Computer Networks-Assignment 3

Written by Akilesh B CS13B1042

September 4, 2015

1.1 nslookup

1. nslookup for google.co.in

Non-authoritative answer:
Name: google.co.in
Address: 216.58.196.99

2. nslookup for determining authoritative DNS server of Georgia tech (gatech.edu)

main name server : brahma5.dns.gatech.edu

all authoritative servers: including backup servers
gatech.edu nameserver = dns3.gatech.edu.
gatech.edu nameserver = dns2.gatech.edu.
gatech.edu nameserver = dns1.gatech.edu.

1.3 Tracing DNS for web browsing

To clear local DNS cache => *nscd -i hosts*

1. DNS query and response messages are sent over UDP.

2. Destination port of DNS query message is 53 and Source port of DNS response message is 53.

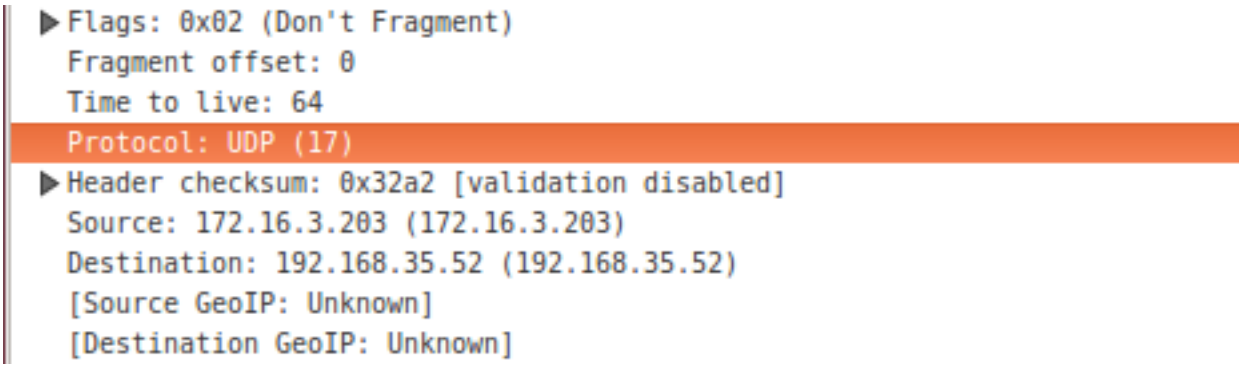
3. Destination IP address of DNS query message is 192.168.35.52
IP address of local DNS server can be determined by cat /etc/resolv.conf This also gives 192.168.35.52
Yes, both the IP addresses are the same.

4. DNS query message is of type 'A'. No, the query message does not contain any answers. Answer RRs is 0, Authority RRs is 0, Additional RRs is 0.

5. DNS response message contains the following answers. Answer RRs is 3, Authority RRs is 2, Additional RRs is 2.
Answer RRs contain Name, Type, Class, Time to live, Data length, Addr. One answer is of type CNAME which is Canonical name for an alias. Other two answers are of type A. Authoritative answers are of type NS. Time to live indicates how long will it live in the DNS cache before being erased.

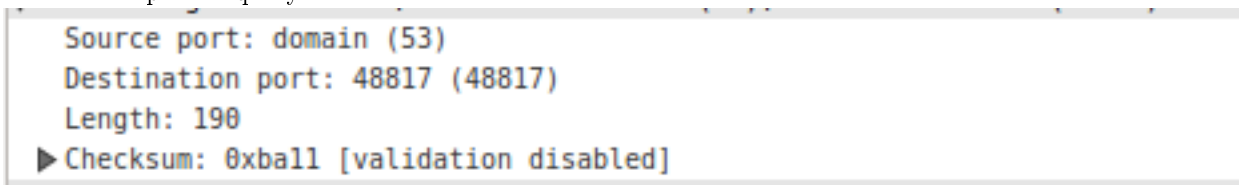
6. Yes, subsequent TCP SYN packet sent by my host contain the IP address provided in the DNS response message
It was sent from 172.16.3.203 to 104.20.0.85

7. No, the images are all loaded, retrieved from www.ietf.org, so no additional DNS queries are necessary (the host uses a cached address).

