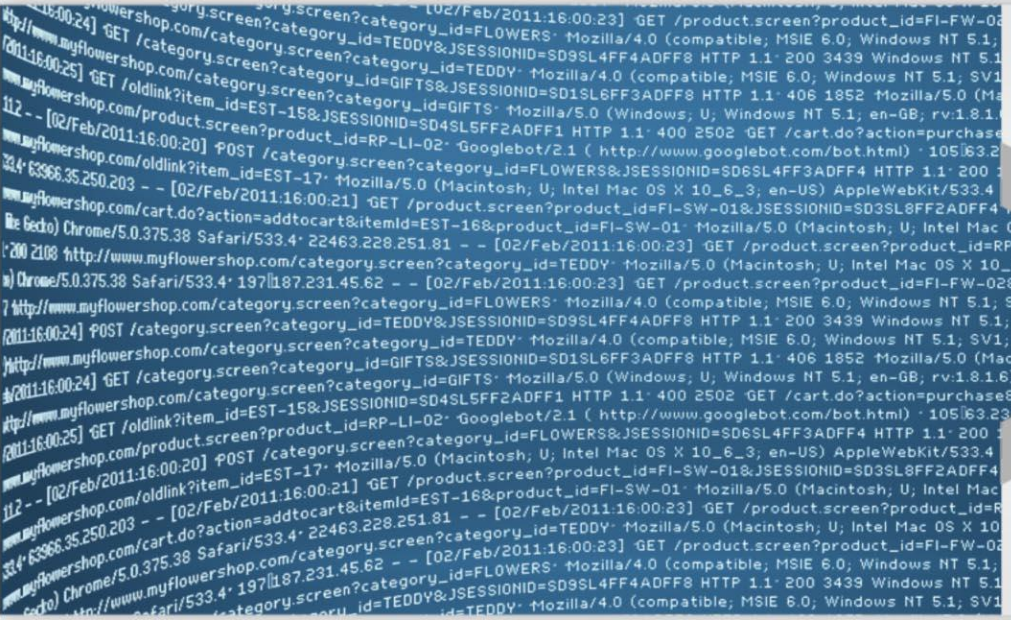
splunk> MOS



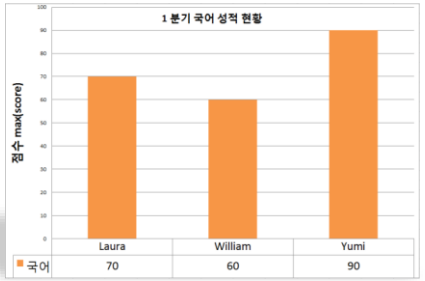
분석의 기초

splunk>

분석 기법 유형 개요

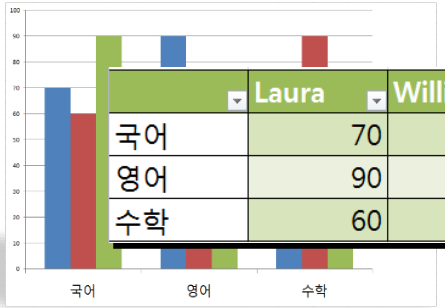
1. Distribution 분석 : stats

- 분석 대상의 비교 분석 (예 : 학생들간의 성적 비교)



2. Matrix 분석 : chart

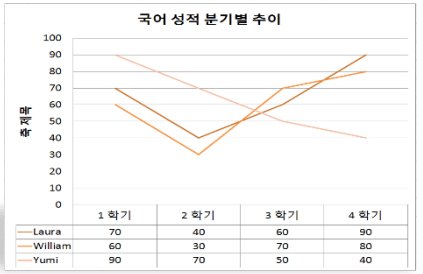
- 분석 대상의 다중 비교 분석 (예 : 학생들간의 국영수 성적 비교, pivot Chart)



