INVESTIGASI LIVE FORENSIK DARI SISI PENGGUNA UNTUK MENGANALISA SERANGAN *MAN IN THE MIDDLE ATTACK* BERBASIS *EVIL TWIN*

Muhammad Sabri Ahmad
14917154

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi {Nama Konsentrasi}

Program Studi Magister Teknik Informatika

Program PascasarjanaFakultas Teknologi Industri

Universitas Islam Indonesia

2017

Lembar Pengesahan Pembimbing

INVESTIGASI LIVE FORENSIK DARI SISI PENGGUNA UNTUK MENGANALISA SERANGAN MAN IN THE MIDDLE ATTACK BERBASIS EVIL TWIN

Nama: Muhammad Sabri Ahmad

NIM: 14917154

Yogyakarta, Januari 2017

Pembimbing I	Pembimbing II
Dr.Imam Riadi, M.Kom	Yudi Prayudi,.S.Si.,M.Kom

Lembar Pengesahan Penguji

INVESTIGASI LIVE FORENSIK DARI SISI PENGGUNA UNTUK MENGANALISA SERANGAN MAN IN THE MIDDLE ATTACK BERBASIS EVIL TWIN

Nama: Muhammad Sabri Ahmad

NIM: 14917154

Yogyakarta, Januari 2017

Tim Penguji,

Dr. Imam Riadi, M.Kom
Ketua

Yudi Prayudi, S.SI., M.Kom
Anggota I

Dr Bambang Sugiantoro.,M.Kom
Anggota II

Mengetahui,
Direktur Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, ST., M.Sc

Abstrak

MITM Based Evil Twin menjadi suatu ancaman yang berbahaya bagi para pengguna jaringan *Wifi*. Pelaku penyerangan ini memanfaatkan AP (*access point*) palsu dengan setingan *gateway* yang berbeda dengan *legitimate* AP, sehingga jenis serangan ini menjadi cukup sulit untuk dideteksi. Proses pengungkapan kasus serangan *MITM based Evil Twin* hanya sebatas mendeteksi aktivitas serangan dan belum ada pembahasan lebih lanjut terkait digital forensik, hal ini di sebabkan karena masih kurangnya SOP (*standart operational Procedure*) dalam menangani kasus ini. Penelitian ini dilakukan dengan tujuan untuk membuat suatu model forensik berdasarkan tahapan analisa dalam kasus *MITM based Evil Twin.*

Proses dalam investigasi *MITM based Evil Twin* dilakukan dengan menggunakan metode *live* forensik berbasis *user side*, kemudian dibagi kedalam dua fokus penelitian yaitu, proses analisa *Wifi scanning* untuk melakukan investigasi serangan *Evil Twin* dengan menganalisa atribut maupun kegitan-kegitan yang mencurigakan lainya. Analisa investigasi serangan *MITM* dilakukan dengan menganalisa *network traffic* dalam *area Evil Twin.*

Hasil investigasi forensik dalam penelitian, 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.

Kata kunci: *Wifi, Evil Twin, Live, forensik, MITM.*

Abstract

Based MITM Evil Twin become a dangerous threat to the Wifi network users. The perpetrators of the attacks take advantage of the AP (access point) with a fake gateway settings that differ from legitimate AP, so that this type of attack is becoming quite difficult to detect. The disclosure of MITM attack case based Evil Twin merely detect seizure activity and there has been no further discussion related to digital forensics, this is caused because there is a lack of SOP (standard operational procedure) in handling this case. This research was conducted with the aim to create a model based on the phases of forensic analysis in the case of MITM based Evil Twin.

The process in the investigation of MITM based Evil Twin performed using user-based live forensic side, then split into two, namely research focus, process analysis Wifi scanning to investigate Evil Twin attacks by analyzing the attribute or activity suspicious-activity of others. MITM attacks investigative analysis is done by analyzing network traffic in the area of Evil Twin.

The results of forensic investigations in research, produce a model investigation ENFGP (Extendend NFGP) which is divided into 10 stages and consists of 30 steps - steps completion, which is obtained through the process of testing and implenmentasi method in case of a MITM attack Based Evil Twin and further testing by some forensic previous models.

***Keywords**: Wifi, Evil Twin, Live, forensics, MITM*

iii

Pernyataan keaslian tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak ciptayang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, 14 januari 2017

Muhammad Sabri Ahmad.,S.Kom

Publikasi selama masa studi

Tidak ada publikasi yang menjadi bagian dari tesis

Kontribusi yang diberikan oleh pihak lain dalam tesis ini

Tidak ada kontribusi dari pihak lain

Halaman Persembahan

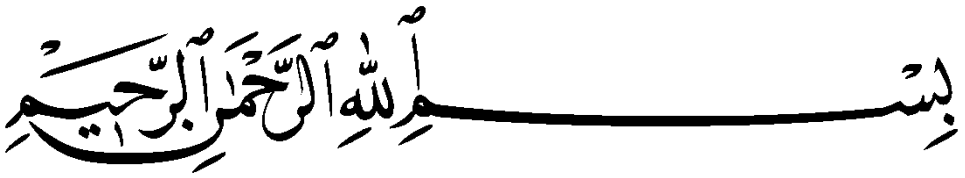
Alhamdulillah atas segala rahmat, hidayah, berkah dan kasih sayang Allah SWT yang selalu menemani disetiap langkah dan kondisi penulis..

Alhamdulillah atas kehadiran Baginda Rosulullah SAW yang menjadi pelita dalam ilmu pengetahuan..

Terima kasih kepada Bapak, Mama, dan kakak serta keluarga besar dan Teman-teman angkatan X forensik Digital yang telah mensupport penulis dalam setiap proses memperbaiki diri, salah satunya dengan medmberikan kesempatan untuk mengenyam pendidikan hingga saat ini.. terima kasih atas segala upaya yang dicurahkan disetiap waktu..

Terima kasih kepada teman dan sahabat yang telah bersedia berbagi ilmu, pengalaman dan kisah serta dukungan yang membangun..

Kata Pengantar



Assalamu'alaikum Wr. Wb.

Alhamdulillah segala puji bagi Allah SWT atas segala rahmat, hidayah, dan kehadirat-Nya, sehingga penulisan laporan tesis sebagai salah satu syarat memperoleh gelar Pascasarjana Magister Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia yang berjudul "Investigasi Live Forensik Dari Sisi Pengguna Untuk Menganalisa Serangan Man In The Middle Attack Berbasis Evil Twin" dapat diselesaikan dengan baik. Shalawat serta salam semoga senantiasa tercurah atas Nabi Muhammad SAW, para sahabat, serta pengikutnya.

Penyusunan tesis ini tidak lepas dari bimbingan, dukungan, dan bantuan dari berbagai pihak. Oleh Karena itu dalam kesempatan ini dan segala kerendahan hati, ucapan terima kasih diucapkan dengan setulus-tulusnya kepada:

1. Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis selalu diberkan kesehatan dan kemudahan selama masa pengerjaan tesis ini.
2. Bapak, Ibu, kakak, beserta keluarga besar yang telah mendoakan dan memberikan restu dan semangatnya.
3. Bapak Rektor dan seluruh jajaran rektorat Universitas Islam Indonesia.
4. Dr. R. Teduh Dirgahayu, ST., M.Sc selaku direktur Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia.
5. Dr. Imam Riadi, M.Kom dan Yudi Prayudi, S.Si.,M.Kom selaku dosen pembimbing yang telah memberikan pengarahan, bimbingan, masukan, serta dorongan semangat selama pengerjaan tesis ini.
6. Dosen-dosen Magister Teknik Informatika dan seluruh jajaran staf program Pascasarjana. Terima kasih atas semua ilmu pengetahuan, saran, motivasi, serta bantuannya.

7. Rekan-rekan Forensik Digital UII Angkatan X. terima kasih atas semua dukungan dan kerja samanya selama ini.
8. Keluarga besar Magister Teknik Informatika UII.
9. Rekan-Rekan Collayers, Rekan-Rekan Kosan Degolan, terima kasih atas semua dukungan dan kerja samanya selama ini
10. Terimakasih kepada kekasih tercinta yang jauh di malang, terimakasih atas dukunganya.
11. Sahabat-sahabat yang jauh disana dan selalu mendoakan, terima kasih.
12. Semua pihak yang telah memberikan bantuan dan dorongan yang tidak dapat disebutkan satu-persatu.

Saya menyadari bahwa dalam penulisan dan penyusunan laporan tesis ini masih banyak terdapat kekurangan. Untuk itu saya sampaikan permohonan maaf serta sangat mengharapkan kritik dan saran yang membangun untuk penyempurnaan di masa yang akan datang.

Yogyakarta, 2016

Muhammad Sabri Ahmad

Daftar Isi

Daftar Gambar

Daftar Tabel

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)

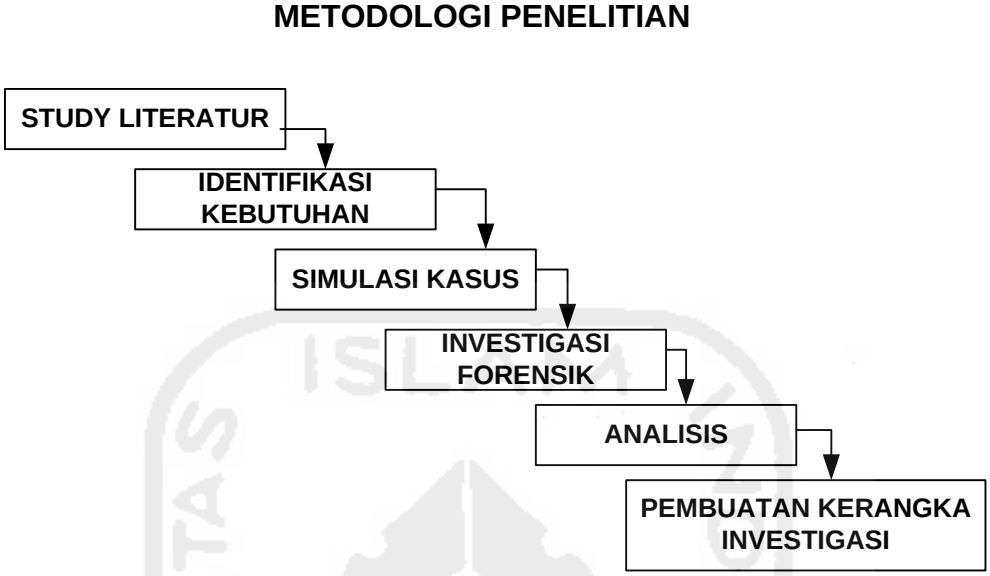
No	Paper utama	Kasus penelitian		Teknik pendeteksian	Metode forensik
		Evil twin	*MITM*		
6	(anmulwar et al. 2014)	√	–	Mendeteksi serangan *evil twin* menggunakan metode review berdasarkan pendekatan metode hybrid	–
7	(nakhila et al. 2015)	√	–	Mendeteksi serangan *evil twin* yang menggunakan *gateway* 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.

Bab II Landasan Teori

2.1 *Cyber Crime*

Cybercrime adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara *online*, pemalsuan cek, penipuan kartu kredit/*carding*, *confidence* fraud, penipuan identitas, pornografi anak, dll

Menurut brenda nawawi (2001) kejahatan cyber merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi beberapa sebutan diberikan pada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain: sebagai " kejahatan dunia maya" (*cyberspace/virtual-space offence*), dimensi baru dari "*hi-tech crime*", dimensi baru dari "*transnational crime*", dan dimensi baru dari "*white collar crime*".

Secara hukum di Indonesia pun telah memiliki undang- undang khusus menyangkut kejahatan dunia maya, yaitu undang ITE tahun 2008, yang membahas tentang tata Cara, batasan penggunaan computer dan sangsi yang akan diberikan jika terdapat pelanggaran. Misalnya perbuatan *illegal* access atau melakukan akses secara tidak sah perbuatan ini sudah diatur dalam pasal 30 undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik disebutkan, bahwa: "setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain ayat (1)) dengan cara apapun, (ayat (2)) dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, (ayat (3)) dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol system pengaman

2.1.1 Jenis –Jenis *Cybercrime*.

Cybercrime pada dasarnya tindak pidana yang berkenaan dengan informasi, sistem informasi (information system) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi itu kepada pihak lainnya (transmitter/originator to recipient) menurut (sutanto) dalam bukunya tentang *cybercrime*-motif dan penindakan *cybercrime* terdiri dari dua jenis, yaitu:

a. Kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas. Contoh-contoh dari aktivitas cybercrime jenis pertama ini adalah pembajakan (*copyright* atau hak cipta intelektual, dan lain-lain); pornografi; pemalsuan dan pencurian kartu kredit (carding); penipuan lewat e-mail; penipuan dan pembobolan rekening bank; perjudian on line; terorisme; situs sesat; materi-materi internet yang berkaitan dengan sara (seperti penyebaran kebencian etnik dan ras atau agama); transaksi dan penyebaran obat terlarang; transaksi seks; dan lain-lain
b. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi (ti) sebagai sasaran. *Cybercrime* jenis ini bukan memanfaatkan komputer dan internet sebagai media atau sarana tindak pidana, melainkan menjadikannya sebagai sasaran. Contoh dari jenis-jenis tindak kejahatannya antara lain pengaksesan ke suatu sistem secara ilegal (*hacking*), perusakan situs *internet* dan *server data* (*cracking*), serta *defecting*.

Menurut freddy haris, *cybercrime* merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut:

a. *Unauthorized access* (dengan maksud untuk memfasilitasi kejahatan);
b. Unauthorized alteration or destruction of data;
c. Mengganggu/merusak operasi komputer

2.1.2 Kualifikasi *CyberCrime*

Kualifikasi kejahatan dunia maya (*cybercrime*), sebagaimana dalam buku Barda nawawi arief, adalah kualifikasi (*cybercrime*) menurut convention on *cybercrime* 2001 di Budapest Hongaria, yaitu: *illegal* access: yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak. Sedangkan kualifikasi kejahatan dunia maya (cybercrime), sebagaimana dalam buku barda nawawi arief, adalah kualifikasi (cybercrime) menurut Convention on *cybercrime* 2001 di Budapest Hongaria, yaitu:

a. *Illegal interception*: yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu.
b. *Data interference*: yaitu sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer.
c. *System interference*: yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer.
d. *Misuse of devices*: penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (*access code*).
e. *Computer related forgery:* pemalsuan (dengan sengaja dan tanpa hak memasukkan mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik)
f. *Computer related fraud*: penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain);
g. *Content-related offences*: delik-delik yang berhubungan dengan pornografi anak (*child pornography*);
h. *Offences related to infringements of copyright and related rights:* delik-delik. Yang terkait dengan pelanggaran hak cipta.

2.2 Forensik

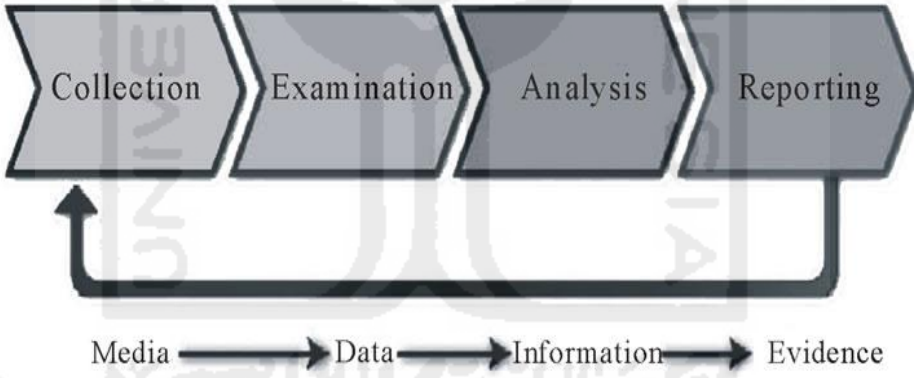
Forensik merupakan salah satu cabang bidang forensik paling muda diantara beberapa bidang forensik lainnya, *digital* forensik merupakan salah satu cabang ilmu forensik yang berhubungan dengan bukti hukum yang ditemukan dalam komputer maupun media penyimpanan secara *digital, Digital* forensik ini dikenal sebagai komputer forensik banyak bidang ilmu yang dimanfaatkan dan dilibatkan pada suatu kasus kejahatan atau kriminal untuk suatu kepentingan hukum dan keadilan, dimana ilmu pengetahuan tersebut dikenal dengan ilmu forensik

Pada awal abad 19 (1822-1911), seorang ilmu an bernama Francis Galton menemukan sebuah metode, dimana menggunakan “sidik jari” sebagai media untuk mengungkap sebuah kasus, kemudian diikuti oleh ilmu an bernama Leone lattes (1887-1954) yang menemukan konsep penanganan barang bukti menggunakan golongan darah (a,b,ab & o), dan di akhir abad 19 (1891-1955), ditemukannya senjata dan peluru (balistik) oleh seorang ilmu an bernama Calvin goddard, dan Albert osborn (1858-1946) menemukan metode *document* examination,

selanjutnya HANS gross (1847-1915) yang menerapkan ilmiah dalam investigasi criminal dalam pengungkapan sebuah kasus, dan yang terakhir, FBI pada tahun (1932) membuat lab forensik.

