ElasticSearch, Logstash ve Kibana ile Logging

Gurkan Oluc

@grkn

me@gurkanoluc.com

Ajanda

- Giriş
- ElasticSearch
- Logstash
- Kibana
- Demo
- Alternatifler
- Soru - Cevap

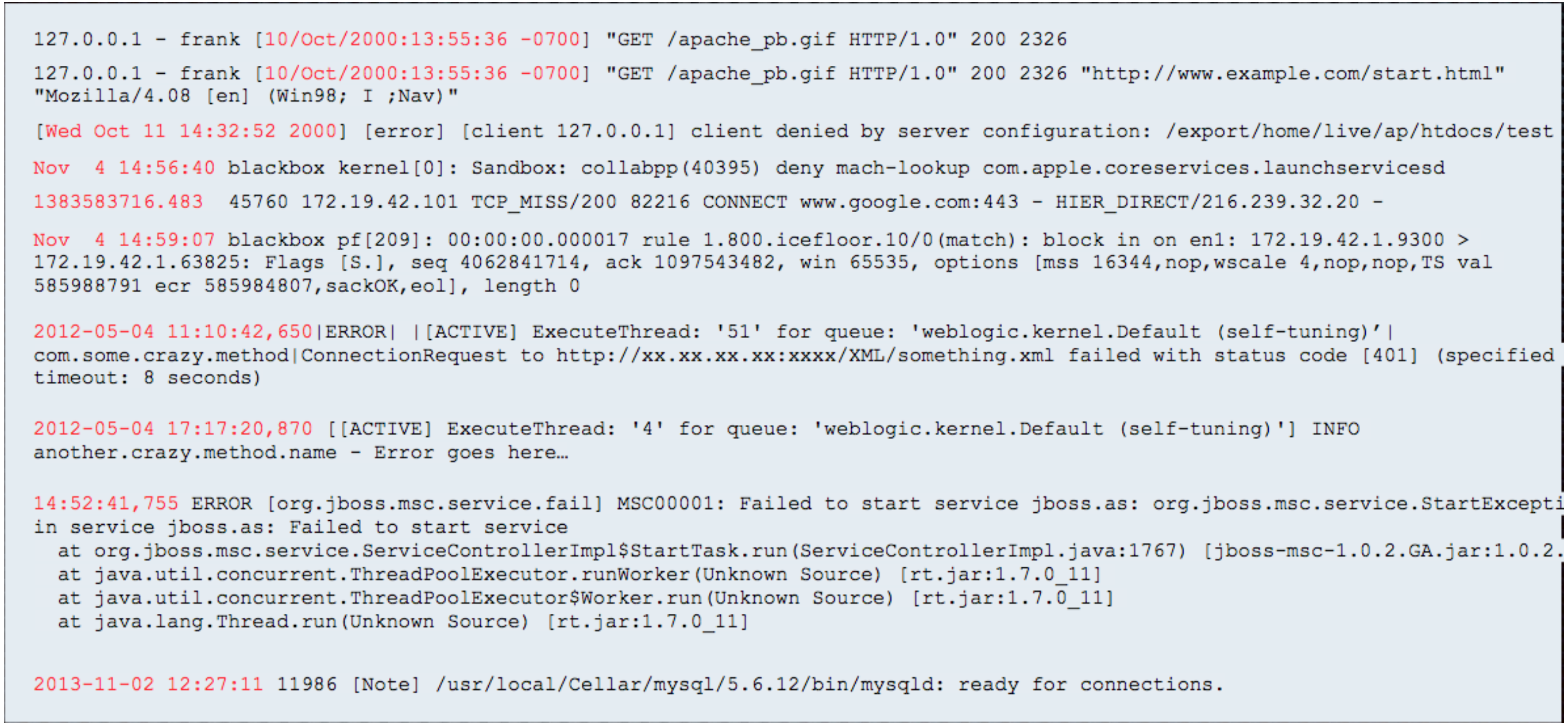
Giriş - Kimim ben?

- Gürkan Oluç
- Software Developer @ LoyaltyLion
- 2 yıldır ElasticSearch ile ilgileniyor
- me@gurkanoluc.com

Giriş - Log derken?

> “In computing, a **logfile** (or simply **log**) is a file that records either the events which happen while an operating system or other software runs, or the personal messages between different users of a communication software. The act of keeping a logfile is called logging. In the simplest case, log messages are written to a single log file.”

