

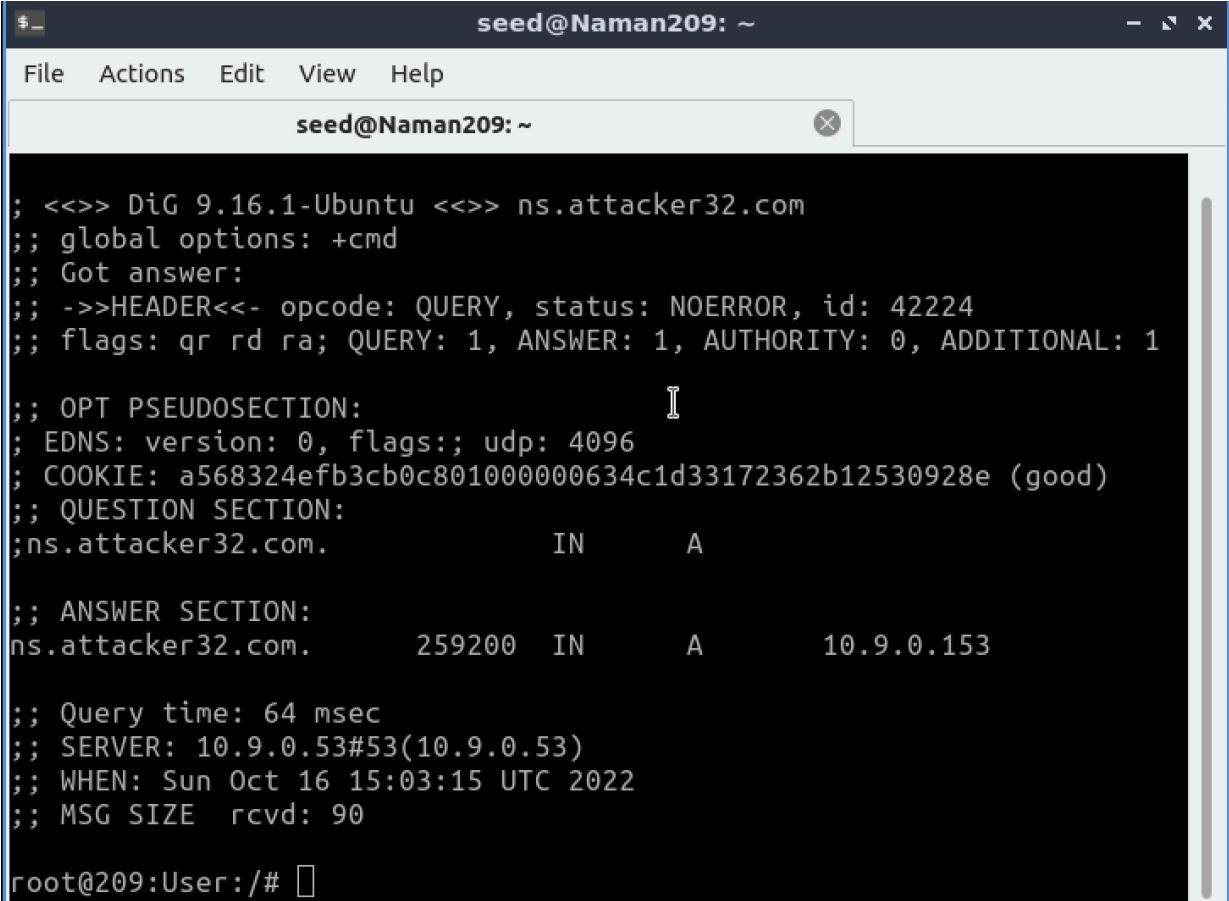
# Computer Network Security

Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

## Local DNS Attack Lab

### Task 0: Verification of the DNS setup

```
dig ns.attacker32.com
```



```
seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
; <>> DiG 9.16.1-Ubuntu <>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42224
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: a568324efb3cb0c801000000634c1d33172362b12530928e (good)
;; QUESTION SECTION:
;ns.attacker32.com.           IN      A
;;
;; ANSWER SECTION:
ns.attacker32.com.      259200  IN      A      10.9.0.153
;;
;; Query time: 64 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 16 15:03:15 UTC 2022
;; MSG SIZE  rcvd: 90
root@209:User:/#
```

