

# ELK Kibana 사용법

*Data Visualization Tool*



GS SHOP 벤처투자팀

2016. 02

# ELK Kibana 사용법

## 데이터 시각화 도구

### 데이터 시각화(DataViz)

컴퓨팅 세상이 발전하면서, 예전에는 쉽게 볼 수 없었던 데이터를 활용할 수 있는 수단이 많아졌다. 대표적인 것이 웹서버의 접속로그(access log)인데, 접속 로그를 통해서 서비스를 이용하는 패턴을 파악하고, 서비스 개선 포인트를 예전보다 쉽게 찾아낼 수 있게 되었다. 데이터를 시각화하면 이러한 패턴을 더욱 쉽게 찾아낼 수 있다. 이 문서에서는 오픈소스 데이터 시각화 도구인 Kibana의 사용법을 설명하려고 한다.

Kibana는 로그수집기(Logstash)에서 검색엔진(elasticsearch)에 모아진 데이터를 쉽게 검색하고, 필터링하며, 다양한 차트를 통해서 시각화할 수 있는 도구이다.



Kibana가 설치된 서버에 [http://kibana\\_ip:5601](http://kibana_ip:5601) 주소로 브라우저에서 접속이 가능하며 우측 상단을 클릭해서 조회 기간을 설정할 수 있다.

화면 상단에 Discover, Visualize, Dashboard, Settings 메뉴가 있으며, 상단 맨 우측에는 조회 기간이 보여진다.




Kibana를 사용하는 순서는 다음과 같다.

1. Discover에서 원하는 페이지 URL을 찾아서 저장한다.
2. Visualize에서 앞서 저장된 정보를 차트로 표현한다.
3. Dashboard에서 저장된 차트를 배치하여 한 눈에 볼 수 있도록 한다.

## 1. Discover

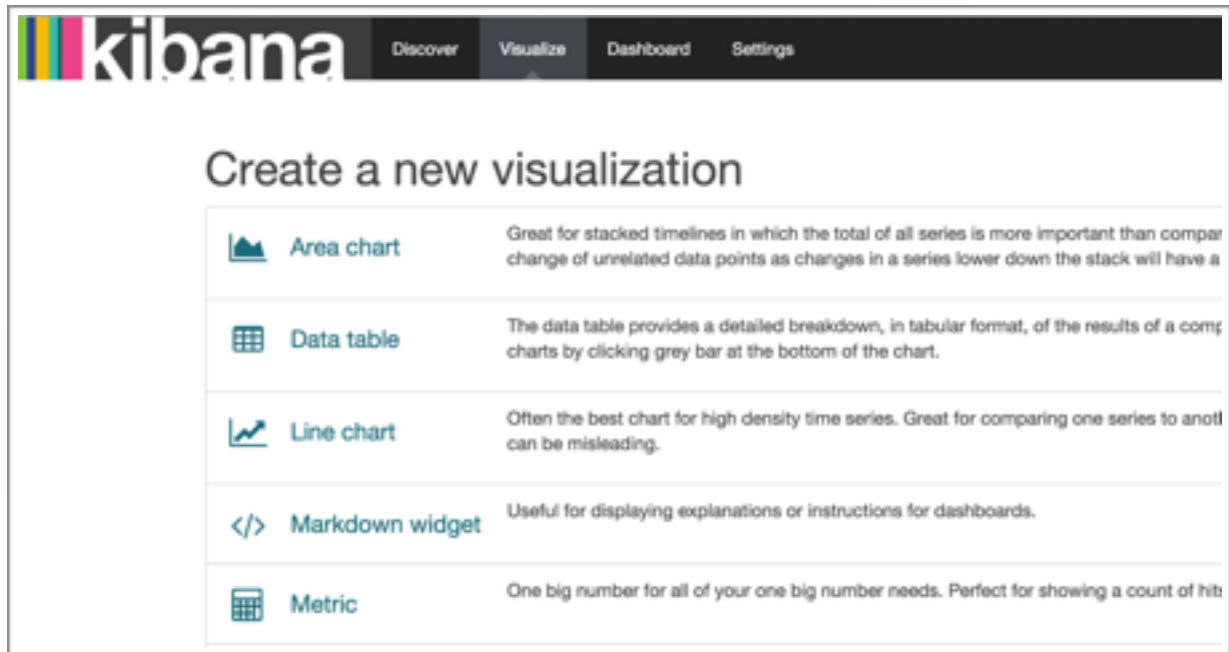
조회할 수 있는 정보는 다양하다. IP, URL, 등의 키워드를 사용할 수 있으며, 조회한 키워드를 저장했다가 나중에 다시 불러올 수도 있다.

