Kibana for Splunk SPL Users

An Elastic Training Course

7.4.2

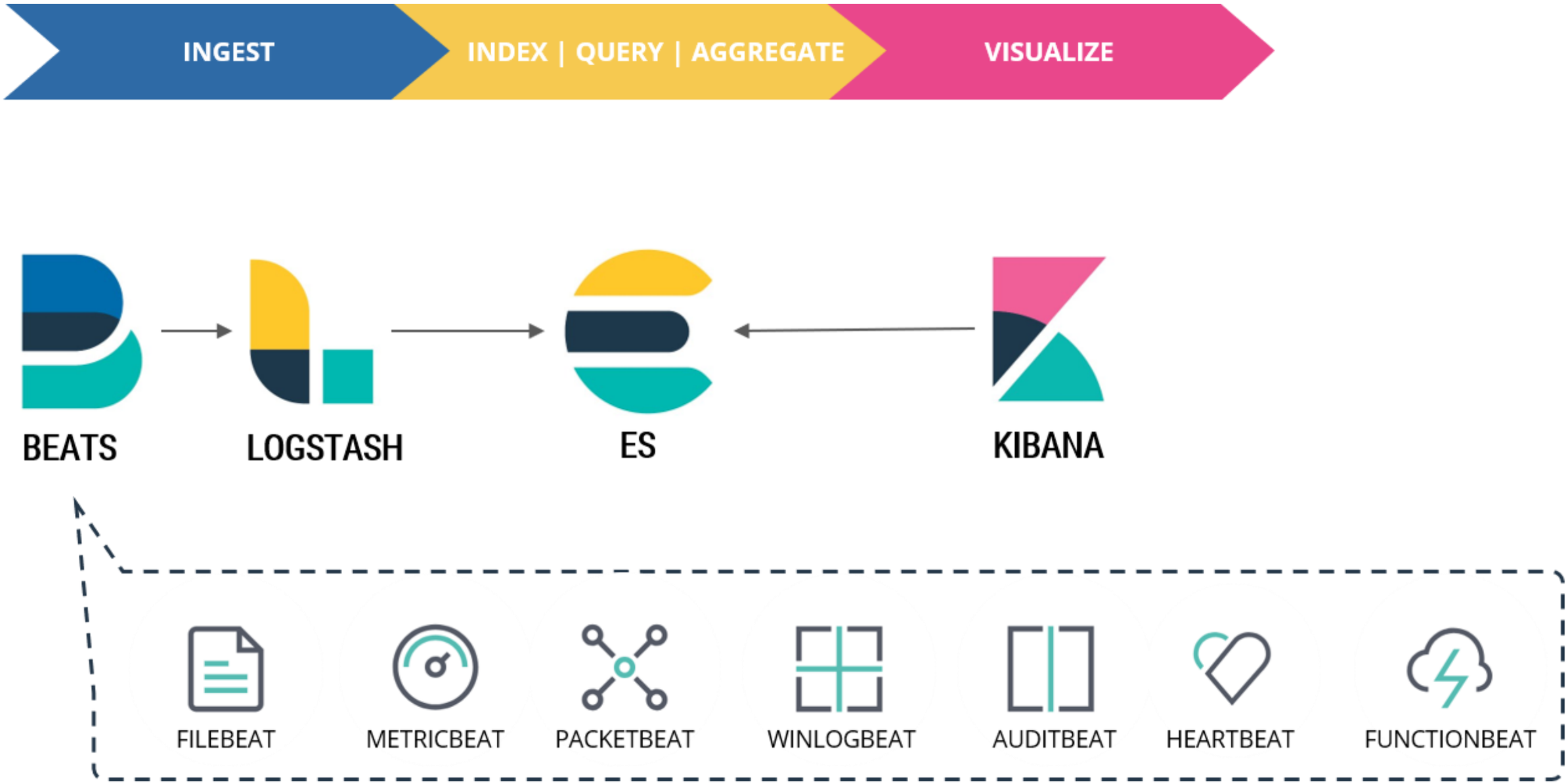
elastic.co/training

Lesson 1

Index=main

elastic

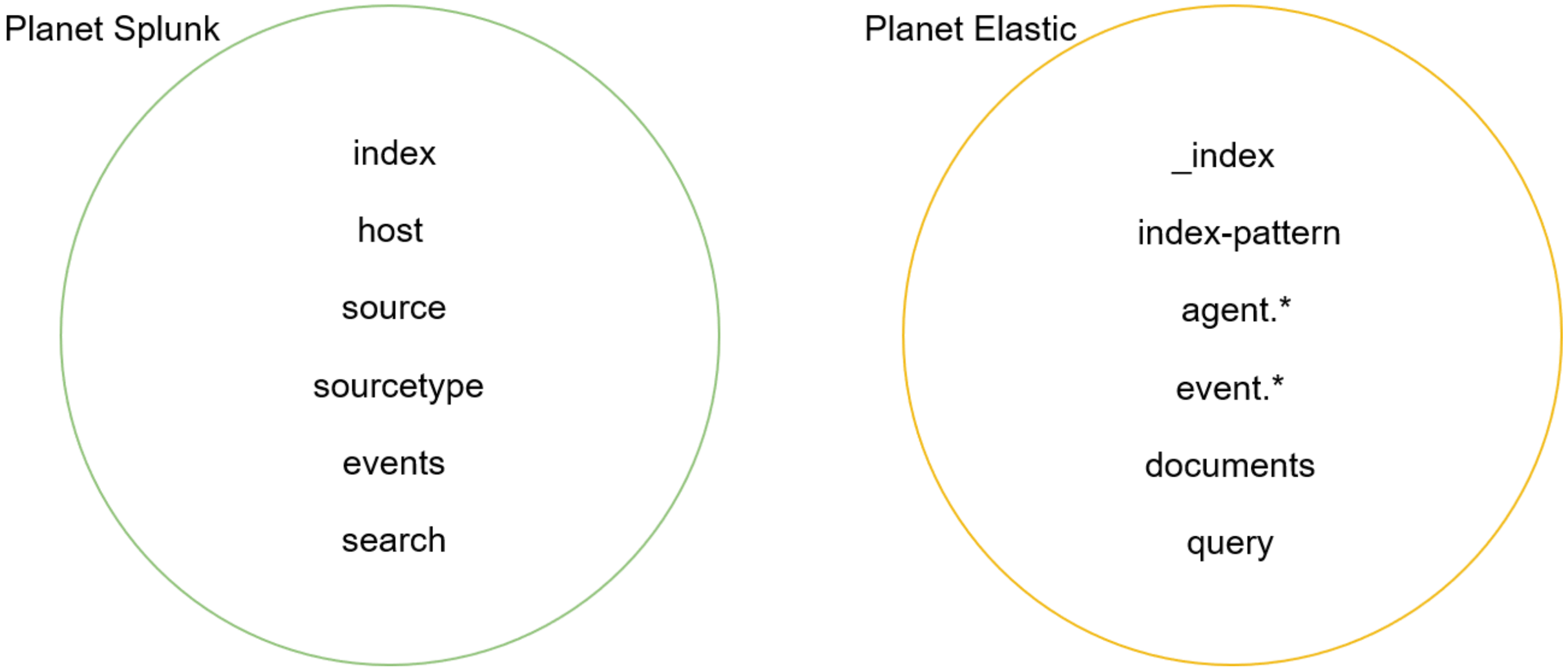
Elastic Stack Overview



Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

elastic

