ABSTRACT

We are trying to detect P2P protocols in a network packet using a traffic classification library known as Libprotoident. This very library uses a technique which has accuracy like DPI and takes less time than complete payload based DPI. This library uses the technique called **Lightweight Packet Inspection** in which it uses only first four bytes of the packet payload to detect the protocols. With the help of this library we are trying to develop a tool with GUI which would detect 12 P2P application protocols(Initially) and give some statistics based on traffic and related information like protocol name, source MAC, source IP, source port, destination MAC destination IP and destination port. In case the user wants to examine the payload part of the packet, along with theses information we are providing the payload data also. Our tool has the ability to capture live traffic almost in real time along with the capability of analyzing the offline network dump files.