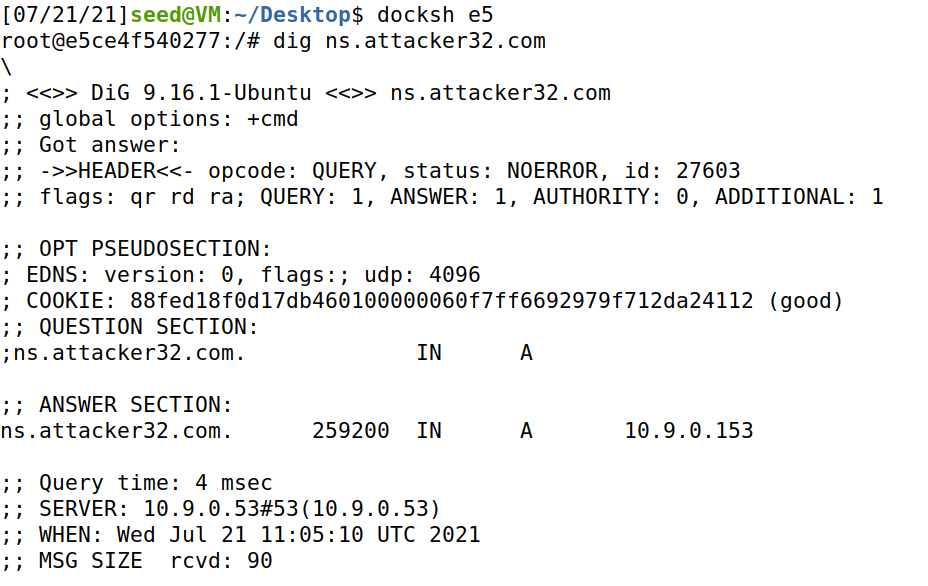
**Local DNS Attack**

姓名：齐天一　学号：57118223

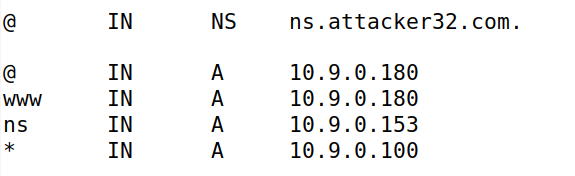
**Testing the DNS Setup**

**Get the IP address of ns.attacker32.com**

使用挖掘命令dig ns.attacker32.com 查询该域名的地址

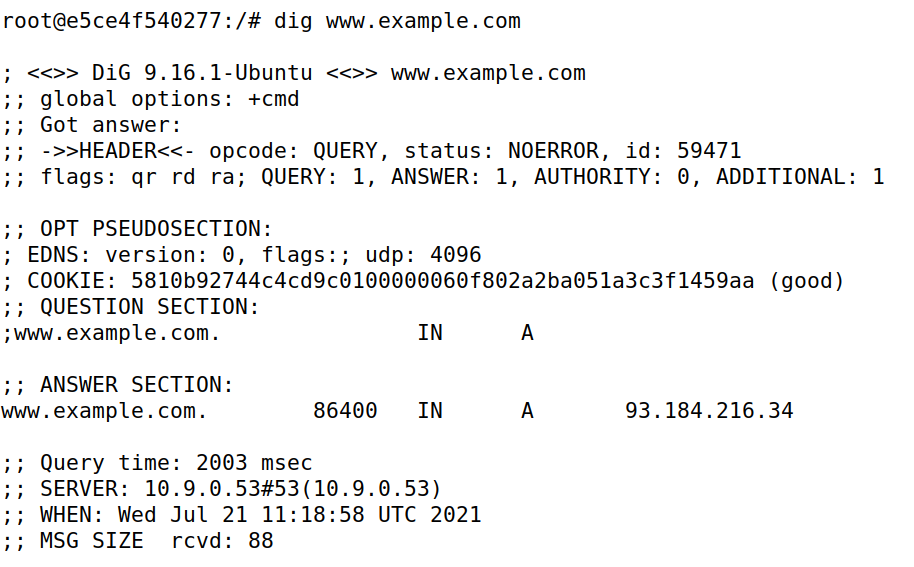


ns对应的ip为10.9.0.153



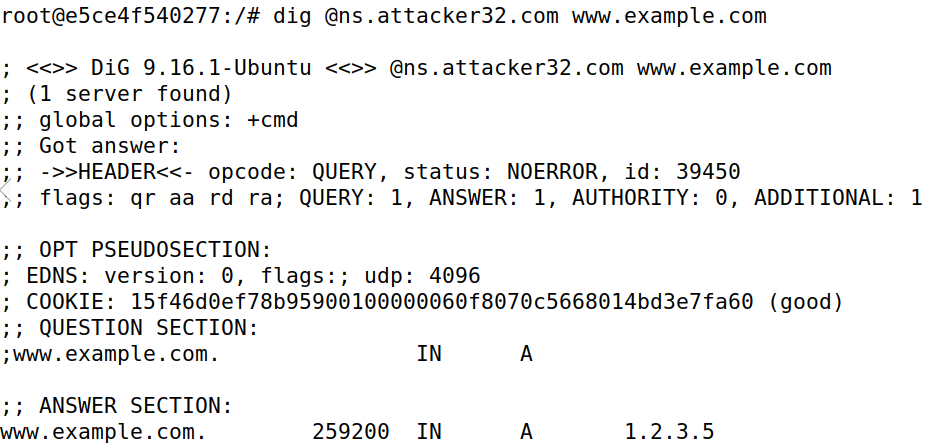
**Get the IP address of www.example.com**

