Hints on how to do well on the final project (and how do not do so well):

Attention to the following will get you a favorable evaluation:

- Professionally formatted report with a clear and concise executive summary and conclusion.
- Good use of tables, graphs, and diagrams.
- Extensive usage of technical terms in your analysis of the data.
- A well-designed approach to the methods and tools used in the analysis of the data.
- Clearly stated assumptions and definitions
- Clearly present and explain the reasons for drawing conclusions vis-à-vis benign and malicious traffic.
- Properly identify security incidents of concern and justify your reasoning.
- Use the output from the analysis tools used to reinforce and justify your analysis and explanations. In the analysis sections of the report use the appropriate and relevant output from the analysis tools only. I can view all of the raw data if I wish in your appendix.
- Good use of qualified references for your analysis, incidents and attacks.
- An Appendix that contains the raw data from your analysis tools.

Overall I will be looking for usage and application of all the concepts that have been covered in the course. **A reminder that this project is worth 35% of your course mark. You are going to have to earn it.**

Here is how to get a poor evaluation:

- Not paying attention to the section above.
- Poorly formatted document without a table of contents, pages numbers, cover sheet, appropriate sections (in a typical technical report), etc.
- Fluffing up your report with reams of pages from your analysis tools. Save that for the Appendix.
- Drawing conclusions and making assertions without any technical or analytic backup from the raw data.
- Weak or no application of technical terms and concepts in your analysis and discussions.