Team 1: **Hung Wei Lin, Chan KeiYiu YVone, Thien Liu, Yusuf Fahry**

This scanning activity was performed on macOS. Some of the commands are not applicable to Windows users.

How many hops from your machine to your assigned website?

- There are 17 hops from the local machine to the assigned website

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

- The last two steps (16 and 17) took the longest, with average latency of **337.358ms** and **369.260ms**, respectively.

- Run **traceroute loadedwithstuff.co.uk**

```
) traceroute loadedwithstuff.co.uk
traceroute to loadedwithstuff.co.uk (68.66.247.187), 64 hops max, 52 byte packets
 1  192.168.68.1 (192.168.68.1)  10.909 ms  3.130 ms  4.442 ms
 2  192.168.1.1 (192.168.1.1)  4.277 ms  4.514 ms  4.143 ms
 3  localhost (27.71.251.150)  7.267 ms  7.039 ms  6.283 ms
 4  10.255.40.5 (10.255.40.5)  6.621 ms  6.578 ms
    10.255.40.9 (10.255.40.9)  7.712 ms
 5  * localhost (27.68.210.36)  19.039 ms *
 6  localhost (27.68.237.186)  14.212 ms
    localhost (27.68.237.138)  6.896 ms
    localhost (27.68.237.140)  8.003 ms
 7  localhost (27.68.250.169)  31.881 ms  30.094 ms  30.307 ms
 8  xe-2-2-3-xcr1.hke.cw.net (195.89.113.21)  33.172 ms  31.858 ms  31.811 ms
 9  ae4-xcr1.hkg.cw.net (195.2.10.97)  186.599 ms
    ae0-xcr2.lax.cw.net (195.2.8.142)  189.536 ms  188.901 ms
10  ae2-xcr1.tyo.cw.net (195.2.10.18)  182.678 ms  185.149 ms
    telia-gw.lax.cw.net (195.2.22.74)  186.271 ms
11  ae8-xcr1.mry.cw.net (195.2.28.162)  82.184 ms  80.482 ms
    rest-bb1-link.ip.twelve99.net (62.115.114.87)  286.126 ms
12  prs-bb1-link.ip.twelve99.net (62.115.112.243)  306.103 ms
    ae7-xcr1.lax.cw.net (195.2.28.1)  179.109 ms
    prs-bb1-link.ip.twelve99.net (62.115.112.243)  331.826 ms
13  telia-gw.lax.cw.net (195.2.22.74)  183.161 ms
    adm-bb3-link.ip.twelve99.net (62.115.134.96)  267.692 ms  265.837 ms
14  adm-b10-link.ip.twelve99.net (62.115.120.227)  305.016 ms
    ash-bb2-link.ip.twelve99.net (62.115.121.221)  306.898 ms
    rest-bb1-link.ip.twelve99.net (62.115.114.87)  306.698 ms
15  a2hosting-svc080530-ic370345.ip.twelve99-cust.net (62.115.145.217)  337.517 ms
    prs-bb2-link.ip.twelve99.net (62.115.122.158)  275.539 ms  306.272 ms
16  adm-bb3-link.ip.twelve99.net (62.115.134.96)  263.233 ms
    v401.r1.nl1.a2webhosting.com (209.124.94.237)  337.339 ms  337.377 ms
17  68.66.247.187.static.a2webhosting.com (68.66.247.187)  340.758 ms  340.411 ms  426.612 ms
```

What are the main nameservers for the website?

- ns3.a2hosting.com.
- ns1.a2hosting.com.
- ns4.a2hosting.com.
- ns2.a2hosting.com.

There are several ways to get the name servers for a website

- Run **host -t ns loadedwithstuff.co.uk**

```
❯ host -t ns loadedwithstuff.co.uk
loadedwithstuff.co.uk name server ns3.a2hosting.com.
loadedwithstuff.co.uk name server ns1.a2hosting.com.
loadedwithstuff.co.uk name server ns2.a2hosting.com.
loadedwithstuff.co.uk name server ns4.a2hosting.com.
```

- Run **dig ns loadedwithstuff.co.uk**

```
❯ dig ns loadedwithstuff.co.uk

; <<>> DiG 9.10.6 <<>> ns loadedwithstuff.co.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32022
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;loadedwithstuff.co.uk.         IN      NS

;; ANSWER SECTION:
loadedwithstuff.co.uk.  86400   IN      NS      ns3.a2hosting.com.
loadedwithstuff.co.uk.  86400   IN      NS      ns1.a2hosting.com.
loadedwithstuff.co.uk.  86400   IN      NS      ns4.a2hosting.com.
loadedwithstuff.co.uk.  86400   IN      NS      ns2.a2hosting.com.

;; ADDITIONAL SECTION:
ns1.a2hosting.com.      99767   IN      A       162.159.25.95
ns2.a2hosting.com.      115286  IN      A       162.159.24.221
ns3.a2hosting.com.      159993  IN      A       162.159.25.82
ns4.a2hosting.com.      99767   IN      A       162.159.24.227

;; Query time: 277 msec
;; SERVER: 10.255.255.3#53(10.255.255.3)
;; WHEN: Sat Mar 26 18:10:45 +07 2022
;; MSG SIZE  rcvd: 390
```

