FORENSIK *E-MAIL*

Kundang Karsono
Fakultas Ilmu Komputer Universitas Esa Unggul, Jakarta
Jln. Arjuna Utara Tol Tomang Kebun Jeruk, Jakarta 11510
Joko.dewanto@esaunggul.ac.id

Abstrak

Forensik yang identik dengan tindakan kriminal, sampai saat ini hanya sebatas identifikasi, proses, dan analisa pada bagian umum. Untuk kejahatan komputer di Indonesia, forensik di bidang komputer biasanya dilakukan tanpa melihat apa isi di dalam komputer. Justru lebih banyak bukti jika forensik di dalam komputer itu terindetifikasi. Metode yang umum digunakan untuk forensik pada komputer ada dua, yaitu search and seizure dan pencarian informasi (*discovery information*). Metode ini juga dikembangkan dengan manajemen bukti, antara lain *the change of custody* dan *rules of evidence*. Penekanan metode yang digunakan serta apa saja yag perlu dilakukan, akan lebih banyak dibahas dari pada manajemen bukti. Bukti di sini bukan hanya berupa barang secara fisik, tetapi juga dapat non-fisik. Studi ilmiah ini juga mengambil beberapa acuan forensik dari perusahaan keamanan komputer dan Hongkong *Police Force* , sehingga diharapkan akan berguna bagi pihak yang berwenang untuk menyidik sesuatu yang berkaitan dengan kejahatan komputer.

Kata kunci : Komputer, Forensik, Bukti

Pendahuluan

Internet dan teknologi informasi meningkatkan permasalahan kejahatan dunia maya (*cyber-crime*) adalah bentuk ancaman baru yang belum pernah ada sebelumnya pada masyarakat dunia. *Hacking*, *cracking*, *defancing*, *sniffing*, *carding*, *phishing*, *spamming*, *scam* adalah sederet kejahatan internet yang cukup berbahaya dan telah menimbulkan kerugian nyata pada banyak pihak.

Memerangi kejahatan internet telah menjadi porsi utama bagi agen-agen penegak hukum dan intelejen baik nasional maupun internasional, tak terkecuali praktisi-praktisi bisnis, *merchant*, para pelanggan, sampai kepada *end-user*. Pada kebanyakan kasus, kejahatan internet dimulai dengan mengeksploitasi *host-host* dan jaringan komputer. Oleh karena itu, para penipu dan *intruder* datang melintasi jaringan, terutama sekali jaringan-jaringan yang berbasiskan protokol TCP/IP.

Mengingat besarnya resiko kerugian yang bisa ditimbulkan dan semakin menjamurnya praktik-praktik kejahatan ini, maka tuntutan *Internet forensics* menjadi sesuatu yang tidak bisa ditawar lagi. Kegiatan forensik merupakan kegiatan yang diakui atau dilegalkan secara hukum dalam memperoleh bukti-bukti untuk menggambarkan suatu peristiwa atau kejadian pada tempat kejadian perkara. Karena dilegalkan secara hukum, maka seseorang yang melakukan kegiatan forensik harus mempunyai kewenangan yang diakui oleh hukum yang berlaku di wilayah tersebut.

Secara umum tujuan kegiatan forensik adalah untuk menemukan jawaban dari pertanyaan-pertanyan yang muncul dalam proses penyidikan suatu peristiwa atau kejadian.

Penerapan komputer forensik pada e-mail meliputi :

1. Untuk mengungkap para pelaku kejahatan-kejahatan internet dan mengadili mereka sesuai hukum yang berlaku.
2. Agar pembaca dapat mencegah atau terhindar dari kejahatan-kejahatan internet yang menggunakan e-mail.
3. Memberikan informasi kepada para pembaca maupun profesional IT untuk mengusut dan mempertahankan diri dari kejahatan internet yang menggunakan e-mail, Agar dapat lebih meningkatkan lagi sistem keamanan *e-mail server* mereka dan juga mengingatkan kepada user mereka untuk selalu mewaspadai terhadap e-mail-e-mail yang masuk ke inbox mereka kalo perlu di laporkan kepada admin mereka.

Forensik

Kata Forensik (berasal dari bahasa Yunani *Forensis* yang berarti "debat" atau "perdebatan") adalah bidang ilmu pengetahuan yang digunakan untuk membantu proses penegakan keadilan melalui proses penerapan ilmu atau sains. Dalam kelompok ilmu-ilmu forensik ini dikenal antara lain ilmu fisika forensik, ilmu kimia forensik, ilmu psikologi forensik, ilmu kedokteran forensik, ilmu toksikologi forensik, ilmu psikiatri forensik, komputer forensik dan sebagainya.

Empat Elemen Kunci Forensik Komputer

Adanya empat elemen kunci forensik adalah sebagai berikut :

1. Identifikasi dari Bukti Digital Merupakan tahapan paling awal forensik dalam teknologi informasi. Pada tahapan ini dilakukan identifikasi di mana bukti itu berada, di mana bukti itu disimpan, dan bagaimana penyimpanannya untuk mempermudah tahapan selanjutnya. Banyak pihak yang mempercayai bahwa forensik di bidang teknologi informasi itu merupakan forensik pada komputer. Sebenarnya forensik bidang teknologi informasi sangat luas, bisa pada telepon seluler, kamera digital, smart cards, dan sebagainya. Memang banyak kasus kejahatan di bidang teknologi informasi itu berbasiskan komputer. Tetapi perlu diingat, bahwa teknologi informasi tidak hanya komputer/internet.
2. Penyimpanan Bukti Digital Termasuk tahapan yang paling kritis dalam forensik. Pada tahapan ini, bukti digital dapat saja hilang karena penyimpanannya yang kurang baik. Penyimpanan ini lebih menekankan bahwa bukti digital pada saat ditemukan akan tetap tidak berubah baik bentuk, isi, makna, dan sebagainya dalam jangka waktu yang lama. Ini adalah konsep ideal dari penyimpanan bukti digital.
3. Analisa Bukti Digital Pengambilan, pemrosesan, dan interpretasi dari bukti digital merupakan bagian penting dalam analisa bukti digital. Setelah diambil dari tempat asalnya, bukti tersebut harus diproses sebelum diberikan kepada pihak lain yang membutuhkan. Tentunya pemrosesan di sini memerlukan beberapa skema tergantung dari masing-masing kasus yang dihadapi.
4. Presentasi Bukti Digital Adalah proses persidangan di mana bukti digital akan diuji otentifikasi dan korelasi dengan kasus yang ada. Presentasi di sini berupa penunjukan bukti digital yang berhubungan dengan kasus yang disidangkan. Karena proses penyidikan sampai dengan proses persidangan memakan waktu yang cukup lama, maka sedapat mungkin bukti digital masih asli dan sama pada saat diidentifikasi oleh investigator untuk pertama kalinya. (Rodney McKemmish, *"What is Forensic Computing", Australian Institut of Criminology, Canberra, June 1999,*

(http://www.aic.gov.au/publications/tandi, 10 Desember 2009)).

Bukti Digital (Digital Evidence)

Bukti digital adalah informasi yang didapat dalam bentuk/format digital, Bukti digital ini bisa berupa bukti yang riil maupun abstrak (perlu diolah terlebih dahulu sebelum menjadi bukti yang riil). Beberapa contoh bukti digital antara lain :

a. *e-mail*, alamat *e-mail*
b. *Wordprocessor/spreadsheet files*
c. *source code* dari perangkat lunak
d. *Files* berbentuk image (.jpeg, .tif, dan sebagainya)
e. *Web browser bookmarks, cookies*
f. Kalender, *to-do list*
g. (feri sulianta 2008, p25).

