Log

Simonas Šerlinskas

simonas.serlinskas@nfq.com
@saimazz
http://github.com/saimaz
https://speakerdeck.com/saimaz

PSX

enterprise. e-commerce. accelerator.


oyatego

kiveda

.NFQ

AKADEMIJA

PRAKTIKA ++

http://nfqakademija.lt

OMNITEL 3G 4:12 AM

Messages

Jenkins

Edit

Hi

Send

OMNITEL 3G 4:17 AM

Messages

Jenkins

Edit

Hi

Hey wake up!

Send

OMNITEL 3G 4:17 AM

Messages Jenkins Edit

Hi

Hey wake up!

What??

Send

OMNITEL 3G 4:17 AM

Messages Jenkins Edit

Hi

Hey wake up!

What??

There is huge amount of error logs from xxx provider.

Send

OMNITEL 3G 4:17 AM

Messages Jenkins Edit

Hi

Hey wake up!

What??

There is huge amount of error logs from xxx provider.

Fuck off!

Send

OMNITEL 3G 4:30 AM

Messages Jenkins Edit

Hi

Hey wake up!

What??

There is huge amount of error logs from xxx provider.

Fuck off!

Someone will definitely call you tomorrow. I'm jut saying...

Send

OMNITEL 3G 4:30 AM

Messages Jenkins Edit

Hi

Hey wake up!

What??

There is huge amount of error logs from xxx provider.

Fuck off!

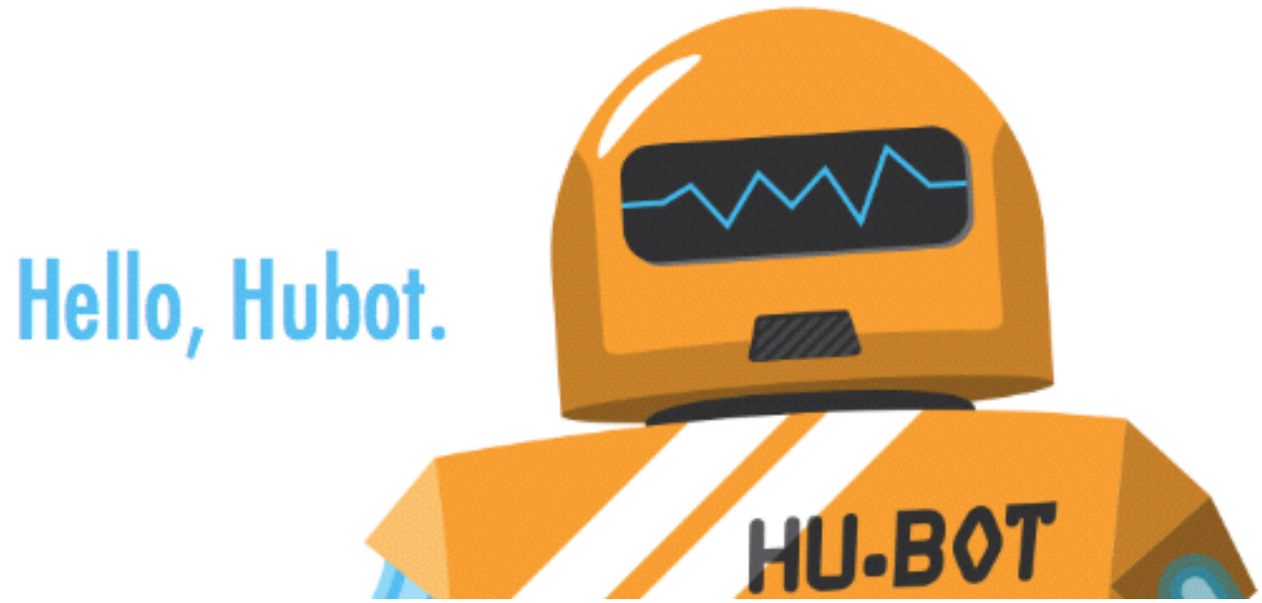
Someone will definitely call you tomorrow. I'm jut saying...

