19CSE301 Computer Networks Lab

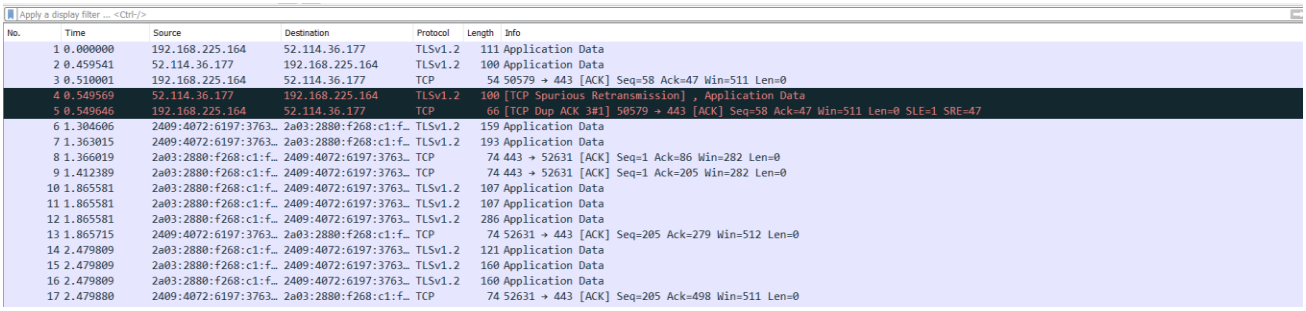
Lab Sheet 2

Analyzing HTTP using Wireshark

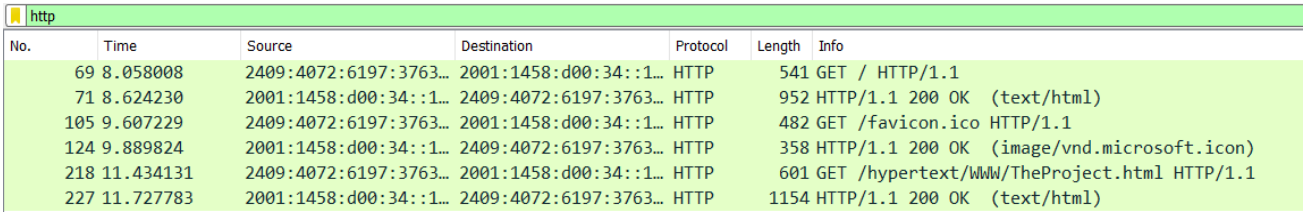
S Abhishek

AM.EN.U4CSE19147

1. Open Packet sniffer [Wireshark] Application and Capture **YOUR NETWORK** Interface.

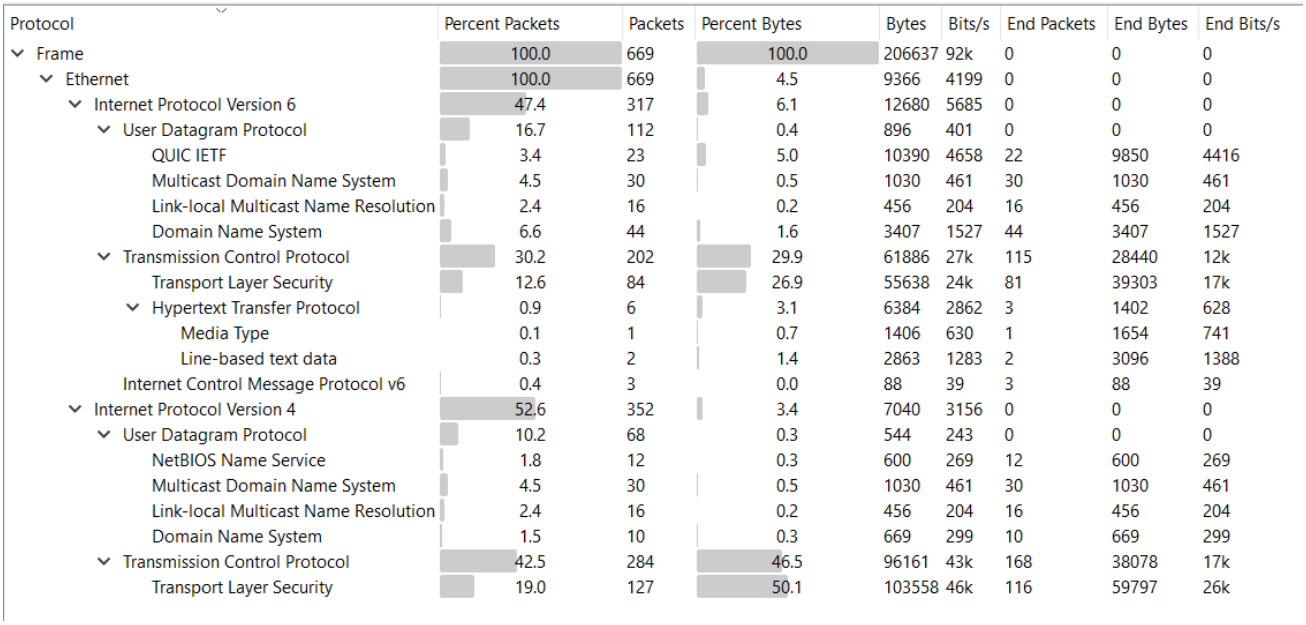


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.225.164	52.114.36.177	TLSv1.2	111	Application Data
2	0.459541	52.114.36.177	192.168.225.164	TLSv1.2	100	Application Data
3	0.510001	192.168.225.164	52.114.36.177	TCP	54	50579 → 443 [ACK] Seq=58 Ack=47 Win=511 Len=0
4	0.549569	52.114.36.177	192.168.225.164	TLSv1.2	100	[TCP Spurious Retransmission] , Application Data
5	0.549646	192.168.225.164	52.114.36.177	TCP	66	[TCP Dup ACK 3#1] 50579 → 443 [ACK] Seq=58 Ack=47 Win=511 Len=0 SLE=1 SRE=47
6	1.304606	2409:4072:6197:3763…	2a03:2880:f268:c1:f…	TLSv1.2	159	Application Data
7	1.363015	2409:4072:6197:3763…	2a03:2880:f268:c1:f…	TLSv1.2	193	Application Data
8	1.366019	2a03:2880:f268:c1:f…	2409:4072:6197:3763…	TCP	74	443 → 52631 [ACK] Seq=1 Ack=86 Win=282 Len=0
9	1.412389	2a03:2880:f268:c1:f…	2409:4072:6197:3763…	TCP	74	443 → 52631 [ACK] Seq=1 Ack=205 Win=282 Len=0
10	1.865581	2a03:2880:f268:c1:f…	2409:4072:6197:3763…	TLSv1.2	107	Application Data
11	1.865581	2a03:2880:f268:c1:f…	2409:4072:6197:3763…	TLSv1.2	107	Application Data
12	1.865581	2a03:2880:f268:c1:f…	2409:4072:6197:3763…	TLSv1.2	286	Application Data
13	1.865715	2409:4072:6197:3763…	2a03:2880:f268:c1:f…	TCP	74	52631 → 443 [ACK] Seq=205 Ack=279 Win=512 Len=0
14	2.479809	2a03:2880:f268:c1:f…	2409:4072:6197:3763…	TLSv1.2	121	Application Data
15	2.479809	2a03:2880:f268:c1:f…	2409:4072:6197:3763…	TLSv1.2	160	Application Data
16	2.479809	2a03:2880:f268:c1:f…	2409:4072:6197:3763…	TLSv1.2	160	Application Data
17	2.479880	2409:4072:6197:3763…	2a03:2880:f268:c1:f…	TCP	74	52631 → 443 [ACK] Seq=205 Ack=498 Win=511 Len=0



http

No.	Time	Source	Destination	Protocol	Length	Info
69	8.058008	2409:4072:6197:3763…	2001:1458:d00:34::1…	HTTP	541	GET / HTTP/1.1
71	8.624230	2001:1458:d00:34::1…	2409:4072:6197:3763…	HTTP	952	HTTP/1.1 200 OK (text/html)
105	9.607229	2409:4072:6197:3763…	2001:1458:d00:34::1…	HTTP	482	GET /favicon.ico HTTP/1.1
124	9.889824	2001:1458:d00:34::1…	2409:4072:6197:3763…	HTTP	358	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
218	11.434131	2409:4072:6197:3763…	2001:1458:d00:34::1…	HTTP	601	GET /hypertext/WWW/TheProject.html HTTP/1.1
227	11.727783	2001:1458:d00:34::1…	2409:4072:6197:3763…	HTTP	1154	HTTP/1.1 200 OK (text/html)



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	669	100.0	206637	92k	0	0	0
Ethernet	100.0	669	4.5	9366	4199	0	0	0
Internet Protocol Version 6	47.4	317	6.1	12680	5685	0	0	0
User Datagram Protocol	16.7	112	0.4	896	401	0	0	0
QUIC IETF	3.4	23	5.0	10390	4658	22	9850	4416
Multicast Domain Name System	4.5	30	0.5	1030	461	30	1030	461
Link-local Multicast Name Resolution	2.4	16	0.2	456	204	16	456	204
Domain Name System	6.6	44	1.6	3407	1527	44	3407	1527
Transmission Control Protocol	30.2	202	29.9	61886	27k	115	28440	12k
Transport Layer Security	12.6	84	26.9	55638	24k	81	39303	17k
Hypertext Transfer Protocol	0.9	6	3.1	6384	2862	3	1402	628
Media Type	0.1	1	0.7	1406	630	1	1654	741
Line-based text data	0.3	2	1.4	2863	1283	2	3096	1388
Internet Control Message Protocol v6	0.4	3	0.0	88	39	3	88	39
Internet Protocol Version 4	52.6	352	3.4	7040	3156	0	0	0
User Datagram Protocol	10.2	68	0.3	544	243	0	0	0
NetBIOS Name Service	1.8	12	0.3	600	269	12	600	269
Multicast Domain Name System	4.5	30	0.5	1030	461	30	1030	461
Link-local Multicast Name Resolution	2.4	16	0.2	456	204	16	456	204
Domain Name System	1.5	10	0.3	669	299	10	669	299
Transmission Control Protocol	42.5	284	46.5	96161	43k	168	38078	17k
Transport Layer Security	19.0	127	50.1	103558	46k	116	59797	26k

A – Request for a web page from amrita.edu and search for some keyword in the webpage.

1007	10.267535	192.168.225.164	192.168.225.1	DNS	74	Standard query 0x73e3 AAAA www.amrita.edu
1008	10.267535	192.168.225.164	192.168.225.1	DNS	80	Standard query 0xc013 A fonts.googleapis.com
1009	10.267536	192.168.225.164	192.168.225.1	DNS	80	Standard query 0x50ef AAAA fonts.googleapis.com
1010	10.267539	192.168.225.164	192.168.225.1	DNS	76	Standard query 0x1827 AAAA cdn.jsdelivr.net
1011	10.267544	192.168.225.164	192.168.225.1	DNS	76	Standard query 0x4964 A cdn.jsdelivr.net
1012	10.363384	fe80::44c3:20ff:fe4…	fe80::a038:fe5f:7dd…	DNS	157	Standard query response 0x73e3 AAAA www.amrita.edu CNAME amrita.edu SOA ns1.amrita.edu
1013	10.371404	fe80::44c3:20ff:fe4…	fe80::a038:fe5f:7dd…	DNS	116	Standard query response 0xc013 A fonts.googleapis.com A 172.217.166.106
1014	10.371404	fe80::44c3:20ff:fe4…	fe80::a038:fe5f:7dd…	DNS	128	Standard query response 0x50ef AAAA fonts.googleapis.com AAAA 2404:6800:4009:801::200a
1015	10.371404	fe80::44c3:20ff:fe4…	fe80::a038:fe5f:7dd…	DNS	146	Standard query response 0x4964 A cdn.jsdelivr.net CNAME jsdelivr.map.fastly.net A 151.101.157.229
1016	10.371404	fe80::44c3:20ff:fe4…	fe80::a038:fe5f:7dd…	DNS	158	Standard query response 0x1827 AAAA cdn.jsdelivr.net CNAME jsdelivr.map.fastly.net AAAA 2a04:4e42:25::485
1017	10.379457	157.240.228.60	192.168.225.164	TCP	54	443 → 59747 [ACK] Seq=1 Ack=32 Win=439 Len=0
1018	10.383316	192.168.225.164	103.10.24.196	TCP	66	52794 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1019	10.383806	fe80::a038:fe5f:7dd…	ff02::1:3	LLMNR	90	Standard query 0xc8d7 AAAA sfziasohmb

```
Frame 1012: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface \Device\NPF_{83E20D82-7C71-476A-9C13-1D72C91D36AE}, id 0
  Interface id: 0 (\Device\NPF_{83E20D82-7C71-476A-9C13-1D72C91D36AE})
      Interface name: \Device\NPF_{83E20D82-7C71-476A-9C13-1D72C91D36AE}
      Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 25, 2021 08:15:18.987918000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1629859518.987918000 seconds
    [Time delta from previous captured frame: 0.095840000 seconds]
    [Time delta from previous displayed frame: 0.095840000 seconds]
    [Time since reference or first frame: 10.363384000 seconds]
    Frame Number: 1012
    Frame Length: 157 bytes (1256 bits)
    Capture Length: 157 bytes (1256 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: 46:c3:20:4f:88:7e (46:c3:20:4f:88:7e), Dst: IntelCor_8e:5f:f3 (0c:54:15:8e:5f:f3)
  Destination: IntelCor_8e:5f:f3 (0c:54:15:8e:5f:f3)
      Address: IntelCor_8e:5f:f3 (0c:54:15:8e:5f:f3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: 46:c3:20:4f:88:7e (46:c3:20:4f:88:7e)
      Address: 46:c3:20:4f:88:7e (46:c3:20:4f:88:7e)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fe80::44c3:20ff:fe4c:857b, Dst: fe80::a038:fe5f:7dda:4228
    0110 .... = Version: 6
```

