## 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 11 – Using Pivot

> **NOTE:** 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 <span style="color:red">red</span>.

## Description

In this lab, you will be building a report using the Pivot interface.

## Steps

**Scenario:** The CFO loved the simple dashboard you created, but would like to add a report of where our customers are coming from. She would like to know what items users added to the shopping cart, and where those users originated from.

**Task 1:  Use a non-transforming command with instant Pivot.**

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 green 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.

2. Enter in a search that returns all web application events for all time.
3. Click on the **Visualization** tab to see three icons: Pivot, Quick Reports, and Search Command.
*Example:*

ⓘ Your search isn't generating any statistic or visualization results. Here are some possible ways to get results.

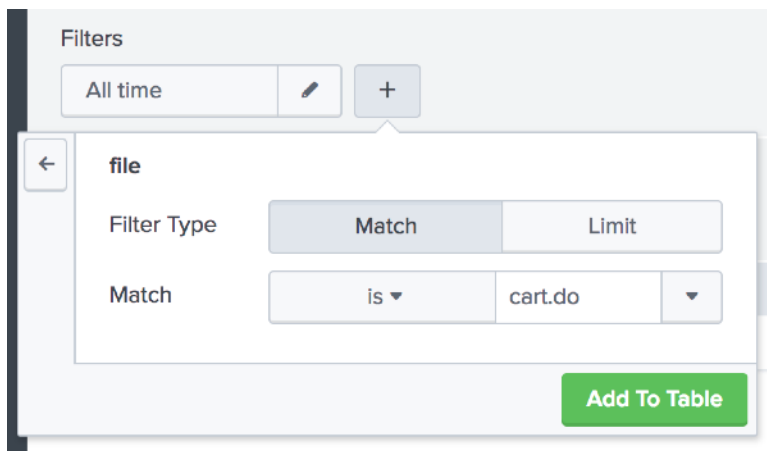| Pivot | Quick Reports | Search Commands ⬈ |
|---|---|---|
| Build tables and visualizations using multiple fields and metrics without writing searches. | Click on any field in the events tab for a list of quick reports like 'Top Referrers' and 'Top Referrers by time'. | Use a transforming search command, like timechart or stats, to summarize the data. |

4. Click on the **Pivot** icon.
5. In the modal window, select to show **All Fields** and click **OK**.

**Task 2: Build a report using the Pivot interface.**

6. Under **Filters**, click [+] to open the filter selector, and select **file** from the **Fields list**.
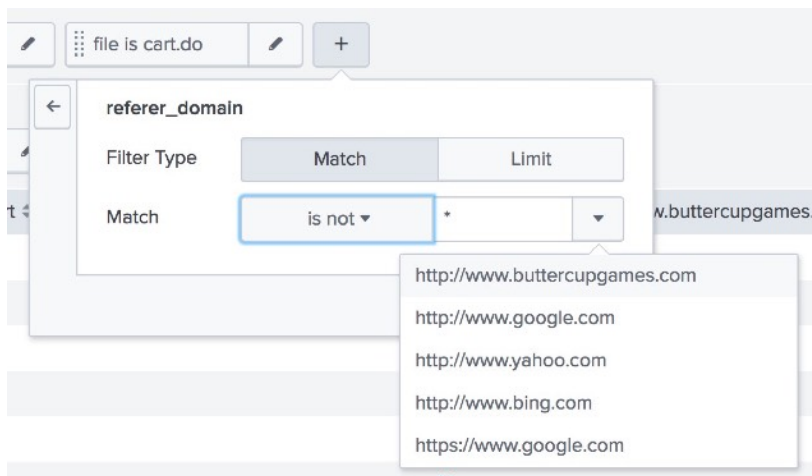7. Select **cart.do** from the match menu and click **Add To Table**.

