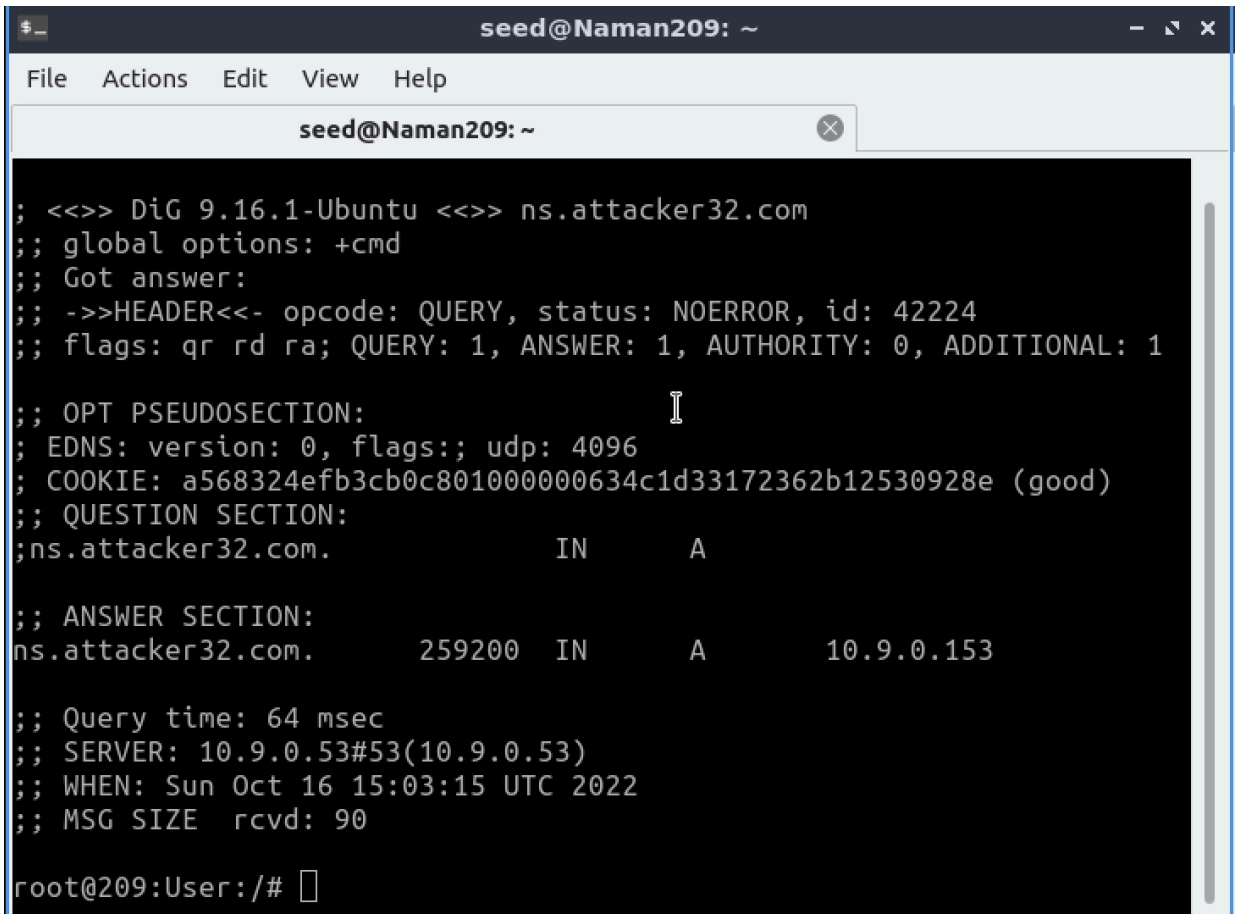
Computer Network Security

Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

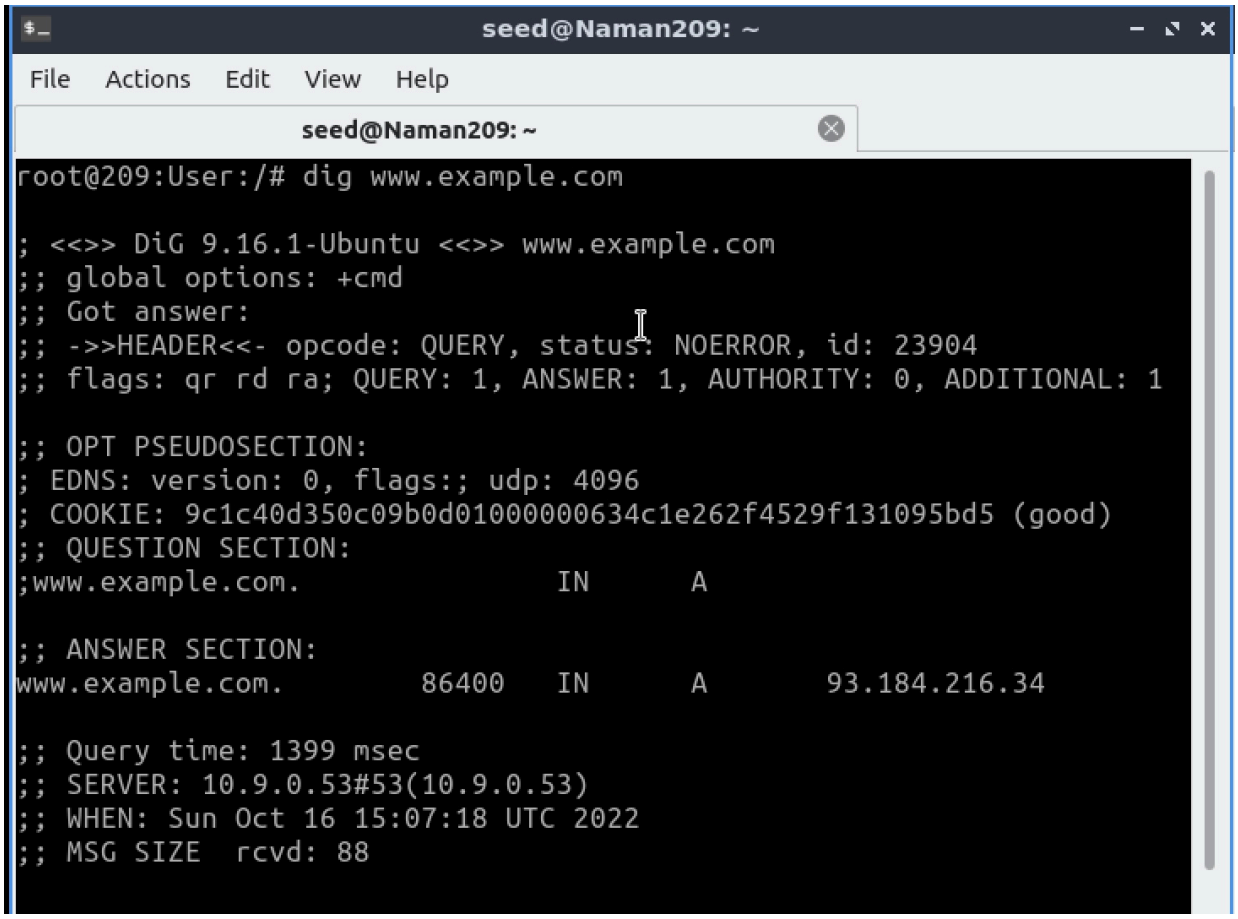
Local DNS Attack Lab

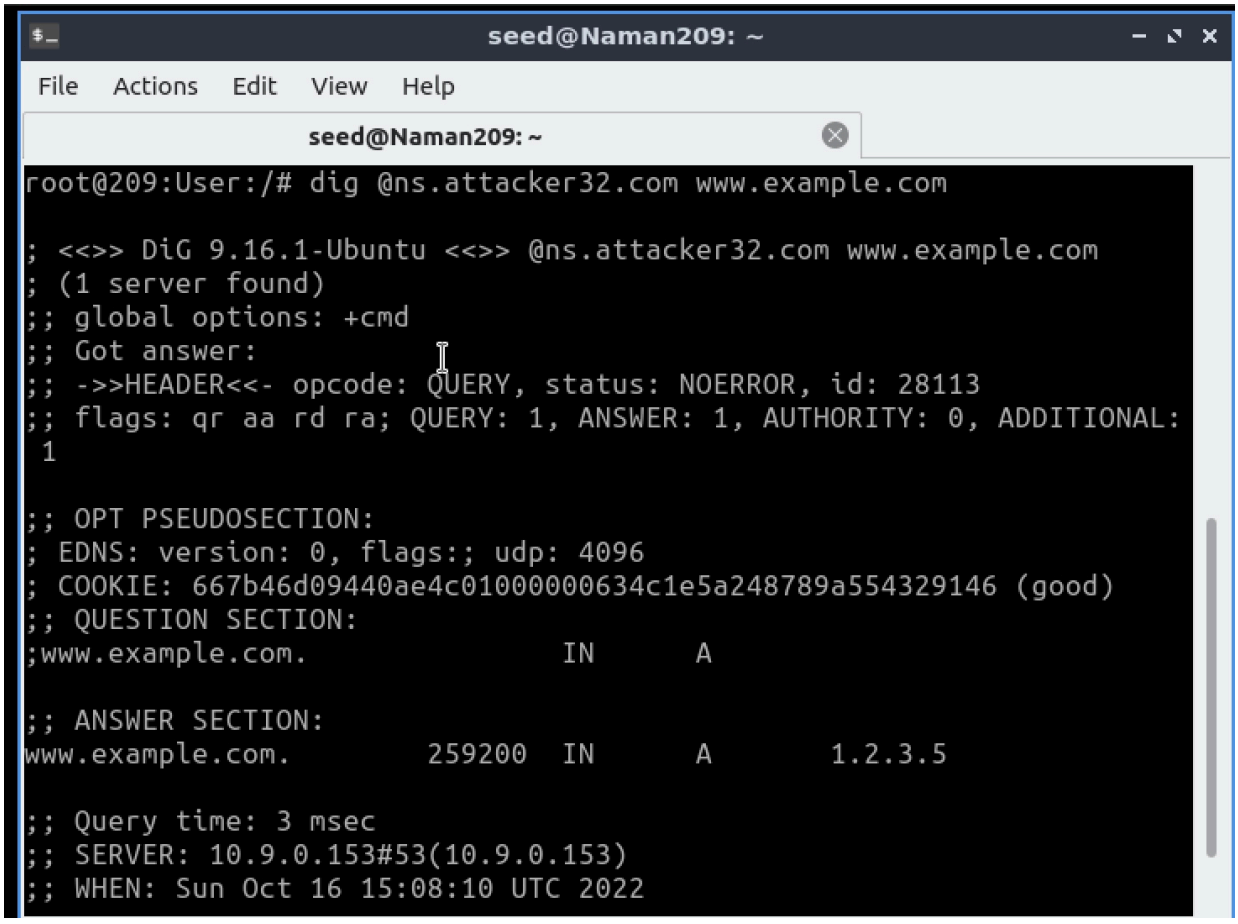