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	15310	100.0	15381563	2599k	0	0	0
Ethernet	100.0	15310	1.4	214340	36k	0	0	0
Internet Protocol Version 6	11.0	1683	0.4	67320	11k	0	0	0
User Datagram Protocol	3.7	571	0.0	4568	772	0	0	0
QUIC IETF	3.0	464	1.8	281972	47k	425	254399	43k
Multicast Domain Name System	0.2	24	0.0	824	139	24	824	139
Link-local Multicast Name Resolution	0.1	12	0.0	340	57	12	340	57
Domain Name System	0.7	110	0.1	8277	1399	110	8277	1399
Transmission Control Protocol	7.2	1098	4.0	611702	103k	483	99135	16k
Transport Layer Security	4.1	629	3.9	604486	102k	615	566680	95k
Internet Control Message Protocol v6	0.1	14	0.0	432	73	14	432	73
Internet Protocol Version 4	89.0	13622	1.8	272440	46k	0	0	0

158	3.811498	fe80::a038:fe5f:7dd…	fe80::44c3:20ff:fe4…	DNS	95	Standard query 0x7b37 AAAA scratchpads.org
159	3.814196	fe80::44c3:20ff:fe4…	fe80::a038:fe5f:7dd…	DNS	95	Standard query response 0x7b37 AAAA scratchpads.org
160	3.816535	192.168.225.164	157.140.2.32	TCP	66	55549 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
161	3.816952	192.168.225.164	157.140.2.32	TCP	66	60864 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
162	3.937674	fe80::a038:fe5f:7dd…	fe80::44c3:20ff:fe4…	DNS	96	Standard query 0xc519 A api.hsselite.com
163	3.938209	fe80::a038:fe5f:7dd…	fe80::44c3:20ff:fe4…	DNS	96	Standard query 0x4473 AAAA api.hsselite.com
164	3.948125	fe80::a038:fe5f:7dd…	fe80::44c3:20ff:fe4…	DNS	100	Standard query 0xd933 AAAA event.shelljacket.us
165	3.951369	fe80::44c3:20ff:fe4…	fe80::a038:fe5f:7dd…	DNS	100	Standard query response 0xd933 AAAA event.shelljacket.us
166	3.952421	192.168.225.164	209.97.170.78	TCP	66	65072 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
167	3.955358	192.168.225.164	157.140.2.32	TCP	66	55069 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
168	3.998742	fe80::44c3:20ff:fe4…	fe80::a038:fe5f:7dd…	DNS	128	Standard query response 0xc519 A api.hsselite.com A 52.9.81.184 A 184.169.221.190
169	4.003953	fe80::44c3:20ff:fe4…	fe80::a038:fe5f:7dd…	DNS	178	Standard query response 0x4473 AAAA api.hsselite.com SOA ns-1489.awsdns-58.org
170	4.005218	192.168.225.164	52.9.81.184	TCP	66	49442 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
171	4.022702	157.140.2.32	192.168.225.164	TCP	66	80 → 55549 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1370 SACK_PERM=1 WS=128
172	4.022702	157.140.2.32	192.168.225.164	TCP	66	80 → 60864 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1370 SACK_PERM=1 WS=128
173	4.022853	192.168.225.164	157.140.2.32	TCP	54	55549 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0

http

No.	Time	Source	Destination	Protocol	Length	Info
175	4.023419	192.168.225.164	157.140.2.32	HTTP	525	GET /css/main.css HTTP/1.1
176	4.023740	192.168.225.164	157.140.2.32	HTTP	533	GET /css/summary-stats.css HTTP/1.1
188	4.156080	192.168.225.164	157.140.2.32	HTTP	525	GET /css/page.css HTTP/1.1
193	4.246546	157.140.2.32	192.168.225.164	HTTP	769	HTTP/1.1 304 Not Modified
196	4.255367	157.140.2.32	192.168.225.164	HTTP	770	HTTP/1.1 304 Not Modified
210	4.287902	192.168.225.164	157.140.2.32	HTTP	585	GET /assets/logo/logo-explore.png HTTP/1.1
211	4.366477	157.140.2.32	192.168.225.164	HTTP	768	HTTP/1.1 304 Not Modified
214	4.390003	192.168.225.164	157.140.2.32	HTTP	588	GET /assets/sidebar/shrimp-202px.png HTTP/1.1
215	4.449185	192.168.225.164	157.140.2.32	HTTP	582	GET /assets/external-link-explore.png HTTP/1.1
219	4.500775	157.140.2.32	192.168.225.164	HTTP	719	HTTP/1.1 304 Not Modified
236	4.582266	157.140.2.32	192.168.225.164	HTTP	751	HTTP/1.1 304 Not Modified
238	4.662297	157.140.2.32	192.168.225.164	HTTP	728	HTTP/1.1 304 Not Modified
279	4.994000	192.168.225.164	157.140.2.32	HTTP	546	GET /assets/fonts/Ubuntu.woff HTTP/1.1
316	5.201993	157.140.2.32	192.168.225.164	HTTP	750	HTTP/1.1 304 Not Modified
349	5.385119	192.168.225.164	157.140.2.32	HTTP	584	GET /assets/sponsor-logos/ner.png HTTP/1.1
350	5.386370	192.168.225.164	157.140.2.32	HTTP	589	GET /assets/sponsor-logos/emonocot.png HTTP/1.1
351	5.386821	192.168.225.164	157.140.2.32	HTTP	589	GET /assets/sponsor-logos/vibrant.png HTTP/1.1
352	5.387201	192.168.225.164	157.140.2.32	HTTP	588	GET /assets/sponsor-logos/einfra.png HTTP/1.1
411	5.603125	157.140.2.32	192.168.225.164	HTTP	729	HTTP/1.1 304 Not Modified
413	5.603834	192.168.225.164	157.140.2.32	HTTP	585	GET /assets/sponsor-logos/nhm.png HTTP/1.1
414	5.604186	192.168.225.164	157.140.2.32	HTTP	582	GET /assets/external-link-develop.png HTTP/1.1
415	5.607095	157.140.2.32	192.168.225.164	HTTP	749	HTTP/1.1 304 Not Modified

```
Hypertext Transfer Protocol
GET /css/main.css HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /css/main.css HTTP/1.1\r\n]
     [GET /css/main.css HTTP/1.1\r\n]
     [Severity level: Chat]
     [Group: Sequence]
   Request Method: GET
   Request URI: /css/main.css
   Request Version: HTTP/1.1
Host: scratchpads.org\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36\r\n
Accept: text/css,*/*;q=0.1\r\n
Sec-GPC: 1\r\n
Referer: http://scratchpads.org/explore/sites-list\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-IN,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\r\n
If-None-Match: W/"60be06bf-2305"\r\n
If-Modified-Since: Mon, 07 Jun 2021 11:45:03 GMT\r\n
\r\n
[Full request URI: http://scratchpads.org/css/main.css]
[HTTP request 1/5]
[Response in frame: 196]
[Next request in frame: 210]
```

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP Requests by HTTP Host	16				0.0064	100%	0.0400	5.385
scratchpads.org	16				0.0064	100.00%	0.0400	5.385
/favicon.ico	1				0.0004	6.25%	0.0100	6.327
/css/summary-stats.css	1				0.0004	6.25%	0.0100	4.024
/css/page.css	1				0.0004	6.25%	0.0100	4.156
/css/main.css	1				0.0004	6.25%	0.0100	4.023
/assets/sponsor-logos/vibrant.png	1				0.0004	6.25%	0.0100	5.387
/assets/sponsor-logos/nhm.png	1				0.0004	6.25%	0.0100	5.604
/assets/sponsor-logos/ner.png	1				0.0004	6.25%	0.0100	5.385
/assets/sponsor-logos/emonocot.png	1				0.0004	6.25%	0.0100	5.386
/assets/sponsor-logos/einfra.png	1				0.0004	6.25%	0.0100	5.387
/assets/sidebar/shrimp-202px.png	1				0.0004	6.25%	0.0100	4.390
/assets/logo/logo-explore.png	1				0.0004	6.25%	0.0100	4.288
/assets/fonts/Ubuntu.woff	1				0.0004	6.25%	0.0100	4.994
/assets/fonts/Ubuntu-Medium.woff	1				0.0004	6.25%	0.0100	5.711
/assets/external-link-support.png	1				0.0004	6.25%	0.0100	5.608
/assets/external-link-explore.png	1				0.0004	6.25%	0.0100	4.449
/assets/external-link-develop.png	1				0.0004	6.25%	0.0100	5.604

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	32	100.0	20981	66k	0	0	0
Ethernet	100.0	32	2.1	448	1428	0	0	0
Internet Protocol Version 4	100.0	32	3.1	640	2040	0	0	0
Transmission Control Protocol	100.0	32	94.8	19893	63k	0	0	0
Hypertext Transfer Protocol	100.0	32	91.8	19253	61k	32	19253	61k

B – Open some URL (*in which you can post some comments*) in your browser and post a comment in it.

http

No.	Time	Source	Destination	Protocol	Length	Info
206	7.023509	192.168.1.100	119.36.33.85	HTTP	582	GET /index.html HTTP/1.1
269	7.332573	119.36.33.85	192.168.1.100	HTTP	1123	HTTP/1.1 200 OK (text/html)
1188	14.004175	192.168.1.100	119.36.33.85	HTTP	528	GET /images/zncm.jpg HTTP/1.1
1231	14.301452	119.36.33.85	192.168.1.100	HTTP	377	HTTP/1.1 304 Not Modified
1395	15.035729	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/76/1?_=1629893735054 HTTP/1.1
1398	15.036078	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/71/1?_=1629893735055 HTTP/1.1
1461	15.320077	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/62/1?_=1629893735056 HTTP/1.1
1464	15.320608	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/63/1?_=1629893735057 HTTP/1.1
1470	15.321568	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/64/1?_=1629893735058 HTTP/1.1
1472	15.323547	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/65/1?_=1629893735059 HTTP/1.1