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

```
seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
root@209:User:/# dig www.example.com

; <>> DiG 9.16.1-Ubuntu <>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23904
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 9c1c40d350c09b0d01000000634c1e262f4529f131095bd5 (good)
;; QUESTION SECTION:
;www.example.com.           IN      A

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

;; Query time: 1399 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 16 15:07:18 UTC 2022
;; MSG SIZE  rcvd: 88
```

```
seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
root@209: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: 28113
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

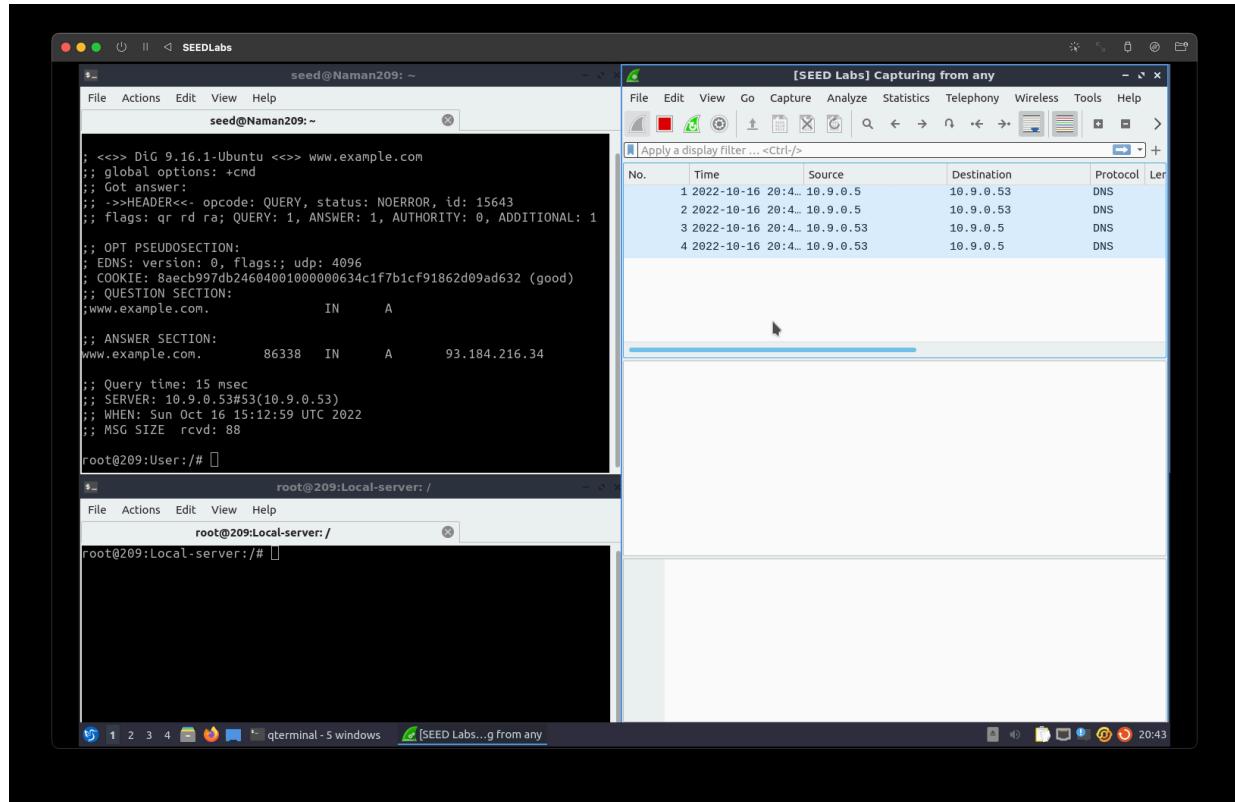
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 667b46d09440ae4c01000000634c1e5a248789a554329146 (good)
;; QUESTION SECTION:
;www.example.com.           IN      A

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

;; Query time: 3 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Sun Oct 16 15:08:10 UTC 2022
```