2.3 *Digital* Forensik

Digital forensik merupakan salah satu cabang ilmu forensik yang berhubungan dengan bukti hukum yang ditemukan dalam komputer maupun media penyimpanan secara *digital*, *digital* forensik ini dikenal sebagai komputer forensik menurut Marcella *digital* forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti *digital* dalam kejahatan computer. Sedangkan menurut Casey: *digital* forensik adalah karakteristik bukti yang mempunyai kesesuaian dalam mendukung pembuktian fakta dan mengungkap kejadian berdasarkan bukti statistik yang meyakinkan. Dari beberapa pendapat sebelumnya dapat disimpulkan bahwa *digital* forensik suatu kegiatan pencarian yang melalui proses identification, filterisation dan dokumentasi yang mempunyai kekuatan sebagai pendukung pembuktian fakta. Gambar 2.1 merupakan tahapan implementasi metode dalam *digital* forensik



Gambar 2. 1 tahapan-tahapan investigasi *digital* forensik

Tahapan metode *digital* forensik terdiri atas tahap yaitu:

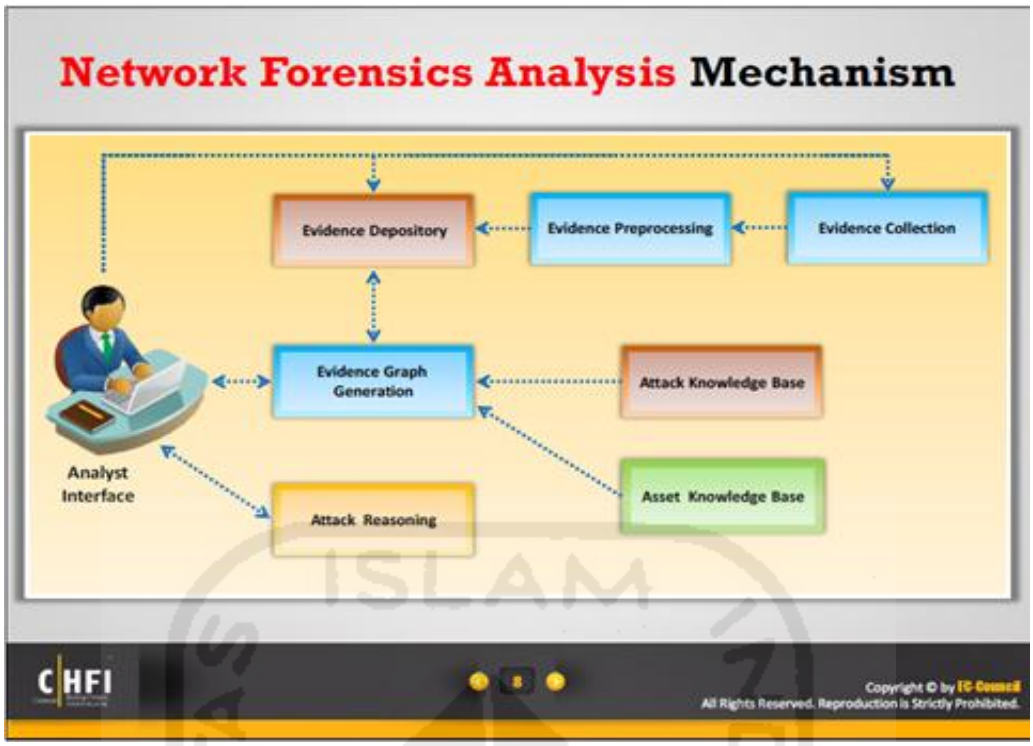
- Pengumpulan(*collection*) : merupakan metode awal dalam melakukan proses investigasi, dengan cara mengumpulkan data-data yang dianggap terkait dengan kasus yang terjadi.
- Pemeliharaan (*examination*) : merupakan kegiatan pengumpulan atau pemeliharaan barang bukti yang akan digunakan sebagai analisa.
- Analisa (*analysis*) merupakan tahapan dalam menganalisa berkas barang bukti yang ditemukan.

- Presentasi (*presentation*) merupakan kegiatan akhir dalam suatu proses investigasi forensik, yang mana biasanya berupa sebuah re*port* hasil dari penyelidikan.

2.4 *Network* Forensik

Network forensik adalah salah satu cabang dalam ilmu forensik yang dikhususkan dalam bidang *Networking* dimana Cara kerjanya meliputi semua kemungkinan yang dapat menyebabkan pelanggaran keamanan *system* dengan Cara melakukan identification melalui analisa *trafik* data, *sniffing* dan lain-lain

(Ruchandani b. 2006) forensik jaringan merupakan bagian dari forensik *digital*, dimana bukti ditangkap dari jaringan dan diinterpretasikan berdasarkan pengetahuan dari serangan jaringan hal ini bertujuan untuk menemukan penyerang dan merekonstruksi tindakan serangan penyerang melalui analisis bukti penyusupan menurut (Singh, o. 2009) *network* forensik adalah kegiatan menangkap, mencatat dan menganalisis kejadian pada jaringan untuk menemukan sumber serangan keamanan atau masalah kejadian lainnya. Karena demikianlah data merupakan suatu hal yang sangat penting untuk mendukung suatu proses investigasi. Sedangkan menurut Ec-council (2010) suatu lembaga pelatihan yang bergerak khusus dibidang *digital* forensik, dalam salah satu bukunya, mengatakan bahwa *network* forensik adalah kegiatan pengumpulan barang bukti dengan Cara merekam, dan analisa lalu lintas data pada suatu jaringan dengan tujuan untuk menemukan sumber dari sebuah serangan. Demikian maka *network* forensik merupakan suatu aktifitas pengumpulan barang bukti yang dilakukan melalui beberapa Cara salah satunya dengan Cara pengamatan dari *traffic* atau lalu lintas jaringan, dikarenakan lalulintas jaringan internet banyak terdapat data penting yang mungkin bisa dianalisa dan dijadikan barang bukti Gambar.2.2 menunjukkan tahapan dalam proses pencarian barang bukti pada *network* forensik.



Gambar 2. 2 Mekanisme Analisa *Network* Forensik

(Sumber modul 16 *CHFI*)

2.5 Bukti *Digital*

Bukti *digital* didefinisikan sebagai fisik atau informasi elektronik (seperti tertulis atau dokumentasi elektronik, komputer *file log*, data, laporan, fisik *hardware*, *software*, disk gambar, dan sebagainya) yang dikumpulkan selama investigasi komputer dilakukan bukti mencakup, namun tidak terbatas pada, komputer *file* (seperti *file log* atau dihasilkan laporan) dan file yang dihasilkan manusia (seperti *spreadsheet*, dokumen, atau pesan email).

Menurut (t. Sukardi. 2012) Dalam bukunya "forensik komputer prinsip dasar", mengatakan bahwa barang bukti pada dasarnya Sama yaitu merupakan informasi dan data, hanya saja kompleksitas dan media penyimpanannya yang mengubah sudut pandang dalam penanganannya. Barang bukti *digital* dalam komputer forensik secara garis besar terbagi menjadi 3 jenis, yaitu:

1. Data *aktif*, yaitu data yang terlihat dengan mudah karena digunakan untuk berbagai kepentingan yang berkaitan erat dengan kegiatan yang sedang dilakukan, misalnya program, *file* gambar, dan dokumen teks.
2. Data arsip, yaitu data yang telah disimpan untuk keperluan backup misalnya dokumen *file* yang digitalization untuk disimpan dalam format *tiff* dengan tujuan menjaga kualitas dokumen.

3. Data *laten*, disebut juga data *ambient* yaitu data yang tidak dapat dilihat langsung karena tersimpan pada lokasi yang tidak umum dan dalam format yang tidak umum misalnya, *database log* dan *internet log*. Data lay juga disebut sebagai *residual* data yang artinya adalah data sisa ataupun data sementara.

2.6 *Live* Forensik

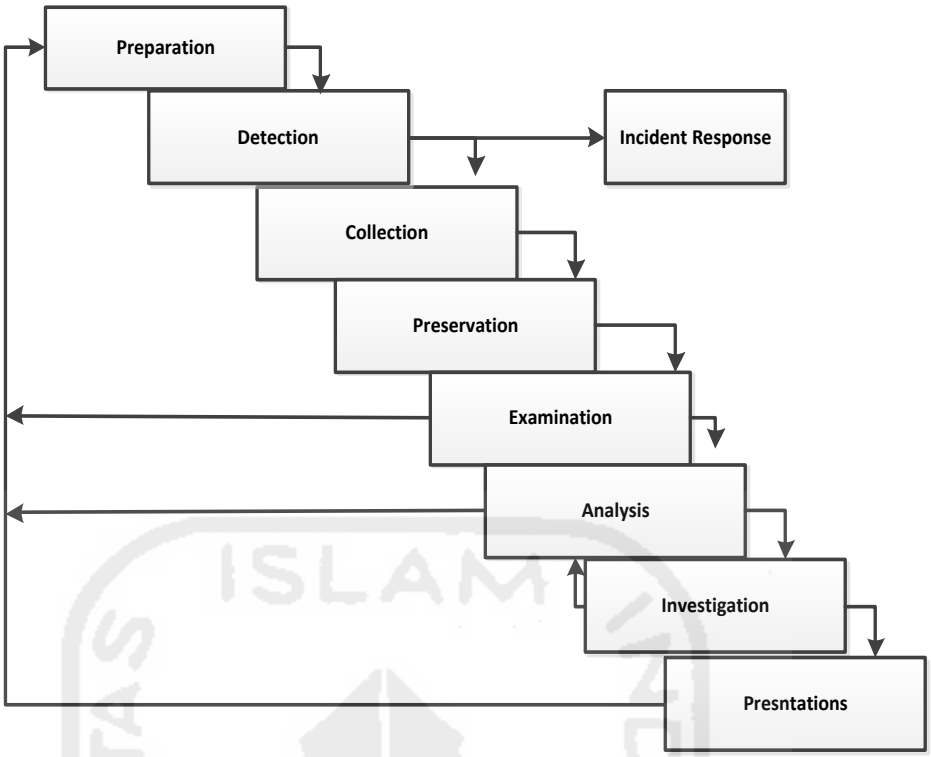
Live forensik merupakan salah satu teknik dalam investigasi digital, pada dasarnya memiliki kesamaan pada teknik forensik tradisonal dalam hal metode yang dipakai yaitu identifikasi penyimpanan, analisis, dan presentasi, hanya hanya saja *live* forensik merupakan respon dari kekurangan teknik forensik tradisonal yang tidak bisa mendapatkan informasi dari data dan informasi yang hanya ada ketika sistem sedang berjalan misalnya aktifitas memory, *network* proses, swap file, running system proses, dan informasi dari file sistem dan ini menjadi kelebihan dari teknik *live* forensik

Menurut (Rahman & Khan 2015). Teknik *live* forensik telah berkembang dalam dekade terakhir, seperti analisis konten *memory* untuk mendapatkan gambaran yang lebih baik mengenai aplikasi dan proses yang sedang berjalan.

Live forensik dilakukan dengan cara mengumpulkan data ketika sistem yang terkena serangan masih berjalan (*running*/*alive*). Data forensik yang dikumpulkan melalui sistem yang *live* tersebut dapat memberikan bukti yang tidak dapat diperoleh dari *static disk image*. Data yang dikumpulkan tersebut merupakan representasi dari sistem yang dinamis dan tidak mungkin untuk diproduksi ulang pada waktu berikutnya (Adelstein 2006).

2.7 *Network* Forensik Generic Proses Model

Network forensik *generic* proses *model* (NFGP), merupakan suatu model atau *framework* forensik yang dirancang untuk menangani kasus –kasus terkait *networking* (Pilli et al. 2010), NFGP sendiri terdiri dari beberapa tahapan seperti yang ter lihat pada Gambar 2.3 dimulai dengan tahapan preparation atau biasa juga disebut sebagai tahap awal persiapan, tahapan *detection* atau tahapan mendeteksi adanya serangan, incident respond atau respon awal apa bila terjadinya serangan, selanjutnya tahapan collection atau tahap pengumpulan data-data terkait barang bukti, tahapan *preservation, examination, analysis, investigation* dan yang terakhir yaitu tahapan *presentation* atau merupakan suatu tahapan akhir dari hasil evaluasi kasus untuk dilanjutkan ke tahap pembuatan laporan.



Gambar 2. 3 *Network* Forensik *Generic* Proses *Model*

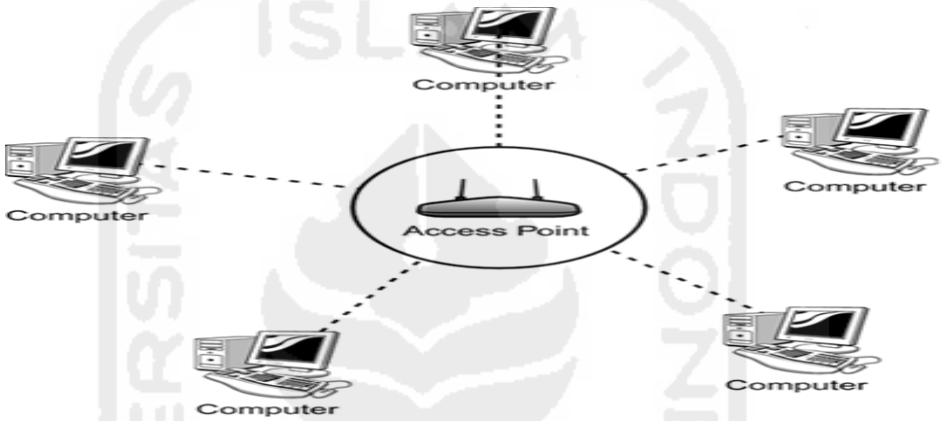
2.8 Wireless Lan

Wireless network merupakan sekumpulan komputer yang saling terhubung antara satu dengan lainnya sehingga terbentuk sebuah jaringan komputer dengan menggunakan media udara/gelombang sebagai jalur lintas datanya pada dasarnya *wireless* dengan *lan* merupakan sama-sama jaringan komputer yang saling terhubung antara satu dengan lainnya, yang membedakan antara keduanya adalah media jalur lintas data yang digunakan, jika *lan* masih menggunakan kabel sebagai media lintas data, sedangkan *wireless* menggunakan media gelombang radio/udara. Penerapan dari aplikasi *wireless network* adalah jaringan *nirkabel* di perusahaan, atau *mobile communication* seperti handphone, dan *ht*. Adapun pengertian lainnya adalah sekumpulan standar yang digunakan untuk jaringan lokal *nirkabel* (*wireless local area networks – wlan*) yang didasari pada spesifikasi IEEE 802.11. Terdapat tiga varian terhadap standard tersebut yaitu 802.11b atau dikenal dengan *Wifi (wireless fidelity), 802.11a (Wifi5), dan 802.11* ketiga standard tersebut biasa disingkat *802.11a/b/g*. *Versi wireless lan 802.11b* memilik kemampuan transfer data kecepatan tinggi hingga 11mbps pada band *frekuensi 2, 4 ghz*. Versi berikutnya *802.11a*, untuk *transfer* data kecepatan tinggi hingga 54 *mbps* pada *frekuensi* 5 GHz Sedangkan 802.11g berkecepatan 54 *mbps* dengan frekuensi 2, 4 *GHz*.

Proses komunikasi tanpa kabel ini dimulai dengan bermunculannya peralatan berbasis gelombang radio, seperti *walkie talkie*, *remote control*, *cordless phone*, telepon cellular, dan

peralatan radio lainnya. Lalu adanya kebutuhan untuk menjadikan komputer sebagai barang yang mudah dibawa (*mobile*) dan mudah digabungkan dengan jaringan yang sudah ada hal-hal seperti *ionic* akhirnya mendorong pengembangan teknologi *wireless* untuk jaringan komputer.

Mode jaringan *wireless local area network* terdiri dari dua jenis yaitu model *ad-hoc* dan model infrastruktur. Sebenarnya jaringan *wireless LAN* hampir Sama dengan jaringan *LAN* kabel, Akan tetapi setiap node pada *wlan* menggunakan piranti *wireless* agar dapat berhubungan dengan jaringan, node pada *wlan* menggunakan kanal *frekuensi* yang Sama dan *SSID* yang menunjukkan identitas dari piranti *wireless*. Gambar 2.5 menunjukkan schema dari topology jaringan *wireless LAN*



Gambar 2. 4 Topology Wlan

Sumber: http://etutorials.org/

Jaringan *wireless* memiliki dua model yang dapat digunakan: infrastruktur dan ad-hoc. Konfigurasi infrastruktur berikut merupakan beberapa komponen utama pada *wireless LAN*

2.7.1 *Access Point* (AP)

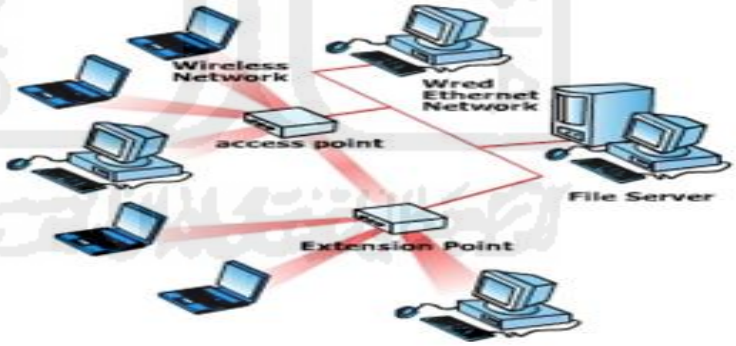
Pada wlan, alat untuk data disebut dengan AP dan terhubung dengan jaringan LAN melalui kabel Fungsi dari access poin adalah mengirim dan menerima data, sebagai buffer data antara wlan dengan wired lan, mengkonversi sinyal frekuensi radio (rf) menjadi sinyal digital yang akan disalurkan melalui kabel atau disalurkan ke perangkat wlan yang lain dengan dikonversi ulang menjadi sinyal frekuensi radio. Satu access poin dapat melayani sejumlah *user* sampai 30 *user* karena dengan semakin banyaknya *user* yang terhubung ke access poin maka kecepatan yang diperoleh tiap *user* juga Akan semakin berkurang Gambar 2.6 merupakan salah satu contoh dari hardware produk access poin yang sering digunakan, dan dijual dipasaran

Gambar 2. 5 Access Point

(Sumber: http://hendri.staff.uns.ac.id/)

2.7.2 *Extension Point*

Mengatasi berbagai problem khusus dalam topology jaringan, designer dapat menambahkan extension point untuk memperluas cakupan jaringan seperti yang terlihat pada Gambar 2.7, extension point hanya berfungsi layaknya repeater untuk client di tempat yang lebih jauh syarat agar antara *akses point* bisa berkomunikasi satu dengan yang lain, yaitu *setting channel* di masing-masing AP harus sama. Selain itu *SSID* (*service set identifier*) yang digunakan juga harus Sama dalam praktek di lapangan biasanya untuk aplikasi *extension point* hendaknya dilakukan dengan menggunakan merk AP yang Sama.



