

**Maybe U2 should have  
used Elasticsearch**

Jurgens du Toit

Jrgns

Eager  ELK

**Search is simple, right?**



# Search is simple, right?



```
SELECT * FROM `content`  
WHERE `body` LIKE '%term%'
```

# Search is simple, right?



```
SELECT * FROM `content`  
WHERE `body` LIKE '%term%'
```

# Search

```
1 {
2   "status" : 200,
3   "name" : "Crimson Craig",
4   "cluster_name" : "elasticsearch",
5   "version" : {
6     "number" : "1.7.0",
7     "build_hash" : "929b9739cae115e73c346cb5f9a",
8     "build_timestamp" : "2015-07-16T14:31:07Z",
9     "build_snapshot" : false,
10    "lucene_version" : "4.10.4"
11  },
12  "tagline" : "You Know, for Search"
13 }
```

# Search



# What is it?



elastic



elasticsearch.

distributed restful search and analytics



kibana



# What is it?

elasticsearch

Search term

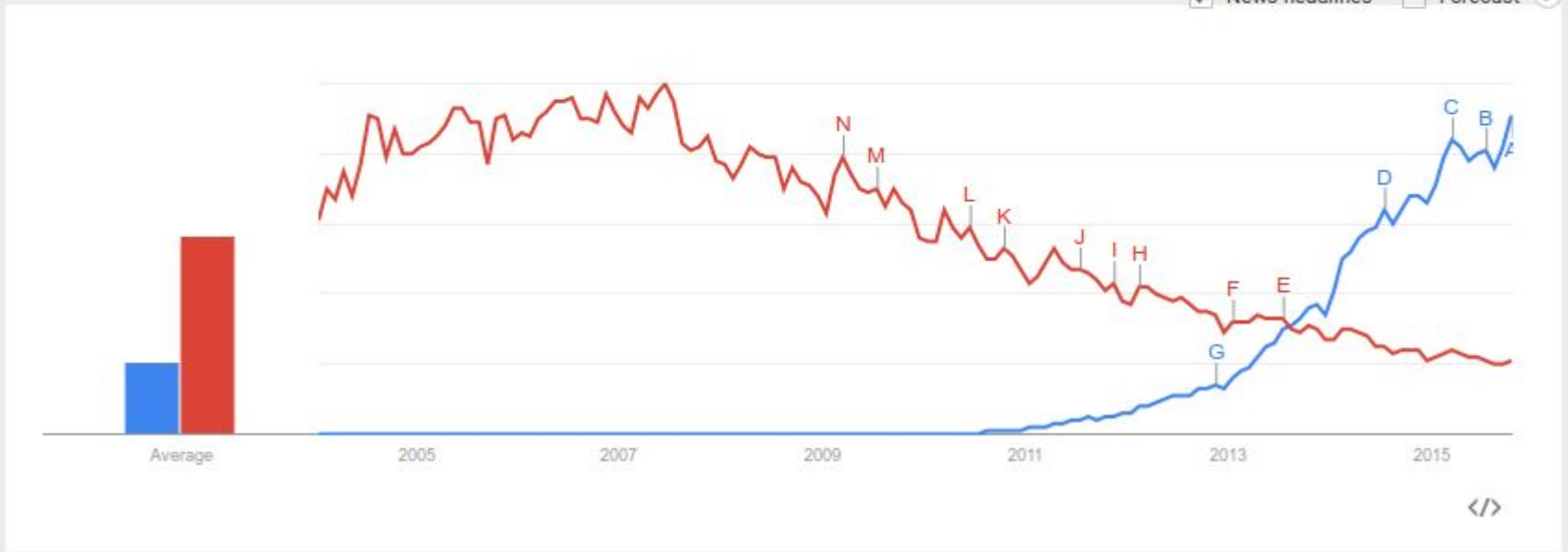
lucene

Search term

+ Add term

Interest over time ?

