CS 491 NETWORK SECURITY

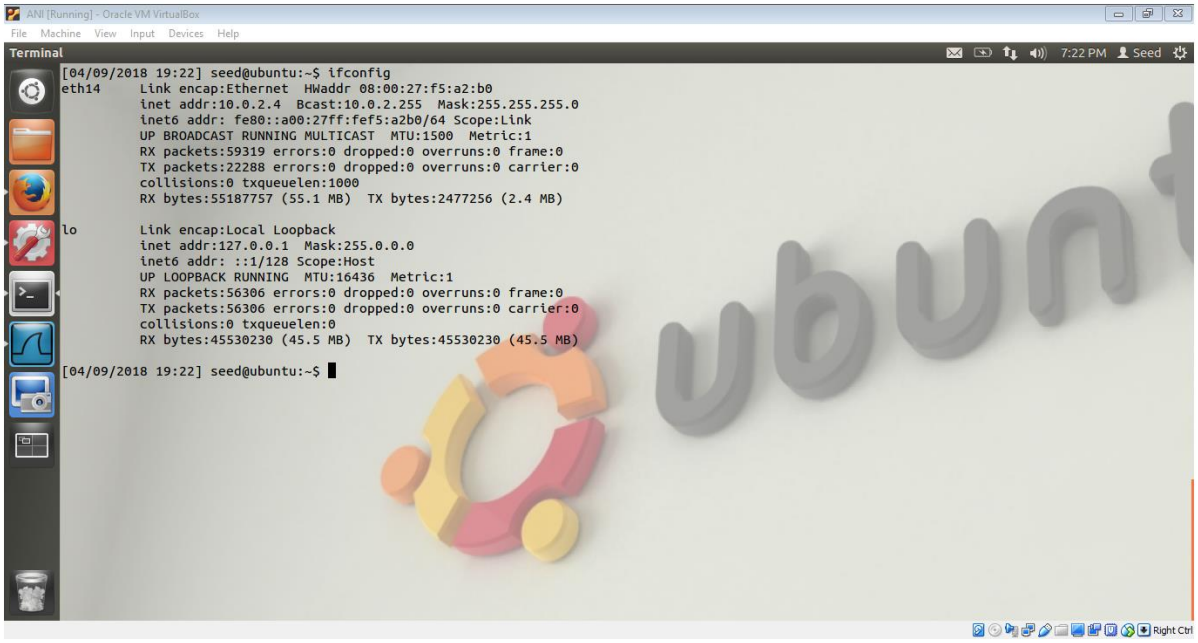
HOMEWORK-2 REPORT

ANIMESH JAIN

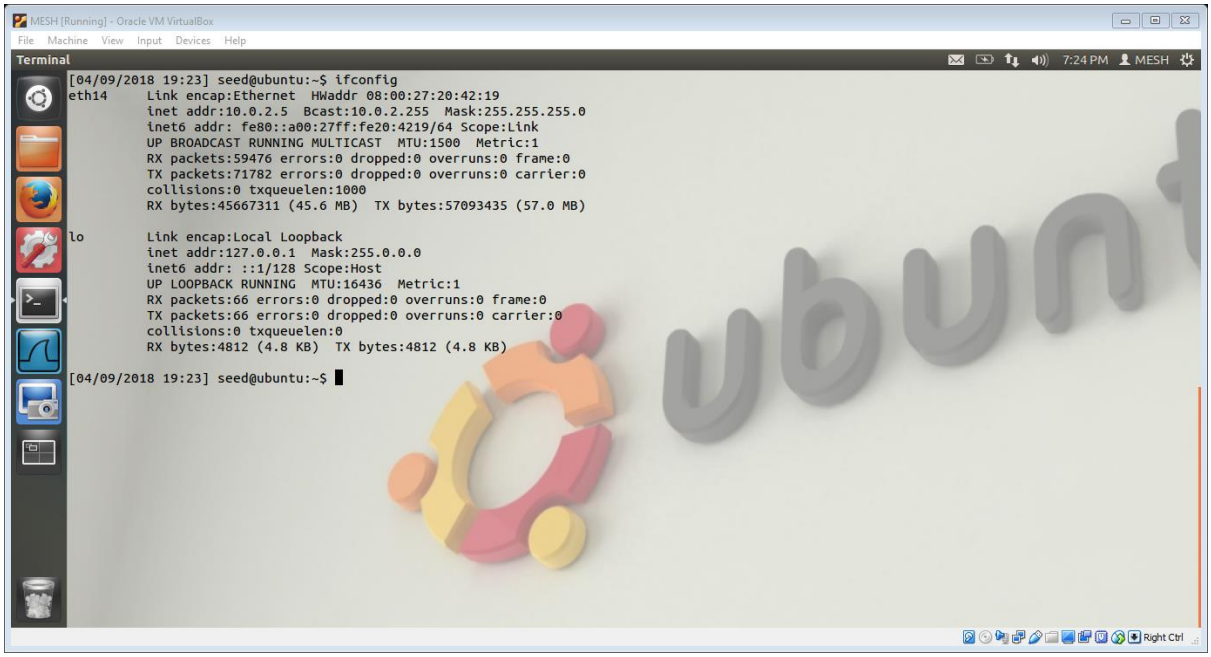
UIN:- 669653208

TASK 1 – USING FIREWALL

MACHINE "ANI" (IP address – 10.0.2.4)



MACHINE “MESH” (IP Address – 10.0.2.5)



Preventing “ANI” from telnetting “MESH”

In this task the purpose is to prevent machine “ANI” from telnetting machine “MESH”. To do this we give the following commands on the terminal of machine “ANI”.

- Sudo ufw deny out from 10.0.2.4 to 10.0.2.5 port 23

  10.0.2.4 – address od machine “ANI”.
  10.0.2.5 – address of machine “MESH”
  23 – Telnet port

  Also we need to enable the firewall and to do so we give

- Sudo ufw enable
  Now when we try to telnet machine “MESH” by giving command “telnet 10.0.2.5” on terminal of machine “ANI” we get the following output.

We have to make sure before telnetting that the firewall is enabled. To check we can use “sudo ufw status” or “sudo ufw status numbered “command.

Preventing MESH from Telnetting ANI

This can be achieved in the similar way as we did in the above task. Commands that we use are: -

- Sudo ufw deny out from 10.0.2.5 to 10.0.2.4 port 23
- Sudo ufw enable
- Sudo ufw status
- telnet 10.0.2.4

After we give the above commands we see that telnetting from machine “MESH” to machine “ANI” is not successful as the machine is unable to connect to the remote host. We get the following output.

Preventing ANI from accessing oistbpl.com

Here I am trying to prevent machine "ANI" from accessing a site to Oriental Institute of Technology, Bhopal in India i.e www.oistbpl.com. So in order to do this I will have to add a rule in the firewall for blocking oistbpl.com from machine "ANI" i.e from 10.0.2.4 and since the connection will be http so I will have to block it on port 80.

To add the rule to firewall we need to have the ip address of the site we are blocking. We can find it out by using the following command:-

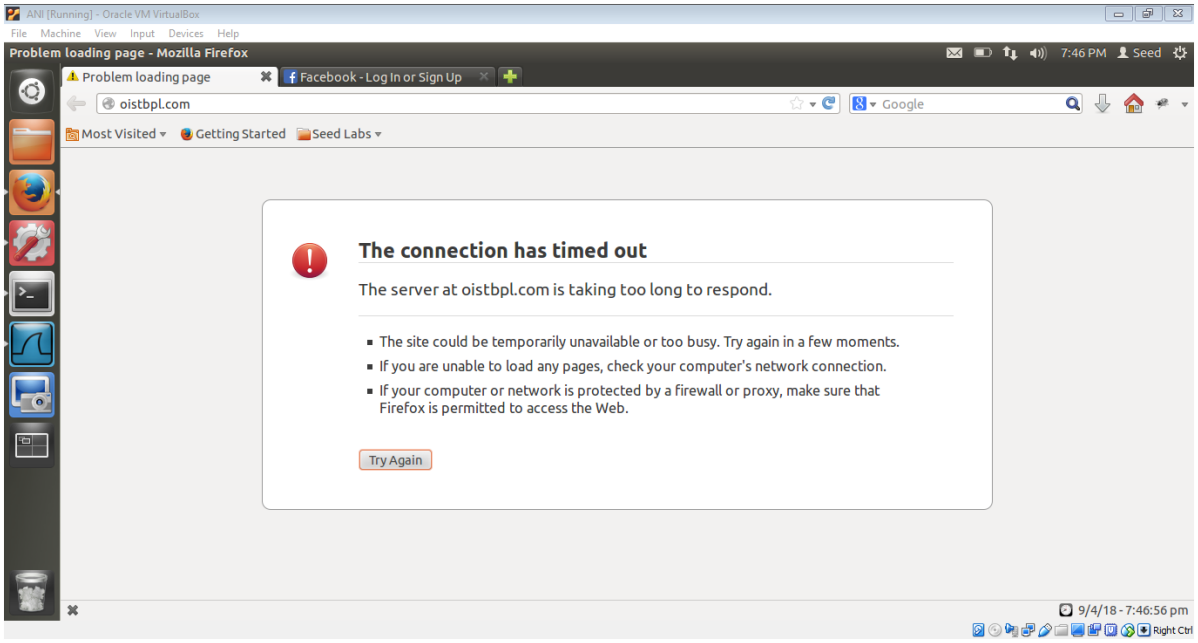
- nslookup oistbpl.com

on doing this we come to know the ip address of oistbpl.com i.e 103.251.24.104

Command that I will use to add the rule to the firewall will be:-

- sudo ufw deny out from 10.0.2.4 to 103.251.24.104 port 80

  we will also check the status of the firewall (sudo ufw status) just to be sure whether it is enabled or not. After setting up everything we will try to access oistbpl.com from the Firefox. On doing this I got the following result.

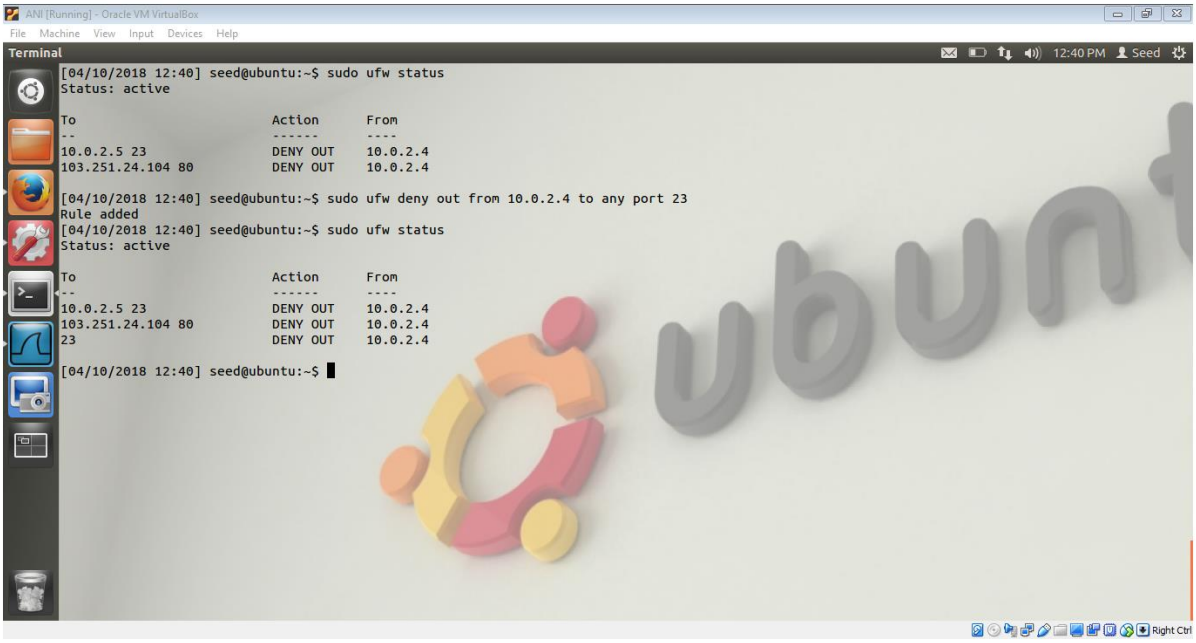


We see that we are unable to access the desired site. Apart from oistbpl.com we can access other sites like www.google.com , www.facebook.com etc. as the rule we added to the firewall just blocks the address that corresponds to www.oistbpl.com .

