WIRESHARK

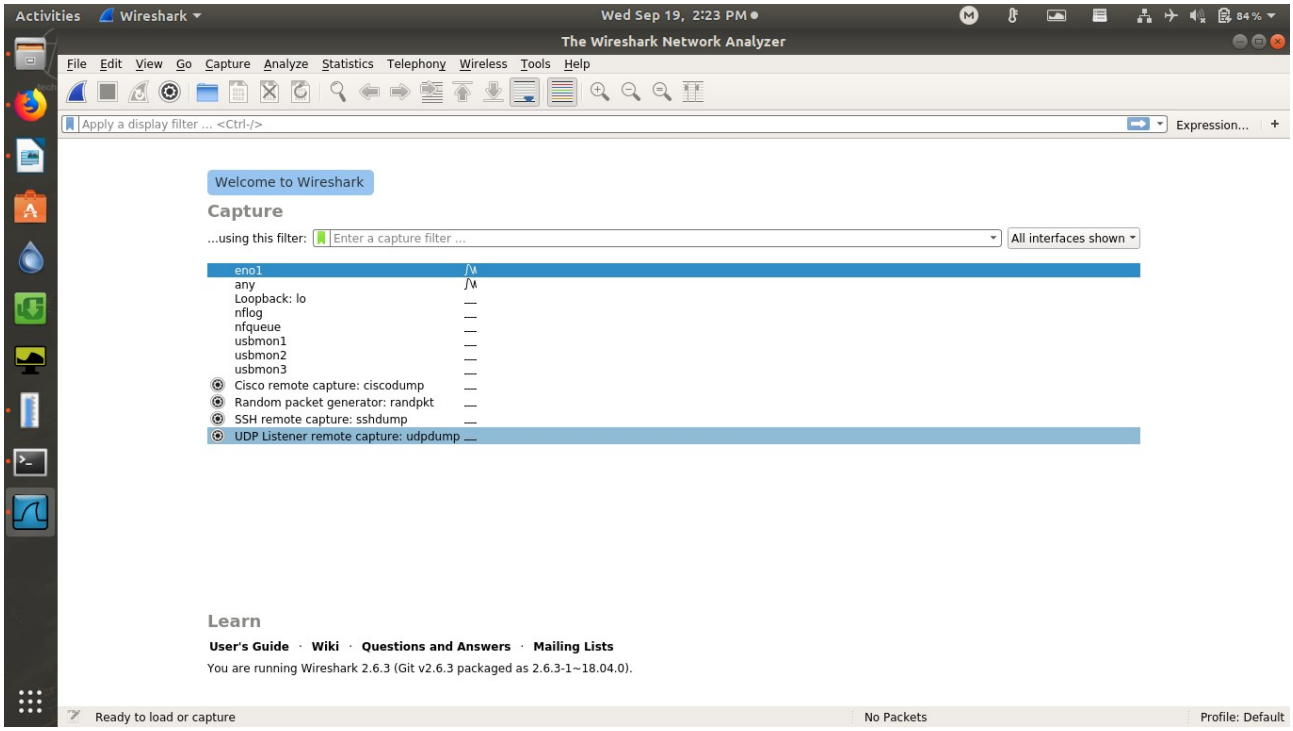
Introduction :

- It is the most popular open source network sniffer and packet / protocol analyzer solutions.
- It was previously known as ethereal . But renamed as wireshark.

