

The background features a complex network of thin grey lines and dots, forming a web-like structure. Scattered throughout are various triangles of different sizes and orientations, some with solid dots at their vertices. The overall aesthetic is technical and modern.

NXDOMAIN Answer for A Record Queries

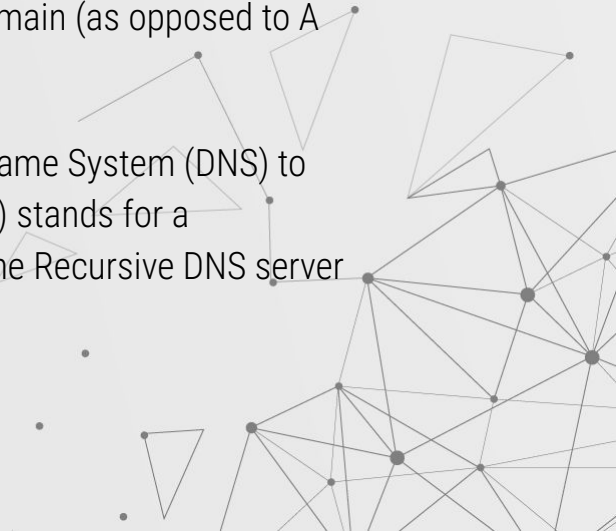
Yves Dantas Neves

BRIEF INTRO TO DNS RECORDS AND ERROR CODES

DNS records are instructions that live in authoritative DNS servers and provide information about a domain including what IP address is associated with that domain and how to handle requests for that domain. The following are common DNS Records which are part of this technical case study:

- **A Record** - The record that holds the IP address of a domain.
- **AAAA Record** - The record that contains the IPv6 address for a domain (as opposed to A records, which list the IPv4 address).

A DNS error code is a standardized response code used by the Domain Name System (DNS) to indicate the outcome of a query. The **NXDOMAIN** Error (Response Code 3) stands for a non-existent domain and represents an error DNS message received by the Recursive DNS server when the requested domain cannot be resolved to an IP address.

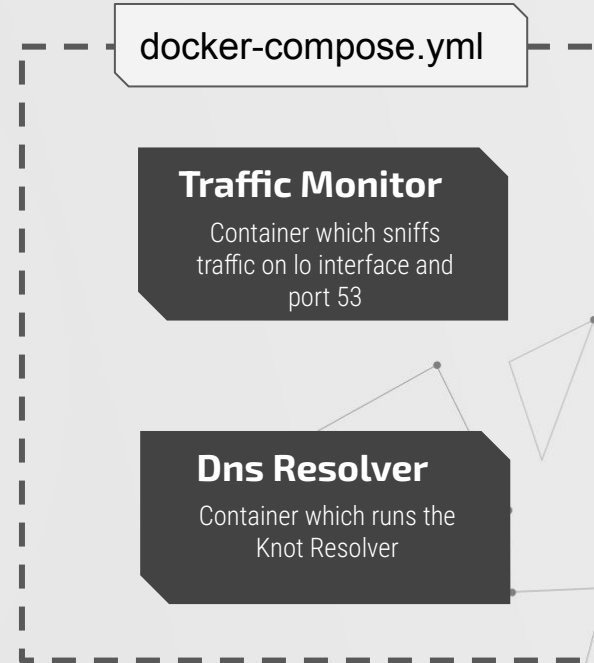


LAB ENVIRONMENT

Requirements

To replicate the scenario, a linux machine with docker installed is required. The environment is composed by a linux container which runs tcpdump and save the results to a .pcap file and a containerized DNS (Knot Resolver) which will resolve our testing queries.

The deployment is defined and streamlined with **docker-compose**.





