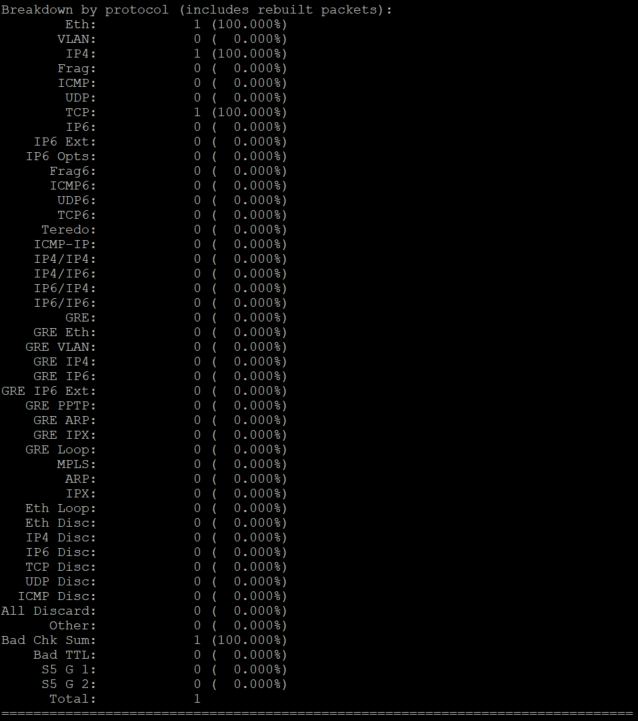
## **Task 1**: Discovery Flag: Display data-link headers and the application layer data

* **Solution:**

|  |
| --- |
| Sudo snort -de |

* + d: show application data in transit
  + Text

    Description automatically generatede: show the data link layer headers

**research:** http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node4.html

## **Task 2**: Capture only ICMP

* **Solution:**

|  |
| --- |
| Sudo snort -vde icmp |

* + Snort use sniffer mode and apply BPF filter that only retrieve ICMP packet.

Text

Description automatically generated

## **Task 3:** Check Alerts

cm