

Elastic Stack 을 활용한 Data Dashboard 만들기

Week 3 - 데이터를 검색/필터링 해보자



Fast Campus

내용	페이지
Kibana 기타	
Scripted Field	3
Data Format	39
Dashboard	
기본 기능	71
Object Import/Export	91
데이터 검색 및 필터링	
Filter	108
Lucene Query Syntax	126
Discover	153

Scripted Field 

String Concatenation 연산은 안되나?

Field 간 연산은 안되나?

Date Field에서 연/월/일/시/분/초 등 접근 안되나?

기존 Field에 조건을 적용해서 새로운 Field를 만들 수 없나?

String Concatenation 연산은 안되나?



Field 간 연산은 안되나?

Date Field에서 연/월/일/시/분/초 등 접근 안되나?

기존 Field에 조건을 적용해서 새로운 Field를 만들 수 없나?

예시

특정한 두 개 혹은 그 이상의 Field를 합쳐서
하나의 Field를 만들고 싶으면 어떻게 해야할까?

scripted field를 추가하자

The screenshot shows the Kibana Management interface with the following steps highlighted:

- 1. 선택**: A hand icon points to the "Management" button in the sidebar.
- 2. 선택**: A hand icon points to the "Index Patterns" tab in the top navigation bar.
- 3. id_2018.06.17 선택**: A hand icon points to the index pattern "test1_*".
- 4. 선택**: A hand icon points to the "scripted fields (0)" tab.
- 5. 선택**: A hand icon points to the "+ Add Scripted Field" button.

The main content area displays the "test1_*" index pattern details, including a note about time filtering and a section for managing scripted fields.

script를 작성하자

Management / Kibana / Indices / test1_*

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ test1_*

>Create Scripted Field

Name

성별-카드

2. 생성할 Field 이름 입력

Language

painless

Type

string

3. string 선택

Format (Default: String)

string

4. string 선택

Popularity

0

+

-

Script

doc['고객성별'].value + '-' + doc['결제카드'].value

5. 다음과 같이 script 작성

doc['고객성별'].value + '-' + doc['결제카드'].value

Create Field Cancel

6. 선택



The screenshot shows the Kibana Management interface under the 'Indices' section for the 'test1_*' index pattern. A new 'Scripted Field' is being created. The 'Name' is set to '성별-카드'. The 'Type' is selected as 'string'. In the 'Script' field, the expression 'doc['고객성별'].value + '-' + doc['결제카드'].value' is entered. The interface includes numbered steps in pink: 1. 확인 (Check), 2. 입력 (Input), 3. 선택 (Select), 4. 선택 (Select), 5. 작성 (Write), and 6. 선택 (Select).

Discover에 가서 확인하자

95 hits

New Save Open Share Auto-refresh < This month >

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

shopping

Selected Fields

t 결제카드
t 고객성별
t 성별-카드

Available Fields

July 1st 2018, 00:00:00.000 - July 31st 2018, 23:59:59.999 — Auto

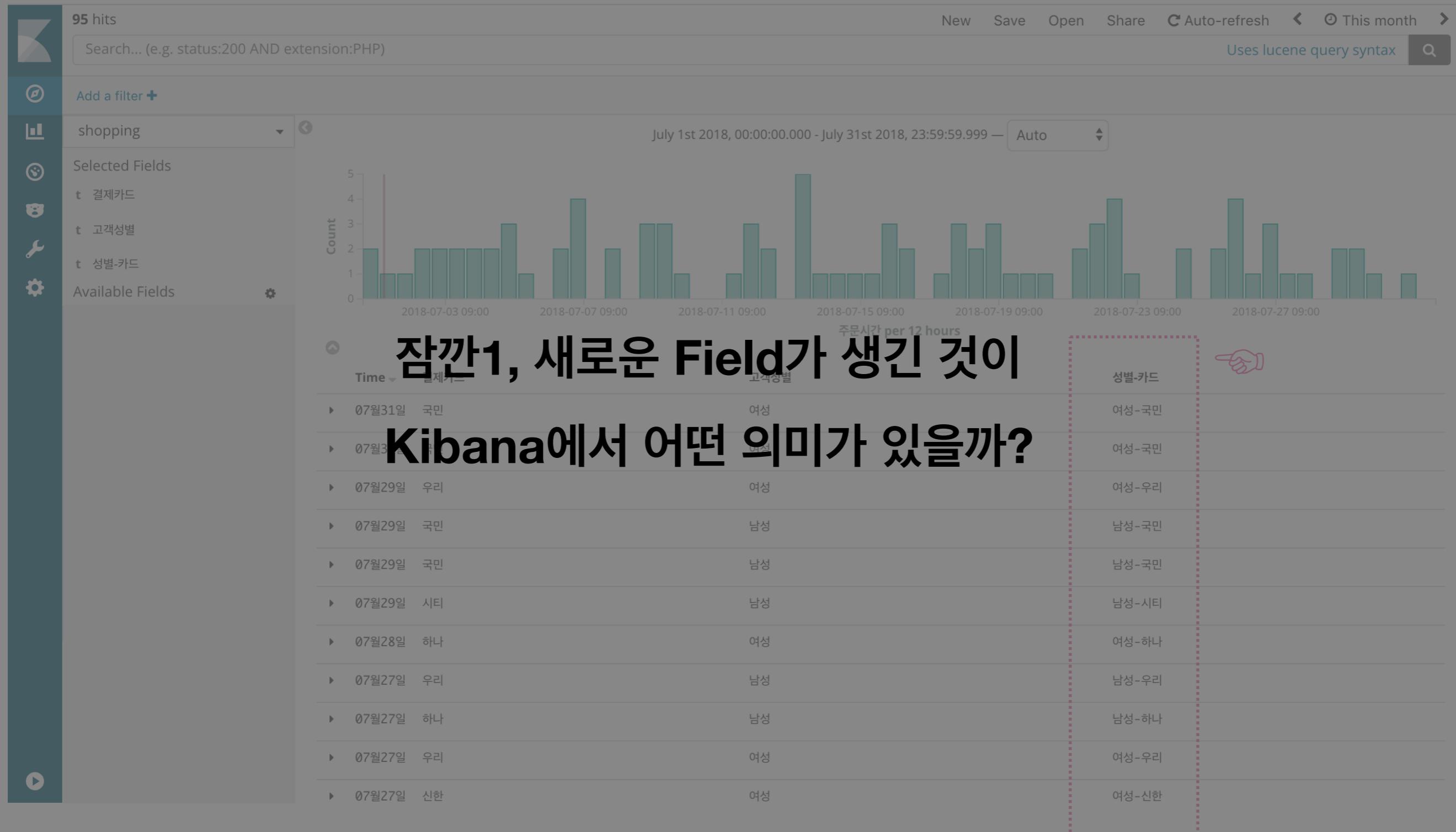
Count

주문시간 per 12 hours

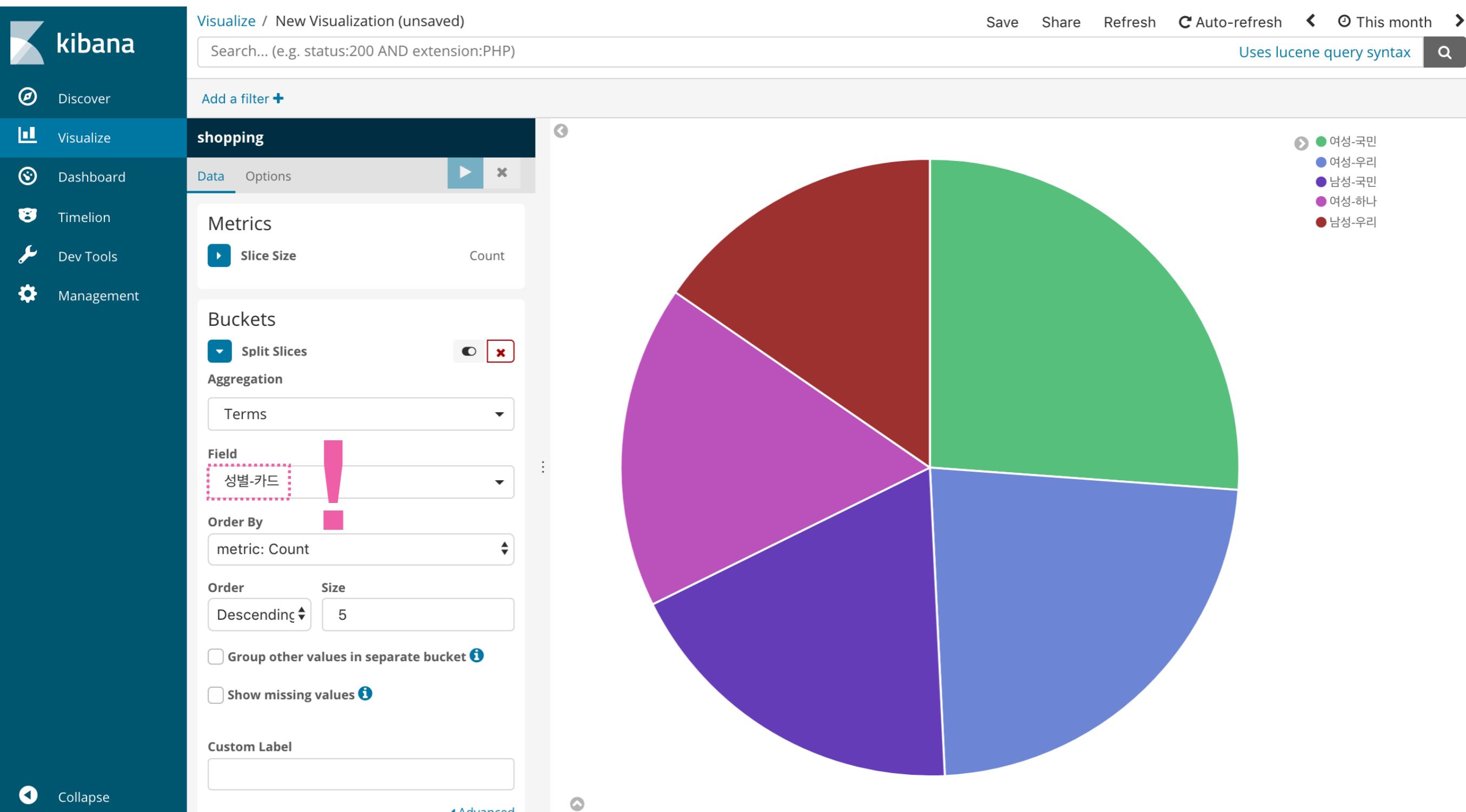
Time	결제카드	고객성별	성별-카드
07월31일	국민	여성	여성-국민
07월30일	국민	여성	여성-국민
07월29일	우리	여성	여성-우리
07월29일	국민	남성	남성-국민
07월29일	국민	남성	남성-국민
07월29일	시티	남성	남성-시티
07월28일	하나	여성	여성-하나
07월27일	우리	남성	남성-우리
07월27일	하나	남성	남성-하나
07월27일	우리	여성	여성-우리
07월27일	신한	여성	여성-신한

A pink dashed box highlights the last four rows of the table, which correspond to the '성별-카드' column. A pink hand icon points to the top-right corner of this box.

Discover에 가서 확인하자



방금 생성한 Field를 이용하여 Visualization을 생성할 수 있다는 것이다



String Concatenation 연산은 안되나?

Field 간 연산은 안되나?



Date Field에서 연/월/일/시/분/초 등 접근 안되나?

기존 Field에 조건을 적용해서 새로운 Field를 만들 수 없나?

예시

2개의 Date Field 값의 차이를 통해
특정한 event의 처리시간을 구하고 싶다면?

scripted field를 추가하자



2. 선택

Management / Kibana

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern ★ test1_*

Time Filter field name: 주문시간

This page lists every field in the **test1_*** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's [Mapping API](#).

fields (21) **scripted fields (0)** source filters (0)

Filter **4. 선택**

3. id_2018.06.17 선택

Scripted fields

These scripted fields are computed on the fly from your data. They can be used in visualizations and displayed in your documents, however they can not be searched. You can manage them here and add new ones as you see fit, but be careful, scripts can be tricky!

+ Add Scripted Field **5. 선택**

No scripted fields found.

A large pink hand icon points to the 'scripted fields (0)' button. A smaller pink hand icon points to the 'Add Scripted Field' button.

script를 작성하자

Management / Kibana / Indices / test1_*

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern ★ test1_*

Create Scripted Field

Name 배송소요시간  1. 본인 index가 맞는지 확인

Language painless

Type number  2. 생성할 Field 이름 입력

Format (Default: Number) number  3. number 선택 

Popularity 0 + -

Script  4. number 선택

```
(doc['수령시간'].value.getMillis()-doc['주문시간'].value.getMillis())/1000/60/60
```

Create Field Cancel  5. 다음과 같이 script 작성
`(doc['수령시간'].value.getMillis()-doc['주문시간'].value.getMillis())/1000/60/60`

6. 선택

Discover에 가서 확인하자

kibana

95 hits

New Save Open Share Auto-refresh < This month >

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

shopping

Selected Fields

수령시간
주문시간
배송소요시간

Available Fields

July 1st 2018, 00:00:00.000 - July 31st 2018, 23:59:59.999 — Auto

Count

July 1st 2018, 00:00:00.000 - July 31st 2018, 23:59:59.999 — Auto

주문시간 per 12 hours

Time	주문시간	수령시간	배송소요시간
July 31st 2018, 10:57:56.000	July 31st 2018, 10:57:56.000	August 5th 2018, 02:03:56.000	111
July 30th 2018, 06:29:11.000	July 30th 2018, 06:29:11.000	July 30th 2018, 16:48:11.000	10
July 29th 2018, 14:41:58.000	July 29th 2018, 14:41:58.000	August 1st 2018, 01:50:58.000	59
July 29th 2018, 14:00:31.000	July 29th 2018, 14:00:31.000	July 31st 2018, 18:55:31.000	52
July 29th 2018, 09:18:29.000	July 29th 2018, 09:18:29.000	July 29th 2018, 22:05:29.000	12
July 29th 2018, 06:06:17.000	July 29th 2018, 06:06:17.000	July 30th 2018, 15:00:17.000	32
July 28th 2018, 11:17:05.000	July 28th 2018, 11:17:05.000	August 1st 2018, 18:26:05.000	103
July 27th 2018, 13:32:10.000	July 27th 2018, 13:32:10.000	July 30th 2018, 09:09:10.000	67
July 27th 2018, 11:22:35.000	July 27th 2018, 11:22:35.000	July 30th 2018, 14:30:35.000	75
July 27th 2018, 10:02:49.000	July 27th 2018, 10:02:49.000	July 28th 2018, 15:21:49.000	29
July 27th 2018, 02:06:27.000	July 27th 2018, 02:06:27.000	July 29th 2018, 12:35:27.000	58

Collapse

A pink dashed box highlights the "배송소요시간" column, and a pink hand icon points to the same column.

예제 1 - Scripted Field

kibana

95 hits

New Save Open Share Auto-refresh < This month >

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Discover Add a filter +

Visualize shopping July 1st 2018, 00:00:00.000 - July 31st 2018, 23:59:59.999 — Auto

Selected Fields

- # 상품가격
- # 상품개수
- # 매출

Dashboard

Timeline

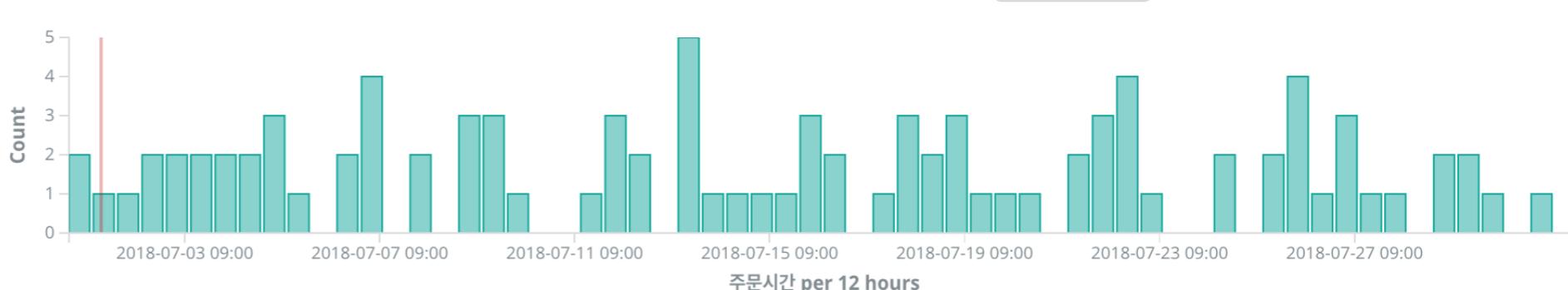
Dev Tools

Management Available Fields

Count

July 1st 2018, 00:00:00.000 - July 31st 2018, 23:59:59.999 — Auto

주문시간 per 12 hours



Time	상품가격	상품개수	매출
July 31st 2018, 10:57:56.000	29,000	7	203,000
July 30th 2018, 06:29:11.000	21,000	7	147,000
July 29th 2018, 14:41:58.000	24,000	1	24,000
July 29th 2018, 14:00:31.000	18,000	7	126,000
July 29th 2018, 09:18:29.000	26,000	1	26,000
July 29th 2018, 06:06:17.000	19,000	7	133,000
July 28th 2018, 11:17:05.000	16,000	1	16,000
July 27th 2018, 13:32:10.000	9,000	1	9,000
July 27th 2018, 11:22:35.000	29,000	1	29,000
July 27th 2018, 10:02:49.000	13,000	7	91,000
July 27th 2018, 09:46:27.000	7,000	1	7,000

Time

상품가격

상품개수

매출

Collapse

String Concatenation 연산은 안되나?

Field 간 연산은 안되나?

Date Field에서 연/월/일/시/분/초 등 접근 안되나?



기존 Field에 조건을 적용해서 새로운 Field를 만들 수 없나?

예시

특정 Date Field에서 시간대 및 요일 등을 추출해서
요일 별 시간대 별 Heat Map을 시각화 하고 싶을 때 사용!

Lucene Expression을 이용하면 날짜 관련 정보를 쉽게 추출할 수 있다

Expression	Description
<code>doc['field_name'].date.centuryOfEra</code>	Century (1-2920000)
<code>doc['field_name'].date.dayOfMonth</code>	Day (1-31), e.g. 1 for the first of the month.
<code>doc['field_name'].date.dayOfWeek</code>	Day of the week (1-7), e.g. 1 for Monday.
<code>doc['field_name'].date.dayOfYear</code>	Day of the year, e.g. 1 for January 1.
<code>doc['field_name'].date.era</code>	Era: 0 for BC, 1 for AD.
<code>doc['field_name'].date.hourOfDay</code>	Hour (0-23).
<code>doc['field_name'].date.millisOfDay</code>	Milliseconds within the day (0-86399999).
<code>doc['field_name'].date.millisOfSecond</code>	Milliseconds within the second (0-999).
<code>doc['field_name'].date.minuteOfDay</code>	Minute within the day (0-1439).
<code>doc['field_name'].date.minuteOfHour</code>	Minute within the hour (0-59).
<code>doc['field_name'].date.monthOfYear</code>	Month within the year (1-12), e.g. 1 for January.
<code>doc['field_name'].date.secondOfDay</code>	Second within the day (0-86399).
<code>doc['field_name'].date.secondOfMinute</code>	Second within the minute (0-59).
<code>doc['field_name'].date.year</code>	Year (-292000000 - 292000000).
<code>doc['field_name'].date.yearOfCentury</code>	Year within the century (1-100).
<code>doc['field_name'].date.yearOfEra</code>	Year within the era (1-292000000).

scripted field를 추가하자

The screenshot shows the Kibana Management interface. On the left sidebar, under the 'Management' section, there is a 'Management / Kibana' link. The main area displays an index pattern named 'test1_*'. A pink callout points to the 'Index Patterns' tab at the top. Another pink callout points to the 'Management / Kibana' link. A third pink callout points to the 'Add Scripted Field' button. A fourth pink callout points to the 'Scripted fields (0)' tab. A fifth pink callout points to the 'No scripted fields found.' message.

1. 선택

2. 선택

Management / Kibana

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ test1_*

Time Filter field name: 주문시간

This page lists every field in the **test1_*** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's [Mapping API](#).

fields (21) scripted fields (0) source filters (0)

Filter

3. id_2018.06.17 선택

4. 선택

Scripted fields

These scripted fields are computed on the fly from your data. They can be used in visualizations and displayed in your documents, however they can not be searched. You can manage them here and add new ones as you see fit, but be careful, scripts can be tricky!

+ Add Scripted Field

5. 선택

No scripted fields found.

