COL334 - Computer Networks

Prakhar Aggarwal 2019CS50441

Assignment-1

August 22, 2021

1. Networking Tools

(a) IP addresses are provided by an Internet Service Provider (ISP). Most likely, the ISP will provide us with a dynamic IP address (In essence, that IP address is borrowed or “leased” whenever we go online).

1. When connected to the Netplus Network, IP address is: **192.168.1.10**
2. When connected to ZTE Network, the IP address is: **192.168.1.4**
3. When connected to Airtel Network, the IP address is: **192.168.43.75**

(b) IP address associated with

www.google.com:

IPv4: 142.250.194.68

(using default local DNS server)

```
prakank@prakank:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.194.68
Name:   www.google.com
Address: 2404:6800:4002:820::2004
```

www.facebook.com:

IPv4: 157.240.198.35

```
prakank@prakank:~$ nslookup www.facebook.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.198.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f144:181:face:b00c:0:25de
```

Using the Google Public DNS (8.8.8.8), IP address change as follows:

www.google.com:

IPv4: 142.250.194.196

```
prakank@prakank:~$ nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> www.google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.194.196
Name:   www.google.com
Address: 2404:6800:4002:824::2004
```

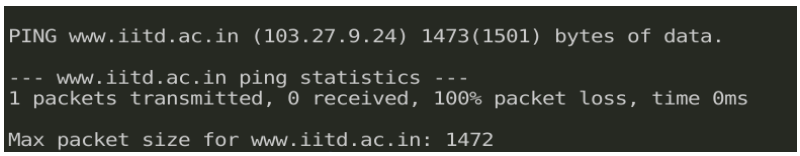
www.facebook.com:
IPv4: 157.240.198.35

Different DNS server stores different IP address for the same domain name.Large websites like www.google.com and www.facebook.com have large database, hence, they have multiple IP address to prevent traffic. So, different DNS server can either store the same IP address or a different one for the same domain name.

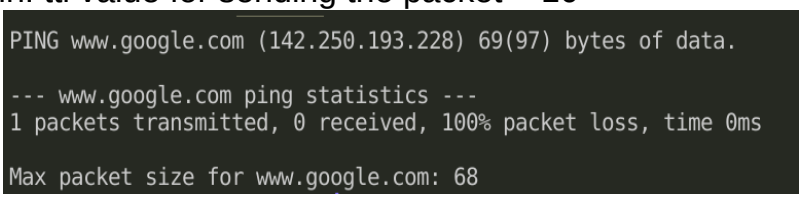
(c) *ping*

The maximum size of packet that is successfully sent is different for different domains. It was calculated using a Python script (attached in the zip file)

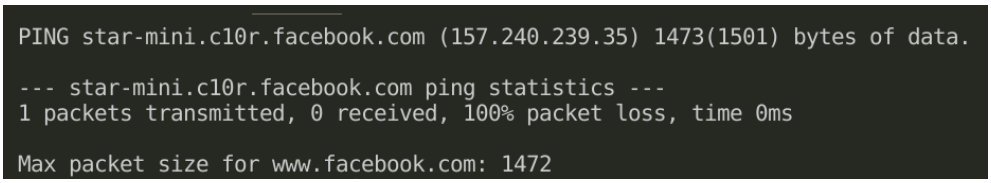
Max. size of packets for www.iitd.ac.in is: 1472 (1427 + 28) with rtt = 18.1ms
Min. ttl value for sending the packet = 15



For www.google.com, it is: 68 (68 + 28) with rtt = 17.4ms
Min. ttl value for sending the packet = 10



For www.facebook.com, it is: 1472 (1472 + 28) with rtt = 35.7ms
Min. ttl value for sending the packet = 10