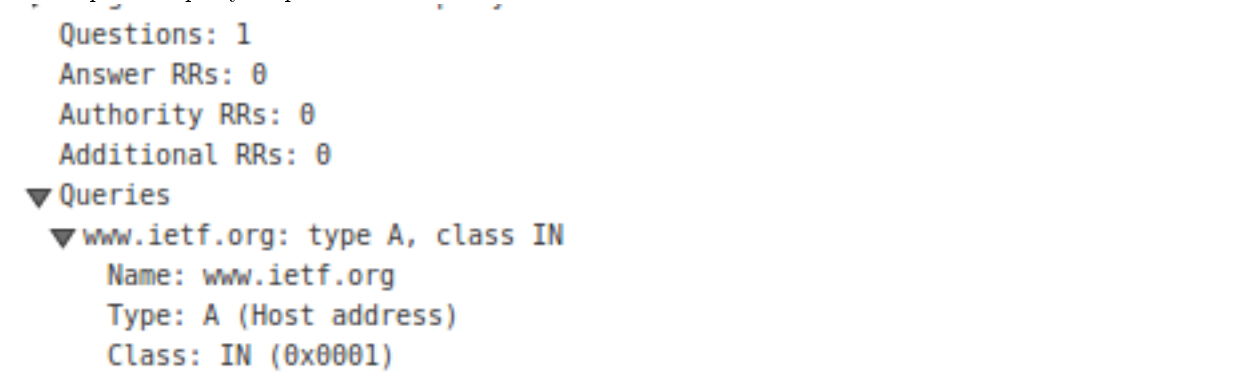


Protocol is UDP

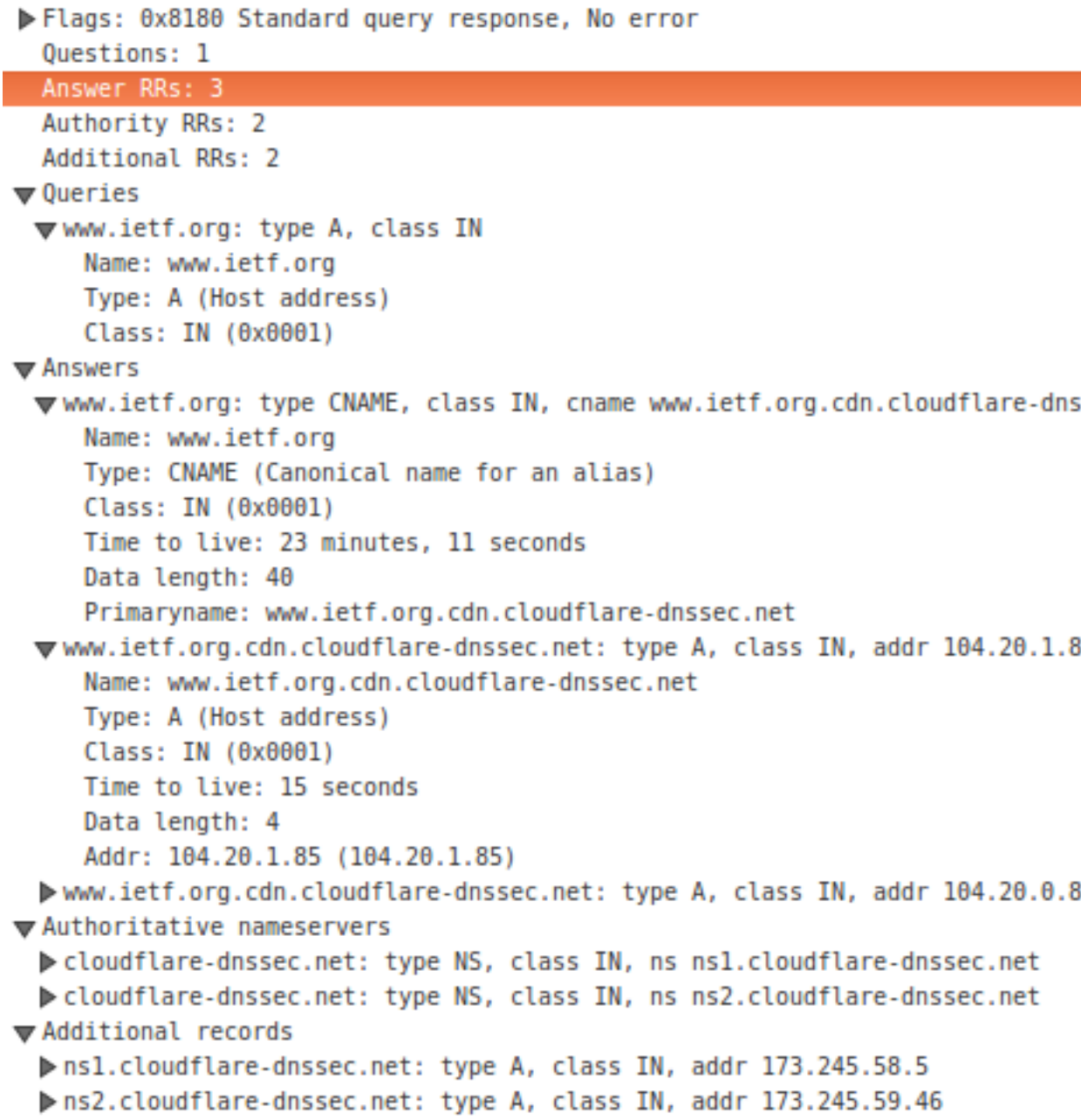
Destination port of query.



Source port of query response



DNS query.



DNS query response

1.4 Tracing DNS for nslookup

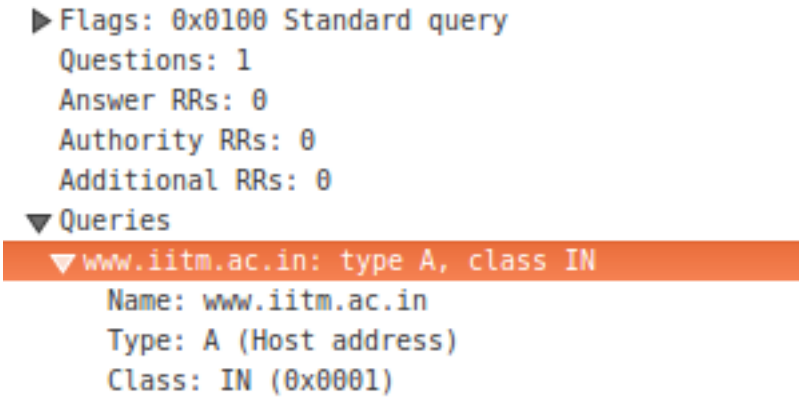
nslookup was done on www.iitm.ac.in => *nslookup www.iitm.ac.in*

1. Destination port of DNS query message is 53 and Source port of DNS response message is 53.

2. Destination IP address of DNS query message is 192.168.35.52
IP address of local DNS server can be determined by cat /etc/resolv.conf This also gives 192.168.35.52
Yes, both the IP addresses are the same.

3. DNS query message is of type 'A' . No, the query message does not contain any answers. Answer RRs is 0, Authority RRs is 0, Additional RRs is 0.

4. DNS response message contains the following answers. Answer RRs is 2, Authority RRs is 3, Additional RRs is 3. Answer RRs contain Name, Type, Class, Time to live, Data length, Primary name / Addr. One is of type CNAME (Canonical name for an alias) and the other is of type A (Host address). Authoritative RRs contain Name, Type, Class, Time to live, Data length, Name server. Type is NS where as Name server is dns2.iitm.ac.in etc.



DNS query

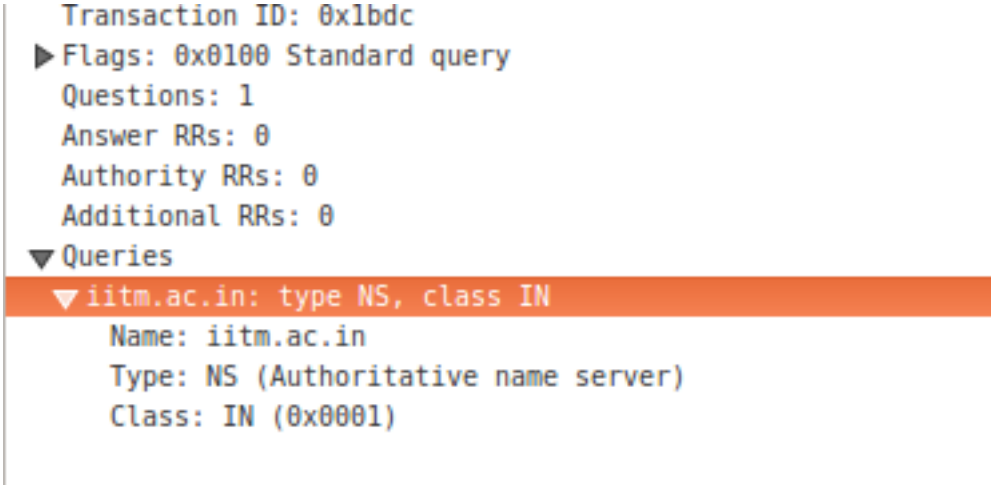
```
  Answer RRs: 2
  Authority RRs: 3
  Additional RRs: 3
▼ Queries
  ▼ www.iitm.ac.in: type A, class IN
      Name: www.iitm.ac.in
      Type: A (Host address)
      Class: IN (0x0001)
▼ Answers
  ▼ www.iitm.ac.in: type CNAME, class IN, cname iitmwww.iitm.ac.in
      Name: www.iitm.ac.in
      Type: CNAME (Canonical name for an alias)
      Class: IN (0x0001)
      Time to live: 3 hours, 59 minutes, 53 seconds
      Data length: 10
      Primaryname: iitmwww.iitm.ac.in
  ▼ iitmwww.iitm.ac.in: type A, class IN, addr 203.199.213.13
      Name: iitmwww.iitm.ac.in
      Type: A (Host address)
      Class: IN (0x0001)
      Time to live: 3 hours, 59 minutes, 53 seconds
      Data length: 4
      Addr: 203.199.213.13 (203.199.213.13)
▼ Authoritative nameservers
  ▼ iitm.ac.in: type NS, class IN, ns dns2.iitm.ac.in
      Name: iitm.ac.in
      Type: NS (Authoritative name server)
      Class: IN (0x0001)
      Time to live: 3 hours, 38 minutes, 25 seconds
      Data length: 7
      Name Server: dns2.iitm.ac.in
  ▼ iitm.ac.in: type NS, class IN, ns dns1.iitm.ac.in
      Name: iitm.ac.in
      Type: NS (Authoritative name server)
      Class: IN (0x0001)
      Time to live: 3 hours, 38 minutes, 25 seconds
      Data length: 7
      Name Server: dns1.iitm.ac.in
  ▼ iitm.ac.in: type NS, class IN, ns dns3.iitm.ac.in
      Name: iitm.ac.in
      Type: NS (Authoritative name server)
      Class: IN (0x0001)
      Time to live: 3 hours, 38 minutes, 25 seconds
      Data length: 7
```

