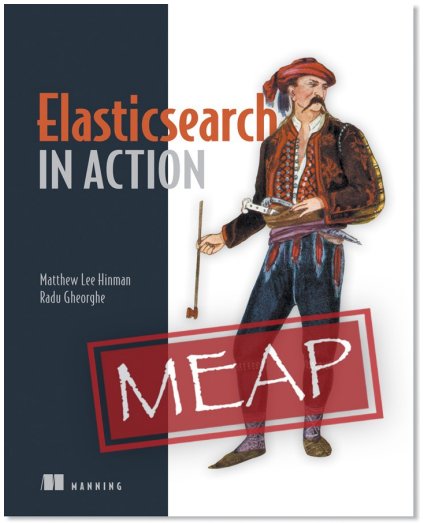
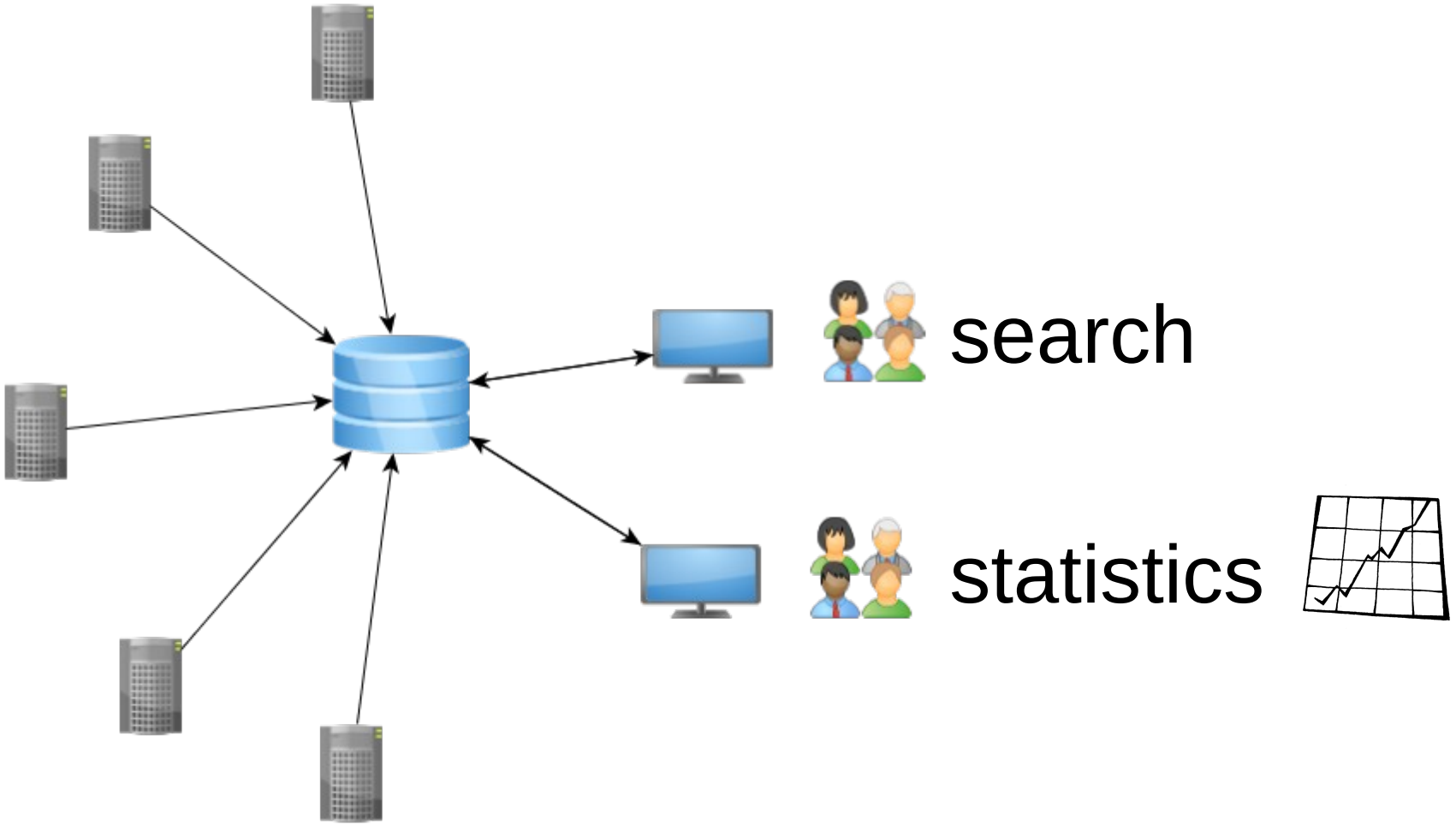
JSON Logging with Elasticsearch

