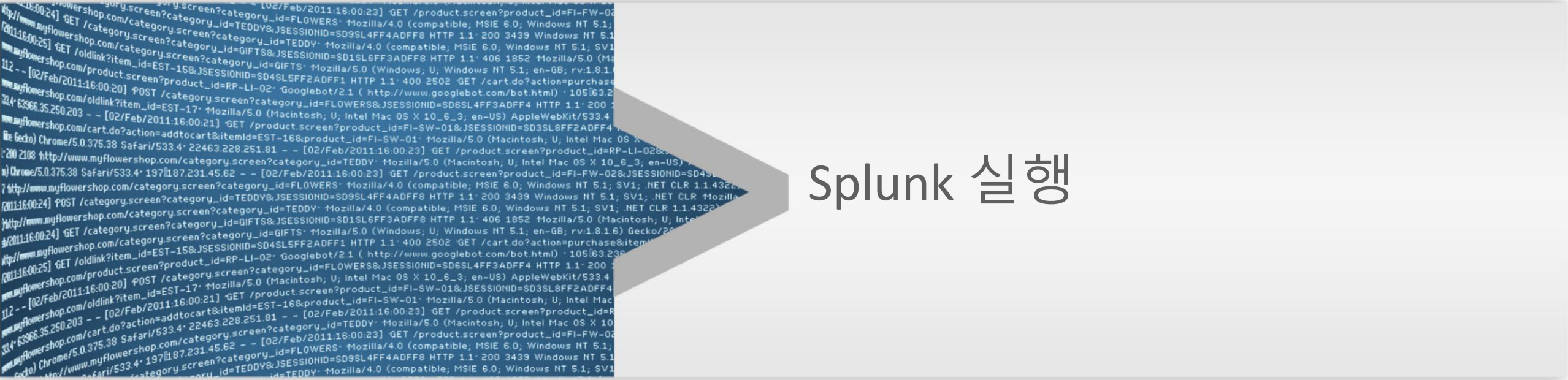
splunk> MOS



splunk>

Splunk 검색 개요

- 여러 이종의 데이터의 복합 검색 및 분석의 요구사항 충족

splunk>

Database

미들웨어 오류

서비스 시스템

외부 인터넷 데이터

문제 ID

세션정보

사용자 ID

ORDER,2012-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213.
Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException:
weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The
DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port:
ACMEDB-01:1521. Reason: Connection refused

프로세스

문제 ID

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type

서비스 정보

0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-13ae51a6d092, Trunk T451.16

05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

CUSTID 10098213

문제 ID

05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:
"http://dallascowboys.com/",location:{displayName:"Irving, TX",objectType:"place"},
objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought
this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if
you hate @ACME!!",objectType:"activity",postedTime:"2012-05-21T16:39:40.647-0600"}