DNS query response
Subpart: When we do *nslookup -type=NS www.iitm.ac.in*

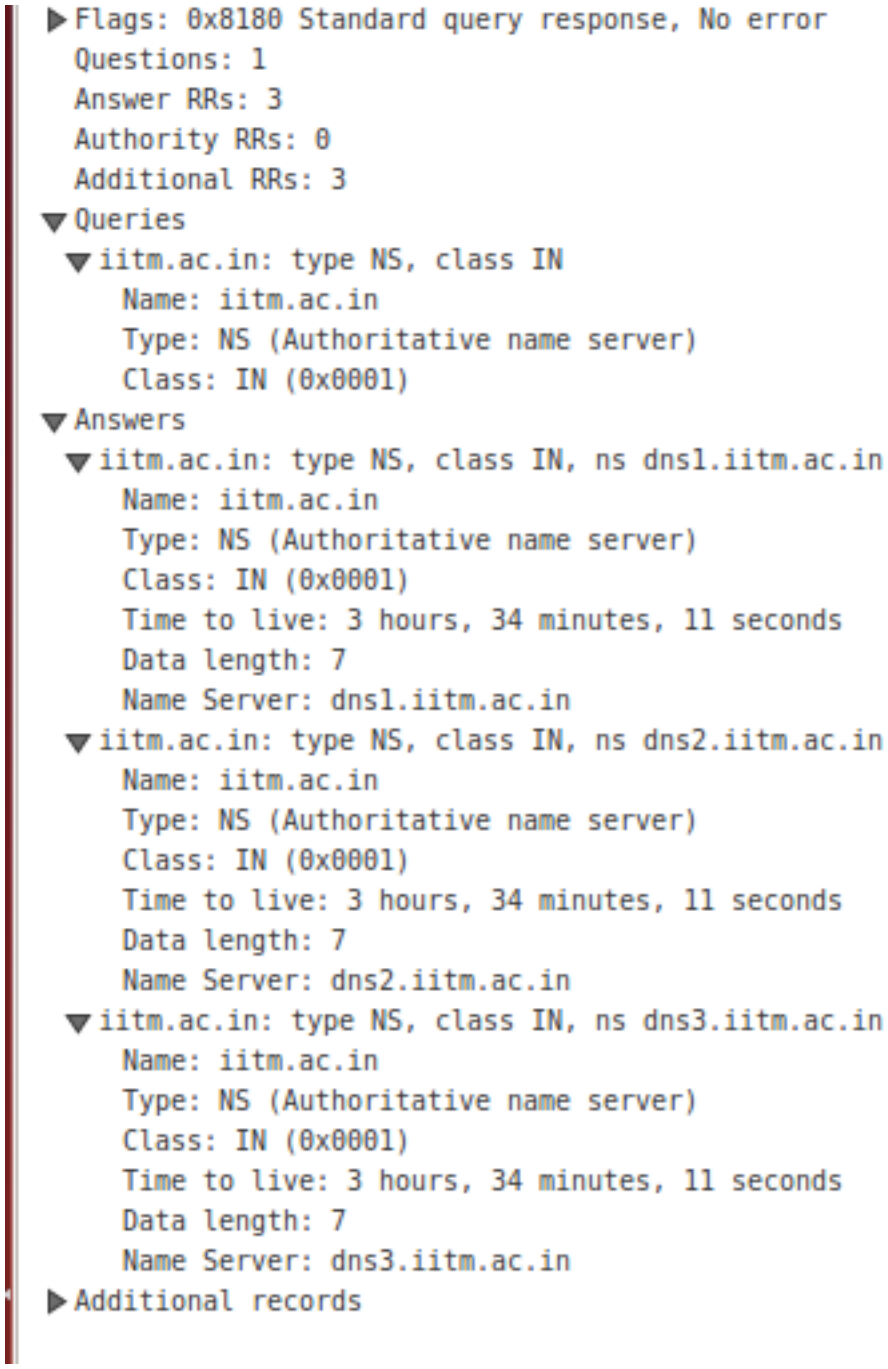
1. The DNS query message is sent to 192.168.35.52 which is also the IP address of local DNS server. Yes, both the IP address are the same.

2. The DNS query message is of type NS. No, the query message does not contain any answers. Answer RRs is 0, Authority RRs is 0, Additional RRs is 0.

3. The DNS response message provides the following IITM nameservers : dns1.iitm.ac.in, dns.iitm.ac.in, dns3.iitm.ac.in Answer RRs is 3, Authority RRs is 0, Additional RRs is 3. Answer RRs does not provide the IP address of the IITM name servers where as Additional record RRs contain the IP address of the name server.



