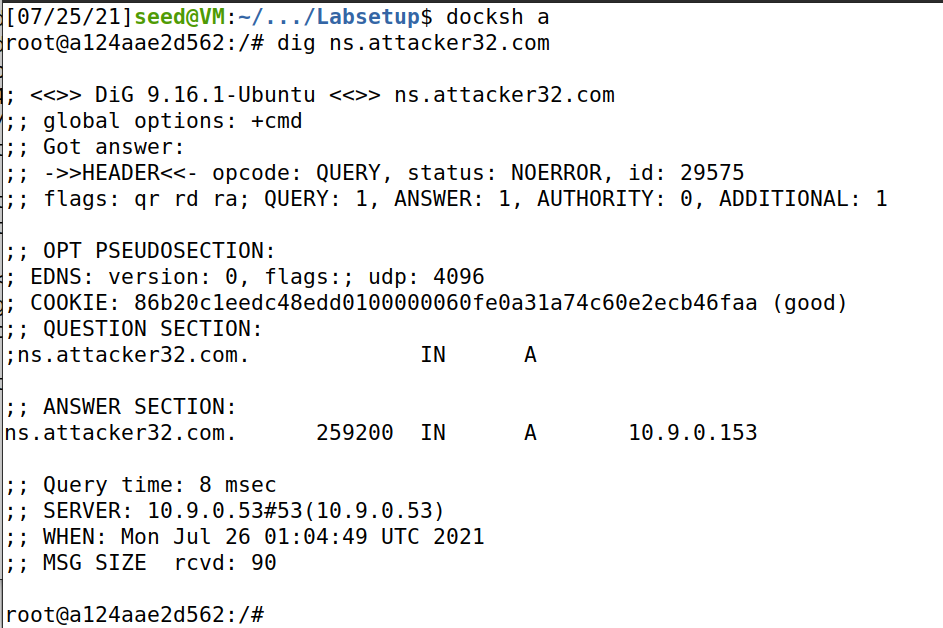
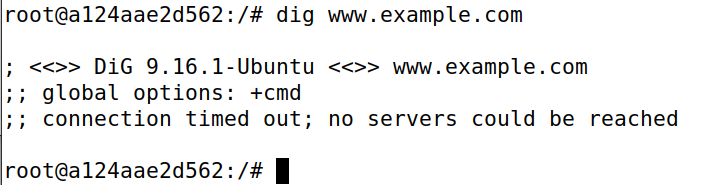
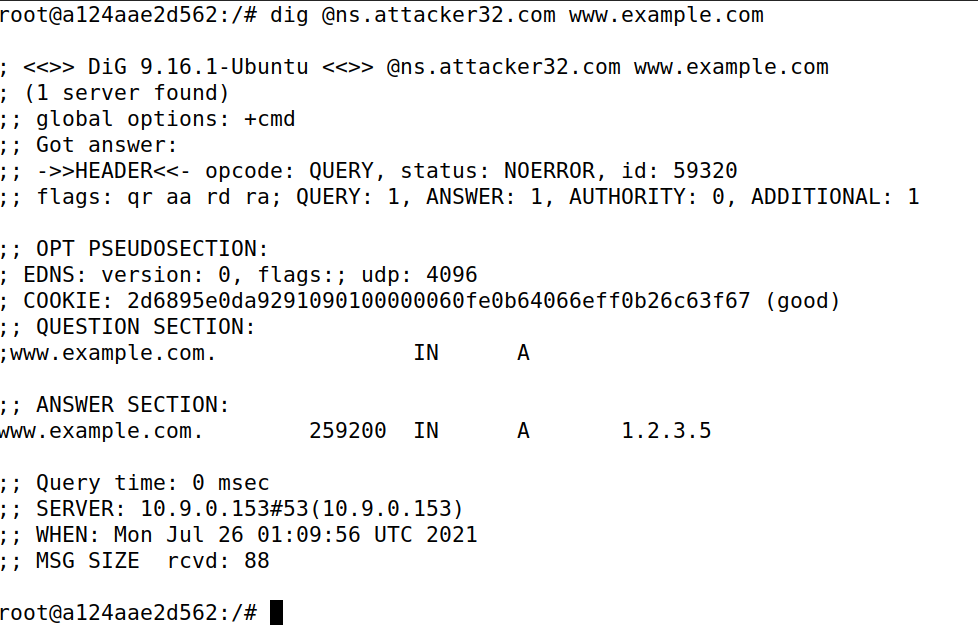
测试设置，发现符合对于本地DNS解析和恶意解析服务器的设置

