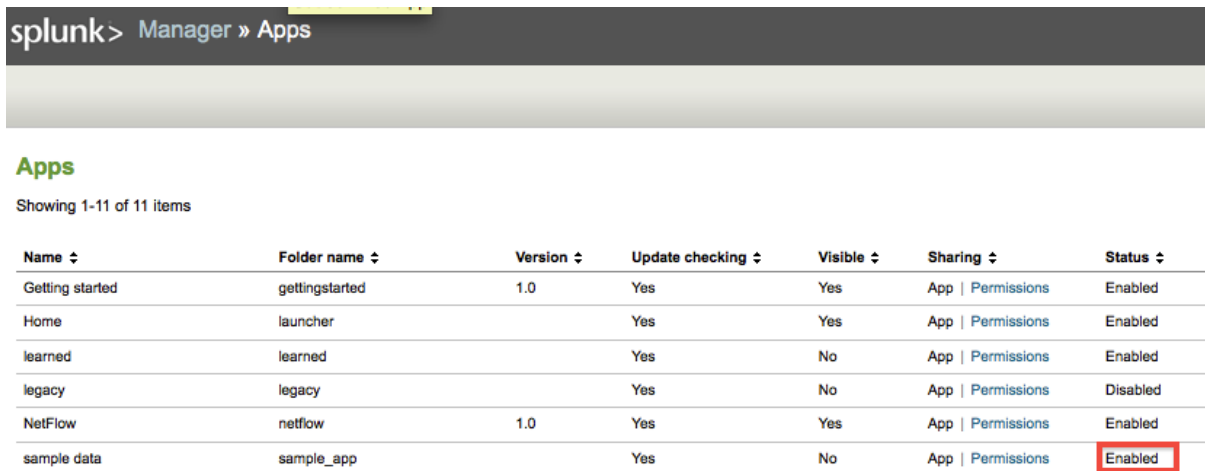


Splunk Interactive Tutorial

Task 1 – Create a Dashboard for mail

We're using Splunk's built in Demo mail log data to produce a dashboard.

1. If it's not already enabled, please enable the sample data, via Manager -> Apps:



splunk> Manager » Apps

Apps

Showing 1-11 of 11 items

Name	Folder name	Version	Update checking	Visible	Sharing	Status
Getting started	gettingstarted	1.0	Yes	Yes	App Permissions	Enabled
Home	launcher		Yes	Yes	App Permissions	Enabled
learned	learned		Yes	No	App Permissions	Enabled
legacy	legacy		Yes	No	App Permissions	Disabled
NetFlow	netflow	1.0	Yes	Yes	App Permissions	Enabled
sample data	sample_app		Yes	No	App Permissions	Enabled

2. Next let's run a quick search to see the data we are using. Make sure you check out the fields extracted and that Field Discovery is on:



Search | Actions

index=sample from=*

my search history
index=sample from="*" to="*"

my command history | more »

Retrieves events from index(es) and filter them using keywords or key/value expressions.

examples

Keep only search results that have the specified "src" or "dst" values.
src="10.9.165.*" OR dst="10.9.165.8"

Search for events with either codes 10 or 29, and a host that isn't "localhost" and an xqp that is greater than 5
(code=10 OR code=29) host!=""localhost" xqp>5

Search for events with "404" and from host "webserv1"
404 host="webserv1"

Field discovery: On

Selected fields (3)
host (1)
source (2)
sourcetype (1)

1 4/8/11 11:25:11.000 AM Apr 8 11:25:11 splunk3 sendmail[4668]: n38IP85B004668: from=<spammer@spandomain.com>, size=1032, class=0, nrpts=1, msgid=<200904081825.n38IP8M2021146@virt2.int.splunk.com>, proto=ESMTP, daemon=MTA, relay=[64.127.105.34]
host=logs-01.asia.local | sourcetype=sendmail | source=opt/welovesplunk/splunk/etc/apps/sample_app/logs/maillog

Build report

- Now we can use the Build Report Link to go to the report builder and work on what we want to show on the dashboard, which is the total data volume per sender:

1: Define report content

Search | Define report using search language

index=sample from=* | timechart sum(size) by from

Time range
All time

Report Data

Report type: Values over time

Report will display: Single field split by another field

Fields

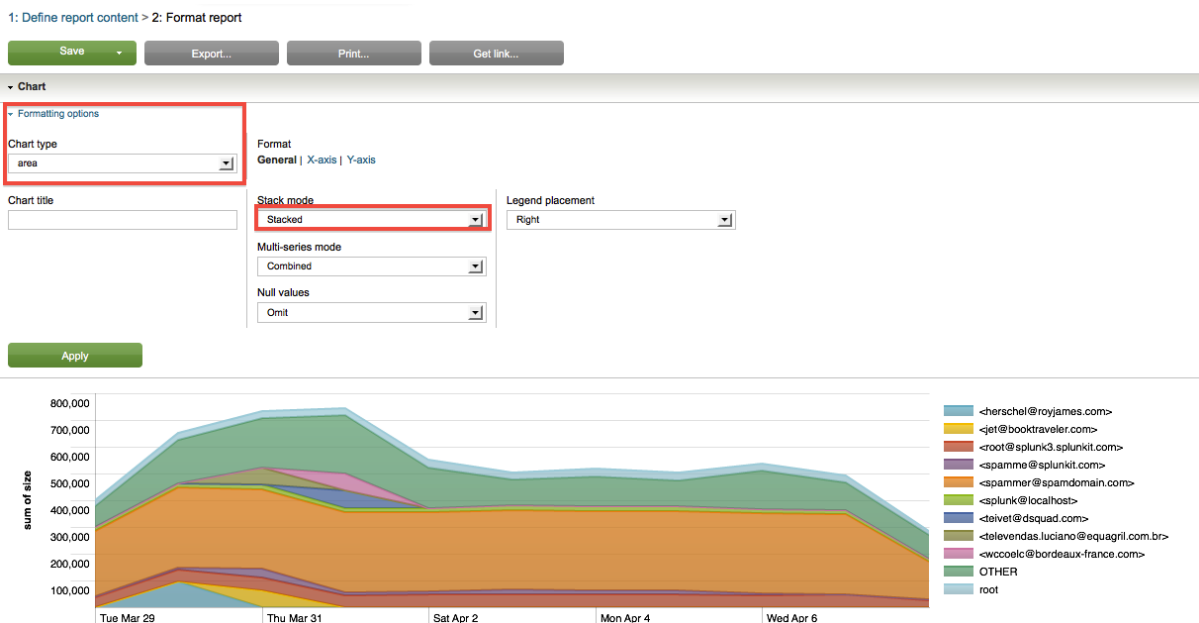
Show: Sum of size (n)

split by: from

▶ Set span for time axis intervals (for example: every 10 minutes)

