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,

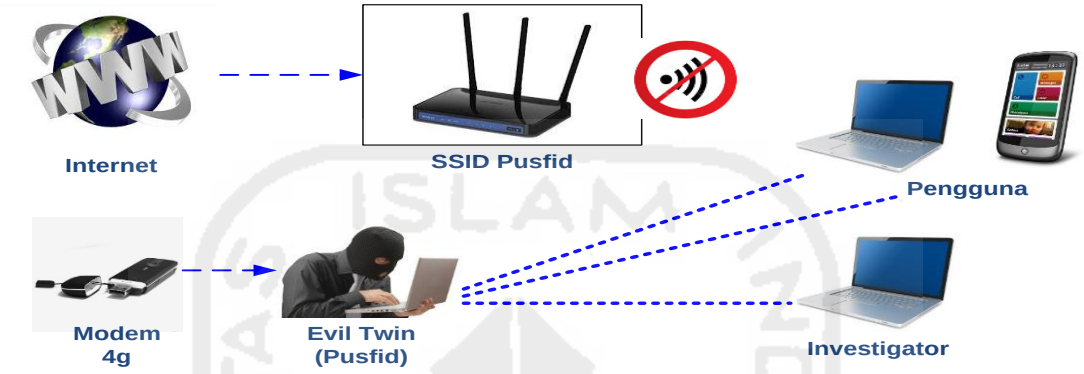
- OS windows 7 64/32 bit
- Chelam.exe
- Xarp.exe
- Wire shark
- Vistumbler
- VMware versi 11
- OS kali Linux 2.0
- Ettercap.
- *Wifi* pumpkin
- *Network* stumbler
- Mozilla Firefox / Google crime.

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*

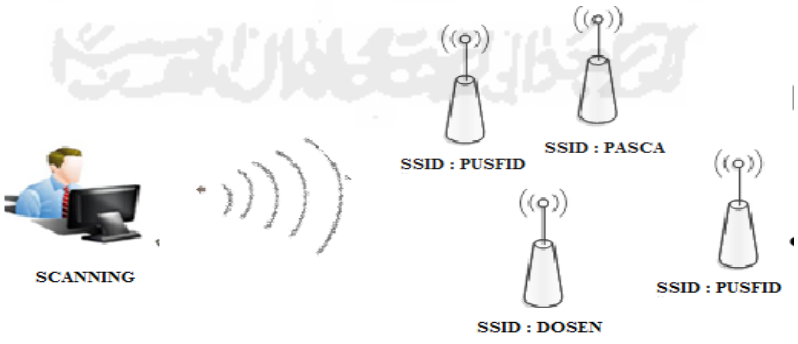
Pola serangan yang digunakan pelaku adalah dengan melaukan kofigurasi AP palsu yang menggunakan *SSID* yang mirip dengan salah satu *SSID* target di sekitar area *Wifi* yang terdapat di fakultas teknologi industri universitas islam indonesia, pada kasus ini pelaku menggunakan AP palsu dengan *SSID* "pusfid" 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.

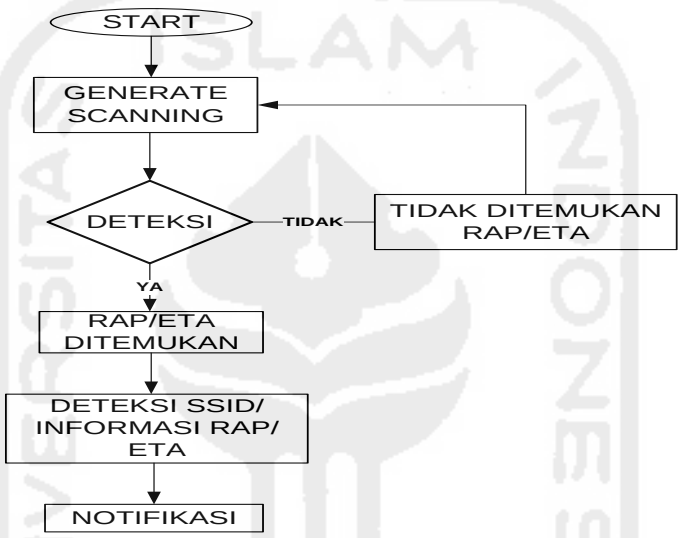


Gambar 4. 3 *Scanning Access Point*

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.