I'm scared.. :(

Send

http://logstash.net

http://elasticsearch.org



http://hubot.github.com

http://www.twilio.com

```
 - - [18/Jan/2013:19:57:13 -0500] "GET /robots.txt HTTP/1.1" 301 303 "-" "msnbot-media/1.1 (+http://search.msn.com/msnbo
 - - [18/Jan/2013:19:57:13 -0500] "GET /gallery/gallery/Subaru/ormeau_-_25_April_2005/thumbs/IMG_2854.JPG HTTP/1.1" 301
(+http://search.msn.com/msnbot.htm)"
9 - - [18/Jan/2013:20:02:41 -0500] "GET /robots.txt HTTP/1.1" 301 303 "-" "Mozilla/5.0 (compatible; Exabot/3.0; +http://

9 - - [18/Jan/2013:20:02:42 -0500] "GET /wordpress/tag/smoke/ HTTP/1.1" 301 303 "-" "Mozilla/5.0 (compatible; Exabot/3.0
o/robot)"
- - [18/Jan/2013:20:08:19 -0500] "GET /wordpress/cooking/mozambique-style-piri-piri-chicken/feed/ HTTP/1.1" 301 351 "-"
Googlebot/2.1; +http://www.google.com/bot.html)"
- - [18/Jan/2013:20:17:53 -0500] "GET /favicon.ico HTTP/1.1" 301 303 "http://www.eatinginabox.com/2009/10/foodblogger-ev
zilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"
- - [18/Jan/2013:20:21:19 -0500] "GET /wordpress/cooking/mushroom-ragu-on-creamy-polenta/trackback/ HTTP/1.1" 301 348 "-
; Googlebot/2.1; +http://www.google.com/bot.html)"
- - [18/Jan/2013:20:23:44 -0500] "GET /favicon.ico HTTP/1.1" 301 303 "http://www.eatinginabox.com/2011/10/paleo-diet-ber
dows NT 6.1; WOW64) AppleWebKit/537.17 (KHTML, like Gecko) Chrome/24.0.1312.52 Safari/537.17"
 - - [18/Jan/2013:20:23:45 -0500] "GET /wordpress/feed/ HTTP/1.1" 301 303 "-" "Feedfetcher-Google; (+http://www.google.c
bscribers; feed-id=12636598490283692241)"
- - [18/Jan/2013:20:34:00 -0500] "GET /wordpress/cooking/fettucini-with-fresh-vegetables/comment-page-1/ HTTP/1.1" 301 3
tible; Googlebot/2.1; +http://www.google.com/bot.html)"
- - [18/Jan/2013:20:48:51 -0500] "GET /robots.txt HTTP/1.1" 301 303 "-" "Mozilla/5.0 (compatible; bingbot/2.0; +http://w

- - [18/Jan/2013:20:50:50 -0500] "GET /wordpress/tag/cheese/ HTTP/1.1" 301 303 "-" "Mozilla/5.0 (compatible; bingbot/2.0
gbot.htm)"
```

```
- - [18/Jan/2013:21:00:01 -0500] "GET /wordpress/cooking/cider-bean-stew-with-truffle-pate-stuffed-chicken-legs/trackbac
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
 - [18/Jan/2013:21:00:04 -0500] "GET /wordpress/cooking/pate-de-campagne-meatball-bacon-and-pastrami-pizza-with-garlic-p
 352 "http://xesla.ro/wordpress/cooking/pate-de-campagne-meatball-bacon-and-pastrami-pizza-with-garlic-pizza-fritta/" "C
 Win64; x64; U; ru) Presto/2.10.289 Version/12.00"
1 - - [18/Jan/2013:21:06:00 -0500] "GET /wordpress/cooking/wild-duck-gumbo/ HTTP/1.1" 301 332 "http://honest-food.net/wi
nison-stews/wild-game-gumbo/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/536.26.17 (KHTML, like Gecko)
6.17"
 - - [18/Jan/2013:21:23:45 -0500] "GET /wordpress/feed/ HTTP/1.1" 301 303 "-" "Feedfetcher-Google; (+http://www.google.c
bscribers; feed-id=12636598490283692241)"
- - [18/Jan/2013:21:26:07 -0500] "GET /wordpress/cooking/jagerbomb-icecream-cake/ HTTP/1.1" 301 340 "-" "Mozilla/5.0 (co
http://www.google.com/bot.html)"
- - [18/Jan/2013:21:28:57 -0500] "GET /wordpress/cooking/sous-vide-party/ HTTP/1.1" 301 332 "-" "DoCoMo/2.0 N905i(c100;T
glebot-Mobile/2.1; +http://www.google.com/bot.html)"
5 - - [18/Jan/2013:21:29:07 -0500] "GET /robots.txt HTTP/1.1" 301 303 "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http

5 - - [18/Jan/2013:21:29:07 -0500] "GET /robots.txt HTTP/1.1" 301 307 "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http

5 - - [18/Jan/2013:21:29:08 -0500] "GET / HTTP/1.1" 301 303 "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.
5 - - [18/Jan/2013:21:29:08 -0500] "GET / HTTP/1.1" 301 307 "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.
 - - [18/Jan/2013:21:30:08 -0500] "GET /wordpress/cooking/chocolate-bread/feed/ HTTP/1.1" 301 332 "-" "magpie-crawler/1.
+http://www.brandwatch.net)"
```


