Scanning exercise

This exercise tasked us to use a variety of tools to scan a vulnerable website given by the tutor. The tools are commonly known as ‘Internet Protocol suite’ and are readily available or easily installed on Windows and Linux.

For the purpose of this task, I will use a virtualisation of Kali Linux on a Windows 11 laptop and the webpage is https://customersrus.co.uk.

The Internet Protocol suite tools are as follows:

Dig

Traceroute

Nslookup

Whois

Nmap

MTR

Limitations

Due to the nature of the vulnerable website sharing hosts with other webpages, using the PING utility and ICMP scans were not advised as it could cause interference.

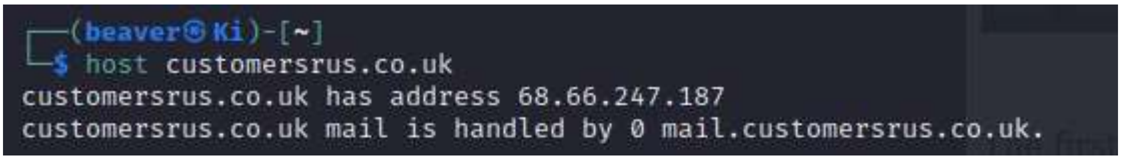
Task

Perform basic scans using basic tools such as traceroute (not ICMP version). Then answer the following questions:

- How many hops from your machine to your assigned website?
- Which step causes the biggest delay in the route? What is the average duration of that delay?
- What are the main nameservers for the website?
- Who is the registered contact?
- What is the MX record for the website?
- Where is the website hosted?

Basic scans

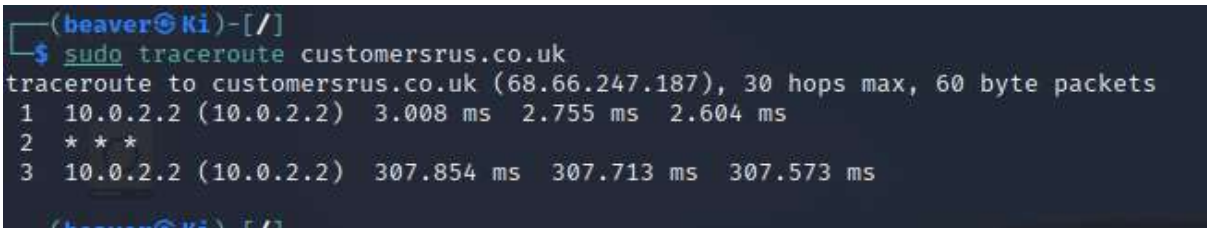
Finding the IP address



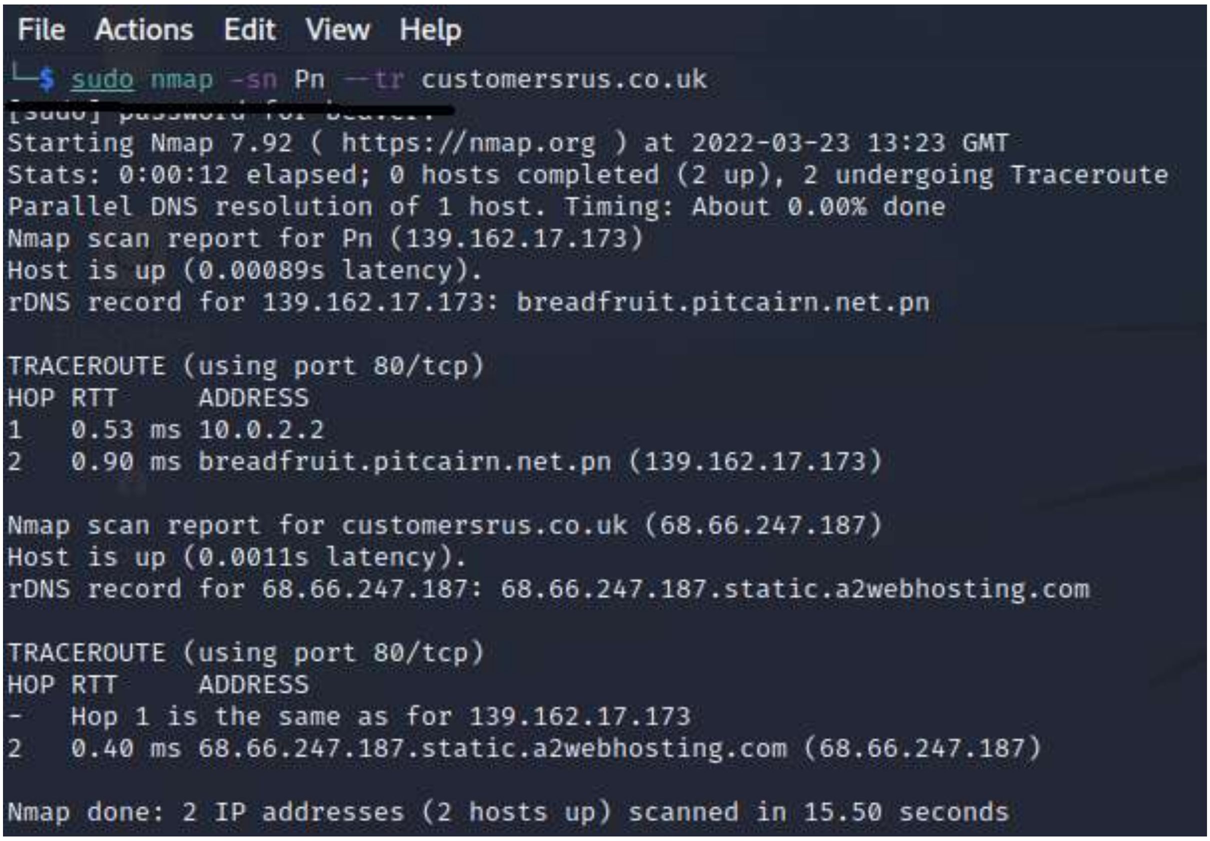
```
┌──(beaver㉿Ki)-[~]
└─$ host customersrus.co.uk
customersrus.co.uk has address 68.66.247.187
customersrus.co.uk mail is handled by 0 mail.customersrus.co.uk.
```

IP address is 68.66.247.187

1.How many hops from your machine to your assigned website?



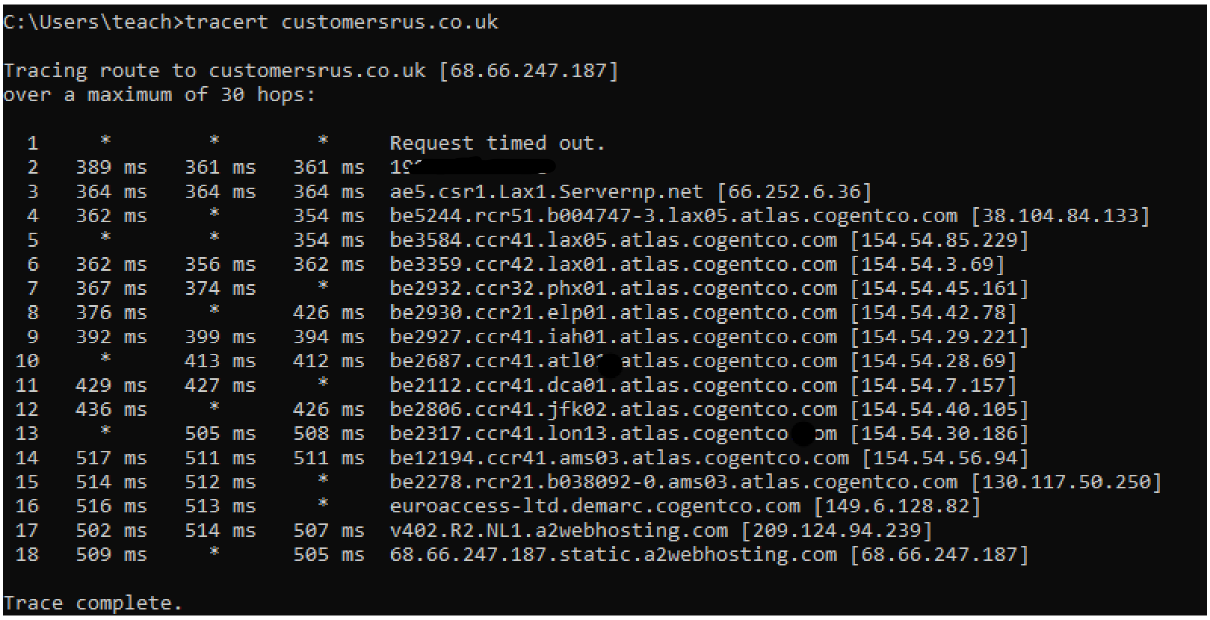
```
┌──(beaver㉿Ki)-[/]
└─$ sudo traceroute customersrus.co.uk
traceroute to customersrus.co.uk (68.66.247.187), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  3.008 ms  2.755 ms  2.604 ms
 2  * * *
 3  10.0.2.2 (10.0.2.2)  307.854 ms  307.713 ms  307.573 ms
```



```
└─$ sudo nmap -sn Pn --tr customersrus.co.uk
[redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 13:23 GMT
Stats: 0:00:12 elapsed; 0 hosts completed (2 up), 2 undergoing Traceroute
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for Pn (139.162.17.173)
Host is up (0.00089s latency).
rDNS record for 139.162.17.173: breadfruit.pitcairn.net.pn

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.53 ms 10.0.2.2
2   0.90 ms breadfruit.pitcairn.net.pn (139.162.17.173)

Nmap scan report for customersrus.co.uk (68.66.247.187)
Host is up (0.0011s latency).
rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 139.162.17.173
2   0.40 ms 68.66.247.187.static.a2webhosting.com (68.66.247.187)

Nmap done: 2 IP addresses (2 hosts up) scanned in 15.50 seconds
```

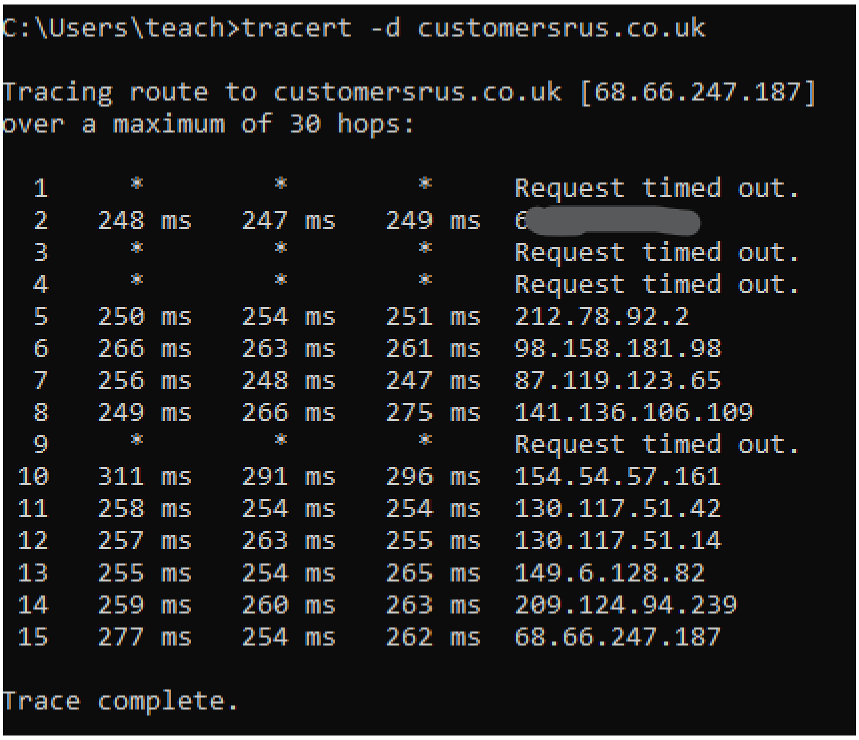
Here, I used options -sn (omits the default port scan), -Pn (avoids discovering the host), and -tr to trace all the hops.