(d) traceroute to www.iitd.ac.in (connected to Netplus) (192.168.1.10)

```
prakank@prakank:~$ traceroute -I www.iitd.ac.in
traceroute to www.iitd.ac.in (103.27.9.24), 64 hops max
  1   192.168.1.1  2.349ms  5.583ms  5.687ms
  2   100.66.0.1  4.438ms  4.836ms  2.847ms
  3   192.168.241.38  6.027ms  6.008ms  6.874ms
  4   192.168.241.37  6.124ms  7.275ms  6.741ms
  5   192.168.252.17  6.427ms  *  10.237ms
  6   192.168.200.2  12.229ms  7.765ms  7.919ms
  7   14.141.116.85  7.862ms  7.828ms  6.985ms
  8   172.28.144.26  17.042ms  15.548ms  16.062ms
  9   14.140.210.22  15.001ms  15.828ms  14.704ms
 10   *  *  *
 11   *  *  *
 12   *  *  *
 13   103.27.9.24  16.369ms  15.563ms  17.166ms
```

traceroute to www.iitd.ac.in (connected to Airtel) (192.168.43.75)

```
prakank@prakank:~$ traceroute -I www.iitd.ac.in
traceroute to www.iitd.ac.in (103.27.9.24), 64 hops max
  1   192.168.43.1  59.156ms  3.556ms  2.665ms
  2   106.200.136.225  77.960ms  46.289ms  36.570ms
  3   106.193.253.121  28.610ms  46.514ms  34.885ms
  4   122.185.217.85  36.002ms  43.152ms  26.316ms
  5   182.79.181.219  35.087ms  31.822ms  43.530ms
  6   115.110.232.173  37.694ms  35.759ms  70.499ms
  7   *  *  *
  8   14.140.210.22  155.193ms  59.381ms  176.131ms
  9   10.119.234.161  146.038ms  51.235ms  153.234ms
 10   10.119.233.65  54.468ms  150.104ms  39.791ms
 11   10.119.233.66  38.407ms  126.259ms  43.753ms
 12   103.27.9.24  41.131ms  119.786ms  30.076ms
```

traceroute to www.facebook.com (connected to Airtel) (192.168.43.75)

```
prakank@prakank:~$ traceroute -I www.facebook.com
traceroute to star-mini.c10r.facebook.com (157.240.239.35), 64 hops max
  1   192.168.43.1  4.549ms  4.134ms  3.806ms
  2   192.168.59.1  190.116ms  25.117ms  77.646ms
  3   122.185.39.38  45.585ms  30.258ms  29.518ms
  4   122.185.39.37  29.916ms  29.787ms  29.773ms
  5   116.119.49.32  30.636ms  45.825ms  53.301ms
  6   157.240.70.154  219.724ms  51.911ms  323.709ms
  7   74.119.78.201  35.528ms  66.069ms  83.010ms
  8   157.240.36.19  70.178ms  53.475ms  50.216ms
  9   157.240.239.35  42.328ms  38.276ms  41.639ms
```

traceroute to www.facebook.com (connected to Netplus) (192.168.1.10)

```
prakank@prakank:~$ traceroute -I www.facebook.com
traceroute to star-mini.c10r.facebook.com (157.240.239.35), 64 hops max
  1   192.168.1.1  3.374ms  1.287ms  1.388ms
  2   100.66.0.1  9.072ms  2.262ms  2.479ms
  3   192.168.241.38  5.965ms  5.720ms  4.888ms
  4   192.168.241.37  7.745ms  8.144ms  124.270ms
  5   192.168.252.17  8.822ms  *  8.528ms
  6   192.168.200.2  8.750ms  8.669ms  10.019ms
  7   157.240.79.134  25.974ms  16.803ms  20.579ms
  8   74.119.78.33  13.593ms  16.547ms  31.224ms
  9   157.240.36.23  13.836ms  19.824ms  14.134ms
 10   157.240.239.35  13.730ms  20.821ms  17.263ms
```

- The routers to www.iitd.ac.in has more non-responding routers as compared to www.facebook.com.
- In Ubuntu, traceroute uses IPv4 addresses. We have traceroute6 in Ubuntu which uses IPv6 addresses.
- For the unresponding routers, we can find its address using the ping command.
- We can check the hop number in traceroute command whose IP address is unknown and can provide that hop number as ttl value in the ping command.