KNOT RESOLVER CONFIG

config.yaml

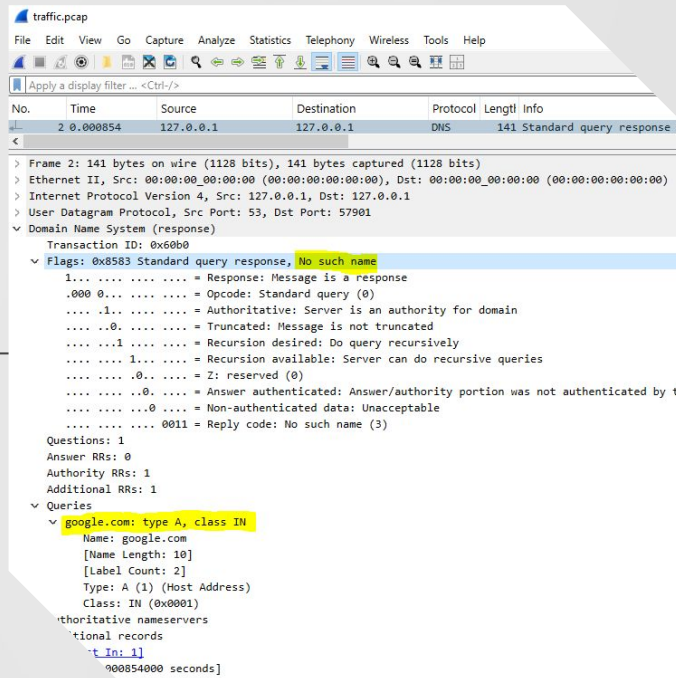
The default DNS Resolver configuration was kept and a customized filter to match and block *A Record Queries and domains saved in the blocklist.rpz* file was created and added to the configuration.

```
4 network:
5   listen:
6     - interface: lo@53
7       interface: lo@853
8       kind: dot
9     - interface: lo@443
10      kind: doh2
11 management:
12   interface: 127.0.0.1@5000
13 lua:
14   script: |
15
16     function endswith(str, ending)
17       -- Check if the ending is longer than the string
18       if #ending > #str then
19         return false
20       end
21       -- Compare the end of the string with the ending
22       return string.sub(str, -#ending) == ending
23     end
24
25     function filter_blocklist(action, target_qtype, block_qname)
26       return function (state, query)
27         query_check = endswith(kres.dname2str(query.sname), block_qname)
28         if query.stype == target_qtype and query_check then
29           return action
30         else
31           return nil
32         end
33       end
34     end
35
36     file = io.open("/etc/knot-resolver/blocklist.rpz", "r")
37     for line in file:lines() do
38       dname = string.gsub(line, "[\r\n]+$", "")
39       policy.add(filter_blocklist(policy.DENY, kres.type.A, dname))
40     end
```

EXPERIMENT RESULTS

dig google.com @127.0.0.1 A

The DNS Resolver inspects the query and the policy for query blocking is matched since google.com is added to the *blocklist.rpz* file. The resolver returns a *NXDOMAIN Error* to this query.

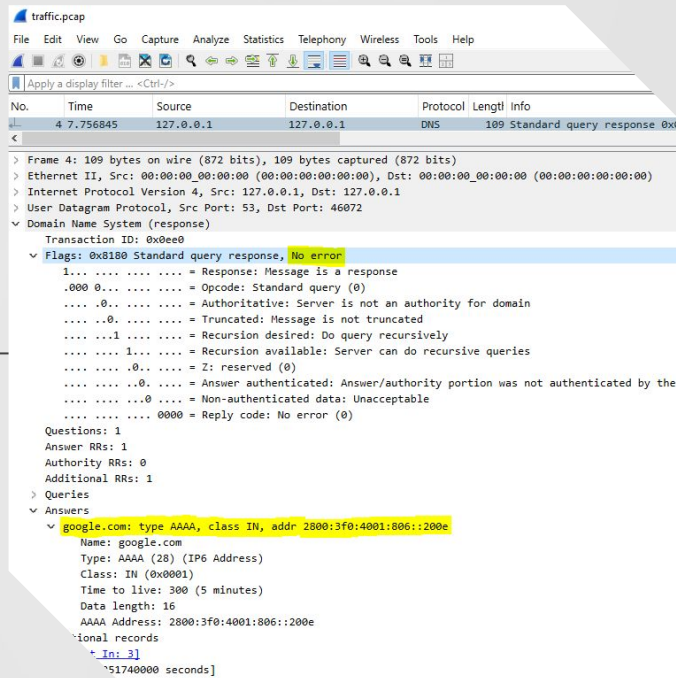


```
traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
2 0.000854 127.0.0.1 127.0.0.1 DNS 141 Standard query response
<
> Frame 2: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits)
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> User Datagram Protocol, Src Port: 53, Dst Port: 57901
v Domain Name System (response)
Transaction ID: 0x60b0
v Flags: 0x8583 Standard query response, No such name
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
... .1... .. = Authoritative: Server is an authority for domain
... .0... .. = Truncated: Message is not truncated
... .1... .. = Recursion desired: Do query recursively
... ..1... .. = Recursion available: Server can do recursive queries
... ..0... .. = Z: reserved (0)
... ..0... .. = Answer authenticated: Answer/authority portion was not authenticated by t
... ..0... .. = Non-authenticated data: Unacceptable
... ..0011 = Reply code: No such name (3)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 1
v Queries
v google.com: type A, class IN
Name: google.com
[Name Length: 10]
[Label Count: 2]
Type: A (1) (Host Address)
Class: IN (0x0001)
Authoritative nameservers
Additional records
t In: 1]
900854000 seconds]
```

EXPERIMENT RESULTS

dig google.com @127.0.0.1 AAAA

As the blocking policy is only applicable to A queries,
the DNS Resolver is able to answer this query.