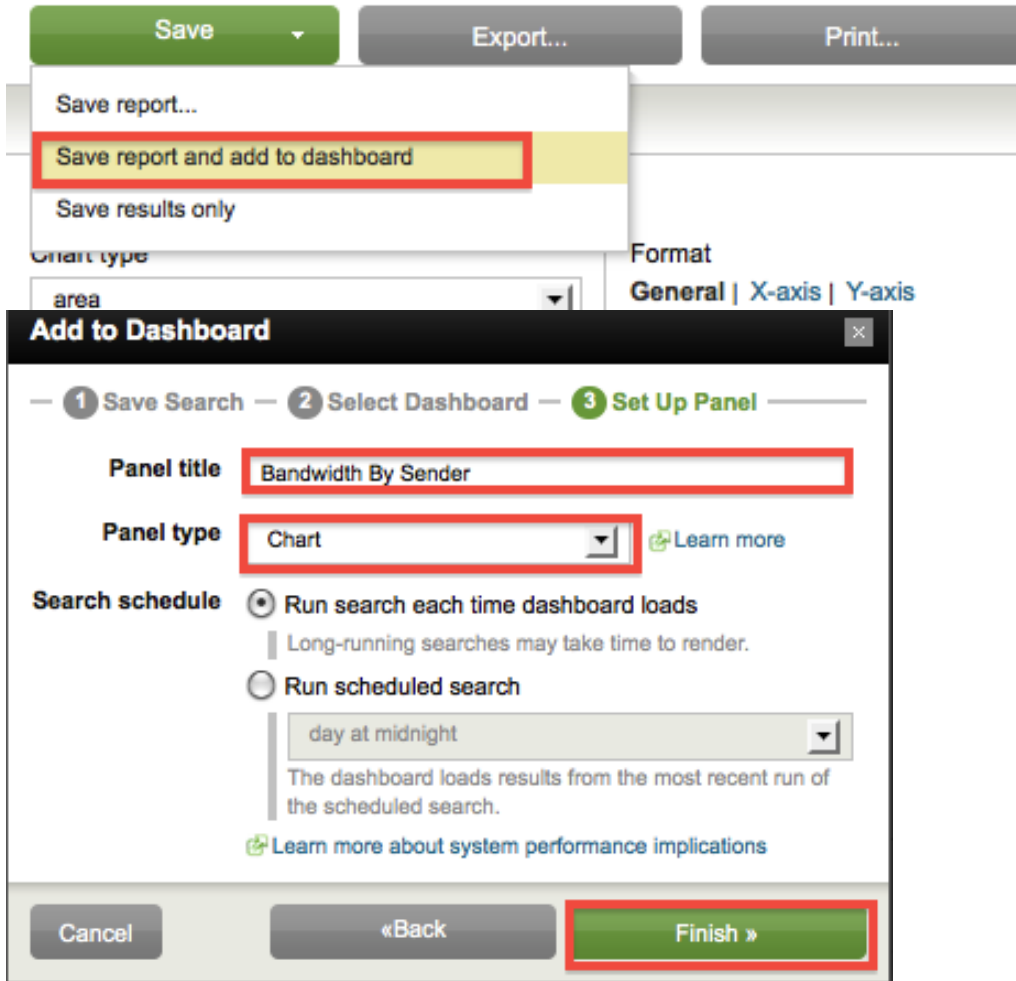
Next Step: Format Report

- Now we have selected our data, we can format it as a stacked area graph to show total volume easily:



5. We now want to save our report and add it to a new dashboard, give your search a name, and name a new dashboard, then add your panel as a chart:

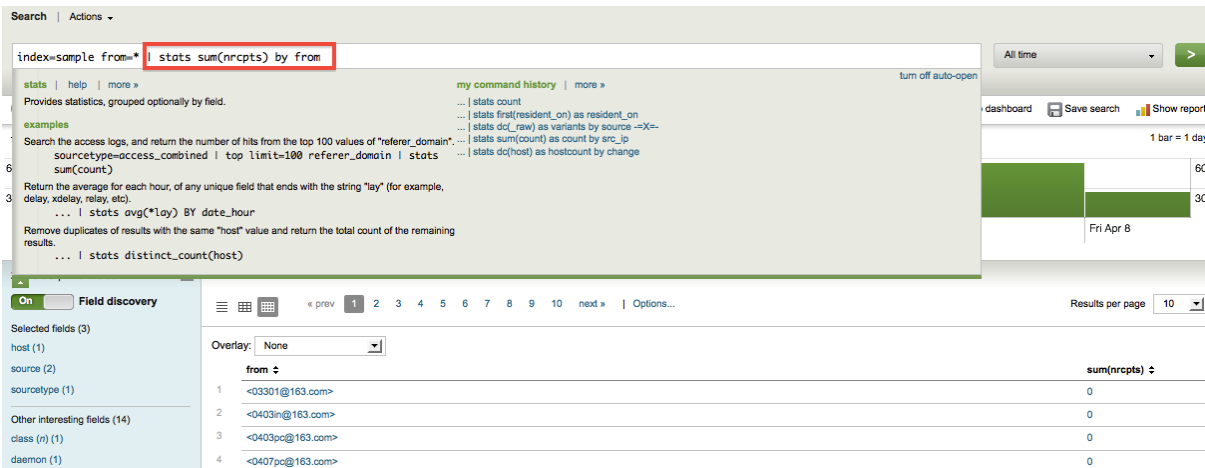
1: Define report content > 2: Format report



The screenshot shows the Splunk interface. At the top, there are buttons for 'Save', 'Export...', and 'Print...'. The 'Save' button is highlighted with a green background. A dropdown menu is open under 'Save', with the option 'Save report and add to dashboard' highlighted in yellow and a red border. Below this, there are options for 'Chart type' (set to 'area') and 'Format' (set to 'General | X-axis | Y-axis').

The 'Add to Dashboard' dialog box is open, showing three steps: 1. Save Search, 2. Select Dashboard, and 3. Set Up Panel. The 'Set Up Panel' step is active. The 'Panel title' field is set to 'Bandwidth By Sender'. The 'Panel type' dropdown is set to 'Chart'. The 'Search schedule' is set to 'Run search each time dashboard loads'. The 'Finish' button is highlighted with a red border.

