

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

Muhammad Sabri Ahmad¹, Imam Riadi², Yudi Prayudi³

E-mail: abhyoffu@gmail.com¹, imam.riadi@is.uad.ac.id², prayudi@uii.ac.id³

Program Studi Magister Teknik Informatika – Universitas Islam Indonesia^{1,3}

Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia²

Abstrak

MITM based Evil twin menjadi suatu ancaman yang berbahaya bagi para pengguna jaringan *Wifi*. Pelaku penyerangan ini memanfaatkan AP (*Access Point*) palsu dengan konfigurasi *gateway* yang berbeda dengan *legitimate AP*, sehingga jenis serangan ini menjadi cukup sulit untuk dideteksi, disisi lain proses pengungkapan kasus serangan *MITM based Evil Twin* hanya sebatas mendeteksi aktivitas serangan dan belum ada pembahasan lebih lanjut terkait digital forensik. Penelitian ini dilakukan dengan menerapkan pendekatan metode *Live forensik* dan pendekatan dari sisi *user*, untuk mendeteksi aktivitas ilegal yang terjadi di dalam jaringan *Wifi*, Proses investigasi *MITM Based Evil* dibagi menjadi empat tahapan, dimulai dari proses *collection, examination, analysis* dan *reporting* dan analisa Forensik, selain itu penelitian ini difokuskan pada dua proses penelitian yaitu proses analisa *Wifi scanning* dan analisa *network* trafik untuk proses penemuan barang bukti *digital* berupa informasi trafik data dari serangan *mitm based evil twin*.

Kata kunci: *Wifi, Evil Twin Attack, Live forensik, MITM, User side*

1. PENDAHULUAN

Wifi kini telah menjamur di berbagai tempat *public area*, mulai dari *cafe*, restoran, universitas hingga beberapa tempat umum lainnya. Selain dapat diakses dengan kecepatan tinggi juga lebih murah, sehingga minat para pengguna *Internet* menjadi semakin antusias untuk menggunakan *Wifi*. namun sayangnya tanpa disadari hal ini dapat mengundang bahaya yang tidak terduga. Hal ini terlihat dari fakta banyaknya ancaman dalam jaringan *Wifi*. Jenis ancaman-ancaman yang sering terjadi pada jaringan *Wifi* adalah *ETA (Evil Twin Attack)*. Serangan ini dilakukan dengan memanfaatkan AP (*Access Point*) palsu yang dibuat sama persis dengan *legitimate AP* dengan tujuan untuk menjebak para pengguna jaringan *Wifi* [1], kemudian pelaku dapat melancarkan serangan *MITM (Man In The Middle Attack)* untuk melakukan aktivitas *snifing, spoofing* dan kegiatan ilegal lainnya.

Penanganan serangan *MITM Based Evil Twin* pada saat ini masih sangat terbatas, umumnya yang dilakukan hanya sebatas aktivitas deteksi terhadap serangan *MITM Based Evil Twin*. Seperti yang dilakukan oleh [2], [3], [4], namun hal terkait dengan proses investigasi forensika digital untuk mengungkapkan bukti adanya serangan masih belum banyak dibahas lebih lanjut padahal dalam proses pengungkapan kasus dibutuhkan lebih dari sekadar proses pendekteksian untuk pencarian bukti karena itu pendekatan forensik sangatlah penting dalam proses mengungkapkan kasus *MITM Based Evil Twin*.

Evil twin attack dapat dijalankan dengan menggunakan dua metode penyerangan, yaitu metode serangan yang memanfaatkan *IP gateway* yang sama dengan *IP gateway legitimate AP* dan metode serangan yang memanfaatkan jaringan modem *GSM/CDMA* atau menggunakan *IP gateway* yang berbeda dari *legitimate AP*. Penelitian ini dilakukan pada kasus serangan *MITM Based Evil twin* yang menggunakan *gateway* yang berbeda dengan AP target. hal ini dikarenakan jenis serangan ini lebih sering digunakan dan sulit untuk dideteksi dari sisi *administrator* [5], Oleh karena itu dibutuhkan pendekatan dari sisi *user* dan metode forensik yang dapat digunakan untuk menemukan bukti *digital* pada *sistem* yang sedang berjalan yaitu metode *Live forensik*. Penelitian ini akan meliputi bagaimana melakukan proses tahapan investigasi *Live forensik* dan bagaimana melakukan pendeteksian serangan *MITM Based Evil Twin* dari sisi *user* untuk menemukan informasi yang dapat dijadikan barang bukti.