Giriş - Log derken?



```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326

127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326 "http://www.example.com/start.html"
"Mozilla/4.08 [en] (Win98; I ;Nav)"

[Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/home/live/ap/htdocs/test

Nov  4 14:56:40 blackbox kernel[0]: Sandbox: collabpp(40395) deny mach-lookup com.apple.coreservices.launchservicesd

1383583716.483  45760 172.19.42.101 TCP_MISS/200 82216 CONNECT www.google.com:443 - HIER_DIRECT/216.239.32.20 -

Nov  4 14:59:07 blackbox pf[209]: 00:00:00.000017 rule 1.800.icefloor.10/0(match): block in on en1: 172.19.42.1.9300 >
172.19.42.1.63825: Flags [S.], seq 4062841714, ack 1097543482, win 65535, options [mss 16344,nop,wscale 4,nop,nop,TS val
585988791 ecr 585984807,sackOK,eol], length 0

2012-05-04 11:10:42,650|ERROR| |[ACTIVE] ExecuteThread: '51' for queue: 'weblogic.kernel.Default (self-tuning)'|
com.some.crazy.method|ConnectionRequest to http://xx.xx.xx.xx:xxxx/XML/something.xml failed with status code [401] (specified
timeout: 8 seconds)

2012-05-04 17:17:20,870 [[ACTIVE] ExecuteThread: '4' for queue: 'weblogic.kernel.Default (self-tuning)'] INFO
another.crazy.method.name - Error goes here…

14:52:41,755 ERROR [org.jboss.msc.service.fail] MSC00001: Failed to start service jboss.as: org.jboss.msc.service.StartExcepti
in service jboss.as: Failed to start service
  at org.jboss.msc.service.ServiceControllerImpl$StartTask.run(ServiceControllerImpl.java:1767) [jboss-msc-1.0.2.GA.jar:1.0.2.
  at java.util.concurrent.ThreadPoolExecutor.runWorker(Unknown Source) [rt.jar:1.7.0_11]
  at java.util.concurrent.ThreadPoolExecutor$Worker.run(Unknown Source) [rt.jar:1.7.0_11]
  at java.lang.Thread.run(Unknown Source) [rt.jar:1.7.0_11]


2013-11-02 12:27:11 11986 [Note] /usr/local/Cellar/mysql/5.6.12/bin/mysqld: ready for connections.
```

{DATE} + {DATA} = LOG

Giriş - Log önemli!

Giriş - Niçin?

- Hangi makinelerde hata var?
- Hangi dosyada?
- Ya aramak istersek?
- Acı çekmek zorunda mıyız?
- Ne olup bitiyor bu sistemde yahu?
- Yaptıklarımızın sonuçları ne?

Giriş - Acı?

- grep
  - cat file.log | grep pattern
  - cat file.log | egrep ‘pattern1|pattern2’
- sort?
- Bu işlem n server’da?

