1. Enter a search that returns all web application events that include a purchase action with a web status of 200

```
index=test sourcetype=access_combined_wcookie action=purchase status=200
```

2. Enter a search that returns all web application events that include a purchase action where product ID is WC-SH-G04

```
index=test sourcetype=access_combined_wcookie action=purchase productId=WC-SH-G04
```

3. case 3:The team is only looking for successful purchases, so change your search to only return those.

```
index=test sourcetype=access_combined_wcookie action=purchase status=200 file=success.do
```

4. The team is only looking for unsuccessful purchases, so change your search to only return those.

```
index=test sourcetype=access_combined_wcookie action=purchase status=200 file=error.do
```

5. Status not equal to 200 and got error

```
index=test sourcetype=access_combined_wcookie action=purchase status!=200 file="error.do"
```

6. You will see fields that do not matter to the team. Use the fields command to only return the action, JSESSIONID and status fields. Does your search run faster using the command?

Ans:
```
index=test sourcetype=access_combined_wcookie action=purchase status=200 file=success.do |
fields action, JSESSIONID, status
```

7. Now tell the difference:

```
index=test sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | fields -
action, JSESSIONID, status
```

```
index=test sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | fields-
action, JSESSIONID, status
```

8. Write a query to provide a statistics of the above activity by JSESSIONID

```
index=test sourcetype=access_combined_wcookie | fields action, JSESSIONID, status | stats count by
JSESSIONID
```

9. Write a query to provide a statistics of the products purchased by productId. Use the fields command to only return the action, productid and status fields

```
index=test sourcetype=access_combined_wcookie | fields action, productId, status | stats count by
productId
```

10. Find the statistics of the productid and clientip

```
index=test sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | fields
action, productId, status, clientip | stats count by productId, clientip
```

11. Find the list of clientips who have visited the URL "Buttercupgames.com" and rename the count as events.

```
index=test sourcetype=access_combined_wcookie action=purchase status=200
referer_domain="http://www.buttercupgames.com" | stats count by clientip | rename count as events
| sort –events.
```