Kibana Workshop

Lab 1 - Discover

Discover

In this section you will learn how to use Discover to explore and understand your data.

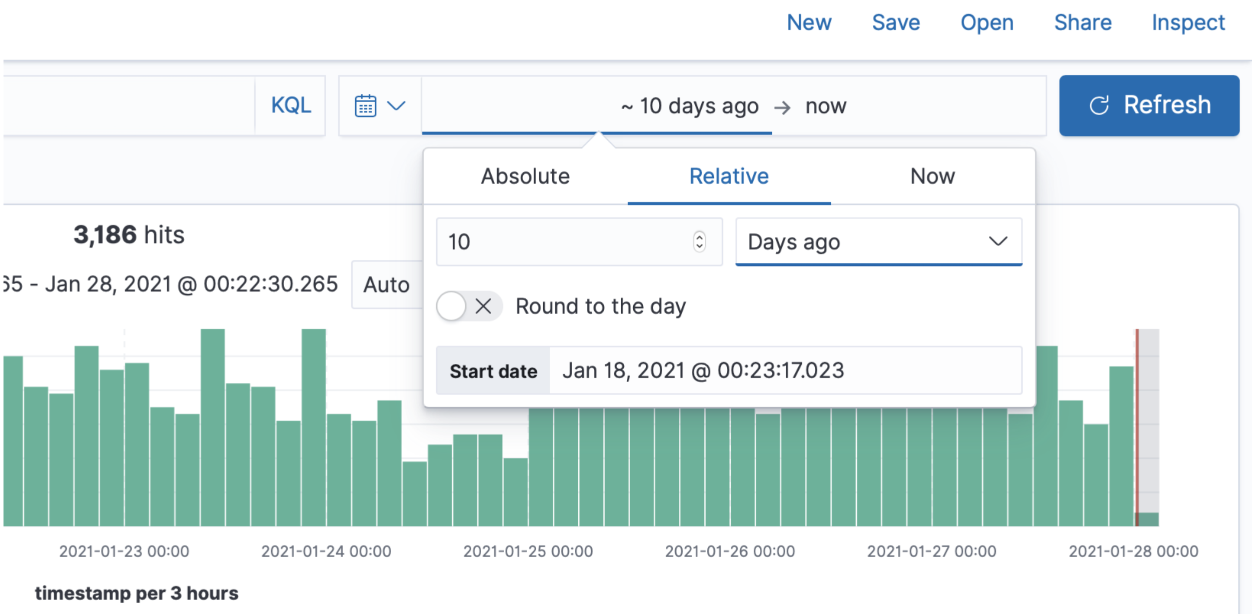
Searching your data

"You know, for search!" Let's learn how to use the search capabilities of Elasticsearch in Kibana. There are several ways to query your data in Kibana, including:

- adding filters under the query bar (as you did in the "Using a dashboard" lab)
- writing a query in the query bar using the Kibana Query Language, KQL. We will cover these here.

Filters

1. Click on the menu button located at the top left to access up the main menu. Select the "**Discover**" option under "Analytics".
2. Make sure the `kibana_sample_data_flights` index is selected in the top left.
3. In the time range filter at the top right, select "Relative" and set `10 days ago` in the From field, to `Now`, and click "Update".



