Lab Exercise 4 – Advanced Visualizations

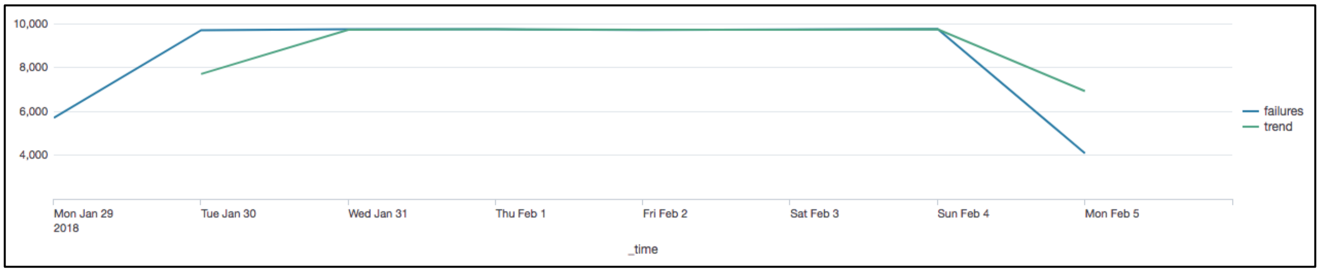
Description

In this lab exercise, use `trendline`, `iplocation`, `geostats`, `geom` and `addtotals` commands – as well as the single-value, choropleth map, and cluster map visualizations.

Steps

Task 1: Display web server failures during the last 7 days in a timechart with a trendline.

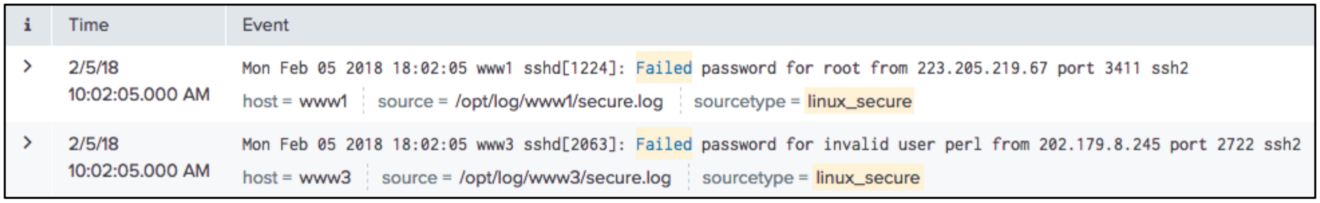
Final Example:



1. Search for failures on the web server [`linux_secure`] during the **last 7 days**.

   index=security sourcetype=linux_secure fail*

Results Example:



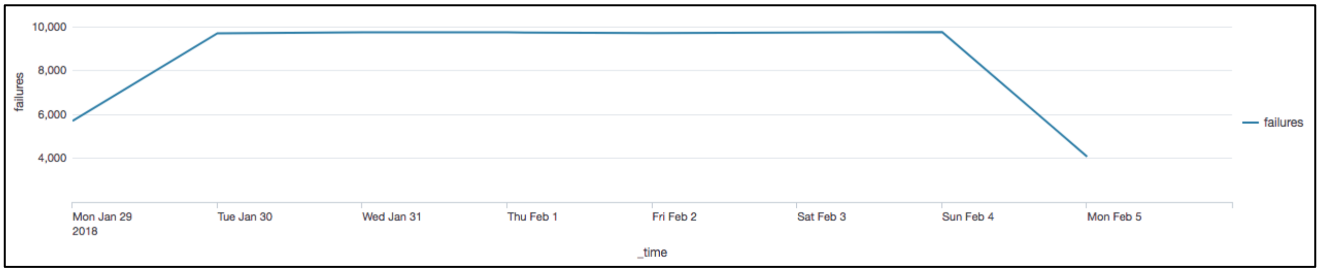
i	Time	Event
>	2/5/18 10:02:05.000 AM	Mon Feb 05 2018 18:02:05 www1 sshd[1224]: Failed password for root from 223.205.219.67 port 3411 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	2/5/18 10:02:05.000 AM	Mon Feb 05 2018 18:02:05 www3 sshd[2063]: Failed password for invalid user perl from 202.179.8.245 port 2722 ssh2 host = www3 source = /opt/log/www3/secure.log sourcetype = linux_secure

