CS447-002 Network and Data Communication

Project Specification/Project #2, Spring 2024

STEP #3: Answer the following questions:

Category I Questions:

(1) Is it possible for you to find the IP address of the host computer that captured this log (using the information you see in the packet capture log given to you)? Please type your explanation ("why yes" or "who not") in Times-New-Roman font, 11-point, single line spacing, the MS Word standard margin (in the separate "answer form"). Note that "a nothing wrong solution" does not necessarily earn full credit (your work will be graded based on "how well" your "yes" (or "no") is explained.

- If yes, why (and which IP address is it)?
- If not, why not?

The focus of grading your work for this question (your work for other questions will be graded in the same/similar way(s)) is how you explain "why or "why not".

For examples:

- "Just because I observed the same IP addresses quite often in the given packet capture log" is not a good reasoning. It is because:

  - If the IP address is "the destination IP addresses", it may not be the IP address of the host computer that captured this log, because the packets can be "broadcasted packets" (those packets any host should receive). Thus, if you observed broadcast packets, you can not use them as a reason for you to conclude the host computer's IP address.

  - Then, the question is how you can tell which packets are broadcast packets, and which are not. It can be determined by the protocol(s) that were used for the packets. Likewise, you can determine which packets are "unicast packets", by their protocol(s). Wireshark determines the protocols using the port number.

(2) Is it possible to find the IP address of the gateway router the host computer of this host (the host computer that was used to perform the packet capture)? The same for (1) above for how you are expected to explain.

- If yes, why?
- If not, why not?

If you can find the packets in the given packet capture log that were transferred by some protocol(s) a gateway router uses, then you can determine its IP address. Is there any

particular protocol only gateway routers use (the answer can be either yes or no)? If such a protocol exists, do you see any packet that was (were) transferred using the protocol(s) (the answer can be either yes or no)? Even if the answer for the first question is “yes”, it can be that the given packet capture log may not contain any. Note that, depending on the packet capture log file given to each of you, the answer for this question can be either yes or no (not the same answer for all of the packet capture log files).