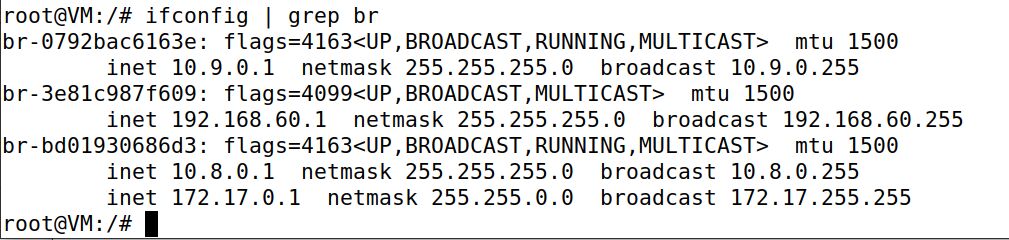




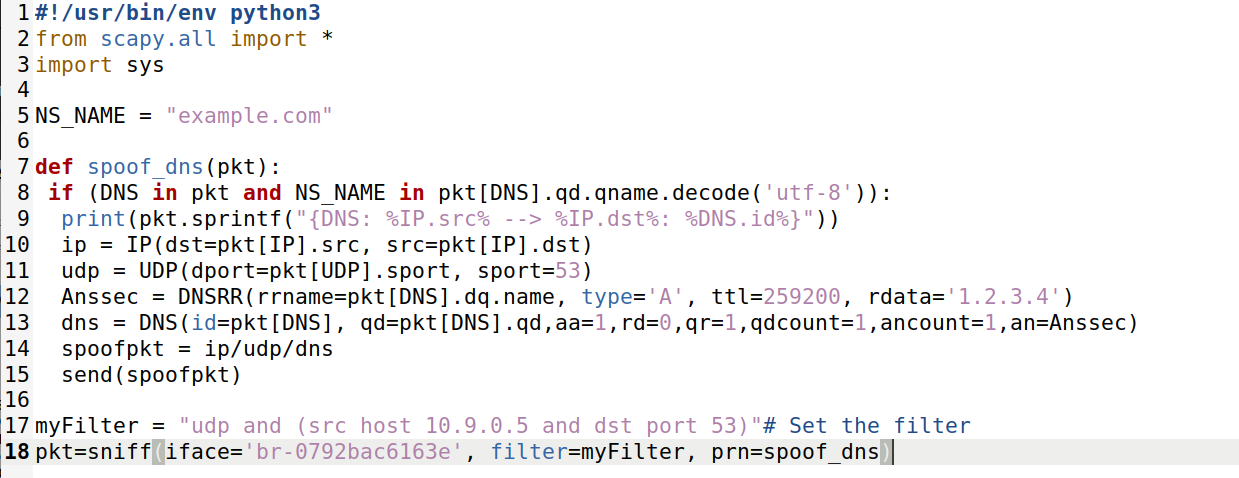


Task1: Directly Spoofing Response to User

查看端口号

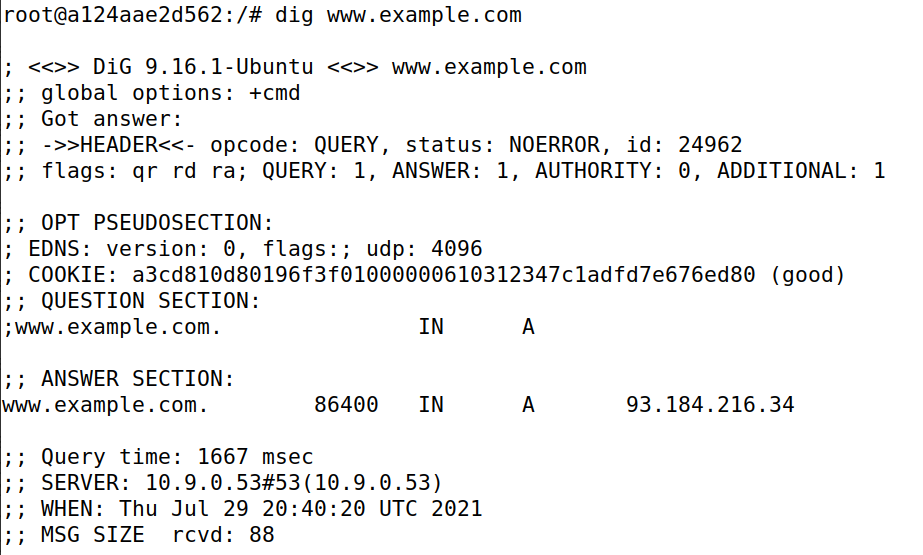


在 attacker 上编写脚本如下：



