Project Title: HTTPS Log Traffic Analysis & Threat Investigation Using Splunk SIEM

Project Objective

To validate the successful ingestion of HTTPS logs in Splunk, analyze traffic behavior through port and IP pattern analysis, and identify potential anomalies such as beaconing, misconfiguration, or internal compromise by drilling into high-traffic destination IPs and their associated source hosts.

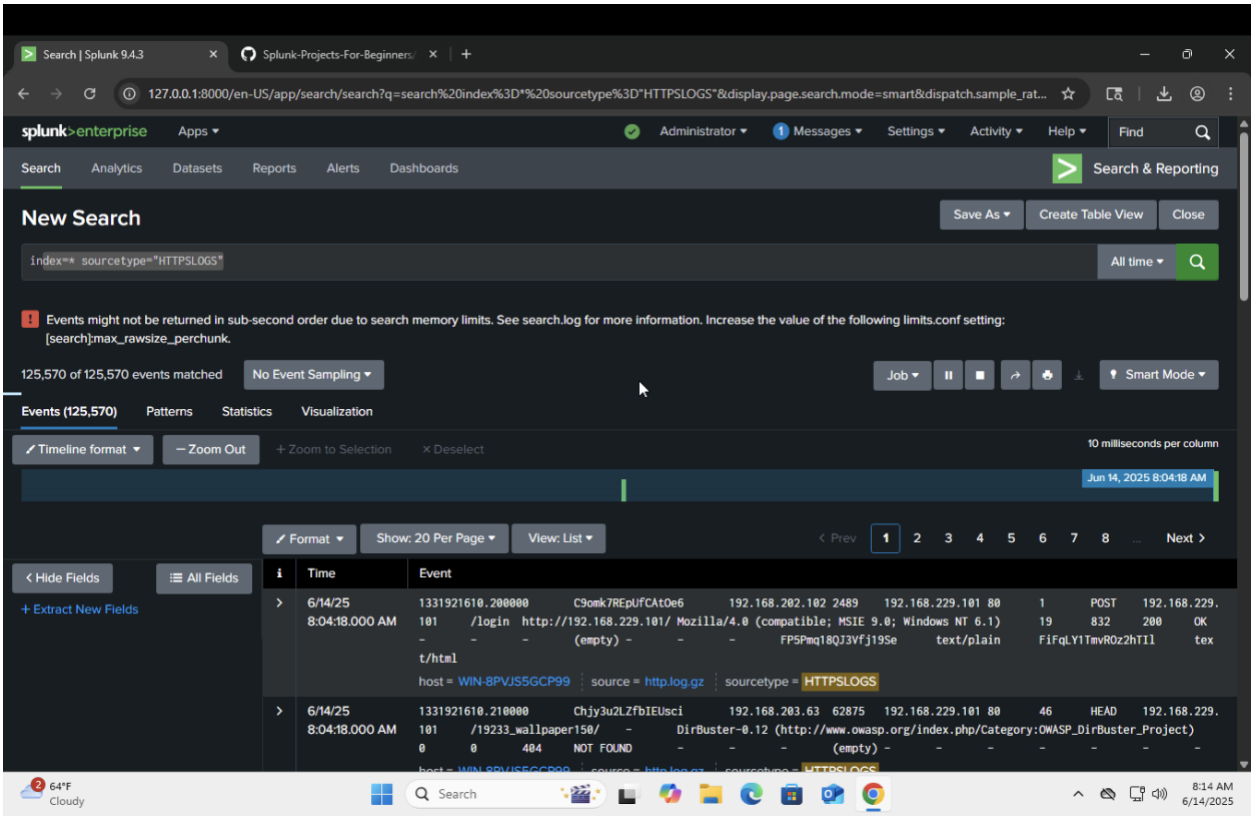
Tools & Technologies Used

- **Splunk Enterprise** (SIEM platform)
- **SPL (Search Processing Language)** for querying
- **HTTPS Log Dataset**
- **Sourcetype:** `HTTPSLOGS`
- **Indexes Used:** `index=*`, `index=_*`

1. Validating HTTPS Logs Ingestion

Objective:
To verify that logs with the sourcetype `HTTPSLOGS` are properly indexed and visible in the Splunk environment before proceeding with detailed analysis.