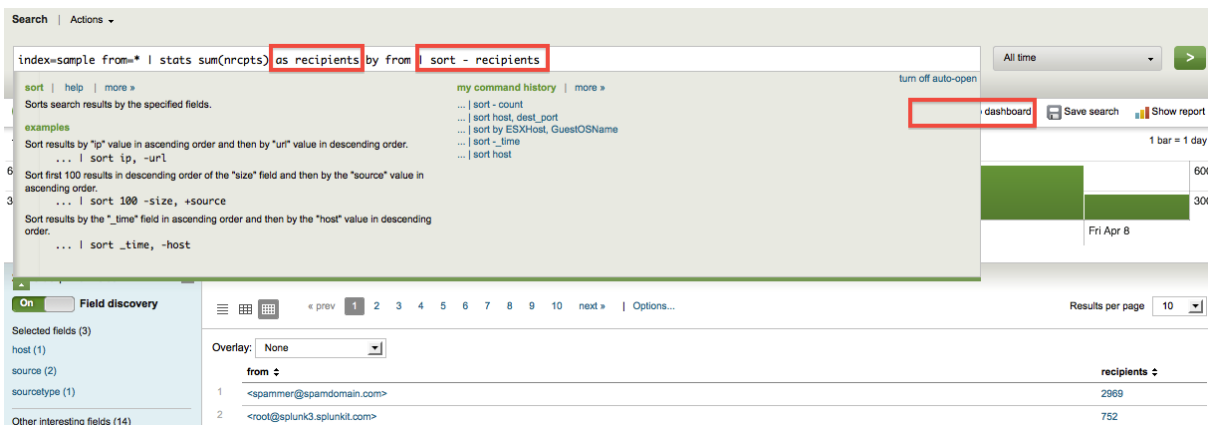
6. We now return to our search and want to get an idea of how many mails are actually landing in inboxes, rather than distinct emails sent, using the stats command



The screenshot shows the Splunk search interface. The search bar contains the query: `index=sample from=* | stats sum(nrpts) by from`. A dropdown menu for the `stats` command is open, showing examples of its usage. The results table below the search bar shows the following data:

from	sum(nrpts)
1 <03301@163.com>	0
2 <0403in@163.com>	0
3 <0403pc@163.com>	0
4 <0407pc@163.com>	0

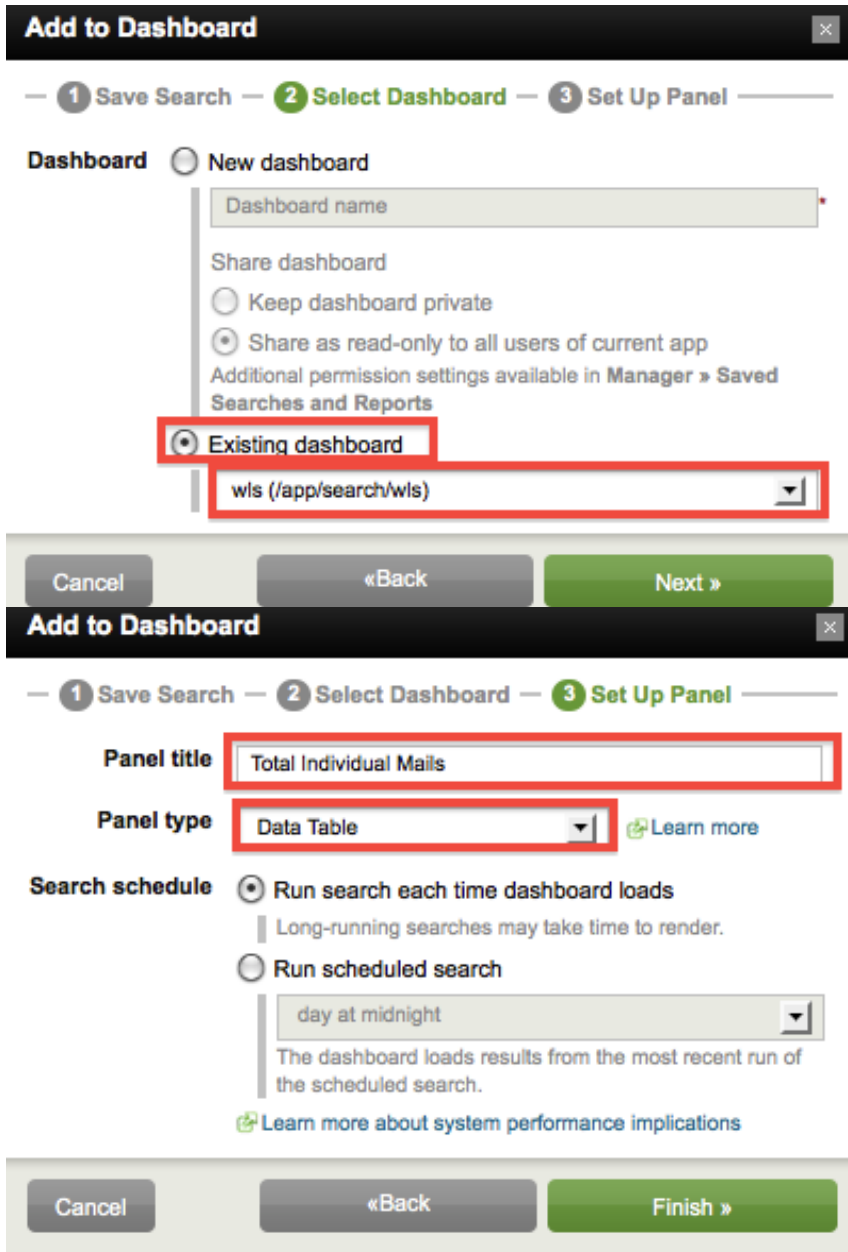
7. It's much more useful to us to show the field with a friendly name, like recipients, and also to sort to show the top sender.