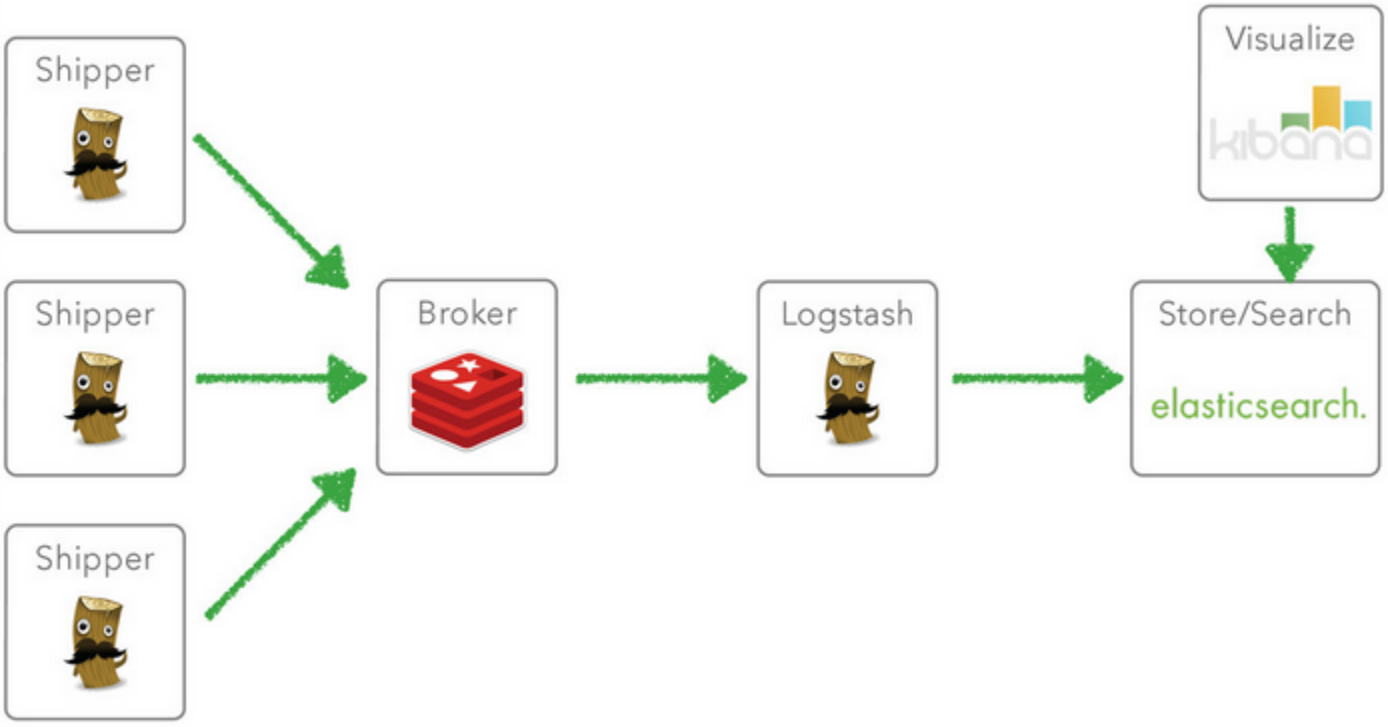
Giriş - Çözüm

Merkezi Log Sistemi!

Giriş - Çözüm

ElasticSearch, Logstash ve Kibana!

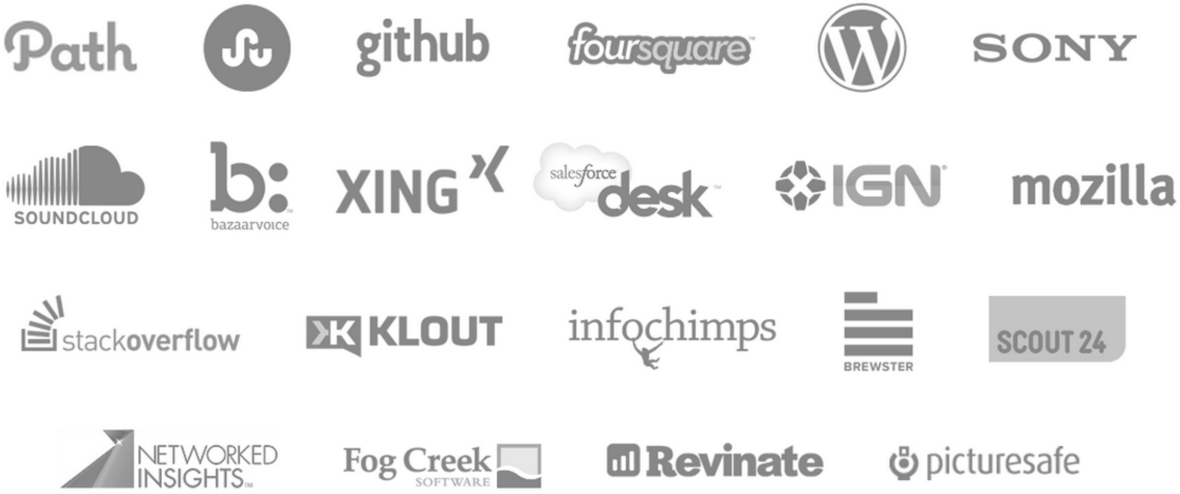
Giriş - Nasıl?


Shipper
Shipper
Shipper
Broker
Logstash
Visualize
kibana
Store/Search
elasticsearch.

ElasticSearch

- Schema-free, REST & JSON tabalı document store
- Lucene tabanlı
- Java ile yazıldı
- Geliştiren şirket en son 70M $ yatırım aldı. (Sağlam yani)

ElasticSearch - Kim kullanıyor?



