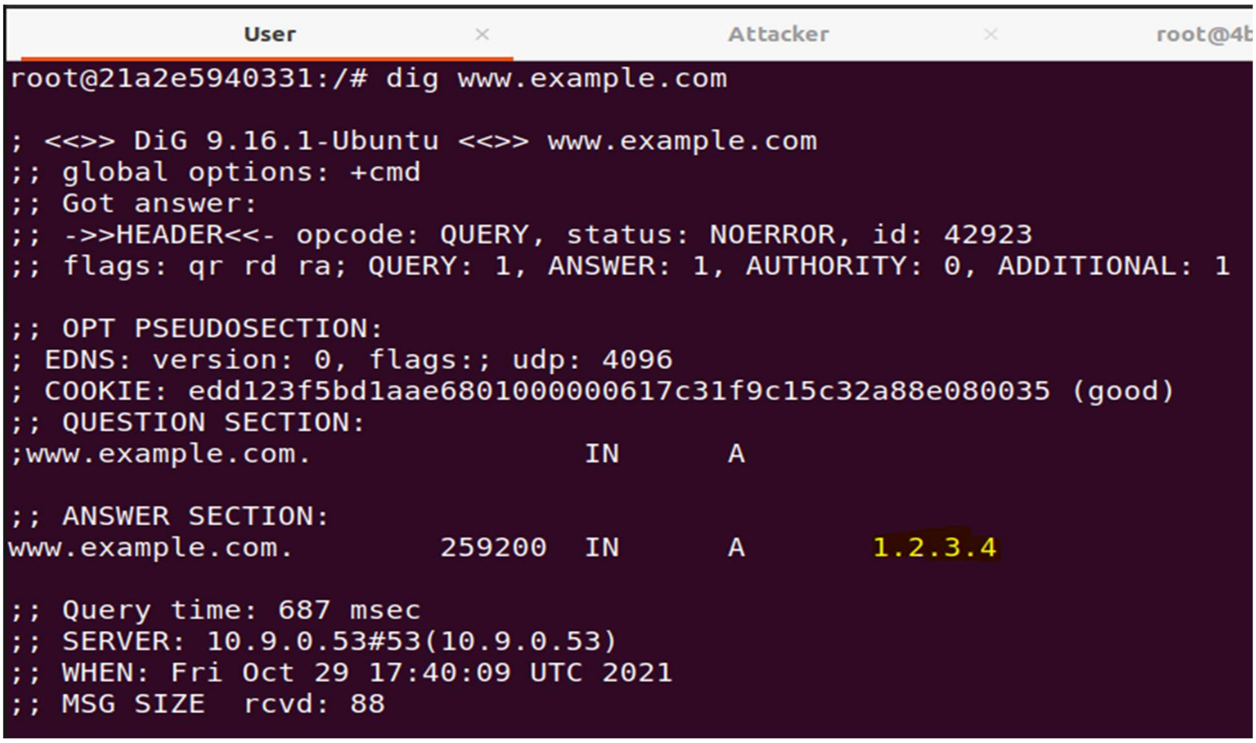
Advanced Computer Networking & Security
Lab Report: 8 - Local DNS Attack Lab

700727822

Task 1: Directly Spoofing Response to User

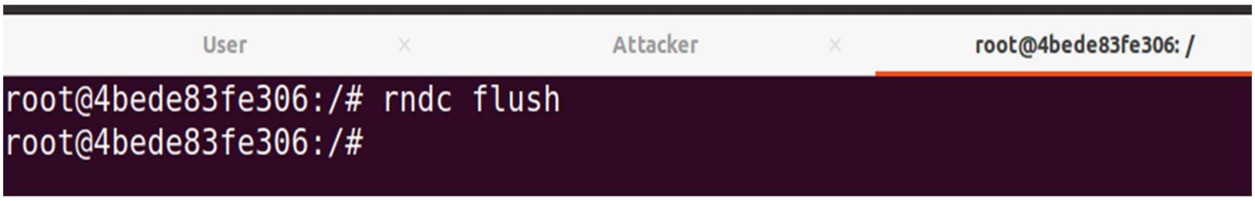
When a user types the name of a web site (a host name, such as www.example.com) in a web browser, the user’s computer will send a DNS request to the local DNS server to resolve the IP address of the host name



```
root@21a2e5940331:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42923
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: edd123f5bd1aae6801000000617c31f9c15c32a88e080035 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.4

;; Query time: 687 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Oct 29 17:40:09 UTC 2021
;; MSG SIZE  rcvd: 88
```

