Bab V Kesimpulan Dan Saran

5.1 Kesimpulan

Berdasarkan hasil yang didapatkan pada proses implementasi hasil dan pembahasan, maka, pada peneltian studi dan analisa forensik digital pada kasus serangan *MITM Based Evil Twin* dapat ditarik beberapa kesimpulan yaitu :

1. Mendeteksi dan menemukan karakteristik serangan *Evil Twin* AP dapat diketahui dengan cara menganalisa atribut-atribut dari AP tersebut, dari hasil analisa diketahui terdapat beberapa informasi yang dapat dijadikan perbandingan yaitu *SSID* yang sama, kekuatan sinyal dengan tingkat yang lebih besar dari signal AP yang asli, dan karakteristik serangan evil twin memiliki tingkat presentasi pengiriman paket *beacon* yang lebih tinggi dari *beacon* signal AP *legal.*
2. Metode pencarian barang bukti dari serangan *MITM*, dilakukan dengan menggunakan metode *live* yang memanfaatkan *sniffing* dalam jaringan wifi pelaku. Proses tahapan investigasi dilakukan dengan menganalisa *port* arp dan http, dari hasil analisa ditemukan beberapa kegitan ilegal seperti file images, html dan bahkan aplikasi berextensi exe. Hasil dari proses analisa investigasi forensik menghasilkan suatu model investigasi ENFGP (*Extendend* NFGP) yang dibagi menjadi 10 tahapan dan terdiri atas 30 langkah – langkah penyelesaian, yang didapatkan melalui proses pengujian dan implenmentasi metode pada kasus serangan *MITM Based Evil Twin* serta pengujian lebih lanjut berdasarkan beberapa model forensik sebelumnya.

5.2 Saran

1. Penelitian selajutnya diharapkana dapat mengimplementasikan dari pendekatan baik secara user side maupun dari server side, dikarekan terbatasnya analisa pencarian barang bukti yang dilakukan pada proses investigasi forensik pada kasus *MITM Based Evil Twin.*
2. Penelitian selanjutnya diharapkan dapat dilakukan pada area publik yang memliki kemungkinanan adanya lebih dari satu *Rogue* AP atau *Evil Twin* AP.

3. Penelitian selanjutnya diharpakan dapat mengikuti perkembngan metode serangan yang dilakukan para pengembangan *MITM Based Evil Twin*.guna untuk pengembangan framework investigasi forensik lebih lanjut.