

# 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: 40e5d85e1cdb72a01000000634954ed6aca8593626cef2c (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: a4f9ea5adf247909010000006349552f5a409a241ca41e4c (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: 2f76740ac632f001010000006349555494cb121595135d54 (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
```

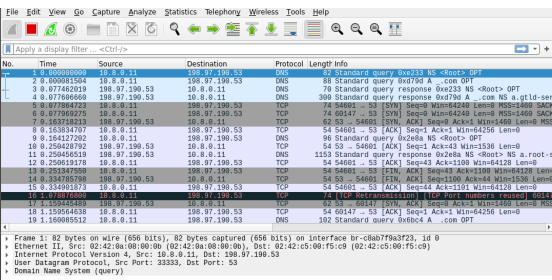
```
PES1UG20CS084@User:/# ip -br a
lo UNKNOWN 127.0.0.1/8
eth0@if9 UP 10.9.0.5/24
PES1UG20CS084@User:/# dig www.example.com

;<<> DiG 9.16.1-Ubuntu <<> www.example.com
; global options: +cmd
; Got answer:
;->HEADER<- opcode: QUERY, status: NOERROR, id: 38817
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::; udp: 4096
; COOKIE: 37b7960ba6c957e201000006349560a054f8b3bd3954c61 (good)
; QUESTION SECTION:
;www.example.com. IN A

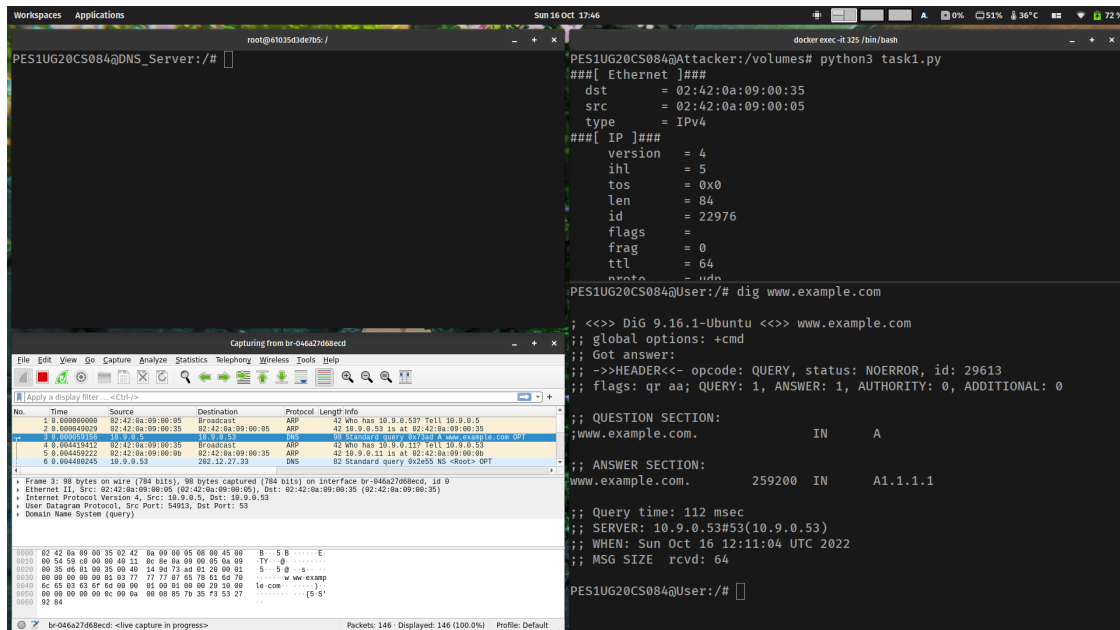
; ANSWER SECTION:
www.example.com. 86400 IN A 93.184.216.34

; Query time: 2680 msec
```



## Running the task

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



## 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. 690817 NS a.iana-servers.net.
20221022214625 20221001223409 16
86 example.com.
www.example.com. 690817 A 93.184.216.34
20221106134841 20221016040716 59
208 example.com.
PES1UG20CS084@DNS_Server:/#
```