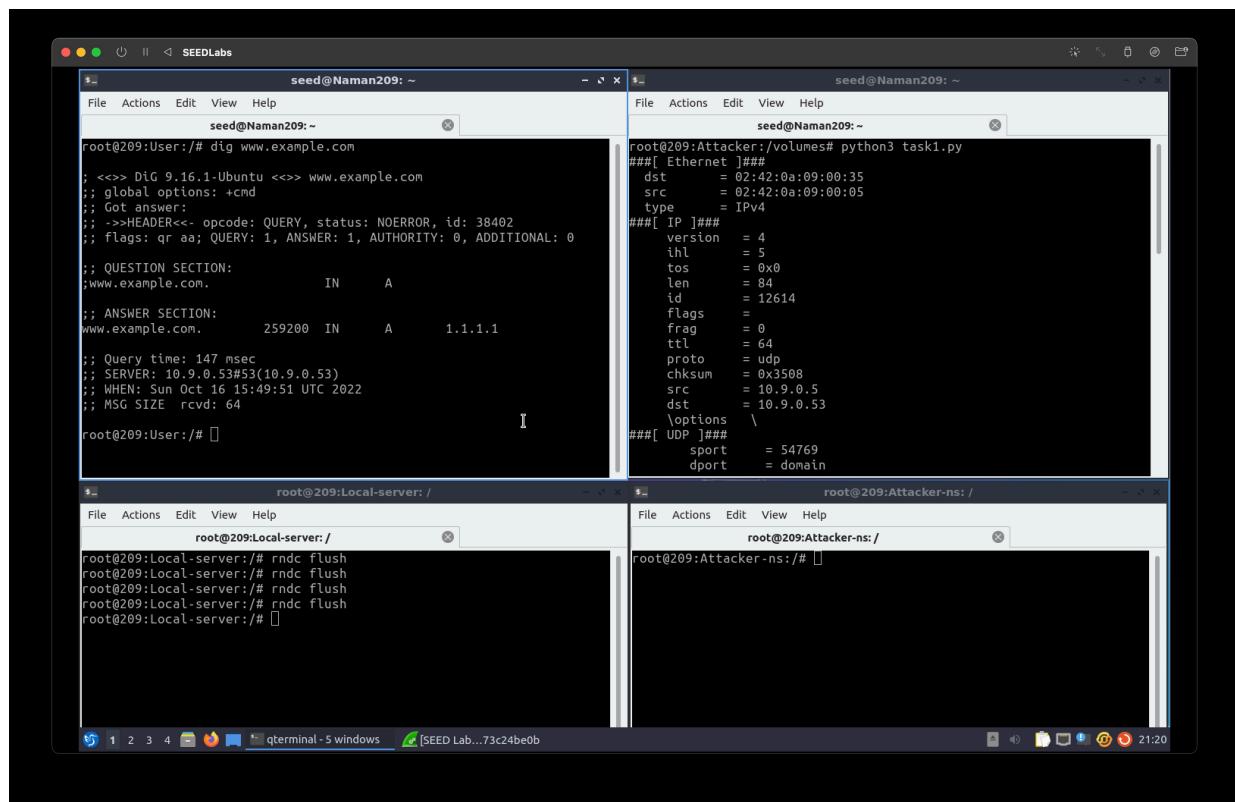
## Task 1: Directly Spoffing Response to User

```
dig www.example.com
```

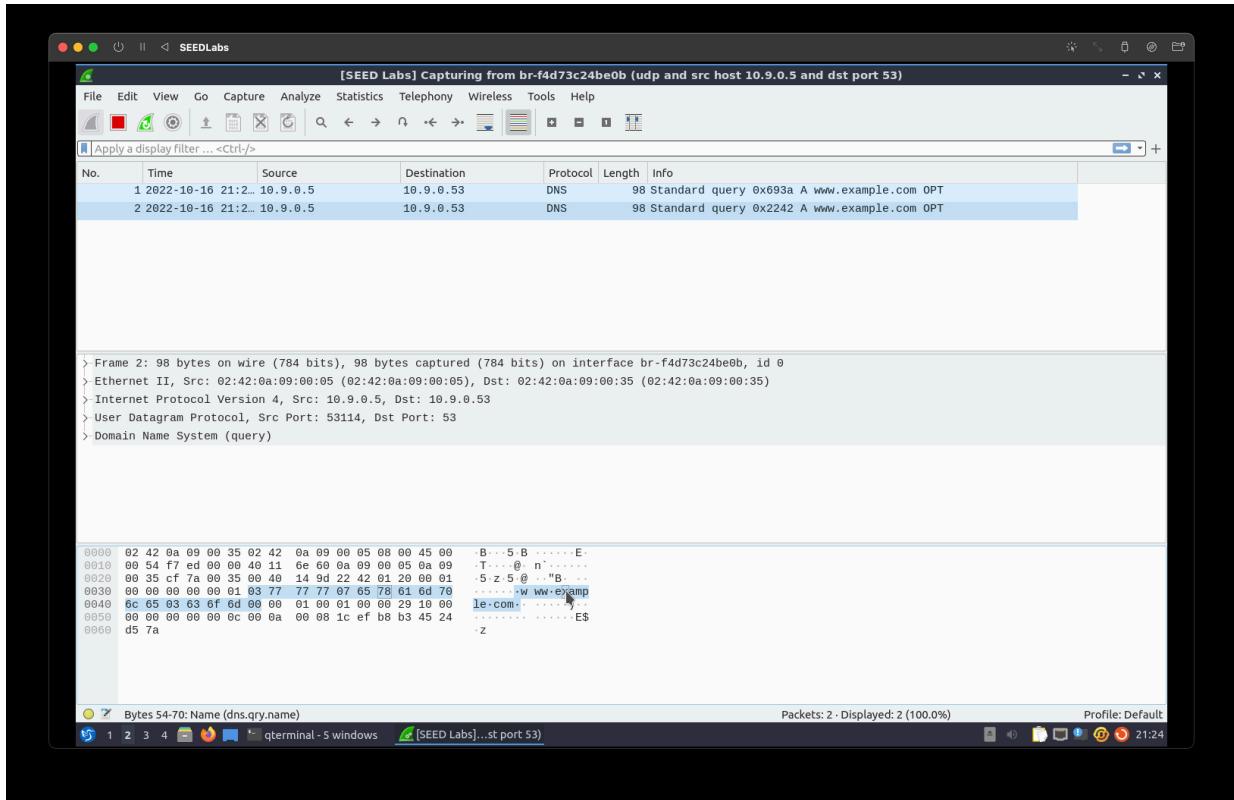


```
python3 task1.py
```

```
dig www.example.com
```



