ABSTRAK

ANALISIS MALWARE PADA SISTEM OPERASI ANDROID MENGGUNAKAN *MEMORY FORENSICS* BERDASARKAN API

Oleh

RIFYANDARU WIBISONO

1202150088

Malware adalah sebuah program yang berada pada sistem operasi dan dapat membahayakan sistem operasi yang terjangkit. Dalam perkembangan internet banyak sekali jenis malware yang dapat ditemukan dalam internet seperti android malware. *Android malware* adalah *malware* yang membuat pengaruh negatif pada sistem operasi android. *Malware* memiliki tujuan untuk merugikan pengguna pada sistem operasi yang terjangkit. Oleh sebab itu digunakanlah *malware analysis* untuk mengidentifikasi *malware*. *Malware analysis* adalah cara untuk mendapatkan informasi dari malware untuk mengatasi serangan terhadap korban yang terinfeksi. Dalam melakukan *malware analysis* bisa digunakan beberapa cara untuk mendeteksi malware seperti mendeteksi berdasarkan penggunaan *memory*. Dalam mendeteksi *malware* berdasarkan *memory* bisa digunakannya *memory forensic* untuk melakukan pendeteksian. Setelah mendapatkan hasil dari deteksi *malware* akan digunakannya sebuah cara untuk melakukan memberikan dampak untuk *malware* berdasarkan API. Dalam menggunakan *memory forensics* digunakan tools volatility untuk mendapatkan hasil analisis *malware* dan menggunakan *reverse engineering* dengan tools APKtools untuk mengetahui *malicious activity* berdasarkan penggunaan API dari aplikasi tersebut. Dalam penelitian ini digunakan 10 malware untuk dilakukan análisis menggunakan volatility dan APKtools untuk memberikan dampak mengunakan hasil dari análisis dan juga berdasarkan *malicious activity* dari API. Maka darii tu hasil dari penelitian ini adalah dampak yang berkaitan dengan API dan hasil análisis.

Kata kunci : *malware, malware analysis, memory, memory usage*.