*Example:*

Filters

| All time | ✏ | + |
|---|---|---|

← **file**

| Filter Type | Match | Limit |
|---|---|---|

| Match | is ▾ | cart.do ▾ |

**Add To Table**

8. Under **Split Rows**, click [+], to open the split rows selector, and then click **productID**.
9. For the **Label**, enter `Product Added To Cart`.
10. Keep other settings at their default values, and click **Add To Table**.
11. Under **Split Columns**, click [+] to open the split columns selector, and then click **referrer_domain**.
12. Keep other settings at their default values, and click **Add To Table**.
13. Notice that a large amount of the web traffic is coming from the buttercupgames.com domain. We will want to filter these out.

*Example Results:*

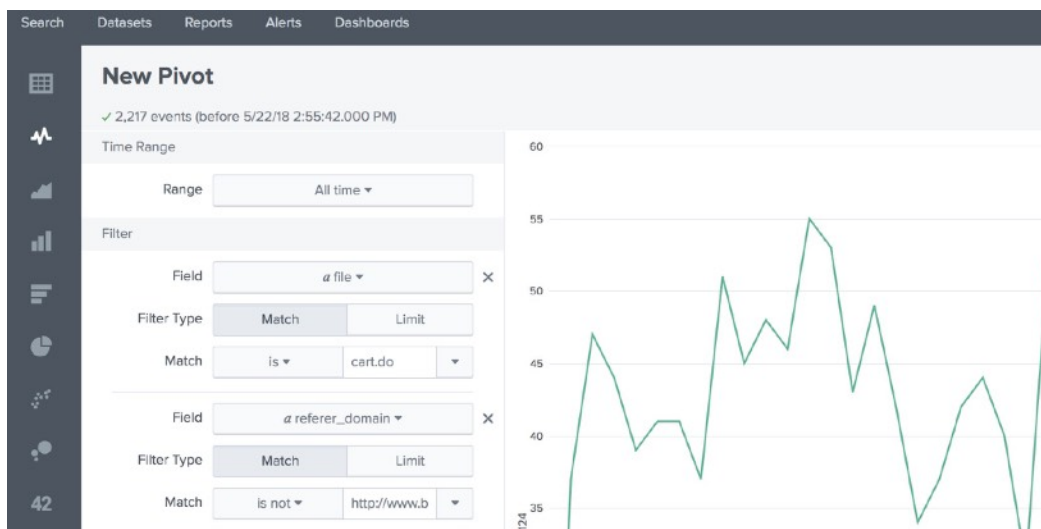| Product Added To Cart ⇕ | ✎ | http://www.bing.com ⇕ | ✎ | http://www.buttercupgames.com ⇕ | ✎ | http://www.google.com ⇕ | ✎ | http://www.yahoo.com ⇕ | ✎ |
|---|---|---|---|---|---|---|---|---|---|
| BS-AG-G09 | | 23 | | 1421 | | 56 | | 36 | |
| CU-PG-G06 | | 17 | | 1452 | | 58 | | 35 | |
| DB-SG-G01 | | 26 | | 2367 | | 100 | | 46 | |
| DC-SG-G02 | | 15 | | 2269 | | 92 | | 34 | |
| FI-AG-G08 | | 12 | | 1603 | | 50 | | 25 | |
| FS-SG-G03 | | 21 | | 1967 | | 85 | | 25 | |

14. Under **Filters**, click [ + ], to open the filter selector, and select **referrer_domain** from the **Fields list**.

