### rex

Extracts the fields from the specified field using a regular expression.

#### Syntax

rex field=FIELD "REGEX"

Required Parameter

**field=FIELD**

Target field from which to extract the string using a regular expression.

**"REGEX"**

Extended regular expression to give the field name. If you specify the group in the form of (?<field>) in the regular expression, the command extracts the string matched to the group to the **field** field.

#### Usage

Look up a file path starting with GET /game/flash/ or POST /game/flash from the **line** field and then return the matched ones to the **filename** field.

rex field=line "(GET|POST) /game/flash/(?<filename>([^ ]\*))"

Extract the string in the timestamp pattern from the **line** field and assign it to the **timestamp** field.

rex field=line "(?<timestamp>\d+-\d+-\d+ \d+:\d+:\d+)"

Extract the strings from the **line** field and assign them to the **url** and **querystring** fields.

rex field=line "(GET|POST) (?<url>[^ ]\*) (?<querystring>[^ ]\*) "