- Even more details, run **dig +trace loadedwithstuff.co.uk** to find the delegation path from the root name servers

```
❯ dig +trace loadedwithstuff.co.uk

; <<>> DiG 9.10.6 <<>> +trace loadedwithstuff.co.uk
;; global options: +cmd
.                       518400  IN      NS      L.ROOT-SERVERS.NET.
.                       518400  IN      NS      G.ROOT-SERVERS.NET.
.                       518400  IN      NS      M.ROOT-SERVERS.NET.
.                       518400  IN      NS      E.ROOT-SERVERS.NET.
.                       518400  IN      NS      C.ROOT-SERVERS.NET.
.                       518400  IN      NS      I.ROOT-SERVERS.NET.
.                       518400  IN      NS      B.ROOT-SERVERS.NET.
.                       518400  IN      NS      D.ROOT-SERVERS.NET.
.                       518400  IN      NS      K.ROOT-SERVERS.NET.
.                       518400  IN      NS      A.ROOT-SERVERS.NET.
.                       518400  IN      NS      J.ROOT-SERVERS.NET.
.                       518400  IN      NS      F.ROOT-SERVERS.NET.
.                       518400  IN      NS      H.ROOT-SERVERS.NET.
;; Received 1471 bytes from 10.255.255.3#53(10.255.255.3) in 225 ms

uk.                     172800  IN      NS      nsa.nic.uk.
uk.                     172800  IN      NS      nsb.nic.uk.
uk.                     172800  IN      NS      nsc.nic.uk.
uk.                     172800  IN      NS      nsd.nic.uk.
uk.                     172800  IN      NS      dns1.nic.uk.
uk.                     172800  IN      NS      dns2.nic.uk.
uk.                     172800  IN      NS      dns3.nic.uk.
uk.                     172800  IN      NS      dns4.nic.uk.
uk.                     86400   IN      DS      43876 8 2 A107ED2AC1BD14D924173BC7E827A1153582072394F9272BA37E
2353 BC659603
uk.                     86400   IN      RRSIG   DS 8 1 86400 20220408050000 20220326040000 9799 . RiRorhbNsHSa
ATC1AiCxi5XIIMY5olsiFPPpSxkdDl9Z5Sn/o658Gegk Le1jSyNzw+VnRrqHtECS0EVMjk1aZ0BEhqsjmn7LtxUm9CaNhoIscEPk e34aKaN1
kuMl/Z0BNb16xHqO8qjq6PKhIB+bJIcu6Sdc7qE2ujWOI6V1 dn1AHF8Of9tL03hyEqinTpzm46LAYeSyE5fCq0ZR1W20eU8P/NhHFV+7 C9pG
b+7v62BMHVp/T6oVIrB1pBrV82sRCO6CG6ZoiqhwEFymxgG4qElg KEtbWy4Tgzc51d6hrI2Nmjqz4ZTCITbbHed1cwGliXKHCCqz+uysTX1a
VObTtw==
;; Received 889 bytes from 198.97.190.53#53(H.ROOT-SERVERS.NET) in 69 ms

loadedwithstuff.co.uk.  172800  IN      NS      ns4.a2hosting.com.
loadedwithstuff.co.uk.  172800  IN      NS      ns1.a2hosting.com.
loadedwithstuff.co.uk.  172800  IN      NS      ns2.a2hosting.com.
loadedwithstuff.co.uk.  172800  IN      NS      ns3.a2hosting.com.
G9F1KIIHM8M9VHJK7LRVETBQCEOGJIQP.co.uk. 10800 IN NSEC3 1 1 0 - G9F3NQ74NTIT1D6QSRKCCS86R4T7H1MD  NS SOA RRSIG
DNSKEY NSEC3PARAM TYPE65534
G9F1KIIHM8M9VHJK7LRVETBQCEOGJIQP.co.uk. 10800 IN RRSIG NSEC3 8 3 10800 20220430034515 20220326033255 33621 co.
uk. RVjqxVDcnyf3sfkCwSAwqGI9Uhl3bh/GsJ6/6GWKLXCsVypAWX3NIb7g /OApgsiq2kOxDBmO6i9BaIk1jxgotRBmR8Yz3y3zvs7GecTJ2
v8e697R q1823Z2pFWbhud4ceKPKl77/uJw/dDJe1iPTTmWNprNJ7G5bc572ofsi tp4=
B7LVCSR8VPKOAUTELL0MFBASMN5FVDJQ.co.uk. 10800 IN NSEC3 1 1 0 - B7MK3R0KTLS3UCG131036DGSVSSP27NC  NS DS RRSIG
B7LVCSR8VPKOAUTELL0MFBASMN5FVDJQ.co.uk. 10800 IN RRSIG NSEC3 8 3 10800 20220424133433 20220320125808 33621 co.
uk. rUd87HJ0mZlySPcmnl5O83DUvhD6kDJAYzms3MRGBXyGrJ99xSF44HmS Nrz1teH/8EhjoRQ4zZ0qjtQ+Dn85fNdnRkv2cady8/rwUsqJD
LOL7wbH yFOctDOQqiUBPSSul3D8P5sKhxUgSgL6a9ruzwq+RuQ6PFb8J67Ty+WN 0Cw=
;; Received 658 bytes from 156.154.102.3#53(nsc.nic.uk) in 33 ms

loadedwithstuff.co.uk.  14400   IN      A       68.66.247.187
;; Received 66 bytes from 162.159.24.227#53(ns4.a2hosting.com) in 34 ms
```