It seems like one of the two hops goes through a VPN server in Singapore.



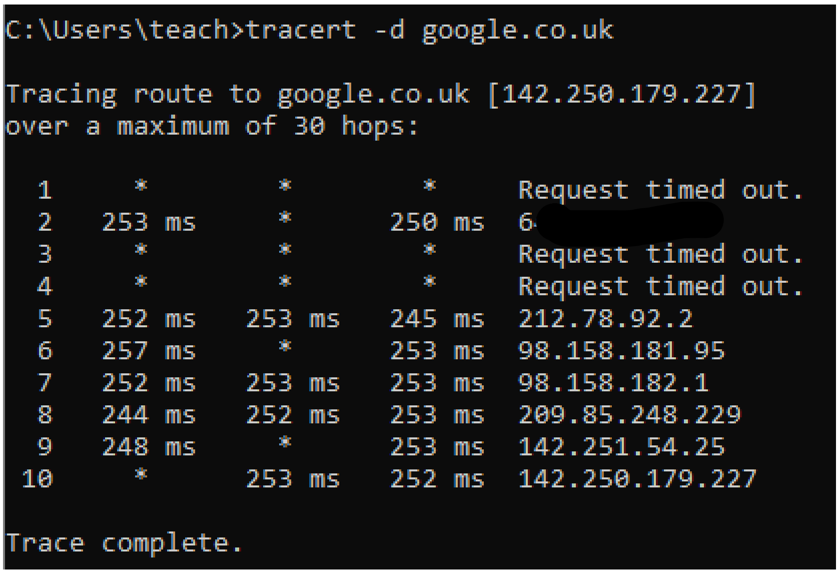
```
C:\Users\teach>tracert customersrus.co.uk

Tracing route to customersrus.co.uk [68.66.247.187]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2   389 ms   361 ms   361 ms  1[redacted]
  3   364 ms   364 ms   364 ms  ae5.csr1.Lax1.Servernp.net [66.252.6.36]
  4   362 ms     *      354 ms  be5244.rcr51.b004747-3.lax05.atlas.cogentco.com [38.104.84.133]
  5     *        *      354 ms  be3584.ccr41.lax05.atlas.cogentco.com [154.54.85.229]
  6   362 ms   356 ms   362 ms  be3359.ccr42.lax01.atlas.cogentco.com [154.54.3.69]
  7   367 ms   374 ms     *     be2932.ccr32.phx01.atlas.cogentco.com [154.54.45.161]
  8   376 ms     *      426 ms  be2930.ccr21.elp01.atlas.cogentco.com [154.54.42.78]
  9   392 ms   399 ms   394 ms  be2927.ccr41.iah01.atlas.cogentco.com [154.54.29.221]
 10     *      413 ms   412 ms  be2687.ccr41.atl0[redacted]atlas.cogentco.com [154.54.28.69]
 11   429 ms   427 ms     *     be2112.ccr41.dca01.atlas.cogentco.com [154.54.7.157]
 12   436 ms     *      426 ms  be2806.ccr41.jfk02.atlas.cogentco.com [154.54.40.105]
 13     *      505 ms   508 ms  be2317.ccr41.lon13.atlas.cogentco[redacted]om [154.54.30.186]
 14   517 ms   511 ms   511 ms  be12194.ccr41.ams03.atlas.cogentco.com [154.54.56.94]
 15   514 ms   512 ms     *     be2278.rcr21.b038092-0.ams03.atlas.cogentco.com [130.117.50.250]
 16   516 ms   513 ms     *     euroaccess-ltd.demarc.cogentco.com [149.6.128.82]
 17   502 ms   514 ms   507 ms  v402.R2.NL1.a2webhosting.com [209.124.94.239]
 18   509 ms     *      505 ms  68.66.247.187.static.a2webhosting.com [68.66.247.187]

Trace complete.
```

Tracecert on Windows seems to have 18 hops



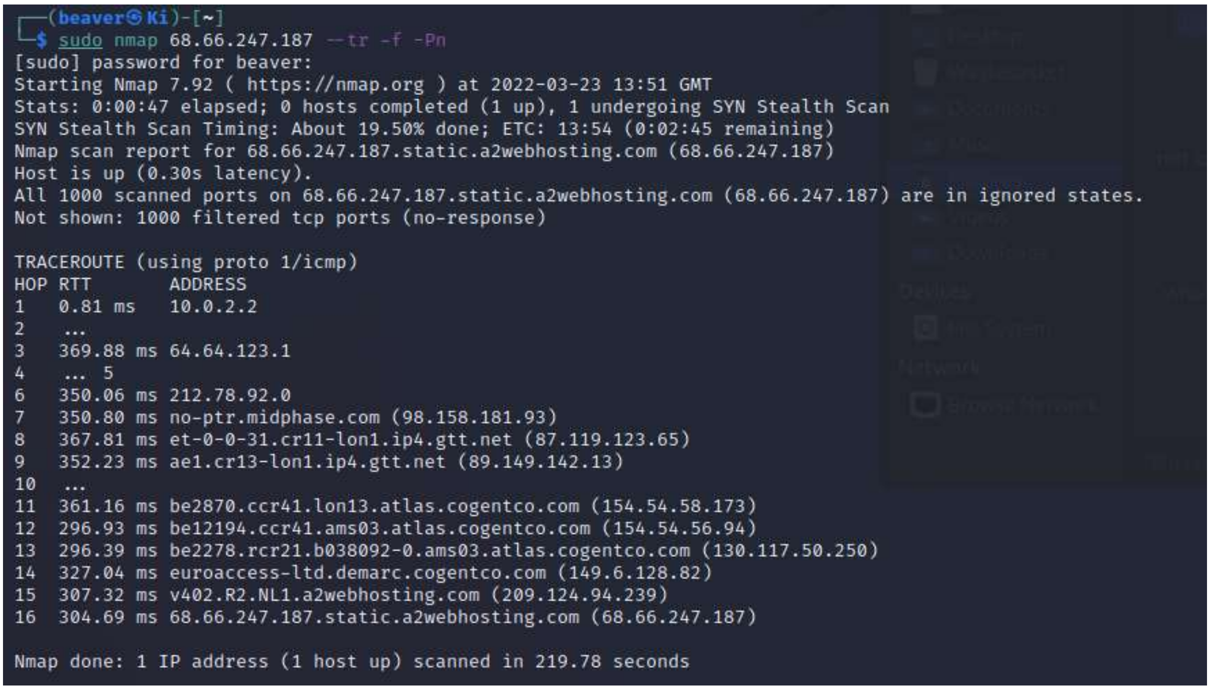
```
C:\Users\teach>tracert -d customersrus.co.uk

Tracing route to customersrus.co.uk [68.66.247.187]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2   248 ms   247 ms   249 ms  6[redacted]
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5   250 ms   254 ms   251 ms  212.78.92.2
  6   266 ms   263 ms   261 ms  98.158.181.98
  7   256 ms   248 ms   247 ms  87.119.123.65
  8   249 ms   266 ms   275 ms  141.136.106.109
  9     *        *        *     Request timed out.
 10   311 ms   291 ms   296 ms  154.54.57.161
 11   258 ms   254 ms   254 ms  130.117.51.42
 12   257 ms   263 ms   255 ms  130.117.51.14
 13   255 ms   254 ms   265 ms  149.6.128.82
 14   259 ms   260 ms   263 ms  209.124.94.239
 15   277 ms   254 ms   262 ms  68.66.247.187

Trace complete.
```

Using tracert -d prevented the hostname being resolved; there are now 15 hops and much quicker time. It seems the initial hope and time is due to connecting to the VPN server in the UK.



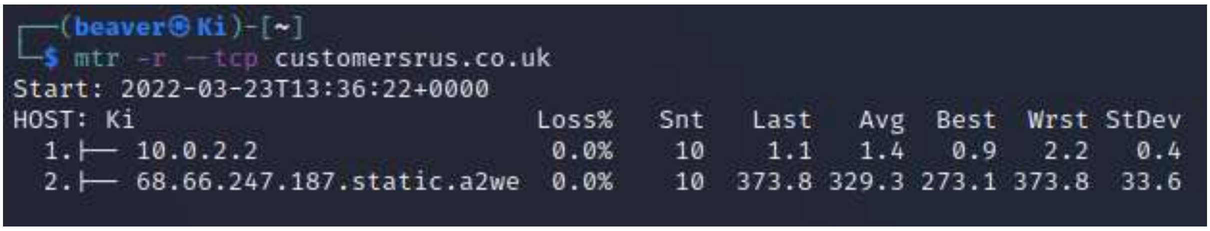
```
C:\Users\teach>tracert -d google.co.uk

Tracing route to google.co.uk [142.250.179.227]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2   253 ms     *      250 ms  6[redacted]
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5   252 ms   253 ms   245 ms  212.78.92.2
  6   257 ms     *      253 ms  98.158.181.95
  7   252 ms   253 ms   253 ms  98.158.182.1
  8   244 ms   252 ms   253 ms  209.85.248.229
  9   248 ms     *      253 ms  142.251.54.25
 10     *      253 ms   252 ms  142.250.179.227

Trace complete.
```

