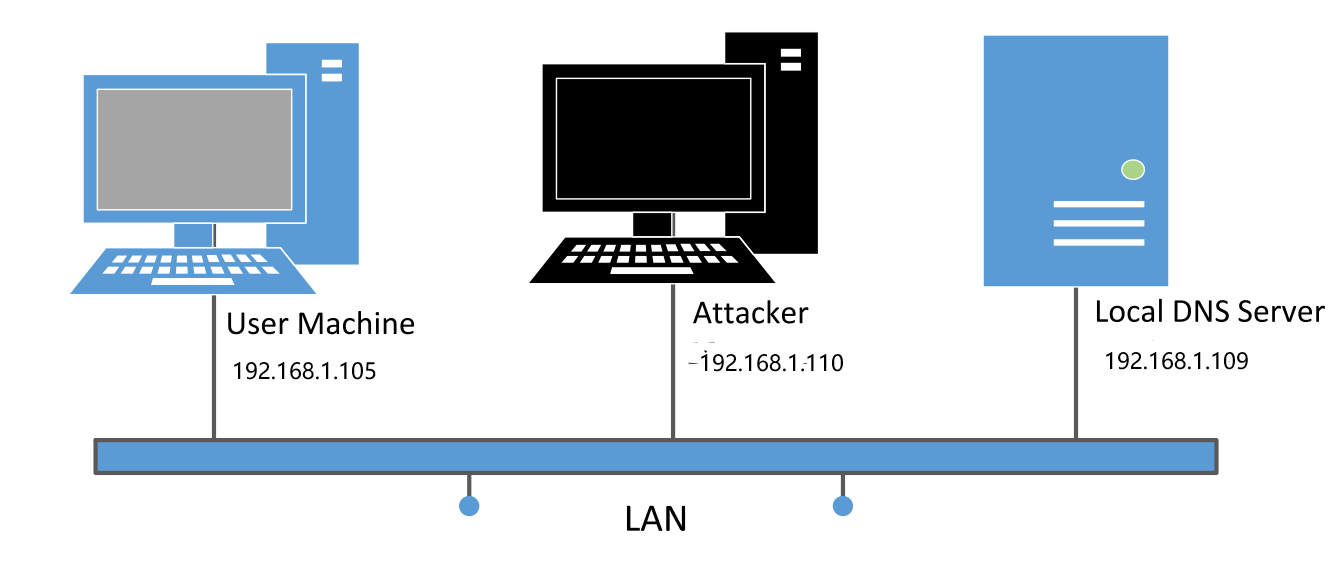
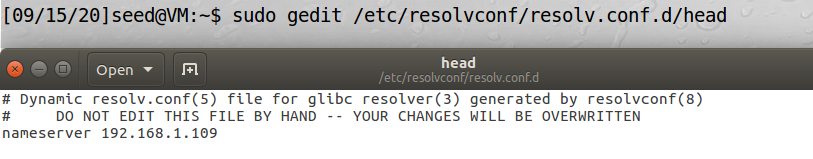
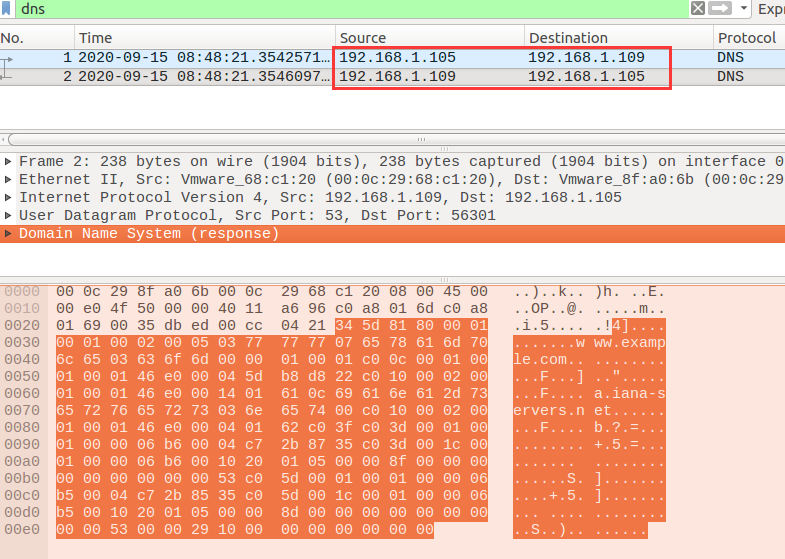
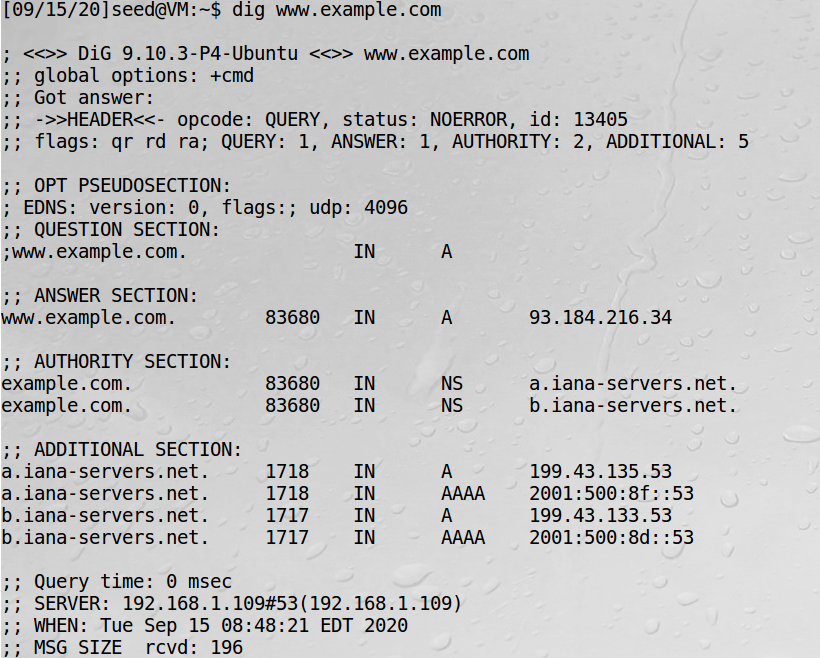
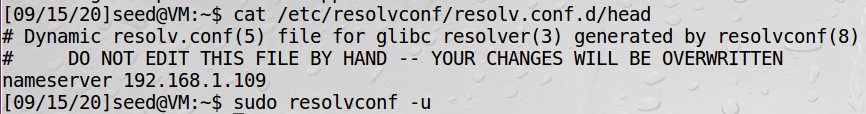
# Local DNS Attack Lab

