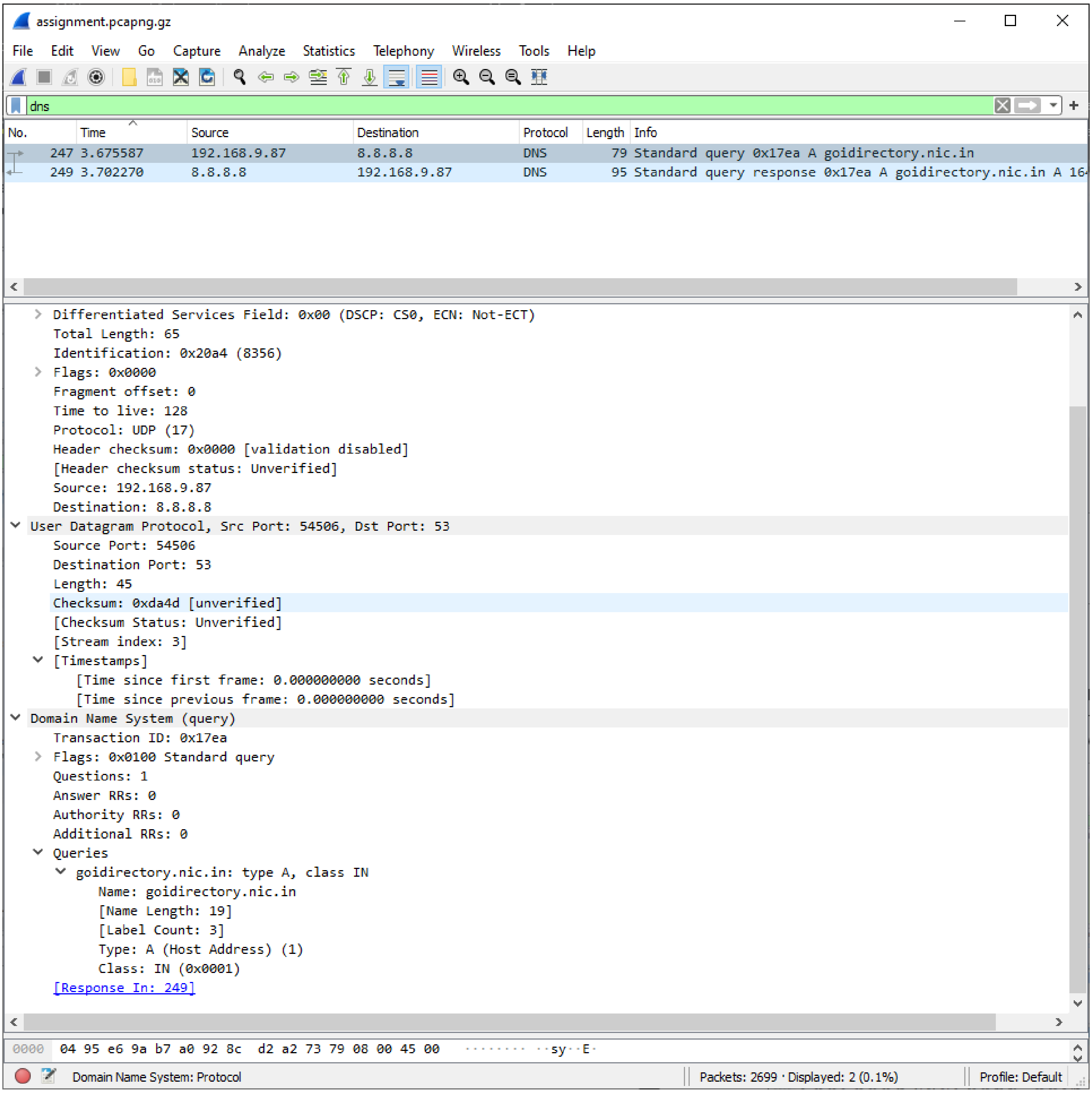
Task 1

How many DNS queries are sent from your browser (host machine) to DNS Server(s)? How many DNS servers are involved? Which DNS Server replies with actual IP Address(es). Do all DNS servers respond? List the resource records involved in resolving the IP address of the site, mentioning, Name, value, type, TTL appropriately in the complete resolving process of this DNS conversation, including query/queries and response/answer(s).

There is one request sent from the host machine to the DNS server. There is just one DNS server (Google DNS) involved in resolving the DNS, which replies to the DNS query. Since there are no other servers involved in DNS resolving, we see no query or response to/from any other server. The same can be seen in the capture and flow graph.

For the request, we see that the name to be resolved is goidirectory.nic.in, which is a Type A (host address) request. The time to live for the request packet is 128s. In the response provided by the DNS server, the time to live is 122s, and the DNS server returns that the IP address is of goidirectory.nic.in 164.100.58.217



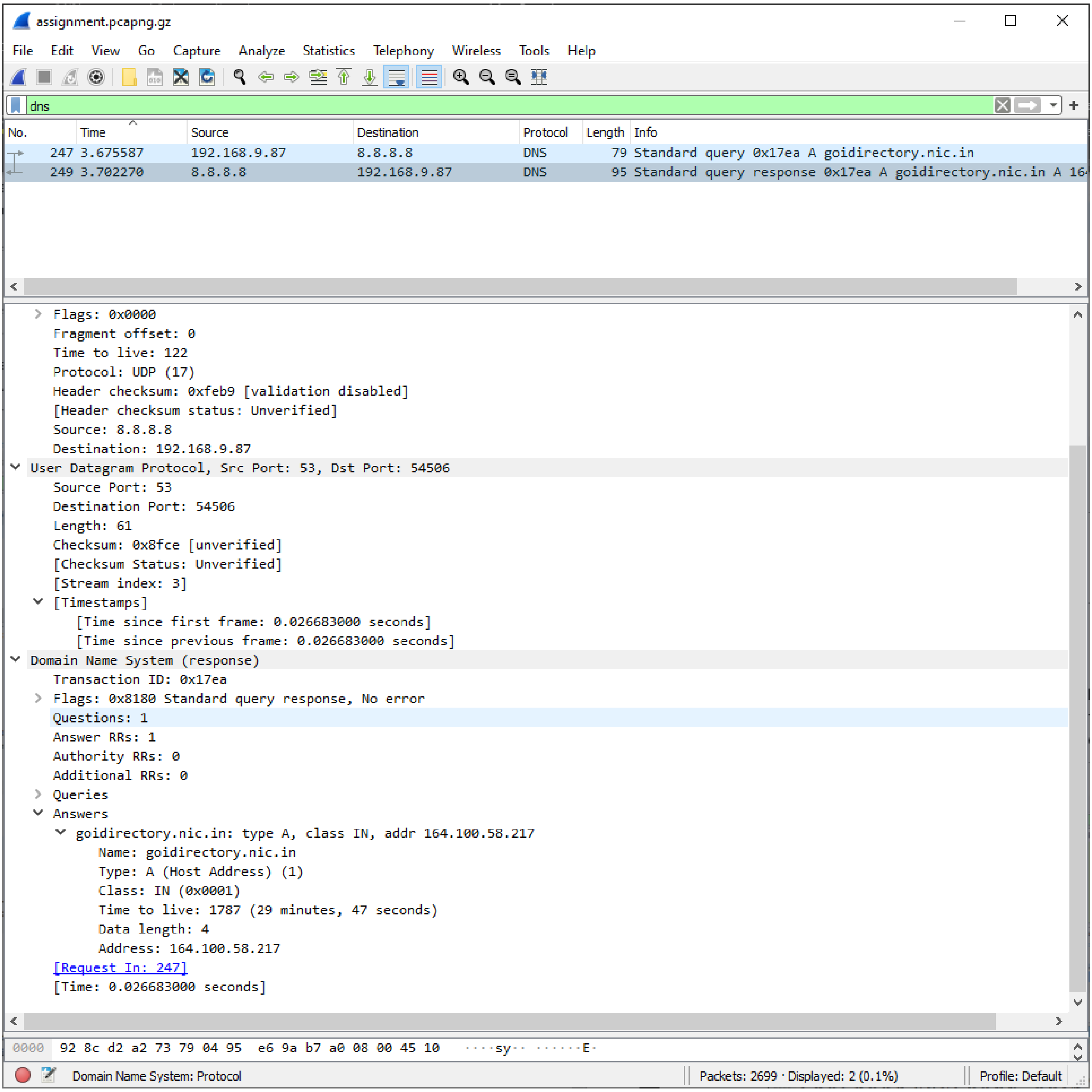
dns

```
No.     Time        Source          Destination     Protocol  Length Info
    247 3.675587    192.168.9.87    8.8.8.8         DNS           79 Standard query 0x17ea A goidirectory.nic.in
    249 3.702270    8.8.8.8         192.168.9.87    DNS           95 Standard query response 0x17ea A goidirectory.nic.in A 16
```

```
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 65
    Identification: 0x20a4 (8356)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.9.87
    Destination: 8.8.8.8
v User Datagram Protocol, Src Port: 54506, Dst Port: 53
    Source Port: 54506
    Destination Port: 53
    Length: 45
    Checksum: 0xda4d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  v [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
v Domain Name System (query)
    Transaction ID: 0x17ea
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v goidirectory.nic.in: type A, class IN
        Name: goidirectory.nic.in
        [Name Length: 19]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 249]
```

```
0000  04 95 e6 9a b7 a0 92 8c  d2 a2 73 79 08 00 45 00   ········ ··sy··E·
```

Domain Name System: Protocol | Packets: 2699 · Displayed: 2 (0.1%) | Profile: Default


assignment.pcapng.gz
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

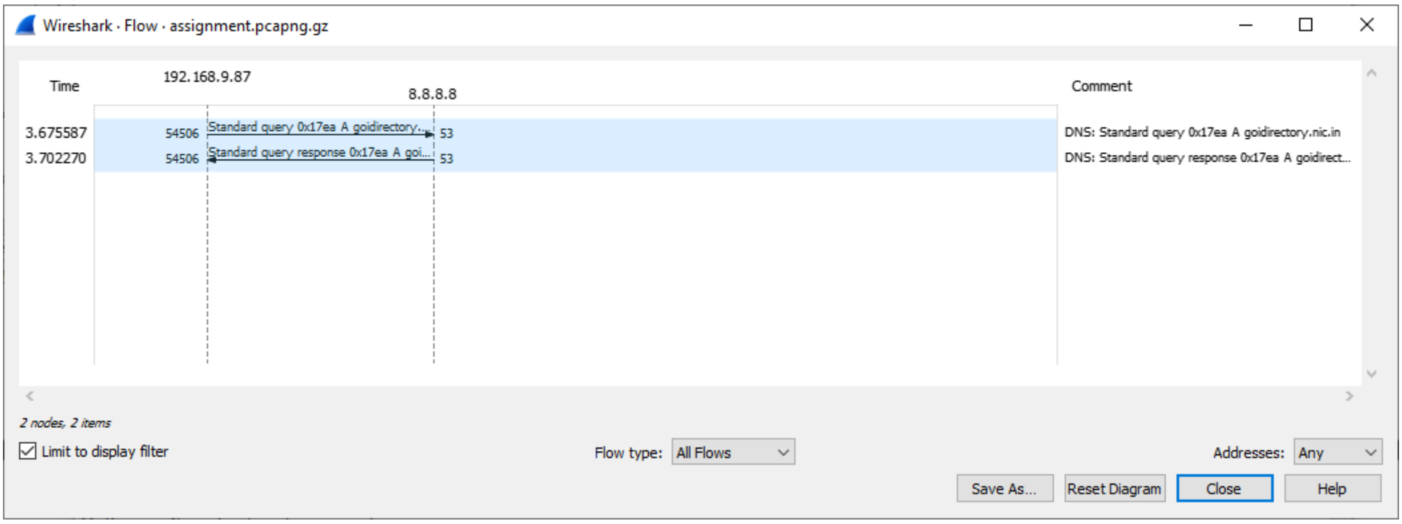
```
No.   Time        Source         Destination    Protocol  Length  Info
  247 3.675587    192.168.9.87   8.8.8.8        DNS           79 Standard query 0x17ea A goidirectory.nic.in
  249 3.702270    8.8.8.8        192.168.9.87   DNS           95 Standard query response 0x17ea A goidirectory.nic.in A 164
```

```
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 122
    Protocol: UDP (17)
    Header checksum: 0xfeb9 [validation disabled]
    [Header checksum status: Unverified]
    Source: 8.8.8.8
    Destination: 192.168.9.87
v User Datagram Protocol, Src Port: 53, Dst Port: 54506
    Source Port: 53
    Destination Port: 54506
    Length: 61
    Checksum: 0x8fce [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  v [Timestamps]
      [Time since first frame: 0.026683000 seconds]
      [Time since previous frame: 0.026683000 seconds]
v Domain Name System (response)
    Transaction ID: 0x17ea
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v goidirectory.nic.in: type A, class IN, addr 164.100.58.217
        Name: goidirectory.nic.in
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1787 (29 minutes, 47 seconds)
        Data length: 4
        Address: 164.100.58.217
    [Request In: 247]
    [Time: 0.026683000 seconds]
```

```
0000  92 8c d2 a2 73 79 04 95  e6 9a b7 a0 08 00 45 10   ····sy·· ······E·
```

Domain Name System: Protocol | Packets: 2699 · Displayed: 2 (0.1%) | Profile: Default

From the flow graph, we can see that the time required is 0.03s


Wireshark · Flow · assignment.pcapng.gz
Time
192.168.9.87
8.8.8.8
Comment

```
3.675587   54506  Standard query 0x17ea A goidirectory...  53   DNS: Standard query 0x17ea A goidirectory.nic.in
3.702270   54506  Standard query response 0x17ea A goi...  53   DNS: Standard query response 0x17ea A goidirect...
```

2 nodes, 2 items

☑ Limit to display filter

Flow type: All Flows

Addresses: Any

Save As... Reset Diagram Close Help

How many HTTP requests (Type and respective count of requests), responses (status code and phrase of each of the responses) did the browser send and receive?

