ELK

Elasticsearch, Logstash and Kibana at Wikimedia

Not this kind of Elk

https://commons.wikimedia.org/wiki/File:Male_Elk_%288005280487%29.jpg

E is for elasticsearch.

Document oriented full text search engine built on top of Apache Lucene.

Licenced under Apache 2 Open Source License by Elasticsearch BV

L is for logstash

Pipeline processing system that connects "inputs" to "outputs" with optional "filters" in between.

```
$ tail -f foo.log | grep bar |
  awk '{print $7 $9}' >> foo-pretty.log
```

Licenced under Apache 2 Open Source License by Elasticsearch BV

K is for

Browser based analytics and search dashboard for Elasticsearch.

Licenced under Apache 2 Open Source License by Elasticsearch BV

How Wikimedia uses ELK

- Log events sent to Logstash by various applications.
- Logstash processes events to clean them up and normalize things where we can.
- Logstash stores events in Elasticsearch.
- Logstash sends some metrics to statsd for trend reporting.
- Use Kibana to search log events from Elasticsearch.
- Icinga alerts to watch for bad trends.

Logstash inputs

- Apache2 & HHVM via rsyslog
- MediaWiki via Monolog and Syslog handler
- scap via log2udp forwarding
- Various nodejs services via Bunyan and gelf-stream
- Cassandra via Logback
- (Beta cluster) Puppet via custom Report plugin
- (Beta cluster) Syslog
- (Labs) IRC
- Many others possible...

Logstash filters

- Strip ansi color escape sequences
- Join sequential lines into a single event for some types
- Normalizations to populate common attributes:
  - **type**: Origin (eg mediawiki, apache2, hhvm)
  - **channel**: Event type (eg memcached, proxy_fcgi)
  - **level**: Severity (eg INFO, WARNING, ERROR
- Normalize event level naming to PSR-3 standard
- Discard junk messages
- Many others possible...

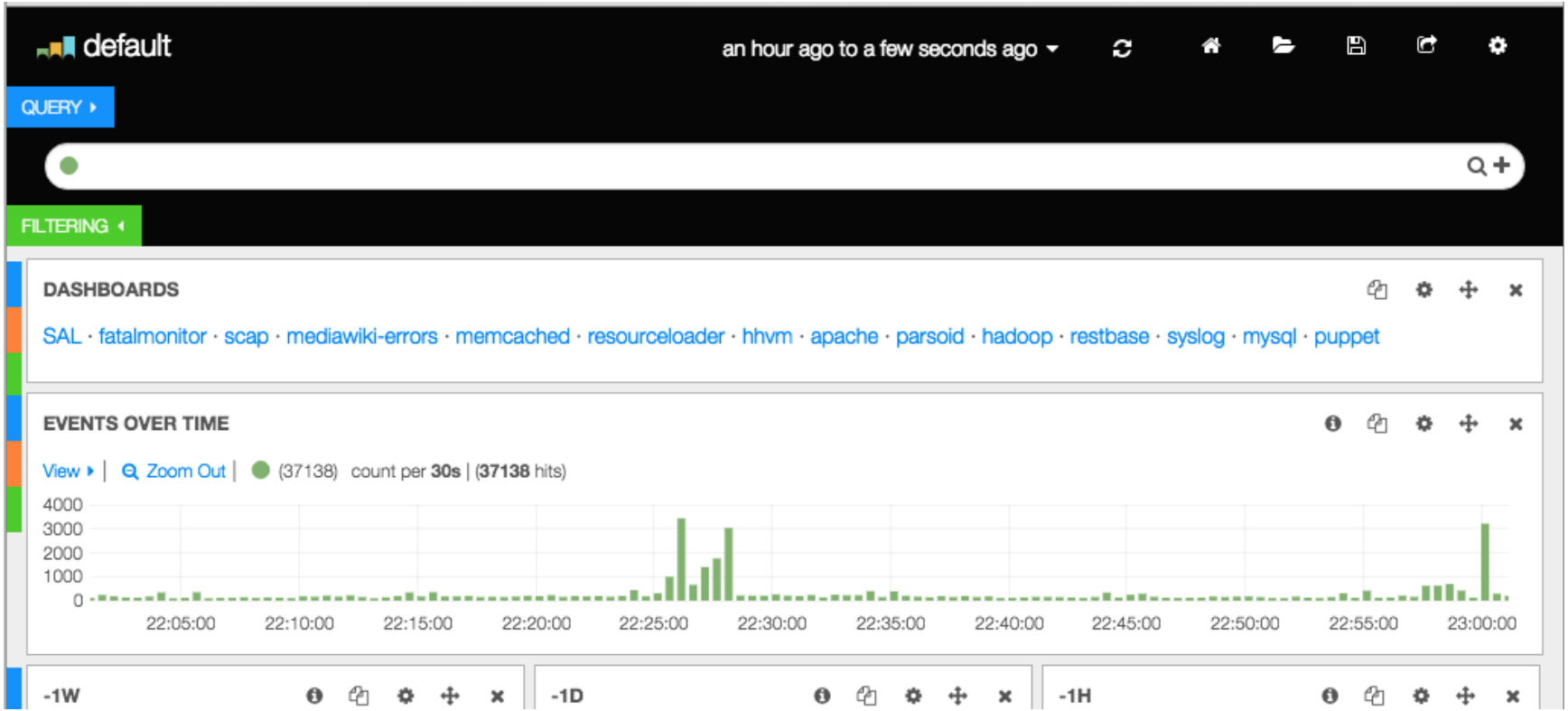
Logstash outputs

- Local Elasticsearch cluster
- Remote Elasticsearch cluster
- Statsd metrics for Graphite storage
- Many others possible...

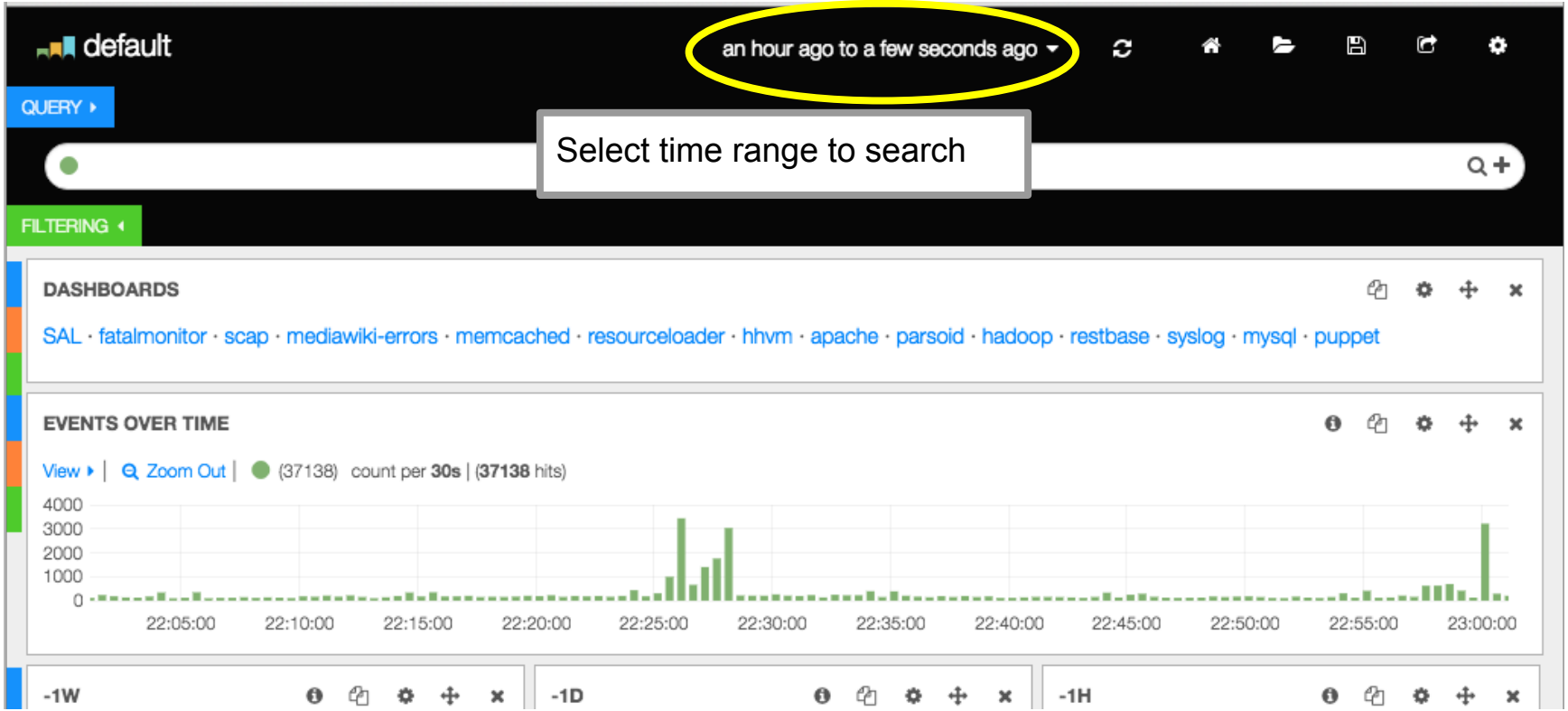
Using Kibana

- WMF production: https://logstash.wikimedia.org/
  - Requires a signed NDA because of access to potentially sensitive data.
- WMF Beta cluster: https://logstash-beta.wmflabs.org/

