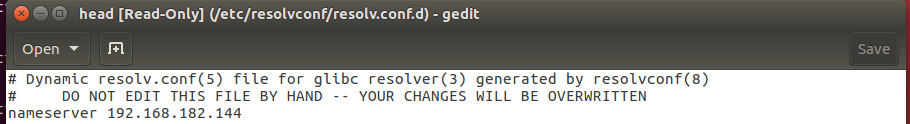
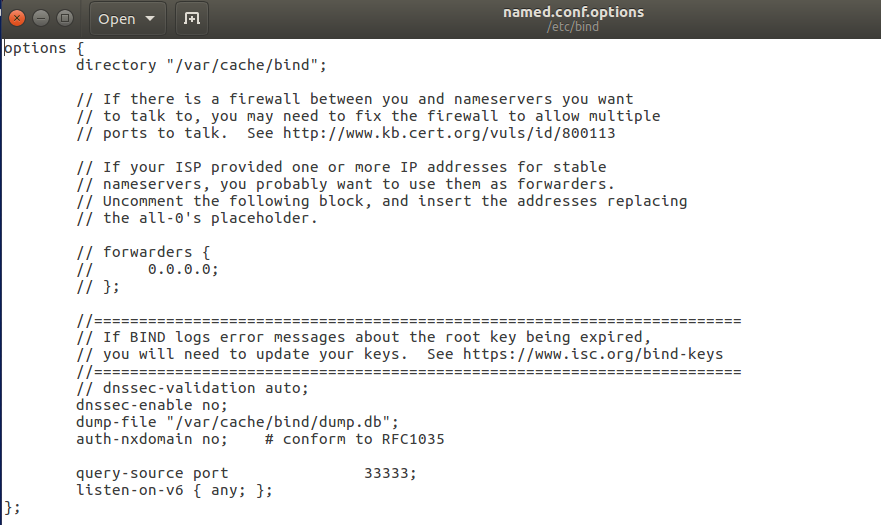
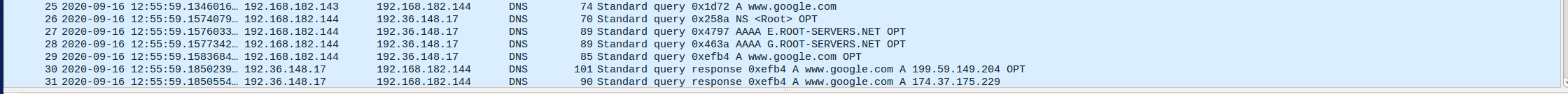
Task1