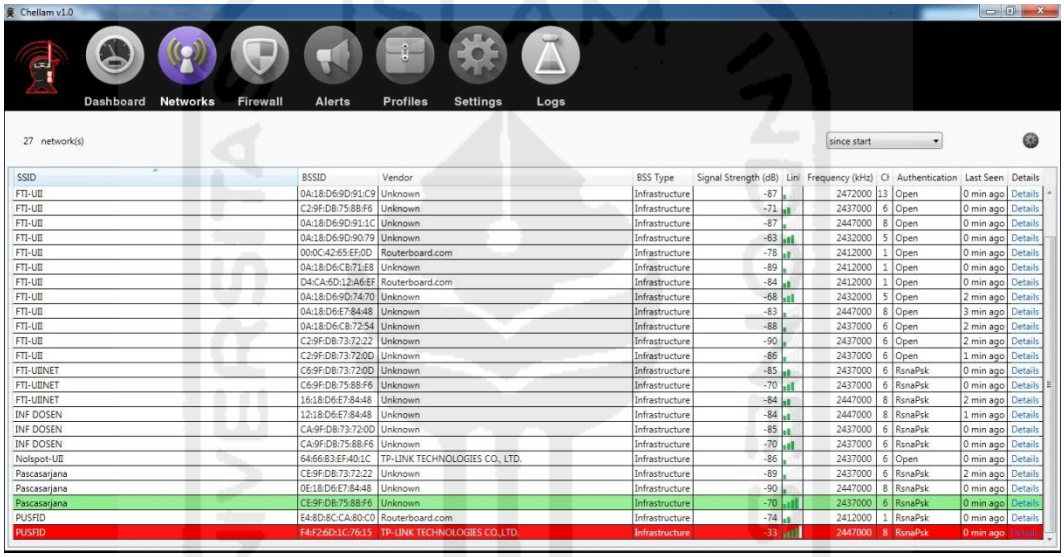


Gambar 4. 4 Proses Detect Chellam

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.

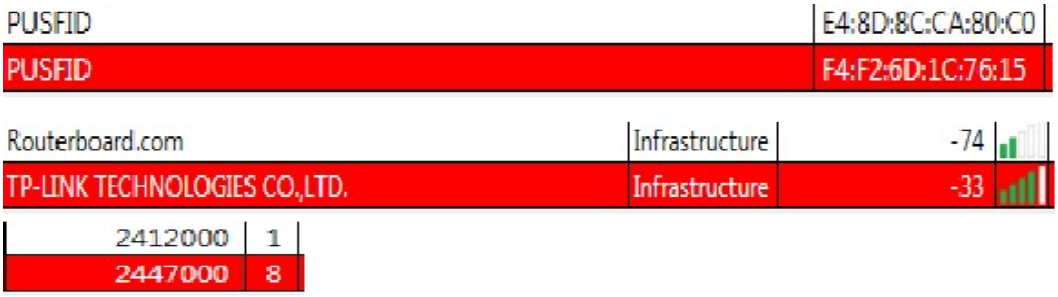
Gambar 4. 5 Notifikasi Chellam

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,



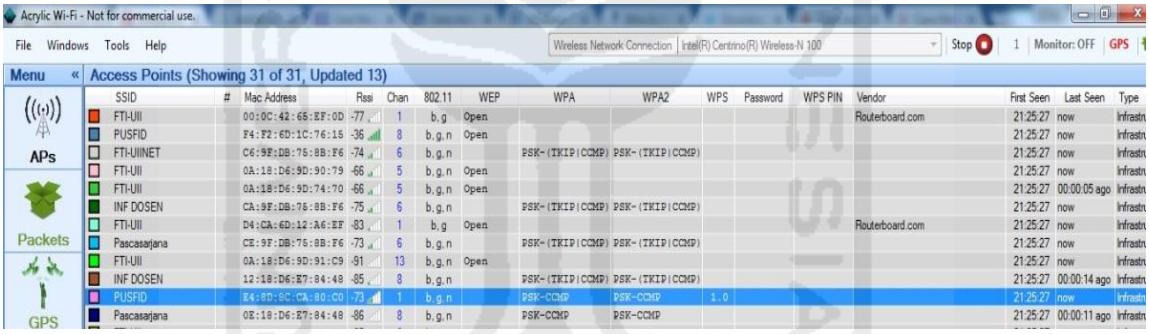
Gambar 4. 6 *Scanning* Analysis *Wifi* Chellam