아래 그림에서 “/order/CartCheckOut.asp” 페이지와 “/order/dispOrder.asp” 페이지를 동시에 검색하기 위해 “or” 키워드를 사이에 추가한 것을 볼 수 있다. 이렇게 검색결과가 보이게 되면 검색칸 우측에 저장 아이콘  을 클릭해서 “\*\*\* 주문”이라고 저장하는 모습이다.

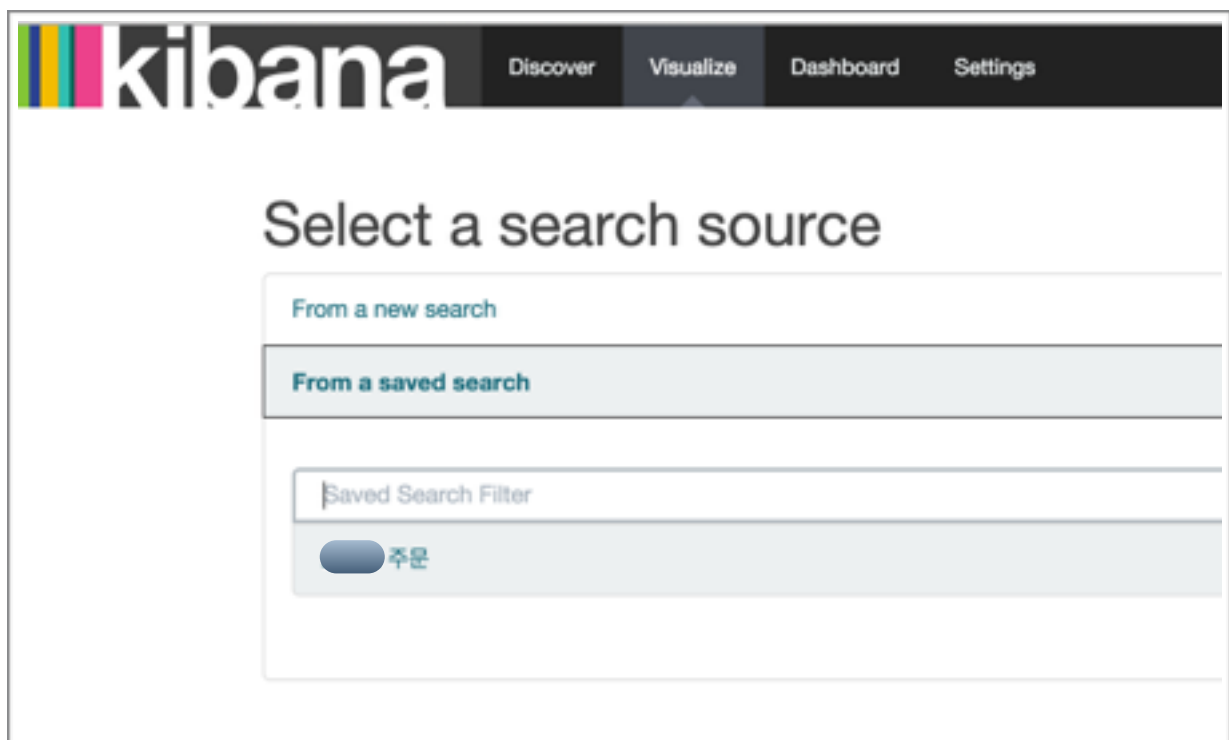


## 2. Visualize

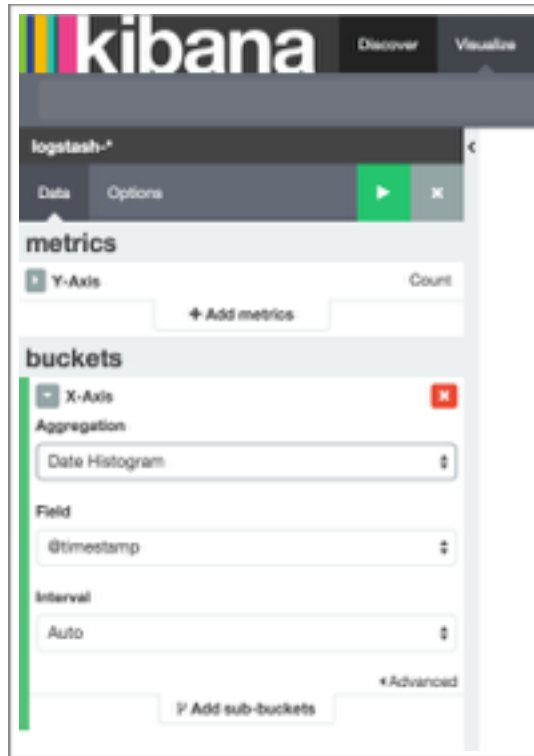
정보를 시각화하는 곳이다. 차트의 종류는 후에 설명하기로 하겠다. Area chart(영역 차트)를 클릭한다.



저장한 검색어가 있기 때문에 From a saved search 라인을 선택한다. 앞서 저장한 “\*\*\* 주문” 항목을 확인하고, 선택한다.



좌측에 buckets에서 X-Axis(축)을 선택한다. Aggregation을 Date Histogram 항목으로 선택하고, 엔터를 누르거나 녹색 아이콘을 클릭한다.



x축이 시간으로 정해지고, 단위 시간에 검색된 페이지의 카운트가 표시되는 차트를 얻을 수 있다. 이제 이 차트를 페이지를 구분할 수 있게 변경해보자. 좌측 하단에 Add sub-buckets를 클릭한다.

