实验二:dns劫持验证

首先伪造一份用于dns劫持的dns资源记录。

gedit /etc/bind/db.google.com

将[www.google.com](http://www.google.com)劫持到baidu.com(220.181.57.217)写入文件：

$TTL 604800

$ORIGIN google.com.

@ IN SOA ns1.google.com. ns2.google.com.(

1 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

@ IN NS ns1.google.com. ; in the domain

ns1 IN A 220.181.57.217 ;web server definition

ns2 IN A 123.1.151.4 ;web server definition

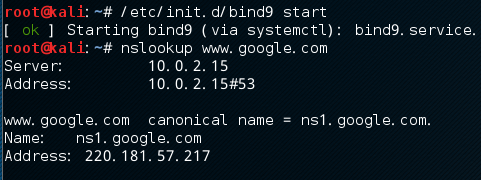
www IN CNAME ns1.google.com. ;web server definition

ftp IN CNAME ns2.google.com. ;ftp server definitionbox

之后，打开dns服务器，进行验证：

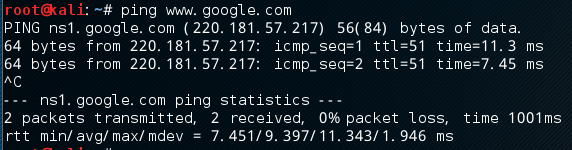
/etc/init.d/bind9 start

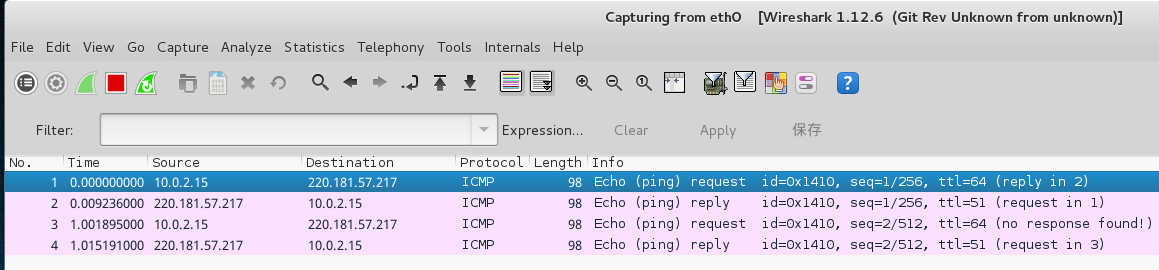
nslookup [www.google.com](http://www.google.com)



确认[www.google.com](http://www.google.com)已被劫持。

打开wireshark，同时ping目标网址，进行抓包验证：





结果成功将本应发送给[www.google.com](http://www.google.com)的包发给了baidu.com，dns劫持成功。