Task 0:Verification of the DNS setup

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



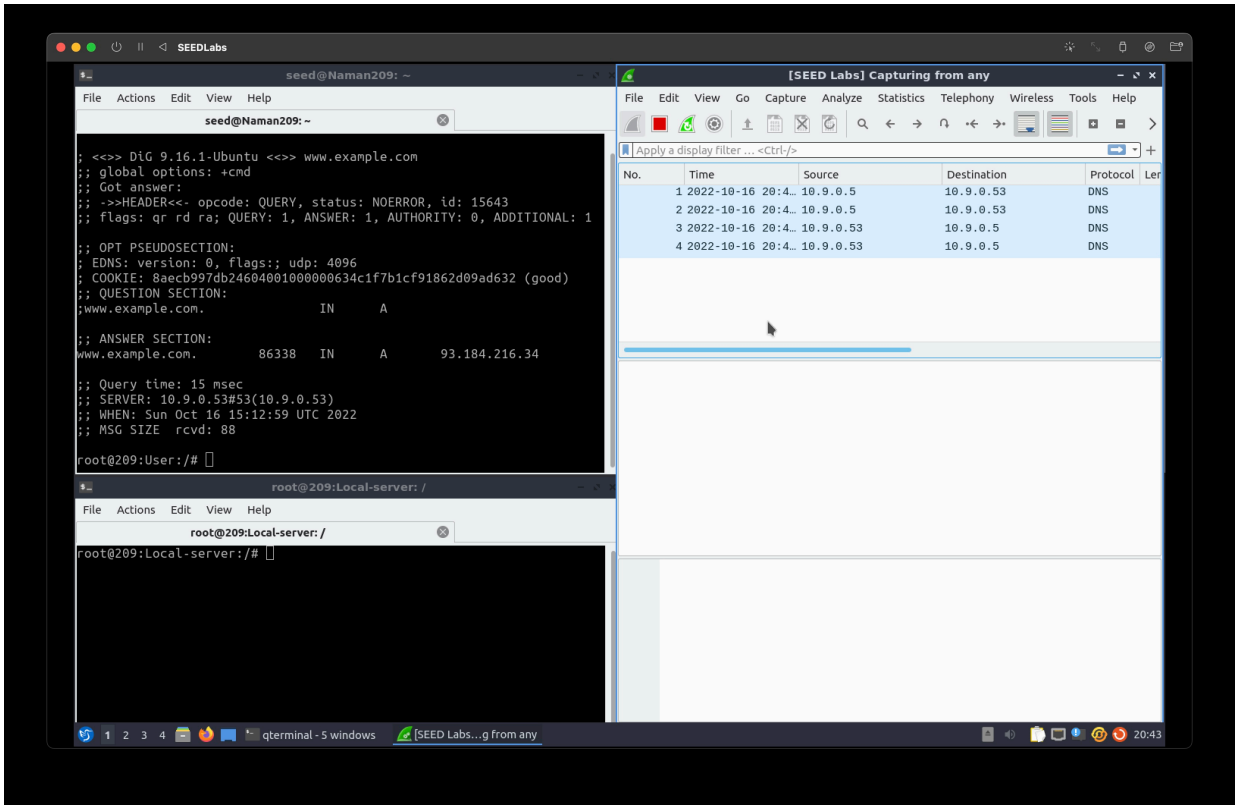

```
dig www.example.com
dig @ns.attacker32.com www.example.com
```