	Laura	William	Yumi
국어	70	60	90
영어	90	70	40
수학	60	90	60

3. 3D Matrix 추이 분석 : timechart

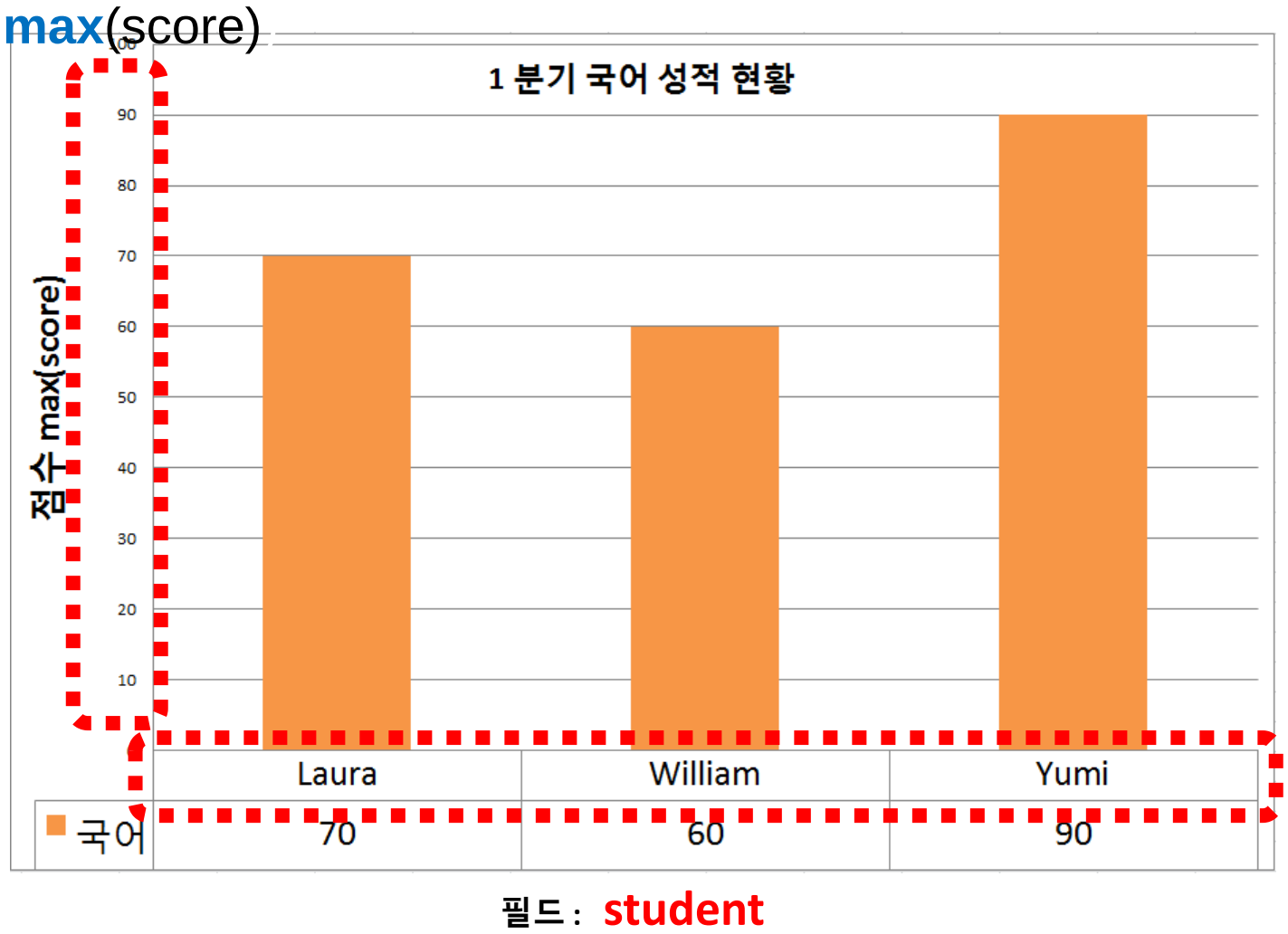
- 분석 대상의 시간적 추이 분석 (예 : 학생들의 국어 성적 시간적, 분기별 성적 추이 비교



