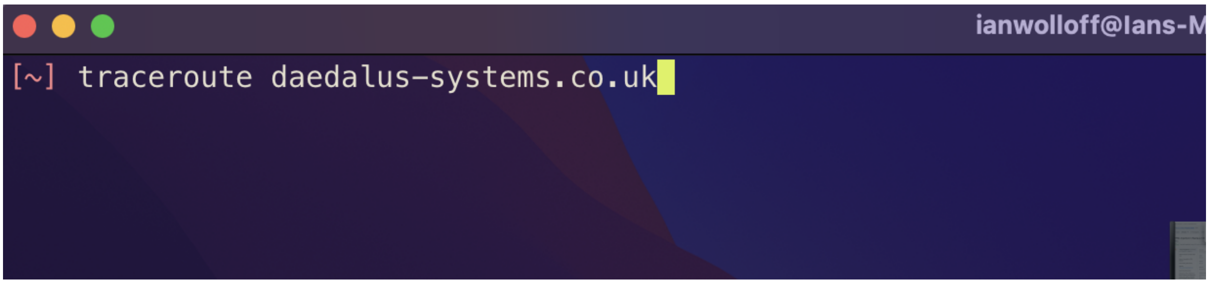
Practical Activity - Scanning Exercise (22nd November 2021)

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

To find out the number of hops from our device to our assigned website we will use the traceroute tool or tracert if on a windows device



```
[~] traceroute daedalus-systems.co.uk
```

Figure 1

The result from running the tool were as follows

Hop	IP Address	Address	Time (ms)
1	192.168.0.1	N/A	16.479
2	***	N/A (Probably Due to Blocked ICMP Traffic)	N/A
3	80.0.142.213	cosh-core-2b-ae50-0.network.virginmedia.net	20.899
4	62.254.42.174	m686-mp2.cvx1-b.lis.dial.ntli.net	20.546
5	213.46.174.118	213.46.174.118	24.314
6	62.115.120.238	ldn-bb4-link.ip.twelve99.net	20.183
7	62.115.122.188	ldn-bb1-link.ip.twelve99.net	18.965
8	213.155.136.99	adm-bb3-link.ip.twelve99.net	24.649
9	62.115.134.26	adm-bb4-link.ip.twelve99.net	25.631
11	62.115.120.227	adm-b10-link.ip.twelve99.net	28.558
12	62.115.120.229	adm-b10-link.ip.twelve99.net	28.077
13	62.115.145.217	a2hosting-svc080530-ic370345.ip.twelve99-cust.net	23.079
14	209.124.94.237	209.124.94.237.static.a2webhosting.com	27.466
15	68.66.247.187	68.66.247.187.static.a2webhosting.com	26.261

Hops (11,12) (6,7) and (8,9) can be treated as one hop each the reason for this on our traceroute output these are also. treated as one hop this is probably down to being a load balanced switch. Which means in answer to the question there are 12 distinct Hops between the starting address and the final website.

Raw Traceroute Dump

```
traceroute to daedalus-systems.co.uk (68.66.247.187), 64 hops max, 52 byte
packets
 1  192.168.0.1 (192.168.0.1) 60 bytes to 192.168.0.208  16.479 ms  3.871
ms  5.468 ms
 2  * * *
 3  cosh-core-2b-ae50-0.network.virginmedia.net (80.0.142.213) 36 bytes to
192.168.0.208  20.899 ms  14.956 ms  13.893 ms
 4  * * *
 5  m686-mp2.cvx1-b.lis.dial.ntli.net (62.254.42.174) 36 bytes to
192.168.0.208  20.546 ms  19.163 ms  18.087 ms
 6  213.46.174.118 (213.46.174.118) 76 bytes to 192.168.0.208  24.314 ms
16.933 ms  17.995 ms
 7  ldn-bb4-link.ip.twelve99.net (62.115.120.238) 148 bytes to
192.168.0.208  20.183 ms  18.327 ms
    ldn-bb1-link.ip.twelve99.net (62.115.122.188) 148 bytes to
192.168.0.208  18.965 ms
 8  adm-bb3-link.ip.twelve99.net (213.155.136.99) 148 bytes to
192.168.0.208  24.649 ms
    adm-bb4-link.ip.twelve99.net (62.115.134.26) 148 bytes to 192.168.0.208
25.631 ms  25.076 ms
 9  adm-b10-link.ip.twelve99.net (62.115.120.227) 76 bytes to 192.168.0.208
28.558 ms  26.196 ms
    adm-b10-link.ip.twelve99.net (62.115.120.229) 76 bytes to 192.168.0.208
28.077 ms
10  a2hosting-svc080530-ic370345.ip.twelve99-cust.net (62.115.145.217) 36
bytes to 192.168.0.208  23.079 ms  29.369 ms  23.149 ms
11  209.124.94.237.static.a2webhosting.com (209.124.94.237) 36 bytes to
192.168.0.208  27.466 ms  27.708 ms  26.002 ms
12  68.66.247.187.static.a2webhosting.com (68.66.247.187) 60 bytes to
192.168.0.208  26.261 ms  28.151 ms  27.116 ms
```