2. Using `timechart`, count the events for each day and rename this new column as `failures`.

   index=security sourcetype=linux_secure fail*
   | timechart span=1d count as failures

3. Change the visualization to **Line Chart**.

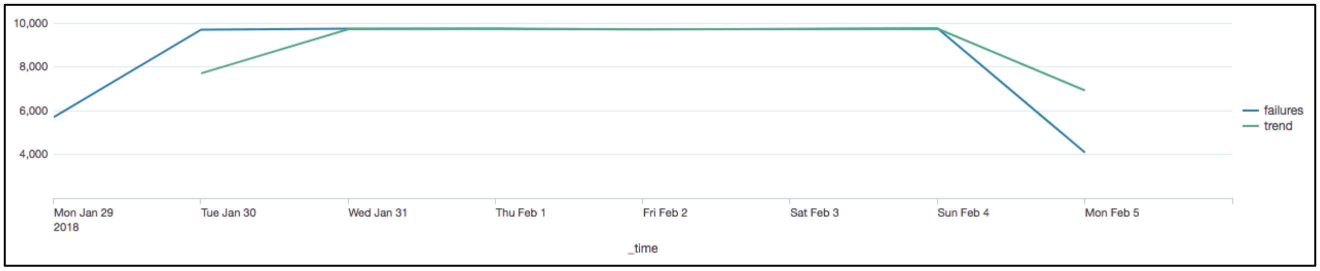
Results Example:



4. Find the `trendline` of failures using a simple moving average (`sma2`).

```
index=security sourcetype=linux_secure fail*
| timechart span=1d count as failures
| trendline sma2(failures) as trend
```

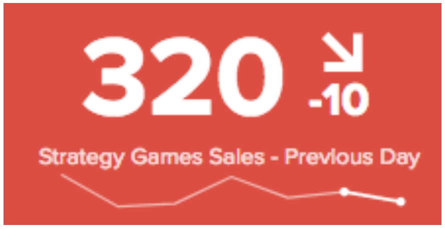
Results Example:



5. Save your search as report, **L3S1**

Task 2: Display the sales count of strategy games per day at Buttercup Games physical sales locations (i.e., not online) during the previous week.

Final Results Example:

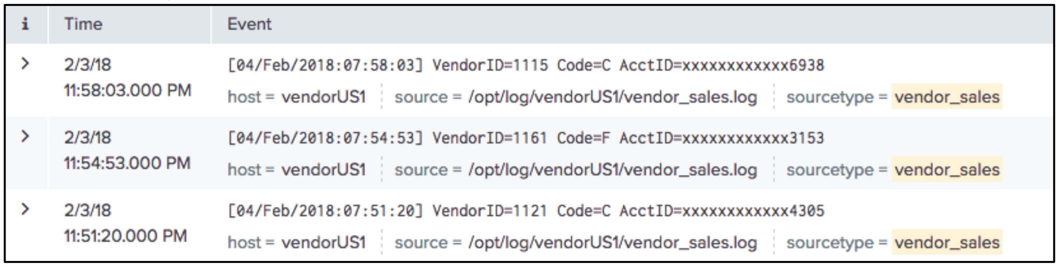


6. Search for retail sales [`vendor_sales`] of strategy games [`categoryId`="STRATEGY"] during the **previous week**.

```
index=sales sourcetype=vendor_sales categoryId= "STRATEGY"
```

NOTE: Since the `categoryId` comes from a lookup, the value being matched is case-sensitive. So be sure to type "STRATEGY" in all caps.

