Network Tools - Bug #2251

Provide contact information in whois lookup

04/27/2018 02:25 AM - Luke Murphey

Status:	Closed	**Start date:**	04/26/2018
Priority:	Normal	**Due date:**	
Assignee:	Luke Murphey	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	1.2.6		

Description

Associated revisions

Revision 266 - 07/26/2018 09:33 PM - lukemurphey

Adding support for contact fields in the lookup output

Reference #2251

Revision 267 - 07/26/2018 09:33 PM - lukemurphey

Adding support for contact fields in the lookup output

Reference #2251

History

#1 - 04/27/2018 02:26 AM - Luke Murphey

See https://answers.splunk.com/answers/623984/try-to-get-list-of-whois-contacts-into-field-resul.html

#2 - 07/26/2018 09:32 PM - Luke Murphey

The fields must be defined ahead of time in transforms.conf. This is difficult since the field values come in like:

- objects.LAS12-ARIN.contact.address.0.value
- objects.LAS12-ARIN.contact.email.0.value
- objects.LAS12-ARIN.contact.phone.0.value
- objects.LINOD.contact.address.0.value
- objects.LINOD.contact.name
- objects.LNO21-ARIN.contact.address.0.value
- objects.LNO21-ARIN.contact.email.0.value

I want to output them as:

- contact.address
- contact.email
- contact.phone
- contact.name

I could do so with some rules like:

- objects.*.contact.address.*.value,

#3 - 07/27/2018 12:56 AM - Luke Murphey

- Status changed from New to Closed

- % Done changed from 0 to 100