CNS Lab 5 Local DNS Cache Poisoning Attack

PES1UG20CS084

Aryansh Bhargavan

Verification of Lab Setup

> **Running**
>
> `dig ns.attacker32.com`
>
> ```
> PES1UG20CS084@User:/# dig ns.attacker32.com
>
> ; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
> ;; global options: +cmd
> ;; Got answer:
> ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37353
> ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
>
> ;; OPT PSEUDOSECTION:
> ; EDNS: version: 0, flags:; udp: 4096
> ; COOKIE: 40e5d85e1cdbc72a01000000634954ed6aca8593626cef2c (good)
> ;; QUESTION SECTION:
> ;ns.attacker32.com.             IN      A
>
> ;; ANSWER SECTION:
> ns.attacker32.com.      259171  IN      A       10.9.0.153
>
> ;; Query time: 0 msec
> ;; SERVER: 10.9.0.53#53(10.9.0.53)
> ;; WHEN: Fri Oct 14 12:24:13 UTC 2022
> ;; MSG SIZE  rcvd: 90
> ```
>
> `dig www.example.com`

```
PES1UG20CS084@User:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43686
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a4f9ea5adf2479090100000063495 52f5a409a241ca41e4c (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        86400   IN      A       93.184.216.34

;; Query time: 1424 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Oct 14 12:25:19 UTC 2022
;; MSG SIZE  rcvd: 88
```

`dig @ns.attacker32.com www.example.com`

```
PES1UG20CS084@User:/# dig @ns.attacker32.com www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @ns.attacker32.com www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2037
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2f76740ac632f0010100000063495 55494cb121595135d54 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.5

;; Query time: 4 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Fri Oct 14 12:25:56 UTC 2022
```

Attack on DNS

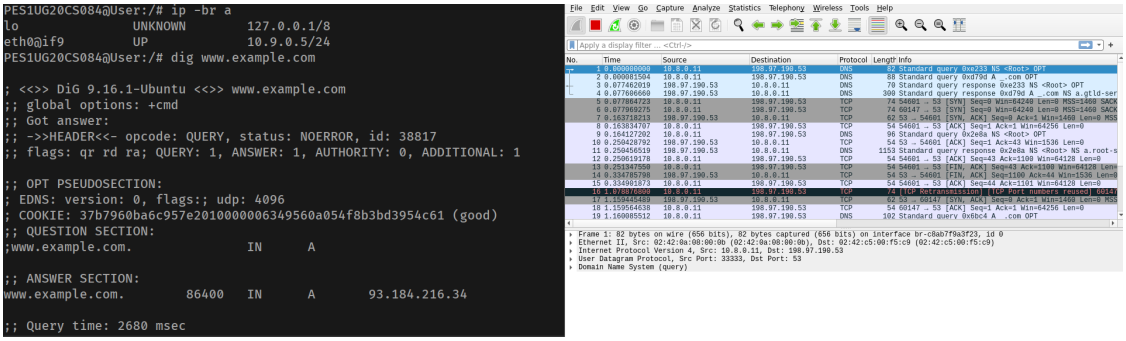
Task 1: Directly Spoofing Response to User

