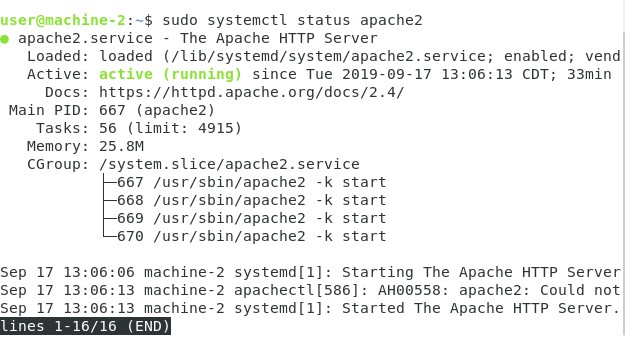
**Web Server:**

**1. Part-1: Setup**

A. The apache2 package was already installed and updated on debian9, so to check the current status of apache2 following command was executed.



B. In order to help set policies and manage exceptions, UFW firewall was installed with the command:

sudo apt-get install ufw

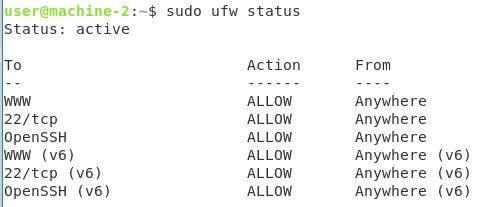
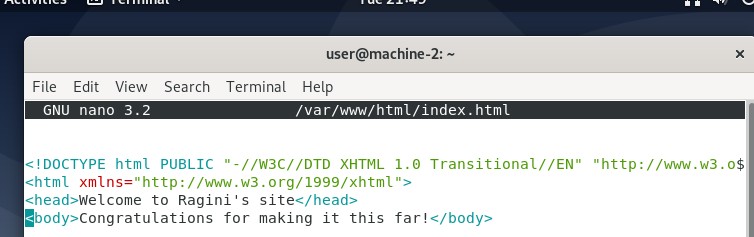
C. To make sure UFW firewall allows SSH connections, TCP, and ‘WWW’ connections, we allow these connections by typing the following commands on the terminal

sudo ufw allow OpenSSH : To allow SSH connections from other VMs in same network

sudo ufw allow ‘WWW’: To open port 80 for unencrypted web (HTTP) traffic. This is done because by default the apache runs on port 80. sudo ufw allow 22/tcp: To open TCP connections, or to allow ssh by port 22.

D. To view if the change has been activated we check the status with the execution of following

command:

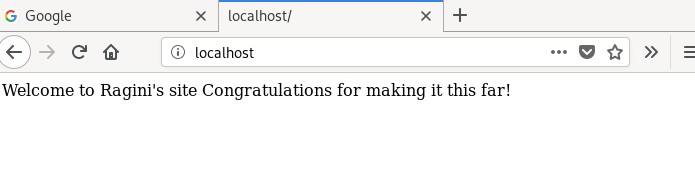
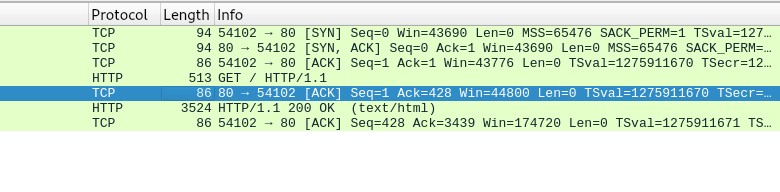
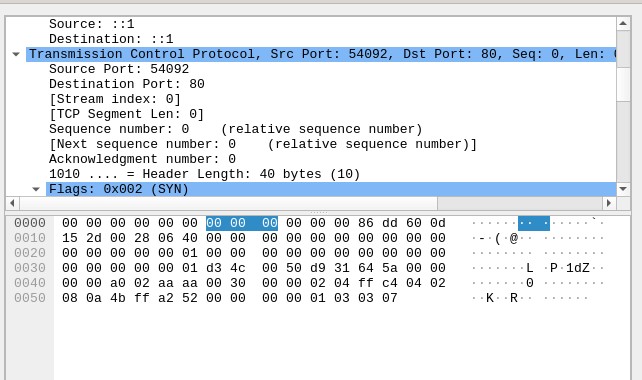