Gambar 2. 6 Extension Point

Sumber: http://www.oke.or.id/

2.7.3 Wireless Card

Gambar 2.8 menggambarkan contoh sebuah *wireless* card, *wireless card* merupakan salah jenis wireless hard ware external yang biasanya digunakan pada pc, biasanya wireless car dapat berupa *Pcmcia* (*personal computer memory card international association), isa card*, *usb card* atau

Ethernet card. *Pcmcia* digunakan untuk *notebook*, sedangkan yang lainnya digunakan pada komputer *desktop Wlan card* ini berfungsi sebagai interface antara sistem operasi jaringan client dengan format interface udara ke ap. Khusus *notebook* yang keluaran terbaru maka *wlan card* sudah menyatu di dalamnya Sehingga tidak keliatan dari luar

Gambar 2. 7 Wireless Card

Sember: (http://www.homeandlearn.co.uk/)

2.9 *Wifi*

Wireless fidelity (*Wifi*), adalah merupakan teknologi yang digunakan untuk mentransmisikan data pada jaringan komputer lokal tanpa penggunaan kabel atau yang biasa disebut dengan jaringan *nirkabel*, dalam proses transmisi data *wireless fidelity* memananfaatkan gelombang radio sebagai media transmisi data. Menurut priyambodo, (2005) *Wifi* adalah satu standar *wireless netwoking* tanpa kabel, hanya dengan komponen yang sesuai dapat terkoneksi ke jaringan (*wireless local area network-wlan*). Yang didasari pada spesifikasi *ieee* 802.11, dengan memanfaatkan standar jaringan *ieee* 802.11, berbagai macam produk *wireless lan* yang berasal dari *vendor* yang berlainan dapat saling bekerja sama/*kompatibel* pada satu jaringan yang sama. Jaringan *wireless lan* terdiri dari komponen *wireless user* dan AP dimana setiap *wireless user* terhubung ke sebuah AP. *Topologi wireless lan* dapat dibuat sederhana atau rumit dan terdapat dua macam topologi yang biasa digunakan, yaitu sebagai berikut (arbough, 2004). *Wifi* memungkinkan *mobile devices* seperti *pda* atau laptop untuk mengirim dan menerima data secara nirkabel dari lokasi manapun. Bagaimana caranya? Titik akses pada lokasi *Wifi* mentransmisikan sinyal *RF* (gelombang radio) ke perangkat yang dilengkapi *Wifi* (laptop/*Pda* tadi) yang berada di dalam jangkauan titik akses, biasanya sekitar 100 meter. Kecepatan transmisi ditentukan oleh kecepatan saluran yang terhubung ke titik akses. Konsekuensinya, tentu saja bila saluran yang terhubung ke titik akses tidak bersih dari gangguan, transmisi akan terganggu. Di dunia informatika, *Wifi* biasa juga disebut sebagai 802.11b, walaupun sebetulnya 802.11a pun termasuk *Wifi*, hanya saja 802.11b lebih umum dipakai. *Wireless Lan* memiliki *SSID* (*service set identifier*) sebagai nama jaringan *wireless* tersebut. Sistem penamaan *SSID* dapat diberikan maksimal sebesar 32 karakter. Karakter-karakter tersebut juga dibuat *case sensitive* sehingga *SSID* dapat

lebih banyak variasinya, dengan adanya *SSID* maka *wireless lan* itu dapat dikenali. Pada saat beberapa komputer terhubung dengan *SSID* yang sama, maka terbentuklah sebuah jaringan infrastruktur.

Pada saat ini *Wifi* dirancang berdasarkan spesifikasi *ieee* 802.11. Seperti yang terlihat pada tabel 2.1, spesifikasi *Wifi* terdiri dari 4 variasi yaitu: 802.11a, 802.11b, 802.11g, dan 802.11n. Spesifikasi b merupakan produk awal *Wifi*. Varian g dan n merupakan salah satu produk yang memiliki penjualan terbanyak di tahun 2005. Frekuensi yang digunakan oleh pengguna *Wifi*, tidak diberlakukan ijin dalam penggunaannya untuk pengaturan lokal sebagai contoh, komisi komunikasi *federal* di a.s. 802.11a menggunakan frekuensi yang lebih tinggi dan oleh karena itu daya jangkaunya lebih sempit, sedangkan yang lainnya tetap sama.

Spesifikasi Wi-Fi

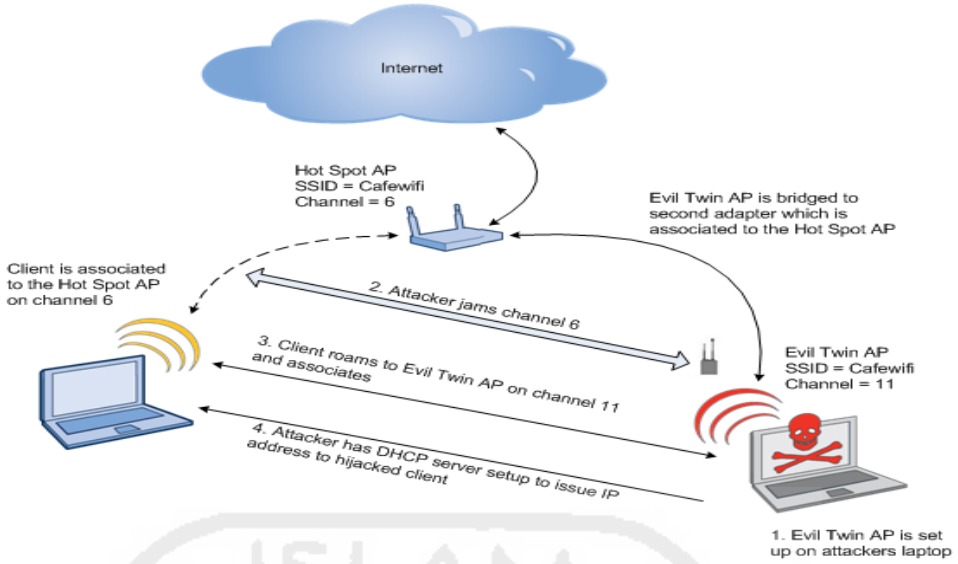
Spesifikasi	Kecepatan	Frekuensi Band	Cocok dengan
802.11b	11 Mb/s	~2.4 GHz	b
802.11a	54 Mb/s	~2.4 GHz	a
802.11g	54 Mb/s	~2.4 GHz	b, g
802.11n	100 Mb/s	~5 GHz	b, g, n

Tabel 2. 1 Spesifikasi Wi-Fi

Sumber : ultramelta.files.wordpress.com.

2.10 *Evil twin*

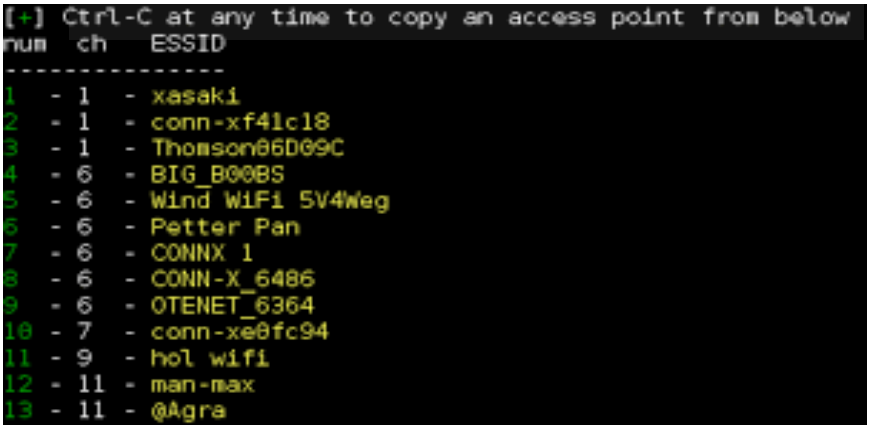
Evil twin merupakan salah satu jenis serangan *Rogue* AP atau *Wifi* phising, *Evil Twin attack* merupakan salah satu jenis serangan yang sangat berbahaya khusus pada para pengguna *Wifi* hot-spot, dalam melakukan aktifitas penyeranganya *Evil Twin* akan membuat sebuah AP phising, dimana di AP tersebut dia buat sengaja untuk mengecoh para pengguna dengan nama AP yang sama bahkannyaris tidak berbeda, seperti yang ditunjuk kan pada Gambar 2.9 dengan menggunakan service set identification (*SSID*) yang sama.



Gambar *2. 8 Evil Twin Attack*

Serangan *Evil Twin* AP digunakan untuk meluncurkan serangan *man-in the-middle attack (MITM)*. Mustafa (2014). Hal ini disebabkan karena hampir seluruh aktifitas para pengguna *Wifi hotspot* melakukan proses pengiriman paket internet dan semua itu harus melalui AP. Menurut Fabian lanze (2015): apabila *Evil Twin* AP memiliki kekuatan sinyal pemancar lebih kuat dari AP yang sah, maka pengguna akan tertipu dan beralih dari AP sah ke *Evil Twin* AP. Hal ini bisa terjadi apabila singnal RSSI dari *Evil Twin* lebih tinggi dari AP yang sah maka akan secara automatis tersambung dan langsung *mengisolasi* para pengguna yang sebelumnya telah berada pada jaringan tersebut. Seperti yang terlihat pada Gambar 2.9 dan Gambar 2.10 merupakan beberapa contoh aplikasi serangan *Evil Twin*

a. *Wifiphisher*: merupakan salah satu aplikasi bawaan *Linux open source*, berisi tentang intrusion – intrusion hacking yang dibuat dalam bentuk files *python*.



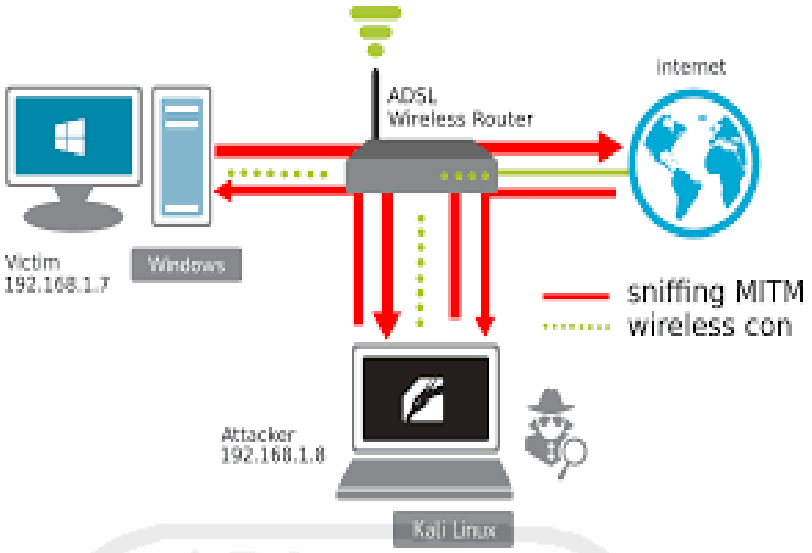
Gambar 2. 9 *Wifi*phisher

b. Wi-fi-pumpkin: juga merupakan salah satu jenis aplikasi yang hampir mirip dengan wi-fi phisher.

Gambar 2. 10 Wifi-pumpkin

2.11 Man In The Middle Attack

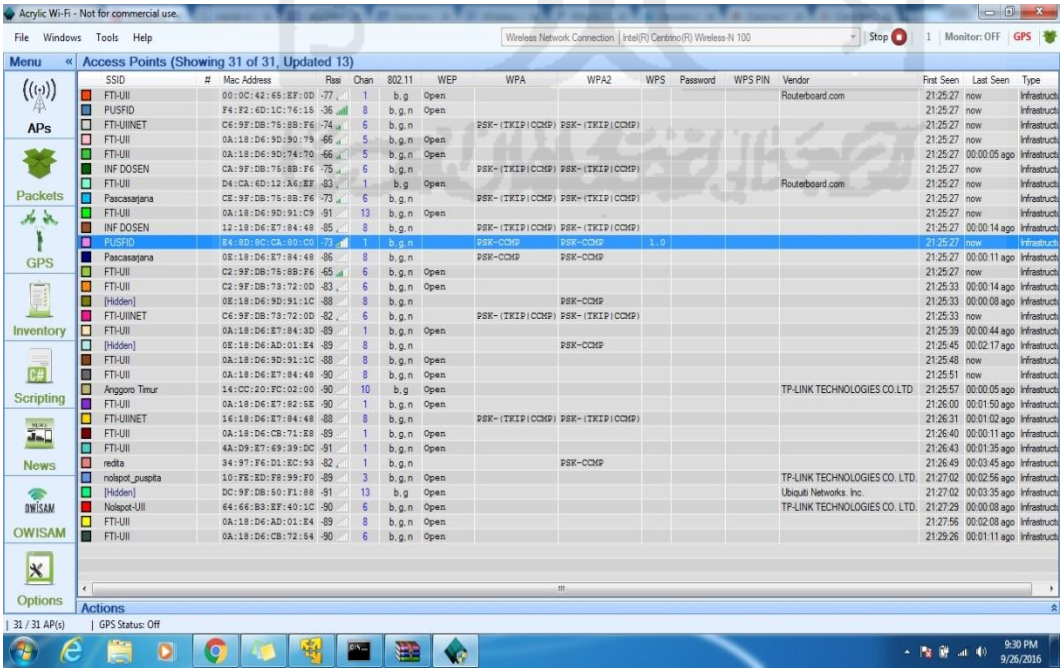
Man in the middle (MITM) merupakan salah satu jenis serangan yang berbahaya karena serangan ini dapat terjadi pada berbagai media informasi seperti *website*, *handphone*, dan bahkan Surat. Oleh karena itu, artikel ini akan membahas tentang *MITM attack* terlepas dari apapun dan dimanapun implementasinya menurut Purbo, o, (2007) serangan *man-in-the-middle*, seorang *user* jahat intercept / menangkap semua komunikasi diantara browser dan *server*. Dengan memberikan sertifikat palsu baik ke *browser* maupun *server*, pemakai jahat bisa melakukan dua sesi yang *dienkripsi* sekaligus karena *user* jahat mengetahui rahasia kedua sambungan, sengat mudah untuk mengamati dan manipulasi data yang diberikan diantara *server* dan *browser*



Gambar 2. 11 Serangan *Man In The Middle Attack*

2.12 Acrylic *Wifi*

Acrylic wi-fi adalah software wi-fi analyzer yang digunakan untuk mengidentifikasi jalur akses dan saluran *Wifi*, dan untuk menganalisis dan menyelesaikan insiden di 802.11a jaringan / b / g / n / ac secara real time tools ini biasa digunakan untuk menganalisis jaringan wi-fi professional dan administrator, untuk mengontrol kinerja nirkabel, jaringan dan siapa saja yang terhubung, mengidentifikasi kecepatan transmisi jalur akses data, dan mengoptimalkan jaringan wi-fi. Tools ini juga cukup memiliki fitur untuk menganalisa kemungkinan terjadinya serangan rouge AP, dengan cara memanfaatkan beberapa fitur analisa wi-fi.

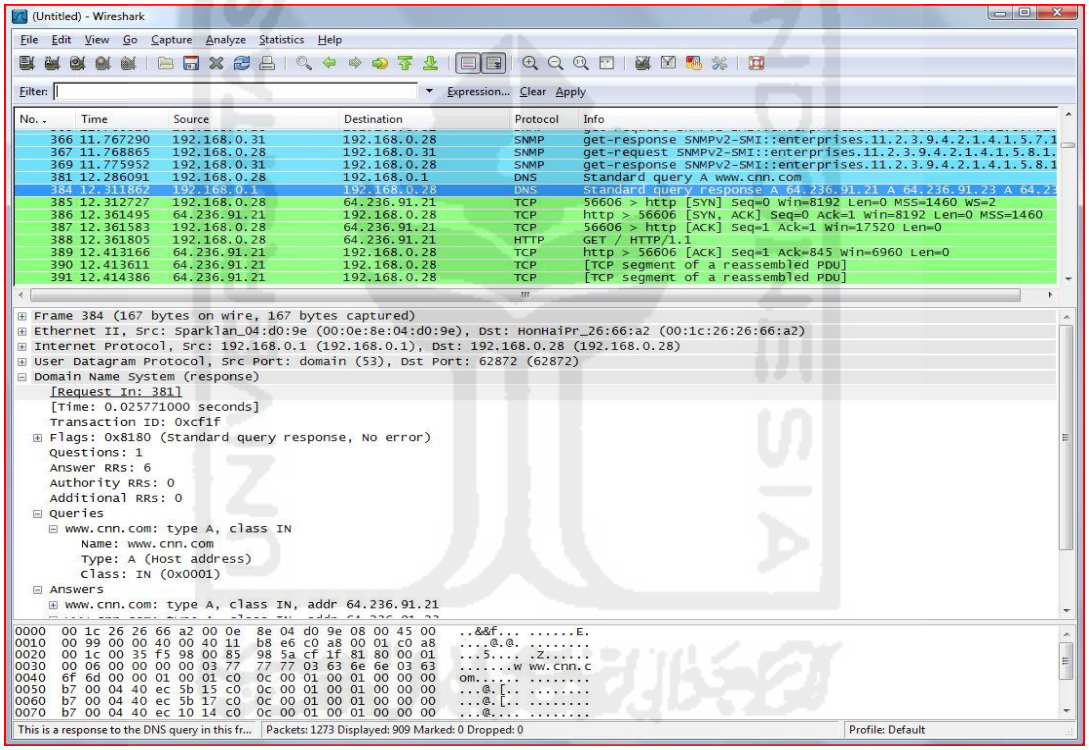


Gambar 2. 12 Acrylic-wi-fi

2.13 Wireshark

Wireshark merupakan salah satu dari software *monitoring* jaringan yang biasanya banyak digunakan oleh para *administrator* jaringan untuk men capture dan menganalisa kinerja jaringan. Salah satu alasan kenapa *Wireshark* banyak dipilih oleh seorang administrator adalah karena interfacenya menggunakan *graphical user unit (GUI)* atau tampilan grafis.