TASK 2 – EVADING EGRESS FILTERING

Setting up the two block rules:-

1. On macine “ANI” we will block all the outgoing traffic to external telnet servers. Command we use to add this rule to the firewall is:- **sudo ufw deny out from 10.0.2.4 to any port 23**. Also we will introduce a third machine called “JAIN”. We will enable the firewall in machine “ANI” in which we de deny all the outgoing traffic to external telnet server. Although we can run telnet server on machine “MESH” and machine “JAIN”. So we will disable the firewall for both machine “MESH” and JAIN” (sudo ufw disable) since there is no restriction on them.



MACHINE "JAIN" (IP address – 10.0.2.6)

2. Blocking all outgoing traffic from machine "ANI" to a website with static IP address. I am again opting to block www.oistbpl.com because it has got a static IP address and the rule to block machine "ANI" from accessing www.oistbpl.com is predefined. Also I deleted the recent search history so as to kill the cached pages.

TASK 2.a:

Egress Filtering is the process of restricting the information flow outsourced from one network to other network. Now the best way to evade the egress filtering is by creating a tunnel. That is exactly what we are going to do here. We will create a tunnel using SSH (Secure Shell) protocol. In this way we can bypass the firewall we created in machine "ANI" without changing any rules. So in a way we

are able to access machine “MESH”. Now we since all the firewalls in machine “MESH” and “JAIN” are disabled, we can Telnet machine “JAIN” from machine “MESH”.

NOTE:- I have created an empty file in every machine. They are:-

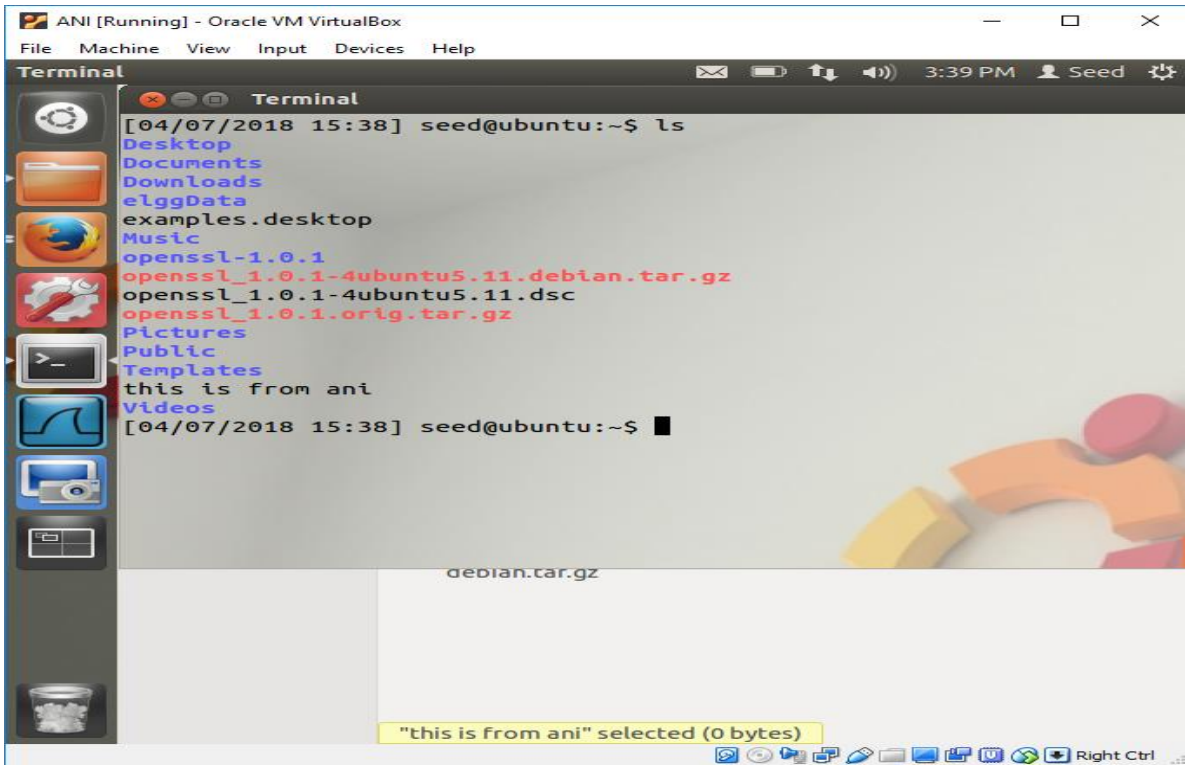
- “this is from ani” – Machine “ANI”
- “this is from mesh” – Machine “MESH”
- “This is JAIN” – Machine “JAIN”
  The purpose of creating these empty files in different machine is just to check for which machine I am in after I do SSH and Telnet from one machine to another.

Command that we will use are:-

- sudo ssh seed@10.0.2.5 – for SSH from machine “ANI” to machine “MESH”.
- telnet 10.0.2.6 – for Telneting to machine “JAIN” from machine “MESH”.

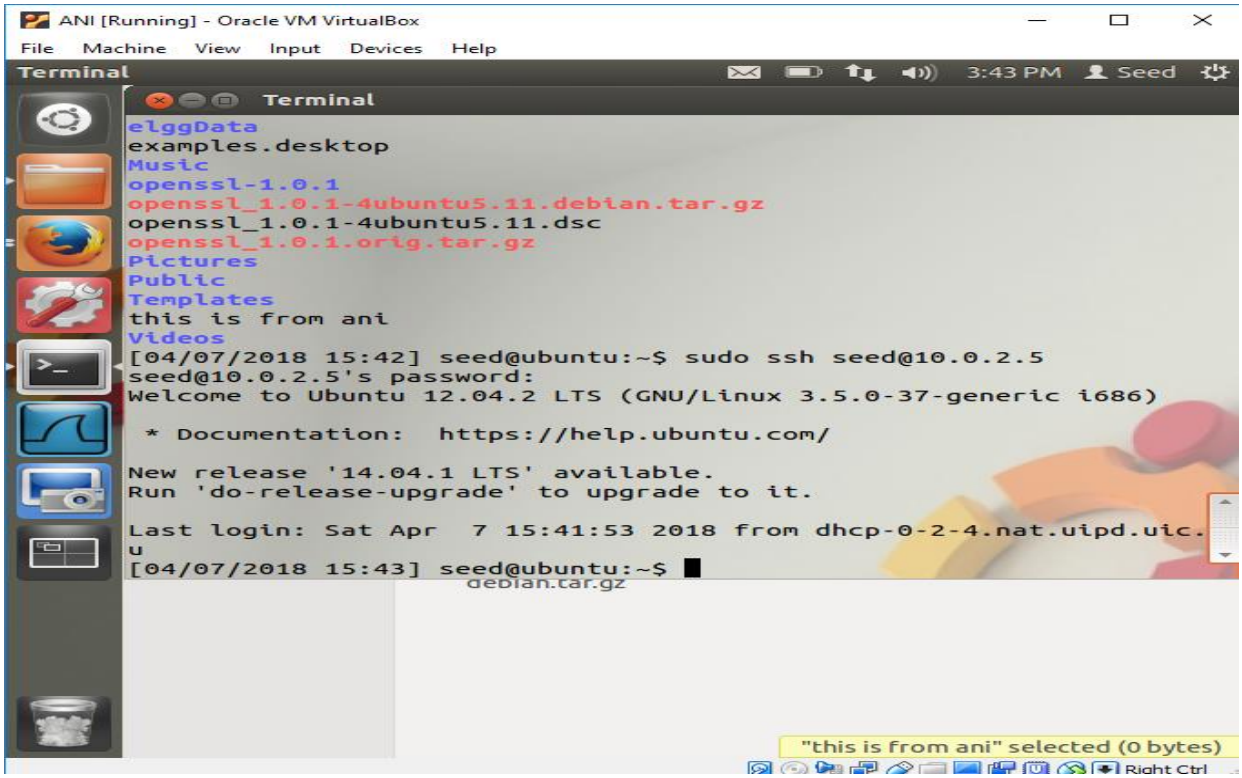
OBSERVATIONS:-

Files in Machine “ANI”

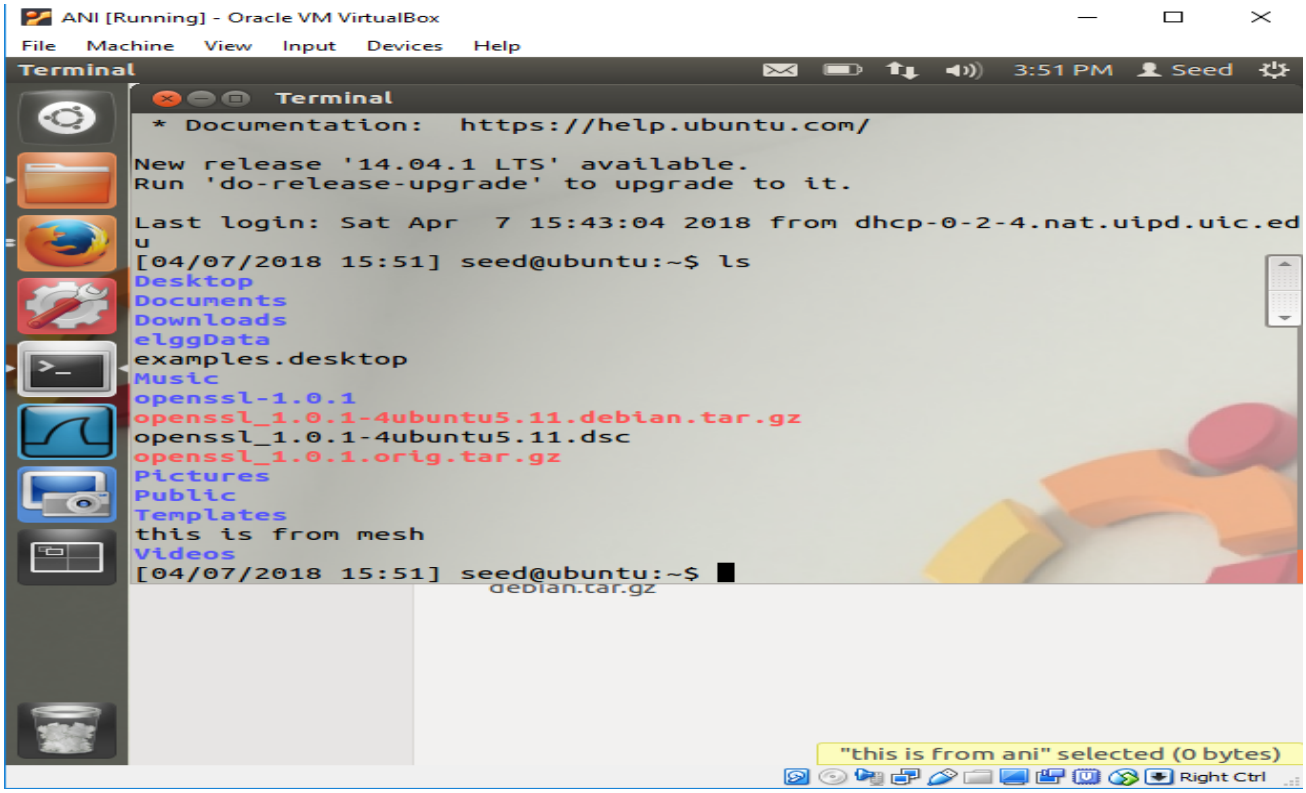


Here we can see that the file “this is from ani” is in machine “ANI”

