Date: 25 - 04 - 2021

**Lab Assignment No: - 6**

# Aim: Installation of WireShark

**Lab Outcome Attained:**

LO 5: -To observe and study the traffic flow and the contents of protocol frames.

# Theory: -

Wireshark: -

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. You could think of a network packet analyzer as a measuring device for examining what’s happening inside a network cable, just like an electrician uses a voltmeter for examining what’s happening inside an electric cable (but at a higher level, of course).

Wireshark intercepts traffic and converts that binary traffic into human-readable format. This makes it easy to identify what traffic is crossing your network, how much of it, how frequently, how much latency there is between certain hops, and so forth.

While Wireshark supports more than two thousand network protocols, many of them esoteric, uncommon, or old, the modern security professional will find analyzing IP packets to be of most immediate usefulness. The majority of the packets on your network are likely to be TCP, UDP, and ICMP.

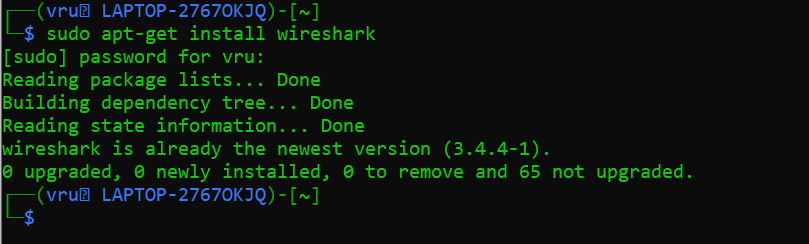
Uses of Wireshark: -

1. It is used by network security engineers to examine security problems.
2. It allows the user to watch all traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can help to analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

# Screenshots

**Installation Process: -**

* 1. Using advanced Package Tool to download and install the wireshark software:
     + Sudo apt-get install wireshark

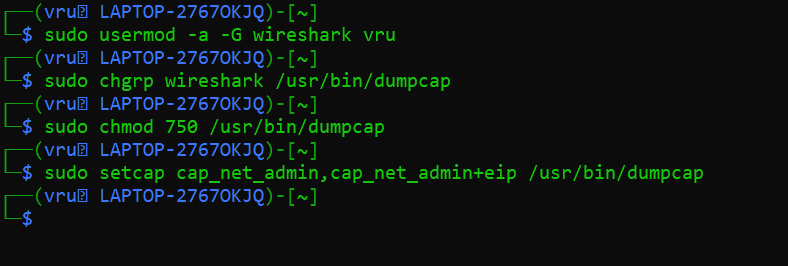


* 1. Creating a group called wireshark
     + Sudo groupadd wireshark
  2. Modify the user. a: append –G: group (appending user to the group named wireshark)
     + Sudo usermod –a –G wireshark YOUR\_USER\_NAME
  3. Changing group ownership
     + Sudo chgrp wireshark /usr/bin/dumpcap
  4. Modifying permissions for the given fie location 7: Owner can read, write, execute

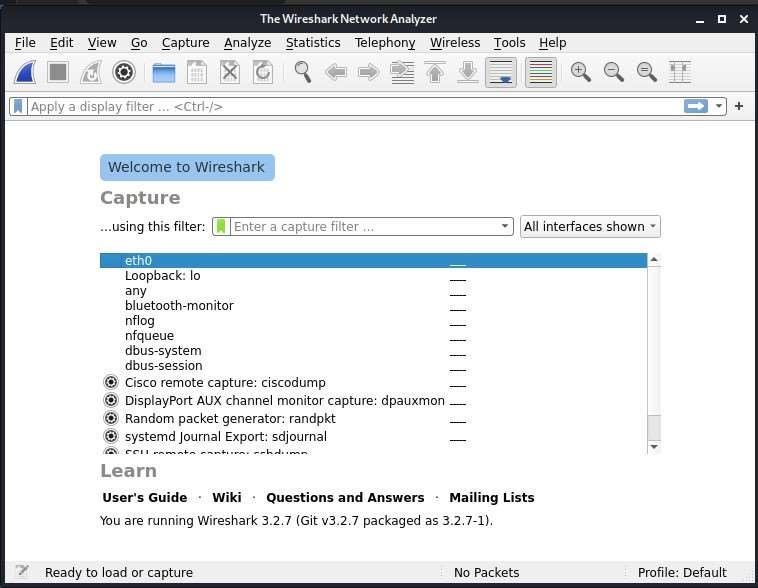
5: Group can read, can’t write and execute

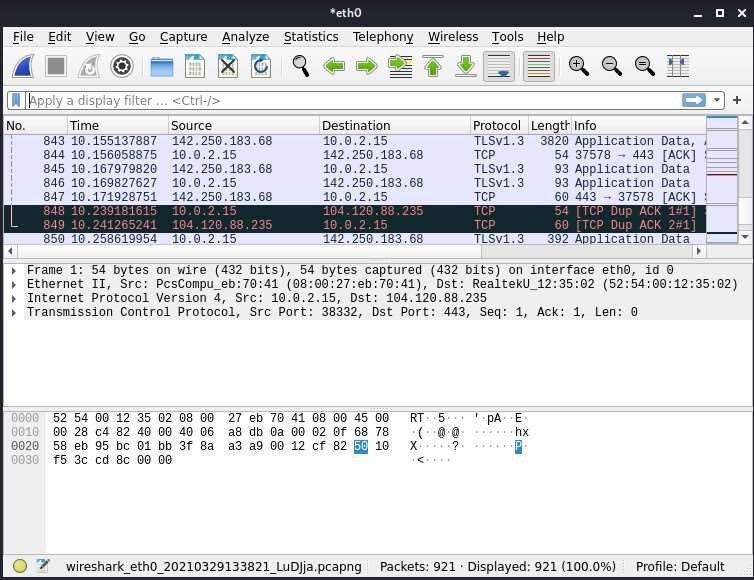
0: others can’t read, can’t write and can’t execute

* + - Sudo chmod 750 /usr/bin/dumpcap
  1. Capabilities cap\_net\_raw, cap\_net\_admin are added to the permitted sets and the effective bit is set.
     + Sudo setcap cap\_net\_raw,cap\_net\_admin=eip /usr/bin/dumpcap
  2. Display the name and capabilities
     + Sudo getcap /usr/bin/dumpcap



* 1. Running wireshark



* 1. Example of wireshark capturing packets transmitting

**Conclusion:** Therefore, wireshark was successfully installed and captured its packets.