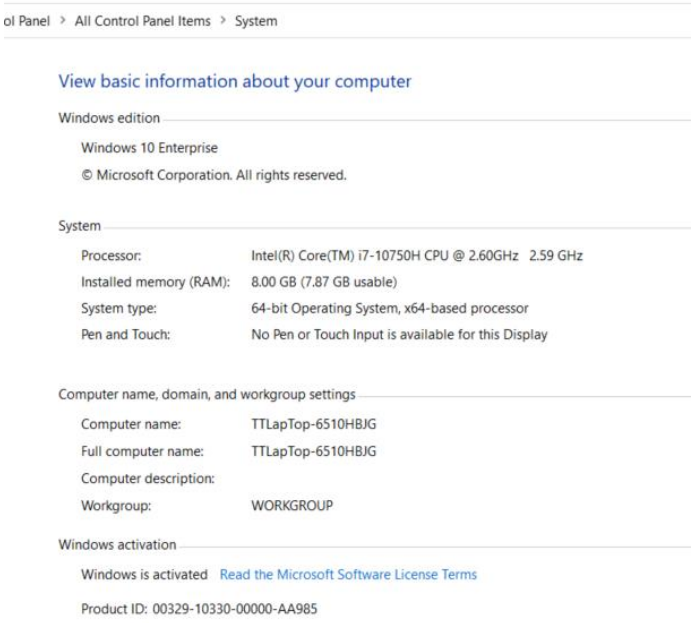
Name: Waris Damkham_____Sec:__1__ID:6388014_____P1

ITCS420 Computer Networks

Lab1 Answer Sheet

Your operating system and version: Windows 10 Education



Exercise1

You type the command "ipconfig /all".

Case 1: If you use a desktop computer at the ICT computer lab, see at the "Ethernet adapter Local Area Connection"

Case 2: If you use laptop computer at home, you may see at the Wireless LAN adapter Wi-Fi.

Answer the following questions.

1. What is the IP address of your computer?
   Answer: _____10.34.14.92_____
2. What is the subnet mask?
   Answer: _____255.255.255.0_____
3. What is the default gateway of your computer?
   Answer: _____10.34.14.254_____
4. What is your Connection-specific DNS suffix?
   Answer: _____ict.mahidol.ac.th_____
5. What is the IP addresses of DNS servers?
   Answer:_____10.34.101.101_____
6. What is your link local IPv6 address?
   Answer:_____ fe80::51a0:eee6:d698:cc70%7_____

Name: Waris Damkham_____Sec:__1__ID:6388014_____P2

7. What is the physical address or MAC address of your LAN/ Wi-Fi?

   Answer:_____ 9C-7B-EF-44-FF-EE _____

8. What is the IP address of DHCP server?

   Answer:_____10.34.101.4_____

Execute the "ipconfig /displaydns" command and answer following questions.

9. What is the IP address of "mycourses.ict.mahidol.ac.th"?

   Answer: _____10.34.101.50_____

10. What is the IP address of "google.com"?

    Answer: _____216.58.221.195_____

11. What is the purpose of the command "ipconfig /displaydns"?

    Answer: displays the contents of the DNS client resolver cache

12. Find the MTU for your LAN/Wi-Fi interface.

     netsh interface ipv4 show interfaces

     ifconfig

    Answer: _____1500 bytes_____

Name: Waris Damkham Sec: 1 ID:6388014 P3

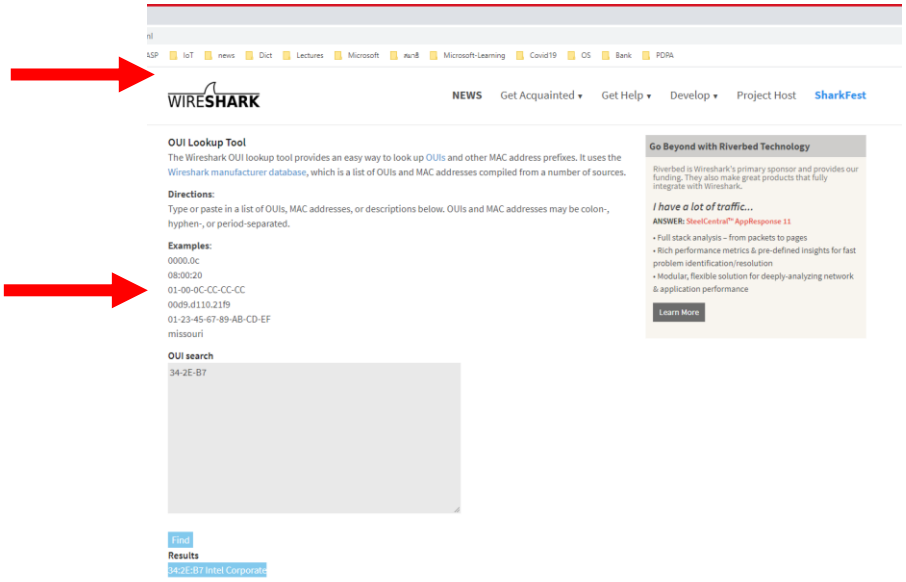
Try to find the company that produced these network devices by performing one of the following:

Look for the company name from their MAC addresses. Use the following URL to search from the IEEE OUI and IAB database.

https://www.wireshark.org/tools/oui-lookup.html or http://aruljohn.com/mac.pl

For example, the MAC address in the above figure for the interface bge0 is "00:04:76:f7:e4:06". The OUI number (company ID) is the first 3 bytes. Therefore, it should be "00:04:76". So, input **00-04-76** into the searching box.

Put the screen output of the searching result in your report.



Exercise2

1. What is the MAC address of your Windows's LAN/WiFi? (from Exercise 1-7)
   Answer: 9C-7B-EF-44-FF-EE
2. After looking at the IEEE database, which company manufactured this LAN/WiFi?
   Answer: Hewlett Packard

Name: Waris Damkham_____Sec:__1__ID:6388014_____P4

PING

Ping indicates whether a remote host can be reached. Ping also displays information about packet loss and packet delivery time.

