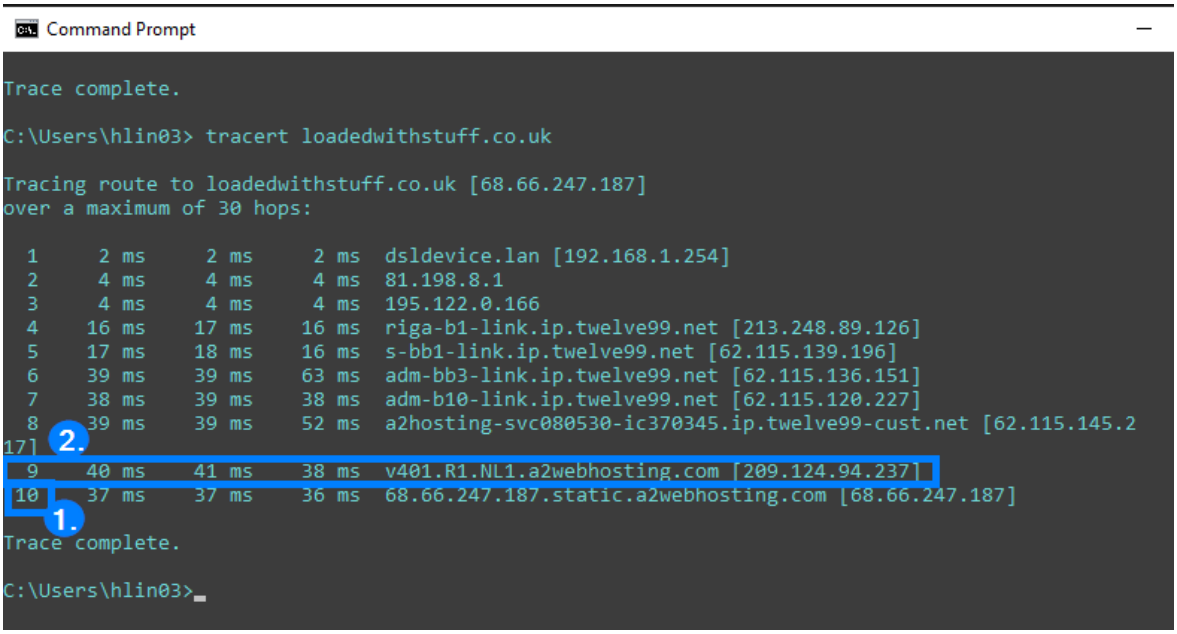
Team 1: **Hung Wei Lin**

Practical Activity - Scanning Exercise

Perform a basic scan using standard tools such as traceroute (not ICMP version). Use these basic tools to compile a list that details the following information:

I am using window10 to run the traceroute and below is the result:

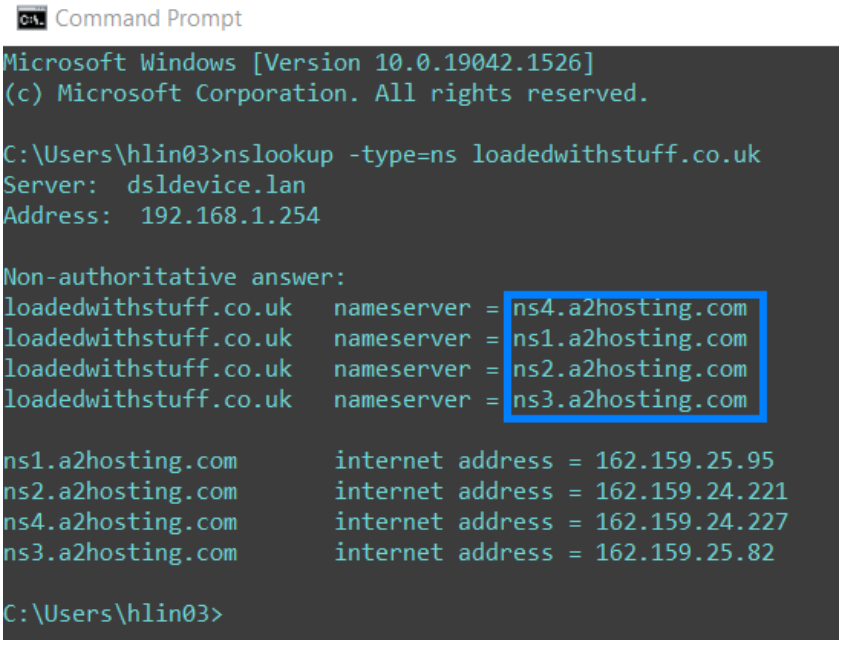


1. **How many hops from your machine to your assigned website?**
   There are 10 hops to get to the assigned website.

