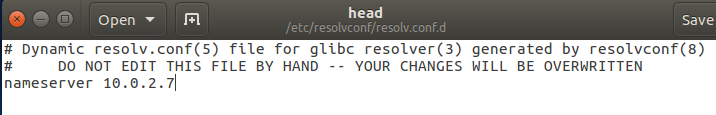
Local DNS Attack Lab

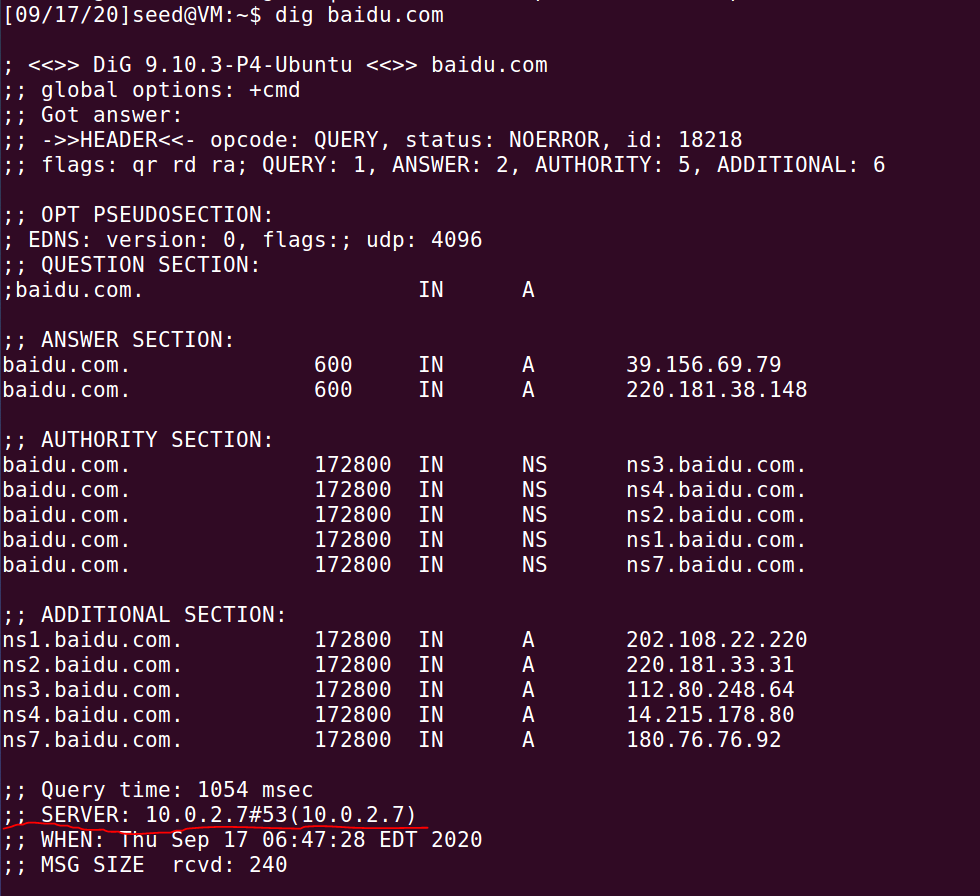
10.0.2.5：user machine

10.0.2.6：attacker

10.0.2.7：Local DNS Server

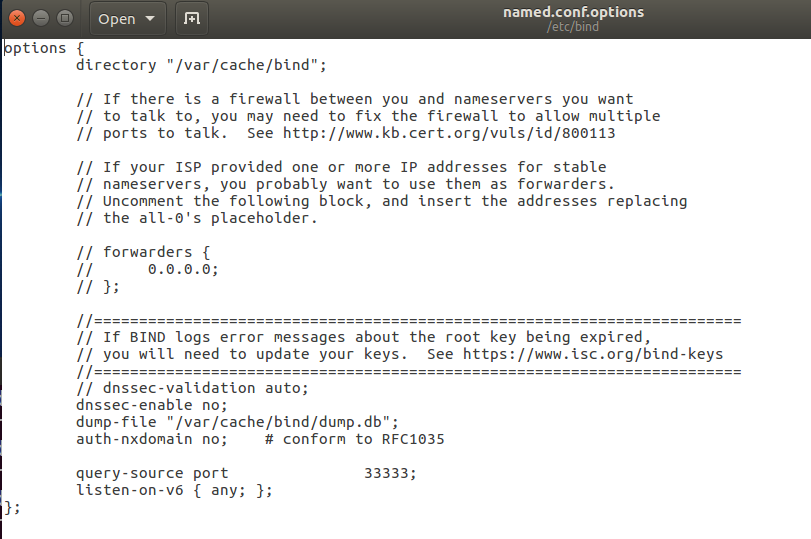
## Task1





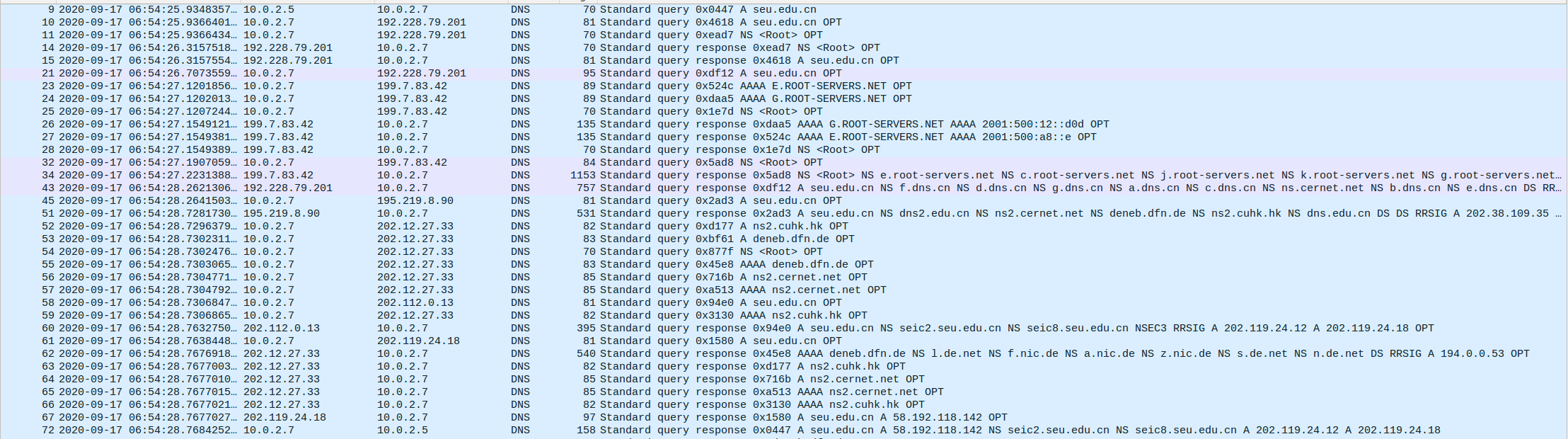
可以看到SERVER是10.0.2.7，成功

## Task2



dump-file已经有了，无需再添加，DNSSEC也已经被禁用

