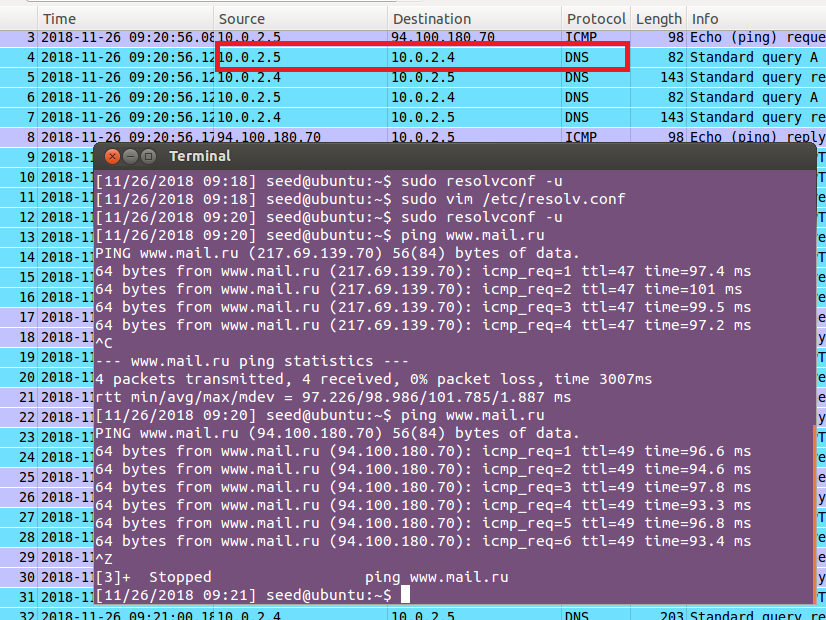
**Name: Alexey Titov**

Local DNS Attack Lab

Lab Tasks (Part I): Setting Up a Local DNS Server

* Task 1: Configure the User Machine & Task 2: Set up a Local DNS Server

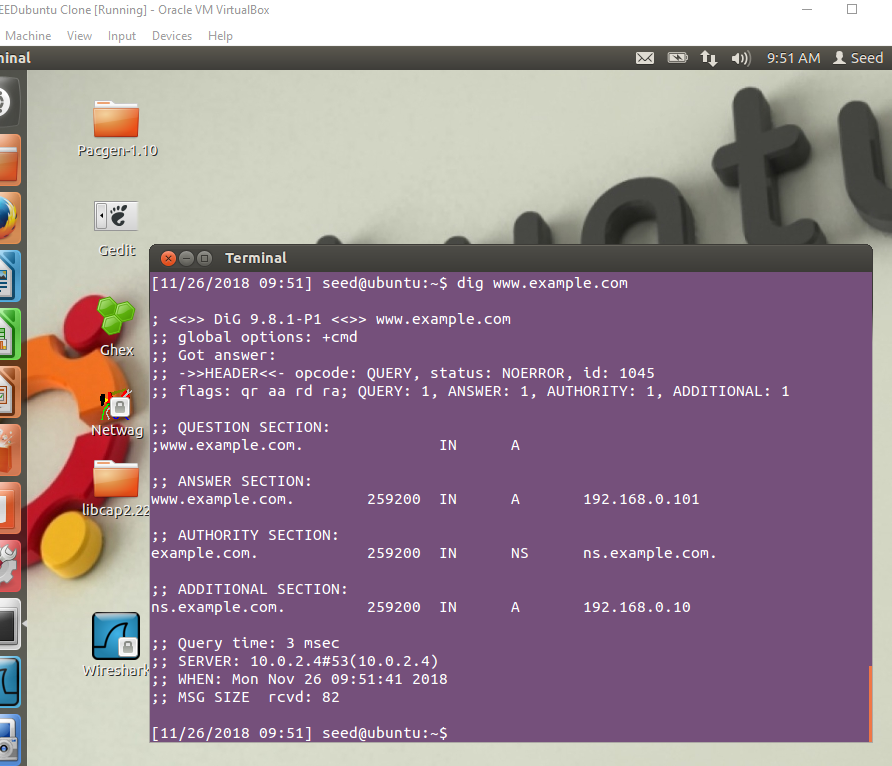


**Observation:**

* + User Machine: 10.0.2.5
  + Local DNS Server: 10.0.2.4
  + Attacker: 10.0.2.15

The user machine sends ping to www.mail.ru and receives the address of the site from Local DNS Server.

