



## 주요 명령어 예제 실습 심화

# 주요 명령어 : 목록

- |                  |                 |                   |
|------------------|-----------------|-------------------|
| 1. TOP           | 9. SORT         | 17. OVERLAY CHART |
| 2. SEARCH        | 10. HEAD        |                   |
| 3. EVAL-IF       | 11. TAIL        |                   |
| 4. EVAL-CASE     | 12. DEDUP       |                   |
| 5. EVAL-MATCH    | 13. FIELDFORMAT |                   |
| 6. EVAL-strftime | 14. RANGEMAP    |                   |
| 7. RENAME        | 15. IPLOCATION  |                   |
| 8. REPLACE       | 16. GEOSTATS    |                   |

# 주요 명령어 : TOP

- TOP: 지정된 필드의 상위 값을 계산
- 문제: 상위 10위까지 고객아이피의 리스트를 만드세요.
- 답: `sourcetype=access_combined | top 10 clientip`

새로운 검색

`sourcetype="access_combined" | top 10 clientip` 최근 60분

21,623 이벤트 (14/07/23 12:36:00.000 ~ 14/07/23 13:36:48.000)

이벤트 (21,623) 통계 (10) 시각화

페이지당 20개 형식 미리보기

clientip	count	percent
141.146.8.66	1864	8.620450
12.130.60.4	1848	8.546455
12.130.60.5	1826	8.444712
125.17.14.100	1795	8.301346
130.253.37.97	1785	8.255099
128.241.220.82	1758	8.130232
131.178.233.243	1734	8.019239
10.2.1.44	709	3.278916
86.9.190.90	184	0.850946
94.229.0.21	174	0.804699

# 주요 명령어 : SEARCH(1)

- SEARCH : 키워드, 따옴표로 묶은 절, 와일드카드 및 키/값 쌍 식을 사용하여 결과를 필터링 합니다.
- 문제 : 최근 15분 동안 접속 횟수가 많은 고객의 IP 중에서 앞자리가 20으로 시작되는 IP를 찾아보세요.
- 답 : `sourcetype=access_combined | stats count by clientip | search clientip=20*.*.*`

새로운 검색

`sourcetype=access_combined | stats count by clientip | search clientip=20*.*.*`

5,416 이벤트 (14/07/23 13:36:37.000 ~ 14/07/23 13:51:37.000)

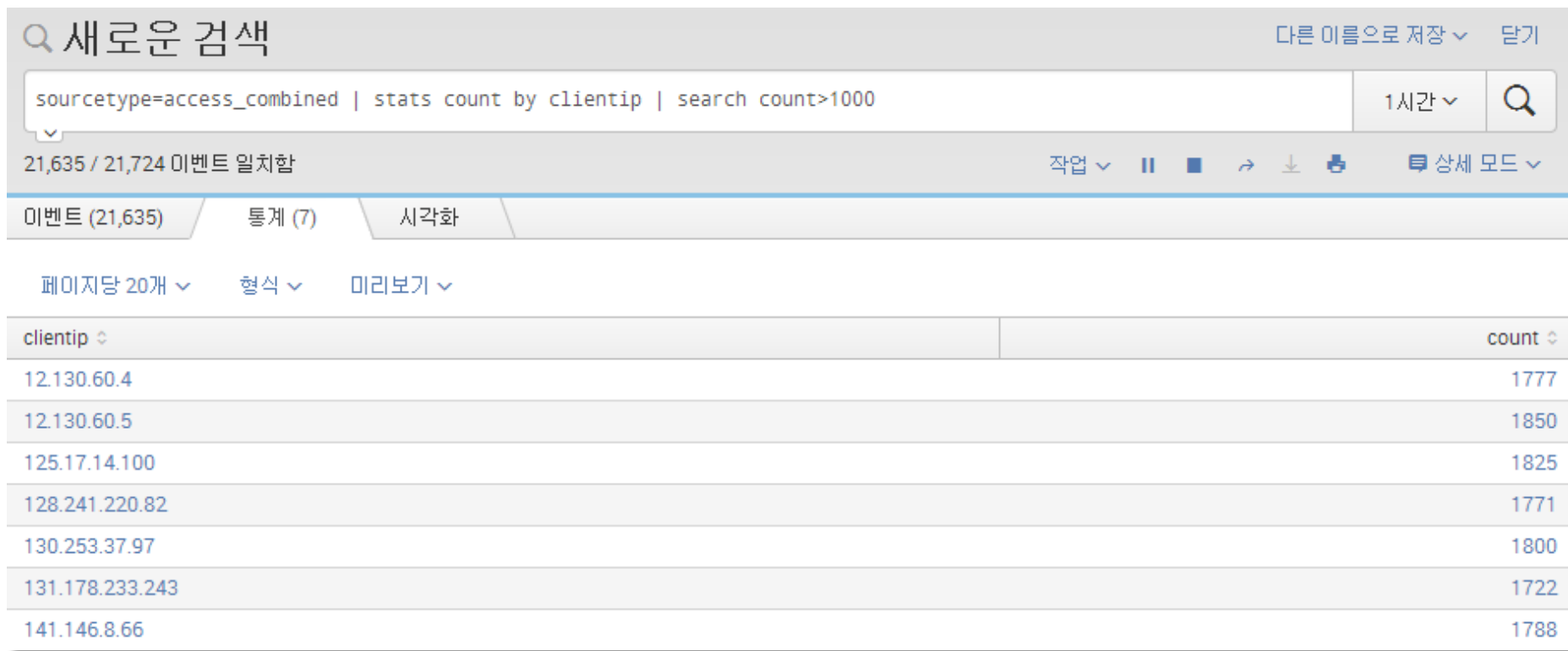
이벤트 (5,416) | 통계 (8) | 시각화

페이지당 20개 | 형식 | 미리보기

clientip	count
200.6.134.23	42
200.122.42.235	24
200.28.109.162	18
200.3.120.132	44
200.42.223.29	28
200.164.25.24	32
200.223.0.20	22
200.92.58.136	28

# 주요 명령어 : SEARCH(2)

- 문제 : 최근 1시간 동안 1000번 이상 방문한 고객의 IP를 찾아보세요.
- 답 : `sourcetype=access_combined | stats count by clientip | search count>1000`



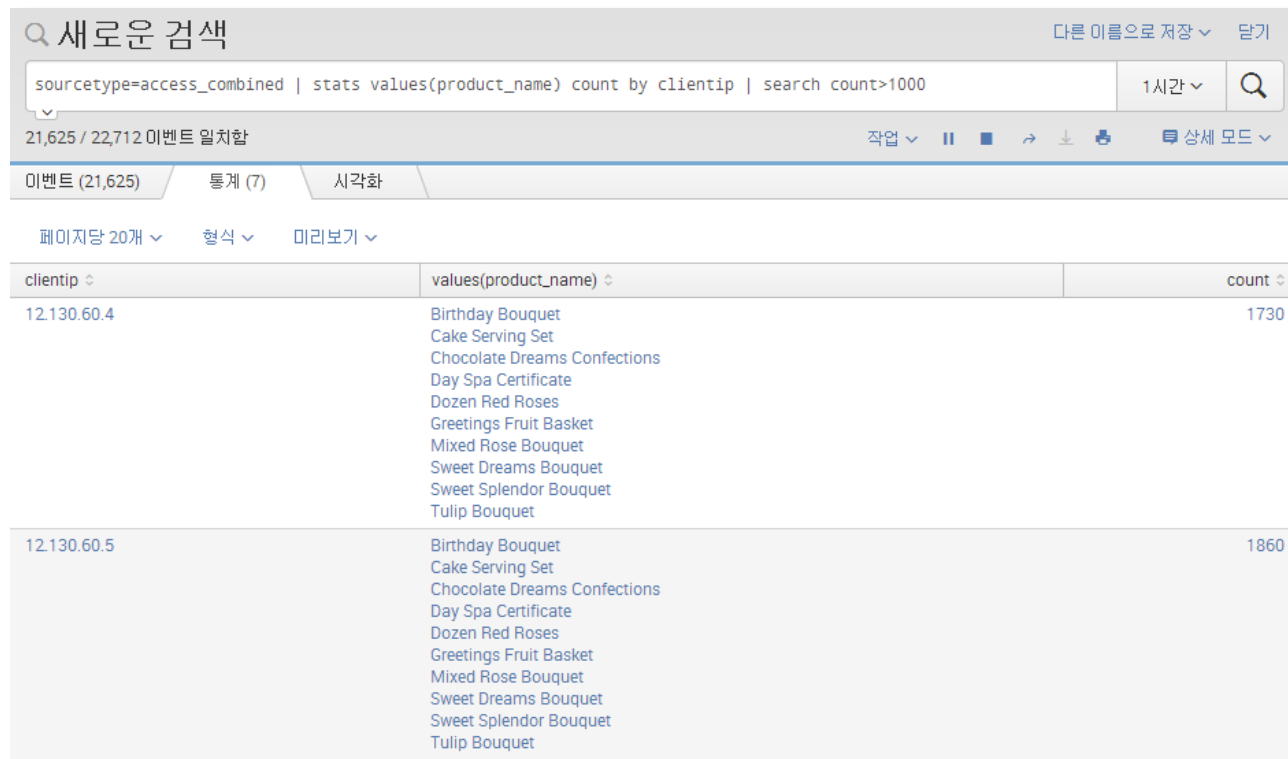
The screenshot shows the Splunk Search interface. At the top, the search bar contains the query `sourcetype=access_combined | stats count by clientip | search count>1000`. Below the search bar, the results are displayed in a table format. The table has two columns: `clientip` and `count`. The results show the following IP addresses and their corresponding counts:

clientip	count
12.130.60.4	1777
12.130.60.5	1850
125.17.14.100	1825
128.241.220.82	1771
130.253.37.97	1800
131.178.233.243	1722
141.146.8.66	1788

# 주요 명령어 : SEARCH(3)

➤ 문제 : 최근 1시간 동안 1000건 이상 방문한 사용자의 관심품목 (product\_name) 명의 리스트를 함께 나타내세요.

