

Splunk 실행

Splunk 검색 개요

- 여러 이종의 데이터의 복합 검색 및 분석의 요구사항 충족

The diagram illustrates the Splunk search interface and its capabilities. On the left, four data sources are listed with corresponding icons: Database (cylinder), 미들웨어 오류 (gear), 서비스 시스템 (stack of papers), and 외부 인터넷 데이터 (Twitter bird). These sources feed into a central search interface. The interface shows a search bar with the query '10098213' and a dropdown menu. Below the search bar, the search results are displayed, showing a list of events. The results are organized into columns: 문제 ID (Problem ID), 세션정보 (Session Info), 사용자 ID (User ID), 프로세스 (Process), 문제 ID (Problem ID), 서비스 정보 (Service Info), 문제 ID (Problem ID), 문제 외부 ID (Problem External ID), and 유해 감염 정보 (Malicious Infection Info). The results show a sequence of events related to a database connection error and a social media post. The search results are also linked to a 'WHO IS의 외부 DB' (WHO IS External DB) at the bottom.

Database

미들웨어 오류

서비스 시스템

외부 인터넷 데이터

검색 10098213 ← 문제의 ID 검색 전체 시간

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: 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

서비스 정보

문제 ID

문제 외부 ID 유해 감염 정보

WHO IS의 외부 DB

Search(검색) App 실행

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

The image illustrates the process of accessing the Splunk Search & Reporting application through four numbered steps:

- 1**: The Splunk login screen. It features the 'splunk>enterprise' logo, fields for '사용자 이름' (Username) and '암호' (Password), and a '로그인' (Login) button. A message indicates a successful login: '로그아웃되었습니다. 로그인하여 시스템으로 돌아가십시오.' (You have been logged out. Please log in to return to the system).
- 2**: The Splunk home page. The 'Search & Reporting' app is highlighted with a green button and an orange arrow pointing to the next step.
- 3**: The Search & Reporting app interface. It shows a search bar, a '검색 방법' (Search Method) section with links to '설명서' (Documentation) and 'Tutorial', and a 'What to Search' section with filters for '839,931 이벤트 INDEXED', '4년 전 EARLIEST EVENT', and '지금 LATEST EVENT'. The 'Data Summary' button is highlighted with an orange arrow pointing to the next step.
- 4**: The Data Summary page. It displays a table of sourcetypes with their respective counts and last update times. The table is filtered by 'Hosts (114)', 'Sources (1,009)', and 'Sourcetypes (47)'.

Sourcetype	개수	Last Update
flightdata	509,264	13. 10. 16. 오후 09시 12분 06.000초
netscout_http	53,871	13. 10. 16. 오후 09시 12분 15.000초
appflow	52,885	13. 10. 16. 오후 09시 11분 08.000초
oracle_listener	29,353	13. 10. 16. 오후 09시 12분 15.000초
flightsummary	28,648	13. 10. 16. 오후 09시 11분 05.000초
access_combined	26,583	13. 10. 16. 오후 10시 13분 45.000초
oracle_alert	22,770	13. 10. 16. 오후 09시 11분 29.000초
aix_audit	17,087	13. 10. 16. 오후 09시 11분 12.000초
WindowsUpdateLog	15,236	13. 10. 16. 오후 09시 11분 06.000초
estreamer	13,810	13. 10. 16. 오후 09시 10분 59.000초
oracle_audit	13,500	13. 10. 16. 오후 09시 12분 01.000초
OrderImage	10,005	13. 10. 16. 오후 09시 11분 17.000초
WLC	10,000	13. 10. 16. 오후 09시 11분 17.000초

Search Summary 뷰 이해

- Splunk에서 가장 기본적인 화면 기능 설명

The main screenshot shows the Splunk Search Summary view. Annotations point to various components:

- 현재 뷰** (Current View): Points to the 'Search & Reporting' app header.
- 검색 박스** (Search Box): Points to the search input field.
- 메뉴와 액션 링크** (Menu and Action Links): Points to the navigation bar (Search, Pivot, Reports, Alerts, Dashboards).
- 시간 범위 설정** (Time Range Setting): Points to the 'Time Range' dropdown menu.
- 실행** (Execute): Points to the search button.

Below the main view are three inset panels showing different views of the 'Data Summary':

- 1 Data Summary**: Shows a table of hosts with columns for host, status, and count.
- 2 Data Summary**: Shows a table of sources with columns for source, status, and count.
- 3 Data Summary**: Shows a table of sourcetypes with columns for sourcetype, status, count, and last update.

호스트	상태	개수
10.250.100.48	all	4
10.250.102.48	all	4
10.250.103.48	all	4
10.250.110.48	all	5
10.250.117.48	all	4
10.250.119.48	all	5
10.250.120.48	all	4
10.250.121.48	all	5
10.250.122.48	all	4

Source	상태	개수
/opt/apache/log/access_combined.log	all	
C:\Program Files (x86)\Splunk/etc/apps/FireEye/logs/172.16.102.7.log	all	
C:\Program Files (x86)\Splunk/etc/apps/FireEye/logs/172.16.216.1.log	all	
C:\Program Files (x86)\Splunk/etc/apps/Openwave/logs/ngp_txn_logs.txt	all	
C:\Program Files (x86)\Splunk/etc/apps/Sourcefire/log/estreamer.log	all	

Sourcetype	상태	개수	Last Update
CDR	all	576	13. 10. 16. 오후 09시 11분 08.000초
FireEye_CEF	all	5,172	13. 10. 16. 오후 09시 10분 58.000초
MonitorWare:Security	all	1,000	13. 10. 16. 오후 09시 11분 13.000초
NTSsyslog:Security	all	256	13. 10. 16. 오후 09시 11분 13.000초
OrderImage	all	10,005	13. 10. 16. 오후 09시 11분 17.000초
Snare:Security	all	67	13. 10. 16. 오후 09시 11분 13.000초
WLC	all	10,000	13. 10. 16. 오후 09시 11분 17.000초
WinEventLog:Security	all	915	13. 10. 16. 오후 09시 11분 13.000초



검색 개요

검색 기초

모든 것이 검색 가능합니다

✓ * 와일드 카드 지원

`fail*`

✓ 검색 패턴의 요건은 대소문자를 구분하지 않습니다.