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



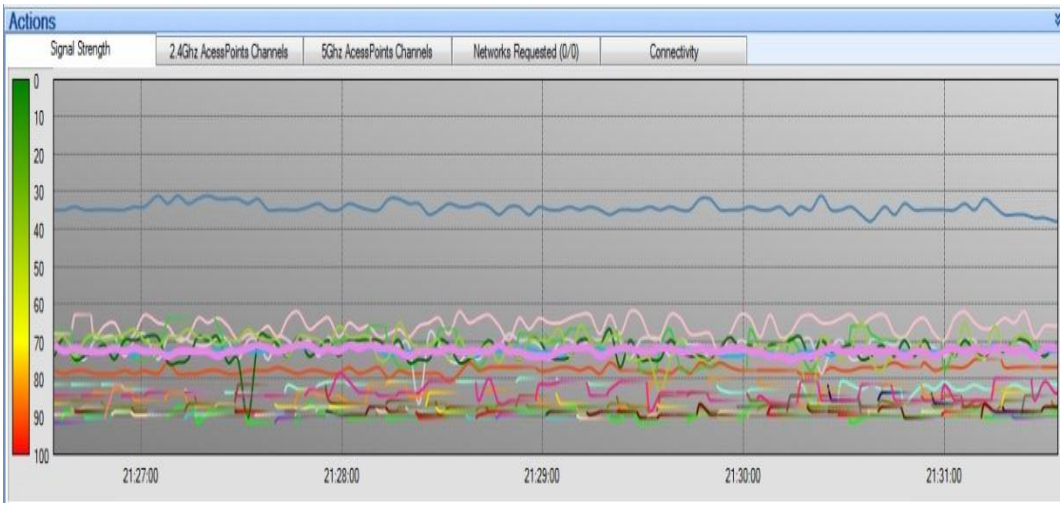
Gambar 4. 7 Analisa *Wifi*

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.

