## KQL CHEAT SHEET



"win xp"  phrase: Matches the exact phrase "win xp" as it appears (all fields)  os: "win xp"  phrase (field-specific): Matches the exact phrase win xp" as it appears in the field os  or. Matches at least one of "chrome", "firefox" or "safari" in the field browser  tags: ("security" and "error")  and: Field tags contain both security and error as list elements  grouping (values): Field tags matches "security" and also either "warning" or "error"  agent: "MSIE 6.0"  machine.os*: win*  response: 583 and agent: "MSIE 6.0"  response: 583 and agent: "MSIE 6.0"  response: 583 and extension: "gz" or extension: "deb"  response: 583 and extension: "gz" or extension: "deb"  response: 593 and (extension: "gz" or extension: "deb")  response: 593 and ot (extension: "gz" or extension: "deb")  response: 593 and ot (extension: "gz" or extension: "deb")  response: 593 and ot (extension: "gz" or extension: "deb")  response: 593 and ot (extension: "gz" or extension: "deb")  response: 593 and ot (extension: "gz" or extension: "deb")  response: 593 and ot (extension: "gz" or extension: "deb")  response: 593 and ot (extension: "gz" or extension: "deb")  response: 593 and ot (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 298 and not (extension: "gz" or extension: "deb")  response: 298 and not (extension: "gz" or extension: "deb")  response: 298 and not (extension: "gz" or extension: "deb")  response: 298 and not (extension: "gz" or extension: "deb")  response: 298 and not (extension: "gz" or extension: "deb")  response: 298 and not (extension: "gz" or extension: "deb")  response: 298 and not (extension: "gz" or extension: "deb")  response: 298 and not (extension: "gz" or extension: "deb")  response: 398 and not (extension: "gz" or extension: "deb")  response: 408 until debetween 208 und 2020 (inclusive)  gtill deservable field response equals 503 and extension is either "gz" or "deb"  date (after). All events aft	chrome firefox safari	free text: Matches "chrome" or "firefox" or "safari" in all fields (default)
browser : (chrome or firefox or safari)  or. Matches at least one of "chrome", "firefox" or "safari" in the field browser  tags: ("security" and "error")  and: Field tags contain both security and also either "waming" or "error"  agent : "and: Field tags matches "security" and also either "waming" or "error"  agent : "MSIE 6.0"  machine.os* : win*  response : 503 and agent : "MSIE 6.0"  response : 404 and not (browser : chrome)  response : 503 and extension : "gz" or extension: "deb"  response : 503 and (extension : "gz" or extension: "deb")  response : 503 and not (extension : "gz" or extension: "deb")  response : 503 and not (extension : "gz" or extension: "deb")  grouping (ralues): Field tesponse equals 503 and field extension is relife to seponse equals 503 and field extension is "gz", or field extension is "deb" (and precedes or)  response : 503 and not (extension : "gz" or extension: "deb")  response : 503 and not (extension : "gz" or extension: "deb")  grouping: Field response equals 503 and field extension is neither "gz" or "deb"  grouping: Field response equals 503 and field extension is neither "gz" or "deb"  grouping: Field response equals 503 and field extension is neither "gz" or "deb"  grouping: Field response equals 503 and field extension is neither "gz" or "deb"  grouping: Field response equals 503 and field extension is neither "gz" or "deb"  grouping: Field response equals 503 and extension is neither "gz" or "deb"  grouping: Field response equals 503 and extension is neither "gz" or "deb"  grouping: Field response equals 503 and extension is neither "gz" or "deb"  grouping: Field response equals 503 and extension is neither "gz" or "deb"  grouping: Field response equals 503 and extension is neither "gz" or "deb"  grouping: Field response equals 503 and extension is neither "gz" or "deb"  grouping: Field response equals 503 and extension is neither "gz" or "deb"  grouping: Field response equals 503 and extension is neither "gz" or "deb"  gt in the field septons in the field browser is not ch	"win xp"	phrase: Matches the exact phrase "win xp" as it appears (all fields)
