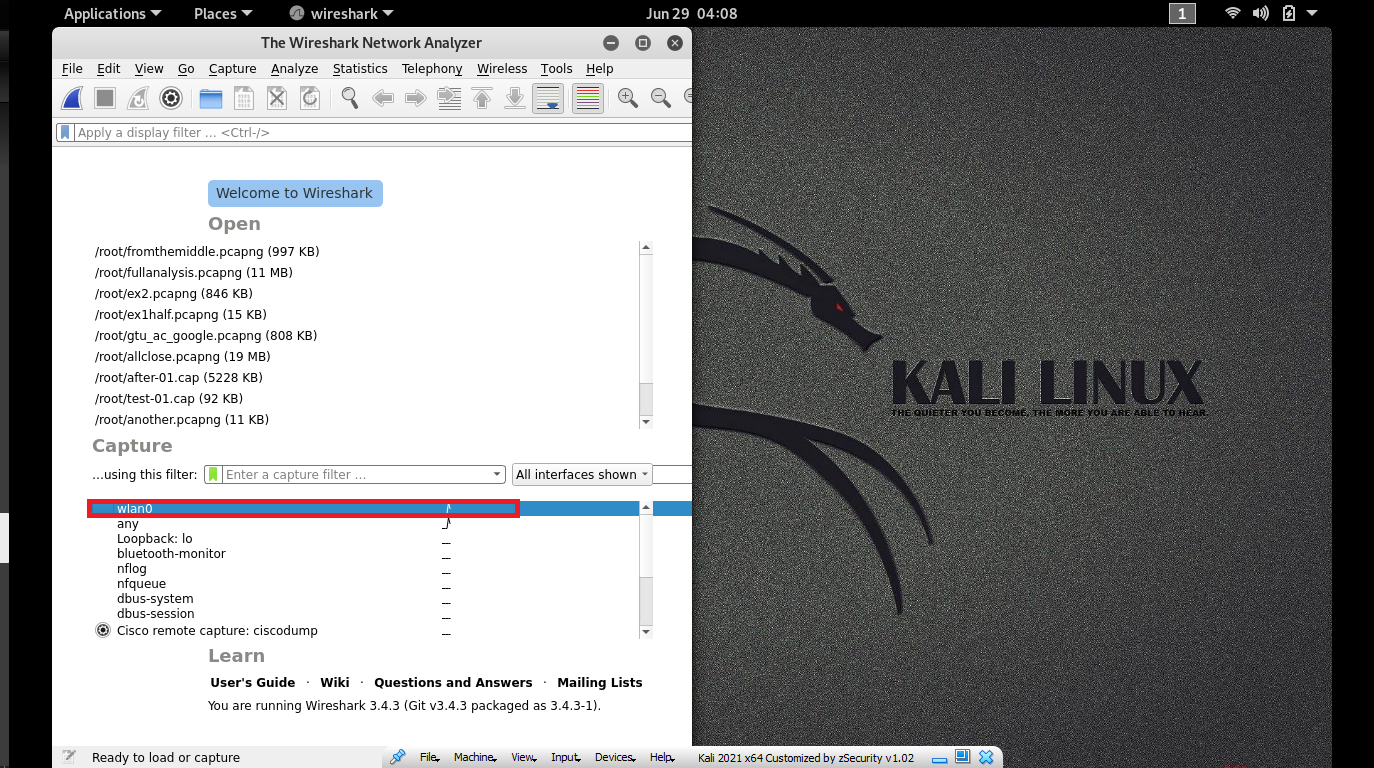
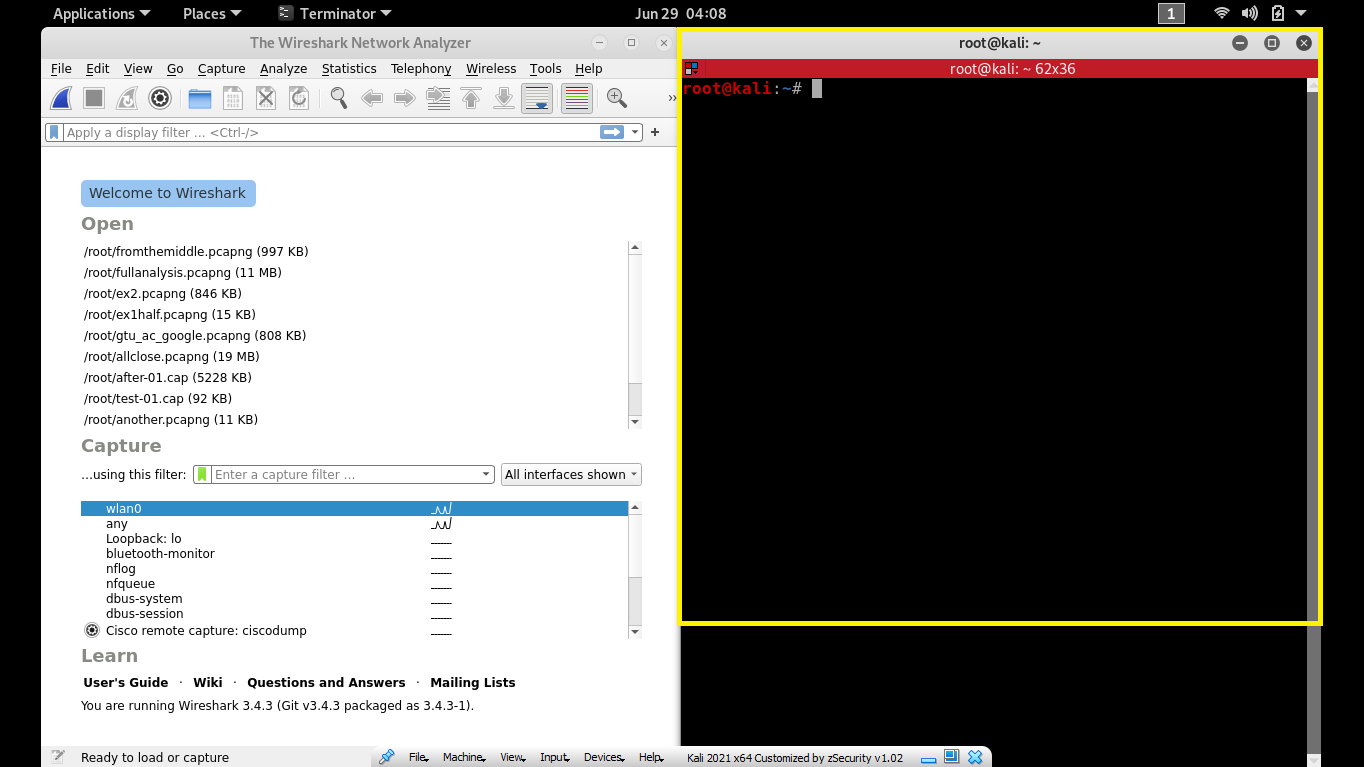
**Start packet capture**

