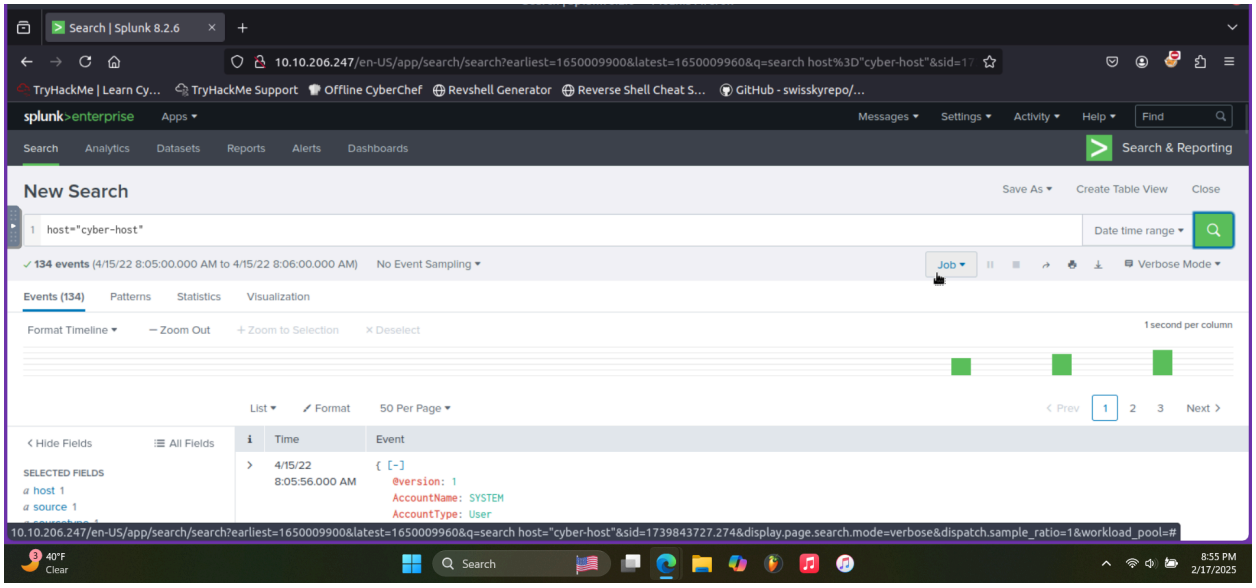
TryHackme: Learning Splunk SPL

Clay Jones

Objective:

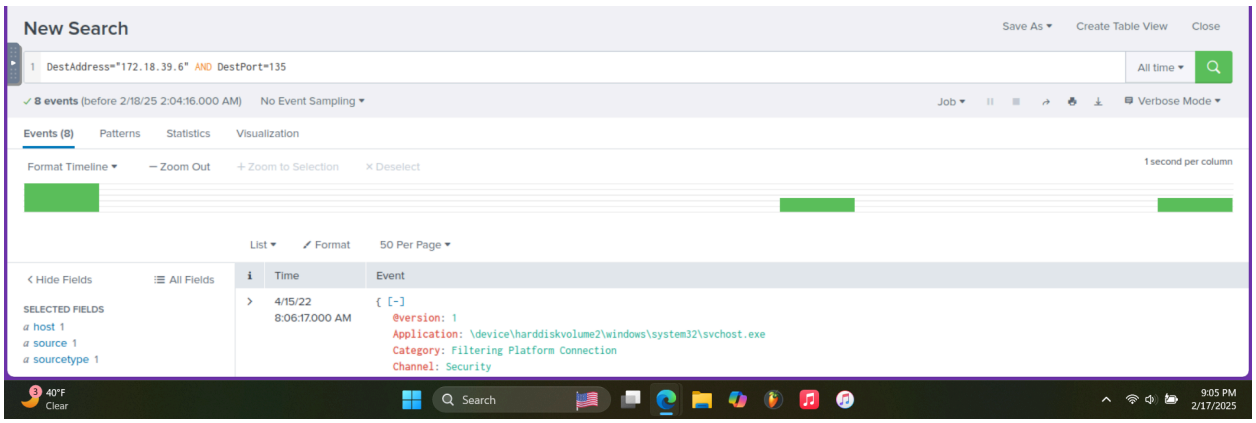
The objective is to learn SPLs in SPlunk, in order to perform SIEM searches more adequately.