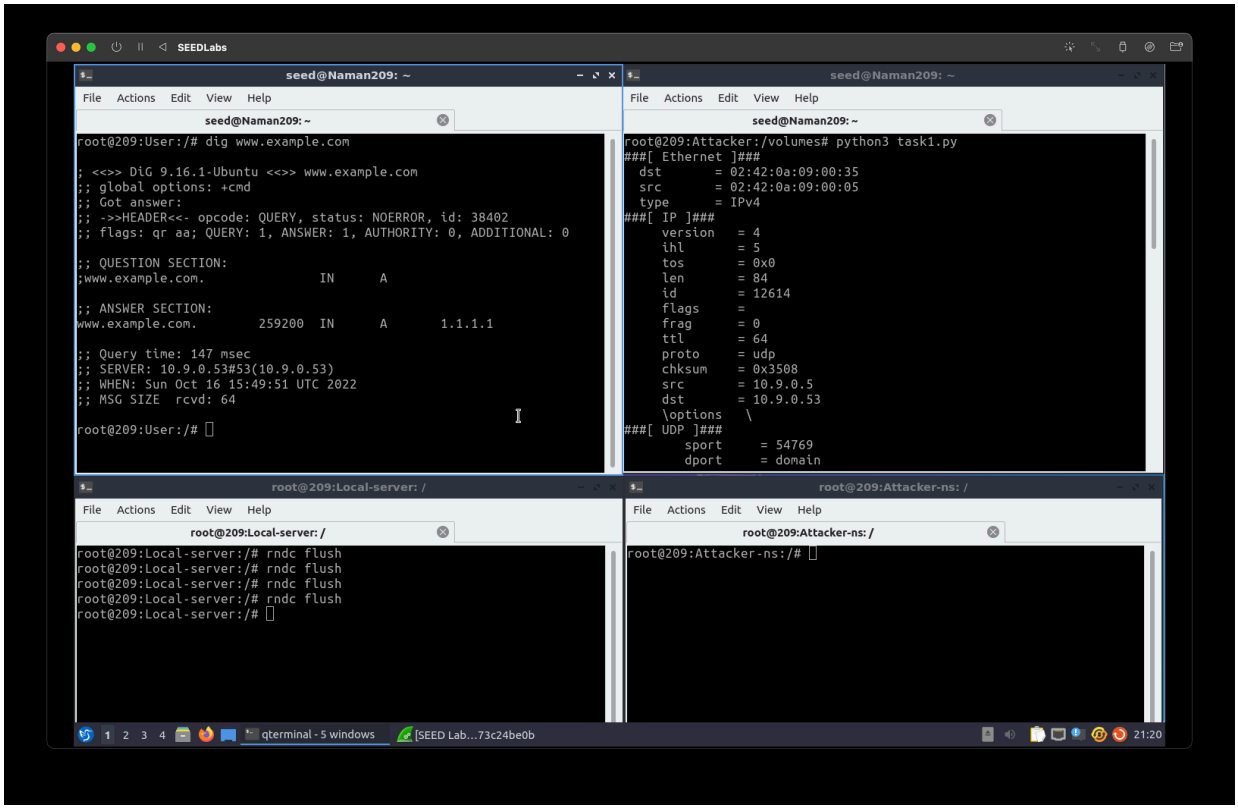
Task 1: Directly Spoffing Response to User

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

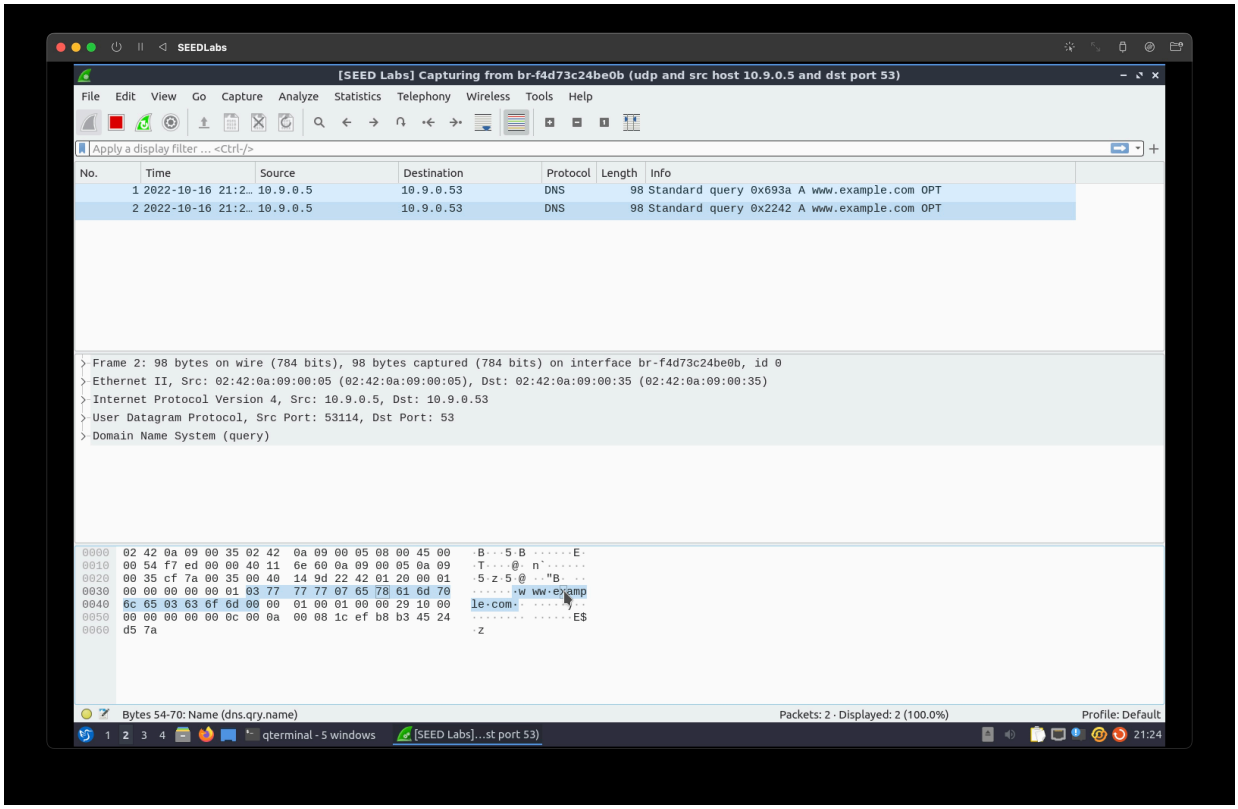



```
python3 task1.py
```

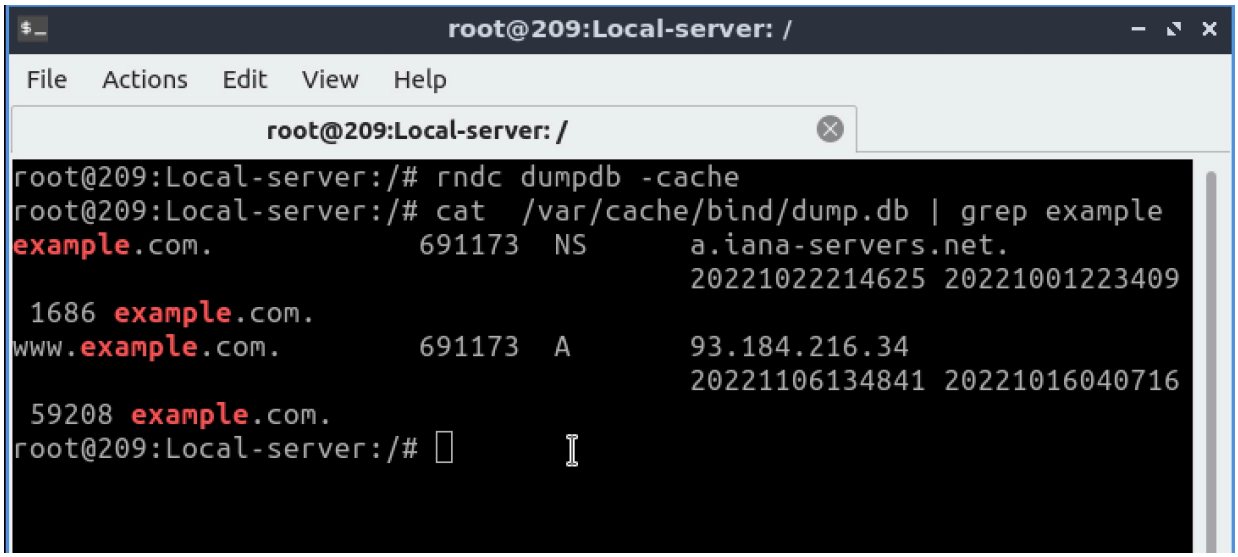
```
dig www.example.com
```



Wireshark:




```
rndc dumpdb -cache
cat /var/cache/bind/dump.db | grep example
```

