Elastic Stack을 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?

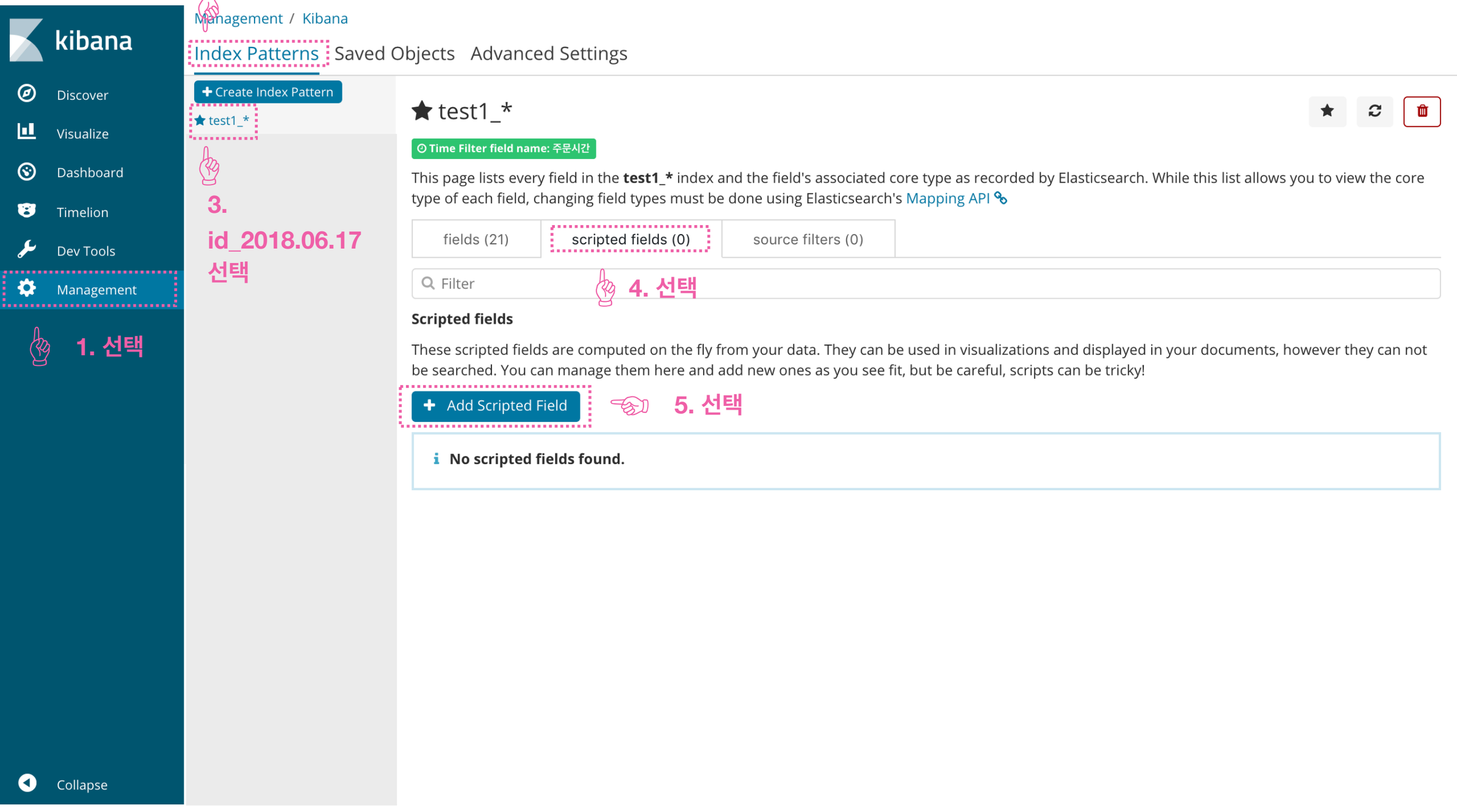
기존 Field에 조건을 적용해서 새로운 Field를 만들 수 없나?

예시

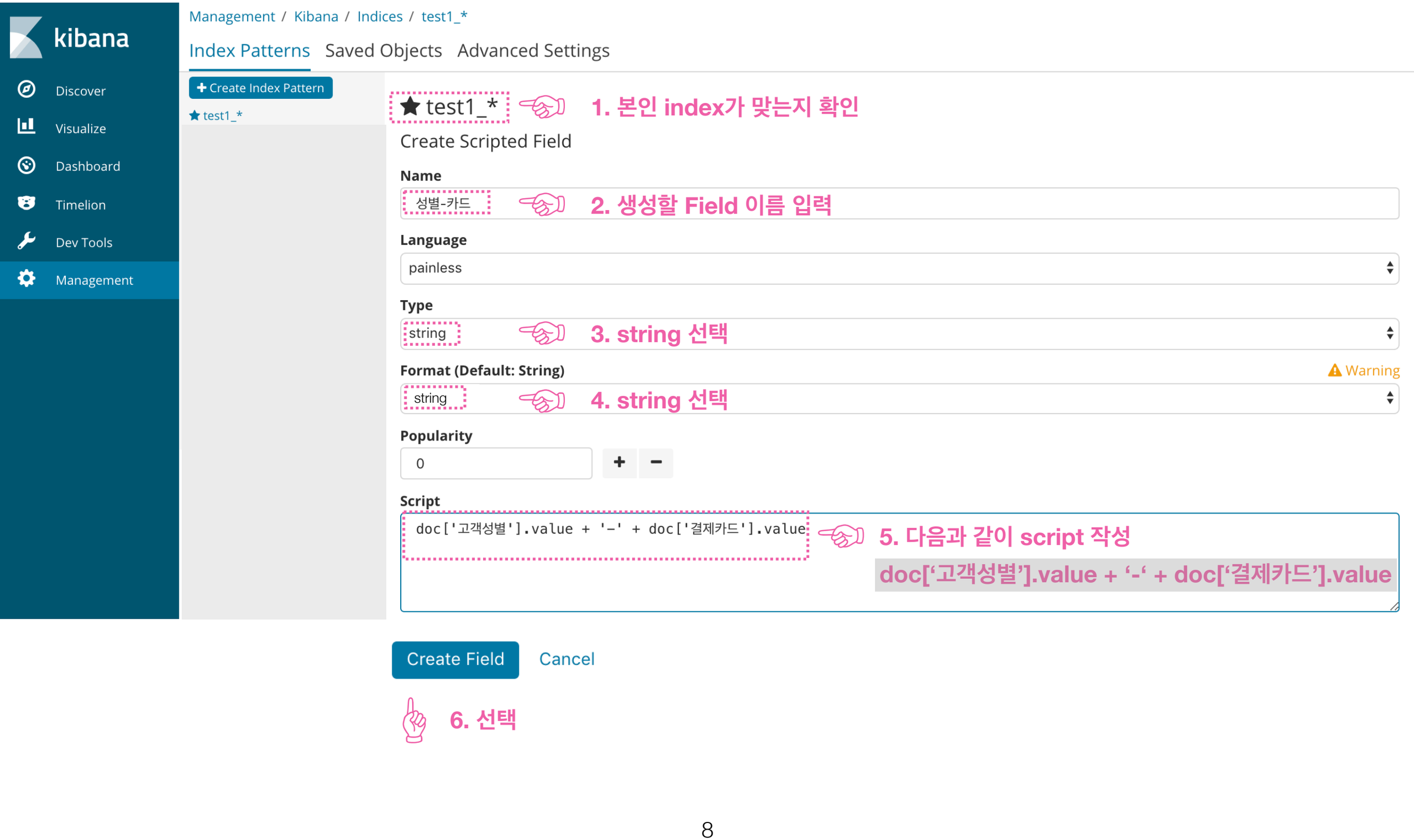
특정한 두 개 혹은 그 이상의 Field를 합쳐서

하나의 Field를 만들고 싶으면 어떻게 해야할까?

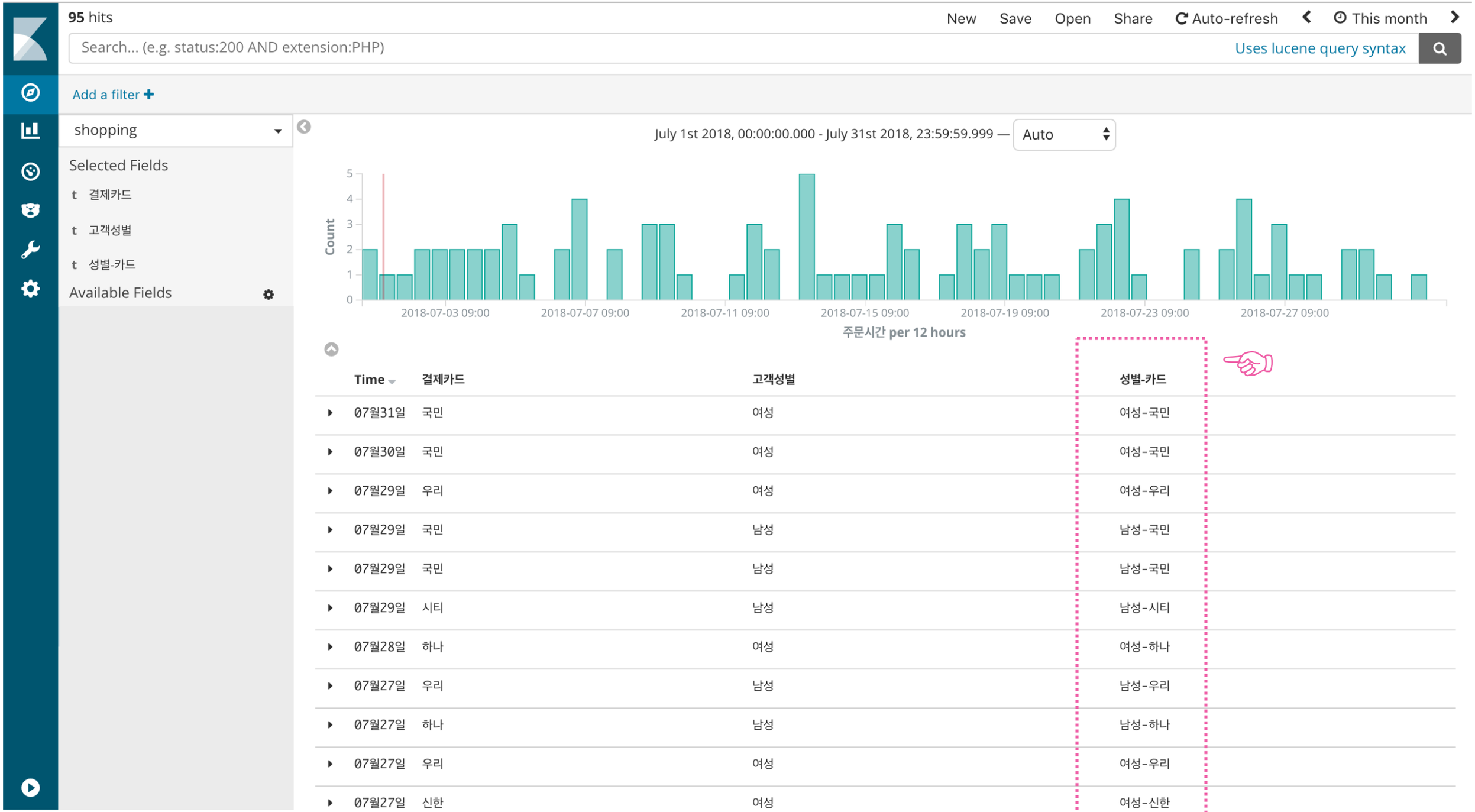
scripted field를 추가하자



script를 작성하자 ♕

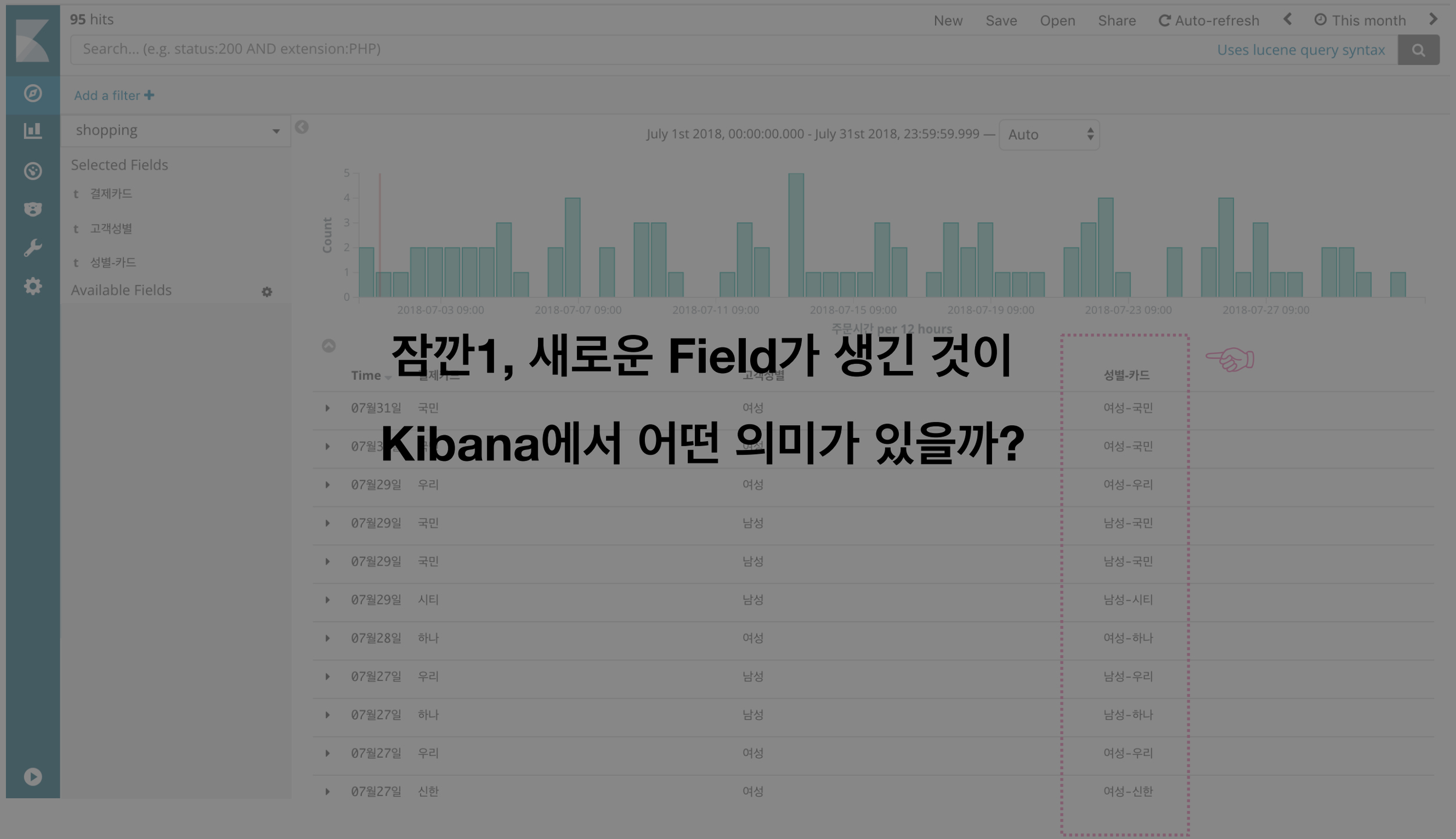


Discover에 가서 확인하자



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

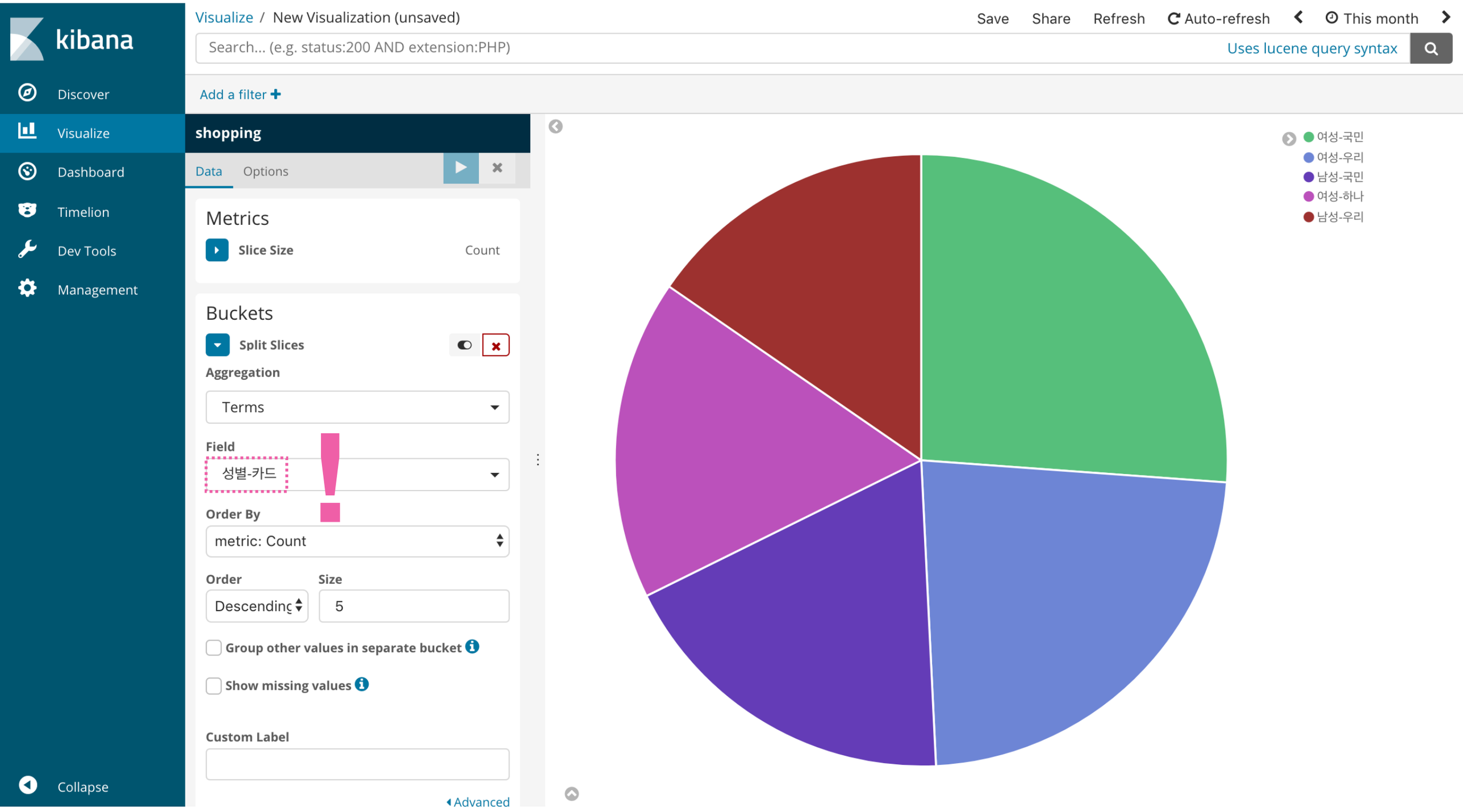
Discover에 가서 확인하자



잠깐1, 새로운 Field가 생긴 것이

Kibana에서 어떤 의미가 있을까?

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?

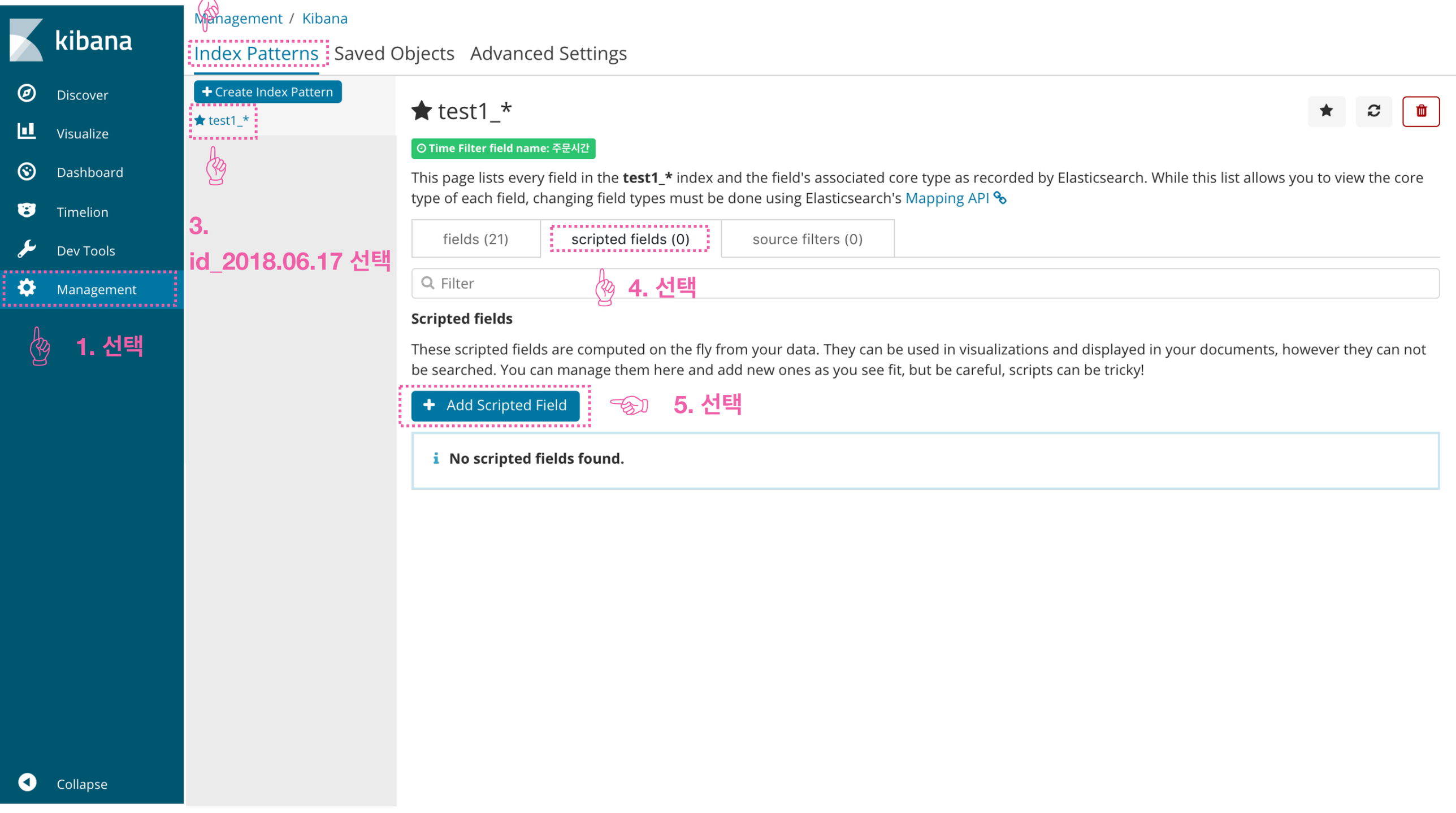
기존 Field에 조건을 적용해서 새로운 Field를 만들 수 없나?

예시

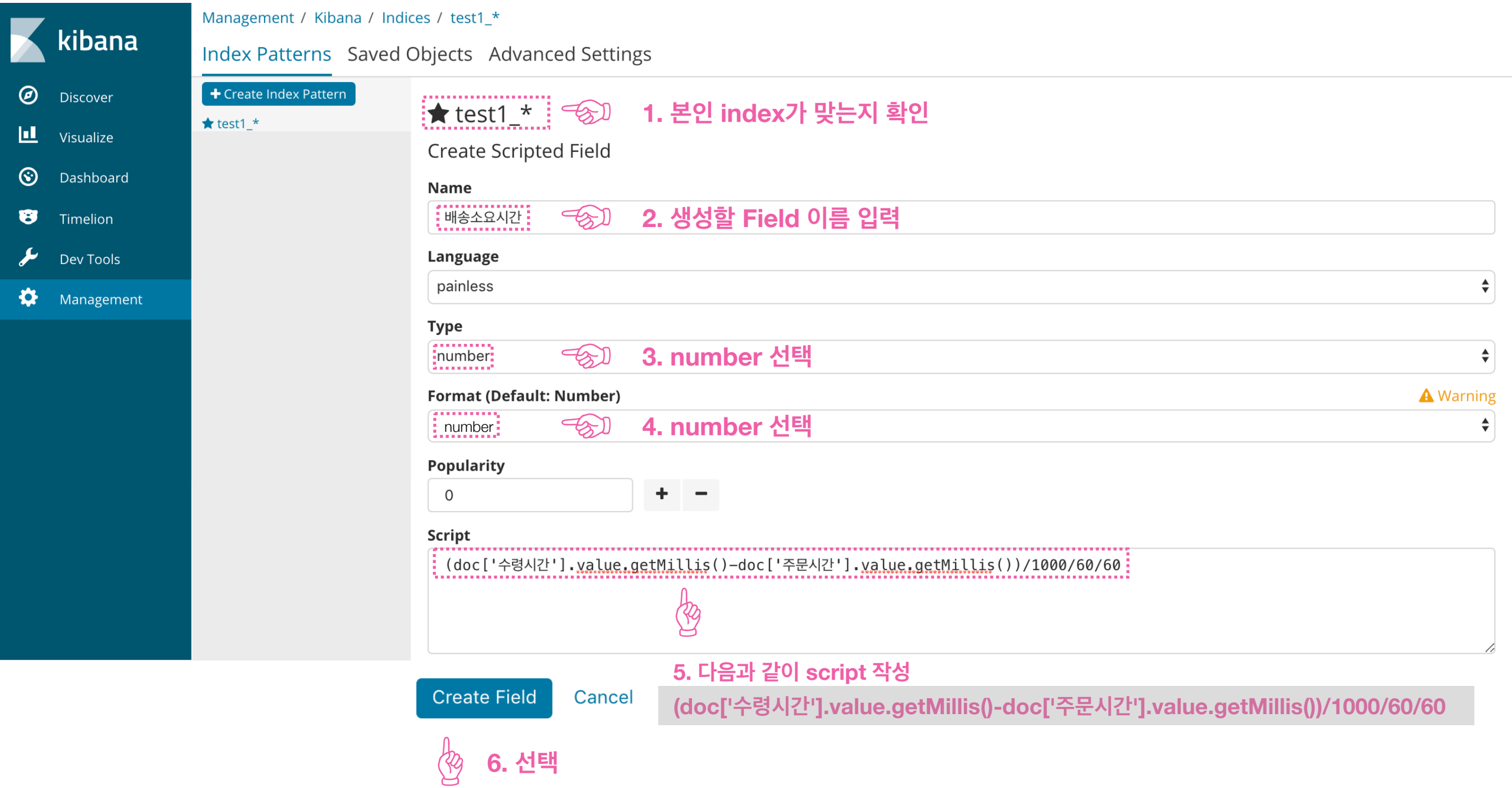
2개의 Date Field 값의 차이를 통해

특정한 event의 처리시간을 구하고 싶다면?

scripted field를 추가하자



script를 작성하자 👑



Discover에 가서 확인하자

kibana

95 hits

New Save Open Share Auto-refresh This month

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

Add a filter +

- Discover
- Visualize
- Dashboard
- Timelion
- Dev Tools
- Management

Collapse

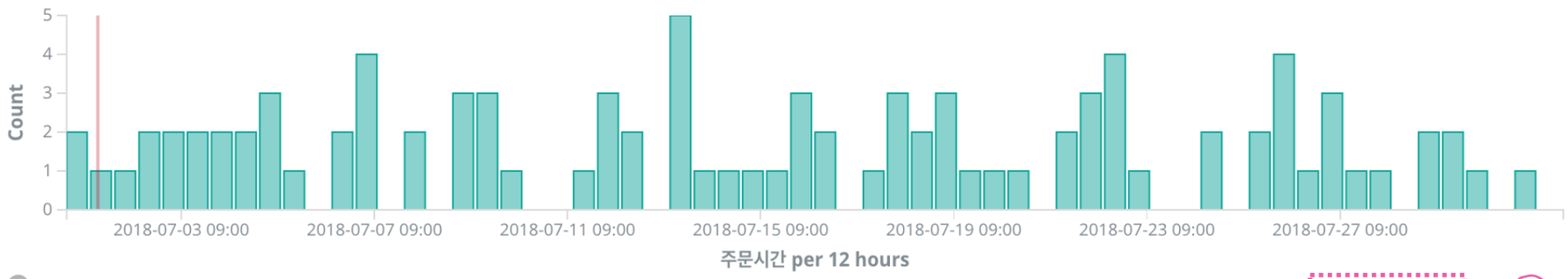
shopping

Selected Fields

- 수령시간
- 주문시간
- # 배송소요시간

Available Fields

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



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

예제 1 - Scripted Field 👑

kibana

95 hits

New Save Open Share Auto-refresh This month

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

Add a filter +

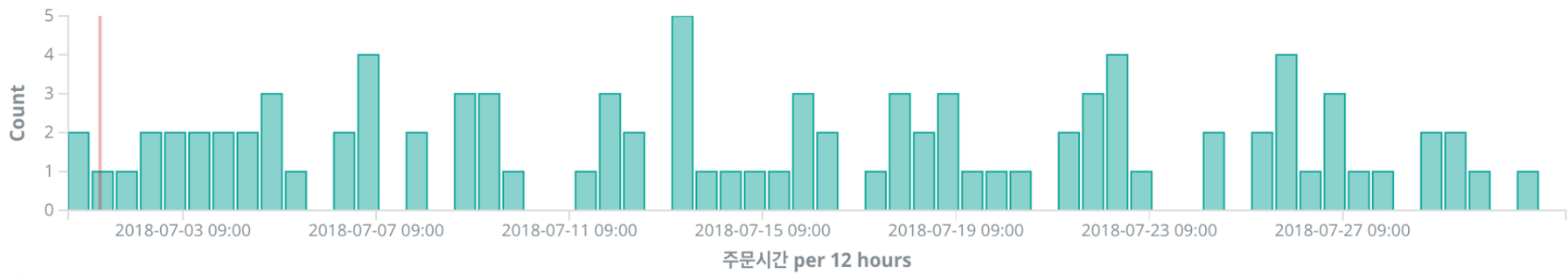
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management

shopping

Selected Fields
상품가격
상품개수
매출

Available Fields

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



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

Collapse

String Concatenation 연산은 안되나?

Field 간 연산은 안되나?

Date Field에서 연/월/일/시/분/초 등 접근 안되나? 

기존 Field에 조건을 적용해서 새로운 Field를 만들 수 없나?

예시

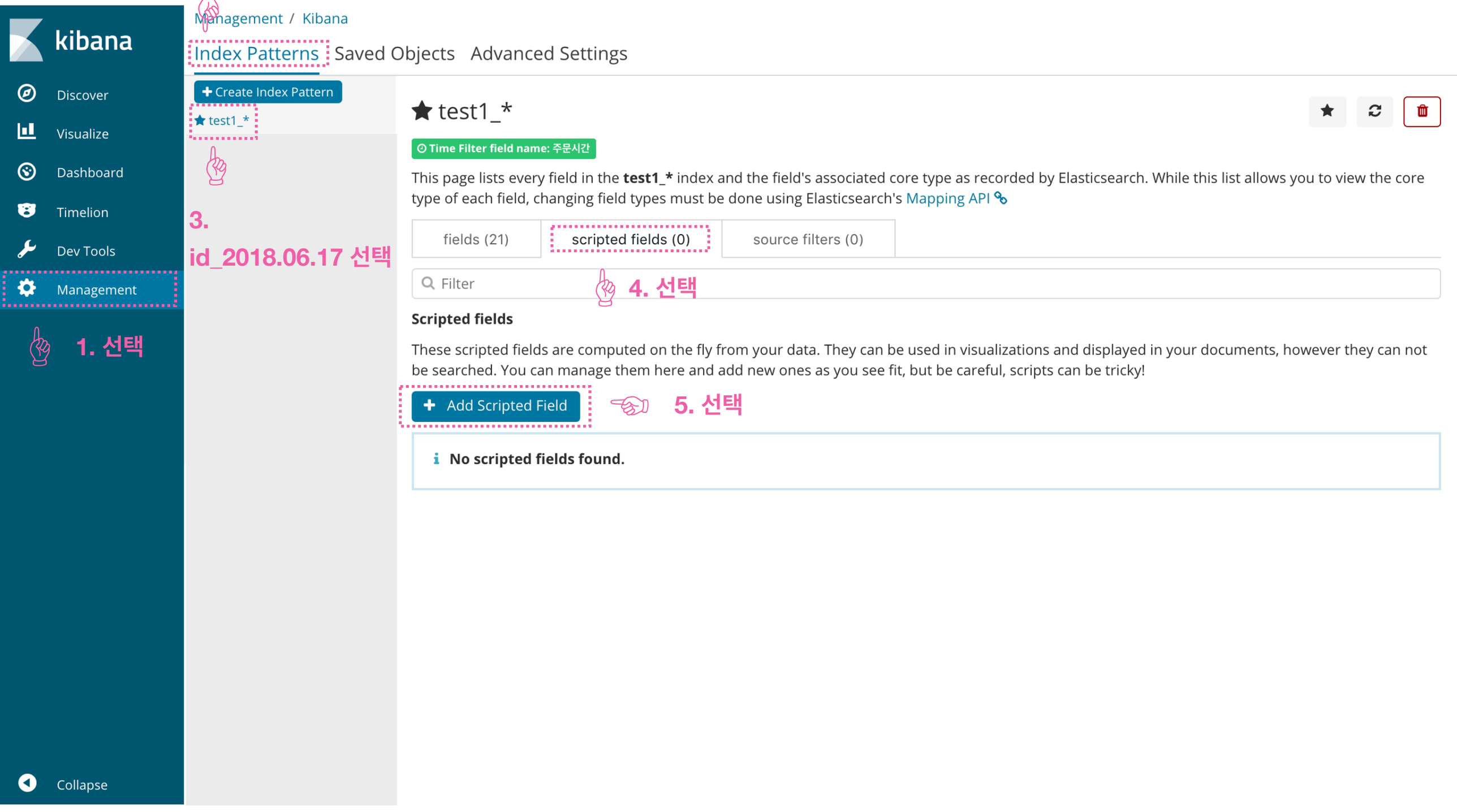
특정 Date Field에서 시간대 및 요일 등을 추출해서

요일 별 시간대 별 Heat Map을 시각화 하고 싶을 때 사용!

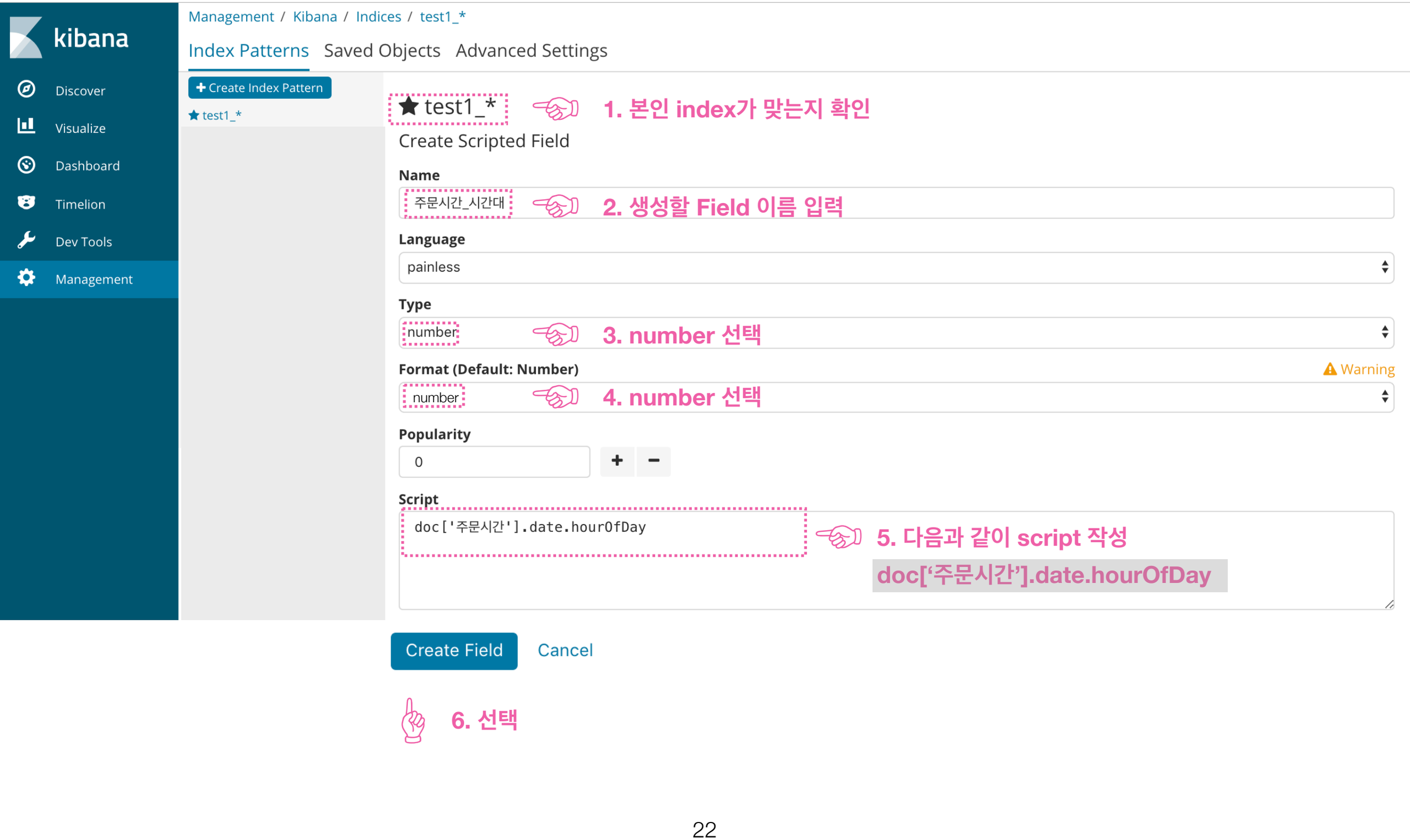
Lucene Expression을 이용하면 날짜 관련 정보를 쉽게 추출할 수 있다 👑

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

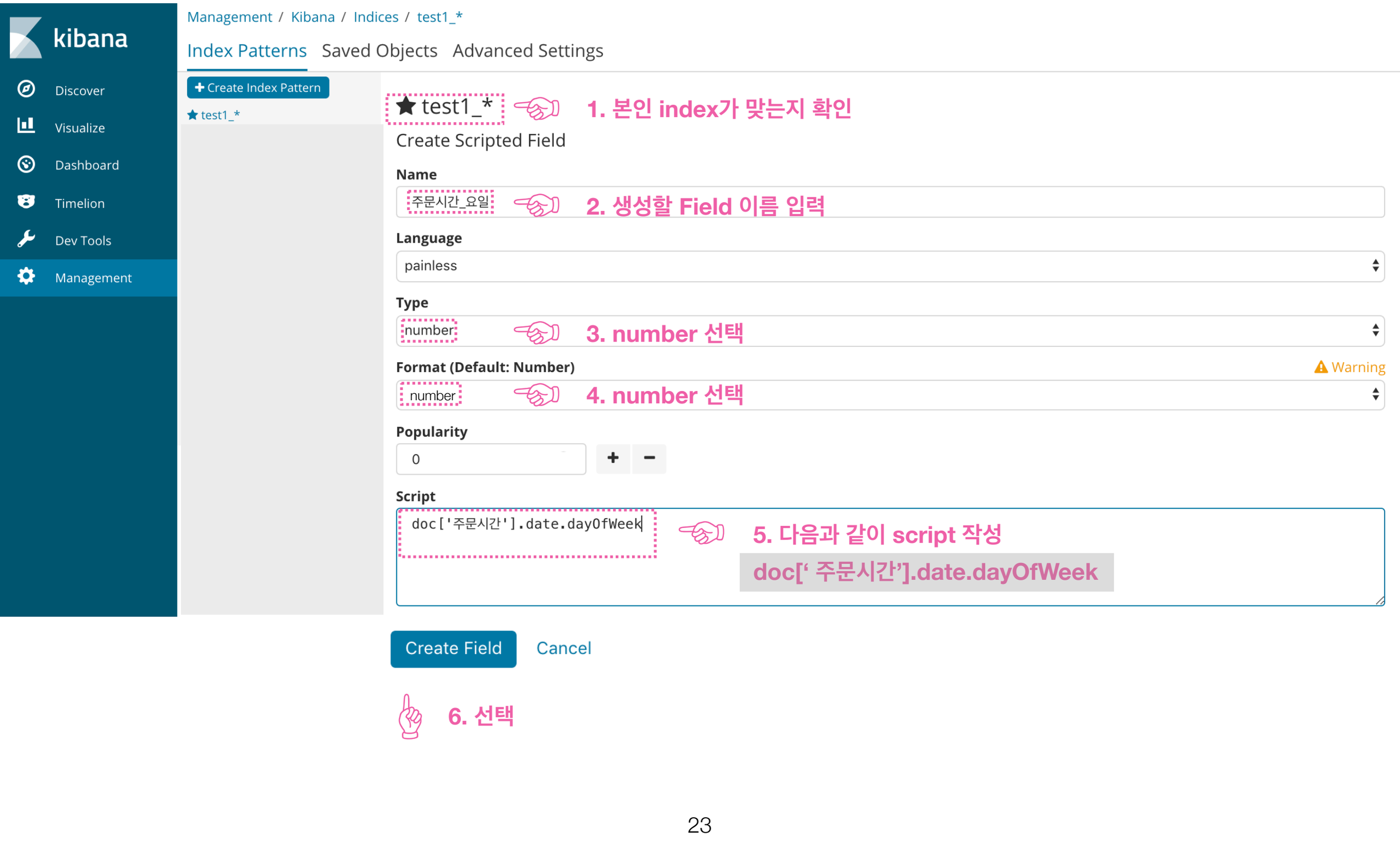
scripted field를 추가하자



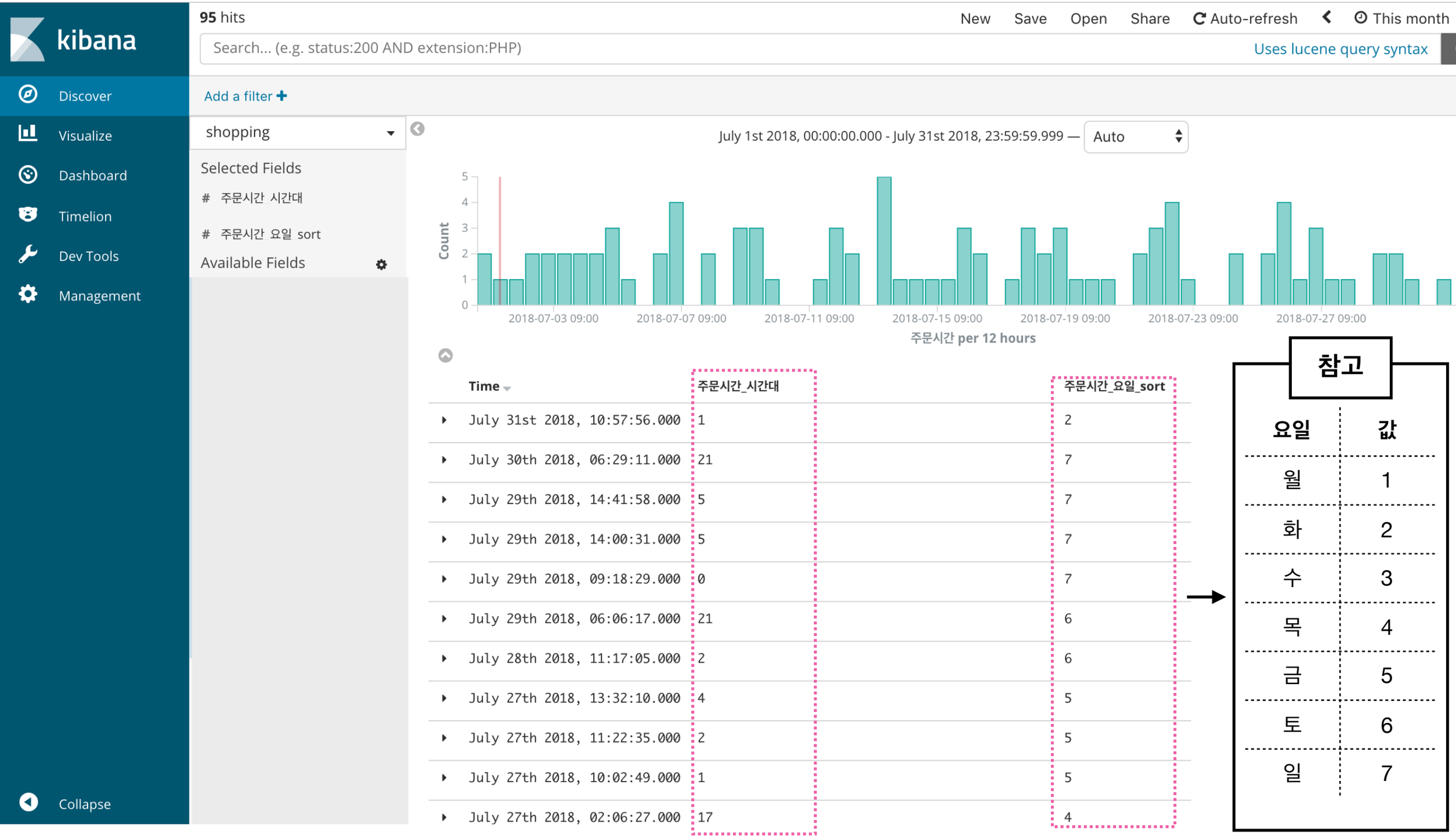
script를 작성하자 ♕



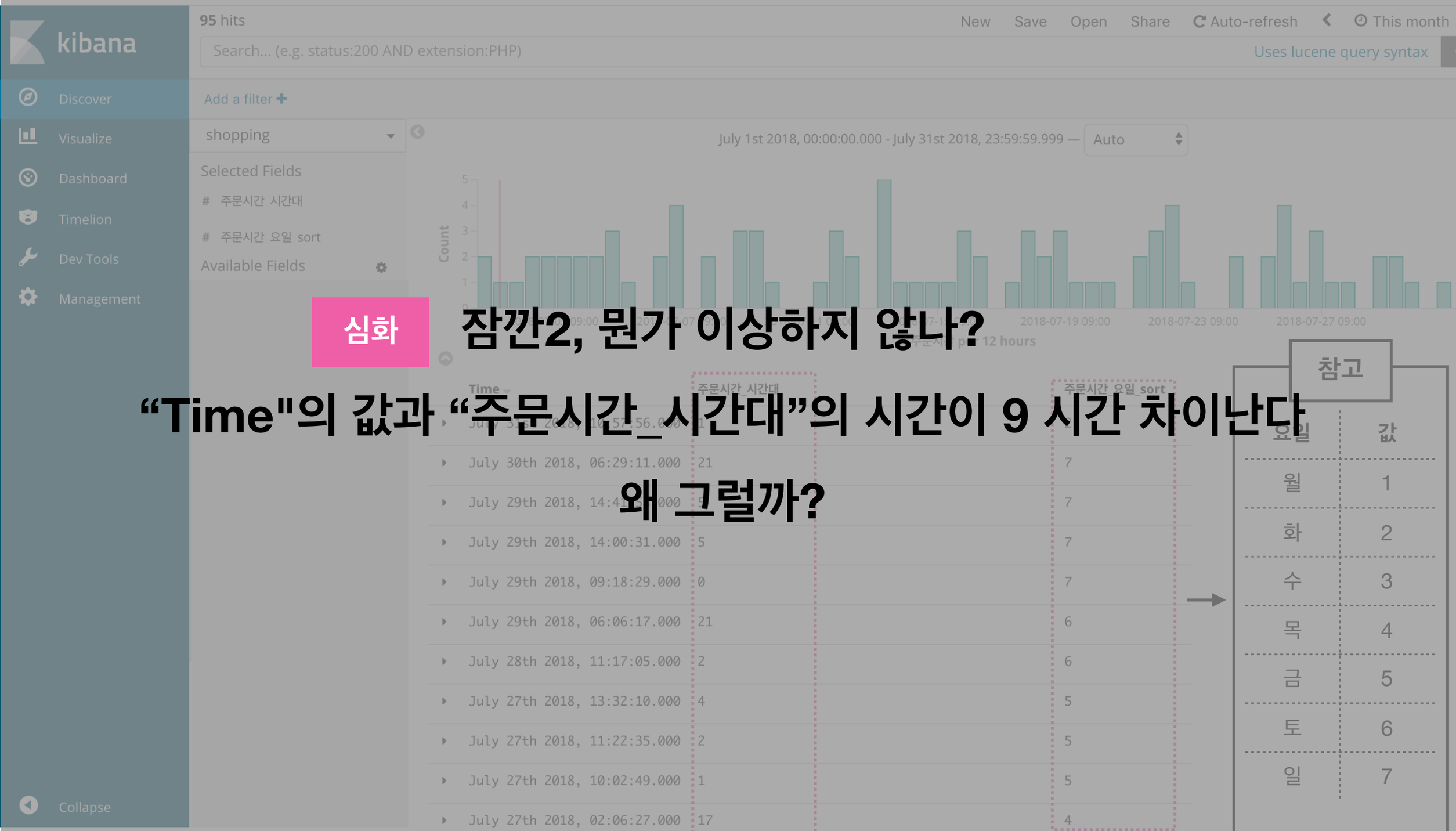
script를 작성하자 ♕



Discover에 가서 확인하자



Discover에 가서 확인하자



심화 **잠깐2, 뭔가 이상하지 않나?**

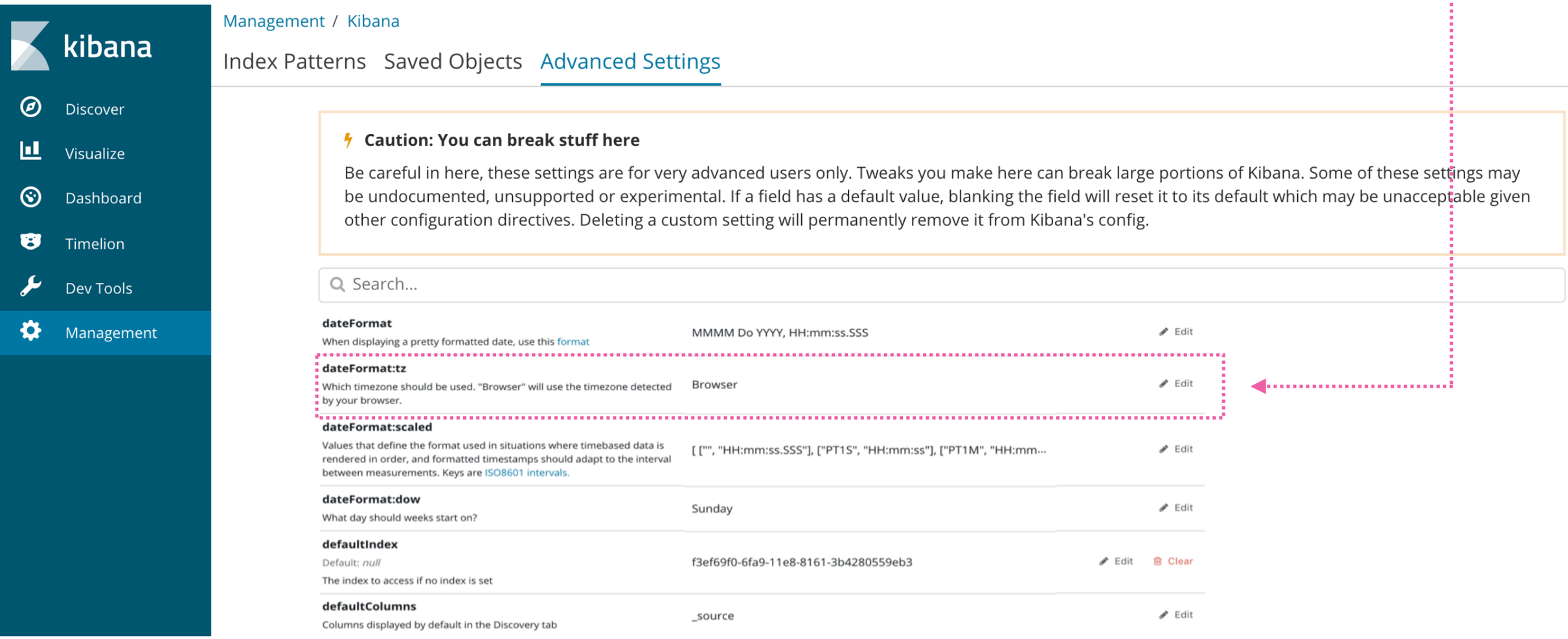
“Time"의 값과 “주문시간_시간대”의 시간이 9 시간 차이난다

왜 그럴까?

