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

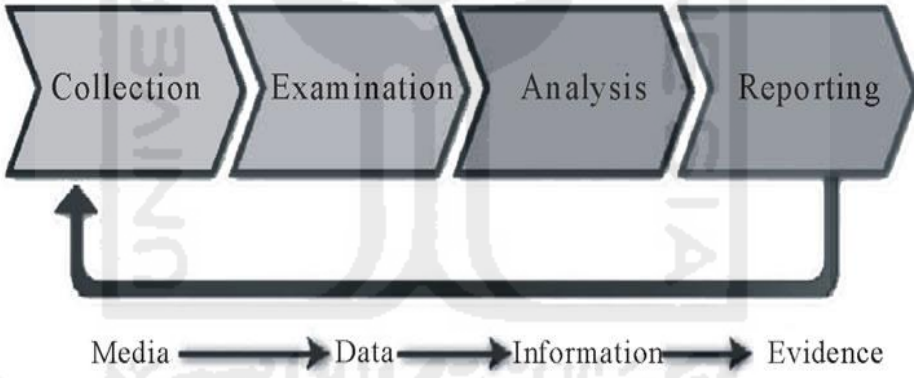
Forensik merupakan salah satu cabang bidang forensik paling muda diantara beberapa bidang forensik lainnya, *digital* forensik merupakan salah satu cabang ilmu forensik yang berhubungan dengan bukti hukum yang ditemukan dalam komputer maupun media penyimpanan secara *digital, Digital* forensik ini dikenal 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:

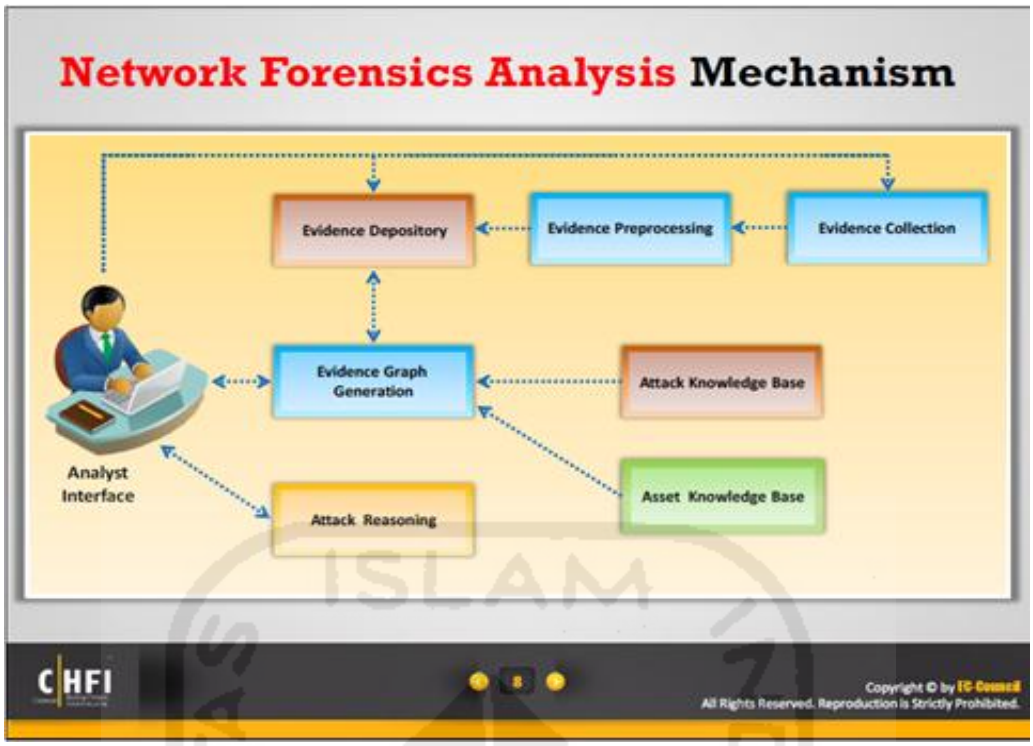
- Pengumpulan(*collection*) : merupakan metode awal dalam melakukan proses investigasi, dengan cara mengumpulkan data-data yang dianggap terkait dengan kasus yang terjadi.
- Pemeliharaan (*examination*) : merupakan kegiatan pengumpulan atau pemeliharaan barang bukti yang akan digunakan sebagai analisa.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