Results Example:

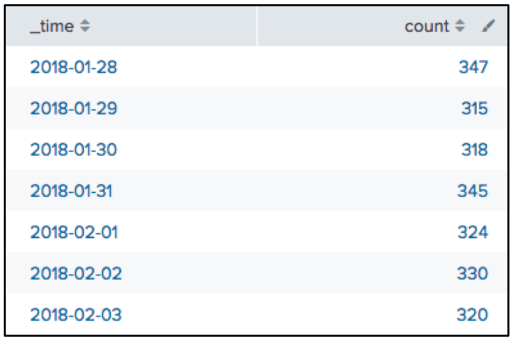


i	Time	Event
>	2/3/18 11:58:03.000 PM	[04/Feb/2018:07:58:03] VendorID=1115 Code=C AcctID=xxxxxxxxxxxx6938 host = vendorUS1 source = /opt/log/vendorUS1/vendor_sales.log sourcetype = vendor_sales
>	2/3/18 11:54:53.000 PM	[04/Feb/2018:07:54:53] VendorID=1161 Code=F AcctID=xxxxxxxxxxxx3153 host = vendorUS1 source = /opt/log/vendorUS1/vendor_sales.log sourcetype = vendor_sales
>	2/3/18 11:51:20.000 PM	[04/Feb/2018:07:51:20] VendorID=1121 Code=C AcctID=xxxxxxxxxxxx4305 host = vendorUS1 source = /opt/log/vendorUS1/vendor_sales.log sourcetype = vendor_sales

7. Using `timechart`, count the sales per day of strategy games.

```
index=sales sourcetype=vendor_sales categoryId="STRATEGY"
| timechart span=1d count
```

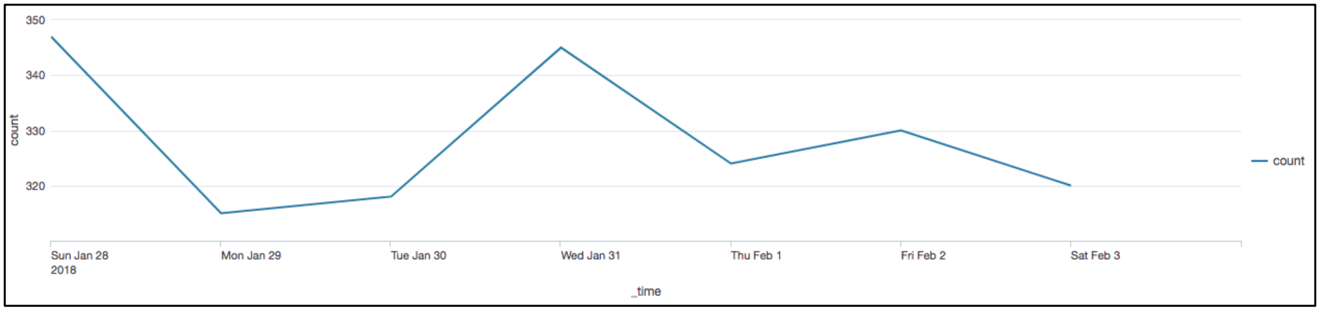
Results Example



_time	count
2018-01-28	347
2018-01-29	315
2018-01-30	318
2018-01-31	345
2018-02-01	324
2018-02-02	330
2018-02-03	320

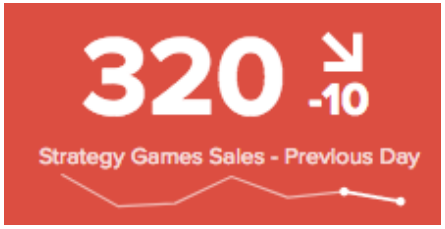
8. Change the visualization to **Line Chart**.

Results Example



9. Change the visualization to **single value** with the following format:
   - Caption: Strategy Games Sales – Previous Day
   - Show Trend Indicator: *Yes*
   - Show Sparkline: *Yes*
   - Color By: Trend
   - Color Mode: Set so that the background shows the color based on the trend (e.g., green for an increasing trend and red for a decreasing trend)