Elasticsearch timezone ≠ Kibana timezone 심화

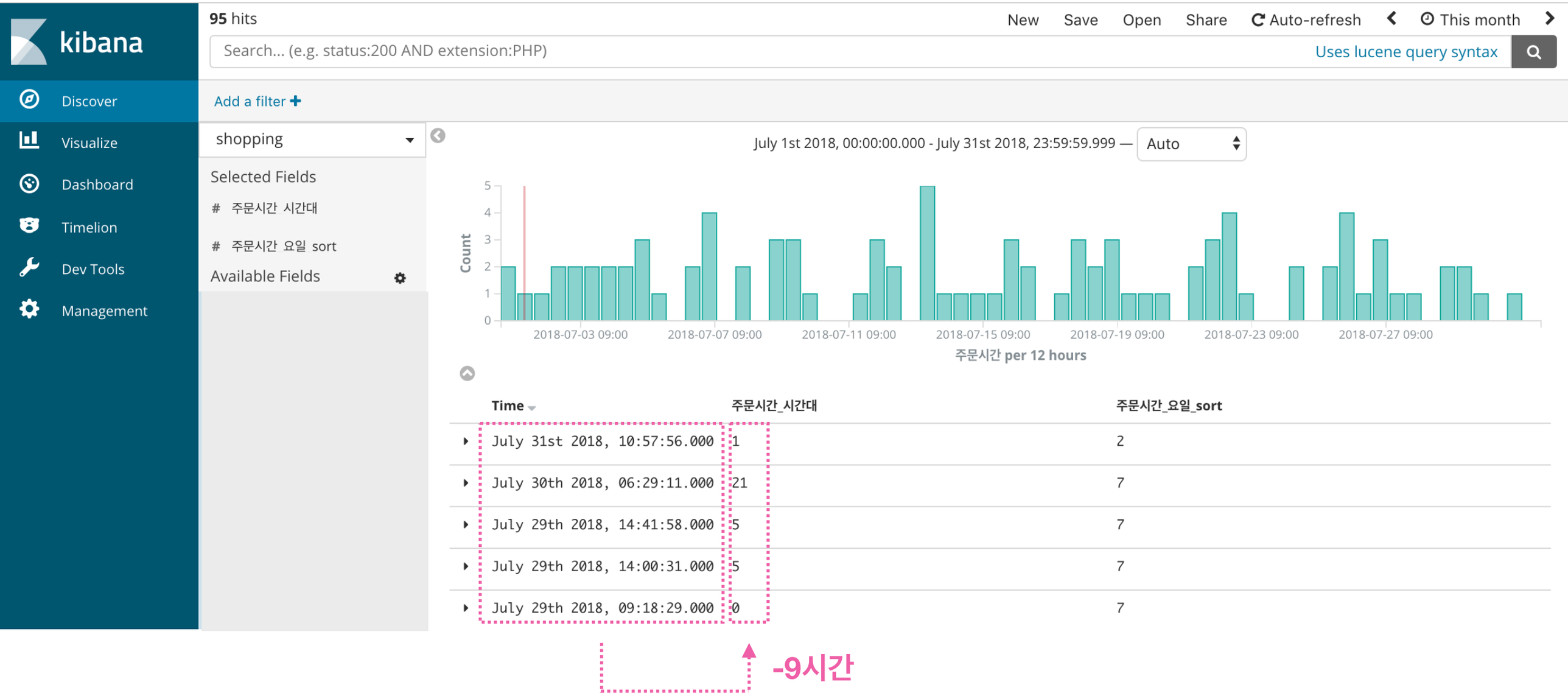
Elasticsearch : 기본적으로 입력된 date field를 **UTC**로 인식한다

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



Elasticsearch timezone ≠ Kibana timezone

심화



즉, Scripted Field로 추출한 시간대 및 요일은

~~Local 시간~~이 아닌 **UTC** 시간이기에

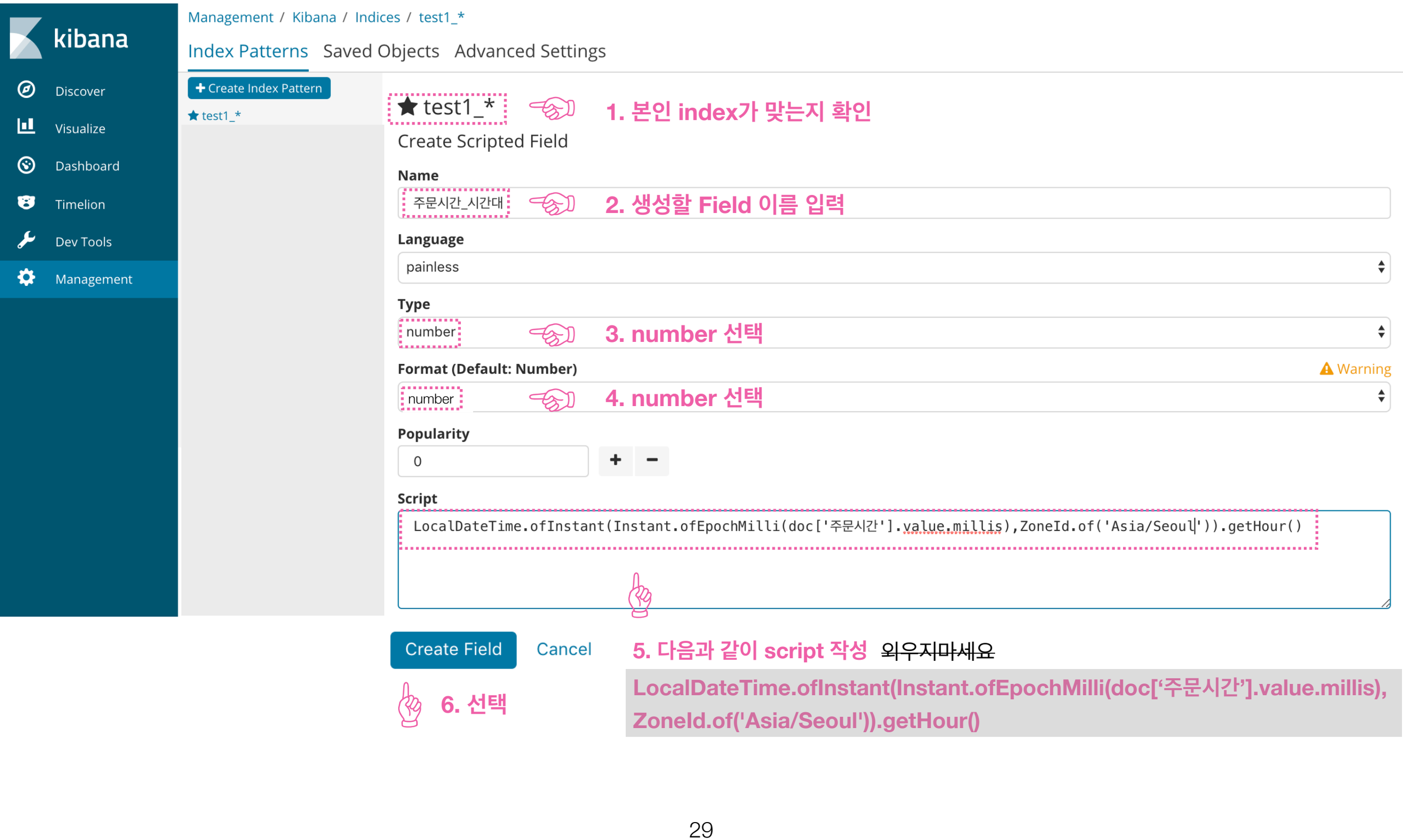
그대로 사용하면 잘못 해석할 여지가 있다

번거롭지만 UTC 시간대로 직접 작업할 것이 아니면

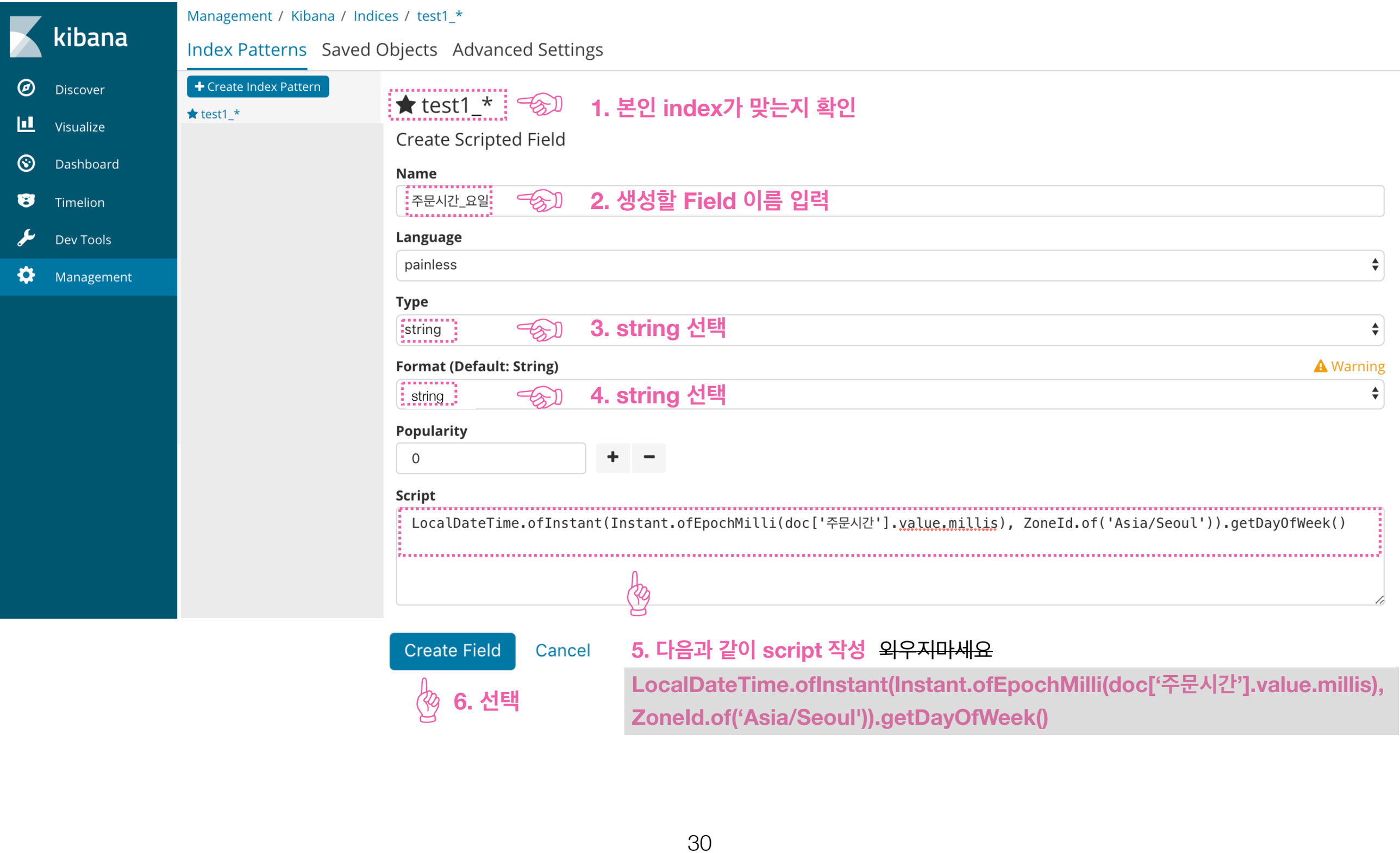
Local 시간대로 변환하는 단계를 거쳐야 한다

(아까 생성한 Scripted Field를 수정하자)

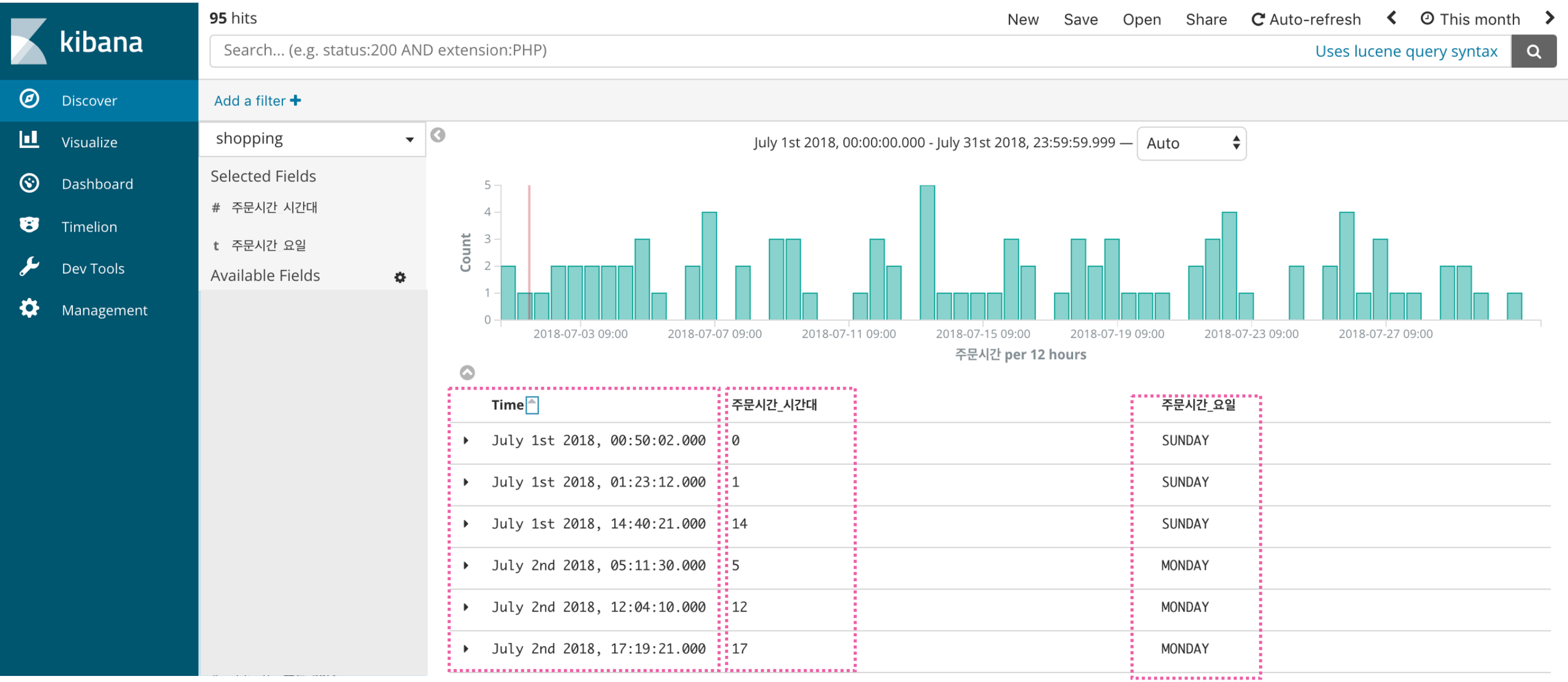
script를 작성하자 심화



script를 작성하자  심화



Discover에 가서 확인하자 심화



Time	주문시간_시간대	주문시간_요일
July 1st 2018, 00:50:02.000	0	SUNDAY
July 1st 2018, 01:23:12.000	1	SUNDAY
July 1st 2018, 14:40:21.000	14	SUNDAY
July 2nd 2018, 05:11:30.000	5	MONDAY
July 2nd 2018, 12:04:10.000	12	MONDAY
July 2nd 2018, 17:19:21.000	17	MONDAY

일치

String Concatenation 연산은 안되나?

Field 간 연산은 안되나?

Date Field에서 연/월/일/시/분/초 등 접근 안되나?

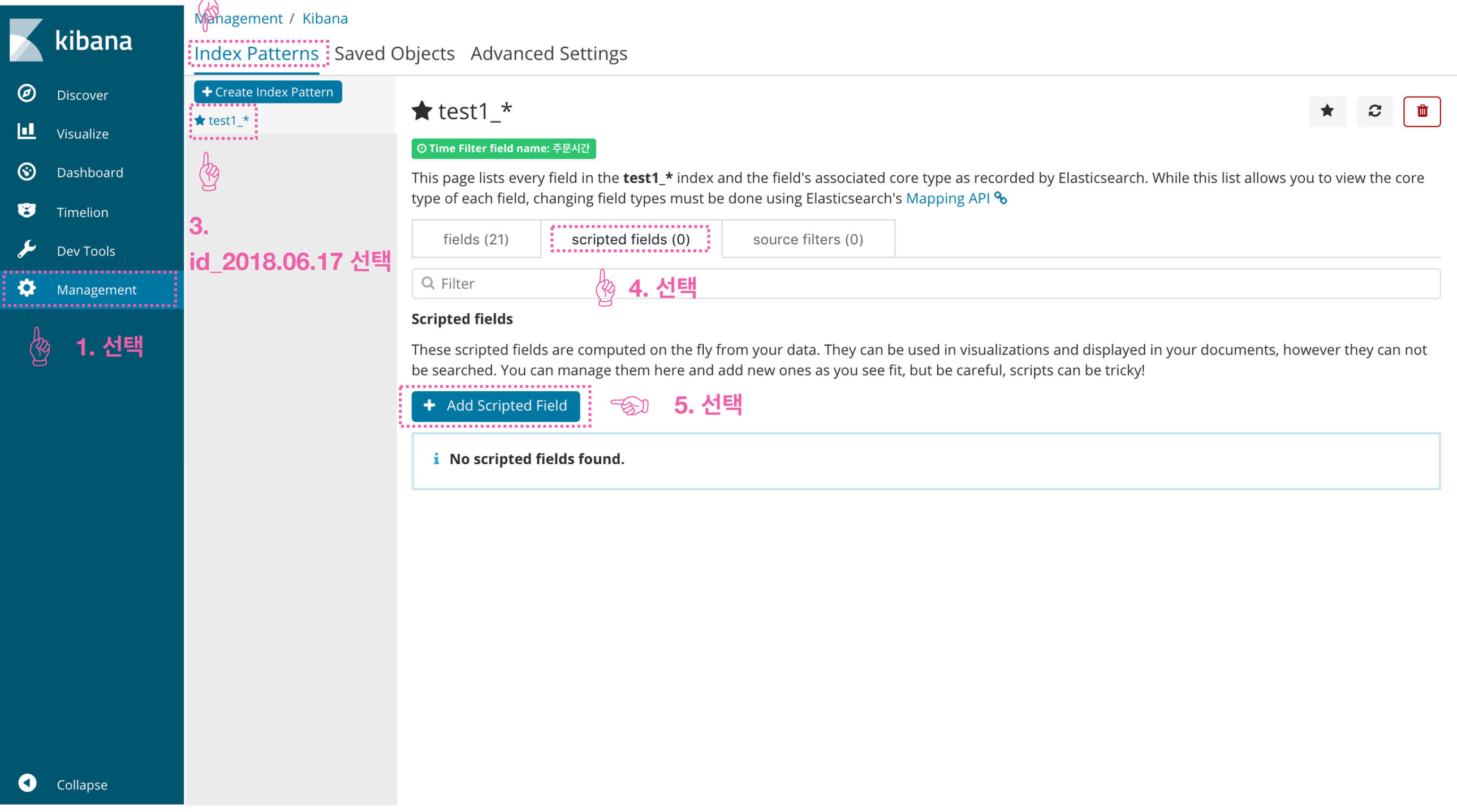
기존 Field에 조건을 적용해서 새로운 Field를 만들 수 없나? 

예시

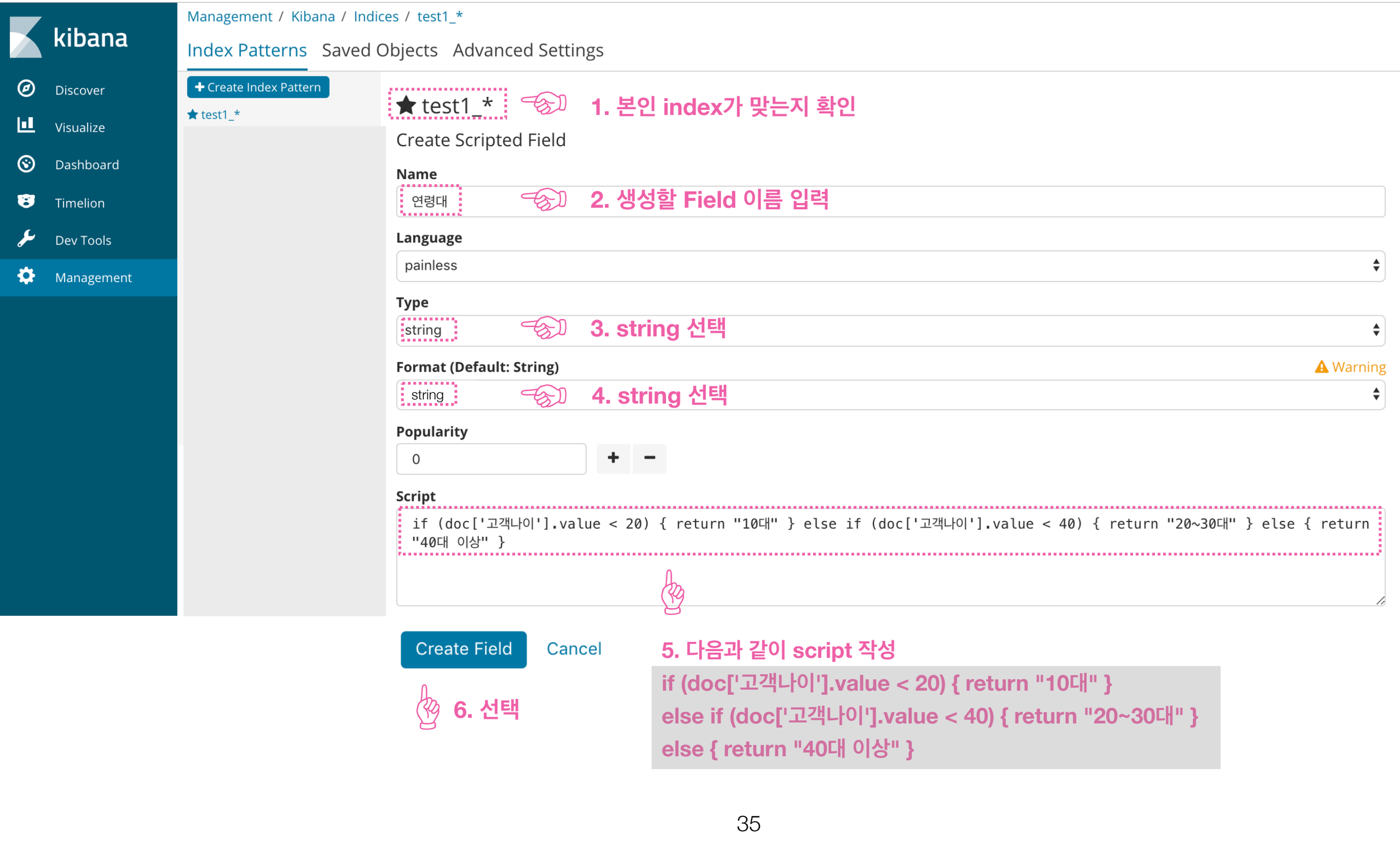
고객나이 Field 값에 따라 10대, 20대, 30대, …

와 같은 값을 갖는 Field를 만들고 싶다면?

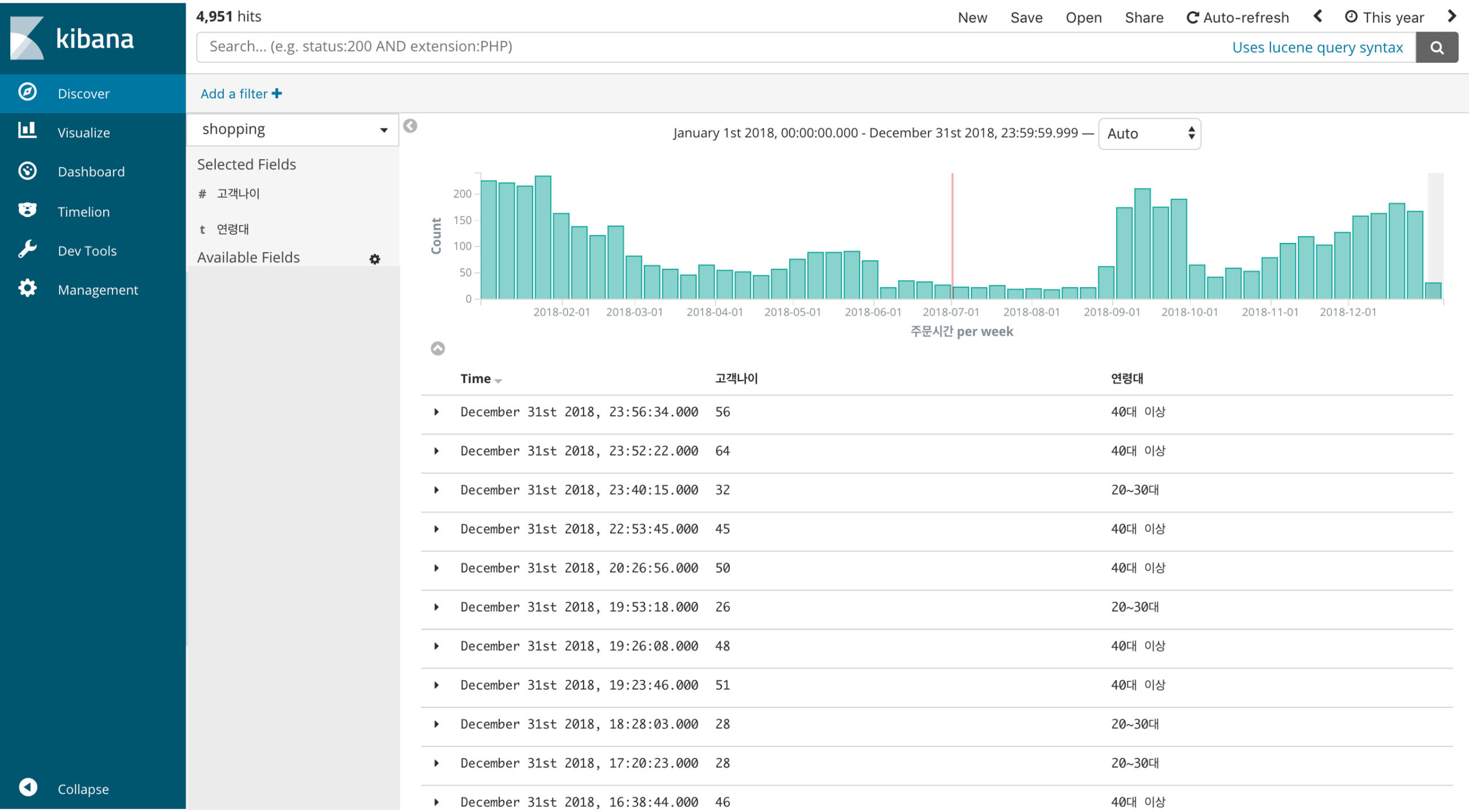
scripted field를 추가하자



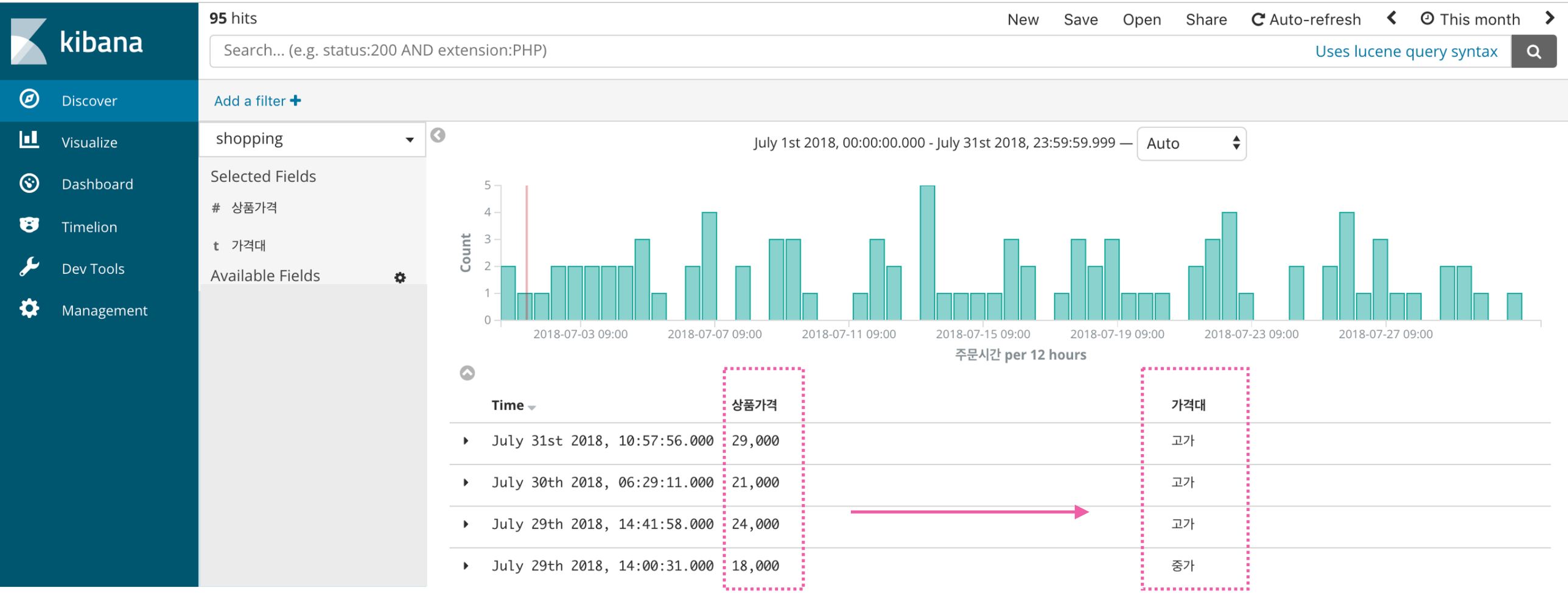
script를 작성하자 ♕



Discover에 가서 확인하자



예제2 - Scripted Field



상품가격	가격대
x < 10,000	저가
10,000 ≤ x < 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 **format만 살짝 변경**해서 보여줄 수 없을까?

Date를 다르게 표현할 수 없나? 👑

20180701

1511199899

Sunday Jul 1st 18

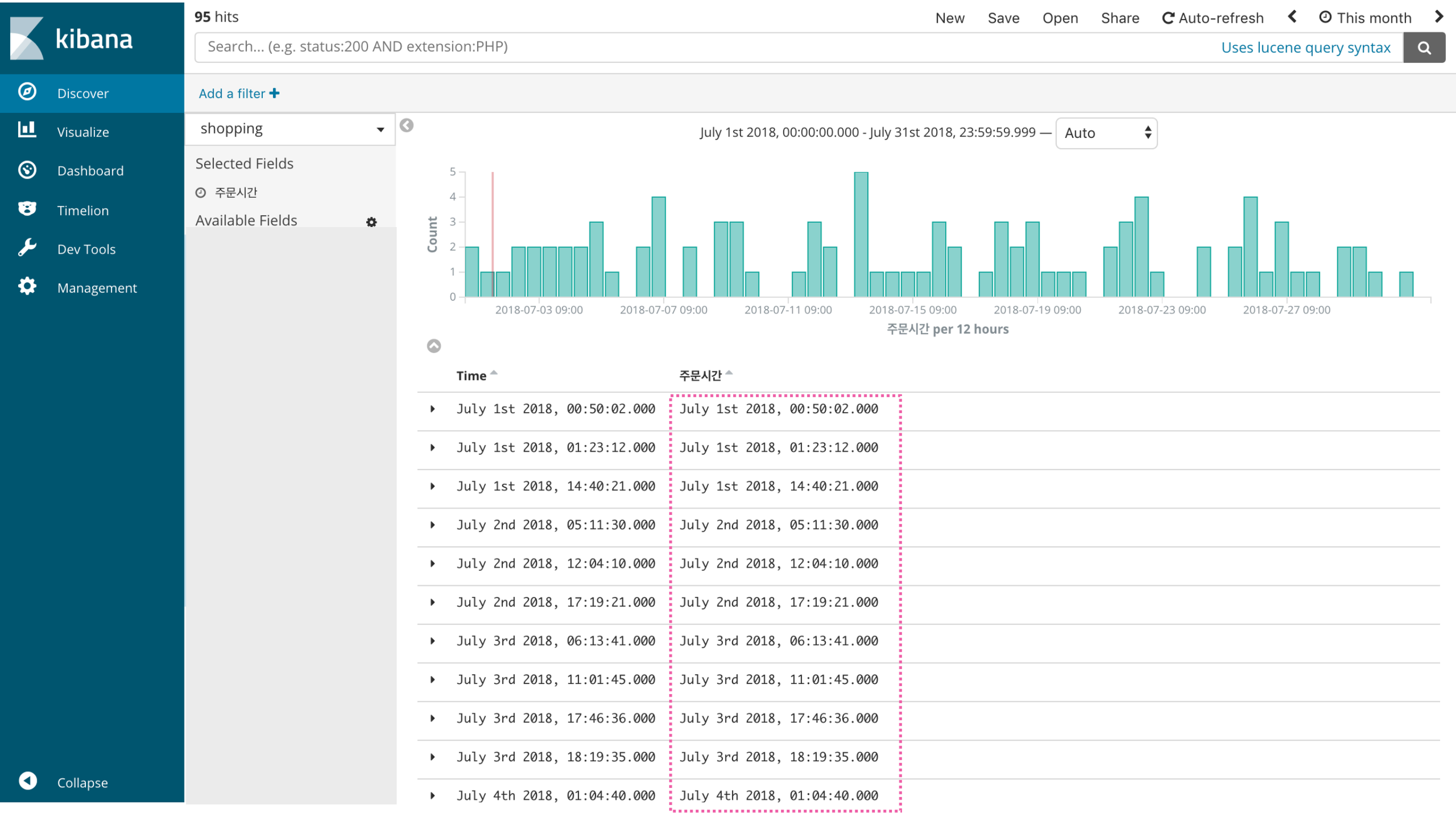
2017년 11월 20일 17시 44분

11/20/2017 5:44pm

2018년07월01일

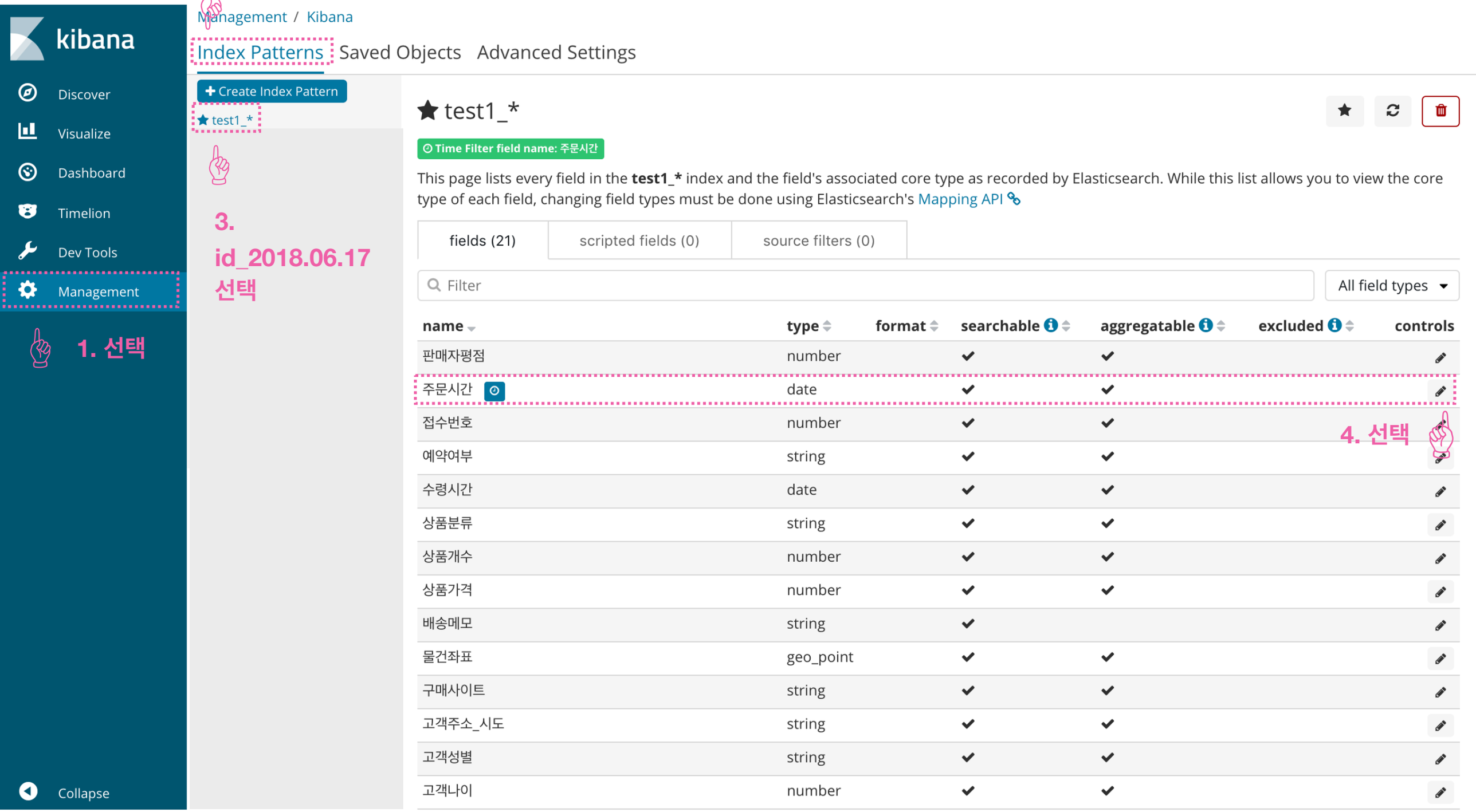
July 1st 2018, 9:05:21 pm

Default는 아래와 같은 Format이다



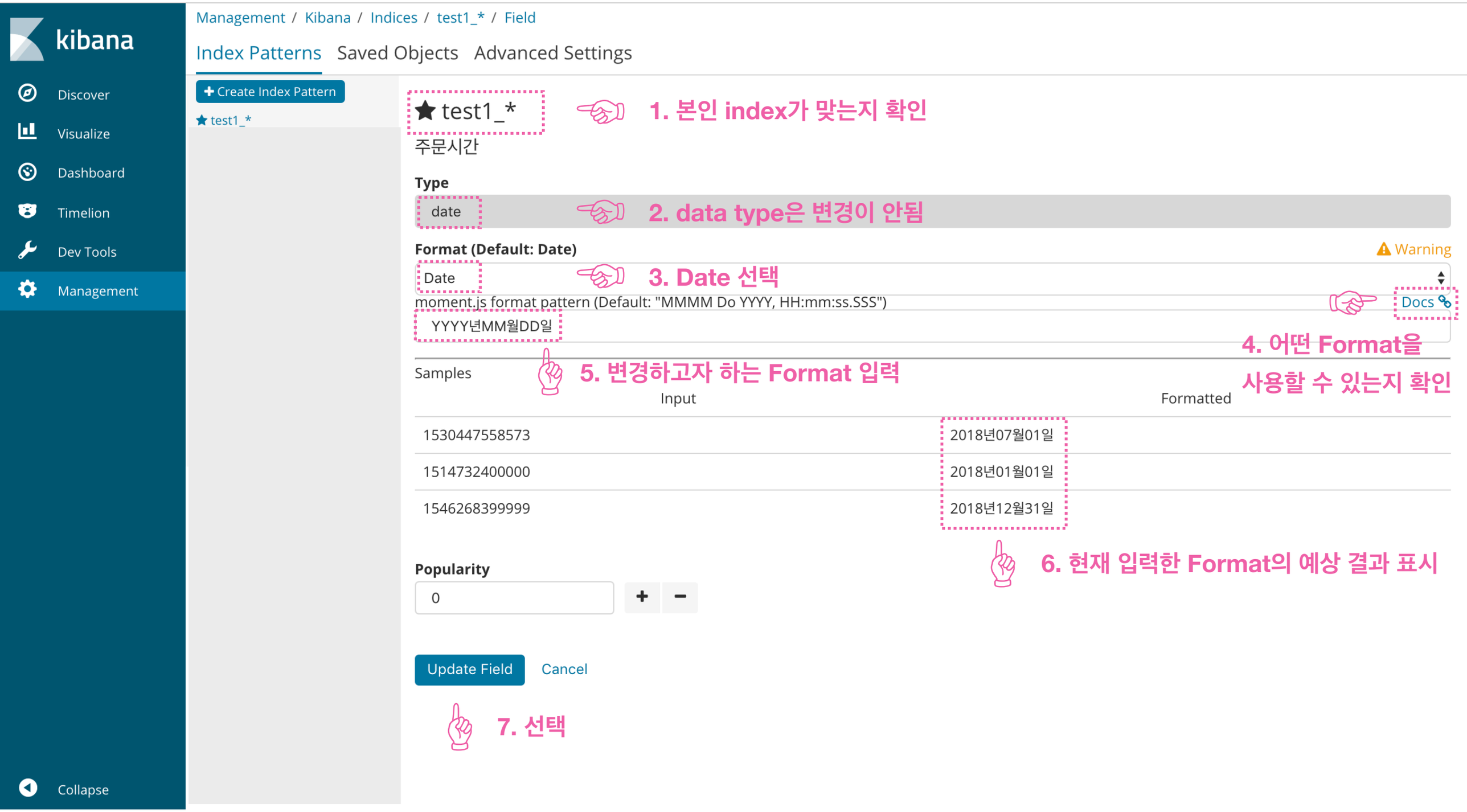
Time	주문시간
July 1st 2018, 00:50:02.000	July 1st 2018, 00:50:02.000
July 1st 2018, 01:23:12.000	July 1st 2018, 01:23:12.000
July 1st 2018, 14:40:21.000	July 1st 2018, 14:40:21.000
July 2nd 2018, 05:11:30.000	July 2nd 2018, 05:11:30.000
July 2nd 2018, 12:04:10.000	July 2nd 2018, 12:04:10.000
July 2nd 2018,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