* Task 3: Host a Zone in the Local DNS Server

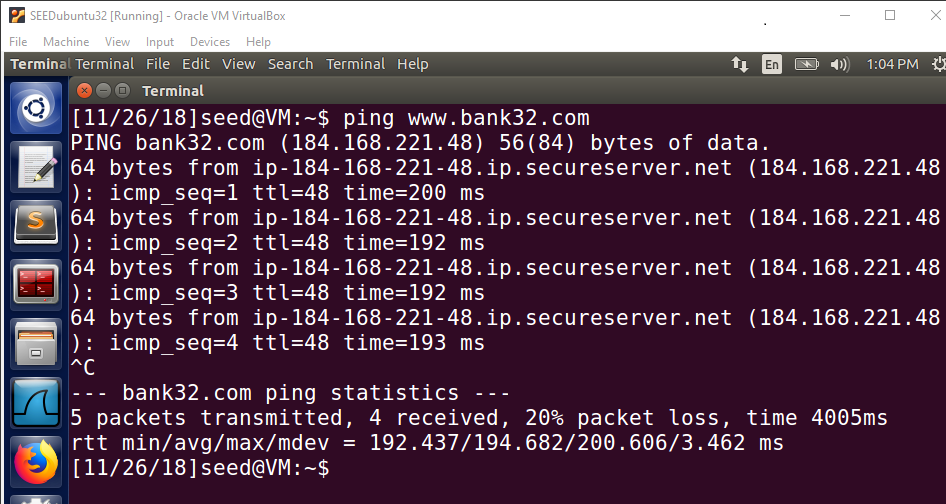


**Observation:**

On Local DNS Server we created zones “example.com” and “0.168.192.in-addr.arpa” and added contents to */etc/bind/named.conf*. The first zone is for forward lookup (from hostname to IP), and the second zone is for reverse lookup (from IP to hostname). We created these zones in the */etc/bind/* . So when User Machine executes the command *dig www.example.com* , he receives the answer that we writes in the zones created by us.