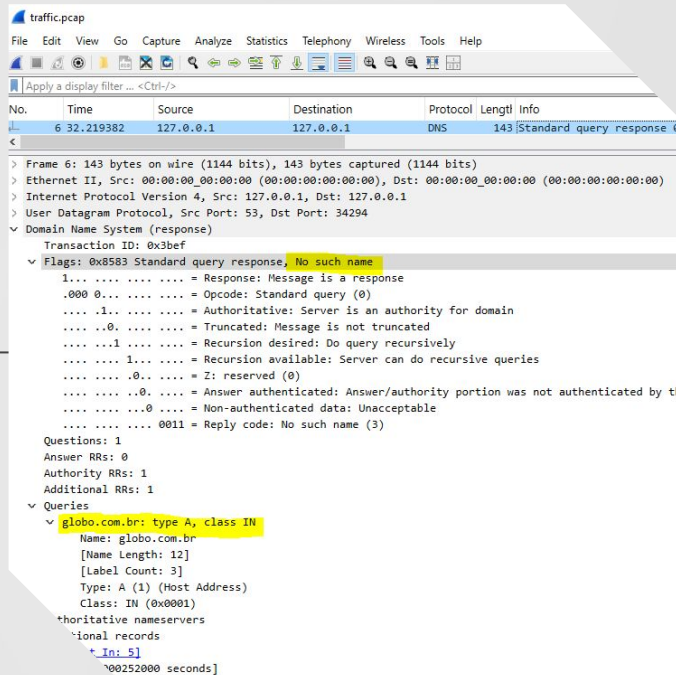
The screenshot shows the Wireshark interface with a packet capture of a DNS response. The packet list shows a DNS packet (Standard query response) from 127.0.0.1 to 127.0.0.1. The packet details pane shows the following information:

- Frame 4: 109 bytes on wire (872 bits), 109 bytes captured (872 bits)
- Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- User Datagram Protocol, Src Port: 53, Dst Port: 46072
- Domain Name System (response)
 - Transaction ID: 0x0ee0
 - Flags: 0x0180 Standard query response, No error
 - 1... .. = Response: Message is a response
 - .000 0... .. = Opcode: Standard query (0)
 -0... .. = Authoritative: Server is not an authority for domain
 -0... .. = Truncated: Message is not truncated
 -1... .. = Recursion desired: Do query recursively
 -1... .. = Recursion available: Server can do recursive queries
 -0... .. = Z: reserved (0)
 -0... .. = Answer authenticated: Answer/authority portion was not authenticated by the
 -0... .. = Non-authenticated data: Unacceptable
 -0000 = Reply code: No error (0)
 - Questions: 1
 - Answer RRs: 1
 - Authority RRs: 0
 - Additional RRs: 1
 - Queries
 - Answers
 - google.com: type AAAA, class IN, addr 2800:3f0:4001:806::200e
 - Name: google.com
 - Type: AAAA (28) (IP6 Address)
 - Class: IN (0x0001)
 - Time to live: 300 (5 minutes)
 - Data length: 16
 - AAAA Address: 2800:3f0:4001:806::200e

EXPERIMENT RESULTS

dig globo.com.br @127.0.0.1 A

This is another example of a query which was added to the *blocklist.rpz* file and consequently matches the blocking policy.



