ABSTRAK

Malware merupakan sebuah perangkat lunak atau *software* yang diciptakan untuk menyusup atau merusak sistem komputer. Penyebaran *malware* saat ini begitu mudah baik melalui iklan-iklan tertentu pada website, *USB flashdrive*, dan media lainnya. Semuanya sangat erat kaitannya dengan tindak kejahatan seperti pencurian *file*, *internet banking*, kartu kredit dan lain sebagainya. Berkaitan dengan hal tersebut, ada suatu bidang yang menangani tindak kejahatan yaitu forensik digital. Salah satu tahapan dalam forensik digital yaitu melakukan analisis terhadap barang bukti digital, dalam hal ini adalah *malware*. Untuk membuktikan suatu *software* dikatakan *malware* adalah dengan mengetahui cara kerja program tersebut pada sistem komputer. Metode pengujian *malware* dengan analisis dinamis merupakan metode yang paling akurat untuk menganalisa cara kerja *malware.*

Pada Tugas Akhir ini, digunakan metode *Malware* Analisis Dinamis melalui pengujian Regshot dan Wireshark untuk menganalisa 6 sample *malware* yang tersedia, yaitu *Poison Ivy*, *Gen Variant Johnnie 97338*, *Trojan GenericKD 40427213*, *Dropped:Trojan.AgentWDCR. PZW*, *32.Trojan.Raasmd.Auto* dan *Gen:Variant.Strictor.171520*. Dari pengujian tersebut diperoleh hasil melalui metode Regshot terdapat perubahan *Registry* terbanyak oleh *malware Dropped:Trojan.AgentWDCR.PZW* yaitu 163 *Registry*. Sedangkan dalam Metode Wireshark, *malware* yang mengirimkan *protocol* paling banyak adalah *Gen:Variant.Strictor.171520* sebanyak 1993 *protocol*.

Kata kunci — Forensik Digital; Analisis Malware; Dynamic Analysis; Trojan; Gen; Poison Ivy; Wireshark; Regshot; Protocol.