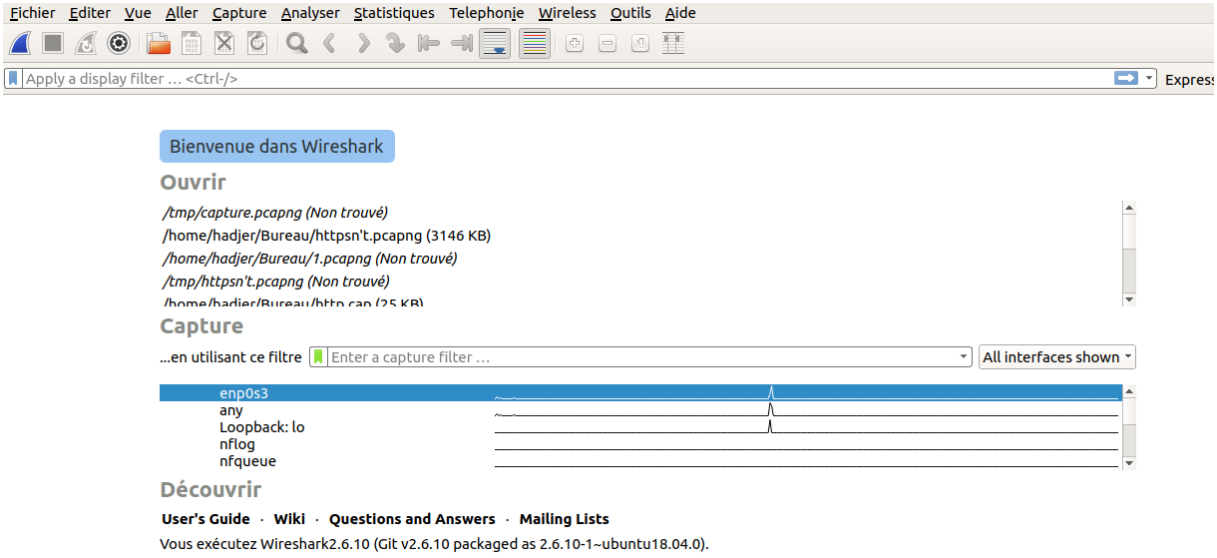
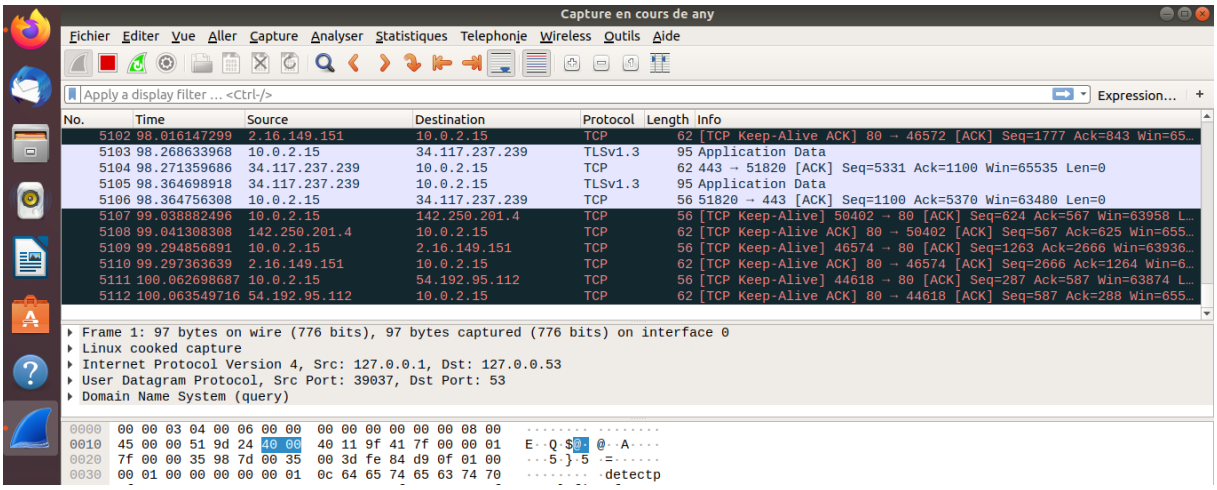
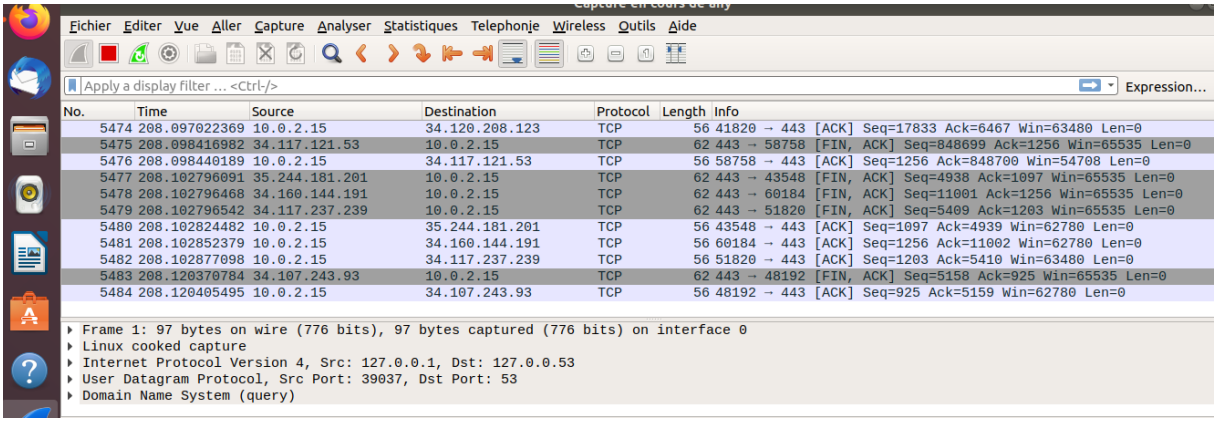
# Network Security checkpoint :

## Act1 :




after opening browser and search, we get the cptures :



Act 2 :

Step 1 - Configure NAT to Allow Hosts to Go Out to the Internet:

Comandes :

object network obj_any

subnet 0.0.0.0 0.0.0.0

nat (inside,outside) dynamic interface

Step 2 - Configure NAT to Access the Web Server from the Internet:

Assuming the web server's private IP is 192.168.1.100, you'll need a static NAT for inbound traffic to reach the server.

Comandes :

object network web_server

host 192.168.1.100

nat (dmz,outside) static 198.51.100.101

Step 3 - Configure ACLs:

Comandes :

Create an ACL to permit outbound traffic from inside and DMZ to the outside:

access-list outside_access_in extended permit ip any any

Create an ACL to permit inbound traffic from the Internet to the DMZ web server:

access-list outside_access_in extended permit tcp any object web_server eq www

Apply the ACLs to the respective interfaces:

access-group outside_access_in in interface outside

Step 4 - Test Configuration with the Packet Tracer Feature:

You can use the Packet Tracer feature to simulate traffic and check if your ACLs and NAT configurations are working as expected

packet-tracer input outside tcp 203.0.113.1 12345 198.51.100.101 www