Who is the registered contact?

- The registered contact of the website can be found by running the following command. Please be noted that the real registration info could be anonymous if private registration is enabled by the domain registrar.
- Run **whois loadedwithstuff.co.uk**

```
❯ whois loadedwithstuff.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 A107ED2AC1BD14D924173BC7E827A1153582072394F9272BA37E2353BC659603

whois:        whois.nic.uk

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

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

What is the MX record for the website?

- Run **dig mx loadedwithstuff.co.uk**

```
❯ dig mx loadedwithstuff.co.uk

; <<>> DiG 9.10.6 <<>> mx loadedwithstuff.co.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62550
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;loadedwithstuff.co.uk.         IN      MX

;; ANSWER SECTION:
loadedwithstuff.co.uk.  14400   IN      MX      0 mail.loadedwithstuff.co.uk.

;; Query time: 234 msec
;; SERVER: 10.255.255.3#53(10.255.255.3)
;; WHEN: Sat Mar 26 18:25:57 +07 2022
;; MSG SIZE  rcvd: 113
```

Where is the website hosted?

- The website is hosted at A2 Hosting, with the IP public address of **68.66.247.187**
- There are 2 steps needed to reveal the address where the website is hosted
    - Run **nslookup loadedwithstuff.co.uk**, this command will return the website's public IP address.

```
❯ nslookup loadedwithstuff.co.uk
Server:         10.255.255.3
Address:        10.255.255.3#53

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

    - Run whois <the_ip_address_from_the_command_above>. In this case, the IP address is **68.66.247.187**

```
❯ whois 68.66.247.187
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.arin.net

inetnum:      68.0.0.0 - 68.255.255.255
organisation: ARIN
status:       ALLOCATED

whois:        whois.arin.net

changed:      2001-06
source:       IANA

# whois.arin.net

NetRange:       68.66.212.0 - 68.66.255.255
CIDR:           68.66.216.0/21, 68.66.224.0/19, 68.66.212.0/22
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


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:        2022-01-04
Comment:        http://www.a2hosting.com
Ref:            https://rdap.arin.net/registry/entity/A2HOS
```