분석 기법 1 : Distribution 분석

- ✓ **stats** 명령어 사용
- ✓ 2D Distribution 분석
- ✓ 목적 : 대상 A, B, C를 특정 function의 결과로 비교.

stats max(score) by student



분석 기법 1 : Distribution 분석

- 구조 :

stats func(field), func(field), func(field) **by** field, field, field

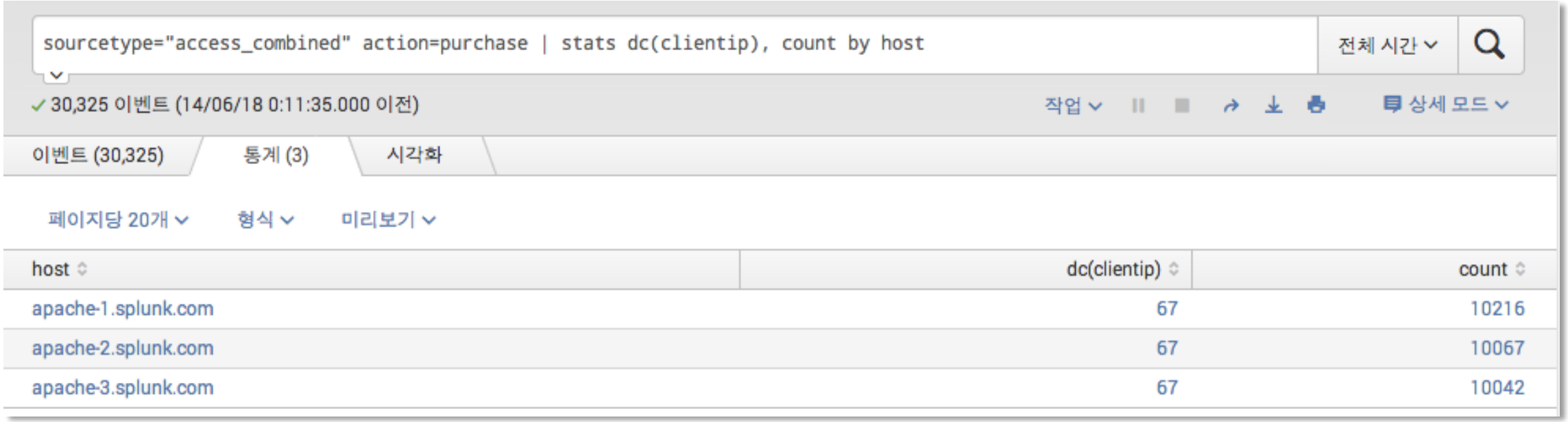
```
* | stats count
* | stats count by host
* | stats  sum(price), list(product_name) by  user_name
```

분석 적용 함수, 통계 stats Functions

FUNCTION	DESCRIPTION
avg(X)	Returns the average of the values of field X.
count(X)	Returns the number of occurrences of the field X. To indicate a specific field value to match, format X as eval(field="value").
dc(X)	Returns the count of distinct values of the field X.
first(X)	Returns the first seen value of the field X. In general, the first seen value of the field is the chronologically most recent instance of field.
last(X)	Returns the last seen value of the field X.
list(X)	Returns the list of all values of the field X as a multi-value entry. The order of the values reflects the order of input events.
max(X)	Returns the maximum value of the field X. If the values of X are non-numeric, the max is found from lexicographic ordering.
median(X)	Returns the middle-most value of the field X.
min(X)	Returns the minimum value of the field X. If the values of X are non-numeric, the min is found from lexicographic ordering.
mode(X)	Returns the most frequent value of the field X.
perc<X>(Y)	Returns the X-th percentile value of the field Y. For example, perc5(total) returns the 5th percentile value of a field "total".
range(X)	Returns the difference between the max and min values of the field X.
stdev(X)	Returns the sample standard deviation of the field X.
stdevp(X)	Returns the population standard deviation of the field X.
sum(X)	Returns the sum of the values of the field X.
sumsq(X)	Returns the sum of the squares of the values of the field X.
values(X)	Returns the list of all distinct values of the field X as a multi-value entry. The order of the values is lexicographical.
var(X)	Returns the sample variance of the field X.