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	86	100.0	48408	11k	0	0	0
Ethernet	100.0	86	2.5	1204	274	0	0	0
Internet Protocol Version 6	2.3	2	0.2	80	18	0	0	0
Transmission Control Protocol	2.3	2	1.5	734	167	0	0	0
Hypertext Transfer Protocol	2.3	2	1.4	694	158	1	155	35
Line-based text data	1.2	1	0.0	22	5	1	22	5
Internet Protocol Version 4	97.7	84	3.5	1680	383	0	0	0
Transmission Control Protocol	97.7	84	92.4	44710	10k	0	0	0
Hypertext Transfer Protocol	97.7	84	177.5	85921	19k	77	39235	8957
Line-based text data	4.7	4	414.9	200852	45k	4	40167	9170
JavaScript Object Notation	3.5	3	9.6	4643	1060	3	6002	1370

http

No.	Time	Source	Destination	Protocol	Length	Info
206	7.023509	192.168.1.100	119.36.33.85	HTTP	582	GET /index.html HTTP/1.1
269	7.332573	119.36.33.85	192.168.1.100	HTTP	1123	HTTP/1.1 200 OK (text/html)
1188	14.004175	192.168.1.100	119.36.33.85	HTTP	528	GET /images/zncm.jpg HTTP/1.1
1231	14.301452	119.36.33.85	192.168.1.100	HTTP	377	HTTP/1.1 304 Not Modified
1395	15.035729	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/76/1?_=1629893735054 HTTP/1.1

```
> Frame 206: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface \Device\NPF_{83E20D82-7C71-476A-9C13-1D72C91D36AE}, id 0
> Ethernet II, Src: IntelCor_8e:5f:f3 (0c:54:15:8e:5f:f3), Dst: Shenzhen_b2:0b:49 (fc:dd:55:b2:0b:49)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 119.36.33.85
> Transmission Control Protocol, Src Port: 64146, Dst Port: 80, Seq: 1, Ack: 1, Len: 528
v Hypertext Transfer Protocol
  v GET /index.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /index.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /index.html
      Request Version: HTTP/1.1
    Host: www.rednet.cn\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/92.0.4515.159 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Sec-GPC: 1\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-IN,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    If-Modified-Since: Wed, 25 Aug 2021 06:30:00 GMT\r\n
    \r\n
    [Full request URI: http://www.rednet.cn/index.html]
    [HTTP request 1/2]
    [Response in frame: 269]
    [Next request in frame: 1188]
```

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	7501	100.0	3921318	635k	0	0	0
Ethernet	100.0	7501	2.7	105014	17k	0	0	0
Internet Protocol Version 6	67.7	5078	5.2	203120	32k	0	0	0
User Datagram Protocol	8.4	632	0.1	5056	818	0	0	0
QUIC IETF	0.1	5	0.2	6650	1076	5	6650	1076
Multicast Domain Name System	1.0	75	0.1	2448	396	75	2448	396
Link-local Multicast Name Resolution	1.0	74	0.0	1786	289	74	1786	289
Domain Name System	6.3	476	1.0	40779	6603	476	40779	6603
DHCPv6	0.0	2	0.0	142	22	2	142	22
Transmission Control Protocol	58.6	4398	76.4	2995112	485k	3320	2107580	341k
Transport Layer Security	13.6	1021	48.4	1898271	307k	997	1727127	279k
Malformed Packet	0.8	63	0.0	0	0	63	0	0
Hypertext Transfer Protocol	0.0	2	0.0	694	112	1	155	25
Line-based text data	0.0	1	0.0	22	3	1	22	3
Domain Name System	0.1	4	0.0	1143	185	4	1143	185
Data	0.2	12	0.3	13337	2159	12	13337	2159
Internet Control Message Protocol v6	0.6	43	0.0	1676	271	43	1676	271
Data	0.1	5	0.2	6520	1055	5	6520	1055
Internet Protocol Version 4	32.2	2413	1.2	48292	7820	0	0	0
User Datagram Protocol	7.7	575	0.1	4600	744	0	0	0
NetBIOS Name Service	0.7	54	0.1	2700	437	54	2700	437
Multicast Domain Name System	1.0	75	0.1	2448	396	75	2448	396
Link-local Multicast Name Resolution	1.0	74	0.0	1786	289	74	1786	289
Dynamic Host Configuration Protocol	0.0	2	0.0	850	137	2	850	137
Domain Name System	4.9	370	0.8	31809	5151	370	31809	5151
Transmission Control Protocol	24.4	1830	11.9	466456	75k	1369	299097	48k
Transport Layer Security	5.2	390	6.3	245368	39k	369	206395	33k
Malformed Packet	0.1	8	0.0	0	0	8	0	0
Hypertext Transfer Protocol	1.1	84	2.2	85921	13k	77	39235	6353
Line-based text data	0.1	4	5.1	200852	32k	4	40167	6504
JavaScript Object Notation	0.0	3	0.1	4643	751	3	6002	971
Internet Group Management Protocol	0.1	8	0.0	152	24	8	152	24
Address Resolution Protocol	0.1	10	0.0	298	48	10	298	48

3. Explain the working of the HTTP protocol [HTTP GET and POST message] briefly with typed answers and answer highlighted screenshots for the above activity from Wireshark.

- HTTP stands for Hypertext Transfer Protocol, and HTTP is the communication protocol used for browsing the web.
- This protocol uses a message-based model where your client makes an HTTP request to a web server and that server responds with a resource which is displayed in the browser.
- In this relationship a web browser may be thought of as the client, whereas the application running which hosts the website would be the server where every HTTP interaction includes a request and a response.

- By its nature, HTTP is stateless. Stateless means that all requests are separate from each other so every request must contain enough information on their own to fulfil the request and so that each transaction of message-based model of HTTP is processed separately from each other.
- In HTTP, every request must have an URL address and additionally, request needs a method.
- All HTTP messages have one or more headers, followed by a optional message body.
- The body contains the data that will be sent with the request or the data received with the response. First part of every HTTP request holds three items:

Example: GET /adds/search-result?item=vw+beetle HTTP/1.1

- When a URL contains a "?" sign means it contains a query which sends parameters of the requested resource.

1. First part is a method which tells which HTTP method is used. Most commonly used is the GET method. GET method retrieves a resource from the web server and since GET doesn't have a message body nothing after the header is needed.
2. Second part is a requested URL.
3. Third part is a HTTP version being used. Version 1.1. is the most common version for most browsers, however, version 2.0 is taking over.

- There are also some other interesting things in a HTTP request:
- Referer header — tell the URL from which the request has originated.
- User-Agent header — additional information about the browser being used to generate the request.
- Host header — uniquely identify a host name, it is necessary when multiple web pages are hosted on the same server.
- Cookie header — submit additional parameters to the client.

HTTP Responses

- Just like in HTTP requests HTTP responses also consist of three items:

Example: HTTP/1.1 200 OK

1. First part is the HTTP version being used.
2. Second part is the numeric code of the result for the request.
3. Third part is a textual description of the second part.

- There are some other interesting things in a HTTP response:
- Server header — information which web server software is being used.
- Set-Cookie header — issues the cookie to the browser.

- Message body — it is common for a HTTP response to hold a message body.

- Content-Length header — tells the size of the message body in bytes.

HTTP Methods

- Most common methods are GET and POST, however there are more of them.

- GET — used to request data from a specified resource where data is not modified it in any way as GET requests do not change the state of resource.

- POST — used to send data to a server to create a resource.

A - Analyze the sender and destination IP address, Port address and Physical address (Proxy Server)

```
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 119.36.33.85
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 568
   Identification: 0x4620 (17952)
 > Flags: 0x40, Don't fragment
   Fragment Offset: 0
   Time to Live: 128
   Protocol: TCP (6)
   Header Checksum: 0x581a [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 192.168.1.100
   Destination Address: 119.36.33.85
```

- Sender IP Address : 192.168.1.100
- Destination IP Address : 119.36.33.85

```
Transmission Control Protocol, Src Port: 64146, Dst Port: 80, Seq: 1, Ack: 1, Len: 528
   Source Port: 64146
   Destination Port: 80
   [Stream index: 10]
   [TCP Segment Len: 528]
```

- Sender Port Address : 64146
- Destination Port Address : 80

```
Ethernet II, Src: IntelCor_8e:5f:f3 (0c:54:15:8e:5f:f3), Dst: Shenzhen_b2:0b:49 (fc:dd:55:b2:0b:49)
> Destination: Shenzhen_b2:0b:49 (fc:dd:55:b2:0b:49)
> Source: IntelCor_8e:5f:f3 (0c:54:15:8e:5f:f3)
   Type: IPv4 (0x0800)
```

- Sender MAC Address (Physical Address) : 0c:54:15:8e:5f:f3
- Destination MAC Address (Physical Address) : fc:dd:55:b2:0b:49

B – Analyze the Host machine and webpage name in the file server

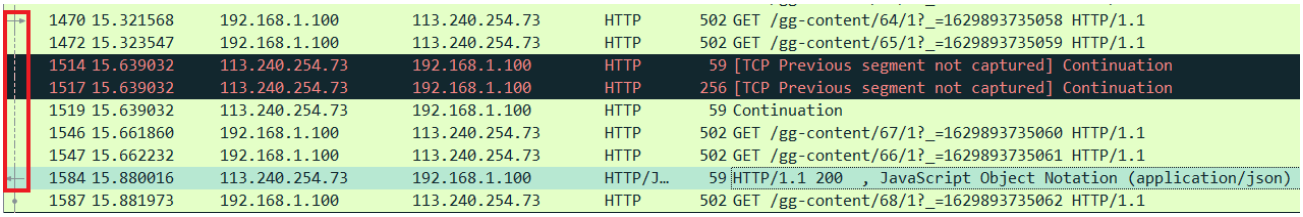
```
Host: news-search.rednet.cn\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Sec-GPC: 1\r\n
Referer: http://www.rednet.cn/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-IN,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\r\n
\r\n
[Full request URI: http://news-search.rednet.cn/search?q=networks]
[HTTP request 1/2]
[Response in frame: 2884]
[Next request in frame: 2886]
```

- Host Name : news-search.rednet.cn
- Webpage Name : http://www.rednet.cn/

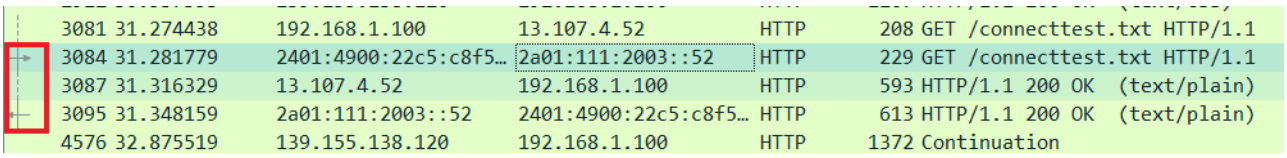
C – Check the acknowledgement frame for successful request and the unsuccessful request

http

No.	Time	Source	Destination	Protocol	Length	Information
206	7.023509	192.168.1.100	119.36.33.85	HTTP	582	GET /index.html HTTP/1.1
269	7.332573	119.36.33.85	192.168.1.100	HTTP	1123	HTTP/1.1 200 OK (text/html)
1188	14.004175	192.168.1.100	119.36.33.85	HTTP	528	GET /images/zncm.jpg HTTP/1.1

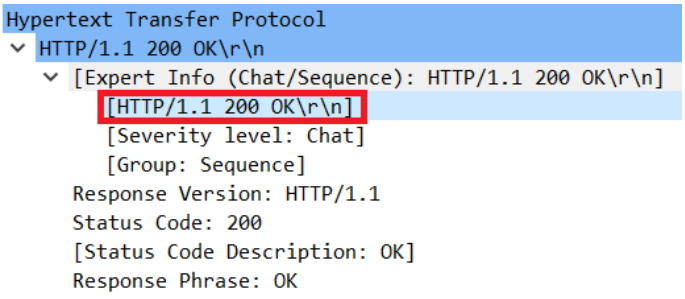


1470	15.321568	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/64/1?_=1629893735058 HTTP/1.1
1472	15.323547	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/65/1?_=1629893735059 HTTP/1.1
1514	15.639032	113.240.254.73	192.168.1.100	HTTP	59	[TCP Previous segment not captured] Continuation
1517	15.639032	113.240.254.73	192.168.1.100	HTTP	256	[TCP Previous segment not captured] Continuation
1519	15.639032	113.240.254.73	192.168.1.100	HTTP	59	Continuation
1546	15.661860	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/67/1?_=1629893735060 HTTP/1.1
1547	15.662232	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/66/1?_=1629893735061 HTTP/1.1
1584	15.880016	113.240.254.73	192.168.1.100	HTTP/J…	59	HTTP/1.1 200 , JavaScript Object Notation (application/json)
1587	15.881973	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/68/1?_=1629893735062 HTTP/1.1



