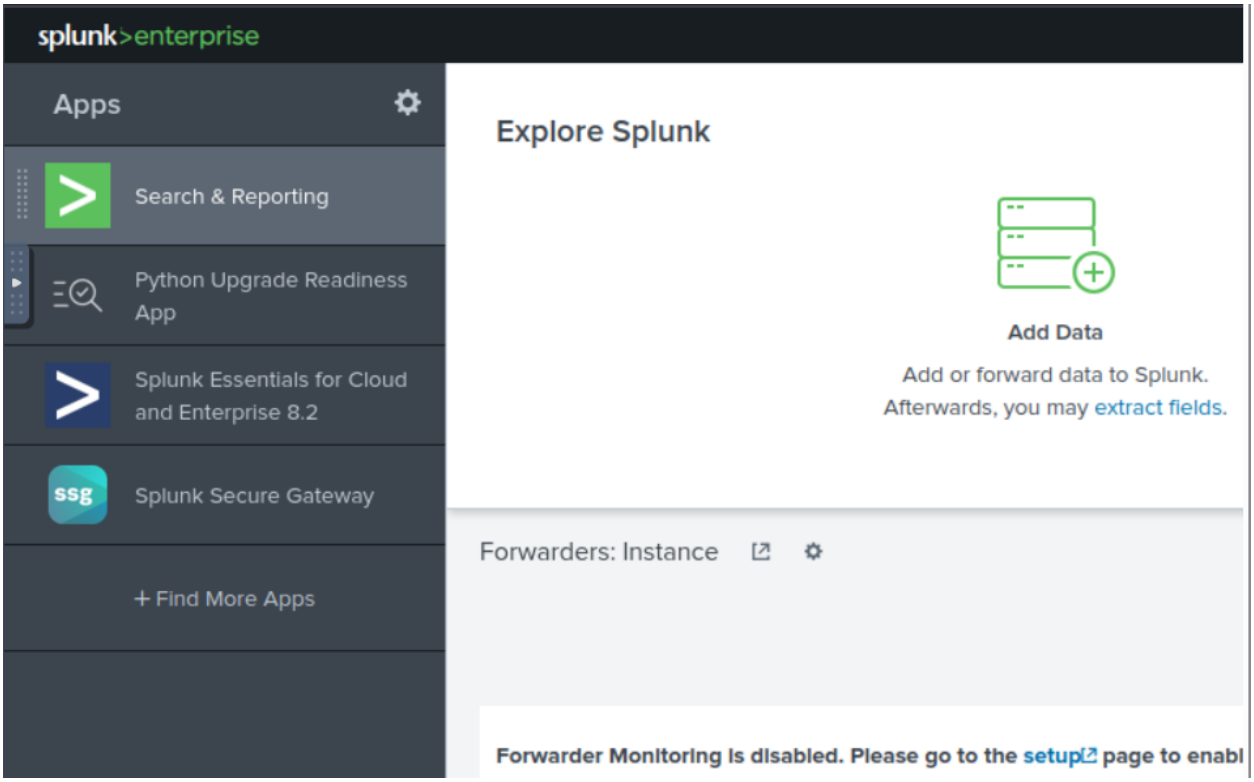
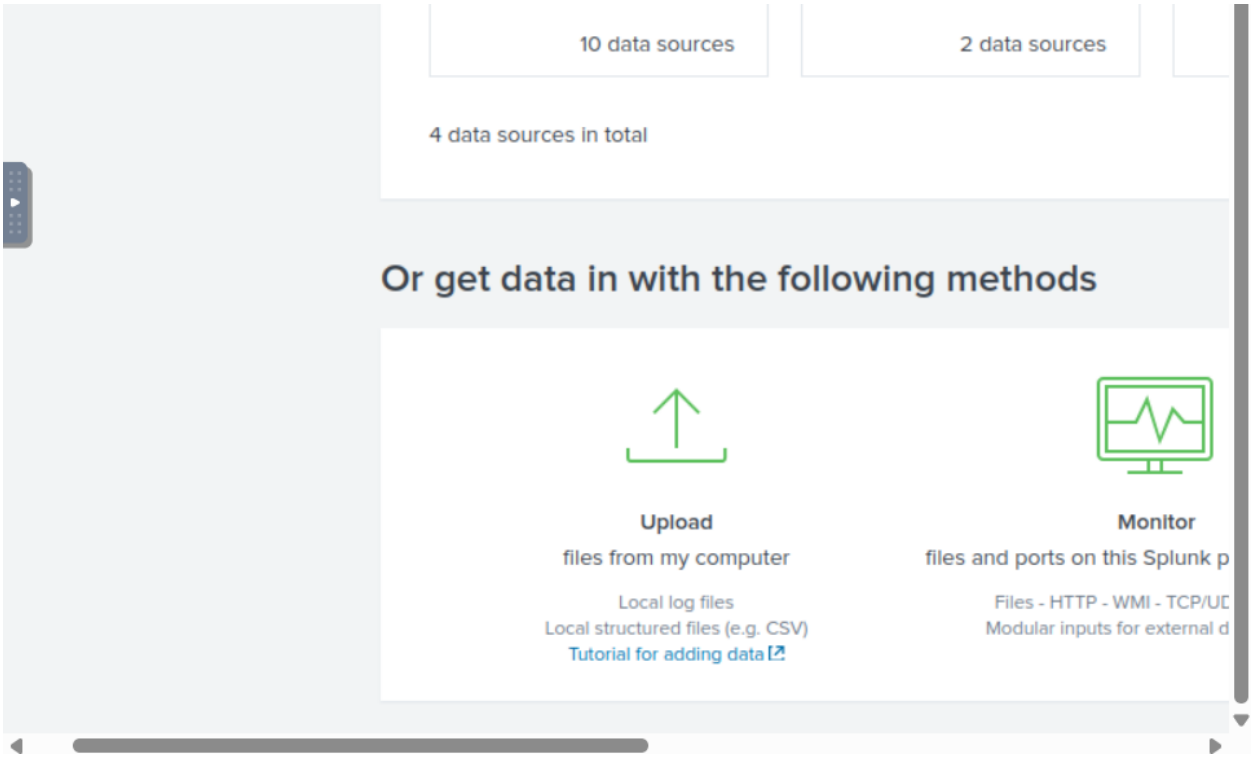
SPLUNK BASIC Report 2025/12/08