使用dig [www.example.com](http://www.example.com) 查询ip

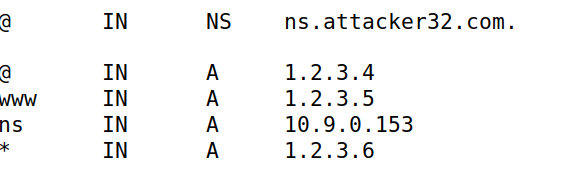


可以看到域名是真实域名，因为是从官方的域名服务器获取的域名。

使用dig @ns.attacker32.com [www.example.com](http://www.example.com查询ip)

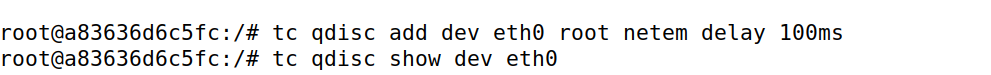


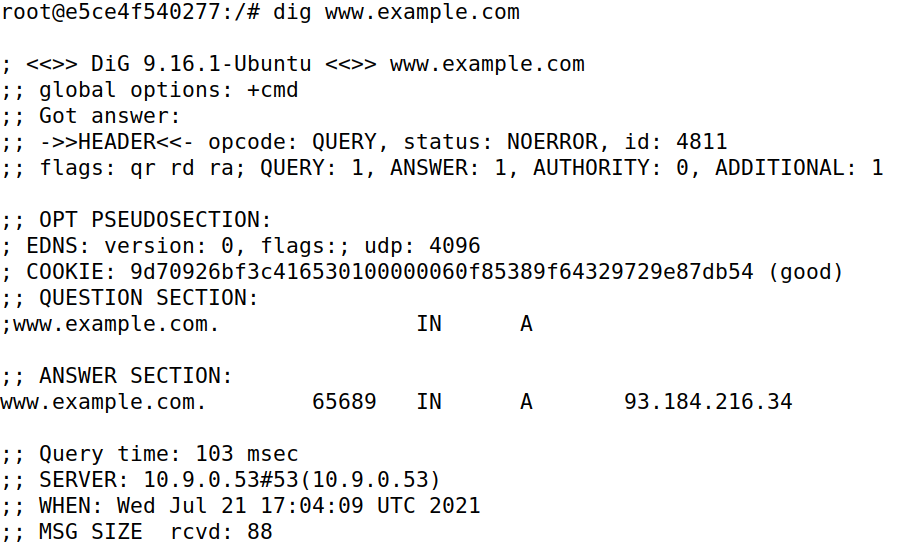
查看配置文件，可以看到攻击成功，ip地址变成了攻击者所设定的值



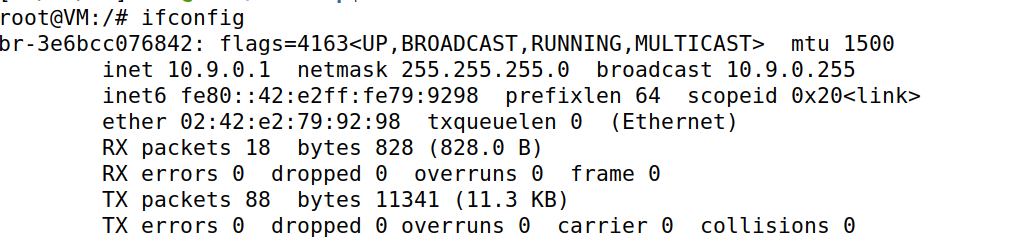
Task 1:

①在正常情况下，在用户主机输入指令查找域名对应的ip，得到正常的ip

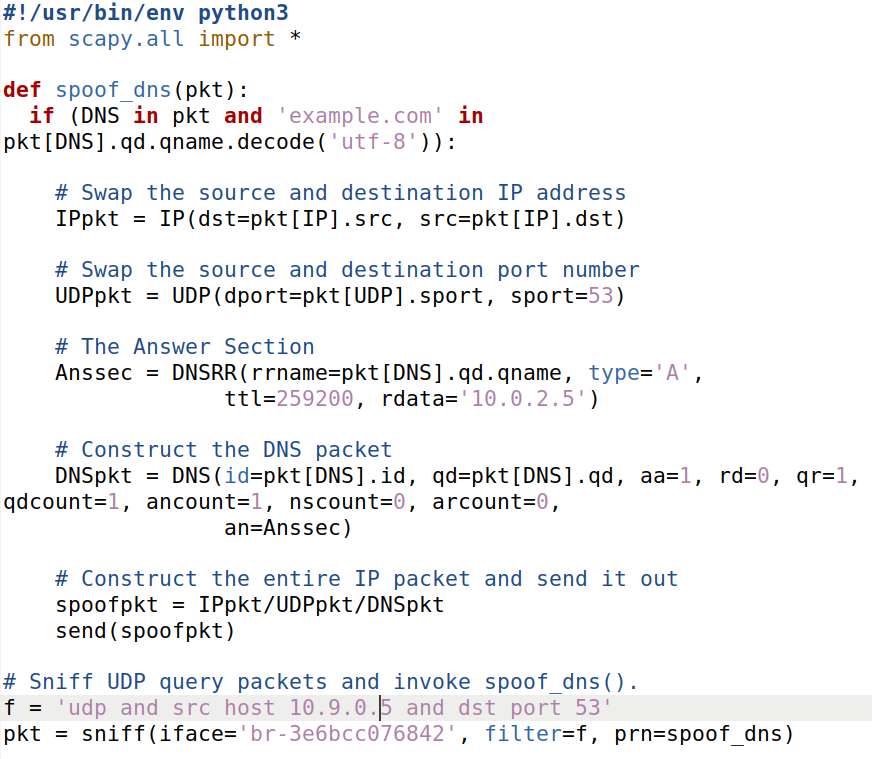




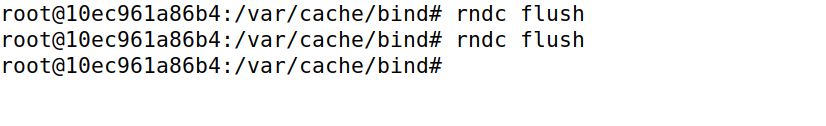
②在攻击者容器查看10.9.0.1对应的端口

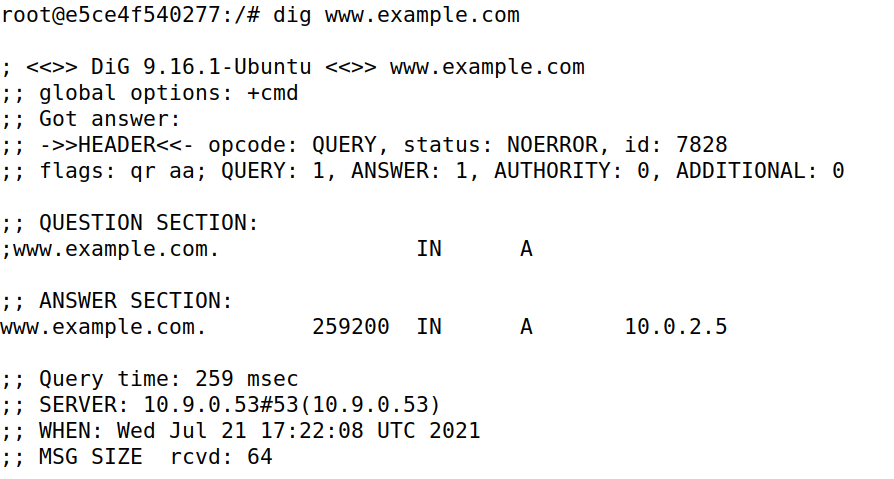


构造攻击程序如下，其中端口修改为10.9.0.1对应的端口，并修改过滤策略，使其只接收来自10.9.0.1的报文：

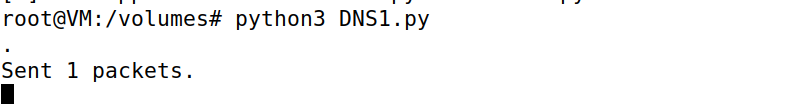


③在路由器容器清除缓存

④在攻击者容器运行程序，同时在用户容器重新输入dig www.example.com查看ip