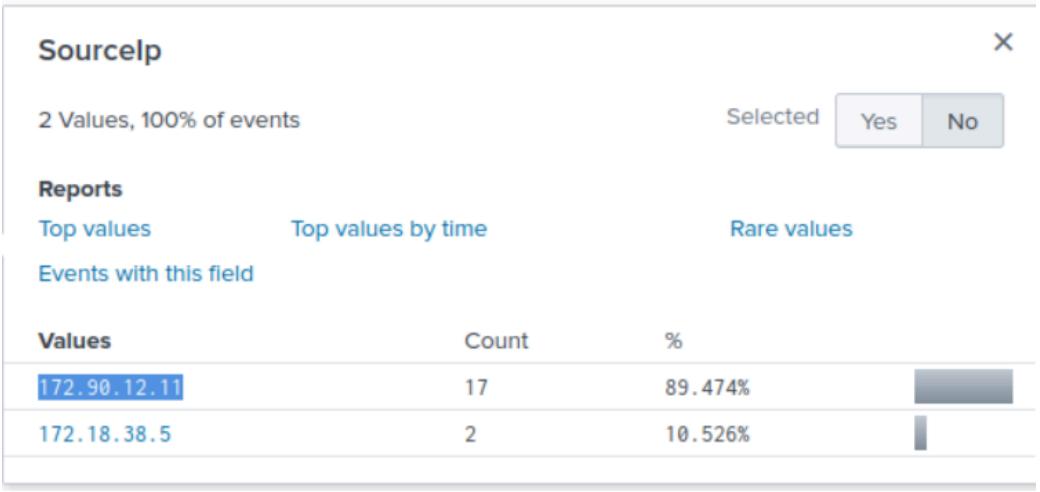
Performing a simple search



Just simply filter logs what contained “cyber-host”