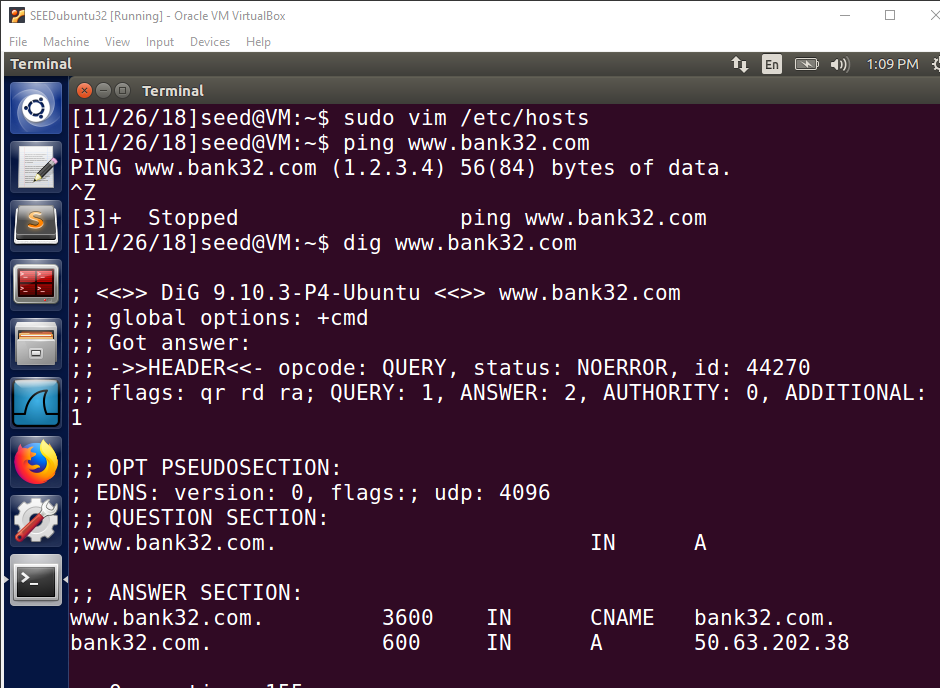
Lab Tasks (Part II): Attacks on DNS

* Task 4: Modifying the Host File



**Observation:**

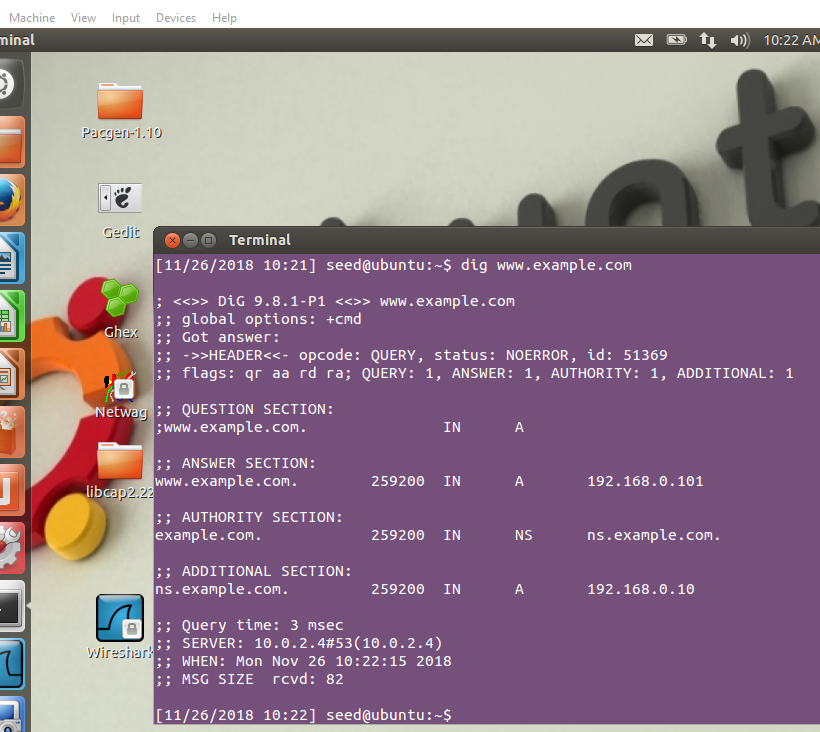
184.168.221.48 is correct address of *www.bank32.com*.



**Observation:**

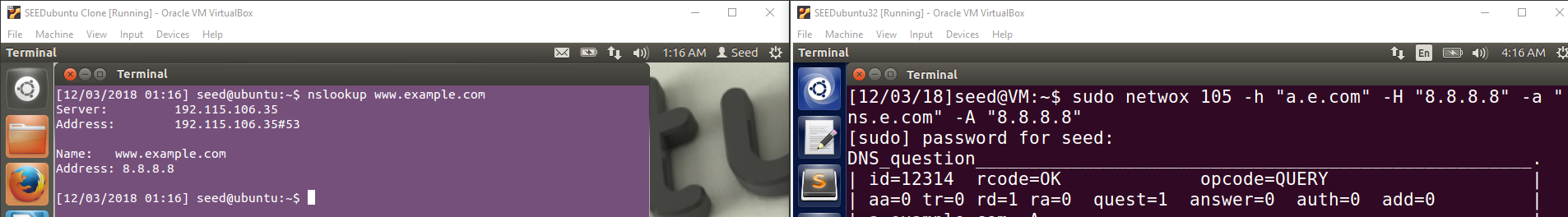
We modified the */etc/hosts* file, so the address of www.bank32.com is 1.2.3.4. But the *dig* command ignore */etc/hosts*.