Normal Usage: send four packets (default IPv4)

Note: *target_host* is your IP gateway or any other websites.

Usage: ping *target_host*

```
C:\> ping  10.34.21.254
```

Ping IPv6

```
C:\> ping  -6  <your IPv6 address>
```

For the Linux

```
$ ping  10.34.21.254
```

This command will send the ping packet forever, so you have to stop it by using Ctrl+C (control-c).

Send ping packets for *count* times

Usage: ping -n *count* *target_host*

Example:

```
C:\> ping  -n  50  10.34.21.254
```

Send ping packets with a specific buffer size (byte)

Usage: ping -l *size* *target_host*

Example:

```
C:\> ping  -l  100  10.34.21.254
```

```
C:\> ping  -t  100  10.34.21.254
```

This command will send the ping packet forever, so you have to stop it by using Ctrl+C (control-c).

Name: Waris Damkham_____Sec: 1 ID:6388014_____P5

Use wireshark to explore IP datagram and fragmentation

```
C:\> ping   -l   4000   10.34.21.254
```

Open wireshark program before you start ping command and other network utility tools. Use the filter like icmp or ip.addr==<your system IP address> to see how ping or traceroute/tracert works out.

Exercise 3

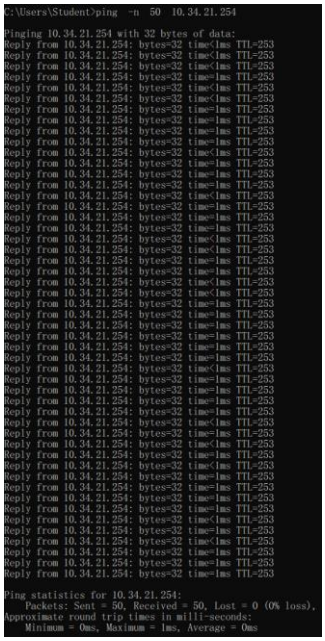
Type all commands above and write the outputs of each.
Note: All commands and their results are from capturing the screen e.g. copy by “PrtSc” and and paste by “ctrl-v”.

Use wireshark with ping -l 4000 <gateway>
Capture the output and show only the packets representing ping.
Show the IP header with MF (more flagment) and offsets.
How many are fragments for 4000 bytes?

ping 10.34.21.254

```
C:\Users\Student>ping 10.34.21.254

Pinging 10.34.21.254 with 32 bytes of data:
Reply from 10.34.21.254: bytes=32 time<1ms TTL=253
Reply from 10.34.21.254: bytes=32 time=1ms TTL=253
Reply from 10.34.21.254: bytes=32 time<1ms TTL=253
Reply from 10.34.21.254: bytes=32 time<1ms TTL=253

Ping statistics for 10.34.21.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

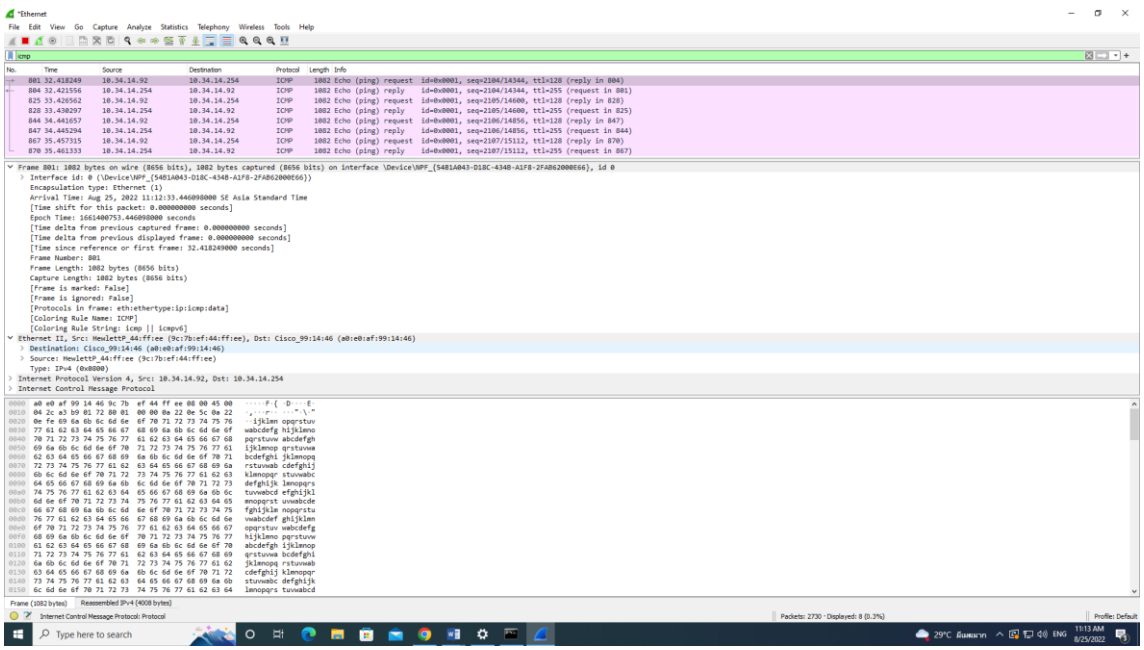
ping -n 50 10.34.21.254



ITCS420-2022: Lab 1: Answer sheet

Name: Waris Damkham_____Sec:___1___ID:6388014_____P6

```
C:\Users\Student>ping  -l  100  10.34.21.254

Pinging 10.34.21.254 with 100 bytes of data:
Reply from 10.34.21.254: bytes=100 time<1ms TTL=253
Reply from 10.34.21.254: bytes=100 time=1ms TTL=253
Reply from 10.34.21.254: bytes=100 time<1ms TTL=253
Reply from 10.34.21.254: bytes=100 time=1ms TTL=253

Ping statistics for 10.34.21.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Student>ping  -l  4000  10.34.21.254

Pinging 10.34.21.254 with 4000 bytes of data:
Reply from 10.34.21.254: bytes=4000 time=1ms TTL=253
Reply from 10.34.21.254: bytes=4000 time<1ms TTL=253
Reply from 10.34.21.254: bytes=4000 time=1ms TTL=253
Reply from 10.34.21.254: bytes=4000 time=1ms TTL=253

Ping statistics for 10.34.21.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



Name: Waris Damkham Sec: 1 ID:6388014 P7

TRACERT (PATHPING)

"Tracert" is a command in the Microsoft Windows, while "traceroute" is a command in the UNIX systems. Both of them prints information about each routing hop that packets take going from your system to a remote system.