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

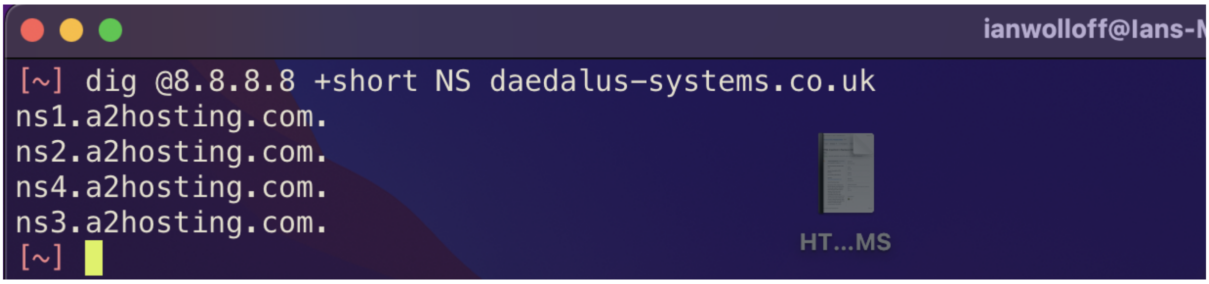
A. The Biggest Delay in the route is 28.588ms (**adm-b10-link.ip.twelve99.net**)
B. From our Traceroute at this step we had the following for 2 packets recorded 28.588 and 26.916 for this link giving an average of

(26.916 + 28.588) / 2 = 27.752

This However is a very small dataset and if we wanted a fair result, we would have to repeat the test a number of times to get a true idea if this really was the link with the lowest performance or if this was due to traffic or some other network conditions at the time we ran the original traceroute command.

Question Three What are the main nameservers for the website?

Using the dig command with the NS flag we can get the nameservers for the website



```
[~] dig @8.8.8.8 +short NS daedalus-systems.co.uk
ns1.a2hosting.com.
ns2.a2hosting.com.
ns4.a2hosting.com.
ns3.a2hosting.com.
[~]
```

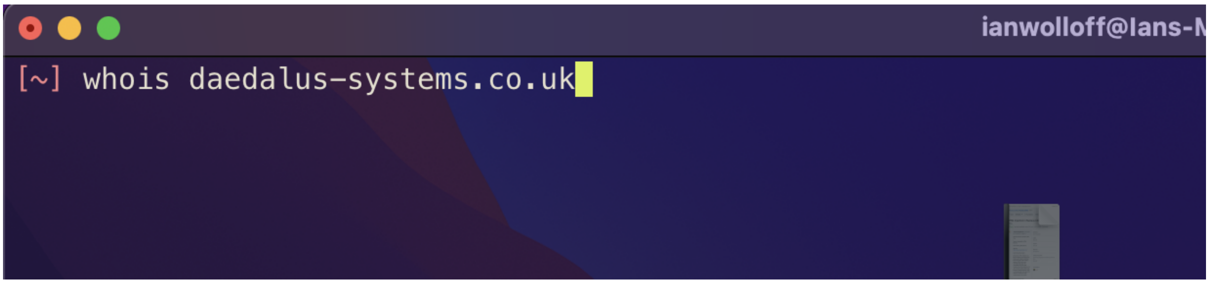
Figure 2

By taking these domains and running a nslookup command on them we can also get the IP address of the name servers producing the list below.

ns1.a2hosting.com (162.159.25.95)
ns2.a2hosting.com (162.159.24.221)
ns3.a2hosting.com (162.159.25.82)
ns4.a2hosting.com (162.159.24.227)

Question 4 Who is the registered contact

This is now not as easy as it once was due to a majority of registrations being hidden behind the hosting provider rather than the actual person who has registered the site but we can query the information held using the whois command.



```
[~] whois daedalus-systems.co.uk
```

Figure 3

This returns the following information.

