



Workshop with log

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) Info Actions	logstash-2015.01.28 size: 280ki (280ki) docs: 186 (186) Info Actions	logstash-2015.01.29 size: 247ki (247ki) docs: 160 (160) Info Actions	logstash-2015.01.30 size: 256ki (256ki) docs: 168 (168) Info Actions	logstash-2015.01.31 size: 285ki (285ki) docs: 189 (189) Info Actions	logstash-2015.02.01 size: 14.2ki (14.2ki) docs: 1 (1) Info Actions
---	---	---	---	---	---

<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

The screenshot displays the Elastic Stack Discover interface. The top navigation bar includes 'Discover', 'Visualize', 'Dashboard', and 'Settings'. A search bar is present with the placeholder text 'Search...'. On the left sidebar, under 'Selected Fields', the field '_source' is listed. The 'Fields' section shows a list of fields including '@timestamp', '@message', '@tags', '_id', '_index', '_type', 'agent', 'bytes', 'clientip', 'extension', 'geo.coordinates', 'geo.dest', and 'geo.src'. The main area shows a 'New Saved Search' with 2001 hits. The search results are displayed as a list of logstash events, each with a timestamp and various fields like index, @timestamp, ip, extension, response, geo.coordinates, geo.src, geo.dest, geo.srcdest, @tags, utc_time, referer, agent, clientip, bytes, host, request, and url.

index	@timestamp	ip	extension	response	geo.coordinates	geo.src	geo.dest	geo.srcdest	@tags	utc_time	referer	agent	clientip	bytes	host	request	url
logstash-2015.01.26	January 26th 2015, 18:49:36.385	151.73.79.213	jpg	200	{"lat":68.34877417,"lon":-166.7993086}	US	CN	US:CN	["success","security"]	January 26th 2015, 18:49:36.385	http://www.slate.com/success/vladimir-lyakhov	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)	151.73.79.213	7190	media-for-the-masses.theacademyofperformingartsandscience.org	/uploads/dick-scobee.jpg	https://media-for-the-ma
logstash-2015.01.26	January 26th 2015, 15:19:11.761	63.162.243.0	jpg	200	{"lat":35.27175278,"lon":-91.27040417}	IN	NP	IN:NP	["warning","login"]	January 26th 2015, 15:19:11.761	http://www.slate.com/success/garrett-reisman	Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24	63.162.243.0	8386	media-for-the-masses.theacademyofperformingartsandscience.org	/uploads/james-mcdivitt.jpg	
logstash-2015.01.26	January 26th 2015, 18:00:33.885	177.214.239.73	css	200	{"lat":44.4937825,"lon":-116.0162422}	RU	PE	RU:PE	["success","info"]	January 26th 2015, 18:00:33.885	http://facebook.com/success/boris-morukov	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)	177.214.239.73	7054	cdn.theacademyofperformingartsandscience.org	/styles/main.css	https://cdn.theacademyofperformingartsandscience.or
logstash-2015.01.26	January 27th 2015, 02:59:41.219	26.17.252.29	jpg	200	{"lat":31.88098556,"lon":-106.7048131}	IN	CN	IN:CN	["success","info"]	January 27th 2015, 02:59:41.219	http://www.slate.com/success/garrett-reisman	Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24	26.17.252.29	8386	media-for-the-masses.theacademyofperformingartsandscience.org	/uploads/james-mcdivitt.jpg	

Try with kibana