Task 2: DNS Cache Poisoning Attack – Spoofing Answers

Command to clear DNS Server’s cache



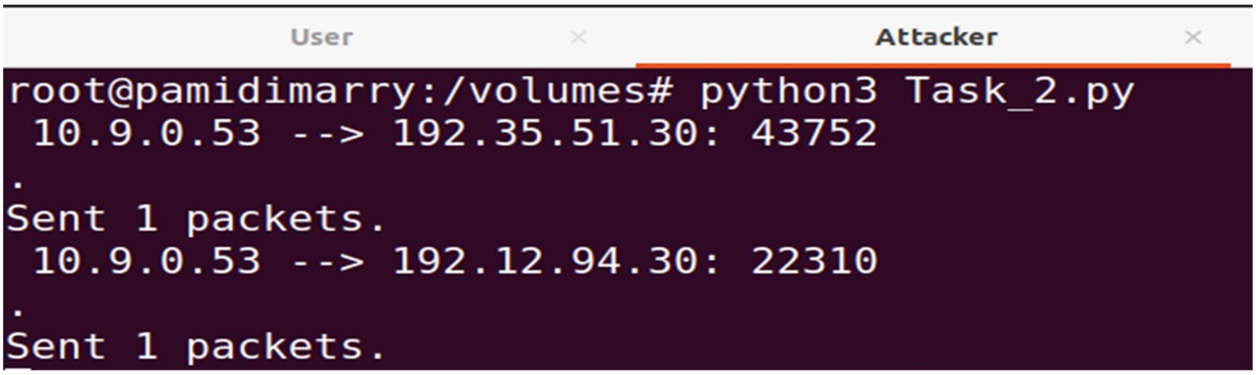
```
root@4bede83fe306:/# rndc flush
root@4bede83fe306:/#
```

Inspecting the cache on the local DNS server to see whether it is poisoned or not.