sematext

Radu Gheorghe

sematext

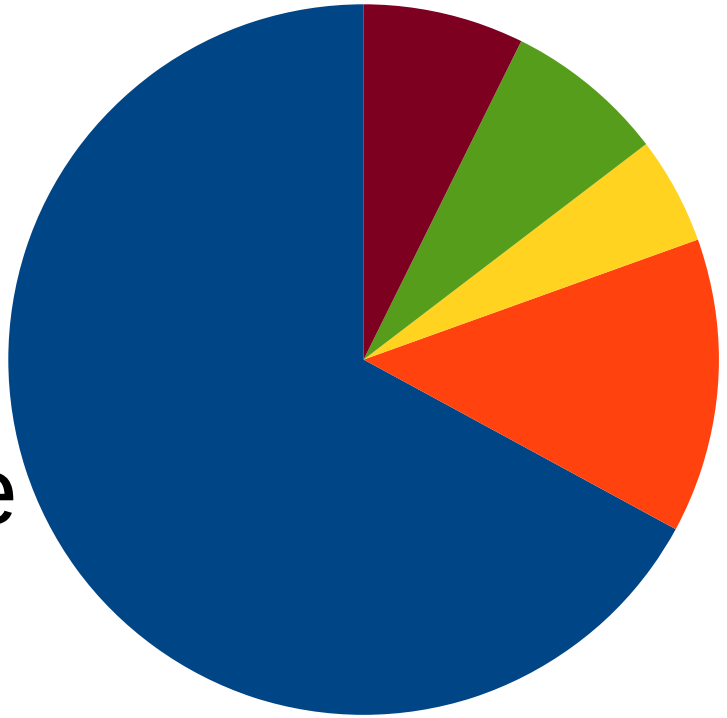

Elasticsearch
IN ACTION
Matthew Lee Hinman
Radu Gheorghe
MEAP
MANNING


search
statistics

Where do your logs end up?