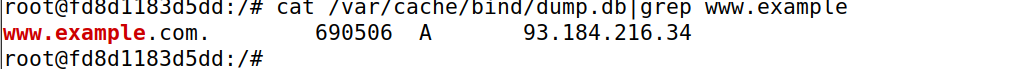
在 attacker 上运行脚本

在 user 上再次运行 dig www.example.com 命令 ，可见地址已被解析为 1.2.3.4

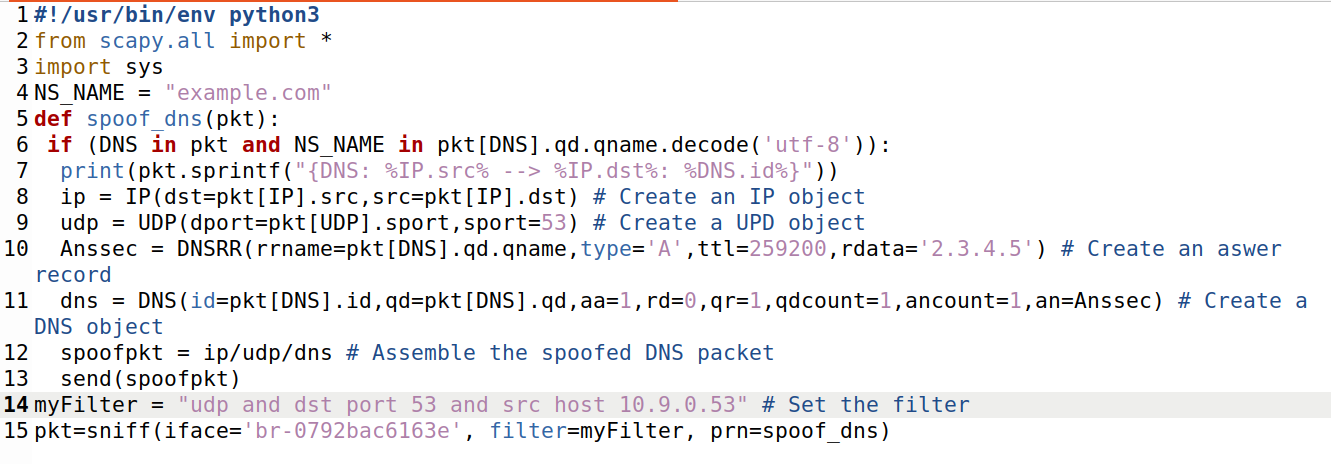


Task2

服务器的初始缓存

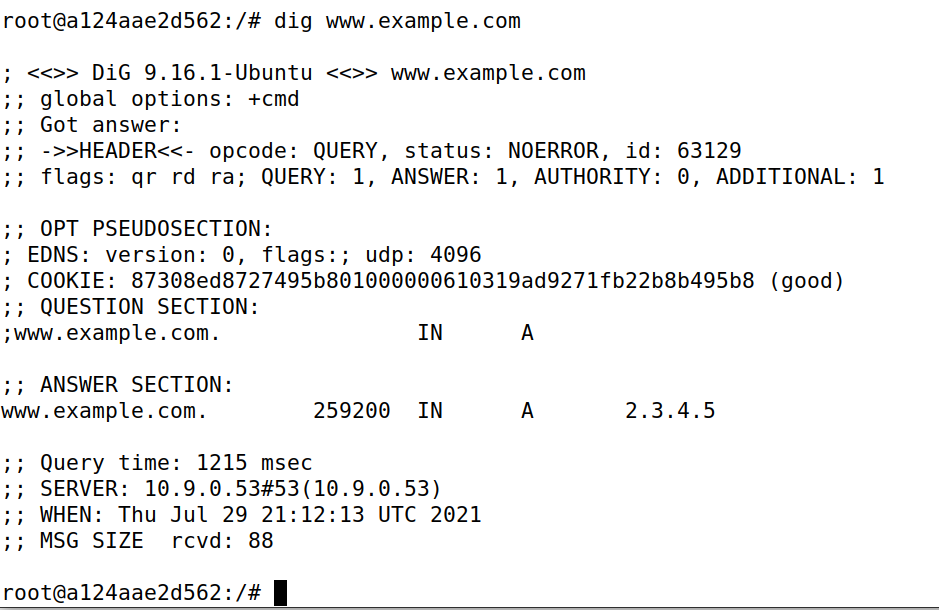


代码如下