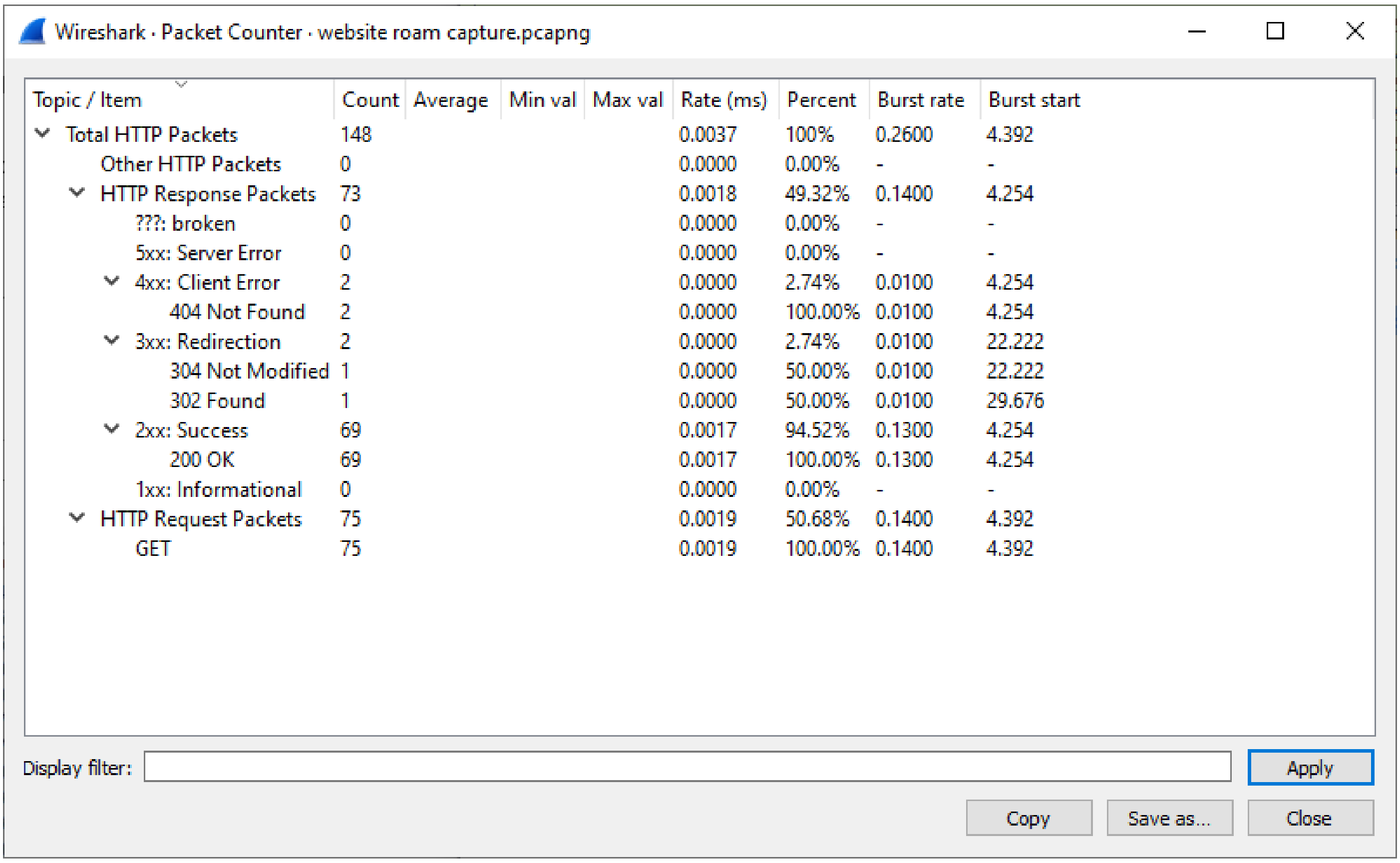
We used the filter `ip.addr == 164.100.58.217` to filter out packets only from/to goidirectory.nic.in. Using this filter and checking the HTTP statistics, we see that a total of 148 packets are sent between the server and browser.

Out of these, there are 75 request packets which are entirely composed of GET requests.

From the remaining, 73 HTTP packets are response packets. The distribution of these is as follows:

- Count: 2 | Status: 404 | Phrase: Not found
- Count: 1 | Status: 304 | Phrase: Not Modified
- Count: 1 | Status: 302 | Phrase: Found
- Count: 69 | Status: 200 | Phrase: OK

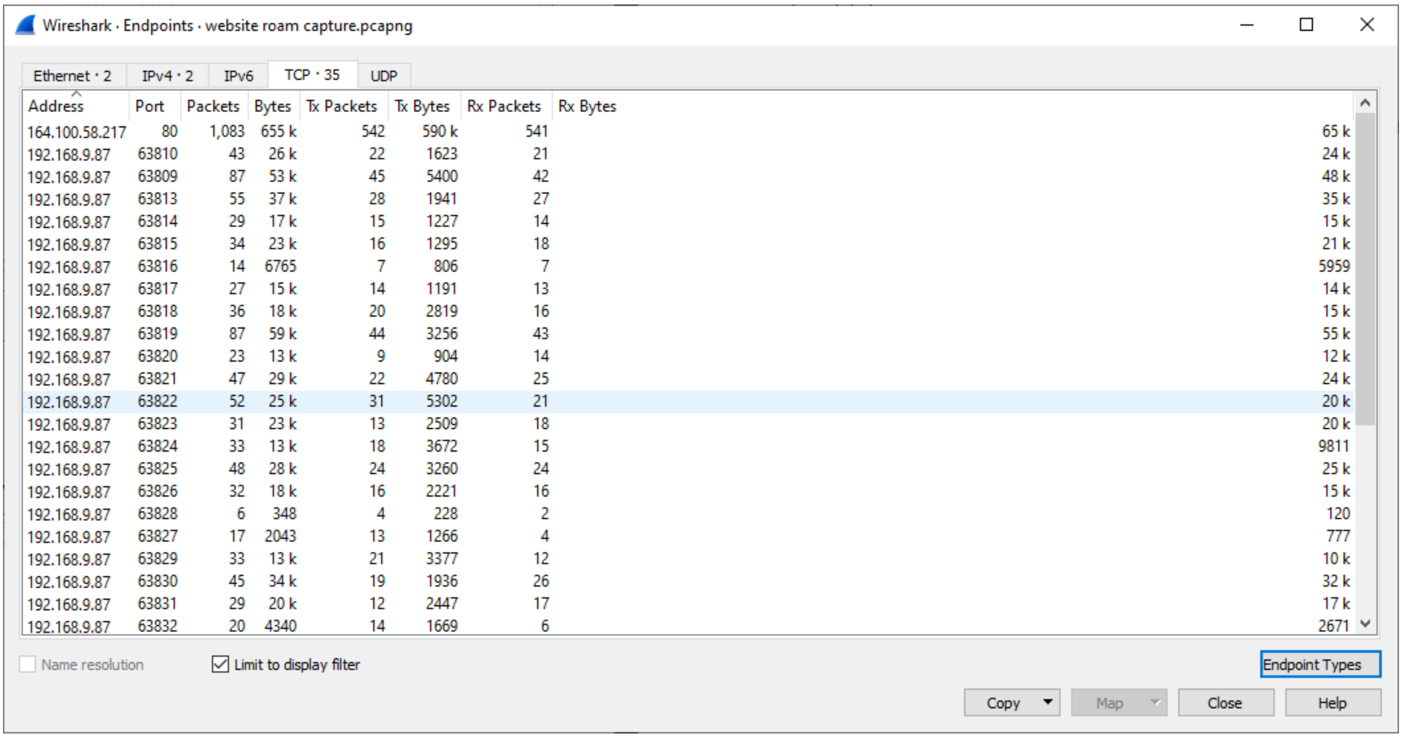
No other type of response packet is received by the browser, which can be seen below.



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Total HTTP Packets	148				0.0037	100%	0.2600	4.392
Other HTTP Packets	0				0.0000	0.00%	-	-
HTTP Response Packets	73				0.0018	49.32%	0.1400	4.254
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	2				0.0000	2.74%	0.0100	4.254
404 Not Found	2				0.0000	100.00%	0.0100	4.254
3xx: Redirection	2				0.0000	2.74%	0.0100	22.222
304 Not Modified	1				0.0000	50.00%	0.0100	22.222
302 Found	1				0.0000	50.00%	0.0100	29.676
2xx: Success	69				0.0017	94.52%	0.1300	4.254
200 OK	69				0.0017	100.00%	0.1300	4.254
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	75				0.0019	50.68%	0.1400	4.392
GET	75				0.0019	100.00%	0.1400	4.392

How many TCP Connections has the browser established overall?

We used the filter `ip.addr == 164.100.58.217` to filter out packets only from/to goidirectory.nic.in. Limiting the endpoint display to the filtered list, we find that the browser established 35 TCP connections between our system and the server. This can be seen in the screenshot of the endpoints given below.



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
164.100.58.217	80	1,083	655 k	542	590 k	541	65 k
192.168.9.87	63810	43	26 k	22	1623	21	24 k
192.168.9.87	63809	87	53 k	45	5400	42	48 k
192.168.9.87	63813	55	37 k	28	1941	27	35 k
192.168.9.87	63814	29	17 k	15	1227	14	15 k
192.168.9.87	63815	34	23 k	16	1295	18	21 k
192.168.9.87	63816	14	6765	7	806	7	5959
192.168.9.87	63817	27	15 k	14	1191	13	14 k
192.168.9.87	63818	36	18 k	20	2819	16	15 k
192.168.9.87	63819	87	59 k	44	3256	43	55 k
192.168.9.87	63820	23	13 k	9	904	14	12 k
192.168.9.87	63821	47	29 k	22	4780	25	24 k
192.168.9.87	63822	52	25 k	31	5302	21	20 k
192.168.9.87	63823	31	23 k	13	2509	18	20 k
192.168.9.87	63824	33	13 k	18	3672	15	9811
192.168.9.87	63825	48	28 k	24	3260	24	25 k
192.168.9.87	63826	32	18 k	16	2221	16	15 k
192.168.9.87	63828	6	348	4	228	2	120
192.168.9.87	63827	17	2043	13	1266	4	777
192.168.9.87	63829	33	13 k	21	3377	12	10 k
192.168.9.87	63830	45	34 k	19	1936	26	32 k
192.168.9.87	63831	29	20 k	12	2447	17	17 k
192.168.9.87	63832	20	4340	14	1669	6	2671

□ Name resolution ☑ Limit to display filter

What is the time taken to establish a TCP connection(s)? List this time taken value for each of the TCP connection(s).

