Module

Kibana Fundamentals

elastic

Topics

- Introduction to Kibana
- Discover Interface
- Visualizing Data

Kibana Fundamentals

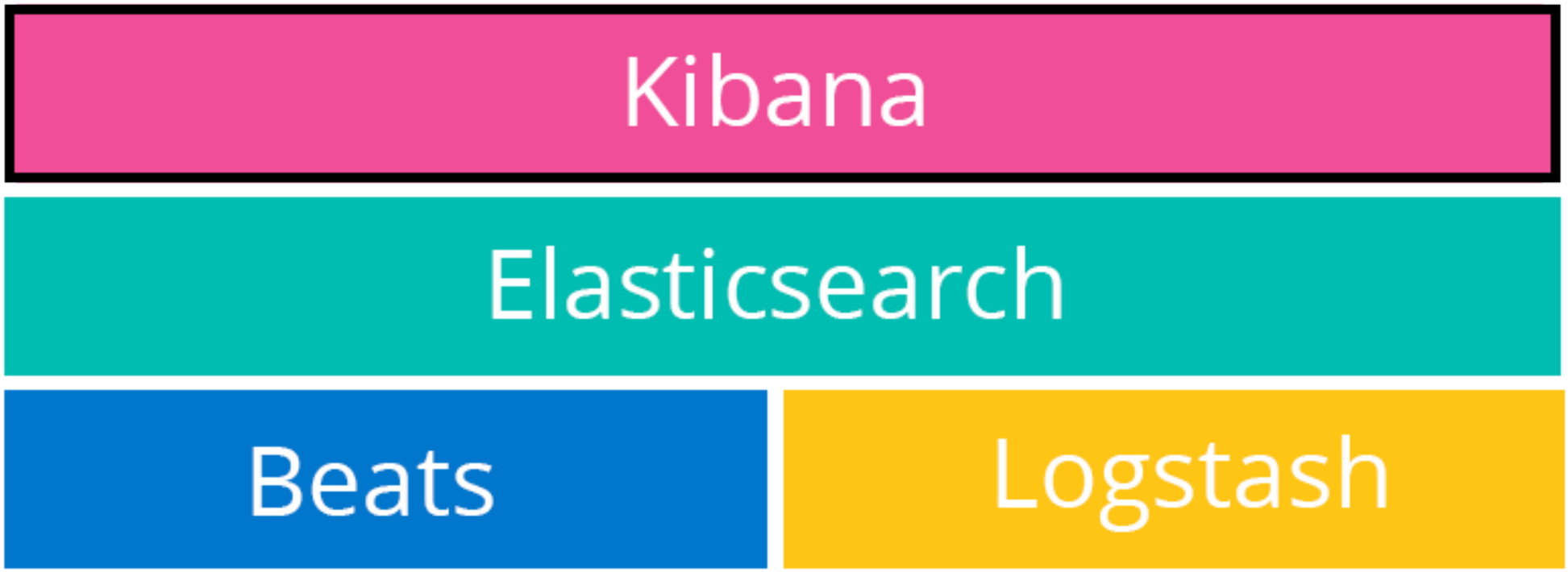
Lesson 1

Introduction to Kibana

elastic

Introduction to Elastic

The Elastic Stack



Ingest: Logstash and Beats

- **Logstash**
  - Server-side data processing
  - Ingests data from multiple sources simultaneously (MongoDB, PostgreSQL, Elasticsearch, ...)
  - Parse, transform and prepare your data for ingestion
- **Beats**
  - Single purpose data shippers
  - Many flavors: Filebeat, Metricbeat, Packetbeat, Winlogbeat, ...
  - Lightweight agents that send data from a machine to Elasticsearch or Logstash