For comparison, using tracert -d on Google.co.uk returned 10 hops but still the time is long.



```
┌──(beaver㉿Ki)-[~]
└─$ sudo nmap 68.66.247.187 --tr -f -Pn
[sudo] password for beaver:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 13:51 GMT
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.50% done; ETC: 13:54 (0:02:45 remaining)
Nmap scan report for 68.66.247.187.static.a2webhosting.com (68.66.247.187)
Host is up (0.30s latency).
All 1000 scanned ports on 68.66.247.187.static.a2webhosting.com (68.66.247.187) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   0.81 ms   10.0.2.2
2   ...
3   369.88 ms 64.64.123.1
4   ... 5
6   350.06 ms 212.78.92.0
7   350.80 ms no-ptr.midphase.com (98.158.181.93)
8   367.81 ms et-0-0-31.cr11-lon1.ip4.gtt.net (87.119.123.65)
9   352.23 ms ae1.cr13-lon1.ip4.gtt.net (89.149.142.13)
10  ...
11  361.16 ms be2870.ccr41.lon13.atlas.cogentco.com (154.54.58.173)
12  296.93 ms be12194.ccr41.ams03.atlas.cogentco.com (154.54.56.94)
13  296.39 ms be2278.rcr21.b038092-0.ams03.atlas.cogentco.com (130.117.50.250)
14  327.04 ms euroaccess-ltd.demarc.cogentco.com (149.6.128.82)
15  307.32 ms v402.R2.NL1.a2webhosting.com (209.124.94.239)
16  304.69 ms 68.66.247.187.static.a2webhosting.com (68.66.247.187)

Nmap done: 1 IP address (1 host up) scanned in 219.78 seconds
```

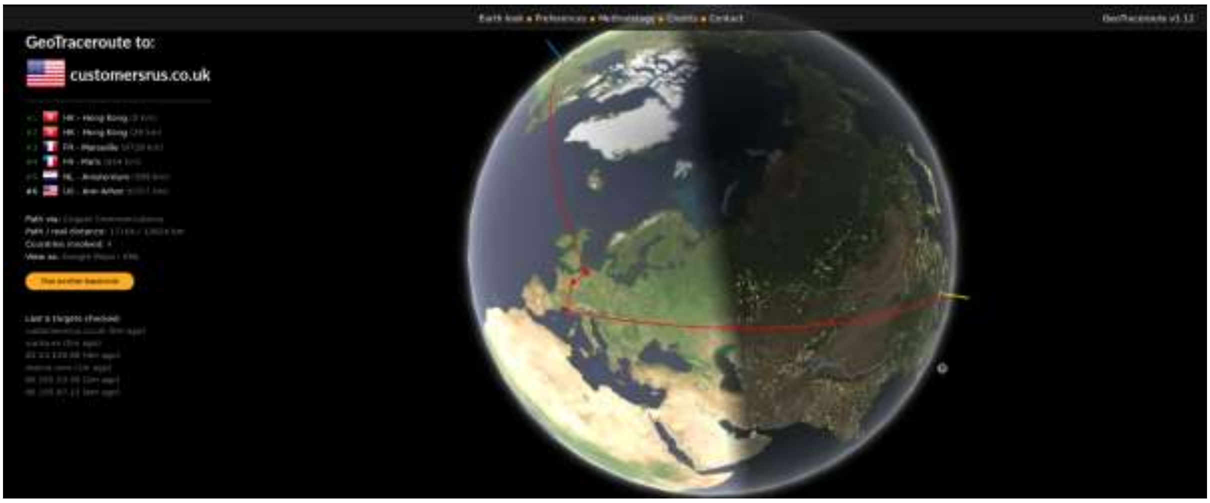
More hops on nmap using fast port scan



```
┌──(beaver㉿Ki)-[~]
└─$ mtr -r --tcp customersrus.co.uk
Start: 2022-03-23T13:36:22+0000
HOST: Ki                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 10.0.2.2                   0.0%    10    1.1   1.4   0.9   2.2   0.4
  2.|-- 68.66.247.187.static.a2we  0.0%    10  373.8 329.3 273.1 373.8  33.6
```

Only two hops using MTR TCP SYN instead of ICMP ECHO requests.

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



GeoTraceroute to:

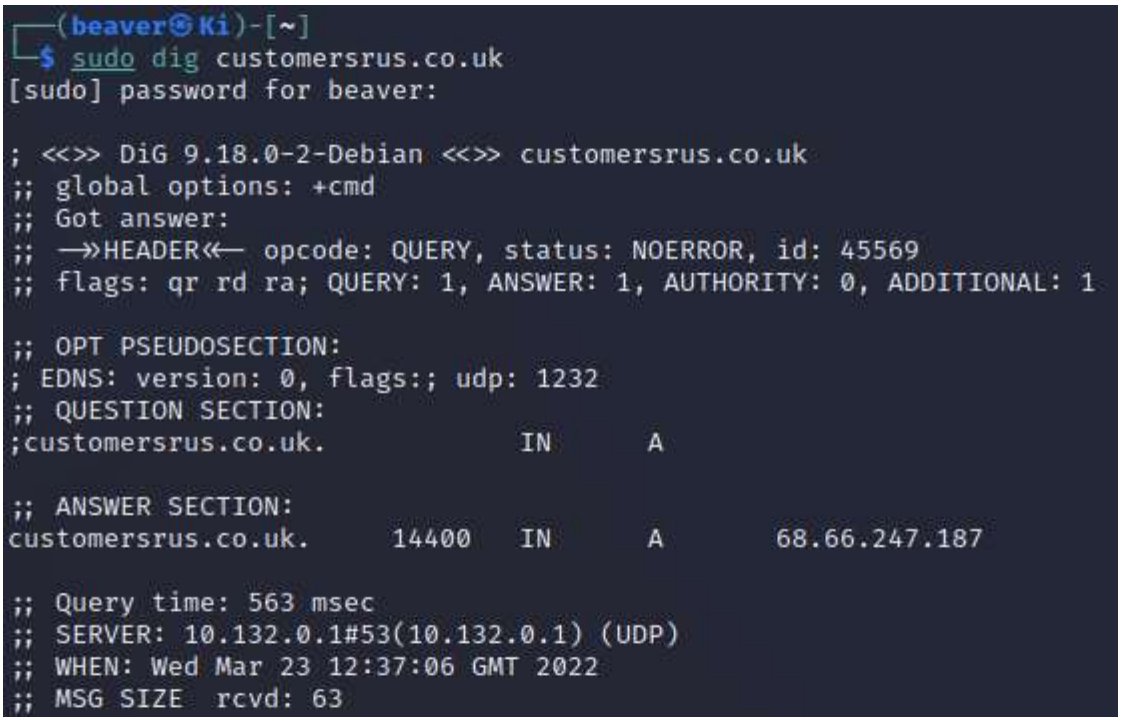
customersrus.co.uk

HK - Hong Kong
HK - Hong Kong
FR - Marseille
FR - Paris
NL - Amsterdam
#6 US - Ann Arbor

Path via:
Path / real distance:
Countries involved: 4
View as:

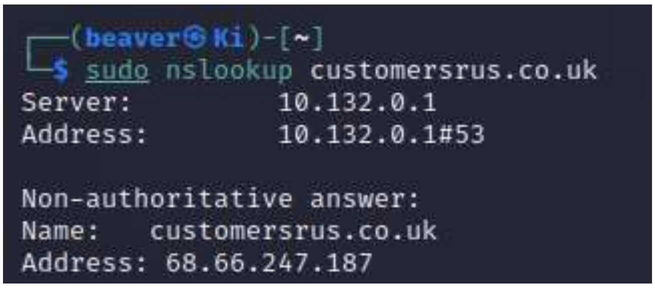
Hong Kong to France: hop 1 to 2

- What are the main nameservers for the website?



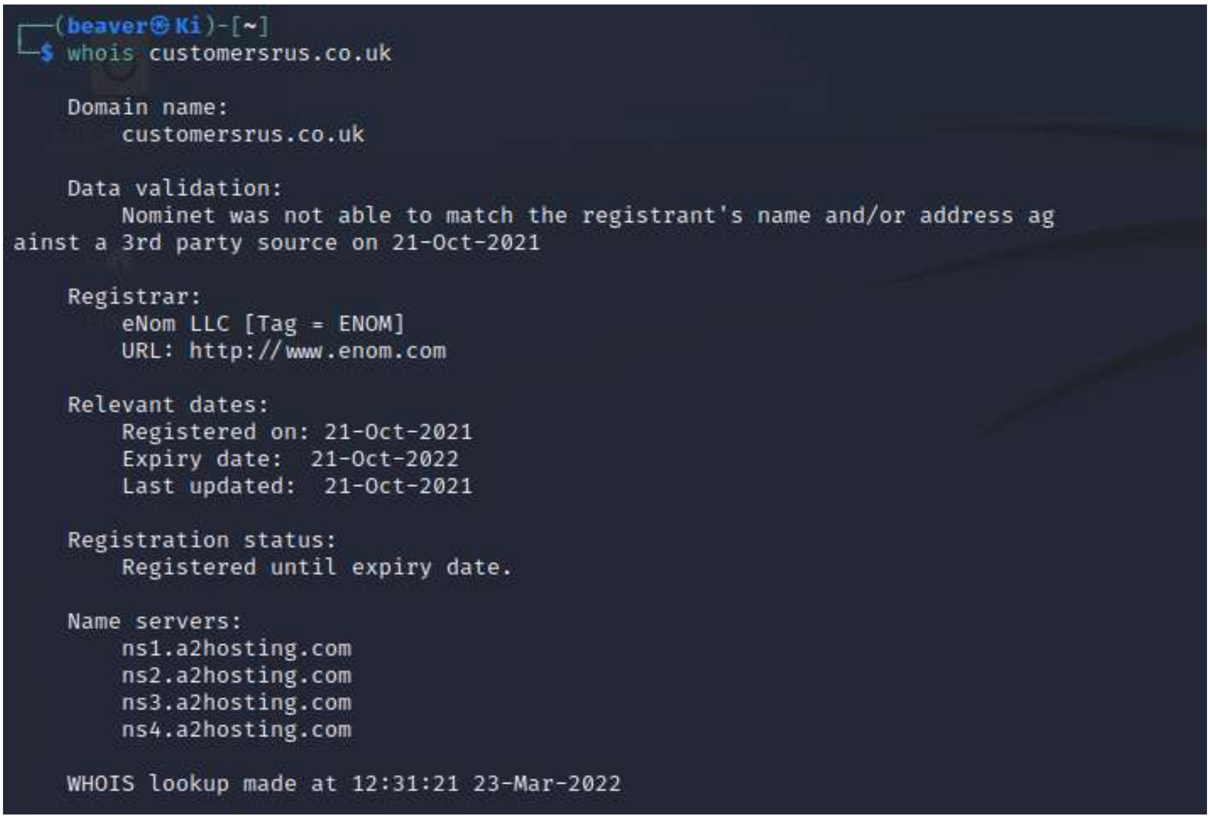
```
┌──(beaver㉿Ki)-[~]
└─$ sudo dig customersrus.co.uk
[sudo] password for beaver:

; <<>> DiG 9.18.0-2-Debian <<>> customersrus.co.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45569
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;customersrus.co.uk.            IN      A

;; ANSWER SECTION:
customersrus.co.uk.     14400   IN      A       68.66.247.187

;; Query time: 563 msec
;; SERVER: 10.132.0.1#53(10.132.0.1) (UDP)
;; WHEN: Wed Mar 23 12:37:06 GMT 2022
;; MSG SIZE  rcvd: 63
```