script를 작성하자

Management / Kibana / Indices / test1_*

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ test1_*

Create Scripted Field

Name 1. 본인 index가 맞는지 확인

Language 2. 생성할 Field 이름 입력

Type 3. number 선택

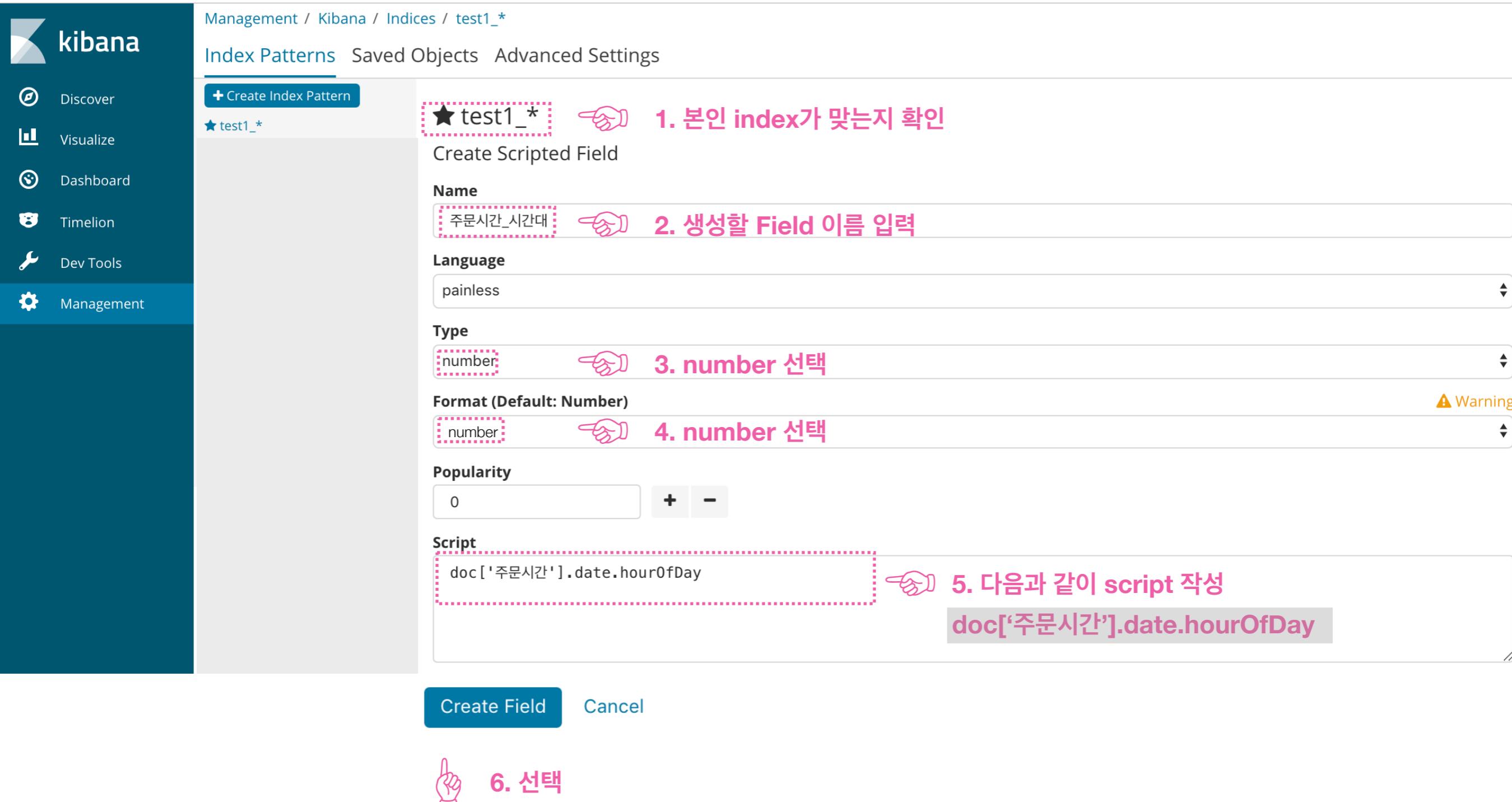
Format (Default: Number) 4. number 선택

Popularity + -

Script 5. 다음과 같이 script 작성
doc['주문시간'].date.hourOfDay

Create Field Cancel

6. 선택



script를 작성하자

Management / Kibana / Indices / test1_*

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ test1_*

>Create Scripted Field

Name 1. 본인 index가 맞는지 확인

Language 2. 생성할 Field 이름 입력

Type 3. number 선택

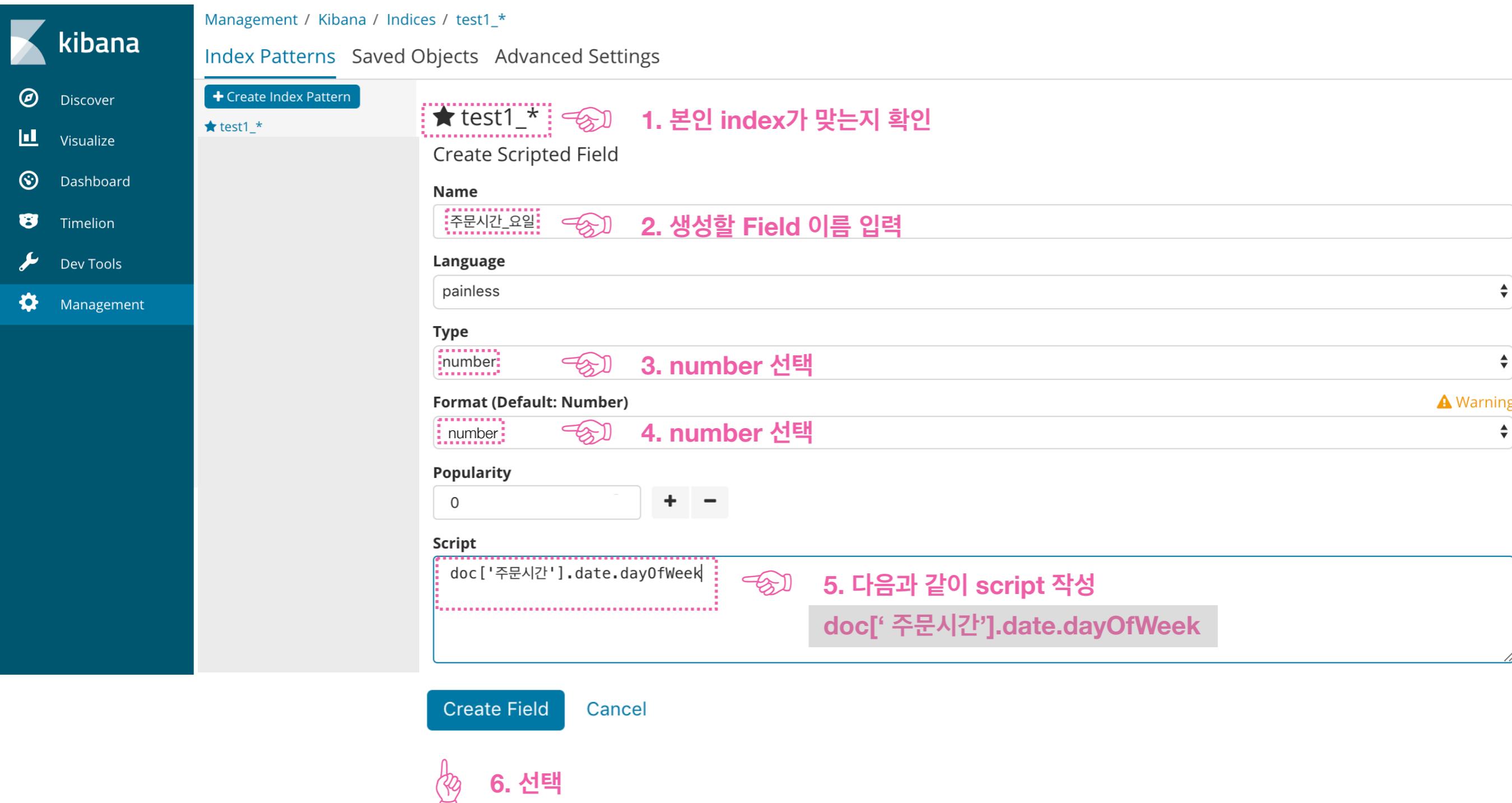
Format (Default: Number) 4. number 선택

Popularity + -

Script 5. 다음과 같이 script 작성
doc[' 주문시간'].date.dayOfWeek

Create Field Cancel

6. 선택



Discover에 가서 확인하자

kibana

95 hits New Save Open Share Auto-refresh < This month >

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

shopping

Selected Fields
 # 주문시간 시간대
 # 주문시간 요일 sort

Available Fields

Count

July 1st 2018, 00:00:00.000 - July 31st 2018, 23:59:59.999 — Auto

주문시간 per 12 hours

Time ▾

Time	주문시간_시간대	주문시간_요일_sort
July 31st 2018, 10:57:56.000	1	2
July 30th 2018, 06:29:11.000	21	7
July 29th 2018, 14:41:58.000	5	7
July 29th 2018, 14:00:31.000	5	7
July 29th 2018, 09:18:29.000	0	7
July 29th 2018, 06:06:17.000	21	6
July 28th 2018, 11:17:05.000	2	6
July 27th 2018, 13:32:10.000	4	5
July 27th 2018, 11:22:35.000	2	5
July 27th 2018, 10:02:49.000	1	5
July 27th 2018, 02:06:27.000	17	4

주문시간_시간대

주문시간_요일_sort

참고

요일	값
월	1
화	2
수	3
목	4
금	5
토	6
일	7

Collapse

Discover에 가서 확인하자

kibana

95 hits

Search... (e.g. status:200 AND extension:PHP)

New Save Open Share Auto-refresh < This month >

Uses lucene query syntax

Discover Add a filter +

Visualize shopping July 1st 2018, 00:00:00.000 - July 31st 2018, 23:59:59.999 — Auto

Dashboard Selected Fields # 주문시간 시간대 # 주문시간 요일 sort Available Fields

Dev Tools Management

심화

잠깐2, 뭔가 이상하지 않나?

Time ▾ July 31st 2018, 10:57:56.000 21

주문시간_시간대

July 30th 2018, 06:29:11.000 21
July 29th 2018, 14:41:51.000 5
July 29th 2018, 14:00:31.000 5
July 29th 2018, 09:18:29.000 0
July 29th 2018, 06:06:17.000 21
July 28th 2018, 11:17:05.000 2
July 27th 2018, 13:32:10.000 4
July 27th 2018, 11:22:35.000 2
July 27th 2018, 10:02:49.000 1
July 27th 2018, 02:06:27.000 17

주문시간_요일_sort

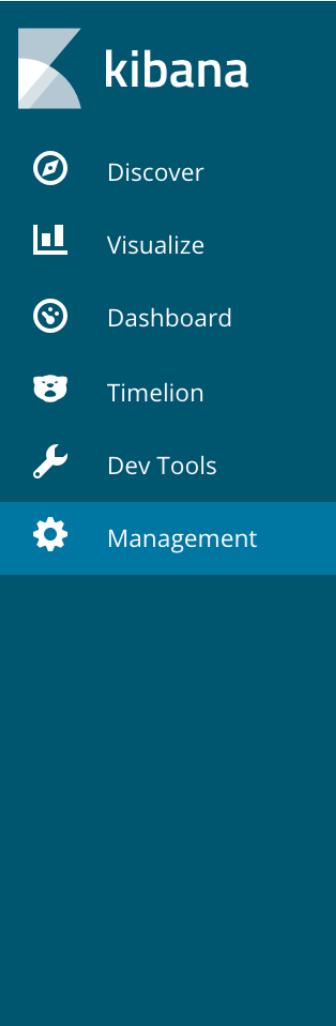
주문시간_요일

월 1
화 2
수 3
목 4
금 5
토 6
일 7

“Time”의 값과 “주문시간_시간대”의 시간이 9 시간 차이난다
왜 그럴까?

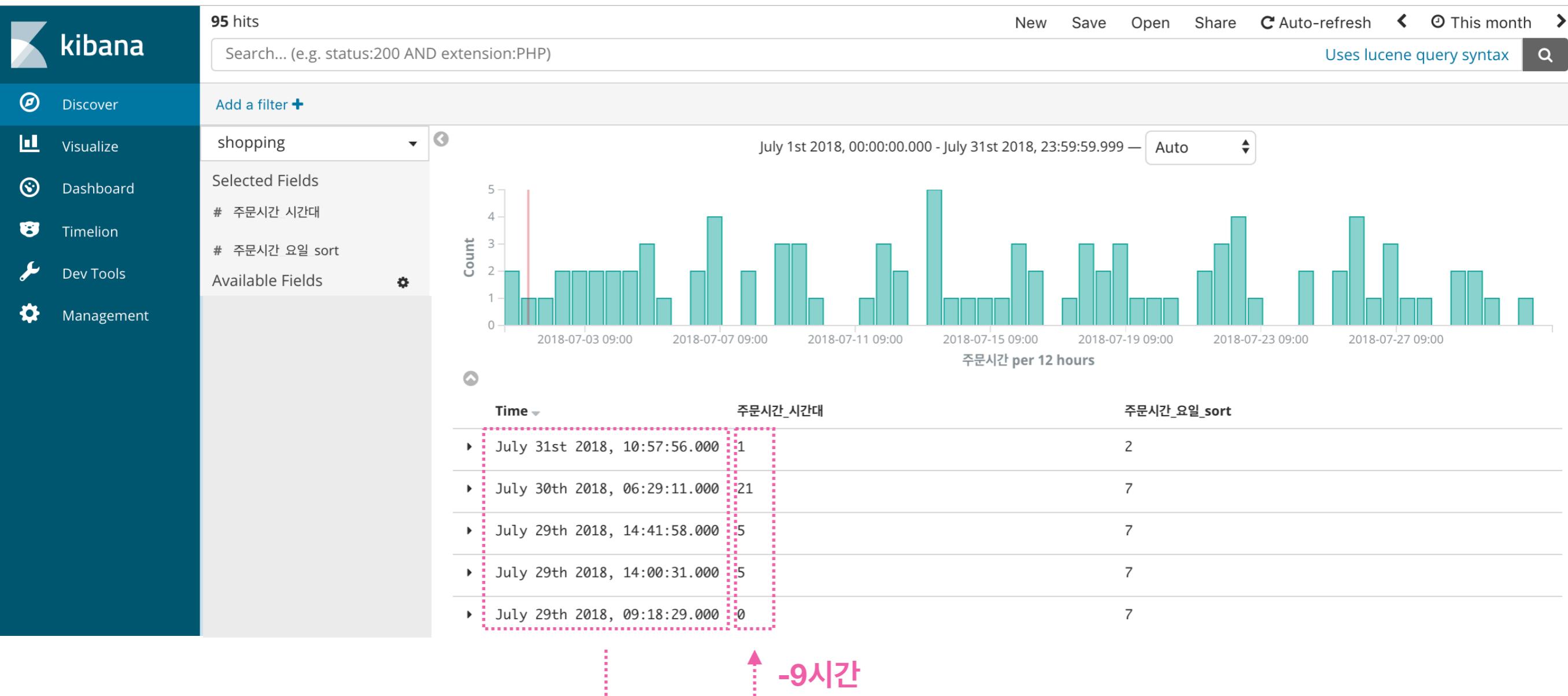
Elasticsearch : 기본적으로 입력된 date field를 **UTC**로 인식한다

Kibana : Management - Advanced Options - dateFormat:tz에서 timezone 설정 (수업 : **Browser**)



Elasticsearch timezone ≠ Kibana timezone

심화



즉, Scripted Field로 추출한 시간대 및曜일은

Local 시간이 아닌 **UTC** 시간이기에

그대로 사용하면 잘못 해석할 여지가 있다

번거롭지만 UTC 시간대로 직접 작업할 것이 아니면
Local 시간대로 변환하는 단계를 거쳐야 한다
(아까 생성한 Scripted Field를 수정하자)

Management / Kibana / Indices / test1_*

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ test1_*

Create Scripted Field

Name 1. 본인 index가 맞는지 확인

Language 2. 생성할 Field 이름 입력

Type 3. number 선택

Format (Default: Number) 4. number 선택

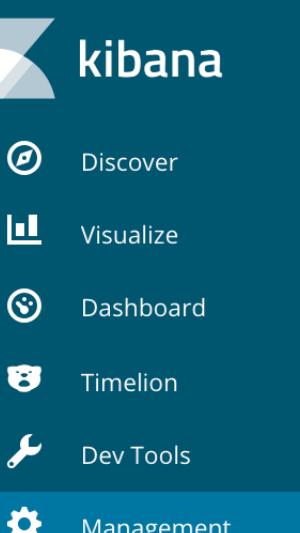
Popularity + -

Script 5. 다음과 같이 script 작성 외우지마세요

LocalDateTime.ofInstant(Instant.ofEpochMilli(doc['주문시간'].value.millis),
ZoneId.of('Asia/Seoul')).getHour()

Create Field Cancel

6. 선택



Management / Kibana / Indices / test1_*

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern ★ test1_*

1. 본인 index가 맞는지 확인

Create Scripted Field

Name 주문시간_요일

2. 생성할 Field 이름 입력

Language painless

Type string

3. string 선택

Format (Default: String) string

4. string 선택

⚠ Warning

Popularity 0 + -

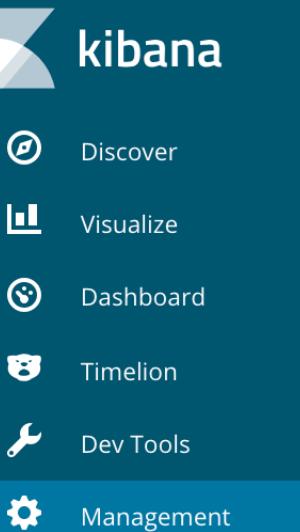
Script

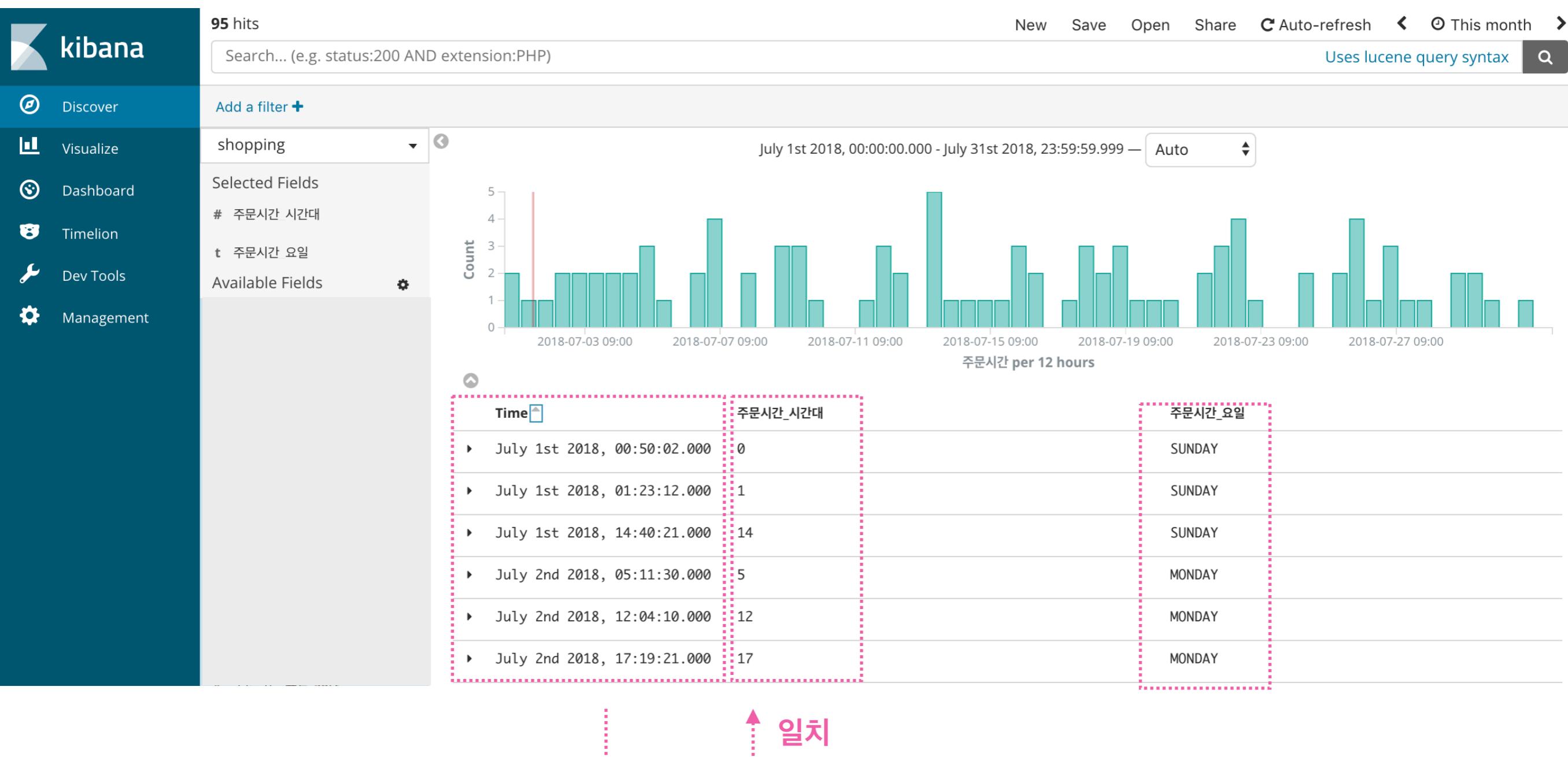
```
LocalDateTime.ofInstant(Instant.ofEpochMilli(doc['주문시간'].value.millis), ZoneId.of('Asia/Seoul')).getDayOfWeek()
```

5. 다음과 같이 script 작성 외우지마세요

LocalDateTime.ofInstant(Instant.ofEpochMilli(doc['주문시간'].value.millis), ZoneId.of('Asia/Seoul')).getDayOfWeek()

6. 선택





String Concatenation 연산은 안되나?

Field 간 연산은 안되나?

Date Field에서 연/월/일/시/분/초 등 접근 안되나?

기존 Field에 조건을 적용해서 새로운 Field를 만들 수 없나?



예시

고객나이 Field 값에 따라 10대, 20대, 30대, ...

와 같은 값을 갖는 Field를 만들고 싶다면?

scripted field를 추가하자

The screenshot shows the Kibana Management interface with the following steps highlighted:

- 1. 선택**: A hand icon points to the "Management" button in the sidebar.
- 2. 선택**: A hand icon points to the "Index Patterns" tab in the top navigation bar.
- 3. id_2018.06.17 선택**: A hand icon points to the "test1_*" index pattern in the list.
- 4. 선택**: A hand icon points to the "scripted fields (0)" tab in the navigation bar.
- 5. 선택**: A hand icon points to the "+ Add Scripted Field" button.

The main content area displays the "test1_*" index pattern details, including a note about time filtering and a section for managing scripted fields. A message indicates no scripted fields have been found.

script를 작성하자 !

Management / Kibana / Indices / test1_*

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern ★ test1_*

Create Scripted Field

Name 연령대

Language painless

Type string

Format (Default: String) string

Popularity 0

Script

```
if (doc['고객나이'].value < 20) { return "10대" } else if (doc['고객나이'].value < 40) { return "20~30대" } else { return "40대 이상" }
```

5. 다음과 같이 script 작성

```
if (doc['고객나이'].value < 20) { return "10대" }
else if (doc['고객나이'].value < 40) { return "20~30대" }
else { return "40대 이상" }
```

6. 선택

Create Field Cancel

The screenshot shows the Kibana Management interface under the 'Indices' tab for 'test1_*'. A new 'Scripted Field' is being created. The 'Name' is set to '연령대' (Age Group). The 'Type' is selected as 'string'. The 'Script' section contains a conditional JavaScript function that returns age groups ('10대', '20~30대', or '40대 이상') based on the value of the '고객나이' (Customer Age) field. Step-by-step instructions are overlaid on the interface, pointing to each step: 1. 확인 (Check), 2. 입력 (Input), 3. 선택 (Select), 4. 선택 (Select), 5. 작성 (Write), and 6. 선택 (Select).

Discover에 가서 확인하자

4,951 hits

New Save Open Share Auto-refresh < This year >

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

Selected Fields: # 고객나이, t 연령대

Available Fields: ⚙️

January 1st 2018, 00:00:00.000 - December 31st 2018, 23:59:59.999 — Auto

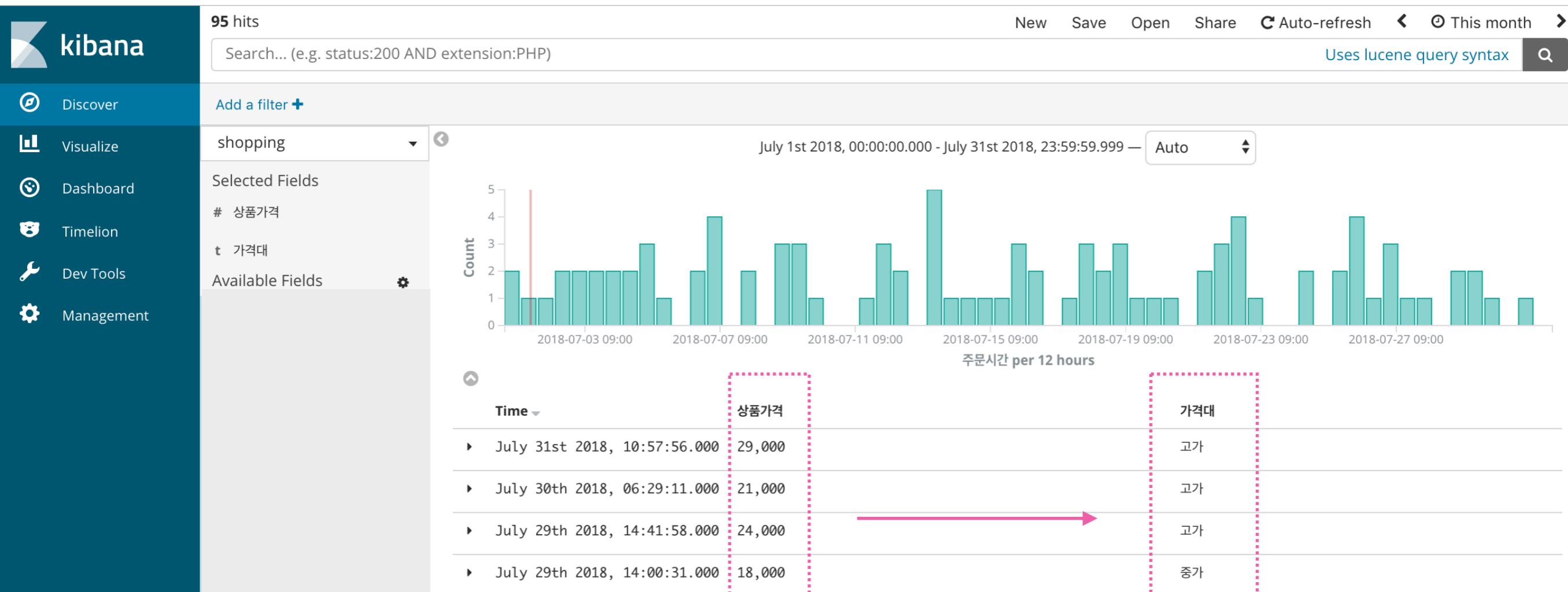
Count

주문시간 per week

Time	고객나이	연령대
December 31st 2018, 23:56:34.000	56	40대 이상
December 31st 2018, 23:52:22.000	64	40대 이상
December 31st 2018, 23:40:15.000	32	20~30대
December 31st 2018, 22:53:45.000	45	40대 이상
December 31st 2018, 20:26:56.000	50	40대 이상
December 31st 2018, 19:53:18.000	26	20~30대
December 31st 2018, 19:26:08.000	48	40대 이상
December 31st 2018, 19:23:46.000	51	40대 이상
December 31st 2018, 18:28:03.000	28	20~30대
December 31st 2018, 17:20:23.000	28	20~30대
December 31st 2018, 16:38:44.000	46	40대 이상

Collapse

예제2 - Scripted Field



상품가격	가격대
$x < 10,000$	저가
$10,000 \leq x < 20,000$	중가
$20,000 \leq x$	고가

단, Scripted Field를 사용할 때 다음과 같은 사항에 주의하자!

1. Kibana 상에서 Lucene Query Syntax로 검색이 안된다

- ☞ 6.X에서는 kuery를 통해서는 가능
- ☞ 5.X에서는 Filter를 이용해서 검색해야 한다

2. 한 번에 한 개의 Document만 조회할 수 있다.

- ☞ 즉, 여러 Documents를 동시에 접근해서 계산하는 시계열 수식은 가능하지 않다

3. Scripted Field를 데이터 색인 시에 application에서 생성하자

- ☞ Scripted Field는 elasticsearch에 저장되지 않고 쿼리 시점에 Elasticsearch에 전달된다 (연산 작업 필요)
- ☞ 그러므로 Kibana에서 사용자 응답시간 단축을 위해 데이터 색인 시에 scripted field를 생성하자

Managing Field 

Elasticsearch에 저장된 데이터를
Kibana에서 **format**만 살짝 변경해서 보여줄 수 없을까?