Penyimpanan bukti digital *(Preserving Digital Evidence)*

Bentuk, isi, makna bukti digital hendaknya disimpan dalam tempat yang aman/*steril*. Untuk benar-benar memastikan tidak ada perubahan-perubahan, hal ini vital untuk diperhatikan. Karena sedikit perubahan saja dalam bukti digital, akan merubah juga hasil penyelidikan. Bukti digital secara alami bersifat sementara (*volatile*), sehingga keberadaannya jika tidak teliti akan sangat mudah sekali rusak, hilang, berubah, mengalami kecelakaan. Step pertama untuk menghindarkan dari kondisi-kondisi demikian adalah salah satunya dengan meng*copy* data secara *Bitstream Image* pada tempat yang sudah pasti aman.

Bitstream image adalah methode penyimpanan digital dengan mengkopi setiap bit demi bit dari data orisinil, termasuk File yang tersembunyi (*hidden files*), File temporer (temp file), File yang terfragmentasi (*fragmen file*), file yang belum ter-*ovverwrite*. Dengan kata lain, setiap biner digit demi digit terkopi secara utuh dalam media baru. Teknik pengkopian ini menggunakan teknik *Komputasi CRC.* Teknik ini umumnya diistilahkan dengan *Cloning Disk* atau *Ghosting*.

Software-software atau alat bantu yang dapat digunakan dalam aktivitas ini antara lain adalah:

a. *Safe Back*. Dipasarkan sejak tahun 1990 untuk penegakan Hukum dan Kepolisian. Digunakan oleh FBI dan Divisi Investigasi Kriminal IRS. Berguna untuk pemakaian partisi tunggal secara virtual dalam segala ukuran. File *Image* dapat ditransformasikan dalam format SCSI atau media storage magnetik lainnya.
b. *EnCase*. Seperti *SafeBack* yang merupakan program berbasis karakter, EnCase adalah program dengan fitur yang relatif mirip, dengan Interface GUI yang mudah dipakai oleh teknisi secara umum. Dapat dipakai dengan Multiple Platform seperti *Windows NT* atau Palm OS. Memiliki fasilitas dengan *Preview* Bukti, Pengkopian target, *Searching* dan *Analyzing.*
c. Pro Discover[5]. Aplikasi berbasis Windows yang didesain oleh tim *Technology Pathways forensics*. Memiliki kemampuan untuk me-*recover* file yang telah terhapus dari *space storage* yang longgar, mengalanalisis Windows 2000/NT *data stream* untuk data yang ter*hidden*,menganalisis data image yang diformat oleh kemampuan*dd UNIX* dan menghasilkan laporan kerja. (http://prayudi.wordpress.com/2007/03/31/komputer-forensik/ 02 februari 2010).

Analisa bukti digital *(Analizing Digital Evidence)*

Barang bukti setelah disimpan, perlu diproses ulang sebelum diserahkan pada pihak yang membutuhkan. Pada proses inilah skema yang diperlukan akan

fleksibel sesuai dengan kasus-kasus yang dihadapi. Barang bukti yang telah didapatkan perlu di*explore* kembali beberapa poin yang berhubungan dengan tindak pengusutan, antara lain:

1. Siapa yang telah melakukan.
2. Apa yang telah dilakukan (Ex. Penggunaan software apa),
3. Hasil proses apa yang dihasilkan.
4. Waktu melakukan.

Setiap bukti yang ditemukan, hendaknya kemudian dilist bukti-bukti potensial apa sajakah yang dapat didokumentasikan. Contoh kasus seperti kejahatan foto pornografi-anak ditemukan barang bukti gambar *a.jpg*, pada bukti ini akan dapat ditemukan data Nama *file*, tempat ditemukan, waktu pembuatan dan data properti yang lain. Selain itu perlu dicatat juga seperti *spaced* dari *storage*, format partisi dan yang berhubungan dengan alokasi lainnya

Tiap-tiap data yang ditemukan sebenarnya merupakan informasi yang belum diolah, sehingga keberadaannya memiliki sifat yang vital dalam kesempatan tertentu. Data yang dimaksud antara lain :

a. Alamat URL yang telah dikunjungi (dapat ditemukan pada *Web cache, History, temporary internet files*)
b. Pesan *e-mail* atau kumpulan alamat e-mail yang terdaftar (dapat ditemukan pada *e-mail server*)
c. Program *Word processing* atau format ekstensi yang dipakai (format yang sering dipakai adalah *.doc, .rtf, .wpd, .wps, .txt*)
d. Dokumen *spreedsheet* yang dipakai (yang sering dipakai adalah *.xls, .wgl, .xkl*)
e. Format gambar yang dipakai apabila ditemukan *(.jpg, .gif, .bmp, .tif* dan yang lainnya)
f. *Registry Windows* (apabila aplikasi)
g. Log Event viewers
h. Log Applications
i. *File print spool*
j. Dan file-file terkait lainnya.

Analisis kemungkinan juga dapat diperoleh dari motif/latar belakang yang ada sebelum didapatkan kesimpulan. Bahwa setiap sebab, tentu saja akan memiliki potensi besar untuk menghasilkan akibat yang relatif seragam. (www.prayudi.wordpress.com/2007/03/31/komputer-forensik/ 02

Subdivisi Komputer Forensik

Komputer Forensik

Komputer forensik yang juga dikenal dengan nama digital forensik, adalah salah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang ditemui pada komputer dan media penyimpanan dijital.

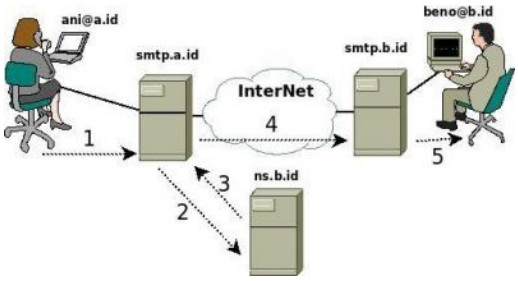
Tujuan dari komputer forensik ada-lah untuk menjabarkan keadaan kini dari suatu artefak *digital*. Istilah artefak *digital* bisa mencakup sebuah sistem komputer, media penyimpanan (seperti flash disk, hard disk, atau CD-ROM), sebuah dokumen elektronik (misalnya sebuah pesan e-mail atau gambar JPEG), atau bahkan sederetan paket yang berpindah dalam jaringan komputer. Penjelasan bisa sekedar "ada informasi apa disini?" sampai serinci "apa urutan peristiwa yang menyebabkan terjadinya situasi kini? ".(http://id.wikipedia.org/wiki/Komputer_forensik, 21 November 2009)

Computer Forensics itu sendiri dikenal dengan *Digital Forensics*, yaitu salah satu cabang ilmu forensik yang berkaitan dengan bukti-bukti legal tentang sebuah aksi kejahatan atau pelanggaran yang ditemui pada komputer dan media-media penyimpanan digital. (Rahmat rafiudin 2009, p2).

Internet Forensik

Internet Forensics adalah suatu usaha tentang bagaimana kita menelusuri

atau menginvestigasi sumber-sumber jahat internet dan sekaligus mempelajari bagaimana ini bisa terjadi. *Internet Forensics* merupakan bagian dari displin *Computer Forensics* yang menggunakan teknik-teknik komputasi lanjutan dan intuisi manusia untuk menemukan petunjuk-petunjuk tentang kejahatan-kejahatan berbasis internet.(Rahmat rafiudin 2009, p2).



Gambar 1
cara kerja email

Sistem Forensik

Sistem forensik adalah untuk mengetahui bagaimana keperluan sistem operasi untuk diimplementasikan pada *workstation* saja atau pada server.