➤ 답 : `sourcetype=access_combined | stats values(product_name) count by clientip | search count>1000`



clientip	values(product_name)	count
12.130.60.4	Birthday Bouquet Cake Serving Set Chocolate Dreams Confections Day Spa Certificate Dozen Red Roses Greetings Fruit Basket Mixed Rose Bouquet Sweet Dreams Bouquet Sweet Splendor Bouquet Tulip Bouquet	1730
12.130.60.5	Birthday Bouquet Cake Serving Set Chocolate Dreams Confections Day Spa Certificate Dozen Red Roses Greetings Fruit Basket Mixed Rose Bouquet Sweet Dreams Bouquet Sweet Splendor Bouquet Tulip Bouquet	1860

# 주요 명령어 : REGEX 예제(1)

- Regex : 특정패턴 검색
- 문제 : 최근 15분 동안 특정패턴 = (^1\d{2}\.)을 보이는 고객의 방문 수를 고객 IP별로 나타내세요.
- 답 : 

```
sourcetype=access_combined  
action=purchase  
| regex clientip="^1\d{2}\."  
| stats count by clientip
```

새로운 검색

sourcetype=access\_combined action=purchase | regex clientip="^1\d{2}\." | stats count by clientip

최근 15분

252 이벤트 (14/07/23 14:08:43.000 ~ 14/07/23 14:23:43.000)

이벤트 (252) 통계 (13) 시각화

페이지당 20개 형식 미리보기

clientip	count
125.17.14.100	56
128.241.220.82	40
130.253.37.97	32
131.178.233.243	44
141.146.8.66	48
142.162.221.28	2
193.33.170.23	6
194.146.236.22	6
194.215.205.19	4
194.8.74.23	6
195.69.160.22	2
195.69.252.22	4
195.80.144.22	2

더 많은 정보를 원하시면 아래의 링크를 따라가주세요.  
<http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Rex>

# 주요 명령어 : REGEX 예제(2)

- 문제 : 수집된 데이터에서 정규식으로 필드 추출( Raw 데이터의 clientip 를 SRC\_IP로 추출)
- 답 : `sourcetype=access_combined | rex field=_raw "(?<SRC_IP>\d+\.\d+\.\d+\.\d+)"`

새로운 검색

sourcetype=access\_combined | rex field=\_raw "(?<SRC\_IP>\d+\.\d+\.\d+\.\d+)"

21,605 / 21,850 이벤트 일치함

이벤트 (21,605) 통계 시각

시간 표시줄 형식 지정 - 축소

선택된 필드

- host 3
- source 2
- sourcetype 1
- SRC\_IP 67

관심 있는 필드

- action 5
- bytes 100+
- category\_id 5
- clientip 67
- date\_hour 2

SRC\_IP

67 값, 100% 이벤트

보고서

상위 값 시간별 상위 값 희귀 값

이 필드가 있는 이벤트

상위 10개 값	개수	%
125.17.14.100	1,857	8.595%
128.241.220.82	1,838	8.507%
12.130.60.4	1,813	8.392%
12.130.60.5	1,790	8.285%
141.146.8.66	1,776	8.22%
131.178.233.243	1,773	8.206%
130.253.37.97	1,676	7.757%
10.2.1.44	791	3.661%
194.146.236.22	174	0.805%
84.34.159.23	164	0.759%



# 주요 명령어 : STRCAT(1)

- STRCAT : 문자열 값을 연결합니다.
- 문제 : clientip 와 host의 값을 "/" 구분으로 COMBO라는 필드를 생성
- 답 : 

```
sourcetype=access_combined  
| stats count by clientip, host  
| strcat clientip "/" host COMBO
```

새로운 검색

sourcetype=access\_combined | stats count by clientip, host | strcat clientip "/" host COMBO

✓ 5,395 이벤트 (14/07/23 14:31:08.000 ~ 14/07/23 14:46:08.000)

이벤트 (5,395) 통계 (200) 시각화

페이지당 20개 ▾ 형식 ▾ 미리보기 ▾

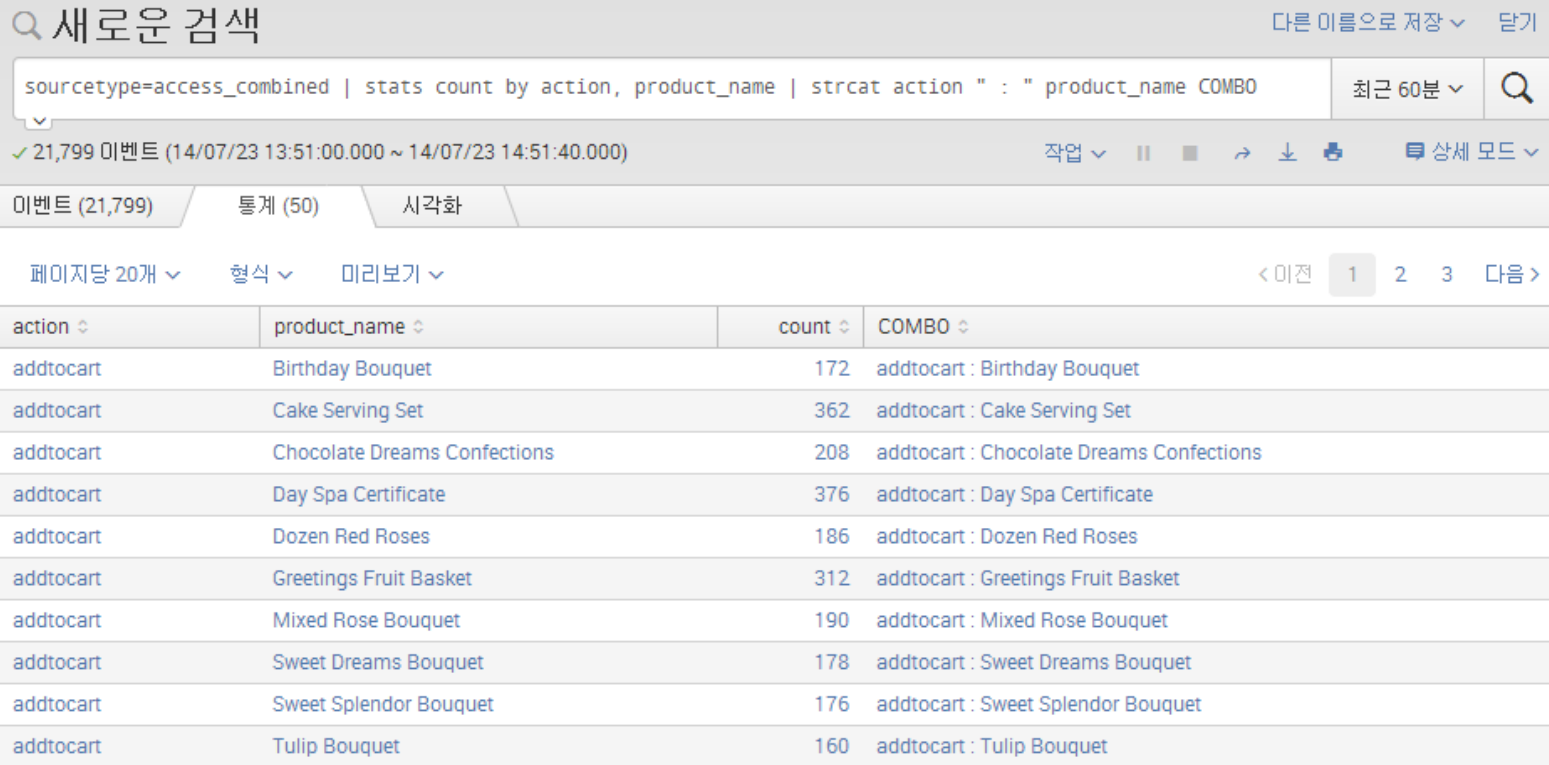
clientip	host	count	COMBO
1.16.0.0	apache-1.splunk.com	10	1.16.0.0/apache-1.splunk.com
1.16.0.0	apache-2.splunk.com	4	1.16.0.0/apache-2.splunk.com
1.16.0.0	apache-3.splunk.com	14	1.16.0.0/apache-3.splunk.com
1.19.11.11	apache-1.splunk.com	10	1.19.11.11/apache-1.splunk.com
1.19.11.11	apache-2.splunk.com	12	1.19.11.11/apache-2.splunk.com
1.19.11.11	apache-3.splunk.com	18	1.19.11.11/apache-3.splunk.com
10.2.1.44	apache-1.splunk.com	67	10.2.1.44/apache-1.splunk.com
10.2.1.44	apache-2.splunk.com	74	10.2.1.44/apache-2.splunk.com
10.2.1.44	apache-3.splunk.com	64	10.2.1.44/apache-3.splunk.com
12.130.60.4	apache-1.splunk.com	172	12.130.60.4/apache-1.splunk.com
12.130.60.4	apache-2.splunk.com	160	12.130.60.4/apache-2.splunk.com
12.130.60.4	apache-3.splunk.com	170	12.130.60.4/apache-3.splunk.com
12.130.60.5	apache-1.splunk.com	176	12.130.60.5/apache-1.splunk.com
12.130.60.5	apache-2.splunk.com	151	12.130.60.5/apache-2.splunk.com