Wireshark:



```
rndc dumpdb -cache  
cat /var/cache/bind/dump.db | grep example
```

```
root@209:Local-server: /  
File Actions Edit View Help  
root@209:Local-server: /  
root@209:Local-server:/# rndc dumpdb -cache  
root@209:Local-server:/# cat /var/cache/bind/dump.db | grep example  
example.com.          691173  NS      a.iana-servers.net.  
                                20221022214625 20221001223409  
1686 example.com.  
www.example.com.       691173  A       93.184.216.34  
                                20221106134841 20221016040716  
59208 example.com.  
root@209:Local-server:/#
```

Observation: When we see the contents of the dump file, we notice that the response is being spoofed to a random ip address

## Task 2: DNS Cache Poisoning Attack – Spoofing Answers

```
python3 task2.py
```

```
dig www.example.com
```

The image shows four terminal windows in a grid, each with a title bar indicating the session name and IP address.

- Top Left Terminal:** seed@Naman209: ~  
Content: A screenshot of the dig command output for www.example.com. It shows a query to port 53, an answer from port 259200, and various flags and time details.
- Top Right Terminal:** seed@Naman209: ~  
Content: A screenshot of the python3 task2.py script. It displays a detailed breakdown of a network packet, including fields like dst, src, type, version, ihl, tos, len, id, flags, frag, ttl, proto, checksum, src, dst, options, sport, and dport.
- Bottom Left Terminal:** root@209:Local-server: /  
Content: A screenshot of the rndc command being used to flush the database cache and flush the database.
- Bottom Right Terminal:** root@209:Attacker-ns: /  
Content: An empty terminal window showing the prompt for the Attacker namespace.

The bottom of the screen features a dock with several icons and the text "qterminal - 5 windows".

## Wireshark:

The screenshot shows the Wireshark interface capturing traffic from the interface `br-f4d73c24be0b` (udp and src host `10.9.0.53` and dst port `53`). The packet list pane displays 31 captured packets, mostly DNS queries for various domains. The details pane shows the structure of a selected DNS query frame, and the bytes pane shows the raw hex and ASCII data.

Selected packet details:

- No. 28: 2022-10-16 21:3... 10.9.0.53 → 199.249.120.1 DNS 95 Standard query 0x37c5 A ns.icann.org OPT
- No. 21: 2022-10-16 21:3... 10.9.0.53 → 199.43.135.53 DNS 98 Standard query 0xide0 A www.example.com OPT
- No. 22: 2022-10-16 21:3... 10.9.0.53 → 192.48.79.30 DNS 102 Standard query 0x58b5 A a.icann-servers.net OPT
- No. 23: 2022-10-16 21:3... 10.9.0.53 → 192.48.79.30 DNS 102 Standard query 0x9786 A b.icann-servers.net OPT
- No. 24: 2022-10-16 21:3... 10.9.0.53 → 192.48.79.30 DNS 102 Standard query 0x9aee AAAA a.icann-servers.net OPT
- No. 25: 2022-10-16 21:3... 10.9.0.53 → 192.48.79.30 DNS 102 Standard query 0x54f0 AAAA b.icann-servers.net OPT
- No. 26: 2022-10-16 21:3... 10.9.0.53 → 192.48.79.30 DNS 102 Standard query 0x26b2 A c.icann-servers.net OPT
- No. 27: 2022-10-16 21:3... 10.9.0.53 → 192.48.79.30 DNS 102 Standard query 0x6255 AAAA c.icann-servers.net OPT
- No. 28: 2022-10-16 21:3... 10.9.0.53 → 199.4.138.53 DNS 95 Standard query 0xbfd7 A ns.icann.org OPT