2. **Which step causes the biggest delay in the route? What is the average duration of that delay?**
   - The 9th step.
   - The average duration of the delay is 39.66 ms.

-

3. **What are the main nameservers for the website?**
   - ns4.a2hosting.com
   - ns1.a2hosting.com
   - ns2.a2hosting.com
   - ns3.a2hosting.com



4. **Who is the registered contact?**
   eNom LLC

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

Command Prompt

```
C:\Users\hlin03>nslookup -q=MX loadedwithstuff.co.uk
Server:  dsldevice.lan
Address:  192.168.1.254

Non-authoritative answer:
loadedwithstuff.co.uk   MX preference = 0, mail exchanger = mail.loadedwithstuff.co.uk

loadedwithstuff.co.uk   nameserver = ns4.a2hosting.com
loadedwithstuff.co.uk   nameserver = ns1.a2hosting.com
loadedwithstuff.co.uk   nameserver = ns3.a2hosting.com
loadedwithstuff.co.uk   nameserver = ns2.a2hosting.com
mail.loadedwithstuff.co.uk      internet address = 68.66.247.187
ns2.a2hosting.com       internet address = 162.159.24.221
ns3.a2hosting.com       internet address = 162.159.25.82
ns1.a2hosting.com       internet address = 162.159.25.95
ns4.a2hosting.com       internet address = 162.159.24.227

C:\Users\hlin03>
```

6. **Where is the website hosted?**

The IP address is 68.66.247.187. (The address can be found from the command run for the first question)

Command Prompt

```
Trace complete.

C:\Users\hlin03> tracert loadedwithstuff.co.uk

Tracing route to loadedwithstuff.co.uk [68.66.247.187]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  dsldevice.lan [192.168.1.254]
  2     4 ms     4 ms     4 ms  81.198.8.1
  3     4 ms     4 ms     4 ms  195.122.0.166
  4    16 ms    17 ms    16 ms  riga-b1-link.ip.twelve99.net [213.248.89.126]
  5    17 ms    18 ms    16 ms  s-bb1-link.ip.twelve99.net [62.115.139.196]
  6    39 ms    39 ms    63 ms  adm-bb3-link.ip.twelve99.net [62.115.136.151]
  7    38 ms    39 ms    38 ms  adm-b10-link.ip.twelve99.net [62.115.120.227]
  8    39 ms    39 ms    52 ms  a2hosting-svc080530-ic370345.ip.twelve99-cust.net [62.115.
17]
  9    40 ms    41 ms    38 ms  v401.R1.NL1.a2webhosting.com [209.124.94.237]
 10    37 ms    37 ms    36 ms  68.66.247.187.static.a2webhosting.com [68.66.247.187]

Trace complete.

C:\Users\hlin03>
```

Team activity

Discuss the results of your scans and answer the following questions with your teammates before Seminar 2.

- **Did you have any issues or challenges with the scans?**
  Challenge – I might have confusion about the question 2 in the Practical Activity. What is the correct way to calculate the duration of the delay?

- **How did you overcome them?**
  I tried to search for the answer to my confusion from the internet resources. Below is the resource I found which is related to the topic. I assume the "latency" in the article might refer to delay
  'This is the amount of time it takes, in milliseconds, for a packet to get to the hop and back to your computer. This is often referred to as latency, ... Traceroute sends three packets to each hop and displays each elapsed time so you can measure how consistent or inconsistent the latency is at that time.' (SugarCRM, 2019)

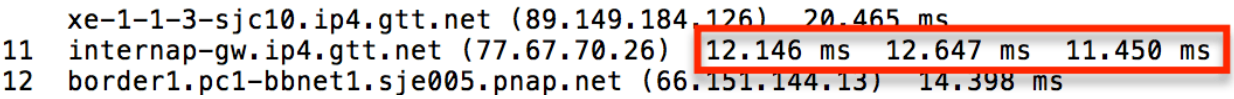


Figure 1: Traceroute Results - RTT1, RTT2, RTT3 (SugarCRM, 2019)

- **How will they affect your final report?**
  The different definition of the delay may end up different ways of calculation. It may cause the differences of the final delay values and further affect the study result.

Reference

SugarCRM (2019). Troubleshooting Latency Using Traceroute. [online] Available at: https://support.sugarcrm.com/Knowledge_Base/Troubleshooting/Troubleshooting_Latency_Using_Traceroute/ [Assessed 26 March 2022]