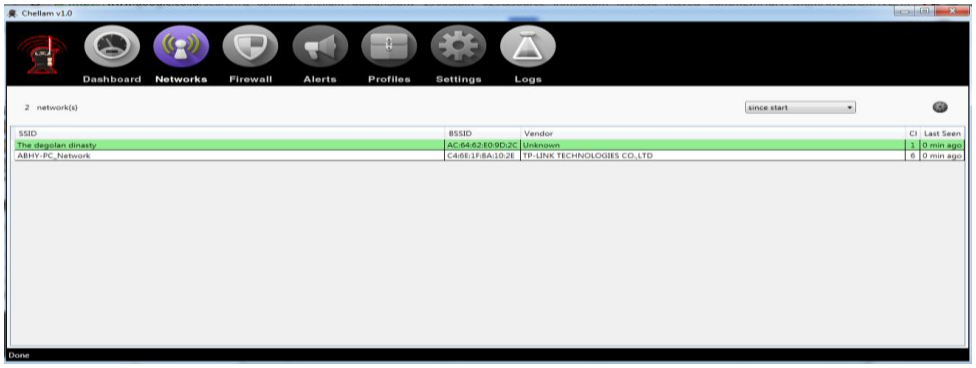
Selain itu *Wireshark* dapat memantau paket -paket data yang diterima dari internet *Wireshark* ini bekerja pada *layer* aplikasi Yaitu layer terakhir dari *OSI layer*. Dengan menggunakan *protocol* di *layer application http, ftp, telnet, SMTP, dns* kita dengan mudah memonitoring jaringan yang ada, maka secara tidak langsung *Wireshark* dapat membaca data secara langsung dari *Ethernet, Token-Ring, Fddi, Serial (Ppp Dan Slip), 802.11 wirelesses lan,* dan koneksi *atm*. Berikut contoh aplikasi *Wireshark*:



Gambar 2. 13 *Wireshark*

2.14 Chellam

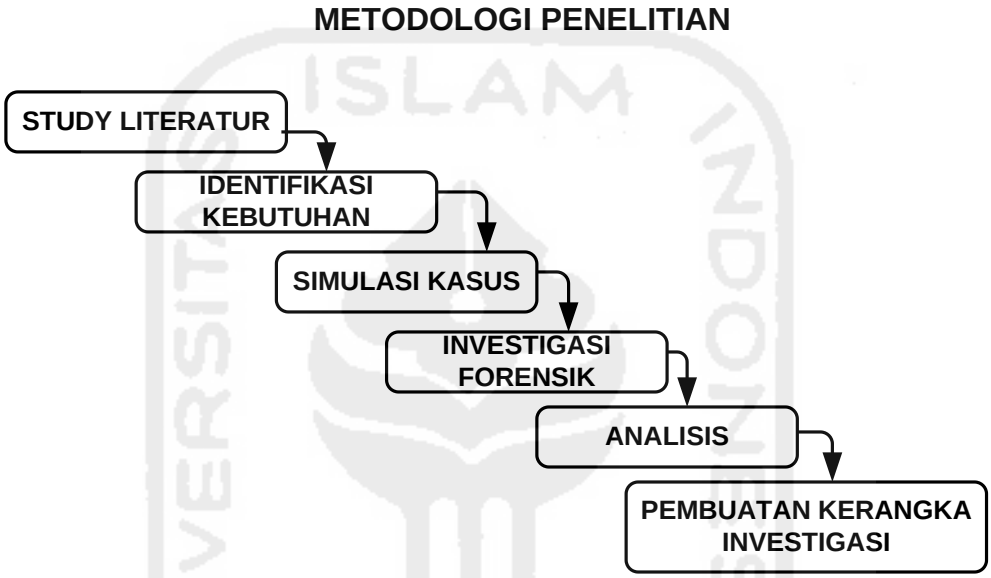
Chellam merupakan salah satu open source yang masih dikembangkan berbasis *windows*, fungsi dari aplikasi Chellam adalah untuk mendeteksi adanya bahaya serangan *wireless* yang dapat merugikan dari segi *user*, tanpa perlu menggunakan *wireless monitoring* untuk melakukan pendeteksian aktifitas serangan *wireless* yang berbahaya. Berikut adalah contoh aplikasi Chellam :



Gambar 2. 14 *Chellam*

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 :

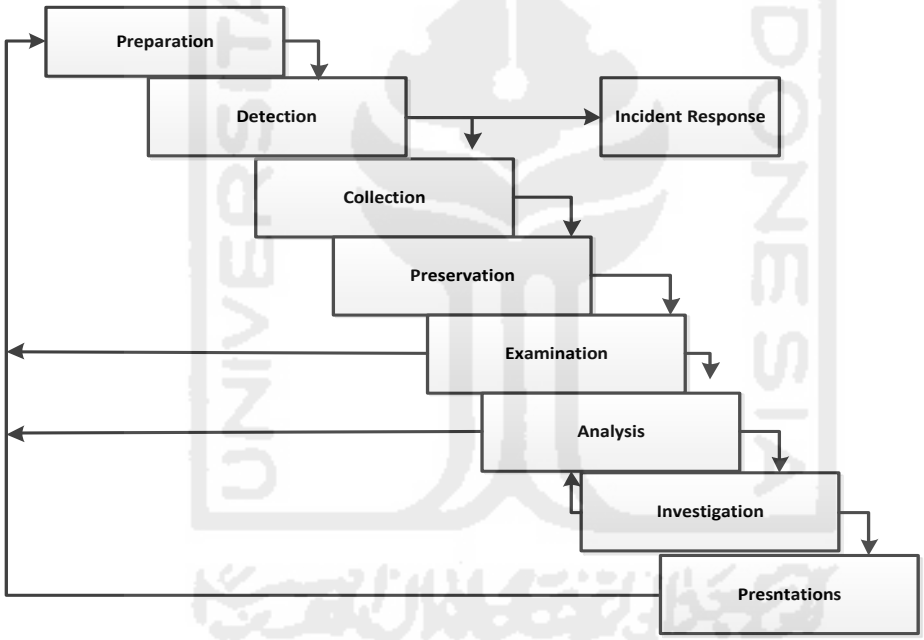
a. *Scanning* populasi dan identification AP: merupakan kegiatan awal dalam investigasi kasus *Evil Twin attack*, dimana *user* mengidentifikasi *Evil Twin* AP dengan cara melakukan proses *scanning* ap, kemudian menganalisa karakteristik dari AP tersebut dari *SSID*, *channel*, *power*, *encrypt* sampai 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.

Bab IV Implementasi Hasil Dan Pembahasan

Bab implementasi hasil dan pembahasan ini merupakan gambaran secara detail dari penelitian dan analisis yang dilakukan. Pada bab ini akan diuraikan bagaimana menyelesaikan masalah yang telah diangkat sebagai tema penelitian.

4.1 Perancangan Skema Penelitian

4.1.1 Batasan Perancangan Skema

Perancangan skema pada penelitian ini, merupakan implementasi atau uji coba penerapan metode *live* forensik terhadap serangan *MITM Based Evil Twin attack*. Dalam penelitian ini terdapat beberapa batasan dari perancangan skema ini antara lain adalah sebagai berikut:

a. Skema merupakan sistem yang menggunakan pendekatan secara *virtual* dengan memanfaatkan alat bantu perangkat lunak *virtual machine* dan beberapa *tools* bantuan lainya.

b. Penerapan skema penelitian akan memanfaatkan jaringan *Wifi* sebagai media dalam melakukan proses investigasi (*live* forensik) yang dilakukan padatahapan pendeteksian Evi ltwin AP dan kemudian pada tahapan analisa serangan MITM, akan digunkan metode statik forensik.

c. Skema pada penelitian hanya terdiri dari beberapa *device* yang terhubung ke dalam jaringan *Wifi* dimana terdapat beberapa *user* yang terhubung salah satunya merupakan komputer investigator, dan salah satunya merupakan juga merupakan komputer dari penyerang.

4.2 *Preparation*

Preparation merupakan tahapan awal dimana berisi tentang langkah -langkah maupun kebutuhan baik *tools software* ataupun hardware yang akan digunakan pada awal investigasi, pembahasan *preparation* akan meliputi beberapa hal antara lain.

4.2.1 *Literature Review*

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

4.3 Indetifikasi Kebutuhan

Identification kebutuhan akan disesuaikan dengan kondisi pada kasus seperti kebutuhan perangkat keras maupun perangkat lunak, sebagai berikut, kebutuhan perangkat keras dalam penelitian ini menggunakan satu buah laptop dengan merek ASUS a43s adalah sebagai berikut:

- Prosesor : intel(r) core(tm) b960 cpu @ 2.20ghz
- Ram : 6 gb
- Hdd : 320 gb
- Graphic card : intel300 dan GeForce 610m

Kemudian menggunakan satu *Wifi* adaptor dengan merek Tp-link dengan no seri TLWN722N, yang nanti digunakan untuk melakukan simulasi penyerangan pada jaringan *Wifi public*,
Selanjutnya kebutuhan perangkat lunak antara lain sebagai berikut,

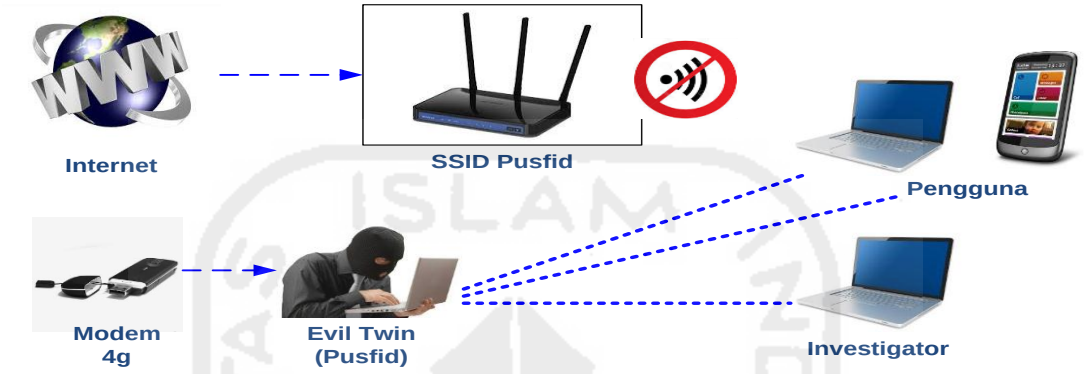
- OS windows 7 64/32 bit
- Chelam.exe
- Xarp.exe
- Wire shark
- Vistumbler
- VMware versi 11
- OS kali Linux 2.0
- Ettercap.
- *Wifi* pumpkin
- *Network* stumbler
- Mozilla Firefox / Google crime.

4.4 Simulasi Kasus

Simulasi kasus merupakan proses uji coba terhadap *MITM Based Evil Twin attack* yang dilakukan pada area *hotspot* fakultas teknologi industri universitas islam indonesia (FTI UII), pada kasus ini pelaku penyerangan *Evil Twin* mengkonfigurasikan *getway* yang berbeda dengan IP *gateway* dari *router* FTI UII, sehingga proses investigasi tidak dapat dilakukan sisi administrator ataupun sever, oleh karena itu dalam melakukan proses indetifikasi dibutuhkan

suatu pendekatan berbasis *wired* atau *user* yang diimpelementasikan dengan metode *live* forensik untuk menganalisa data dari sistem yang sedang berjalan.

Pada skenario ini pelaku akan menggunakan AP palsu untuk menjerat para korban, dan setelah korban terhubung ke dalam AP palsu yang dibuat dengan sengaja, pelaku dan dengan mudah melakukan serangan *MITM* untuk mendapatkan informasi rahasia yang dimiliki korban, seperti yang terlihat pada Gambar 4.1.



Gambar 4. 1 Scenario *MITM Based Evil Twin*

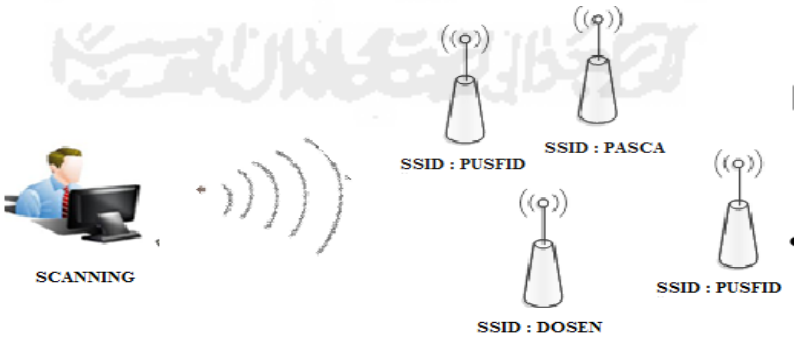
Pola serangan yang digunakan pelaku adalah dengan melaukan kofigurasi AP palsu yang menggunakan *SSID* yang mirip dengan salah satu *SSID* target di sekitar area *Wifi* yang terdapat di fakultas teknologi industri universitas islam indonesia, pada kasus ini pelaku menggunakan AP palsu dengan *SSID* "pusfid" sebagai sarana untuk melakukan penyerangan, AP palsu dikonfigurasi dengan mengabungkan beberapa aplikasi *MITM*, yang mana dapat berfungsi untuk memanipulasi trafik ketika korban terhubung ke internet, segala aktifitas akan diawasi dan kemudian tersimpan sebagai file log, seperti yang terlihat pada Gambar 4.2.

Gambar 4. 2 Scanario *MITM Based Evil Twin*

4.5 Investigasi Forensik

4.5.1 *Detection* Dan *Collection Evil Twin*

Detection merupakan salah tahapan awal dimana, investigator melakukan proses *scanning* untuk menemukan adanya kemungkinan AP palsu, di suatu area, seperti yang terlihat pada Gambar 4.3, dalam skenario kasus ini, *investigtor*/peneliti melakukan aktifitas *scanning* dengan memanfatkan sebuah aplikasi berbasi *windows* yaitu Chellam, aplikasi ini mendeteksi *Evil Twin* melalui sinyal *beacon* dan *probe recquest* yang dipancarkan oleh suatu AP palsu.

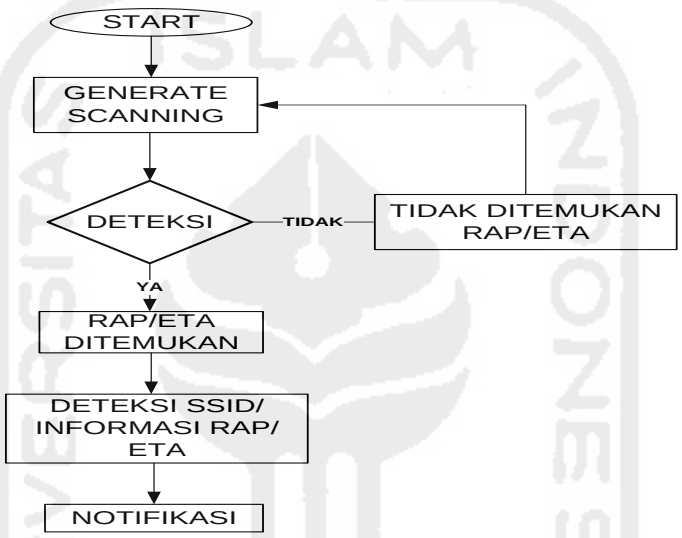


Gambar 4. 3 *Scanning Access Point*

Pada umumnya *Evil Twin* memanfatkan fitur airbase-ng,yang mana merupakan salah satu aplikasi berbasis Linux, Airbase-ng memanfatkan *mode monitor* untuk mendeteksi dan memancarkan sinyal *Wifi* atau AP, yang mana kemudian digabung kan dengan beberapa metode

IP table dan menggunakan gatway dari modem cdma/gsm maupun AP legal. Agar tetap terhubung ke *internet*.

Chellam melakukan scaning dengan menerima sinyal *beacon ,probe recquest* dari AP palsu, kemudian mendeteksi adanya serangan *Evil Twin*/ *Rogue* AP seperti yang terlihat pada Gambar 4. 4 Chellam melakukan *generate scanning* untuk mendeteksi adanya *Evil Twin/Rogue* AP jika ditemukan Chellam akan mendetecsi *SSID* AP dan beberapa informasi lainya dan selanjutnya akan dikirimkan notifikasi ke *desktop*, tetapi apabila hasil deteksi tidak menemukan adanya kemungkinan serangan *Evil Twin/Rogue* AP maka, Chellam akan terus melakukan *generate scanning* hingga ditemukan adanya ancaman serangan *fake* AP.