Objective: Ingesting log data into splunk and performing a log analysis.

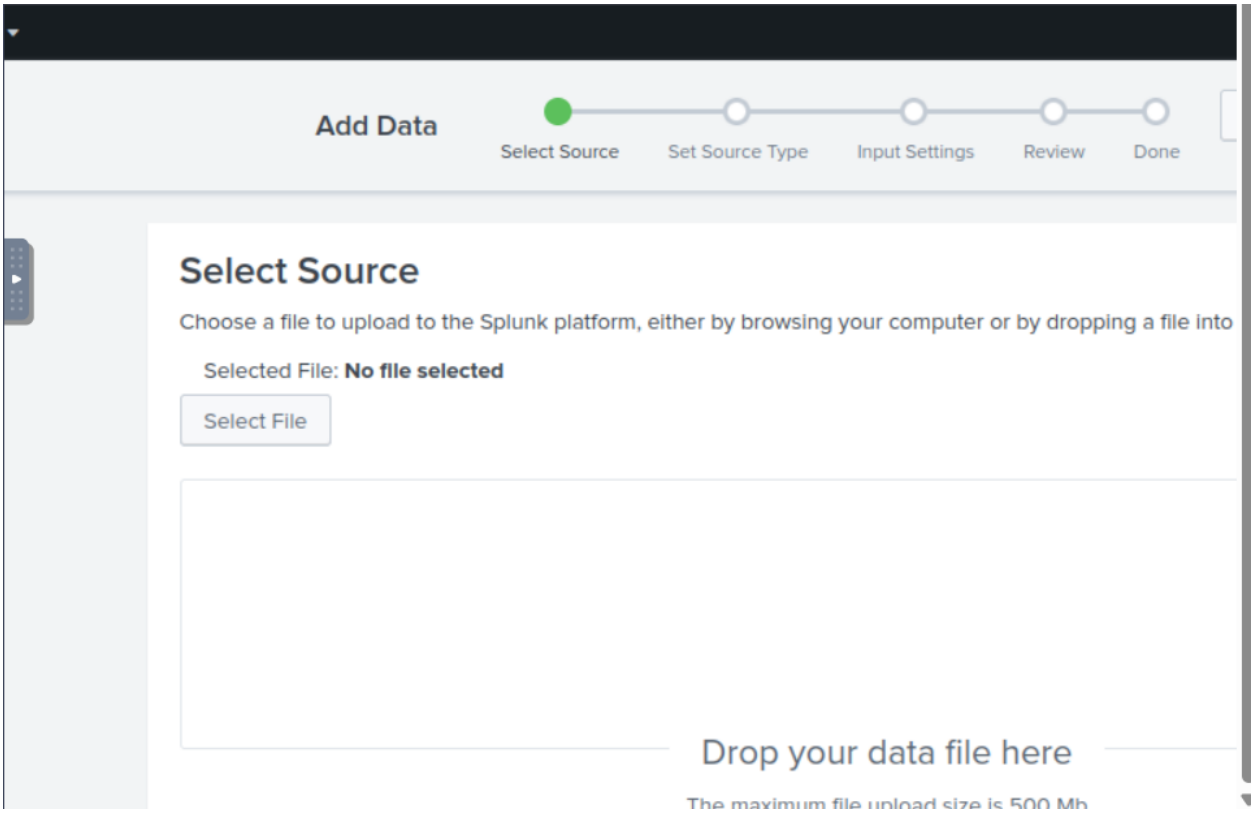
STEP 1: Loading splunk as a web application and ingesting data.



