ABSTRACT

Advancement of information and communication technology at this time making Cybercrime one of the major threats to computer systems or other devices connected to the internet, various ways have been made to overcome this threat one of them with a Honeypot system. Honeypot is one of the new paradigms in network security that aims to detect suspicious activities, set a trap for an attacker and record the activities carried out by the attacker, although the Honeypot system has proven to be a solution to the security of a network but in reading the log activity generated still a problem. Therefore in this study the authors propose the Elasticsearch, Logstash, Kibana and Regular Expression methods to be able to assist in realtime analysis and monitoring on the Honeypot system. In the process of parse data with Regular Expression Cowrie has an accuracy value on pattern 1 of 98.14 percent and pattern 2 got 93.90 percent. Whereas for the 12 data Dionaea in patterns 1 and 2 got 100 percent accuracy.

***Keywords**: Honeypot, log analysis, ELK Stack, IoT Honeypot, visualization, Regular Expressions.*