Making the Pipeline More Readable

- Put each pipe in the pipeline on a separate line as you type by turning on auto-formatting
- Go to **Preferences > SPL Editor** and turn on Search auto-format

Instead of this:

New Search

```
index=web sourcetype=access_* status=503 | stats sum(price) as lost_revenue | eval lost_revenue = "$" + tostring(lost_revenue, "commas")
```

You'll get this:

New Search

```
index=web sourcetype=access_* status=503
| stats sum(price) as lost_revenue
| eval lost_revenue = "$" + tostring(lost_revenue, "commas")
```

Note

You can also use **Shift** + **Enter** to go to a new line.

Syntax Coloring

- You can turn off automatic syntax coloring
  1. Go to **Preferences** > **SPL Editor**
  2. Choose the Themes tab and select Black on White instead of the Light Theme default
  3. Click Apply
- You can also display colored text against a black background by selecting Dark Theme

```
index=web (sourcetype=acc* OR sourcetype=ven*) action=purchase status<400 | timechart span=1h sum(price) by sourcetype
```

Creating a Table

- table command returns a table formed by only fields in the argument list
- Columns are displayed in the order given in the command
  - Column headers are field names
  - Each row represents an event
  - Each row contains field values for that event

```
index=web sourcetype=access_combined
| table clientip, action, productId, status
```

clientip	action	productId	status
220.225.12.171	view	WC-SH-A02	200
220.225.12.171		WC-SH-G04	200
188.173.152.100		CU-PG-G06	200
188.173.152.100	purchase		200
188.173.152.100	purchase	WC-SH-T02	200
188.173.152.100	addtocart	WC-SH-T02	200
188.173.152.100		WC-SH-T02	200
188.173.152.100		WC-SH-A02	200

Renaming Fields in a Table (cont.)

Once you rename a field, you can’t access it with the original name

```
index=web  sourcetype=access_combined
| table  clientip,  action,  productId, status
| rename  productId  as
  ProductID,  action  as
 "Customer  Action”, status
 as  "HTTP  Status"| table  action,  status
```

No results found.

```
index=web  sourcetype=access_combined
| table  clientip,  action,  productId, status
| rename  productId  as ProductID,  action  as “Customer Action”,
  status as  "HTTP  Status"
| table  "Customer  Action",  “HTTP Status"
```

Customer Action	HTTP Status
purchase	200
purchase	200
addtocart	200
	200
	200
view	200
view	200
	200

Using the fields Command

- Field extraction is one of the most costly parts of a search
- fields command allows you to include or exclude specified fields in your search or report
- To include, us e fields + (default)
  - Occurs before field extraction
  - Improves performance
- To exclude, use fields -
  - Occurs after field extraction
  - No performance benefit
  - Exclude fields used in search to make the table/display easier to read

fields Comm and – Examples

Using command improves performance—only specified fields extracted

```
index=security
sourcetype=linux_secure (fail* OR invalid)
```

Returned **6,567** results by scanning **6,567** events in **1.425** seconds:

```
index=security
sourcetype=linux_secure (fail* OR invalid)
 | fields user, app,
 src_ip
```

Returned **6,567** results by scanning **6,567** events in **0.753** seconds:

Using the dedup Command

Use dedup to remove duplicates from your results

index=sales sourcetype=vendor_sales Vendor=Bea* | table Vendor, VendorCity, VendorStateProvince, VendorCountry

Vendor	VendorCity	VendorStateProvince	VendorCountry
Beach Games	Miami	Florida	United States
Beads & Games	Ft. Riley	Kansas	United States
Beach Games	Miami	Florida	United States
Beantown Games	Boston	Massachusetts	United States
Beantown Games	Boston	Massachusetts	United States
Beach Games	Fort Lauderdale	Florida	United States

…| dedup Vendor | table …

Vendor	VendorCity	VendorStateProvince	VendorCountry
Beach Games	Miami	Florida	United States
Beads & Games	Ft. Riley	Kansas	United States
Beantown Games	Boston	Massachusetts	United States
Beauty Games	Butte	Montana	United States