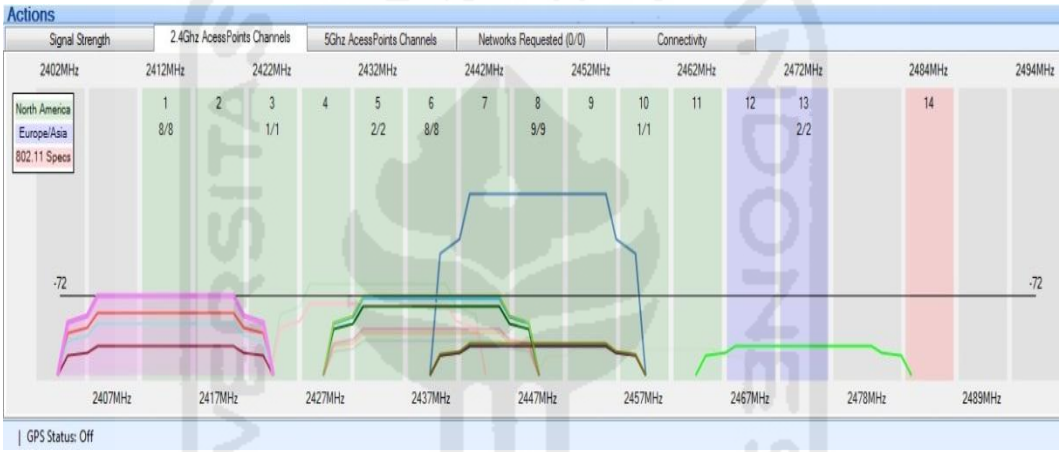


Gambar 4. 8 *Scanning* Analisis Menggunakan Arcliric-Wifi

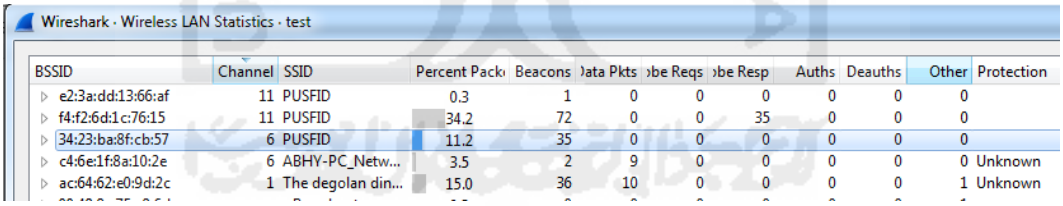
Pada capture jaringan *Wifi* menggunakan acrilyc-*Wifi* ditemukan rangkaian statistic sinyal *Wifi*, AP pusfid yang diberi tanda warna biru menunjukan tingkat kekuatan sinyal di atas rata-rata dengan -37db, dibanding dengan AP yang diberi tanda merah mudah yang hanya berkekutan sinyal -74 db. Menurut (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