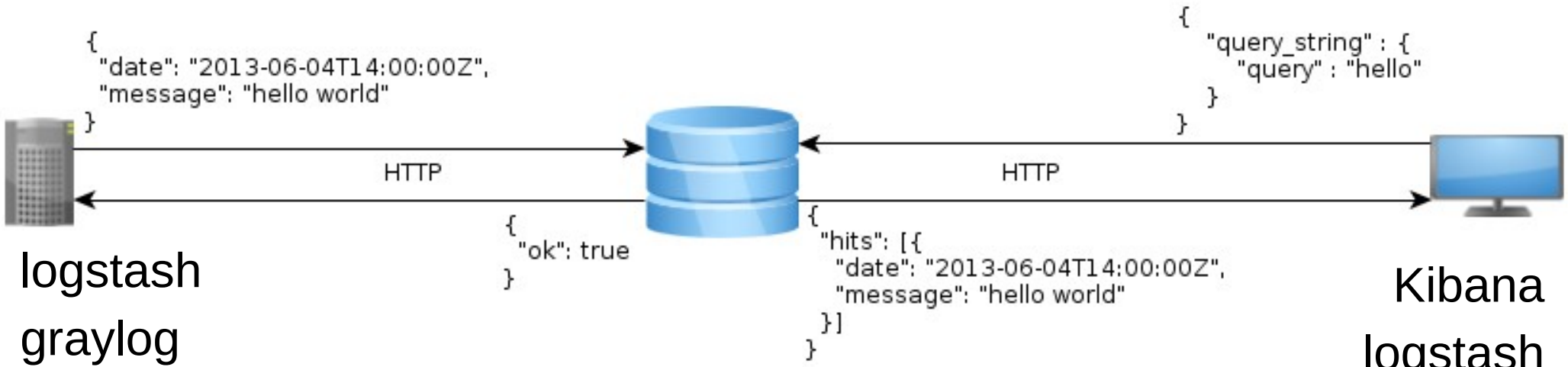
fast

scalable



- Elasticsearch
- Splunk
- MongoDB
- file system
- other

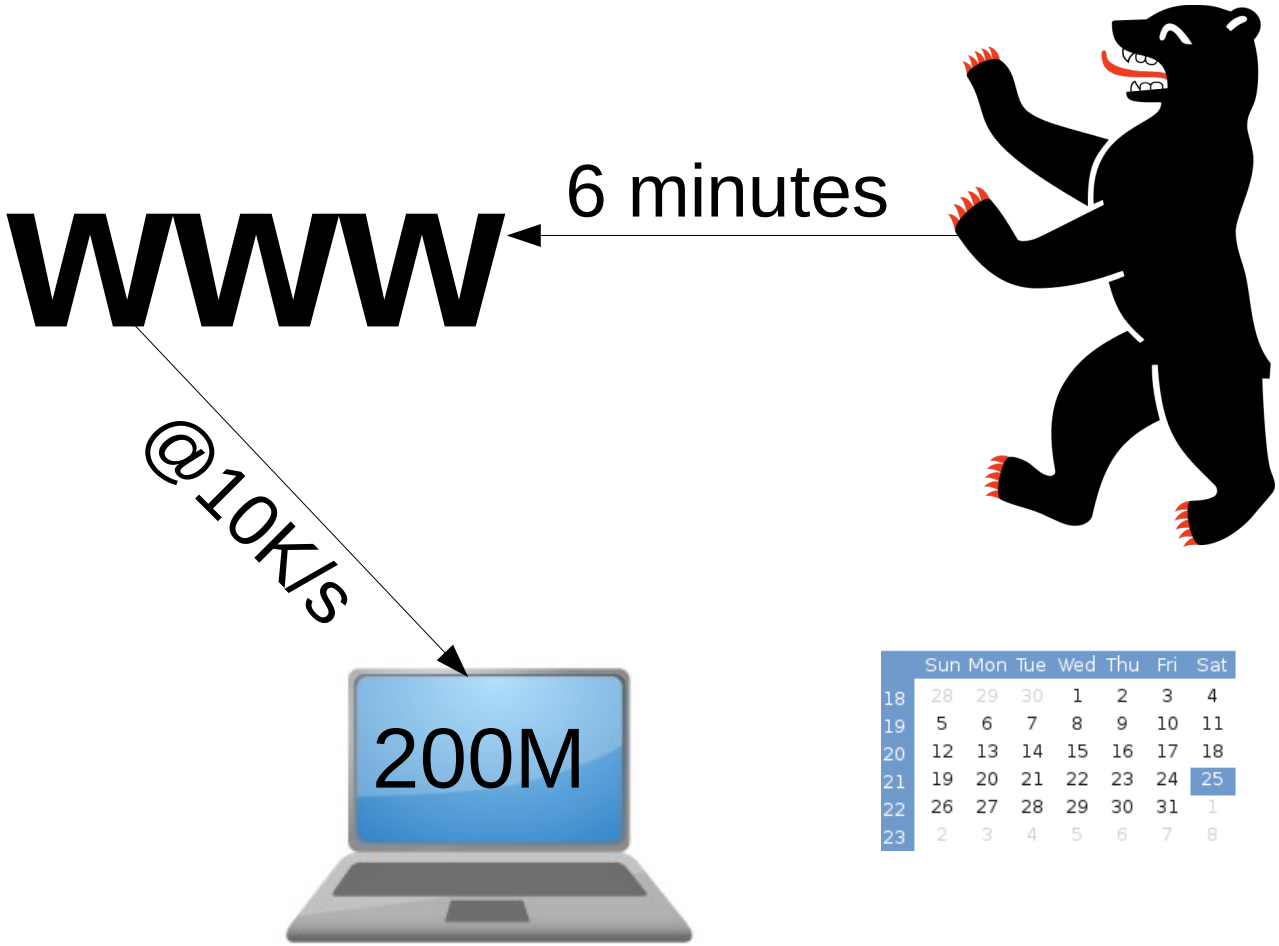
STORE



logstash
graylog
rsyslog
fluentd
Apache Flume

Kibana
logstash
graylog
Elasticsearch Head

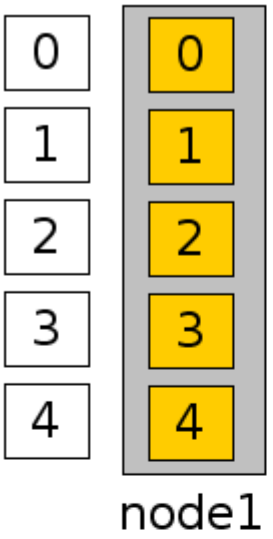
STORE



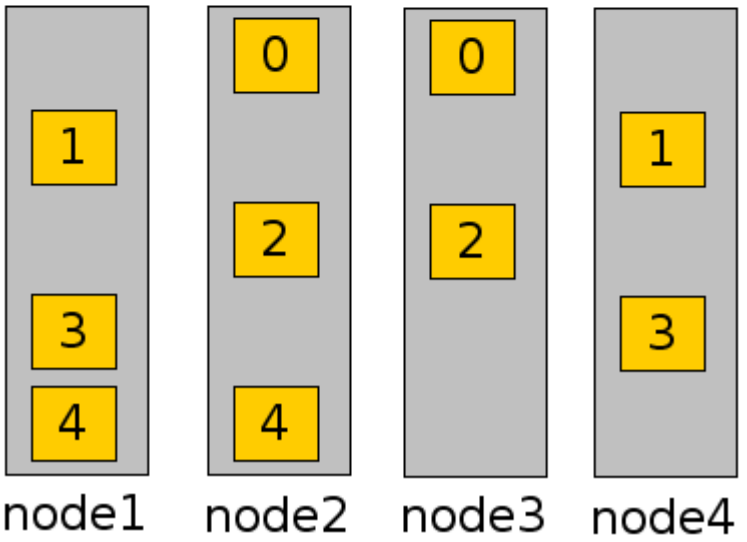
	Sun	Mon	Tue	Wed	Thu	Fri	Sat
18	28	29	30	1	2	3	4
19	5	6	7	8	9	10	11
20	12	13	14	15	16	17	18
21	19	20	21	22	23	24	25
22	26	27	28	29	30	31	1
23	2	3	4	5	6	7	8

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
18	28	29	30	1	2	3	4
19	5	6	7	8	9	10	11
20	12	13	14	15	16	17	18
21	19	20	21	22	23	24	25
22	26	27	28	29	30	31	1
23	2	3	4	5	6	7	8

