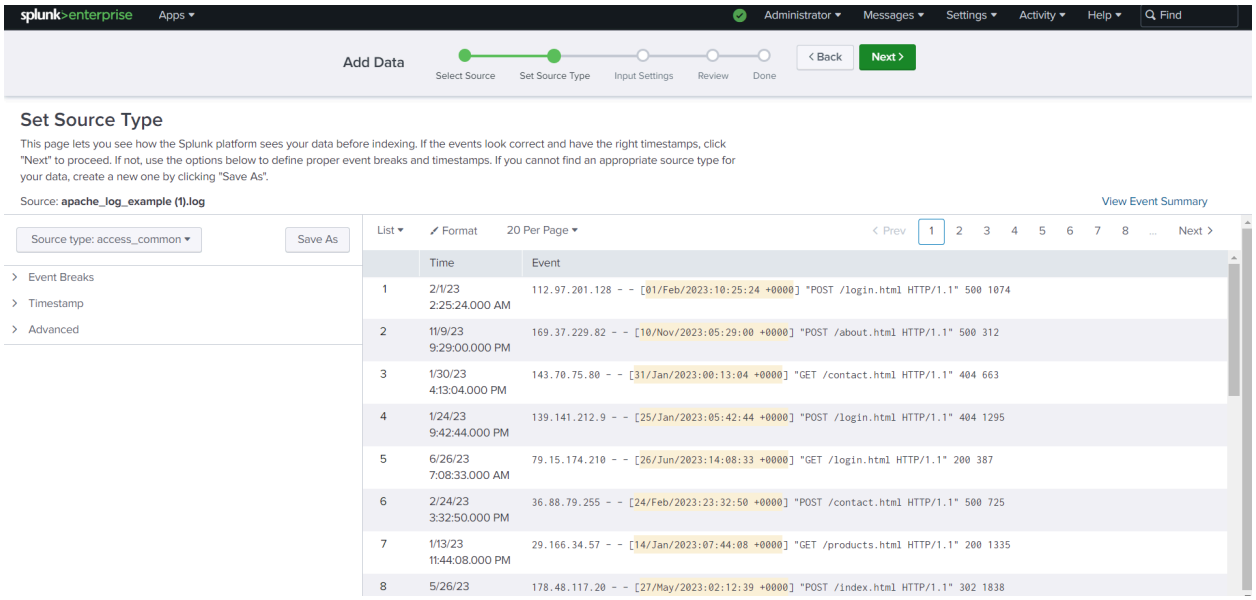
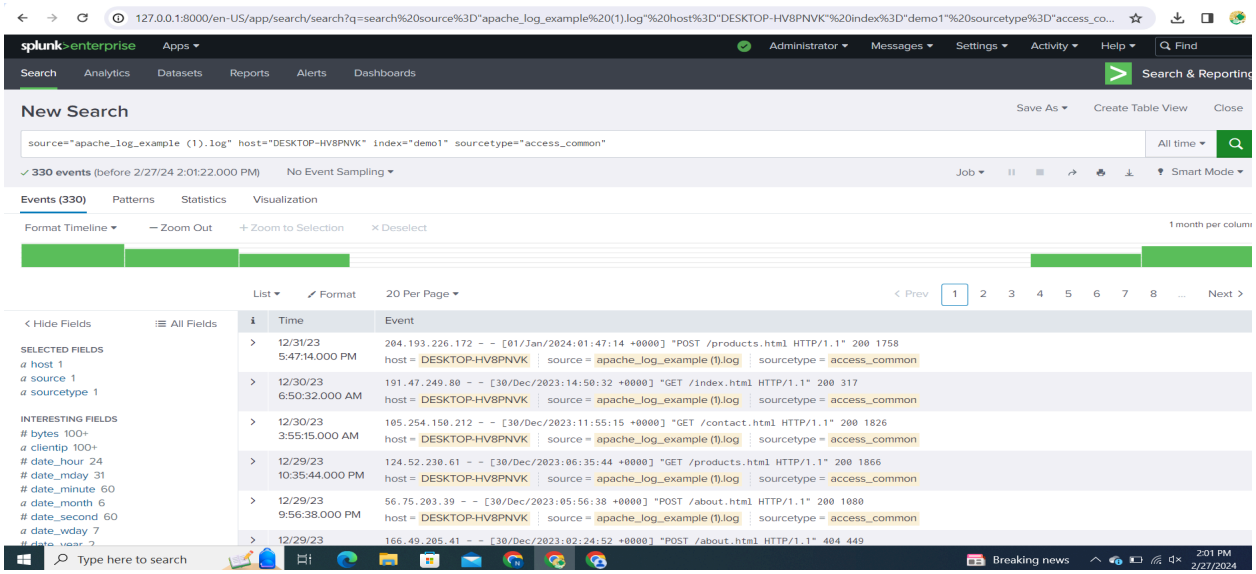
Splunk Analysis Assignment: Apache Log Investigation

The dataset provided in the assignment is a simulated Apache log file containing 1000 entries. Each entry includes details such as the client's IP address, request date and time, the requested resource, HTTP response code, and the size of the response.

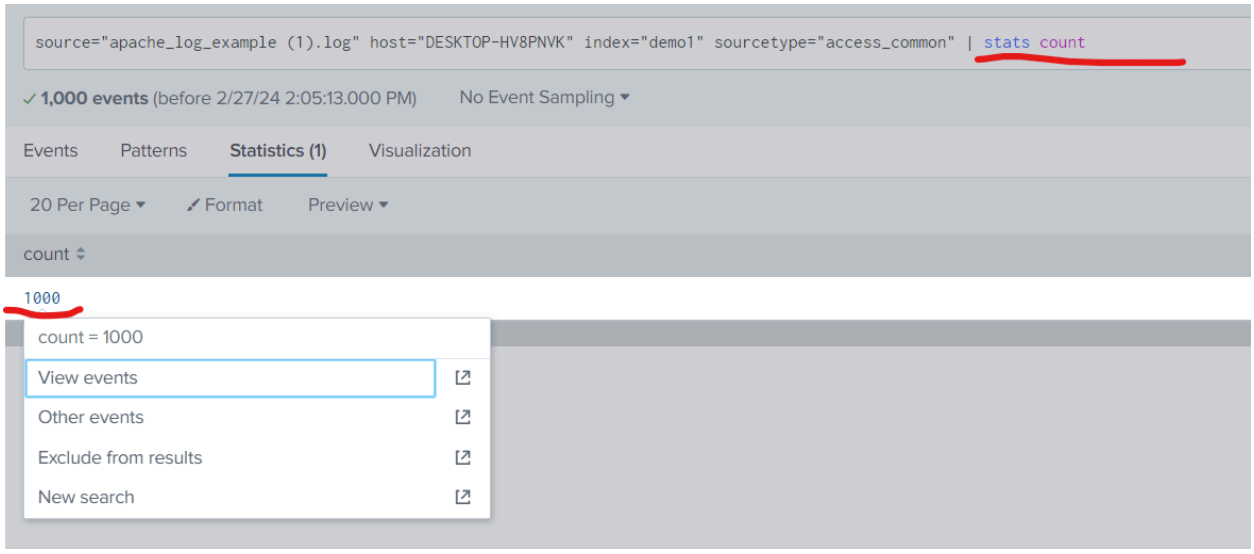
Adding the dataset in splunk and uploading it in the splunk.

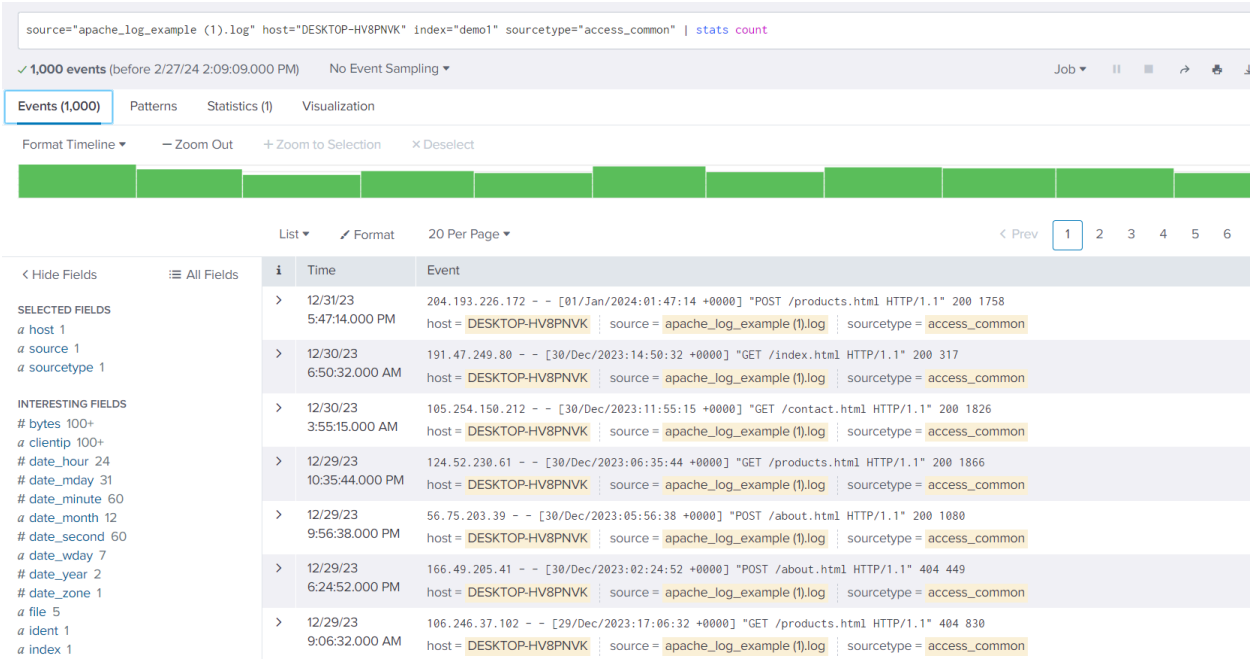


Results of scan and report are events and its shows the logs with event id and timestamp. All total 1000 events

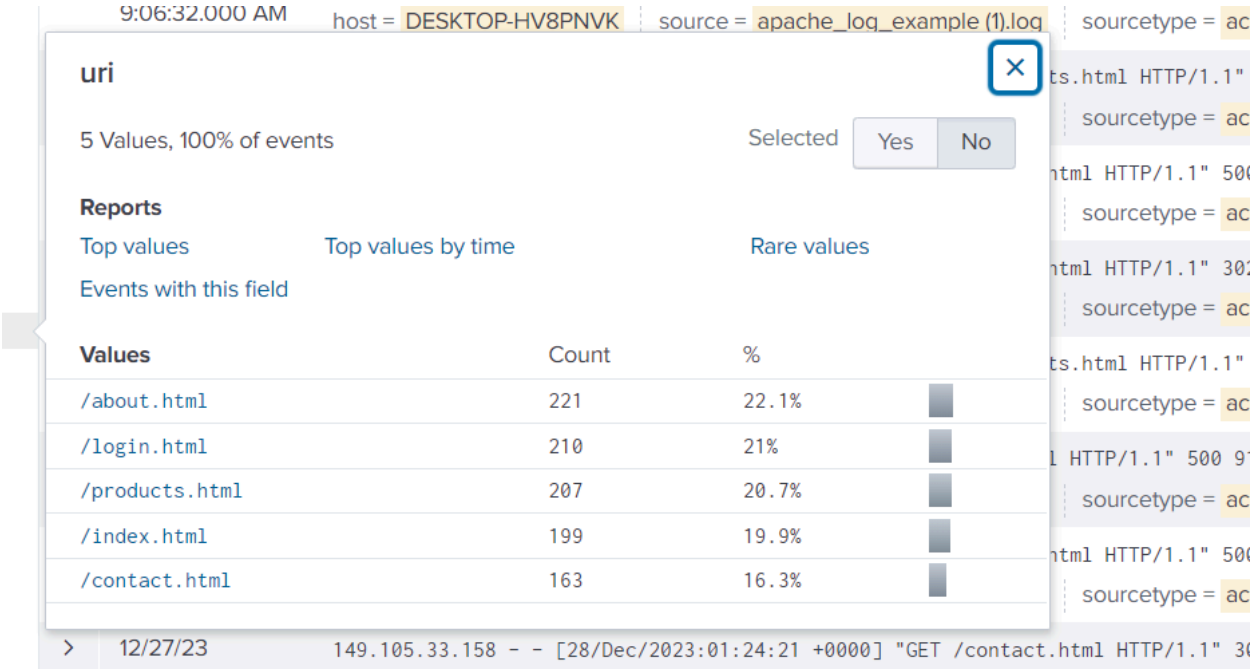


- How many requests were made?



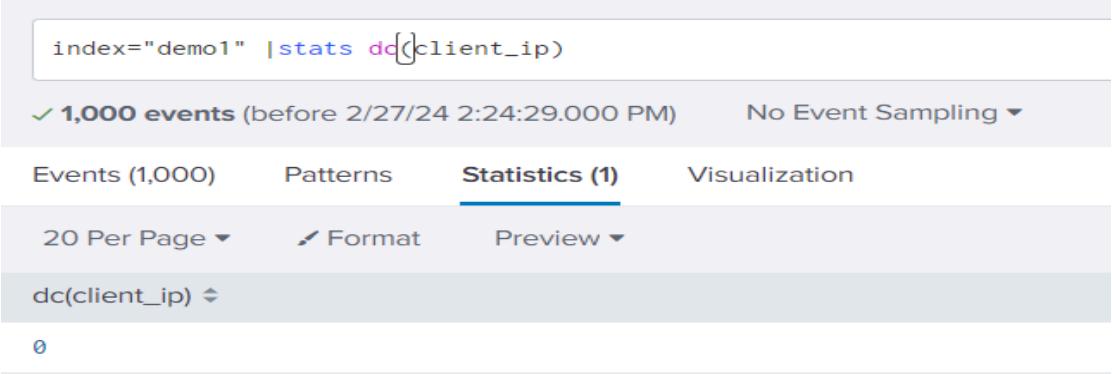


- What are the top requested URLs?



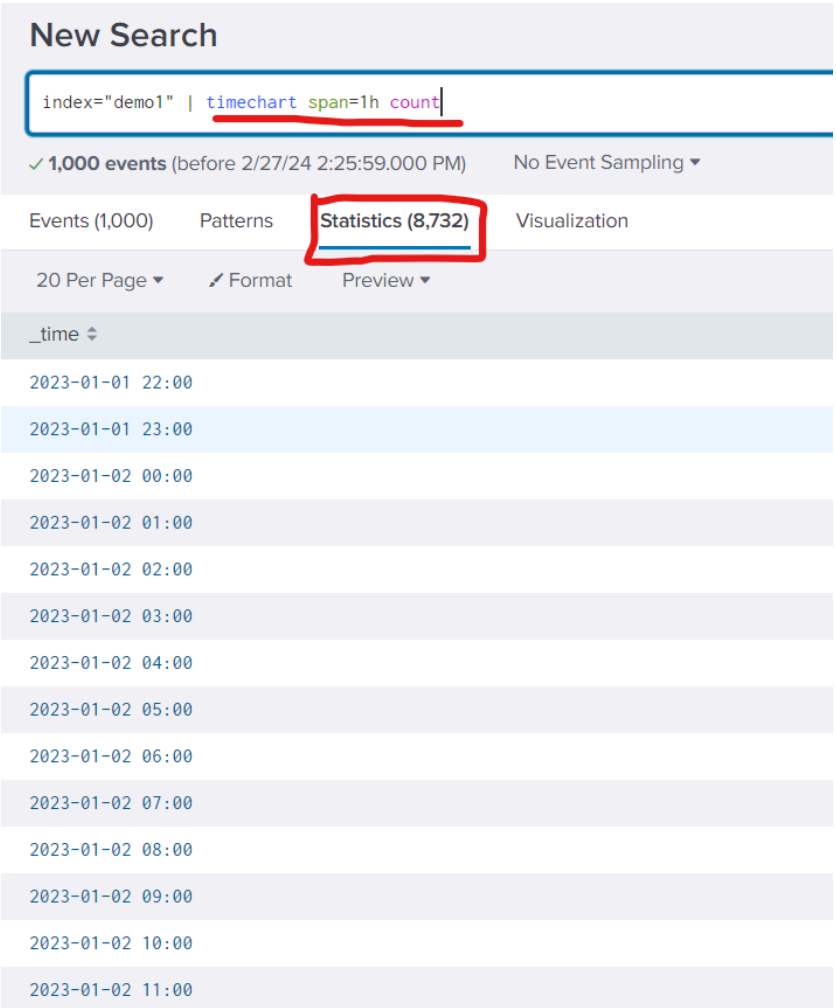
- What are the most common response codes?

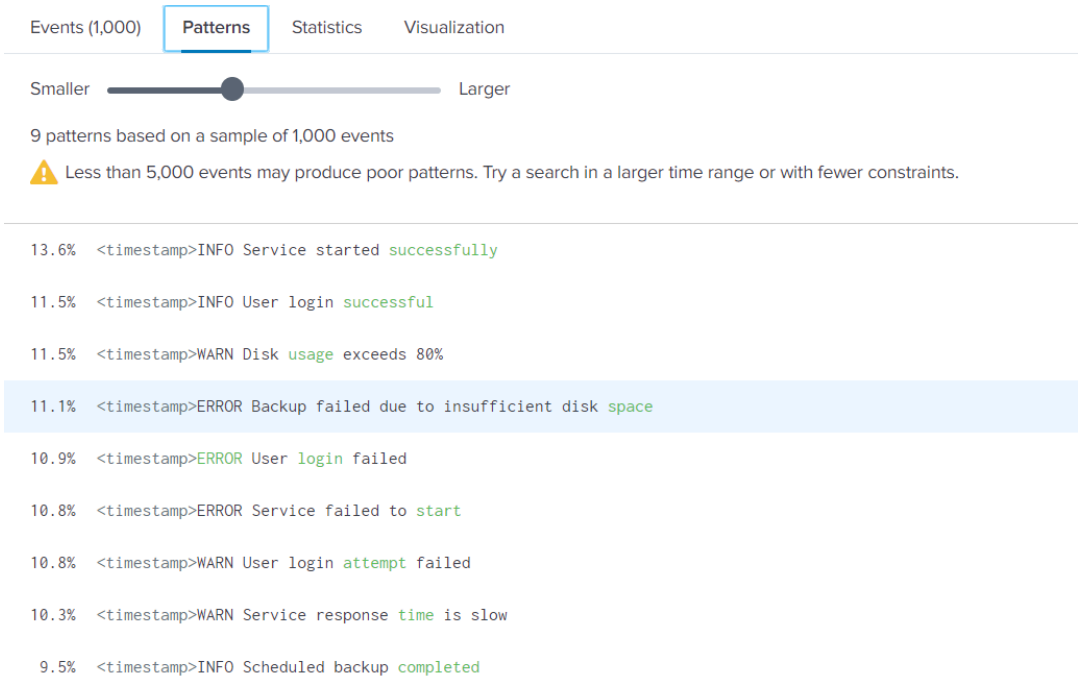
Mostly the replies are 404,200,302, 500



The splunk auto advance search queries.

Time analysis -





If we create a table view we can get all the logs in a table format where you can cleary read the event.