## 쿼리 연습

로그프레소에서 수집한 데이터는 DB 테이블에 저장되어 있습니다. 테이블에 저장되어 있는 데이터를 추출하여 내용을 확인 및 분석하기 위해서는 제공되는 쿼리 문자열과 함수를 사용하여야 합니다. 쿼리 문자열과 함수의 사용법은 쿼리 설명서을 참조하세요.

쿼리 연습은 "쿼리" 메인 메뉴의 왼쪽에 있는 "쿼리" 메뉴를 선택하여 사용할 수 있습니다.

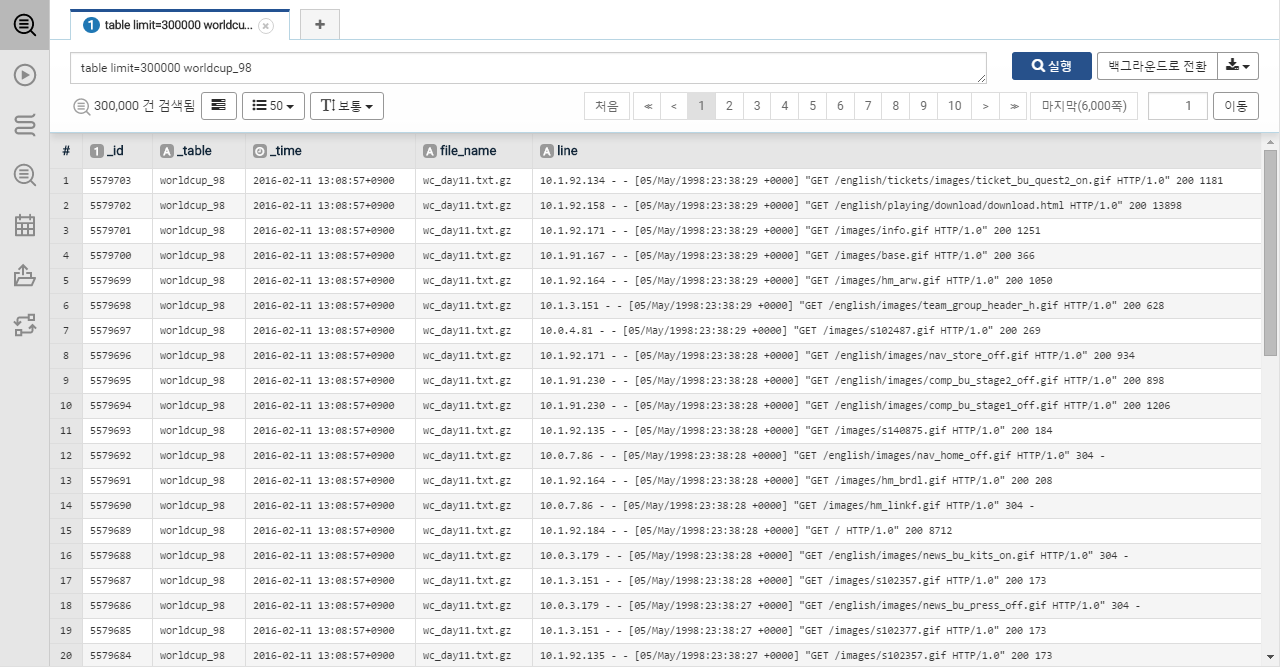
아래 예제는 worldcup\_98 테이블에 저장된 데이터를 추출하는 방법에 대한 예제입니다.

### 단계 1

테이블에 저장된 로그 추출 (원본 line 필드 대상 추출)

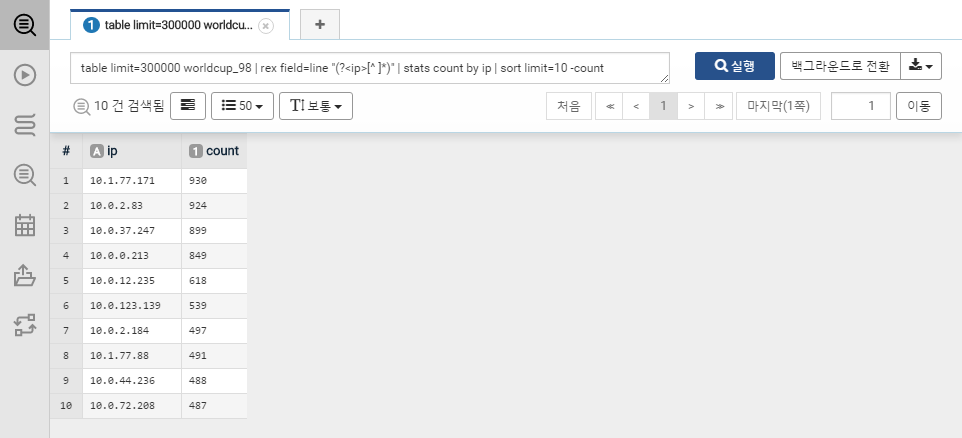
다음 쿼리문은 worldcup\_98 테이블에서 300000 건의 데이터만 추출하는 예시입니다.

table limit=300000 worldcup\_98



다음 쿼리문은 worldcup\_98 테이블에서 ip를 추출한 후 ip를 기준으로 건수를 정렬하여 10건을 추출하는 예시입니다.

table limit=300000 worldcup\_98 | rex field=line "(?<ip>[^ ]\*)" | stats count by ip | sort limit=10 -count



