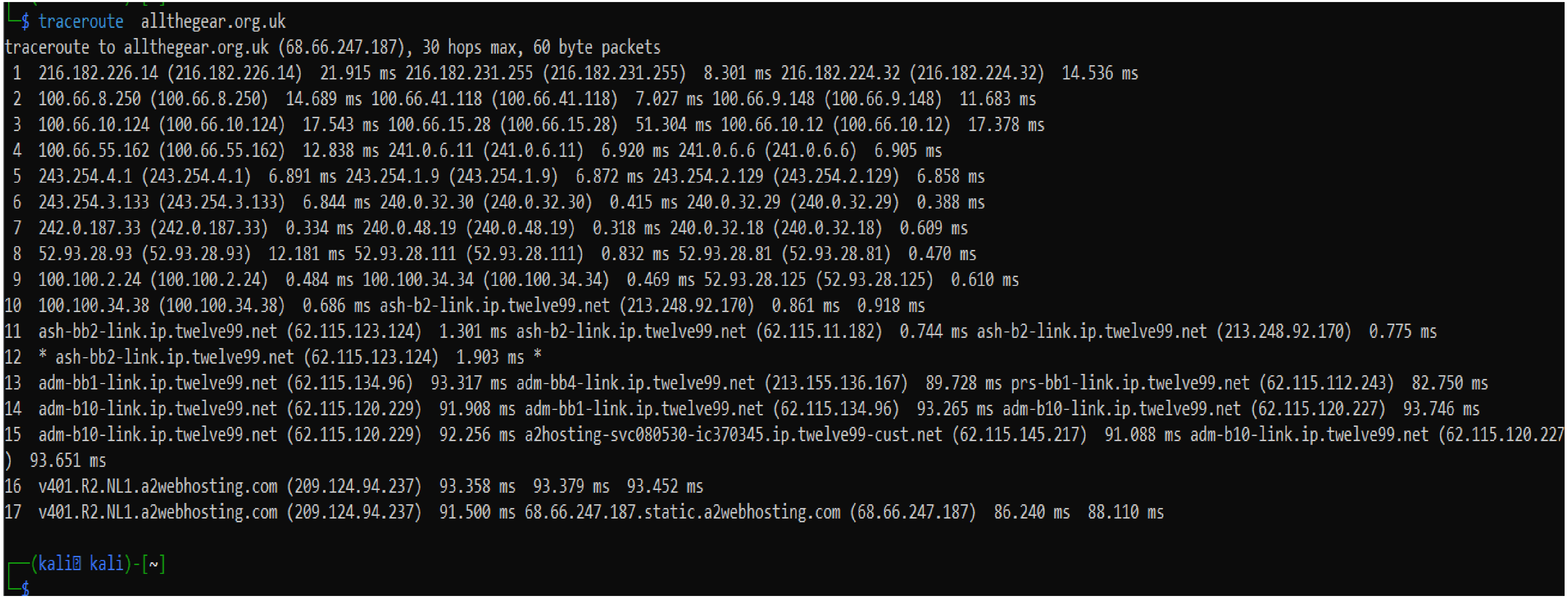
Scanning Activity

Unit 3

SUMMARY

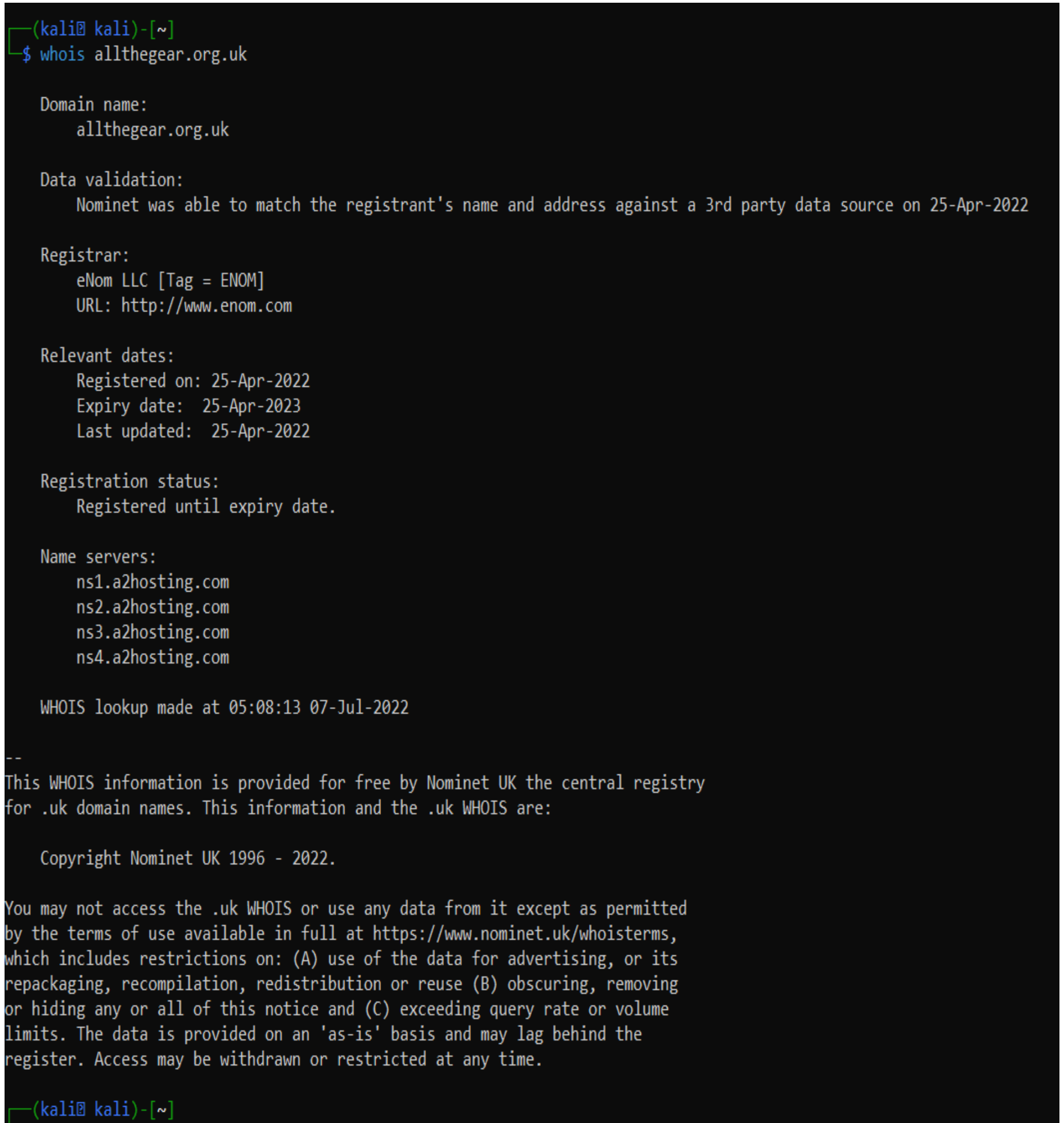
TEST	RESULT
How many hops from your machine to your assigned website?	17
Which step causes the biggest delay in the route? What is the average duration of that delay?	62.115.120.229 (Hop 14) // 93ms
What are the main nameservers for the website?	ns1.a2hosting.com ns2.a2hosting.com ns3.a2hosting.com ns4.a2hosting.com
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?	mail.allthegear.org.uk
Where is the website hosted?	
