**📄 Project Title: Advanced Apache Log Analysis with Splunk Dashboard**

**Project overview**

This project involves analyzing Apache access logs using Splunk. I created a custom dashboard with various visualizations to gain insight into HTTP request patterns, user activity, and potential errors on the server. The purpose is to simulate real world log monitoring and gain hands on experience in log parsing, field extraction, SPL querying, and visual dashboard creation.

**Dataset Used**

* **File Name**: apache\_logs.txt
* **Source Type**: access\_combined
* **Index**: apache\_logs
* **Host**: DESKTOP-U52N20A

**Steps Taken**

**1. Data Upload**

* Launched Splunk via http://127.0.0.1:8000
* Uploaded apache\_logs.txt
* Set **Source Type** as access\_combined
* Created a new **Index** named apache\_logs
* Saved and indexed the file successfully.

**2. Search Processing Language (SPL) Queries**

I ran several SPL queries to generate key metrics and data visualizations. The queries are listed below:

**Visualizations & Queries**

**1. Most Active Users (Bar Chart)**

* **SPL**:
* index=apache\_logs sourcetype=access\_combined
* | top limit=10 user
* **Insight**: The chart displayed a single row with no username, just a count of 20,000 — indicating that the user field is not properly captured or not present in the dataset.

**2. Top User Agents (Pie Chart)**

* **SPL**:
* index=apache\_logs sourcetype=access\_combined
* | top limit=10 useragent
* **Result**: No results found. Likely due to useragent not being extracted or present in this source type.

**3. Top IP Addresses (Bar Chart)**

* **SPL**:
* index=apache\_logs sourcetype=access\_combined
* | top limit=10 clientip
* **Insight**: Showed a bar chart of the top 10 IP addresses with their respective request counts. This helps in identifying the most frequent visitors to the web server.

**4. Top Requested URLs (Line Chart)**

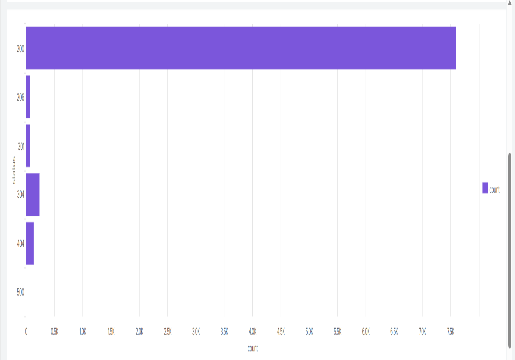
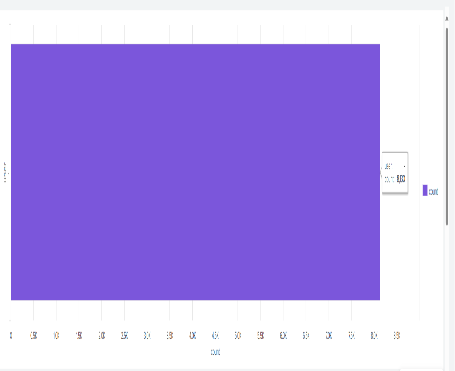
* **SPL**:
* index=apache\_logs sourcetype=access\_combined
* | top limit=10 uri\_path
* **Result**: No results found. The uri\_path field may not be auto-extracted or present in the uploaded file.

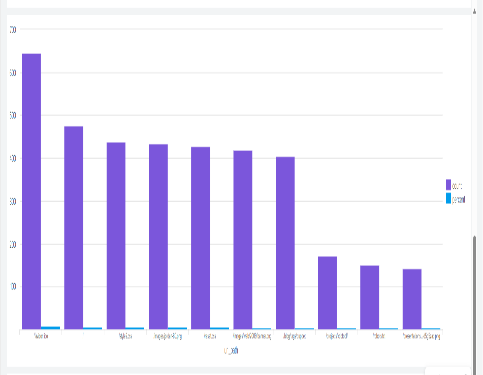
**Dashboard Setup**

* **Tool Used**: Splunk Dashboard Studio
* **Layout Mode**: Grid
* **Dashboard Type**: Classic (via Dashboard Studio)
* **Charts Added**:
  + Bar chart for clientip
  + Bar chart for user
  + Others showed no data

**Screenshots Captured**

1. Individual screenshots of the working charts:



1. SPL search page showing correct query and result for clientip (top IP addresses).

