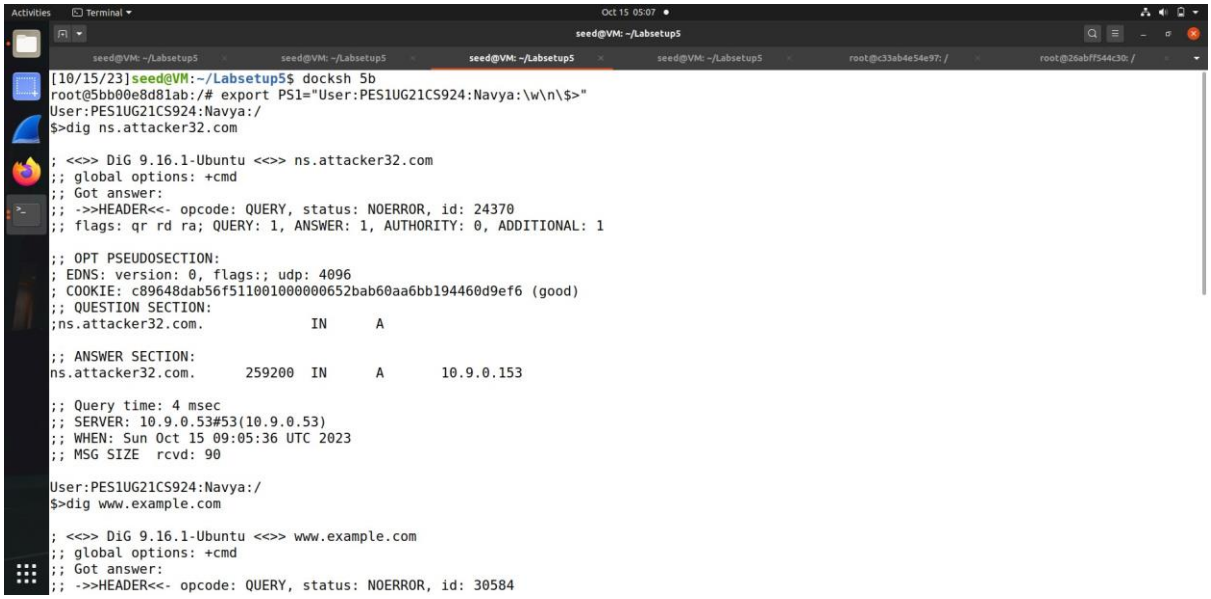
CNS LAB 5 – LOCAL DNS

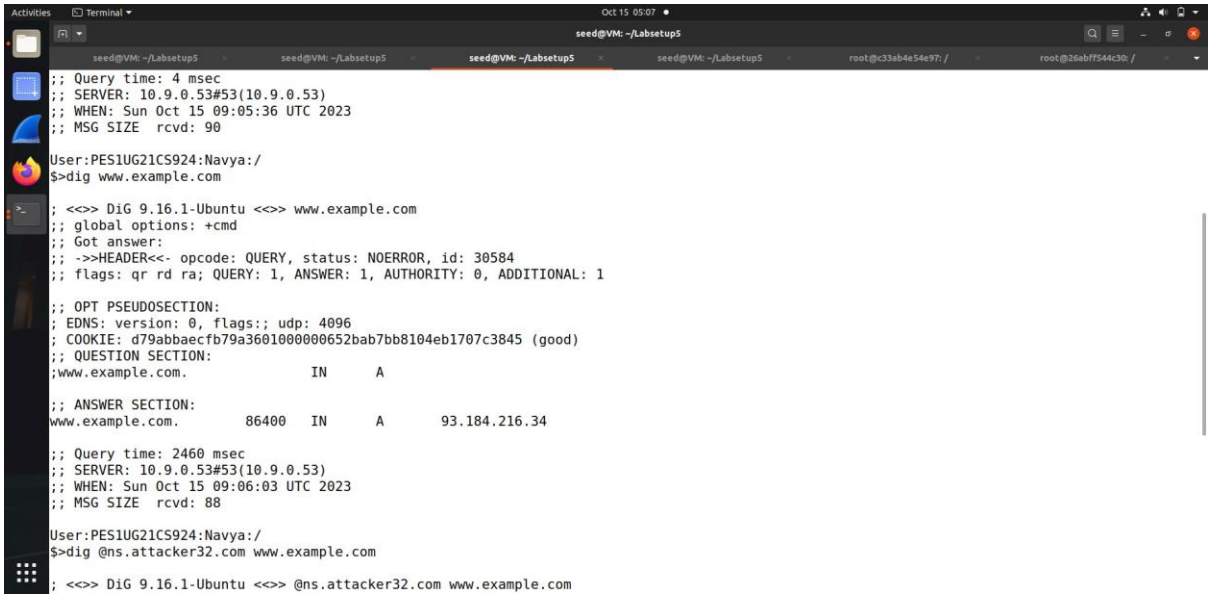
NAME: NAVYA PERAM

SRN: PES1UG21CS924

Checks



The ip address is obtained from the zone file on the attacker nameserver. Since the attacker nameserver has an ip address of 10.9.0.153, we observe that the server was setup in the correct manner.

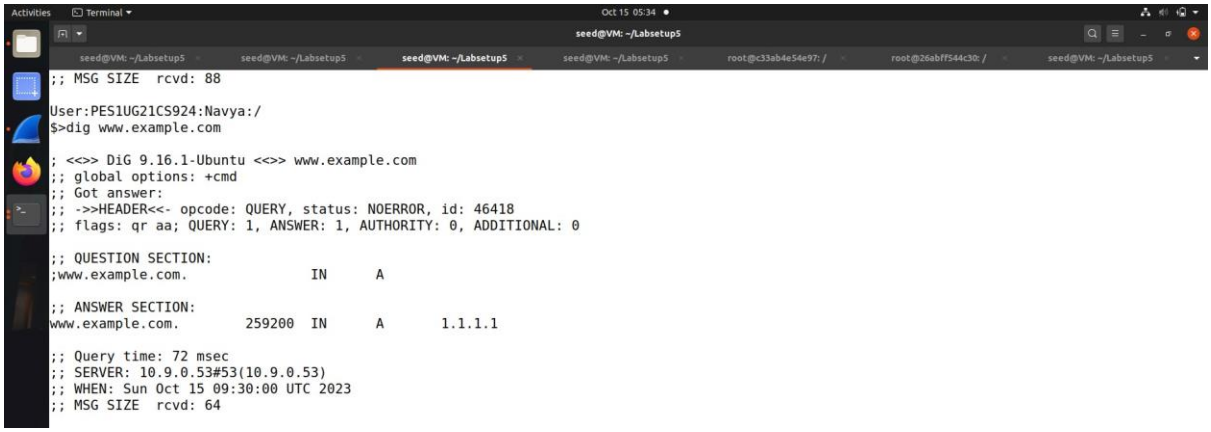


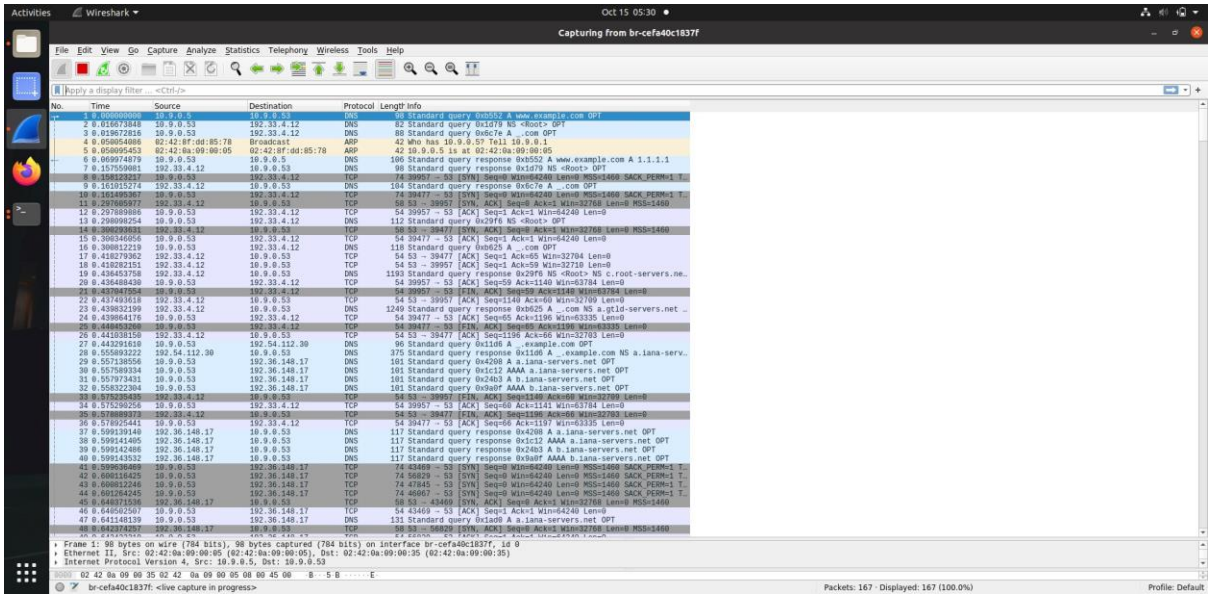
Here, the query goes to the local DNS server and it returns the ip address of example.com, which we know is always constant and of the value 93.184.216.34

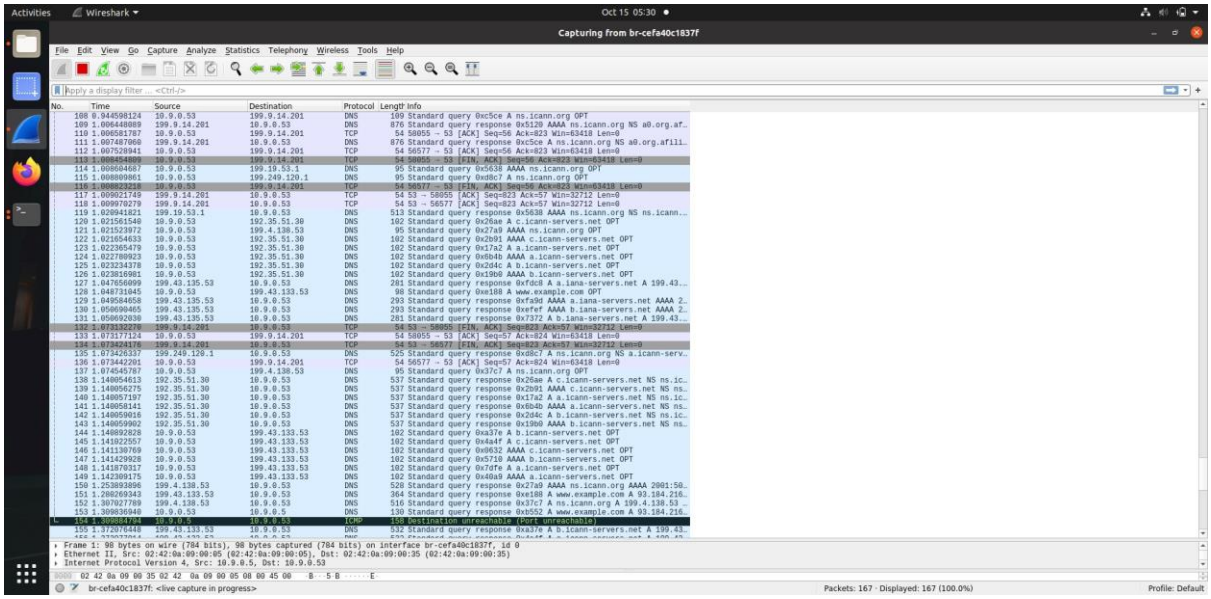
Here, the DNS query for example.com goes to the attacker's nameserver which then returns it's ip address as 1.2.3.5 . On contrasting with the above two methods, we can imply that this ip has been spoofed.