Underline Application server	Apache

TRACEROUTE



```
└─$ traceroute  allthegear.org.uk
traceroute to allthegear.org.uk (68.66.247.187), 30 hops max, 60 byte packets
 1  216.182.226.14 (216.182.226.14)  21.915 ms 216.182.231.255 (216.182.231.255)  8.301 ms 216.182.224.32 (216.182.224.32)  14.536 ms
 2  100.66.8.250 (100.66.8.250)  14.689 ms 100.66.41.118 (100.66.41.118)  7.027 ms 100.66.9.148 (100.66.9.148)  11.683 ms
 3  100.66.10.124 (100.66.10.124)  17.543 ms 100.66.15.28 (100.66.15.28)  51.304 ms 100.66.10.12 (100.66.10.12)  17.378 ms
 4  100.66.55.162 (100.66.55.162)  12.838 ms 241.0.6.11 (241.0.6.11)  6.920 ms 241.0.6.6 (241.0.6.6)  6.905 ms
 5  243.254.4.1 (243.254.4.1)  6.891 ms 243.254.1.9 (243.254.1.9)  6.872 ms 243.254.2.129 (243.254.2.129)  6.858 ms
 6  243.254.3.133 (243.254.3.133)  6.844 ms 240.0.32.30 (240.0.32.30)  0.415 ms 240.0.32.29 (240.0.32.29)  0.388 ms
 7  242.0.187.33 (242.0.187.33)  0.334 ms 240.0.48.19 (240.0.48.19)  0.318 ms 240.0.32.18 (240.0.32.18)  0.609 ms
 8  52.93.28.93 (52.93.28.93)  12.181 ms 52.93.28.111 (52.93.28.111)  0.832 ms 52.93.28.81 (52.93.28.81)  0.470 ms
 9  100.100.2.24 (100.100.2.24)  0.484 ms 100.100.34.34 (100.100.34.34)  0.469 ms 52.93.28.125 (52.93.28.125)  0.610 ms
10  100.100.34.38 (100.100.34.38)  0.686 ms ash-b2-link.ip.twelve99.net (213.248.92.170)  0.861 ms  0.918 ms
11  ash-bb2-link.ip.twelve99.net (62.115.123.124)  1.301 ms ash-b2-link.ip.twelve99.net (62.115.11.182)  0.744 ms ash-b2-link.ip.twelve99.net (213.248.92.170)  0.775 ms
12  * ash-bb2-link.ip.twelve99.net (62.115.123.124)  1.903 ms *
13  adm-bb1-link.ip.twelve99.net (62.115.134.96)  93.317 ms adm-bb4-link.ip.twelve99.net (213.155.136.167)  89.728 ms prs-bb1-link.ip.twelve99.net (62.115.112.243)  82.750 ms
14  adm-b10-link.ip.twelve99.net (62.115.120.229)  91.908 ms adm-bb1-link.ip.twelve99.net (62.115.134.96)  93.265 ms adm-b10-link.ip.twelve99.net (62.115.120.227)  93.746 ms
15  adm-b10-link.ip.twelve99.net (62.115.120.229)  92.256 ms a2hosting-svc080530-ic370345.ip.twelve99-cust.net (62.115.145.217)  91.088 ms adm-b10-link.ip.twelve99.net (62.115.120.227
)  93.651 ms
16  v401.R2.NL1.a2webhosting.com (209.124.94.237)  93.358 ms  93.379 ms  93.452 ms
17  v401.R2.NL1.a2webhosting.com (209.124.94.237)  91.500 ms 68.66.247.187.static.a2webhosting.com (68.66.247.187)  86.240 ms  88.110 ms

┌──(kali□ kali)-[~]
└─$
```

WHOIS



```
┌──(kali⊠ kali)-[~]
└─$ whois allthegear.org.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 05:08:13 07-Jul-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.

