We will use the below commands to showcase how we can use search and dashboarding feature in Splunk:

Searching and reporting feature:

We can Filtering the Data from log files based on one or multiple columns:

| from datamodel:"Zanbil_web_logs" | search request = *image*

| from datamodel:" Zanbil_web_logs " | search client = '31.56.103.4' and referer = *search*

We can also calculate some Basic Stats for a particular feature:

| from datamodel:" Web_logs " | search client = "5.236.43.10" | stats count

Aggregation using Group by – Top 10 Customers with highest web activity

| from datamodel: "Web_logs" | stats count by client | sort count desc | head 10

No of users referred from Website – We will use regex feature in this

| from datamodel:"Web_logs" | rex field=_raw "(?<referer>\w+)\.(com|net|gov|edu|co|ir)" | search referer != "-" | stats count by referer | sort by count desc | head 10

Create a new column of time and showcase distinct user for every hour

| from datamodel: "Web_logs" | eval hour =strftime(_time,"%H") | stats dc(client) by hour

Dashboarding

Distinct user for every 30 mins – Timechart

| from datamodel: "Web_logs" | eval hour =strftime(_time,"%H") | timechart span=30m dc(client) as distinct_users

No of users referred from Website – Bar chart

| from datamodel:"Web_logs" | rex field=_raw "(?<referer>\w+)\.(com|net|gov|edu|co|ir)" | search referer != "-" | stats count by referer | sort by count desc | head 10