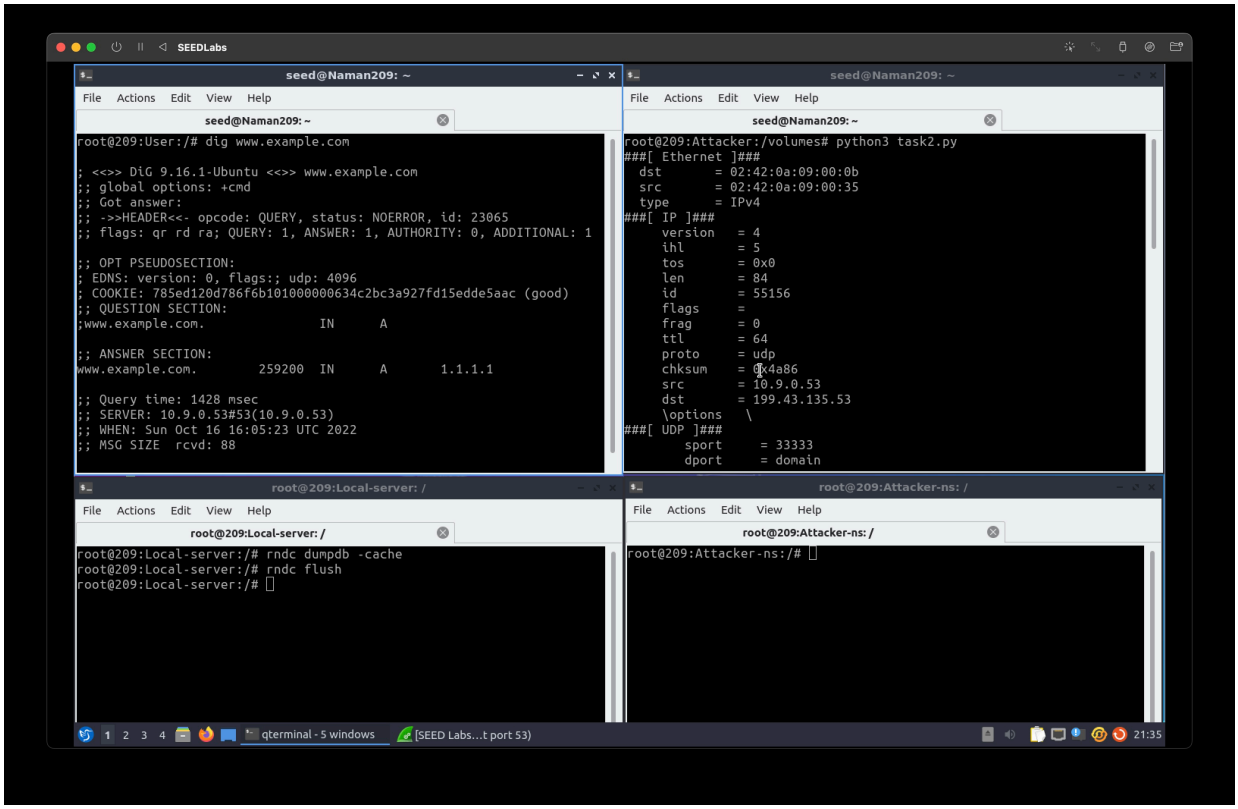


Observation: When we see the contents of the dump file, we notice that the response is being spoofed to a random ip address

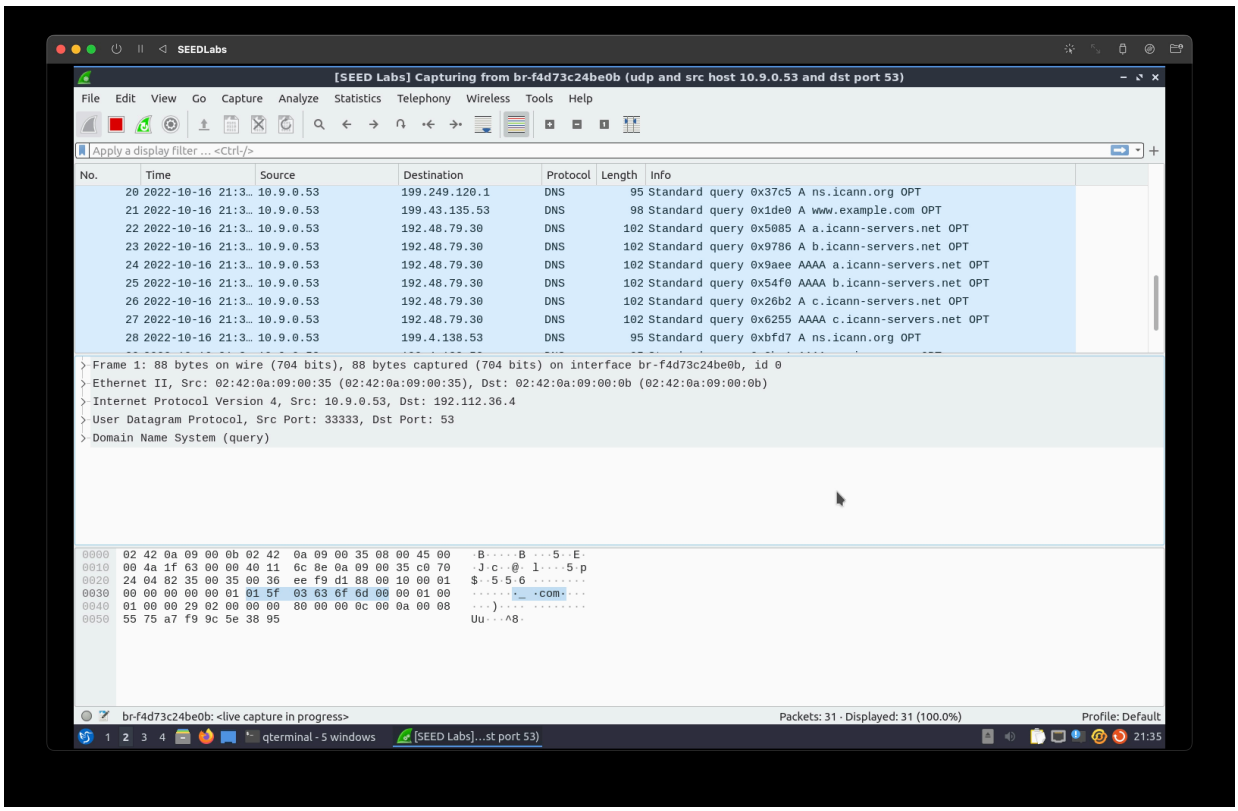
Task 2: DNS Cache Poisoning Attack – Spoofing Answers

```
python3 task2.py
```

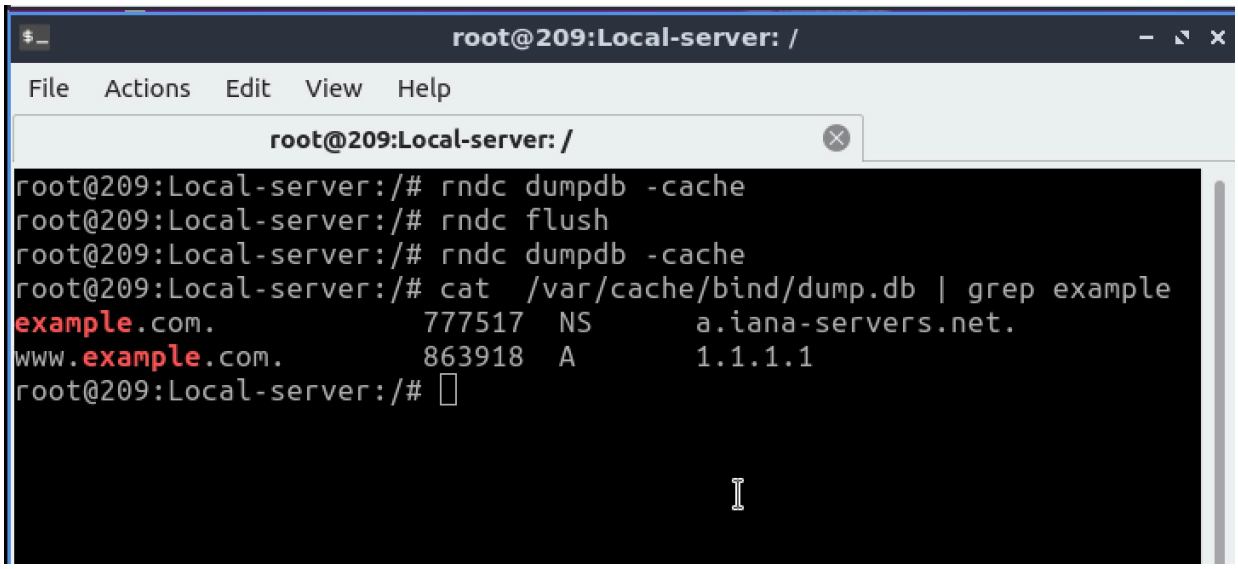
```
dig www.example.com
```



Wireshark:



```
rndc dumpdb -cache
cat /var/cache/bind/dump.db | grep example
```