THERE IS A WAY

LOG = TIME + DATA

- Correct timestamps ISO 8601
- use /var/log (by default)
- logrotate!!
- don’t log sensitive info (passwords, keys..)
- use log levels by RFC 5424


HI: 20000
2300
TIME: 89
Winner(8-12)
LITTLE DEMO
CLASSIC GAMES.cn
Download

Silex

```
{
    "autoload": {
        "psr-0": {
            "": "src/"
        }
    },
    "require": {
        "silex/silex": "~1.1",
        "symfony/monolog-bridge": "*",
        "symfony/console": "*",
        "fzaninotto/faker": "dev-master"
    }
}

```

console — logger (git: master)

composer.json | console

```php
#!/usr/bin/env php
<?php
require_once __DIR__ . '/vendor/autoload.php';

//Include the Console namespaces
use Monolog\Formatter\LogstashFormatter;
use Monolog\Handler\StreamHandler;
use Symfony\Component\Console\Application;
use Symfony\Component\Console\Input\InputInterface;
use Symfony\Component\Console\Input\InputArgument;
use Symfony\Component\Console\Input\InputOption;
use Symfony\Component\Console\Output\OutputInterface;
use Monolog\Logger;

class App extends Silex\Application
{
    use Silex\Application\MonologTrait;
}

$type = "dudes";
$logsPath = __DIR__ . '/logs/app.log';

/** @var Faker/Generator $faker */
$faker = Faker\Factory::create();
$app = new App();
$app->register(
    new Silex\Provider\MonologServiceProvider(),
    [
        'monolog.logfile' => $logsPath,
        'monolog.name' => $type,
    ]
);

/** @noinspection PhpParamsInspection */
$app['monolog'] = $app->share(
```

console

logger
- logs
- src
- vendor
- web
- apache_filtered.con
- apache_raw.conf
- composer.json
- composer.lock
- console
- log.conf