…| dedup Vendor, VendorCity | table …

Vendor	VendorCity	VendorStateProvince	VendorCountry
Beach Games	Miami	Florida	United States
Beads & Games	Ft. Riley	Kansas	United States
Beach Games	Fort Lauderdale	Florida	United States
Beantown Games	Boston	Massachusetts	United States
Beauty Games	Butte	Montana	United States

Using the sort Command

- Use sort to order your results in + ascending (default) or – descending
- To limit the returned results, use the limit option

```
... | sort limit=20 –categoryId, product_name
... | sort 20 count
```

Using the sort Command (cont.)

sort -/+<*fieldname*> sign followed by fieldname sorts results in the sign's order

sort -/+ <*fieldname*> sign followed by **space** and then fieldname applies sort order to **all** following fields without a different explicit sort order

```
index=sales sourcetype=vendor_sales
Vendor=Bea*
| dedup Vendor, VendorCity
| table Vendor, VendorCity,
VendorStateProvince, VendorCountry
| sort –Vendor, VendorCity
```

Vendor	VendorCity	VendorStateProvince	VendorCountry
Beauty Games	Butte	Montana	United States
Beantown Games	Boston	Massachusetts	United States
Beads & Games	Ft. Riley	Kansas	United States
Beach Games	Fort Lauderdale	Florida	United States
Beach Games	Miami	Florida	United States

```
index=sales sourcetype=vendor_sales
Vendor=Bea*
| dedup Vendor, VendorCity
| table Vendor, VendorCity,
VendorStateProvince, VendorCountry
| sort – Vendor, VendorCity
```

Vendor	VendorCity	VendorStateProvince	VendorCountry
Beauty Games	Butte	Montana	United States
Beantown Games	Boston	Massachusetts	United States
Beads & Games	Ft. Riley	Kansas	United States
Beach Games	Miami	Florida	United States
Beach Games	Fort Lauderdale	Florida	United States

Transforming Commands

Getting Top Values

- The top command finds the most common values of a giv en field in the result set
- By default, output displays in table format

src_ip	count	percent
132.55.227.221	105	27.131783
214.156.206.45	9	2.325581
118.6.85.68	9	2.325581
87.194.216.51	8	2.067183
108.65.113.83	6	1.550388
89.11.192.18	5	1.291990
211.166.11.101	5	1.291990
195.69.160.22	5	1.291990
81.18.148.190	4	1.033592
223.205.219.67	4	1.033592

```
index=security sourcetype=linux_secure
(fail* OR invalid)
| top src_ip
```

top Command

- By default, returns top 10 results
- Automatically returns count and percent columns
- Common constraints: limit countfield showperc
- top command with limit=20 is automatically added to your search string when you click Top values in a field window

top Command – Renaming countfield Display

- By default, the display name of the countfield is count
- countfield =*string* renames the field for display purposes

```
index=network sourcetype=cisco_wsa_squid
| top cs_username x_webcat_code_full limit =3
  countfield="Total Viewed" showperc=f
```

rare Command

- The rare command returns the least common field values of a given field in the results
- Options are identical to the `top` command

```
index=sales sourcetype=vendor_sales
| rare product_name showperc=f limit=1
```

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾ Format Preview ▾

product_name	count
Manganiello Bros. Tee	1

stats Command

- stats enables you to calculate statistics on data that matches your search criteria
- Common functions include:
  - count – returns the number of events that match the search criteria
  - distinct_count, dc – returns a count of unique values for a given field
  - sum – re turns a sum of numeric values
  - avg – re turns an average of numeric values
  - list – lists all va lues of a given field
  - values – lis ts unique values of a give n fie ld

stats Command – count

- count returns the number of matching events based on the current search criteria
- Us e the as c laus e to rename the count field

```
index=security  sourcetype=linux_secure
(invalid  OR  failed)
| stats  count
```

```
index=security  sourcetype=linux_secure
(invalid  OR  failed)
| stats  count  as  "Potential  Issues"
```

stats Comm and – by *fields*

```
index=security  sourcetype=linux_secure
| stats  count  by  user,  app,  vendor_action
```

