

AI기법과 활용

Week-10. Elastic Stack

2022-Summer 서중원

Elasticsearch Mapping

Mapping이란?

- 관계형 데이터의 스키마와 동일
- Mapping 없이 데이터를 엘라스틱서치에 삽입?
 - 가능
 - 하지만, Mapping을 없이 데이터를 넣는 것은 데이터의 사용성이 떨어질 수 있음
 - 예를들어 2020-11-07이라는 값을 Mapping없이 넣는다면?
 - String으로 인지할 수 있음
 - 날짜별 정렬, 월별 정렬/필터링과 같은 연산을 사용할 수 없음
 - 숫자를 입력했지만, 문자열로 인식했다?
 - Min, max, mean, median과 같은 연산을 사용할 수 X
- 가능하다면! 항상 Mapping을 먼저 지정해 놓고 데이터를 삽입!
 - 데이터 먼저 넣고, Mapping을 후에 지정해줄 수도 있음

Elasticsearch Search

Search 방식

- request_body에 json 형식으로 조건을 작성!

```
body = {  
    "query": {  
        "term": {  
            "points":30  
        }  
    }  
}  
  
res = es.search(body=body,index=INDEX_NAME)  
pprint.pprint(res)
```

Elasticsearch Aggregation

Aggregation 이란?

- Search Query 사용시 수치적 값들의 다양한 값을 얻어 낼 수 있다.

```
body = {  
    "size" : 0,  
    "aggs" : {  
        "avg_score" : {  
            "avg" : {  
                "field" : "points"  
            }  
        }  
    }  
}  
  
res = es.search(body=body,index=INDEX_NAME)  
pprint.pprint(res)
```

Elasticsearch Bucket Aggregation

Bucket Aggregation 이란?

- RDB의 group by와 유사한 기능
- “document의 bucket을 만든다”

```
body = {  
    "size" : 0,  
    "aggs" : {  
        "team_stats" : {  
            "terms" : {  
                "field" : "team"  
            },  
            "aggs" : {  
                "stats_score" : {  
                    "stats" : {  
                        "field" : "points"  
                    }  
                }  
            }  
        }  
    }  
}  
res = es.search(body=body,index=INDEX_NAME)  
pprint.pprint(res)
```

Kibana

Home - Elastic

주의 요함 | 34.64.152.106:8500/app/home#/

elastic

Search Elastic

Home

Welcome home



Enterprise Search

Create search experiences with a refined set of APIs and tools.



Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.



Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.



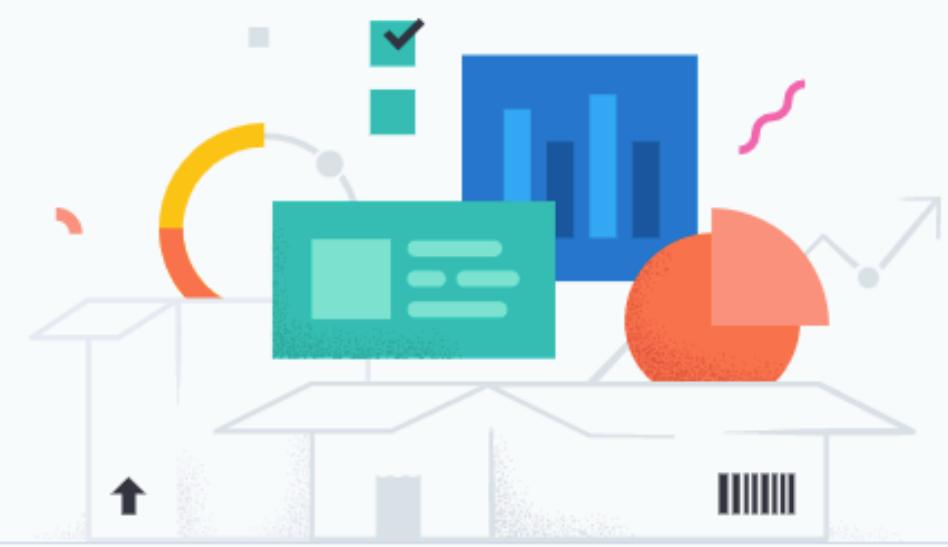
Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, add a sample data set.

[+ Add integrations](#) [Try sample data](#) [Upload a file](#)



Management



Manage permissions

Control who has access and what tasks they can perform.



Monitor the stack

Track the real-time health and performance of your deployment.



Back up and restore

Save snapshots to a backup repository, and restore to recover index and cluster state.



Manage index lifecycles

Define lifecycle policies to automatically perform operations as an index ages.

[Dev Tools](#) [Stack Management](#)

좌측의 메뉴화면에서 Stack Management 클릭후, 그동안 생성한 인덱스들이 잘 들어갔는지 확인

The screenshot shows the Elastic Stack Management interface. On the left, there is a navigation sidebar with several sections:

- Home**: Home, Overview, Alerts, Cases, Logs, Metrics, APM, Uptime, User Experience.
- Security**: Overview, Alerts, Hosts, Network, Timelines, Cases, Endpoints.
- Management**: Dev Tools, Integrations, Fleet, Osquery, Stack Monitoring, **Stack Management**.

The main content area features a "Welcome home" header and four large cards: Enterprise Search, Observability, Security, and Analytics. Below this is a section titled "Get started by adding integrations" with buttons for "Add integrations", "Try sample data", and "Upload a file".

In the bottom right corner of the main content area, there are links for "Dev Tools" and "Stack Management".

The "Management" section at the bottom contains four sub-links: "Manage permissions", "Monitor the stack", "Back up and restore", and "Manage index lifecycles".

The URL in the browser bar is 34.64.152.106:8500/app/home/.

Index Management 클릭

The screenshot shows a web browser window for the 'Elastic' application at the URL 34.64.152.106:8500/app/management. The left sidebar contains a navigation menu with several sections: **Ingest**, **Data** (with **Index Management** highlighted with a red box), **Alerts and Insights**, **Kibana**, and **Stack**. The main content area displays a large gear icon and the text "Welcome to Stack Management 7.17.5". Below this, it says "Manage your indices, index patterns, saved objects, Kibana settings, and more." A note at the bottom states "A complete list of apps is in the menu on the left."

Elastic

주의 요함 | 34.64.152.106:8500/app/management

elastic

Search Elastic

Management

Ingest

Ingest Pipelines

Data

Index Management

Index Lifecycle Policies

Snapshot and Restore

Rollup Jobs

Transforms

Remote Clusters

Alerts and Insights

Rules and Connectors

Reporting

Machine Learning Jobs

Kibana

Index Patterns

Saved Objects

Tags

Search Sessions

Spaces

Advanced Settings

Stack

License Management

Upgrade Assistant

Welcome to Stack Management
7.17.5

Manage your indices, index patterns, saved objects, Kibana settings, and more.

A complete list of apps is in the menu on the left.

잘들어갔네요!

The screenshot shows the Elasticsearch Index Management interface. On the left, there's a sidebar with various management sections like Ingest, Data, Alerts and Insights, Kibana, and Stack. The main area is titled "Index Management" and has tabs for Indices, Data Streams, Index Templates, and Component Templates. The Indices tab is selected. It displays two indices: "classes" and "basketball". Both indices are yellow (warning) and open. The "classes" index has 1 primary, 1 replica, 24 documents, and 9.5kb storage size. The "basketball" index has 1 primary, 1 replica, 16 documents, and 7.2kb storage size. A red box highlights the table containing these index details. At the bottom right of the table, there's a "Rows per page: 10" dropdown and a page number indicator "1".

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
classes	yellow	open	1	1	24	9.5kb	
basketball	yellow	open	1	1	16	7.2kb	

Index Patterns 클릭

The screenshot shows the Elasticsearch Index Management interface. The left sidebar has a red box around the 'Index Patterns' link under the 'Kibana' section. The main area shows the 'Indices' tab selected, displaying a table of indices:

<input type="checkbox"/> Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
classes	● yellow	open	1	1	24	9.5kb	
basketball	● yellow	open	1	1	16	7.2kb	

Below the table, there are buttons for 'Include rollup indices' and 'Include hidden indices'. A 'Search' input field and a 'Reload indices' button are also present.

Index Pattern 생성

Index patterns - Elastic

주의 요함 | 34.64.152.106:8500/app/management/kibana/indexPatterns

elastic

Stack Management Index patterns

Management

Ingest ⓘ

Ingest Pipelines

Data ⓘ

Index Management

Index Lifecycle Policies

Snapshot and Restore

Rollup Jobs

Transforms

Remote Clusters

Alerts and Insights ⓘ

Rules and Connectors

Reporting

Machine Learning Jobs

Kibana ⓘ

Index Patterns

Saved Objects

Tags

Search Sessions

Spaces

Advanced Settings

Stack ⓘ

License Management

Upgrade Assistant

Index patterns

Create and manage the index patterns for your data.

Pattern ↑

Search...

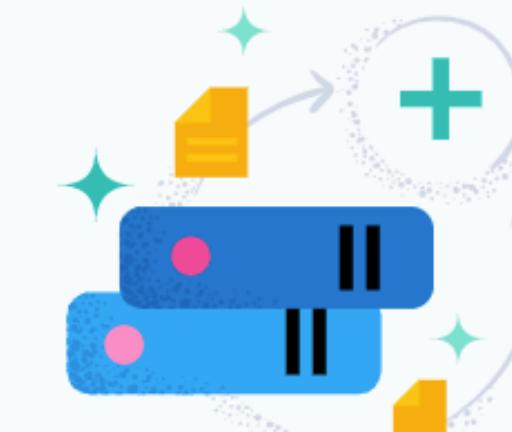
You have data in Elasticsearch.
Now, create an index pattern.

Kibana requires an index pattern to identify which data streams, indices, and index aliases you want to explore. An index pattern can point to a specific index, for example, your log data from yesterday, or all indices that contain your log data.

+ Create index pattern

Want to learn more? [Read documentation](#)

X Close



basketball 입력, submit_date 선택

The screenshot shows the Kibana management interface for creating an index pattern. The left sidebar has sections for Management, Ingest, Data, Alerts and Insights, and Kibana. The 'Index Patterns' section under Kibana is selected and highlighted in blue. The main area is titled 'Create index pattern'. A red box highlights the 'Name' field, which contains 'basketball*'. Another red box highlights the 'Timestamp field' field, which contains 'submit_date'. At the bottom right of the main form, a red box highlights the 'Create index pattern' button. To the right of the main form, a sidebar displays a message: '✓ Your index pattern matches 1 source.' followed by a list of sources: 'basketball' with an 'Index' button. Below this, it says 'Rows per page: 10'.

Index patterns - Elastic

← → C ▲ 주의 요함 | 34.64.152.106:8500/app/management/kibana/indexPatterns

elastic

Management

Ingest

Data

Alerts and Insights

Kibana

Index Patterns

Saved Objects

Tags

Search Sessions

Spaces

Advanced Settings

Stack

License Management

Upgrade Assistant

Stack Management

Index patterns

Create index pattern

Name

basketball*

Use an asterisk (*) to match multiple characters. Spaces and the characters , /, ?, ", <, >, | are not allowed.

Timestamp field

submit_date

Select a timestamp field for use with the global time filter.

Show advanced settings

Close

Create index pattern

✓ Your index pattern matches 1 source.

basketball

Index

Rows per page: 10

각각의 필드가 보입니다!

The screenshot shows the Elasticsearch Kibana Management interface for the **basketball*** index pattern. The left sidebar contains navigation links for Management, Ingest, Data, Alerts and Insights, Kibana, Index Patterns, and Stack. The main area displays the **basketball*** index pattern details. A yellow box highlights the **Time field: 'submit_date'**. Below it, a message says "View and edit fields in **basketball***. Field attributes, such as type and searchability, are based on [field mappings](#) in Elasticsearch." A red box highlights the **Fields (14)** section, which lists the following fields:

Name ↑	Type	Format	Searchable	Aggregatable	Excluded
_id	_id		●	●	
_index	_index		●	●	
_score					
_source	_source				
_type	_type		●	●	
assist	long		●	●	
assists	long		●	●	
blocks	long		●	●	
name	text		●	●	
points	long		●	●	

At the bottom right, there is a message: **✓ Saved 'basketball*'.**

Kibana Discover

Discover로 이동

Discover - Elastic

▲ 주의 요함 | 34.64.152.106:8500/app/discover#/?_a=(columns:!(),filters:!(),index:'585f8e80-09c8-11ed-83bb-5d5fb1e3defd',interval:auto,query:(language:kuery,query:""),sort:!(!(submit_date,desc))...)

elastic

Search Elastic

☰ D Discover Options New Open Share Inspect Save

Home Analytics Overview Discover Dashboard Canvas Maps Machine Learning Visualize Library

Enterprise Search Overview App Search Workplace Search

Observability Overview Alerts Cases Logs Metrics APM Uptime User Experience

Add integrations

No results match your search criteria

Expand your time range

Try searching over a longer period of time.