Running

`rndc flush`

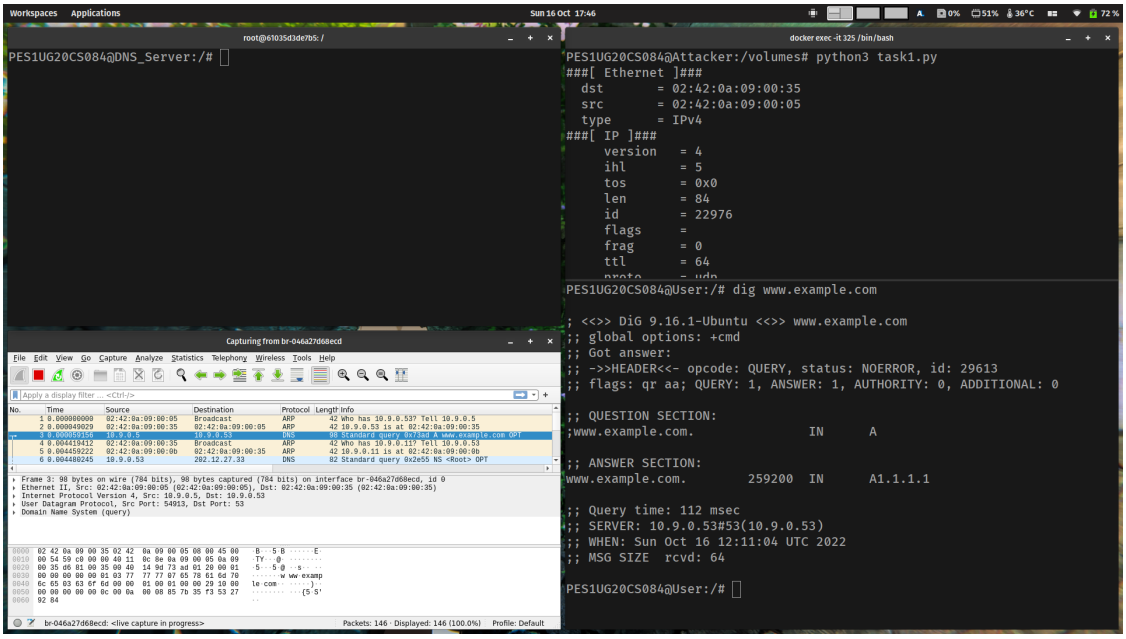
```
PES1UG20CS084@DNS_Server:/# rndc flush
PES1UG20CS084@DNS_Server:/#
```

`dig www.example.com`

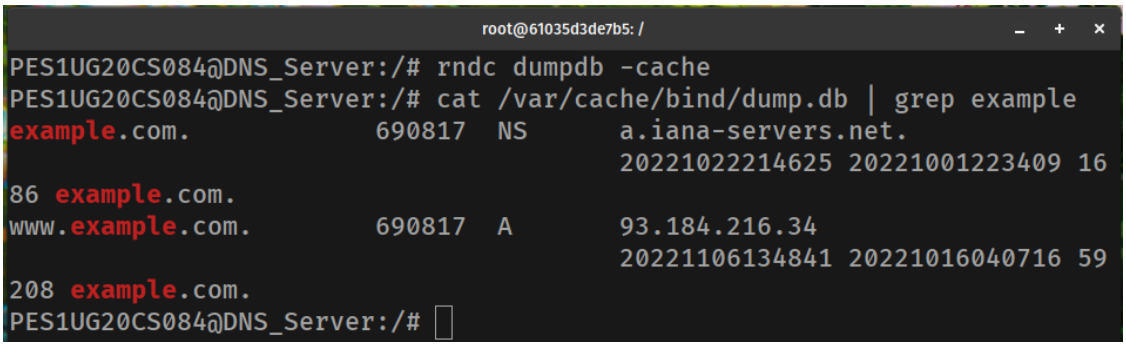


Running the task

`python3 task1.py` on `attacker` and `dig www.example.com` on victim



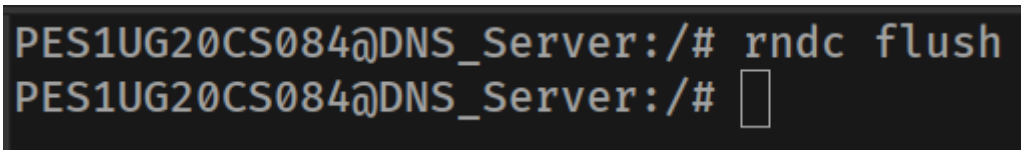
Looking at dns cache



Since the local DNS server is not involved in the spoofing process, the IP address of `example.com` is still accurate

