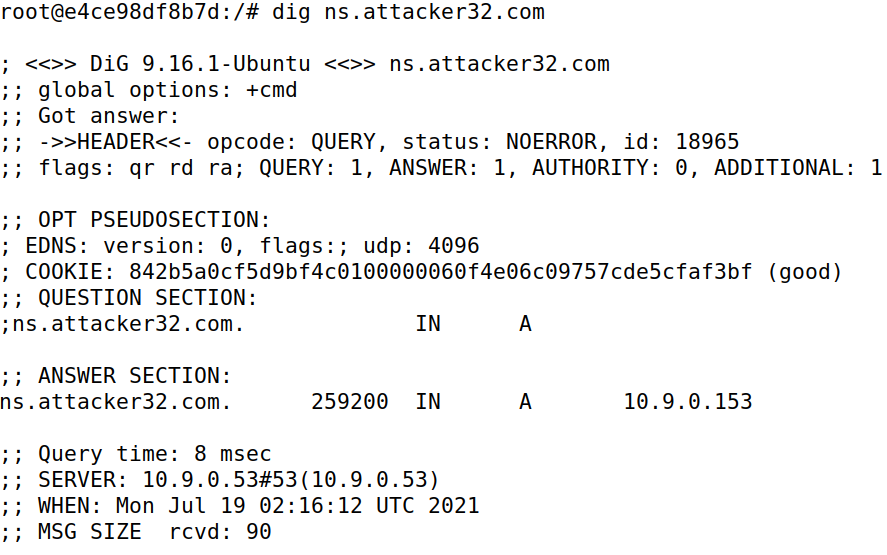
**Lab[5] report**

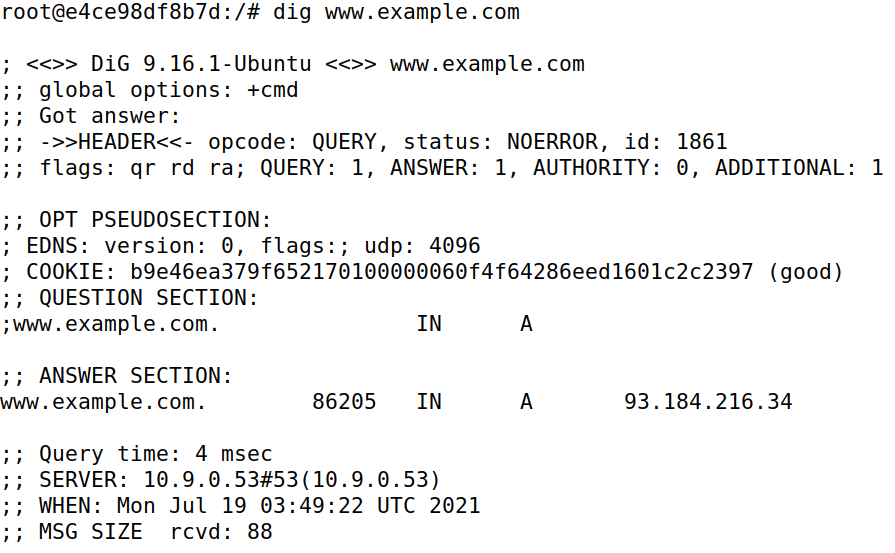
**57118120 黄逸飞**

**#Testing**

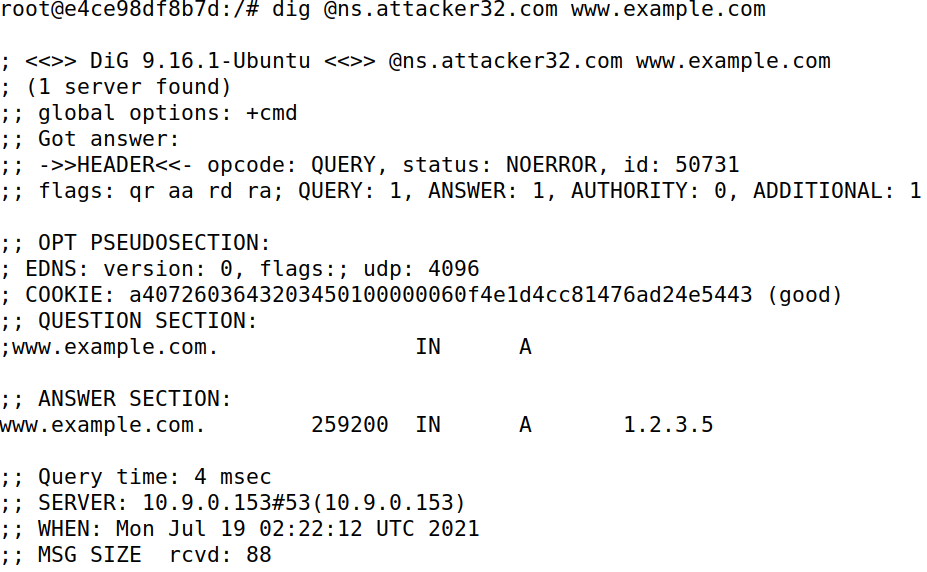
**Dig attacker32.com,正常从attacker获得ip**

****

**Dig** [**www.example.com**](http://www.example.com)**,联网后从外获得了ip**

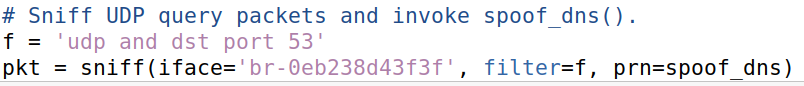
****

**从attacker处获得了ip，是假ip**

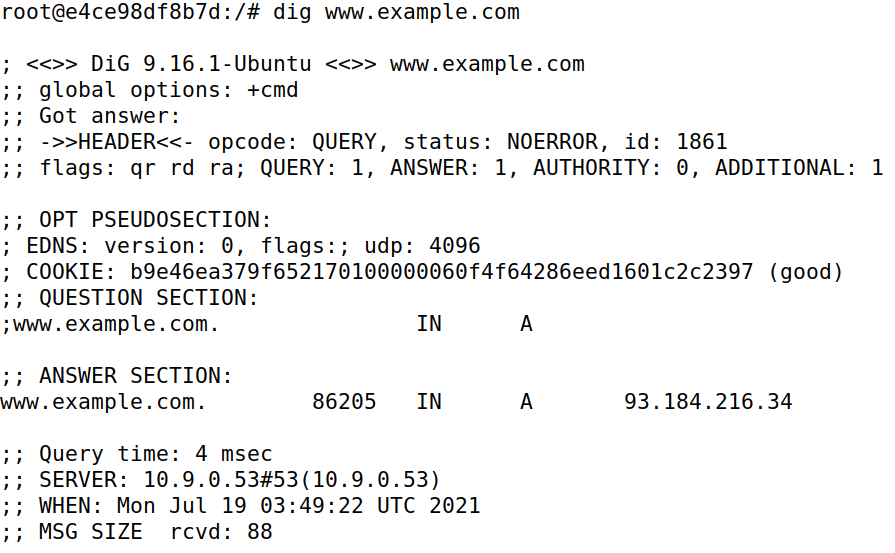
****

**Task1**

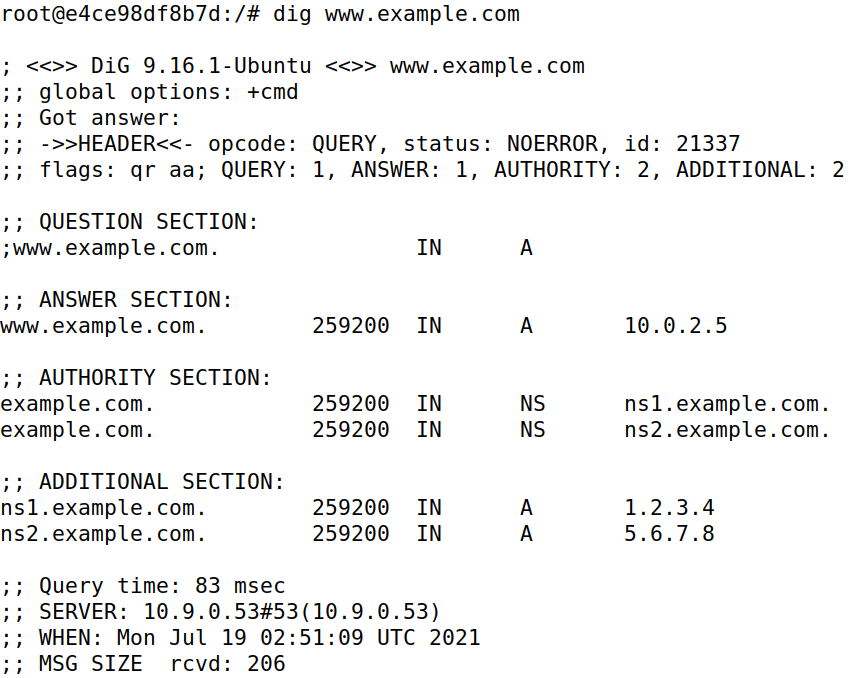