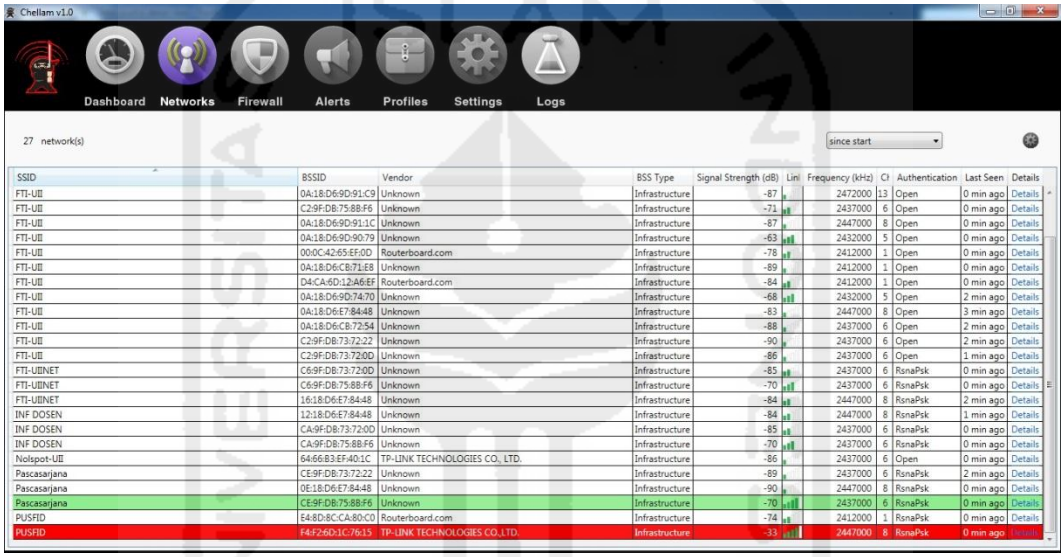


Gambar 4. 4 Proses Detect Chellam

Pada kasus ini proses *scanning* yang dilakukan pada fakultas teknologi industri unisversitas islam indonesia, dalam hasil *scanning* dengan jangkauan 100 m terdapat beberapa *SSID* yang dapat ditemukan pada *area* tersebut, antara lainnya *SSID* AP milik fakultas teknologi industri sendiri seperti fti uii, pascasarjana, inf dosen, fti uiinet dan pusfid dan beberapa *SSID* yang kemungkinan berasal dari luar fakultas teknologi industri antara lain seperti *SSID* nolspot, nolspotpusfita dan lain lain, pada Gambar 4.5, proses *scanning* di *area* tersebut ditemukan adanya ancaman AP palsu dengan *SSID* “pusfid”, dengan membaca notifikasi yang diberikan oleh aplikasi Chellam.

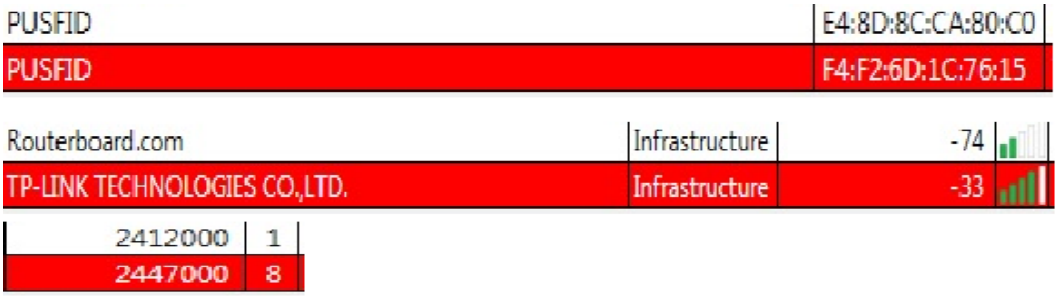
Gambar 4. 5 Notifikasi Chellam

Setelah ditemukan notifikasi adanya ancaman AP palsu, peneliti yang bertindak sebagai investigator akan lakukan proses *scanning* lebih lanjut untuk mencari informasi lebih detail tentang accsses point palsu dan penyerang seperti yang terlihat pada Gambar. 4.6,



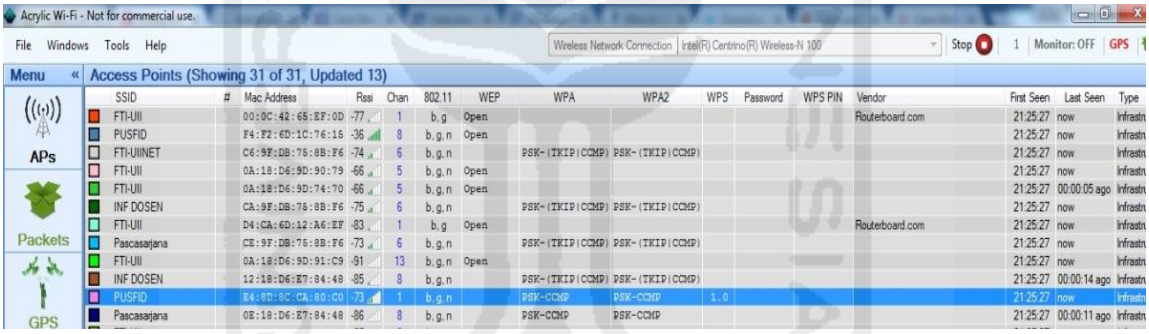
Gambar 4. 6 *Scanning* Analysis *Wifi* Chellam

Dari hasil *scanning* ditemukan adanya dua AP yang menggunakan *SSID* "PUSFID", dengan Mac "e4:8d:8c:ca:80:c0, dengan kode *vendor* : "Routerboard.com, dengan kekuatan sinyal -74 db, aunthentikasi :"Rsnapsk", frekuensi 241200 dan *channel* : 1, sedangkan *SSID* kedua dengan Mac: f4:f2:6d:1c:76:15, dengan kode *Vendor* : "Tp-Link technologies.co.ltd", kekuatan sinyal -34 db, aunthentikasi : "open", frekuensi 241700 dan *channel* : 8. Seperti yang terlihat pada Gambar 4.7



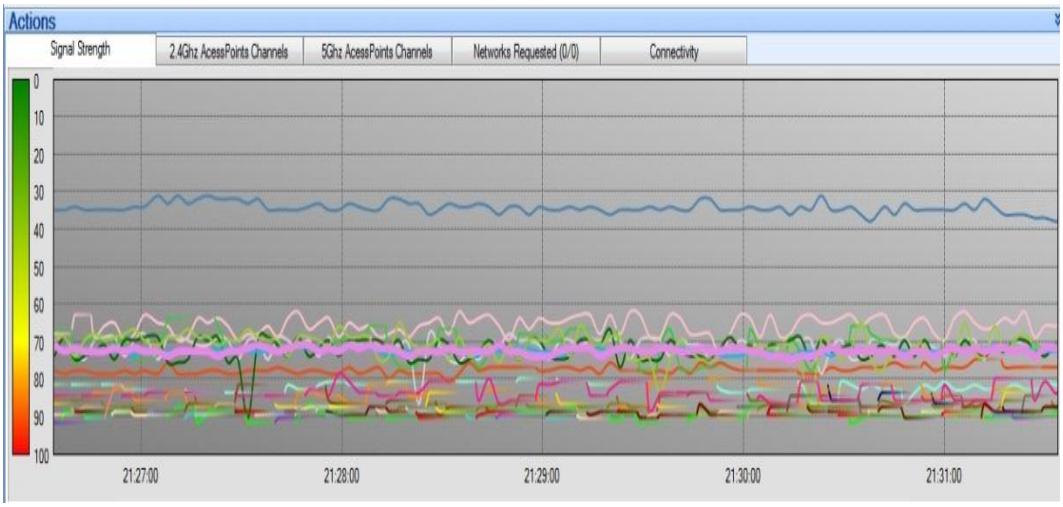
Gambar 4. 7 Analisa *Wifi*

Pada Gambar 4.8 *scanning* dilakukan dengan menggunakan aplikasi bantuan lain yaitu acrlyric-*Wifi*, aplikasi ini digunakan untuk menemukan informasi lebih detail terkait, yang mana berfungsi sebagai aplikasi analisis jaringan *Wifi*, pada hasil *scanning* AP dengan *SSID* : pusfid, diberikan tanda berwana merah muda untuk AP yang menggunakan mac "e4:8d:8c:ca:80:c0, dengan kode *vendor* : "routerboard.com, dengan kekuatan sinyal -74 db, aunthentikasi :"rsnapsk", frekuensi 241200 dan *channel* : 1, sedangkan *SSID* kedua dengan mac: f4:f2:6d:1c:76:15, dengan kode *vendor* : "tp-link technologies.co.ltd", kekuatan sinyal -34 db, aunthentikasi : "*open*", frekuensi 241700 dan *channel* : 8, diberi tanda dengan warna biru.

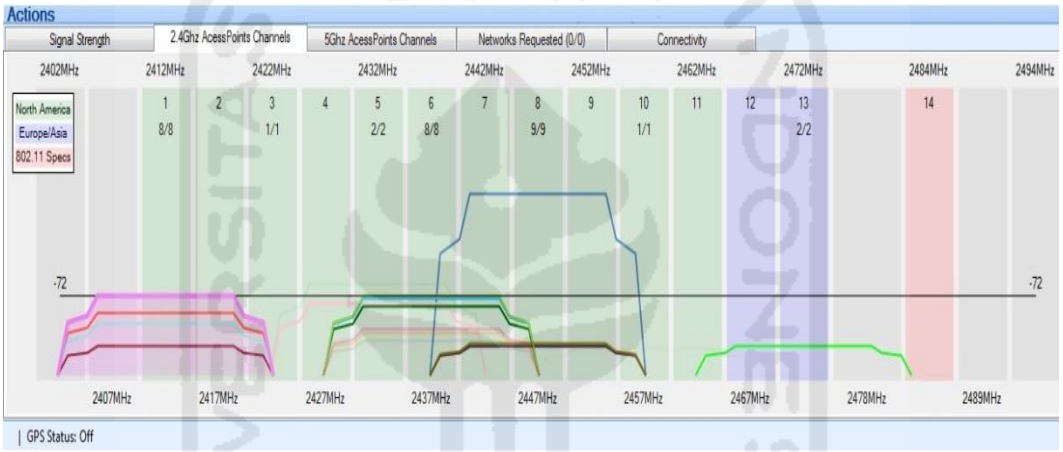


Gambar 4. 8 *Scanning* Analisis Menggunakan Arcliric-Wifi

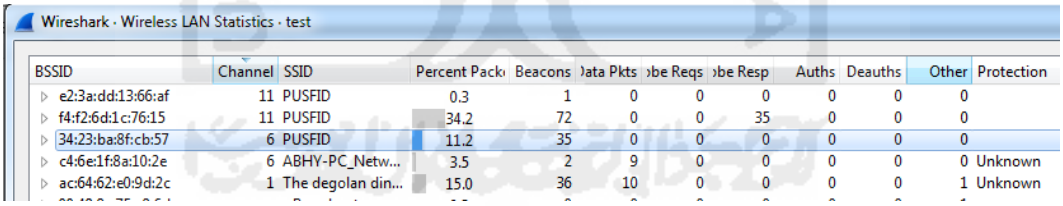
Pada capture jaringan *Wifi* menggunakan acrilyc-*Wifi* ditemukan rangkaian statistic sinyal *Wifi*, AP pusfid yang diberi tanda warna biru menunjukan tingkat kekuatan sinyal di atas rata-rata dengan -37db, dibanding dengan AP yang diberi tanda merah mudah yang hanya berkekutan sinyal -74 db. Menurut (Cai et al. 2014) *Rogue* AP/AP palsu biasanya memiliki *SSID* yang sama dan konfigurasi dengan AP yang sah. Selain itu *Rogue* AP harus memiliki sinyal yang lebih kuat daripada AP legal. Dan *Rogue* AP harus menawarkan otentikasi ulang antara sta (*station*/penerima) dan AP agar tidak membangkitkan kecurigaan. *Rogue* AP dapat dideteksi dengan menganalisa atribut yang dipancarakan oleh sinyal *beacoon* inteval, yaitu dengan *SSID*, vendor, rate sinyal, channel, B*SSID* dan IP, dengan cara dibandingkan dengan informasi AP yang sah, berikut adalah analisa kekuatan sinyal, ber dasarkan kekuatan sinyal, pada rate 2.4 ghz AP/channel,seperti yang terlihat pada Gambar 4.9 dan 4.10.



Gambar 4. 9 Analisa Statistic Kekuatan Signal

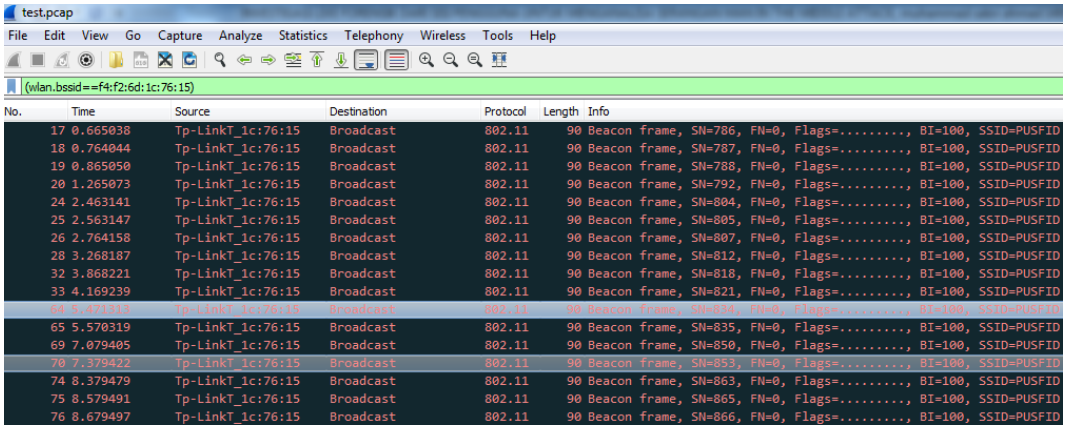


Gambar 4. 10 Analisa Statistik *2.4 Ghz Acsses Point/Channel*



Gambar 4. 11 Prensentasi *Capture Traffic Wifi*

Dari hasil *capture traffic Wifi* ditemukan terdapat SSID PUSFID, *channel* 11 dengan Mac f4:f2:6d:1c:76:15, memiliki presentasi paket yang paling tinggi yaitu 34.2 % dengan singnal *beacon* 72, untuk lebih jelasnya terliahat pada Gambar 4.11 dan 4.12.



Gambar 4. 12 Akuisisi File Pcap *Capture Traffik*

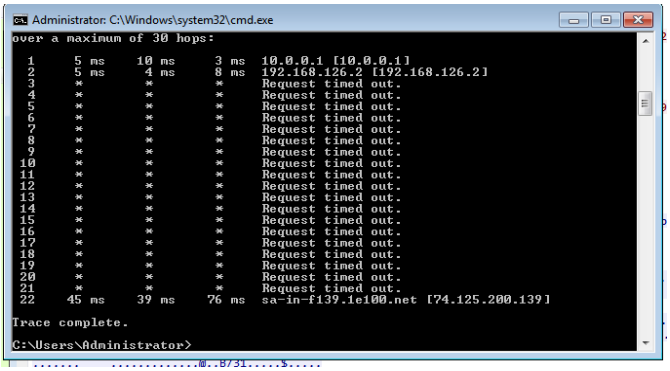
4.5.2 Approach Strategy

Approach Strategy merupakan suatu kegitan dimana peneliti melakukan persiapan untuk menangani kemungkinan-kemungkinan terjadi tindakan ilegal lainya, setelah ditemukan informasi dan data-data terkait AP palsu, peneliti akan berusaha masuk dengan sengaja ke dalam jangkauan AP palsu, seakan akan menjadi *user* dalam area *Evil Twin attack*, dengan tujuan agar dapat menemukan informasi lebih lanjut tentang tindak kejahatan ilegal seperti, serangan *man in the midle attack*, kemudian peneliti melakukan analisa-analisa terkait data-data yang nantinya digunakan untuk menemukan barang bukti. Dengan memanfatkan beberapa *tools* bantu yaitu Wireshark dan *network* miner untuk melakukan proses *sniffing* pada jaringan *Evil Twin* tersebut, selain itu akan digunakan juga salah satu *tools Arp detector* untuk memudahkan proses analisa untuk menemukan barang bukti yaitu xarp, karena pada dasarnya metode *sniffing* yang dilakukan melalui *user side* tidak terlalu efektif, maka dibutuhkan beberapa metode maupun *tools* bantu lainnya.

4.5.3 Deteksi Dan Collection Phase 2

4.5.3.1 Tracert IP

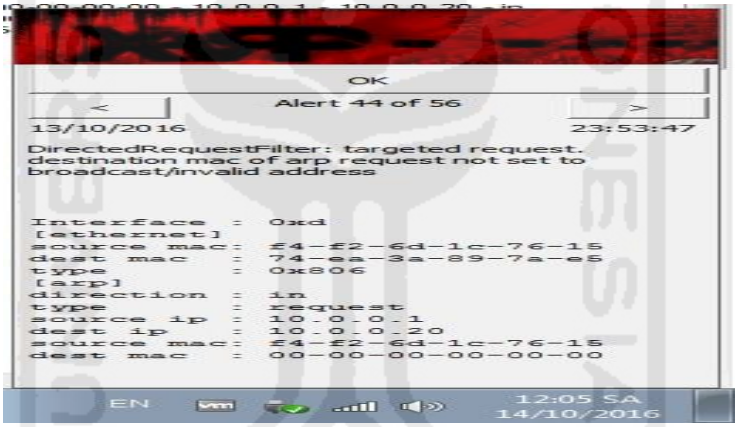
Pada tahapan ini, dimulai dengan mencari tau IP dari *router* pelaku dengan menggunakan perintah *tracert* seperti yang terlihat pada Gambar 4.13, telihat IP yang digunakan oleh pelaku adalah 10.0.0.1 sebagai *gateway* dan 192.168.126.2.