Jaringan Komputer Forensik

Jaringan computer forensik adalah melihat serta memantau bagaimana layer berkomunikasi dalam diagram OSI (*Open System InterConnection*) tujuh lapis. (Feri sulianta 2008, p5).

Perbedaan Komputer Forensik Dan Internet Forensik

Computer Forensics mempelajari bagaimana komputer-komputer terlibat dalam sebuah aksi kejahatan, baik terhubung jaringan atau tidak. Adapun *Internet Forensics* mempelajari bagaimana jaringan internet termasuk komputer-komputer, layanan-layanan dan pengguna (user) didalamnya terlibat dalam sebuah aksi kejahatan. Aksi kejahatan disini dapat beragam bentuk, mulai dari penyerangan, mengeksploitasi layanan-layanan/program-program, penipuan, pelecehan, pencurian, perusakan, dan lain sebagainya yang menimbulkan kerugian bagi pihak lain. Jika *Computer Forensics* lebih banyak berurusan dengan aspek-aspek fisik dan data maka *Internet Forensics* lebih berkaitan dengan aspek-aspek jaringan dan layanan-layanan internet. Dilihat dari definisi-definisi diatas, jelas bahwa Internet Forensics merupakan bagian tak terpisahkan dari *Computer Forensics*. (Rahmat Rafiudin 2009, p2)

Header E-Mail

Definisi Header

Baris awal dari berita *e-mail* atau *news group* yang berisi informasi tentang berita, pengirim, perihal.
(http://www.total.or.id/info.php?kk=Header , 21 November 2009)

Setiap pesan e-mail akan memiliki apa yang dikenal dengan header, yang terdiri dari field-field. Setiap field dalam header memiliki nama dan nilai.

Nama-nama field dan nilai-nilai header merupakan karakter-karakter ASCII 7-bit. Nilai-nilai non ASCII akan direpresentasikan menggunakan kata-kata sandi. (Rahmat raifudin 2009,p9).

Field-Field Header

Sebuah header pesan e-mail setidaknya memuat field-field berikut ini :

1. ***From*** : Alamat e-mail pengirim (*sender*), dan terkadang juga nama pengirimnya.
2. ***To*** : Alamat (-alamat) e-mail penerima (*recepient*), terkadang juga nama-nama penerimanya
3. ***Subject*** : Ringkasan dari konten pesan.
4. ***Date*** : Informasi tanggal dan waktu setempat saat pesan ditulis.
5. *Field-field header* umum lainnya di antaranya :
   a. Bcc : *Blind carbon copy*.
   b. Cc : *Carbon copy.*
   c. Content-Type : Informasi tentang bagaimana pesan harus di

tampilkan, biasanya format MIME.

d. *In-Reply-To* : *Message-ID* dari pesan kemana akan membalas.
e. *Received* : Informasi *track* yang diproduksi oleh *server-server e-mail* yang telah menangani pesan ini.
f. *References* : Messages-ID dari pesan ke mana akan membalas, dan messages-id dari pesan ini, dan lain-lain.
g. *Reply To* : *Address* yang harus digunakan untuk membalas (*reply*) pesan ke pengirim (sender).
h. *X-Face* : Small icon.

Forensik *E-mail*

Definisi Forensik *E-mail*

Berdasarkan definisi Forensik dan e-mail, penulis menyimpulkan definisi Forensik e-mail sebagai "suatu tindakan pengamanan, pengecekkan, serta penelusuran terhadap email palsu, atau terhadap bukti-bukti kejahatan yang menggunakan e-mail.

Pemodelan Forensik E-mail

Model forensik melibatkan tiga komponen terangkai yang dikelola sedemikian rupa hingga menjadi sebuah tujuan akhir dengan segala kelayakan dan hasil yang berkualitas. Ketiga komponen tersebut adalah:

a. Manusia (*People*), diperlukan kualifikasi untuk mencapai manusia yang berkualitas. Memang mudah untuk belajar komputer forensik, tetapi untuk menjadi ahlinya, dibutuhkan lebih dari sekadar pengetahuan dan pengalaman.
b. Peralatan (*Equipment*), diperlukan sejumlah perangkat atau alat yang tepat untuk mendapatkan sejumlah bukti (*evidence*) yang dapat dipercaya dan bukan sekadar bukti palsu.
c. Aturan (*Protocol*), diperlukan dalam menggali, mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat. Dalam komponen aturan, diperlukan pemahaman yang baik dalam segi hukum dan etika, kalau perlu dalam menyelesaikan sebuah kasus perlu melibatkan peran konsultasi yang mencakup pengetahuan akan teknologi informasi dan ilmu hukum.

Hal yang di butuhkan untuk internet forensik

Tidak jauh berbeda dengan tuntutan-tuntutan komputer forensik seorang spesialis internet forensik perlu memiliki segudang informasi atau data untuk penyelidikan.

Data-data ini pada umumnya diperoleh dari catatan-catatan yang direkam oleh *host-host* dan *server-server* internet yang berhubungan, termasuk didalamnya data-data log.

Disamping ketersediaan informasi dan data yang memadai, spesialis forensik juga seringkali membutuhkan tool-tool pembantu yang mampu melakukan tugas-tugas ini secara lebih cepat dan pintar.

Analisis Forensik Email

Studi kasus

Ketika kita menerima suatu email ancaman, atau undangan palsu tentu kita merasa kaget dan langsung segera ingin melaporkan diri ke polisi karena merasa terancam. Tak jarang pemilik alamat email itu akhirnya berurusan dengan polisi dan persidangan. Tetapi tentu saja ini menimbulkan pertanyaan selanjutnya. Apakah dengan bukti salinan email ancaman dari seseorang, telah cukup untuk digunakan di pengadilan? Langkah-langkah apakah yang harus dilakukan sehingga bukti menjadi cukup untuk menyimpulkan email ancaman itu sebagai

suatu hal yang serius ?

Permasalahan menjadi lebih rumit karena beberapa hal. Pertama proses pengiriman email, kedua masalah penanganan bukti digital, ketiga masalah kesiapan pelaksanaan komputer forensik di Indonesia, baik dari sisi aparat ataupun peraturan. Tulisan ini akan mencoba membahas satu per satu masalah tersebut.

Sebetulnya ketika kita menerima sebuah email yang memiliki keterangan berasal dari suatu alamat email tertentu, belum tentu email tersebut hanya berasal dari orang yang bersangkutan. Ada beberapa kemungkinan yang menyebabkan penyelidik tidak boleh langsung memastikan bahwa email tersebut memang berasal dari si pemilik akun email tersebut. Pada dasarnya seorang penyidik, berdasarkan bukti yang ada harus memastikan apakah email tersebut dikirimkan memang benar oleh si pemilik akun tersebut, dan dari komputer tersebut dan pada waktu yang cocok. Tidak mudah memang, karena itu kita membutuhkan beberapa tools dan alikasi web untuk menganalisis.

Analisis Pemilihan Tools Untuk Pembuatan Email Palsu

Tabel 1
Perbandingan Pemilihan Tools Untuk Pembuatan Email Palsu

No	Nama tools	Kelebihan	Kekurangan	Sumber
1	Microsoft outlook	• Free • User friendly	• Harus ijin dengan smtp yang bersangkutan • Mempunyai *logs* file yang tercatat • Hanya berjalan di os *windows*	Microsoft outlook
2	Telnet	• Free • Tidak mempunyai logs	• Tidak user friendly • Menggunakan *cmd* • Terkadang *error* • Harus izin dengan smtp yang bersangkutan • Harus membuka banyak registry komputer • Hanya dapat mengirim dalam satu *mail server* yang sama	cmd
3	Topmail	• User friendly • Bisa mengirim ke semua email server • Tidak mempunyai logfile	• Tidak *free* • Hanya berjalan di OS Windows	www.iiprw.com

Berdasarkan analisa dari Tabel 1 *tools* yang akan di gunakan untuk membuat email palsu adalah topmail. Karena lebih mudah digunakan dan tidak mempunyai banyak kesulitan seperti *tools-tools* yang lainnya.