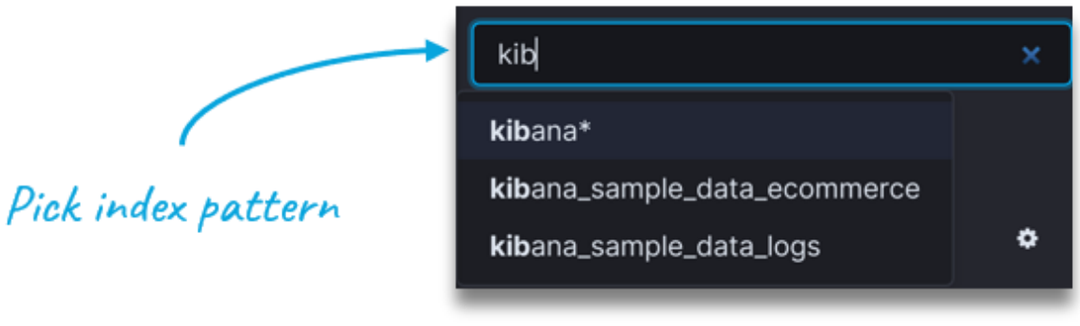
Interplanetary Phrasebook

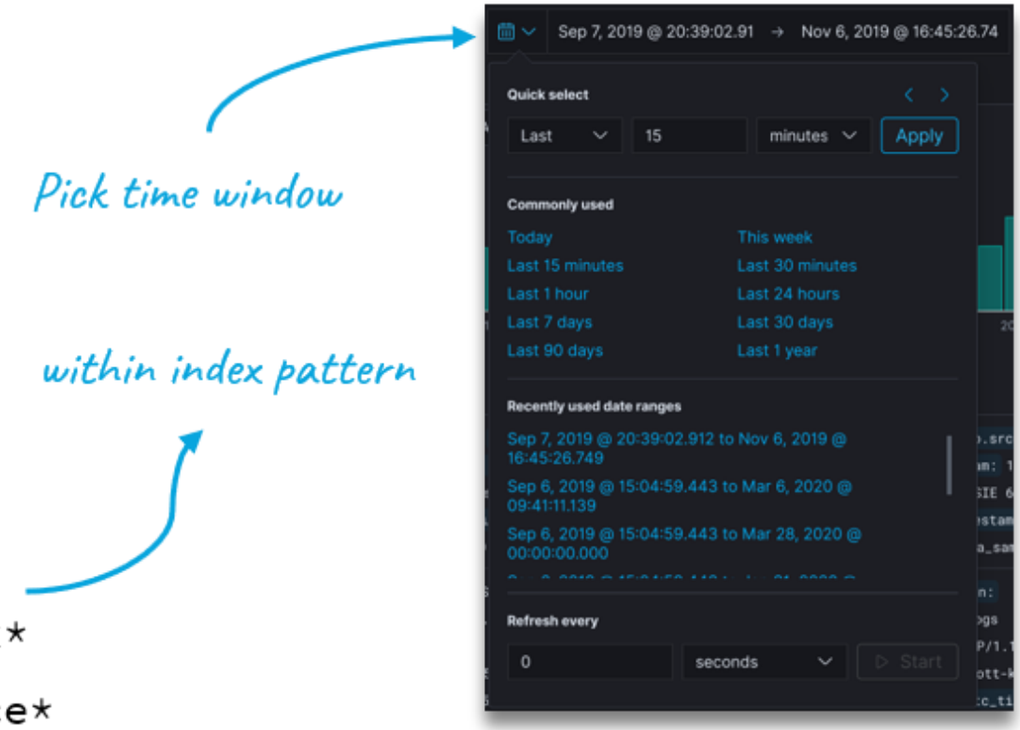


Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

elastic

Scoping Search





SPL

```
index=my_index*
source=my_source*
sourcetype=my_sourcetype*
```

KQL

```
_index: my_index*
source: my_source*
sourcetype: my_sourcetype*
```

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Search Basics

SPL

```
error
response=200
(error AND response=200)
agent=*MSIE*
```

KQL

```
error
response: 200
(error AND response: 200)
agent: MSIE
agent.keyword : *MSIE*
```

