

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?

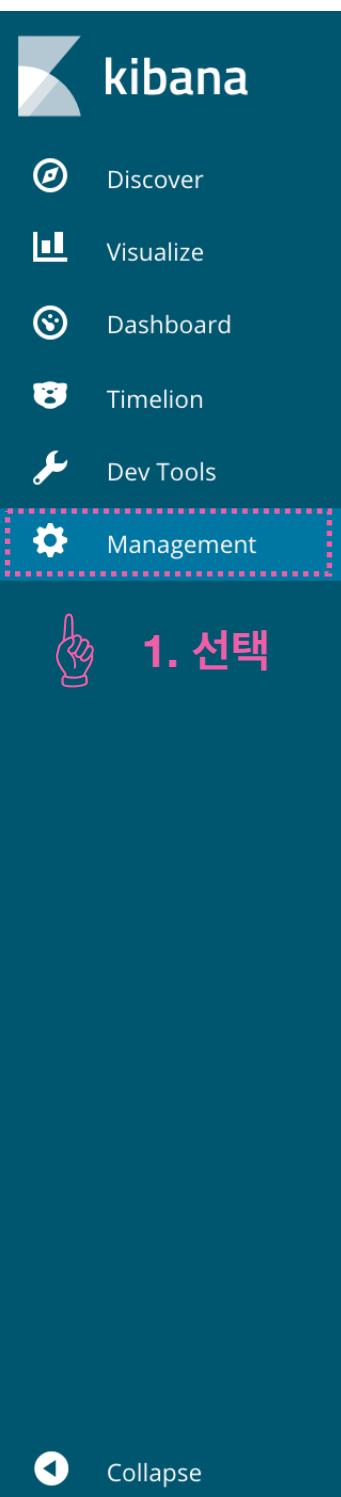
Date Field에서 연/월/일/시/분/초 등 접근 안되나?

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



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_* 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

i No scripted fields found.

Hand icons with numbers 1 through 5 are overlaid on the interface to guide the user through the steps.

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

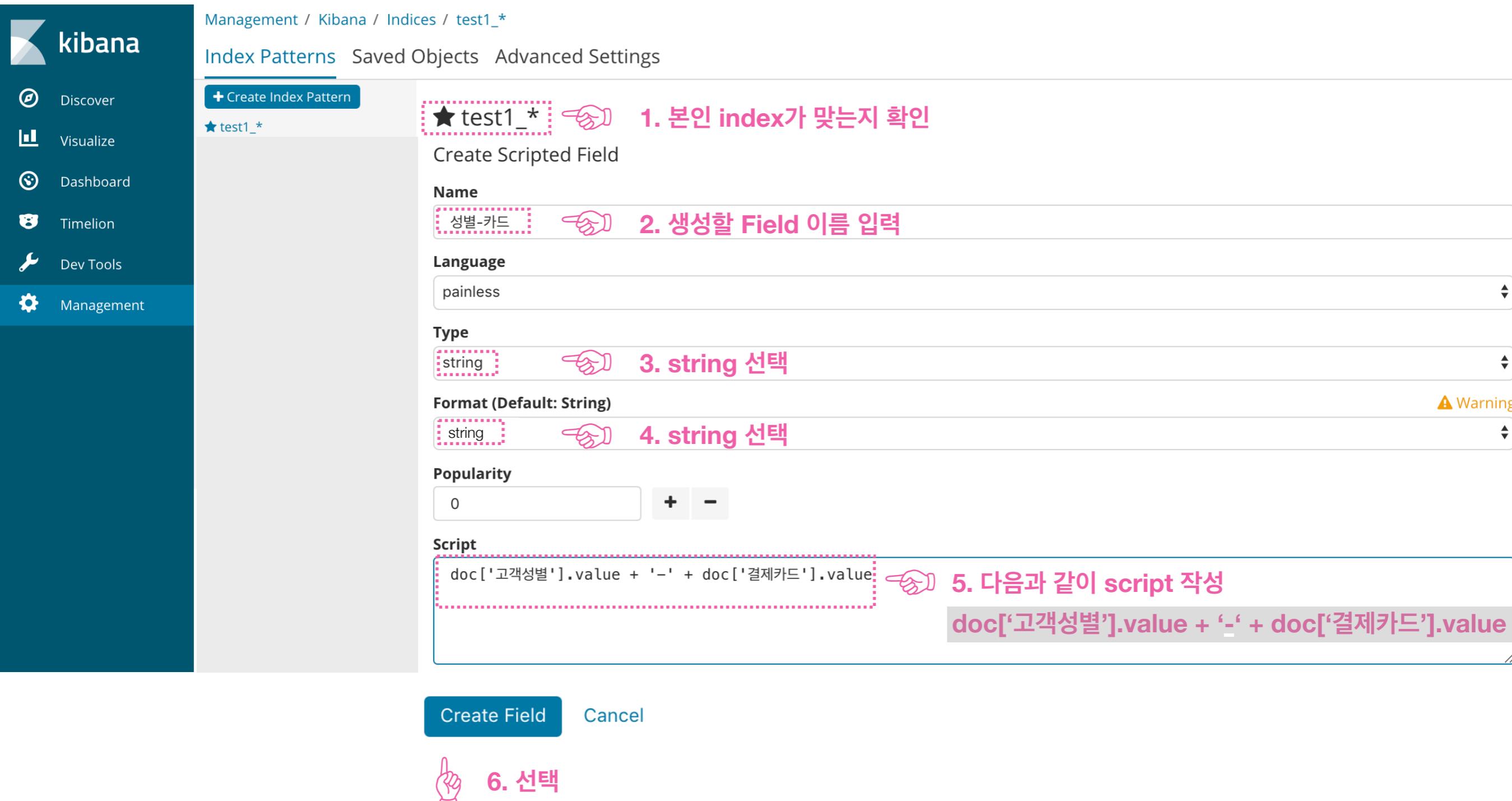
doc['고객성별'].value + '-' + doc['결제카드'].value

5. 다음과 같이 script 작성

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

Create Field Cancel

6. 선택



Discover에 가서 확인하자

276 hits

New Save Open Share C Auto-refresh < ⏪ This month ⏩

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

Add a filter +

Selected Fields: test1_*

Available Fields: t 결제카드, t 고객성별, t 성별-카드, t 상품분류, t id, t index, # score, t type, ☐ 고객ip, t 고객주소 시도, t 구매사이트, ☰ 물건좌표, t 배송메모, # 상품가격, # 상품개수, ⓒ 수령시간

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

Count

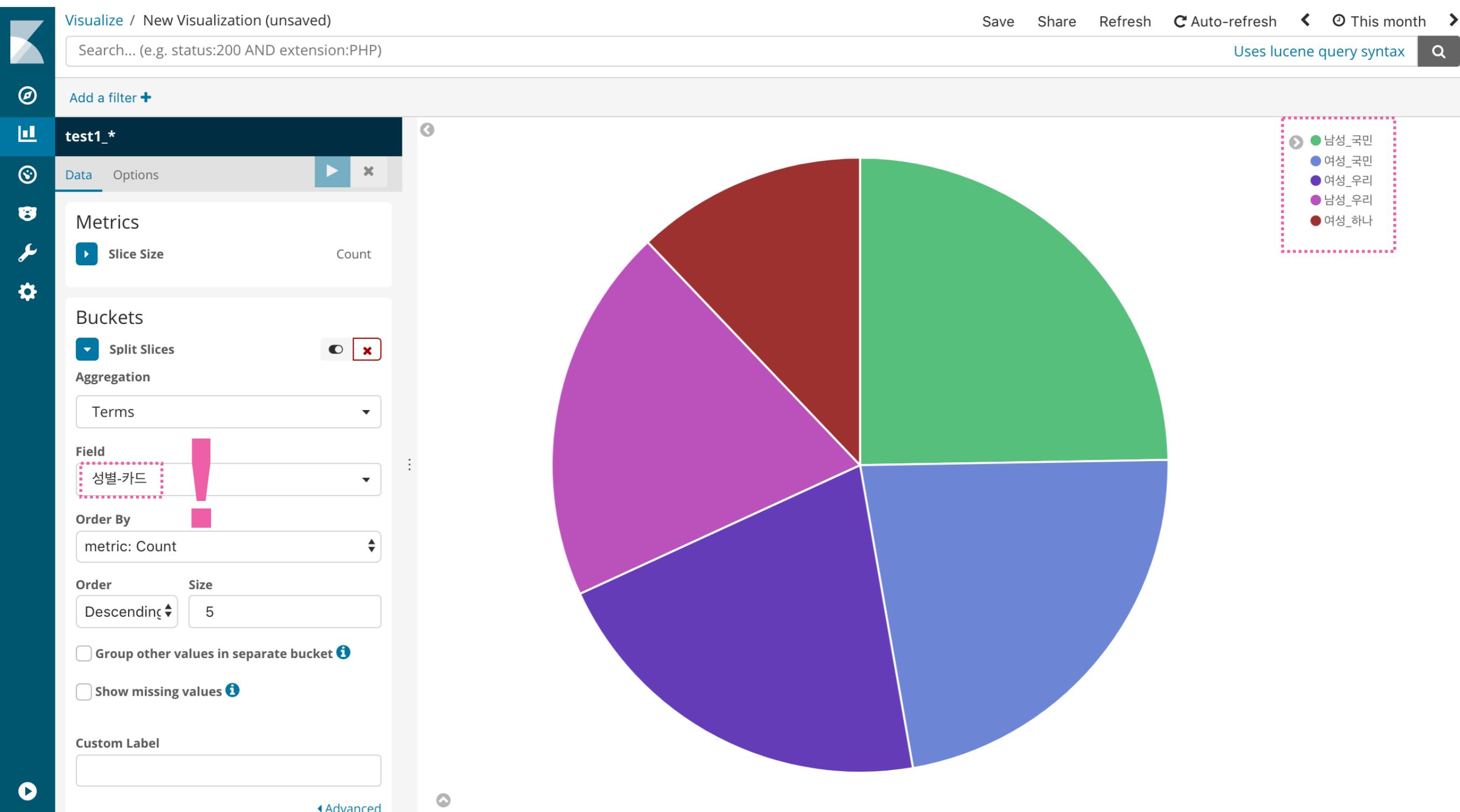
주문시간 per 12 hours

Time	고객성별	결제카드	성별-카드
▶ August 31st 2018, 20:49:41.000	남성	국민	남성_국민
▶ August 31st 2018, 19:34:52.000	여성	국민	여성_국민
▶ August 31st 2018, 17:24:03.000	여성	우리	여성_우리
▶ August 31st 2018, 15:43:58.000	남성	국민	남성_국민
▶ August 31st 2018, 14:55:29.000	남성	롯데	남성_롯데
▶ August 31st 2018, 08:43:43.000	남성	삼성	남성_삼성
▶ August 31st 2018, 05:56:24.000	여성	국민	여성_국민
▶ August 31st 2018, 04:51:39.000	여성	시티	여성_시티
▶ August 31st 2018, 02:19:09.000	남성	롯데	남성_롯데
▶ August 30th 2018, 23:25:52.000	남성	신한	남성_신한
▶ August 30th 2018, 22:09:45.000	남성	우리	남성_우리

Uses lucene query syntax

A pink dashed box highlights the '성별-카드' column, and a pink hand icon points to it.

방금 생성한 Field를 이용하여 Visualization을 생성할 수 있다는 것이다



String Concatenation 연산은 안되나?

Field 간 연산은 안되나?



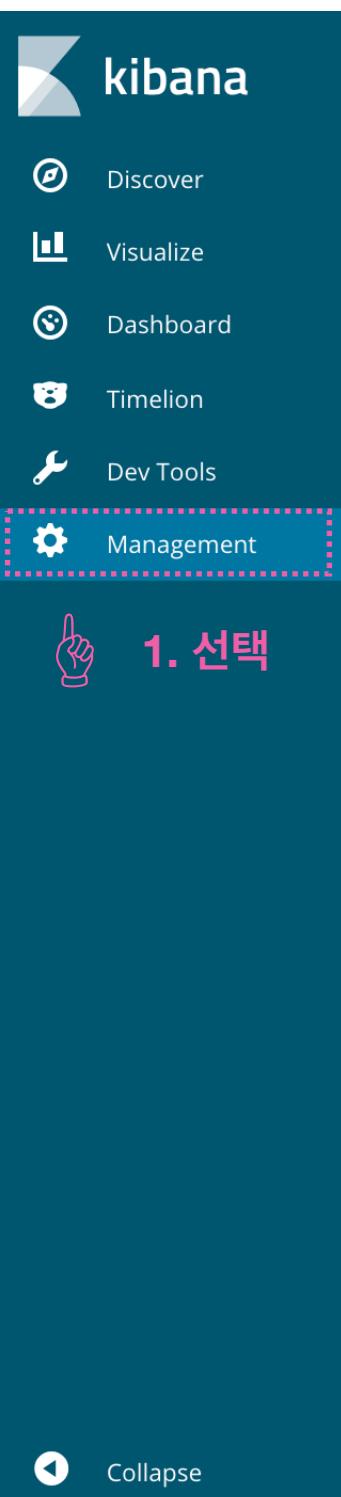
Date Field에서 연/월/일/시/분/초 등 접근 안되나?

기존 Field에 조건을 적용해서 새로운 Field를 만들 수 없나?

예시

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

scripted field를 추가하자



1. 선택 (Hand icon pointing to the Management tab in the sidebar)

2. 선택 (Hand icon pointing to the 'Index Patterns' tab in the top navigation bar)

3. id_* 선택 (Hand icon pointing to the 'test1_*' index pattern in the list)

4. 선택 (Hand icon pointing to the 'scripted fields (0)' tab)

5. 선택 (Hand icon pointing to the '+ Add Scripted Field' button)

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!

No scripted fields found.

script를 작성하자

Management / Kibana / Indices / test1_*

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern ★ test1_*

1. 본인 index가 맞는지 확인

Create Scripted Field

Name 배송소요시간 2. 생성할 Field 이름 입력

Language painless

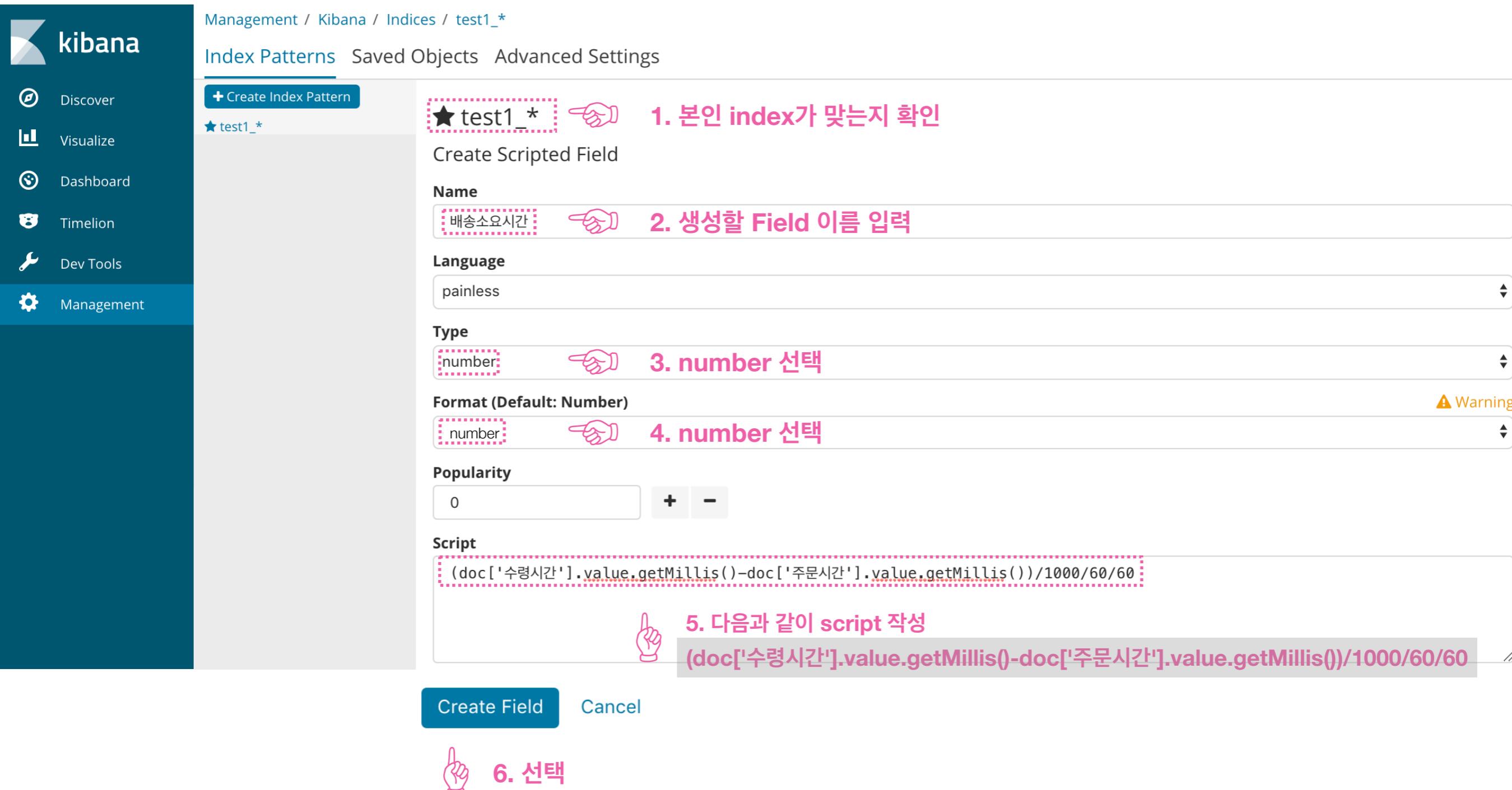
Type number 3. number 선택

Format (Default: Number) number 4. number 선택 ⚠ Warning

Popularity 0 + -

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

Create Field Cancel 6. 선택



Discover에 가서 확인하자

276 hits

New Save Open Share Auto-refresh < This month >

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

Uses lucene query syntax

Add a filter +

Selected Fields: test1_*

Available Fields: 수령시간, 주문시간, 배송소요시간

Time Range: August 1st 2018, 00:00:00.000 - August 31st 2018, 23:59:59.999 — Auto

Count vs 주문시간 per 12 hours

Time	주문시간	수령시간	배송소요시간
August 31st 2018, 20:49:41.000	August 31st 2018, 20:49:41.000	September 3rd 2018, 12:57:41.000	64
August 31st 2018, 19:34:52.000	August 31st 2018, 19:34:52.000	September 2nd 2018, 21:47:52.000	50
August 31st 2018, 17:24:03.000	August 31st 2018, 17:24:03.000	September 1st 2018, 01:08:03.000	7
August 31st 2018, 15:43:58.000	August 31st 2018, 15:43:58.000	September 4th 2018, 13:45:58.000	94
August 31st 2018, 14:55:29.000	August 31st 2018, 14:55:29.000	September 2nd 2018, 14:56:29.000	48
August 31st 2018, 08:43:43.000	August 31st 2018, 08:43:43.000	September 4th 2018, 10:20:43.000	97
August 31st 2018, 05:56:24.000	August 31st 2018, 05:56:24.000	September 2nd 2018, 17:25:24.000	59
August 31st 2018, 04:51:39.000	August 31st 2018, 04:51:39.000	September 1st 2018, 22:58:39.000	42
August 31st 2018, 02:19:09.000	August 31st 2018, 02:19:09.000	September 2nd 2018, 08:04:09.000	53
August 30th 2018, 23:25:52.000	August 30th 2018, 23:25:52.000	September 2nd 2018, 14:13:52.000	62
August 30th 2018, 22:09:45.000	August 30th 2018, 22:09:45.000	August 31st 2018, 14:57:45.000	16

예제 1 - Scripted Field

276 hits

New Save Open Share C Auto-refresh < ⏪ This month ⏩

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

Add a filter +

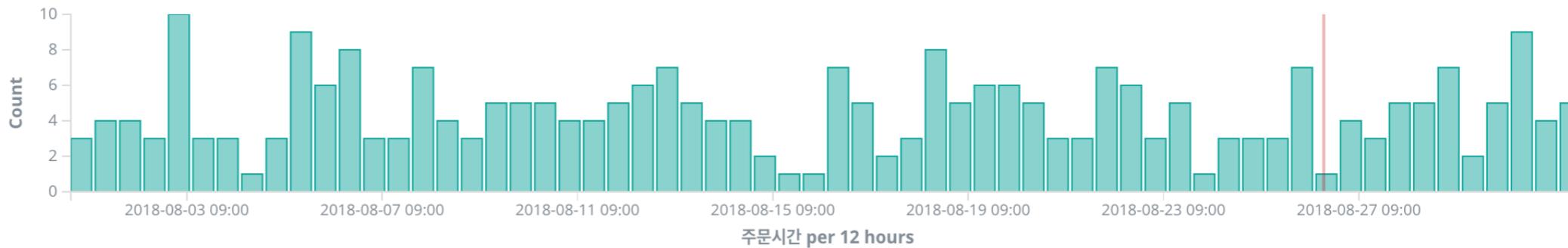
Selected Fields: test1_*

Available Fields: # 상품가격, # 상품개수, # 매출, # 고객나이, t 상품분류, t id, t index, # score, t type, t 결제카드, ☐ 고객ip, t 고객성별, t 고객주소 시도, t 구매사이트, ☺ 물건좌표, t 배송메모, # 배송소요시간

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

Count

주문시간 per 12 hours



Time	상품가격
August 31st 2018, 20:49:41.000	17,000
August 31st 2018, 19:34:52.000	11,000
August 31st 2018, 17:24:03.000	25,000
August 31st 2018, 15:43:58.000	27,000
August 31st 2018, 14:55:29.000	29,000
August 31st 2018, 08:43:43.000	6,000
August 31st 2018, 05:56:24.000	24,000
August 31st 2018, 04:51:39.000	27,000
August 31st 2018, 02:19:09.000	19,000
August 30th 2018, 23:25:52.000	5,000
August 30th 2018, 22:09:45.000	17,000