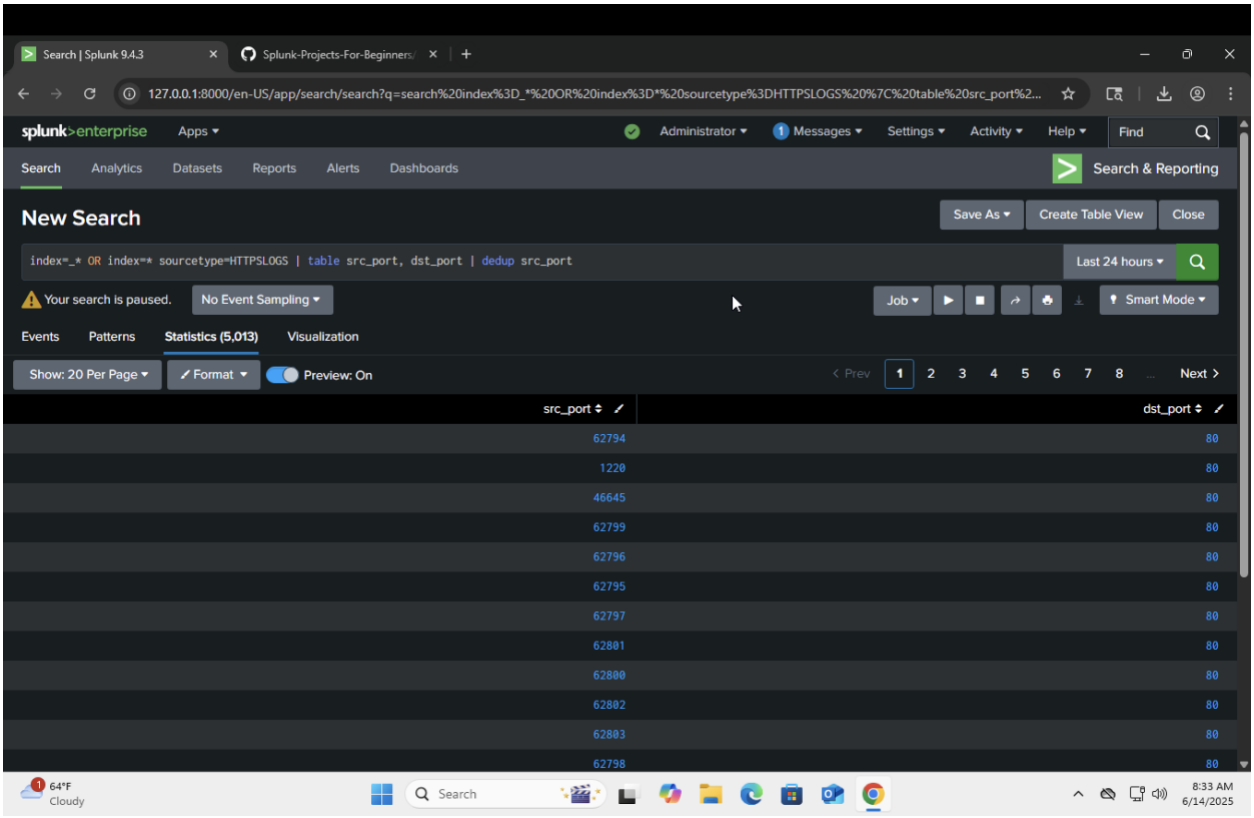
Confirmed that `HTTPSLOGS` entries were successfully ingested and searchable, laying the foundation for further inspection of secure web traffic behavior.



2. Deduplicated Port Analysis in HTTPS Logs

Objective:
To extract and display a unique list of source ports involved in HTTPS communications, along with corresponding destination ports, helping detect unusual or non-standard ports.