Gambar 4. 13 Tracer IP

4.5.3.2 Xarp identifikasi

Pada dasarnya serangan *MITM* akan selalu memnfatkan *broadcase Arp* untuk mencoba melakukan poisioning, dan ketika pelaku memulai serangannya, maka dengan automatis xarp akan memberikan notifikasi adanya serangan *Arp* seperti yang terlihat pada Gambar 4.14, dimana terlihat *source* IP 10.0.0.1 melakukan *recquest* pada IP 10.0.0.20.



Gambar 4. 14 Notifikasi Arp *Attack*

4.5.3.3 Capture trafik

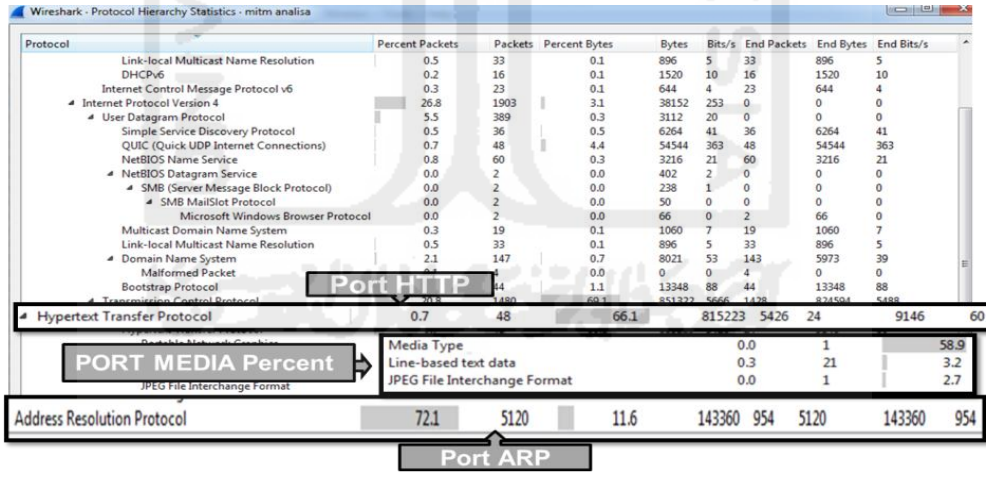
Capture paket trafik dengan menggunakan Wireshark di dalam jaringan *Evil Twin* tersebut, dilakukukan selama beberapa menit untuk menemukan *beberapa* informasi yang dapat digunakan untuk proses analisa selanjutnya, berikut detail file pcap yang akan dianalisa, seperti yang terlihat pada tabel 4.1.

Tabel 4. 1 Tabel File Pcap

Nama	*MITM* analisa,pcap
Tipe	File pcap
Hash (md5)	B9e31516e1b9ff8ab174503373687b82
Ukuran file	1.28 mb
Tools	Wireshark

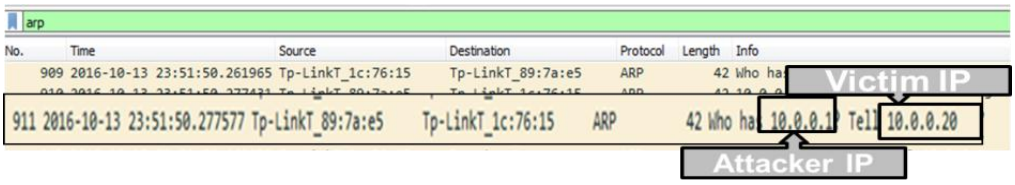
4.5.4 Akuisisi data serangan

Tahapan Akuisisi serangan, dilakukan dengan menganalisa data maupun informasi yang ditemukan dalam tahapan pengkoleksian/ *Collection* sebelumnya. Proses Akusisi data serangan dilakukan dengan menganalisa file hasil capturing sebelumnya, *tools* Wireshark. Proses analisa dilakukan dengan cara memanfaatkan modul hierarki dan *comand-comand* filterisasi paket dari dari *tools* Wireshark. Dari hasil analisa tabel hirarki terdapat 3 objek yang dapat dijadikan sebagai bahan analisa yaitu *port* HTTP, *port* ARP dan presentasi media. Seperti yang terlihat pada Gambar 4.15



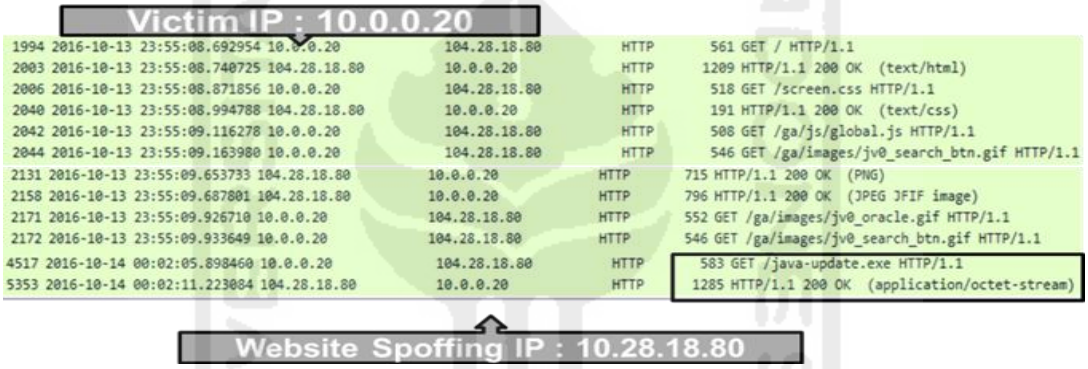
Gambar 4. 15 Wireshark Hirarki Modul

Pada Gambar 4.16, Pada analisa *port* ARP ditemukan kegiatan ARP *broadcase* dari MAC *address* tp_link/ *sourece* 1c: 76:15 dengan IP 10.0.0.1 mencoba menghubungi MAC *address destination* azurewav 79:5a:5c dengan IP 10.0.0.20

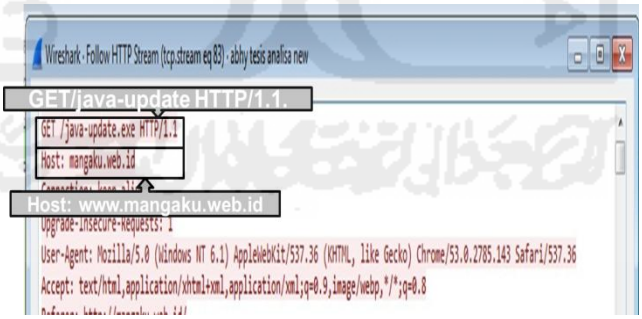


Gambar 4. 16 *Arp* Filter

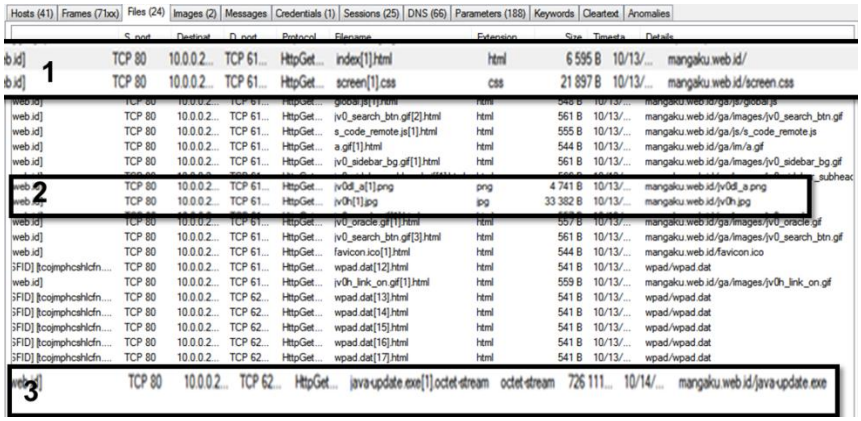
Pada Analisa filterisasi *port* HTTP, terlihat IP 10.0.0.20 melakukan *request* ke IP 104.28.18.80, kemudian IP 10.0.0.20 diarahkan untuk mengakses situs yang kemungkinan sengaja disiapkan. Dari hasil analisa pada *port* HTTP juga terlihat adanya beberapa file yang mencurigakan diantaranya adalah file Html, file.Css, file Jpg, file Png, dan file berksensi Exe yang ditemukan pada paket 5353 yaitu http/get java-update.exe. Untuk lebih jelasnya dapat dilihat pada Gambar 4.17 Kemudian pada Gambar 4.18, ditemukan adanya kegitan yang mencurigkan dimana Host yang sebenarnya dari IP 104.28.18.80 adalah http://www.mangaku.web.id.



Gambar 4. 17 Http Filter



Gambar 4. 18 Http Analisis

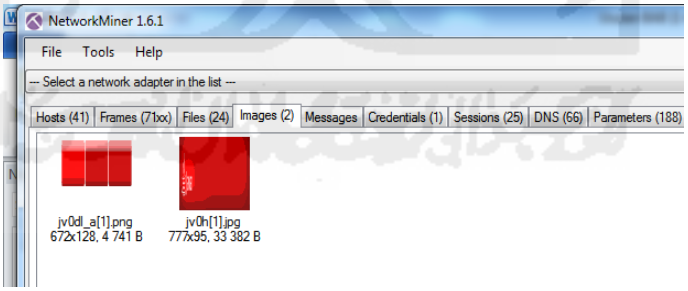


Gambar 4. 19 *Network* Miner File Analisis

Pada proses analisa temuan file dilakukan menggunakan *Tool Network Miner*. Dari hasil analisa ditemukan tiga jenis file, yang diduga merupakan file yang sengaja dibuat untuk menjebak para korban. Untuk lebih jelasnya dapat dilihat pada poin-poin yang terlihat pada Gambar 4.19.

Pada keterangan no 1 ditemukan dua file yaitu file Html dengan sessions index.(1) dan file Css dengan seissions css.(1), yang mana merupakan Website mangaku.web.id yang kemudian dibelokan ke situs yang sengaja dibuat. Pada keterangan no 2 terdapat dua buah file yang berekstensi Png dan Jpg. Selanjutnya pada keterangan no 3 ditemukan adanya sebuah file berextensi .exe. seperti yang ditunjukan pada Gambar 20.

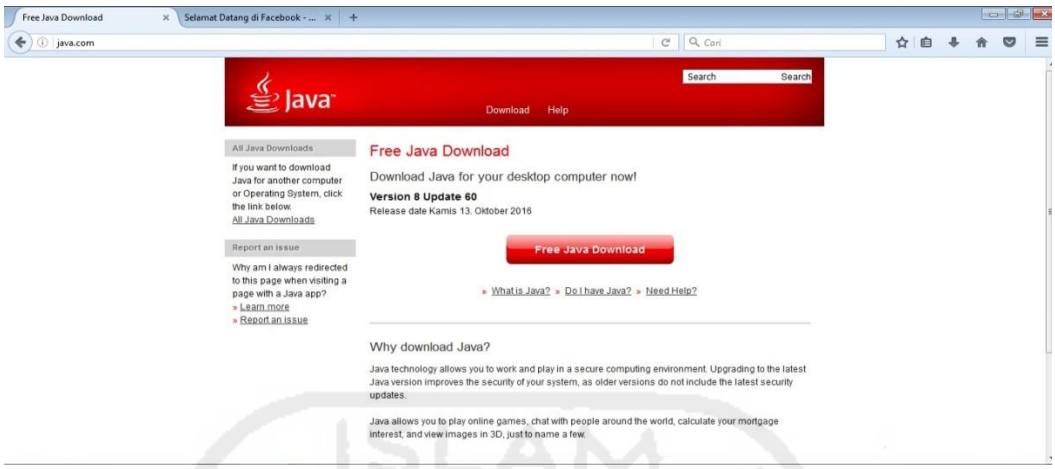
Dari hasil dari analisa sebelumnya, dicurigai pelaku mencoba melakukan *intercept download* dengan cara menggunakan metode DNS *Spoofing*, ARP *spoff*, untuk mengarahkan para korban ke situs yang sengaja dibuat olehnya.



Gambar 4. 20 Images Analisis

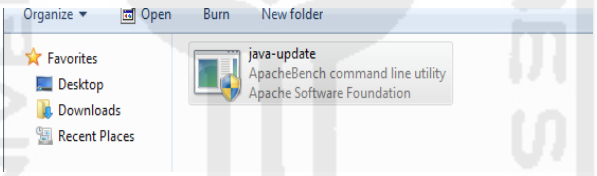
Untuk mengetahui hasil dari analisa sebelumnya, dicurigai pelaku mencoba melakukan *intercept download* dengan cara menggunakan metode dns *spoofing*, *Arp spoff* untuk mencoba mengarahkan para korban ke situs yang sengja dibuatnya, peneliti yang juga merupakan *user* akan mencoba dengan sengaja masuk ke dalam jebakan yang dibuat, pada Gambar 4.21 merupakan sebuah situs yang telah sengaja disiapkan.yaitu situs java.com, disni pelaku berusaha

mengarakan para korban untuk melakukan update java dengan cara mendownload file berekstensi .exe



Gambar 4. 21 Html Java.com

Untuk memastikan file berektensi exe, tersebut adalah merupakan aplikasi yang berbaya atau tidak, maka peneliti mencoba mendownload file tersebut, agar lebih mudah untuk analisa dan diindentifikasi, berikut jenis file yang didownload pada situs palsu tersebut, file dengan nama java-update seperti yang terlihat pada Gambar 4.22



Gambar 4. 22 Java Update.exe

4.6 Prosess Analisa Dan Investigasi

4.6.1 Analisa

Berdasarkan hasil analisa yang dilakukan dalam kasus *MITM Based Evil Twin attack* ini, dengan menggunakan metode *live* forensik dan pendekatan dari sisi user, bedasarkan tahapan –tahapan sebelumnya ditemukan beberapa pentujuk ataupun temuan – temuan yang dapat dijadikan sebagai informasi, yang dapat digunakan sebagai barang bukti, dan dari tahapan-tahapan analisa sebelumnya maka dapat ditarik beberapa kesimpulan sebagai berikut :

1. Mendeteksi serangan *Rogue* AP/*Evil Twin* dan pengumpulan informasi yang dapat digunakan sebagai barang bukti digital.
2. Karakteristik barang bukti digital pada serang *MITM* dan metode penyerangan yang digunakan.

3. Metodologi yang digunakan untuk menemukan barang bukti pada kasus serangan *MITM Based Evil Twin*.

4. Metode efektif untuk investigasi serangan *MITM Based Evil Twin attack.*

4.6.1.1 1. Mendeteksi serangan *Rogue* AP/*Evil Twin* dan pengumpulan informasi yang dapat digunakan sebagai barang bukti digital.

Serang *Evil Twin attack* merupakan serangan yang memeanfatkan AP palsu sebagai sarana untk mengecoh para korbannya, dalam melakukan capture atau *scanning Evil Twin* AP analisa untuk menemukan baranng bukti.

1. *Accsess point* palsu atau *Evil Twin*/ *Rogue* AP, mencoba membuat kembaran atau menyerupai AP yang telah menjadi targetnya, pada kasus ini ditemuklan dua buah AP yang memiliki *SSID* yang sama.

2. untuk mendeteksi adanya serangan *Evil Twin*/*Rogue* AP, dapat dilakukan dengan menggunakan aplikasi Chellam

3. Pengumpulan informasi *fake* AP dapat dilakukan dengan cara menganalisa atribut dari AP tersebut, dari hasil analisa diketahui terdapat bebera informasi yang dapat dijadikan perbandingan yaitu *SSID* "pusfid", dengan mac "e4:8d:8c:ca:80:c0, dengan kode *vendor* : "routerboard.com, dengan kekuatan sinyal -74 db, aunthentikasi :"rsnapsk", frekuensi 241200 dan *channel* : 1, sedangkan *SSID* kedua dengan mac: f4:f2:6d:1c:76:15, dengan kode *vendor* : "tp-link technologies.co.ltd", kekuatan sinyal -34 db, aunthentikasi : "open", frekuensi 241700 dan *channel* : 8, untuk lebih jelasnya dapat dilihat pada tabel 4.2.

Tabel 4. 2 Analisa *Evil Twin Attack*

NO	SSID	BSSID	Vendore	Encriptions	signal	frequency	channel
1	PUSFID	E4:8D:8C:CA:80:C0	Routerboard.com	ccmp	-74	2412000	1
2	PUSFID	F4:F2:6D:1C:76:15	TP-LINK TECHNOLOGIES.co.ltd	ccmp	-33	2447000	8

4.6.1.2 Karakteristik barang bukti pada serang *MITM* dan metode penyerangan yang digunakan.

Proses analisa untuk mengetahui karakteristik pada serangan *MITM*, dilakukan dengn memanfaatkan beberapa tolls bantu, antara lain seperti Xarp, Wireshark dan *network* miner.

1. Mengetahui alamat IP router dan *gateway* ketika telah berada di dalam jaringan *Evil Twin*, karena IP pada *Evil Twin* biasanya menggunakan IP yang berbeda dengan AP yang sah, kemudian deteksi serangan *Arp* menggunakan *Arp detektor*.

2. *Network* trafik

a. Untuk proses pengindetifikasian serangan *MITM* dapat dilakukan dengan menganalisa hirarki yang terdapat pada modul wiresharak seperti yang terllihat pada Gambar 4.13.

b. *Network* trafik dapat digunakan untuk melakukan memonitoring proses yang dilakukan antara client dan activitas yang dilakukan oleh pelaku.