3081	31.274438	192.168.1.100	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
3084	31.281779	2401:4900:22c5:c8f5…	2a01:111:2003::52	HTTP	229	GET /connecttest.txt HTTP/1.1
3087	31.316329	13.107.4.52	192.168.1.100	HTTP	593	HTTP/1.1 200 OK (text/plain)
3095	31.348159	2a01:111:2003::52	2401:4900:22c5:c8f5…	HTTP	613	HTTP/1.1 200 OK (text/plain)
4576	32.875519	139.155.138.120	192.168.1.100	HTTP	1372	Continuation

```
Hypertext Transfer Protocol
  GET /index.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /index.html HTTP/1.1\r\n]
      [GET /index.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /index.html
    Request Version: HTTP/1.1
  Host: www.rednet.cn\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/92.0.4515.159 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Sec-GPC: 1\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-IN,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  If-Modified-Since: Wed, 25 Aug 2021 06:30:00 GMT\r\n
  \r\n
  [Full request URI: http://www.rednet.cn/index.html]
  [HTTP request 1/2]
  [Response in frame: 269]
  [Next request in frame: 1188]
```



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
```

D – Analyze how the uploaded data has reached the server

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.100	64146	119.36.33.85	80	4	2610	2	1110	2	1500	7.023509	7.2779	1220	
192.168.1.100	50384	113.240.254.73	80	8	3430	3	1506	5	1924	15.035729	7.2342	1665	
192.168.1.100	56271	113.240.254.73	80	16	5936	5	2510	11	3426	15.036078	27.0266	742	
192.168.1.100	51399	113.240.254.73	80	7	2289	3	1506	4	783	15.320077	11.2600	1069	
192.168.1.100	58279	113.240.254.73	80	3	1250	1	502	2	748	15.320608	0.8414	4772	
192.168.1.100	51670	113.240.254.73	80	10	3162	5	2509	5	653	15.321568	3.5676	5626	
192.168.1.100	61301	113.240.254.73	80	12	3554	5	2510	7	1044	15.323547	3.9475	5086	
192.168.1.100	62372	139.155.138.120	80	18	21k	2	1055	16	20k	29.280909	8.4375	1000	
192.168.1.100	64214	139.155.138.120	80	2	1559	1	452	1	1107	30.057627	0.4797	7537	
192.168.1.100	49539	13.107.4.52	80	2	801	1	208	1	593	31.274438	0.0419	39k	
192.168.1.100	61488	139.155.138.120	80	2	1209	1	497	1	712	39.303682	1.8593	2138	
2401:4900:22c5:c8f5:acff:bb4c:6931:7d5c	49540	2a01:111:2003::52	80	2	842	1	229	1	613	31.281779	0.0664	27k	

Time

First packet:	2021-08-25 17:45:21
Last packet:	2021-08-25 17:46:10
Elapsed:	00:00:49

Capture

Hardware:	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz (with SSE4.2)
OS:	64-bit Windows 10 (2009), build 19042
Application:	Dumpcap (Wireshark) 3.4.7 (v3.4.7-0-ge42cbf6a415f)

Interfaces

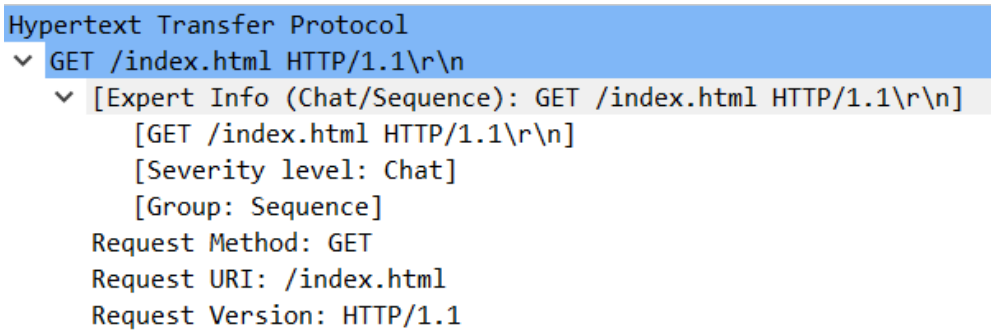
Interface	Dropped packets	Capture filter	Link type	Packet size limit
Wi-Fi	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	7501	7501 (100.0%)	—
Time span, s	49.402	49.402	—
Average pps	151.8	151.8	—
Average packet size, B	523	523	—
Bytes	3921318	3921318 (100.0%)	0
Average bytes/s	79k	79k	—
Average bits/s	635k	635k	—

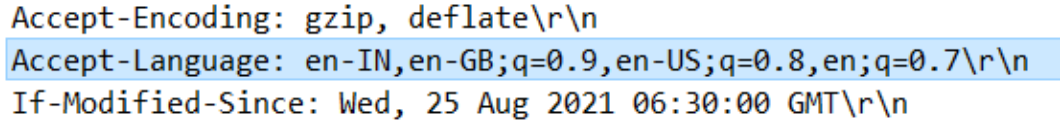
Find the following from frames received for the above activity

Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?



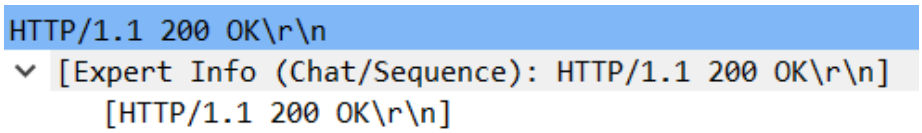
- Version : HTTP 1.1

What languages (if any) does your browser indicate that it can accept to the server?



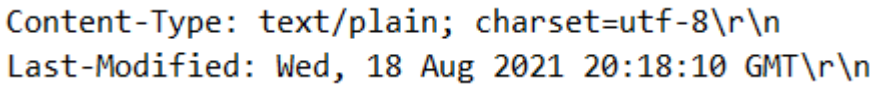
- Accept Language = en-IN

What is the status code returned from the server to your browser?



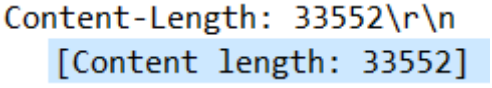
- Status Code = 200 OK

When the HTML file that you are retrieving was last modified at the server?



- Last Modified : Wed, 18 Aug 2021 20:18:10 GMT

How many bytes of content are being returned to your browser?



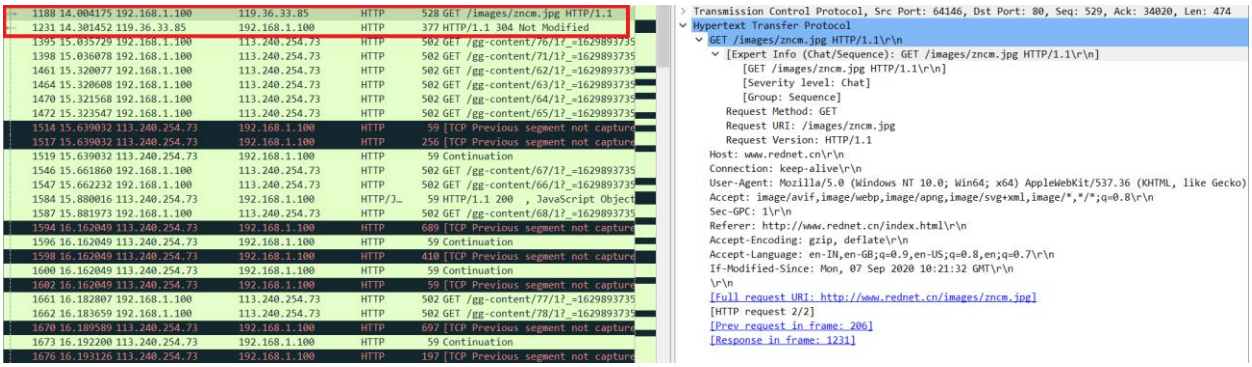
- Content Length = 33552 Bytes

By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

- No, I don't see any headers within the data that are not displayed in the packet-listing window

Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

206	7.023509	192.168.1.100	119.36.33.85	HTTP	582	GET /index.html HTTP/1.1
269	7.332573	119.36.33.85	192.168.1.100	HTTP	1123	HTTP/1.1 200 OK (text/html)
1188	14.004175	192.168.1.100	119.36.33.85	HTTP	528	GET /images/zncm.jpg HTTP/1.1
1231	14.301452	119.36.33.85	192.168.1.100	HTTP	377	HTTP/1.1 304 Not Modified



- The webpage I visited has only 1 image.

What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

- HTTP/1.1 200 OK

4. Open AUMS and download a file. Stop capture. Using statistics tools find the time taken for downloading the file.

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.100	62373	103.10.24.185	443	20	5320	11	3691	9	1629	15.610337	2.0325	14k	6411
192.168.1.100	63158	162.159.134.234	443	39	5154	19	1080	20	4074	0.000000	37.4932	230	869
192.168.1.100	63317	44.240.44.48	443	42	20k	22	13k	20	7390	6.922017	27.0194	3909	2188
192.168.1.100	63462	103.10.24.185	443	598	607k	156	10k	442	597k	25.762438	2.0784	38k	2298k
192.168.1.100	63500	34.201.142.47	443	17	7280	8	1087	9	6193	21.769581	0.8731	9959	56k
192.168.1.100	63589	103.10.24.185	443	55	37k	21	5808	34	32k	20.793985	3.3777	13k	75k
2401:4900:22c5:c8f5:400:53b7:39b6:3e0a	63799	2404:6800:4007:810::2003	443	14	6588	7	1111	7	5477	6.333898	0.2877	30k	152k
2401:4900:22c5:c8f5:400:53b7:39b6:3e0a	64328	2600:9000:2075:e00:15:85fe:56c0:93a1	443	29	15k	11	1877	18	13k	2.654435	0.5493	27k	200k
192.168.1.100	64536	184.169.221.190	443	37	10k	19	2574	18	7855	5.373260	1.1452	17k	54k
192.168.1.100	65224	103.10.24.185	443	18	4640	10	1931	8	2709	21.015910	3.1357	4926	6911

- Time taken for Download = 27.0194
- Time Taken for the entire session = 37.4932

5. Open your SharePoint page (URL in Q2) and download a video file.

- Find the number of routing endpoints visited and the switches visited.
- Find the packet length transmitted and received, give the protocol hierarchy and the Flow graph

Endpoints and Switches:

- Ethernet Endpoints = 15
- IPv4 Endpoints = 23
- IPv6 Endpoints = 25
- TCP Endpoints = 64
- UDP Endpoints = 144

Packet length transmitted and received :

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	29675	1022.15	42	1372	0.5983	100%	2.7000	40.257
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	6829	58.61	42	79	0.1377	23.01%	1.1000	21.771
80-159	771	96.42	80	157	0.0155	2.60%	1.0200	10.595
160-319	158	216.59	161	318	0.0032	0.53%	0.1100	26.787
320-639	187	460.47	323	634	0.0038	0.63%	0.1300	20.829
640-1279	147	895.61	640	1260	0.0030	0.50%	0.1600	6.609
1280-2559	21583	1371.72	1285	1372	0.4352	72.73%	2.2000	22.800
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Protocol hierarchy :

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	29675	100.0	30332359	4892k	0	0	0
Ethernet	100.0	29675	1.4	415450	67k	0	0	0
Internet Protocol Version 6	13.8	4100	0.5	164000	26k	0	0	0
User Datagram Protocol	0.8	235	0.0	1880	303	0	0	0
Multicast Domain Name System	0.3	78	0.0	2660	429	78	2660	429
Link-local Multicast Name Resolution	0.3	75	0.0	1841	296	75	1841	296
Domain Name System	0.3	80	0.0	9919	1599	80	9919	1599
DHCPv6	0.0	2	0.0	142	22	2	142	22
Transmission Control Protocol	12.9	3828	10.8	3290182	530k	2914	2316223	373k
Transport Layer Security	3.1	913	10.5	3185977	513k	901	3116012	502k
Hypertext Transfer Protocol	0.0	2	0.0	694	111	1	155	25
Line-based text data	0.0	1	0.0	22	3	1	22	3
Data	0.0	11	0.0	12029	1940	11	12029	1940
Internet Control Message Protocol v6	0.1	37	0.0	1500	241	37	1500	241
Internet Protocol Version 4	86.1	25563	1.7	511304	82k	0	0	0
User Datagram Protocol	0.8	228	0.0	1824	294	0	0	0
NetBIOS Name Service	0.2	54	0.0	2700	435	54	2700	435
Multicast Domain Name System	0.3	78	0.0	2660	429	78	2660	429
Link-local Multicast Name Resolution	0.3	75	0.0	1841	296	75	1841	296
Dynamic Host Configuration Protocol	0.0	3	0.0	1152	185	3	1152	185
Domain Name System	0.1	18	0.0	1706	275	18	1706	275
Transmission Control Protocol	85.3	25324	85.5	25920930	4181k	15383	13065658	2107k
Transport Layer Security	33.9	10061	82.9	25148672	4056k	9766	17244084	2781k
Malformed Packet	0.0	1	0.0	0	0	1	0	0
Hypertext Transfer Protocol	0.0	2	0.0	693	111	1	154	24
Line-based text data	0.0	1	0.0	22	3	1	22	3
Data	0.6	172	0.7	225081	36k	172	225081	36k
Internet Group Management Protocol	0.0	11	0.0	208	33	11	208	33
Address Resolution Protocol	0.0	12	0.0	372	60	12	372	60

Flow Graph :

6. Capture the frames for the following commands in the command prompt printf "GET /HTTP/1.0\r\n" | nc ac.amrita.ac.in 80. Start up your web browser, and make sure your browser's cache is cleared. Do this activity and capture frames