Selected packet bytes:

0000	02 42 0a 09 00 0b 02 42 0a 09 00 35 00 45 00	B... B... 5. E
0010	00 4a 1f 63 00 00 40 11 6c 09 00 00 35 00 70	J c @ 1 ... 5 p
0020	24 04 02 35 00 35 00 36 ee f9 d1 88 00 10 00 01	\$ 5 5 6 .....
0030	00 00 00 00 00 01 01 5f 03 63 6f 6d 00 01 00	..... .com .....
0040	01 00 00 29 02 00 00 00 80 00 00 0c 00 0a 00 08	(...) .....
0050	55 75 17 f9 9c 5e 38 95	Uu .. ^8.

```
rndc dumpdb -cache  
cat /var/cache/bind/dump.db | grep example
```

A terminal window titled "root@209:Local-server: /". The window contains the following command and its output:

```
root@209:Local-server:# rndc dumpdb -cache  
root@209:Local-server:# rndc flush  
root@209:Local-server:# rndc dumpdb -cache  
root@209:Local-server:# cat /var/cache/bind/dump.db | grep example  
example.com.      777517  NS      a.iana-servers.net.  
www.example.com.  863918  A       1.1.1.1  
root@209:Local-server:#
```

Observation: We observe that a new entry was created because of task2.py

## Task 3: Spoofing NS Records

```
python3 task3.py
```

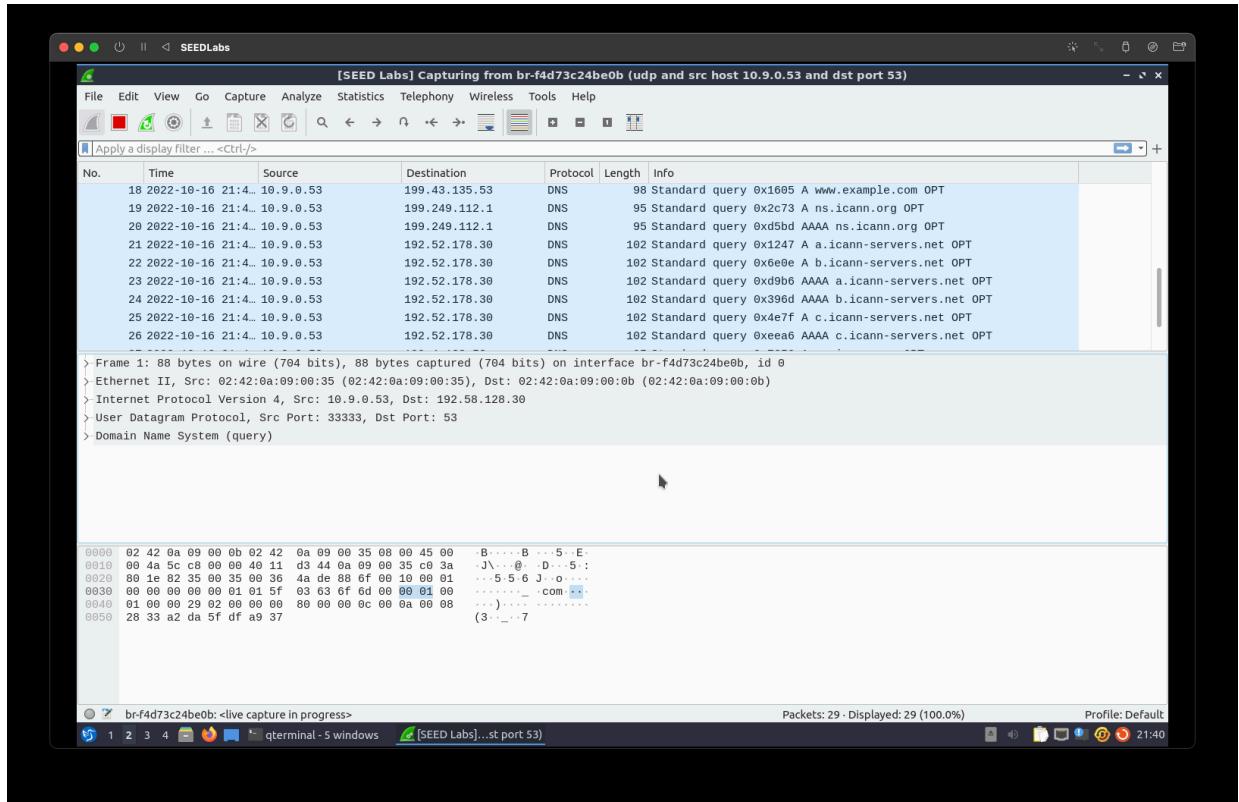
```
dig www.example.com
```

A screenshot of a desktop environment with multiple windows. In the top-left window, a terminal session shows the execution of task3.py and the resulting DNS traffic captured by Wireshark. The terminal output includes:

```
seed@Naman209: ~  
seed@Naman209: ~  
root@209:User:/# dig www.example.com  
;; <>> DiG 9.16.1-Ubuntu <>> www.example.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 27577  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags: udp: 4096  
; COOKIE: f7b47ee7ee0601b701000000634c2ce0f919cf33be8be4b (good)  
;; QUESTION SECTION:  
;www.example.com.      IN      A  
  
;; ANSWER SECTION:  
www.example.com.  259200  IN      A      1.1.1.1  
  
;; Query time: 1332 msec  
;; SERVER: 10.9.0.53#53(10.9.0.53)  
;; WHEN: Sun Oct 16 16:10:08 UTC 2022  
;; MSG SIZE  rcvd: 88
```

The top-right window is a file browser titled "SEEDLabs" showing a directory structure. The bottom-left window is another terminal session titled "root@209:Local-server: /". The bottom-right window is a system tray icon.

## Wireshark:



```
dig www.example.com
dig ftp.example.com
```

```
seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
root@209:User:/# dig ftp.example.com