Analisis Pemilihan Web Sofware dan Web Untuk Forensik Email

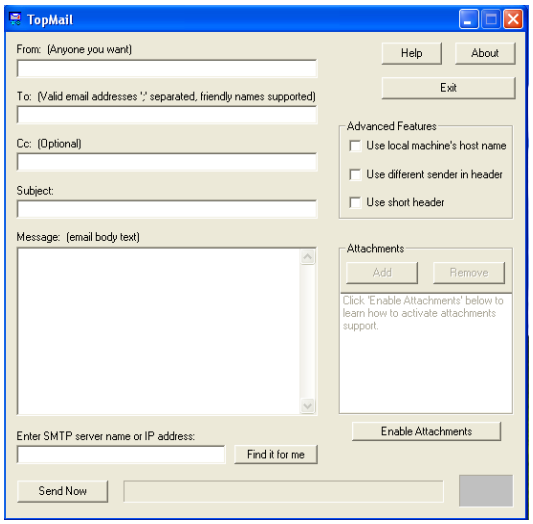
Tabel 2
Tabel Perbandingan Pemilihan Web dan Sofware Untuk Forensik

No	Nama web dan sofware	Kelebihan	Kekurangan	Sumber
1	Apnic, lacnic, ripe, arin.	• lisensi • dibagi perzona • mempunyai akses bebas ke semua daerah • *user friendly*	• hanya daerah kekuasannya saja	www.apnic.net www.lacnic.net www.ripe.net www.arin.net
2	Samspade	• semua zona	• tidak lisensi • terkadang tidak bisa mengetahui • tidak terpercaya	www.samspade.org
3	Ipnetinfo	• semua zona • simpel penggunaannya • sofware • bisa membaca header sekalian	• pembacaan header yang tidak sempurna • menghasilkan terlalu banyak ip • tetap melihat ke web lisensi • tidak mempunyai akses ke beberapa daerah • hanya jalan di OS windows	www.nirsoft.net
	Ip-adress tracer	• dapat melihat gambar lokasi sipengirim email palsu	• tidak user friendly • ada beberapa daerah yang tidak bisa di jangkau • bertujuan ke web lisensi	www.ip-adress.com

Berdasarkan analisa dari Tabel 2 sofware dan web yang akan di gunakan untuk forensik adalah *apnic, lacnic, ripe* dan *arin*. Karena lebih mempunyai akses yang lebih bebas dari yang lainnya juga lebih user friendly dengan yang lainnya.

Pembuatan Email

Berikut ini adalah tampilan dan cara-cara pembuatan email palsu meng-gunakan *software* topmail dari : (www.iiprw.com).

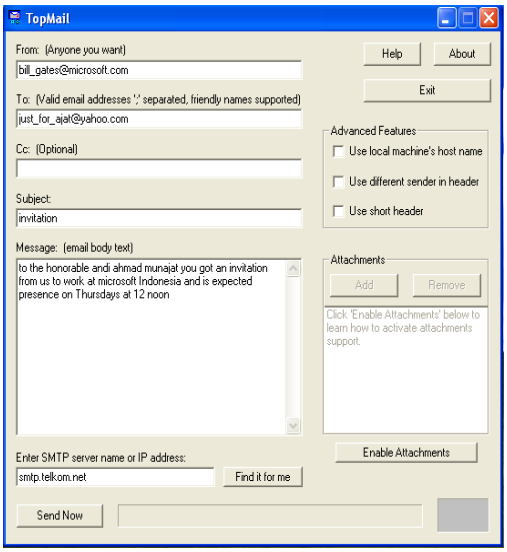


Gambar 1
Jendela TopMail

Selanjutnya penulis akan membuat email palsu dengan menggunakan akun orang pada aplikasi topmail tersebut :

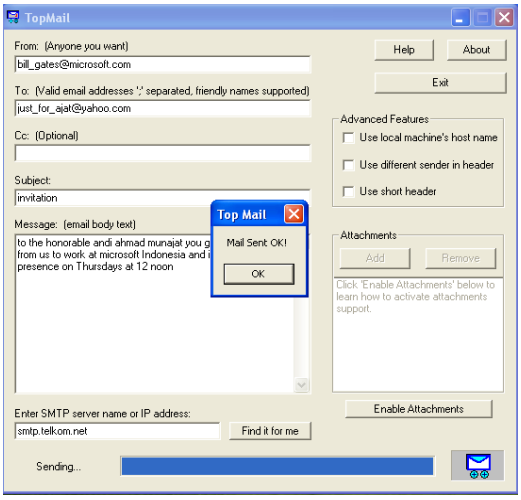
1. Pada bagian *From*, kita menuliskan alamat email yang kita suka, dalam hal ini penulis menggunakan alamat email bill_gates@microsoft.com yang dalam hal sebenarnya email tersebut belum tentu ada.
2. Pada bagian *To*, tuliskan alamat email yang kita tuju untuk kita kelabuhi.
3. Pada bagian *subject*, kita tuliskan subject yang kita inginkan dalam hal ini judul dari pesan email kita.
4. Pada bagian message, kita tuliskan pesan yang ingin kita buat untuk si penerima agar percaya dan terbujuk oleh pesan kita.
5. Pada bagian SMTP server, tuliskan email yang digunakan. Dalam hal ini tuliskan smtp.telkom.net.
6. Klik tombol *send now* jika semua hal tersebut sudah selesai dilakukan.

Berikut gambar dari langkah-langkah tersebut.



Gambar 2
cara pengiriman email palsu

Proses pengiriman email palsu sedang berlangsung dan jika proses pengiriman berhasil maka akan keluar kotak pemberitahuan yang bertuliskan ***Mail Sent OK!***. Klik **OK**.



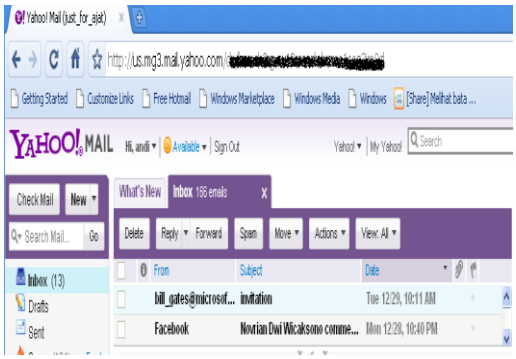
Gambar 3
proses pengiriman email palsu

Pengecekan email

Untuk memeriksa apakah email yang penulis buat sudah sampai ke alamat tujuan maka penulis harus login ke dalam email penulis sendiri dalam kasus ini penulis mengirim email palsu ke email

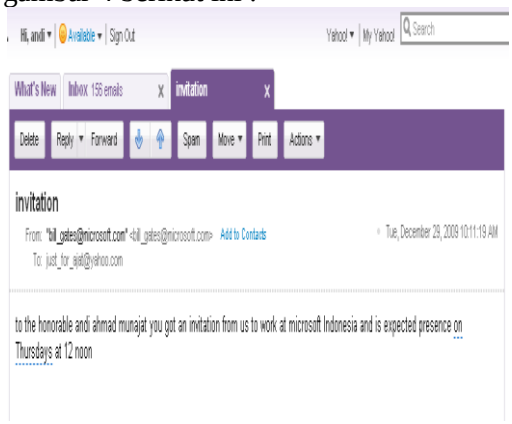
penulis sendiri dimana penulis menggunakan alamat email dari yahoo.