stats 명령어 예제

- 문제 : 구매 고객 중 서버(host)별 access수와 접속자 수의 통계
- 답 : sourcetype=access_combined action=purchase | stats dc(clientip), count by host



host	dc(clientip)	count
apache-1.splunk.com	67	10216
apache-2.splunk.com	67	10067
apache-3.splunk.com	67	10042

분석 기법 2 : Matrix 분석

- ✓ **chart** 명령어 사용
- ✓ Matrix 분석, pivot 차트
- ✓ 목적 : 대상 A, B, C를 다중 Object에 대한 function의 결과로 비교

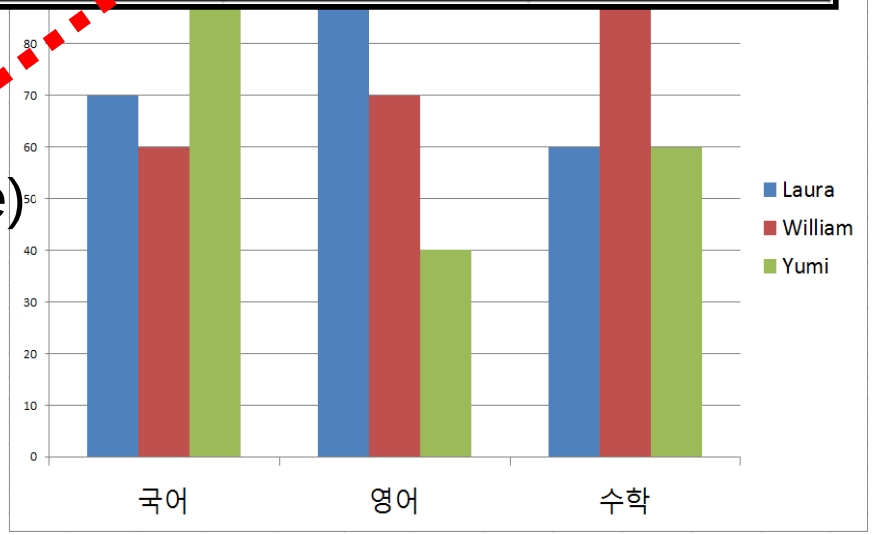
chart max(score) **over** subject **by** student

필드 : **student**

필드 : **subject**

	Laura	William	Yumi
국어	70	60	90
영어	90	70	40
수학	60	90	60

max(score)



분석 기법 2 : Matrix 분석

➢ 구조 :

chart func(field) **over** field **by** field

```
* | chart count over user_name by user_add
```