DNS query



DNS query response

Part 2: HTTP

2.1: The Basic HTTP GET/Response interaction

This was done on www.iith.ac.in/~antony/CS3040/

1. Both the browser and server are running HTTP 1.1

2. Accept-language : en-US, en.

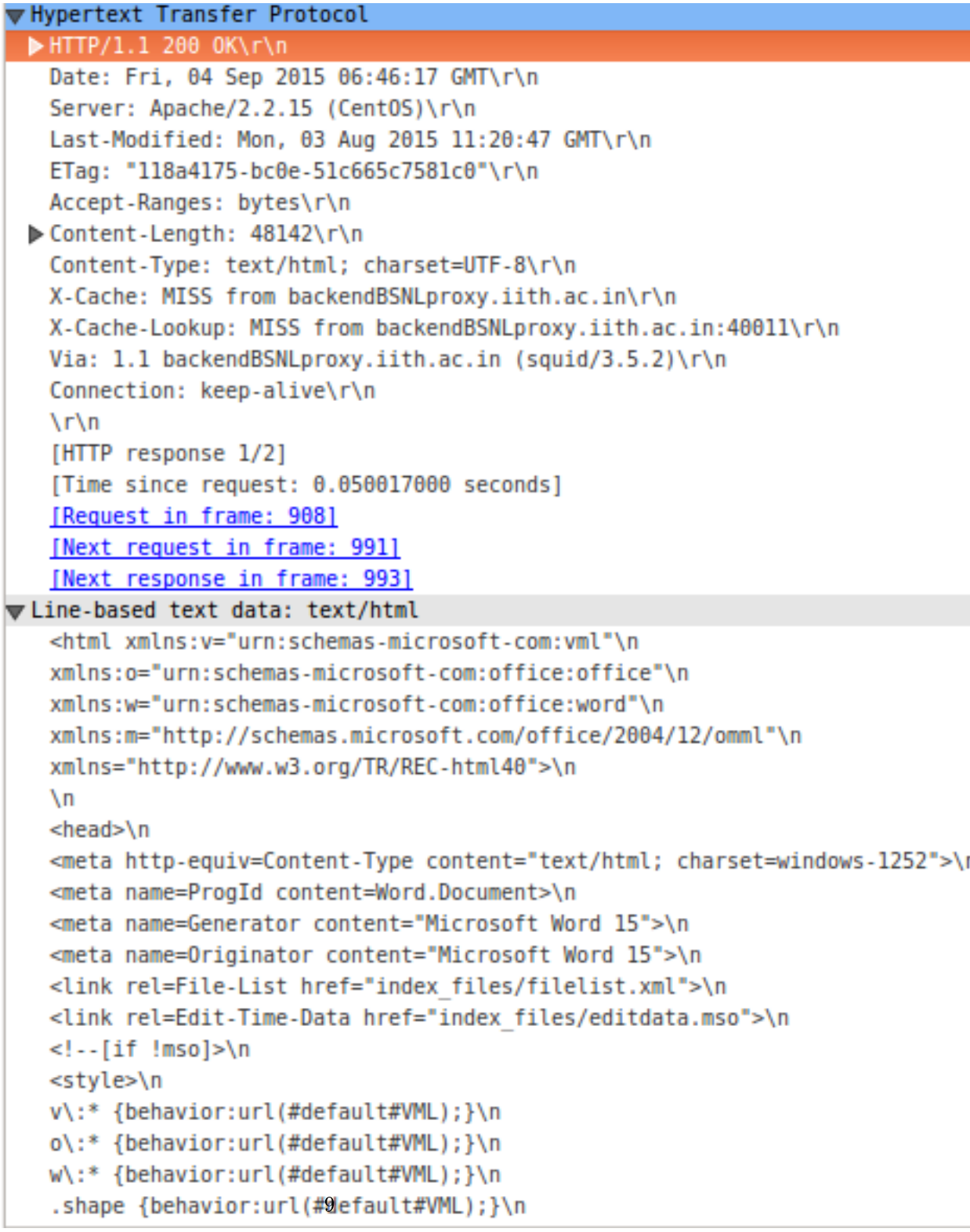
3. IP address of my computer is 172.16.3.203 and IP address of iith.ac.in server is 192.168.35.5 (this proxy was used when iith.ac.in was obtained).

4. Status code returned is HTTP/1.1 200 OK (text/html).

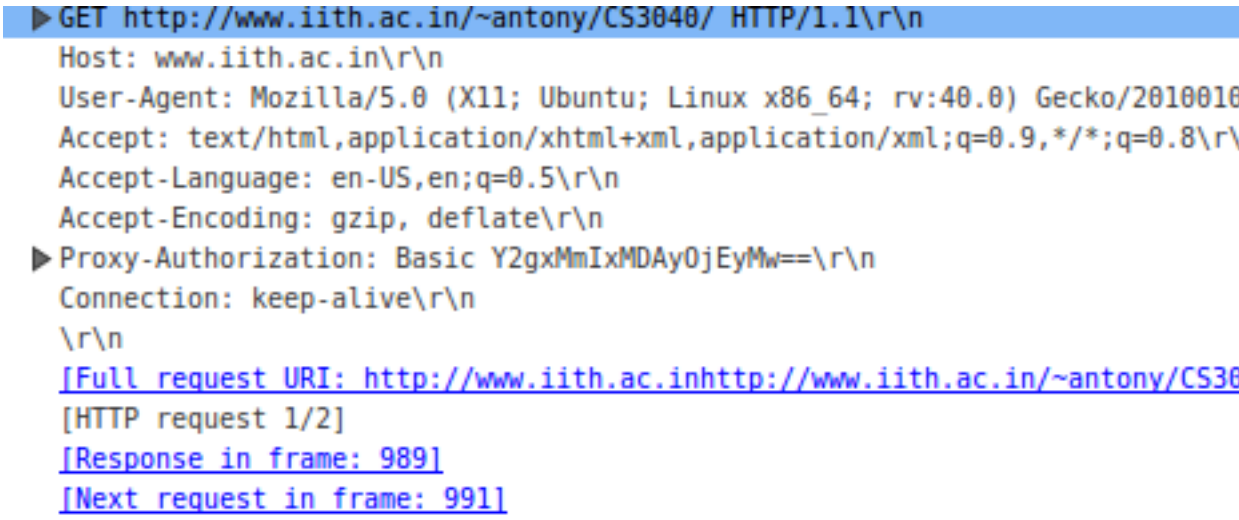
5. HTML file was last modified on: Mon, 03 Aug 2015 11:20:47 GMT

6. Content length is 48142 bytes.

7. No, all the headers can be found in the raw data.


Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Fri, 04 Sep 2015 06:46:17 GMT\r\n
Server: Apache/2.2.15 (CentOS)\r\n
Last-Modified: Mon, 03 Aug 2015 11:20:47 GMT\r\n
ETag: "118a4175-bc0e-51c665c7581c0"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 48142\r\n
Content-Type: text/html; charset=UTF-8\r\n
X-Cache: MISS from backendBSNLproxy.iith.ac.in\r\n
X-Cache-Lookup: MISS from backendBSNLproxy.iith.ac.in:40011\r\n
Via: 1.1 backendBSNLproxy.iith.ac.in (squid/3.5.2)\r\n
Connection: keep-alive\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.050017000 seconds]
[Request in frame: 908]
[Next request in frame: 991]
[Next response in frame: 993]
Line-based text data: text/html
<html xmlns:v="urn:schemas-microsoft-com:vml"\n
xmlns:o="urn:schemas-microsoft-com:office:office"\n
xmlns:w="urn:schemas-microsoft-com:office:word"\n
xmlns:m="http://schemas.microsoft.com/office/2004/12/omml"\n
xmlns="http://www.w3.org/TR/REC-html40">\n
\n
<head>\n
<meta http-equiv=Content-Type content="text/html; charset=windows-1252">\n
<meta name=ProgId content=Word.Document>\n
<meta name=Generator content="Microsoft Word 15">\n
<meta name=Originator content="Microsoft Word 15">\n
<link rel=File-List href="index_files/filelist.xml">\n
<link rel=Edit-Time-Data href="index_files/editdata.mso">\n
<!--[if !mso]>\n
<style>\n
v\:* {behavior:url(#default#VML);}\n
o\:* {behavior:url(#default#VML);}\n
w\:* {behavior:url(#default#VML);}\n
.shape {behavior:url(#default#VML);}\n