KQL Last 15 minutes Show dates Refresh

34.64.152.106:8500/app/discover#/

The screenshot shows the Elastic Discover interface. On the left, there's a navigation sidebar with sections for Analytics, Enterprise Search, Observability, and Security. The 'Discover' link under the Analytics section is highlighted with a red box. The main area displays a message: 'No results match your search criteria' with a magnifying glass icon. Below this, it says 'Expand your time range' and 'Try searching over a longer period of time.' At the bottom of the sidebar, there's a blue button labeled '+ Add integrations'. The URL at the bottom of the page is '34.64.152.106:8500/app/discover#/'. The top bar includes standard browser controls like back, forward, and search, along with the Elastic logo and user profile.

2016년 10월 1일부터 11월 30일까지로 설정

Discover - Elastic

▲ 주의 요함 | 34.64.152.106:8500/app/discover#/?_a=(columns:!(),filters:!(),index:'585f8e80-09c8-11ed-83bb-5d5fb1e3defd',interval:auto,query:(language:kuery,query:""),sort:[!(_id,desc)]...)

elastic

Search Elastic

D Discover

Options New Open Share Inspect Save

Search

KQL

Oct 1, 2016 @ 22:58:39.298 → Nov 30, 2016 @ 23:13:31.648

+ Add filter

basketball*

16 hits

Search field names

Filter by type 0

Available fields 13

_id
_index
_score
_type
assist
assists
blocks
name
points
rebound
rebounds
submit_date
team

Time ↓ Document

> Nov 28, 2016 @ 09:00:00.000 assist: 4 blocks: 1 name: StephenCurry points: 32 rebound: 1 submit_date: Nov 28, 2016 @ 09:00:00.000 team: GoldenStatesWarriors _id: 6 _index: basketball _score: - _type: _doc

> Nov 27, 2016 @ 09:00:00.000 assist: 4 blocks: 5 name: RudyGobert points: 8 rebound: 10 submit_date: Nov 27, 2016 @ 09:00:00.000 team: UtahJazz _id: 12 _index: basketball _score: - _type: _doc

> Nov 27, 2016 @ 09:00:00.000 assist: 14 blocks: 3 name: JohnWall points: 22 rebound: 4 submit_date: Nov 27, 2016 @ 09:00:00.000 team: WashingtonWizards _id: 16 _index: basketball _score: - _type: _doc

> Nov 25, 2016 @ 09:00:00.000 assist: 2 blocks: 1 name: StephenCurry points: 36 rebound: 1 submit_date: Nov 25, 2016 @ 09:00:00.000 team: GoldenStatesWarriors _id: 5 _index: basketball _score: - _type: _doc

> Nov 22, 2016 @ 09:00:00.000 assist: 2 blocks: 7 name: RudyGobert points: 12 rebound: 14 submit_date: Nov 22, 2016 @ 09:00:00.000 team: UtahJazz _id: 11 _index: basketball _score: - _type: _doc

> Nov 22, 2016 @ 09:00:00.000 assist: 12 blocks: 3 name: JohnWall points: 15 rebound: 3 submit_date: Nov 22, 2016 @ 09:00:00.000 team: WashingtonWizards _id: 15 _index: basketball _score: - _type: _doc

> Nov 20, 2016 @ 09:00:00.000 assist: 2 blocks: 1 name: StephenCurry points: 36 rebound: 1 submit_date: Nov 20, 2016 @ 09:00:00.000 team: GoldenStatesWarriors _id: 4 _index: basketball _score: - _type: _doc

> Nov 10, 2016 @ 09:00:00.000 assist: 2 blocks: 6 name: RudyGobert points: 12 rebound: 9 submit_date: Nov 10, 2016 @ 09:00:00.000 team: UtahJazz _id: 10 _index: basketball _score: - _type: _doc

> Nov 10, 2016 @ 09:00:00.000 assist: 12 blocks: 3 name: JohnWall points: 13 rebound: 2 submit_date: Nov 10, 2016 @ 09:00:00.000 team: WashingtonWizards _id: 14 _index: basketball _score: - _type: _doc

> Oct 18, 2016 @ 09:00:00.000 assist: 3 blocks: 6 name: RudyGobert points: 8 rebound: 10 submit_date: Oct 18, 2016 @ 09:00:00.000 team: UtahJazz _id: 9 _index: basketball _score: - _type: _doc

> Oct 18, 2016 @ 09:00:00.000 assist: 13 blocks: 2 name: JohnWall points: 8 rebound: 1 submit_date: Oct 18, 2016 @ 09:00:00.000 team: WashingtonWizards _id: 13 _index: basketball _score: - _type: _doc

name: Stephen* 으로 검색을 합니다.

Discover - Elastic

▲ 주의 요함 | 34.64.152.106:8500/app/discover#/?_a=(columns:!(),filters:!(),index:'585f8e80-09c8-11ed-83bb-5d5fb1e3defd',interval:auto,query:(language:kuery,query:'name%20%20Stephen*'),so...)

elastic

Search Elastic

Discover

name : Stephen*

+ Add filter

basketball*

6 hits

Oct 1, 2016 @ 22:58:39.298 - Nov 30, 2016 @ 23:13:31.648

Time Document

Time	Document
> Nov 28, 2016 @ 09:00:00.000	name: StephenCurry assist: 4 blocks: 1 points: 32 rebound: 1 submit_date: Nov 28, 2016 @ 09:00:00.000 team: GoldenStatesWarriors _id: 6 _index: basketball _score: - _type: _doc
> Nov 25, 2016 @ 09:00:00.000	name: StephenCurry assist: 2 blocks: 1 points: 36 rebound: 1 submit_date: Nov 25, 2016 @ 09:00:00.000 team: GoldenStatesWarriors _id: 5 _index: basketball _score: - _type: _doc
> Nov 20, 2016 @ 09:00:00.000	name: StephenCurry assist: 2 blocks: 1 points: 36 rebound: 1 submit_date: Nov 20, 2016 @ 09:00:00.000 team: GoldenStatesWarriors _id: 4 _index: basketball _score: - _type: _doc
> Oct 17, 2016 @ 09:00:00.000	name: StephenCurry assist: 3 blocks: 1 points: 28 rebound: 2 submit_date: Oct 17, 2016 @ 09:00:00.000 team: GoldenStatesWarriors _id: 3 _index: basketball _score: - _type: _doc
> Oct 13, 2016 @ 09:00:00.000	name: StephenCurry assist: 8 blocks: 5 points: 32 rebound: 5 submit_date: Oct 13, 2016 @ 09:00:00.000 team: GoldenStatesWarriors _id: 2 _index: basketball _score: - _type: _doc
> Oct 11, 2016 @ 09:00:00.000	name: StephenCurry assists: 4 blocks: 5 points: 30 rebounds: 3 submit_date: Oct 11, 2016 @ 09:00:00.000 team: GoldenStatesWarriors _id: 1 _index: basketball _score: - _type: _doc

Available fields

- _id
- _index
- _score
- _type
- assist
- assists
- blocks
- name
- points
- rebound
- rebounds
- submit_date
- team

Chart options

Kibana Visualize

Visualize Library로 이동

The screenshot shows the Elastic Visualize Library interface. At the top, there is a navigation bar with tabs for VM Instances, Compute Engine, Home - Elastic, and Visualize Library - Elastic. Below the navigation bar is a search bar labeled "Search Elastic". On the left side, there is a sidebar with a menu icon and a "D" icon. The main content area displays a "Create your first visualization" guide with a house icon, the text "Create your first visualization", and the sub-instruction "You can create different visualizations based on your data." At the bottom of the main content area is a blue button labeled "+ Create new visualization". The sidebar contains sections for Analytics, Enterprise Search, Observability, and Security, each with its own set of sub-options. A red box highlights the "Visualize Library" link under the Analytics section, and another red box highlights the "+ Create new visualization" button.

보안 안 됨 — 34.64.177.87

VM 인스턴스 – Compute Engine – My First Projec... https://ssh.cloud.google.com/v2/ssh/projects/st... https://ssh.cloud.google.com/v2/ssh/projects/st... https://ssh.cloud.google.com/v2/ssh/projects/st... Home - Elastic Visualize Library - Elastic

elastic

Search Elastic

☰ D Visualize Library

Home

Analytics

- Overview
- Discover
- Dashboard
- Canvas
- Maps
- Machine Learning
- Visualize Library**

Enterprise Search

- Overview
- App Search
- Workplace Search

Observability

- Overview
- Alerts
- Cases
- Logs
- Metrics
- APM
- Uptime
- User Experience

+ Add integrations

Create your first visualization

You can create different visualizations based on your data.

+ Create new visualization

Lens 선택

The screenshot shows the 'Visualize Library - Elastic' interface. A modal window titled 'New visualization' is open, displaying four visualization options: 'Lens', 'TSVB', 'Aggregation based', and 'Maps'. The 'Lens' option is highlighted with a red border. Below the modal, there's a section for 'Tools' with 'Text' and 'Controls' options.

New visualization

- Lens**
Create visualizations with our drag and drop editor. Switch between visualization types at any time. *Recommended for most users.*
- TSVB**
Perform advanced analysis of your time series data.
- Aggregation based**
Use our classic visualize library to create charts based on aggregations.
[Explore options →](#)
- Maps**
Create and style maps with multiple layers and indices.

Tools

- Text** Add text and images to your dashboard.
- Controls** Add dropdown menus and range sliders to your dashboard.

Want to learn more? [Read documentation ↗](#)

Basketball 선택

Lens - Elastic

▲ 주의 요함 | 34.64.152.106:8500/app/lens#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))

elastic

Search Elastic

Visualize Library Create

Inspect Download as CSV Save

Search KQL Oct 1, 2016 @ 22:58:39.29 → Nov 30, 2016 @ 23:13:31.64 Refresh

+ Add filter

basketball*

Search field names

Filter by type 0

All fields

- # assist
- # assists
- # blocks
- t name
- # points
- # rebound
- # rebounds
- submit_date
- t team

Meta fields

Bar vertical stacked

Horizontal axis

Add or drag-and-drop a field

Vertical axis

Add or drag-and-drop a field

Break down by

Add or drag-and-drop a field

Add layer

Drop some fields here to start



Lens is a new tool for creating visualization

Make requests and give feedback

Vertical Axis를 오른쪽과 같이 세팅

Lens - Elastic

주의 요함 | 34.64.152.106:8500/app/lens#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))

Search Elastic

Visualize Library Create Inspect Download as CSV Save

Search KQL Oct 1, 2016 @ 22:58:39.29 → Nov 30, 2016 @ 23:13:31.64 Refresh

+ Add filter

basketball*

Search field names

Filter by type 0

All fields

- # assist
- # assists
- # blocks
- t name
- # points
- # rebound
- # rebounds
- submit_date
- t team

Meta fields

Bar vertical stacked

Average of points

Vertical axis

Quick functions Formula

Select a function

- Average (highlighted)
- Median
- Count
- Minimum
- Counter rate
- Moving average
- Cumulative sum
- Percentile
- Differences
- Sum
- Last value
- Unique count
- Maximum

Select a field

points (highlighted)