```
/mnt/c/Users/abhis/Downloads printf "GET /HTTP/1.0\r\n" | nc ac.amrita.ac.in 80
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://ac.amrita.ac.in/HTTP/1.0">here</a>.</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at ac.amrita.ac.in Port 80</address>
</body></html>
```

1	0.000000	2600:1417:78::6856:…	2401:4900:22c5:c8f5…	TCP	86	80 → 52433 [SYN, ACK] Seq=0 Ack=1 Win=28800 Len=0 MSS=1298 SACK_PERM=1 WS=128
2	0.000060	2401:4900:22c5:c8f5…	2600:1417:78::6856:…	TCP	74	52433 → 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
3	0.000184	2401:4900:22c5:c8f5…	2600:1417:78::6856:…	HTTP	361	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?baad6b8a979a41eb HTTP/1.1
4	0.044577	2600:1417:78::6856:…	2401:4900:22c5:c8f5…	TCP	74	80 → 52433 [ACK] Seq=1 Ack=288 Win=29952 Len=0
5	0.049024	2600:1417:78::6856:…	2401:4900:22c5:c8f5…	HTTP	341	HTTP/1.1 304 Not Modified
6	0.107666	2401:4900:22c5:c8f5…	2600:1417:78::6856:…	TCP	74	52433 → 80 [ACK] Seq=288 Ack=268 Win=511 Len=0
7	0.600771	fe80::8c9b:82ff:fec…	ff02::1	ICMPv6	118	Router Advertisement from fc:dd:55:b2:0b:49
8	2.393796	192.168.1.100	192.168.1.1	DNS	75	Standard query 0xb271 A ac.amrita.ac.in
9	2.399166	192.168.1.100	192.168.1.1	DNS	75	Standard query 0xf3a8 AAAA ac.amrita.ac.in
10	2.532320	192.168.1.1	192.168.1.100	DNS	110	Standard query response 0xb271 A ac.amrita.ac.in CNAME web2.amrita.ac.in A 103.10.24.241
11	2.544080	192.168.1.1	192.168.1.100	DNS	135	Standard query response 0xf3a8 AAAA ac.amrita.ac.in CNAME web2.amrita.ac.in SOA amrita.ac.in
12	2.544590	192.168.1.100	103.10.24.241	TCP	66	52434 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	2.601071	103.10.24.241	192.168.1.100	TCP	66	80 → 52434 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1318 SACK_PERM=1 WS=128
14	2.601136	192.168.1.100	103.10.24.241	TCP	54	52434 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
15	2.601366	192.168.1.100	103.10.24.241	TCP	69	52434 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=15 [TCP segment of a reassembled PDU]
16	2.658903	103.10.24.241	192.168.1.100	TCP	54	80 → 52434 [ACK] Seq=1 Ack=16 Win=14720 Len=0
17	2.662105	103.10.24.241	192.168.1.100	TCP	375	80 → 52434 [PSH, ACK] Seq=1 Ack=16 Win=14720 Len=321
18	2.662105	103.10.24.241	192.168.1.100	TCP	54	80 → 52434 [FIN, ACK] Seq=322 Ack=16 Win=14720 Len=0
19	2.662206	192.168.1.100	103.10.24.241	TCP	54	52434 → 80 [ACK] Seq=16 Ack=323 Win=131328 Len=0
20	2.664949	192.168.1.100	103.10.24.241	TCP	54	52434 → 80 [FIN, ACK] Seq=16 Ack=323 Win=131328 Len=0
21	2.720951	103.10.24.241	192.168.1.100	TCP	54	80 → 52434 [ACK] Seq=323 Ack=17 Win=14720 Len=0
22	5.016234	192.168.1.100	162.159.134.234	TLSv1.2	108	Application Data
23	5.068640	162.159.134.234	192.168.1.100	TCP	54	443 → 60827 [ACK] Seq=1 Ack=55 Win=81 Len=0
24	5.363305	162.159.134.234	192.168.1.100	TLSv1.2	87	Application Data
25	5.417117	192.168.1.100	162.159.134.234	TCP	54	60827 → 443 [ACK] Seq=55 Ack=34 Win=513 Len=0
26	7.980459	fe80::8c9b:82ff:fec…	ff02::1	ICMPv6	118	Router Advertisement from fc:dd:55:b2:0b:49
27	8.540427	162.159.134.234	192.168.1.100	TLSv1.2	107	Application Data
28	8.589305	192.168.1.100	162.159.134.234	TCP	54	60827 → 443 [ACK] Seq=55 Ack=87 Win=513 Len=0
29	8.878127	162.159.134.234	192.168.1.100	TLSv1.2	416	Application Data
30	8.921302	192.168.1.100	162.159.134.234	TCP	54	60827 → 443 [ACK] Seq=55 Ack=449 Win=512 Len=0
31	9.216481	192.168.1.100	192.168.1.255	BROWSER	248	Host Announcement A3X3K, Workstation, Server, NT Workstation

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	31	100.0	3723	3231	0	0	0
Ethernet	100.0	31	11.7	434	376	0	0	0
Internet Protocol Version 6	25.8	8	8.6	320	277	0	0	0
Transmission Control Protocol	19.4	6	18.4	686	595	4	92	79
Hypertext Transfer Protocol	6.5	2	14.9	554	480	2	554	480
Internet Control Message Protocol v6	6.5	2	3.4	128	111	2	128	111
Internet Protocol Version 4	74.2	23	12.4	460	399	0	0	0
User Datagram Protocol	16.1	5	1.1	40	34	0	0	0
NetBIOS Datagram Service	3.2	1	5.5	206	178	0	0	0
SMB (Server Message Block Protocol)	3.2	1	3.3	124	107	0	0	0
SMB MailSlot Protocol	3.2	1	0.7	25	21	0	0	0
Microsoft Windows Browser Protocol	3.2	1	1.0	38	32	1	38	32
Domain Name System	12.9	4	6.1	227	197	4	227	197
Transmission Control Protocol	58.1	18	32.8	1222	1060	14	640	555
Transport Layer Security	12.9	4	13.5	502	435	4	502	435

7. Start up your web browser, and make sure your browser's cache is cleared.

   Do this activity and capture frames

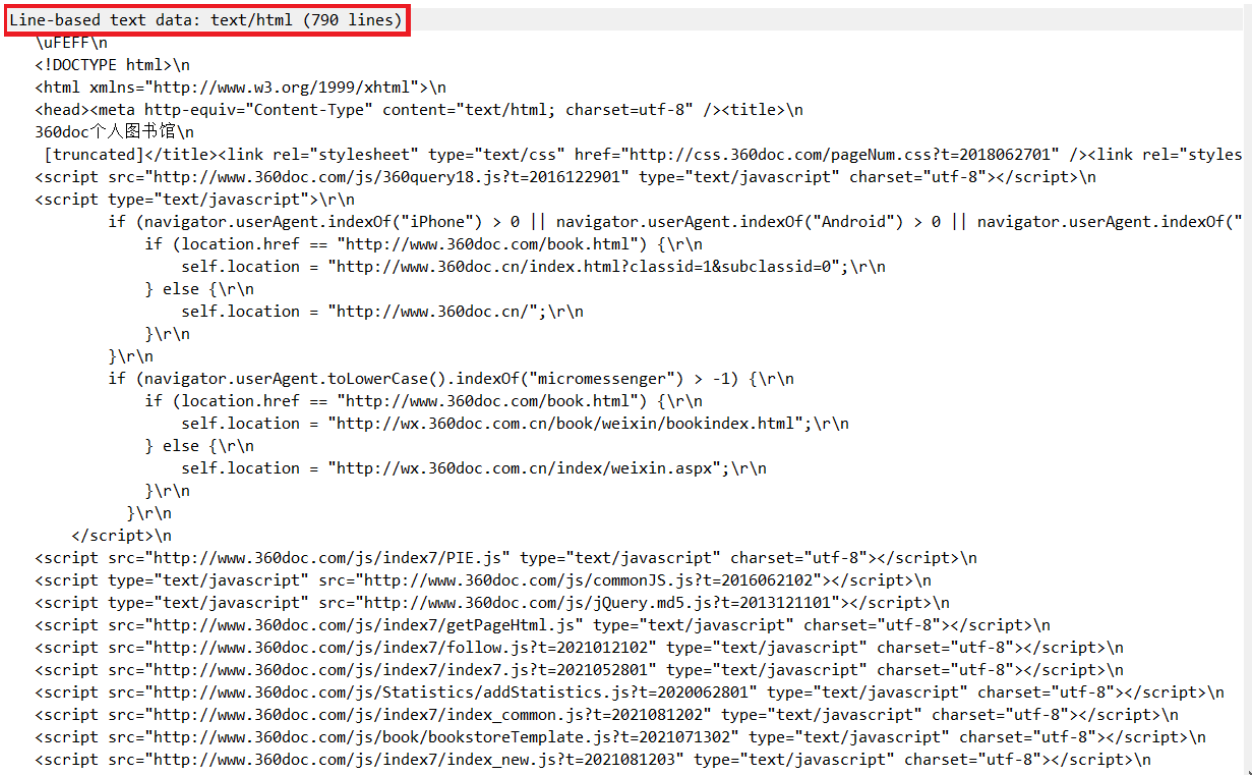
http

No.	Time	Source	Destination	Protocol	Length	Information
206	7.023509	192.168.1.100	119.36.33.85	HTTP	582	GET /index.html HTTP/1.1
269	7.332573	119.36.33.85	192.168.1.100	HTTP	1123	HTTP/1.1 200 OK (text/html)
1188	14.004175	192.168.1.100	119.36.33.85	HTTP	528	GET /images/zncm.jpg HTTP/1.1
1231	14.301452	119.36.33.85	192.168.1.100	HTTP	377	HTTP/1.1 304 Not Modified
1395	15.035729	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/76/1?_=1629893735054 HTTP/1.1
1398	15.036078	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/71/1?_=1629893735055 HTTP/1.1
1461	15.320077	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/62/1?_=1629893735056 HTTP/1.1
1464	15.320608	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/63/1?_=1629893735057 HTTP/1.1
1470	15.321568	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/64/1?_=1629893735058 HTTP/1.1
1472	15.323547	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/65/1?_=1629893735059 HTTP/1.1
1514	15.639032	113.240.254.73	192.168.1.100	HTTP	59	[TCP Previous segment not captured] Continuation
1517	15.639032	113.240.254.73	192.168.1.100	HTTP	256	[TCP Previous segment not captured] Continuation
1519	15.639032	113.240.254.73	192.168.1.100	HTTP	59	Continuation
1546	15.661860	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/67/1?_=1629893735060 HTTP/1.1
1547	15.662232	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/66/1?_=1629893735061 HTTP/1.1
1584	15.880016	113.240.254.73	192.168.1.100	HTTP/J…	59	HTTP/1.1 200 , JavaScript Object Notation (application/json)
1587	15.881973	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/68/1?_=1629893735062 HTTP/1.1
1594	16.162049	113.240.254.73	192.168.1.100	HTTP	689	[TCP Previous segment not captured] Continuation
1596	16.162049	113.240.254.73	192.168.1.100	HTTP	59	Continuation
1598	16.162049	113.240.254.73	192.168.1.100	HTTP	410	[TCP Previous segment not captured] Continuation
1600	16.162049	113.240.254.73	192.168.1.100	HTTP	59	Continuation
1602	16.162049	113.240.254.73	192.168.1.100	HTTP	59	[TCP Previous segment not captured] Continuation
1661	16.182807	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/77/1?_=1629893735063 HTTP/1.1
1662	16.183659	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/78/1?_=1629893735064 HTTP/1.1
1670	16.189589	113.240.254.73	192.168.1.100	HTTP	697	[TCP Previous segment not captured] Continuation
1673	16.192200	113.240.254.73	192.168.1.100	HTTP	59	Continuation
1676	16.193126	113.240.254.73	192.168.1.100	HTTP	197	[TCP Previous segment not captured] Continuation
1686	16.195377	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/73/1?_=1629893735065 HTTP/1.1
1687	16.204828	113.240.254.73	192.168.1.100	HTTP	1372	Continuation
1688	16.204828	113.240.254.73	192.168.1.100	HTTP	560	[TCP Previous segment not captured] Continuation
1689	16.204828	113.240.254.73	192.168.1.100	HTTP	59	Continuation
1697	16.212291	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/74/1?_=1629893735066 HTTP/1.1
1733	16.559585	113.240.254.73	192.168.1.100	HTTP/J…	59	HTTP/1.1 200 , JavaScript Object Notation (application/json)
1769	16.570130	192.168.1.100	113.240.254.73	HTTP	502	GET /gg-content/72/1?_=1629893735067 HTTP/1.1
1784	16.670268	113.240.254.73	192.168.1.100	HTTP	397	[TCP Previous segment not captured] Continuation
1786	16.670800	113.240.254.73	192.168.1.100	HTTP	59	Continuation
1790	16.982068	113.240.254.73	192.168.1.100	HTTP	1050	[TCP Previous segment not captured] Continuation
1791	16.982068	113.240.254.73	192.168.1.100	HTTP	394	[TCP Previous segment not captured] Continuation
1793	16.982068	113.240.254.73	192.168.1.100	HTTP	59	Continuation

