

## Unit 3 Scanning Activity

### Tools Used

Trace Root

Who Is

Name Server Lookup

Who Is Website

### Question One

**Command Used:** `tracert ginandjuice.shop`

**How many hops from your machine to your assigned website?**

More than 30. Most of the requests are blocked. The first hop is my local router with the next couple going through the PlusNet system. At hop six they start getting blocked and this could be due to Amazon blocking ICMP responses, this is common for security reasons.

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

Hop five gives the biggest delay of 24ms with an average delay of 12ms.

Tracing route to ginandjuice.shop [34.249.203.140]  
over a maximum of 30 hops:

1	<1 ms	<1 ms	<1 ms	192.168.1.254
2	5 ms	5 ms	7 ms	251.core.plus.net [195.166.130.251]
3	6 ms	6 ms	6 ms	217.32.25.136
4	5 ms	6 ms	6 ms	109.159.255.40
5	24 ms	6 ms	6 ms	194.74.16.243
6	*	*	*	Request timed out.
7	*	*	*	Request timed out.
8	*	*	*	Request timed out.
9	*	*	*	Request timed out.
10	*	*	*	Request timed out.
11	*	*	*	Request timed out.
12	*	*	*	Request timed out.
13	*	*	*	Request timed out.
14	*	*	*	Request timed out.
15	*	*	*	Request timed out.
16	*	*	*	Request timed out.
17	*	*	*	Request timed out.
18	*	*	*	Request timed out.
19	*	*	*	Request timed out.
20	*	*	*	Request timed out.
21	*	*	*	Request timed out.
22	*	*	*	Request timed out.
23	*	*	*	Request timed out.
24	*	*	*	Request timed out.
25	*	*	*	Request timed out.
26	*	*	*	Request timed out.
27	*	*	*	Request timed out.
28	*	*	*	Request timed out.
29	*	*	*	Request timed out.
30	*	*	*	Request timed out.

Trace complete.

## Question Two

**Command Used:** `nslookup -type=NS ginandjuice.shop`

**Command Used:** `nslookup -type=SOA ginandjuice.shop`

**Command Used:** `nslookup -type=MX ginandjuice.shop`

`-type=NS`

`-type=SOA`

`-type=MX`

Retrieves Name Server (NS) records.

Retrieves the Start of Authority (SOA) record.

Retrieves Mail Exchange (MX) records

**What are the main nameservers for the website?**

ns-1496.awsdns-59.org

ns-1543.awsdns-00.co.uk

ns-1000.awsdns-61.net

ns-110.awsdns-13.com

**What is the MX record for the website?**

Responsible mail address, awsdns-hostmaster.amazon.com or  
awsdns@hostmaster.amazon.com

```
C:\Users\Tim>nslookup -type=soa ginandjuice.shop
```

```
Server:  UnKnown
```

```
Address: 192.168.1.254
```

```
Non-authoritative answer:
```

```
ginandjuice.shop
```

```
primary name server = ns-1496.awsdns-59.org
```

```
responsible mail addr = awsdns-hostmaster.amazon.com
```

```
serial = 1
```

```
refresh = 7200 (2 hours)
```

```
retry = 900 (15 mins)
```

```
expire = 1209600 (14 days)
```

```
default TTL = 86400 (1 day)
```

```
C:\Users\Tim>nslookup -type=MX ginandjuice.shop
```

```
Server:  UnKnown
```

```
Address: 192.168.1.254
```

```
ginandjuice.shop
```

```
primary name server = ns-1496.awsdns-59.org
```

```
responsible mail addr = awsdns-hostmaster.amazon.com
```

```
serial = 1
```

```
refresh = 7200 (2 hours)
```

```
retry = 900 (15 mins)
```

```
expire = 1209600 (14 days)
```

```
default TTL = 86400 (1 day)
```

```
C:\Users\Tim>nslookup -type=NS ginandjuice.shop
```

```
Server:  UnKnown
```

```
Address: 192.168.1.254
```

```
Non-authoritative answer:
```

```
ginandjuice.shop      nameserver = ns-1496.awsdns-59.org
```

```
ginandjuice.shop      nameserver = ns-1543.awsdns-00.co.uk
```

```
ginandjuice.shop      nameserver = ns-1000.awsdns-61.net
```

```
ginandjuice.shop      nameserver = ns-110.awsdns-13.com
```

### Question Three

**Command Used:** *whois ginandjuice.shop*

WHOIS is not installed on Windows by default, so whois.exe was downloaded and installed from Microsoft Sysinternals. The website whois.com was used to confirm the results.

