# splunk>

## Splunk Fundamentals 1 Lab Exercises

Lab typographical conventions:

[`sourcetype=db_audit`] OR [`cs_mime_type`] indicates either a source type or the name of a field.

| | |
|---|---|
| **NOTE:** | Lab work will be done on your personal computer or virtual machine, no lab environment is provided.  We suggest you **DO NOT** do the lab work on your production environment. |

The lab instructions refer to these source types by the types of data they represent:

| Type | Sourcetype | Fields of interest |
|---|---|---|
| Web Application | `access_combined_wcookie` | `action, bytes, categoryId, clientip, itemId, JSESSIONID, productId, referer, referer_domain, status, useragent, file` |
| Database | `db_audit` | `Command, Duration, Type` |
| Web server | `linux_secure` | `COMMAND, PWD, pid, process` |

## Lab Module 6 – Using Fields in Searches

### Description

In this lab, you will use fields to refine your searches.

### Steps

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

**Scenario**:   Our web server has been experiencing some down time.  The Director of Sales has asked your team to examine how this has affected sales on the website.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

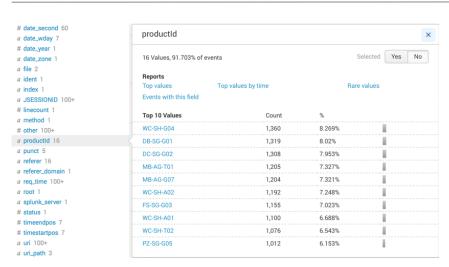**Task 1:   Use the Fields sidebar to examine search results.**

1. In the app navigation bar (i.e., the green bar towards the top of the browser window,) click **Search**.  If you do not see **Search** in the application bar – or to clear the previous search - click the **App: Search & Reporting** in the Splunk bar at the top of the browser window.

2. Search for `index=main sourcetype=access_combined_wcookie action=purchase` for **All time.** This returns all events where a purchase action was taken.

| | |
|---|---|
| **NOTE:** | After the search finalizes, verify that the search executed in Smart Mode. The search mode displays under the time range picker.  If the search did not execute in Smart Mode, change it to Smart Mode, and then re-execute the search. |

3. Examine the Fields sidebar's **Interesting Fields** list. Notice that `productId` is one of the fields extracted by Splunk.

4. In the Fields sidebar, under **Interesting Fields**, click **productId**. Notice the pop-up window shows the top ten purchased products by productId. Close the window by clicking the x in the upper right corner.

*Results Example*

# date_second 60
a date_wday 7
# date_year 1
a date_zone 1
a file 2
a ident 1
a index 1
a JSESSIONID 100+
# linecount 1
a method 1
# other 100+
a productId 16
a punct 5
a referer 16
a referer_domain 1
a req_time 100+
a root 1
a splunk_server 1
# status 1
# timeendpos 7
# timestartpos 7
a uri 100+
a uri_path 3

| productId | | | ✕ |
|---|---|---|---|
| 16 Values, 91.703% of events | | Selected | Yes  No |

**Reports**
Top values          Top values by time                        Rare values
Events with this field

| Top 10 Values | Count | % | |
|---|---|---|---|
| WC-SH-G04 | 1,360 | 8.269% | |
| DB-SG-G01 | 1,319 | 8.02% | |
| DC-SG-G02 | 1,308 | 7.953% | |
| MB-AG-T01 | 1,205 | 7.327% | |
| MB-AG-G07 | 1,204 | 7.321% | |
| WC-SH-A02 | 1,192 | 7.248% | |
| FS-SG-G03 | 1,155 | 7.023% | |
| WC-SH-A01 | 1,100 | 6.688% | |
| WC-SH-T02 | 1,076 | 6.543% | |
| PZ-SG-G05 | 1,012 | 6.153% | |

5. In the Fields sidebar, under **Interesting Fields**, click **status**. This field contains the status of the web request. Anything greater than `200` means that the customer interaction ended in an error, and the purchase was not made.