ElasticSearch - Özellikler

- Real-time search ve analytics
- Dağıtık
- Yüksek bulunurluk
- Restful API
- Sharding
- Replication

ElasticSearch - Loglamak için?

- Biraz garip geliyor olabilir.
- Solr'a tüm logları gönderen oldu mu hiç?
- Günlük sharding
- JSON
- Kolay query
- Facets ve Aggregations!

Logstash

- Herhangi bir kaynaktan log oku
- Filtrele
- Formatla
- Yeni bir kaynaga gönder

Logstash - input

- file
- redis
- rabbitmq
- jmx
- syslog
- tcp
- zeromq
- ...

Logstash - filter

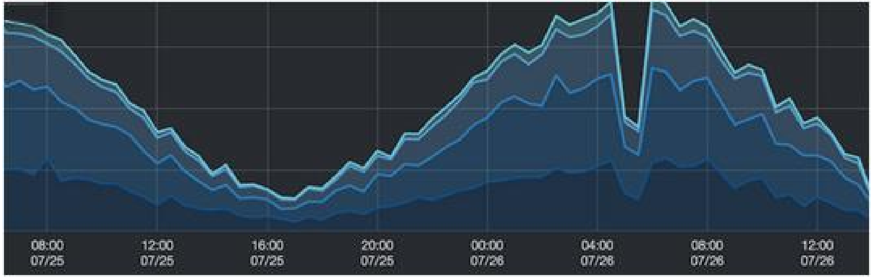
- csv
- grok
  - patterns
- metrics
- multiline
- ...

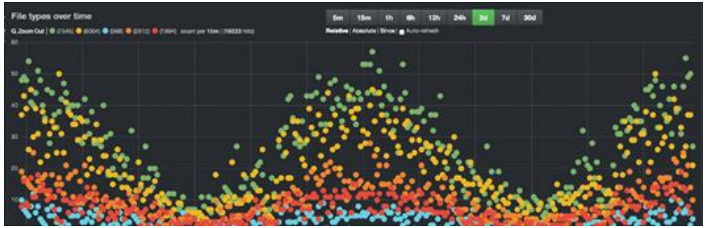
Logstash - output

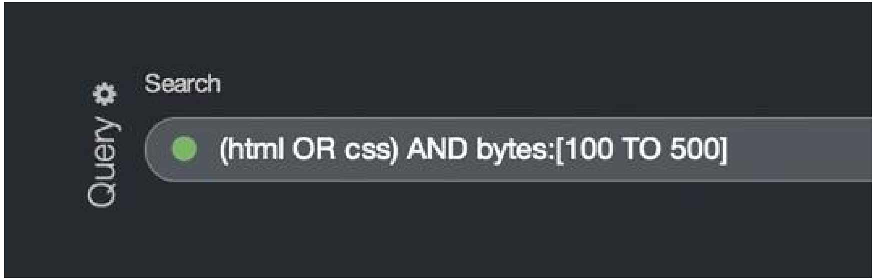
- elasticsearch
- email
- hipchat
- http
- graphite
- rabbitmq
- s3
- statsd..