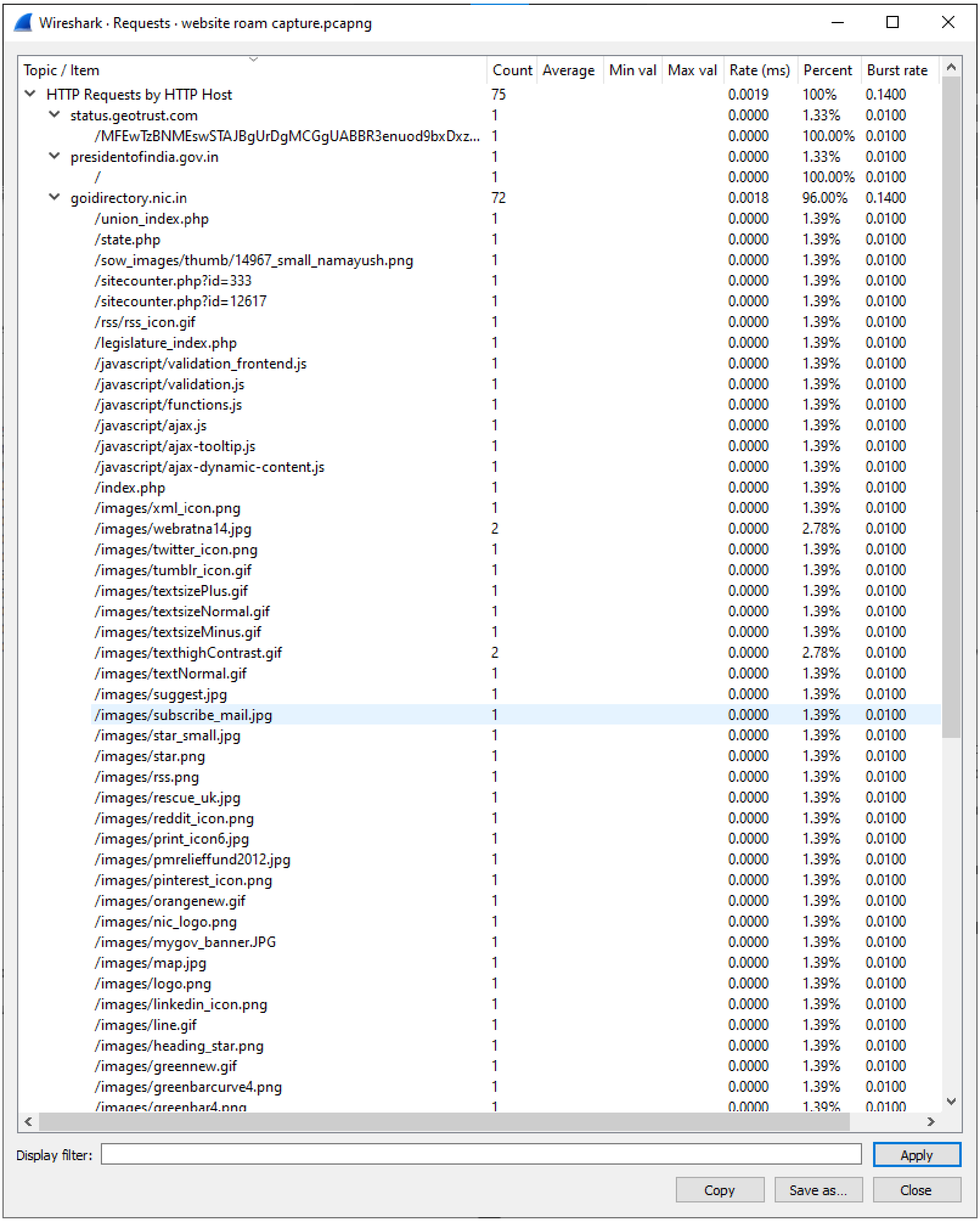
The time taken to establish a TCP connection (or the time for TCP handshake) can be obtained using the duration given in conversation statistics.

Address A	Port A	Address B	Port B	Time taken (s)
192.168.9.87	63810	164.100.58.217	80	0.701187
192.168.9.87	63809	164.100.58.217	80	1.149893
192.168.9.87	63813	164.100.58.217	80	0.581632
192.168.9.87	63814	164.100.58.217	80	0.578251
192.168.9.87	63815	164.100.58.217	80	0.582257
192.168.9.87	63816	164.100.58.217	80	0.500171
192.168.9.87	63817	164.100.58.217	80	0.545401
192.168.9.87	63818	164.100.58.217	80	0.670139
192.168.9.87	63819	164.100.58.217	80	0.468105
192.168.9.87	63820	164.100.58.217	80	0.291312
192.168.9.87	63821	164.100.58.217	80	0.924294
192.168.9.87	63822	164.100.58.217	80	41.695544
192.168.9.87	63823	164.100.58.217	80	0.679071
192.168.9.87	63824	164.100.58.217	80	0.605794
192.168.9.87	63825	164.100.58.217	80	0.607402
192.168.9.87	63826	164.100.58.217	80	0.580879
192.168.9.87	63828	164.100.58.217	80	16.603536
192.168.9.87	63827	164.100.58.217	80	35.538641
192.168.9.87	63829	164.100.58.217	80	42.587351
192.168.9.87	63830	164.100.58.217	80	0.274511
192.168.9.87	63831	164.100.58.217	80	0.269817
192.168.9.87	63832	164.100.58.217	80	42.469497
192.168.9.87	63833	164.100.58.217	80	42.440064
192.168.9.87	63834	164.100.58.217	80	33.0111
192.168.9.87	63839	164.100.58.217	80	20.087001
192.168.9.87	63840	164.100.58.217	80	5.108735
192.168.9.87	63841	164.100.58.217	80	25.079084

192.168.9.87	63842	164.100.58.217	80	27.200757
192.168.9.87	63844	164.100.58.217	80	12.787833
192.168.9.87	63845	164.100.58.217	80	12.788
192.168.9.87	63863	164.100.58.217	80	7.3253
192.168.9.87	63864	164.100.58.217	80	0.008301
192.168.9.87	63866	164.100.58.217	80	4.664844
192.168.9.87	63865	164.100.58.217	80	4.664612

How many objects/files are downloaded?

We check the HTTP packet counter statistics. Using this, we observe that 72 objects/ files are downloaded from the server at goidirectory.nic.in



Wireshark · Requests · website roam capture.pcapng

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate
HTTP Requests by HTTP Host	75				0.0019	100%	0.1400
status.geotrust.com	1				0.0000	1.33%	0.0100
/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR3enuod9bxDxz...	1				0.0000	100.00%	0.0100
presidentofindia.gov.in	1				0.0000	1.33%	0.0100
/	1				0.0000	100.00%	0.0100
goidirectory.nic.in	72				0.0018	96.00%	0.1400
/union_index.php	1				0.0000	1.39%	0.0100
/state.php	1				0.0000	1.39%	0.0100
/sow_images/thumb/14967_small_namayush.png	1				0.0000	1.39%	0.0100
/sitecounter.php?id=333	1				0.0000	1.39%	0.0100
/sitecounter.php?id=12617	1				0.0000	1.39%	0.0100
/rss/rss_icon.gif	1				0.0000	1.39%	0.0100
/legislature_index.php	1				0.0000	1.39%	0.0100
/javascript/validation_frontend.js	1				0.0000	1.39%	0.0100
/javascript/validation.js	1				0.0000	1.39%	0.0100
/javascript/functions.js	1				0.0000	1.39%	0.0100
/javascript/ajax.js	1				0.0000	1.39%	0.0100
/javascript/ajax-tooltip.js	1				0.0000	1.39%	0.0100
/javascript/ajax-dynamic-content.js	1				0.0000	1.39%	0.0100
/index.php	1				0.0000	1.39%	0.0100
/images/xml_icon.png	1				0.0000	1.39%	0.0100
/images/webratna14.jpg	2				0.0000	2.78%	0.0100
/images/twitter_icon.png	1				0.0000	1.39%	0.0100
/images/tumblr_icon.gif	1				0.0000	1.39%	0.0100
/images/textsizePlus.gif	1				0.0000	1.39%	0.0100
/images/textsizeNormal.gif	1				0.0000	1.39%	0.0100
/images/textsizeMinus.gif	1				0.0000	1.39%	0.0100
/images/texthighContrast.gif	2				0.0000	2.78%	0.0100
/images/textNormal.gif	1				0.0000	1.39%	0.0100
/images/suggest.jpg	1				0.0000	1.39%	0.0100
/images/subscribe_mail.jpg	1				0.0000	1.39%	0.0100
/images/star_small.jpg	1				0.0000	1.39%	0.0100
/images/star.png	1				0.0000	1.39%	0.0100
/images/rss.png	1				0.0000	1.39%	0.0100
/images/rescue_uk.jpg	1				0.0000	1.39%	0.0100
/images/reddit_icon.png	1				0.0000	1.39%	0.0100
/images/print_icon6.jpg	1				0.0000	1.39%	0.0100
/images/pmrelieffund2012.jpg	1				0.0000	1.39%	0.0100
/images/pinterest_icon.png	1				0.0000	1.39%	0.0100
/images/orangenew.gif	1				0.0000	1.39%	0.0100
/images/nic_logo.png	1				0.0000	1.39%	0.0100
/images/mygov_banner.JPG	1				0.0000	1.39%	0.0100
/images/map.jpg	1				0.0000	1.39%	0.0100
/images/logo.png	1				0.0000	1.39%	0.0100
/images/linkedin_icon.png	1				0.0000	1.39%	0.0100
/images/line.gif	1				0.0000	1.39%	0.0100
/images/heading_star.png	1				0.0000	1.39%	0.0100
/images/greennew.gif	1				0.0000	1.39%	0.0100
/images/greenbarcurve4.png	1				0.0000	1.39%	0.0100
/images/greenbar4.png	1				0.0000	1.39%	0.0100

Display filter:

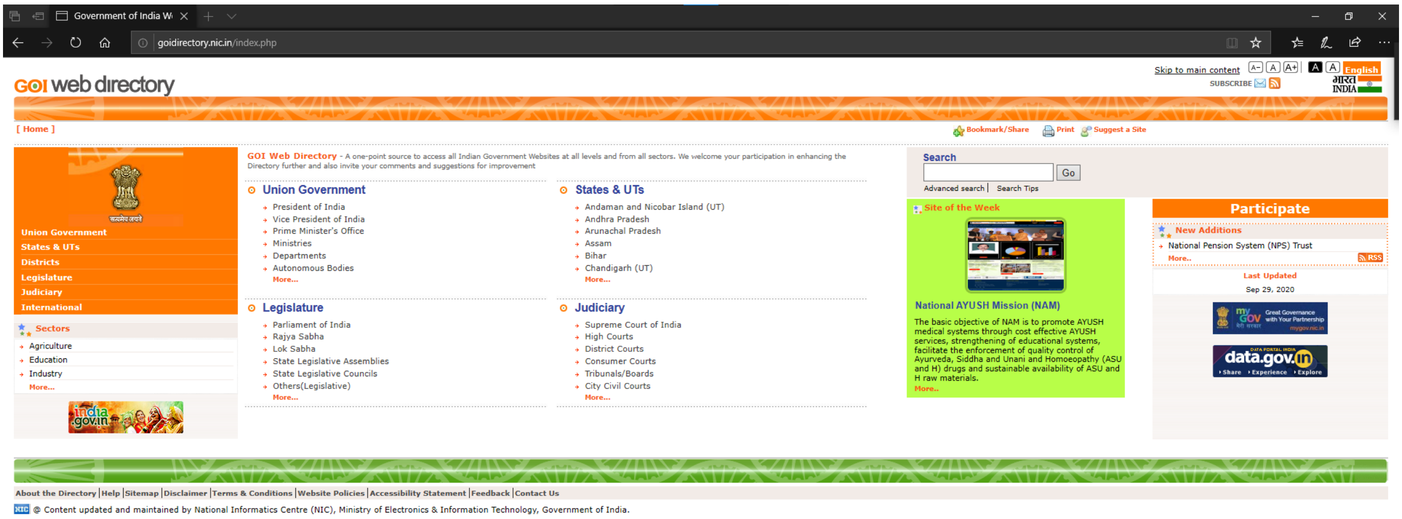
Make a detailed list for each object/file downloaded, the time taken for downloading the objects, the size of the object downloaded, object name, last modified time at the server.

We use the HTTP object list to find all the objects that were downloaded with their size and file name.

Content Type	Size	Filename
application/javascript	5092 bytes	ajax-dynamic-content.js
application/javascript	14 kB	functions.js
application/javascript	11 kB	validation.js
application/javascript	52 kB	validation_frontend.js
application/javascript	5492 bytes	ajax.js
application/javascript	9655 bytes	ajax-tooltip.js
image/gif	236 bytes	textsizeNormal.gif
image/gif	261 bytes	textsizePlus.gif
image/gif	54 bytes	line.gif
image/gif	244 bytes	textNormal.gif
image/gif	229 bytes	textsizeMinus.gif
image/gif	635 bytes	tumblr_icon.gif
image/gif	1202 bytes	rss_icon.gif
image/gif	239 bytes	texthighContrast.gif
image/gif	2700 bytes	orangenew.gif
image/gif	2671 bytes	greennew.gif
image/gif	50 bytes	expand-bulett.gif
image/gif	203 bytes	bg_stripes_new.gif
image/gif	99 bytes	dot.gif
image/jpeg	407 bytes	subscribe_mail.jpg
image/jpeg	292 bytes	delicious_icon.jpg
image/jpeg	393 bytes	suggest.jpg
image/jpeg	423 bytes	print_icon6.jpg
image/jpeg	393 bytes	suggest.jpg
image/jpeg	292 bytes	14967_small_namayush.png
image/jpeg	423 bytes	pmrelieffund2012.jpg
image/jpeg	15kB	banner.jpg
image/jpeg	4357 bytes	rescue_uk.jpg
image/jpeg	3370 bytes	mygov_banner.JPG
image/jpeg	13 kB	pmrelieffund2012.jpg
image/jpeg	427 bytes	Share16.jpg
image/jpeg	11 kB	data_gov.jpg
image/jpeg	498 bytes	blogger_icon.jpg
image/jpeg	27 kB	map.jpg
image/jpeg	708 bytes	star_small.jpg
image/jpeg	14 kB	webratna14.jpg
image/png	782 bytes	bharatindiasmall.png
image/png	2820 bytes	logo.png
image/png	764 bytes	rss.png
image/png	1509 bytes	twitter_icon.png
image/png	759 bytes	facebook_icon.png
image/png	968 bytes	google_plus_icon.png
image/png	1512 bytes	linkedin_icon.png

image/png	3351 bytes	pintrest_icon.png
image/png	589 bytes	reddit_icon.png
image/png	764 bytes	xml_icon.png
image/png	1992 bytes	StumbleUpon_icon.png
image/png	469 bytes	digg_icon.png
image/png	469 bytes	digg_icon.png
image/png	18kB	14967_small_namayush.png
image/png	358 bytes	star.png
image/png	1038 bytes	corner_orange.png
image/png	3317 bytes	bg_header.png
image/png	197 bytes	heading_star.png
image/png	1363 bytes	greenbarcurve4.png
text/css	22 kB	style1.css
text/css	33 kB	static_style.css
text/css	20 kB	unionnew_style.css
text/css	3187 bytes	ajax-tooltip.css
text/css	13kB	leve12.css

How many other websites are visited from this site, by clicking on to various possible links which take you to the other sites (other than http://goidirectory.nic.in/)



GOI Web Directory - A one-point source to access all Indian Government Websites at all levels and from all sectors. We welcome your participation in enhancing the Directory further and also invite your comments and suggestions for improvement

Union Government
States & UTs
Districts
Legislature
Judiciary
International

Sectors
- Agriculture
- Education
- Industry

More...