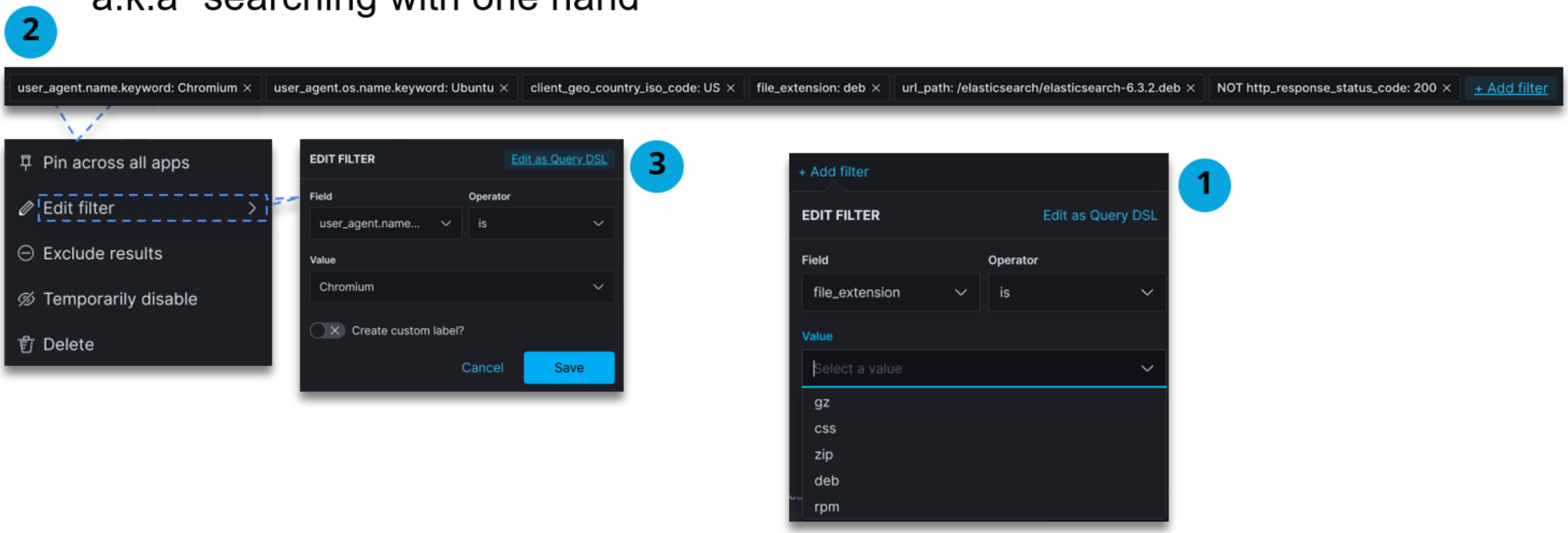
analyzed text field

agent	[“mozilla”, “4.0”, “compatible”, “msie”, “6.0”, “windows”, “nt”, “5.1”, “sv1”, “net”, “clr”, “1.1.4322”]
agent.keyword	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Filtering

a.k.a “searching with one hand”