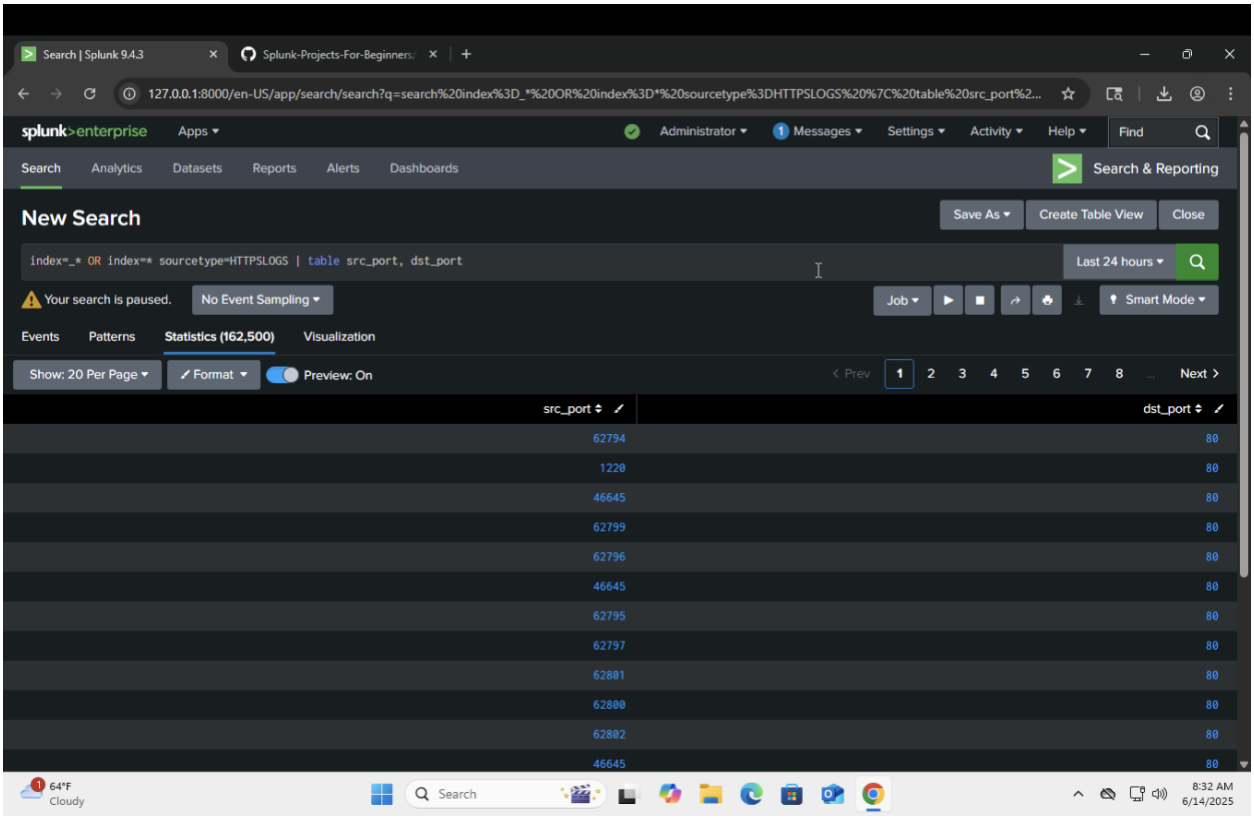
Outcome:
Produced a deduplicated list of source ports and associated destination ports, offering clarity on port usage trends and potentially suspicious traffic behavior.



3. Reviewing Port Distribution in System and HTTPS Indexes

Objective:
To analyze HTTPS log data across both default (`index=*`) and internal Splunk system indexes (`index=_*`), ensuring no relevant port activity is overlooked.