15. Select **is not** and http://www.buttercupgames.com from the match menu.

*Example:*



16. Click **Add To Table**.

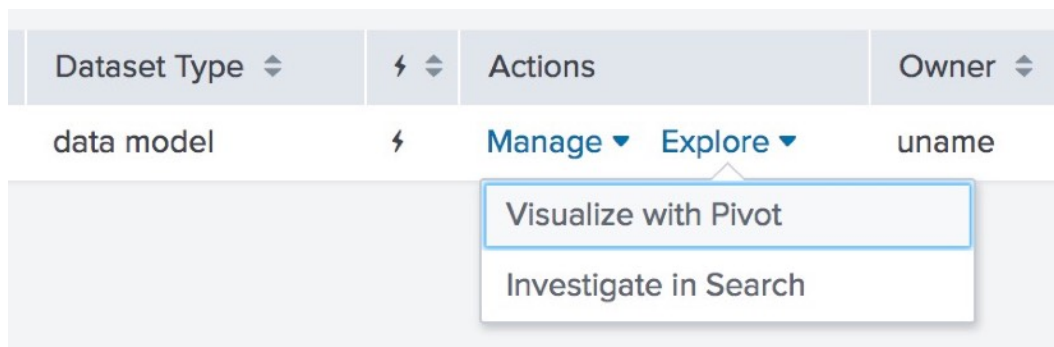17. Use the black sidebar to select the **Line Chart** visualization.

*Example:*



**Task 3: Add a panel to a dashboard from a pivot, and create a Data Model.**

18. Use the **Save As** menu to select **Dashboard Panel.**

19. Notice that there are form fields for **Model Title** and **Model ID**. Pivot reports require a data model. Since you used Instant Pivot from the **Visualization** tab, there is currently not a data model for this report. Saving the report will create a new data model from the original search.

20. Save the dashboard with these values:

- Dashboard:  *Existing*
- Dashboard Title:  *Sales Dashboard*
- Panel Title**:**  *Sales By Referral Domain*
- Model Title:  Web Application Dataset
- Model ID:  web_app_ds

21. Click **View Dashboard** to view the dashboard.

22. Click the **Datasets** menu option on the bar at the top of the screen.

23. Click **Yours** on the filter toolbar to show only your Datasets.

24. Select **Explore** from the actions menu and click **Visualize with Pivot**.

*Example:*

| Dataset Type ⇕ | ⚡ ⇕ | Actions | Owner ⇕ |
|---|---|---|---|
| data model | ⚡ | Manage ▾ Explore ▾ | uname |
| | | Visualize with Pivot | |
| | | Investigate in Search | |

25. Use the **Filter** and **Split** tools to explore your data in the pivot interface.

## 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 11 – Using Pivot with Solutions

> **NOTE:** 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 building a report using the Pivot interface.

## Steps

**Scenario**: The CFO loved the simple dashboard you created, but would like to add a report of where our customers are coming from. She would like to know what items users added to the shopping cart, and where those users originated from.

**Task 1: Use a non-transforming command with instant Pivot.**

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 green 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 in a search that returns all web application events for all time.

2. (index=main sourcetype=access_combined_wcookie)

Click on the **Visualization** tab to see three icons: Pivot, Quick Reports, and Search Command.

3.

*Example:*

ⓘ Your search isn't generating any statistic or visualization results. Here are some possible ways to get results.

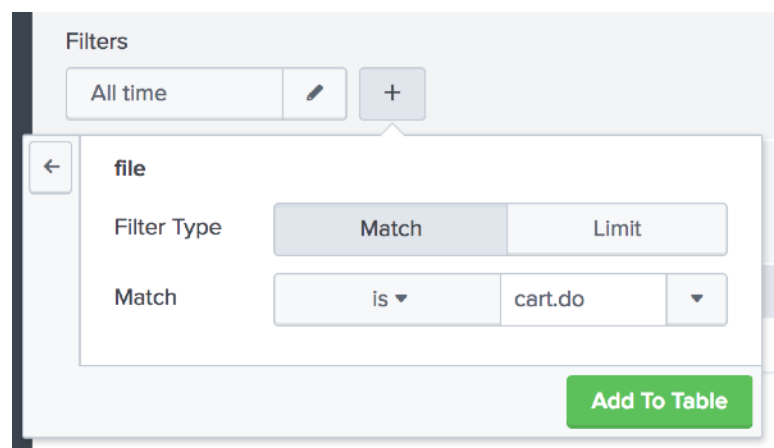| Pivot | Quick Reports | Search Commands ⬈ |
|---|---|---|
| Build tables and visualizations using multiple fields and metrics without writing searches. | Click on any field in the events tab for a list of quick reports like 'Top Referrers' and 'Top Referrers by time'. | Use a transforming search command, like timechart or stats, to summarize the data. |

