Exercise

The website investigated is https://www.readmyblog.co.uk/

For this exercise, I chose to use traceroute, and WHOIS for good measure.

The outputs of tools used are presented below.

`traceroute`:

```
shan@shan-Virtual-Machine:~$ traceroute www.readmyblog.co.uk
traceroute to www.readmyblog.co.uk (68.66.247.187), 30 hops max, 60 byte packets
 1  DESKTOP-3LC07Q9.mshome.net (172.24.112.1)  0.187 ms  0.171 ms  0.167 ms
 2  myhome.mynet (192.168.1.1)  2.371 ms  2.362 ms  2.355 ms
 3  100.97.202.65 (100.97.202.65)  10.406 ms  10.397 ms  10.389 ms
 4  172.17.8.22 (172.17.8.22)  4.261 ms  4.609 ms  4.696 ms
 5  172.17.60.180 (172.17.60.180)  10.374 ms  7.411 ms  10.353 ms
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  172.17.16.13 (172.17.16.13)  9.487 ms  9.479 ms  9.799 ms
11  ae62.mcs1.lhr15.uk.zip.zayo.com (94.31.42.137)  7.344 ms  5.381 ms  4.141 ms
12  * * ae1.cs1.lhr15.uk.eth.zayo.com (64.125.29.128)  5.360 ms
13  ae3.mpr1.lhr15.uk.zip.zayo.com (64.125.28.151)  3.609 ms  3.804 ms  5.336 ms
14  be3108.rcr21.b023101-0.lon13.atlas.cogentco.com (130.117.15.181)  5.296 ms
7.812 ms  5.281 ms
15  be2350.ccr42.lon13.atlas.cogentco.com (130.117.51.137)  5.635 ms
be2348.ccr41.lon13.atlas.cogentco.com (130.117.51.73)  4.928 ms  5.182 ms
16  be12194.ccr41.ams03.atlas.cogentco.com (154.54.56.94)  12.528 ms  14.555 ms
be12488.ccr42.ams03.atlas.cogentco.com (130.117.51.42)  12.090 ms
17  be2283.rcr21.b038092-0.ams03.atlas.cogentco.com (130.117.51.14)  14.247 ms
14.519 ms be2278.rcr21.b038092-0.ams03.atlas.cogentco.com (130.117.50.250)  14.328
ms
18  euroaccess-ltd.demarc.cogentco.com (149.6.128.82)  13.131 ms  14.655 ms
14.648 ms
19  v402.R2.NL1.a2webhosting.com (209.124.94.239)  14.606 ms  14.383 ms  14.350 ms
20  68.66.247.187.static.a2webhosting.com (68.66.247.187)  13.921 ms  10.715 ms
9.907 ms
```

`ping`:

```
shan@shan-Virtual-Machine:~$ ping www.readmyblog.co.uk
PING readmyblog.co.uk (68.66.247.187) 56(84) bytes of data.
64 bytes from 68.66.247.187.static.a2webhosting.com (68.66.247.187): icmp_seq=1
ttl=248 time=9.53 ms
64 bytes from 68.66.247.187.static.a2webhosting.com (68.66.247.187): icmp_seq=2
ttl=248 time=9.62 ms
64 bytes from 68.66.247.187.static.a2webhosting.com (68.66.247.187): icmp_seq=3
ttl=248 time=9.84 ms
```

```
64 bytes from 68.66.247.187.static.a2webhosting.com (68.66.247.187): icmp_seq=4
ttl=248 time=13.6 ms
64 bytes from 68.66.247.187.static.a2webhosting.com (68.66.247.187): icmp_seq=5
ttl=248 time=9.49 ms
```

Question: How many hops from your machine to your assigned website?

Based on the output of `ping`, we know that the destination is 68.66.247.187.static.a2webhosting.com. The amount of hops it took to reach this site, according to the `traceroute` output, is 20. Asterisks are also routers, however, details cannot be given about them because they did not respond to the packets in time.

Question: Which step causes the biggest delay in the route? What is the average duration of that delay?

The 17th step took the longest. `traceroute` displays the round-trip time for each packet, and by default, `traceroute` sends 3 packets. The average duration of the delay is therefore the average of the 3 round-trips (14.247ms, 14.519ms, and 14.328ms), which is 14.37ms.

```
17 be2283.rcr21.b038092-0.ams03.atlas.cogentco.com (130.117.51.14) 14.247 ms 14.519 ms
be2278.rcr21.b038092-0.ams03.atlas.cogentco.com (130.117.50.250) 14.328 ms
```

Question: What are the main nameservers for the website?

