**Large PCAP File Performance & Optimizations**

**PCAP File Used:** <https://drive.google.com/file/d/1eubdn3dXrk2KaEVsDJzx7x1sOweNHOUu/view?usp=sharing> (It is a combination of many files taken from: <https://www.netresec.com/?page=PcapFiles>) (files link: <https://drive.google.com/drive/folders/1AAS345pfwXbh3m3cqMS-j8zAvYpWXvmf?usp=sharing>).

**Performance Metrics:**

* **Time Taken:**
  + Total time to process the file: 12.016 seconds.
* **Packet Statistics:**
  + Total packets analyzed: 955,110.
  + Packets per second: 95,511.
  + Packet types: TCP (77.32%), UDP (0.34%), IPv4 (99.75%), etc.
* **System Resource Usage:**
  + CPU Usage: During the execution of the file we used htop and saw that cpu usage was 90-100%, while normally is 20-30%, with a user time of 8.811 seconds.
  + Memory Usage: Normally system uses 1.41 GB / 3.82 GB, but during the execution of the pcap file, it used 1.43 - 1.44 GB / 3.82 GB.
* **Errors/Warnings:**
  + No critical errors reported during execution.

**Suggested Optimization Actions:**

1. **Enable Multi-Threading:**

* Upgrading to Snort 3 can take advantage of multi-threading and faster processing.

1. **Increase System Resources:**

* If more CPU and memory are allocated, then larger files can be handled more efficiently.

1. **Optimize Configuration:**
   * Buffer sizes and memory settings can be adjusted in snort.conf to achieve better performance.
2. **Run in a Minimal Environment:**
   * Background processes can be reduced to dedicate more resources to Snort.

**Summary:** Snort handled the large PCAP file well, processing nearly a million packets in just over 12 seconds with no significant issues. By implementing these optimization tips, it can further improve its performance and efficiency, especially in busy network environments.