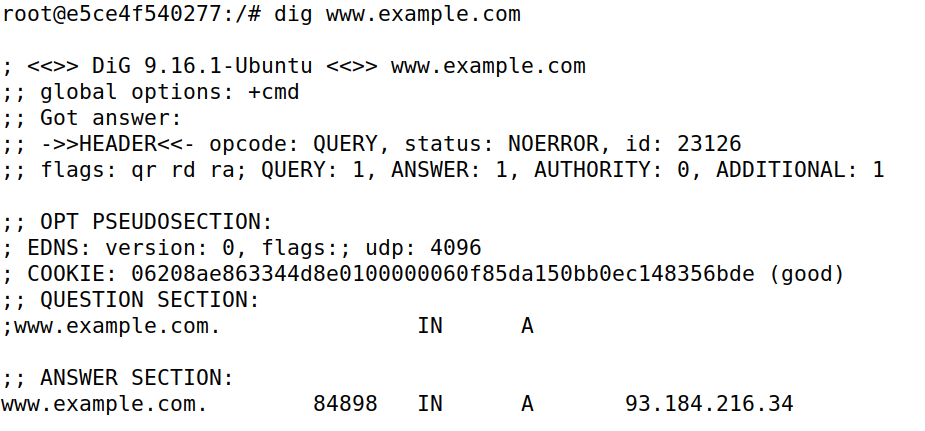
可以看到域名对应的ip被修改为攻击者设定的ip，说明攻击成功。



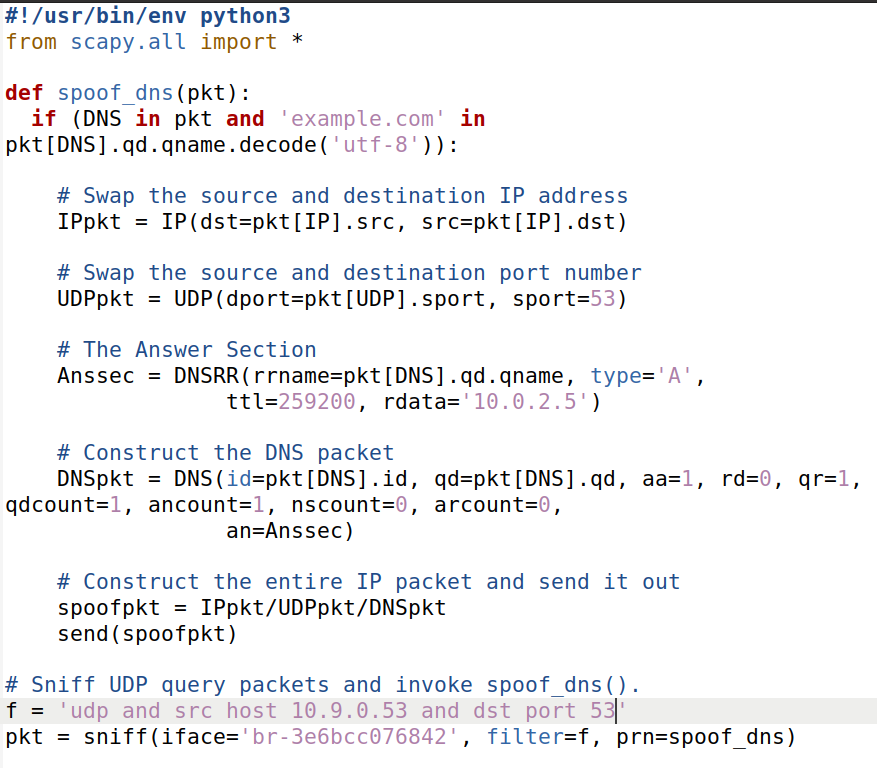
查看攻击者容器，可以看到发送了一个包，这个包就是伪造的DNS响应报文。

Task2：

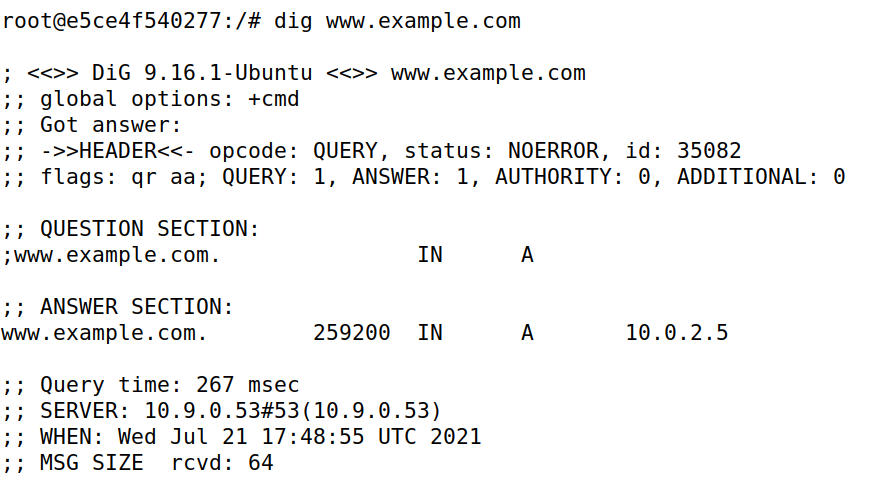
①攻击开始前，查看该域名对应的ip，显示正常



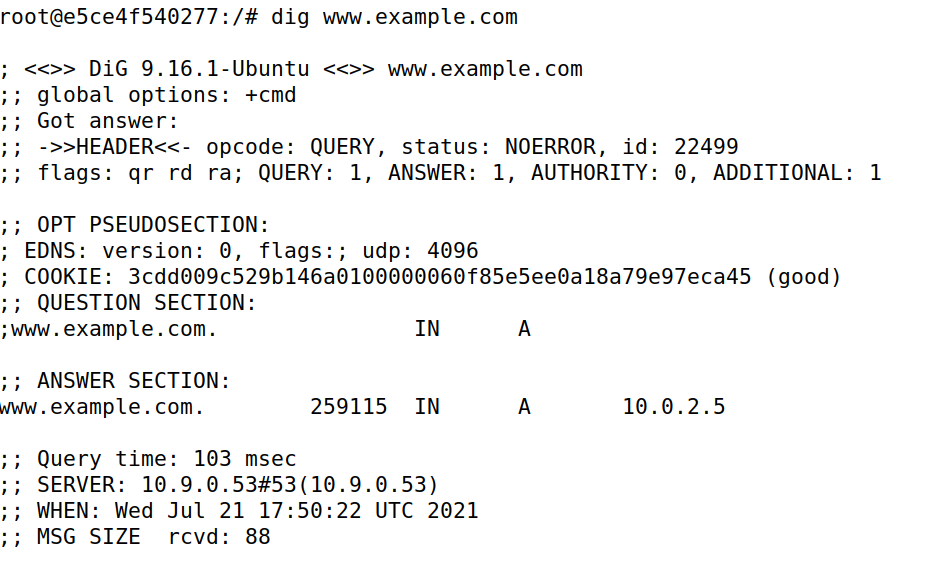
②构造程序如下，相较于task1修改了过滤器，使得程序能够筛选出来自本地域名服务器（10.9.0.53）的报文。