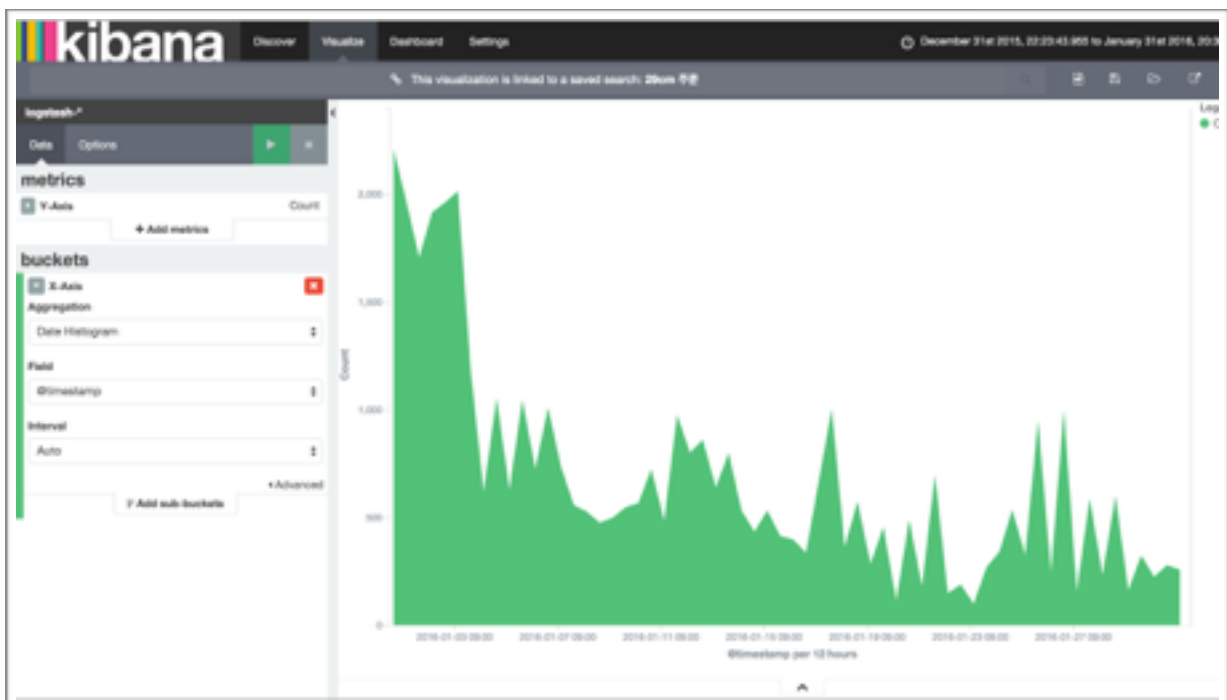
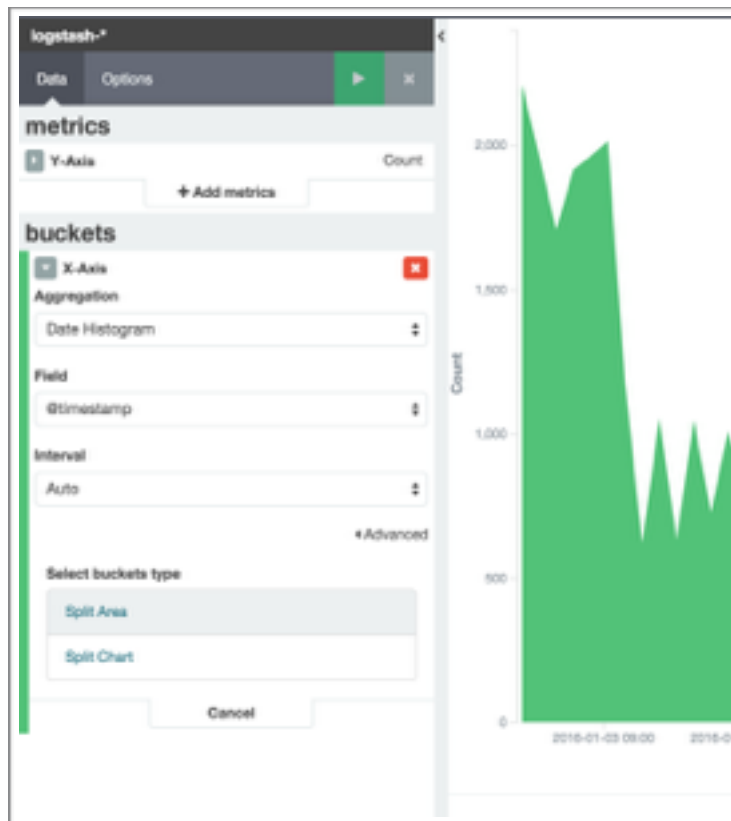