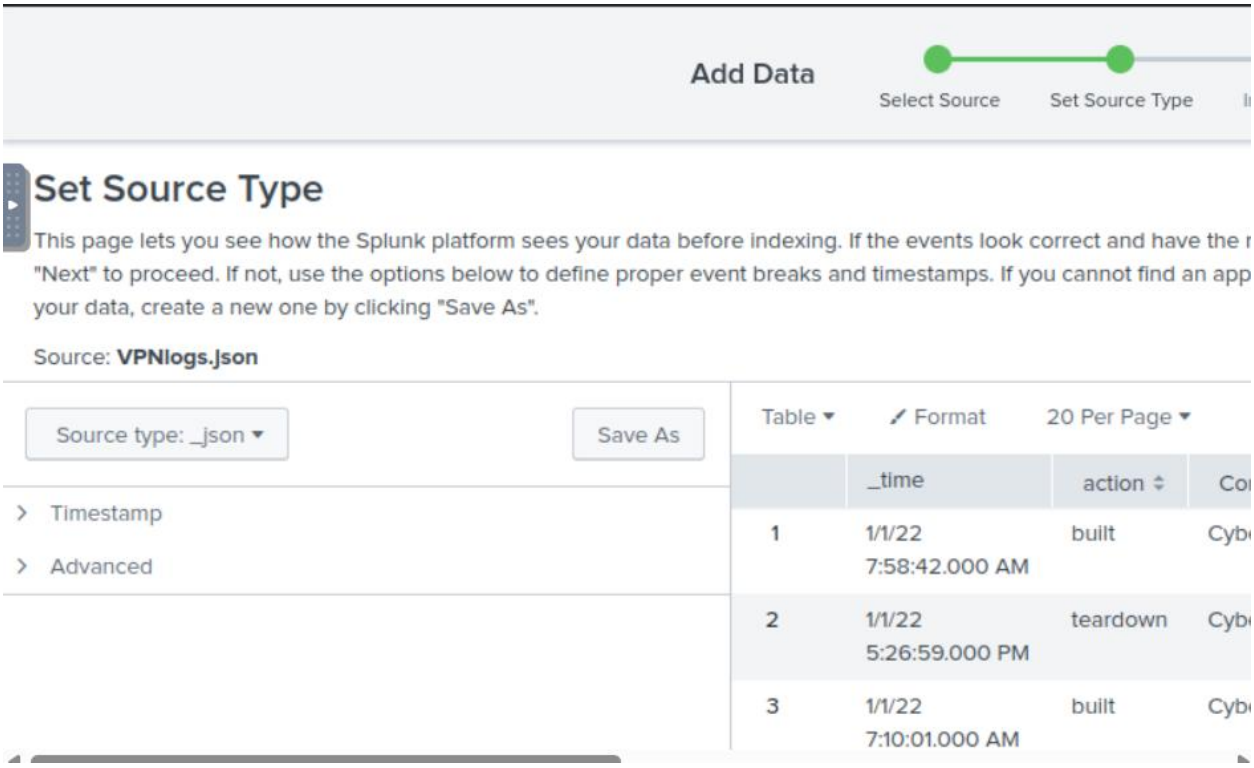
I clicked ‘Add Data’ in the ‘Explore Splunk’ section.



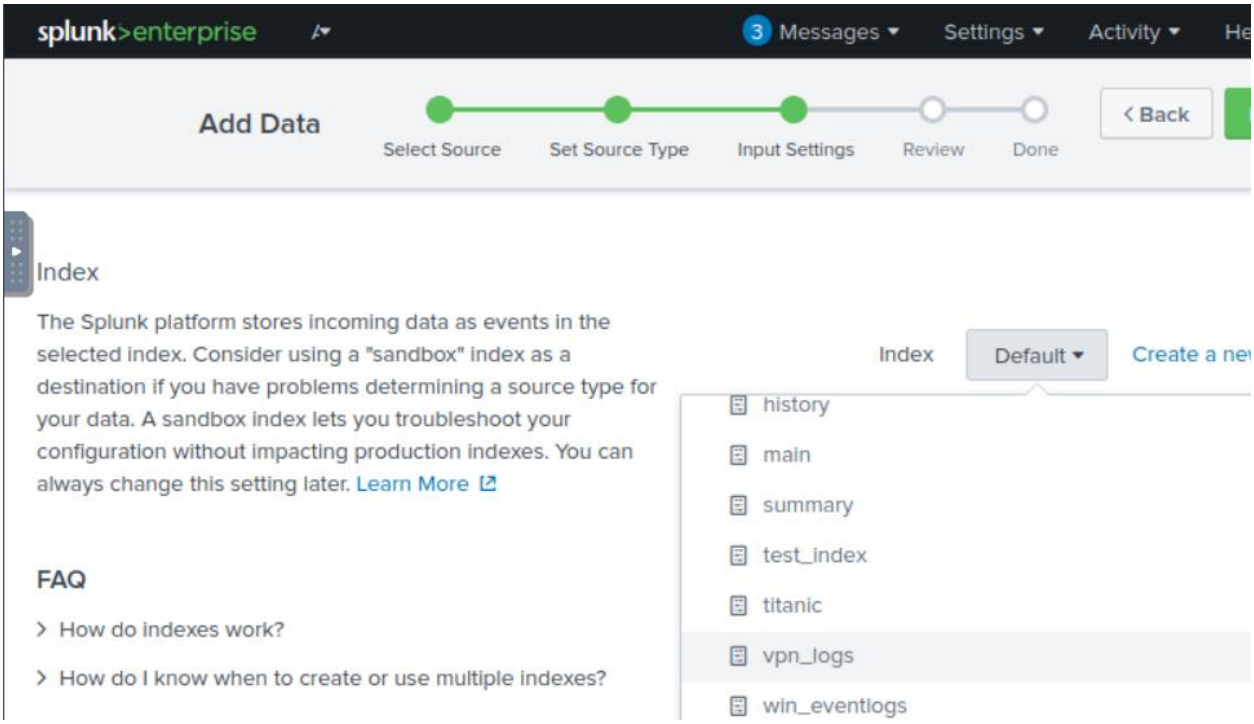
I then scrolled down just a bit and clicked on ‘Upload’, navigated my way to the correct directory then into the correct folders to upload the relevant files from my computer.



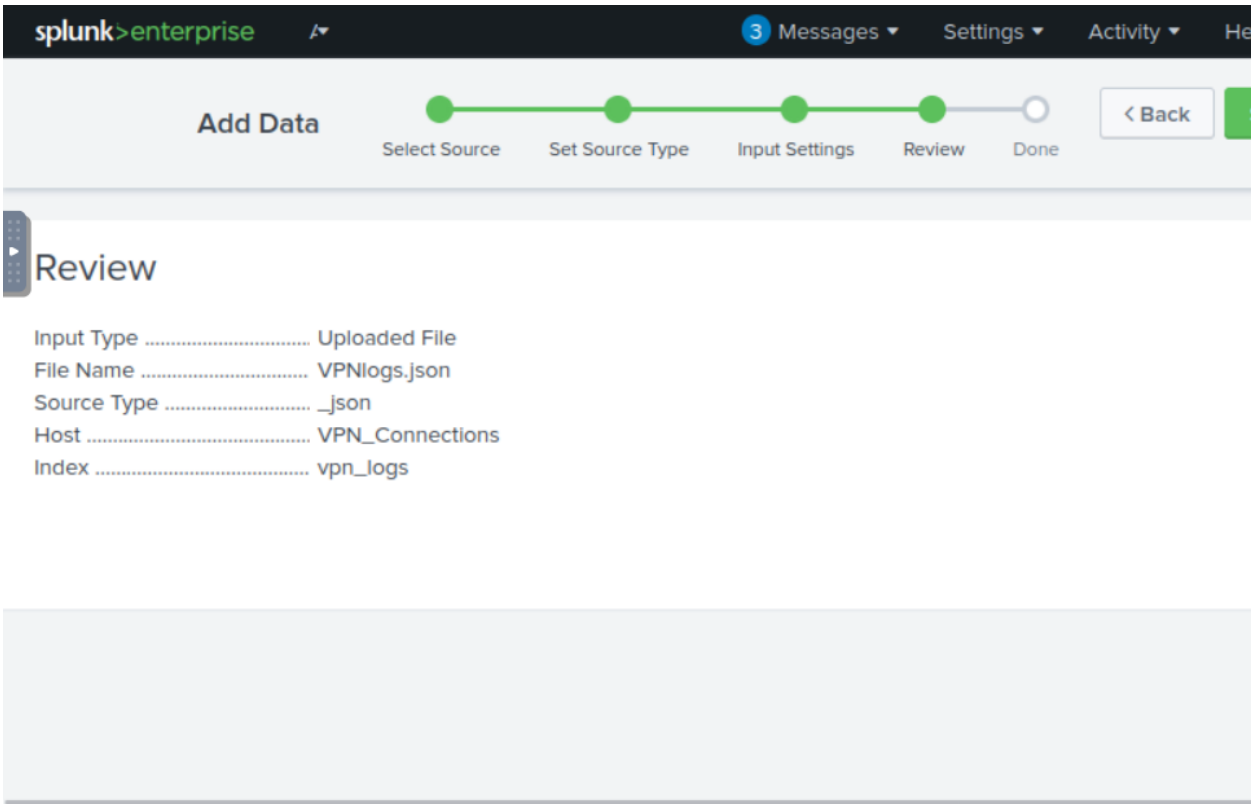
I was then faced with the ‘Select Source’ page and chose the log file as well as the data source.



Next was the ‘Set Source Type’ where I had to select the type of logs being ingested but, in this case, all I had to do was verify that it was in the intended format.

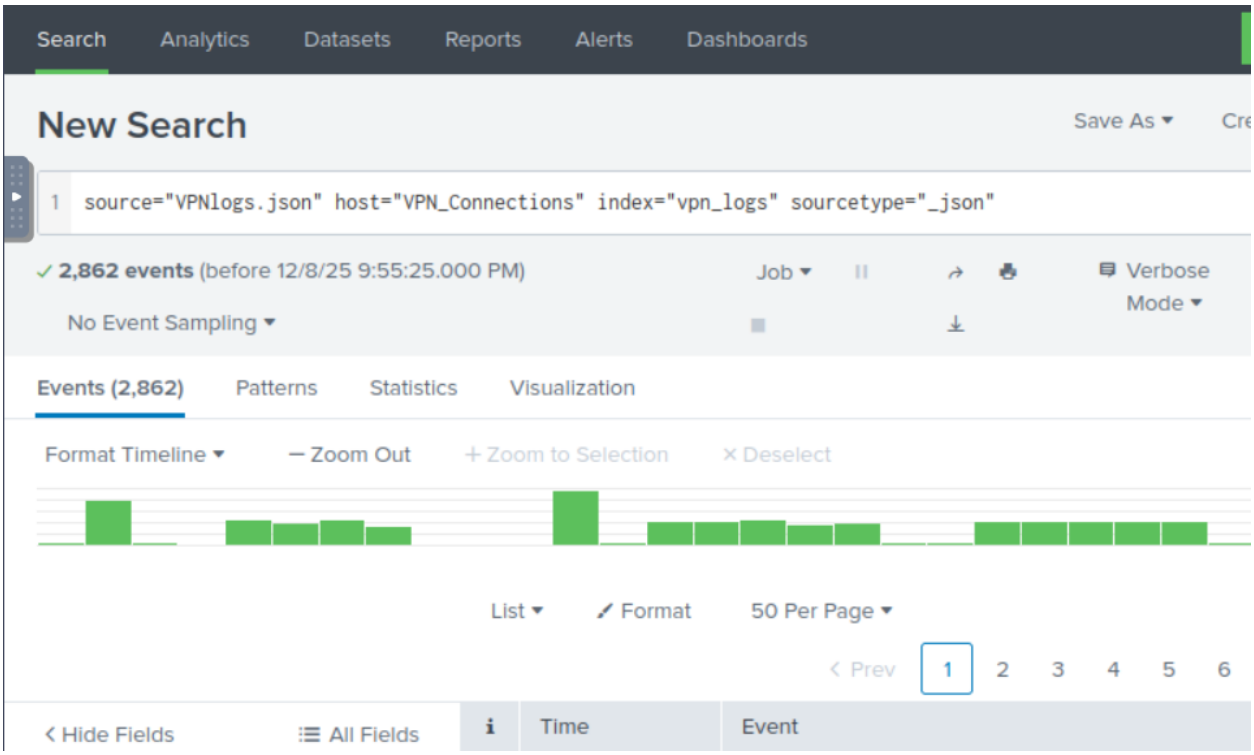


After that I landed on 'Input Settings' where I created the Index and selected it as the default index where the logs would then be dumped and associated it with the HOSTNAME of my choice.



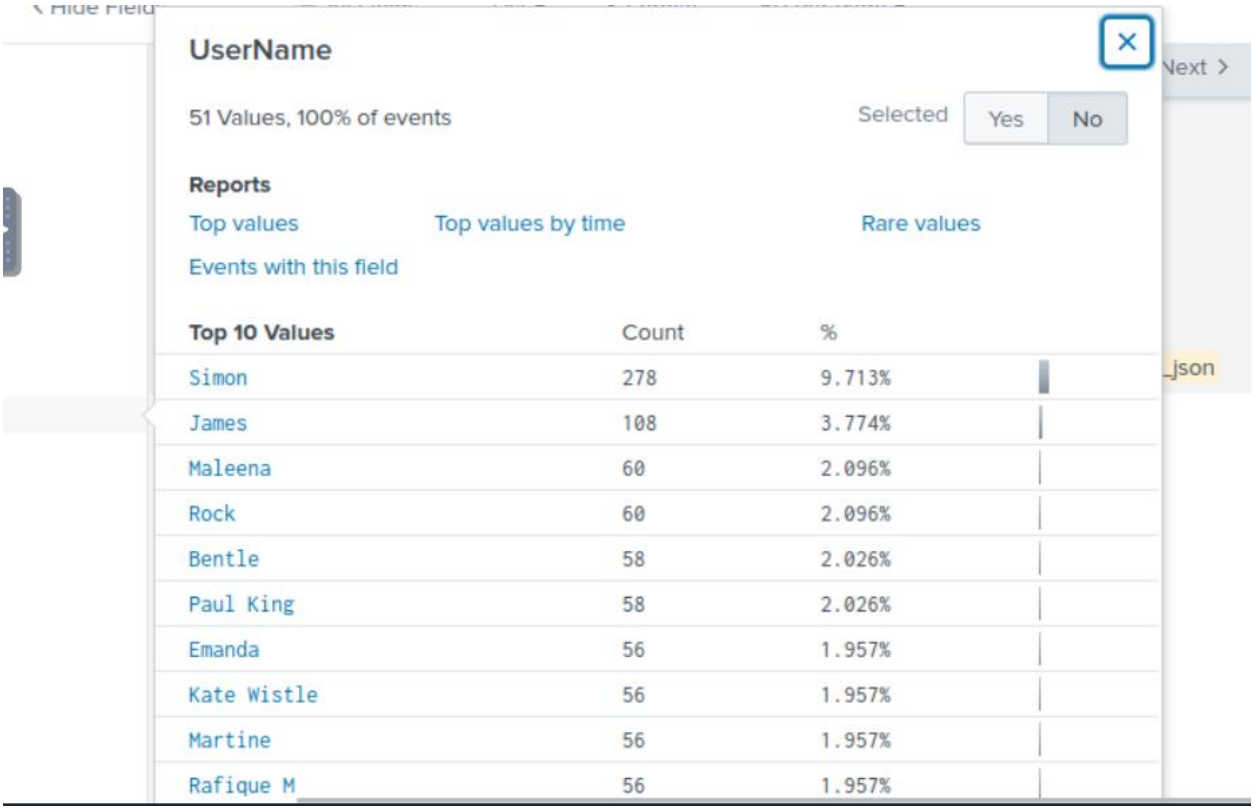
Before landing on the 'Done' page and wrapping up the ingestion phase and loading the data, I was faced with the preceding 'Review' page where I had a chance to double check the choices I had made and was happy so I proceeded onto the next step.

STEP 2: Finding how many events are present in the file.



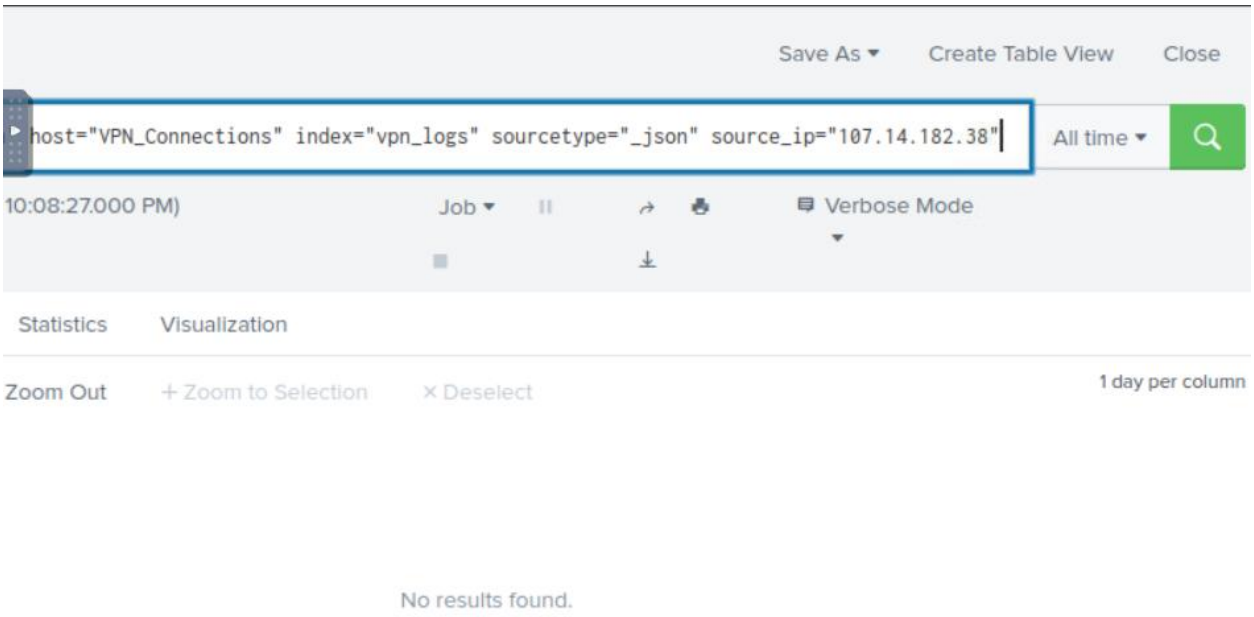
I skimmed through the page where the data loaded manifests itself and identified the number of events (2862).

STEP 2: Discovering the number of log events by the user Maleena.