Date Format 변경하려는 Field의 Controls 선택

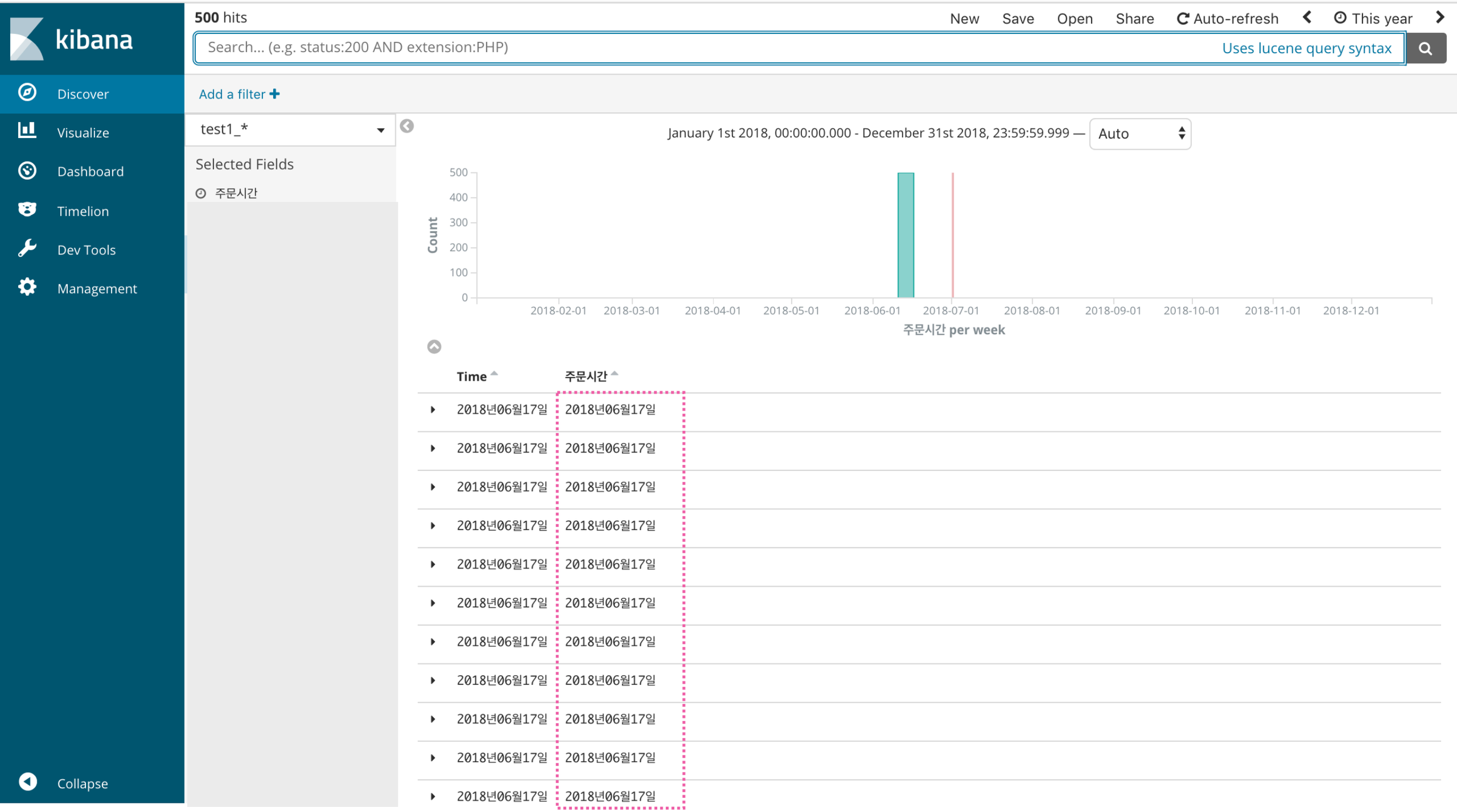


name	type	format	searchable	aggregatable	excluded	controls
판매자평점	number		✔	✔		
주문시간	date		✔	✔		
접수번호	number		✔	✔		
예약여부	string		✔	✔		
수령시간	date		✔	✔		
상품분류	string		✔	✔		
상품개수	number		✔	✔		
상품가격	number		✔	✔		
배송메모	string		✔			
물건좌표	geo_point		✔	✔		
구매사이트	string		✔	✔		
고객주소_시도	string		✔	✔		
고객성별	string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

적절한 Format으로 수정하자



Discover에 돌아가서 확인하자



예제3 - 아래 표를 이용해서 여러가지 Format을 테스트해보자

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

String를 다르게 표현할 수 없나? 👑

higee.io/221111469658

221111469658

higee.io/221111469658 (링크 형식)

221111469658 (링크 형식)

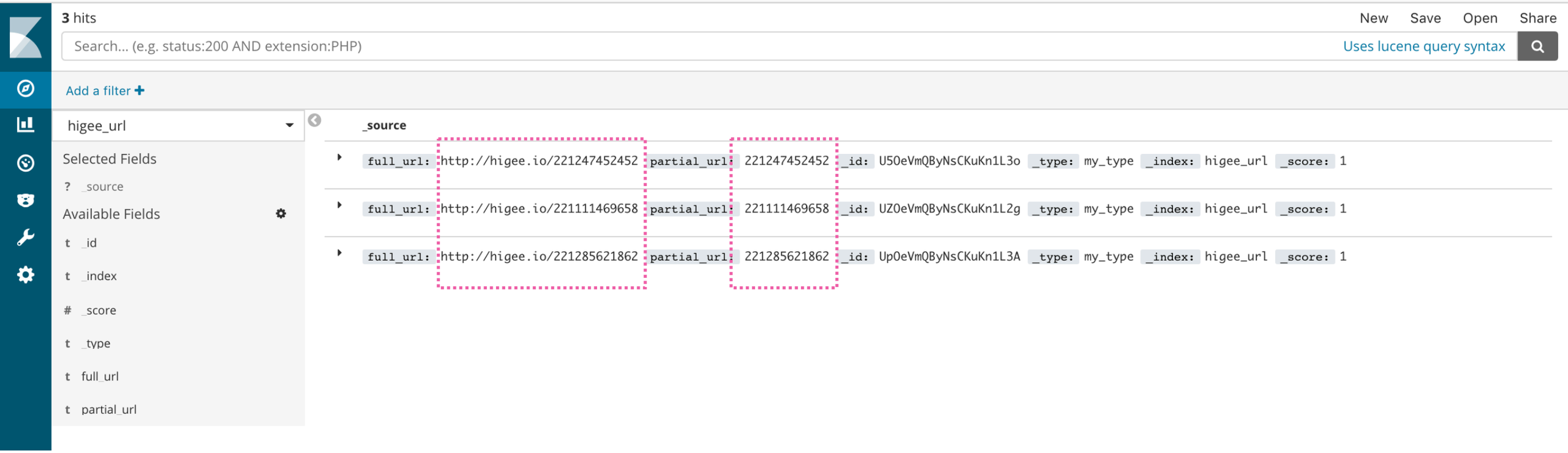
HIGEE/IO/221111469658 (대문자)

String Type의 Format 전환 실습을 위해 Index를 등록하자

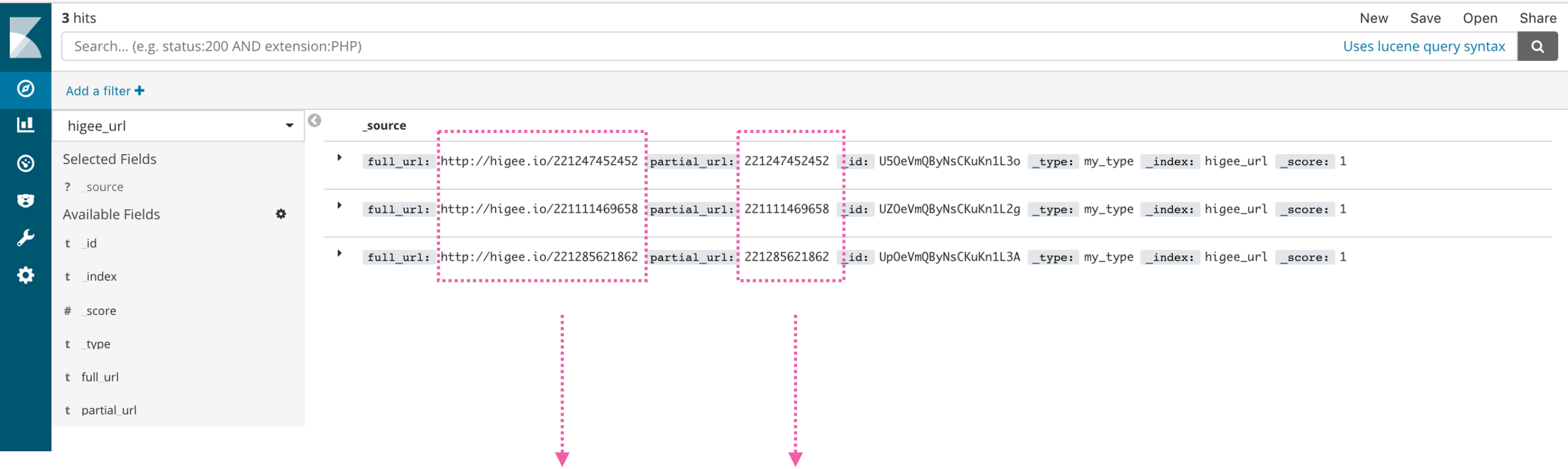
Index : {id}_url

Time Filter Field : 없음

Default는 아래와 같은 Format이다



Default는 아래와 같은 Format이다



URL 형태를 띄는 두 Field의 Format을 String 에서 **URL**로 변경해보자

Data Format 변경하려는 Field의 Control 선택 - **full_url**

2. 선택

Management / Kibana

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

higee_url

3. id_url 선택

1. 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

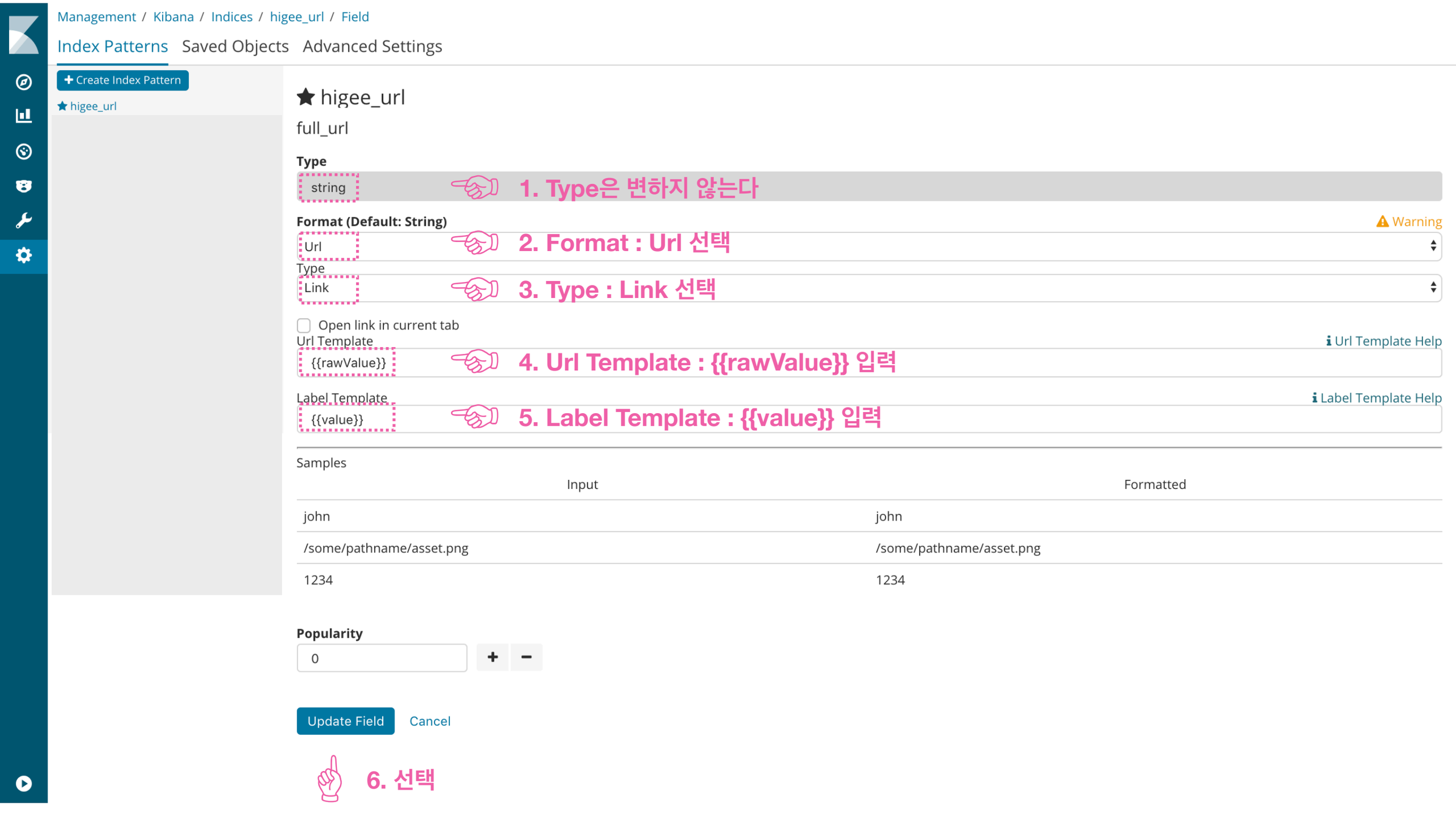
name	type	format	searchable	aggregatable	excluded	controls
_id	string		✔	✔		
_index	string		✔	✔		
_score	number					
_source	_source					
_type	string		✔	✔		
full_url	string		✔	✔		
partial_url	string		✔	✔		

4. 선택

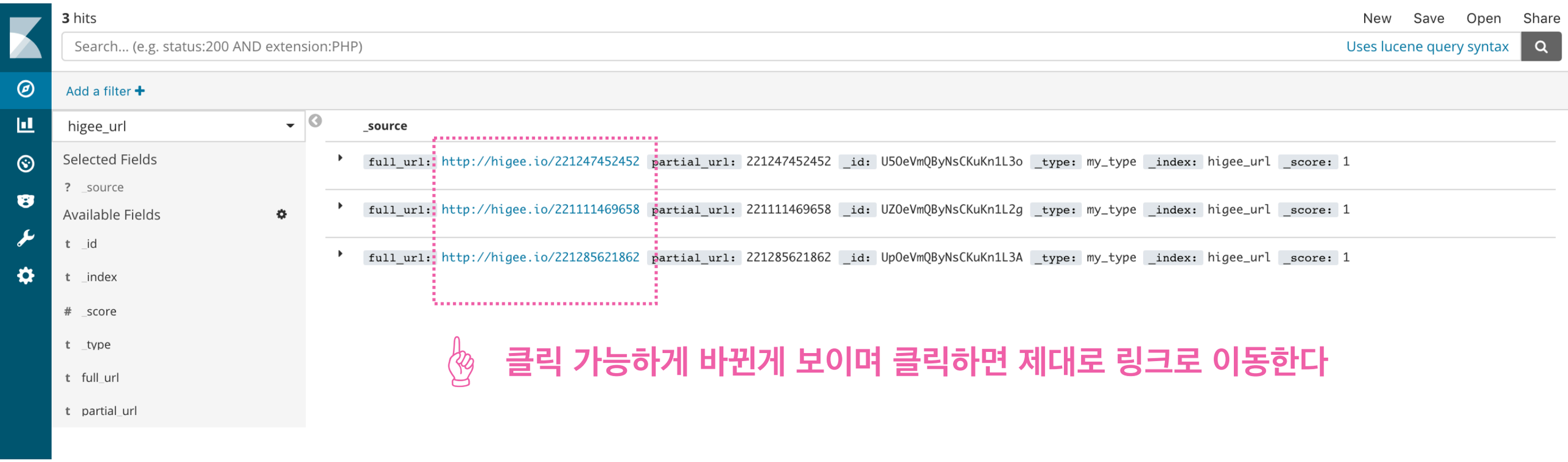
Scroll to top

Page Size 25

Url Templates에 적절한 값을 입력하자



Discover에 돌아가서 확인하자



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

1. 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

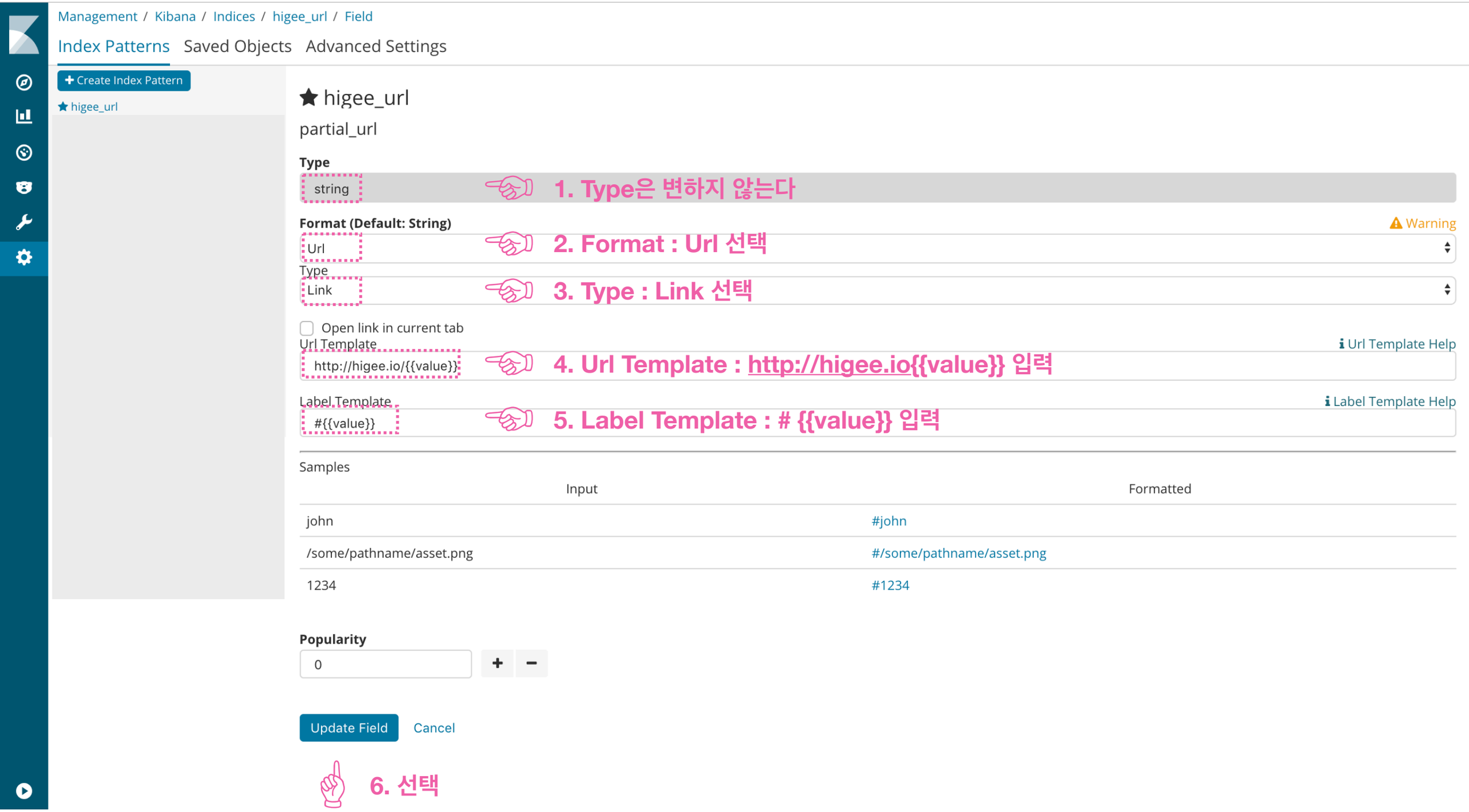
name	type	format	searchable	aggregatable	excluded	controls
_id	string		✔	✔		
_index	string		✔	✔		
_score	number					
_source	_source					
_type	string		✔	✔		
full_url	string	Url	✔	✔		
partial_url	string		✔	✔		

Scroll to top

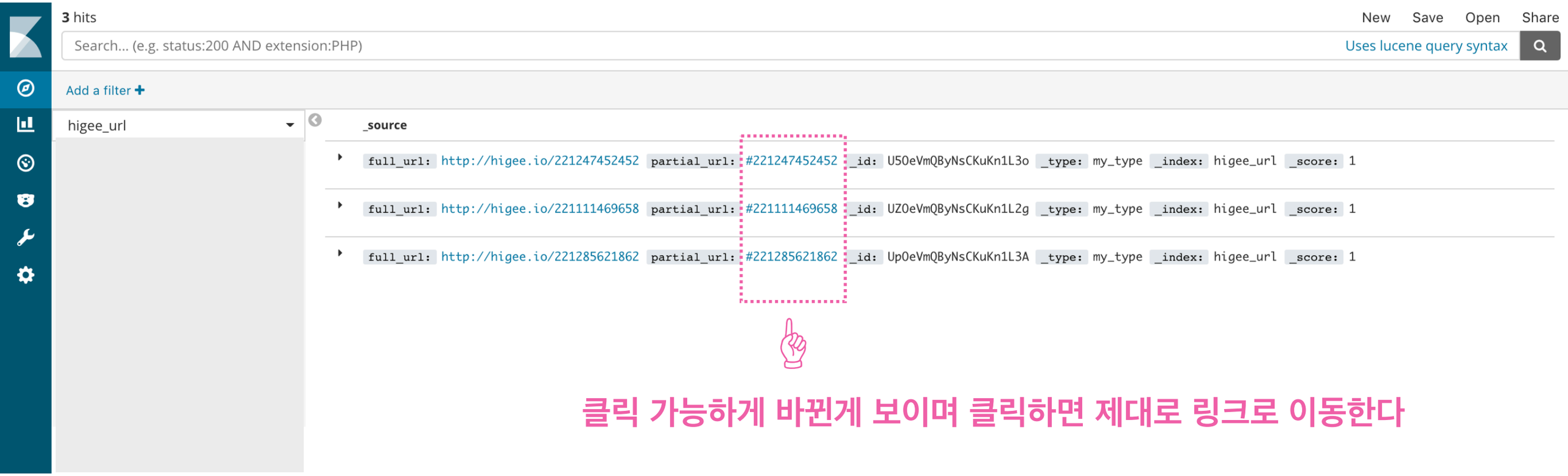
Page Size 25

4. 선택

Url Templates에 적절한 값을 입력하자

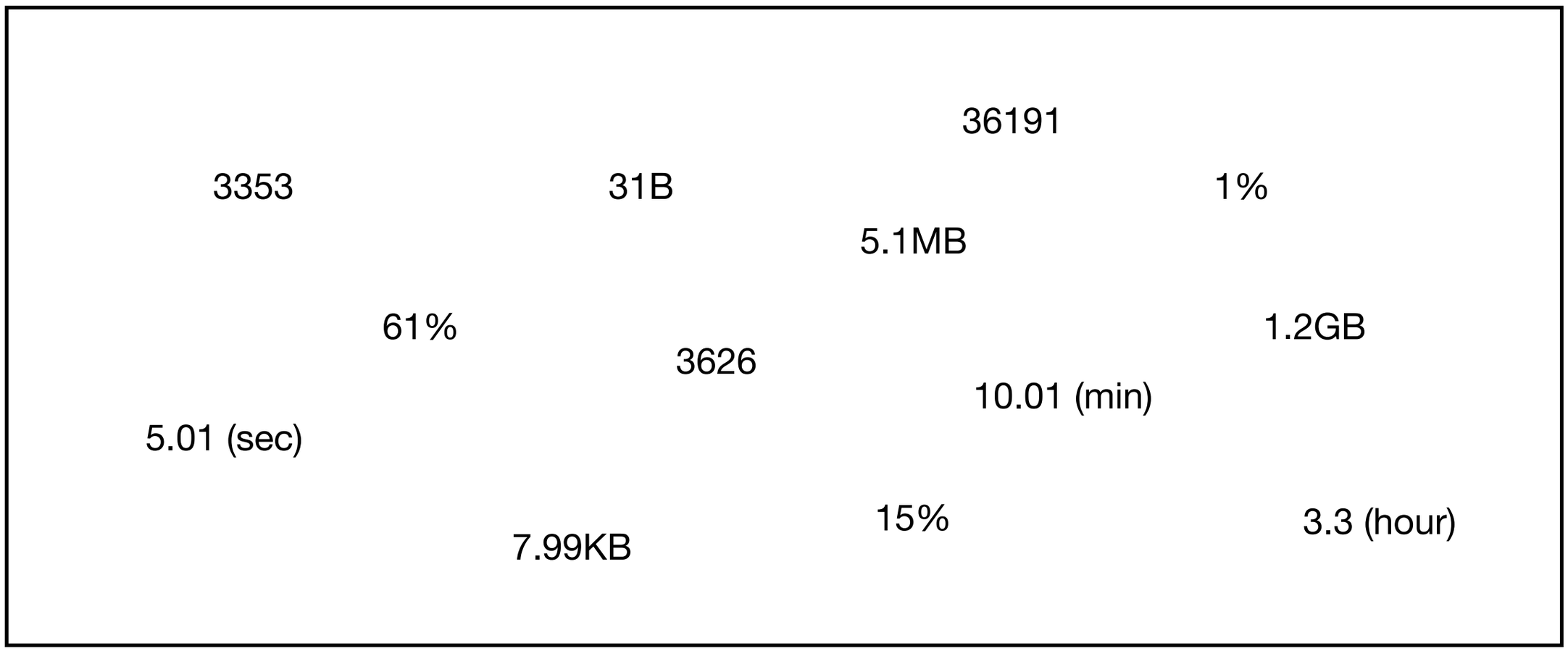


Discover에 돌아가서 확인하자



클릭 가능하게 바뀐게 보이며 클릭하면 제대로 링크로 이동한다

Number를 다르게 표현할 수 없나? 👑

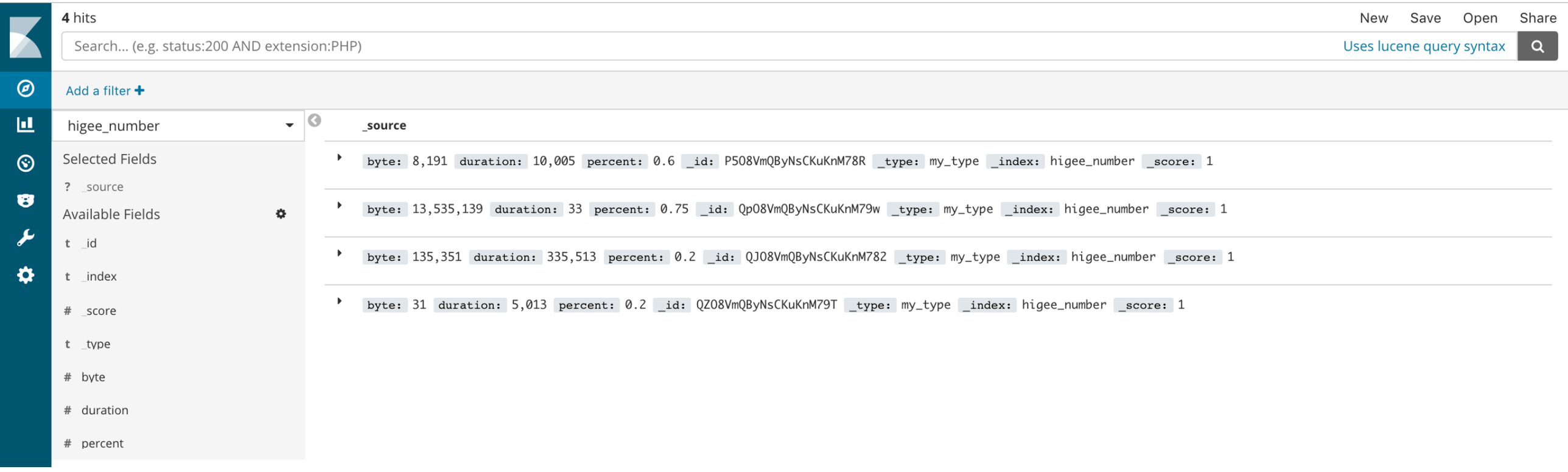


Number Type의 Format 전환 실습을 위해 Index를 등록하자

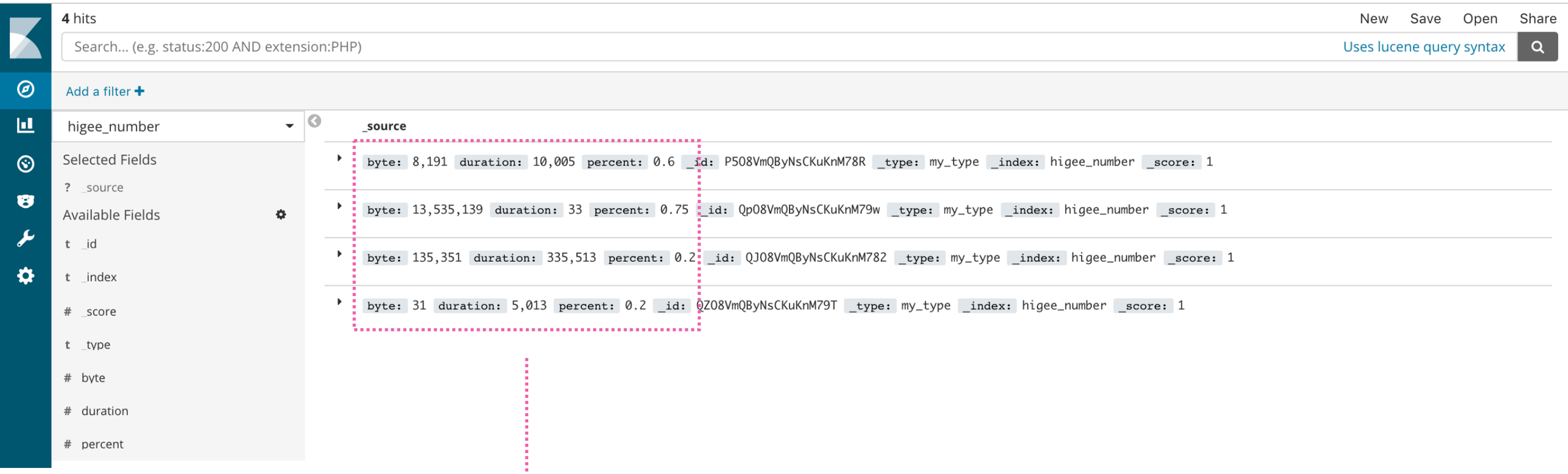
Index : {id}_number

Time Filter Field : 없음

Default는 아래와 같은 Format이다

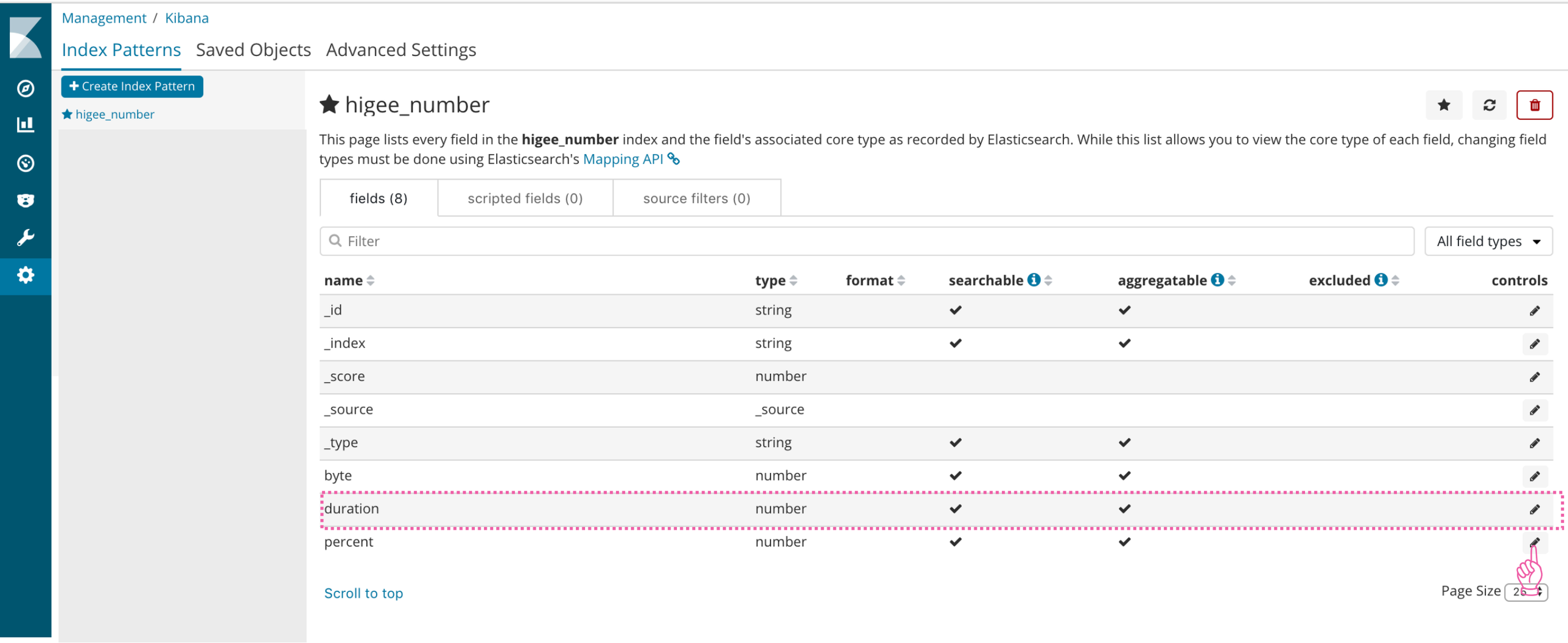


Default는 아래와 같은 Format이다

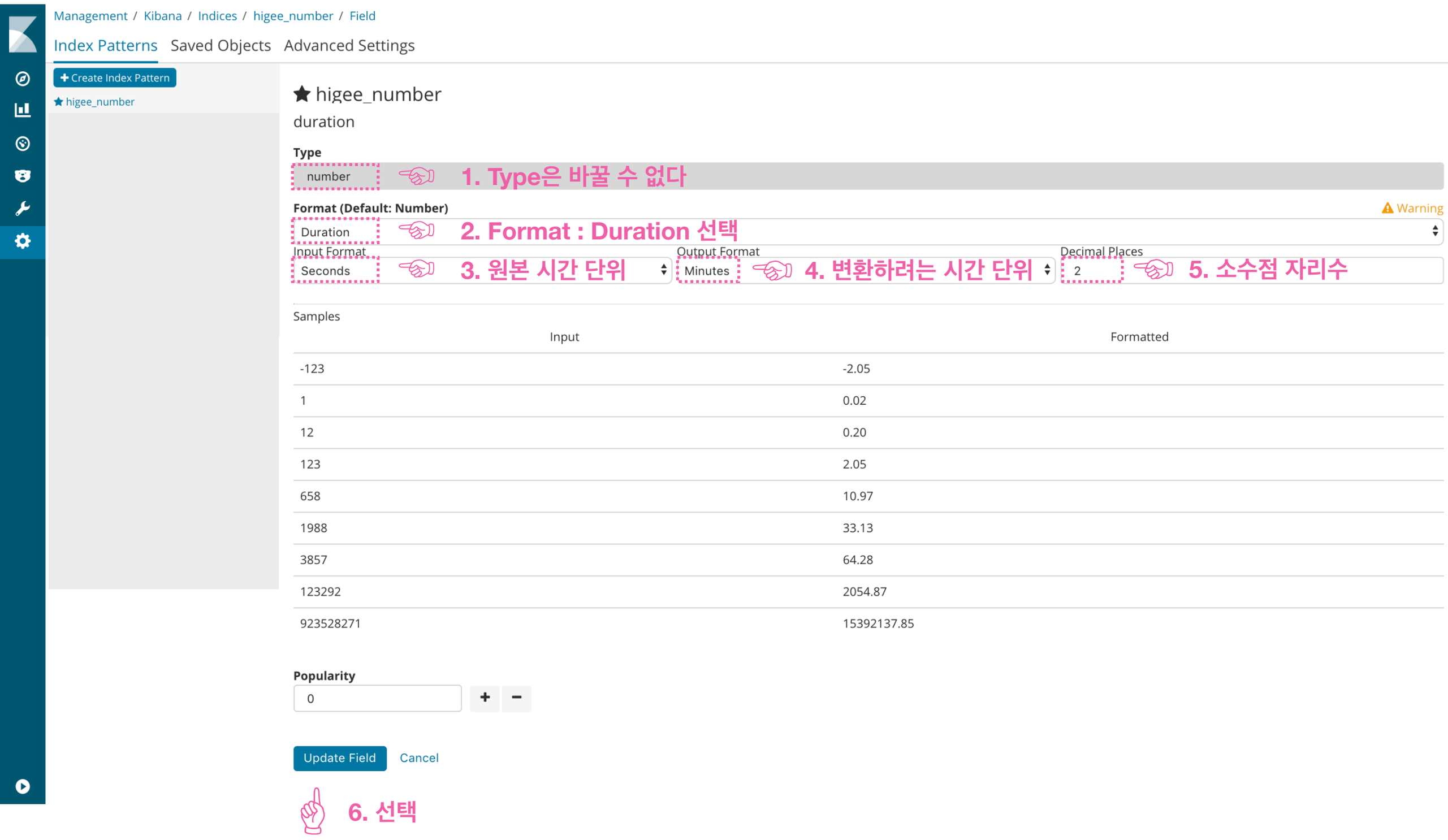


Number 들에 의미를 부여해보자

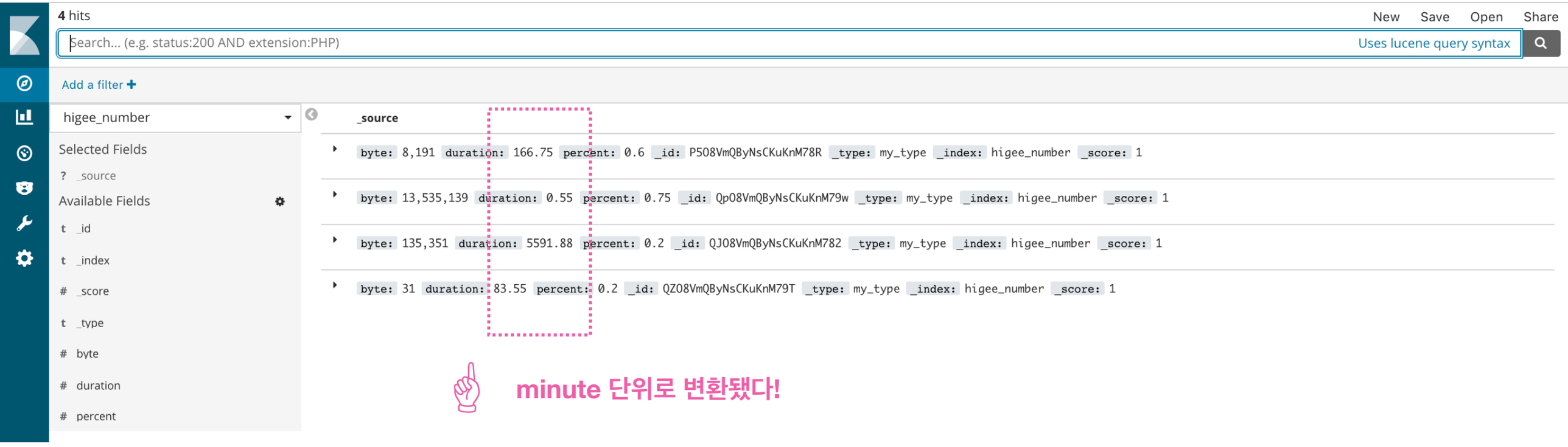
Data Format 변경하려는 Field의 Control 선택 - duration



duration Field Format을 변경하자

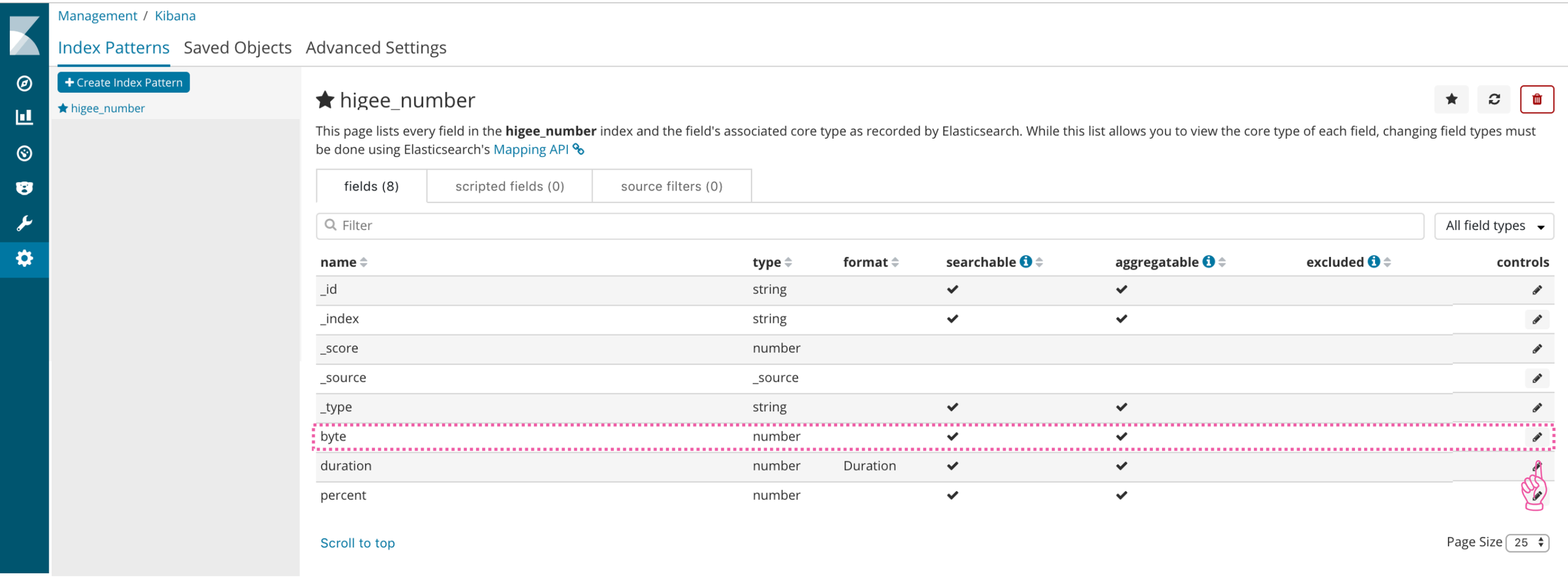


Discover에 돌아가서 확인하자



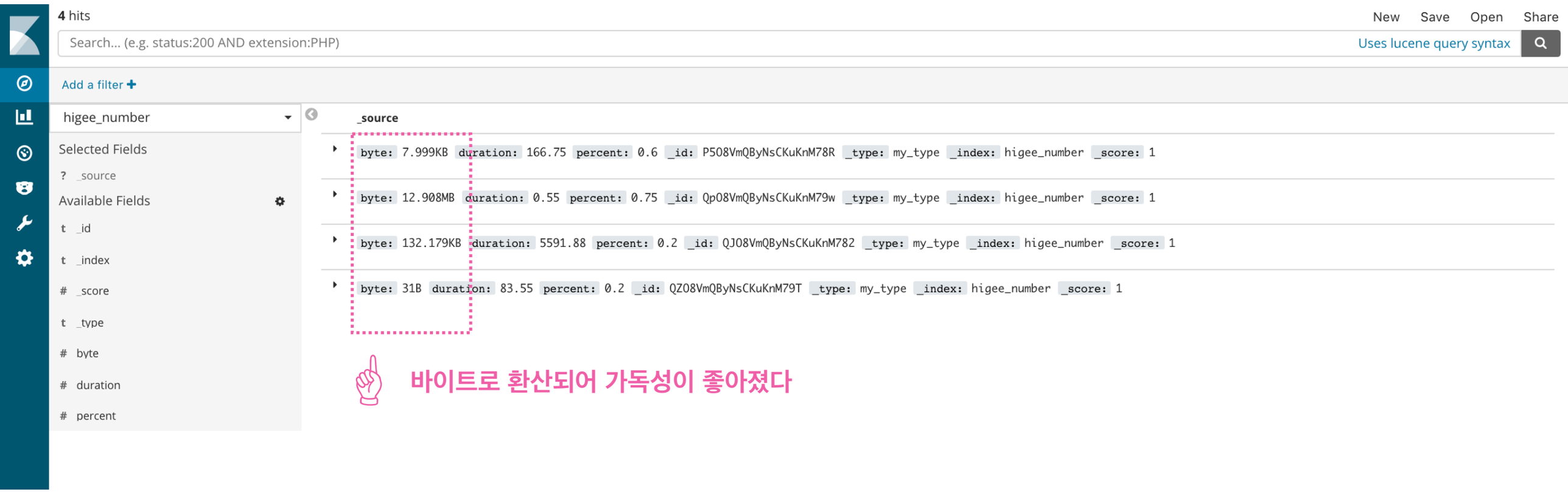
minute 단위로 변환됐다!