#### Who is the registered contact?

The registered contact details are protected and only GoDaddy, the registrar, has access to them.

```
Domain Name: GINANDJUICE.SHOP
Registry Domain ID: D06465675-GMO
Registrar WHOIS Server:
Registrar URL: http://www.godaddy.com
Updated Date: 2024-06-24T18:54:28.0Z
Creation Date: 2022-01-12T09:31:25.0Z
Registry Expiry Date: 2027-01-12T23:59:59.0Z
Registrar: GoDaddy.com LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant State/Province: Arizona
Registrant Country: US
Registrant Email:
Admin Email:
Tech Email:
Name Server: NS-1000.AWSDNS-61.NET
Name Server: NS-110.AWSDNS-13.COM
Name Server: NS-1496.AWSDNS-59.ORG
Name Server: NS-1543.AWSDNS-00.CO.UK
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/whois-inaccuracy-complaint-form
>>> Last update of WHOIS database: 2025-03-04T21:43:04.0Z <<<
```

## ginandjuice.shop

Updated 7 hours ago ↻



### Domain Information

Domain:	ginandjuice.shop
Registered On:	2022-01-12
Expires On:	2027-01-12
Updated On:	2024-06-24
Status:	client renew prohibited client transfer prohibited client update prohibited client delete prohibited
Name Servers:	ns-1000.awsdns-61.net ns-110.awsdns-13.com ns-1496.awsdns-59.org ns-1543.awsdns-00.co.uk



### Registrar Information

Registrar:	GoDaddy.com LLC
IANA ID:	146
Abuse Email:	abuse@godaddy.com

#### Question Four

**Command Used:** *nslookup ginandjuice.shop*

**Command Used:** *nslookup 34.249.203.140*

**Command Used:** *nslookup 34.249.169.176*

**Command Used:** *whois 34.249.203.140*

#### Where is the website hosted?

Hosted by Amazon AWS based in Dublin.

Running nslookup on ginandjuice.shop returns two possible IP addresses, likely for load balancing or redundancy. Running a reverse DNS lookup on the two IPs returns that the servers are owned by Amazon and are part of the EU West 1 group.

Then, ran whois on 34.249.203.140. Running this on Windows did not return the expected results, so whois was used from Kali Linux and confirmed with the WHOIS website.

```
C:\Users\Tim>nslookup ginandjuice.shop
Server: UnKnown
Address: 192.168.1.254

Non-authoritative answer:
Name:    ginandjuice.shop
Addresses: 34.249.203.140
          34.246.169.176
```

```
C:\Users\Tim>nslookup 34.249.203.140
Server: UnKnown
Address: 192.168.1.254

Name:    ec2-34-249-203-140.eu-west-1.compute.amazonaws.com
Address: 34.249.203.140
```

```
C:\Users\Tim>nslookup 34.249.169.176
Server: UnKnown
Address: 192.168.1.254

Name:    ec2-34-249-169-176.eu-west-1.compute.amazonaws.com
Address: 34.249.169.176
```

```
NetRange:      34.248.0.0 - 34.255.255.255
CIDR:          34.248.0.0/13
NetName:       AMAZON-DUB
NetHandle:     NET-34-248-0-0-1
Parent:        AT-88-Z (NET-34-192-0-0-1)
NetType:       Reallocated
OriginAS:      AS16509
Organization:  Amazon Data Services Ireland Limited (ADSIL-1)
RegDate:       2016-11-30
Updated:       2016-11-30
Ref:           https://rdap.arin.net/registry/ip/34.248.0.0
```

```
OrgName:       Amazon Data Services Ireland Limited
OrgId:         ADSIL-1
Address:        Unit 4033, Citywest Avenue Citywest Business Park
City:           Dublin
StateProv:      D24
PostalCode:
Country:        IE
RegDate:        2014-07-18
Updated:        2014-07-18
Ref:           https://rdap.arin.net/registry/entity/ADSIL-1
```

```
NetRange:      34.248.0.0 - 34.255.255.255
CIDR:          34.248.0.0/13
NetName:       AMAZON-DUB
NetHandle:     NET-34-248-0-0-1
Parent:        AT-88-Z (NET-34-192-0-0-1)
NetType:       Reallocated
OriginAS:      AS16509
Organization:  Amazon Data Services Ireland Limited (ADSIL-1)
RegDate:       2016-11-30
Updated:       2016-11-30
Ref:           https://rdap.arin.net/registry/ip/34.248.0.0
```

```
OrgName:       Amazon Data Services Ireland Limited
OrgId:         ADSIL-1
Address:        Unit 4033, Citywest Avenue Citywest Business Park
City:           Dublin
StateProv:      D24
PostalCode:
Country:        IE
RegDate:        2014-07-18
Updated:        2014-07-18
Ref:           https://rdap.arin.net/registry/entity/ADSIL-1
```

## References

Kali Linux. (no date). *Kali Linux – Penetration Testing and Ethical Hacking Linux Distribution*. Available at: <https://www.kali.org/> [Accessed 3 Mar. 2025].

Microsoft. (no date). *Whois v1.20*. Microsoft Learn. Available at: <https://learn.microsoft.com/en-us/sysinternals/downloads/whois#introduction> [Accessed 3 Mar. 2025].

Microsoft. (no date). *nslookup*. Microsoft Learn. Available at: <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup> [Accessed 3 Mar. 2025].

Microsoft. (no date). *tracert*. Microsoft Learn. Available at: <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/tracert> [Accessed 3 Mar. 2025].

Whois.com. (no date). *WHOIS Lookup*. Available at: <https://www.whois.com/whois/> [Accessed 3 Mar. 2025].