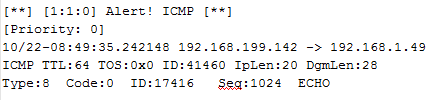
Snort Lab

|  |
| --- |
| * This is an assignment, and worth 2 points. * The due date is the same day midnight. It will be graded as pass/fail (2 or 0 points). |

**Task 1.**

* Create a Snort rule that captures ICMP Echo Request from Kali and shows alerts with the message “Alert! ICMP”. (The *icode* and *itype* options are not necessary.)
* Send five (5) ICMP Echo Request messages from the Kali.
* Display your Snort rule.
* Go to **c:\snort\log** and find the **alert.ids** file. Open it with a text editor. Provide a screenshot for the five alerts you have captured.



|  |
| --- |
| **Dr. Im, I tried indexes 1-10 and only 6 displayed anything in the log files. I only received 4 alerts back even though the kali command has 5. I’m unsure why, but I’ve attached screenshots to show you that I’ve configured the file and run the commands correctly.** |
|  |
| **More below** |
|  |