~ 10 days ago → now

3,186 hits

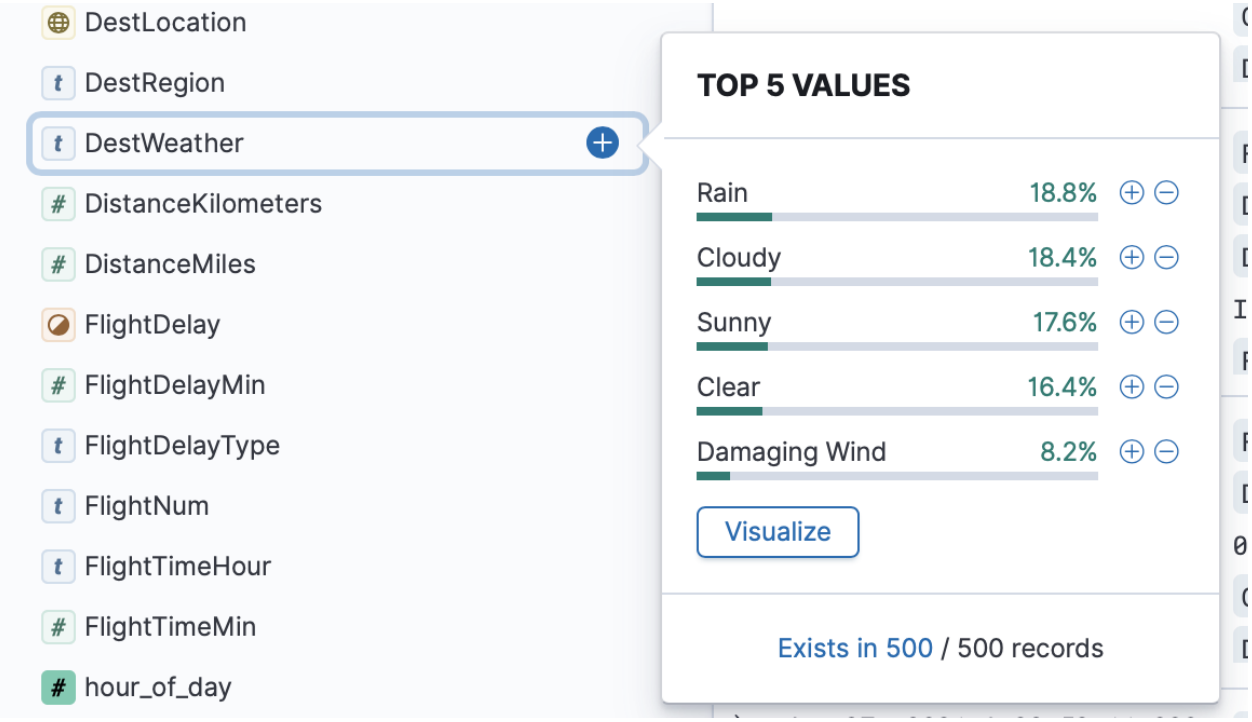
55 - Jan 28, 2021 @ 00:22:30.265

10 Days ago

Round to the day

Start date Jan 18, 2021 @ 00:23:17.023

4. Click on "`DestWeather`" in the list of fields on the left to view the most common values for that field:



TOP 5 VALUES

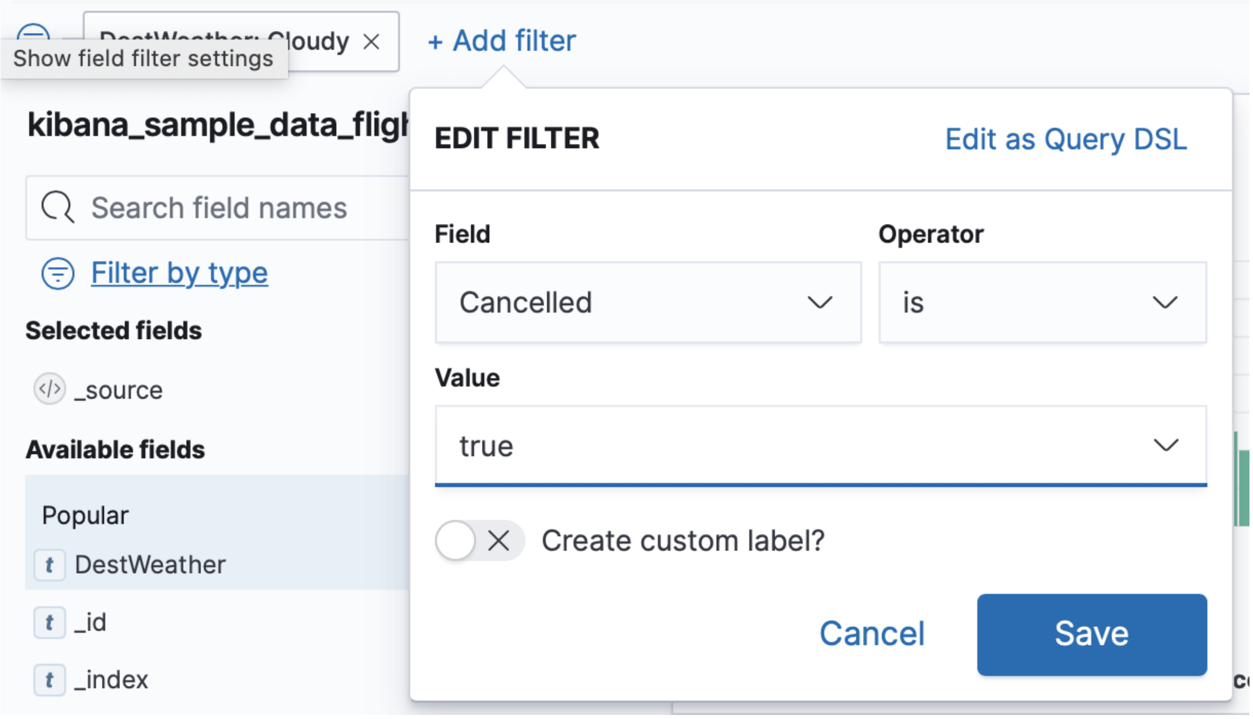
Rain	18.8%
Cloudy	18.4%
Sunny	17.6%
Clear	16.4%
Damaging Wind	8.2%

Exists in 500 / 500 records

5. On the list of values, click on the + symbol after the "Cloudy" value. This creates a filter on this value. The results table now only shows flights where

the destination weather was cloudy. Note that the filter is added at the top under the search bar.

6. Click the "`+ Add filter`" link in the top left. Select the `Cancelled` field, `is` for the operator, and then select `true` for the value. You can create the filter by clicking "`Save`":