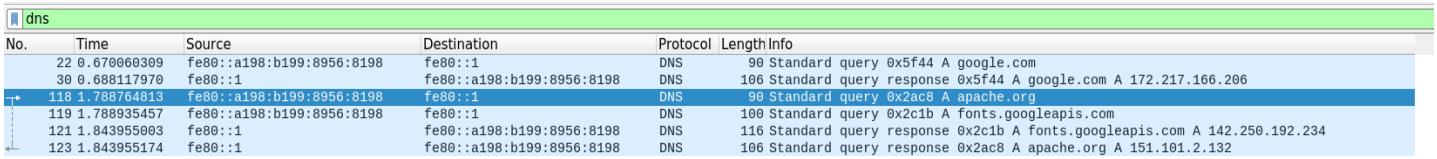
```
prakank@prakank:~$ traceroute -I www.iitd.ac.in
traceroute to www.iitd.ac.in (103.27.9.24), 64 hops max
  1   192.168.1.1  1.335ms  1.129ms  1.134ms
  2   100.66.0.1  1.936ms  3.246ms  1.741ms
  3   192.168.241.38  5.136ms  4.931ms  5.131ms
  4   192.168.241.37  5.443ms  6.041ms  58.101ms
  5   192.168.252.17  5.909ms  *  *
  6   192.168.200.2  6.999ms  7.736ms  8.725ms
  7   14.141.116.85  15.945ms  7.068ms  12.908ms
  8   172.28.144.26  14.600ms  58.139ms  14.862ms
  9   14.140.210.22  13.929ms  14.730ms  14.123ms
 10   *  *  *
^C
```

```
prakank@prakank:~$ ping -t 8 -c 1 www.iitd.ac.in
PING www.iitd.ac.in (103.27.9.24) 56(84) bytes of data.
From 172.28.144.26 (172.28.144.26) icmp_seq=1 Time to live exceeded

--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

prakank@prakank:~$ ping -t 9 -c 1 www.iitd.ac.in
PING www.iitd.ac.in (103.27.9.24) 56(84) bytes of data.
From 14.140.210.22.static-Delhi-vsnl.net.in (14.140.210.22) icmp_seq=1 Time to live exceeded

--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

2.) Packet Analysis (Wireshark)

To capture http://apache.org/ packets, I closed all other pages and stopped capturing the packets in wireshark once the page was loaded completely.

(a) For capturing dns packets, I cleared the DNS cache from the system as well as from the browser.



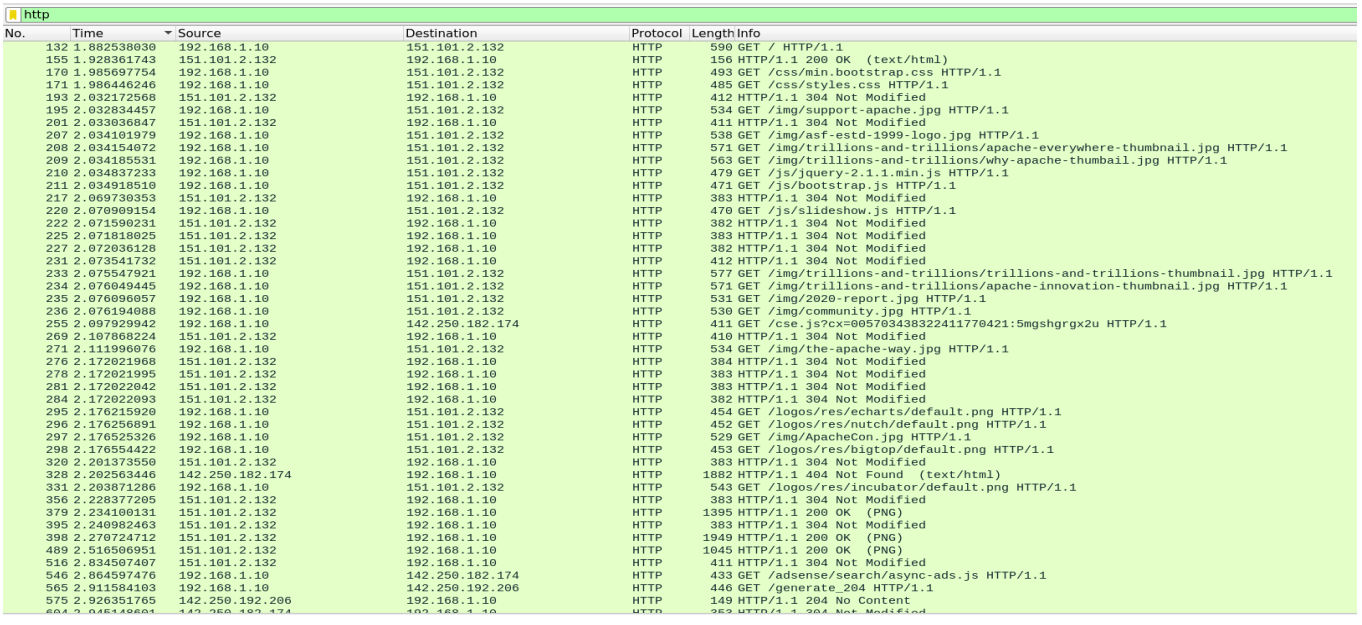
dns

No.	Time	Source	Destination	Protocol	Length	Info
22	0.670060309	fe80::a198:b199:8956:8198	fe80::1	DNS	90	Standard query 0x5f44 A google.com
30	0.688117970	fe80::1	fe80::a198:b199:8956:8198	DNS	106	Standard query response 0x5f44 A google.com A 172.217.166.206
118	1.788764813	fe80::a198:b199:8956:8198	fe80::1	DNS	90	Standard query 0x2ac8 A apache.org
119	1.788935457	fe80::a198:b199:8956:8198	fe80::1	DNS	100	Standard query 0x2c1b A fonts.googleapis.com
121	1.843955003	fe80::1	fe80::a198:b199:8956:8198	DNS	116	Standard query response 0x2c1b A fonts.googleapis.com A 142.250.192.234
123	1.843955174	fe80::1	fe80::a198:b199:8956:8198	DNS	106	Standard query response 0x2ac8 A apache.org A 151.101.2.132

It took a total of 1.8439 – 1.7887 = 55.2ms for the DNS request-response to complete.

(b) Approximately 48 HTTP requests were generated for loading the http://apache.org/ page completely.

