

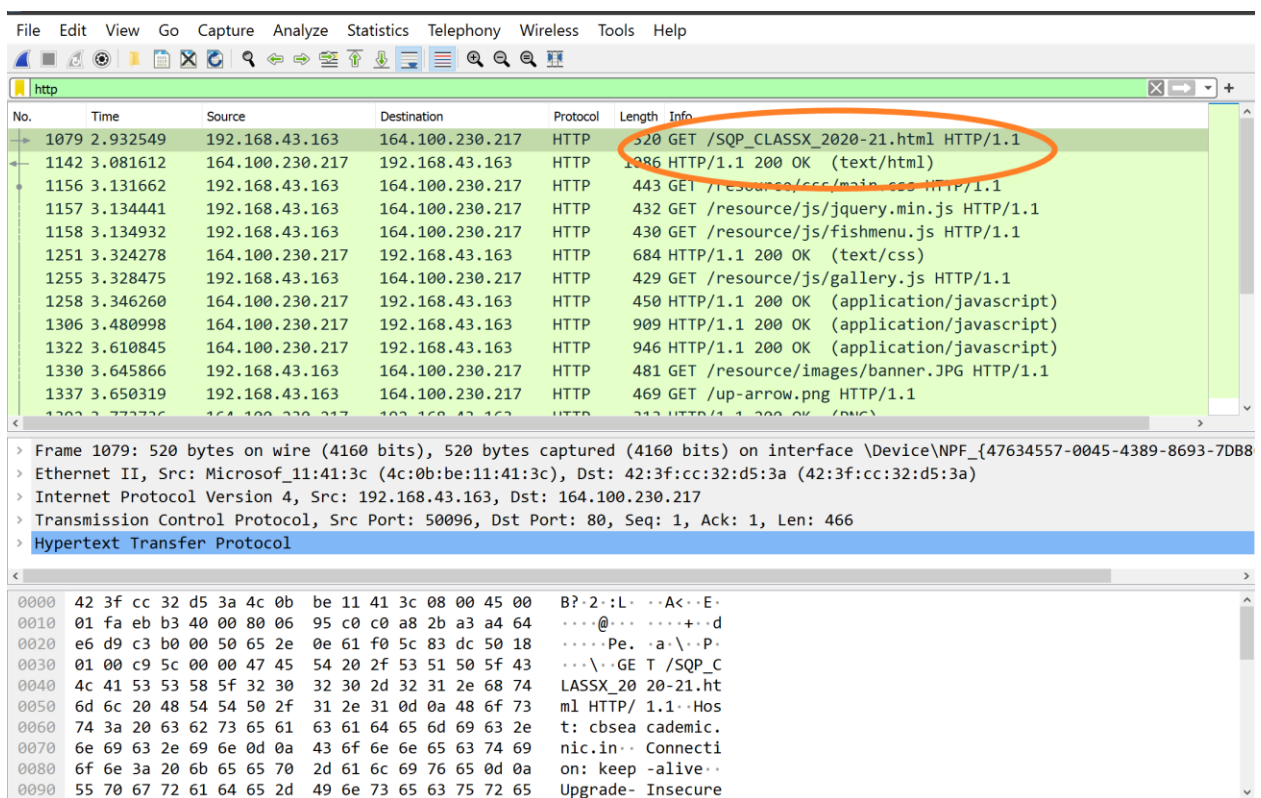
Name: Prit Amin

Student ID: 216831232

ASSIGNMENT 1 EECS 3214 Winter 2021

Getting an HTTP Message

1A)



The image shows a Wireshark packet capture of an HTTP message. The packet list pane shows a GET request for /SQP_CLASSX_2020-21.html. The packet details pane shows the HTTP structure with status 200 OK. The packet bytes pane shows the raw data including the URL and headers.