Union Government
- President of India
- Vice President of India
- Prime Minister's Office
- Ministries
- Departments
- Autonomous Bodies

More...

States & UTs
- Andaman and Nicobar Island (UT)
- Andhra Pradesh
- Arunachal Pradesh
- Assam
- Bihar
- Chandigarh (UT)

More...

Legislature
- Parliament of India
- Rajya Sabha
- Lok Sabha
- State Legislative Assemblies
- State Legislative Councils
- Others(Legislative)

More...

Judiciary
- Supreme Court of India
- High Courts
- District Courts
- Consumer Courts
- Tribunals/Boards
- City Civil Courts

More...

Site of the Week

National AYUSH Mission (NAM)

The basic objective of NAM is to promote AYUSH medical systems through cost effective AYUSH services, strengthening of educational systems, facilitate the enforcement of quality control of Ayurveda, Siddha and Unani and Homoeopathy (ASU and H) drugs and sustainable availability of ASU and H raw materials.
More..

Participate

New Additions
- National Pension System (NPS) Trust

More..

Last Updated
Sep 29, 2020

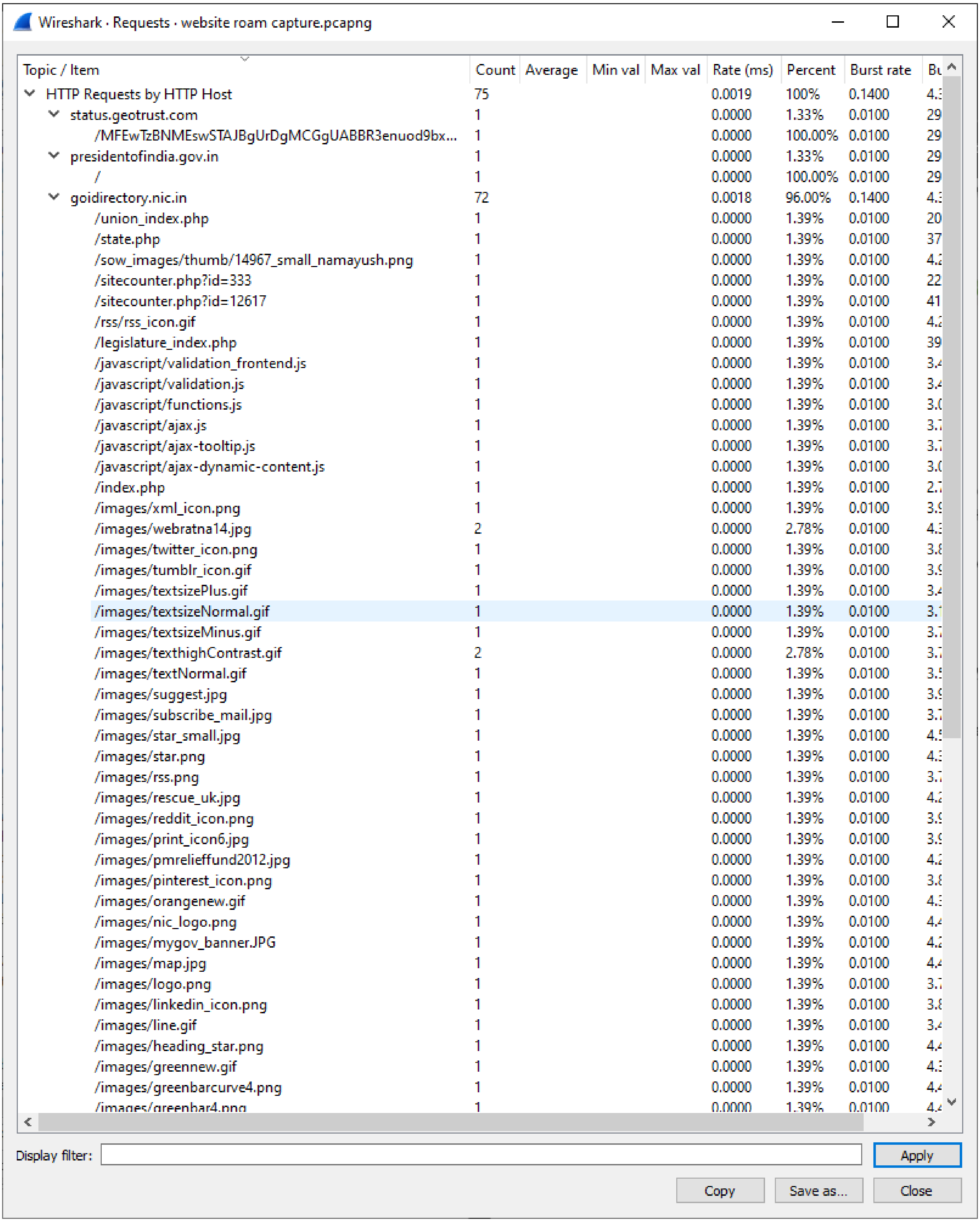
About the Directory |Help |Sitemap |Disclaimer |Terms & Conditions |Website Policies |Accessibility Statement |Feedback |Contact Us

NIC @ Content updated and maintained by National Informatics Centre (NIC), Ministry of Electronics & Information Technology, Government of India.

We are using only the links available on the home page of goidirectory.nic.in, we find that the links for President of India, Vice President of India, Prime Minister’s Office, National AYUSH mission, mygov.in, india.gov.in, data.gov.in, and National pension trust are reachable. Rest all URLs refer to pages on the same site. Hence, we can say that a total of 8 external websites are accessible from the home page of goidirectory.nic.in.

When http://goidirectory.nic.in/ is entered, is there any embedded object shown/downloaded from a different site(s) (other than http://goidirectory.nic.in/)?

After visiting goidirectory.nic.in multiple times to remove any possibility of getting capture from non-intended sources, we find that no other embedded object is shown/ downloaded from any other website other than goidirectory.nic.in when the website goidirectory.nic.in is visited.