Line: 21:30-21:33 | PHP | Soft Tabs: 4 | App

https://github.com/saimaz/logstash_demo

simas@pro: ~/Sites/kibana/logger — zsh — 89×29

..kibana/logger | ..kibana/logger

```
➜  logger git:(master) ✗
```

```
{
  "@timestamp": "2014-01-24T08:31:58.166+02:00",
  "@version": 1,
  "message": "User wehner.ava bought",
  "host": "pro.local",
  "type": "dudes",
  "channel": "dudes",
  "level": "INFO",
  "ctxt_type": "bought",
  "ctxt_name": "Rita",
  "ctxt_surname": "Lindgren",
  "ctxt_street": "Romaguera Parkway",
  "ctxt_city": "Newelltown",
  "ctxt_country": "Italy",
  "ctxt_ip": "10.60.6.7",
  "ctxt_browser": "Mozilla\/5.0 (Macintosh; ........"
  "ctxt_language": "en",
  "ctxt_locale": "mn_MN",
  "ctxt_lonlat": "-39.213434,63.176546",
  "ctxt_registered": "1975-03-06T21:35:26+0000"
}
```

```
{"@timestamp":"2014-01-24T08:31:58.166+02:00","@version":1,"message":"User wehner.ava
bought","host":"pro.local","type":"dudes","channel":"dudes","level":"INFO","ctxt_type":"bought","ctxt_na
Rita","ctxt_surname":"Lindgren","ctxt_street":"Romaguera
Parkway","ctxt_city":"Newelltown","ctxt_country":"Italy","ctxt_ip":"10.60.6.7","ctxt_browser":"Mozilla/5
(Macintosh; U; PPC Mac OS X 10_5_2 rv:6.0; en-US) AppleWebKit/534.26.6 (KHTML, like Gecko) Version/5.0.4
Safari/
534.26.6","ctxt_language":"en","ctxt_locale":"mn_MN","ctxt_lonlat":"-39.213434,63.176546","ctxt_register
1975-03-06T21:35:26+0000"}
{"@timestamp":"2014-01-24T08:31:58.168+02:00","@version":1,"message":"User lkeebler
canceled","host":"pro.local","type":"dudes","channel":"dudes","level":"INFO","ctxt_type":"canceled","ctx
e":"Percy","ctxt_surname":"Robel","ctxt_street":"Tillman
Prairie","ctxt_city":"Nyasiashire","ctxt_country":"Serbia","ctxt_ip":"159.1.47.22","ctxt_browser":"Opera
(X11; Linuxx86_64; en-US) Presto/2.9.162 Version/
11.00","ctxt_language":"cn","ctxt_locale":"en_US","ctxt_lonlat":"-53.358862,-43.815396","ctxt_registered
80-08-24T23:23:02+0000"}
{"@timestamp":"2014-01-24T08:31:58.169+02:00","@version":1,"message":"User cankunding
canceled","host":"pro.local","type":"dudes","channel":"dudes","level":"INFO","ctxt_type":"canceled","ctx
e":"Aniyah","ctxt_surname":"Morar","ctxt_street":"Dina
Terrace","ctxt_city":"Baumbachchester","ctxt_country":"Botswana","ctxt_ip":"40.182.75.36","ctxt_browser"
illa/5.0 (Windows; U; Windows 98) AppleWebKit/532.13.5 (KHTML, like Gecko) Version/5.0.2 Safari/
532.13.5","ctxt_language":"en","ctxt_locale":"bs_BA","ctxt_lonlat":"-4.193961,-83.662772","ctxt_register
1997-12-11T02:15:30+0000"}
{"@timestamp":"2014-01-24T08:31:58.172+02:00","@version":1,"message":"User elyse.wintheiser
canceled","host":"pro.local","type":"dudes","channel":"dudes","level":"INFO","ctxt_type":"canceled","ctx
e":"Maryjane","ctxt_surname":"Watsica","ctxt_street":"Ronaldo Mission","ctxt_city":"South
Antonina","ctxt_country":"Senegal","ctxt_ip":"197.41.118.31","ctxt_browser":"Mozilla/5.0 (Windows; U; Wi
NT 5.0) AppleWebKit/531.3.5 (KHTML, like Gecko) Version/5.0.2 Safari/
531.3.5","ctxt_language":"de","ctxt_locale":"wo_SN","ctxt_lonlat":"168.781940,-0.184951","ctxt_registere
989-12-03T05:04:47+0000"}
{"@timestamp":"2014-01-24T08:31:58.174+02:00","@version":1,"message":"User collier.garnet added to
cart","host":"pro.local","type":"dudes","channel":"dudes","level":"INFO","ctxt_type":"cart","ctxt_name":
","ctxt_surname":"Maggio","ctxt_street":"Lazaro
Views","ctxt_city":"Hesselbury","ctxt_country":"Australia","ctxt_ip":"133.74.58.205","ctxt_browser":"Moz
5.0 (Macintosh; U; PPC Mac OS X 10_5_1) AppleWebKit/5362 (KHTML, like Gecko) Chrome/15.0.832.0 Safari/
5362","ctxt_language":"en","ctxt_locale":"kpe_GN","ctxt_lonlat":"-121.402069,-6.526117","ctxt_registered
82-01-31T18:42:26+0000"}
{"@timestamp":"2014-01-24T08:31:58.176+02:00","@version":1,"message":"User snitzsche added to
watchlist","host":"pro.local","type":"dudes","channel":"dudes","level":"INFO","ctxt_type":"watchlist","c
ame":"Vergie","ctxt_surname":"Batz","ctxt_street":"Stanton
Wall","ctxt_city":"Langchester","ctxt_country":"Andorra","ctxt_ip":"48.219.75.27","ctxt_browser":"Mozill
```