상품개수
7
7
7
1
1
7
1
7
7
7

매출
119,000
77,000
175,000
27,000
29,000
42,000
24,000
189,000
133,000
5,000
119,000

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



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

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.

script(시간대)를 작성하자

Management / Kibana / Indices / test1_*

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

★ test1_*

Create Scripted Field

Name

주문시간_시간대

Language

painless

Type

number

Format (Default: Number)

number

Popularity

0 + -

Script

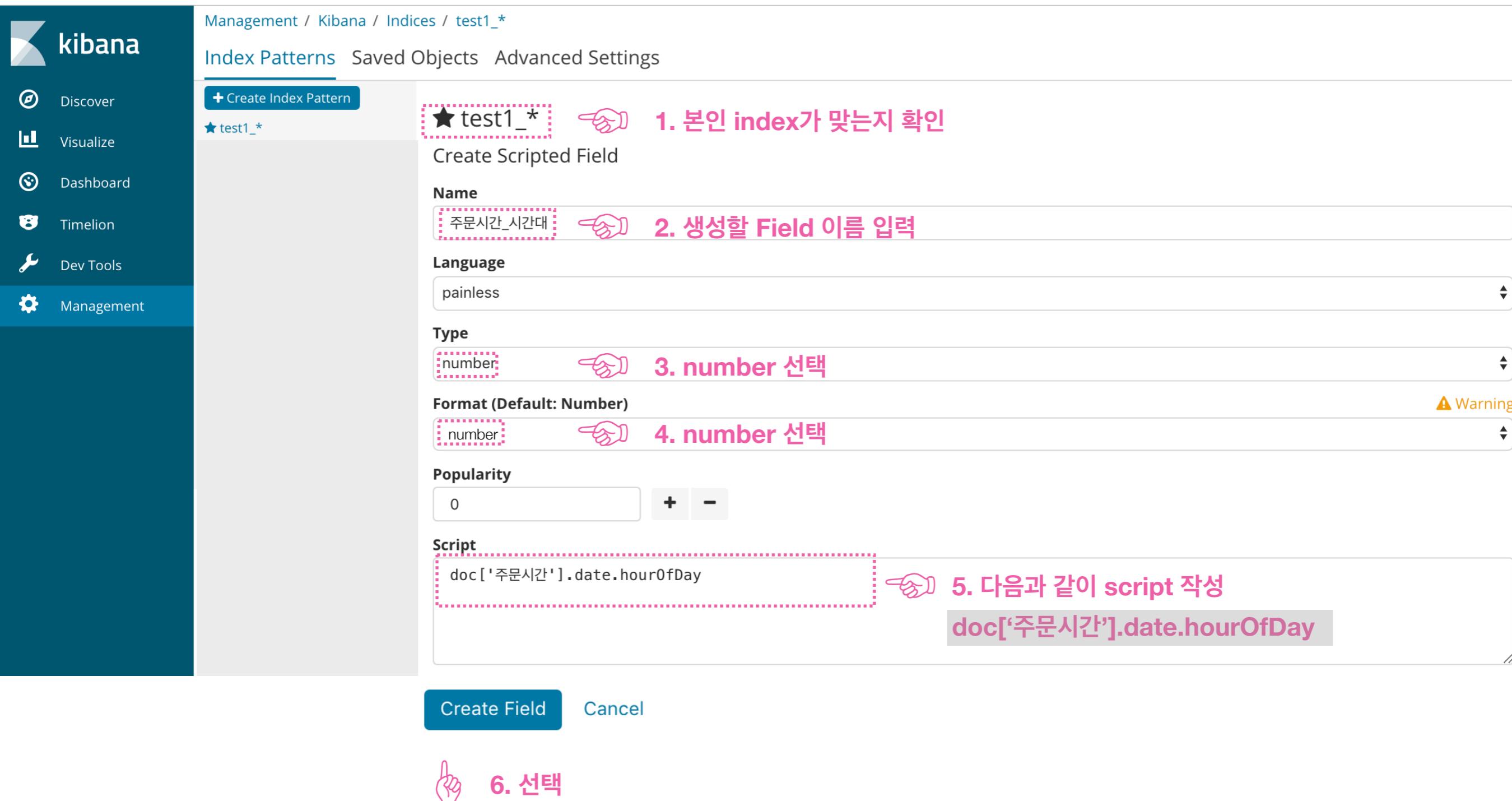
doc['주문시간'].date.hourOfDay

⚠ Warning

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

6. 선택

Create Field Cancel



script(요일)를 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

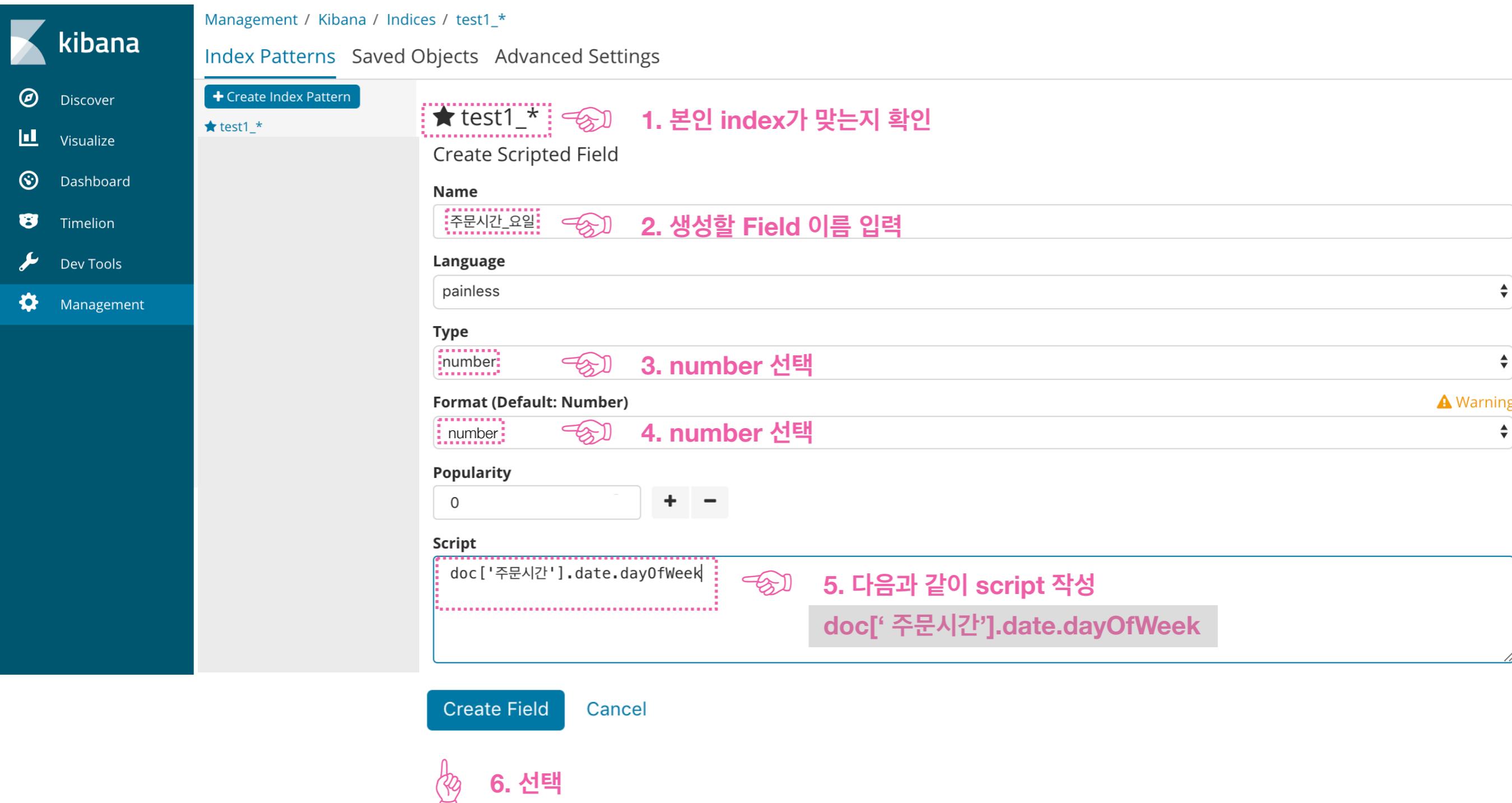
Format (Default: Number) 4. number 선택

Popularity + -

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

Create Field Cancel

6. 선택



Discover에 가서 확인하자

276 hits

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

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

Uses lucene query syntax

Add a filter +

Selected Fields

- # 주문시간_시간대
- # 주문시간_요일
- Available Fields
- Popular
- # 고객나이
- t 상품분류
- t _id
- t _index
- # score
- t type
- t 결제카드
- 고객ip
- t 고객성별
- t 고객주소_시도
- t 구매사이트
- # 매출
- ⌚ 물건좌표
- t 배송메모
- # 배송소요시간

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

Count

주문시간 per 12 hours

주문시간	Count
2018-08-03 09:00	3
2018-08-04 09:00	4
2018-08-05 09:00	1
2018-08-06 09:00	3
2018-08-07 09:00	9
2018-08-08 09:00	3
2018-08-09 09:00	7
2018-08-10 09:00	3
2018-08-11 09:00	5
2018-08-12 09:00	4
2018-08-13 09:00	6
2018-08-14 09:00	7
2018-08-15 09:00	2
2018-08-16 09:00	1
2018-08-17 09:00	7
2018-08-18 09:00	3
2018-08-19 09:00	6
2018-08-20 09:00	5
2018-08-21 09:00	3
2018-08-22 09:00	2
2018-08-23 09:00	5
2018-08-24 09:00	3
2018-08-25 09:00	7
2018-08-26 09:00	2
2018-08-27 09:00	4
2018-08-28 09:00	7
2018-08-29 09:00	4
2018-08-30 09:00	10
2018-08-31 09:00	11

Time ▾

주문시간_시간대

- ▶ August 31st 2018, 20:49:41.000 11
- ▶ August 31st 2018, 19:34:52.000 10
- ▶ August 31st 2018, 17:24:03.000 8
- ▶ August 31st 2018, 15:43:58.000 6
- ▶ August 31st 2018, 14:55:29.000 5
- ▶ August 31st 2018, 08:43:43.000 23
- ▶ August 31st 2018, 05:56:24.000 20
- ▶ August 31st 2018, 04:51:39.000 19
- ▶ August 31st 2018, 02:19:09.000 17
- ▶ August 30th 2018, 23:25:52.000 14
- ▶ August 30th 2018, 22:09:45.000 13

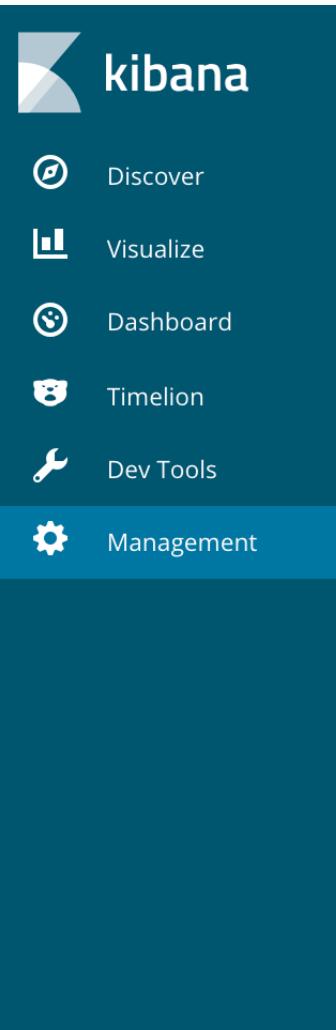
주문시간_요일

참고

요일	값
월	1
화	2
수	3
목	4
금	5
토	6
일	7

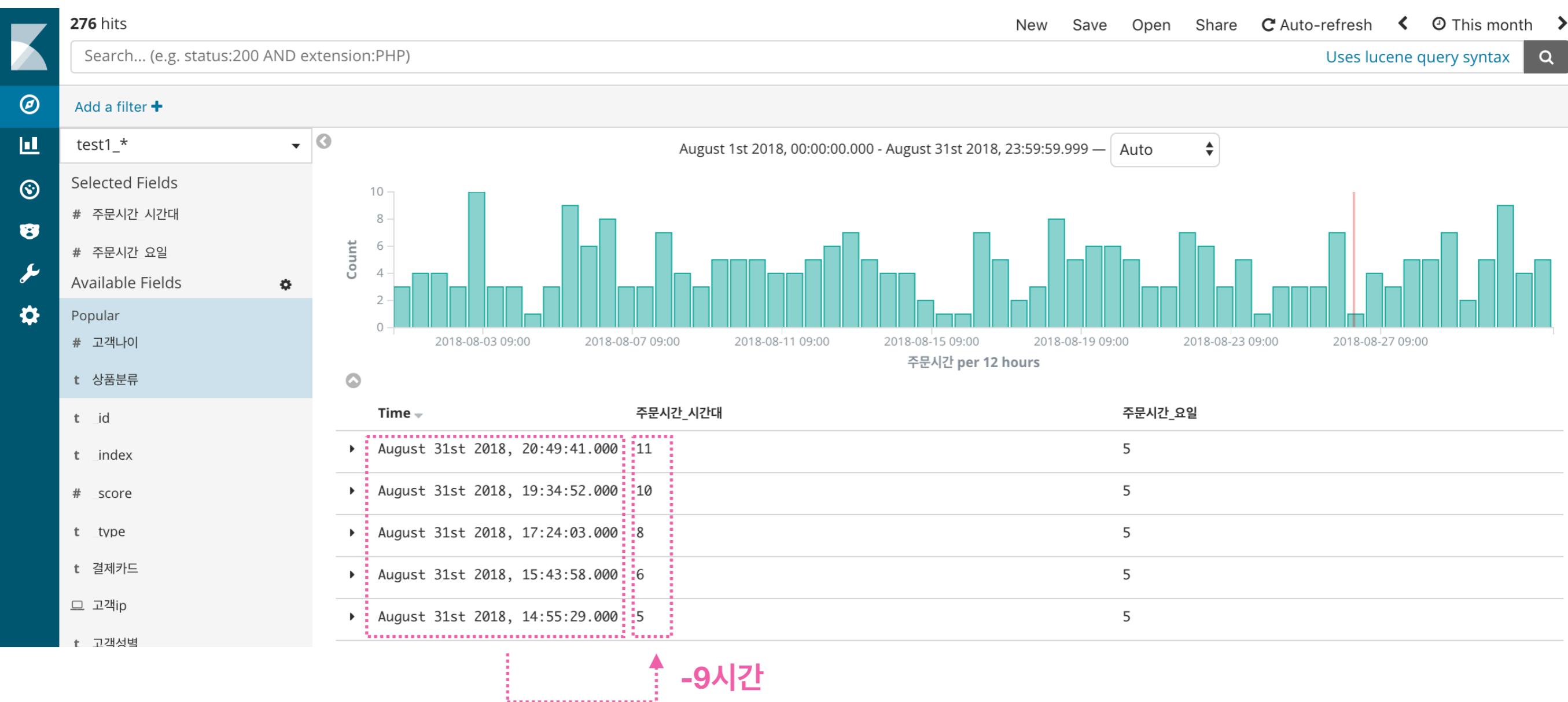
Elasticsearch : 기본적으로 입력된 date field를 **UTC**로 인식한다

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



Elasticsearch timezone ≠ Kibana timezone

심화



즉, Scripted Field로 추출한 (elasticsearch의) 주문시간 field의
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 주문시간_시간대_local

Language painless

Type number

Format (Default: Number)

Number Numeral.js format pattern (Default: "0,0.[000]") 0,0.[000]

Warning Docs

Popularity 0 + -

Script Instant.ofEpochMilli(doc['주문시간'].date.millis).atZone(ZoneId.of("Asia/Seoul")).hour

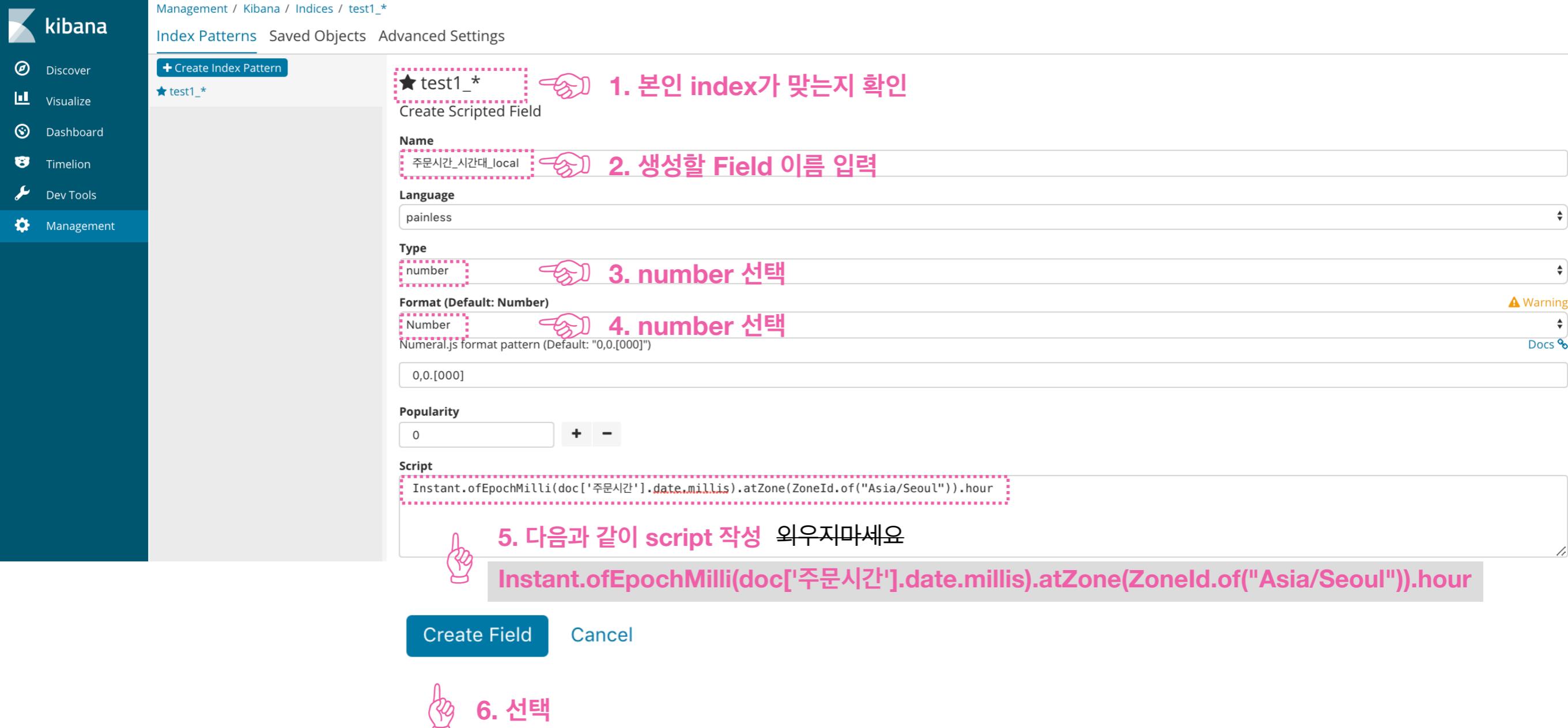
⚠ Warning Docs

5. 다음과 같이 script 작성 외우지마세요

Instant.ofEpochMilli(doc['주문시간'].date.millis).atZone(ZoneId.of("Asia/Seoul")).hour

Create Field Cancel

6. 선택



Management / Kibana / Indices / test1_*

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern ★ test1_*

Create Scripted Field

Name 주문시간_요일_local

Language painless

Type string

Format (Default: String) String

Transform - none -

Popularity 0 + -

Script

```
Instant.ofEpochMilli(doc['주문시간'].date.millis).atZone(ZoneId.of("Asia/Seoul")).dayOfWeek
```

5. 다음과 같이 script 작성 외우지마세요
Instant.ofEpochMilli(doc['주문시간'].date.millis).atZone(ZoneId.of("Asia/Seoul")).dayOfWeek

Create Field Cancel



6. 선택

Management / Kibana / Indices / test1_*

Index Patterns Saved Objects Advanced Settings

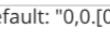
+ Create Index Pattern ★ test1_* Create Scripted Field

Name 주문시간_요일_local_sort  1. 본인 index가 맞는지 확인

Language painless

Type number  2. 생성할 Field 이름 입력

Format (Default: Number) Number  3. number 선택

Numerals.js format pattern (Default: "0,0,[000]") 0,0,[000]  4. number 선택 ⚠ Warning Docs