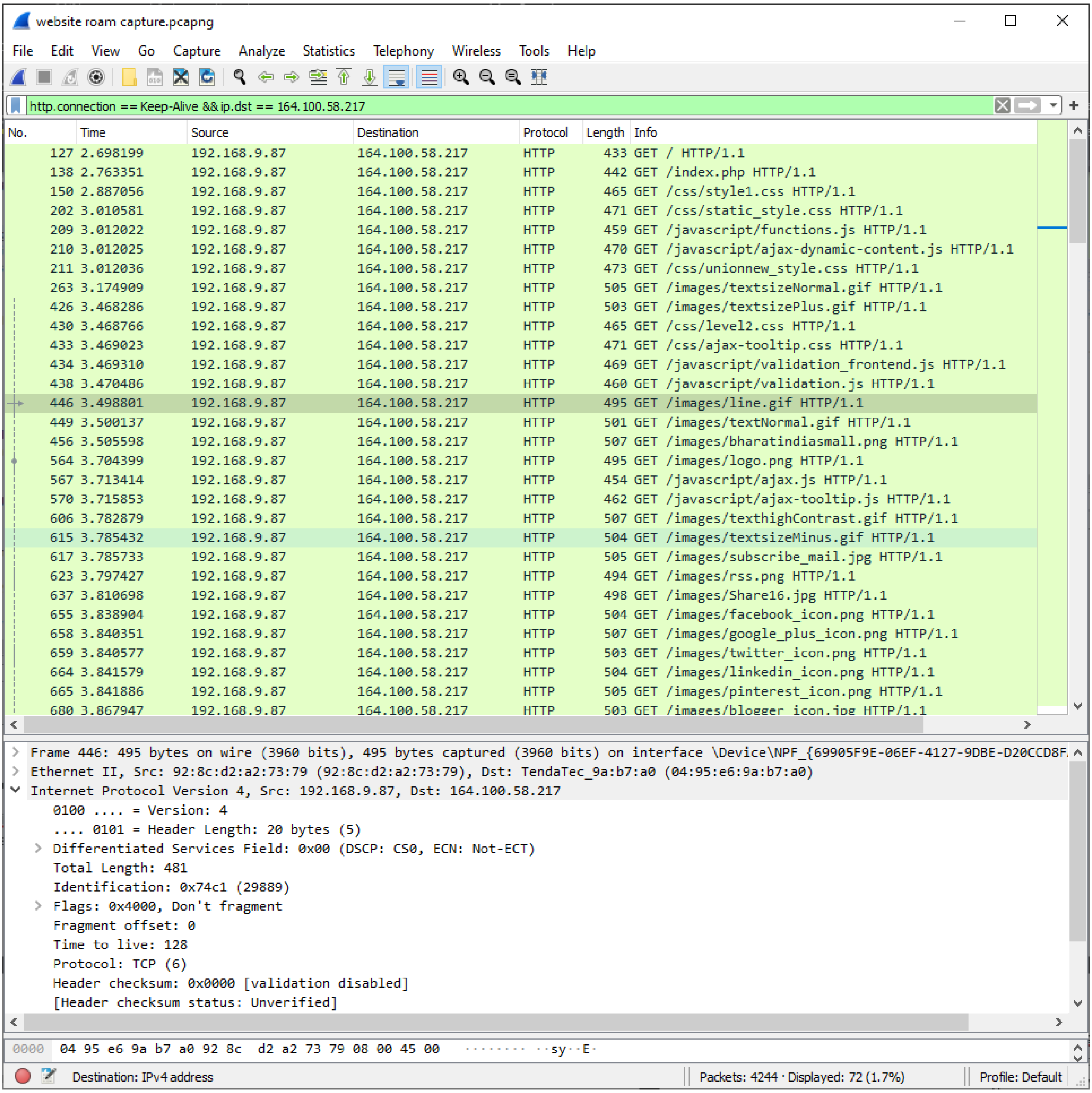


Wireshark · Requests · website roam capture.pcapng

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Bu
HTTP Requests by HTTP Host	75				0.0019	100%	0.1400	4.3
status.geotrust.com	1				0.0000	1.33%	0.0100	29
/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR3enuod9bx...	1				0.0000	100.00%	0.0100	29
presidentofindia.gov.in	1				0.0000	1.33%	0.0100	29
/	1				0.0000	100.00%	0.0100	29
goidirectory.nic.in	72				0.0018	96.00%	0.1400	4.3
/union_index.php	1				0.0000	1.39%	0.0100	20
/state.php	1				0.0000	1.39%	0.0100	37
/sow_images/thumb/14967_small_namayush.png	1				0.0000	1.39%	0.0100	4.2
/sitecounter.php?id=333	1				0.0000	1.39%	0.0100	22
/sitecounter.php?id=12617	1				0.0000	1.39%	0.0100	41
/rss/rss_icon.gif	1				0.0000	1.39%	0.0100	4.2
/legislature_index.php	1				0.0000	1.39%	0.0100	39
/javascript/validation_frontend.js	1				0.0000	1.39%	0.0100	3.4
/javascript/validation.js	1				0.0000	1.39%	0.0100	3.4
/javascript/functions.js	1				0.0000	1.39%	0.0100	3.0
/javascript/ajax.js	1				0.0000	1.39%	0.0100	3.7
/javascript/ajax-tooltip.js	1				0.0000	1.39%	0.0100	3.7
/javascript/ajax-dynamic-content.js	1				0.0000	1.39%	0.0100	3.0
/index.php	1				0.0000	1.39%	0.0100	2.7
/images/xml_icon.png	1				0.0000	1.39%	0.0100	3.9
/images/webratna14.jpg	2				0.0000	2.78%	0.0100	4.3
/images/twitter_icon.png	1				0.0000	1.39%	0.0100	3.8
/images/tumblr_icon.gif	1				0.0000	1.39%	0.0100	3.9
/images/textsizePlus.gif	1				0.0000	1.39%	0.0100	3.4
/images/textsizeNormal.gif	1				0.0000	1.39%	0.0100	3.1
/images/textsizeMinus.gif	1				0.0000	1.39%	0.0100	3.7
/images/texthighContrast.gif	2				0.0000	2.78%	0.0100	3.7
/images/textNormal.gif	1				0.0000	1.39%	0.0100	3.5
/images/suggest.jpg	1				0.0000	1.39%	0.0100	3.9
/images/subscribe_mail.jpg	1				0.0000	1.39%	0.0100	3.7
/images/star_small.jpg	1				0.0000	1.39%	0.0100	4.5
/images/star.png	1				0.0000	1.39%	0.0100	4.3
/images/rss.png	1				0.0000	1.39%	0.0100	3.7
/images/rescue_uk.jpg	1				0.0000	1.39%	0.0100	4.2
/images/reddit_icon.png	1				0.0000	1.39%	0.0100	3.9
/images/print_icon6.jpg	1				0.0000	1.39%	0.0100	3.9
/images/pmrelieffund2012.jpg	1				0.0000	1.39%	0.0100	4.2
/images/pinterest_icon.png	1				0.0000	1.39%	0.0100	3.8
/images/orangenew.gif	1				0.0000	1.39%	0.0100	4.3
/images/nic_logo.png	1				0.0000	1.39%	0.0100	4.4
/images/mygov_banner.JPG	1				0.0000	1.39%	0.0100	4.2
/images/map.jpg	1				0.0000	1.39%	0.0100	4.4
/images/logo.png	1				0.0000	1.39%	0.0100	3.7
/images/linkedin_icon.png	1				0.0000	1.39%	0.0100	3.8
/images/line.gif	1				0.0000	1.39%	0.0100	3.4
/images/heading_star.png	1				0.0000	1.39%	0.0100	4.4
/images/greennew.gif	1				0.0000	1.39%	0.0100	4.3
/images/greenbarcurve4.png	1				0.0000	1.39%	0.0100	4.4
/images/greenbar4.png	1				0.0000	1.39%	0.0100	4.4

How many times does the browser ask the site to keep the connection alive?

We use the filter `http.connection == Keep-Alive && ip.dst == 164.100.58.217` to filter out keep-alive packets sent to goidirectory.nic.in. We find that the browser sends a total of 72 keep-alive packets to the server at goidirectory.nic.in.


website roam capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.connection == Keep-Alive && ip.dst == 164.100.58.217

No.	Time	Source	Destination	Protocol	Length	Info
127	2.698199	192.168.9.87	164.100.58.217	HTTP	433	GET / HTTP/1.1
138	2.763351	192.168.9.87	164.100.58.217	HTTP	442	GET /index.php HTTP/1.1
150	2.887056	192.168.9.87	164.100.58.217	HTTP	465	GET /css/style1.css HTTP/1.1
202	3.010581	192.168.9.87	164.100.58.217	HTTP	471	GET /css/static_style.css HTTP/1.1
209	3.012022	192.168.9.87	164.100.58.217	HTTP	459	GET /javascript/functions.js HTTP/1.1
210	3.012025	192.168.9.87	164.100.58.217	HTTP	470	GET /javascript/ajax-dynamic-content.js HTTP/1.1
211	3.012036	192.168.9.87	164.100.58.217	HTTP	473	GET /css/unionnew_style.css HTTP/1.1
263	3.174909	192.168.9.87	164.100.58.217	HTTP	505	GET /images/textsizeNormal.gif HTTP/1.1
426	3.468286	192.168.9.87	164.100.58.217	HTTP	503	GET /images/textsizePlus.gif HTTP/1.1
430	3.468766	192.168.9.87	164.100.58.217	HTTP	465	GET /css/level2.css HTTP/1.1
433	3.469023	192.168.9.87	164.100.58.217	HTTP	471	GET /css/ajax-tooltip.css HTTP/1.1
434	3.469310	192.168.9.87	164.100.58.217	HTTP	469	GET /javascript/validation_frontend.js HTTP/1.1
438	3.470486	192.168.9.87	164.100.58.217	HTTP	460	GET /javascript/validation.js HTTP/1.1
446	3.498801	192.168.9.87	164.100.58.217	HTTP	495	GET /images/line.gif HTTP/1.1
449	3.500137	192.168.9.87	164.100.58.217	HTTP	501	GET /images/textNormal.gif HTTP/1.1
456	3.505598	192.168.9.87	164.100.58.217	HTTP	507	GET /images/bharatindiasmall.png HTTP/1.1
564	3.704399	192.168.9.87	164.100.58.217	HTTP	495	GET /images/logo.png HTTP/1.1
567	3.713414	192.168.9.87	164.100.58.217	HTTP	454	GET /javascript/ajax.js HTTP/1.1
570	3.715853	192.168.9.87	164.100.58.217	HTTP	462	GET /javascript/ajax-tooltip.js HTTP/1.1
606	3.782879	192.168.9.87	164.100.58.217	HTTP	507	GET /images/texthighContrast.gif HTTP/1.1
615	3.785432	192.168.9.87	164.100.58.217	HTTP	504	GET /images/textsizeMinus.gif HTTP/1.1
617	3.785733	192.168.9.87	164.100.58.217	HTTP	505	GET /images/subscribe_mail.jpg HTTP/1.1
623	3.797427	192.168.9.87	164.100.58.217	HTTP	494	GET /images/rss.png HTTP/1.1
637	3.810698	192.168.9.87	164.100.58.217	HTTP	498	GET /images/Share16.jpg HTTP/1.1
655	3.838904	192.168.9.87	164.100.58.217	HTTP	504	GET /images/facebook_icon.png HTTP/1.1
658	3.840351	192.168.9.87	164.100.58.217	HTTP	507	GET /images/google_plus_icon.png HTTP/1.1
659	3.840577	192.168.9.87	164.100.58.217	HTTP	503	GET /images/twitter_icon.png HTTP/1.1
664	3.841579	192.168.9.87	164.100.58.217	HTTP	504	GET /images/linkedin_icon.png HTTP/1.1
665	3.841886	192.168.9.87	164.100.58.217	HTTP	505	GET /images/pinterest_icon.png HTTP/1.1
680	3.867947	192.168.9.87	164.100.58.217	HTTP	503	GET /images/blogger_icon.jpg HTTP/1.1

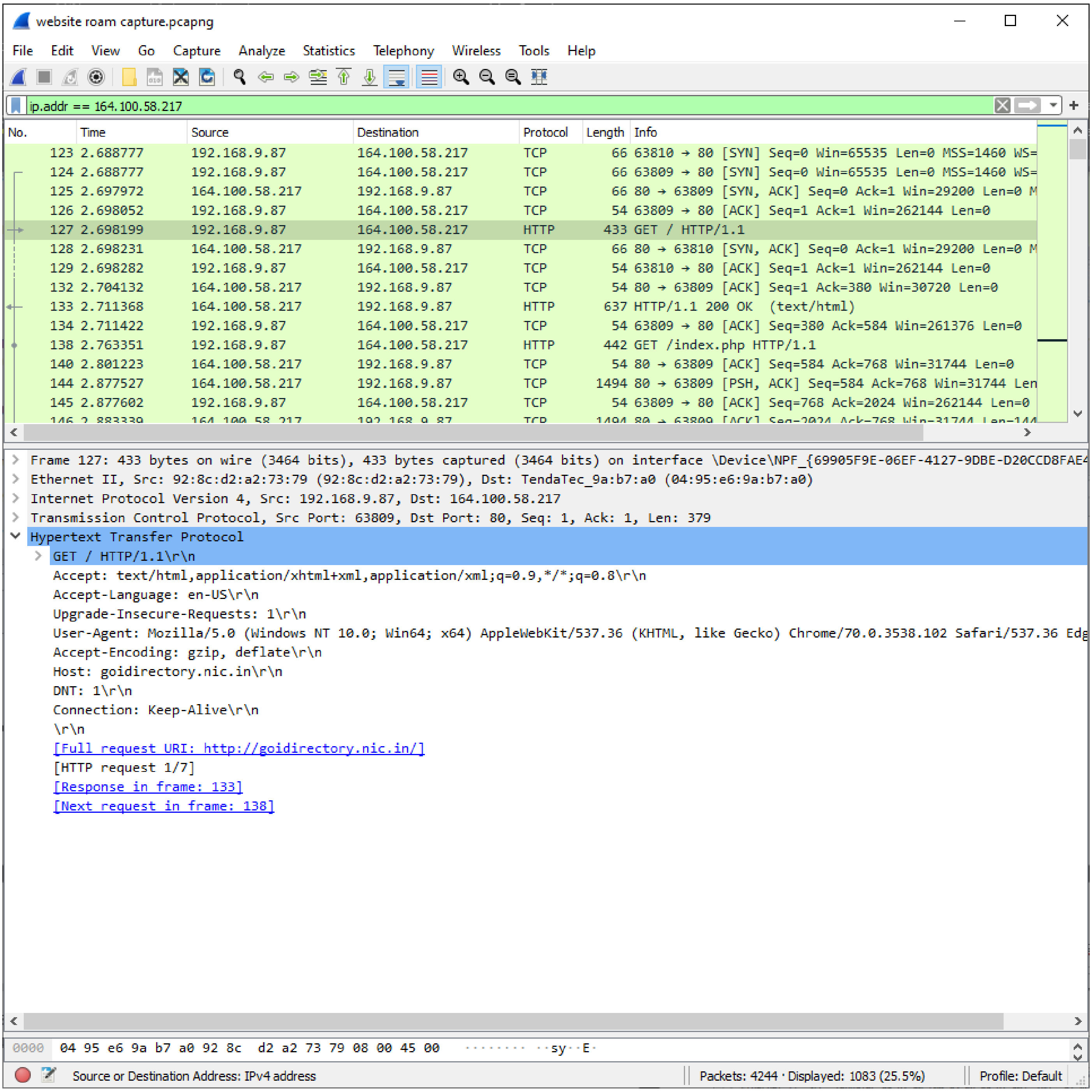
```
> Frame 446: 495 bytes on wire (3960 bits), 495 bytes captured (3960 bits) on interface \Device\NPF_{69905F9E-06EF-4127-9DBE-D20CCD8F.
> Ethernet II, Src: 92:8c:d2:a2:73:79 (92:8c:d2:a2:73:79), Dst: TendaTec_9a:b7:a0 (04:95:e6:9a:b7:a0)
v Internet Protocol Version 4, Src: 192.168.9.87, Dst: 164.100.58.217
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 481
    Identification: 0x74c1 (29889)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  04 95 e6 9a b7 a0 92 8c  d2 a2 73 79 08 00 45 00   ·········sy··E·
```

Destination: IPv4 address | Packets: 4244 · Displayed: 72 (1.7%) | Profile: Default

Which version of the HTTP is your browser running?

We observe that the requests sent by the browser contain the HTTP protocol as HTTP/1.1 in the header. From this, we can conclude that our browser is using HTTP/1.1.


website roam capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 164.100.58.217
```

```
No.   Time      Source          Destination     Protocol Length Info
  123 2.688777  192.168.9.87    164.100.58.217  TCP        66 63810 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=
  124 2.688777  192.168.9.87    164.100.58.217  TCP        66 63809 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=
  125 2.697972  164.100.58.217  192.168.9.87    TCP        66 80 → 63809 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 M
  126 2.698052  192.168.9.87    164.100.58.217  TCP        54 63809 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
  127 2.698199  192.168.9.87    164.100.58.217  HTTP      433 GET / HTTP/1.1
  128 2.698231  164.100.58.217  192.168.9.87    TCP        66 80 → 63810 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 M
  129 2.698282  192.168.9.87    164.100.58.217  TCP        54 63810 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
  132 2.704132  164.100.58.217  192.168.9.87    TCP        54 80 → 63809 [ACK] Seq=1 Ack=380 Win=30720 Len=0
  133 2.711368  164.100.58.217  192.168.9.87    HTTP      637 HTTP/1.1 200 OK  (text/html)
  134 2.711422  192.168.9.87    164.100.58.217  TCP        54 63809 → 80 [ACK] Seq=380 Ack=584 Win=261376 Len=0
  138 2.763351  192.168.9.87    164.100.58.217  HTTP      442 GET /index.php HTTP/1.1
  140 2.801223  164.100.58.217  192.168.9.87    TCP        54 80 → 63809 [ACK] Seq=584 Ack=768 Win=31744 Len=0
  144 2.877527  164.100.58.217  192.168.9.87    TCP      1494 80 → 63809 [PSH, ACK] Seq=584 Ack=768 Win=31744 Len
  145 2.877602  192.168.9.87    164.100.58.217  TCP        54 63809 → 80 [ACK] Seq=768 Ack=2024 Win=262144 Len=0
  146 2.883339  164.100.58.217  192.168.9.87    TCP      1494 80 → 63809 [ACK] Seq=2024 Ack=768 Win=31744 Len=144
```