- by clause returns a count for each value of a named field or set of fields
- Can use any number of fields in the by *field* list

user	app	vendor_action	count
administrator	sshd	Failed	1
agushto	sshd	Failed	1
backup	sshd	Failed	1
bin	sshd	Failed	2
brian	sshd	Failed	1
db	sshd	Failed	2
db2fenc1	sshd	Failed	2
db4	sshd	Failed	1
dba	sshd	Failed	1
demon	sshd	Failed	1

stats Command – distinct_count(*field*)

- distinct_count() or dc() provides a count of how many unique values there are for a given field in the result set
- This example counts how many unique values for s_hostname

```
index=network sourcetype=cisco_wsa_squid
| stats dc(s_hostname) as "Websites visited:"
```

stats Comm and – sum(*field*) – (co nt.)

A single stats command can have multiple functions

The by clause is applied to both functions

sort Total Sales in descending order

```
index=sales sourcetype=vendor_sales
| stats count(price) as "Units Sold"
  sum(price) as "Total Sales" by product_name
| sort -"Total Sales"
```

stats Comm and – avg(*field*)

- The avg function provides the average numeric value for the given numeric field
- An event is not considered in the calculation if it:
  - Does not have the field
  - Has an invalid value for the field

```
index=network sourcetype=cisco_wsa_squid
| stats avg( sc_by tes) as "Average By tes"
  by usage
```

stats Command – list(*field*)

- list function lists all field values for a given field
- This example lists the websites visited by each employee
  - Security logs generate an event for each network request
    - The same hostname appears multiple times
  - To return a list of "unique" field values, use the values function

```
index=network  sourcetype=cisco_wsa_squid
| stats  list(s_hostname)  as  "Websites
  visited:"  by  cs_username
```

cs_username	Websites visited:
	www.filmschoolrejects.com
apucci@buttercupgames.com	www.zimbio.com
arangel@buttercupgames.com	www.cnet.com
basselin@buttercupgames.com	www.americangangster.net www.americangangster.net www.americangangster.net www.blossomfloristla.com 84654321.cn
bgenin@buttercupgames.com	www.ambrosiasw.com www.ambrosiasw.com www.ambrosiasw.com

stats Comm and – values(*field*)

```
index=security  sourcetype=linux_secure  fail*
 | stats  values(user)  as  "User  Names",
    count(user)  as  Attempts  by  src_ip
```

values function lists unique values for the specified field

src_ip	User Names	Attempts
107.3.146.207	administrator pat uni	3
109.169.32.135	harrypotter irc	2
110.138.30.229	daemon	1
111.161.27.20	administrator daemon games	3
112.111.162.4	noone	1

Formatting stats Tables

- Tables created with stats commands can be formatted
- Color code data in each column, based on rules you define
- Add number formatting (e.g. currency symbols, thousands separators)
- Can also format data on a per-column basis by clicking the icon above that column

product_name	Units Sold	Total Sales
Benign Space Debris	16	399.84
Curling 2014	35	699.65
Dream Crusher	23	919.77
Final Sequel	27	674.73

Formatti ng stats Tables – Exam ples

product_name	Units Sold	Total Sales
Benign Space Debris	16	399.84
Curling 2014	35	699.65
Dream Crusher	23	919.77
Final Sequel	27	674.73
Fire Resistance Suit of Provolone	17	67.83
Holy Blade of Gouda	44	263.56

Total Sales
£ 399.84
£ 699.65
£ 919.77
£ 674.73
£ 67.83
£ 263.56
£ 999.75
£ 359.64

Creating Reports and Dashboards

What Are Reports?

