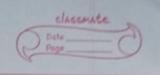
17)Tool Exploration -Wireshark (Documentation)

Constant
Q Sate
Wireshark Documentation
Wireshark is a widely used open-source
had at miller and at miller
at the transfer of Dellander
communication, protocol aring
fillering etc Wile shark is a network packet analyses
which presents captured packet data in as much
detail as possible.
active to position
Some purposes of wireshark:
· Melwork administrators use it to troubleshoot
network problems
· Network security engineers use it to examine
socurity problems
· Developers we it to debug protocol implementate
enternals
Unter rices
Features of wixeshark;
· Available for UNIX and Windows
· Capture live data from a network interface
· Display packets with vory detailed protoco,
information.
· Sare packet data captured
· Filler packets on criteria.
· Export some or all files packets in a
number of capture file formats.
· Colorise packet display based filters
· The information of the packets include
Il number, time, Source IP, address,
destination (P address, protoco) name, len



and other important information.

in the filter to capture only packets sent out to that particular IP address.

set that ensure only triggered teaffic appear.

Functionality of wireshark

packets and sinds captured packets to a machine running wireshark, it directs the packets so it can analysize packets captured on a remote machine at the time they are captured.

It has a graphic and filtering functions. It also monitors the unicast traffic.

e Port moving is a method to monitor network.

traffic. When it is enabled switch sends copies of
of all network packets present at one post to
another port.

Tt also supports capture formats from several other commercial and open source network shitlers.

on hollers that support promisers made in that mode so that they can see all traffic in the interface.