Kibana

- time-series data
- eldeki data’yı anlamak
- büyük data içerisinde arama



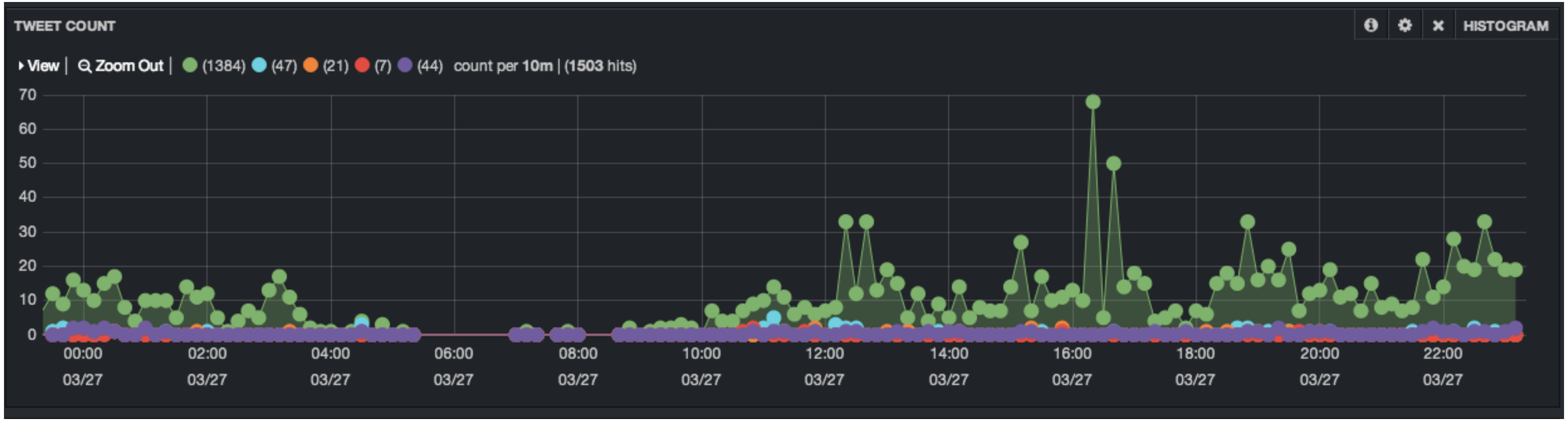




(html OR css) AND bytes:[100 TO 500]