Data Format 변경하려는 Field의 Control 선택 - byte



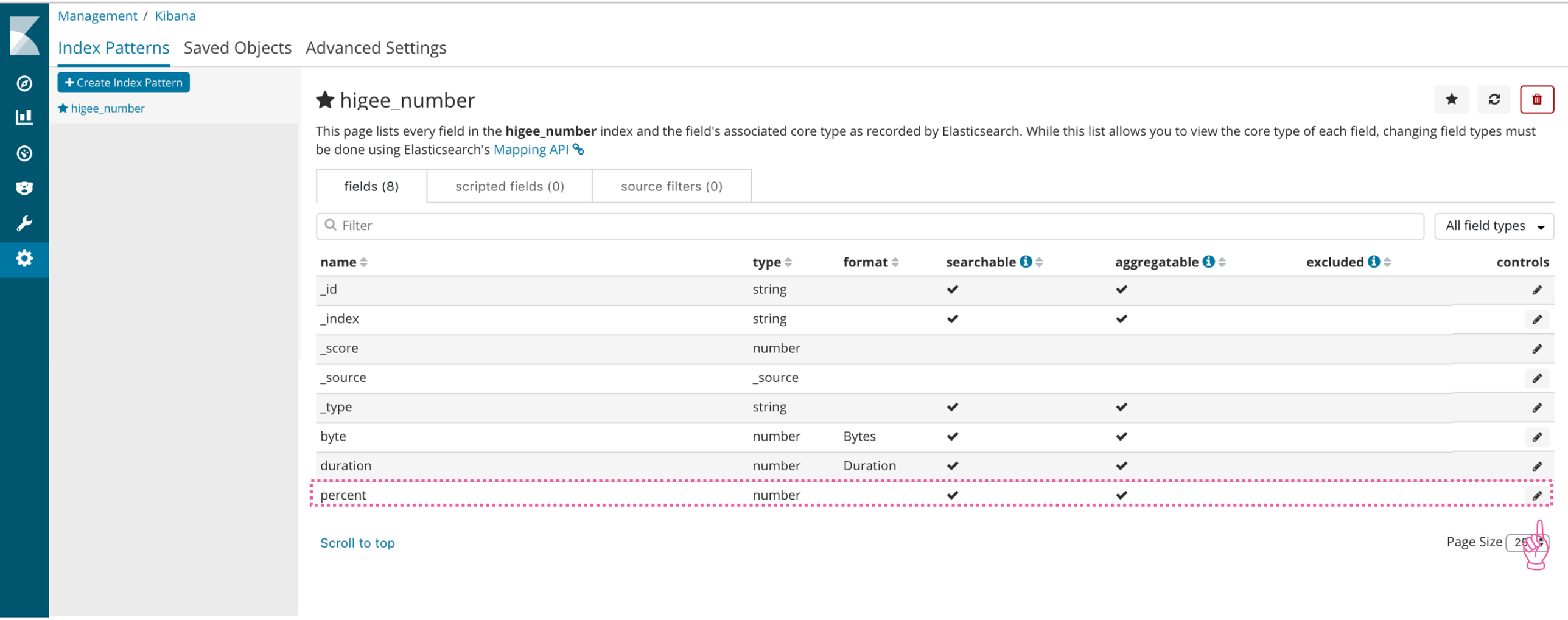
duration Field Format을 변경하자

Discover에 돌아가서 확인하자

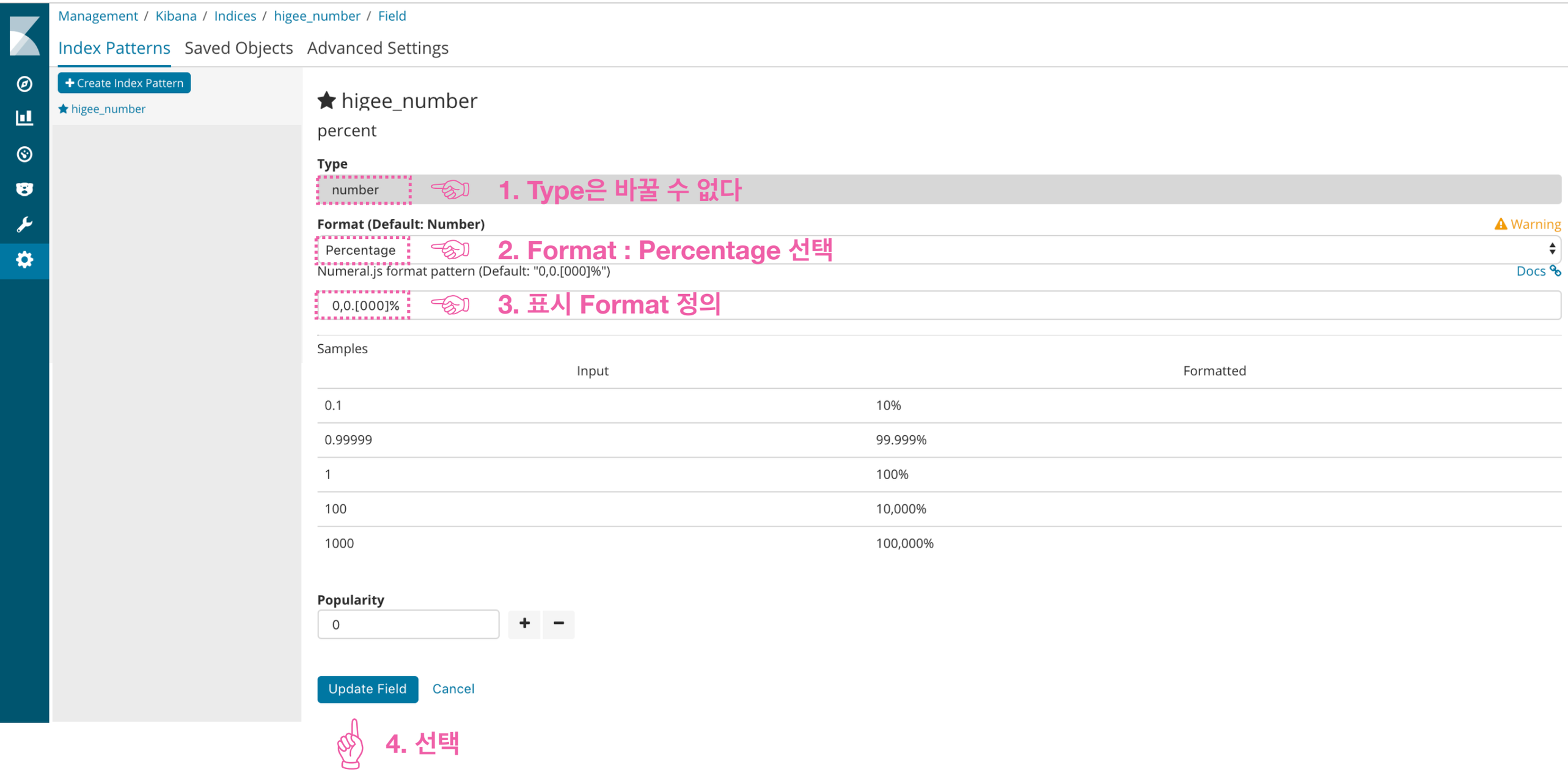


바이트로 환산되어 가독성이 좋아졌다

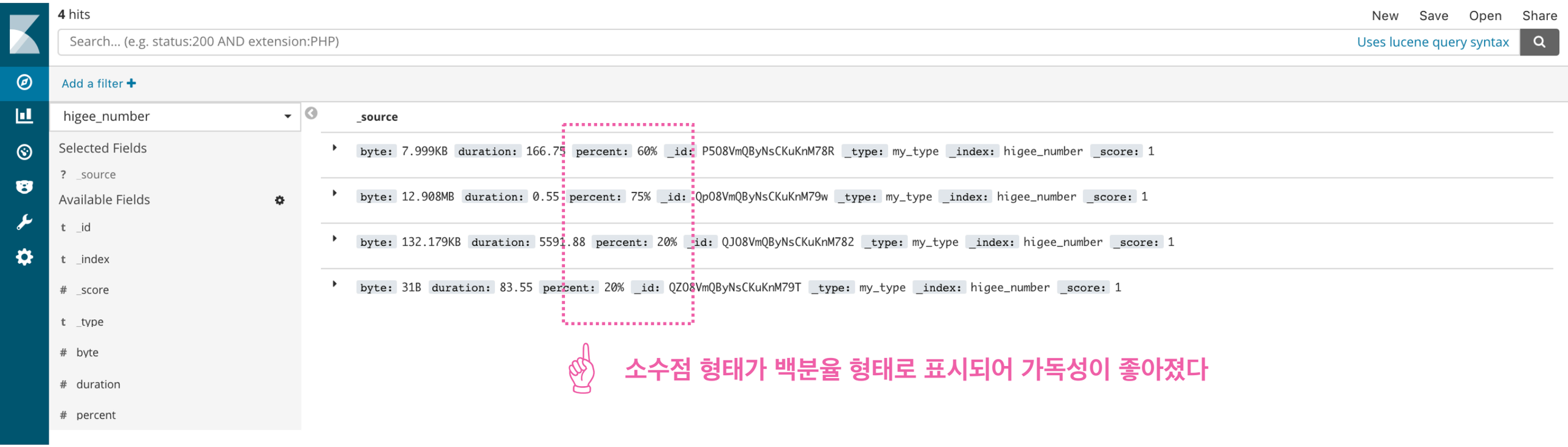
Data Format 변경하려는 Field의 Control 선택 - percentage



duration Field Format을 변경하자



Discover에 돌아가서 확인하자



소수점 형태가 백분율 형태로 표시되어 가독성이 좋아졌다

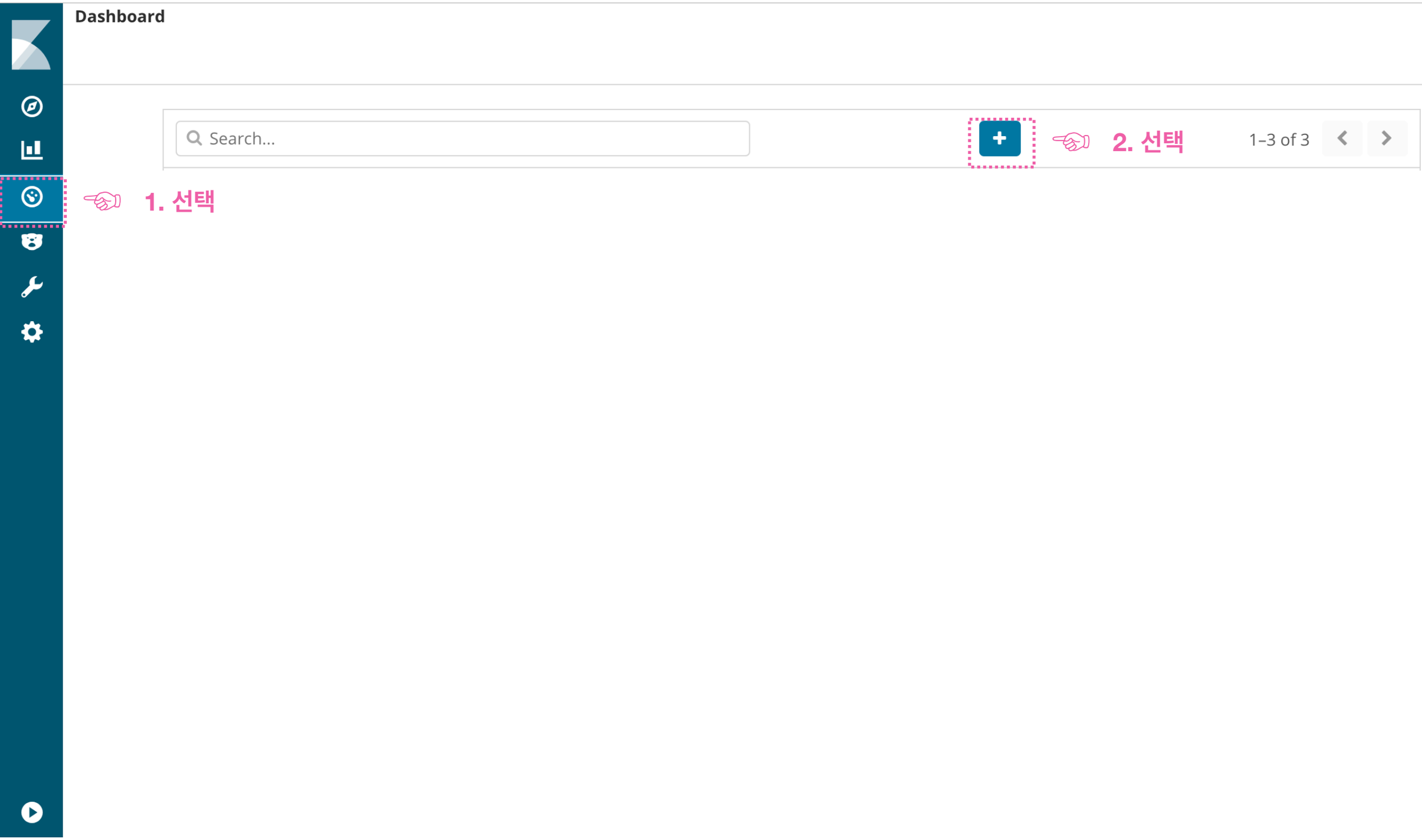
잠깐3

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

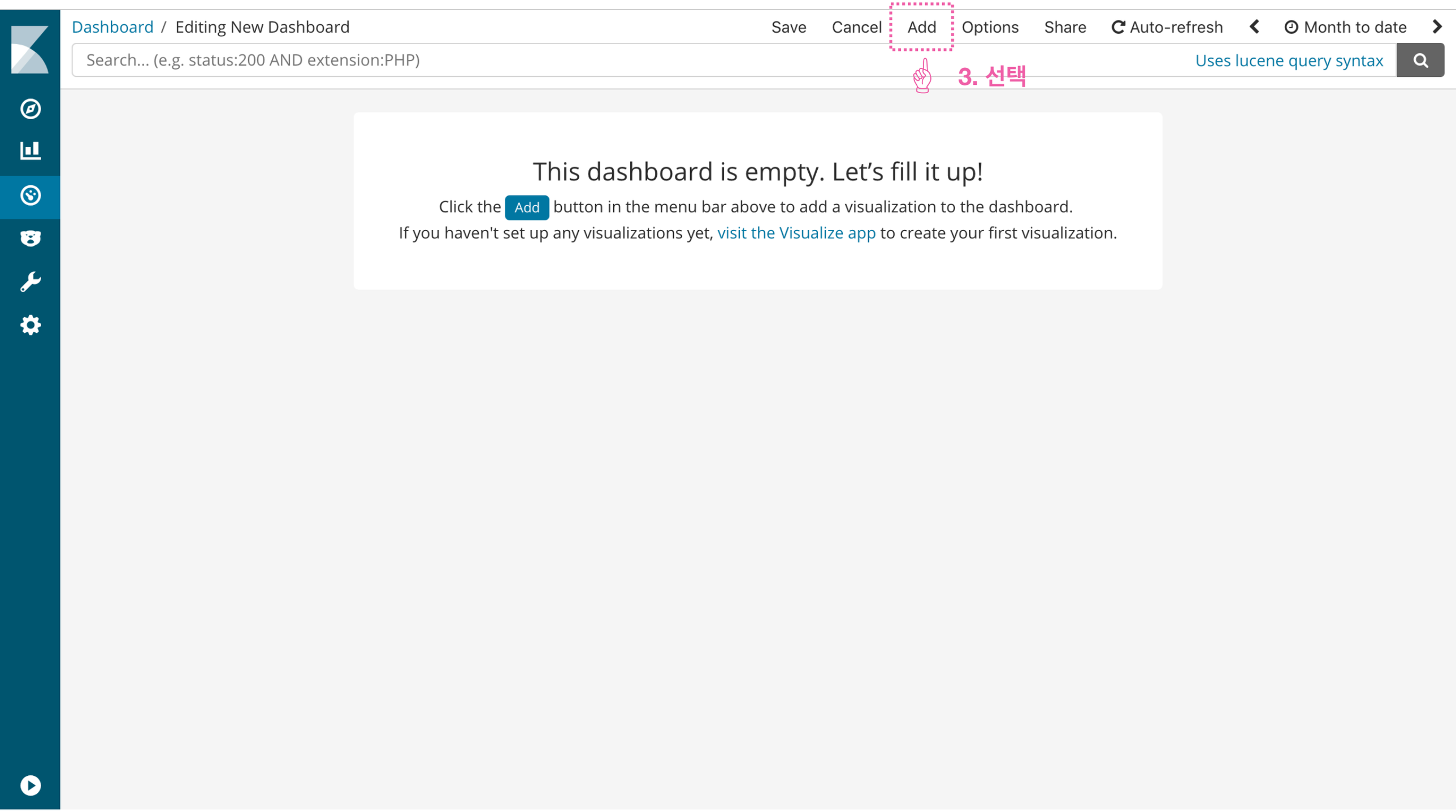
그러므로 Elasticsearch에 저장된 데이터 자체는 변하지 않는다!

Dashboard 기능

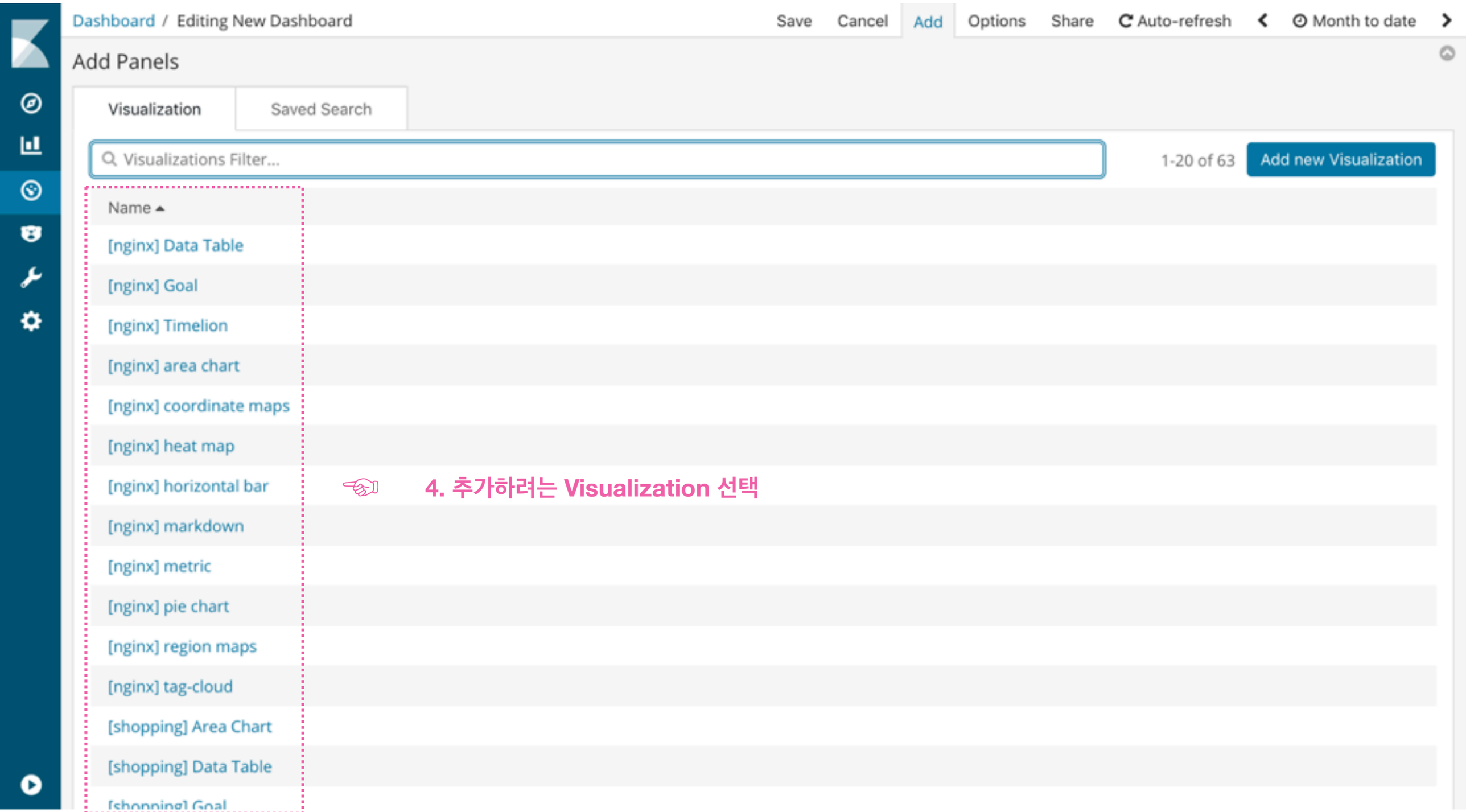
우선 새로운 Dashboard를 만들자



우선 새로운 Dashboard를 만들자



우선 새로운 Dashboard를 만들자

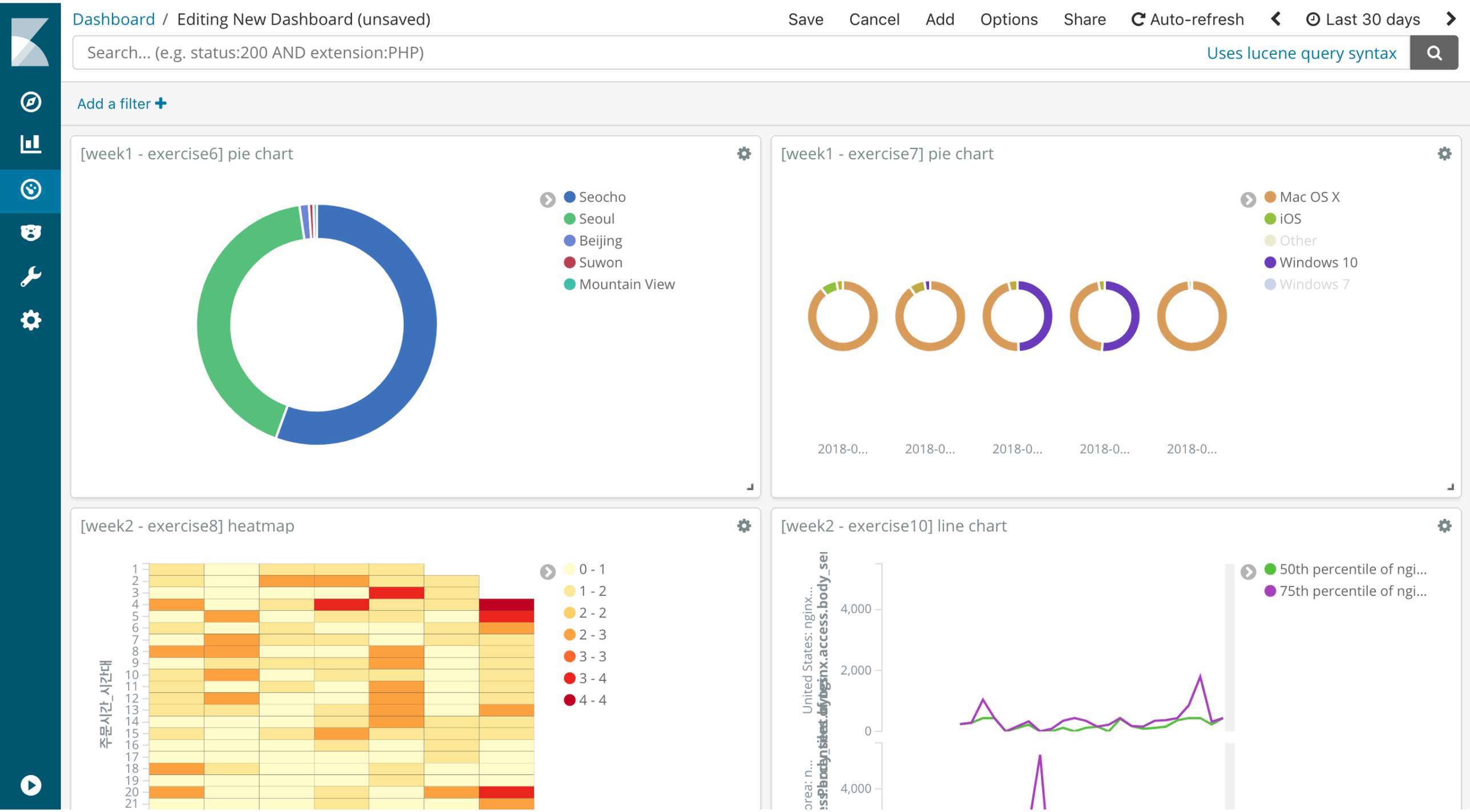


Visualization을 추가하자

ID가 higee인 경우,

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

Visualization을 적당히 배치하자



Dashboard를 저장하자

Dashboard / Editing New Dashboard (unsaved)

Save Cancel Add Options Share Auto-refresh Last 30 days

Save dashboard

1. 선택

Title

New Dashboard 2. Dashboard Title 입력

Description

Dashboard description

Store time with dashboard

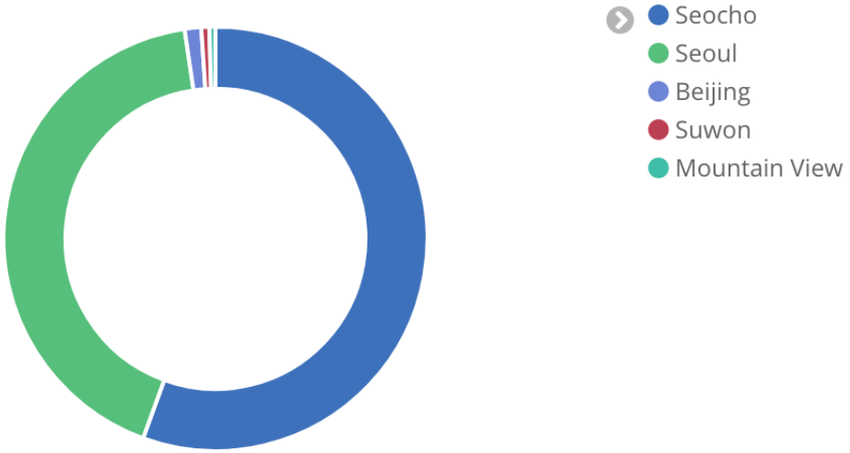
This changes the time filter to the currently selected time each time this dashboard is loaded.

Save 3. 선택

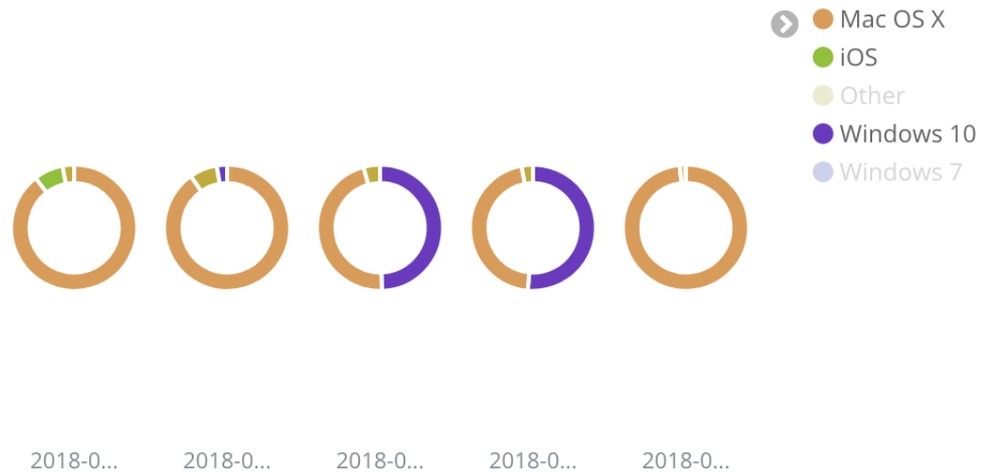
Search... (e.g. status:200 AND extension:PHP) Uses lucene query syntax

Add a filter +

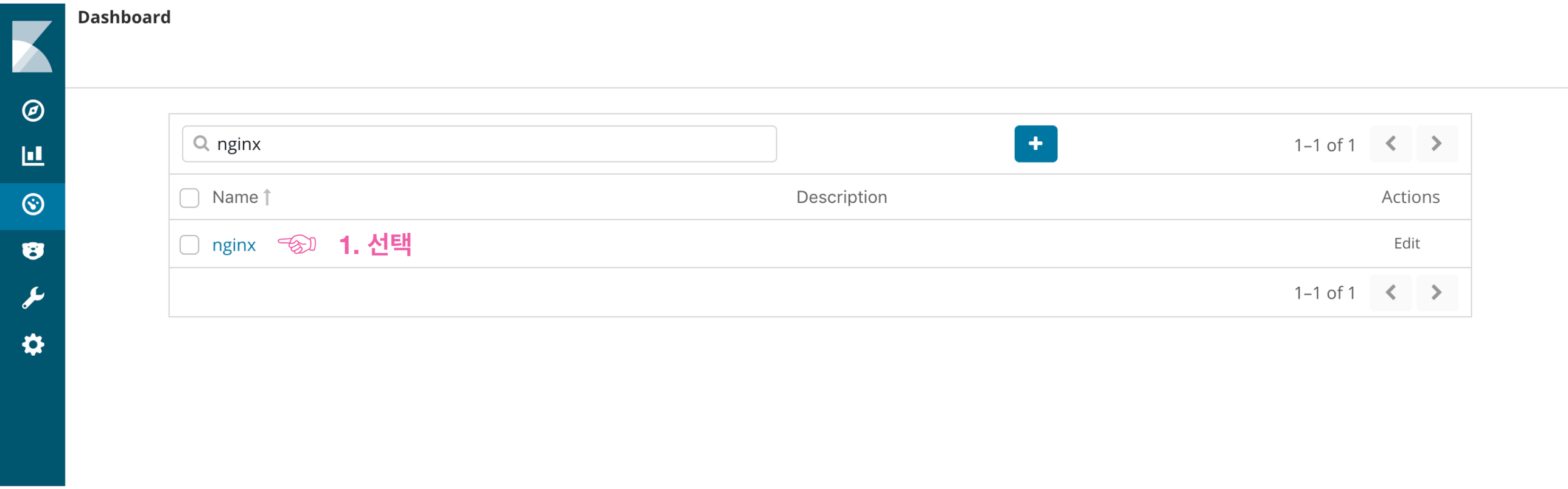
[week1 - exercise6] pie chart



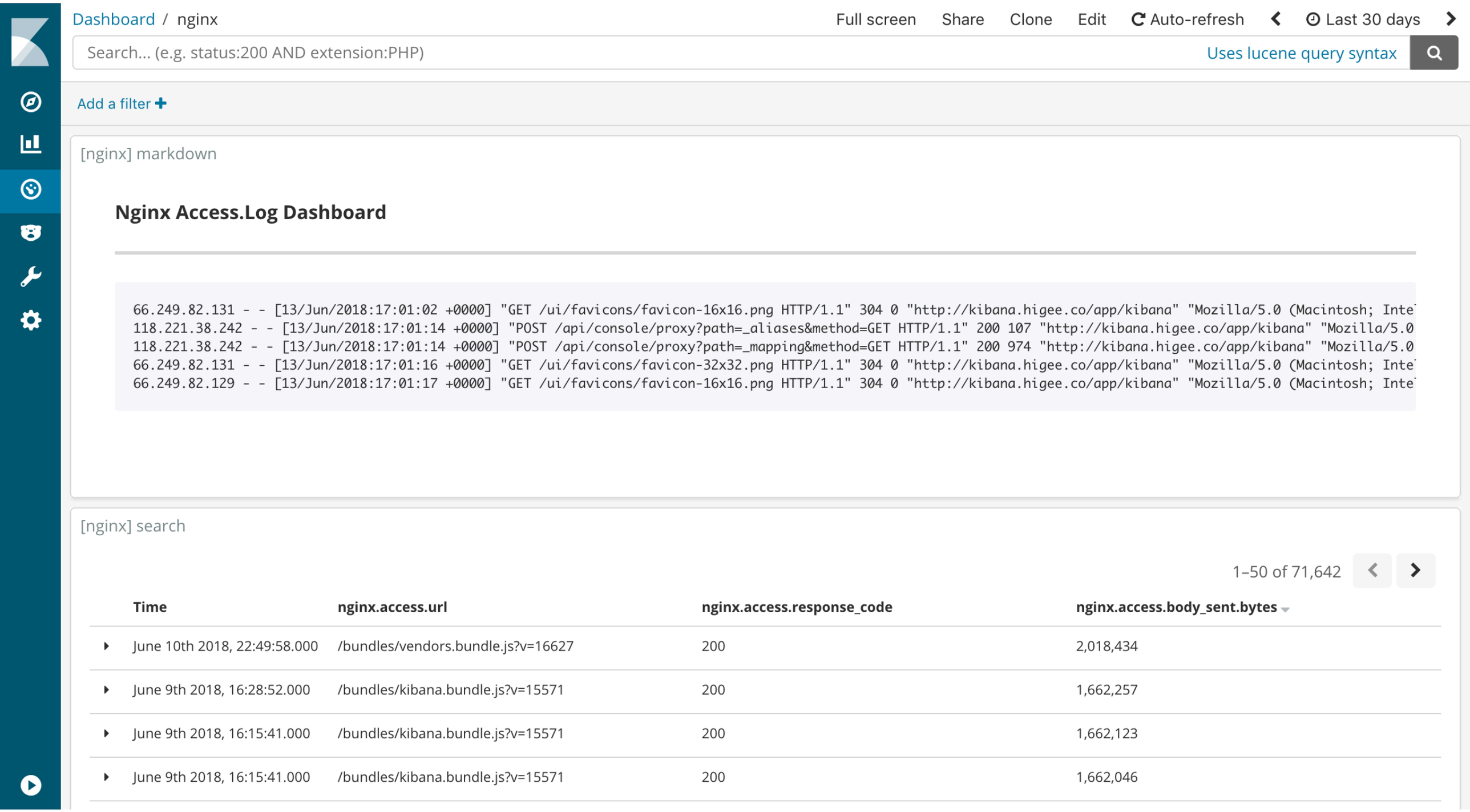
[week1 - exercise7] pie chart



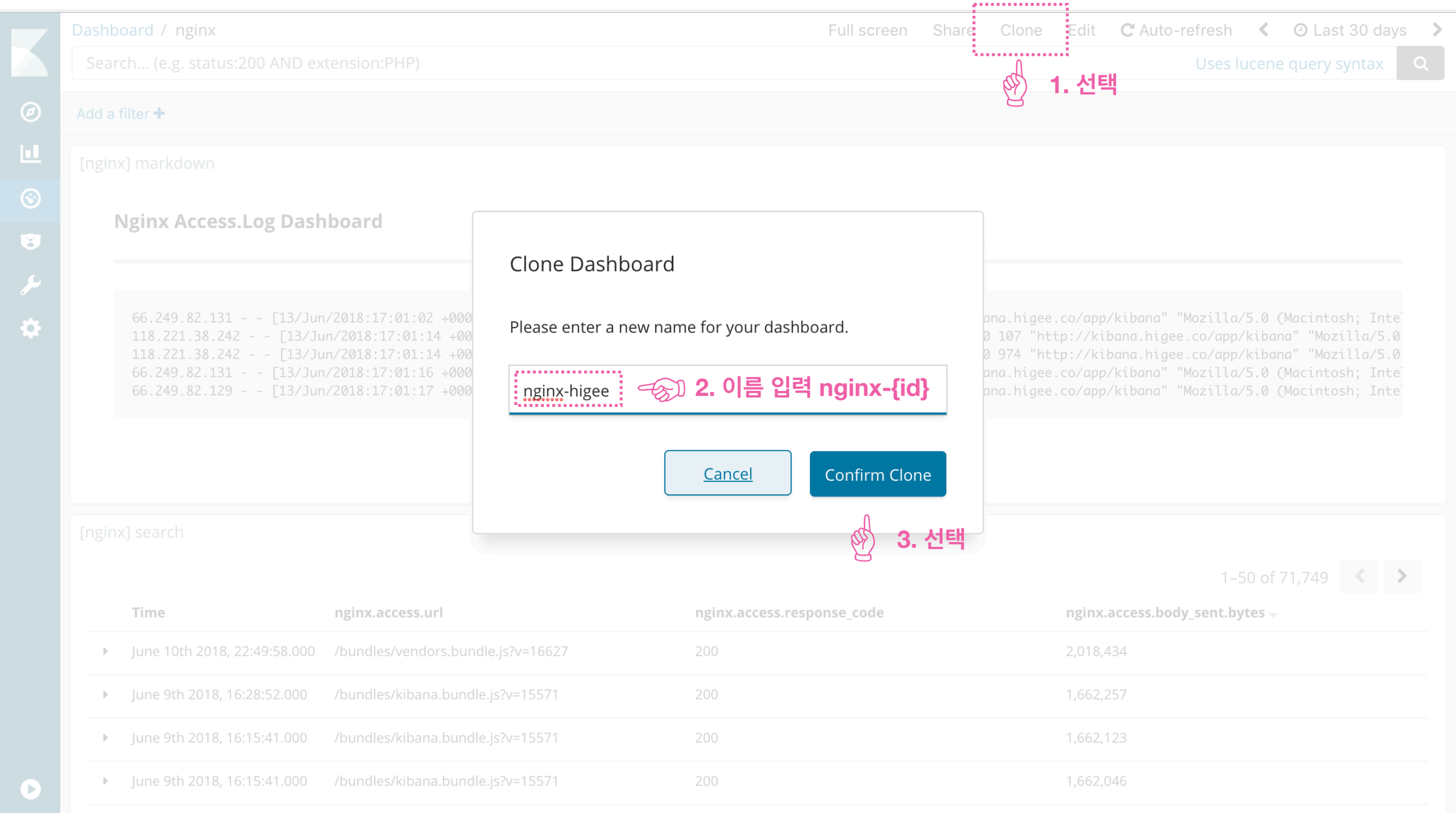
Dashboard를 조회하자



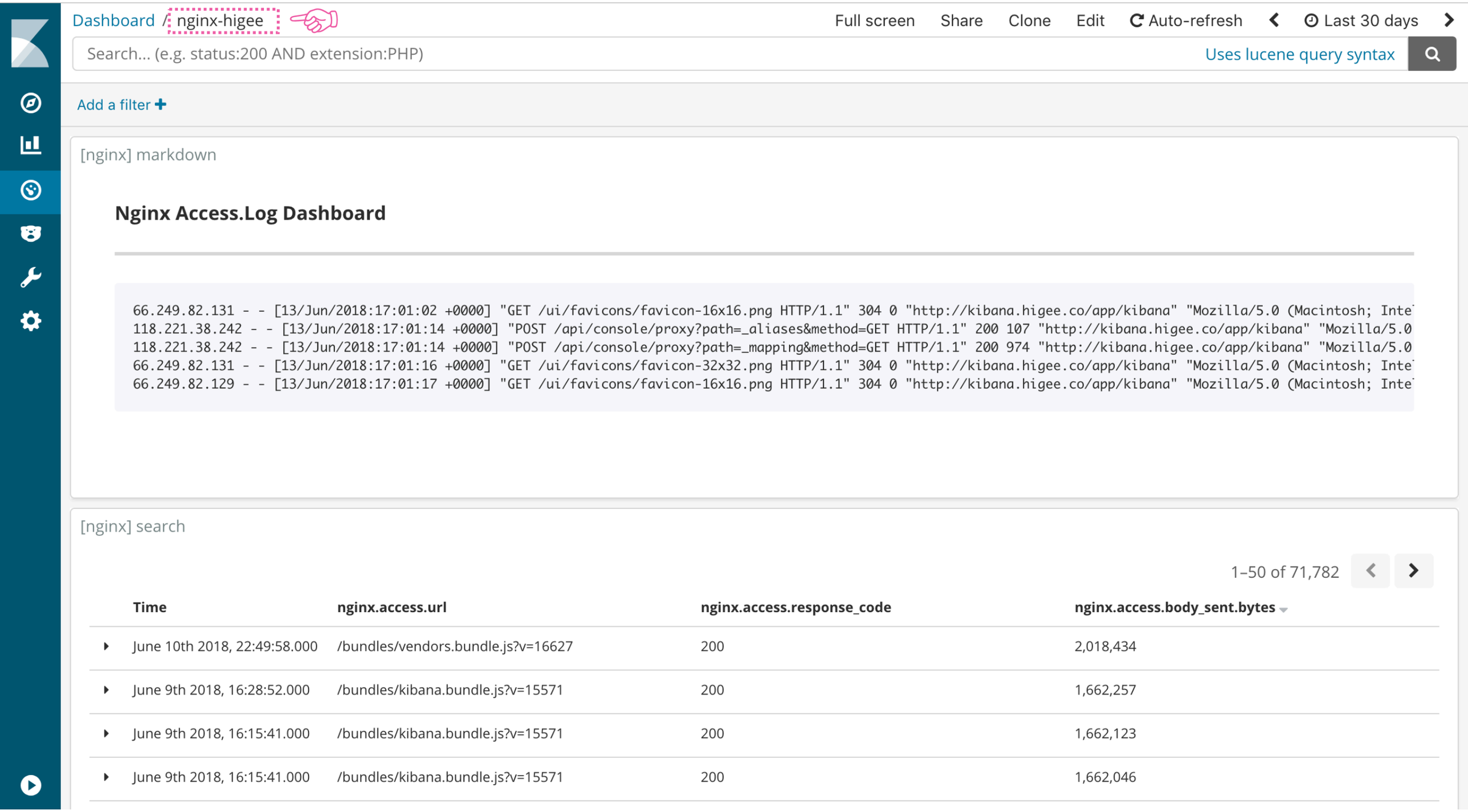
Dashboard를 조회하자



Dashboard를 clone하자

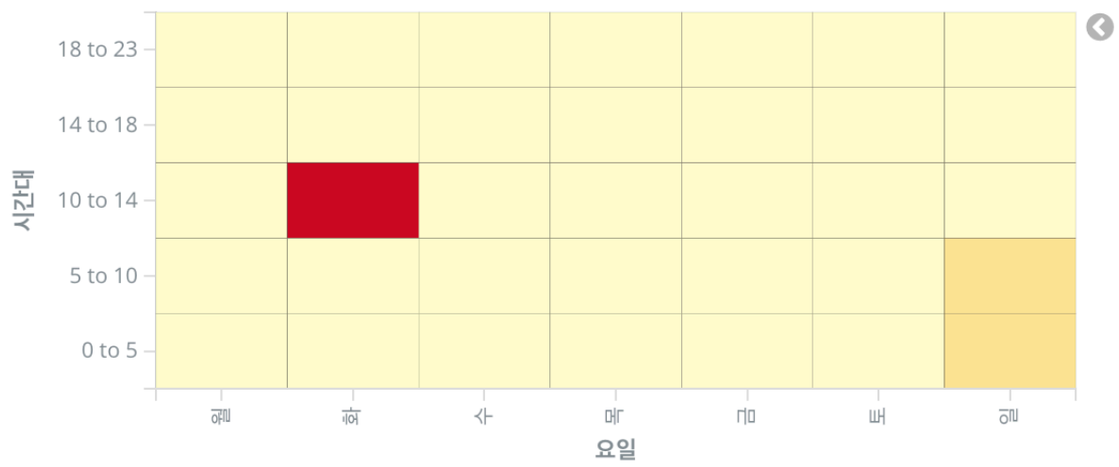


Clone 받은 환경에서 Dashboard를 사용할 수 있다



Dashboard가 Interactive하다!

[nginx] heat map

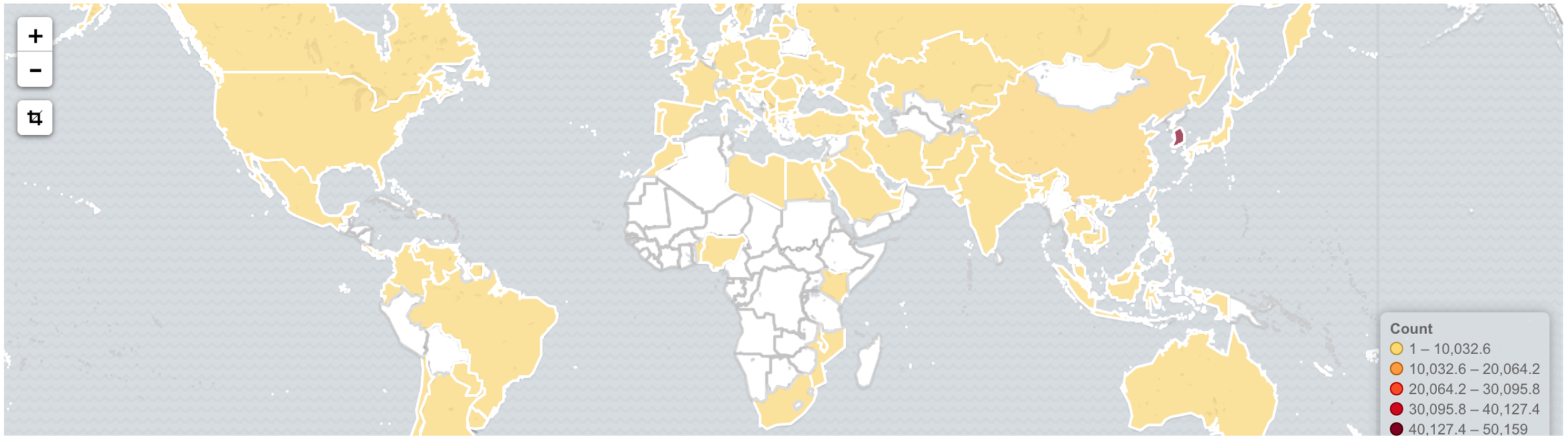


[nginx] tag-cloud

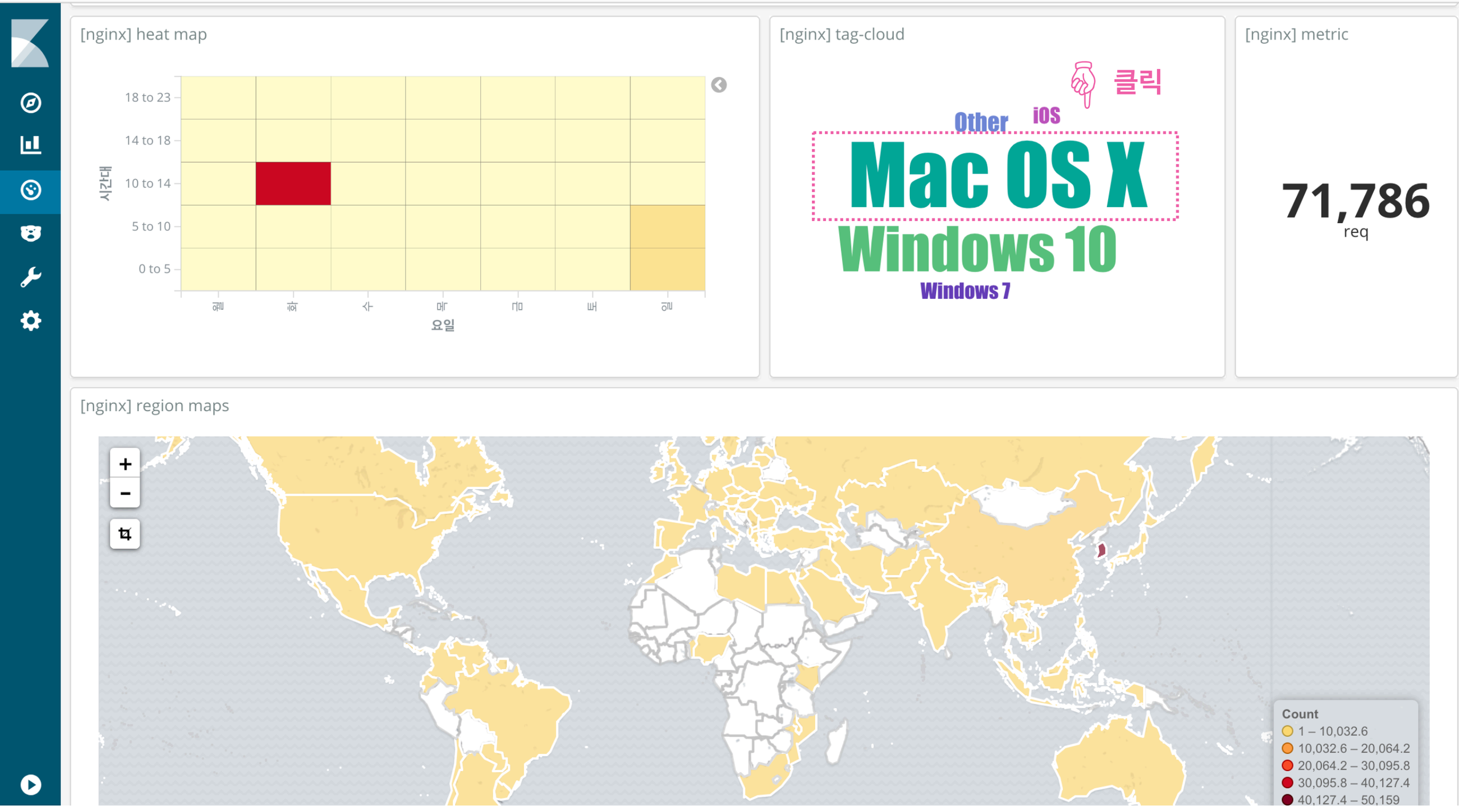
[nginx] metric

71,786
req

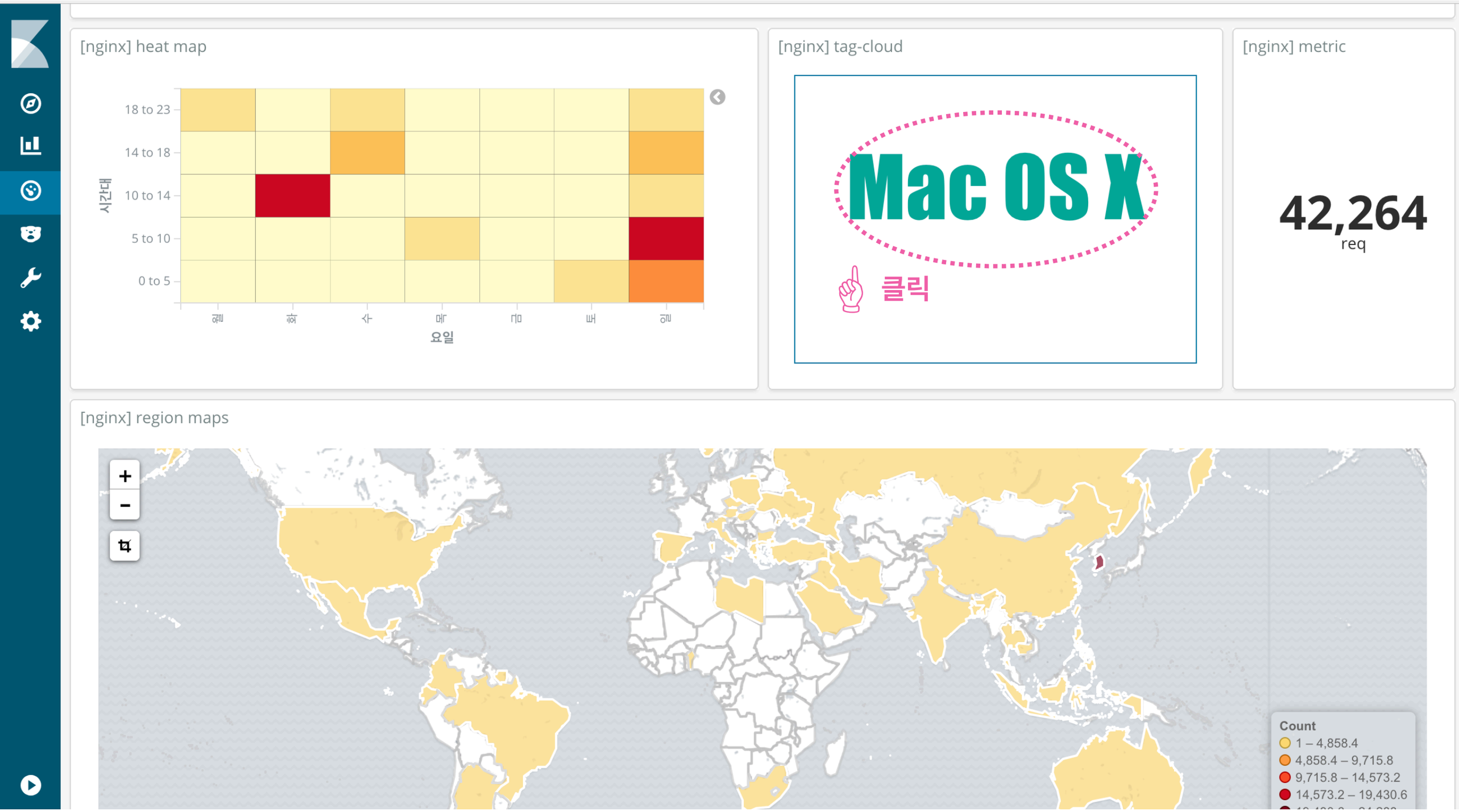
[nginx] region maps



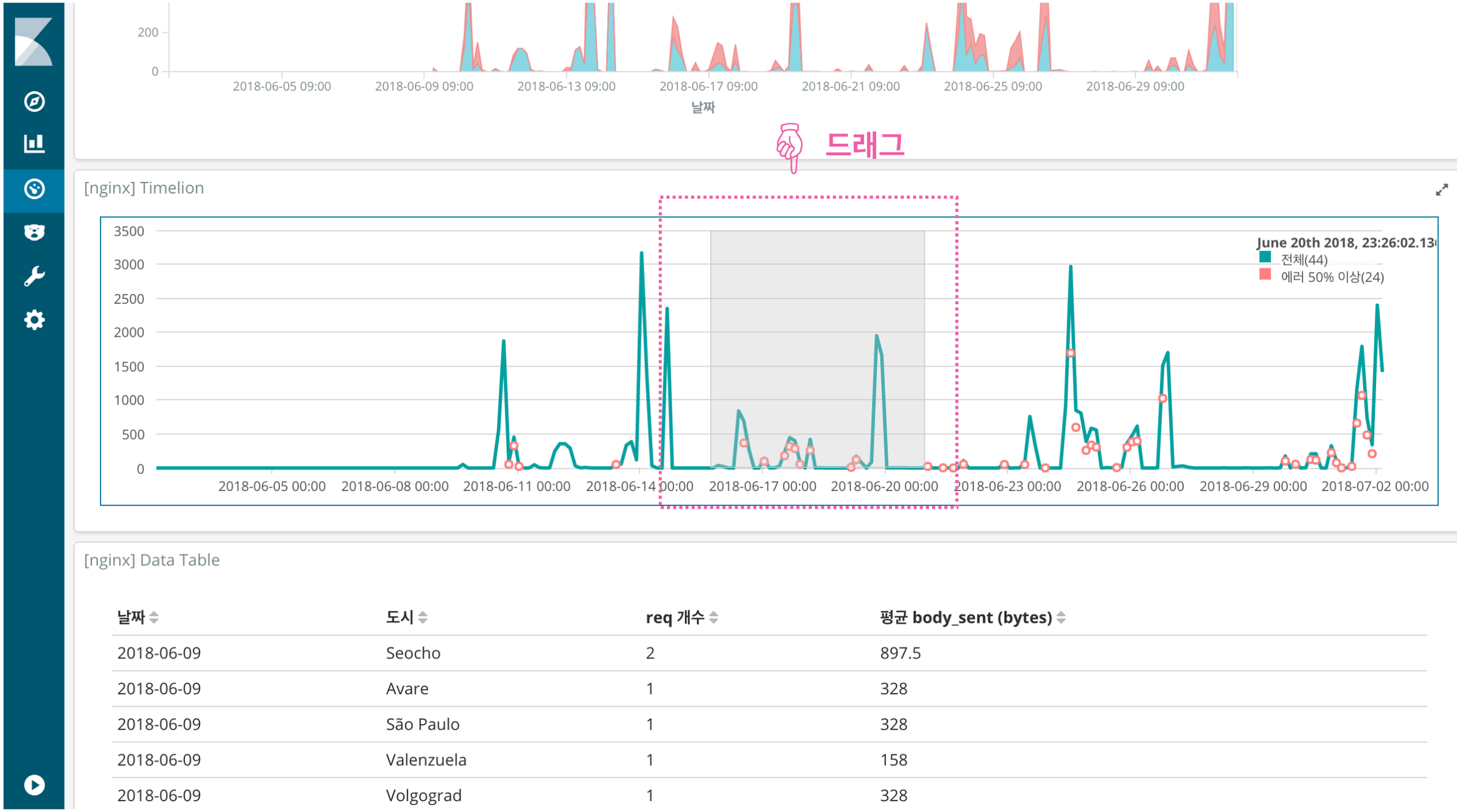
아래의 Dashboard에서 “Mac OS X”에 해당하는 데이터만 보고 싶다고 하자



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



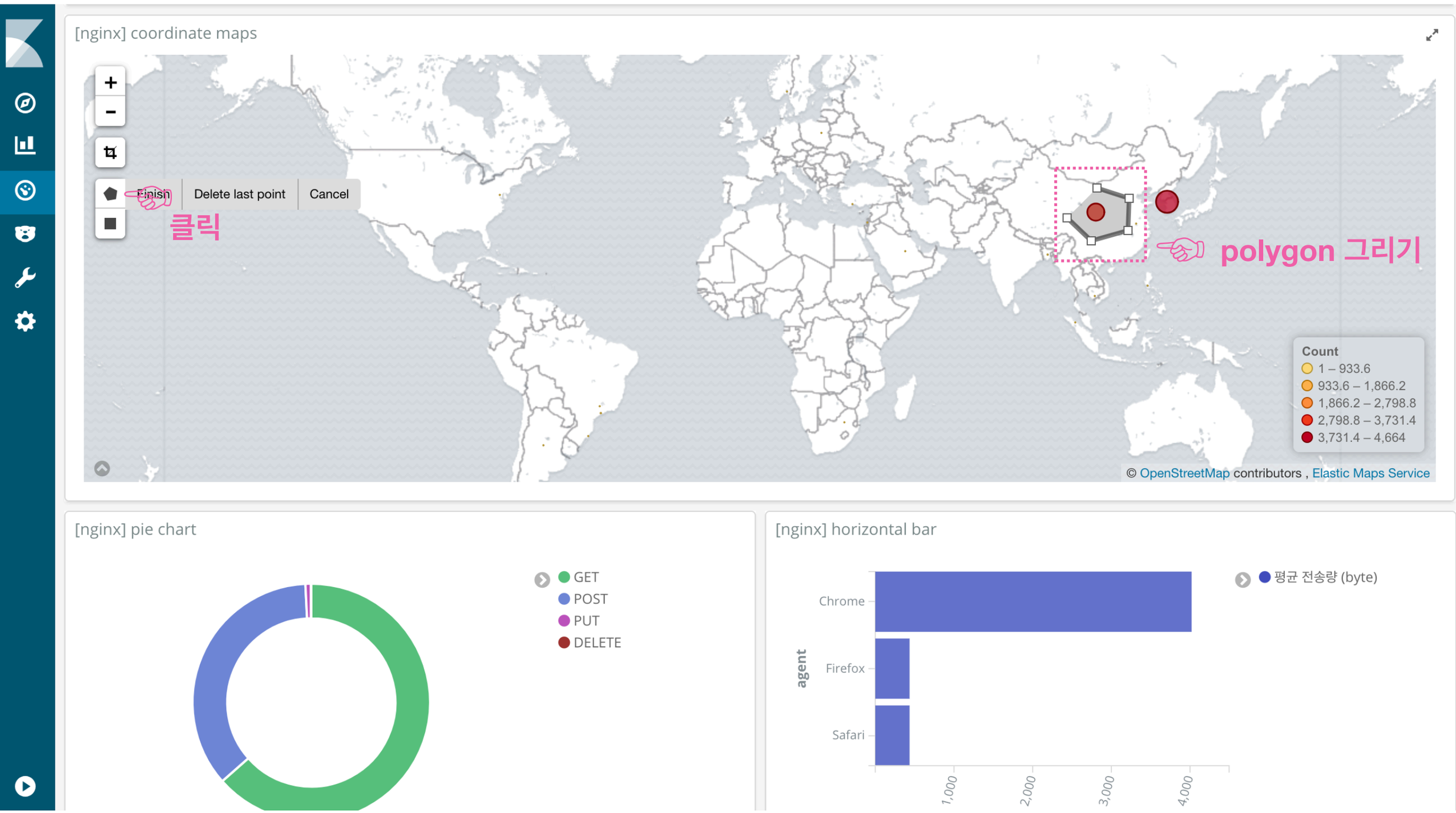
특정 기간을 집중해서 보고 싶으면 Drag를 하자



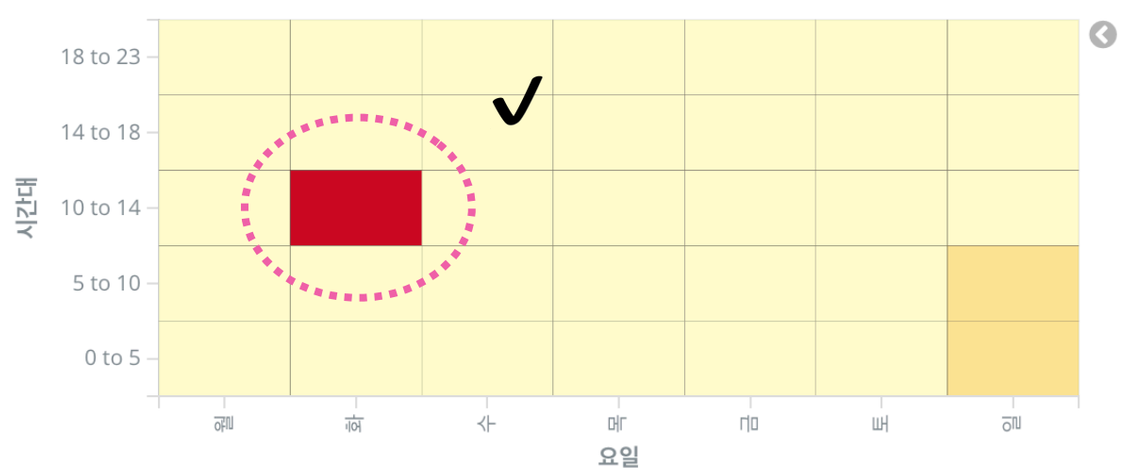
[nginx] Data Table

날짜	도시	req 개수	평균 body_sent (bytes)
2018-06-09	Seocho	2	897.5
2018-06-09	Avare	1	328
2018-06-09	São Paulo	1	328
2018-06-09	Valenzuela	1	158
2018-06-09	Volgograd	1	328

특정 지역의 데이터만 보고 싶으면 polygon/rectangle을 그리자

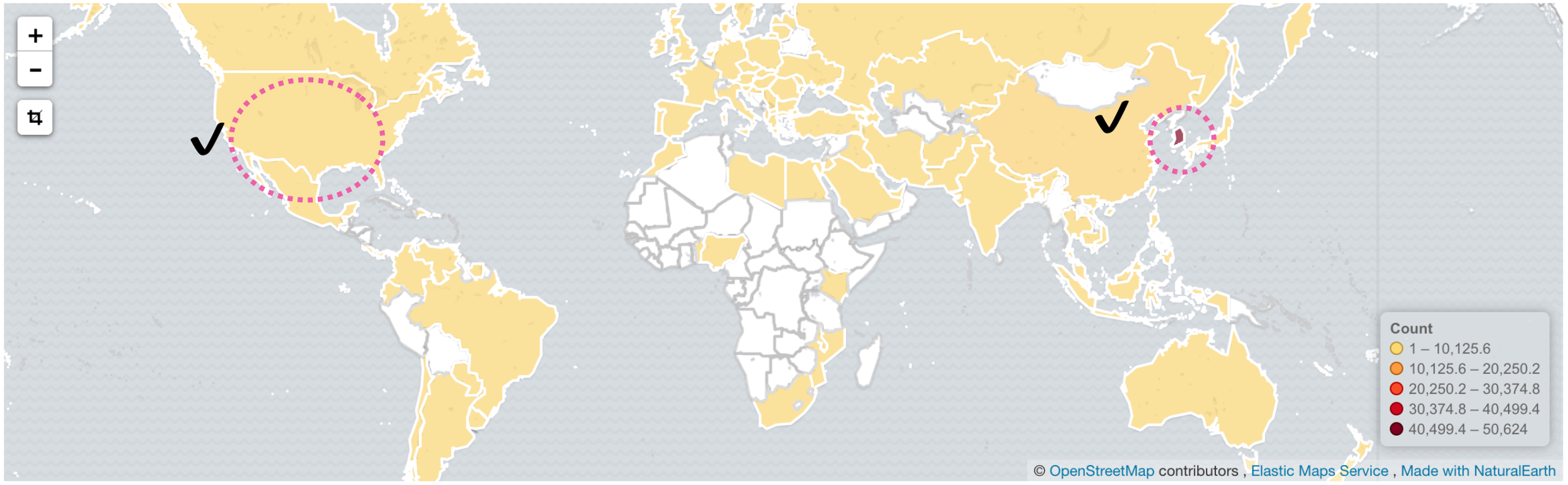


여러 visualization을 클릭하면서 Interactive한 Dashboard를 경험해보자



72,350
req

[nginx] region maps



Auto Refresh 기능을 이용하자

1. Auto-refresh 선택

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

Refresh Interval

Off	5 seconds	1 minute	1 hour
	10 seconds	5 minutes	2 hour
	30 seconds	15 minutes	12 hour
	45 seconds	30 minutes	1 day

2. Refresh 간격 설정

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

Add a filter +

설정한 간격 마다 Index 데이터를 확인하여
새로운 데이터가 있으면 Dashboard에 반영한다

[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; Inte
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
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
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; Inte
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; Inte
```

[nginx] search

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

dashboard를 공유하자

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

dashboard를 공유하자

1. Share 선택

Dashboard / nginx-higee

Full screen | Share | Clone | Edit | Auto-refresh | Last 30 days

Share saved dashboard

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

Embedded iframe Copy

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

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

Link Copy

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

Share Snapshot

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

Embedded iframe Short URL Copy

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

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

Link Short URL Copy

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

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

Search... (e.g. status:200 AND extension:PHP) **Saved Dashboard** ⟷ **Snapshot** Uses lucene query syntax

Add a filter +

[nginx] markdown

Nginx Access.Log Dashboard

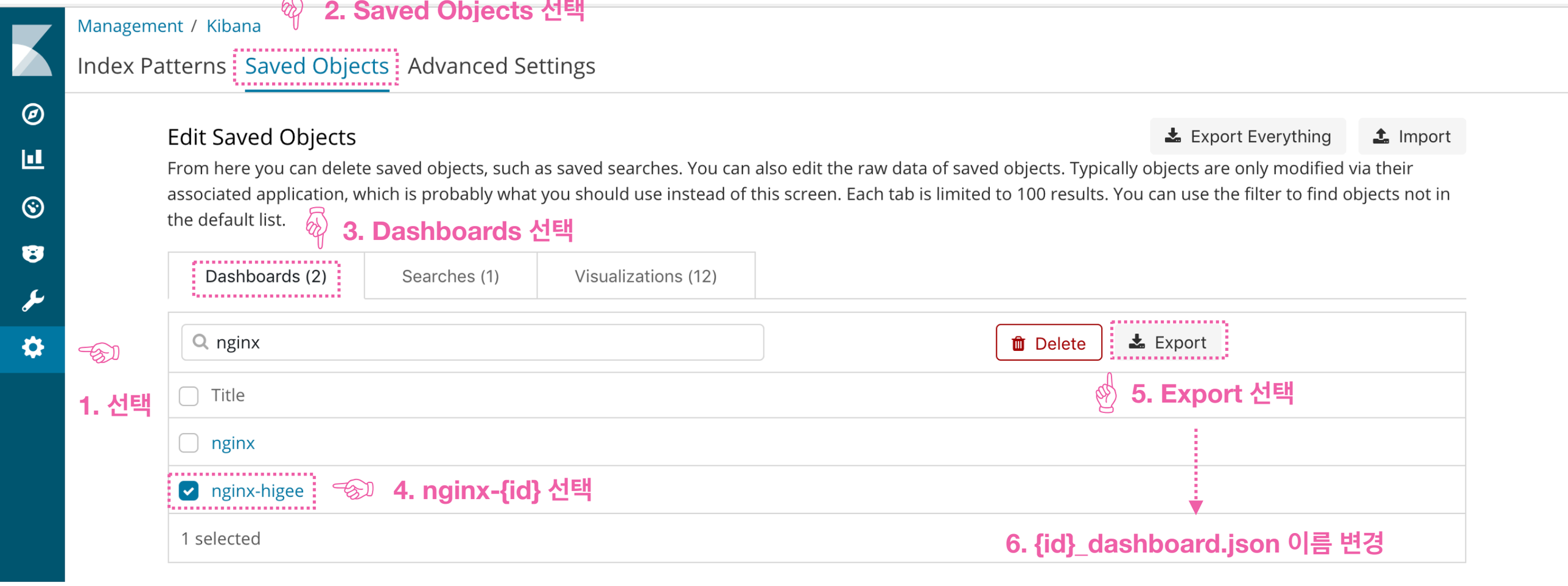
```
66.249.82.131 - - [13/Jun/2018:17:01:02 +0000] "GET /ui/favicons/favicon-16x16.png HTTP/1.1" 304 0 "http://kibana.higee.co/app/kibana" "Mozilla/5.0 (Macintosh; Inte
118.221.38.242 - - [13/Jun/2018:17:01:14 +0000] "POST /api/console/proxy?path=_aliases&method=GET HTTP/1.1" 200 107 "http://kibana.higee.co/app/kibana" "Mozilla/5.0
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
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; Inte
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; Inte
```

Dashboard/Visualization export

Dashboard 및 Visualize Object를 Import/Export 할 수 없나?

- ~~데이터 백업~~
- **UI** 백업

Dashboard export



Dashboard export

export.json


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

Dashboard export

대시보드를 export 하면 export.json으로 저장한 json 파일이 생기는데,

대시보드에 어떤 visualization이 어느 위치에 어떤 크기로 생성되었는지에 관한 정보를 담고 있다.

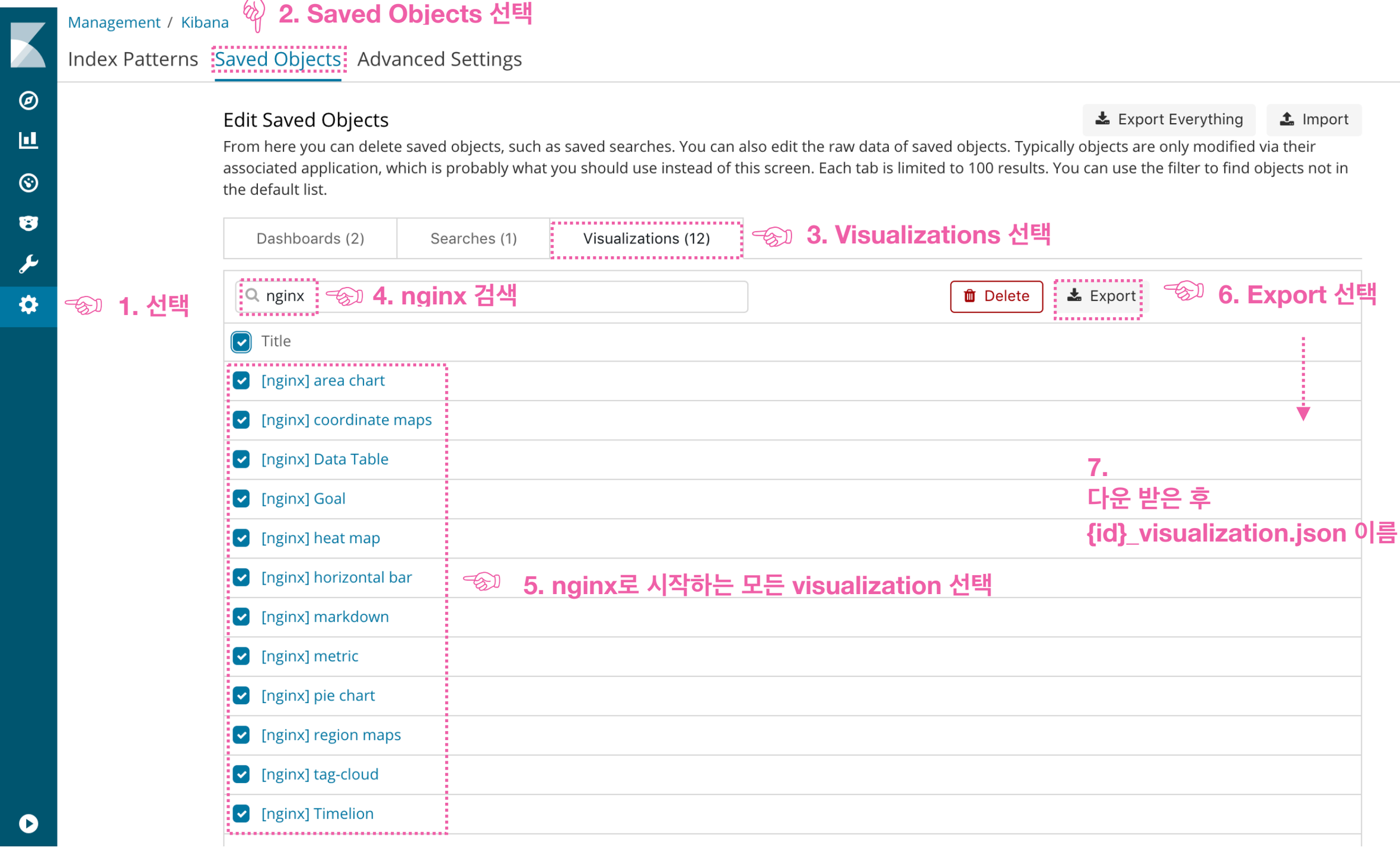
↓

개별 visualization 들이 어떤 aggregation으로 만들어졌는지 등에 관한 정보는 없다.

↓

Visualization 백업 필요!

Visualization export



Visualization export

export (1).json