3. Analisa *Arp attack* dilakukan dengan menggunakan modul dan *comand-comand* yang terdapat pada Wireshark dapat dilihat pada Gambar 4.14, karena pada dasarnya serangan *MITM* selallu memanfaatkan metode *Arp attack* maupun *Arp poisioning*.

4. *Port* http, dilakukan untuk mengindetifikasi aktifitas yang mencurigakan, dari hasil analisa filterisasi *port* http, terlihat IP 10.0.0.20 melakukan *request* ke IP 104.28.18.80 kemudian mengakses situs yang kemungkinan sengaja disiapkan ,dan dari hasil analisa *port* http terlihat adanya beberapa file yang mencurigakan, diantaranya file.html, file.css, file jpg, file png, dan file berksensi exe, pada paket 5353, yaitu http/get java-update.exe, untuk lebih jelasnya dapat dilihat pada tabel analisa 4.3.

Tabel 4. 3 Analisa File Pcap

No	Time	Source	Destination	Protocol	Length	info
ARP PORT ANALYSIS						
1936	11:54:59 PM	Tp-LinkT_89:7a:e5	Tp-LinkT_1c:76:15	ARP	42	Who has 10.0.0.1? Tell 10.0.0.20
263	11:50:09 PM	Tp-LinkT_1c:76:15	Tp-LinkT_89:7a:e5	ARP	42	10.0.0.1 is at f4:f2:6d:1c:76:15
1937	11:54:59 PM	Tp-LinkT_1c:76:15	Tp-LinkT_89:7a:e5	ARP	42	10.0.0.1 is at f4:f2:6d:1c:76:15
http PORT ANALYSIS						
2042	11:55:09 PM	10.0.0.20	104.28.18.80	HTTP	508	GET /ga/js/global.js HTTP/1.1
2044	11:55:09 PM	10.0.0.20	104.28.18.80	HTTP	546	GET /ga/images/jv0_search_btn.gif HTTP/1.1
4517	12:02:06 AM	10.0.0.20	104.28.18.80	HTTP	583	GET /java-update.exe HTTP/1.1
FILE INDETIFICATION ANALYSIS						
5353	12:02:11 AM	104.28.18.80	10.0.0.20	HTTP	1285	HTTP/1.1 200 OK (application/octet-stream)
2131	11:55:10 PM	104.28.18.80	10.0.0.20	HTTP	715	HTTP/1.1 200 OK (PNG)
2158	11:55:10 PM	104.28.18.80	10.0.0.20	HTTP	796	HTTP/1.1 200 OK (JPEG JFIF image)
2003	11:55:09 PM	104.28.18.80	10.0.0.20	HTTP	1209	HTTP/1.1 200 OK (text/html)
2040	11:55:09 PM	104.28.18.80	10.0.0.20	HTTP	191	HTTP/1.1 200 OK (text/css)

5. Analisa file kemunginan adanya penyusupan data-data yang mencurigakan, analisa digunakan menggunakan *network* miner, dari hasil penamatan ditemukan beberapa file mencurigakan seperti 2 buah file images, dan satu file berextensi .exe. Seperti yang terlihat pada Gambar 4.17.

4.6.1.3 Metodologi yang digunakan untuk menemukan barang bukti pada kasus serangan *MITM Based Evil Twin*

Metode yang digunakan pada kasus ini adalah *live* forensik dimana data yang diambil lebih bersifat *live* atau secara langsung, selain itu digunakan juga pendekatan yang bersifat *user side*, dimana proses analisa dilakukan dari sudut padang *user/ client*, pada kasus ini peneliti sengaja masuk ke dalam jangkauan jaringan dari *Evil Twin Based MITM* itu sendiri, dan dari hasil penelitian dapat ditarik beberapa tahapan metode yang telah dilakukan.

1. Proses *scanning* identifikasi serangan *Evil Twin*. Dilakukan dengan menggunakan aplikasi Chellam.
2. Analisa *network scanning* lebih lanjut dengan menggunakan tools bantuan seperti Chellam, Acrlyric-*Wifi*.
3. Setelah diindetifikasi adanya serangan *Evil Twin*, maka masuk dengan sengaja ke dalam jaringan *Evil Twin*.
4. Proses *packet capture network* trafik dilakukan dengan menggunakan tools Wireshark dan *network miner*.
5. setelah mendapatkan hasil capture trafik, dilakukan analisa lebih lanjut untuk menemukan informasi yang dapat dijadikan barang bukti.

4.7 Pembuatan kerangka investigasi forensik

Pembuatan kerangka investigasi dilakukan berdasarkan tahapan –tahapan yang dilalui dari proses analisa forensik sebelumnya untuk menemukan barang bukti, kemudian dikembangkan berdasarkan model (NFGP) *network* forensik *generik* proses seperti yang terlihat pada Gambar 2.3*(Pilli et al. 2010), (Pilli et al. 2010),* NFGP merupakan suatu model investigasi forensik yang dibuat untuk menangani kasus terkait *network*ing, model NFGP terdiri dari 9 tahapan analisa forensik yaitu.

1. *Preparation*: merupakan tahapan awal investigasi yang membahas tentang bagaimana melakukan persiapan dalam proses analisa investigasi.
2. *Detection*: merupakan proses dalam menemukan ancaman serangan atau *ilegal activity* yang terjadi dalam suatu jaringan *network*
3. *Collection*: merupakan tahapan pengumpulan informasi terkait ancaman-ancaman maupun informasi yang dapat dianalisa untuk dijadikan barang bukti.

4. *Preservation*: merupakan tahapan pemeliharaan atau pengamanan informasi ataupun data yang dikumpulkan untuk menjaga keaslian barang bukti
5. *Acquisitions*: merupakan tahapan pengecekan keaslian informasi yang dikumpulkan melalui tahapan pemeriksaan.
6. Analisis: merupakan proses menganalisa informasi maupun data yang ditemukan di suatu jaringan komputer untuk menemukan barang bukti. Investigation: merupakan tahapan final investigasi dimana dilakukan metode forensik untuk menemukan barang bukti yang dilakukan setelah proses analisa.
7. *Reporting*: merupakan proses akhir, yaitu penyusunnan laporan dari hasil informasi barang bukti yang ditemukan dari beberapa tahapan analisa sebelumnya.

Prosess Pembuatan model forensik pada kasus ini, dilakukan berdasarkan hasil evaluasi kekurangan model NFGP dalam penyelesaikan kasus serangan *Evil Twin based MITM*, dan dari hasil evaluasi ditemukan beberapa kelebihan maupun kekurangan pada model forensik tersebut.

1. Kelebihan model dari NFGP berdasarkan fungsi dan tahapan-tahapan investigasi forensik yaitu

a. Terdapat banyak tahapan yang tersistematis dan teratur khususnya dalam penanganan kasus terkait *networking*.
b. Merupakan model yang dikembangkan dari beberapa modul investigasi sebelumnya
c. Tahapan investigasi juga terdiri dari possess detection dan incident respond.

2. Kekurangan model NFGP dalam penanganan kasus *MITM Based Evil Twin* yaitu :

a. Pada dasarnya kasus *MITM Based Evil Twin* merupakan dua jenis serangan yang digabungkan menjadi satu yaitu serangan pada jaringan komputer yang memanfaatkan media *fake* AP sebagai pelantarnya selanjutnya digabungkan dengan teknik *Man In The Middle Attack* dimana seorang *attack* berusaha memanfaatkan *traffic* jaringan untuk melakukan kegiatan *sniffing, spoofing*, dll, sehingga dibutuhkan dua kali tahapan pendeteksian dalam melakukan proses investigasi, sedangkan pada modul NFGP hanya memiliki satu tahapan pendeteksian.
b. Proses tahapan pengumpulan data harus dilakukan dua kali untuk menentukan jenis serangan *Evil Twin* kemudian dilanjutkan pada tahapan deteksi dan koleksi serangan *MITM*.
c. Proses analisis digabungkan dengan proses investigasi untuk mempermudah tahapan penyelesaian kasus

4.7.1 Proses Pembutan Kerangka Model Forensik Extendend NFGP

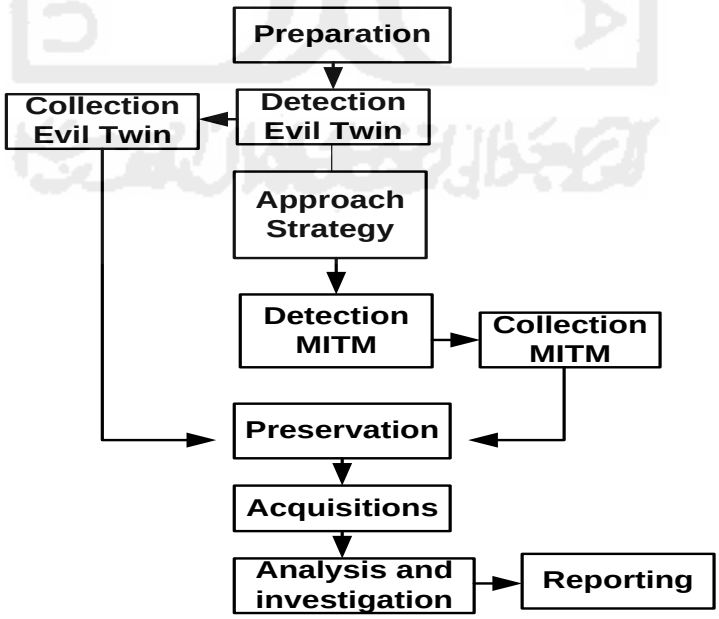
Evalusi model NFGP untuk kasus *Evil Twin Based MITM* sebelumnya, ditemukan beberapa kekurangan dalam proses pengungkapan kasus, antara lain adalah proses tahapan *detections* dan *collection* hanya dilakukan satu kali, akan tetapi dalam proses *detections* maupun *collection* data pada kasus Evil Twin based *MITM*, harus dibutuhkan dua kali tahapan *detection* dan *collection*, hal ini disebabkan kasus ini merupakan dua jenis metode serangan yang digabungkan menjadi satu metode serangan.

Berikut merupakan tabel proses pengusulan kerangka model forensik ENFGP yang diimplentasi dari kekurangan Kerangka model NFGP. Dari hasil evaluasi diusulkan 10 tahapan forensik, untuk lebih jelasnya dapat dilihat pada Tabel 4.4

Tabel 4. 4 Tabel Pengembangan Kerangka *Extendendd NFGP*

Extendend NFGP	Preparation	Detection Evil Twin	Collection Evil Twin	Approach Strategy	Detection MITM	Collection MITM	Preservation	Acquisitions	Analysis and Investigation	Reporting
NFGP	Preparation	Detection Evil Twin	Collection	X	X	X	Preservation	Examinations	X	Reporting

Proses Pembuatan model ENFGP dihasilkan dari hasil evaluasi kekurangan model NFGP dalam menangani kasus *MITM Based Evil Twin*, dan dari hasil evaluasi dihasilkan suatu bagan alur/ model forensik *Eextendend* NFGP (NFGP), untuk lebih jelasnya dapat dilihat pada Gambar 4.23.



Gambar 4. 23 Bagan Alur *Extendend* NFGP Untuk *MITM* Based *Evil Twin*

Pengujian tahapan dilakukan berdasarkan beberapa model forensik dari penelitian-penelitian sebelumnya, dan data dari keterangan model forensik diambil dari beberapa *review paper* pengembangan model forensik sebelumnya seperti (Yusoff et al. 2011), dengan menerapkan metode eliminasi, dalam pembuatan pengembangan model NFGP. Tahapan eliminasi dilakukan dalam dengan cara mengeliminasi tahapan – tahapan dari langkah tahapan yang sebelumnya telah ada, untuk di gunkan lebih lanjut sebagai acuan pengembangan framework.

Pengujian kerangka dalam penelitian ini akan dibuat sebuah tabel pengujian yang dilakukan berdasarkan model forensik dari penelitian sebelumnya yang kemudian akan di terapakan dengan metode *elimination similar state* seperti yang terlihat pada Tabel 4.5, dimana tahapan eliminasi dilakukan dengan mengidentifikasi seluruh tahpan dari model sebelumnya kemudian jika ditemukan adanya deskripsi tahapan yang tidak sama maka akan dihapus/digabungkan dan apabila jika pada prosess eliminasi terdapa tahapan yang memiliki deskripsi yang sama maka, akan dipertahankan.

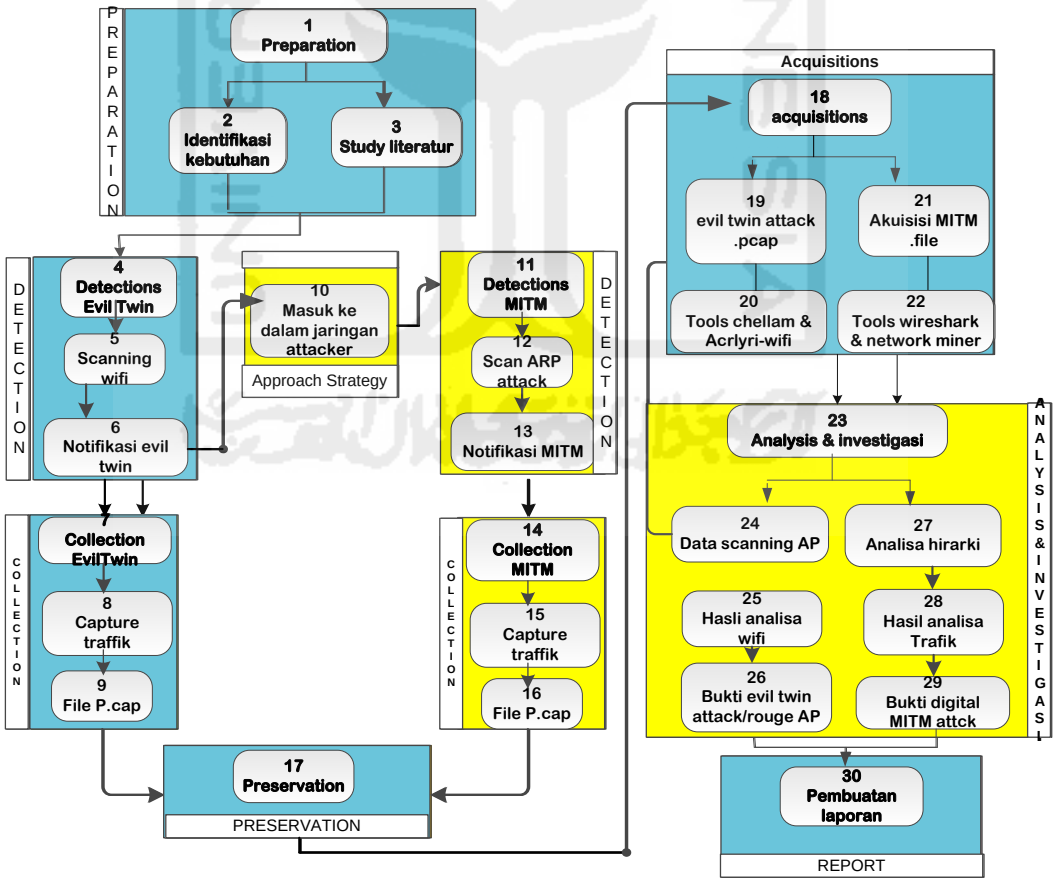
Tabel 4. 5 Pengujian Model Forensik Sebelumnya

No ID	Tahun	Nama Model
M1	1995	Computer Forensic Investigative Process
M2	2001	DFRWS Investigative Model
M3	2002	Abstract Digital Forensic Model
M4	2003	End to End Digital Investigation
M5	2004	Enhance Digital Investigation Process
M6	2004	Extended Model of Cybercrime Investigation
M7	2004	A Hierarchical, Objective-Based Framework for the Digital Investigation
M8	2006	Framework for a Digital Forensic Investigation
M9	2007	Dual Data Analysis Process
M10	2009	Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)
M11	2010	Network Forensic Generic Process Model

Tabel 4. 6 Pengujian Kerangaka ENFGP

No	Extendend NFGP generic phase	Available phase	No phase
1	Preparation	M3,M7, M9,M10	1.2, 1.3
2	Detection Evil twin	M15	4.5.6
3	Collection Evil Twin	M2,M3,M4,M6,M7,M11	7.8.9
4	Approach Strategy	M5	10
5	Detection MITM	M15	11.12.13
6	Collection MITM	M2,M3,M4,M6,M7,M15	14.15.16
7	Preservation	M2,M4,M15	17
8	Acquisitions	M9	18.19.20, 18.21.22
9	Analysis And Investigation	M2,M1,M11	23.24.25.26, 23.27.28.29
10	Reporting	M3,M4,M6,M7M,M8,M11	30

Proses tahapan pengujian selajutnya dilakukan berdasarkan implementasi kasus dari *MITM based Evil Twin*, yang dilakukan dalam penelitian ini, untuk lebih lengkapnya dapat dilihat pada Tabel.4.7 dalam lampiran.



Gambar 4. 24 Bagan Alur Detail Bagan Alur *Extendend* NFGP Untuk *MITM* Based *Evil Twin*

Gambar 4.24 merupakan proses investigasi forensik *Extendend* NFGP yang diimplementasikan dari kasus *MITM based Evil Twin.* Pengembangan model dilakukan berdasarkan proses pengujian menggunakan model-model sebelumnya. Tahapan –tahapan dalam model yang diberi tanda warna biru merupakan tahapan umum yang terdapat dalam model NFGP, sedangakan tahapan yang diberi tanda warna kuning merupakan tahapan-tahapan yang diusulkan dari penelitian ini yaitu tahapan *Aproach Strategy, detection MITM, collection MITM* dan *analysis* and investigasi.

