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

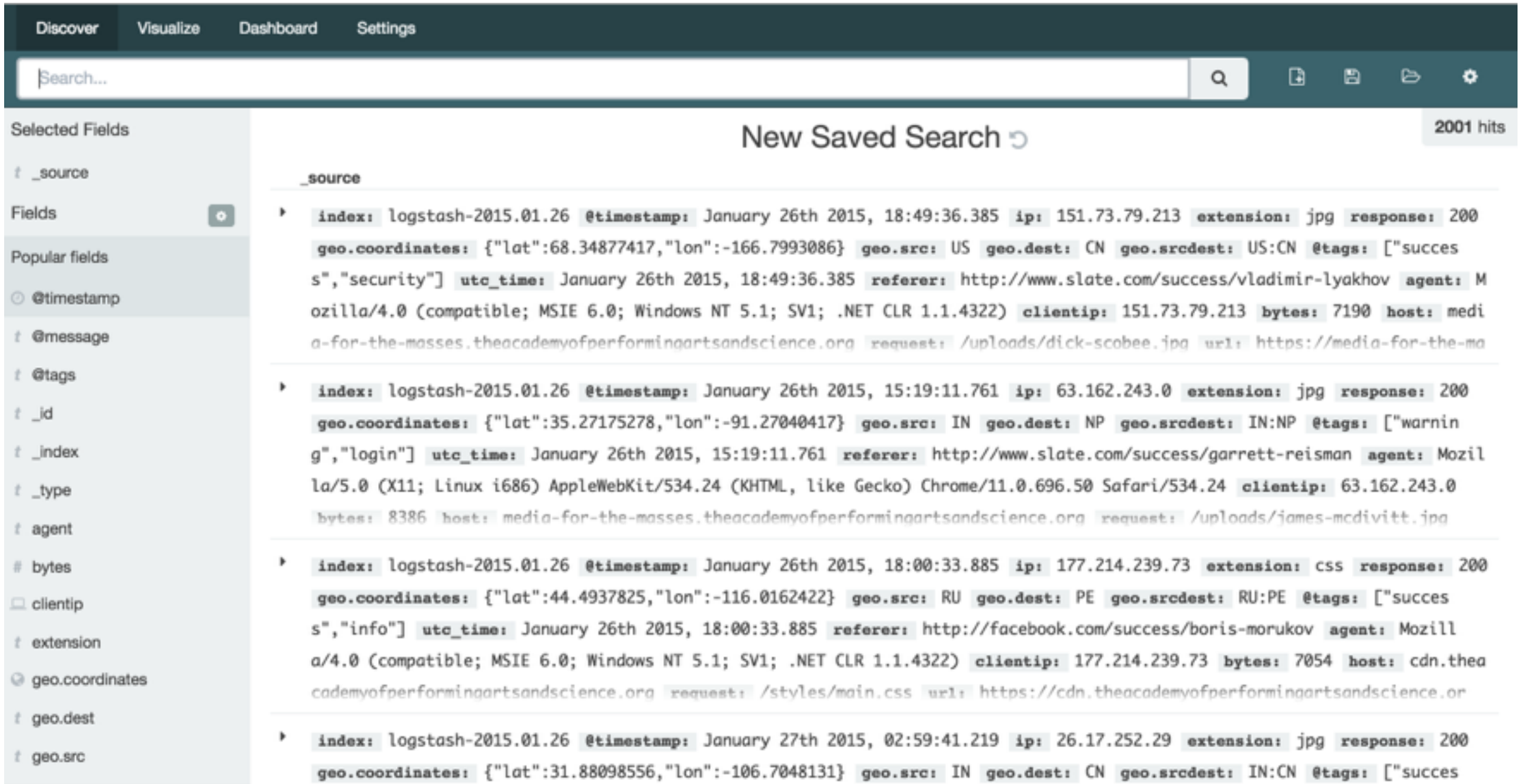
$makelogs --count=1000 --days=-5,0 --host=localhost:9200

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



Try with kibana