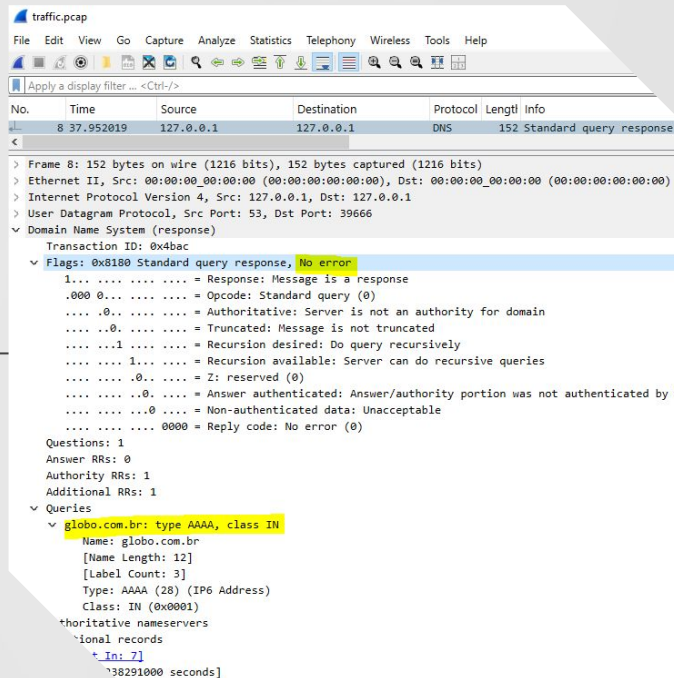
The screenshot shows the Wireshark interface with a packet capture of a DNS query. The packet list shows a DNS Standard query response from 127.0.0.1 to 127.0.0.1. The packet details pane shows the transaction ID 0x3bef and the query for globo.com.br. The query is a type A query with a class of IN. The packet bytes pane shows the raw data of the query.

```
traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
6 32.219382 127.0.0.1 127.0.0.1 DNS 143 Standard query response
> Frame 6: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits)
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> User Datagram Protocol, Src Port: 53, Dst Port: 34294
v Domain Name System (response)
Transaction ID: 0x3bef
v Flags: 0x8583 Standard query response, No such name
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
... 1... .. = Authoritative: Server is an authority for domain
... 0... .. = Truncated: Message is not truncated
... 1... .. = Recursion desired: Do query recursively
... 1... .. = Recursion available: Server can do recursive queries
... 0... .. = Z: reserved (0)
... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by t
... 0... .. = Non-authenticated data: Unacceptable
... 0011 = Reply code: No such name (3)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 1
v Queries
v globo.com.br: type A, class IN
Name: globo.com.br
[Name Length: 12]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)
*Authoritative nameservers
*ional records
* [In: 5]
*00252000 seconds]
```

EXPERIMENT RESULTS

dig globo.com.br @127.0.0.1 AAAA

For this example, as expected the policy is not matched but the query does not bring any answers since the domain globo.com.br does not offer IPv6 services at this moment.



The screenshot shows the Wireshark network protocol analyzer interface. The title bar indicates the file is 'traffic.pcap'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions. The display filter is set to 'Apply a display filter ... <Ctrl-/>'. The packet list shows a single packet, No. 8, at time 37.952019, from source 127.0.0.1 to destination 127.0.0.1, protocol DNS, length 152, and info 'Standard query response'. The packet details pane shows the following structure:

- > Frame 8: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits)
- > Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
- > Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- > User Datagram Protocol, Src Port: 53, Dst Port: 39666
- ✓ Domain Name System (response)
 - Transaction ID: 0x4bac
 - ✓ Flags: 0x8180 Standard query response, No error
 - 1... .. = Response: Message is a response
 - .000 0... .. = Opcode: Standard query (0)
 -0... .. = Authoritative: Server is not an authority for domain
 -0... .. = Truncated: Message is not truncated
 -1... .. = Recursion desired: Do query recursively
 -1... .. = Recursion available: Server can do recursive queries
 -0... .. = Z: reserved (0)
 -0... .. = Answer authenticated: Answer/authority portion was not authenticated by
 -0... .. = Non-authenticated data: Unacceptable
 -0000 = Reply code: No error (0)
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 1
 - Additional RRs: 1
 - ✓ Queries
 - ✓ globo.com.br: type AAAA, class IN
 - Name: globo.com.br
 - [Name Length: 12]
 - [Label Count: 3]
 - Type: AAAA (28) (IPv6 Address)
 - Class: IN (0x0001)
 - Authoritative nameservers
 - Additional records
 - ↳ In: 7]
 - ↳ 38291000 seconds]

REFERENCES

- <https://datatracker.ietf.org/doc/html/rfc1035>
- <https://www.knot-resolver.cz/documentation/latest/config-lua.html>
- <https://knot-resolver.readthedocs.io/en/stable/modules-policy.html>
- https://docs.whalebone.io/en/immunity/knot_tips_tricks.html#deny-list-of-domains
- <https://github.com/yvesdantas/dns-resolver-nxdomain>



Thank you!

