# Lab 07 – Security Onion 2

## Overview

The ability to provide basic statistics or information on a packet capture is one of the first steps in incident response. You'll need to use your Security Onion VM in the IAlab or one you have locally for this lab. This lab can be completed by using the following CLI tools: capinfos, argus, racluster, tshark (other tools can be used, however). nsm01.pcap will be the file used for this lab.

## Tasks

Answer the following questions with a short explanation and screenshot. After you've answered your questions, paste screenshots showing the use of the CLI tools to find the information used to answer the questions.

1. How many packets exist in the capture?
2. At what time did the packet capture occur?
3. What is the timespan, in seconds, of the traffic? (How many seconds of traffic were captured?)
4. Is there any traffic other than TCP sessions?
5. How many TCP sessions exist in the packet capture?
6. How many sessions involve the IP address 203.0.113.15?
7. How many bytes of non-TCP traffic exist in the traffic?
8. Using Argus, determine how many bytes were transferred between 203.0.113.15 and 172.16.0.37.
9. Using tshark, determine how many bytes were transferred between 203.0.113.15 and 172.16.0.37.
10. What website was the user trying to access in the port 80 session on IP 199.59.150.7 (hint: use tshark)?
11. Bonus: How did the server on IP/port 199.59.150.7:80 respond?