더 많은 정보를 원하시면 아래의 링크를 따라가주세요.

<http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Strcat>

# 주요 명령어 : STRCAT(2)

- 문제 : action의 내용과 product\_name 을 ":" 로 연결하세요.
- 답 : sourcetype=access\_combined | stats count by action, product\_name | strcat action " : " product\_name COMBO



새로운 검색

sourcetype=access\_combined | stats count by action, product\_name | strcat action " : " product\_name COMBO

✓ 21,799 이벤트 (14/07/23 13:51:00.000 ~ 14/07/23 14:51:40.000)

이벤트 (21,799) | 통계 (50) | 시각화

페이지당 20개 | 형식 | 미리보기

action	product_name	count	COMBO
addtocart	Birthday Bouquet	172	addtocart : Birthday Bouquet
addtocart	Cake Serving Set	362	addtocart : Cake Serving Set
addtocart	Chocolate Dreams Confections	208	addtocart : Chocolate Dreams Confections
addtocart	Day Spa Certificate	376	addtocart : Day Spa Certificate
addtocart	Dozen Red Roses	186	addtocart : Dozen Red Roses
addtocart	Greetings Fruit Basket	312	addtocart : Greetings Fruit Basket
addtocart	Mixed Rose Bouquet	190	addtocart : Mixed Rose Bouquet
addtocart	Sweet Dreams Bouquet	178	addtocart : Sweet Dreams Bouquet
addtocart	Sweet Splendor Bouquet	176	addtocart : Sweet Splendor Bouquet
addtocart	Tulip Bouquet	160	addtocart : Tulip Bouquet

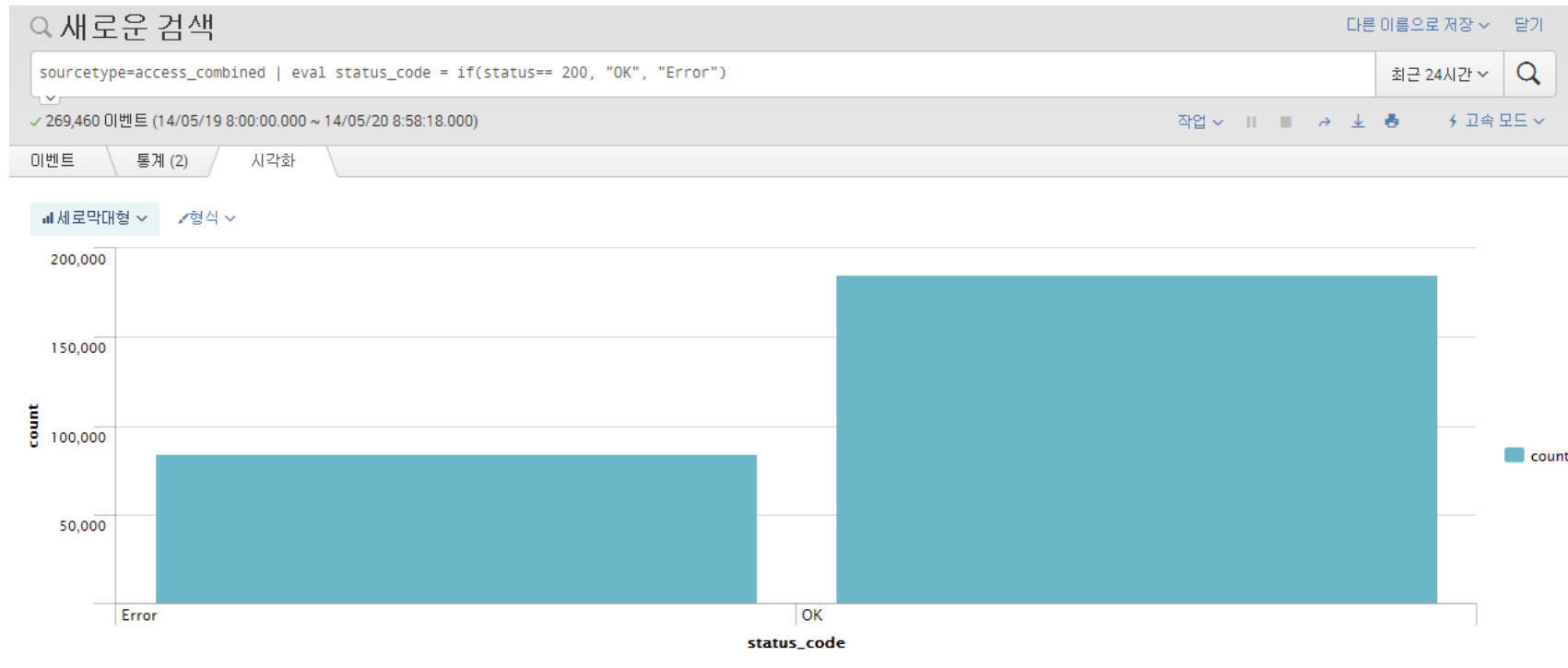
# 주요 명령어 : STRCAT(3)

- 문제 : 최근 24시간 동안 이벤트에서 관심 물품의 대한 접속 자 수, 총 금액을 하나의 Value로 표현해보세요.

이벤트 (43,477)    통계 (10)    시각화			
페이지당 20개 ▼    형식 ▼    미리보기 ▼			
product_name ↕	count ↕	sum(price) ↕	COMBO ↕
Birthday Bouquet	2699	807001	Birthday Bouquet : 2699( \$807001 )
Cake Serving Set	5568	495552	Cake Serving Set : 5568( \$495552 )
Chocolate Dreams Confections	2851	1080529	Chocolate Dreams Confections : 2851( \$1080529 )
Day Spa Certificate	5561	194635	Day Spa Certificate : 5561( \$194635 )
Dozen Red Roses	2895	286605	Dozen Red Roses : 2895( \$286605 )
Greetings Fruit Basket	5577	66924	Greetings Fruit Basket : 5577( \$66924 )
Mixed Rose Bouquet	2784	41760	Mixed Rose Bouquet : 2784( \$41760 )
Sweet Dreams Bouquet	2841	252849	Sweet Dreams Bouquet : 2841( \$252849 )
Sweet Splendor Bouquet	2718	133182	Sweet Splendor Bouquet : 2718( \$133182 )
Tulip Bouquet	2844	711000	Tulip Bouquet : 2844( \$711000 )