Double click on selected interface

****

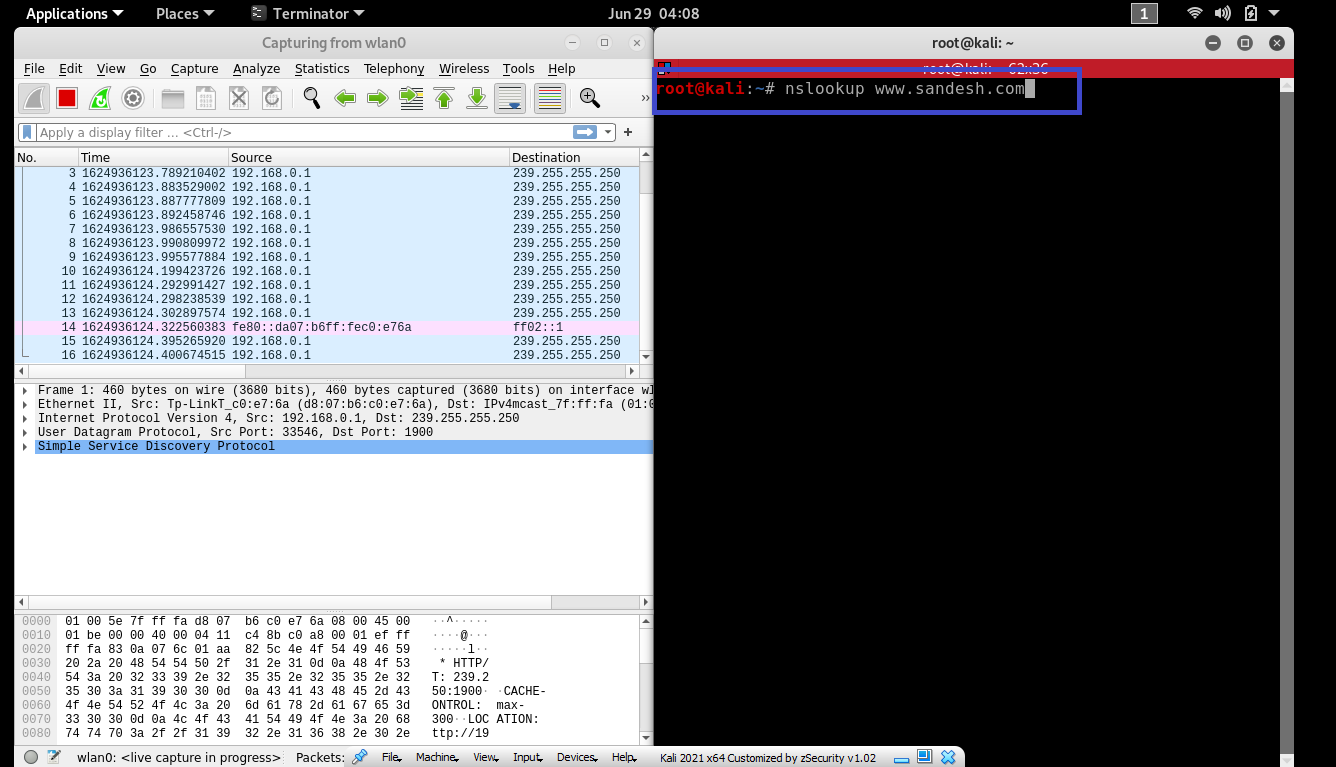
**At Command prompt > Nslookup** [**www.sandesh.com**](http://www.sandesh.com)