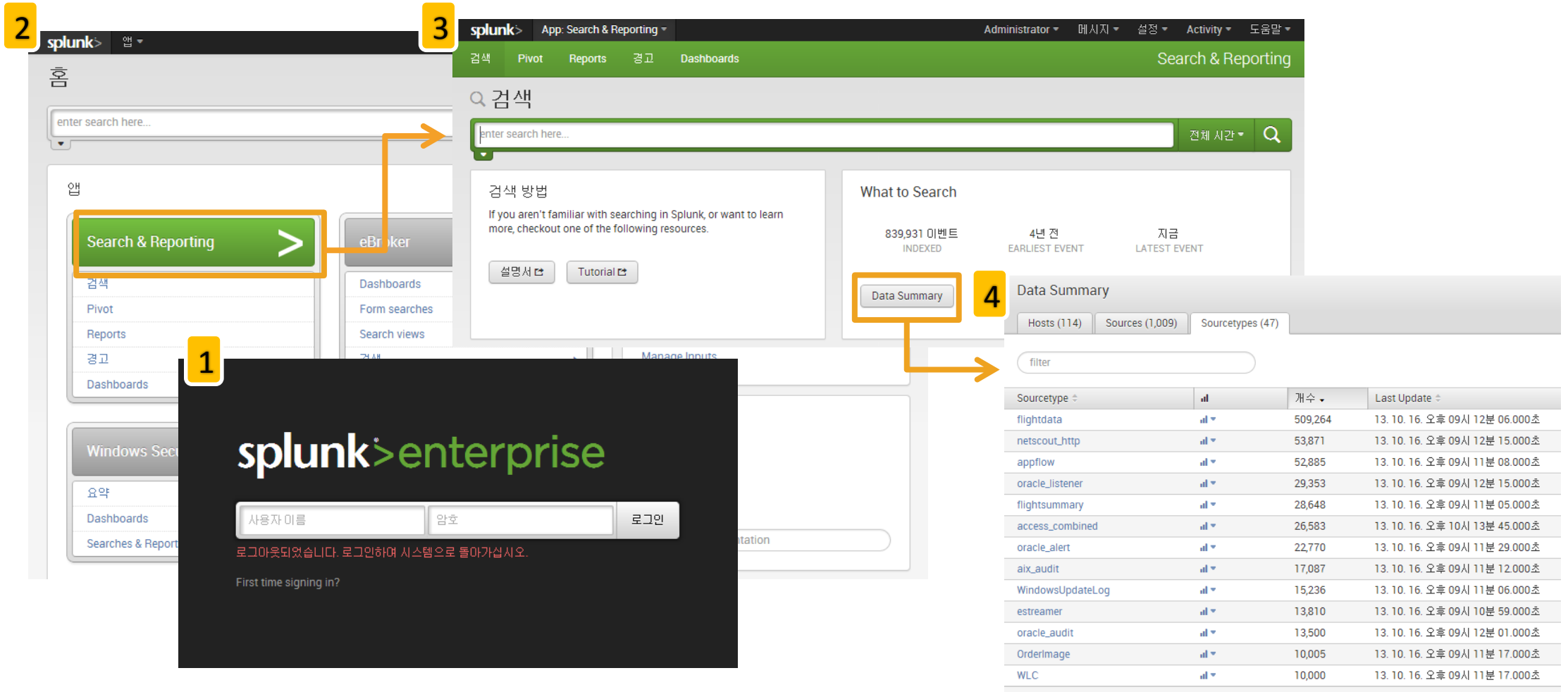
문제 외부 ID

유해 감염 정보

WHO IS 의 외부 DB

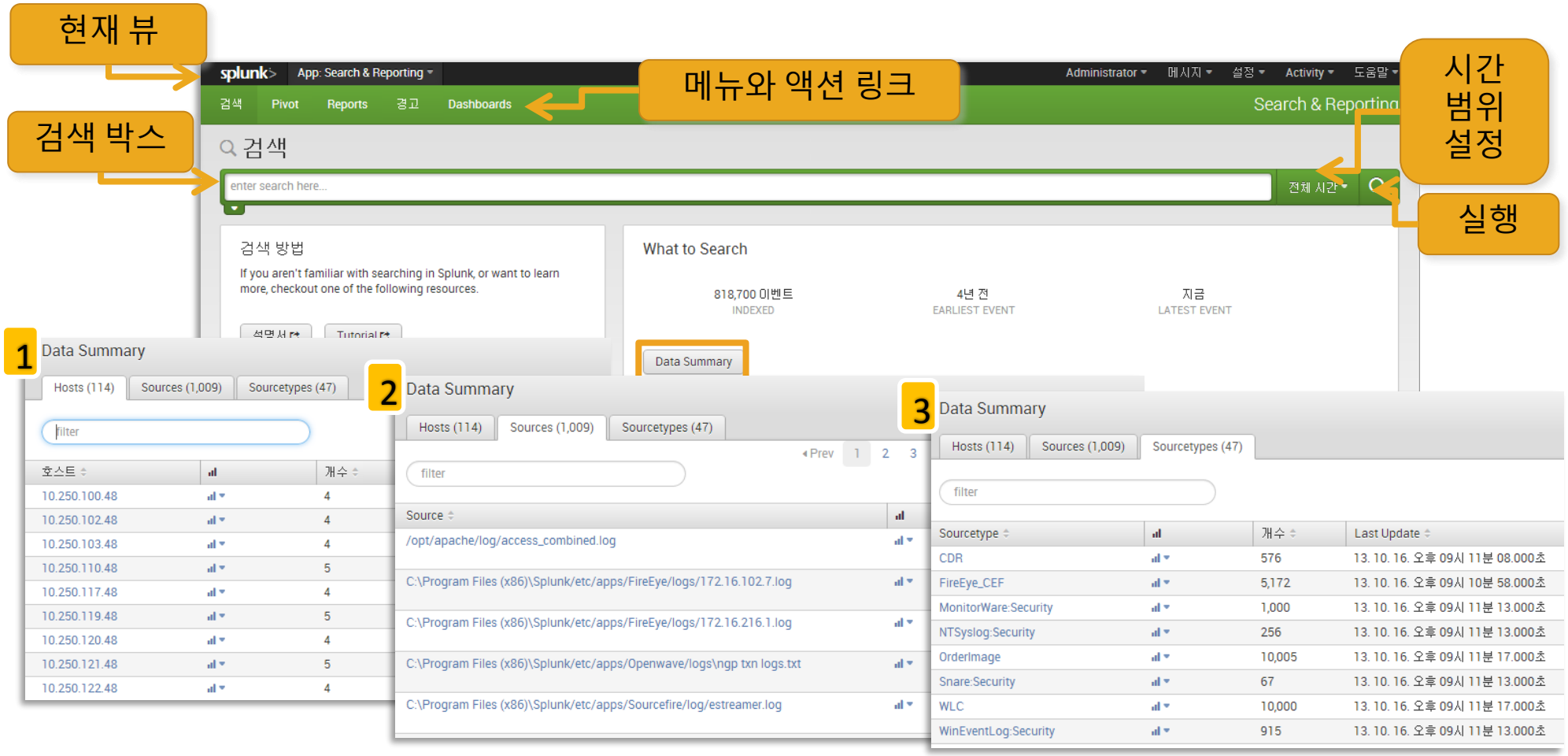
Search(검색) App 실행

- Splunk 검색 방법 및 현재 검색 할 수 있는 Data 확인 방법

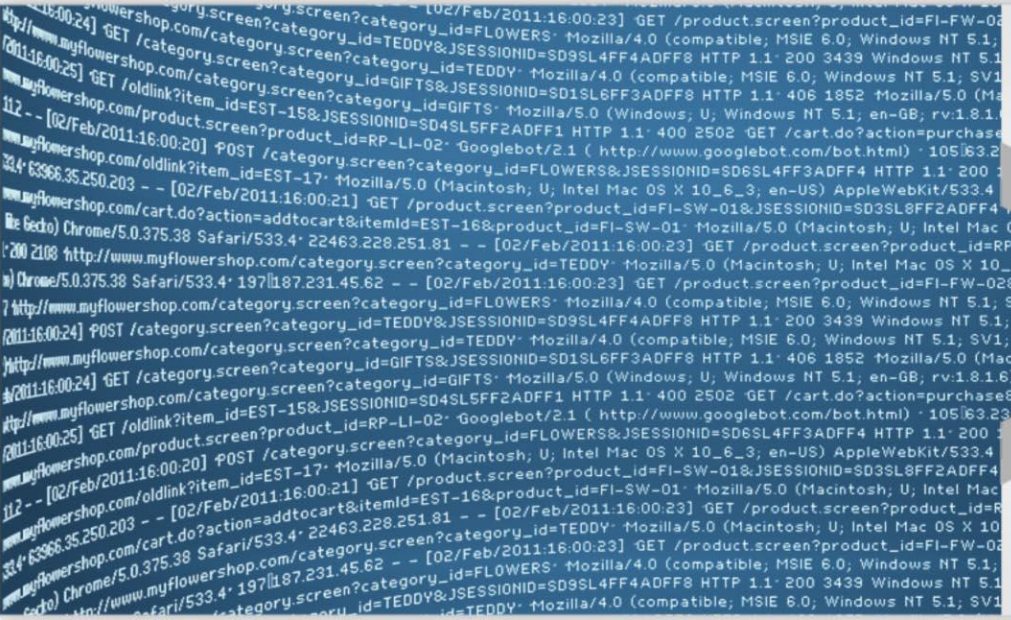


Search Summary 뷰 이해

- Splunk에서 가장 기본 적인 화면 기능 설명



splunk> MOS



검색 개요

splunk>

검색 기초

모든 것이 검색 가능 합니다

```
fail*
```

✓ * 와일드 카드 지원

```
fail* nfs
```

✓ 검색 패턴의 요건은 대소문자를 구분하지 않습니다.

✓ Booleans “AND”, “OR”, “NOT”

- Booleans의 표현은 대문자로 표시

```
error OR 404
```

- 검색 패턴의 요건의 중간에 적용
- 복잡한 검색 요건을 “( )” 그룹화 함

```
error OR failed OR server OR (sourcetype=access_* (404 OR 500 OR 503))
```

✓ 정확한 단어열은 “ “로 표현

```
“login failure”
```

“검색 엔진”, 그 이상의 기능

- ✓비교 operators 검색을 더 강력하게 합니다
- ✓수치 비교 operators (!= > < <= >=)

```
sourcetype=access_combined action!=view
```

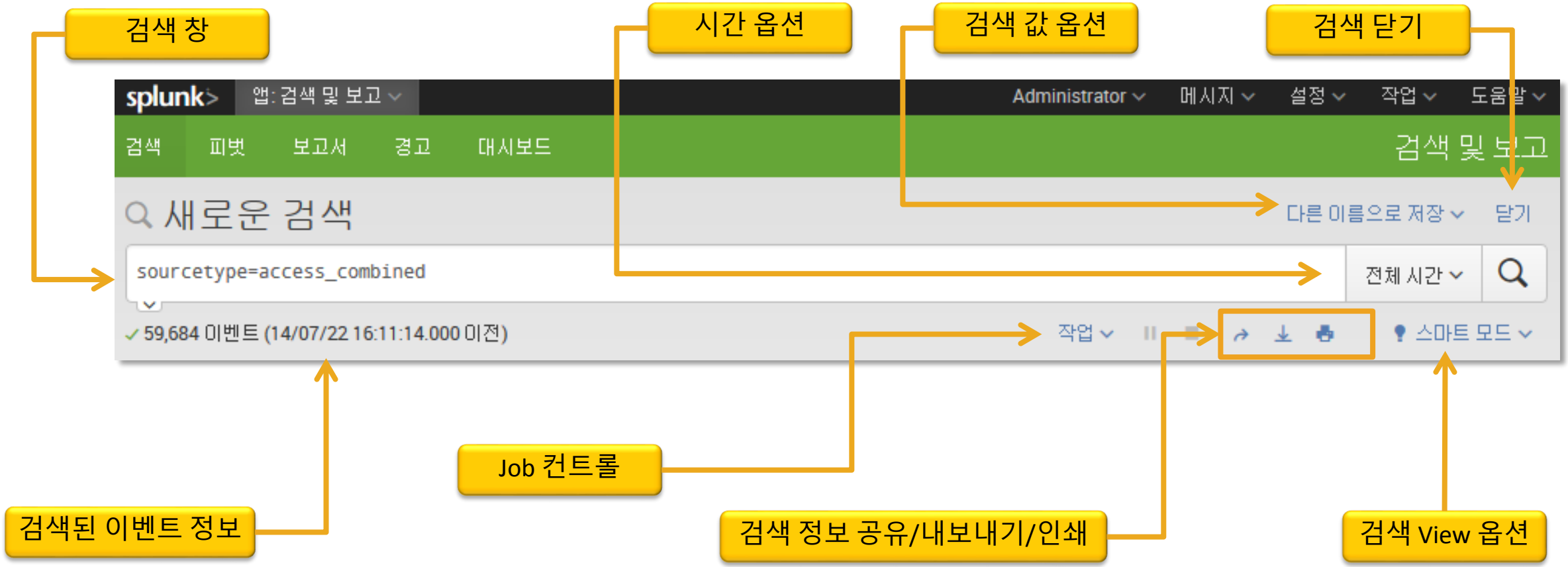
```
sourcetype=access_combined status>=300
```

```
sourcetype=access_combined req_time > “20/May/2014 07:25:19:104”
```

```
sourcetype=access_combined clientip=“125.17.*”
```