Task 2: DNS Cache Poisoning Attack – Spoofing Answers

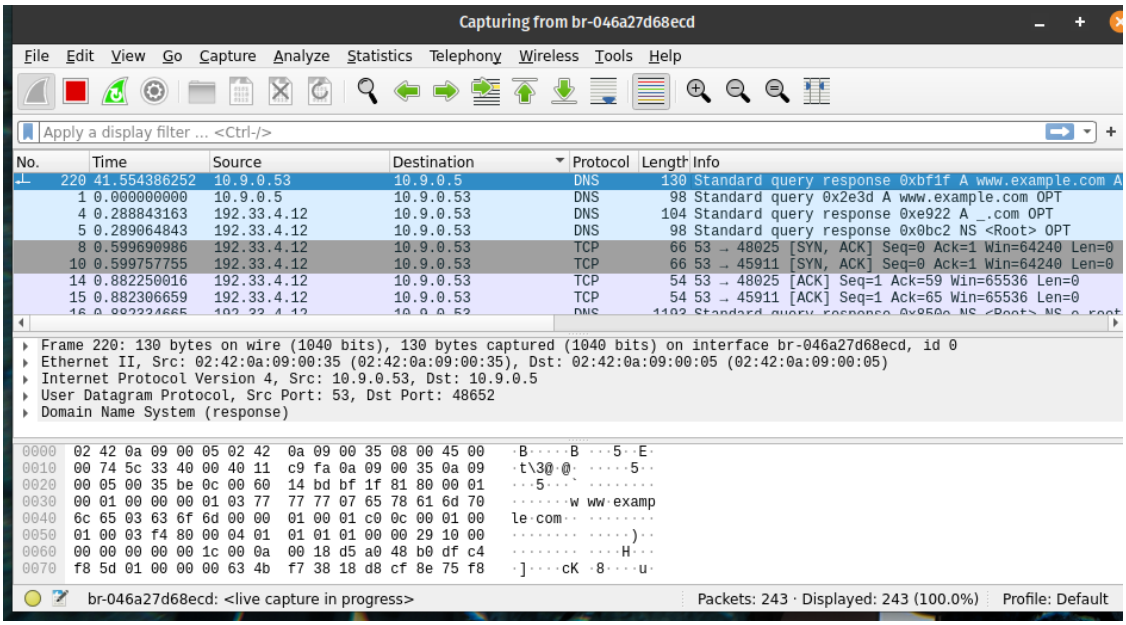
Running `rndc flush`



Running `python3 task2.py` and `dig www.example.com`

```
docker exec -it 325 /bin/bash
PES1UG20CS084@Attacker:/volumes# python3 task2.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:0b
  src       = 02:42:0a:09:00:35
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 30942
     flags     =
     frag      = 0
     ttl       = 64
     proto     = udp
PES1UG20CS084@User:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48927
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d5a048b0dfc4f85d01000000634bf73818d8cf8e75f8c3c6 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.1.1.1

;; Query time: 2232 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 16 12:21:12 UTC 2022
;; MSG SIZE  rcvd: 88
```

Spoofed Response



Looking at dns cache

```
root@61035d3de7b5: /
PES1UG20CS084@DNS_Server:/# rndc dumpdb -cache
PES1UG20CS084@DNS_Server:/# cat /var/cache/bind/dump.db | grep example
example.com.            777468  NS      a.iana-servers.net.
www.example.com.        863868  A       1.1.1.1
PES1UG20CS084@DNS_Server:/#
```

This time, DNS gets poisoned since the spoofed reply came to local DNS before the actual reply

