ABSTRAK

Kemajuan teknologi, terutama di bidang penggunaan internet, membawa dampak baik dan buruk. Di satu sisi, internet memberikan kemudahan dalam mendapatkan informasi dan melakukan berbagai aktivitas. Namun, sisi lain, penggunaan internet juga membawa ancaman terhadap serangan siber, salah satunya adalah *malware*. *Malware* merupakan program jahat yang dibuat untuk masuk ke dalam, atau merusak sistem komputer. Maka dari itu, diperlukan deteksi yang efektif yang dapat membedakan *malware* dan *non-malware*. Salah satunya menerepkan *Machine Learning* yang berfungsi untuk membedakan serangan *malware* atau bukan. Penelitian ini bertujuan untuk menemukan model *Machine Learning* yang memiliki kinerja optimal dalam deteksi *malware* dengan melakukan perbandingan tiga model yaitu, model *Random Forest, Support Vector Machine,* dan *Naïve Bayes*. Hasil penelitian menunjukan bahwa *Random Forest* memiliki kinerja terbaik dengan *F1-score* 0.99. Penelitian ini menunjukan bahwa pemilihan model *Machine Learning* yang tepat sangat berpengaruh terhadap akurasi deteksi *malware*.

Kata Kunci: ***Malware*, Deteksi, *Machine Learning*, *Random Forest*, *Support Vector Machine*, *Naïve Bayes*.**