According to the output of the `host` command, these are the main servers:

```
shan@shan-Virtual-Machine:~$ host -t ns readmyblog.co.uk
readmyblog.co.uk name server ns1.a2hosting.com.
readmyblog.co.uk name server ns4.a2hosting.com.
readmyblog.co.uk name server ns2.a2hosting.com.
readmyblog.co.uk name server ns3.a2hosting.com.
```

This can also be verified by using the `whois` command:

```
shan@shan-Virtual-Machine:~$ whois whois readmyblog.co.uk

    Domain name:
        readmyblog.co.uk

    Data validation:
        Nominet was not able to match the registrant's name and/or address against
a 3rd party source on 21-Oct-2021

    Registrar:
        eNom LLC [Tag = ENOM]
        URL: http://www.enom.com

    Relevant dates:
        Registered on: 21-Oct-2021
```

```
        Expiry date:  21-Oct-2022
        Last updated:  21-Oct-2021

    Registration status:
        Registered until expiry date.

    Name servers:
        ns1.a2hosting.com
        ns2.a2hosting.com
        ns3.a2hosting.com
        ns4.a2hosting.com

    WHOIS lookup made at 17:01:12 19-Feb-2022

--
This WHOIS information is provided for free by Nominet UK the central registry
for .uk domain names. This information and the .uk WHOIS are:

    Copyright Nominet UK 1996 - 2022.

You may not access the .uk WHOIS or use any data from it except as permitted
by the terms of use available in full at https://www.nominet.uk/whoisterms,
which includes restrictions on: (A) use of the data for advertising, or its
repackaging, recompilation, redistribution or reuse (B) obscuring, removing
or hiding any or all of this notice and (C) exceeding query rate or volume
limits. The data is provided on an 'as-is' basis and may lag behind the
register. Access may be withdrawn or restricted at any time.
```

Question: Who is the registered contact?

According to the output of the `whois` command, it is eNOM.

Question: What is the MX record for the website?

```
shan@shan-Virtual-Machine:~$ dig readmybog.co.uk MX

; <<>> DiG 9.17.19-3-Debian <<>> readmybog.co.uk MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 45874
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;readmybog.co.uk.               IN      MX

;; Query time: 8 msec
;; SERVER: 172.29.208.1#53(172.29.208.1) (UDP)
;; WHEN: Sat Feb 19 17:03:58 GMT 2022
;; MSG SIZE  rcvd: 44
```

Where is the website hosted?

The Netherlands, although the domain is in the United Kingdom. Using https://ipinfo.io/, I checked the IP of the website (which I obtained from `ping`), and obtained the following results:

```
ip: "68.66.247.187"
hostname: "68.66.247.187.static.a2webhosting.com"
city: "Amsterdam"
region: "North Holland"
country: "NL"
loc: "52.3740,4.8897"
org: "AS55293 A2 Hosting, Inc."
postal: "1012"
timezone: "Europe/Amsterdam"
asn: Object
asn: "AS55293"
name: "A2 Hosting, Inc."
domain: "a2hosting.com"
route: "68.66.240.0/20"
type: "hosting"
company: Object
name: "A2 Hosting, Inc."
domain: "a2hosting.com"
type: "hosting"
privacy: Object
vpn: false
proxy: false
tor: false
relay: false
hosting: true
service: ""
abuse: Object
address: "US, MI, Ann Arbor, P.O. Box 2998, 48106"
country: "US"
email: "abuse@a2hosting.com"
name: "Network Operations"
network: "68.66.212.0-68.66.255.255"
phone: "+1-734-222-4678"
domains: Object
ip: "68.66.247.187"
total: 2
domains: Array
0: "tech-sourcery.co.uk"
1: "daedalus-systems.co.uk"
```

Bibliography

Mrozek, M. (2010) How to interpret traceroute information? Available from: https://unix.stackexchange.com/questions/1023/how-to-interpret-traceroute-information [Accessed 19

February 2022].
Ramesh. (2014) traceroute gives only stars + how to fix. Available from: https://unix.stackexchange.com/questions/127002/traceroute-gives-only-stars-how-to-fix [Accessed 19 February 2022].
Timofey. (2013) What does an asterisk/star in traceroute mean? Available from: https://webmasters.stackexchange.com/questions/17793/what-does-an-asterisk-star-in-traceroute-mean [Accessed 19 February 2022].