Elasticsearch Lab 1

Objectif : In this lab, you will index some sample data that ships with Kibana and view some of the other features of using Kibana.

1. Sign-in to your kibana instance using your **elastic** user.

2. From the **Home** page of Kibana, scroll to **Get started by adding integrations.**

3. Notice Kibana has a lot of built-in tutorials in ingesting data from many different sources. In this lab you are going to index some sample data that ship with Kibana, so click on the **Sample data** tab.

4. Click on **Other sample data sets** and add the **Sample eCommerce orders** dataset by clicking the **Add data** button.

5. To view your newly-indexed data, view the **Discover** app in Kibana (by clicking on the menu in the top-left corner and selecting **Discover** under the **Analytics** heading).

6. **Discover** shows you the volume of documents being indexed, along with a table displaying recently added documents. Notice you are viewing the **Last 15 minutes** of data, as shown in the Kibana **time filter**. Click on the calendar icon in the time filter and select **Last 24 hours**.

7. You should see a regular stream of eCommerce orders from the last 24 hours.

8. From the Kibana menu, click on **Dashboard**. You will see a list of all dashboards - which should only be one dashboard created when you imported the sample dataset. Click on the name of the dashboard (**[eCommerce] Revenue Dashboard**) to view it.

9. A dashboard consists of one or more *visualizations*. Notice you can drag-and-drop and resize the visualizations to your liking, as well as add and remove them from a dashboard.

10. From the Kibana menu, click on **Dev Tools**, which contains a collection of developer tools. The default tool displayed is the **Console**, which allows you to send HTTP requests to the cluster and view the results in a quick and convenient manner. There is a match_all query written for you already but go ahead and delete it.

    1. Enter the following command into the **Console**, then click the **play** icon to send the request:

```
Unset
GET /
```

    2. Notice that a simple GET request to a cluster returns basic details about the cluster, along with Shay Banon's famous **"You Know, for Search"** tagline! **Tip:** You can also send a request in the **Console** by pressing **Ctrl+enter** (or **Cmd+enter** on a Mac).
    3. Use the **Console** to send the following request, which displays the current indexes in the cluster:

```
Unset
GET _cat/indices
```

    4. Let's start with a simple "match all" search that simply returns 10 documents in an index. Submit the following request in **Console**:

```
Unset
GET kibana_sample_data_ecommerce/_search
```

    5. Page down through the results and you will see that the search returned the _source of 10 documents.

    6. Now let’s run some search queries to discover our data.

7. Running the below query, you will search for products under the Men's Clothing category.

```
Unset
GET kibana_sample_data_ecommerce/_search{
   "query": {
   "match": {
         "category": "Men's Clothing"
      }
   }
}
```

8. The result will show you **4213** doc matched, however, not all of them have only Men's Clothing as category you will find some of them having Men's Accessories also, The match query uses **or** logic by default, so a query for Men's Clothing returns blogs with either "Men's" or "Clothing"in the category.

9. To improve the previous query result let's run this one.

```
Unset
GET kibana_sample_data_ecommerce/_search
{
   "query": {
      "match_phrase": {
         "category": "Men's Clothing"
      }
   }
}
```

10. Now the results you will get is **2024**.

That's all for your first lab, you can look for elastic documentations and play more with the queries.