**1 ) open terminal**

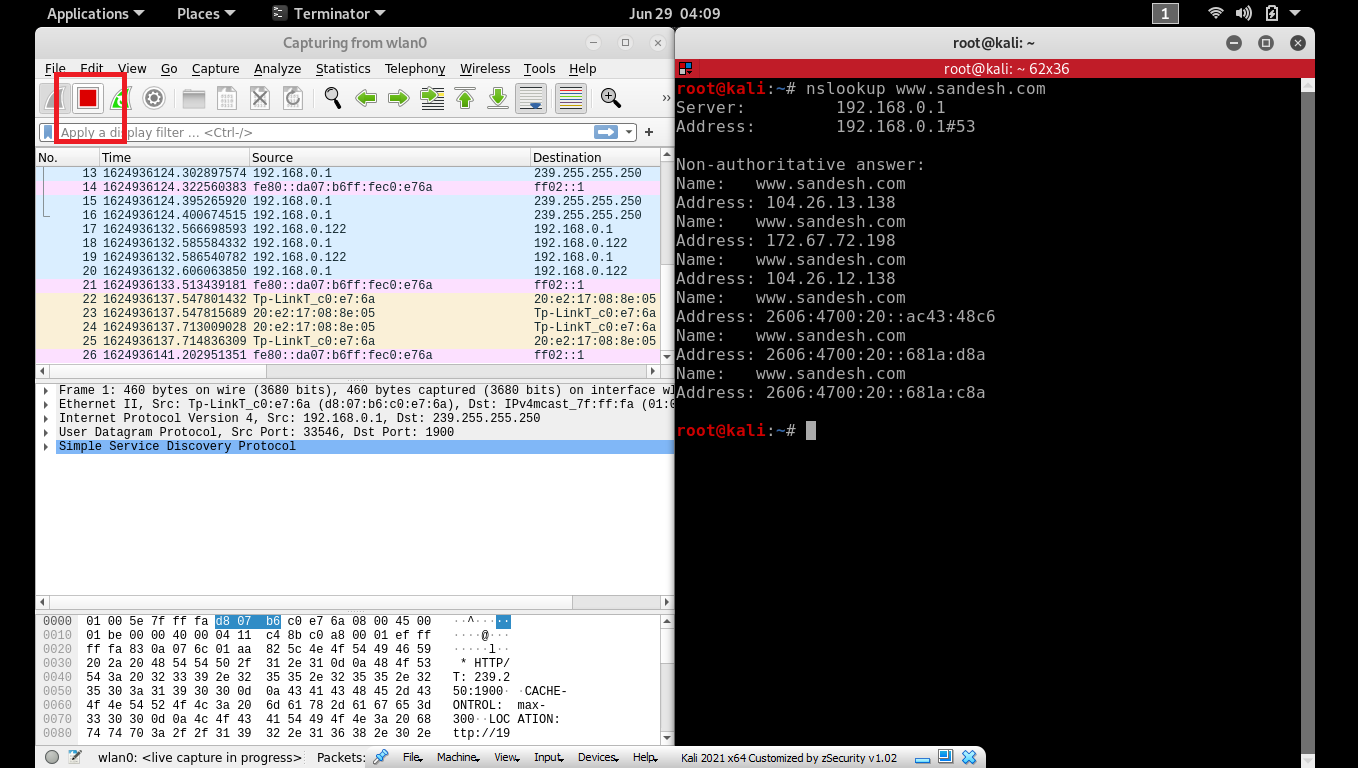
****

**I have linux so I’ve terminator…(if you are on window os just press start type cmd and press enter)**

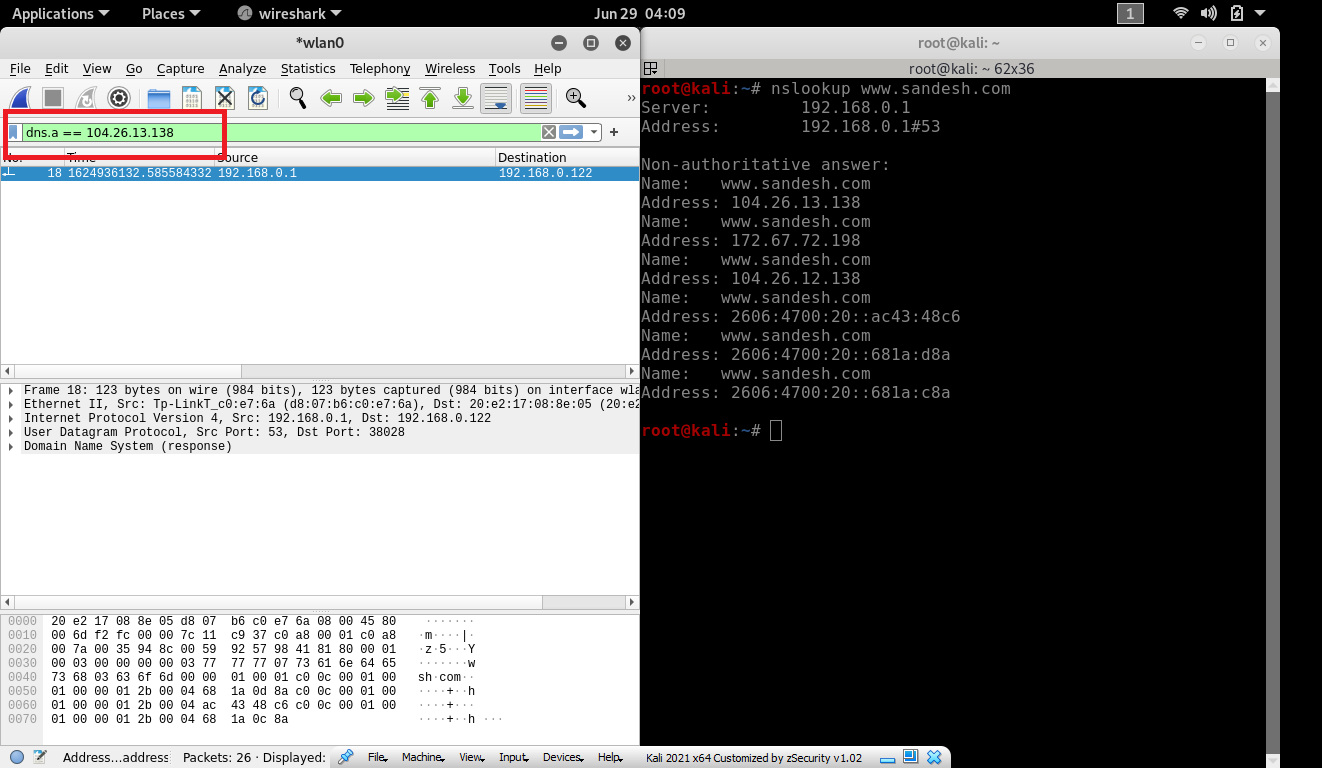
**2) after open cmd or terminator type Nslookup** [**www.sandesh.com**](http://www.sandesh.com)