* Task 5: Directly Spoofing Response to User



**Observation:**

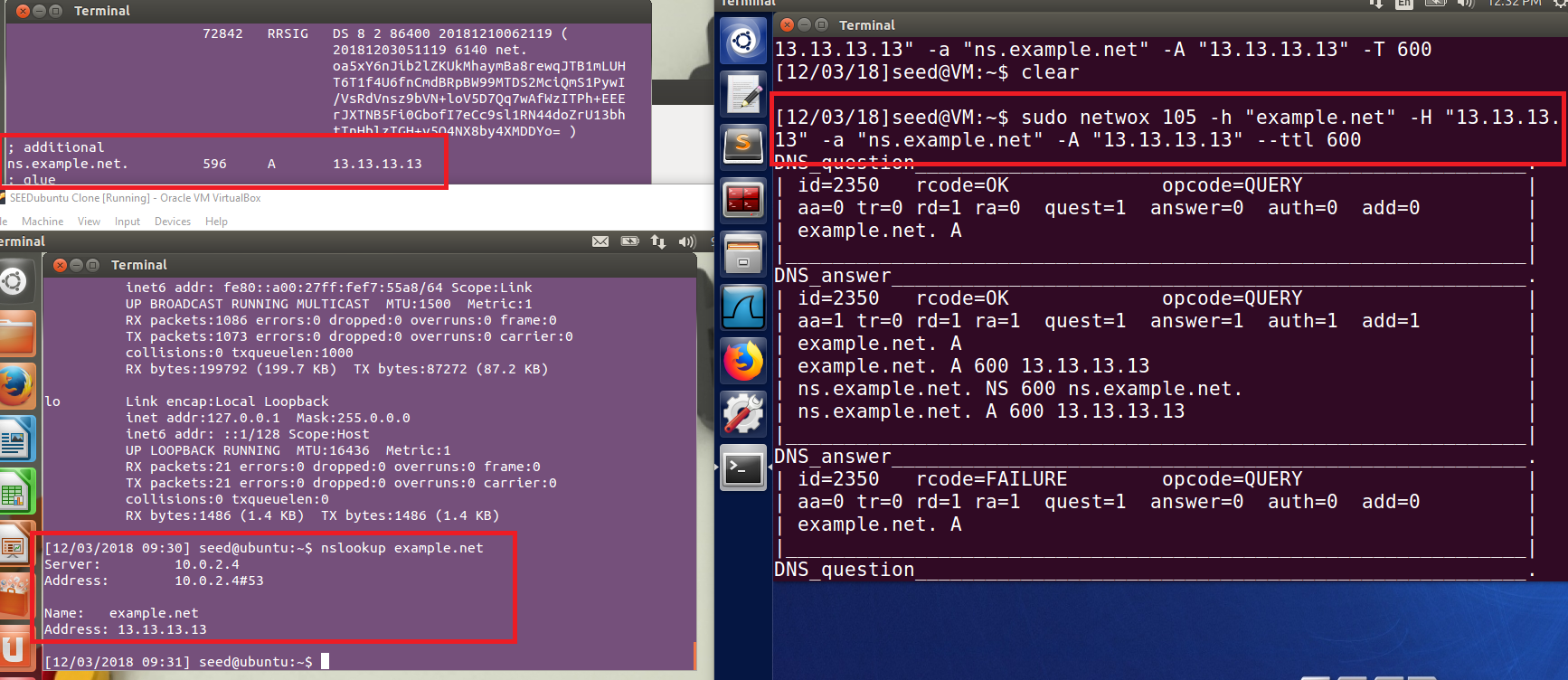
Before the attack, cache contain the answer.



**Observation:**

After the attack, cache does not contain the answer, so User Machine send out a DNS query to the local DNS server and Attacker manages to receive the fake address.