---

Task 3: Spoofing NS Records

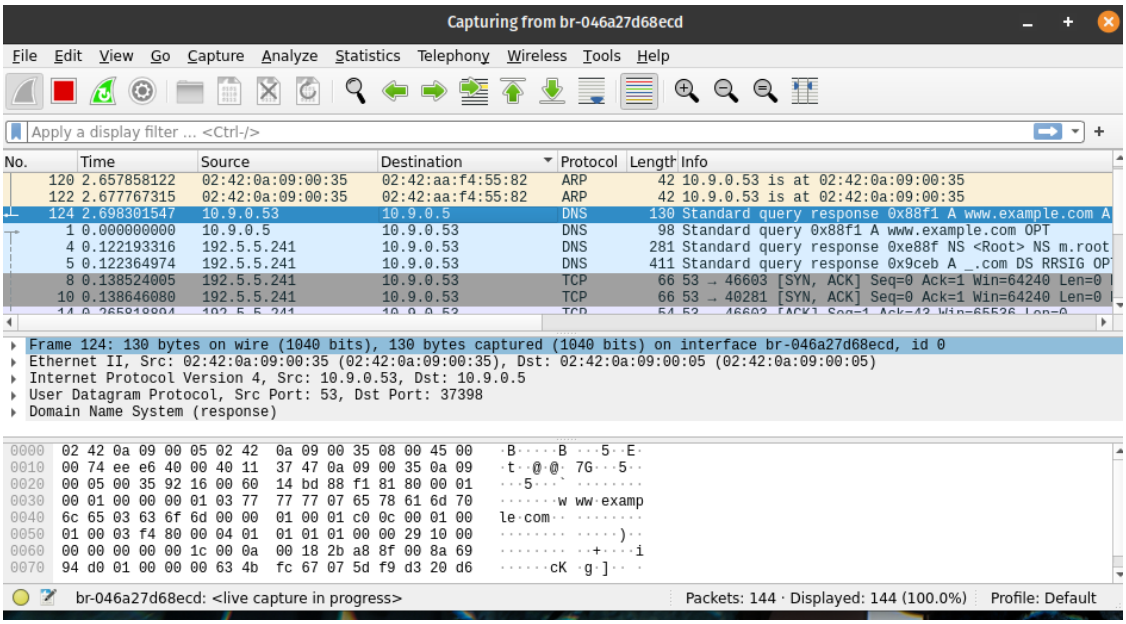
Running `rndc flush`

```
PES1UG20CS084@DNS_Server:/# rndc flush
PES1UG20CS084@DNS_Server:/#
```

Running `python3 task3.py` and `dig www.example.com`

```
docker exec -it 325 /bin/bash
PES1UG20CS084@Attacker:/volumes# python3 task3.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:0b
  src       = 02:42:0a:09:00:35
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 29968
     flags     =
     frag      = 0
     ttl       = 64
     proto     = udp
     chksum    = 0xacea
     src       = 10.9.0.53
     dst       = 199.43.135.53
PES1UG20CS084@User:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35057
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2ba88f008a6994d001000000634bfc67075df9d320d691e8 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.1.1.1

;; Query time: 2699 msec
```

Spoofed Response



If we query some other subdomain under `example.com` domain, we get the spoofed IP address `1.2.3.6`

```
PES1UG20CS084@User:/# dig ftp.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> ftp.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3859
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7b52776feaa9068f01000000634bfdff8ecca8eaca87b4b5 (good)
;; QUESTION SECTION:
;ftp.example.com.               IN      A

;; ANSWER SECTION:
ftp.example.com.        259200  IN      A       1.2.3.6

;; Query time: 0 msec
```

Checking dns cache

```
root@61035d3de7b5: /
PES1UG20CS084@DNS_Server:/# rndc dumpdb -cache
PES1UG20CS084@DNS_Server:/# cat /var/cache/bind/dump.db | grep example
example.com.            777258  NS      ns.attacker32.com.
www.example.com.        863660  A       1.1.1.1
PES1UG20CS084@DNS_Server:/# rndc dumpdb -cache
PES1UG20CS084@DNS_Server:/# cat /var/cache/bind/dump.db | grep example
example.com.            777172  NS      ns.attacker32.com.
ftp.example.com.        863982  A       1.2.3.6
www.example.com.        863574  A       1.1.1.1
PES1UG20CS084@DNS_Server:/#
```