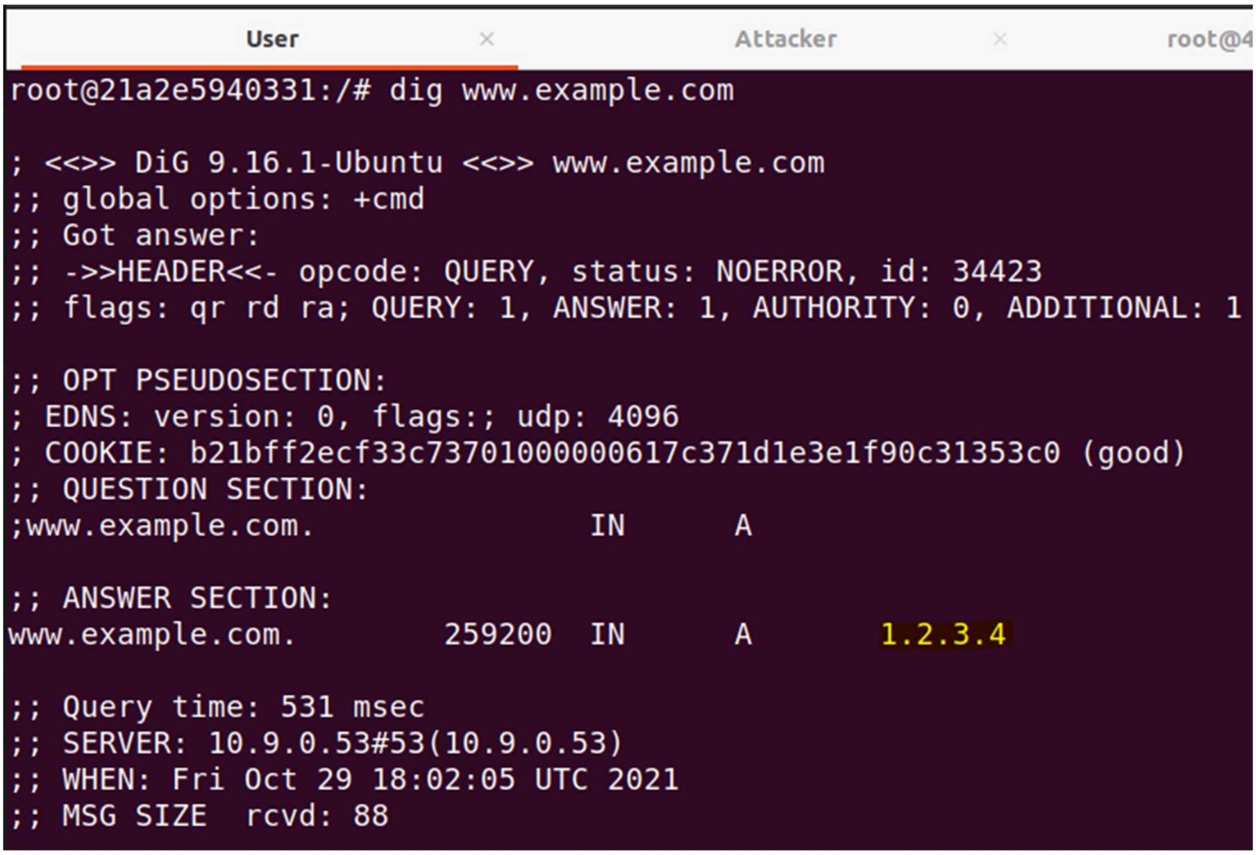
#rndc dumpdb -cache

# cat /var/cache/bind/dump.db

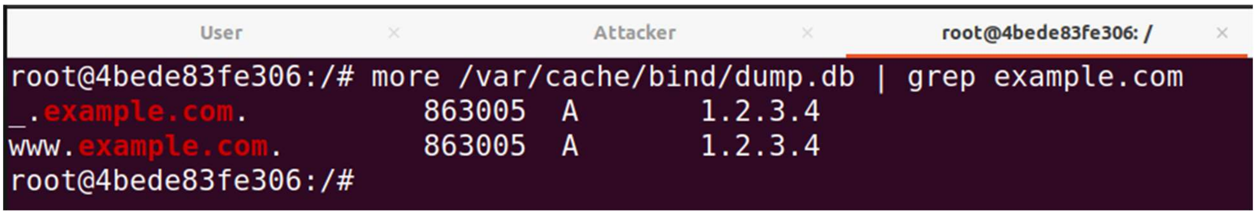
DNS cache poisoning attack:



```
root@pamidimarry:/volumes# python3 Task_2.py
 10.9.0.53 --> 192.35.51.30: 43752
.
Sent 1 packets.
 10.9.0.53 --> 192.12.94.30: 22310
.
Sent 1 packets.
```



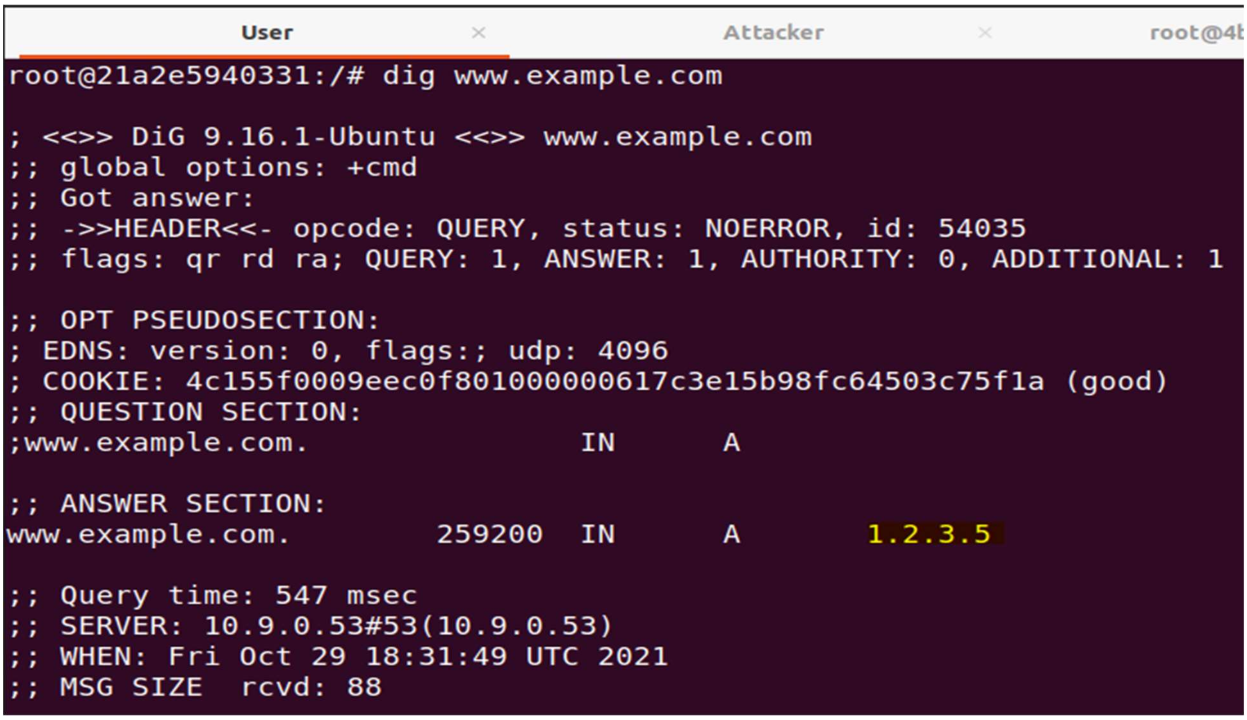
```
root@21a2e5940331:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34423
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: b21bff2ecf33c73701000000617c371d1e3e1f90c31353c0 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.4

;; Query time: 531 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Oct 29 18:02:05 UTC 2021
;; MSG SIZE  rcvd: 88
```