Machine “ANI” to MAchine “MESH” through SSH



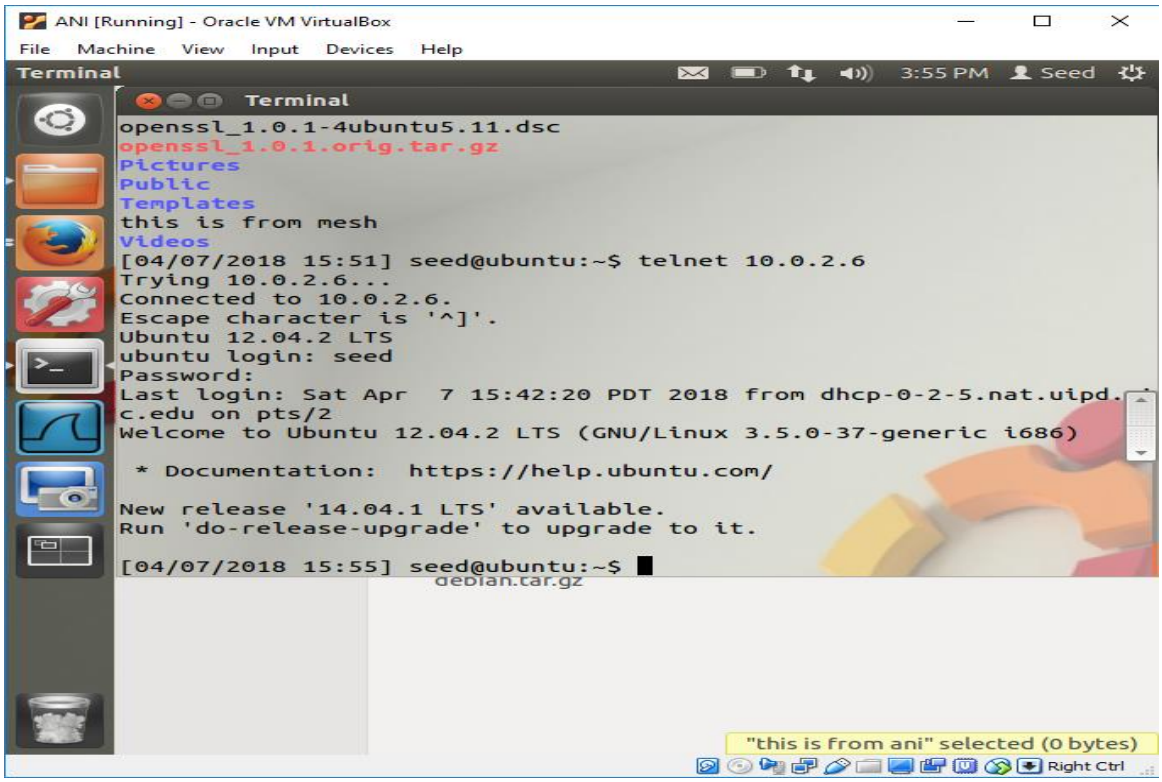
Files in Machine “ANI” after SSH to machine “MESH”



After SSH from machine “ANI” to machine “MESH” we see that the file “this is from mesh” that originally belongs to machine “MESH” is in machine “ANI”i.e I am able to access files in machine

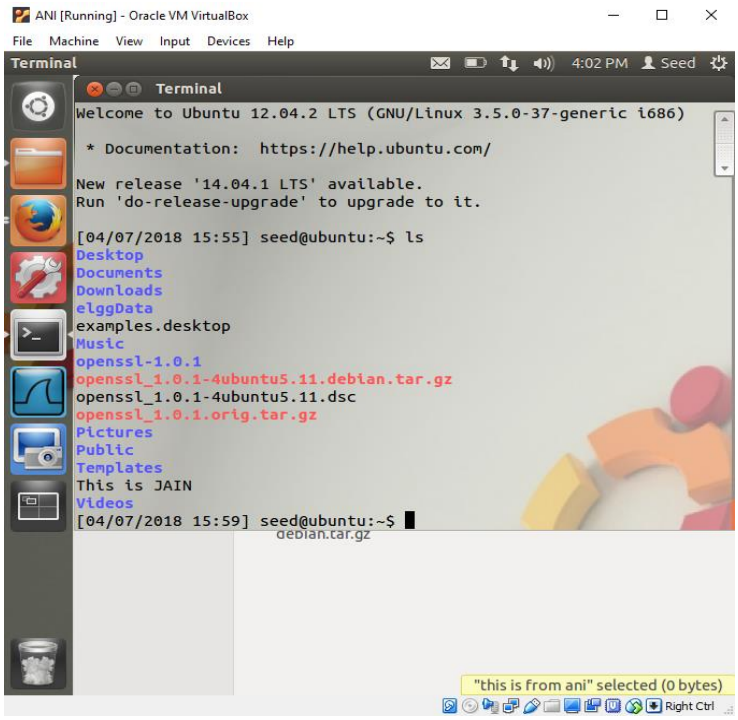
“MESH” from machine “ANI”. Earlier in Task 1 we observed that when Telnet was blocked from machine “ANI” to machine “MESH”, we were not able to gain access to machine “MESH”. But although now we did not change our firewall rules for machine “ANI” but still we are able to evade the firewall and access machine “MESH”. This is because we created a tunnel using SSH protocol.

Machine “MESH” to machine “JAIN” through Telnet

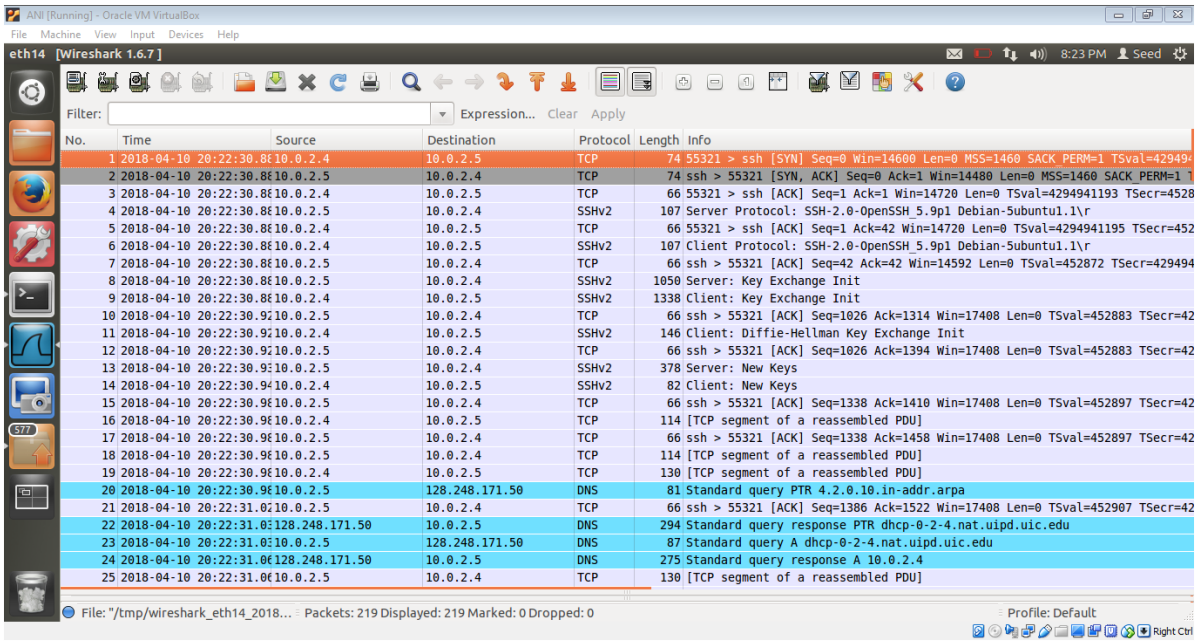


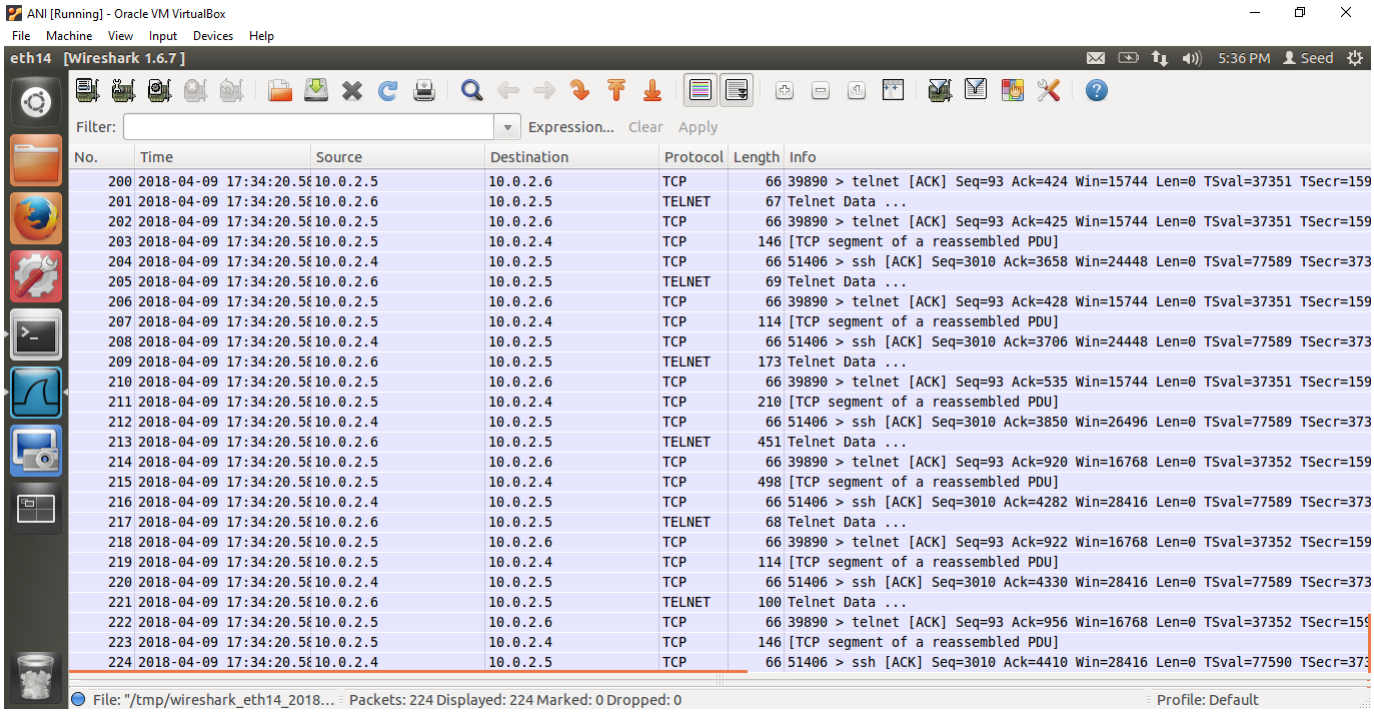
Files in machine “ANI” after Telnet to machine “JAIN” from machine “MESH”

We can see from the following screenshot that there is a file named “This is JAIN”. This is file that belongs to machine “JAIN”. So, it makes clear that machine “ANI” can access the files from machine “JAIN”. So it can be said that packets from machine “JAIN” are reaching to machine “ANI” through Telnet to Machine “MESH” and finally through SSH tunnel.