`fail* nfs`

✓ Booleans “AND”, “OR”, “NOT”

- Booleans의 표현은 대문자로 표시
- 검색 패턴의 요건의 중간에 적용
- 복잡한 검색 요건을 “()” 그룹화 함

`error OR 404`

✓ 정확한 단어열은 “”로 표현

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

`“login failure”`

“검색 엔진”, 그 이상의 기능

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

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

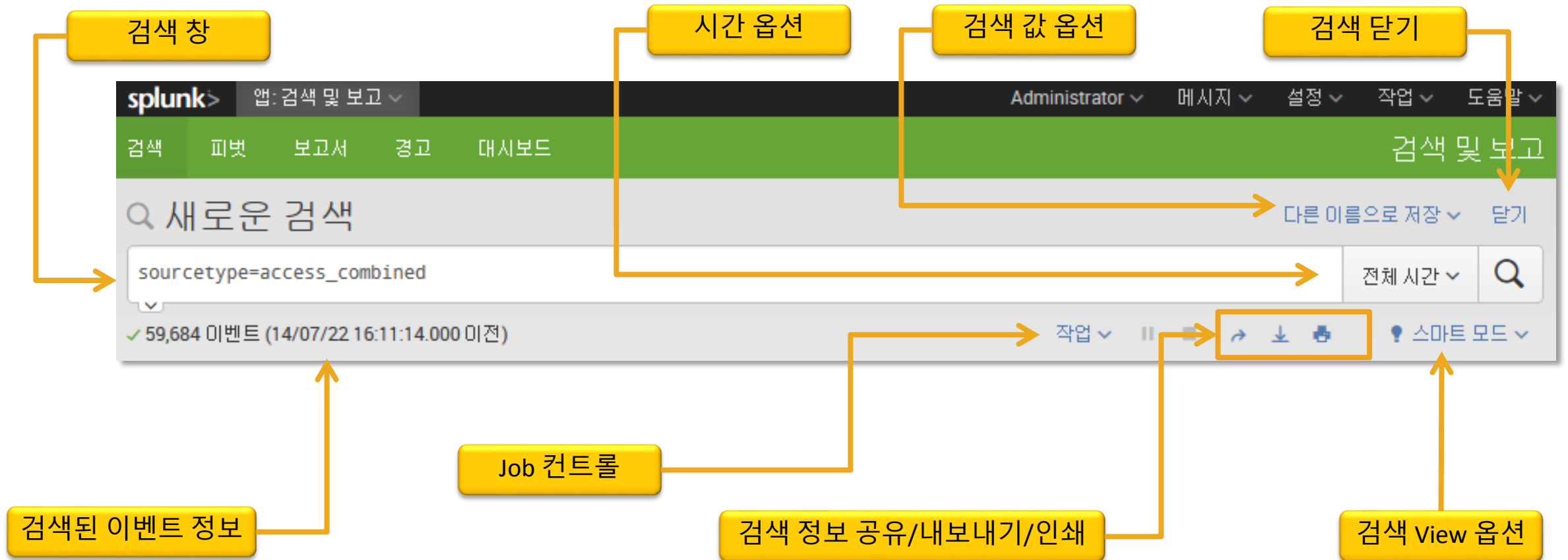
```
sourcetype=access_combined status>=300
```

```
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 Splunk 검색 도우미 기능은 해당 명령어의 빠른 사용법을 찾아 보여주고, 특정 필드의 input이 필요할 경우 선택 가능한 필드의 종류도 호출하여 줍니다.

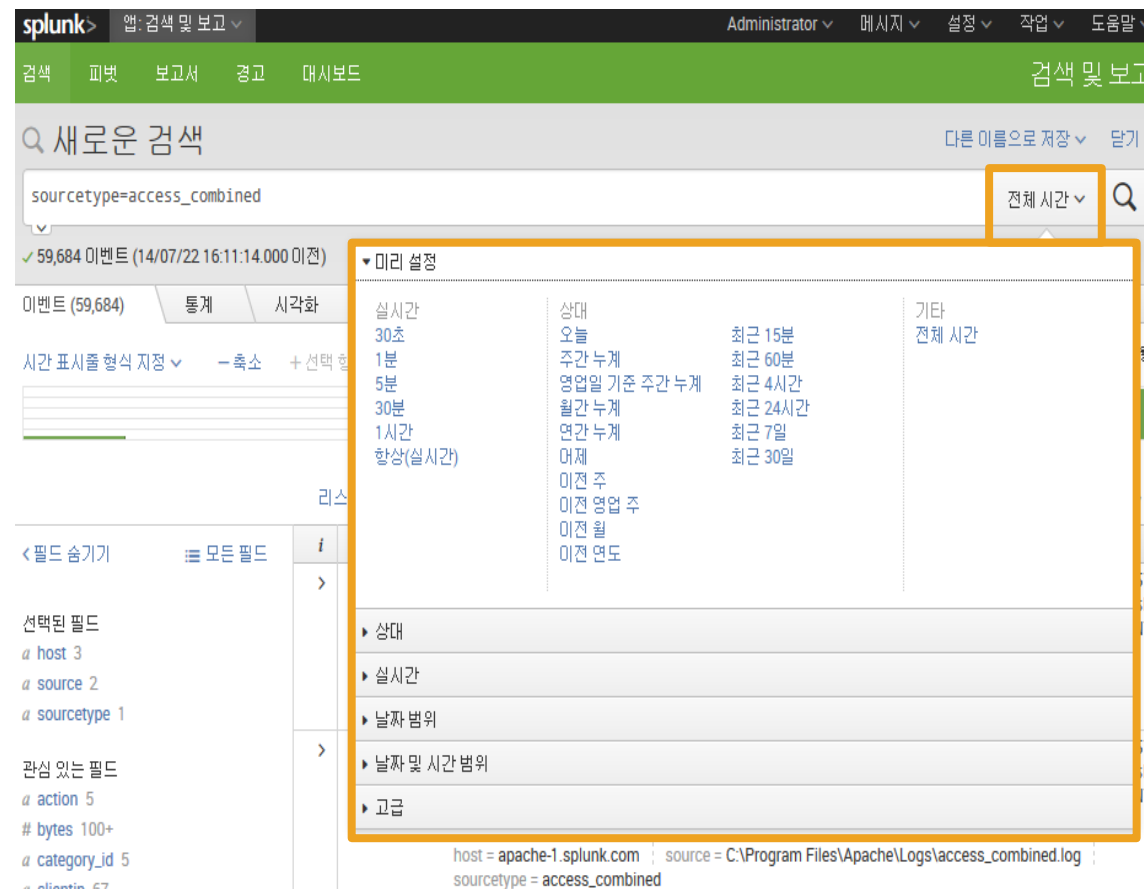
The screenshot shows the Splunk search interface with the command `sourcetype=access_combined clientip="125.17.*" | sort|` entered in the search bar. Below the search bar, there are two main sections:

- 명령어 내역 (Command History):** A list of commands including `| sort -count`, `| sort _time`, `| sort -sourcetype`, `| sort host, dest_port`, and `| sort host`. A yellow box highlights this list, and an arrow points from a yellow box labeled "선택 가능한 필드 종류" (Selectable field types) to it.
- sort 도움말 (sort Help):** A section titled "sort" with a "도움말" (Help) link. It explains that the command sorts search results by a specified field. It provides examples:
 - Sorting by "ip" field in ascending order, then by "url" field in descending order: `| sort ip, -url`.
 - Sorting the first 100 results by "size" field in descending order, then by "source" field in ascending order: `| sort 100 -size, +source`.