2. Metode

2.1 Network Forensik

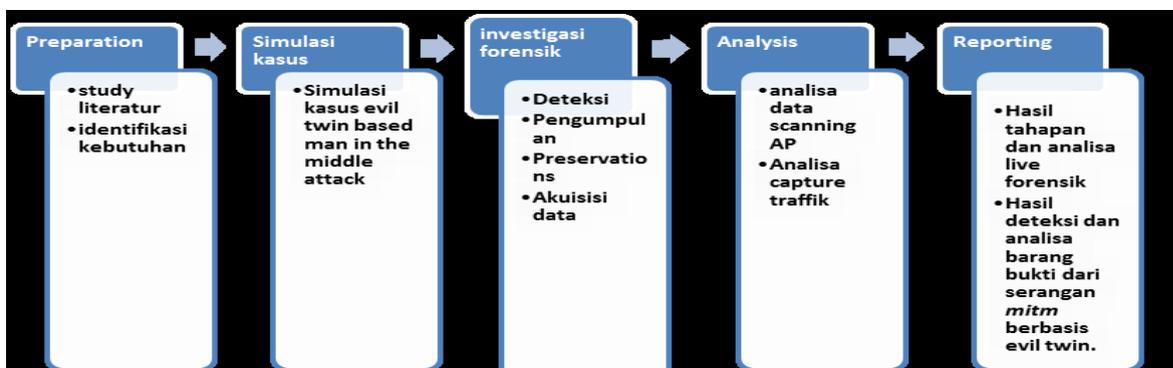
Network Forensik digunakan dalam menganalisa kasus-kasus ilegal terkait jaringan komputer, fungsinya meliputi semua kemungkinan yang dapat menyebabkan pelanggaran keamanan *sistem*, seperti yang pernah disampaikan oleh [5]. Forensik jaringan merupakan bagian dari Forensik *digital*, di mana bukti ditangkap dari jaringan dan diinterpretasikan berdasarkan pengetahuan dari serangan jaringan, dengan tujuan untuk menemukan penyerang dan merekonstruksi tindakan serangan penyerang melalui analisis bukti penyusupan. Menurut [6] suatu lembaga pelatihan yang bergerak khusus dibidang *digital Forensik*, mengatakan bahwa *Network forensik* adalah kegiatan pengumpulan barang bukti *digital* dengan cara merekam, dan analisa lalu lintas data pada suatu jaringan dengan tujuan untuk menemukan sumber dari sebuah serangan.

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

2.2 Live Forensik

Metode Live forensik pada dasarnya memiliki kesamaan pada teknik forensik tradisional yaitu identifikasi penyimpanan, analisis, dan presentasi, metode *Live forensik* merupakan respon dari kekurangan teknik forensik tradisional yang tidak bisa mendapatkan informasi dari data dan informasi yang hanya ada ketika sistem sedang berjalan misalnya aktivitas *Memory*, *Network proses*, *Swap file*, *running sistem proses*, dan informasi dari *file* sistem dan ini menjadi kelebihan dari teknik *Live forensik*, menurut [7] teknik *Live forensik* telah berkembang dalam dekade terakhir, seperti analisis *content memory* untuk mendapatkan gambaran yang lebih baik mengenai aplikasi dan proses yang sedang berjalan.

