Bab I Pendahuluan

1.1 Latar Belakang

Internet telah menjadi bagian dari kehidupan kita sehari-hari, menurut beberapa infomasi yang dilansir dari surat kabar. Indonesia merupakan salah satu negara yang memiliki tingkat penggunaan *internet* yang cukup tinggi, penggunanya dari tahun ke tahun meningkat dari angka yang sangat signifikan. Menurut asosiasi penyedia jasa *internet* Indonesia (APJII) pada tahun 2015 pengguna *internet* di Indonesia telah mencapai angka 139 juta pengguna, jika dibandingkan dengan angka 107 juta jiwa, pada tahun 2014, pengguna internet di Indonesia mengalami pertumbuhan 32 juta jiwa di tahun 2014 lalu, bahkan diperkirakan angka pengguna internet ini akan semakin bertambah di tahun- tahun berikutnya. Berikut adalah data pengguna internet dari tahun 1998 – 2015 (asosiasi penyelenggara jasa internet Indonesia) Gambar 1.1 menunjukkan statistik jumlah pengguna internet di Indonesia dari tahun 1998 – 2015, yang dilansir dari situs jasa pengguna internet (APJII).

Gambar 1. 1 jumlah pengguna *internet*

(Sumber: https: //www Inovasipintar.com)

Wifi public (jaringan *nirkabel*) merupakan salah satu sarana yang juga cukup berperan penting dalam peningkatan pengguna internet di Indonesia, menurut (tempo.co, nusa dua) - Indonesia Akan menjadi negara dengan jumlah *Wifi public* terbesar di Asia. Program *Wifi id*

yang digagas pada tahun 2015 oleh pt. Telekomunikasi Indonesia menargetkan pemasangan 10 juta titik AP (*Access point)* di tanah air, dimungkinkan Indonesia akan menjadi salah satu negara dengan jumlah pemasangan *Wifi public* terbesar di dunia, didukung dengan tingginya minat masyarakat dalam pemanfaatan internet, kini telah banyak dibangun hot-spot diberbagai tempat seperti café, restoran dan supermarket dan *area* bisnis lainnya dengan alasan bisa agar dapat menarik para pengujung walaupun dengan tingkat keamanan yang rendah (nakhila et al. 2015).

Internet pada jaringan *Wifi* banyak diminati masyarakat sebagai sarana untuk melakukan berbagai macam aktivitas seperti, bisnis, transaksi jual beli, aktivitas pembayaran dan berbagai macam hal lain, namun tanpa disadari hal ini bisa mengundang bahaya yang tak diduga, faktanya telah terjadi banyak kasus pencurian data melalui jaringan *Wifi* dimana para pelaku mencoba melakukan tindak kejahatan seperti dengan melancarkan serangan *Evil Twin* untuk memantau lalu lintas data dengan menggunakan teknik *Man In The Middle Attack* pada jaringan *Wifi* kemudian menggali data maupun informasi penting milik *user* untuk kepentingannya.

