Introduction to Kibana

Overview

Familiarise with the functionalities of Kibana

Know how to load, map and index data for analysis and visualisation in the Elastic Stack

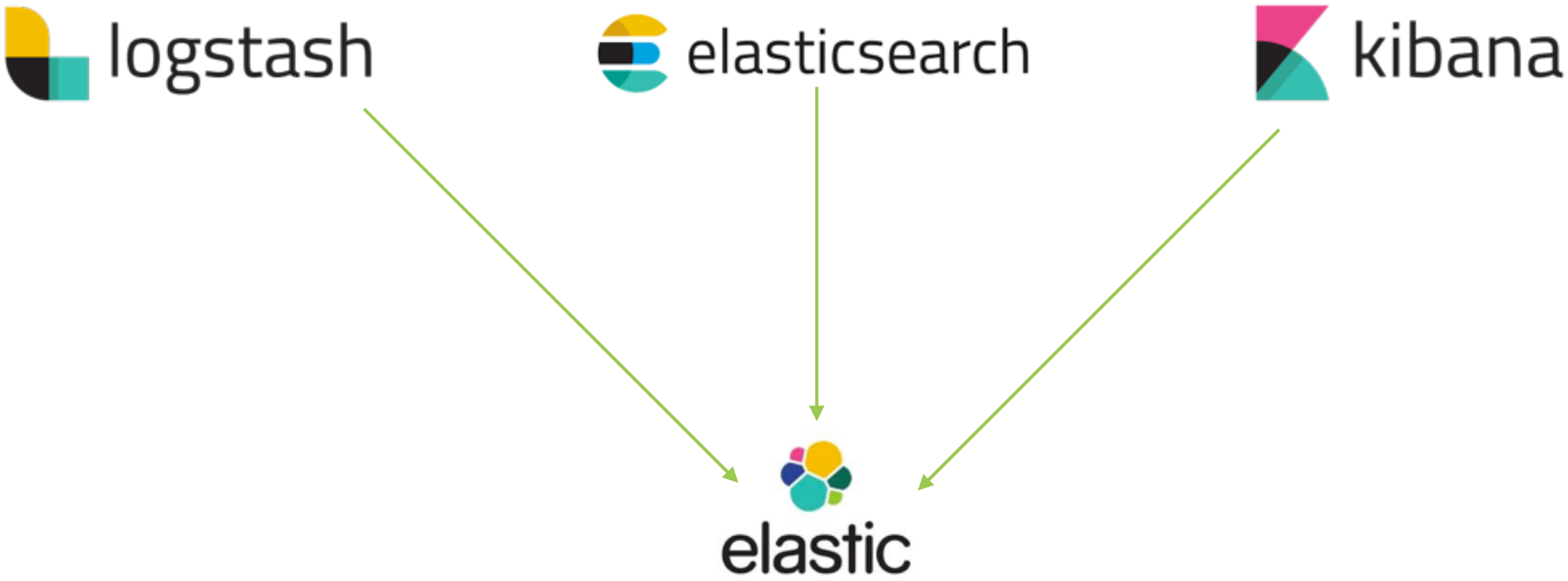
Analyse relationships using graphs

Identify trends using time series analysis

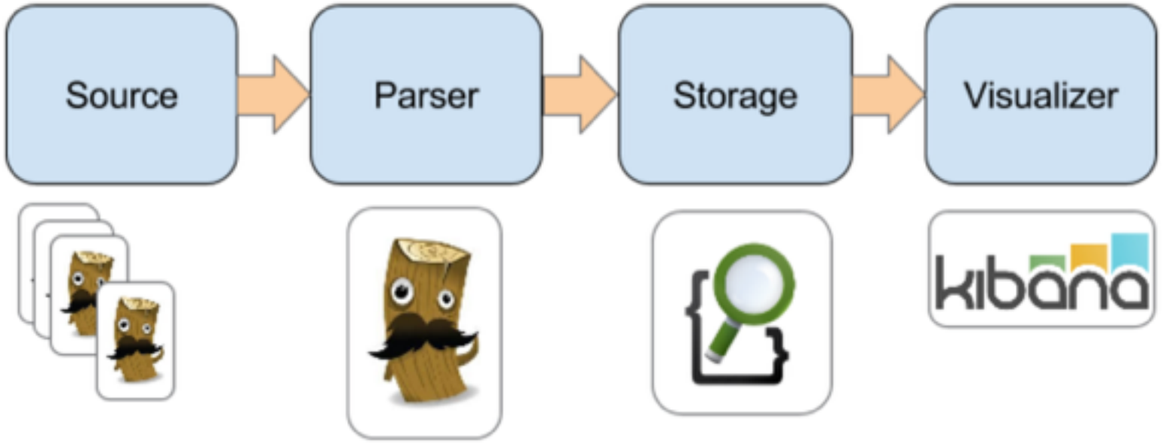
Assemble visualisations into dashboards

What is Kibana?

The Elastic Stack or ELK stack has three main components:



Logstash collects, parses, and stores logs for future use.



Elasticsearch converts raw data such as log files into internal documents and stores them on a distributed storage where they can be queried.

Kibana is a browser interface that can be used to search and visualise the data Elasticsearch has indexed.

Search Engine

Visualisation Tool

Elasticsearch helps you store and query data.

Kibana helps you make sense of that data.

kibana

Kibana is an open source analytics and visualisation platform designed to work with Elasticsearch. You use Kibana to search, view, and interact with data stored in Elasticsearch indices. You can easily perform advanced data analysis and visualize your data in a variety of charts, tables, and maps.

kibana

Kibana is an open source analytics and visualization platform designed to work with Elasticsearch. You use Kibana to search, view, and interact with data stored in Elasticsearch indices. You can easily perform advanced data analysis and visualize your data in a variety of charts, tables, and maps.

kibana

Kibana is an open source analytics and visualization platform designed to work with Elasticsearch. You use Kibana to **search, view, and interact with data stored in Elasticsearch indices.** You can easily perform advanced data analysis and visualize your data in a variety of charts, tables, and maps.

kibana

Kibana is an open source analytics and visualization platform designed to work with Elasticsearch. You use Kibana to search, view, and interact with data stored in Elasticsearch indices. You can easily perform **advanced data analysis and visualize your data in a variety of charts, tables, and maps.**

Use cases

Where is it used?
What is it used for?
Who is it for?

Centralized Logging
Application Management
Security Analytics

Infrastructure Monitoring
Operational Dashboards
Edge/Device Monitoring

Marketing Insights
Business Development
Customer Sentiment

Security Analytics | Log Analytics | Metrics Analytics | Operational Analytics | Marketing Analytics | Business Analytics

Developers / IT Operations → Data Scientists / Business Analysts

Developers Architects IT/Ops Business Analysts CTO/CIO/CDO

Get the same version as elastic search

Demo

Installation and setup

Elastic search will be running on 9200

kibana

The default location for kibana is:

http://localhost:5601

Functionalities of Kibana

Four Major Functionalities

Discover

Visualize

Timelion

Dashboard

Four Major Functionalities

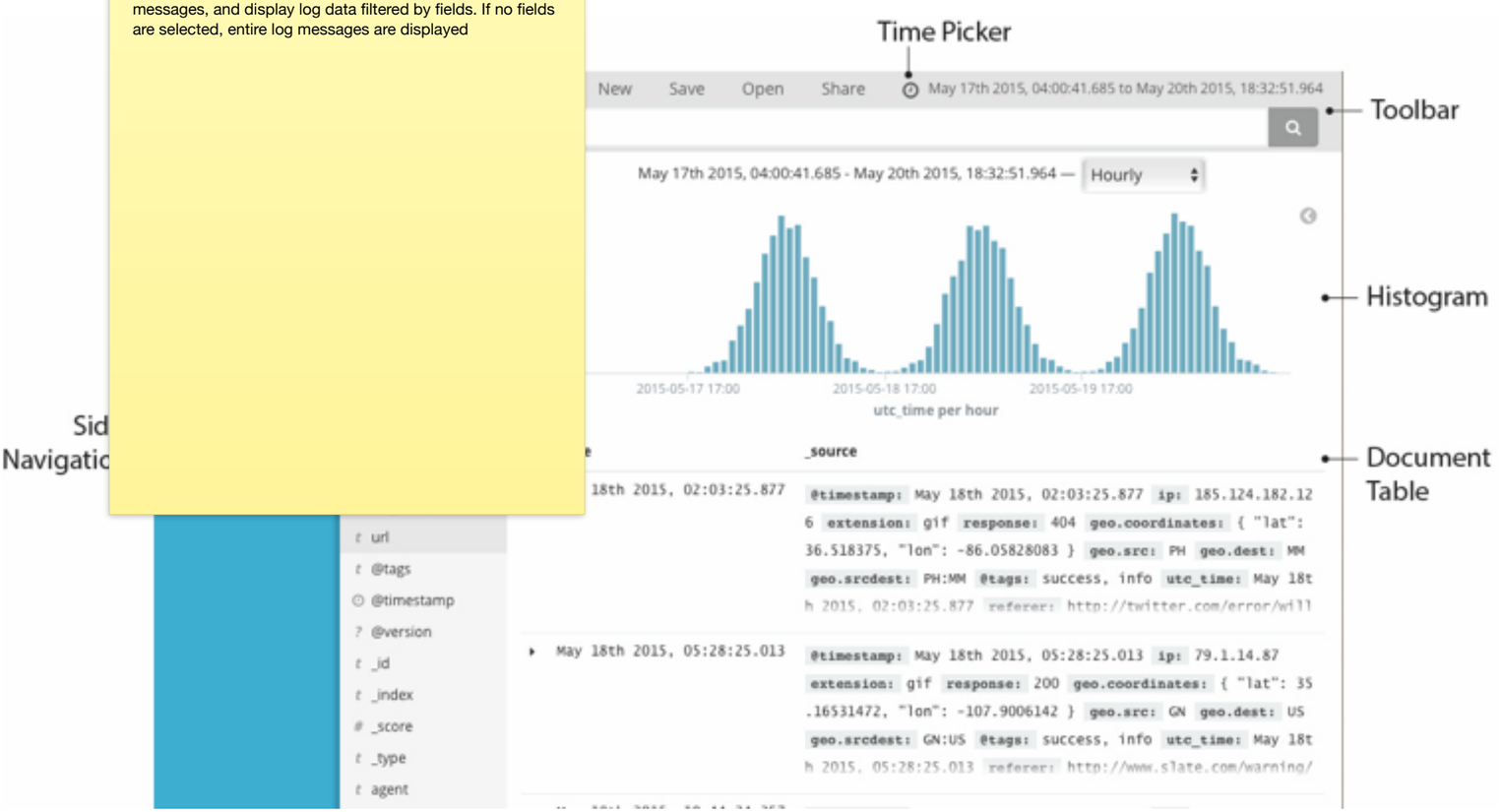
Discover

Visualize

Timelion

Dashboard

Search Bar: Directly under the main navigation menu. Use this to search specific fields and/or entire messages
Time Filter: Top-right (clock icon). Use this to filter logs based on various relative and absolute time ranges
Field Selector: Left, under the search bar. Select fields to modify which ones are displayed in the Log View
Date Histogram: Bar graph under the search bar. By default, this shows the count of all logs, versus time (x-axis), matched by the search and time filter. You can click on bars, or click-and-drag, to narrow the time filter
Log View: Bottom-right. Use this to look at individual log messages, and display log data filtered by fields. If no fields are selected, entire log messages are displayed



Discover

Interactively explore your data

- submit search queries
- filter the search results
- view document data
- get field value statistics & histograms