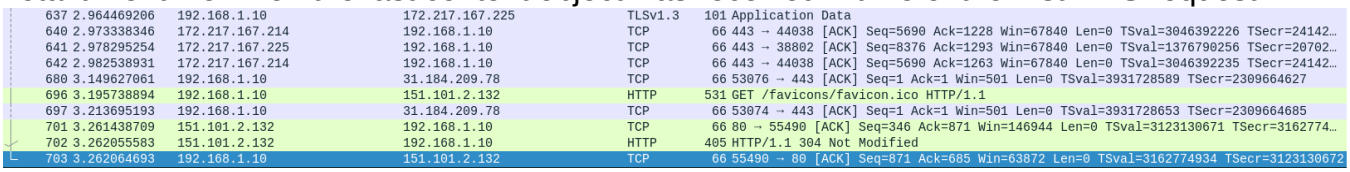
Page is loaded in chunks and not in entirety. Browser renders as soon as a packet arrives and leaves space for the remaining packets.
Server sends the DOM which helps the browser to know the layout of the page. After this, the browser reads CSS files (style, font, color). CSS files have the link for the images and other files to be loaded, so the browser generates a GET request for such files and starts downloading them in the background. As soon as the file is downloaded, it is rendered on the web page. Meanwhile, browser also receives the Javascript files (js files) which helps to make the web page responsive.



http

No.	Time	Source	Destination	Protocol	Length	Info
132	1.882538030	192.168.1.10	151.101.2.132	HTTP	590	GET / HTTP/1.1
155	1.928361743	151.101.2.132	192.168.1.10	HTTP	156	HTTP/1.1 200 OK (text/html)
170	1.985697754	192.168.1.10	151.101.2.132	HTTP	493	GET /css/min.bootstrap.css HTTP/1.1
171	1.986446246	192.168.1.10	151.101.2.132	HTTP	485	GET /css/styles.css HTTP/1.1
193	2.032172568	151.101.2.132	192.168.1.10	HTTP	412	HTTP/1.1 304 Not Modified
195	2.032834457	192.168.1.10	151.101.2.132	HTTP	534	GET /img/support-apache.jpg HTTP/1.1
201	2.033036847	151.101.2.132	192.168.1.10	HTTP	411	HTTP/1.1 304 Not Modified
207	2.034101979	192.168.1.10	151.101.2.132	HTTP	538	GET /img/asf-estd-1999-logo.jpg HTTP/1.1
208	2.034154072	192.168.1.10	151.101.2.132	HTTP	571	GET /img/trillions-and-trillions/apache-everywhere-thumbnail.jpg HTTP/1.1
209	2.034185531	192.168.1.10	151.101.2.132	HTTP	563	GET /img/trillions-and-trillions/why-apache-thumbail.jpg HTTP/1.1
210	2.034837233	192.168.1.10	151.101.2.132	HTTP	479	GET /js/jquery-2.1.1.min.js HTTP/1.1
211	2.034918510	192.168.1.10	151.101.2.132	HTTP	471	GET /js/bootstrap.js HTTP/1.1
217	2.069730353	151.101.2.132	192.168.1.10	HTTP	383	HTTP/1.1 304 Not Modified
220	2.070909154	192.168.1.10	151.101.2.132	HTTP	470	GET /js/slideshow.js HTTP/1.1
222	2.071590231	151.101.2.132	192.168.1.10	HTTP	382	HTTP/1.1 304 Not Modified
225	2.071818025	151.101.2.132	192.168.1.10	HTTP	383	HTTP/1.1 304 Not Modified
227	2.072036128	151.101.2.132	192.168.1.10	HTTP	382	HTTP/1.1 304 Not Modified
231	2.073541732	151.101.2.132	192.168.1.10	HTTP	412	HTTP/1.1 304 Not Modified