Namun sayangnya penanganan tindak kejahatan yang melibatkan teknologi *wireless* khususnya serangan *MITM* dengan teknologi *wireless* masih sangatlah minim untuk saat ini, dikarenakan masih kurangnya sumber daya manusia yang tersedia, dan kurangnya (SOP) *standard operational procedure* dalam penanganan dibidang forensik sehingga mengakibatkan semakin meningkatnya kriminalitas berbasis *cybercrime* khususnya pada kasus *MITM Based Evil Twin,* yang merupakan salah jenis tindak kejahatan berbasis jaringan wireless, *Evil Twin* adalah sebuah AP palsu yang dibuat sengaja untuk mengecoh para pengguna, dengan nama (*SSID*) (*service set identification*) yang sama bahkan nyaris tidak berbeda dengan *legitimate* AP atau AP yang sah (lanze et al. 2015). Hal ini lah yang menyebabkan banyaknya para pengguna jaringan *wireless* yang terkecoh dan masuk dalam jebakan pelaku, selanjutnya pelaku dapat dengan leluasa melakukan *sniffing, phishing,* dan *illegal activity* lainya, dengan menggunakan teknik *Man In The Middle Attack* (mustafa & xu 2014). Terdapat dua jenis serangan pada *Evil Twin*, pertama yaitu *Evil Twin* dikonfigurasikan menggunakan IP *getaway* yang disamakan dengan *router* AP oleh pelaku, sedangkan yang kedua *Evil Twin* AP dikonfigurasikan menggunakan *getaway* yang berbeda dengan *router* AP. Pada kasus ini pembahasan akan lebih mengarah pada jenis serangan yang ke dua, dimana *Evil Twin* mengkonfigurasi kan IP *getaway* yang berbeda dengan *getaway router* AP, sehingga mengakibatkan pelaku tak dapat dijangkau oleh pengawasan administrator, dalam menganalisa dan mendeteksi serangan, dibutuhkan metode lain yang dapat menangani jenis serangan tersebut, yaitu dengan menggunakan pendekatan berbasis *wired* atau *user*, Sehingga dapat membantu penyidik dalam melakukan investigasi

Beberapa praktisi IT sebelumnya pernah melakukan penelitian terkait penanganan serangan *Evil Twin* dengan menggunakan berbagai metode, seperti (mustafa & xu 2014) membahas tentang bagaimana mendeteksi serangan *Evil Twin attack* berbasis *mobile,* (Yang et al. 2012). Membahas tentang bagaimana mendeteksi serangan *Evil Twin* menggunakan metode *statically detection,* (nakhila et al. 2015). Membahas tentang bagaimana mendeteksi serangan *Evil Twin* menggunakan *protocol* TCP /IP, Namun sayangnya penanganan serangan *Evil Twin* yang dilakukan hanya bersifat mendeteksi dan melakukan langkah mitigasi serangan, tanpa adanya tindakan lebih lanjut yang berhubungan dengan forensik, dikarenakan alasan inilah dalam penelitian ini akan membahas bagaimana melakukan investigasi forensik pada kasus *MITM Based Evil Twin attack,* dengan menerapkan beberapa metode forensik seperti metode *live* forensik yaitu suatu proses pengumpulan data pada sebuah sistem yang sedang berjalan, menurut (adelstein 2006) data forensik yang dikumpulkan melalui sistem sedang berjalan tersebut dapat memberikan bukti yang tidak dapat diperoleh dari statik disk *image*. Data yang dikumpulkan tersebut merupakan representasi dari sistem yang dinamis dan tidak mungkin untuk diproduksi ulang pada waktu berikutnya (adelstein 2006), selanjutnya hasil penelitian Akan dibuatkan suatu bagan alur yang efektif dalam melakukan penanganan investigasi forensik pada kasus *MITM Based Evil Twin attack*

1.2 Rumusan Masalah

Merujuk kepada latar belakang yang telah dipaparkan sebelumnya, maka dapat diambil rumusan masalah di dalam penelitian ini, yaitu sebagai berikut :

a. Bagaimana Cara mendeteksi dan mengetahui karakteristik dari serangan *MITM Based Evil Twin,* dengan menggunakan pendekatan *wired* (*user side*)?
b. Bagaimana melakukan tahapan *live* forensik untuk investigasi kasus *MITM Based Evil Twin,* sehingga dapat dirancang kerangka tahapan investigasi?

1.3 Batasan Masalah

Beberapa batasan masalah yang ditetapkan di dalam penelitian ini adalah sebagai berikut :

c. Penelitian dilakukan pada hot spot area universitas islam indonesia yogyakarta, yaitu fakultas teknik industri
d. Jenis serangan Evil Twin menggunakan konfigurasi IP getaway yang berbeda dengan gateway router AP.
e. Pendeteksian serangan Evil Twin menggunakan pendekatan wired atau user side.
f. Identifikasi illegal activity membahas tentang serangan Man in The Middle (MITM) yang digabungkan dengan serangan Evil Twin.

g. Data-data maupun barang bukti yang ditemukan menggunakan beberapa tools bantuan seperti Chellam, Xarp, Arcilyric-Wifi, dan Wireshark.
h. Proses investigasi forensik menggunakan metode live forensik yang disesuaikan dengan sifat kasus dari Evil Twin Based MITM sehingga dapat membantu proses pencarian bukti dalam investigasi forensik.
i. Kerangka investigasi diimplementasikan dengan model network forensik *generic* proses (NFGP), yang Akan dikembangkan berdasarkan kasus yang diteliti.