开启DNS服务器，ping seu.edu.cn，过了一会才开始发送ICMP报文，因为可能没有DNS缓存，Wireshark抓包：

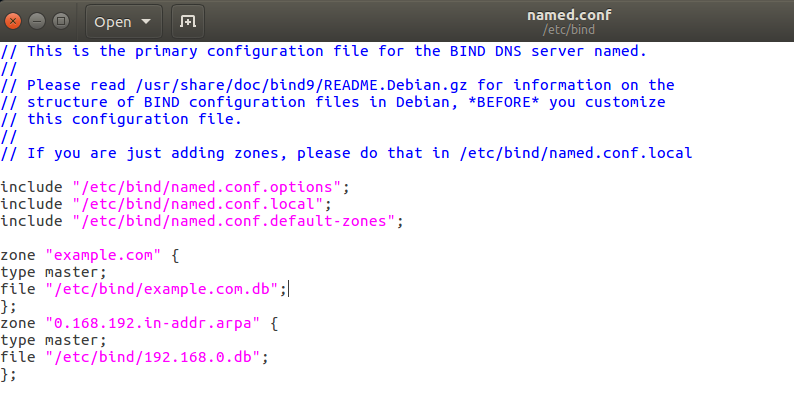


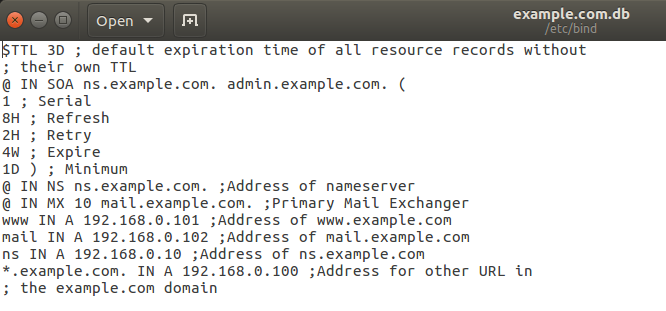
可以看到DNS服务器由于没有seu.edu.cn这个域名的缓存，向其他域名服务器请求查询这个域名，然后再发给用户机。如果再ping baidu.com:



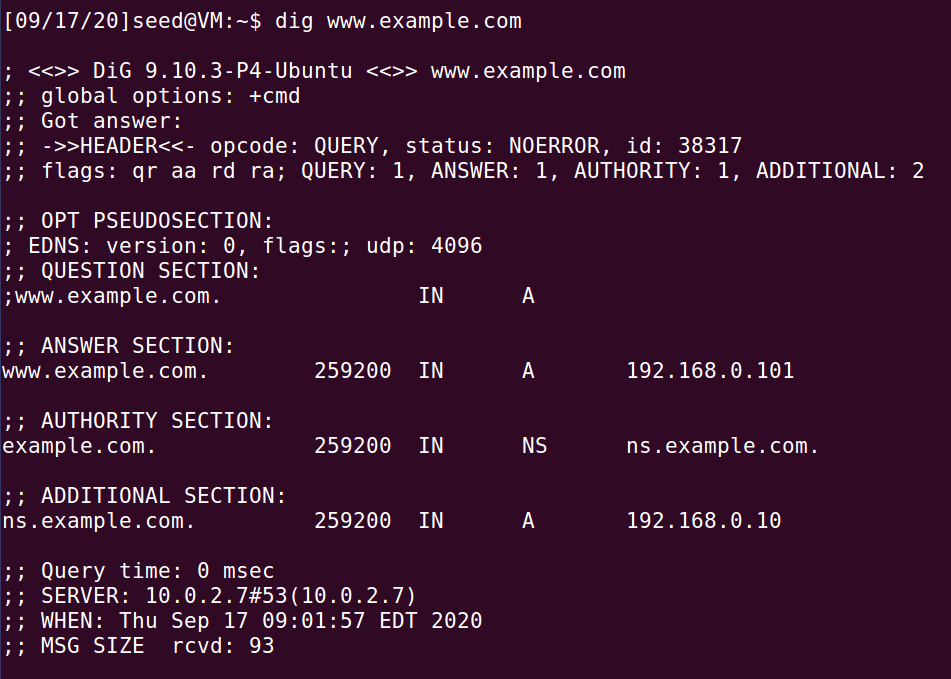
DNS服务器直接返回IP地址，因为之前ping过baidu.com，DNS服务器中有缓存