No.	Time	Source	Destination	Protocol	Length	Info
1079	2.932549	192.168.43.163	164.100.230.217	HTTP	520	GET /SQP_CLASSX_2020-21.html HTTP/1.1
1142	3.081612	164.100.230.217	192.168.43.163	HTTP	1086	HTTP/1.1 200 OK (text/html)
1156	3.131662	192.168.43.163	164.100.230.217	HTTP	443	GET /resource/css/main.css HTTP/1.1
1157	3.134441	192.168.43.163	164.100.230.217	HTTP	432	GET /resource/js/jquery.min.js HTTP/1.1
1158	3.134932	192.168.43.163	164.100.230.217	HTTP	430	GET /resource/js/fishmenu.js HTTP/1.1
1251	3.324278	164.100.230.217	192.168.43.163	HTTP	684	HTTP/1.1 200 OK (text/css)
1255	3.328475	192.168.43.163	164.100.230.217	HTTP	429	GET /resource/js/gallery.js HTTP/1.1
1258	3.346260	164.100.230.217	192.168.43.163	HTTP	450	HTTP/1.1 200 OK (application/javascript)
1306	3.480998	164.100.230.217	192.168.43.163	HTTP	909	HTTP/1.1 200 OK (application/javascript)
1322	3.610845	164.100.230.217	192.168.43.163	HTTP	946	HTTP/1.1 200 OK (application/javascript)
1330	3.645866	192.168.43.163	164.100.230.217	HTTP	481	GET /resource/images/banner.JPG HTTP/1.1
1337	3.650319	192.168.43.163	164.100.230.217	HTTP	469	GET /up-arrow.png HTTP/1.1

Frame 1079: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{47634557-0045-4389-8693-7DB8} Ethernet II, Src: Microsof_11:41:3c (4c:0b:be:11:41:3c), Dst: 42:3f:cc:32:d5:3a (42:3f:cc:32:d5:3a) Internet Protocol Version 4, Src: 192.168.43.163, Dst: 164.100.230.217 Transmission Control Protocol, Src Port: 50096, Dst Port: 80, Seq: 1, Ack: 1, Len: 466 Hypertext Transfer Protocol

0000 42 3f cc 32 d5 3a 4c 0b be 11 41 3c 08 00 45 00 B? 2.:L. ..A<..E.
0010 01 fa eb b3 40 00 80 06 95 c0 c0 a8 2b a3 a4 64@... ..+...d
0020 e6 d9 c3 b0 00 50 65 2e 0e 61 f0 5c 83 dc 50 18Pe. .a\...P.
0030 01 00 c9 5c 00 00 47 45 54 20 2f 53 51 50 5f 43 ...\\...GE T /SQP_C
0040 4c 41 53 53 58 5f 32 30 32 30 2d 32 31 2e 68 74 LASSX_20 20-21.ht
0050 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 ml HTTP/ 1.1..Hos
0060 74 3a 20 63 62 73 65 61 63 61 64 65 6d 69 63 2e t: cbsea cademic.
0070 6e 69 63 2e 69 6e 0d 0a 43 6f 6e 6e 65 63 74 69 nic.in.. Connecti
0080 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep -alive..
0090 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade- Insecure

1B) URL: http://cbseacademic.nic.in/SQP_CLASSX_2020-21.html

Fields that can be used to acquire URL are GET and HOST.

```
1306 3.480998 164.100.230.217 192.168.43.163 HTTP 909 HTTP/1.1 200 OK (application/javascript)
1322 3.610845 164.100.230.217 192.168.43.163 HTTP 946 HTTP/1.1 200 OK (application/javascript)
1330 3.645866 192.168.43.163 164.100.230.217 HTTP 481 GET /resource/images/banner.JPG HTTP/1.1
1337 3.650319 192.168.43.163 164.100.230.217 HTTP 469 GET /up-arrow.png HTTP/1.1
1343 3.732726 164.100.230.217 192.168.43.163 HTTP 313 HTTP/1.1 200 OK (text/html)

> Frame 1079: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{47634557-0045-4389-8693-7DE}
> Ethernet II, Src: Microsof_11:41:3c (4c:0b:be:11:41:3c), Dst: 42:3f:cc:32:d5:3a (42:3f:cc:32:d5:3a)
> Internet Protocol Version 4, Src: 192.168.43.163, Dst: 164.100.230.217
> Transmission Control Protocol, Src Port: 50096, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
< Hypertext Transfer Protocol
  GET /SQP_CLASSX_2020-21.html HTTP/1.1\r\n
  Host: cbseacademic.nic.in\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/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
```

1C) Submitted via 216831232.txt

Analyzing HTTP message

2A) Content length shows bytes of message in body segment of the html page whereas length shows bytes captured by a packet from that html page.