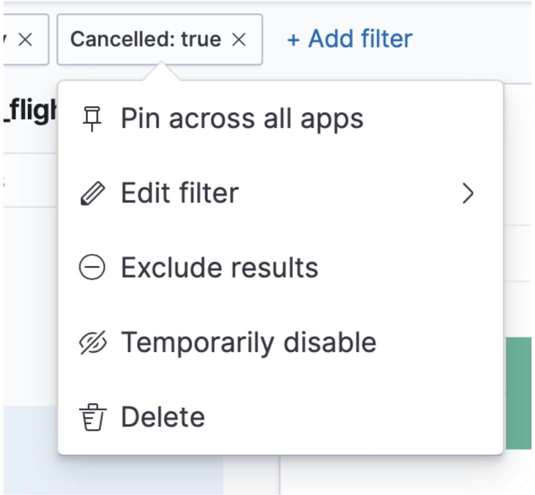


Field: Cancelled

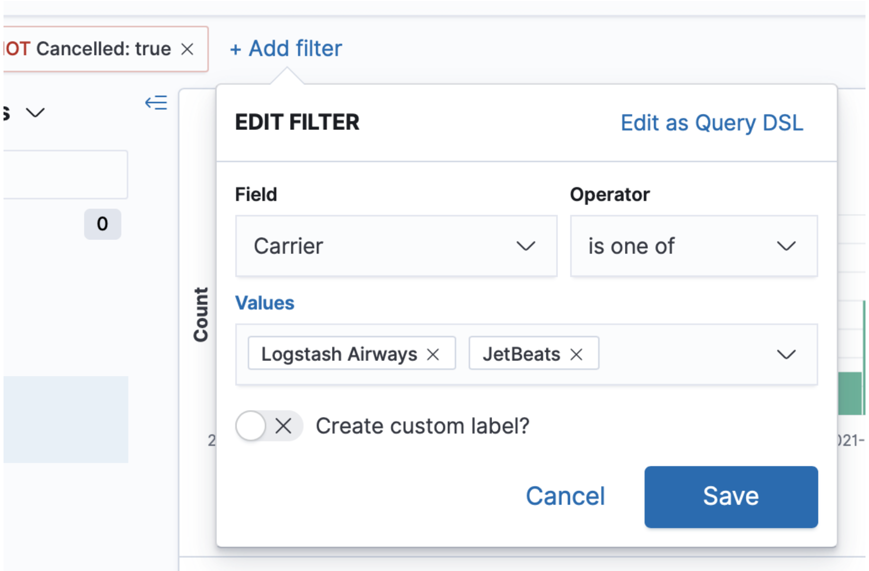
Operator: is

Value: true

7. When you click on the filter you just created, a few actions appear. Click the "`Exclude results`" option to negate the filter. Now, only flights that were not cancelled are displayed.



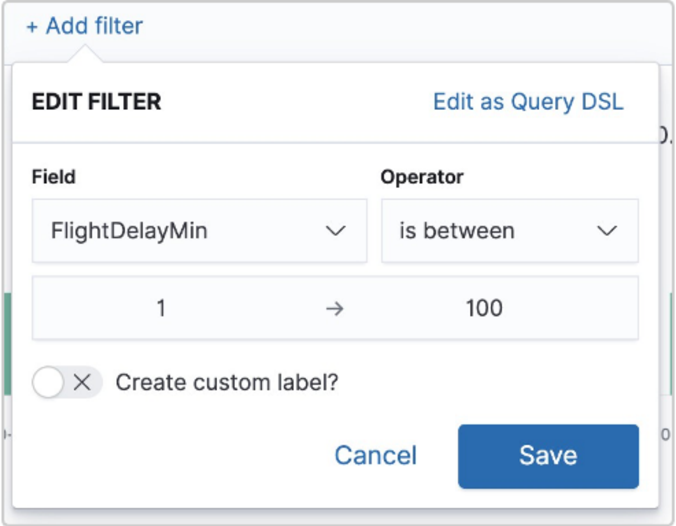
8. Add a new filter on Carrier – is one of – `Logstash Airways` or `JetBeats`. Click "Save".



EDIT FILTER
Edit as Query DSL

Field: Carrier
Operator: is one of
Values: Logstash Airways × JetBeats ×

9. Finally, add a filter on the `FlightDelayMin` (minutes of delay) between `1` and `100`:



EDIT FILTER
Edit as Query DSL

Field: FlightDelayMin
Operator: is between
1 → 100

Kibana Query Language (KQL)

You will now use the query bar to get to the same results as the filters you have just created.

1. Click "**New**" in the top menu.
2. Enter the following query in the query bar and hit "Enter":

   ```
   DestWeather:Cloudy
   ```

   The number of hits (just above the date histogram) changes. Notice the auto complete feature for both fields and values as you type the query.
3. Add the condition on flight not being cancelled to the query:

   ```
   and not Cancelled:true
   ```

   Of course we could have set `and Cancelled:false` but we wanted to explicitly use the `not` to negate the filter.
4. Add the condition on carrier by adding the following to the query:

   ```
   and Carrier:("Logstash Airways" or "JetBeats")
   ```

5. Add the following to restrict the search on flight delay:

   ```
   and FlightDelayMin>0 and FlightDelayMin<=100
   ```

6. The full query should now be:

```
DestWeather:Cloudy and not Cancelled:true and
Carrier:("Logstash Airways" or "JetBeats") and
FlightDelayMin>0 and FlightDelayMin<=100
```

KQL is a powerful query language. You can also use it for full text search. For example if you look for destination city starting with B you can add and `DestCityName:B*`. This will match Bari, Bergamo, Buenos Aires, etc. You can even do a free search on any field. For example, `and Thunder*` that searches for "Thunder*" in any field. It will match both origin or destination weather.