Penelitian ini pada dasarnya menggunakan pendekatan dari metodologi yang digunakan oleh teknik *Live forensik*, secara lengkapnya dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Metodologi Penelitian

2.3 Preparation

Preparation merupakan tahapan awal untuk mengidentifikasi kebutuhan dalam menganalisa kasus, dalam kasus ini tahapan *preparation* terbagi menjadi 2 bagian yaitu, tahapan identifikasi kebutuhan yang merupakan tahapan persiapan *tools* yang akan digunakan baik *software* maupun *hardware*. *Study literature* adalah tahapan awal untuk menganalisa dengan menggunakan teori-teori maupun penelitian yang mendukung penyelesaian kasus.

2.4 Simulasi Kasus

Simulasi kasus dilakukan berdasarkan skenario serangan *MITM Based Evil Twin* yang dilakukan disalah satu area *hotspot*, dalam kasus ini pelaku penyerangan *Evil Twin* membuat konfigurasi *gateway* yang berbeda dengan *IP gateway* dari *router AP* yang sah, sehingga proses investigasi tidak dapat dilakukan dari sisi *administrator*. Proses investigasi dibutuhkan suatu pendekatan berbasis *wired* atau *user* yang diimplementasikan dengan metode *Live Forensik*, untuk menganalisa data dari sistem yang berjalan.

Pada simulasi kasus adapun beberapa *tools* yang Akan digunakan dalam proses investigasi baik *Hardware* maupun *Software*. Untuk lebih jelasnya dapat dilihat pada Tabel 1.

Tabel 1 Kebutuhan Perangkat

No	Software	Hardware
1	OS kali linux	2 unit notebook
2	Os Windows 64 bit	2 unit wifi adaptor
3	Chellam	
4	Xarp, Wireshark	
5	Acrlyric-wifi	
6	Ettercap	
7	Wifipumpkin	

Pada skenario ini pelaku akan menggunakan AP palsu untuk menjerat para korban dan setelah korban terhubung ke dalam AP palsu yang dibuat dengan sengaja. Dengan demikian pelaku akan dengan mudah melakukan serangan *MITM* untuk mendapatkan informasi rahasia yang dimiliki korban. Dapat dilihat pada Gambar 2 Skenario *MITM Based Evil twin*.



Gambar 2. Skenario *MITM Based Evil twin*

Pola serangan yang digunakan pelaku adalah dengan melakukan konfigurasi AP palsu yang menggunakan SSID yang mirip dengan salah satu SSID target di sekitar *area Wifi*. Pada kasus ini pelaku menggunakan AP palsu dengan SSID "Pusfid" sebagai sarana untuk melakukan penyerangan. AP palsu dikonfigurasi dengan menggabungkan beberapa metode *MITM*, berfungsi untuk memanipulasi *traffik* ketika korban terhubung ke AP palsu tersebut, maka secara otomatis segala aktifitas para korban akan dilakukan proses *snifing* dan kemudian tersimpan sebagai *file log*.

3. Analisa Dan Hasil Investigasi Forensik

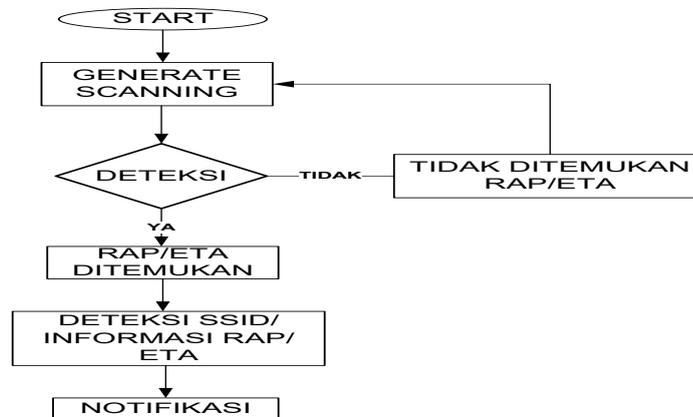
Tahapan investigasi dan hasil dilakukan berdasarkan proses analisa forensik, untuk menemukan data-data terkait barang bukti *digital* pada kasus *MITM Based Evil Twin Attack*. Untuk lebih jelas dapat dilihat pada Gambar 1.