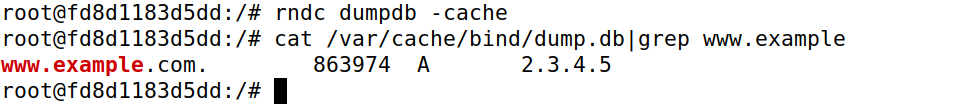


在attacker上运行攻击程序

解析更改成功

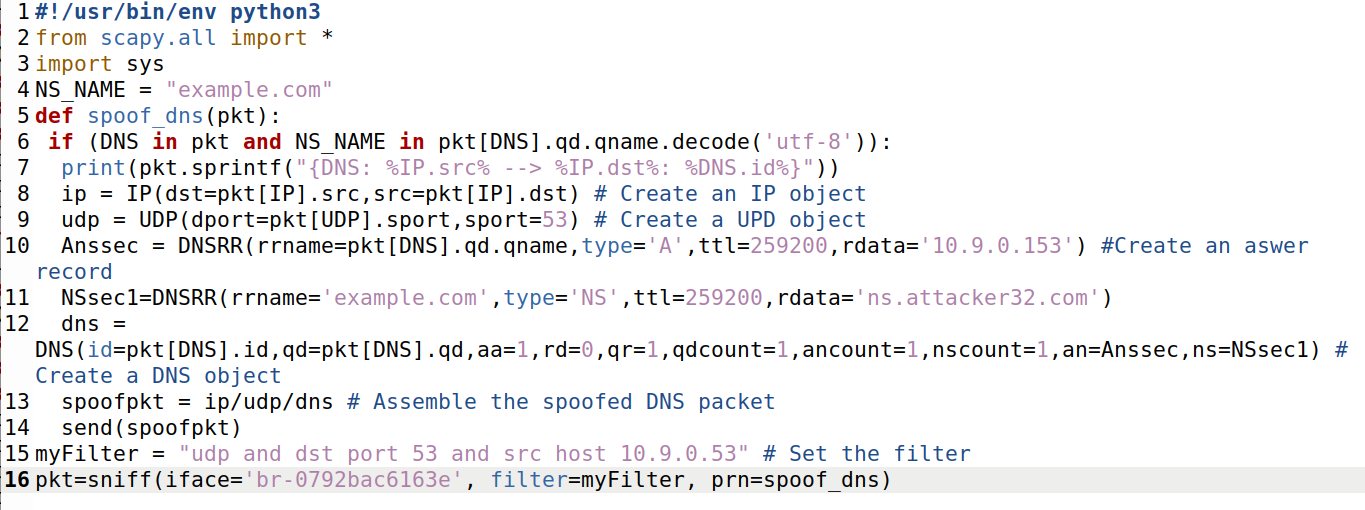


dns服务器中被污染

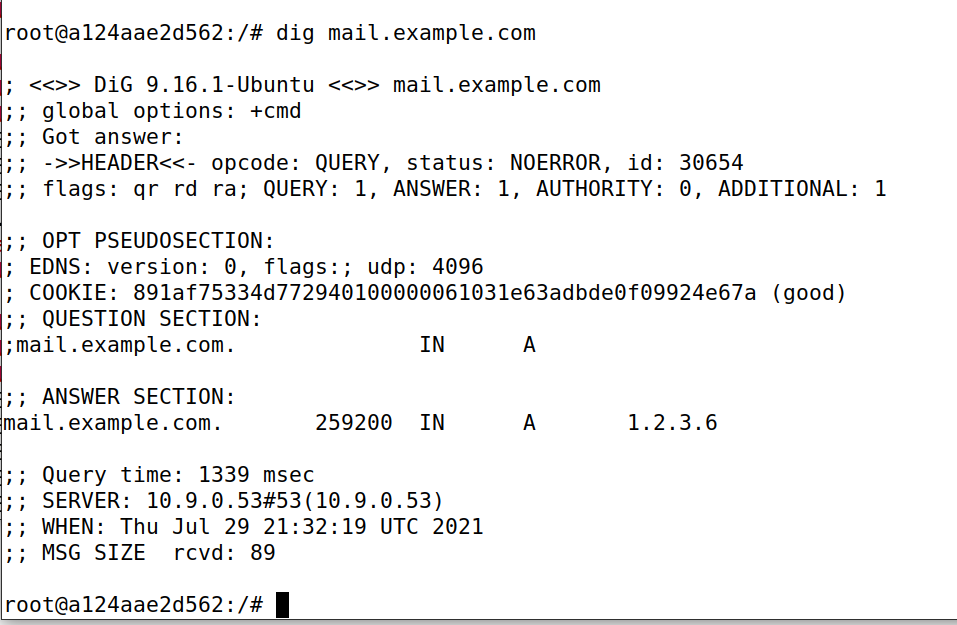


Task3

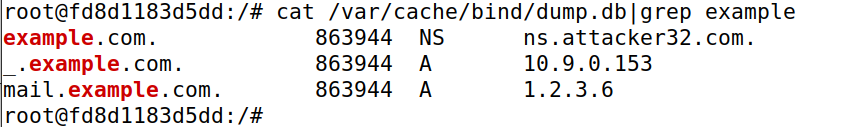
