net 205.234.218.129

[www.log.go.com](http://www.log.go.com) -→ 68.71.209.72

[www.content.dl-rms.com.edgesuite.net](http://www.content.dl-rms.com.edgesuite.net) -→ redirected to Akamai.net

**Justify your answers.**

**Finally, why are there only two MAC addresses involved in all exchanges? Who owns the other MAC address?**

There are only two MAC address because each network interface in a computer can have unique address as in our case the Source MAC address from where the request is sent and the MAC address of the destination server(router) which responds.

Here on of the MAC address is from the source machine where the connection to ESPN is established , so one of them is for the browser where the client requests and the other one is the destination MAC address of the ESPN server(router).