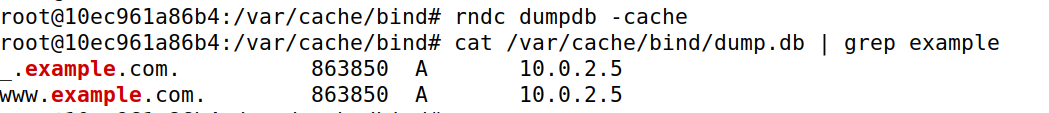
③攻击时使用dig [www.example.com](http://www.example.com端口) 查看ip地址，可以看到被修改了



④关闭攻击程序，并再次使用命令查看ip，可以看到仍然是修改后的结果，说明伪造的域名地址已经存在于本地dns域名服务器的缓存中了。



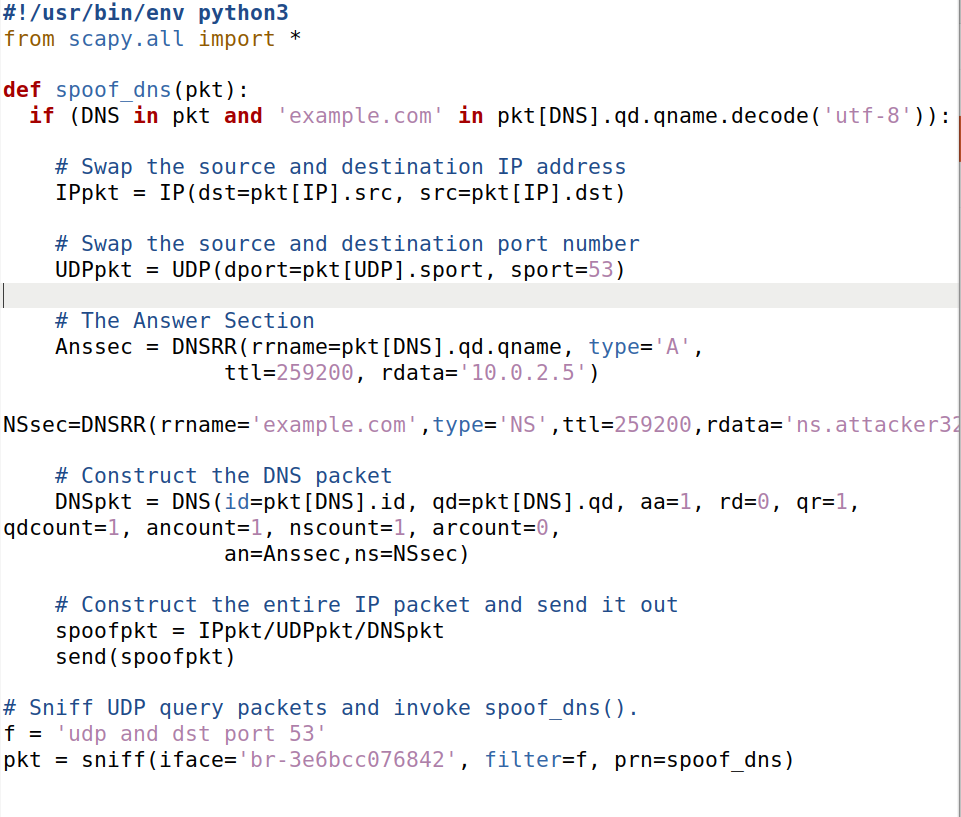
查看本地DNS服务器缓存



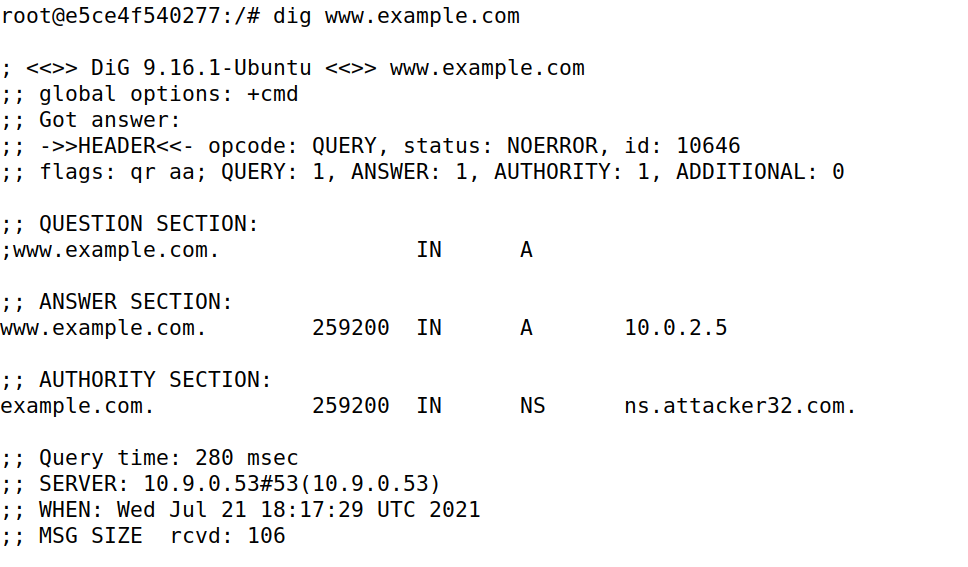
可以看到example对应的ip为10.0.2.5，证明了成功在DNS服务器中留下了错误的缓存。

Task3：

①构造攻击程序如下，其中添加一条NS记录，当服务器或用户将其存入缓存，就会将攻击者域名服务器用作名称服务器，从而向其查询域名。

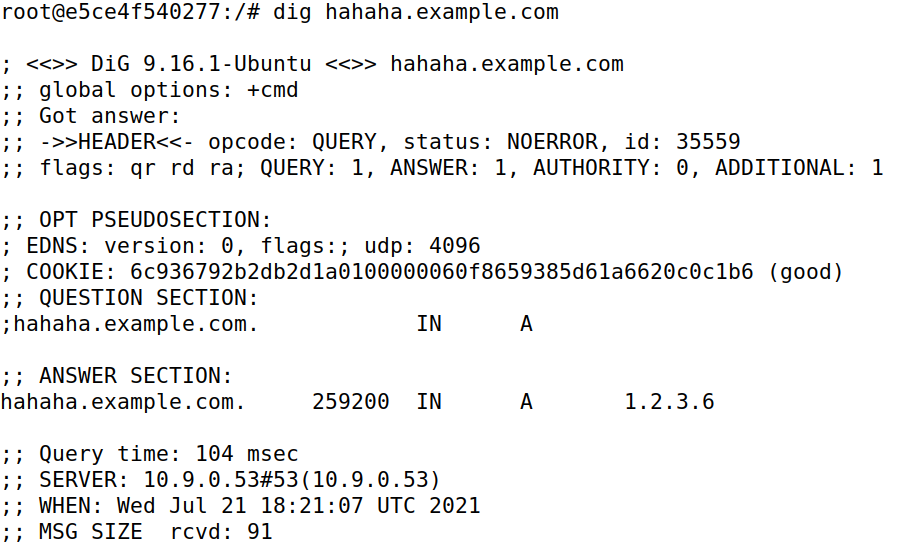


②运行程序，同时使用dig查看域名对应ip

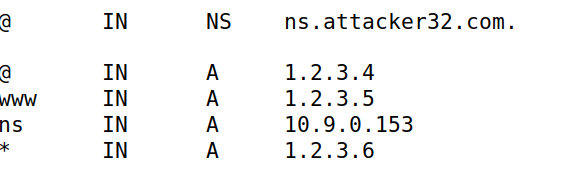


可以看到该地址对应的域名就是攻击者的域名。

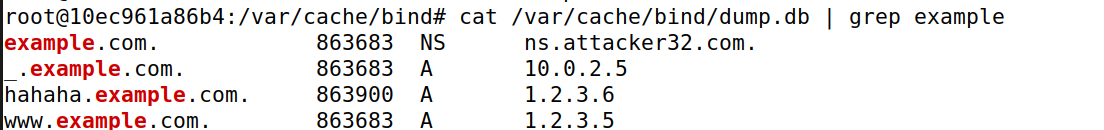
③使用dig指令查看一个不存在的域名



可以看到，域名被解析为1.2.3.6。可以看到在攻击者容器中，“其它域名”的ip对应1.2.3.6，hahaha.example.com属于这一类，说明攻击成功，域名被解析为攻击者服务器中的ip。