There seems to be only one IP address



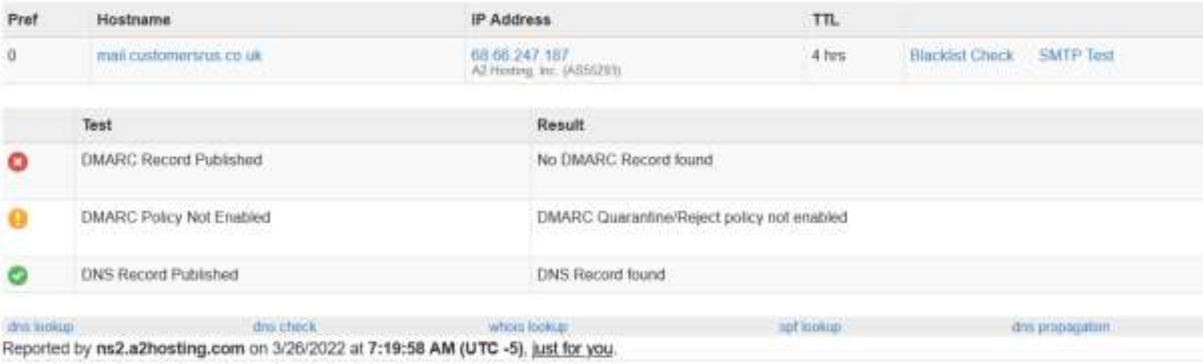
```
┌──(beaver㉿Ki)-[~]
└─$ sudo nslookup customersrus.co.uk
Server:         10.132.0.1
Address:        10.132.0.1#53

Non-authoritative answer:
Name:   customersrus.co.uk
Address: 68.66.247.187
```

- Who is the registered contact?



```
┌──(beaver㉿Ki)-[~]
└─$ whois customersrus.co.uk

    Domain name:
        customersrus.co.uk

    Data validation:
        Nominet was not able to match the registrant's name and/or address ag
ainst 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 12:31:21 23-Mar-2022
```

- What is the MX record for the website?

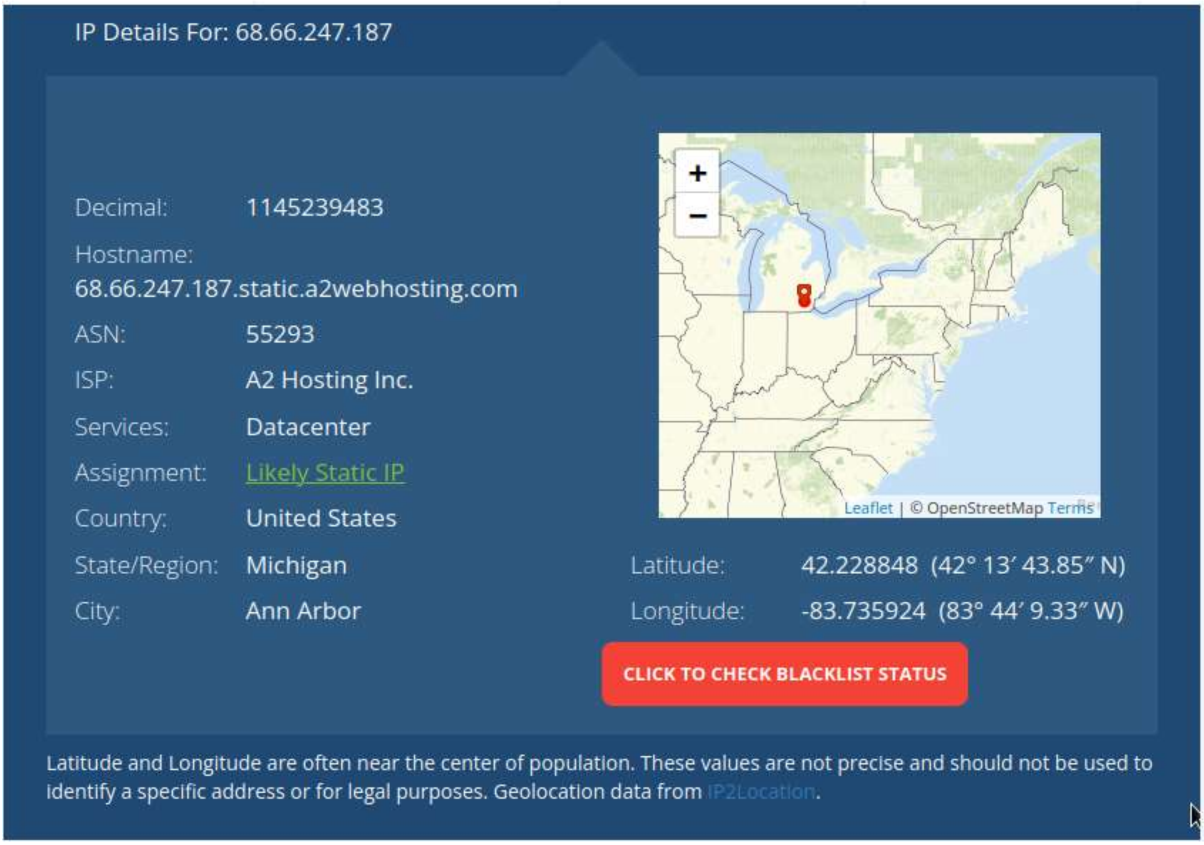


Pref	Hostname	IP Address	TTL		
0	mail.customersrus.co.uk	68.66.247.187 A2 Hosting, Inc. (AS55293)	4 hrs	Blacklist Check	SMTP Test

	Test	Result
✖	DMARC Record Published	No DMARC Record found
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
✓	DNS Record Published	DNS Record found

Reported by **ns2.a2hosting.com** on 3/26/2022 at **7:19:58 AM (UTC -5)**, just for you.

- Where is the website hosted?



IP Details For: 68.66.247.187

Decimal:	1145239483
Hostname:	68.66.247.187.static.a2webhosting.com
ASN:	55293
ISP:	A2 Hosting Inc.
Services:	Datacenter
Assignment:	Likely Static IP
Country:	United States
State/Region:	Michigan
City:	Ann Arbor

Latitude:	42.228848 (42° 13′ 43.85″ N)
Longitude:	-83.735924 (83° 44′ 9.33″ W)

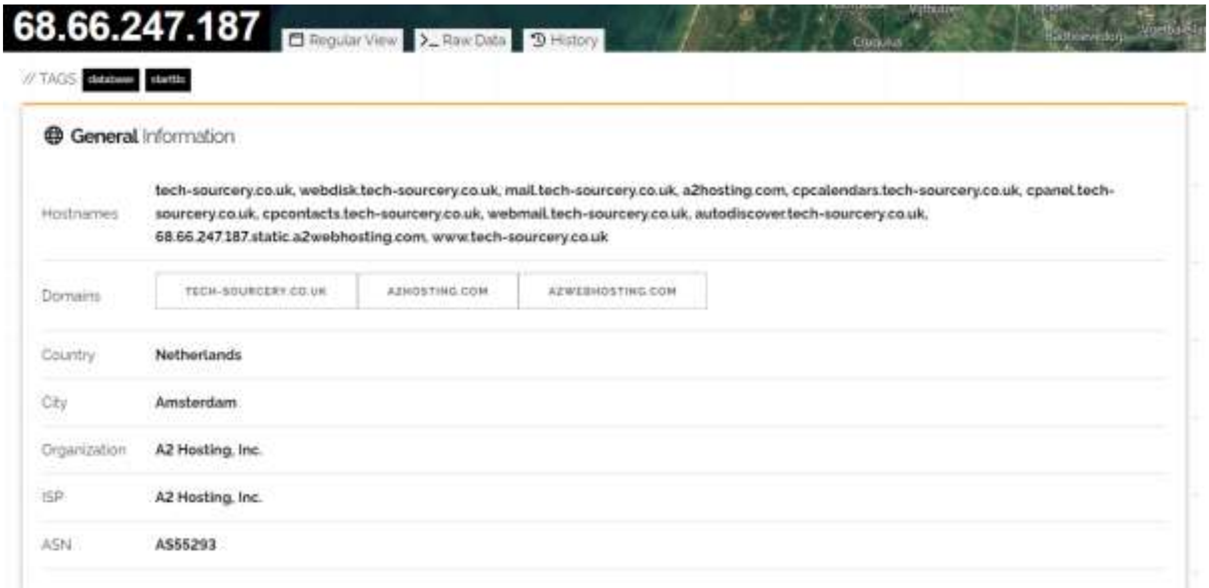
+
−
Leaflet | © OpenStreetMap Terms
CLICK TO CHECK BLACKLIST STATUS

Latitude and Longitude are often near the center of population. These values are not precise and should not be used to identify a specific address or for legal purposes. Geolocation data from IP2Location.

Further investigation

This made me curious about my initial findings as I originally stated Ann Arbor was the physical location. I returned to my scans and did some digging.