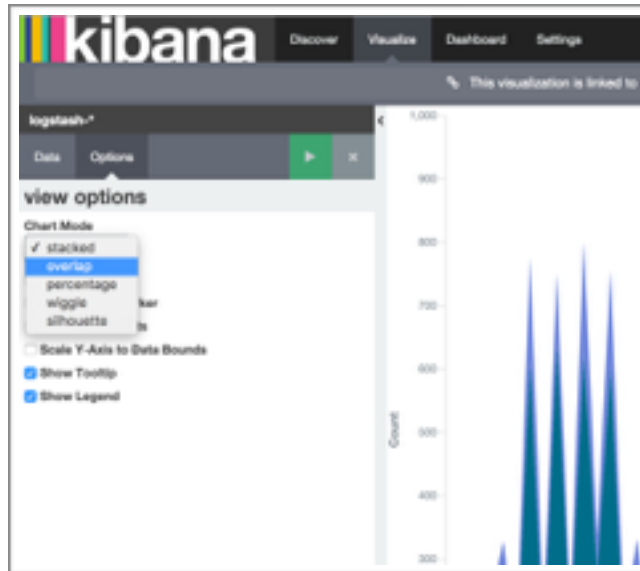
차트 영역을 구분할 것이기 때문에 Split Area 타입을 선택한다.