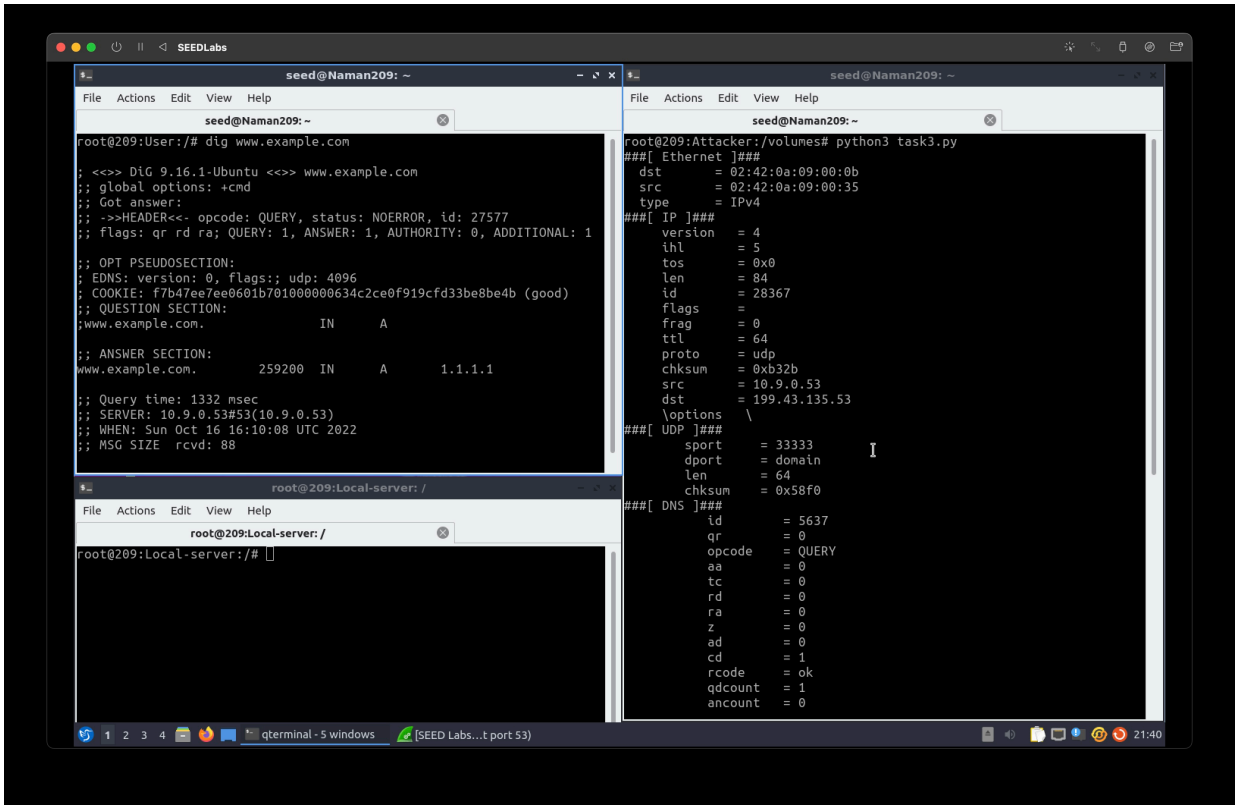


Observation: We observe that a new entry was created because of `task2.py`

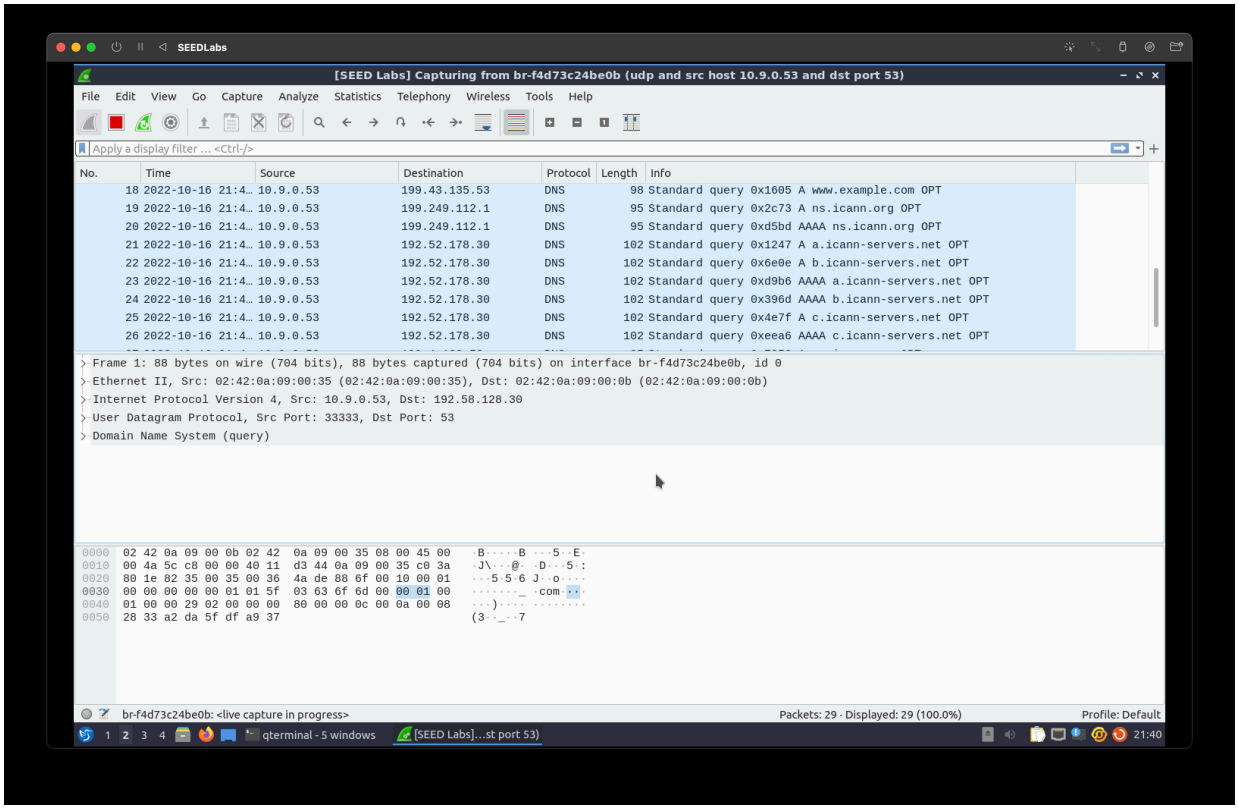
Task 3: Spoofing NS Records

```
python3 task3.py
```