修改代码如下



dig 得到如下结果，www.example.com 被解析到了 1.2.3.6

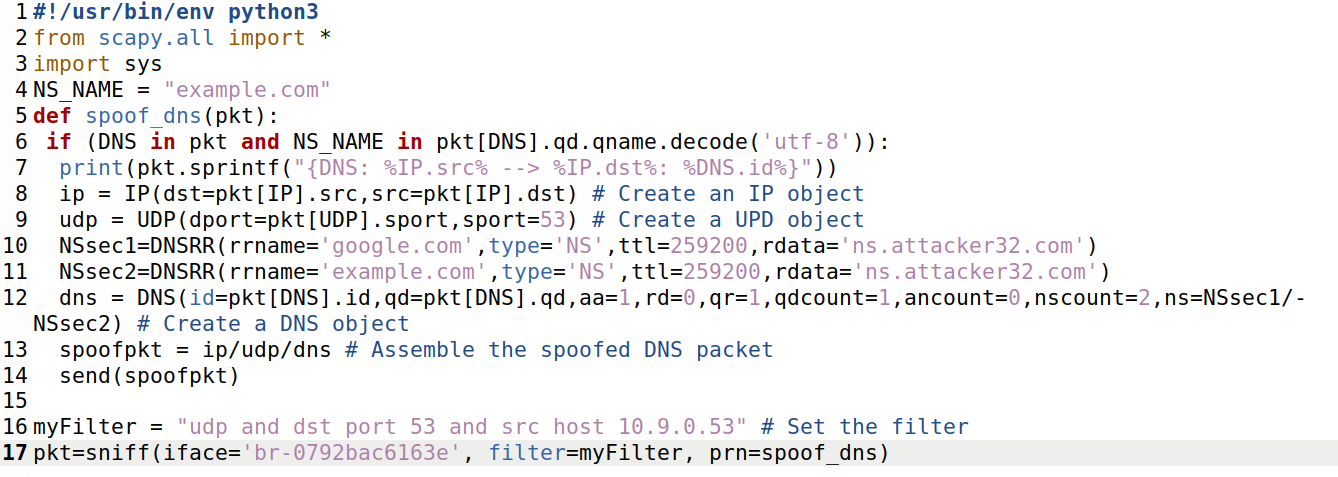


服务器已经把 ns.attack32.com 作为了 example.com 的 DNS

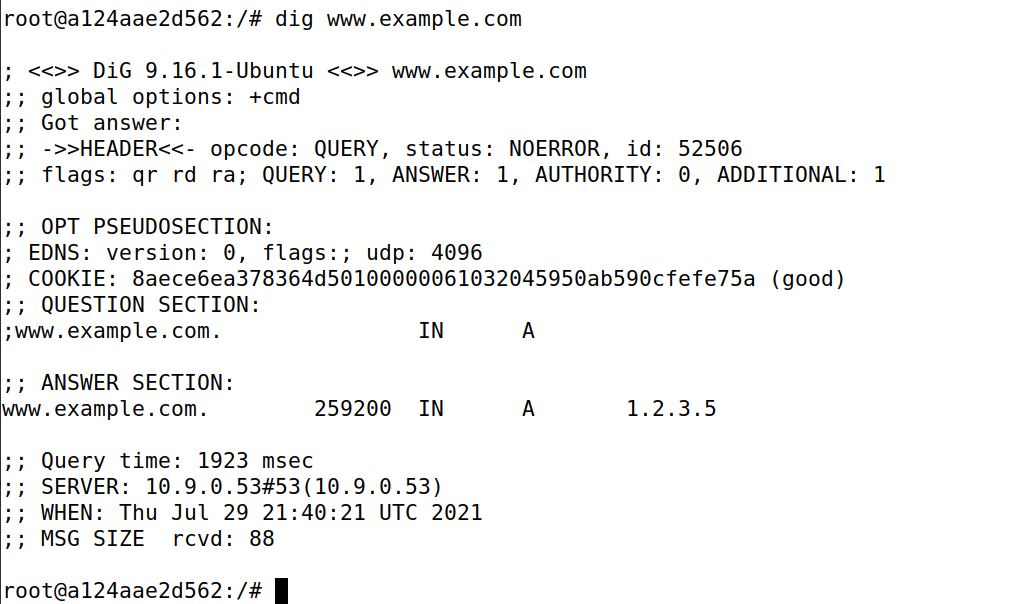


Task4