Windows Usage: tracert *target_host*

```
C:\> tracert   10.22.5.254
C:\> tracert   www.mahidol.ac.th
```

Unfortunately, according to Mahidol's network policy, we are trying to block the ICMP packets for security reasons. So, it is mostly difficult to trace to the destination even the path to that destination is available.

However, if you stay at home, you can use traceroute.

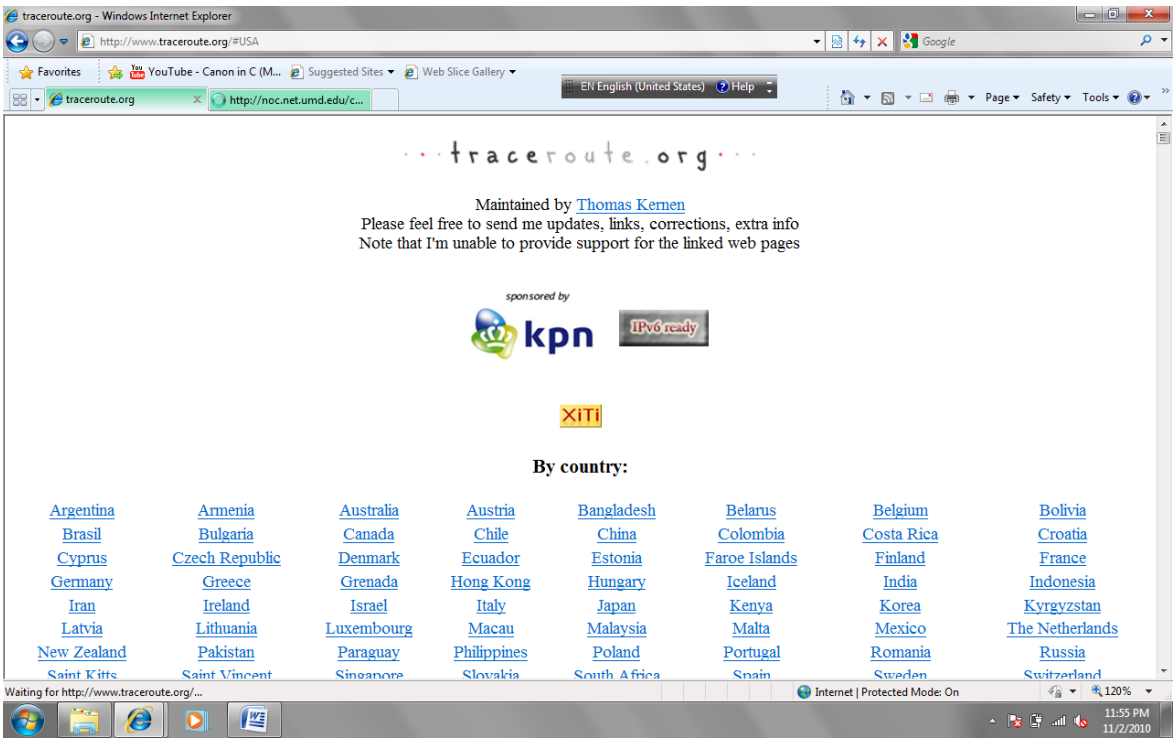
Note: There are some available traceroute websites like:

https://network-tools.com/

https://www.uptrends.com/tools/traceroute

https://tools.keycdn.com/traceroute

Another option to see how the traceroute program works is to use the Web-based program http://www.traceroute.org



Name: Waris Damkham_____Sec:__1__ID:6388014_____P8

Select Traceroute from USA → Princeton University or Univ of Wisconsin-Madison or https://www.net.princeton.edu/traceroute.html

Get the screen output of the tracing result and put it in your report.