Popularity 0 + -

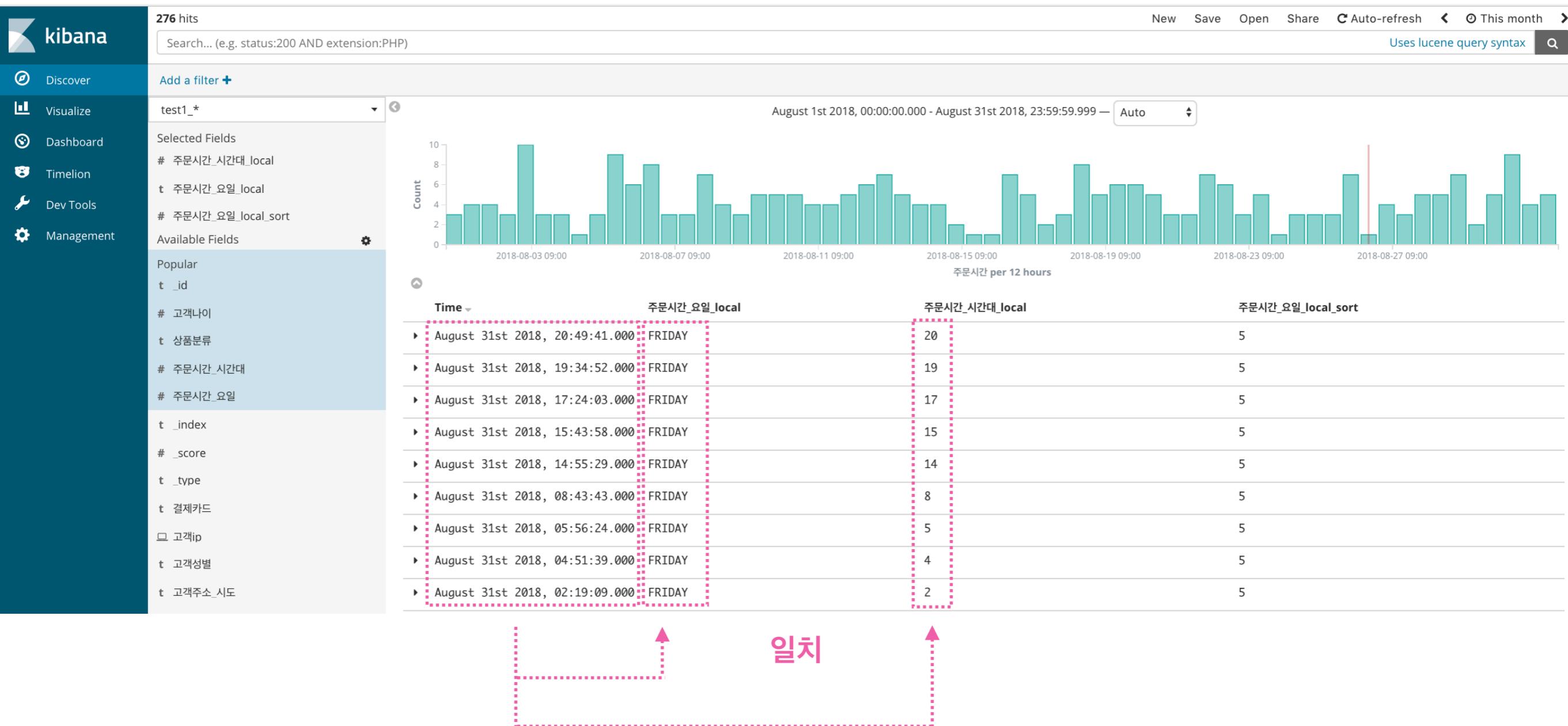
Script  5. 다음과 같이 script 작성  외우지마세요

```
Instant.ofEpochMilli(doc['주문시간'].date.millis).atZone(ZoneId.of("Asia/Seoul")).dayOfWeek.getValue()
```

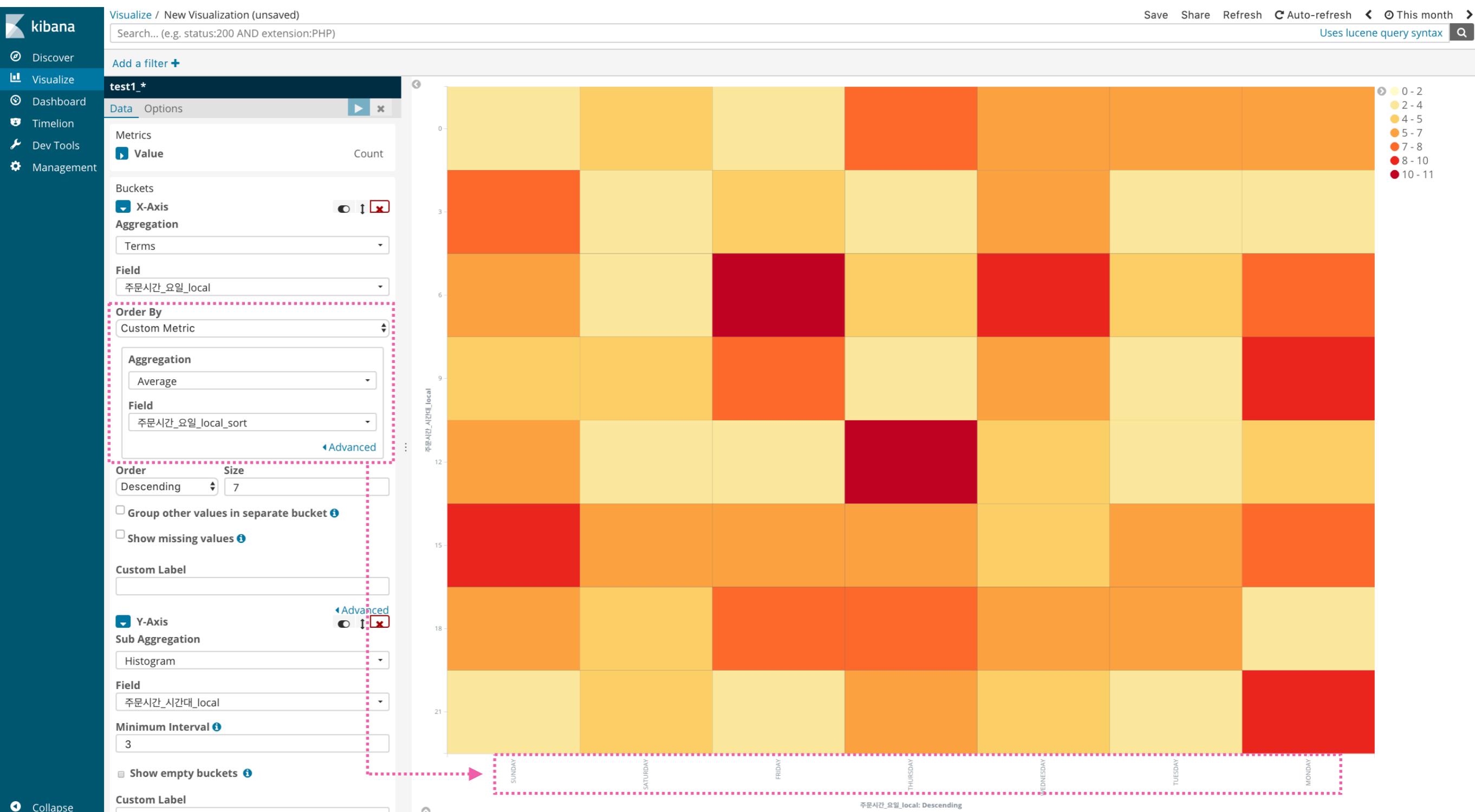
Create Field Cancel



6. 선택



앞의 결과를 이용하면 Local Time 기준을
활용해서 Visualization을 생성할 수 있다.
(Week1-2에서 사용했던 Heat Map은 UTC 기준)



요일 순서로 정렬하기 위해 필요

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?

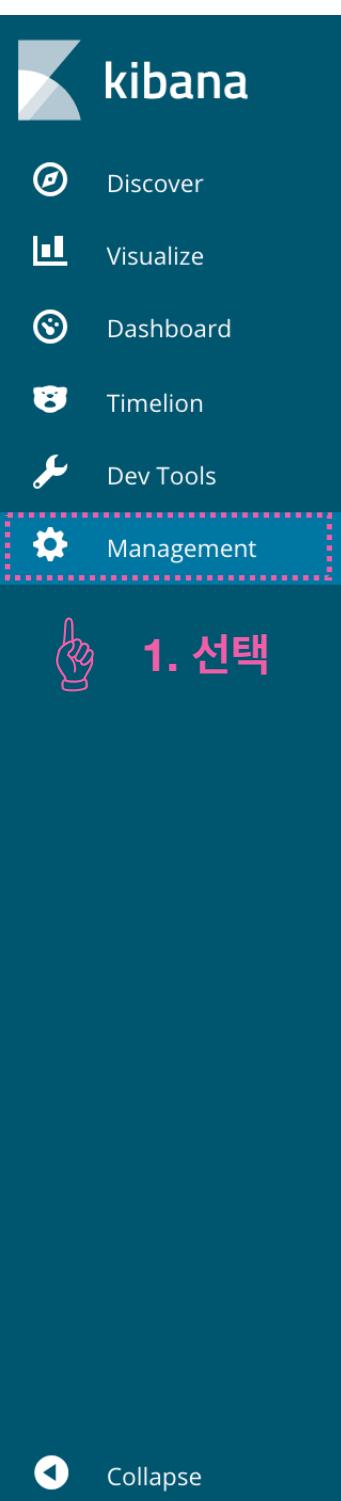


예시

고객나이 Field 값에 따라 10대, 20대, 30대, ...

와 같은 값을 갖는 Field를 만들고 싶다면?