**将接口改为10.9.0.0段的接口**

****

**没有运行代码时dig**

****

**运行后dig**

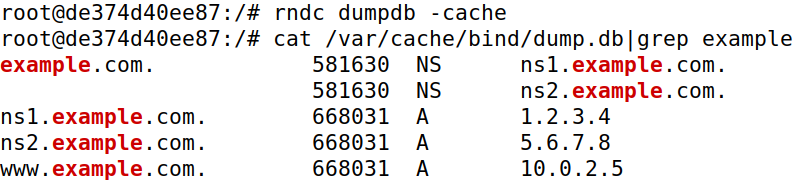
****

**Task2**

**代码：将接口换成10.8.0.0的**

****

**运行后dig，可以从dns服务器cache中看到有10.0.2.25的假ip（由于默认代码的其余代码没有删，有些和本题无关的东西）**

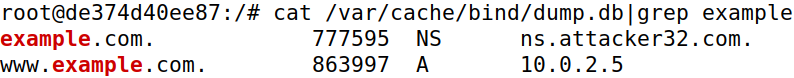
****

**Task3**

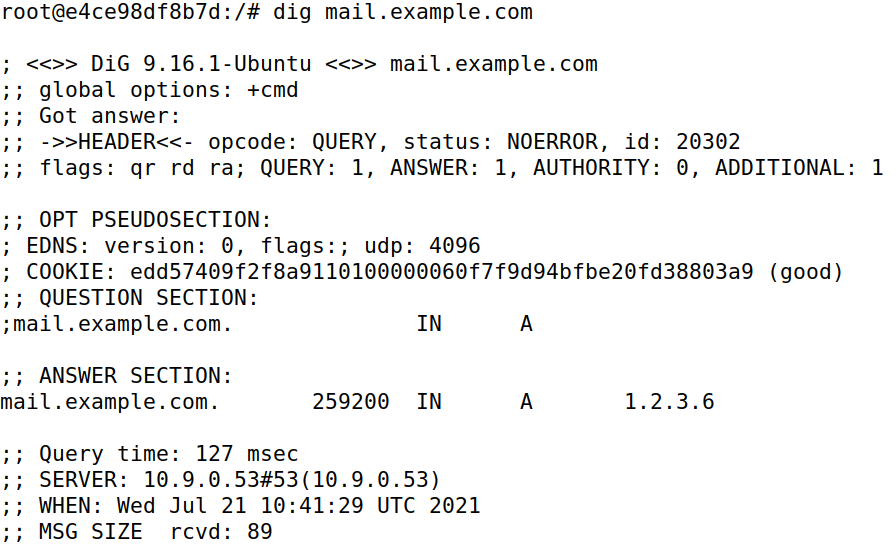
**代码中加入：**

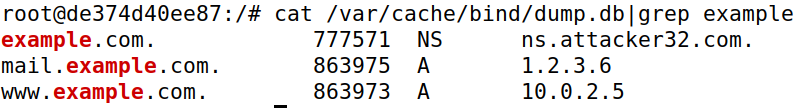
****

**运行代码并dig后可以在DNS服务器cache中看到：**

****

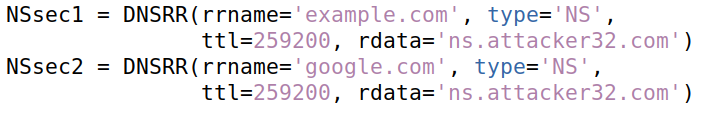
**在user中dig mail.example.com后可以看到获得了一个伪造的1.2.3.6**

****

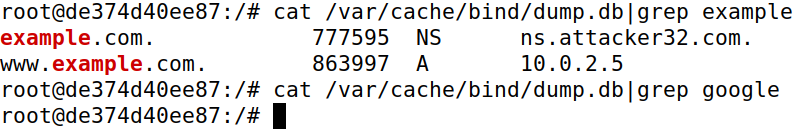