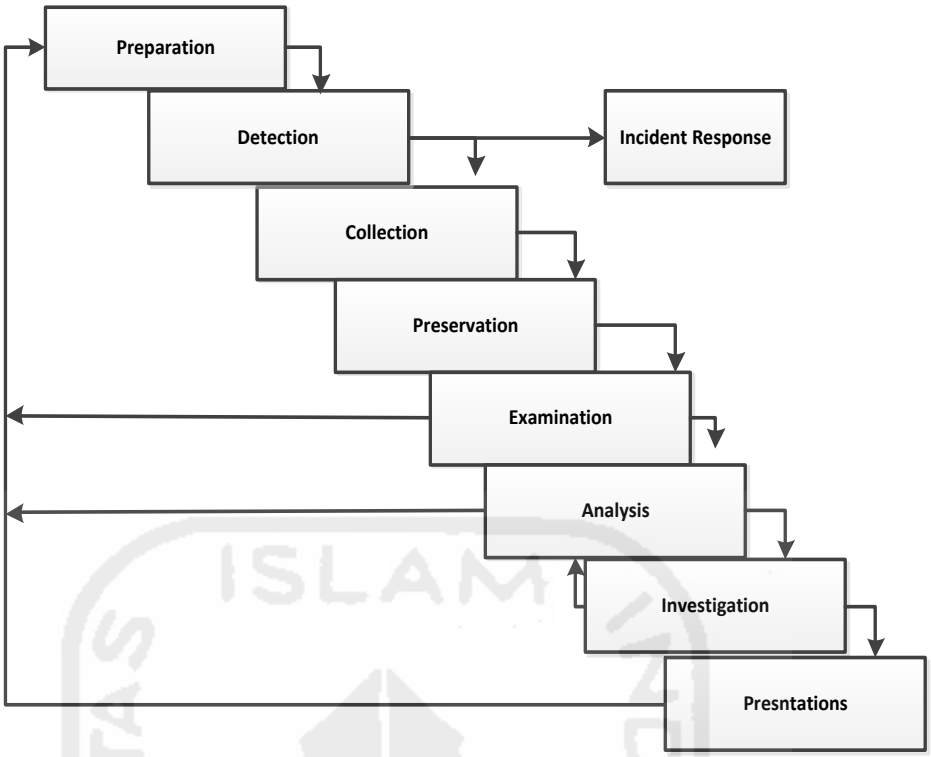
Live forensik merupakan salah satu teknik dalam investigasi digital, pada dasarnya memiliki kesamaan pada teknik forensik tradisonal dalam hal metode yang dipakai yaitu identifikasi penyimpanan, analisis, dan presentasi, hanya hanya saja *live* forensik merupakan respon dari kekurangan teknik forensik 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*

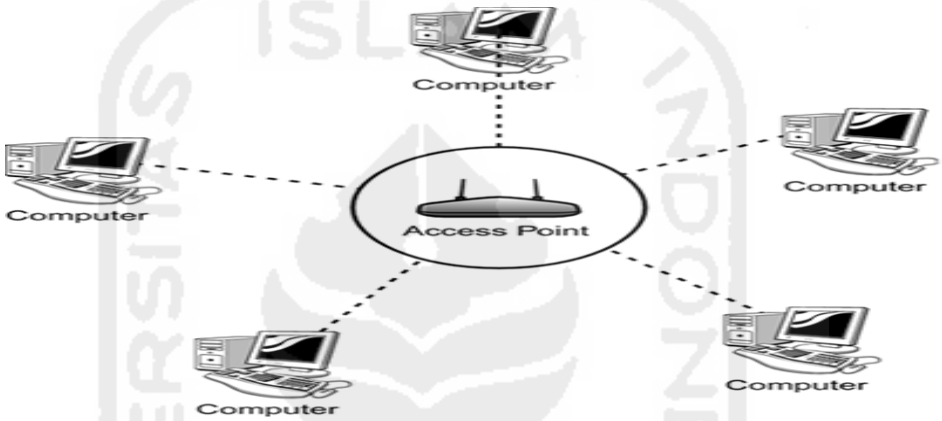
2.8 Wireless Lan

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)