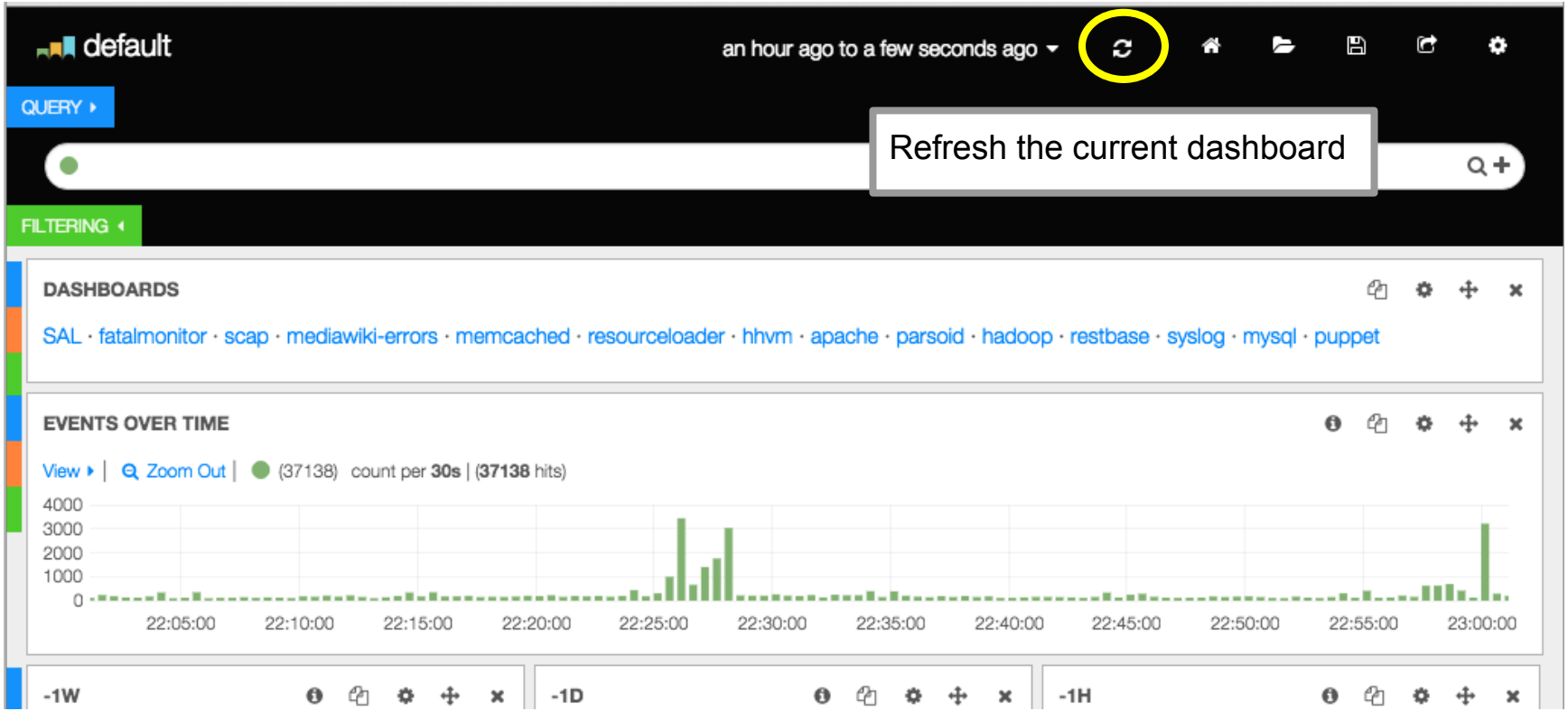
Using Kibana



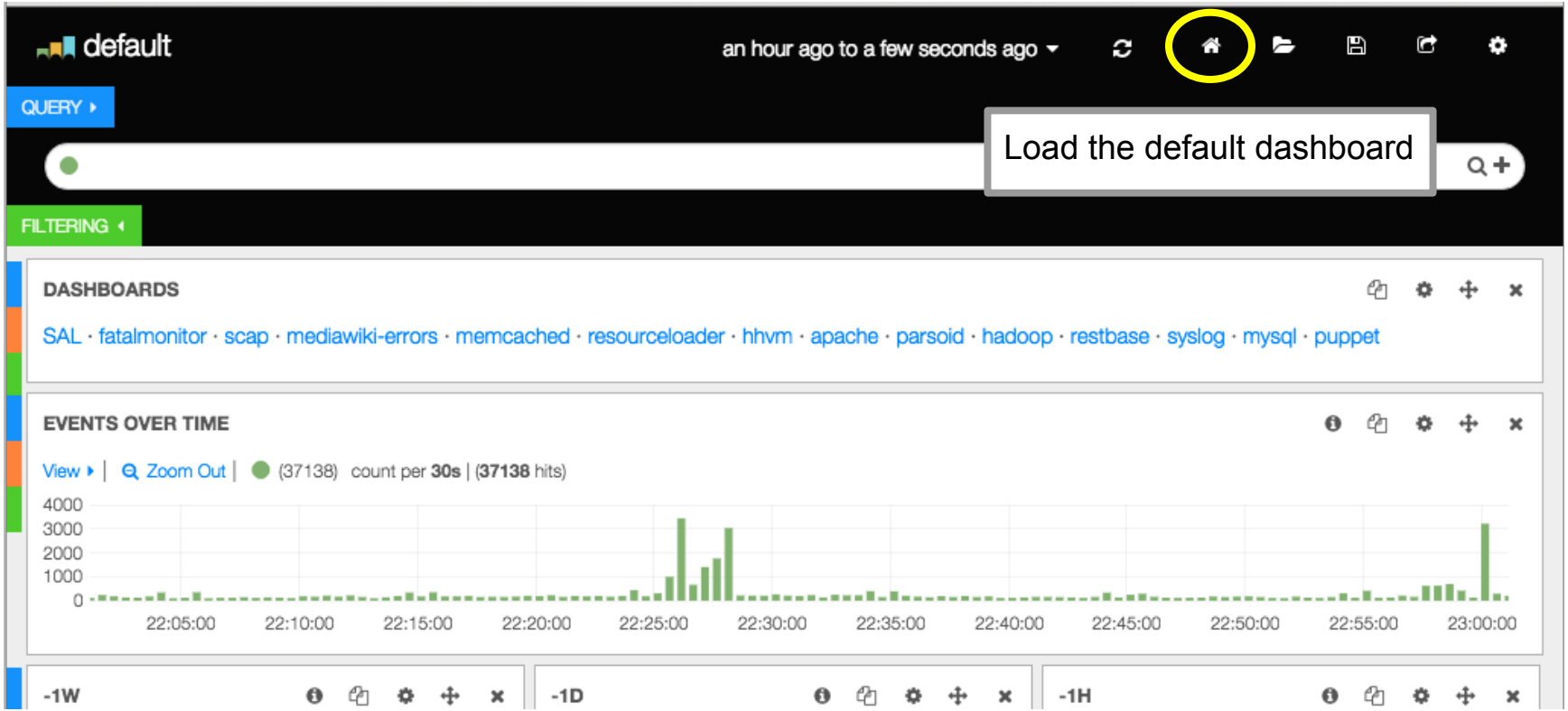
Using Kibana



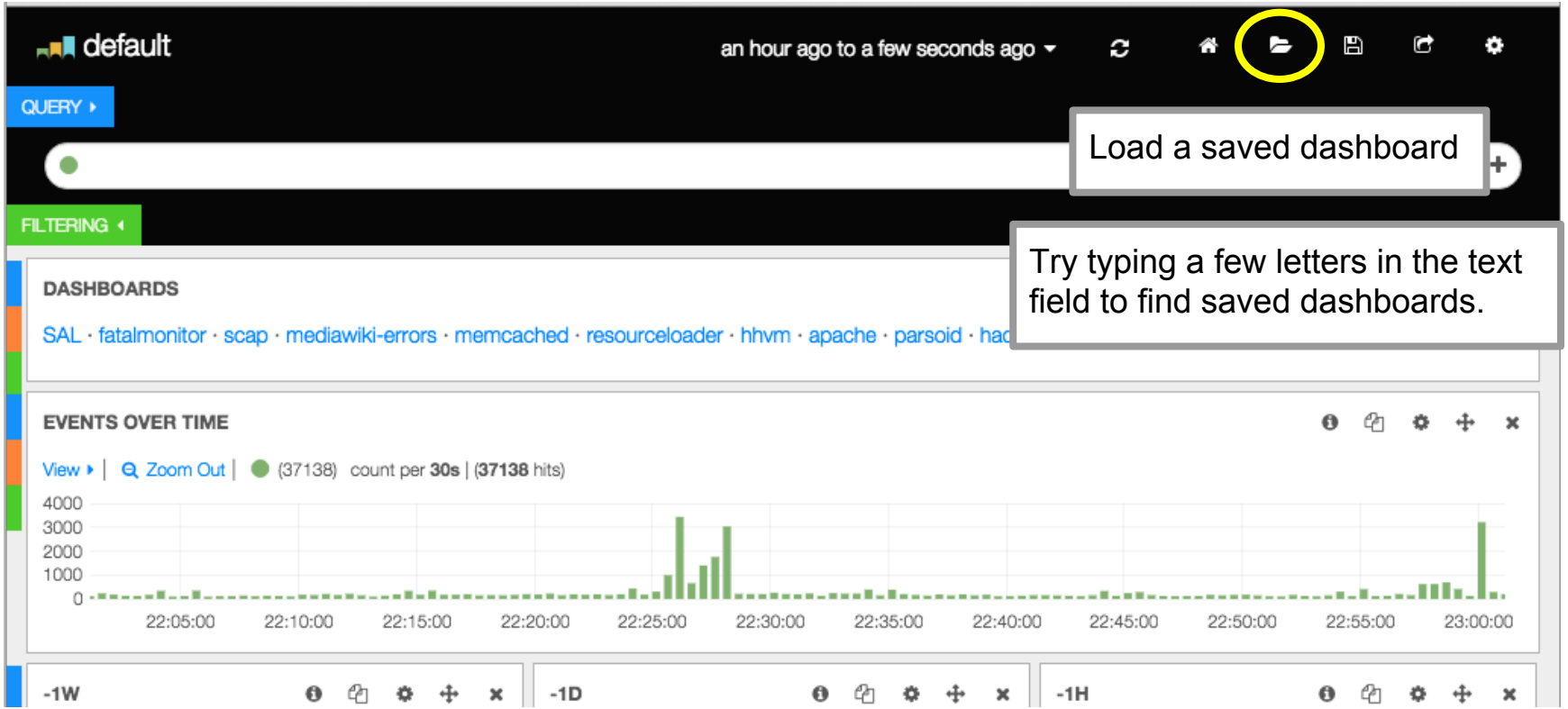
Using Kibana



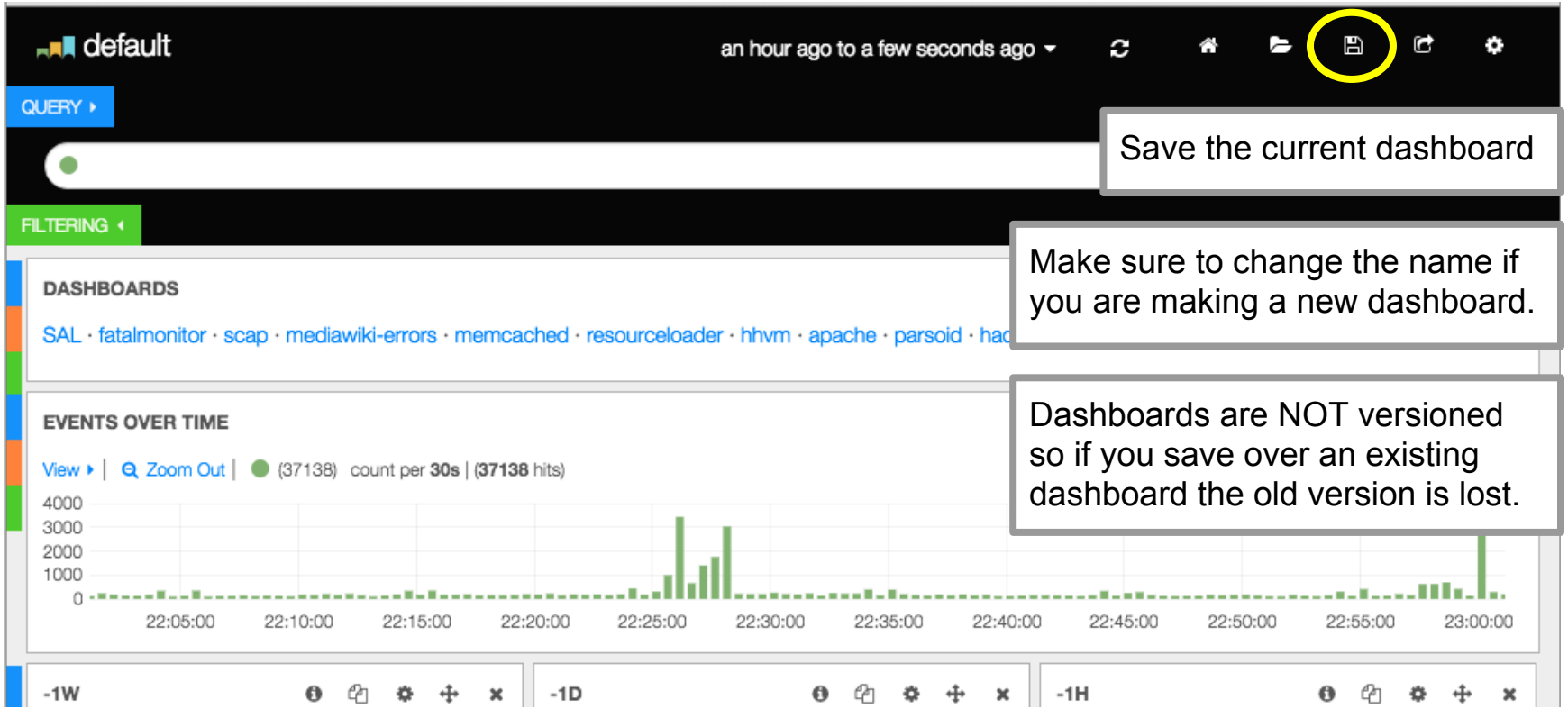
Using Kibana



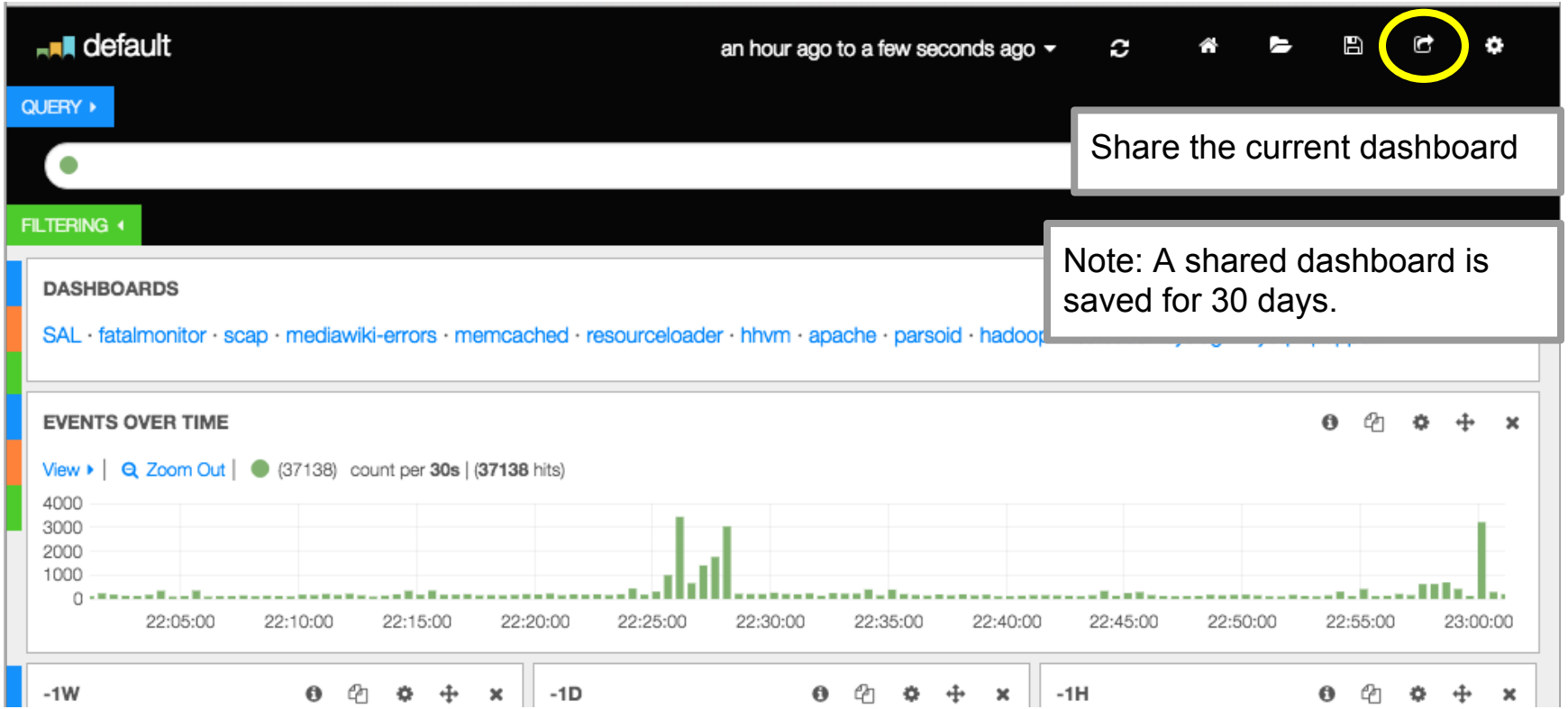
Using Kibana



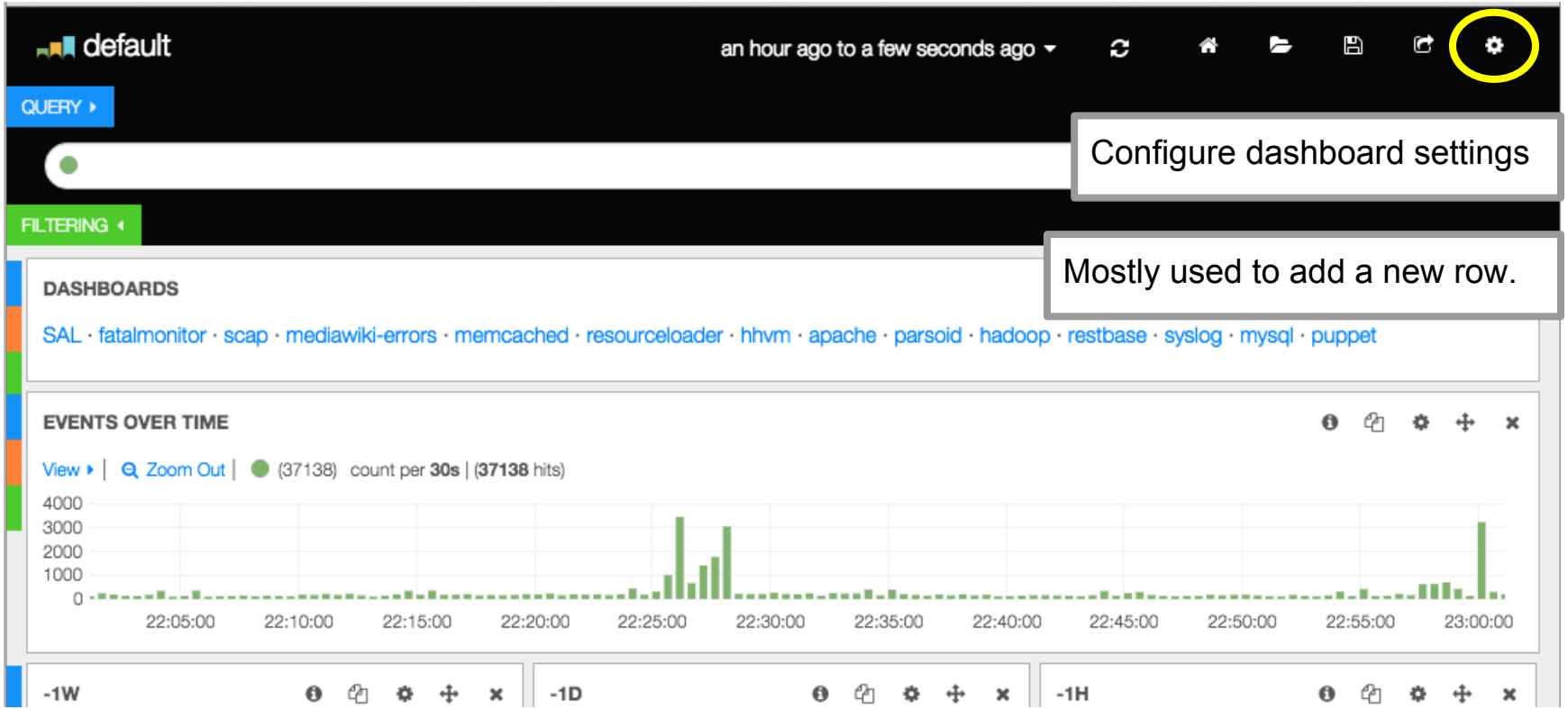
Using Kibana



Using Kibana

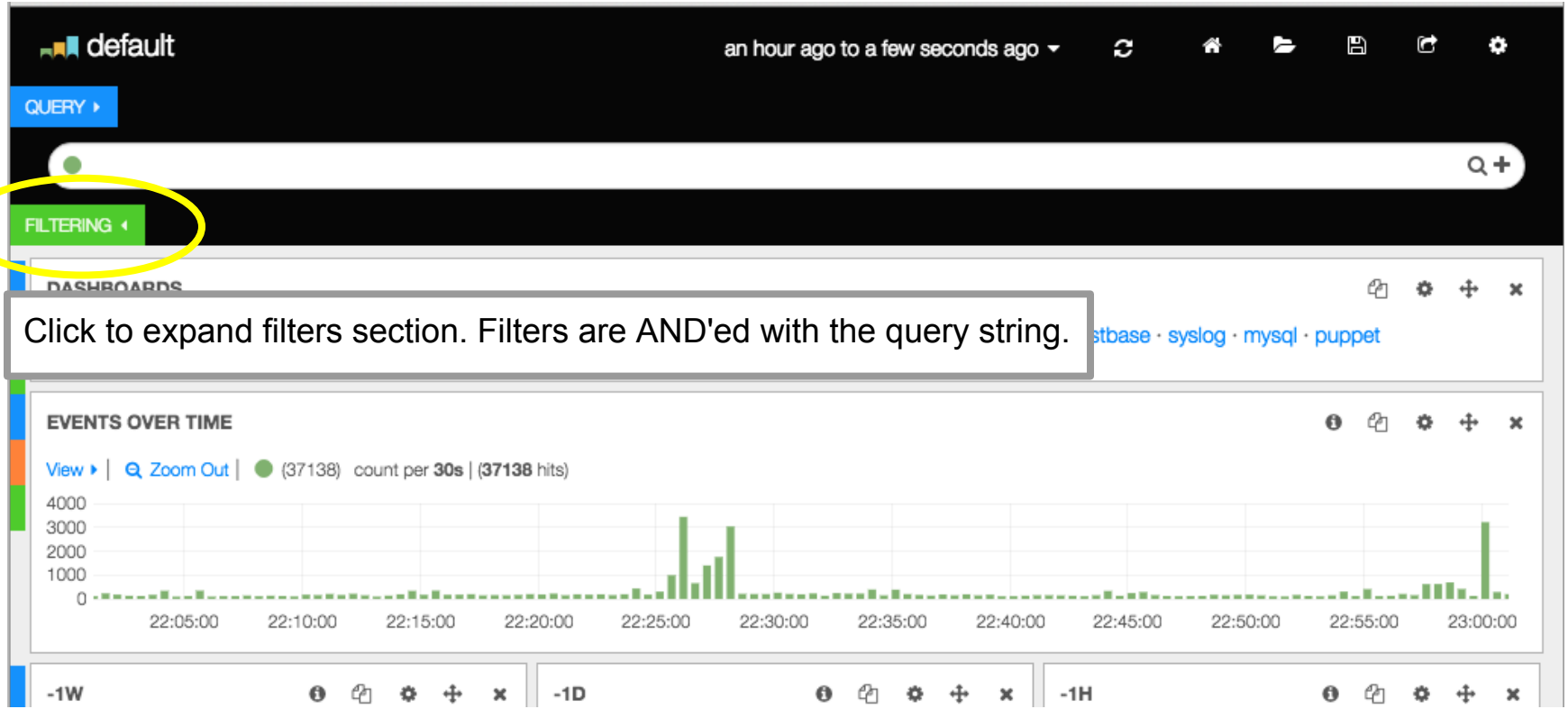