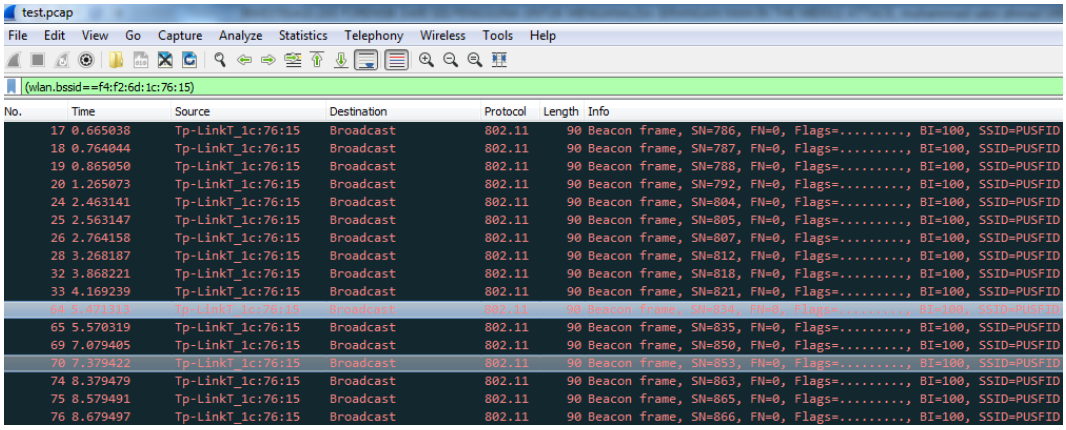


Gambar 4. 10 Analisa Statistik *2.4 Ghz Acsses Point/Channel*



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*

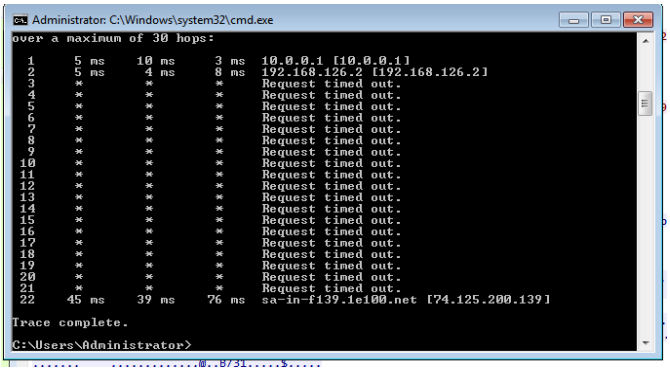
4.5.2 Approach Strategy

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

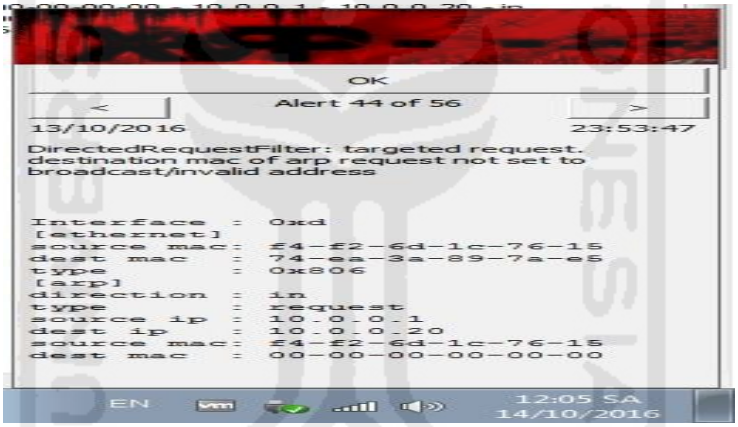
Pada tahapan ini, dimulai dengan mencari tau IP dari *router* pelaku dengan menggunakan perintah *tracert* seperti yang terlihat pada Gambar 4.13, telihat IP yang digunakan oleh pelaku adalah 10.0.0.1 sebagai *gateway* dan 192.168.126.2.



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

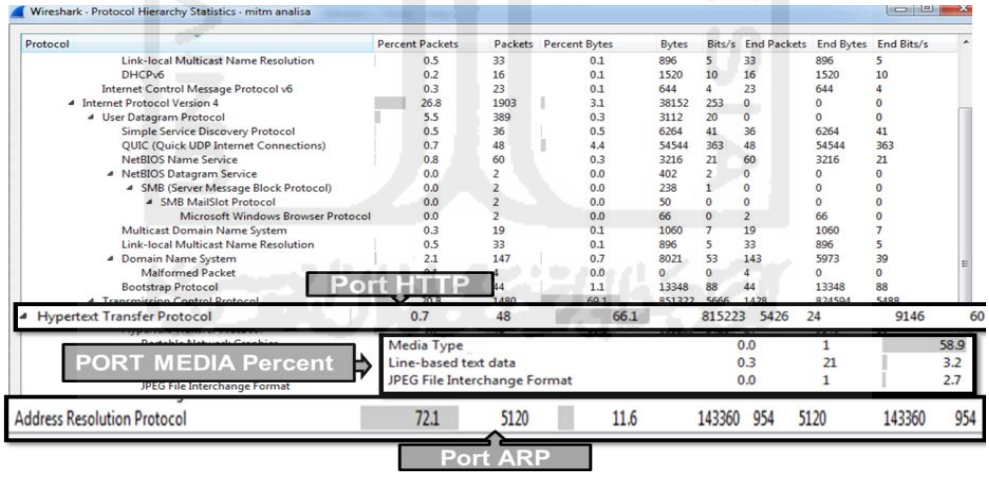
Capture paket trafik dengan menggunakan Wireshark di dalam jaringan *Evil Twin* tersebut, dilakukukan selama beberapa menit untuk menemukan *beberapa* informasi yang dapat digunakan untuk proses analisa selanjutnya, berikut detail file pcap yang akan dianalisa, seperti yang terlihat pada tabel 4.1.