Hasil akihir dari pengujian model pengembangan *Extendent* NFGP didapatkan 10 tahapan analisa dan 30 langkah investigasi, yang didapatkan melalui tahapan–tahapan yang dikembangakan berdasarkan metodologi yang diimplementasikan dari beberapa model forensik sebelumnya, seperti yang terlihat pada Tabel 4.5 dan Tabel 4.6

Implenmentasi proses bagan alur *Extendend* NFGP ini dapat dijalankan pada kondisi-kondisi seperti dibawah ini :

1. Teridentifikasi adanya serangan *Evil Twin* AP*/ Rougue Ap*.
2. Terhubung ke AP palsu untuk melakukan proses *sniffing*.

Apabila kondisi diatas tidak terpenuhi maka dapat dilakukan modifikasi pada bagian-bagian tertentu. Bagian yang memungkinkan untuk dilakukan proses modifikasi adalah bagian *acquisition* dan bagian *analisys,* yang dapat dimodifikasi sesuai kebutuhan proses investigasi.

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.

Daftar Pusataka

Adelstein, F., 2006. Diagnosing your system without killing it first. *Communications of the ACM*, 49(2), pp.63–66.

Anmulwar, S. et al., 2014. Rogue access point detection methods: A review. *International Conference on Information Communication and Embedded Systems (ICICES2014)*, (978), pp.1–6. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7034106.

Cai, M., Wu, Z. & Zhang, J., 2014. Research and Prevention of Rogue AP Based *MITM* in Wireless Network. *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, (2013), pp.538–542. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7024642.

Chandavarkar, B.R. et al., 2015. Detecting Rogue Access Points using Kismet., pp.172–175.

Client P. Garrison, 2010. *Digital Forensic for Network, Internet, and Clud Computing*,

Dong, Z. et al., 2015. Detecting and Locating Man-in-the-Middle *Attack*s in Fixed Wireless Networks., pp.283–293.

Lanze, F. et al., 2015. Hacker's toolbox: Detecting software-based 802.11 *Evil Twin* access points. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CC{Bibliography}NC 2015*, pp.225–232.

Mangut, H.A. et al., 2015. ARP Cache Poisoning Mitigation and Forensics Investigation. *2015 IEEE Trustcom/BigDataSE/ISPA*, pp.1392–1397. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7345444.

Mustafa, H. & Xu, W., 2014. CETAD: Detecting *Evil Twin* access point *attack*s in wireless *hotspot*s. *2014 IEEE Conference on Communications and Network Security, CNS 2014*, pp.238–246.

Nakhila, O. et al., 2015. User-side Wi-Fi *Evil Twin Attack* detection using SSL/TCP protocols. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, pp.239–244.

Nanavare, V. V, 2016. Robust and Effective *Evil Twin* Access Point., pp.9074–9084.

Pilli, E.S., Joshi, R.C. & Niyogi, R., 2010. A Generic Framework for Network Forensics. *International Journal of Computer Applications*, 1(11), pp.1–6.

Rahman, S. & Khan, M.N.A., 2015. Review of live forensic analysis techniques. *International Journal of Hybrid Information Technology*, 8(2), pp.379–388. Available at: http://www.sersc.org/journals/IJHIT/.

Utami Putri, R. & Istiyanto, J.E., 2012. Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. *International Journal of Computer Science and Security*, 6(2). Available at: http://journal.ugm.ac.id/index.php/ijccs/article/view/2157.

Yang, C., Song, Y.M. & Gu, G.F., 2012. Active User-Side *Evil Twin* Access Point Detection Using Statistical Techniques. *Ieee Transactions on Information Forensics and Security*, 7(5), pp.1638–1651.

Yusoff, Y., Ismail, R. & Hassan, Z., 2011. Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, 3(3), pp.17–31.

Adelstein, F., 2006. Diagnosing your system without killing it first. *Communications of the ACM*, 49(2), pp.63–66.

Anmulwar, S. et al., 2014. Rogue access point detection methods: A review. *International Conference on Information Communication and Embedded Systems (ICICES2014)*, (978), pp.1–6. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7034106.

Cai, M., Wu, Z. & Zhang, J., 2014. Research and Prevention of Rogue AP Based *MITM* in Wireless Network. *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, (2013), pp.538–542. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7024642.

Chandavarkar, B.R. et al., 2015. Detecting Rogue Access Points using Kismet., pp.172–175.

Client P. Garrison, 2010. *Digital Forensic for Network, Internet, and Clud Computing*,

Dong, Z. et al., 2015. Detecting and Locating Man-in-the-Middle *Attack*s in Fixed Wireless Networks., pp.283–293.

Lanze, F. et al., 2015. Hacker's toolbox: Detecting software-based 802.11 *Evil Twin* access points. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, pp.225–232.

Mangut, H.A. et al., 2015. ARP Cache Poisoning Mitigation and Forensics Investigation. *2015 IEEE Trustcom/BigDataSE/ISPA*, pp.1392–1397. Available at:

http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7345444.

Mustafa, H. & Xu, W., 2014. CETAD: Detecting *Evil Twin* access point *attack*s in wireless *hotspot*s. *2014 IEEE Conference on Communications and Network Security, CNS 2014*, pp.238–246.

Nakhila, O. et al., 2015. User-side Wi-Fi *Evil Twin Attack* detection using SSL/TCP protocols. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, pp.239–244.

Nanavare, V. V, 2016. Robust and Effective *Evil Twin* Access Point., pp.9074–9084.

Pilli, E.S., Joshi, R.C. & Niyogi, R., 2010. A Generic Framework for Network Forensics. *International Journal of Computer Applications*, 1(11), pp.1–6.

Rahman, S. & Khan, M.N.A., 2015. Review of live forensic analysis techniques. *International Journal of Hybrid Information Technology*, 8(2), pp.379–388. Available at: http://www.sersc.org/journals/IJHIT/.

Utami Putri, R. & Istiyanto, J.E., 2012. Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. *International Journal of Computer Science and Security*, 6(2). Available at: http://journal.ugm.ac.id/index.php/ijccs/article/view/2157.

Yang, C., Song, Y.M. & Gu, G.F., 2012. Active User-Side *Evil Twin* Access Point Detection Using Statistical Techniques. *Ieee Transactions on Information Forensics and Security*, 7(5), pp.1638–1651.

Yusoff, Y., Ismail, R. & Hassan, Z., 2011. Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, 3(3), pp.17–31.

Singh, O., 2009. *Network* Forensik. Indian Computer *Response Team (CERT-In). Department of Information Technology*, New Delhi, India.

Sulianta, F., 2008, *Komputer* Forensik. Jakarta : PT. Elex Media Komputindo.

Volonino, L. and Reynaldo A., 2008, *Computer* Forensik *For Dummies*. Indianapolis, Indiana : Wiley Publishing, Inc.

Ruchandani, B., Kumar, M., Kumar, A., Kumari, K., Sinha., A.,K., 2006, Ekperimentation In *Network* Forensik Analysis. *Proceedings of the Term Paper Series under CDACCNIE Bangalore*, India, December 2006.

Dhinda. maydhita dcp 2014. Implementasi Teknik Mitigasi *ARP Cache Poisoning* Dengan Kendali Penulisan *Arp Cache Table*. Tugas Akhir, Program Teknologi Informasi dan Ilmu Komputer Universitas Brawijaya, Malang.

Marcella, Albert J., and Robert S. Greenfiled, "*Cyber* Forensik *a field manual for collecting, examining, and preserving evidence of computer crimes*", by CRC Press LLC, United States of America

Casey. "*Digital Evidence and Computer Crime*", 2nd ed., hal. 20

Arbough, William A, Narendar Shankar and Y.C Justine Wan, 2001. Your 802.11 *Wireless Network* Has No Clothes. Departemen of Computer *Science* University of Mary*LAN*d. 22 September 2004.

Eoghan Casey. *Digital Evidence and Computer Crime - 2nd Edition. Academic* Press, 2004.

Purbo, O., Tanuhandaru, P., Noertam, P., & Djajadikara, M. (2007) Jaringan *Wireless* Di Dunia Berkembang. Andi Yogyakarta, 425. http://doi.org/004.68 PUR j

Naskah akademik RUU tindak pidana di bidang Teknologi Informasi disusun oleh Mas Wigantoro Roes Setiyadi, Op.Cit, hal.25-26

Barda Nawawi Arief., Antisipasi Penanggulangan "*Cybercrime*" dengan hukum Pidana.,makalah pada seminar Nasional mengenai "*Cyberlaw*"., di STHB, Bandung, Hotel Grand *Aquila*, 9 April 2001.

Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarto, Cybercrime-Motif dan Penindakan, Pensil 324, Jakarta, hal.13-14

T. Sukardi, "Forensik Komputer Prinsip Prinsip Dasar," pp. 1– 21, 2012.

Diakses dari http://vistumbler.id.uptodown.com/ di acsses pada tanggal 24 April 2016.21.00 WIB

Diakses dari http://file.scirp.org/Html/3-7800083_21340.htm di accsess tanggal 24 April 2016 21.00 WIB

Diakses dari http://etutorials.org/*Network*ing/ di accsess tanggal 24 April 2016 21.00 WIB

Diakses dari http://syworks.blogspot.co.id/2014/01/wireless-ids-intrusion-detection system.html di akses pada tanggal 24 April 2016. 21.00 WIB.

Lampiran

Tabel 4. 7 Pengujian Hasil Tahapan ENFGP

NO	TAHAPAN INVESTIGASI		KETERANGAN	HASIL PENGUJIAN
1	**Preparation**		Preparation merupakan tahapan awal di mana berisi tentang langkah -langkah maupun kebutuhan baik *tools software* ataupun *hardware* yang akan digunakan pada awal investigasi	• Identifikasi kebutuhan • *Lireture Review*
2		**Indentifikasi Kebutuhan**	*Literatur review* akan membahas tentang uraian dari teori, temuan-temuan maupun rangkuman – rangkuman dari penelitian sebelumnya yang nanti dapat digunakan sebagai landasan atau acuan dalam melakukan kegiatan penelitian	• *Software* • *Hardware*
3		**Study literature**	*Identification* kebutuhan akan disesuaikan dengan kondisi pada kasus seperti kebutuhan perangkat keras maupun perangkat lunak	• *Network* Forensik • Penelitian Sebelumnya • konsep dasar deteksi MITM base *Evil Twin*
4	**Detection Evil twin**		*Detection* merupakan salah tahapan awal dimana, investigator melakukan prosess *scanning* untuk menemukan adanya kemungkinan AP palsu	• *Detection* menggunakan Chellam
5		**Scanning**	Scanning merupakan tahapan prosess *scanning population* AP yang di lakukan di suatu *public Area*	• *Scanning* ditemukan adanya ancaman serangan *Evil Twin*
6		**Notification**	*Notification* merupakan pemberi informasi apabila ditemukanadanya serangan *Evil Twin/Rogue* AP.	• Notifikasi serangan *Evil Twin*, untuk Lebih jelasnya dapat di lihat pada Gambar 4.5

Tabel Hasil Tahapan ENFGP Lanjutan

NO	TAHAPAN INVESTIGASI		KETERANGAN	HASIL PENGUJIAN
7	**Collection Evil Twin**		*Collection Evil Twin* merupakan tahapan pengumpulan data dan informasi terkait AP yang mencurigakan.	
8		**Scanning AP & Capture wifi Traffik**	*Scanning* AP di lakukan dengan menggunakan aplikasi Chellam dan Acrlyric-wifi, dengan bertujuan untuk menggumpulkan data data AP	• *Scanning* detail info menggunakan Chellam • *Capture* Traffik menggunakan Acrlyric-
9		**Data Scanning Population**	data *scanning* berupa tabel informasi hasil *capture* traffik *wfii*	• Tabel info detail • file Pcap
10	**Approach Strategy**	**Entry into the network evil twin AP**	Masuk ke dalam jaringan Evil Twin ketika ditemukan adanya Notifikasi serangan *Evil twin* dengan Tujuan Untuk mengumpulkan informasi lebih lanjut	• Masuk ke dalam jangkaun *Evil twin* untuk melakukan proses *caprture* Traffik
11	**Detection MITM**		Proses *detection* MITM di lakukan Untuk menidentifikasi adanya kemungkan serangan MITM.	• Deteksi Arp attack menggunkan Xarp
12		**Scan Arp Attack**	Proses *Scanning* Arp Attack menggunakan Aplikasi Xarp, untuk menemukan adanya serangan ARP	• Dari hasil *scan* ditemukan adanya serangan ARP *attack*, dimana terlihat

Tabel Hasil Tahapan ENFGP Lanjutan

NO	TAHAPAN INVESTIGASI		KETERANGAN	HASIL PENGUJIAN
13		**Notification**	*Notication* di berikan apabila ditemukan adanya serangan ARP.	• Notifikasi serangan dapat di lihat pada Gambar 4.12
14	**Collection MITM**		*Collection* MITM, merupakan tahapan penggumpulan informasi terkait dengan serangan MITM	• Proses *collection* di lakukan menggunakan aplikasi Wireshark, dan
15		**Capture wifi Traffik**	*Capture* Traffik dilakukan dengan mengamati laluntas data di dalam jaringan *Evil Twin* , dengan menggunkan aplikasi Wireshark	• File Pcap dengan nama : Mitm analisa.Pcap
16		**File Pcap**	File Pcap merupakan file hasil capture traffik yang di simpan dalam bentuk pcap. File Pcap berisitentang informasi laluntas data yang teriadi di dalam jaringan	• Hasi *capture* file dapat dilihat pada tabel 4.1
17	**Preservation**		*Preservation* adalah tahapan pengamann informasi yang ditemukan dalam prosses *collection*	• Dari hasil *scan* ditemukan adanya serangan ARP *attack*, dimana terlihat *source* IP 10.0.0.1 melakukan recquest pada

Tabel Hasil Tahapan ENFGP Lanjutan

NO	TAHAPAN INVESTIGASI		KETERANGAN	HASIL PENGUJIAN
18	**Acquisitions**		Akuisisi data serangan merupakan hasil pengakuisisian data network traffik dengan menggunakan beberapa metode seperti filterisasi maupun memanfaatkan modul modul pada wireshark lainnya	• Proses akuisisi dengan menggunkan *tools* Wireshark, Networkminer, Chellam dan Acrlyric-wifi
19		**Tabel informasi Evil Twin attack**	Tabel informasi merupakan data dari tabel scanning dan file pcap, hasil dari prosses Capture Traffik	• Tabel dan informasi *Evil Twin Attack* merupakan informasi yang dikumpulakan pada tahapan *collection*
20		**Tools Chellam & Acrlyric-wifi**	Chellam digunakan untuk menaganalisa data *scanning* AP dan Acrlyric digunakan untuk melakukan *capture* traffik	• Hasil analisa dapat dilihat pada Gambar 4.7, 4.8, 4.9, 4.10
21		**MITM attack .pcap**	File Pcap hasil capture traffik lalulintas data dalam jaringan *Evil Twin*	• Akuisisi file pcap • Akuisisi menggunkan modul hirarki
22		**Tools wireshark & network miner**	Prosses akuisisi dilakukan menggunkan aplikasi Wireshark dan Networkminer	• Dari hasil *scan* ditemukan adanya serangan ARP *attack*, dimana terlihat *source* IP 10.0.0.1

Tabel Hasil Tahapan ENFGP Lanjutan

NO	TAHAPAN INVESTIGASI		KETERANGAN	HASIL PENGUJIAN
23	**Analysis And Investigation**		Merupakan tahapan proses analisis dan investigasi forensik	• Proses analisa daninvestigasi menggunakan Metode *live* forensik
24		**Analisa data scanning AP**	Merupakan tahapan dalam menganalisa data scanning dan file Pcap	• Analisa di lakukan dari data yang terlihat pada Gambar 4.7, 4.8, 4.9, 4.10
25		**Hasli analisa wifi**	Merupakan proses akhir dan menemukan hasil analisa dari proses sebelumnya.	• Dari hasil scanning ditemukan adanya dua AP yang menggunakan SSID "PUSFID", dengan Mac "e4:8d:8c:ca:80:c0, dengan kode vendor : "Routerboard.com,

Tabel Hasil Tahapan ENFGP Lanjutan

NO	TAHAPAN INVESTIGASI		KETERANGAN	HASIL PENGUJIAN
26		**Bukti evil twin attack/rouge AP**	Proses penemuan barang bukti *digital Evil Twin* Ap yang ditemukan melalui prosses analisa sebelumnya.	• Notifikasi dari Chellam • SSID dengan Mac: f4:f2:6d:1c:76:15, dengan kode Vendor : "Tp-Link technologies.co.ltd", kekuatan
27		**Analisa File pcap**	Merupakan tahapan tahapan untuk menganalisa file Pcap dari hasil *capture* traffik pada jaringan *Evil Twin* .	• Deteksi IP • Analisa Port ARP
28		**Hasil analisa Trafik**	Merupakan tahapan akhir dari proses analisa *capture* trafik.	• hasil analisa dapat dilihat pada Gambar 4.14, 4.15, 4.16 dan 4.7
29		**Bukti digital MITM attck**	Proses penemuan barang bukti *digital* MITM *Attcak* yang ditemukan melalui prosses analisa sebelumnya.	• IP dan Mac pelaku : 10.0.0.1/Tp-link_89:7a:15
30	**Reporting**		merupakan proses akhir, yaitu penyusunnan laporan dari hasil informasi barang bukti yang ditemukan dari beberapa tahapan analisa sebelumnya	• Hasil laporan di buat berdasarkan evaluasi dan hasil dari tahapan analisa

ISLAM
UNIVERSITAS
INDONESIA

ISLAM
UNIVERSITAS
INDONESIA