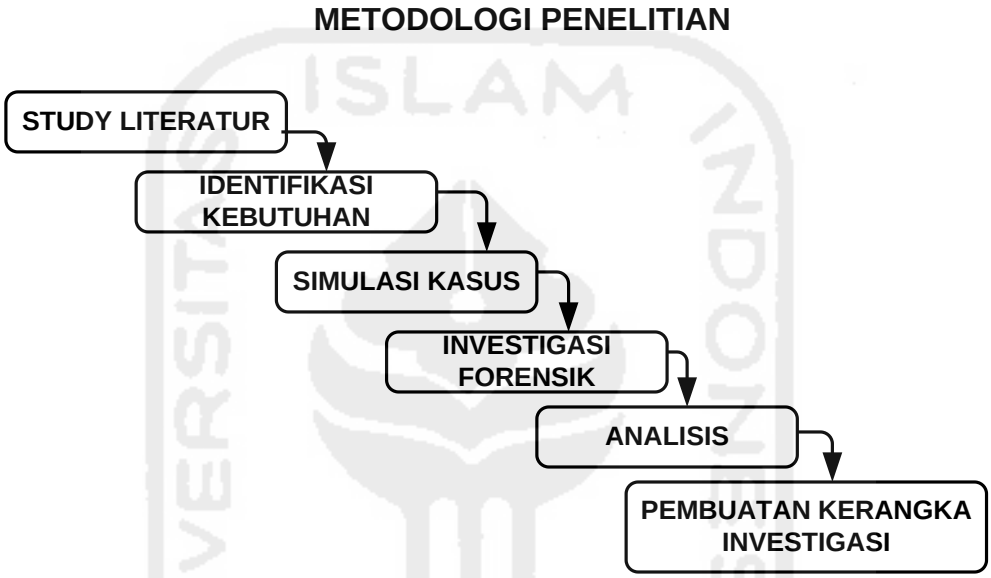
Bab III Metodologi Penelitian

Dalam bab ini akan dijabarkan tentang bagaimana proses dan tahap- tahap yang akan dilakukan di dalam penelitian sehingga dapat mengahsilkan poin - poin utama yang dapat dijadikan sebagai pedoman. Pada penelitian ini akan diterapkan metode



Gambar 3. 1 Tahapan Metodologi Penelitian

Berikut pengusulan metodelogi penelitian yang akan digunakan :

Berdasarkan skema di atas, usulan metodologi penelitian

3.1 Literatur *Review*

Literatur review Akan membahas tentang uraian dari teori - teori, temuan-temuan maupun rangkuman – rangkuman dari penelitian sebelumnya yang nanti dapat digunakan sebagai landasan atau acuan dalam melakukan kegiatan penelitian.

3.2 Identifikasi Kebutuhan

Identifikasi kebutuhan merupakan tahapan dimana, melakukan persiapan –persiapan yang harus dipenuhi untuk melakukan proses investigasi baik berupa kebutuhan perangkat keras maupun perangkat lunak, sebagai media pelantara untuk membantu proses investigasi

3.3 Simulasi Kasus

Simulasi *kasus* merupakan kegiatan uji coba serangan *Evil Twin* yang dilakukan di area *hotspot* fakultas teknologi industri universitas Islam Indonesia (Fti UII), pada kasus ini pelaku penyerangan *Evil Twin* membuat setting an *getaway* yang berbeda dengan IP *getaway* dari *router* Fti UII, sehingga proses investigasi tidak dapat dilakukan sisi *administrator* ataupun *router*, oleh karena itu dalam melakukan proses identifikasi dibutuhkan suatu pendekatan berbasis *wired* atau *user* yang diimplementasikan dengan metode *live* forensik untuk menganalisa data dari system yang berjalan, seperti yang terlihat pada Gambar 3.2 yang menunjukkan bagaimana pola dari penyerangan *MITM Based Evil Twin,* dimana pelaku mencoba membuat AP palsu, dan setelah korban terhubung, pelaku dapat dengan mudah melakukan *sniffing* untuk mencari informasi penting milik korban, disisi lain investigator yang sengaja masuk ke dalam jaringan korban, berusaha melakukan *sniffing* diantara komunikasi pelaku dan korban lainnya.

Gambar 3. 2 Simulasi Kasus

3.4 Investigasi Forensik

Tahapan investigasi merupakan tahapan dimana *user* melakukan proses identification dengan menerapkan metode forensik ketika *user* telah masuk ke dalam jangkauan *Evil Twin*. Pada penelitian ini metode yang digunakan adalah *live* forensik, untuk lebih jelas dapat diliat pada Gambar 3.3. Proses investigasi terdiri beberapa tahapan yang dimulai dari proses *identification* sampai pada proses tahapan analisis.