tags: ("security" and "error")  and: Field tags contain both security and error as list elements  tags: security and (warning or error)  agent : "ASIE 6.0"  machine.os* : win*  response : 503 and agent : "MSIE 6.0"  mot Field tags matches exact phrase "MSIE 6.0"  mot Field tags matches exact phrase "MSIE 6.0"  mot Field seginning with machine.os matches values beginning with win  response : 503 and agent : "MSIE 6.0"  mot Field response equals 503 and field agent contains the phrase "MSIE 6.0"  response : 503 and extension : "gz" or extension: "deb"  response : 503 and extension : "gz" or extension: "deb"  response : 503 and not (extension : "gz" or extension: "deb")  response : 503 and not (extension : "gz" or extension: "deb")  grouping : Field response equals 503 and extension is either "gz" or "deb"  grouping with negation: Field response equals 503 and field extension is "gz", or field extension is "deb" (and precedes or)  response : 503 and not (extension : "gz" or extension: "deb")  grouping : Field response equals 503 and extension is either "gz" or "deb"  grouping with negation: Field response equals 503 and field extension is regiment is either "gz" or "deb"  grouping : Field response equals 503 and extension is either "gz" or "deb"  grouping : Field response equals 503 and extension is either "gz" or "deb"  grouping : Field response equals 503 and extension is either "gz" or "deb"  grouping : Field response equals 503 and extension is either "gz" or "deb"  grouping : Field response equals 503 and extension is either "gz" or "deb"  grouping : Field response equals 503 and extension is either "gz" or "deb"  grouping : Field response equals 503 and extension is either "gz" or "deb"  grouping : Field response equals 503 and extension is either "gz" or "deb"  grouping : Field response equals 503 and extension is either "gz" or "deb"  grouping : Field response equals 503 and extension is either "gz" or "deb"  grouping : Field response equals 503 and extension is either "gz" or deb"  grouping : Field respon	os : "win xp"	phrase (field-specific): Matches the exact phrase "win xp" as it appears in the field os
agent: "MSIE 6.0"  agent: "MSIE 6.0"  machine.os*: win*  response: 593 and agent: "MSIE 6.0"  response: 593 and extension: "gz" or extension: "deb"  response: 593 and (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  grouping with negation. Field response equals 503 and extension is reported attension is repo	browser : (chrome or firefox or safari)	or: Matches at least one of "chrome", "firefox" or "safari" in the field browser
agent: "MSIE 6.0"  machine.os*: win*  machine.os*: win*  mothine.os*: win*  mothine.os* matches values beginning with win  and (multiple fields): Field response equals 503 and field agent contains the phrase "MSIE 6.0"  mothine.os*: win*  mothine.os*: win*  mothine.os*: win*  mothine.os* matches values beginning with win  and (multiple fields): Field response equals 503 and field extension is repured between on the order of the order o	tags: ("security" and "error")	and: Field tags contain both security and error as list elements
agent: "MSIE 6.0"  machine.os*: win*  wildcard: Fields beginning with machine.os matches values beginning with win  response: 503 and agent: "MSIE 6.0"  response: 404 and not (browser: chrome)  response: 503 and extension: "gz" or extension: "deb"  response: 503 and extension: "gz" or extension: "deb"  response: 503 and (extension: "gz" or extension: "deb")  response: 503 and ot (extension: "gz" or extension: "deb")  response: 503 and not (extension: "gz" or extension: "deb")  response: 503 and not (extension: "gz" or extension: "deb")  grouping: Field response equals 503 and field extension is either "gz" or "deb"  response: 503 and not (extension: "gz" or extension: "deb")  grouping with negation: Field response equals 503 but field extension is neither "gz" or "deb"  date (after): All events after 2 Mar 2020  date (between): All events between 2 Mar 2020 and 5 Mar 2020 (inclusive)  bytes > 1000  ip: 192.168.0.0/16  IPV4 CIDR: Field ip is between 192.168.0.1 and 192.168.0.254  ** throws error as: is not needed in KQL  ** throws error as: is not needed in KQL	tags: security and (warning or error)	grouping (values): Field tags matches "security" and also either "warning" or "error"