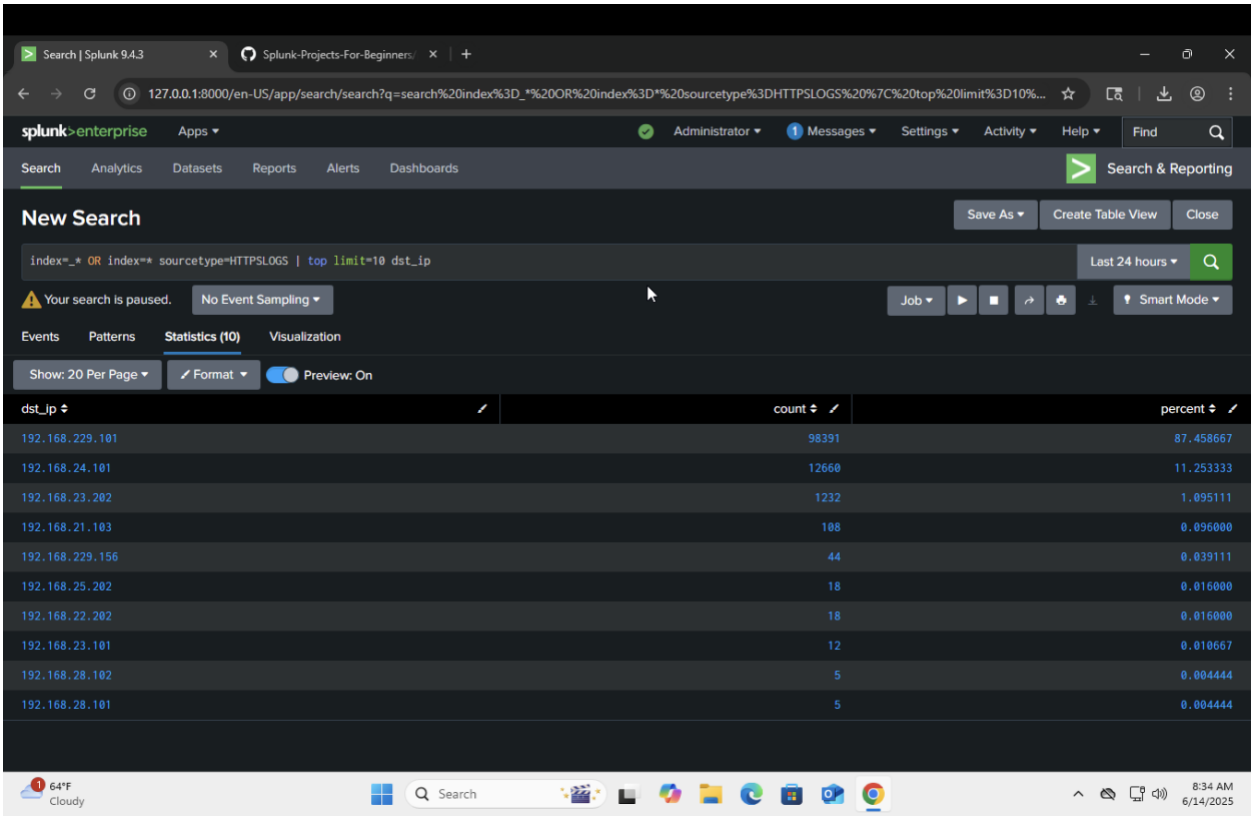
Outcome:
Returned a complete view of `src_port` and `dst_port` across all available indexes, confirming that port activity tied to HTTPS logs is captured and uniformly available.



4. Identifying Top Destination IPs in HTTPS Logs

Objective:
To identify the most frequently contacted destination IP addresses across all logs tagged with `HTTPSLOGS`. This step is critical for spotlighting high-traffic endpoints that may be legitimate services—or potential exfiltration or beaconing targets.