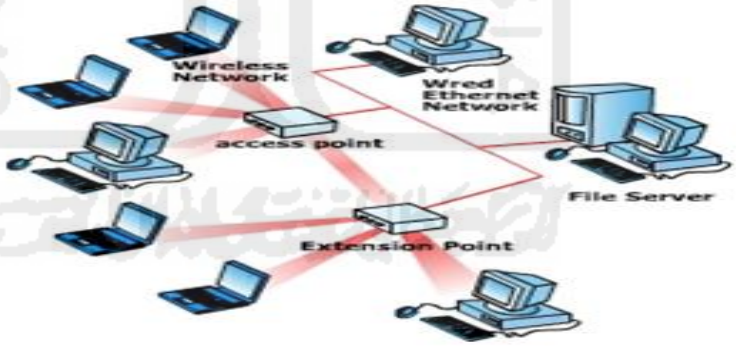
Pada wlan, alat untuk data disebut dengan AP dan terhubung dengan jaringan LAN melalui kabel Fungsi dari access poin adalah mengirim dan menerima data, sebagai buffer data antara wlan dengan wired lan, mengkonversi sinyal frekuensi radio (rf) menjadi sinyal digital yang akan disalurkan melalui kabel 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

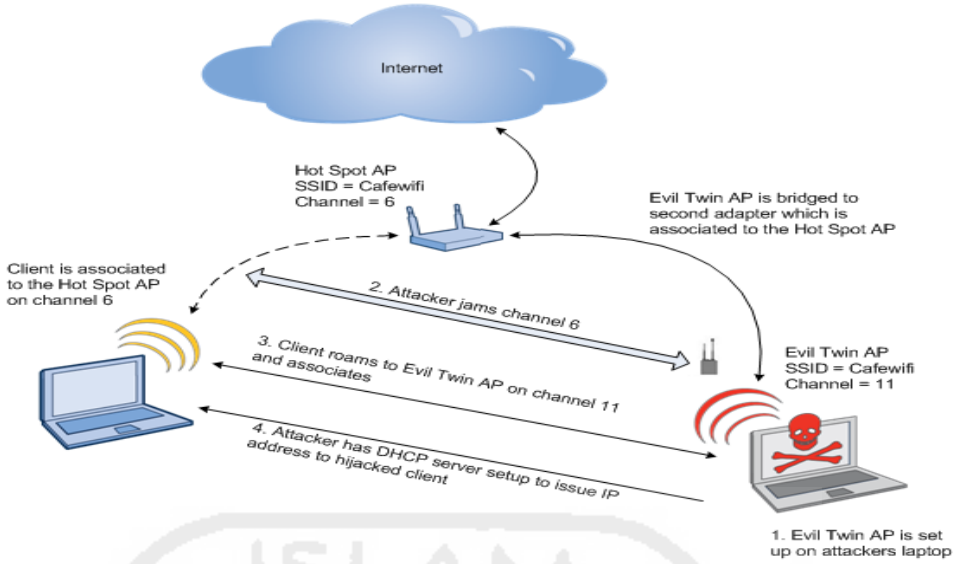
Spesifikasi	Kecepatan	Frekuensi Band	Cocok dengan
802.11b	11 Mb/s	~2.4 GHz	b
802.11a	54 Mb/s	~2.4 GHz	a
802.11g	54 Mb/s	~2.4 GHz	b, g
802.11n	100 Mb/s	~5 GHz	b, g, n

Tabel 2. 1 Spesifikasi Wi-Fi

Sumber : ultramelta.files.wordpress.com.

2.10 *Evil twin*

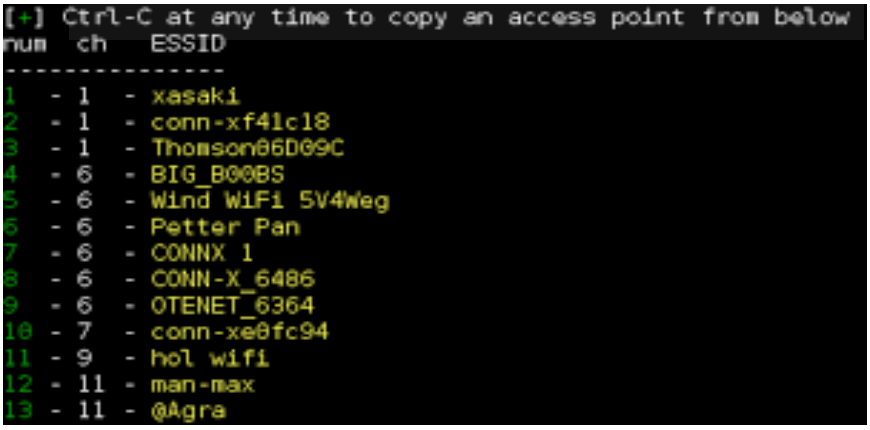
Evil twin merupakan salah satu jenis serangan *Rogue* AP atau *Wifi* phising, *Evil Twin attack* merupakan salah satu jenis serangan yang sangat berbahaya khusus pada para pengguna *Wifi* hot-spot, dalam melakukan aktifitas penyeranganya *Evil Twin* akan membuat sebuah AP phising, dimana di AP tersebut 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*.