Add advanced options

Display name Average of points

Value format Default

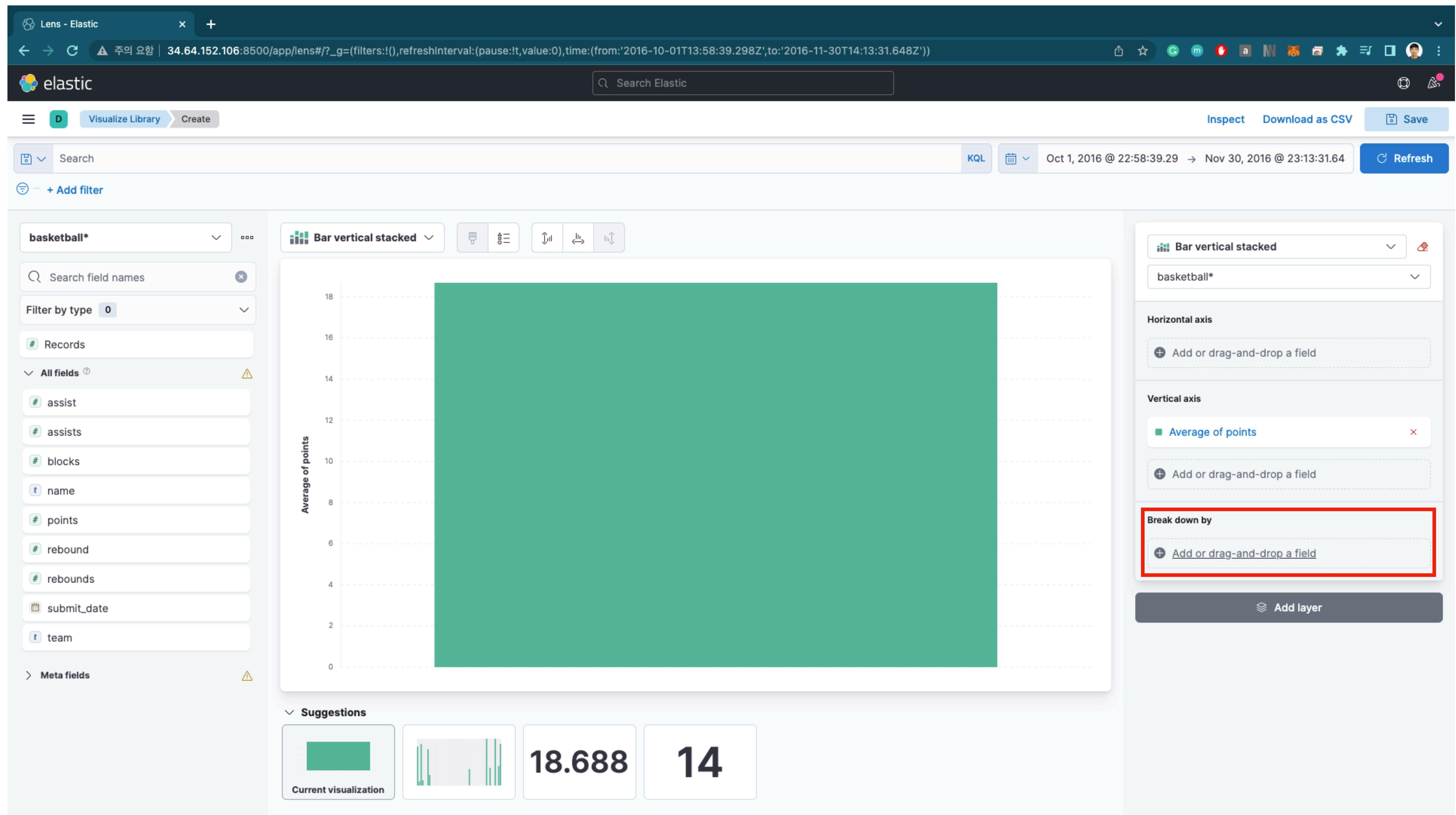
Series color #54B399

Axis side Auto (highlighted) Left Right

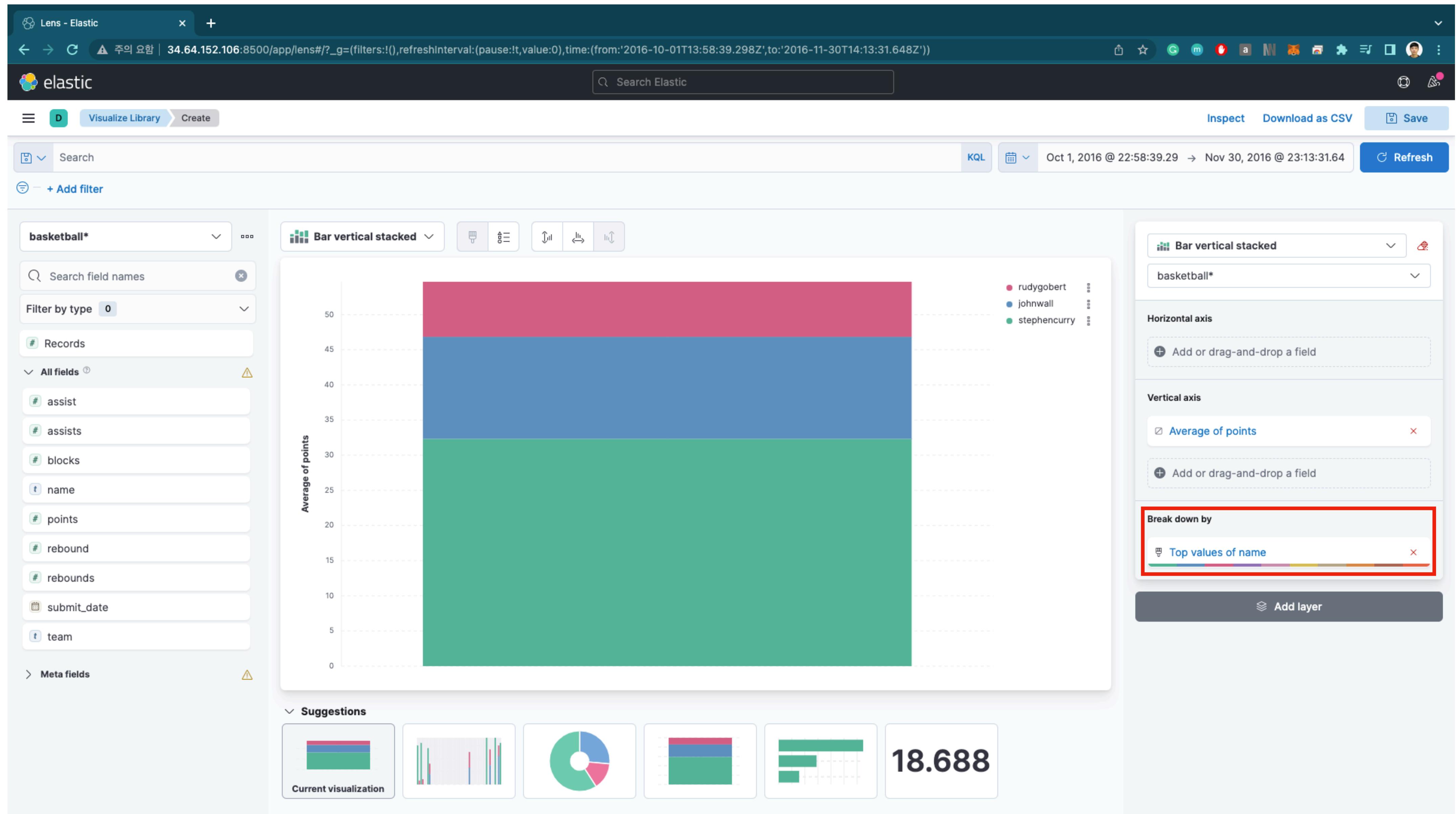
Suggestions

- Current visualization
- 18.688
- 14

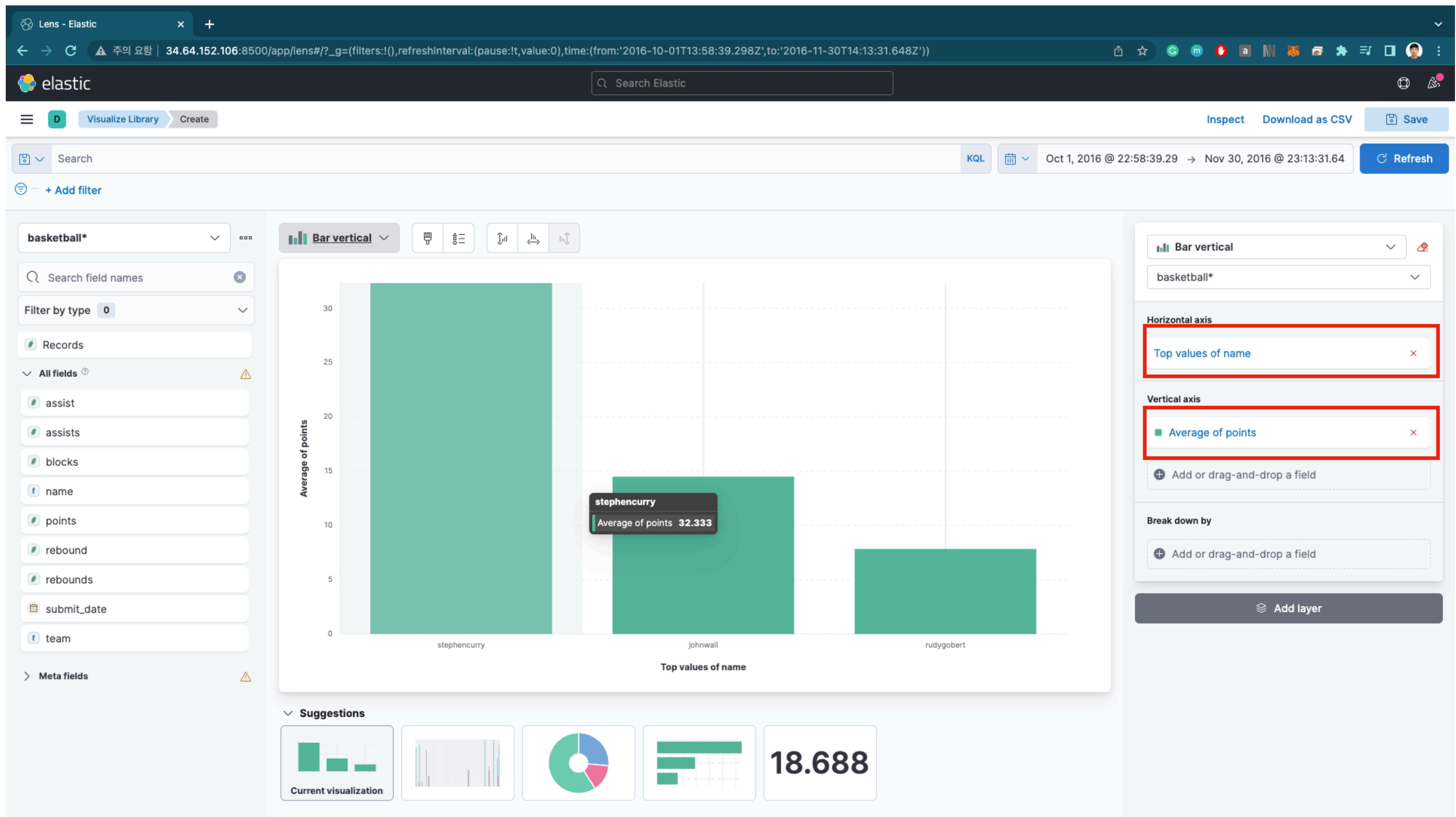
Break down by 세팅



선수별 평균 득점



일반 바차트로 변경



저장

The screenshot shows the Elastic Lens interface with a bar chart visualization for basketball data. A modal dialog box titled "Save Lens visualization" is open in the center. The dialog has the following fields:

- Title:** Bar Chart (highlighted with a red box)
- Add to dashboard:**
 - Existing
 - New (highlighted with a red box)
 - None
- Add to library
- Cancel**
- Save and go to Dashboard** (highlighted with a red box)

Below the dialog, the main interface shows a bar chart with the following data:

Name	Average of points
stephencurry	~30
johnwall	~7
rudygobert	~7

The interface also includes a search bar, filter panels for "basketball*", "Search field names", and "Filter by type", and a "Suggestions" section with various visualization options.

차트들을 한번에 보기 위한 대시보드 생성

New Dashboard - Elastic +

▲ 주의 요함 | 34.64.152.106:8500/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))

elastic

Search Elastic

Dashboard Editing New Dashboard

Unsaved changes Options Share Switch to view mode Save

Search KQL Oct 1, 2016 @ 22:58:39.29 → Nov 30, 2016 @ 23:13:31.64 Refresh

+ Add filter

Create visualization

All types Add from library

Bar Chart

Average of points

Top values of name	Average of points
stephencurry	31
johnwall	14
rudygobert	8

Bar Chart showing the average number of points for three NBA players: Steph Curry (31), John Wall (14), and Rudy Gobert (8).

