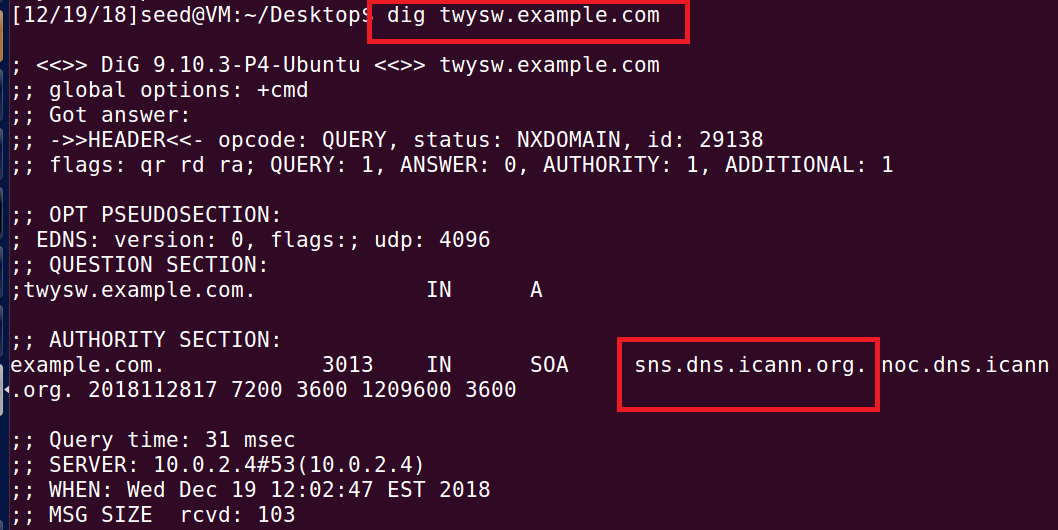
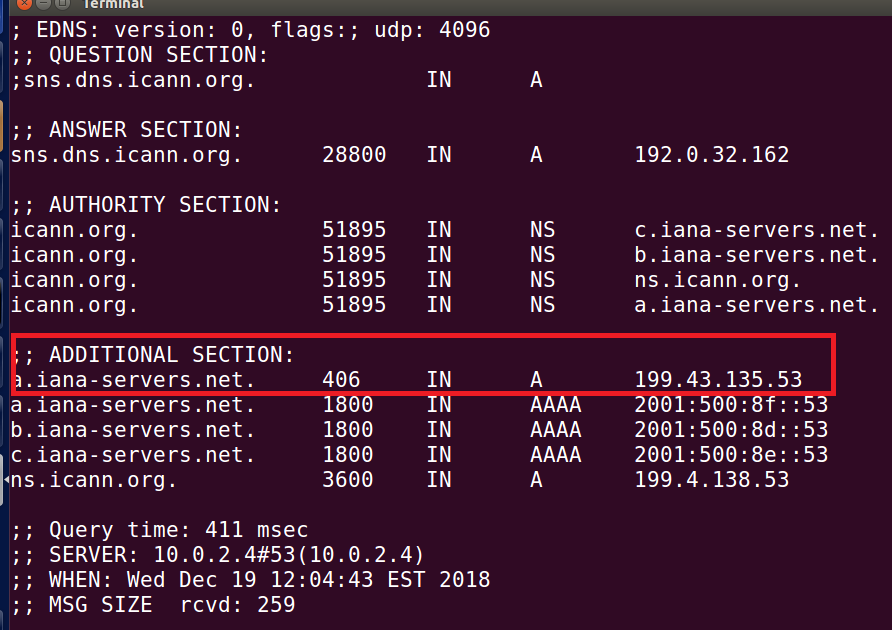
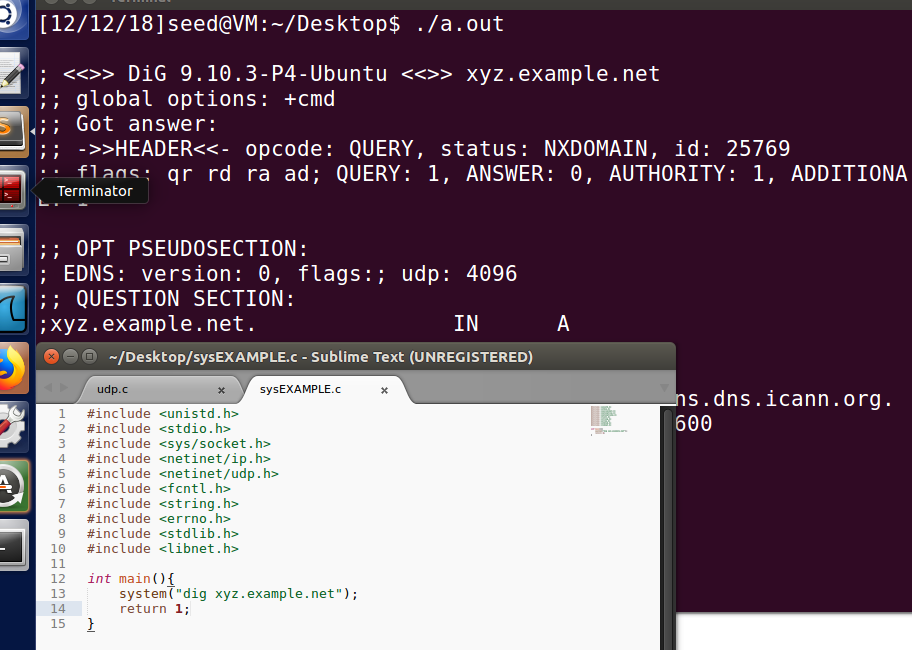
**Remote DNS Cache Poisoning Attack Lab**