필드 : **student**

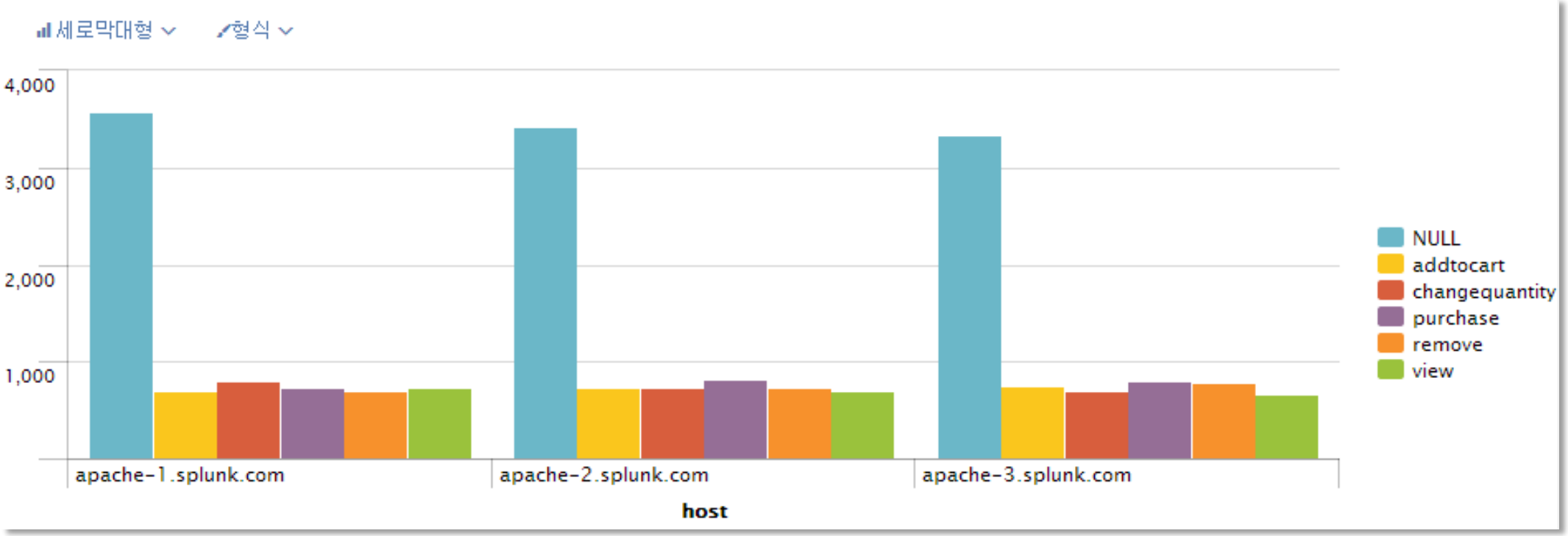
필드 : **subject**

	Laura	William	Yumi
국어	70	60	90
영어	90	70	40
수학	60	90	60

max(score)

Chart 예제

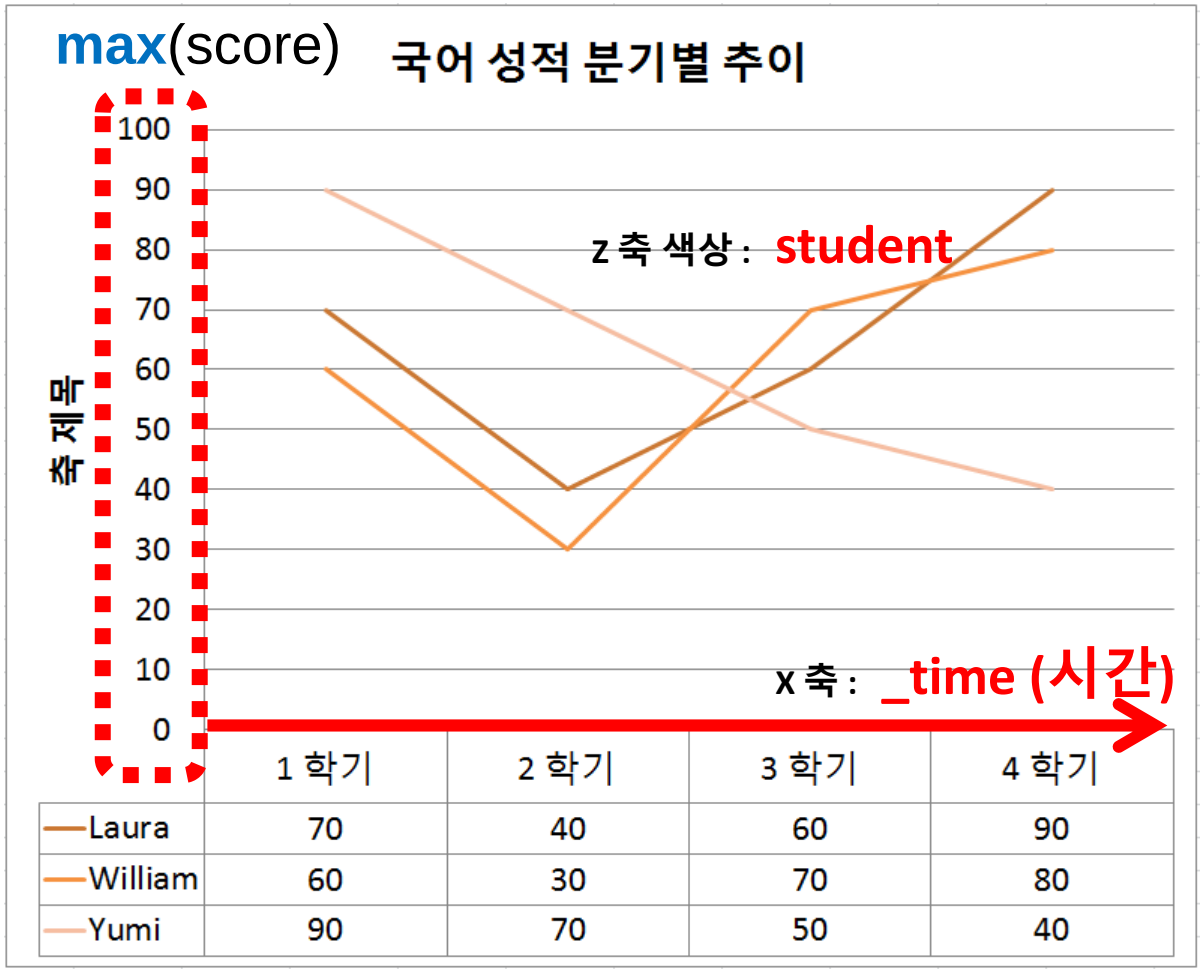
- 문제 : sourcetype=access_combined 에서 각 action 별 host 값을 count 하여 chart 로 표현 하세요.
- 답 : sourcetype=access_combined | chart count over host by action



