CNS: EXPERIMENT - 8

Aim:
Study of packet sniffer tools Wireshark :-

a. Observer performance in promiscuous as well as non-promiscuous mode.
b. Show the packets can be traced based on different filters
   Port Filters, Address Filters, Protocol Filters, String Filters

Theory:
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).

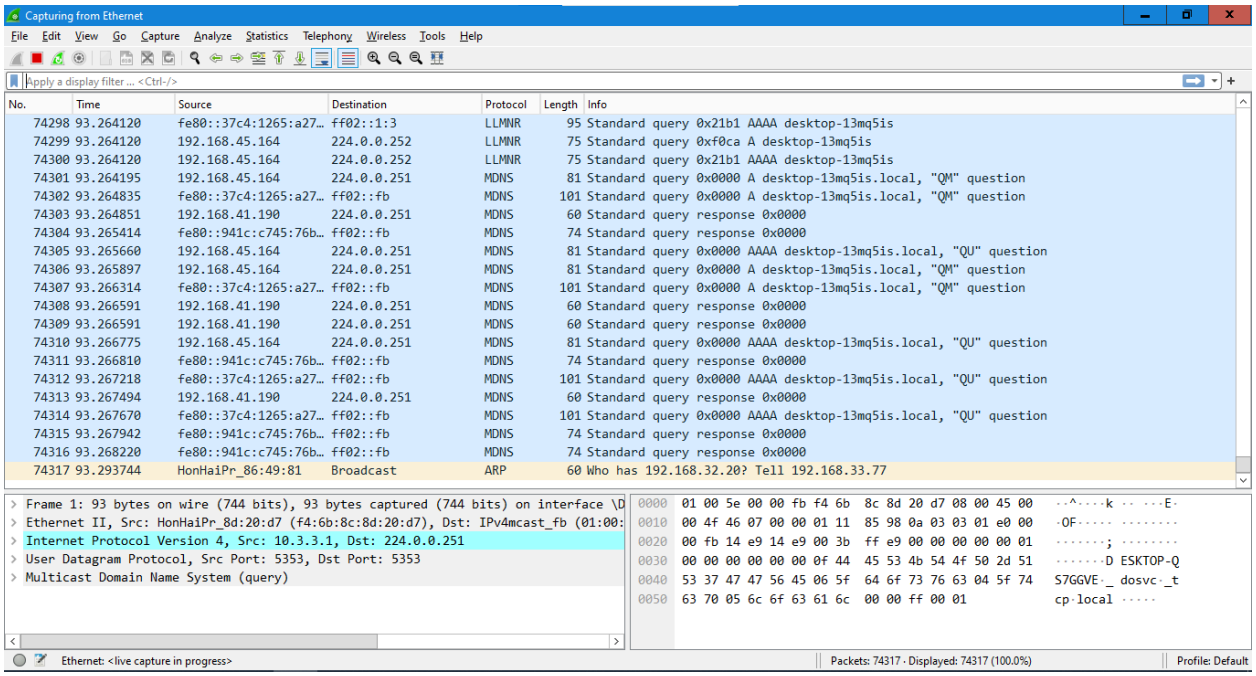
In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Applications of wireshark:-

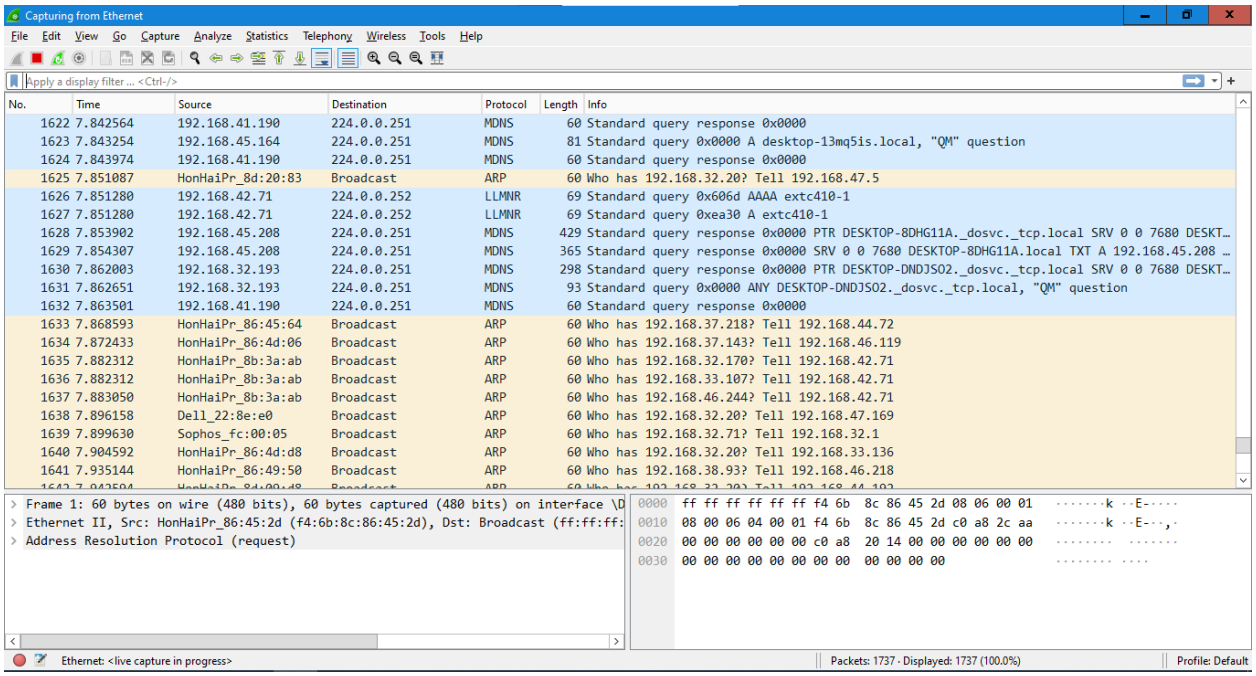
- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- QA engineers use it to verify network applications
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