Tabel 4. 1 Tabel File Pcap

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

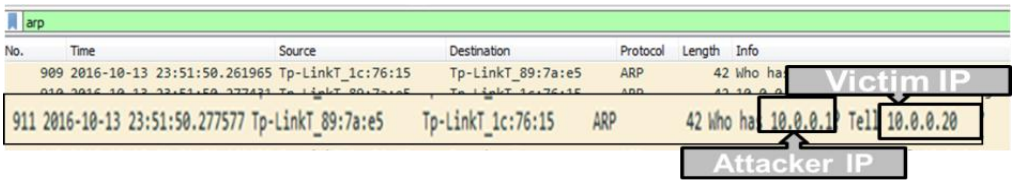
4.5.4 Akuisisi data serangan

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



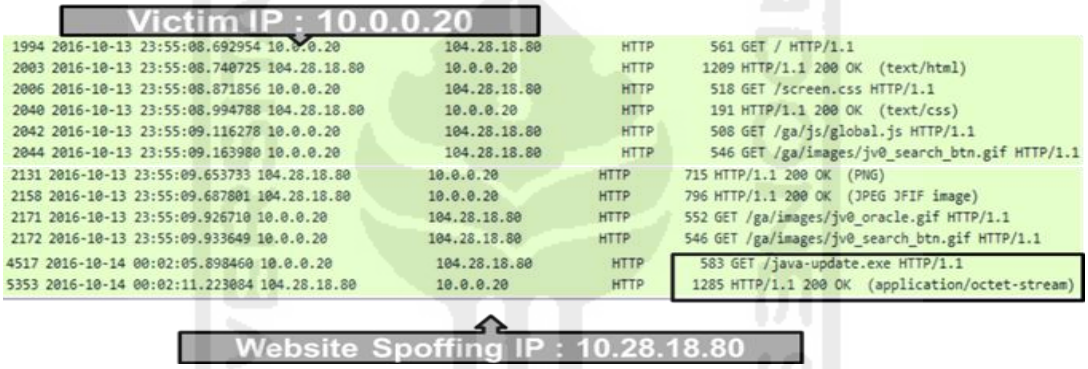
Gambar 4. 15 Wireshark Hirarki Modul

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

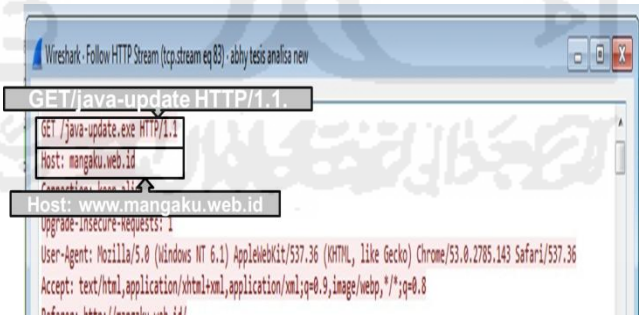


Gambar 4. 16 *Arp* Filter

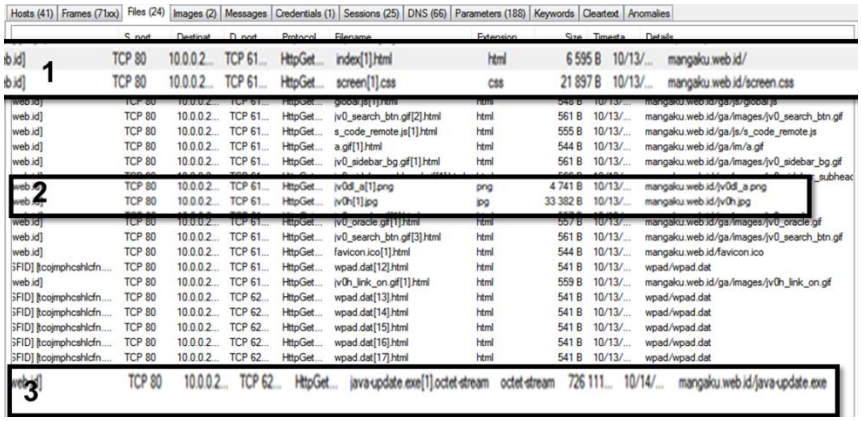
Pada Analisa filterisasi *port* HTTP, terlihat IP 10.0.0.20 melakukan *request* ke IP 104.28.18.80, kemudian IP 10.0.0.20 diarahkan untuk mengakses situs yang kemungkinan sengaja disiapkan. Dari hasil analisa pada *port* HTTP juga terlihat adanya beberapa file yang mencurigakan diantaranya adalah file 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

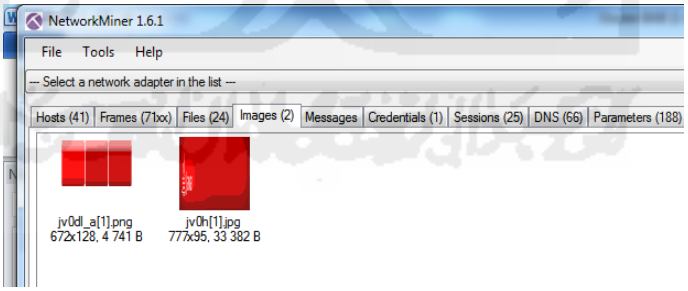


Gambar 4. 19 *Network* Miner File Analisis

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.