****

**Task4**

**代码中加入google.com的假权威服务器**

****

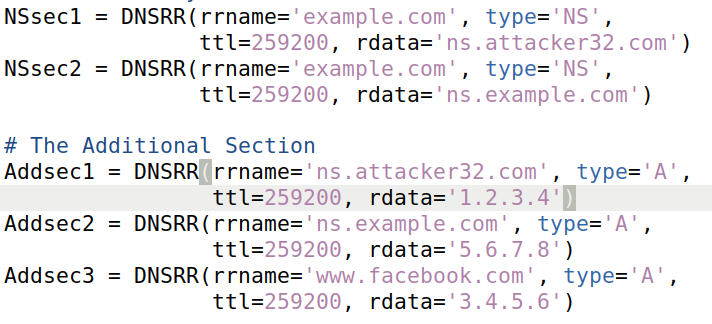
**结果中没有**

****

**DNS服务器会自己通过域名判断发过来的域名是否属于询问的域名，不是的话不加入cache**

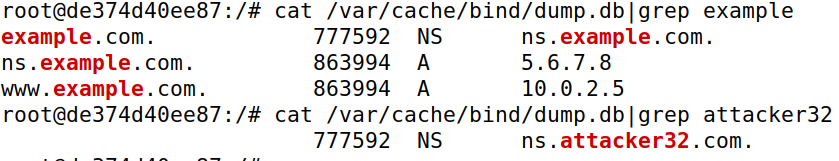
**Task5**

**代码如下**

****

**DNS服务器cache如下，其中example.com成功设置了两个权威服务器，ns.example.com也成功和ip5.6.7.8匹配**

****

****

**但是ns.attacker.com 和**[**www.facebook.com都没有成功和ip**](http://www.facebook.com都没有成功和ip)**匹配，看来DNS服务器只缓存带有询问的域名的服务器的IP，未询问的即使是询问的域名的权威服务器也不缓存。**