**Leonard M. Estos  
*Cybersecurity Researcher & Technical Author*  
Edmonton, Alberta, Canada**

**2025**

Project Name: **Project Splunk Installation and Sample Analyzes**

Project Overview

This project presents a simplified yet functional **Security Operations Center (SOC)** architecture designed for home lab experimentation and learning. It simulates real-world SOC workflows using open-source tools, enabling hands-on experience with threat detection, incident response, and automation.

The **goal** is to empower aspiring SOC analysts and cybersecurity enthusiasts with a practical environment to understand how data flows through a security ecosystem—from endpoint agents to centralized analysis platforms.

**Resources:**

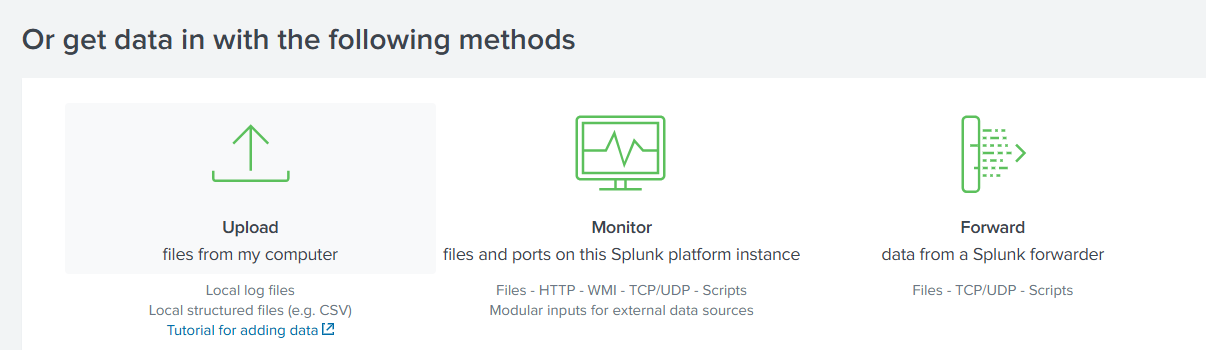
1. Splunk Enterprise Website: [*https://www.splunk.com/*](https://www.splunk.com/)
2. How to install SPLUNK in Kali Linux: <https://www.youtube.com/watch?v=hJhwzGR_Y5Q>
3. How to access SPLUNK in my Kali Linux: <http://172.26.154.185:8000> or <http://localhost:8000>
4. SPLUNK 101: **IP/Traffic | DORA Process** = **Discover** message, **Offer** message, **Request** message, **Acknowledge** message = all the message has their own **Packets**.
5. **Sample Query and Logs Analysis:** 
   1. <https://www.youtube.com/watch?v=LbR5cqqaFVk&t=1s>

5.2 [GitHub - 0xrajneesh/Splunk-Projects-For-Beginners: Unlock the power of Splunk SIEM for comprehensive log analysis. Collaborate and innovate with our Splunk Log Analysis Projects on GitHub](https://github.com/0xrajneesh/Splunk-Projects-For-Beginners)

5.3 **Splunk Log Analysis.docx =** *:\Ogz\CyberSecurity\01\_HowTo\1\_Documentation\13\_SecuringMyEnterprise\SOC\_Analyst\SPLUNK\_SIEM\Project\Leo\_Project\*