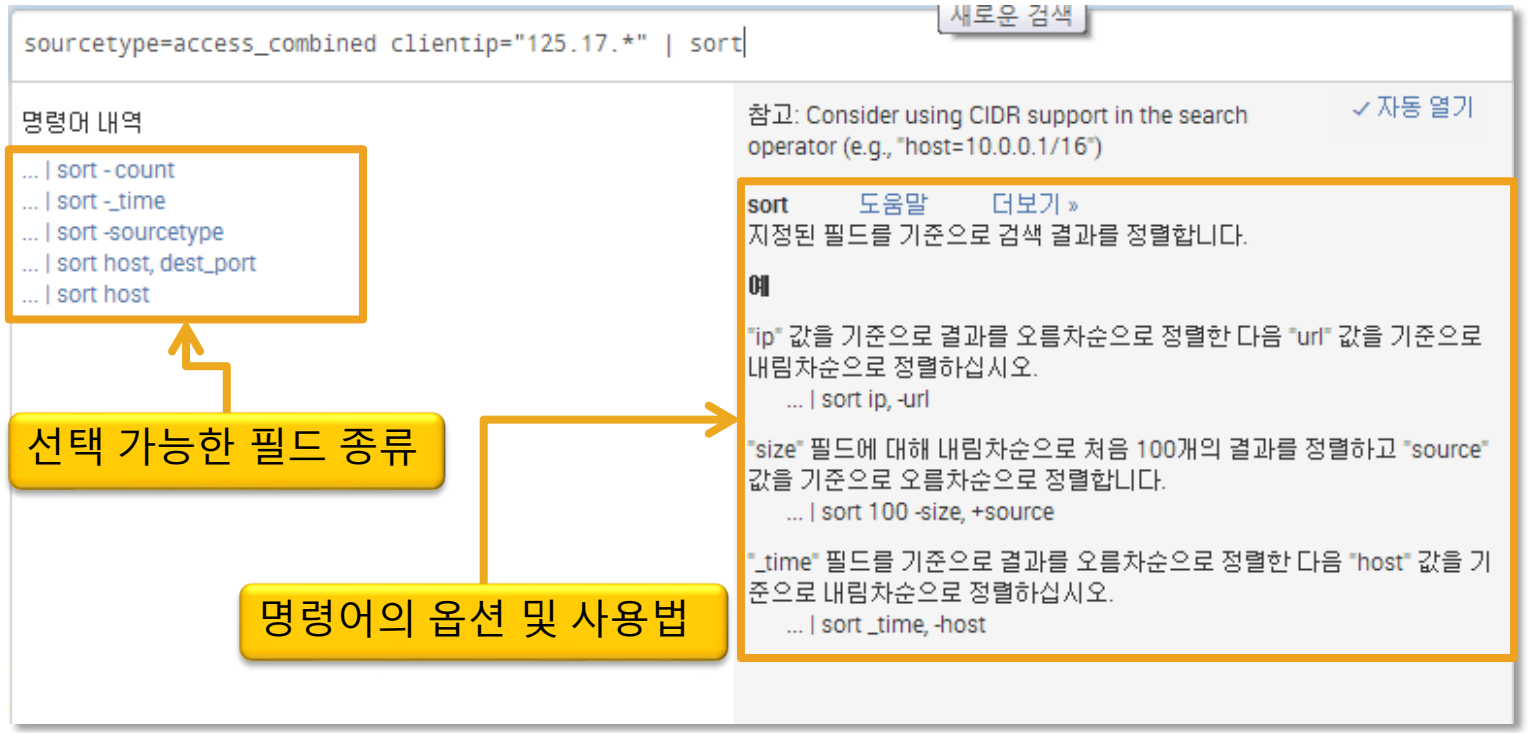
검색 View

- Splunk 기본 검색 및 분석 하는 기본 페이지



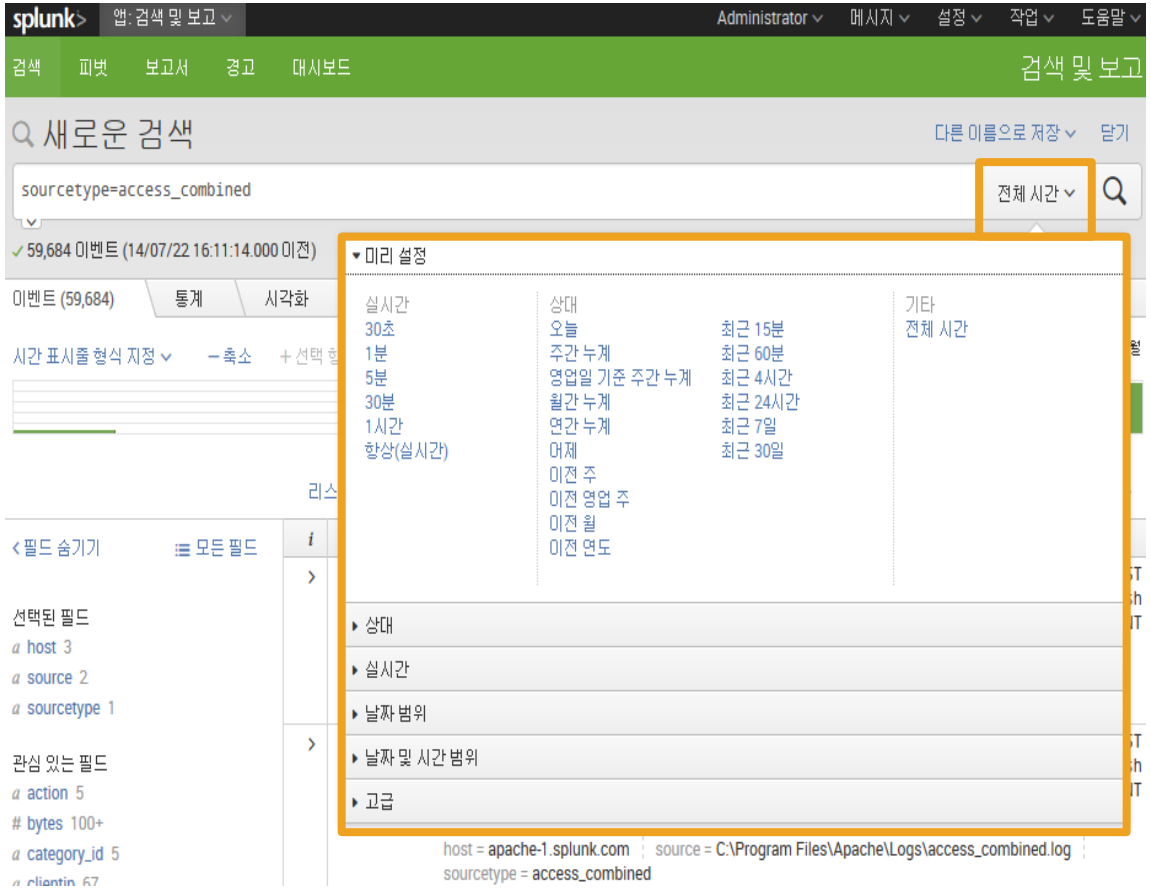
쉬운 Splunk 검색 언어 도우미

- ✓ 특정한 Splunk의 명령어를 검색 창에 입력하는 중 Splunk검색 도우미 기능은 해당 명령어의 빠를 사용법을 찾아 보여주고, 특정 필드의 input이 필요할 경우 선택 가능한 필드의 종류도 호출하여 줍니다.



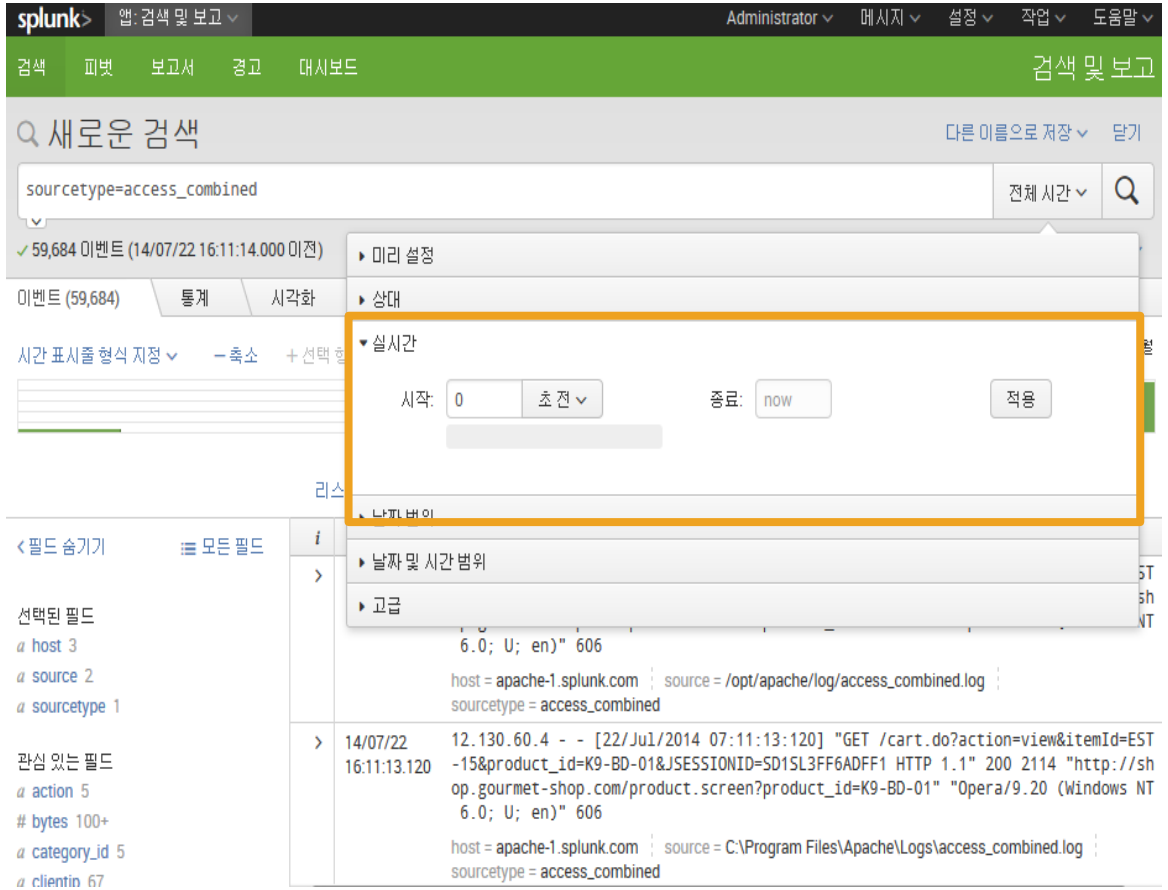
검색의 시간 범위 조정

- ✓기본적으로 Splunk 전체 시간 범위에서 검색됨
- ✓시간 범위를 선택하여 검색의 과거 범위를 설정하고, 또는 실시간 검색의 요건을 설정 합니다.

