**Splunk Project – Apache Access Log Analysis**

**Project Title:** Analyzing Apache Web Server Logs using Splunk

**Description:**

This project involved uploading real-world Apache access logs into Splunk and running key search queries to gain insights into server activity. The goal was to identify general trends, top resources accessed, frequent IP addresses, and client requests resulting in errors, all of which are essential for system monitoring and security operations.

**Log Upload Details:**

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

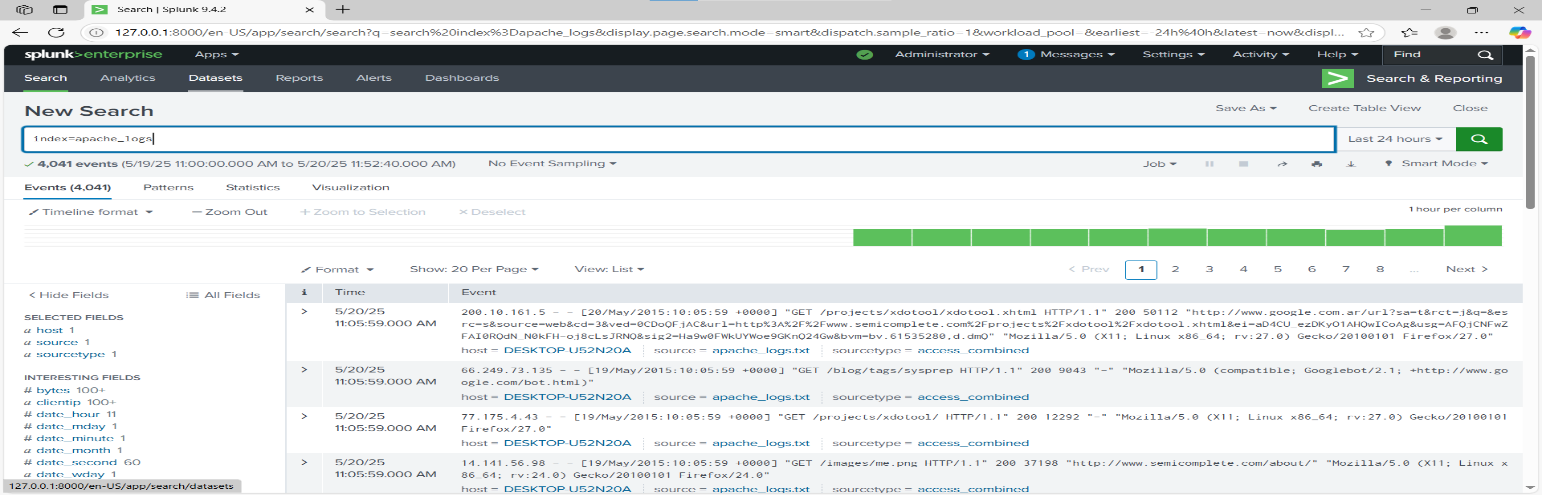
**Queries and Results**

**1. General Logs View**

**Search:**

index=apache\_logs

**Purpose:**  
To confirm data ingestion and view all available log entries. This is useful for baseline activity monitoring and general troubleshooting.