scripted field를 추가하자



1. 선택

Management / Kibana

Index Patterns Saved Objects Advanced Settings

2. 선택

+ Create Index Pattern
★ test1_*

3. id_* 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 **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 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" }
```

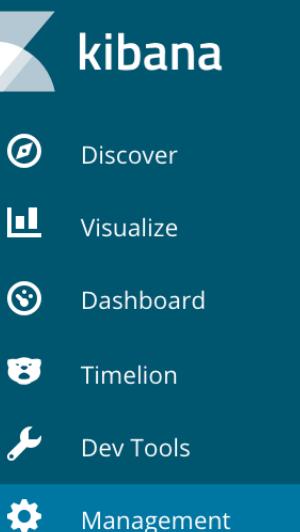
Warning

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



1. 본인 index가 맞는지 확인



2. 생성할 Field 이름 입력



3. string 선택



4. string 선택



5. 다음과 같이 script 작성



6. 선택

Discover에 가서 확인하자

kibana

276 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 test1_*

Selected Fields

- # 고객나이
- t 연령대

Available Fields

- Popular
- t _id
- t 상품분류
- # 주문시간_시간대
- # 주문시간_시간대_local
- # 주문시간_요일
- t 주문시간_요일_local
- t _index
- # _score
- t _type
- t 결제카드
- 고객ip
- t 고객성별
- t 고객주소_시도
- t 구매사이트
- # 매출
- ⌚ 물건좌표
- t 배송메모
- ↳ 비속어 처리

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

Count

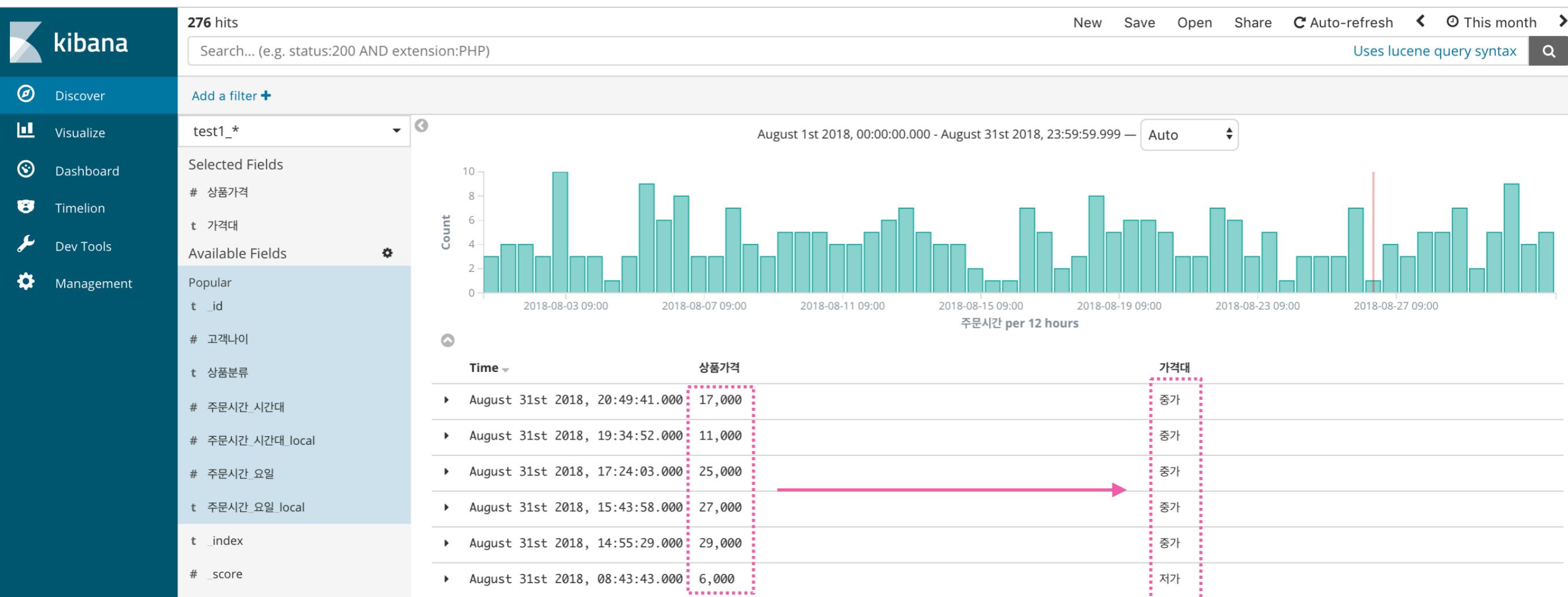
August 1st 2018, 00:00:00.000 - August 31st 2018, 23:59:59.999 — Auto

주문시간 per 12 hours

Time ▾ 고객나이 연령대

Time	고객나이	연령대
▶ August 31st 2018, 20:49:41.000	36	20~30대
▶ August 31st 2018, 19:34:52.000	47	40대 이상
▶ August 31st 2018, 17:24:03.000	54	40대 이상
▶ August 31st 2018, 15:43:58.000	18	10대
▶ August 31st 2018, 14:55:29.000	58	40대 이상
▶ August 31st 2018, 08:43:43.000	42	40대 이상
▶ August 31st 2018, 05:56:24.000	31	20~30대
▶ August 31st 2018, 04:51:39.000	31	20~30대
▶ August 31st 2018, 02:19:09.000	33	20~30대
▶ August 30th 2018, 23:25:52.000	26	20~30대
▶ August 30th 2018, 22:09:45.000	37	20~30대
▶ August 30th 2018, 19:31:05.000	52	40대 이상
▶ August 30th 2018, 18:35:08.000	46	40대 이상
▶ August 30th 2018, 16:37:22.000	43	40대 이상

예제2 - Scripted Field



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

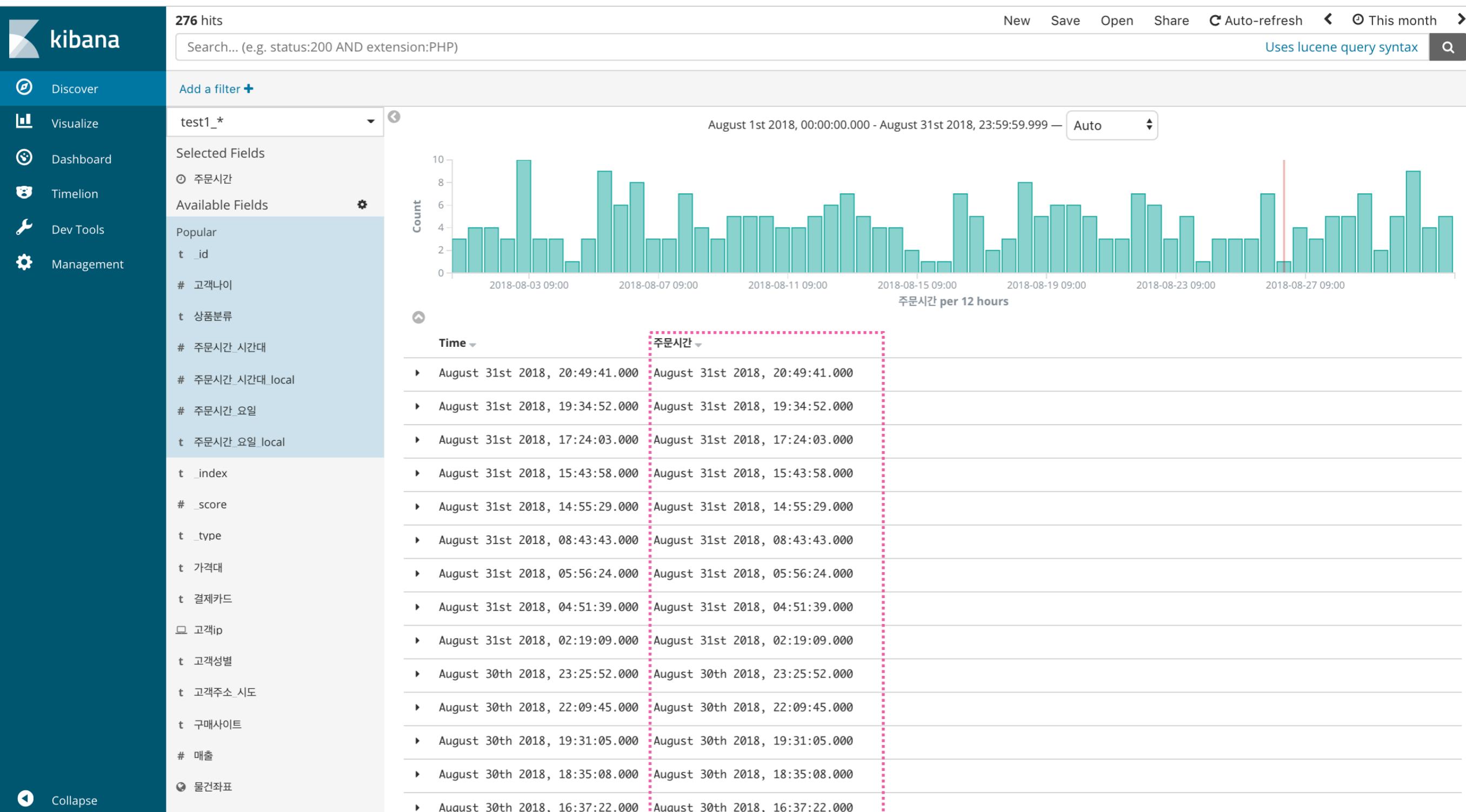
2017년 11월 20일 17시 44분

11/20/2017 5:44pm

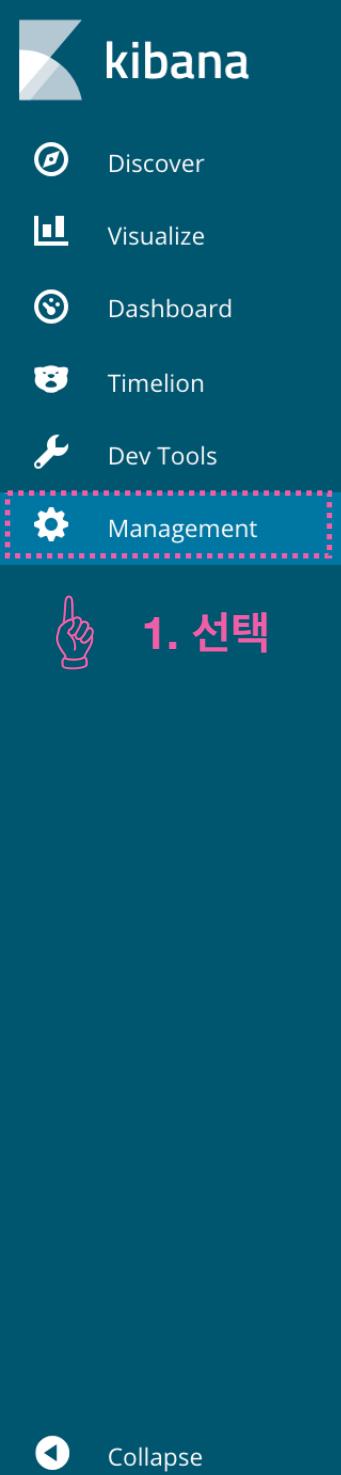
2018년07월01일

July 1st 2018, 9:05:21 pm

Default는 아래와 같은 Format이다



Date Format 변경하려는 Field의 Controls 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 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		✓	✓		

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

Collapse

Discover에 돌아가서 확인하자

아래 표를 이용해서 여러가지 Format을 테스트해보자 (권장)

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 Timestamp 밀리초

String를 다르게 표현할 수 없나?

higee.io/221111469658

221111469658

higee.io/221111469658 (링크 형식)

[221111469658](https://221111469658.higee.io) (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

kibana

10 hits

New Save Open Share

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

Add a filter +

Discover Visualize Dashboard Timelion Dev Tools Management

Selected Fields Available Fields

higee_url

full_url partial_url

full_url	partial_url
http://higee.io/221111469658	221111469658
http://higee.io/221285621862	221285621862
http://higee.io/221285621862	221285621862
http://higee.io/221111469658	221111469658
http://higee.io/221247452452	221247452452
http://higee.io/221111469658	221111469658
http://higee.io/221247452452	221247452452

The screenshot shows the Kibana Discover interface with 10 hits. The results are categorized into two columns: 'full_url' and 'partial_url'. The 'full_url' column contains full URLs like 'http://higee.io/221111469658' and 'http://higee.io/221285621862'. The 'partial_url' column contains the numeric parts of the URLs, such as '221111469658' and '221285621862'. Both columns have their first 10 entries highlighted with a pink dashed box.

Default는 아래와 같은 Format이다

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

- Header:** 10 hits, New, Save, Open, Share, Uses lucene query syntax.
- Search Bar:** Search... (e.g. status:200 AND extension:PHP)
- Left Sidebar:** Discover, Visualize, Dashboard, Timelion, Dev Tools, Management.
- Selected Field:** higee_url
- Available Fields:** t _id, t _index, # _score, t _type, # age, t city.
- Table Data:** Two columns are shown:
 - full_url:** A column containing URLs like "http://higee.io/221111469658". This column is highlighted with a pink dashed border.
 - partial_url:** A column containing the numeric parts of the URLs, such as "221111469658". This column is also highlighted with a pink dashed border.

Two pink arrows point downwards from the bottom of the "full_url" and "partial_url" columns towards the text "URL 형태를 띠는 두 Field의 Format을 String에서 URL로 변경해보자".

full_url	partial_url
http://higee.io/221111469658	221111469658
http://higee.io/221285621862	221285621862
http://higee.io/221285621862	221285621862
http://higee.io/221111469658	221111469658
http://higee.io/221247452452	221247452452
http://higee.io/221111469658	221111469658
http://higee.io/221247452452	221247452452

URL 형태를 띠는 두 Field의 Format을 String에서 URL로 변경해보자

Data Format 변경하려는 Field의 Control 선택 - full_url

2. 선택 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

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

kibana

10 hits

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

New Save Open Share

Uses lucene query syntax

Discover Add a filter +

Visualize higee_url

Dashboard Selected Fields

Timelion t full_url

Dev Tools t partial_url

Management Available Fields

t _id

t _index

_score

t _type

age

t city

full_url	partial_url
http://higee.io/221111469658	221111469658
http://higee.io/221285621862	221285621862
http://higee.io/221285621862	221285621862
http://higee.io/221111469658	221111469658
http://higee.io/221247452452	221247452452
http://higee.io/221111469658	221111469658
http://higee.io/221247452452	221247452452

 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

Label.Template

#{{value}}

5. Label Template : # {{value}} 입력

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

The screenshot shows the Kibana Discover interface. On the left sidebar, the 'Discover' icon is highlighted. The main area displays 10 hits for the query 'Search... (e.g. status:200 AND extension:PHP)'. The results are grouped under two fields: 'full_url' and 'partial_url'. A pink dashed box highlights the 'partial_url' section, which contains multiple entries, each preceded by a '#' symbol. A pink hand icon points to one of these entries.

Field	Value
full_url	http://higee.io/221111469658 http://higee.io/221285621862 http://higee.io/221285621862 http://higee.io/221111469658 http://higee.io/221111469658 http://higee.io/221111469658 http://higee.io/221111469658 http://higee.io/221247452452 http://higee.io/221111469658 http://higee.io/221247452452
partial_url	#221111469658 #221285621862 #221285621862 #221111469658 #221111469658 #221111469658 #221111469658 #221111469658 #221247452452 #221111469658 #221247452452

클릭 가능하게 바꿔보이며 클릭하면 제대로 링크로 이동한다

url 변환 작업은 어떤 경우에 유용하게 사용할 수 있을까?

블로그 포스트 별 metric을 시각화하고 원문을 쉽게 확인할 수 있다

kibana

Visualize / New Visualization (unsaved)

Save Share Refresh

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

Add a filter +

higee_url

Data Options

Metrics

- Metric Count
- Metric Average age
- Metric Unique count of city

Add metrics

Buckets

Split Rows partial_url: Descending

Add sub-buckets

Export: Raw Formatted

글 번호	조회수	평균 연령	접속 도시
#221111469658	6	29.833	4
#221247452452	2	17	2
#221285621862	2	20	2

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 Discover interface. The left sidebar has icons for Discover (selected), Visualize, Dashboard, Timelion, Dev Tools, and Management. The main area shows a search bar with "Search... (e.g. status:200 AND extension:PHP)" and a "Uses lucene query syntax" link. The results section shows 4 hits for the query "higee_number". The results are listed as follows:

- byte: 31 duration: 5,013 percent: 0.2 _id: 5bg1dmUB989Vp88ExThR _type: test _index: higee_number _score: 1
- byte: 8,191 duration: 1,005 percent: 0.6 _id: 4rg1dmUB989Vp88ExDja _type: test _index: higee_number _score: 1
- byte: 135,351 duration: 335,513 percent: 0.2 _id: 5Lg1dmUB989Vp88ExTgr _type: test _index: higee_number _score: 1
- byte: 13,535,139 duration: 33 percent: 0.75 _id: 47g1dmUB989Vp88ExTgD _type: test _index: higee_number _score: 1

Default는 아래와 같은 Format이다

Kibana Discover interface showing search results for the field 'higee_number'. The results are highlighted with a red dashed box. A pink arrow points from the bottom of the highlighted area down to the text 'Number 들에 의미를 부여해보자'.

Selected Fields: higee_number

Available Fields:

- _id
- _index
- _score
- _type
- byte
- duration
- percent

Results:

- byte: 31 duration: 5,013 percent: 0.2 _id: 5bg1dmUB989Vp88ExThR _type: test _index: higee_number _score: 1
- byte: 8,191 duration: 1,005 percent: 0.6 _id: 4rg1dmUB989Vp88ExDja _type: test _index: higee_number _score: 1
- byte: 135,351 duration: 335,513 percent: 0.2 _id: 5Lg1dmUB989Vp88ExTgr _type: test _index: higee_number _score: 1
- byte: 13,535,139 duration: 33 percent: 0.75 _id: 47g1dmUB989Vp88ExTgD _type: test _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

The screenshot shows the Kibana Discover interface. On the left, there's a sidebar with icons for Discover, Visualize, Dashboard, Timelion, Dev Tools, and Management. The 'Discover' icon is highlighted. The main area shows a dropdown menu for the 'duration' field, which is currently selected. The dropdown contains five items: 83.55, 16.75, 5591.88, 0.55, and duration (초). A pink dashed box highlights the 'duration (초)' item. To the right of the dropdown, a large black-bordered box displays the same five values. Below this box is a pink hand icon pointing towards it, with the text 'minute 단위로 변환됐다!' (Converted to minute units!) written next to it.

4 hits

New Save Open Share

Uses lucene query syntax

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

Discover

Add a filter +

higee_number

Selected Fields

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

duration

duration (초)

83.55

16.75

5591.88

0.55

duration (초)

5,013

1,005

335,513

33

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](#).

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

Numeral.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

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

- Left Sidebar:** Includes icons for kibana, Discover (selected), Visualize, Dashboard, Timelion, Dev Tools, and Management.
- Header:** Shows "4 hits" and a search bar with placeholder text "(e.g. status:200 AND extension:PHP)".
- Selected Fields:** A dropdown menu is open, showing "higee_number" and "Selected Fields". Under "Selected Fields", the "byte" field is highlighted with a pink dashed box. Other available fields listed include # _id, # _index, # _score, # _type, # duration, and # percent.
- Visualizations:** A histogram visualization for the "byte" field is displayed. The x-axis is labeled "byte (바이트)" and the y-axis shows the count of documents. The data points are:
 - 31B
 - 7.999KB
 - 132.179KB
 - 12.908MB
- Text Overlay:** A pink callout bubble with a hand icon contains the text "바이트(B, KB, MB, ...)로 표시되어 가독성이 좋아졌다" (It's good that it's displayed in bytes (B, KB, MB, ...)).

Data Format 변경하려는 Field의 Control 선택 - percentage

Management / Kibana

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern ★ higee_number

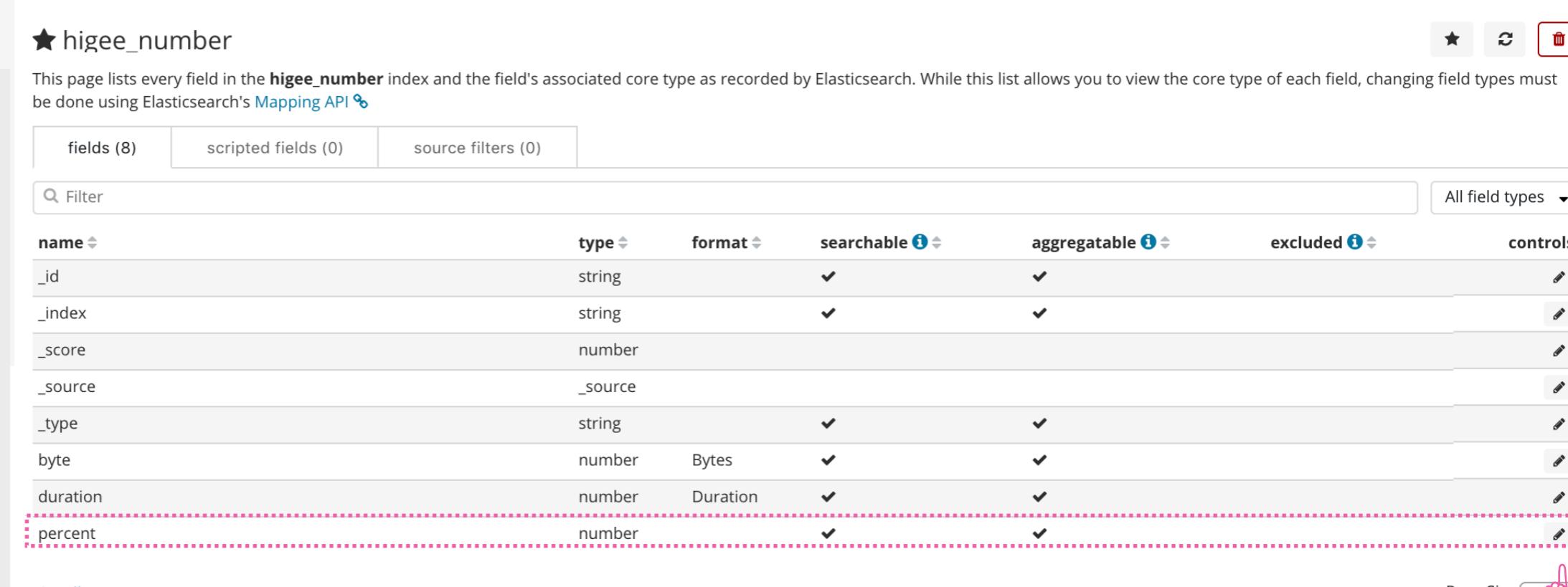
This page lists every field in the **higee_number** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's [Mapping API](#).

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

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

- Header:** 4 hits, New, Save, Open, Share, Uses lucene query syntax.
- Search Bar:** Search... (e.g. status:200 AND extension:PHP)
- Left Sidebar (Discover tab selected):**
 - Selected Fields: higee_number
 - Available Fields: # percent, t _id, t _index, # _score, t _type, # byte, # duration
- Visualizations:** A histogram visualization for the 'percent' field. The x-axis represents the 'percent' field values, and the y-axis represents the frequency or count of those values. The histogram bars are labeled with their corresponding percentages: 20%, 60%, 20%, and 75%. A pink dashed box highlights the 'percent' field name in the dropdown menu.
- Annotation:** A pink callout bubble with a hand icon points to the 'percent' field in the dropdown menu, with the text "소수점 형태가 백분율 형태로 표시되어 가독성이 좋아졌다" (The decimal point form is displayed as a percentage, making it more readable).

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 main area is titled "Dashboard". At the top right, there is a search bar with the placeholder "Search...", a blue button with a plus sign, a hand icon, the text "2. 선택", and navigation arrows. A pink dashed box highlights the "Select" icon and its corresponding step text. The main workspace is currently empty.

Dashboard

Search... + 2. 선택

1. 선택

Dashboard에 visualizations를 추가하자

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.

Dashboard에 visualizations를 추가하자

Dashboard / Editing New Dashboard

Save Cancel Add Options Share Auto-refresh < ⏪ Last 15 minutes >

Add Panels

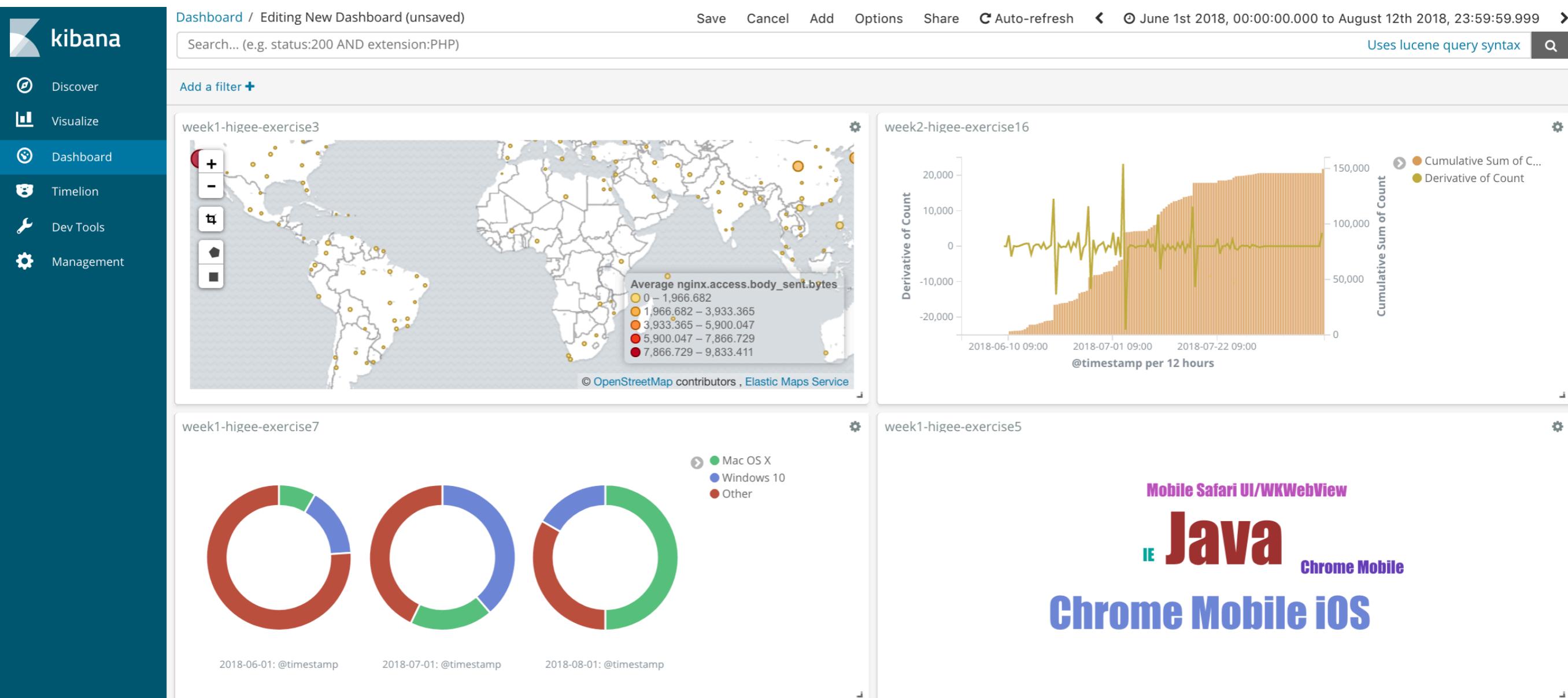
Visualization Saved Search

🔍 higee 4. id 입력 1-15 of 15 Add new Visualization

Name ▲

- week1-higee-exercise1
- week1-higee-exercise2
- week1-higee-exercise3
- week1-higee-exercise5
- week1-higee-exercise7
- week2-higee-exercise10
- week2-higee-exercise11
- week2-higee-exercise12
- week2-higee-exercise13
- week2-higee-exercise14
- week2-higee-exercise15
- week2-higee-exercise16
- week2-higee-exercise17
- week2-higee-exercise8
- week2-higee-exercise9

Visualization을 적당히 배치하자 (위치, 크기)



Dashboard를 저장하자

Dashboard / Editing higee-dashboard (unsaved)

Save dashboard

Title  **2. Dashboard Title 입력 (id-dashboard)**

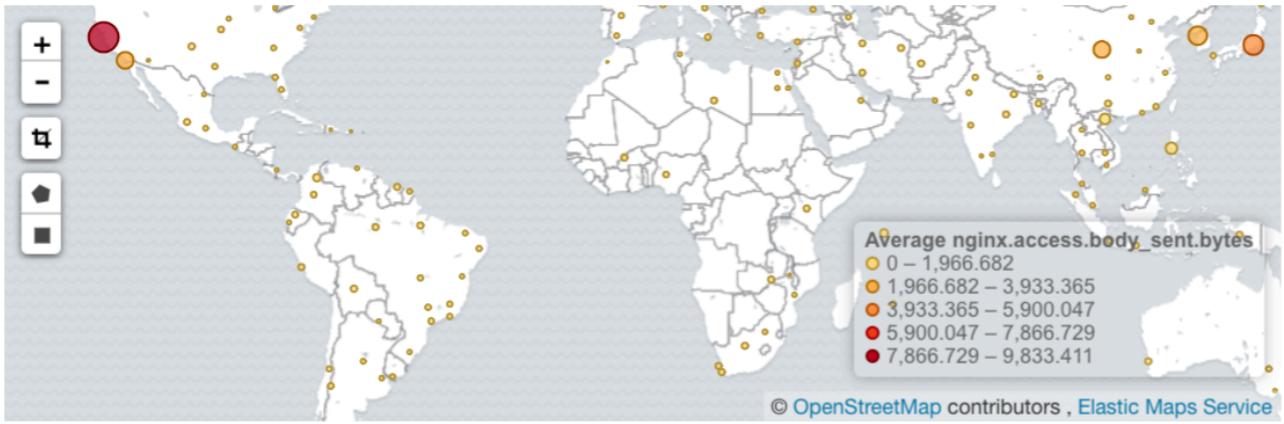
Description

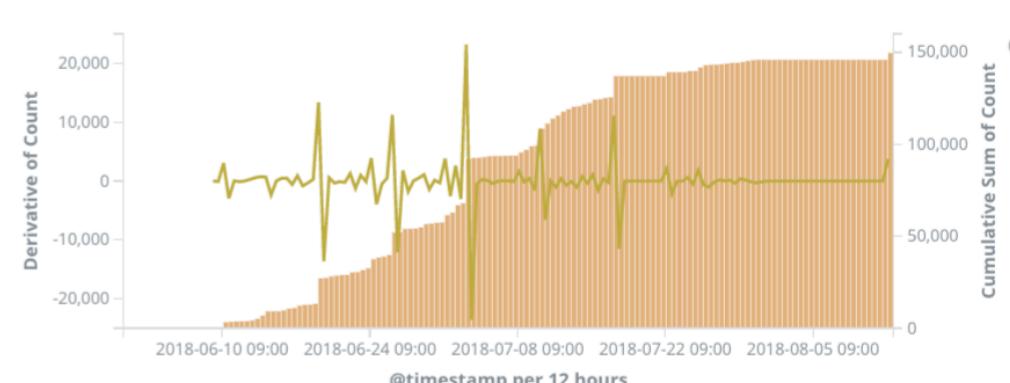
Store time with dashboard
This changes the time filter to the currently selected time each time this dashboard is loaded.

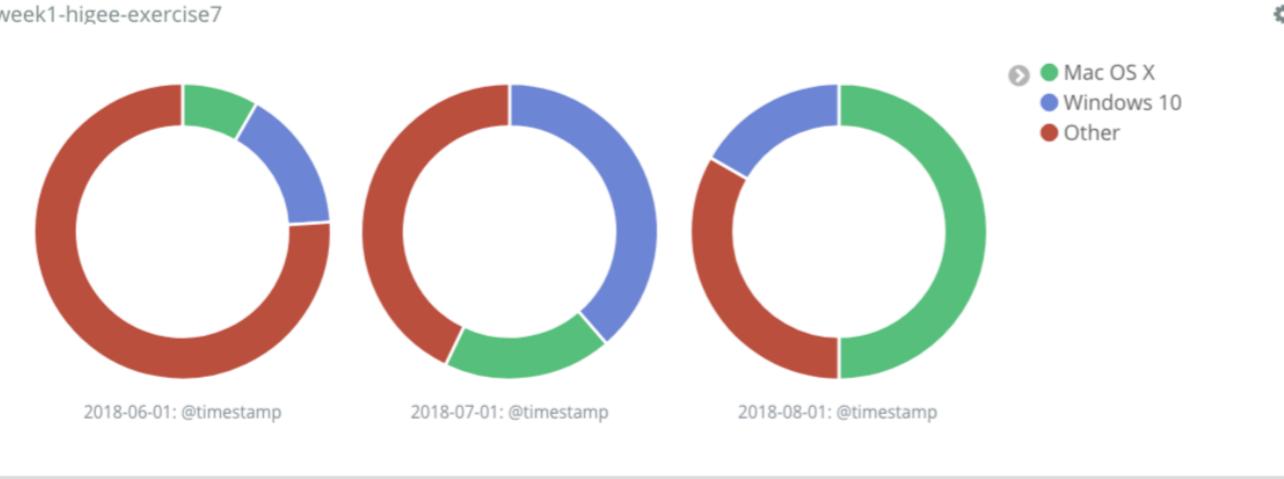
Save  **3. 선택**

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

Add a filter +

week1-higee-exercise3 

week2-higee-exercise16 

week1-higee-exercise7 

week1-higee-exercise5 

Chrome Mobile **Java** **IE** **Mobile Safari UI/WKWeb**
Chrome Mobile iOS

1. 선택 

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

Dashboard를 조회하자

Dashboard / nginx

Full screen Share Clone Edit Auto-refresh < ⌚ June 1st 2018, 00:00:00.000 to August 12th 2018, 23:59:59.999 >

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/67.0.3396.99 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/67.0.3396.99 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/67.0.3396.99 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/67.0.3396.99 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/67.0.3396.99 Safari/537.36"
```

[nginx] region maps

A world map where countries are colored based on their traffic volume. A legend on the right shows five categories of traffic count:

Count
1 – 23,274.8
23,274.8 – 46,548.6
46,548.6 – 69,822.4
69,822.4 – 93,096.2
93,096.2 – 116,370

© OpenStreetMap contributors, Elastic Maps Service, Made with NaturalEarth

Collapse

Dashboard를 clone하자

Dashboard / nginx

Full screen Share Clone Edit Auto-refresh June 1st 2018, 00:00:00.000 to August 12th 2018, 23:59:59.999

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

Add a filter +

[nginx] markdown

Nginx Access.Log Dashboard

66.249.82.131 - - [13/Jun/2018:17:01:02 +0000] "GET /index.html HTTP/1.1" 200 12345 "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] "GET /index.html HTTP/1.1" 200 12345 "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] "GET /index.html HTTP/1.1" 200 12345 "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 /index.html HTTP/1.1" 200 12345 "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 /index.html HTTP/1.1" 200 12345 "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] region maps