분석 기법 3 : 3D Matrix 추이 분석

- ✓ **timechart** 명령어 사용
- ✓ 3D Matrix 추이 분석
- ✓ 목적 : 대상 A, B, C의 변화 추이를 function의 결과로 분석

timechart max(score) by student



	1 학기	2 학기	3 학기	4 학기
Laura	70	40	60	90
William	60	30	70	80
Yumi	90	70	50	40

분석 기법 3 : 3D Matrix 추이 분석

- 구조 : **timechart** func(field), func(field), func(field) **by** field

```
* | timechart count by host
```

```
* | timechart sum(price) by user_name
```

```
* | timechart sum(price), dc(product_name) by user_name
```

```
*| timechart count(eval(method="GET")) as GET,
count(eval(method="POST")) as POST by host
```

3D Matrix 추이 분석

- 문제 : sourcetype=access_combined 에서 10 분 단위로 제품별 구매 수를 카운트 하세요.

- 답 : sourcetype=access_combined | chart count over host by action

새로운 검색

다른 이름으로 저장 닫기

```
sourcetype=access_combined action=purchase | timechart span=10m count by product_name
```

최근 60분

✓ 2,372 이벤트 (14/07/23 12:29:00.000 ~ 14/07/23 13:29:46.000)

작업 상세 모드

이벤트 (2,372) 통계 (7) 시각화

페이지당 20개 형식 미리보기

_time	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
2014/07/23 12:20:00	8	4	4	10	2	12	0	6	0	2
2014/07/23 12:30:00	30	54	26	48	32	46	34	30	22	27
2014/07/23 12:40:00	26	48	24	52	34	64	38	22	34	20
2014/07/23 12:50:00	14	68	34	58	40	70	18	26	28	46
2014/07/23 13:00:00	38	68	28	40	28	70	34	24	30	22
2014/07/23 13:10:00	26	94	32	50	40	68	34	60	28	22
2014/07/23 13:20:00	36	50	18	78	33	56	34	24	30	16