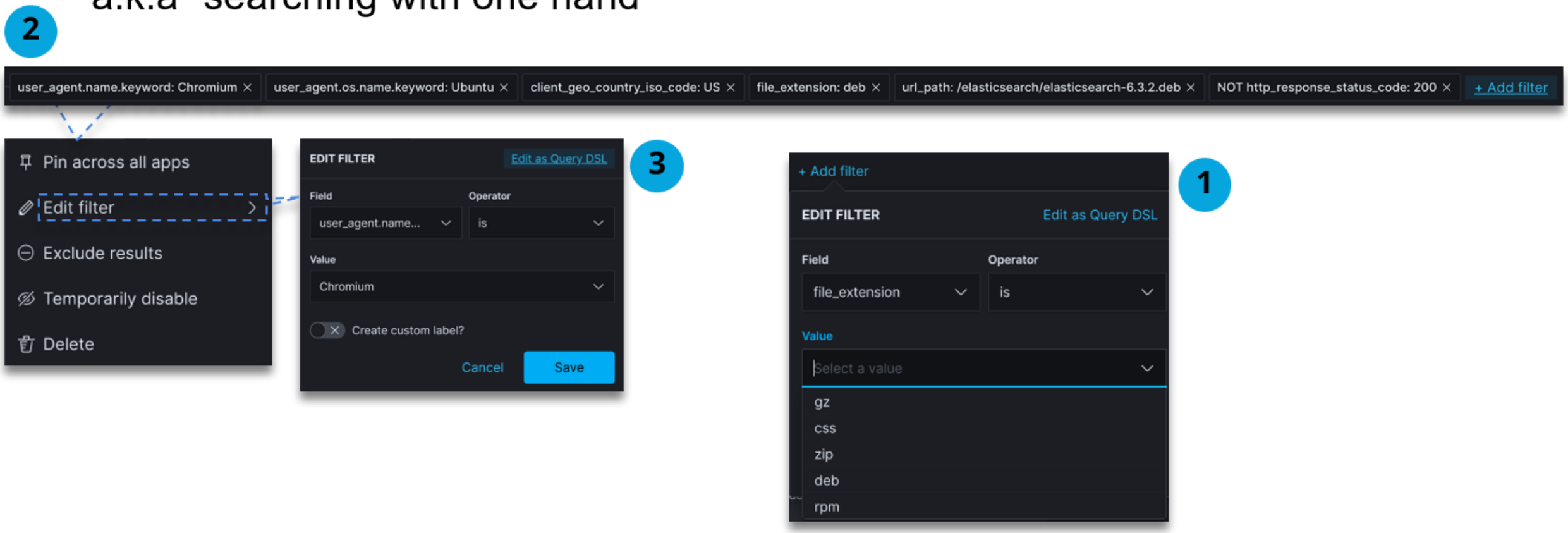


Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

elastic

Top n Analysis

a.k.a “searching with one hand”



Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

elastic

Module Name

Lesson 1

Review - index=main

elastic

Summary

- An index pattern tells Kibana which Elasticsearch indices contain the data that you want to work with
- You can configure the time field for time based indices and use the time picker to scope data analysis
- KQL and Kibana Filters are two main ways to search and filter data from within Kibana
- Data Tables can be used to perform top N analysis in Kibana and operate similar to Pivot tables in spreadsheets

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Quiz

1. Which type of field is available in the search bar offers typehead values?
2. In the background, Kibana filters get translated to which of the following choices below?
3. When creating a data table, which type of aggregation would you use to group fields by?