Mapping

Mapping is the process of defining how a document, and the

which string fields should be treated as full text fields.
- which fields contain numbers, dates, or geolocations.
- whether the values of all fields in the document should be indexed into the catch-all _allfield.
- the format of date values.
- custom rules to control the mapping for dynamically added fields.

https://www.elastic.co/guide/en/elasticsearch/reference/current/indices-put-mapping.html

Demo

Loading sample data for visualisation

Specify mappings for the sample data

Defining index patterns

Discovering the data

Saving searches for visualisations

saved objects and index patterns can be viewed under the management tab

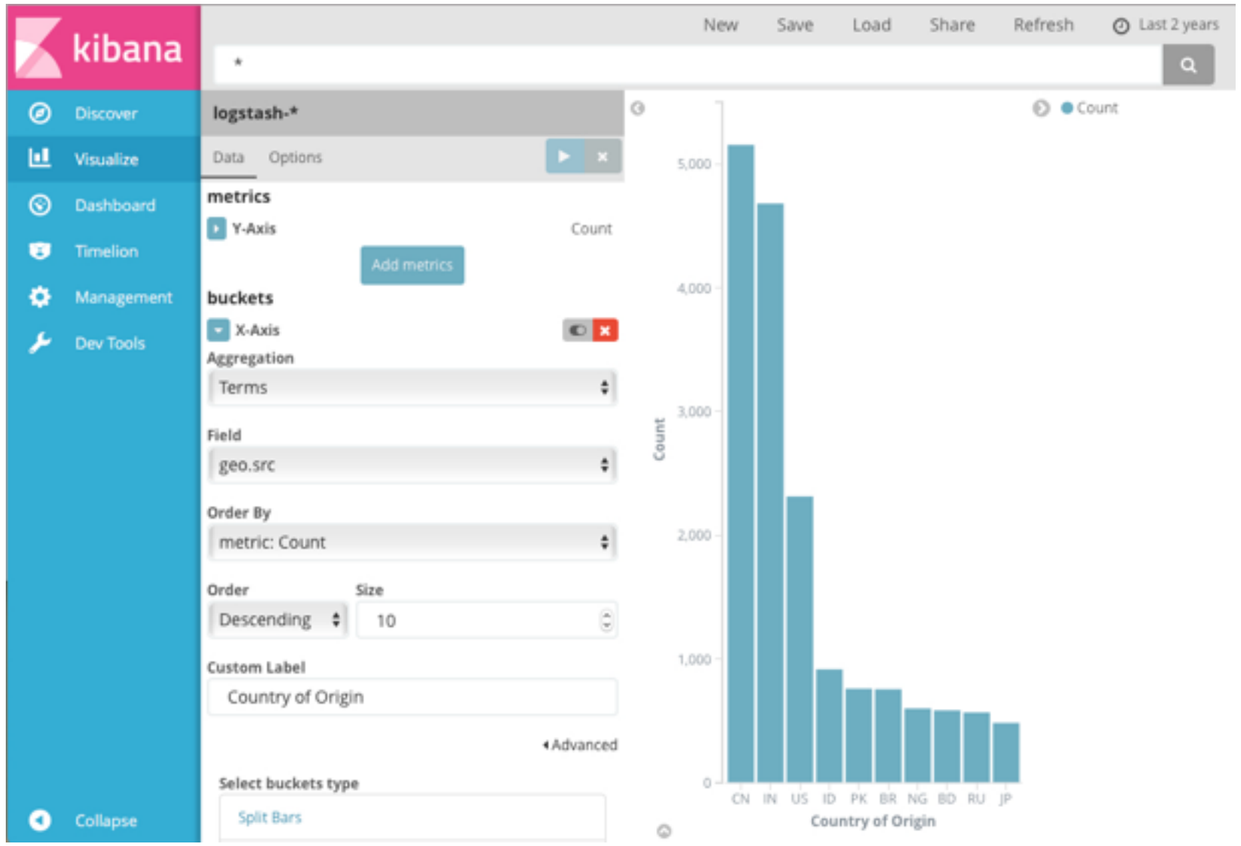
Four Major Functionalities

Discover

Visualize

Timelion

Dashboard



Visualize

Create visualisations of the data in your Elasticsearch indices.