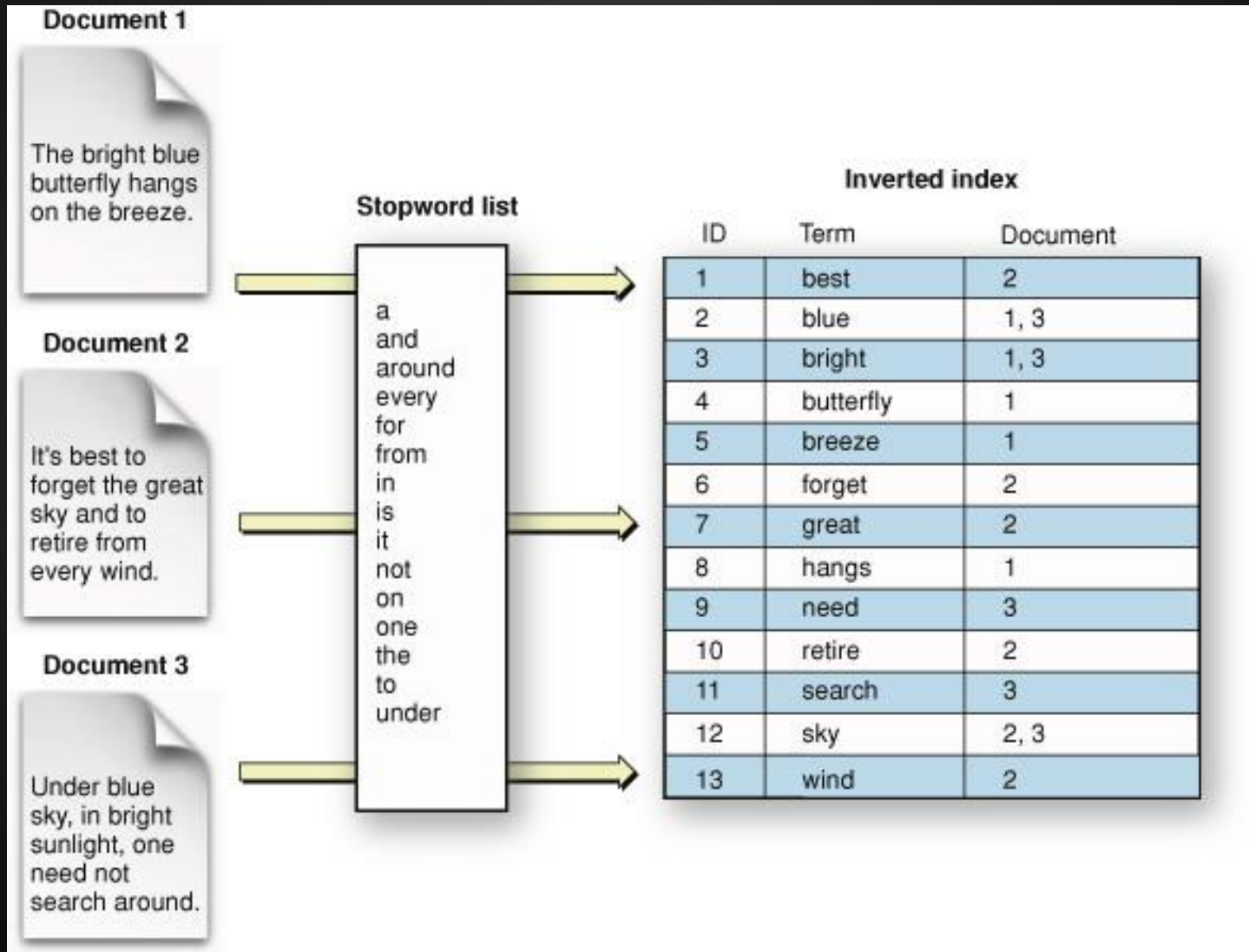
News headlines  Forecast ?



# Architecture



# Indexing



# Use cases

Search

Time Series & Log Analysis

Application Database

# Use cases

Search

Time Series & Log Analysis

Application Database

# Search Features

Go!

Showing 1 to 10 of 1110 results. Search took 150ms

New Intel Item

<< < - > >>

Number of results: 10

Clinton's personal email server was vulnerable to hackers Reference: 1444747895000005625

Relevant	
Score:	751.60172
Author:	Joshua Barajas
Timestamp:	2015-10-13T14:17:04Z
Language:	en
Cluster size:	1
Locations:	<span>Show / Edit</span>

**guide risks infectious chance failing washington break time**  
**hillary clinton hillary report**

Report: Company has no knowledge Clinton server was 'wiped' Records show that Clinton additionally operated two more devices on her home network in Chappaqua, New York, that also were directly accessible from the Internet. One contained similar remote-control software that also has suffered from security vulnerabilities, known as Virtual Network Computing, and the other appeared to be configured to run websites.

The new details provide the first clues about how Clinton's computer, running Microsoft's server software, was set up and protected when she used it exclusively over four years as secretary of state for all work messages. Clinton's

Status

Relevant 70

Irrelevant 41

Dismiss 25

None 974

Publisher type

WEBLOG 580

# Search Features

email

Showing 1 to 10 of 1110 results. Search took 150ms



Number of results:

10



Status

Relevant

70

Irrelevant

41

Dismiss

25

None

974

Publisher type

WEBLOG

580

# Search Features

```
1 -- Actual Search
2 SELECT * FROM `items` WHERE `content` LIKE '%email%'
3 -- Total number of items
4 SELECT COUNT(*) FROM `items` WHERE `content` LIKE '%email%'
5 -- Status aggregation - Search
6 SELECT `status`, COUNT(*) AS `count`
7     FROM `items` WHERE `content` LIKE '%email%' GROUP BY `status`
8 -- Status aggregation - Global
9 SELECT `status`, COUNT(*) AS `count`
10    FROM `items` GROUP BY `status`
```



# Search Features

```
1 curl -s 'localhost:9200/_search?pretty' -d '  
2 {  
3     "query": {  
4         "match": { "message": "email" }  
5     },  
6     "aggregations": {  
7         "status_values": {  
8             "terms": {  
9                 "field": "status"  
10            }  
11        }  
12    }  
13 }'
```

# Search Features

- Queries
- Filters
- Aggregations

# Search Features

- Query String
- Match
- Match Phrase / Spans
- More Like This
- Boolean
- Fuzzy
- ...

# Time Series Data / Logs

- A LOT of Data
- Difficult to manage
- Notorious to parse
- A wealth of information, if...



**LIVE DEMO**

**I ALSO LIKE TO LIVE  
DANGEROUSLY**

# Resources

- **Reference Guide**

<https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html>

- **The Definitive Guide**

<https://www.elastic.co/guide/en/elasticsearch/guide/current/index.html>

- **Resiliency Status**

<https://www.elastic.co/guide/en/elasticsearch/resiliency/current/index.html>

- **Jo'burg Elastic Meetup**

<http://www.meetup.com/Elasticsearch-South-Africa/>

**Questions?**