1.4 Tujuan Penelitian

Tujuan penelian yang di harapkan dari penelitian ini adalah :

a. Mendeteksi dan mengetahui karakteristik dari serangan MITM Based Evil Twin, dengan menggunakan pendekatan wired (user side).
b. Melakukan tahapan live forensik untuk investigasi kasus MITM Based Evil Twin, sehingga dapat dirancang kerangka tahapan investigasi.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah :

a. Pengembangan ilmu *network* forensik khususnya dalam bidang *Wireless* forensik.
b. Memberikan informasi tentang pola penyerangan *Evil Twin* AP *based MITM*.
c. Memberikan informasi *step-by step* penangan serangan *MITM Based Evil Twin* dari sisi *user*.
d. Mengembangan penelitian penelitian sebelumnya.
e. Dapat mengetahui proses penyerangan *Evil Twin* untuk mendapatkan bukti *digital* pada serangan dalam serangan *Evil Twin* AP.
f. Bagi penulis penelitian ini diharapkan dapat menambah wawasan, kualitas keilmuan baik dalam hal teori maupun praktek.

1.6 Review Penelitian

Serangan *Evil Twin* merupakan suatu jenis serangan yang sangat berbahaya dan telah banyak mengakibatkan kerugian bagi para pengguna jaringan *wireless*, dengan Cara menggabungkan teknik *Man In The Middle Attack* mengakibatkan semakin berbahayanya jenis serangan ini Beberapa peneliti sebelumnya telah berusaha melakukan penelitian untuk menindak lanjuti kasus ini seperti, mustafa & xu (2014) melakukan penelitian untuk mendeteksi *Evil Twin* AP dengan membuat *tools* Cetad. Yang merupakan sebuah aplikasi untuk ponsel berbasis android yang dapat digunakan untuk mendeteksi serangan *Evil Twin* dalam suatu *hotspot* nirkabel, dengan menggunakan mekanisme yang dapat mendeteksi serangan *Evil Twin* pada *hotspot* nirkabel dan dapat diinstal pada *Wifi*, ketika *tool* diaktifkan tanpa perlu menginstal

perangkat keras atau perangkat lunak dalam infrastruktur *hotspot* Selanjutnya penelitian lain dilakukan oleh

Sandeep b. Vanjale (2015) mengatakan bahwa jaringan serangan *Evil Twin* pada dasarnya sangat berbahaya karena mereka dapat melakukan (*phishing*) jalur akses *Wifi* AP *(Access Point*) dengan menggunakan *SSID* yang sama, dengan demikian penyerang dapat dengan mudah mengatur jalur akses berbahaya dengan menjebak *user*, penyerang dapat melancarkan serangan yang lebih serius seperti *Dos, MITM, Syn Attack, dan Fin Attack.*

Penelitian lain dilakukan oleh lanze et al (2015) menuliskan bahwa ancaman *hotspot Wifi* publik *Evil Twin attack,* dimana penyerang membuat sebuah AP palsu, sehingga mengakibatkan para pengguna *Wireless network* tidak dapat membedakan AP yang sah dan AP palsu, setelah terjebak pada AP palsu, pelaku dapat dengan mudah menyerang koneksi klien dan mencuri data sensitif, banyak *tools* dapat ditemukan pada *internet* yang tidak memerlukan keahlian khusus dan dapat digunakan keluar dari kotak untuk me-*Mount* serangan *Evil Twin* dari perangkat komoditas klien. Serangan tersebut dilakukan dengan menggunakan software khusus.airodump-ng, salah satu alat yang paling digunakan. Selanjutnya penelitian lain dilakukan oleh nakhila et al (2015) membahas tentang teknik deteksi baru untuk serangan *Evil Twin attack* dan diusulkan untuk mendeteksi *Evil Twin attack* yang menggunakan *gateway* yang berbeda dibandingkan dengan *gateway* digunakan oleh *hotspot Wifi* sah, teknik deteksi cukup mudah digunakan, karena metode pendeteksian menggunakan pendekatan *user -side* dan dievaluasi dengan menggunakan sample real.