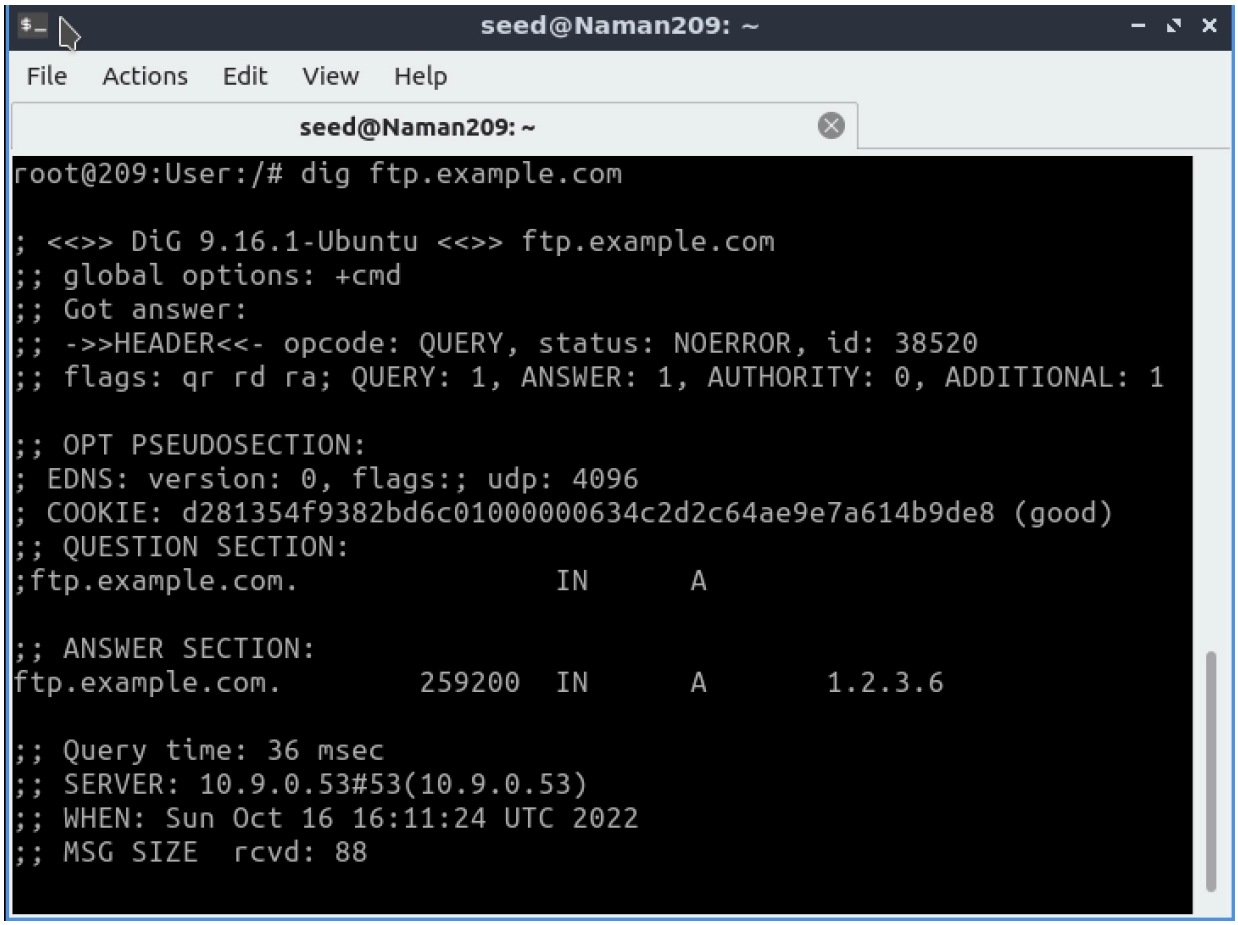
```
dig www.example.com
```



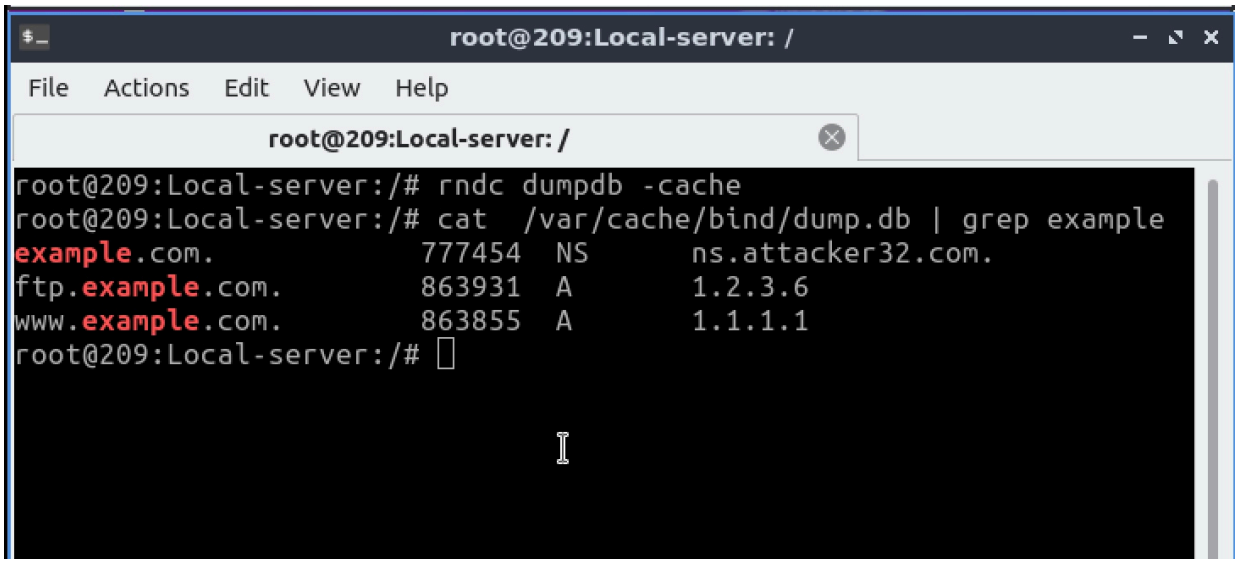
Wireshark:




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




```
rndc dumpdb -cache
cat /var/cache/bind/dump.db | grep example
```