57117217戚吴祺



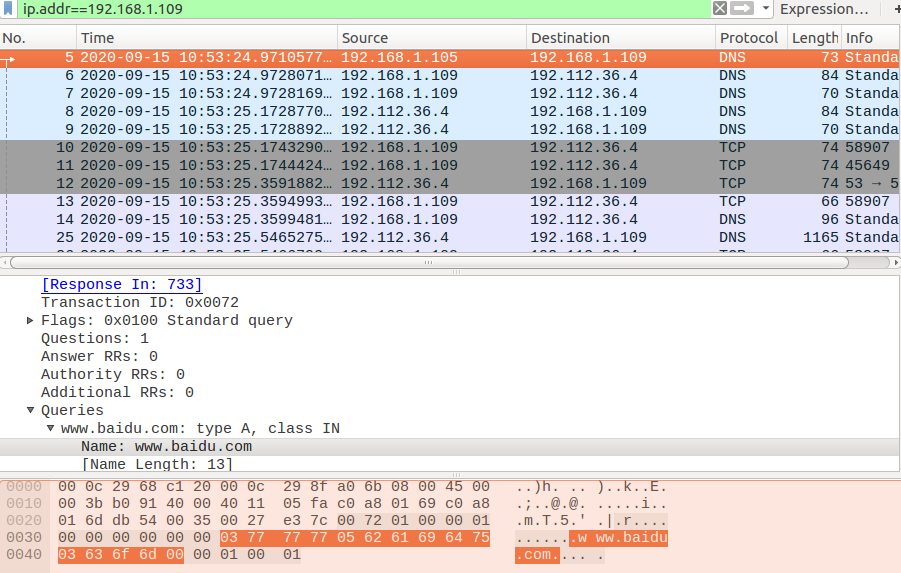
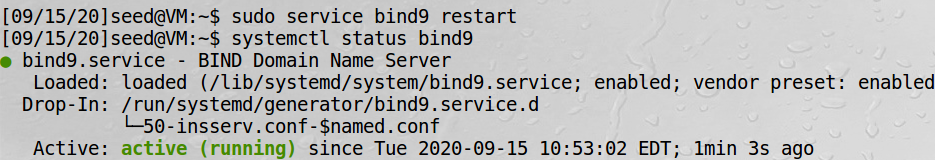
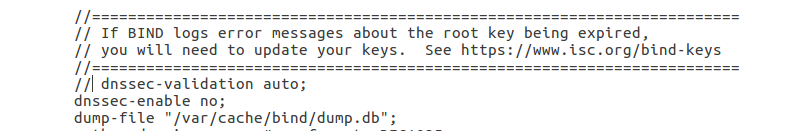
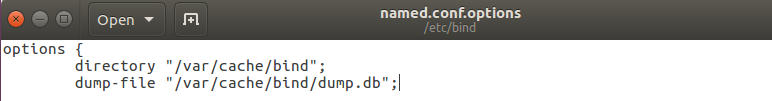
## Task 1: Configure the User Machine





