**Lab Exercise 11- Using Transformation Commands on Price log Data**

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

Save the following sample data as price\_data.log:

Laptop Electronics 10 1000

Smartphone Electronics 20 800

Shoes Fashion 50 60

Watch Fashion 30 150

Table Home 5 200

Chair Home 15 75

**Step 2: Configure Splunk to Parse .log Data**

**Option 1: Configure Sourcetype in Splunk Web**

1. Navigate to **Settings > Sourcetypes**.
2. Click **New Sourcetype** and provide the following details:
   * **Name**: price\_log.
   * **Category**: Custom.
3. Save the sourcetype.

**Option 2: Edit props.conf for Manual Configuration**

If you prefer editing the configuration files manually, add the following to your ***props.conf*** file:

[price\_log]

SHOULD\_LINEMERGE = false

LINE\_BREAKER = ([\r\n]+)

NO\_BINARY\_CHECK = true

TIME\_FORMAT = %Y-%m-%d %H:%M:%S

MAX\_TIMESTAMP\_LOOKAHEAD = 0

Restart Splunk for the changes to take effect:

splunk restart

**Step 3: Ingest the .log File**

1. Navigate to **Settings > Add Data > Upload**.
2. Select the price\_data.log file.
3. Assign the file to the newly created price\_log sourcetype and an index (e.g., price\_data\_index).
4. Complete the ingestion process.

**Step 4: Validate the Data**

Search the index to confirm each line is treated as a separate event:

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

**Step 5: Use Transformation Commands**

After confirming the data is correctly ingested, use the following transformation queries to analyze the .log data.

**Task 1: Extract Fields Using rex**

Extract fields such as Product, Category, Quantity, and Price using regular expressions.

* **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

* **Goal**: Display all extracted fields in a table.

**Task 2: Calculate Total Price**

Calculate the total price by multiplying Quantity and 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

* **Goal**: Add a new field total\_price and display it alongside the other fields.

**Task 3: Categorize Products by Price**

Add a Price Range field:

* Price < 100: Low
* 100 ≤ Price < 500: Medium
* Price ≥ 500: High
* **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

* **Goal**: Display each product with its Price and Price Range.

**Task 4: Identify Top Categories**

Count the number of products in each category.

* **Query**:

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

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

| stats count by Category

* **Goal**: Display the count of products grouped by category.

**Deliverables**

1. **Queries**: Submit all SPL queries used for the tasks.
2. **Screenshots**: Include screenshots of the query results.
3. **Insights**: Summarize findings such as:
   * Total price of products.
   * Distribution of products across price ranges.
   * Most common product categories.

**Expected Outcomes**

* Splunk will treat each line in the .log file as a separate event.
* You will successfully extract and manipulate fields using transformation commands.
* Insights will be generated from the price data.