

EXPERIMENT 8

AIM: Study of packet sniffer tools Wireshark: -

- Observer performance in promiscuous as well as non-promiscuous mode.
- Show the packets can be traced based on different 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).

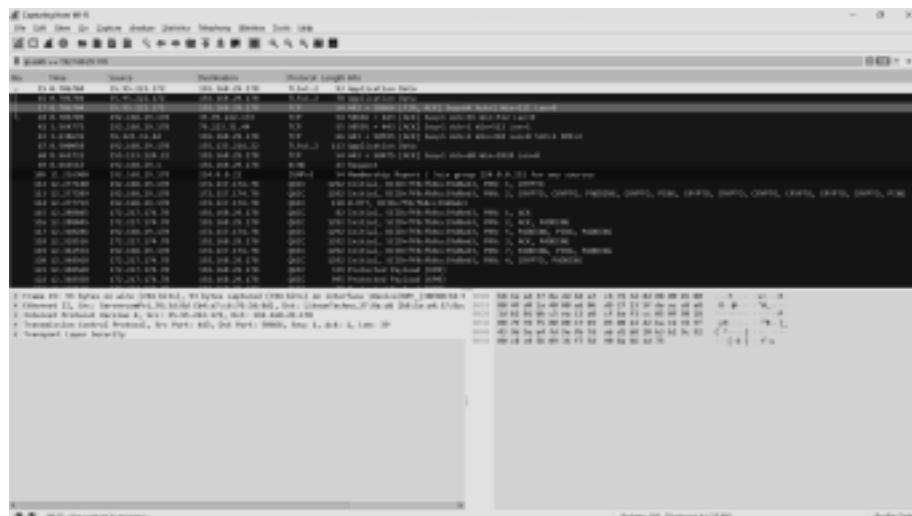
In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

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

Filter: IP Address

Promiscuous off



[illegible]

Promiscuous off

The screenshot displays the Wireshark 2.10.2 interface with a packet capture of an HTTP GET request. The packet list at the top shows a single packet (No. 1) from 192.168.1.100 to 192.168.1.1. The packet details pane on the left shows the structure of the HTTP request, including the GET method, the URL, and the User-Agent. The packet bytes pane on the right shows the raw data of the packet.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	192.168.1.1	HTTP	1000	GET / HTTP/1.1

Packet Details:

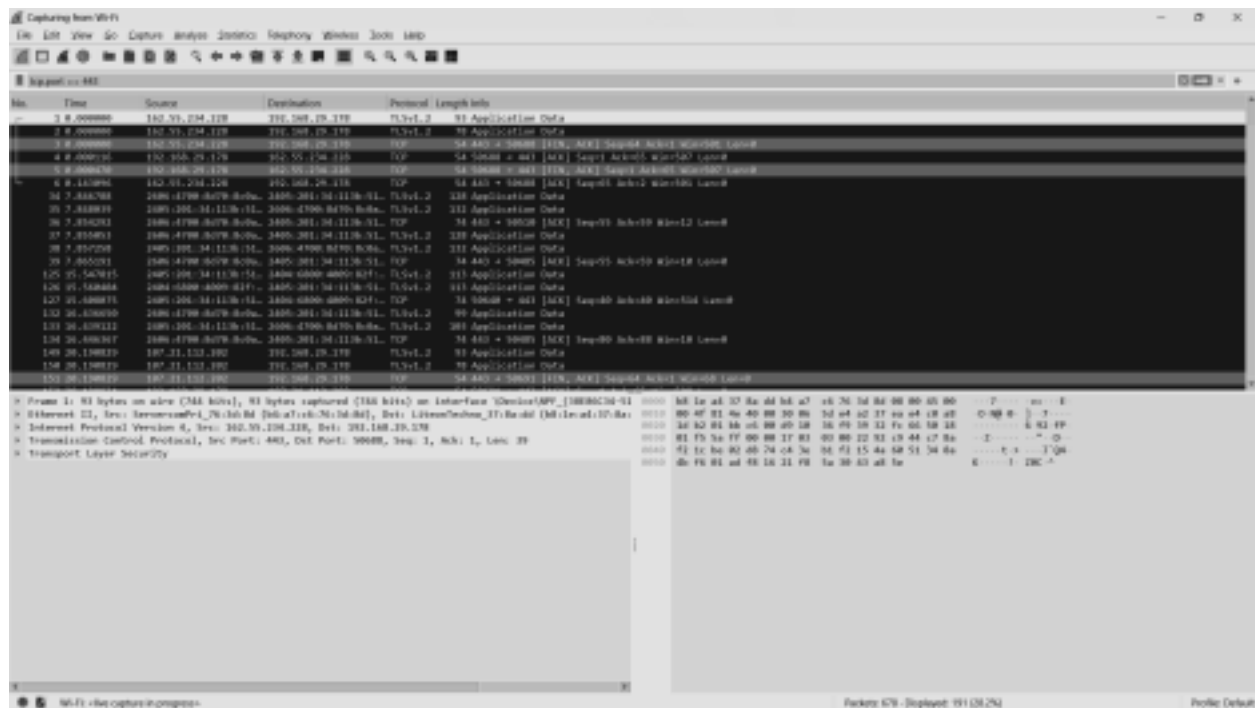
- Frame 1: 1000 bytes on wire (800 bytes captured) on interface eth0**
- Ethernet II, Src: Intel(R) Ethernet Controller (3:0:1:0), Dst: Intel(R) Ethernet Controller (3:0:1:0)**
- Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.1**
- Transmission Control Protocol, Src Port: 54400, Dst Port: 80, Seq: 1, Len: 0**
- Hypertext Transfer Protocol**