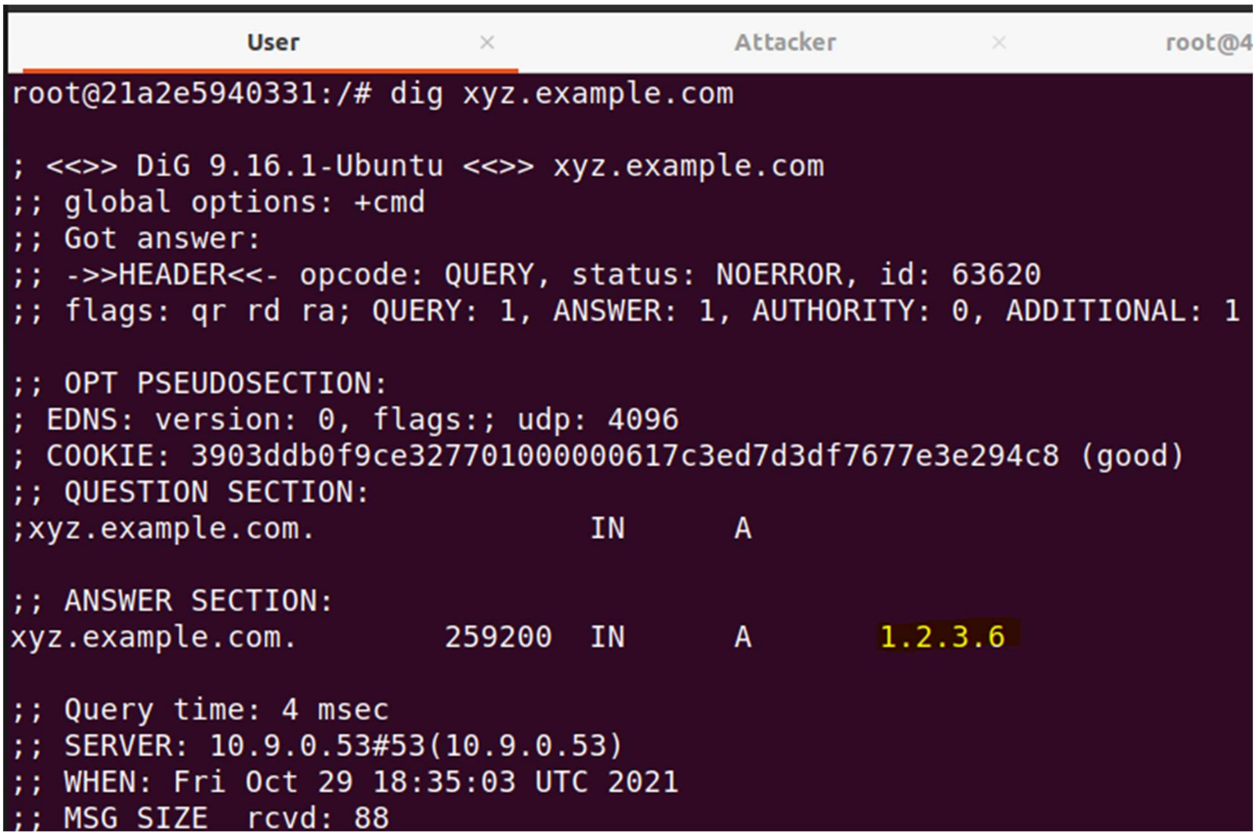
```
root@4bede83fe306:/# more /var/cache/bind/dump.db | grep example.com
_.example.com.          863005  A       1.2.3.4
www.example.com.        863005  A       1.2.3.4
root@4bede83fe306:/#
```