Features :

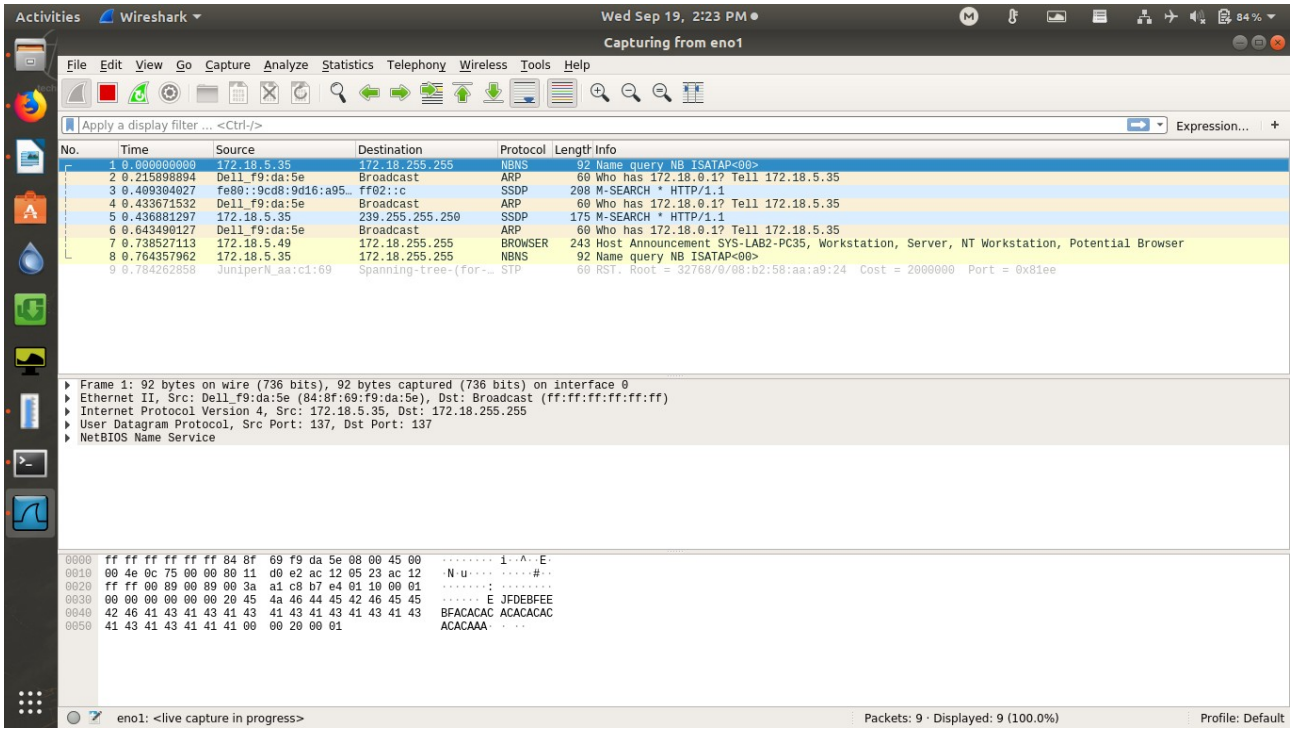
- Live data capture
- support for offline protocol analysis
- Enriched UI
- Supports almost all network , application and transport protocols.
- Display packets with very detailed protocol information
- Save captured packet data.

wireshark main window :