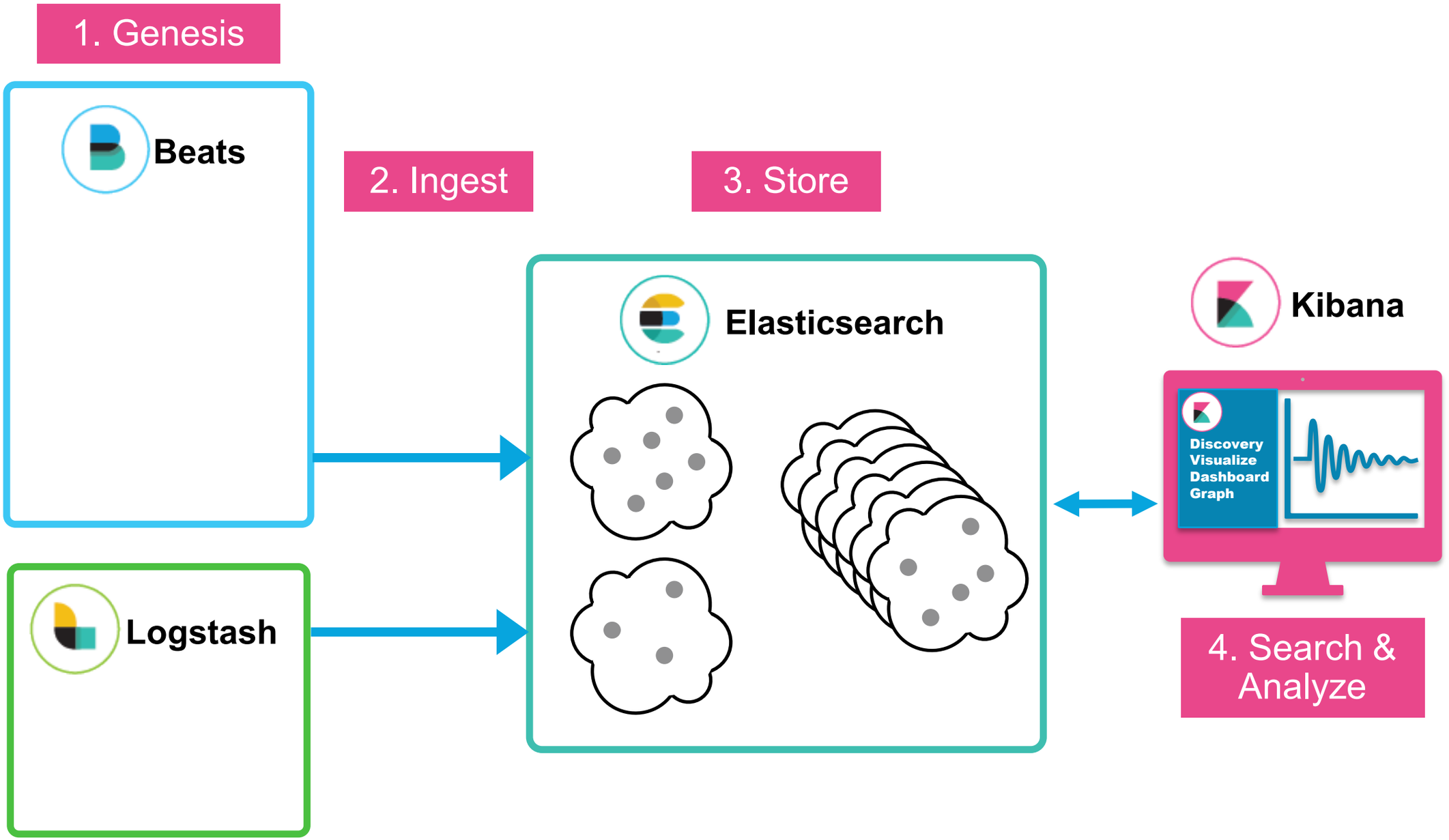
Index: Query and Aggregations

- Elasticsearch
  - Heart of the Elastic Stack
  - **distributed**: easy to scale
  - **RESTful**: easy to communicate with using APIs
  - search, analyze and store data

Visualize

- **Kibana**
  - Window into Elastic Stack
  - Provides Web-based UI to
    - Manage the stack
    - Interact with the data
    - Get data in
    - And more…

Data Journey



Document

- Document
  - Serialized JSON Object
  - Stored in Elasticsearch
  - Has Unique ID

title	category	author_first_name	author_last_name	author_company
Fighting Ebola with Elastic	User Stories	Emily	Mosher	

A row in a table

```
{
  "title": "Fighting Ebola with
Elastic",
  "category": "User Stories",
  "author": {
    "first_name": "Emily",
    "last_name": "Mosher"
  }
}
```

JSON

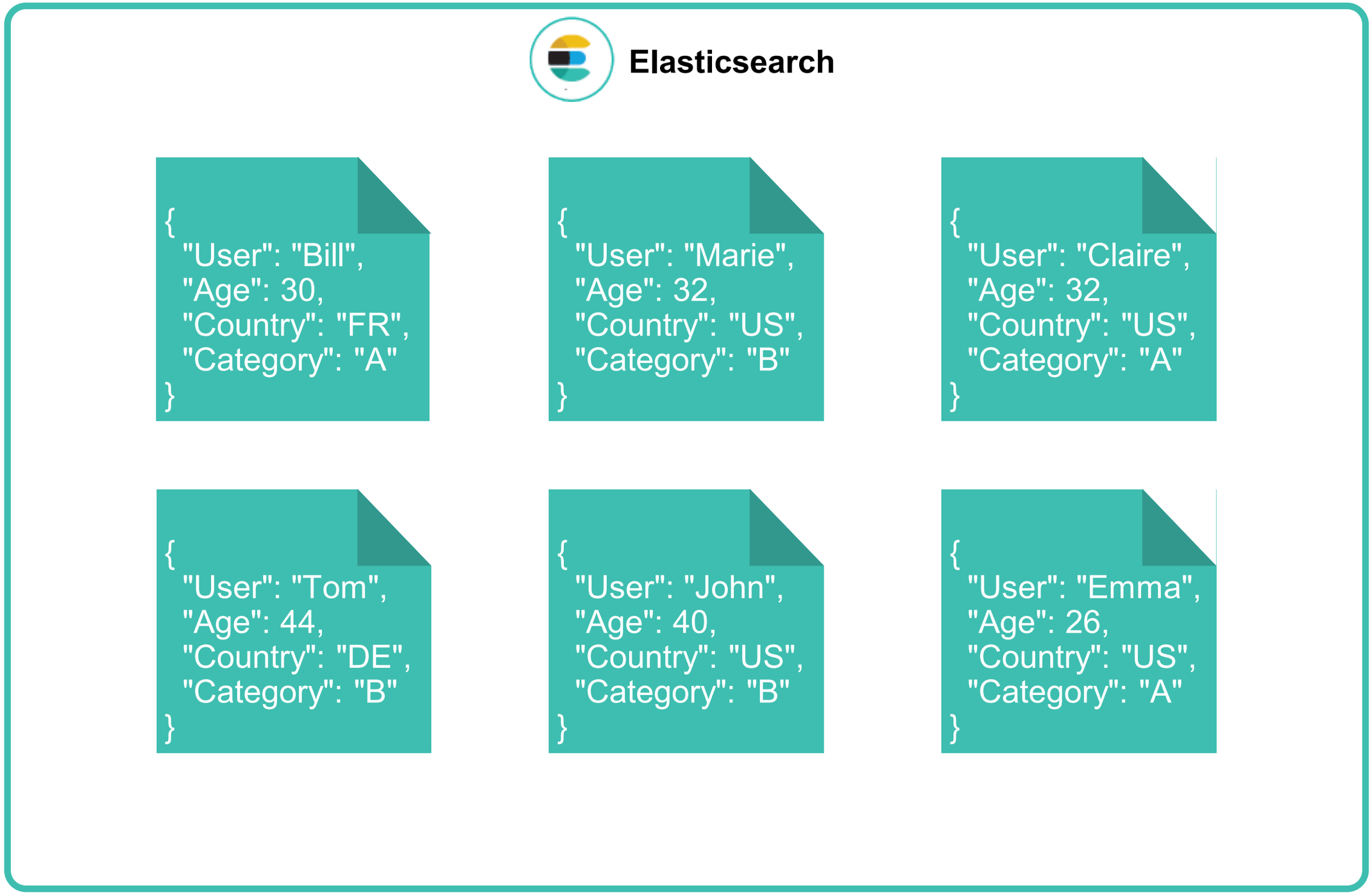
```
<?xml version="1.0" encoding="UTF-8"?>
<root>
   <author>
      <first_name>Emily</first_name>
      <last_name>Mosher</last_name>
   </author>
   <category>User Stories</category>
   <title>Fighting Ebola with Elastic</title>
</root>
```

XML

A Simple Example: Spreadsheet

id	user	age	country	category
1	Bill	30	FR	A
2	Marie	32	US	A
3	Claire	32	US	A
4	Tom	44	DE	B
5	John	40	US	B
6	Emma	26	US	B

A Simple Example: Elasticsearch



Data Categories

- **Time Series Data**
  - Event data associated with a moment in time
  - typically grows rapidly
- **Static Data**:
  - relatively slower growth