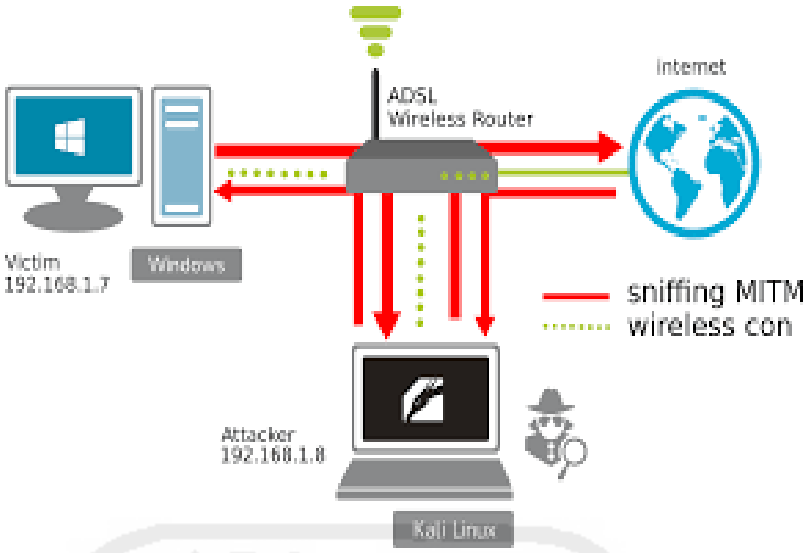
Gambar 2. 9 *Wifi*phisher

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

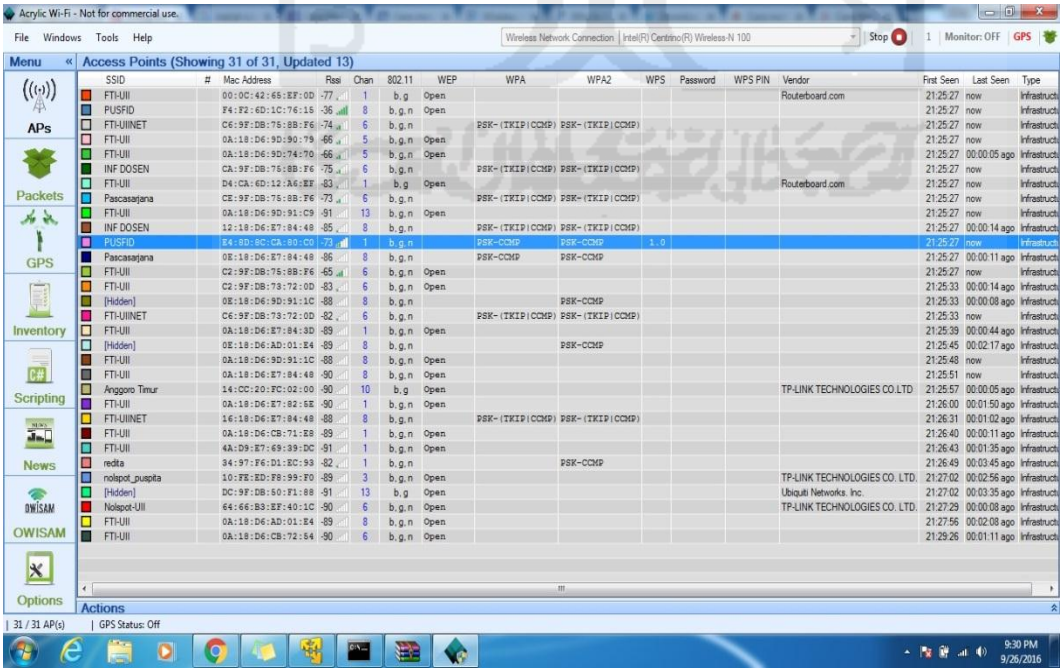
Man in the middle (MITM) merupakan salah satu jenis serangan yang berbahaya karena serangan ini dapat terjadi pada berbagai media informasi seperti *website*, *handphone*, dan bahkan Surat. Oleh karena itu, artikel ini akan membahas tentang *MITM attack* terlepas dari apapun dan dimanapun implementasinya 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.