```
> Frame 127: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface \Device\NPF_{69905F9E-06EF-4127-9DBE-D20CCD8FAE4
> Ethernet II, Src: 92:8c:d2:a2:73:79 (92:8c:d2:a2:73:79), Dst: TendaTec_9a:b7:a0 (04:95:e6:9a:b7:a0)
> Internet Protocol Version 4, Src: 192.168.9.87, Dst: 164.100.58.217
> Transmission Control Protocol, Src Port: 63809, Dst Port: 80, Seq: 1, Ack: 1, Len: 379
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US\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/70.0.3538.102 Safari/537.36 Edg
    Accept-Encoding: gzip, deflate\r\n
    Host: goidirectory.nic.in\r\n
    DNT: 1\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://goidirectory.nic.in/]
    [HTTP request 1/7]
    [Response in frame: 133]
    [Next request in frame: 138]
```

```
0000  04 95 e6 9a b7 a0 92 8c  d2 a2 73 79 08 00 45 00   ········ ··sy··E·
```

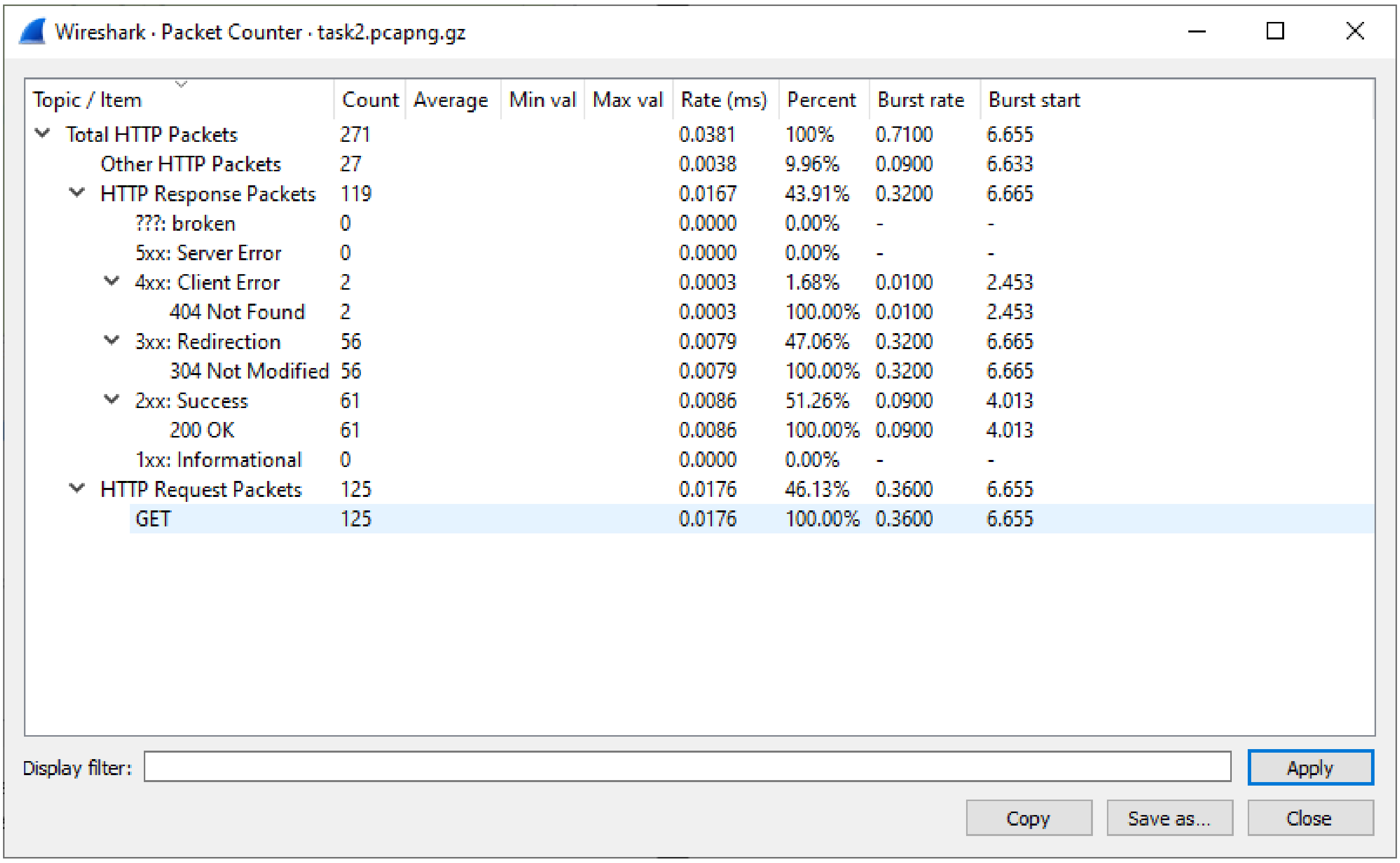
Source or Destination Address: IPv4 address | Packets: 4244 · Displayed: 1083 (25.5%) | Profile: Default

Task 2

How many conditional GETs are sent by the browser to the server?

We apply `ip.dst == 164.100.58.217 && http` filter to filter out packets that are sent from browser to server at http://goidirectory.nic.in/ (164.100.58.217). We find that there are 125 GET requests sent by the browser to the server.

Since the conditional GET uses 304 NOT MODIFIED status code, we check the HTTP statistics with this filter. We find that there are 56 conditional GET requests from the browser to the server.



Wireshark · Packet Counter · task2.pcapng.gz

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Total HTTP Packets	271				0.0381	100%	0.7100	6.655
Other HTTP Packets	27				0.0038	9.96%	0.0900	6.633
HTTP Response Packets	119				0.0167	43.91%	0.3200	6.665
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	2				0.0003	1.68%	0.0100	2.453
404 Not Found	2				0.0003	100.00%	0.0100	2.453
3xx: Redirection	56				0.0079	47.06%	0.3200	6.665
304 Not Modified	56				0.0079	100.00%	0.3200	6.665
2xx: Success	61				0.0086	51.26%	0.0900	4.013
200 OK	61				0.0086	100.00%	0.0900	4.013
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	125				0.0176	46.13%	0.3600	6.655
GET	125				0.0176	100.00%	0.3600	6.655

Display filter:

Make a list for each of the file/objects downloaded; how many times the server sends the full contents of the respective file/object?

We use HTTP request sequences in statistics to find the downloaded files and the number of times these were downloaded. The full list is as follows:

Topic / Item	Count
http://goidirectory.nic.in/sow_images/thumb/14967_small_namayush.png	1
http://goidirectory.nic.in/rss/rss_icon.gif	1
http://goidirectory.nic.in/javascript/validation_frontend.js	1
http://goidirectory.nic.in/javascript/validation.js	1
http://goidirectory.nic.in/javascript/functions.js	1
http://goidirectory.nic.in/javascript/ajax.js	1
http://goidirectory.nic.in/javascript/ajax-tooltip.js	1
http://goidirectory.nic.in/javascript/ajax-dynamic-content.js	1
http://goidirectory.nic.in/images/xml_icon.png	1
http://goidirectory.nic.in/images/webratna14.jpg	1

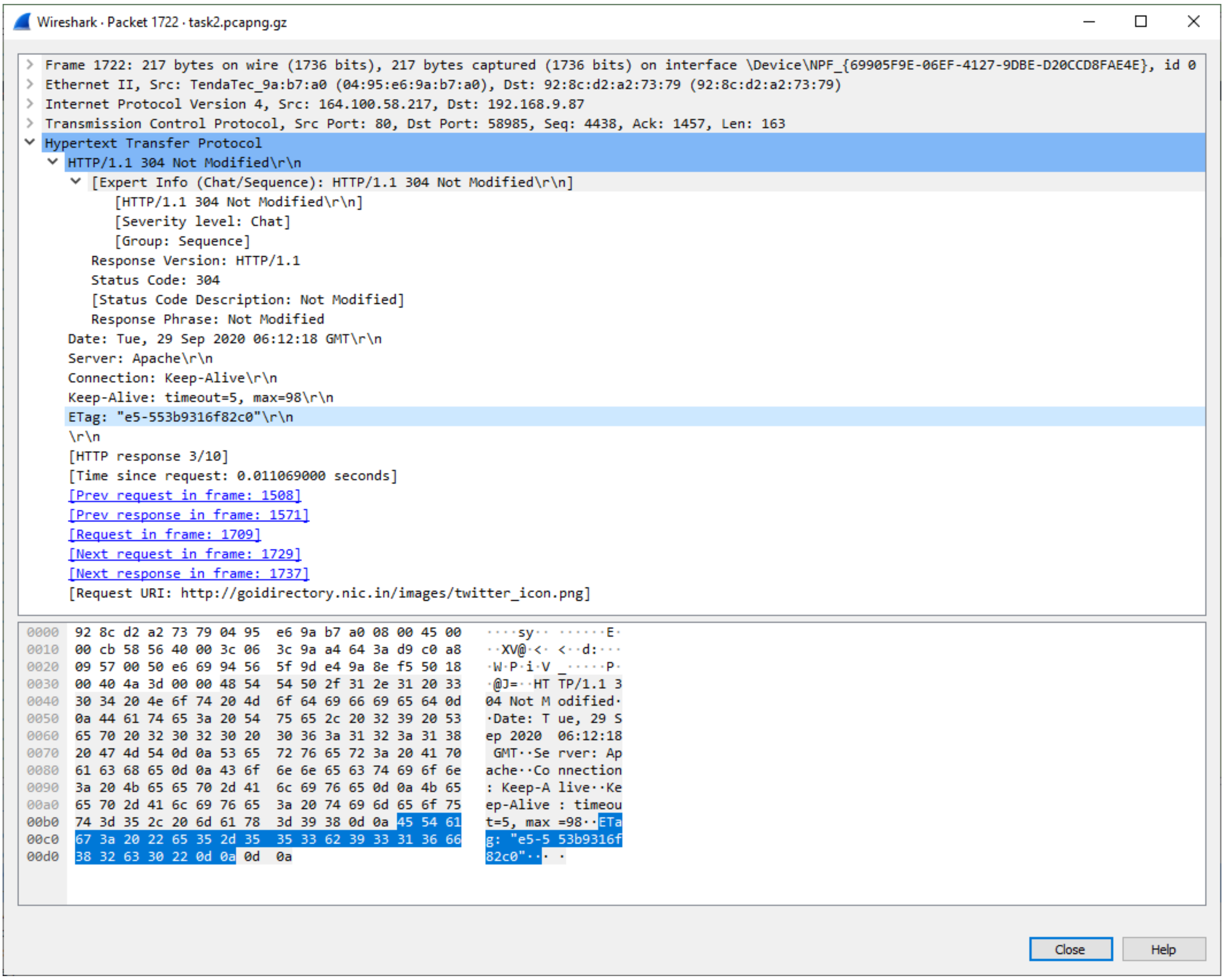
http://goidirectory.nic.in/images/twitter_icon.png	1
http://goidirectory.nic.in/images/tumblr_icon.gif	1
http://goidirectory.nic.in/images/textsizePlus.gif	1
http://goidirectory.nic.in/images/textsizeNormal.gif	1
http://goidirectory.nic.in/images/textsizeMinus.gif	1
http://goidirectory.nic.in/images/texthighContrast.gif	1
http://goidirectory.nic.in/images/textNormal.gif	1
http://goidirectory.nic.in/images/suggest.jpg	1
http://goidirectory.nic.in/images/subscribe_mail.jpg	1
http://goidirectory.nic.in/images/star_small.jpg	1
http://goidirectory.nic.in/images/star.png	1
http://goidirectory.nic.in/images/rss.png	1
http://goidirectory.nic.in/images/rescue_uk.jpg	1
http://goidirectory.nic.in/images/reddit_icon.png	1
http://goidirectory.nic.in/images/print_icon6.jpg	1
http://goidirectory.nic.in/images/pmrelieffund2012.jpg	1
http://goidirectory.nic.in/images/pinterest_icon.png	1
http://goidirectory.nic.in/images/orangenew.gif	1
http://goidirectory.nic.in/images/nic_logo.png	1
http://goidirectory.nic.in/images/mygov_banner.JPG	1
http://goidirectory.nic.in/images/map.jpg	1
http://goidirectory.nic.in/images/logo.png	1
http://goidirectory.nic.in/images/linkedin_icon.png	1
http://goidirectory.nic.in/images/line.gif	3
http://goidirectory.nic.in/images/heading_star.png	1
http://goidirectory.nic.in/images/greennew.gif	1
http://goidirectory.nic.in/images/greenbarcurve4.png	1
http://goidirectory.nic.in/images/greenbar4.png	1
http://goidirectory.nic.in/images/google_plus_icon.png	1
http://goidirectory.nic.in/images/facebook_icon.png	1
http://goidirectory.nic.in/images/expand-bulett.gif	1
http://goidirectory.nic.in/images/dot.gif	1
http://goidirectory.nic.in/images/digg_icon.png	1
http://goidirectory.nic.in/images/delicious_icon.jpg	1
http://goidirectory.nic.in/images/data_gov.jpg	1
http://goidirectory.nic.in/images/corner_orange.png	1
http://goidirectory.nic.in/images/blogger_icon.jpg	1
http://goidirectory.nic.in/images/bharatindiasmall.png	1
http://goidirectory.nic.in/images/bg_stripes_new.gif	1
http://goidirectory.nic.in/images/bg_header.png	1
http://goidirectory.nic.in/images/banner.jpg	1
http://goidirectory.nic.in/images/StumbleUpon_icon.png	1
http://goidirectory.nic.in/images/Share16.jpg	1
http://goidirectory.nic.in/css/unionnew_style.css	1
http://goidirectory.nic.in/css/style1.css	1
http://goidirectory.nic.in/css/static_style.css	1
http://goidirectory.nic.in/css/level2.css	1
http://goidirectory.nic.in/css/ajax-tooltip.css	3

Explain in detail what is the difference in server's behaviour between first and second request/browsing?

We see that for the first time, the webpage is requested all the resources such as images and scripts are sent by the server to the browser. The next time we load the page, a lot of the GET requests return with code 304 NOT MODIFIED. This indicates to the browser that the respective file has not changed on the server and to fetch the resource from browser’s cache. The contents of these resources are not provided by the server to the browser. This results in much faster page loading times as the resources do not need to be fetched again.

List the headers of HTTP which influence this functionality.

The header which influences this functionality is the ETag header. This header stores the information about the version of resource stored in the cache. This allows the caches to be more efficient and allows the browser to renew the resource in its cache if the resource changes on the server as a new ETag code is generated every time a resource is updated/ generated.



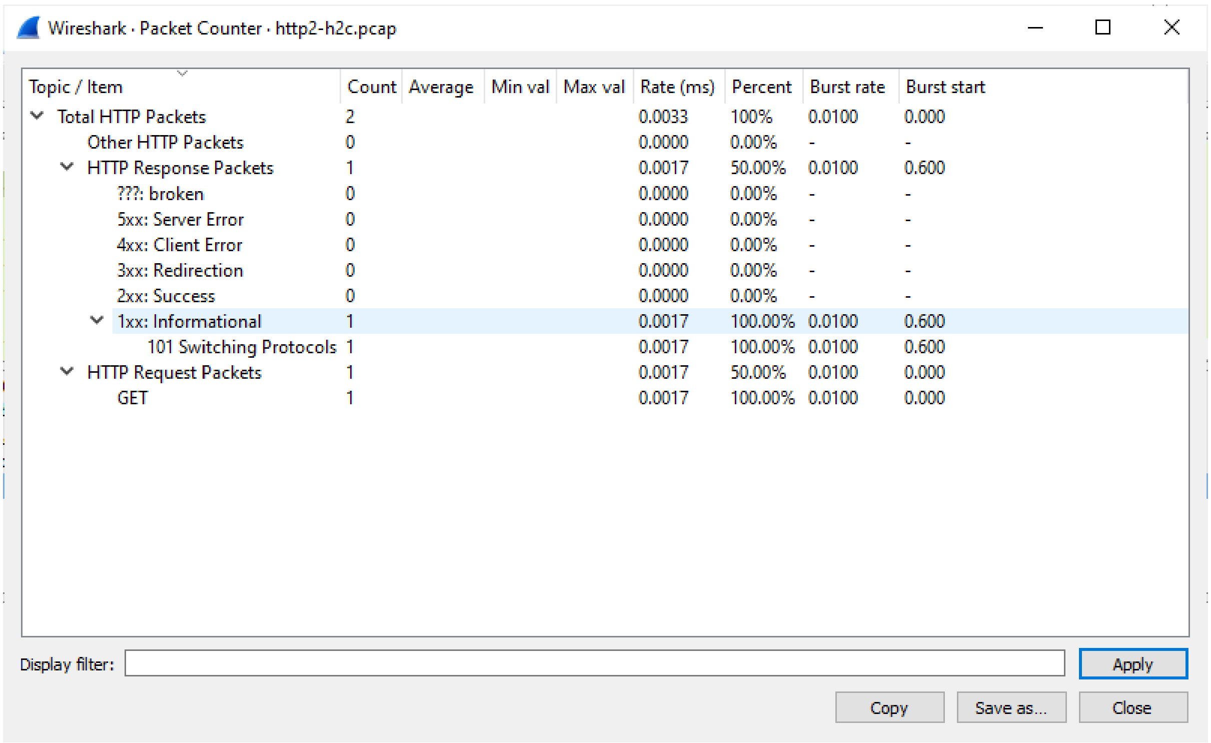
```
> Frame 1722: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{69905F9E-06EF-4127-9DBE-D20CCD8FAE4E}, id 0
> Ethernet II, Src: TendaTec_9a:b7:a0 (04:95:e6:9a:b7:a0), Dst: 92:8c:d2:a2:73:79 (92:8c:d2:a2:73:79)
> Internet Protocol Version 4, Src: 164.100.58.217, Dst: 192.168.9.87
> Transmission Control Protocol, Src Port: 80, Dst Port: 58985, Seq: 4438, Ack: 1457, Len: 163
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        [HTTP/1.1 304 Not Modified\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Tue, 29 Sep 2020 06:12:18 GMT\r\n
    Server: Apache\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=98\r\n
    ETag: "e5-553b9316f82c0"\r\n
    \r\n
    [HTTP response 3/10]
    [Time since request: 0.011069000 seconds]
    [Prev request in frame: 1508]
    [Prev response in frame: 1571]
    [Request in frame: 1709]
    [Next request in frame: 1729]
    [Next response in frame: 1737]
    [Request URI: http://goidirectory.nic.in/images/twitter_icon.png]
```