No.	Time	Source	Destination	Protocol	Length	Info
1079	2.932549	192.168.43.163	164.100.230.217	HTTP	520	GET /SQP_CLASSX_2020-21.html HTTP/1.1
1142	3.081612	164.100.230.217	192.168.43.163	HTTP	1086	HTTP/1.1 200 OK (text/html)
1156	3.131662	192.168.43.163	164.100.230.217	HTTP	443	GET /resource/css/main.css HTTP/1.1
1157	3.134441	192.168.43.163	164.100.230.217	HTTP	432	GET /resource/js/jquery.min.js HTTP/1.1
1158	3.134932	192.168.43.163	164.100.230.217	HTTP	430	GET /resource/js/fishmenu.js HTTP/1.1
1251	3.324278	164.100.230.217	192.168.43.163	HTTP	684	HTTP/1.1 200 OK (text/css)
1255	3.328475	192.168.43.163	164.100.230.217	HTTP	429	GET /resource/js/gallery.js HTTP/1.1
1258	3.346260	164.100.230.217	192.168.43.163	HTTP	450	HTTP/1.1 200 OK (application/javascript)
1306	3.480998	164.100.230.217	192.168.43.163	HTTP	909	HTTP/1.1 200 OK (application/javascript)
1322	3.610845	164.100.230.217	192.168.43.163	HTTP	946	HTTP/1.1 200 OK (application/javascript)
1330	3.645866	192.168.43.163	164.100.230.217	HTTP	481	GET /resource/images/banner.JPG HTTP/1.1
1337	3.650319	192.168.43.163	164.100.230.217	HTTP	469	GET /up-arrow.png HTTP/1.1
1342	3.737736	164.100.230.217	192.168.43.163	HTTP	313	HTTP/1.1 200 OK (PNG)

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n
Content-Type: text/html\r\n
Content-Encoding: gzip\r\n
Last-Modified: Fri, 06 Nov 2020 09:57:22 GMT\r\n
Accept-Ranges: bytes\r\n
ETag: "0ad923823b4d61:0"\r\n
Vary: Accept-Encoding\r\n
Server: Microsoft-IIS/8.0\r\n
X-Powered-By: ASP.NET\r\n
Date: Sat, 06 Feb 2021 16:34:39 GMT\r\n
Content-Length: 3478\r\n
\r\n
[HTTP response 1/4]

2B) When I refreshed the page, “IF-MODIFIED-SINCE” segment showed no change. As we can see 304 error is found in the later Get message. If it was 200, modified would have changed.

2286	3.877046	188.172.246.175	192.168.1.101	HTTP	210	HTTP/1.1 200 OK
2340	4.192831	192.168.1.101	188.172.246.175	HTTP	239	GET /din.aspx?s=26430098&id=1702156116&client=DynGate&p=1
2343	4.201307	188.172.246.175	192.168.1.101	HTTP	210	[TCP Spurious Retransmission] HTTP/1.1 200 OK
2662	5.002018	192.168.1.101	164.100.230.217	HTTP	520	GET /SQP_CLASSX_2020-21.html HTTP/1.1
2686	5.048511	164.100.230.217	192.168.1.101	HTTP	922	HTTP/1.1 200 OK (text/html)
3373	8.188645	192.168.1.101	164.100.230.217	HTTP	432	GET /resource/js/jquery.min.js HTTP/1.1
3374	8.189618	192.168.1.101	164.100.230.217	HTTP	430	GET /resource/js/fishmenu.js HTTP/1.1
3412	8.261910	164.100.230.217	192.168.1.101	HTTP	286	HTTP/1.1 200 OK (application/javascript)
3424	8.269475	192.168.1.101	164.100.230.217	HTTP	443	GET /resource/css/main.css HTTP/1.1
3425	8.270757	192.168.1.101	164.100.230.217	HTTP	429	GET /resource/js/gallery.js HTTP/1.1
3455	8.324078	164.100.230.217	192.168.1.101	HTTP	1250	HTTP/1.1 200 OK (application/javascript)
3468	8.355422	164.100.230.217	192.168.1.101	HTTP	663	HTTP/1.1 200 OK (application/javascript)
3469	8.355423	164.100.230.217	192.168.1.101	HTTP	602	HTTP/1.1 200 OK (text/css)