utami putri & istiyanto (2012) menuliskan bahwa investigasi forensik jaringan dilakukan untuk mengetahui apaa saja yang terjadi pada jaringan sehingga dapat ditelusuri jejak jejak dari penyerang. Pencarian jejak dari tindakan *illegal* pada jaringan didapatkan dari file log.

mangut et al. (2015) mengatakan bahwa *tools Tcpdump, Wireshark, Tcpstat, dan Ntop* sebagai berguna alat dan teknik yang akan digunakan dalam forensik investigasi *Arp serangan Spoofing.* Penelitian selanjutnya, sandeep b. Vanjale (2015) mengatakan bahwa serangan *Mallisius wireless* sangat berbahaya karena melalui sinyal nir kabel saja, penyerang dapat menyerang dengan sesuatu yang lebih serius seperti *Dos, MITM, Syn Attack, dan Fin attack,* serangan berbahaya adalah ancaman yang sangat buruk untuk keamanan *wlan*, dan mereka menyajikan solusi suatu aplikasi berupa *intrusion* sederhana untuk deteksi dan pencegahan *Acsess point* berbahaya dalam jaringan *wireless lan.*

cai et al. (2014) mengatakan bahwa jaringan nirkabel jauh lebih rentan terhadap serangan *MITM* (*Man In The Middle*) jaringan mobile tidak dapat melakukan validasi karena memiliki fitur *authentication* yang terbatas dalam menggunakan metode *EAPS, EAPS* adalah salah satu metode yang digunakan untuk melindungi komunikasi dan melakukan transaction authentication

di 802.1x, metode EAPS menyediakan : *authentication*, *resistensi* terhadap serangan *MITM*, dan perlindungan *cipher suite negotiation*.

dong et al (2015) mengatakan bahwa pendeteksian *MITM* (*man- in-the middle-attack*), dapat dilakukan dengan menggunakan beberapa metode seperti *K Nearest Neighbors*, *Gaussian Naive bayes, and Support vector machine*, untuk mendapatkan akurasi dalam mendeteksi lokasi dari para pelaku dengan lebih maksimal.

anmulwar et al (2014) mengatakan bahwa pendeksian dapat dilakukan dengan menggunkan metode *hybrid* yaitu dengan cara menggunakan dua pendekatan yang berbeda dalam mengatasi serangan *Rogue Access point.* Metode *hybrid* adalah penggabungan antara pendekatan keamanan *server* dan keamanan dari sisi *client*, (Chandavarkar et al. 2015) menuliskan bahwa *Rogue Access Point* telah menjadi suatu ancaman yang sangat berbahaya bagi keamanan jaringan *Wifi*. Pendeteksian dapat dilakukan dengan menggunkan metode *kismet* berbasis GUI, yang berfungsi untuk membantu dalam pelacakan semua titik-titik yang menyebabkan masalah keamanan ke jaringan, dan juga mampu menganalisis kekuatan sinyal yang berbeda jaringan dan menjaga melacak jalur akses terbaik.

nanavare (2016) menuliskan identifications serangan *Evil Twin* dapat digunakan dengan menerapkan pendekatan dari sisi pengguna pendekatan wired, dikarenakan kebanyakan metode pendeteksian dari sisi administrator diharuskan memiliki autorisasi AP dan menurutnya metode ini relative sulit karena itu diusung sebuah metode yang dapat mendeteksi *Evil Twin attack* dari sisi user.

