BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari penelitian analisa *ransomware* menggunakan metode *Surface analysis Runtime Analysis* dan *static code analaysis* terhadap *ransomware* cryptolocker dapat disimpulkan :

1. Untuk mensimulasikan penyerangan cryptolocker harus disiapkan unit laptop dan jaringan internet yang bagus, pencarian sample *ransomware* harus terus di update, karena kemampuan sample *ransomware* ada batas waktunya, sehingga apabila mendapatkan sample *ransomware* yang sudah diputus mata rantainya dengan server *ransomware* maka *ransomware* dengan sendirinya tidak bisa melakukan enkripsi terhadap data kita, meskipun komputer kita sudah terinfeksi dengan *ransomware* tersebut.
2. Karakteristik *Cryptolocker* pada analisa *malware* dengan metode surface analysis, *bahwa malware* mempunyai kemampuan perlindungan diri dengan diketahui bahwa badan malware dipacked dengan NSIS, karakteristik *Cryptolocker* dalam menyerang sistem pada analisa Runtime Analysis melakukan perubahan registry, memantau aktifitas pada file system, proses dan thread yang terjadi, melakukan hubungan koneksi yang dilakukan oleh *ransomware* terhadap server *ransomware*, sedang pada analisis *static code* dapat memberikan informasi yang sebelumnya tidak ditemukan dengan metode lain, yaitu *ransomware* mampu untuk berlindng dari pengawasan sistem keamanan komputer dan mematikannya seperti mematikan firewall, dan antivirus.
3. Metode Surface Analysis, Runtime Analysis dan Static Code Analysis mampu mendapatkan bukti digital untuk mendukung investigasi penyidikan dalam *ransomware forensics,* Berdasarkan penelitian yang dilakukan, ditemukan beberapa file yang menjadi bukti digital seperti *encrypted* file, *Log file* packet data internet, yang bisa digunakan untuk mendukung investigasi penyidikan dalam *malware forensics.*

5.2 Saran

1. Analisa *ransomware* metode *Surface analysis, Runtime Analysis* dan *static code analaysis* memerlukan waktu yang lama dalam prosesnya. Untuk penelitian berikutnya perlu membuat sebuah metode penanganan terhadap serangan *ransomware* yang mampu memberikan langkah-langkah tepat yang harus dilakukan pada server yang terinfeksi *ransomware* dan penanganannya secara langsung tanpa merusak atau menggangu kegiatan yang sedang berlangsung.
2. Analisa *ransomware* akan terus berkembang seiring dengan semakin canggihnya *ransomware* yang dibuat. Oleh karena itu pengembangan terhadap analisa *ransomware* masih perlu dilakukan seperti analisis dengan menggunakan metode *signature based* dan *anomaly based.* Selain itu untuk mencegah berkembangnya wilayah serang dari ransomware diperlukan juga analisis penggabungan antara analisis *ransomware* dengan analisis keamanan jaringan atau antara analisis ransomware dengan analisis keamanan database.
3. Dengan adanya beberapa keterbatasan dalam penelitian ini, kepada peneliti lain diharapkan untuk mengadakan penelitian sejenis lebih lanjut dengan mengambil wilayah penelitian yang lebih luas, sampel *ransomware* yang terbaru dan menggunakan rancangan metode penelitian yang lebih kompleks, sehingga dapat ditemukan hasil yang lebih update dan bisa dimanfaatkan oleh masyarakat lebih luas. Perkembangan ransomware terkini sudah mulai menyerang terhadap perbankan dan jaringan perusahaan, kombinasi analisis keamanan jaringan dan analisis ransomware untuk pencegahan menjadi peluang untuk penelitian selanjutnya. Karena penjahat *cyber* sudah mulai mempertimbangkan bahwa serangan ransomware ditargetkan terhadap korporasi berpotensi lebih menguntungkan daripada serangan terhadap pengguna pribadi.