Assignment 11

Download the provided SMTP traffic logs (e.g., a11.SMTP.txt file) and use any analysis tool you desire to analyze the logs and answer the following questions. Your answers will be submitted via CANVAS. Submission must be in either Word or PDF format.

1. What tools did you use to analyze the sample (if any)?

    - How many records where loaded into your tool?
    - How did you prepare and load the sample into your analysis tool?
    - Note any errors in the sample and how you handled them. Did you ignore or correct them?

2. What is the domain of the SMTP server(s) being monitored? How was that determined?

3. List all valid email senders (e.g. email addresses) in the SMTP sample, excluding SPAM related addresses?

4. Plot the volume of SMTP traffic over time in a time series. Describe the characteristics of the traffic. Describe the peaks and valleys seen in the time series? *Hint: this is talked about in the second video*

5. List all Spamming IP addresses and describe how you know each to be spammers.

6. What spam messages made it past the reputation-based filter? Describe two methods for detecting these messages at the message level. *Hint: if the AV verdict is CLEAN and the spam CASE engine reports "negative", then the emails are not detected as spam and will pass through the reputation-based filter. (e.g. not blocked by policy or signatures). If the AV verdict is "NOT" CLEAN and the spam CASE engine reports "positive" then emails are SPAM and will not pass (e.g. get blocked) at the reputation-based filter.*