Task 3: Spoofing NS Records

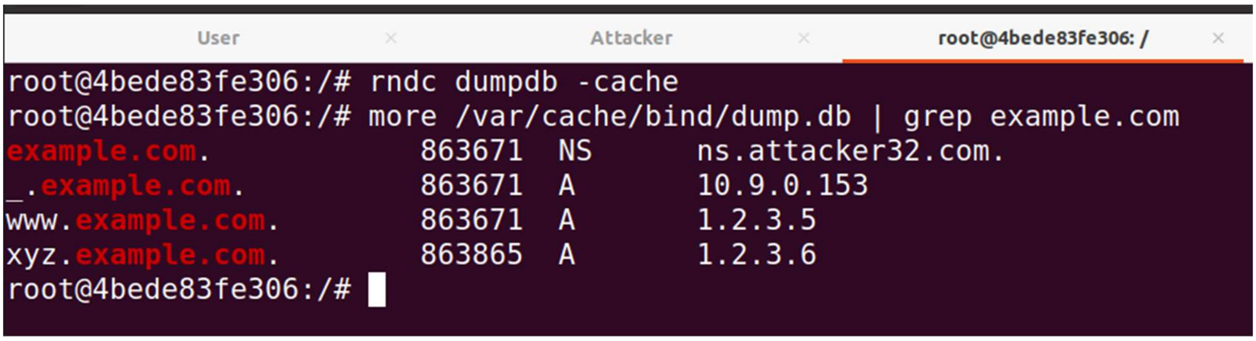
DNS Attack using Authority section in DNS replies



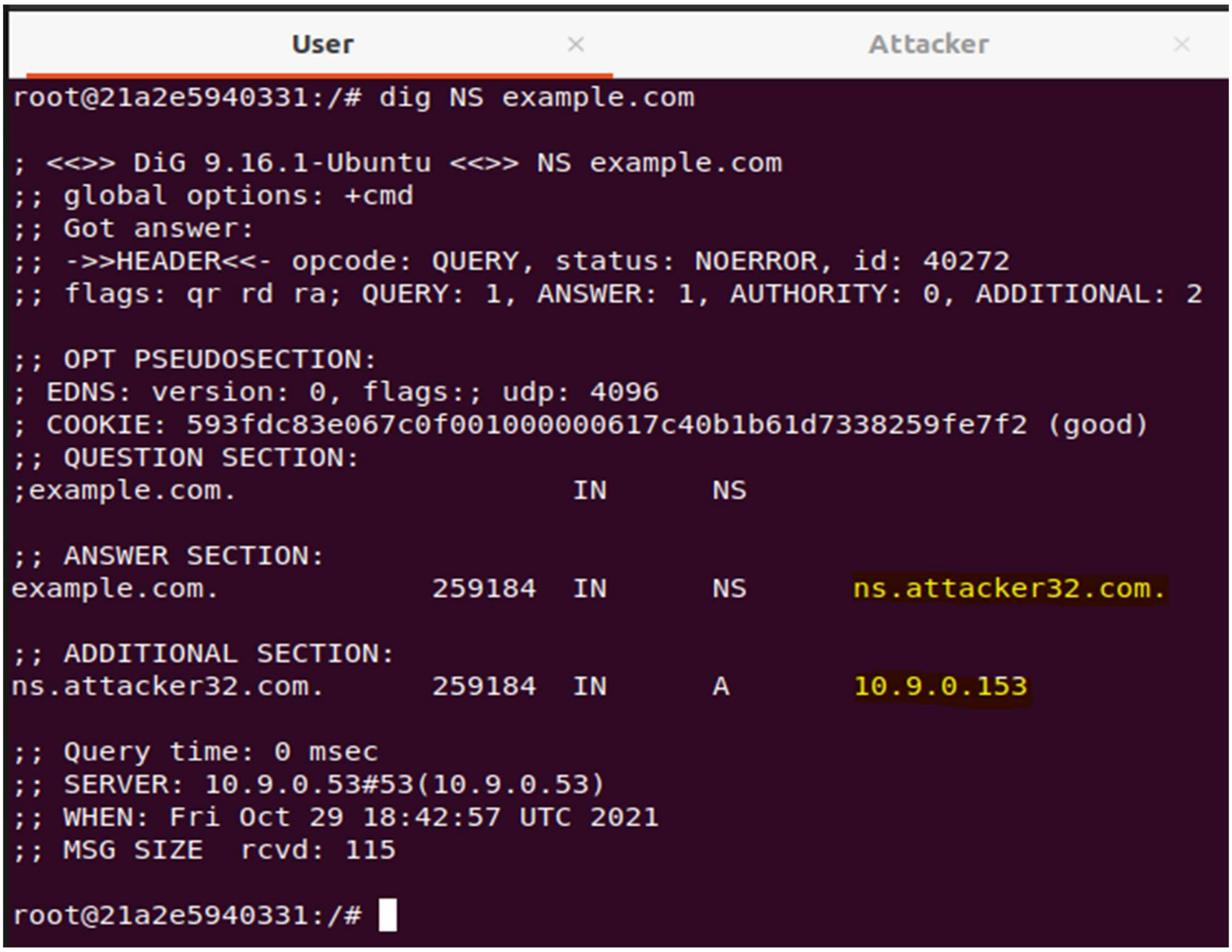
```
root@21a2e5940331:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54035
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4c155f0009eec0f801000000617c3e15b98fc64503c75f1a (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

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

;; Query time: 547 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Oct 29 18:31:49 UTC 2021
;; MSG SIZE  rcvd: 88
```



```
root@21a2e5940331:/# dig xyz.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> xyz.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63620
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3903ddb0f9ce327701000000617c3ed7d3df7677e3e294c8 (good)
;; QUESTION SECTION:
;xyz.example.com.               IN      A

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

;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Oct 29 18:35:03 UTC 2021
;; MSG SIZE  rcvd: 88
```

