**Lab Exercise 12- Command Breakdown**

**Step 1: Prepare the .log File**

**Command Breakdown**

**1. rex**

* **Purpose**: Extract fields from raw log data using regular expressions (regex).
* **Syntax**:

rex "(?<FieldName>regex\_pattern)"

* **Example**:

| rex "(?<Product>\w+)\s(?<Category>\w+)\s(?<Quantity>\d+)\s(?<Price>\d+)"

* + Extracts fields:
    - Product: First word in the line.
    - Category: Second word in the line.
    - Quantity: First number in the line.
    - Price: Last number in the line.
* **Explanation**: The regex pattern (?<FieldName>regex\_pattern) captures specific parts of the data and assigns them to named fields like Product, Category, etc.

**2. eval**

* **Purpose**: Create or modify fields based on expressions or calculations.
* **Syntax**:

eval NewField=expression

* **Example 1**: Calculate total price:

| eval total\_price=Quantity\*Price

* + Multiplies the values in Quantity and Price to create a new field, total\_price.
* **Example 2**: Categorize products by price:

| eval price\_range=case(Price<100, "Low", Price<500, "Medium", Price>=500, "High")

* + Uses case to assign a price\_range based on the value of Price.

**3. table**

* **Purpose**: Display selected fields in a tabular format.
* **Syntax**:

table Field1, Field2, Field3

* **Example**:

| table Product, Quantity, Price, total\_price

* + Displays only the specified fields (Product, Quantity, Price, total\_price) in the search results.

**4. stats**

* **Purpose**: Perform statistical calculations (e.g., count, sum, average) on data.
* **Syntax**:

stats function(field) by Field

* **Example**: Count products in each category:

| stats count by Category

* + Groups the data by Category and counts the number of products in each.

**Query Breakdown**

**Task 1: Extract Fields**

* **Query**:

index=price\_data\_index sourcetype=price\_log

| rex "(?<Product>\w+)\s(?<Category>\w+)\s(?<Quantity>\d+)\s(?<Price>\d+)"

| table Product, Category, Quantity, Price

* **Explanation**:
  1. Search data in the specified index and sourcetype.
  2. Use rex to extract Product, Category, Quantity, and Price from the raw log.
  3. Use table to display these fields in a clean format.

**Task 2: Calculate Total Price**

* **Query**:

index=price\_data\_index sourcetype=price\_log

| rex "(?<Product>\w+)\s(?<Category>\w+)\s(?<Quantity>\d+)\s(?<Price>\d+)"

| eval total\_price=Quantity\*Price

| table Product, Quantity, Price, total\_price

* **Explanation**:
  1. Extract fields (Product, Category, Quantity, Price).
  2. Use eval to calculate total\_price as the product of Quantity and Price.
  3. Display the extracted and calculated fields in a table.

**Task 3: Categorize Products by Price**

* **Query**:

index=price\_data\_index sourcetype=price\_log

| rex "(?<Product>\w+)\s(?<Category>\w+)\s(?<Quantity>\d+)\s(?<Price>\d+)"

| eval price\_range=case(Price<100, "Low", Price<500, "Medium", Price>=500, "High")

| table Product, Price, price\_range

* **Explanation**:
  1. Extract Product, Category, Quantity, and Price.
  2. Use eval and case to assign price\_range values based on Price.
  3. Display Product, Price, and price\_range in a table.

**Task 4: Identify Top Categories**

* **Query**:

index=price\_data\_index sourcetype=price\_log

| rex "(?<Product>\w+)\s(?<Category>\w+)\s(?<Quantity>\d+)\s(?<Price>\d+)"

| stats count by Category

* **Explanation**:
  1. Extract Category and other fields.
  2. Use stats count by Category to count the number of products in each category.

**Deliverables and Insights**

1. **Queries**: The provided queries extract, transform, and analyze data effectively.
2. **Results**:
   * A breakdown of product details (Product, Category, Quantity, Price).
   * Total price for each product.
   * Price categorization (Low, Medium, High).
   * Count of products per category.