## Task3





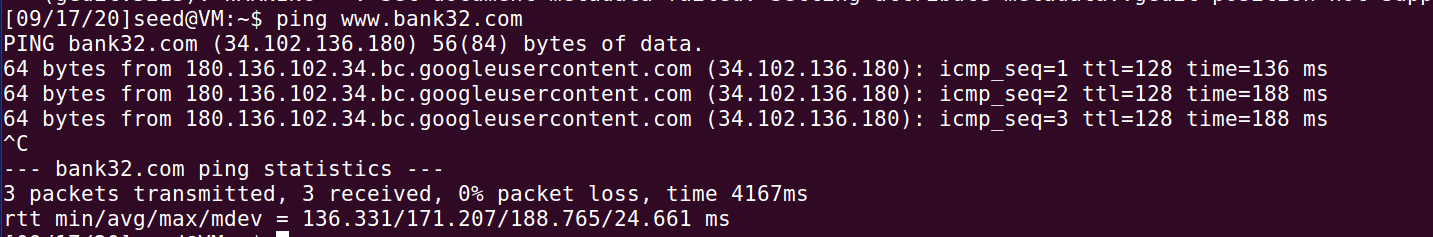




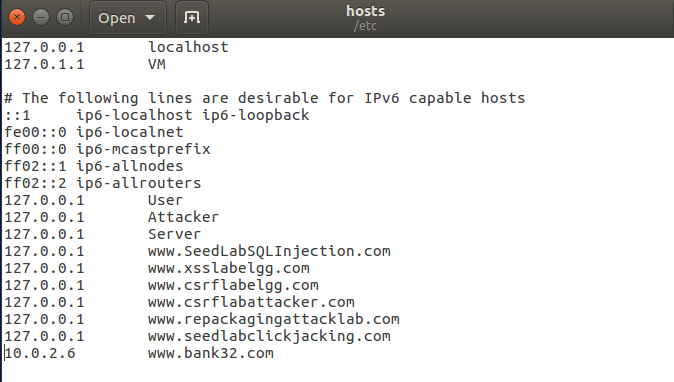
成功获得[www.exaple.com的IP](http://www.exaple.com的IP)地址。