- Reports are saved searches
- Reports can show events, statistics (tables), or visualizations (charts)
- Running a report returns fresh results each time you run it
- Statistics and visualizations allow you to drill down by default to see the underlying events
- Reports can be shared and added to dashboards

Smart Naming

- Before you begin using Splunk on the job, define a naming convention so you can always find your reports and tell them apart
- For example, you can create something simple like this:
  - <group>_<object>_<description>

    group : the name of the group or department using the knowledge object such as sales, IT, finance, etc.

    object : report, dashboard, macro, etc.

    description : WeeklySales, FailedLogins, etc.
  - Using this example, a quarterly sales report can be identified as:

    Sales_Report_QuarterlySalesRevenue

Running Reports

- Click **Reports**, then click the report title to run it
  - The report runs using the time range that was specified when it was saved
- Use the time range picker to change the time range of the report (if available)

Creating Tables and Visualizations

Three main methods to create tables and visualizations in Splunk are:

1. Select a field from the fields sidebar and choose a report to run
2. Use the Pivot interface
   - Start with a dataset

     or
   - Start with Instant Pivot
   - See Module 11 in this presentation for more information about Pivot
3. Use the Splunk search language transforming commands in the Search bar

Viewing Tables and Visualizations

- Statistical reports leverage Splunk's built-in visualizations or table format
- These views give you insights into your organization’s data

Creating Reports From the Field Window

- Numeric fields: choose from six report types with mathematical functions, such as average, maximum value, and minimum value
- This example generates a report that shows the average over time
  - This is known as a **timechart**

Creating a Top Values Report

- For alphanumeric character fields, there are only 3 available reports
- In this example, you want a report that shows the top **categories** purchased

1. Run basic search: sourcetype=access_combined status=200 action=purchase
2. Click the **categoryId** field
3. Click **Top values**

Creating a Top Values Report (cont.)

4. The top command with limit=20 i s added to the search s tri ng
5. A bar chart is returned on the Visualizations tab, displaying the top categories purchased

Changing the Visualization

- Select a visualization from the visualization type dropdown menu
- In this example, the column chart is changed to a pie chart

Changing the Visualization Format

- The **Format** menu allows you to change formatting options
- For example, for bar and column charts:
  - The **General** tab allows you to change Stack and Multi-series modes
  - The **X-Axis** and **Y-Axis** tabs allow you to change the axis labels and orientation
  - **Chart Overlay** allows you to add context to the chart by overlaying other field values

  - The **Legend** tab allows you to position the visualization legend as desired
  - **Stack Mode** allows you to stack colors to improve column chart readability when several colors are involved

Changing the Visualization Format (cont.)

- Show Data Values determines whether to show data values in the visualization
- If Min/Max is selected, data is only shown on the bars containing the minimum and maximum values

Viewing Results as a Table

Switch to the **Statistics** tab to view the results as a table

Events | Patterns | Statistics (7) | Visualization

20 Per Page ▾ | Format | Preview ▾

categoryId	count	percent
STRATEGY	900	30.622661
ARCADE	554	18.849949
ACCESSORIES	409	13.916298
TEE	385	13.099694
SHOOTER	282	9.595100
SIMULATION	269	9.152773
SPORTS	140	4.763525

Using the Data Overlay Format

- **Heat map** highlights outstanding values

- **High and low values** highlights max and min of non zero values

What Is a Dashboard?

- A dashboard consists of one or more panels displaying data visually in a useful way – such as events, tables, or charts
- A report can be used to create a panel on a dashboard

Adding a Report to a Dashboard

In the report, click Add to Dashboard to begin

Why Create Panels from Reports?

- It is efficient to create most dashboard panels based on reports because
  - A single report can be used across different dashboards
  - This links the report definition to the dashboard
- Any change to the underlying report affects every dashboard panel that utilizes that report

Editing Panels

- After saving the panel, a window appears from which you can view the updated dashboard
- Click Edit to customize the dashboard

Editing Panel Layout

Click on the dotted bar on a panel to drag the panel to a new location

More Options icon (discussed on next slide)

Drilldown from Visualization to Search

Once drilldown option is set, click an object in a chart or table to see its underlying events in Search view

Export a Dashboard

Dashboards can be exported as PDF or printed

Pivot & Datasets

Selecting a Dataset

1. From the Search & Reporting app, select the **Datasets** tab
   - Displays a list of available lookup table files ("lookups") and data models
   - Each lookup and data model represent a specific category of data
   - Prebuilt lookups and data models make it easier to interact with your data

2. Click **Explore > Visualize with Pivot**

Opening in Pivot

- The Pivot automatically populates with a count of events for the selected object
- In this example, it shows all successful purchase requests for all time

Selecting a Time Range

- The default is **All time**
- Click the pencil icon to select the desired time range
- The pivot runs immediately upon selecting the new time range

Split Rows

- Click + under **Split Rows** for a list of available attributes to populate the rows
- In this example, the rows are split by the **category** attribute, which lists:
  - Each game category on a separate row
  - A count of successful requests for each game category

Split Rows (cont.)