Add everything to

elasticsearch

ElasticSearch

http://localhost:9200/ Connect

Alexander, Caleb

Overview | Browser | Structured Query [+] | Any Request [+]

Cluster Overview

New Index | Sort Cluster

Alexander, Caleb

pro.local

Info | Actions

logstash

```
input {
    file {
        codec => "json"
        path => "/path/to/logs/app.log"
        type => "dudes"
        #debug => true
    }
}
output {
    elasticsearch_http {
        host => "localhost"
        port => 9200
        index => "dudes"
        type => "dudes"
        flush_size => 1000
    }
}
```

simas@pro: ~/Sites/kibana/logger — zsh — 111×34

..kibana/logger | ..kibana/logger

```
→  logger git:(master) ✗
```

Kibana

http://www.kibana.com

Logstash Search

Kibana 3 milestone pre-3

Options

Query

Search

php | png OR gif | css

Query Alias

Images

Chart

Zoom Out | Dynamic (12239) | Images (1 | nt per 30m | (40354 hits)

800
600
400
200
0

16:00 07/24 | 20:00 07/24 | 00:00 07/25 | 04:00 07/25 | 08:00 07/25 | 12:00 07/25 | 16:00 07/25 | 20:00 07/25 | 00:00 07/26 | 04:00 07/26 | 08:00 07/26 | 12:00 07/26

Terms

Term	Count	Action
id	1856	
br	1567	
pk	1437	
ng	1207	
bd	1172	
ru	1078	
jp	959	
mx	678	
Missing field	9818	
Other values	20582	

id (1856) br (1567) pk (1437) ng (1207) bd (1172) ru (1078) jp (959) mx (678)

2000
1500
1000
500
0

filtering

time must
field : @timestamp
from : "2013-07-24T21:13:04.742Z"
to : "2013-07-26T21:13:04.743Z"