Frame 2662: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{47634557-0045-4389-8693-7D}
Ethernet II, Src: Microsof_11:41:3c (4c:0b:be:11:41:3c), Dst: BestITwo_3a:02:90 (00:1e:a6:3a:02:90)
Internet Protocol Version 4, Src: 192.168.1.101, Dst: 164.100.230.217
Transmission Control Protocol, Src Port: 50158, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
Hypertext Transfer Protocol

GET /SQP_CLASSX_2020-21.html HTTP/1.1\r\n
Host: cbseacademic.nic.in\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/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n

```
3468 8.355422 164.100.230.217 192.168.1.101 HTTP 663 HTTP/1.1 200 OK (application/javascript)
3469 8.355422 164.100.230.217 192.168.1.101 HTTP 602 HTTP/1.1 200 OK (text/css)
3765 9.656094 192.168.1.101 164.100.230.217 HTTP 481 GET /resource/images/banner.JPG HTTP/1.1
3823 9.894010 164.100.230.217 192.168.1.101 HTTP 593 HTTP/1.1 200 OK (JPEG JFIF image)
3826 9.911868 192.168.1.101 164.100.230.217 HTTP 469 GET /up-arrow.png HTTP/1.1
3835 9.957342 164.100.230.217 192.168.1.101 HTTP 231 HTTP/1.1 200 OK (PNG)
4478 13.942445 192.168.1.101 164.100.230.217 HTTP 468 GET /favicon.ico HTTP/1.1
4484 13.983373 164.100.230.217 192.168.1.101 HTTP 1454 HTTP/1.1 200 OK (image/x-icon)
5505 17.066809 192.168.1.101 164.100.230.217 HTTP 631 GET /SQP_CLASSX_2020-21.html HTTP/1.1
5534 17.117996 164.100.230.217 192.168.1.101 HTTP 146 HTTP/1.1 304 Not Modified
5623 17.525408 192.168.1.101 164.100.230.217 HTTP 511 GET /favicon.ico HTTP/1.1
5634 17.568610 164.100.230.217 192.168.1.101 HTTP 1454 HTTP/1.1 200 OK (image/x-icon)

Hypertext Transfer Protocol
> GET /SQP_CLASSX_2020-21.html HTTP/1.1\r\n
Host: cbseacademic.nic.in\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "0ad923823b4d61:0"\r\n
If-Modified-Since: Fri, 06 Nov 2020 09:57:22 GMT\r\n
\r\n
[Full request URI: http://cbseacademic.nic.in/SQP_CLASSX_2020-21.html]
```

2C) No, OK message is send at the end when all TCP segments are received, not after each TCP segment.

```
2286 3.877046 188.172.246.175 192.168.1.101 HTTP 210 HTTP/1.1 200 OK
2340 4.192831 192.168.1.101 188.172.246.175 HTTP 239 GET /din.aspx?s=26430098&id=1702156116&client=DynGate&p=1 HTTP/1.1
2343 4.201307 188.172.246.175 192.168.1.101 HTTP 210 [TCP Spurious Retransmission] HTTP/1.1 200 OK
2662 5.002018 192.168.1.101 164.100.230.217 HTTP 520 GET /SQP_CLASSX_2020-21.html HTTP/1.1
2686 5.048511 164.100.230.217 192.168.1.101 HTTP 922 HTTP/1.1 200 OK (text/html)
3373 8.188645 192.168.1.101 164.100.230.217 HTTP 432 GET /resource/js/jquery.min.js HTTP/1.1
3374 8.189618 192.168.1.101 164.100.230.217 HTTP 430 GET /resource/js/fishmenu.js HTTP/1.1
3412 8.261910 164.100.230.217 192.168.1.101 HTTP 286 HTTP/1.1 200 OK (application/javascript)
3424 8.269475 192.168.1.101 164.100.230.217 HTTP 443 GET /resource/css/main.css HTTP/1.1
3425 8.270757 192.168.1.101 164.100.230.217 HTTP 429 GET /resource/js/gallery.js HTTP/1.1
3455 8.324078 164.100.230.217 192.168.1.101 HTTP 1250 HTTP/1.1 200 OK (application/javascript)
3468 8.355422 164.100.230.217 192.168.1.101 HTTP 663 HTTP/1.1 200 OK (application/javascript)
3469 8.355422 164.100.230.217 192.168.1.101 HTTP 602 HTTP/1.1 200 OK (text/css)

> Frame 2686: 922 bytes on wire (7376 bits), 922 bytes captured (7376 bits) on interface \Device\NPF_{47634557-0045-4389-8693-7DE}
> Ethernet II, Src: BestITWo_3a:02:90 (00:1e:a6:3a:02:90), Dst: Microsof_11:41:3c (4c:0b:be:11:41:3c)
> Internet Protocol Version 4, Src: 164.100.230.217, Dst: 192.168.1.101
> Transmission Control Protocol, Src Port: 80, Dst Port: 50158, Seq: 2905, Ack: 467, Len: 868
> [3 Reassembled TCP Segments (3772 bytes): #2683(1452), #2684(1452), #2686(868)]
  [Frame: 2683, payload: 0-1451 (1452 bytes)]
  [Frame: 2684, payload: 1452-2903 (1452 bytes)]
  [Frame: 2686, payload: 2904-3771 (868 bytes)]
  [Segment count: 3]
  [Reassembled TCP length: 3772]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a436f6e74656742d547970653a20746578742f...]

Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Content-Type: text/html\r\n
```