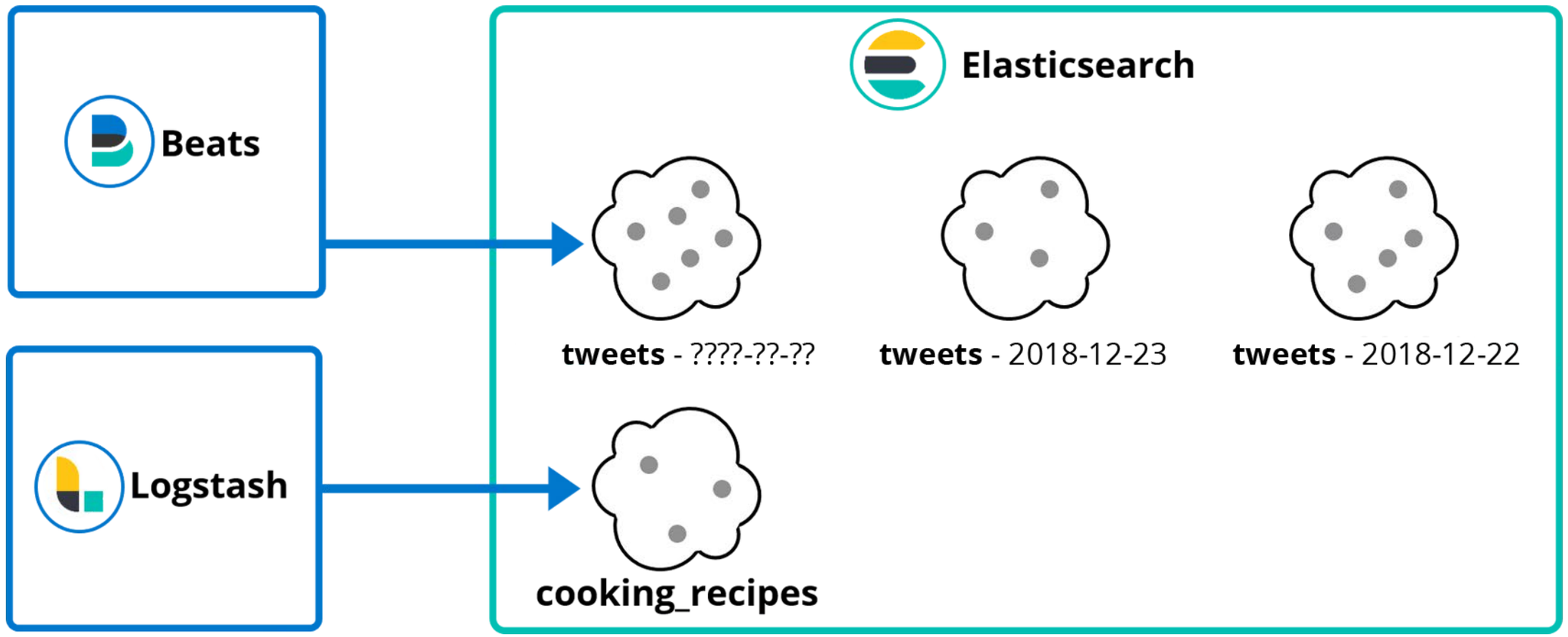
```
{
  "cuisine": "French",
  "ingredients": "Cheese, flour, butter, eggs, milk, nutmeg",
  "time_in_min": 50,
  "level": "easy"
}
```

Which category do these documents belong to?

```
{
  "tweet": "Wow Elasticsearch 7.0 seems awesome!",
  "hashtags": ["elasticsearch", "kibana"]
  "timestamp": September 1st 2017, 07:15:40.035
}
```