HTTP/1.1 200 OK



GET

2.2: HTTP conditional GET/Response interaction

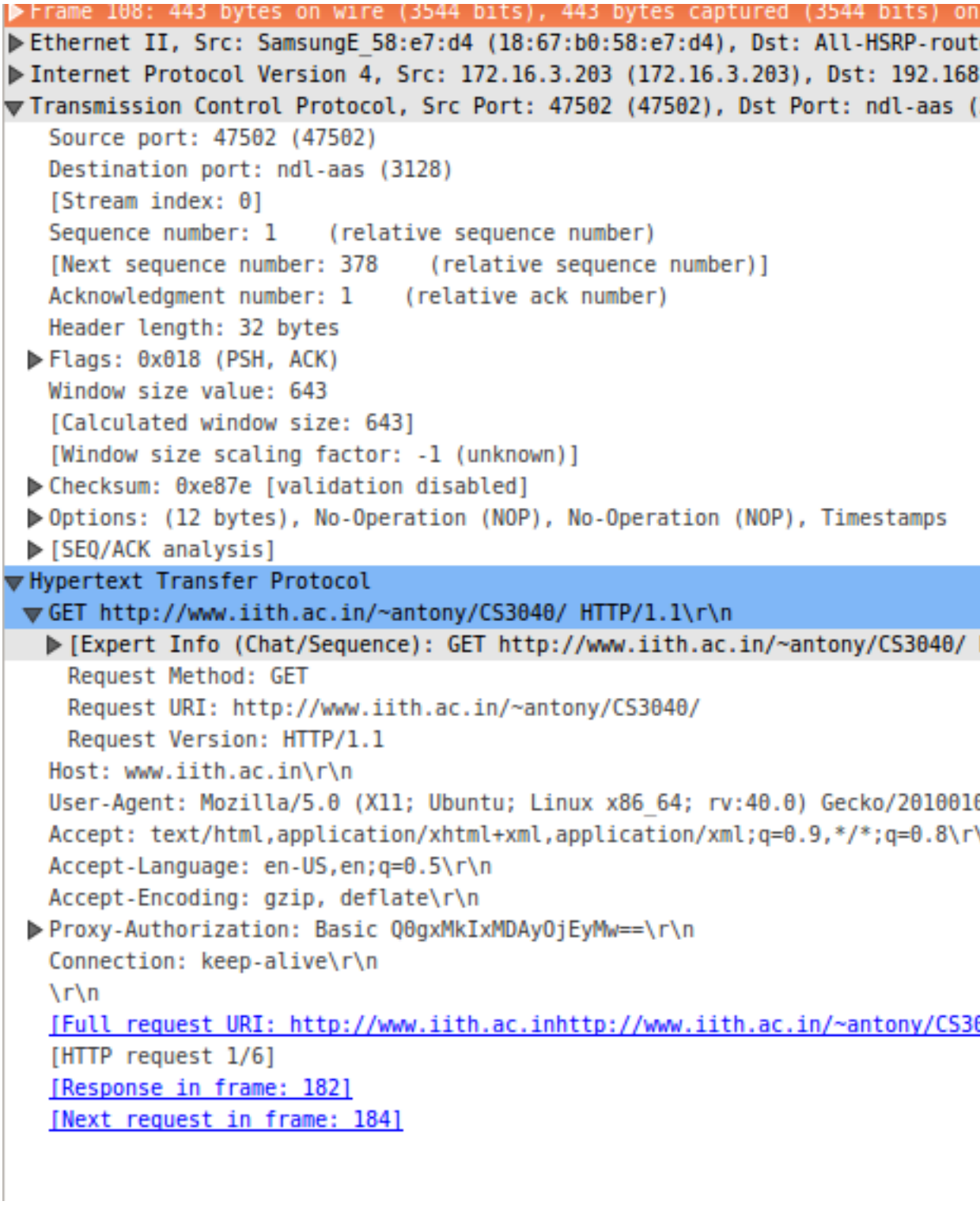
This was done on www.iith.ac.in/~antony/CS3040/

1. No. IF-MODIFIED-SINCE line is not present in HTTP GET.

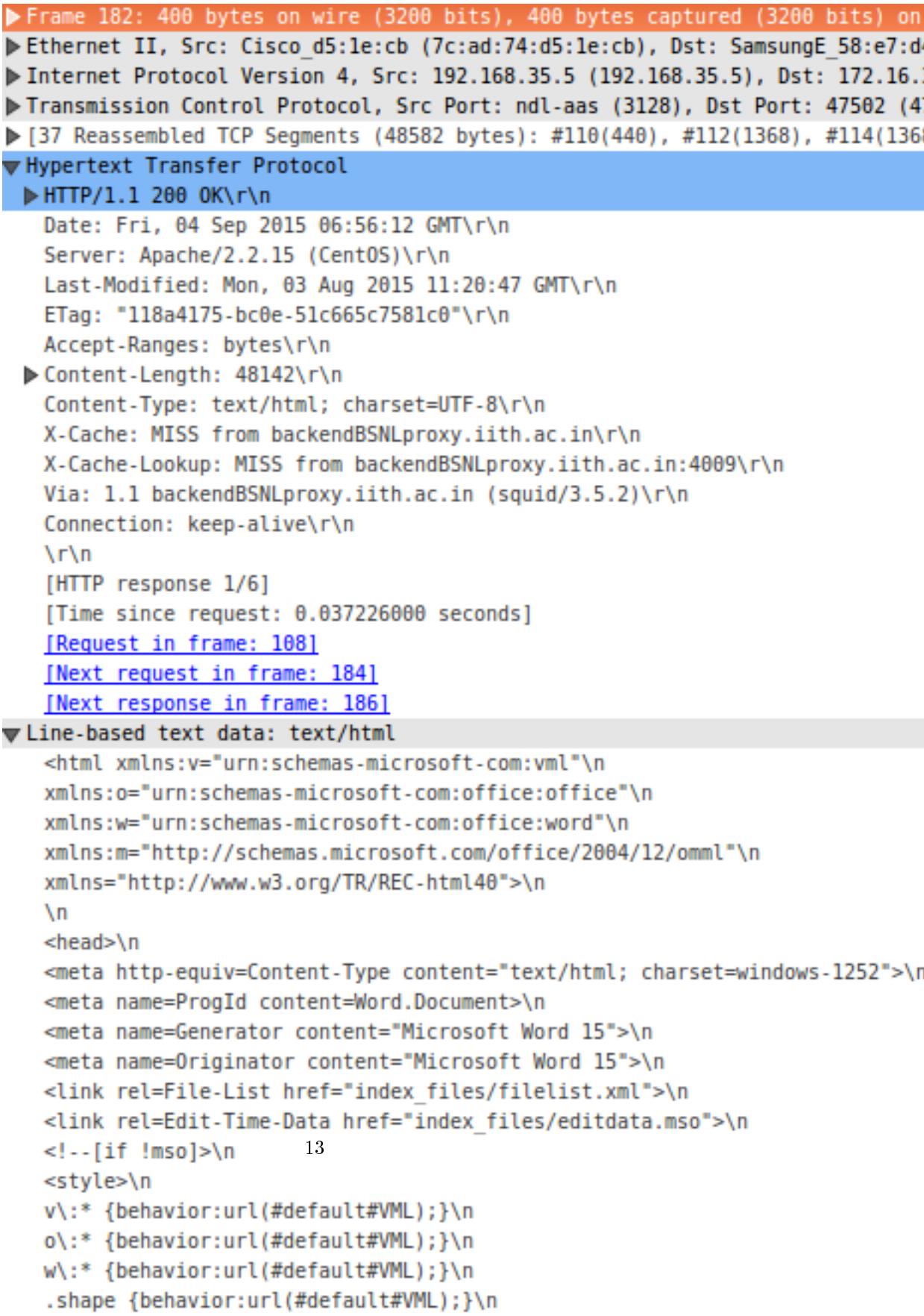
2. Yes, the server explicitly returns the contents of the file. It is because we see the contents in *Line-based text data* field.

3. Yes. The information followed is: *Mon, 03 Aug 2015 11:20:47 GMT|r|n* which is the date of last modification of the file from the previous get request.