Pada email tujuan akan muncul email palsu tersebut, seperti pada gambar berikut ini :



Gambar 4
email palsu diterima di inbox sasaran

Jika email palsu tersebut di klik maka akan muncul isi dari email palsu tersebut. Kalo diperhatikan secara sekilas email tersebut asli bahkan user biasa pun tidak dapat membedakannya seperti dalam gambar 4 berikut ini :



Gambar 5
isi dari email palsu

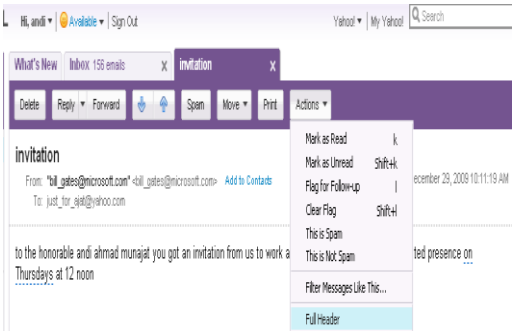
Dalam pesan tersebut menyatakan bahwa si pemilik email mendapat undangan untuk datang dan bergabung dengan perusahaan Microsoft Indonesia pada hari kamis jam 12 siang, maka dari itu kita harus melihat header email tersebut untuk mengetahui keapsahan email tersebut.

Analisis header email

Sebelum kita menganalisis email tersebut, kita harus memastikan bahwa email asli tidak akan di buang, atau dalam hal lain di *deleted*.

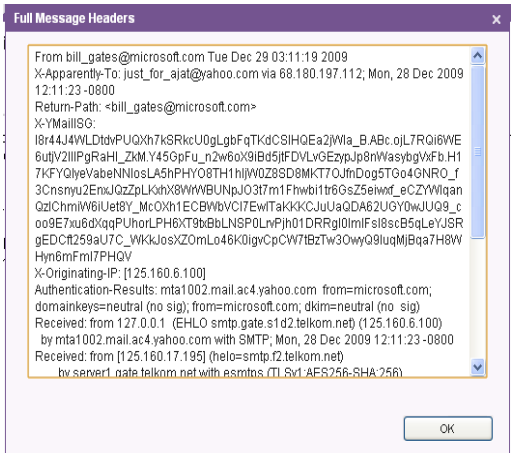
Untuk mengetahui keaslian/keabsahan dari email tersebut maka diperlukan untuk melakukan analisis header dari email tersebut.

Analisis header email tersebut dapat dilakukan dengan cara melakukan klik fungsi Actions lalu sorot dan klik full header seperti dalam gambar 6 berikut :



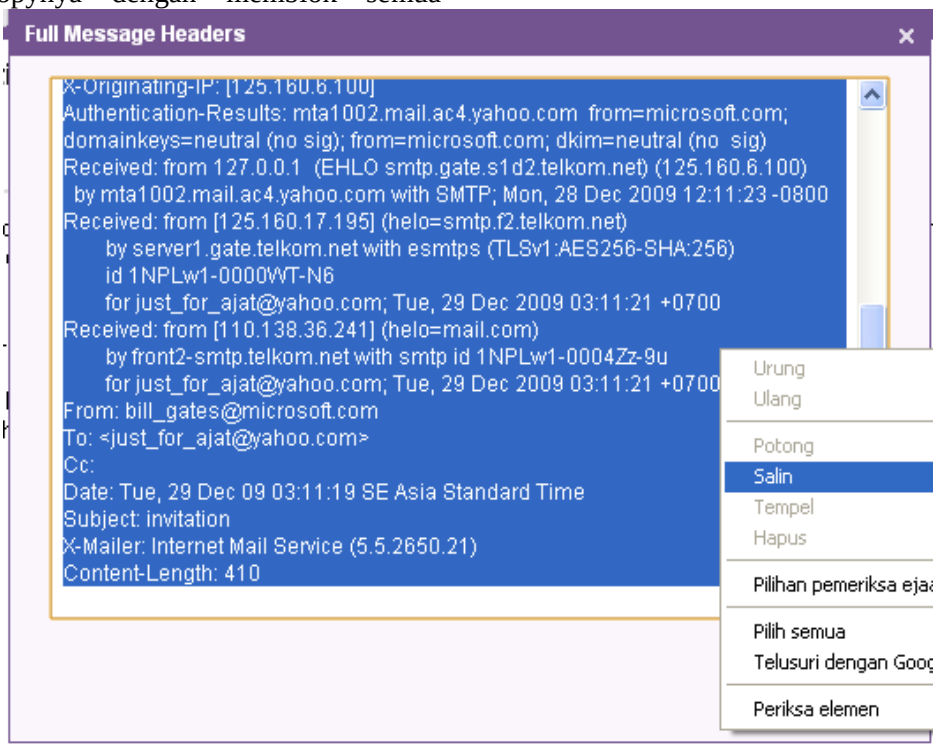
Gambar 6
melihat header email

Maka tampilan header email tersebut dapat dilihat dalam gambar 4.7 header tersebut memberitahukan bahwa email tersebut dikirim melalui beberapa server.



Gambar 7
isi dari header email

Agar dapat menganalisa header email tersebut maka langkah yang harus dilakukan adalah mencopy header email tersebut ke dalam notepad, cara mengopynya dengan memblok semua tulisan yang ada di kolom header lalu mengklik kanan dan sorot dan pilih tulisan salin, seperti Gambar 8 berikut :