Task 1

Before

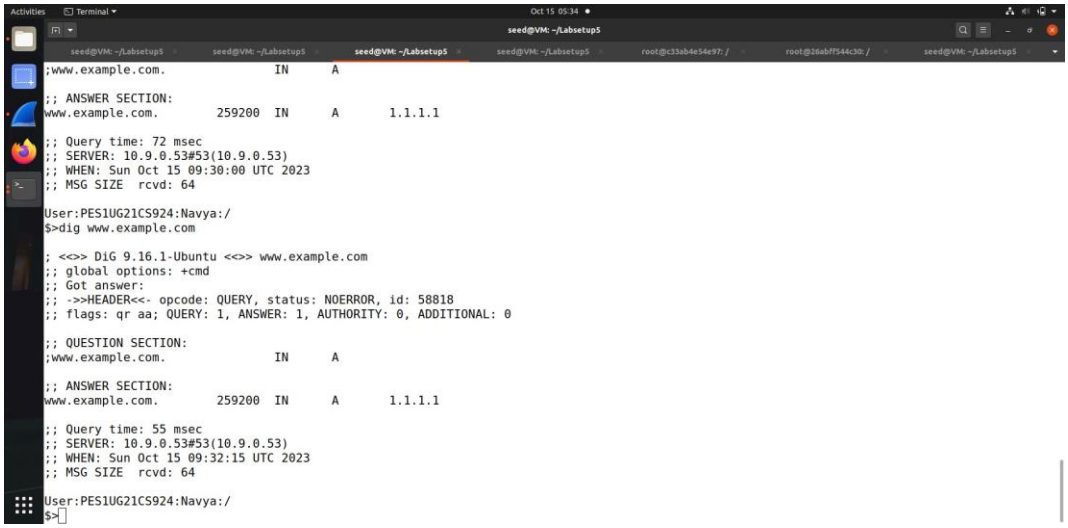




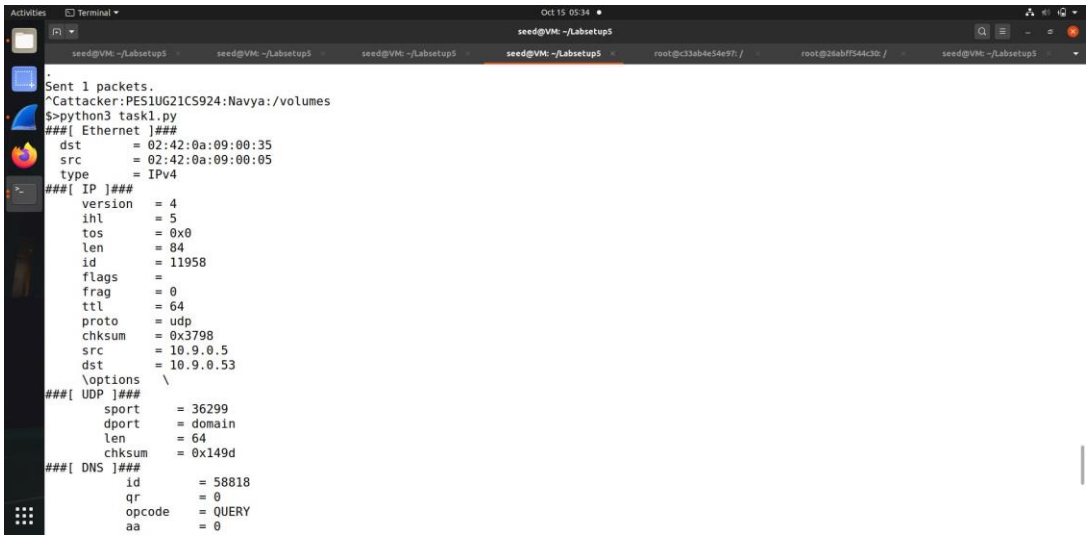


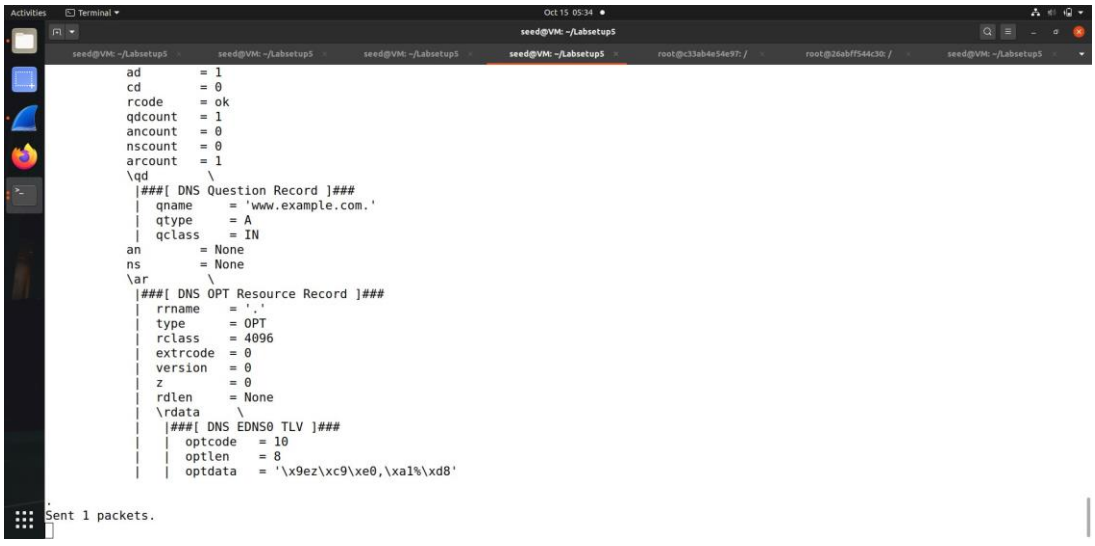
Here, the router queries the other DNS servers to find the ip address of example.com. This process is iterative as the router is querying other servers and is able to receive the replies from them. After it receives the ip address of example.com it sends it to the user.

After

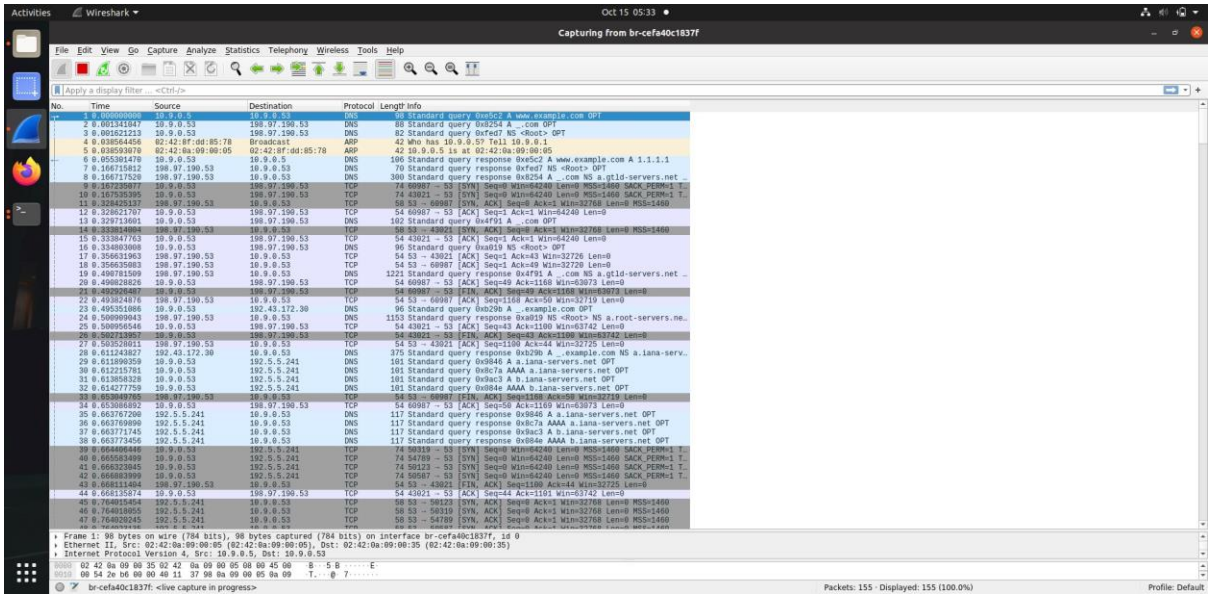


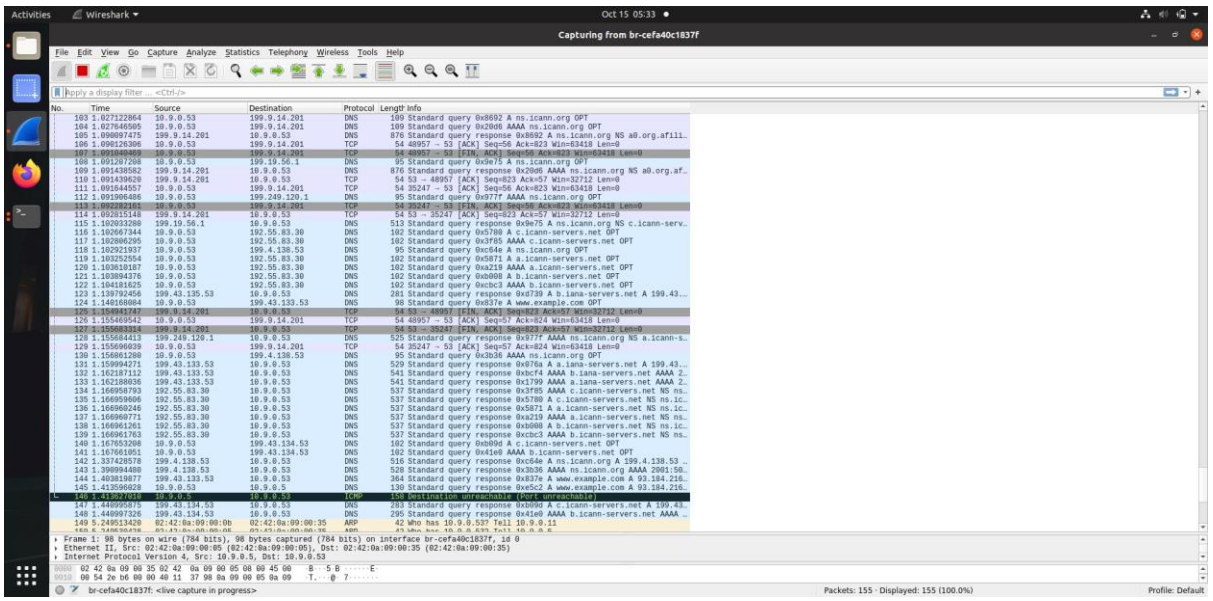
We observe that the response to the DNS query sent by the user of example.com is spoofed by the attacker to be 1.1.1.1

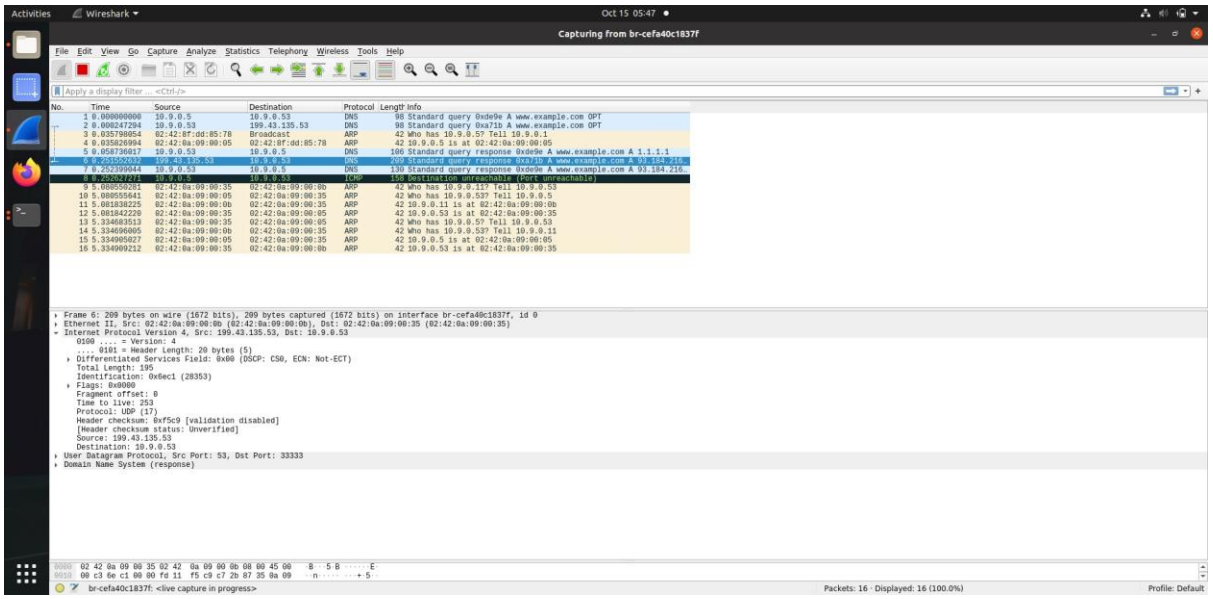




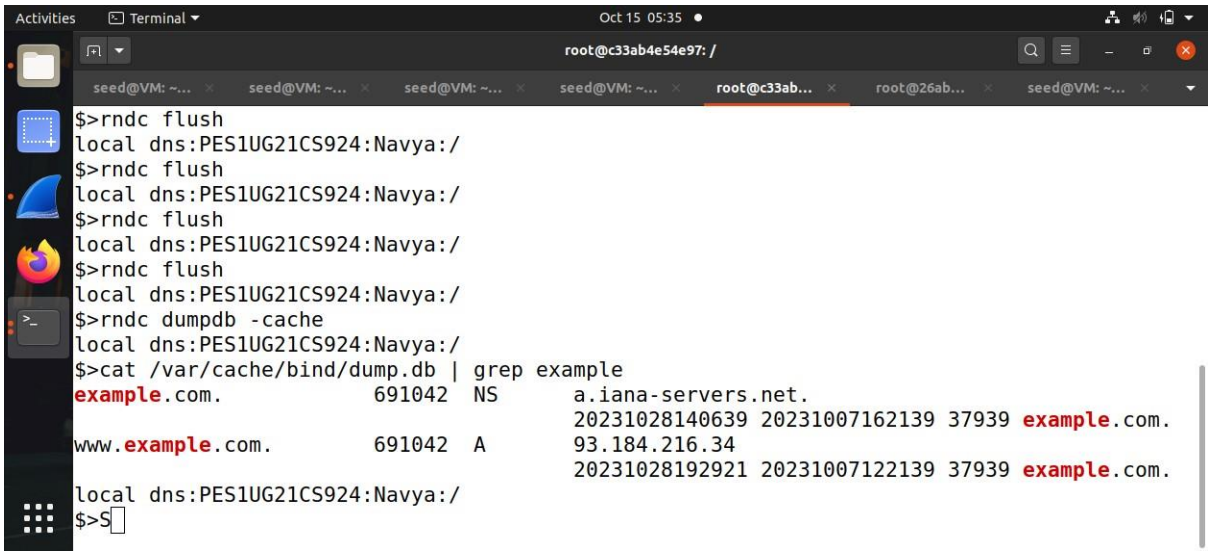
We observe that the packet is sent by the attacker. The packet has the DNS reply for the user's query.


