ABSTRAK

ANALISIS *MALWARE* PADA *TRAFFIC* JARINGAN MENGGUNAKAN SECURITYONION

Oleh

AHMAD BAHRI AL-ANWAR

1202150111

Malware merupakan suatu perangkat lunak yang digunakan dengan tujuan untuk mencoba melanggar kebijakan keamanan sistem komputer terkait dengan kerahasiaan, integritas, atau ketersediaan. Tujuan dari analisis *malware* adalah untuk memberikan informasi yang dibutuhkan untuk menanggapi intrusi jaringan. Sasarannya adalah untuk menentukan dengan tepat apa yang terjadi, dan memastikan ditemukannya seluruh komputer dan *file* terinfeksi. Ketika menganalisis malware yang dicurigai, tujuannya adalah menentukan secara tepat apa yang dapat dilakukan oleh seorang tersangka tertentu, Oleh karena itu perlu adanya analisis pada *packet capture* untuk mengetahui serangan *malware* terhadap komputer yang mencurigakan pada jaringan dan mengetahui *anomaly* yang disebabkan oleh malware tersebut. Penelitian ini dilakukan dengan menguji enam sampel PCAP yang di unduh secara *random*, kemudian dianalisis menggunakan SecurityOnion. Analisis yang dilakukan menggunakan metode analisis statis yang berfokus pada *traffic* yang melintas dalam suatu jaringan berdasarkan *anomaly* dan *behavior* yang dilakukan oleh malware tersebut. Hasil dari analisis ini adalah kategorisasi *malware* berdasarkan ancaman dan dampak yang dihasilkan. Berdasarkan data tersebut peneliti melakukan analisis tindakan preventif terhadap dampak yang dihasilkan.

Kata kunci : *Malware, Malware analysis, cyber crime, traffic analysis, Packet capture, Network analyzer, SecurityOnion*