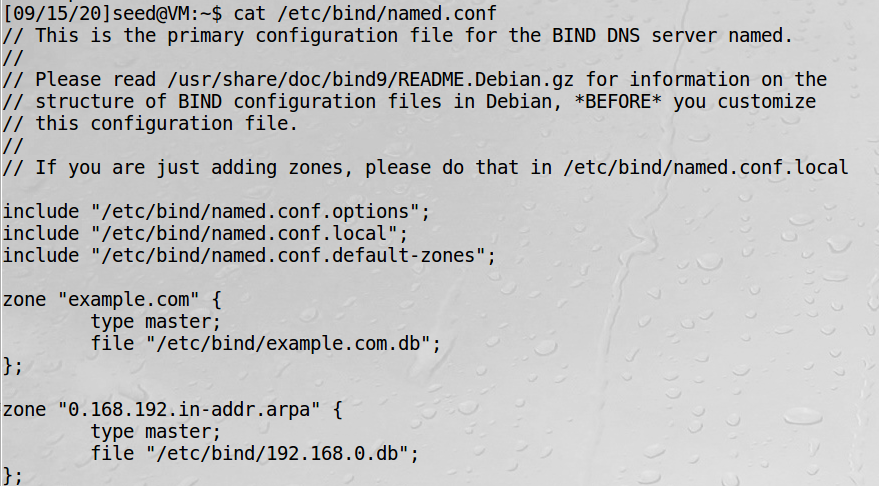
The evidence is above. Therefore, the setup is successful.