233	2.075547921	192.168.1.10	151.101.2.132	HTTP	577	GET /img/trillions-and-trillions/trillions-and-trillions-thumbnail.jpg HTTP/1.1
234	2.076049445	192.168.1.10	151.101.2.132	HTTP	571	GET /img/trillions-and-trillions/apache-innovation-thumbnail.jpg HTTP/1.1
235	2.076096057	192.168.1.10	151.101.2.132	HTTP	531	GET /img/2020-report.jpg HTTP/1.1
236	2.076194088	192.168.1.10	151.101.2.132	HTTP	530	GET /img/community.jpg HTTP/1.1
255	2.097929942	192.168.1.10	142.250.182.174	HTTP	411	GET /cse.js?cx=005703438322411770421:5mgshgrgx2u HTTP/1.1
269	2.107868224	151.101.2.132	192.168.1.10	HTTP	410	HTTP/1.1 304 Not Modified
271	2.111996076	192.168.1.10	151.101.2.132	HTTP	534	GET /img/the-apache-way.jpg HTTP/1.1
276	2.172021968	151.101.2.132	192.168.1.10	HTTP	384	HTTP/1.1 304 Not Modified
278	2.172021995	151.101.2.132	192.168.1.10	HTTP	383	HTTP/1.1 304 Not Modified
281	2.172022042	151.101.2.132	192.168.1.10	HTTP	383	HTTP/1.1 304 Not Modified
284	2.172022093	151.101.2.132	192.168.1.10	HTTP	382	HTTP/1.1 304 Not Modified
295	2.176215920	192.168.1.10	151.101.2.132	HTTP	454	GET /logos/res/echarts/default.png HTTP/1.1
296	2.176256891	192.168.1.10	151.101.2.132	HTTP	452	GET /logos/res/nutch/default.png HTTP/1.1
297	2.176525326	192.168.1.10	151.101.2.132	HTTP	529	GET /img/ApacheCon.jpg HTTP/1.1
298	2.176554422	192.168.1.10	151.101.2.132	HTTP	453	GET /logos/res/bigtop/default.png HTTP/1.1
320	2.201373550	151.101.2.132	192.168.1.10	HTTP	383	HTTP/1.1 304 Not Modified
328	2.202563446	142.250.182.174	192.168.1.10	HTTP	1882	HTTP/1.1 404 Not Found (text/html)
331	2.203871286	192.168.1.10	151.101.2.132	HTTP	543	GET /logos/res/incubator/default.png HTTP/1.1
356	2.228377205	151.101.2.132	192.168.1.10	HTTP	383	HTTP/1.1 304 Not Modified
379	2.234100131	151.101.2.132	192.168.1.10	HTTP	1395	HTTP/1.1 200 OK (PNG)
395	2.240982463	151.101.2.132	192.168.1.10	HTTP	383	HTTP/1.1 304 Not Modified
398	2.270724712	151.101.2.132	192.168.1.10	HTTP	1949	HTTP/1.1 200 OK (PNG)
489	2.516506951	151.101.2.132	192.168.1.10	HTTP	1045	HTTP/1.1 200 OK (PNG)
516	2.834507407	151.101.2.132	192.168.1.10	HTTP	411	HTTP/1.1 304 Not Modified
546	2.864597476	192.168.1.10	142.250.182.174	HTTP	433	GET /adsense/search/async-ads.js HTTP/1.1
565	2.911584103	192.168.1.10	142.250.192.206	HTTP	446	GET /generate_204 HTTP/1.1
575	2.926351765	142.250.192.206	192.168.1.10	HTTP	149	HTTP/1.1 204 No Content