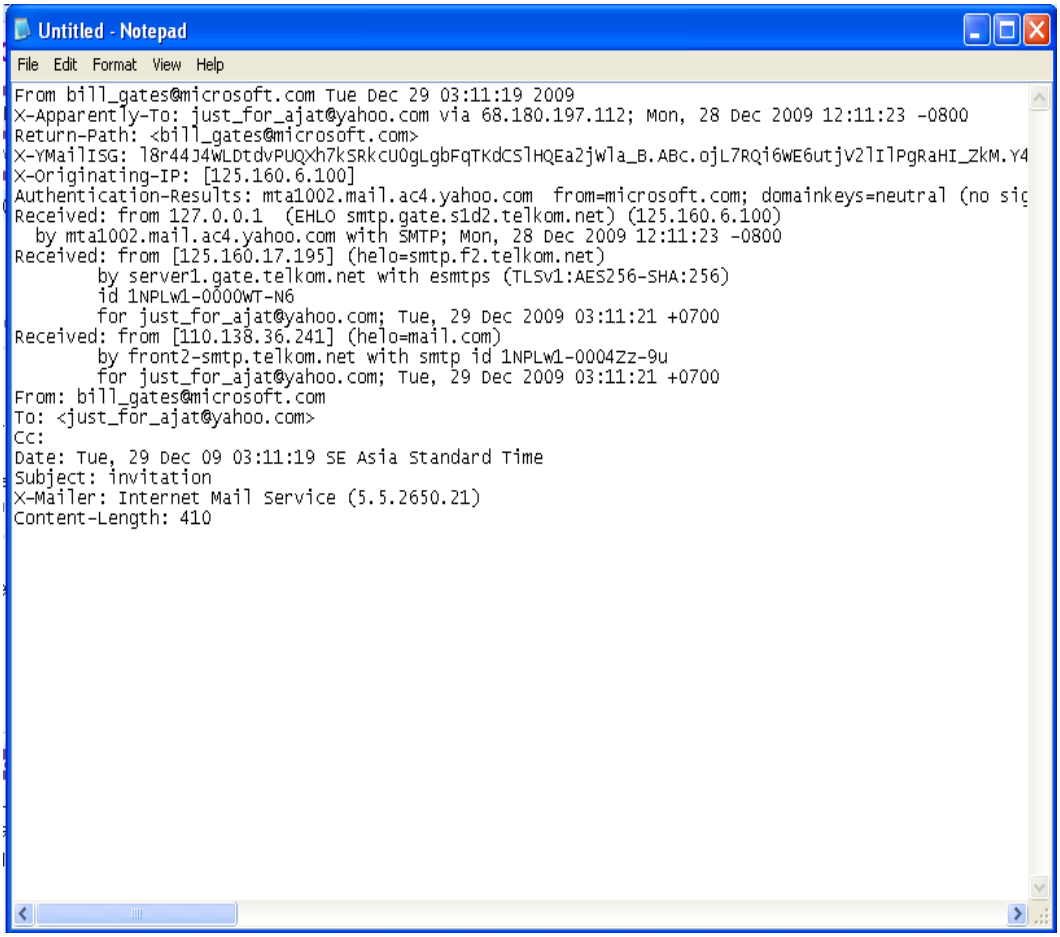
Gambar 8
meng*copy* isi *header email*

Setelah kita mengopy isi header email maka kita buka notepad dengan mengklik tombol start lalu pilih run dan mengetikan notepad di kolom isian run tersebut, setelah notepad muncul lalu kita mempastekan isi header email yang sudah kita copy tersebut ke dalam notepad seperti dalam Gambar 9 tersebut.

Untuk lebih jelasnya maka penulis akan menjelaskan tentang isi header tersebut.

From bill_gates@microsoft.com Tue Dec 29 03:11:19 2009
X-Apparently-To: just_for_ajat@yahoo.com via 68.180.197.112; Mon, 28 Dec 2009 12:11:23 -0800
Return-Path: <bill_gates@microsoft.com>
X-YMailISG: l8r44J4WLDtdvPUQXh7kSRkcU0gLgbFqTKdCSlHQEa2jWla_B.ABc.ojL7RQi6WE6utjV2lIlPgRaHI_ZkM.Y45GpFu_n2w6oX9iBd5jtFDVLvGEzypJp8nWasybgVxFb.H17KFYQIyeVabeNNIosLA5hPHYO8TH1hIjW0Z8SD8MKT7OJfnDog5TGo4GNRO_f3Cnsnyu2EnxJQzZpLKxhX8WrWBUNpJO3t7m1Fhwbi1tr6GsZ5eiwxf_eCZYWlqanQzIChmiW6iUet8Y_McOXh1ECBWbVCI7EwITaKKKCJuUaQDA62UGY0wJUQ9_coo9E7xu6dXqqPUhorLPH6XT9txBbLNSP0LrvPjh01DRRgl0ImIFsl8scB5qLeYJSRgEDCft259aU7C_WKkJosXZOmLo46K0igvCpCW7tBzTw3OwyQ9luqMjBqa7H8WHyn6mFmI7PHQV
X-Originating-IP: [125.160.6.100]
Authentication-Results:

mta1002.mail.ac4.yahoo.com from=microsoft.com; domainkeys=neutral (no sig); from=microsoft.com; dkim=neutral (no sig)
Received: from 127.0.0.1 (EHLO smtp.gate.s1d2.telkom.net) (125.160.6.100)
by mta1002.mail.ac4.yahoo.com with SMTP; Mon, 28 Dec 2009 12:11:23 -0800
Received: from [125.160.17.195] (helo=smtp.f2.telkom.net)
by server1.gate.telkom.net with esmtps (TLSv1:AES256-SHA:256)
id 1NPLw1-0000WT-N6
for just_for_ajat@yahoo.com; Tue, 29 Dec 2009 03:11:21 +0700
Received: from [110.138.36.241] (helo=mail.com)
by front2-smtp.telkom.net with smtp id 1NPLw1-0004Zz-9u
for just_for_ajat@yahoo.com; Tue, 29 Dec 2009 03:11:21 +0700
From: bill_gates@microsoft.com
To: <just_for_ajat@yahoo.com>
Cc:
Date: Tue, 29 Dec 09 03:11:19 SE Asia Standard Time
Subject: invitation
X-Mailer: Internet Mail Service (5.5.2650.21)
Content-Length: 410



Gambar 9
mem*paste* isi *header* email ke *notepad*

Email seolah-olah berasal dari "bill_gates@microsoft.com" akan tetapi kalau kita telusuri stempel headernya, tidak satupun stempel yang menunjukkan bahwa email pernah singgah di MTA "kantor Pos" microsoft, MTA yang seharusnya memberikan stempel pada email tersebut, header email justru menunjukkan asal email bukanlah dari domain Microsoft.com, akan tetapi dari alamat *ip address* 110.138.36.241.

Cara membaca stempel pada header email adalah dari dari bawah ke atas sehingga dapat ditelusuri aliran email tersebut.

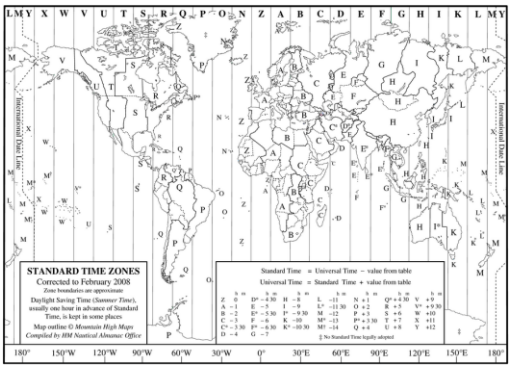
- *Received: from [110.138.36.241] (helo=mail.com) by front2-smtp.telkom.net with smtp id*
  Seseorang dari alamat ip address 110.138.36.241 menulis surat dan dikirimkan "Kantor Pos" smtp.telkom.net.
- *Received: from [125.160.17.195] (helo=smtp.f2.telkom.net) by server1.gate.telkom.net with esmtps*
  Ip address 125.160.17.195 mengirim ke *server1.gate*.telkom
- *Received: from 127.0.0.1 (EHLO smtp.gate.s1d2.telkom.net) (125.160.6.100)* by mta1002.mail.ac4.yahoo.com with SMTP
  Alamat ip 127.0.0.1 mengirim ke mail.ac4.yahoo.com

Dan akhirnya sampailah email yang seolah-olah dari bill_gates@microsoft.com ke MTA di yahoo.com ke "just_for_ajat" di mesin 68.180.197.112.

Dari header email, email palsu dapat ditelusuri dari mana asalnya, akan tetapi belum dapat diketahui siapa orang yang melakukannya karena yang tercatat adalah IP Address atau domain mesin, seperti contoh diatas.

Untuk itu kita harus lebih dahulu untuk mengetahui pembagian waktu dunia di seluruh Negara agar proses analisis dan pelacakan email palsu tersebut dapat di ketahui dengan mudah, Hubungan waktu dengan email adalah proses email terkirim ke dalam inbox seseorang tercatat waktu sampainya email tersebut.

Untuk itu kita harus menuju website http://aa.usno.navy.mil/graphics/TimeZoneMap0802.png agar dapat mengetahui email tersebut di kirim dengan menggunakan bagian waktu manakah? Pada Gambar 10 menerangkan bagian-bagian waktu Negara di seluruh dunia.