- Once selected, you can:
  - Modify the label
  - Change the sort order

    Default – sorts by the field value in ascending order

    Ascending - sorts by the count in ascending order

    Descending – sorts by the count in descending order
  - Define maximum # of rows to display
- Click **Add to Table** to view the results

Results

categories

count by category

To format the results, click here

Updated Results (with Total)

Filtered Pivot

- The ACCESSORIES category is filtered out
- All the other categories remain

category	Benign Space Debris	Curling 2014	Dream Crusher	Final Sequel	Manganiello Bros.	Manganiello Bros. Tee	Mediocre Kingdoms	Orvil the Wolverine	Puppies vs. Zombies	SIM Cubicle	World of Cheese	World of Cheese Tee	ALL
STRATEGY	0	0	1322	1130	0	0	1320	0	968	0	0	0	4740
ARCADE	827	0	0	0	1266	0	0	888	0	0	0	0	2981
TEE	0	0	0	0	0	1186	0	0	0	0	0	917	2103
SHOOTER	0	0	0	0	0	0	0	0	0	0	1494	0	1494
SIMULATION	0	0	0	0	0	0	0	0	0	1385	0	0	1385
SPORTS	0	872	0	0	0	0	0	0	0	0	0	0	872
	827	872	1322	1130	1266	1186	1320	888	968	1385	1494	917	13575

Select a Visualization Format

You can display your pivot as a table or a visualization, such as a column chart

Saving a Pivot

When you click **View**, the report is displayed with a Time Range Picker (if that's the option you chose)

Mouse Actions

- Mouse over an object to reveal its details
- If drilldown is enabled, it is possible to click on the object to expose the underlying search

Instant Pivot Overview

- Instant pivot allows you to utilize the pivot tool without a preexisting data model
  - Instant pivot creates an underlying data model utilizing the search criteria entered during the initial search
- To create an Instant Pivot
  1. Execute a search (search criteria only, no search commands)
  2. Click the **Statistics** or **Visualization** tab
  3. Click the **Pivot** icon
  4. Select the fields to be included in the data model object
  5. Create the pivot (table or chart)

Creating and Using Lookups

What Is a Lookup?

- Sometimes static (or relatively unchanging) data is required for searches, but isn't available in the index
- Lookups pull such data from standalone files at search time and add it to search results

What Is a Lookup? (cont.)

- Lookups allow you to add more fields to your events, such as:
  - Descriptions for HTTP status codes (“File Not Found”, “Service Unavailable”)
  - Sale prices for products
  - User names, IP addresses, and workstation IDs associated with RFIDs
- After a lookup is configured, you can use the lookup fields in searches
- The lookup fields also appear in the Fields sidebar
- Lookup field values are case sensitive by default

A Sample Lookup File

- This example displays a lookup .csv file use d to associate p roduct information with productId
- First row represents field names (header)