machine.os*: win*  wildcard: Fields beginning with machine.os matches values beginning with win  response: 503 and agent: "MSIE 6.0"  not Field response equals 503 and field agent contains the phrase "MSIE 6.0"  response: 404 and not (browser: chrome)  response: 503 and extension: "gz" or extension: "deb"  response: 503 and extension: "gz" or extension: "deb")  response: 503 and (extension: "gz" or extension: "deb")  response: 503 and not (extension: "gz" or extension: "deb")  response: 503 and not (extension: "gz" or extension: "deb")  grouping with negation: Field response equals 503 and field extension is "gz" or "deb"  grouping with negation: Field response equals 503 and extension is either "gz" or "deb"  grouping with negation: Field response equals 503 and extension is either "gz" or "deb"  date (after): All events after 2 Mar 2020  gtimestamp > "2020-03-02" and @timestamp <= "2020-03-05" date (between): All events between 2 Mar 2020 and 5 Mar 2020 (inclusive)  bytes > 1000  ip: 192.168.0.0/16  IPV4 CIDR: Field ip is between 192.168.0.1 and 192.168.0.254  response: 200 agent: chrome  X throws error as: is not needed in KQL.  X throws error as: is not needed in KQL.	agent :*	exists: Field agent exists in any form
response: 593 and agent: "MSIE 6.0"  response: 494 and not (browser: chrome)  response: 593 and extension: "gz" or extension: "deb"  response: 593 and (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and not (extension: "gz" or extension: "deb")  response: 593 and retrieves: 593 and field extension is rigter sporse equals 503 and field extension is rigter sporse or deb"  response: 593 and field extension is "gz", or field extension is "gz", or field response equals 503 and field extension is rigter sporse or deb"  response: 593 and field extension is "gz", or field extension is rigter sporse equals 503 and extension is either "gz" or "deb"  date (after): All events after 2 Mar 2020 and 5 Mar 2020 (inclusive)  presponse: 593 and not (extension: after sporse equals	agent : "MSIE 6.0"	phrase: Field agent matches exact phrase "MSIE 6.0"
response : 404 and not (browser : chrome)  response : 503 and extension : "gz" or extension: "deb"  response : 503 and (extension : "gz" or extension: "deb")  response : 503 and (extension : "gz" or extension: "deb")  response : 503 and not (extension : "gz" or extension: "deb")  grouping: Field response equals 503 and extension is either "gz" or "deb"  response : 503 and not (extension : "gz" or extension: "deb")  grouping: Field response equals 503 and extension is either "gz" or "deb"  grouping with negation: Field response equals 503 but field extension is neither "gz" or "deb"  date (after): All events after 2 Mar 2020  date (after): All events after 2 Mar 2020 and 5 Mar 2020 (inclusive)  greater: Field bytes has value greater than 1000  ip: 192.168.0.0/16  IPV4 CIDR: Field ip is between 192.168.0.1 and 192.168.0.254  x throws error as and / or is required between criteria in KQL. However will work in legacy Lucene syntax  bytes :>	machine.os* : win*	wildcard: Fields beginning with machine.os matches values beginning with win
response : 503 and extension : "gz" or extension: "deb"  response : 503 and (extension : "gz" or extension: "deb")  response : 503 and (extension : "gz" or extension: "deb")  response : 503 and not (extension : "gz" or extension: "deb")  grouping: Field response equals 503 and extension is either "gz" or "deb"  response : 503 and not (extension : "gz" or extension: "deb")  grouping with negation: Field response equals 503 but field extension is neither "gz" or "deb"  date (after): All events after 2 Mar 2020  @timestamp >= "2020-03-02" and @timestamp <= "2020-03-05" date (between): All events between 2 Mar 2020 and 5 Mar 2020 (inclusive)  bytes > 1000  greater: Field bytes has value greater than 1000  ip: 192.168.0.0/16  IPV4 CIDR: Field ip is between 192.168.0.1 and 192.168.0.254  response : 200 agent: chrome  X throws error as and / or is required between criteria in KQL. However will work in legacy Lucene syntax  X throws error as: is not needed in KQL	response : 503 and agent : "MSIE 6.0"	and (multiple fields): Field response equals 503 and field agent contains the phrase "MSIE 6.0"