3.1 Detection /Deteksi

Detection adalah salah tahapan awal, dimana investigator melakukan proses *scanning* untuk menemukan adanya kemungkinan AP palsu di suatu area publik. Skenario pada kasus ini peneliti melakukan aktivitas *scanning* dengan memanfaatkan sebuah aplikasi berbasis *windows* yaitu *Chellam*, aplikasi ini berfungsi untuk mendeteksi serangan *Evil Twin* melalui sinyal *beacon* dan *probe request* yang dipancarkan oleh AP palsu. Pada umumnya *Evil Twin* memanfaatkan fitur *Airbase-ng*, yang mana merupakan salah satu aplikasi berbasis *linux*. *Airbase-ng* memanfaatkan mode *monitor* untuk mendeteksi dan memancarkan sinyal *Wifi* atau AP yang digabungkan dengan beberapa metode *IP table* dan *gateway* dari modem *CDMA/GSM* maupun AP legal, agar dapat tetap terhubung ke *Internet*.

Aplikasi *Chellam* melakukan proses *scanning* dengan menerima sinyal *beacon* dari AP palsu. Proses lebih lanjut dilakukan dengan Menganalisa atribut maupun informasi yang mencurigakan maka aplikasi dengan otomatis mengirimkan notifikasi ke *desktop* dan jika hasil *scanning* tidak ditemukan

adanya serangan *Evil Twin*, maka aplikasi *Chellam* akan terus melakukan *generate scanning* hingga ditemukan kemungkinan adanya serangan *Evil Twin*. untuk lebih jelasnya dapat dilihat pada Gambar 3.



Gambar 3. Proses Detect *Chellam*

Scanning dilakukan dalam jangkauan 100 m dari lokasi publik area. Hasil *scanning* ditemukan pada beberapa AP yang sedang aktif antara lain yaitu, FTIUII, Pascasarjana, INFDOSEN, FTI UIINET dan PUSFI. Hasil pada proses *scanning* pada area tersebut ditemukan adanya ancaman AP palsu dengan SSID “PUSFID”. Sesuai yang ditunjukkan pada Gambar 4.



Gambar 4. Notifikasi *Chellam*

Tahapan selanjutnya, setelah ditemukan notifikasi adanya ancaman AP palsu. Proses *scanning* lebih lanjut akan dilakukan dengan tujuan untuk mengumpulkan informasi detail dari AP palsu tersebut. untuk lebih jelasnya dapat dilihat pada Gambar 5.

PUSFID	E4:8D:8C:CA:80:C0
PUSFID	F4:F2:6D:1C:76:15
Routerboard.com	Infrastructure -74
TP-LINK TECHNOLOGIES CO.,LTD.	Infrastructure -33
2412000	1
2447000	8

Gambar 5. Detail Analisa *WIFI*

3.2 Collection

Proses *collection* merupakan proses pengumpulan data dari serangan *Evil Twin* dan *MITM*, Pada hasil deteksi *Evil Twin Attack* ditemukan adanya notifikasi serangan *Evil Twin* dan juga informasi AP palsu dari proses *scanning* sebelumnya. Proses Tahapan *collection* pada serangan *MITM* dilakukan dengan menerapkan pendekatan *User side*, di mana investigator akan masuk dengan sengaja ke dalam jangkauan *Evil Twin* dan kemudian melakukan analisa serangan dari sudut pandang *user*. Adapun *tools* yang akan digunakan untuk mengumpulkan informasi serangan *MITM*, yaitu dengan menggunakan *tools* Wireshark untuk melakukan proses *capturing Network Trafik*. Proses *capturing* akan dilakuakn selama beberapa menit selanjutnya disimpan ke dalam bentuk *file* Pcap.

3.3 Akuisisi Data Serangan

Tahapan Akuisisi serangan dilakukan dengan menganalisa data maupun informasi yang ditemukan dalam tahapan pengkoleksian/ *Collection sebelumnya*. Proses akuisisi data serangan

ILKOM Jurnal Ilmiah Volume 9 Nomor 1 April 2017

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*. Hasil analisa tabel *hierarki* terdapat 3 objek yang dapat dijadikan sebagai bahan analisa yaitu *port HTTP*, *port ARP* dan *Port presentasi media*. Untuk lebih jelasnya dapat dilihat yang ditunjukkan pada Gambar 6.