```
[
  {
    "_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\":\"eb4d54b0-6fa9-11e8-8161-3b4280559eb3\",\"filter\":[],\"query\":{\"query\":\"\",\"language\":\"lucene\"}}"
      }
    }
  },
  {
    "_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,\"heat
      "uiStateJSON": "{}",
      "description": "",
      "version": 1,
      "kibanaSavedObjectMeta": {
        "searchSourceJSON": "{\"index\":\"eb4d54b0-6fa9-11e8-8161-3b4280559eb3\",\"filter\":[],\"query\":{\"query\":\"\",\"language\":\"lucene\"}}"
      }
    }
  },
  {
    "_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\":\"eb4d54b0-6fa9-11e8-8161-3b4280559eb3\",\"filter\":[],\"query\":{\"query\":\"\",\"language\":\"lucene\"}}"
      }
    }
  },
  {
    "_id": "25a7f140-6f20-11e8-a0fb-51f0eb991705",
    "_type": "visualization",
    "_source": {
      "title": "[nginx] tag-cloud",
      "visState": "{\"title\":\"[nginx] tag-cloud\",\"type\":\"tagcloud\",\"params\":{\"scale\":\"linear\",\"orientation\":\"single\",\"minFontSize\":18,\"maxFontSize\":72},\"aggs
      "uiStateJSON": "{}",
      "description": "",
      "version": 1,
      "kibanaSavedObjectMeta": {
        "searchSourceJSON": "{\"index\":\"eb4d54b0-6fa9-11e8-8161-3b4280559eb3\",\"filter\":[],\"query\":{\"query\":\"\",\"language\":\"lucene\"}}"
      }
    }
  },
```

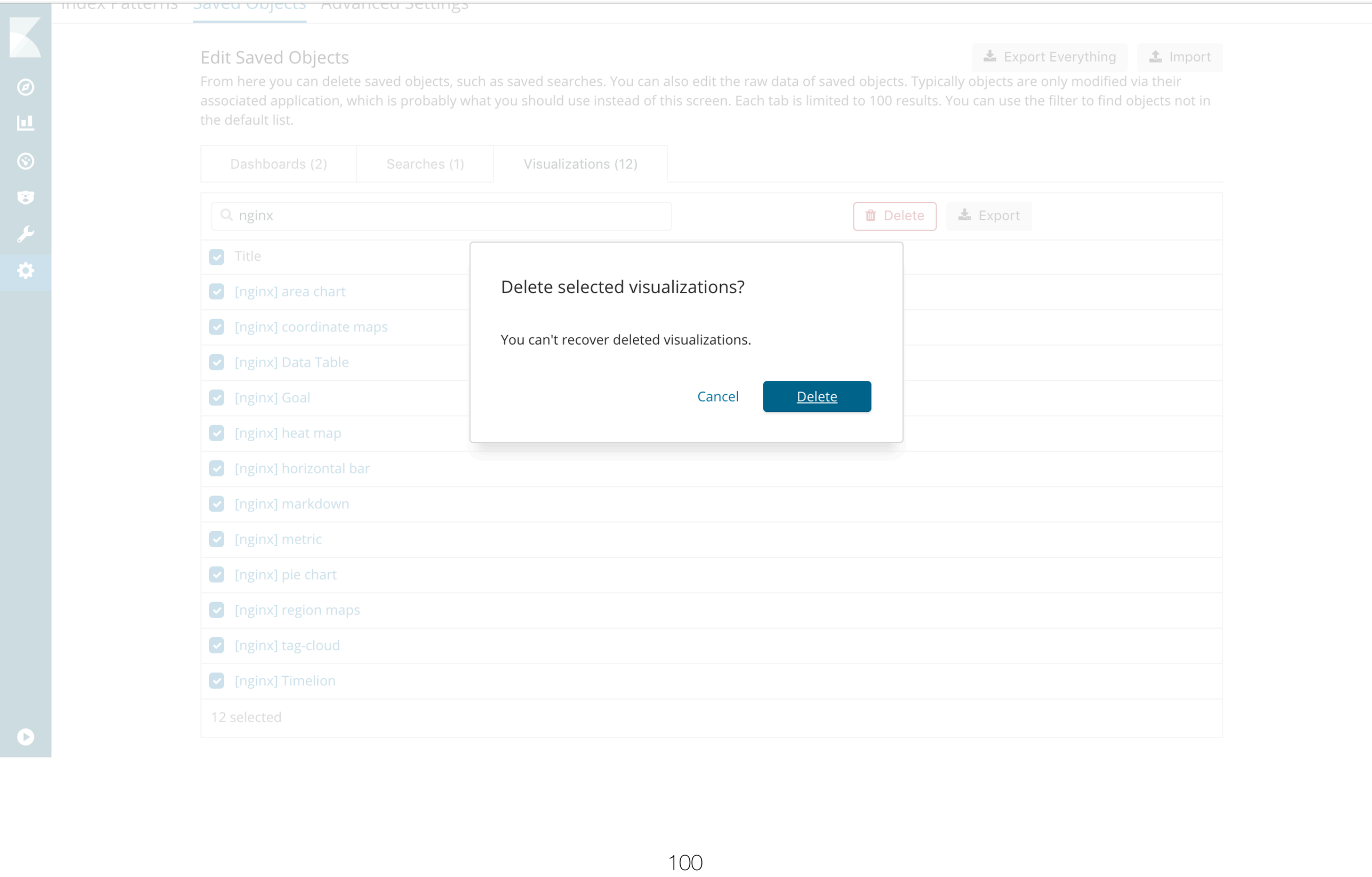
Visualization export

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

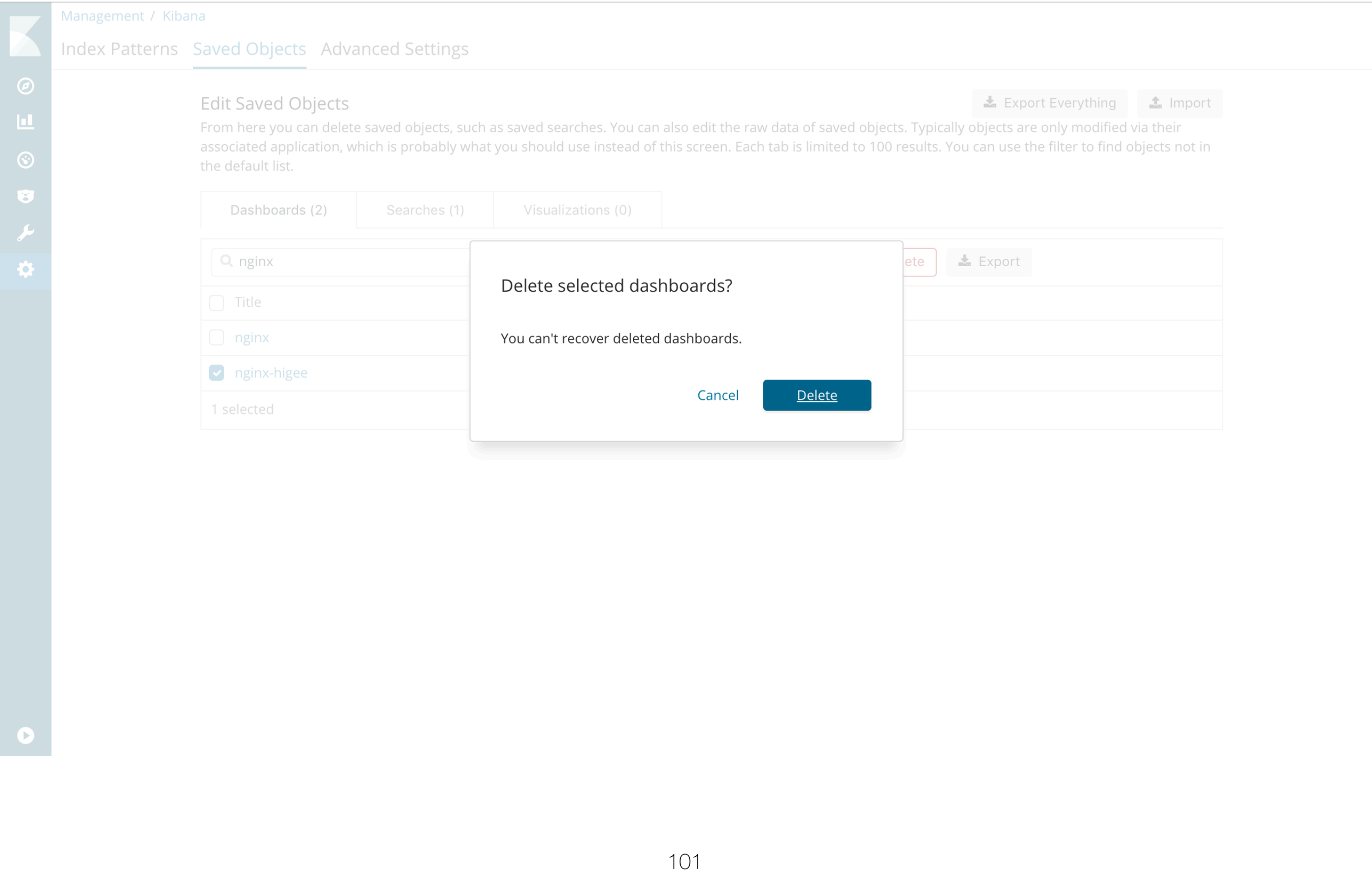
즉, dashboard UI를 온전히 백업 받으려면 dashboard와 visualization을 모두 백업 받아야 한다

Dashboard/Visualization import

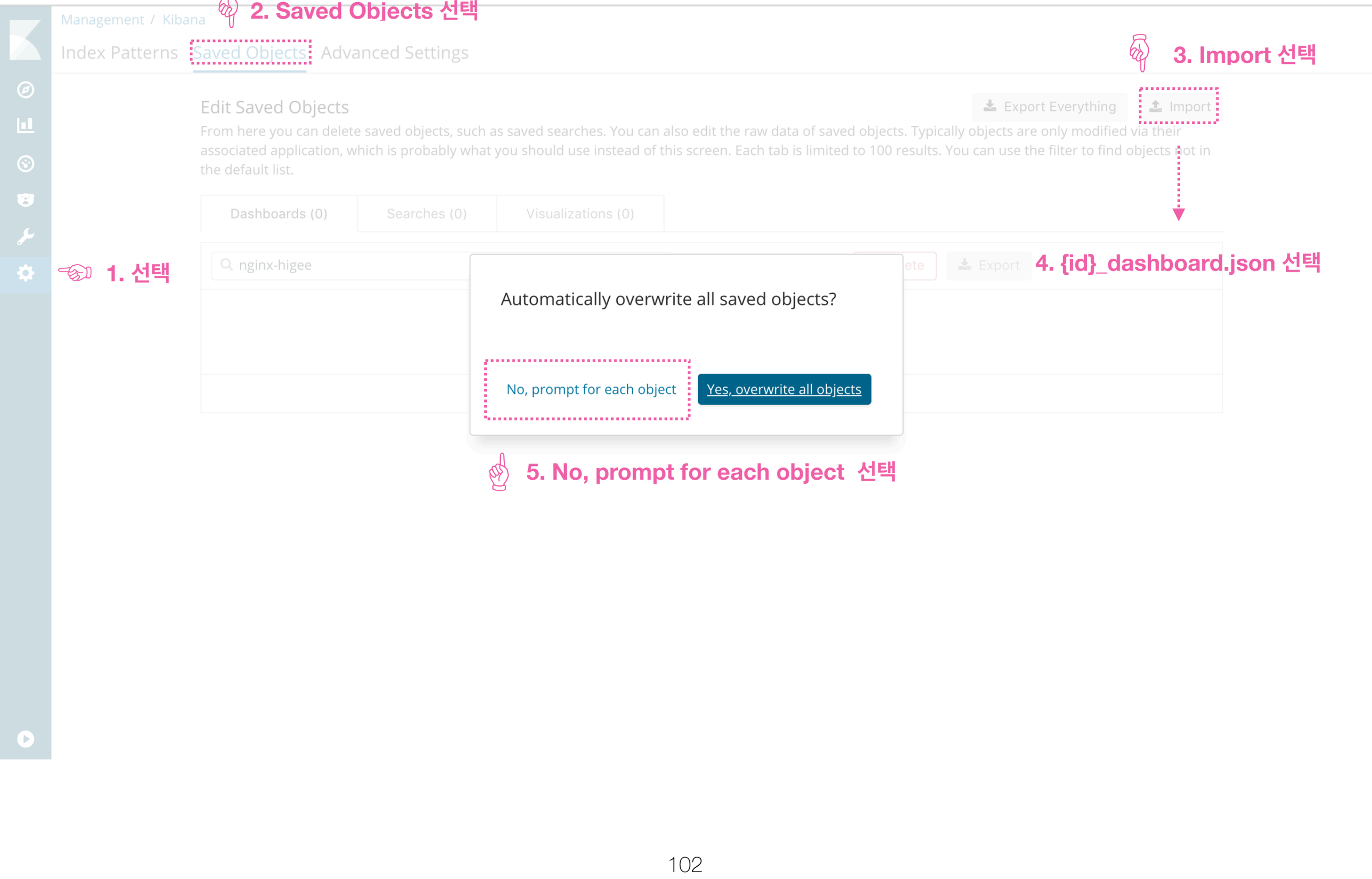
visualization 삭제



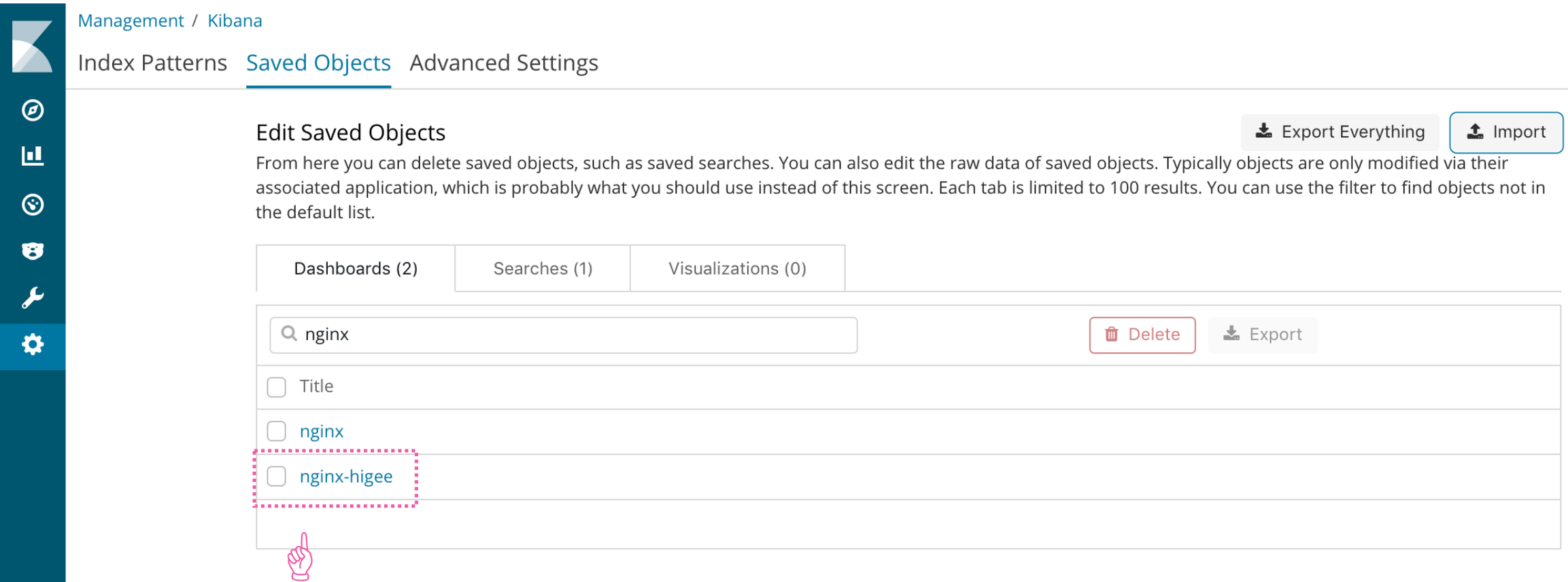
dashboard 삭제



Dashboard import

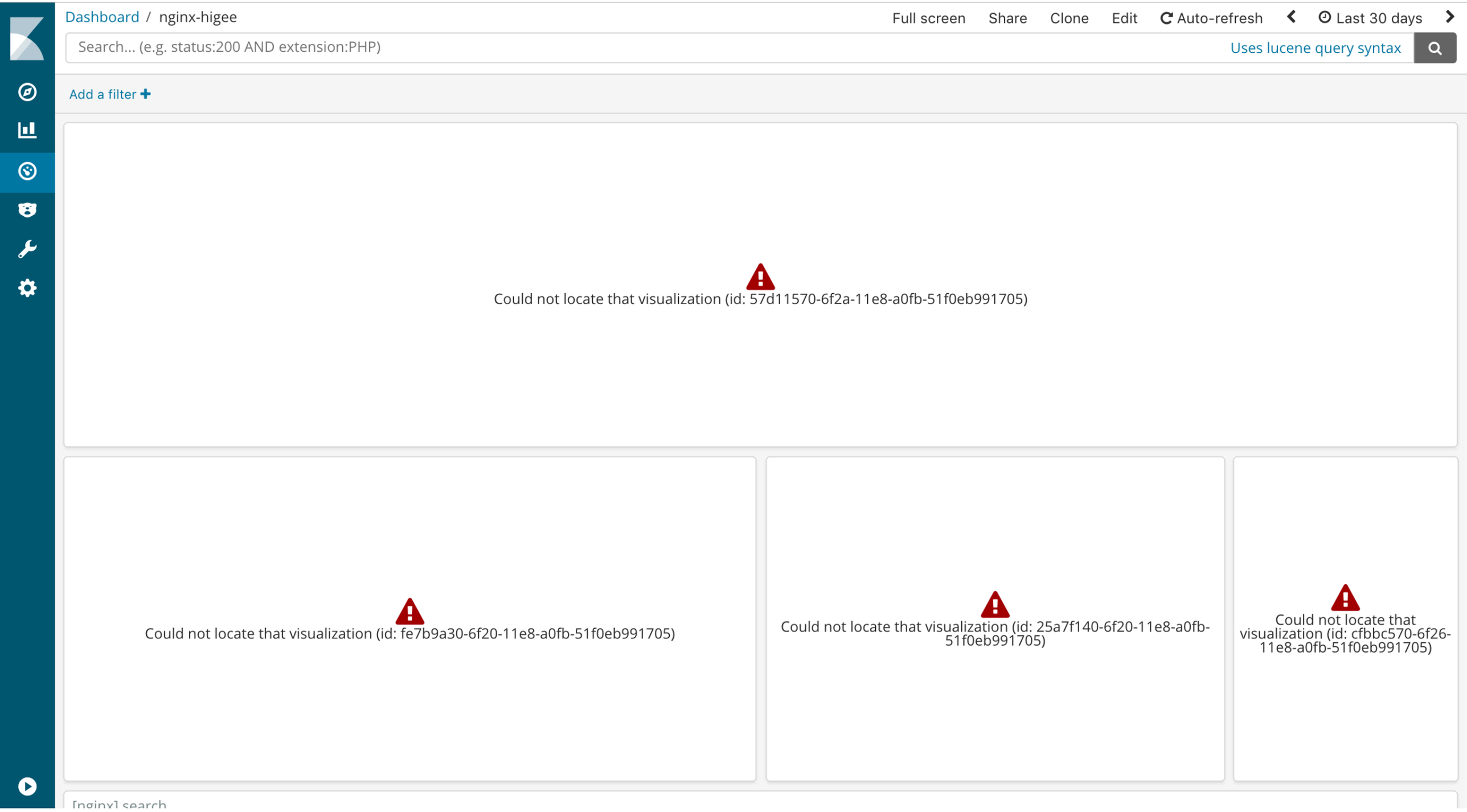


Dashboard import

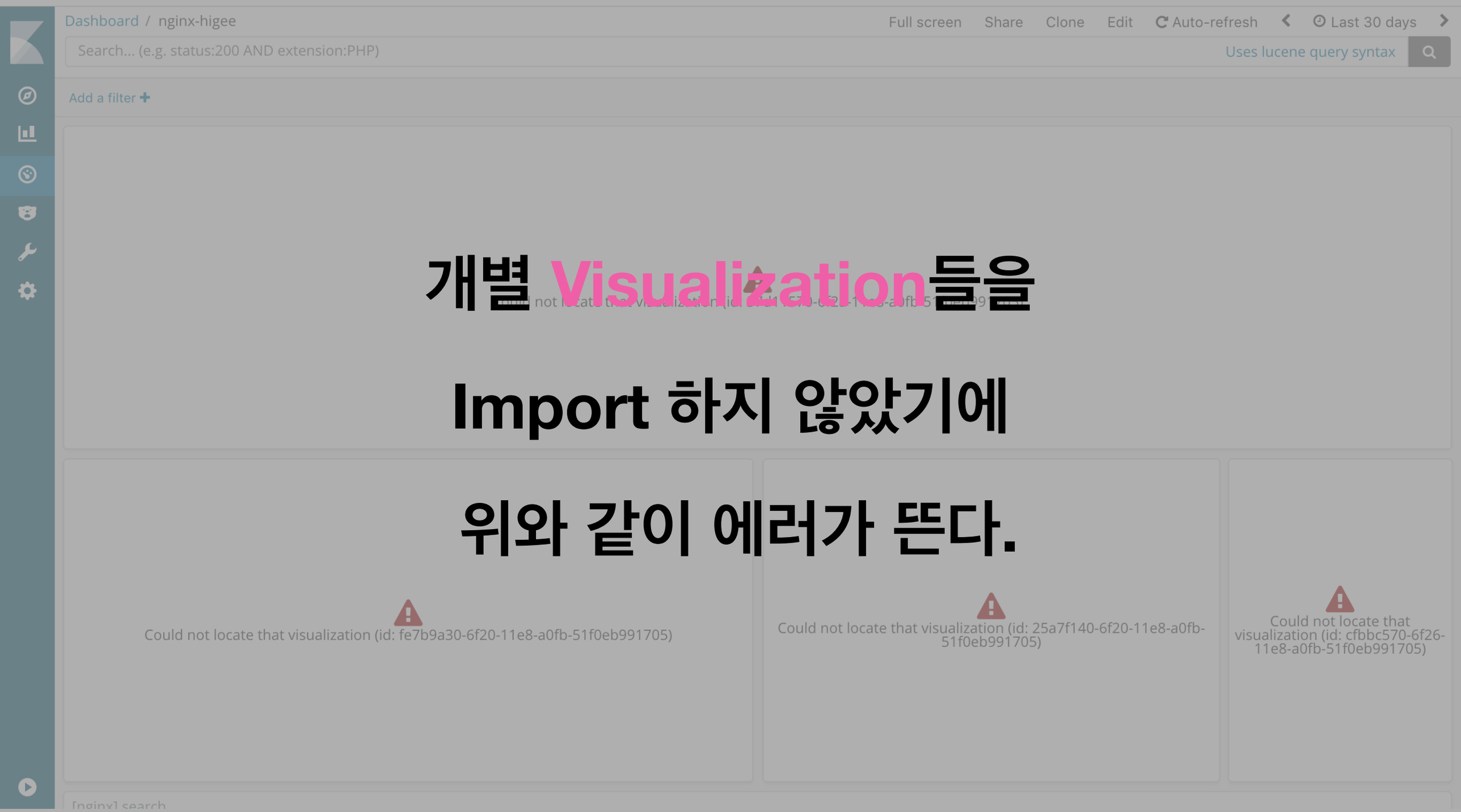


한 번 지웠던 nginx-higee가 제대로 Import 된 걸 확인할 수 있다

Import한 Dashboard에 가보면



Import한 Dashboard에 가보면

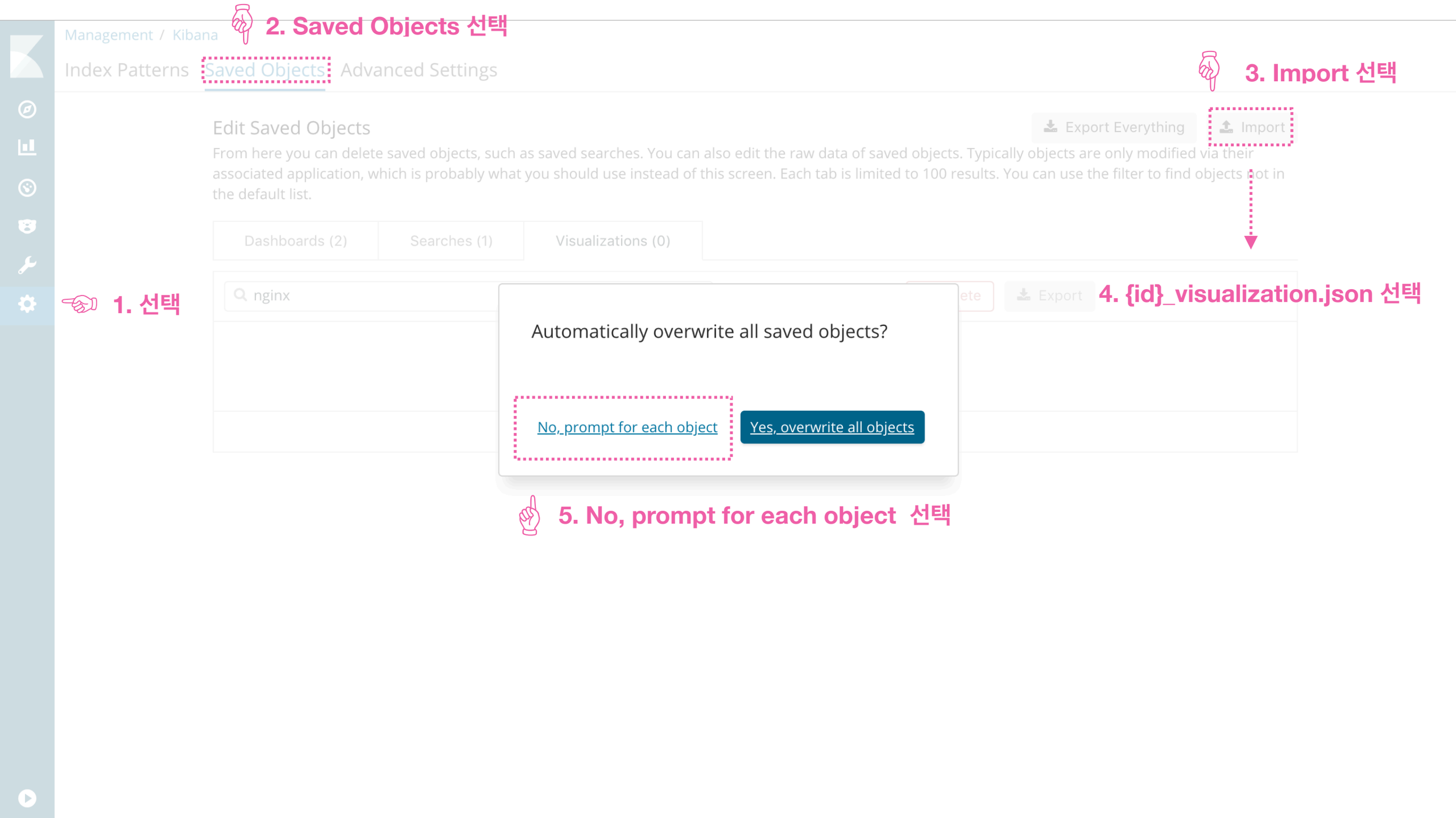


개별 Visualization들을

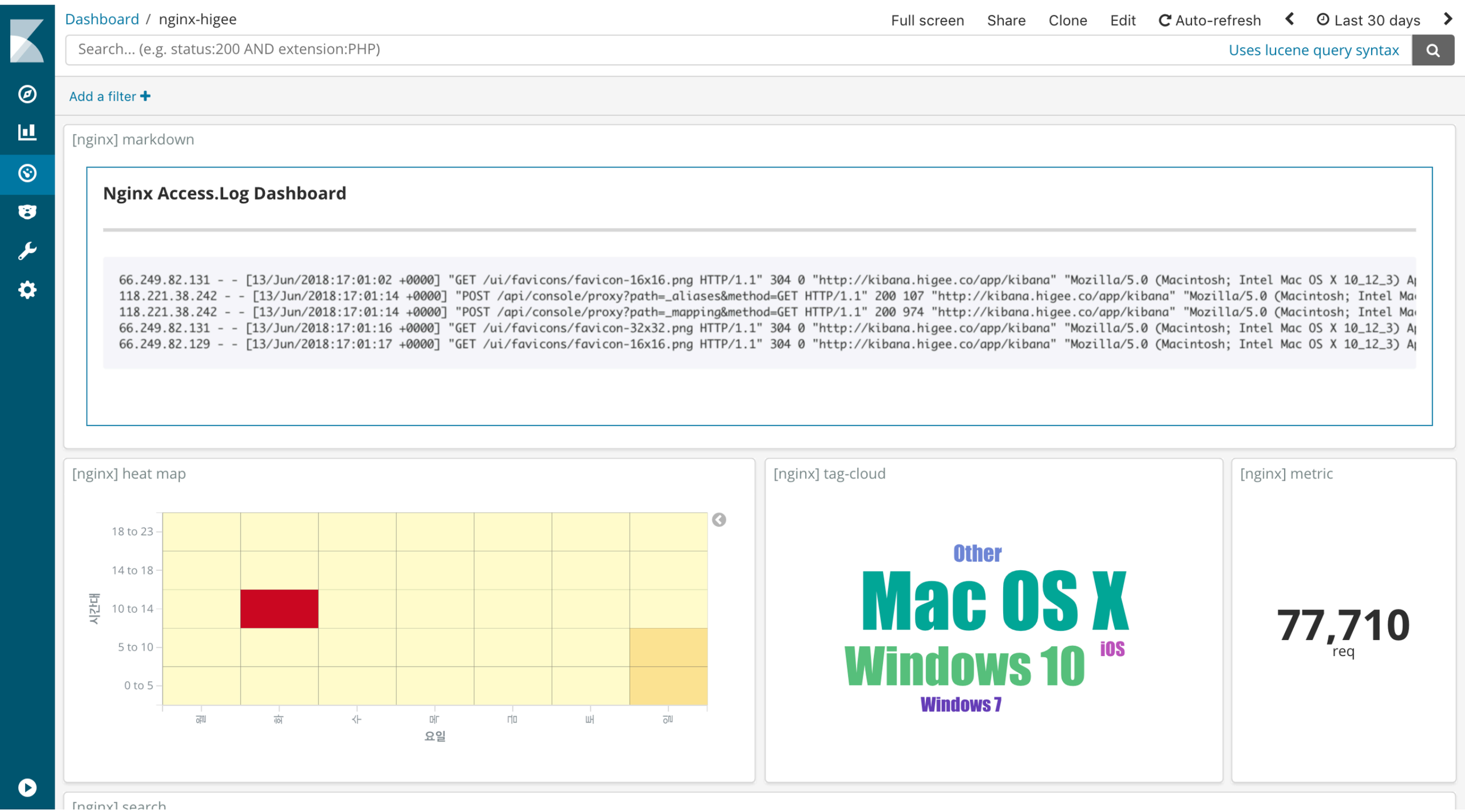
Import 하지 않았기에

위와 같이 에러가 뜬다.

Visualization import



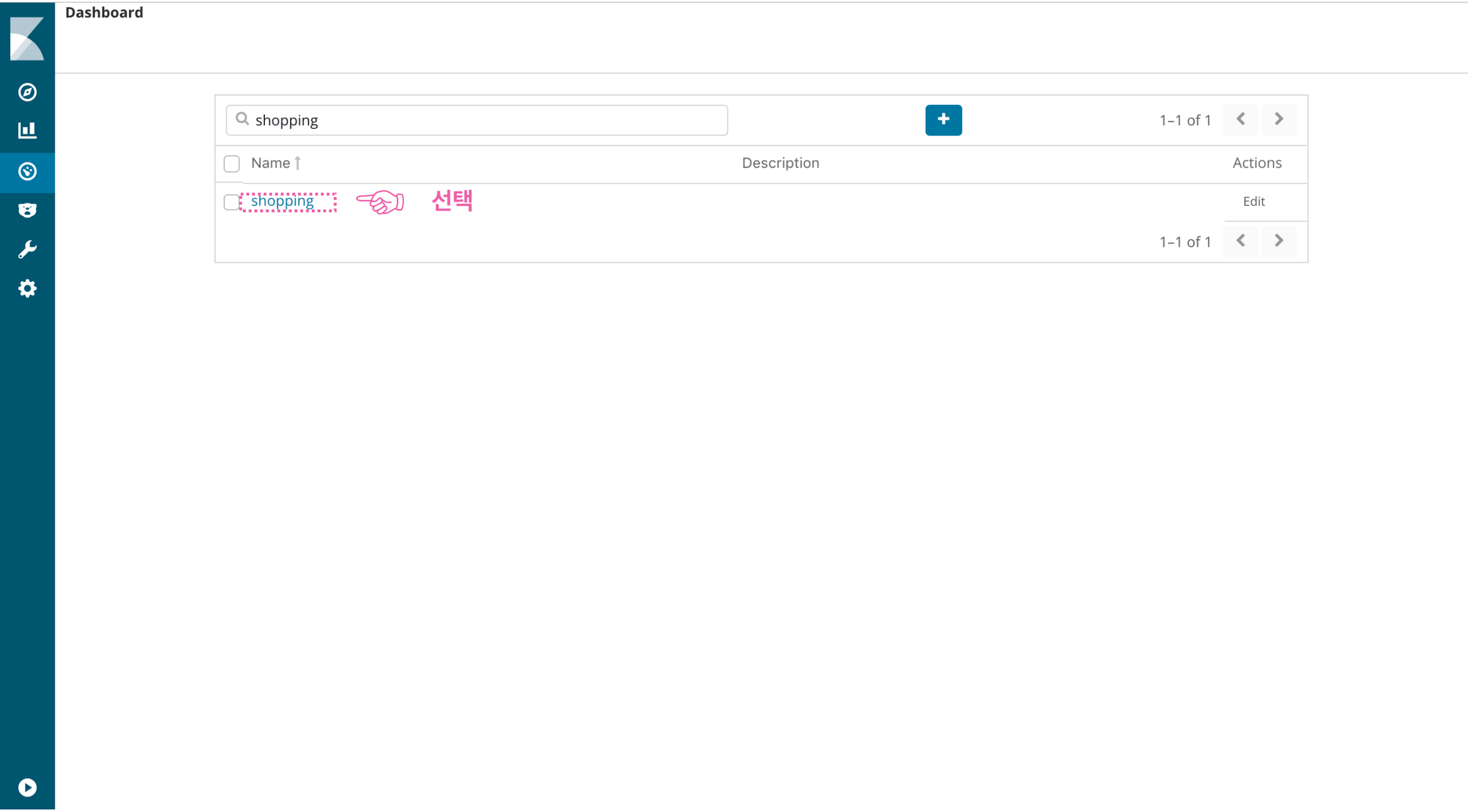
Import한 Dashboard에 다시 가보면



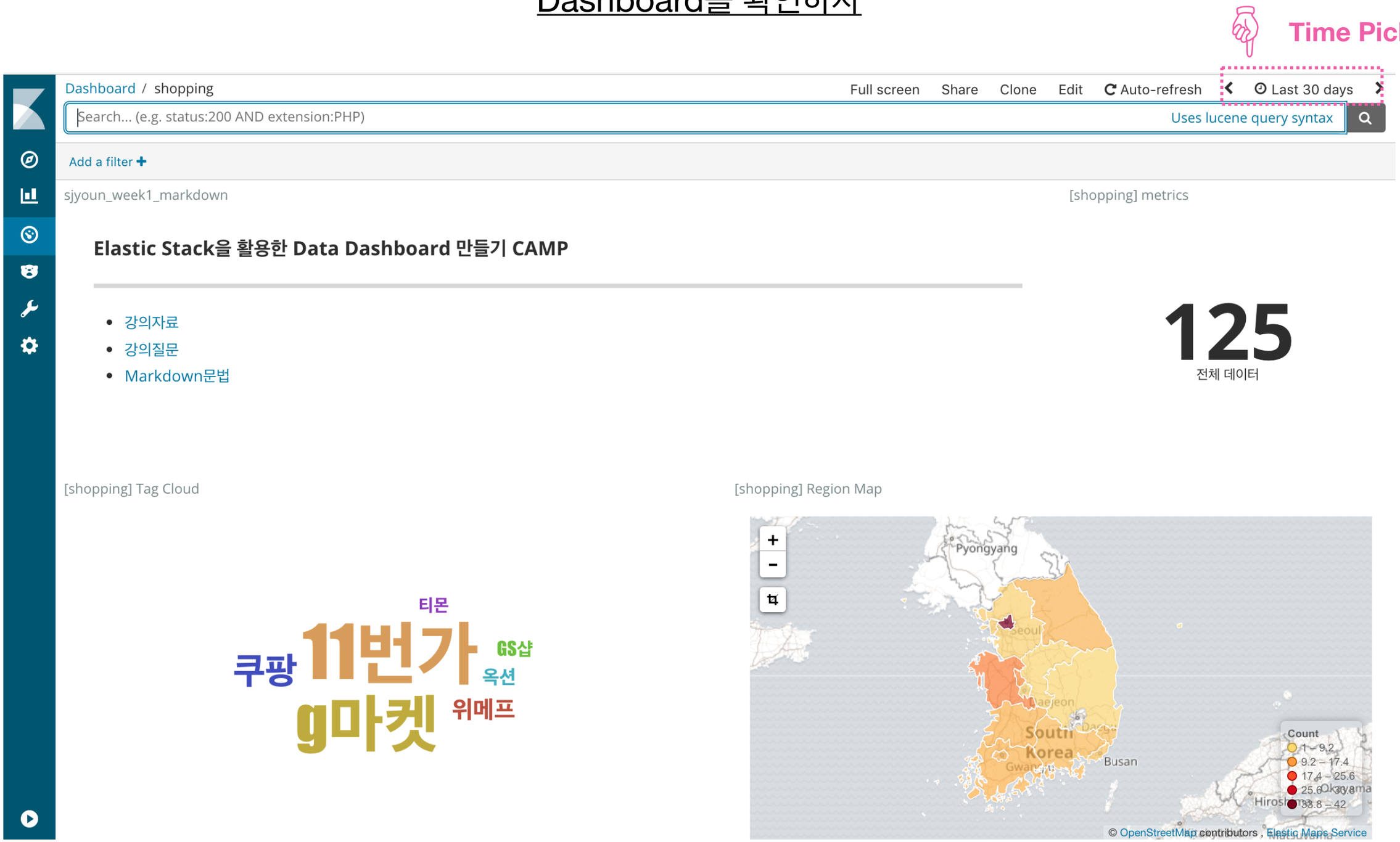
Filtering by Field ♕

Dashboard를 만들었는데 원하는 조건의 데이터만 보고 싶다면?

Dashboard 선택



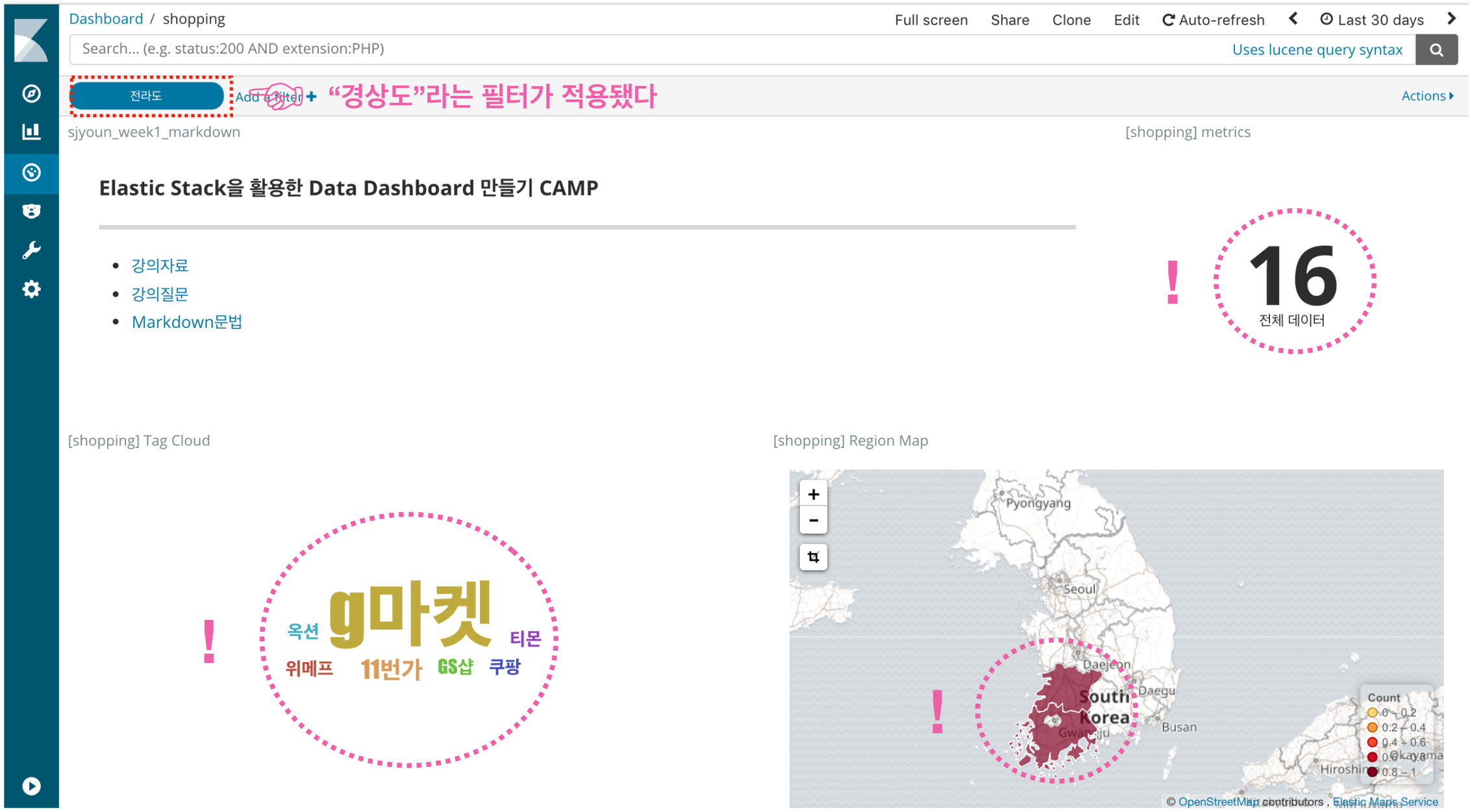
Dashboard를 확인하자



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

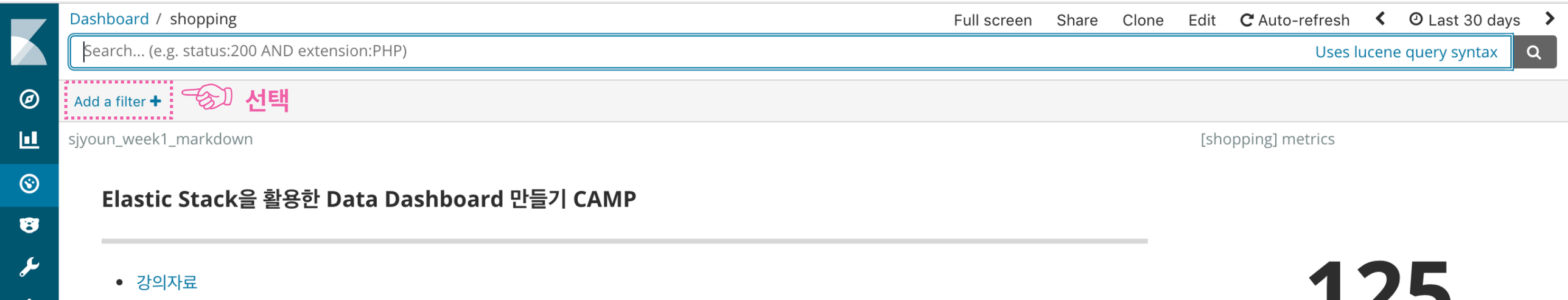


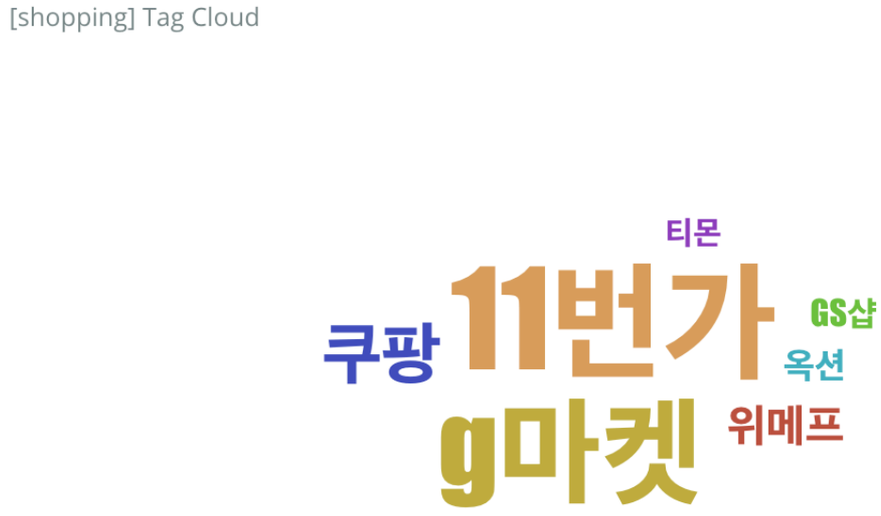
Filter를 이용하면 **특정 조건을 만족**하는

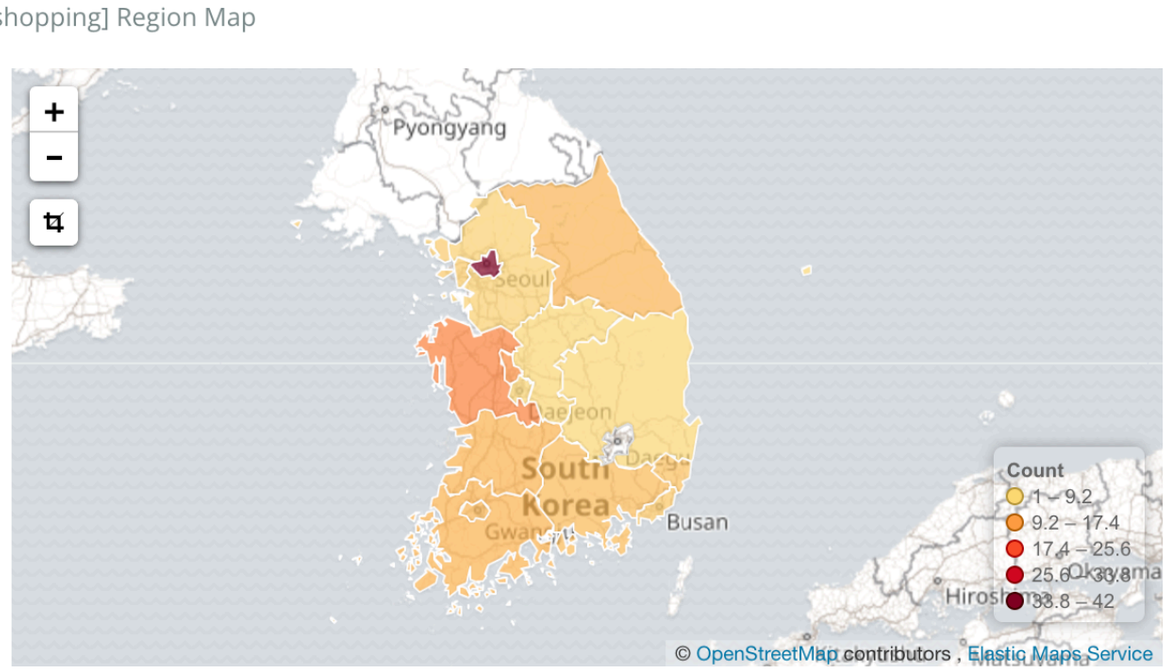
데이터만 선별하여 Dashboard에 시각화할 수 있다.

그렇다면 어떻게 사용할까?

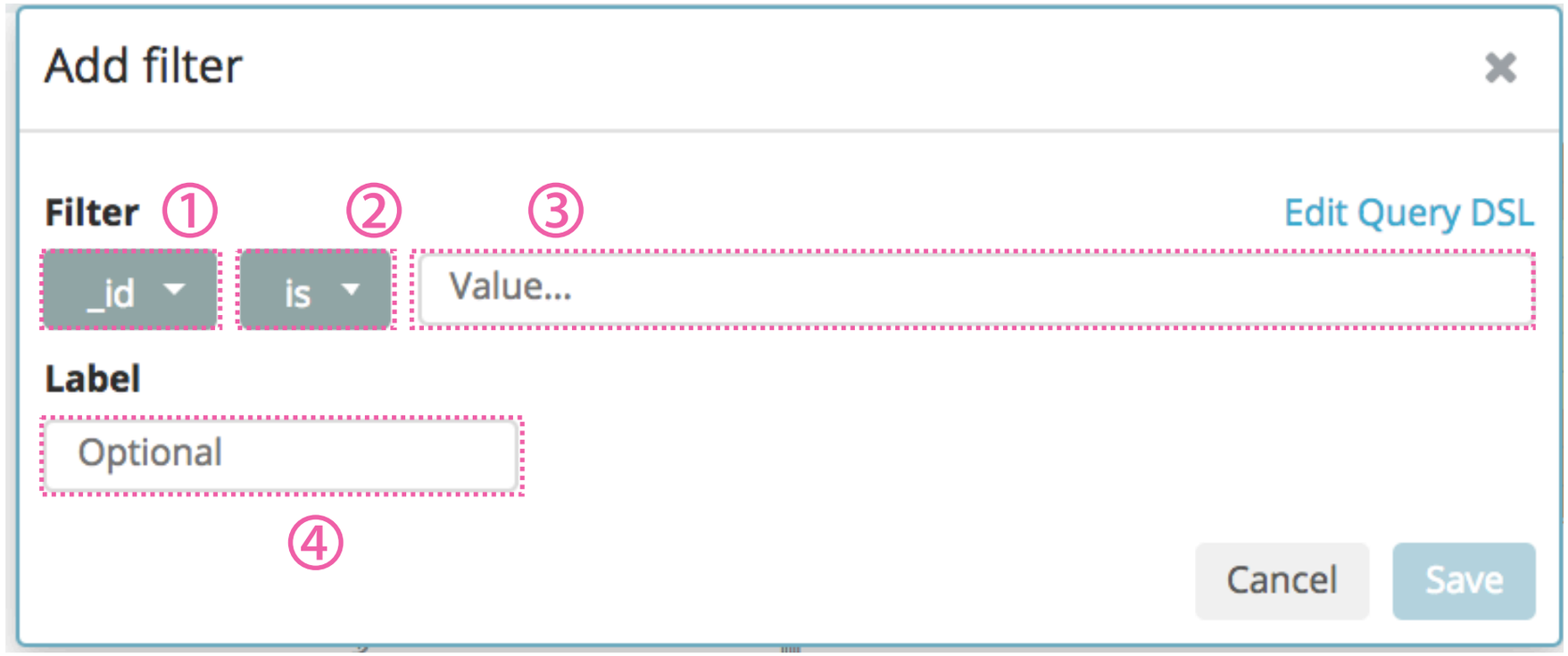
Filter를 실행하자







Filter의 사용법을 익히자



① Filter 적용할 Field 선택

② 적용할 Operator 선택 (다음 페이지 참조)

③ Filter에 적용하려는 Value 입력

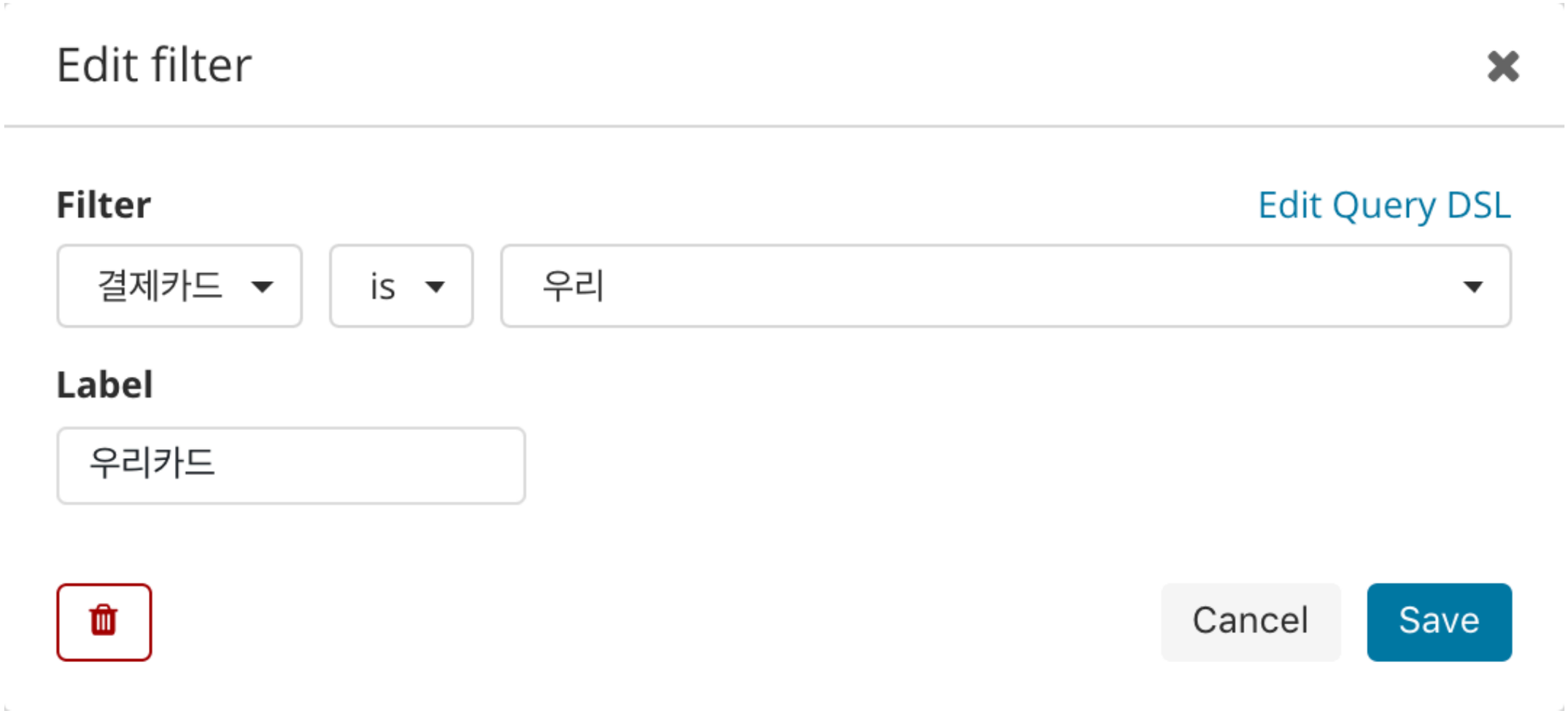
④ (여러 Filter 구분하기 위한) 이름 입력

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

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

우리카드 Add a filter + Actions

sjyoun_week1_markdown

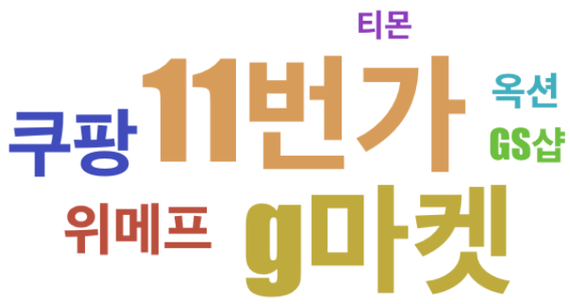
[shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

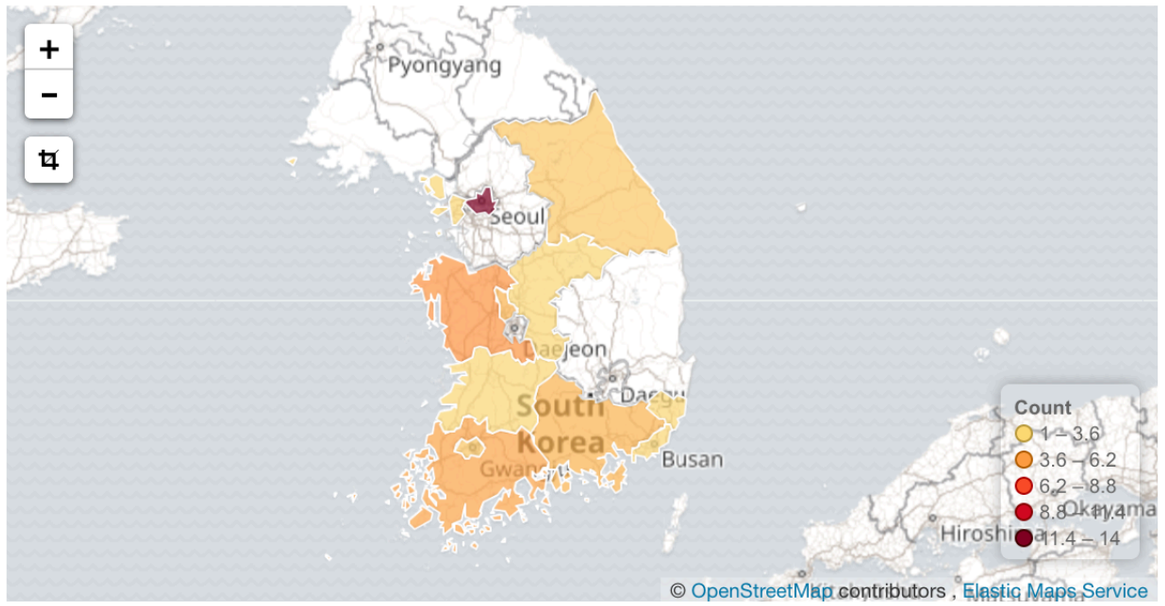
- 강의자료
- 강의질문
- Markdown문법

38
전체 데이터

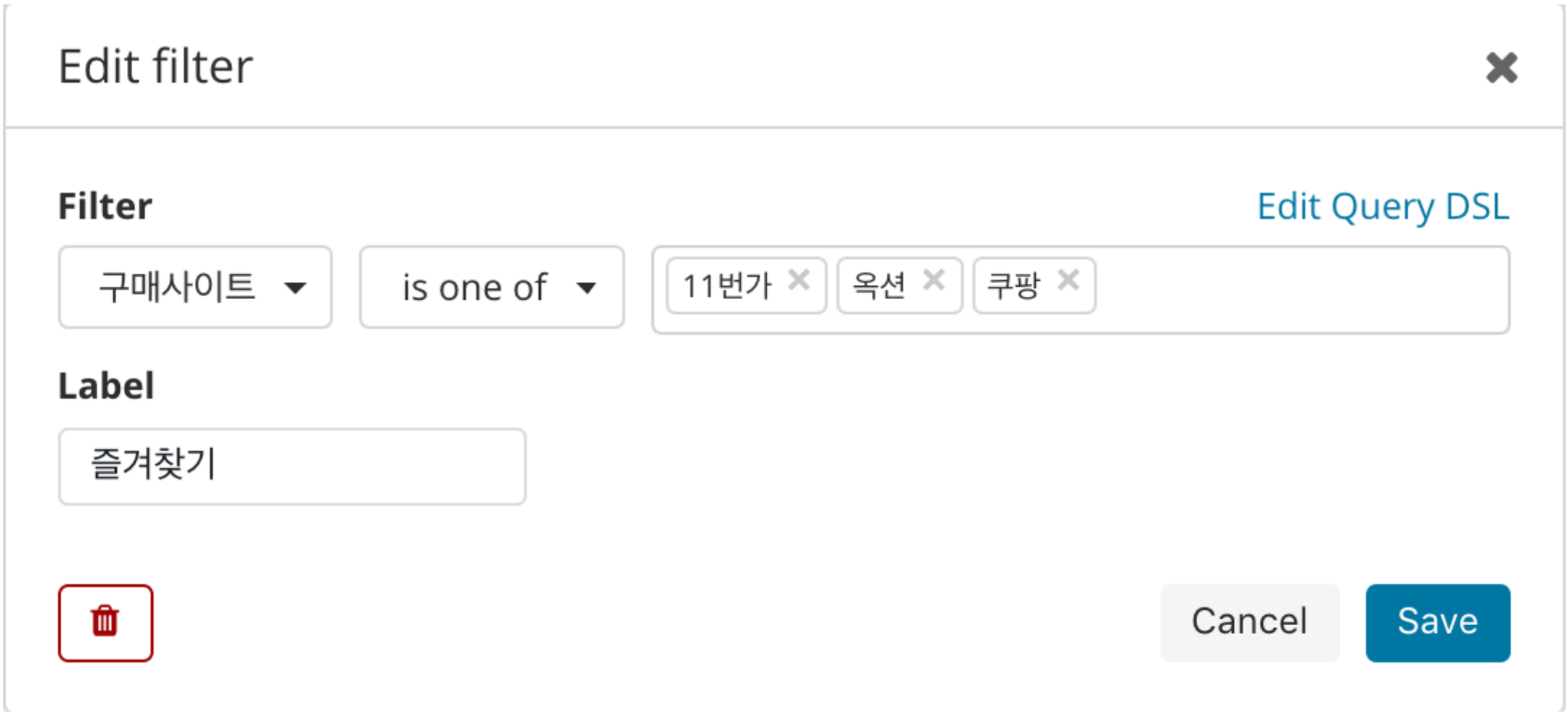
[shopping] Tag Cloud



[shopping] Region Map



Operator - is one of



Operator - is one of

Dashboard / shopping

Full screen Share Clone Edit Auto-refresh Last 30 days

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

Uses lucene query syntax

즐겨찾기 Add a filter +

Actions

sjyoun_week1_markdown

[shopping] metrics

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

20

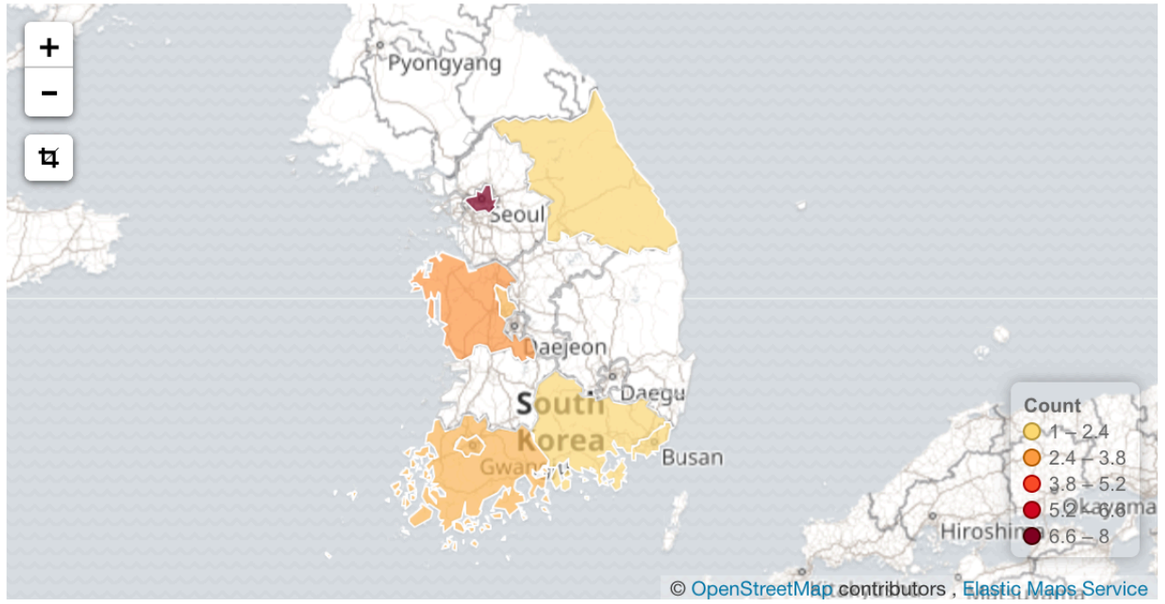
전체 데이터

[shopping] Tag Cloud

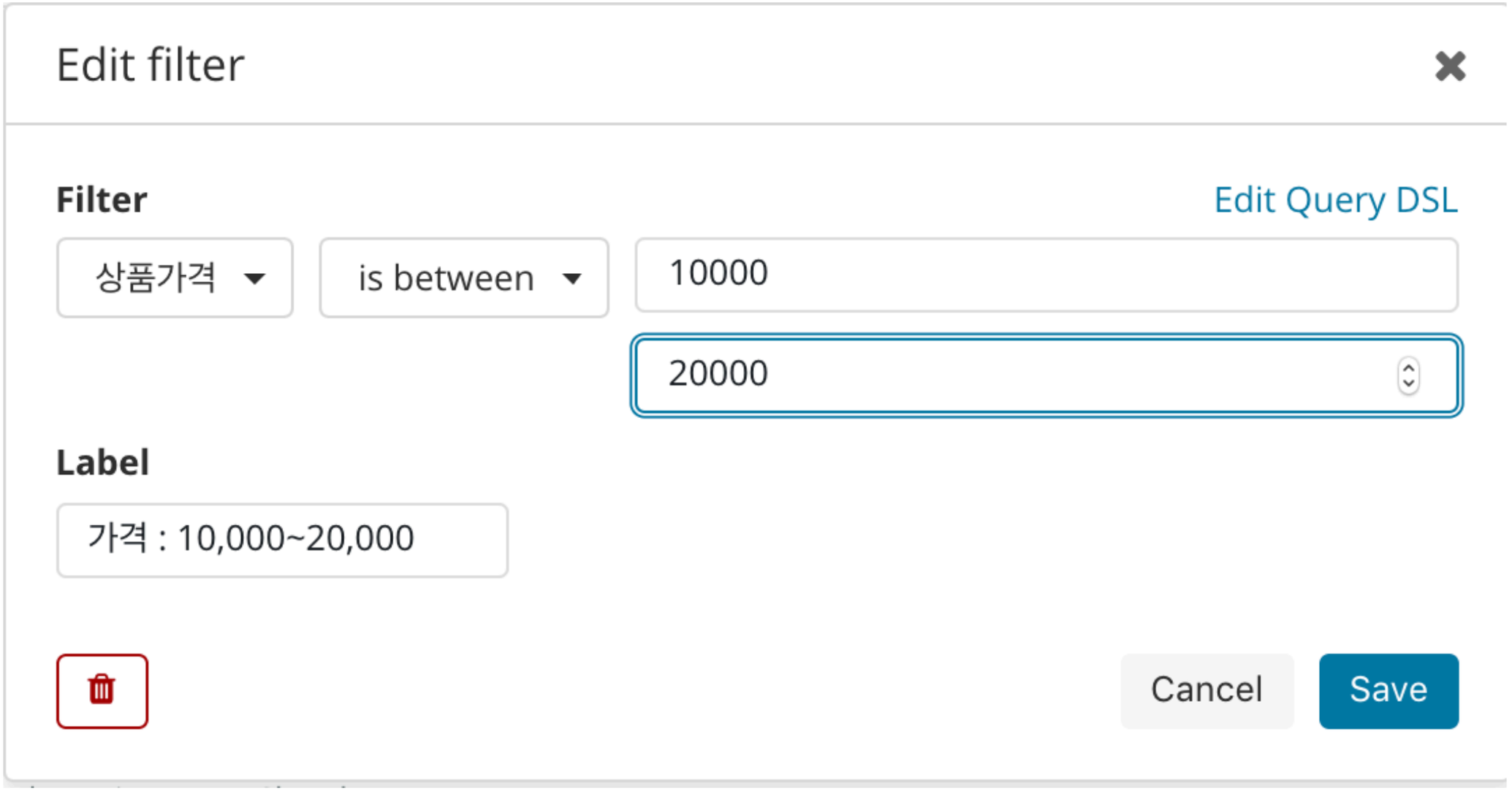
11번가

쿠팡 옥션

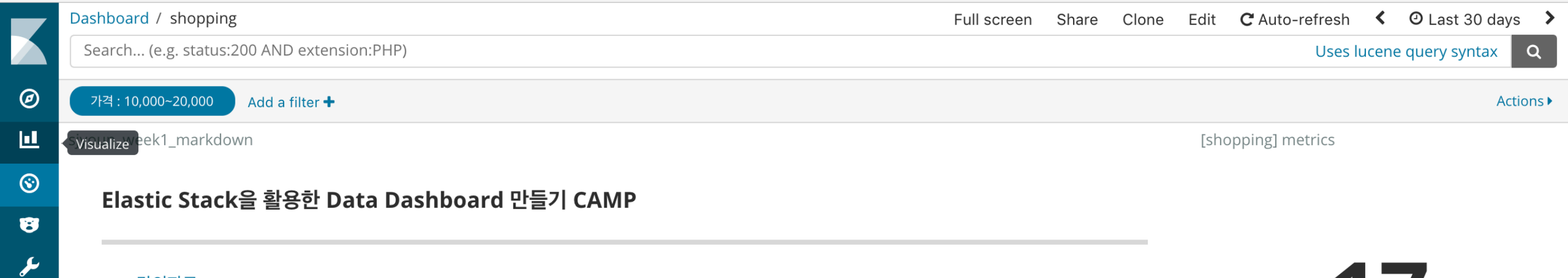
[shopping] Region Map



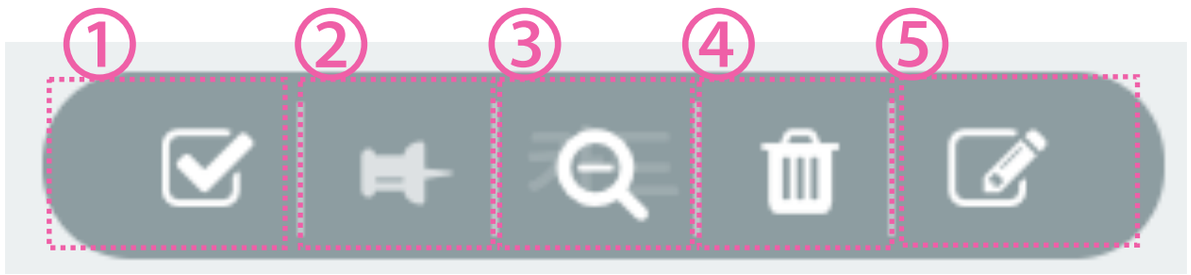
Operator - **is between**



Operator - is between



필터에 마우스오버하면…



안내

① 필터 적용 <=> 필터 적용 해제

② 필터 고정 (Discover, Visualize, Dashboard)

③ 필터 효과 적용 <=> 필터 효과 반대 적용

④ 필터 삭제

⑤ 필터 수정

예제4 - 아래와 같은 Filter를 Dashboard에 적용해보자

Dashboard : nginx-*

Time Range : Past 30 days

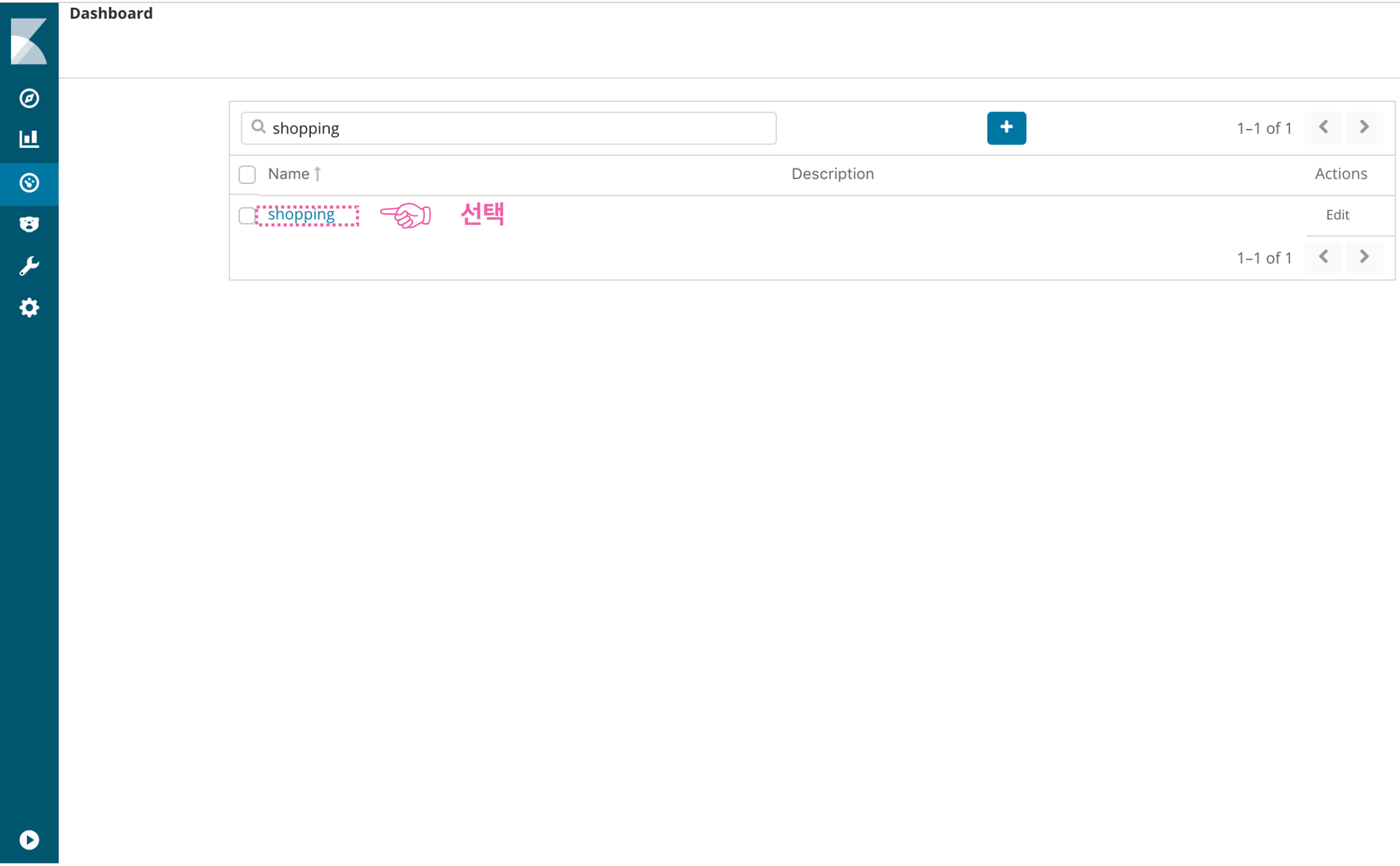
문제	operator
nginx.access.response_code가 200인 Doc 필터링	is
nginx.access.method가 GET 또는 POST인 Doc 필터링	is one of
nginx.access.geoip.region_name가 non-null값만 가지는 Doc 필터링	exists
nginx.access.geoip.city_name이 Seoul이면서 nginx.access.user_agent.name이 Chrome인 Doc 필터링	is
nginx.access.geoip.city_name이 Seoul이거나 nginx.access.user_agent.name이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

Lucene Query ♕

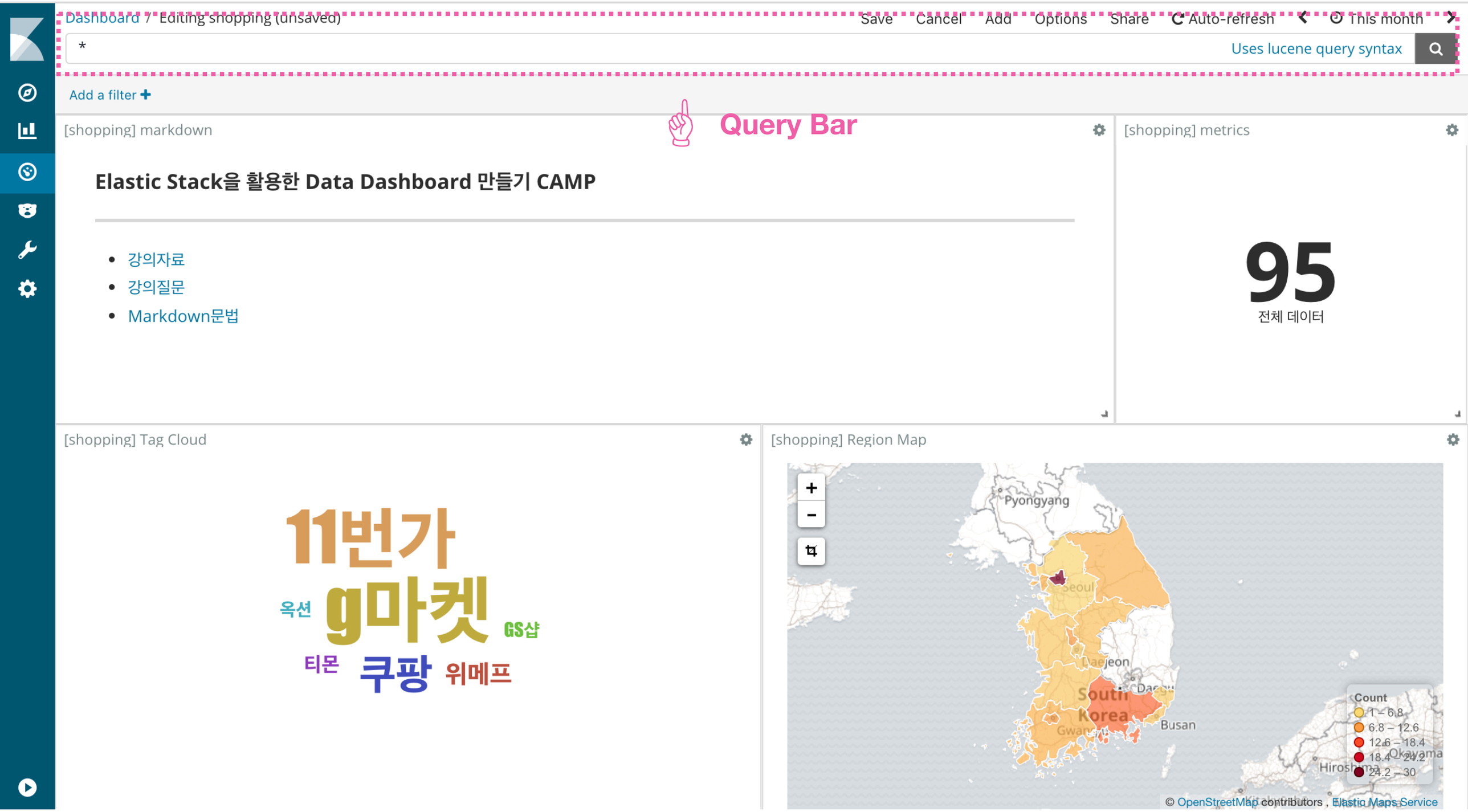
Filter는 사용하기 간단하나 기능이 제한적이다

그렇다면 다른 방법이 더 있을까?

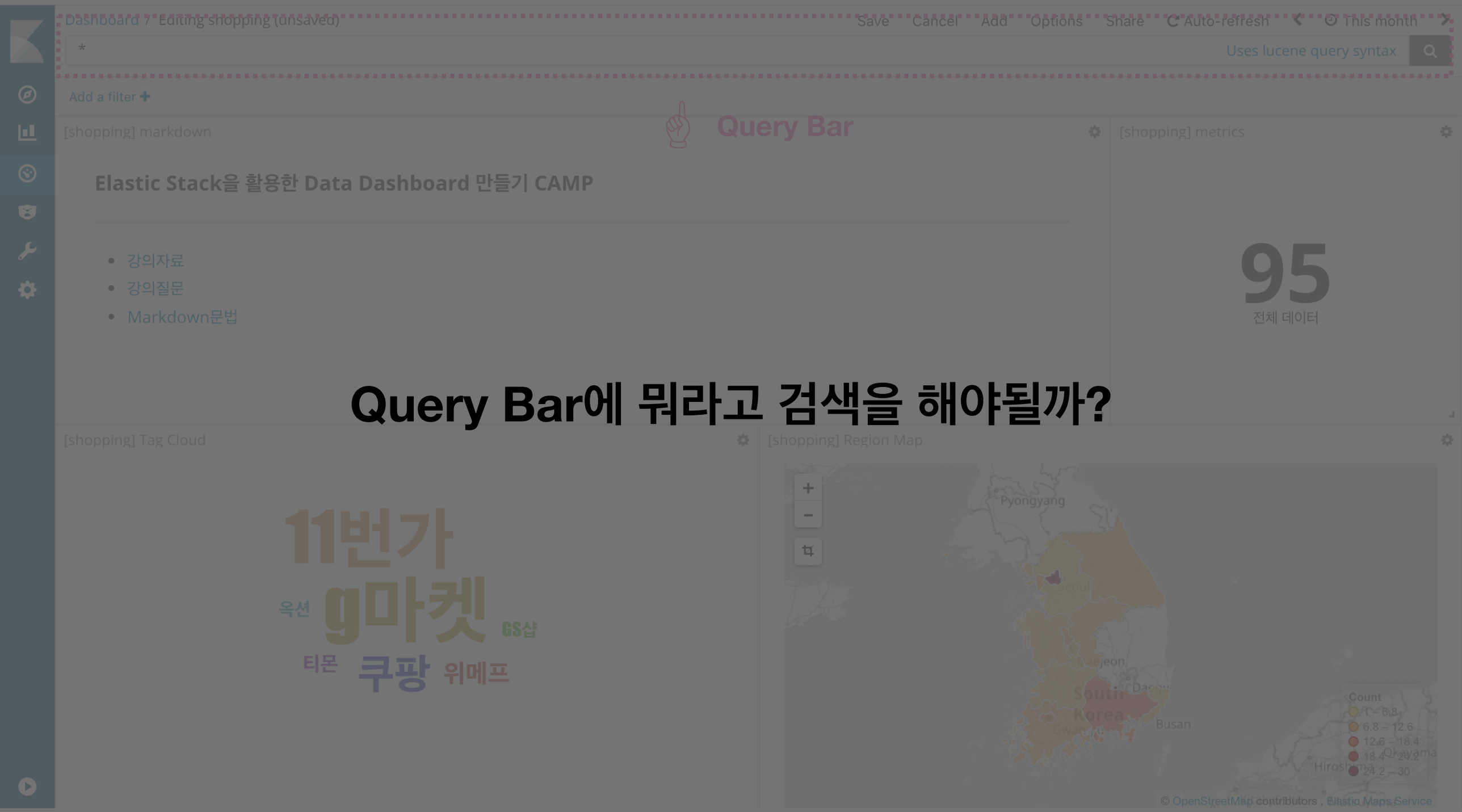
우선 Dashboard를 열자



Query Bar를 확인하자



Query Bar를 확인하자

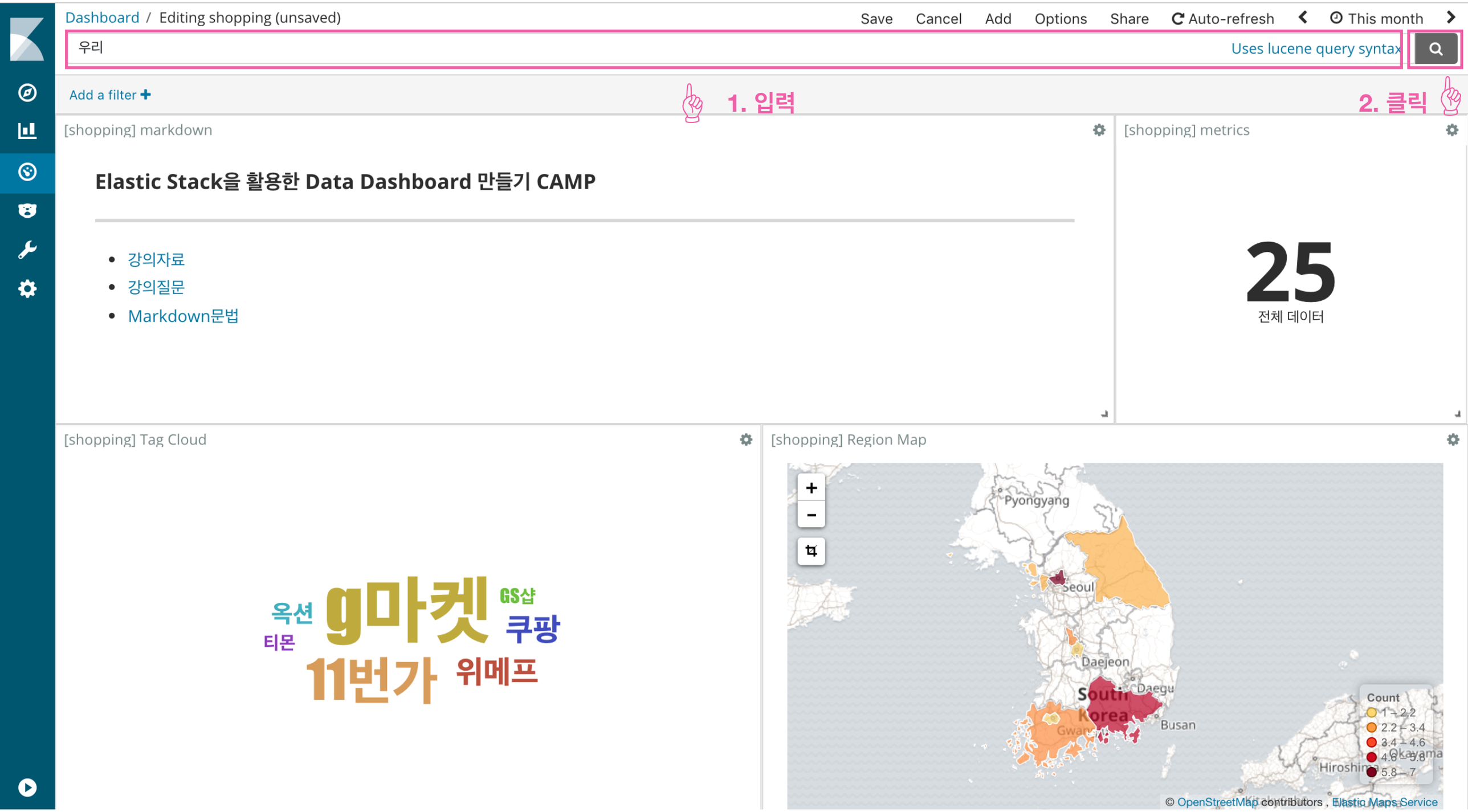


Query Bar에 뭐라고 검색을 해야될까?

Lucene Query의 사용법을 익히자

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

Search Type - Keyword



Search Type - Field Match

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh This month

결제카드:우리

Uses lucene query syntax

Add a filter +

1. 입력

2. 클릭

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

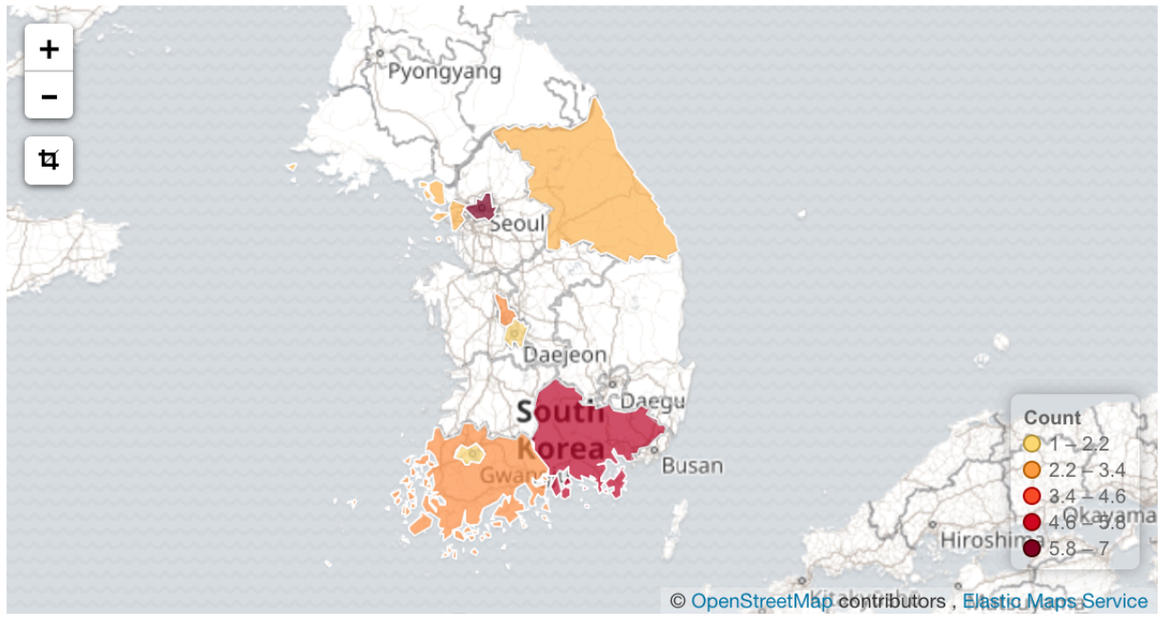
25

전체 데이터

[shopping] Tag Cloud

옥션 g마켓 GS샵 쿠팡 티몬 11번가 위메프

[shopping] Region Map



Search Type - Exact Field Match