Traceroute

tracing path from www.net.princeton.edu to 202.28.152.207 ...

```
traceroute to 202.28.152.207 (202.28.152.207), 30 hops max, 40 byte packets
 1  core-ns-router (128.112.128.2)  0.962 ms  0.914 ms  0.764 ms
 2  rtr-core-east-router.princeton.edu (128.112.12.225)  0.867 ms  0.763 ms  0.620 ms
 3  fw-border-87-router.princeton.edu (128.112.12.10)  1.045 ms  1.045 ms  0.982 ms
 4  rtr-border-87-router.princeton.edu (204.153.48.1)  1.506 ms  1.480 ms  1.478 ms
 5  130.156.252.57 (130.156.252.57)  3.275 ms  3.165 ms  3.162 ms
 6  130.156.35.46 (130.156.35.46)  6.915 ms  6.574 ms  3.994 ms
 7  130.156.35.13 (130.156.35.13)  6.380 ms  6.397 ms  6.093 ms
 8  130.156.35.65 (130.156.35.65)  3.892 ms  3.931 ms 130.156.34.189 (130.156.34.189)  4.150 ms
 9  be-107-2005-pe01.60hudson.ny.ibone.comcast.net (96.87.9.157)  4.837 ms  4.762 ms  4.555 ms
10  be-4301-cs03.newyork.ny.ibone.comcast.net (96.110.41.153)  5.050 ms be-4201-cs02.newyork.ny.ibone.comcast.net (96.110.41.149)  5.005 ms be-4101-cs01.newyork.ny.ibone.comcast.net (96.110.41.145)  5.356 ms
11  be-1411-cr11.newyork.ny.ibone.comcast.net (96.110.35.126)  5.380 ms be-1311-cr11.newyork.ny.ibone.comcast.net (96.110.35.122)  5.602 ms be-1211-cr11.newyork.ny.ibone.comcast.net (96.110.35.118)  5.224 ms
12  be-302-cr12.350ecermak.il.ibone.comcast.net (96.110.38.69)  21.784 ms be-301-cr12.350ecermak.il.ibone.comcast.net (96.110.38.65)  21.798 ms  21.802 ms
13  be-1212-cs02.350ecermak.il.ibone.comcast.net (96.110.35.21)  21.328 ms  21.846 ms  21.118 ms
14  be-1411-cr11.350ecermak.il.ibone.comcast.net (96.110.35.14)  21.837 ms be-1211-cr11.350ecermak.il.ibone.comcast.net (96.110.35.6)  21.894 ms  21.520 ms
15  be-301-cr11.1601milehigh.co.ibone.comcast.net (96.110.37.146)  50.027 ms  50.329 ms be-303-cr11.1601milehigh.co.ibone.comcast.net (96.110.37.154)  49.407 ms
16  be-1311-cs03.1601milehigh.co.ibone.comcast.net (96.110.39.73)  49.347 ms be-1111-cs01.1601milehigh.co.ibone.comcast.net (96.110.39.65)  49.520 ms be-1211-cs02.1601milehigh.co.ibone.comcast.net (96.110.39.69)  50.219 ms
17  be-1214-cr14.1601milehigh.co.ibone.comcast.net (96.110.39.118)  49.508 ms  49.668 ms be-1313-cr13.1601milehigh.co.ibone.comcast.net (96.110.39.106)  49.612 ms
18  * be-301-cr14.champa.co.ibone.comcast.net (96.110.39.1)  49.811 ms be-303-cr14.champa.co.ibone.comcast.net (96.110.39.9)  49.374 ms
19  be-1213-cs02.champa.co.ibone.comcast.net (96.110.37.229)  50.281 ms be-1414-cs04.champa.co.ibone.comcast.net (96.110.37.253)  50.003 ms  49.787 ms
20  be-1212-cr12.champa.co.ibone.comcast.net (96.110.37.214)  49.923 ms be-1312-cr12.champa.co.ibone.comcast.net (96.110.37.218)  50.426 ms  49.947 ms
21  be-302-cr11.sunnyvale.ca.ibone.comcast.net (96.110.39.22)  69.701 ms be-301-cr11.sunnyvale.ca.ibone.comcast.net (96.110.39.18)  69.076 ms be-304-cr11.sunnyvale.ca.ibone.comcast.net (96.110.39.30)  69.986 ms
22  be-1411-cs04.sunnyvale.ca.ibone.comcast.net (96.110.46.37)  69.754 ms be-1311-cs03.sunnyvale.ca.ibone.comcast.net (96.110.46.25)  69.909 ms  69.713 ms
23  be-1212-cr12.sunnyvale.ca.ibone.comcast.net (96.110.46.18)  69.801 ms be-1112-cr12.sunnyvale.ca.ibone.comcast.net (96.110.46.6)  69.701 ms be-1212-cr12.sunnyvale.ca.ibone.comcast.net (96.110.46.18)  69.055 ms
24  be-304-cr12.9greatoaks.ca.ibone.comcast.net (96.110.37.182)  69.905 ms  69.576 ms be-301-cr12.9greatoaks.ca.ibone.comcast.net (96.110.37.170)  69.758 ms
25  be-1112-cs01.9greatoaks.ca.ibone.comcast.net (68.86.166.133)  70.247 ms be-1312-cs03.9greatoaks.ca.ibone.comcast.net (68.86.166.157)  69.923 ms be-1212-cs02.9greatoaks.ca.ibone.comcast.net (68.86.166.145)  69.570 ms
26  be-2101-pe01.9greatoaks.ca.ibone.comcast.net (96.110.36.218)  69.516 ms  69.440 ms  69.366 ms
27  50.242.150.146 (50.242.150.146)  69.410 ms  69.436 ms  69.313 ms
28  mx-ll-110.164.0-44.static.3bb.co.th (110.164.0.44)  221.508 ms mx-ll-110.164.0-84.static.3bb.co.th (110.164.0.84)  238.002 ms mx-ll-110.164.0-44.static.3bb.co.th (110.164.0.44)  222.729 ms
29  mx-ll-110.164.0-115.static.3bb.co.th (110.164.0.115)  248.936 ms mx-ll-110.164.0-144.static.3bb.co.th (110.164.0.144)  257.054 ms mx-ll-110.164.0-115.static.3bb.co.th (110.164.0.115)  248.651 ms
30  * * *
```

Done.

Name: Waris Damkham_____Sec:__1__ID:6388014_____P9

Exercise 4:

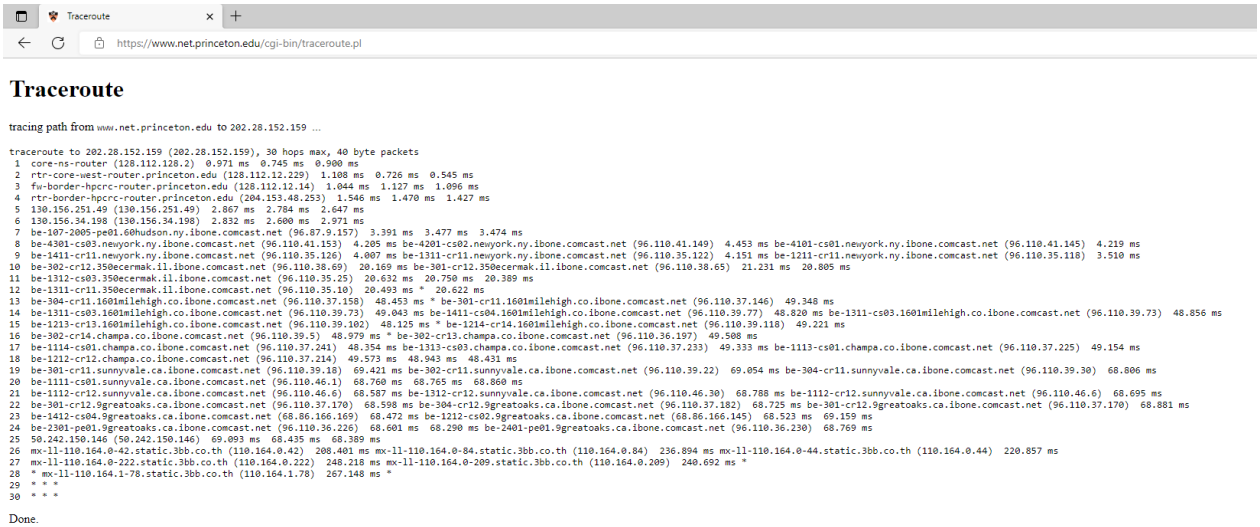
1. Type the command "tracert www.ict.mahidol.ac.th" in the command prompt of Windows/MACOS machine. Get the screen output.

```
C:\Users\Student>tracert www.ict.mahidol.ac.th

Tracing route to www.ict.mahidol.ac.th [10.34.101.80]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  10.34.14.254
  2    <1 ms    <1 ms    <1 ms  10.34.166.1
  3    <1 ms    <1 ms    <1 ms  10.34.101.80

Trace complete.
```

2. How many routers or hops your packets have to pass through when sent from your computer to the www.ict.mahidol.ac.th?
   Answer: _____3_____

3. Totally how many mili-seconds required in average for sending the packet in round trip from your computer to the www.ict.mahidol.ac.th?
   Answer: _____1.33 ms_____

4. Go to the web site www.traceroute.org. Select a server from any country you like or https://www.net.princeton.edu/traceroute.html. Then, perform traceroute from their server to www.ict.mahidol.ac.th. Get the screen outputs. > … ms
   Ans 267.148 ms



Traceroute

https://www.net.princeton.edu/cgi-bin/traceroute.pl

Traceroute

tracing path from www.net.princeton.edu to 202.28.152.159 ...

```
traceroute to 202.28.152.159 (202.28.152.159), 30 hops max, 40 byte packets
 1  core-ns-router (128.112.128.2)  0.971 ms  0.745 ms  0.900 ms
 2  rtr-core-west-router.princeton.edu (128.112.12.229)  1.108 ms  0.726 ms  0.545 ms
 3  fw-border-hpcrc-router.princeton.edu (128.112.12.14)  1.044 ms  1.127 ms  1.096 ms
 4  rtr-border-hpcrc-router.princeton.edu (204.153.48.253)  1.546 ms  1.470 ms  1.427 ms
 5  130.156.251.49 (130.156.251.49)  2.867 ms  2.784 ms  2.647 ms
 6  130.156.34.198 (130.156.34.198)  2.832 ms  2.600 ms  2.971 ms
 7  be-107-2005-pe01.60hudson.ny.ibone.comcast.net (96.87.9.157)  3.391 ms  3.477 ms  3.474 ms
 8  be-4301-cs03.newyork.ny.ibone.comcast.net (96.110.41.153)  4.205 ms be-4201-cs02.newyork.ny.ibone.comcast.net (96.110.41.149)  4.453 ms be-4101-cs01.newyork.ny.ibone.comcast.net (96.110.41.145)  4.219 ms
 9  be-1411-cr11.newyork.ny.ibone.comcast.net (96.110.35.126)  4.007 ms be-1311-cr11.newyork.ny.ibone.comcast.net (96.110.35.122)  4.151 ms be-1211-cr11.newyork.ny.ibone.comcast.net (96.110.35.118)  3.510 ms
10  be-302-cr12.350ecermak.il.ibone.comcast.net (96.110.38.69)  20.169 ms be-301-cr12.350ecermak.il.ibone.comcast.net (96.110.38.65)  21.231 ms  20.805 ms
11  be-1312-cs03.350ecermak.il.ibone.comcast.net (96.110.35.25)  20.632 ms  20.750 ms  20.389 ms
12  be-1311-cr11.350ecermak.il.ibone.comcast.net (96.110.35.10)  20.493 ms *  20.622 ms
13  be-304-cr11.1601milehigh.co.ibone.comcast.net (96.110.37.158)  48.453 ms * be-301-cr11.1601milehigh.co.ibone.comcast.net (96.110.37.146)  49.348 ms
14  be-1311-cs03.1601milehigh.co.ibone.comcast.net (96.110.39.73)  49.043 ms be-1411-cs04.1601milehigh.co.ibone.comcast.net (96.110.39.77)  48.820 ms be-1311-cs03.1601milehigh.co.ibone.comcast.net (96.110.39.73)  48.856 ms
15  be-1213-cr13.1601milehigh.co.ibone.comcast.net (96.110.39.102)  48.125 ms * be-1214-cr14.1601milehigh.co.ibone.comcast.net (96.110.39.118)  49.221 ms
16  be-302-cr14.champa.co.ibone.comcast.net (96.110.39.5)  48.979 ms * be-302-cr13.champa.co.ibone.comcast.net (96.110.36.197)  49.508 ms
17  be-1114-cs01.champa.co.ibone.comcast.net (96.110.37.241)  48.354 ms be-1313-cs03.champa.co.ibone.comcast.net (96.110.37.233)  49.333 ms be-1113-cs01.champa.co.ibone.comcast.net (96.110.37.225)  49.154 ms
18  be-1212-cr12.champa.co.ibone.comcast.net (96.110.37.214)  49.573 ms  48.943 ms  48.431 ms
19  be-301-cr11.sunnyvale.ca.ibone.comcast.net (96.110.39.18)  69.421 ms be-302-cr11.sunnyvale.ca.ibone.comcast.net (96.110.39.22)  69.054 ms be-304-cr11.sunnyvale.ca.ibone.comcast.net (96.110.39.30)  68.806 ms
20  be-1111-cs01.sunnyvale.ca.ibone.comcast.net (96.110.46.1)  68.760 ms  68.765 ms  68.860 ms
21  be-1112-cr12.sunnyvale.ca.ibone.comcast.net (96.110.46.6)  68.587 ms be-1312-cr12.sunnyvale.ca.ibone.comcast.net (96.110.46.30)  68.788 ms be-1112-cr12.sunnyvale.ca.ibone.comcast.net (96.110.46.6)  68.695 ms
22  be-301-cr12.9greatoaks.ca.ibone.comcast.net (96.110.37.170)  68.598 ms be-304-cr12.9greatoaks.ca.ibone.comcast.net (96.110.37.182)  68.725 ms be-301-cr12.9greatoaks.ca.ibone.comcast.net (96.110.37.170)  68.881 ms
23  be-1412-cs04.9greatoaks.ca.ibone.comcast.net (68.86.166.169)  68.472 ms be-1212-cs02.9greatoaks.ca.ibone.comcast.net (68.86.166.145)  68.523 ms  69.159 ms
24  be-2301-pe01.9greatoaks.ca.ibone.comcast.net (96.110.36.226)  68.601 ms  68.290 ms be-2401-pe01.9greatoaks.ca.ibone.comcast.net (96.110.36.230)  68.769 ms
25  50.242.150.146 (50.242.150.146)  69.093 ms  68.435 ms  68.389 ms
26  mx-ll-110.164.0-42.static.3bb.co.th (110.164.0.42)  208.401 ms mx-ll-110.164.0-84.static.3bb.co.th (110.164.0.84)  236.894 ms mx-ll-110.164.0-44.static.3bb.co.th (110.164.0.44)  220.857 ms
27  mx-ll-110.164.0-222.static.3bb.co.th (110.164.0.222)  248.218 ms mx-ll-110.164.0-209.static.3bb.co.th (110.164.0.209)  240.692 ms *
28  * mx-ll-110.164.1-78.static.3bb.co.th (110.164.1.78)  267.148 ms *
29  * * *
30  * * *
```