E. Accessing the web server using localhost on the same VM displays the following on the web browser:



F. Edit the index.html file in the directory as follows:

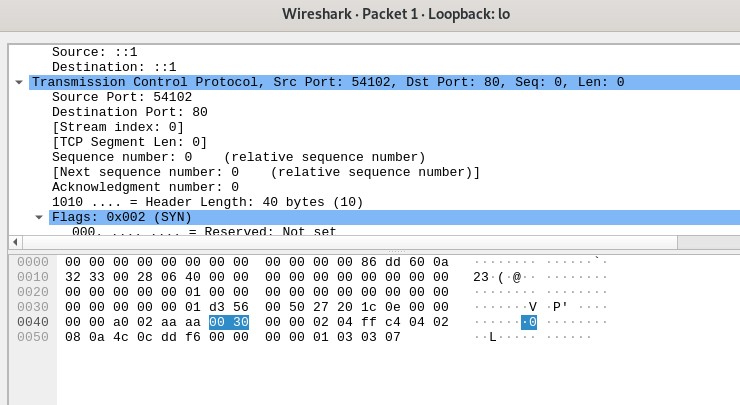
G. Accessing the web server on the browser displays the customized index.html as follows:



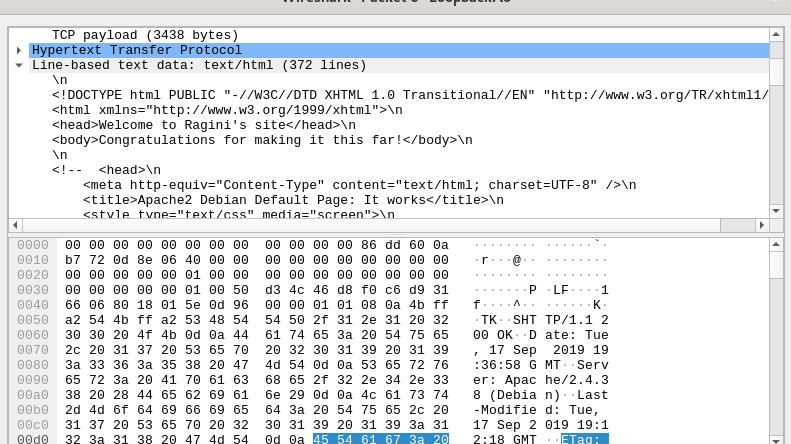
**2. PART-2 Wireshark:**

A. Monitoring the traffic on Wireshark displays the following:

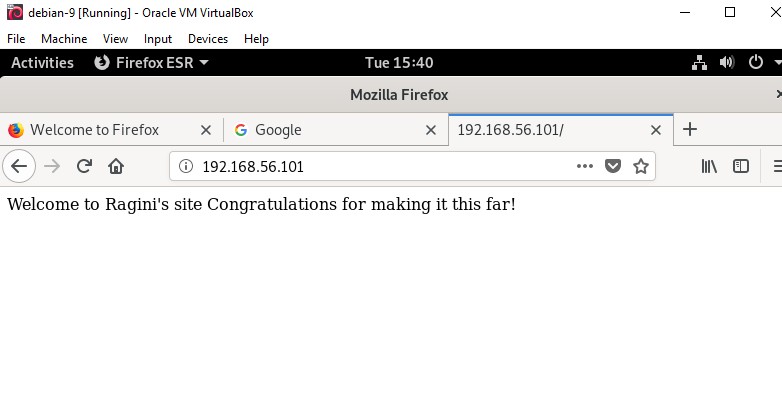
From the above screenshot, we observe that there is a three-way handshake between the client browser and the server following which the HTTP GET request is sent, which serves back at port 80 with the ACK message rendering the index.html on the browser.



B. The response message is the TEXT/HTML as shown in the screenshot below.



**C. Visit your web server running in one VM, from the other VM.**



In order to do that, we enter the IP address of VM-1(where the web server is running) into the web browser of other VM instead of using localhost. This will render the index.html on the browser of second VM

**RA-02**

**1. Setup:**

A. Changing the hostname of both names with a domain name added to it. This is done by ONLY

editing the hostname for respective VM and NOT the hosts file.

VM-1 (with DNS server):

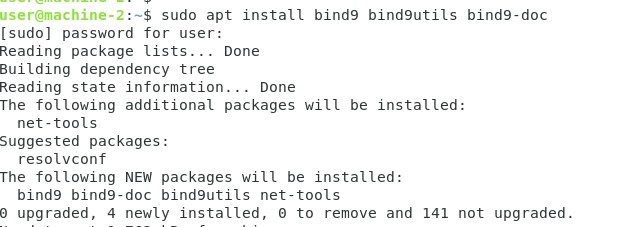
sudo nano /etc/hostname: machine-2.ragini.com