Literature review dari beberapa penelitian terdahulu dengan penelitian yang akan dilakukan disajikan ke dalam tabel 1.1 seperti dibawah ini

Tabel 1.1 literatur review

No	Paper utama	Kasus penelitian		Teknik pendeteksian	Metode forensik
		Evil twin	***MITM***		
1	(utami putri & istiyanto 2012)	–	–	Teknik pendeteksian menggunakan pendekatan dari sisi *administrator*/ server	Analisis forensik jaringan menggunakan metode proses forensik
2	(cai et al. 2014)	√	√	Menggunakan pendekatan *user* berbasis mobile, untuk mendeteksi serangan *mitm based evil twin*	–
3	(mustafa & xu 2014)	√	–	Deteksi serangan *evil twin attack* berbasis mobile	–
4	(mangut et al. 2015)	–	√	Melakukan pendeteksian serangan *MITM*, *menggunakan tools* forensik	Investigasi forensik teknik *live* forensik dengan pemanfaatan *tools* forensik
5	(dong et al. 2015)	–	–	Menggunakan penggabungan dua metode k nearest neighbors, gaussian naive bayes, and sup*port* vector machine, untuk mendeteksi serangan *MITM*	–

Tabel 1.1 literatur review (lanjutan)

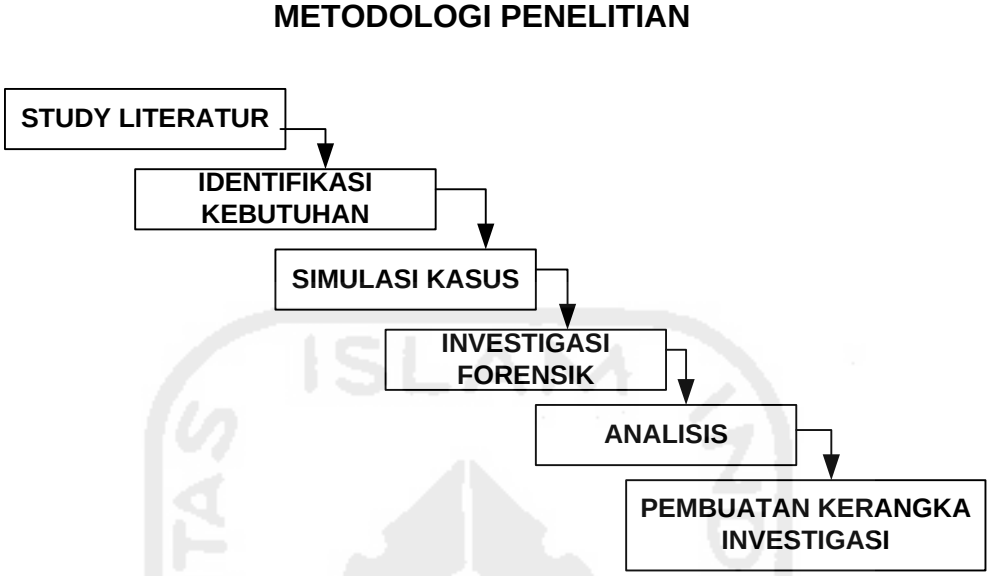
No	Paper utama	Kasus penelitian		Teknik pendeteksian	Metode forensik
		Evil twin	*MITM*		
6	(anmulwar et al. 2014)	√	–	Mendeteksi serangan *evil twin* menggunakan metode review berdasarkan pendekatan metode hybrid	–
7	(nakhila et al. 2015)	√	–	Mendeteksi serangan *evil twin* yang menggunakan *gateway* yang berbeda di bandingan *gateway hotspot*. Dengan *menggunakan* metode wired atau *user* side.	–
8	(chandavarkar et al. 2015)	√	–	Deteksi rogue AP dengan menggunakan aplikasi kismet, pendeteksian ini lebih mengarah pada metode wireless atau pendeteksian yang di lakukan di dalam area administrator	–
9	(lanze et al. 2015)	√	–	Mendeteksi serangan *evil twin* menggunakan tool box detection software berdasarkan pendekatan wireless	–

