SCANNING ACTIVITY

Unit 3

SUMMARY

Ask	Results
How many hops from your machine to your assigned website?	20 Hops
Which step causes the biggest delay in the route? What is the average duration of that delay?	103.198.140.45 and delay is 175.185
What are the main nameservers for the website?	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
Who is the registered contact?	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
What is the MX record for the website?	allthegear.org.uk mail exchanger = 0 mail.allthegear.org.uk.
Where is the website hosted?	Region : Michigan & North Holland City : Ann Arbor &Amsterdam
Underline Application server	Apachi

TRACEROUTE

```
traceroute allthegear.org.uk
traceroute to allthegear.org.uk (68.66.247.187), 64 hops max, 52 byte packets
 1  reliance.reliance (192.168.29.1)  3.618 ms  2.689 ms  3.032 ms
 2  10.43.128.1 (10.43.128.1)  6.377 ms  4.780 ms  6.958 ms
 3  172.31.0.148 (172.31.0.148)  14.925 ms  13.767 ms  14.569 ms
 4  192.168.92.70 (192.168.92.70)  14.631 ms
    192.168.92.72 (192.168.92.72)  12.609 ms  16.638 ms
 5  172.26.103.68 (172.26.103.68)  14.070 ms  14.628 ms  15.734 ms
 6  172.26.103.131 (172.26.103.131)  19.915 ms
    172.26.103.130 (172.26.103.130)  14.375 ms
    172.26.103.131 (172.26.103.131)  16.942 ms
 7  192.168.83.28 (192.168.83.28)  19.194 ms
    192.168.83.24 (192.168.83.24)  18.486 ms  18.570 ms
 8  * * *
 9  * * *
10  103.198.140.176 (103.198.140.176)  45.746 ms  38.521 ms
    103.198.140.174 (103.198.140.174)  40.204 ms
11  103.198.140.54 (103.198.140.54)  160.242 ms
    103.198.140.213 (103.198.140.213)  170.342 ms  171.572 ms
12  103.198.140.107 (103.198.140.107)  163.216 ms
    103.198.140.45 (103.198.140.45)  175.875 ms
    103.198.140.107 (103.198.140.107)  155.258 ms
13  103.198.140.45 (103.198.140.45)  174.080 ms
    hu0-4-0-1.agr21.lhr01.atlas.cogentco.com (149.14.196.81)  155.268 ms  156.390 ms
14  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com (149.14.196.81)  161.858 ms
    be3671.ccr51.lhr01.atlas.cogentco.com (130.117.48.137)  167.701 ms
    hu0-4-0-1.agr21.lhr01.atlas.cogentco.com (149.14.196.81)  156.422 ms
15  be3671.ccr51.lhr01.atlas.cogentco.com (130.117.48.137)  165.761 ms
    be3488.ccr42.lon13.atlas.cogentco.com (154.54.60.13)  162.475 ms  160.964 ms
16  be3488.ccr42.lon13.atlas.cogentco.com (154.54.60.13)  162.466 ms
    be3487.ccr41.lon13.atlas.cogentco.com (154.54.60.5)  161.665 ms
    be3488.ccr42.lon13.atlas.cogentco.com (154.54.60.13)  163.864 ms
17  be12488.ccr42.ams03.atlas.cogentco.com (130.117.51.42)  167.307 ms
    be2278.rcr21.b038092-0.ams03.atlas.cogentco.com (130.117.50.250)  165.825 ms
    be12488.ccr42.ams03.atlas.cogentco.com (130.117.51.42)  173.948 ms
18  be2278.rcr21.b038092-0.ams03.atlas.cogentco.com (130.117.50.250)  161.275 ms  168.084 ms
    be2283.rcr21.b038092-0.ams03.atlas.cogentco.com (130.117.51.14)  160.656 ms
19  v402.r2.nl1.a2webhosting.com (209.124.94.239)  160.352 ms
    euroaccess-ltd.demarc.cogentco.com (149.6.128.82)  160.471 ms  167.205 ms
20  v402.r2.nl1.a2webhosting.com (209.124.94.239)  168.056 ms
    68.66.247.187.static.a2webhosting.com (68.66.247.187)  169.455 ms
    v402.r2.nl1.a2webhosting.com (209.124.94.239)  166.626 ms
```