****

**Stop packet capture**

****

**Filter : ip.address== IP address of sandesh.com**

****

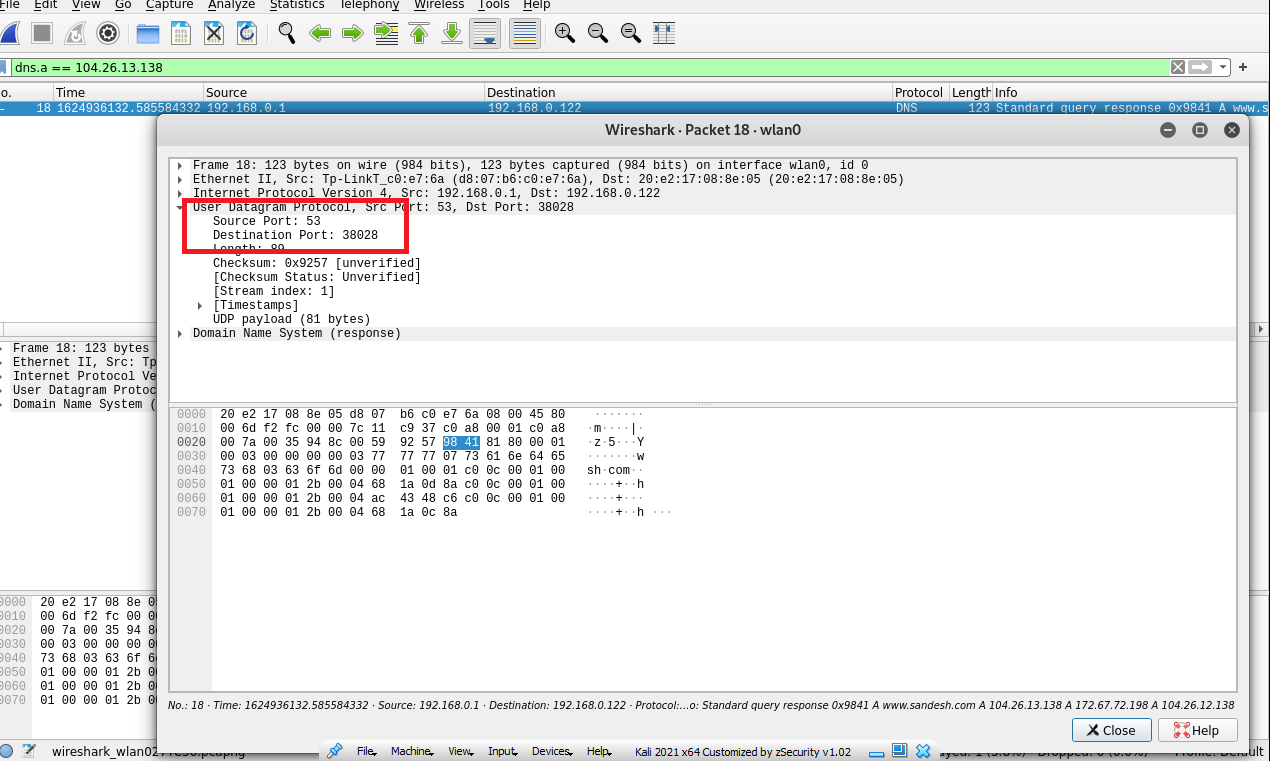
**Find These Questions**

**1. What is the destination port for the DNS query message ? What is the source port of of**

**DNS response message?**

**Ans 🡪 destination port : 38028**

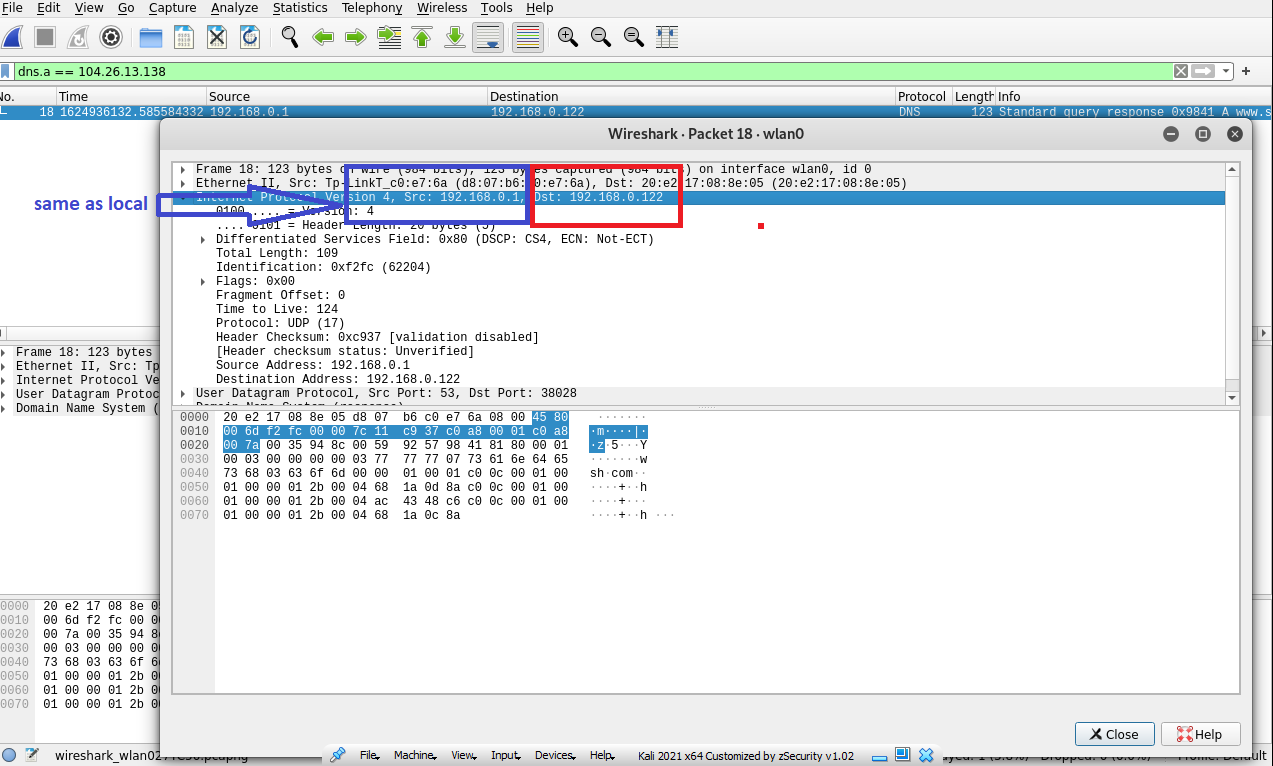