**Hands-on:** This will be applicable once Splunk Manager installation has been completed.

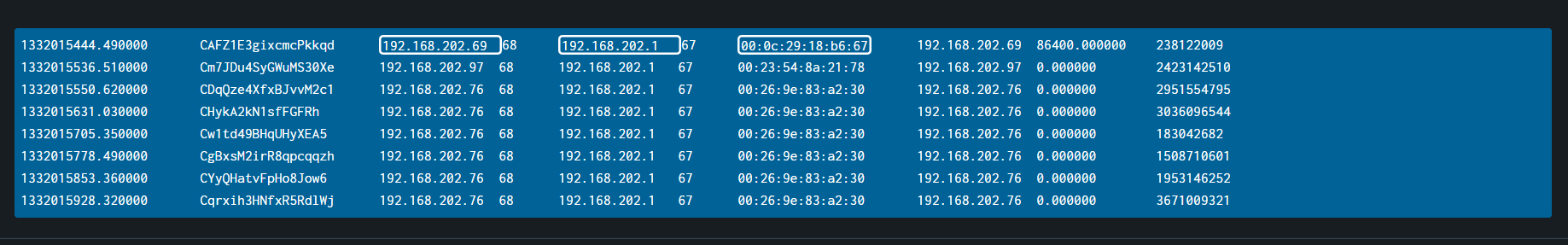
* 1. Download first a sample **DHCP logs** = Sample logs is located in *E:\Ogz\CyberSecurity\01\_HowTo\1\_Documentation\13\_SecuringMyEnterprise\SOC\_Analyst\SPLUNK\_SIEM\Project\Leo\_Project\dhcp.log*
  2. Upload your Raw Data to SPLUNK for analyses. **Go to Settings > Click Add Data > Click Upload**



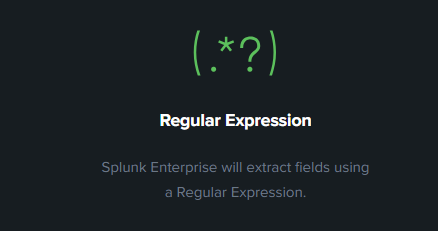
* 1. Create a new **FIELDS**, click Extract **New Fields**



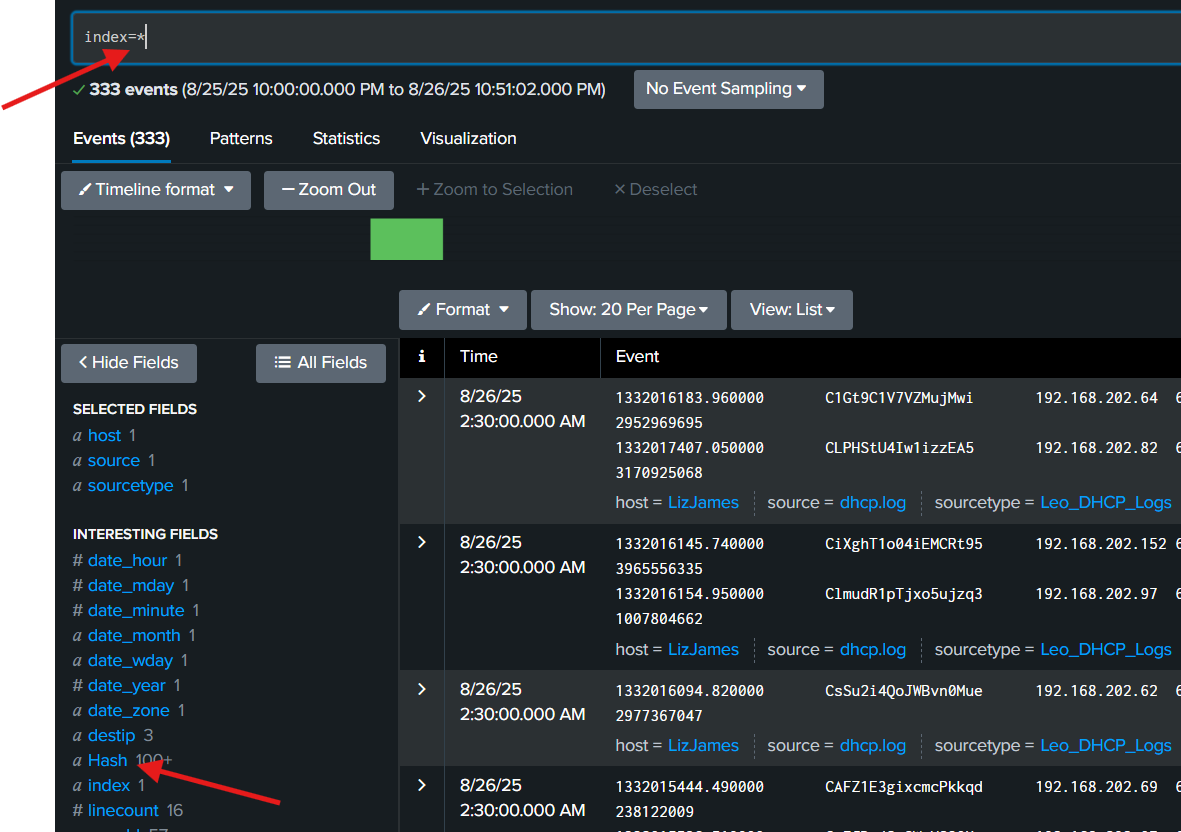
* 1. Click the **group of raw data** to make a new Fields