```
0000  92 8c d2 a2 73 79 04 95  e6 9a b7 a0 08 00 45 00   ····sy·· ······E·
0010  00 cb 58 56 40 00 3c 06  3c 9a a4 64 3a d9 c0 a8   ··XV@·<· <··d:···
0020  09 57 00 50 e6 69 94 56  5f 9d e4 9a 8e f5 50 18   ·W·P·i·V _·····P·
0030  00 40 4a 3d 00 00 48 54  54 50 2f 31 2e 31 20 33   ·@J=··HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified·
0050  0a 44 61 74 65 3a 20 54  75 65 2c 20 32 39 20 53   ·Date: T ue, 29 S
0060  65 70 20 32 30 32 30 20  30 36 3a 31 32 3a 31 38   ep 2020  06:12:18
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0080  61 63 68 65 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   ache··Co nnection
0090  3a 20 4b 65 65 70 2d 41  6c 69 76 65 0d 0a 4b 65   : Keep-A live··Ke
00a0  65 70 2d 41 6c 69 76 65  3a 20 74 69 6d 65 6f 75   ep-Alive : timeou
00b0  74 3d 35 2c 20 6d 61 78  3d 39 38 0d 0a 45 54 61   t=5, max =98··ETa
00c0  67 3a 20 22 65 35 2d 35  35 33 62 39 33 31 36 66   g: "e5-5 53b9316f
00d0  38 32 63 30 22 0d 0a 0d  0a                        82c0"··· ·
```

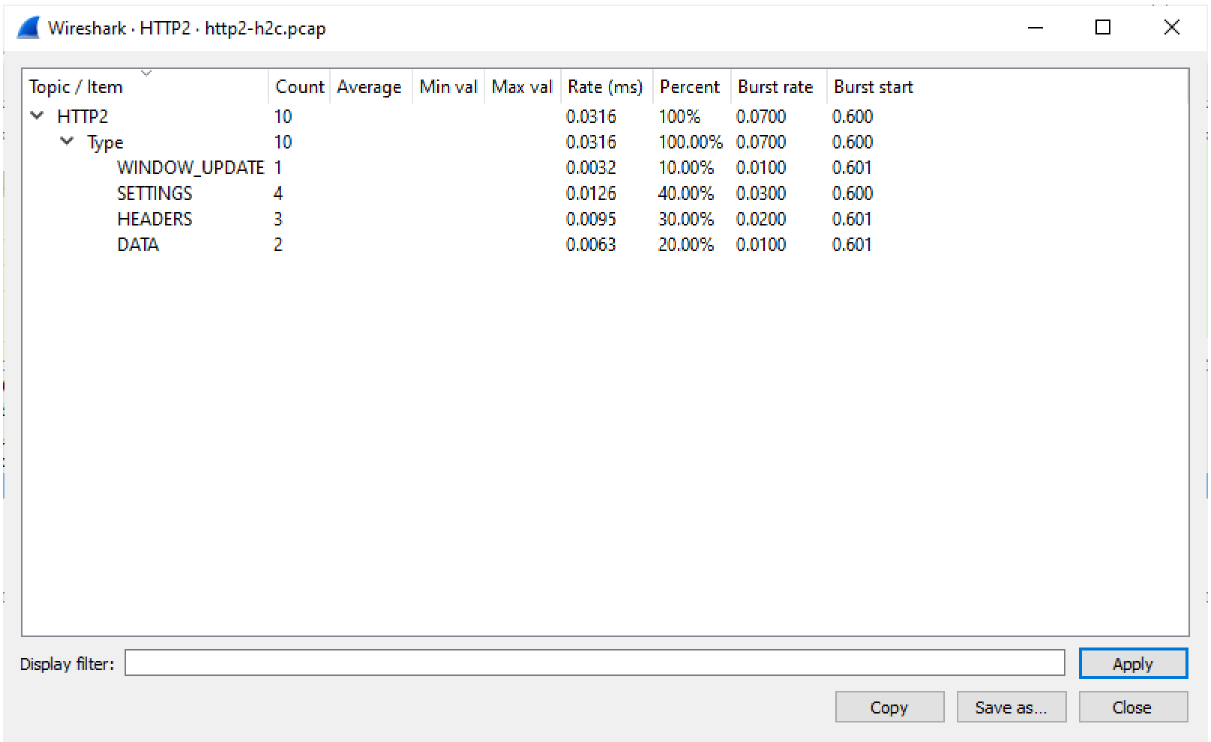
Task 3

How many HTTP/2 and HTTP/1.1 packets are present?

The capture contains 10 HTTP/2 packets and 2 HTTP/1.1 packets. This can be seen in the stats shown by HTTP -> packet counter for HTTP/1.1 and HTTP2 for HTTP/2



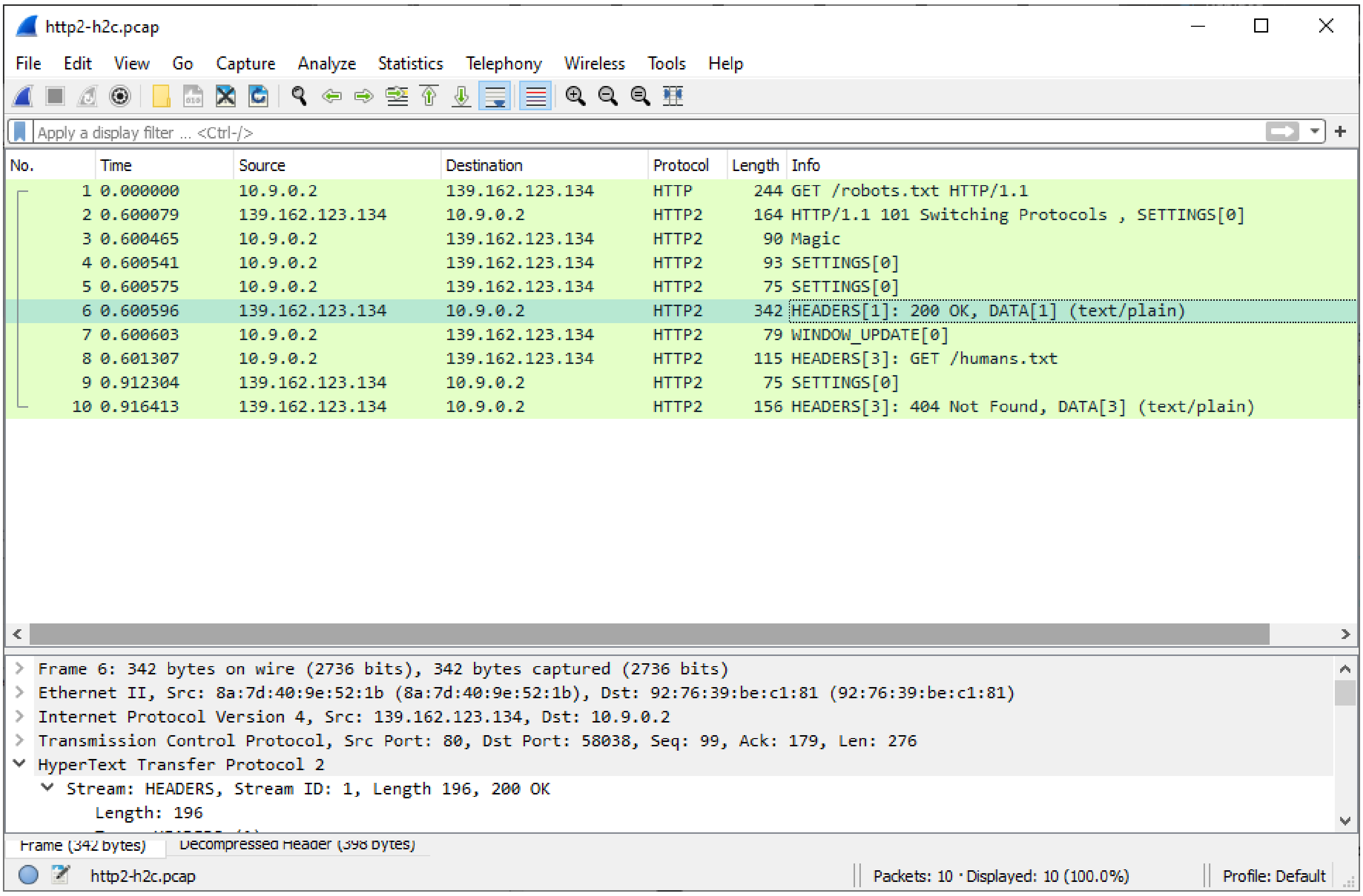
Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Total HTTP Packets	2				0.0033	100%	0.0100	0.000
Other HTTP Packets	0				0.0000	0.00%	-	-
HTTP Response Packets	1				0.0017	50.00%	0.0100	0.600
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
3xx: Redirection	0				0.0000	0.00%	-	-
2xx: Success	0				0.0000	0.00%	-	-
1xx: Informational	1				0.0017	100.00%	0.0100	0.600
101 Switching Protocols	1				0.0017	100.00%	0.0100	0.600
HTTP Request Packets	1				0.0017	50.00%	0.0100	0.000
GET	1				0.0017	100.00%	0.0100	0.000



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
HTTP2	10				0.0316	100%	0.0700	0.600
Type	10				0.0316	100.00%	0.0700	0.600
WINDOW_UPDATE	1				0.0032	10.00%	0.0100	0.601
SETTINGS	4				0.0126	40.00%	0.0300	0.600
HEADERS	3				0.0095	30.00%	0.0200	0.601
DATA	2				0.0063	20.00%	0.0100	0.601

How many HTTP/2 packets are exchanged between the client and server here before the first object is fetched?

We see that the first packet in which data is transferred is packet number 6. Since the first packet is HTTP/1.1 packet, there are four HTTP/2 packets that are exchanged before the first object is fetched.



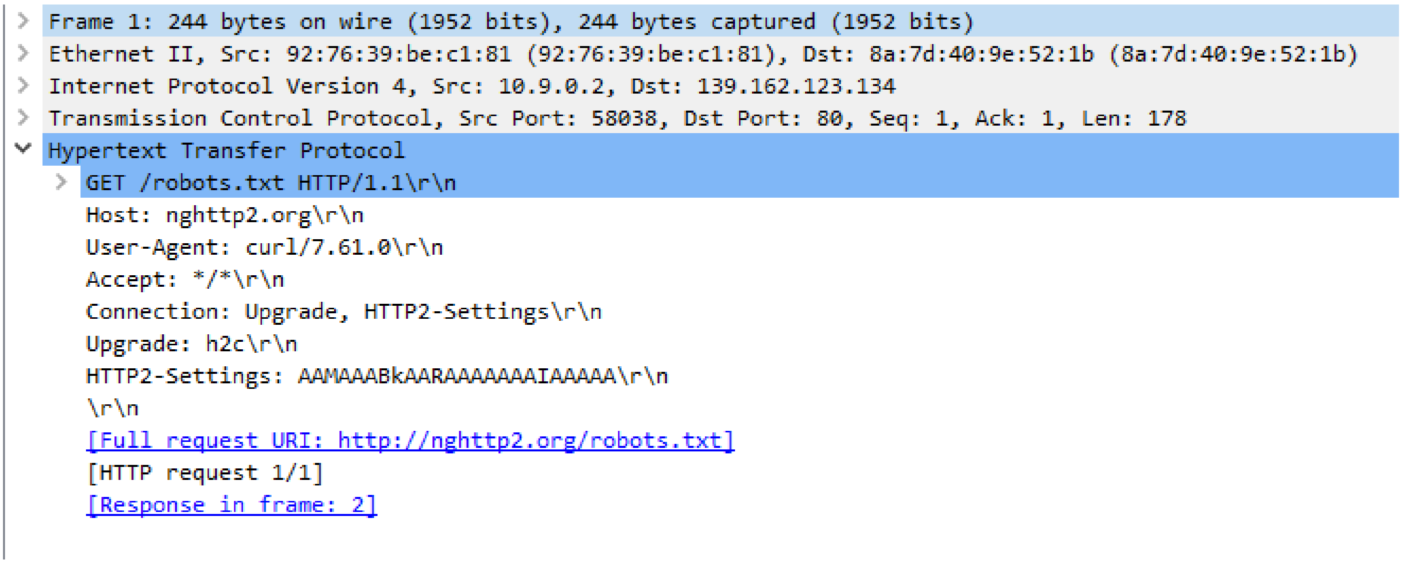
http2-h2c.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source           Destination      Protocol Length Info
   1 0.000000  10.9.0.2         139.162.123.134  HTTP      244 GET /robots.txt HTTP/1.1
   2 0.600079  139.162.123.134  10.9.0.2         HTTP2     164 HTTP/1.1 101 Switching Protocols , SETTINGS[0]
   3 0.600465  10.9.0.2         139.162.123.134  HTTP2      90 Magic
   4 0.600541  10.9.0.2         139.162.123.134  HTTP2      93 SETTINGS[0]
   5 0.600575  10.9.0.2         139.162.123.134  HTTP2      75 SETTINGS[0]
   6 0.600596  139.162.123.134  10.9.0.2         HTTP2     342 HEADERS[1]: 200 OK, DATA[1] (text/plain)
   7 0.600603  10.9.0.2         139.162.123.134  HTTP2      79 WINDOW_UPDATE[0]
   8 0.601307  10.9.0.2         139.162.123.134  HTTP2     115 HEADERS[3]: GET /humans.txt
   9 0.912304  139.162.123.134  10.9.0.2         HTTP2      75 SETTINGS[0]
  10 0.916413  139.162.123.134  10.9.0.2         HTTP2     156 HEADERS[3]: 404 Not Found, DATA[3] (text/plain)
```