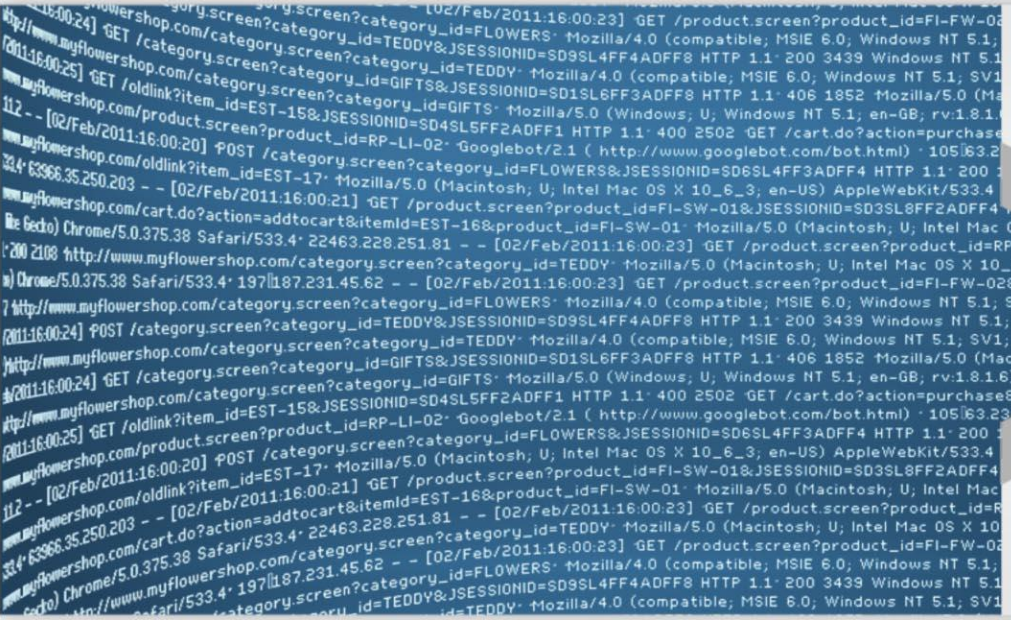


Real-time 검색

- ✓Real-time 검색은 실시간으로 데이터가 들어오면서 호출되어 보여지며 분석 됩니다.
- ✓Critical 한 문제에 대한 실시간 인지나 대응을 가능하게 합니다.