Activities
Wireshark
Oct 15 05:33
Capturing from br-cefa40c1837f
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 10.9.0.5 10.9.0.53 DNS 98 Standard query 0xe5c2 A www.example.com OPT
2 0.001341047 10.9.0.53 198.97.190.53 DNS 80 Standard query 0x8254 A _.com OPT
3 0.001621213 10.9.0.53 198.97.190.53 DNS 82 Standard query 0xfed7 NS <Root> OPT
4 0.038564456 02:42:8f:dd:85:78 Broadcast ARP 42 Who has 10.9.0.5? Tell 10.9.0.1
5 0.038593070 02:42:0a:09:00:05 02:42:8f:dd:85:78 ARP 42 10.9.0.5 is at 02:42:0a:09:00:05
6 0.055301470 10.9.0.53 10.9.0.5 DNS 106 Standard query response 0xe5c2 A www.example.com A 1.1.1.1
7 0.166715812 198.97.190.53 10.9.0.53 DNS 70 Standard query response 0xfed7 NS <Root> OPT
8 0.166717520 198.97.190.53 10.9.0.53 DNS 300 Standard query response 0x8254 A _.com NS a.gtld-servers.net …
9 0.167225077 10.9.0.53 198.97.190.53 TCP 74 60987 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
10 0.167535395 10.9.0.53 198.97.190.53 TCP 74 43021 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
11 0.328425137 198.97.190.53 10.9.0.53 TCP 58 53 → 60987 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
12 0.328621707 10.9.0.53 198.97.190.53 TCP 54 60987 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
13 0.329713601 10.9.0.53 198.97.190.53 DNS 102 Standard query 0x4f91 A _.com OPT
14 0.331014024 198.97.190.53 10.9.0.53 TCP 58 53 → 43021 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
15 0.333847763 10.9.0.53 198.97.190.53 TCP 54 43021 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16 0.334803008 10.9.0.53 198.97.190.53 DNS 96 Standard query 0xa019 NS <Root> OPT
17 0.356631963 198.97.190.53 10.9.0.53 TCP 54 53 → 43021 [ACK] Seq=1 Ack=43 Win=32726 Len=0
18 0.356635083 198.97.190.53 10.9.0.53 TCP 54 53 → 60987 [ACK] Seq=1 Ack=49 Win=32720 Len=0
19 0.490781509 198.97.190.53 10.9.0.53 DNS 1221 Standard query response 0x4f91 A _.com NS a.gtld-servers.net …
20 0.490828826 10.9.0.53 198.97.190.53 TCP 54 60987 → 53 [ACK] Seq=49 Ack=1168 Win=63073 Len=0
21 0.492926487 198.97.190.53 10.9.0.53 TCP 54 60987 → 53 [FIN, ACK] Seq=49 Ack=1168 Win=63073 Len=0
22 0.493824876 198.97.190.53 10.9.0.53 TCP 54 53 → 60987 [ACK] Seq=1168 Ack=50 Win=32719 Len=0
23 0.495351086 10.9.0.53 192.43.172.30 DNS 96 Standard query 0xb29b A _.example.com OPT
24 0.500999043 198.97.190.53 10.9.0.53 DNS 1153 Standard query response 0xa019 NS <Root> NS a.root-servers.ne…
25 0.500956546 10.9.0.53 198.97.190.53 TCP 54 43021 → 53 [ACK] Seq=43 Ack=1100 Win=63742 Len=0
26 0.502713957 10.9.0.53 198.97.190.53 TCP 54 43021 → 53 [FIN, ACK] Seq=43 Ack=1100 Win=63742 Len=0
27 0.503528011 198.97.190.53 10.9.0.53 TCP 54 53 → 43021 [ACK] Seq=1100 Ack=44 Win=32725 Len=0
28 0.611243827 192.43.172.30 10.9.0.53 DNS 375 Standard query response 0xb29b A _.example.com NS a.iana-serv…
29 0.611890359 10.9.0.53 192.5.5.241 DNS 101 Standard query 0x9846 A a.iana-servers.net OPT
30 0.612215781 10.9.0.53 192.5.5.241 DNS 101 Standard query 0x8c7a AAAA a.iana-servers.net OPT
31 0.613858328 10.9.0.53 192.5.5.241 DNS 101 Standard query 0x9ac3 A b.iana-servers.net OPT
32 0.614277759 10.9.0.53 192.5.5.241 DNS 101 Standard query 0x984e AAAA b.iana-servers.net OPT
33 0.651044755 198.97.190.53 10.9.0.53 TCP 54 53 → 60987 [FIN, ACK] Seq=1168 Ack=50 Win=32719 Len=0
34 0.653066892 10.9.0.53 198.97.190.53 TCP 54 60987 → 53 [ACK] Seq=50 Ack=1169 Win=63073 Len=0
35 0.663767200 192.5.5.241 10.9.0.53 DNS 117 Standard query response 0x9846 A a.iana-servers.net OPT
36 0.663769090 192.5.5.241 10.9.0.53 DNS 117 Standard query response 0x8c7a AAAA a.iana-servers.net OPT
37 0.663771745 192.5.5.241 10.9.0.53 DNS 117 Standard query response 0x9ac3 A b.iana-servers.net OPT
38 0.663773456 192.5.5.241 10.9.0.53 DNS 117 Standard query response 0x984e AAAA b.iana-servers.net OPT
39 0.664496446 10.9.0.53 192.5.5.241 TCP 74 56319 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
40 0.665583499 10.9.0.53 192.5.5.241 TCP 74 54789 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
41 0.666323045 10.9.0.53 192.5.5.241 TCP 74 59123 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
42 0.666883999 10.9.0.53 192.5.5.241 TCP 74 50587 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
43 0.668114404 198.97.190.53 10.9.0.53 TCP 54 53 → 43021 [FIN, ACK] Seq=1100 Ack=44 Win=32725 Len=0
44 0.668135874 10.9.0.53 198.97.190.53 TCP 54 43021 → 53 [ACK] Seq=44 Ack=1101 Win=63742 Len=0
45 0.764015454 192.5.5.241 10.9.0.53 TCP 58 53 → 59123 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
46 0.764018055 192.5.5.241 10.9.0.53 TCP 58 53 → 56319 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
47 0.764020245 192.5.5.241 10.9.0.53 TCP 58 53 → 54789 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface br-cefa40c1837f, 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
0000 02 42 0a 09 00 35 02 42 0a 09 00 05 08 00 45 00 ·B···5·B ·····E·
0010 00 54 2e b6 00 00 40 11 37 98 0a 09 00 05 0a 09 ·T....@· 7·····
br-cefa40c1837f: <live capture in progress>
Packets: 155 · Displayed: 155 (100.0%)
Profile: Default


Activities
Wireshark
Oct 15 05:33
Capturing from br-cefa40c1837f
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
103 1.027122864 10.9.0.53 199.9.14.201 DNS 109 Standard query 0x8692 A ns.icann.org OPT
104 1.027646505 10.9.0.53 199.9.14.201 DNS 109 Standard query 0x20d6 AAAA ns.icann.org OPT
105 1.090097475 199.9.14.201 10.9.0.53 DNS 876 Standard query response 0x8692 A ns.icann.org NS a0.org.afili…
106 1.090126306 10.9.0.53 199.9.14.201 TCP 54 48957 → 53 [ACK] Seq=56 Ack=823 Win=63418 Len=0
107 1.091004409 10.9.0.53 199.9.14.201 TCP 54 48957 → 53 [FIN, ACK] Seq=56 Ack=823 Win=63418 Len=0
108 1.091207208 10.9.0.53 199.19.56.1 DNS 95 Standard query 0x9e75 A ns.icann.org OPT
109 1.091438582 199.9.14.201 10.9.0.53 DNS 876 Standard query response 0x20d6 AAAA ns.icann.org NS a0.org.af…
110 1.091439620 199.9.14.201 10.9.0.53 TCP 54 53 → 48957 [ACK] Seq=823 Ack=57 Win=32712 Len=0
111 1.091644557 10.9.0.53 199.9.14.201 TCP 54 35247 → 53 [ACK] Seq=56 Ack=823 Win=63418 Len=0
112 1.091906486 10.9.0.53 199.249.120.1 DNS 95 Standard query 0x977f AAAA ns.icann.org OPT
113 1.092282161 10.9.0.53 199.9.14.201 TCP 54 35247 → 53 [FIN, ACK] Seq=56 Ack=823 Win=63418 Len=0
114 1.092815148 199.9.14.201 10.9.0.53 TCP 54 53 → 35247 [ACK] Seq=823 Ack=57 Win=32712 Len=0
115 1.102033280 199.19.56.1 10.9.0.53 DNS 513 Standard query response 0x9e75 A ns.icann.org NS c.icann-serv…
116 1.102667344 10.9.0.53 192.55.83.30 DNS 102 Standard query 0x5780 A c.icann-servers.net OPT
117 1.102806295 10.9.0.53 192.55.83.30 DNS 102 Standard query 0x3f85 AAAA c.icann-servers.net OPT
118 1.102921937 10.9.0.53 199.4.138.53 DNS 95 Standard query 0xc64e A ns.icann.org OPT
119 1.103252554 10.9.0.53 192.55.83.30 DNS 102 Standard query 0x5871 A a.icann-servers.net OPT
120 1.103610187 10.9.0.53 192.55.83.30 DNS 102 Standard query 0xa219 AAAA a.icann-servers.net OPT
121 1.103894376 10.9.0.53 192.55.83.30 DNS 102 Standard query 0xb006 A b.icann-servers.net OPT
122 1.104181625 10.9.0.53 192.55.83.30 DNS 102 Standard query 0xcbc3 AAAA b.icann-servers.net OPT
123 1.139792456 199.43.135.53 10.9.0.53 DNS 281 Standard query response 0xd739 A a.iana-servers.net A 199.43.…
124 1.140168604 10.9.0.53 199.43.133.53 DNS 98 Standard query 0x837e A www.example.com OPT
125 1.154941747 199.9.14.201 10.9.0.53 TCP 54 53 → 48957 [FIN, ACK] Seq=823 Ack=57 Win=32712 Len=0
126 1.155469542 10.9.0.53 199.9.14.201 TCP 54 48957 → 53 [ACK] Seq=57 Ack=824 Win=63418 Len=0
127 1.155683314 199.9.14.201 10.9.0.53 TCP 54 53 → 35247 [FIN, ACK] Seq=823 Ack=57 Win=32712 Len=0
128 1.155684413 199.249.120.1 10.9.0.53 DNS 525 Standard query response 0x977f AAAA ns.icann.org NS a.icann-s…
129 1.155696039 10.9.0.53 199.9.14.201 TCP 54 35247 → 53 [ACK] Seq=57 Ack=824 Win=63418 Len=0
130 1.156861280 10.9.0.53 199.4.138.53 DNS 95 Standard query 0x3b36 AAAA ns.icann.org OPT
131 1.159994271 199.43.133.53 10.9.0.53 DNS 529 Standard query response 0x076a A a.iana-servers.net A 199.43.…
132 1.162187112 199.43.133.53 10.9.0.53 DNS 541 Standard query response 0xbcf4 AAAA b.iana-servers.net AAAA 2…
133 1.162188036 199.43.133.53 10.9.0.53 DNS 541 Standard query response 0x1799 AAAA a.iana-servers.net AAAA 2…
134 1.166958793 192.55.83.30 10.9.0.53 DNS 537 Standard query response 0x3f85 AAAA c.icann-servers.net NS ns…
135 1.166959606 192.55.83.30 10.9.0.53 DNS 537 Standard query response 0x5780 A c.icann-servers.net NS ns.ic…
136 1.166960246 192.55.83.30 10.9.0.53 DNS 537 Standard query response 0x5871 A a.icann-servers.net NS ns.ic…
137 1.166960771 192.55.83.30 10.9.0.53 DNS 537 Standard query response 0xa219 AAAA a.icann-servers.net NS ns…
138 1.166961261 192.55.83.30 10.9.0.53 DNS 537 Standard query response 0xb008 A b.icann-servers.net NS ns.ic…
139 1.166961763 192.55.83.30 10.9.0.53 DNS 537 Standard query response 0xcbc3 AAAA b.icann-servers.net NS ns…
140 1.167053208 10.9.0.53 199.43.134.53 DNS 102 Standard query 0xb006 A c.icann-servers.net OPT
141 1.167661051 10.9.0.53 199.43.134.53 DNS 102 Standard query 0x41e0 AAAA b.icann-servers.net OPT
142 1.337428578 199.4.138.53 10.9.0.53 DNS 516 Standard query response 0xc64e A ns.icann.org A 199.4.138.53 …
143 1.390994480 199.4.138.53 10.9.0.53 DNS 528 Standard query response 0x3b36 AAAA ns.icann.org AAAA 2001:50…
144 1.403819877 199.43.133.53 10.9.0.53 DNS 364 Standard query response 0x837e A www.example.com A 93.184.216…
145 1.413596028 10.9.0.5 10.9.0.53 DNS 130 Standard query response 0xe5c2 A www.example.com A 93.184.216…
146 1.413827018 10.9.0.5 10.9.0.53 ICMP 158 Destination unreachable (Port unreachable)
147 1.440995875 199.43.134.53 10.9.0.53 DNS 283 Standard query response 0xb09d A c.icann-servers.net A 199.43…
148 1.440997326 199.43.134.53 10.9.0.53 DNS 295 Standard query response 0x41e0 AAAA b.icann-servers.net AAAA …
149 5.249513420 02:42:0a:09:00:0b 02:42:0a:09:00:35 ARP 42 Who has 10.9.0.53? Tell 10.9.0.11
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface br-cefa40c1837f, 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
0000 02 42 0a 09 00 35 02 42 0a 09 00 05 08 00 45 00 ·B···5·B ·····E·
0010 00 54 2e b6 00 00 40 11 37 98 0a 09 00 05 0a 09 ·T....@· 7·····
br-cefa40c1837f: <live capture in progress>
Packets: 155 · Displayed: 155 (100.0%)
Profile: Default