## Task4

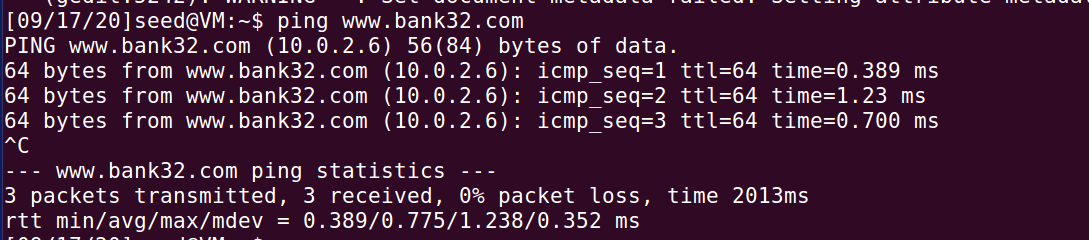
之前：



修改：



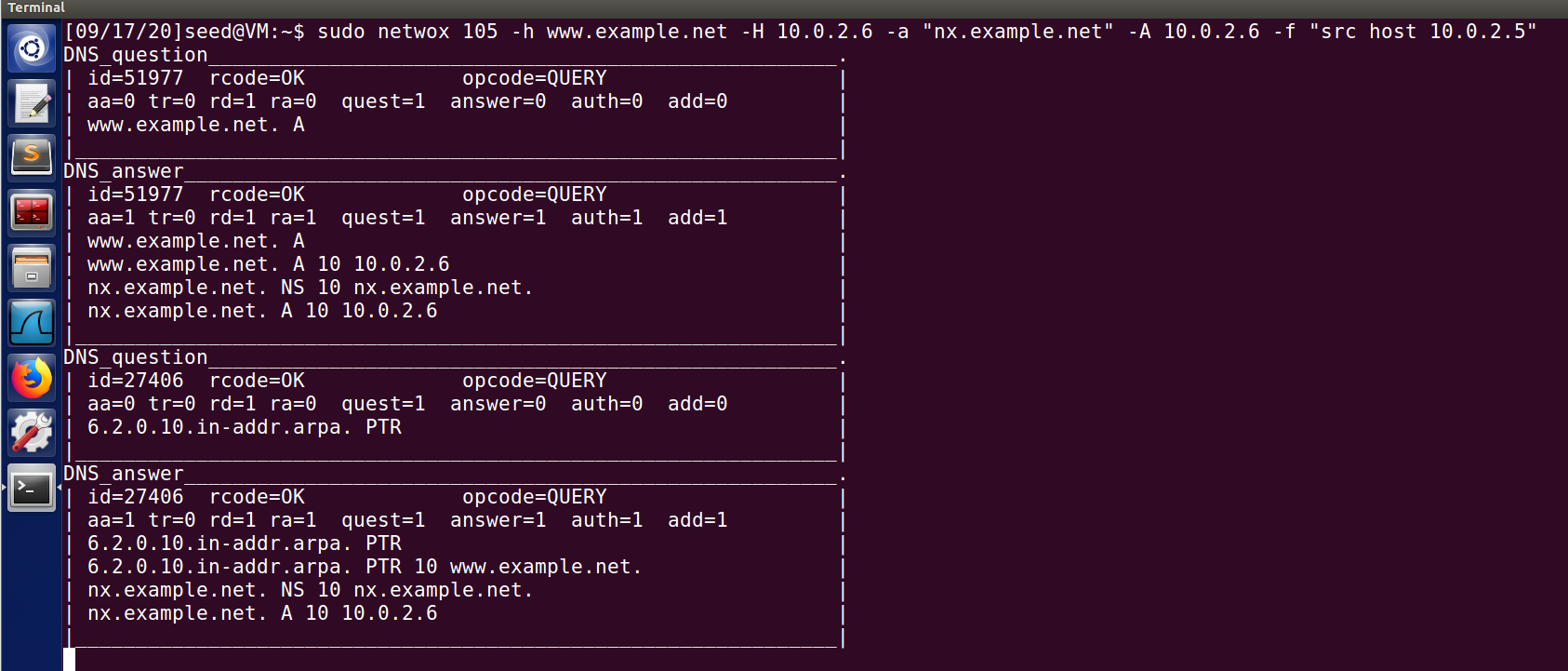
之后：



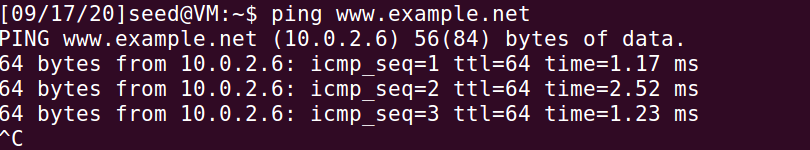
可以看到域名对应的IP地址变成了attacker的IP地址10.0.2.6

