Lab 5: Hands On

Hurricane Labs

- Run a basic search on the firewall logs
  - sourcetype=linux:netfilter src_ip=<your machine's IP>
- Toggle between fast, smart, and verbose modes and observe the results
  - What fields are extracted in each mode?
- Expand the search
  - sourcetype=linux:netfilter src_ip=<your machine's IP> dest_port=8000
    - Do the field extractions change at all?