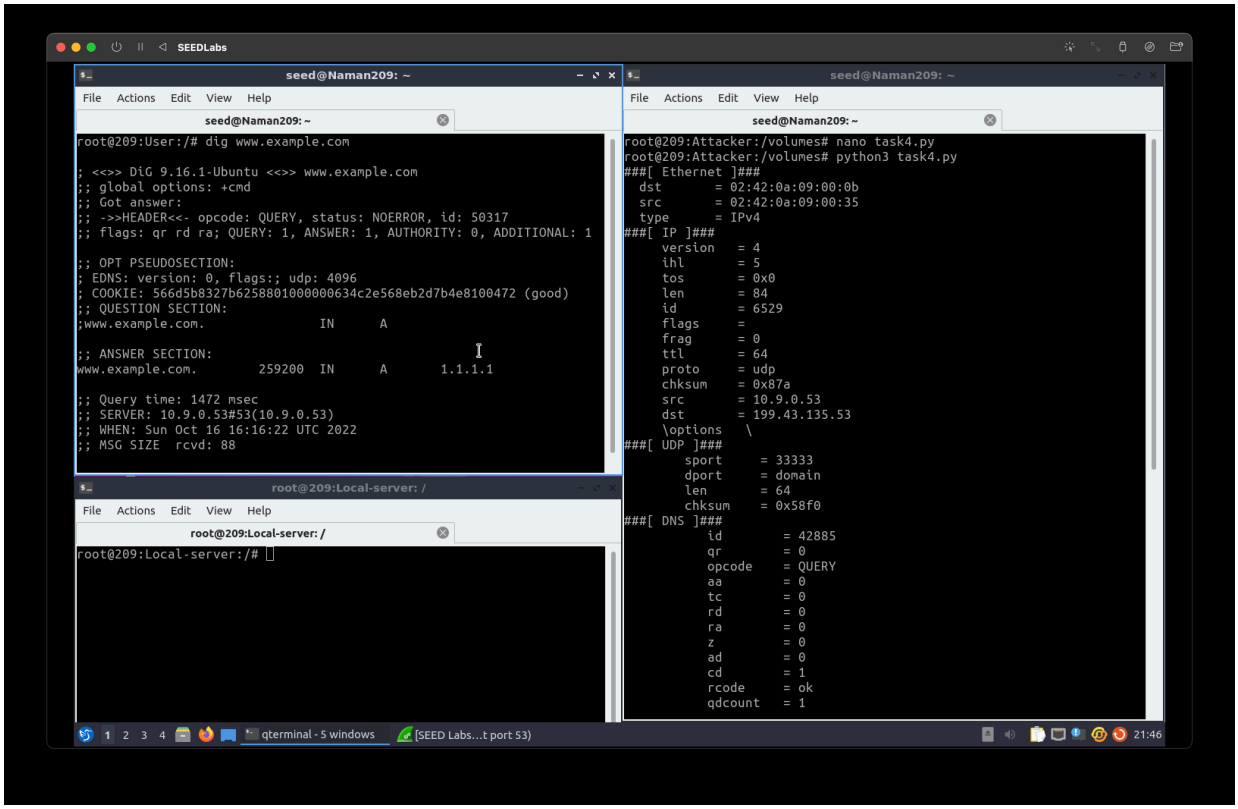


Observation: The spoofing of the packed has been reflected in the dump file

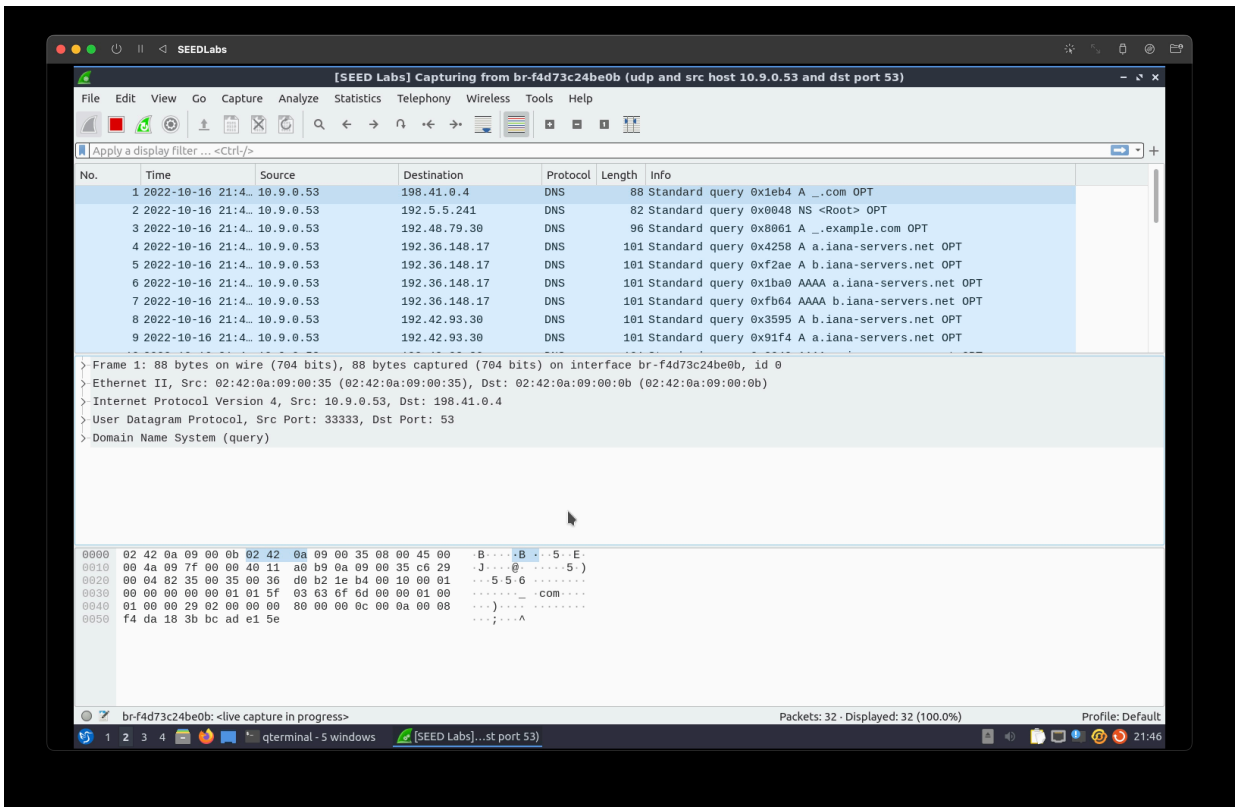
Task 4: Spoofing NS Records for Another Domain

```
python3 task3.py
```

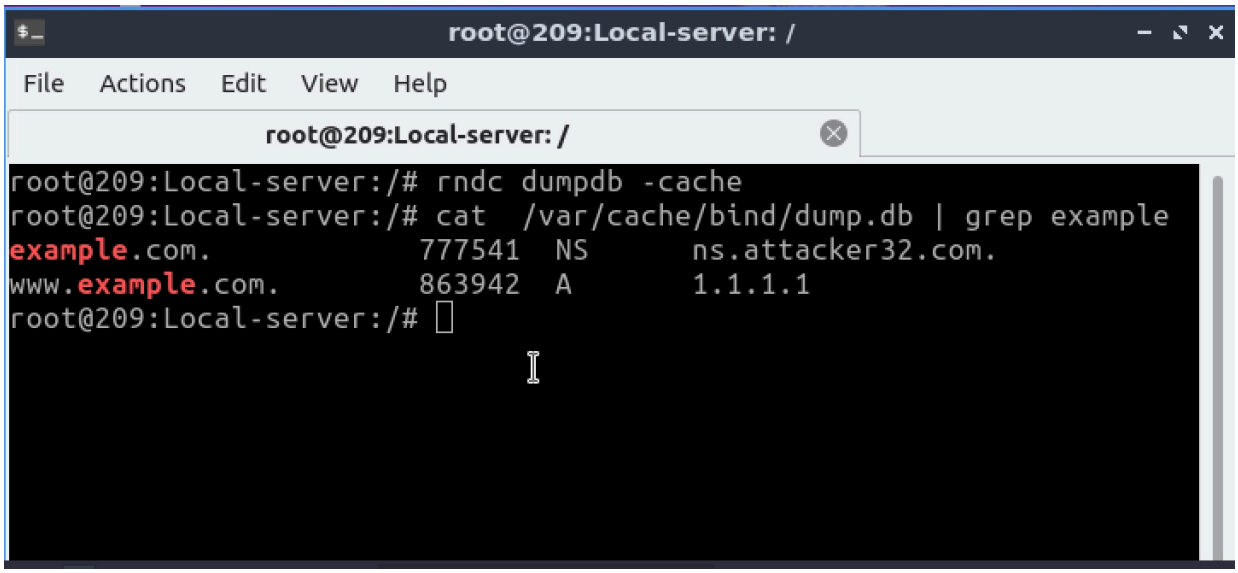
```
dig www.example.com
```



Wireshark:



```
rndc dumpdb -cache
cat /var/cache/bind/dump.db | grep example
```