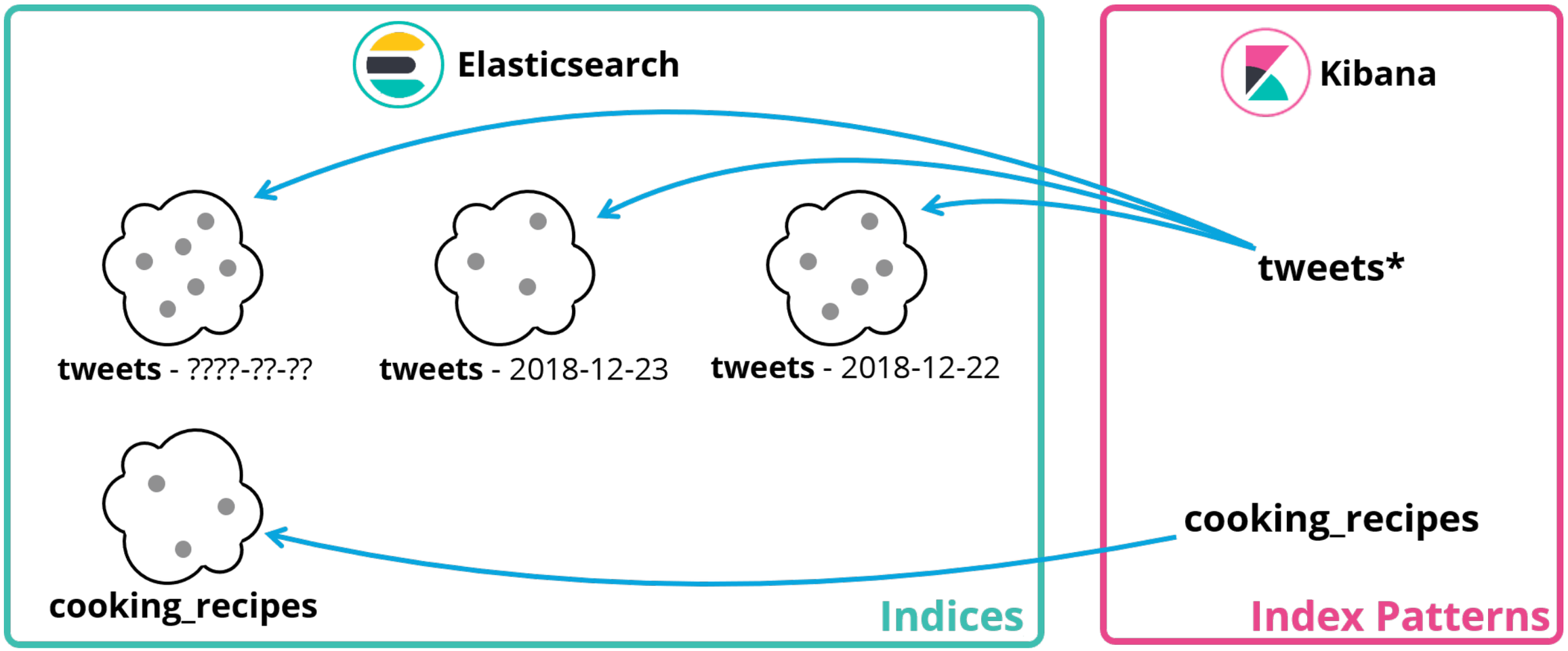
Elasticsearch Index

- Data Container
  - Categorical Index
  - Time Based Index



Kibana Index Pattern

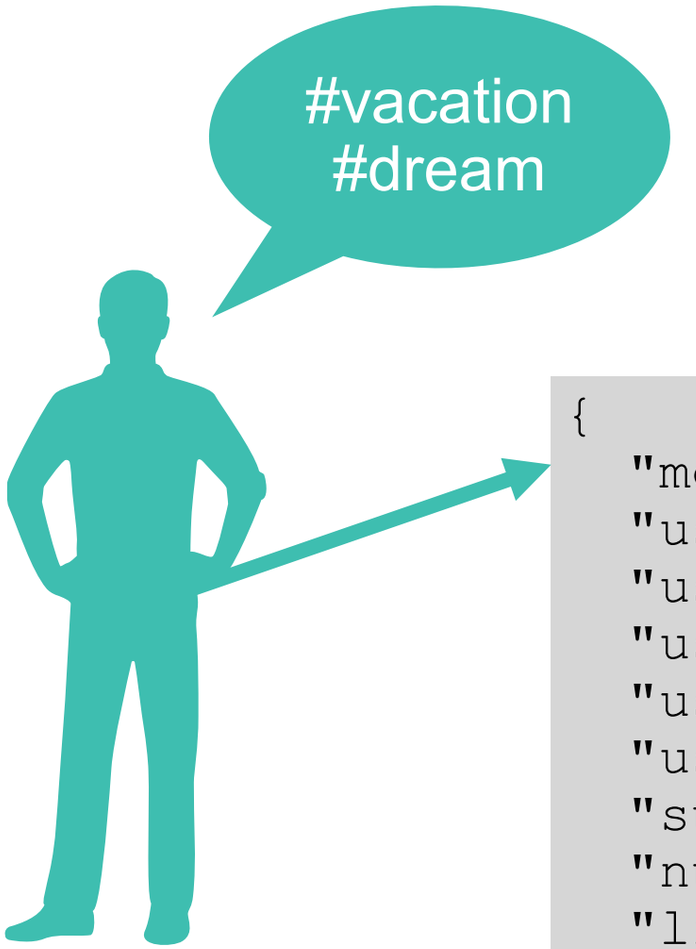
- Points to one or more Elasticsearch **indices**
- Tells Kibana which data you want to work with