# 주요 명령어 : EVAL – IF(1)

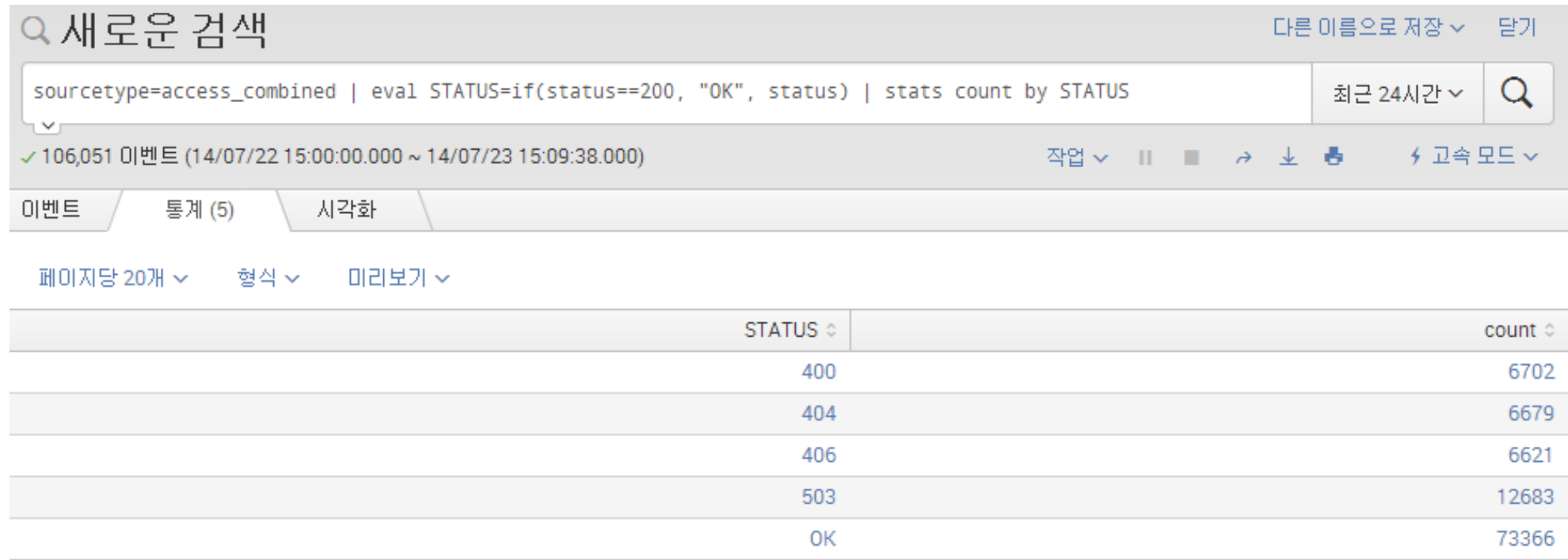
- 문제 : eval\_status\_code 라는 가상의 Field를 생성 하여, status 값이 200이면 "OK" 200이 아니면 "Error"로 표시하세요.
- 답 : `sourcetype=access_combined | eval status_code = if(status== 200, "OK", "Error") | stats count by status`



더 많은 정보를 원하시면 링크를 따라가주세요. <http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Eval>

# 주요 명령어 : EVAL – IF(2)

- 문제 : STATUS가 200이면 "OK"로 필드를 변경 변경
- 답 : `sourcetype=access_combined | eval STATUS=if(status==200, "OK", status)`  
| stats count by STATUS



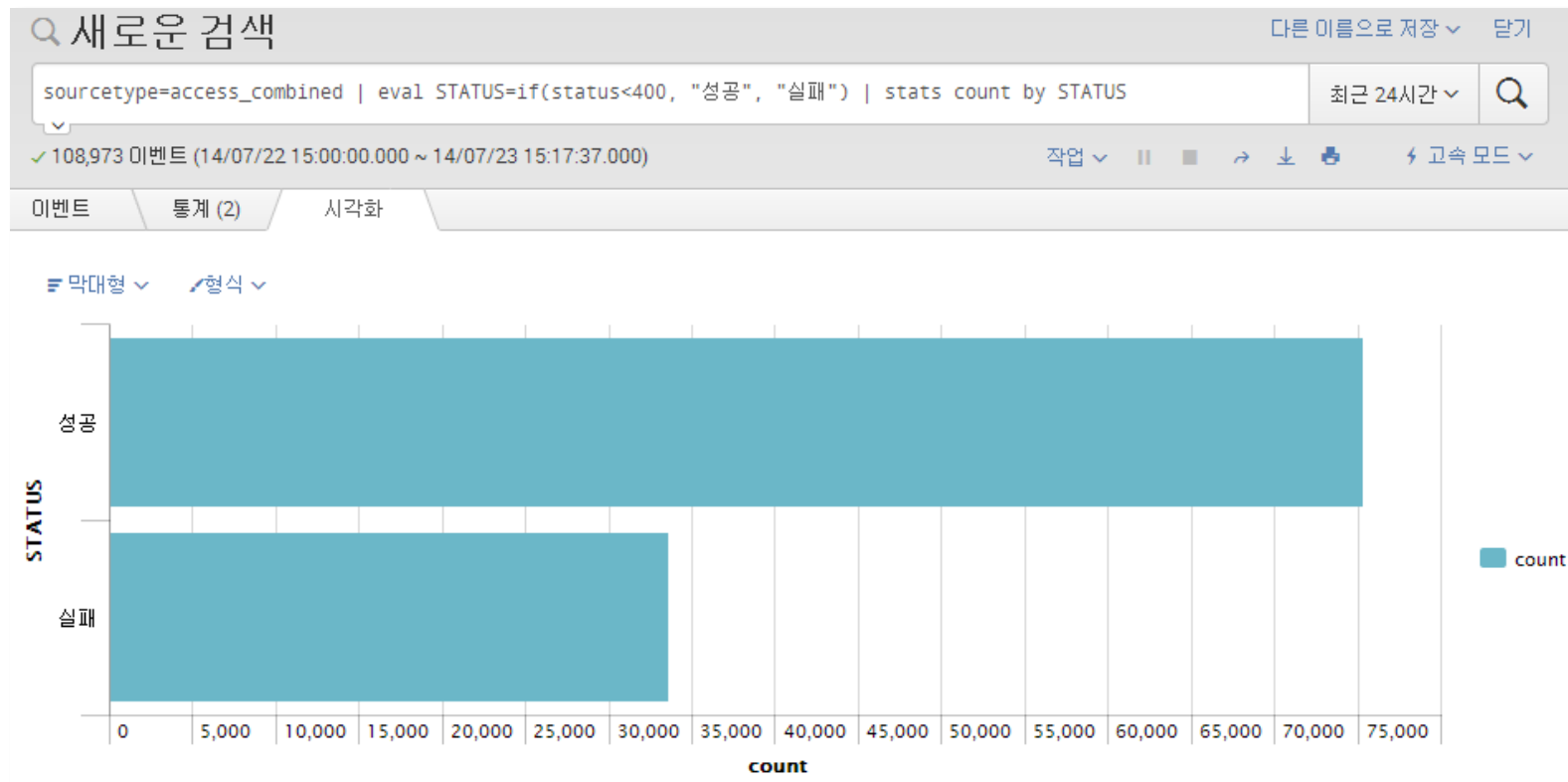
The screenshot shows the Splunk search interface. The search bar contains the query: `sourcetype=access_combined | eval STATUS=if(status==200, "OK", status) | stats count by STATUS`. The results show 106,051 events from 14/07/22 15:00:00.000 to 14/07/23 15:09:38.000. The table below displays the results of the stats command.

STATUS	count
400	6702
404	6679
406	6621
503	12683
OK	73366

# 주요 명령어 : EVAL-IF(3)

➤ 문제 : Status가 400 이하이면 성공, 이상이면 실패로 status의 통계를 구하여 막대형 차트로 표현하세요.

➤ 답 : `sourcetype=access_combined | eval STATUS=if(status<400, "성공", "실패") | stats count by STATUS`



# 주요 명령어 : EVAL – CASE

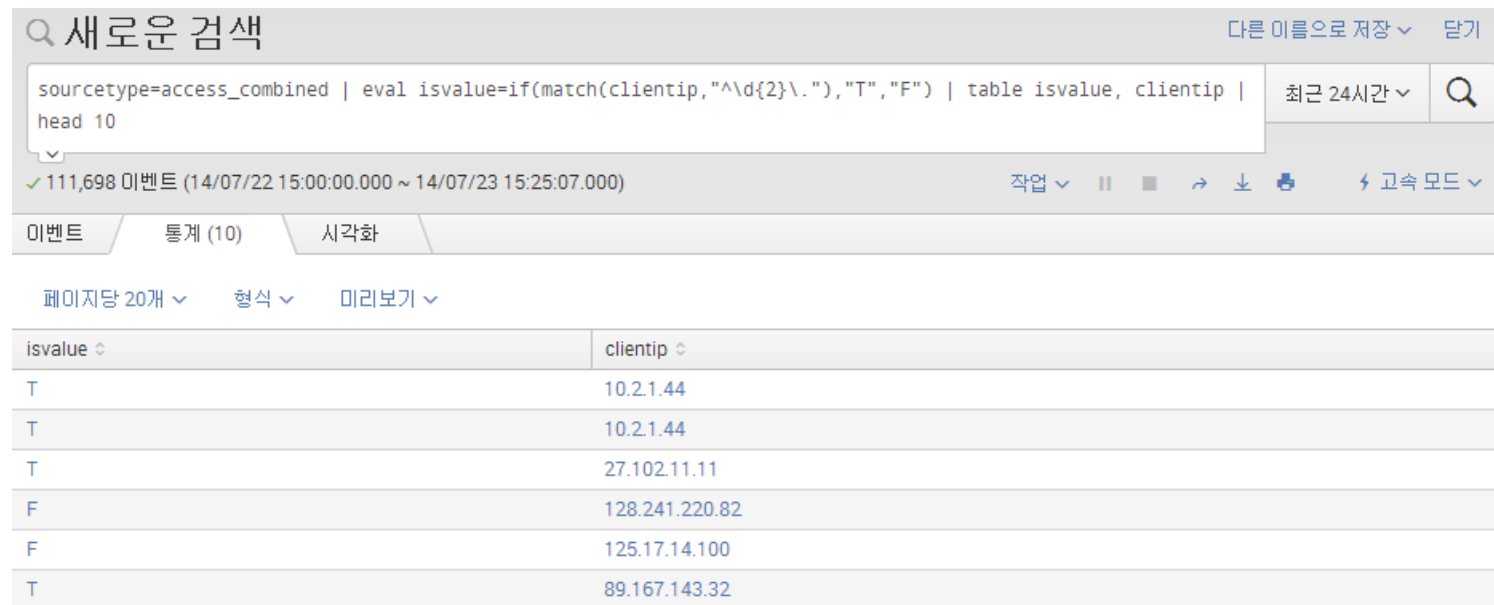
- 문제 : 최근 24시간 동안 status가 400 이하이면 “성공”, status가 400보다 크거나 같으면 “에러”로 status의 통계를 구하여 막대형 차트로 표현하세요.
- 답 : `sourcetype=access_combined | eval STATUS=case(status<400, "성공", status>=400,"에러") | stats count by STATUS`