splunk> MOS

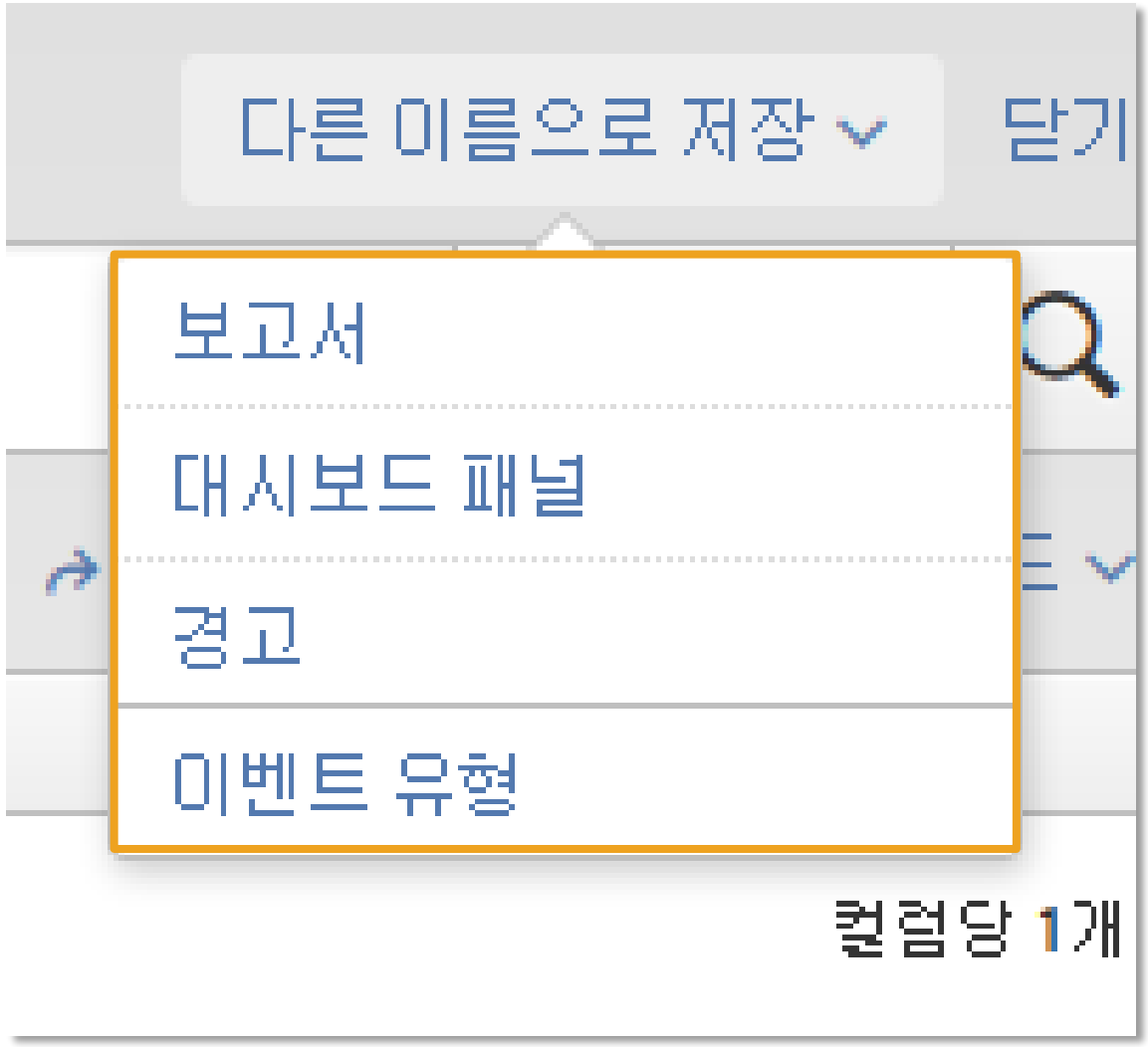


결과와의 Interaction

splunk>

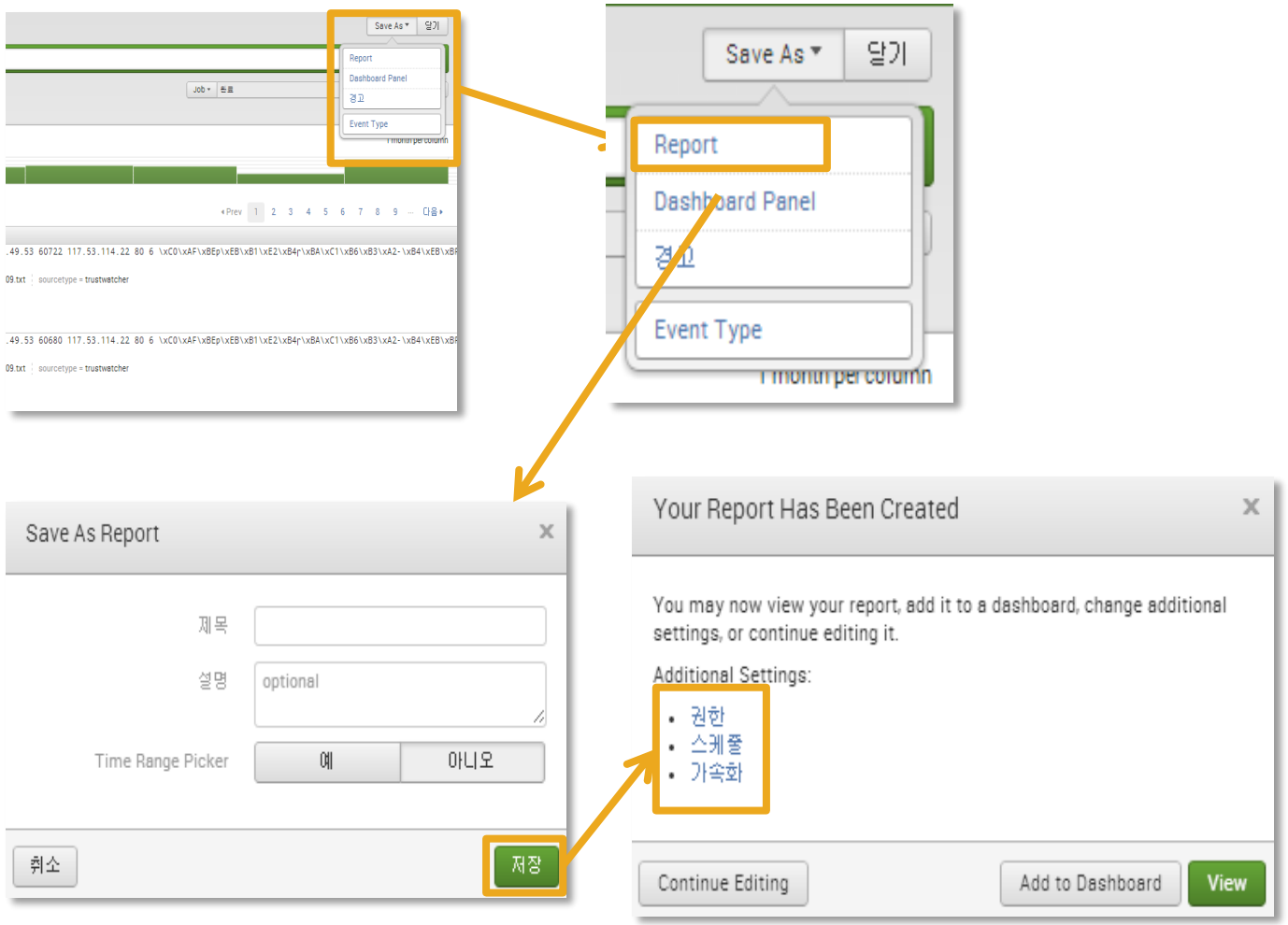
결과 저장 및 연계

- ✓“보고서” 기능을 통해 결과 값을 신속하게 차트화된 보고서를 만들 수 있습니다.
- ✓“대시보드 패널” 은 검색된 내용을 바로 dashboard로 만들 수 있습니다.
- ✓“경고” 설정을 합니다.
- ✓“이벤트 유형” 의 분류를 저장 합니다.



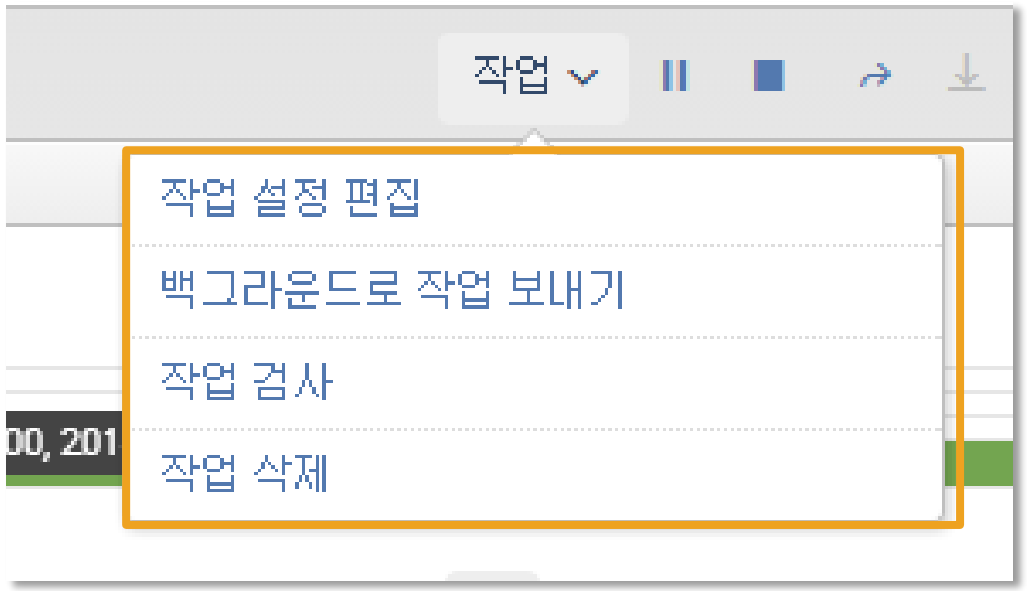
검색 저장

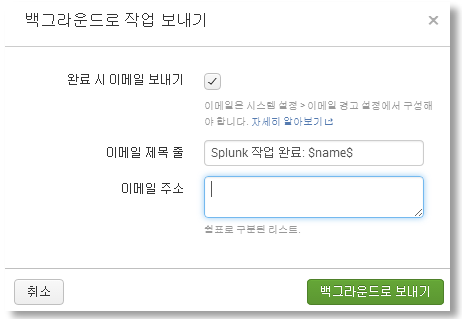
- ✓ “Save As” -> Report 아이콘을 클릭 합니다.
- ✓ 검색 명을 저장 합니다.
  - 검색 분석 요건과 시간을 저장 및 수정
  - 타 사용자와 동일한 검색을 공유 할 수 있음



Job 제어

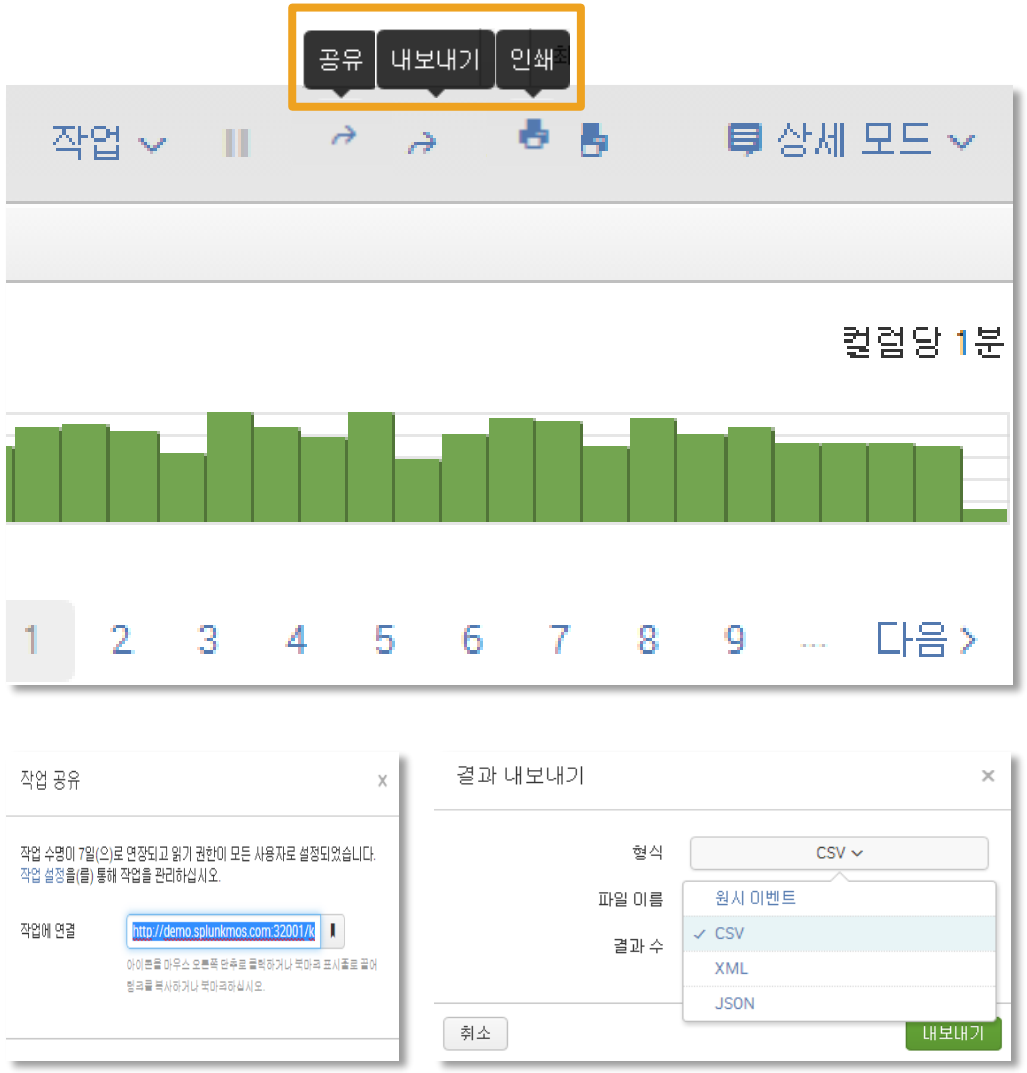
- ✓'작업 설정 편집'은 검색 작업 내용의 읽기권한, 주기를 설정할 수 있고 검색된 결과를 Link URL 을 통해 공유 할 수 있습니다.
- ✓'백그라운드로 작업 보내기' 는 현재 작업을 백그라운드로 보냅니다.
- ✓'작업검사'는 작업의 상세내역을 확인 할 수 있습니다.