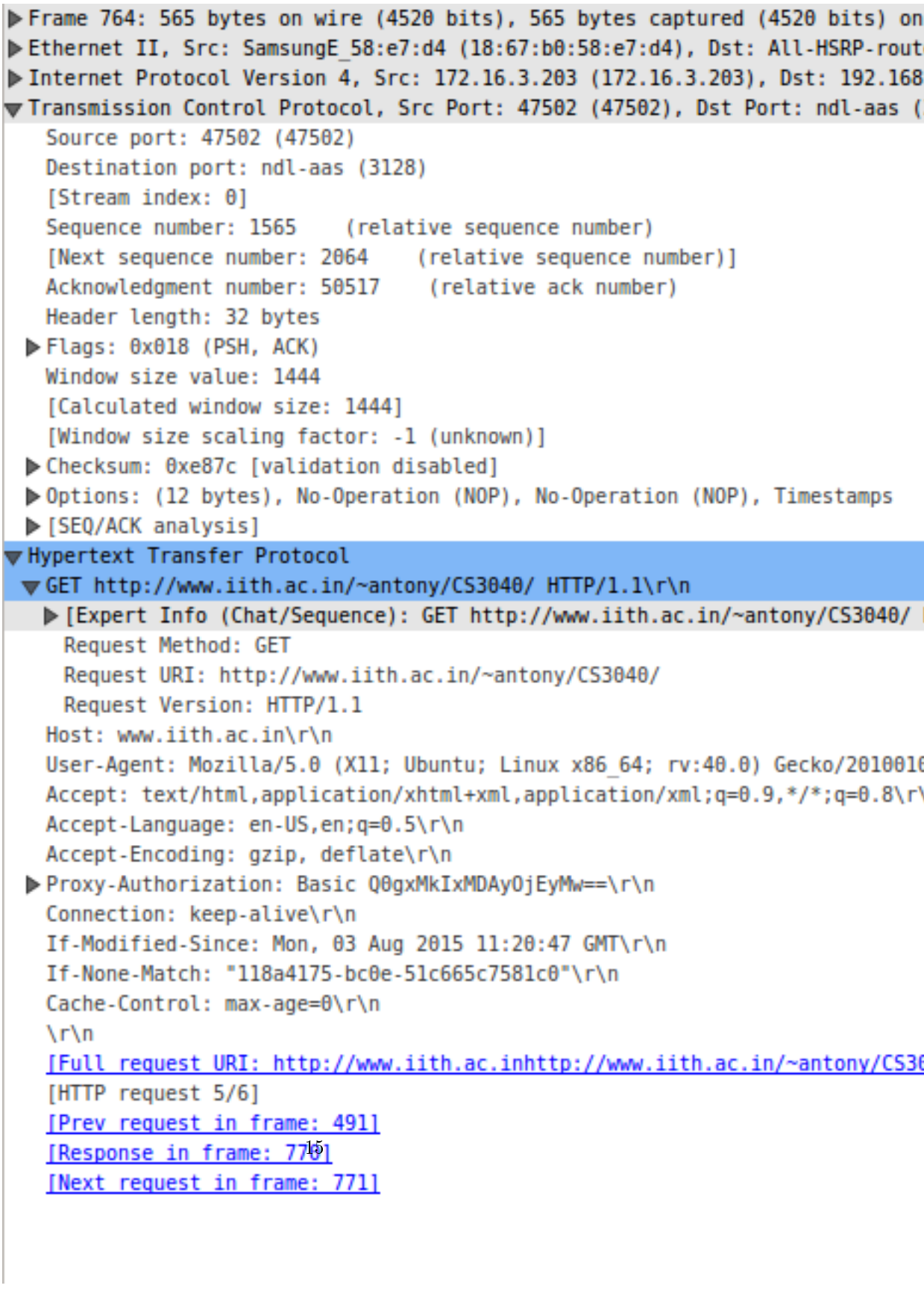
4. The status code and the corresponding phrase returned from the server is *HTTP/1.1 304 Not Modified*. The server didn't return the contents of the page since the browser loaded it from its cache.


Frame 108: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on
Ethernet II, Src: SamsungE_58:e7:d4 (18:67:b0:58:e7:d4), Dst: All-HSRP-rout
Internet Protocol Version 4, Src: 172.16.3.203 (172.16.3.203), Dst: 192.168
Transmission Control Protocol, Src Port: 47502 (47502), Dst Port: ndl-aas (
Source port: 47502 (47502)
Destination port: ndl-aas (3128)
[Stream index: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 378 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header length: 32 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 643
[Calculated window size: 643]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xe87e [validation disabled]
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
Hypertext Transfer Protocol
GET http://www.iith.ac.in/~antony/CS3040/ HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET http://www.iith.ac.in/~antony/CS3040/
Request Method: GET
Request URI: http://www.iith.ac.in/~antony/CS3040/
Request Version: HTTP/1.1
Host: www.iith.ac.in\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/2010010
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Proxy-Authorization: Basic Q0gxMkIxMDAyOjEyMw==\r\n
Connection: keep-alive\r\n
\r\n
[Full request URI: http://www.iith.ac.inhttp://www.iith.ac.in/~antony/CS30
[HTTP request 1/6]
[Response in frame: 182]
[Next request in frame: 184]