Task 4: Spoofing NS Records for Another Domain

Running `rndc flush`

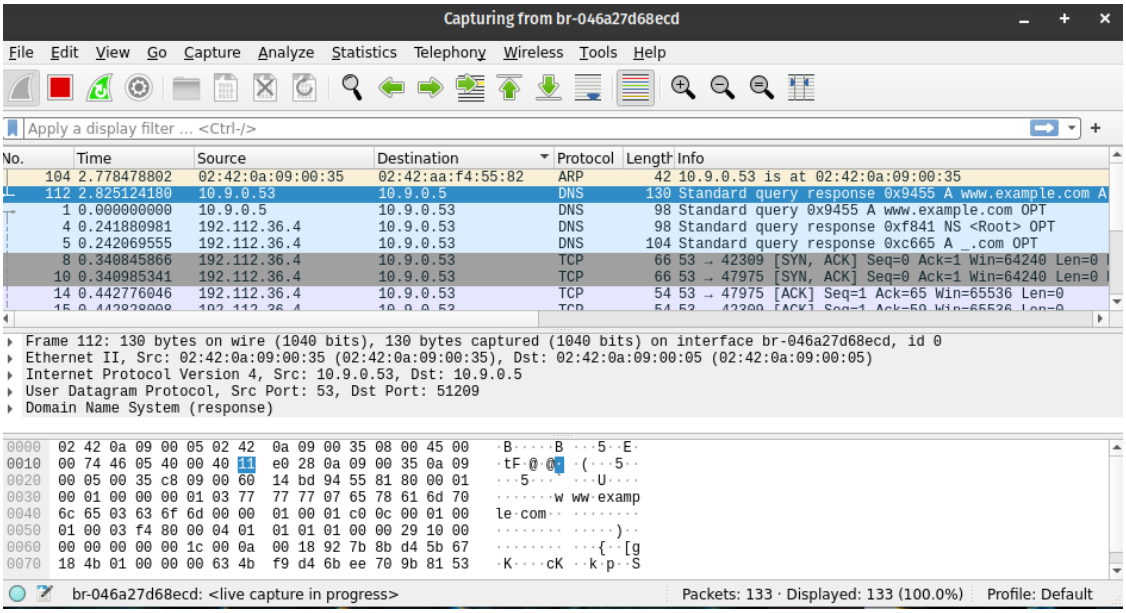
```
PES1UG20CS084@DNS_Server:/# rndc flush
PES1UG20CS084@DNS_Server:/#
```

Running `python3 task4.py` and `dig www.example.com`

```
docker exec -it 325 /bin/bash
PES1UG20CS084@Attacker:/volumes# python3 task4.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:0b
  src       = 02:42:0a:09:00:35
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 2759
     flags     =
     frag      = 0
     ttl       = 64
     proto     = udp
```

```
PES1UG20CS084@User:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37973
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 927b8bd45b67184b01000000634bf9d46bee709b8153816b (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.1.1.1

;; Query time: 2828 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 16 12:32:20 UTC 2022
;; MSG SIZE  rcvd: 88
```

Spoofed response



Response contains answer as spoofed IP address since the queries are forwarded to the attacker's nameserver

Checking Cache

```
root@61035d3de7b5: /
PES1UG20CS084@DNS_Server:/# rndc dumpdb -cache
PES1UG20CS084@DNS_Server:/# cat /var/cache/bind/dump.db | grep example
example.com.            777076  NS      ns.attacker32.com.
www.example.com.        863478  A       1.1.1.1
PES1UG20CS084@DNS_Server:/#
```

Since the spoofed NS record for `google.com` is considered out of zone, it is not cached by the DNS server

