Bab 5 Kesimpulan dan Saran

Pada bagian ini menjelaskan kesimpulan dari hasil penelitian yang telah dilakukan berdasarkan tujuan dan perumusan masalah penelitian, yaitu: 1) apakah pemasangan Snort mampu meberikan informasi dalam mendeteksi serangan *flooding,* dan 2) bagaimana hasil *file log* Snort dalam menemukan barang bukti digital forensik.

5.1 Kesimpulan

Kesimpulan yang telah didapatkan selama proses penelitian dalam melakukan deteksi serangan *flooding* pada web server menyimpulkan bahwa:

1. Pengimplementasian *Intrusion Detection System* (IDS) Snort pada web server dilingkungan Universitas Muhammadiyah Magelang dapat digunakan untuk membantu memberikan informasi terkait deteksi adanya serangan *flooding* dengan memanfaatkan *rule* khusus *flooding* yang diterapkan pada *Intrusion Detection System* (IDS) Snort.
2. *File log* didapatkan dari pengimplementasian Snort guna kebutuhan analisis aktivitas tindakan illegal yang terjadi pada lingkungan web server Universitas Muhammadiyah Magelang, berdasarkan analisis file log terdapat sebanyak 15 IP *address* penyerang yang melakukan tindakan illegal dengan *frekuensi* penerimaan data *timestamp, destination port,* dan pesan/*payload*. Dari hasil analisis yang dijabarkan pada BAB IV tersebut menunjukkan bahwa ada serangan *flooding*, serangan yang mengirimkan banyak data pada target, sehingga dapat mengintervensi serta merusak sumber daya khusunya IT yang ada pada Universitas Muhammadiyah Magelang.

Berdasarkan penelitian yang telah dilakukan, *Intrusion Detection System* (IDS) Snort yang diimplementasikan pada *environment web server* di lingkungan Universitas Muhammadiyah Magelang dapat memberikan Informasi terkait deteksi serangan, khususnya serangan *flooding*.

5.2 Saran

Saran yang dapat digunakan untuk penelitian berikutnya terkait dengan Intrusion Detection System (IDS) adalah:

a. Saran yang dapat diberikan untuk keperluan penelitian selanjutnya adalah pengembangan system deteksi menggunakan Intrusion Detection System (IDS) Snort dalam mendeteksi serangan lain, seperti: SQL *Injectin*, *Brute Force*, dll.
b. Melakukan pengembangan unuk melakukan implementasi Snort pada system jaringan workstation yang lebih besar seperti multi WAN.