**Source port : 53**

****

**2. To what IP address is the DNS query message sent ? Is this the IP address of your default**

**local DNS server ?**

**ans 🡪 The DNS Query is sent to IP Address 192.168.0.1, the same address as my default local DNS Server.**

****

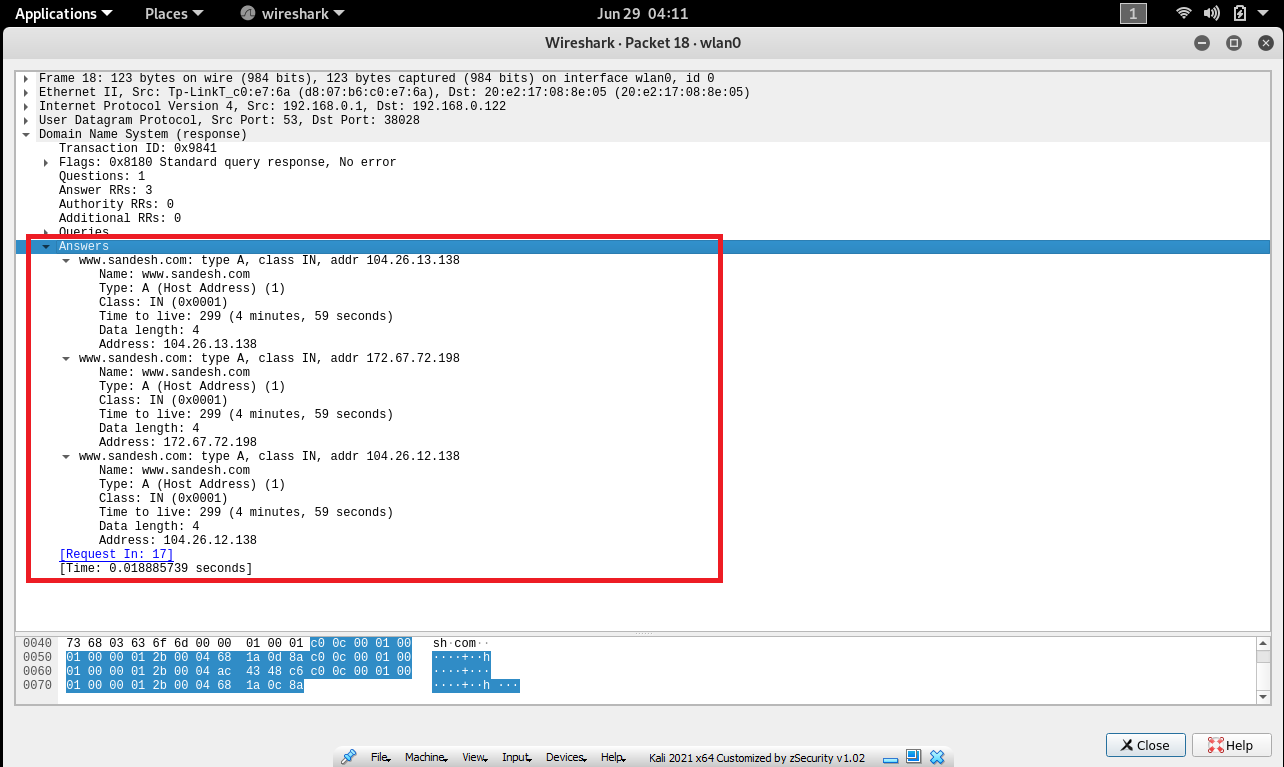
**3. Examine the DNS query message. What “Type” of DNS query is it? Does the query**