Hypertext Transfer Protocol	0.7	48	66.1	815223	5426	24	9146	60
Portable Network Graphics	0.0	1	0.4	4741	31	1	4848	32
Media Type	0.0	1	58.9	726111	4833	1	726235	4834
Line-based text data	0.3	21	3.2	38917	259	21	41503	276
JPEG File Interchange Format	0.0	1	2.7	33382	222	1	33491	222
Internet Group Management Protocol	0.3	23	0.0	368	2	23	368	2
Internet Control Message Protocol	0.2	11	0.1	1599	10	11	1599	10
Address Resolution Protocol	72.1	5120	11.6	143360	954	5120	143360	954

Gambar 6. Wireshark Hierarki Modul

Gambar 7 menunjukkan adanya kegiatan *ARP broadcast* dari *MAC address tp_link/ source* 1c: 76:15 dengan *IP* 10.0.0.1 mencoba menghubungi *MAC address destination azurewav* 79:5a:5c dengan *IP* 10.0.0.20.

1936	395.587549	Tp-LinkT_89:7a:e5	Tp-LinkT_1c:76:15	ARP	42 Who has 10.0.0.1? Tell 10.0.0.20
1937	395.647628	Tp-LinkT_1c:76:15	Tp-LinkT_89:7a:e5	ARP	42 10.0.0.1 is at f4:f2:6d:1c:76:15

Gambar 7. Port 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. 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*. Hasil yang ditemukan diperlihatkan pada Gambar 8.

IP Korban : 10.0.0.20					
1994	405.519403	10.0.0.20	104.28.18.80	HTTP	561 GET / HTTP/1.1
2003	405.567174	104.28.18.80	10.0.0.20	HTTP	1209 HTTP/1.1 200 OK (text/html)
2006	405.698305	10.0.0.20	104.28.18.80	HTTP	518 GET /screen.css HTTP/1.1
2040	405.821237	104.28.18.80	10.0.0.20	HTTP	191 HTTP/1.1 200 OK (text/css)
2131	406.480182	104.28.18.80	10.0.0.20	HTTP	715 HTTP/1.1 200 OK (PNG)
2158	406.514250	104.28.18.80	10.0.0.20	HTTP	796 HTTP/1.1 200 OK (JPEG JFIF image)
2171	406.753159	10.0.0.20	104.28.18.80	HTTP	552 GET /ga/images/jv0_oracle.gif HTTP/1.1
4517	822.724909	10.0.0.20	104.28.18.80	HTTP	583 GET /java-update.exe HTTP/1.1
5353	828.049533	104.28.18.80	10.0.0.20	HTTP	1285 HTTP/1.1 200 OK (application/octet-stream)
Website IP : 10.28.18.80					

Gambar 8. Http Filter

Analisa *port HTTP*, untuk lebih jelasnya dapat dilihat pada Gambar 9, dari hasil analisa menunjukkan adanya kegiatan yang mencurigakan di mana *Host* yang sebenarnya dari *IP* 104.28.18.80 adalah (<http://www.mangaku.web.id>).

Wireshark - Follow TCP Stream (tcp.stream eq 42) - mitm analisa	
GET /ga/images/jv0_sidebar_bg.gif HTTP/1.1	
Host: mangaku.web.id	
Connection: keep-alive	
Cache-Control: max-age=0	

Gambar 9. Port Http Analisis

Proses analisa temuan *file* dilakukan menggunakan *tool Network Miner*. Berdasarkan hasil analisa ditemukan tiga jenis *file*, yang diduga merupakan *file* yang sengaja dibuat untuk menjebak para korban sesuai yang ditunjukkan pada poin-poin pada Gambar 10.

