

ABSTRAK

ANALISIS *MALWARE* PADA SISTEM OPERASI ANDROID MENGUNAKAN METODE *NETWORK TRAFFIC ANALYSIS*

Oleh

ACHMAD FARHAN FEBRIANTO

1202154208

Malware bisa disebut juga *malicious software* merupakan perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer dan juga dapat mempengaruhi *network traffic*. Dengan meningkatnya penyebaran *malware* pada sistem operasi android saat ini. Untuk itu dilakukannya *malware analysis* pada android, *Malware analysis* pada sistem operasi android ini ada dua cara yaitu *Static Analysis* dan *Dynamic Analysis*. *Static analysis* dilakukan tanpa menjalankan *malware* tersebut dan hanya melihat segmen code pada aplikasi. *Dynamic Analysis* mengeksekusi program dan mengamati hasilnya Metode statik yang digunakan pada penelitian ini adalah *reverse engineering*. *Reverse engineering* digunakan untuk ekstraksi aplikasi kedalam *source code*, data tersebut akan dihasilkan informasi bahwa *malware* tersebut mengakses jaringan, Kemudian metode selanjutnya untuk mendekteksi *malware*-nya adalah *network traffic analysis*. Kelebihan *network traffic analysis* ini yaitu dapat mengetahui *malware* yang terhubung langsung dengan website dan dengan analisis ini juga dapat mengetahui aktivitas *malware* terhadap *network traffic* dari melihat *bandwidth*, *time since request* dan *payload* yang dimiliki *malware*. Dari hasil analisis, informasi yang didapat adalah *malicious activity* yang mempengaruhi *network traffic*.

Kata kunci : *Malware, malware analysis, static analysis, dynamic analysis, network traffic analysis*