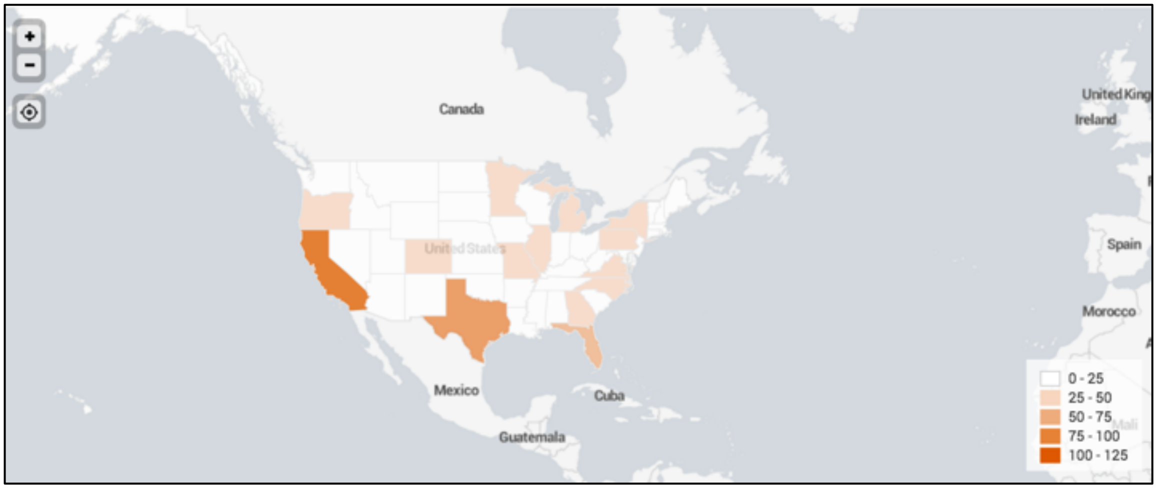
Results Example:



10. Save your search as report, **L3S2**.

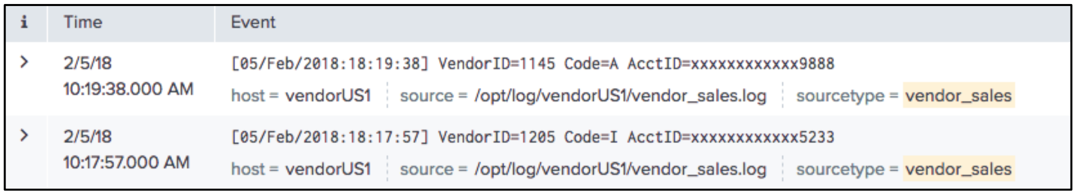
Task 3: Display a choropleth map of United States retail sales during the last 7 Days.

Final Results Example:



11. Search for United States retail sales during the **last 7 Days**.
    Hint: United States vendors have a VendorID less than 3000.
    index=sales sourcetype=vendor_sales VendorID < 3000

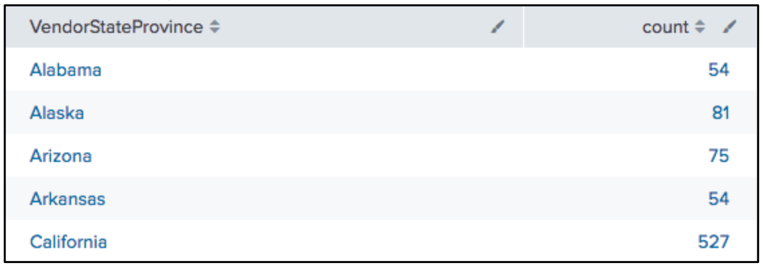
Results Example:



i	Time	Event
>	2/5/18 10:19:38.000 AM	[05/Feb/2018:18:19:38] VendorID=1145 Code=A AcctID=xxxxxxxxxxxx9888 host = vendorUS1 source = /opt/log/vendorUS1/vendor_sales.log sourcetype = vendor_sales
>	2/5/18 10:17:57.000 AM	[05/Feb/2018:18:17:57] VendorID=1205 Code=I AcctID=xxxxxxxxxxxx5233 host = vendorUS1 source = /opt/log/vendorUS1/vendor_sales.log sourcetype = vendor_sales

12. Using the `chart` command, count the events over `VendorStateProvince`.
    index=sales sourcetype=vendor_sales VendorID<3000
    | chart count over VendorStateProvince

Results Example:



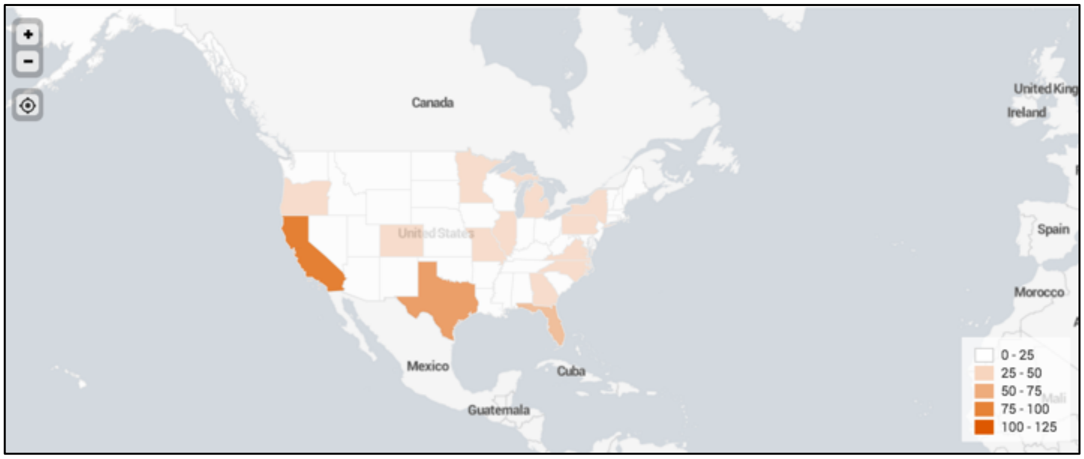
VendorStateProvince	count
Alabama	54
Alaska	81
Arizona	75
Arkansas	54
California	527

13. To display the data as a choropleth map, use the `geom` command to map `VendorStateProvince` to the geo_us_states KMZ file (`geom geo_us_states featureIdField=VendorStateProvince`).

```
index=sales sourcetype=vendor_sales VendorID<3000
| chart count by VendorStateProvince
| geom geo_us_states featureIdField=VendorStateProvince
```

14. Click the **Visualization** tab.
15. Change the visualization to use the **Choropleth Map**.
16. Zoom in on the map so you can clearly see the United States.

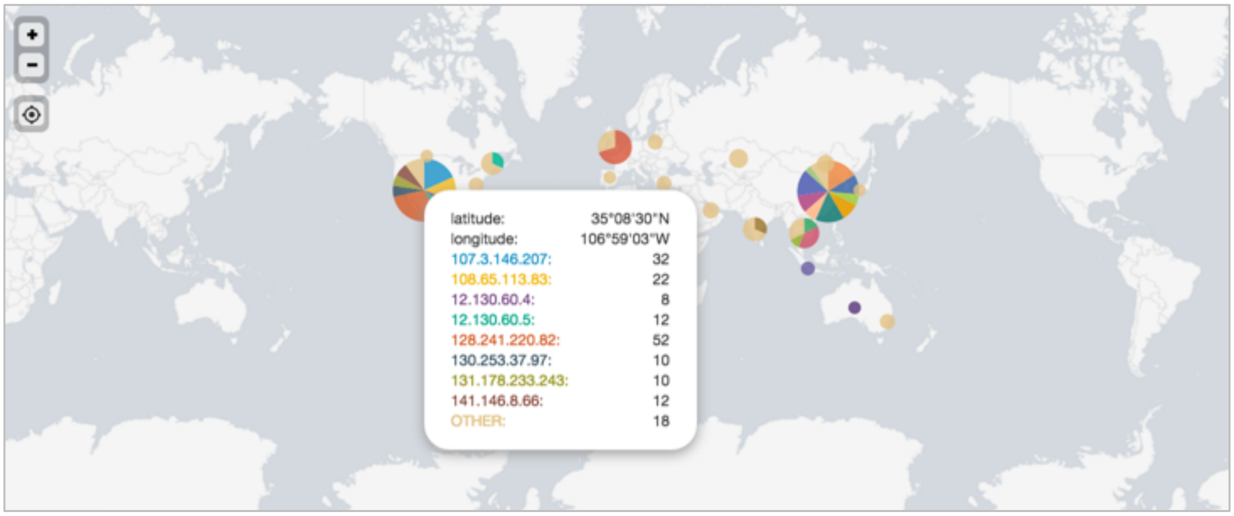
Results Example:



17. Click **Format**.
18. Click **Tiles**.
19. Click Populate from preset configuration.
20. Click Open Street Map.
21. Save your search as report, **L3S3**.

Task 4: Display a map of online sales by country during the previous week.