* 1. Click Next
  2. Choose **Regular Expression** > Click Next



* 1. **Double clicks** a data that you want to create a new **Field Name** e.g. Hash
  2. Click Add Extraction > Click Next > Click Next again > Click Finish
  3. **The new Field will be added in the Interesting Fields.**
  4. Type **index=\*** to check the new added Fields below.



**Proceed with sample query/search below.**

Sample: **index=\*** **(search all)**

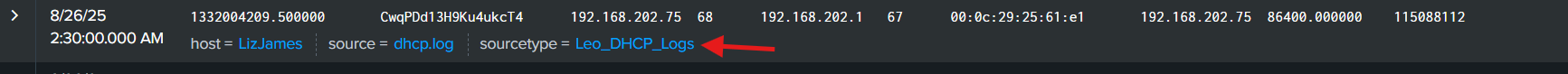
source="dhcp.log" host="LizJames" sourcetype="Leo\_DHCP\_Logs" **(Initial Search)**

index=\* sourcetype="leo\_dhcp\_logs" | table srcip, destip

index=\* sourcetype="leo\_dhcp\_logs" | top limit=10 srcip

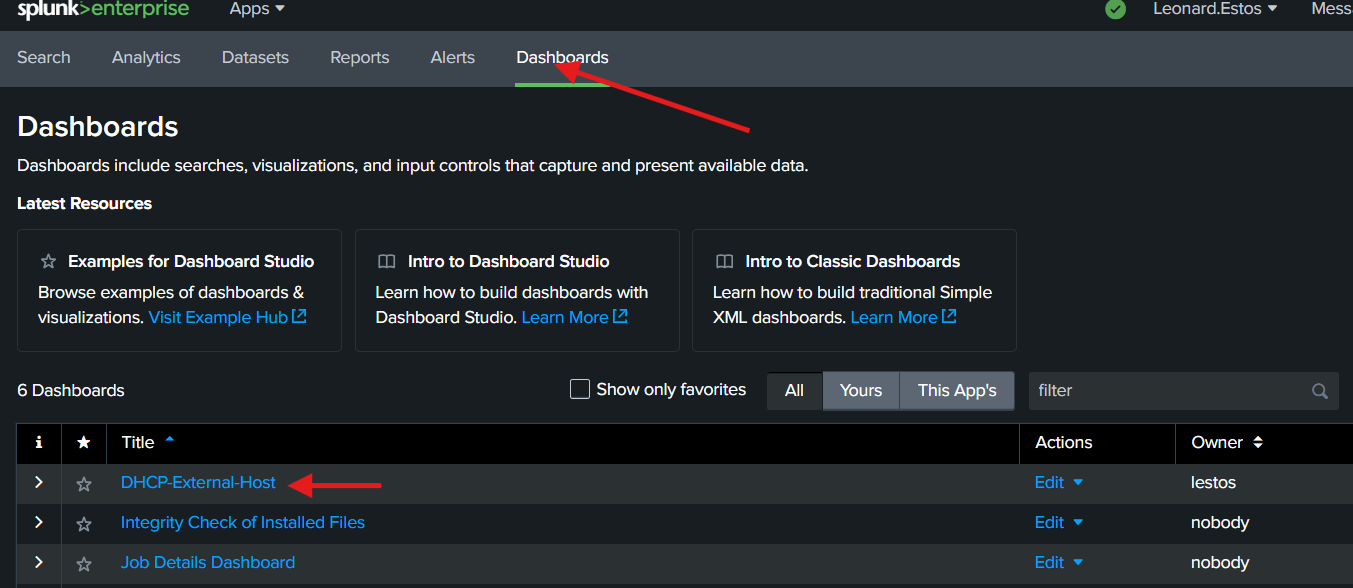
index=\* sourcetype="leo\_dhcp\_logs" | timechart span=1d count by leased\_ip

index=\* sourcetype="leo\_dhcp\_logs" | top limit=10 srcip, destip | dedup srcip, destip

