How To Check DNS Blacklist Entries

In case you ever happen to be listed on a DNS blacklist you'll propably find it useful checking for the actual DNS reply.
The point is that many popular blacklists usually provide information and database checks on their websites, however the latter one very often do not reflect current entries withint the blacklist.

So, the way to go is either using 'host', 'dig' or 'nslookup'. Requested addresses must be specified equally as if you were actually searching for a reverse entry (PTR).

In the example given, the IP address "192.168.0.1" (reversed 1.0.168.192) is assumed, while 'ns.of.choice' is a synonym for your local nameserver.

So a query for 'dig' might look like this (output stripped a little):

```
#dig 1.0.168.192.blacklist.domain.tld @ns.of.choice  ANY
;; QUESTION SECTION:
;1.0.168.192.blacklist.domain.tld. IN      ANY

;; ANSWER SECTION:
1.0.168.192.blacklist.domain.tld. 3600 IN  A       127.0.0.6
1.0.168.192.blacklist.domain.tld. 3600 IN  TXT     "sample for typical rbl message"
```

The same query for the 'host' command:

```
#host -t any 1.0.168.192.blacklist.domain.tld ns.of.choice
Using domain server:
Name: ns.of.choice
Address: 192.168.1.1#53
Aliases:

1.0.168.192.blacklist.domain.tld has address 127.0.0.6
1.0.168.192.blacklist.domain.tld descriptive text "sample for a typical rbl message"
```

And the same again using 'nslookup':

```
#nslookup -class=any 1.0.168.192.blacklist.domain.tld ns.of.choice
Server:         ns.of.choice
Address:      192.168.1.1#53

Name:   1.0.168.192.blacklist.domain.tld
Address: 127.0.0.6
1.0.168.192.blacklist.domain.tld   text = "sample for typical rbl message"
```

You may also choose to query any authoritative nameserver of the blacklist in particular (refer to authority section or the SOA records respectively), since querying your local name-server may be not be accurate due to TTL intervals.

CompleteWhois also provides a conventient interface for searching multiple RBL's at once.