┌──(kali⊠ kali)-[~]
```

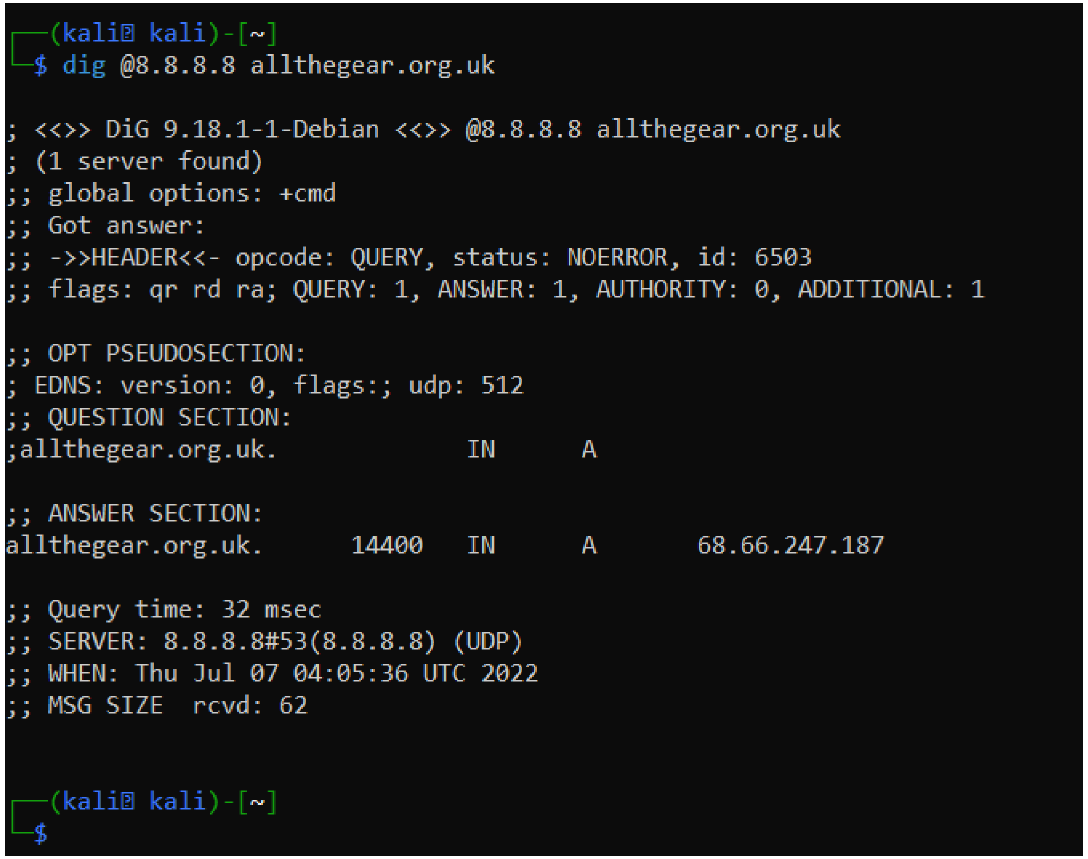
```
nserver:     DNS1.NIC.UK 213.248.216.1 2a01:618:400:0:0:0:0:1
nserver:     DNS2.NIC.UK 103.49.80.1 2401:fd80:400:0:0:0:0:1
nserver:     DNS3.NIC.UK 213.248.220.1 2a01:618:404:0:0:0:0:1
nserver:     DNS4.NIC.UK 2401:fd80:404:0:0:0:0:1 43.230.48.1
nserver:     NSA.NIC.UK 156.154.100.3 2001:502:ad09:0:0:0:0:3
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
```

WHOIS

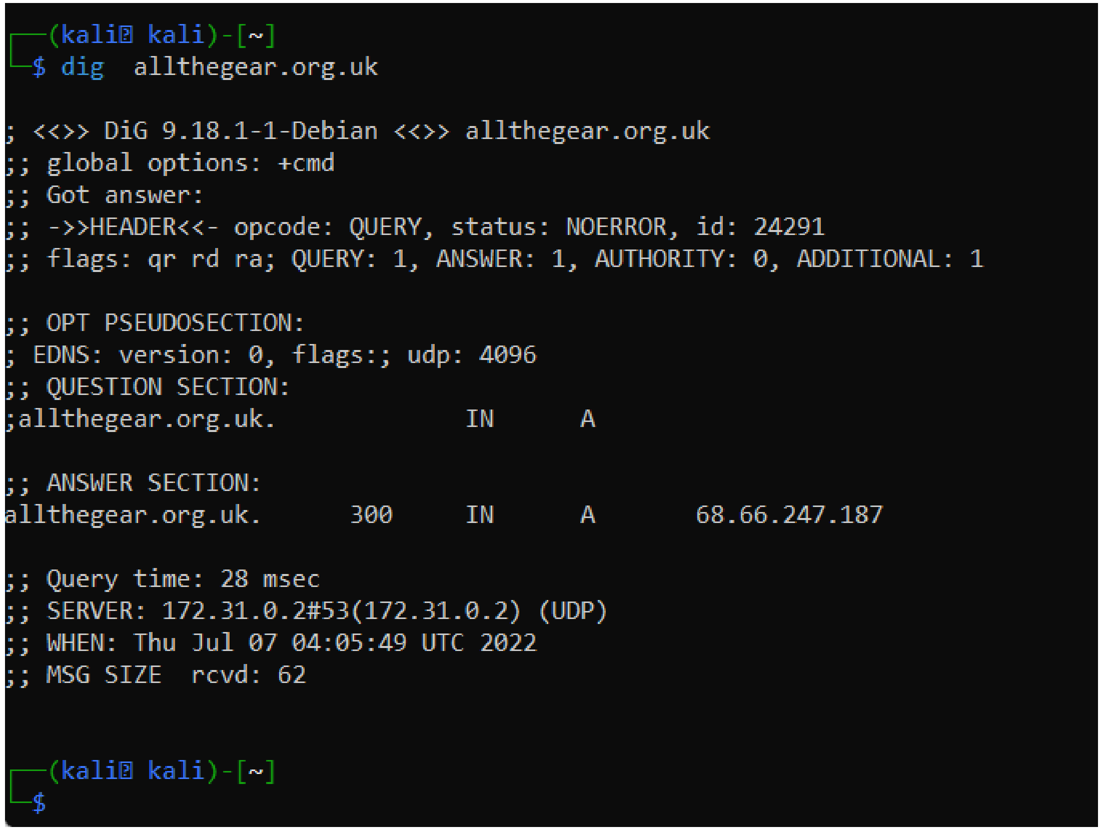
```
macbook-pro ~ % whois allthegear.org.uk
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

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
```

NAME-SERVER

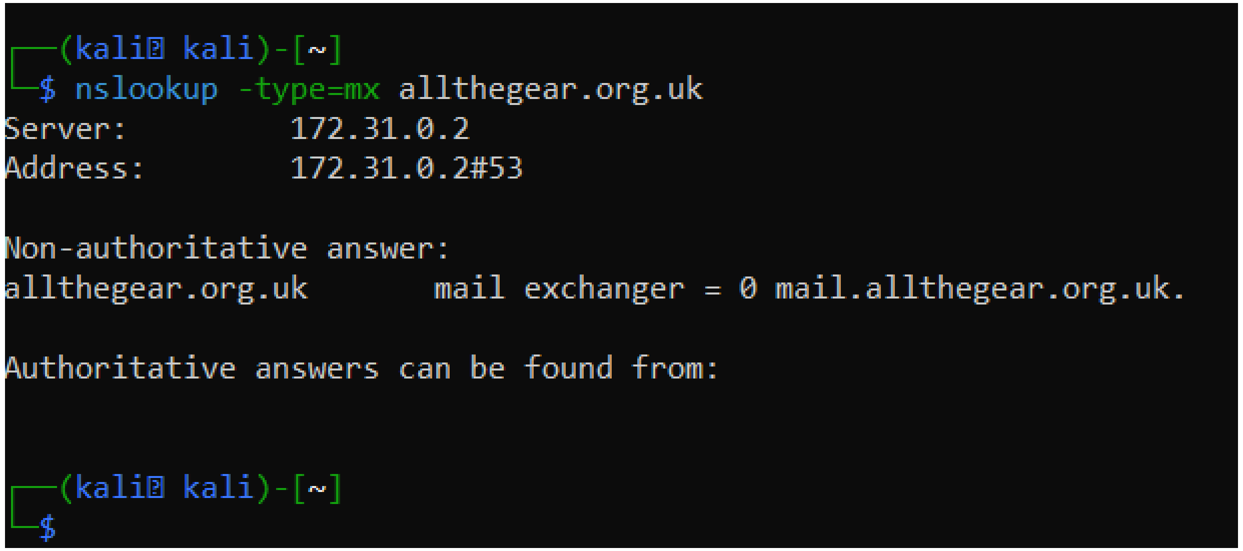


```
┌──(kali㉿ kali)-[~]
└─$ dig @8.8.8.8 allthegear.org.uk

; <<>> DiG 9.18.1-1-Debian <<>> @8.8.8.8 allthegear.org.uk
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6503
;; 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.      14400   IN      A       68.66.247.187

;; Query time: 32 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Thu Jul 07 04:05:36 UTC 2022
;; MSG SIZE  rcvd: 62


┌──(kali㉿ kali)-[~]
└─$
```



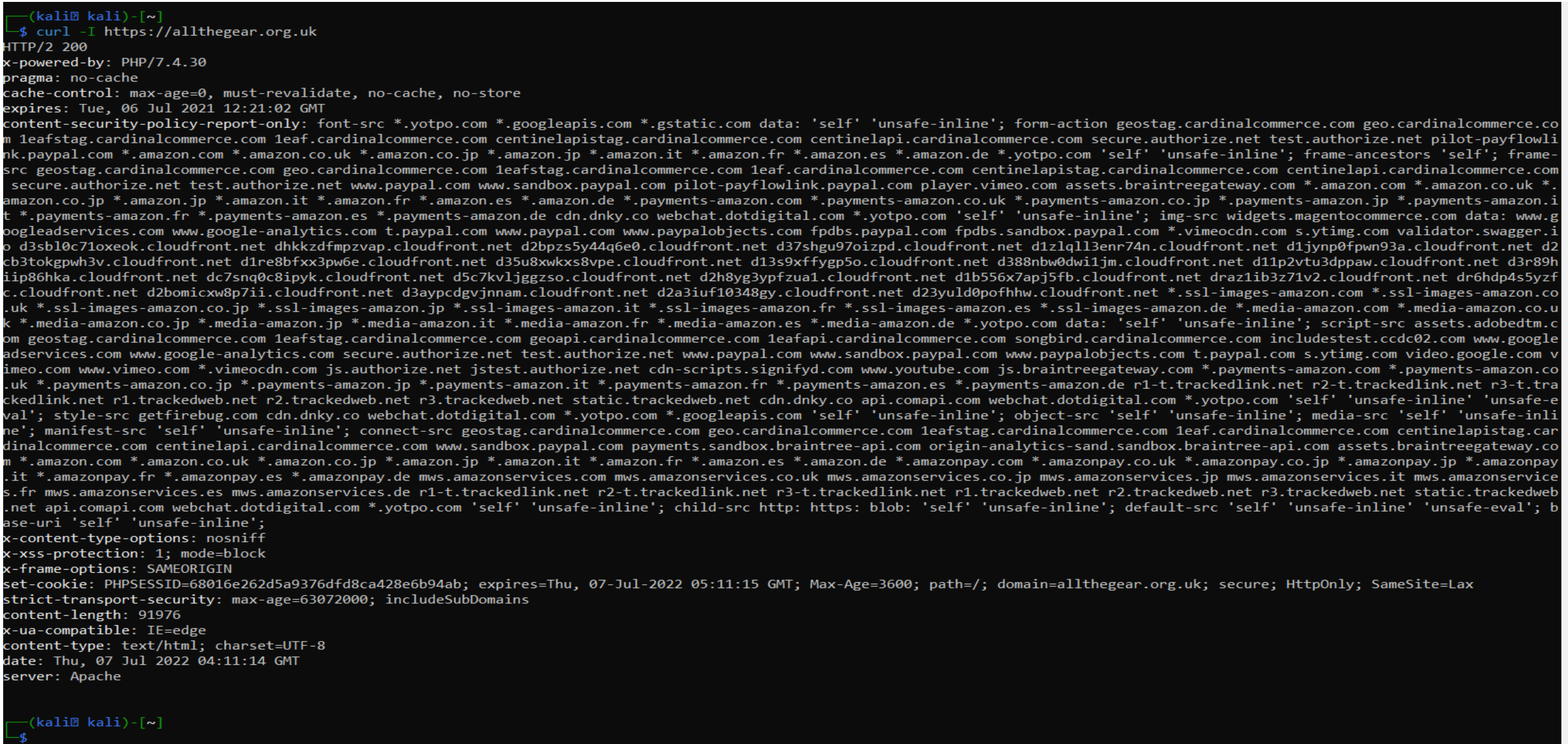
```
┌──(kali㉿ kali)-[~]
└─$ dig  allthegear.org.uk

; <<>> DiG 9.18.1-1-Debian <<>> allthegear.org.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24291
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;allthegear.org.uk.             IN      A

;; ANSWER SECTION:
allthegear.org.uk.      300     IN      A       68.66.247.187

;; Query time: 28 msec
;; SERVER: 172.31.0.2#53(172.31.0.2) (UDP)
;; WHEN: Thu Jul 07 04:05:49 UTC 2022
;; MSG SIZE  rcvd: 62


┌──(kali㉿ kali)-[~]
└─$
```

MX-RECORD



```
┌──(kali㉿ kali)-[~]
└─$ nslookup -type=mx allthegear.org.uk
Server:         172.31.0.2
Address:        172.31.0.2#53

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

Authoritative answers can be found from:


┌──(kali㉿ kali)-[~]
└─$
```

WEB SERVER



```
┌──(kali㉿ kali)-[~]
└─$ 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: Tue, 06 Jul 2021 12:21:02 GMT
content-security-policy-report-only: font-src *.yotpo.com *.googleapis.com *.gstatic.com data: 'self' 'unsafe-inline'; form-action geostag.cardinalcommerce.com geo.cardinalcommerce.co
m 1eafstag.cardinalcommerce.com 1eaf.cardinalcommerce.com centinelapistag.cardinalcommerce.com centinelapi.cardinalcommerce.com secure.authorize.net test.authorize.net pilot-payflowli
nk.paypal.com *.amazon.com *.amazon.co.uk *.amazon.co.jp *.amazon.jp *.amazon.it *.amazon.fr *.amazon.es *.amazon.de *.yotpo.com 'self' 'unsafe-inline'; frame-ancestors 'self'; frame-
src geostag.cardinalcommerce.com geo.cardinalcommerce.com 1eafstag.cardinalcommerce.com 1eaf.cardinalcommerce.com centinelapistag.cardinalcommerce.com centinelapi.cardinalcommerce.com
 secure.authorize.net test.authorize.net www.paypal.com www.sandbox.paypal.com pilot-payflowlink.paypal.com player.vimeo.com assets.braintreegateway.com *.amazon.com *.amazon.co.uk *.