**Screenshot:**  


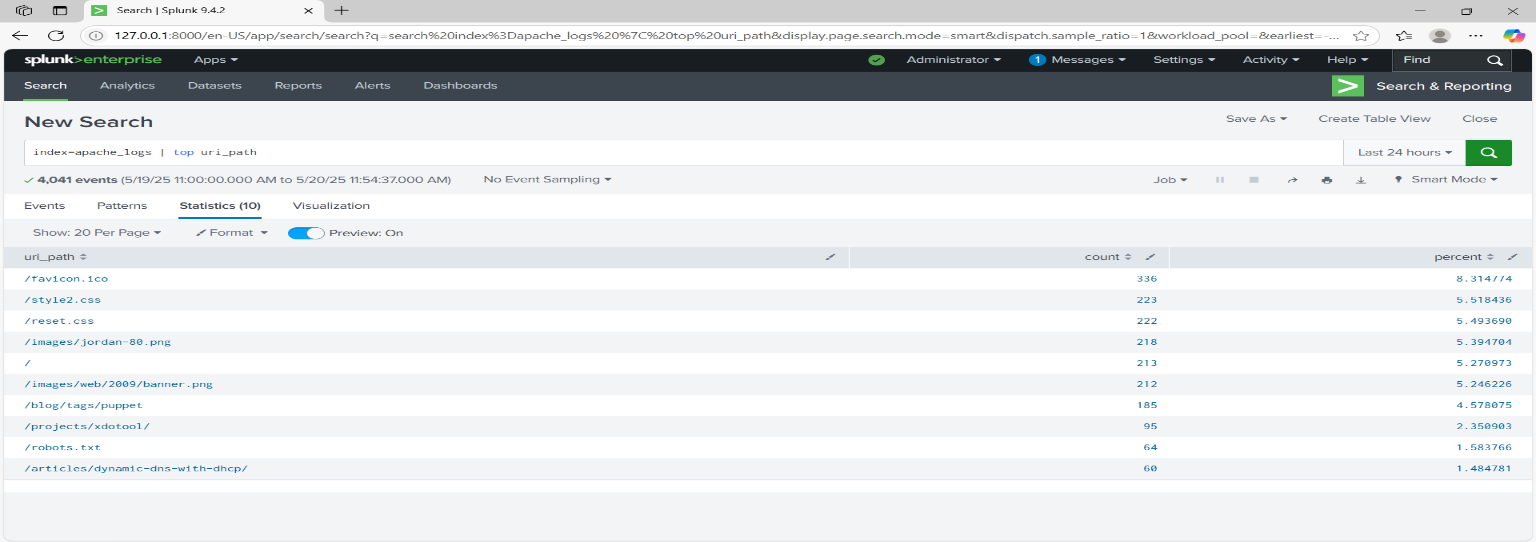
**2. Top Requested URLs**

**Search:**

index=apache\_logs | top uri\_path

**Purpose:**  
To identify the most frequently accessed web resources. This helps with performance monitoring and detecting abnormal access patterns (e.g., repeated hits to sensitive paths).