OUTPUT

Promiscuous Mode:

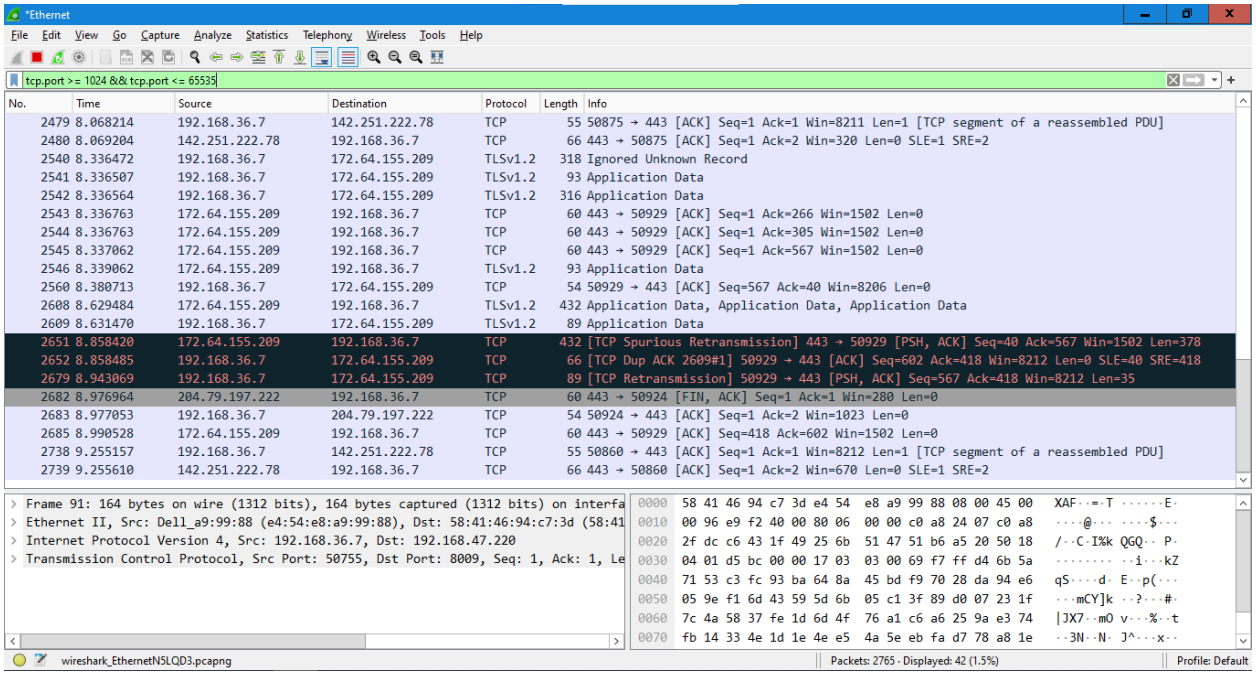


Non Promiscious Mode:



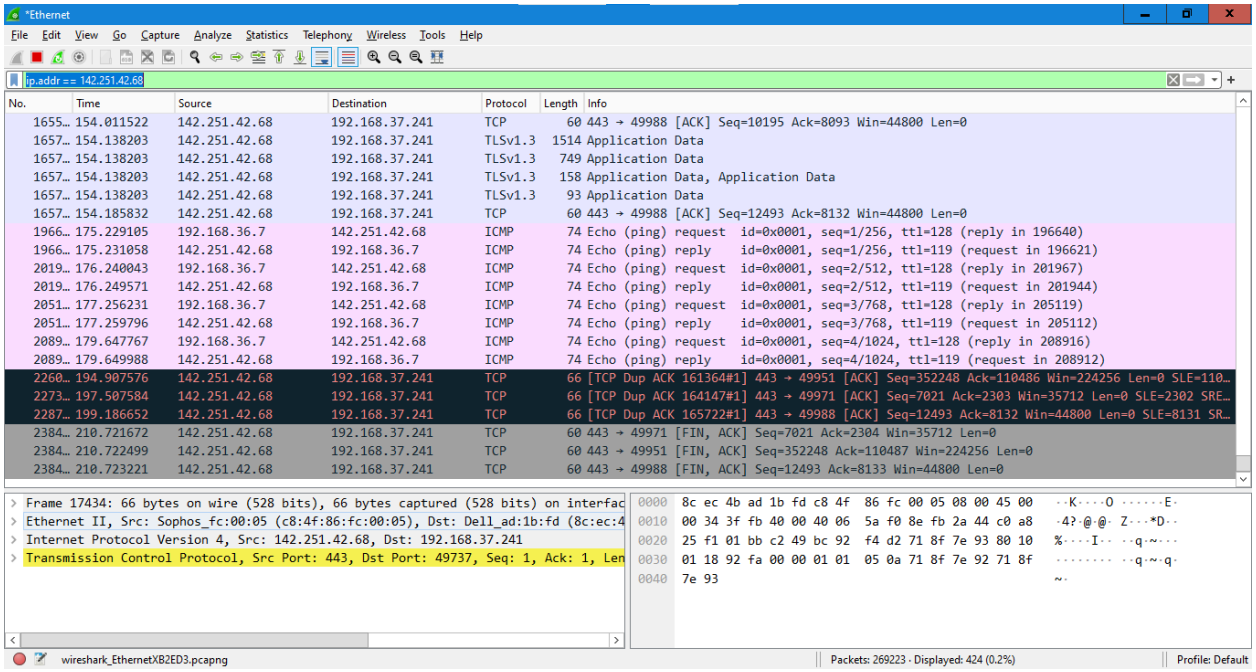
Port Filters:

tcp.port ⩾ 1024 && tcp.port ⩽ 65535



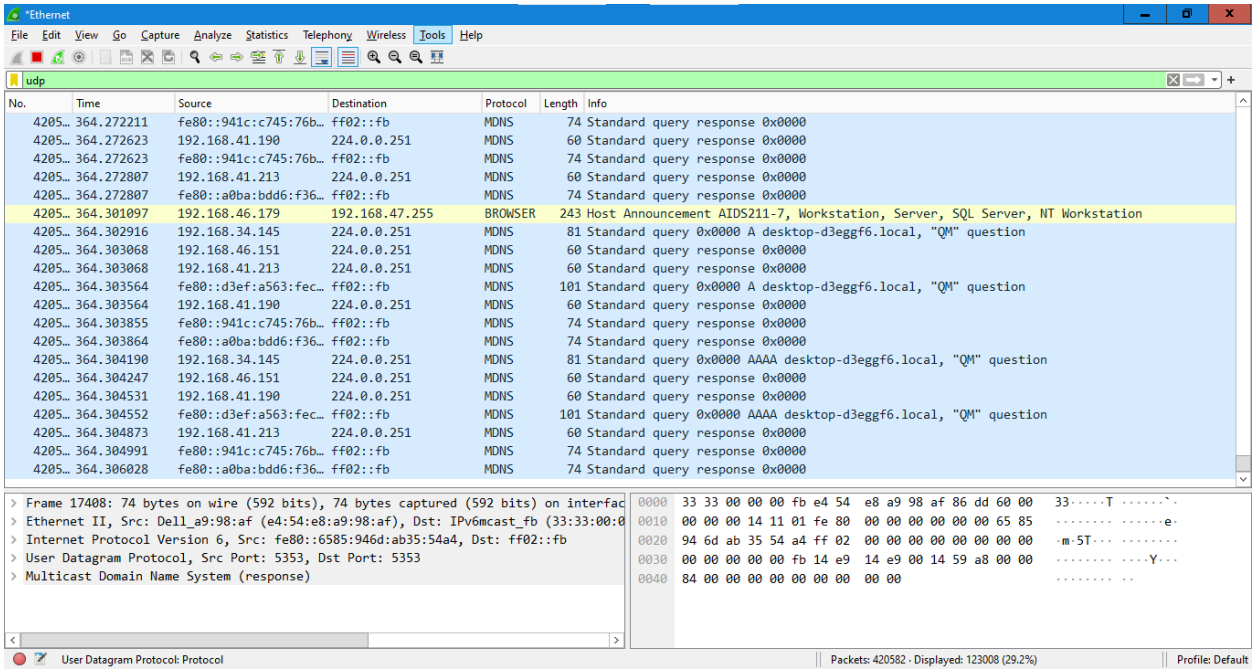
Address Filter:

ip.addr == 142.251.42.68



Protocol Filters:

udp



String Filter:

tcp contains "HTTP"