Date를 다르게 표현할 수 없나? 🤔

20180701

1511199899

Sunday

Jul 1st 18

2017년 11월 20일 17시 44분

11/20/2017 5:44pm

2018년07월01일

July 1st 2018, 9:05:21 pm

Default는 아래와 같은 Format이다

kibana

95 hits

New Save Open Share C Auto-refresh < ⏴ This month >

Search... (e.g. status:200 AND extension:PHP)

Add a filter +

shopping

July 1st 2018, 00:00:00.000 - July 31st 2018, 23:59:59.999 — Auto

Selected Fields
주문시간

Available Fields

Count

July 1st 2018, 00:00:00.000 - July 31st 2018, 23:59:59.999 — Auto

주문시간 per 12 hours

Time ↑ 주문시간 ↑

Time	주문시간
▶ July 1st 2018, 00:50:02.000	July 1st 2018, 00:50:02.000
▶ July 1st 2018, 01:23:12.000	July 1st 2018, 01:23:12.000
▶ July 1st 2018, 14:40:21.000	July 1st 2018, 14:40:21.000
▶ July 2nd 2018, 05:11:30.000	July 2nd 2018, 05:11:30.000
▶ July 2nd 2018, 12:04:10.000	July 2nd 2018, 12:04:10.000
▶ July 2nd 2018, 17:19:21.000	July 2nd 2018, 17:19:21.000
▶ July 3rd 2018, 06:13:41.000	July 3rd 2018, 06:13:41.000
▶ July 3rd 2018, 11:01:45.000	July 3rd 2018, 11:01:45.000
▶ July 3rd 2018, 17:46:36.000	July 3rd 2018, 17:46:36.000
▶ July 3rd 2018, 18:19:35.000	July 3rd 2018, 18:19:35.000
▶ July 4th 2018, 01:04:40.000	July 4th 2018, 01:04:40.000

Collapse

Date Format 변경하려는 Field의 Controls 선택

2. 선택

Management / Kibana

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ test1_*



3.

id_2018.06.17

선택



1. 선택

★ test1_*

Time Filter field name: 주문시간

This page lists every field in the **test1_*** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's [Mapping API](#).

fields (21)

scripted fields (0)

source filters (0)

Filter

All field types ▾

name	type	format	searchable	aggregatable	excluded	controls
판매자평점	number		✓	✓		
주문시간	date		✓	✓		
접수번호	number		✓	✓		
예약여부	string		✓	✓		
수령시간	date		✓	✓		
상품분류	string		✓	✓		
상품개수	number		✓	✓		
상품가격	number		✓	✓		
배송메모	string		✓			
물건좌표	geo_point		✓	✓		
구매사이트	string		✓	✓		
고객주소_시도	string		✓	✓		
고객성별	string		✓	✓		
고객나이	number		✓	✓		

4. 선택



적절한 Format으로 수정하자

Management / Kibana / Indices / test1_* / Field

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern ★ test1_*

주문시간

Type date

Format (Default: Date) Date moment.js format pattern (Default: "MMMM Do YYYY, HH:mm:ss.SSS") YYYY년MM월DD일

Samples Input Formatted

1530447558573 2018년07월01일

1514732400000 2018년01월01일

1546268399999 2018년12월31일

Popularity 0 + -

Update Field Cancel

1. 본인 index가 맞는지 확인

2. data type은 변경이 안됨

3. Date 선택

4. 어떤 Format을 사용할 수 있는지 확인

5. 변경하고자 하는 Format 입력

6. 현재 입력한 Format의 예상 결과 표시

7. 선택

A screenshot of the Kibana Management interface under the 'Indices' tab for the 'test1_*' index. On the left sidebar, 'Management' is selected. The main area shows an index pattern 'test1_*' with a star icon. The 'Type' is set to 'date'. In the 'Format' section, the default pattern 'moment.js format pattern (Default: "MMMM Do YYYY, HH:mm:ss.SSS")' is shown as 'YYYY년MM월DD일'. Below this, there's a 'Samples' table with three rows of timestamp data: 1530447558573, 1514732400000, and 1546268399999, each with its corresponding 'Formatted' date (2018년07월01일, 2018년01월01일, 2018년12월31일). A 'Popularity' slider is set to 0. At the bottom are 'Update Field' and 'Cancel' buttons. Hand icons with numbered steps 1 through 7 point to specific parts of the interface: 1 points to the index name, 2 points to the type, 3 points to the format dropdown, 4 points to the format examples, 5 points to the input field, 6 points to the formatted output, and 7 points to the popularity slider.

Discover에 돌아가서 확인하자

예제3 - 아래 표를 이용해서 여러가지 Format을 테스트해보자

날짜 단위	문법	예시	설명
Year	YYYY	2014	4자리 표시
Year	YY	14	2자리 표시
Month	M	1	1~2자리 표시
Month	MM	01	2자리 표시
Day	D	1	1~2자리 표시
Day	DD	01	2자리 표시
Day	Do	1st	며칠째인지 표시
Hour	H	1	1자리 표시 (24시)
Hour	HH	01	1~2자리 표시 (24시)
Hour	h	1	1자리 표시 (12시)
Hour	hh	01	1~2자리 표시 (12시)
a	h	am/pm	소문자 표시
A	hh	AM/PM	대문자 표시
Minute	m	1	1자리 표시
Minute	mm	01	1~2자리 표시
Second	s	1	1자리 표시
Second	ss	01	1~2자리 표시
Second	X	1410715640.579	Unix Timestamp 초
Millisecond	x	1410715640579	Unix Timestam 밀리초

String를 다르게 표현할 수 없나? 🤔

higee.io/221111469658

221111469658

higee.io/221111469658 (링크 형식)

221111469658 (링크 형식)

HIGEE/IO/221111469658 (대문자)

String Type의 Format 전환 실습을 위해 Index를 등록하자

Index : {id}_url
Time Filter Field : 없음

Default는 아래와 같은 Format이다

3 hits

New Save Open Share

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax Q

Add a filter +

Selected Fields higee_url

Available Fields t _id t _index # _score t _type t full_url t partial_url

_source

- ▶ full_url: http://higee.io/221247452452 partial_url: 221247452452 _id: U50eVmQByNsCKuKn1L3o _type: my_type _index: higee_url _score: 1
- ▶ full_url: http://higee.io/221111469658 partial_url: 221111469658 _id: UZ0eVmQByNsCKuKn1L2g _type: my_type _index: higee_url _score: 1
- ▶ full_url: http://higee.io/221285621862 partial_url: 221285621862 _id: Up0eVmQByNsCKuKn1L3A _type: my_type _index: higee_url _score: 1

Default는 아래와 같은 Format이다

3 hits

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

Selected Fields: higee_url

Available Fields: _id, _index, _score, _type, full_url, partial_url

_source
full_url: http://higee.io/221247452452 partial_url: 221247452452 id: U50eVmQByNsCKuKn1L3o _type: my_type _index: higee_url _score: 1
full_url: http://higee.io/221111469658 partial_url: 221111469658 id: UZ0eVmQByNsCKuKn1L2g _type: my_type _index: higee_url _score: 1
full_url: http://higee.io/221285621862 partial_url: 221285621862 id: Up0eVmQByNsCKuKn1L3A _type: my_type _index: higee_url _score: 1

URL 형태를 띠는 두 Field의 Format을 String에서 **URL**로 변경해보자

Data Format 변경하려는 Field의 Control 선택 - full_url

Management / Kibana

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ higee_url

This page lists every field in the **higee_url** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's Mapping API.

fields (7) scripted fields (0) source filters (0)

Filter All field types ▾

name	type	format	searchable	aggregatable	excluded	controls
_id	string		✓	✓		
_index	string		✓	✓		
_score	number					
_source	_source					
_type	string		✓	✓		
full_url	string		✓	✓		
partial_url	string		✓	✓		

1. 선택 2. 선택 3. id_url 선택 4. 선택

Scroll to top Page Size 25 ▾

Url Templates에 적절한 값을 입력하자

Management / Kibana / Indices / higee_url / Field

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ higee_url

full_url

Type

string

1. Type은 변하지 않는다

Format (Default: String)

Url

2. Format : Url 선택

Type

Link

3. Type : Link 선택

Open link in current tab

Url Template

{{rawValue}}

4. Url Template : {{rawValue}} 입력

Warning

Url Template Help

Label Template

{{value}}

5. Label Template : {{value}} 입력

Label Template Help

Samples

Input

Formatted

john

john

/some pathname/asset.png

/some pathname/asset.png

1234

1234

Popularity

0

+

-

Update Field

Cancel



6. 선택

Discover에 돌아가서 확인하자

3 hits New Save Open Share

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

Selected Fields Available Fields

higee_url

_source

- ▶ full_url: <http://higee.io/221247452452> partial_url: 221247452452 _id: U50eVmQByNsCKuKn1L3o _type: my_type _index: higee_url _score: 1
- ▶ full_url: <http://higee.io/221111469658> partial_url: 221111469658 _id: UZ0eVmQByNsCKuKn1L2g _type: my_type _index: higee_url _score: 1
- ▶ full_url: <http://higee.io/221285621862> partial_url: 221285621862 _id: Up0eVmQByNsCKuKn1L3A _type: my_type _index: higee_url _score: 1

_score t _id t _index t _partial_url t _partial_url t _partial_url

 클릭 가능하게 바뀐게 보이며 클릭하면 제대로 링크로 이동한다

Data Format 변경하려는 Field의 Control 선택 - partial_url

2. 선택

Management / Kibana

Index Patterns

Saved Objects Advanced Settings

+ Create Index Pattern

★ higee_url

3. id_url 선택

★ higee_url

This page lists every field in the **higee_url** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's [Mapping API](#).

fields (7) scripted fields (0) source filters (0)

Filter

All field types ▾

name	type	format	searchable	aggregatable	excluded	controls
_id	string		✓	✓		
_index	string		✓	✓		
_score	number					
_source	_source					
_type	string		✓	✓		
full_url	string	Url	✓	✓		
partial_url	string		✓	✓		

Scroll to top

Page Size 25

1. 선택

4. 선택

Url Templates에 적절한 값을 입력하자

Management / Kibana / Indices / higee_url / Field

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ higee_url

partial_url

Type

string

1. Type은 변하지 않는다

Format (Default: String)

Url

2. Format : Url 선택

Type

Link

3. Type : Link 선택

Open link in current tab

Url Template

http://higee.io/{{value}}

4. Url Template : <http://higee.io{{value}}> 입력

⚠ Warning

Url Template Help

Label.Template

#{{value}}

5. Label Template : # {{value}} 입력

Label Template Help

Samples

Input

Formatted

john

#john

/some pathname/asset.png

#/some pathname/asset.png

1234

#1234

Popularity

0

+ -

Update Field

Cancel



6. 선택

Discover에 돌아가서 확인하자

3 hits

New Save Open Share

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

higee_url

	_source
▶	full_url: http://higee.io/221247452452 partial_url: #221247452452 _id: U50eVmQByNsCKuKn1L3o _type: my_type _index: higee_url _score: 1
▶	full_url: http://higee.io/221111469658 partial_url: #221111469658 _id: UZ0eVmQByNsCKuKn1L2g _type: my_type _index: higee_url _score: 1
▶	full_url: http://higee.io/221285621862 partial_url: #221285621862 _id: Up0eVmQByNsCKuKn1L3A _type: my_type _index: higee_url _score: 1



클릭 가능하게 바뀐게 보이며 클릭하면 제대로 링크로 이동한다

Number를 다르게 표현할 수 없나? 🤔

3353	31B	36191
5.01 (sec)	61%	1%
7.99KB	3626	5.1MB
15%	10.01 (min)	1.2GB
		3.3 (hour)

Number Type의 Format 전환 실습을 위해 Index를 등록하자

Index : {id}_number
Time Filter Field : 없음

Default는 아래와 같은 Format이다

The screenshot shows the Kibana interface with the following details:

- Top Bar:** Shows "4 hits" and navigation links for "New", "Save", "Open", and "Share".
- Search Bar:** Contains the placeholder "Search... (e.g. status:200 AND extension:PHP)" and a "Uses lucene query syntax" link.
- Left Sidebar:** Includes icons for Add a filter, Selected Fields, Available Fields, and various settings. The "Selected Fields" section has "higee_number" selected.
- Result List:** The results are displayed under the "_source" field. There are four entries, each showing fields: byte, duration, percent, _id, _type, _index, and _score. The first entry is expanded to show its full value.

_source
byte: 8,191 duration: 10,005 percent: 0.6 _id: P508VmQByNsCKuKnM78R _type: my_type _index: higee_number _score: 1
byte: 13,535,139 duration: 33 percent: 0.75 _id: Qp08VmQByNsCKuKnM79w _type: my_type _index: higee_number _score: 1
byte: 135,351 duration: 335,513 percent: 0.2 _id: QJ08VmQByNsCKuKnM782 _type: my_type _index: higee_number _score: 1
byte: 31 duration: 5,013 percent: 0.2 _id: QZ08VmQByNsCKuKnM79T _type: my_type _index: higee_number _score: 1

Default는 아래와 같은 Format이다

The screenshot shows the Kibana interface with the following details:

- Top Bar:** 4 hits, New, Save, Open, Share.
- Search Bar:** Search... (e.g. status:200 AND extension:PHP) and a link to [Uses lucene query syntax](#).
- Left Sidebar:** Icons for Add a filter, Selected Fields, Available Fields, and various metrics like byte, duration, percent, id, type, index, and score.
- Selected Field:** higee_number is selected.
- Result List:** The results are displayed under the `_source` field. Each result is a document with fields: byte, duration, percent, id, type, index, and score. The first four results are highlighted with a pink dashed border.
- Bottom:** A large pink arrow points downwards from the highlighted results towards the text "Number 들에 의미를 부여해보자".

Field	Value
byte	8,191
duration	10,005
percent	0.6
id	P508VmQByNsCKuKnM78R
type	my_type
index	higee_number
score	1
byte	13,535,139
duration	33
percent	0.75
id	Qp08VmQByNsCKuKnM79w
type	my_type
index	higee_number
score	1
byte	135,351
duration	335,513
percent	0.2
id	QJ08VmQByNsCKuKnM782
type	my_type
index	higee_number
score	1
byte	31
duration	5,013
percent	0.2
id	QZ08VmQByNsCKuKnM79T
type	my_type
index	higee_number
score	1

Number 들에 의미를 부여해보자

Data Format 변경하려는 Field의 Control 선택 - duration

Management / Kibana

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ higee_number

This page lists every field in the **higee_number** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's [Mapping API](#).

fields (8) scripted fields (0) source filters (0)

Filter All field types ▾

name	type	format	searchable	aggregatable	excluded	controls
_id	string		✓	✓		edit
_index	string		✓	✓		edit
_score	number					edit
_source	_source					edit
_type	string		✓	✓		edit
byte	number		✓	✓		edit
duration	number		✓	✓		edit
percent	number		✓	✓		edit

Scroll to top Page Size 25

duration Field Format을 변경하자

Management / Kibana / Indices / higee_number / Field

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ higee_number

★ higee_number

duration

Type

number

1. Type은 바꿀 수 없다

Format (Default: Number)

Duration

2. Format : Duration 선택

Input Format

Seconds

3. 원본 시간 단위

Output Format

Minutes

4. 변환하려는 시간 단위

Decimal Places

2

5. 소수점 자리수

Samples

Input

Formatted

-123

-2.05

1

0.02

12

0.20

123

2.05

658

10.97

1988

33.13

3857

64.28

123292

2054.87

923528271

15392137.85

Popularity

0

+

-

Update Field

Cancel



6. 선택

Discover에 돌아가서 확인하자

4 hits

New Save Open Share

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

Selected Fields: higee_number

Available Fields: _id, _index, _score, _source, _type, byte, duration, percent

_source

- byte: 8,191 duration: 166.75 percent: 0.6 _id: P508VmQByNsCKuKnM78R _type: my_type _index: higee_number _score: 1
- byte: 13,535,139 duration: 0.55 percent: 0.75 _id: Qp08VmQByNsCKuKnM79w _type: my_type _index: higee_number _score: 1
- byte: 135,351 duration: 5591.88 percent: 0.2 _id: QJ08VmQByNsCKuKnM782 _type: my_type _index: higee_number _score: 1
- byte: 31 duration: 83.55 percent: 0.2 _id: QZ08VmQByNsCKuKnM79T _type: my_type _index: higee_number _score: 1

minute 단위로 변환됐다!

Data Format 변경하려는 Field의 Control 선택 - byte

Management / Kibana

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ higee_number

This page lists every field in the **higee_number** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's [Mapping API](#).

fields (8) scripted fields (0) source filters (0)

Filter All field types ▾

name	type	format	searchable	aggregatable	excluded	controls
_id	string		✓	✓		
_index	string		✓	✓		
_score	number					
_source	_source					
_type	string		✓	✓		
byte	number		✓	✓		
duration	number	Duration	✓	✓		
percent	number		✓	✓		

Scroll to top Page Size 25 ▾

duration Field Format을 변경하자

Management / Kibana / Indices / higee_number / Field

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ higee_number

byte

Type

number 1. Type은 바꿀 수 없다

Format (Default: Number) Docs

Bytes 2. Format : Duration 선택

Numerical.js format pattern (Default: "0,0.[000]b")

0,0.[000]b 3. 표시 Format 정의

Samples

Input	Formatted
1024	1KB
5150000	4.911MB
19900000000	1.853GB

Popularity

0

Update Field Cancel

4. 선택

Discover에 돌아가서 확인하자

4 hits New Save Open Share

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

Selected Fields Available Fields

higee_number

_source

byte: 7.999KB duration: 166.75 percent: 0.6 _id: P508VmQByNsCKuKnM78R _type: my_type _index: higee_number _score: 1

byte: 12.908MB duration: 0.55 percent: 0.75 _id: Qp08VmQByNsCKuKnM79w _type: my_type _index: higee_number _score: 1

byte: 132.179KB duration: 5591.88 percent: 0.2 _id: QJ08VmQByNsCKuKnM782 _type: my_type _index: higee_number _score: 1

byte: 31B duration: 83.55 percent: 0.2 _id: QZ08VmQByNsCKuKnM79T _type: my_type _index: higee_number _score: 1

_score # byte # duration # percent

바이트로 환산되어 가독성이 좋아졌다

Data Format 변경하려는 Field의 Control 선택 - percentage

Management / Kibana

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern ★ higee_number

This page lists every field in the **higee_number** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's [Mapping API](#).

fields (8) scripted fields (0) source filters (0)

Filter All field types ▾

name	type	format	searchable	aggregatable	excluded	controls
_id	string		✓	✓		
_index	string		✓	✓		
_score	number					
_source	_source					
_type	string		✓	✓		
byte	number	Bytes	✓	✓		
duration	number	Duration	✓	✓		
percent	number		✓	✓		

Scroll to top Page Size 25



duration Field Format을 변경하자

Management / Kibana / Indices / higee_number / Field

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ higee_number

percent

Type

number 1. Type은 바꿀 수 없다

Format (Default: Number) Docs

Percentage 2. Format : Percentage 선택
Numeral.js format pattern (Default: "0,0.[000]%)

0,0.[000]% 3. 표시 Format 정의

Samples

Input	Formatted
0.1	10%
0.99999	99.999%
1	100%
100	10,000%
1000	100,000%

Popularity + -

Update Field Cancel

4. 선택

Discover에 돌아가서 확인하자

4 hits

New Save Open Share

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

Selected Fields higee_number

Available Fields t _id
t _index
_score
t _type
byte
duration
percent

_source

- ▶ byte: 7.999KB duration: 166.75 percent: 60% _id: P508VmQByNsCKuKnM78R _type: my_type _index: higee_number _score: 1
- ▶ byte: 12.908MB duration: 0.55 percent: 75% _id: Qp08VmQByNsCKuKnM79w _type: my_type _index: higee_number _score: 1
- ▶ byte: 132.179KB duration: 5591.88 percent: 20% _id: QJ08VmQByNsCKuKnM782 _type: my_type _index: higee_number _score: 1
- ▶ byte: 31B duration: 83.55 percent: 20% _id: QZ08VmQByNsCKuKnM79T _type: my_type _index: higee_number _score: 1

소수점 형태가 백분율 형태로 표시되어 가독성이 좋아졌다

잠깐3

Data Format이 변하는 것이지 **Data Type**이 변하는 것이 아니다.

그러므로 Elasticsearch에 저장된 데이터 자체는 변하지 않는다!

Dashboard 기능

우선 새로운 Dashboard를 만들자

The screenshot shows a user interface for creating a new dashboard. On the left, there is a vertical sidebar with icons for different sections: a blue square (Dashboard), a magnifying glass (Search), a bar chart (Metrics), a hand icon (Select), a gear (Settings), and a play button (Run). The 'Select' icon is highlighted with a red dashed box and labeled '1. 선택' (Step 1). At the top right, there is a search bar with the placeholder 'Search...', a blue plus button, a hand icon, and the text '2. 선택'. Below the plus button, it says '1-3 of 3' and has navigation arrows. The main area is currently empty.

우선 새로운 Dashboard를 만들자

Dashboard / Editing New Dashboard

Save

Cancel

Add

Options

Share

Auto-refresh



Month to date



Search... (e.g. status:200 AND extension:PHP)

Uses lucene query syntax



3. 선택

This dashboard is empty. Let's fill it up!

Click the Add button in the menu bar above to add a visualization to the dashboard.

If you haven't set up any visualizations yet, visit the [Visualize app](#) to create your first visualization.

우선 새로운 Dashboard를 만들자

Dashboard / Editing New Dashboard Save Cancel Add Options Share Auto-refresh < ⏪ Month to date ⏩

Add Panels

Visualization Saved Search

Visualizations Filter... 1-20 of 63 Add new Visualization

Name ▲

- [nginx] Data Table
- [nginx] Goal
- [nginx] Timelion
- [nginx] area chart
- [nginx] coordinate maps
- [nginx] heat map
- [nginx] horizontal bar
- [nginx] markdown
- [nginx] metric
- [nginx] pie chart
- [nginx] region maps
- [nginx] tag-cloud
- [shopping] Area Chart
- [shopping] Data Table
- [shopping] Goal

☞ 4. 추가하려는 Visualization 선택

Visualization을 추가하자

ID가 higee인 경우,

- [higee-week1-exercise6]
- [higee-week1-exercise7]
- [higee-week2-exercise8]
- [higee-week2-exercise10]
- [higee-week2-exercise15]
- [higee-week2-exercise16]
- [higee-week2-exercise17]

Visualization을 적당히 배치하자

Dashboard / Editing New Dashboard (unsaved)

Save Cancel Add Options Share Auto-refresh Last 30 days

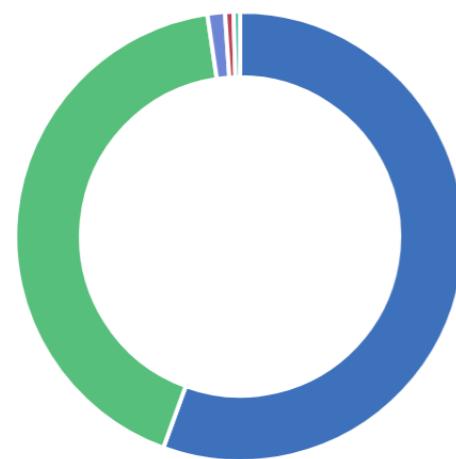
Search... (e.g. status:200 AND extension:PHP)

Uses lucene query syntax



Add a filter +

[week1 - exercise6] pie chart



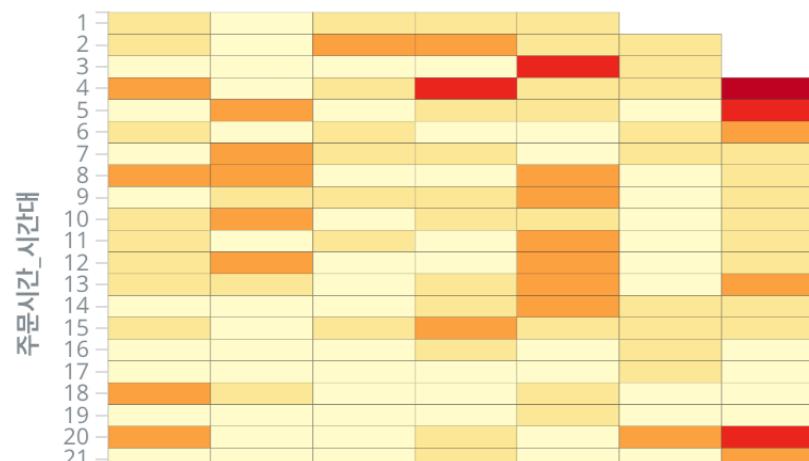
- Seocho
- Seoul
- Beijing
- Suwon
- Mountain View

[week1 - exercise7] pie chart



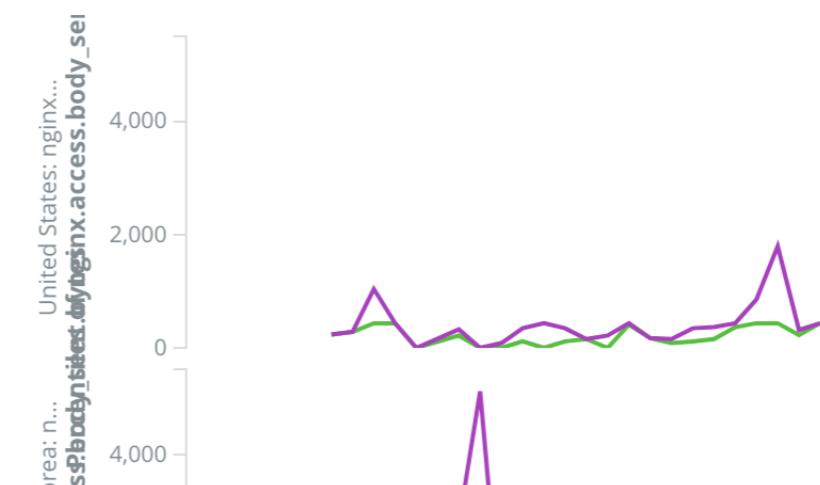
- Mac OS X
- iOS
- Other
- Windows 10
- Windows 7

[week2 - exercise8] heatmap



- 0 - 1
- 1 - 2
- 2 - 2
- 2 - 3
- 3 - 3
- 3 - 4
- 4 - 4

[week2 - exercise10] line chart



- 50th percentile of nginx.access.body_size
- 75th percentile of nginx.access.body_size

Dashboard를 저장하자

Dashboard / Editing New Dashboard (unsaved)



Save

Cancel

Add

Options

Share

Auto-refresh

Last 30 days

Save dashboard

Title

New Dashboard

👉 2. Dashboard Title 입력



Description

Dashboard description

Store time with dashboard

This changes the time filter to the currently selected time each time this dashboard is loaded.