 - Sorting by "_time" field in ascending order, then by "host" field in descending order: `| sort _time, -host`.

A yellow box labeled "명령어의 옵션 및 사용법" (Command options and usage) has an arrow pointing to the "sort" help section.

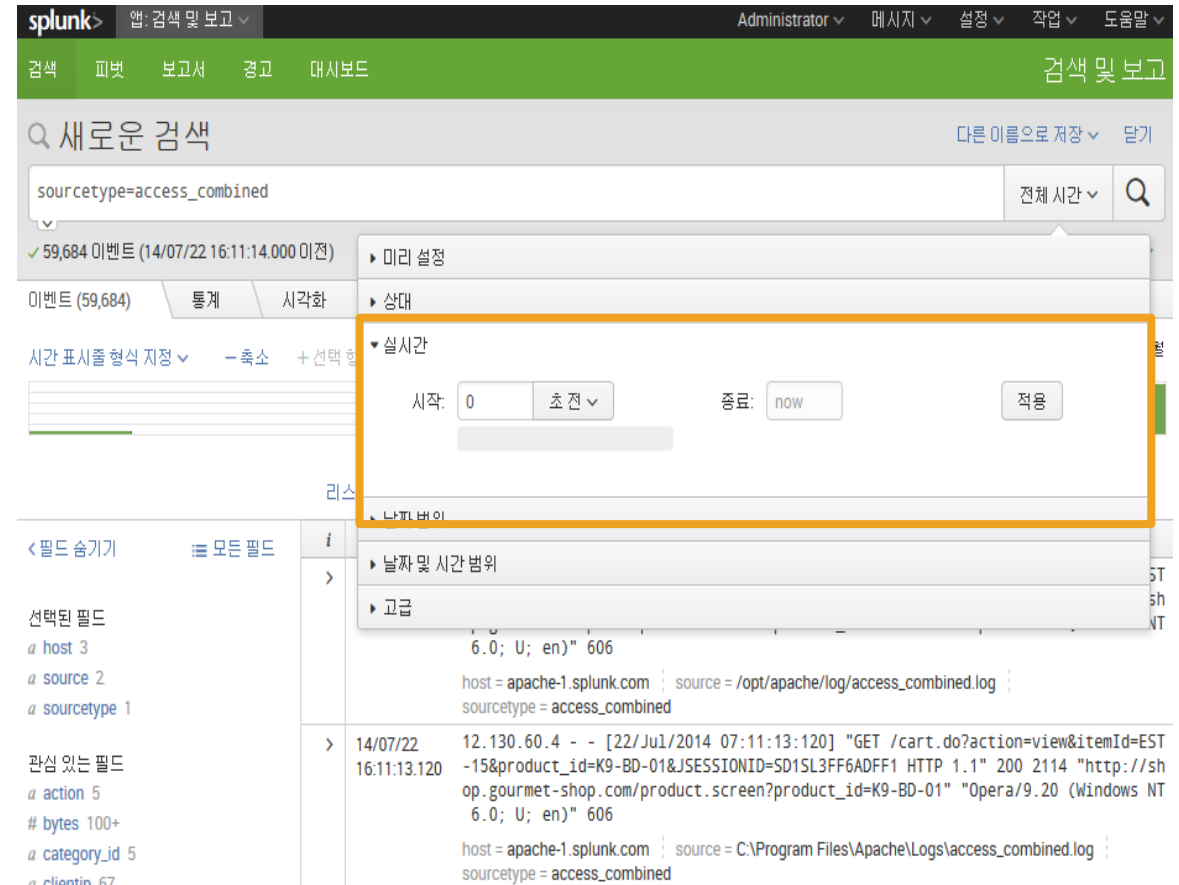
검색의 시간 범위 조정

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



Real-time 검색

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

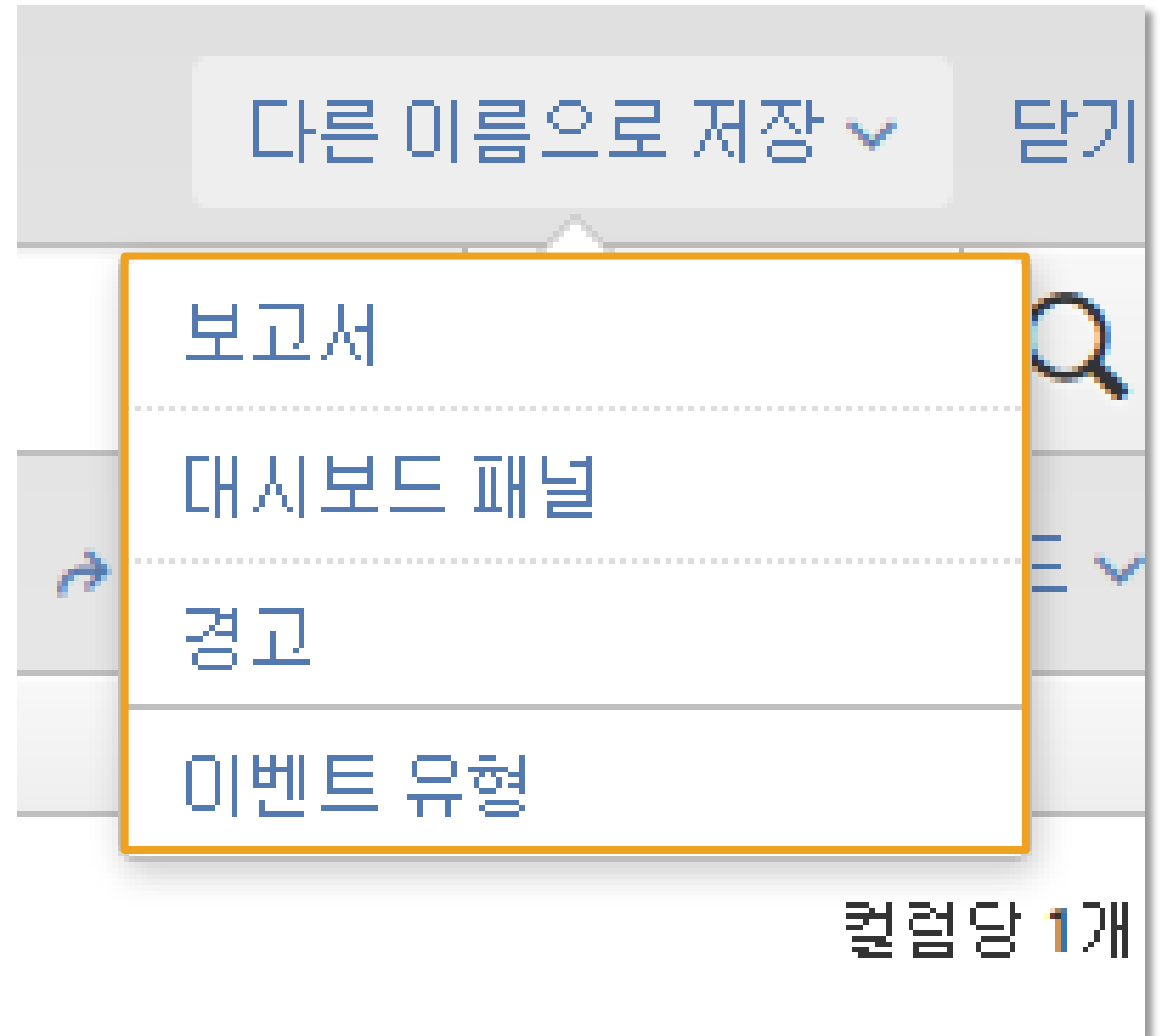




결과와의 Interaction

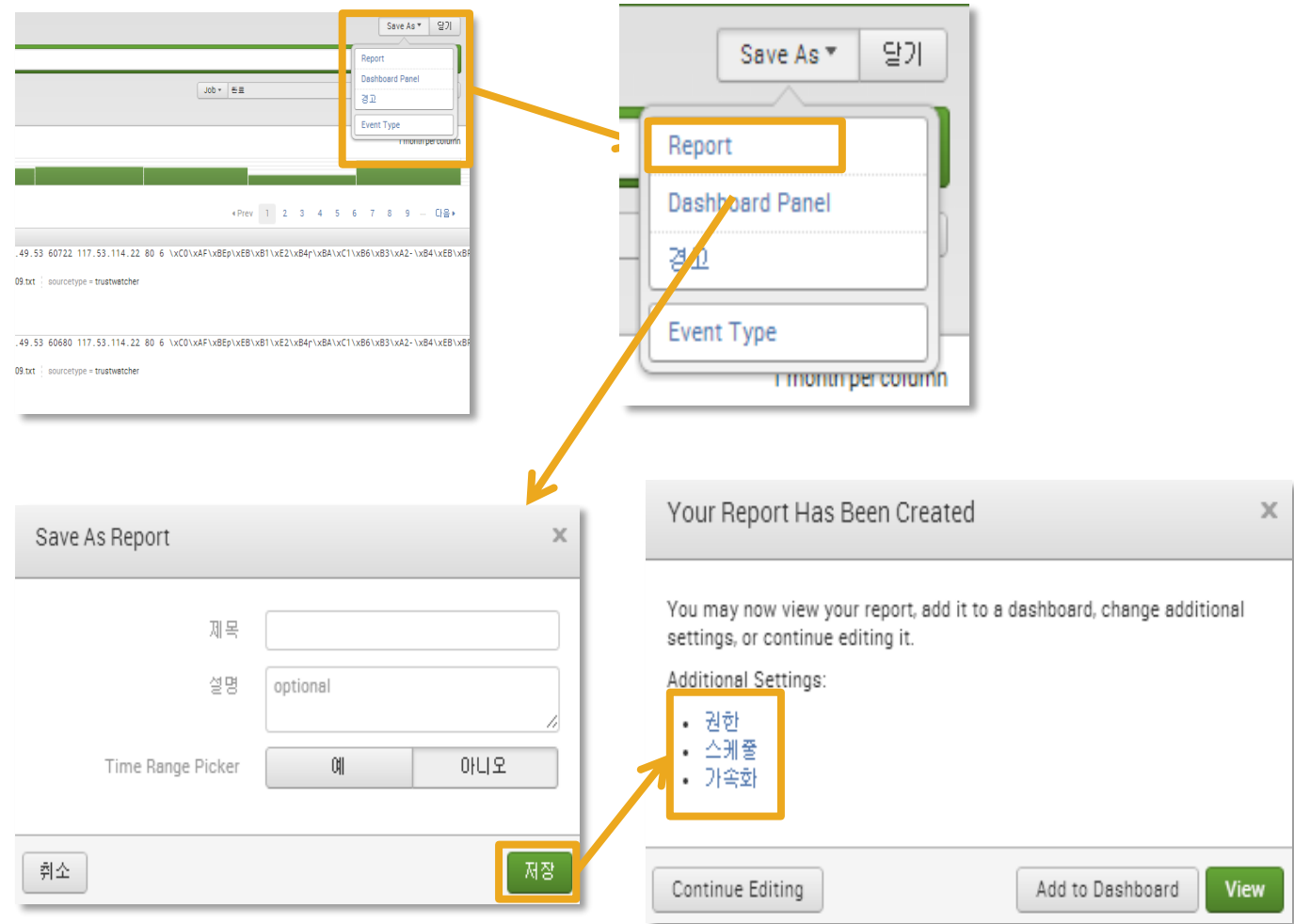
결과 저장 및 연계

- ✓ “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.



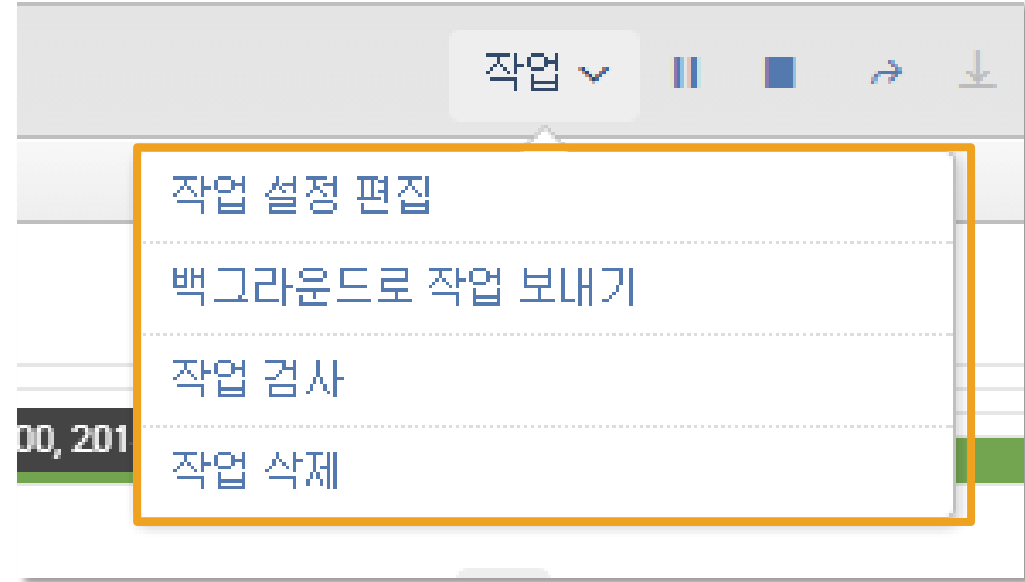
검색 저장

- ✓ “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

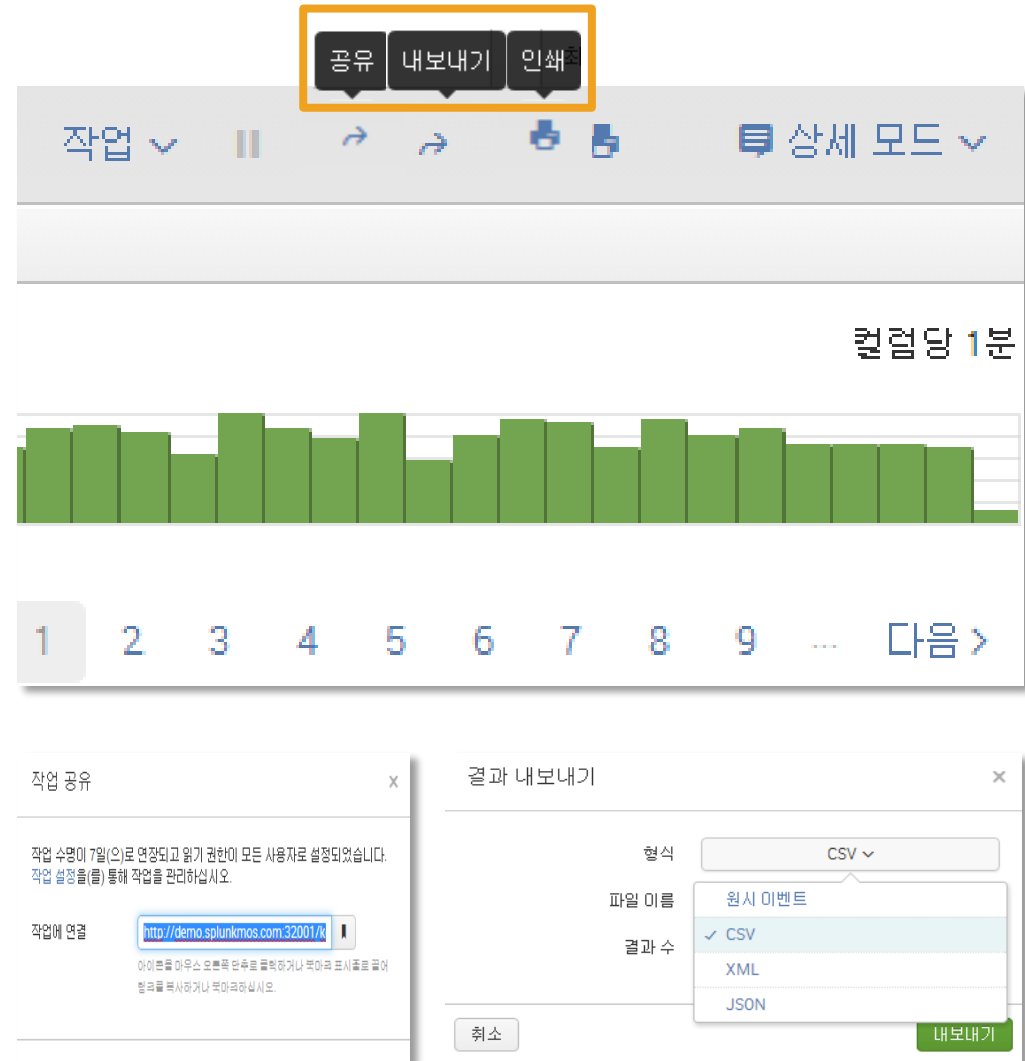
- ✓ '작업 설정 편집'은 검색 작업 내용의 읽기권한, 주기를 설정할 수 있고 검색된 결과를 Link URL 을 통해 공유 할 수 있습니다.
- ✓ '백그라운드로 작업 보내기'는 현재 작업을 백그라운드로 보냅니다.
- ✓ '작업검사'는 작업의 상세내역을 확인 할 수 있습니다.

A screenshot of the '작업 설정' (Job Settings) dialog box. It contains fields for '소유자' (Owner) set to 'admin', '업' (Job) set to 'search', '읽기 권한' (Read Permission) with buttons for '비공개' (Private) and '모든 사용자' (All Users), '수명' (Lifetime) with buttons for '10분' (10 min) and '7일' (7 days), and '작업에 연결' (Link to Job) with a URL 'http://demo.splunkmos.com:32001/k'. There are '취소' (Cancel) and '저장' (Save) buttons at the bottom.A screenshot of the '백그라운드로 작업 보내기' (Send Job to Background) dialog box. It has a checkbox '완료 시 이메일 보내기' (Send email when complete) which is checked. Below it is a text