Datasets

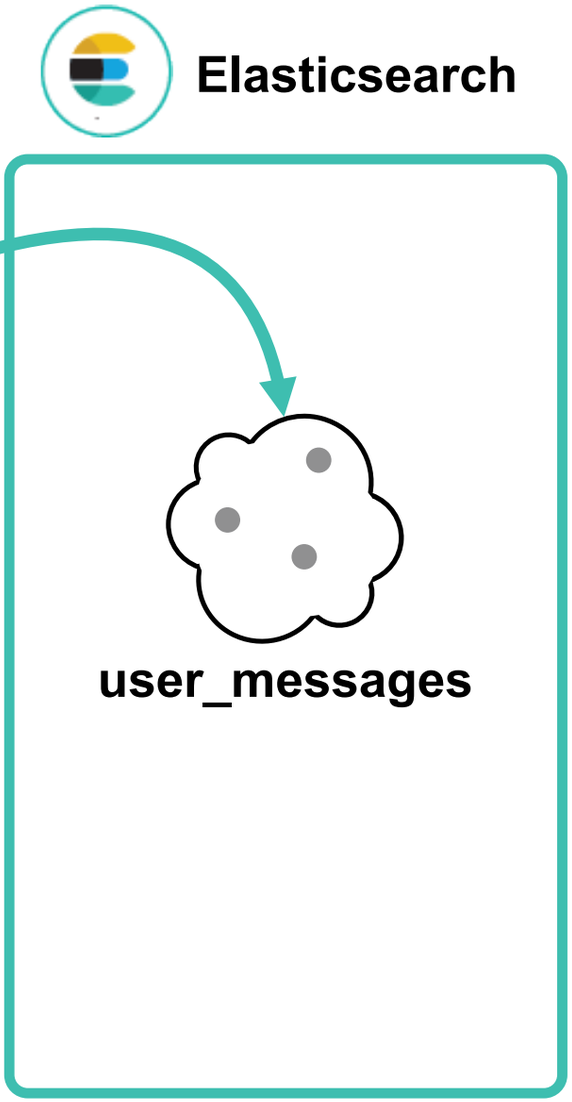
elastic

Messages

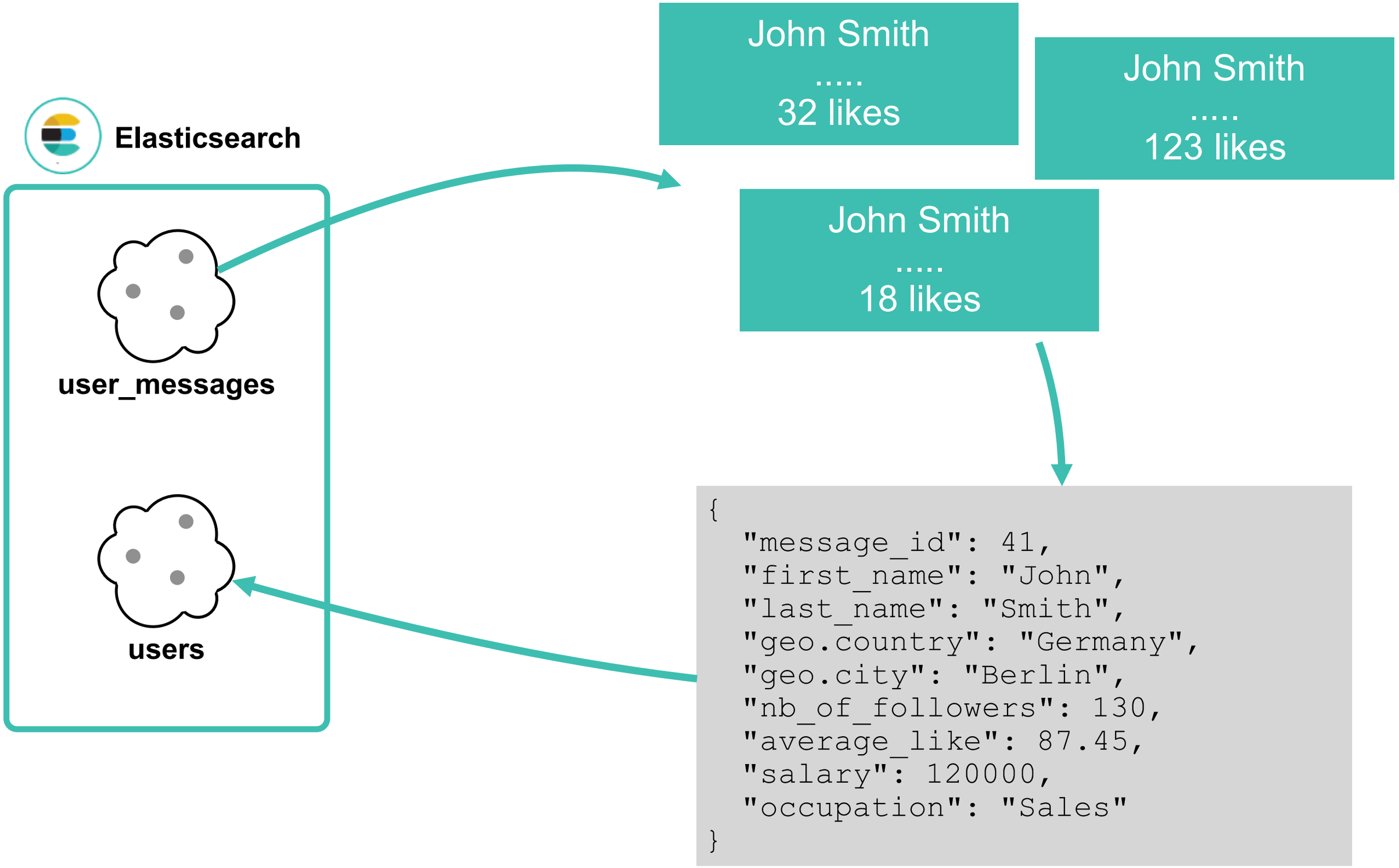


John Smith
Germany
Berlin
130 Followers

```
{
  "message_id": 1,
  "user.first_name": "John",
  "user.last_name": "Smith",
  "user.geo.country": "Germany",
  "user.geo.city": "Berlin",
  "user.nb_of_followers": 130,
  "subjects": "#vacation #dream",
  "number_of_subjects": 2,
  "likes": 32,
  "geo.country": "United Kingdom",
  "geo.city": "London"
}
```

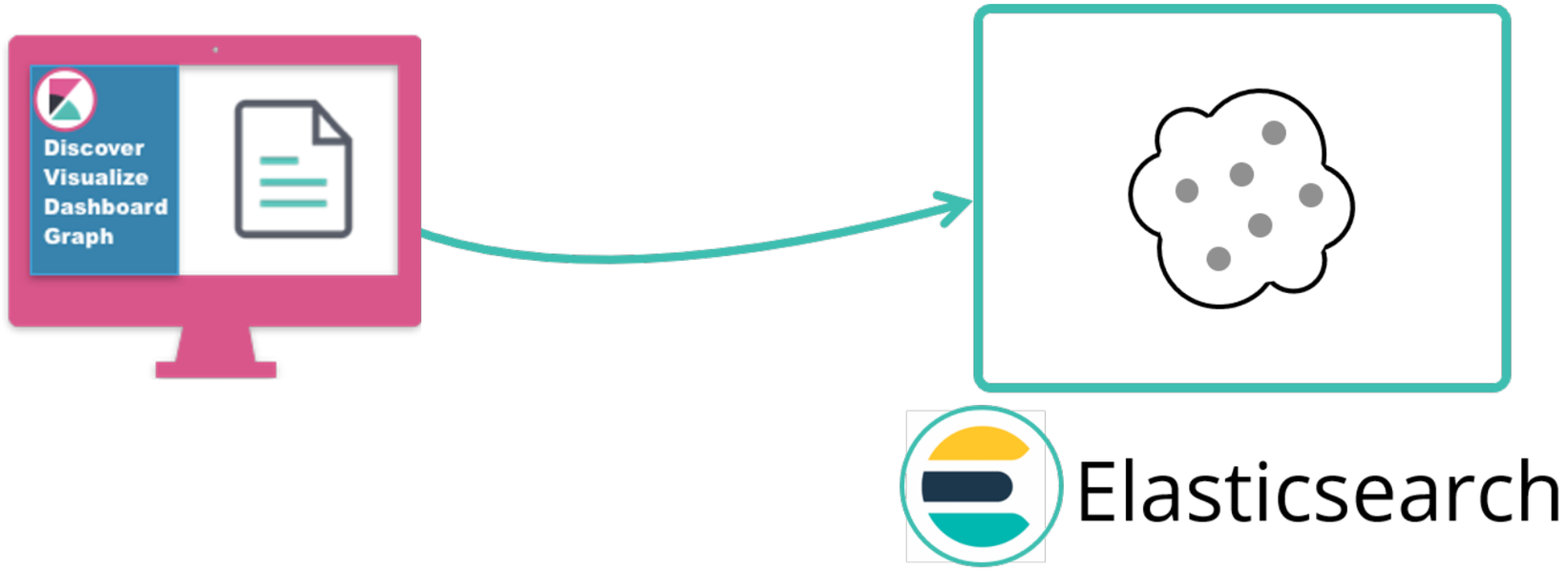


Users



Uploading Data

- Kibana is a powerful tool but it does not store data
  - If data needs to be stored then it needs to go into Elasticsearch
- Once the data is stored in Elasticsearch they can be leveraged by Kibana to create a visualization for instance



Lesson 1

Review - Introduction to Kibana

elastic

Summary

- Kibana can be used to analyze, search, interact with, and visualize the data in Elasticsearch
- Kibana can be used to manage the Elastic Stack
- Data is sent as JSON objects into Elasticsearch
- In Kibana, an index pattern can be created to target a specific set of indices

Quiz

1. What are the four main components of the Elastic Stack?
2. **True or False**: Data is stored inside Kibana.
3. What would be a suitable index pattern for accessing both **cooking_recipes** and **cooking_user** indices?

