elasticsearch
for developer

Workshop with log

SPRINT3R

Siam Chamnankit Co., Ltd., Odd-e (Thailand) Co., Ltd. and Alliance

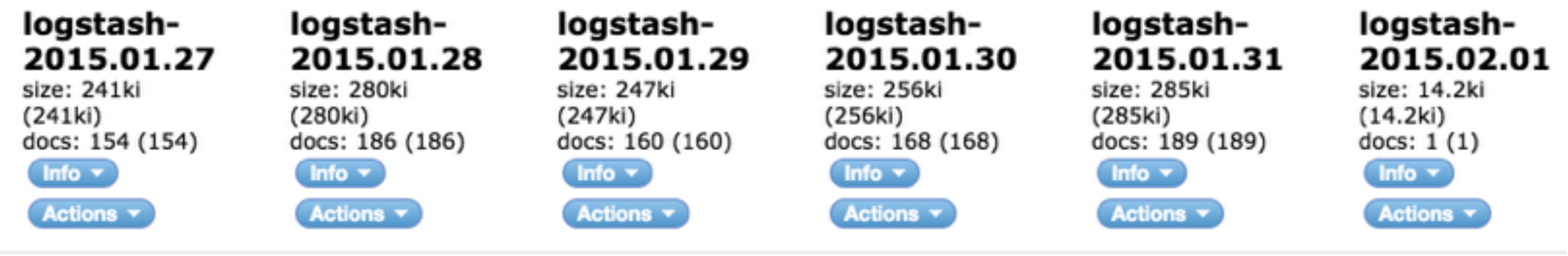
Install log generator

```
$npm install -g makelogs
```

https://www.npmjs.com/package/makelogs

Log generator

```
$makelogs --count=1000 --days=-5,0  --host=localhost:9200
```



logstash-2015.01.27
size: 241ki (241ki)
docs: 154 (154)

logstash-2015.01.28
size: 280ki (280ki)
docs: 186 (186)

logstash-2015.01.29
size: 247ki (247ki)
docs: 160 (160)

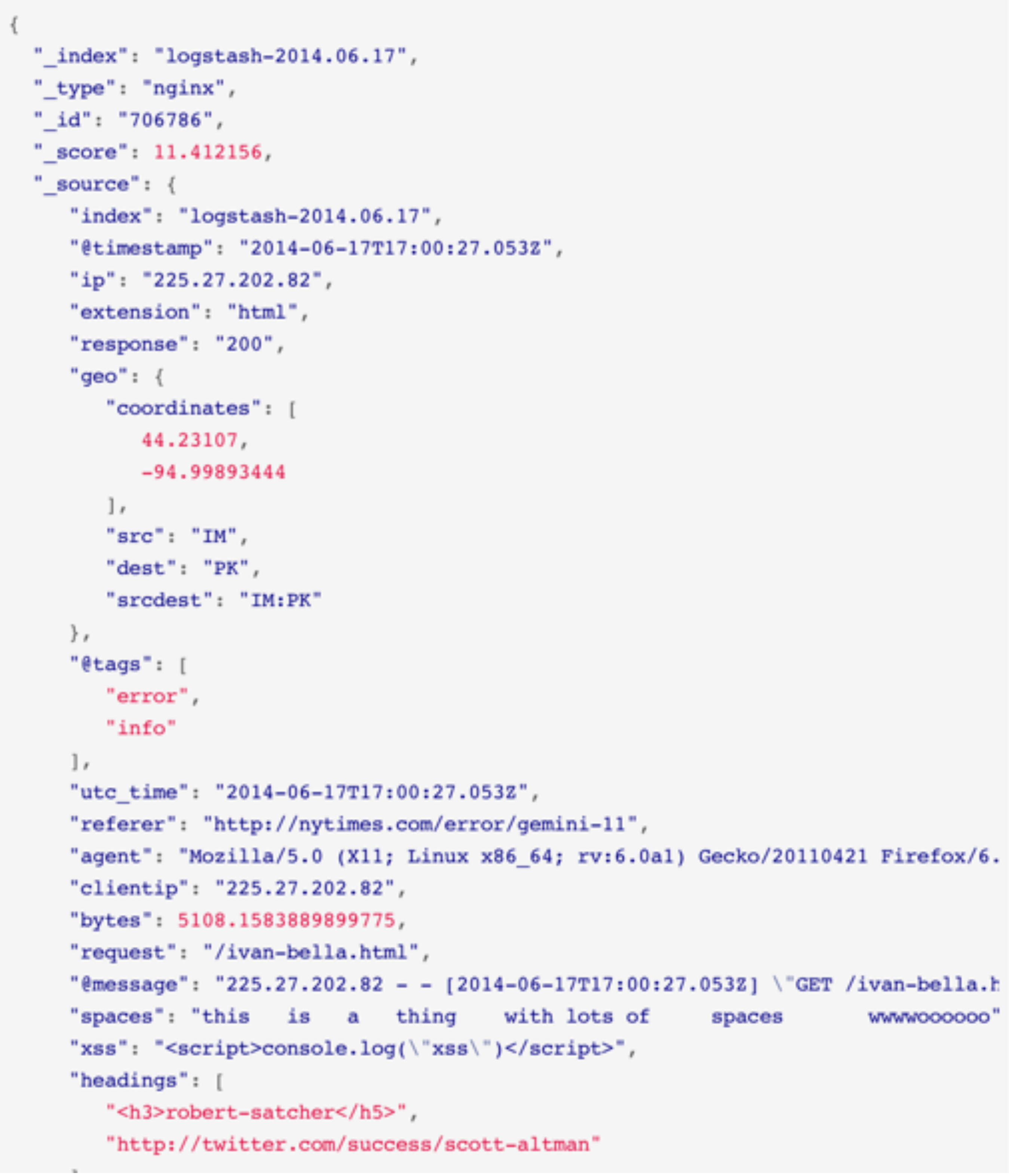
logstash-2015.01.30
size: 256ki (256ki)
docs: 168 (168)