field '이메일 제목 줄' (Email subject line) with the value 'Splunk 작업 완료: \$name\$'. There is also an '이메일 주소' (Email address) field. At the bottom, there is a '취소' (Cancel) button and a green '백그라운드로 보내기' (Send to background) button.A screenshot of the '검색 작업 검사기' (Search Job Inspector) window. It displays a table with job details. The table has columns: '이름(표)' (Name), 'Component', '프로' (Process), '입력 수' (Input), and '출력 수' (Output).

이름(표)	Component	프로	입력 수	출력 수
0.076	command fields	87	637,369	637,369
04.222	command search	194	637,369	1,274,735
0.775	command search filter	211	-	-
0.711	command search fieldes	114	637,369	637,369
0.456	command search index	449	-	-
0.135	command search calchelds	114	637,369	637,369
0	command search index uac_1_3	1,769	-	-
0	command search index uac_3_04	182	-	-
04.040	command search type	97	637,369	637,369

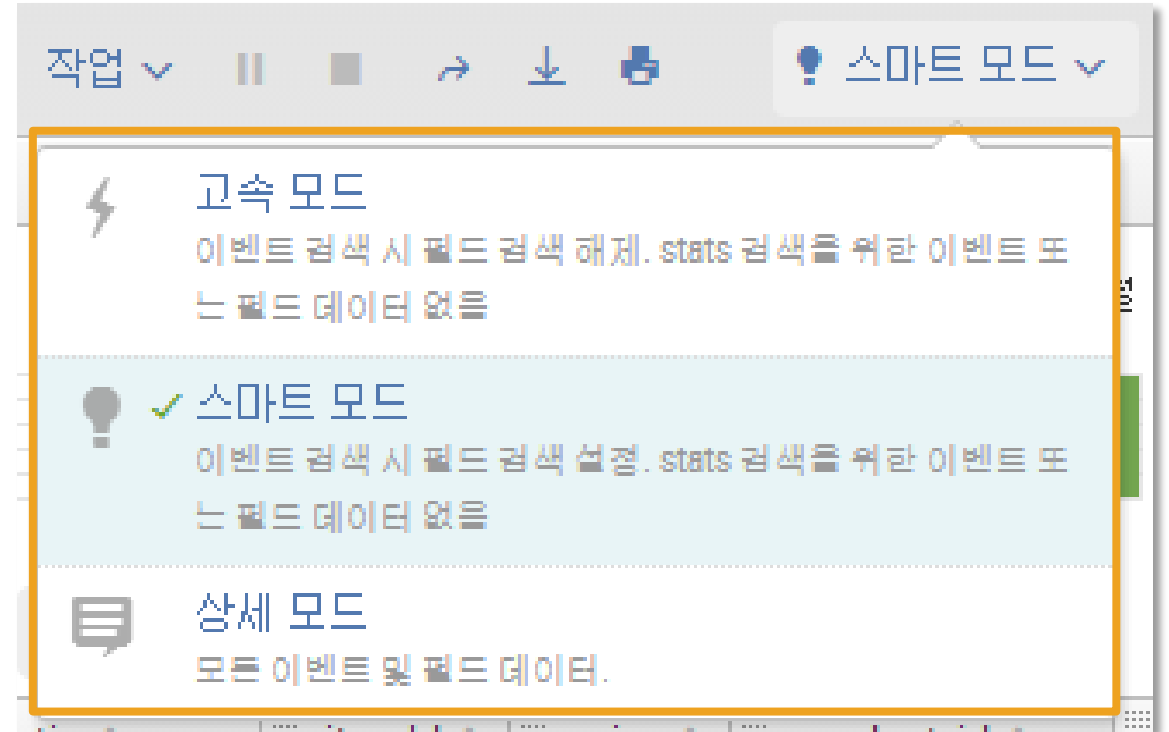
검색 정보 공유/내보내기/인쇄

- ✓ 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 제공합니다.
- ✓ 상세 모드는 필드 추출 및 모든 시각적 검색 현황을 같이 출력합니다.



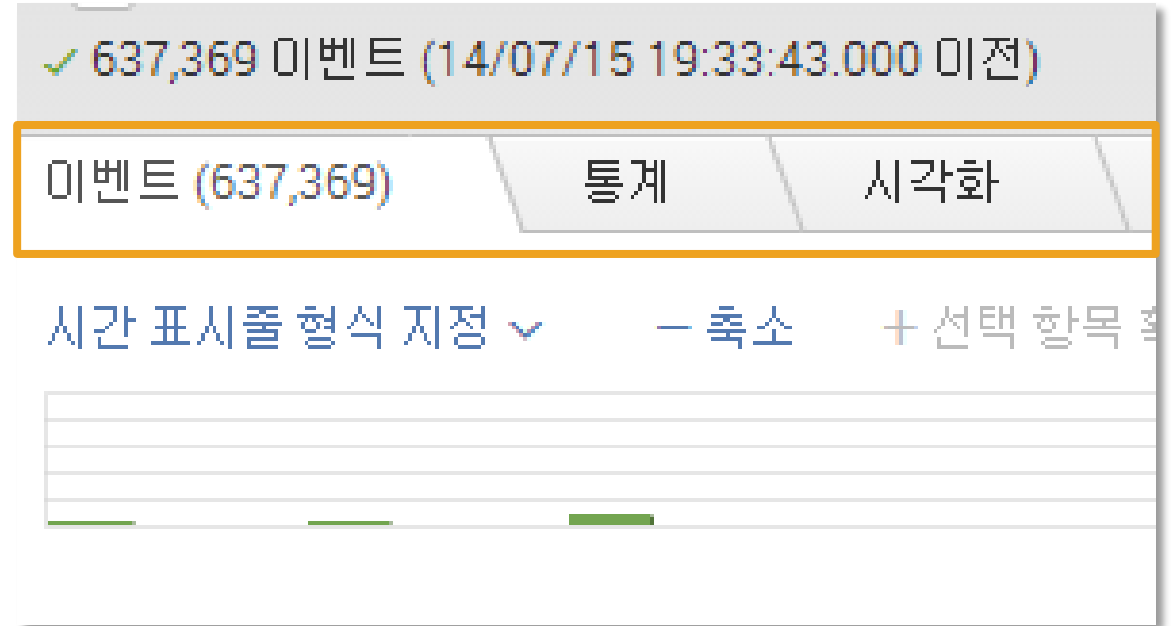
Timeline 네비게이션

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



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 비주얼한 chart 형태로 데이터를 표현해 줍니다.



검색된 결과 옵션

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

원시 View

i	이벤트
>	125.17.14.100 - - [15/Jul/2014 10:50:09:192] "GET /cart.do?actuct_id=K9-CW-01&JSESSIONID=SD10SL7FF7ADFF9 HTTP 1.1" 400 2955 tegory.screen?category_id=BOUQUETS" "Mozilla/5.0 (Macintosh; UAppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safar
>	10.2.1.34 201.3. HARGERS&JSESSION=purchase&itemId4_3_3 like Mac O.3;FBBV/4030.0;FBID/phone;FBLC/j

리스트 View

i	시간	이벤트
>	14/07/15 19:50:09.192	125.17.14.100 - - [15/Jul/2014 10:50:09:192] "GET =EST-21&product/5.0.375.38 Safa

테이블 View

i	_time	action	category_id	clientip	itemId
>	14/07/15 19:50:09.192	purchase	BOUQUETS	125.17.14.100	EST-21
>	14/07/15 19:50:06.741	purchase	CHARGERS	201.3.120.132	EST-27

새로운 검색

sourcetype=acc*

✓ 637,369 이벤트 (14/07/15 19:33:43.000 이전)

이벤트 (637,369) | 통계 | 시각화

시간 표시줄 형식 지정 | - 축소 | + 선택 항목 확대/축소 | × 선택 취소

2011/03/01

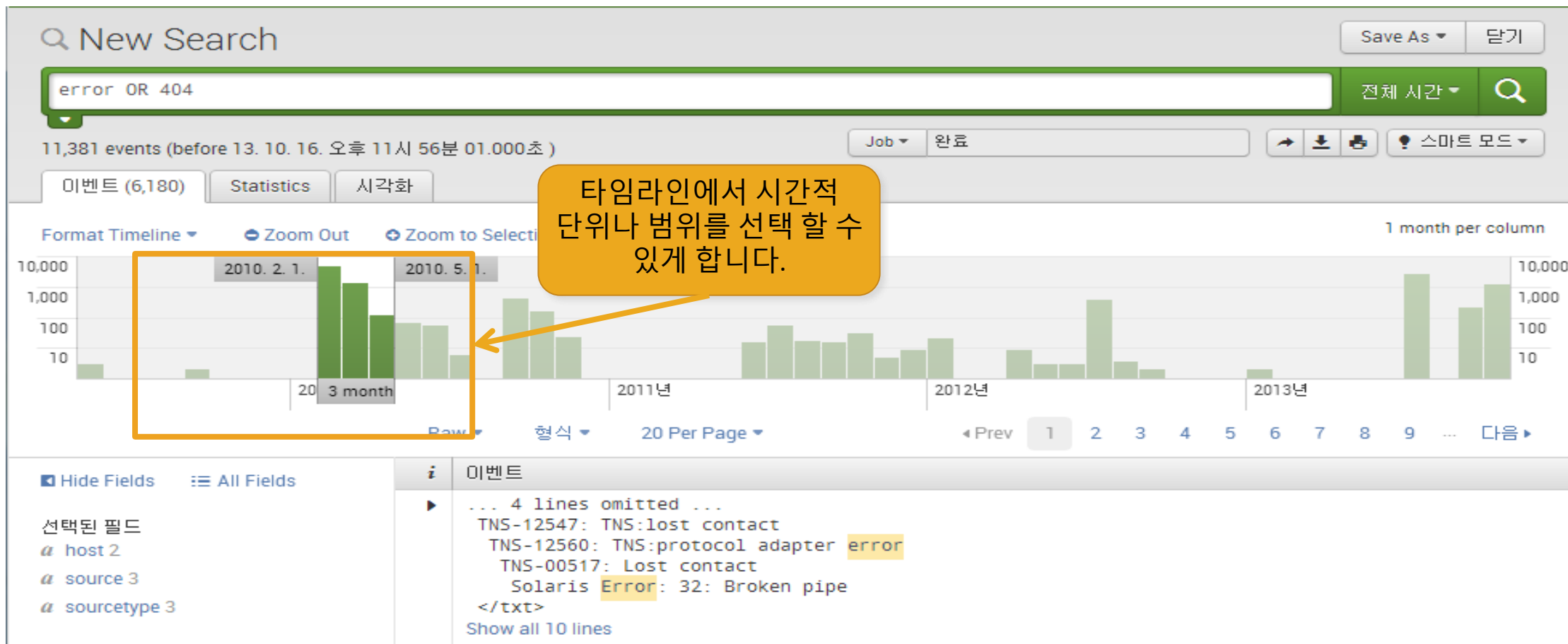
3 years 5 months

테이블 View 선택

action	category_id	clientip	itemId
addtocart		91.214.92.22	
		12.130.60.4	EST-7
changequantity	MEMORYCARDS	141.146.8.66	EST-19

결과 탐색 - Timeline

✓ 검색된 결과의 범위를 선택하여 내용의 위치를 조정 합니다.



결과 탐색-Timeline (cont.)

- ✓ Timeline 네비게이션 기능을 통하여 Interactive하게 데이터의 범위를 조정 합니다.

The screenshot shows the Splunk Timeline interface. At the top, there is a search bar with the query `sourcetype=access_combined NOT "itemId=EST"` and a result count of 263,128 events. Below the search bar, there are tabs for '이벤트 (75,493)', '통계', and '시각화'. The '시각화' tab is selected, showing a timeline view. The timeline has a green bar representing the selected time range, with a label '7 hours' below it. Two orange callout boxes provide instructions: one points to the '+ 선택 항목 확대/축소' button, stating '“선택 항목 확대/축소” 는 검색영역의 범위를 한 번 더 확대 및 축소 합니다.' (The 'Expand/Reduce selected items' button further expands and reduces the search area range). The other points to the timeline itself, stating '타임라인에서 시간적 단위나 범위를 선택 할 수 있게 합니다.' (Allows selecting time units or ranges in the timeline). The interface also includes a '공유' (Share) button, a '최근 24시간' (Last 24 hours) dropdown, and a '상세 모드' (Detailed mode) dropdown.

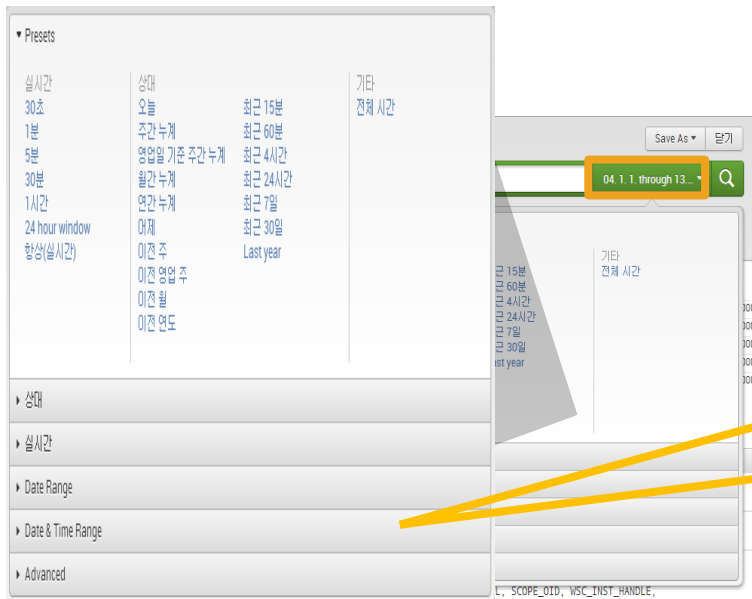
“선택 항목 확대/축소” 는
검색영역의 범위를 한 번 더 확대
및 축소 합니다.

타임라인에서 시간적
단위나 범위를 선택 할 수
있게 합니다.

새로운 검색
sourcetype=access_combined NOT "itemId=EST"
263,128 이벤트 (14/05/19 8:00:00.000 ~ 14/05/20 8:22:56.000)
이벤트 (75,493) 통계 시각화
시간 표시줄 형식 지정 - 축소 + 선택 항목 확대/축소 x 선택 취소
2014/05/19 16:00 2014/05/19 23:00
7 hours
다른 이름으로 저장 달기
공유 최근 24시간 상세 모드
컬럼당 1시간

사용자 지정 시간 설정

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



▶ Presets

▶ 상대

▶ 실시간

▶ Date Range

▼ Date & Time Range

시작: 2004-01-01 00:00:00.000 종료: 2014-01-01 00:00:00.000 적용

▶ Advanced

검색 결과

✓ 검색 결과 창에서는 검색 된 결과의 출력 방식을 설정 합니다.

검색된 데이터 보는 방법 선택기

필드 선택기

리스트 ▾ 형식 ▾ 페이지당 20개 ▾ < 이전 1 2 3 4 5 6 7 8 9 ... 다음 >

	i	시간	이벤트
< 필드 숨기기	>	14/05/20 8:14:23.107	141.146.8.66 - - [20/May/2014 08:14:23:107] "GET /product.screen?product_id=RP-SN-01&JSESSIONID=SD75L1FF10ADFF3 HTTP 1.1" 200 879 "http://www.myflowershop.com/cart.do?action=purchase&itemId=EST-14&product_id=RP-SN-01" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6" 801 host = apache-1.splunk.com source = /opt/apache/log/access_combined.log sourcetype = access_combined
선택된 필드 a host 3 a source 1 a sourcetype 1	>	14/05/20 8:14:21.116	12.130.60.5 - - [20/May/2014 08:14:21:116] "GET /cart.do?action=purchase&itemId=EST-19&product_id=AV-SB-02&JSESSIONID=SD10SL4FF10ADFF4 HTTP 1.1" 200 3219 "http://www.myflowershop.com/oldlink?item_id=EST-19" "Opera/9.01 (Windows NT 5.1; U; en)" 615 host = apache-2.splunk.com source = /opt/apache/log/access_combined.log sourcetype = access_combined
관심 있는 필드 a action 1 # bytes 100+ a category_id 5			

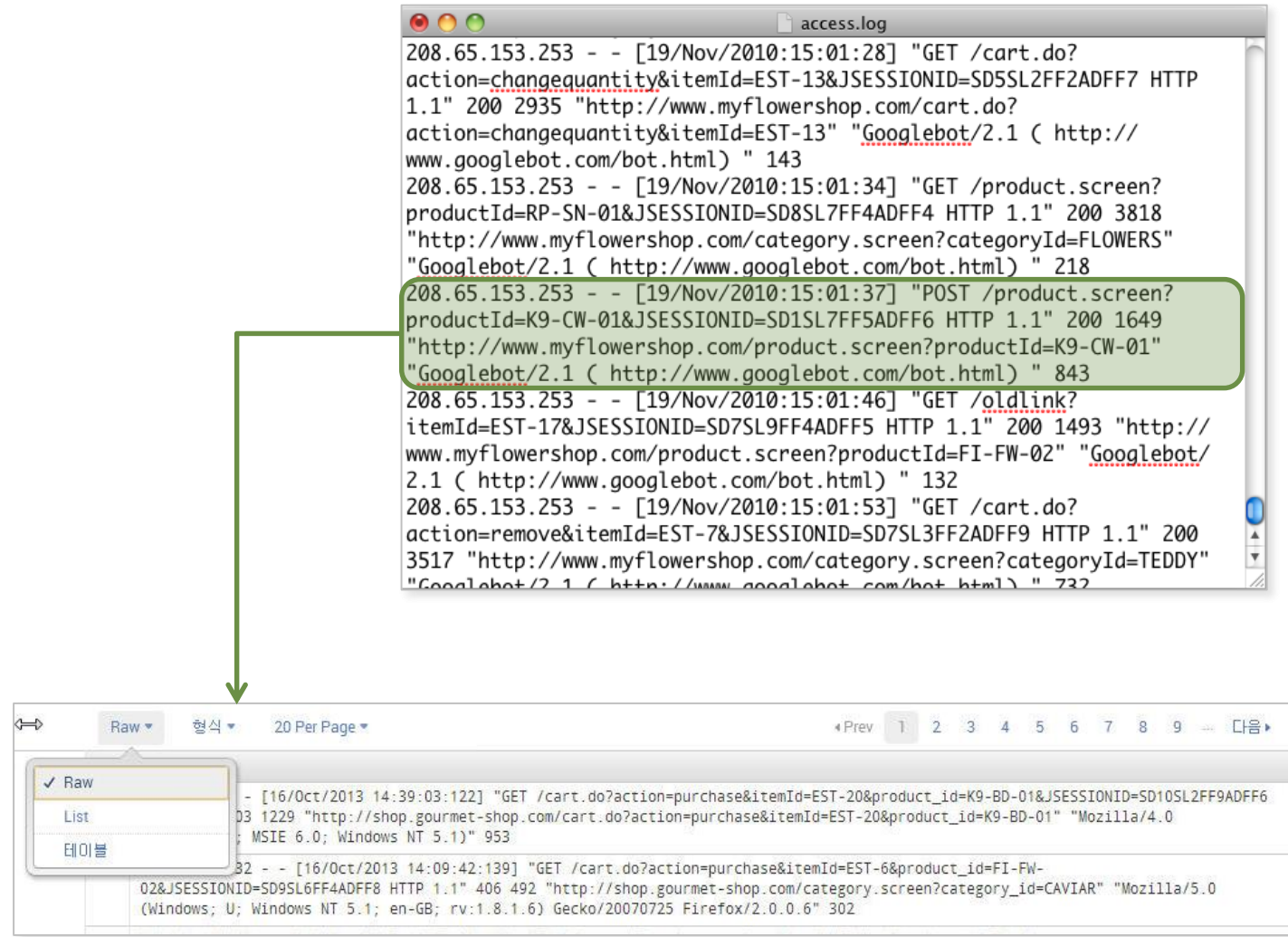
이벤트 데이터 / 검색된 Row

검색된 확인된 결과 Highlight

시간 Stamp

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

New Search

error OR 404 "action=addtocart"

138 events (before 13. 10. 16. 오후 11시 50분 34.000초)

이벤트 (138) Statistics 시각화

Format Timeline Zoom Out Zoom to Selection 선택 취소

Raw 형식 20 Per Page

i	이벤트
▶	131.178.233.243 - - [16/Oct/2013 14:50:02:195] "GET /cart.co?action=addtocart&itemId=EST-20&product_id=FI-SW-01&JSESSIONID=SD4SL1FF8ADFF9 HTTP 1.1" 404 3142 "http://shop.gourmet-shop.com/product.screen?product_id=FI-SW-01" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6" 690
▶	131.178.233.243 - - [16/Oct/2013 14:50:02:195] "GET /cart.co?action=addtocart&itemId=EST-20&product_id=FI-SW-01&JSESSIONID=SD4SL1FF8ADFF9 HTTP 1.1" 404 3142 "http://shop.gourmet-shop.com/product.screen?product_id=FI-SW-01" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6" 690

Hide Fields All Fields

선택된 필드

- host 3
- source 2
- sourcetype 1

Interesting Fields

Save As 닫기

전체 시간

Job 완료

스마트 모드

검색된 결과를 "클릭" 하여 추가적인 검색요건을 검색 박스에 추가 반영 합니다.

결과 탐색- “Alt” + “Click”

✓ 검색 된 결과 값에서 제외할 세부 검색문 추가

The screenshot shows the Splunk search interface. The search bar contains the query: `error OR 404 "action=addtocart" NOT itemId=EST-7`. The `NOT itemId=EST-7` part is highlighted with an orange box. An orange arrow points from a callout box to this highlight. The callout box contains the text:
[alt] + [click] 하게 되면 반대로 해당 패턴의 결과를 검색 조건에서 제외 합니다.
“NOT”을 적용하는 것과 같은 것을 제공합니다.
Below the search bar, it shows 119 events. The results table is displayed in 'Raw' format, showing three log entries. In each entry, the `action=addtocart` part is highlighted with an orange box. The first two entries are 404 errors, and the third is a 421 status code.

이벤트
27.1.11.11 - - [16/Oct/2013 14:42:54:170] "POST /cart.do action=addtocart &itemId=EST-13&product_id=RP-SN-01&JSESSIONID=SD2SL10FF9ADFF7 HTTP 1.1" 404 3488 "http://shop.gourmet-shop.com/product.screen?product_id=RP-SN-01" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 183
27.1.11.11 - - [16/Oct/2013 14:42:54:170] "POST /cart.do action=addtocart &itemId=EST-13&product_id=RP-SN-01&JSESSIONID=SD2SL10FF9ADFF7 HTTP 1.1" 404 3488 "http://shop.gourmet-shop.com/product.screen?product_id=RP-SN-01" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 183
195.80.144.22 - - [16/Oct/2013 14:42:45:176] "GET /category.screen?category_id=CONDIMENTS&JSESSIONID=SD2SL7FF9ADFF1 HTTP 1.1" 404 1298 "http://shop.gourmet-shop.com/cart.do action=addtocart &itemId=EST-26&product_id=FL-DLH-02" "Opera/9.01 (Windows NT 5.1; U; en)" 421