The screenshot shows the Splunk search interface with the search query: `index=sample from=* | stats sum(nrpts) as recipients by from | sort - recipients`. A dropdown menu for the `stats` command is open, showing examples of its usage. The results table below the search bar shows the following data:

from	recipients
1 <spammer@spamdmain.com>	2969
2 <root@splunk3.splunkit.com>	752

8. We add this to the existing dashboard as before, this time selecting our existing dashboard:



Add to Dashboard

— 1 Save Search — 2 Select Dashboard — 3 Set Up Panel —

Dashboard New dashboard

Dashboard name

Share dashboard

Keep dashboard private

Share as read-only to all users of current app

Additional permission settings available in [Manager](#) » [Saved Searches and Reports](#)

Existing dashboard

wls (/app/search/wls)

Cancel «Back Next »

Add to Dashboard

— 1 Save Search — 2 Select Dashboard — 3 Set Up Panel —

Panel title Total Individual Mails

Panel type Data Table [Learn more](#)

Search schedule Run search each time dashboard loads

Long-running searches may take time to render.

Run scheduled search

day at midnight

The dashboard loads results from the most recent run of the scheduled search.

[Learn more about system performance implications](#)

Cancel «Back Finish »

9. For the next report we need to extract a new field (using the rex regular expression command) and use a number of stats functions to produce a comprehensive report for each sender domain:

```
index=sample from=* | rex field=from "@(?<domain>.+)" | stats values(from) sum(nrpts) as recipients sum(size) as bytes by domain
```

10. Now we can save our work and view the dashboard:

Add to Dashboard

1 Save Search — 2 Select Dashboard — 3 Set Up Panel

Panel title


Panel type [Learn more](#)

Search schedule Run search each time dashboard loads
Long-running searches may take time to render.

Run scheduled search

The dashboard loads results from the most recent run of the scheduled search.
[Learn more about system performance implications](#)

