Network Tools - Feature #1707

Add ability to perform a DNS lookup

01/29/2017 06:11 AM - Luke Murphey

Status:	Closed	**Start date:**	01/29/2017
Priority:	Normal	**Due date:**	
Assignee:	Luke Murphey	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	0.5		

Description

```
import socket

addr = socket.gethostbyname('google.com')
print addr
```

Associated revisions

Revision 64 - 02/10/2017 09:06 AM - lmurphey

Adding support for a nslookup search command

Reference #1707

Revision 73 - 02/11/2017 06:18 AM - lmurphey

Finalizing the nslookup dashboard

Closes #1707

History

#1 - 01/29/2017 06:12 AM - Luke Murphey

Might want to consider http://www.dnspython.org/

Could allow zone transfers too.

#2 - 02/10/2017 08:03 AM - Luke Murphey

http://stackoverflow.com/questions/13842116/how-do-we-get-txt-cname-and-soa-records-from-dnspython
http://stackoverflow.com/questions/4066614/how-can-i-find-the-authoritative-dns-server-for-a-domain-using-dnspython
http://www.bortzmeyer.org/files/soa.py
https://www.adampalmer.me/iodigitalsec/2014/11/21/performing-dns-queries-python/
http://stackoverflow.com/questions/17681230/how-make-dns-queries-in-dns-python-as-dig-with-aditional-records-section

#3 - 02/10/2017 08:55 AM - Luke Murphey

Might want to handle reverse DNS lookups.

#4 - 02/10/2017 08:56 AM - Luke Murphey

Might want to print the DNS server being used too.

#5 - 02/10/2017 09:00 AM - Luke Murphey

This person is using *dict* to dump the records: http://stackoverflow.com/questions/5903097/python-dns-resolver-get-dns-record-type

#6 - 02/10/2017 09:02 AM - Luke Murphey

Looks like other exceptions may be raised:

```
@raises Timeout: no answers could be found in the specified lifetime
        @raises NXDOMAIN: the query name does not exist
        @raises YXDOMAIN: the query name is too long after DNAME substitution
        @raises NoAnswer: the response did not contain an answer and
        raise_on_no_answer is True.
        @raises NoNameservers: no non-broken nameservers are available to
        answer the question."""
```

#7 - 02/10/2017 09:03 AM - Luke Murphey

Also, custom DNS server is not yet supported.

#8 - 02/10/2017 09:03 AM - Luke Murphey

- % Done changed from 0 to 50

The data is not being indexed yet too.

#9 - 02/11/2017 06:18 AM - Anonymous

- Status changed from New to Closed

- % Done changed from 50 to 100

Applied in changeset splunk-network-tools-svn|r73.