---

Task 5: Spoofing Records in the Additional Section

Running `rndc flush`

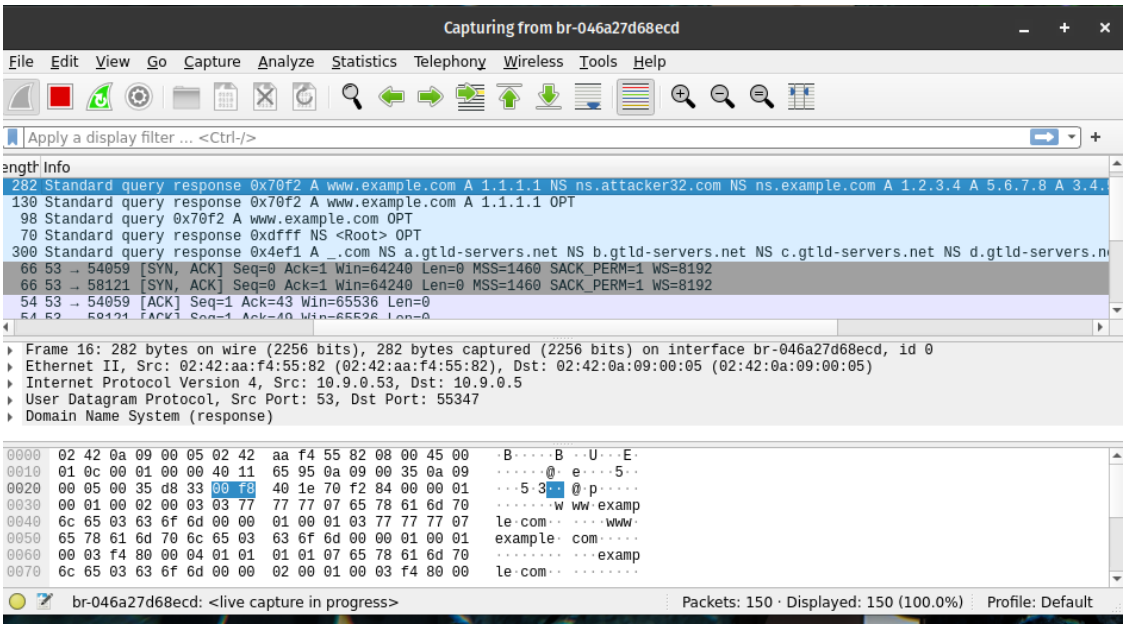
```
PES1UG20CS084@DNS_Server:/# rndc flush
PES1UG20CS084@DNS_Server:/#
```

Running `python3 task5.py` and `dig www.example.com`

```
docker exec -it 325 /bin/bash
PES1UG20CS084@Attacker:/volumes# python3 task5.py
.
Sent 1 packets.
.
Sent 1 packets.
```

```
www.example.com.        259200  IN      A       1.1.1.1

;; AUTHORITY SECTION:
example.com.            259200  IN      NS      ns.attacker32.com.
example.com.            259200  IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.attacker32.com.      259200  IN      A       1.2.3.4
ns.example.net.         259200  IN      A       5.6.7.8
www.facebook.com.       259200  IN      A       3.4.5.6

;; Query time: 100 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 16 12:51:21 UTC 2022
;; MSG SIZE  rcvd: 240

PES1UG20CS084@User:/#
```

Spoofed Reply containing records in additional section



Checking DNS Cache

```
root@61035d3de7b5: /
PES1UG20CS084@DNS_Server:/# rndc dumpdb -cache
PES1UG20CS084@DNS_Server:/# cat /var/cache/bind/dump.db | grep example
example.com.            777460  NS      ns.attacker32.com.
www.example.com.        863862  A       1.1.1.1
PES1UG20CS084@DNS_Server:/#
```

All the content in the additional section is regarded out of zone and is hence discarded by local dns and not cached