Sample Lookup

Generally, this query is done by mail servers or antispam gateways themselves. But maybe you want to check manually:

- with commands : (Example for 1.2.3.4 ip address)

```
:~$ dig -t TXT 4.3.2.1.rbl.honeypots.tk #optional - @(DNS-SERVER-
ADDRESS)
...
;; ANSWER SECTION:
4.3.2.1.rbl.honeypots.tk. 300 IN TXT "Blacklisted:
https://www.honeypots.tk/data.html?ip=1.2.3.4"
...

:~$ nslookup -type=txt 4.3.2.1.rbl.honeypots.tk #optional - (DNS-
SERVER-
ADDRESS)
...
Non-authoritative answer:
4.3.2.1.rbl.honeypots.tk text = "Blacklisted:
https://www.honeypots.tk/data.html?ip=1.2.3.4"
...
```

- for response code : (Example for 1.2.3.4 ip address)

```
:~$ dig -t A 4.3.2.1.rbl.honeypots.tk #optional - @(DNS-SERVER-
ADDRESS)
...
;; ANSWER SECTION:
4.3.2.1.rbl.honeypots.tk. 299 IN A 127.0.0.1
...
```

Response Code List

Response codes are the expression of which service the IP address can attack for us. The following response codes will tell you everything when using blackhole list :

127.0.0.1 ftp protocol
127.0.0.2 smtp protocol
127.0.0.3 proxy protocol
127.0.0.4 telnet protocol
127.0.0.5 http protocol
127.0.0.6 ssh protocol
127.0.0.7 https protocol

127.0.0.8 dns protocol
127.0.0.9 sip protocol
127.0.0.10 tftp protocol

Warning with Blackhole List

RBL replies are addressed to mail servers trying to send you e-mails. The main purpose is to inform the sending user about the server he is on and direct to the IT department.

"Blacklisted: https://www.honeypots.tk/data.html?ip=1.2.3.4"