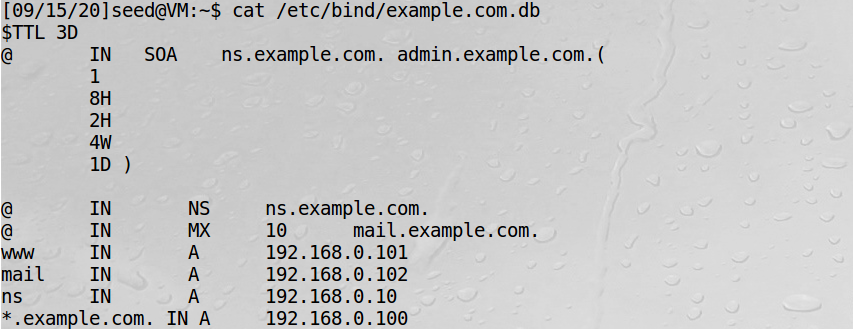
## Task 2: Set up a Local DNS Server

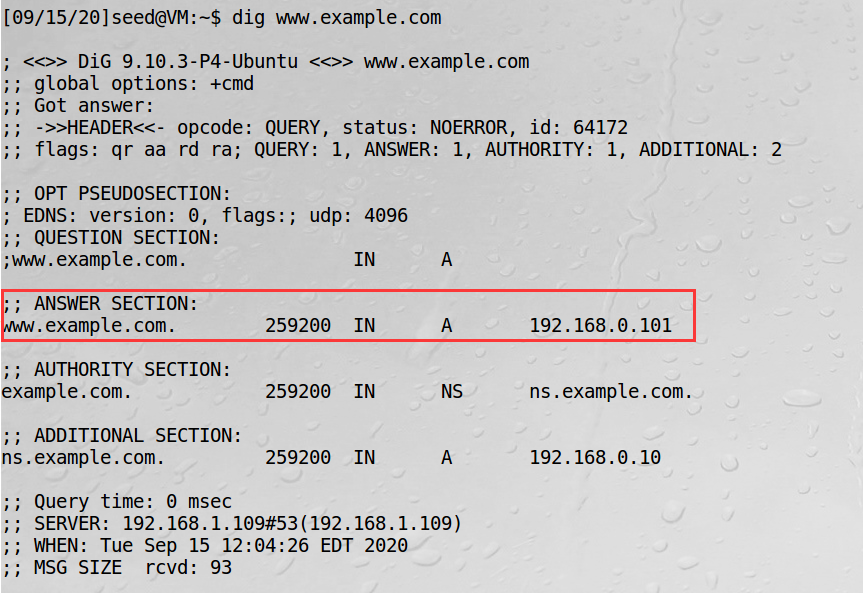


当dns cache 被命中时，即当查询的hostname存在于cache中，才会被使用

## Task 3: Host a Zone in the Local DNS Server



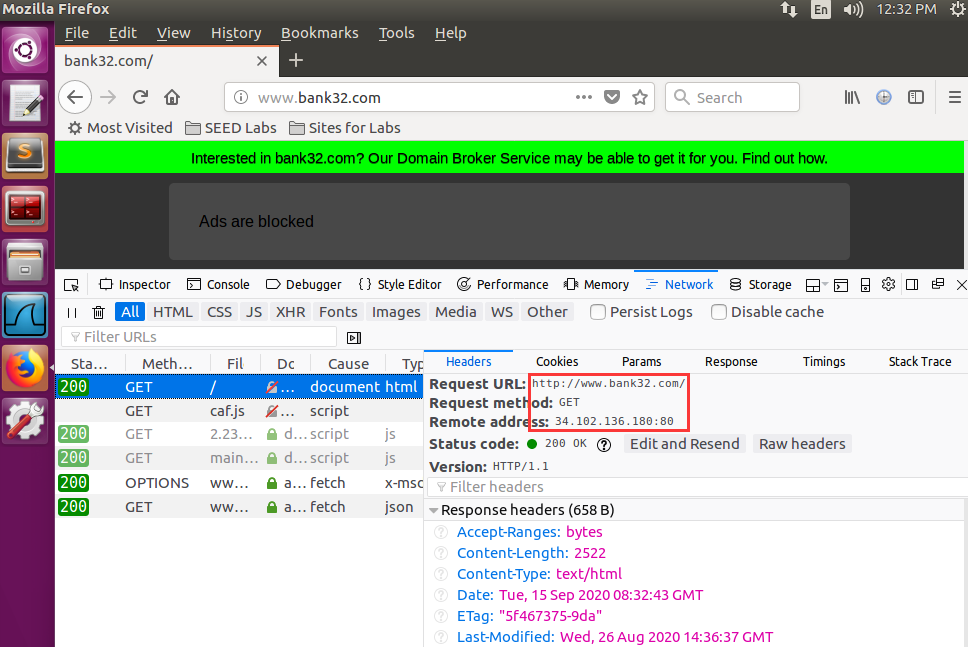




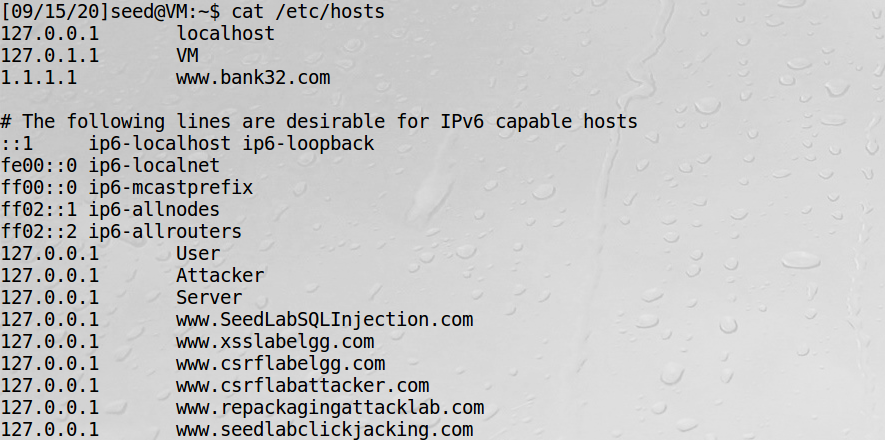
[www.example.com](http://www.example.com) was resolved to 192.168.0.101 which we set.