**message contain any “answers”?**

**ans🡪 The DNS query message is a type “A” query,containg only one questions and not containing any answers**

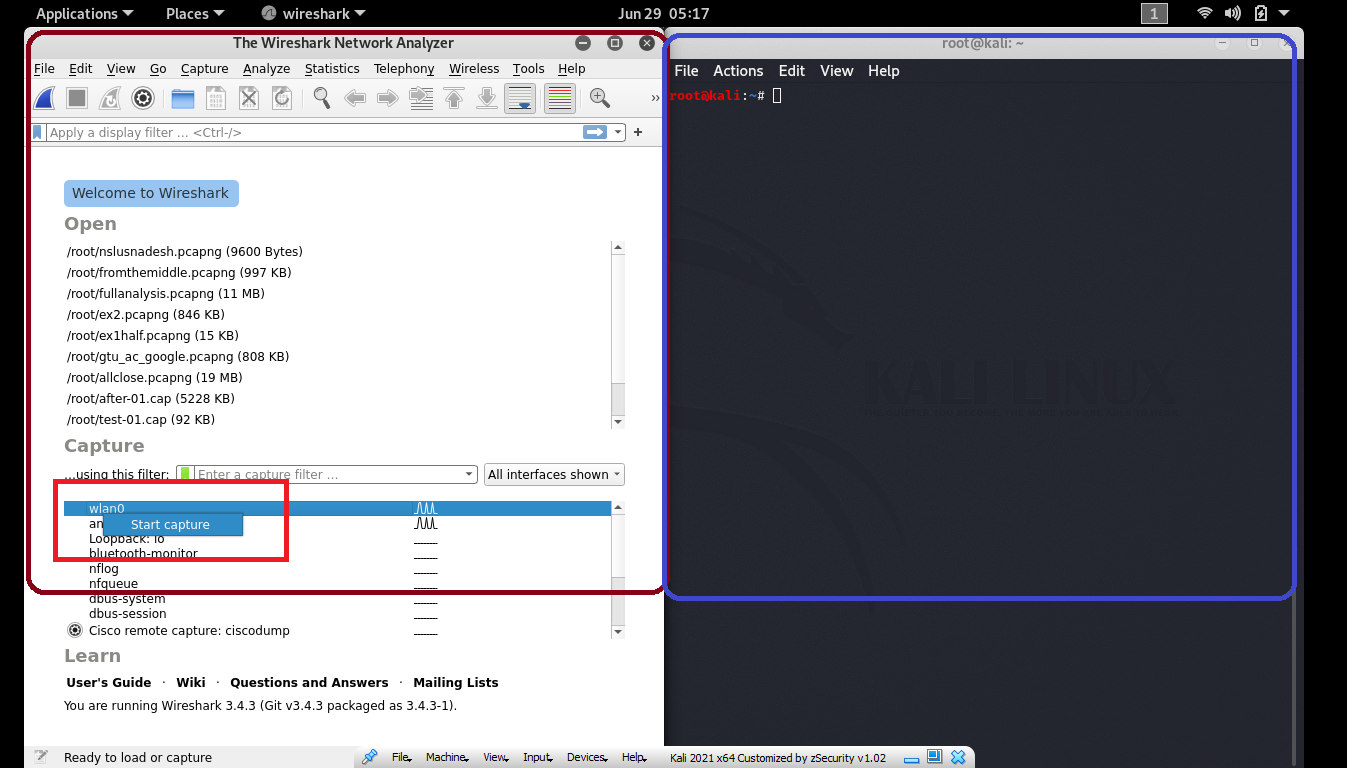
**4. Examine the DNS response message. How many “answers” are provided? What does each**

**of these answers contain?**

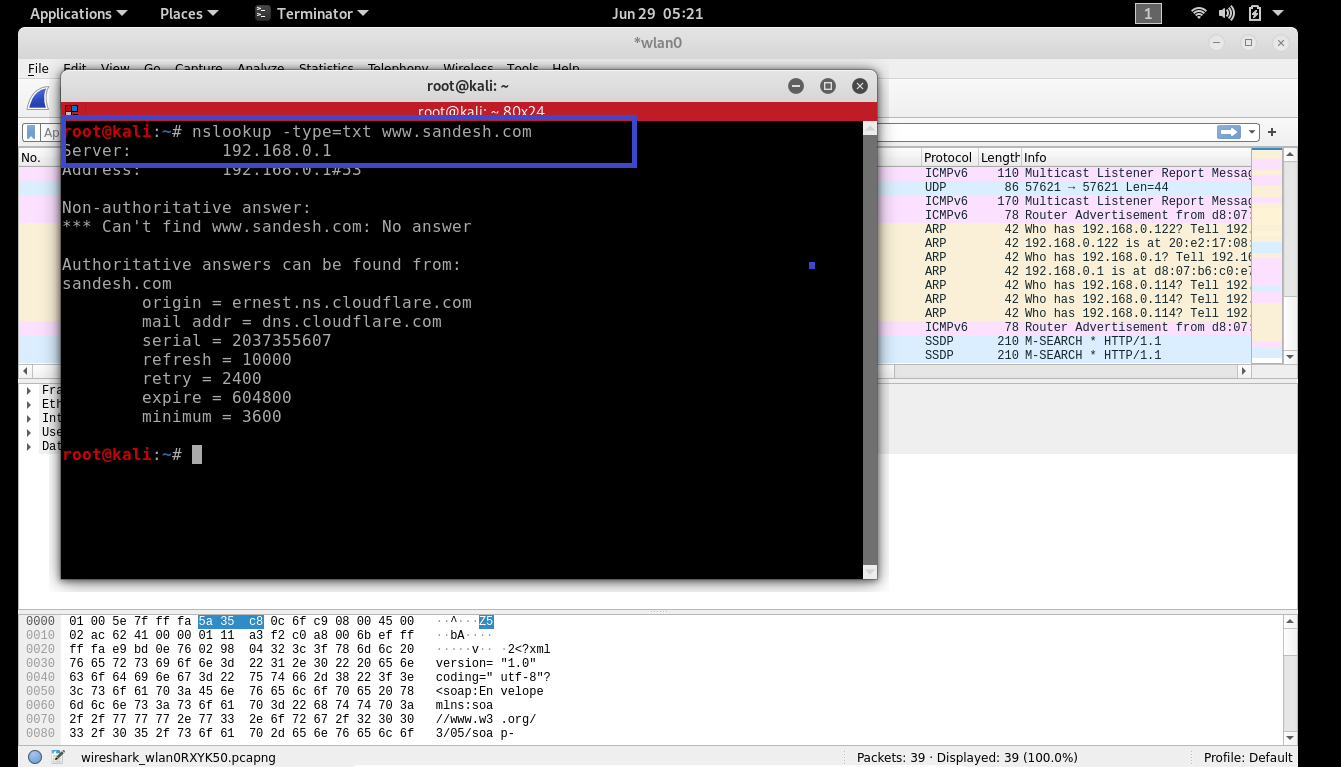
**ANS🡪 The response message contains one anser to the aforementioned query which is the type “A” address of** [**www.sandesh.com**](http://www.sandesh.com) **or 104.26.13.138.it also contained information about class,time to live and data length **