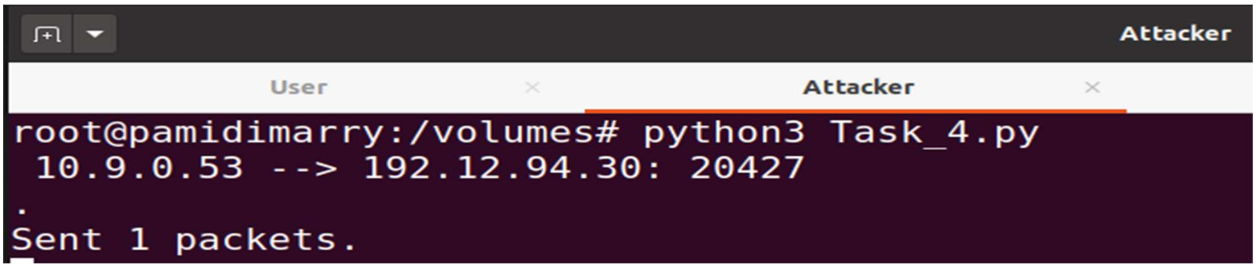


```
root@4bede83fe306:/# rndc dumpdb -cache
root@4bede83fe306:/# more /var/cache/bind/dump.db | grep example.com
example.com.            863671  NS      ns.attacker32.com.
_.example.com.          863671  A       10.9.0.153
www.example.com.        863671  A       1.2.3.5
xyz.example.com.        863865  A       1.2.3.6
root@4bede83fe306:/#
```

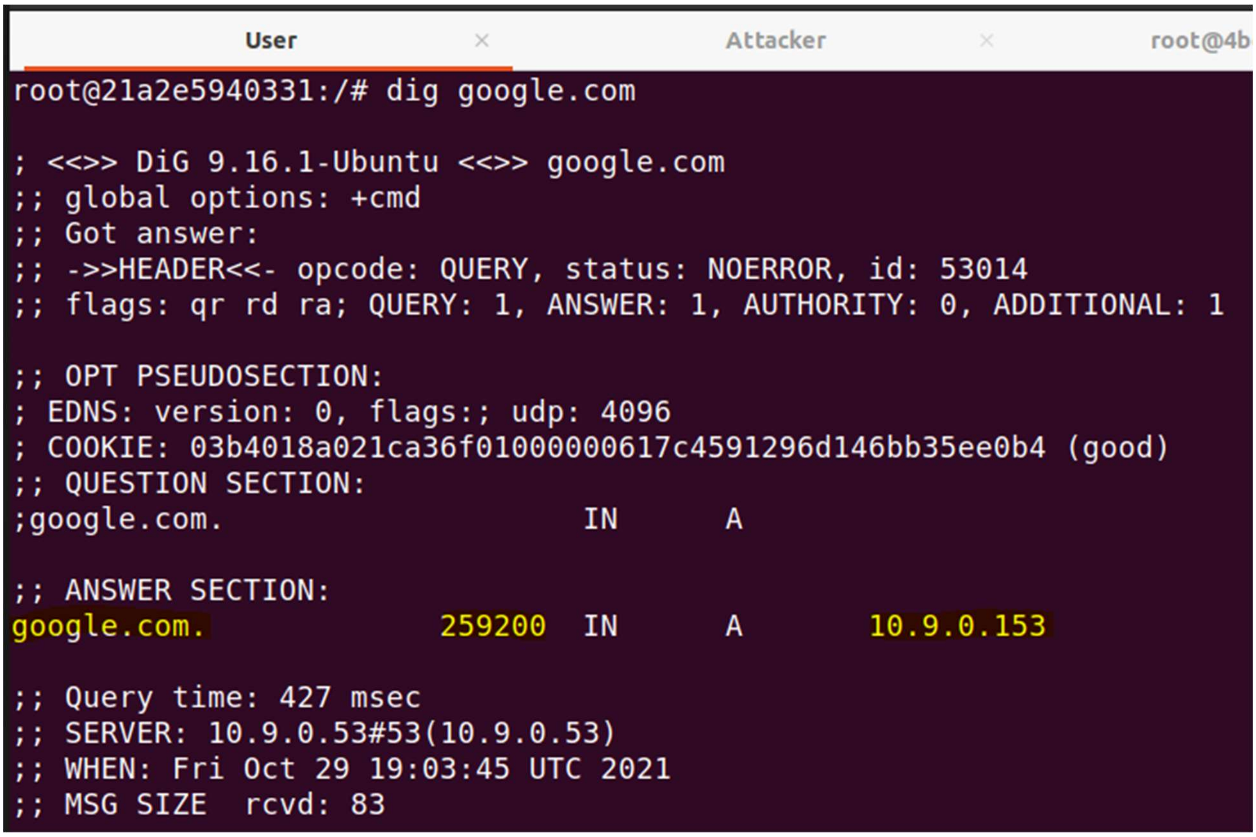


```
root@21a2e5940331:/# dig NS example.com

; <<>> DiG 9.16.1-Ubuntu <<>> NS example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40272
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 593fdc83e067c0f001000000617c40b1b61d7338259fe7f2 (good)
;; QUESTION SECTION:
;example.com.                   IN      NS

;; ANSWER SECTION:
example.com.            259184  IN      NS      ns.attacker32.com.

;; ADDITIONAL SECTION:
ns.attacker32.com.      259184  IN      A       10.9.0.153

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Oct 29 18:42:57 UTC 2021
;; MSG SIZE  rcvd: 115

root@21a2e5940331:/#
```

