ANALISIS SERANGAN SIBER DENGAN WIRESHARK UNTUK *NETWORK FORENSIC*

Ilham Fadilah

ABSTRAK

Network Forensic adalah kegiatan menangkap , merekam, dan menganalisis kejadian di dalam jaringan untuk menemukan sumber dan melakukan analisis jenis dari serangan. *Network Forensic* jika dilakukan secara manual akan membutuhkan waktu yang lama dalam mengumpulkan data dan melakukan Analisa jenis serangan dan mencari IP address sumber dari serangan. Maka digunakan *tool* utnuk mengumpulkan log. Emotet adalah Trojan yang terutama disebarkan melalui email spam (malspam). Infeksi mungkin datang melalui skrip berbahaya, file dokumen berkemampuan makro, atau tautan berbahaya. Dengan muncul kembalinya malware tersebut maka diperlu diketahui bagaimana ciri-ciri log koneksi yang terjadi oleh malware tersebut maka dilakukan analisa menggunakan metode *network forensic*, setelah analisa dilakukan ditemukan bahwa malware emotet menggunakan protokol http untuk melakukan pengambilan data dari server *command center*.

Kata Kunci : *Network Forensic*, *Emotet*.

CYBER ATTACK ANALYSIS WITH WIRESHARK FOR NETWORK FORENSIC

Ilham Fadilah

ABSTRACT

Network forensics is the activity of capturing, recording, and analyzing events in the network to find the source and analyze the type of attack. Network forensics if done manually will take a long time to collect data and analyze the type of attack and find the source IP address of the attack. Then used tools to collect logs. Emotet is a Trojan that is mainly spread via spam email (malspam). Infections may come via malicious scripts, macro-enabled document files, or malicious links. With the reappearance of the malware, it is necessary to know how the characteristics of the connection logs that occur by the malware are analyzed using the network forensic method after the analysis, it was found that the emotet malware uses the http protocol to retrieve data from the command center server.

Kata Kunci : *Network Forensic, Emotet*.