Kibana Fundamentals

Lesson 1

Lab - Introduction to Kibana

elastic

Kibana Fundamentals

Lesson 2

Discover Interface

elastic

Overview

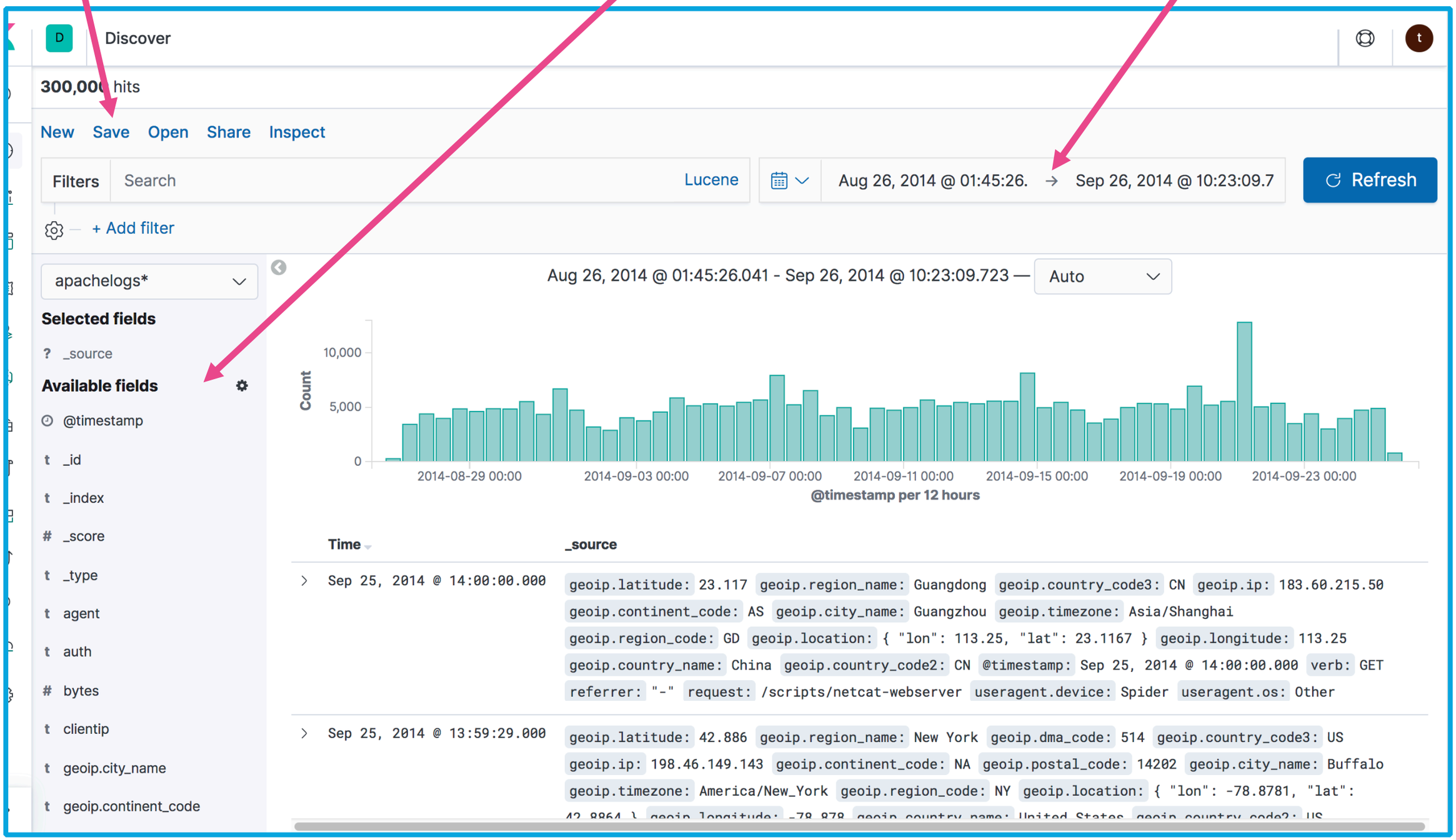
- Elasticsearch data types:
  - numeric
  - text
  - date
  - keywords
  - ...
- Discover interface
  - Explore data in Elasticsearch
  - Slice and Dice (Analyze) Data