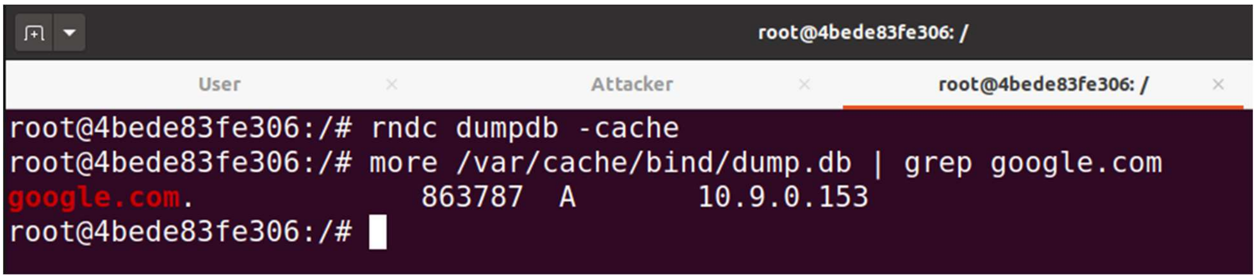
Task 4: Spoofing NS Records for Another Domain



```
root@pamidimarry:/volumes# python3 Task_4.py
 10.9.0.53 --> 192.12.94.30: 20427
.
Sent 1 packets.
```

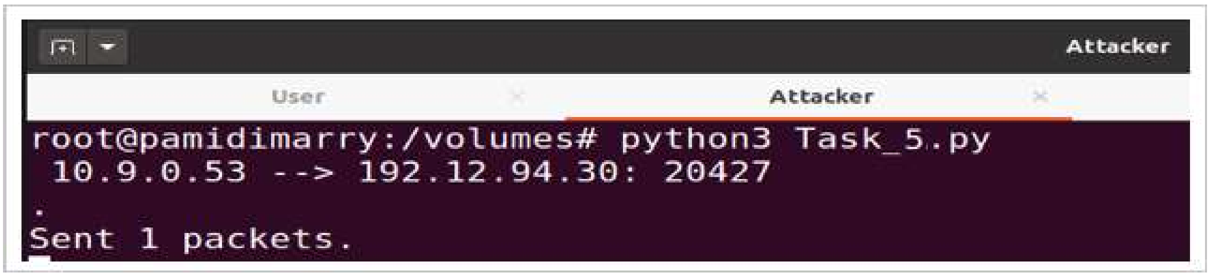


```
root@21a2e5940331:/# dig google.com

; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53014
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 03b4018a021ca36f01000000617c4591296d146bb35ee0b4 (good)
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             259200  IN      A       10.9.0.153

;; Query time: 427 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Oct 29 19:03:45 UTC 2021
;; MSG SIZE  rcvd: 83
```