Task 1: Remote Cache Poisoning

Task 1.1: Spoofing DNS request

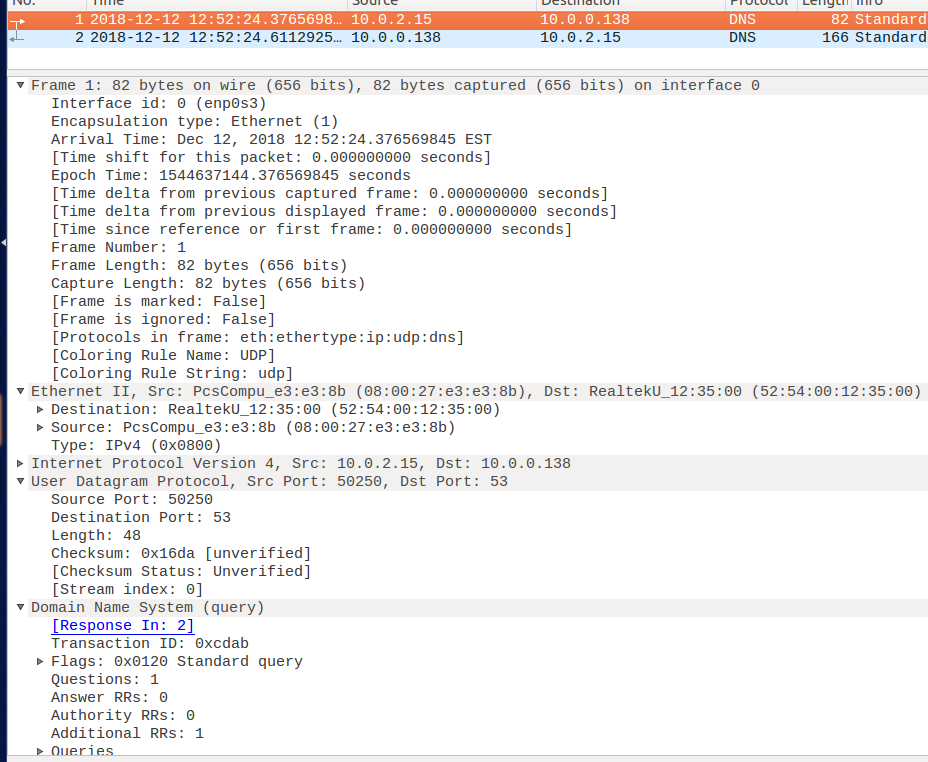




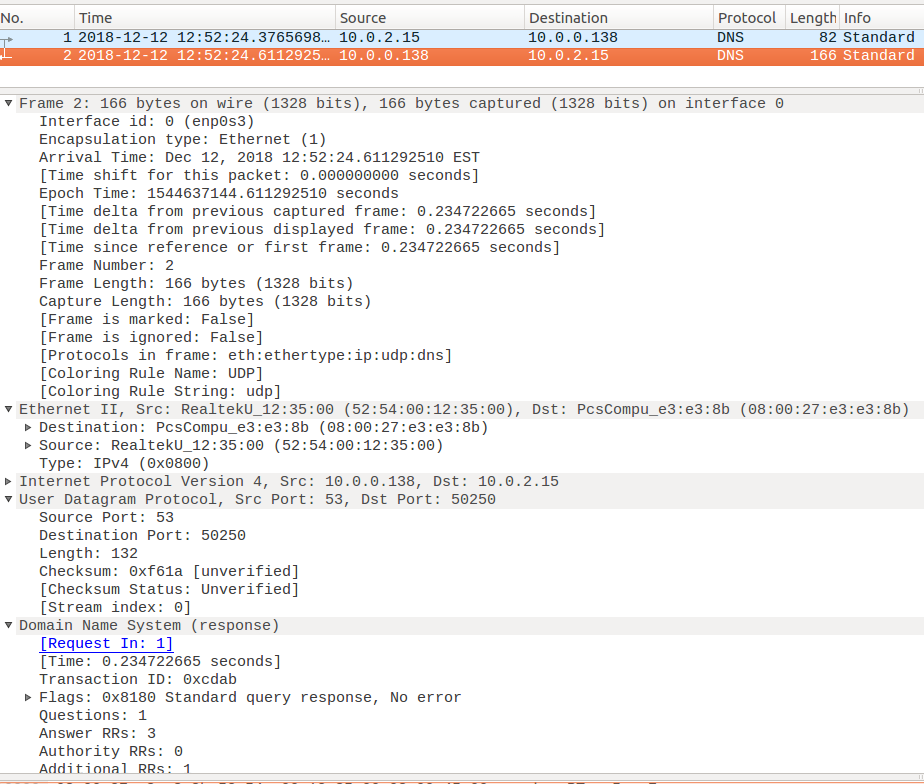


Task 1.2: Spoofing DNS Replies

Request:

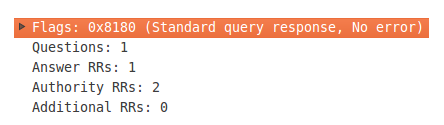


Response:

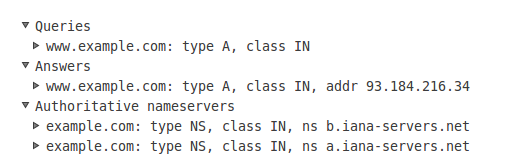


**Observation:** Not all DNS messages have the above parts. The “12 bytes” indicated in the figure are the DNS header. This piece will definitely be there. The body part under the heading is the main part of the request. In addition, the response, authorization, and additional information sections are present only in the response DNS message, and all three have the same format as the resource record (resource record), which will be mentioned later. DNS messages are analyzed field by field below.

|  |  |
| --- | --- |
| Transaction ID | Flags |
| Questions | Answer RRS |
| Authority RRS | Additional RRS |