logstash-2015.01.31
size: 285ki (285ki)
docs: 189 (189)

logstash-2015.02.01
size: 14.2ki (14.2ki)
docs: 1 (1)

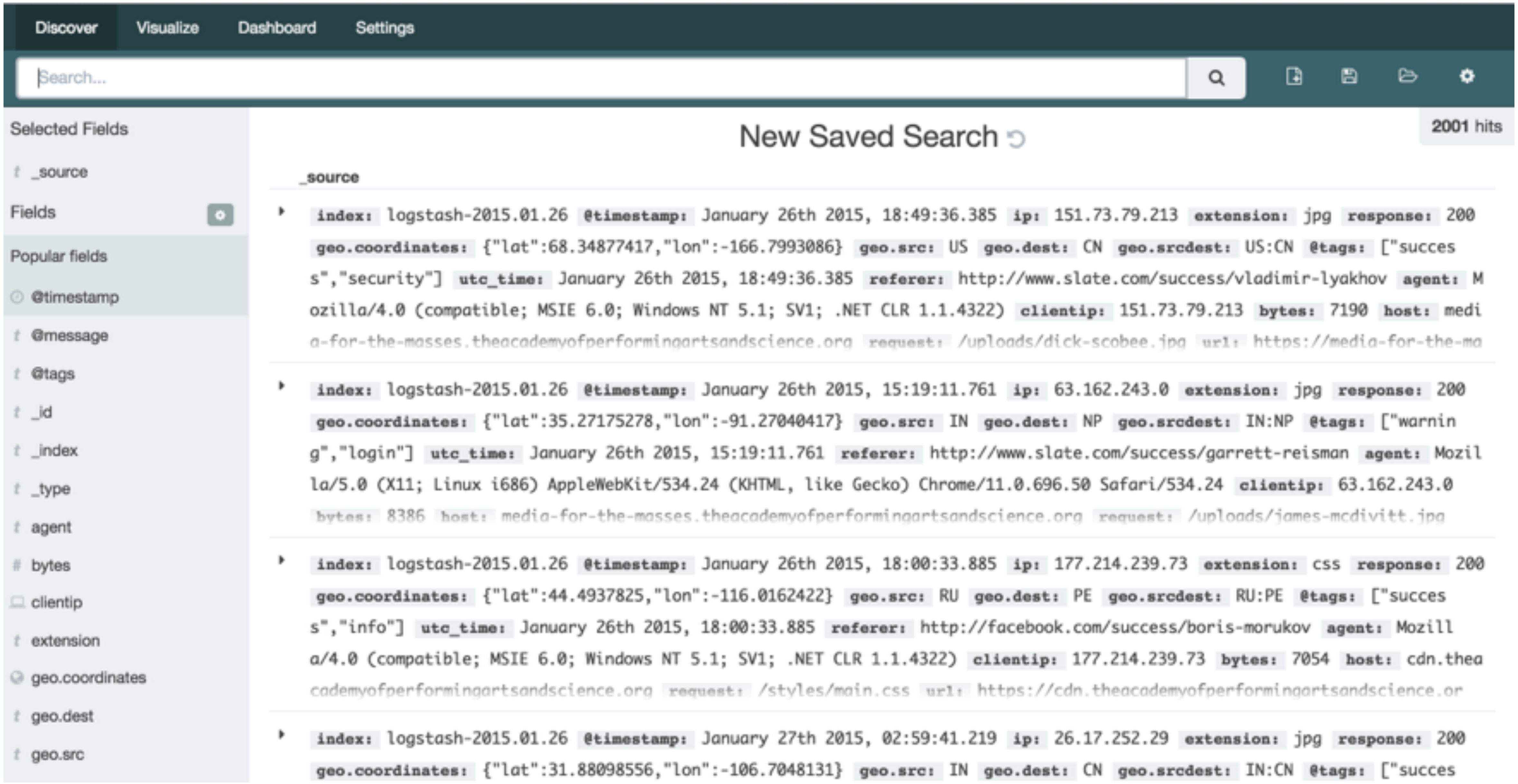
https://www.npmjs.com/package/makelogs

Example data



```
{
  "_index": "logstash-2014.06.17",
  "_type": "nginx",
  "_id": "706786",
  "_score": 11.412156,
  "_source": {
     "index": "logstash-2014.06.17",
     "@timestamp": "2014-06-17T17:00:27.053Z",
     "ip": "225.27.202.82",
     "extension": "html",
     "response": "200",
     "geo": {
        "coordinates": [
           44.23107,
           -94.99893444
        ],
        "src": "IM",
        "dest": "PK",
        "srcdest": "IM:PK"
     },
     "@tags": [
        "error",
        "info"
     ],
     "utc_time": "2014-06-17T17:00:27.053Z",
     "referer": "http://nytimes.com/error/gemini-11",
     "agent": "Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.
     "clientip": "225.27.202.82",
     "bytes": 5108.1583889899775,
     "request": "/ivan-bella.html",
     "@message": "225.27.202.82 - - [2014-06-17T17:00:27.053Z] \"GET /ivan-bella.h
     "spaces": "this   is   a   thing    with lots of     spaces       wwwwoooooo"
     "xss": "<script>console.log(\"xss\")</script>",
     "headings": [
        "<h3>robert-satcher</h5>",
        "http://twitter.com/success/scott-altman"
```