Gambar 10
waktu dunia

Administrator IP

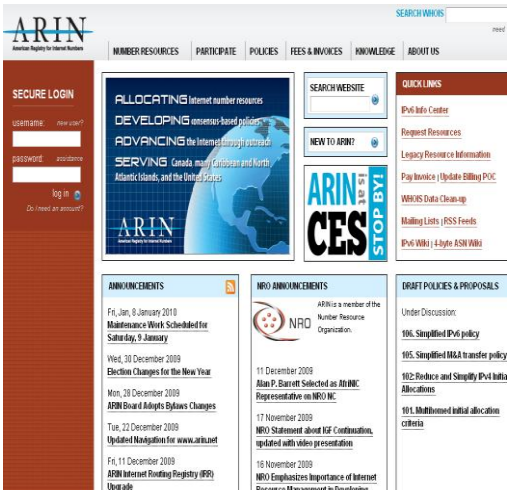
Untuk mencari pemilik IP yang mengirimkan email palsu tersebut, maka kita harus ke administrator penggunaan IP address.

Administrator ip address ada 4 di dunia ini, keempat administrator ini yang mengatur penggunaan ip address yang ada di setiap komputer di dunia. Keempat administrator tersebut adalah :

1. ARIN (*North America and sub-Sharan Africa*)
2. RIPE (*Eropa and northen Africa*)
3. APNIC (*asia pacific*)
4. LACNIC (*Southern and Central America and the Caribbean*)

ARIN (www.arin.net)

ARIN (*North America and sub-Sharan Africa*) seluruh ip address yang berada di daerah amerika utara dan bagian Sharan, Afrika diketuai oleh arin, dan gambar 11 adalah tampilan dari arin.



Gambar 11
ARIN

Ripe (www.ripe.net)

RIPE (*Eropa and northen Africa*) seluruh ip *address* yang berada di daerah eropa dan afrika utara diketuai oleh RIPE, dan gambar 12 adalah tampilan dari RIPE.

Gambar 12
RIPE

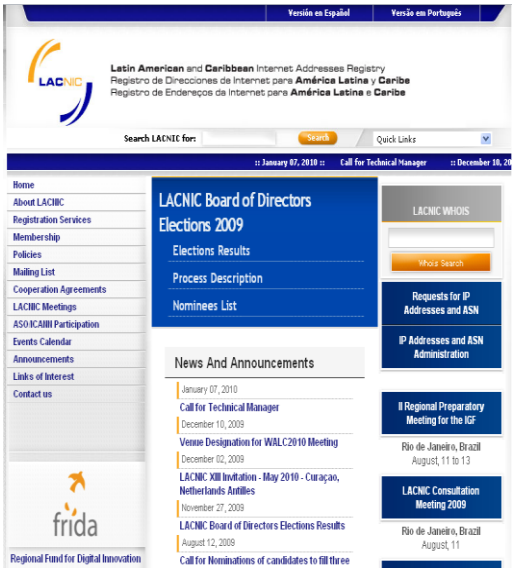
Apnic (www.apnic.net)

Apnic (*asia pacific*) seluruh ip address yang berada di asia pasifik diketuai oleh apnic, gambar 13 adalah tampilan dari APNIC.

Gambar 13
apnic

lapnic (www.lacnic.net)

Lapnic (*Southern and Central America and the Caribbean*) semua ip address yang berada di daerah selatan dan amerika tengah juga yang berada di Karibia diketuai oleh lapnic, gambar 14 adalah tampilan dari lapnic.



Gambar 14
lapnic

Menelusuri IP address email palsu

Untuk mengetahui IP address dari email palsu tersebut, maka ip address yang tercatat di header email tersebut di laporkan ke administrator ip.

Karena penulis tidak mengetahui ip address tersebut dari Negara mana maka penulis harus menanyakan satu persatu ke administrator ip.

Gambar 15
memasukkan *ip address* ke website ARIN

Masukkan *ip address* yang ingin kita ketahui kedalam kolom *whois* dan tekan *enter* atau tombol *search*.

```
OrgName:    Asia Pacific Network Information Centre
OrgID:      APNIC
Address:    PO Box 2131
City:       Milton
StateProv:  QLD
PostalCode: 4064
Country:    AU

ReferralServer: whois://whois.apnic.net

NetRange:   110.0.0.0 - 110.255.255.255
CIDR:       110.0.0.0/8
NetName:    APNIC-AP
NetHandle:  NET-110-0-0-0-1
Parent:
NetType:    Allocated to APNIC
NameServer: NS1.APNIC.NET
NameServer: NS3.APNIC.NET
NameServer: NS4.APNIC.NET
NameServer: TINNIE.ARIN.NET
NameServer: NS2.LACNIC.NET
NameServer: NS-SEC.RIPE.NET
Comment:    This IP address range is not registered in the ARIN database.
Comment:    For details, refer to the APNIC Whois Database via
Comment:    WHOIS.APNIC.NET or http://wq.apnic.net/apnic-bin/whois.pl
Comment:    ** IMPORTANT NOTE: APNIC is the Regional Internet Registry
Comment:    for the Asia Pacific region. APNIC does not operate networks
Comment:    using this IP address range and is not able to investigate
Comment:    spam or abuse reports relating to these addresses. For more
Comment:    help, refer to http://www.apnic.net/apnic-info/whois_search2/abuse-and-spamming
RegDate:    2008-11-12
Updated:    2009-10-08

OrgTechHandle: AWC12-ARIN
OrgTechName:   APNIC Whois Contact
OrgTechPhone:  +61 7 3858 3188
```

Gambar 16
ARIN memberitahukan ip kekuasaan punya APNIC

Arin memberitahukan bahwa ip address 110.138.36.241 bukanlah punya arin melainkan punya apnic.

Berikut adalah hasil dari pencarian arin yang menyatakan bahwa ip tersebut bukan milik arin melainkan milik apnic.

OrgName : Asia Pacific Network Information Centre
OrgID : APNIC
Address: PO Box 2131
City : Milton
StateProv : QLD
PostalCode : 4064
Country : AU
ReferralServer : whois://whois.apnic.net
NetRange : 110.0.0.0 - 110.255.255.255
CIDR : 110.0.0.0/8
NetName : APNIC-AP
NetHandle : NET-110-0-0-0-1
Parent : -
NetType : Allocated to APNIC
NameServer : NS1.APNIC.NET
NameServer : NS3.APNIC.NET
NameServer : NS4.APNIC.NET
NameServer : TINNIE.ARIN.NET
NameServer : NS2.LACNIC.NET
NameServer : NS-SEC.RIPE.NET
Comment : This IP address range is not registered in the ARIN database.
Comment : For details, refer to the APNIC Whois Database via
Comment : WHOIS.APNIC.NET or http://wq.apnic.net/apnic-bin/whois.pl
Comment : IMPORTANT NOTE: APNIC is the Regional Internet Registry
Comment : for the Asia Pacific region. APNIC does not operate networks
Comment : using this IP address range and is not able to investigate
Comment : spam or abuse reports relating to these addresses. For more
Comment : help, refer to www.apnic.net/apnic-info/whois_search2/abuse-and-spamming
RegDate : 2008-11-12

Updated : 2009-10-08
OrgTechHandle: AWC12-ARIN
OrgTechName : APNIC Whois Contact
OrgTechPhone : +61 7 3858 3188
OrgTechEmail : search-apnic-not-arin@apnic.net
 # ARIN WHOIS database, last updated 2010-01-13 20:00
 # Enter ? for additional hints on searching ARIN's WHOIS database.
#
 # ARIN WHOIS data and services are subject to the Terms of Use
 # available at https://www.arin.net/whois_tou.html

Karena ARIN sudah memeberitahukan bahwa ip 110.138.36.241 adalah punya apnic maka penulis akan membuka web site apnic, untuk mencari tahu Negara manakah yang mempunyai ip tersebut.