Save

👉 3. 선택

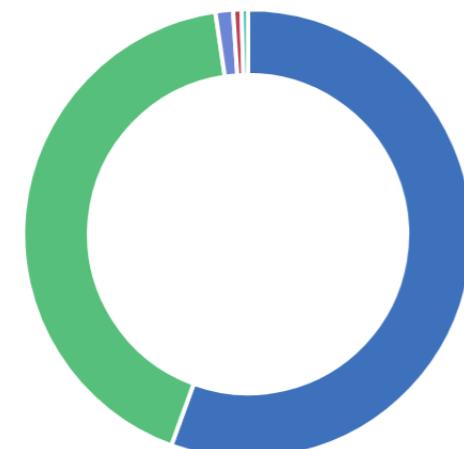
Search... (e.g. status:200 AND extension:PHP)

Uses lucene query syntax



Add a filter +

[week1 - exercise6] pie chart



- Seocho
- Seoul
- Beijing
- Suwon
- Mountain View

[week1 - exercise7] pie chart



- Mac OS X
- iOS
- Other
- Windows 10
- Windows 7

Dashboard를 조회하자



Dashboard

Dashboard		
<input type="text" value="nginx"/> + 1-1 of 1 < >		
<input type="checkbox"/> Name ↑	Description	Actions
<input type="checkbox"/> nginx	1. 선택	Edit
1-1 of 1 < >		

Dashboard를 조회하자

Dashboard / nginx

Full screen Share Clone Edit ⚙ Auto-refresh ⏪ ⏩ Last 30 days

Search... (e.g. status:200 AND extension:PHP)

Uses lucene query syntax



Add a filter +

[nginx] markdown

Nginx Access Log Dashboard

```
66.249.82.131 - - [13/Jun/2018:17:01:02 +0000] "GET /ui/favicons/favicon-16x16.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
118.221.38.242 - - [13/Jun/2018:17:01:14 +0000] "POST /api/console/proxy?path=_aliases&method=GET HTTP/1.1" 200 107 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
118.221.38.242 - - [13/Jun/2018:17:01:14 +0000] "POST /api/console/proxy?path=_mapping&method=GET HTTP/1.1" 200 974 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
66.249.82.131 - - [13/Jun/2018:17:01:16 +0000] "GET /ui/favicons/favicon-32x32.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
66.249.82.129 - - [13/Jun/2018:17:01:17 +0000] "GET /ui/favicons/favicon-16x16.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
```

[nginx] search

1-50 of 71,642



Time	nginx.access.url	nginx.access.response_code	nginx.access.body_sent.bytes
▶ June 10th 2018, 22:49:58.000	/bundles/vendors.bundle.js?v=16627	200	2,018,434
▶ June 9th 2018, 16:28:52.000	/bundles/kibana.bundle.js?v=15571	200	1,662,257
▶ June 9th 2018, 16:15:41.000	/bundles/kibana.bundle.js?v=15571	200	1,662,123
▶ June 9th 2018, 16:15:41.000	/bundles/kibana.bundle.js?v=15571	200	1,662,046

Dashboard를 clone하자

The screenshot shows the Kibana interface for an 'nginx' dashboard. At the top, there are several icons: a magnifying glass, a bar chart, a clock, a user icon, a wrench, and a gear. Below these are two search/filter sections: '[nginx] markdown' and '[nginx] search'. The search section contains a table with columns: Time, nginx.access.url, nginx.access.response_code, and nginx.access.body_sent.bytes. The table data is as follows:

Time	nginx.access.url	nginx.access.response_code	nginx.access.body_sent.bytes
▶ June 10th 2018, 22:49:58.000	/bundles/vendors.bundle.js?v=16627	200	2,018,434
▶ June 9th 2018, 16:28:52.000	/bundles/kibana.bundle.js?v=15571	200	1,662,257
▶ June 9th 2018, 16:15:41.000	/bundles/kibana.bundle.js?v=15571	200	1,662,123
▶ June 9th 2018, 16:15:41.000	/bundles/kibana.bundle.js?v=15571	200	1,662,046

At the top right, there are buttons for Full screen, Share, Clone (highlighted with a red dashed box), Edit, Auto-refresh, and a time range selector. A search bar says 'Search... (e.g. status:200 AND extension:PHP)'. To the right of the search bar are buttons for 'Uses lucene query syntax' and a magnifying glass icon.

A modal window titled 'Clone Dashboard' is open in the center. It asks 'Please enter a new name for your dashboard.' with a text input field containing 'nginx-higee' (also highlighted with a red dashed box). Below the input field is a pink hand icon pointing to it, followed by the text '2. 이름 입력 nginx-{id}'. At the bottom of the modal are 'Cancel' and 'Confirm Clone' buttons. A pink hand icon points to the 'Confirm Clone' button, followed by the text '3. 선택'.

At the bottom right of the main interface, there is a page number '1-50 of 71,749' and navigation arrows.

Clone 받은 환경에서 Dashboard를 사용할 수 있다

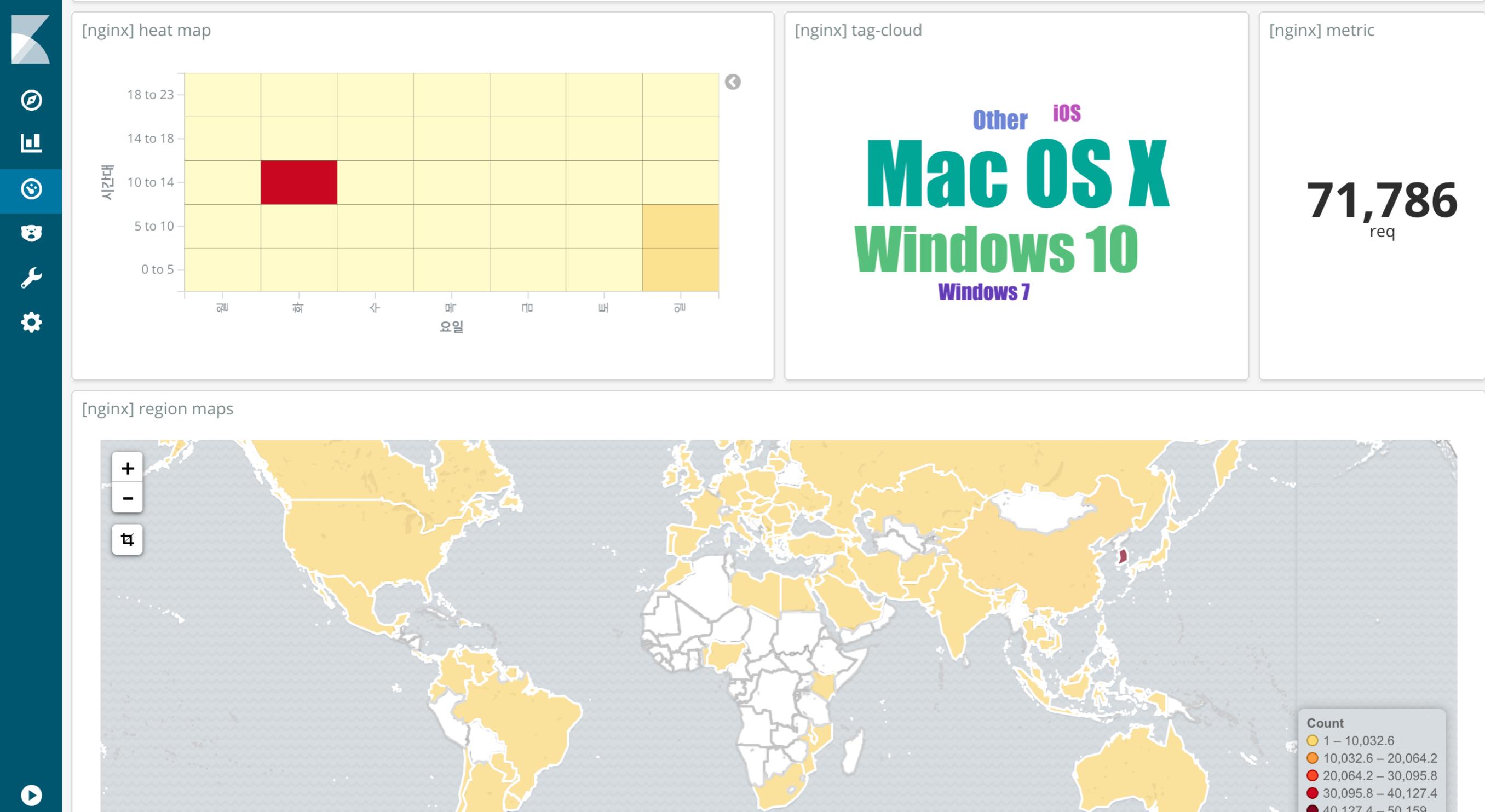
The screenshot shows a Kibana dashboard interface with the following components:

- Header:** Includes "Dashboard / nginx-higee" with a clone icon, search bar ("Search... (e.g. status:200 AND extension:PHP)"), and navigation buttons for "Full screen", "Share", "Clone", "Edit", "Auto-refresh" (with a refresh icon), and time range ("Last 30 days").
- Left Sidebar:** A vertical sidebar with icons for Kibana, Logstash, Elasticsearch, and file system.
- Section [nginx] markdown:** Displays the title "Nginx Access.Log Dashboard".
- Section [nginx] search:** Shows a table with the following data:

Time	nginx.access.url	nginx.access.response_code	nginx.access.body_sent.bytes
▶ June 10th 2018, 22:49:58.000	/bundles/vendors.bundle.js?v=16627	200	2,018,434
▶ June 9th 2018, 16:28:52.000	/bundles/kibana.bundle.js?v=15571	200	1,662,257
▶ June 9th 2018, 16:15:41.000	/bundles/kibana.bundle.js?v=15571	200	1,662,123
▶ June 9th 2018, 16:15:41.000	/bundles/kibana.bundle.js?v=15571	200	1,662,046

Page navigation buttons at the bottom right indicate "1-50 of 71,782" with previous and next arrow icons.

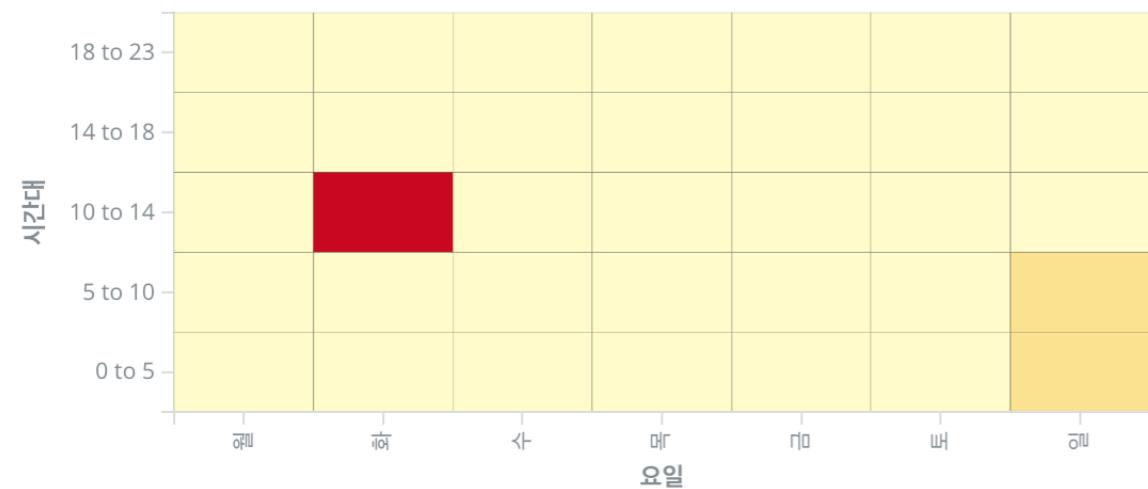
Dashboard가 Interactive하다!



아래의 Dashboard에서 “Mac OS X”에 해당하는 데이터만 보고 싶다고 하자



[nginx] heat map



[nginx] tag-cloud



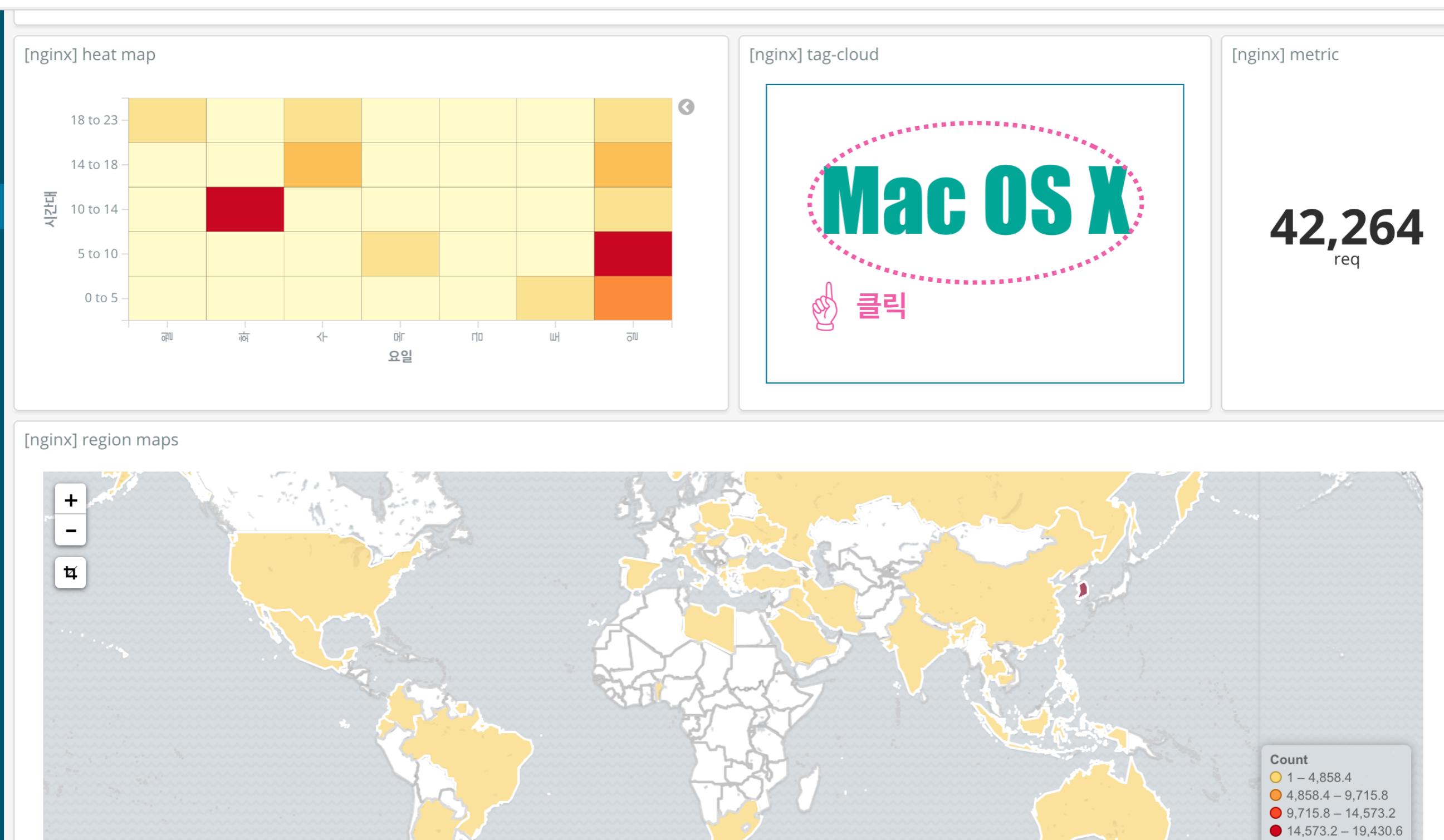
[nginx] metric

71,786
req

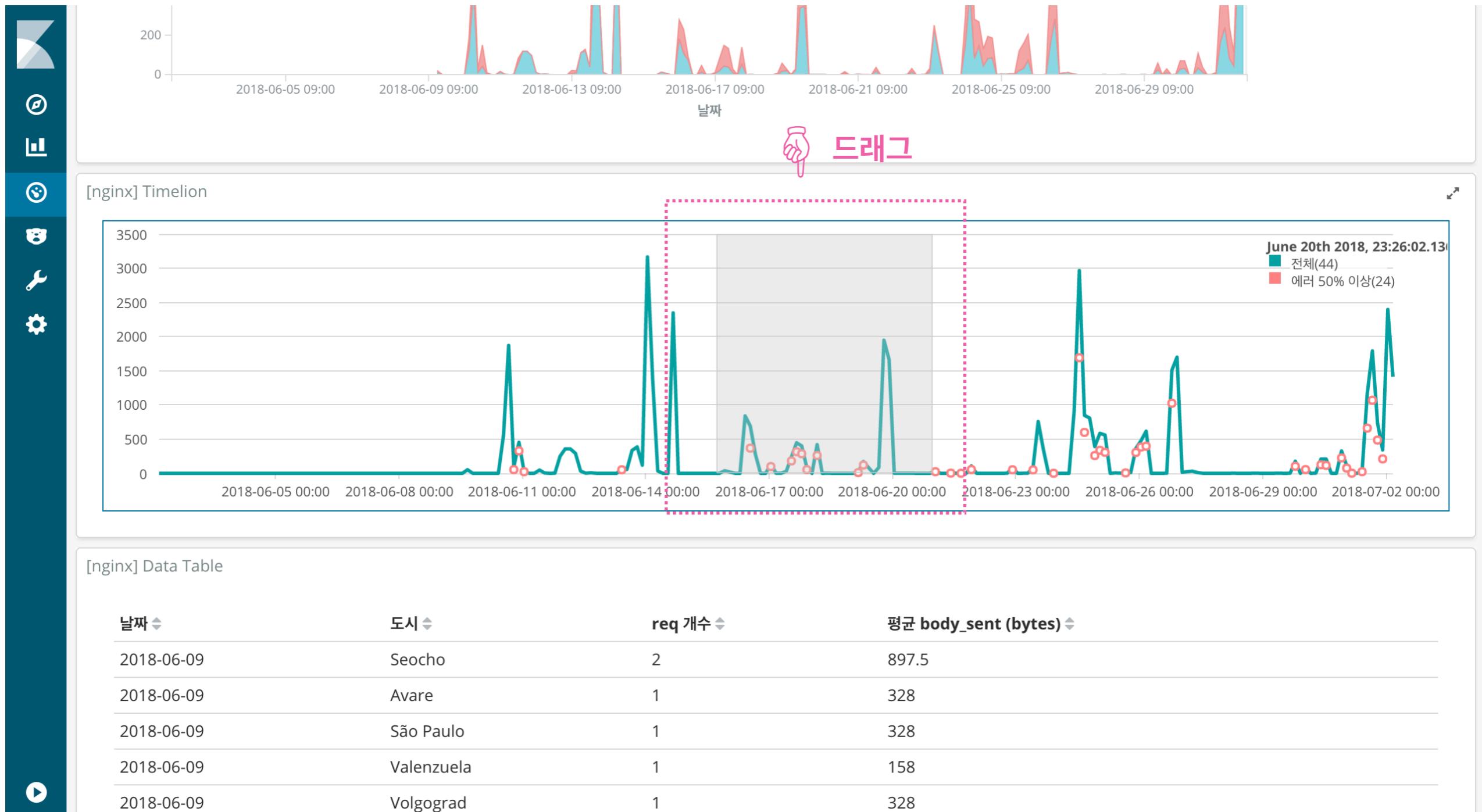
[nginx] region maps



Dashboard 전체적인 UI는 유지한채 “Mac OS X”에 해당하는 값만 필터링되어 보여진다



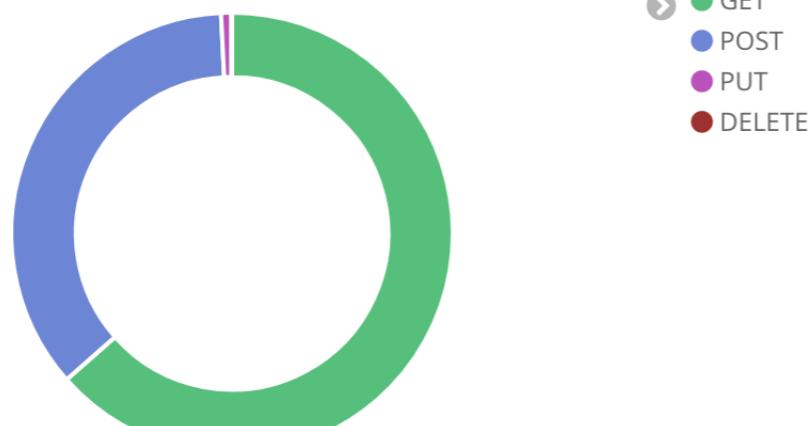
특정 기간을 집중해서 보고 싶으면 Drag를 하자



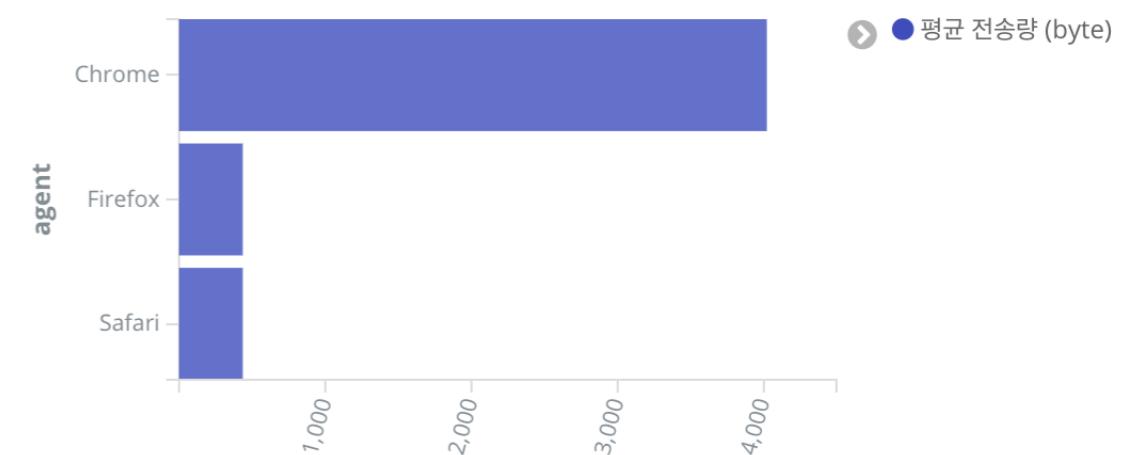
특정 지역의 데이터만 보고 싶으면 polygon/rectangle을 그리자