Final Results Example:

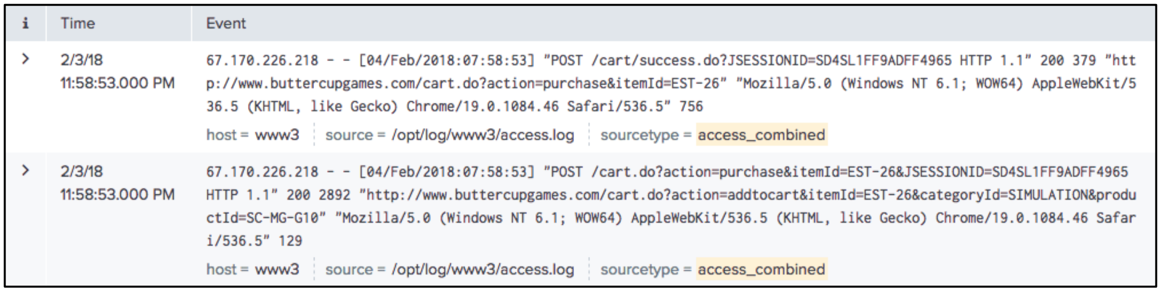


latitude:	35°08'30"N
longitude:	106°59'03"W
107.3.146.207:	32
108.65.113.83:	22
12.130.60.4:	8
12.130.60.5:	12
128.241.220.82:	52
130.253.37.97:	10
131.178.233.243:	10
141.146.8.66:	12
OTHER:	18

22. Find successful online purchases [`access_combined`] during the **Previous week**.
    Hint: You can use the Fields sidebar to narrow your search results. From `action`, select purchase and from `status`, 200.

    index=web sourcetype=access_combined action=purchase status=200

Results Example:



i	Time	Event
>	2/3/18 11:58:53.000 PM	67.170.226.218 - - [04/Feb/2018:07:58:53] "POST /cart/success.do?JSESSIONID=SD4SL1FF9ADFF4965 HTTP 1.1" 200 379 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-26" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 756 host = www3 source = /opt/log/www3/access.log sourcetype = access_combined
>	2/3/18 11:58:53.000 PM	67.170.226.218 - - [04/Feb/2018:07:58:53] "POST /cart.do?action=purchase&itemId=EST-26&JSESSIONID=SD4SL1FF9ADFF4965 HTTP 1.1" 200 2892 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-26&categoryId=SIMULATION&productId=SC-MG-G10" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 129 host = www3 source = /opt/log/www3/access.log sourcetype = access_combined

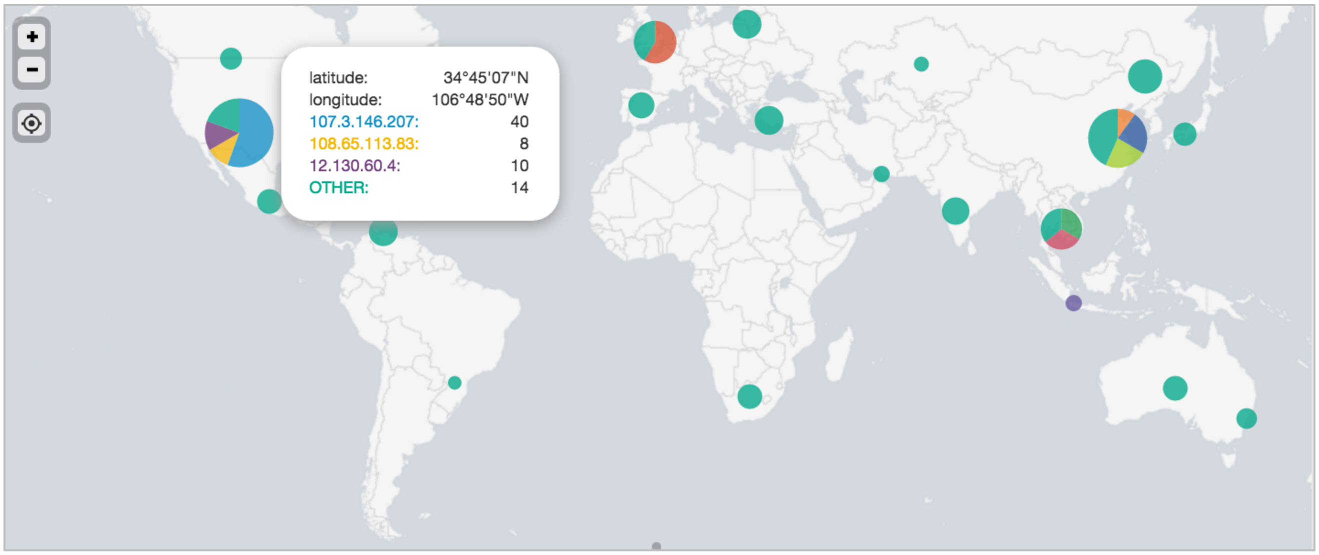
23. Use `iplocation` to extract the location of the purchases based on **clientip**. (You will see the `lat` and `lon` fields on the Fields sidebar.)