Activities
Wireshark
Oct 15 05:47
Capturing from br-cefa40c1837f
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 10.9.0.5 10.9.0.53 DNS 98 Standard query 0xde9e A www.example.com OPT
2 0.000247204 10.9.0.53 199.43.135.53 DNS 98 Standard query 0xa71b A www.example.com OPT
3 0.035798054 02:42:8f:dd:85:78 Broadcast ARP 42 Who has 10.9.0.5? Tell 10.9.0.1
4 0.035826994 02:42:0a:09:00:05 02:42:8f:dd:85:78 ARP 42 10.9.0.5 is at 02:42:0a:09:00:05
5 0.043736017 10.9.0.53 10.9.0.5 DNS 106 Standard query response 0xde9e A www.example.com A 1.1.1.1
6 0.251552632 199.43.135.53 10.9.0.53 DNS 209 Standard query response 0xa71b A www.example.com A 93.184.216…
7 0.252399044 10.9.0.53 10.9.0.5 DNS 130 Standard query response 0xde9e A www.example.com A 93.184.216…
8 0.252624721 10.9.0.5 10.9.0.53 ICMP 158 Destination unreachable (Port unreachable)
9 5.080550281 02:42:0a:09:00:35 02:42:0a:09:00:0b ARP 42 Who has 10.9.0.11? Tell 10.9.0.53
10 5.080555641 02:42:0a:09:00:0b 02:42:0a:09:00:35 ARP 42 Who has 10.9.0.53? Tell 10.9.0.5
11 5.081838225 02:42:0a:09:00:0b 02:42:0a:09:00:35 ARP 42 10.9.0.11 is at 02:42:0a:09:00:0b
12 5.081842220 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
13 5.334603513 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
14 5.334696005 02:42:0a:09:00:0b 02:42:0a:09:00:35 ARP 42 Who has 10.9.0.53? Tell 10.9.0.11
15 5.334905027 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
16 5.334909212 02:42:0a:09:00:35 02:42:0a:09:00:0b ARP 42 10.9.0.53 is at 02:42:0a:09:00:35
Frame 6: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface br-cefa40c1837f, id 0
Ethernet II, Src: 02:42:0a:09:00:0b (02:42:0a:09:00:0b), Dst: 02:42:0a:09:00:35 (02:42:0a:09:00:35)
Internet Protocol Version 4, Src: 199.43.135.53, Dst: 10.9.0.53
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 195
Identification: 0x6ec1 (28353)
Flags: 0x0000
Fragment offset: 0
Time to live: 253
Protocol: UDP (17)
Header checksum: 0xf5c9 [validation disabled]
[Header checksum status: Unverified]
Source: 199.43.135.53
Destination: 10.9.0.53
User Datagram Protocol, Src Port: 53, Dst Port: 33333
Domain Name System (response)
0000 02 42 0a 09 00 35 02 42 0a 09 00 0b 08 00 45 00 ·B···5·B ·····E·
0010 00 c3 6e c1 00 00 fd 11 f5 c9 c7 2b 87 35 0a 09 ··n····· ···+·5··
br-cefa40c1837f: <live capture in progress>
Packets: 16 · Displayed: 16 (100.0%)
Profile: Default

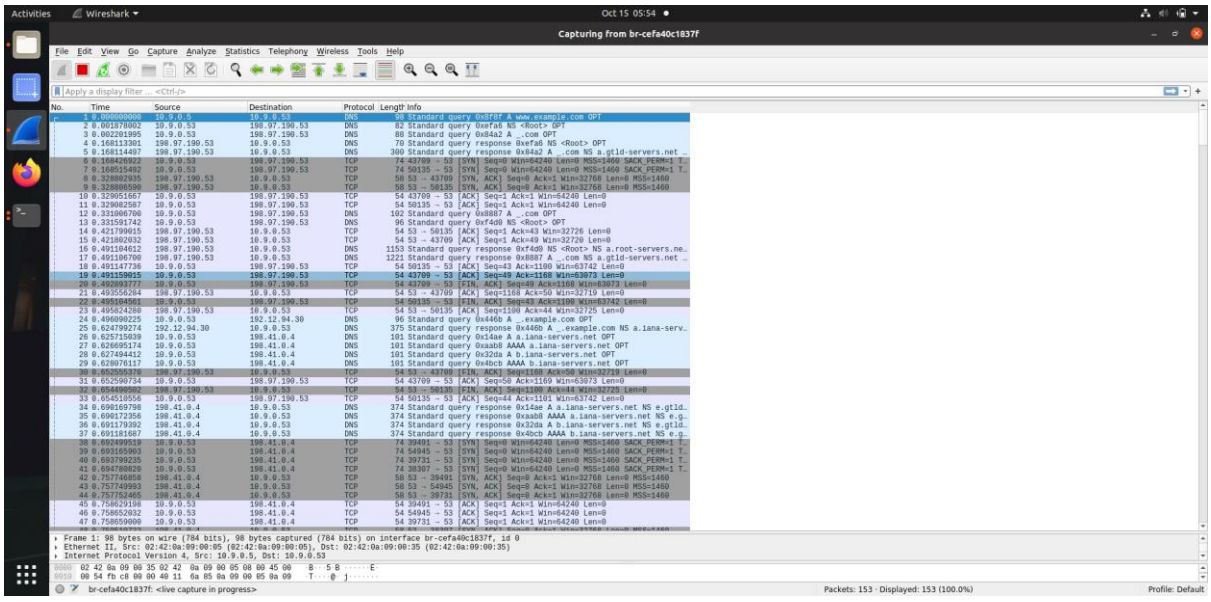
We can observe that the spoofed packet arrives much before the actual packet. The spoofed packet is sent from 10.9.0.5 and is considered by the user/victim to be the actual ip address of their query.

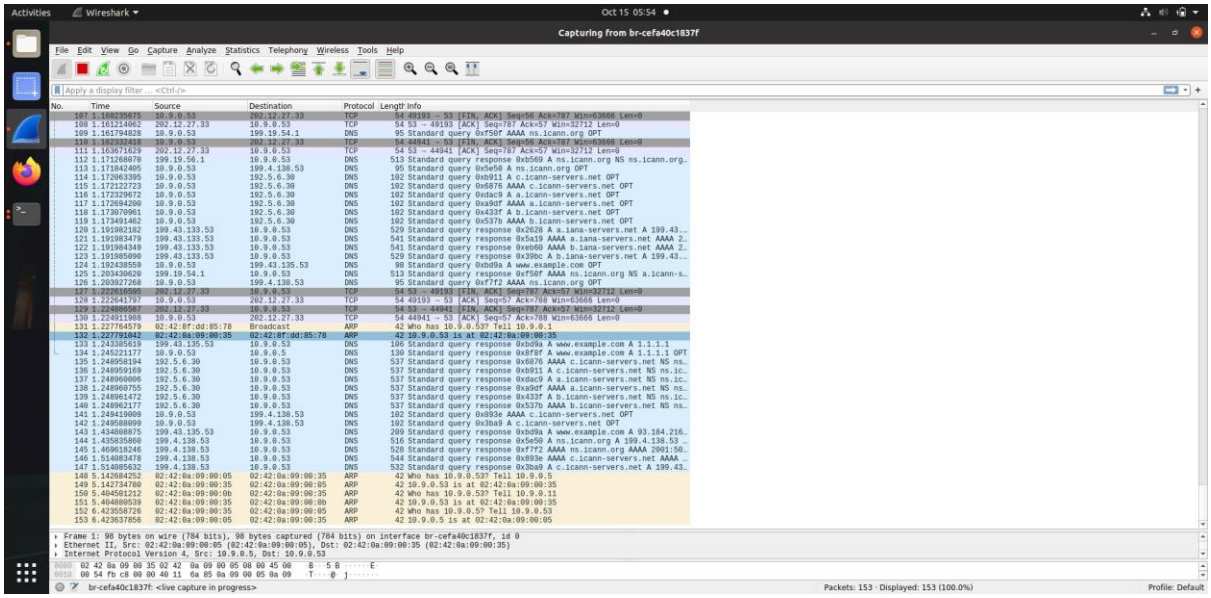


We use rndc flush to clear the cache.

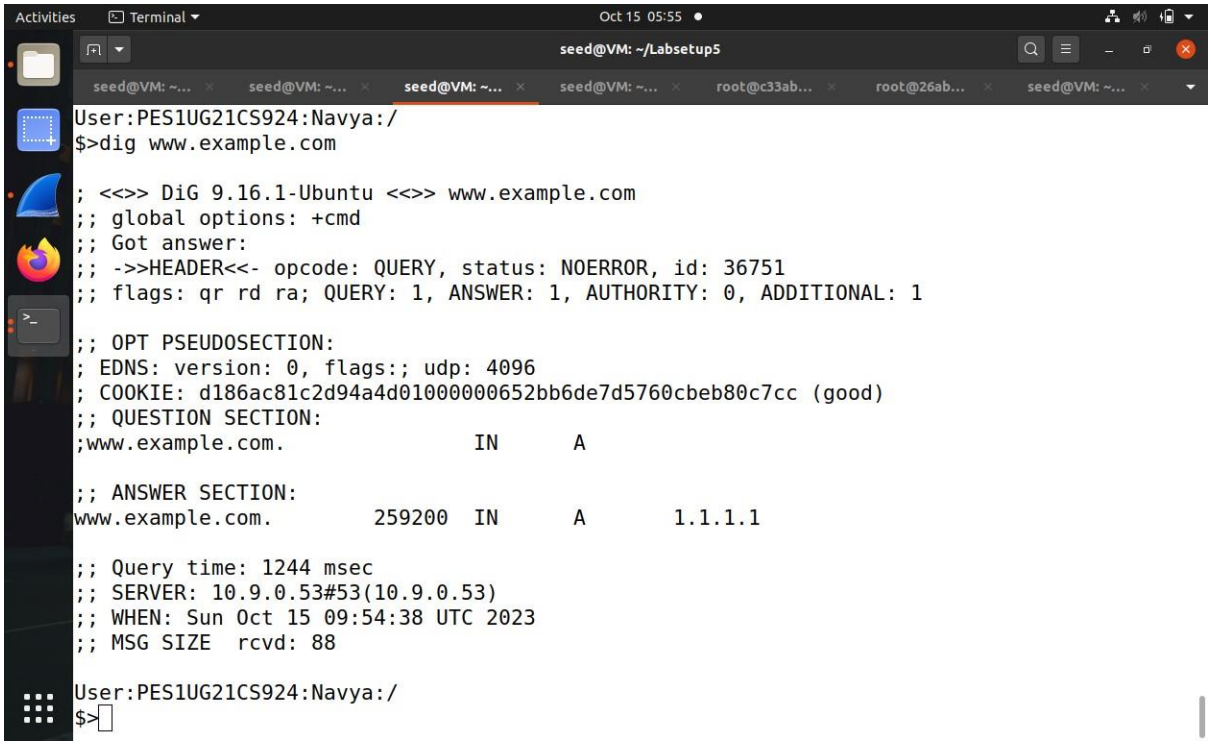
Here, we can view the cache of the DNS server and find no change, as the spoofed packet was sent to the user by the attacker. There is no change in the ip address here.