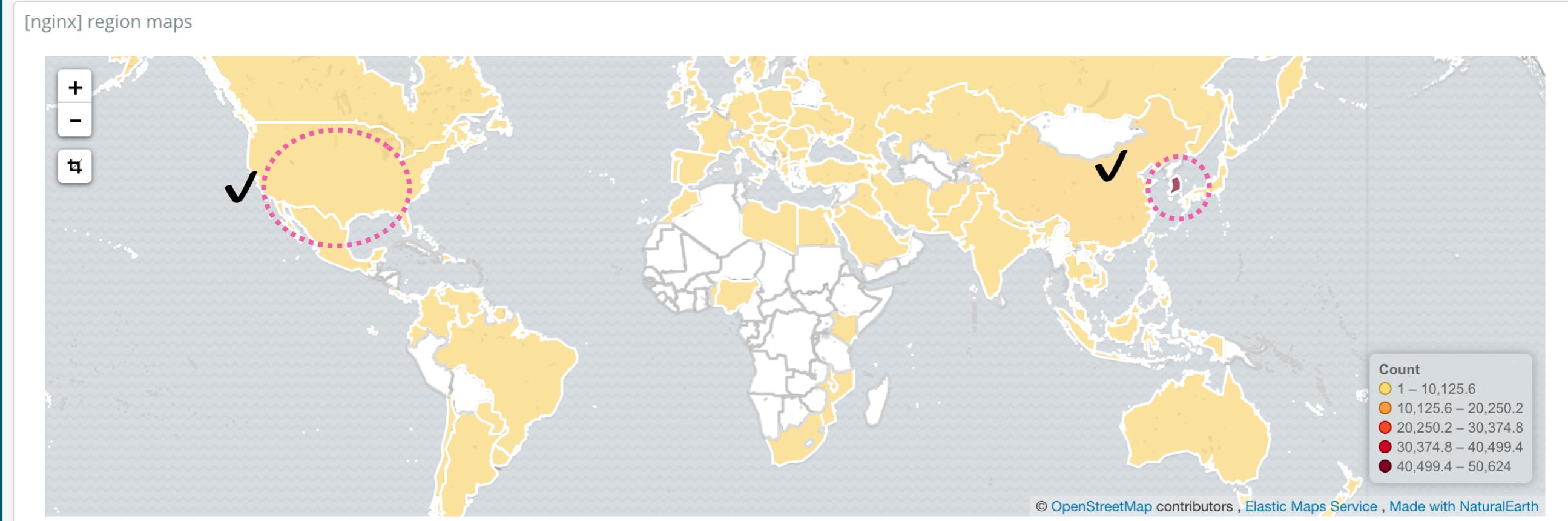
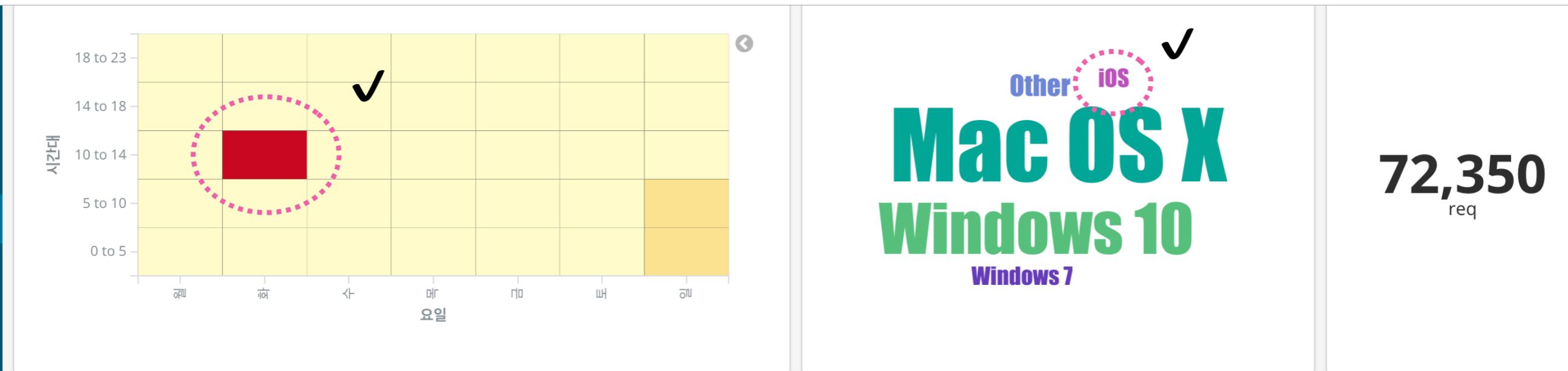
[nginx] pie chart



[nginx] horizontal bar



여러 visualization을 클릭하면서 Interactive한 Dashboard를 경험해보자



Auto Refresh 기능을 이용하자



1. Auto-refresh 선택

Dashboard / nginx-higee

Full screen Share Clone Edit C Auto-refresh < ⏪ Last 30 days > ⏩

Refresh Interval

Off

5 seconds

10 seconds

30 seconds

45 seconds

1 minute

5 minutes

15 minutes

30 minutes

1 hour

2 hour

12 hour

1 day



2. Refresh 간격 설정

Search... (e.g. status:200 AND extension:PHP)

Uses lucene query syntax



Add a filter +

[nginx] markdown

Nginx Access.Log Dashboard

설정한 간격마다 Index 데이터를 확인하여
새로운 데이터가 있으면 Dashboard에 반영한다

```
66.249.82.131 - - [13/Jun/2018:17:01:02 +0000] "GET /ui/favicons/favicon-16x16.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
118.221.38.242 - - [13/Jun/2018:17:01:14 +0000] "POST /api/console/proxy?path=_aliases&method=GET HTTP/1.1" 200 107 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
118.221.38.242 - - [13/Jun/2018:17:01:14 +0000] "POST /api/console/proxy?path=_mapping&method=GET HTTP/1.1" 200 974 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
66.249.82.131 - - [13/Jun/2018:17:01:16 +0000] "GET /ui/favicons/favicon-32x32.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
66.249.82.129 - - [13/Jun/2018:17:01:17 +0000] "GET /ui/favicons/favicon-16x16.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
```

[nginx] search

▶ June 14th 2018, 16:48:38.000	/bundles/kibana.bundle.js?v=16627	200	1,257,713
▶ June 14th 2018, 03:49:34.000	/bundles/kibana.bundle.js?v=16627	200	1,257,695
▶ June 27th 2018, 06:10:08.000	/bundles/kibana.bundle.js?v=16627	200	1,257,667

dashboard를 공유하자

	dashboard 공유하기 전 변경 사항	dashboard 공유 후 변경 사항
saved dashboard	반영 o	반영 o
Snapshot	반영 o	반영 x (url이 변경됨)

dashboard를 공유하자



1. Share 선택

Dashboard / nginx-higee

Full screen

Share

Clone

Edit

Auto-refresh

Last 30 days

Share saved dashboard

You can share this URL with people to let them load the most recent saved version of this dashboard.

Copy

Embedded iframe

```
<iframe src="http://kibana.higee.co/app/kibana#/dashboard/891b7600-7d64-11e8-8161-3b4280"
```

Add to your HTML source. Note that all clients must be able to access Kibana.

Copy

Link

<http://kibana.higee.co/app/kibana#/dashboard/891b7600-7d64-11e8-8161-3b4280>

Share Snapshot

Snapshot URLs encode the current state of the dashboard in the URL itself. Edits to the saved dashboard won't be visible via this URL.

Short URL Copy

Embedded iframe

```
<iframe src="http://kibana.higee.co/app/kibana#/dashboard/891b7600-7d64-11e8-8161-3b4280"
```

Add to your HTML source. Note that all clients must be able to access Kibana.

Short URL Copy

Link

<http://kibana.higee.co/app/kibana#/dashboard/891b7600-7d64-11e8-8161-3b4280>

We recommend sharing shortened snapshot URLs for maximum compatibility. Internet Explorer has URL length restrictions, and some wiki and markup parsers don't do well with the full-length version of the snapshot URL, but the short URL should work great.

Search... (e.g. status:200 AND extension:PHP)

Saved Dashboard



Snapshot

Uses lucene query syntax



Add a filter +

[nginx] markdown

Nginx Access Log Dashboard

```
66.249.82.131 - - [13/Jun/2018:17:01:02 +0000] "GET /ui/favicon/favicon-16x16.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
118.221.38.242 - - [13/Jun/2018:17:01:14 +0000] "POST /api/console/proxy?path=_aliases&method=GET HTTP/1.1" 200 107 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
118.221.38.242 - - [13/Jun/2018:17:01:14 +0000] "POST /api/console/proxy?path=_mapping&method=GET HTTP/1.1" 200 974 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
66.249.82.131 - - [13/Jun/2018:17:01:16 +0000] "GET /ui/favicon/favicon-32x32.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
66.249.82.129 - - [13/Jun/2018:17:01:17 +0000] "GET /ui/favicon/favicon-16x16.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
```

Dashboard/Visualization export

Dashboard 및 Visualize Object를 Import/Export 할 수 없나?

- 데이터 백업
- UI 백업

Dashboard export



Management / Kibana

Index Patterns **Saved Objects** Advanced Settings

2. Saved Objects 선택

Edit Saved Objects

From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. Typically objects are only modified via their associated application, which is probably what you should use instead of this screen. Each tab is limited to 100 results. You can use the filter to find objects not in the default list.

3. Dashboards 선택

Export Everything Import

Dashboard (2) Searches (1) Visualizations (12)

nginx

Delete Export

1. 선택

Title nginx **nginx-higee**

4. nginx-{id} 선택

1 selected

5. Export 선택

6. {id}_dashboard.json 이름 변경

A screenshot of the Kibana 'Saved Objects' interface. The 'Dashboards' tab is selected. A pink dashed box highlights the 'nginx-higee' item in the list. A pink arrow points from the 'nginx-higee' item to the 'Export' button. A pink arrow points from the 'Export' button to the '6. {id}_dashboard.json 이름 변경' text at the bottom right.

Dashboard export



A screenshot of a code editor window titled "export.json". The file contains a single JSON object representing a dashboard. The JSON structure includes fields for _id, _type, _source, panelsJSON, optionsJSON, version, timeRestore, and kibanaSavedObjectMeta. The _source field contains detailed information about the dashboard's title, hits, description, panel layout, and visualization settings.

```
1 [  
2 {  
3   "_id": "891b7600-7d64-11e8-8161-3b4280559eb3",  
4   "_type": "dashboard",  
5   "_source": {  
6     "title": "nginx-higee",  
7     "hits": 0,  
8     "description": "",  
9     "panelsJSON": "[{\\"panelIndex\\":\\"1\\",\\"gridData\\":{\\\"x\\":0,\\\"y\\":6,\\\"w\\":6,\\\"h\\":3,\\\"i\\":\\"1\\"},\\"embeddableConfig\\":{\\\"vis\\\":{\\\"defaultColors\\":  
10    "optionsJSON": "{\\\"darkTheme\\":false,\\\"hidePanelTitles\\":false,\\\"useMargins\\":true}",  
11    "version": 1,  
12    "timeRestore": false,  
13    "kibanaSavedObjectMeta": {  
14      "searchSourceJSON": "{\\\"query\\\":{\\\"language\\\":\\\"lucene\\\",\\\"query\\\":\\\"\\\"},\\\"filter\\\":[],\\\"highlightAll\\\":true,\\\"version\\\":true}"  
15    }  
16  }  
17 }]  
18 ]
```

Dashboard export

대시보드를 export 하면 export.json으로 저장한 json 파일이 생기는데,
대시보드에 어떤 visualization이 어느 위치에 어떤 크기로 생성되었는지에 관한 정보를 담고 있다.



개별 visualization 들이 어떤 aggregation으로 만들어졌는지 등에 관한 정보는 없다.



Visualization 백업 필요!

Visualization export

Management / Kibana



2. Saved Objects 선택

Index Patterns Saved Objects Advanced Settings

Edit Saved Objects

Export Everything Import

From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. Typically objects are only modified via their associated application, which is probably what you should use instead of this screen. Each tab is limited to 100 results. You can use the filter to find objects not in the default list.

Dashboards (2)

Searches (1)

Visualizations (12)

3. Visualizations 선택



4. nginx 검색

Delete

Export

6. Export 선택

Title

[nginx] area chart

[nginx] coordinate maps

[nginx] Data Table

[nginx] Goal

[nginx] heat map

[nginx] horizontal bar

[nginx] markdown

[nginx] metric

[nginx] pie chart

[nginx] region maps

[nginx] tag-cloud

[nginx] Timelion

7.
다운 받은 후
`{id}_visualization.json` 이름 변경

5. nginx로 시작하는 모든 visualization 선택

Visualization export

```
export (1).json x

1 [
2 {
3     "_id": "08e28cc0-6f28-11e8-a0fb-51f0eb991705",
4     "_type": "visualization",
5     "_source": {
6         "title": "[nginx] region maps",
7         "visState": "{\"title\":\"[nginx] region maps\",\"type\":\"region_map\",\"params\":{\"legendPosition\":\"bottomright\",\"addTooltip\":true,\"colorSchema\":\"Yellow to Red\"},\"uiStateJSON\": {\"mapZoom\":2,\"mapCenter\": [11.695272733029402,24.433593750000004]}",
8         "description": "",
9         "version": 1,
10        "kibanaSavedObjectMeta": {
11            "searchSourceJSON": "{\"index\":\"eb4d54b0-6fa9-11e8-8161-3b4280559eb3\",\"filter\":[],\"query\":{\\\"query\\\":\\\"\\\",\\\"language\\\":\\\"lucene\\\"}}"
12        }
13    }
14 },
15 {
16     "_id": "7a9123a0-6f27-11e8-a0fb-51f0eb991705",
17     "_type": "visualization",
18     "_source": {
19         "title": "[nginx] coordinate maps",
20         "visState": "{\"title\":\"[nginx] coordinate maps\",\"type\":\"tile_map\",\"params\":{\"mapType\":\"Scaled Circle Markers\",\"isDesaturated\":true,\"addTooltip\":true,\"heat\"},\"uiStateJSON\": {},\"description\": "",\"version\": 1,
21        "kibanaSavedObjectMeta": {
22            "searchSourceJSON": "{\"index\":\"eb4d54b0-6fa9-11e8-8161-3b4280559eb3\",\"filter\":[],\"query\":{\\\"query\\\":\\\"\\\",\\\"language\\\":\\\"lucene\\\"}}"
23        }
24    }
25 },
26 {
27     "_id": "cfbbc570-6f26-11e8-a0fb-51f0eb991705",
28     "_type": "visualization",
29     "_source": {
30         "title": "[nginx] metric",
31         "visState": "{\"title\":\"[nginx] metric\",\"type\":\"metric\",\"params\":{\"addTooltip\":true,\"addLegend\":false,\"type\":\"metric\",\"metric\":{\\\"percentageMode\\\":false,\"scale\\\":100}},\"uiStateJSON\": {},\"description\": "",\"version\": 1,
32        "kibanaSavedObjectMeta": {
33            "searchSourceJSON": "{\"index\":\"eb4d54b0-6fa9-11e8-8161-3b4280559eb3\",\"filter\":[],\"query\":{\\\"query\\\":\\\"\\\",\\\"language\\\":\\\"lucene\\\"}}"
34        }
35    }
36 },
37 {
38     "_id": "25a7f140-6f20-11e8-a0fb-51f0eb991705",
39     "_type": "visualization",
40     "_source": {
41         "title": "[nginx] tag-cloud",
42         "visState": "{\"title\":\"[nginx] tag-cloud\",\"type\":\"tagcloud\",\"params\":{\"scale\":\"linear\",\"orientation\":\"single\",\"minFontSize\":18,\"maxFontSize\":72},\"uiStateJSON\": {},\"description\": "",\"version\": 1,
43        "kibanaSavedObjectMeta": {
44            "searchSourceJSON": "{\"index\":\"eb4d54b0-6fa9-11e8-8161-3b4280559eb3\",\"filter\":[],\"query\":{\\\"query\\\":\\\"\\\",\\\"language\\\":\\\"lucene\\\"}}"
45        }
46    }
47 }
```

Visualization export

visualization을 백업 받으면 위와 같은 json 파일이 생기는데, 각 visualization이 어떻게 구성되었는지에 대한 정보를 담고 있다



즉, dashboard UI를 온전히 백업 받으려면 dashboard와 visualization을 모두 백업 받아야 한다

Dashboard/Visualization import

visualization 삭제

The screenshot shows the Kibana interface with the 'Saved Objects' tab selected. A search bar at the top contains the query 'nginx'. Below the search bar, there are three tabs: 'Dashboards (2)', 'Searches (1)', and 'Visualizations (12)'. The 'Visualizations' tab is active. On the right side of the screen, there are two buttons: 'Export Everything' and 'Import'. A modal dialog box is centered over the list of visualizations. The dialog has a title 'Delete selected visualizations?' and a message 'You can't recover deleted visualizations.' It contains two buttons: 'Cancel' and a highlighted 'Delete' button.

Index Patterns Saved Objects Advanced Settings

Edit Saved Objects

From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. Typically objects are only modified via their associated application, which is probably what you should use instead of this screen. Each tab is limited to 100 results. You can use the filter to find objects not in the default list.

Export Everything Import

Dashboards (2) Searches (1) Visualizations (12)

nginx

Delete Export

✓ Title
✓ [nginx] area chart
✓ [nginx] coordinate maps
✓ [nginx] Data Table
✓ [nginx] Goal
✓ [nginx] heat map
✓ [nginx] horizontal bar
✓ [nginx] markdown
✓ [nginx] metric
✓ [nginx] pie chart
✓ [nginx] region maps
✓ [nginx] tag-cloud
✓ [nginx] Timelion

12 selected

Delete selected visualizations?
You can't recover deleted visualizations.
Cancel Delete

dashboard 삭제

Management / Kibana

Index Patterns Saved Objects Advanced Settings

Edit Saved Objects

From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. Typically objects are only modified via their associated application, which is probably what you should use instead of this screen. Each tab is limited to 100 results. You can use the filter to find objects not in the default list.

Dashboards (2) Searches (1) Visualizations (0)

nginx

Title

nginx

nginx-higee

1 selected

Delete selected dashboards?

You can't recover deleted dashboards.

[Cancel](#) [Delete](#)

[Export Everything](#) [Import](#)

The screenshot shows the Kibana Management interface under the 'Saved Objects' tab. A search bar at the top contains 'nginx'. Below it, there are three tabs: 'Dashboards (2)', 'Searches (1)', and 'Visualizations (0)'. Under the 'Dashboards' tab, a list shows three items: 'Title' (unchecked), 'nginx' (unchecked), and 'nginx-higee' (checked). A message '1 selected' is displayed below the list. A modal dialog box is centered on the page, asking 'Delete selected dashboards?'. It includes a warning 'You can't recover deleted dashboards.' and two buttons: 'Cancel' and 'Delete'. Above the modal, there are links for 'Export Everything' and 'Import'. On the far left, a vertical sidebar displays icons for various Kibana features: Kibana logo, Index Patterns, Visualizations, Dashboards, Settings, and a play button.

Dashboard import

The screenshot shows the Kibana Management interface with the following steps highlighted:

- 1. 선택**: A hand icon points to the 'Saved Objects' tab in the top navigation bar.
- 2. Saved Objects 선택**: A hand icon points to the 'Saved Objects' tab in the top navigation bar.
- 3. Import 선택**: A hand icon points to the 'Import' button in the top right corner.
- 4. {id}_dashboard.json 선택**: A hand icon points to the search bar containing 'nginx-higee'.
- 5. No, prompt for each object 선택**: A hand icon points to the 'No, prompt for each object' button in a modal dialog.

The interface includes tabs for Dashboards (0), Searches (0), and Visualizations (0). It also features 'Export Everything' and 'Import' buttons. A modal dialog asks 'Automatically overwrite all saved objects?' with options 'No, prompt for each object' (selected) and 'Yes, overwrite all objects'.

Dashboard import

Management / Kibana

Index Patterns [Saved Objects](#) Advanced Settings

Edit Saved Objects

From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. Typically objects are only modified via their associated application, which is probably what you should use instead of this screen. Each tab is limited to 100 results. You can use the filter to find objects not in the default list.

Dashboards (2) Searches (1) Visualizations (0)

nginx

Delete Export

<input type="checkbox"/> Title
<input type="checkbox"/> nginx
<input type="checkbox"/> nginx-higee



The screenshot shows the 'Saved Objects' section of the Kibana Management interface. It displays three tabs: Dashboards (2), Searches (1), and Visualizations (0). A search bar at the top contains the text 'nginx'. Below the search bar, there are three items in a list: 'Title', 'nginx', and 'nginx-higee'. The 'nginx-higee' item is highlighted with a red dashed box. A pink hand icon points to this highlighted row. At the top right, there are 'Export Everything' and 'Import' buttons. The 'Import' button is highlighted with a blue border.

한 번 지웠던 nginx-higee가 제대로 Import 된 걸 확인할 수 있다

Import한 Dashboard에 가보면

Dashboard / nginx-higee Full screen Share Clone Edit Auto-refresh < ⏴ Last 30 days >

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

Could not locate that visualization (id: 57d11570-6f2a-11e8-a0fb-51f0eb991705)

Could not locate that visualization (id: fe7b9a30-6f20-11e8-a0fb-51f0eb991705)

Could not locate that visualization (id: 25a7f140-6f20-11e8-a0fb-51f0eb991705)

Could not locate that visualization (id: cfbbc570-6f26-11e8-a0fb-51f0eb991705)

Inquery search

Import한 Dashboard에 가보면

Dashboard / nginx-higee Full screen Share Clone Edit Auto-refresh Last 30 days Add a filter + Uses lucene query syntax

Search... (e.g. status:200 AND extension:PHP)

Not located visualization (id: fe7b9a30-6f20-11e8-a0fb-51f0eb991705)

Not located visualization (id: 25a7f140-6f20-11e8-a0fb-51f0eb991705)

Not located visualization (id: cfbcc570-6f26-11e8-a0fb-51f0eb991705)

개별 **Visualization**들을 Import 하지 않았기에 위와 같이 에러가 뜬다.

Could not locate that visualization (id: fe7b9a30-6f20-11e8-a0fb-51f0eb991705)

Could not locate that visualization (id: 25a7f140-6f20-11e8-a0fb-51f0eb991705)

Could not locate that visualization (id: cfbcc570-6f26-11e8-a0fb-51f0eb991705)

Visualization import

The screenshot shows the Kibana interface for managing saved objects. A vertical sidebar on the left contains icons for management, dashboards, searches, visualizations, and other settings. The main area is titled "Management / Kibana" and has tabs for "Index Patterns", "Saved Objects" (which is selected and highlighted with a pink border), and "Advanced Settings". Below these tabs is a section titled "Edit Saved Objects" with a sub-section for "Visualizations". There are three tabs at the top of this section: "Dashboards (2)", "Searches (1)", and "Visualizations (0)". On the right side of the interface, there are buttons for "Export Everything" and "Import". A pink callout bubble labeled "1. 선택" points to the "Import" button. Another pink callout bubble labeled "2. Saved Objects 선택" points to the "Saved Objects" tab. A third pink callout bubble labeled "3. Import 선택" points to the "Import" button again. A fourth pink callout bubble labeled "4. {id}_visualization.json 선택" points to the "Import" button. A fifth pink callout bubble labeled "5. No, prompt for each object 선택" points to the "No, prompt for each object" button in a modal dialog. The dialog asks "Automatically overwrite all saved objects?" with two options: "No, prompt for each object" (highlighted with a pink border) and "Yes, overwrite all objects".

👉 5. No, prompt for each object 선택

Import한 Dashboard에 다시 가보면

Dashboard / nginx-higee Full screen Share Clone Edit Auto-refresh < ⏴ Last 30 days >

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

[nginx] markdown

Nginx Access.Log Dashboard

```
66.249.82.131 - - [13/Jun/2018:17:01:02 +0000] "GET /ui/favicons/favicon-16x16.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
118.221.38.242 - - [13/Jun/2018:17:01:14 +0000] "POST /api/console/proxy?path=_aliases&method=GET HTTP/1.1" 200 107 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
118.221.38.242 - - [13/Jun/2018:17:01:14 +0000] "POST /api/console/proxy?path=_mapping&method=GET HTTP/1.1" 200 974 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
66.249.82.131 - - [13/Jun/2018:17:01:16 +0000] "GET /ui/favicons/favicon-32x32.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
66.249.82.129 - - [13/Jun/2018:17:01:17 +0000] "GET /ui/favicons/favicon-16x16.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36"
```

[nginx] heat map

[nginx] tag-cloud

Other
Mac OS X
Windows 10
Windows 7
iOS

[nginx] metric

77,710 req

Inbox search

Filtering by Field 

Dashboard를 만들었는데 원하는 조건의 데이터만 보고 싶다면?

Dashboard 선택

Dashboard

shopping		+	1-1 of 1	<	>
Name ↑	Description	Actions			
<input type="checkbox"/> shopping	선택		Edit	<	>
			1-1 of 1	<	>

Dashboard를 확인하자



Time Picker

Dashboard / shopping

Full screen Share Clone Edit Auto-refresh < ⏪ Last 30 days ⏩

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

sjyoun_week1_markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

125 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map

Count
1~9.2
9.2~17.4
17.4~25.6
25.6~33.8
33.8~42

© OpenStreetMap contributors, Elastic Maps Service

티몬
11번가 GS샵
쿠팡 옥션
g마켓 위메프

전체 Documents 중에서 **Time Picker** 구간에 속한 Documents만 보여준다.