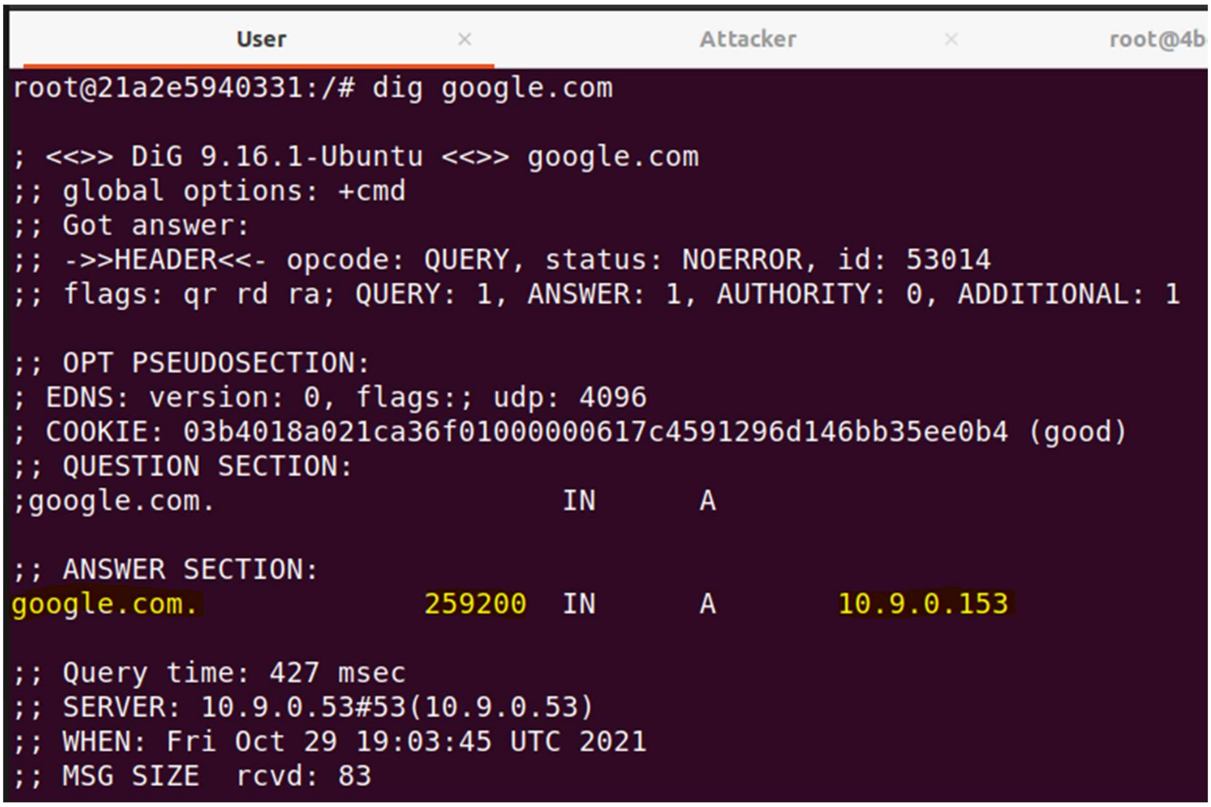


```
root@4bede83fe306:/# rndc dumpdb -cache
root@4bede83fe306:/# more /var/cache/bind/dump.db | grep google.com
google.com.             863787  A       10.9.0.153
root@4bede83fe306:/#
```

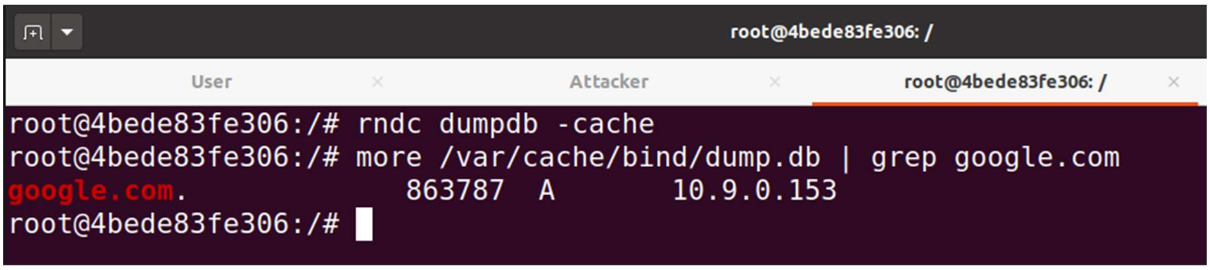
Task 5: Spoofing Records in the Additional Section



```
root@pamidimarry:/volumes# python3 Task_5.py
 10.9.0.53 --> 192.12.94.30: 20427
.
Sent 1 packets.
```



```
root@21a2e5940331:/# dig google.com

; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53014
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 03b4018a021ca36f01000000617c4591296d146bb35ee0b4 (good)
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             259200  IN      A       10.9.0.153

;; Query time: 427 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Fri Oct 29 19:03:45 UTC 2021
;; MSG SIZE  rcvd: 83
```



```
root@4bede83fe306:/# rndc dumpdb -cache
root@4bede83fe306:/# more /var/cache/bind/dump.db | grep google.com
google.com.             863787  A       10.9.0.153
root@4bede83fe306:/# 
```