Task 2

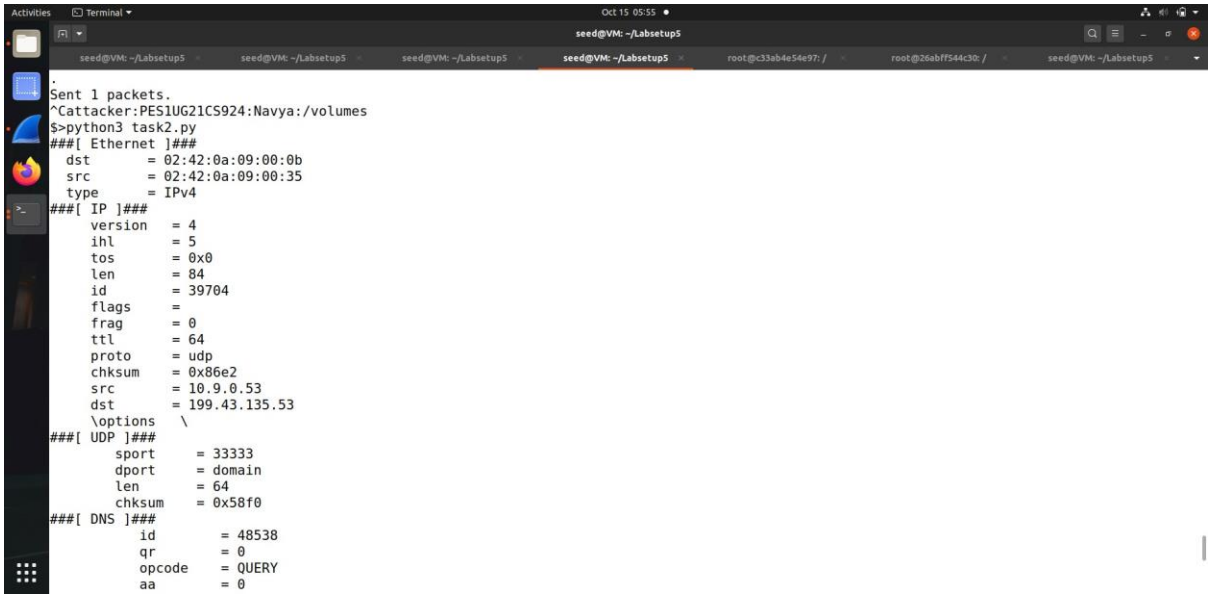


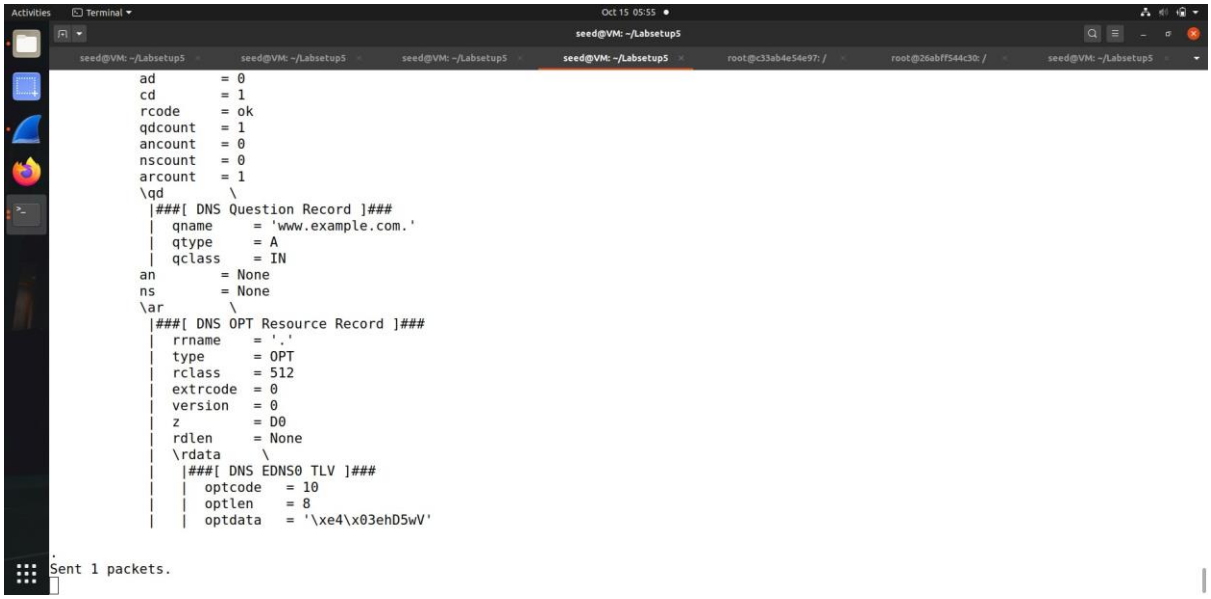


We can observe that the spoofed packet has reached the user much before the actual response.

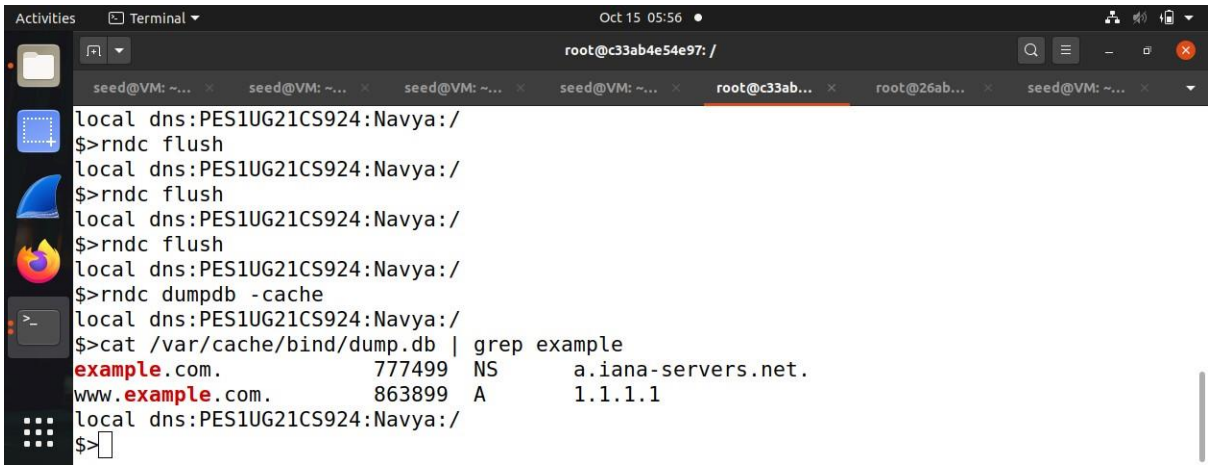


We find out the response to the DNS query has been spoofed by the attacker to be 1.1.1.1



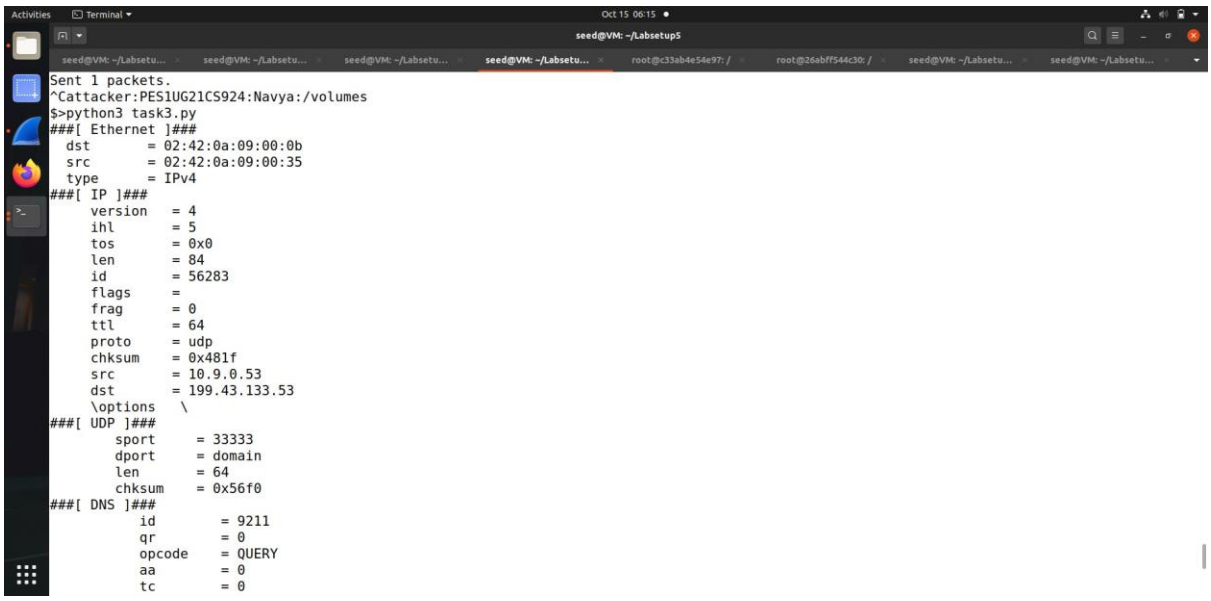


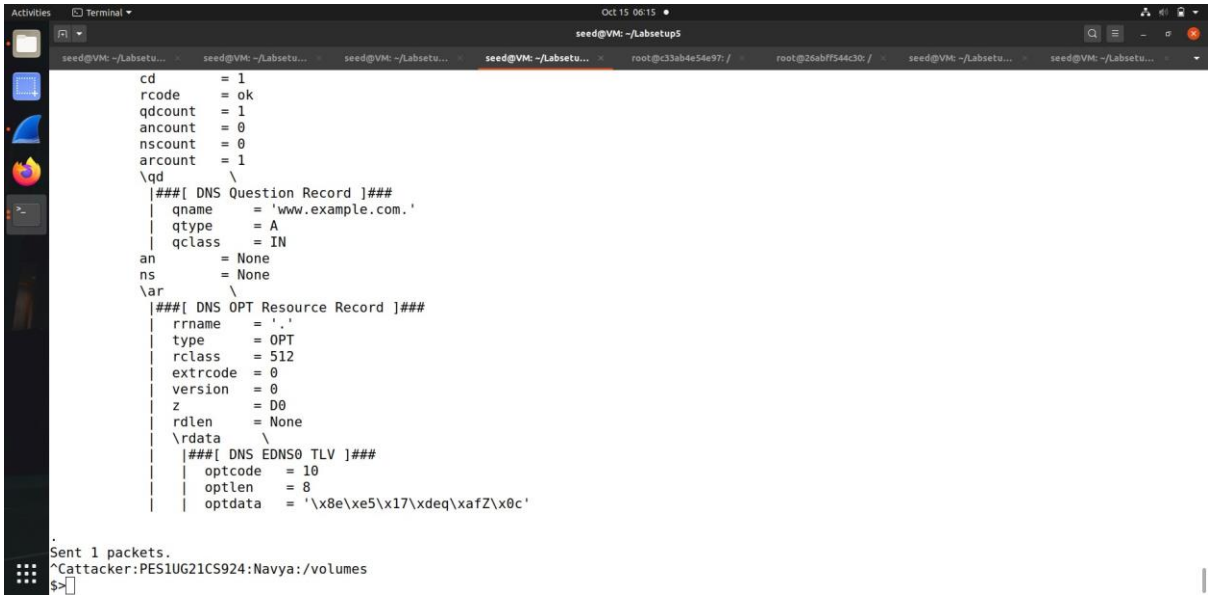
This shows the spoofed packet sent by the attacker. One packet is sent here.