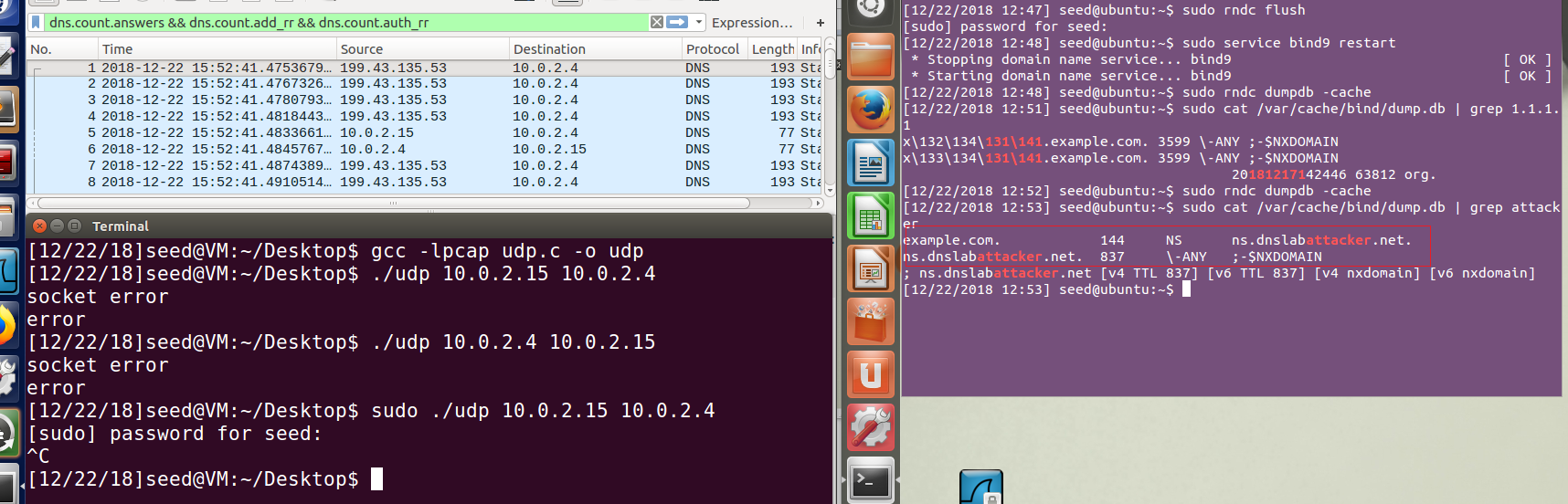


**Observation:** Flag (2 bytes): this part is very important and should be analyzed bit by bit. Then borrow the image: QR (1 bit): request / response flag, 1 is the answer, and 0 is the request. Operation code (4 bits): Determines the type of request or response (if 0, it means standard, if it is 1, it is reversed, if it is 2, it is a server status request). AA (1 bit): authorized response flag. This bit is valid in the response message, 1 means that the name server is a rights server (discussed later on the rights server) TC (1 bit): truncation flag. 1 indicates that the response exceeded 512 bytes and was truncated (we seem to remember where to mention this truncation and the associated UDP, remember first) RD (1 bit): this bit is 1, means that the client wants to receive a recursive response (recursive later) Discussion RA (1 bit): only 1 can be set in the response message, indicating that a recursive response can be received. Zero (3 bits): if you do not say this, you know that this is 0 and save the fields. Rcode (4 bits): a return code indicating the error status of the response, usually 0 and 3.