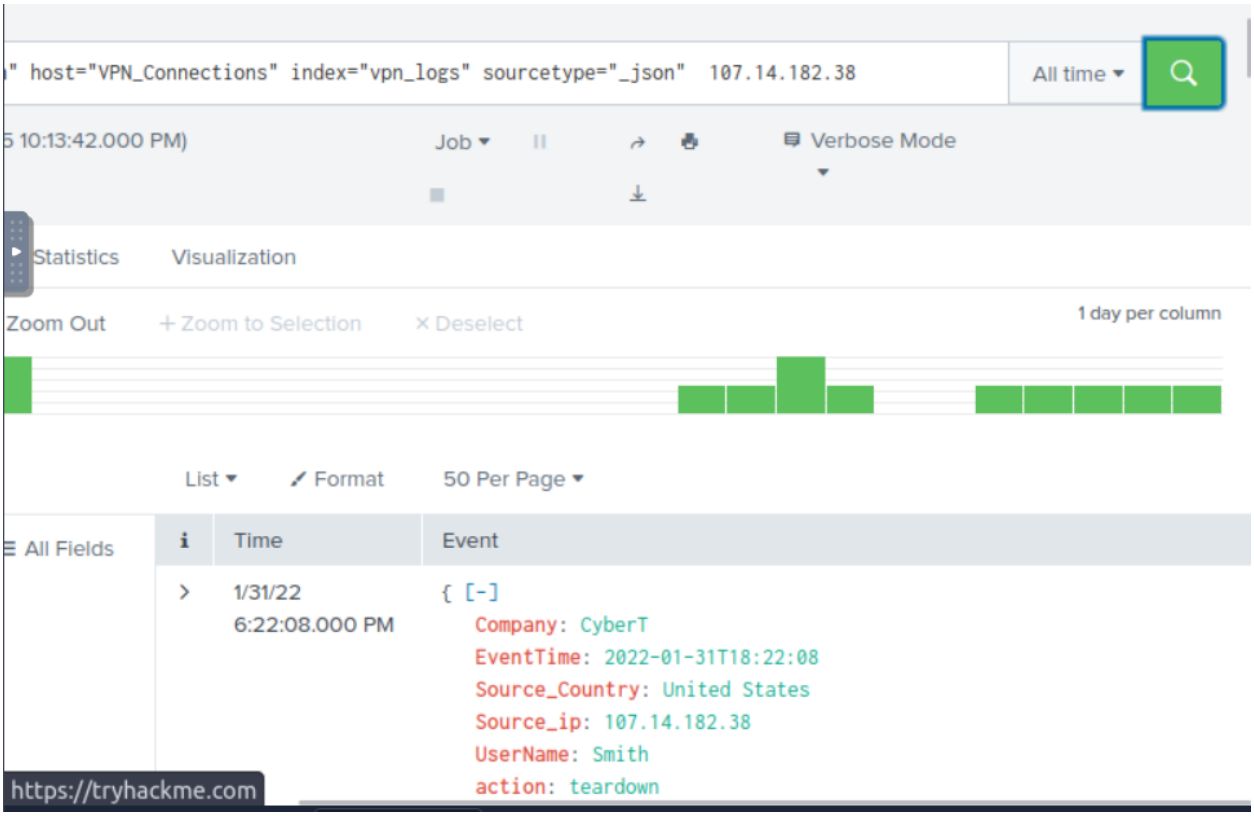


I looked to the left side of the page and scrolled down to find the target name in the 'UserName' filter and clicked on it. I looked through the section and spotted the target name as well as the Count of events associated with the name – 60.

STEP 3: Locating the name associated with username associated with IP 107.14.182.38.