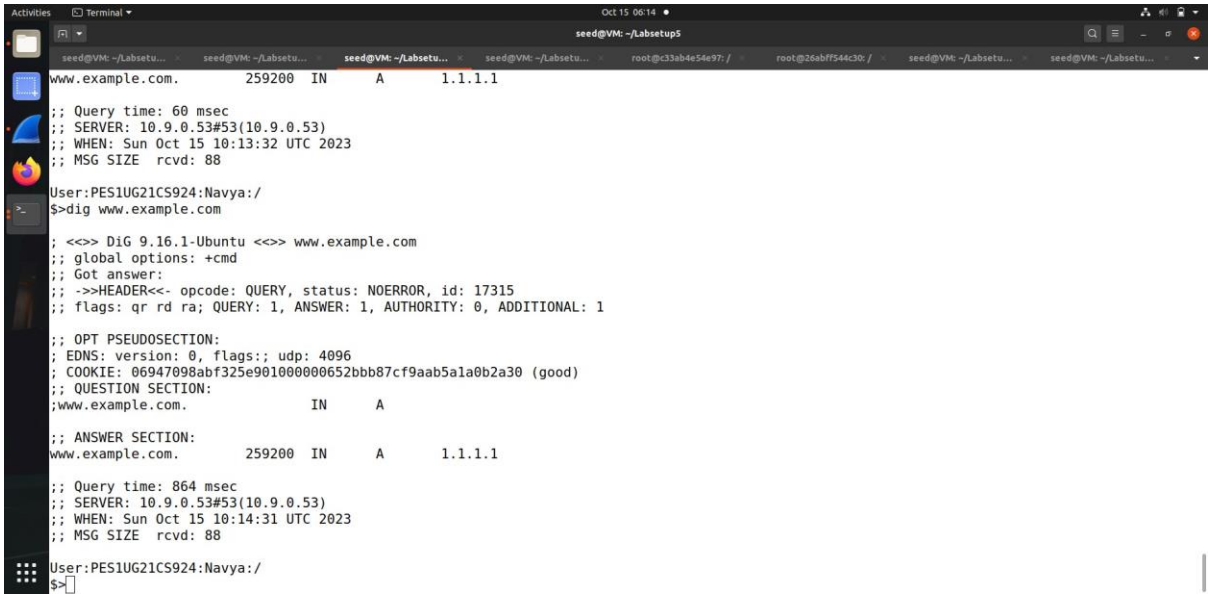
We observe that the cache of the local DNS server is updated to the ip address of the spoofed reply, from which we can infer that the attack was successful.

Task 3

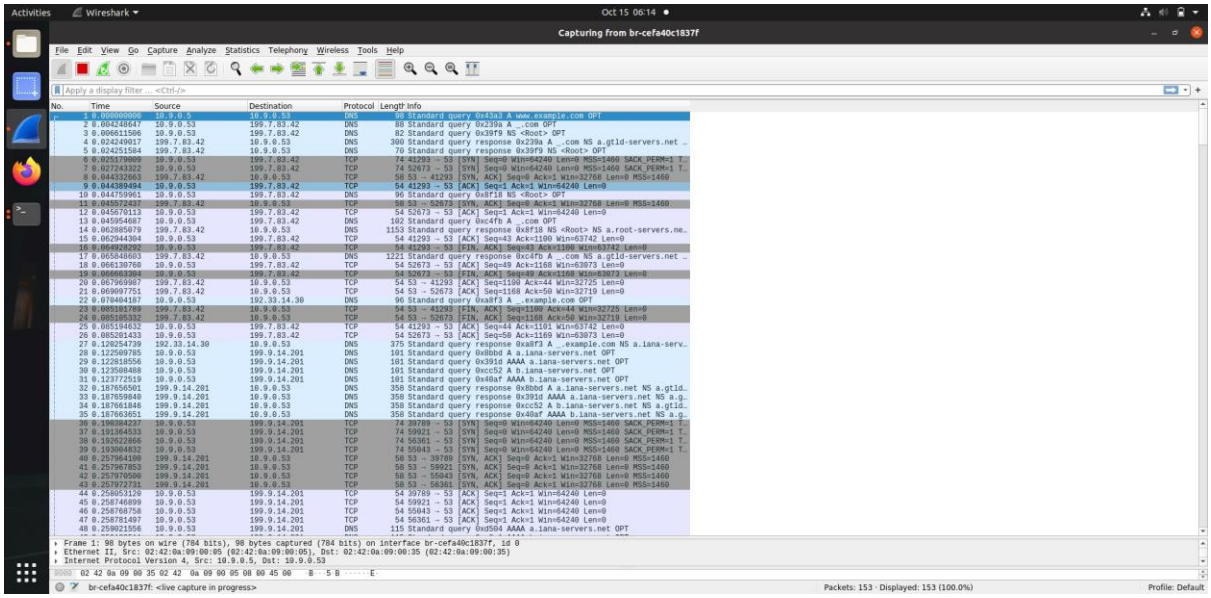


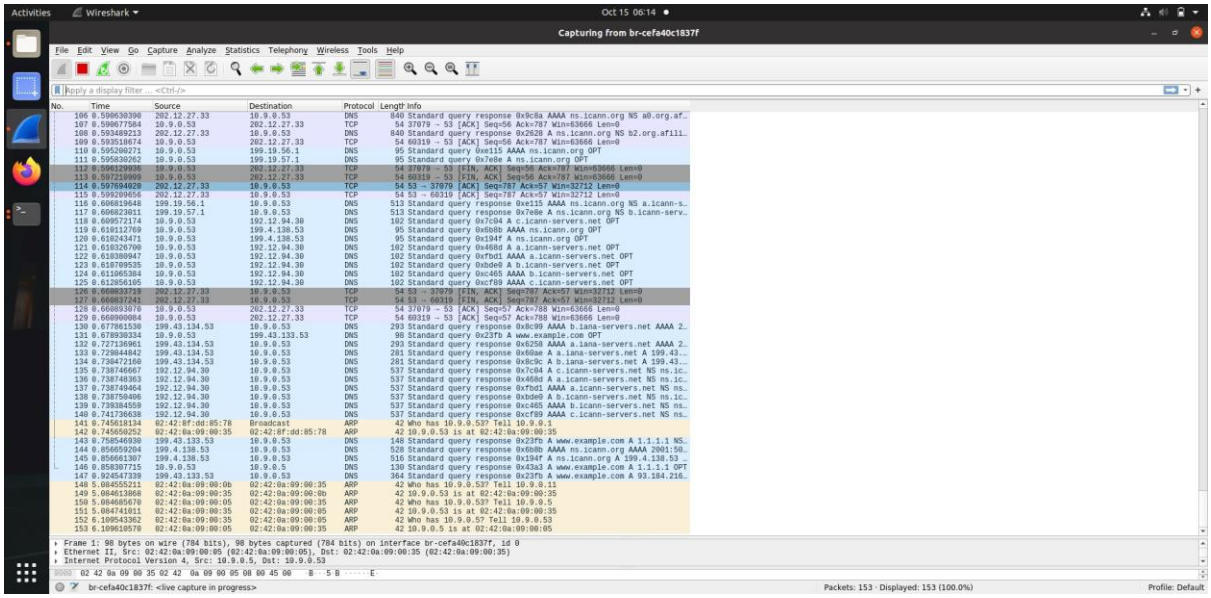


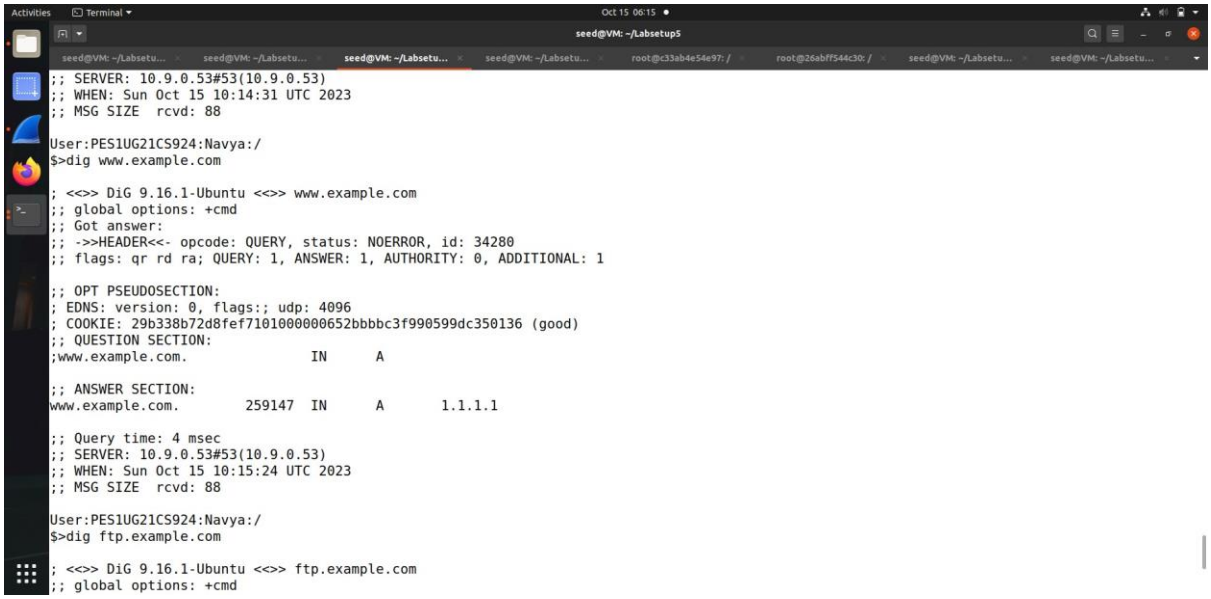
We observe that the spoofed reply is sent by the attacker.

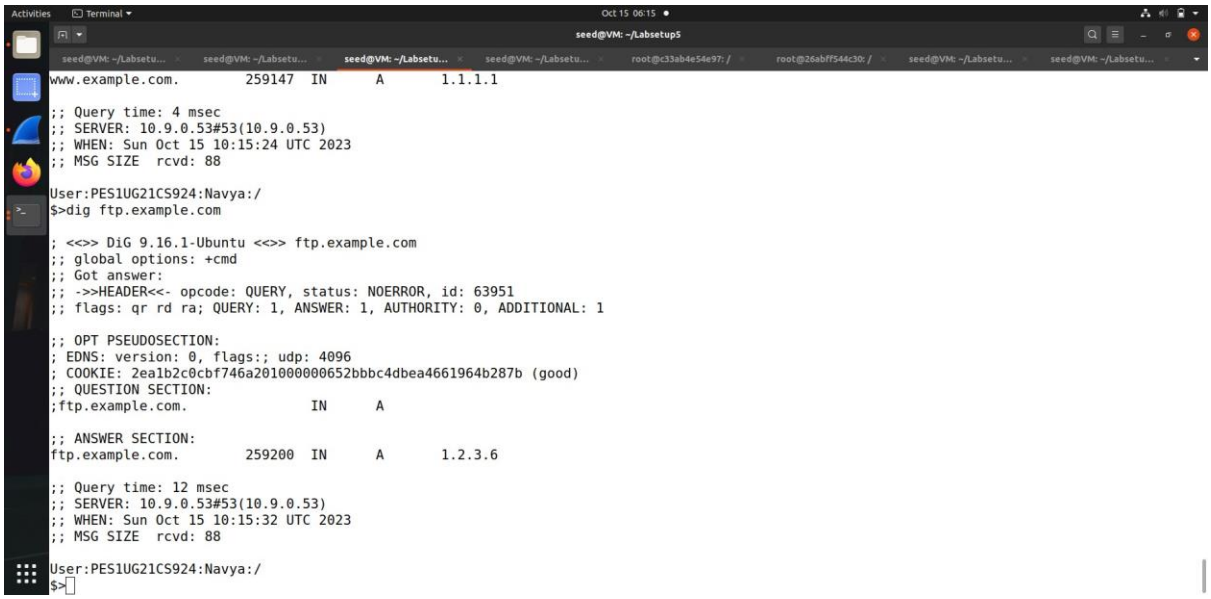


We observe that the response is spoofed by the attacker to be 1.1.1.1. This response is then sent to the DNS query.