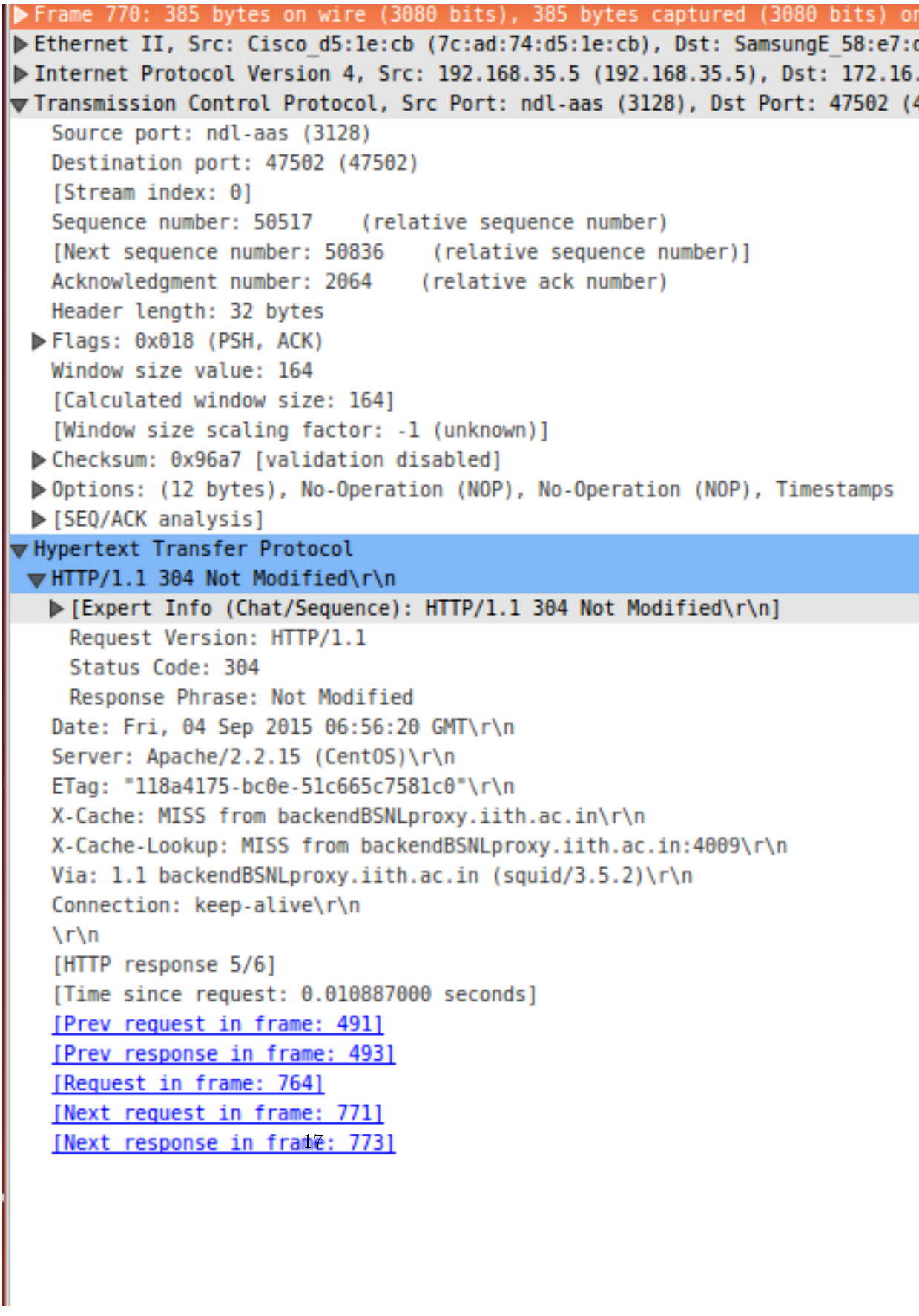
First GET


Frame 182: 400 bytes on wire (3200 bits), 400 bytes captured (3200 bits) on
Ethernet II, Src: Cisco_d5:1e:cb (7c:ad:74:d5:1e:cb), Dst: SamsungE_58:e7:d
Internet Protocol Version 4, Src: 192.168.35.5 (192.168.35.5), Dst: 172.16.
Transmission Control Protocol, Src Port: ndl-aas (3128), Dst Port: 47502 (4
[37 Reassembled TCP Segments (48582 bytes): #110(440), #112(1368), #114(136
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Fri, 04 Sep 2015 06:56:12 GMT\r\n
Server: Apache/2.2.15 (CentOS)\r\n
Last-Modified: Mon, 03 Aug 2015 11:20:47 GMT\r\n
ETag: "118a4175-bc0e-51c665c7581c0"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 48142\r\n
Content-Type: text/html; charset=UTF-8\r\n
X-Cache: MISS from backendBSNLproxy.iith.ac.in\r\n
X-Cache-Lookup: MISS from backendBSNLproxy.iith.ac.in:4009\r\n
Via: 1.1 backendBSNLproxy.iith.ac.in (squid/3.5.2)\r\n
Connection: keep-alive\r\n
\r\n
[HTTP response 1/6]
[Time since request: 0.037226000 seconds]
[Request in frame: 108]
[Next request in frame: 184]
[Next response in frame: 186]
Line-based text data: text/html
<html xmlns:v="urn:schemas-microsoft-com:vml"\n
xmlns:o="urn:schemas-microsoft-com:office:office"\n
xmlns:w="urn:schemas-microsoft-com:office:word"\n
xmlns:m="http://schemas.microsoft.com/office/2004/12/omml"\n
xmlns="http://www.w3.org/TR/REC-html40">\n
\n
<head>\n
<meta http-equiv=Content-Type content="text/html; charset=windows-1252">\n
<meta name=ProgId content=Word.Document>\n
<meta name=Generator content="Microsoft Word 15">\n
<meta name=Originator content="Microsoft Word 15">\n
<link rel=File-List href="index_files/filelist.xml">\n
<link rel=Edit-Time-Data href="index_files/editdata.mso">\n
<!--[if !mso]>\n
<style>\n
v\:* {behavior:url(#default#VML);}\n
o\:* {behavior:url(#default#VML);}\n
w\:* {behavior:url(#default#VML);}\n
.shape {behavior:url(#default#VML);}\n

First GET response having HTTP/1.1 200 OK


▶ Frame 764: 565 bytes on wire (4520 bits), 565 bytes captured (4520 bits) on
▶ Ethernet II, Src: SamsungE_58:e7:d4 (18:67:b0:58:e7:d4), Dst: All-HSRP-rout
▶ Internet Protocol Version 4, Src: 172.16.3.203 (172.16.3.203), Dst: 192.168
▼ Transmission Control Protocol, Src Port: 47502 (47502), Dst Port: ndl-aas (
Source port: 47502 (47502)
Destination port: ndl-aas (3128)
[Stream index: 0]
Sequence number: 1565 (relative sequence number)
[Next sequence number: 2064 (relative sequence number)]
Acknowledgment number: 50517 (relative ack number)
Header length: 32 bytes
▶ Flags: 0x018 (PSH, ACK)
Window size value: 1444
[Calculated window size: 1444]
[Window size scaling factor: -1 (unknown)]
▶ Checksum: 0xe87c [validation disabled]
▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▶ [SEQ/ACK analysis]
▼ Hypertext Transfer Protocol
▼ GET http://www.iith.ac.in/~antony/CS3040/ HTTP/1.1\r\n
▶ [Expert Info (Chat/Sequence): GET http://www.iith.ac.in/~antony/CS3040/
Request Method: GET
Request URI: http://www.iith.ac.in/~antony/CS3040/
Request Version: HTTP/1.1
Host: www.iith.ac.in\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:40.0) Gecko/2010010
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
▶ Proxy-Authorization: Basic Q0gxMkIxMDAyOjEyMw==\r\n
Connection: keep-alive\r\n
If-Modified-Since: Mon, 03 Aug 2015 11:20:47 GMT\r\n
If-None-Match: "118a4175-bc0e-51c665c7581c0"\r\n
Cache-Control: max-age=0\r\n
\r\n
[Full request URI: http://www.iith.ac.inhttp://www.iith.ac.in/~antony/CS30
[HTTP request 5/6]
[Prev request in frame: 491]
[Response in frame: 770]
[Next request in frame: 771]

Second GET


Frame 770: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits) on
Ethernet II, Src: Cisco_d5:1e:cb (7c:ad:74:d5:1e:cb), Dst: SamsungE_58:e7:c
Internet Protocol Version 4, Src: 192.168.35.5 (192.168.35.5), Dst: 172.16.
Transmission Control Protocol, Src Port: ndl-aas (3128), Dst Port: 47502 (4
Source port: ndl-aas (3128)
Destination port: 47502 (47502)
[Stream index: 0]
Sequence number: 50517 (relative sequence number)
[Next sequence number: 50836 (relative sequence number)]
Acknowledgment number: 2064 (relative ack number)
Header length: 32 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 164
[Calculated window size: 164]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x96a7 [validation disabled]
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
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: Fri, 04 Sep 2015 06:56:20 GMT\r\n
Server: Apache/2.2.15 (CentOS)\r\n
ETag: "118a4175-bc0e-51c665c7581c0"\r\n
X-Cache: MISS from backendBSNLproxy.iith.ac.in\r\n
X-Cache-Lookup: MISS from backendBSNLproxy.iith.ac.in:4009\r\n
Via: 1.1 backendBSNLproxy.iith.ac.in (squid/3.5.2)\r\n
Connection: keep-alive\r\n
\r\n
[HTTP response 5/6]
[Time since request: 0.010887000 seconds]
[Prev request in frame: 491]
[Prev response in frame: 493]
[Request in frame: 764]
[Next request in frame: 771]
[Next response in frame: 773]