## Task5

攻击者：



用户机：

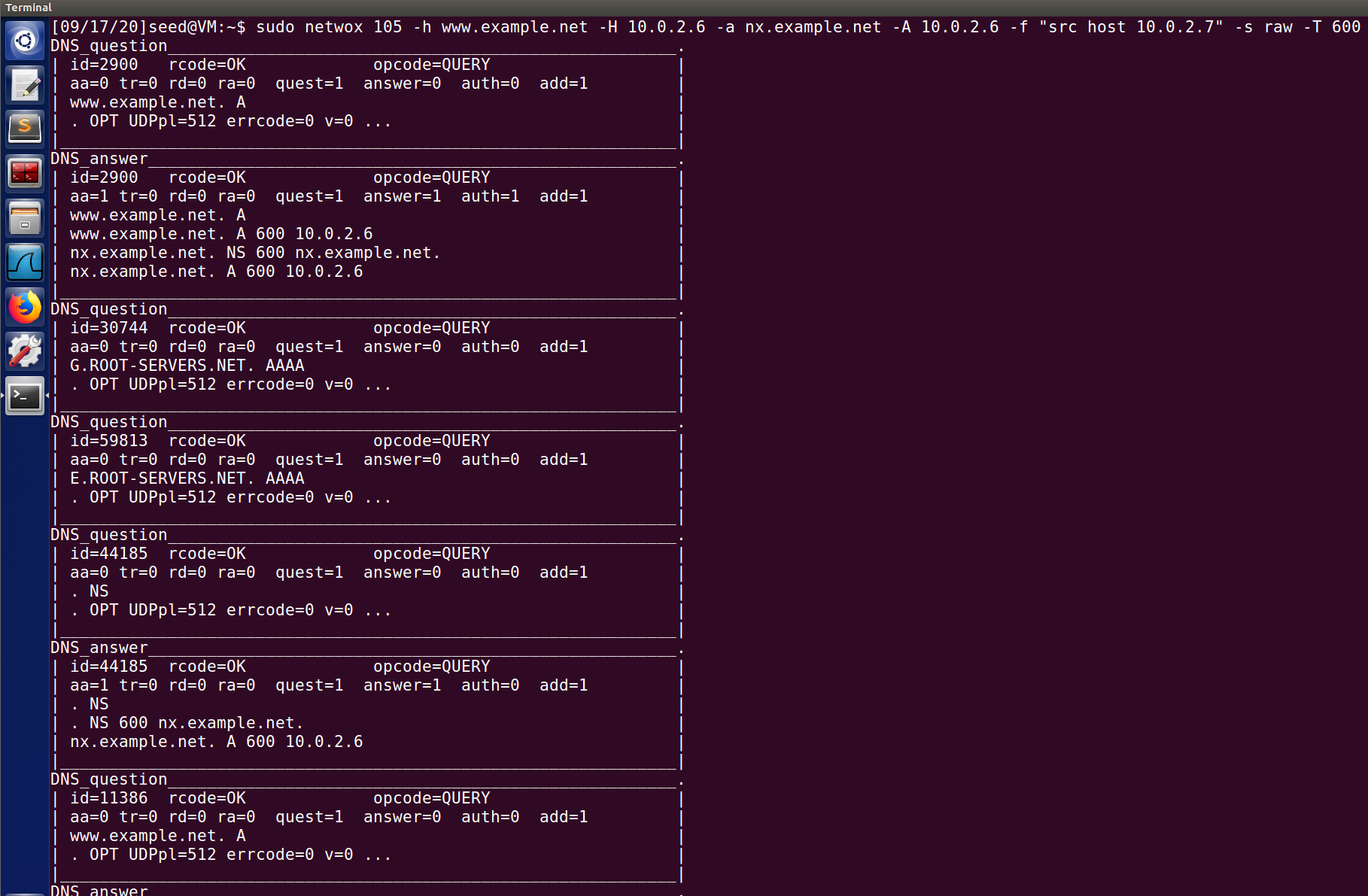


可以看到，攻击者嗅探到了用户发往DNS服务器的关于域名[www.example.net](http://www.example.net)的DNS请求，并成功伪造了回复报文，将IP设置为本机IP