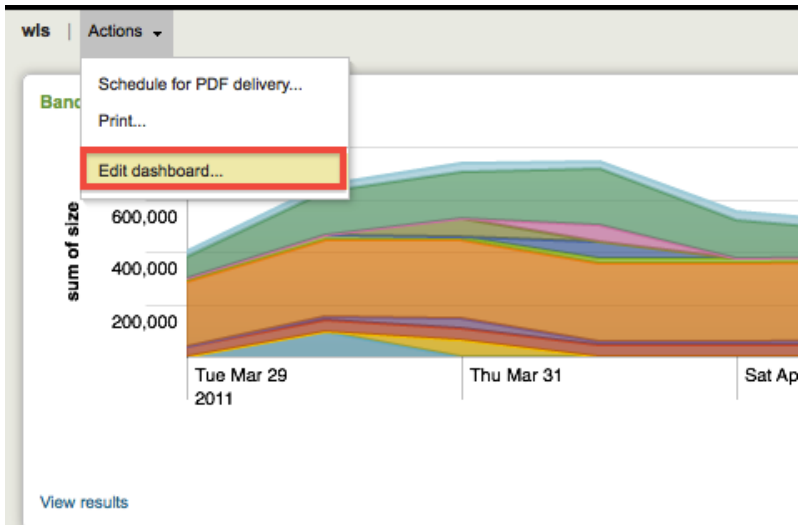
Add to Dashboard

 **Dashboard saved successfully**

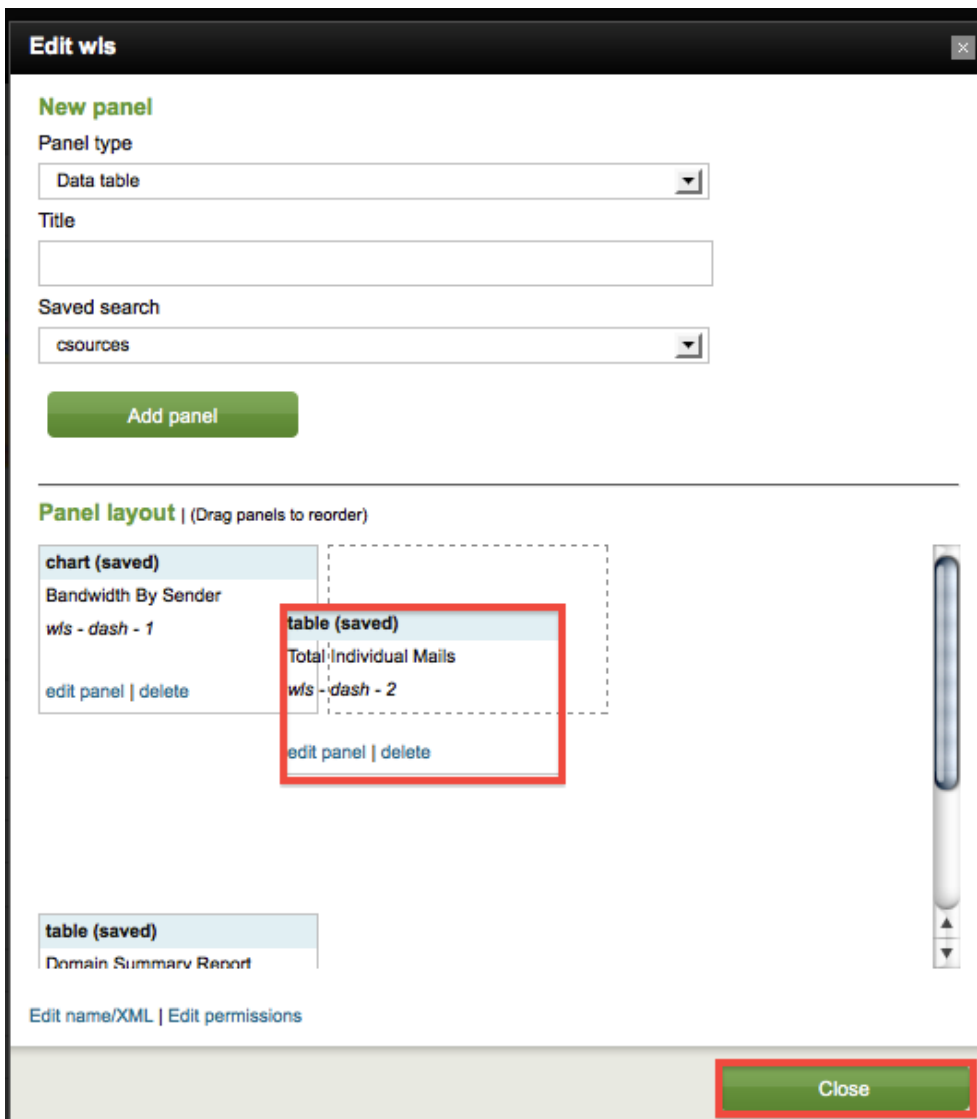
Modify the saved search at [Manager » Searches and Reports » wls - dash - 3.](#)

[View dashboard | wls.](#)

11. It's good, but we can make it better by changing the layout, via Edit Dashboard:



12. Drag and drop to form a better layout:



The screenshot shows the 'Edit wls' dialog box. It has a title bar 'Edit wls' with a close button. The main content is divided into two sections: 'New panel' and 'Panel layout'.
 In the 'New panel' section, there is a 'Panel type' dropdown set to 'Data table', a 'Title' text input field, and a 'Saved search' dropdown set to 'csources'. Below this is a green 'Add panel' button.
 The 'Panel layout' section is titled '(Drag panels to reorder)'. It contains several panels:
 - A 'chart (saved)' panel titled 'Bandwidth By Sender' with 'wls - dash - 1' below it and 'edit panel | delete' links.
 - A 'table (saved)' panel titled 'Total Individual Mails' with 'wls - dash - 2' below it and 'edit panel | delete' links. This panel is highlighted with a red border.
 - A 'table (saved)' panel titled 'Domain Summary Report' at the bottom.
 At the bottom right of the dialog is a green 'Close' button, also highlighted with a red border.

13. You can still interact with your finished dashboard; we could have presorted the domain report, but you can click on any of the column headings to sort it for your needs:

View results

Domain Summary Report refreshed: today at 1:44:46 PM.

	domain ↕	values(from) ↕	recipients ↕	bytes ↕
1	spamdomain.com	<spammer@spamdomain.com>	2969	3062791
2	alerts.bounces.google.com	<-3-inbSRQKBq;NVVNSLHSLYeZ-UVYLWSINVVNSL_JVTZWHTTLZWSbURPa.JVT@alerts.bounces.google.com> <-3-VJRSRQKBm0RZZRWPLWPced-YZcPaWjRZZRWP.NZXdaLXXPdaWYVTe.NZX@alerts.bounces.google.com> <-30_VTJSRQKBuwUccUZSOZSfng-bcfSdZmUccUZS.QcagdOaaSgdZibYWWh.Qca@alerts.bounces.google.com> <-30eHUSRQKBIE3BB381x81EGF-ABE1C8L3BB381.zB9FCx991FC8HA75G.zB9@alerts.bounces.google.com> <-310XbSRQKBkiksskpiepivxw-rsvitp2ksskpi.gsqwteqiwpyromx.gsq@alerts.bounces.google.com>	129	655801