- 20 hops to reach allthegear.org.uk
- 12 hop has the highest delay which is 175.875 ms
- Hop 8 & 9 gateway are not reported – this is because of any firewall or ICMP reply been filtered or blocked
- Average time to reach the website is 152.324 ms
- Ip address 68.66.247.187 is owned by A2 Hosting, Inc

NetRange: 68.66.212.0 - 68.66.255.255
CIDR: 68.66.212.0/22, 68.66.216.0/21, 68.66.224.0/19
NetName: INTERNET-BLK-A2HOS-13
NetHandle: NET-68-66-212-0-1
Parent: NET68 (NET-68-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS55293
Organization: A2 Hosting, Inc. (A2HOS)
RegDate: 2009-09-01
Updated: 2020-01-07
Ref: https://rdap.arin.net/registry/ip/68.66.212.0

NAME SERVER

macbook-pro ~ % dig @8.8.8.8 allthegear.org.uk

; <<>> DiG 9.10.6 <<>> @8.8.8.8 allthegear.org.uk
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14845
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;allthegear.org.uk. IN A

;; ANSWER SECTION:
allthegear.org.uk. 14231 IN A 68.66.247.187

;; Query time: 51 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Jul 04 12:18:52 EDT 2022
;; MSG SIZE rcvd: 62

MX RECORD

macbook-pro ~ % nslookup -type=mx allthegear.org.uk
Server: 192.168.87.1
Address: 192.168.87.1#53

Non-authoritative answer:
allthegear.org.uk mail exchanger = 0 mail.allthegear.org.uk.

Authoritative answers can be found from:

WHOIS

```
macbook-pro ~ % whois allthegear.org.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 A107ED2AC1BD14D924173BC7E827A1153582072394F9272BA37E2353BC659603

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:
      allthegear.org.uk
   Data validation:
      Nominet was able to match the registrant's name and address against a 3rd party data source on 25-Apr-2022
   Registrar:
      eNom LLC [Tag = ENOM]
      URL: http://www.enom.com
   Relevant dates:
      Registered on: 25-Apr-2022
      Expiry date:  25-Apr-2023
      Last updated:  25-Apr-2022
   Registration status:
      Registered until expiry date.
   Name servers:
      ns1.a2hosting.com
      ns2.a2hosting.com
      ns3.a2hosting.com
      ns4.a2hosting.com

   WHOIS lookup made at 17:20:01 04-Jul-2022
```

WEBSITE LOCATION

- Based on the iplocation.net, this website is hosted in two geographical locations

Domain Name	Country	Region	City
Allthegear.org.uk	United states of America	Michigan	Ann Arbor
Allthegear.org.uk	Nethralands	North Holland	Amsterdam

WEB SERVER – DETAILS

@macbook-pro ~ % curl -I https://allthegear.org.uk
HTTP/2 200
x-powered-by: PHP/7.4.30
pragma: no-cache
cache-control: max-age=0, must-revalidate, no-cache, no-store
expires: Sun, 04 Jul 2021 12:28:21 GMT
content-security-policy-report-only:**output removed**
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
x-frame-options: SAMEORIGIN
set-cookie: PHPSESSID=790203a3b987bbf26d30dc488dd6d5da; expires=Mon, 04-Jul-2022 19:14:18 GMT; Max-Age=3600; path=/; domain=allthegear.org.uk; secure; HttpOnly; SameSite=Lax
strict-transport-security: max-age=63072000; includeSubDomains
content-length: 91952
x-ua-compatible: IE=edge
content-type: text/html; charset=UTF-8
date: Mon, 04 Jul 2022 18:14:17 GMT
server: Apache