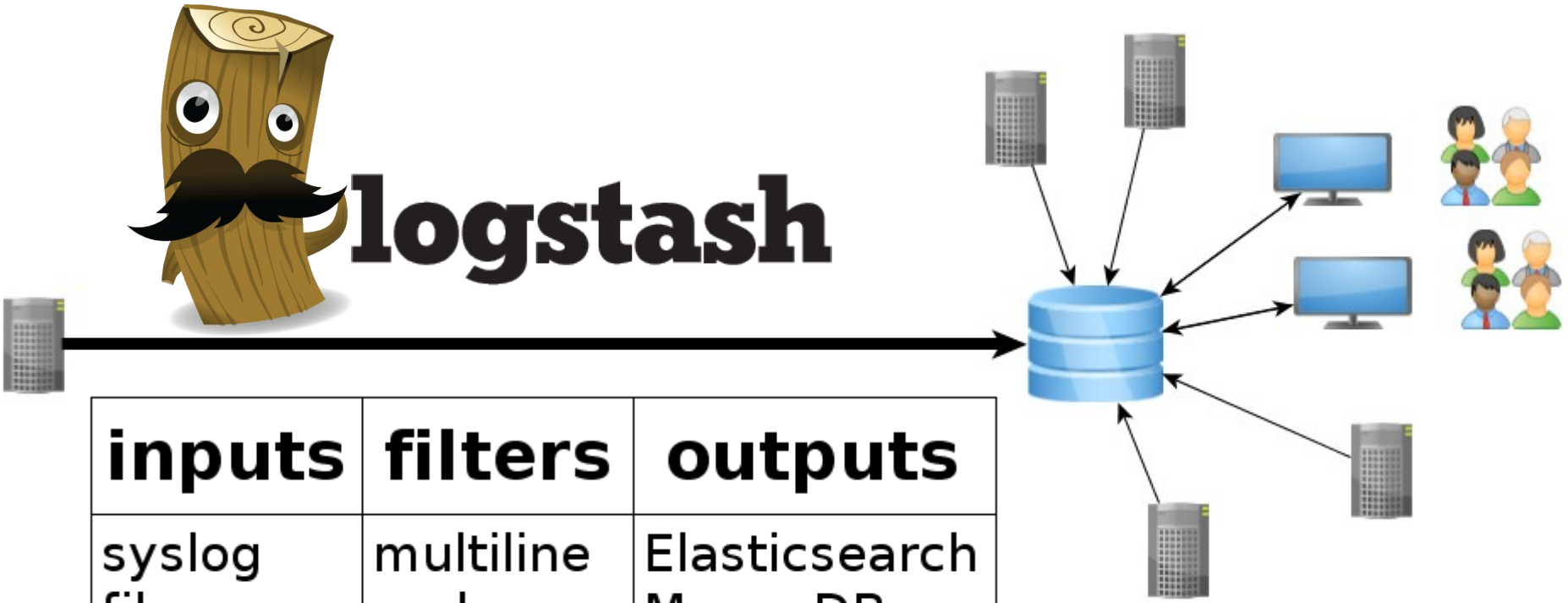
now



later

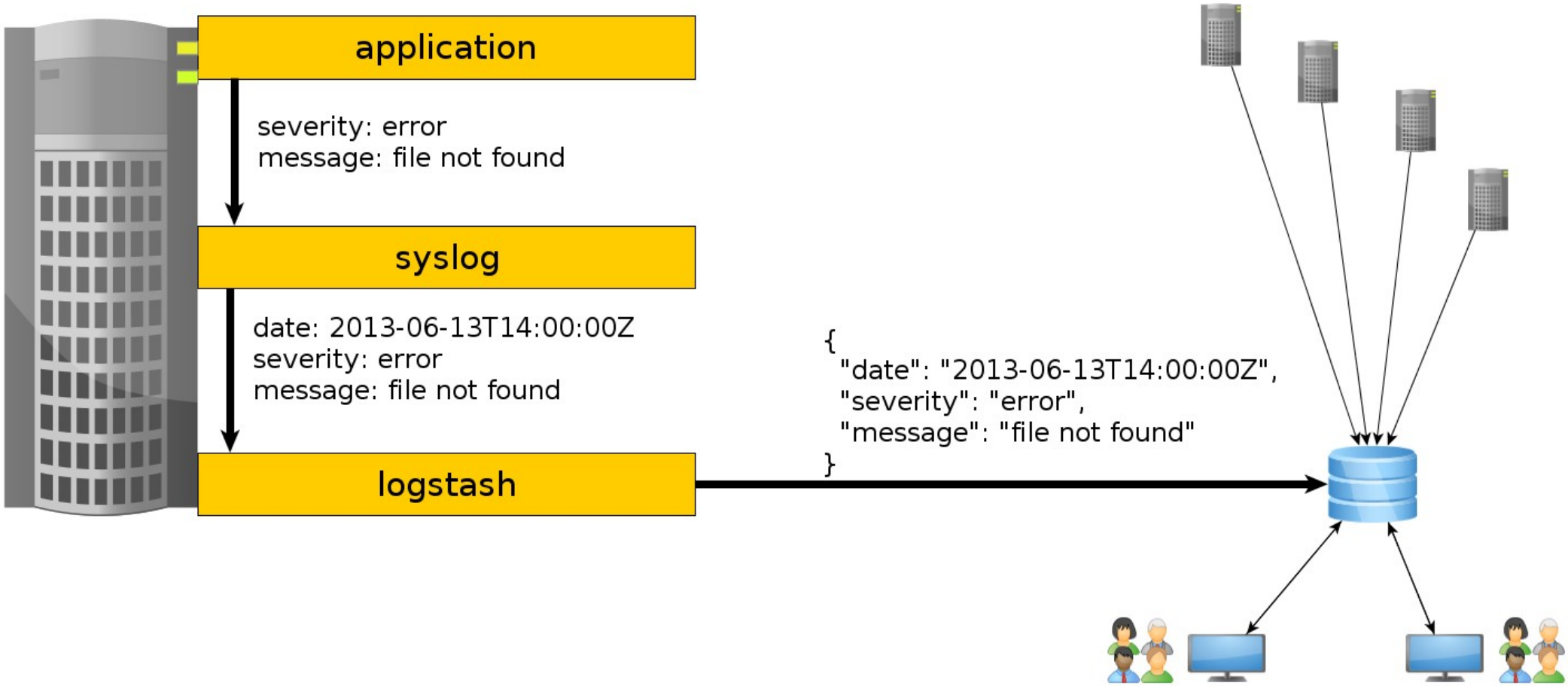


STORE SEND



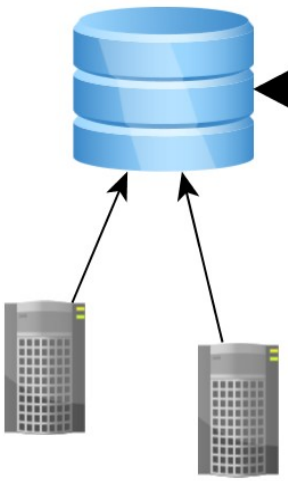
inputs	filters	outputs
syslog file imap +32	multiline grok date +26	Elasticsearch MongoDB Nagios +44