4. Click on the **Pivot** icon.
5. In the modal window, select to show **All Fields** and click **OK**.

**Task 2: Build a report using the Pivot interface.**

6. Under **Filters**, click ⊞ to open the filter selector, and select **file** from the **Fields list**.
7. Select **cart.do** from the match menu and click **Add To Table**.
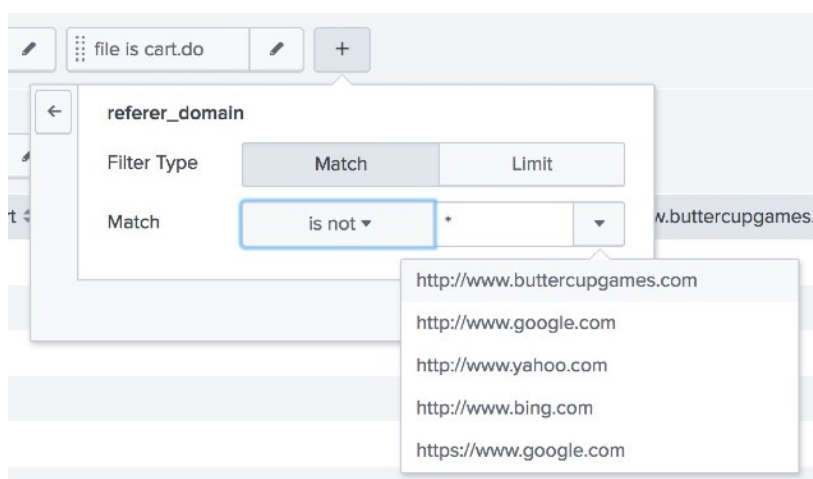
*Example:*

Filters

| All time | ✏ | + |
|---|---|---|

← **file**

| Filter Type | Match | Limit |
|---|---|---|
| Match | is ▾ | cart.do ▾ |

**Add To Table**

8. Under **Split Rows**, click ⊞ to open the split rows selector, and then click **productID**.
9. For the **Label**, enter `Product Added To Cart`.
10. Keep other settings at their default values, and click **Add To Table**.
11. Under **Split Columns**, click ⊞ to open the split columns selector, and then click **referrer_domain**.
12. Keep other settings at their default values, and click **Add To Table**.
13. Notice that a large amount of the web traffic is coming from the buttercupgames.com domain. We will want to filter these out.

*Example Results:*

| Product Added To Cart ⇕ | ✎ | http://www.bing.com ⇕ | ✎ | http://www.buttercupgames.com ⇕ | ✎ | http://www.google.com ⇕ | ✎ | http://www.yahoo.com ⇕ | ✎ |
|---|---|---|---|---|---|---|---|---|---|
| BS-AG-G09 | | 23 | | 1421 | | 56 | | 36 | |
| CU-PG-G06 | | 17 | | 1452 | | 58 | | 35 | |
| DB-SG-G01 | | 26 | | 2367 | | 100 | | 46 | |
| DC-SG-G02 | | 15 | | 2269 | | 92 | | 34 | |
| FI-AG-G08 | | 12 | | 1603 | | 50 | | 25 | |
| FS-SG-G03 | | 21 | | 1967 | | 85 | | 25 | |