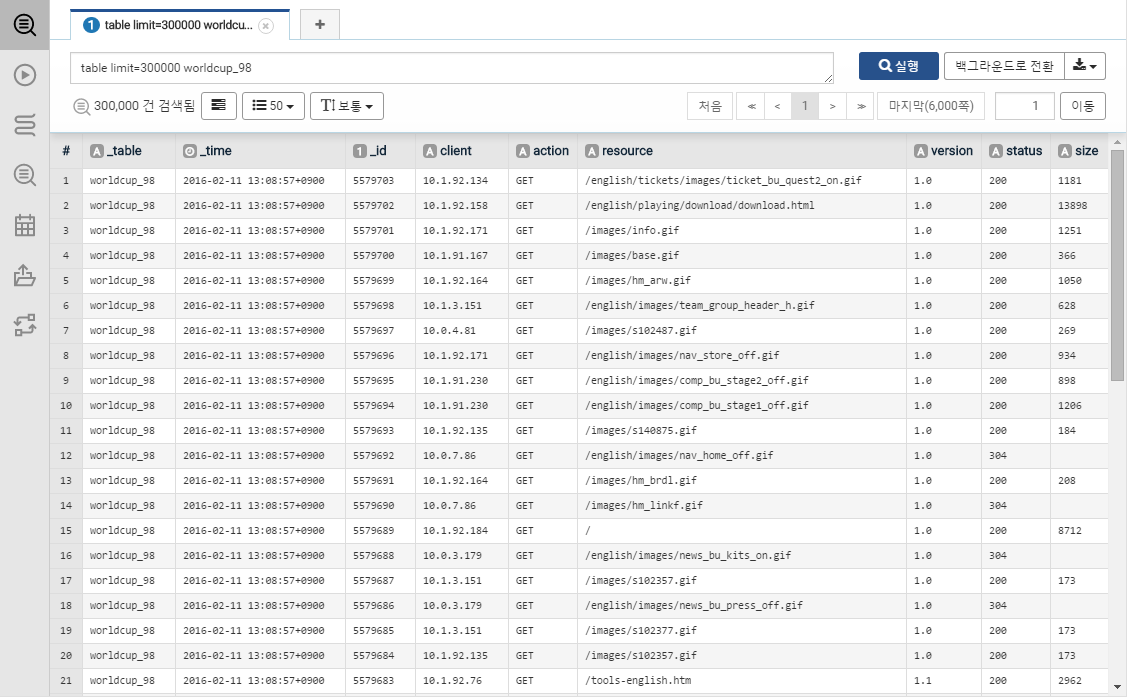
### 단계 2

테이블에 파서가 적용되어 있을 경우

테이블에 파서가 적용되어 있을 경우는 테이블의 내용이 쿼리 문자열로 추출될 때 적용한 파서의 포맷으로 변환되어 추출됩니다. 그래서 필드명이 원본 line이 아닌 파서의 적용을 받은 필드로 결과가 추출됩니다.

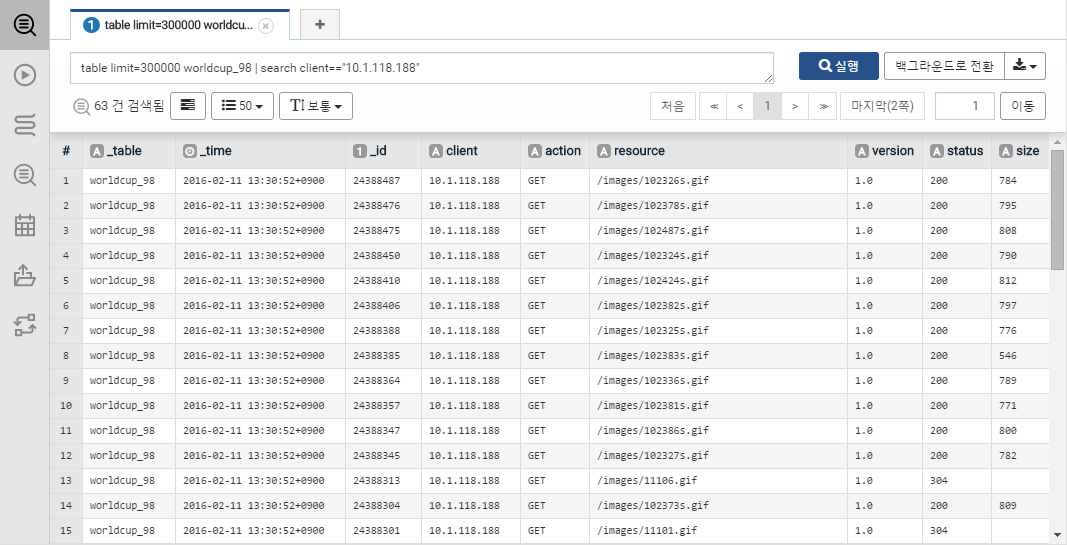
table limit=300000 worldcup\_98

파서에 표현한 형식으로 데이터가 필드로 구분되어 추출됩니다.



다음 쿼리문은 worldcup\_98 테이블에 있는 client 필드에서 특정한 IP 주소를 검색해 데이터를 보여주는 예시입니다.

table limit=300000 worldcup\_98 | search client=="10.1.118.188"



### 단계 3

테이블에 인덱스가 적용되어 있을 경우

테이블에 인덱스가 적용되어 있을 경우는 fulltext 명령어를 사용하여 테이블의 데이터를 추출합니다. 다음 쿼리문은 fulltext 명령을 이용해 인덱스를 검색하는 예시입니다.

fulltext "10.1.172.254" from worldcup\_98 | limit 10

