BCIT

COMP 3721 **Assignment 3**

Note:

- Submit a single PDF file.
- Answer the questions according to textbook, lecture notes and class discussions, not ChatGPT or Google.

Q1:

For a target IP address of 14.12.72.8/24, find the following.

(a) Target IP address in binary
(b) Subnet mask in binary
(c) Subnet mask in dotted decimal
(d) First address (i.e., network address) of the block
(e) Last address (i.e., broadcast address) of the block
(f) First host address of the block
(g) Last host address of the block
(h) Number of addresses in the block
(i) Maximum number of hosts in the block

Q2:

For a target IP address of 200.107.16.17/18, find the following.

(a) Target IP address in binary
(b) Subnet mask in binary
(c) Subnet mask in dotted decimal
(d) First address (i.e., network address) of the block
(e) Last address (i.e., broadcast address) of the block
(f) First host address of the block
(g) Last host address of the block
(h) Number of addresses in the block
(i) Maximum number of hosts in the block

Q3:
Download and install Wireshark (https://www.wireshark.org/). Open "trace.cap" (provided with the assignment) by either

- Double-click the capture file (if the extension is associated with Wireshark), or
- Open Wireshark, click File → Open → browse and choose the file.

Capture the Wireshark screen that shows the following by applying correct filters.

- One capture per question.
- Must show the display filter.
- Only need show the first few rows of the results, if any.

(a) Display all the packets with source address 192.168.100.102.
(b) Display all the packets with source address: 192.168.100.102 and destination address: 142.104.193.247.
(c) Display all the HTTP packets.
(d) Display all the TCP packets with source address 192.168.100.102.
(e) Display all ICMP packets.

Appendix – Some Wireshark Display Filters:

- Comparing rules
  - English: `eq`, `le`, `ge`, `lt`, `gt`, `ne`
  - C-like: `==`, `<=`, `>=`, `<`, `>`, `!`
- Logical operators
  - English: `and`, `or`, `xor`, `not`
  - C-like: `&&`, `||`, `^^`, `!`
- Boolean – when the field is present, the value is true.
  - For example, `tcp.flags.syn` is present in all TCP packets containing the flag, whether the SYN flag is 0 or 1. To only match TCP packets with the SYN flag set, you need to use `tcp.flags.syn == 1` or `tcp.flags.syn == True`.
- Addresses
  - IPv4 address: e.g., `ip.addr == 192.168.0.1`
  - IPv4 source address: e.g., display packets from 192.168.100.102 → `ip.src == 192.168.100.102`
  - Ethernet (link layer/MAC) address. e.g., `eth.dst == ff:ff:ff:ff:ff:ff`

For more information, consult Wireshark documentations on display filter expressions (https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html).

— End of Assignment 3 —