Capturing Packets through Wireshark

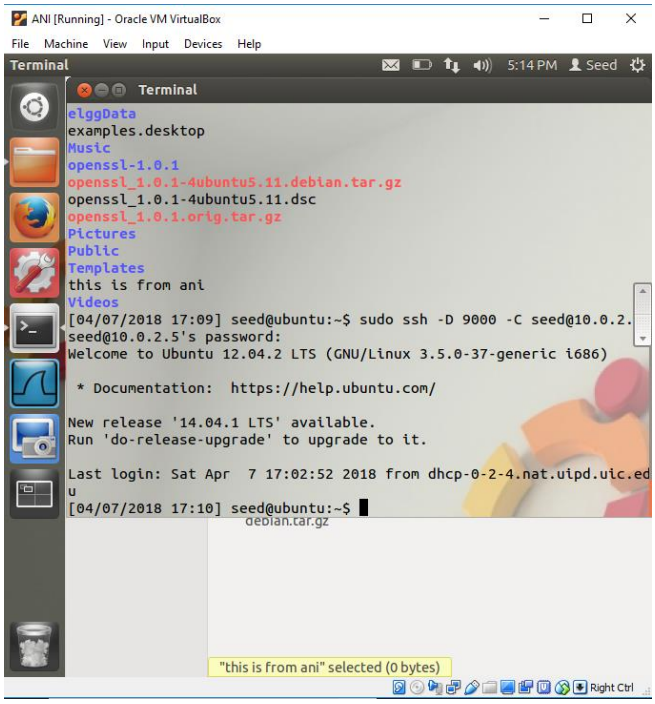


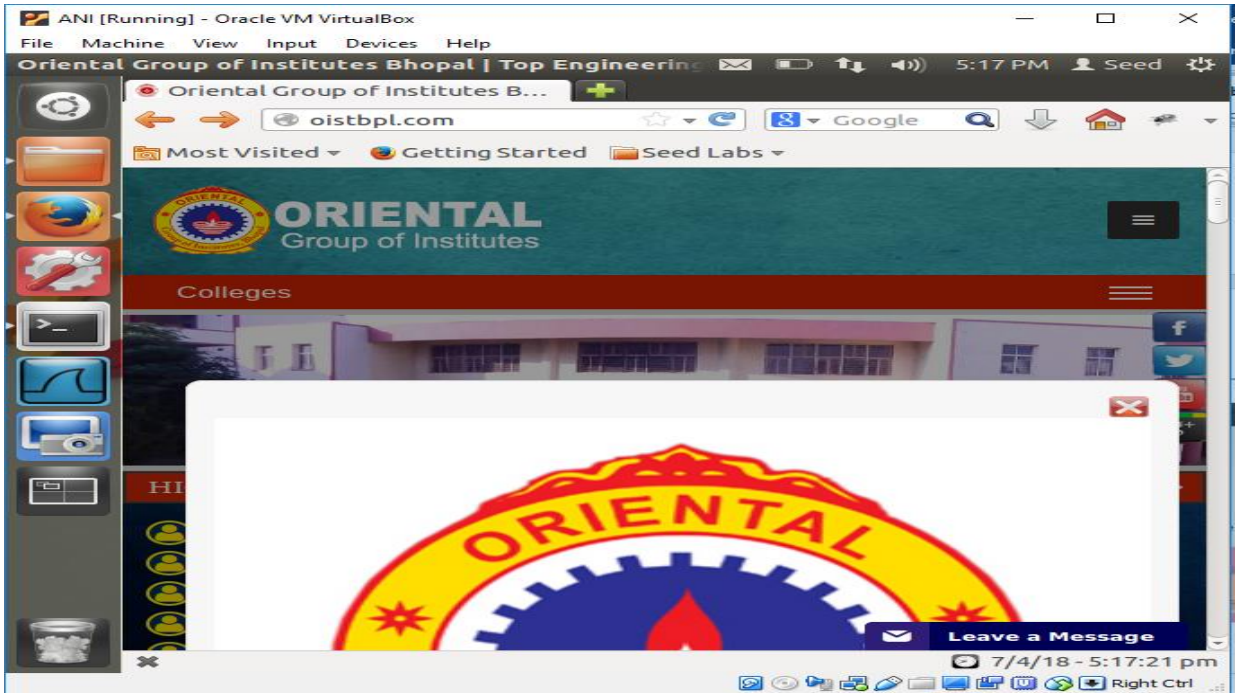


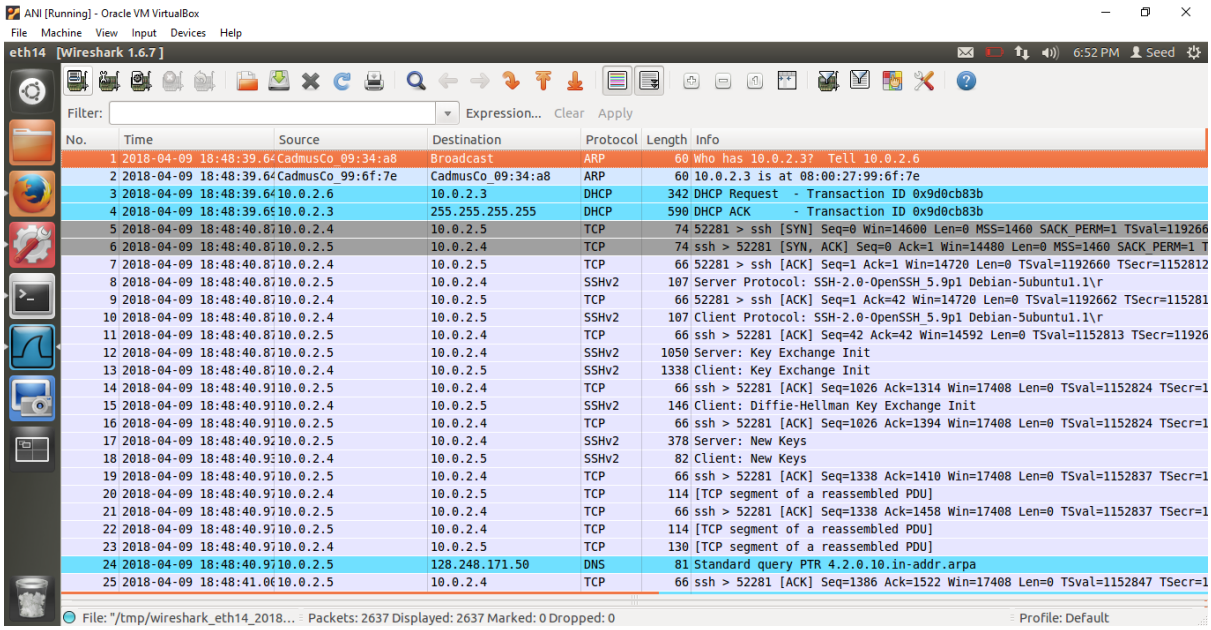
From the above two Wireshark captures we observe that machine “ANI” successfully established SSH connection with machine “MESH” and via machine “MESH” we successfully telneted machine “JAIN”.

Task 2.b:

1) Accessing oistbpl.com through machine “ANI” once the entire setup is done (i.e after changing the proxy settings and doing SSH from machine “ANI” to machine “MESH”. We observe that we are able to access www.oistbpl.com

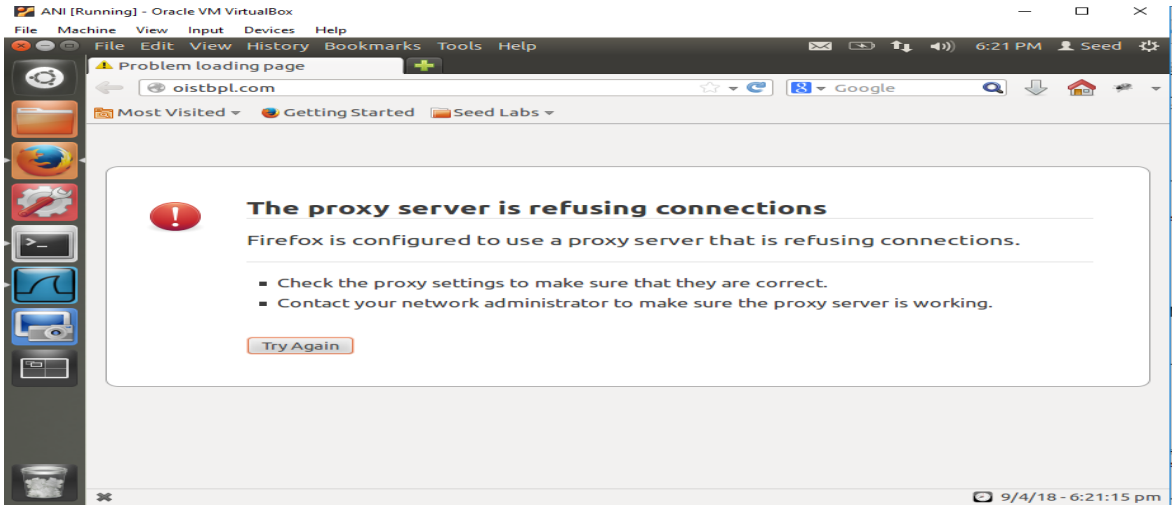




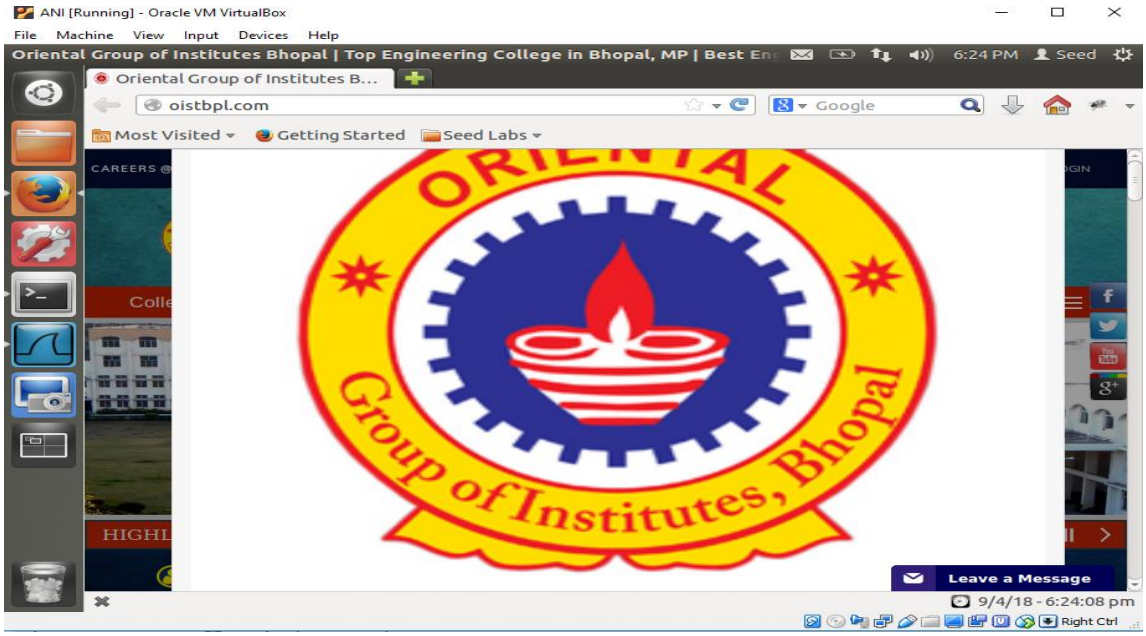


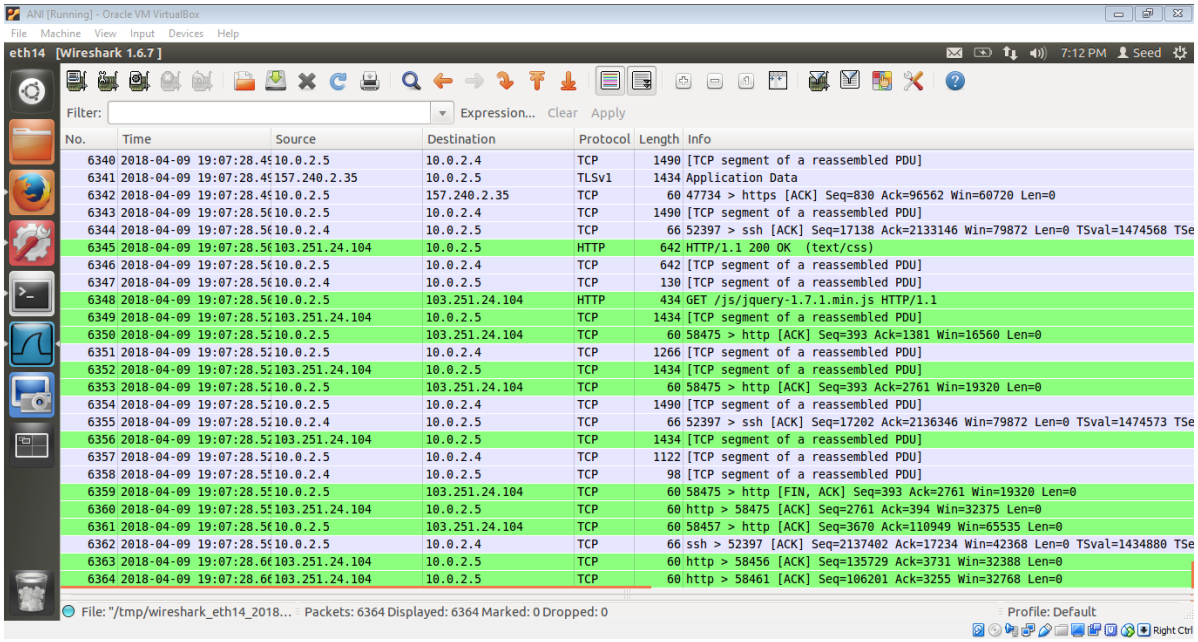
From the Wireshark pictures we observe that SSH connection between Machine “ANI” and machine “MESH” is established.