Discover data



New Saved Search

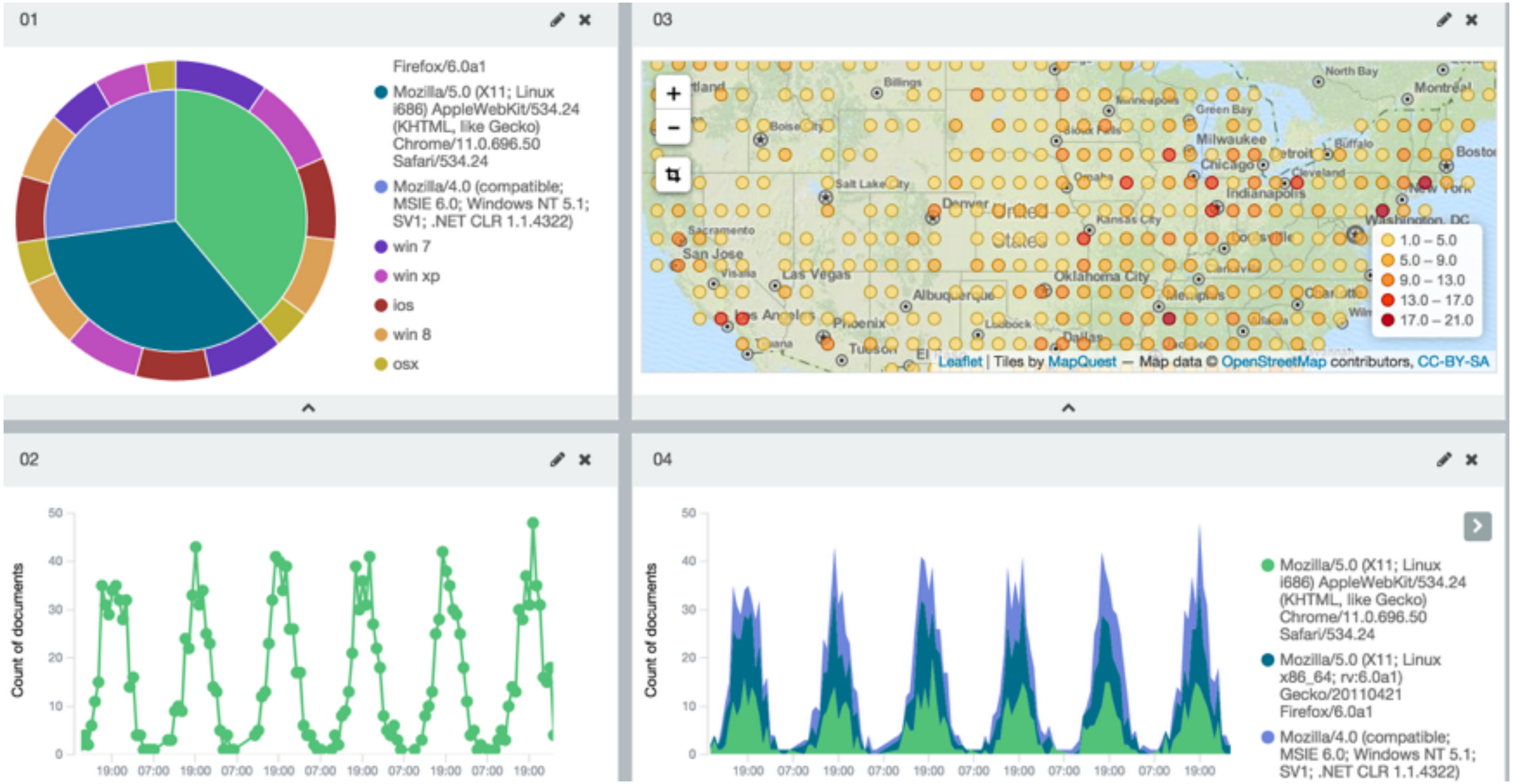
```
index: logstash-2015.01.26 @timestamp: January 26th 2015, 18:49:36.385 ip: 151.73.79.213 extension: jpg response: 200
geo.coordinates: {"lat":68.34877417,"lon":-166.7993086} geo.src: US geo.dest: CN geo.srcdest: US:CN @tags: ["succes
s","security"] utc_time: January 26th 2015, 18:49:36.385 referer: http://www.slate.com/success/vladimir-lyakhov agent: M
ozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) clientip: 151.73.79.213 bytes: 7190 host: medi
a-for-the-masses.theacademyofperformingartsandscience.org request: /uploads/dick-scobee.jpg url: https://media-for-the-ma

index: logstash-2015.01.26 @timestamp: January 26th 2015, 15:19:11.761 ip: 63.162.243.0 extension: jpg response: 200
geo.coordinates: {"lat":35.27175278,"lon":-91.27040417} geo.src: IN geo.dest: NP geo.srcdest: IN:NP @tags: ["warnin
g","login"] utc_time: January 26th 2015, 15:19:11.761 referer: http://www.slate.com/success/garrett-reisman agent: Mozil
la/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24 clientip: 63.162.243.0
bytes: 8386 host: media-for-the-masses.theacademyofperformingartsandscience.org request: /uploads/james-mcdivitt.jpg

index: logstash-2015.01.26 @timestamp: January 26th 2015, 18:00:33.885 ip: 177.214.239.73 extension: css response: 200
geo.coordinates: {"lat":44.4937825,"lon":-116.0162422} geo.src: RU geo.dest: PE geo.srcdest: RU:PE @tags: ["succes