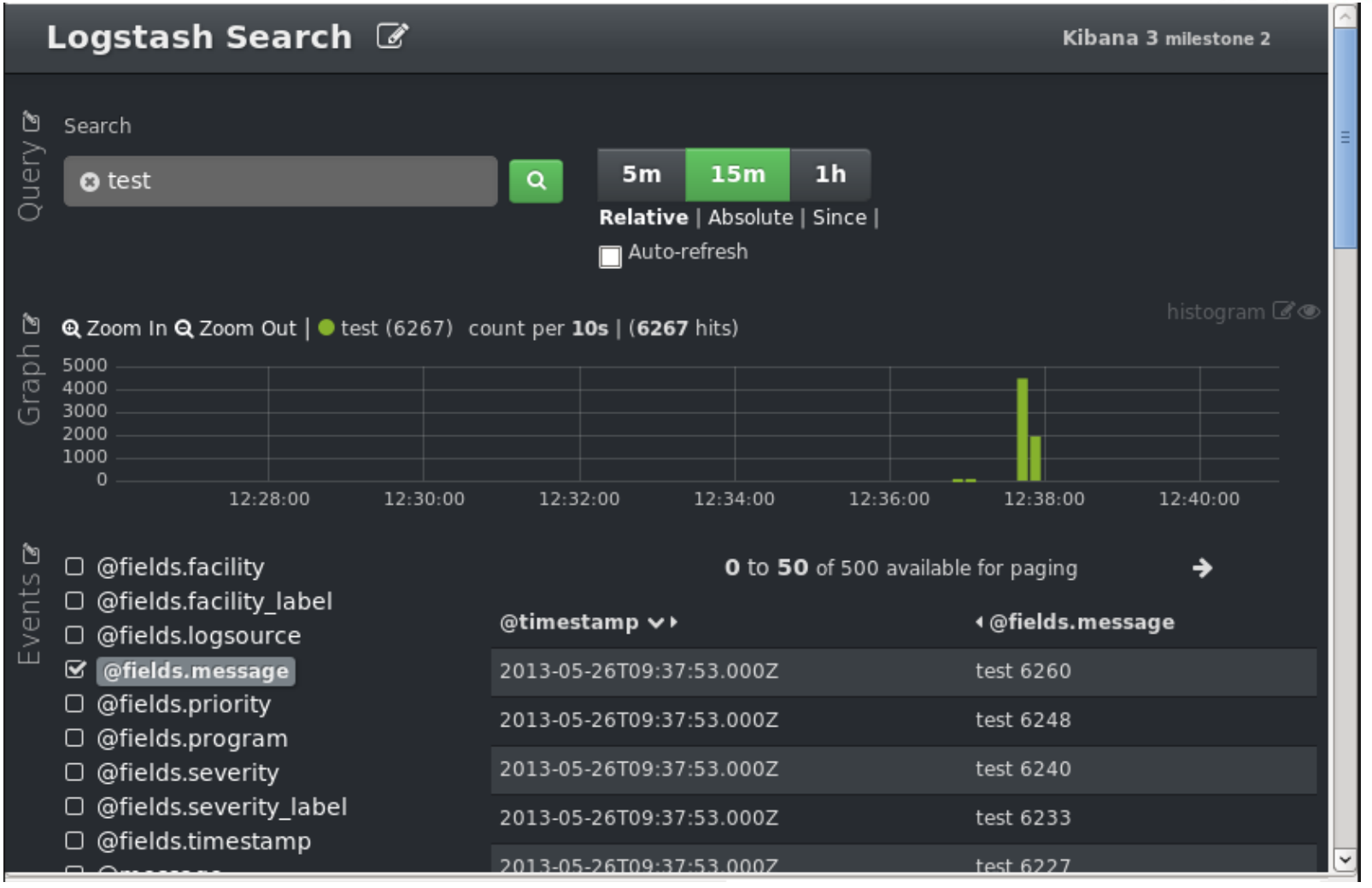
STORE SEND


application
severity: error
message: file not found
syslog
date: 2013-06-13T14:00:00Z
severity: error
message: file not found
logstash
{
"date": "2013-06-13T14:00:00Z",
"severity": "error",
"message": "file not found"
}