만약에 다른 조건을 추가하고 싶다면? 예를 들어, “**전라도**” 데이터만 보고 싶으면 어떻게 할까?

원하는 조건의 데이터만 조회하기 위해 필터를 적용했다

Dashboard / shopping

Full screen Share Clone Edit Auto-refresh < Last 30 days >

Search... (e.g. status:200 AND extension:PHP)

Uses lucene query syntax

전라도 + “경상도”라는 필터가 적용됐다

[shopping] metrics

sjyoun_week1_markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

! 16 전체 데이터

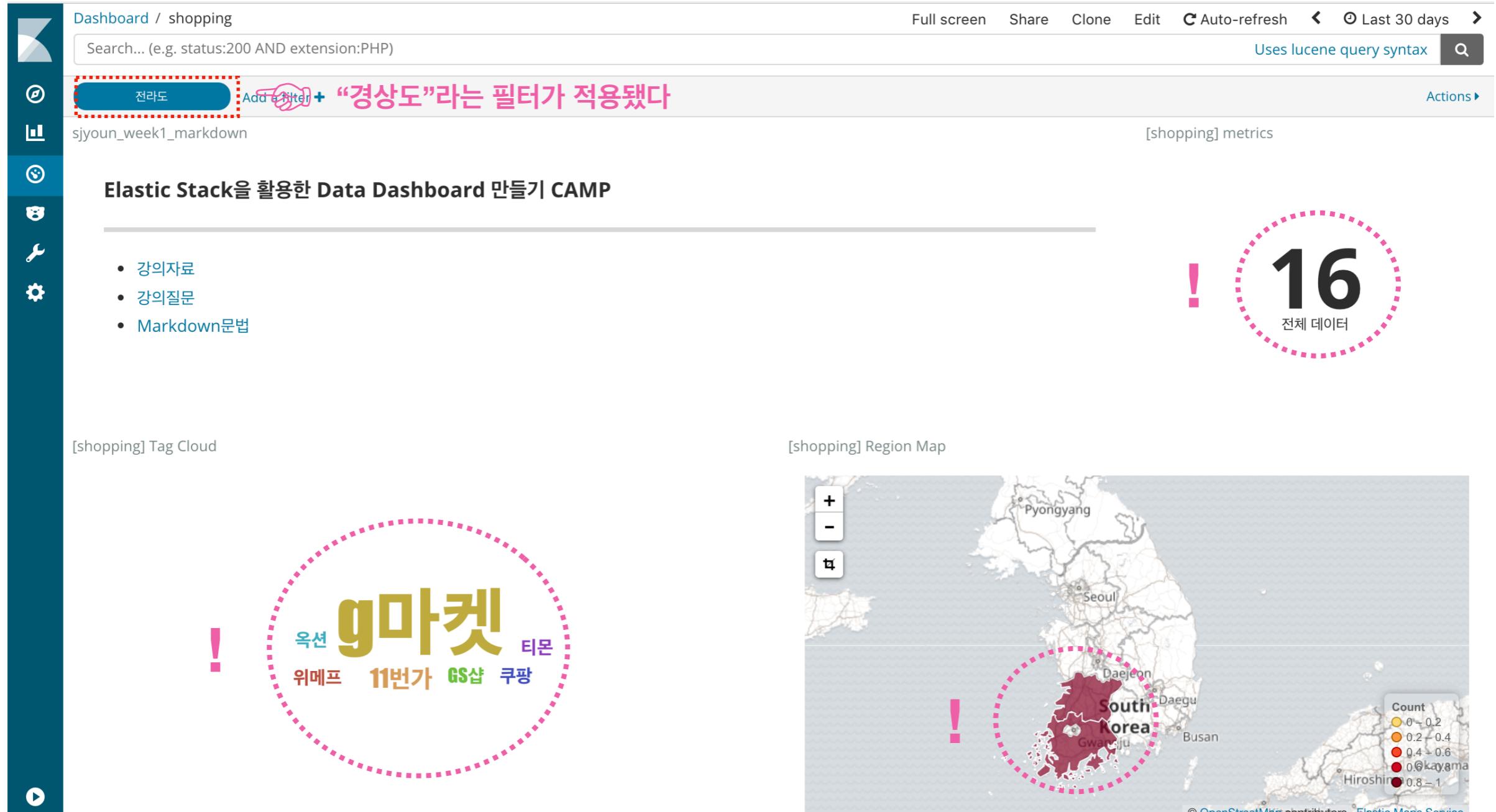
[shopping] Tag Cloud

g마켓 옥션 위메프 11번가 GS샵 쿠팡 티몬

[shopping] Region Map

Pyongyang Seoul Daejeon Daegu Busan Gwangju South Korea

Count
0 ~ 0.2
0.2 ~ 0.4
0.4 ~ 0.6
0.6 ~ 1
© OpenStreetMap contributors, Elastic Maps Service



Filter를 이용하면 **특정 조건을 만족하는**
데이터만 선별하여 Dashboard에 시각화할 수 있다.
그렇다면 어떻게 사용할까?

Filter를 실행하자

Dashboard / shopping

Full screen Share Clone Edit Auto-refresh < Last 30 days >

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter + 선택

sjyoun_week1_markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

125
전체 데이터

[shopping] Tag Cloud

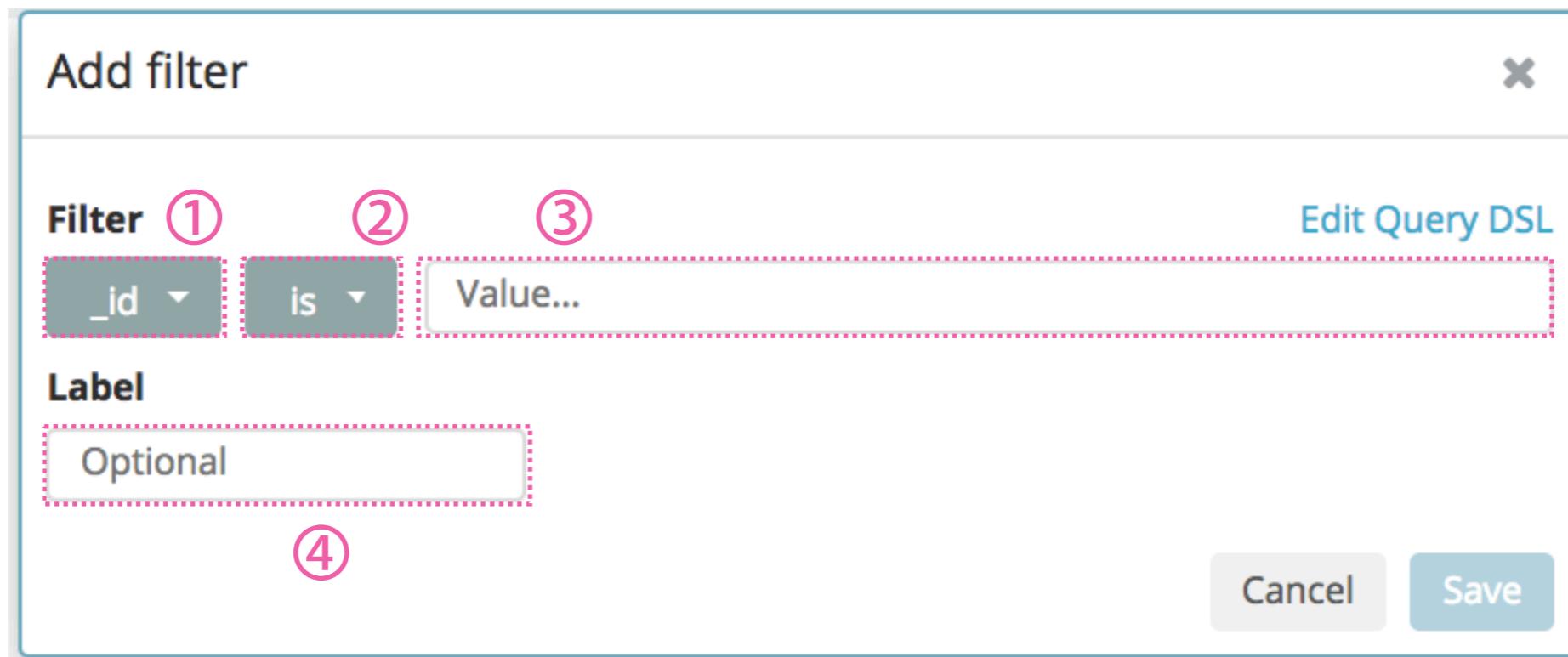
[shopping] Region Map

티몬
GS샵
옵션
위메프

쿠팡 11번가 g마켓

© OpenStreetMap contributors, Elastic Maps Service

Filter의 사용법을 익히자



- ① Filter 적용할 Field 선택
- ② 적용할 Operator 선택 (다음 페이지 참조)
- ③ Filter에 적용하려는 Value 입력
- ④ (여러 Filter 구분하기 위한) 이름 입력

Operator 설명

Operator	역할
is	Field의 Value가 입력한 값과 일치하는 Documents 선택
is not	Field의 Value가 입력한 값과 일치하지 않는 Documents 선택
is one of	Field의 Value가 입력한 값 중에 존재하는 Documents 선택
is not one of	Field의 Value가 입력한 값 중에 존재하지 않는 Documents 선택
exists	Field가 적어도 한 개의 non-null 값을 가지는 Documents 선택
does not exist	Field가 존재하지 않거나 null 값만 가지는 Documents 선택
is between	Field의 Value가 입력한 값 사이에 존재하는 Documents 검색
is not between	Field의 Value가 입력한 값 사이에 존재하지 않는 Documents 검색

실제로 Filter를 적용해보자

Operator - is

Edit filter



Filter

[Edit Query DSL](#)

결제카드 ▾

is ▾

우리



Label

우리카드



Cancel

Save

Operator - is

Dashboard / shopping

Full screen Share Clone Edit Auto-refresh < Last 30 days >

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax Search

우리카드 Add a filter + Actions ▶

sjyoun_week1_markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

38
전체 데이터

[shopping] Tag Cloud

[shopping] Region Map

티몬
쿠팡 11번가 옥션 GS샵
위메프 g마켓

Count
1-3.6
3.6-6.2
6.2-8.8
8.8-11.4
11.4-14

© OpenStreetMap contributors, Elastic Maps Service

Operator - **is one of**

Edit filter ×

Filter [Edit Query DSL](#)

구매사이트 ▾ is one of ▾ 11번가 ✕ 옵션 ✕ 쿠팡 ✕

Label

즐겨찾기

✖ Cancel Save

Operator - is one of

Dashboard / shopping

Full screen Share Clone Edit Auto-refresh < ⏪ Last 30 days >

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

즐겨찾기 Add a filter + Actions ▶

sjyoun_week1_markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

20
전체 데이터

[shopping] Tag Cloud

[shopping] Region Map

A choropleth map of South Korea showing data distribution across regions. The map uses a color scale from light yellow (low count) to dark red (high count). Major cities labeled include Pyongyang, Seoul, Daegu, Busan, Gwangju, Daejeon, and Hiroshima. A legend titled 'Count' is provided on the right, showing the following ranges:

Count Range
1 ~ 2.4
2.4 ~ 3.8
3.8 ~ 5.2
5.2 ~ 6.6
6.6 ~ 8

© OpenStreetMap contributors, Elastic Maps Service

11번가
쿠팡 옵션

Operator - is between

Edit filter ✖

Filter [Edit Query DSL](#)

상품가격 ▼ is between ▼ 10000
20000 ^ v

Label

가격 : 10,000~20,000

✖ Cancel Save

Operator - **is between**

Dashboard / shopping

Full screen Share Clone Edit Auto-refresh < Last 30 days >

Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

가격 : 10,000~20,000 Add a filter + Actions ▾

-Visualize week1_markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

• 강의자료
• 강의질문
• Markdown문법

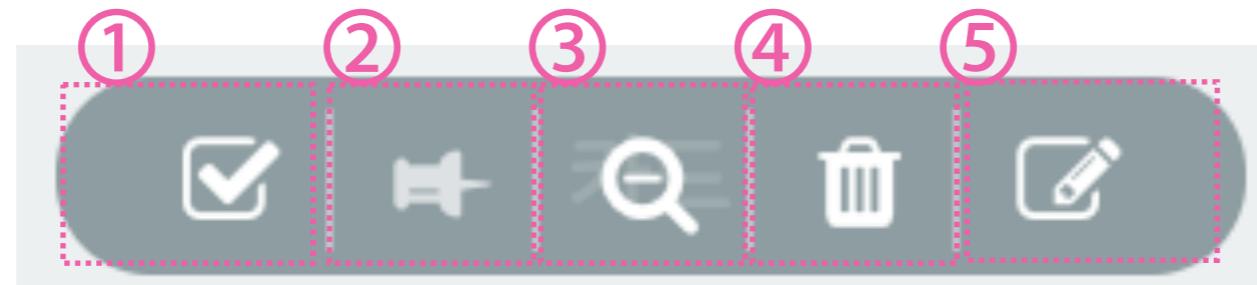
17 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map

Pyongyang
Seoul
Daejeon
Daegu
Busan
Gwangju
Hiroshima
South Korea
Count
1 ~ 2.4
2.4 ~ 3.8
3.8 ~ 5.2
5.2 ~ 6.6
6.6 ~ 8

필터에 마우스오버하면...



안내

- ① 필터 적용 <=> 필터 적용 해제
- ② 필터 고정 (Discover, Visualize, Dashboard)
- ③ 필터 효과 적용 <=> 필터 효과 반대 적용
- ④ 필터 삭제
- ⑤ 필터 수정

예제4 - 아래와 같은 Filter를 Dashboard에 적용해보자

Dashboard : nginx-*
Time Range : Past 30 days

문제	operator
nginx.access.response_code가 200인 Doc 필터링	is
nginx.access.method가 GET 또는 POST인 Doc 필터링	is one of
nginx.access.geoip.region_name가 non-null값만 가지는 Doc 필터링	exists
nginx.access.geoip.city_name이 Seoul이면서 nginx.access.user_agent.name이 Chrome인 Doc 필터링	is
nginx.access.geoip.city_name이 Seoul이거나 nginx.access.user_agent.name이 Chrome인 Doc 필터링	?
요일_local이 Sunday인 Doc 필터링	is
nginx.access.geoip.country_name 가 “Republic of”로 시작하는 Doc 필터링	?
nginx.access.geoip.continent_code가 “AS”와 유사한 Doc 필터링	?

Lucene Query 

Filter는 사용하기 간단하나 기능이 제한적이다
그렇다면 다른 방법이 더 있을까?

우선 Dashboard를 열자

Dashboard

A screenshot of a dashboard application. On the left, there is a vertical sidebar with several icons: a blue square at the top, followed by a magnifying glass, a person icon, a bar chart, a clock, a gear, and a play button at the bottom. The main area has a white background. At the top, there is a search bar containing the text "shopping". To the right of the search bar is a blue button with a white plus sign. Further to the right, it says "1-1 of 1" and has navigation arrows. Below the search bar is a table with three columns: "Name ↑", "Description", and "Actions". There is one row in the table. The "Name" column contains a checkbox next to the word "shopping". The "Description" column is empty. The "Actions" column contains a "Edit" link. A pink hand icon with the text "선택" (Select) is overlaid on the checkbox in the "Name" column. The entire screenshot is framed by a thin gray border.

Name ↑	Description	Actions
<input type="checkbox"/> shopping		Edit

Query Bar를 확인하자

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh This month >

* Uses lucene query syntax

Add a filter + [shopping] markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

• 강의자료
• 강의질문
• Markdown문법

Query Bar 95 전체 데이터

[shopping] Tag Cloud [shopping] Region Map

11번가 옥션 g마켓 GS샵 티몬 쿠팡 위메프

Pyongyang Seoul Daejeon Gwangju Busan South Korea Hiroshima Okayama

Count
1 ~ 6.8
6.8 ~ 12.6
12.6 ~ 18.4
18.4 ~ 24.2
24.2 ~ 30

© OpenStreetMap contributors, Elastic Maps Service

Query Bar를 확인하자

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh This month  Uses lucene query syntax

Add a filter + [shopping] markdown [shopping] metrics 

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

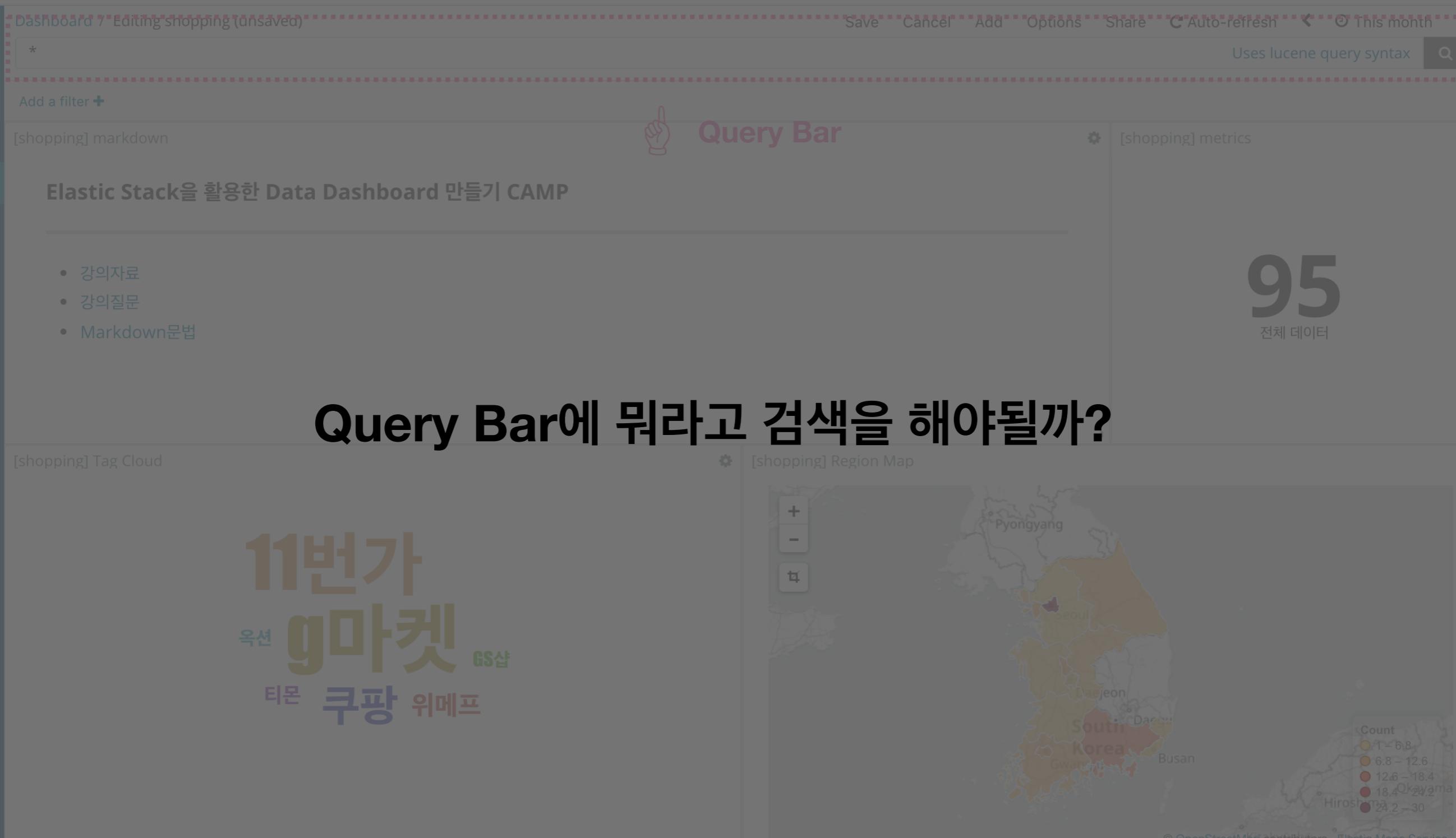
- 강의자료
- 강의질문
- Markdown문법

95 전체 데이터

Query Bar에 뭐라고 검색을 해야될까?

[shopping] Tag Cloud [shopping] Region Map 

11번가 옥션 g마켓 GS샵 티몬 쿠팡 위메프



Lucene Query의 사용법을 익하자

종류	기능	Query 예시
Keyword 검색	Field에 상관없이 검색어와 일치하는 Doc 검색	여성
Field Match 검색	특정 Field 값이 검색어와 일치하는 Doc 검색	고객성별:여성
Exact Field Match 검색	특정 Field 값이 검색어와 정확히 일치하는 Doc 검색	배송메모:"상품 이상"
Must be 검색	특정 Field가 exists한 Doc 검색	_exists_:구매사이트
Term 검색	특정 Field 값이 검색어 중 하나라도 일치하는 Doc 검색	상품분류: (니트 코트)
Fuzzy 검색	검색어와 유사한 Doc 검색	경상복도~
Proximity 검색	검색어의 순서를 변경해서 Doc 검색	배송메모: "내에 시간 배송 못함"~2
Numeric Value 검색	특정 Field 값이 입력값보다 크거나 (작은) Doc 검색	상품가격:>5000
Range 검색	특정 Field 값이 입력 범위 내에 존재하는 Doc 검색	고객나이: [10 TO 30]
Wildcard ? 검색	Wildcard ? (한글자)를 활용해서 Doc 검색	서?특별시
Wildcard * 검색	Wildcard * (생략 혹은 그 이상)를 활용해서 Doc 검색	상품*:셔츠
OR 연산	여러 검색 조건들을 OR로 묶어 검색 수행	고객성별:여성 OR 상품분류:셔츠
AND 연산	여러 검색 조건들을 AND로 묶어 검색 수행	고객성별:여성 AND 상품분류:셔츠
NOT 연산	뒤이어 오는 조건을 부정해서 검색 수행	NOT 구매사이트:옵션
+ 연산	바로 뒤에 오는 조건을 만족하는 Doc 검색	+예약여부:예약
- 연산	바로 뒤에 오는 조건을 만족하지 않는 Doc 검색	-구매사이트:11번가

Search Type - Keyword

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh < This month >

우리 Uses lucene query syntax 

Add a filter + [shopping] markdown [shopping] metrics

1. 입력 2. 클릭 

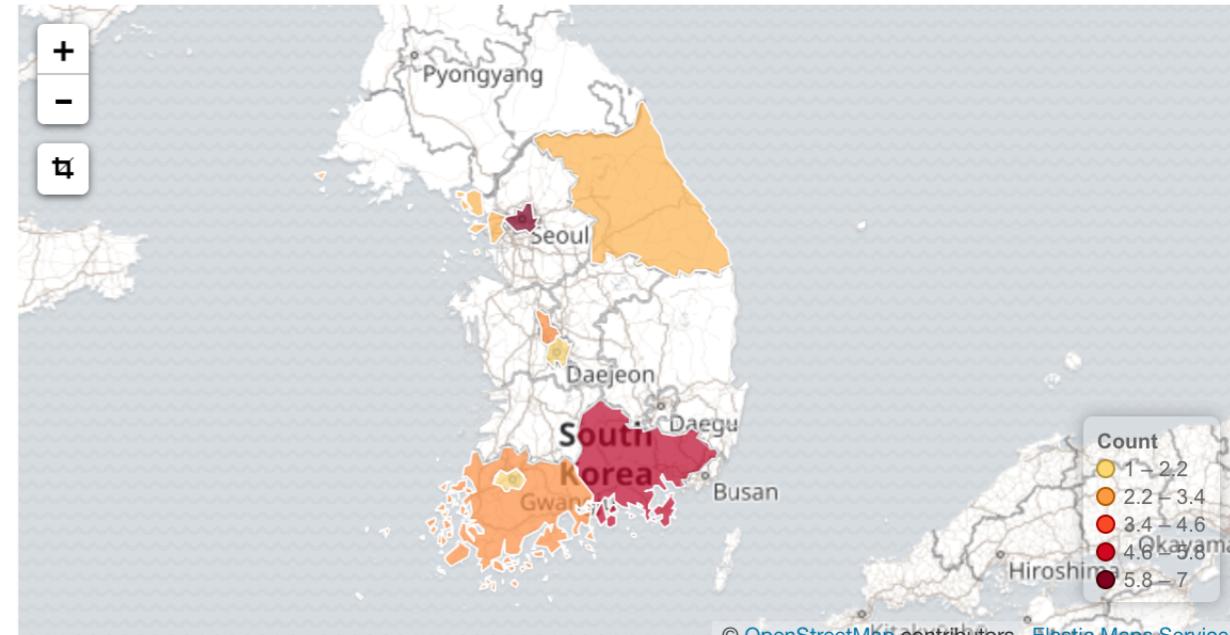
Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

25 전체 데이터

[shopping] Tag Cloud [shopping] Region Map

g마켓 GS샵
옵션 티몬 쿠팡
11번가 위메프



Count
1 → 2.2
2.2 → 3.4
3.4 → 4.6
4.6 → 5.8
5.8 → 7

© OpenStreetMap contributors, Elastic Maps Service

Search Type - Field Match

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh < This month >

결제카드:우리 Uses lucene query syntax 

Add a filter + [shopping] markdown [shopping] metrics []