; <>> DiG 9.16.1-Ubuntu <>> ftp.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38520
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: d281354f9382bd6c01000000634c2d2c64ae9e7a614b9de8 (good)
;; QUESTION SECTION:
;ftp.example.com.           IN      A

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

;; Query time: 36 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 16 16:11:24 UTC 2022
;; MSG SIZE  rcvd: 88
```

```
rndc dumpdb -cache
cat /var/cache/bind/dump.db | grep example
```

```
root@209:Local-server: /
File Actions Edit View Help
root@209:Local-server: /
root@209:Local-server:/# rndc dumpdb -cache
root@209:Local-server:/# cat /var/cache/bind/dump.db | grep example
example.com.      777454  NS      ns.attacker32.com.
ftp.example.com.  863931  A       1.2.3.6
www.example.com. 863855  A       1.1.1.1
root@209:Local-server:/#
```

Observation: The spoofing of the packed has been reflected in the dump file

## Task 4: Spoofing NS Records for Another Domain

```
python3 task3.py
```

```
dig www.example.com
```

seed@Naman209: ~

```
File Actions Edit View Help
seed@Naman209:~
```

```
root@209:User:/# dig www.example.com

; <>> DIG 9.16.1-Ubuntu <>> www.example.com
; global options: +cmd
; Got answer:
; -->>HEADER<< opcode: QUERY, status: NOERROR, id: 50317
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
EDNS: version: 0, flags: udp: 4096
COOKIE: 566d5b8327b625880100000634c2e568eb2d7b4e8100472 (good)
; QUESTION SECTION:
www.example.com. IN A

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

; Query time: 1472 msec
; SERVER: 10.9.0.53#53(10.9.0.53)
; WHEN: Sun Oct 16 16:16:22 UTC 2022
; MSG SIZE rcvd: 88
```

seed@Naman209: ~

```
File Actions Edit View Help
seed@Naman209:~
```

```
root@209:Attacker:/volumes# nano task4.py
root@209: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       = 6529
flags    =
frag    = 0
ttl     = 64
proto   = udp
chksum  = 0x87a
src      = 10.9.0.53
dst      = 199.43.135.53
\options \
###[ UDP ]###
sport    = 33333
dport    = domain
len      = 64
checksum = 0x58f0
###[ DNS ]###
id       = 42885
qr      = 0
opcode  = QUERY
aa      = 0
tc      = 0
rd      = 0
ra      = 0
z       = 0
ad      = 0
cd      = 1
rcode   = ok
qdcount = 1
```

root@209:Local-server: /

```
File Actions Edit View Help
root@209:Local-server:/
```

```
root@209:Local-server:/# []
```