Clone Dashboard

Please enter a new name for your dashboard.

nginx-higee

Cancel Confirm Clone

3. 선택

Count

- 1 – 23,274.8
- 23,274.8 – 46,548.6
- 46,548.6 – 69,822.4
- 69,822.4 – 93,096.2
- 93,096.2 – 116,370

© OpenStreetMap contributors , Elastic Maps Service , Made with NaturalEarth

Collapse

1. 선택

2. 이름 입력 nginx-{id}

3. 선택

Clone 받은 환경에서 Dashboard를 사용할 수 있다

Dashboard / nginx-higee 

Full screen Share Clone Edit Auto-refresh June 1st 2018, 00:00:00.000 to August 12th 2018, 23:59:59.999

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

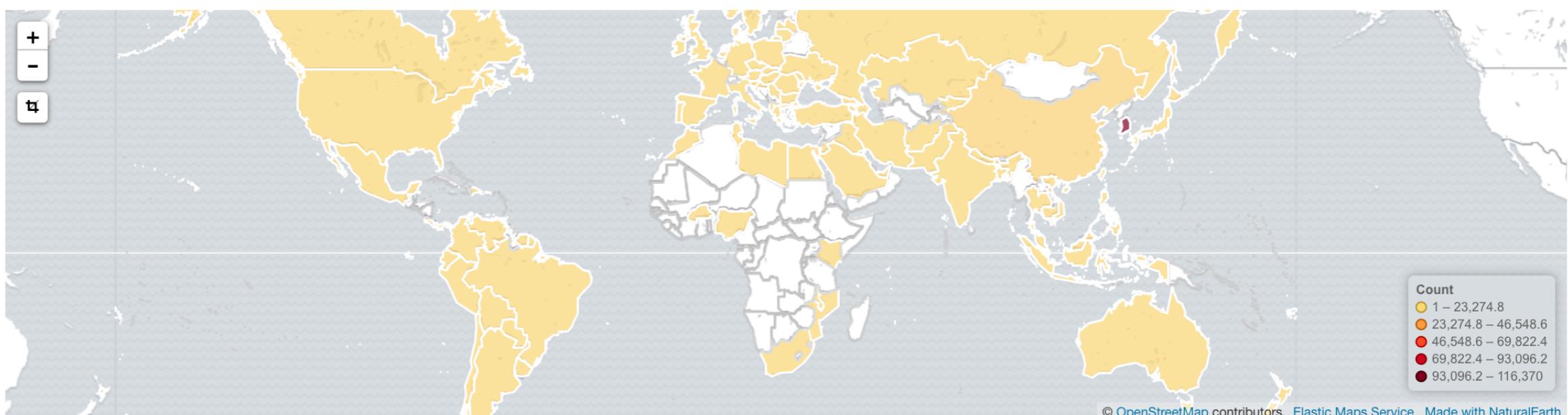
Add a filter +

[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/67.0.3396.99 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/67.0.3396.99 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/67.0.3396.99 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/67.0.3396.99 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/67.0.3396.99 Safari/537.36"
```

[nginx] region maps



A world map where countries are colored based on their count of something. The legend indicates the following ranges:

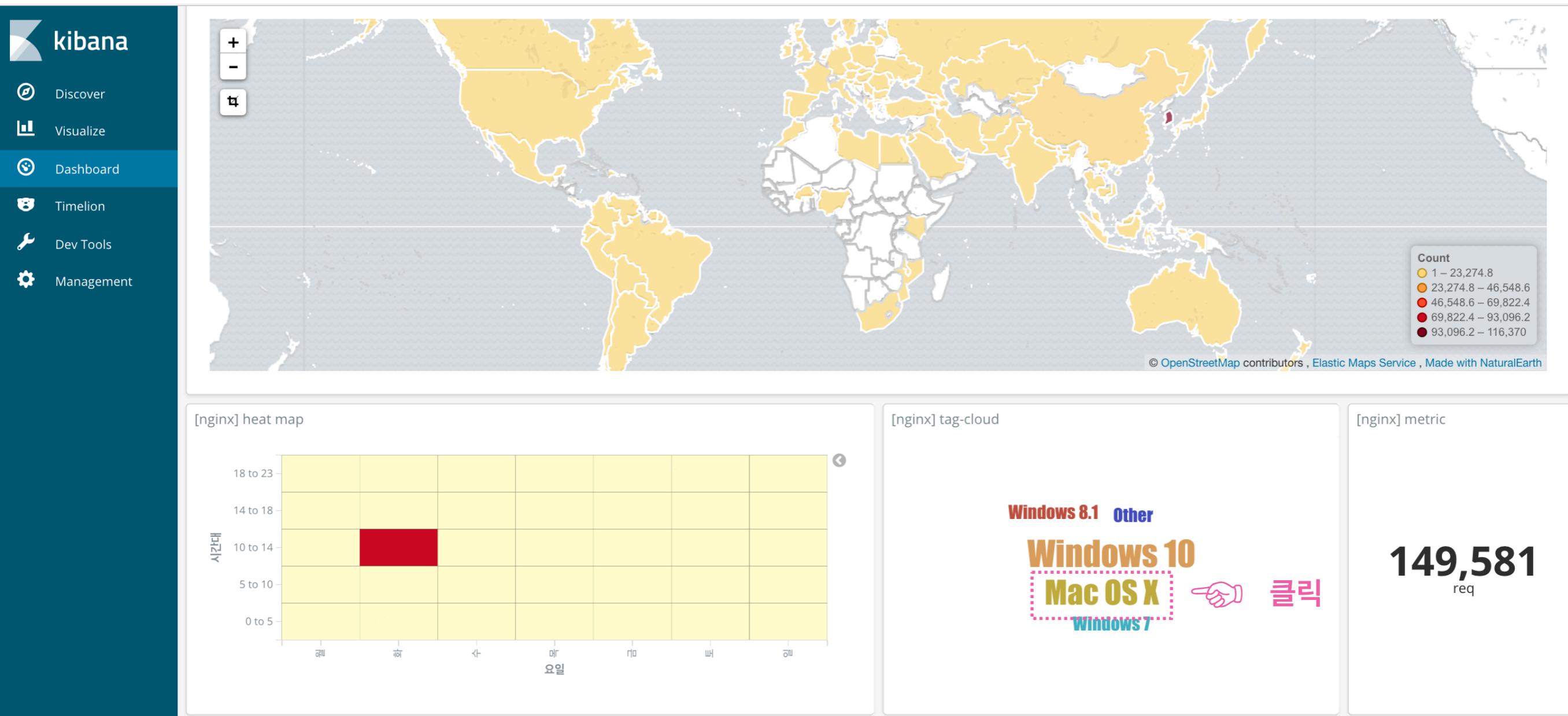
Count Range	Color
1 – 23,274.8	Yellow
23,274.8 – 46,548.6	Orange
46,548.6 – 69,822.4	Red
69,822.4 – 93,096.2	Dark Red
93,096.2 – 116,370	Maroon

© OpenStreetMap contributors, Elastic Maps Service, Made with NaturalEarth

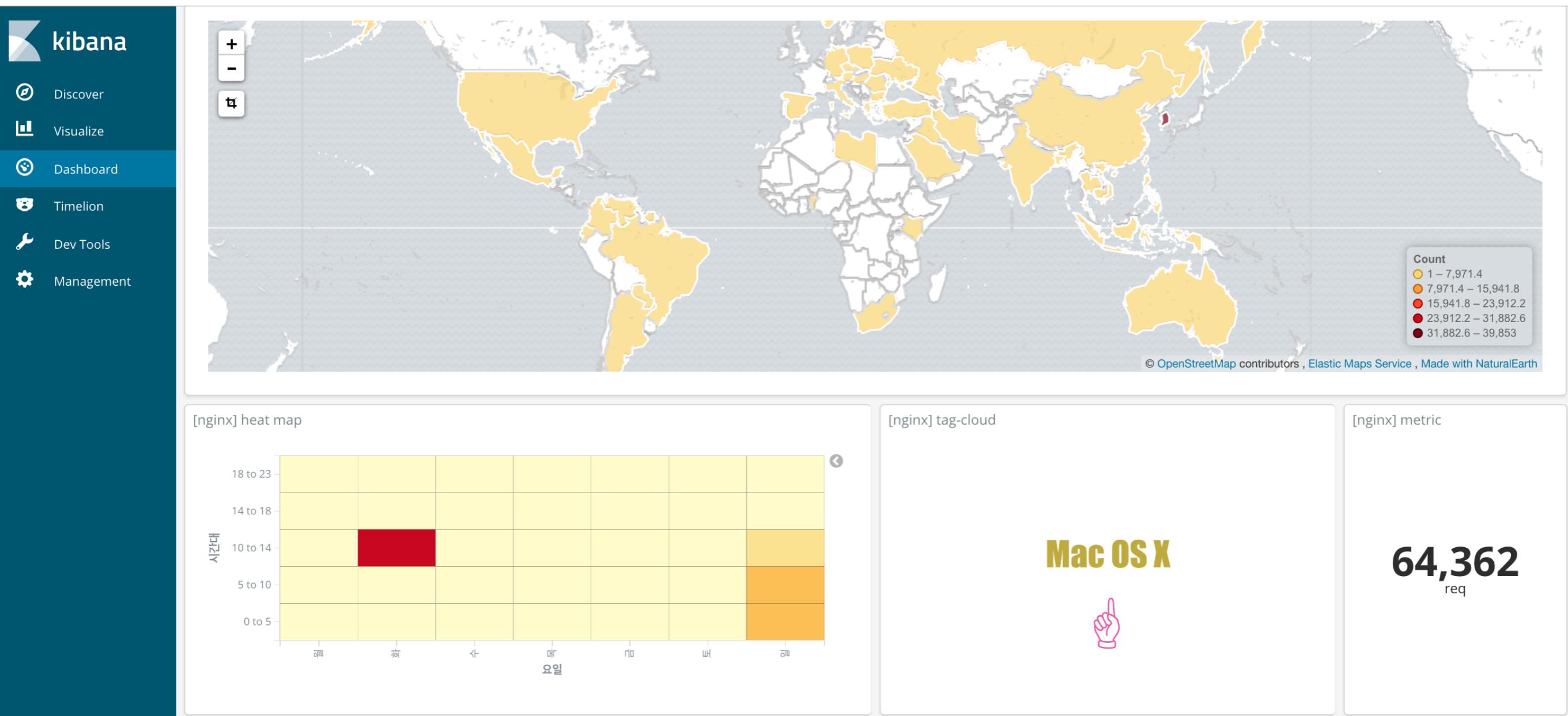
Collapse

Dashboard가 Interactive하다!

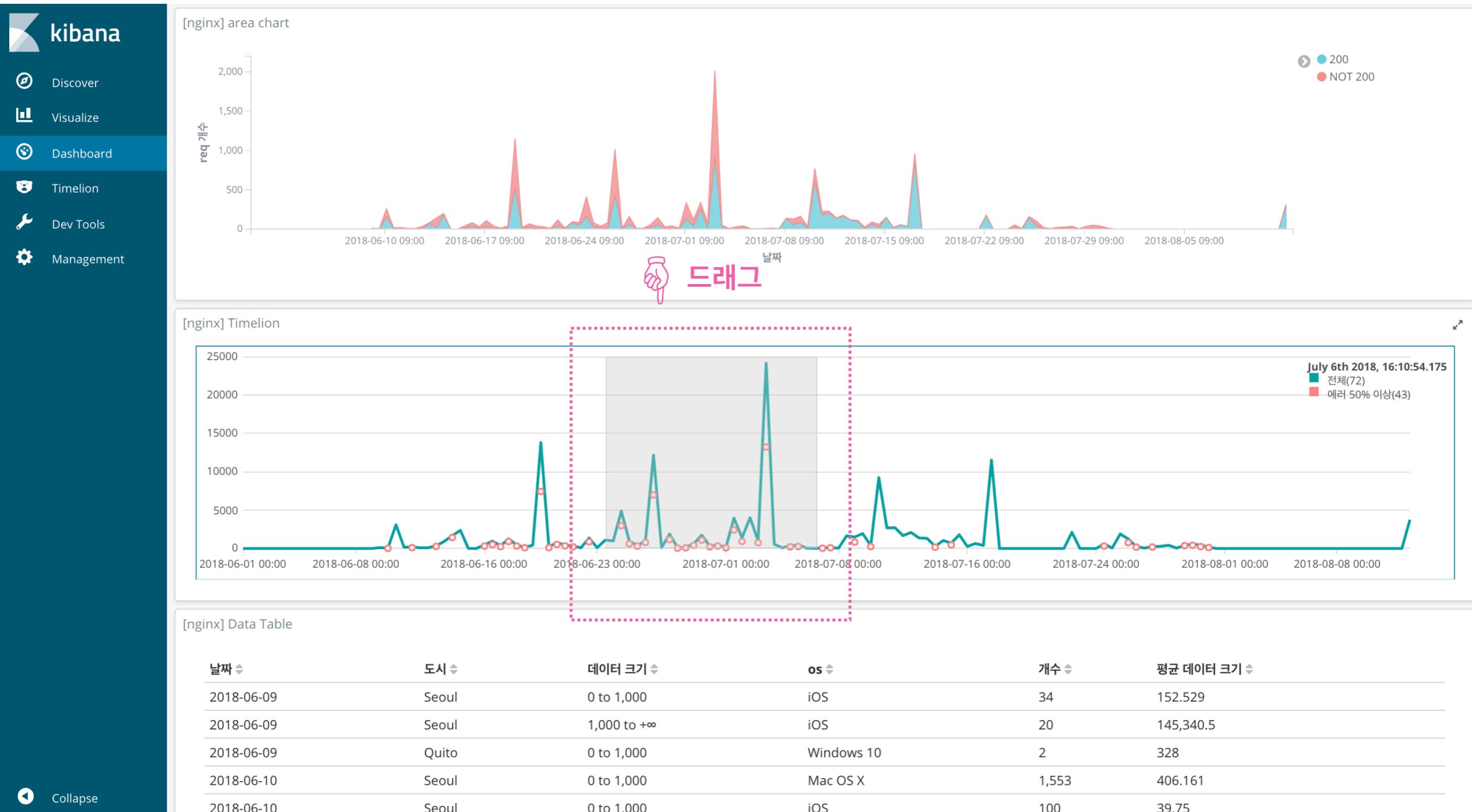
아래의 Dashboard에서 “Mac OS X”에 해당하는 데이터만 보고 싶다고 하자



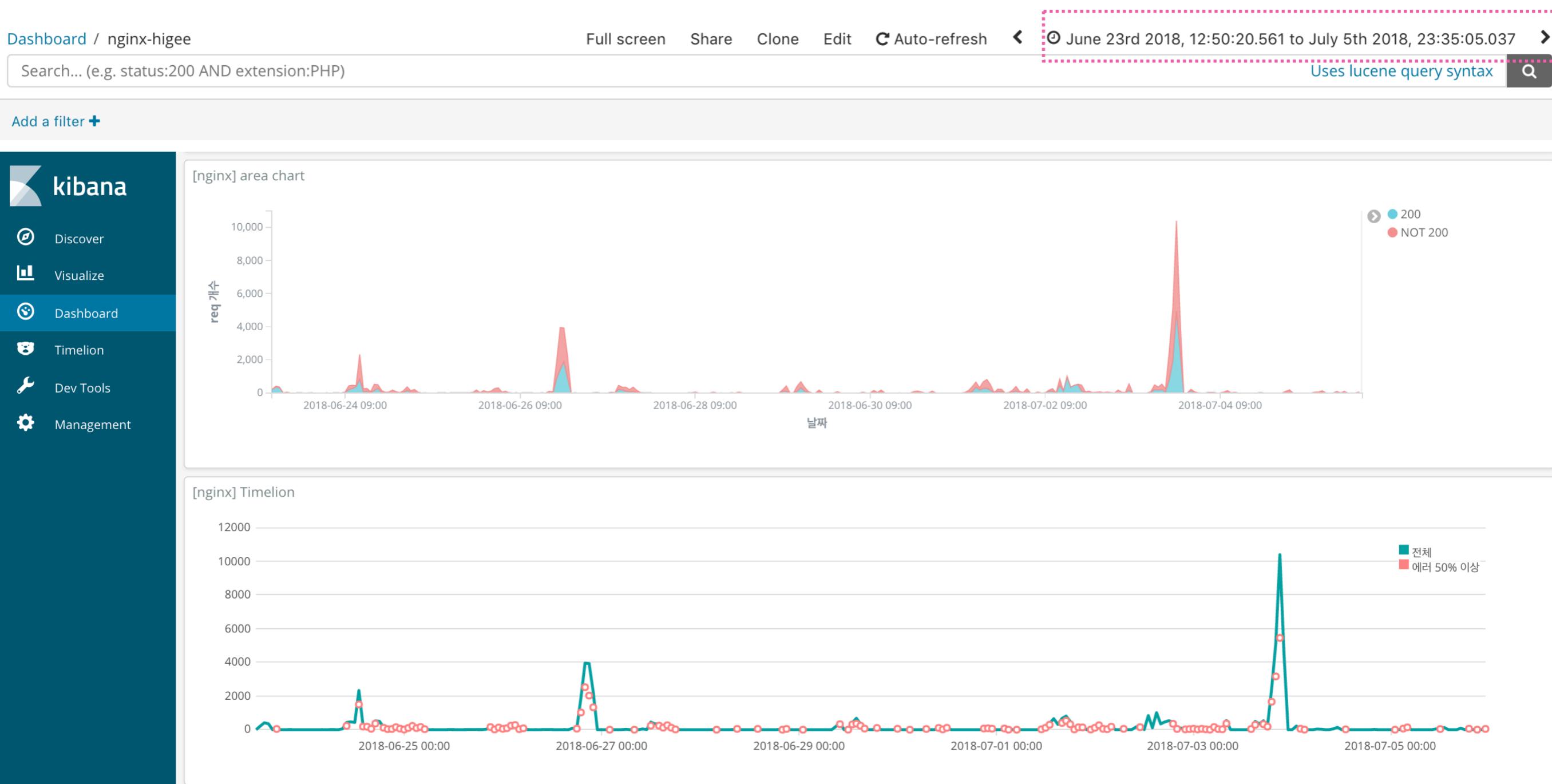
Dashboard 전체적인 UI는 유지한채 “Mac OS X”에 해당하는 값만 필터링되어 보여진다



특정 기간을 집중해서 보고 싶으면 Drag를 하자

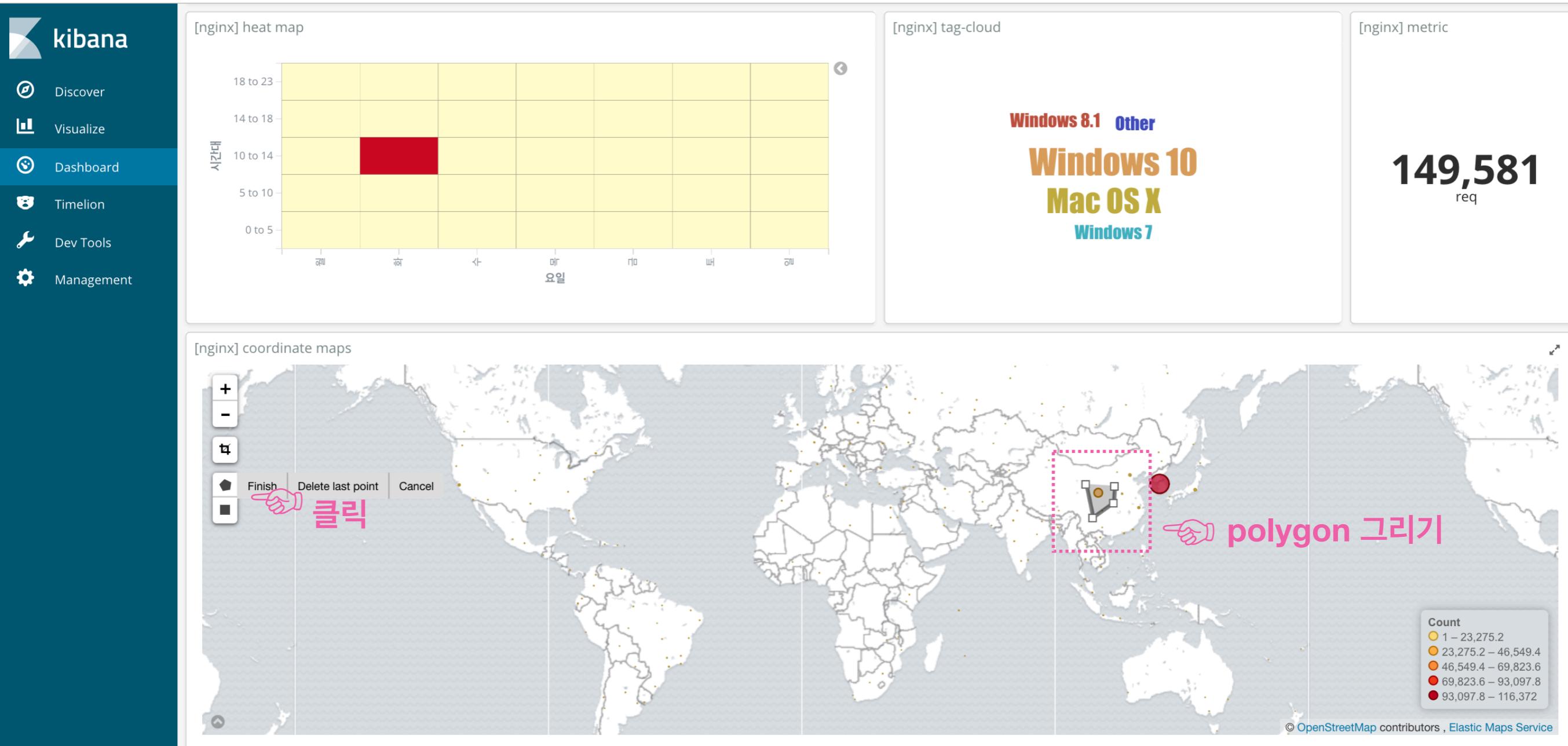


특정 기간을 집중해서 보고 싶으면 Drag를 하자



드래그한 기간 내의 데이터만 보여진다

특정 지역의 데이터만 보고 싶으면 polygon/rectangle을 그려자



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** < ⏪ June 1st 2018, 00:00:00.000 to August 12th 2018, 23:59:59.999 ⏩

Discover Visualize Dashboard Timelion Dev Tools Management

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/favicon/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/537.31 (KHTML, like Gecko) Chrome/65.0.3325.185 Safari/537.31"
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/537.31 (KHTML, like Gecko) Chrome/65.0.3325.185 Safari/537.31"
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/537.31 (KHTML, like Gecko) Chrome/65.0.3325.185 Safari/537.31"
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_12_3) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/65.0.3325.185 Safari/537.31"
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_12_3) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/65.0.3325.185 Safari/537.31"
```

[nginx] region maps

Count
1 – 23,274.8
23,274.8 – 46,548.6
46,548.6 – 69,822.4
69,822.4 – 93,096.2
93,096.2 – 116,370

© OpenStreetMap contributors, Elastic Maps Service, Made with NaturalEarth

설정한 간격마다 Index 데이터를 확인하여 새로운 데이터가 있으면 Dashboard에 반영한다

dashboard를 공유하자

1. Share 선택

The screenshot shows the Kibana interface for sharing a dashboard. On the left, there's a sidebar with icons for Discover, Visualize, Dashboard, Timelion, Dev Tools, and Management. The main area has a title "Dashboard / nginx-higee". It contains sections for "Share saved dashboard" and "Share Snapshot".