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

배송메모:"상품 이상" Uses lucene query syntax

Add a filter +

1. 입력

2. 클릭

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

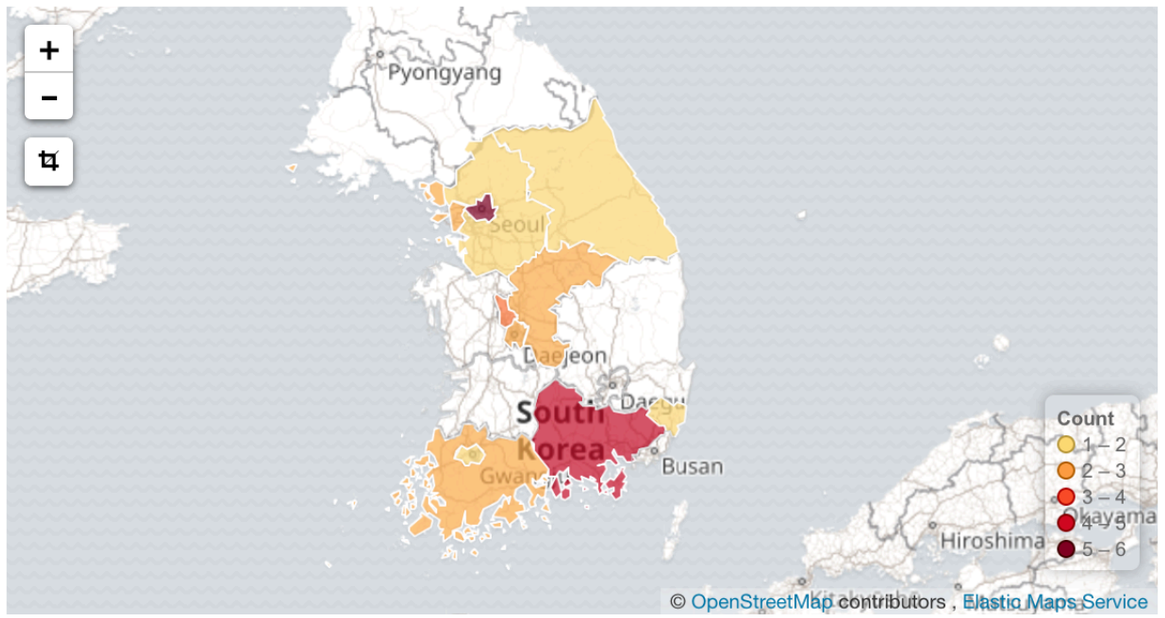
26

전체 데이터

[shopping] Tag Cloud

쿠팡
위메프 11번가 옥션
g마켓 GS샵

[shopping] Region Map



Search Type - Term

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh This month

상품분류: ("니트" "코트")

Uses lucene query syntax

Add a filter +

1. 입력

2. 클릭

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

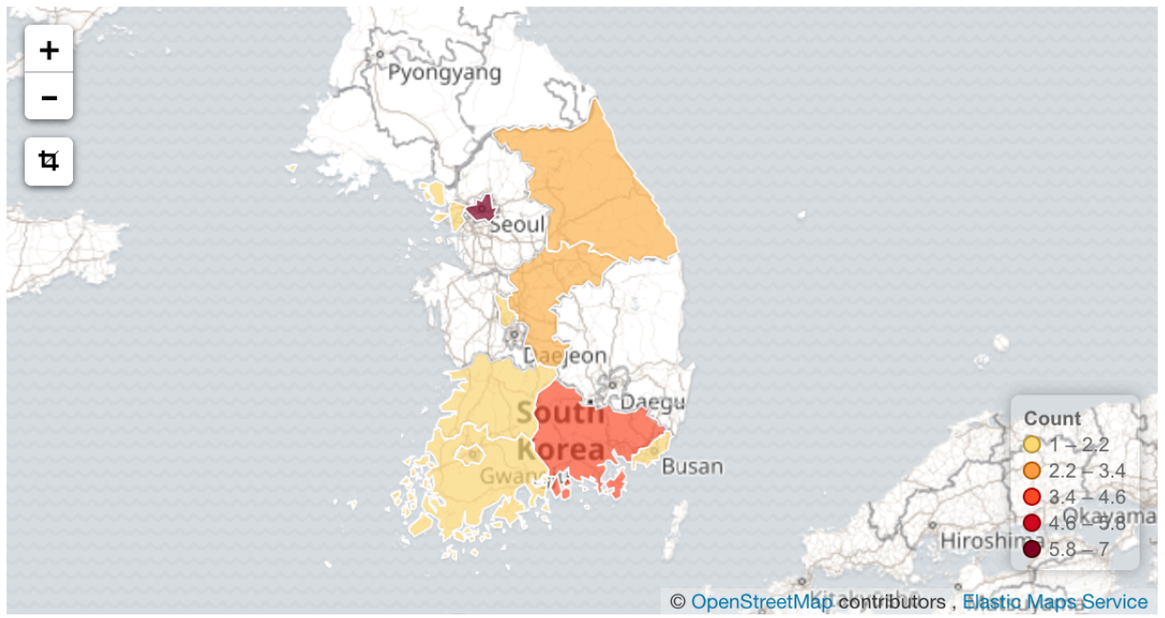
21

전체 데이터

[shopping] Tag Cloud

11번가 쿠팡 위메프 g마켓 티몬

[shopping] Region Map



Search Type - Fuzzy

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

고객주소_시도:전라도~1 Uses lucene query syntax

Add a filter +

1. 입력

2. 클릭

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

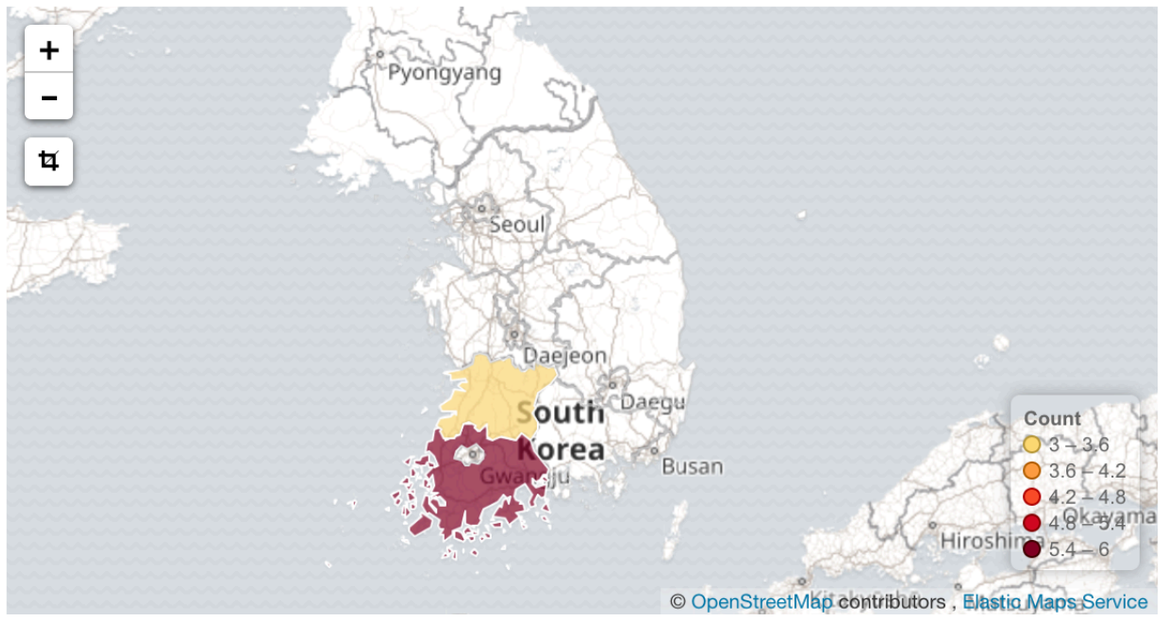
9

전체 데이터

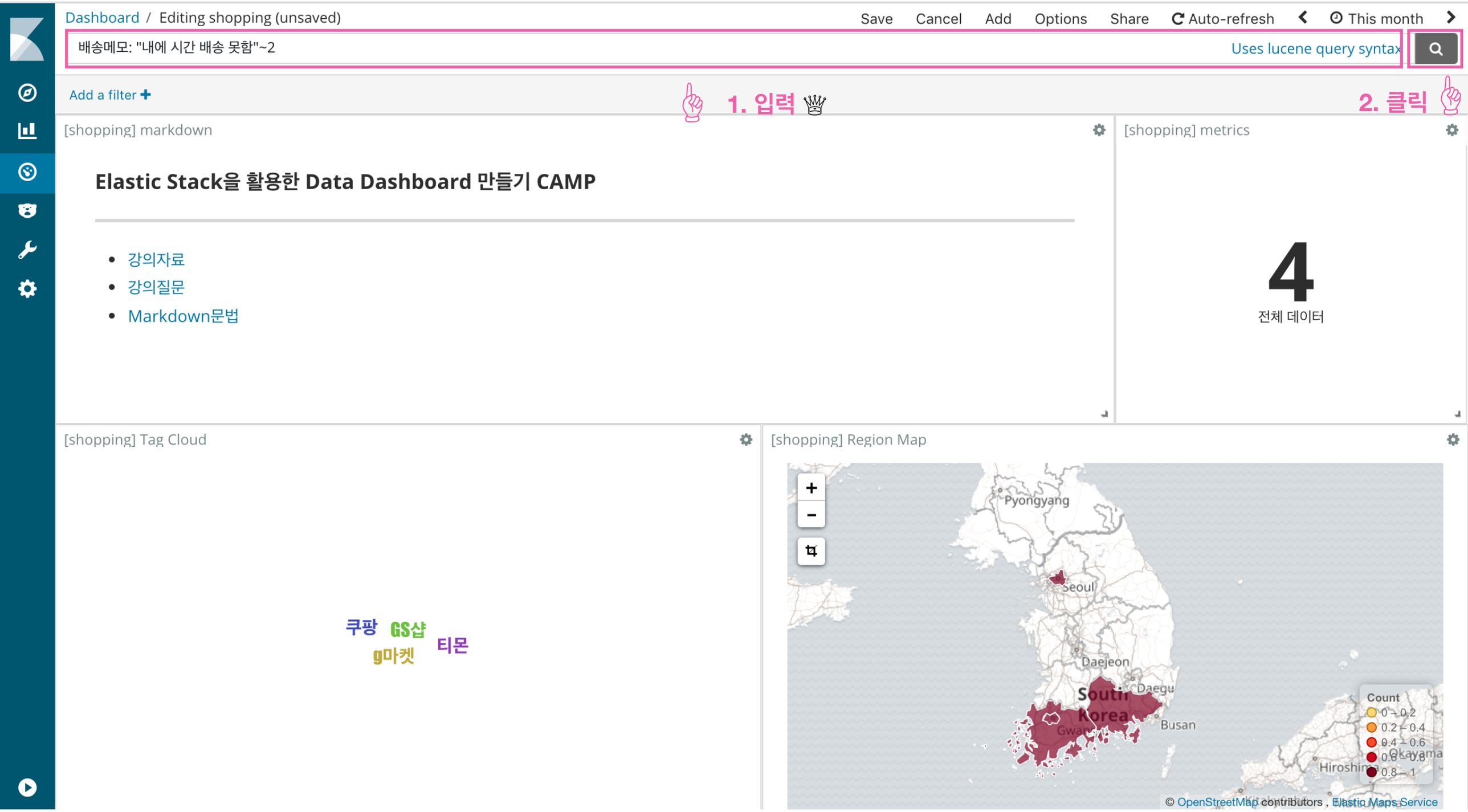
[shopping] Tag Cloud

g마켓 쿠팡 티몬 옥션 위메프

[shopping] Region Map



Search Type - Proximity 👑



Search Type - Numeric

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

상품가격:>5000 Uses lucene query syntax

Add a filter +

1. 입력

2. 클릭

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

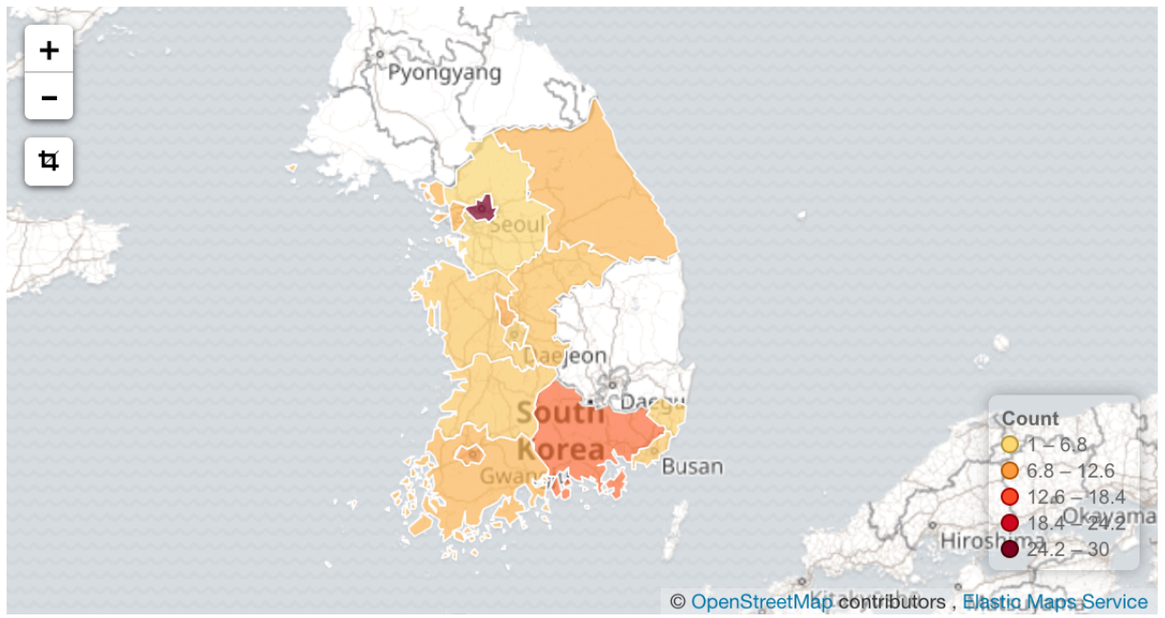
92

전체 데이터

[shopping] Tag Cloud

옥션
위메프 11번가 GS샵
티몬
g마켓 쿠팡

[shopping] Region Map



Search Type - Range

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh This month

고객나이: [10 TO 30}

Uses lucene query syntax

Add a filter +

1. 입력

2. 클릭

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

36

전체 데이터

[shopping] Tag Cloud

옥션 g마켓 위메프
티몬
쿠팡 11번가

[shopping] Region Map

Search Type - Wildcard

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

고객주소_시도:서?특별시 Uses lucene query syntax

Add a filter +

1. 입력

2. 클릭

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

30

전체 데이터

[shopping] Tag Cloud

쿠팡
11번가
위메프
티몬
GS샵
g마켓
옥션

[shopping] Region Map

Search Type - Wildcard

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh This month

상품*:셔츠

Uses lucene query syntax

Add a filter +

1. 입력

2. 클릭

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

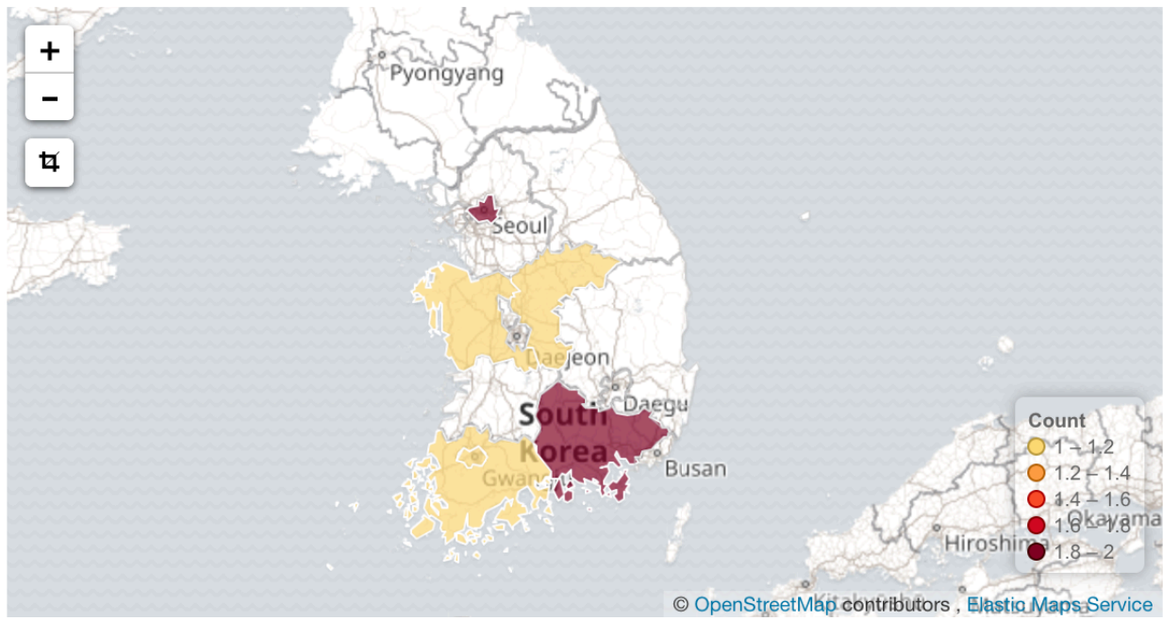
8

전체 데이터

[shopping] Tag Cloud

g마켓 옥션 쿠팡 티몬

[shopping] Region Map



Search Type - OR ♛

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh This month

고객성별:여성 OR 상품분류:셔츠 Uses lucene query syntax

Add a filter +

1. 입력

2. 클릭

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

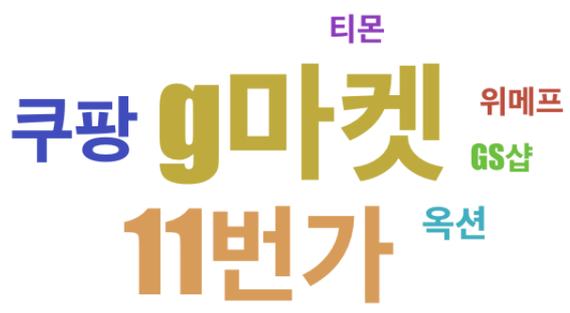
- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

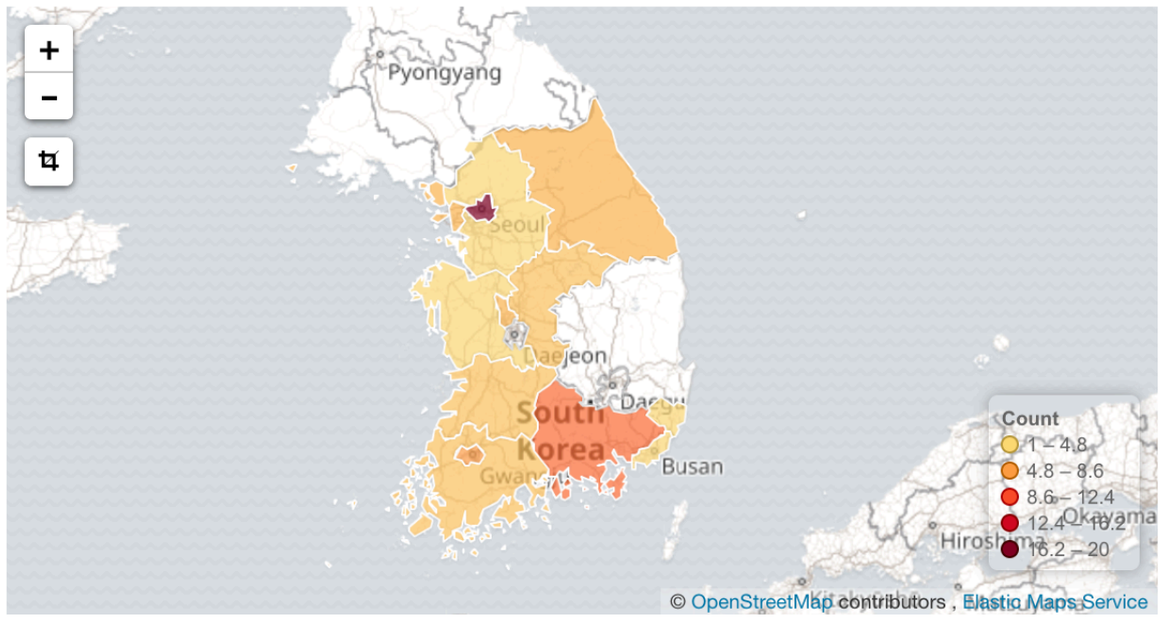
60

전체 데이터

[shopping] Tag Cloud



[shopping] Region Map



Search Type - AND

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh This month

고객성별:여성 AND 상품분류:셔츠

Uses lucene query syntax

Add a filter +

1. 입력

2. 클릭

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

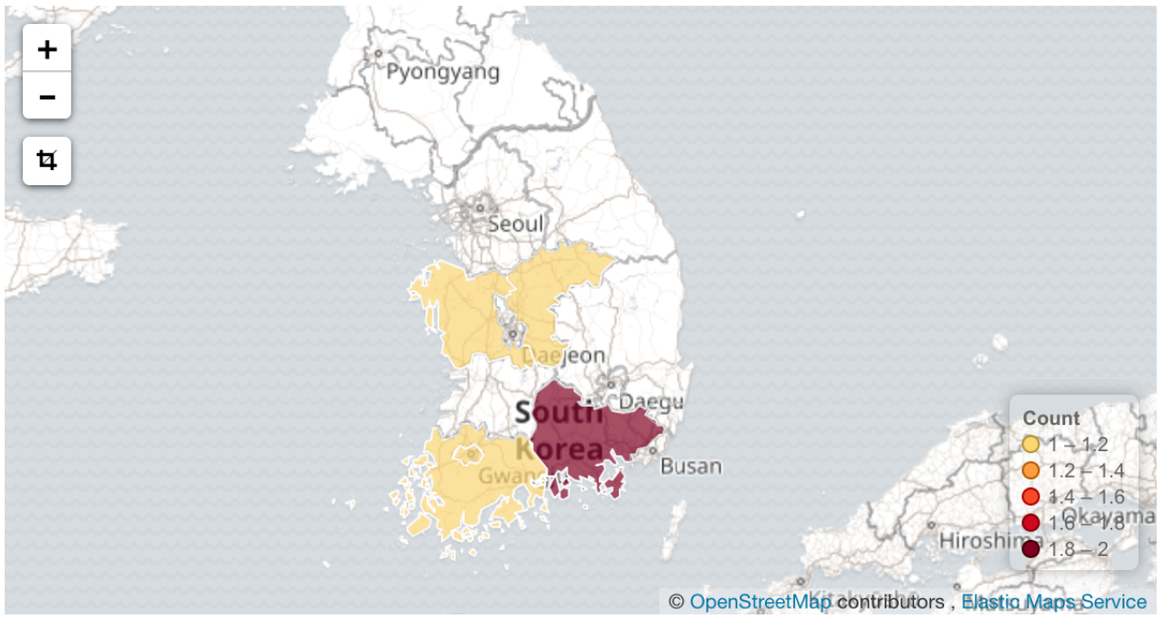
6

전체 데이터

[shopping] Tag Cloud

g마켓 옥션 쿠팡 티몬

[shopping] Region Map



Search Type - NOT

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh This month

NOT 구매사이트:옥션

Uses lucene query syntax

Add a filter +

1. 입력

2. 클릭

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

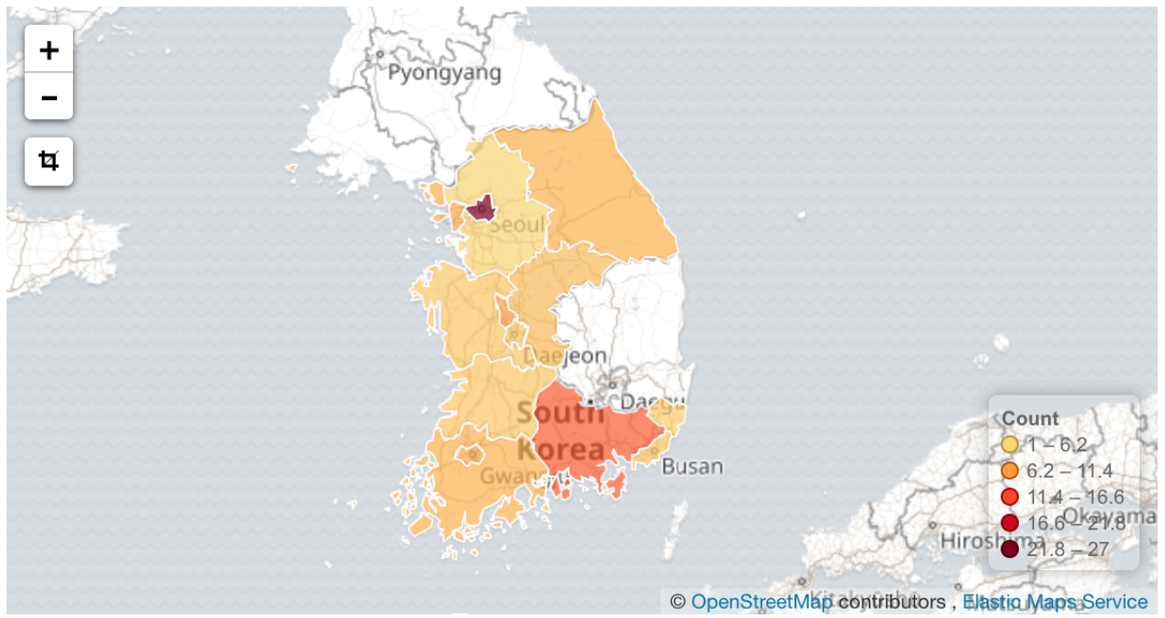
89

전체 데이터

[shopping] Tag Cloud

11번가
g마켓
GS샵
티몬
쿠팡
위메프

[shopping] Region Map



Search Type +

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh This month

+예약여부:예약

Uses lucene query syntax

Add a filter +

1. 입력

2. 클릭

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

12

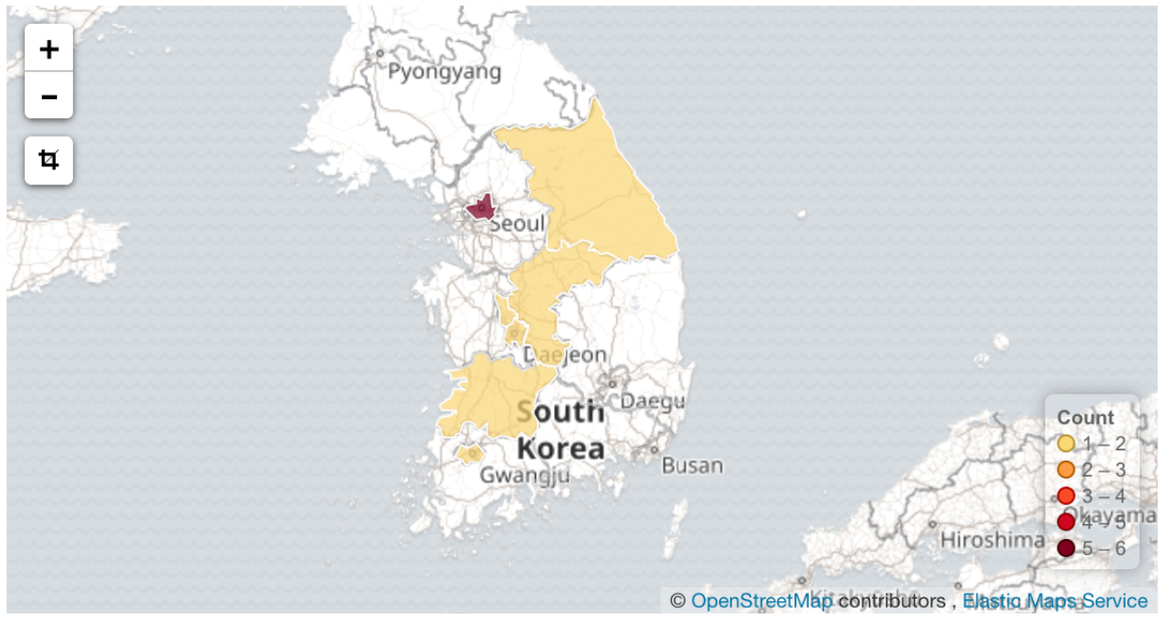
전체 데이터

[shopping] Tag Cloud

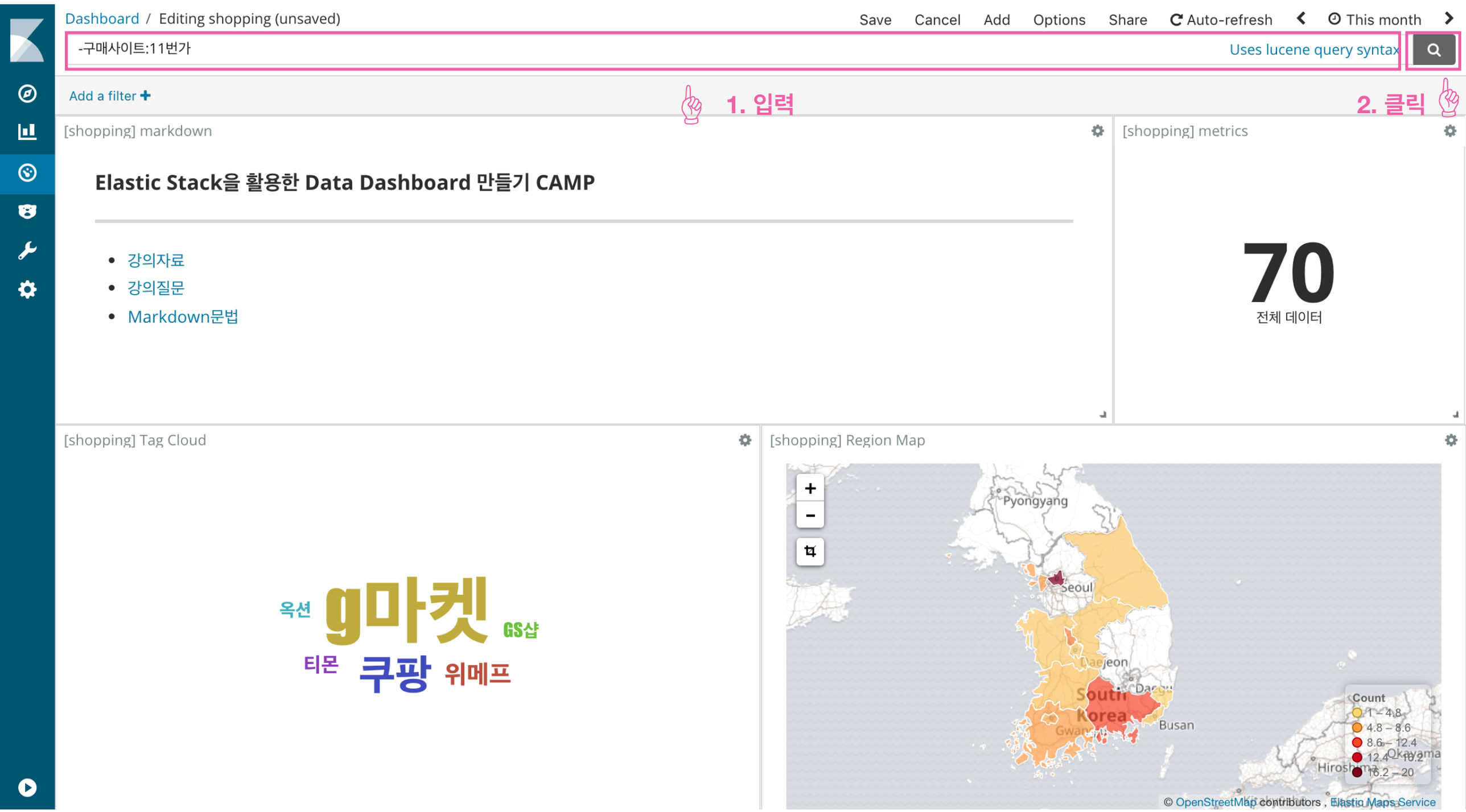
옥션 11번가 GS샵

g마켓 쿠팡

[shopping] Region Map



Search Type -


Dashboard / Editing shopping (unsaved)
Save
Cancel
Add
Options
Share
Auto-refresh
This month
-구매사이트:11번가
Uses lucene query syntax
Add a filter +
1. 입력
2. 클릭
[shopping] markdown
Elastic Stack을 활용한 Data Dashboard 만들기 CAMP
강의자료
강의질문
Markdown문법
[shopping] metrics
70
전체 데이터
[shopping] Tag Cloud
옥션
g마켓
GS샵
티몬
쿠팡
위메프
[shopping] Region Map
Pyongyang
Seoul
Daejeon
South Korea
Busan
Hiroshima
Okayama
Count
1 – 4.8
4.8 – 8.6
8.6 – 12.4
12.4 – 16.2
16.2 – 20
© OpenStreetMap contributors , Elastic Maps Service

잠깐4 심화

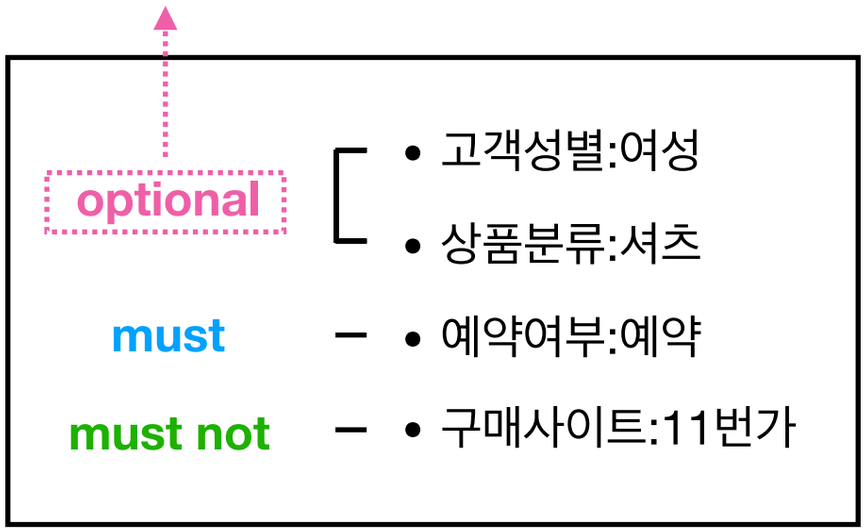
AND, OR, NOT으로도 충분해 보이는데

+, - 은 왜 필요할까? 👑

다음과 같은 조건으로 검색하려면 Query Bar에 뭐라고 입력해야 할까?

심화

필수는 아니지만 만족하는 Doc의 **score** ↑



조건이 너무 복잡하고, 가독성이 떨어지며, 에러 내기 쉽다 **심화**

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

이 때 +, -을 사용하면 쉽게 구현할 수 있다 👑 **심화**

Dashboard / Editing shopping (unsaved)

Save Cancel Add Options Share Auto-refresh This month

여성 셔츠 +예약 -11번가

Uses lucene query syntax

Add a filter +

[shopping] markdown

Elastic Stack을 활용한 Data Dashboard 만들기 CAMP

- 강의자료
- 강의질문
- Markdown문법

[shopping] metrics

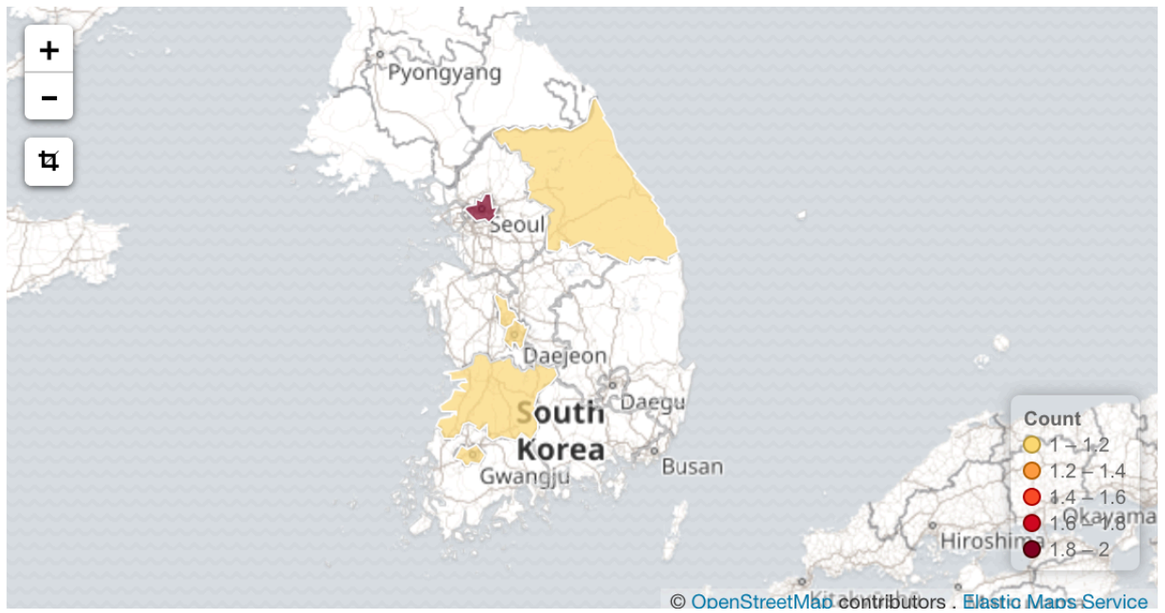
7

전체 데이터

[shopping] Tag Cloud

g마켓 옥션 쿠팡 GS샵

[shopping] Region Map



예제 5 - 아래와 같은 Query를 Dashboard에서 검색해보자

Dashboard : nginx-*

Time Range : Past 30 days

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

Filter와 Search를 비교해보자

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		✓
요일_local이 Sunday인 Doc 필터링	✓	
nginx.access.geoip.country_name 가 Republic of로 시작하는 Doc		✓
nginx.access.geoip.continent_code가 AS와 유사한 Doc		✓