s","info"] utc_time: January 26th 2015, 18:00:33.885 referer: http://facebook.com/success/boris-morukov agent: Mozill
a/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) clientip: 177.214.239.73 bytes: 7054 host: cdn.thea
cademyofperformingartsandscience.org request: /styles/main.css url: https://cdn.theacademyofperformingartsandscience.or

index: logstash-2015.01.26 @timestamp: January 27th 2015, 02:59:41.219 ip: 26.17.252.29 extension: jpg response: 200
geo.coordinates: {"lat":31.88098556,"lon":-106.7048131} geo.src: IN geo.dest: CN geo.srcdest: IN:CN @tags: ["succes
```

Try with kibana


01
Firefox/6.0a1
● Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24
● Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
● win 7
● win xp
● ios
● win 8
● osx
03
+
−
Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA
● 1.0 – 5.0
● 5.0 – 9.0
● 9.0 – 13.0
● 13.0 – 17.0
● 17.0 – 21.0
United States
Salt Lake City
Denver
Kansas City
Oklahoma City
Albuquerque
Phoenix
Tucson
Las Vegas
Los Angeles
San Jose
Sacramento
Chicago
Milwaukee
Detroit
Indianapolis
Washington, DC
New York
Boston
Montreal
Dallas
Memphis
02
Count of documents
50
40
30
20
10
0
19:00
07:00
04
Count of documents
● Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24
● Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1
● Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)