Share saved dashboard: This section allows sharing the most recent saved version of the dashboard. It includes an "Embedded iframe" code snippet and a "Link" URL.

Share Snapshot: This section allows sharing the current state of the dashboard. It also includes an "Embedded iframe" code snippet and a "Link" URL. A note says: "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."

Bottom Content: The "Saved Dashboard" and "Snapshot" sections are connected by a double-headed arrow. Below them is a "Nginx Access Log Dashboard" section showing log entries:

```
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_12_3) AppleWebKit/537.3  
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)  
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)  
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_12_3) AppleWebKit/537.3  
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_12_3) AppleWebKit/537.3
```

dashboard를 공유하자

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

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' page. The 'Dashboards' tab is selected. A pink dashed box highlights the 'nginx-higee' item in the list, with a callout '4. nginx-{id} 선택'. Another pink dashed box highlights the 'Export' button, with a callout '5. Export 선택'. A pink dashed arrow points down from the 'Export' button to the '6. {id}_dashboard.json 이름 변경' callout at the bottom right.

Dashboard export



```
higee-dashboard.json  ×
1 [
2 {
3   "_id": "a267afc0-a942-11e8-8d82-2973ec7f077b",
4   "_type": "dashboard",
5   "_source": {
6     "title": "nginx-higee",
7     "hits": 0,
8     "description": "",
9     "panelsJSON": "[{\\"embeddableConfig\\":{\\"vis\\":{\\"defaultColors\\":{\\\"0 - 350\\\":\\\"rgb(247,252,245)\\\",\\\"1,050 - 1,400\\\":\\\"rgb(35,139,69)\\\",\\\"350 - 700\\\":\\\"rgb(199,233,192)\\\"}}}],\\\"optionsJSON\\":{\\"darkTheme\\":false,\\\"hidePanelTitles\\":false,\\\"useMargins\\":true}}",
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



2. Saved Objects 선택

Management / Kibana

Index Patterns Saved Objects Advanced Settings

Edit Saved Objects

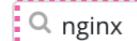
Export Everything

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 (13)

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] heat map2

[nginx] horizontal bar

[nginx] markdown

[nginx] metric

[nginx] pie chart

[nginx] region maps

[nginx] tag-cloud

[nginx] Timelion

13 selected

7.

다운 받은 후

{id}_visualization.json 이름 변경

5. nginx로 시작하는 모든 visualization 선택

Visualization export

```
higee-visualizations.json  x
[
  {
    "_id": "7a9123a0-6f27-11e8-a0fb-51f0eb991705",
    "_type": "visualization",
    "_source": {
      "title": "[nginx] coordinate maps",
      "visState": "{\"title\":\"[nginx] coordinate maps\",\"type\":\"tile_map\",\"params\":{\"mapType\":\"Scaled Circle Markers\",\"isDesaturated\":true,\"addTooltip\":true,\"heatmaps\":false},\"uiStateJSON\":{},\"description\": \"\",\"version\": 1,\"kibanaSavedObjectMeta\": {\"searchSourceJSON\": \"{\\\"index\\\":\\\"b8c6bd20-87db-11e8-8161-3b4280559eb3\\\",\\\"filter\\\":[],\\\"query\\\":{\\\"query\\\":\\\"\\\",\\\"language\\\":\\\"lucene\\\"}}\"}}",
      "kibanaObjectMeta": {}
    }
  },
  {
    "_id": "08e28cc0-6f28-11e8-a0fb-51f0eb991705",
    "_type": "visualization",
    "_source": {
      "title": "[nginx] region maps",
      "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]},\"description\": \"\",\"version\": 1,\"kibanaSavedObjectMeta\": {\"searchSourceJSON\": \"{\\\"index\\\":\\\"b8c6bd20-87db-11e8-8161-3b4280559eb3\\\",\\\"filter\\\":[],\\\"query\\\":{\\\"query\\\":\\\"\\\",\\\"language\\\":\\\"lucene\\\"}}\"}}",
      "kibanaObjectMeta": {}
    }
  },
  {
    "_id": "cfbbc570-6f26-11e8-a0fb-51f0eb991705",
    "_type": "visualization",
    "_source": {
      "title": "[nginx] metric",
      "visState": "{\"title\":\"[nginx] metric\",\"type\":\"metric\",\"params\":{\"addTooltip\":true,\"addLegend\":false,\"type\":\"metric\",\"metric\":{},\"percentageMode\":false,\"uiStateJSON\":{},\"description\": \"\",\"version\": 1,\"kibanaSavedObjectMeta\": {\"searchSourceJSON\": \"{\\\"index\\\":\\\"b8c6bd20-87db-11e8-8161-3b4280559eb3\\\",\\\"filter\\\":[],\\\"query\\\":{\\\"query\\\":\\\"\\\",\\\"language\\\":\\\"lucene\\\"}}\"}}",
      "kibanaObjectMeta": {}
    }
  },
  {
    "_id": "c1d84360-6f2c-11e8-a0fb-51f0eb991705",
    "_type": "visualization",
    "_source": {
      "title": "[nginx] area chart",
      "visState": "{\"title\":\"[nginx] area chart\",\"type\":\"line\",\"params\":{\"type\":\"line\",\"grid\":{},\"categoryLines\":false,\"style\":{\\\"color\\\":\\\"#eee\\\"}},\"categoryAxe",
      "uiStateJSON": "{\"vis\":{\\\"colors\\\":{\\\"200\\\":\\\"#6D0E0\\\",\\\"nginx.access.response_code:200\\\":\\\"#F29191\\\"},\\\"legendOpen\":false}}",
      "description": \"\",\"version\": 1,\"kibanaSavedObjectMeta\": {\"searchSourceJSON\": \"{\\\"index\\\":\\\"b8c6bd20-87db-11e8-8161-3b4280559eb3\\\",\\\"filter\\\":[],\\\"query\\\":{\\\"query\\\":\\\"\\\",\\\"language\\\":\\\"lucene\\\"}}\"}}",
      "kibanaObjectMeta": {}
    }
  }
]
```

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 for managing saved objects. At the top, there are tabs for 'Index Patterns', 'Saved Objects' (which is selected), and 'Advanced Settings'. Below the tabs, there are three buttons: 'Dashboards (2)', 'Searches (1)', and 'Visualizations (12)'. A search bar contains the text 'nginx'. On the right side, there are 'Export Everything' and 'Import' buttons. The main area displays a list of 12 selected visualizations, all of which have a checkmark next to them. The list includes: 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, and [nginx] Timelion. A modal dialog box is centered over the list, asking 'Delete selected visualizations?' and stating 'You can't recover deleted visualizations.' It has 'Cancel' and 'Delete' buttons.

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 (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 'Saved Objects' page. On the left, there's a sidebar with various icons. The main area has tabs for 'Dashboards' (2), 'Searches' (1), and 'Visualizations' (0). A search bar at the top says 'nginx'. Below it, there's a list of objects: 'Title' (unchecked), 'nginx' (unchecked), and 'nginx-higee' (checked). A message '1 selected' is shown below the list. A modal dialog box is centered over the list, asking 'Delete selected dashboards?'. It contains the text 'You can't recover deleted dashboards.' and two buttons: 'Cancel' and 'Delete'. Above the modal, there are buttons for 'Export Everything' and 'Import'.

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). The 'Import' button is located next to 'Export Everything'. 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



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

개별 Visualization들을 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: cfbbc570-6f26-11e8-a0fb-51f0eb991705)

Visualization 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}_visualization.json 선택**: A hand icon points to the "Import" modal window.
- 5. No, prompt for each object 선택**: A hand icon points to the "No, prompt for each object" button in the modal window.

The interface includes tabs for Dashboards (2), Searches (1), and Visualizations (0). A search bar at the top contains "nginx". The "Import" modal window asks "Automatically overwrite all saved objects?" with two options: "No, prompt for each object" (highlighted with a red dashed box) and "Yes, overwrite all objects".

Import한 Dashboard에 다시 가보면

Dashboard / nginx-higee Full screen Share Clone Edit Auto-refresh June 1st 2018, 00:00:00.000 to August 12th 2018, 23:59:59.999 < >

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/67.0.3396.99 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/67.0.3396.99 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/67.0.3396.99 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/67.0.3396.99 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/67.0.3396.99 Safari/537.36"
```

[nginx] region maps

Count

- 1 – 23,274.8
- 23,274.8 – 46,548.6
- 46,548.6 – 69,822.4
- 69,822.4 – 93,096.2
- 93,096.2 – 116,370

© OpenStreetMap contributors , Elastic Maps Service , Made with NaturalEarth

Collapse

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				
			1-1 of 1	<	>

Dashboard를 확인하자



Time Picker

Dashboard / shopping

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

Full screen Share Clone Edit ⚡ Auto-refresh < ⏴ This year >

Uses lucene query syntax

Add a filter +

[shopping] markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

• 강의자료
• 강의질문
• Markdown문법

14,977
전체 데이터

[shopping] Tag Cloud

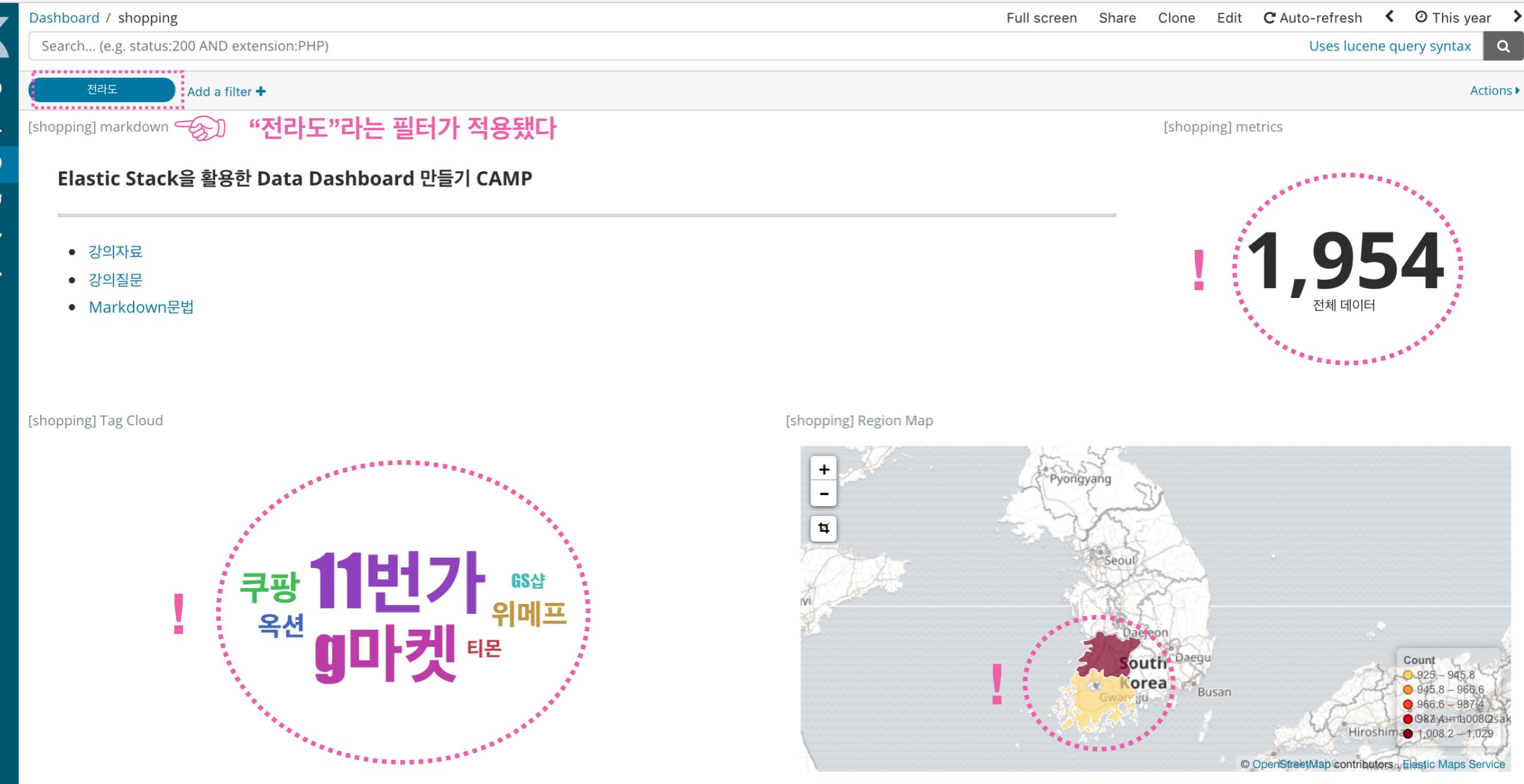
[shopping] Region Map

GS샵
위메프 11번가 티몬
11번가 옥션
g마켓 쿠팡

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



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

Filter를 실행하자

Dashboard / shopping

Full screen Share Clone Edit C Auto-refresh < This year >

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

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

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

14,977 전체 데이터

[shopping] Tag Cloud

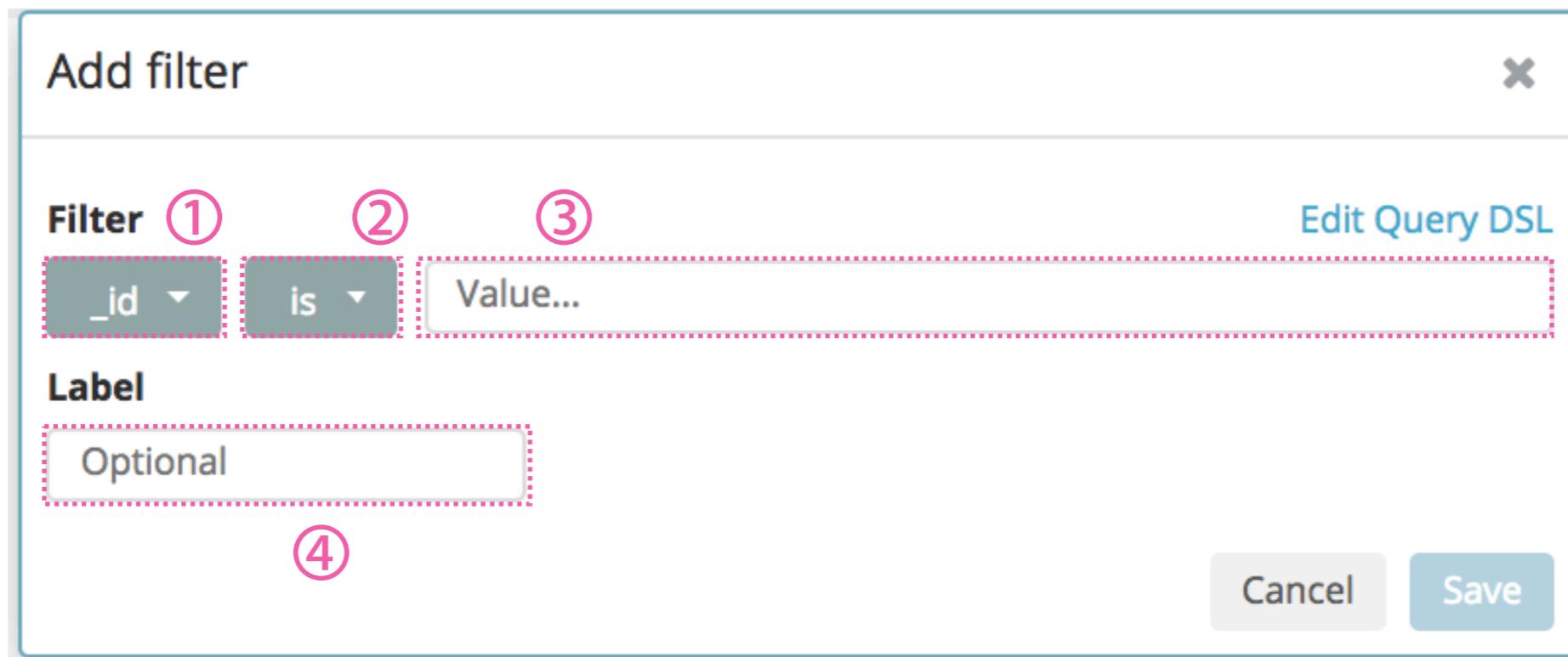
[shopping] Region Map

GS샵
11번가 티몬
옵션 쿠팡
g마켓
위메프
11번가 티몬 옵션 쿠팡

Count
15 – 897.4
897.4 – 1,779.8
1,779.8 – 2,662.2
2,662.2 – 3,544.6
3,544.6 – 4,427

© 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 C Auto-refresh < ⏴ This year >

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

우리카드 Add a filter + Actions ▾

[shopping] markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

4,504
전체 데이터

[shopping] Tag Cloud

[shopping] Region Map

Count
4 - 259.2
259.2 - 514.4
514.4 - 769.6
769.6 - 1,024.0
1,024.8 - 1,280

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

위메프 11번가 티몬 옥션
g마켓 쿠팡 GS샵

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 < This year >

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

즐겨찾기 Add a filter + Actions ▾

[shopping] markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

7,784 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map

© 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 ⏪ ⏴ This year >

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

Uses lucene query syntax

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

[shopping] markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

• 강의자료
• 강의질문
• Markdown문법

6,029 전체 데이터

[shopping] Tag Cloud

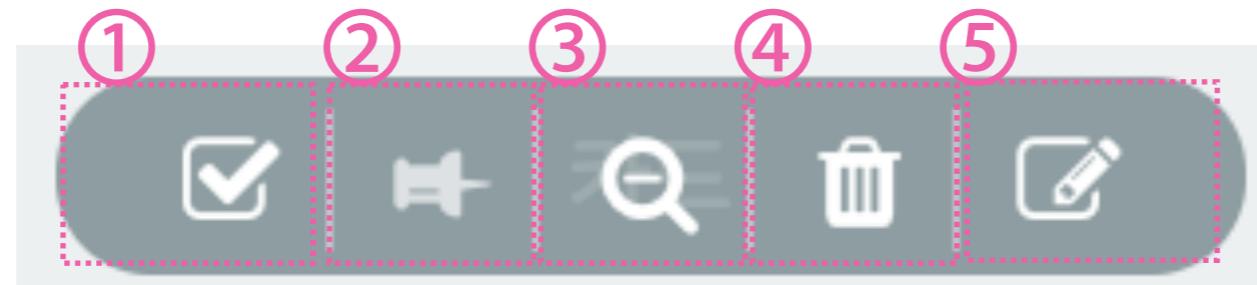
[shopping] Region Map

A choropleth map of South Korea's administrative regions (Gyeonggi-do, Seoul, Incheon, Gwangju, Daejeon, Daegu, Busan, South Korea, North Korea) colored according to data density. The legend indicates five count ranges: 7-358.2 (light yellow), 358.2-709.4 (orange), 709.4-1,060.6 (red), 1,060.6-1,411.8 (dark red), and 1,411.8-1,763 (black).

© OpenStreetMap contributors, Elastic Maps Service

쿠팡 GS샵 11번가 위메프 옥션 티몬
11번가 g마켓

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 : 2018년 6월 1일 ~ 2018년 8월 26일

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 interface. 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 header with a search bar containing the text "shopping". Below the header is a table with the following columns: "Name ↑", "Description", and "Actions". There is one row in the table, which contains the text "shopping" in a blue box, a small icon of a hand pointing right, and the word "선택" (Select). A blue plus sign button is located above the table. At the bottom of the table are navigation arrows and the text "1-1 of 1".