terms mustNot
field : country
value : cn

Toggle

terms mustNot
field : country
value : us

terms mustNot
field : country
value : id

Logstash Search

Kibana 3 milestone 2

Options

5m | 15m | 1h | 6h | 12h | 24h | 2d | 5d

Relative | **Absolute** | **Since** | Auto-refresh

Dashboard Control

Query

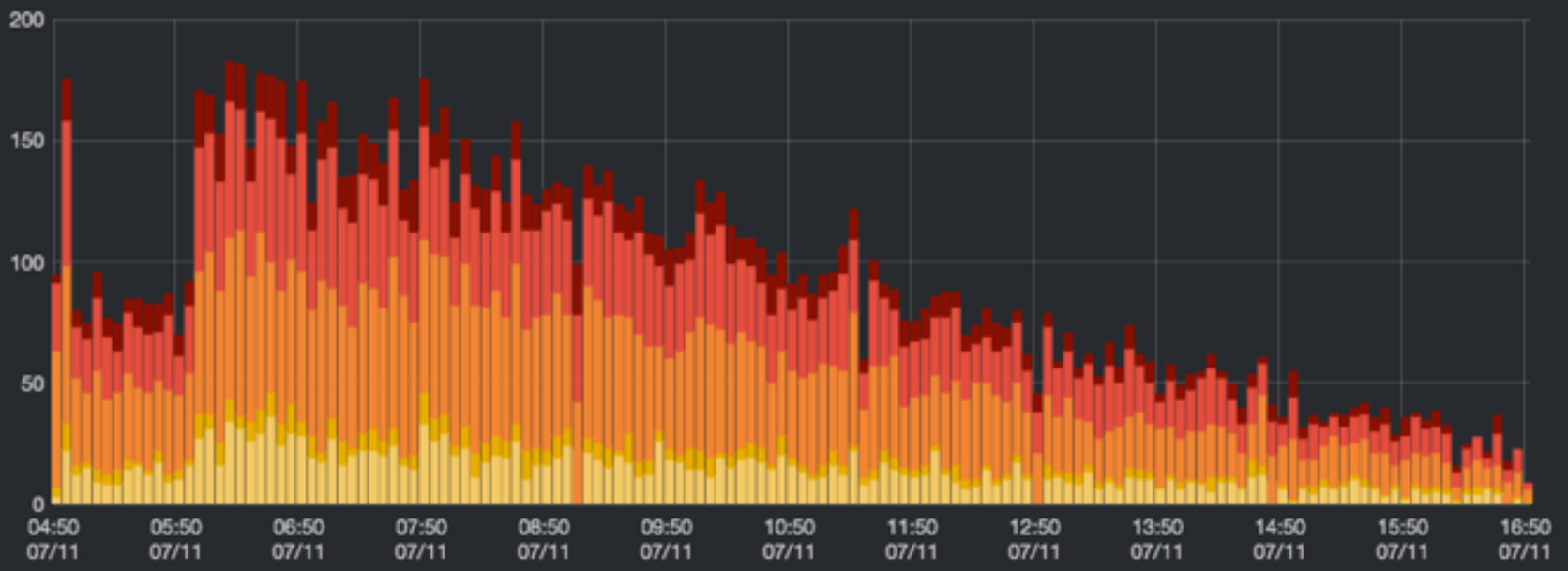
Search

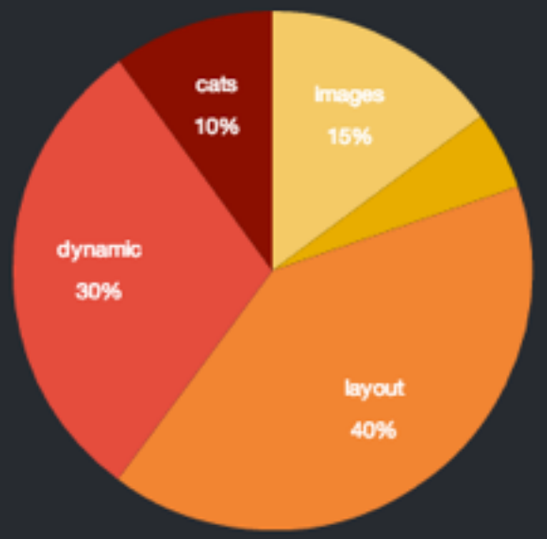
png OR jpg | css | html | php OR pl | gif