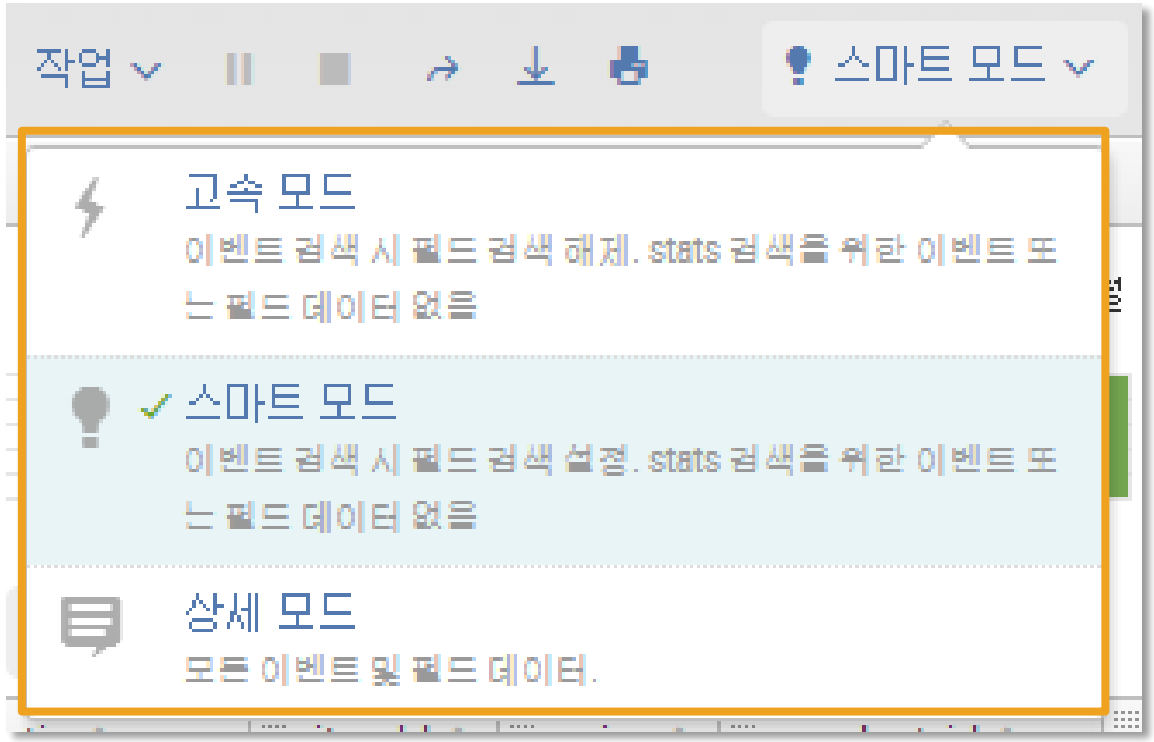
검색 정보 공유/내보내기/인쇄

- ✓공유기능을 통해 검색된 결과를 Link URL 을 통해 공유 할 수 있습니다.
- ✓내보내기를 통해 검색 결과를 파일 형태로 저장 할 수 있습니다.
- ✓검색 결과를 출력합니다.



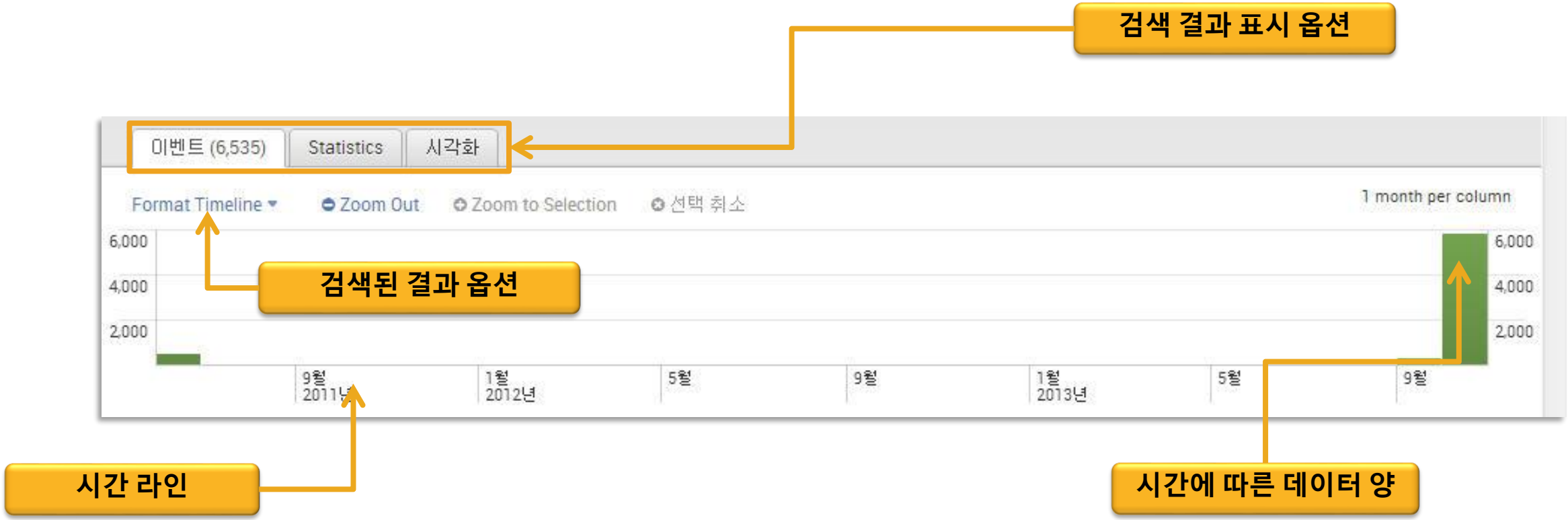
검색 View 옵션

- ✓고속 모드는 검색 속도에 최적화된 모드로 검색 결과를 빠르게 확인하는 목적으로 필드 추출 등을 하지 않습니다.
- ✓스마트 모드는 상황에 따라 필드 추출 및 분류를 제공 합니다.
- ✓상세 모드는 필드 추출 및 모든 시각적 검색 현황을 같이 출력 합니다.



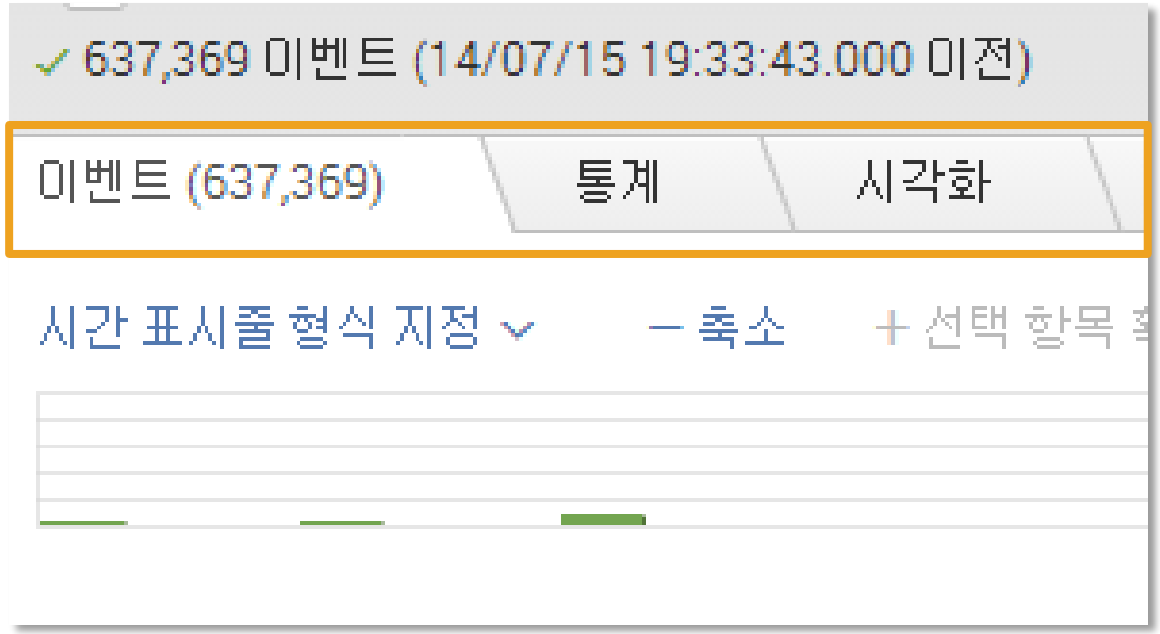
Timeline 네비게이션

✓타임라인 네비게이션을 통하여 쿼리 결과의 Volume, Velocity 를 인지하고 분석하고자 하는 결과의 범위로 시각적 네비게이션을 제공 합니다.



