{{ softshake }}

MAKE SENSE OF YOUR (BIG) DATA!

Building analytics live

elasticsearch ?

plug & play

elasticsearch ?

plug & play

elasticsearch ?

Lucene

plug & play

elasticsearch ?

REST

Lucene

plug & play

scalable

elasticsearch ?

REST

Lucene

plug & play

scalable

elasticsearch

Apache 2 license

REST

Lucene

INSTALLATION

```
$ wget https://download.elasticsearch.org/elasticsearch/elasticsearch/
elasticsearch-0.90.5.tar.gz
$ tar -xf elasticsearch-0.90.5.tar.gz
$ ./elasticsearch-0.90.5/bin/elasticsearch -f
... [INFO ][node][Ghost Maker] {0.90.5}[5645]: initializing ...
```

INDEX A DOCUMENT

```
$ curl -XPUT localhost:9200/sessions/session/1 -d '{
  "title" : "Welcome!"
}'
```

UPDATE A DOCUMENT

```
$ curl -XPUT localhost:9200/sessions/session/1 -d '{
    "title"     : "Welcome to the elasticsearch session!",
    "date"      : "2013-10-24T16:30:00",
    "attendees" : 25,
    "tags"      : [ "nosql", "bigdata", "cloud" ],
    "author"    : {
        "first_name" : "David",
        "last_name" : "Pilato",
        "email" : "david.pilato@elasticsearch.com"
    }
}'
```

SEARCH FOR DOCUMENTS

```
$ curl localhost:9200/sessions/_search?q=welcome
```

ELASTICSEARCH

A search engine? For analytics? Seriously?

ELASTICSEARCH

A search engine? For analytics? Seriously?

David Pilato
Technical advocate

elasticsearch.
@dadoonet

elasticsearch.com

David Pilato
Technical advocate

elasticsearch.
@dadoonet

Created in 2012 by elasticsearch authors

- Training (public and on site): http://training.elasticsearch.com/
- Development support: http://elasticsearch.com/support/
- Production support: http://elasticsearch.com/support/

Softshake 2013 sponsor: visit our booth

QUERY DSL & ANALYTICS

```
$ curl localhost:9200/sessions/_search -d '{
   "query": { "bool": { "should": [
       { "match": { "title": "ElASTICsearch" } },
       { "range": { "date": { "from": "2013", "to": "2014" } } }
   ] } },
   "facets": {
      "tags": { "terms": { "field": "tags" } },
      "histo":{ "date_histogram": { "field": "date", "interval": "month" } }
   }
}'
```

RESULTS

```
{   // ... Header
   "hits": { "total": 12638920, "max_score": 1.0010123,
      "hits": [ {
            "_index": "sessions", "_type": "session", "_id": "1",
            "_score": 1.0010123, "_source": {
                  "title": "Welcome to the elasticsearch session!",
                  // ... }
   } ] },
   // ... Facets
}
```

RESULTS

```
{   // ... Header
    "hits": { "total": 12638920, "max_score": 1.0010123,
        "hits": [ {
              "_index": "sessions", "_type": "session", "_id": "1",
              "_score": 1.0010123, "_source": {
                    "title": "Welcome to the elasticsearch session!",
                    // ... }
    } ] },
}
```

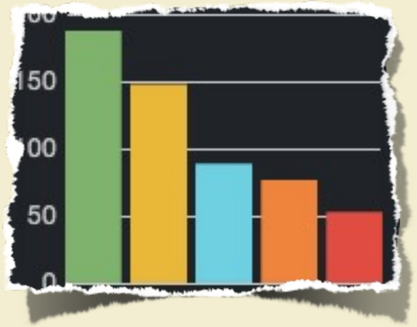
number	state	created_at	closed_at	user.login	title
1	closed	2010-02-09T20:08:08Z	2010-02-09T20:19:00Z	kimchy	Query DSL: Terms Filter
2	closed	2010-02-10T22:10:55Z	2010-02-10T22:12:58Z	kimchy	Discovery: Support local (JVM level) discovery
3	closed	2010-02-11T17:28:41Z	2010-02-11T17:29:31Z	kimchy	Transport: Support local (JVM level) transport
4	closed	2010-02-11T17:51:37Z	2010-02-12T13:17:46Z	simonw	Any plans to add geospatial search?