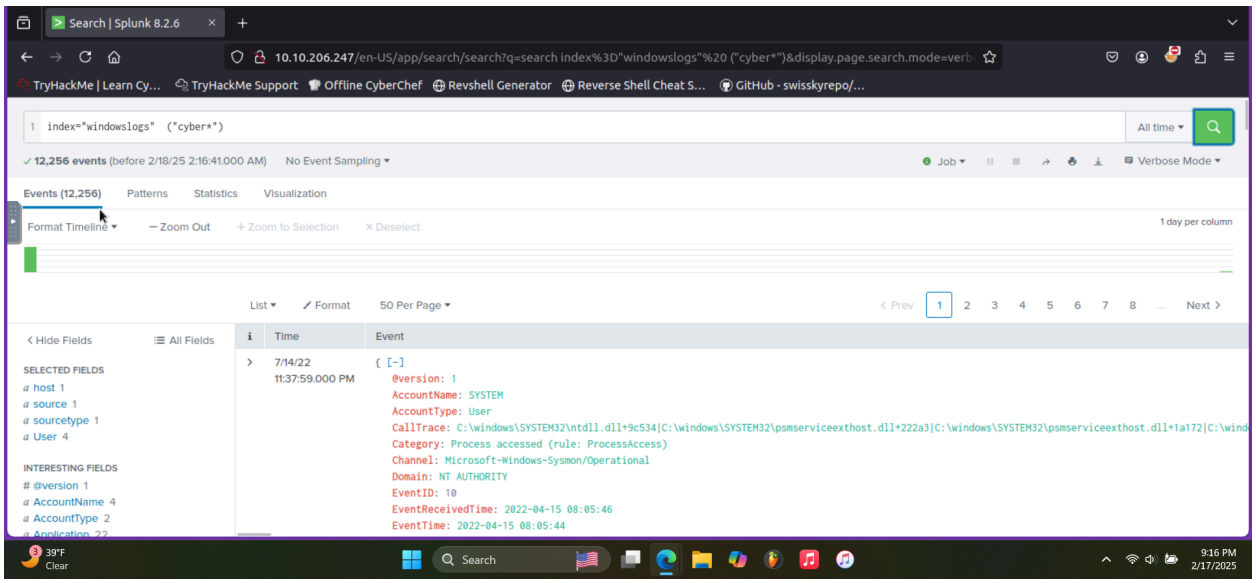
Using Boolean Operators





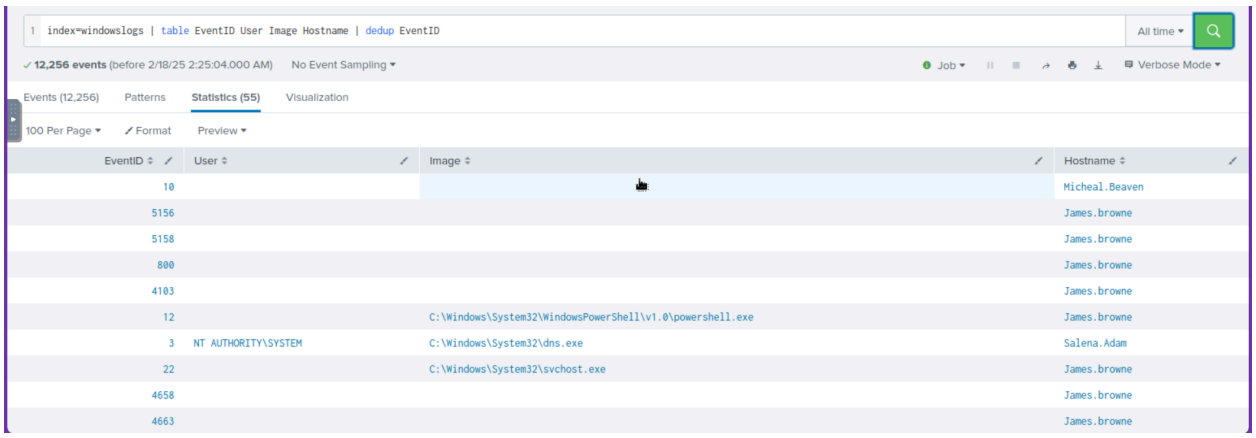
Using Boolean operators to filter logs and finding the source ips to the destination address.

