ABSTRACT

The emergence of a Software Defined Network architecture that is not focused on network security so that it has weaknesses in network security [3]. The OpenFlow controller has limitations in storing flow entries so that it can cause OpenFlow Flow Table, this deficiency can be exploited by hackers to hack. Given the negative side of the use of computer networks, it is necessary to develop network forensics to be able to identify investigations. To increase time cost efficiency in the investigation process, analysis is needed so that log files can be carried out automatically. The clustering method was chosen because it can handle noise and can perform clustering on high data dimensions (attributes) and K-Mean Clustering was chosen because this algorithm has a fast and efficient computation time with a large amount of data. The results of this test will display the attacker so that the log file can be easily read by ordinary people.

Keywords : Software Define Network(SDN), OpenFlow, OverTable, Forensik, Digital Evidence