**Screenshot:**



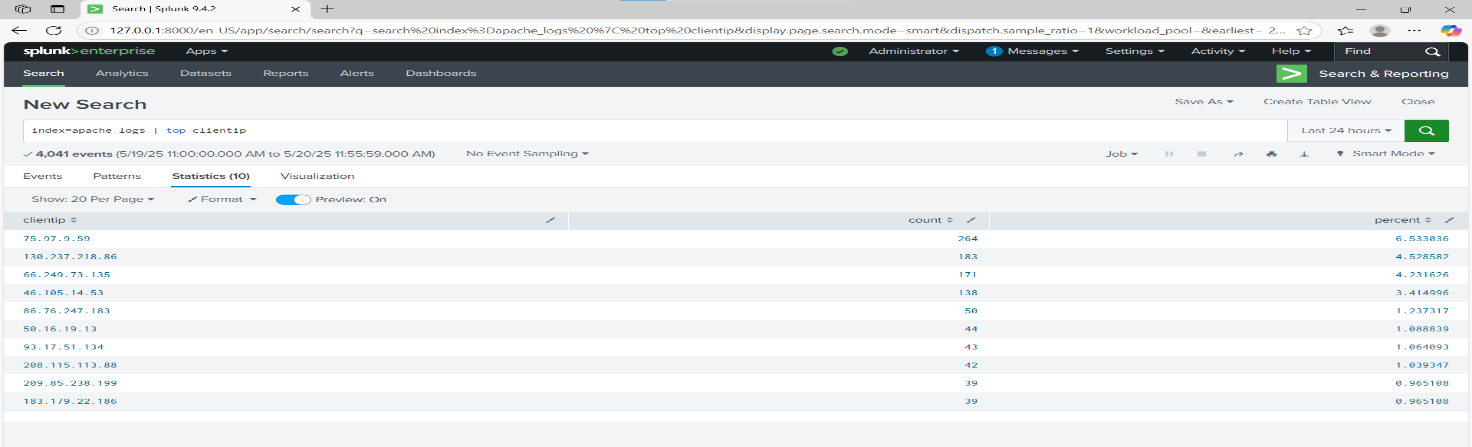
**3. Top Client IPs**

**Search:**

index=apache\_logs | top clientip

**Purpose:**  
To track which IP addresses generate the most traffic. Useful in detecting potential attackers, DDoS sources, or identifying heavy users.

**Screenshot:**



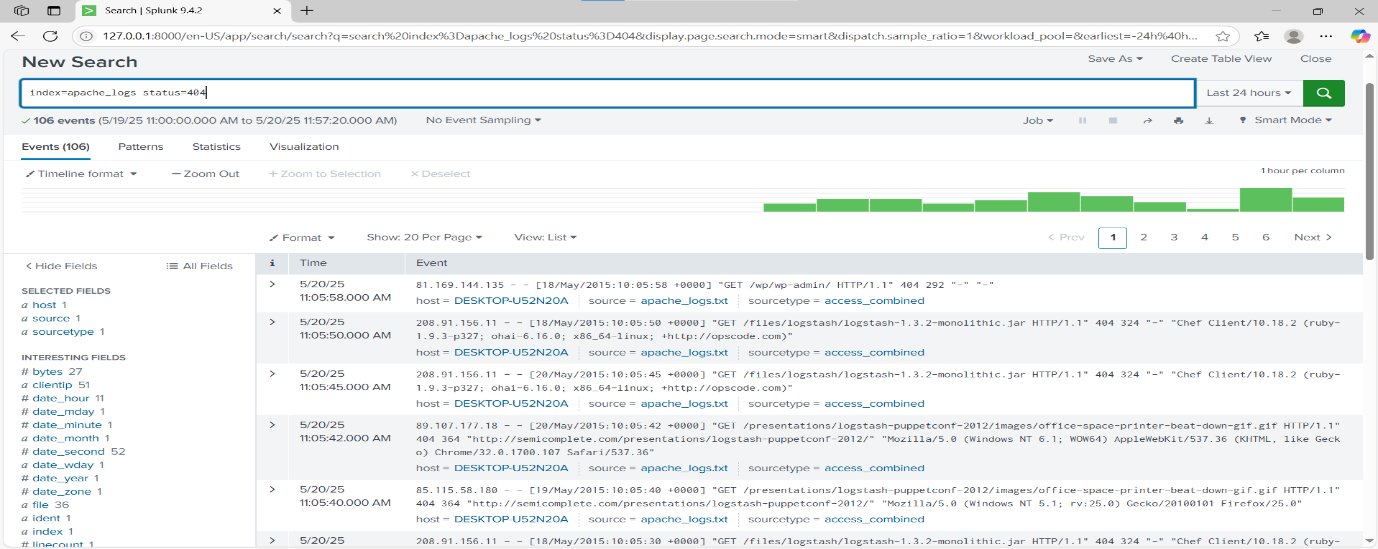
**4. 404 Not Found Errors**

**Search:**

index=apache\_logs status=404

**Purpose:**  
To monitor failed access attempts. Repeated 404s may indicate broken links, misconfigured services, or probing by attackers.

**Screenshot:**



**Security and Operational Relevance**

|  |  |
| --- | --- |
| **Query** | **Relevance in Organizations** |
| index=apache\_logs | Baseline monitoring and verification of incoming logs. |
| top uri\_path | Understanding user behavior; detecting abuse of certain endpoints. |
| top clientip | Identifying suspicious or high-volume sources. |
| status=404 | Spotting scans for vulnerabilities or missing/misconfigured resources. |