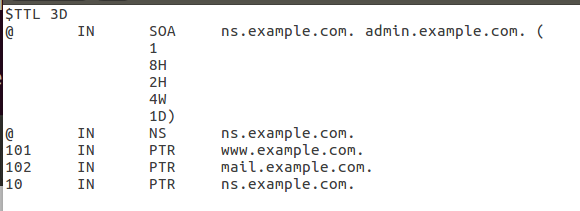
Task2

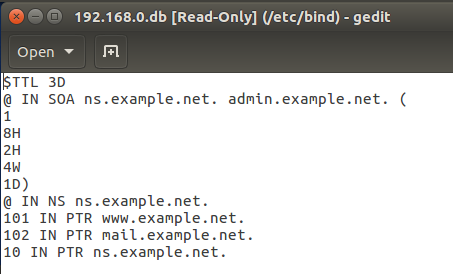


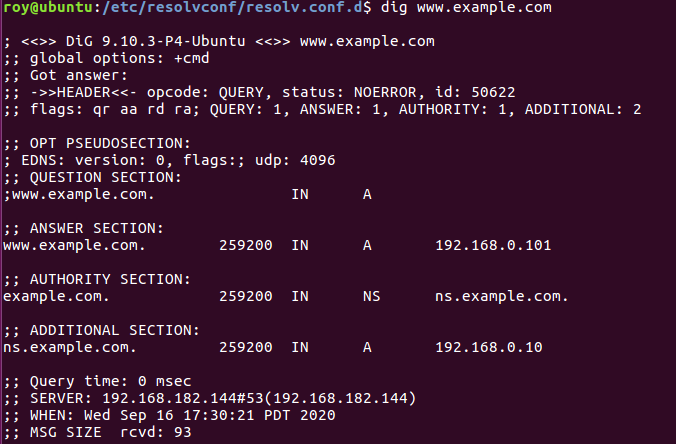


用户机知道了目标ip地址后在一定时间内使用dns缓存

Task3

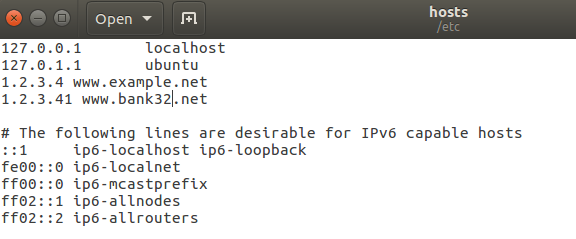






如图所示按照之前配置的返回了响应的section

Task4



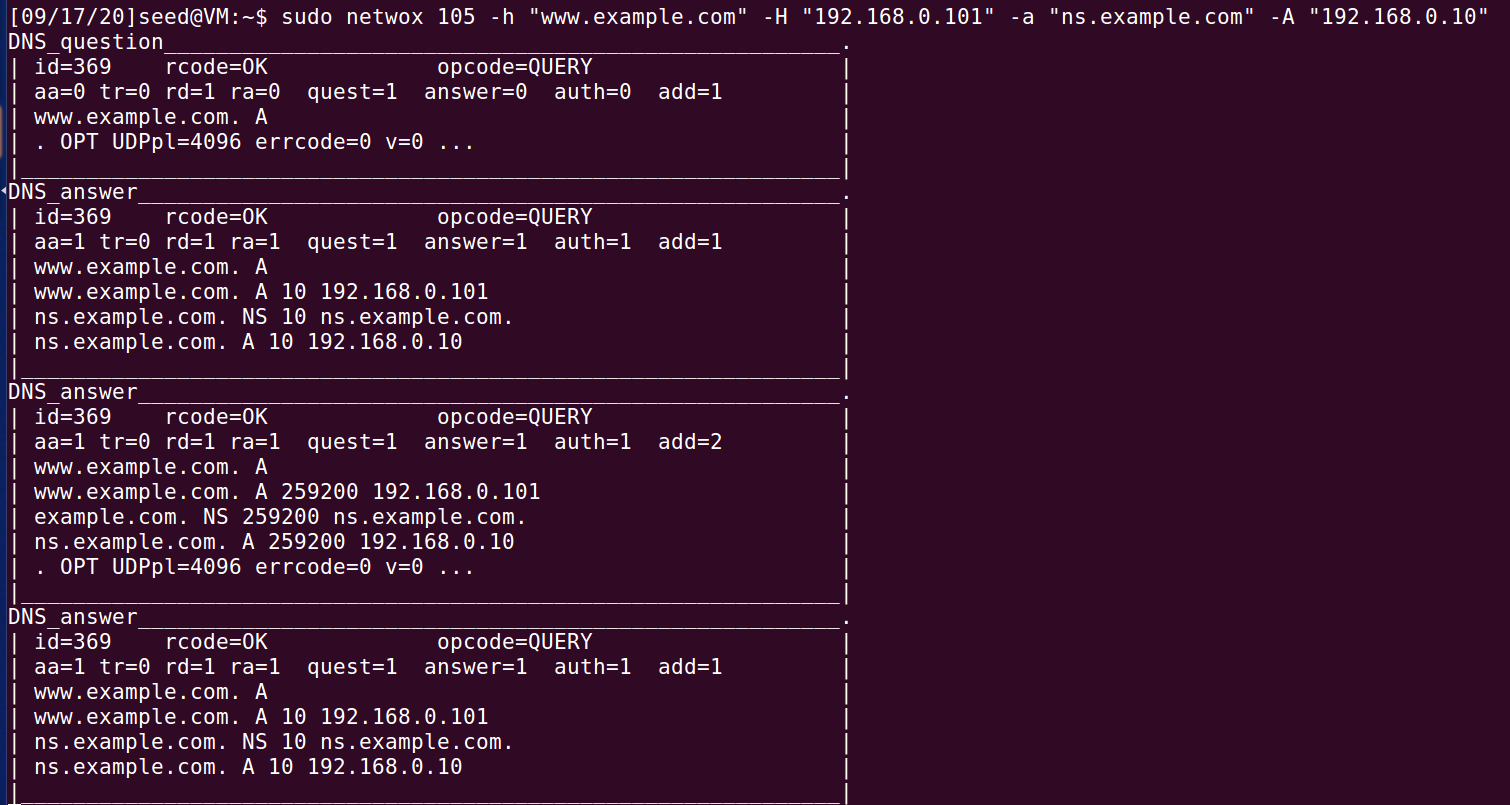
修改/etc/host文件

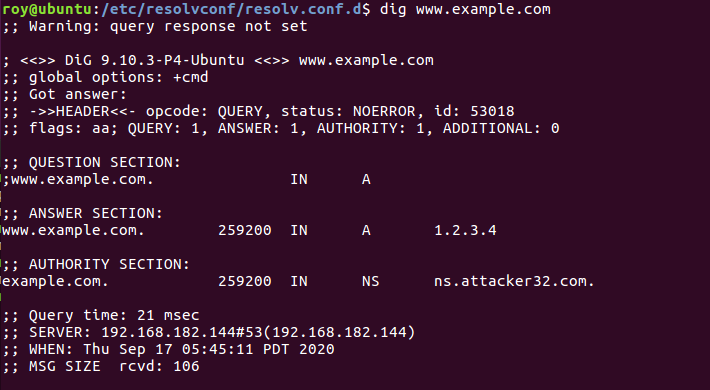


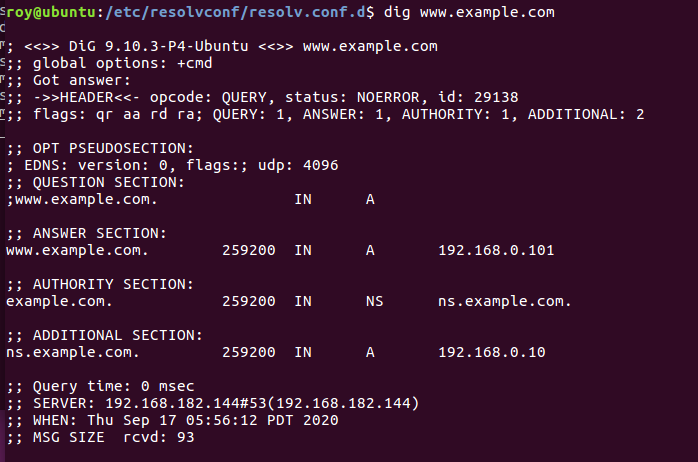