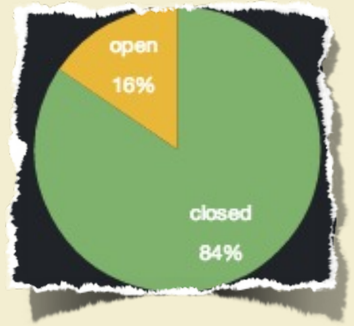
FACETS

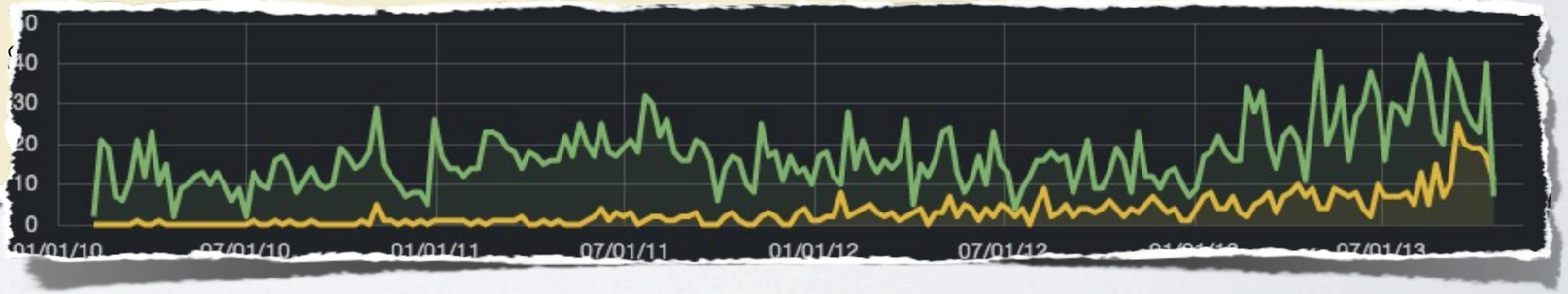
```
{  // ... Header & Hits
   "facets": {
      "tags": { "_type": "terms", "terms": [
            { "term": "nosql", "count": 160 },
            { "term": "cloud", "count": 148 },
            { "term": "bigdata", "count": 82 } ] },
      "histo": {
         "_type": "date_histogram", "entries": [
            { "time": 1380585600000, "count": 1 },
            { "time": 1380598300000, "count": 1 }
         ] } } }
```

FACETS

```
{   // ... Header & Hits
    "facets": {
        "tags": { "_type": "terms", "terms": [
                { "term": "nosql", "count": 160 },
                { "term": "cloud", "count": 148 },
                { "term": "bigdata", "count": 82 } ] },
        "histo": {
            "_type": "date_histogram", "entries": [
                { "time": 1380585600000, "count": 1 },
                { "time": 138059
            ] } } }
```