```
   Request Method: GET
   Request URI: /index.html
   Request Version: HTTP/1.1
Host: www.360doc.com\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/92.0.4515.159 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Sec-GPC: 1\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-IN,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\r\n
Cookie: 360docsn=UEM3RQ38LR1O6CQU; 360doc3=iEAitnNcrtbr4AOHKkPhE1X7jYGbTLOLQ2b1UGGZ0SUZuBQ3wU2rWSLkteU/Q80f\r\n
\r\n
[Full request URI: http://www.360doc.com/index.html]
[HTTP request 1/7]
[Response in frame: 945]
[Next request in frame: 1461]
```

- No, I don't see an "IF-MODIFIED-SINCE" line in the first HTTP GET request.

Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?



```
Line-based text data: text/html (790 lines)
    \uFEFF\n
    <!DOCTYPE html>\n
    <html xmlns="http://www.w3.org/1999/xhtml">\n
    <head><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><title>\n
    360doc个人图书馆\n
     [truncated]</title><link rel="stylesheet" type="text/css" href="http://css.360doc.com/pageNum.css?t=2018062701" /><link rel="styles
    <script src="http://www.360doc.com/js/360query18.js?t=2016122901" type="text/javascript" charset="utf-8"></script>\n
    <script type="text/javascript">\r\n
            if (navigator.userAgent.indexOf("iPhone") > 0 || navigator.userAgent.indexOf("Android") > 0 || navigator.userAgent.indexOf("
                if (location.href == "http://www.360doc.com/book.html") {\r\n
                    self.location = "http://www.360doc.cn/index.html?classid=1&subclassid=0";\r\n
                } else {\r\n
                    self.location = "http://www.360doc.cn/";\r\n
                }\r\n
            }\r\n
            if (navigator.userAgent.toLowerCase().indexOf("micromessenger") > -1) {\r\n
                if (location.href == "http://www.360doc.com/book.html") {\r\n
                    self.location = "http://wx.360doc.com.cn/book/weixin/bookindex.html";\r\n
                } else {\r\n
                    self.location = "http://wx.360doc.com.cn/index/weixin.aspx";\r\n
                }\r\n
              }\r\n
        </script>\n
    <script src="http://www.360doc.com/js/index7/PIE.js" type="text/javascript" charset="utf-8"></script>\n
    <script type="text/javascript" src="http://www.360doc.com/js/commonJS.js?t=2016062102"></script>\n
    <script type="text/javascript" src="http://www.360doc.com/js/jQuery.md5.js?t=2013121101"></script>\n
    <script src="http://www.360doc.com/js/index7/getPageHtml.js" type="text/javascript" charset="utf-8"></script>\n
    <script src="http://www.360doc.com/js/index7/follow.js?t=2021012102" type="text/javascript" charset="utf-8"></script>\n
    <script src="http://www.360doc.com/js/index7/index7.js?t=2021052801" type="text/javascript" charset="utf-8"></script>\n
    <script src="http://www.360doc.com/js/Statistics/addStatistics.js?t=2020062801" type="text/javascript" charset="utf-8"></script>\n
    <script src="http://www.360doc.com/js/index7/index_common.js?t=2021081202" type="text/javascript" charset="utf-8"></script>\n
    <script src="http://www.360doc.com/js/book/bookstoreTemplate.js?t=2021071302" type="text/javascript" charset="utf-8"></script>\n
    <script src="http://www.360doc.com/js/index7/index_new.js?t=2021081203" type="text/javascript" charset="utf-8"></script>\n
```

- Yes, the server explicitly returned the contents of the file because there is a Line-based text data field in the server response frame.
- This section shows the content of the server which showed up in the browser.

Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?

```
    Request Method: GET
    Request URI: /index.html
    Request Version: HTTP/1.1
Host: www.360doc.com\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/92.0.4515.159 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
Sec-GPC: 1\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-IN,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\r\n
Cookie: 360docsn=UEM3RQ38LR1O6CQU; 360doc3=iEAitnNcrtbr4AOHKkPhE1X7jYGbTLOLQ2b1UGGZ0SUZuBQ3wU2rWSLkteU/Q80f\r\n
If-None-Match: W/"89ae7db7c8fd71:0"\r\n
If-Modified-Since: Thu, 12 Aug 2021 13:20:45 GMT\r\n
\r\n
[Full request URI: http://www.360doc.com/index.html]
[HTTP request 5/7]
[Prev request in frame: 3972]
[Response in frame: 4918]
[Next request in frame: 4946]
```

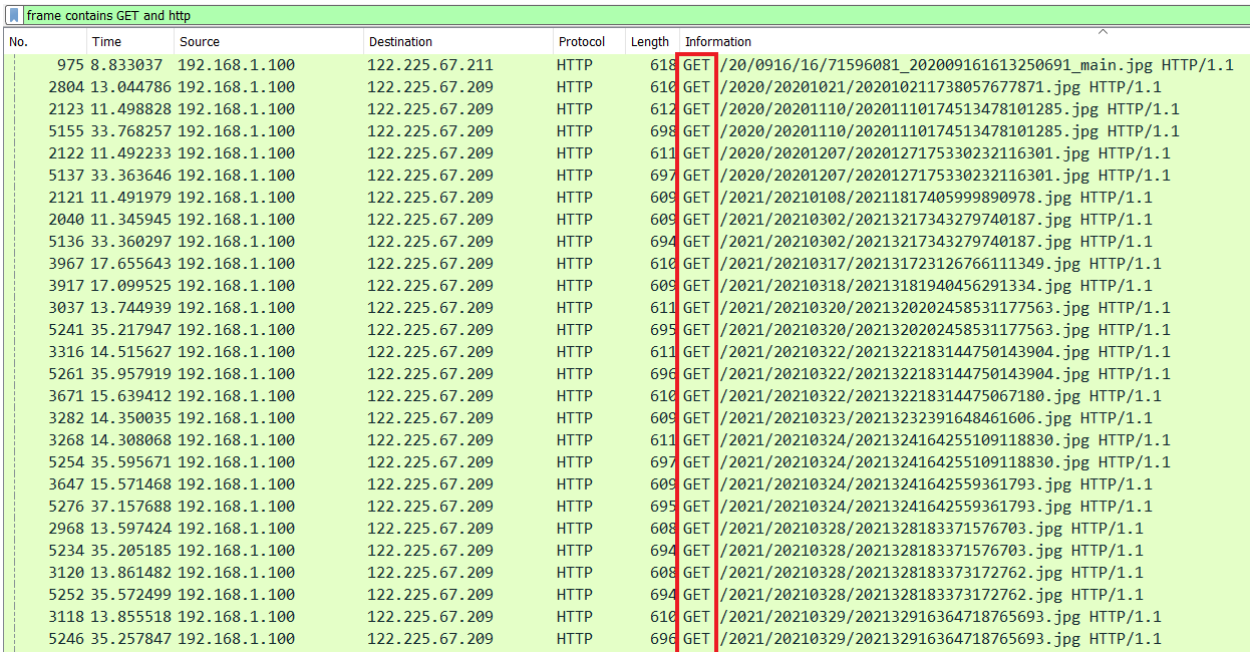
- The information that follows the "IF-MODIFIED-SINCE:" header is the **date and time** the webpage was accessed at last.

What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