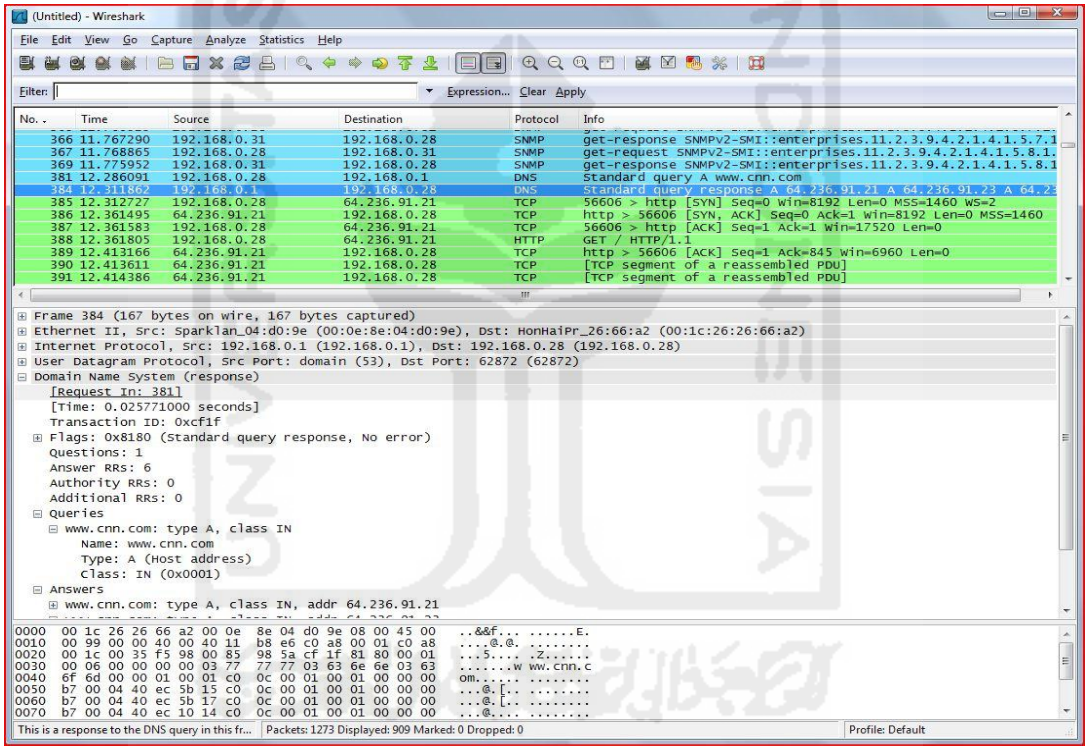


Gambar 2. 12 Acrylic-wi-fi

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.

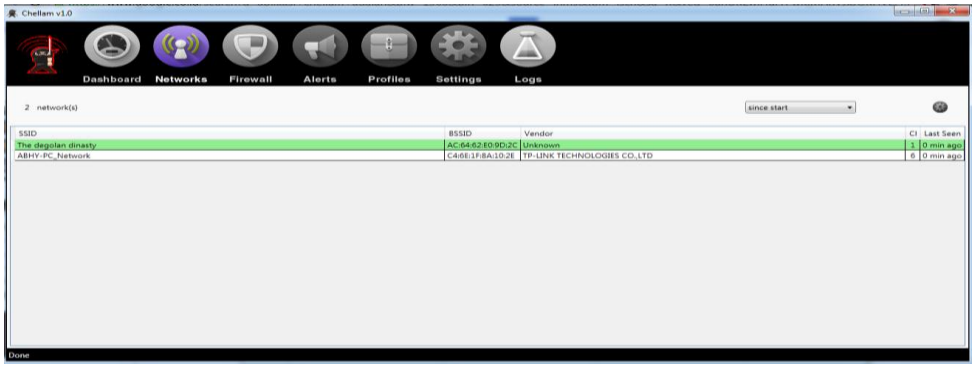
Selain itu *Wireshark* dapat memantau paket -paket data yang diterima dari internet *Wireshark* ini bekerja pada *layer* aplikasi Yaitu layer terakhir dari *OSI layer*. Dengan menggunakan *protocol* di *layer application http, ftp, telnet, SMTP, dns* kita dengan mudah memonitoring jaringan yang ada, 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*