Experiment No 9

Aim: Study of packet sniffer tool "wireshark":

a) Download and install wireshark and capture icmp, tcp, and http packets in promiscuous mode.

b) Explore how the packets can be traced based on different filters.

Requirements: Compatible version of Wireshark.

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).

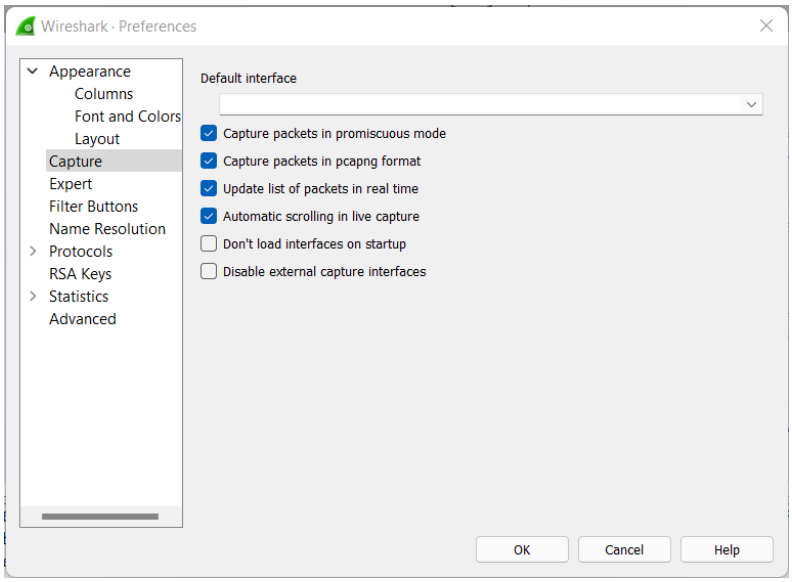
In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Intended purposes

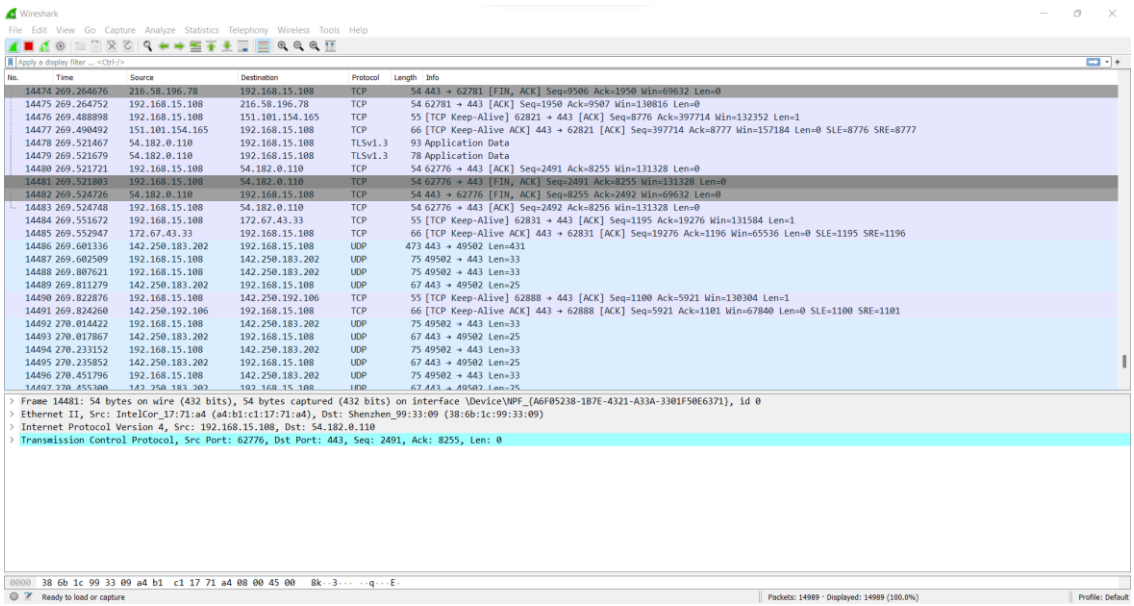
- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- QA engineers use it to *verify network applications*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol* internals

Output:

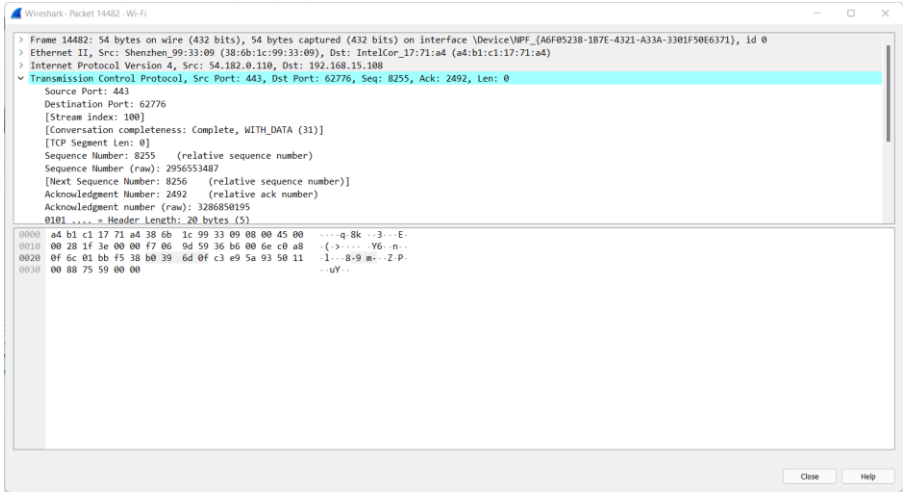
Turning on promiscuous mode



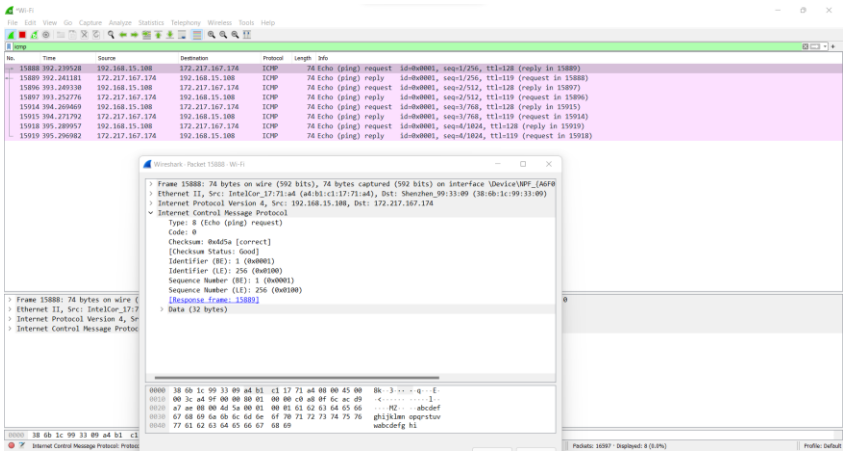
Monitoring all packets routing through Wi-Fi



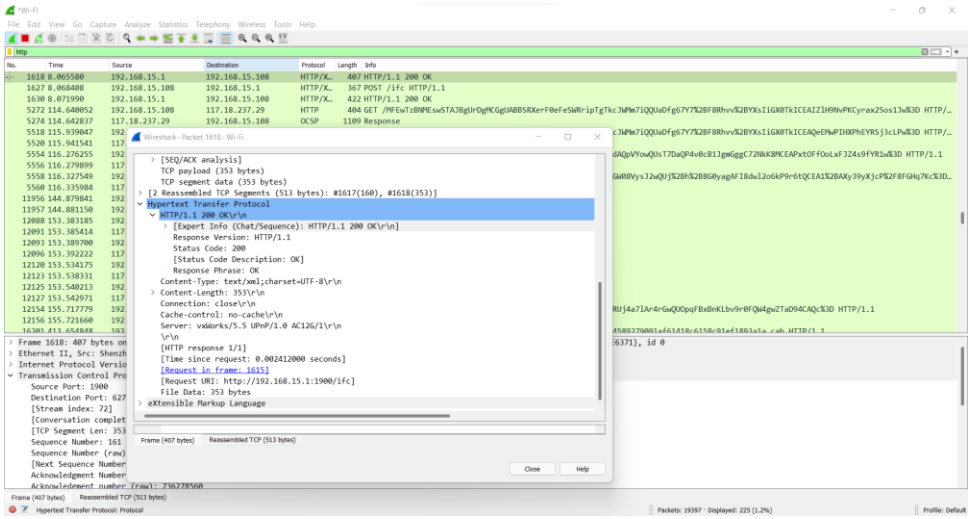
TCP packet



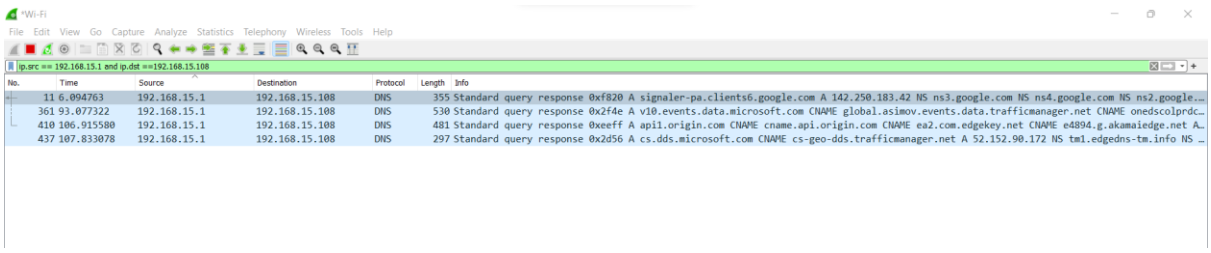
Filter ICMP packet



HTTP packet



Filter source and destination IP



Filter IP and protocols