response : 503 and (extension : "gz" or extension: "deb")  response : 503 and not (extension : "gz" or extension: "deb")  grouping: Field response equals 503 and extension is either "gz" or "deb"  grouping with negation: Field response equals 503 but field extension is neither "gz" or "deb"  date (after): All events after 2 Mar 2020  @timestamp >= "2020-03-02" and @timestamp <= "2020-03-05" date (between): All events between 2 Mar 2020 and 5 Mar 2020 (inclusive)  bytes > 1000  ip: 192.168.0.0/16  IPV4 CIDR: Field ip is between 192.168.0.1 and 192.168.0.254  x throws error as and / or is required between criteria in KQL. However will work in legacy Lucene syntax  bytes :>	response : 404 and not (browser : chrome)	not: Field response equals 404 but field browser is not chrome
response : 503 and not (extension : "gz" or extension: "deb")  @timestamp > "2020-03-02"  @timestamp >= "2020-03-02" and @timestamp <= "2020-03-05"  bytes > 1000  ip: 192.168.0.0/16  response : 200 agent: chrome  grouping with negation: Field response equals 503 but field extension is neither "gz" or "deb"  date (after): All events after 2 Mar 2020  date (between): All events between 2 Mar 2020 and 5 Mar 2020 (inclusive)  greater: Field bytes has value greater than 1000  IPV4 CIDR: Field ip is between 192.168.0.254  X throws error as and / or is required between criteria in KQL. However will work in legacy Lucene syntax  bytes :>	response : 503 and extension : "gz" or extension: "deb"	precedence: Either field response equals 503 and field extension is "gz", or field extension is "deb" (and precedes or)
@timestamp > "2020-03-02"date (after): All events after 2 Mar 2020@timestamp >= "2020-03-02" and @timestamp <= "2020-03-05"	response : 503 and (extension : "gz" or extension: "deb")	grouping: Field response equals 503 and extension is either "gz" or "deb"
@timestamp >= "2020-03-02" and @timestamp <= "2020-03-05"date (between): All events between 2 Mar 2020 and 5 Mar 2020 (inclusive)bytes > 1000greater: Field bytes has value greater than 1000ip: 192.168.0.0/16IPV4 CIDR: Field ip is between 192.168.0.1 and 192.168.0.254response : 200 agent: chromeX throws error as and / or is required between criteria in KQL. However will work in legacy Lucene syntaxbytes :>X throws error as: is not needed in KQL	response : 503 and not (extension : "gz" or extension: "deb")	grouping with negation: Field response equals 503 but field extension is neither "gz" or "deb"
bytes > 1000  ip: 192.168.0.0/16  IPV4 CIDR: Field ip is between 192.168.0.1 and 192.168.0.254  response: 200 agent: chrome  X throws error as and / or is required between criteria in KQL. However will work in legacy Lucene syntax  bytes:>	@timestamp > "2020-03-02"	date (after): All events after 2 Mar 2020
ip: 192.168.0.0/16  IPV4 CIDR: Field ip is between 192.168.0.1 and 192.168.0.254  response: 200 agent: chrome  X throws error as and / or is required between criteria in KQL. However will work in legacy Lucene syntax  bytes:>	@timestamp >= "2020-03-02" and @timestamp <= "2020-03-05"	date (between): All events between 2 Mar 2020 and 5 Mar 2020 (inclusive)
response: 200 agent: chrome  * throws error as and / or is required between criteria in KQL. However will work in legacy Lucene syntax  bytes:>	bytes > 1000	greater: Field bytes has value greater than 1000
bytes :> X throws error as: is not needed in KQL	ip: 192.168.0.0/16	<b>IPV4 CIDR:</b> Field ip is between 192.168.0.1 and 192.168.0.254
	response : 200 agent: chrome	x throws error as and / or is required between criteria in KQL. However will work in legacy Lucene syntax
bytes: [1000 TO 5000]	bytes :>	throws error as: is not needed in KQL
	bytes:[1000 TO 5000]	* throws error, expand as bytes >= 1000 and bytes <= 5000 in KQL