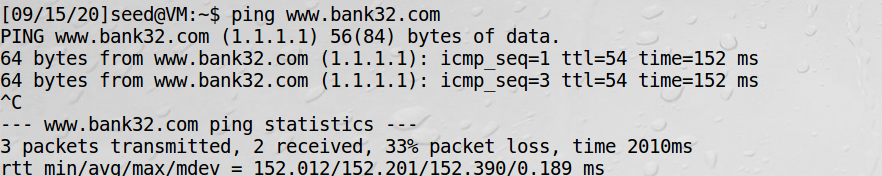
## Task 4: Modifying the Host File

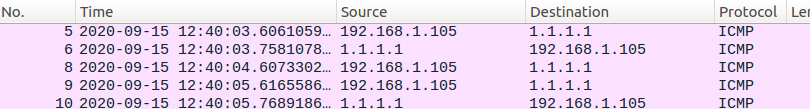
Before: [www.bank32.com](http://www.bank32.com) was resolved to 32.102.136.180



After: [www.bank32.com](http://www.bank32.com) was resolved to 1.1.1.1 which we set in /etc/hosts

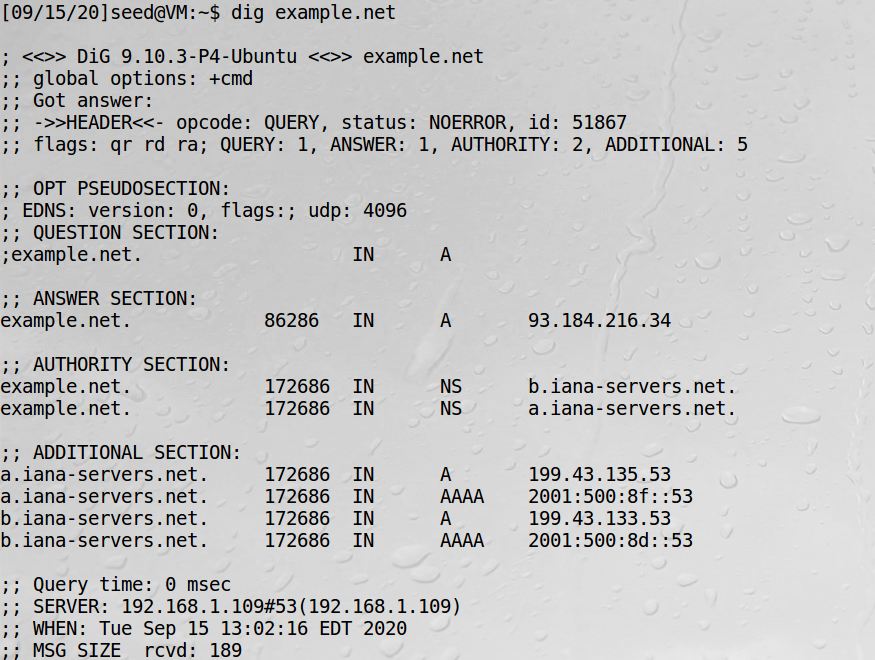




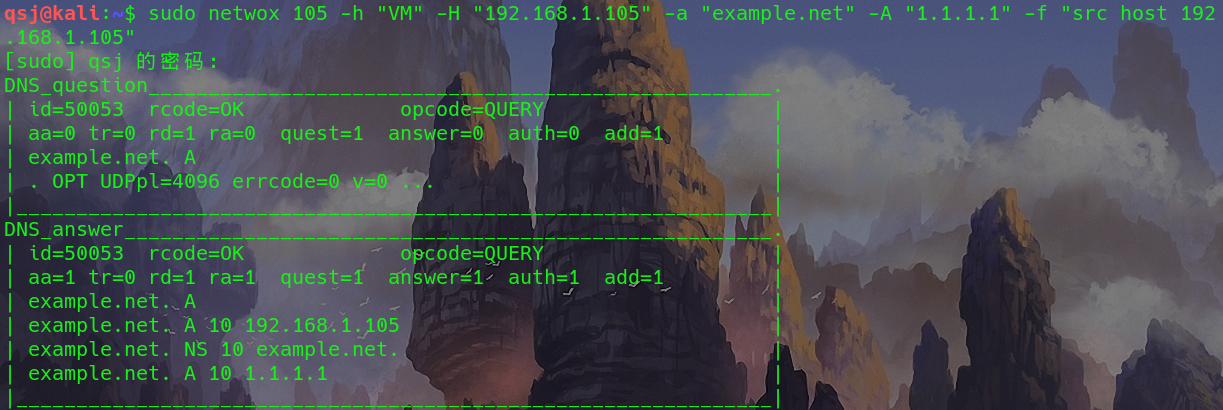


