ABSTRAK

Forensik jaringan merupakan aspek penting untuk mengidentifikasi penyadapan atau penyusupan pada suatu jaringan. Penyadapan yang dilakukan oleh *attacker* dapat memicu suatu serangan yang lebih besar lagi, oleh karena itu dibutuhkan sebuah metode forensik jaringan untuk mengumpulkan catatan lalu lintas jaringan untuk mencari barang bukti jika terjadi suatu serangan. Pada penelitian ini dilakukan investigasi forensik dalam mengidentifiksi adanya serangan ARP *Poisoning* dengan menggunakan metode *Live Forensic*. Uji coba serangan dilakukan ketika *client* mengakses server menggunakan protokol SSL dan FTP yang menyebabkan tersadapnya data-data pribadi milik *client*, dalam upaya mengungkap identitas pelaku serangan ARP *Poisoning* memerlukan *tools* agar pelaku serangan dapat segera ditemukan dengan cepat maka dari itu dalam penilitian ini menggunakan *tools* XARP yang dapat memberikan *alert* (notifikasi) dan mendeteksi identitas pelaku serangan secara *real time*, selain itu penelitian ini menggunakan *tools* Wireshark yang mana *tools* ini dapat melakukan *monitoring* untuk melihat kondisi lalu lintas jaringan pada saat dalam kondisi normal maupun pada saat kondisi setelah diserang. Hasil dari penilitian ini mengacu pada konsep data kuantitatif dimana dalam penerapan riset dibutuhkan serangkaian uji coba untuk mengetahui hasil akhir data secara valid dari berbagai sumber berupa IP *address* penyerang, IP *address victim*, waktu serta tanggal terjadinya serangan ARP *Poisoning*.

Kata Kunci : Forensik Jaringan, *Live Forensic*, *Attacker*, ARP *Poisoning*, Wireshark