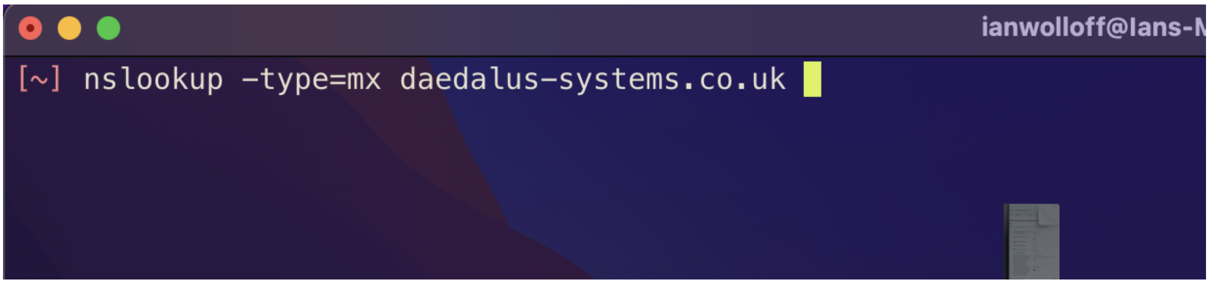
```
[~] whois daedalus-systems.co.uk
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.nic.uk

domain:       UK

organisation: Nominet UK
address:      Minerva House
address:      Edmund Halley Road
```

```
address:       Oxford Science Park
address:       Oxford  OX4 4DQ
address:       United Kingdom

contact:       administrative
name:          Managing Director
organisation: Nominet UK
address:       Minerva House
address:       Edmund Halley Road
address:       Oxford Science Park
address:       Oxford  OX4 4DQ
address:       United Kingdom
phone:         +44 1865 332211
fax-no:        +44 1865 332299
e-mail:        md@nominet.org.uk

contact:       technical
name:          Technical Director
organisation: Nominet UK
address:       Minerva House
address:       Edmund Halley Road
address:       Oxford Science Park
address:       Oxford  OX4 4DQ
address:       United Kingdom
phone:         +44 1865 332211
fax-no:        +44 1865 332299
e-mail:        td@nominet.org.uk

nserver:       DNS1.NIC.UK 213.248.216.1 2a01:618:400:0:0:0:0:1
nserver:       DNS2.NIC.UK 103.49.80.1 2401:fd80:400:0:0:0:0:1
nserver:       DNS3.NIC.UK 213.248.220.1 2a01:618:404:0:0:0:0:1
nserver:       DNS4.NIC.UK 2401:fd80:404:0:0:0:0:1 43.230.48.1
nserver:       NSA.NIC.UK 156.154.100.3 2001:502:ad09:0:0:0:0:3
nserver:       NSB.NIC.UK 156.154.101.3 2001:502:2eda:0:0:0:0:3
nserver:       NSC.NIC.UK 156.154.102.3 2610:a1:1009:0:0:0:0:3
nserver:       NSD.NIC.UK 156.154.103.3 2610:a1:1010:0:0:0:0:3
ds-rdata:      43876 8 2
A107ED2AC1BD14D924173BC7E827A1153582072394F9272BA37E2353BC6596
03

whois:         whois.nic.uk

status:        ACTIVE
remarks:       Registration information: http://www.nic.uk/

created:       1985-07-24
changed:       2021-10-07
source:        IANA
```

```
# whois.nic.uk


    Domain name:
        daedalus-systems.co.uk

    Data validation:
        Nominet was able to match the registrant's name and
address against a 3rd party data source on 01-Aug-2020

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

    Relevant dates:
        Registered on: 01-Aug-2020
        Expiry date:  01-Aug-2022
        Last updated:  01-Aug-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 10:23:48 22-Nov-2021
```

Question Five What is the MX record for the website?