이번에는 도넛차트 생성

Lens - Elastic

▲ 주의 요함 | 34.64.152.106:8500/app/lens#/?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))

elastic

Search Elastic

Dashboard Create

Inspect Download as CSV Cancel Save to library Save and return

Search KQL Oct 1, 2016 @ 22:58:39.29 → Nov 30, 2016 @ 23:13:31.64 Refresh

+ Add filter

basketball*

Search field names

Filter by type 0

Records

All fields assist assists blocks name points rebound rebounds submit_date team

Bar vertical stacked

Visualization type

- Filter options
- Bar vertical stacked
- Line and area

 - Area
 - Area percentage
 - Area stacked
 - Line

- Proportion

 - Donut
 - Pie
 - Treemap

- Heatmap
- Experimental

Drop some fields here to start

Lens is a new tool for creating visualization

Make requests and give feedback

Horizontal axis

Vertical axis

Break down by

Add layer

Bar vertical stacked

basketball*

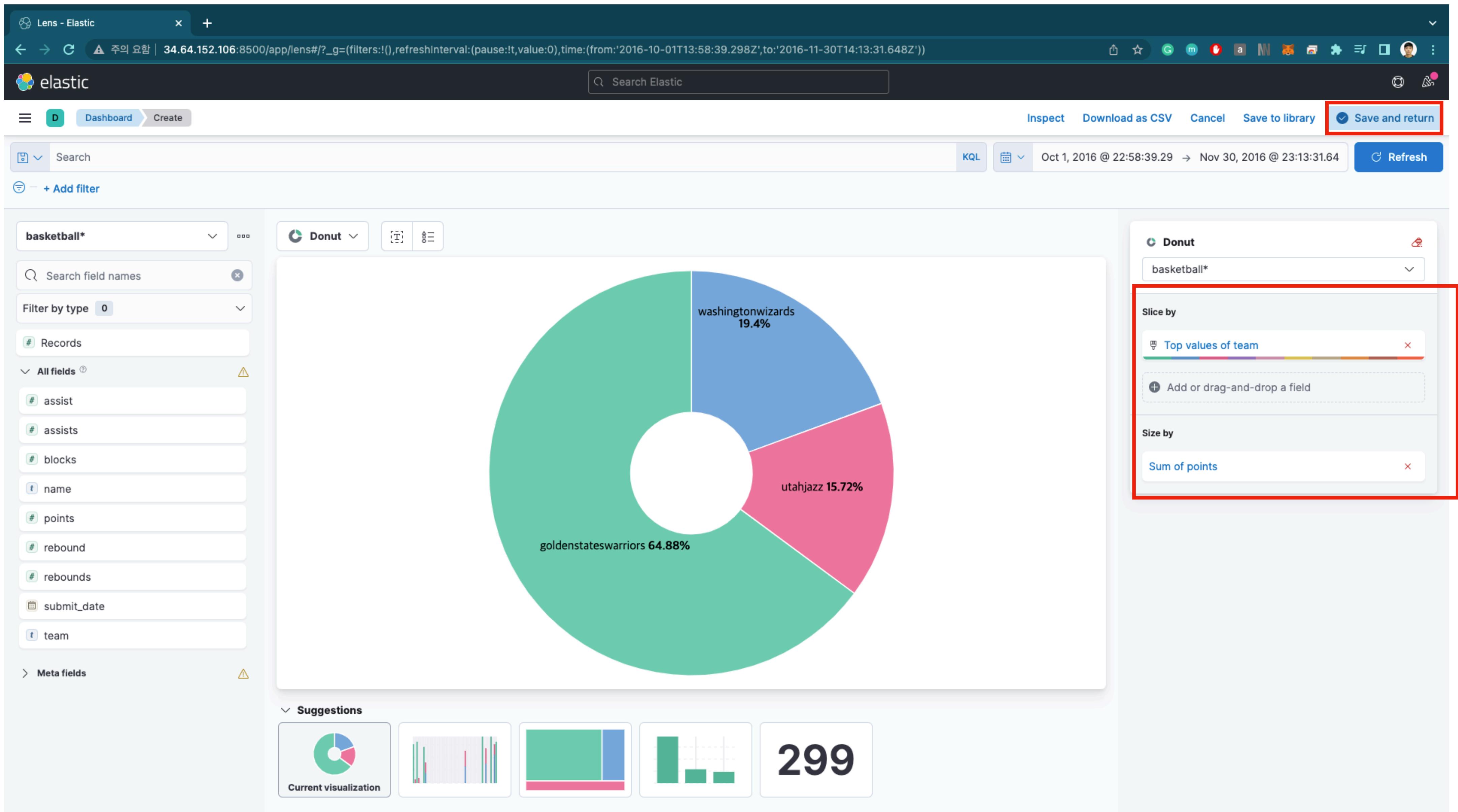
Horizontal axis

Vertical axis

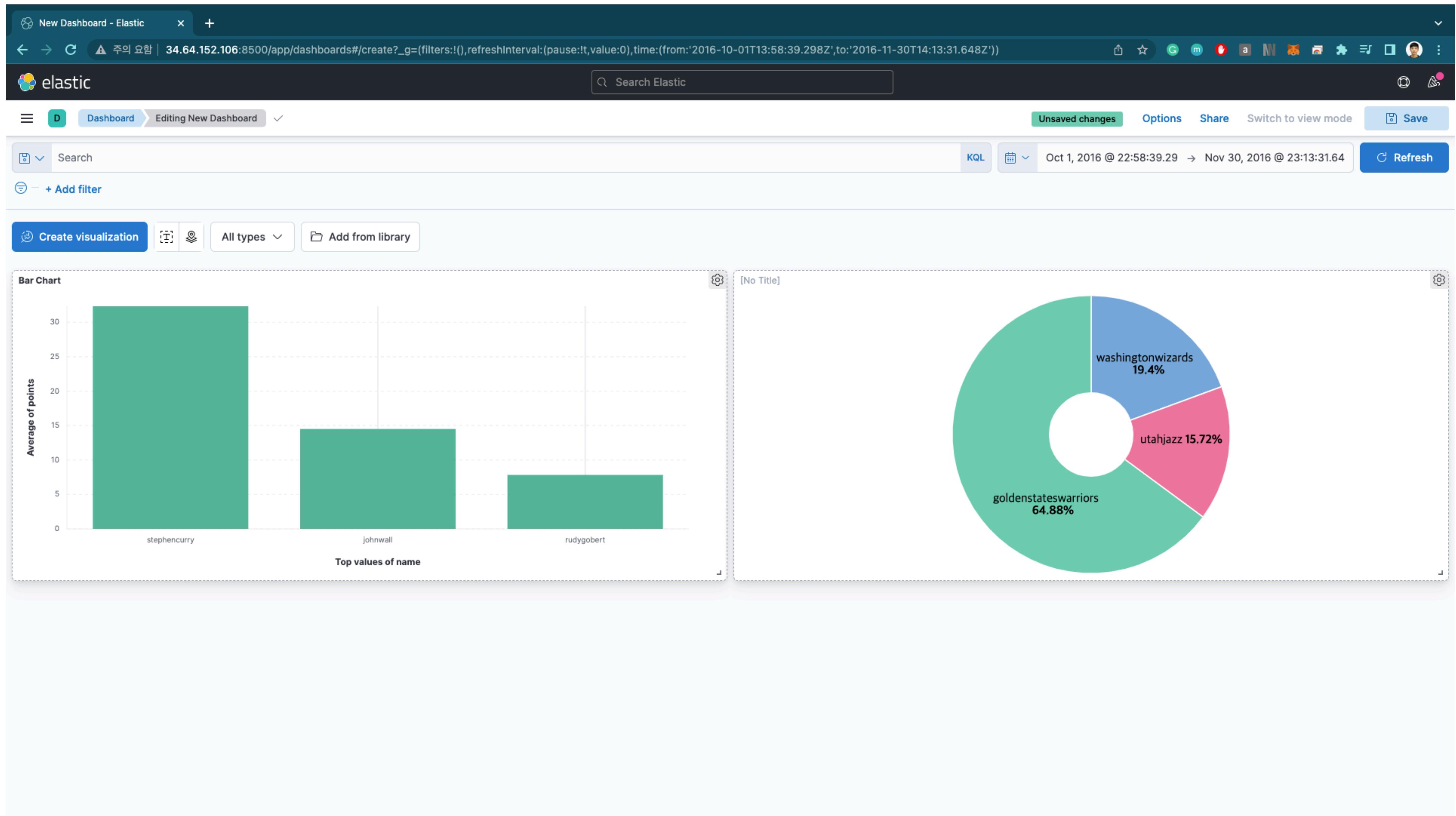
Break down by

Add layer

값을 오른쪽과 같이 구성



대쉬 보드에 도넛 차트도 추가



다른 인덱스도 세팅

New Dashboard - Elastic +

▲ 주의 요함 | 34.64.152.106:8500/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))

elastic

Search Elastic

☰ D Dashboard Editing New Dashboard ✓

Home Overview Alerts Cases Logs Metrics APM Uptime User Experience

All types Add from library

KQL Oct 1, 2016 @ 22:58:39.29 → Nov 30, 2016 @ 23:13:31.64 Refresh

☰ Security Overview Alerts Hosts Network Timelines Cases Endpoints

Top values of name

[No Title]

washingtonwizards 19.4%

utahjazz 15.72%

goldenstateswarriors 64.88%

☰ Management Dev Tools Integrations Fleet Osquery Stack Monitoring Stack Management

Add integrations

34.64.152.106:8500/app/management

The screenshot displays the Elasticsearch dashboard editor interface. On the left, a sidebar menu is open, showing sections such as Home, Security, and Management. Under the Management section, 'Stack Management' is highlighted with a red box. In the main workspace, there are two visualizations: a bar chart titled 'Top values of name' and a donut chart titled '[No Title]'. The bar chart has three bars labeled 'johnwall', 'rudygobert', and another unlabeled bar. The donut chart shows three segments representing percentages: 'goldenstateswarriors' at 64.88% (green), 'washingtonwizards' at 19.4% (blue), and 'utahjazz' at 15.72% (pink). The top navigation bar shows the URL '34.64.152.106:8500/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))' and includes a search bar, a save button, and other dashboard settings.

새로운 인덱스 패턴 세팅

The screenshot shows the Kibana Management interface with the following details:

- Header:** Index patterns - Elastic
- Address Bar:** 주의 요함 | 34.64.152.106:8500/app/management/kibana/indexPatterns
- Search Bar:** Search Elastic
- Left Sidebar (Management):**
 - Ingest: Ingest Pipelines
 - Data: Index Management, Index Lifecycle Policies, Snapshot and Restore, Rollup Jobs, Transforms, Remote Clusters
 - Alerts and Insights: Rules and Connectors, Reporting, Machine Learning Jobs
 - Kibana:
 - Index Patterns** (highlighted with a red box)
 - Saved Objects
 - Tags
 - Search Sessions
 - Spaces
 - Advanced Settings
 - Stack: License Management, Upgrade Assistant
- Main Content Area:**
 - Section Header:** Index patterns
 - Description:** Create and manage the index patterns that help you retrieve your data from Elasticsearch.
 - Search Bar:** Search...
 - Table Headers:** Pattern ↑, basketball*, Default
 - Table Footer:** Rows per page: 10, Page 1 of 1

The screenshot shows the Elasticsearch Kibana Management interface. On the left, there's a sidebar with sections for Management, Ingest, Data, Alerts and Insights, and Kibana. The 'Index Patterns' section under Kibana is currently selected. The main area is titled 'Create index pattern' and contains fields for 'Name' (set to 'classes*') and 'Timestamp field' (set to 'submit_date'). A note below the timestamp field says: 'Select a timestamp field for use with the global time filter.' At the bottom right of the main form is a blue button labeled 'Create index pattern'. To the right of the main form, a sidebar displays the created index pattern 'classes' with an 'Index' tab selected. Above this, a message states 'Your index pattern matches 1 source.' The browser address bar shows the URL '34.64.152.106:8500/app/management/kibana/indexPatterns'.

잘 설정되었네요!