  productId,
  product_name,
  categoryId, price,
  sale_price, Code
- Th e productId fie ld ex is ts in th e access_combined events
  - This is the **input** field
- All of the fields listed above are available to search after the lookup is defined
  - These are the **output** fields

```
  GNU nano 2.3.1              File: products.csv

productId,product_name,categoryId,price,sale_price,Code
DB-SG-G01,Mediocre Kingdoms,STRATEGY,24.99,19.99,A
DC-SG-G02,Dream Crusher,STRATEGY,39.99,24.99,B
FS-SG-G03,Final Sequel,STRATEGY,24.99,16.99,C
WC-SH-G04,World of Cheese,SHOOTER,24.99,19.99,D
WC-SH-T02,World of Cheese Tee,TEE,9.99,6.99,E
PZ-SG-G05,Puppies vs. Zombies,STRATEGY,4.99,1.99,F
CU-PG-G06,Curling 2014,SPORTS,19.99,16.99,G
MB-AG-G07,Manganiello Bros.,ARCADE,39.99,24.99,H
MB-AG-T01,Manganiello Bros. Tee,TEE,9.99,6.99,I
FI-AG-G08,Orvil the Wolverine,ARCADE,39.99,24.99,J
BS-AG-G09,Benign Space Debris,ARCADE,24.99,19.99,K
SC-MG-G10,SIM Cubicle,SIMULATION,19.99,16.99,L
WC-SH-A01,Holy Blade of Gouda,ACCESSORIES,5.99,2.99,M
WC-SH-A02,Fire Resistance Suit of Provolone,ACCESSORIES,3.99,1.99,N
```

input lookup Command

- Use the inputlookup command to load the results from a specified static lookup
- Useful to:
  - Review the data in the .csv file
  - Validate the lookup

Code	categoryId	price	productId	product_name	sale_price
A	STRATEGY	24.99	DB-SG-G01	Mediocre Kingdoms	19.99
B	STRATEGY	39.99	DC-SG-G02	Dream Crusher	24.99
C	STRATEGY	24.99	FS-SG-G03	Final Sequel	16.99
D	SHOOTER	24.99	WC-SH-G04	World of Cheese	19.99
E	TEE	9.99	WC-SH-T02	World of Cheese Tee	6.99
F	STRATEGY	4.99	PZ-SG-G05	Puppies vs. Zombies	1.99
G	SPORTS	19.99	CU-PG-G06	Curling 2014	16.99
H	ARCADE	39.99	MB-AG-G07	Manganiello Bros.	24.99
I	TEE	9.99	MB-AG-T01	Manganiello Bros. Tee	6.99
J	ARCADE	39.99	FI-AG-G08	Orvil the Wolverine	24.99
K	ARCADE	24.99	BS-AG-G09	Benign Space Debris	19.99
L	SIMULATION	19.99	SC-MG-G10	SIM Cubicle	16.99
M	ACCESSORIES	5.99	WC-SH-A01	Holey Blade of Gouda	2.99
N	ACCESSORIES	3.99	WC-SH-A02	Fire Resistance Suit of Provolone	1.99

lookup Command

- If a lookup is not configured to run automatic ally, us e the lookup command in your search to use the lookup fields
- The OUTPUT argument is optional
  - If OUTPUT not specified, lookup returns all the fields from the lookup table except the match fields
  - If OUTPUT is specified, the fields overwrite existing fields
- The output lookup fields exist only for the current search
- Use OUTPUTNEW when you do not want to overwrite existing fields

Using the lookup Comm and

Using an Automatic Lookup

To use an automatic lookup, specify the output fields in your search

```
index=web sourcetype=access* action=purchase productId=*
| stats sum(price) as sales by productId product_name
```

Last 24 hours

i	Time	Event
>	1/9/18 10:56:54.000 PM	203.45.206.135 - - [09/Jan/2018:22:56:54] "POST /cart.do?action=purchase&itemId=EST-19&JSESSIONID=SD5SL5FF10ADFF4951 HTTP 1.1" 200 1427 "http://www.buttercupgames.com/cart.do?action=addtocart&itegoryId=STRATEGY&productId=DC-SG-G02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) Ap (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 314 host = www4 productId = DC-SG-G02 source = /opt/log/www1/access.log sourcetype = acce
>	1/9/18 10:56:08.00	203.45.206.135 - - [09/Jan/2018:22:56:08] "POST /cart.do?action=purchase&itemId=EST-7&JSE art&it AppleW = access_combined

Events Patterns **Statistics (14)** Visualization

20 Per Page ▾ Format Preview ▾

productId	product_name	sales
BS-AG-G09	Benign Space Debris	274.89
CU-PG-G06	Curling 2014	319.84
DB-SG-G01	Mediocre Kingdoms	499.80
DC-SG-G02	Dream Crusher	879.78
FI-AG-G08	Orvil the Wolverine	479.88

price	productId	product_name
24.99	DB-SG-G01	Mediocre Kingdoms
39.99	DC-SG-G02	Dream Crusher
24.99	FS-SG-G03	Final Sequel
24.99	WC-SH-G04	World of Cheese
9.99	WC-SH-T02	World of Cheese Tee