```
HTTP/1.1 304 Not Modified\r\n
  [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
Server: Tengine\r\n
Content-Type: text/html; charset=utf-8\r\n
Connection: keep-alive\r\n
Date: Thu, 26 Aug 2021 07:01:37 GMT\r\n
Vary: Accept-Encoding\r\n
Via: ali com main, cache18.l2sg52[430,430,200-0,M], cache12.l2sg52[431,0], cache3.sg6[433,432,304-0,M]
Last-Modified: Thu, 12 Aug 2021 13:20:45 GMT\r\n
```

- HTTP status code : “304: Not Modified”
- This is because the browser simply retrieved the contents from its cache.
- If the contents of the webpage have been changed in the server, then it would have returned the contents of the file.
- But in this case no changes are made and thus it retrieves the old file from its cached memory.

How many HTTP GET request messages were sent by your browser?



frame contains GET and http

No.	Time	Source	Destination	Protocol	Length	Information
975	8.833037	192.168.1.100	122.225.67.211	HTTP	618	GET /20/0916/16/71596081_202009161613250691_main.jpg HTTP/1.1
2804	13.044786	192.168.1.100	122.225.67.209	HTTP	610	GET /2020/20201021/20201021173805767787l.jpg HTTP/1.1
2123	11.498828	192.168.1.100	122.225.67.209	HTTP	612	GET /2020/20201110/20201110174513478101285.jpg HTTP/1.1
5155	33.768257	192.168.1.100	122.225.67.209	HTTP	698	GET /2020/20201110/20201110174513478101285.jpg HTTP/1.1
2122	11.492233	192.168.1.100	122.225.67.209	HTTP	611	GET /2020/20201207/202012717533023211630l.jpg HTTP/1.1
5137	33.363646	192.168.1.100	122.225.67.209	HTTP	697	GET /2020/20201207/202012717533023211630l.jpg HTTP/1.1
2121	11.491979	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210108/20211817405999890978.jpg HTTP/1.1
2040	11.345945	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210302/20213217343279740187.jpg HTTP/1.1
5136	33.360297	192.168.1.100	122.225.67.209	HTTP	694	GET /2021/20210302/20213217343279740187.jpg HTTP/1.1
3967	17.655643	192.168.1.100	122.225.67.209	HTTP	610	GET /2021/20210317/20213172312676611134l.jpg HTTP/1.1
3917	17.099525	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210318/20213181940456291334.jpg HTTP/1.1
3037	13.744939	192.168.1.100	122.225.67.209	HTTP	611	GET /2021/20210320/20213202024585311775631.jpg HTTP/1.1
5241	35.217947	192.168.1.100	122.225.67.209	HTTP	695	GET /2021/20210320/20213202024585311775631.jpg HTTP/1.1
3316	14.515627	192.168.1.100	122.225.67.209	HTTP	611	GET /2021/20210322/20213221831447501439041.jpg HTTP/1.1
5261	35.957919	192.168.1.100	122.225.67.209	HTTP	696	GET /2021/20210322/20213221831447501439041.jpg HTTP/1.1
3671	15.639412	192.168.1.100	122.225.67.209	HTTP	610	GET /2021/20210322/2021322183144750671801.jpg HTTP/1.1
3282	14.350035	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210323/2021323239164846160 6.jpg HTTP/1.1
3268	14.308068	192.168.1.100	122.225.67.209	HTTP	611	GET /2021/20210324/20213241642551091188301.jpg HTTP/1.1
5254	35.595671	192.168.1.100	122.225.67.209	HTTP	697	GET /2021/20210324/20213241642551091188301.jpg HTTP/1.1
3647	15.571468	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210324/2021324164255936179 3.jpg HTTP/1.1
5276	37.157688	192.168.1.100	122.225.67.209	HTTP	695	GET /2021/20210324/2021324164255936179 3.jpg HTTP/1.1
2968	13.597424	192.168.1.100	122.225.67.209	HTTP	608	GET /2021/20210328/2021328183371576703.jpg HTTP/1.1
5234	35.205185	192.168.1.100	122.225.67.209	HTTP	694	GET /2021/20210328/2021328183371576703.jpg HTTP/1.1
3120	13.861482	192.168.1.100	122.225.67.209	HTTP	608	GET /2021/20210328/2021328183373172762.jpg HTTP/1.1
5252	35.572499	192.168.1.100	122.225.67.209	HTTP	694	GET /2021/20210328/2021328183373172762.jpg HTTP/1.1
3118	13.855518	192.168.1.100	122.225.67.209	HTTP	610	GET /2021/20210329/20213291636471876569 3.jpg HTTP/1.1
5246	35.257847	192.168.1.100	122.225.67.209	HTTP	696	GET /2021/20210329/20213291636471876569 3.jpg HTTP/1.1

3513	14.934417	192.168.1.100	122.225.67.209	HTTP	610	GET /2021/20210329/20213291638188284604 2.jpg HTTP/1.1
5269	36.246522	192.168.1.100	122.225.67.209	HTTP	696	GET /2021/20210329/20213291638188284604 2.jpg HTTP/1.1
2960	13.480285	192.168.1.100	122.225.67.209	HTTP	610	GET /2021/20210330/20213301725459310704 6.jpg HTTP/1.1
5224	34.866269	192.168.1.100	122.225.67.209	HTTP	696	GET /2021/20210330/20213301725459310704 6.jpg HTTP/1.1
1863	10.993399	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210330/2021330172546098955 4.jpg HTTP/1.1
5099	32.573165	192.168.1.100	122.225.67.209	HTTP	695	GET /2021/20210330/2021330172546098955 4.jpg HTTP/1.1
3083	13.783697	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210401/2021411722162654877 6.jpg HTTP/1.1
5242	35.218825	192.168.1.100	122.225.67.209	HTTP	694	GET /2021/20210401/2021411722162654877 6.jpg HTTP/1.1
2924	13.393951	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210401/2021411722162814619 0.jpg HTTP/1.1
5222	34.835180	192.168.1.100	122.225.67.209	HTTP	694	GET /2021/20210401/2021411722162814619 0.jpg HTTP/1.1
2923	13.393148	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210405/2021452340384849344 5.jpg HTTP/1.1
5219	34.826180	192.168.1.100	122.225.67.209	HTTP	693	GET /2021/20210405/2021452340384849344 5.jpg HTTP/1.1
3386	14.709226	192.168.1.100	122.225.67.209	HTTP	610	GET /2021/20210405/2021452340385011145 47.jpg HTTP/1.1
2922	13.392925	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210407/2021471628504215696 3.jpg HTTP/1.1
5218	34.824674	192.168.1.100	122.225.67.209	HTTP	694	GET /2021/20210407/2021471628504215696 3.jpg HTTP/1.1
1465	10.518098	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210805/2021851534237623626 6.jpg HTTP/1.1
4987	31.382170	192.168.1.100	122.225.67.209	HTTP	694	GET /2021/20210805/2021851534237623626 6.jpg HTTP/1.1
1463	10.516670	192.168.1.100	122.225.67.209	HTTP	610	GET /2021/20210806/2021861532426722461 14.jpg HTTP/1.1
4960	31.087391	192.168.1.100	122.225.67.209	HTTP	696	GET /2021/20210806/2021861532426722461 14.jpg HTTP/1.1
1462	10.515595	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210809/2021891615714015468 5.jpg HTTP/1.1
4957	31.060210	192.168.1.100	122.225.67.209	HTTP	694	GET /2021/20210809/2021891615714015468 5.jpg HTTP/1.1
1452	10.467758	192.168.1.100	122.225.67.209	HTTP	610	GET /2021/20210810/2021810155321402240 94.jpg HTTP/1.1
4950	31.012573	192.168.1.100	122.225.67.209	HTTP	696	GET /2021/20210810/2021810155321402240 94.jpg HTTP/1.1
1466	10.519637	192.168.1.100	122.225.67.209	HTTP	610	GET /2021/20210810/2021810155912875923 61.jpg HTTP/1.1
5007	31.464660	192.168.1.100	122.225.67.209	HTTP	696	GET /2021/20210810/2021810155912875923 61.jpg HTTP/1.1
964	8.821063	192.168.1.100	122.225.67.209	HTTP	610	GET /2021/20210811/2021811155161251105 51.jpg HTTP/1.1
4939	30.628803	192.168.1.100	122.225.67.209	HTTP	696	GET /2021/20210811/2021811155161251105 51.jpg HTTP/1.1
949	8.799904	192.168.1.100	122.225.67.209	HTTP	610	GET /2021/20210811/2021811155161401120 62.jpg HTTP/1.1
4936	30.627020	192.168.1.100	122.225.67.209	HTTP	696	GET /2021/20210811/2021811155161401120 62.jpg HTTP/1.1
965	8.821326	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210811/2021811155163110930 3.jpg HTTP/1.1
4940	30.664790	192.168.1.100	122.225.67.209	HTTP	695	GET /2021/20210811/2021811155163110930 3.jpg HTTP/1.1
953	8.808341	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210811/2021811155167810633 2.jpg HTTP/1.1
4937	30.627349	192.168.1.100	122.225.67.209	HTTP	695	GET /2021/20210811/2021811155167810633 2.jpg HTTP/1.1
959	8.812295	192.168.1.100	122.225.67.209	HTTP	608	GET /2021/20210811/202181115516939146 4.jpg HTTP/1.1
4938	30.627965	192.168.1.100	122.225.67.209	HTTP	694	GET /2021/20210811/202181115516939146 4.jpg HTTP/1.1
968	8.826104	192.168.1.100	122.225.67.209	HTTP	609	GET /2021/20210811/2021811159979618448 3.jpg HTTP/1.1
4945	30.750459	192.168.1.100	122.225.67.209	HTTP	693	GET /2021/20210811/2021811159979618448 3.jpg HTTP/1.1
1739	10.977689	192.168.1.100	122.225.67.209	HTTP	611	GET /2021/20210811/20218111642166871495 86.jpg HTTP/1.1

5017	31.712140	192.168.1.100	122.225.67.209	HTTP	696	GET /2021/20210811/20218111642166871495 86.jpg HTTP/1.1
1565	10.723311	192.168.1.100	163.181.36.230	HTTP	614	GET /ajax/ReadingRoom/getJCWJJData.ashx?cid=0&pagenum=21&_=1629961279223 HTTP/1.1
4963	31.117006	192.168.1.100	163.181.36.230	HTTP	614	GET /ajax/ReadingRoom/getJCWJJData.ashx?cid=0&pagenum=21&_=1629961299624 HTTP/1.1
399	7.013005	192.168.1.100	163.181.36.224	HTTP	544	GET /chat/chat.css?t=2018091401 HTTP/1.1
3972	17.744650	192.168.1.100	163.181.36.230	HTTP	588	GET /clippertool/getnoteclipperASHX.ashx?type=10&jsoncallback=jsonp1629961276990 HTTP/1.1
4946	30.770424	192.168.1.100	163.181.36.230	HTTP	588	GET /clippertool/getnoteclipperASHX.ashx?type=10&jsoncallback=jsonp1629961299072 HTTP/1.1
4716	19.904205	192.168.1.100	47.103.42.25	HTTP	487	GET /images/cert/bottom_large_img.png HTTP/1.1
4948	30.978243	192.168.1.100	47.103.42.25	HTTP	487	GET /images/cert/bottom_large_img.png HTTP/1.1
115	6.070096	192.168.1.100	163.181.36.230	HTTP	642	GET /index.html HTTP/1.1
4888	29.457759	192.168.1.100	163.181.36.230	HTTP	755	GET /index.html HTTP/1.1
4485	19.069105	192.168.1.100	163.181.36.227	HTTP	584	GET /index/beian.png HTTP/1.1
4497	19.080633	192.168.1.100	163.181.36.227	HTTP	585	GET /index/jubao2.jpg HTTP/1.1
4516	19.150415	192.168.1.100	163.181.36.227	HTTP	587	GET /index/jubao3_1.jpg HTTP/1.1
4490	19.072194	192.168.1.100	163.181.36.227	HTTP	585	GET /index/jubao4.jpg HTTP/1.1
4337	18.621145	192.168.1.100	163.181.36.227	HTTP	584	GET /index/num-1.gif HTTP/1.1
4382	18.783199	192.168.1.100	163.181.36.227	HTTP	585	GET /index/num-10.gif HTTP/1.1
4338	18.621494	192.168.1.100	163.181.36.227	HTTP	584	GET /index/num-2.gif HTTP/1.1
4339	18.623278	192.168.1.100	163.181.36.227	HTTP	584	GET /index/num-3.gif HTTP/1.1
4368	18.651103	192.168.1.100	163.181.36.227	HTTP	584	GET /index/num-4.gif HTTP/1.1
4370	18.702213	192.168.1.100	163.181.36.227	HTTP	584	GET /index/num-5.gif HTTP/1.1
4373	18.716035	192.168.1.100	163.181.36.227	HTTP	584	GET /index/num-6.gif HTTP/1.1
4374	18.719619	192.168.1.100	163.181.36.227	HTTP	584	GET /index/num-7.gif HTTP/1.1