STORE SEND SEARCH

Kibana





userID item

Mike 20 mouse 0

time error code


```
{
  "userID": "Mike",
  "time": 20,
  "item": "mouse",
  "errorCode": 0
}
```

Mike 20 mouse 0

```
filter {
  grok {
    type => "unstructured"
    pattern => "%{WORD:userID} %{NUMBER:time} %{WORD:item} %{NUMBER:errorCode}"
  }
}
```

```
{
  "userID": "Mike",
  "time": 20,
  "item": "mouse",
  "errorCode": 0
}
```

Mike 20 mouse **firefox** 0

```
filter {
  grok {
    type => "unstructured"
    pattern => "%{WORD:user} %{NUMBER:time} %{WORD:item} %{NUMBER:errorCode}"
  }
}
```

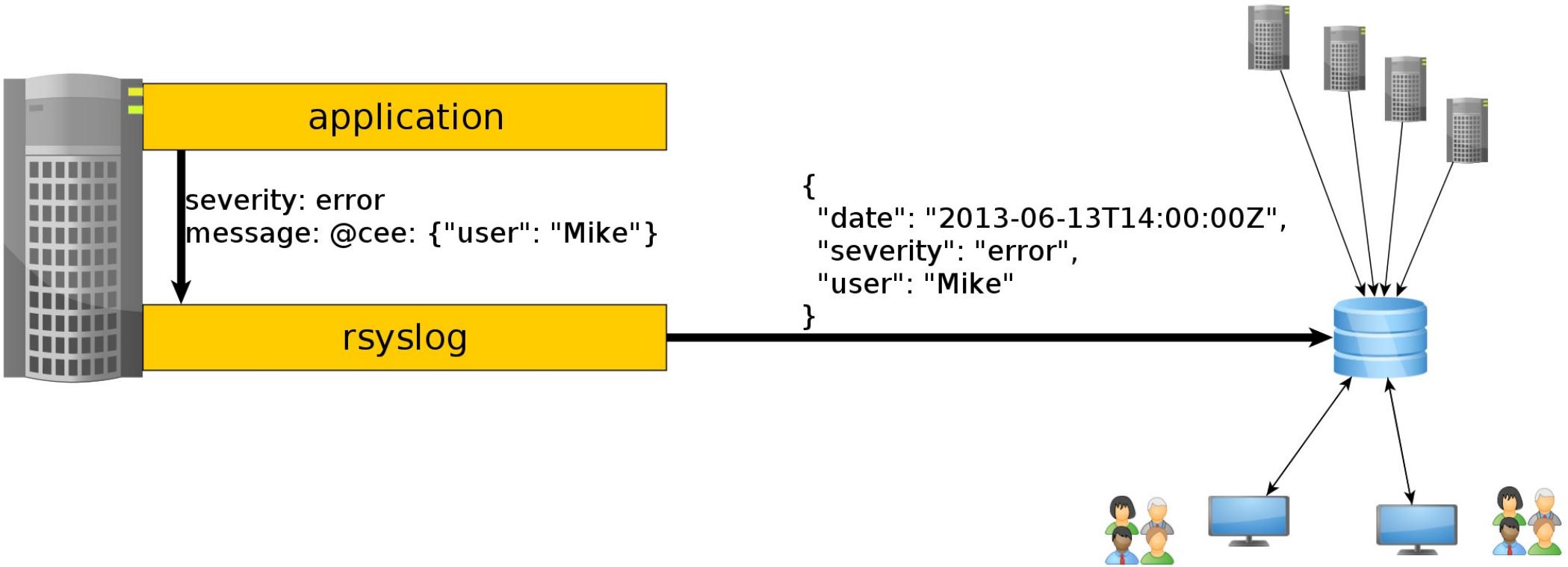
```
{
  "userID": "Mike",
  "time": 20,
  "item": "mouse",
  "errorCode": 0
}
```