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

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

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

Capturing from br-046a27d68ecd

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
220	41.554386252	10.9.0.53	10.9.0.5	DNS	130	Standard query response 0xb1f1 A www.example.com A
1	0.000000000	10.9.0.5	10.9.0.53	DNS	98	Standard query 0x2e3d A www.example.com OPT
4	0.288843163	192.33.4.12	10.9.0.53	DNS	104	Standard query response 0xe922 A __.com OPT
5	0.289064843	192.33.4.12	10.9.0.53	DNS	98	Standard query response 0x0bc2 NS <Root> OPT
8	0.599690986	192.33.4.12	10.9.0.53	TCP	66	53 → 48025 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
10	0.599757755	192.33.4.12	10.9.0.53	TCP	66	53 → 45911 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
14	0.882250016	192.33.4.12	10.9.0.53	TCP	54	53 → 48025 [ACK] Seq=1 Ack=59 Win=65536 Len=0
15	0.882306659	192.33.4.12	10.9.0.53	TCP	54	53 → 45911 [ACK] Seq=1 Ack=65 Win=65536 Len=0
16	0.000000000	10.9.0.53	10.9.0.5	DNS	1102	Standard query response 0x850c NS <Root> NS <Root> NS <Root>

Frame 220: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface br-046a27d68ecd, id 0

Ethernet II, Src: 02:42:0a:09:00:35 (02:42:0a:09:00:35), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)

Internet Protocol Version 4, Src: 10.9.0.53, Dst: 10.9.0.5

User Datagram Protocol, Src Port: 53, Dst Port: 48652

Domain Name System (response)

```
0000  02 42 0a 09 00 05 02 42 0a 09 00 35 08 00 45 00  B...B...5..E
0010  00 74 5c 33 40 00 40 11 c9 fa 0a 09 00 35 0a 09  t\3@.0...5..
0020  00 05 00 35 be 0c 00 60 14 bd bf 1f 81 80 00 01  ...5...
0030  00 01 00 00 00 01 03 77 77 77 07 65 78 61 6d 70  ....w ww-examp
0040  6c 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00  le.com...
0050  01 00 03 f4 80 00 04 01 01 01 01 00 00 29 10 00  .....})..
0060  00 00 00 00 00 1c 00 0a 00 18 d5 a0 48 b0 df c4  .....H...
0070  f8 5d 01 00 00 00 63 4b f7 38 18 d8 cf 8e 75 f8  .]...cK..8...u
```

br-046a27d68ecd: <live capture in progress> Packets: 243 · Displayed: 243 (100.0%) Profile: Default

## 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

Capturing from br-046a27d68ecd

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
120	2.657858122	02:42:0a:09:00:35	02:42:aa:f4:55:82	ARP	42	10.9.0.53 is at 02:42:0a:09:00:35
122	2.677767315	02:42:0a:09:00:35	02:42:aa:f4:55:82	ARP	42	10.9.0.53 is at 02:42:0a:09:00:35
124	2.698301547	10.9.0.53	10.9.0.5	DNS	130	Standard query response 0x88f1 A www.example.com A
1	0.000000000	10.9.0.5	10.9.0.53	DNS	98	Standard query 0x88f1 A www.example.com OPT
4	0.122193316	192.5.5.241	10.9.0.53	DNS	281	Standard query response 0xe88f NS <Root> NS m.root
5	0.122364974	192.5.5.241	10.9.0.53	DNS	411	Standard query response 0x9ceb A .com DS RRSIG OP
8	0.138524005	192.5.5.241	10.9.0.53	TCP	66	53 → 46603 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
10	0.138646080	192.5.5.241	10.9.0.53	TCP	66	53 → 40281 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
14	0.265040804	192.5.5.241	10.9.0.53	TCP	54	53 → 46603 [ACK] Seq=1 Ack=42 Win=65536 Len=0

Frame 124: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface br-046a27d68ecd, id 0

- Ethernet II, Src: 02:42:0a:09:00:35 (02:42:0a:09:00:35), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
- Internet Protocol Version 4, Src: 10.9.0.53, Dst: 10.9.0.5
- User Datagram Protocol, Src Port: 53, Dst Port: 37398
- Domain Name System (response)

0000 02 42 0a 09 00 05 02 42 0a 09 00 35 08 00 45 00 B.....B.....5..E..

0010 00 74 ee e6 40 00 40 11 37 47 0a 09 00 35 0a 09 .t..@..7G.....5..

0020 00 05 00 35 92 16 00 60 14 bd 88 f1 81 80 00 01 ...5.....

0030 00 01 00 00 00 01 03 77 77 77 07 65 78 61 6d 70 .....wwww.examp

0040 6c 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 le.com.....

0050 01 00 03 f4 80 00 04 01 01 01 01 00 00 29 10 00 .....+.....1

0060 00 00 00 00 00 1c 00 0a 00 18 2b a8 8f 00 8a 69 .....ck.g.j....