**Repeat the following steps**

Open wireshark and terminator then start capturing



At Command prompt > Nslookup –type=NS [www.sandesh.com](http://www.sandesh.com)



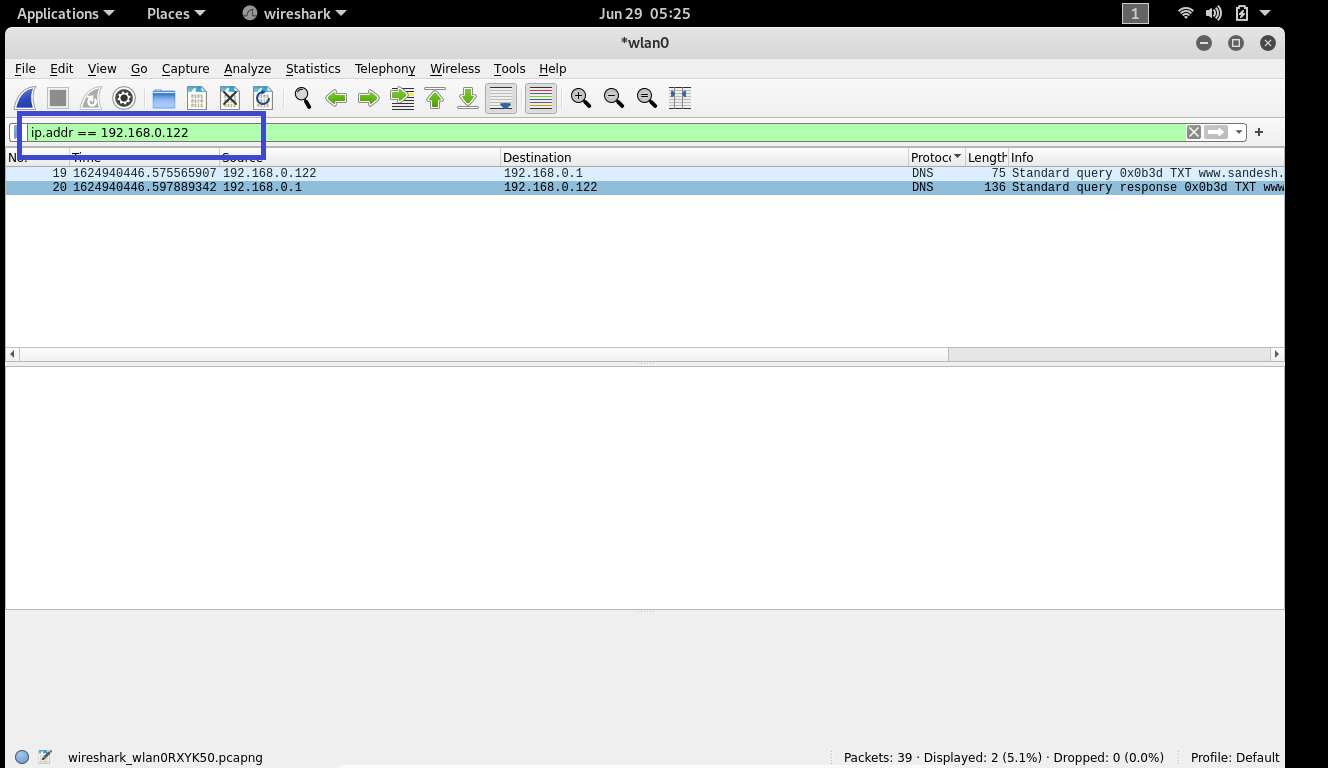
Differences in command

For linux os : Nslookup –type=NS [www.sandesh.com](http://www.sandesh.com)