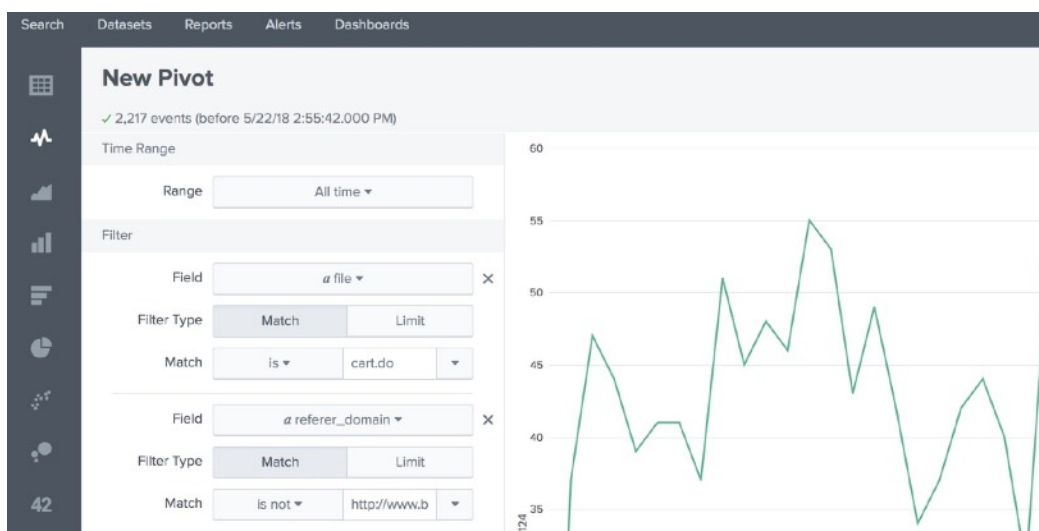14. Under **Filters**, click [ + ], to open the filter selector, and select **referrer_domain** from the **Fields list**.
15. Select **is not** and http://www.buttercupgames.com from the match menu.

*Example:*



16. Click **Add To Table**.
17. Use the black sidebar to select the **Line Chart** visualization.
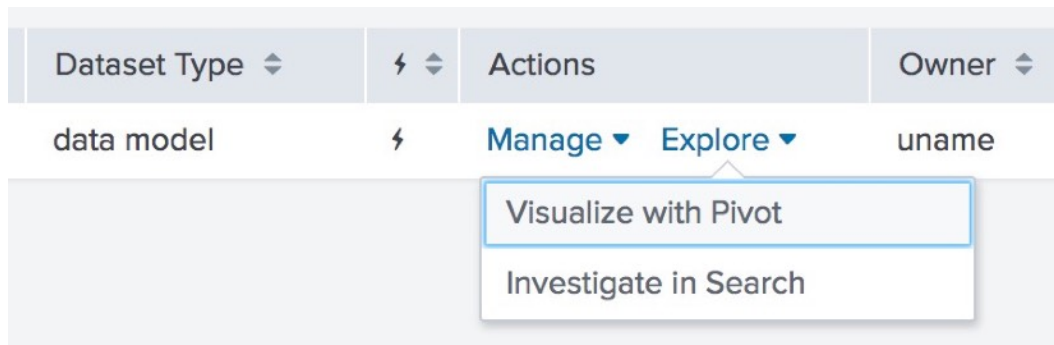
*Example:*



**Task 3:  Add a panel to a dashboard from a pivot, and create a Data Model.**

18. Use the **Save As** menu to select **Dashboard Panel.**

19. Notice that there are form fields for **Model Title** and **Model ID**. Pivot reports require a data model. Since you used Instant Pivot from the **Visualization** tab, there is currently not a data model for this report. Saving the report will create a new data model from the original search.

20. Save the dashboard with these values:
    - Dashboard:             *Existing*
    - Dashboard Title:       *Sales Dashboard*
    - Panel Title**:**         *Sales By Referral Domain*
    - Model Title:           Web Application Dataset
    - Model ID:              web_app_ds

21. Click **View Dashboard** to view the dashboard.

22. Click the **Datasets** menu option on the bar at the top of the screen.

23. Click **Yours** on the filter toolbar to show only your Datasets.

24. Select **Explore** from the actions menu and click **Visualize with Pivot**.

*Example:*

| Dataset Type ⇕ | ⚡ ⇕ | Actions | Owner ⇕ |
|---|---|---|---|
| data model | ⚡ | Manage ▾  Explore ▾ | uname |
| | | Visualize with Pivot | |
| | | Investigate in Search | |

25. Use the **Filter** and **Split** tools to explore your data in the pivot interface.