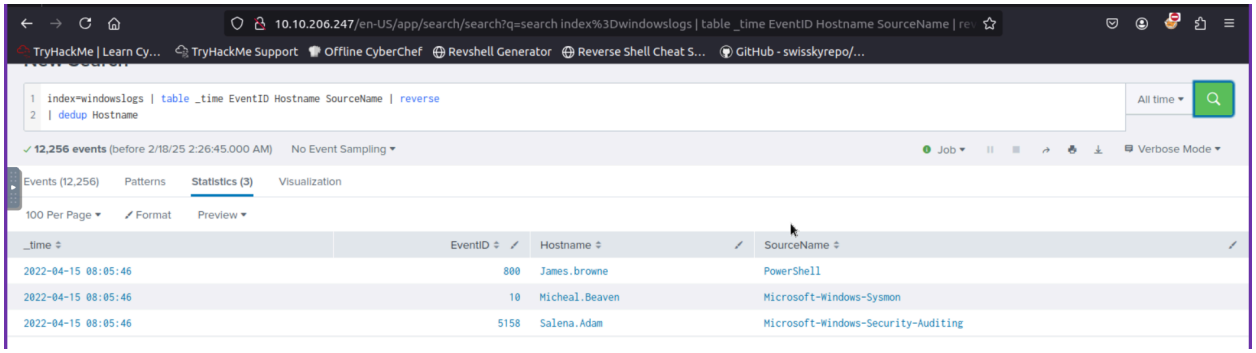
Find cases of a word

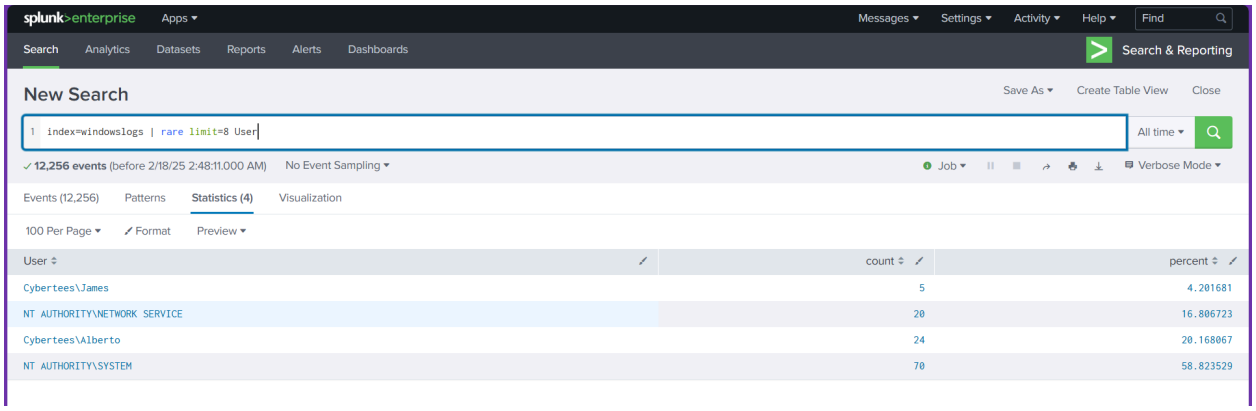


This searches for the cases that “cyber*” shows up.

Sorting Data

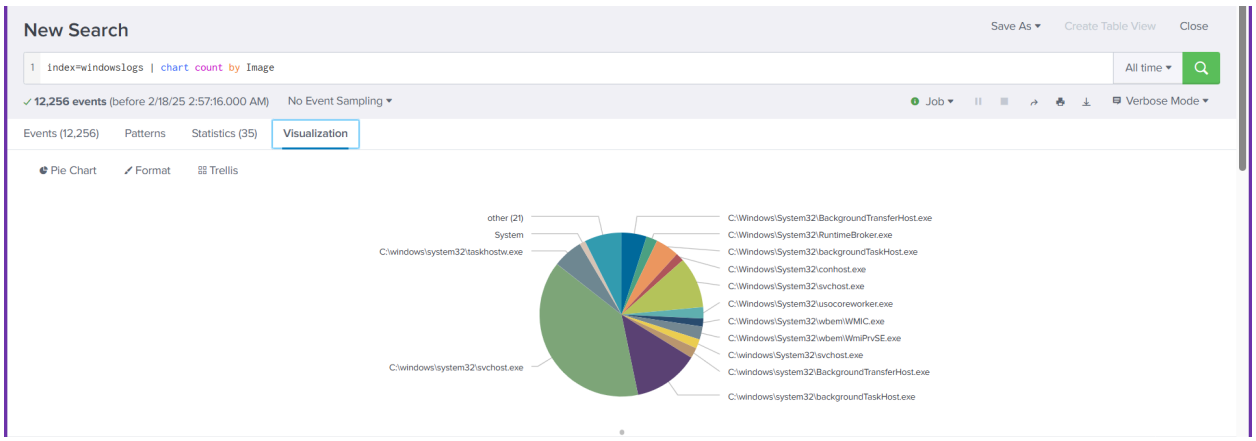






I created tables and sorted the data via the reverse filter. I also used the head and tail commands to show the top and bottom. Depup was used to ignore duplicates.

Creating a graph



Using a graph to sort the data.

Important SPL commands