Packet Bytes:

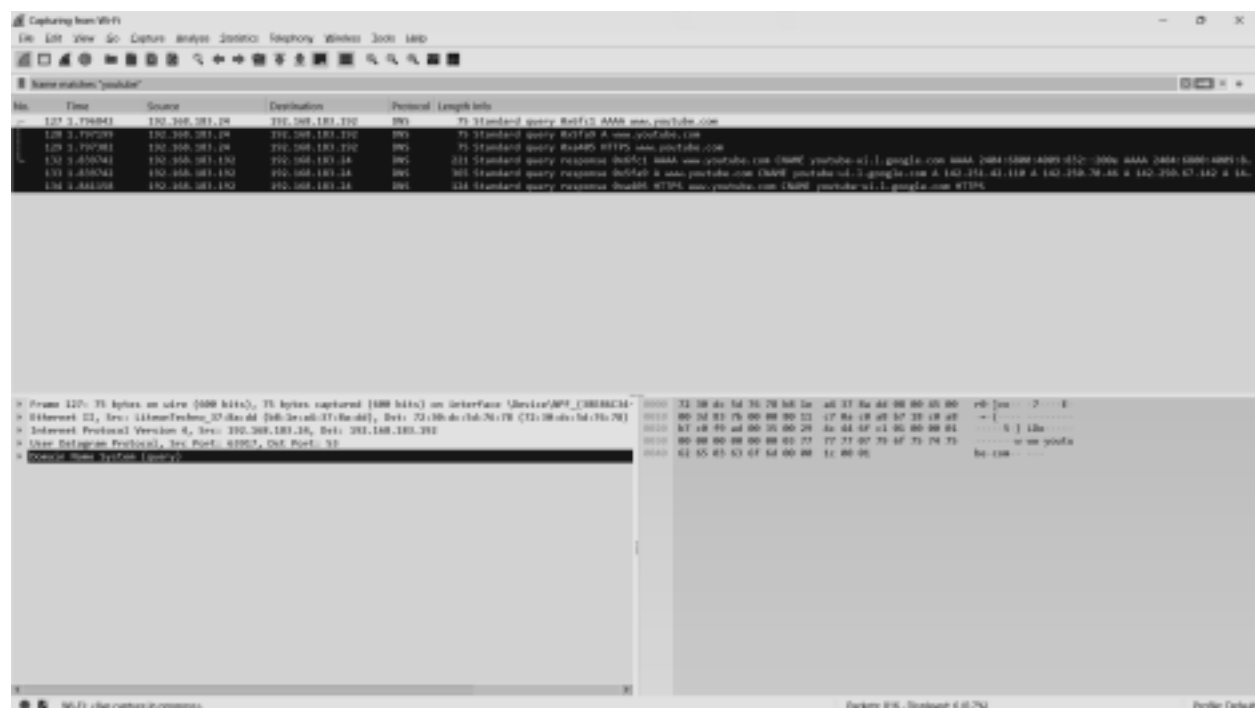
```

0000  45 2d 00 54 00 00 40 06 00 00 00 00 00 00 00 00  ...
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0200  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0210  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0220  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0230  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0240  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0250  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0260  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0270  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0280  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0290  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0300  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0310  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0320  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0330  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0340  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0350  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0360  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0370  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0380  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0390  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0400  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0410  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0420  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0430  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0440  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0450  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0460  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0470  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0480  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0490  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0500  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0510  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0520  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0530  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0540  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0550  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0560  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0570  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0580  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0590  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0600  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0610  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
0620  
```