To lookup the MX (Mail Exchange) record for a site we can use the nslookup command with the type set to mx



```
[~] nslookup -type=mx daedalus-systems.co.uk
```

Figure 4

This then returns the following information on the MX record

```
Server:      208.67.222.222
Address:     208.67.222.222#53

Non-authoritative answer:
daedalus-systems.co.uk  mail exchanger = 0 mail.daedalus-systems.co.uk.
```

Question 6 Where is the website hosted?

To Determine this there are a number of techniques that can be used but the one used here is using the lookup of IP address to geographic location for this a python script was written that takes a dictionary of IP addresses obtained from our traceroute and using the dataset provided by freegeoip returns information about the IP address based on the whois record that allows us to determine the location of the site.

```
import json
import urllib.request
import socket

IP_Address = ["62.115.120.238", "209.124.94.237"]
Resolver = "https://freegeoip.app/json/"

try:
    for hop, ip in enumerate(IP_Address):
        with urllib.request.urlopen(Resolver + ip) as url:
            data = json.loads(url.read().decode())
            print("Hop Number:" + str(hop))
            print("IP Address:" + data["ip"]
            print("Country Code:" + data["country_code"])
            print("Country Name:" + data["country_name"])
            print("Time Zone:" + data["time_zone"])
            print("Latitude:" + str(data["latitude"]))
            print("Longitude:" + str(data["longitude"]) + "\n")

except urllib.request.URLError:
    print("Error Getting Data")

except KeyError:
    print("Error Getting JSON Key")
```

This then returns the following data from the JSON webservice

Hop Number	**0**
IP Address	**192.168.0.1**
Country Code	
Country Name	
Time Zone	
Latitude	**0**
Longitude	**0**

Hop Number	**1**

IP Address	80.0.142.213
Country Code	GB
Country Name	United Kingdom
Time Zone	Europe/London
Latitude	52.5852
Longitude	-0.236

Hop Number	2
IP Address	62.254.42.174
Country Code	GB
Country Name	United Kingdom
Time Zone	Europe/London
Latitude	51.4964
Longitude	-0.1224

Hop Number	3
IP Address	213.46.174.118
Country Code	NL
Country Name	Netherlands
Time Zone	Europe/Amsterdam
Latitude	52.3824
Longitude	4.8995

Hop Number	4
IP Address	62.115.120.238
Country Code	SE
Country Name	Sweden
Time Zone	Europe/Stockholm
Latitude	59.3247
Longitude	18.056

Hop Number	5
IP Address	62.115.122.188
Country Code	SE
Country Name	Sweden
Time Zone	Europe/Stockholm
Latitude	59.3247
Longitude	18.056

Hop Number	6
IP Address	213.155.136.99
Country Code	SE
Country Name	Sweden
Time Zone	Europe/Stockholm
Latitude	59.3247
Longitude	18.056

Hop Number	7
IP Address	62.115.134.26
Country Code	SE
Country Name	Sweden
Time Zone	Europe/Stockholm
Latitude	59.3247
Longitude	18.056

Hop Number	8
IP Address	62.115.120.227
Country Code	SE
Country Name	Sweden
Time Zone	Europe/Stockholm
Latitude	59.3247
Longitude	18.056

Hop Number	9
IP Address	62.115.120.229
Country Code	SE
Country Name	Sweden
Time Zone	Europe/Stockholm
Latitude	59.3247
Longitude	18.056

Hop Number	10
IP Address	62.115.145.217
Country Code	SE
Country Name	Sweden
Time Zone	Europe/Stockholm
Latitude	59.3247
Longitude	18.056

Hop Number	11
IP Address	209.124.94.237
Country Code	US
Country Name	United States
Time Zone	America/Chicago
Latitude	37.751
Longitude	-97.822