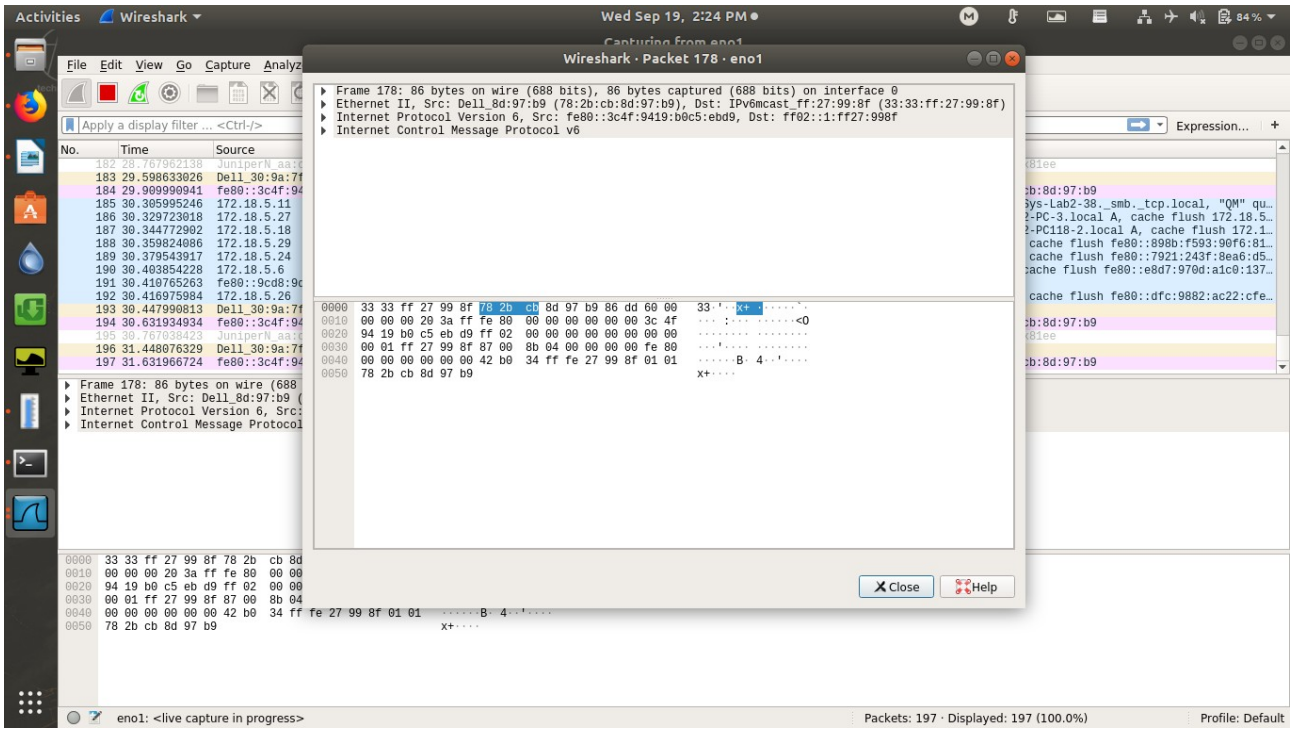


WIRESHARK

Ethernet interface monitoring :



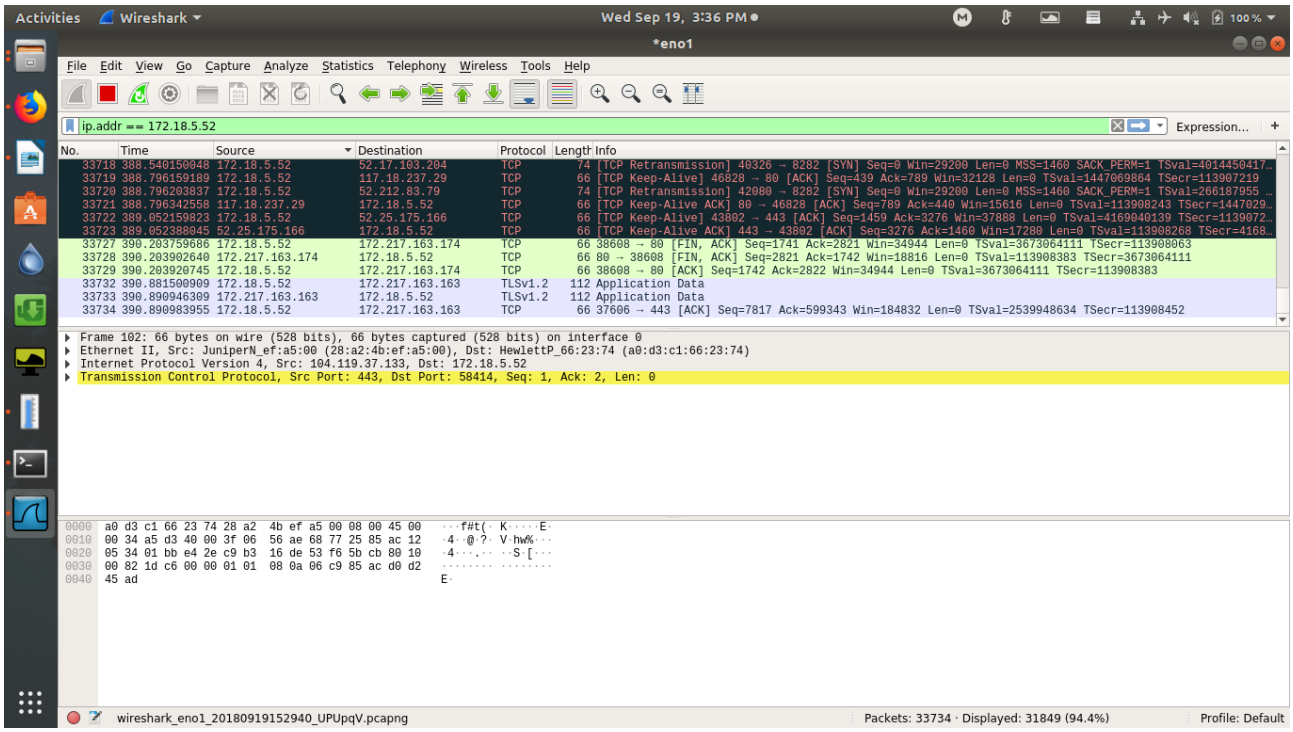
Packet details :