ILKOM Jurnal Ilmiah Volume 9 Nomor 1 April 2017

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 dibelokkan ke situs yang sengaja dibuat. Keterangan no 2 terdapat dua buah file yang berekstensi *Png* dan *Jpg*. Selanjutnya pada keterangan no 3 ditemukan adanya sebuah file berekstensi *exe*.

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.

Source host	S. port	Destination host	D. port	Protocol	Filename	Extension
26.96.63.180 [wpad.BUSEID] [noipmhsblefo.BUSEID] [a	TCP 80	10.0.0.20 [WIN-OPEN2N2K6V6] (Windows)	TCP 61430	HttpGetNormal	wpad.dat.html	html
104.28.18.80 [mangaku.web.id]	TCP 80	10.0.0.20 [WIN-OPFN2N2K6V6] (Windows)	TCP 61431	HttpGetNormal	index.html	html 1
104.28.18.80 [mangaku.web.id]	TCP 80	10.0.0.20 [WIN-OPFN2N2K6V6] (Windows)	TCP 61432	HttpGetNormal	screen.css	css
104.28.18.80 [mangaku.web.id]	TCP 80	10.0.0.20 [WIN-OPFN2N2K6V6] (Windows)	TCP 61438	HttpGetNormal	iv0d_a.png	png 2
104.28.18.80 [mangaku.web.id]	TCP 80	10.0.0.20 [WIN-OPFN2N2K6V6] (Windows)	TCP 61436	HttpGetNormal	iv0h.jpg	jpg
104.28.18.80 [mangaku.web.id]	TCP 80	10.0.0.20 [WIN-OPFN2N2K6V6] (Windows)	TCP 62556	HttpGetNormal	java-update.exe	exe 3

Gambar 10. Network Miner File Analisis

3.4 Analisis

Berdasarkan hasil analisa yang dilakukan dalam kasus *MITM Based Evil Twin Attack* yang dilakukan dengan menggunakan metode *Live Forensik* dan pendekatan dari sisi *user*. Ditemukan beberapa petunjuk ataupun temuan – temuan yang dapat dijadikan informasi yaitu berupa *IP address*, *MAC address* pelaku dan beberapa file yang mencurigakan seperti file *html*, *css*, *jpg* dan *png*.

Bukti *digital* yang ditemukan dalam serangan *Man In The Middle*, dilakukan setelah menerima notifikasi adanya serangan *Evil Twin*, kemudian investigator dengan sengaja masuk ke dalam jangkauan serangan *Evil Twin*, untuk mendeteksi adanya serangan *MITM* dengan cara melakukan *capturing* trafik.

Proses analisa hirarki, ditemukan dua objek yang dapat dianalisa lebih lanjut, karena memiliki tingkat presentasi aktivitas yang cukup tinggi, Seperti yang ditunjukkan pada Gambar 7 sebelumnya, yaitu *port ARP* dan *Port HTTP*. Proses analisa *ARP Attack* dilakukan dengan menggunakan modul dan *comand-comand* yang terdapat pada *wireshark* dapat dilihat pada Gambar 8.

Proses analisa *Port HTTP* dilakukan untuk mengidentifikasi aktivitas yang mencurigakan. Dari hasil analisa filterisasi *port HTTP* ditemukan *IP* 10.0.0.20 melakukan *request* ke *IP* 104.28.18.80, kemudian mengakses situs *http/get java-update.exe*. Gambar 9 menunjukkan kegiatan ilegal di mana pelaku mencoba melakukan *redirect* ke situs *Web* yang sengaja dibuat, di mana *host* yang sebenarnya adalah *http://www.mangaku.web.id*, untuk menganalisa kemungkinan adanya penyusupan file yang mencurigakan, analisa lebih lanjut dilakukan menggunakan *Network Miner*. Hasil pengamatan ditujukan pada Gambar 10, ditemukannya beberapa file mencurigakan seperti dua buah file *images* dan satu file berextensi *exe*.