    ```
    index=web sourcetype=access_combined action=purchase status=200
    | iplocation clientip
    ```

24. To place the events on a map, use `geostats` to count by `clientip`. (Note that you may need to manually change the visualization to a Cluster Map.)

    ```
    index=web sourcetype=access_combined action=purchase status=200
    | iplocation clientip
    | geostats count by clientip
    ```

Results Example:



latitude: 34°45'07"N
longitude: 106°48'50"W
107.3.146.207: 40
108.65.113.83: 8
12.130.60.4: 10
OTHER: 14

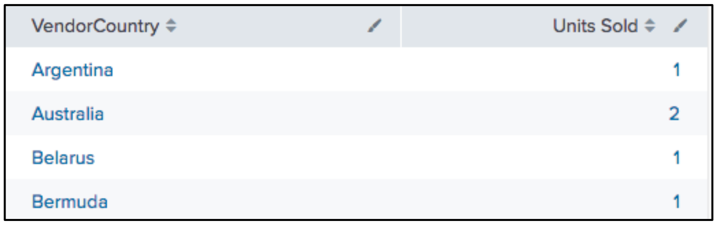
25. Save your search as report, **L3S4**.

Task 5: Count the retail sales units sold by country and include a grand total row.

26. Count the number of retail store purchases [`vendor_sales`] by `VendorCountry` during the **last 4 hours**, and rename the new column to “Units Sold.”

```
index=sales sourcetype=vendor_sales
| stats count as "Units Sold" by VendorCountry
```

Results Example:

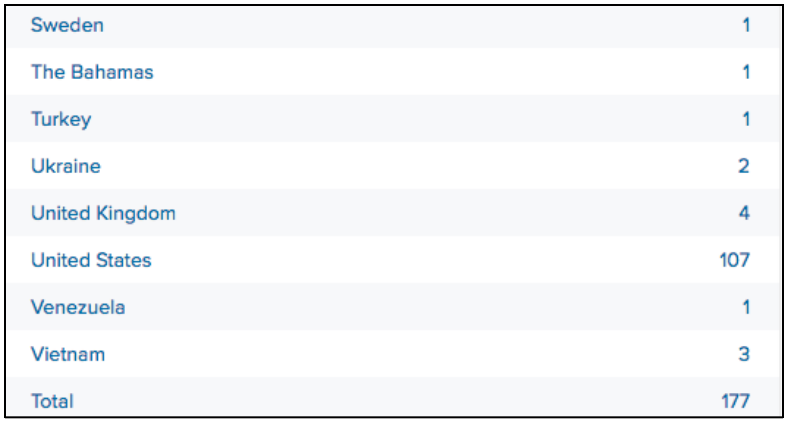


VendorCountry	Units Sold
Argentina	1
Australia	2
Belarus	1
Bermuda	1

27. Use `addtotals` with the col and row options to display the column total and suppress the row total. Modify the search to include a `Total` label for the last row of the table as shown in the results below.

```
index=sales sourcetype=vendor_sales
| stats count as "Units Sold" by VendorCountry
| addtotals col=t row=f labelfield="VendorCountry"
```

Results Example:



Sweden	1
The Bahamas	1
Turkey	1
Ukraine	2
United Kingdom	4
United States	107
Venezuela	1
Vietnam	3
Total	177

28. Save your search as report, **L3S5**.