2) After breaking the SSH tunnel and clearing the Firefox cache we observe that on searching for oistbpl.com on machine “ANI” we are not able to access it as the proxy server refuses the connection.



3) On establishing the SSH tunnel connection again we observe that we are again able to access www.oistbpl.com on machine “ANI”.





From the above wireshark capture we observe that the HTTP request is successful and that is why we are able to access the website again.

TASK 3

WEB PROXY (APPLICATION FIREWALL)

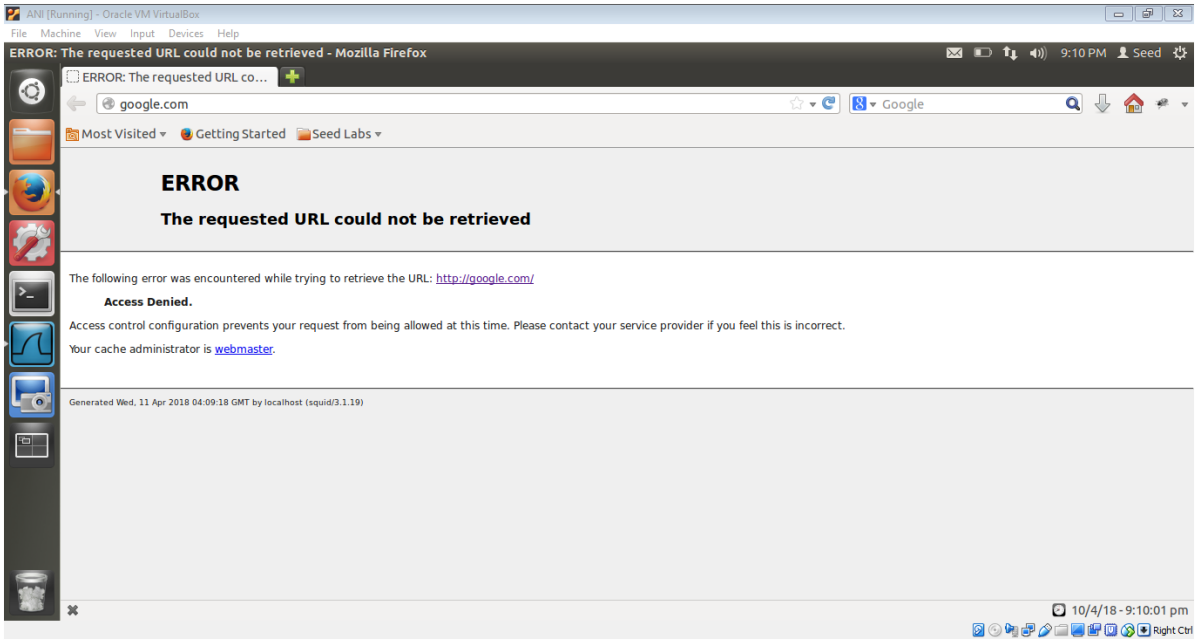
In this task we have to setup a web proxy. In this task we are using a free web proxy software called Squid. Commands we use are:-

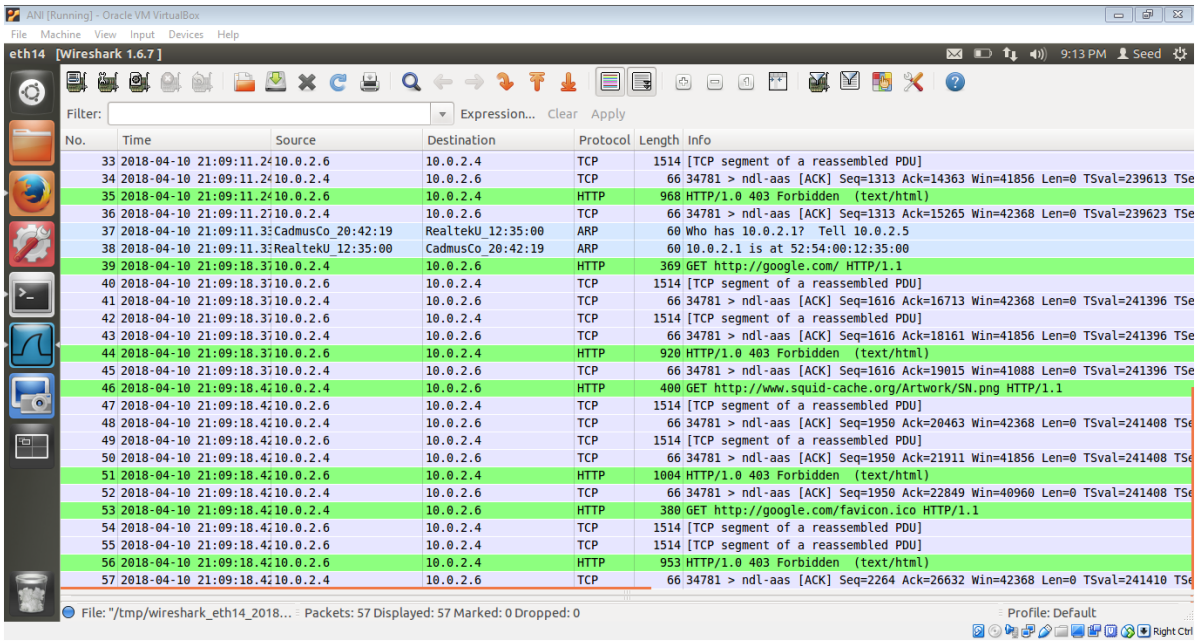
- sudo apt-get install squid (if the softwareis not installed already)
- sudo service squid3 start (to start the server)
- sudo service squid3 restart (to restart the server)

After locating the squid.conf file we can start changing the firewall policies according to our will. Only thing we have to keep in our mind is to restart the configuration file every time after making changes to it. On machine “ANI” we will restrict the browsing behavior. We will run the web proxy on machine “MESH”. We will configure the Firefox setting in machine “ANI” as told in question manual.

OBSERVATIONS:-

1). After the entire setup when I try to access www.google.com on machine “ANI”’s Firefox browser we see we are not able to access it. The result that we get is in the following screenshot.

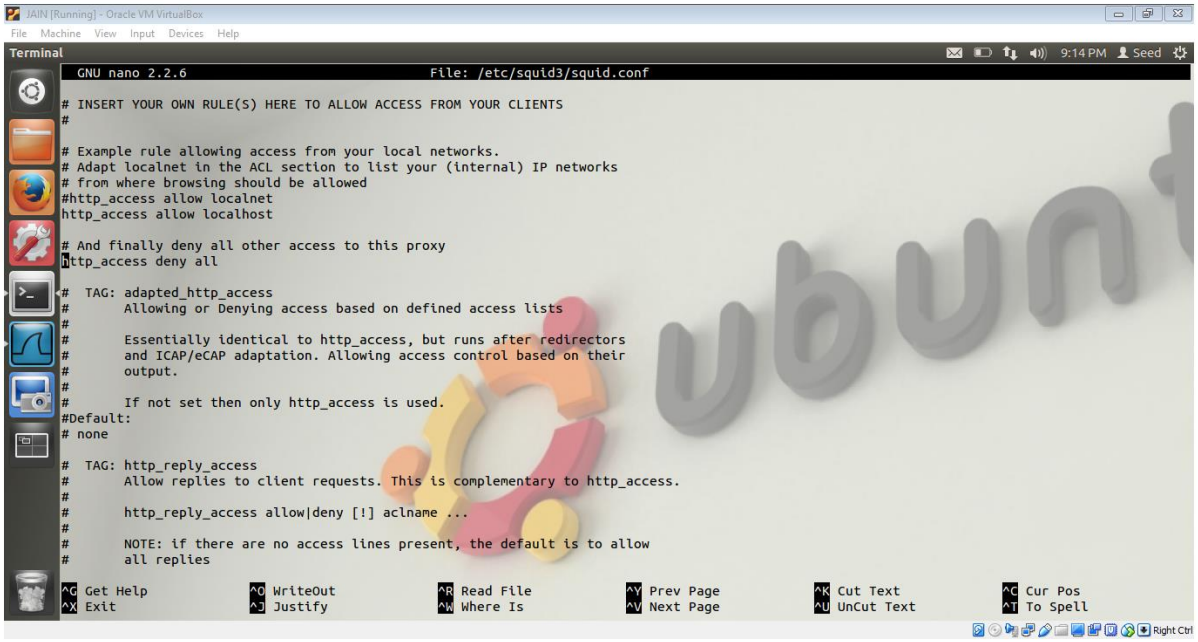




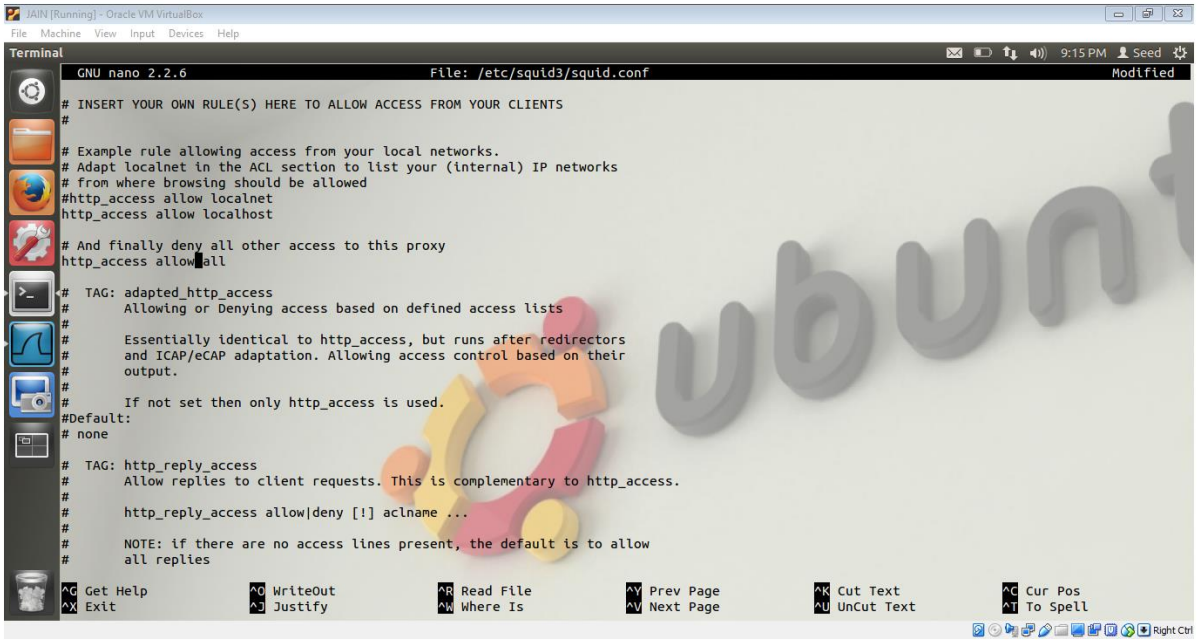
From the wireshark we observe that all the HTTP requestfrom machine “ANI” is being blocked by the squid server in machin “MESH”. It is giving a message 403 Forbidden.

2). When we have a look at the configuration file (under the http_access tag), we see that http access is denied to all the sites. So this is the reason why we were not able to access www.google.com in the previous case.