Graph

Zoom In | Zoom Out | images (1992) | styles (655) | layout (5412) | dynamic (3996) | cats (1344) count per **5m** | (**13399** hits)

histogram





Trend

-4.6% (images) | 4.63% (styles) | -0.62% (layout) | -4.8% (dynamic) | -1.18% (cats)

Web Cluster

Kibana 3 milestone pre-2

Options

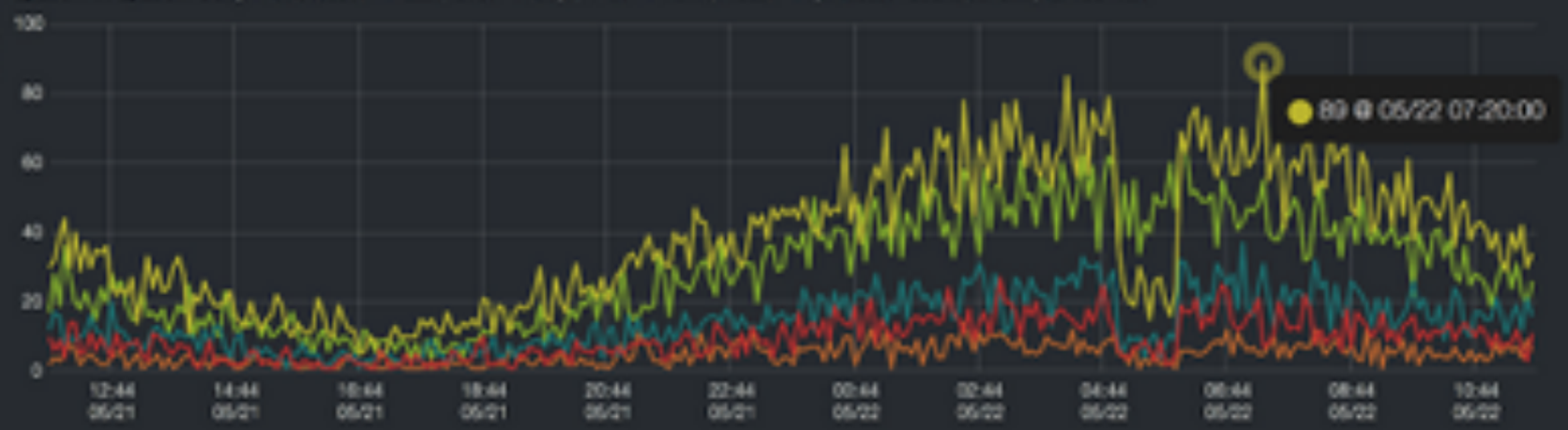
Query

php | css | png | html | gif

Search | +

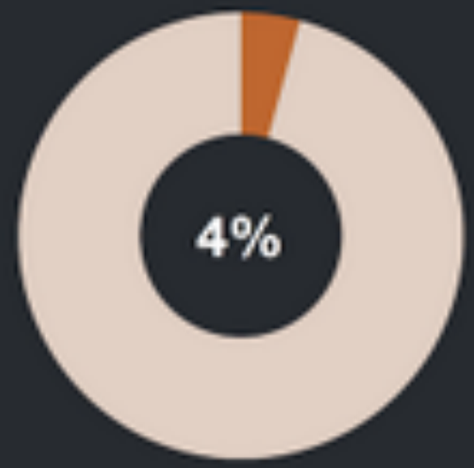
Graph

Zoom In | Zoom Out | php (8559) | css (1375) | png (4142) | html (11025) | gif (2682) count per 5m | (27783 hits)



Histogram

Map+Pie



Demo

a day ago to a few seconds ago

*

QUERY

FILTERING

ADD A ROW

http://logstash.net/

http://kibana.org

http://www.elasticsearch.org/

https://github.com/Seldaek/monolog

http://silex.sensiolabs.org/

ANYTHING?