(c) Total time: time when the last content object was received – time of the first DNS request



637	2.964469206	192.168.1.10	172.217.167.225	TLSv1.3	101	Application Data
640	2.973338346	172.217.167.214	192.168.1.10	TCP	66	443 → 44038 [ACK] Seq=5690 Ack=1228 Win=67840 Len=0 TSval=3046392226 TSecr=24142…
641	2.978295254	172.217.167.225	192.168.1.10	TCP	66	443 → 38802 [ACK] Seq=8376 Ack=1293 Win=67840 Len=0 TSval=1376790256 TSecr=20702…
642	2.982538931	172.217.167.214	192.168.1.10	TCP	66	443 → 44038 [ACK] Seq=5690 Ack=1263 Win=67840 Len=0 TSval=3046392235 TSecr=24142…
680	3.149627061	192.168.1.10	31.184.209.78	TCP	66	53076 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3931728589 TSecr=2309664627
696	3.195738894	192.168.1.10	151.101.2.132	HTTP	531	GET /favicons/favicon.ico HTTP/1.1
697	3.213695193	192.168.1.10	31.184.209.78	TCP	66	53074 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3931728653 TSecr=2309664685
701	3.261438709	151.101.2.132	192.168.1.10	TCP	66	80 → 55490 [ACK] Seq=346 Ack=871 Win=146944 Len=0 TSval=3123130671 TSecr=3162774…
702	3.262055583	151.101.2.132	192.168.1.10	HTTP	405	HTTP/1.1 304 Not Modified
703	3.262064693	192.168.1.10	151.101.2.132	TCP	66	55490 → 80 [ACK] Seq=871 Ack=685 Win=63872 Len=0 TSval=3162774934 TSecr=3123130672

: 3.2620 – 1.7887 = 1.4733sec

(d) There is no HTTP packet. (this website follows HTTPS protocol)

HTTPS means that the content is encrypted. As Wireshark can not decrypt the content, the used protocol inside the TLS connection is unknown to Wireshark - it can be HTTP or any other protocol. Therefore they are displayed as TLSv1.2/TCP. Only the ports indicate that most likely it is HTTPS traffic.

3.) Traceroute Implementation

```
sudo python3 main.py www.google.com
traceroute to www.google.com (142.250.193.228), 60 hops max
1       192.168.1.1                     1.749 ms
2       100.66.0.1                      4.771 ms
3       192.168.241.38                  6.13 ms
4       192.168.241.37                  7.421 ms
5       192.168.252.17                  5.861 ms
6       192.168.200.2                   10.325 ms
7       103.41.23.97                    16.985 ms
8       74.125.244.193                  16.744 ms
9       142.251.54.99                   17.09 ms
10      142.250.193.228                 16.732 ms
```