DNS

This part was done on York server.

3A) Default server: 130.63.94.4

IP Address: 130.63.94.4#53

```
Microsoft Windows [Version 10.0.19042.746]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\aminp>ssh prit2000@red.cse.yorku.ca

*****
* ATTENTION:
*****
* For the duration of the COVID-19 pandemic, 2 additional "red" servers have *
* been setup - red1.eecs.yorku.ca and red2.eecs.yorku.ca. All 3 red servers *
* can be accessed remotely.
*
* Please send technical support requests to tech@eecs.yorku.ca.
*****

Password:
Last login: Sun Feb  7 13:16:47 2021 from 103.206.137.180
Default printer is: prism
red 293 % nslookup www.whatsapp.com
Server:          130.63.94.4
Address:         130.63.94.4#53

Non-authoritative answer:
www.whatsapp.com      canonical name = mmx-ds.cdn.whatsapp.net.
Name:   mmx-ds.cdn.whatsapp.net
Address: 31.13.80.53
Name:   mmx-ds.cdn.whatsapp.net
Address: 2a03:2880:f20e:c5:face:b00c:0:167
```

3B)

1) Given url is Asian server with IP address 103.27.9.24

```
red 297 % nslookup home.iitd.ac.in
Server:          130.63.94.4
Address:         130.63.94.4#53

Non-authoritative answer:
Name:   home.iitd.ac.in
Address: 103.27.9.24

red 298 %
```

2) Following are the authorized servers of University of Barcelona.

rnpro01.com.ub.edu

rnpro04.com.ub.edu

rnpro07.com.ub.edu

```
red 298 % nslookup -type=NS ub.edu
Server:          130.63.94.4
Address:         130.63.94.4#53

Non-authoritative answer:
ub.edu  nameserver = rnpro07.com.ub.edu.
ub.edu  nameserver = chico.rediris.es.
ub.edu  nameserver = rnpro01.com.ub.edu.
ub.edu  nameserver = rnpro04.com.ub.edu.
ub.edu  nameserver = sun.rediris.es.

Authoritative answers can be found from:
rnpro01.com.ub.edu      internet address = 161.116.160.1
rnpro04.com.ub.edu      internet address = 161.116.110.95
rnpro07.com.ub.edu      internet address = 161.116.230.1

red 299 %
```


3) Server refuses mail.yahoo.com.

```
red 301 % nslookup mail.yahoo.com rnpro01.com.ub.edu
Server:         rnpro01.com.ub.edu
Address:        161.116.160.1#53

** server can't find mail.yahoo.com.eecs.yorku.ca: REFUSED

red 302 % nslookup mail.yahoo.com rnpro04.com.ub.edu
Server:         rnpro04.com.ub.edu
Address:        161.116.110.95#53

** server can't find mail.yahoo.com.eecs.yorku.ca: REFUSED

red 303 % nslookup mail.yahoo.com rnpro07.com.ub.edu
Server:         rnpro07.com.ub.edu
Address:        161.116.230.1#53

** server can't find mail.yahoo.com.eecs.yorku.ca: REFUSED

red 304 %
```

3C) According Python dictionary, we can write this as

```
{
  "Name": "ub.edu",
  "Value": "rnpro01.com.ub.edu",
  "Type": "NS",
  "IP": "161.116.160.1"
}
```