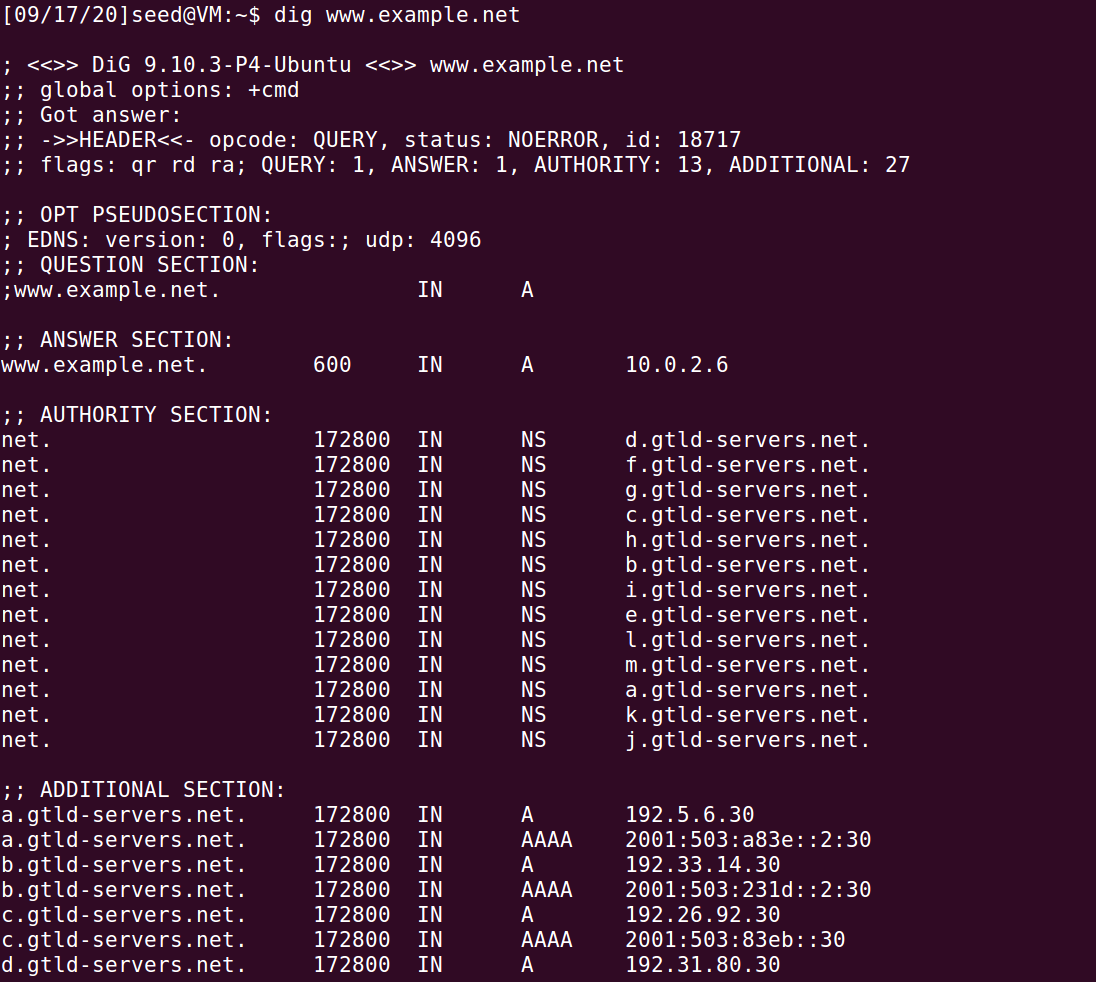
## Task6

思路和Task5一致，只不过嗅探DNS服务器的DNS请求，然后伪造回复，让这条记录存在于DNS服务器的缓存里。

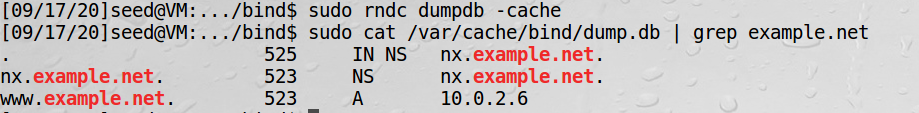
攻击者：



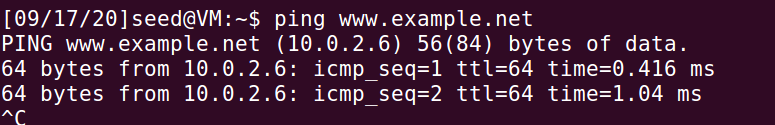
用户去访问这个域名：



然后看DNS服务器的缓存：



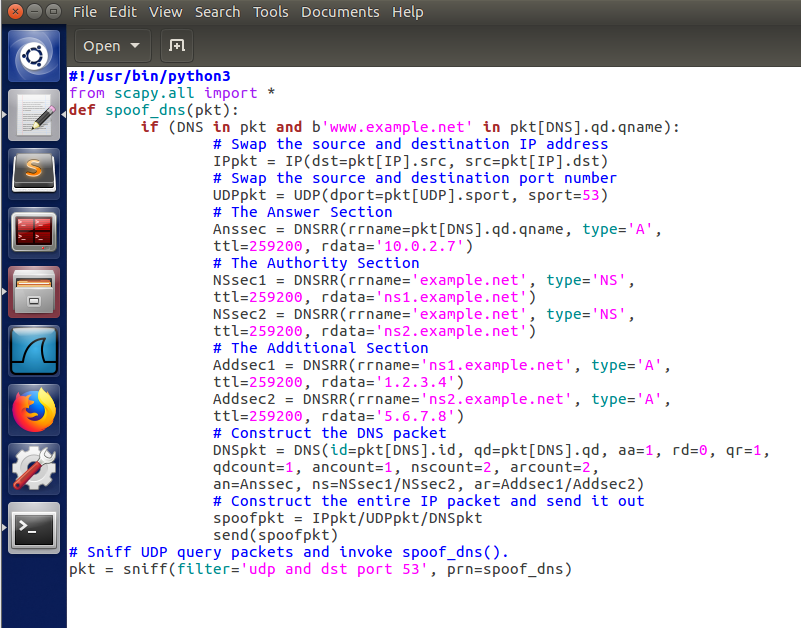
可以看到缓存被污染了，此时，用户再访问[www.example.com](http://www.example.com):