Filters를 선택하고, 페이지 URL을 입력한다. 다른 페이지는 까만 줄의 Add Filter를 클릭하고 추가할 수 있다. 우측에 범례(Legend)를 보면 해당 URL과 적용된 색상을 볼 수 있다. 영역을 나눈 것이기 때문에 옵션을 통해서 겹쳐보이도록 바꿔보자.

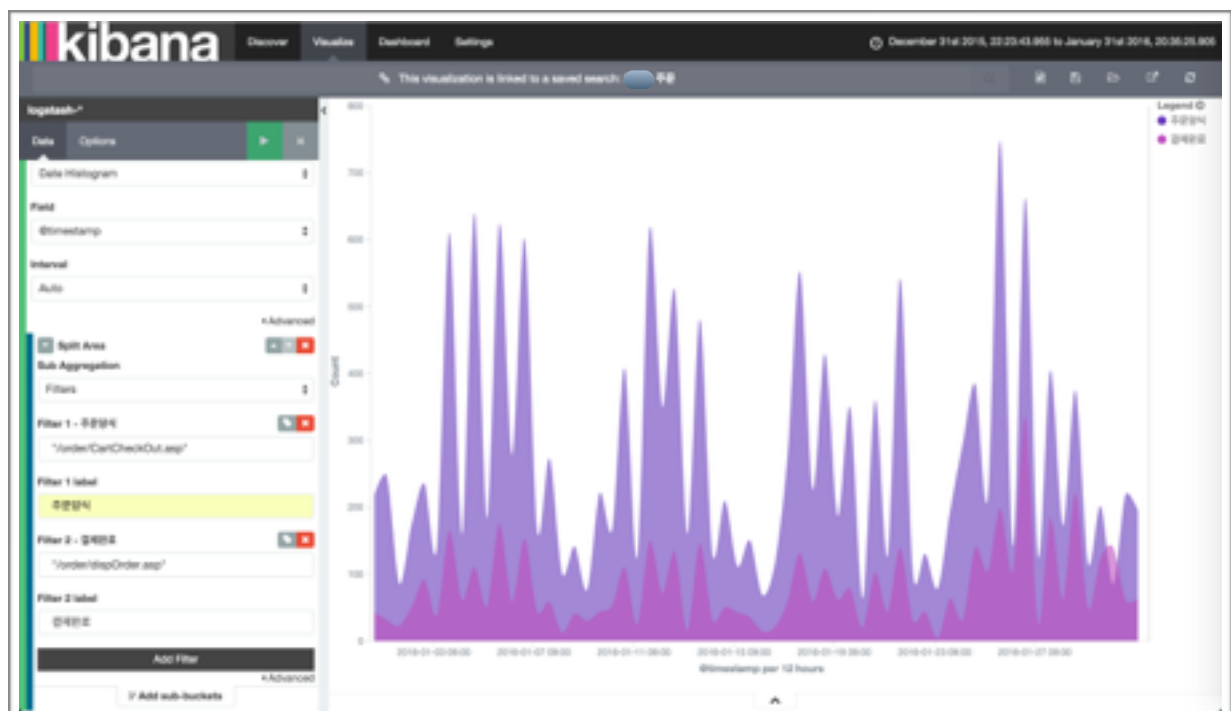


좌측 Data옆에 Options탭을 클릭한다. Chart Mode를 overlap으로 변경한다. 아울러 Smooth Lines 체크박스를 활성화하면 부드러운 선으로 겹쳐진 차트를 통해서 두 페이지의 통계를 비교할 수 있다.



Filter로 정해진 URL 우측에 태그 아이콘을 클릭하면 라벨(Label)을 추가할 수 있다. “주문양식”, “결제완료”로 지정하면 차트 우측의 범례가 바뀔 것을 확인할 수 있다.