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

1-1 of 1 < >

Query Bar를 확인하자

Dashboard / shopping

Full screen Share Clone Edit C Auto-refresh This year > Uses lucene query syntax

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

Add a filter +

[shopping] markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

• 강의자료
• 강의질문
• Markdown문법

14,977
전체 데이터

[shopping] Tag Cloud

[shopping] Region Map

GS샵
위메프 11번가 티몬
11번가 옥션
g마켓 쿠팡

Count
15 – 897.4
897.4 – 1,779.8
1,779.8 – 2,662.2
2,662.2 – 3,544.6
3,544.6 – 4,427

© OpenStreetMap contributors, Elastic Maps Service

Query Bar를 확인하자

The screenshot shows a Data Dashboard interface for the 'shopping' index pattern. At the top, there's a search bar with placeholder text 'Search... (e.g. status:200 AND extension:PHP)' and a note 'Uses lucene query syntax'. To the right are buttons for 'Full screen', 'Share', 'Clone', 'Edit', 'Auto-refresh' (with a refresh icon), and date range selection ('This year'). Below the search bar is a 'Query Bar' section with a hand icon pointing to the text 'Query Bar'. On the left, there are navigation icons for Kibana, Home, Settings, and others. A sidebar on the left lists filters: '[shopping] markdown' and 'Elastic Stack을 활용한 Data Dashboard 만들기 CAMP'. In the center, there's a large number '14,977' with the text '전체 데이터' below it. On the right, there's a map of South Korea with a color-coded legend for 'Count' (yellow for 15-897.4, orange for 897.4-1,779.8, red for 1,779.8-2,662.2, dark red for 2,662.2-5,544.0, black for 5,544.0-4,427). The map shows higher counts in the southern part of the country.

Query Bar에 뭐라고 검색을 해야될까?

GS샵
위메프 11번가 티몬
옵션
g마켓 쿠팡

Lucene Query의 사용법을 익히자

종류	기능	예시
Keyword 검색	Field에 상관없이 검색어와 일치하는 Doc 검색	여성
Field Match 검색	특정 Field 값이 검색어와 일치하는 Doc 검색	고객성별:여성
Exact Match 검색	특정 Field 값이 검색어와 정확히 일치하는 Doc 검색	배송메모: "상품 이상"
Exists 검색	특정 Field가 non-null value를 가진 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 큰 (또는 작은) Doc 검색	상품가격:>5000
Range 검색	특정 Field 값이 입력값 사이에 있는 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
Must be Present 연산	바로 뒤에 오는 조건을 만족하는 Doc 검색	+예약여부:예약
Must not be Present 연산	바로 뒤에 오는 조건을 만족하지 않는 Doc 검색	-구매사이트:11번가

Search Type - Keyword

Dashboard / shopping

Full screen Share Clone Edit ▶ 5 seconds < ⏪ This year >

우리 Uses lucene query syntax 

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

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

• 강의자료
• 강의질문
• Markdown문법

4,504 전체 데이터

[shopping] Tag Cloud [shopping] Region Map



위메프 11번가 티몬 옥션
g마켓 쿠팡 GS샵

Search Type - Field Match

Dashboard / shopping

Full screen Share Clone Edit ▶ 5 seconds < ⏴ This year >

결제카드:우리 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

4,504 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map



Count
4 - 259.2
259.2 - 514.4
514.4 - 769.6
769.6 - 1,024.8
1,024.8 - 1,280

© OpenStreetMap contributors, Elastic Maps Service

위메프 11번가 티몬 옥션 GS샵
g마켓 쿠팡

Search Type - Exact Field Match

Dashboard / shopping

Full screen Share Clone Edit ▶ 5 seconds < ⏴ This year >

배송메모: "상품 이상"

Add a filter +

[shopping] markdown

1. 입력  [shopping] metrics

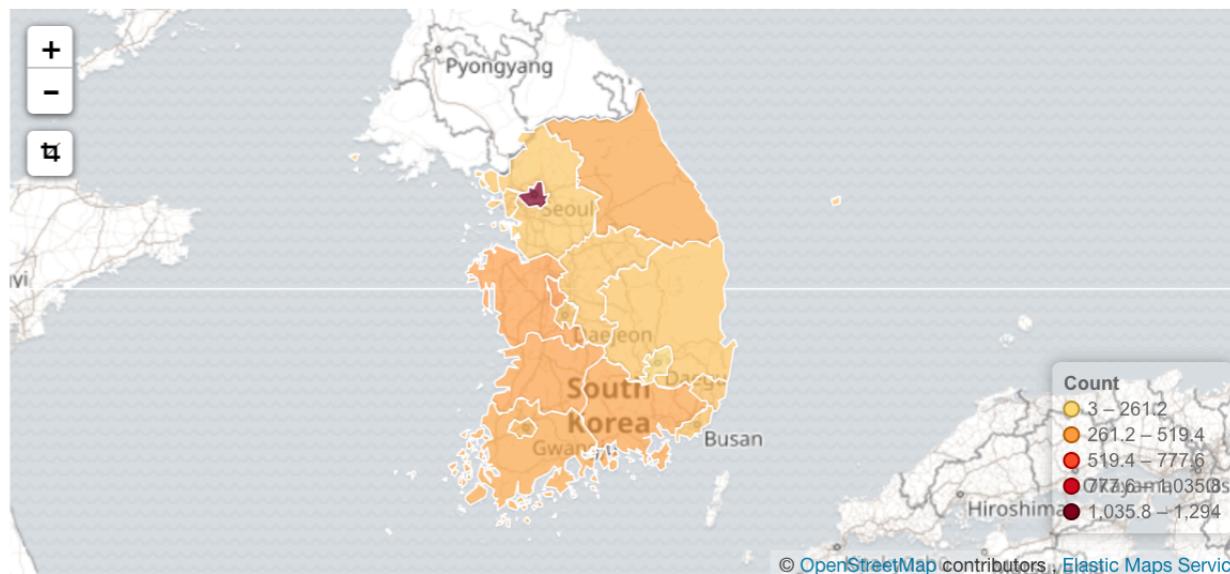
Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

2. 클릭  4,398 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map



GS샵
위메프 11번가 티몬
11번가 옥션
g마켓 쿠팡

Search Type - Term

Dashboard / shopping

상품분류:(“니트” “코트”)

Full screen Share Clone Edit ▶ 5 seconds < ⏴ This year >

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

2,389 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map



Count

- 5 – 144.8
- 144.8 – 284.6
- 284.6 – 424.4
- 424.4 – 564.2
- 564.2 – 704

© OpenStreetMap contributors, Elastic Maps Service

쿠팡 GS샵 11번가 티몬 위메프
g마켓 옥션

Search Type - Fuzzy

Dashboard / shopping

Full screen Share Clone Edit ▶ 5 seconds < ⏴ This year >

고객주소_시도: 전라도~1

Uses lucene query syntax



Add a filter +

[shopping] markdown

1. 입력 

[shopping] metrics

2. 클릭 

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

1,954
전체 데이터

[shopping] Tag Cloud

[shopping] Region Map

쿠팡 옥션 11번가 GS샵 위메프 티몬
g마켓



“전라남도” 와 “전라북도”가 위의 검색에 match된다

Search Type - Proximity

Dashboard / shopping

Full screen Share Clone Edit ▶ 5 seconds < ⏴ This year >

배송메모: "내에 시간 배송 못함"~2

Add a filter +

[shopping] markdown [shopping] metrics

Uses lucene query syntax 

1. 입력  2. 클릭 

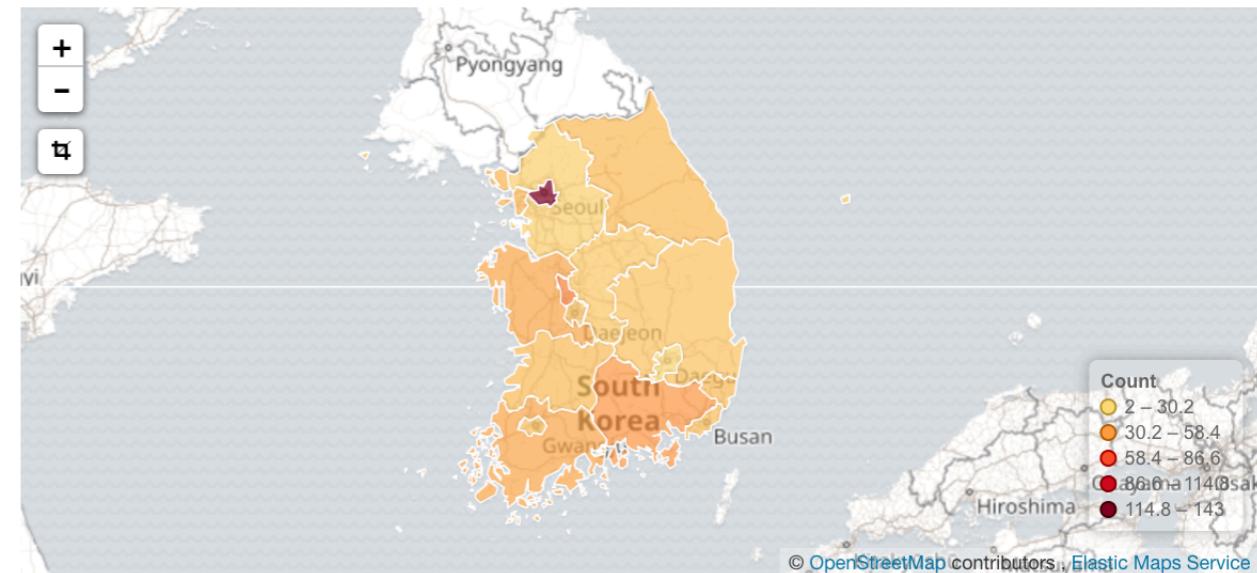
Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

• 강의자료
• 강의질문
• Markdown문법

473 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map



Count

- 2 – 30.2
- 30.2 – 58.4
- 58.4 – 86.6
- 86.6 – 114.8
- 114.8 – 143

© OpenStreetMap contributors, Elastic Maps Service

쿠팡 티몬 11번가 GS샵 옵션 g마켓 위메프

“시간 내에 배송 못함”이 위의 검색에 match된다

Search Type - Numeric

Dashboard / shopping

상품가격:>5000

Full screen Share Clone Edit ▶ 5 seconds < ⏴ This year >

Uses lucene query syntax 

Add a filter +

[shopping] markdown

[shopping] metrics

1. 입력  2. 클릭 

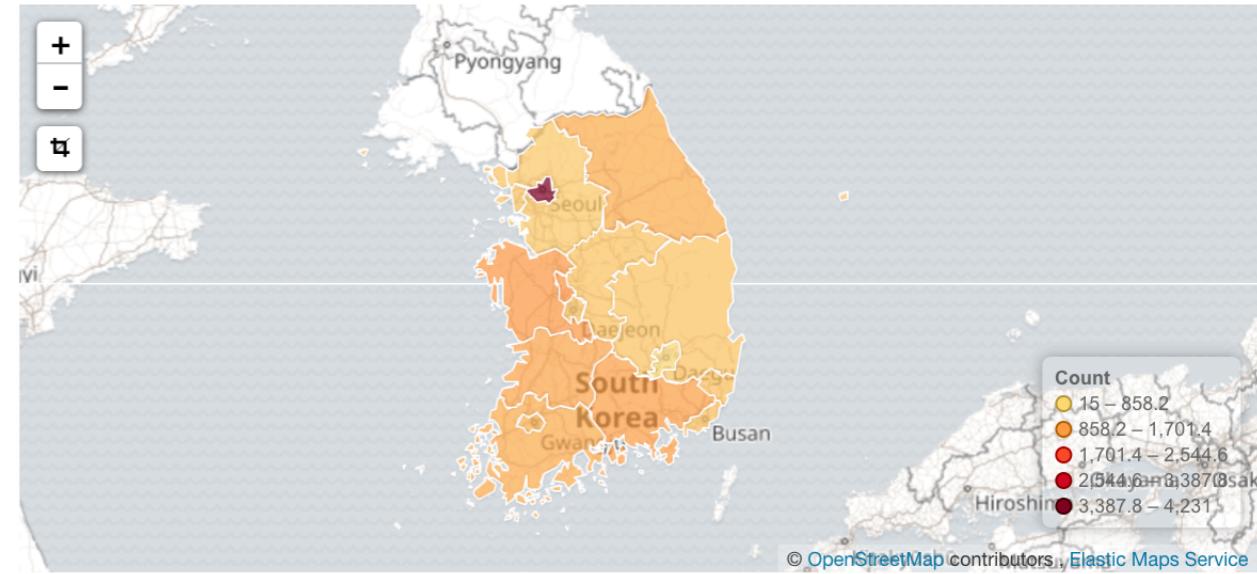
Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

14,339 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map



GS샵
위메프 11번가 티몬
11번가 옥션
g마켓 쿠팡

Search Type - Range

Dashboard / shopping

고객나이: [10 TO 30]

Full screen Share Clone Edit ▶ 5 seconds < ⏴ This year >

Uses lucene query syntax



Add a filter +

[shopping] markdown

1. 입력 

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

4,376
전체 데이터

[shopping] Tag Cloud

[shopping] Region Map

11번가
위메프 g마켓 GS샵 티몬
쿠팡 옥션



Search Type - Wildcard

Dashboard / shopping

Full screen Share Clone Edit ▶ 5 seconds < ⏴ This year >

고객주소_시도: 전라?도

Uses lucene query syntax: 

Add a filter +

[shopping] markdown

[shopping] metrics

1. 입력  2. 클릭 

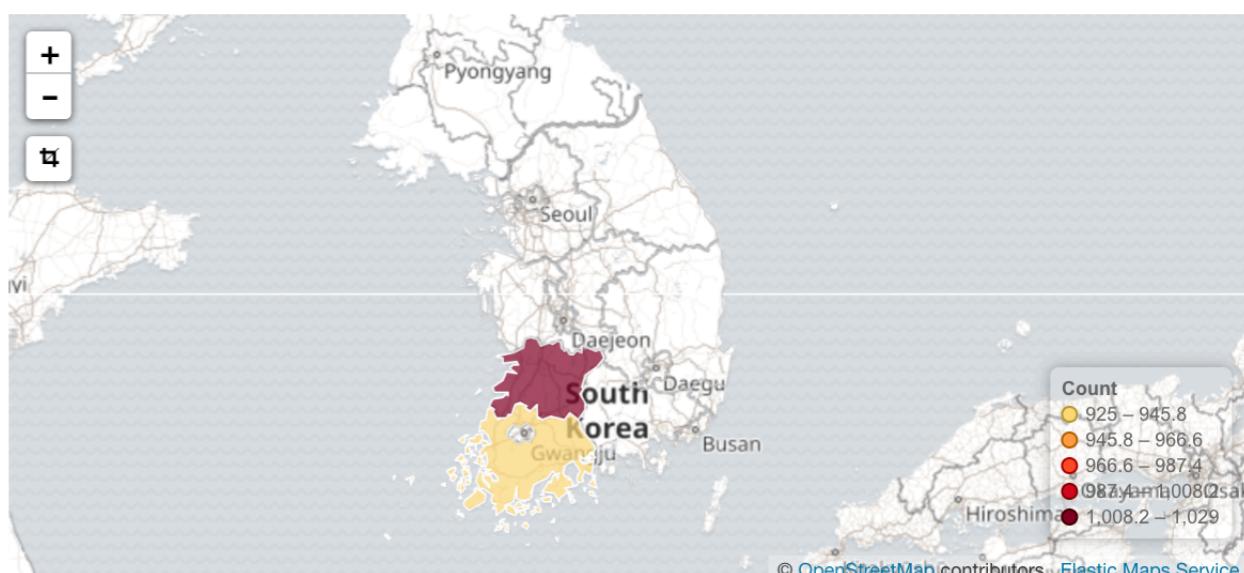
Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

• 강의자료
• 강의질문
• Markdown문법

1,954 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map



쿠팡 옥션 11번가 g마켓 GS샵 위메프 티몬

“전라남도” 와 “전라북도”가 위의 검색에 match된다

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 +

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

1. 입력 

2. 클릭 

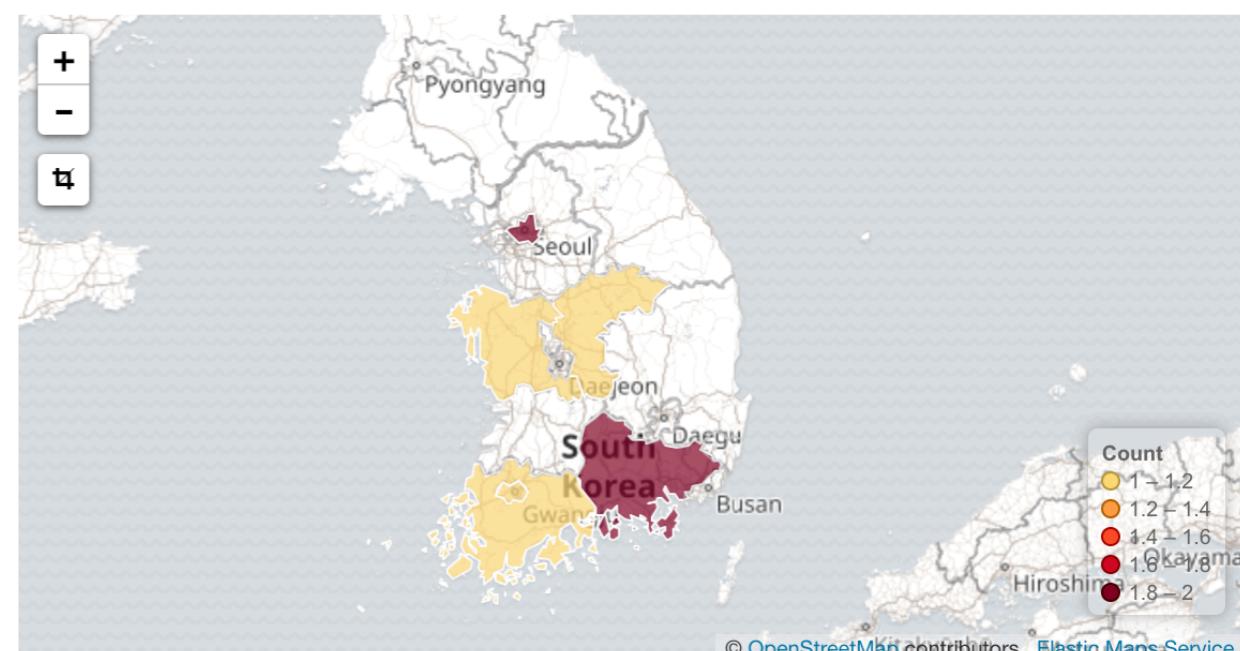
[shopping] metrics

8
전체 데이터

[shopping] Tag Cloud

g마켓
옵션 쿠팡 티몬

[shopping] Region Map



“상품_분류” Field의 값이 셔츠인 Documents가 match된다

Search Type - OR

Dashboard / shopping

Full screen Share Clone Edit ▶ 5 seconds < ⏴ This year >

고객성별: 여성 OR 상품분류: 셔츠 Uses lucene query syntax 

Add a filter +

[shopping] markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

• 강의자료
• 강의질문
• Markdown문법

 1. 입력  2. 클릭

8,904 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 to dark red to represent different count ranges. Labels on the map include Pyongyang, Seoul, Daegu, Busan, Gwangju, Daejeon, and Hiroshima. A legend titled 'Count' is located in the bottom right corner, showing five categories: 9 – 540.8 (light yellow), 540.8 – 1,072.6 (orange), 1,072.6 – 1,604.4 (red), 1,604.4 – 2,136.2 (dark red), and 2,136.2 – 2,668 (black). The map also includes a zoom control with '+' and '-' buttons and a location pin icon.

쿠팡 GS샵 11번가 옥션 위메프 티몬
g마켓

Search Type - AND

Dashboard / shopping

고객성별: 여성 AND 상품분류: 셔츠

Full screen Share Clone Edit ▶ 5 seconds < ⏴ This year >

Uses lucene query syntax



Add a filter +

[shopping] markdown

1. 입력


Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

657

전체 데이터

[shopping] Tag Cloud

GS샵
쿠팡 g마켓 옥션
11번가 위메프
티몬

[shopping] metrics

2. 클릭


[shopping] Region Map



Search Type - NOT

Dashboard / shopping

Full screen Share Clone Edit ▶ 5 seconds ⏪ ⏩ This year >

NOT 구매사이트:옵션

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

13,503 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map



위메프 11번가 GS샵 티몬 g마켓 쿠팡

Search Type +

Dashboard / shopping

+예약여부:예약

Full screen Share Clone Edit ▶ 5 seconds < ⏴ This year >

Uses lucene query syntax 

Add a filter +

[shopping] markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

• 강의자료
• 강의질문
• Markdown문법

1. 입력  2. 클릭 

1,545 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map

11번가
티몬 GS샵 **g마켓** 위메프
쿠팡 옥션



Count
1 – 100.8
100.8 – 200.6
200.6 – 300.4
300.4 – 400.2
400.2 – 500

© OpenStreetMap contributors, Elastic Maps Service

Search Type -

Dashboard / shopping

-구매사이트:11번가

Full screen Share Clone Edit ▶ 5 seconds < ⏴ This year >

Add a filter +

[shopping] markdown [shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

• 강의자료
• 강의질문
• Markdown문법

10,464
전체 데이터

[shopping] Tag Cloud [shopping] Region Map

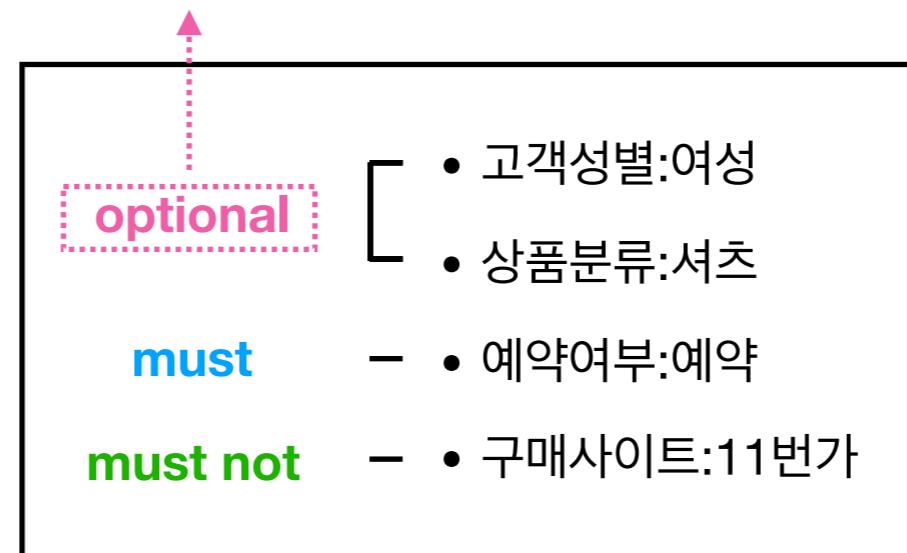
g마켓 티몬
옵션 GS샵 쿠팡 위메프

잠깐4

심화

AND, OR, NOT으로도 충분해 보이는데 +, - 은 왜 필요할까? 