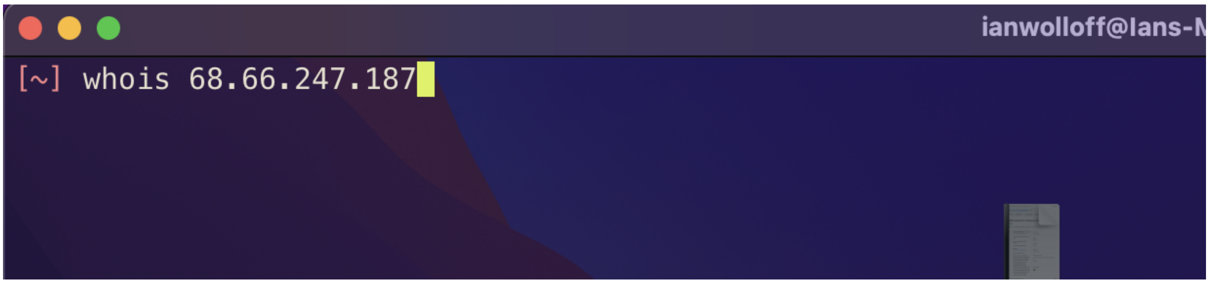
Hop Number	12
IP Address	68.66.247.187
Country Code	US
Country Name	United States

Time Zone	**America/Chicago**
Latitude	**37.751**
Longitude	**-97.822**

From this data our estimated traffic path is

No	**Country**
1	United Kingdom
2	Netherlands
3	Sweden
4	United States

The end point can be further verified by doing a whois on the last IP address in our traceroute chain



```
[~] whois 68.66.247.187
```

Figure 5

This command returns the following data

OrgName:	**A2 Hosting, Inc.**
OrgId:	**A2HOS**
Address:	**P.O. Box 2998**
City:	**Ann Arbor**
StateProv:	**MI**
PostalCode:	**48106**
Country:	**US**
RegDate:	**2004-03-16**
Updated:	**2021-10-13**
Comment:	**http://www.a2hosting.com**
Ref:	**https://rdap.arin.net/registry/entity/A2HOS**

This however is not the whole story as we now know the site is hosted with a2hosting while this provider is US based hence the US information in the Geocoded and whois record. Their core network is US based but from lookup up public information about this provider https://www.a2hosting.com/about/data-center (Anon) we can see that they have a number of datacentres located in the following areas.

Country	**City**	**IP Range**
USA	Michigan	75.98.175.109

USA	Arizona	68.66.224.6
Netherlands	Amsterdam	68.66.248.31
Asia	Singapore	03.227.176.4

From our traceroute result we can see our last hop is **68.66.247.187** which would seem to indicate that our site is actually physically hosted in the a2hosting Amsterdam datacentre. So, in answer to the question our site is located in **Amsterdam** which would also tie in with GDPR regulations as hosting a site outside of Europe for a European organisation can be complex in regard to data protection and compliancy legislation.

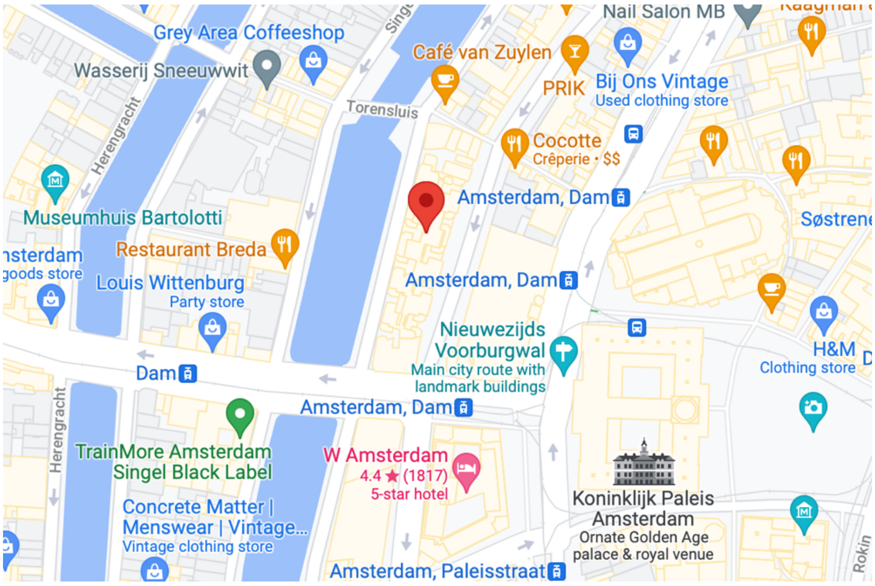


Figure 6 (Likely Location of Amsterdam Datacentre based on Public Lat / Lon Values)

References

Data Center | Datacenter Hosting Options. [Online]. Available at: https://www.a2hosting.com/about/data-center [Accessed 22 November 2021].