Nested JSON Parsing Task Report

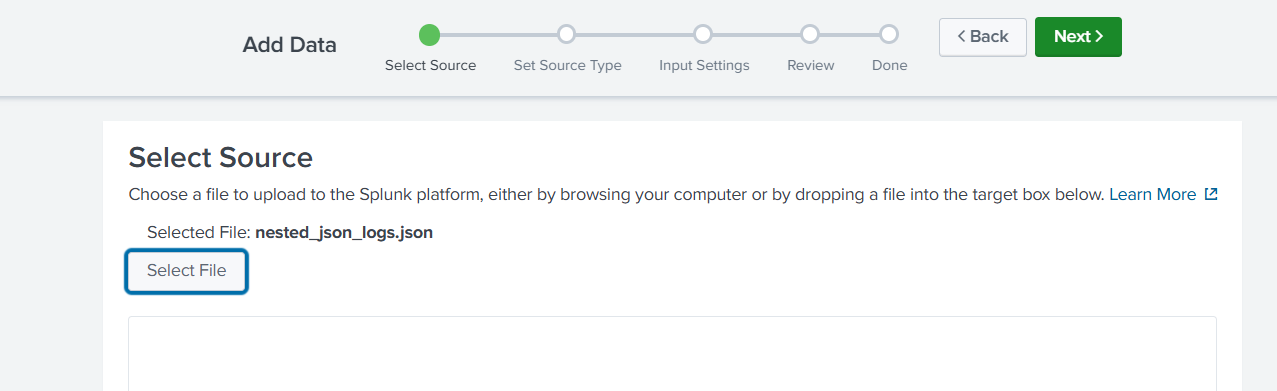
This document summarizes the completion of the Nested JSON Parsing task using Splunk's SPL commands to extract fields from deeply nested JSON logs.

# Task Description

The objective was to extract fields from deeply nested JSON log events using the `spath` command in Splunk. The nested JSON structure included user information, event details, and timestamps, which needed to be parsed and displayed in a table.

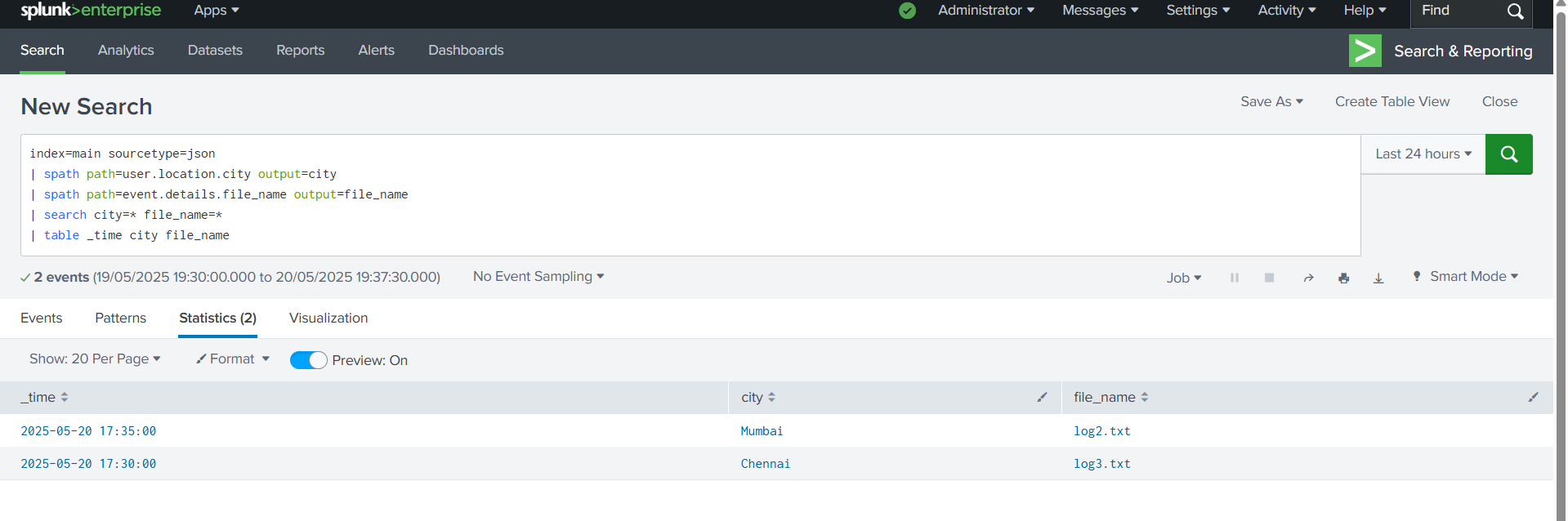
# Steps Followed

* Uploaded a properly formatted NDJSON file to Splunk.
* Ran base search with index and sourcetype filtering.
* Used multiple ‘spath’ commands to extract nested fields such as user location city and event details file name.
* Used ‘table’command to display extracted fields in a readable tabular format.



# Final SPL Query Used

index=main sourcetype=json  
| spath path=user.location.city output=city  
| spath path=event.details.file\_name output=file\_name  
| table \_time city file\_name

Sample Output

\_time city file\_name  
2025-05-20 17:35:00 Mumbai log2.txt  
2025-05-20 17:30:00 Chennai log3.txt