Using Kibana

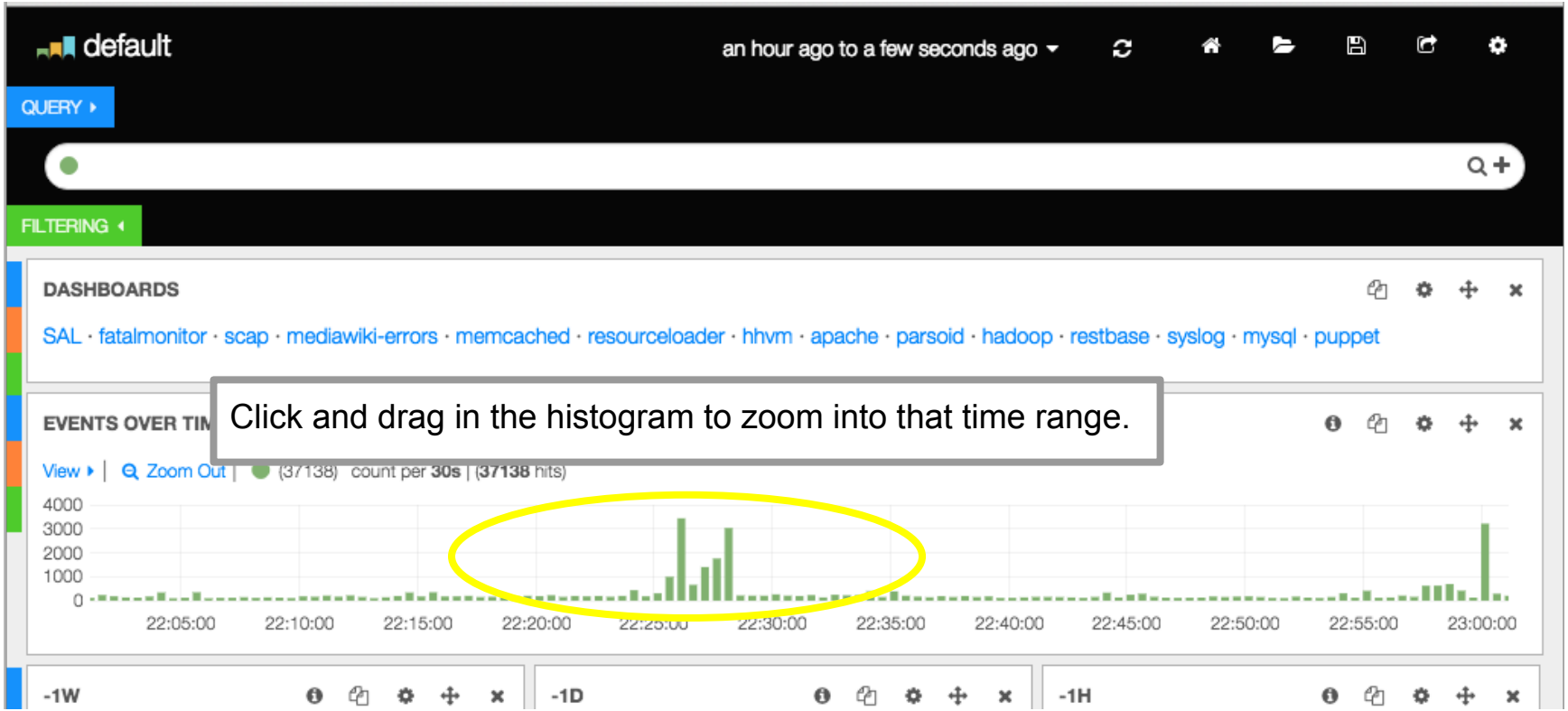


Using Kibana

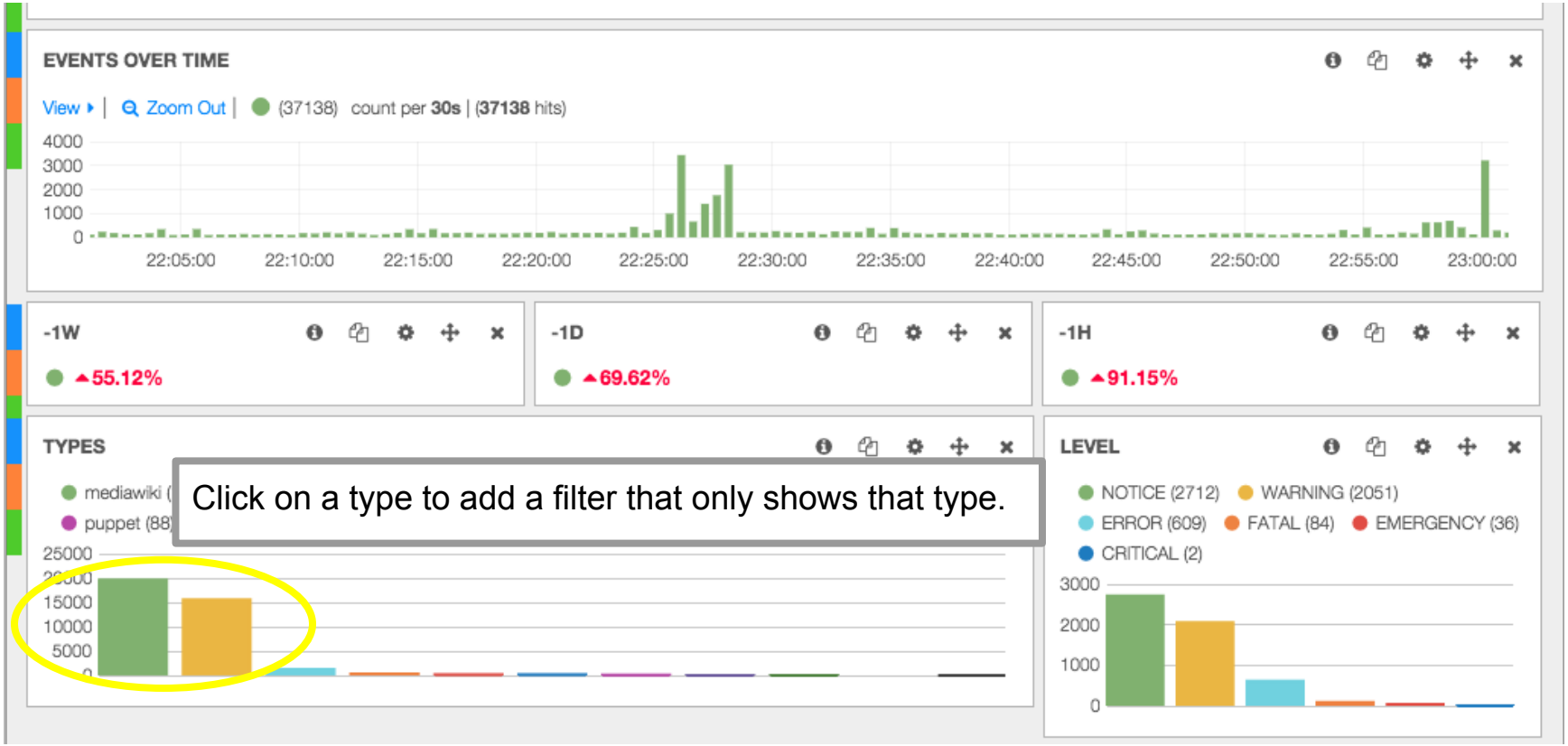
Using Kibana



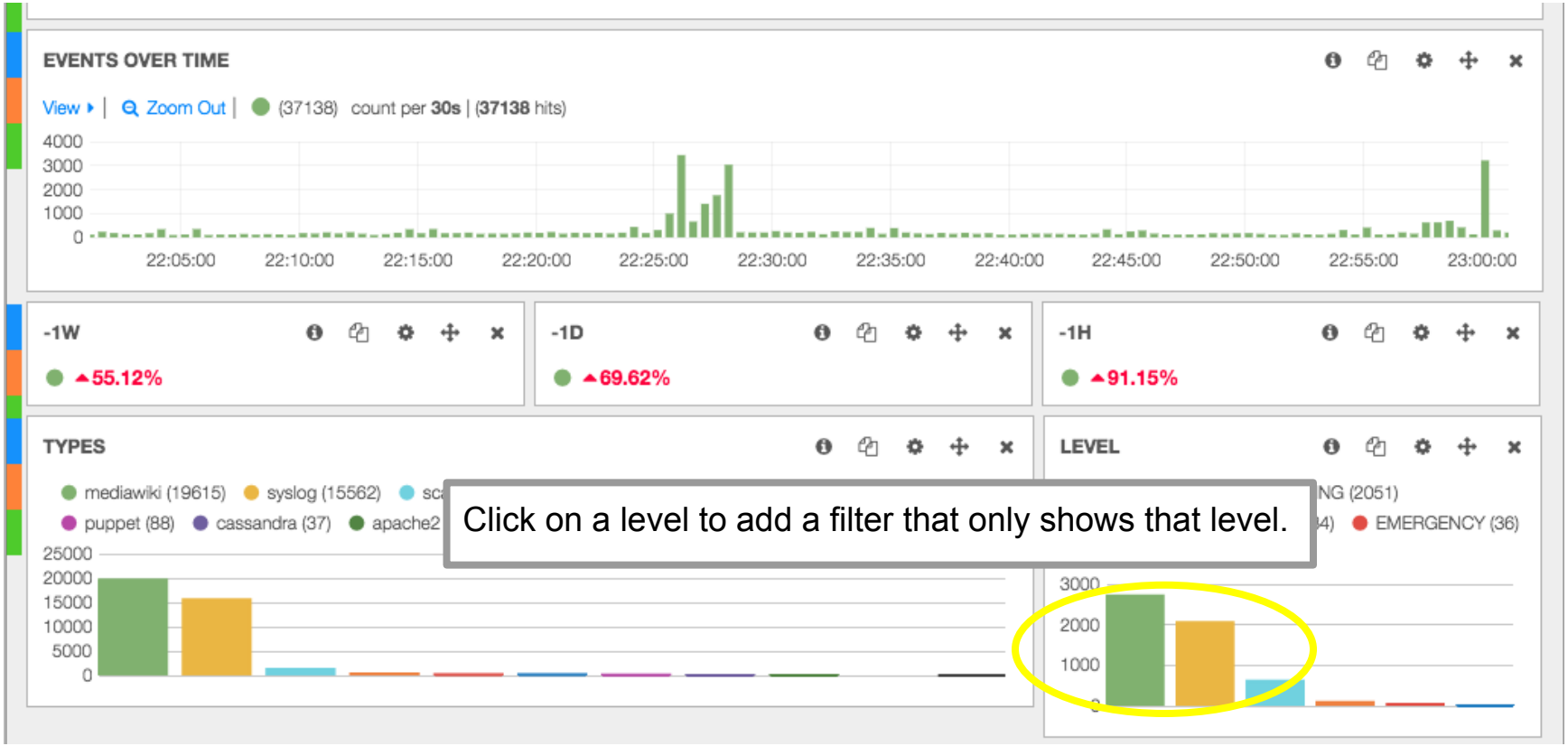
Using Kibana



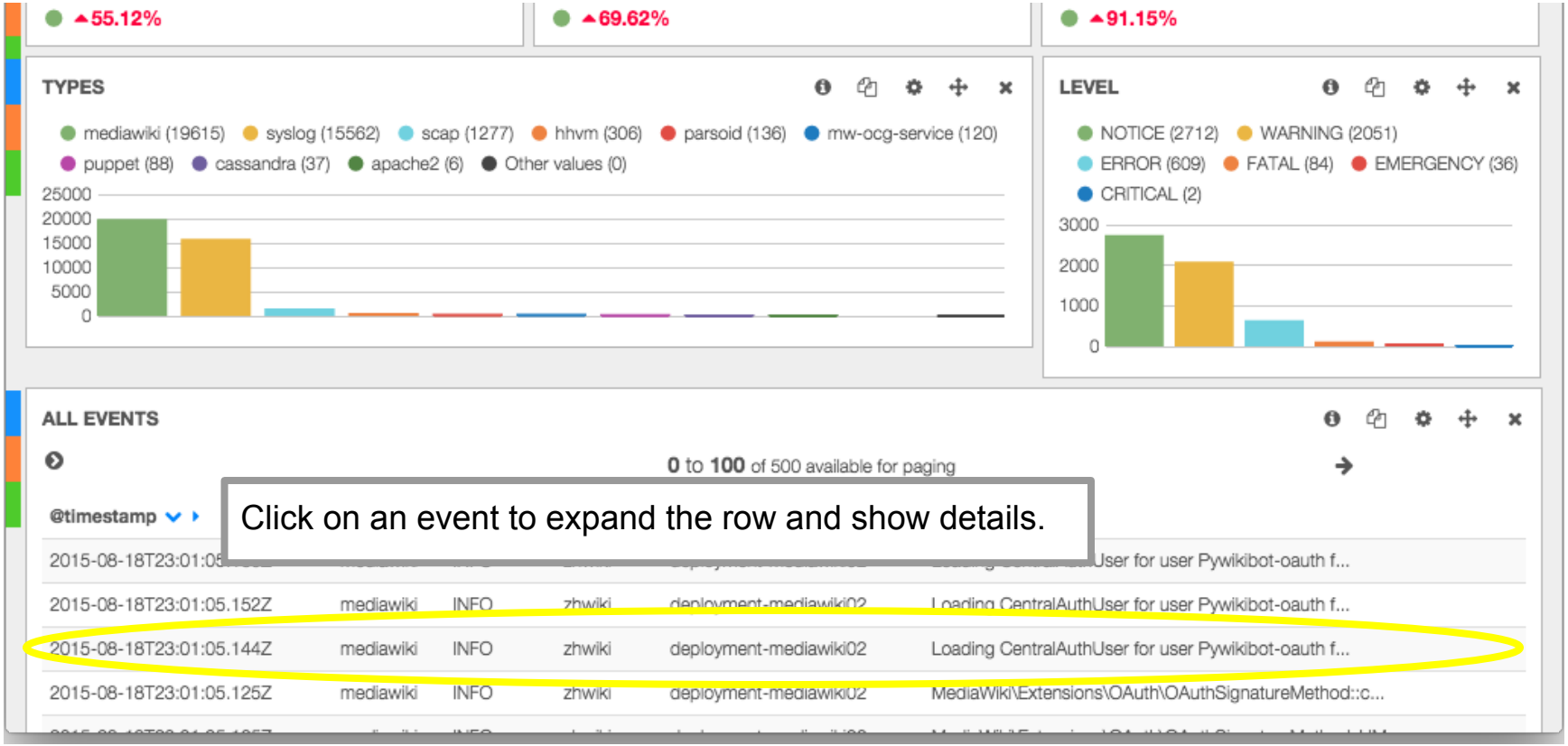
Using Kibana



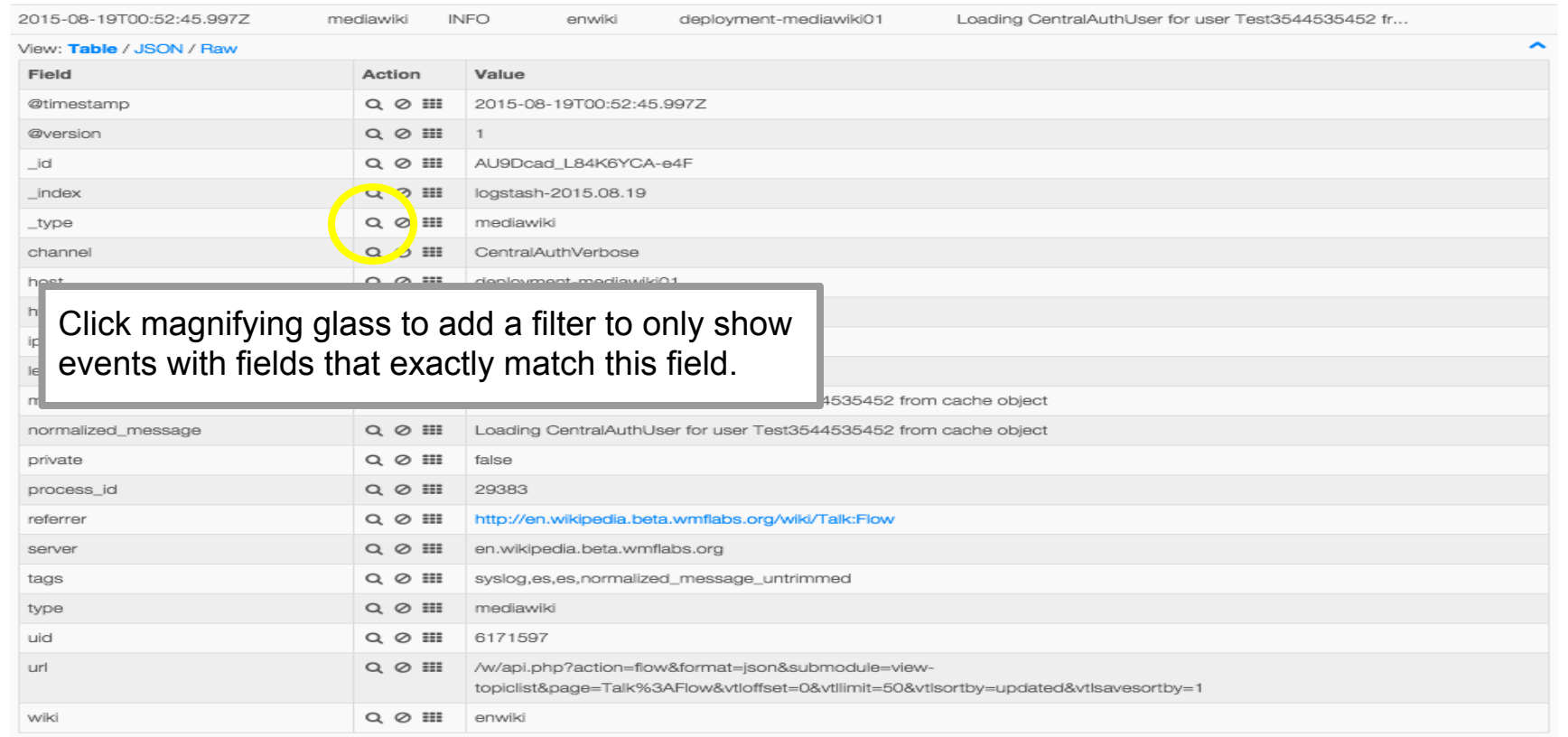
Using Kibana



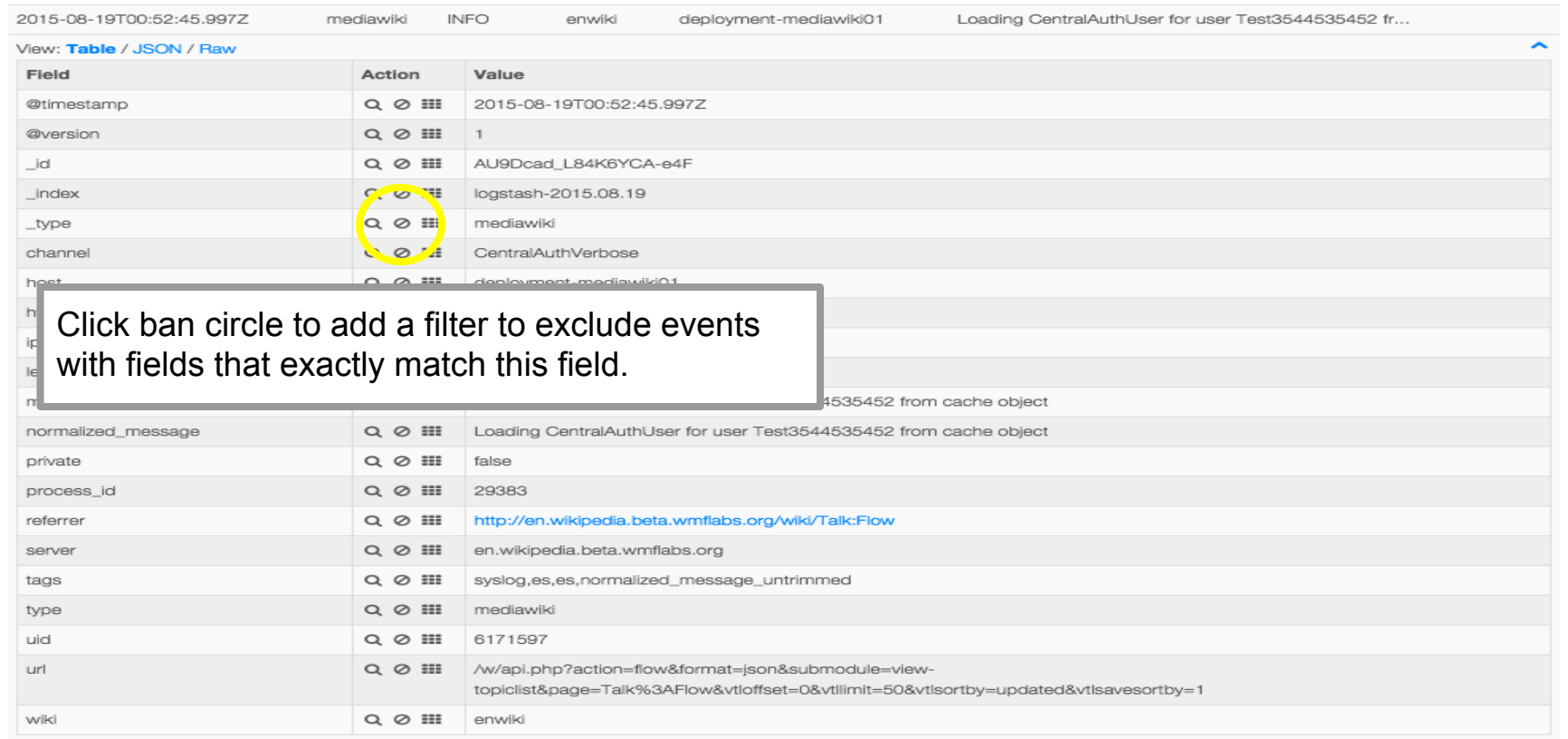
Using Kibana



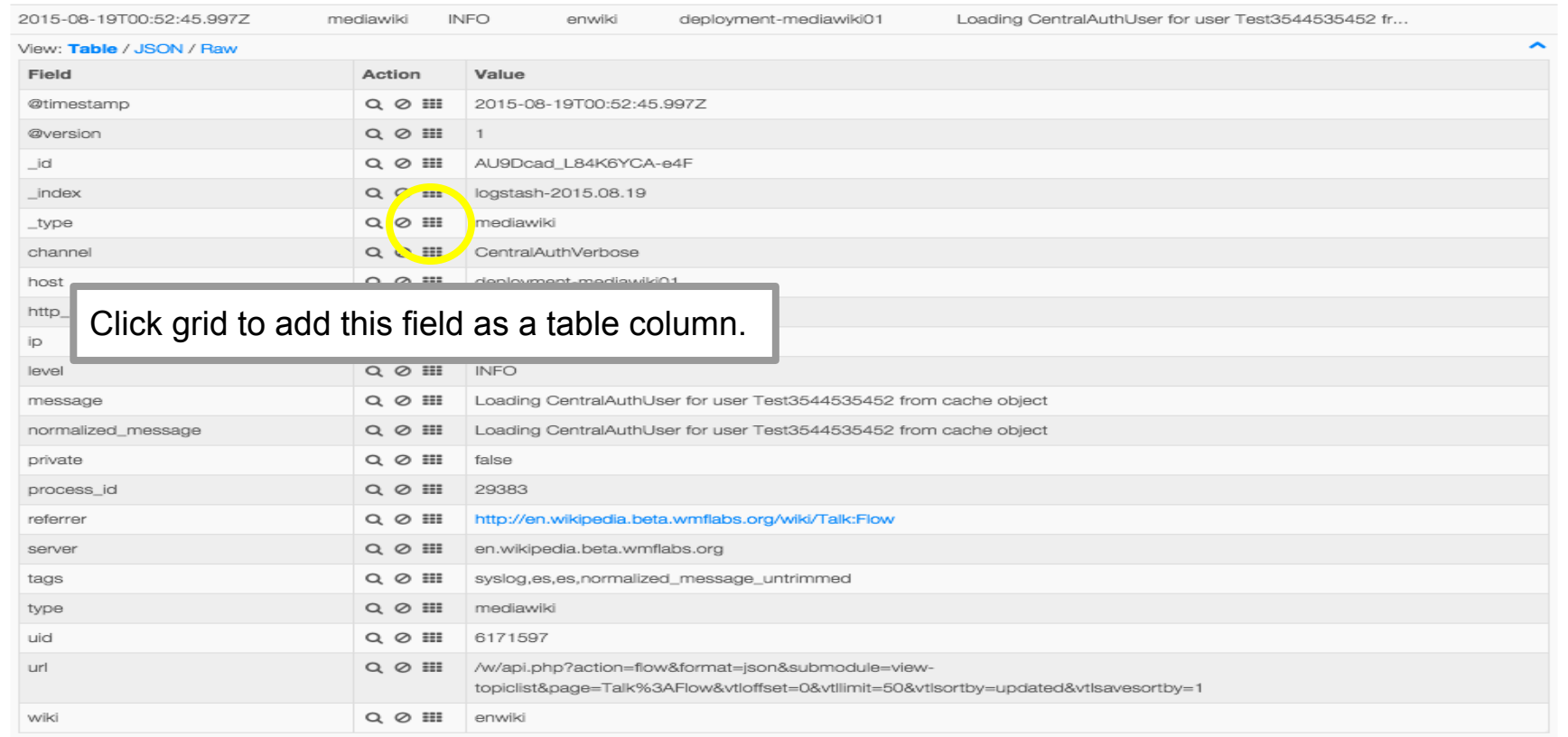