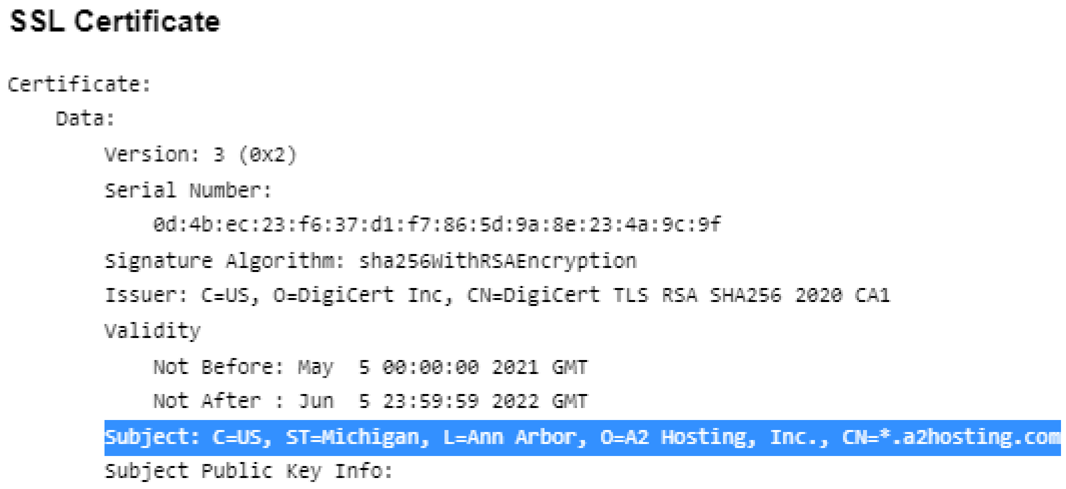
I now used Shodan (2022) and searched 66.66.24.187; it returned Amsterdam, Netherlands. It also showed which ports are open and what services are being used. Port 21 states that Pureftpd.org (FTP Unix server) is using it with an SSL certificate:



68.66.247.187

General Information

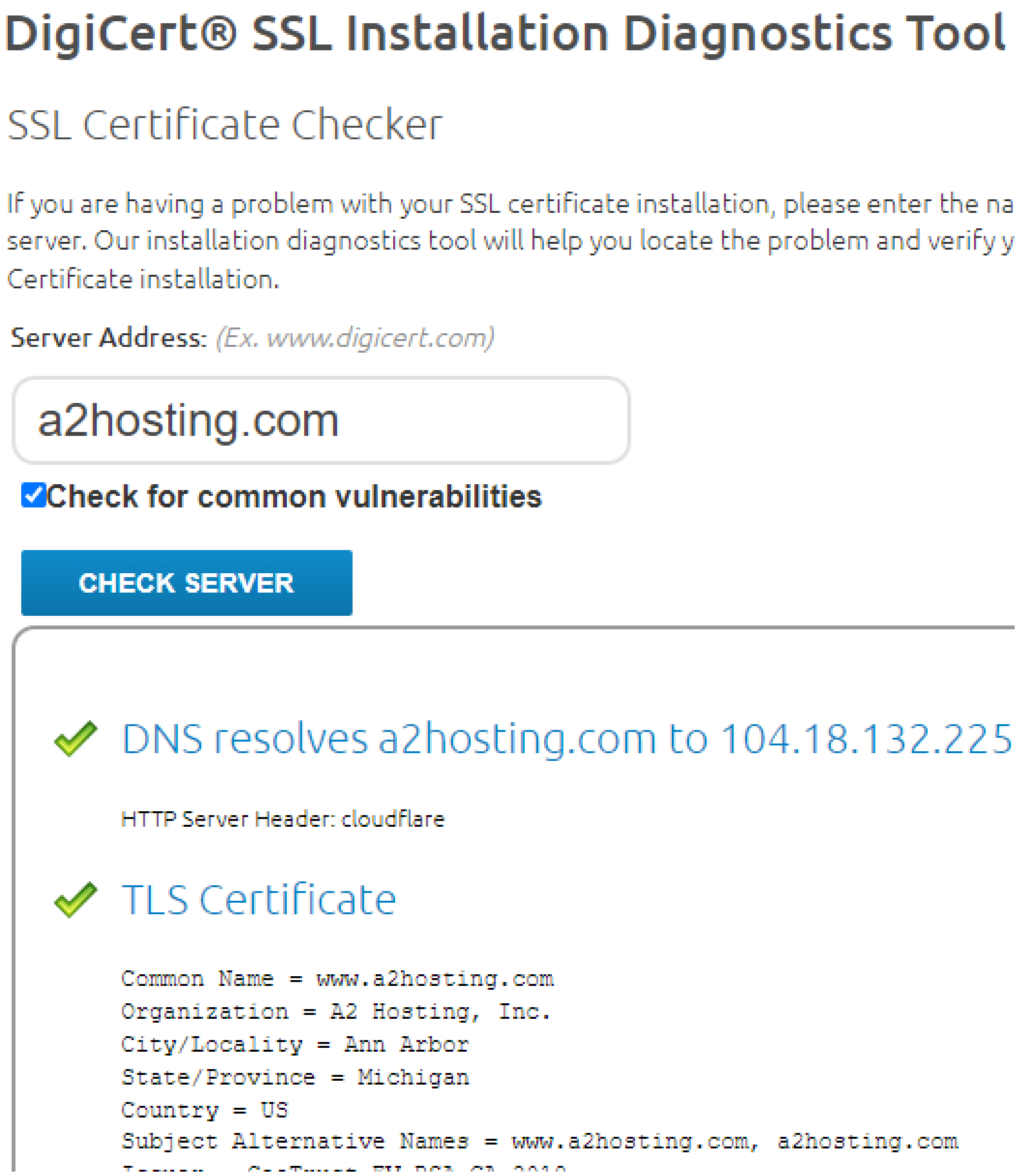
Hostnames	tech-sourcery.co.uk, webdisk.tech-sourcery.co.uk, mail.tech-sourcery.co.uk, a2hosting.com, cpcalendars.tech-sourcery.co.uk, cpanel.tech-sourcery.co.uk, cpcontacts.tech-sourcery.co.uk, webmail.tech-sourcery.co.uk, autodiscover.tech-sourcery.co.uk, 68.66.247.187.static.a2webhosting.com, www.tech-sourcery.co.uk
Domains	TECH-SOURCERY.CO.UK A2HOSTING.COM A2WEBHOSTING.COM
Country	Netherlands
City	Amsterdam
Organization	A2 Hosting, Inc.
ISP	A2 Hosting, Inc.
ASN	AS55293



SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0d:4b:ec:23:f6:37:d1:f7:86:5d:9a:8e:23:4a:9c:9f
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
        Validity
            Not Before: May  5 00:00:00 2021 GMT
            Not After : Jun  5 23:59:59 2022 GMT
        Subject: C=US, ST=Michigan, L=Ann Arbor, O=A2 Hosting, Inc., CN=*.a2hosting.com
        Subject Public Key Info:
```

The information also showed that the SSL certificate was issued by digicert, a digital security company. Using the digicert’s SSL Certificate Checker, I input the server address ‘a2hosting.com’, and it returned this information:



DigiCert® SSL Installation Diagnostics Tool

SSL Certificate Checker

If you are having a problem with your SSL certificate installation, please enter the na
server. Our installation diagnostics tool will help you locate the problem and verify y
Certificate installation.

Server Address: *(Ex. www.digicert.com)*

a2hosting.com

☑Check for common vulnerabilities

✓ DNS resolves a2hosting.com to 104.18.132.225

HTTP Server Header: cloudflare

✓ TLS Certificate

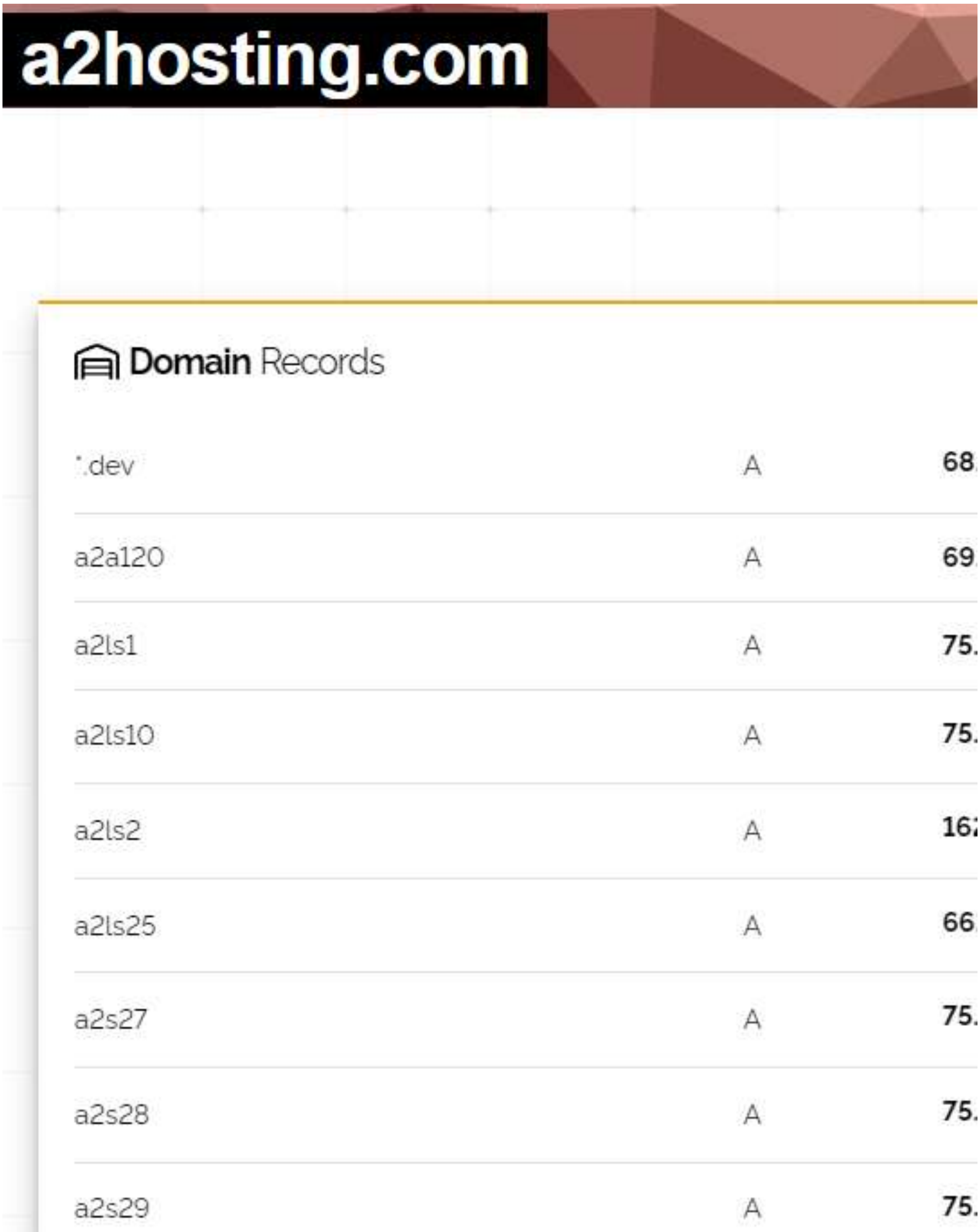
```
Common Name = www.a2hosting.com
Organization = A2 Hosting, Inc.
City/Locality = Ann Arbor
State/Province = Michigan
Country = US
Subject Alternative Names = www.a2hosting.com, a2hosting.com
```

Using Shodan again, I searched 104.18.132.225 which returned the following:

General *Information*

Hostnames	**a2hosting.com, www.a2hosting.com**
Domains	A2HOSTING.COM
Country	United States
City	San Francisco
Organization	Cloudflare, Inc.
ISP	Cloudflare, Inc.
ASN	AS13335

Using Shodan again, I searched A2hosting.com domain records, and it listed hundreds of domains and IP addresses.

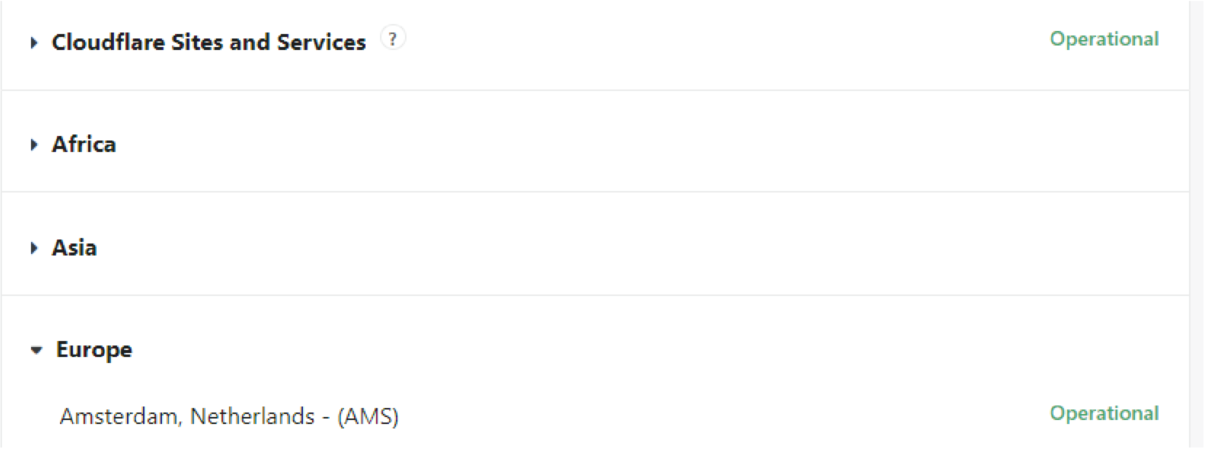


a2hosting.com

Domain Records

*.dev	A	68.
a2a120	A	69.
a2ls1	A	75.
a2ls10	A	75.
a2ls2	A	16
a2ls25	A	66.
a2s27	A	75.
a2s28	A	75.
a2s29	A	75.

CloudFlare (2022) is a Content Delivery Network (CDN), networking, firewall provider which helps entities to cache files in edge locations globally. Interestingly, I used their Cloud flare system status page, and they have an operational data centre in Amsterdam. This makes sense to have cache files near the website/server.



▸ Cloudflare Sites and Services ? Operational

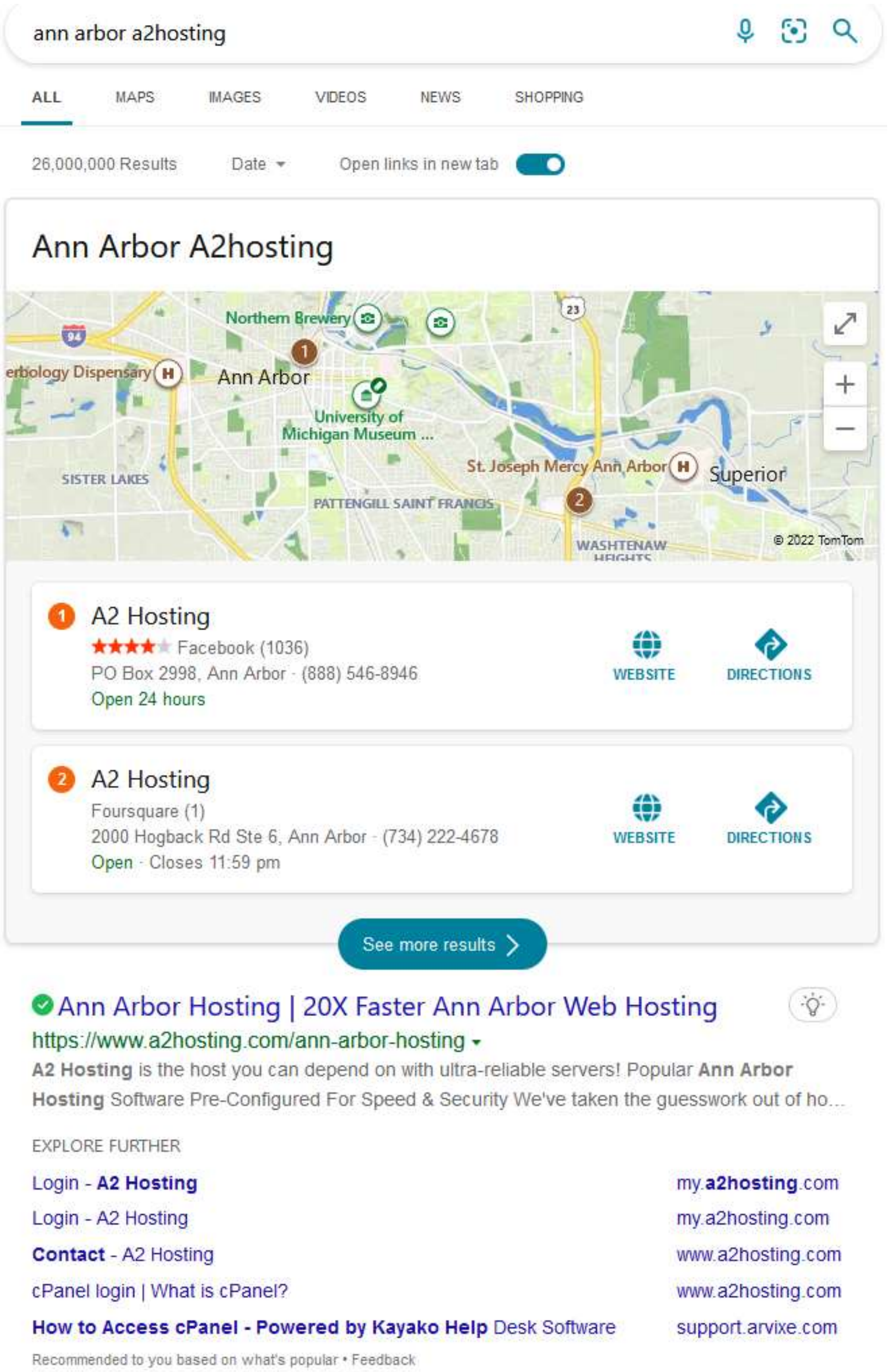
▸ Africa

▸ Asia

▾ Europe

Amsterdam, Netherlands - (AMS) Operational

Next, I searched ‘A2hosting.com Ann Arbor’ and found their PO Box address, website, telephone, Facebook, and LinkedIn information.



26,000,000 Results · Date · Open links in new tab

Ann Arbor A2hosting

1 A2 Hosting
★★★★☆ Facebook (1036)
PO Box 2998, Ann Arbor · (888) 546-8946
Open 24 hours
WEBSITE DIRECTIONS

2 A2 Hosting
Foursquare (1)
2000 Hogback Rd Ste 6, Ann Arbor · (734) 222-4678
Open · Closes 11:59 pm
WEBSITE DIRECTIONS

See more results >

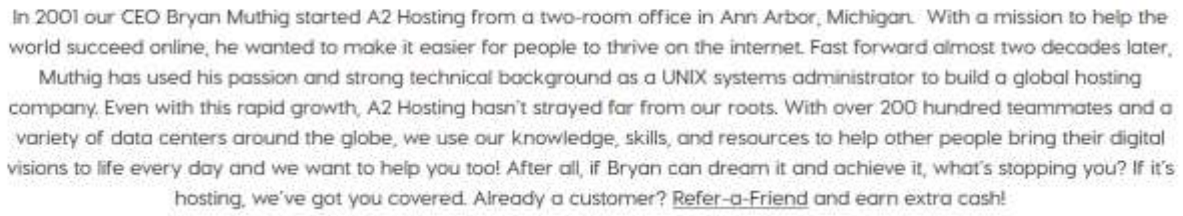
Ann Arbor Hosting | 20X Faster Ann Arbor Web Hosting
https://www.a2hosting.com/ann-arbor-hosting
A2 Hosting is the host you can depend on with ultra-reliable servers! Popular **Ann Arbor Hosting** Software Pre-Configured For Speed & Security We've taken the guesswork out of ho…

EXPLORE FURTHER

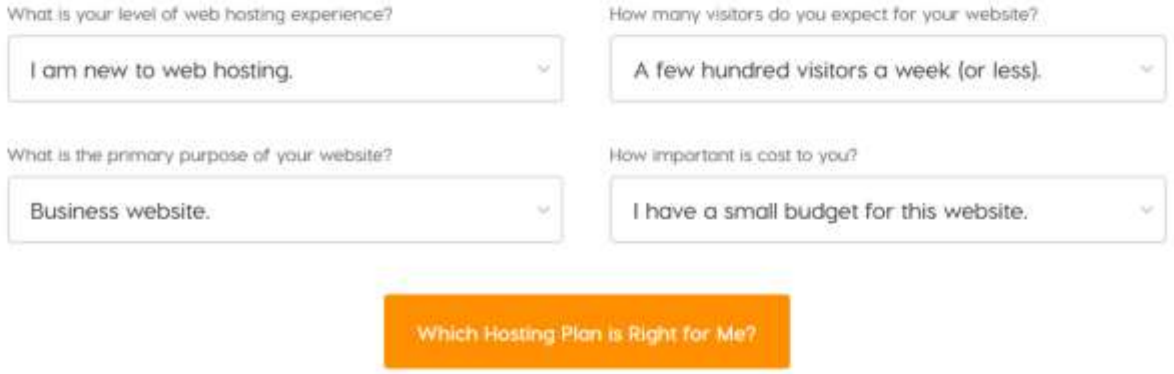
Login - **A2 Hosting**	my.**a2hosting**.com
Login - A2 Hosting	my.a2hosting.com
Contact - A2 Hosting	www.a2hosting.com
cPanel login | What is cPanel?	www.a2hosting.com
How to Access cPanel - Powered by Kayako Help Desk Software	support.arvixe.com

Recommended to you based on what's popular • Feedback

Amazingly, A2hosting is named after Ann Arbor (Ax2) and has existed since 2001.


In 2001 our CEO Bryan Muthig started A2 Hosting from a two-room office in Ann Arbor, Michigan. With a mission to help the world succeed online, he wanted to make it easier for people to thrive on the internet. Fast forward almost two decades later, Muthig has used his passion and strong technical background as a UNIX systems administrator to build a global hosting company. Even with this rapid growth, A2 Hosting hasn't strayed far from our roots. With over 200 hundred teammates and a variety of data centers around the globe, we use our knowledge, skills, and resources to help other people bring their digital visions to life every day and we want to help you too! After all, if Bryan can dream it and achieve it, what's stopping you? If it's hosting, we've got you covered. Already a customer? Refer-a-Friend and earn extra cash!

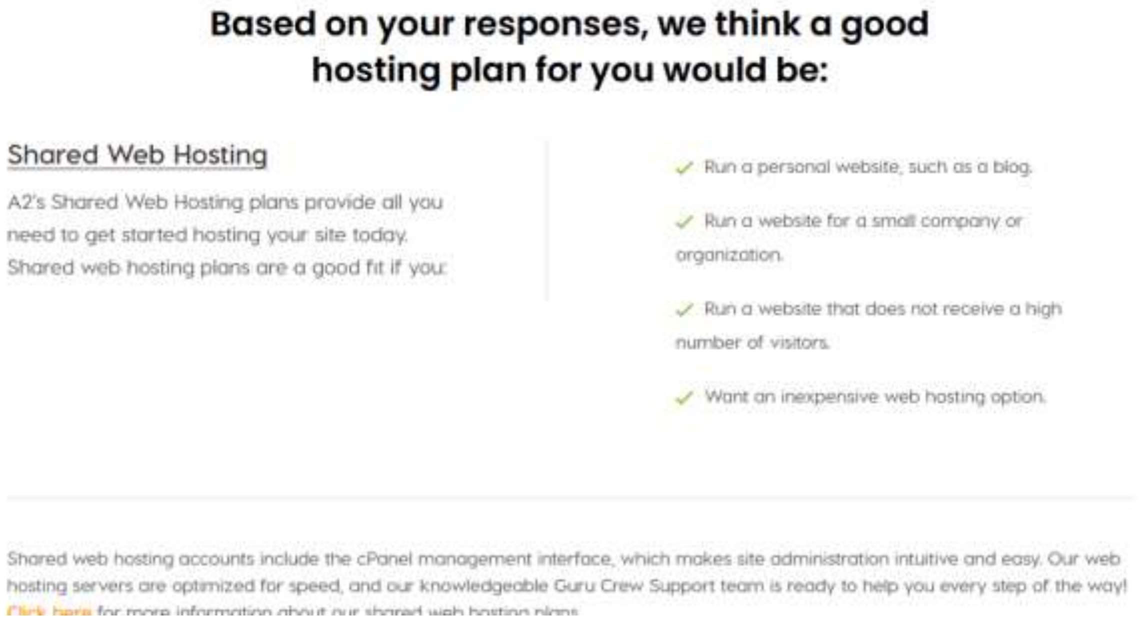
I used their 'hosting is it right for you' tool to see if I could mimic 'customersrus.co.uk' business 'needs'. I selected:


What is your level of web hosting experience? I am new to web hosting.

How many visitors do you expect for your website? A few hundred visitors a week (or less).

What is the primary purpose of your website? Business website.

How important is cost to you? I have a small budget for this website.


Based on your responses, we think a good hosting plan for you would be:

Shared Web Hosting

A2's Shared Web Hosting plans provide all you need to get started hosting your site today. Shared web hosting plans are a good fit if you:

- ✓ Run a personal website, such as a blog.
- ✓ Run a website for a small company or organization.
- ✓ Run a website that does not receive a high number of visitors.
- ✓ Want an inexpensive web hosting option.

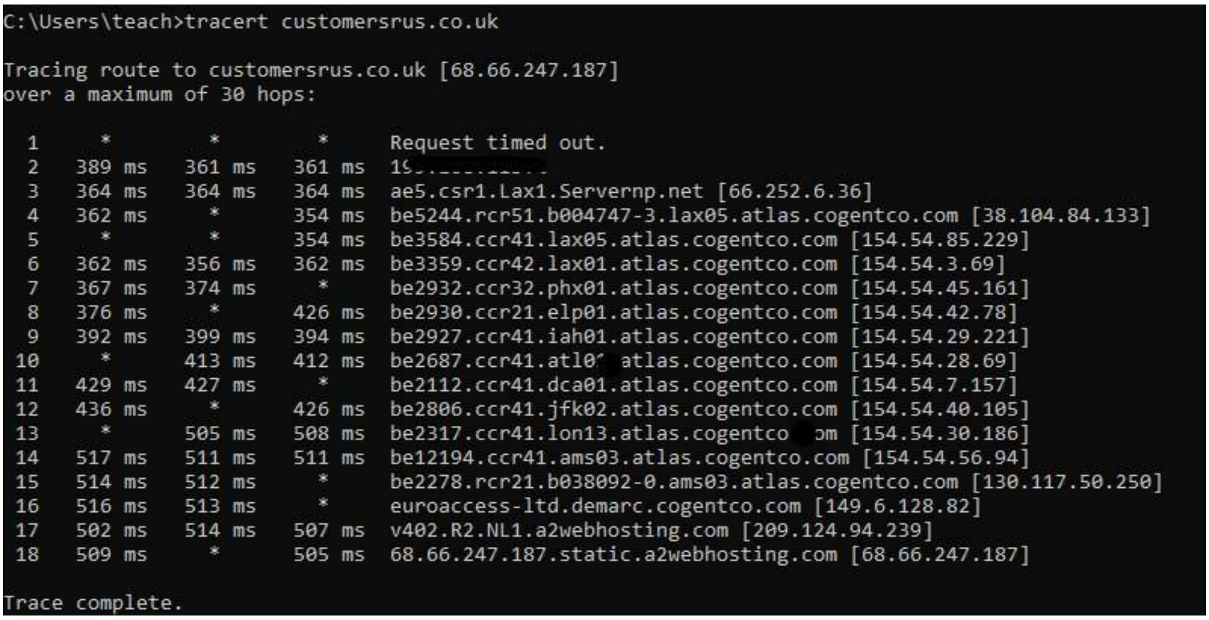
Shared web hosting accounts include the cPanel management interface, which makes site administration intuitive and easy. Our web hosting servers are optimized for speed, and our knowledgeable Guru Crew Support team is ready to help you every step of the way! Click here for more information about our shared web hosting plans.

It returned 'Shared Web Hosting' which is a shared server. Also, a2.hosting offer add-ons such SSL certificates including digicert and Cloudflare CDN. It is worth noting that a2hosting has a data centre in Amsterdam.

Where We Are
A2 HOSTING
OUR SPEED, YOUR SUCCESS
CANADA
UNITED STATES OF AMERICA
UNITED KINGDOM
UKRAINE
BULGARIA
PAKISTAN
INDIA
UNITED ARAB EMIRATES
PHILIPPINES
SINGAPORE
KENYA
COLOMBIA
BRASIL
AUSTRALIA
NUMBER OF EMPLOYEES
most
fewest
🟩 Data Centers
● Headquarters

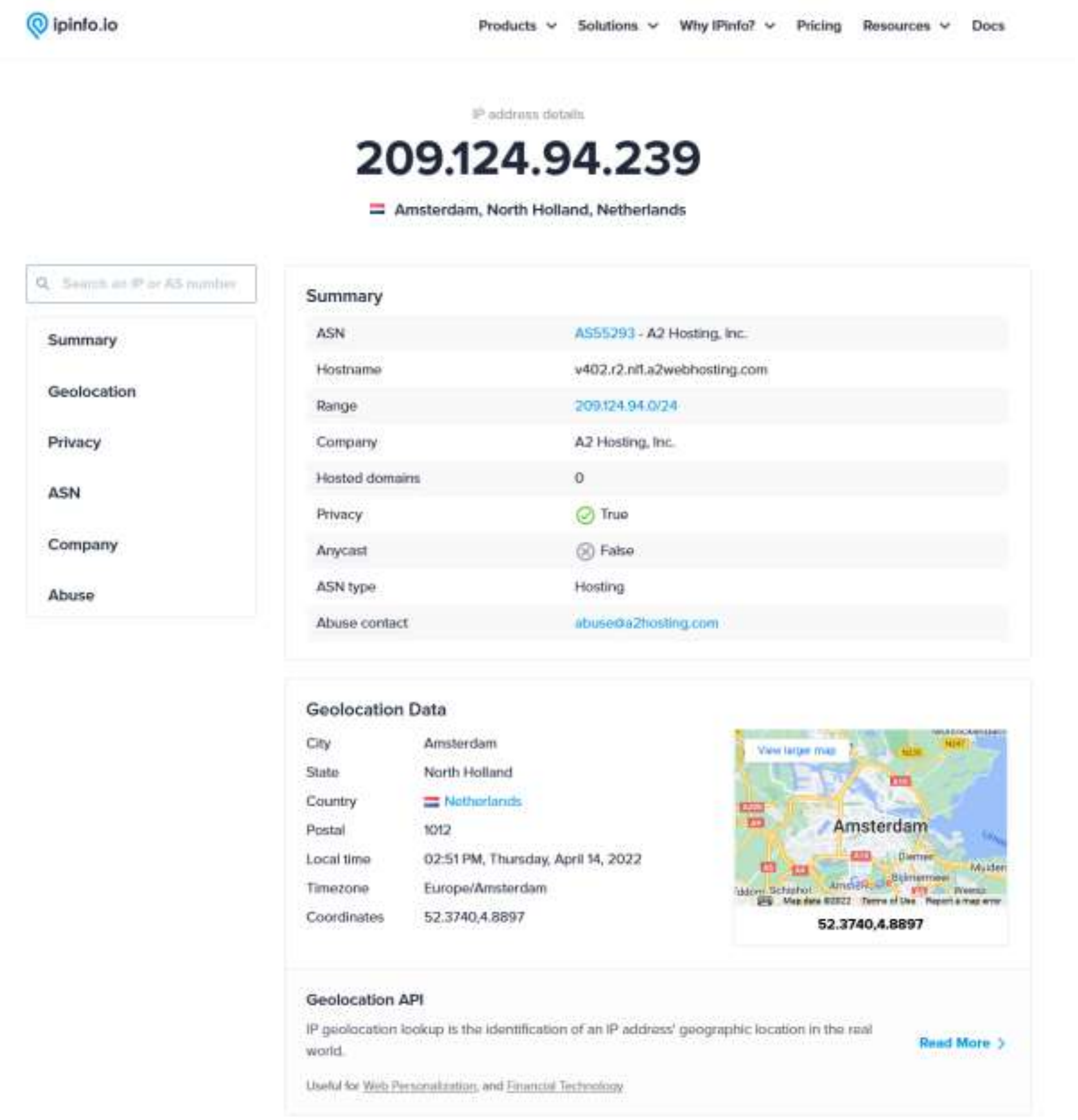
I rechecked my previous scans and noticed my tracert scan showed this:

- v402.R2.NL1.a2webhosting [209.124.94.239]
- 66.66.247.187 static.a2webhosting.com [68.66.247.178]