Gambar 3. 3 Tahapan Investigasi

3.4.1 Tahapan Investigasi

Berdasarkan Gambar 3.3 tahapan investigasi merupakan penerapan metode forensik pada kasus, berikut tahapan investigasi terdiri dari beberapa langkah yaitu :

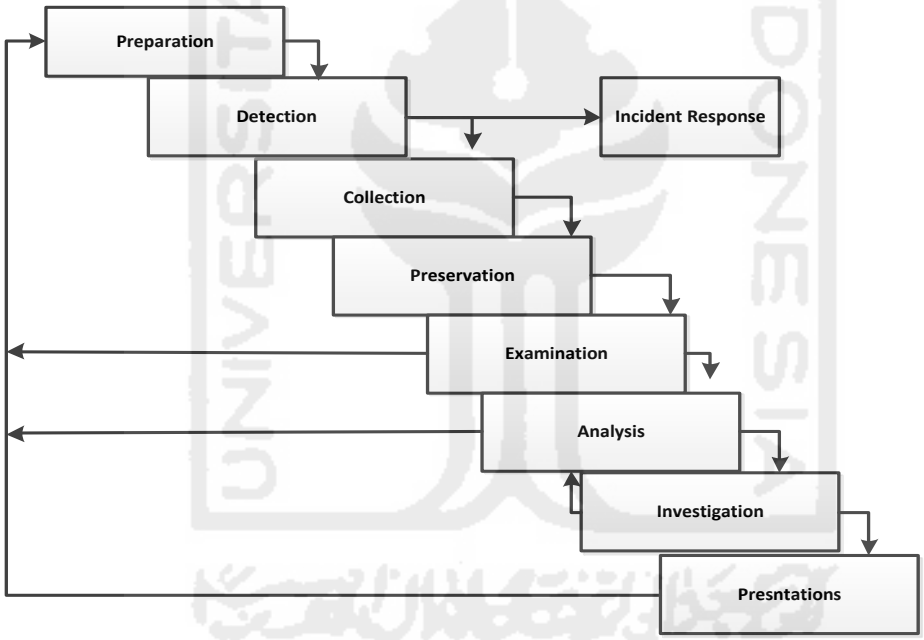
a. *Scanning* populasi dan identification AP: merupakan kegiatan awal dalam investigasi kasus *Evil Twin attack*, dimana *user* mengidentifikasi *Evil Twin* AP dengan cara melakukan proses *scanning* ap, kemudian menganalisa karakteristik dari AP tersebut dari *SSID*, *channel*, *power*, *encrypt* sampai dengan *BSSID* dari AP yang ditemukan, dengan menggunakan beberapa aplikasi berbasis windows yaitu *Chelam* dan *Arcilyric-Wifi*
b. Masuk ke jangkauan: pada tahapan ini peneliti akan berusaha masuk ke jangkauan dari *Evil Twin*, hal ini dilakukan karena pelaku menggunakan *getaway* yang berbeda dari *getaway hotspot/router* yang ada sehingga serangan tak dapat diidentifikasi dari *area administrator* atau *server*, untuk itu dibutuhkan pendekatan secara *user* atau *wired* untuk mengidentifikasi serangan, yaitu dengan cara masuk ke jangkauan *Evil Twin*.
c. Identifikasi serangan: *user* mendeteksi serangan ketika *user* telah berada di dalam jangkauan *Evil Twin*, dengan menggunakan beberapa aplikasi berbasis windows yaitu: *Chelam* dan *x Arp* aplikasi ini akan mendeteksi secara automatis apabila terdapat AP yang mencurigakan.
d. *Collection* atau pengumpulan: merupakan satu tahapan pengumpulan bukti digital dengan menggunakan *tools* maupun metode yang ada, dalam kasus ini proses pengumpulan barang bukti dilakukan ketika *user* sadar telah terjebak masuk di dalam perangkap *Evil Twin*, kemudian *user* mencoba melakukan *capture* trafik pada jaringan tersebut untuk mengetahui *illegal activity* atau serangan *MITM* dengan menggunakan Tcpdump atau Wireshark.
e. *Acquisition:* merupakan tahapan *extract capture traffic* yang dilakukan sebelumnya, disini peneliti menggunakan *tools* Wireshark *network* miner. Tcpdump

3.5 Tahapan analisa

Merupakan suatu proses akhir dalam menganalisa identification *Evil Twin* AP dan file Pcap dari hasil *capture* sebelumnya, dengan tujuan untuk menemukan data-data yang dapat mendukung proses investigasi. Di dalam penelitian ini Akan digunakan beberapa metode filterisation yang telah disediakan oleh aplikasi Wireshark ataupun untuk memudahkan proses identification forensik

3.5.1 Tahapan Pembuatan Laporan Dan Penyusunan Kerangka Investigasi

Tahapan penyusunan kerangka investigasi pada penelitian ini Akan disusun berdasarkan model *network* forensik *generic* proses *(*NFGP*)*, seperti yang terlihat pada Gambar 3.4, dan yang nanti akan disesuaikan dengan kasus *MITM based Evil Twin*.



Gambar 3. 4 *Network* forensik generic proses model

Sedangkan pembuatan laporan merupakan hasil dari pengujian dan investigasi forensik terhadap kasus serangan *MITM based Evil Twin*, pembahasan laporan akan dimulai dari pendahuluan, kajian pustaka, metodologi penelitian, hasil dan pembahasan, serta penutup. Kesimpulan dan saran atau solusi yang diperoleh dari penelitian ini, akan dimasukkan ke dalam bagian penutup dari laporan, berikut juga dengan rekomendasi atau saran untuk penelitian-penelitian selanjutnya.