The screenshot shows the Splunk search interface. At the top, there's a search bar with the query: `sourcetype=access_combined | eval STATUS=case(status<400, "성공", status>=400,"에러") | stats count by STATUS`. Below the search bar, it indicates 110,555 events for the time range 14/07/22 15:00:00.000 ~ 14/07/23 15:22:01.000. The interface has tabs for '이벤트' (Events), '통계 (2)' (Statistics), and '시각화' (Visualizations). The '통계 (2)' tab is selected, showing a table with two columns: 'STATUS' and 'count'. The table contains two rows: '성공' (Success) with a count of 76468, and '에러' (Error) with a count of 34087.

STATUS	count
성공	76468
에러	34087

# 주요 명령어 : EVAL – MATCH

- 문제 : 최근 24시간 동안 접속한 고객아이피의 앞자리가 숫자 두 자리면 “T” 로, 그렇지 않으면 “F”로 표시하세요. 그리고 필드명을 “isvalue”, “clientip”로 하여 table로 나타내세요.
- 답 : `sourcetype=access_combined | eval isvalue=if(match(clientip,"^\d{2}\."),"T","F") | table isvalue, clientip | head 10`



새로운 검색

다른 이름으로 저장 ▼ 닫기

sourcetype=access\_combined | eval isvalue=if(match(clientip,"^\d{2}\."),"T","F") | table isvalue, clientip | head 10

최근 24시간 ▼ 🔍

✓ 111,698 이벤트 (14/07/22 15:00:00.000 ~ 14/07/23 15:25:07.000) 작업 ▼ || ▶ ⬇️ ⬆️ ⚡ 고속 모드 ▼

이벤트 통계 (10) 시각화

페이지당 20개 ▼ 형식 ▼ 미리보기 ▼

isvalue ◊	clientip ◊
T	10.2.1.44
T	10.2.1.44
T	27.102.11.11
F	128.241.220.82
F	125.17.14.100
T	89.167.143.32



# 주요 명령어 : EVAL – strftime

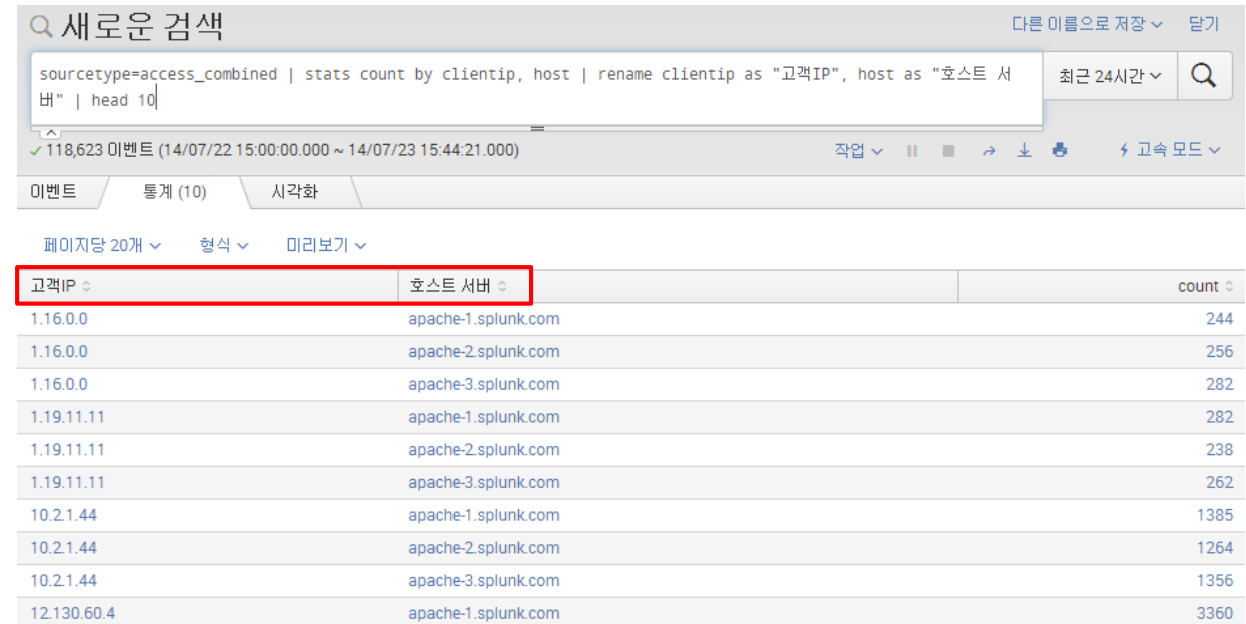
➤ 시간 형태를 바꾸어 나타내기

➤ `sourcetype=access_combined | eval TIME=strftime(_time, "%Y년%m월%d일 %H:%M:%S") | table _time, TIME | head 10`

_time ↕	TIME ↕
2014/07/23 14:39:03	2014년07월23일 14:39:03
2014/07/23 14:02:35	2014년07월23일 14:02:35
2014/07/23 15:37:28	2014년07월23일 15:37:28
2014/07/23 15:37:27	2014년07월23일 15:37:27
2014/07/23 15:37:28	2014년07월23일 15:37:28
2014/07/23 15:37:28	2014년07월23일 15:37:28
2014/07/23 15:37:26	2014년07월23일 15:37:26
2014/07/23 15:37:29	2014년07월23일 15:37:29
2014/07/23 15:37:29	2014년07월23일 15:37:29
2014/07/23 15:37:29	2014년07월23일 15:37:29

# 주요 명령어 : RENAME(1)

- RENAME : 지정된 필드의 이름을 변경합니다. 필드를 여러 개 지정할 경우 와일드카드(\*)를 사용할 수 있습니다.
- 문제 : 최근 24시간 동안 접속한 고객 아이피와 호스트의 필드 명을 “고객IP”, “호스트 서버” 로 변경하여 테이블 형태로 나타내세요.
- 답 : `sourcetype=access_combined | stats count by clientip, host | rename clientip as "고객IP", host as "호스트 서버"`



The screenshot shows the Splunk search interface. The search bar contains the query: `sourcetype=access_combined | stats count by clientip, host | rename clientip as "고객IP", host as "호스트 서버" | head 10`. The results are displayed in a table with columns: 고객IP, 호스트 서버, and count. The table shows 10 rows of data, with the first row highlighted in red.

고객IP	호스트 서버	count
1.16.0.0	apache-1.splunk.com	244
1.16.0.0	apache-2.splunk.com	256
1.16.0.0	apache-3.splunk.com	282
1.19.11.11	apache-1.splunk.com	282
1.19.11.11	apache-2.splunk.com	238
1.19.11.11	apache-3.splunk.com	262
10.2.1.44	apache-1.splunk.com	1385
10.2.1.44	apache-2.splunk.com	1264
10.2.1.44	apache-3.splunk.com	1356
12.130.60.4	apache-1.splunk.com	3360

더 많은 정보를 원하시면 링크를 따라가주세요. <http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Rename>

# 주요 명령어 : RENAME(2)

- `sourcetype=access_combined | eval TYPE=if(date_hour>=7 ,if(date_hour<=20, "S","M"),"M") | stats count, count(eval(match(TYPE,"S"))) as Sun, count(eval(match(TYPE,"M"))) as Moon by action | rename Sun as "독수리", Moon as "올빼미"`

새로운 검색 다른 이름으로 저장 달기

`sourcetype=access_combined | eval TYPE=if(date_hour>=7 ,if(date_hour<=20, "S","M"),"M") | stats count, count(eval(match(TYPE,"S"))) as Sun, count(eval(match(TYPE,"M"))) as Moon by action | rename Sun as "독수리", Moon as "올빼미"` 최근 24시간 🔍