0070 94 d0 01 00 00 00 63 4b fc 67 07 5d f9 d3 20 d6

br-046a27d68ecd: <live capture in progress> Packets: 144 · Displayed: 144 (100.0%) Profile: Default

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: 7b52776feaa9068f01000000634bfdf8eacca8eaca87b4b5 (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

Capturing from br-046a27d68ecd

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
104	2.778478802	02:42:0a:09:00:35	02:42:aa:f4:55:82	ARP	42	10.9.0.53 is at 02:42:0a:09:00:35
112	2.825124180	10.9.0.53	10.9.0.5	DNS	130	Standard query response 0x9455 A www.example.com A
1	0.000000000	10.9.0.5	10.9.0.53	DNS	98	Standard query 0x9455 A www.example.com OPT
4	0.241880981	192.112.36.4	10.9.0.53	DNS	98	Standard query response 0xf841 NS <Root> OPT
5	0.242069555	192.112.36.4	10.9.0.53	DNS	104	Standard query response 0xc665 A .com OPT
8	0.340845866	192.112.36.4	10.9.0.53	TCP	66	53 → 42309 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
10	0.340985341	192.112.36.4	10.9.0.53	TCP	66	53 → 47975 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
14	0.442776046	192.112.36.4	10.9.0.53	TCP	54	53 → 47975 [ACK] Seq=1 Ack=65 Win=65536 Len=0
15	0.442920000	192.112.36.4	10.9.0.53	TCP	54	53 → 47975 [ACK] Seq=1 Ack=65 Win=65536 Len=0

Frame 112: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface br-046a27d68ecd, id 0

- Ethernet II, Src: 02:42:0a:09:00:35 (02:42:0a:09:00:35), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
- Internet Protocol Version 4, Src: 10.9.0.53, Dst: 10.9.0.5
- User Datagram Protocol, Src Port: 53, Dst Port: 51209
- Domain Name System (response)

```
0000  02 42 0a 09 00 05 02 42 0a 09 00 35 08 00 45 00  B....B...5..E
0010  00 74 46 05 40 00 40 11 e0 28 0a 09 00 35 0a 09  tF.0.0. (...5..
0020  00 05 00 35 c8 09 00 60 14 bd 94 55 81 80 00 01  ...5....U...
0030  00 01 00 00 00 01 03 77 77 77 07 65 78 61 6d 70  ....wwww-examp
0040  6c 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00  le.com.....
0050  01 00 03 f4 80 00 04 01 01 01 01 00 00 29 10 00  ....[g
0060  00 00 00 00 00 00 1c 00 0a 00 18 92 7b 8b d4 5b 67  .....{...[g
0070  18 4b 01 00 00 00 63 4b f9 d4 6b ee 70 9b 81 53  .K...cK...k.p..S
```

br-046a27d68ecd: <live capture in progress> Packets: 133 · Displayed: 133 (100.0%) Profile: Default

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

The image shows a Wireshark packet capture window titled "Capturing from br-046a27d68ecd". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a display filter set to "Apply a display filter ... <Ctrl-/>".

The packet list on the left shows several DNS and TCP packets. The selected packet is a "Standard query response" (Frame 16) with details as follows:

- Frame 16: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface br-046a27d68ecd, id 0
- Ethernet II, Src: 02:42:aa:f4:55:82 (02:42:aa:f4:55:82), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
- Internet Protocol Version 4, Src: 10.9.0.53, Dst: 10.9.0.5
- User Datagram Protocol, Src Port: 53, Dst Port: 55347
- Domain Name System (response)

The packet bytes pane shows the raw data of the DNS response, including the header and the additional section records:

```
0000  02 42 0a 09 00 05 02 42  aa f4 55 82 08 00 45 00  B....B...U...E
0010  01 0c 00 01 00 00 40 11  65 95 0a 09 00 35 0a 09  ....@...e...5..
0020  00 05 00 35 d8 33 00 f8  40 1e 70 f2 84 00 00 01  ...5-3...@:p...
0030  00 01 00 02 00 03 03 77  77 77 07 65 78 61 6d 70  ....WWW...exam
0040  6c 65 03 63 6f 6d 00 00  01 00 01 03 77 77 07 07  le.com...www
0050  65 78 61 6d 70 6c 65 03  63 6f 6d 00 00 01 00 01  example.com...
0060  00 03 f4 80 00 04 01 01  01 01 07 65 78 61 6d 70  ....exam
0070  6c 65 03 63 6f 6d 00 00  02 00 01 00 03 f4 80 00  le.com.....
```

The status bar at the bottom indicates "br-046a27d68ecd: <live capture in progress>" and "Packets: 150 · Displayed: 150 (100.0%) Profile: Default".

## 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