*Results Example*

| Values | Count | % | |
|---|---|---|---|
| 200 | 17,934 | 93.236% | |
| 503 | 797 | 4.143% | |
| 408 | 104 | 0.541% | |
| 400 | 94 | 0.489% | |
| 406 | 87 | 0.452% | |
| 500 | 84 | 0.437% | |
| 505 | 69 | 0.359% | |
| 404 | 39 | 0.203% | |
| 403 | 27 | 0.14% | |

6. To quickly view the status for each event, you can make it selected. From the status field window, click **Yes** in the upper right corner next to **Selected**. Close the window by clicking the x in the upper right corner.

7. Notice `status` is now a selected field in the Fields sidebar and `status=value` is displayed below each event.

*Results Example*

| > | 4/30/17 11:59:43.000 PM | 212.235.92.150 - - [30/Apr/2017:23:59:43] "POST /success.do?action=purchase&categoryId=ARCADE&productId=MB-AG-G07&J SESSIONID=SD4SL6FF7ADFF4963 HTTP 1.1" 503 2198 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=A RCADE&productId=MB-AG-G07" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) V ersion/5.1 Mobile/9B206 Safari/7534.48.3" 926 |
|---|---|---|
| | | host = web_application   productId = MB-AG-G07   source = access_30DAY.log   sourcetype = access_combined_wcookie   status = 503 |
| > | 4/30/17 11:57:14.000 PM | 109.169.32.135 - - [30/Apr/2017:23:57:14] "POST /cart/success.do?JSESSIONID=SD1SL7FF6ADFF89341&productId=FI-AG-G08 HTTP 1.1" 200 3767 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Win dows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 986 |
| | | host = web_application   productId = FI-AG-G08   source = access_30DAY.log   sourcetype = access_combined_wcookie   status = 200 |

8. In the Fields sidebar, under **Selected Fields**, click the `status` field. From the field window, click the value with the highest number (listed at the top). Notice the field and value have been added to the search criteria in the search bar. Also, this selection causes a new search to be executed using the new search criteria.

9. Since the value that shows up in the most results is 200, you are not seeing the server errors. Changing the comparison operator will correct this.

10. Change the status search to: `status!=200` and re-execute the search.

11. Notice that you now have a search that returns only web purchases that ended in an error.

12. How many events ended in error? You can see the event count under the search bar. Take note of this number as you might be asked for it during the quiz.

(1301)

13. In the Fields sidebar, click **status** again and select **No** in the upper right corner next to **Selected.** This will remove it from the **Selected Fields** list. Click the x in the upper right corner to close the field window.

**Task 2:   Use Search History to browse previously run searches.**

14. In the Search History section, click **> Expand your search history**. Unlike jobs, which save the results of your search for a short time, here you only see your search criteria, which are saved for a long time. You will often have many searches. You can filter by time or content to find a search.

15. Click inside the Search History filter box, and type `purchase`. Notice the search list is shortened. Only the searches that contain the word purchase remain.

*Results Example*

| purchase ⊗ | No Time Filter ⌄ | 20 Per Page ⌄ | ‹ Prev | 1 | 2 | 3 | 4 | 5 | Next › |

| *i* | Search ⇕ | Actions | Last Run ⇕ |
|---|---|---|---|
| › | sourcetype=access_combined_wcookie action=purchase | Add to Search | 6 minutes ago |
| › | sourcetype=access_combined_wcookie action=purchase status=200 | Add to Search | 11 minutes ago |

16. For one of the searches, click **Add to Search.** Notice that the search criteria appears in the Search bar, but the time range still displays the default setting.

17. Change the time range, optionally add to or change the search criteria, and then execute the search.

**Task 3:   View your recent searches using the Jobs page.**

18. In the Splunk bar (which is the black bar towards the top of the browser window), click **Activity > Jobs**.

19. Look at the search strings to see if there were any keystroke mistakes. You may see listings like " | `metadata ...` " or " | `history ...` ", which appear when you have accessed the **Expand your search history**.