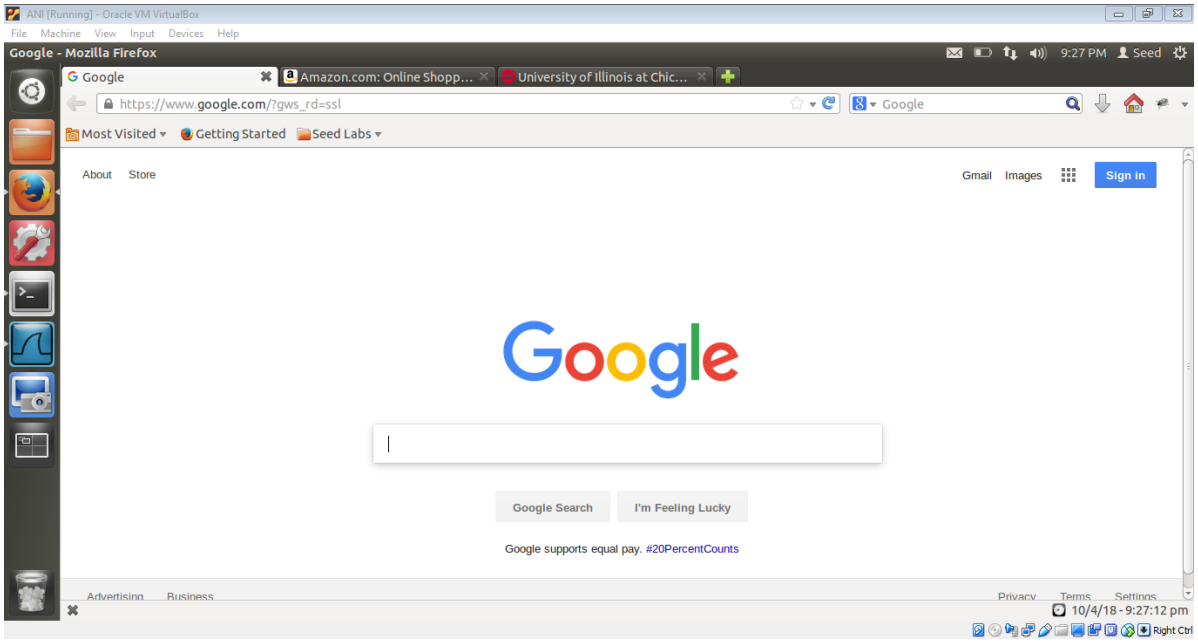
http_access deny all – denies http access to all the sites.

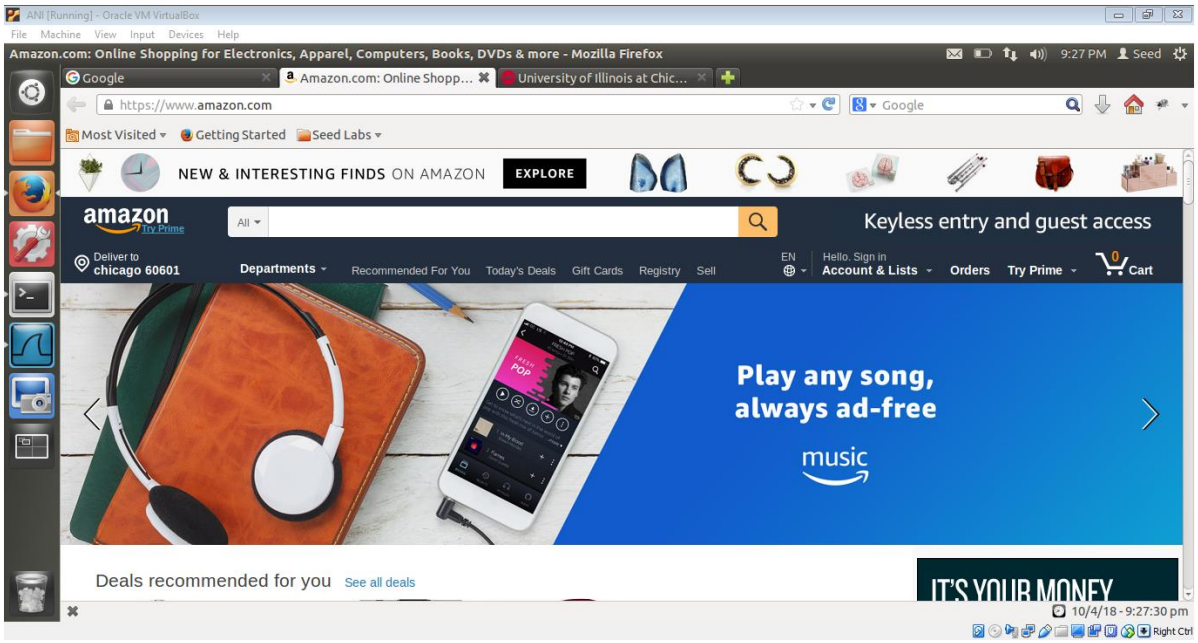


3). Making changes to the configuration file such that all the websites are allowed. We will replace http_access deny all by **http_access allow all**. This way we can access www.google.com as well as all other websites.

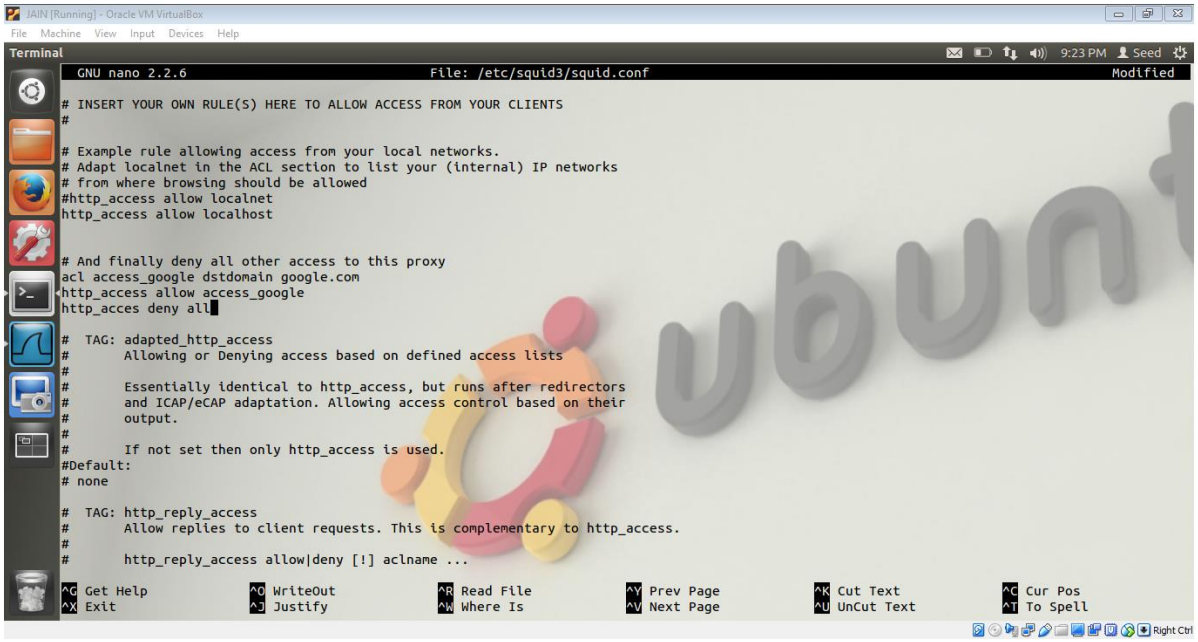


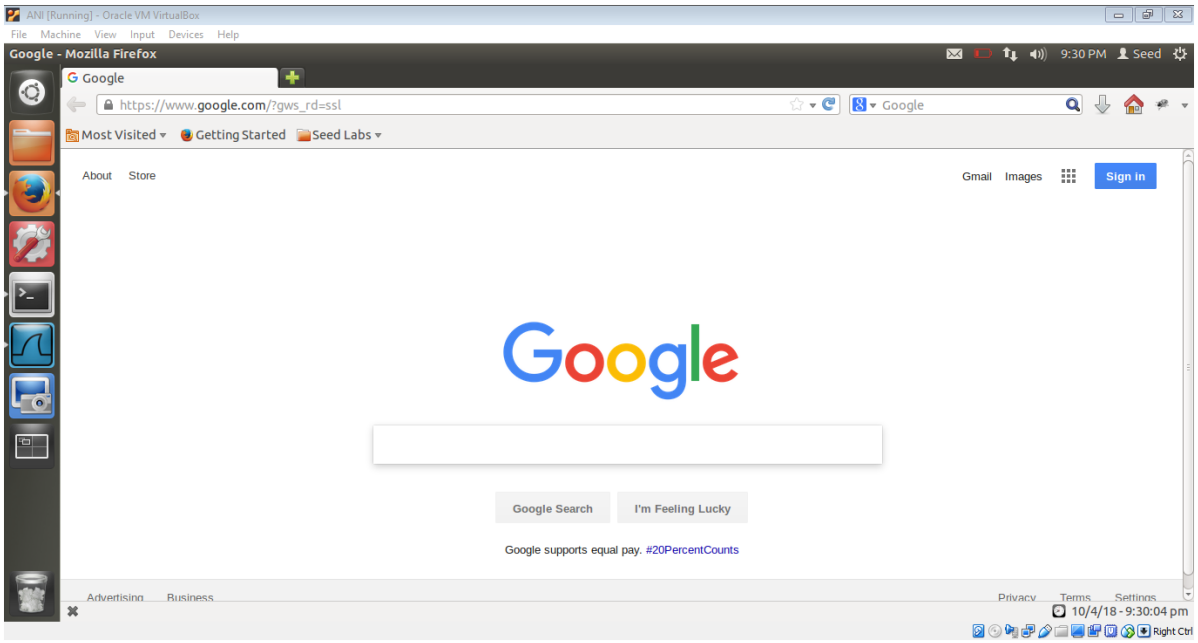
After making changes we can access google.com. Here we observe that along with www.google.com we are able to access other websites as well like www.amazon.com etc.

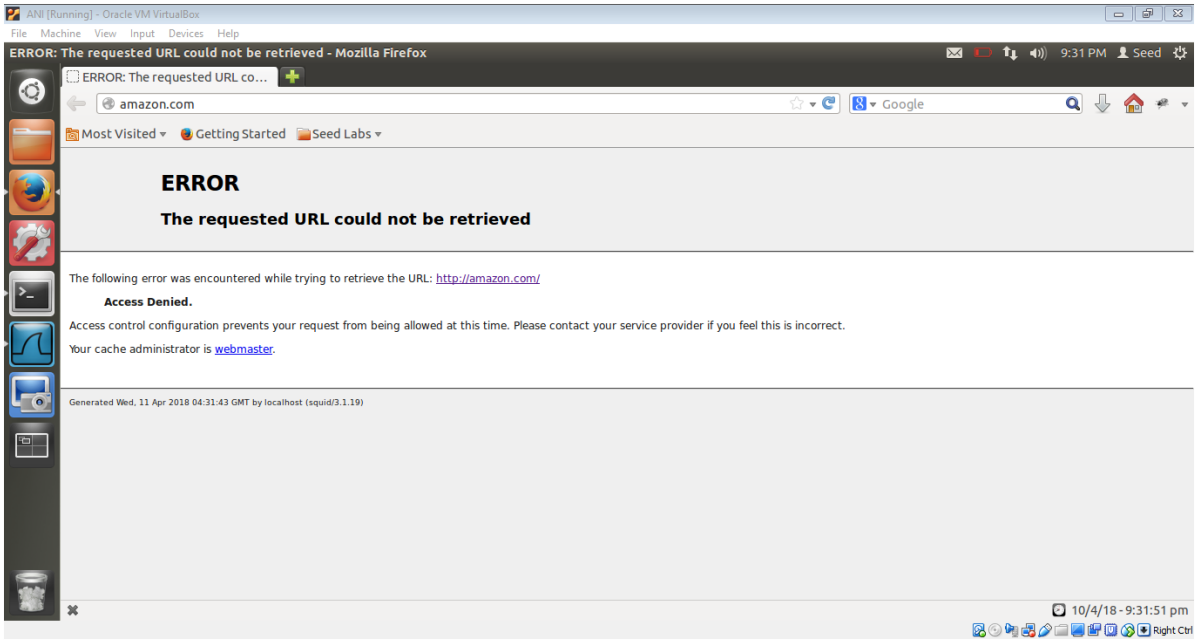




4). Making changes to the configuration file such that we allow access to google.com and blocking all other sites. Here we observe that we are able to block just www.google.com. Other sites we were able to access in the previous case are no more accessible.

