**INT207 Network I**

**Lab 1: Network tools, CLI commands**

**Learn how to use and interpret basic network commands on CLI**

**Hostname**

**Ping**

**Nslookup, dig, whois**

**Ipconfig (Windows), ifconfig, ip**

**Tracert (Windows), traceroute, tracepath**

Homework 1:

1. What is the hostname of your computer?
2. What IP addresses/mask are devices using in your house/apartment? (notebook, phone, tablet, TV …)
3. What are the IP addresses for 3 Thai web sites and 3 foreign websites (each in different countries)?
4. What are the names and addresses of the company that registered the domain names for the websites in Q3?
5. What ISPs, countries are on the route to the 3 foreign websites in Q3?

References  
คู่มือติดตั้ง Whois on windows   
[https://docs.microsoft.com/en-us/sysinternals/downloads/whois](https://docs.microsoft.com/en-us/sysin%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20)

copy program whois ไปใส่ที่ Windows\System32 หรือสร้าง PATH ไป folder ที่ติดตั้ง whois

<https://kingbond470.medium.com/how-to-install-and-run-a-whois-in-windows-10-4544744b639f>

NOC RMUTP, คำสั่ง Command Prompt ที่เกี่ยวกับ Internet

<https://noc.rmutp.ac.th/commandpromptinternet/>

Redhat.com, 7 Linux networking commands that every sysadmin should know

<https://www.redhat.com/sysadmin/7-great-network-commands>

**Lab 2: Wireshark, Traffic Analysis Tool**

LO: Can use Wireshark to capture and view traffic information by applying the following techniques.

-Conversation filter, Follow stream, Flow graph

Team collaboration:

-Work with your team to make voice and video calls and capture traffic.

-Discuss traffic data and information with your teammates and analyze

Copy rubric paste on first paragraph and self-assessment after your homework

Homework 2:

1 .Capture and show the request and reply data in a domain name lookup (whois). Create a table to compare the answers to the following questions for the whois reply messages.

a. How many TCP messages were sent and received on your computer for the whoiscommand?

What TCP port is used on the server to receive your lookup request?

b. How many TCP messages were used to send the replies to your query (use flowgraph)?

• What is the L2 Frame Length for each message?

• What is the L3 Payload Header Length and Total Length for each message?

• What is the L4 payload size for each message?

c. View the TCP payload data for each message and show where each reply message is in the Follow TCP Stream output.

For example, first reply message payload ends at “H.EDU-”

A picture containing text, screen, screenshot

Description automatically generated

And the next message starts with “SE RVERS.NE”

A screenshot of a computer

Description automatically generated with low confidence

Location in Follow TCP stream output.

A picture containing letter

Description automatically generated

2. Choose 3 applications that communicate over the internet (not HTTP, HTTPs), MUST be different from app in question 3. Answer the following questions.

a. What are the addresses used at the source and destination at L2 (Physical or MAC address), L3 (IP address), L4 (port address), L5 (URL)?

b. What protocols are used at L4, L5?

3. TEAM work: Choose two (or more) text/voice/video communication application like LINE, FB Messenger, Skype, etc. Use the app with your teammates (2-3 persons for each app), capture data/output and answer the following questions. Each team member must submit their own results and answers.

a. Show the communication flow between users and server when you make a voice/video call, until you hang-up. L5: TLS, STUN, TURN, ICE, <Application data>, L4: TCP, UDP, L3: IP, IGMP

b. What protocols are used during setup and calling, until the call ends?

c.Can you view the protocol of the payload data being transmitted during texting, voice or video call?

4. List background protocols you can capture at L2, L3, L4, L5 in your home network, when you are NOT actively using any online app.

References

[Wireshark User’s Guide](https://www.wireshark.org/docs/wsug_html_chunked/index.html):

[How to Use Wireshark to Capture, Filter and Inspect Packets](https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/), by Chris Hoffman

[What Is Wireshark and How Is It Used?](https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it) By CompTIA, includes more resources