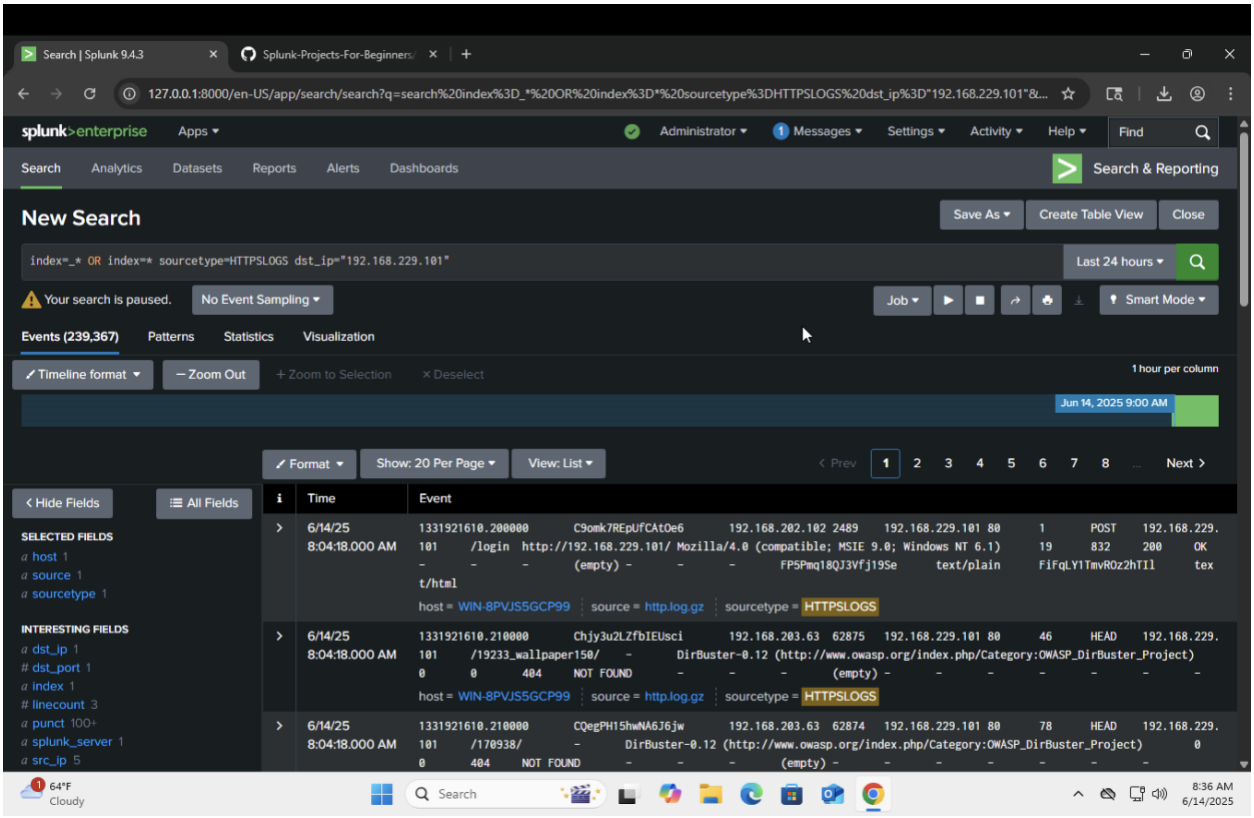
Outcome:
Discovered that the IP address `192.168.229.101` appeared **98,391 times**, making it the top destination in the data set. This raised flags for possible internal server activity, misconfigured systems, or targeted communications worthy of deeper inspection.



5. Deep-Dive on High-Volume Destination IP

Objective:
To conduct a focused query on the specific destination IP (`192.168.229.101`) identified in Step 4. The goal was to isolate all logs involving this IP and analyze the nature of its interactions, helping determine if this is normal system behavior or an anomaly.