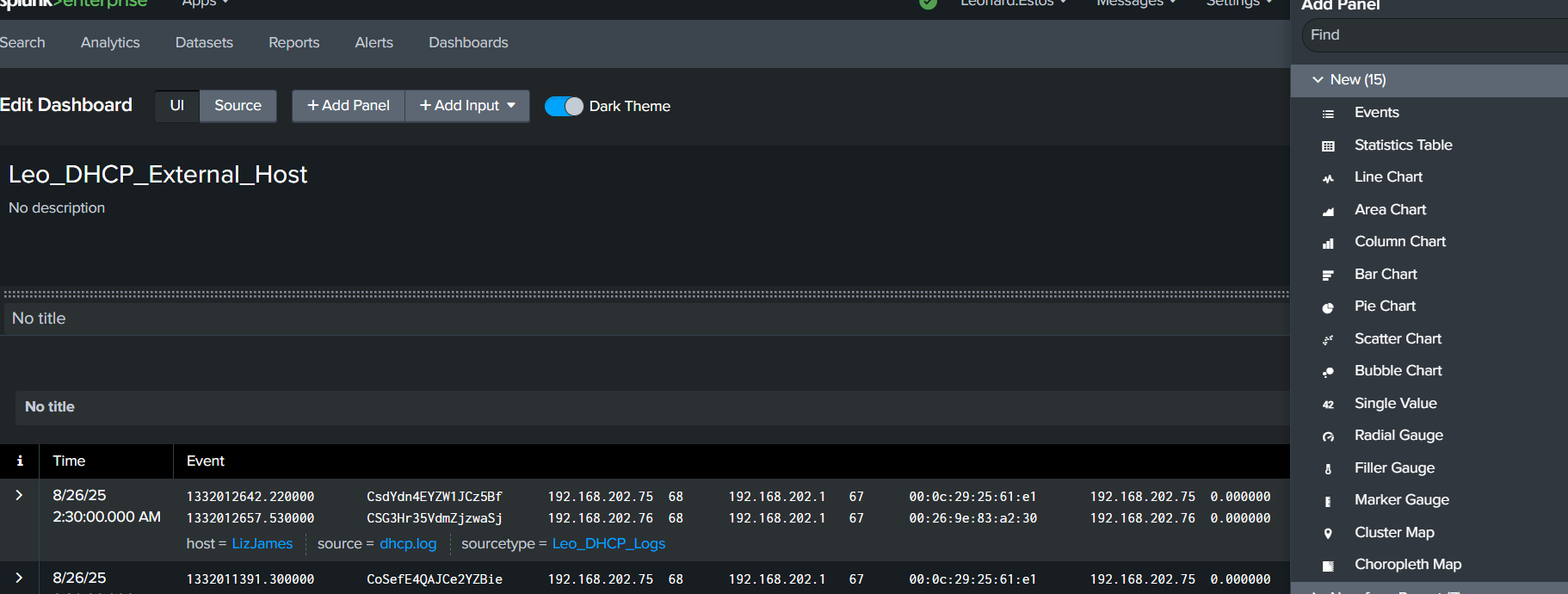


**How to create a new Dashboard in Splunk:**

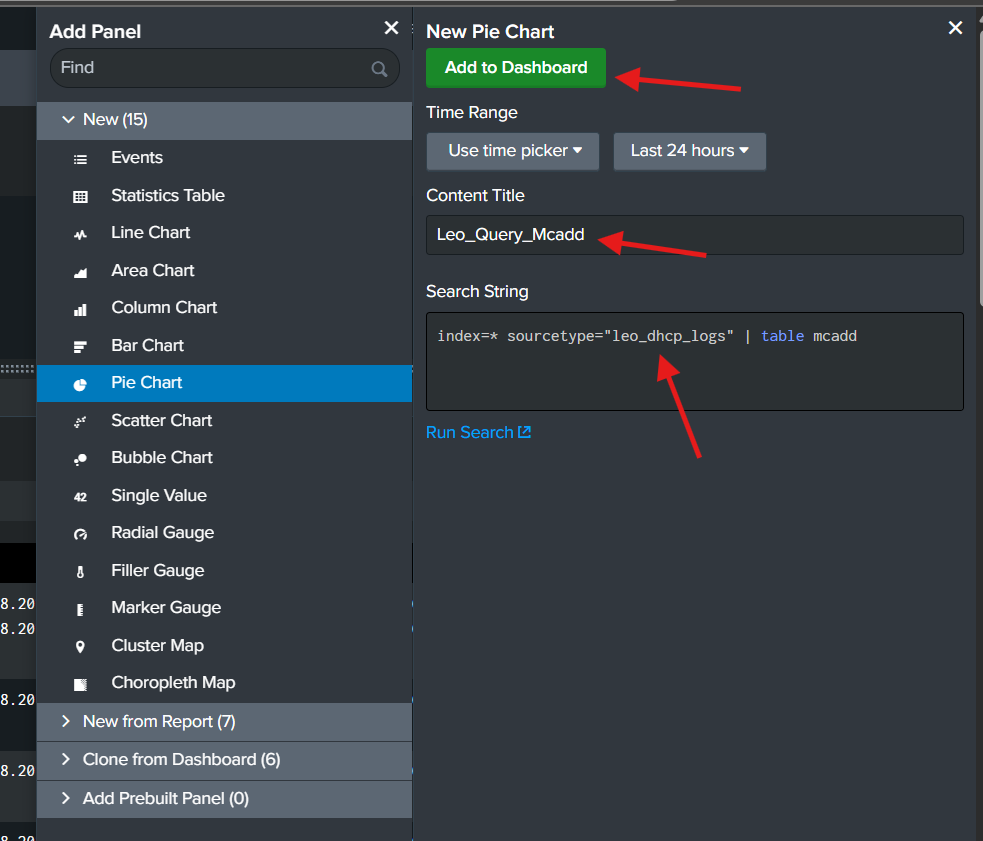
1. How to create a **new Dashboard** – The purpose of this is that your will not need to run the query again, just to to Dashboards only and check your created Dashboards
   1. Run query index=\* sourcetype="leo\_dhcp\_logs" | top limit=10 srcip, destip | dedup srcip, destip
   2. Click SAVE AS > New Dashboard > Click Save to Dashboard
   3. View this in the Dashboard