Second GET response with HTTP/1.1 304 Not Modified

2.3: Retrieving Long documents

This was done on http://www.ietf.org/rfc/rfc2616.txt

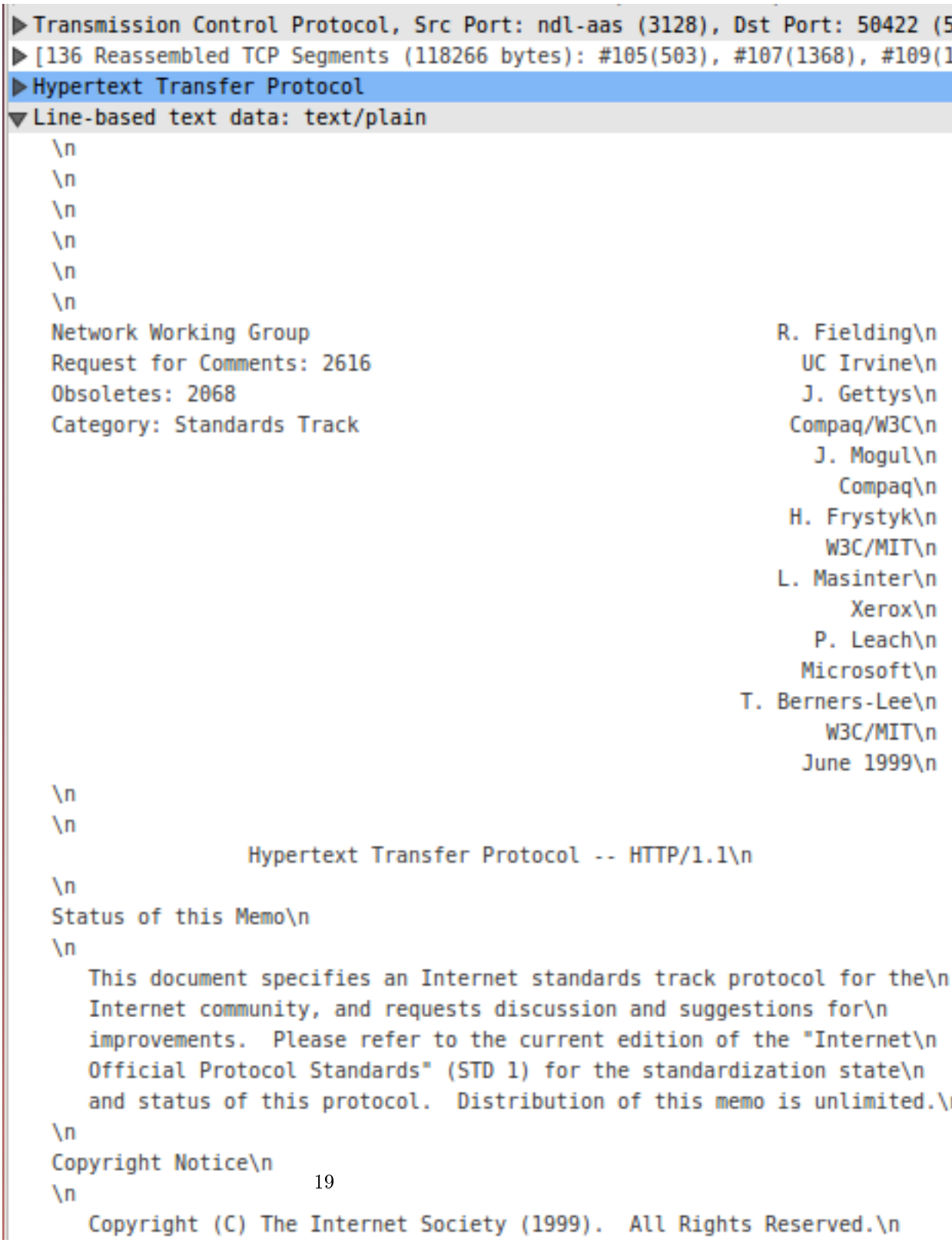
1. There were 2 HTTP GET request message sent by my browser (shown in the screen shot).

2. There were 136 reassembled TCP segments carrying a total of 118266 bytes.

3. The status code and phrase of first GET was HTTP/1.1 200 OK (text/plain) and that of second is HTTP/1.1 200 OK (image/x-icon).

4. No, there are no HTTP status lines in the transmitted data associated with a TCP induced "Continuation" .

65	1.047680000	172.16.3.203	192.168.35.5
414	2.648203000	192.168.35.5	172.16.3.203
416	2.709999000	172.16.3.203	192.168.35.5
466	2.943844000	192.168.35.5	172.16.3.203


▶ Transmission Control Protocol, Src Port: ndl-aas (3128), Dst Port: 50422 (5
▶ [136 Reassembled TCP Segments (118266 bytes): #105(503), #107(1368), #109(1
▶ Hypertext Transfer Protocol
▼ Line-based text data: text/plain
\n
\n
\n
\n
\n
\n
Network Working Group R. Fielding\n
Request for Comments: 2616 UC Irvine\n
Obsoletes: 2068 J. Gettys\n
Category: Standards Track Compaq/W3C\n
J. Mogul\n
Compaq\n
H. Frystyk\n
W3C/MIT\n
L. Masinter\n
Xerox\n
P. Leach\n
Microsoft\n
T. Berners-Lee\n
W3C/MIT\n
June 1999\n
\n
\n
Hypertext Transfer Protocol -- HTTP/1.1\n
\n
Status of this Memo\n
\n
This document specifies an Internet standards track protocol for the\n
Internet community, and requests discussion and suggestions for\n
improvements. Please refer to the current edition of the "Internet\n
Official Protocol Standards" (STD 1) for the standardization state\n
and status of this protocol. Distribution of this memo is unlimited.\
\n
Copyright Notice\n
\n
Copyright (C) The Internet Society (1999). All Rights Reserved.\n

136 reassembled TCP segments.

2.4: HTML Documents with Embedded objects

This was done on www.cricbuzz.com

1. 92 HTTP GET requests were sent by my browser. These were sent to IP 119.81.109.17, 119.81.209.122, 210.176.156.25, 54.254.149.133 etc. These are the set of IP addresses which belong to cricbuzz.

2. The browser downloaded different images in parallel because in the screen shot we can see that HTTP GET requests for new images was placed before old image was received.

578	3.174569000	119.81.209.86	172.16.3.203
580	3.176289000	172.16.3.203	119.81.209.86
591	3.213041000	172.16.3.203	119.81.209.86
595	3.222991000	172.16.3.203	119.81.209.86
618	3.246391000	172.16.3.203	117.239.141.19
638	3.445665000	119.81.209.86	172.16.3.203
656	3.445919000	119.81.209.86	172.16.3.203
660	3.445968000	172.16.3.203	119.81.212.8
664	3.446012000	172.16.3.203	119.81.212.8
674	3.448980000	172.16.3.203	119.81.212.8
675	3.451220000	172.16.3.203	119.81.109.11
676	3.451292000	172.16.3.203	119.81.109.11
677	3.451337000	172.16.3.203	119.81.109.11
678	3.451386000	172.16.3.203	119.81.109.11
679	3.451430000	172.16.3.203	119.81.212.8
680	3.451473000	172.16.3.203	119.81.115.200
681	3.451517000	172.16.3.203	119.81.115.200
701	3.507455000	117.239.141.19	172.16.3.203