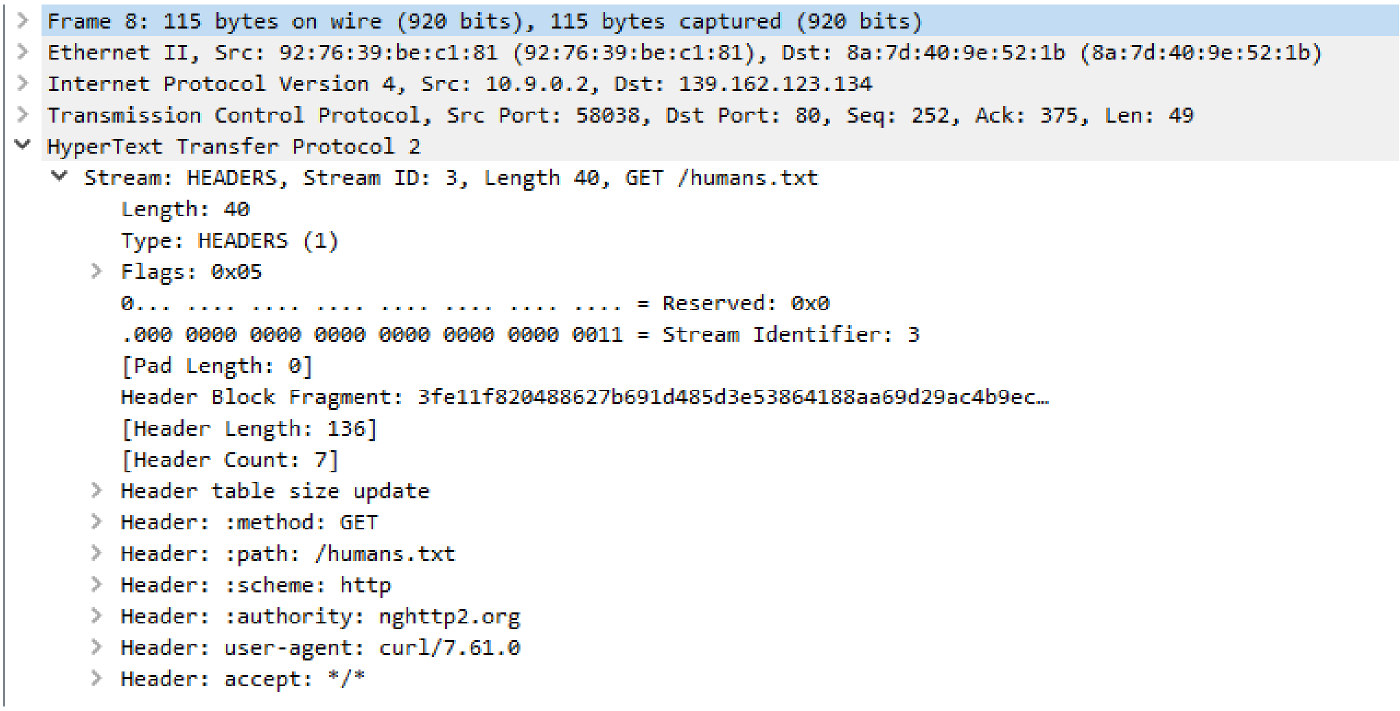
```
> Frame 6: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b), Dst: 92:76:39:be:c1:81 (92:76:39:be:c1:81)
> Internet Protocol Version 4, Src: 139.162.123.134, Dst: 10.9.0.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 58038, Seq: 99, Ack: 179, Len: 276
v HyperText Transfer Protocol 2
  v Stream: HEADERS, Stream ID: 1, Length 196, 200 OK
        Length: 196
```

Frame (342 bytes)
Decompressed Header (398 bytes)
http2-h2c.pcap
Packets: 10 · Displayed: 10 (100.0%)
Profile: Default

What main difference do you observe in headers of HTTP/2 packets displayed here, compared to the headers of HTTP/1.1 packets?



```
> Frame 1: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)
> Ethernet II, Src: 92:76:39:be:c1:81 (92:76:39:be:c1:81), Dst: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b)
> Internet Protocol Version 4, Src: 10.9.0.2, Dst: 139.162.123.134
> Transmission Control Protocol, Src Port: 58038, Dst Port: 80, Seq: 1, Ack: 1, Len: 178
v Hypertext Transfer Protocol
  > GET /robots.txt HTTP/1.1\r\n
    Host: nghttp2.org\r\n
    User-Agent: curl/7.61.0\r\n
    Accept: */*\r\n
    Connection: Upgrade, HTTP2-Settings\r\n
    Upgrade: h2c\r\n
    HTTP2-Settings: AAMAAABkAARAAAAAAAIAAAAA\r\n
    \r\n
    [Full request URI: http://nghttp2.org/robots.txt]
    [HTTP request 1/1]
    [Response in frame: 2]
```



```
> Frame 8: 115 bytes on wire (920 bits), 115 bytes captured (920 bits)
> Ethernet II, Src: 92:76:39:be:c1:81 (92:76:39:be:c1:81), Dst: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b)
> Internet Protocol Version 4, Src: 10.9.0.2, Dst: 139.162.123.134
> Transmission Control Protocol, Src Port: 58038, Dst Port: 80, Seq: 252, Ack: 375, Len: 49
v HyperText Transfer Protocol 2
  v Stream: HEADERS, Stream ID: 3, Length 40, GET /humans.txt
      Length: 40
      Type: HEADERS (1)
    > Flags: 0x05
      0... .... .... .... .... .... .... .... = Reserved: 0x0
      .000 0000 0000 0000 0000 0000 0000 0011 = Stream Identifier: 3
      [Pad Length: 0]
      Header Block Fragment: 3fe11f820488627b691d485d3e53864188aa69d29ac4b9ec…
      [Header Length: 136]
      [Header Count: 7]
    > Header table size update
    > Header: :method: GET
    > Header: :path: /humans.txt
    > Header: :scheme: http
    > Header: :authority: nghttp2.org
    > Header: user-agent: curl/7.61.0
    > Header: accept: */*
```

We are comparing the HTTP/1.1 packet for GET /robots.txt and HTTP/2 packet for GET /humans.txt.

The first thing we notice is HTTP/2 has more header fields than HTTP/1.1. The HTTP/2 header has flags and stream identifiers that are not present in HTTP/1.1 header. Since there is a presence of header block fragment it might be possible for the header to be divided into parts, and each part can be provided a sequence number which can then combine at the receiver to form a single header. One more thing is the header table size update, which is not present in HTTP/1.1 but present in HTTP/2. This is used to update the dynamic table as specified in RFC7541.

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my responsibility to report honour violations by other students if I become aware of it.