Gambar 17
memasukkan ip address ke web site APNIC

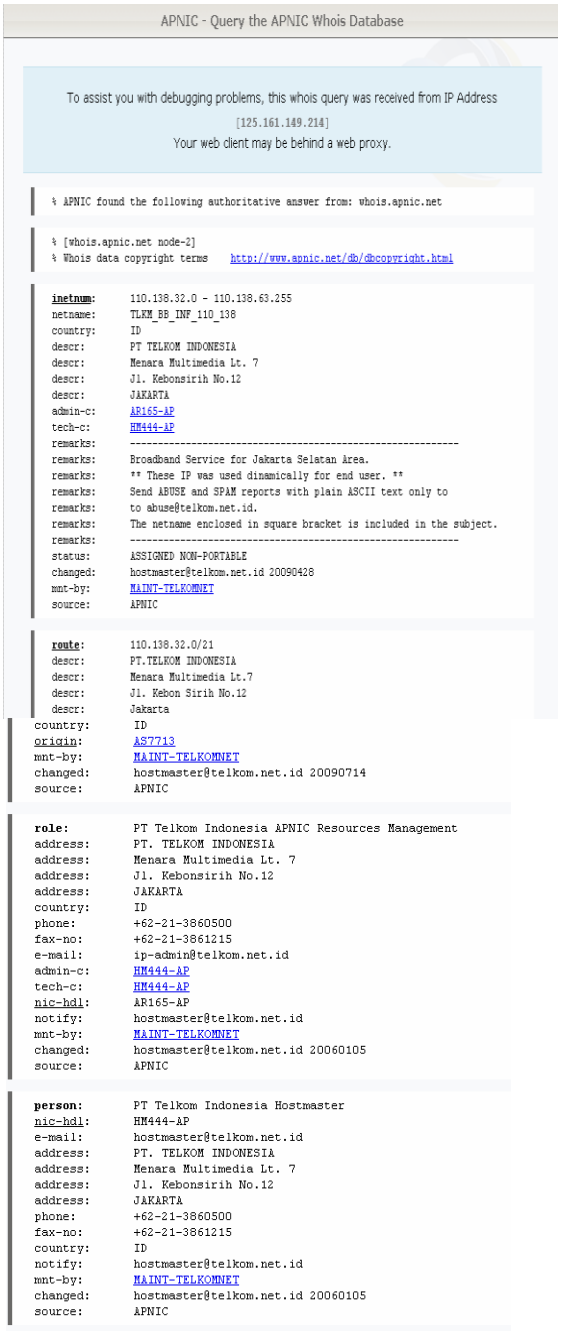
Masukkan alamat ip tersebut ke dalam kolom *whois* dan tekan *enter* atau klik tombol search.

Hasil pencarian dari apnic menyatakan bahwa ip address 110.138.36.241 adalah punya Negara Indonesia, milik perusahaan PT Telkom Indonesia yang beralamatkan di jalan kebon sirih no 12.

Untuk lebih jelasnya penulis akan menuliskan isi hasil pencarian dari apnic tersebut, sebagai berikut :

% APNIC found the following authoritative answer from: whois.apnic.net
% [whois.apnic.net node-2]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html
Inetnum : 110.138.32.0 - 110.138.63.255
Netname : TLKM_BB_INF_110_138
Country : ID
Descr : PT TELKOM INDONESIA
Descr : Menara Multimedia Lt. 7
Descr : Jl. Kebonsirih No.12
Descr : JAKARTA
admin-c : AR165-AP
tech-c : HM444-AP
remarks : ----------
remarks : Broadband Service for Jakarta Selatan Area.
remarks : ** These IP was used dinamically for end user. **
remarks : Send ABUSE and SPAM reports with plain ASCII text only to
remarks : to abuse@telkom.net.id.

remarks : The netname enclosed in square bracket is included in the subject.
remarks : ----------
status : ASSIGNED NON-PORTABLE
changed : hostmaster@telkom.net.id 20090428
mnt-by : MAINT-TELKOMNET
source : APNIC
route : 110.138.32.0/21
descr : PT.TELKOM INDONESIA
descr : Menara Multimedia Lt.7
descr : Jl. Kebon Sirih No.12
descr : Jakarta
country : ID
origin : AS7713
mnt-by : MAINT-TELKOMNET
changed : hostmaster@telkom.net.id 20090714
source : APNIC
role : PT Telkom Indonesia APNIC Resources Management
address : PT. TELKOM INDONESIA
address : Menara Multimedia Lt. 7
address : Jl. Kebonsirih No.12
address : JAKARTA
country : ID
phone : +62-21-3860500
fax-no : +62-21-3861215
e-mail : ip-admin@telkom.net.id
admin-c : HM444-AP
tech-c : HM444-AP
nic-hdl : AR165-AP
notify : hostmaster@telkom.net.id
mnt-by : MAINT-TELKOMNET
changed : hostmaster@telkom.net.id 20060105
source : APNIC
person : PT Telkom Indonesia Hostmaster
nic-hdl : HM444-AP
e-mail : hostmaster@telkom.net.id
address : PT. TELKOM INDONESIA
address : Menara Multimedia Lt. 7
address : Jl. Kebonsirih No.12
address : JAKARTA
phone : +62-21-3860500
fax-no : +62-21-3861215
country : ID
notify : hostmaster@telkom.net.id
mnt-by : MAINT-TELKOMNET
changed : hostmaster@telkom.net.id 20060105
source : APNIC



Gambar 18
hasil APNIC

Daftar Pustaka

_____,Australian Institute of Criminology http://www.aic.gov.au/publications/tandi (diakses pada tanggal : 21 November 2009).

_____,computer forensik yusuf yudi prayudi, http://prayudi.wordpress.com/2007/03/31/komputer-forensik (diakses pada tanggal : 02 februari 2010).

_____,digital forensik menelusuri email palsu, students.ee.itb.ac.id/~alkebumeny/lecture/../menelusuri_**email**_palsu.doc. (diakses pada tanggal : 21 november 2009).

_____,efran blogspot http://f4123n.blogspot.com/2009/01/definisi-komputer.html (diakses pada tanggal : 24 februari 2010).

_____,Email bombing, en.kioskea.net/contents/attaques/mailbombing.php3 (diakses pada tanggal : 10 desember 2009).

Feri sulianta, "komputer forensik *"*, 2008.

_____,forum folambor, http://www.flobamor.com/forum/showthread.php?p=26787 (diakses tanggal : 20 Mei 2008).

_____,journal portal Islamic university of Indonesia, http://journal.uii.ac.id/index.php/Snati/article/viewFile/1634/1409M (diakses pada tanggal : 21 november 2009).

_____,Management Information System School Trimana Djaya http://misstriad.wordpress.com/2006/10/05/definisi-komputer (diakses pada tanggal : 24 februari 2010).

_____**,**Network Management: Covering today's Network topics http://searchnetworkeing.techtarget.com, (diakses pada tanggal : 21 November 2009).

_____,pengertian email elbert's blog, http://elbertasia.wordpress.com/2008/11/11/pengertian-e-mail (diakses pada tanggal : 21 november 2009).

Rahmad rafiudin., "internet *forensics*" 2009.

_____,sutisna senjaya situs pribadi sutsen http://sutisna.com/pendidikan/strategi-belajar-mengajar/pengertian-metode-mengajar (diakses pada tanggal : 23 februari 2010).

_____,scridb http://www.scribd.com/doc/24558054/PENGERTIAN-METODE (diakses pada tanggal : 23 februari 2010).

_____,spamming-echo.or.id, http://ezine.echo.or.id/ezine3/ez-r03-z3r0byt3-spamming.txt (diakses pada tanggal : 21 november 2009).

_____,thing quest, http://www.thinkquest.org (diakses pada tanggal : 21 November 2009).

_____,welcome in my blog cara kerja email http://amblog1803.blogspot.com/2009/02/cara-kerja-e-mail.html (diakses pada tanggal : 21 november 2009).