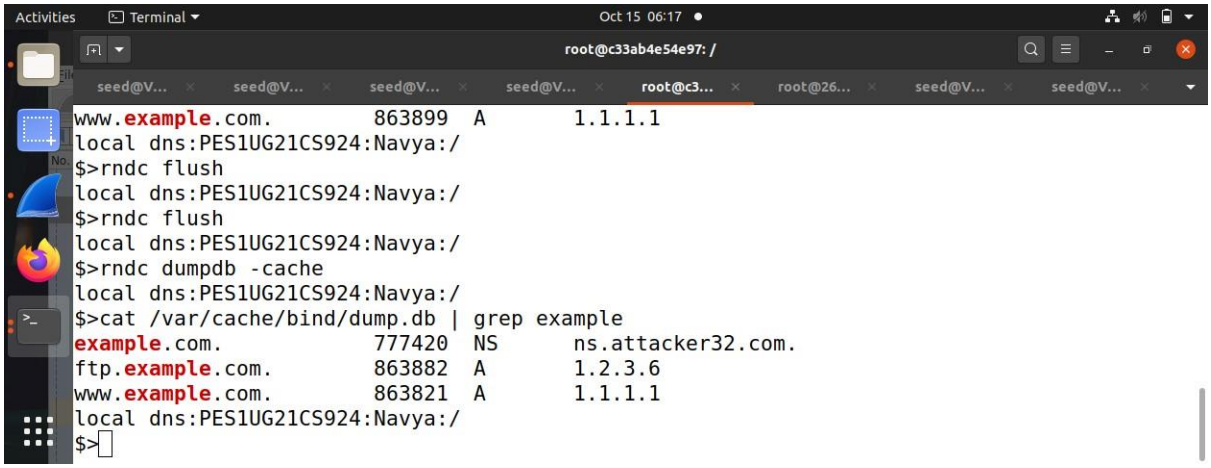



Activities
Wireshark
Oct 15 06:14
Capturing from br-cefa40c1837f
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
br-cefa40c1837f: <live capture in progress>
Packets: 153 · Displayed: 153 (100.0%)
Profile: Default


Activities
Terminal
Oct 15 06:15
seed@VM: ~/Labsetup5
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:14:31 UTC 2023
;; MSG SIZE rcvd: 88
User:PES1UG21CS924:Navya:/
$>dig www.example.com
; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34280
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 29b338b72d8fef7101000000652bbbbc3f990599dc350136 (good)
;; QUESTION SECTION:
;www.example.com. IN A
;; ANSWER SECTION:
www.example.com. 259147 IN A 1.1.1.1
;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:15:24 UTC 2023
;; MSG SIZE rcvd: 88
User:PES1UG21CS924:Navya:/
$>dig ftp.example.com
; <<>> DiG 9.16.1-Ubuntu <<>> ftp.example.com
;; global options: +cmd

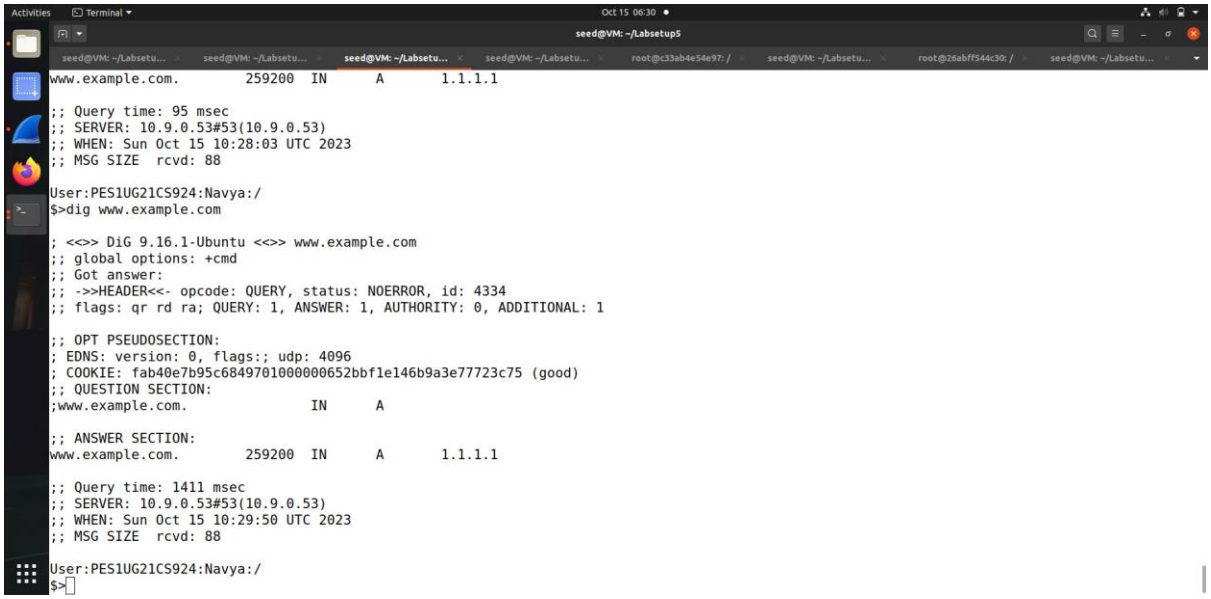

Activities
Terminal
Oct 15 06:15
seed@VM: ~/Labsetup5
www.example.com. 259147 IN A 1.1.1.1
;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:15:24 UTC 2023
;; MSG SIZE rcvd: 88
User:PES1UG21CS924:Navya:/
$>dig ftp.example.com
; <<>> DiG 9.16.1-Ubuntu <<>> ftp.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63951
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2ea1b2c0cbf746a201000000652bbbc4dbea4661964b287b (good)
;; QUESTION SECTION:
;ftp.example.com. IN A
;; ANSWER SECTION:
ftp.example.com. 259200 IN A 1.2.3.6
;; Query time: 12 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun Oct 15 10:15:32 UTC 2023
;; MSG SIZE rcvd: 88
User:PES1UG21CS924:Navya:/
$>

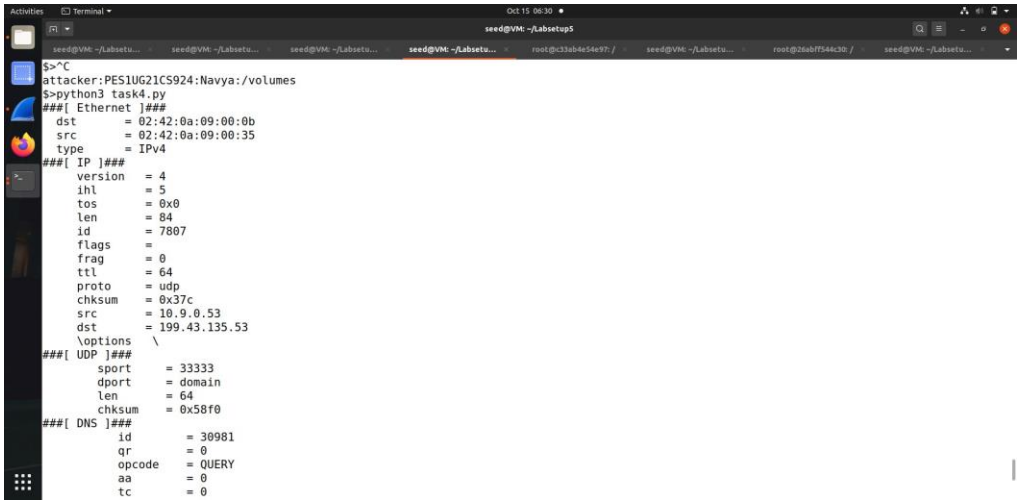
We observe that various fake ip addresses are given to the example domains, from which we can infer that the ns record has been spoofed.

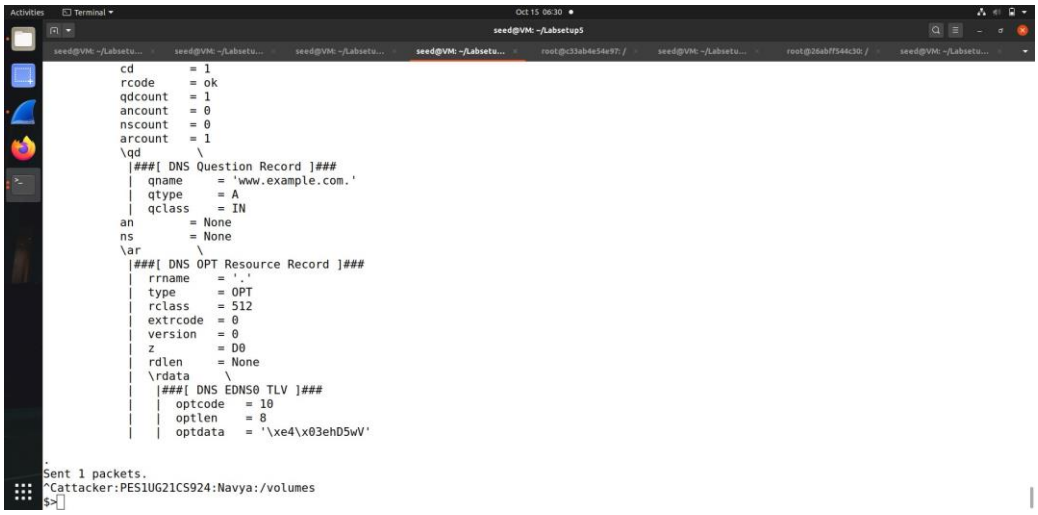


We can observe the updated fake ip addresses of example.com in the cache of the local dns server. Proving that it has been spoofed.

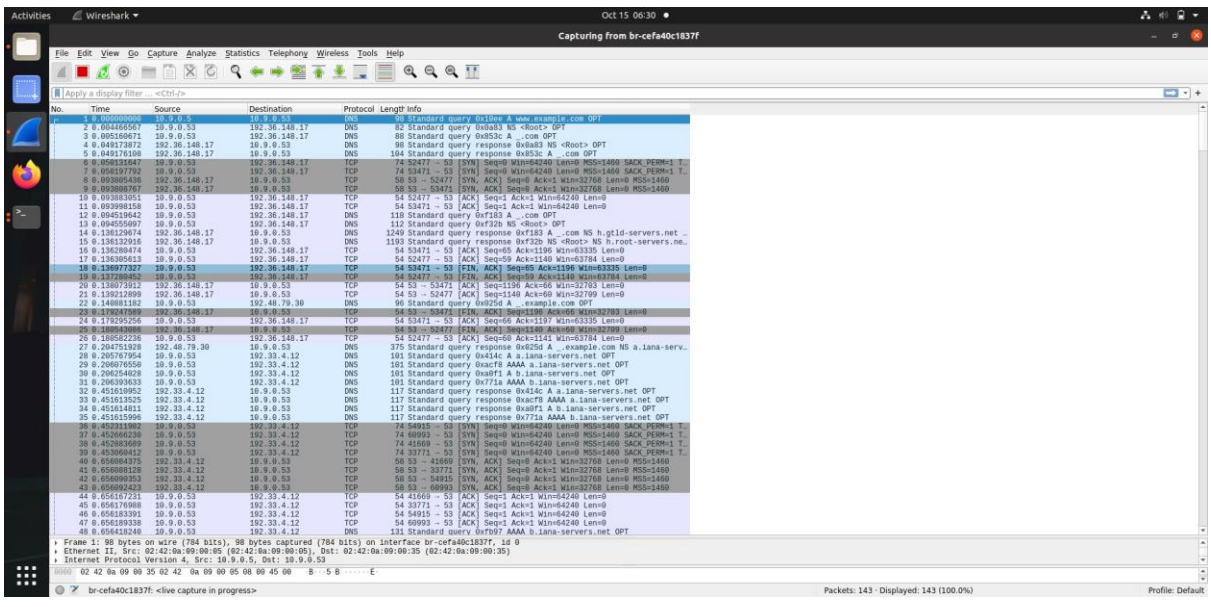
Task 4

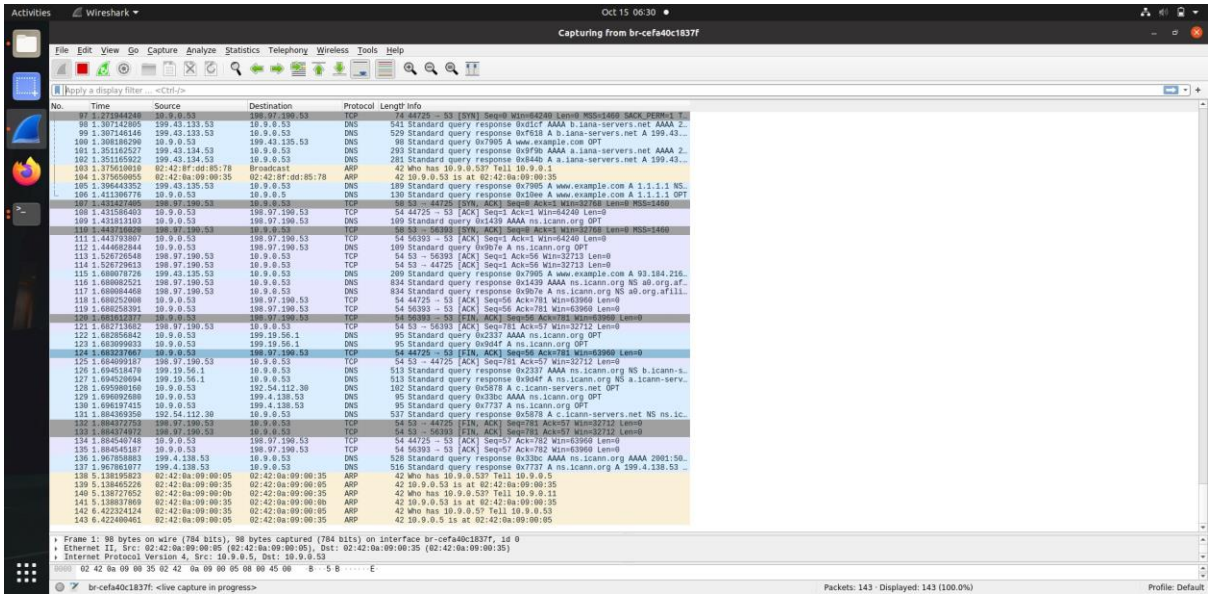






We observe that the spoofed packet is sent by the attacker.