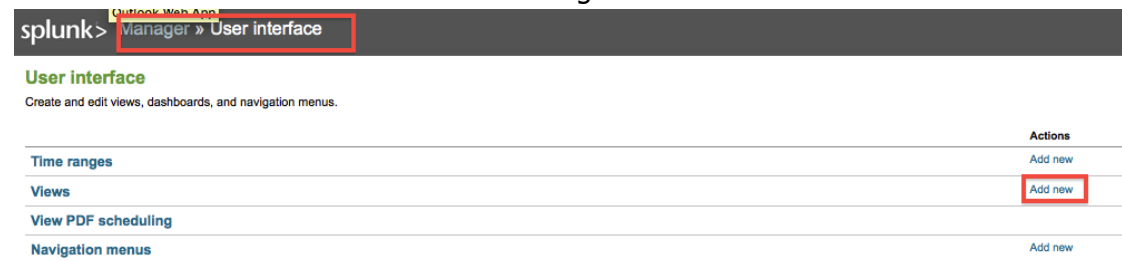
Task 2 – Simple Form Search

To define a form search is a little trickier, as we need to write some XML which defines our inputs, reports and how the two are connected.

We want to be able to search on the from address, and get details of:

- Mail volume over time
- Relay hosts used
- Mail size statistics

1. First we have to add a view in manager:

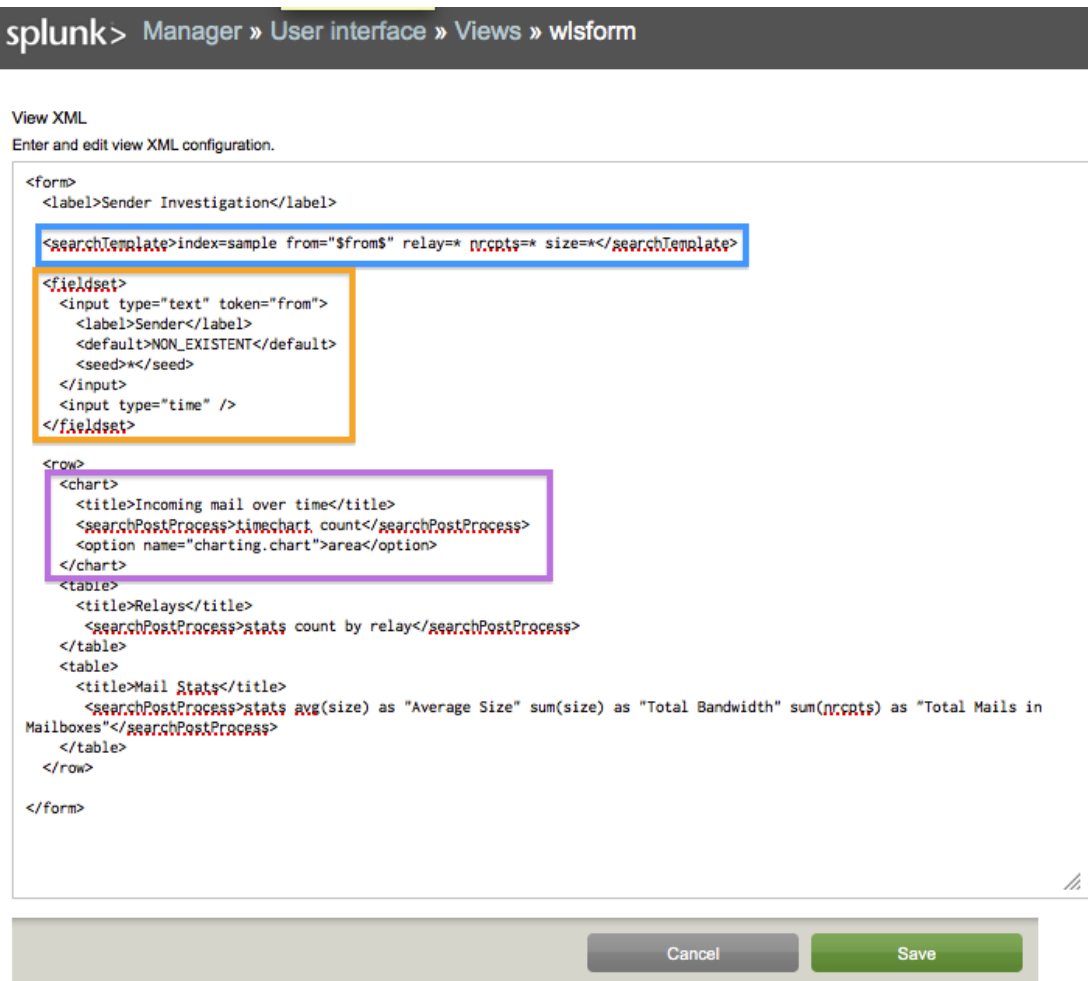


splunk> Outlook Web App
Manager » User interface

User interface
Create and edit views, dashboards, and navigation menus.

	Actions
Time ranges	Add new
Views	Add new
View PDF scheduling	
Navigation menus	Add new

2. Then we can define it in XML, The blue defines our search, the orange our form and the purple the output:



splunk> Manager » User interface » Views » wlsform

View XML
Enter and edit view XML configuration.

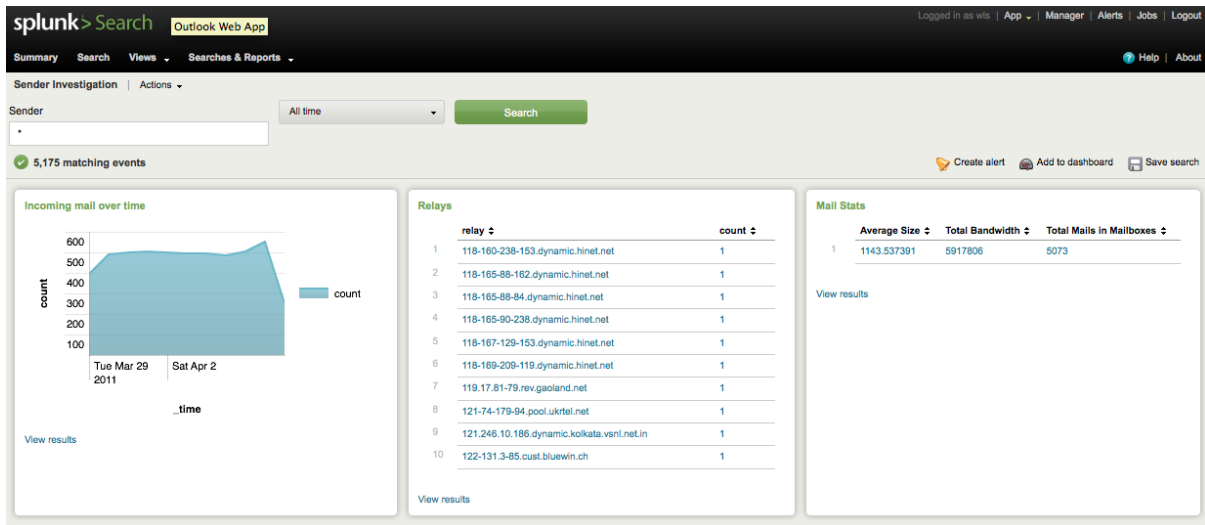
```

<form>
  <label>Sender Investigation</label>
  <searchTemplate>index=sample from="$from$" relay=* nrcnts=* size=*</searchTemplate>
  <fieldset>
    <input type="text" token="from">
      <label>Sender</label>
      <default>NON_EXISTENT</default>
      <seed></seed>
    </input>
    <input type="time" />
  </fieldset>
  <row>
    <chart>
      <title>Incoming mail over time</title>
      <searchPostProcess>timechart count</searchPostProcess>
      <option name="charting.chart">area</option>
    </chart>
    <table>
      <title>Relays</title>
      <searchPostProcess>stats count by relay</searchPostProcess>
    </table>
    <table>
      <title>Mail Stats</title>
      <searchPostProcess>stats avg(size) as "Average Size" sum(size) as "Total Bandwidth" sum(nrcnts) as "Total Mails in Mailboxes"</searchPostProcess>
    </table>
  </row>
</form>

```

Cancel Save

3. We can now view our form:



Resources

- Satisnet offer a range of Splunk Training courses, including the Searching and Reporting class which empowers users to make the most of Splunk's unique features. See more information at our website - http://satisnet.co.uk/training_splunk.htm. We also offer a Using and an Administrating course, as well as consultancy on all aspects of Splunk.
- If you want assistance to explore on your own Splunk instance, please email Duncan.Turnbull@satisnet.co.uk.