Network Tools - Feature #1706

Dashboard: traceroute

01/29/2017 05:59 AM - Luke Murphey

Status:	Closed	**Start date:**	01/28/2017
Priority:	Normal	**Due date:**	
Assignee:	Luke Murphey	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	0.5		

Description

Associated revisions

Revision 31 - 02/02/2017 03:42 AM - lmurphey

Initial version of traceroute view

Reference #1706

Revision 36 - 02/02/2017 06:31 AM - lmurphey

Including the dest info in the traceroute search output

Including the dest_ip and dest_name so that the traceroute dashboard can
display the information

Reference #1706

History

#1 - 01/31/2017 09:09 AM - Luke Murphey

Need to:

- Make sure bnf is accurate
- Show existing output in textbox of widget or display the dest
- Make sure drilldown uses the correct search

#2 - 01/31/2017 09:09 AM - Luke Murphey

- % Done changed from 0 to 70

#3 - 02/02/2017 06:55 AM - Luke Murphey

- % Done changed from 70 to 80

The traceroute dashboard isn't showing the correct cached results. They are not getting extracted properly.

#4 - 02/08/2017 06:15 AM - Luke Murphey

These two searches perform differently.

This works:

```
sourcetype="traceroute" unique_id=26ebc82b | rex field=_raw "rtt=\"(?<rtt>[.0-9]+)\"" max_match=5 | rex field=_raw "name=\"(?<name>[.0-9]+)\"" max_match=5 | rex field=_raw "ip=\"(?<ip>[.0-9]+)\"" max_match=5 | stats values(rtt) as rtt values(ip) as ip values(name) as name first(dest_host) as dest_host first(dest_ip) as dest_ip by hop | sort hop
```

This doesn't:

```
sourcetype=traceroute | head 1 | join unique_id max=100 [| search sourcetype=traceroute] | rex field=_raw "rtt=\"(?<rtt>[.0-9]+)\"" max_match=5 | rex field=_raw "name=\"(?<name>[.0-9]+)\"" max_match=5 | rex field=_raw "ip=\"(?<ip>[.0-9]+)\"" max_match=5 | stats values(rtt) as rtt values(ip) as ip values(name) as name first(dest_host) as dest_host first(dest_ip) as dest_ip by hop | sort hop |  fields - dest_host dest_ip
```

#5 - 02/08/2017 06:43 AM - Luke Murphey

- Status changed from New to Closed

- % Done changed from 80 to 100