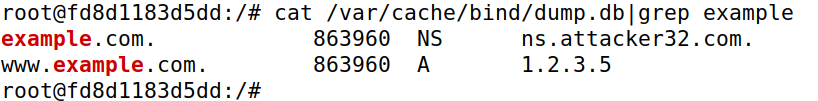
修改代码



dig 得到如下结果，www.example.com 被解析到了 1.2.3.5



服务器已经把 ns.attack32.com 作为example.com 的 DNS。



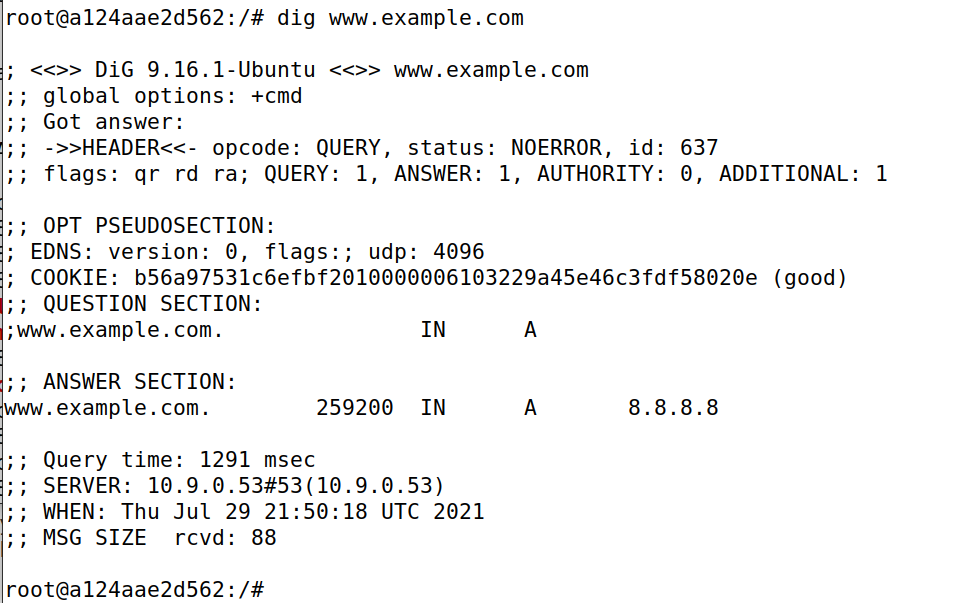
查询google失败



Task5

代码修改如下

运行代码，dig结果如下



本地缓存如下