Aggregations to extract and process data.

Create charts that show the trends, spikes, and dips.

Demo

Visualising data using aggregations and nested aggregations

Visualising data from saved searches

Graphs, charts & markdown widgets

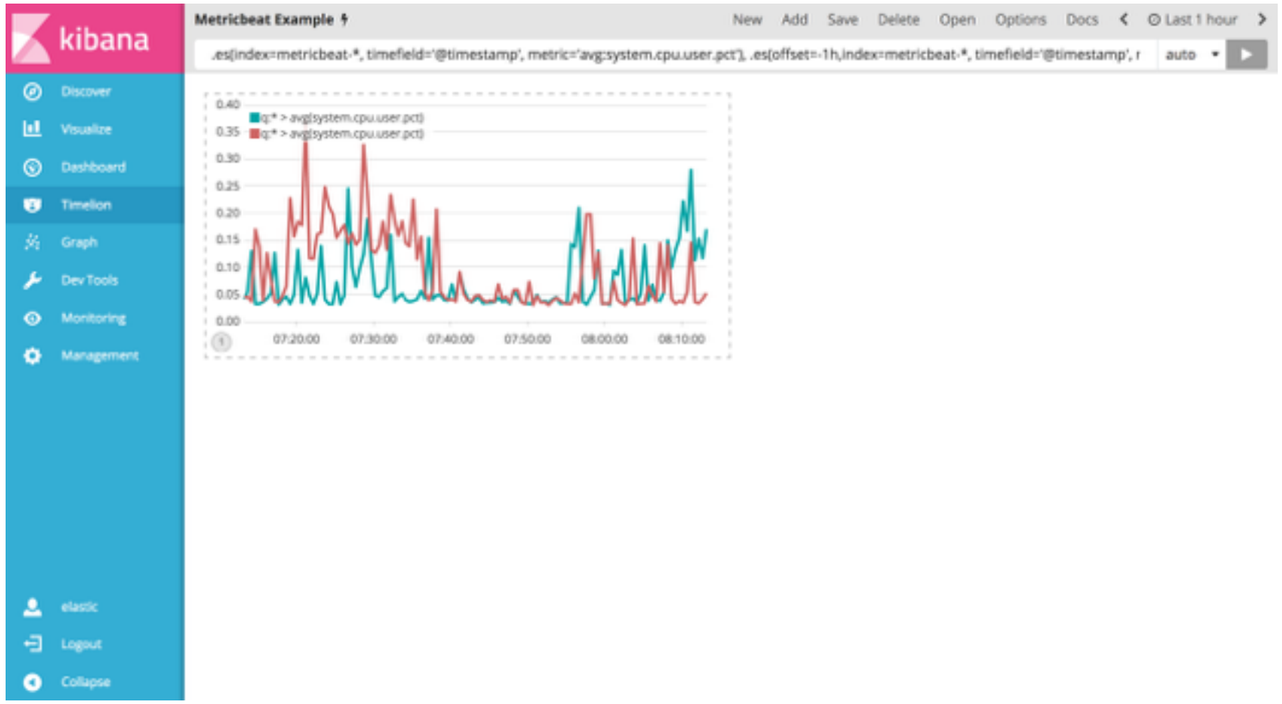
Four Major Functionalities

Discover

Visualize

Timelion

Dashboard



Timelion

A time series data visualiser

Driven by a simple expression language

Retrieve time series data, perform calculations and visualise the results.