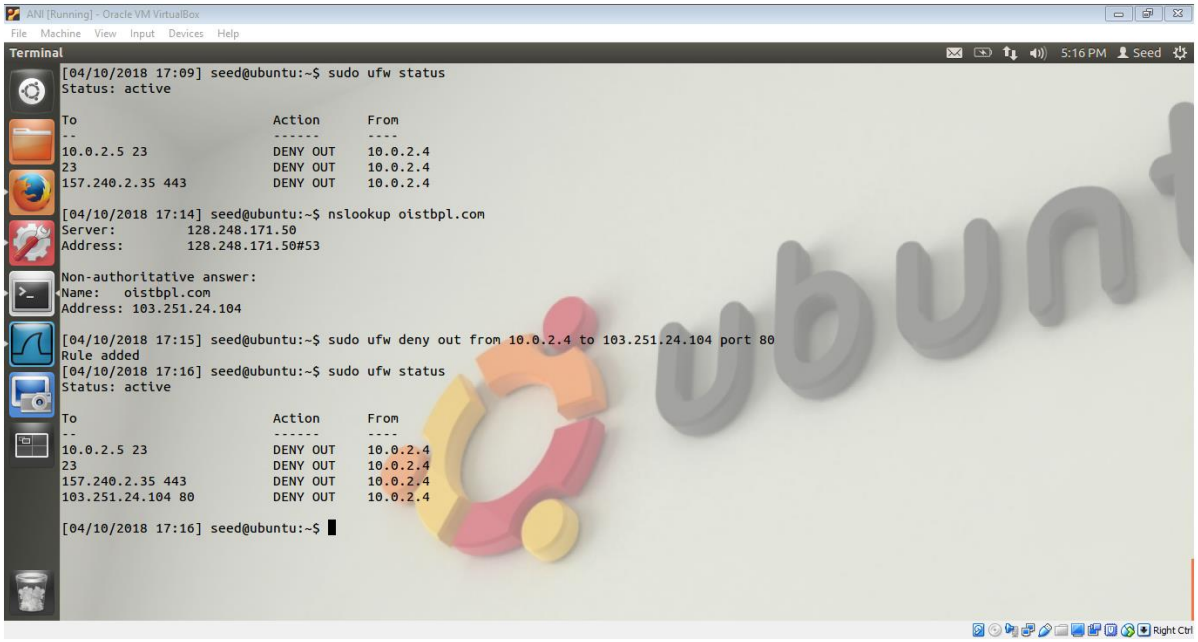

JAIN [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
9:23 PM Seed
GNU nano 2.2.6 File: /etc/squid3/squid.conf Modified
INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
from where browsing should be allowed
#http_access allow localnet
http_access allow localhost
And finally deny all other access to this proxy
acl access_google dstdomain google.com
http_access allow access_google
http_acces deny all
TAG: adapted_http_access
Allowing or Denying access based on defined access lists
#
Essentially identical to http_access, but runs after redirectors
and ICAP/eCAP adaptation. Allowing access control based on their
output.
#
If not set then only http_access is used.
#Default:
none
TAG: http_reply_access
Allow replies to client requests. This is complementary to http_access.
#
http_reply_access allow|deny [!] aclname ...
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
Right Ctrl

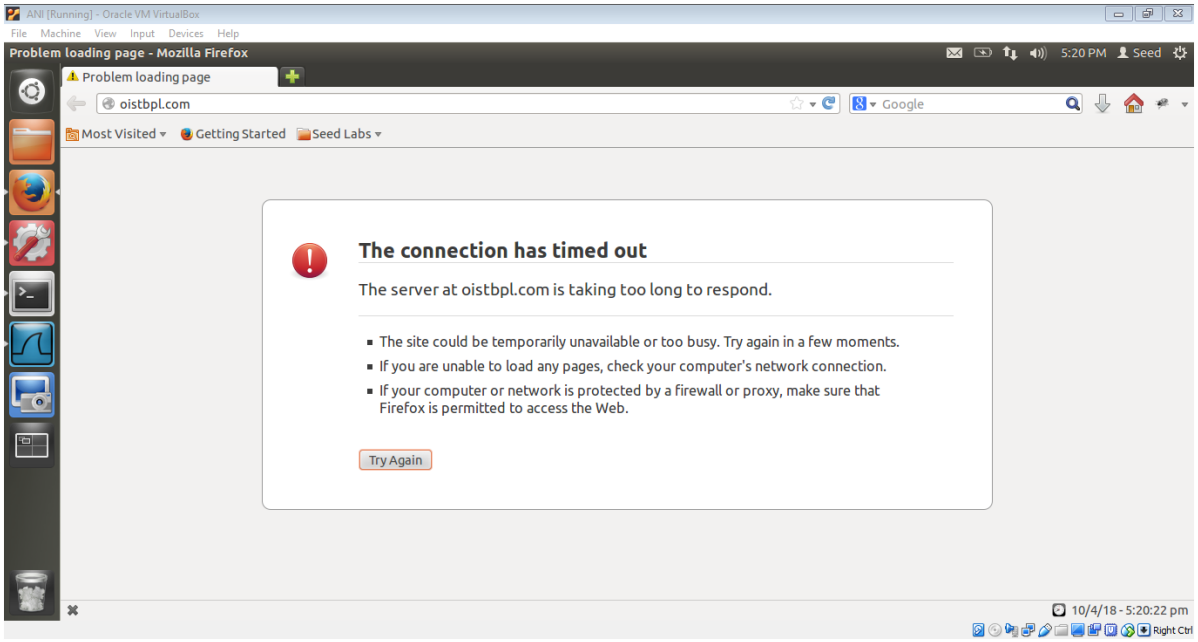

ANI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Google - Mozilla Firefox
9:30 PM Seed
Google
https://www.google.com/?gws_rd=ssl
Most Visited Getting Started Seed Labs
About Store
Gmail Images
Sign in
Google
Google Search
I'm Feeling Lucky
Google supports equal pay. #20PercentCounts
Advertising Business
Privacy Terms Settings
10/4/18 - 9:30:04 pm
Right Ctrl



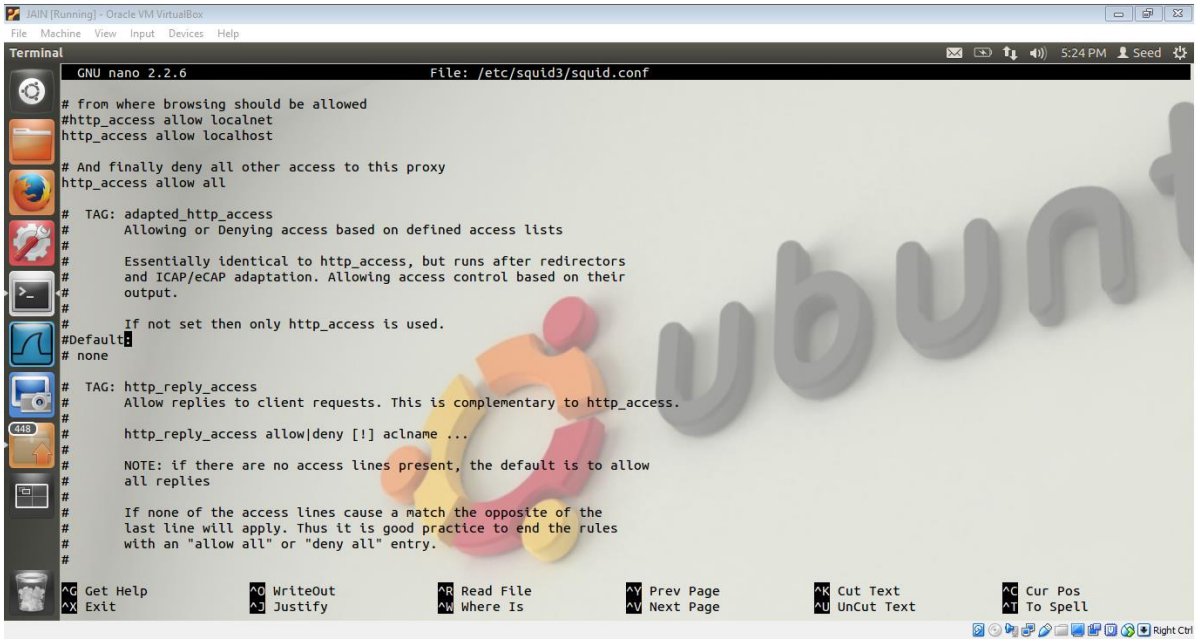
Task 3.b: Using Web Proxy to evade Firewall.

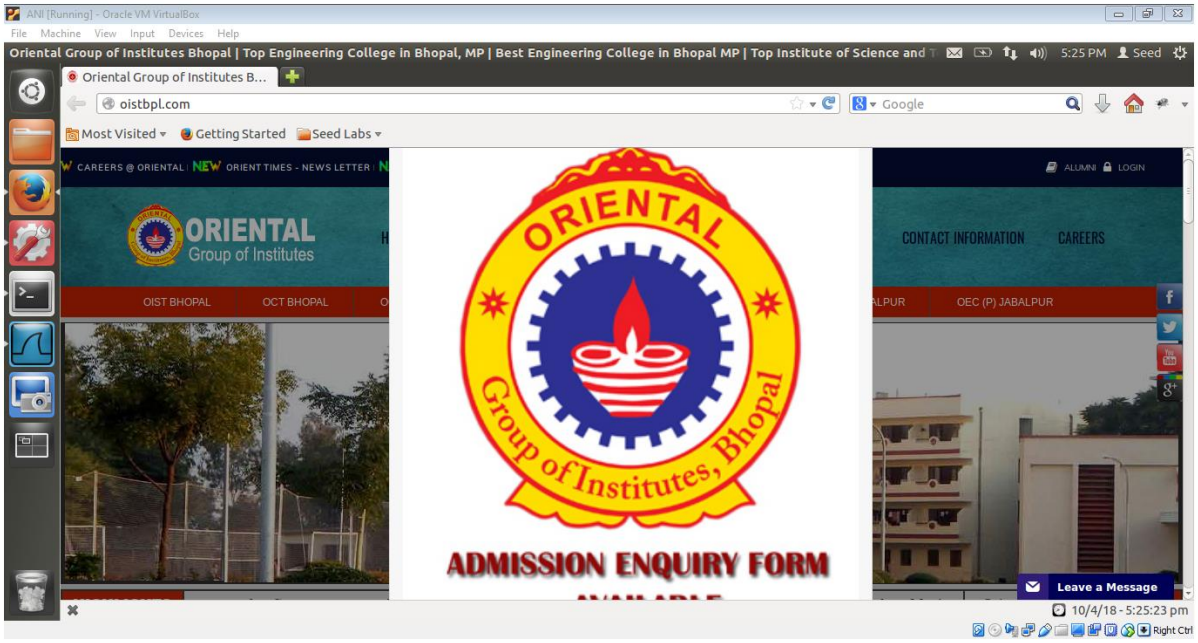
In this task we will add a rule on machine “ANI” to block www.oistbpl.com using **sudo ufw deny out from 10.0.2.4 to 103.251.24.104 port 80** command.





Now we want to access www.oistbpl.com on machine “ANI” using web proxy. So we will change the configuration in squid.conf file on machine “JAIN” such that we are able to access www.oistbpl.com even when we have blocked it on machine “ANI” using ufw command. We will give the command **http_access allow all** to do so. After doing this we observe that we are able to access www.oistbpl.com on machine “ANI”.