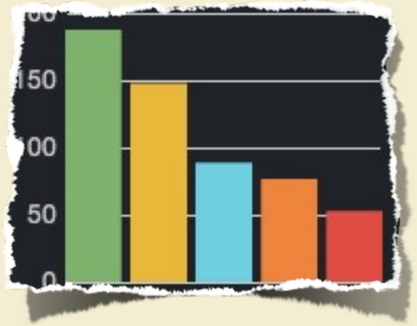


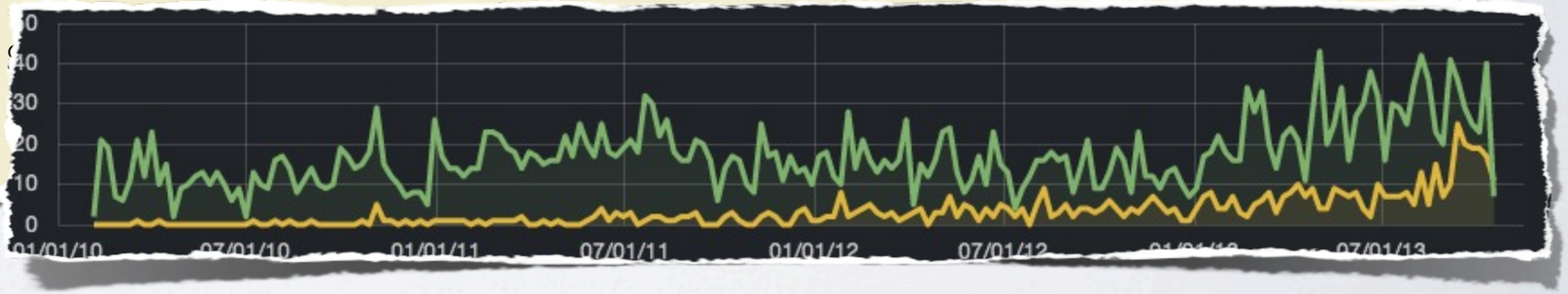


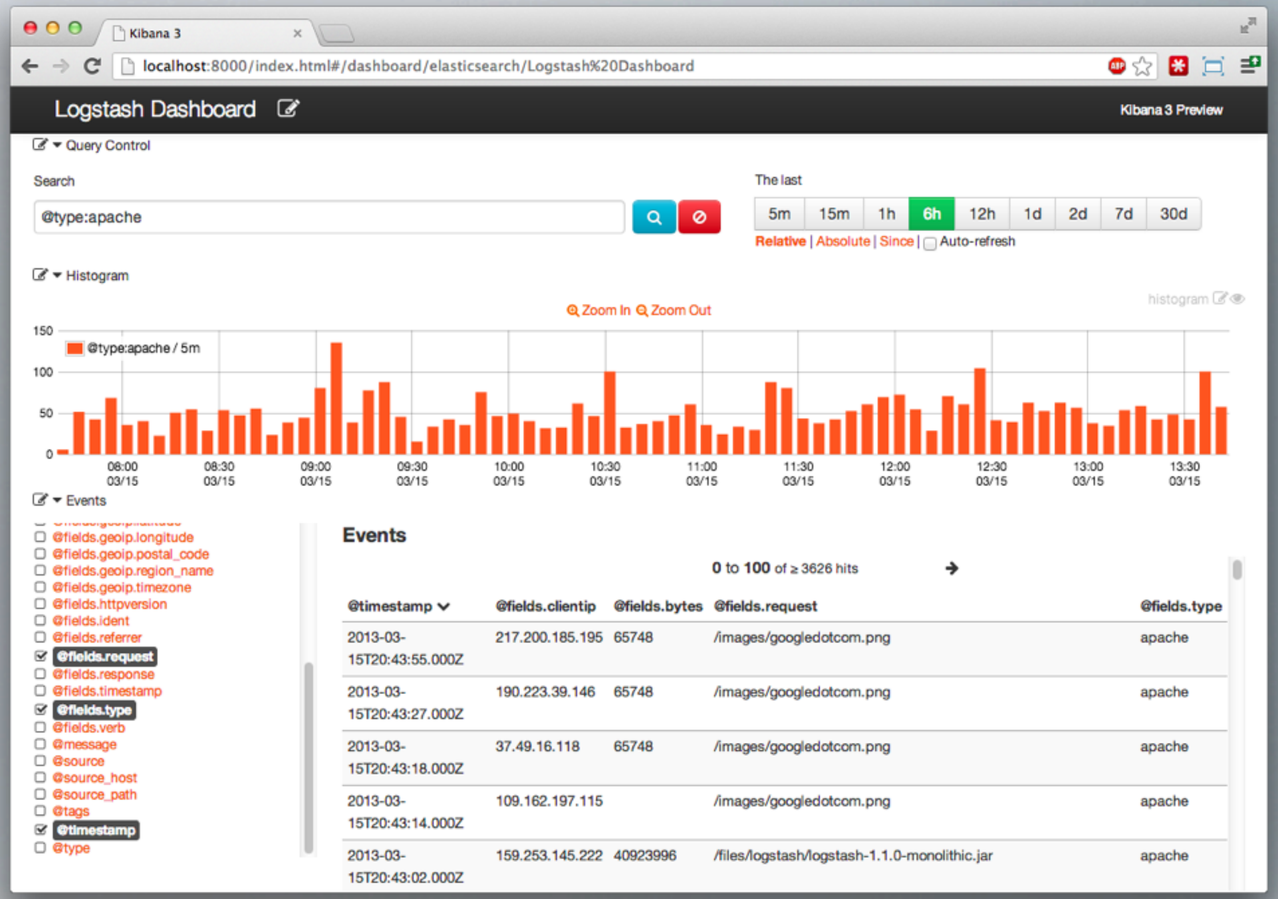
FACETS

```
{   // ... Header & Hits
    "facets": {
        "tags": { "_type": "terms", "terms": [
                { "term": "nosql", "count": 160 },
                { "term": "cloud", "count": 148 },
                { "term": "bigdata", "count": 82 } ] },
        "histo": {
            "_type": "date_histogram", "entries": [
                { "time": 1380585600000, "count": 1 },
                { "time": 138059
            ] } } }
```

Real Time







KIBANA

Yeah! I know! For logs analysis with logstash!