## Wireshark:

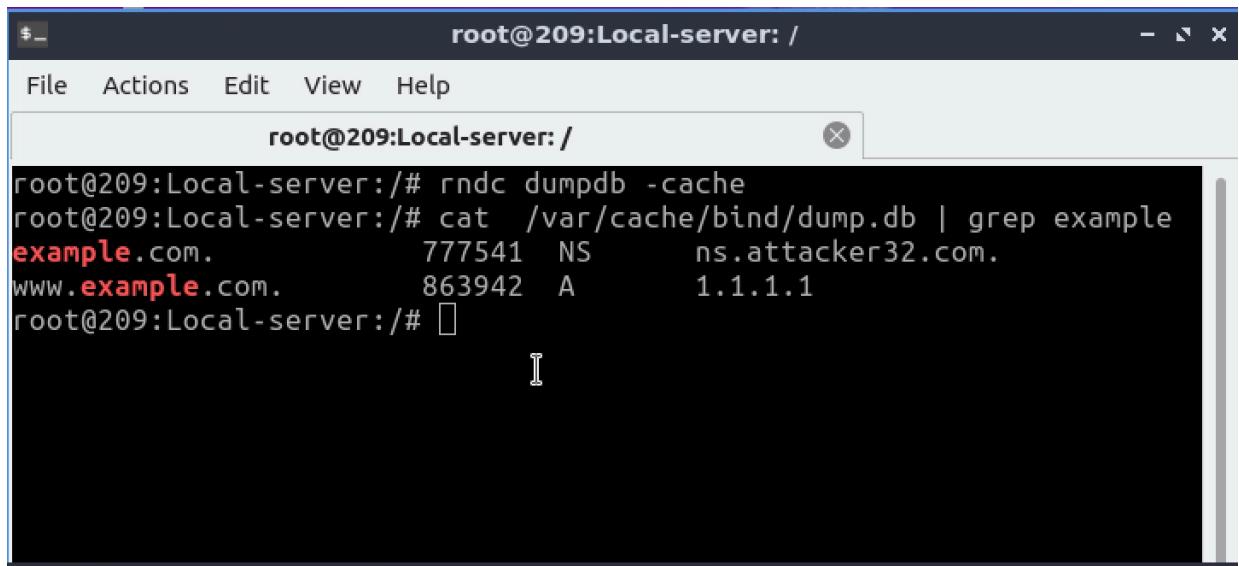
The screenshot shows a Wireshark capture session titled "[SEED Labs] Capturing from br-f4d73c24be0b (udp and src host 10.9.0.53 and dst port 53)". The packet list pane displays 32 captured and 32 displayed packets. The details pane shows the first DNS query for '\_example.com' (Frame 1). The bytes pane shows the raw hex and ASCII data for the captured frame.

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-10-16 21:4... 10.9.0.53		198.41.0.4	DNS	88	Standard query 0x1eb4 A _._com OPT
2	2022-10-16 21:4... 10.9.0.53		192.5.5.241	DNS	82	Standard query 0x0048 NS <Root> OPT
3	2022-10-16 21:4... 10.9.0.53		192.48.79.36	DNS	96	Standard query 0x8661 A _._example.com OPT
4	2022-10-16 21:4... 10.9.0.53		192.36.148.17	DNS	101	Standard query 0x4258 A a.iana-servers.net OPT
5	2022-10-16 21:4... 10.9.0.53		192.36.148.17	DNS	101	Standard query 0xf2ae A b.iana-servers.net OPT
6	2022-10-16 21:4... 10.9.0.53		192.36.148.17	DNS	101	Standard query 0x1ba0 AAAA a.iana-servers.net OPT
7	2022-10-16 21:4... 10.9.0.53		192.36.148.17	DNS	101	Standard query 0xfb64 AAAA b.iana-servers.net OPT
8	2022-10-16 21:4... 10.9.0.53		192.42.93.30	DNS	101	Standard query 0x3595 A b.iana-servers.net OPT
9	2022-10-16 21:4... 10.9.0.53		192.42.93.30	DNS	101	Standard query 0x91f4 A a.iana-servers.net OPT

> Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface br-f4d73c24be0b, id 0  
> Ethernet II, Src: 02:42:0a:09:00:35 (02:42:0a:09:00:35), Dst: 02:42:0a:09:00:0b (02:42:0a:09:00:0b)  
> Internet Protocol Version 4, Src: 10.9.0.53, Dst: 198.41.0.4  
> User Datagram Protocol, Src Port: 33333, Dst Port: 53  
> Domain Name System (query)

0000 82 42 0a 09 00 0b 02 42 0a 09 00 35 00 00 45 00 B .. .B .. .5 - E  
0001 00 4a 00 7f 00 00 40 11 a0 b0 00 00 00 35 06 20 J .. @ .. 5 )  
0020 00 04 02 35 00 35 00 36 d0 b2 1e b4 00 10 00 01 5 5 6 .. .  
0030 00 00 00 00 00 01 01 5f 03 63 6f 6d 00 00 01 00 ..... - .com .. .  
0040 01 00 00 29 02 00 00 00 80 00 00 00 0a 00 08 00 ..... ) .. .  
0050 f4 da 18 3b bc ad e1 5e ..... ; .. ^

```
rndc dumpdb -cache  
cat /var/cache/bind/dump.db | grep example
```



