Practical Activity

Scanning Exercise

How many hops from your machine to your assigned website?

```
traceroute to next.anrichp.com (194.163.132.235), 30 hops max, 60 byte packets
 1  DESKTOP-5IUQR7U.mshome.net (172.27.224.1)  0.264 ms  0.232 ms  0.222 ms
 2  192.168.1.1 (192.168.1.1)  0.729 ms  1.056 ms  1.304 ms
 3  * * *
 4  10.248.29.57 (10.248.29.57)  27.686 ms  27.480 ms  27.526 ms
 5  10.247.85.27 (10.247.85.27)  24.227 ms  19.500 ms  27.461 ms
 6  * * *
 7  10.247.85.9 (10.247.85.9)  24.660 ms  28.781 ms  28.765 ms
 8  10.247.85.18 (10.247.85.18)  34.667 ms  26.848 ms  26.799 ms
 9  87.237.20.220 (87.237.20.220)  30.269 ms  18.710 ms  26.818 ms
10  87.237.20.69 (87.237.20.69)  23.683 ms  30.280 ms  33.394 ms
11  * * *
12  ae-2-3207.edge6.Dusseldorf1.Level3.net (4.69.161.198)  41.900 ms  41.890 ms  38.087 ms
13  GIGA-HOSTIN.edge6.Dusseldorf1.Level3.net (62.67.22.194)  34.347 ms  41.258 ms  34.517 ms
14  vmi592253.contaboserver.net (194.163.132.235)  41.211 ms *  44.319 ms
```

Longest Delay

```
13  GIGA-HOSTIN.edge6.Dusseldorf1.Level3.net (62.67.22.194)  34.347 ms  41.258 ms  34.517 ms
14  vmi592253.contaboserver.net (194.163.132.235)  41.211 ms *  44.319 ms
```

The round trip time was the longest at the 14th hop taking an average time of 42.765 ms

What are the main nameservers for the website?

Command#: dig ns next.anrichp.com

```
;; AUTHORITY SECTION:
anrichp.com.            379     IN      SOA     dns1.registrar-servers.com. hostmaster.registrar-servers.com. 1621327238 43200 3600 604800 3601
```

Main ns: dns1.registrar-servers.com

Registered Contact

Command#: whois 194.163.132.235

```
person:          Wilhelm Zwalina
address:         Contabo GmbH
address:         Aschauer Str. 32a
address:         81549 Muenchen
phone:           +49 89 21268372
fax-no:          +49 89 21665862
nic-hdl:         MH7476-RIPE
mnt-by:          MNT-CONTABO
mnt-by:          MNT-GIGA-HOSTING
created:         2010-01-04T10:41:37Z
last-modified:   2020-04-24T16:09:30Z
source:          RIPE
```

What is the MX record for the website?

```
└─$ nslookup
> set type=mx
> anrichp.com
Server:         172.27.224.1
Address:        172.27.224.1#53

Non-authoritative answer:
anrichp.com     mail exchanger = 10 eforward1.registrar-servers.com.
anrichp.com     mail exchanger = 20 eforward5.registrar-servers.com.
anrichp.com     mail exchanger = 10 eforward3.registrar-servers.com.
anrichp.com     mail exchanger = 10 eforward2.registrar-servers.com.
anrichp.com     mail exchanger = 15 eforward4.registrar-servers.com.
Name:   a.gtld-servers.net
Address: 192.5.6.30
Name:   b.gtld-servers.net
Address: 192.33.14.30
Name:   c.gtld-servers.net
Address: 192.26.92.30
Name:   d.gtld-servers.net
Address: 192.31.80.30
Name:   e.gtld-servers.net
Address: 192.12.94.30
Name:   f.gtld-servers.net
Address: 192.35.51.30
```

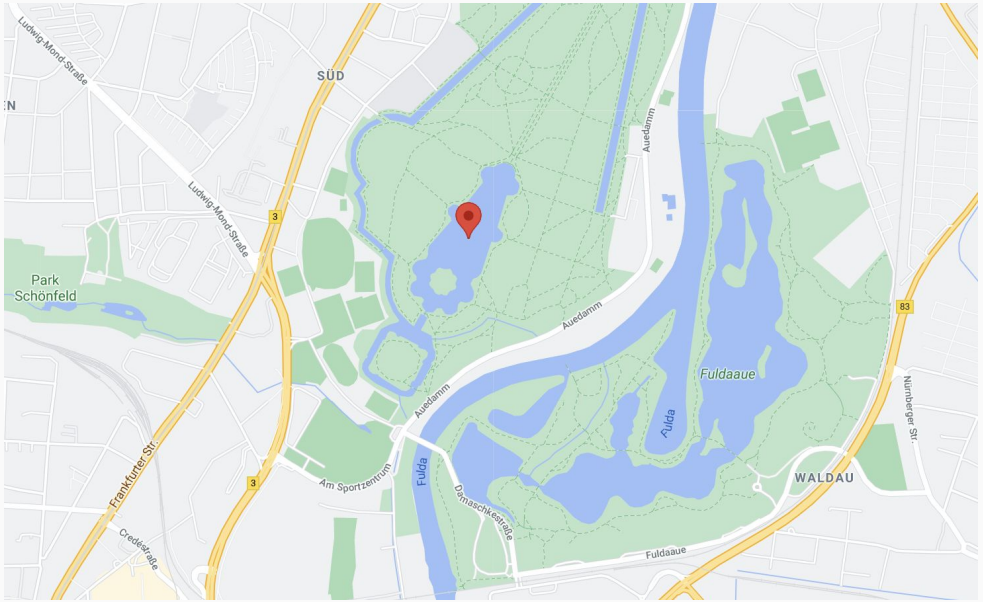
Where is the website hosted?

```
└─$ dig -x 194.163.132.235

; <<>> DiG 9.16.15-Debian <<>> -x 194.163.132.235
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7597
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;235.132.163.194.in-addr.arpa.  IN      PTR

;; ANSWER SECTION:
235.132.163.194.in-addr.arpa. 0 IN      PTR     vmi592253.contaboserver.net.

;; Query time: 590 msec
;; SERVER: 172.27.224.1#53(172.27.224.1)
;; WHEN: Wed May 26 18:44:29 BST 2021
;; MSG SIZE  rcvd: 115
```

Geolocation

```
└─$ nmap --script ip-geolocation-geoplugin 194.163.132.235
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-29 11:34 BST
Stats: 0:00:57 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 62.36% done; ETC: 11:35 (0:00:27 remaining)
Nmap scan report for 194.163.132.235
Host is up (0.043s latency).
Not shown: 991 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
443/tcp   open     https
5060/tcp  open     sip
8000/tcp  open     http-alt
8080/tcp  open     http-proxy
9000/tcp  open     cslistener
32772/tcp filtered sometimes-rpc7

Host script results:
| ip-geolocation-geoplugin: coordinates: 51.2993, 9.491
|_location: , Germany
```

Google Maps


Ludwig-Mond-Straße
SÜD
Ludwig-Mond-Straße
Auedamm
Park
Schönfeld
Auedamm
Fuldaaue
Auedamm
Fulda
Nürnberger Str.
Frankfurter Str.
Am Sportzentrum
Fulda
Damaschkestraße
WALDAU
Credéstraße
Fuldaaue
3
3
83