To learn more about the KQL syntax, visit
https://www.elastic.co/guide/en/kibana/current/kuery-query.html

Saved search

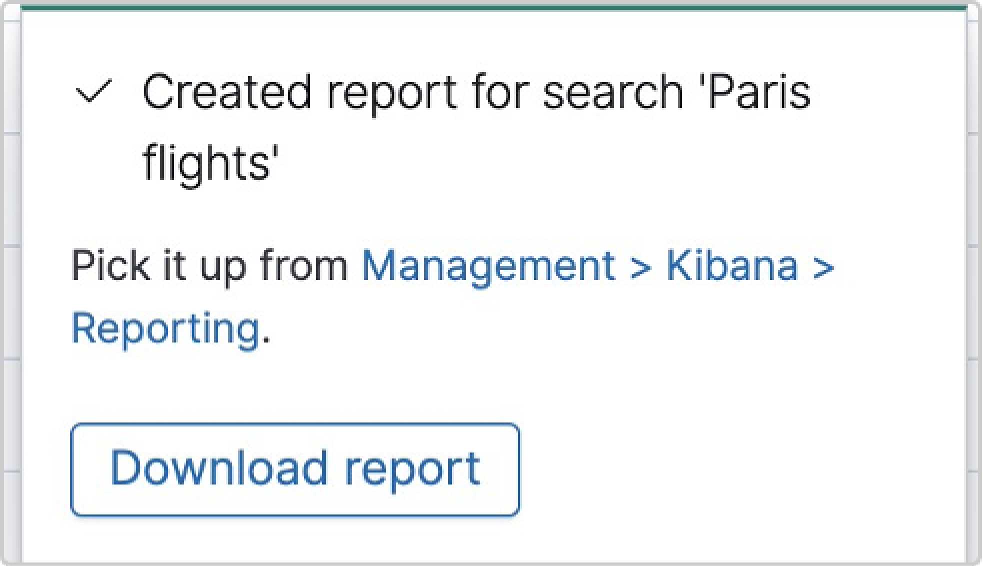
In this exercise you will customize the table view, and save it as a saved search.

1. Click "New" in the top menu.
2. Now, expand one of the documents with the arrow on the left of a line.
3. As you hover with your mouse over the different fields on the left hand side, a blue + appears. Click on the + for "OriginCityName", "DestCityName", "Carrier" and "FlightDelayMin". This creates a custom table view that only includes these fields.
4. Use query or filter to only show flights that have been delayed. (Hint: the field that indicates whether a flight was delayed or not is called "FlightDelay".)
5. Click Save and enter a name "Delayed flights saved search"
6. Click "New" to reset the table view to its original layout.
7. To return to your saved search, click "Open" and select "Delayed flights saved search".

Exporting to CSV

In this exercise you will create a search and then export the results as a CSV report.