INSTALL KIBANA

```
# Install Kibana as a site plugin and open it in a browser
$ bin/plugin -install elasticsearch/kibana
$ open http://localhost:9200/_plugin/kibana/


# Even better: get the standalone version and add it to your favorite web server
$ wget https://download.elasticsearch.org/kibana/kibana/kibana-3.0.0milestone4.tar.gz
$ tar -xf kibana-3.0.0milestone4.tar.gz
$ vi kibana-3.0.0milestone4/config.js # and set elasticsearch parameter to localhost:9200
$ mv kibana-3.0.0milestone4 /usr/local/apache/htdocs/kibana
$ open http://localhost/kibana/
```

MAKE SENSE OF TWITTER

```
# Add Twitter river: https://github.com/elasticsearch/elasticsearch-river-twitter/
$ bin/plugin -install elasticsearch/elasticsearch-river-twitter/1.4.0


# Start river
$ curl -XPUT localhost:9200/_river/twitter/_meta -d '{
  "type" : "twitter",
  "twitter" : {
    "oauth" : { ... }
  }
}'
```


Make sense of twitter
2 days ago to a few seconds ago
*
Pinned
FR
GB
US
QUERY
FILTERING
HITS
HITS
FR (89) GB (54) US (432) All (41054)
50000
40000
30000
20000
10000
0
TWEET DATE
HISTOGRAM
View | Zoom Out | FR (89) GB (54) US (432) count per 30m | (575 hits)
600
400
200
0
16:00 10/20
00:00 10/21
08:00 10/21
16:00 10/21
00:00 10/22
08:00 10/22
ACCOUNT
TERMS
jeehan983hmd (4) elraiekg (4) alofq_news (4)
Job_Bosch (4) yokel_chang (3)
yokel_chang 16%
jeehan983hmd 21%
Job_Bosch 21%
elraiekg 21%
alofq_news 21%
HASHTAGS
TERMS
gameinsight (160) 142) (غرد_يذكر_الله HoldTight (139) cumanNANYA (90)
androidgames (89)
200
150
100
50
0
TRENDS
TRENDS
0% (FR)
0% (GB)
0% (US)
0% (All)
WORLD MAP
MAP
EUROPEAN MAP
MAP

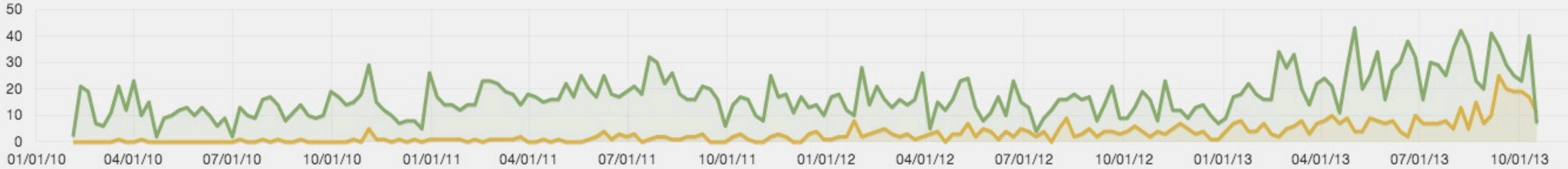
MAKE SENSE OF GITHUB

```
$ curl -i "https://api.github.com/repos/elasticsearch/elasticsearch/issues?state=closed"
{ // Skipped some fields
    "number": 3937,
    "title": "Fix small typo in terms lookup tests mapping.",
    "user": { "login": "mattweber", // Skipped some fields },
    "labels": [ { "name": "bug", "color": "9e2c2c", // Skipped some fields } ],
    "state": "closed",
    "assignee": { "login": "javanna", // Skipped some fields },
    "comments": 2,
    "created_at": "2013-10-18T15:40:25Z",
    "updated_at": "2013-10-18T15:57:23Z",
    "closed_at": "2013-10-18T15:57:23Z",
    "body": "terms -> term and terms -> arr.term as used in the actual tests.  The tests had a
mapping defined but were actually using dynamic mapping since docs were indexing with a field
name other than what was defined in the mapping."
}
```

BY TIME

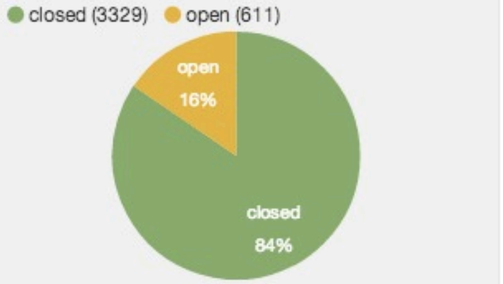
HISTOGRAM

View | Zoom Out | Open (611) Closed (3329) count per **7d** | (**3940** hits)