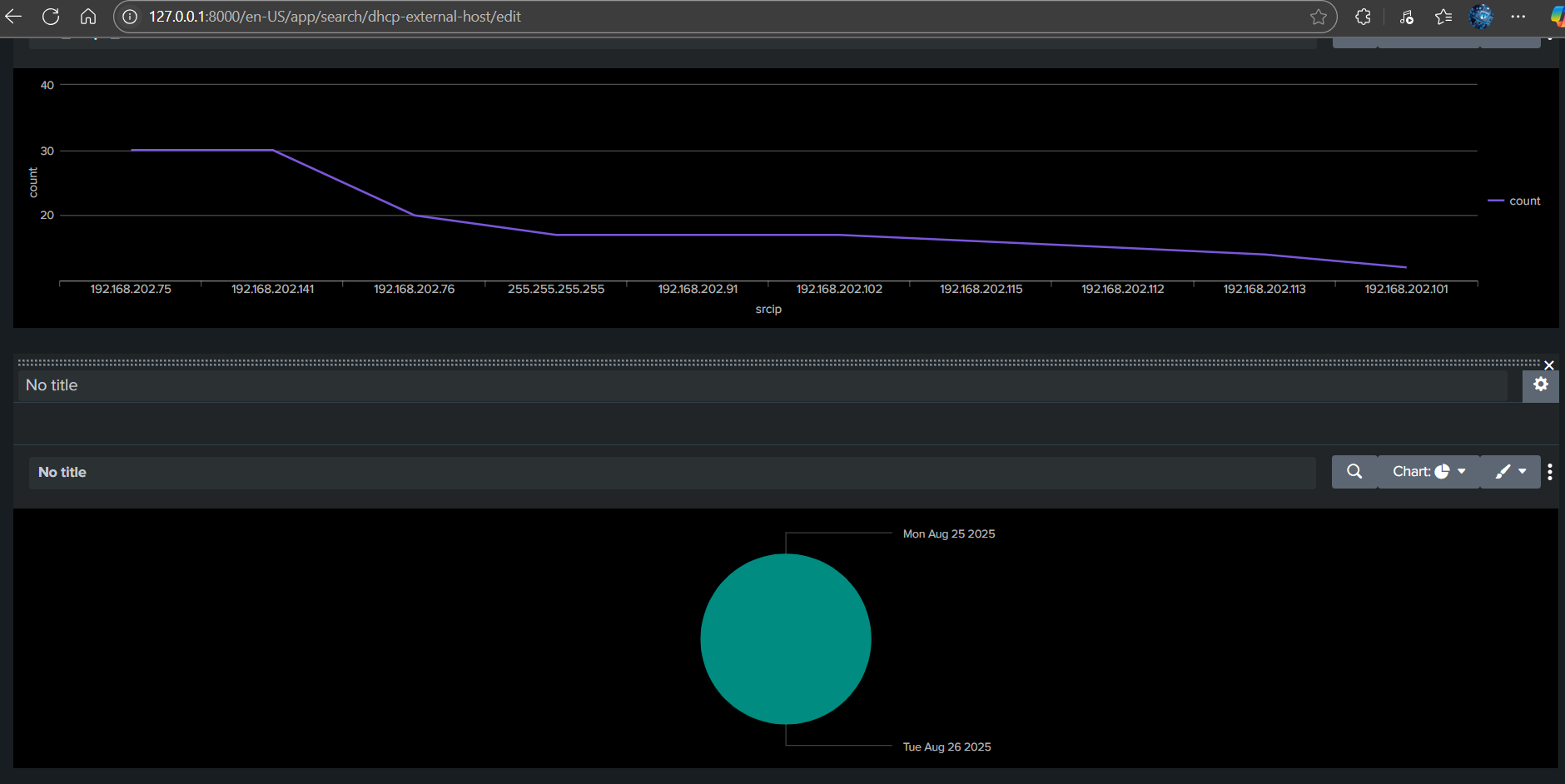
1. How to create a Dashboard with Graph for reporting.
   1. Click your Dashboard > Click Leo\_DHCP\_External\_Host > Click EDIT > Click Add Panel
   2. Choose any report that you want like graph



* 1. Put the Content Title > Search String/Query > ADD To Dashboard

****

* 1. Click SAVE > See Output Dashboard below.