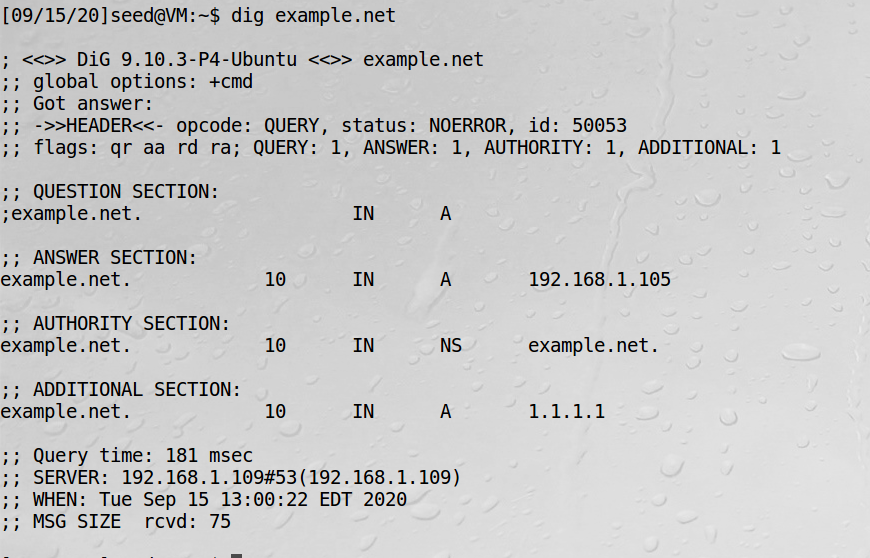
## Task 5: Directly Spoofing Response to User

Before:



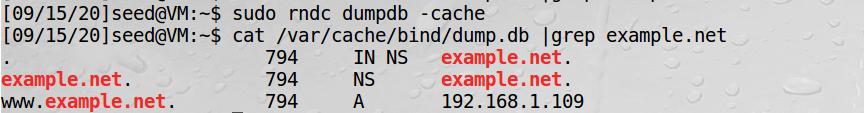
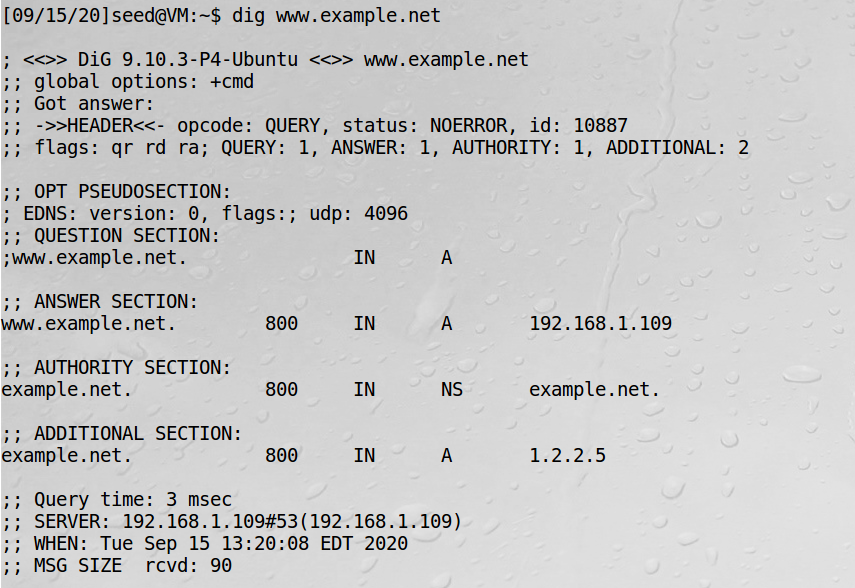
After:





My attack is successful.

## Task 6: DNS Cache Poisoning Attack

The DNS server is poisoned

## Task 7: DNS Cache Poisoning: Targeting the Authority Section