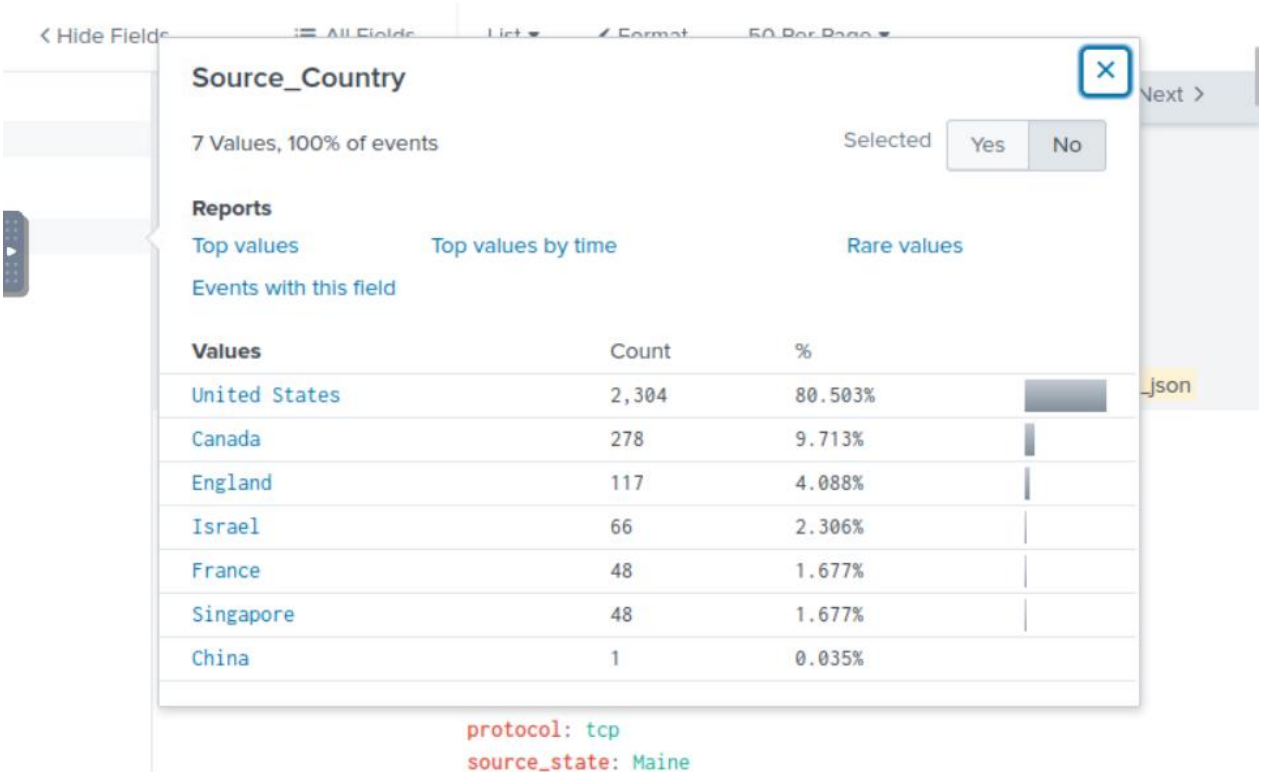


I entered the following query (source_ip=”107.14.182.38”) and nothing showed up. I took a few steps back and took a breather prior to me second attempt.



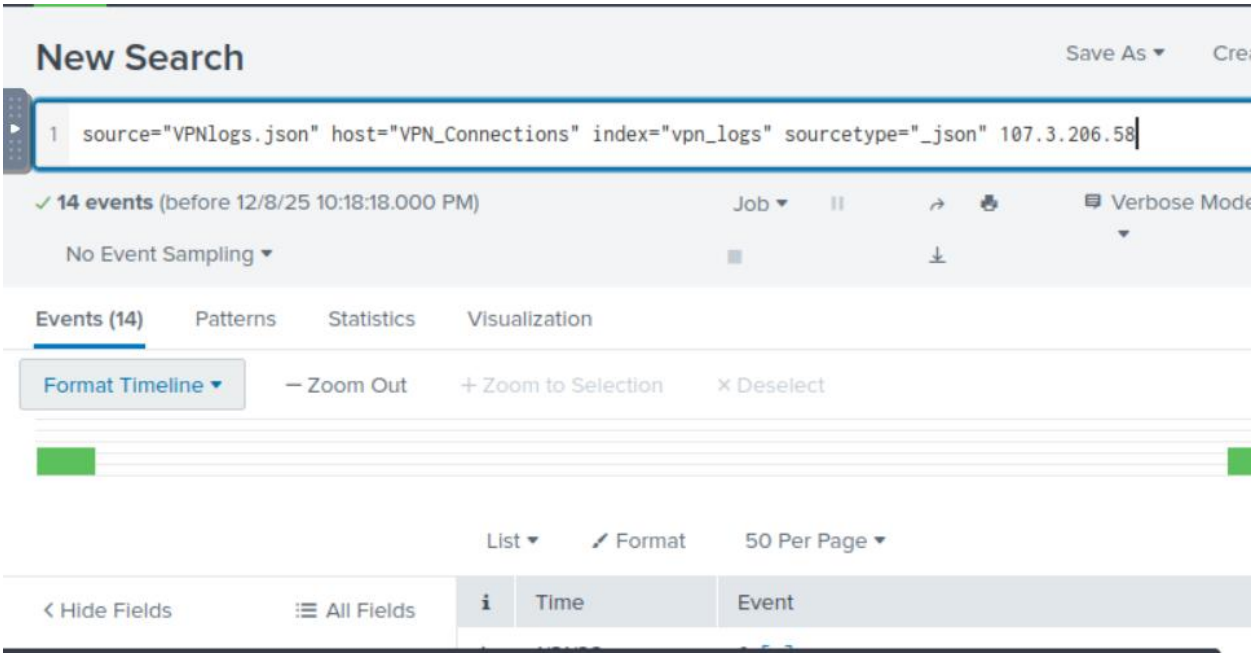
I then remover the filter and pasted only the desired IP and voila! UserName identified – Smith.

STEP 4: What is the number of events that originated from all countries except France?



There were a total of 2862 events from the countries and I looked at France and saw 48. I took the 48 and differenced it from the total and got the answer – 2814.

STEP 5: How many VPN events were associated with the IP 107.3.206.58



I pasted the IP address in the filter/search section and got the number of events associated with it - 14.

Summary Conclusion

This exercise demonstrated the complete process of ingesting and analysing log data in Splunk. I successfully uploaded data, verified the source type, configured input settings, and created a custom index for log storage. Once ingested, I carried out several analysis tasks, including identifying total events, filtering events by specific users, locating usernames linked to IP addresses, and calculating event counts based on geographic sources. Through targeted searches and filters, I identified user activity patterns, IP-associated behaviours, and event counts across different criteria. Overall, this exercise strengthened my understanding of Splunk's workflow, search capabilities, and practical log analysis techniques essential for cybersecurity monitoring.