3.5 Laporan

Laporan disusun berdasarkan hasil dari pengujian dan investigasi Forensik terhadap kasus serangan *Man In The Middle Attack Based Evil Twin*. Berdasarkan hasil analisa sebelumnya ditemukan beberapa informasi yang dapat dijadikan sebagai bukti *digital*. Data yang diperoleh didapatkan hasil proses tahapan analisa *Wifi scanning* ditujukan pada Tabel 2.

Tabel 2. Hasil 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

Hasil laporan serangan *MITM*, diperoleh dari tahapan analisa *network* trafik yang dilakukan di dalam jaringan *Evil Twin*, sesuai yang di tunjukkan pada Tabel 3.

Tabel 3 Hasil analisa *File Pcap*

No	Time	Source	Destination	Protocol	Length	info
<i>ARP PORT ANALYSIS</i>						
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
<i>http PORT ANALYSIS</i>						
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
<i>FILE INDETIFICATION ANALYSIS</i>						
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)

4. Kesimpulan

Berdasarkan Analisa yang didapatkan dari proses hasil dan investigasi forensik, maka pada penelitian studi dan analisa Forensik *digital* pada kasus serangan *Evil Twin Based MITM*. Dapat ditarik kesimpulan bahwa barang bukti *digital* dari serangan *Evil Twin AP* dapat diketahui dengan cara menganalisa atribut-atribut dari AP tersebut. Berikut beberapa informasi yang dapat dijadikan sebagai perbandingan yaitu *SSID*, *Mac Kode Vendor*, kekuatan Sinyal, *Authentication*, *Frequency* dan *Channel*.

Barang bukti yang ditemukan dari serangan *MITM*, dilakukan dengan menggunakan metode *sniffing* pada jaringan *Wifi*, dengan memanfaatkan modul-modul maupun filterisasi pada *tool* pada Wireshark. Proses dalam tahapan analisa dan pengumpulan barang bukti dilakukan dengan menerapkan metode *Live Forensik*. hal ini dikarenakan pengumpulan barang bukti dilakukan dalam sistem yang sedang berjalan, selain itu pendekatan *user side* cukup efektif dalam proses pengidentifikasian aktifitas serangan *Evil Twin Based MITM*.

Proses investigasi dilakukan dengan cara masuk ke dalam jangkauan *Evil Twin* dan sengaja menjadi korban, dengan tujuan melakukan proses dengan tujuan melakukan *capturing* trafik untuk mendapatkan informasi lebih lanjut tentang kemungkinan terjadinya aktivitas ilegal yang dilakukan oleh pelaku.

Daftar Pustaka

- [1] Anmulwar, Sweta, Srivastava S., Shrinivas P., Mahajan, Anil Kumar Gupta AK., Kumar V. 2014. Rogue Access Point Detection Methods: A Review." International Conference on Information Communication and Embedded Systems. (ICICES2014) (978):1–6.
- [2] Chhabra, Singh G. 2015. Distributed Network Forensics Framework : A Systematic Review. International Journal of Computer Applications (IJCA) 119(19):31–35.
- [3] Lanze, Fabian, Panchenko A., Ignacio AK., Thomas Engel. 2015. Hacker's Toolbox: Detecting Software-Based 802.11 Evil Twin Access Points. 2th Annual IEEE Consumer Communications and Networking Conference. (CCNC2015) 225–32.

- [4] Nakhila, Omar, Dondyk E., Faisal A., Cliff Zou. 2015. User-Side Wi-Fi Evil Twin Attack Detection Using SSL/TCP Protocols. IEEE Consumer Communications and Networking Conference. (CCNC 2015) 239–44.
- [5] Nanavare, Vibhawari V. 2016. Robust and Effective Evil Twin Access Point. Annual IEEE Consumer Communications and Networking Conference. (CCNC2015) 9074–84.
- [6] Rahman, Shuaibur, M. N. A. Khan. 2015. Review of Live Forensic Analysis Techniques. International Journal of Hybrid Information Technology 8(2):379–88.
- [7] Syngress. 2002. Scene of the Cybercrime: Computer Forensics Handbook: Computer Forensics Handbook.