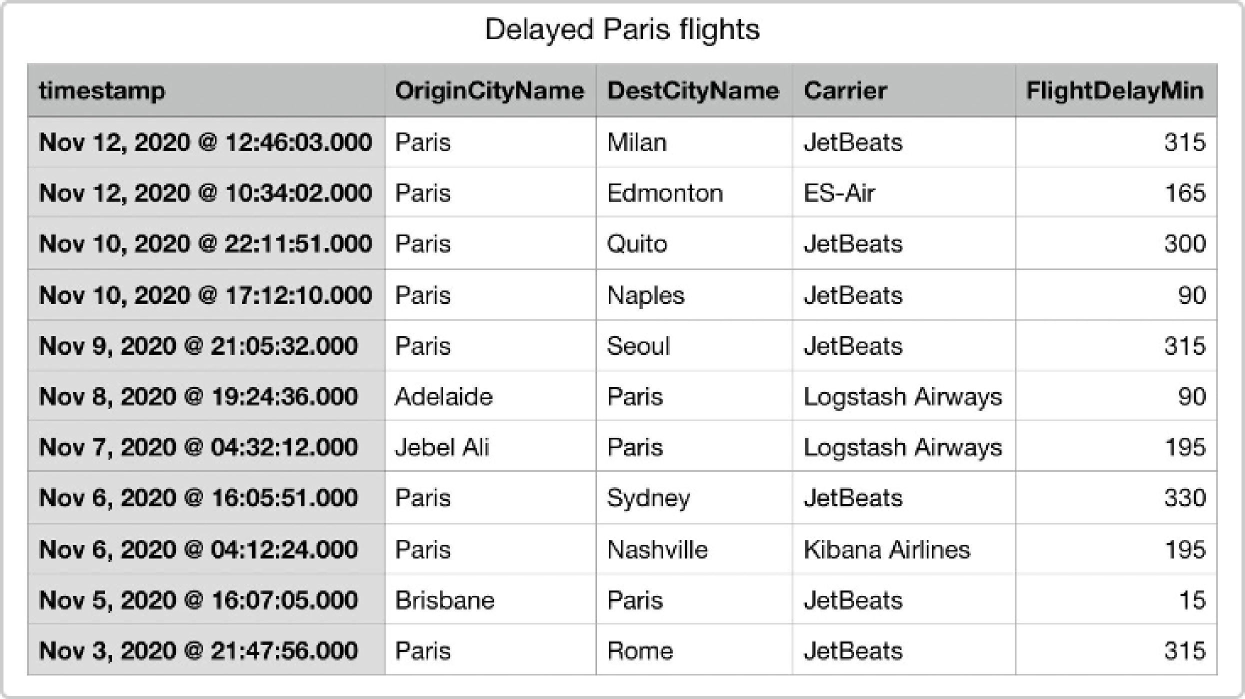
1. Click "Open" and select "Delayed flights saved search" to return to your saved search, if it is not already open.
2. Enter `Paris` in the search bar and press Enter.
3. Save again as a new saved search called "Delayed Paris flights".
4. Click "Share" in the top bar, then select "CSV Reports" and click the "Generate CSV" button.
5. The CSV is being generated in the background. Once ready, a popup will appear in the bottom right corner of the screen:



✓ Created report for search 'Paris flights'

Pick it up from Management > Kibana > Reporting.

6. You can retrieve generated CSVs or see progress. Click "Stack Management" from the main menu (under "Management"). Next, select "Reporting" from the "Alerts and insights" section.
7. Wait until the CSV has been generated (if not ready) and click the download icon.



Delayed Paris flights

timestamp	OriginCityName	DestCityName	Carrier	FlightDelayMin
Nov 12, 2020 @ 12:46:03.000	Paris	Milan	JetBeats	315
Nov 12, 2020 @ 10:34:02.000	Paris	Edmonton	ES-Air	165
Nov 10, 2020 @ 22:11:51.000	Paris	Quito	JetBeats	300
Nov 10, 2020 @ 17:12:10.000	Paris	Naples	JetBeats	90
Nov 9, 2020 @ 21:05:32.000	Paris	Seoul	JetBeats	315
Nov 8, 2020 @ 19:24:36.000	Adelaide	Paris	Logstash Airways	90
Nov 7, 2020 @ 04:32:12.000	Jebel Ali	Paris	Logstash Airways	195
Nov 6, 2020 @ 16:05:51.000	Paris	Sydney	JetBeats	330
Nov 6, 2020 @ 04:12:24.000	Paris	Nashville	Kibana Airlines	195
Nov 5, 2020 @ 16:07:05.000	Brisbane	Paris	JetBeats	15
Nov 3, 2020 @ 21:47:56.000	Paris	Rome	JetBeats	315