kibana | Mathematical Functions

Demo

Time Series Analysis

Formatting timeline

Mathematical Functions on timeline

Tracking trends on timeline

can either be saved as visualisation or an entire timeline sheet

Four Major Functionalities

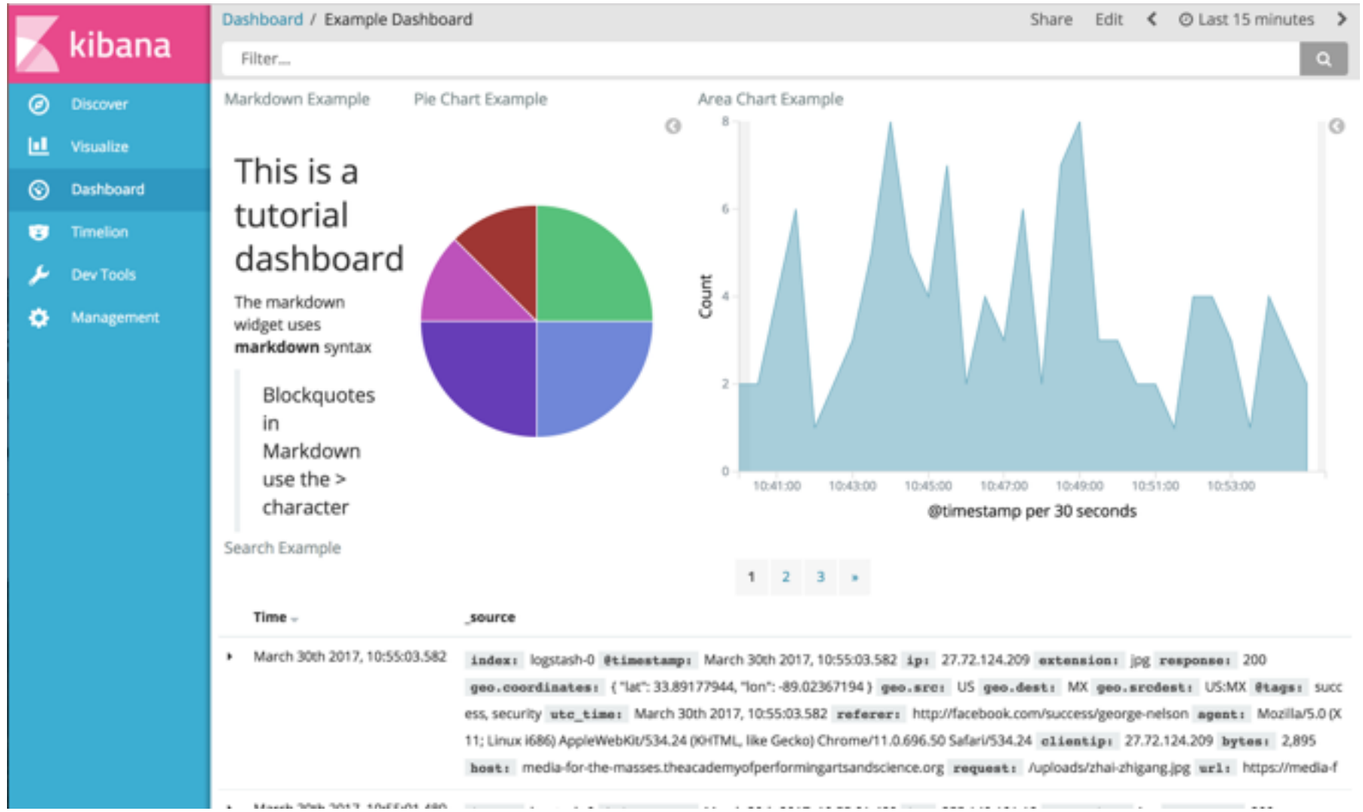
Discover

Visualize

Timelion

Dashboard

Dashboards



A collection of saved visualisations.

Allows edit, move, delete, and resize operations on visualisations.

Can be shared as json file,link or HTML code.

Demo

Loading dashboards

Formatting dashboards

Sharing dashboards

Summary

Performed search queries on Elasticsearch data using the discover page

Performed and visualised aggregations on data as charts and graphs.

Analysed trends using time series analysis.

Built and shared dashboards.