Time-based Lookups

- If a field in the lookup table represents a timestamp, you can create a time-based lookup
- In this example, the search retrieved events for December and January and calculated the sales based on the correct unit price for those dates

product_time	productId	product_name	categoryId	price	sale_price
12/1/17	DB-SG-G01	Mediocre Kingdoms	STRATEGY	24.99	19.99
12/1/17	DC-SG-G02	Dream Crusher	STRATEGY	39.99	24.99
12/1/17	FS-SG-G03	Final Sequel	STRATEGY	24.99	16.99
12/1/17	WC-SH-G04	World of Cheese	SHOOTER	24.99	19.99
12/1/17	WC-SH-T02	World of Cheese Tee	TEE	9.99	6.99
12/1/17	PZ-SG-G05	Puppies vs. Zombies	STRATEGY	4.99	1.99
12/1/17	CU-PG-G06	Curling 2014	SPORTS	19.99	16.99
12/1/17	MB-AG-G07	Manganiello Bros.	ARCADE	39.99	24.99
12/1/17	MB-AG-T01	Manganiello Bros. Tee	TEE	9.99	6.99
12/1/17	FI-AG-G08	Orvil the Wolverine	ARCADE	39.99	24.99
12/1/17	BS-AG-G09	Benign Space Debris	ARCADE	24.99	19.99
12/1/17	SC-MG-G10	SIM Cubicle	SIMULATION	19.99	16.99
12/1/17	WC-SH-A01	Holey Blade of Gouda	ACCESSORIES	5.99	2.99
12/1/17	WC-SH-A02	Fire Resistance Suit of Provolone	ACCESSORIES	3.99	1.99
1/1/18	DB-SG-G01	Mediocre Kingdoms	STRATEGY	24.99	19.99
1/1/18	DC-SG-G02	Dream Crusher	STRATEGY	40.99	24.99
1/1/18	FS-SG-G03	Final Sequel	STRATEGY	25.99	16.99
1/1/18	WC-SH-G04	World of Cheese	SHOOTER	24.99	19.99
1/1/18	WC-SH-T02	World of Cheese Tee	TEE	9.99	6.99
1/1/18	PZ-SG-G05	Puppies vs. Zombies	STRATEGY	4.99	1.99
1/1/18	CU-PG-G06	Curling 2014	SPORTS	20.99	16.99
1/1/18	MB-AG-G07	Manganiello Bros.	ARCADE	39.99	24.99
1/1/18	MB-AG-T01	Manganiello Bros. Tee	TEE	9.99	6.99
1/1/18	FI-AG-G08	Orvil the Wolverine	ARCADE	39.99	24.99
1/1/18	BS-AG-G09	Benign Space Debris	ARCADE	25.99	19.99
1/1/18	SC-MG-G10	SIM Cubicle	SIMULATION	19.99	16.99
1/1/18	WC-SH-A01	Holey Blade of Gouda	ACCESSORIES	6.99	2.99
1/1/18	WC-SH-A02	Fire Resistance Suit of Provolone	ACCESSORIES	4.99	1.99

product_name	Month	price	count	sales	SubTotal Sales
Benign Space Debris	Dec	24.99	828	42,211.44	
Benign Space Debris	Jan	25.99	646	32,933.08	
Benign Space Debris Subtotal					150,289.04
Curling 2014	Dec	19.99	868	35,570.64	
Curling 2014	Jan	20.99	620	25,407.60	
Curling 2014 Subtotal					121,956.48
Dream Crusher	Dec	39.99	1,360	110,132.80	
Dream Crusher	Jan	40.99	1,004	81,303.92	
Dream Crusher Subtotal					382,873.44
Final Sequel	Dec	24.99	1,200	61,176.00	
Final Sequel	Jan	25.99	812	41,395.76	
Final Sequel Subtotal					205,143.52