Discover Interface

Tool bar

Side navigation

Time picker



elastic

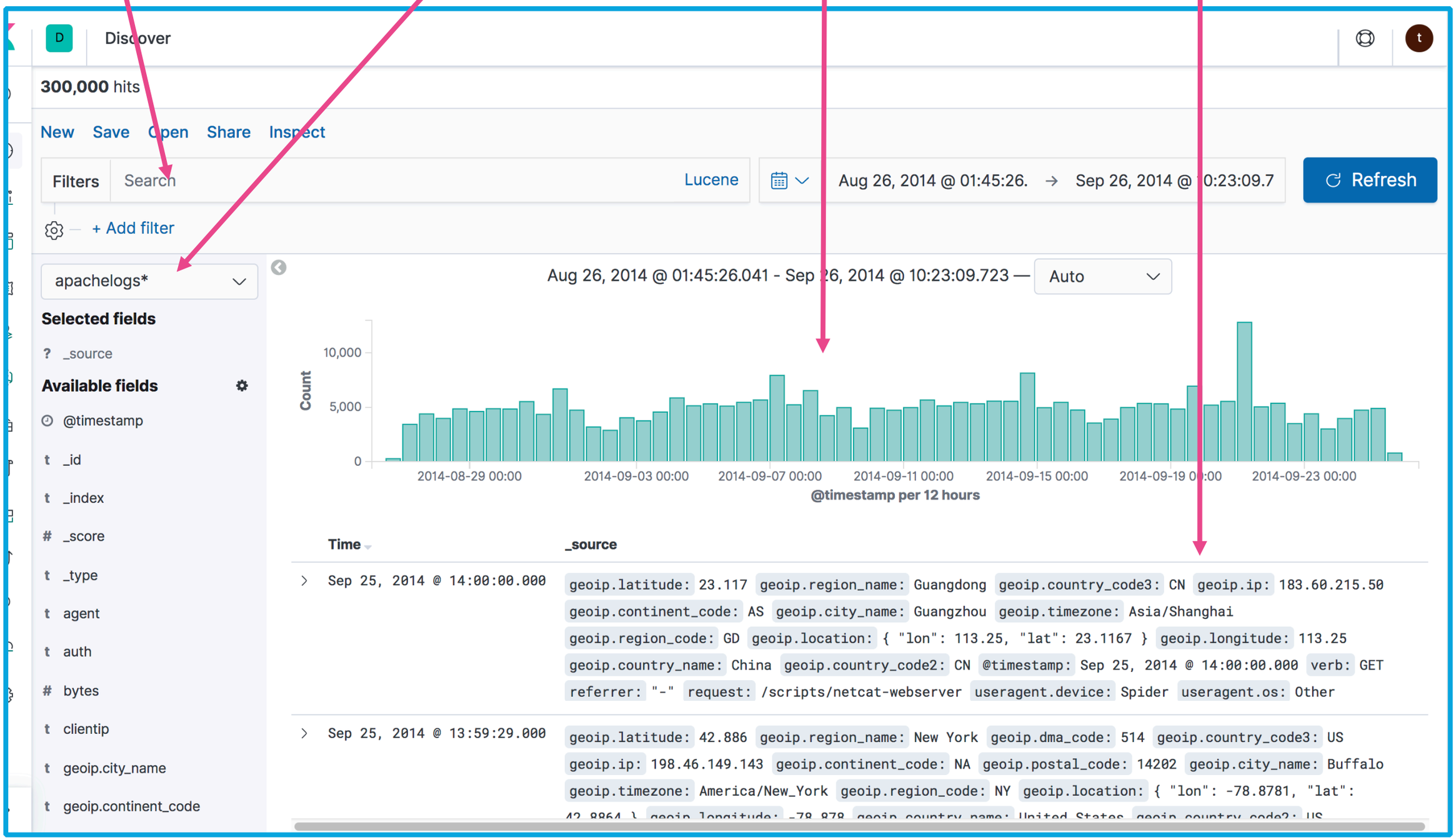
Discover Interface

Query bar

Index pattern

Histogram

Document table



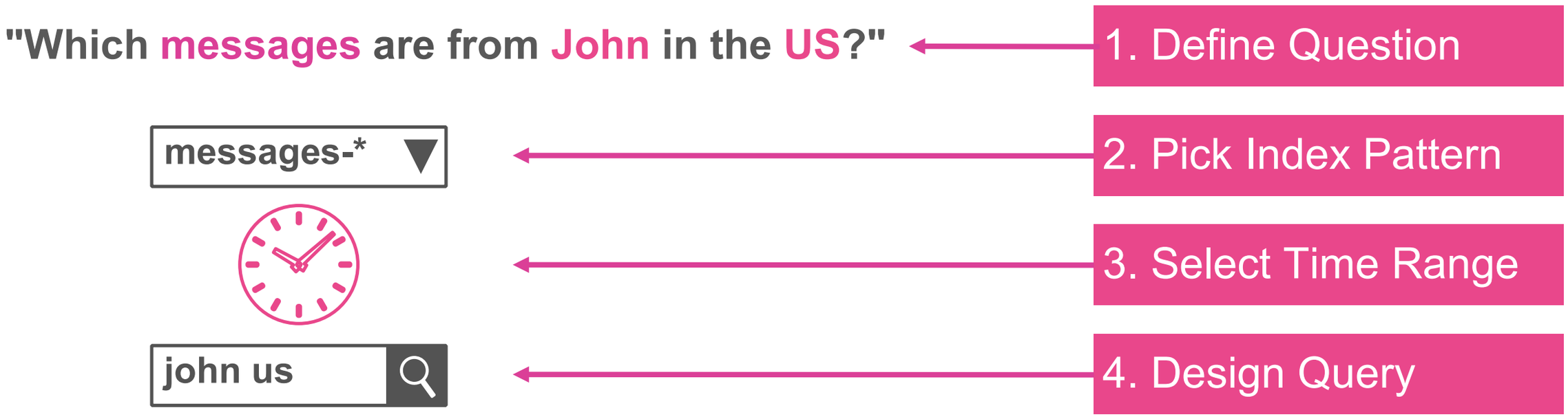
elastic

Search is Everywhere

- Elasticsearch is a search engine
  - Kibana can be used to search documents in Elasticsearch
- A search is executed by sending a **query** to Elasticsearch
  - A query can answer many different types of **questions**:
    - who are the users that are called Melissa?
    - what are the names of the people living in France?
    - are there any messages about Netflix?
- In Kibana, a search can be executed from the **query bar**
  - Kibana supports multiple query languages

Querying

- Kibana supports multiple query languages



id	user	age	country	category
1	Bill	30	FR	A
2	Marie	32	US	A
3	Claire	32	US	A
4	John	40	DE	B
5	John	44	US	B
6	Emma	44	US	B

Search a Specific Field

- By default, the query below will search all **fields** for all values

  - but being more specific will improve search

What are the messages published by user John from country US?

- Query above can be made more specific like this

  - Elasticsearch will only need to search limited **fields**

Boolean Operators

- By default, Kibana uses the **or** logic
  - so it matches any documents containing *john* **or** *us*
- Kibana allows you to use the following **boolean operators**:
  - **and**, **or**, and **not**
- Now, you can rewrite the query with the and logic

user:john and country:us

	id	user	age	country	category
✗	1	Bill	30	FR	A
✗	2	Marie	32	US	A
✗	3	Claire	32	US	A
✓	4	John	40	DE	B
✗	5	John	44	US	B
	6	Emma	44	US	B

Querying Numeric Fields

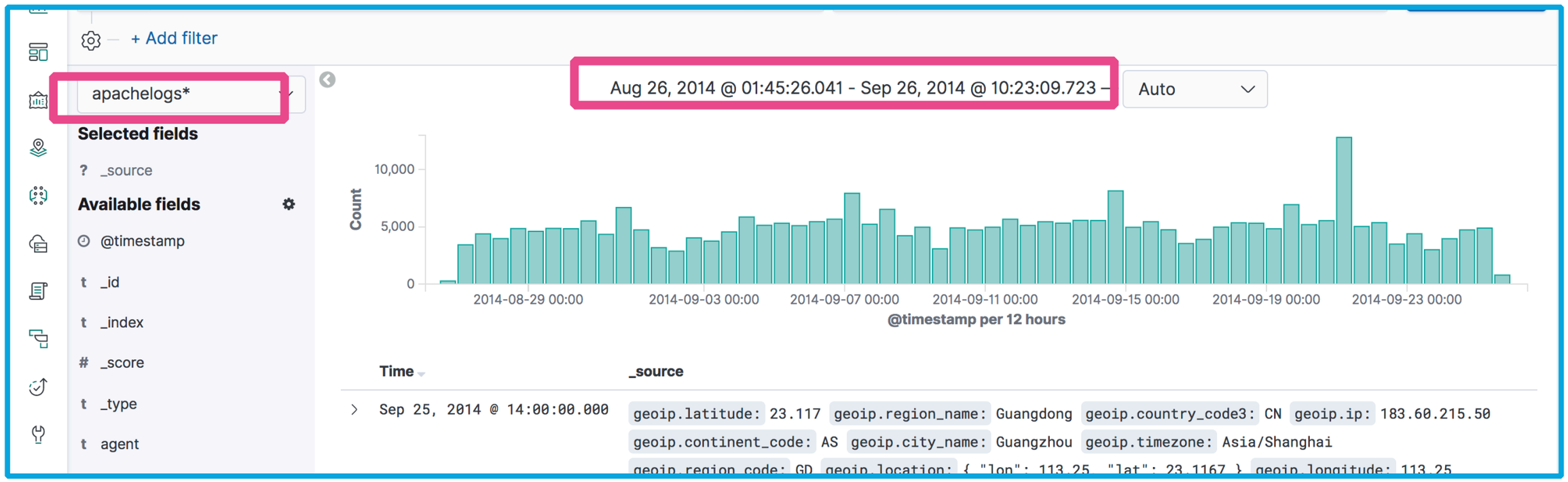
- Let's add some complexity to the question:

  What are the messages in which the user is John in the US country whose age is over 40?