4376	18.735346	192.168.1.100	163.181.36.227	HTTP	584	GET /index/num-8.gif HTTP/1.1
4380	18.750659	192.168.1.100	163.181.36.227	HTTP	584	GET /index/num-9.gif HTTP/1.1
1498	10.561016	192.168.1.100	163.181.36.227	HTTP	584	GET /index/sy-11.gif HTTP/1.1
4403	18.847533	192.168.1.100	163.181.36.227	HTTP	584	GET /index/sy-17.gif HTTP/1.1
4405	18.865702	192.168.1.100	163.181.36.227	HTTP	584	GET /index/sy-19.gif HTTP/1.1
4389	18.823412	192.168.1.100	163.181.36.227	HTTP	584	GET /index/sy-20.gif HTTP/1.1
4407	18.870437	192.168.1.100	163.181.36.227	HTTP	584	GET /index/sy-24.gif HTTP/1.1
4311	18.595299	192.168.1.100	163.181.36.227	HTTP	584	GET /index/sy-33.gif HTTP/1.1
4438	18.930584	192.168.1.100	163.181.36.227	HTTP	584	GET /index/tit22.gif HTTP/1.1
4442	18.969801	192.168.1.100	163.181.36.227	HTTP	584	GET /index/tit24.gif HTTP/1.1
4462	19.054791	192.168.1.100	163.181.36.227	HTTP	584	GET /index/tit25.gif HTTP/1.1
4441	18.969284	192.168.1.100	163.181.36.227	HTTP	581	GET /index/wx.gif HTTP/1.1
4026	18.119452	192.168.1.100	163.181.36.227	HTTP	588	GET /index7/banner_6.jpg HTTP/1.1
5160	33.984750	192.168.1.100	163.181.36.227	HTTP	590	GET /index7/banner_btn.png HTTP/1.1
4030	18.122328	192.168.1.100	163.181.36.227	HTTP	589	GET /index7/bannerl_1.jpg HTTP/1.1
4036	18.133871	192.168.1.100	163.181.36.227	HTTP	602	GET /index7/bannerl_2.jpg?t=2019012801 HTTP/1.1
4128	18.284968	192.168.1.100	163.181.36.227	HTTP	589	GET /index7/bannerl_3.jpg HTTP/1.1

4141	18.296138	192.168.1.100	163.181.36.227	HTTP	589 GET /index7/bannerl_4.jpg HTTP/1.1
4153	18.312171	192.168.1.100	163.181.36.227	HTTP	589 GET /index7/bannerl_5.jpg HTTP/1.1
3989	18.029388	192.168.1.100	163.181.36.227	HTTP	586 GET /index7/dingtu.gif HTTP/1.1
4168	18.382434	192.168.1.100	163.181.36.227	HTTP	597 GET /index7/dsfs.jpg?t=2019012801 HTTP/1.1
1496	10.560529	192.168.1.100	163.181.36.227	HTTP	589 GET /index7/icon_yuan.gif HTTP/1.1
1529	10.654817	192.168.1.100	163.181.36.227	HTTP	590 GET /index7/icon_yuan2.png HTTP/1.1
4436	18.908236	192.168.1.100	163.181.36.227	HTTP	595 GET /index7/index_footerimg.jpg HTTP/1.1
4202	18.410614	192.168.1.100	163.181.36.227	HTTP	593 GET /index7/index_rightgg.jpg HTTP/1.1
4270	18.496554	192.168.1.100	163.181.36.227	HTTP	595 GET /index7/indexallbg.png?2021 HTTP/1.1
1484	10.556992	192.168.1.100	163.181.36.227	HTTP	589 GET /index7/jiangnew2.gif HTTP/1.1
4384	18.805303	192.168.1.100	163.181.36.227	HTTP	585 GET /index7/lv_b1.png HTTP/1.1
1495	10.560158	192.168.1.100	163.181.36.227	HTTP	592 GET /index7/main_rightbg.gif HTTP/1.1
396	7.012335	192.168.1.100	163.181.36.224	HTTP	553 GET /index7/newSiteBase.css?t=2021041205 HTTP/1.1
397	7.012627	192.168.1.100	163.181.36.224	HTTP	554 GET /index7/newindex2020.css?t=2021080901 HTTP/1.1
3983	18.029035	192.168.1.100	163.181.36.227	HTTP	585 GET /index7/nlogo.jpg HTTP/1.1
4232	18.426102	192.168.1.100	163.181.36.227	HTTP	588 GET /index7/str_jcyc.png HTTP/1.1
4233	18.426602	192.168.1.100	163.181.36.227	HTTP	588 GET /index7/str_ycdr.gif HTTP/1.1
1527	10.653515	192.168.1.100	163.181.36.227	HTTP	588 GET /index7/str_yczs.png HTTP/1.1
1499	10.561237	192.168.1.100	163.181.36.227	HTTP	593 GET /index7/top_slide_btn.png HTTP/1.1
1497	10.560785	192.168.1.100	163.181.36.227	HTTP	582 GET /index7/w.png? HTTP/1.1
356	6.905097	192.168.1.100	163.181.36.230	HTTP	542 GET /js/360query18.js?t=2016122901 HTTP/1.1
713	7.671350	192.168.1.100	163.181.36.230	HTTP	556 GET /js/Statistics/addStatistics.js?t=2020062801 HTTP/1.1
720	7.706280	192.168.1.100	163.181.36.230	HTTP	554 GET /js/book/bookstoreTemplate.js?t=2021071302 HTTP/1.1
839	8.082121	192.168.1.100	163.181.36.230	HTTP	550 GET /js/book/couponReceive.js?t=2020011901 HTTP/1.1
1461	10.482403	192.168.1.100	163.181.36.230	HTTP	547 GET /js/chat/createchat.js?t=2018082901 HTTP/1.1
829	7.986842	192.168.1.100	163.181.36.230	HTTP	533 GET /js/common/docgjio.js HTTP/1.1
394	7.011931	192.168.1.100	163.181.36.230	HTTP	540 GET /js/commonJS.js?t=2016062102 HTTP/1.1
377	6.990638	192.168.1.100	163.181.36.230	HTTP	529 GET /js/index7/PIE.js HTTP/1.1
509	7.123513	192.168.1.100	163.181.36.230	HTTP	545 GET /js/index7/follow.js?t=2021012102 HTTP/1.1
398	7.012829	192.168.1.100	163.181.36.230	HTTP	537 GET /js/index7/getPageHtml.js HTTP/1.1
712	7.670059	192.168.1.100	163.181.36.230	HTTP	545 GET /js/index7/index7.js?t=2021052801 HTTP/1.1
714	7.673820	192.168.1.100	163.181.36.230	HTTP	551 GET /js/index7/index_common.js?t=2021081202 HTTP/1.1
721	7.706963	192.168.1.100	163.181.36.230	HTTP	548 GET /js/index7/index_new.js?t=2021081203 HTTP/1.1
830	7.987261	192.168.1.100	163.181.36.230	HTTP	560 GET /js/index7/jquery.roundabout.min.js?t=2018102601 HTTP/1.1
828	7.985030	192.168.1.100	163.181.36.230	HTTP	545 GET /js/index7/paging.js?t=2017012001 HTTP/1.1
395	7.012149	192.168.1.100	163.181.36.230	HTTP	542 GET /js/jQuery.md5.js?t=2013121101 HTTP/1.1
831	7.988971	192.168.1.100	163.181.36.230	HTTP	566 GET /js/study/common/jquery.nicescroll.min.js?t=2018102401 HTTP/1.1
4886	29.411039	2401:4900:22c5:d8e0…	2001:1900:2381:c02:…	HTTP	361 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?3437b9c4c754cfbd HTTP/1.1
1528	10.654344	192.168.1.100	163.181.36.227	HTTP	585 GET /newsite/dian.gif HTTP/1.1

389	7.011663	192.168.1.100	163.181.36.224	HTTP	542 GET /pageNum.css?t=2018062701 HTTP/1.1
4619	19.252514	192.168.1.100	59.110.16.57	HTTP	601 GET /pcpage.jpg?code=69-1&1629961276846 HTTP/1.1
4941	30.703281	192.168.1.100	59.110.16.57	HTTP	601 GET /pcpage.jpg?code=69-1&1629961299015 HTTP/1.1
1601	10.790596	192.168.1.100	106.4.83.215	HTTP	616 GET /productinfo/4908/4908_cover_1581675364498.jpg HTTP/1.1
1464	10.517008	192.168.1.100	106.4.83.215	HTTP	616 GET /productinfo/4919/4919_cover_1581675372529.jpg HTTP/1.1
3418	14.801339	192.168.1.100	106.4.83.215	HTTP	616 GET /productinfo/5034/5034_cover_1581675468201.jpg HTTP/1.1
1507	10.577862	192.168.1.100	106.4.83.215	HTTP	616 GET /productinfo/5081/5081_cover_1581675512873.jpg HTTP/1.1
3971	17.744194	192.168.1.100	106.4.83.215	HTTP	616 GET /productinfo/5217/5217_cover_1581675622670.jpg HTTP/1.1
979	8.936998	192.168.1.100	106.4.83.215	HTTP	616 GET /productinfo/5305/5305_cover_1585299349107.jpg HTTP/1.1
972	8.829891	192.168.1.100	106.4.83.215	HTTP	617 GET /productinfo/5438/5438_cover_1586922120787.jpeg HTTP/1.1
1957	11.190658	192.168.1.100	106.4.83.215	HTTP	616 GET /productinfo/5451/5451_cover_1587523790062.jpg HTTP/1.1
4942	30.731559	192.168.1.100	106.4.83.215	HTTP	690 GET /productinfo/5451/5451_cover_1587523790062.jpg HTTP/1.1
5023	31.834153	192.168.1.100	106.4.83.215	HTTP	690 GET /productinfo/5451/5451_cover_1587523790062.jpg HTTP/1.1
958	8.812073	192.168.1.100	106.4.83.215	HTTP	616 GET /productinfo/5809/5809_cover_1595225030178.jpg HTTP/1.1
3119	13.858899	192.168.1.100	106.4.83.215	HTTP	616 GET /productinfo/5825/5825_cover_1595225048631.jpg HTTP/1.1
3279	14.327986	192.168.1.100	106.4.83.215	HTTP	616 GET /productinfo/5937/5937_cover_1595399919475.jpg HTTP/1.1
4542	19.165503	192.168.1.100	163.181.36.227	HTTP	582 GET /read/wz22.gif HTTP/1.1
4210	18.415641	192.168.1.100	163.181.36.227	HTTP	597 GET /register/snswarningtip11.gif HTTP/1.1
5022	31.830150	106.4.83.215	192.168.1.100	HTTP	1031 HTTP/1.1 206 Partial Content (image/jpeg)

Hypertext Transfer Protocol: Protocol | Packets: 5329 · Displayed: 162 (3.0%) · Dropped: 0 (0.0%)

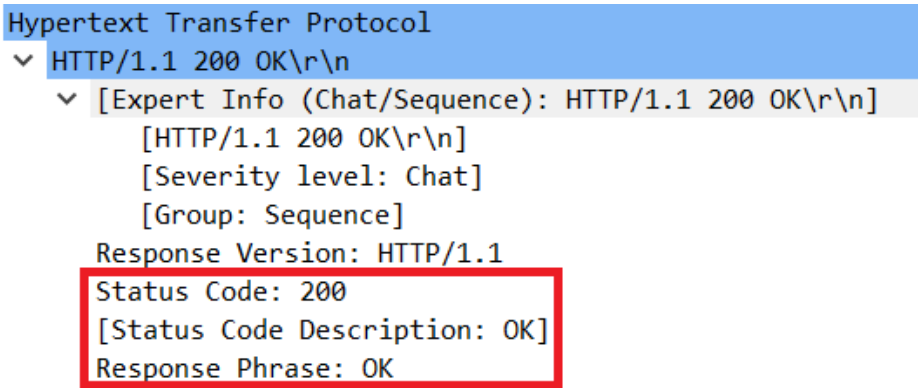
- Totally **162** HTTP GET Request messages were sent by my browser.

How many data-containing TCP segments were needed to carry the single HTTP response? What is the size for each of the segment?

[Frame: 163, payload: 0-1317 (1318 bytes)]
[Frame: 164, payload: 1318-2635 (1318 bytes)]
[Frame: 167, payload: 2636-3953 (1318 bytes)]
[Frame: 168, payload: 3954-5017 (1064 bytes)]
[Frame: 301, payload: 5018-6294 (1277 bytes)]
[Frame: 302, payload: 6295-7612 (1318 bytes)]
[Frame: 303, payload: 7613-8930 (1318 bytes)]
[Frame: 304, payload: 8931-9206 (276 bytes)]
[Frame: 312, payload: 9207-9587 (381 bytes)]
[Frame: 420, payload: 9588-10729 (1142 bytes)]
[Frame: 422, payload: 10730-12047 (1318 bytes)]
[Frame: 423, payload: 12048-12364 (317 bytes)]
[Frame: 424, payload: 12365-12497 (133 bytes)]
[Frame: 610, payload: 12498-13499 (1002 bytes)]
[Frame: 611, payload: 13500-14817 (1318 bytes)]
[Frame: 612, payload: 14818-16135 (1318 bytes)]
[Frame: 614, payload: 16136-17246 (1111 bytes)]
[Frame: 684, payload: 17247-17890 (644 bytes)]
[Frame: 685, payload: 17891-19208 (1318 bytes)]
[Frame: 687, payload: 19209-20526 (1318 bytes)]
[Frame: 688, payload: 20527-21421 (895 bytes)]
[Frame: 715, payload: 21422-22323 (902 bytes)]
[Frame: 716, payload: 22324-23641 (1318 bytes)]
[Frame: 717, payload: 23642-24959 (1318 bytes)]
[Frame: 718, payload: 24960-25484 (525 bytes)]
[Frame: 807, payload: 25485-26120 (636 bytes)]
[Frame: 809, payload: 26121-27438 (1318 bytes)]
[Frame: 810, payload: 27439-28756 (1318 bytes)]
[Frame: 811, payload: 28757-29161 (405 bytes)]
[Frame: 881, payload: 29162-30479 (1318 bytes)]
[Frame: 882, payload: 30480-31797 (1318 bytes)]
[Frame: 884, payload: 31798-33115 (1318 bytes)]
[Frame: 885, payload: 33116-33232 (117 bytes)]
[Frame: 889, payload: 33233-33991 (759 bytes)]
[Frame: 890, payload: 33992-35309 (1318 bytes)]
[Frame: 891, payload: 35310-36455 (1146 bytes)]
[Frame: 931, payload: 36456-37773 (1318 bytes)]
[Frame: 932, payload: 37774-39091 (1318 bytes)]
[Frame: 933, payload: 39092-39519 (428 bytes)]
[Frame: 939, payload: 39520-40114 (595 bytes)]
[Frame: 940, payload: 40115-40425 (311 bytes)]
[Frame: 941, payload: 40426-41743 (1318 bytes)]
[Frame: 942, payload: 41744-42652 (909 bytes)]
[Frame: 943, payload: 42653-43970 (1318 bytes)]
[Frame: 944, payload: 43971-44174 (204 bytes)]
[Frame: 945, payload: 44175-44194 (20 bytes)]
[Segment count: 46]
[Reassembled TCP length: 44195]

- **46** data-containing TCP segments were needed to carry the single HTTP response and most of the segments are of size 1318 bytes.

What is the status code and phrase associated with the response to the HTTP GET request?



- Status Code : 200
- Response Phrase : OK

Thankyou!!