Done.

Name: Waris Damkham_____Sec:___1___ID:6388014_____P10
>

5. From the question 4 above, how many hops of routers in order to reach our ICT web server?
   Answer: _____30 hops_____

6. From the question 4 above, how many mili-second of the round-trip time for sending and receiving packets from their server to our ICT web server?
   Answer: _____267.148 ms _____

7. From the question 4 above, change the destination to www.facebook.com, and get the screen output.

Traceroute

tracing path from www.net.princeton.edu to 31.13.71.36 ...

```
traceroute to 31.13.71.36 (31.13.71.36), 30 hops max, 40 byte packets
 1  core-ns-router (128.112.128.2)  1.112 ms  0.802 ms  0.840 ms
 2  rtr-core-east-router.princeton.edu (128.112.12.225)  0.723 ms  0.999 ms  0.695 ms
 3  fw-border-87-router.princeton.edu (128.112.12.10)  0.977 ms  0.919 ms  0.998 ms
 4  rtr-border-87-router.princeton.edu (204.153.48.1)  1.421 ms  1.434 ms  1.215 ms
 5  172-96-130.unassigned.userdns.com (172.96.130.53)  3.188 ms  3.117 ms  2.904 ms
 6  172-96-130.unassigned.userdns.com (172.96.130.61)  4.549 ms  4.617 ms  4.601 ms
 7  bundle-ether240.202.core1.newy32aoa.net.internet2.edu (198.71.47.232)  7.139 ms  5.881 ms  6.137 ms
 8  fourhundredge-0-0-0-48.4079.agg1.newy2.net.internet2.edu (163.253.2.123)  6.404 ms fourhundredge-0-0-0-48.4079.agg2.newy2.net.internet2.edu (163.253.2.149)  8.031 ms  7.752 ms
 9  162.252.69.207 (162.252.69.207)  4.757 ms 162.252.69.205 (162.252.69.205)  5.060 ms  4.425 ms
10  po104.psw02.lga3.tfbnw.net (157.240.47.29)  4.592 ms po103.psw02.lga3.tfbnw.net (157.240.47.21)  4.557 ms  4.515 ms
11  173.252.67.107 (173.252.67.107)  4.525 ms 157.240.38.169 (157.240.38.169)  4.510 ms 157.240.38.177 (157.240.38.177)  4.533 ms
12  edge-star-mini-shv-01-lga3.facebook.com (31.13.71.36)  4.393 ms  4.422 ms  4.543 ms

Done.
```

8. From the question 7 above, how many hops of routers and how many mili-second of the round-trip time for sending and receiving packets from their server to www.facebook.com
   Answer: _____12 hops____4.452_____