✓ 122,994 이벤트 (14/07/22 15:00:00.000 ~ 14/07/23 15:56:47.000) 작업 ⏏ 🔄 ⬇ 🖨 ⚡ 고속 모드

이벤트 / 통계 (5) / 시각화

페이지당 20개 ↓ 형식 ↓ 미리보기 ↓

action <span>↕</span>	count <span>↕</span>	독수리 <span>↕</span>	올빼미 <span>↕</span>
addtocart	12676	858	11818
changequantity	12766	890	11876
purchase	12596	826	11770
remove	12481	878	11603
view	12457	871	11586

## 주요 명령어 : REPLACE(1)

- 문제 : 최근 24시간 동안 action 별 count를 구하고 addtocart -> "장바구니"로 changequantity -> "수량 변경"으로 purchase -> "구매" 로 필드명을 변경하세요.
- 답 : `sourcetype=access_combined | stats count by action | replace addtocart with "장바구니", changequantity with "수량 변경", purchase with "구매"`

**새로운 검색** 다른 이름으로 저장 ▼ 닫기

```
sourcetype=access_combined | stats count by action | replace addtocart with "장바구니", changequantity with "수량 변경", purchase with "구매"
```

최근 24시간 ▼ 🔍

✓ 127,216 이벤트 (14/07/22 16:00:00.000 ~ 14/07/23 16:08:20.000) 작업 ▼ || ■ ➡ ⬇ 🖨 ⚡ 고속 모드 ▼

이벤트 / 통계 (5) / 시각화

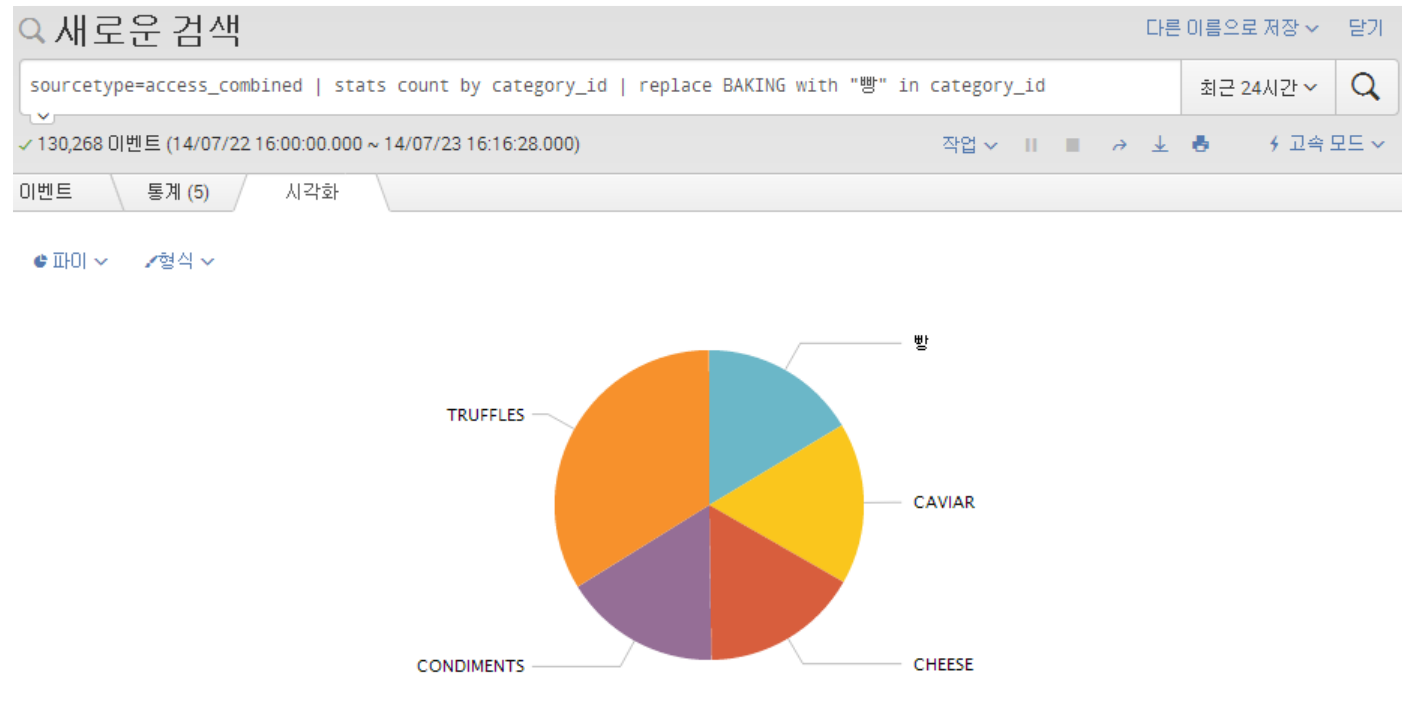
페이지당 20개 ▼ 형식 ▼ 미리보기 ▼

action ↕	count ↕
장바구니	13098
수량 변경	13184
구매	13088
remove	12908
view	12893

더 많은 정보를 원하시면 링크를 따라가주세요. <http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Replace>

# 주요 명령어 : REPLACE(2)

- 문제 : 최근 24시간 동안 category\_id 별 count를 구하고 BAKING->"빵"로 필드명을 변경한 후 파이차트로 나타내세요.
- 답 : `sourcetype=access_combined | stats count by category_id`  
`| replace BAKING with "빵" in category_id`



# 주요 명령어 : SORT(1)

- SORT: 지정된 필드를 기준으로 검색 결과를 정렬합니다.
- 문제: 최근 60분 동안 clientip 별 count를 구하고 count의 내림차순으로 정렬하세요.
- 답 : `sourcetype=access_combined | stats count by clientip | sort - count`

이벤트

통계 (67)

시각화

페이지당 20개 ▼

형식 ▼

미리보기 ▼

< 이전

1

2

3

4

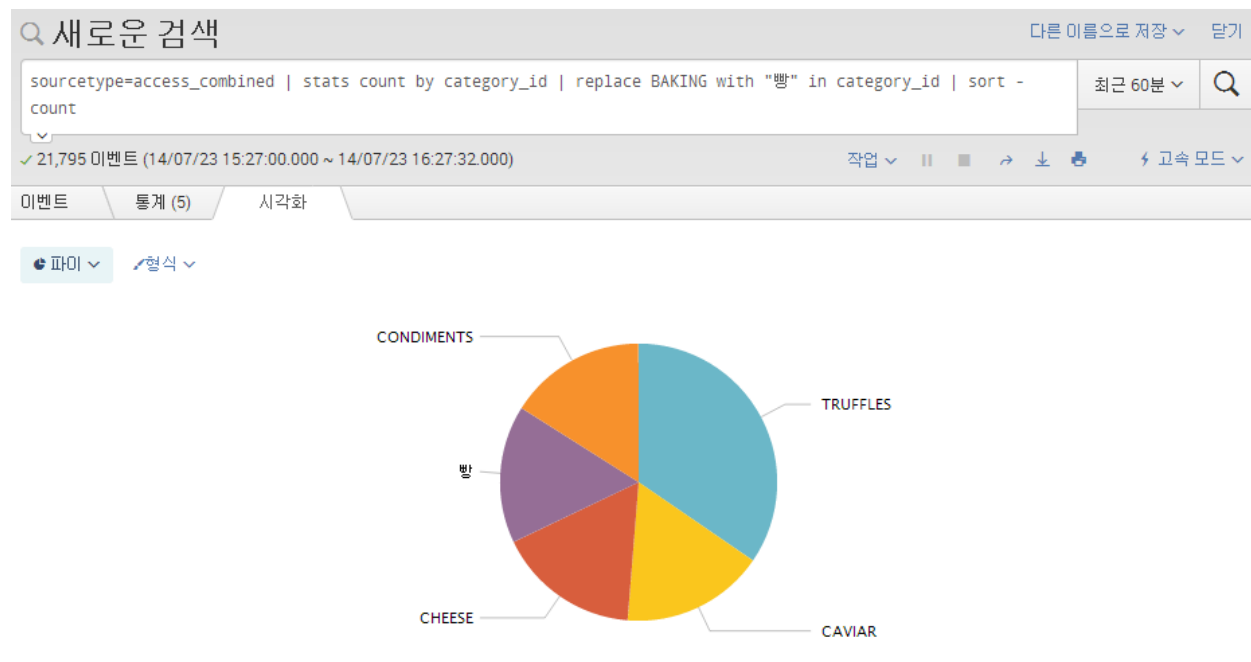
다음 >

clientip ↕	count ↕
12.130.60.5	1908
12.130.60.4	1862
130.253.37.97	1858
141.146.8.66	1824
131.178.233.243	1815
125.17.14.100	1810
128.241.220.82	1759
10.2.1.44	730

더 많은 정보를 원하시면 링크를 따라가주세요. <http://docs.splunk.com/Documentation/Splunk/6.1.1/SearchReference/Sort>

