INL/MIS-24-79658-Revision-0

Automating Log Synthesis and Visualization with Python and Splunk

August 2024

Daija Imani Freeman

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-24-79658-Revision-0

Automating Log Synthesis and Visualization with Python and Splunk

Daija Imani Freeman

August 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Automating Log Synthesis and Visualization with Python and Splunk

Daija Freeman | UT at San Antonio | Mentor: Dr. Robert Ivans (D520)

The Problem

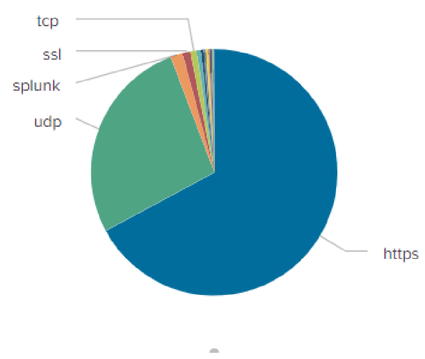
The amount of information that comes from logs can take a while to parse through

The Goal

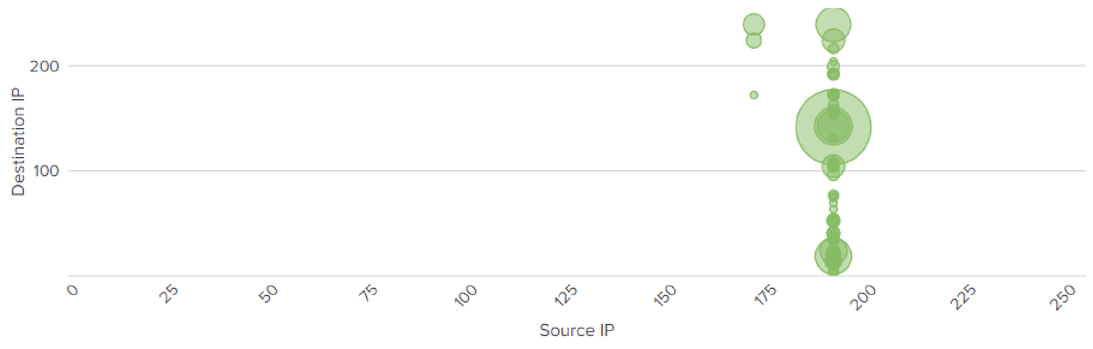
Synthesize the information from pcap files and network logs to ease the analysis process

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
09:06:36.030355 IP messiah.mshome.net.51881 > 239.255.255.250.1900: UDP, len
gth 175
09:06:36.034649 IP messiah.mshome.net.51886 > 239.255.255.250.1900: UDP, len
gth 176
09:06:37.040908 IP messiah.mshome.net.51886 > 239.255.255.250.1900: UDP, len
gth 176
09:06:37.041589 IP messiah.mshome.net.51881 > 239.255.255.250.1900: UDP, len
gth 175
09:06:38.051237 IP messiah.mshome.net.51886 > 239.255.255.250.1900: UDP, len
gth 176
09:06:38.051368 IP messiah.mshome.net.51881 > 239.255.255.250.1900: UDP, len
gth 175
09:06:39.066482 IP messiah.mshome.net.51886 > 239.255.255.250.1900: UDP, len
gth 176
09:06:39.066664 IP messiah.mshome.net.51881 > 239.255.255.250.1900: UDP, len
gth 175
09:08:36.029299 IP messiah.mshome.net.58618 > 239.255.255.250.1900: UDP, len
gth 175
09:08:36.057049 IP messiah.mshome.net.58623 > 239.255.255.250.1900: UDP, len
gth 176
09:08:37.046831 IP messiah.mshome.net.58618 > 239.255.255.250.1900: UDP, len
gth 175
09:08:37.058766 IP messiah.mshome.net.58623 > 239.255.255.250.1900: UDP, len
gth 176
09:08:38.056947 IP messiah.mshome.net.58618 > 239.255.255.250.1900: UDP, len
gth 175
09:08:38.072198 IP messiah.mshome.net.58623 > 239.255.255.250.1900: UDP, len
gth 176
09:08:39.070254 IP messiah.mshome.net.58618 > 239.255.255.250.1900: UDP, len
gth 175
09:08:39.085053 IP messiah.mshome.net.58623 > 239.255.255.250.1900: UDP, len
gth 176
09:10:36.031185 IP messiah.mshome.net.49305 > 239.255.255.250.1900: UDP, len
gth 175
09:10:36.051215 IP messiah.mshome.net.49310 > 239.255.255.250.1900: UDP, len
gth 176
09:10:37.047094 IP messiah.mshome.net.49305 > 239.255.255.250.1900: UDP, len
gth 175
```

Top Applications by Volume (Bytes)

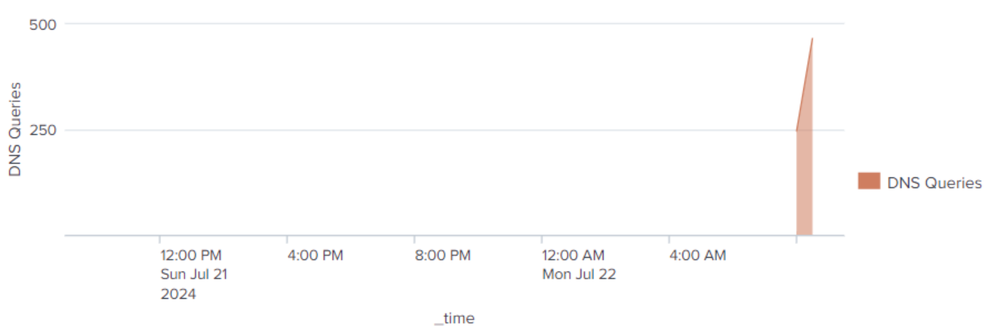


Flow Visualization

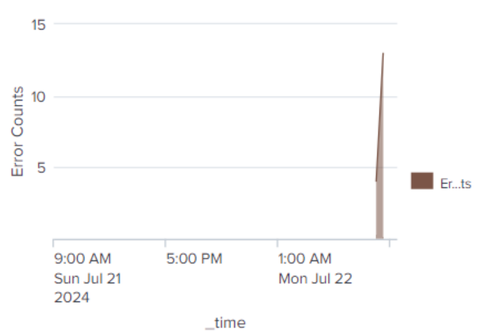


DNS Analytics — DNS Activity — DNS Overview

DNS Queries



Error Count



Total Errors

17

The Methods

Develop Bash scripts with Crontab to run network sniffing applications and Python scripts to extract information using Scapy and visualize important information using Splunk