ABSTRACT

Distributed Denial of Service (DDoS) attacks in a network continue to grow and are still widely used by attackers. Where this attack has a target that is the router network. DDoS attacks are attacks carried out by flooding the bandwidth to the network in large numbers. The target of the attack is not able to meet the demand in large numbers thereby making the network router go down. Therefore we need a forensic analysis of DDoS attacks on routers and search for information, and pull forensic data to be made as digital evidence using the live forensics method. In this study, the output made is interesting information created as digital evidence consisting of forensic log data and IP address that occur in cases of DDoS attacks on routers using the live forensic method.
Keywords*:* DDoS, *Router, Log Forensics, Live Forensics*