

---

## 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 8 – Basic Commands

**NOTE:** Now that you understand the basics of searching in Splunk, we will make labs a little more challenging. This lab document has two sections. The first section includes the instructions without answers. The second section includes instructions with the expected search string (answer) in **red**.

### Description

In this lab, you will be using some of the common Splunk commands including fields, table, rename and dedup.

### Steps

---

**Scenario:** The Marketing team tracks all user sessions related to marketing campaigns. It would like a report of all user sessions that include purchase actions so that it can put a value on the different campaigns it's running.

---

#### Task 1: Search for the requested data.

---

1. Navigate to the Search view. (If you are in the **Home** app, click **Search & Reporting** from the column on the left side of the screen. You can also access the Search view by clicking the **Search** menu option on the bar at the top of the screen.)

**NOTE:** For this course, you will be searching across all time using the main index. This is NOT a best practice in a production environment, but needed for these labs due to the nature of the limited dataset.

- Results Example:*

3. Select the `file` field in the **Interesting Fields** list.

Values	Count	%	
success.do	16,139	89.991%	<div></div>
error.do	1,795	10.009%	<div></div>

- Results Example:*

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?

- Results Example:*

## INTERESTING FIELDS

*a* action 1

*a* JSESSIONID 100+

*#* status 1

7. The fields list looks cleaner, but seeing the events like this might still be confusing for the team.

### Task 2: Put the data into an easy to read table.

8. Replace the `fields` command with the `table` command to display the data as a table.

*Results Example:*

20 Per Page ▾ / Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

action ▾ /	JSESSIONID ▾ /	status ▾ /
purchase	SD6SL5FF6ADFF89354	200
purchase	SD6SL5FF6ADFF89354	200
purchase	SD6SL5FF6ADFF89354	200
purchase	SD6SL5FF6ADFF89354	200
purchase	SD6SL5FF6ADFF89354	200

9. Change the order of the fields so that `JSESSIONID` is the first column.

*Results Example:*

20 Per Page ▾ / Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

JSESSIONID ▾ /	action ▾ /	status ▾ /
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200

10. Session IDs are called "UserSessions" in the marketing data. Rename `JSESSIONID` so that your report matches the marketing data.

*Results Example:*

UserSessions ▾ /	action ▾ /	status ▾ /
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200

11. Sort `UserSessions` using the `sort` command.

12. Notice that some `UserSessions` values show up multiple times. Also notice the number of events returned on the **Statistics** tab.

13. Remove the `sort` command and use `dedup` to remove any identical session values.

*Results Example:*

UserSessions ↕	action ↕	status ↕
SD1SL7FF6ADFF89341	purchase	200
SD8SL8FF6ADFF4957	purchase	200
SD2SL10FF6ADFF4955	purchase	200

14. How many events are now listed on the **Statistics** tab?

**NOTE:** As a best practice and for best performance, place dedup as early in the search as possible.

15. While having `action` and `status` fields displayed was nice for a sanity check of the data, the marketing team will not need to have these displayed. Remove them from your table display.

*Results Example:*

UserSessions ↕
SD1SL7FF6ADFF89341
SD8SL8FF6ADFF4957
SD2SL10FF6ADFF4955
SD3SL5FF3ADFF89564

---

## 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 8 – Basic Commands with Solutions

**NOTE:** Now that you understand the basics of searching in Splunk, we will make labs a little more challenging. This lab document has two sections. The first section includes the instructions without answers. The second section includes instructions with the expected search string (answer) in **red**.

### Description

In this lab, you will be using some of the common Splunk commands including fields, table, rename and dedup.

### Steps

---

**Scenario:** The Marketing team tracks all user sessions related to marketing campaigns. It would like a report of all user sessions that include purchase actions so that it can put a value on the different campaigns it's running.

---

#### Task 1: Search for the requested data.

---

1. Navigate to the Search view. (If you are in the **Home** app, click **Search & Reporting** from the column on the left side of the screen. You can also access the Search view by clicking the **Search** menu option on the bar at the top of the screen.)

**NOTE:** For this course, you will be searching across all time using the main index. This is NOT a best practice in a production environment, but needed for these labs due to the nature of the limited dataset.

- Enter a search that returns all web application events that include a purchase action with a web status of 200. (`index=main sourcetype=access_combined_wcookie action=purchase status=200`)

Results Example:

< Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1		>	5/21/18 11:57:14.000 PM	109.169.32.135 - - [21/May/2018:23:57:14] "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; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 986 host = web_application   source = access_30DAY.log   sourcetype = access_combined_wcookie
INTERESTING FIELDS a action 1 # bytes 100+ a categoryid 7 a clientip 100+ # date_hour 24 # date_mday 30 # date_minute 60 # date_month 2 # date_wday 7 # date_year 1 a date_zone 1 a file 2		>	5/21/18 11:57:13.000 PM	109.169.32.135 - - [21/May/2018:23:57:13] "POST /success.do?action=purchase&categoryid=SHOOTER&productId=WC-SH-G04&JSESSIONID=SD1SL7FF6ADFF89341 HTTP/1.1" 200 268 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryid=SHOOTER&productId=WC-SH-G04" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application   source = access_30DAY.log   sourcetype = access_combined_wcookie
		>	5/21/18 11:53:43.000 PM	198.35.3.23 - - [21/May/2018:23:53:43] "POST /success.do?action=purchase&categoryid=ARCADE&productId=MB-AG-G07&JSESSIONID=SD8SL8FF6ADFF4957 HTTP/1.1" 200 2915 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryid=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application   source = access_30DAY.log   sourcetype = access_combined_wcookie
		>	5/21/18 11:51:56.000 PM	198.35.3.23 - - [21/May/2018:23:51:56] "POST /cart/success.do?JSESSIONID=SD8SL8FF6ADFF4957&productId=DC-SG-G02 HTTP/1.1" 200 594 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application   source = access_30DAY.log   sourcetype = access_combined_wcookie

- Select the file field in the Interesting Fields list.

Results Example:

Values	Count	%
success.do	16,139	89.991%
error.do	1,795	10.009%

- Notice that there are two different files that were returned from the web server. They are: `error.do` and `success.do`. Our web development team informs us that the `success.do` is served when the order is processed and `error.do` is served when there is an error with the information being processed.
- The team is only looking for successful purchases, so change your search to only return those. (`index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do`)

Results Example:

< Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1		>	5/21/18 11:57:14.000 PM	109.169.32.135 - - [21/May/2018:23:57:14] "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; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 986 host = web_application   source = access_30DAY.log   sourcetype = access_combined_wcookie
INTERESTING FIELDS a action 1 # bytes 100+ a categoryid 7 a clientip 100+ # date_hour 24 # date_mday 30 # date_minute 60 # date_month 2		>	5/21/18 11:57:13.000 PM	109.169.32.135 - - [21/May/2018:23:57:13] "POST /success.do?action=purchase&categoryid=SHOOTER&productId=WC-SH-G04&JSESSIONID=SD1SL7FF6ADFF89341 HTTP/1.1" 200 268 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryid=SHOOTER&productId=WC-SH-G04" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application   source = access_30DAY.log   sourcetype = access_combined_wcookie
		>	5/21/18 11:53:43.000 PM	198.35.3.23 - - [21/May/2018:23:53:43] "POST /success.do?action=purchase&categoryid=ARCADE&productId=MB-AG-G07&JSESSIONID=SD8SL8FF6ADFF4957 HTTP/1.1" 200 2915 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryid=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application   source = access_30DAY.log   sourcetype = access_combined_wcookie

- 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?  
(`index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | fields action, JSESSIONID, status`)

Results Example:



## INTERESTING FIELDS

*a* action 1

*a* JSESSIONID 100+

*#* status 1

7. The fields list looks cleaner, but seeing the events like this might still be confusing for the team.

### Task 2: Put the data into an easy to read table.

8. Replace the `fields` command with the `table` command to display the data as a table. (`index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table action, JSESSIONID, status`).


Results Example:




20 Per Page ▾  Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

action ▾ 	JSESSIONID ▾ 	status ▾ 
purchase	SD6SL5FF6ADFF89354	200
purchase	SD6SL5FF6ADFF89354	200
purchase	SD6SL5FF6ADFF89354	200
purchase	SD6SL5FF6ADFF89354	200
purchase	SD6SL5FF6ADFF89354	200

9. Change the order of the fields so that `JSESSIONID` is the first column. (`index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status`).




Results Example:

20 Per Page ▾  Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

JSESSIONID ▾ 	action ▾ 	status ▾ 
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200

10. Session IDs are called "UserSessions" in the marketing data. Rename `JSESSIONID` so that your report matches the marketing data. (`index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | rename JSESSIONID as UserSessions`).

Results Example:

UserSessions ▾ 	action ▾ 	status ▾ 
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200
SD6SL5FF6ADFF89354	purchase	200

11. Sort `UserSessions` using the `sort` command. (`index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | rename JSESSIONID as UserSessions | sort UserSessions`)

- 
12. Notice that some `UserSessions` values show up multiple times. Also notice the number of events returned on the **Statistics** tab.
  13. Remove the `sort` command and use `dedup` to remove any identical session values. (`index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | dedup JSESSIONID | table JSESSIONID, action, status | rename JSESSIONID as UserSessions`)

*Results Example:*

UserSessions ⌵	action ⌵	status ⌵
SD1SL7FF6ADFF89341	purchase	200
SD8SL8FF6ADFF4957	purchase	200
SD2SL10FF6ADFF4955	purchase	200

14. How many events are now listed on the **Statistics** tab?

**NOTE:** As a best practice and for best performance, place `dedup` as early in the search as possible.

15. While having `action` and `status` fields displayed was nice for a sanity check of the data, the marketing team will not need to have these displayed. Remove them from your table display. (`index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | dedup JSESSIONID | table JSESSIONID | rename JSESSIONID as UserSessions`).

*Results Example:*

UserSessions ⌵
SD1SL7FF6ADFF89341
SD8SL8FF6ADFF4957
SD2SL10FF6ADFF4955
SD3SL5FF3ADFF89564