VM-2:

sudo nano /etc/hostname: machine-1.ragini.com

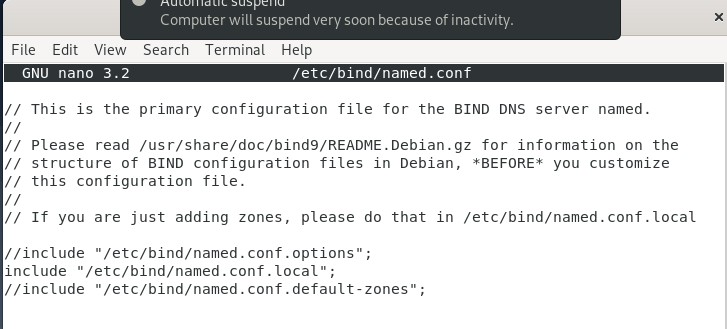
(ragini.com is the domain name)

B. Installing the BIND DNS software on VM-1 to translate domain names into IP addresses as follows:



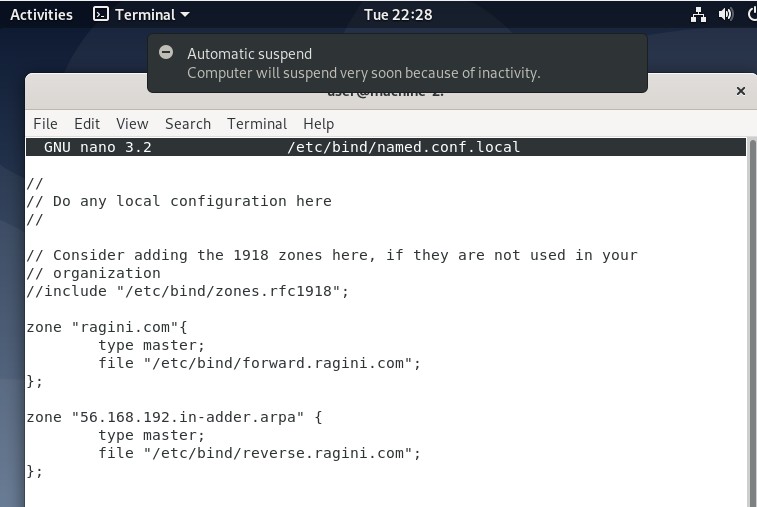
The DNS configuration files are stored in the **/etc/bind** directory. The primary configuration file is **/etc/bind/named.conf**.

C. Since, we are only dealing with primary DNS server here and need no forwarders we edit only the /etc/bind/named.conf.local and comment the other two lines in named.conf file as follows:



D. Open DNS port 53 using ufw for all

E. Open the named.conf.local file to add the following lines to define forward and reverse zone files.

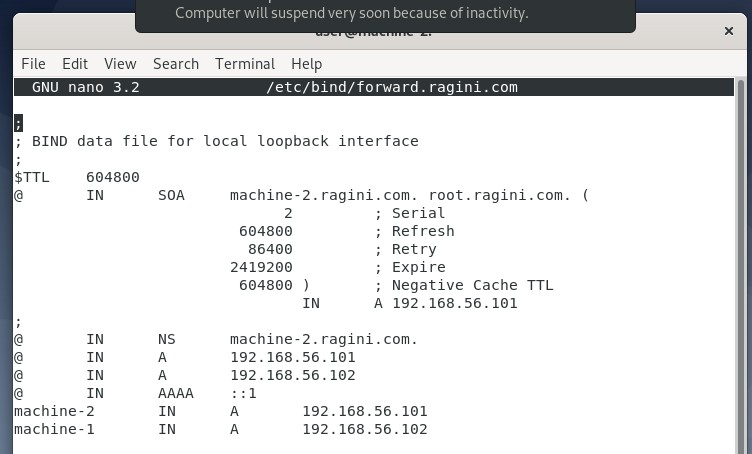


Domain Name

It is worth mentioning that “ragini.com” is the domain name here.

F. Edit the forward.ragini.com file with the domain name of the dns server and ip address of both

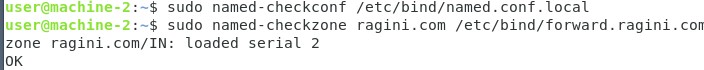
VM-1 (SOA/DNS server) and VM-2 (Client) as follows:



Primary name server

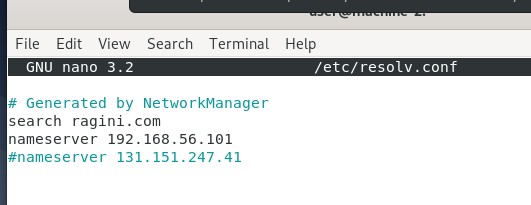
Client

G. Testing the DNS configuration and zone file as follows:



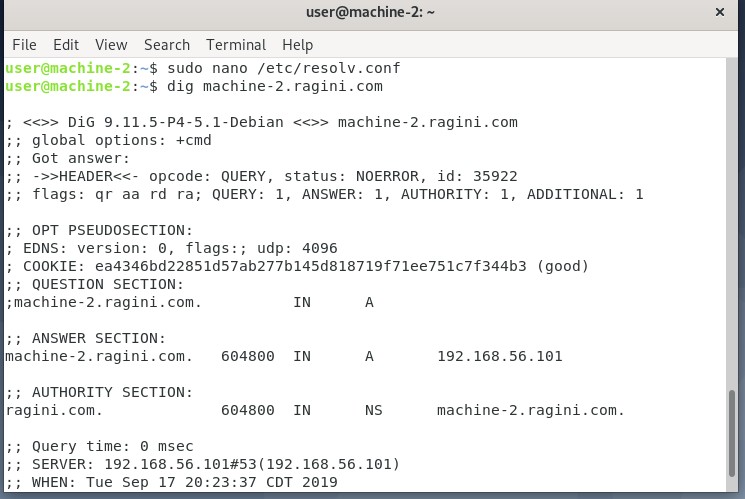
The configuration files had no syntax errors on executing the commands shown in screenshot.

H. Testing the master DNS server by editing the resolv.conf file on VM-1 machine



Rebooting the system to bring the changes into effect and starting the named service.

I. Checking the Master DNS server with the following $dig command as follows:



The above output verifies that our server is working fine.

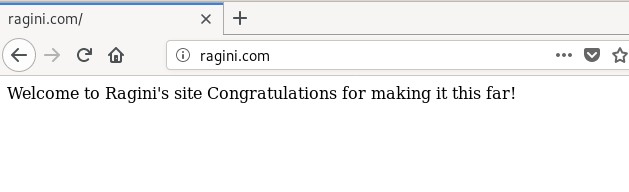
J. Running the ‘**nslookup**‘ command against our DNS server to confirm the output of dig command

as follows:

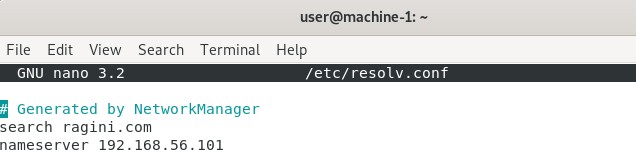


K. Accessing the website, [http://ragini.com from the browser renders the following page](http://ragini.com/)

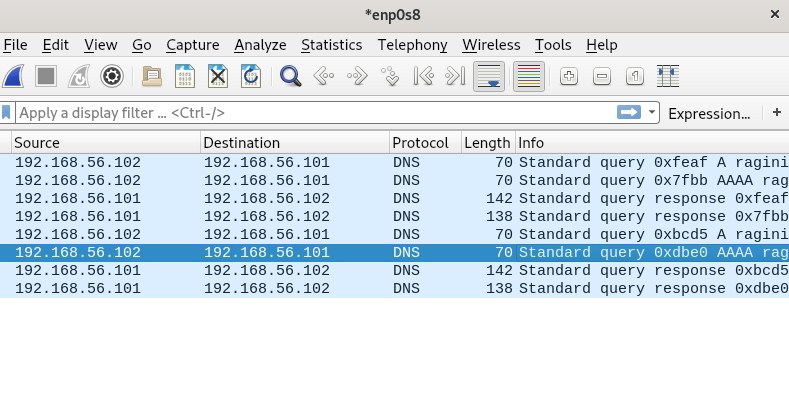
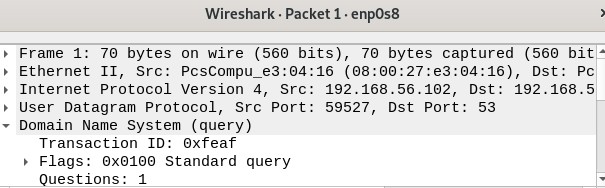
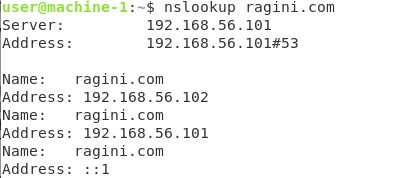
(index.html) as follows:



L. Client Configuration: By editing the resolv.conf file on VM-2(client) machine as follows. In the conf file, the IP address of primary DNS server is added.



M. Nslookup command execution on the client-side:



**Network traffic analysis on Wireshark:**

N. Accessing the website [http://ragini.com and analyzing packets on Wireshark as follows:](http://ragini.com/)

Client DNS server

The underlying protocol is: DNS as shown in packet analyzer.