1. 입력 2. 클릭 

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

25 전체 데이터

[shopping] Tag Cloud [shopping] Region Map 

옵션 티몬 g마켓 GS샵 쿠팡 11번가 위메프

Pyongyang Seoul Daejeon Daegu Gwangju Busan Hiroshima South Korea © OpenStreetMap contributors, Elastic Maps Service

Count
1 ~ 2.2
2.2 ~ 3.4
3.4 ~ 4.6
4.8 ~ 5.8
5.8 ~ 7

Search Type - Exact Field Match

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh < This month >

배송메모:"상품 이상" Uses lucene query syntax 

Add a filter + [shopping] markdown [shopping] metrics 

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

1. 입력  2. 클릭 

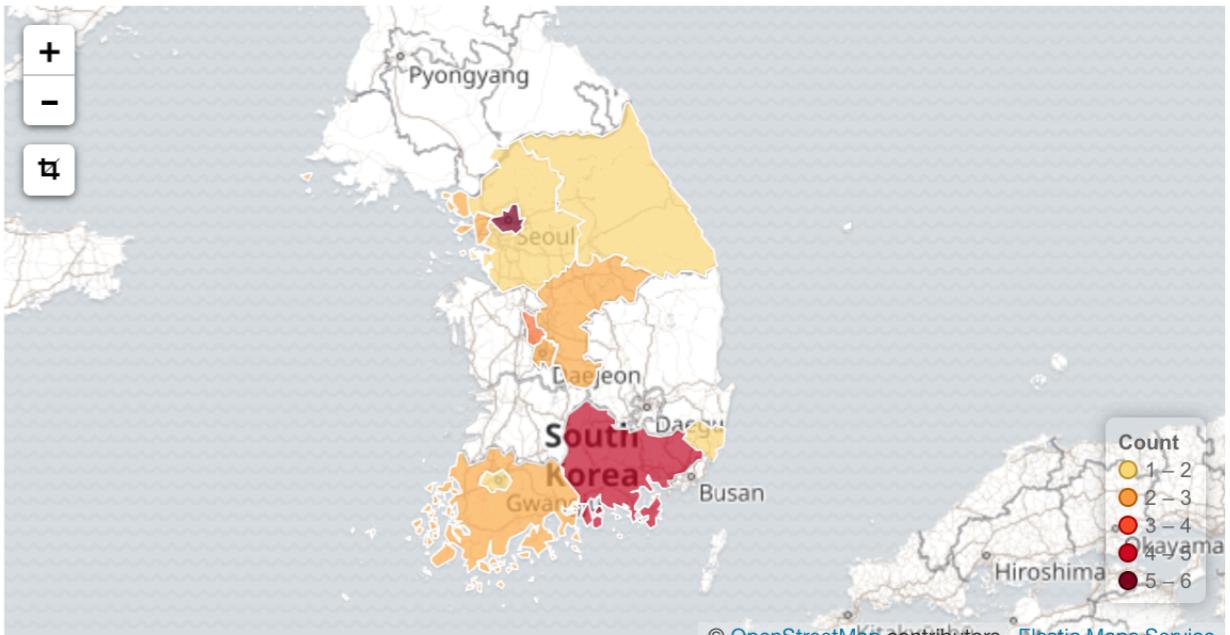
- 강의자료
- 강의질문
- Markdown문법

26 전체 데이터

[shopping] Tag Cloud

쿠팡
위메프 11번가 옥션
g마켓 GS샵

[shopping] Region Map



Count
1 – 2
2 – 3
3 – 4
4 – 5
5 – 6

© OpenStreetMap contributors, Elastic Maps Service

Search Type - Term

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh < This month >

상품분류: ("니트" "코트") Uses lucene query syntax 

Add a filter + [shopping] markdown [shopping] metrics

1. 입력  2. 클릭 

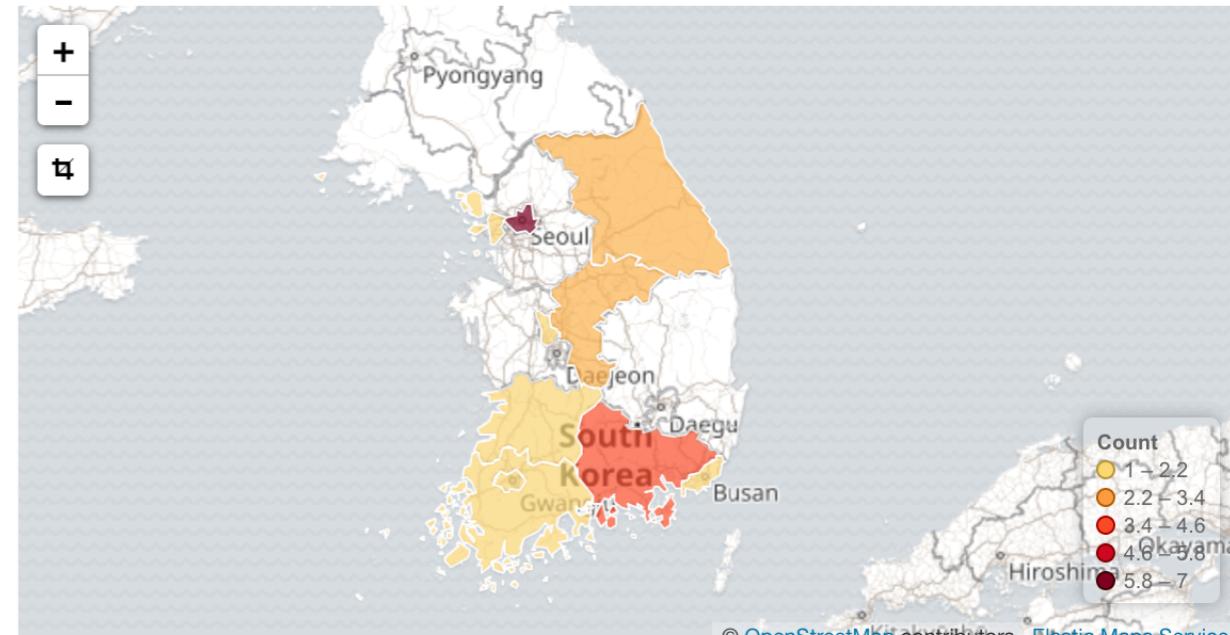
Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

21 전체 데이터

[shopping] Tag Cloud [shopping] Region Map

11번가 쿠팡
위메프 g마켓 티몬



Count
1 ~ 2.2
2.2 ~ 3.4
3.4 ~ 4.6
4.6 ~ 5.8
5.8 ~ 7

Pyongyang Seoul Daejeon Daegu Busan Gwangju South Korea Hiroshima Okinawa © OpenStreetMap contributors, Elastic Maps Service

Search Type - Fuzzy

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh < This month >

고객주소_시도:전라도~1 Uses lucene query syntax 

Add a filter + [shopping] markdown [shopping] metrics

1. 입력  2. 클릭 

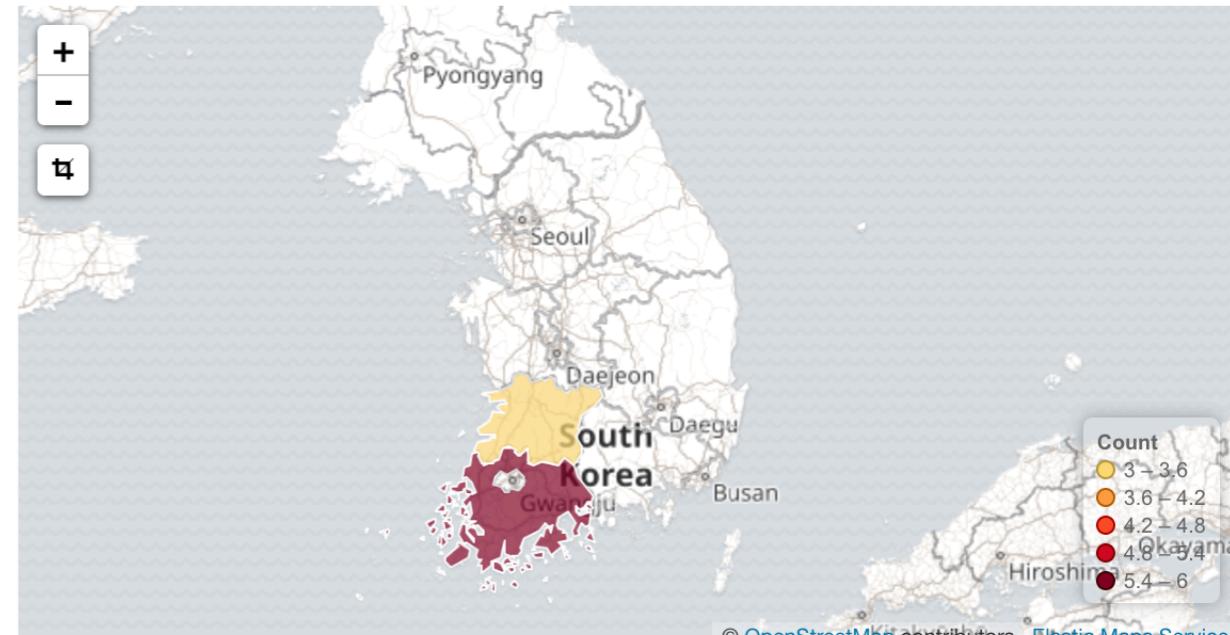
Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

9 전체 데이터

[shopping] Tag Cloud [shopping] Region Map

g마켓 티몬 옥션 위메프 쿠팡



Count
3 ~ 3.6
3.6 ~ 4.2
4.2 ~ 4.8
4.8 ~ 5.4
5.4 ~ 6

© OpenStreetMap contributors, Elastic Maps Service

Search Type - Proximity

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh < This month >

배송메모: "내에 시간 배송 못함"~2 Uses lucene query syntax 

Add a filter + 1. 입력  2. 클릭 

[shopping] markdown [shopping] metrics

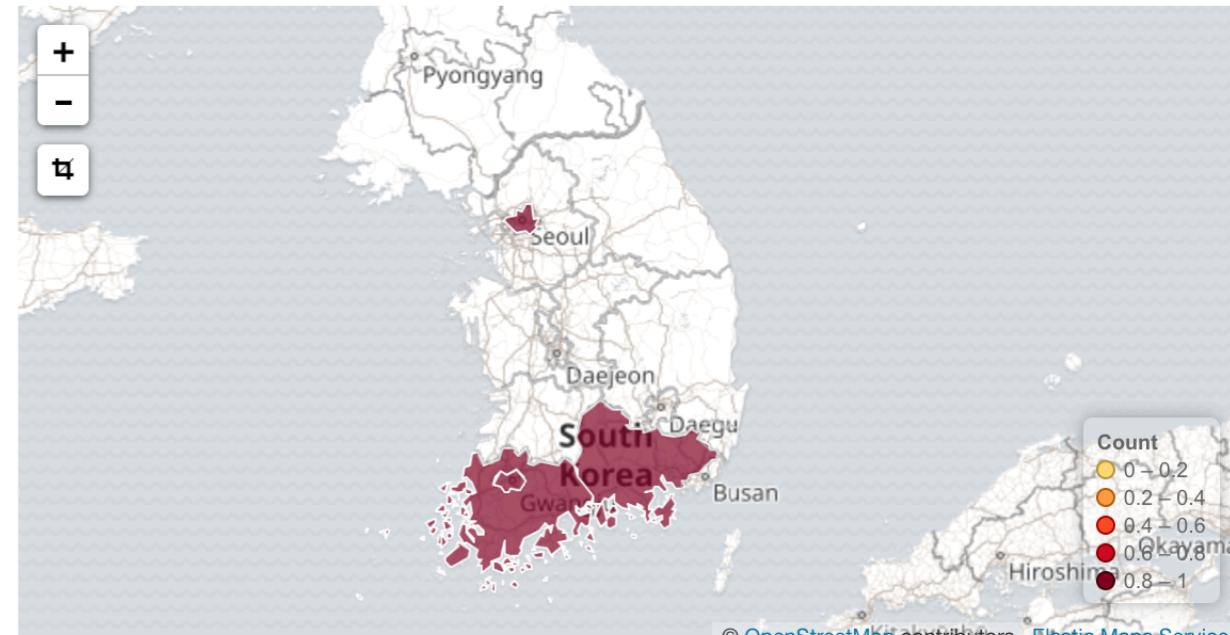
Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

4 전체 데이터

[shopping] Tag Cloud [shopping] Region Map

쿠팡 GS샵 g마켓 티몬



Count
0 ~ 0.2
0.2 ~ 0.4
0.4 ~ 0.6
0.6 ~ 0.8
0.8 ~ 1

© OpenStreetMap contributors, Elastic Maps Service

Search Type - Numeric

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh < This month >

상품가격:>5000 Uses lucene query syntax 

Add a filter +

[shopping] markdown

1. 입력  2. 클릭 

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

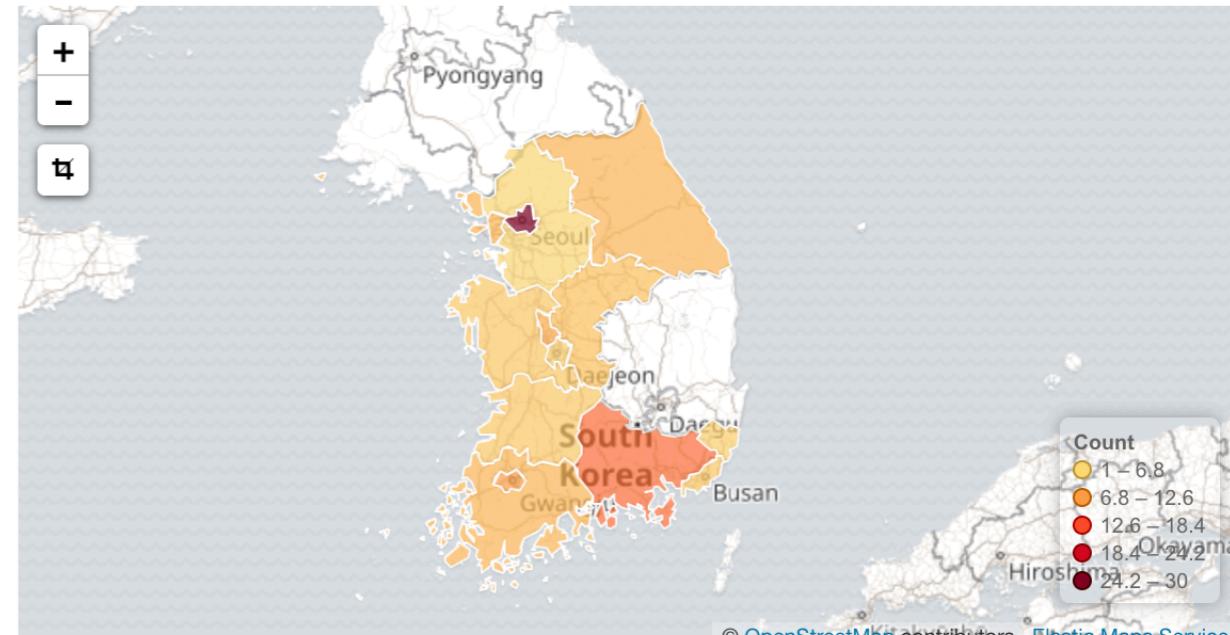
- 강의자료
- 강의질문
- Markdown문법

92 전체 데이터

[shopping] Tag Cloud

옵션
위메프 11번가 GS샵 티몬
g마켓 쿠팡

[shopping] Region Map



Count
1 – 6.8
6.8 – 12.6
12.6 – 18.4
18.4 – 24.2
24.2 – 30

© OpenStreetMap contributors, Elastic Maps Service

Search Type - Range

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh < This month >

고객나이: [10 TO 30]

Uses lucene query syntax



Add a filter +

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법



1. 입력



2. 클릭

[shopping] metrics

36
전체 데이터

[shopping] Tag Cloud

옵션
티몬

g마켓 위메프
쿠팡 11번가

[shopping] Region Map



Search Type - Wildcard

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh < This month >

고객주소_시도:서?특별시 Uses lucene query syntax 

Add a filter + [shopping] markdown [shopping] metrics 

1. 입력  2. 클릭 

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

30 전체 데이터

[shopping] Tag Cloud

쿠팡
11번가
g마켓 옵션
위메프 GS샵

[shopping] Region Map



Count
0 ~ 0.2
0.2 ~ 0.4
0.4 ~ 0.6
0.6 ~ 0.8
0.8 ~ 1

© OpenStreetMap contributors, Elastic Maps Service

Search Type - Wildcard

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh < This month >

상품*:셔츠 Uses lucene query syntax 

Add a filter + 1. 입력  2. 클릭 

[shopping] markdown [shopping] metrics

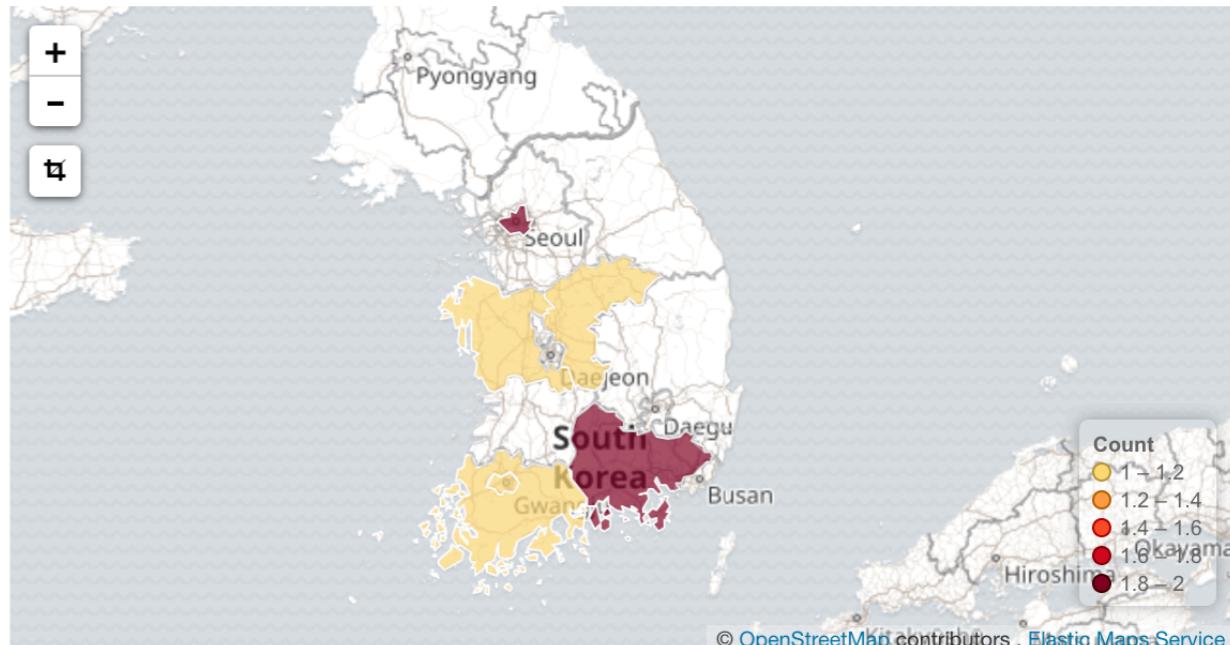
Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

8 전체 데이터

[shopping] Tag Cloud [shopping] Region Map

g마켓
옵션 쿠팡 티몬



Count
1 ~ 1.2
1.2 ~ 1.4
1.4 ~ 1.6
1.6 ~ 1.8
1.8 ~ 2

© OpenStreetMap contributors, Elastic Maps Service

Search Type - OR

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh < This month >

고객성별:여성 OR 상품분류:셔츠

Uses lucene query syntax



Add a filter +

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법



1. 입력



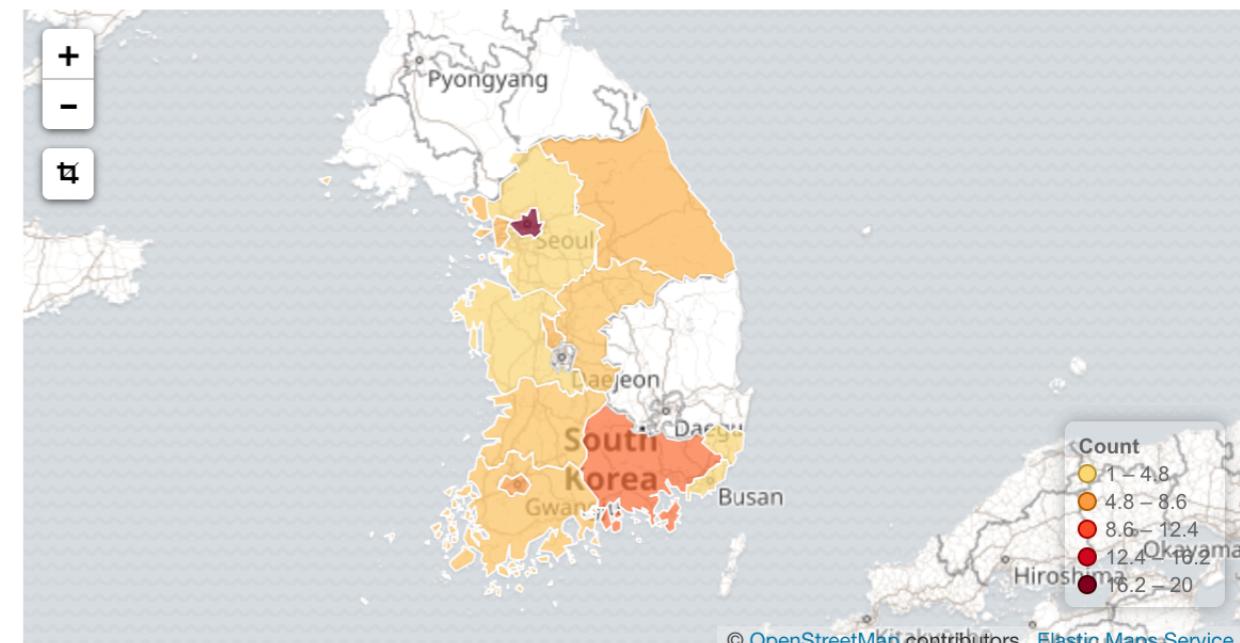
2. 클릭

60
전체 데이터

[shopping] Tag Cloud

티몬
쿠팡 g마켓
11번가 옥션
위메프
GS샵

[shopping] Region Map



Search Type - AND

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh < This month >

고객성별:여성 AND 상품분류:셔츠 Uses lucene query syntax 

Add a filter + [shopping] markdown 1. 입력 [shopping] metrics 2. 클릭

[shopping] Tag Cloud [shopping] Region Map

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

전체 데이터 6

g마켓 옵션 쿠팡 티몬

© OpenStreetMap contributors, Elastic Maps Service

Search Type - NOT

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh < This month >

NOT 구매사이트:옵션 Uses lucene query syntax 

Add a filter + [shopping] markdown [shopping] metrics 

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

1. 입력  2. 클릭 

- 강의자료
- 강의질문
- Markdown문법

89 전체 데이터

[shopping] Tag Cloud

11번가 g마켓 GS샵
티몬 쿠팡 위메프

[shopping] Region Map



Count
1 – 6.2
6.2 – 11.4
11.4 – 16.6
16.6 – 21.8
21.8 – 27

© OpenStreetMap contributors, Elastic Maps Service

Search Type

Dashboard / Editing shopping (unsaved) Save Cancel Add Options Share Auto-refresh < This month >

+예약여부:예약 Uses lucene query syntax 

Add a filter +

[shopping] markdown 1. 입력  2. 클릭 

[shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

12 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map

Pyongyang Seoul Daejeon Daegu Gwangju Busan Hiroshima South Korea © OpenStreetMap contributors, Elastic Maps Service