dig没有被影响，而ping受到了影响

task5

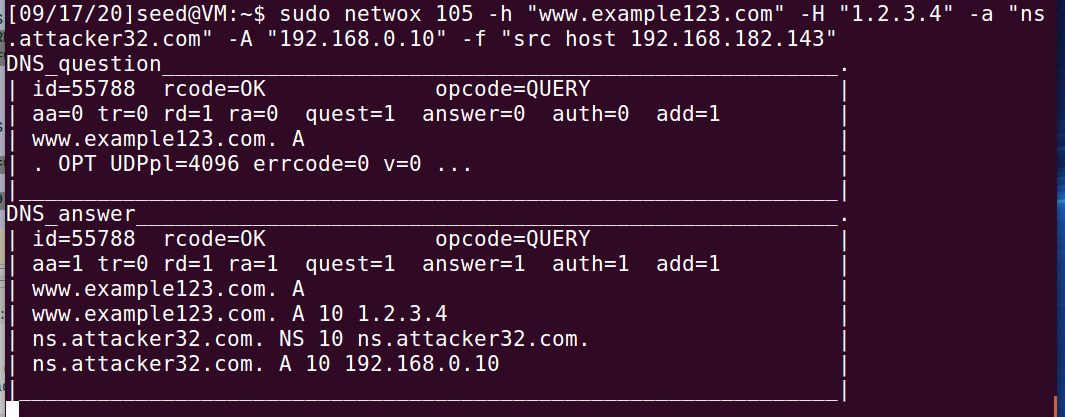






对应的section被攻击者篡改

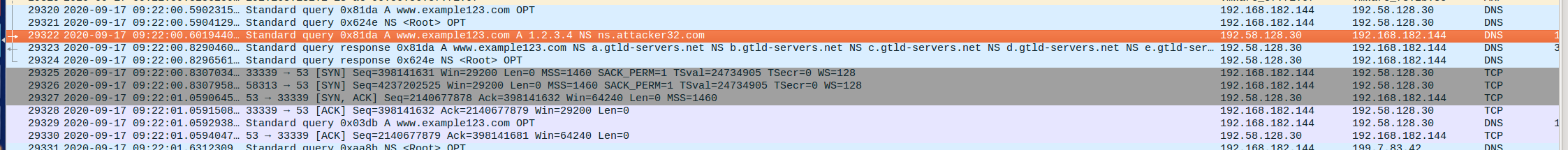
Task6



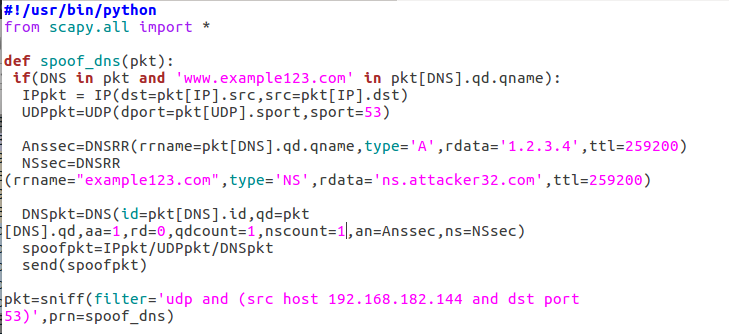


伪造了[www.example123.com](http://www.example123.com) 这个不存在于缓存的地址，当用户机dig这个地址，dns服务器会去询问，而攻击机趁此机会污染dns服务器。

Task7







通过对方访问的某个网站的时机，污染dns的对应authsec，通过抓包可以看出本地dns服务器已经去查询对应网址，我们的程序伪造报文让本地dns服务器相信并写入cache，完成攻击。