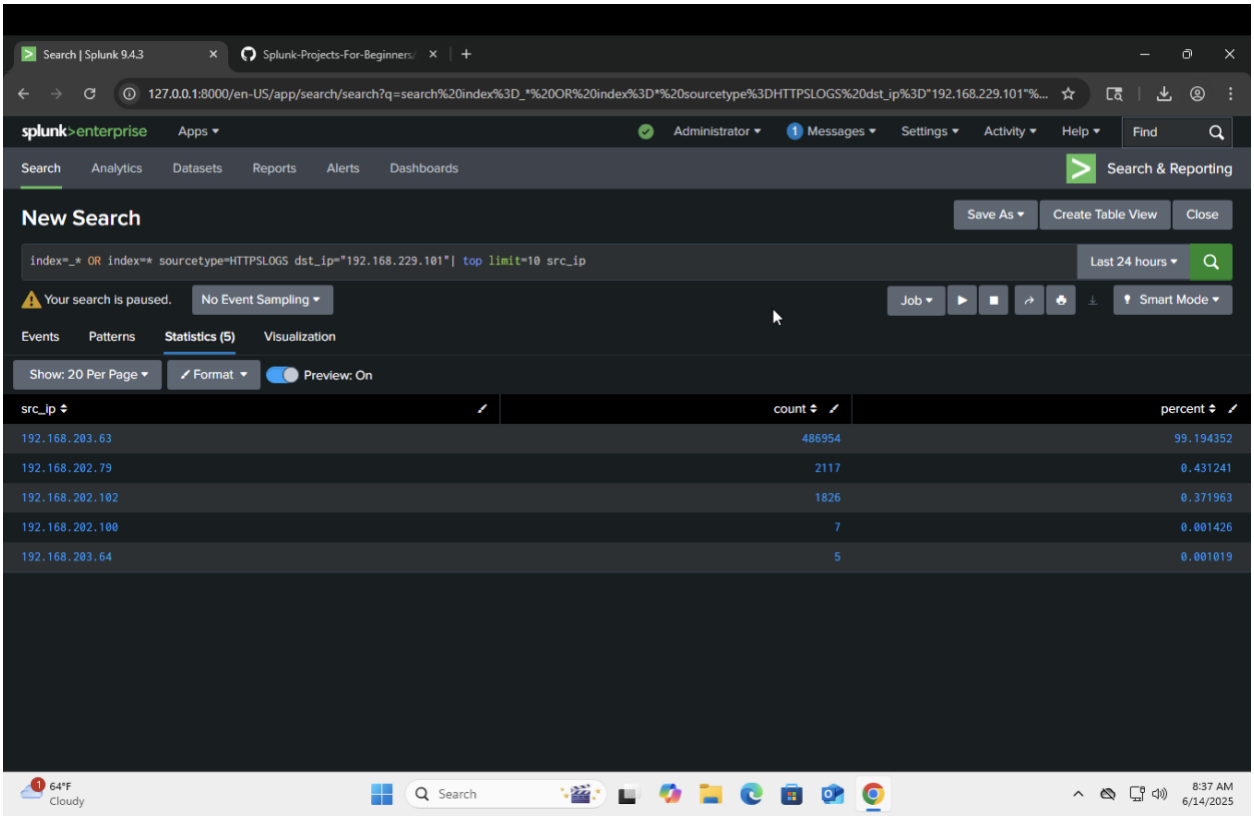
Outcome:
Retrieved all relevant entries for `192.168.229.101`, enabling further inspection of traffic patterns, involved source systems, and communication volume. This step allowed for targeted threat hunting, log correlation, or escalation for network segmentation if needed.



6. Identify Top Source IPs Communicating with Suspicious Destination

Objective:
To determine which source IP addresses have communicated most frequently with the high-volume destination IP `192.168.229.101`. This step helps uncover which internal systems or users are involved in this traffic, which could indicate misconfiguration, scanning activity, or even compromised endpoints.

Outcome:
Generated a ranked list of the top 10 source IPs contacting `192.168.229.101`. This narrowed the investigation to specific internal hosts and provided a shortlist of endpoints for deeper forensic review or threat correlation.



Conclusion

This project successfully leveraged Splunk SIEM to transform raw HTTPS log data into actionable intelligence. By systematically validating ingestion, extracting key fields, and analyzing high-frequency communication patterns, the investigation surfaced critical insights about internal traffic behavior. It also demonstrated how Splunk can help detect potentially compromised systems or misconfigurations in enterprise environments.