검색 결과 표시 옵션

- ✓'이벤트 View ' 는 쿼리 결과의 이벤트적인 요소의 결과 뷰를 제공 합니다.
- ✓'통계 View' 는 검색 결과를 내용을 Cell 형태의 테이블로 보여 줍니다.
- ✓'시각화 View' 는 검색된 결과를 비쥬얼한 chart형태로 데이터를 표현해 줍니다.

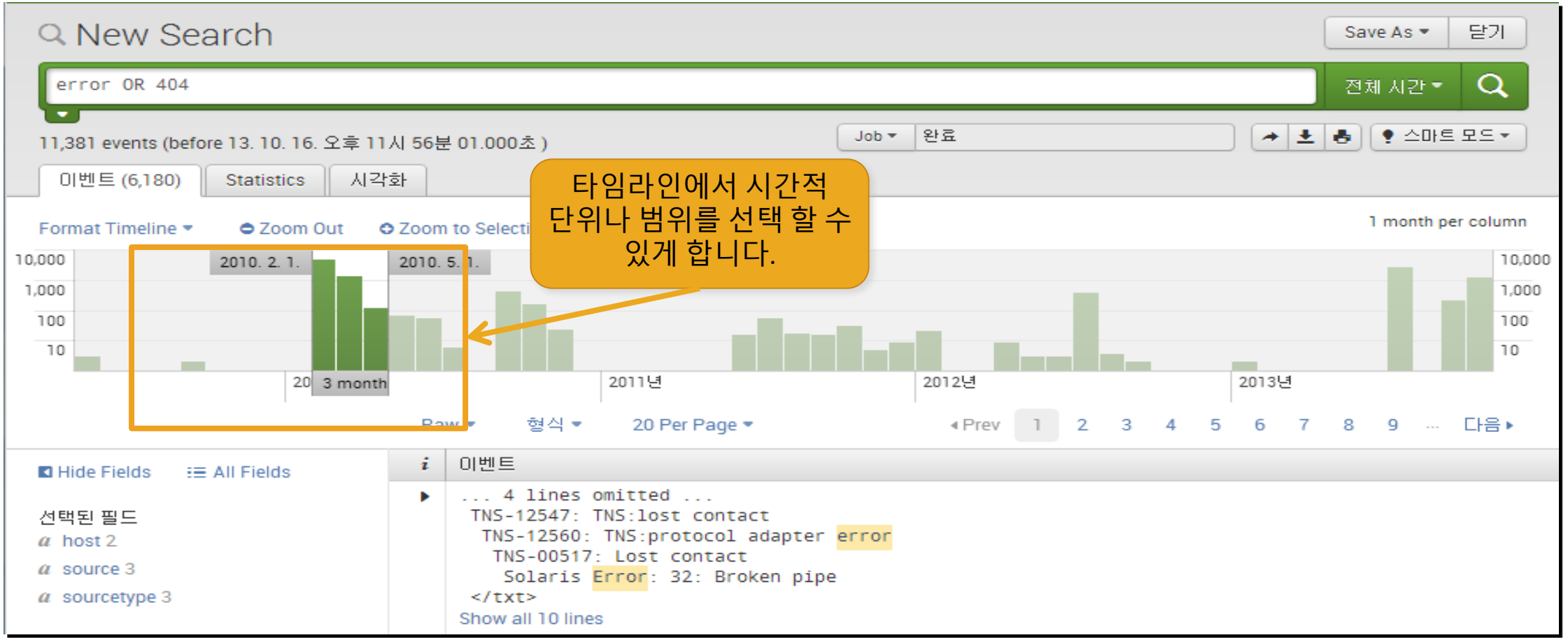


검색된 결과 옵션

- ✓ 검색된 데이터의 View를 '원시', '리스트', '테이블' 의 형태로 지원합니다.

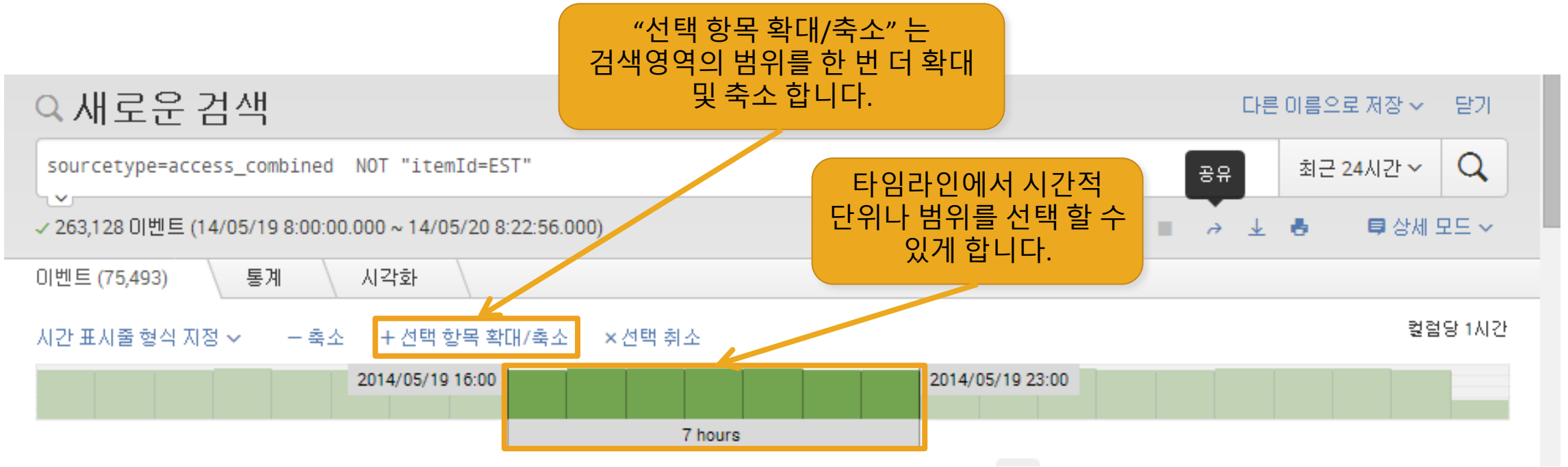
결과 탐색 – Timeline

✓검색된 결과의 범위를 선택하여 내용의 위치를 조정 합니다.



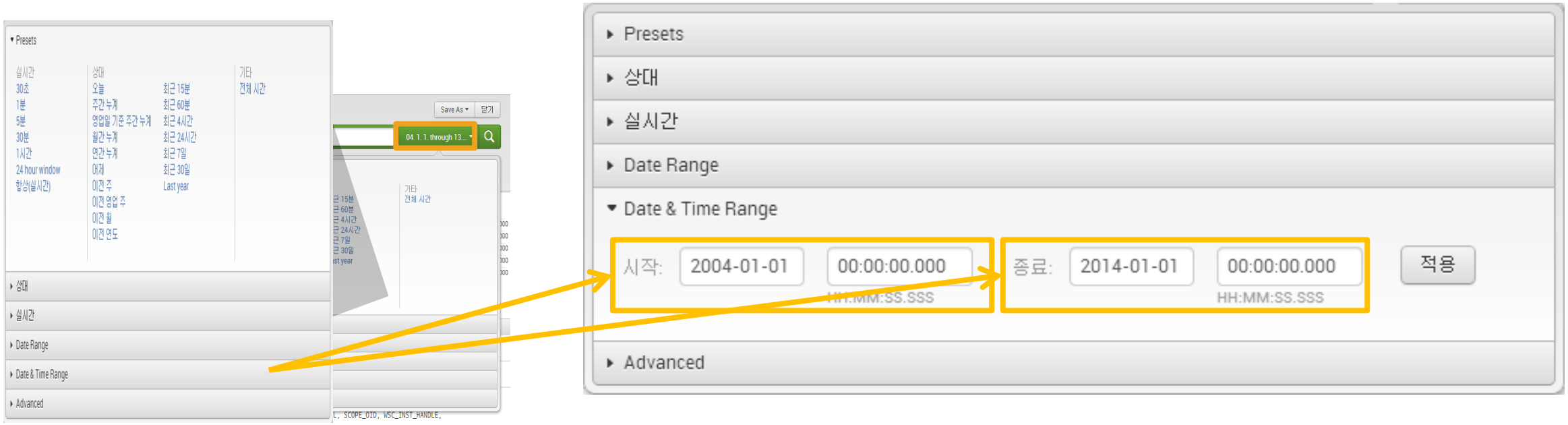
결과 탐색– Timeline (cont.)