AND 연산

OR 연산

Scripted Field

Wildcard 검색

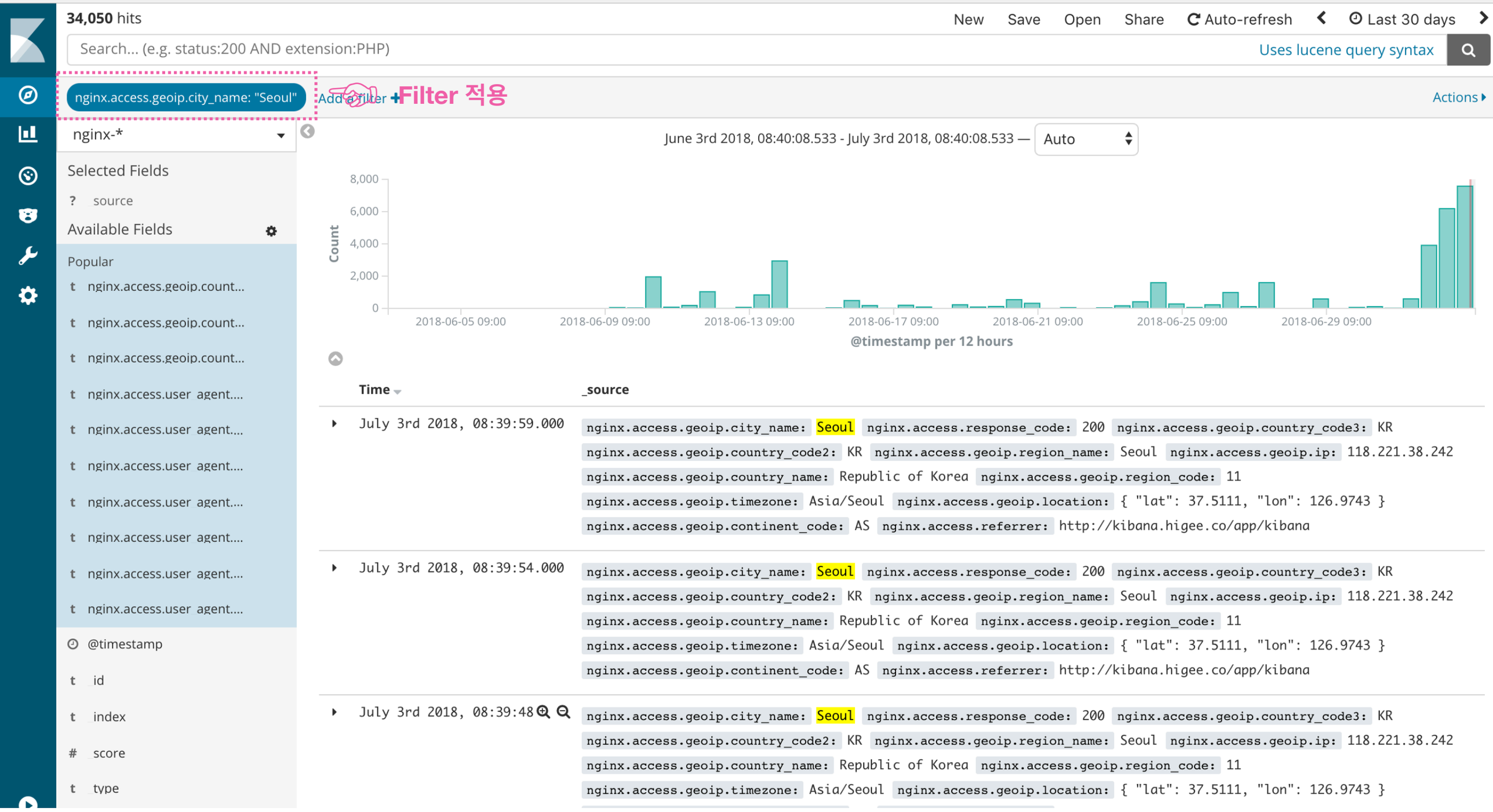
Fuzzy/Proximity 검색


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~~	• ~~특정 Document를 Table/JSON 형태 조회~~ • ~~Histogram 특정 구간 내의 데이터 조회~~ • ~~Histogram Bin 간격 설정~~ • ~~Histogram 데이터를 csv 출력~~ • ~~특정 Field의 정보만 조회~~ • ~~특정 Field 값을 기준으로 정렬~~
~~데이터 통계~~	• ~~(선택한 Time Range 내의) Documents 개수 확인~~ • ~~특정 Field Value의 분포 확인 (주로 Categorical Data, 상위 500개)~~ • ~~특정 Field에 non-null Value가 아닌 Documents 수 확인~~

Discover에서 Filter를 적용해보자



Discover에서 Search를 해보자

34,053 hits

New Save Open Share Auto-refresh Last 30 days

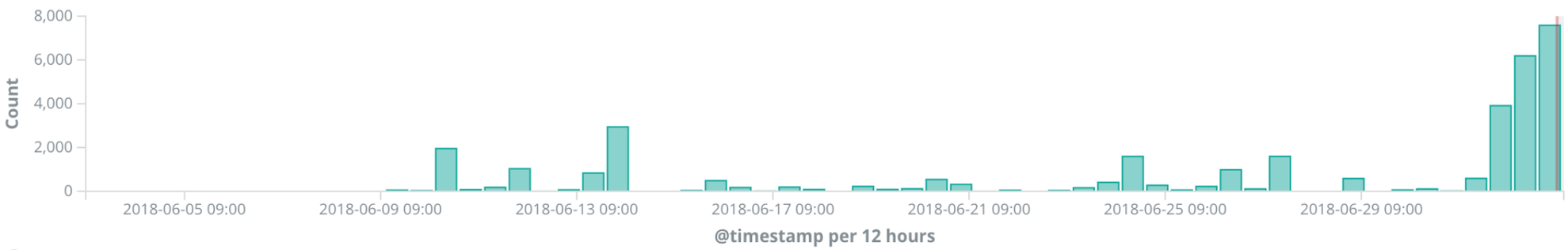
nginx.access.geoip.city_name: Seoul

Uses lucene query syntax

Add a filter +

nginx-*

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



Selected Fields

? source

Available Fields

Popular

t nginx.access.geoip.count...

t nginx.access.geoip.count...

t nginx.access.geoip.count...

t nginx.access.user_agent....

t nginx.access.user_agent....

t nginx.access.user_agent....

t nginx.access.user_agent....

t nginx.access.user_agent....

t nginx.access.user_agent....

@timestamp

t _id

t _index

_score

t _type

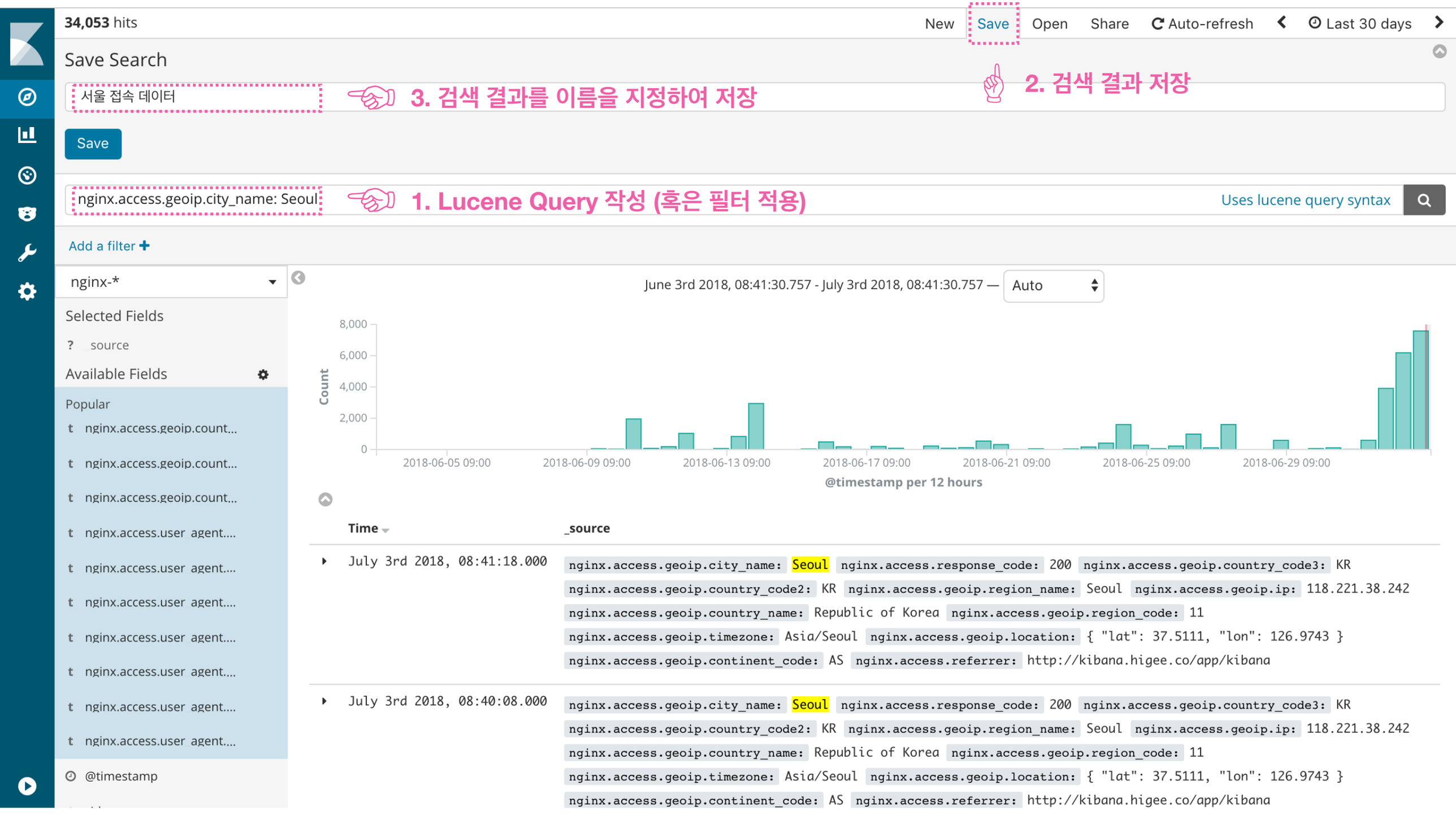
t access.user_agent

Time	_source
July 3rd 2018, 08:41:18.000	nginx.access.geoip.city_name: Seoul nginx.access.response_code: 200 nginx.access.geoip.country_code3: KR nginx.access.geoip.country_code2: KR nginx.access.geoip.region_name: Seoul nginx.access.geoip.ip: 118.221.38.242 nginx.access.geoip.country_name: Republic of Korea nginx.access.geoip.region_code: 11 nginx.access.geoip.timezone: Asia/Seoul nginx.access.geoip.location: { "lat": 37.5111, "lon": 126.9743 } nginx.access.geoip.continent_code: AS nginx.access.referrer: http://kibana.higee.co/app/kibana
July 3rd 2018, 08:40:08.000	nginx.access.geoip.city_name: Seoul nginx.access.response_code: 200 nginx.access.geoip.country_code3: KR nginx.access.geoip.country_code2: KR nginx.access.geoip.region_name: Seoul nginx.access.geoip.ip: 118.221.38.242 nginx.access.geoip.country_name: Republic of Korea nginx.access.geoip.region_code: 11 nginx.access.geoip.timezone: Asia/Seoul nginx.access.geoip.location: { "lat": 37.5111, "lon": 126.9743 } nginx.access.geoip.continent_code: AS nginx.access.referrer: http://kibana.higee.co/app/kibana
July 3rd 2018, 08:40:06.000	nginx.access.geoip.city_name: Seoul nginx.access.response_code: 200 nginx.access.geoip.country_code3: KR nginx.access.geoip.country_code2: KR nginx.access.geoip.region_name: Seoul nginx.access.geoip.ip: 118.221.38.242 nginx.access.geoip.country_name: Republic of Korea nginx.access.geoip.region_code: 11 nginx.access.geoip.timezone: Asia/Seoul nginx.access.geoip.location: { "lat": 37.5111, "lon": 126.9743 } nginx.access.geoip.continent_code: AS nginx.access.referrer: http://kibana.higee.co/app/kibana

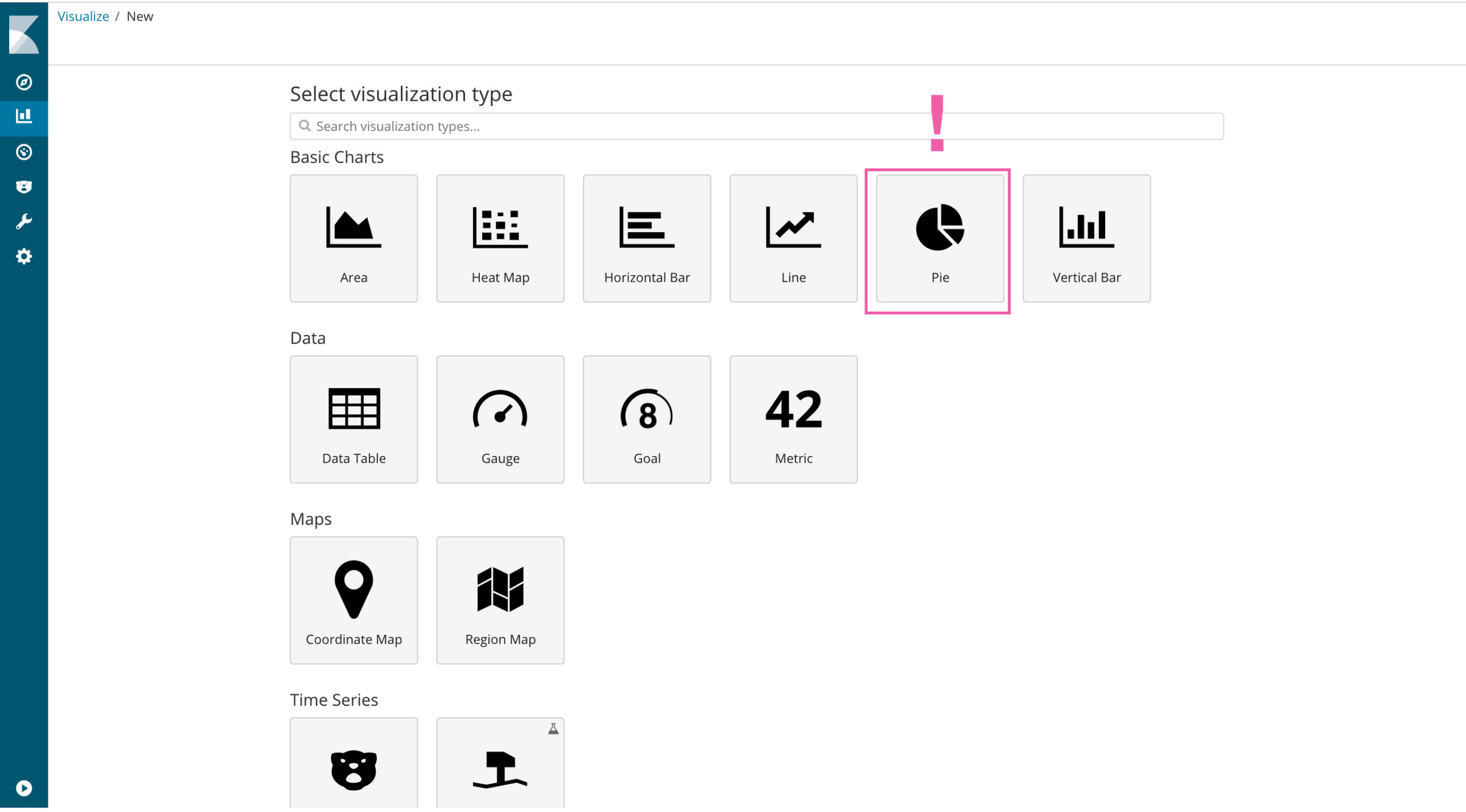
잠깐5, 이걸로 뭘 할 수 있을까?

: 특정한 조건을 만족하는 데이터만 선별해서 시각화 할 수 있다.

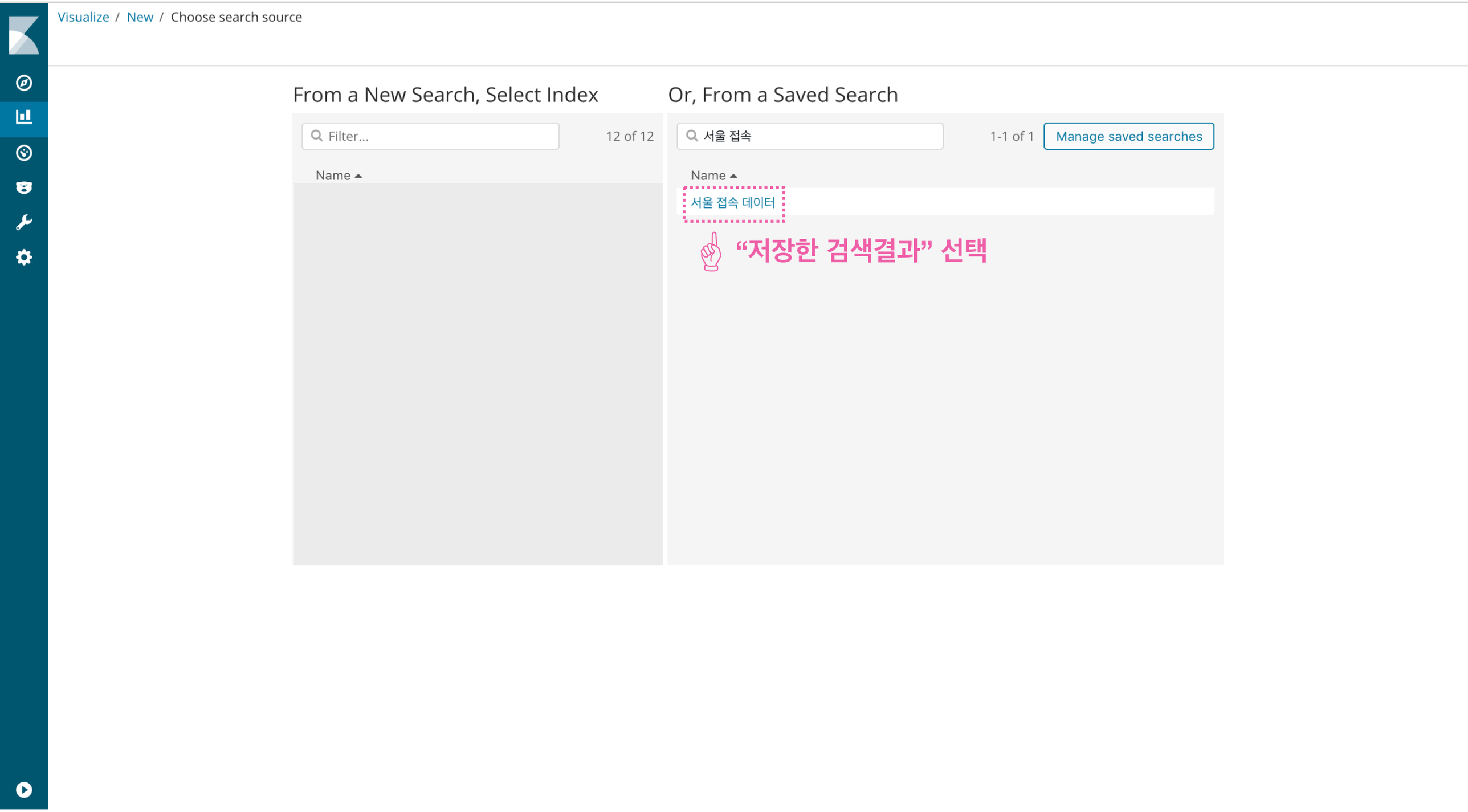
검색 결과 저장


34,053 hits
New
Save
Open
Share
Auto-refresh
Last 30 days
Save Search
서울 접속 데이터
3. 검색 결과를 이름을 지정하여 저장
2. 검색 결과 저장
Save
nginx.access.geoip.city_name: Seoul
1. Lucene Query 작성 (혹은 필터 적용)
Uses lucene query syntax
Add a filter +
nginx-*
Selected Fields
? source
Available Fields
Popular
t nginx.access.geoip.count...
t nginx.access.geoip.count...
t nginx.access.user agent....
t nginx.access.user agent....
t nginx.access.user agent....
t nginx.access.user agent....
t nginx.access.user agent....
t nginx.access.user agent....
t nginx.access.user agent....
@timestamp
June 3rd 2018, 08:41:30.757 - July 3rd 2018, 08:41:30.757 —
Auto
Count
8,000
6,000
4,000
2,000
0
2018-06-05 09:00
2018-06-09 09:00
2018-06-13 09:00
2018-06-17 09:00
2018-06-21 09:00
2018-06-25 09:00
2018-06-29 09:00
@timestamp per 12 hours
Time
_source
July 3rd 2018, 08:41:18.000
nginx.access.geoip.city_name: Seoul nginx.access.response_code: 200 nginx.access.geoip.country_code3: KR nginx.access.geoip.country_code2: KR nginx.access.geoip.region_name: Seoul nginx.access.geoip.ip: 118.221.38.242 nginx.access.geoip.country_name: Republic of Korea nginx.access.geoip.region_code: 11 nginx.access.geoip.timezone: Asia/Seoul nginx.access.geoip.location: { "lat": 37.5111, "lon": 126.9743 } nginx.access.geoip.continent_code: AS nginx.access.referrer: http://kibana.higee.co/app/kibana
July 3rd 2018, 08:40:08.000
nginx.access.geoip.city_name: Seoul nginx.access.response_code: 200 nginx.access.geoip.country_code3: KR nginx.access.geoip.country_code2: KR nginx.access.geoip.region_name: Seoul nginx.access.geoip.ip: 118.221.38.242 nginx.access.geoip.country_name: Republic of Korea nginx.access.geoip.region_code: 11 nginx.access.geoip.timezone: Asia/Seoul nginx.access.geoip.location: { "lat": 37.5111, "lon": 126.9743 } nginx.access.geoip.continent_code: AS nginx.access.referrer: http://kibana.higee.co/app/kibana

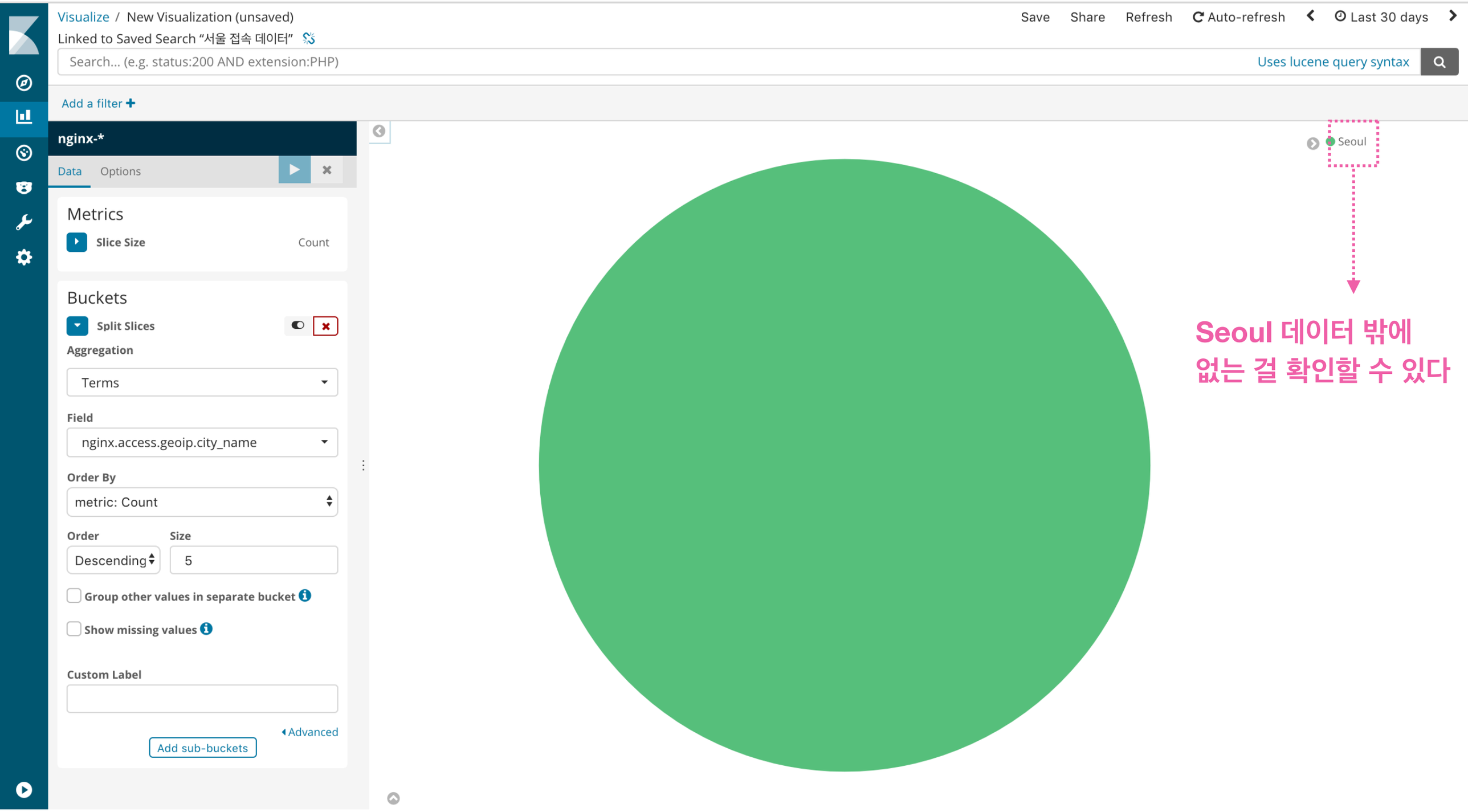
저장된 검색 결과를 이용한 시각화 1단계



저장된 검색 결과를 이용한 시각화 2단계



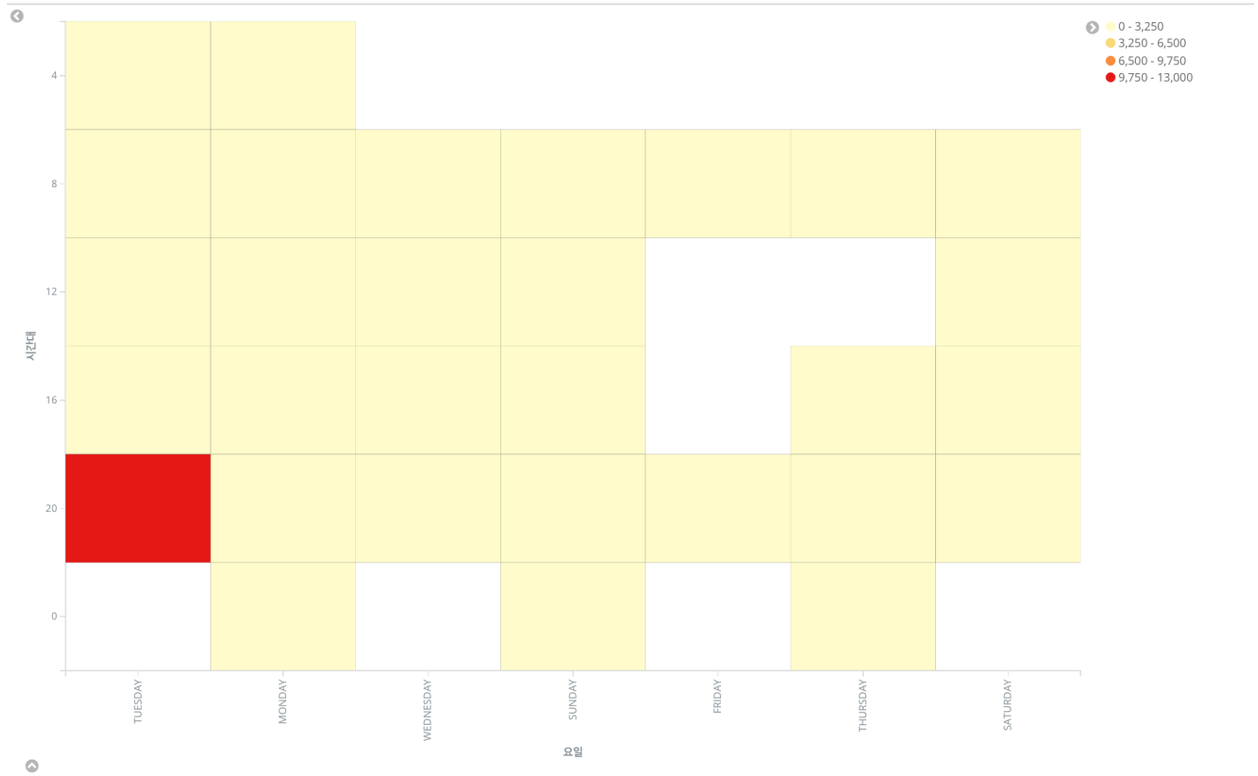
저장된 검색 결과를 이용한 시각화 3단계



예제 6.1 - 필터 혹은 검색을 이용해서 아래와 같은 데이터를 저장하자

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

예제 6.2- 앞서 저장한 결과로 아래와 같은 시각화를 하자



조건

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

질문 및 Feedback은

gshock94@gmail.com로 주세요