**Observation:** Then the data part is the one-to-one correspondence.

Task 1.3: The Kaminsky Attack

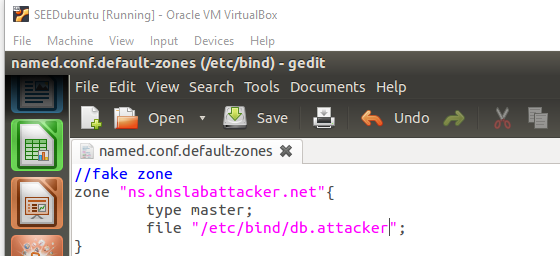




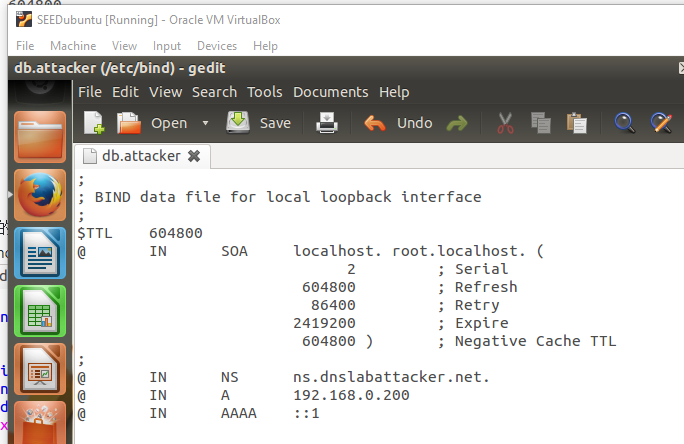
Task 2: Result Verification

The answer is no, the reason and the previous analysis of why Apollo does not directly accept the return of the DNS .com for the DNS address example.com a.iana-servers.net coincide. Since our fake response packets are returned from a.iana-servers.net or b.iana-servers.net domain name servers, they are not official domain name servers responsible for the example.com domain, so even if we set the IP Address of Apollo will be accepted.

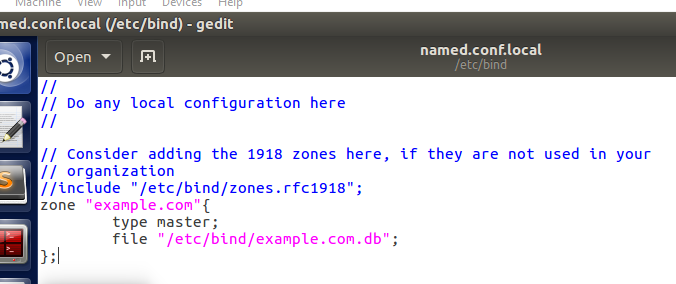
Step 1: Add fake zone to the file *named.conf.default-zones*



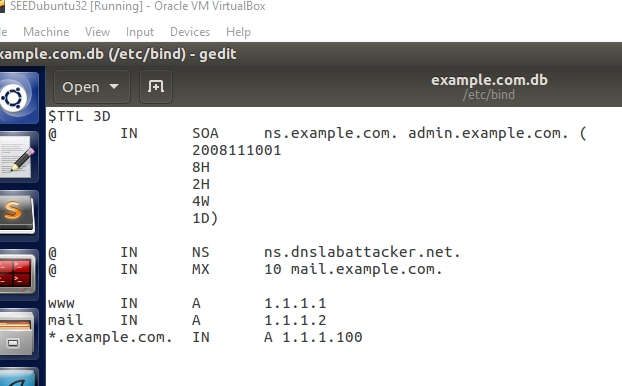
Step 2: Create the file */etc/bind/db.attacker*



Step 3: Add new configuration in */etc/bind/named.conf.local* on 10.0.2.15 (Attacker)



Step 4: Create a file called */etc/bind/example.com.db*



Step 5:

