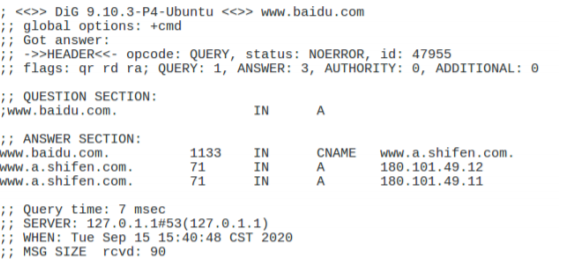
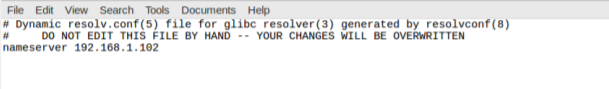
**Local DNS Attack Lab**

**Task1**

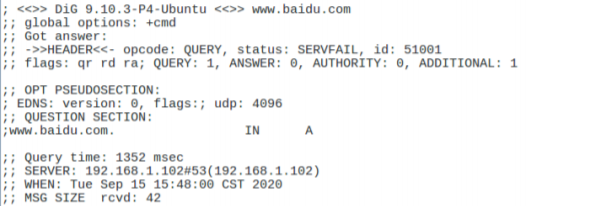
DNS 服务器所在虚拟机 IP 为 192.168.1.102，为一台普通 ubuntu16.04 用户虚拟机为 192.168.1.104，为一台 securityonion 修改用户机的 DNS 服务器前：



修改相关配置，并且关闭 DNS 服务器上的 DNS 服务



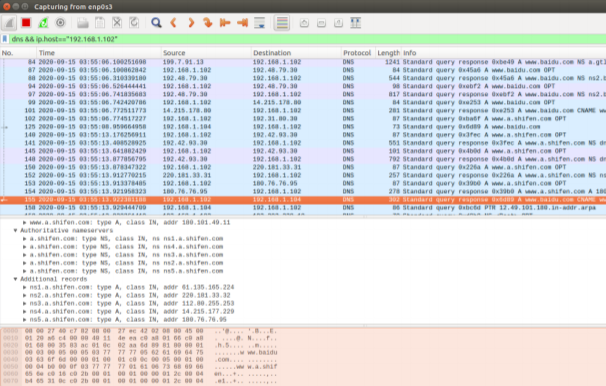
再次运行 dig 命令后，开启 192.168.1.102 上的 DNS 服务后再运行：



可以看到 SERVER 一项是 192.168.1.102

**Task2**

启动第三台虚拟机（seed）IP 为 192.168.1.107，这是以后攻击发起的虚拟机，也是 wireshark 进行观察的虚拟机 我们清空 DNS 服务器的缓存。 在用户虚拟机上 ping 百度的域名：



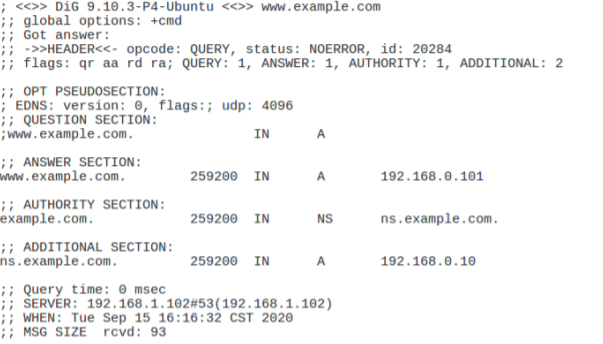
现在有了缓存之后，次 ping 一次：



只有两次交互，只发生在用户虚拟机和本地 DNS 服务器虚拟机之间，分别为请求域名和反向请求

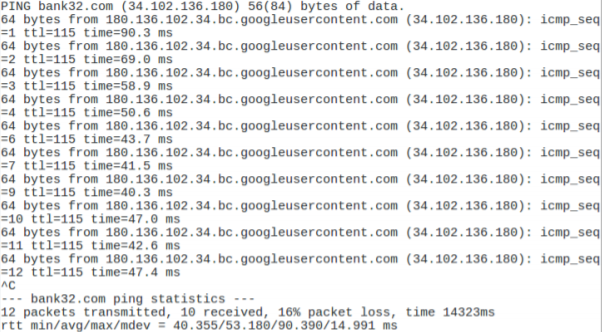
**Task3**

设置好各项文件后，结果如下：

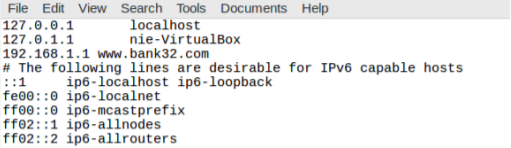


**Task4**

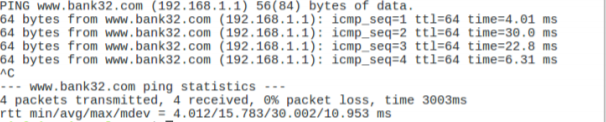
在修改用户虚拟机的 host 文件前：



可以看到是某国外 IP 修改/etc/host

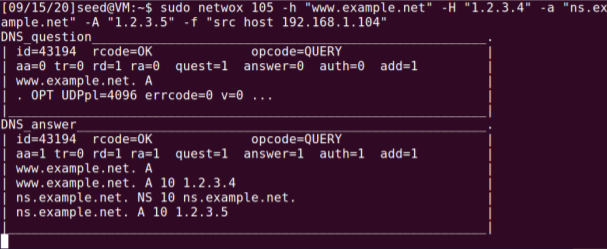


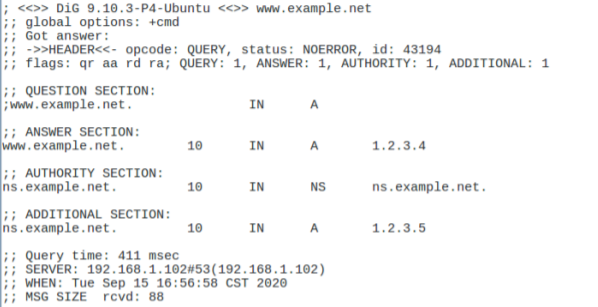
把这个域名绑定到网关上



**Task5**

命令和执行结果如下：



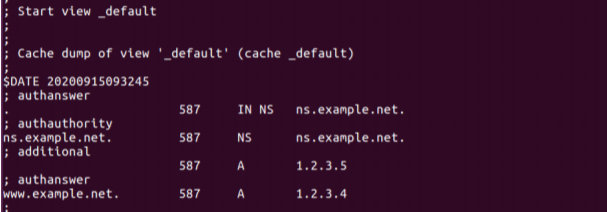


**Task6**

首先清除 DNS 服务器上的缓存 攻击者命令如下：

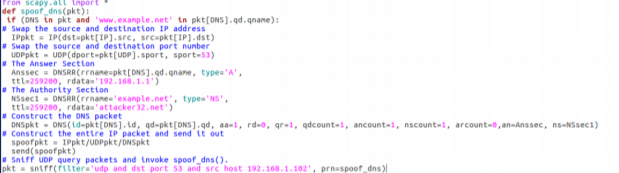


查看本地 DNS 服务器缓存：



**Task7**

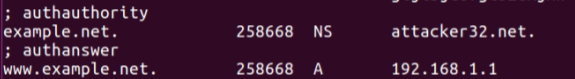
程序如下



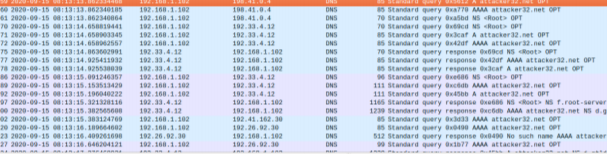
清空 dns 服务器缓存之后，用户机请求 [www.example.net](http://www.example.net):



查看 dns 缓存;



然后用户机对 mail.example.net 进行查找：

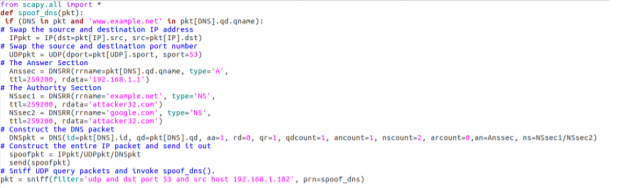


可以看到有对 attacker32.net 发起的查找 （指导手册里是 attacker32.com，最后才注意到，不过应该不影响）

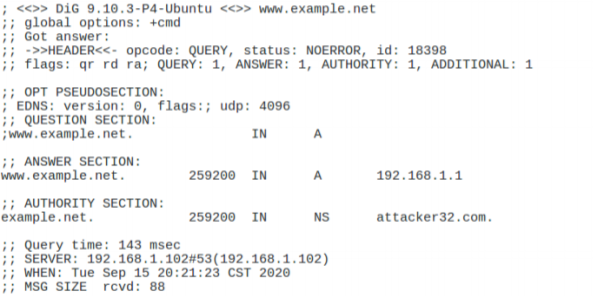
**Task8**

首先清空 dns 缓存

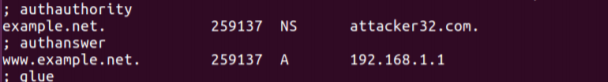
程序如下



用户机查询 [www.example.net](http://www.example.net)



查看 dns 缓存：



可以看到，NS 项的 google.com 项没有被缓存，被忽略了。