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Lesson 1

Lab - index=main

elastic

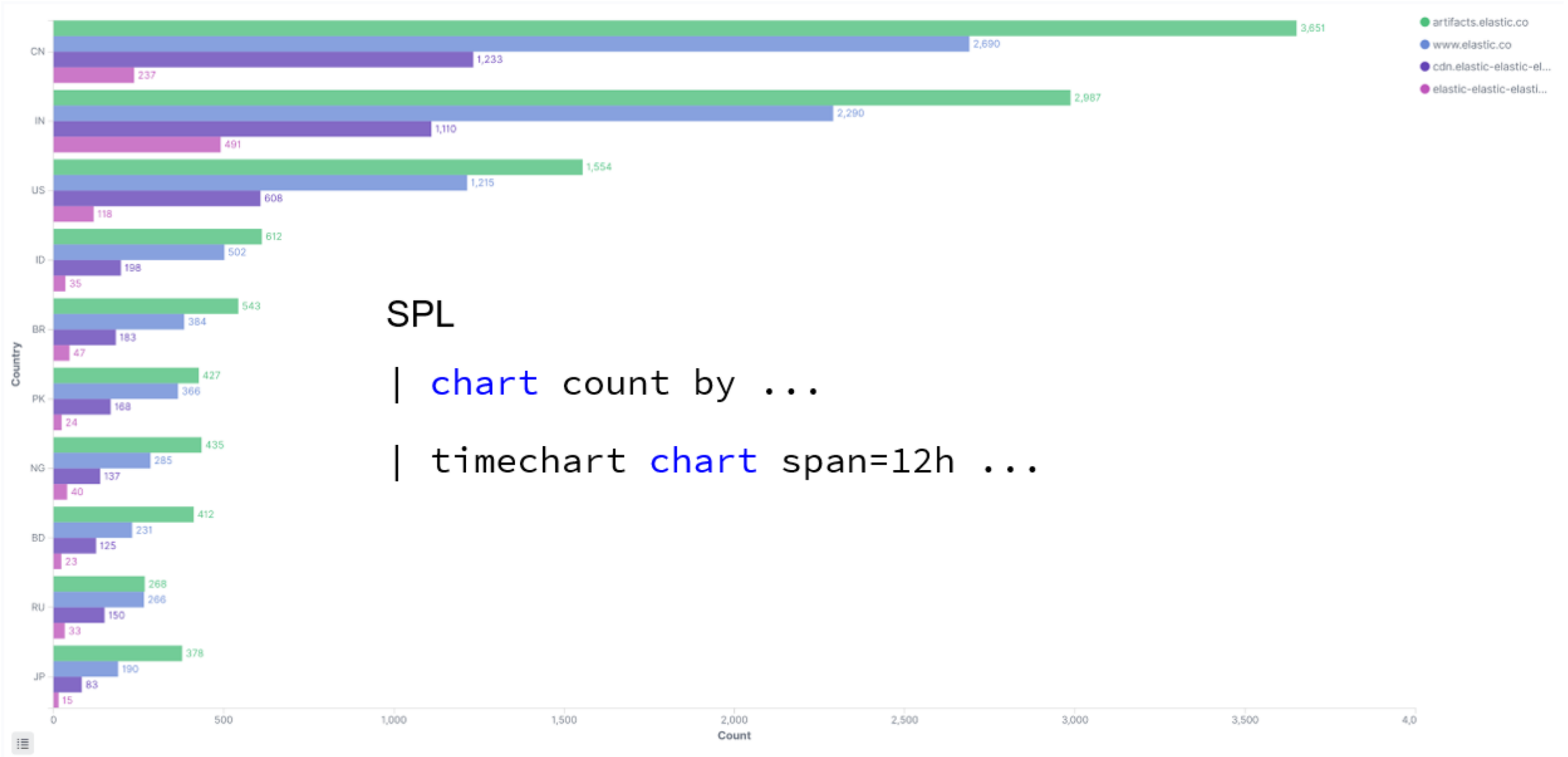
Kibana for Splunk SPL Users

Lesson 2

| chart

elastic

Simple Charting



SPL

```
| chart count by ...
| timechart chart span=12h ...
```

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

elastic

Aggregation

Bucket by	Aggregation
Time Period	Date Range
	Date Histogram
Strings	Terms
	Significant Terms
Numerics	Range
	Histogram
IP Address	IPV4 Range

What do you want to group by?

What do you want to calculate for those groups?

Metric
Count
Distinct Count
Min/Max
Sum
Average
Median
Percentile
...

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Lesson 2

Review - | chart

elastic

Summary

- You can start visualizations from Exploratory Data Analysis using the fields list in the Discover App
- Time charts can be created by visualizing on the time field and by default, the date histogram aggregation will be used
- Elasticsearch Bucket and Metric aggregations are fundamental to visualizing data in Kibana
- TSVB provides an integrated analysis interface that enables us to create multiple visualizations that are related

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Quiz

1. **True or False.** To be able to visualize on a field from fields, the field must be aggregatable.
2. Which bucket aggregation is supported on a time field?
3. What is **NOT** a valid visualization in TSVB?

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Lesson 2

Lab - | chart

elastic

Kibana for Splunk SPL Users

Lesson 3

| eval

elastic

Eval

200	OK
404	Created
503	Service Unavailable

SPL

```
| eval status=case(code == 200, "OK", code == 404, "Not found", code
==503, "Service Unavailable",true(), "Other")
```

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Eval

200	OK
404	Created
503	Service Unavailable

PAINLESS

```
def codes = ['200': 'OK', '404': 'Not Found', '503': 'Service Unavailable'];
return codes[doc['response'].value];
```

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Replace

Useragent	Browser
Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1	Firefox
Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24	Chrome
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)	IE

SPL

```
| replace *Firefox* with Firefox, *Chrome* with Chrome, *MSIE* with “IE”
```

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Replace

PAINLESS

1

```
if(doc['agent.keyword'].value.contains('Firefox')) {
    return 'Firefox'
} else if(doc['agent.keyword'].value.contains('MSIE')) {
    return 'IE'
} else if(doc['agent.keyword'].value.contains('Chrome')) {
    return 'Chrome'
}
```

2

```
def m = /.*(Chrome|Firefox|MSIE).*/.matcher(doc['agent.keyword'].value);
return m.matches() ? m.group(1) : "Other"
```

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Lookup

Suspicious
177.120.218.48
70.35.217.22
112.82.236.207
236.212.255.77
44.209.117.254
167.94.220.213
97.135.81.200

SPL

```
| lookup suspicious.csv | ...
```

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Lookup

Suspicious
177.120.218.48
70.35.217.22
112.82.236.207
236.212.255.77
44.209.117.254
167.94.220.213
97.135.81.200

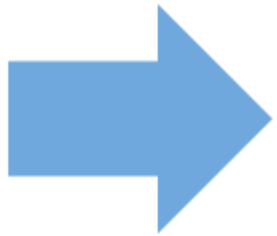
PAINLESS

```
def s = [
 '177.120.218.48',
 '70.35.217.22',
 '112.82.236.207',
 '236.212.255.77',
 '44.209.117.254',
 '167.94.220.213',
 '97.135.81.200'];
return s.contains(doc['clientip'].value) ? "Yes" : "No";
```