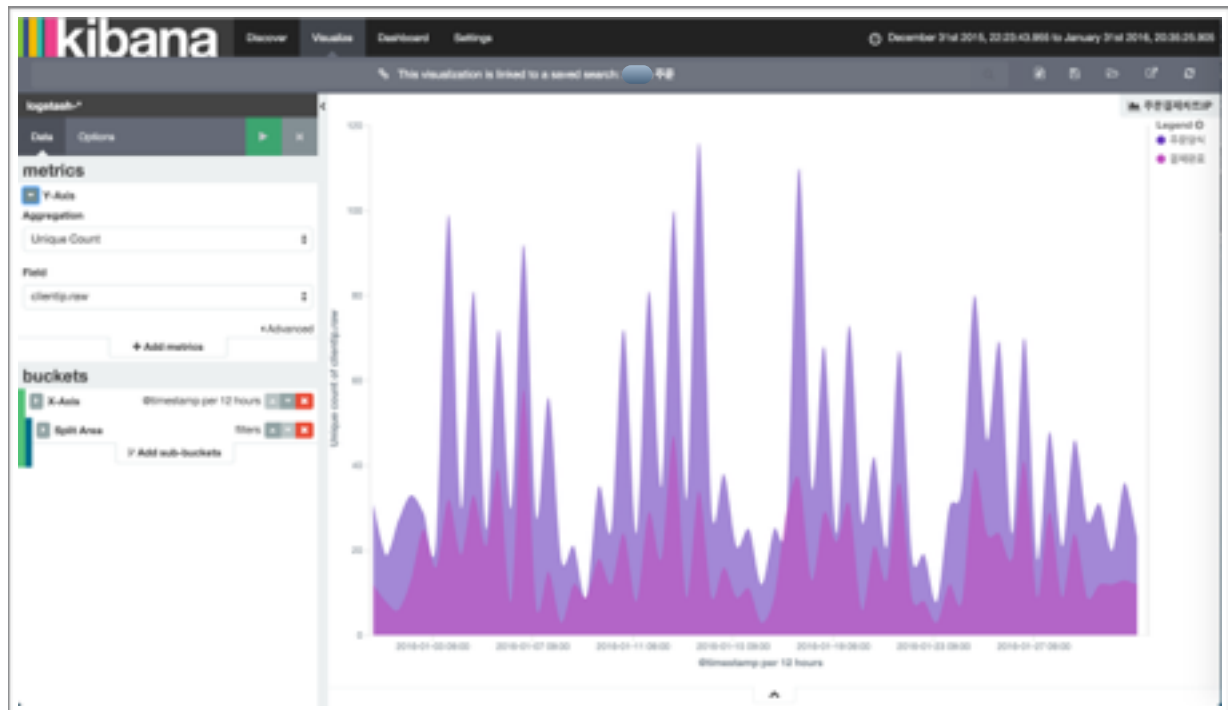
완성된 차트는 우측의 저장 아이콘을 클릭해서 “주문결제차트”라고 저장한다. 이렇게 저장된 차트는 Dashboard에서 사용할 것이다.






위의 차트는 페이지뷰(PV)를 기준으로 보여주는 것인데, IP를 통해서 실제 사용자수에 가까운 유니크한 정보를 볼 수 있도록 변경해 보려 한다.

좌측 Data탭에서 Y-Axis의 Aggregation을 Unique Count로 변경하고 Field를 clientip.raw 항목을 선택하면 된다. 차트의 왼쪽 상단 값이 변하는 것으로 차트가 변한 것을 확인할 수 있다. 저장 아이콘을 클릭해서 “주문결제차트IP”라고 이름을 붙인다.



