Task 1: Trace Route to Remote Server.

Step 1: Trace the route to a distant network.

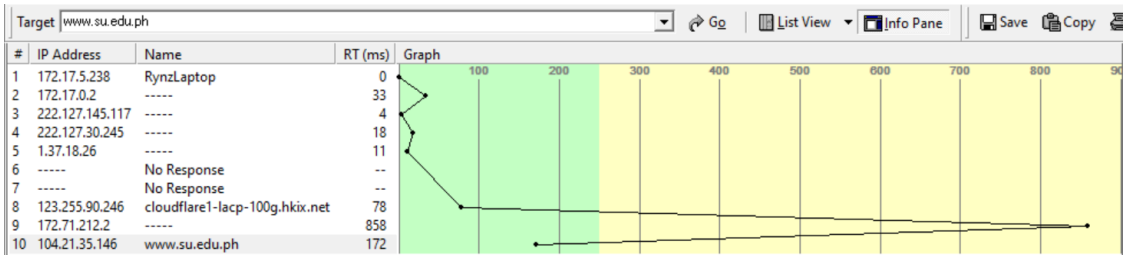
2. How many hops between the source and destination?
    - There were a total of 9 hops from my laptop to *www.su.edu.ph*. 3 of the hops were Request timed out, so it only hopped from 6 routers in total.

Step 2: Try another trace route on the same PC, and examine your output.

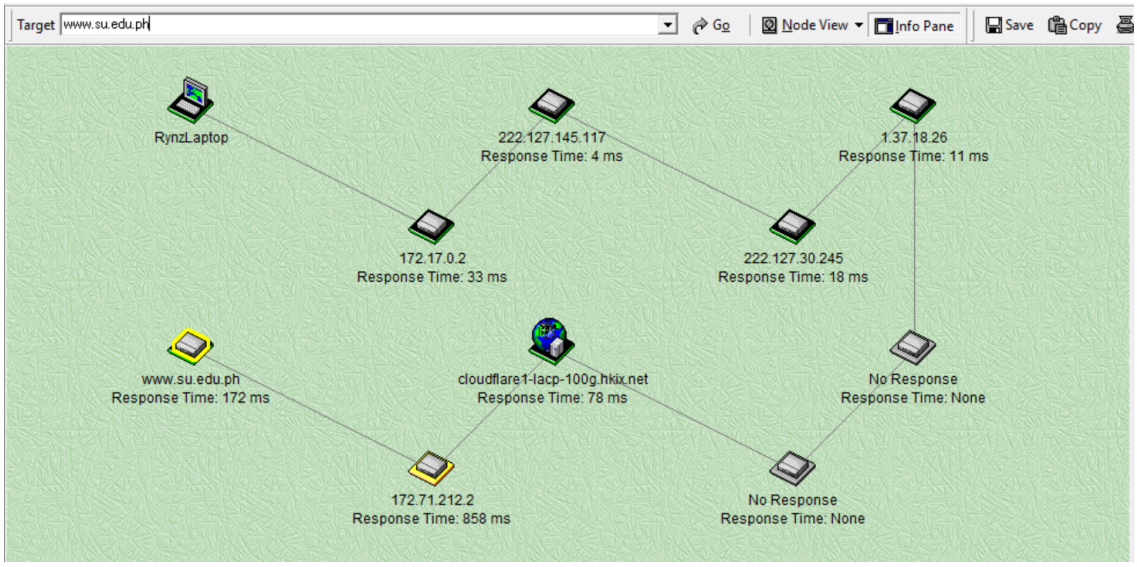
- Destination URL: *www.freetetris.org*
- Destination IP Address: *172.67.178.197*

Task 2: Trace Route using NeoTrace.

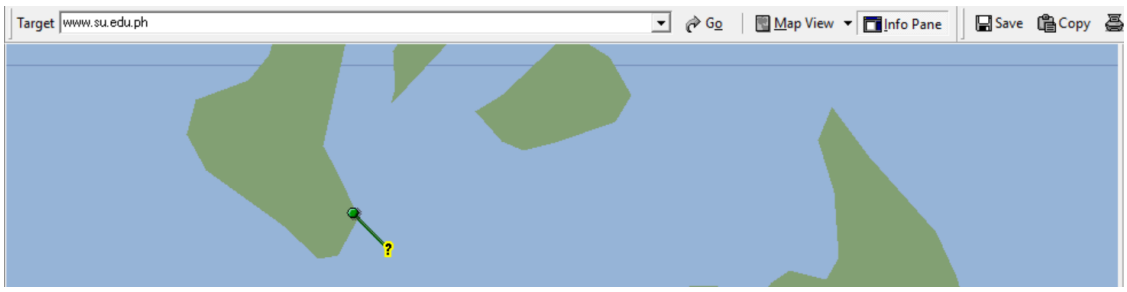
- List View:



- Node View:



- Map View:



9. Select each view in turn and note the differences and similarities.
    - Each view offers different information that helps a lot in making that information understandable. The List View helps illustrate the distance between each route through the time taken to hop, the Node View shows a clear path from each router, and the Map View shows on a real map where exactly the end router is compared to the original location.
10. Try a number of different URLS and view the routes to those destinations.
    - The NeoTrace program was useful in terms of List View and Node View and it shows how different destinations can have different routes to getting there. Unfortunately in terms of Map View, I was not able to find a destination with a location that can be viewed and so this mode was not particularly helpful.

Task 3: Reflection

- While it is not the first time that I used traceroute, using NeoTrace really helped me in visualizing how the networks of our internet works. Our data does not just travel from one router to the final destination in one go, it instead goes through intermediary routers along the way. There's a reason why the internet is described as a web, after all. It is simply fascinating to see how this technology works, even though this is simply just a surface view of what's truly going on.

Task 4: Challenge

- One form of misuse of these programs could be DoS attacks, where a user's IP is flooded with excessive traffic in order to interrupt their internet connection. Privacy breach could also be a concern which could be used for personal harassment and disruption of online activities. It could also be used to identify the weak points of a person's network, making them vulnerable to attacks. One way of protecting against these risks is using a VPN to mask the real IP with the VPN's IP.