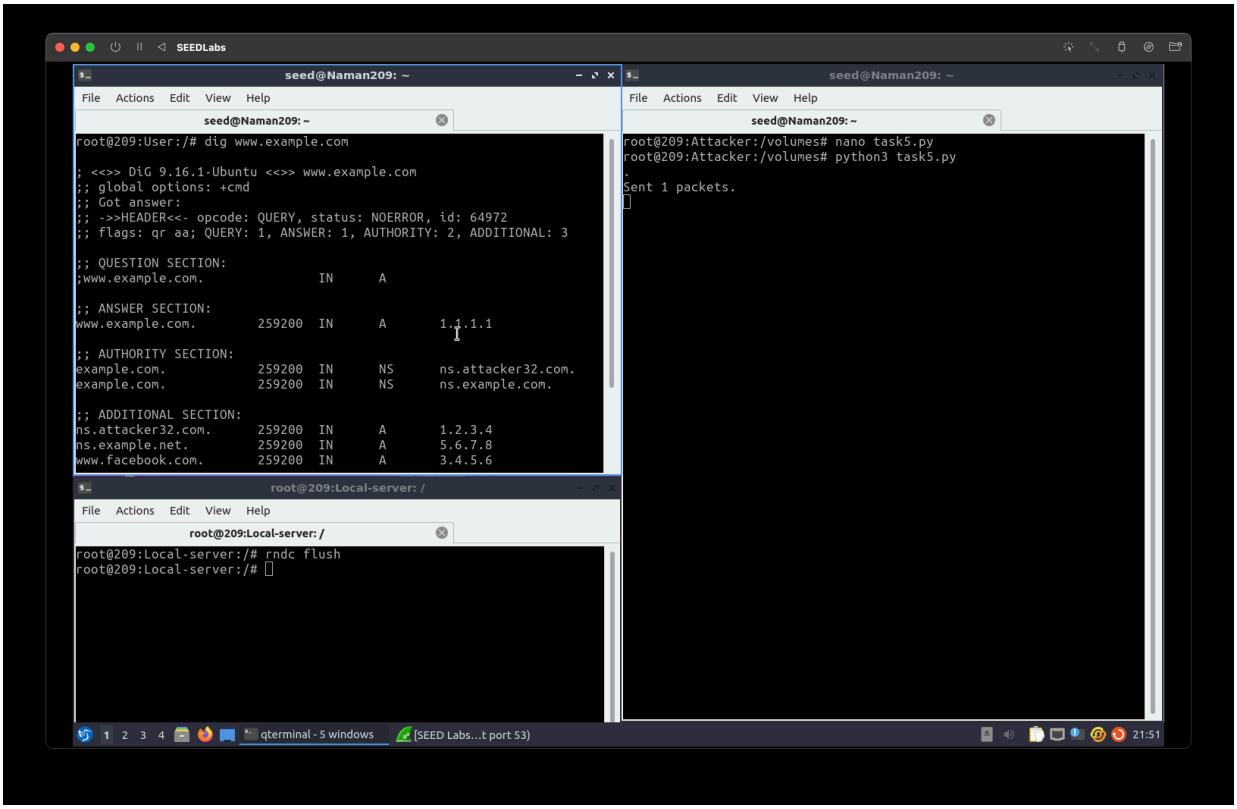


Observation: ns attacker now becomes the default nameserver due to entries in authority section

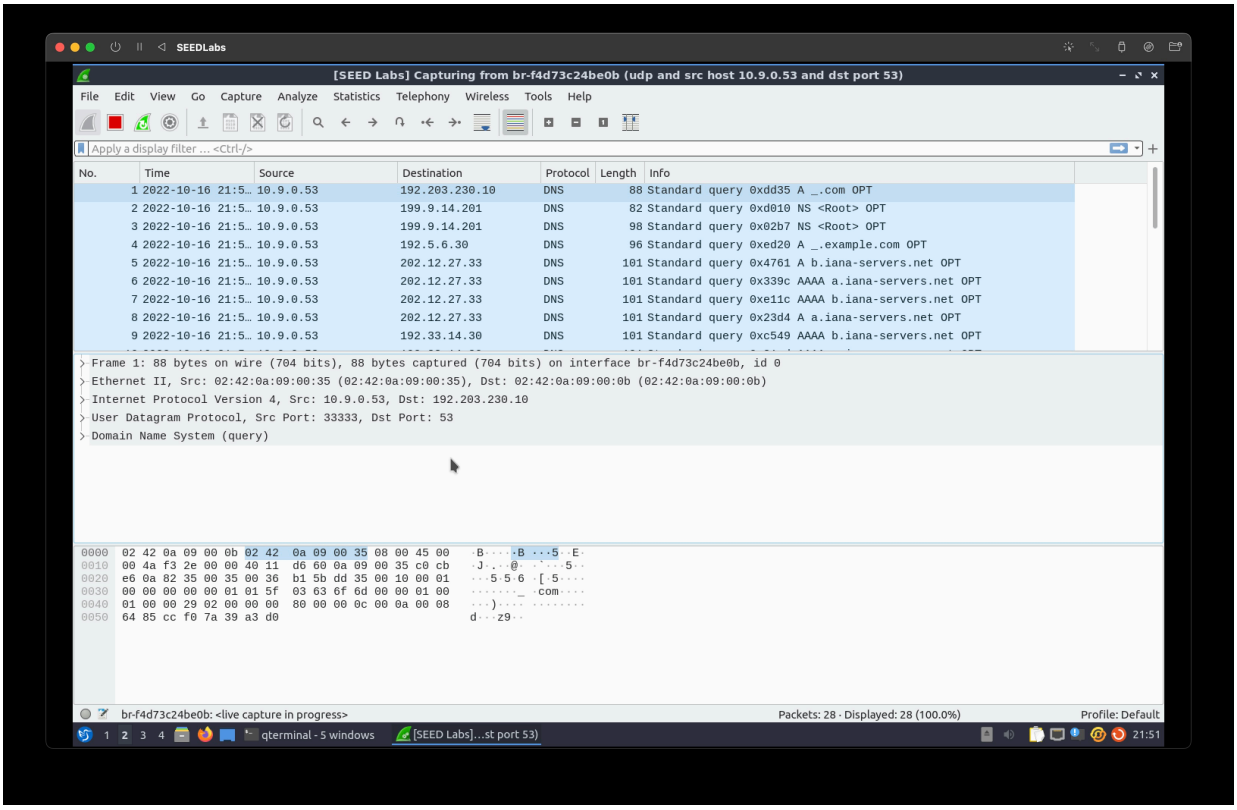
Task 5: Spoofing Records in the Additional Section

```
python3 task3.py
```

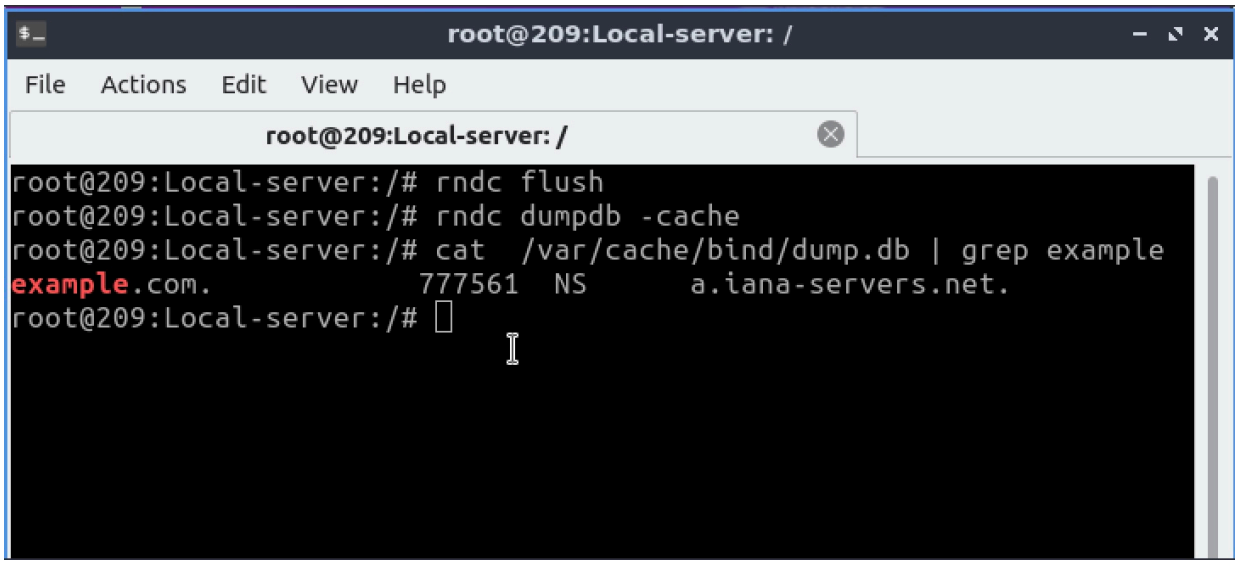
```
dig www.example.com
```



Wireshark:




```
rndc dumpdb -cache
cat /var/cache/bind/dump.db | grep example
```



Observation: attack successful on the default nameserver due to entries in additional section