Using Kibana



Using Kibana



Using Kibana



Search tips

- Equivalent of /a/mw-log/fatal.log on fluorine:
  - `type:mediawiki AND channel:fatal`
- In general:
  - `type:mediawiki AND channel:$logGroup`
- If you get no results:
  - try a larger time range
  - check for filters in the collapsed filter section
- Shorter time ranges == faster searches

Better log output from MediaWiki

```php
<?php
use MediaWiki\Logger\LoggerFactory;

$logger = LoggerFactory::getInstance( "channel_name" );

$logger->debug( "Something too spammy for prod logging" );
$logger->info( "Valuable state change info" );
$logger->warning( "Soft error condition" );
$logger->error( "Hard error that needs attention" );
```

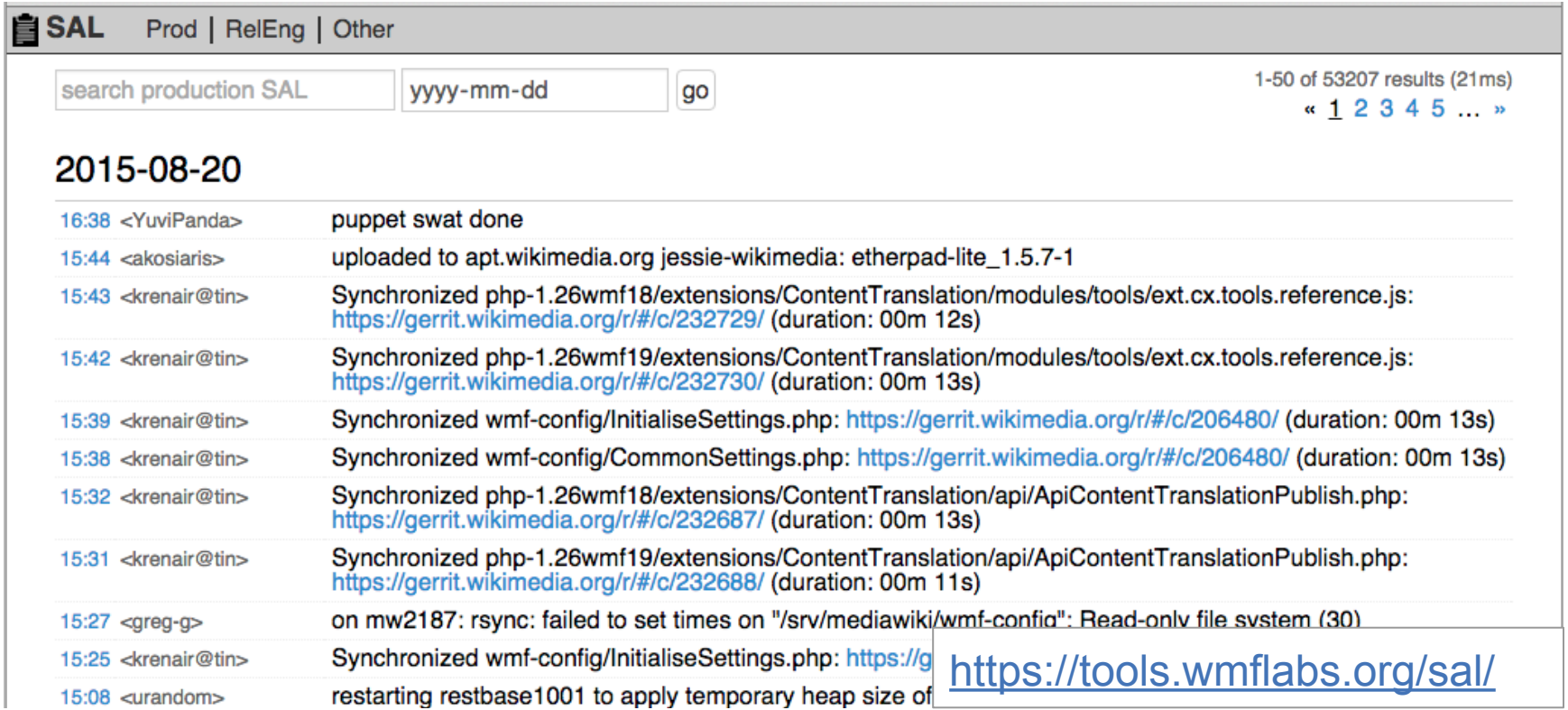
Adding context to messages

```php
<?php

$logger->info( "Valuable state change", array(
        'thing' => $thing,
        'method' => __METHOD__,
        'line' => __LINE__,
) );

$logger->error( "Badness {exception}", array(
        'exception' => $exception,
) );
```

More fun with Logstash



More fun with Logstash

https://tools.wmflabs.org/bash/

Learning more

- https://www.elastic.co/
- https://www.elastic.co/webinars/introduction-elk-stack
- https://www.elastic.co/guide/en/kibana/3.0/index.html
- https://wikitech.wikimedia.org/wiki/Logstash
- https://phabricator.wikimedia.org/tag/elk/
- https://phabricator.wikimedia.org/diffusion/OPUP/browse/production/files/logstash/
- https://www.mediawiki.org/wiki/Structured_logging
- https://phabricator.wikimedia.org/tag/psr3/

Credits

- "Male Elk (8005280487)" by Tony Hisgett from Birmingham, UK. Licensed under CC BY 2.0 via Wikimedia Commons.
- Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries.
- Kibana is a trademark of Elasticsearch BV, registered in the U.S. and in other countries.
- logstash is a trademark of Elasticsearch BV

Copyright © 2015, Bryan Davis and the Wikimedia Foundation.

This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.