A terminal window titled "root@209:Local-server: /". The window shows the command "rndc dumpdb -cache" followed by "cat /var/cache/bind/dump.db | grep example". The output lists two entries: "example.com." and "www.example.com.". Both entries have an NS record pointing to "ns.attacker32.com." and an A record pointing to "1.1.1.1".

```
root@209:Local-server:/# rndc dumpdb -cache  
root@209:Local-server:/# cat /var/cache/bind/dump.db | grep example  
example.com. 777541 NS ns.attacker32.com.  
www.example.com. 863942 A 1.1.1.1  
root@209:Local-server:/#
```

Observation: ns attacker now becomes the default nameserver due to entries in authority section

## Task 5: Spoofing Records in the Additional Section

```
python3 task3.py
```

```
dig www.example.com
```

```

seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
root@209:User:/# dig www.example.com
; <>> DiG 9.16.1-Ubuntu <>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 64972
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
;; QUESTION SECTION:
;www.example.com.      IN      A
;; ANSWER SECTION:
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
root@209:Local-server: /
File Actions Edit View Help
root@209:Local-server: /root@209:Local-server: /# rndc flush
root@209:Local-server: /# []

```

## Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-10-16 21:5...	10.9.0.53	192.203.230.10	DNS	88	Standard query 0xdd35 A ...com OPT
2	2022-10-16 21:5...	10.9.0.53	199.9.14.201	DNS	82	Standard query 0xd010 NS <Root> OPT
3	2022-10-16 21:5...	10.9.0.53	199.9.14.201	DNS	98	Standard query 0x02b7 NS <Root> OPT
4	2022-10-16 21:5...	10.9.0.53	192.5.6.30	DNS	96	Standard query 0xed20 A ...example.com OPT
5	2022-10-16 21:5...	10.9.0.53	202.12.27.33	DNS	181	Standard query 0x4761 A b.iana-servers.net OPT
6	2022-10-16 21:5...	10.9.0.53	202.12.27.33	DNS	181	Standard query 0x339c AAAA a.iana-servers.net OPT
7	2022-10-16 21:5...	10.9.0.53	202.12.27.33	DNS	181	Standard query 0xe11c AAAA b.iana-servers.net OPT
8	2022-10-16 21:5...	10.9.0.53	202.12.27.33	DNS	181	Standard query 0x23d4 A a.iana-servers.net OPT
9	2022-10-16 21:5...	10.9.0.53	192.33.14.30	DNS	181	Standard query 0xc549 AAAA b.iana-servers.net OPT

> Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface br-f4d73c24be0b, id 0  
> Ethernet II, Src: 02:42:0a:09:00:35 (02:42:0a:09:00:35), Dst: 02:42:0a:09:00:0b (02:42:0a:09:00:0b)  
> Internet Protocol Version 4, Src: 10.9.0.53, Dst: 192.203.230.10  
> User Datagram Protocol, Src Port: 33333, Dst Port: 53  
> Domain Name System (query)

0000 02 42 0a 09 00 35 02 42 0a 09 00 35 08 00 45 00 .B...B...5.E.  
0001 f3 2e 00 00 00 46 1d 69 0a 09 00 35 c9 cb ..J...@...5...  
0002 05 0a 82 35 00 35 00 00 b1 5b dd 35 00 10 00 01 ..5.5.6 [5...  
0003 00 00 00 00 00 01 01 5f 03 03 6f 6d 00 00 01 00 .....com....  
0004 01 00 00 29 02 00 00 00 00 00 00 00 0a 00 00 08 ....)-.....  
0005 64 85 cc f0 7a 39 a3 d8 d...z9...

```

rndc dumpdb -cache
cat /var/cache/bind/dump.db | grep example

```

The screenshot shows a terminal window titled "root@209:Local-server: /". The terminal window has a menu bar with "File", "Actions", "Edit", "View", and "Help". The title bar also displays "root@209:Local-server: /". The main area of the terminal shows the following command-line session:

```
root@209:Local-server:/# rndc flush
root@209:Local-server:/# rndc dumpdb -cache
root@209:Local-server:/# cat /var/cache/bind/dump.db | grep example
example.com.      777561  NS      a.iana-servers.net.
root@209:Local-server:/#
```

Observation: attack successful on the default nameserver due to entries in additional section