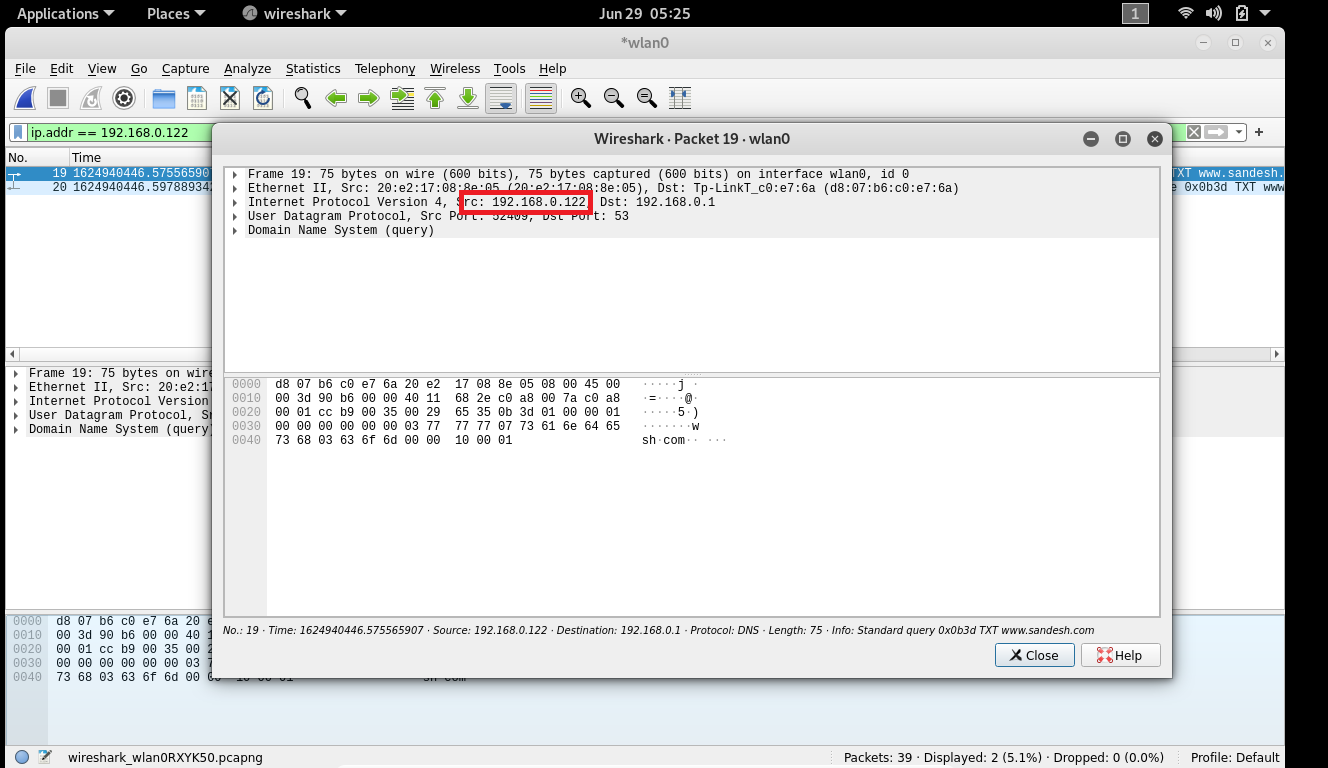
For windpws os : Nslookup –type=txt [www.sandesh.com](http://www.sandesh.com)

NOW stop the capturing

**Filter : ip.address== IP address of sandesh.com**

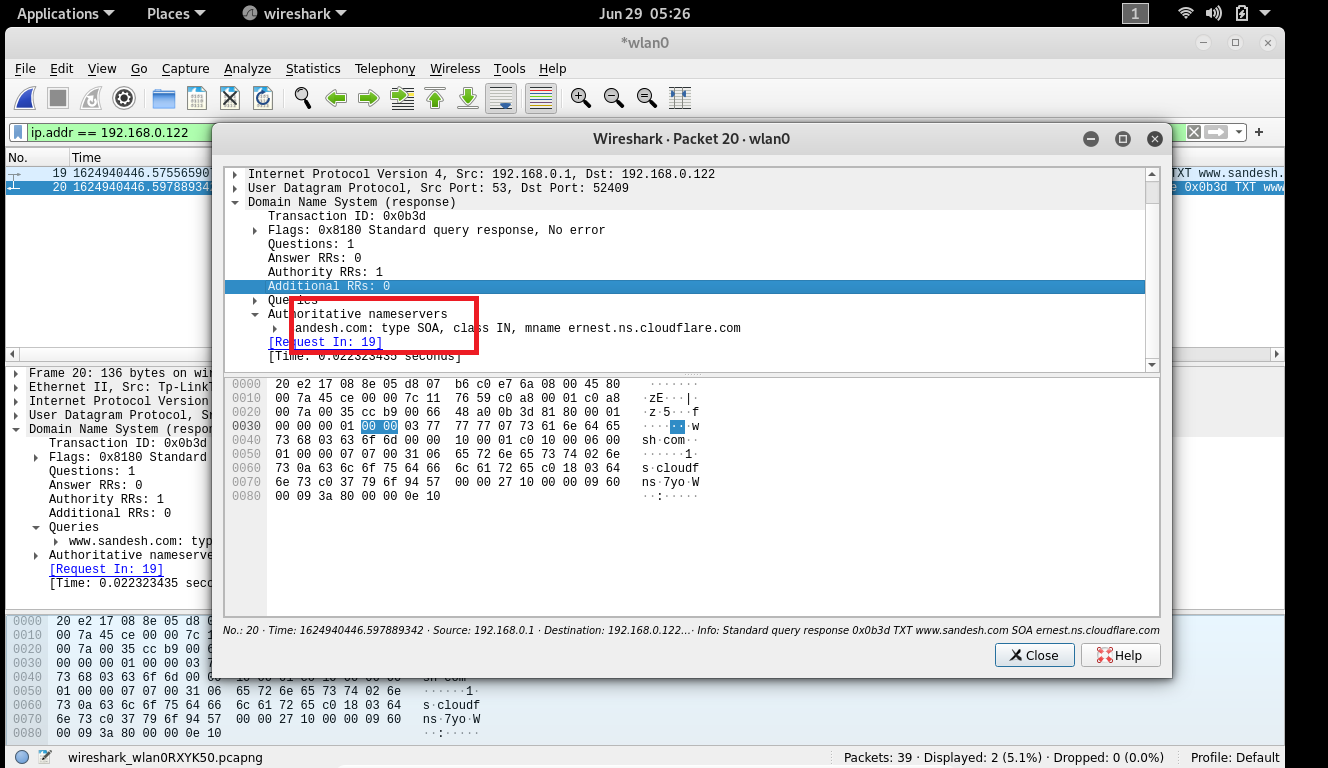
****

1. **To what IP address is the DNS query message sent ? Is this the IP address of your default local DNS server ?**

****

**2. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

**ans🡪** type “SOA” which contain one question

****

**3. Examine the DNS response message.What sandesh.com name servers does the response message provide ? Does this response message also provide the IP addresses of the Sandesh name servers ?**

**Ans🡪** The DNS Response not contained any answer.