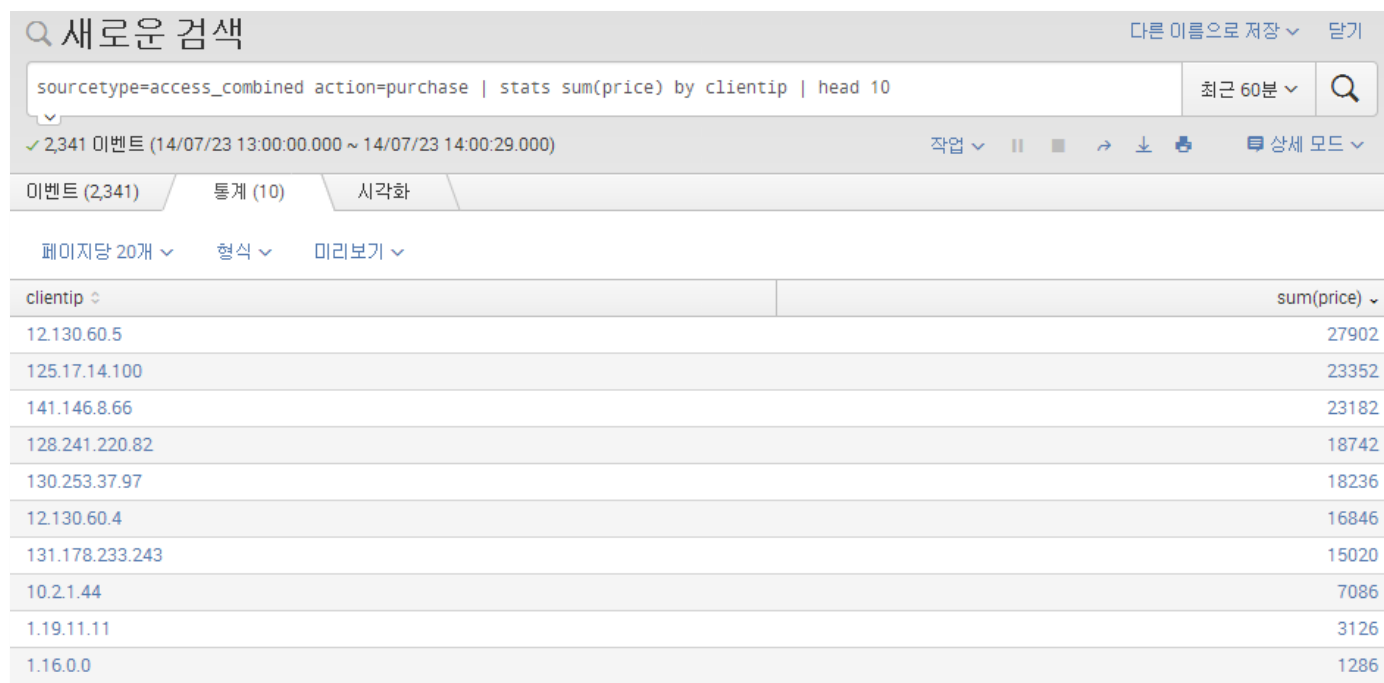
# 주요 명령어 : SORT(2)

- 문제 : 최근 60분 동안 category\_id 별 count를 구하고, BAKING->"빵"으로 변경한 후 count의 내림차순으로 정렬하여 파이차트로 나타내세요.
- 답 : `sourcetype=access_combined | stats count by category_id | replace BAKING with "빵" in category_id | sort - count`



# 주요 명령어 : HEAD

- Head: 지정된 결과의 첫 번째 n개를 반환합니다
- 문제: 최근 60분 동안 고객 IP별 구매 가격의 합을 10개만 나타내세요.
- 답 : `sourcetype=access_combined action=purchase | stats sum(price) by clientip | head 10`



새로운 검색

sourcetype=access\_combined action=purchase | stats sum(price) by clientip | head 10

✓ 2,341 이벤트 (14/07/23 13:00:00.000 ~ 14/07/23 14:00:29.000)

이벤트 (2,341) 통계 (10) 시각화

페이지당 20개 형식 미리보기

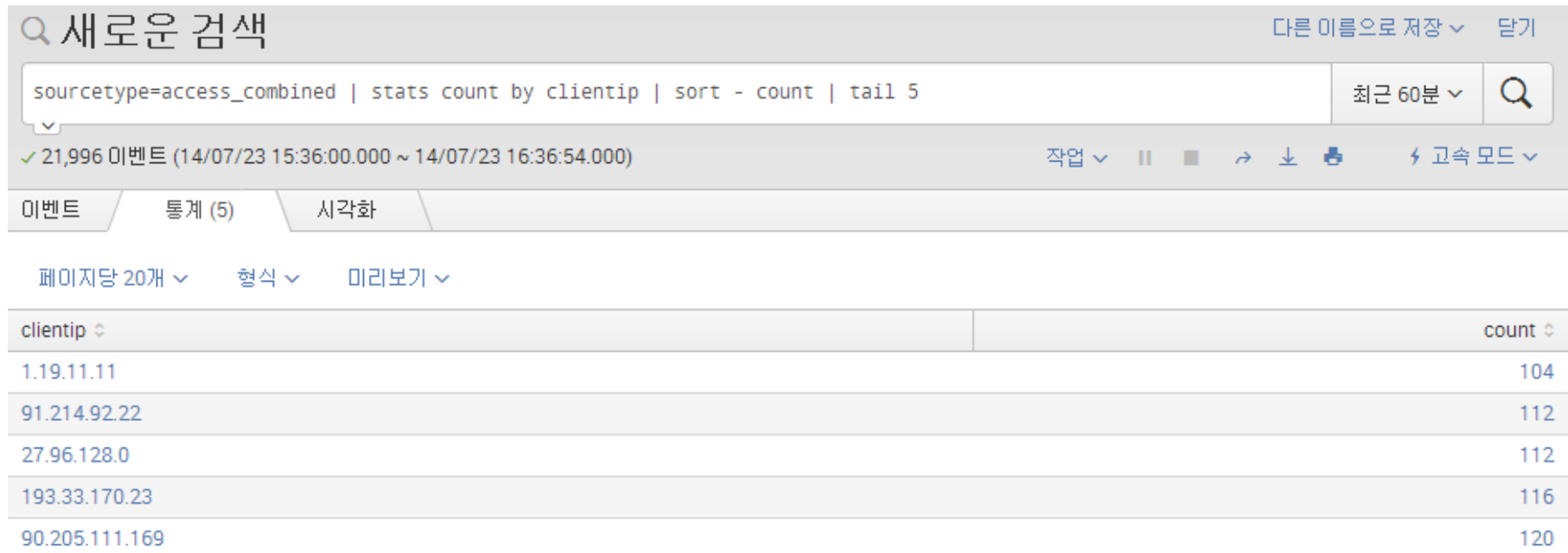
clientip	sum(price)
12.130.60.5	27902
125.17.14.100	23352
141.146.8.66	23182
128.241.220.82	18742
130.253.37.97	18236
12.130.60.4	16846
131.178.233.243	15020
10.2.1.44	7086
1.19.11.11	3126
1.16.0.0	1286

더 많은 정보를 원하시면 링크를 따라가주세요. <http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Head>



# 주요 명령어 : TAIL

- TAIL : 지정된 결과의 마지막 n개를 반환합니다.
- 문제 : 최근 60분 동안 고객 IP별 구매 가격의 합을 count별로 내림차순 한 후 마지막 5개를 반환해 보세요.
- 답 : `sourcetype=access_combined | stats count by clientip | sort - count | tail 5`



새로운 검색

`sourcetype=access_combined | stats count by clientip | sort - count | tail 5`

✓ 21,996 이벤트 (14/07/23 15:36:00.000 ~ 14/07/23 16:36:54.000)

이벤트 | 통계 (5) | 시각화

페이지당 20개 | 형식 | 미리보기

clientip	count
1.19.11.11	104
91.214.92.22	112
27.96.128.0	112
193.33.170.23	116
90.205.111.169	120

# 주요 명령어 : DEDUP

- DEDUP: 지정된 기준과 일치하는 최신 결과를 보여줍니다.
- 문제: 최근 60분 동안 접속한 최신 고객의 정보를 고객IP기준으로 나타내세요.
- 답 : `sourcetype=access_combined | dedup clientip`

The screenshot shows the Splunk search interface. At the top, the search bar contains the query `sourcetype=access_combined | dedup clientip`. Below the search bar, it indicates 67 events for the time range 14/07/23 15:41:00.000 ~ 14/07/23 16:41:35.000. A bar chart shows the event distribution over time. Below the chart, a table displays the search results. The table has columns for index, time, and event. The first result shows a GET request from 201.122.42.235 to /category.screen?category\_id=B... with a status of 200. The source is C:\Program Files\Apache\Logs\access\_combined.log.