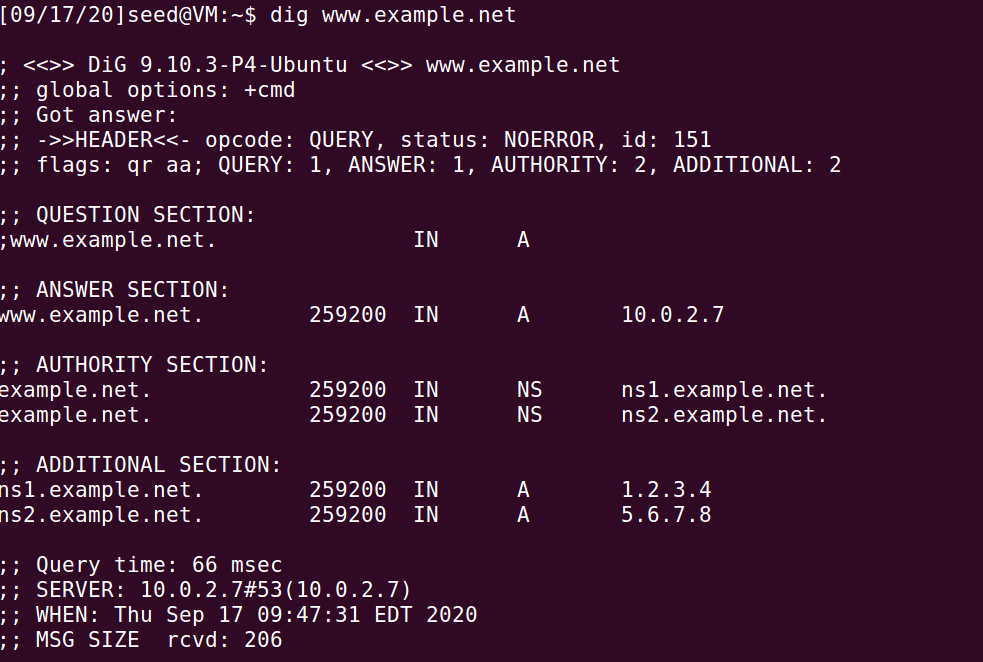
IP地址是10.0.2.6

## Task7

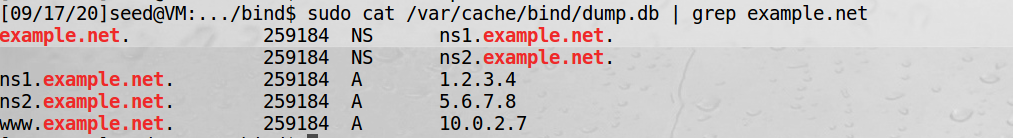
代码：



用户机：

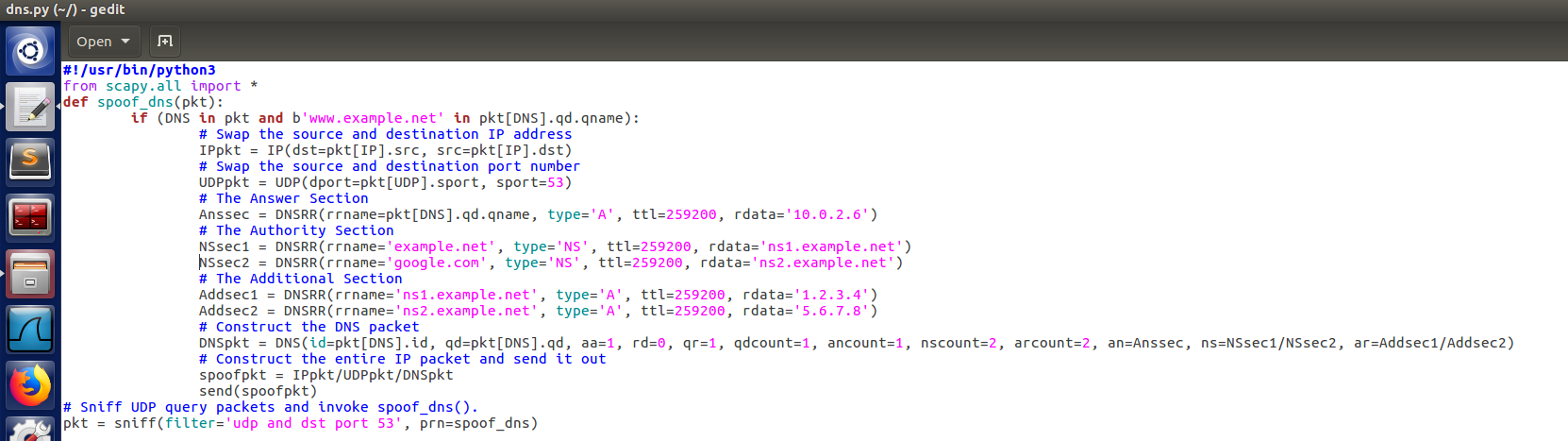


DNS服务器：

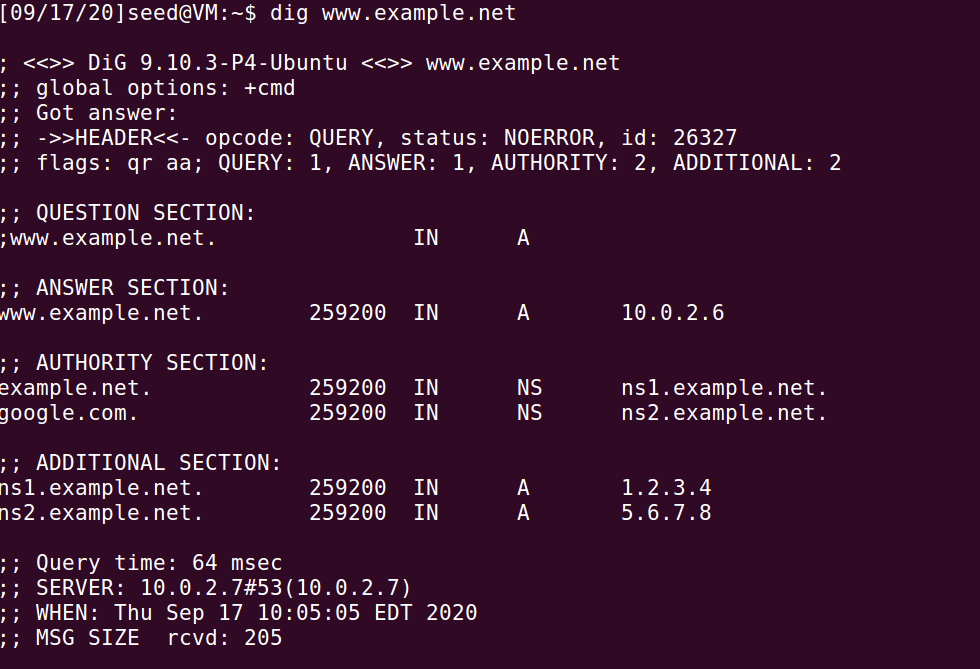


## Task8

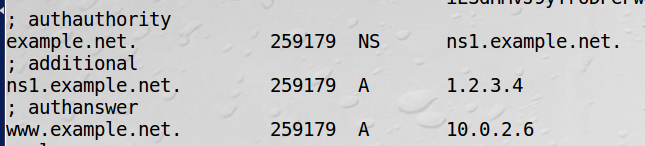
代码:



用户：



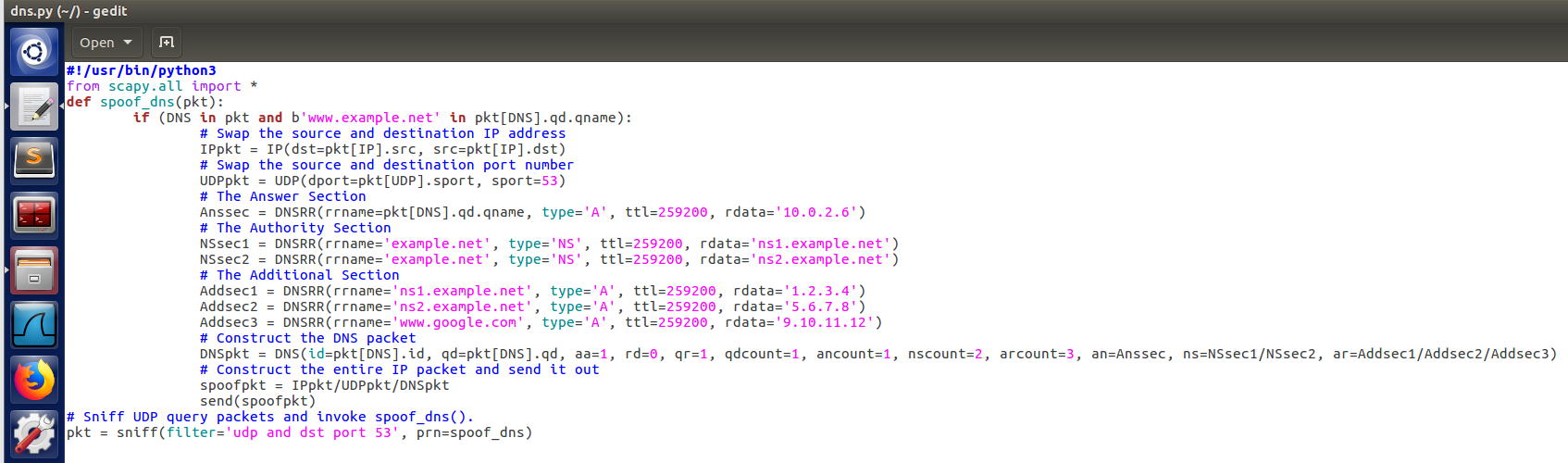
可以看到成功加入google.com。但是在DNS缓存里：



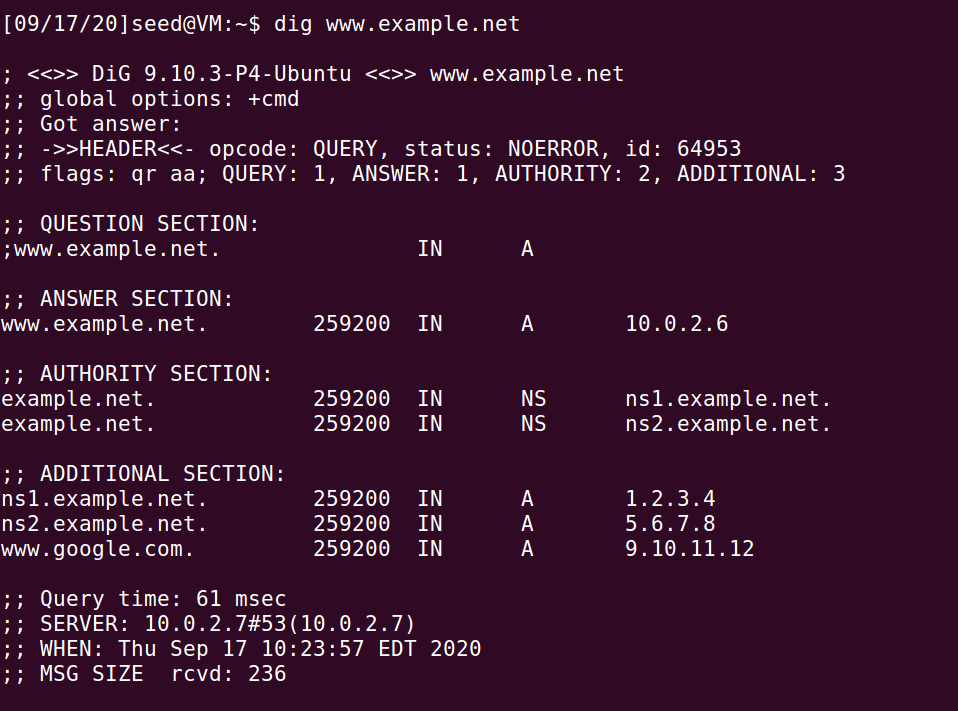
并没有记录

## Task9

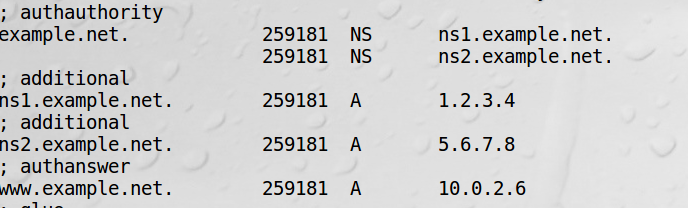
代码:



用户：成功加入



DNS缓存：



并没有www.google.com那一条记录，所以并没有被缓存，因为它只在addition section中存在。