- Numbers are different than text
  - instead of exact matches you often have relations:
    - less than (<)
    - less than or equal (<=)
    - greater than (>)
    - greater than or equal (>=)
- Now, you can rewrite the query as:

Query "Context"

- Query includes criteria about where to search based on
  - Distribution in Elasticsearch ← Index Pattern
  - Distribution in Time Period ← Time Picker
- Make sure to set the correct index pattern and timeframe:



elastic

Demo

Instructor Demo

Lesson 2

Review - Discover Interface

elastic

Summary

- The discover interface allows you to explore the different aspects of your data
- The most common mistake in the discover interface is not checking the **index pattern** and **time picker**
- The search bar can be used to search all the data inside Elasticsearch
- The document table can be customized to display a table of only selected fields

Quiz

1. What are the first two settings someone should check when using the discover interface?
2. What are the three different boolean operators?
3. Build the query: "Find the messages from **Claire** younger than **30** years old that belong to the category **A**?"

Kibana Fundamentals

Lesson 2

Lab - Discover Interface

elastic

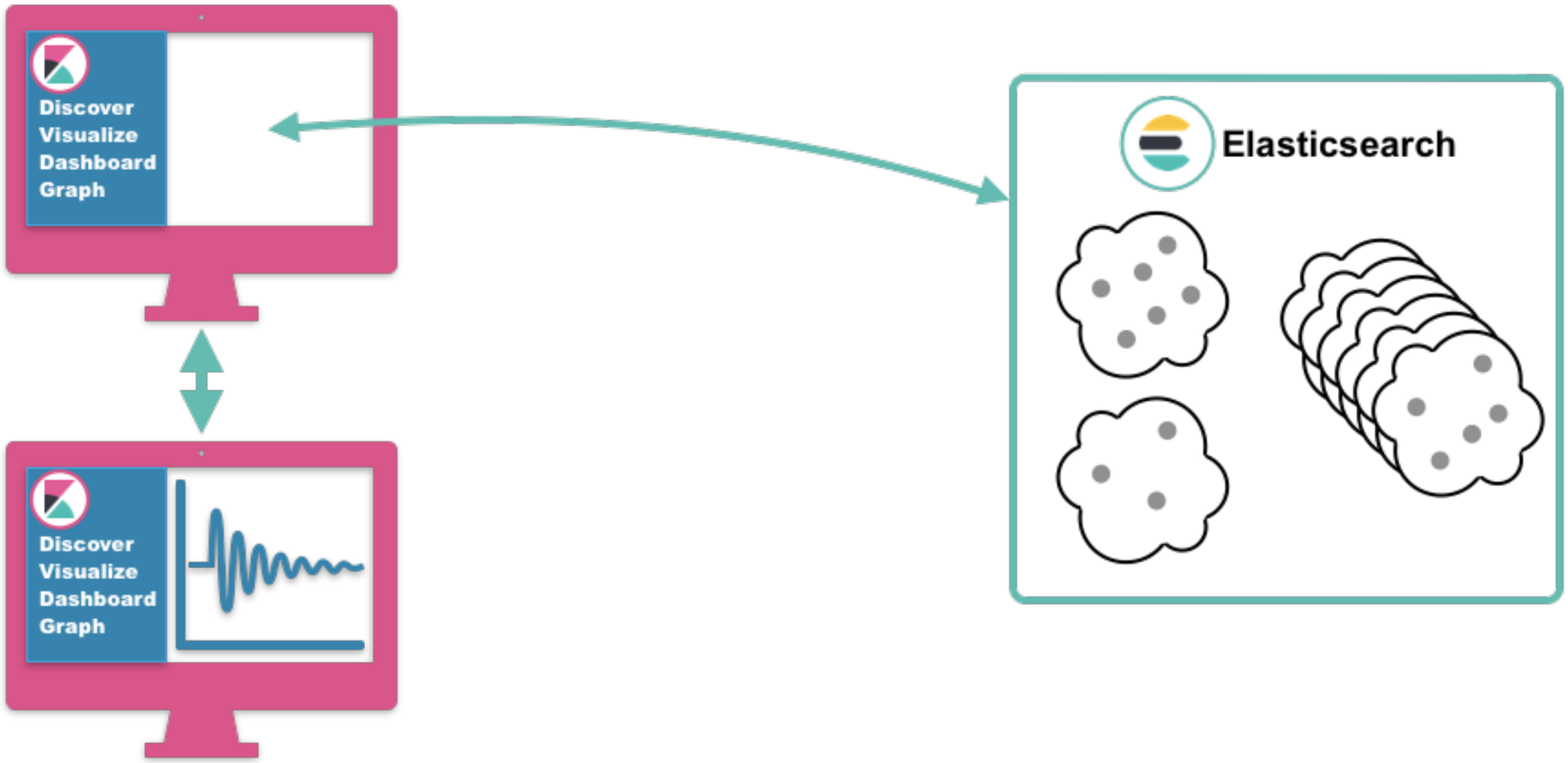
Kibana Fundamentals

Lesson 3

Visualizing Data

elastic

Kibana a Visualization Tool



Elasticsearch is Powering Kibana

- Kibana is a tool that anybody can use
- Knowing Elasticsearch will help a lot in using Kibana, but Kibana offers a wide variety of tools for every type of user and Kibana Lens is the perfect tool to start with

Kibana Lens

- Kibana Lens is an easy-to-use and intuitive UI
- It aims at simplifying the creation of visualizations. With this visualization, you will be able to:
  - Use the drag and drop feature
  - Explore the different types of visualizations
  - Create a visualization in just a few clicks

Lesson 3

Review – Visualizing Data

Summary

- Elasticsearch is computing the data that are going to be displayed in Kibana
- Someone does not need to be an expert in Elasticsearch to be able to use Kibana
- Kibana Lens is a type of visualization introduced in order to make the creation of a visualization simple

Quiz

1. **True or False:** Kibana Lens visualizations cannot be added to a dashboard.
2. **True or False:** Only people knowing Elasticsearch can create visualizations in Kibana.
3. **True or False:** Kibana computes and displays data.

Lesson 3

Lab – Visualizing Data

Conclusions

Thank You!

Please complete the online survey.

elastic

Quiz Answers

elastic

Introduction to Kibana

1. Elasticsearch, Kibana, Beats, Logstash
2. False
3. cooking_

Discover Interface

1. The time picker and the index pattern
2. and, or, not
3. user:claire and age<30 and category:a

Visualizing Data

1. False
2. False
3. False