The screenshot shows the Elasticsearch Kibana Management interface. The left sidebar contains navigation links for Management, Ingest, Data, Alerts and Insights, Kibana, Index Patterns, and Stack. The main area is titled "classes*" and displays the field mappings for this index pattern. A note at the top says "Time field: 'submit_date'". Below this, a message states: "View and edit fields in **classes***. Field attributes, such as type and searchability, are based on [field mappings](#) in Elasticsearch." The "Fields (16)" tab is selected, showing a table of fields with columns: Name, Type, Format, Searchable, Aggregatable, and Excluded. The table lists the following fields:

Name	Type	Format	Searchable	Aggregatable	Excluded
Professor	text		●		Edit
Professor.keyword	keyword		●	●	Edit
_id	_id		●	●	Edit
_index	_index		●	●	Edit
_score					Edit
_source	_source				Edit
_type	_type		●	●	Edit
major	text		●		Edit
professor	text		●		Edit
rating	integer		●	●	Edit

At the bottom, there are pagination controls for "Rows per page: 10" and page numbers 1, 2, >.

이번에는 지도 세팅

Elastic

▲ 주의 요함 | 34.64.152.106:8500/app/maps/map#?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))&_a=(filters:!(),query:(lang...)

elastic

Search Elastic

Maps Create

Map settings Inspect Full screen Save

Home

Analytics Overview Discover Dashboard Canvas Maps Machine Learning Visualize Library

Enterprise Search Overview App Search Workplace Search

Observability Overview Alerts Cases Logs Metrics APM Uptime User Experience

Add integrations

34.64.152.106:8500/app/maps

KQL Oct 1, 2016 @ 22:58:39.29 → Nov 30, 2016 @ 23:13:31.64 Refresh

LAYERS Road map Add layer

Southern

Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

Elasticsearch에 저장된 Document 선택

The screenshot shows the Elastic Maps Service interface with a world map centered on Europe and Africa. The map includes labels for countries and major bodies of water. A sidebar on the left contains navigation icons for zooming and panning.

In the top right corner, there is a search bar labeled "Search Elastic" and several status indicators and links. Below the search bar, the "Maps" tab is selected, followed by "Create".

A "LAYER" panel is open, showing a "Road map" layer. To the right of the map, a modal dialog titled "Add layer" is displayed. This dialog has a tab bar with "All" (selected), "Elasticsearch" (highlighted with a red box), "Reference", and "Solutions".

The "Elasticsearch" tab is currently active, showing a list of available layers:

- Documents** (highlighted with a red box): Points, lines, and polygons from Elasticsearch.
- Clusters and grids**: Geospatial data grouped in grids with metrics for each gridded cell.
- Top hits per entity**: Display the most relevant documents per entity, e.g. the most recent GPS hits per vehicle.

On the far right, there are two more options: "Choropleth" and "Heat map".

At the bottom of the dialog, there are "Cancel" and "BETA" buttons.

classes 선택

Elastic

주의 요함 | 34.64.152.106:8500/app/maps/map#?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))&_a=(filters:!(),query:(lang...)

elastic

Search Elastic

Maps Create

Map settings Inspect Full screen Save

Search KQL Oct 1, 2016 @ 22:58:39.29 → Nov 30, 2016 @ 23:13:31.64 Refresh

+ Add filter

LAYERS

- classes*
- Road map

Add layer

Add layer

Index pattern classes*

Geospatial field school_location

Scaling

- Limit results to 10,000
- Show clusters when results exceed 10,000
- Use vector tiles

Cancel Add layer →

The screenshot shows a world map with country boundaries. Several countries are highlighted with green dots, indicating they have been selected or are part of a cluster. The 'Add layer' modal is open, prompting the user to choose an index pattern ('classes*') and a geospatial field ('school_location'). The 'school_location' field is highlighted with a red box. At the bottom right of the modal, there is another red box around the 'Add layer →' button.

지도에서 데이터 확인

Elastic

주의 요함 | 34.64.152.106:8500/app/maps/map#?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))&_a=(filters:!(),query:(lang...)

elastic

Search Elastic

Maps Create

Map settings Inspect Full screen Save

Search KQL Oct 1, 2016 @ 22:58:39.29 → Nov 30, 2016 @ 23:13:31.64 Refresh

+ Add filter

classes*

Professor JenifferAnderson
school_location 39.96999999973923, -89.78000001981854

1 of 3

LAYERS

classes* Road map

Add layer

IN

classes*

> Source details

Layer settings

Name
Visibility Zoom levels 0 → 24
Opacity 75%
Attribution + Add attribution
Include layer in fit to data bounds computation

Tooltip fields

Professor
school_location

Sorting

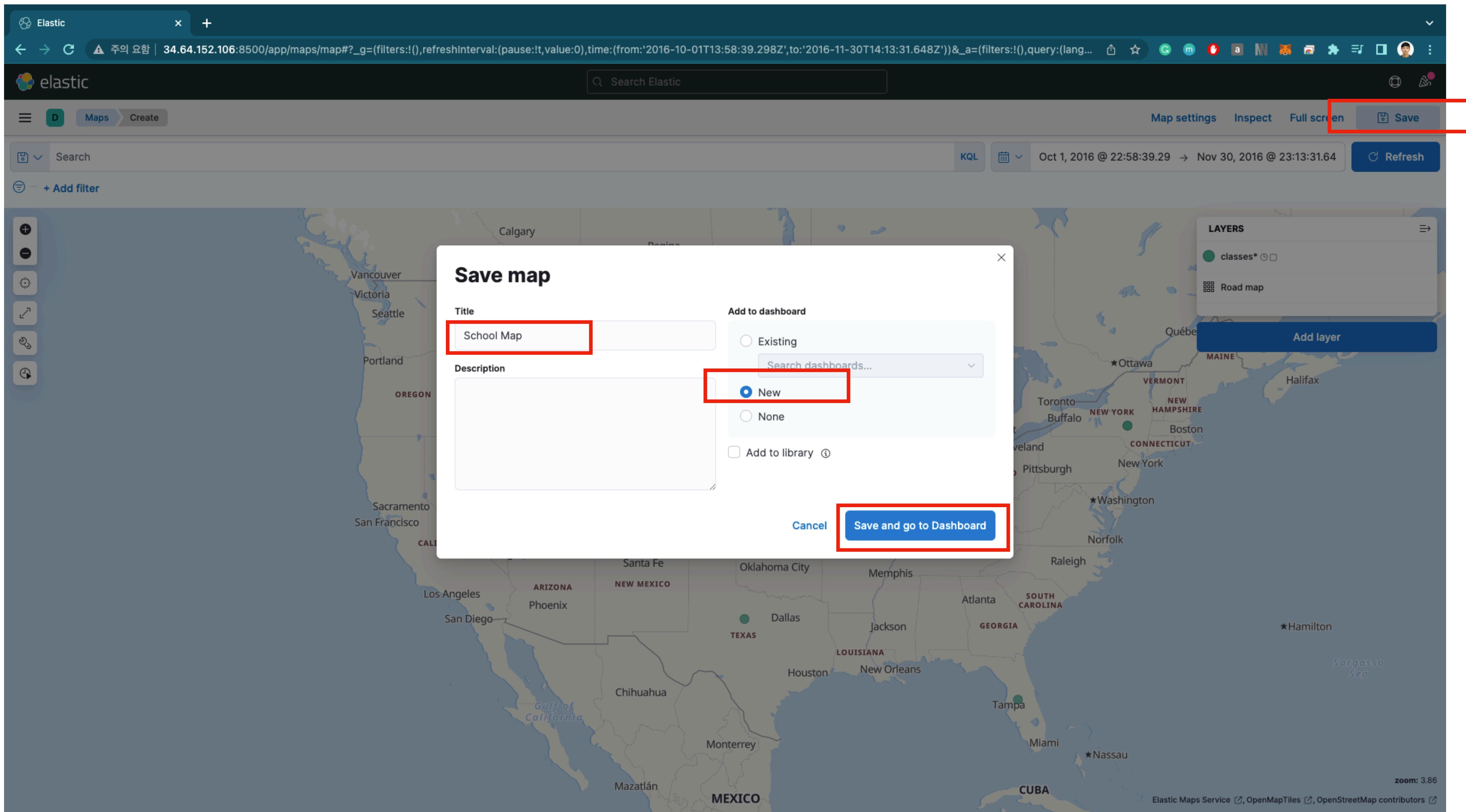
Field Select sort field
Order descending

Scaling

Cancel Remove layer Save & close

The screenshot shows the Elastic Maps interface. A tooltip is open over a point on the map, displaying 'classes*' with 'Professor' and 'JenifferAnderson' under it, and 'school_location' with coordinates '39.96999999973923, -89.78000001981854'. The tooltip also indicates '1 of 3'. To the right, a sidebar titled 'classes*' shows 'Layer settings' for 'classes*', including fields for Name, Visibility (Zoom levels 0 to 24), Opacity (75%), Attribution, and a toggle for 'Include layer in fit to data bounds computation'. A red box highlights the 'Tooltip fields' section, which lists 'Professor' and 'school_location'. Another red box highlights the 'Save & close' button at the bottom right of the sidebar.

지도도 대쉬보드에 저장



New Dashboard - Elastic +

▲ 주의 요함 | 34.64.152.106:8500/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2016-10-01T13:58:39.298Z',to:'2016-11-30T14:13:31.648Z'))

elastic

Search Elastic

Dashboard Editing New Dashboard

Unsaved changes Options Share Switch to view mode Save

Search KQL Oct 1, 2016 @ 22:58:39.29 → Nov 30, 2016 @ 23:13:31.64 Refresh

+ Add filter

Create visualization

All types Add from library

Bar Chart

Average of points

Top values of name	Average of points
stephencurry	30
johnwall	14
rudygobert	8

School Map

REGION

Boise IDAHO WYOMING

CALIFORNIA NEVADA UTAH COLORADO KANSAS TEXAS OREGON

Las Vegas Salt Lake City Cheyenne Denver

Minneapolis

LAYERS

- classes*
- Road map

PIERRE DENVER CINCINNATI SAINT LOUIS MEMPHIS NASHVILLE RALEIGH

[No Title]

washingtonwizards 19.4%

utahjazz 15.72%

goldenstateswarriors 64.88%

The screenshot shows a dashboard titled 'New Dashboard - Elastic' with three main visualizations:

- Bar Chart:** A chart showing the average of points for three names: stephencurry (30), johnwall (14), and rudygobert (8). The Y-axis ranges from 0 to 30.
- Pie Chart:** A donut chart titled '[No Title]' showing the distribution of something across three categories: goldenstateswarriors (64.88%), washingtonwizards (19.4%), and utahjazz (15.72%).
- School Map:** A map of the United States with various states labeled. It includes a legend for 'classes*' and 'Road map'. The map also shows major cities like Boise, Salt Lake City, Denver, and Minneapolis.

The 'Create visualization' button is highlighted with a red box in the top-left corner of the dashboard area.