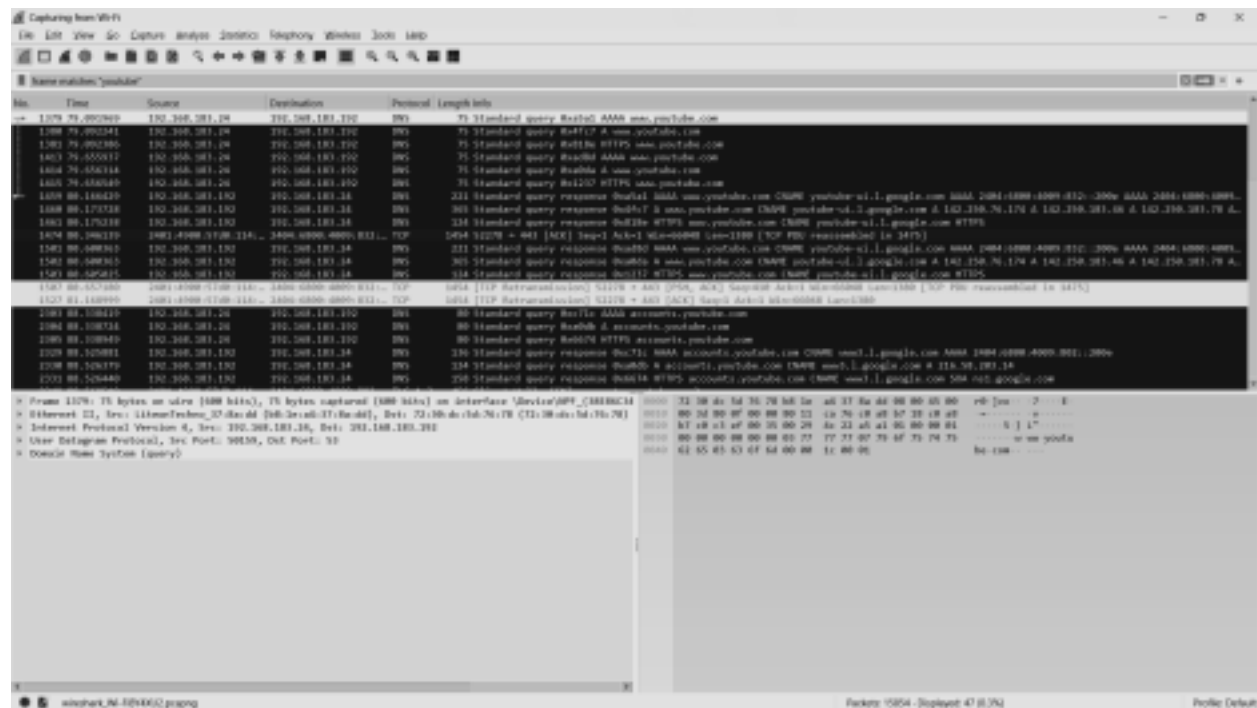
Promiscuous on



Filter: String matching
Promiscuous off



Promiscuous on



Conclusion: Thus, by performing this experiment, we have studied and implemented packet sniffing tool Wireshark.