9. Use pathping www.google.com and tracert www.google.com, compare and describe the obtained results.
   Answer: _____

```
C:\Users\Student>pathping www.google.com

Tracing route to www.google.com [216.58.196.4]
over a maximum of 30 hops:
  0  DESKTOP-901VUA0.ict.mahidol.ac.th [10.34.14.92]
  1  10.34.14.254
  2  10.34.166.254
  3  10.166.1.21
  4  10.41.131.100
  5  202.28.154.1
  6  202.28.151.253
  7  202.28.220.97
  8  202.28.218.17
  9  202.28.218.17
 10  122.155.225.5
 11  74.125.242.35
 12  216.239.35.168
 13  216.239.35.168
 14  108.170.250.17
 15  209.85.249.35
 16  kul08s09-in-f4.1e100.net [216.58.196.4]

Computing statistics for 400 seconds...
```

```
C:\Users\Student>tracert www.google.com

Tracing route to www.google.com [216.58.196.4]
over a maximum of 30 hops:

  1    2 ms     3 ms     2 ms  10.34.14.254
  2   <1 ms    <1 ms    <1 ms  10.34.166.254
  3   <1 ms    <1 ms    <1 ms  10.166.1.21
  4    1 ms     1 ms    <1 ms  10.41.131.100
  5    2 ms     1 ms     1 ms  202.28.154.2
  6    1 ms     1 ms     1 ms  202.28.220.97
  7    1 ms     1 ms     2 ms  100.64.251.197
  8    2 ms     2 ms     2 ms  202.28.218.17
  9    2 ms     2 ms     2 ms  202.28.218.17
 10    2 ms    28 ms     2 ms  122.155.225.5
 11   30 ms    30 ms     *     74.125.242.35
 12    *        *       30 ms  216.239.35.168
 13    *       34 ms     *     209.85.250.18
 14    *       33 ms    36 ms  209.85.250.18
 15   33 ms    33 ms    33 ms  209.85.249.35
 16   32 ms    32 ms    32 ms  209.85.249.35
 17   35 ms    34 ms    32 ms  kul08s09-in-f4.1e100.net [216.58.196.4]

Trace complete.
```

Name: Waris Damkham Sec: 1 ID:6388014 P11

NSLOOKUP

Exercise 5:

1. Perform command “nslookup www.nectec.or.th” to find the IP address.
   2001:f00:1fff:2::1067
2. Perform command “nslookup 203.185.132.65” to find the hostname.
   www.nectec.or.th
3. Think about the reason why you cannot get the hostname from Step 2.
   It same as IP address
4. Perform command “nslookup google.com” to find the IP address.
   2404:6800:4001:803::200e
5. Perform command “nslookup 172.217.24.174” to find the hostname.
   kul08s01-in-f14.1e100.net

Name: Waris Damkham Sec: 1 ID:6388014 P12

Interactive mode

For students, practice below, get the screen outputs before exit nslookup.

Exercise 6:

1. Perform the following command and see what happens.
   - nslookup
   - set type=ANY
   - www.facebook.com
   - exit

```
C:\Users\Student>nslookup
Default Server:  world.ict.mahidol
Address:  10.34.101.101

> set type=ANY
> www.facebook.com
Server:  world.ict.mahidol
Address:  10.34.101.101

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com
> exit
```

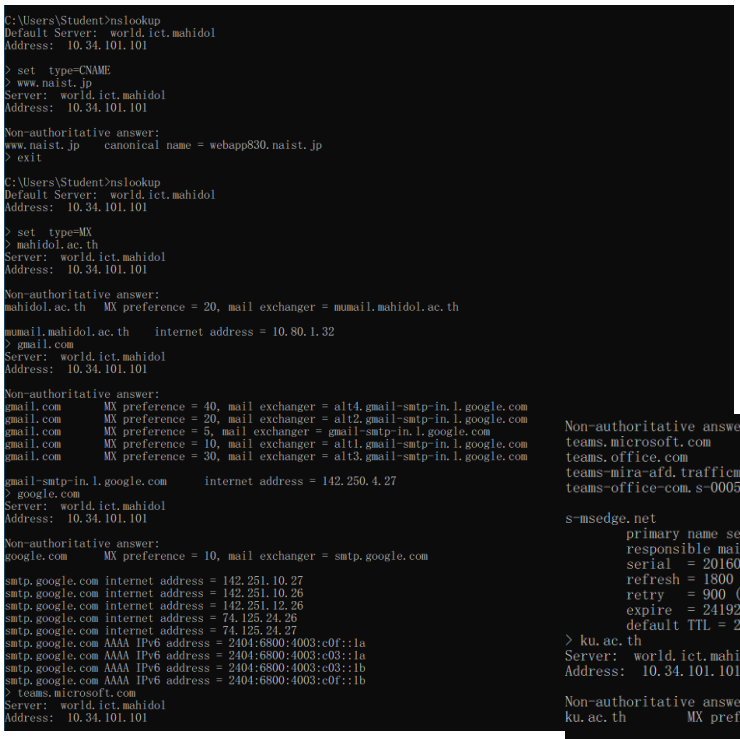
2. Perform the following command and see what happens.
   - nslookup
   - set type=CNAME
   - www.naist.jp ….(1)
   - Exit

```
C:\Users\Student>nslookup
Default Server:  world.ict.mahidol
Address:  10.34.101.101

> set  type=CNAME
> www.naist.jp
Server:  world.ict.mahidol
Address:  10.34.101.101

Non-authoritative answer:
www.naist.jp    canonical name = webapp830.naist.jp
> exit
```