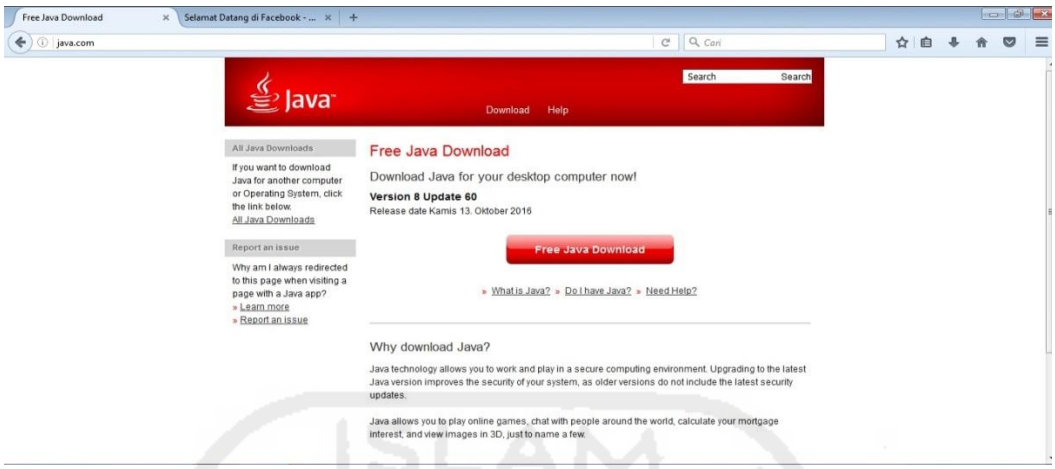
Dari hasil dari analisa sebelumnya, dicurigai pelaku mencoba melakukan *intercept download* dengan cara menggunakan metode DNS *Spoofing*, ARP *spoff*, untuk mengarahkan para korban ke situs yang sengaja dibuat olehnya.



Gambar 4. 20 Images Analisis

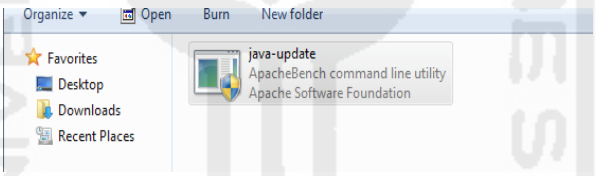
Untuk mengetahui hasil dari analisa sebelumnya, dicurigai pelaku mencoba melakukan *intercept download* dengan cara menggunakan metode dns *spoofing*, *Arp spoff* untuk mencoba mengarahkan para korban ke situs yang sengja dibuatnya, peneliti yang juga merupakan *user* akan mencoba dengan sengaja masuk 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

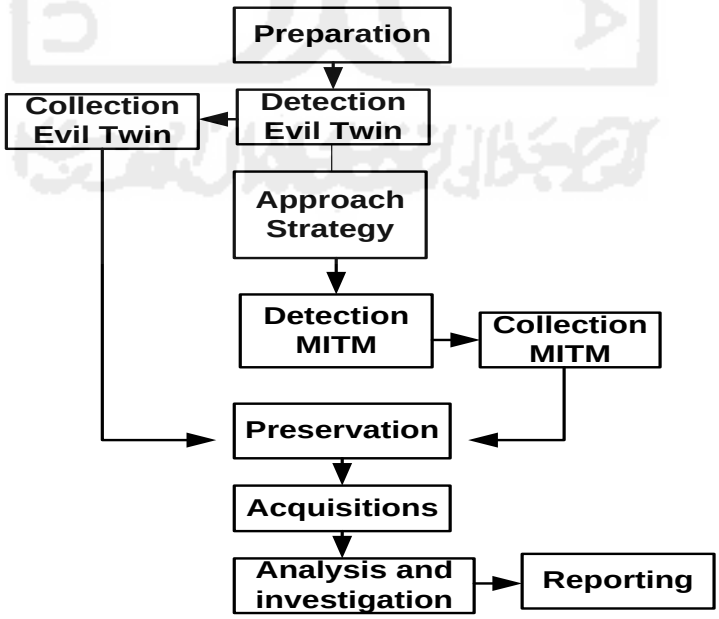
Evalusi model NFGP untuk kasus *Evil Twin Based MITM* sebelumnya, ditemukan beberapa kekurangan dalam proses pengungkapan kasus, antara lain adalah proses tahapan *detections* dan *collection* hanya dilakukan satu kali, akan tetapi dalam proses *detections* maupun *collection* data pada kasus Evil Twin 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.