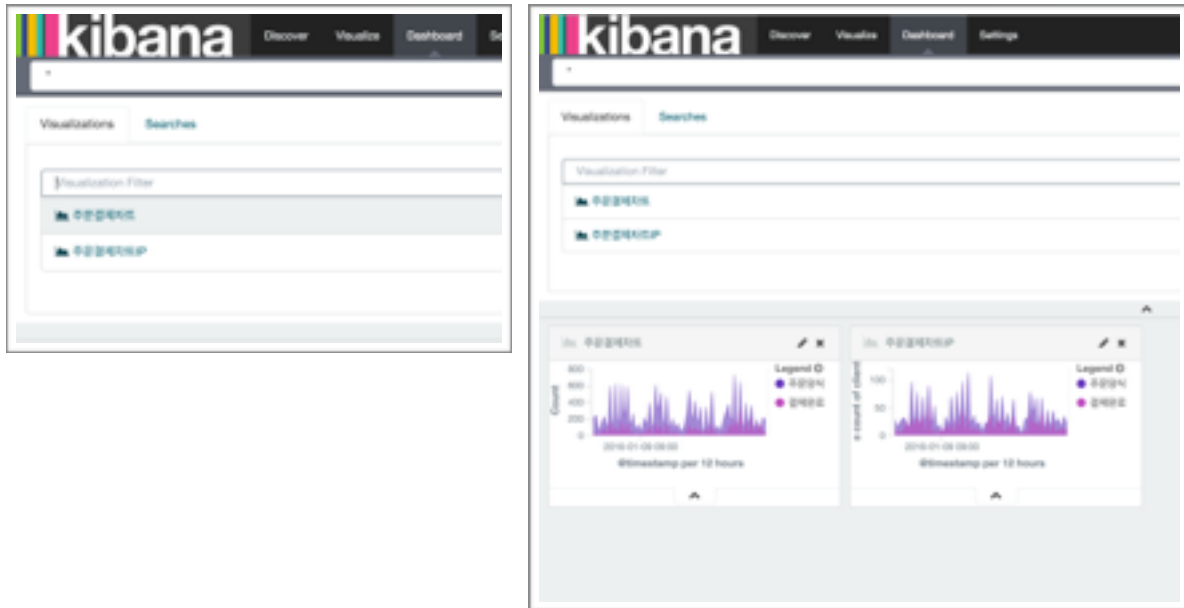
### 3. Dashboard

자동차의 대시보드는 자동차의 상태를 한 눈에 파악할 수 있도록 정보를 모아놓은 것이다. 마찬가지로 서비스의 상태를 한 눈에 파악할 수 있도록 여러 차트를 모아놓은 곳이 Dashboard이다.

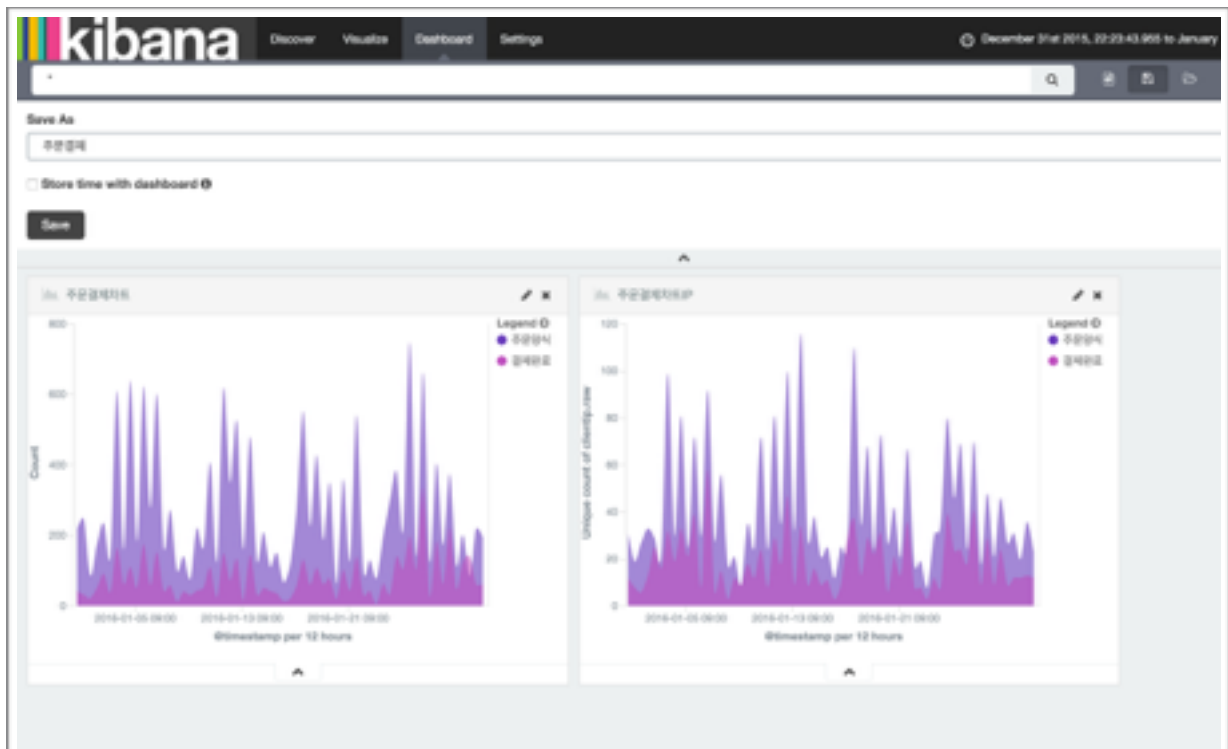
빈 화면이 보이는데, 설명처럼 추가  아이콘을 클릭한다.




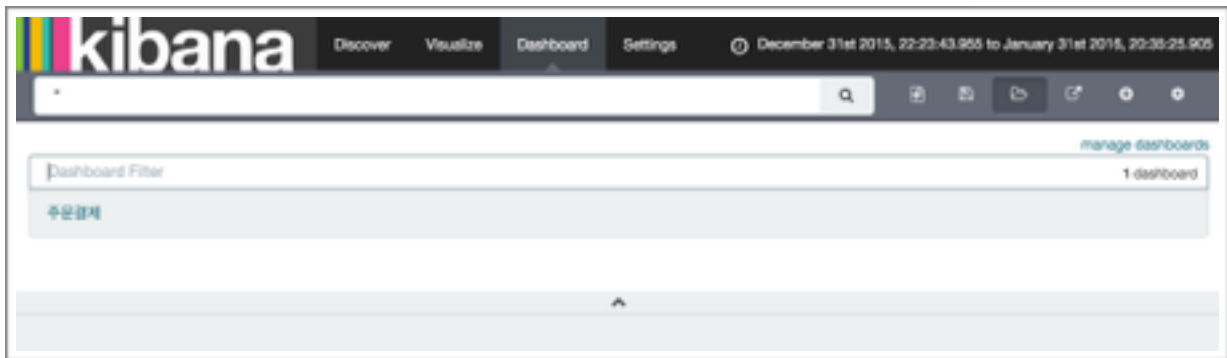
저장된 차트가 보일 것이다. “주문결제차트”, “주문결제차트IP”를 차례대로 클릭하면 자동으로 Dashboard에 추가된다.



화면에 추가된 차트의 우측하단을 클릭해서 드래그하면 크기를 자유롭게 조정할 수 있다. 마찬가지로 완성된 Dashboard를 저장한다. “주문결제”라는 이름으로 저장해 보자. 제목칸 바로 아래 Store time with dashboard 항목을 체크하면 조회한 기간까지 동시에 저장된다. 나중에 불러 올 때에 기간이 적용된 차트를 볼 수 있게 된다.



우측의 열기  아이콘을 클릭하면 저장된 Dashboard가 보인다. 클릭해서 해당 화면을 다시 확인할 수 있다.



#### 4. 기타 기능

이제까지 가장 기본적인 Kibana의 기능들을 알아보았다. 어느 상품을 제일 많이 보았는지, 어느 IP가 어떤 페이지를 거쳐갔는지, 등 검색, 차트, 옵션을 조정해서 데이터를 시각화할 수 있고, 저장한 뒤에 팀원들과도 공유할 수 있다.

#### 5. GA(Google Analytics)와의 차이점

GA는 페이지에 삽입된 JavaScript를 통해서만 통계가 누적된다. 만약 팝업레이어처럼 JavaScript가 실행될 수 없는 화면이라면 GA를 통해서 해당 정보를 볼 수 없다는 뜻이다.

Kibana는 웹서버의 로그파일을 분석하는 것이기 때문에 누락된 정보가 없다. 데이터를 외부 서비스를 통해서 확인하는 것이 아니기 때문에 더 정확한 분석이 가능하다.

#### 6. 참고 자료

\* ELK 스택을 사용한 서울시 지하철 대시보드 만들기

\* [https://youtu.be/ec-XzM6\\_CgU](https://youtu.be/ec-XzM6_CgU)

\* 초간단 ELK 설치하기 동영상

\* <http://bit.ly/okdevtv-elk>