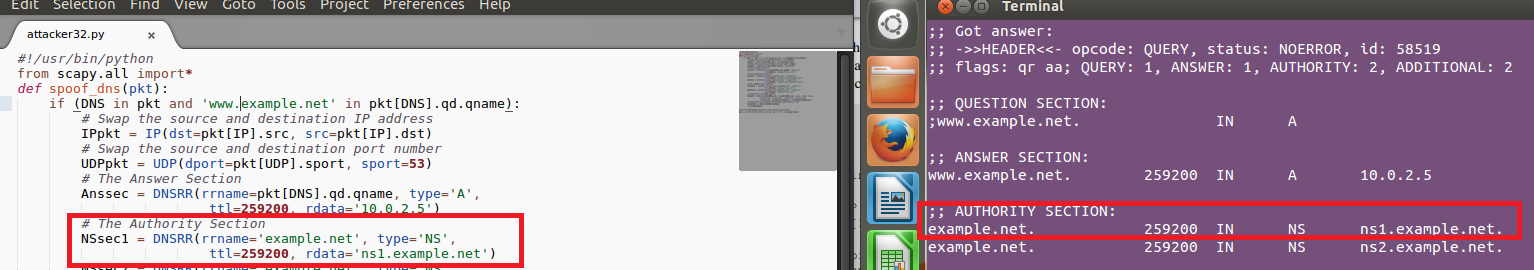
* Task 6: DNS Cache Poisoning Attack



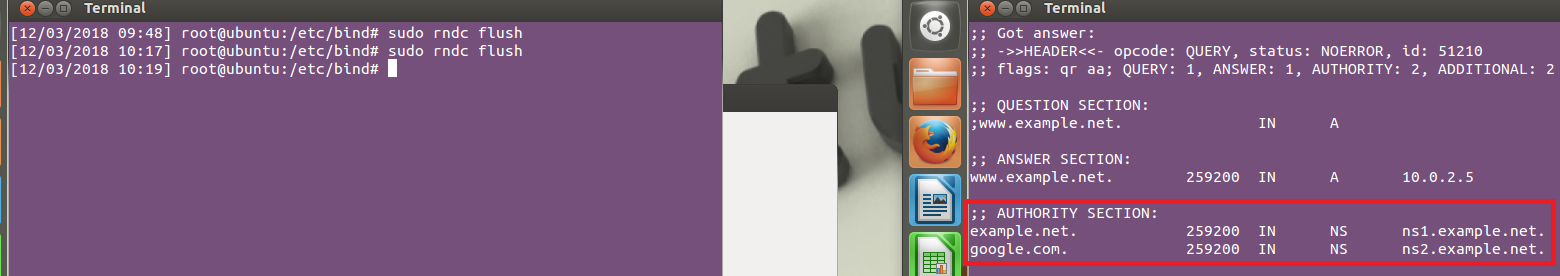
**Observation:**

We dumped the local DNS server’s cache. We set ttl to 600 (seconds), then DNS server will keep giving out the fake answer for the next 10 minutes.

* Task 7: DNS Cache Poisoning: Targeting the Authority Section



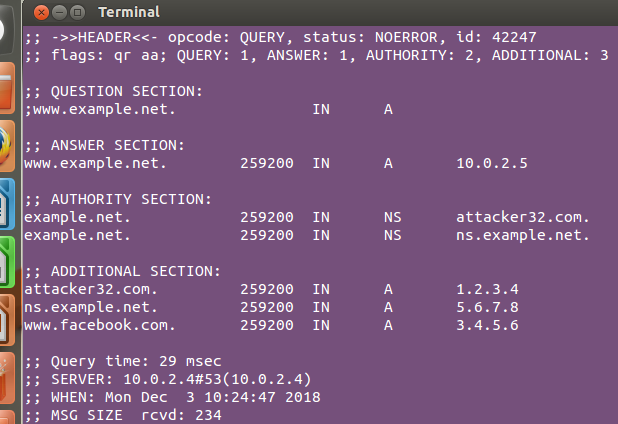
* Task 8: Targeting Another Domain



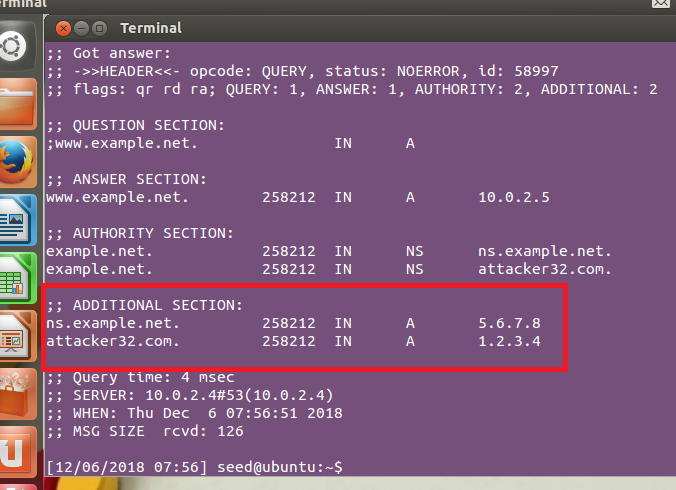
**Observation:**

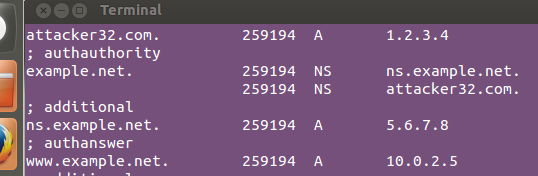
Now, ns2.example.net is also used as the nameserver for google.com.

* Task 9: Targeting the Additional Section









**Observation:**

*www.example.net*, *ns.example.net*, *attacker32.com* be successfully cached. *www.facebok.com* not be cached, because he was only in ADDITIONAL SECTION: This displays the ip address of the name servers listed in the AUTHORITY SECTION. AUTHORITY SECTION: This displays the DNS name server that has the authority to respond to this query.