i	시간	이벤트
>	14/07/23 16:41:34.146	201.122.42.235 - - [23/Jul/2014 07:41:34:146] "GET /category.screen?category_id=B... AKING&JSESSIONID=SD2SL10FF9ADFF5 HTTP 1.1" 200 1696 "http://shop.gourmet-shop.com /product.screen?product_id=AV-CB-01" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 488 host = apache-2.splunk.com   source = C:\Program Files\Apache\Logs\access_combined.log   sourcetype = access_combined

더 많은 정보를 원하시면 링크를 따라가주세요. <http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Dedup>

# 주요 명령어 : FIELDFORMAT

- Fieldformat: 원복 값은 변경하지 않고 출력시만 지정한 포맷으로 변경합니다.
- 문제: 최근 4시간 동안 카운트를 출력하고 숫자를 comma를 넣어서 출력하세요
- 답 : `sourcetype=access_combined | stats count | fieldformat cnt=tostring(count,"commas")`

The screenshot shows the Splunk search interface. The search bar contains the query: `sourcetype=access_combined | stats count | fieldformat cnt=tostring(count,"commas")`. The results bar indicates 43,237 events for the time range 14/06/18 6:48:00.000 ~ 14/06/18 10:48:13.000. Below the search bar, there are tabs for '이벤트 (43,237)', '통계 (1)', and '시각화'. The '통계 (1)' tab is selected. The results table shows two columns: 'count' and 'cnt'. The 'count' column has the value 43237, and the 'cnt' column has the value 43,237, demonstrating the effect of the fieldformat command.

count	cnt
43237	43,237

# 주요 명령어 : RANGEMAP

- RANGEMAP : 결과값을 일정범위로 구분하여 표현합니다.
- `sourcetype=access_combined action=purchase | stats count by category_id | rangemap field=count green=1-100 blue=100-200 red=200-300 default=gray | stats count by range`

```
sourcetype=access_combined action=purchase | stats count by category_id | rangemap field=count green=1-100  
blue=100-200 red=200-300 default=gray
```

✓ 4,366 이벤트 (14/06/18 7:04:00.000 ~ 14/06/18 11:04:25.000)

이벤트 (4,366) 통계 (5) 시각화

페이지당 20개 ▼ 형식 ▼ 미리보기 ▼

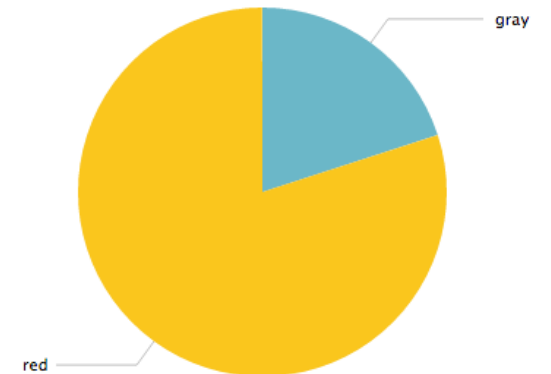
category_id	count	range
BAKING	276	red
CAVIAR	248	red
CHEESE	249	red
CONDIMENTS	263	red
TRUFFLES	553	gray

```
sourcetype=access_combined action=purchase | stats count by category_id | rangemap field=count green=1-100  
blue=100-200 red=200-300 default=gray | stats count by range
```

✓ 4,360 이벤트 (14/06/18 7:02:00.000 ~ 14/06/18 11:02:51.000)

이벤트 (4,360) 통계 (2) 시각화

파이 ▼ 형식 ▼



더 많은 정보를 원하시면 링크를 따라가주세요.

<http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/rangemap>

# 주요 명령어 : IPLOCATION

- IPLOCATION: IP와 일치하는 도시, 나라, 위도, 경도 보여줍니다.
- `sourcetype=access_combined | iplocation clientip | table clientip, City, Country, lat, lon`



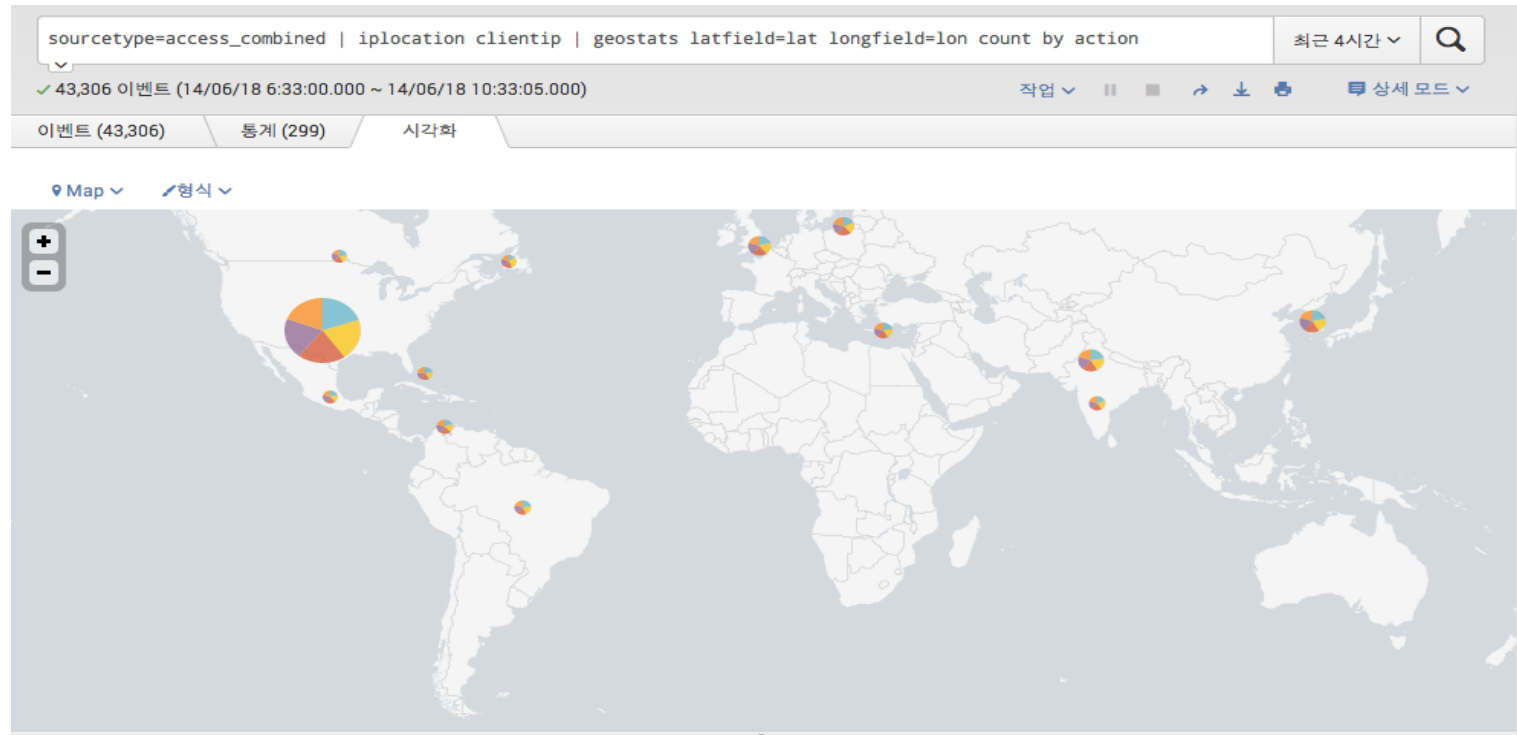
Search Query: `sourcetype=access_combined | head 10 | iplocation clientip | table clientip, City, Country, lat, lon`

Results: 10 이벤트 (14/06/18 6:31:00.000 ~ 14/06/18 10:31:05.000)

clientip	City	Country	lat	lon
12.130.60.4		United States	38.00000	-97.00000
128.241.220.82	Englewood	United States	39.62370	-104.87380
141.146.8.66	Austin	United States	30.26720	-97.74310
201.3.120.132		Brazil	-10.00000	-55.00000
131.178.233.243	Monterrey	Mexico	25.66670	-100.31670
128.241.220.82	Englewood	United States	39.62370	-104.87380
131.178.233.243	Monterrey	Mexico	25.66670	-100.31670
92.1.170.135		United Kingdom	51.50000	-0.13000
81.11.191.113	Vilvoorde	Belgium	50.93330	4.43330
128.241.220.82	Englewood	United States	39.62370	-104.87380

# 주요 명령어 : GEOSTATS

- GEOSTATS: 지정된 기준과 일치하는 결과 구글맵상에 통계를 보여줍니다.  
... | geostats latfield=위도좌표 longfield=경도좌표 function by groupby\_name
- sourcetype=access\_combined | iplocation clientip | geostats latfield=lat longfield=lon  
count by action



더 많은 정보를 원하시면 링크를 따라가주세요.

<http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Geostats>

# 주요 명령어 : OVERLAY CHART

- 동일 차트에 두 개의 값을 표현합니다.
- `sourcetype=access_combined | iplocation clientip | stats count, dc(clientip) as dcip by Country`