Name: Waris Damkham_____Sec:__1__ID:6388014_____P13

3. Perform the following command and see what happens.

- nslookup
- set type=MX
- mahidol.ac.th
- gmail.com
- google.com
- teams.microsoft.com
- ku.ac.th
- naist.jp
- wide.ad.jp
- daad.de
- exit



```
C:\Users\Student>nslookup
Default Server:  world.ict.mahidol
Address:  10.34.101.101

> set  type=CNAME
> www.naist.jp
Server:  world.ict.mahidol
Address:  10.34.101.101

Non-authoritative answer:
www.naist.jp    canonical name = webapp830.naist.jp
> exit

C:\Users\Student>nslookup
Default Server:  world.ict.mahidol
Address:  10.34.101.101

> set  type=MX
> mahidol.ac.th
Server:  world.ict.mahidol
Address:  10.34.101.101

Non-authoritative answer:
mahidol.ac.th   MX preference = 20, mail exchanger = mumail.mahidol.ac.th

mumail.mahidol.ac.th    internet address = 10.80.1.32
> gmail.com
Server:  world.ict.mahidol
Address:  10.34.101.101

Non-authoritative answer:
gmail.com       MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com
gmail.com       MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
gmail.com       MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
gmail.com       MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com

gmail-smtp-in.l.google.com      internet address = 142.250.4.27
> google.com
Server:  world.ict.mahidol
Address:  10.34.101.101

Non-authoritative answer:
google.com      MX preference = 10, mail exchanger = smtp.google.com

smtp.google.com internet address = 142.251.10.27
smtp.google.com internet address = 142.251.10.26
smtp.google.com internet address = 142.251.12.26
smtp.google.com internet address = 74.125.24.26
smtp.google.com internet address = 74.125.24.27
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c0f::1a
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c03::1a
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c03::1b
smtp.google.com AAAA IPv6 address = 2404:6800:4003:c0f::1b
> teams.microsoft.com
Server:  world.ict.mahidol
Address:  10.34.101.101

Non-authoritative answer:
teams.microsoft.com     canonical name = teams.office.com
teams.office.com        canonical name = teams-mira-afd.trafficmanager.net
teams-mira-afd.trafficmanager.net       canonical name = teams-office-com.s-0005.s-msedge.net
teams-office-com.s-0005.s-msedge.net    canonical name = s-0005.s-msedge.net

s-msedge.net
        primary name server = ns1.s-msedge.net
        responsible mail addr = msnhst.microsoft.com
        serial  = 2016060801
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 2419200 (28 days)
        default TTL = 240 (4 mins)
> ku.ac.th
Server:  world.ict.mahidol
Address:  10.34.101.101

Non-authoritative answer:
ku.ac.th        MX preference = 10, mail exchanger = antispam2.ku.ac.th

antispam2.ku.ac.th      internet address = 158.108.216.32
antispam2.ku.ac.th      AAAA IPv6 address = 2406:3100:1010:100::32
> naist.jp
Server:  world.ict.mahidol
Address:  10.34.101.101

Non-authoritative answer:
naist.jp        MX preference = 10, mail exchanger = mailsgw30.naist.jp

mailsgw30.naist.jp      internet address = 163.221.12.248
> wide.ad.jp
Server:  world.ict.mahidol
Address:  10.34.101.101

Non-authoritative answer:
wide.ad.jp      MX preference = 10, mail exchanger = mail.wide.ad.jp

mail.wide.ad.jp internet address = 203.178.136.30
> daad.de
Server:  world.ict.mahidol
Address:  10.34.101.101

Non-authoritative answer:
daad.de MX preference = 1, mail exchanger = daad-de.mail.protection.outlook.com

daad-de.mail.protection.outlook.com     internet address = 104.47.9.36
daad-de.mail.protection.outlook.com     internet address = 104.47.51.138
> exit
```

CURL (Laptop)

A geolocation service tries to tell, approximately, where a given IP address is located physically. They can't be completely accurate—but they probably get at least the country right most of the time.

You can access a web-based geolocation utility on the command line, using the curl command, which can send HTTP requests and display the response. The following command uses curl to contact a public web service that will look up an IP address for you: curl ipinfo.io/<IP-address>

For examples:

curl ipinfo.io


```
{
  "ip": "202.28.158.145",
  "city": "Salaya",
  "region": "Nakhon Pathom",
  "country": "TH",
  "loc": "13.8020,100.3211",
  "org": "AS4762 Mahidol University, Thailand",
  "postal": "11140",
  "timezone": "Asia/Bangkok",
  "readme": "https://ipinfo.io/missingauth"
}
```


curl ipinfo.io/129.64.99.200


```
{
  "ip": "129.64.99.200",
  "hostname": "websrv-prod.unet.brandeis.edu",
  "city": "Waltham",
  "region": "Massachusetts",
  "country": "US",
  "loc": "42.3567,-71.2505",
  "org": "AS10561 Brandeis University",
  "postal": "02454",
  "timezone": "America/New_York",
  "readme": "https://ipinfo.io/missingauth"
}
```

Exercise 7 (without proxy):

Perform the following command and see what happens.

a. curl ipinfo.io … (1)

//copy and paste the results here.

{
"ip": "202.28.158.61",
"city": "Salaya",
"region": "Nakhon Pathom",
"country": "TH",
"loc": "13.8020,100.3211",
"org": "AS4762 Mahidol University, Thailand",
"postal": "10160",
"timezone": "Asia/Bangkok",
"readme": "https://ipinfo.io/missingauth"
}

Go to https://geoiptool.com/ (2)

//copy and paste the results here

Hostname: 202.28.154.180

IP Address: 202.28.154.180

Country: Thailand

Country Code: TH ()

Region: Nakhon Pathom

City: Salaya

Postal Code: 11140

Latitude: 13.802000

Longitude: 100.321110

Compare the results between (1) and (2)

What kind of information do you obtain from this command?

Hostname,IP address, Country, Postal Code, Location

b. curl ipinfo.io/157.240.10.35

{
"ip": "157.240.10.35",
"hostname": "edge-star-mini-shv-01-kut2.facebook.com",
"city": "Kuala Lumpur",
"region": "Kuala Lumpur",
"country": "MY",
"loc": "3.1412,101.6865",
"org": "AS32934 Facebook, Inc.",
"postal": "50050",
"timezone": "Asia/Kuala_Lumpur",
"readme": "https://ipinfo.io/missingauth"
}

https://geoiptool.com/ and fill in Host/IP: 157.240.10.35

Hostname: edge-star-mini-shv-01-kut2.facebook.com

IP Address: 157.240.10.35

Country: Netherlands

Country Code: NL ()

Region: Noord-Holland

City: Amsterdam

Latitude: 52.374030

Longitude: 4.889690

Is there any different information from curl command and the web service geoiptool.com? Explain.

In the geoiptool show Netherlands but in curl show “MY”.