Tabel 1.1 literatur review (lanjutan)

No	Paper utama	Kasus penelitian		Teknik pendeteksian	Metode forensik
		Evil twin	***MITM***		
10	(nanavare 2016)	√	–	Melakukan pendeteksian *evil twin* AP dengan menerapkan pendekatan *wired* atau bar basis *user side*	–
11	**Usulan penelitian**	√	√	Deteksi serangan *evil twin* based menggunakan pendekatan wired atau *user*	Melakukan investigasi forensik *menggunakan* metode *live* forensik untuk membuat kerangka investigasi
		Dari beberapa review penelitian sebelumnya dapat di ketahui bahwa belum ada penelitian tentang implementasi metode forensik dalam penanganan *MITM Based Evil Twin attack*, sebagian besar hasil penelitian *paper* di atas hanya meliputi tentang bagaimana cara mendeteksi pola penyerangan dari *MITM based evil twin*, berdasarkan hal ini, pengusulan penelitian akan mencoba membahas bagaimana melakukan investigasi forensik pada kasus *evil twin* ini dengan menggunakan pendekatan berbasis *user* atau wired, dalam menangani kasus *evil twin* yang menggunakan *getaway* yang berbeda.			

1.7 Metodologi Penelitian

Dalam melakukan penelitian, perlu disusun langkah – langkah metodologi dalam menyelesaikan penelitian.



Gambar 1. 2 skema metodologi penelitian

Berdasarkan skema di atas, usulan metodologi penelitian

1. *Study literatur* Akan membahas tentang uraian dari teori, temuan maupun rangkuman – rangkuman dari penelitian sebelumnya yang nanti dapat digunakan sebagai landasan atau acuan dalam melakukan kegiatan penelitian.
2. Identifikasi kebutuhan merupakan suatu presses persiapan alat dan bahan yang Akan digunakan dalam melakukan proses investigasi, seperti *tools* bantuan, *hardware* maupun *software* yang dapat digunakan dalam penelitian.
3. *Simulasi* kasus merupakan kegiatan uji coba serangan *Evil Twin* di area *hotspot*, identification serangan dari sisi *user* dan proses implementasi metode forensik terhadap kasus yang Akan diteliti.
4. Tahapan investigasi merupakan tahapan dimana *user* melakukan proses identification dengan menerapkan metode forensik, pada penelitian ini metode yang digunakan adalah metode *live* forensik, yang mana terdiri atas beberapa tahapan yaitu: tahapan pra analisis, dan tahapan analisis.
5. Perancangan kerangka investigasi adalah tahapan hasil akhir dari hasil penelitian berupa sebuah rancangan kerangka investigasi yang dikhususkan untuk penanganan kasus *Evil Twin Based MITM*

1.8 Sistematika Penulisan

Dalam penyusunan penelitian ini, systematic penulisan terbagi dalam beberapa Bab yaitu:

Bab I Pendahuluan

Pendahuluan, merupakan pengantar terhadap permasalahan yang Akan dibahas. Di dalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, serta systemati penulisan.

Bab II Landasan Teori a

Pada bab ini menjelaskan teori-teori yang digunakan untuk memecahkan masalah
Dalam penelitian ini.

Bab III Metodologi Penelitian

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat keras dan perangkat lunak yang Akan digunakan serta perancangan antarmuka aplikasi yang Akan dibuat.

Bab IV Hasil dan Pembahasan

Hasil dan pembahasan, berisi tentang pembahasan penyelesaian masalah yang diangkat yaitu dengan melakukan analisis dan uji coba dan penerapan metode forensik sesuai dengan yang diusulkan.

Bab v kesimpulan dan saran

Simpulan dan saran, memuat kesimpulan-kesimpulan dari hasil penelitian dan saran-saran yang perlu diperhatikan berdasar keterbatasan yang ditemukan dan asumsi-asumsi yang dibuat selama melakukan penelitian dan juga rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.