### rex

지정된 필드에서 정규표현식을 이용하여 필드를 추출합니다.

#### 문법

rex field={FIELD|line} "REGEX"

필수 매개변수

**field=FIELD**

정규 표현식을 이용하여 문자열을 추출할 대상 필드.

**"REGEX"**

필드 이름을 부여할 수 있도록 확장된 정규표현식. 정규표현식 그룹을 만들 때 (?<field>.\*) 형식으로 지정하면 그룹에 매칭된 문자열을 **field** 필드에 출력합니다.

#### 사용 예

**line** 필드에서 GET /game/flash/ 또는 POST /game/flash/으로 시작하는 파일 경로를 검색해 매칭된 문자열을 **filename** 필드에 출력

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

**line** 필드에서 타임스탬프 패턴의 문자열을 추출해 **timestamp** 필드에 출력

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

**line** 필드에서 문자열을 추출해 **url**과 **querystring** 필드에 출력

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