이번에는 테이블 형태의 시각화 추가

The screenshot shows the Elastic Lens interface for creating a new visualization. The main area displays a table titled "Top values of Professor.keyword" with the metric "Sum of student_count". The table lists several names with their corresponding counts:

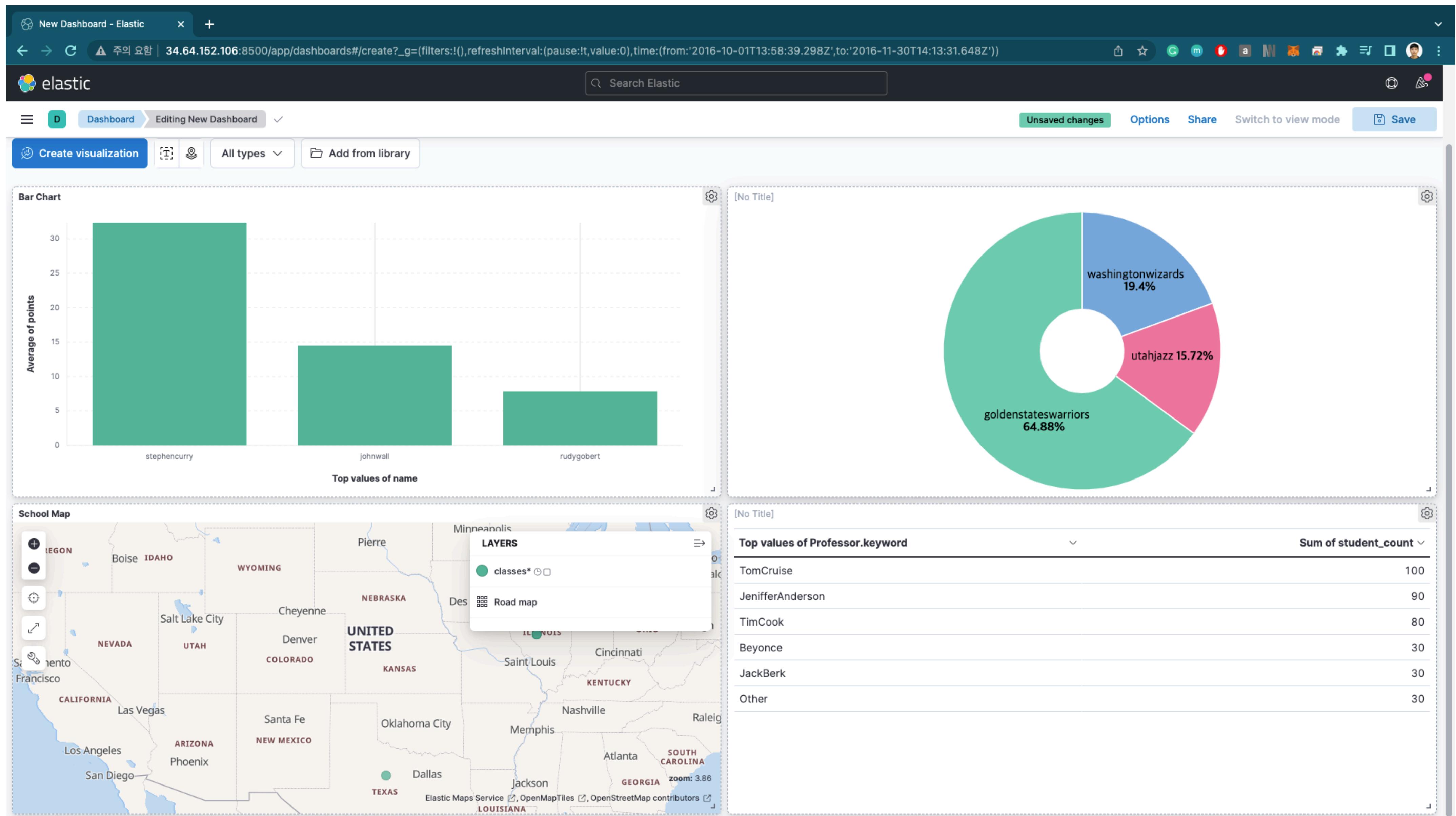
Professor.keyword	Sum of student_count
TomCruise	100
JenifferAnderson	90
TimCook	80
Beyonce	30
JackBerk	30
Other	30

The visualization configuration panel on the right side of the screen is highlighted with a red box. It includes sections for "Rows", "Columns", and "Metrics", each with a placeholder field labeled "Add or drag-and-drop a field".

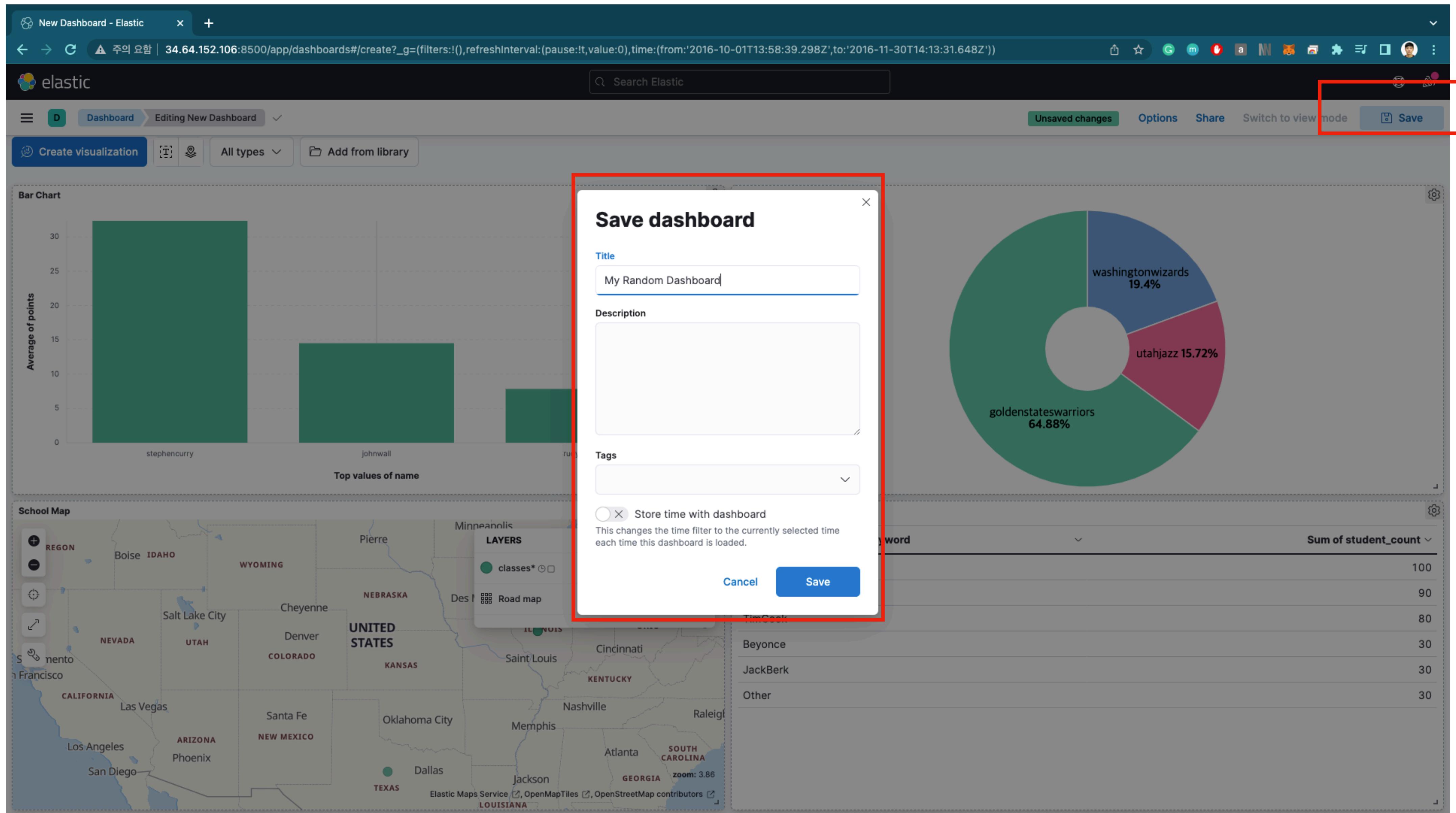
At the top right of the main interface, there is a "Save and return" button also highlighted with a red box.

On the left sidebar, under "All fields", the "Professor.keyword" field is selected and highlighted with a red box. The "Table" icon in the top navigation bar is also highlighted with a red box.

At the bottom, there is a "Suggestions" section with various visualization icons and a large "360" number.



대쉬보드 저장!



짜잔!

The screenshot shows the 'Dashboards' page of the Elastic Stack interface. At the top, there's a header bar with the title 'Dashboards - Elastic', a search bar labeled 'Search Elastic', and various browser icons. Below the header is a navigation bar with a menu icon, a 'Dashboard' tab (which is selected and highlighted in green), and other tabs like 'Discover' and 'Visualize'. The main content area has a title 'Dashboards' and a 'Create dashboard' button. There's a search bar and a 'Tags' dropdown. A table lists one dashboard entry:

Title	Description	Tags	Actions
<input type="checkbox"/> My Random Dashboard			

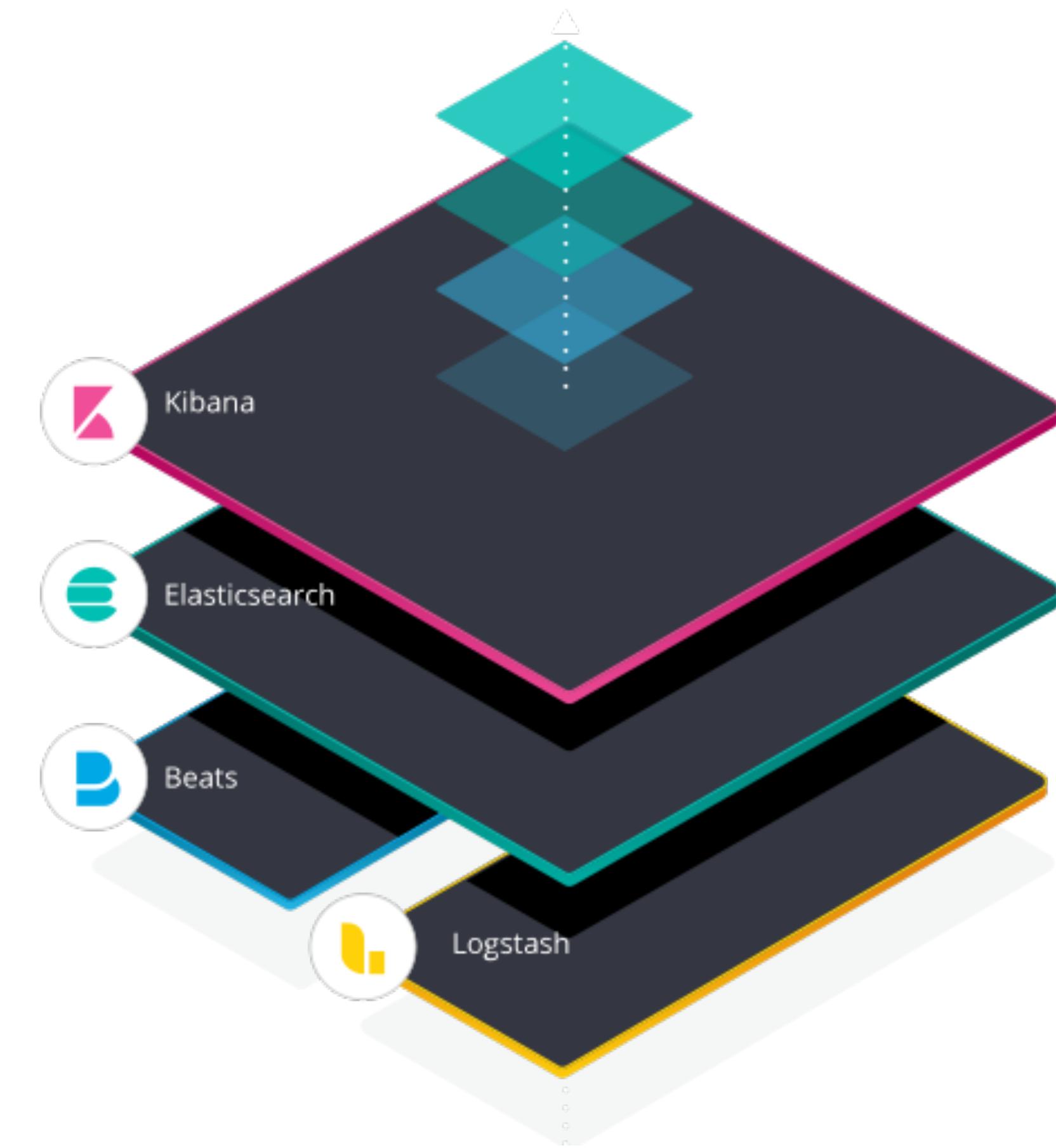
At the bottom, there are pagination controls for 'Rows per page' (set to 20) and a page number indicator '1'.

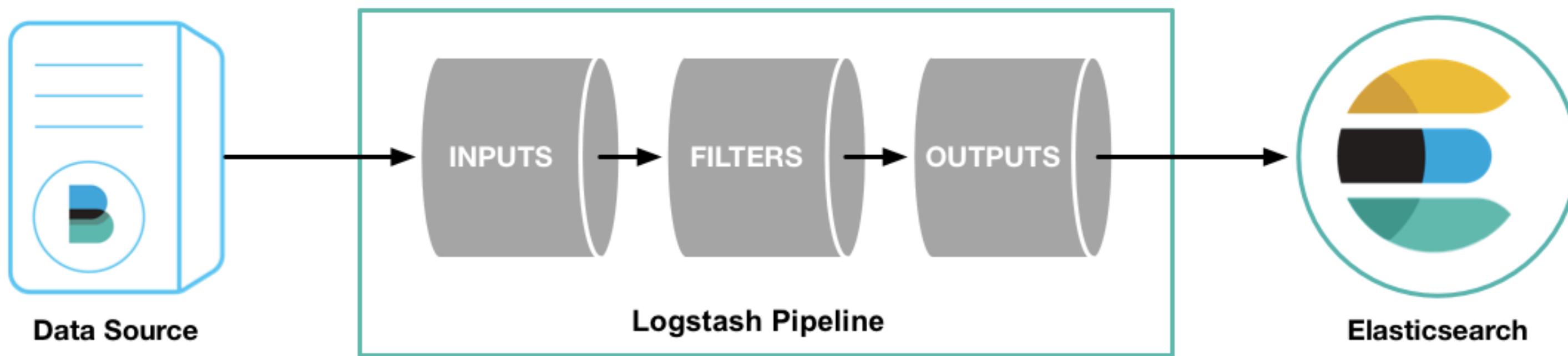
LOGSTASH

ELK Stack

Elasticsearch, Logstash, Kibana

- Elasticsearch
 - 검색 및 분석 엔진
- Logstash
 - 데이터 처리 파이프라인
 - 여러 소스에서 동시에 데이터를 수집 및 변환
- Kibana
 - 차트와 그래프를 이용해 데이터 시각화
- Beat
 - 파일 추적
 - Beat가 추가됨으로써 ELK Stack에서 Elastic Stack으로!





Covid 인덱스 추가

The screenshot shows the Elastic Stack Management interface. On the left, a sidebar titled "Management" lists various sections: Ingest, Data, Alerts and Insights, Kibana, and Stack. The "Index Patterns" section under Kibana is highlighted with a red box. The main content area is titled "Create index pattern". The "Name" field contains "covid*" and the "Timestamp field" dropdown is set to "@timestamp". A success message at the top right states "Your index pattern matches 1 source." and shows the index "covid_index". The bottom right features a blue "Create index pattern" button.

보안 안 됨 — 34.64.177.87

VM 인스턴스 – Compute Engine – My First Project... https://ssh.cloud.google.com/v2/ssh/projects/st... https://ssh.cloud.google.com/v2/ssh/projects/st... https://ssh.cloud.google.com/v2/ssh/projects/st... Home - Elastic Index patterns - Elastic

elasticsearch

Stack Management Index patterns

Management

Ingest ⓘ

Ingest Pipelines

Data ⓘ

Index Management

Index Lifecycle Policies

Snapshot and Restore

Rollup Jobs

Transforms

Remote Clusters

Alerts and Insights ⓘ

Rules and Connectors

Reporting

Machine Learning Jobs

Kibana ⓘ

Index Patterns

Saved Objects

Tags

Search Sessions

Spaces

Advanced Settings

Stack ⓘ

License Management

Upgrade Assistant

Index patterns

Create index pattern

covid*

@timestamp

Your index pattern matches 1 source.

covid_index

Index

Rows per page: 10

x Close

필드 확인

The screenshot shows the Elasticsearch Stack Management interface with the URL <https://ssh.cloud.google.com/v2/ssh/projects/st...>. The main page displays the 'Management' section for the 'covid*' index pattern. A sidebar on the left lists various management sections like Ingest, Data, Alerts and Insights, Kibana, Index Patterns, and Stack.

The central area is titled 'covid*' and contains a note: 'Time field: '@timestamp''. It says, 'View and edit fields in covid*. Field attributes, such as type and searchability, are based on [field mappings](#) in Elasticsearch.' Below this, there are tabs for 'Fields (21)', 'Scripted fields (0)', and 'Field filters (0)'. A search bar and a dropdown for 'All field types' are also present.

A table lists the 21 fields:

Name ↑	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		●	●	
@version	text		●		
@version.keyword	keyword		●	●	
_id	_id		●	●	
_index	_index		●	●	
_score					
_source	_source				
_type	_type		●	●	
addr	text		●	●	
city	text		●	●	

At the bottom right, a message box says '✓ Saved 'covid*''.

지도로 다시 이동

The screenshot shows the Elastic Maps Service interface. At the top, there is a header bar with tabs for "VM 인스턴스 – Compute Engine – My First Projec...", "https://ssh.cloud.google.com/v2/ssh/projects/st...", "https://ssh.cloud.google.com/v2/ssh/projects/st...", "Home - Elastic", and "Elastic". Below the header is a search bar labeled "Search Elastic". The main area features a world map with country boundaries and labels. On the left side of the map, there are zoom controls (+, -, location). Above the map, there is a toolbar with "Map settings", "Inspect", "Full screen", and "Save" buttons. To the right of the map, there is a "LAYER" panel with a single item "Road map". A red box highlights the "Add layer" button in this panel. The bottom right corner of the map area displays the coordinates "lat: 54.53546, lon: 34.34849, zoom: 1.64" and the footer text "Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors".

Covid 인덱스로 추가

The screenshot shows the Elastic Maps interface with a world map. A green dot representing the 'covid*' index pattern is visible over South Korea. A floating 'LAYER' panel shows the current layers: 'covid*' and 'Road map'. A modal window titled 'Add layer' is open, containing the following configuration:

- Index pattern:** covid*
- Geospatial field:** location
- Scaling:**
 - Limit results to 10,000
 - Show clusters when results exceed 10,000
 - Use vector tiles

At the bottom right of the 'Add layer' dialog is a large blue 'Add layer →' button.

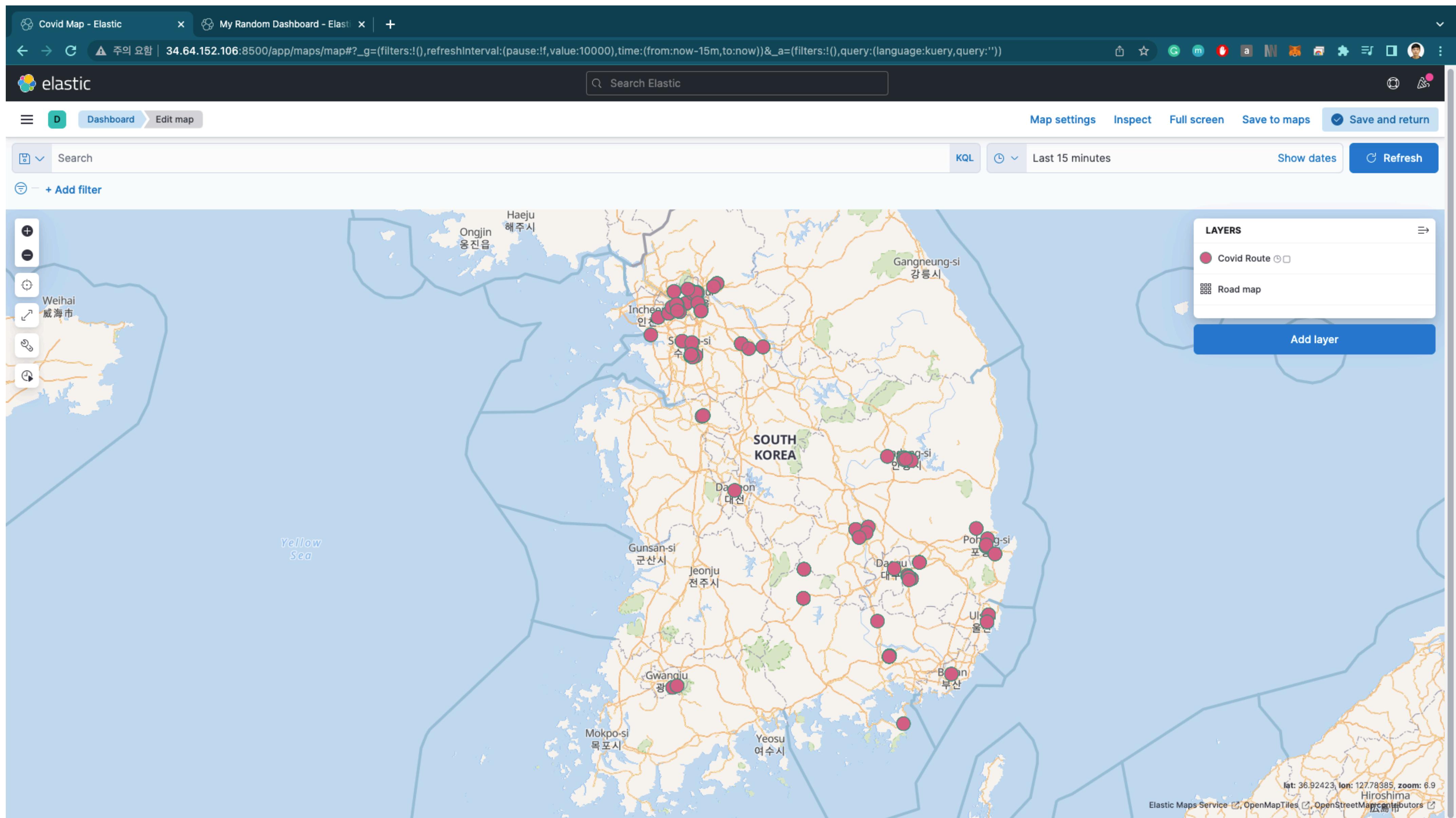
Refresh Every 10 seconds

The screenshot shows the Elastic Maps interface with a world map. A green dot representing the 'covid*' layer is visible over South Korea. On the right side, there is a sidebar with various controls. Two specific areas are highlighted with red boxes:

- Top right (Calendar icon):** Shows a date range from "Jul 23, 2015 @ 10:01:26.485" to "now". The calendar icon is highlighted.
- Bottom right (Refresh every section):** Shows a dropdown menu set to "10 seconds" with a "Start" button. This section is also highlighted with a red box.

The map itself shows major oceans and continents, with country boundaries and names labeled. A legend on the right indicates the 'covid*' layer and a 'Road map' layer.

감상



대쉬보드에 저장

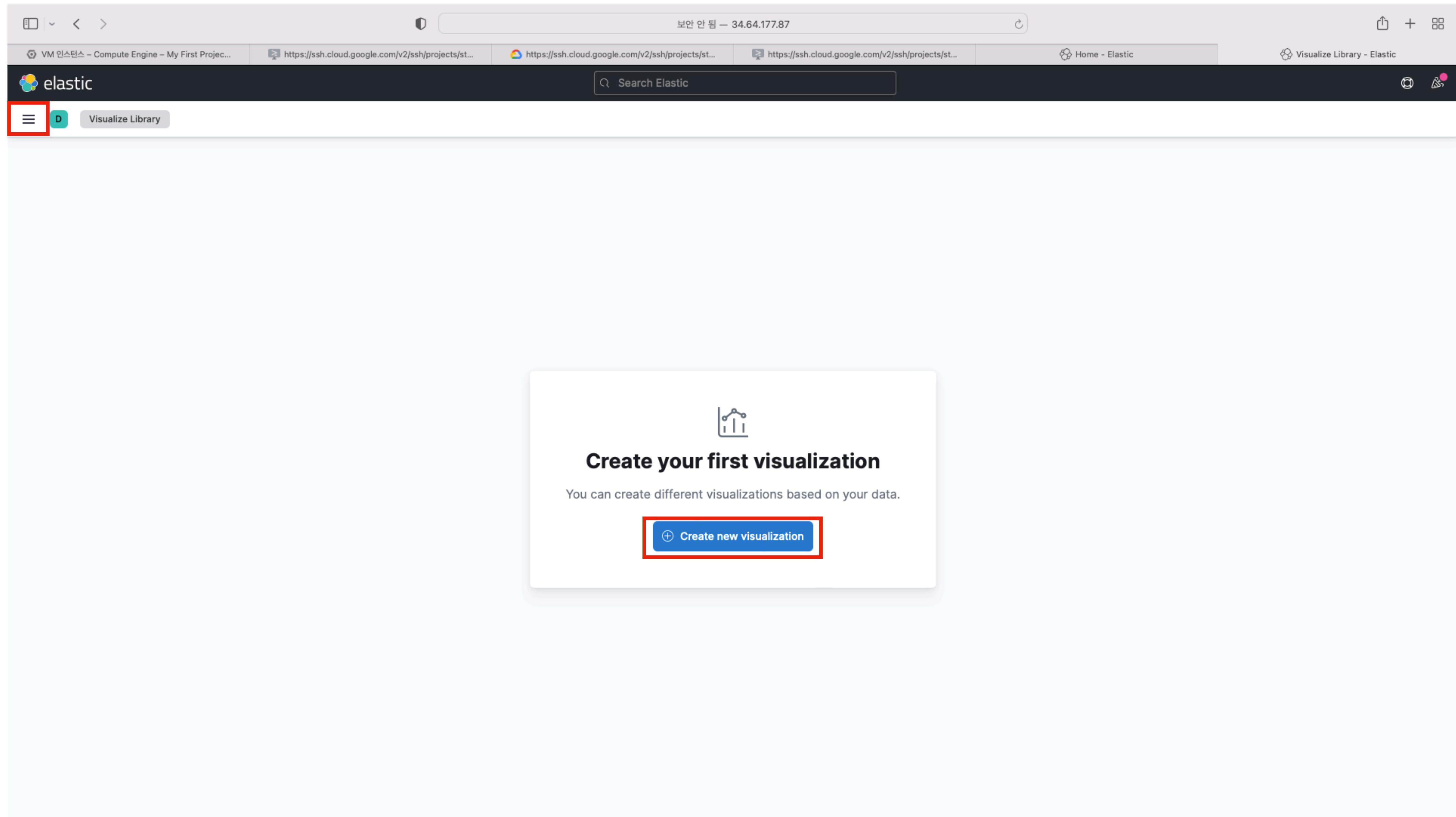
The screenshot shows the Elastic Maps interface with a map of East Asia (China, Korea, Japan) displayed. A modal dialog box titled "Save map" is open in the center. The "Title" field contains "MyCovidMap". The "Add to dashboard" section has "Existing" selected, with a dropdown menu showing "Search dashboards...". There are also "New" and "None" options, and a checkbox for "Add to library". Below the dialog is a "Cancel" button and a "Save and go to Dashboard" button.