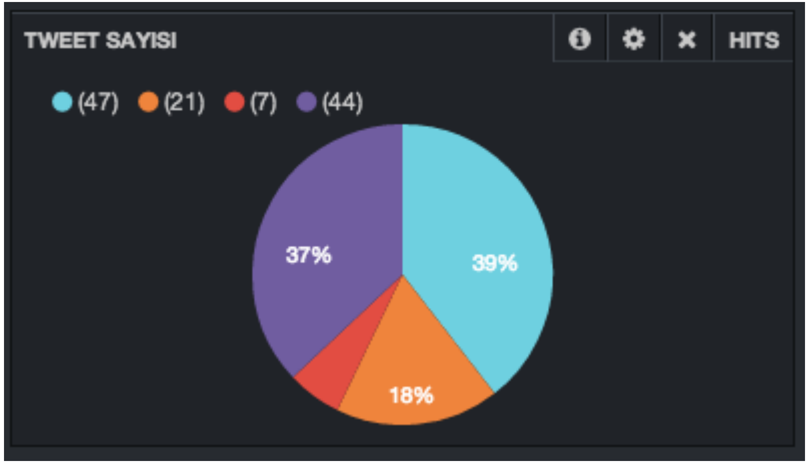
Kibana - Ornek

- Histogram



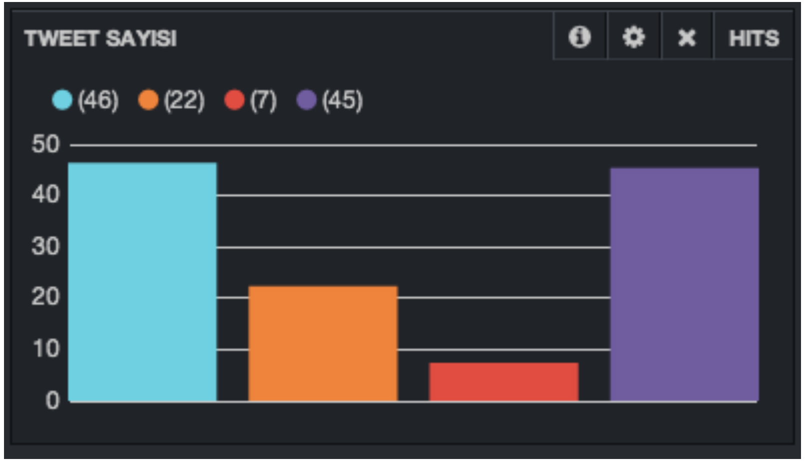
Kibana - Ornek

- Pie



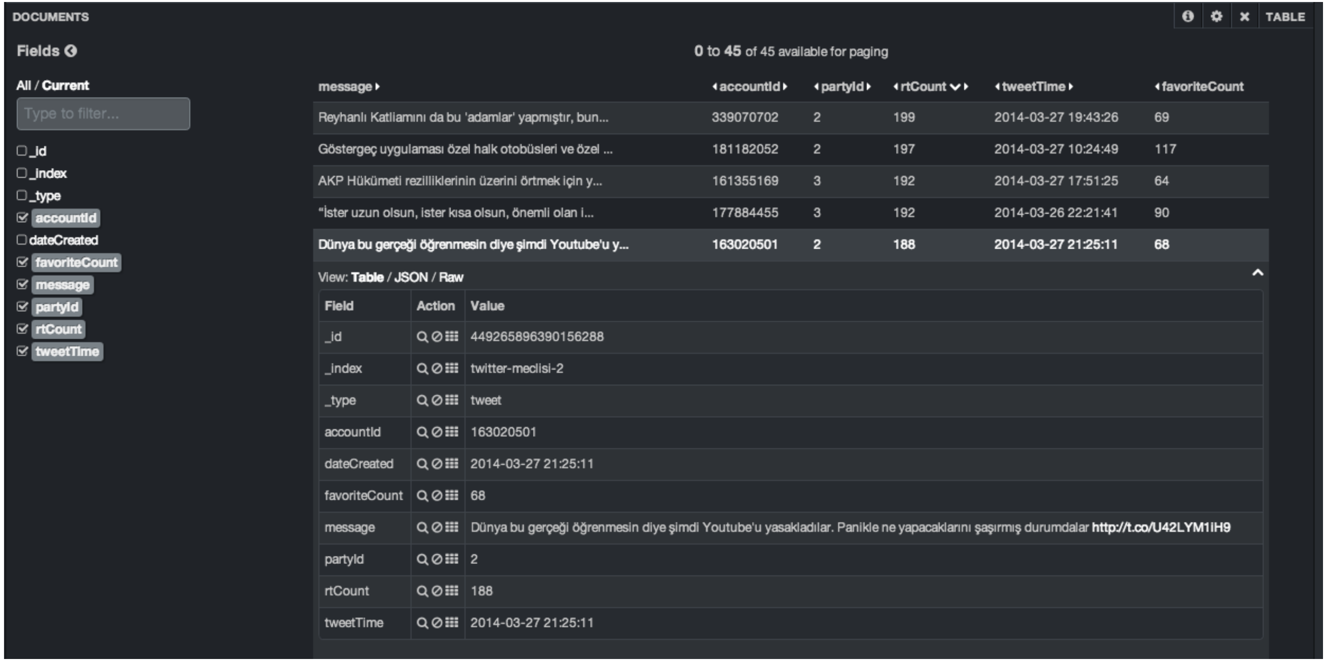
Kibana - Ornek

- Bar



Kibana - Ornek

- Table



DOCUMENTS

Fields

All / Current

Type to filter...

☐ _id
☐ _index
☐ _type
☑ accountId
☐ dateCreated
☑ favoriteCount
☑ message
☑ partyId
☑ rtCount
☑ tweetTime

0 to **45** of 45 available for paging

message ▸	◂ accountId ▸	◂ partyId ▸	◂ rtCount ⌄ ▸	◂ tweetTime ▸	◂ favoriteCount
Reyhanlı Katliamını da bu 'adamlar' yapmıştır, bun...	339070702	2	199	2014-03-27 19:43:26	69
Göstergeç uygulaması özel halk otobüsleri ve özel ...	181182052	2	197	2014-03-27 10:24:49	117
AKP Hükümeti rezilliklerinin üzerini örtmek için y...	161355169	3	192	2014-03-27 17:51:25	64
"İster uzun olsun, ister kısa olsun, önemli olan i...	177884455	3	192	2014-03-26 22:21:41	90
Dünya bu gerçeği öğrenmesin diye şimdi Youtube'u y...	**163020501**	**2**	**188**	**2014-03-27 21:25:11**	**68**

View: **Table** / JSON / Raw

Field	Action	Value
_id	🔍 ⊘ ▦	449265896390156288
_index	🔍 ⊘ ▦	twitter-meclisi-2
_type	🔍 ⊘ ▦	tweet
accountId	🔍 ⊘ ▦	163020501
dateCreated	🔍 ⊘ ▦	2014-03-27 21:25:11
favoriteCount	🔍 ⊘ ▦	68
message	🔍 ⊘ ▦	Dünya bu gerçeği öğrenmesin diye şimdi Youtube'u yasakladılar. Panikle ne yapacaklarını şaşırmış durumdalar **http://t.co/U42LYM1IH9**
partyId	🔍 ⊘ ▦	2
rtCount	🔍 ⊘ ▦	188
tweetTime	🔍 ⊘ ▦	2014-03-27 21:25:11

Alternatifler ve Tavsiyeler

- fluentd
- graylog2
- https://github.com/josegonzalez/beaver

Sorular?

Teşekkürler!