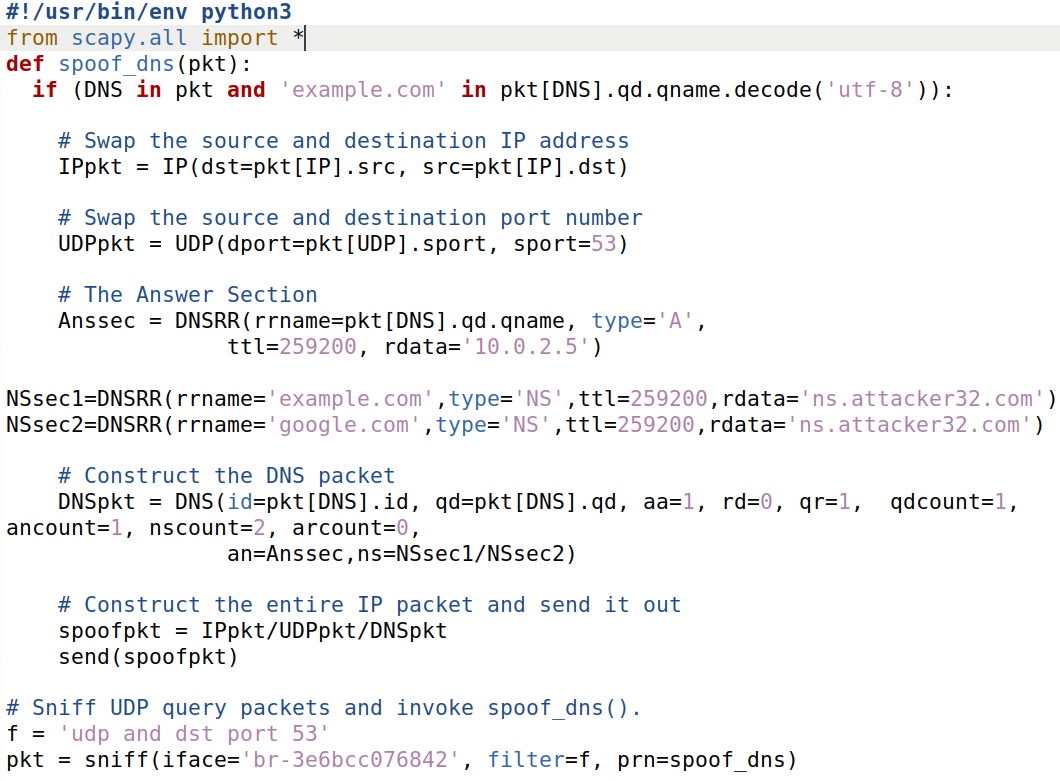


查看DNS缓存，可以看到，该域名成功被解析为攻击者制定的ip

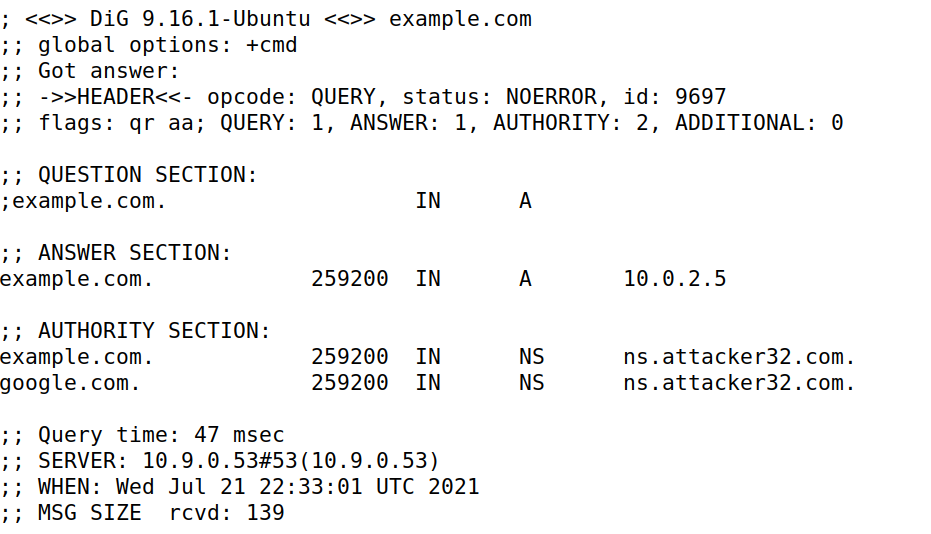


Task4：

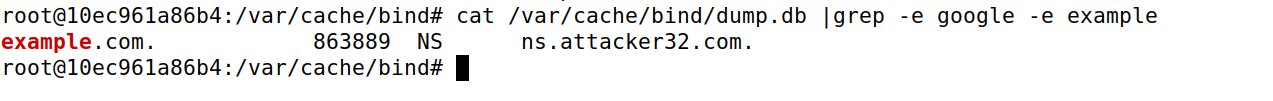
①构造攻击程序，新增一条NS记录，并添加到报文

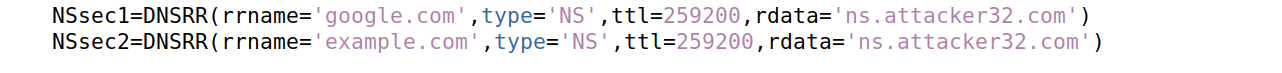


②使用dig example.com指令查看，效果如下：

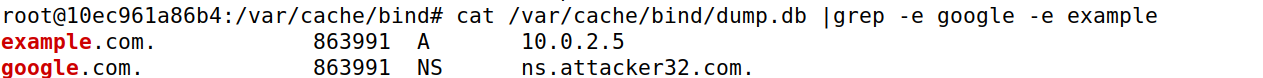


③在本地路由器查看缓存，可以看到新增一条记录，是关于example.com的，但没有google.com的记录