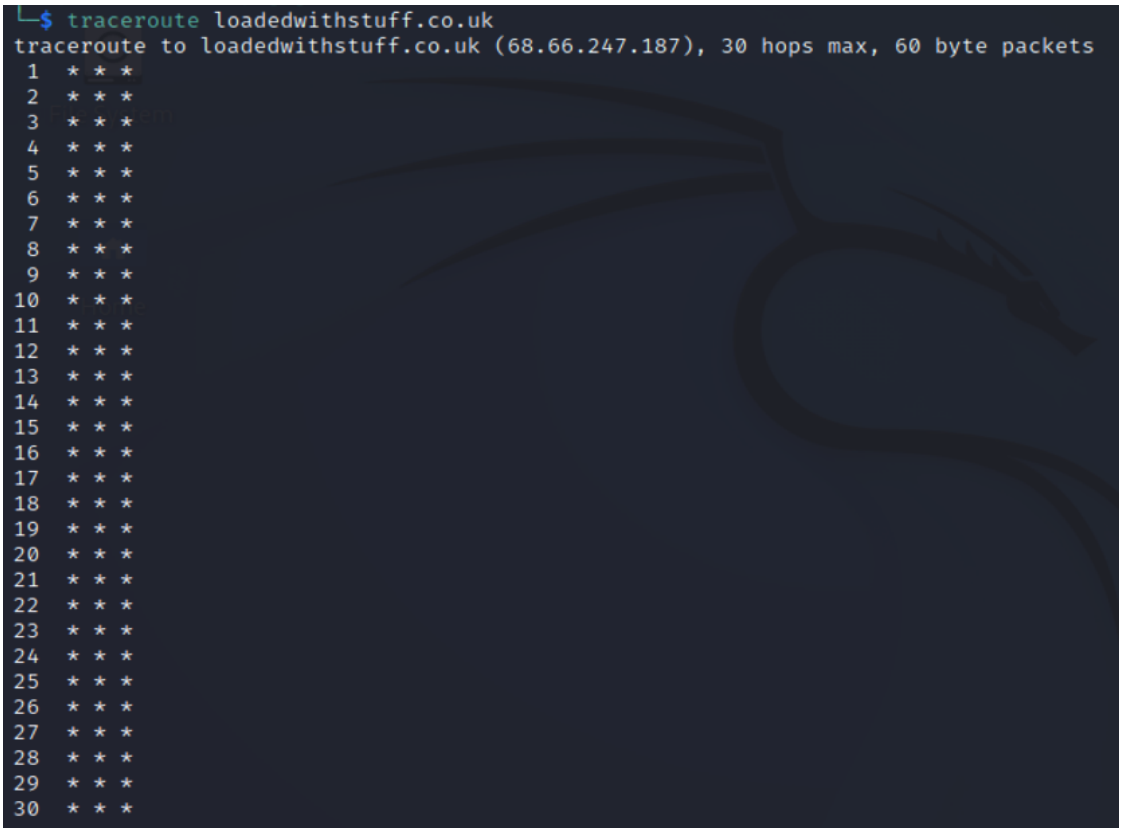
```
OrgTechHandle: FITEJ4-ARIN
OrgTechName:   Fite, Joe
OrgTechPhone:  +1-734-222-4678
OrgTechEmail:  jfite@a2hosting.com
OrgTechRef:    https://rdap.arin.net/registry/entity/FITEJ4-ARIN

OrgTechHandle: FATHA-ARIN
OrgTechName:   Fath-Azam, Siena
OrgTechPhone:  +1-734-222-4678
OrgTechEmail:  sfathazam@a2hosting.com
OrgTechRef:    https://rdap.arin.net/registry/entity/FATHA-ARIN

OrgAbuseHandle: NETWO5169-ARIN
OrgAbuseName:   Network Operations
OrgAbusePhone:  +1-734-222-4678
OrgAbuseEmail:  abuse@a2hosting.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/NETWO5169-ARIN

OrgTechHandle: NETWO8213-ARIN
OrgTechName:   Network Operations
OrgTechPhone:  +1-734-222-4678
OrgTechEmail:  noc@a2hosting.com
OrgTechRef:    https://rdap.arin.net/registry/entity/NETWO8213-ARIN

OrgNOCHandle: NETWO8213-ARIN
OrgNOCName:   Network Operations
OrgNOCPhone:  +1-734-222-4678
OrgNOCEmail:  noc@a2hosting.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/NETWO8213-ARIN

OrgTechHandle: RUBIO60-ARIN
OrgTechName:   RUBIO-DORSEY, CHASE
OrgTechPhone:  +1-410-294-2401
OrgTechEmail:  crd1113@gmail.com
OrgTechRef:    https://rdap.arin.net/registry/entity/RUBIO60-ARIN

OrgTechHandle: MACNI2-ARIN
OrgTechName:   MacNish, Matthew
OrgTechPhone:  +1-734-222-4678
OrgTechEmail:  mmacnish@a2hosting.com
OrgTechRef:    https://rdap.arin.net/registry/entity/MACNI2-ARIN
```

Challenges

- Setting up a Kali Linux is the first challenge. Initially, running the **traceroute** command on Kali only returns 1 hop. At the end of the day, we discovered that the Bridge Network Adapter should be used instead of Shared Network Adapter to enable proper network connection. Moreover, most of the scanning tools are available on macOS, or at least they can be easily installed. As a result, all the activities were performed using a Mac machine.

```
└─$ traceroute loadedwithstuff.co.uk
traceroute to loadedwithstuff.co.uk (68.66.247.187), 30 hops max, 60 byte packets
 1  68.66.247.187.static.a2webhosting.com (68.66.247.187)  269.790 ms  271.481 ms *
```

- After a few scanning activities, the website recognized unusual traffic then blocked the detected IP address, we had to bypass the security gateway on the website to complete the scanning. The below image illustrates the situation when the website blocked the traffic from our local IP address, all the connections were timeout



References:

A2hosting.com. (2019). *How To Use Ping Test & Tracert For Network Troubleshooting*. [online] Available at: https://www.a2hosting.com/kb/getting-started-guide/internet-and-networking/troubleshooting-network-connectivity-with-ping-and-traceroute.