WIRESHARK

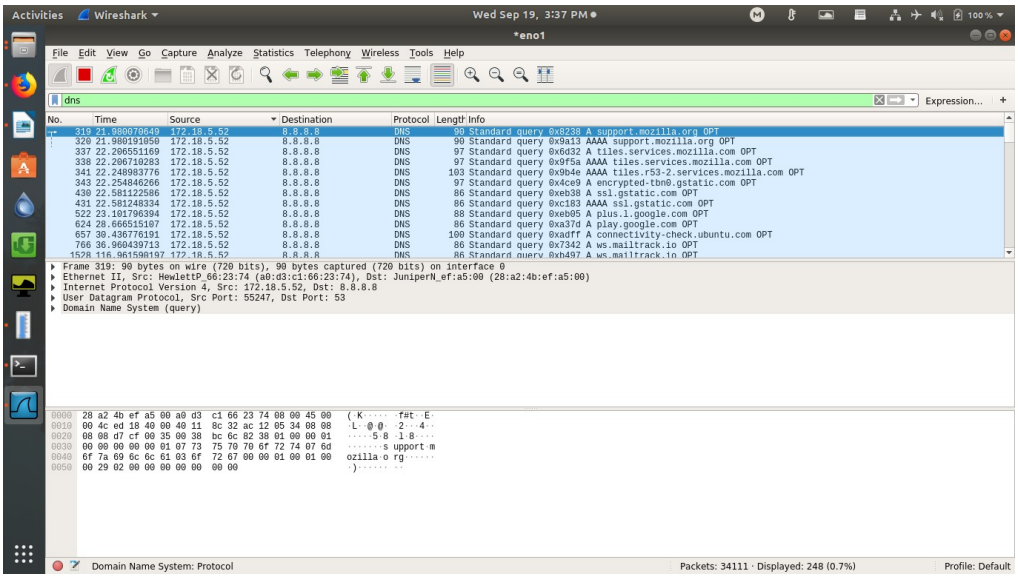
filter packet by ip address

syntax :ip.addr == <ip_addr> -> put this in display filter



filter packet by protocol name

syntax : <protocol> -> put this in display filter



WIRESHARK

FIND Packet :

if you want find the syn packet for some specific ip address then go to EDIT --> Find packet then enter

syntax : ip.src == <ip.addr> and tcp.flags.syn==1