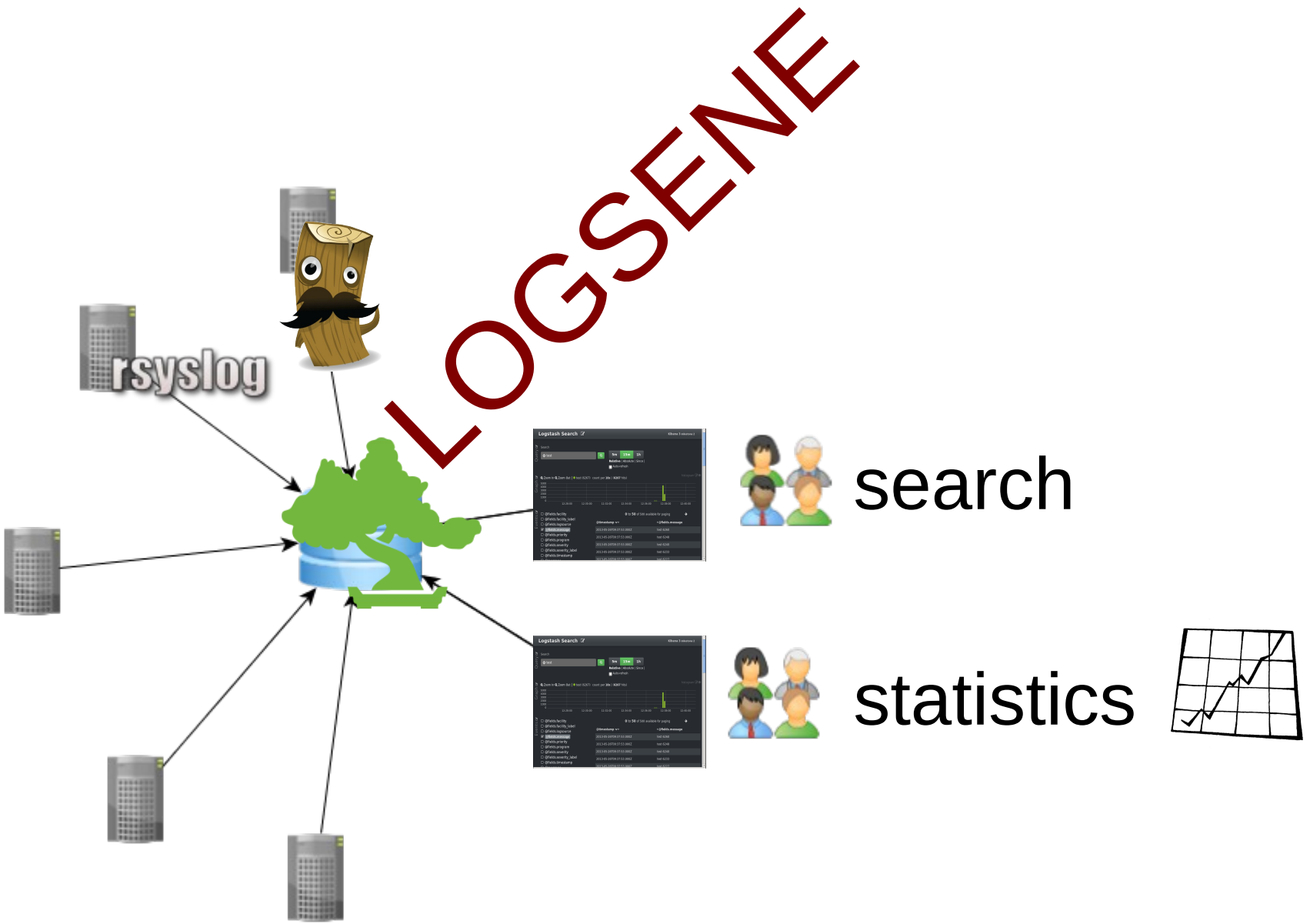
```
@cee: {
        "userID": "Mike",
        "time": 20,
        "item": "mouse",
        "errorCode": 0
      }
```

rsyslog

syslog-ng
Open Source Edition

STORE SEND SEARCH LOGS




LOGSENE
rsyslog
search
statistics

We're hiring!

Dig Search?

Dig Big Data?

Dig open–source?

We’re hiring world–wide!

http://sematext.com/about/jobs.html

Thank you!

radu.gheorghe@sematext.com

@sematext
http://sematext.com
http://blog.sematext.com

BETA: http://sematext.com/logsene/

42% off all MEAPs at
http://manning.com/
12mp25