④在攻击程序中调换两个域名位置  


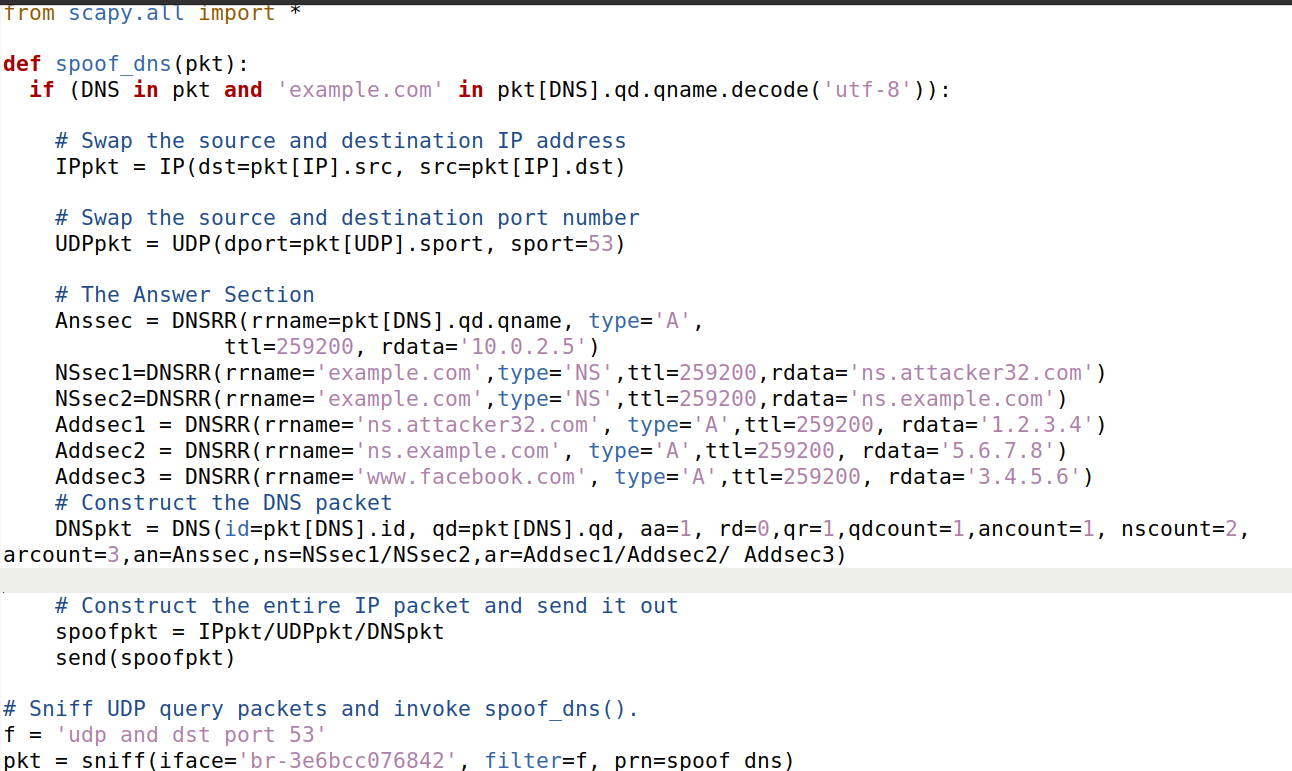
清空缓存后，重新实验，并查看缓存记录



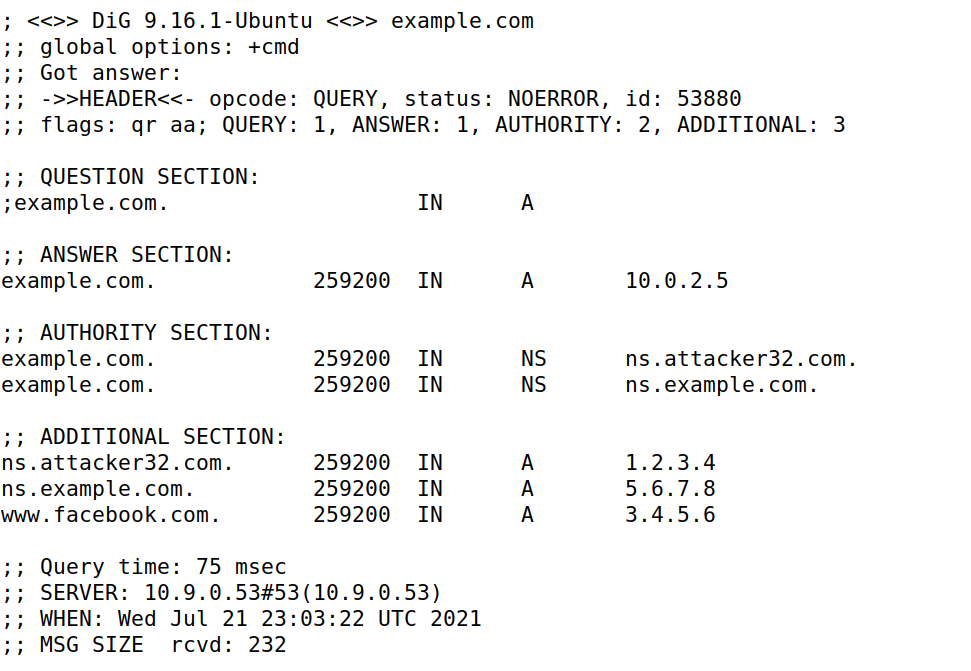
客户以看到出现了google.com的NS记录，而example.com则是A记录，说明缓存只保存一个NS记录且是第一个记录。

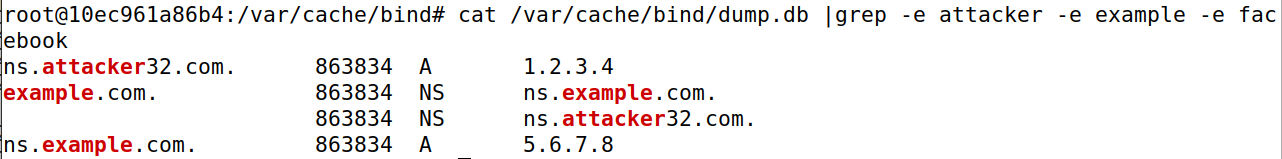
Task5：

①构造攻击程序，添加三条附加字段内容，同时将数目设为3.



②运行程序，使用dig example.com查看ip，可以看到附加的内容

  
③查看DNS缓存



可以看到example和attacker的缓存，而没有看到facebook网站的域名，这是因为其没有出现在权威字段的条目中。