ABSTRACT

Network forensics is an important aspect to identify eavesdropping or intrusion on a network. Wiretapping by the attacker can trigger an even bigger attack, therefore a network forensics method is needed to collect network traffic records to look for evidence in the event of an attack. In this study, a forensic investigation was conducted to identify ARP poisoning using the Live Forensic. Attack trials are carried out when client accesses the server using the SSL and FTP protocols, this situation causes the client's personal data to be intercepted , in an effort to reveal the identity of the attacker, it requires tools so that the attacker can be found quickly, therefore in this research using tools XARPcan provide alerts (notifications) and detect the identity of the perpetrator of the attack in real time, besides this research uses tool which tool can monitor to see the condition of network traffic when in normal conditions or during conditions after being attacked. The results of this research refer to the concept of quantitative data where in the application of research using a series of trials to find out the final valid data in the form of address the attacker's IP victim's IP address, the time and date of the ARP Poisoning attack.

Keywords : *Network Forensics, Live Forensic, Attacker, XARP, Wireshark*