Count
1 – 2
2 – 3
3 – 4
4 – 5
5 – 6

11번가 GS샵 옵션 g마켓 쿠팡

Search Type -

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh < This month >

-구매사이트:11번가

Uses lucene query syntax



Add a filter +



1. 입력

[shopping] markdown

[shopping] metrics

2. 클릭 

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

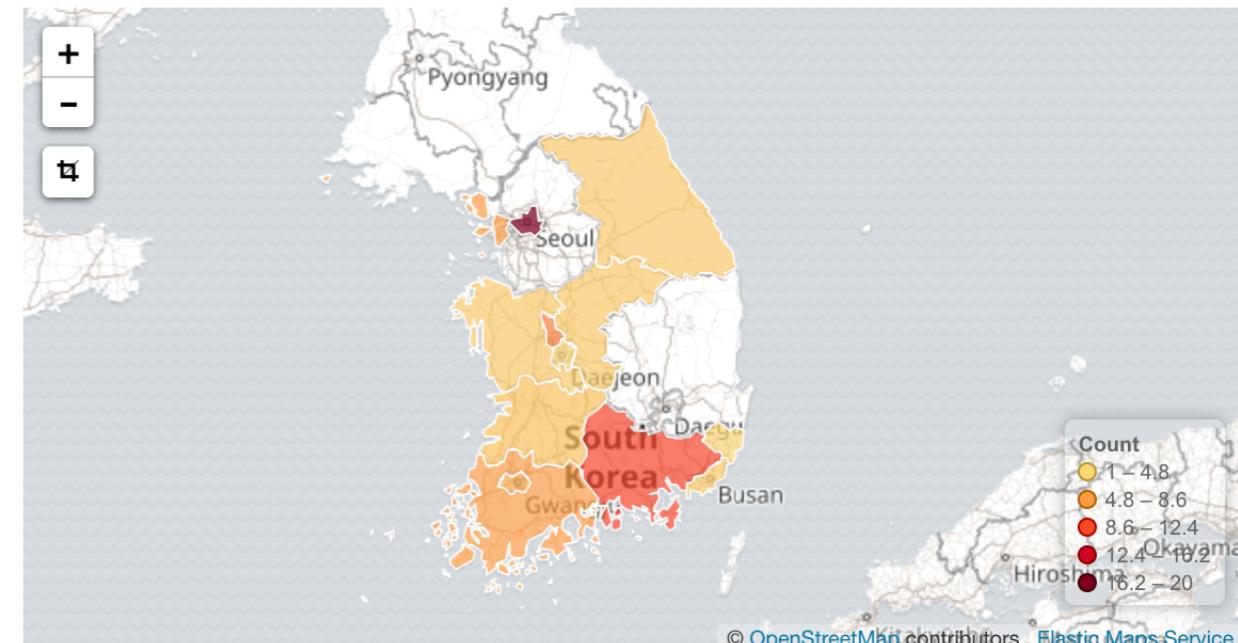
- 강의자료
- 강의질문
- Markdown문법

70
전체 데이터

[shopping] Tag Cloud

옵션 **g마켓** GS샵
티몬 쿠팡 위메프

[shopping] Region Map



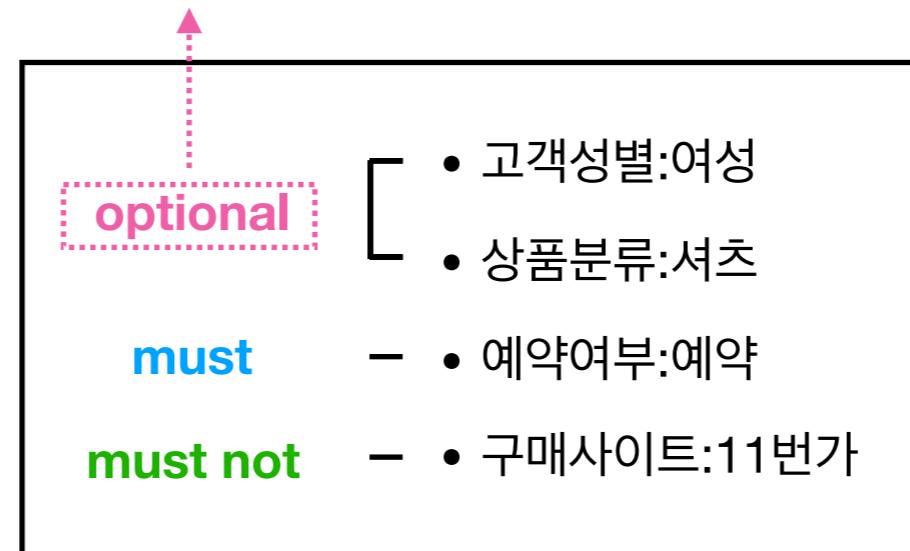
잠깐4

심화

AND, OR, NOT으로도 충분해 보이는데

+, - 은 왜 필요할까? 

필수는 아니지만 만족하는 Doc의 score ↑



조건이 너무 복잡하고, 가독성이 떨어지며, 에러 내기 쉽다

심화

- 여성 OR 셔츠 AND 예약 AND NOT 11번가
- (여성 OR 셔츠) AND 예약 AND NOT 11번가
- ((여성 AND 예약) OR (셔츠 AND 예약) OR 예약) AND NOT 11번가

이 때 +, -을 사용하면 쉽게 구현할 수 있다 

심화

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh < This month >

여성 셔츠+예약=11번가

Add a filter +

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

7 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map



g마켓
쿠팡 GS샵 옵션

예제 5 - 아래와 같은 Query를 Dashboard에서 검색해보자

Dashboard : nginx-*

Time Range : Past 30 days

문제	operator
nginx.access.response_code가 200인 Doc 필터링	is
nginx.access.method가 GET 또는 POST인 Doc 필터링	is one of
nginx.access.geoip.region_name가 non-null 값만 가지는 Doc 필터링	exists
nginx.access.geoip.city_name이 Seoul이면서 nginx.access.user_agent.name이 Chrome인 Doc 필터링	is
nginx.access.geoip.city_name이 Seoul이거나 nginx.access.user_agent.name이 Chrome인 Doc 필터링	?
요일_local이 Sunday인 Doc 필터링	is
nginx.access.geoip.country_name 가 “Republic of”로 시작하는 Doc 필터링	?
nginx.access.geoip.continent_code가 “AS”와 유사한 Doc 필터링	?

Filter와 Search를 비교해보자

AND 연산
OR 연산
Scripted Field
Wildcard 검색
Fuzzy/Proximity 검색

	문제	Filter	Search
	nginx.access.response_code가 200인 Doc	✓	✓
	nginx.access.method가 GET 또는 POST인 Doc	✓	✓
	nginx.access.geoip.region_name가 non-null값만 가지는 Doc	✓	✓
	nginx.access.geoip.city_name이 Seoul이면서 nginx.access.user_agent.name이 Chrome인 Doc	✓	✓
	nginx.access.geoip.city_name이 Seoul이거나 nginx.access.user_agent.name이 Chrome인 Doc		✓
AND 연산	요일_local이 Sunday인 Doc 필터링	✓	
OR 연산	nginx.access.geoip.country_name 가 Republic of로 시작하는 Doc		✓
Scripted Field	nginx.access.geoip.continent_code가 AS와 유사한 Doc		✓
Wildcard 검색			
Fuzzy/Proximity 검색			

Discover

데이터를 시각화하기 전에 데이터를 탐색하는 과정

주요 기능

세부 기능

데이터 검색

(복잡한) 조건을 만족하는 데이터 선별적 탐색 가능

데이터 필터링

(간단한) 특정 조건을 만족하는 데이터 선별적 탐색 가능

데이터 검색 저장

검색한 결과를 저장하여 Visualize에서 사용

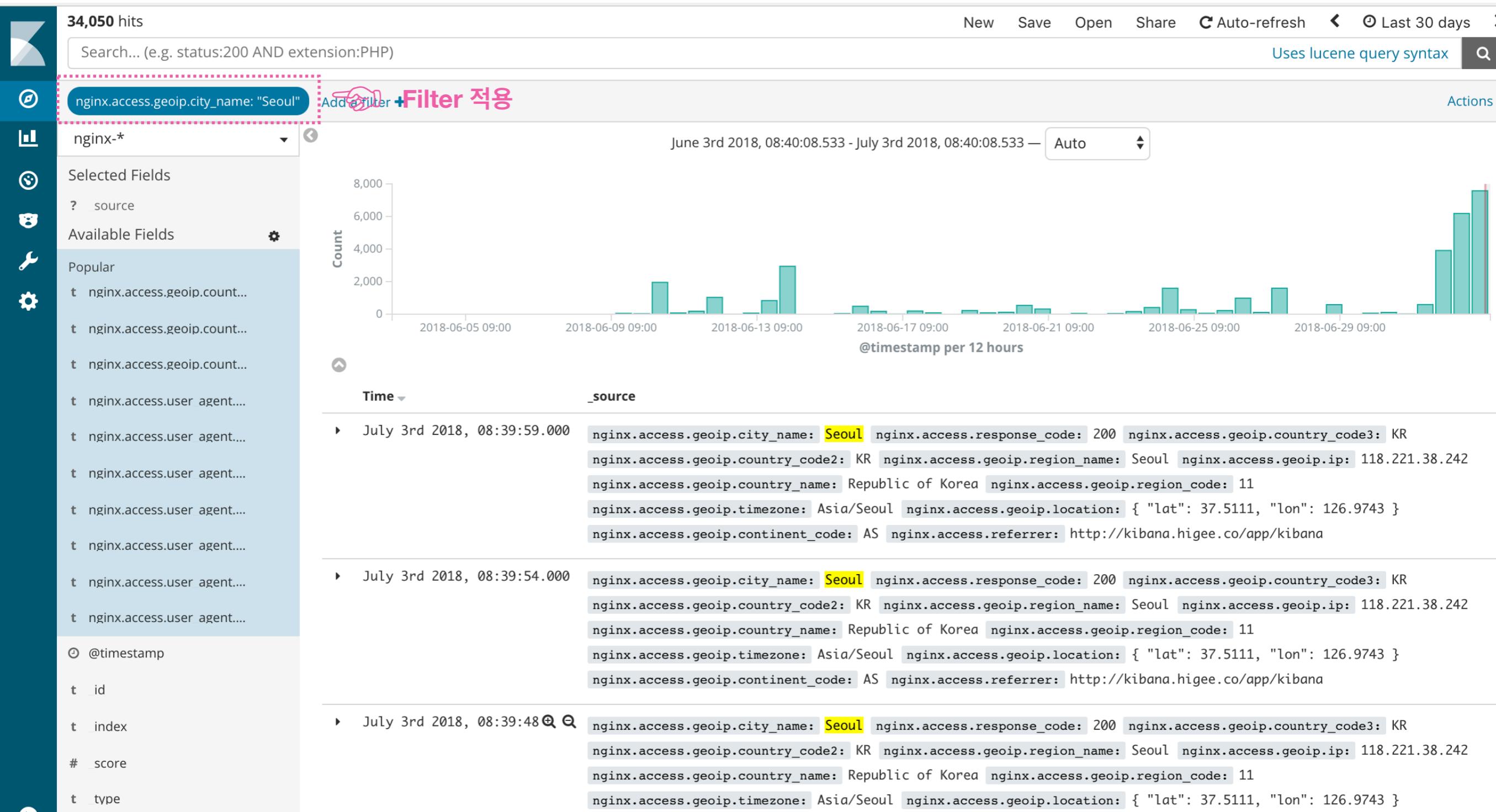
데이터 조회

- 특정 Document를 Table/JSON 형태 조회
- Histogram 특정 구간 내의 데이터 조회
- Histogram Bin 간격 설정
- Histogram 데이터를 csv 출력
- 특정 Field의 정보만 조회
- 특정 Field 값을 기준으로 정렬

데이터 통계

- (선택한 Time Range 내의) Documents 개수 확인
- 특정 Field Value의 분포 확인 (주로 Categorical Data, 상위 500개)
- 특정 Field에 non-null Value가 아닌 Documents 수 확인

Discover에서 Filter를 적용해보자



Discover에서 Search를 해보자

34,053 hits

nginx.access.geoip.city_name: Seoul

New Save Open Share Auto-refresh Last 30 days < > Uses lucene query syntax

Add a filter +

Selected Fields: source

Available Fields: Popular, @timestamp, id, index, # score, type, access.user.agent

Time: June 3rd 2018, 08:41:30.757 - July 3rd 2018, 08:41:30.757 — Auto

Count: @timestamp per 12 hours

Time _source

July 3rd 2018, 08:41:18.000

```
nginx.access.geoip.city_name: Seoul nginx.access.response_code: 200 nginx.access.geoip.country_code3: KR
nginx.access.geoip.country_code2: KR nginx.access.geoip.region_name: Seoul nginx.access.geoip.ip: 118.221.38.242
nginx.access.geoip.country_name: Republic of Korea nginx.access.geoip.region_code: 11
nginx.access.geoip.timezone: Asia/Seoul nginx.access.geoip.location: { "lat": 37.5111, "lon": 126.9743 }
nginx.access.geoip.continent_code: AS nginx.access.referrer: http://kibana.higee.co/app/kibana
```

July 3rd 2018, 08:40:08.000

```
nginx.access.geoip.city_name: Seoul nginx.access.response_code: 200 nginx.access.geoip.country_code3: KR
nginx.access.geoip.country_code2: KR nginx.access.geoip.region_name: Seoul nginx.access.geoip.ip: 118.221.38.242
nginx.access.geoip.country_name: Republic of Korea nginx.access.geoip.region_code: 11
nginx.access.geoip.timezone: Asia/Seoul nginx.access.geoip.location: { "lat": 37.5111, "lon": 126.9743 }
nginx.access.geoip.continent_code: AS nginx.access.referrer: http://kibana.higee.co/app/kibana
```

July 3rd 2018, 08:40:06.000

```
nginx.access.geoip.city_name: Seoul nginx.access.response_code: 200 nginx.access.geoip.country_code3: KR
nginx.access.geoip.country_code2: KR nginx.access.geoip.region_name: Seoul nginx.access.geoip.ip: 118.221.38.242
nginx.access.geoip.country_name: Republic of Korea nginx.access.geoip.region_code: 11
nginx.access.geoip.timezone: Asia/Seoul nginx.access.geoip.location: { "lat": 37.5111, "lon": 126.9743 }
nginx.access.geoip.continent_code: AS nginx.access.referrer: http://kibana.higee.co/app/kibana
```

잠깐5, 이걸로 뭘 할 수 있을까?

: 특정한 조건을 만족하는 데이터만 선별해서 시각화 할 수 있다.

검색 결과 저장

34,053 hits

New Save Open Share Auto-refresh < ⏪ Last 30 days > ⏩

Save Search

서울 접속 데이터

Save

nginx.access.geoip.city_name: Seoul

1. Lucene Query 작성 (혹은 필터 적용)

Uses lucene query syntax

Add a filter +

Selected Fields

? source

Available Fields

Popular

t nginx.access.geoip.count...

t nginx.access.geoip.count...

t nginx.access.geoip.count...

t nginx.access.user agent....

@timestamp

June 3rd 2018, 08:41:30.757 - July 3rd 2018, 08:41:30.757 — Auto

Count

8,000
6,000
4,000
2,000
0

2018-06-05 09:00 2018-06-09 09:00 2018-06-13 09:00 2018-06-17 09:00 2018-06-21 09:00 2018-06-25 09:00 2018-06-29 09:00

@timestamp per 12 hours

Time ▾

_source

▶ July 3rd 2018, 08:41:18.000

```
nginx.access.geoip.city_name: Seoul nginx.access.response_code: 200 nginx.access.geoip.country_code3: KR
nginx.access.geoip.country_code2: KR nginx.access.geoip.region_name: Seoul nginx.access.geoip.ip: 118.221.38.242
nginx.access.geoip.country_name: Republic of Korea nginx.access.geoip.region_code: 11
nginx.access.geoip.timezone: Asia/Seoul nginx.access.geoip.location: { "lat": 37.5111, "lon": 126.9743 }
nginx.access.geoip.continent_code: AS nginx.access.referrer: http://kibana.higee.co/app/kibana
```

▶ July 3rd 2018, 08:40:08.000

```
nginx.access.geoip.city_name: Seoul nginx.access.response_code: 200 nginx.access.geoip.country_code3: KR
nginx.access.geoip.country_code2: KR nginx.access.geoip.region_name: Seoul nginx.access.geoip.ip: 118.221.38.242
nginx.access.geoip.country_name: Republic of Korea nginx.access.geoip.region_code: 11
nginx.access.geoip.timezone: Asia/Seoul nginx.access.geoip.location: { "lat": 37.5111, "lon": 126.9743 }
nginx.access.geoip.continent_code: AS nginx.access.referrer: http://kibana.higee.co/app/kibana
```

2. 검색 결과 저장

3. 검색 결과를 이름을 지정하여 저장

The screenshot shows the Kibana interface with a search results page. The search bar contains the query 'nginx.access.geoip.city_name: Seoul'. The results show a histogram of access counts over time and two specific log entries for July 3rd, 2018. Three pink callouts provide instructions: 1. 'Lucene Query 작성 (혹은 필터 적용)' (Create a Lucene query (or filter)), 2. '검색 결과 저장' (Save search results), and 3. '검색 결과를 이름을 지정하여 저장' (Name the search results and save). The sidebar on the left lists available fields like '_source', 'nginx.access.geoip.count...', and 'nginx.access.user agent....'.

저장된 검색 결과를 이용한 시각화 1단계

Visualize / New

Select visualization type

Search visualization types...



Basic Charts



Area



Heat Map



Horizontal Bar



Line

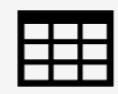


Pie



Vertical Bar

Data



Data Table



Gauge



Goal



Metric

Maps



Coordinate Map



Region Map

Time Series



저장된 검색 결과를 이용한 시각화 2단계

Visualize / New / Choose search source

From a New Search, Select Index

Or, From a Saved Search

Filter...

12 of 12

서울 접속

1-1 of 1

[Manage saved searches](#)

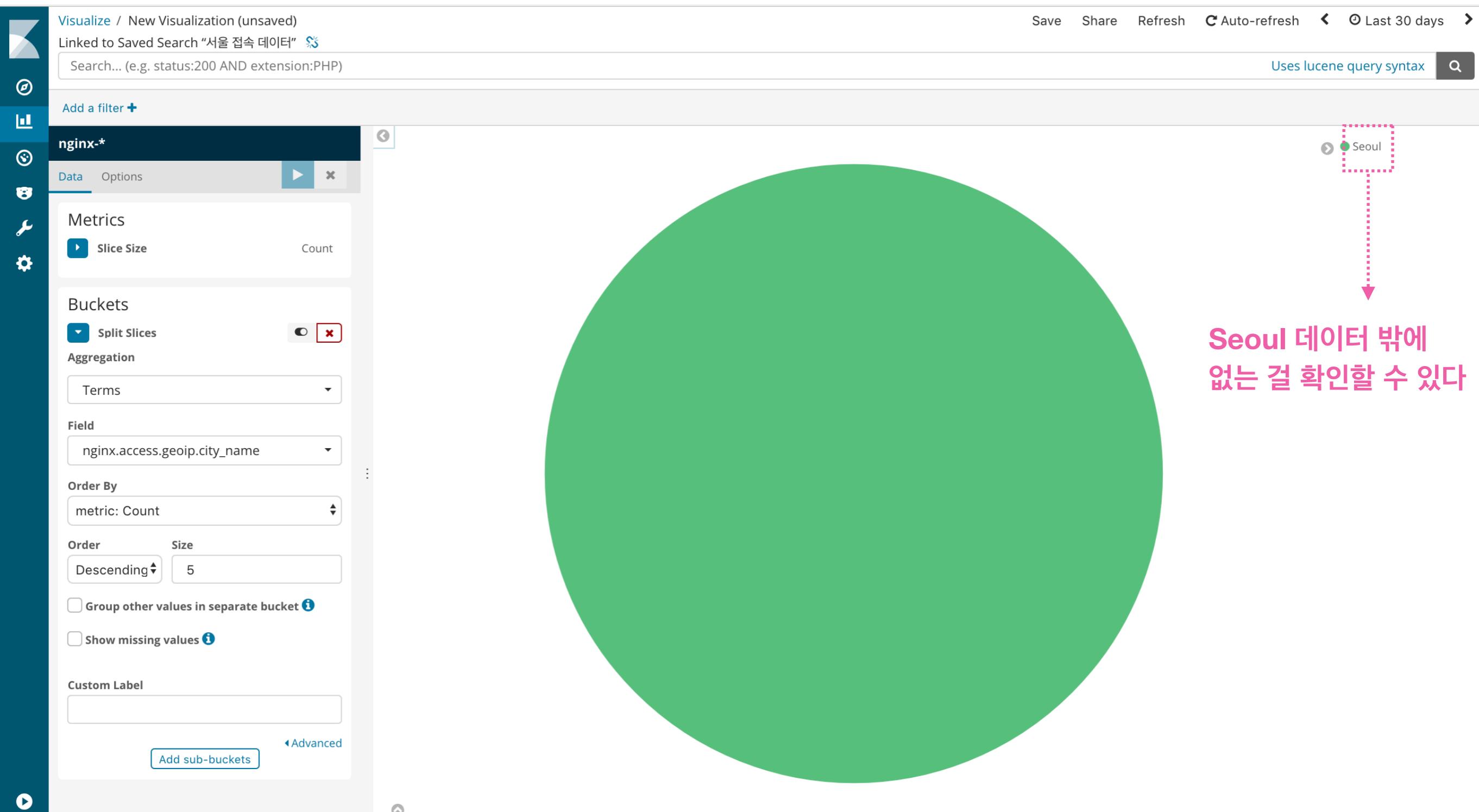
Name ▲

Name ▲

서울 접속 데이터

👉 “저장한 검색결과” 선택

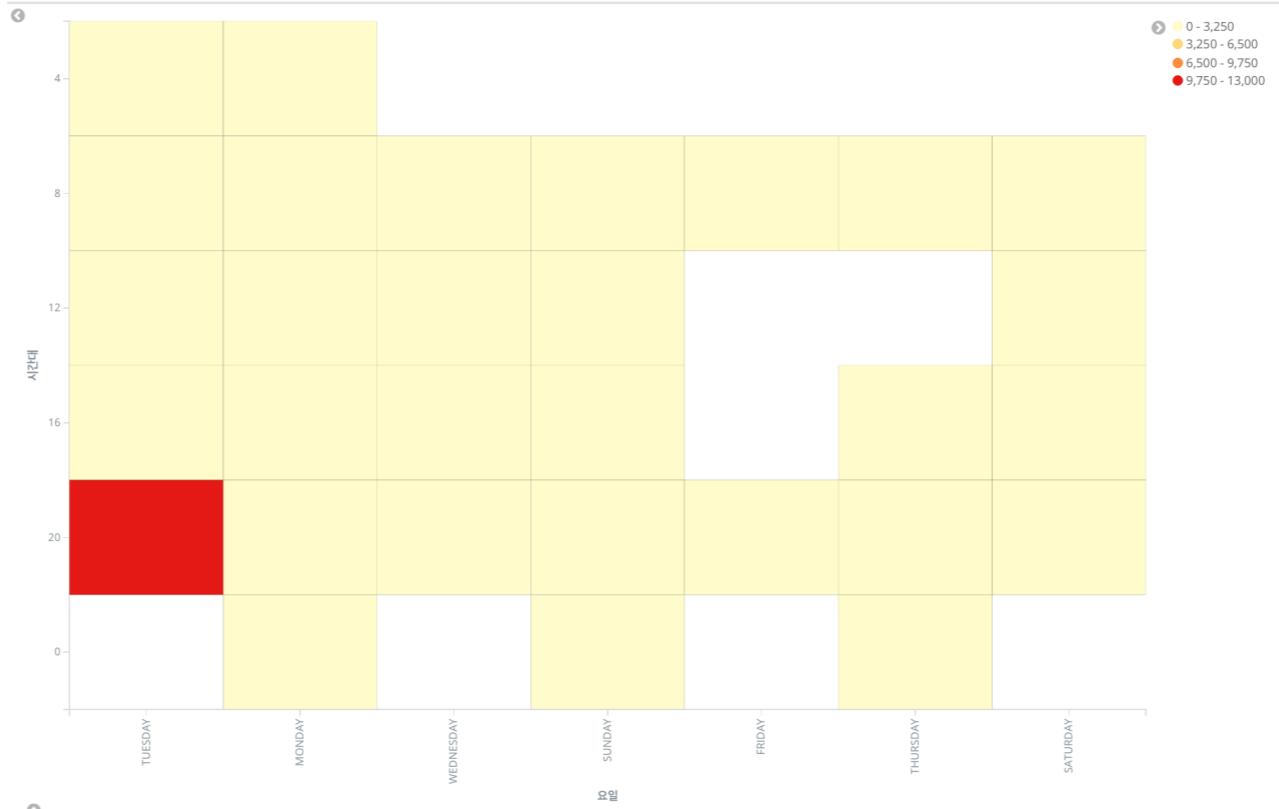
저장된 검색 결과를 이용한 시각화 3단계



예제 6.1 - 필터 혹은 검색을 이용해서 아래와 같은 데이터를 저장하자

- Index : nginx-*
- 조건 :
 - must
 - nginx.access.geoip.region_name가 non-null value인 Doc
 - nginx.access.geoip.city_name가 “Se”로 시작하는 Doc
 - must not : nginx.access.response_code가 200 및 405이 아닌 Doc
 - optional : nginx.access.method가 POST인 Doc

예제 6.2- 앞서 저장한 결과로 아래와 같은 시각화를 하자



조건

- "@timestamp" field 기준 **Last 30 days** 동안
- 요일별 시간대별 접속자 수
 - 요일별 : 요일_local Field 사용
 - 시간대별 : 시간대_local Field를 사용하여 4시간 간격으로 집계

질문 및 Feedback은

gshock94@gmail.com로 주세요