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Split

Referrer
http://www.elastic-elastic-elastic.com/success/alan-g-poindexter
http://twitter.com/success/elliot-see
http://twitter.com/success/michael-mcculley
http://www.elastic-elastic-elastic.com/success/pham-tuan
http://twitter.com/success/andr-kuipers



Domain
www.elastic-elastic-elastic.com
twitter.com
twitter.com
www.elastic-elastic-elastic.com
twitter.com

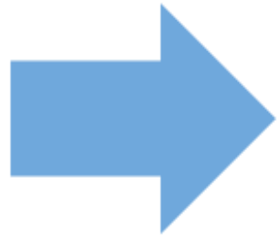
SPL

```
| eval temp=split(referrer,"/") | eval domain=mvindex(temp,0)
```

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Split

Referrer
http://www.elastic-elastic-elastic.com/success/alan-g-poindexter
http://twitter.com/success/elliot-see
http://twitter.com/success/michael-mcculley
http://www.elastic-elastic-elastic.com/success/pham-tuan
http://twitter.com/success/andr-kuipers



Domain
www.elastic-elastic-elastic.com
twitter.com
twitter.com
www.elastic-elastic-elastic.com
twitter.com

PAINLESS

```
return doc['referrer'].value.splitOnToken('/')[2];
```

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Syntax Review

```
return x;
```

```
def r = doc['response.keyword'].value;
```

```
def s = ['177.120.218.48','70.35.217.22', ...];
```

```
def m = /my_pattern/.matcher("text");
```

```
m.matches() ? m.group(1) : "Other"
```

```
if (x) { // do something } else { // do something else }
```

```
s.contains(doc['clientip'].value) ? "Yes" : "No";
```

```
doc['referrer'].value.splitOnToken('/')[2];
```

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Lesson 3

Review - | eval

elastic

Summary

- Scripted Fields are fields whose values are computed at search time by running a script
- Painless is the default scripting language in Elasticsearch and can be used in Kibana to compute values for scripted fields
- Painless supports all of Java's control flow statements except the switch statement
- Painless also supports many statements with Apache Groovy programming language syntax

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Quiz

1. If you need to access the value of a field called 'my_field' in your documents in Painless, which syntax would you use?
2. Using `def` to define a variable in Painless will make it a _____ type.
3. In Painless, how would you check membership of 'apple' in a list called fruits?

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

elastic

Lesson 3

Lab - | eval

elastic

Thank You!

Please complete the online survey.

elastic

Lesson 1: Quiz Answers

1. Keyword. Short strings that typically fit into a dropdown box are good candidates for keyword type. Internally a data structure called doc values are created for these types of fields that makes it easier to be retrieved and made available for UI functions like typeahead.

2. Elasticsearch Query DSL. Query DSL is based on JSON and can be used to define queries. It is very extensive and offers a lot of flexibility to construct precise queries.

3. Bucket aggregations can be used to group data by both categorical fields and numeric/date ranges. More specifically, the terms aggregation is a good choice when grouping your data by categorical values.

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

Lesson 2: Quiz Answers

1. True. Fields can either be aggregatable or not, and for visualizing on a field from the fields list in Discover app, the field must be aggregatable.

2. Date Histogram

3. Heatmap. TSVB combines time series, metric, top N, gauges, markdown, and table visualizations.

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

elastic

Lesson 3: Quiz Answers

1. doc['field_name'].value and ctx._source.field_name can be used to access the value of a field in documents although the former is more efficient than the later. If you need to access the value of a string field indexed as an analyzed text field, you cannot use the doc['field_name'].value syntax.

2. Dynamic. A dynamic type value can represent the value of any primitive type or reference type using a single type name def. A def type value mimics the behavior of whatever value it represents at run-time and will always represent the child-most descendant type value of any type value when evaluated during operations.

3. `fruits.contains ('apple')` is supported in Painless to check for membership.

Copyright Elasticsearch BV 2015-2019 Copying, publishing and/or distributing without written permission is strictly prohibited

elastic

Thank You!

Please complete the online survey.

elastic