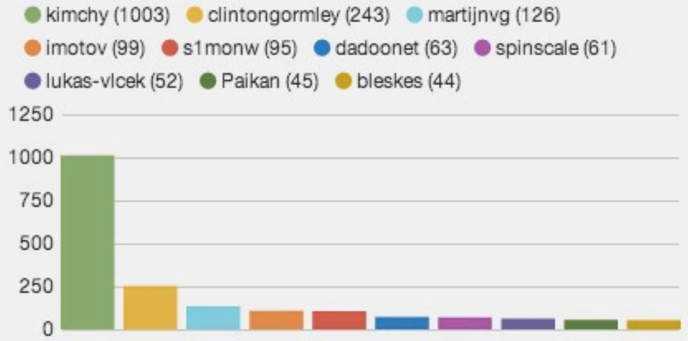
STATE

TERMS



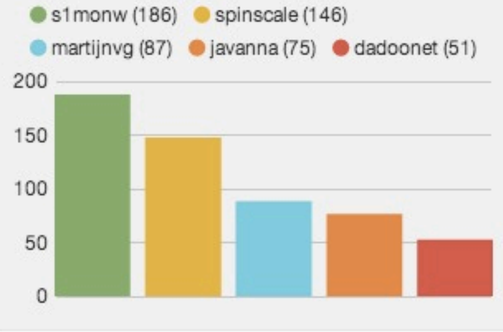
BY REPORTER

TERMS



BY ASSIGNEE

TERMS



TRENDS

TRENDS (6 MONTHS)

▲ 23.99% (Closed)

▲ 64.69% (Open)

▲ 28.93% (All)

ISSUES

TABLE

0 to **100** of 500 available for paging

number	state	created_at	closed_at	user.login	title
1	closed	2010-02-09T20:08:08Z	2010-02-09T20:19:00Z	kimchy	Query DSL: Terms Filter
2	closed	2010-02-10T22:10:55Z	2010-02-10T22:12:58Z	kimchy	Discovery: Support local (JVM level) discovery
3	closed	2010-02-11T17:28:41Z	2010-02-11T17:29:31Z	kimchy	Transport: Support local (JVM level) transport
4	closed	2010-02-11T17:51:37Z	2010-02-12T13:17:46Z	simonw	Any plans to add geospatial search?
5	closed	2010-02-11T17:52:36Z	2010-02-12T13:18:05Z	simonw	Any plans to support faceting?
6	closed	2010-02-12T13:20:07Z	2010-02-12T13:24:25Z	kimchy	Query DSL: Bool query/filter to be valid JSON
7	closed	2010-02-12T16:08:42Z	2010-02-12T16:09:21Z	kimchy	Discovery/Jgroups: Upgrade to 2.9.0

MAKE SENSE OF MARKETING DATA

```
$ curl "localhost:9200/person/person/hYlnmjhLT5iQfjO9Kr9X5w"
{
   "name":"Pilato David",
   "dateOfBirth":"1971-12-26",
   "gender":"male",
   "marketing":{
      "fashion":334,
      "music":3363,
      "hifi":2351
   },
   "address":{
      "country":"France",
      "city":"Paris",
      "countrycode":"FR"
   }
}
```


Hifi and Fashion
Set a time filter
QUERY
FILTERING
Toggle query
DATE OF BIRTH
HISTOGRAM
View | Zoom Out | Hifi (102885) Fashion (86811) count per 1y | (189696 hits)
3000
2000
1000
0
01/45
01/50
01/55
01/60
01/65
01/70
01/75
01/80
01/85
01/90
01/95
01/00
01/05
HITS
HITS
Hifi (102885) Fashion (86811)
120000
100000
80000
60000
40000
20000
0
RESULTS
TABLE
0 to 100 of 500 available for paging
name
gender
dateOfBirth
address.country
marketing.hifi
marketing.fashion
Ludmila Rachel female 2009-12-28 France 1092
Kenzi Helene male 2009-12-28 Germany 1213
Elsa Angele female 2009-12-28 England 1161
Florence Naomie female 2009-12-28 England 1543
Adrien Halima male 2009-12-28 France 1240
Nils Rosalie male 2009-12-28 Germany 1112
GENDER
TERMS
female (91891) male (88691)
male
49%
female
51%
COUNTRY
MAP
CITIES
TERMS
plymouth (30120) bonn (30036) liverpool (15242) barcelona (15083)
nantes (15053) munich (14960) london (14921) berlin (14890)
pampelune (6188) madrid (4637)
40000
30000
20000
10000
0

MAKE SENSE OF YOUR (BIG) DATA!

Building analytics live

That's all Folks!

Any Question ?

{{ softshake }}

David Pilato
Technical advocate

elasticsearch.
@dadoonet