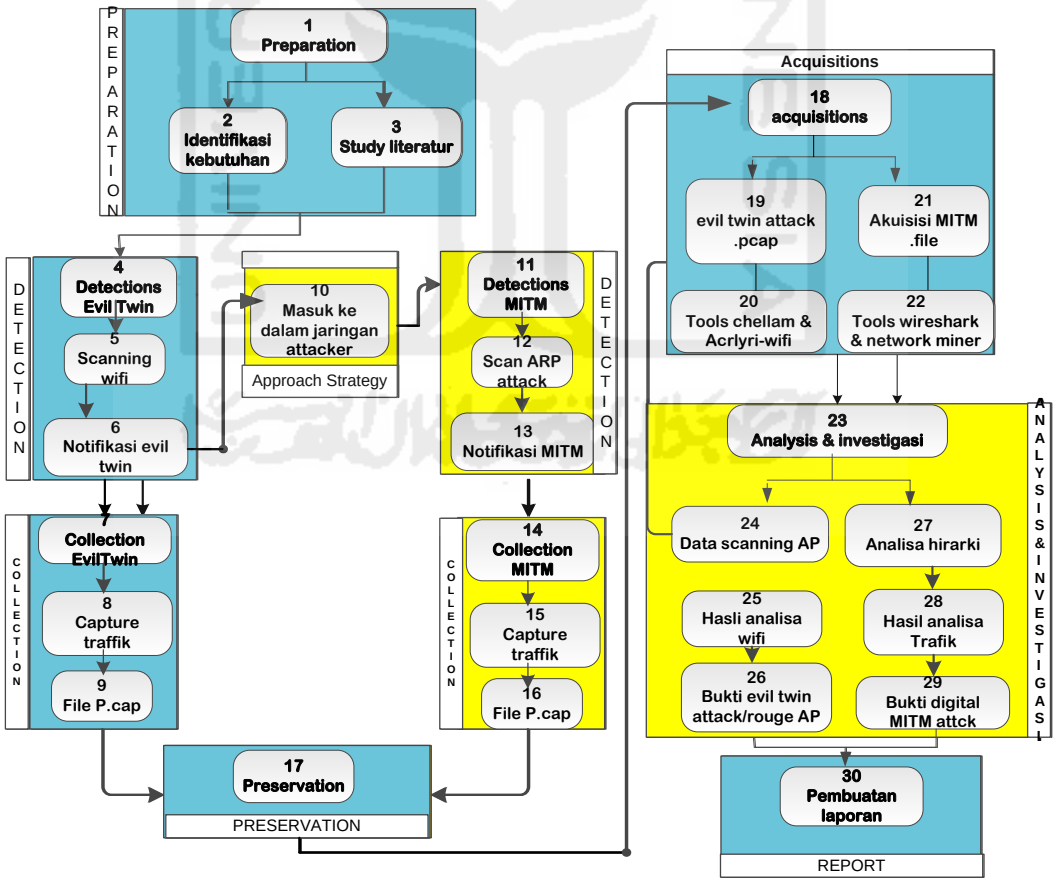
Tabel 4. 5 Pengujian Model Forensik Sebelumnya

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.