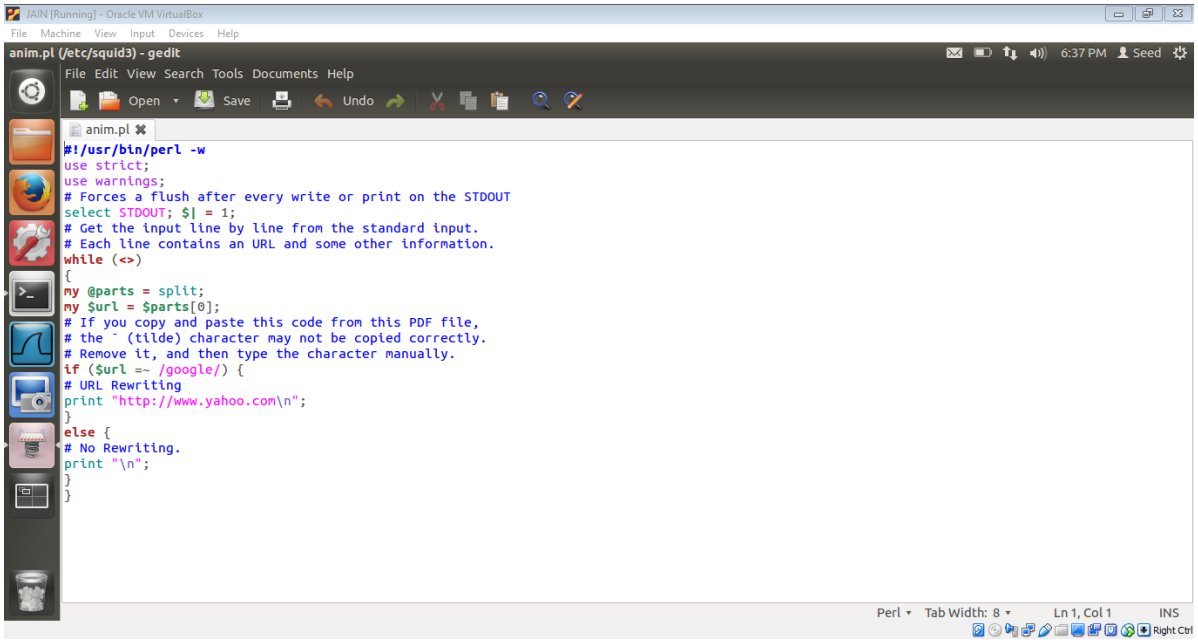


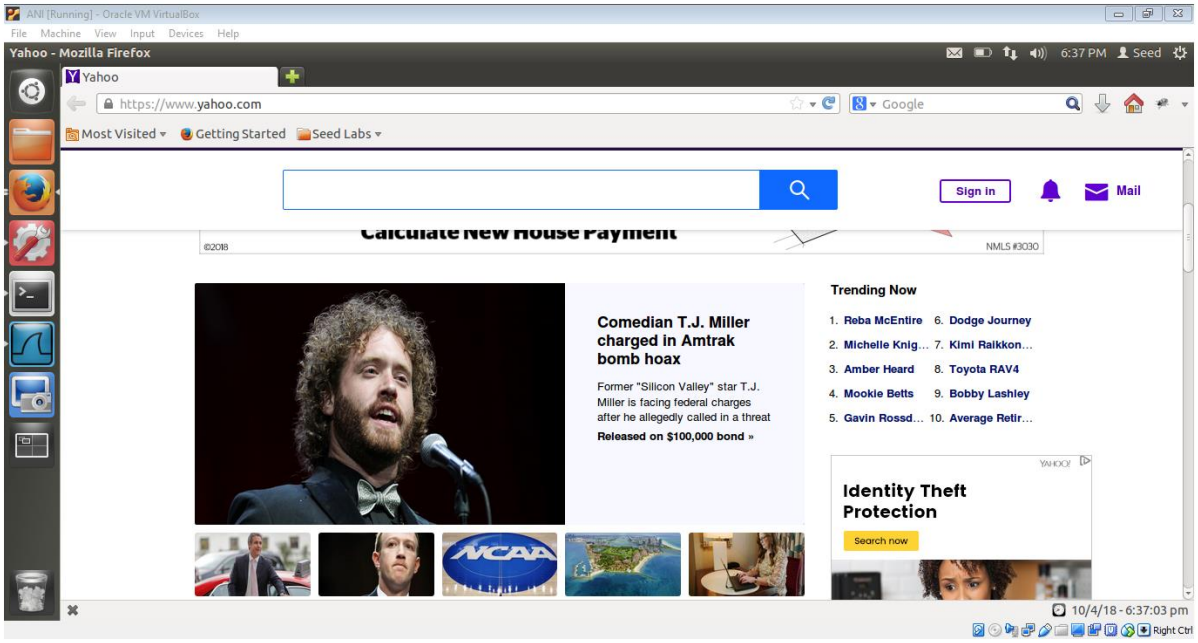
Question 3: - If ufw blocks the tcp port 3128 , can you still use web proxy to evade the firewall?

Answer 3: - Yes we can still use web proxy to evade firewall even if the ufw blocks the tcp port 3128. Squid uses the port 3128 as the default port. If it gets blocked then we can change the port in the squid.conf file.

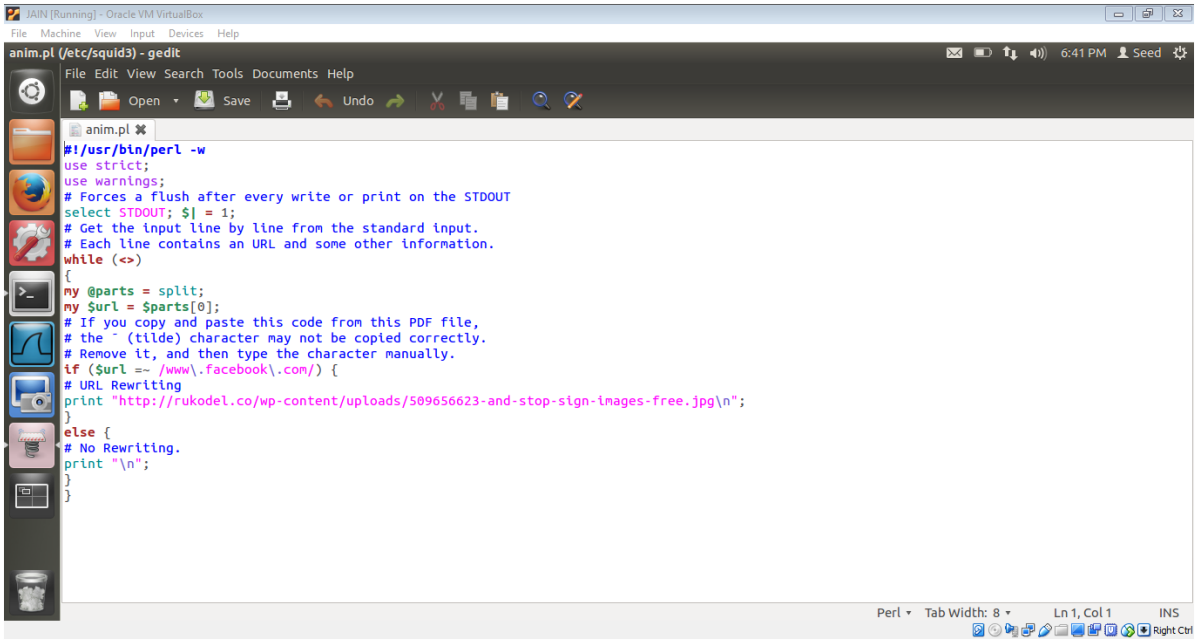
Task 3c:-

1) The command in the below screenshot performs redirecting the user on Machine "ANI" from google to www.yahoo.com. Each time we give the url as google.com we will be redirected to www.yahoo.com.

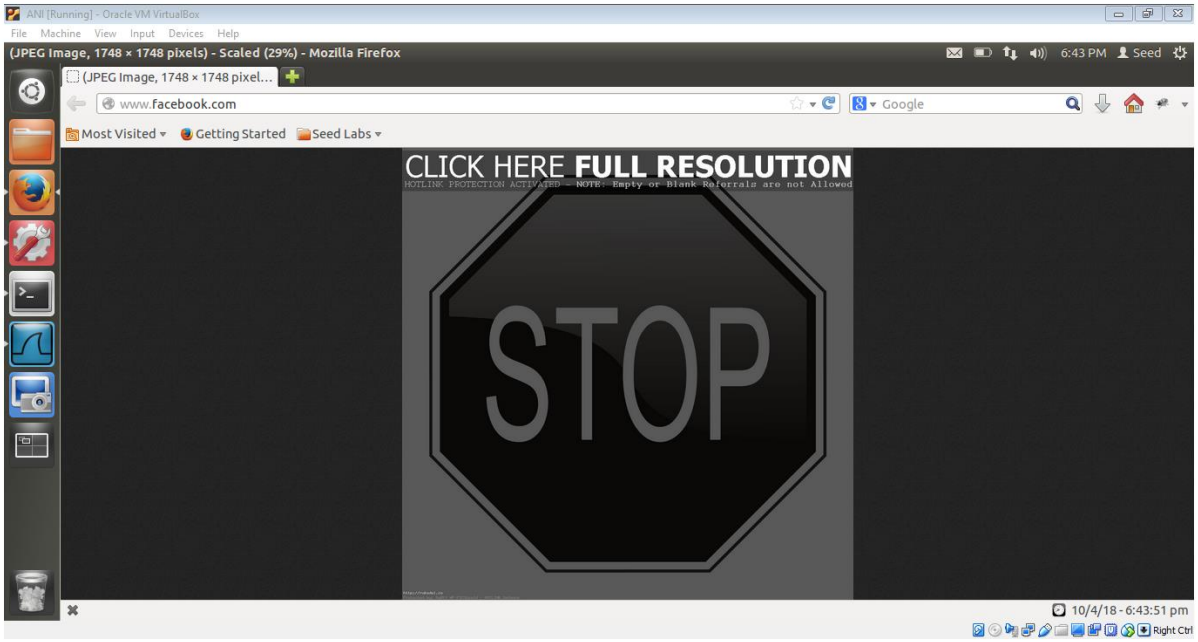



ANI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Yahoo - Mozilla Firefox
6:37 PM Seed
Yahoo
https://www.yahoo.com
Google
Most Visited Getting Started Seed Labs
Sign in
Mail
©2018
NMLS #3030
Comedian T.J. Miller charged in Amtrak bomb hoax
Former "Silicon Valley" star T.J. Miller is facing federal charges after he allegedly called in a threat
Released on $100,000 bond »
Trending Now
1. Reba McEntire
2. Michelle Knig…
3. Amber Heard
4. Mookie Betts
5. Gavin Rossd…
6. Dodge Journey
7. Kimi Raikkon…
8. Toyota RAV4
9. Bobby Lashley
10. Average Retir…
YAHOO!
Identity Theft Protection
Search now
10/4/18 - 6:37:03 pm
Right Ctrl

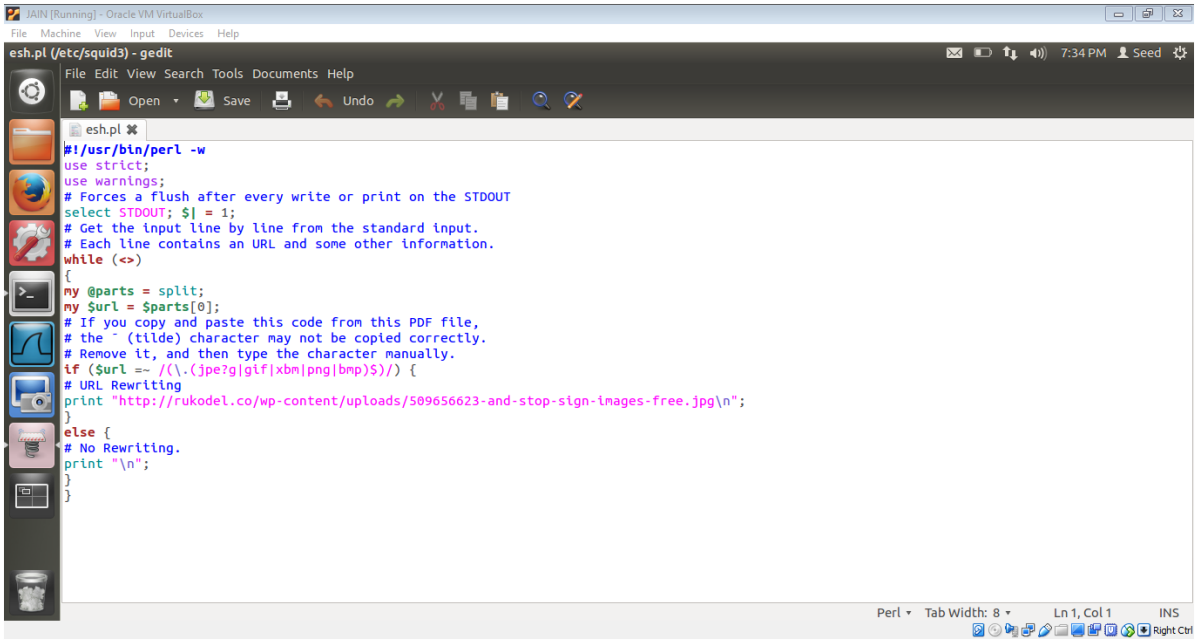
2)



In this program we changed the program in such a way that every time user on machine “ANI” tries to access www.facebook.com, the user will be redirected to http://rukodel.co/wp-content/uploads/509656623-and-stop-sign-images-free.jpg i.e a picture of a stop sign.



3)



When we give the above program, on machine “ANI” when I access any website (in my case it is www.uic.edu), all the pictures on that website will be replaced with the image whose url I provided.