amazon.co.jp *.amazon.jp *.amazon.it *.amazon.fr *.amazon.es *.amazon.de *.payments-amazon.com *.payments-amazon.co.uk *.payments-amazon.co.jp *.payments-amazon.jp *.payments-amazon.i
t *.payments-amazon.fr *.payments-amazon.es *.payments-amazon.de cdn.dnky.co webchat.dotdigital.com *.yotpo.com 'self' 'unsafe-inline'; img-src widgets.magentocommerce.com data: www.g
oogleadservices.com www.google-analytics.com t.paypal.com www.paypal.com www.paypalobjects.com fpdbs.paypal.com fpdbs.sandbox.paypal.com *.vimeocdn.com s.ytimg.com validator.swagger.i
o d3sbl0c71oxeok.cloudfront.net dhkkzdfmpzvap.cloudfront.net d2bpzs5y44q6e0.cloudfront.net d37shgu97oizpd.cloudfront.net d1zlqll3enr74n.cloudfront.net d1jynp0fpwn93a.cloudfront.net d2
cb3tokgpwh3v.cloudfront.net d1re8bfxx3pw6e.cloudfront.net d35u8xwkxs8vpe.cloudfront.net d13s9xffygp5o.cloudfront.net d388nbw0dwi1jm.cloudfront.net d11p2vtu3dppaw.cloudfront.net d3r89h
iip86hka.cloudfront.net dc7snq0c8ipyk.cloudfront.net d5c7kvljggzso.cloudfront.net d2h8yg3ypfzua1.cloudfront.net d1b556x7apj5fb.cloudfront.net draz1ib3z71v2.cloudfront.net dr6hdp4s5yzf
c.cloudfront.net d2bomicxw8p7ii.cloudfront.net d3aypcdgvjnnam.cloudfront.net d2a3iuf10348gy.cloudfront.net d23yuld0pofhhw.cloudfront.net *.ssl-images-amazon.com *.ssl-images-amazon.co
.uk *.ssl-images-amazon.co.jp *.ssl-images-amazon.jp *.ssl-images-amazon.it *.ssl-images-amazon.fr *.ssl-images-amazon.es *.ssl-images-amazon.de *.media-amazon.com *.media-amazon.co.u
k *.media-amazon.co.jp *.media-amazon.jp *.media-amazon.it *.media-amazon.fr *.media-amazon.es *.media-amazon.de *.yotpo.com data: 'self' 'unsafe-inline'; script-src assets.adobedtm.c
om geostag.cardinalcommerce.com 1eafstag.cardinalcommerce.com geoapi.cardinalcommerce.com 1eafapi.cardinalcommerce.com songbird.cardinalcommerce.com includestest.ccdc02.com www.google
adservices.com www.google-analytics.com secure.authorize.net test.authorize.net www.paypal.com www.sandbox.paypal.com www.paypalobjects.com t.paypal.com s.ytimg.com video.google.com v
imeo.com www.vimeo.com *.vimeocdn.com js.authorize.net jstest.authorize.net cdn-scripts.signifyd.com www.youtube.com js.braintreegateway.com *.payments-amazon.com *.payments-amazon.co
.uk *.payments-amazon.co.jp *.payments-amazon.jp *.payments-amazon.it *.payments-amazon.fr *.payments-amazon.es *.payments-amazon.de r1-t.trackedlink.net r2-t.trackedlink.net r3-t.tra
ckedlink.net r1.trackedweb.net r2.trackedweb.net r3.trackedweb.net static.trackedweb.net cdn.dnky.co api.comapi.com webchat.dotdigital.com *.yotpo.com 'self' 'unsafe-inline' 'unsafe-e
val'; style-src getfirebug.com cdn.dnky.co webchat.dotdigital.com *.yotpo.com *.googleapis.com 'self' 'unsafe-inline'; object-src 'self' 'unsafe-inline'; media-src 'self' 'unsafe-inli
ne'; manifest-src 'self' 'unsafe-inline'; connect-src geostag.cardinalcommerce.com geo.cardinalcommerce.com 1eafstag.cardinalcommerce.com 1eaf.cardinalcommerce.com centinelapistag.car