✓Timeline 네비게이션 기능을 통하여 Interactive하게 데이터의 범위를 조정 합니다.



사용자 지정 시간 설정

✓사용자 지정 시간은 달력 툴에서 검색 시작과 끝을 정의하며 쿼리의 절대적 및 상대적 시간 범위를 정의 합니다.

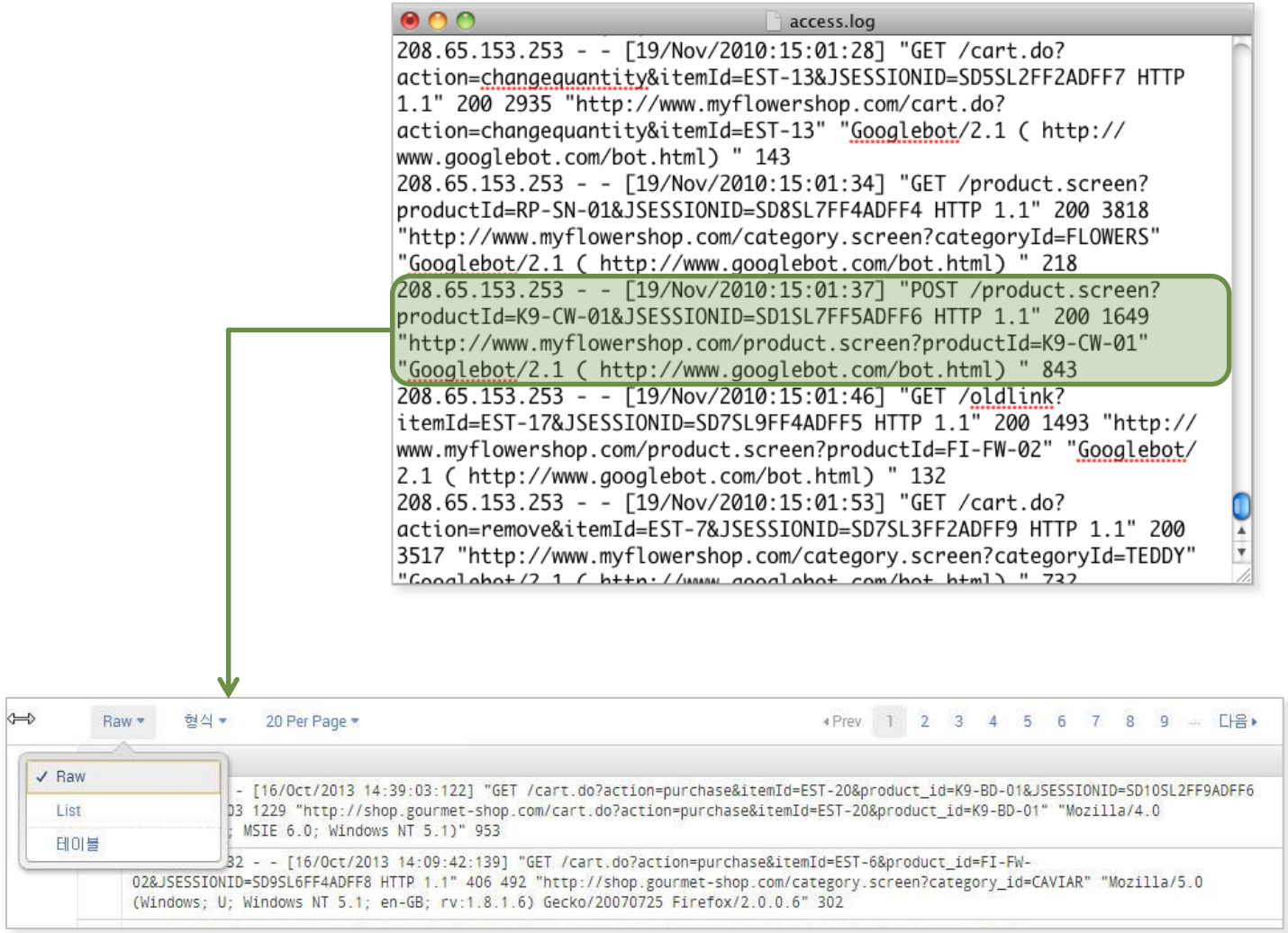


검색 결과

✓검색 결과 창에서는 검색 된 결과의 출력 방식을 설정 합니다.

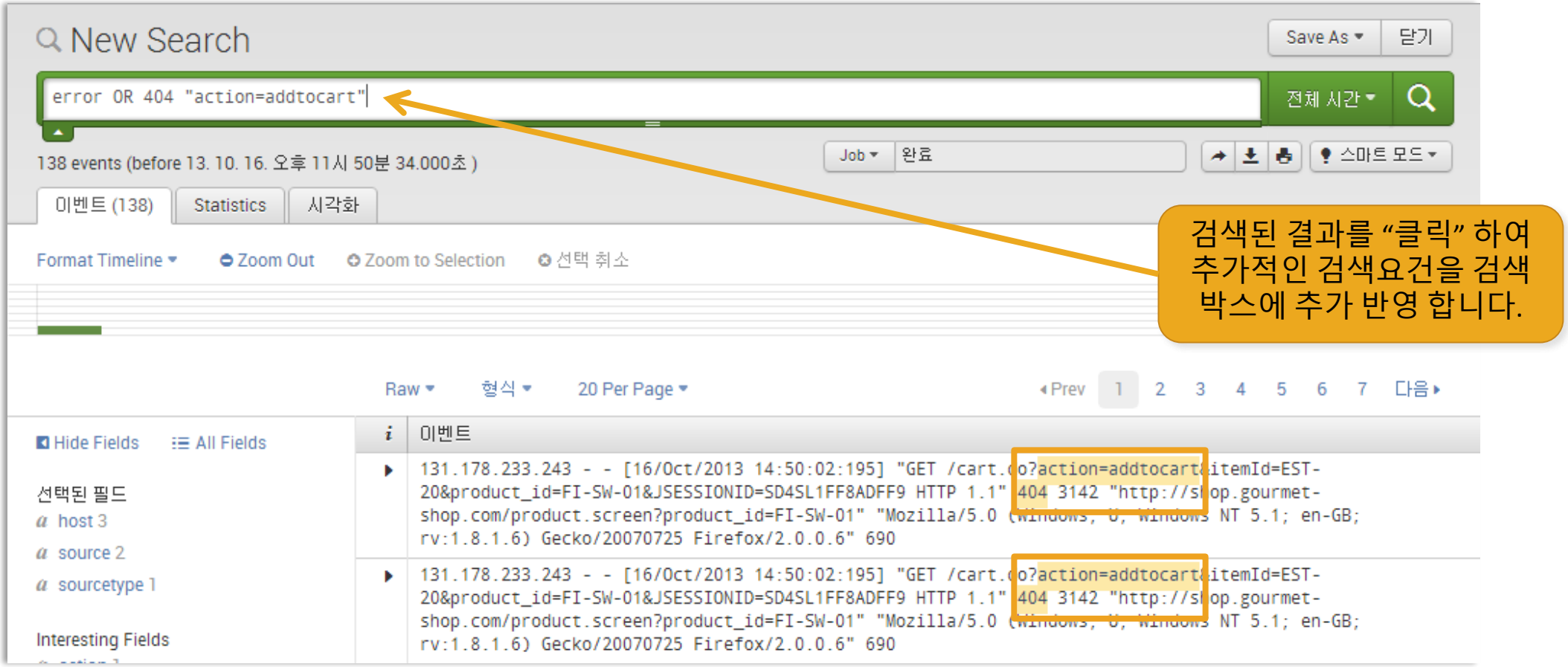
이벤트

- ✓검색은 이벤트/ Row 를 결과를 호출
- ✓하나의 이벤트는 Splunk내 저장된 데이터 하나의 Record 입니다. 예를 들어 로그의 한 줄 이나 DB상의 하나의 ROW와 같은 단위 입니다.
- ✓단일 이벤트는 timestamp, host, source, sourcetype 등의 metadata를 tagging 하여 저장되며 이에 따라 호출 될 수 있습니다.



검색 결과 내 이동– 클릭

✓결과값에서 간단하게 세부 검색 가능



결과 탐색– “Alt” + “Click”

✓검색 된 결과 값에서 제외할 세부 검색문 추가