On the right side of the interface, there are several panels:

- covid***: A title panel with a link to "Source details".
- Layer settings**: Includes fields for "Name", "Visibility" (Zoom levels 0 to 24), "Opacity" (75%), "Attribution", and a toggle for "Include layer in fit to data bounds computation".
- Tooltip fields**: A section for adding tooltip fields to create filters from field values, with a "+ Add" button.
- Sorting**: Fields for "Field" (Select sort field) and "Order" (descending).
- Scaling**: A zoom control panel with a "zoom: 6.3" indicator.

At the bottom right of the interface, there are "Close", "Remove layer", and "Save & close" buttons.

Visualize Library로 다시 이동



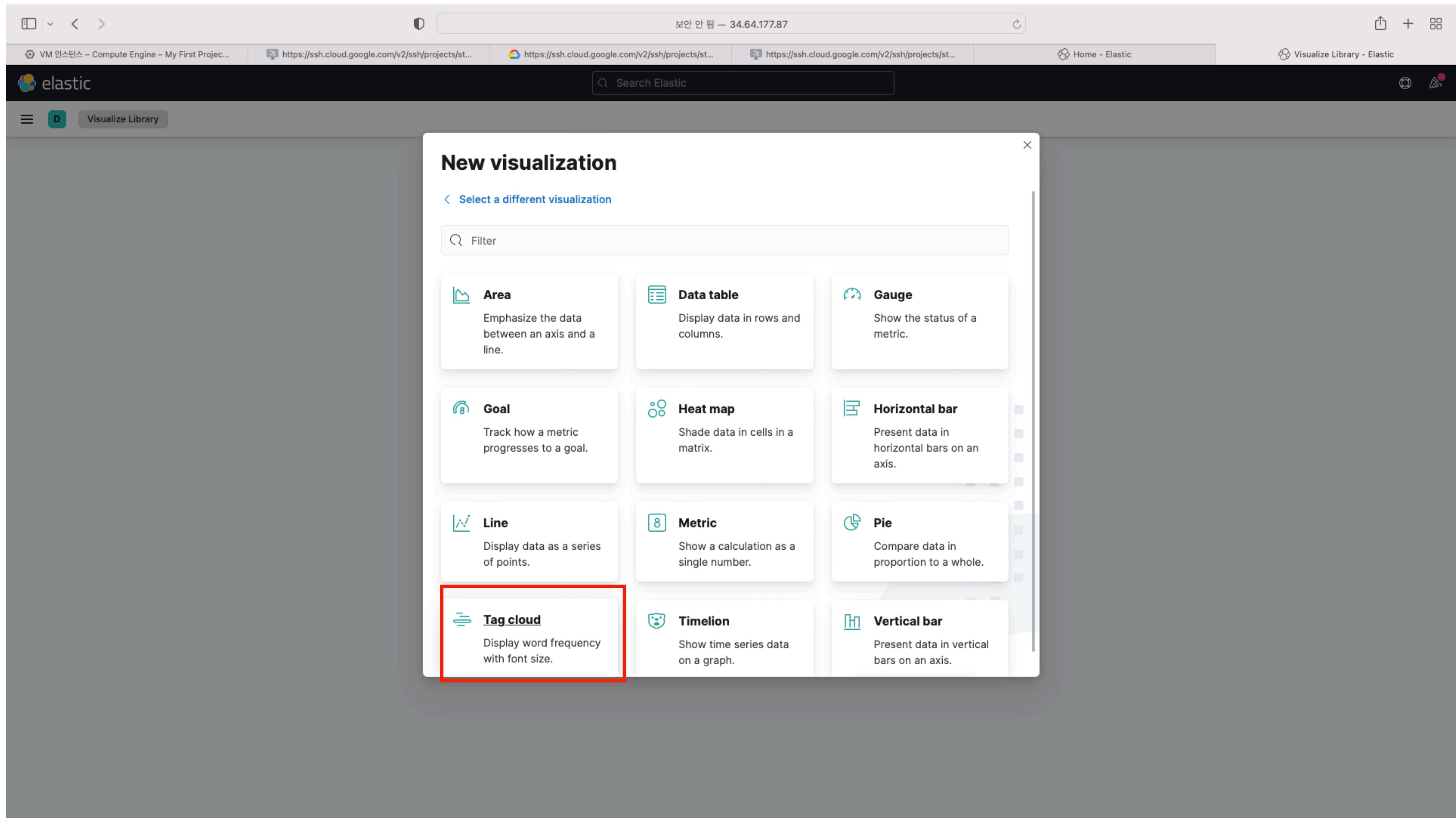
Aggregation based 선택

The screenshot shows a web browser window with multiple tabs open, including 'Home - Elastic' and 'Visualize Library - Elastic'. A modal window titled 'New visualization' is displayed in the foreground. The modal lists several visualization types:

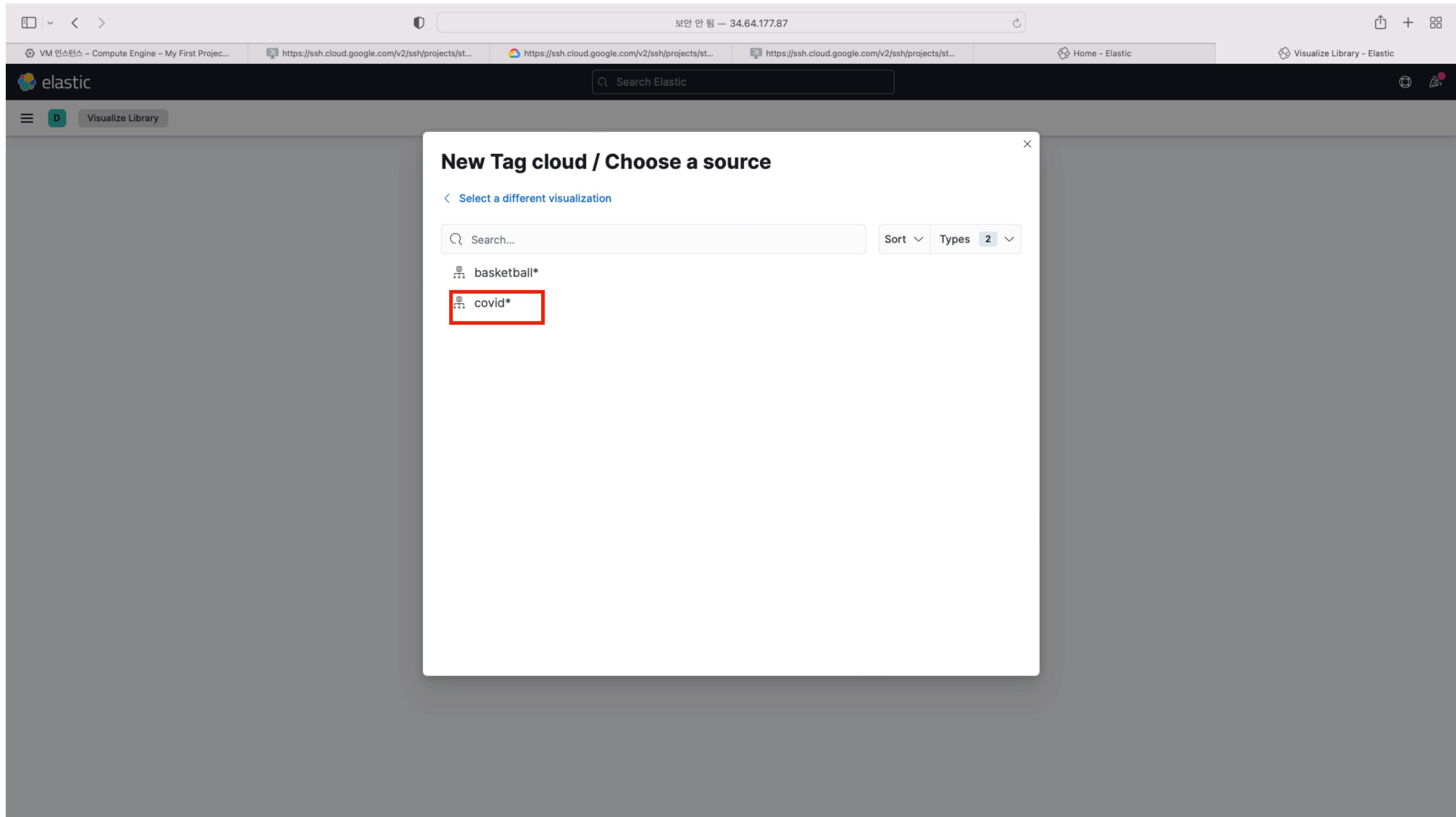
- Lens**: Create visualizations with our drag and drop editor. Switch between visualization types at any time. *Recommended for most users.*
- Maps**: Create and style maps with multiple layers and indices.
- TSVB**: Perform advanced analysis of your time series data.
- Custom visualization**: Use Vega to create new types of visualizations. *Requires knowledge of Vega syntax.*
- Aggregation based**: Use our classic visualize library to create charts based on aggregations. This option is highlighted with a red rectangular box.

Below the list, there's a section titled 'Tools' with two items: 'Text' and 'Controls'. At the bottom of the modal, there are links for 'Want to learn more?' and 'Read documentation'.

Tag cloud 선택



Covid 선택



오른쪽과 같이 옵션설정!

Visualize Library - Elastic

▲ 주의 요함 | 34.64.152.106:8500/app/visualize#/create?type=tagcloud&indexPattern=4ac20430-09d0-11ed-83bb-5d5fb1e3defd&_g=(filters:!(),refreshInterval:(pause:!f,value:10000),time:(from:now...)

elastic

Search Elastic

Inspect Share Save

Search KQL Last 15 minutes Show dates Refresh

+ Add filter

covid_index*

Data Options

Metrics

> Tag size Count

Buckets

Tags

Aggregation Terms help

Terms

Field name

Order by Metric: Count

Order Descending Size 100

Group other values in separate bucket

Show missing values

Custom label

> Advanced

Discard Update

점약국

하양 남촌 고기 양주 김덕성 최 살 산 랑 불 선 대 혐 대 역 하나 당

여의도 수퍼 온누리 총 마스크 상봉 학원 천 포항 보건 착용 혐 대 역

이비인후 GS 방문 4 19 서울 천 포항 선 불

승급 숯 도 호 동 소독 일 방역 보건 착용 혐 대 역

복이 농협 2 병원 의원 점약국 플러스 하나 당

정육 예 코로나 마트 이 1 소 완료 센터 9 CU 마켓 공방

무 육 새 동점 진료 3 소 과 안동 안 무동 가 은행

식 창원 떡 은 남 소선 흘 별 시 연합 제주 로 화

창원 떡 은 남 소선 흘 별 시 연합 제주 로 화

다이소 주민 트튼

성모 성모 밥 시 참 것 실 학교

name: Descending - Count

E.O.D