Cheatography

Kibana Search Tips Cheat Sheet

by maurermj08 via cheatography.com/30033/cs/8894/

Searching

Search Type	Example 1	Example 2
Keyword	usbstor	
OR Keyword	usbstor OR deviceclasses	usbstor deviceclasses
AND Keyword	usbstor AND deviceclasses	
NOT Keyword	NOT usbstor	
Phrase*	"/WINDOWS/system32/config/"	“WINDOWS system32 config”
Field Match	termname:keywordone	source_short:webhist
Exact Field Match**	parser.raw:"sqlite/firefox_cookies"	
OR Term Search	source_short:(reg evt)	source_short:reg source_short:evt
Field Exists	_exists_:star	
Field Missing	_missing_:star	
Wildcards***	*.exe	*.ppt?
Regular Expressions	/doc([mx]?)/	name:/joh?n(ath[oa]n)/
Fuzzy	svchost~	lsass~1

*Double quotes are required for phrase searching, single quotes do not work

**Not analyzed fields are case sensitive

***Allowing a wildcard at the beginning of a word (eg "*ing") is particularly heavy, because all terms in the index need to be examined, just in case they match

Reference: https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html

Analyzed vs Not Analyzed (.raw)

String (Not Analyzed)	"Set the shape to semi-transparent by calling set_trans(5)"
Standard Analyzed	set, the, shape, to, semi, transparent, by, calling, set_trans, 5

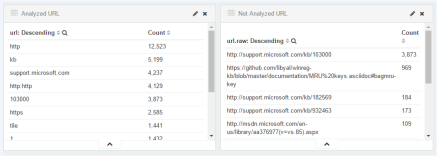
Above is how Elasticsearch stores analyzed vs not analyzed strings for searching.

Not analyzed fields need to be searched as one phrase.

Analyzed fields can be searched using one or more of its sections.

See: https://www.elastic.co/guide/en/elasticsearch/guide/current/mapping-intro.html

Analyzed vs Not Analyzed



By **maurermj08**

cheatography.com/maurermj08/

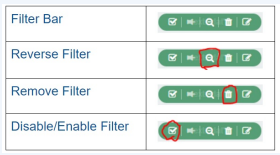
Published 20th August, 2016.

Last updated 20th August, 2016.

Kibana Search Tips Cheat Sheet

by maurermj08 via cheatography.com/30033/cs/8894/

Filters



By **maurermj08**

cheatography.com/maurermj08/

Published 20th August, 2016.
Last updated 20th August, 2016.