```
C:\Users\teach>tracert customersrus.co.uk

Tracing route to customersrus.co.uk [68.66.247.187]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2   389 ms   361 ms   361 ms  [redacted]
  3   364 ms   364 ms   364 ms  ae5.csr1.Lax1.Servernp.net [66.252.6.36]
  4   362 ms     *      354 ms  be5244.rcr51.b004747-3.lax05.atlas.cogentco.com [38.104.84.133]
  5     *        *      354 ms  be3584.ccr41.lax05.atlas.cogentco.com [154.54.85.229]
  6   362 ms   356 ms   362 ms  be3359.ccr42.lax01.atlas.cogentco.com [154.54.3.69]
  7   367 ms   374 ms     *     be2932.ccr32.phx01.atlas.cogentco.com [154.54.45.161]
  8   376 ms     *      426 ms  be2930.ccr21.elp01.atlas.cogentco.com [154.54.42.78]
  9   392 ms   399 ms   394 ms  be2927.ccr41.iah01.atlas.cogentco.com [154.54.29.221]
 10     *      413 ms   412 ms  be2687.ccr41.atl0[redacted]atlas.cogentco.com [154.54.28.69]
 11   429 ms   427 ms     *     be2112.ccr41.dca01.atlas.cogentco.com [154.54.7.157]
 12   436 ms     *      426 ms  be2806.ccr41.jfk02.atlas.cogentco.com [154.54.40.105]
 13     *      505 ms   508 ms  be2317.ccr41.lon13.atlas.cogentco[redacted]om [154.54.30.186]
 14   517 ms   511 ms   511 ms  be12194.ccr41.ams03.atlas.cogentco.com [154.54.56.94]
 15   514 ms   512 ms     *     be2278.rcr21.b038092-0.ams03.atlas.cogentco.com [130.117.50.250]
 16   516 ms   513 ms     *     euroaccess-ltd.demarc.cogentco.com [149.6.128.82]
 17   502 ms   514 ms   507 ms  v402.R2.NL1.a2webhosting.com [209.124.94.239]
 18   509 ms     *      505 ms  68.66.247.187.static.a2webhosting.com [68.66.247.187]