dinalcommerce.com centinelapi.cardinalcommerce.com www.sandbox.paypal.com payments.sandbox.braintree-api.com origin-analytics-sand.sandbox.braintree-api.com assets.braintreegateway.co
m *.amazon.com *.amazon.co.uk *.amazon.co.jp *.amazon.jp *.amazon.it *.amazon.fr *.amazon.es *.amazon.de *.amazonpay.com *.amazonpay.co.uk *.amazonpay.co.jp *.amazonpay.jp *.amazonpay
.it *.amazonpay.fr *.amazonpay.es *.amazonpay.de mws.amazonservices.com mws.amazonservices.co.uk mws.amazonservices.co.jp mws.amazonservices.jp mws.amazonservices.it mws.amazonservice
s.fr mws.amazonservices.es mws.amazonservices.de r1-t.trackedlink.net r2-t.trackedlink.net r3-t.trackedlink.net r1.trackedweb.net r2.trackedweb.net r3.trackedweb.net static.trackedweb
.net api.comapi.com webchat.dotdigital.com *.yotpo.com 'self' 'unsafe-inline'; child-src http: https: blob: 'self' 'unsafe-inline'; default-src 'self' 'unsafe-inline' 'unsafe-eval'; b
ase-uri 'self' 'unsafe-inline';
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
x-frame-options: SAMEORIGIN
set-cookie: PHPSESSID=68016e262d5a9376dfd8ca428e6b94ab; expires=Thu, 07-Jul-2022 05:11:15 GMT; Max-Age=3600; path=/; domain=allthegear.org.uk; secure; HttpOnly; SameSite=Lax
strict-transport-security: max-age=63072000; includeSubDomains
content-length: 91976
x-ua-compatible: IE=edge
content-type: text/html; charset=UTF-8
date: Thu, 07 Jul 2022 04:11:14 GMT
server: Apache


┌──(kali㉿ kali)-[~]
└─$
```