**DNS Logs Analyses:**

1. Upload the DNS logs
2. Initial query once uploaded or default search.

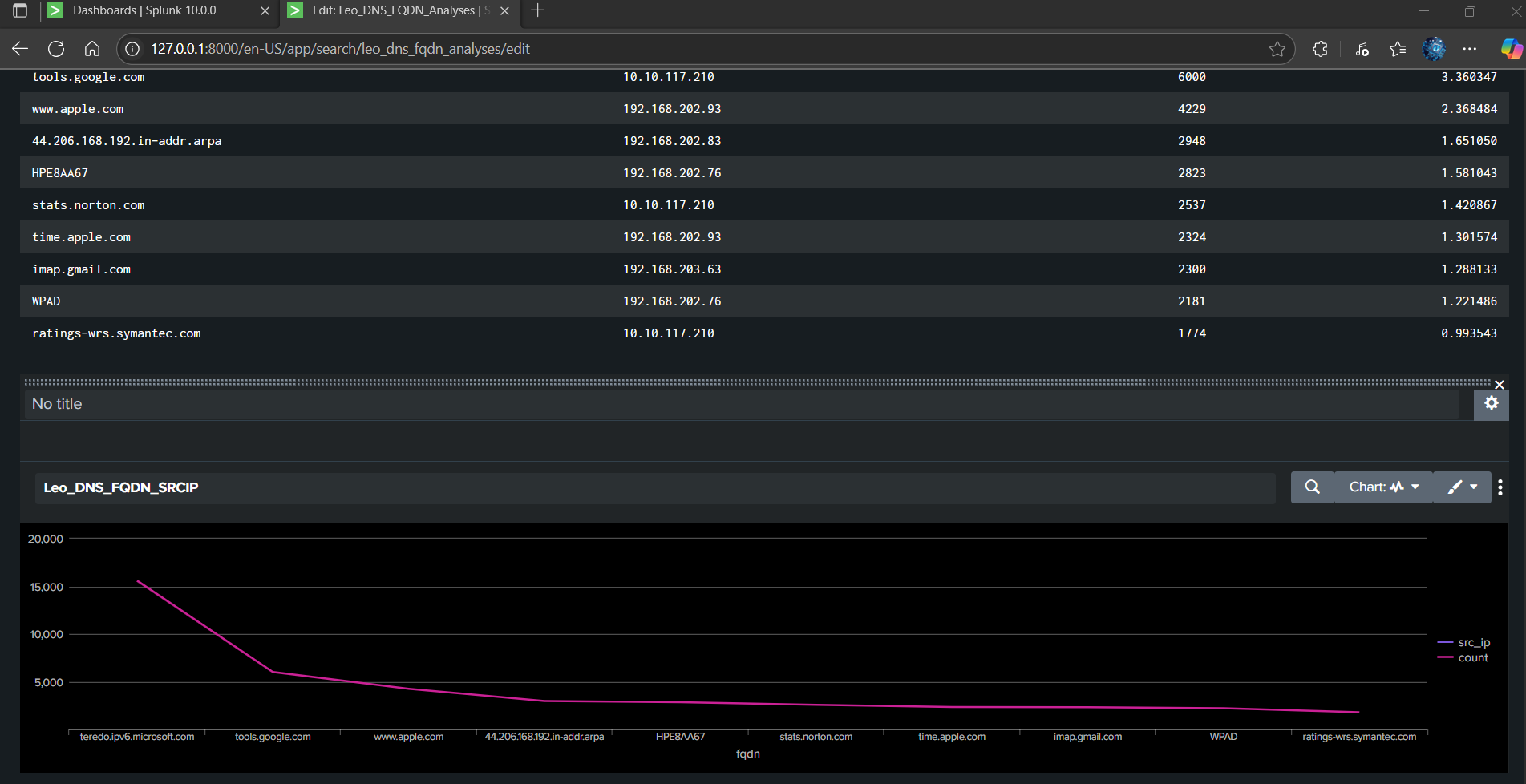
***source="dns.log" host="LizJames" sourcetype="Leo\_DNS\_Logs"***

1. Sample queries available in GitHub: <https://github.com/0xrajneesh/Splunk-Projects-For-Beginners/blob/main/Project%231-analyzing-dns-log-using%20splunk-siem.md>
2. Note, create your own **FIELDS** first and do the query below.

***index=\* sourcetype=Leo\_DNS\_Logs | top fqdn, src\_ip***

***index=\* sourcetype=Leo\_DNS\_Logs | top limit=20 fqdn*** = This will show DNS that is access as per count could be a malicious access.

1. Create a New Dashboard and Panel Report



**The Mitigation, Identification, Analysis, Response and Detection.**

1. **Go to**[***https://www.virustotal.com/gui/home/upload***](https://www.virustotal.com/gui/home/upload) **and check the File, URL, IP Address, and Domain that is Malicious.**
2. **Mx Toolbox**[***https://mxtoolbox.com/SuperTool.aspx***](https://mxtoolbox.com/SuperTool.aspx) **for Analyses | Reconnaissance as well.**

**SPLUNK Enterprise Security: This will be the SOC Analyst use all the time.**

*” When you train Smarter, you defend Stronger”*

*Leonard Estos*