Trace complete.
```

Using Ipinfo (2022), it listed 209.124.94.239 in Amsterdam. In other words, the packets' last two hops were sent to Amsterdam and finishing in Ann Arbor.



IP address details

209.124.94.239

Amsterdam, North Holland, Netherlands

Summary

ASN	AS55293 - A2 Hosting, Inc.
Hostname	v402.r2.nl1.a2webhosting.com
Range	209.124.94.0/24
Company	A2 Hosting, Inc.
Hosted domains	0
Privacy	✓ True
Anycast	☒ False
ASN type	Hosting
Abuse contact	abuse@a2hosting.com

Geolocation Data

City	Amsterdam
State	North Holland
Country	Netherlands
Postal	1012
Local time	02:51 PM, Thursday, April 14, 2022
Timezone	Europe/Amsterdam
Coordinates	52.3740,4.8897

52.3740,4.8897

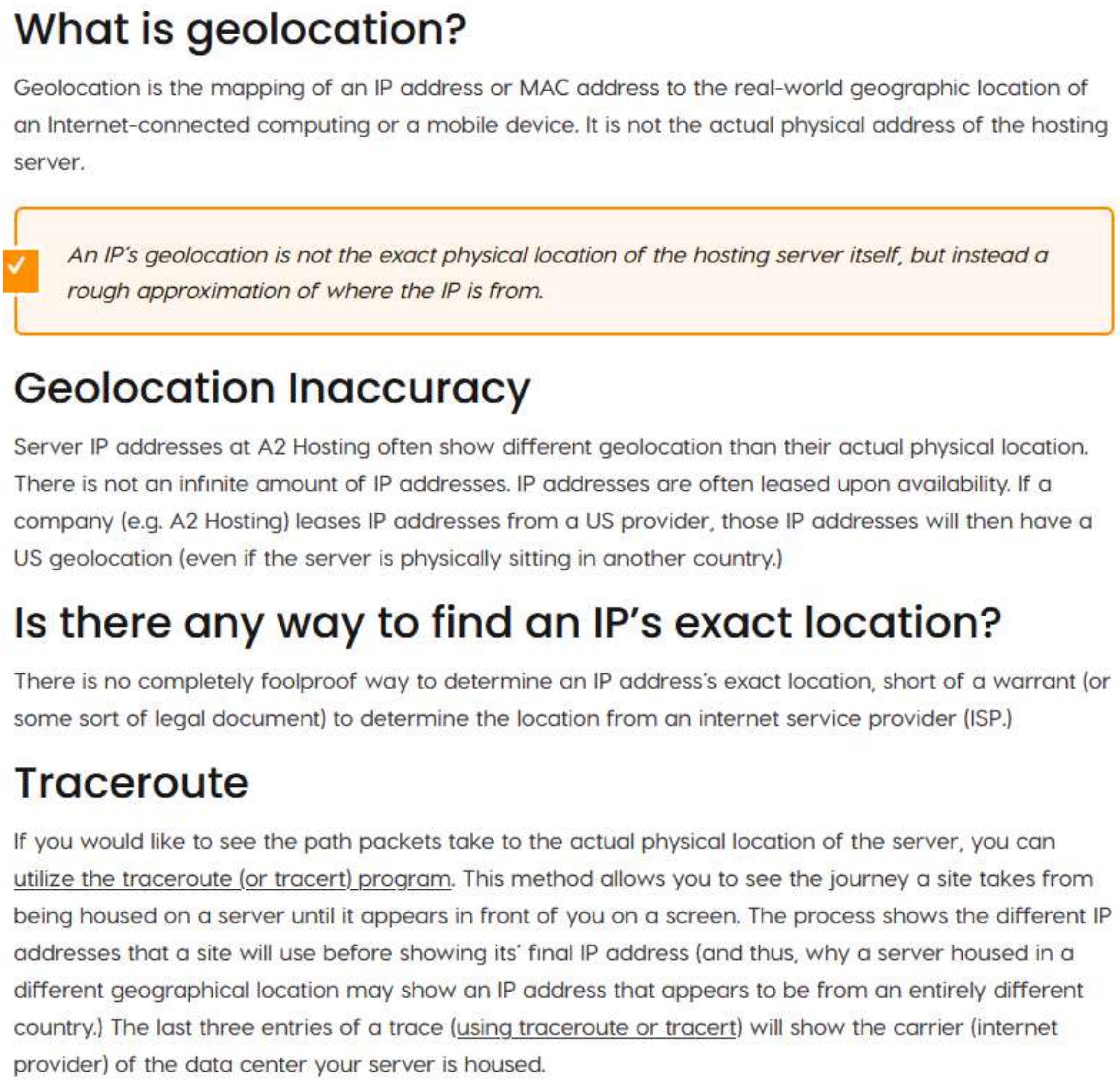
Geolocation API

IP geolocation lookup is the identification of an IP address' geographic location in the real world.

Read More ›

Useful for Web Personalization, and Financial Technology

Finally, a.2hosting (2022) offer further information on their Knowledge Base ‘Off-shore IP addresses’ section. They state there is no real way to know for certain an IP address location unless a warrant is issued, and that due to a finite number of IP address, if a.2hosting leases IP addresses from a US provider then it will have a US geolocation even if the server is in foreign country.



What is geolocation?

Geolocation is the mapping of an IP address or MAC address to the real-world geographic location of an Internet-connected computing or a mobile device. It is not the actual physical address of the hosting server.

> ✓ *An IP's geolocation is not the exact physical location of the hosting server itself, but instead a rough approximation of where the IP is from.*

Geolocation Inaccuracy

Server IP addresses at A2 Hosting often show different geolocation than their actual physical location. There is not an infinite amount of IP addresses. IP addresses are often leased upon availability. If a company (e.g. A2 Hosting) leases IP addresses from a US provider, those IP addresses will then have a US geolocation (even if the server is physically sitting in another country.)

Is there any way to find an IP's exact location?

There is no completely foolproof way to determine an IP address's exact location, short of a warrant (or some sort of legal document) to determine the location from an internet service provider (ISP.)

Traceroute

If you would like to see the path packets take to the actual physical location of the server, you can utilize the traceroute (or tracert) program. This method allows you to see the journey a site takes from being housed on a server until it appears in front of you on a screen. The process shows the different IP addresses that a site will use before showing its' final IP address (and thus, why a server housed in a different geographical location may show an IP address that appears to be from an entirely different country.) The last three entries of a trace (using traceroute or tracert) will show the carrier (internet provider) of the data center your server is housed.

It seems that the hosting company is headquartered in Ann Arbor, USA but has data centres in many countries including Netherlands, and it offers CDN and SSL third party services. The web site ‘customersrus.co.uk’ is using a.2hosting shared server located in Amsterdam, and as it is using a US leased IP address from a.2hosting, the final destination shows a US location.

References

Admin (2020) How to check domain’s MX (mail exchange) records using dig command on Linux. [online] Linux Tutorials - Learn Linux Configuration. Available at: https://linuxconfig.org/how-to-check-domain-s-mx-mail-exchange-records-using-dig-command-on-linux [Accessed 24 Mar. 2022].

Cloudflare. (2022) Cloudflare CDN | Content Delivery Network. Available from: https://www.cloudflare.com/cdn/.

blog.certcube.com. (2021) Nmap Scanning Cheatsheet For Beginners - 101 | Certcube Labs. [online] Available from: https://blog.certcube.com/nmap-scanning-cheatsheet-for-beginners/?msclkid=085d2ba0ab7411ecbb022c4bceb84e8d.

Buzdar, K. (n.d.) How to use the Linux mtr (My Traceroute) command – VITUX. vitux.com. Available from: https://vitux.com/how-to-use-the-linux-mtr-command/#:~:text=1%20How%20to%20use%20the%20Linux%20mtr%20%28My [Accessed 24 Mar. 2022].

Ipinfo.io. (2013) IP Address API and Data Solutions - geolocation, company, carrier info, type and more - IPinfo IP Address Geolocation API. Available from: https://ipinfo.io/.

Kacherginsky, P. (2018) Nmap Scanning Tips and Tricks. [online] Medium. Available from: https://iphelix.medium.com/nmap-scanning-tips-and-tricks-5b4a3d2151b3 [Accessed 24 Mar. 2022].

Knowledge Base by phoenixNAP. (2022) How to Use the nslookup Command {10 Examples}. Available from: https://phoenixnap.com/kb/nslookup-command [Accessed 24 Mar. 2022].

Shodan (2013). Shodan. Available from: https://www.shodan.io/

WhatIsMyIPAddress.com. (2022). What Is My IP Address? IP Address Tools and More. [online] Available from: https://whatismyipaddress.com/ [Accessed 24 Mar. 2022].

www.a2hosting.com. (2022a) Using Cloudflare. Available from: https://www.a2hosting.com/kb/add-on-services/cloudflare [Accessed 14 Apr. 2022].

www.a2hosting.com. (2022b) Web Hosting Services | 2020’s BEST Shared Hosting. Available from: https://www.a2hosting.com/web-hosting.

www.digicert.com. (2022) SSL Certificate Checker - Diagnostic Tool | DigiCert.com. Available from: https://www.digicert.com/help/ [Accessed 14 Apr. 2022].