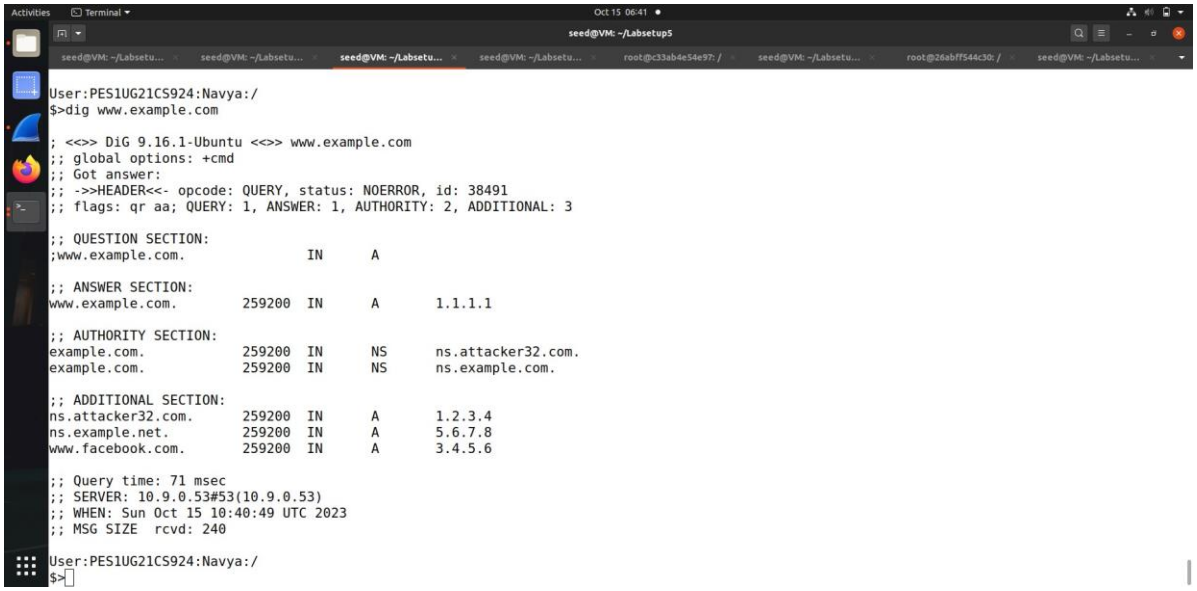




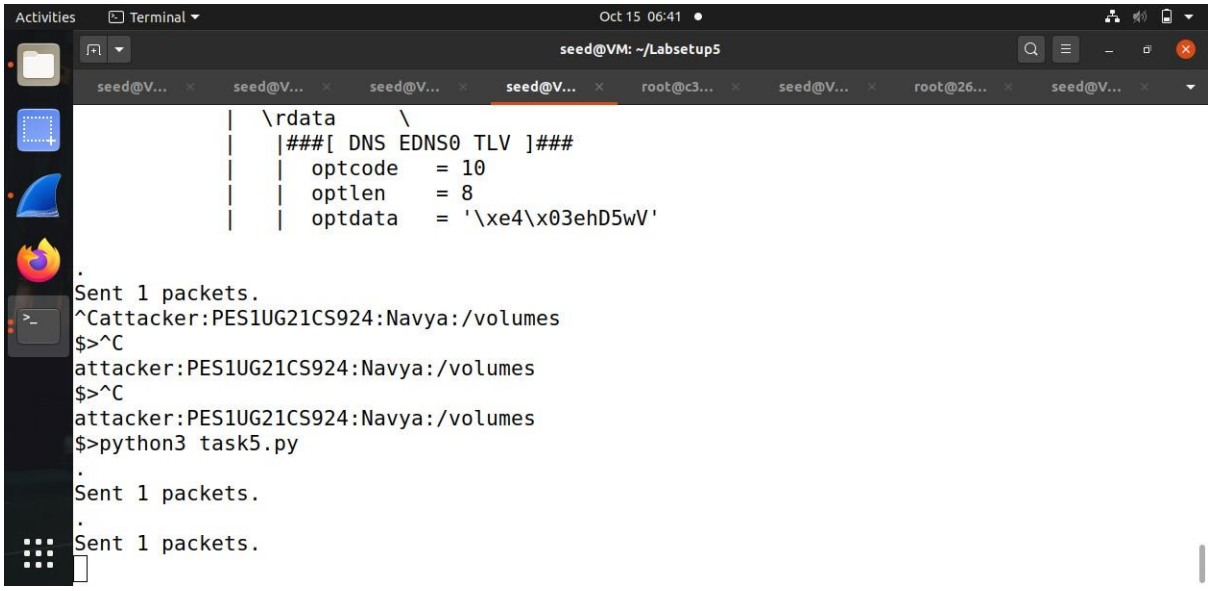
The packets which modify the authority section are captured and can be viewed in the above wireshark screenshot.

We observe that the spoofed ip for example.com gets stored in the cache. However, the spoofed ip for google.com isn't stored which may occur due to dnssec validation. This usually occurs when dnssec is enabled for a website but the spoofed response doesn't have the correct dnssec signature leading the packet to be rejected by the server.

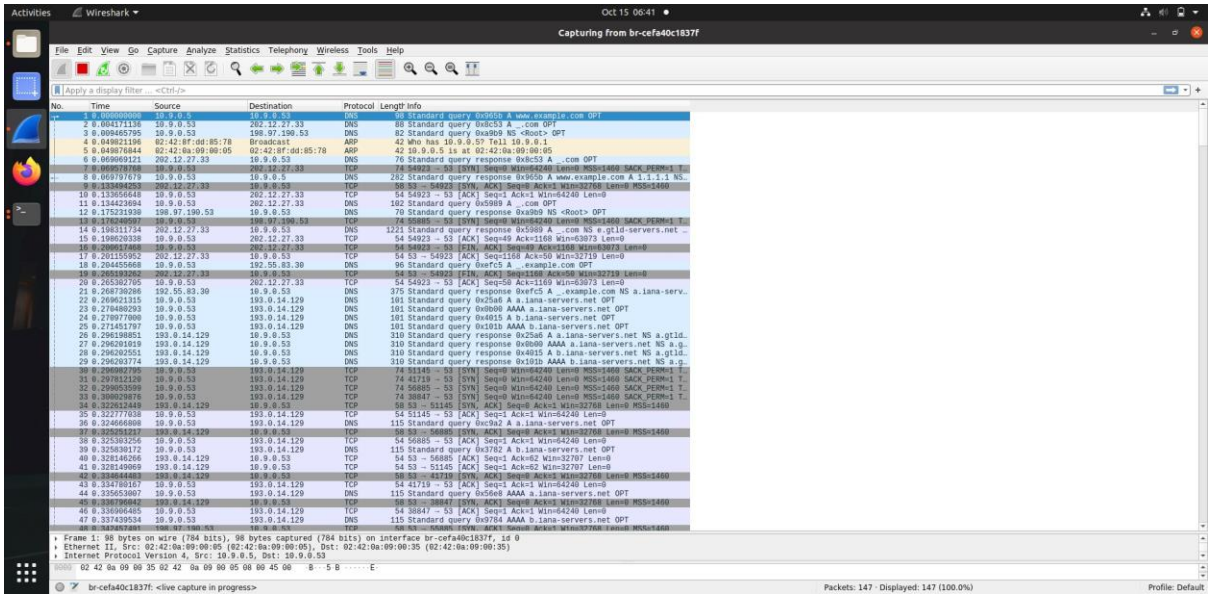
Task 5

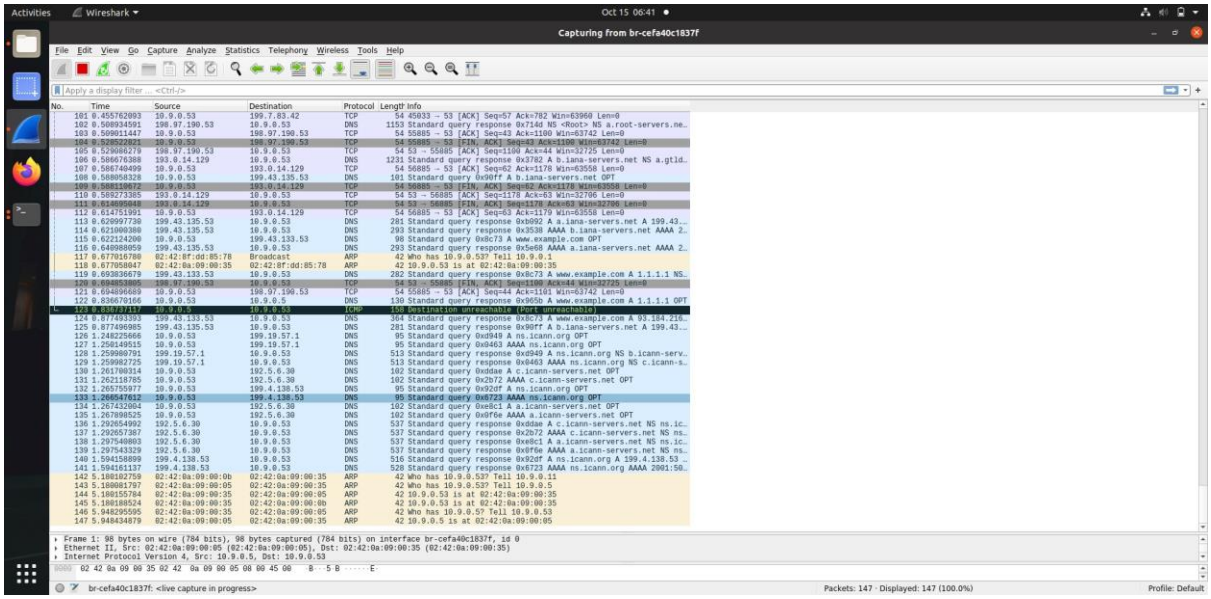


We observe that the spoofed packet is received in the additional section of the DNS reply along with the spoofed records.

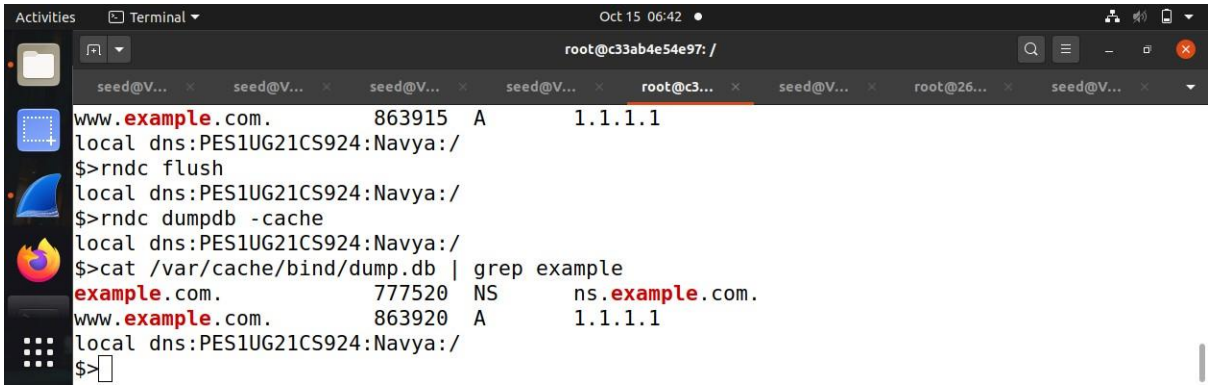


We observe that two packets have been sent by the attacker since there are two ns fields in the written code.





From these screenshots we can observe both the first and second spoofed packet.



We observe that the DNS records of the additional section are not cached. This occurs as they are not given a high priority compared to that of the authoritative section. This might be due to increasing the security and making only specific sections high priority.