필수는 아니지만 만족하는 Doc의 score ↑



- 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 / shopping

여성 셔츠 +예약 -11번가

Add a filter +

[shopping] markdown [shopping] metrics

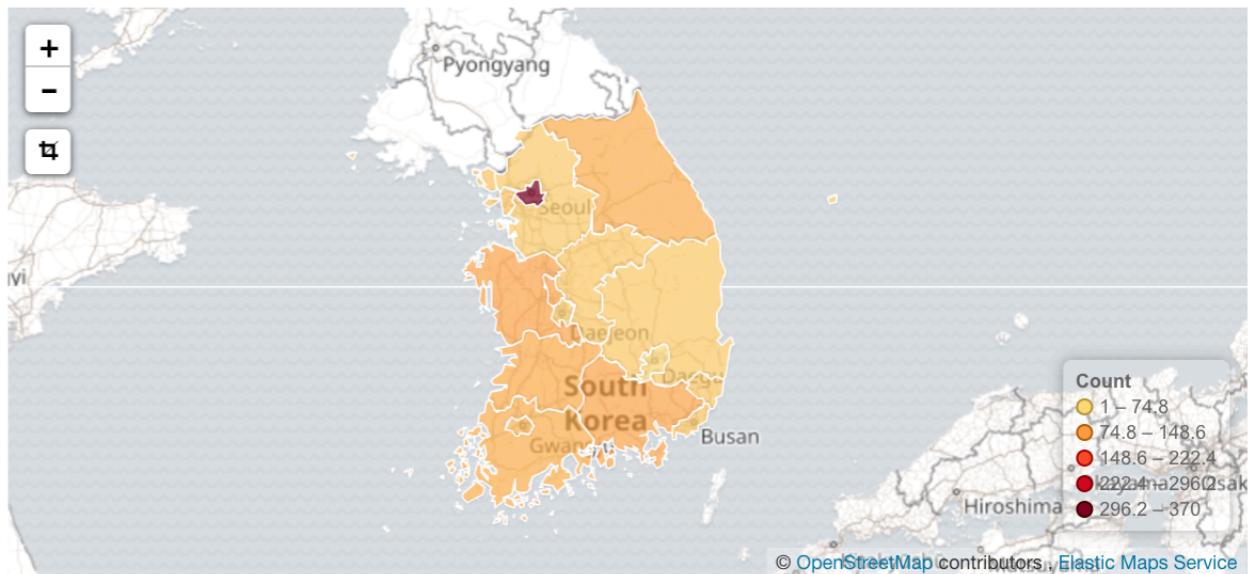
Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

1,091 전체 데이터

[shopping] Tag Cloud

[shopping] Region Map



티몬 GS샵 g마켓 위메프
쿠팡 옥션

예제 5 - 아래와 같은 Query를 Dashboard에서 검색해보자

Dashboard : nginx-*

Time Range : 2018년 6월 1일 ~ 2018년 8월 26일

문제	종류
nginx.access.response_code가 200인 Doc 필터링	Field Match
nginx.access.method가 GET 또는 POST인 Doc 필터링	Term
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	AND 연산
nginx.access.geoip.city_name이 Seoul이거나 nginx.access.user_agent.name이 Chrome인 Doc 필터링	OR 연산
요일_local이 SUNDAY인 Doc 필터링	?
nginx.access.geoip.country_name 가 “Republic of”로 시작하는 Doc 필터링	Wildcard
nginx.access.geoip.continent_code가 “AS”와 유사한 Doc 필터링	Fuzzy

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 시각화 하기 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	<ul style="list-style-type: none">특정 Document를 Table/JSON 형태 조회Histogram 특정 구간 내의 데이터 조회Histogram Bin 간격 설정Histogram 데이터를 csv 출력특정 Field의 정보만 조회특정 Field 값을 기준으로 정렬
데이터 통계	<ul style="list-style-type: none">(선택한 Time Range 내의) Documents 개수 확인특정 Field Value의 분포 확인 (주로 Categorical Data, 상위 500개)특정 Field에 non-null Value가 아닌 Documents 수 확인

Discover에서 Filter를 적용해보자

33,800 hits

New Save Open Share ► 5 seconds ◀ ⓘ June 1st 2018, 00:00:00.000 to August 26th 2018, 23:59:59.999

Uses lucene query syntax

Filter 적용

Seoul

Add a Filter

nginx-*

Selected Fields

? _source

Available Fields

Popular

- # nginx.access.body_sent.bytes
- t nginx.access.geoip.city_name
- t nginx.access.geoip.country_na...
- nginx.access.geoip.location
- t nginx.access.user_agent.name
- t nginx.access.user_agent.os_n...
- t nginx.access.user_agent.patch
- t nginx.access.user_name

@timestamp

t _id

t _index

_score

t _type

t nginx.access.geoip.continent ...

t nginx.access.geoip.country_co...

t nginx.access.geoip.country_co...

nginx.access.geoip.ip

t nginx.access.geoip.region_code

June 1st 2018, 00:00:00.000 - August 26th 2018, 23:59:59.999 — Auto

Count

4,000

3,000

2,000

1,000

0

2018-06-03 2018-06-10 2018-06-17 2018-06-24 2018-07-01 2018-07-08 2018-07-15 2018-07-22 2018-07-29 2018-08-05 2018-08-12 2018-08-19

@timestamp per day

Time

_source

▶ June 19th 2018, 09:04:35.000

```
nginx.access.geoip.city_name: Seoul nginx.access.remote_ip: 175.223.23.111 nginx.access.body_sent.bytes: 0 nginx.access.user_name: - nginx.access.referrer: http://kibana.higee.co/app/kibana nginx.access.user_agent.os_minor: 4 nginx.access.user_agent.name: Chrome Mobile iOS nginx.access.user_agent.patch: 3396 nginx.access.user_agent.os_name: iOS nginx.access.user_agent.build: nginx.access.user_agent.major: 67 nginx.access.user_agent.os_major: 11 nginx.access.user_agent.os: iOS nginx.access.user_agent.device: iPhone nginx.access.user_agent.minor: 0 nginx.access.method: GET nginx.access.http_version: 1.1
```

▶ June 19th 2018, 09:04:47.000

```
nginx.access.geoip.city_name: Seoul nginx.access.remote_ip: 175.223.23.111 nginx.access.body_sent.bytes: 152 nginx.access.user_name: - nginx.access.referrer: http://kibana.higee.co/app/kibana nginx.access.user_agent.os_minor: 4 nginx.access.user_agent.name: Chrome Mobile iOS nginx.access.user_agent.patch: 3396 nginx.access.user_agent.os_name: iOS nginx.access.user_agent.build: nginx.access.user_agent.major: 67 nginx.access.user_agent.os_major: 11 nginx.access.user_agent.os: iOS nginx.access.user_agent.device: iPhone nginx.access.user_agent.minor: 0 nginx.access.method: POST nginx.access.http_version: 1.1
```

▶ June 19th 2018, 09:04:47.000

```
nginx.access.geoip.city_name: Seoul nginx.access.remote_ip: 175.223.23.111 nginx.access.body_sent.bytes: 151 nginx.access.user_name: - nginx.access.referrer: http://kibana.higee.co/app/kibana nginx.access.user_agent.os_minor: 4 nginx.access.user_agent.name: Chrome Mobile iOS nginx.access.user_agent.patch: 3396 nginx.access.user_agent.os_name: iOS nginx.access.user_agent.build: nginx.access.user_agent.major: 67 nginx.access.user_agent.os_major: 11 nginx.access.user_agent.os: iOS nginx.access.user_agent.device: iPhone nginx.access.user_agent.minor: 0 nginx.access.method: POST nginx.access.http_version: 1.1
```

▶ June 19th 2018, 09:09:07.000

```
nginx.access.geoip.city_name: Seoul nginx.access.remote_ip: 175.223.23.111 nginx.access.body_sent.bytes: 0 nginx.access.user_name: - nginx.access.referrer: http://kibana.higee.co/app/kibana nginx.access.user_agent.os_minor: 4 nginx.access.user_agent.name: Chrome Mobile iOS nginx.access.user_agent.patch: 3396 nginx.access.user_agent.os_name: iOS nginx.access.user_agent.build:
```

Discover에서 Search를 해보자

33,800 hits

nginx.access.geoip.city_name: Seoul

New Save Open Share ▶ 5 seconds ⏪ ⏩ June 1st 2018, 00:00:00.000 to August 26th 2018, 23:59:59.999

Add a filter +

Selected Fields

? _source

Available Fields

Popular

- # nginx.access.body_sent.bytes
- t nginx.access.geoip.city_name
- t nginx.access.geoip.country_na...
- nginx.access.geoip.location
- t nginx.access.user_agent.name
- t nginx.access.user_agent.os_n...
- t nginx.access.user_agent.patch
- t nginx.access.user_name

@timestamp

- t _id
- t _index
- # _score
- t _type
- t nginx.access.geoip.continent ...
- t nginx.access.geoip.country_co...
- t nginx.access.geoip.country_co...
- nginx.access.geoip.ip
- t nginx.access.geoip.region_code
- * nginx.access.geoip.region_na...

June 1st 2018, 00:00:00.000 - August 26th 2018, 23:59:59.999 — Auto

Count

June 1st 2018, 00:00:00.000 - August 26th 2018, 23:59:59.999 — Auto

2018-06-03 2018-06-10 2018-06-17 2018-06-24 2018-07-01 2018-07-08 2018-07-15 2018-07-22 2018-07-29 2018-08-05 2018-08-12 2018-08-19

@timestamp per day

Time _source

▶ June 19th 2018, 09:04:35.000 nginx.access.geoip.city_name: Seoul nginx.access.remote_ip: 175.223.23.111 nginx.access.body_sent.bytes: 0 nginx.access.user_name: - nginx.access.referrer: http://kibana.higee.co/app/kibana nginx.access.user_agent.os_minor: 4 nginx.access.user_agent.name: Chrome Mobile iOS nginx.access.user_agent.patch: 3396 nginx.access.user_agent.os_name: iOS nginx.access.user_agent.build: nginx.access.user_agent.major: 67 nginx.access.user_agent.os_major: 11 nginx.access.user_agent.os: iOS nginx.access.user_agent.device: iPhone nginx.access.user_agent.minor: 0 nginx.access.method: GET nginx.access.http_version: 1.1

▶ June 19th 2018, 09:04:47.000 nginx.access.geoip.city_name: Seoul nginx.access.remote_ip: 175.223.23.111 nginx.access.body_sent.bytes: 152 nginx.access.user_name: - nginx.access.referrer: http://kibana.higee.co/app/kibana nginx.access.user_agent.os_minor: 4 nginx.access.user_agent.name: Chrome Mobile iOS nginx.access.user_agent.patch: 3396 nginx.access.user_agent.os_name: iOS nginx.access.user_agent.build: nginx.access.user_agent.major: 67 nginx.access.user_agent.os_major: 11 nginx.access.user_agent.os: iOS nginx.access.user_agent.device: iPhone nginx.access.user_agent.minor: 0 nginx.access.method: POST nginx.access.http_version: 1.1

▶ June 19th 2018, 09:04:47.000 nginx.access.geoip.city_name: Seoul nginx.access.remote_ip: 175.223.23.111 nginx.access.body_sent.bytes: 151 nginx.access.user_name: - nginx.access.referrer: http://kibana.higee.co/app/kibana nginx.access.user_agent.os_minor: 4 nginx.access.user_agent.name: Chrome Mobile iOS nginx.access.user_agent.patch: 3396 nginx.access.user_agent.os_name: iOS nginx.access.user_agent.build: nginx.access.user_agent.major: 67 nginx.access.user_agent.os_major: 11 nginx.access.user_agent.os: iOS nginx.access.user_agent.device: iPhone nginx.access.user_agent.minor: 0 nginx.access.method: POST nginx.access.http_version: 1.1

▶ June 19th 2018, 09:09:07.000 nginx.access.geoip.city_name: Seoul nginx.access.remote_ip: 175.223.23.111 nginx.access.body_sent.bytes: 0 nginx.access.user_name: - nginx.access.referrer: http://kibana.higee.co/app/kibana nginx.access.user_agent.os_minor: 4 nginx.access.user_agent.name: Chrome Mobile iOS nginx.access.user_agent.patch: 3396 nginx.access.user_agent.os_name: iOS nginx.access.user_agent.build:

잠깐5, 이걸로 뭘 할 수 있을까?

: 특정한 조건을 만족하는 데이터만 선별해서 시각화 할 수 있다.

검색 결과 저장



2. 검색 결과 저장

New

Save

Open

Share

▶ 5 seconds

◀

⌚ June 1st 2018, 00:00:00.000 to August 26th 2018, 23:59:59.999

33,800 hits

Save Search

서울 접속 데이터

Save

nginx.access.geoip.city_name: Seoul

☞ 3. 검색 결과를 이름을 지정하여 저장

☞ 1. Lucene Query 작성 (혹은 필터 적용)

Uses lucene query syntax



Add a filter +

nginx-*

June 1st 2018, 00:00:00.000 - August 26th 2018, 23:59:59.999 — Auto

Selected Fields

? _source

Available Fields

Popular

nginx.access.body_sent.bytes

t nginx.access.geoip.city_name

t nginx.access.geoip.country_na...

nginx.access.geoip.location

t nginx.access.user_agent.name

t nginx.access.user_agent.os_n...

t nginx.access.user_agent.patch

t nginx.access.user_name

@timestamp

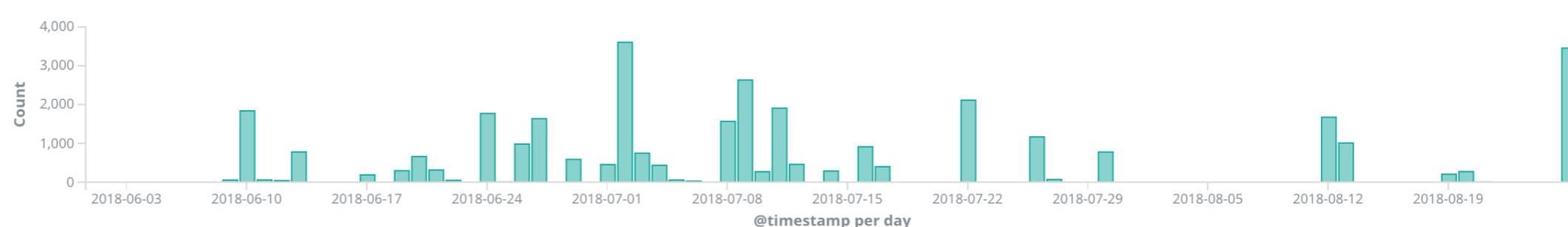
t _id

t _index

_score

t _type

t nginx.access.geoip.continent...



Time	_source
June 19th 2018, 09:04:35.000	nginx.access.geoip.city_name: Seoul nginx.access.remote_ip: 175.223.23.111 nginx.access.body_sent.bytes: 0 nginx.access.user_name: - nginx.access.referrer: http://kibana.higee.co/app/kibana nginx.access.user_agent.os_minor: 4 nginx.access.user_agent.name: Chrome Mobile iOS nginx.access.user_agent.patch: 3396 nginx.access.user_agent.os_name: iOS nginx.access.user_agent.build: nginx.access.user_agent.major: 67 nginx.access.user_agent.os_major: 11 nginx.access.user_agent.os: iOS nginx.access.user_agent.device: iPhone nginx.access.user_agent.minor: 0 nginx.access.method: GET nginx.access.http_version: 1.1
June 19th 2018, 09:04:47.000	nginx.access.geoip.city_name: Seoul nginx.access.remote_ip: 175.223.23.111 nginx.access.body_sent.bytes: 152 nginx.access.user_name: - nginx.access.referrer: http://kibana.higee.co/app/kibana nginx.access.user_agent.os_minor: 4 nginx.access.user_agent.name: Chrome Mobile iOS nginx.access.user_agent.patch: 3396 nginx.access.user_agent.os_name: iOS nginx.access.user_agent.build: nginx.access.user_agent.major: 67 nginx.access.user_agent.os_major: 11 nginx.access.user_agent.os: iOS nginx.access.user_agent.device: iPhone nginx.access.user_agent.minor: 0 nginx.access.method: POST nginx.access.http_version: 1.1
June 19th 2018, 09:04:47.000	nginx.access.geoip.city_name: Seoul nginx.access.remote_ip: 175.223.23.111 nginx.access.body_sent.bytes: 151 nginx.access.user_name: - nginx.access.referrer: http://kibana.higee.co/app/kibana nginx.access.user_agent.os_minor: 4 nginx.access.user_agent.name: Chrome Mobile iOS nginx.access.user_agent.patch: 3396 nginx.access.user_agent.os_name: iOS

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

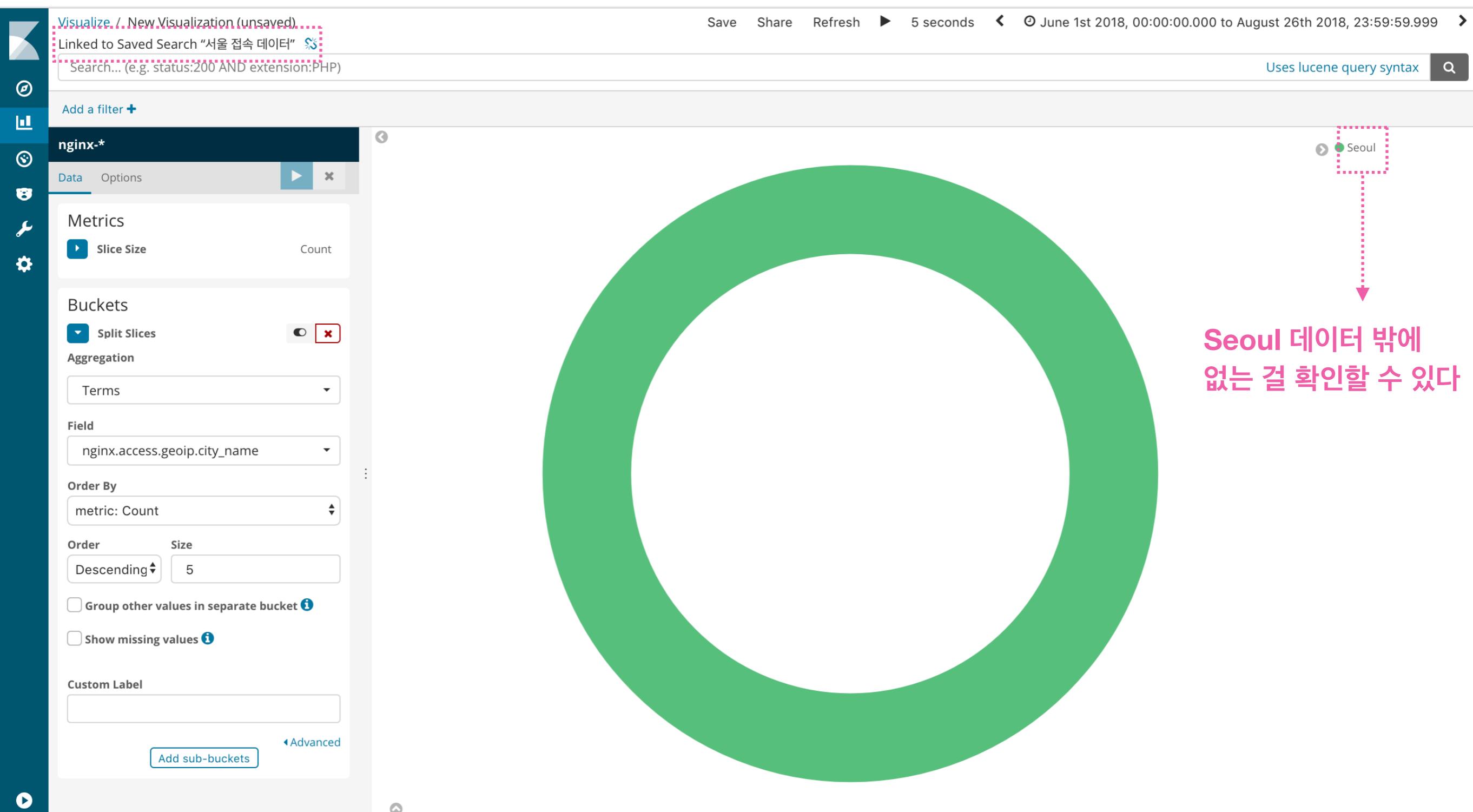
서울 접속 1-1 of 1 Manage saved searches

Name ▲

서울 접속 데이터

저장한 검색결과 선택

저장된 검색 결과를 이용한 시각화 3단계



예제 6.1 - 검색을 이용해서 아래 조건에 해당하는 데이터만 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

저장시 이름은 id-search 형식. 예시) higee-search

예제 6.2- 앞서 저장한 결과로 아래와 같은 시각화를 하자



조건

- "@timestamp" field 기준 “**2018-06-01 ~ 2018-08-26**” 동안
- 요일별 시간대별 접속자 수
 - 요일별 : 요일_local Field 사용 (요일_local_sort field 이용해 요일 정렬)
 - 시간대별 : 시간대_local Field를 사용하여 4시간 간격으로 집계

질문 및 Feedback은

gshock94@gmail.com로 주세요