ANALISIS VISUALISASI DATA KEAMANAN JARINGAN

Tati Ernawati
Jurusan Teknik Informatika, Politeknik TEDC Bandung
Jalan Pasantren Km.2 Cibabat Cimahi Utara
E-mail: tatiernawati@yahoo.com

ABSTRACT

Network security monitoring activity would be a big problem if the data processed are too much while the analytical tool that is used still manually. The issues raised about the network security based on the concept that a computer connected to a network is vulnerable to be attacked, otherwise the majority of users do not have a security background to identify malicious activity. Many users often negligent in monitoring the large amount of traffic in a complex network. This occurance was only realized when a computer or system is infected by a virus or suspicious malware.

This paper describes the analysis of network security data visualization. The methodology used is a case study. An analysis was performed on text/numeric and visual-based network monitoring. The analysis showed the using of visualized observations could examine network traffic and detect anomalies faster than the manual way (based on text/numeric).

Keywords: data visualization, text/numeric, anomalous

INTISARI

Aktivitas monitoring keamanan jaringan akan menjadi masalah besar apabila data yang diolah sangat banyak sementara alat analisis yang digunakan masih manual. Isu yang muncul tentang keamanan jaringan didasari atas konsep sebuah komputer yang terhubung ke dalam sebuah jaringan yang rentan terhadap serangan, selain itu mayoritas pengguna tidak memiliki latar belakang keamanan untuk mengidentifikasi aktivitas yang berbahaya sehingga seringkali lalai dalam memonitor sejumlah besar lalu lintas dalam sebuah jaringan yang kompleks. Hal ini baru disadari setelah sebuah komputer atau sistem terinfeksi oleh virus atau perangkat lunak yang mencurigakan.

Paper ini menjelaskan tentang analisis visualisasi data keamanan jaringan. Metodologi yang digunakan adalah studi kasus, analisis dilakukan pada monitoring jaringan berbasis teks/numerik dan berbasis visual. Hasil analisis menunjukan bahwa hasil pengamatan dengan menggunakan visual dapat memeriksa lalu lintas jaringan dan mendeteksi anomali jauh lebih cepat daripada dengan cara manual (berbasis teks/numerik).

Kata Kunci : visualisasi data, teks/numerik, anomali

PENDAHULUAN

Pendeteksian serangan terhadap sebuah jaringan sebagian besar masih didasarkan pada cara-cara tradisional dengan membaca data secara numerikal, hal ini mengakibatkan proses monitoring yang dilakukan lebih rumit dan tidak langsung dapat terbaca secara visual sementara proses infeksi terus berjalan. Selain itu para administrator keamanan jaringan cenderung menggantungkan keamanan jaringan pada sistem *firewall* yang ada tanpa harus memonitor lalu lintas jaringan secara *real-time*, sehingga seringkali sebuah jaringan baru diketahui setelah terjadi masalah tanpa sempat melakukan tindakan preventif (Tri dkk, 2009).

Mekanisme visualisasi secara grafis (2 atau 3 dimensi) dalam monitoring sistem keamanan yang cepat dan akurat dibutuhkan untuk mengatasi kebutuhan keamanan jaringan, terutama dalam pemahaman lalu lintas data pada sebuah sistem jaringan yang kompleks. Hal ini jauh lebih mudah dan cepat untuk mengidentifikasi kejadian jaringan abnormal dari model visual sebagai kebalikan dari teknik tradisional yang meliputi analisis sekuensial berbasis teks atau numerik (Schwagele, 2010).

Visualisasi tidak hanya sebatas metode yang digunakan dalam menganalisis keamanan, tetapi merupakan proses transformasi informasi ke dalam bentuk visual yang memungkinlan untuk diamati dan

dipahami oleh pengguna. Komputer digunakan untuk memproses dan melihat gambaran informasi menggunakan teknik grafik interaktif, gambar dan desain visual. Konsepnya didasarkan pada sistem visual dalam memproses informasi.

Informasi melalui visualisasi sangat jelas karena dikomunikasikan melalui perangkat visual yang interaktif. Data yang dihasilkan dipresentasikan secara visual sehingga informasi yang didapat mudah dimengerti otak manusia. Sistem aplikasi visualisasi dapat meningkatkan penglihatan terhadap aspek tiga dimensi, warna dan pola (Akindeinde, 2009).

Paper ini menyajikan analisis visualisasi data keamanan jaringan yang dibandingkan dengan data secara numerikal berbasis teks (tradisional). Dalam studi kasus ini dipilih jaringan internal yang berada di Institut Teknologi Bandung sebagai jaringan lalu lintas yang dianalisis. Tool analisis dilakukan dengan menggunakan perangkat lunak berbasis teks yaitu *wireshark* dan berbasis visual yaitu *Internet Visual (InetVis).* Penelitian ini menggunakan data hasil pengamatan pada studi kasus yang dilakukan.

TINJAUAN PUSTAKA

Konsep Visualisasi Data

Visualisasi adalah konversi data ke dalam format visual (tabel atau grafik) sehingga karakteristik dari data dan relasi di antara item data atau atribut dapat dianalisis atau dilaporkan. Visualisasi data adalah satu dari teknik yang paling baik dan menarik untuk eksplorasi data. Manusia memiliki kemampuan untuk menganalisis sejumlah besar informasi yang dipresentasi secara visual.

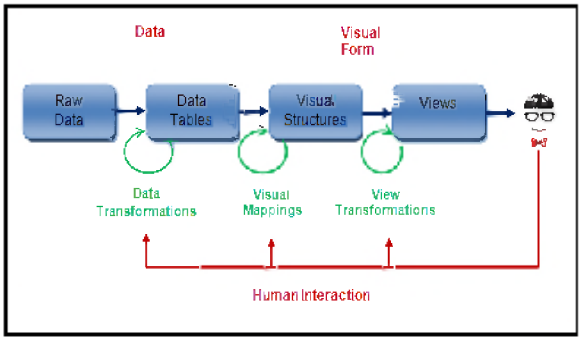
Sementara itu, visualisasi data didefinisikan sebagai berbagai jenis cara untuk membuat gambar, diagram atau animasi dengan tujuan untuk mengkomunikasikan sebuah pesan/informasi (Mihaly, 2008). Pada umumnya visualisasi digunakan untuk mengagregasi data dalam jumlah yang sangat besar yang kemudian dipresentasikan dengan berbagai model.

Monitoring sebuah jaringan dengan memanfaatkan kapabilitas mata manusia melalui sebuah grafis tiga dimesi (*3D)* dapat memberikan sebuah informasi yang lebih bermanfaat dalam dalam mendeteksi anomali lalu lintas data. Pendeteksian dan pengklasifikasian aktivitas mencurigakan dalam sebuah lalu lintas jaringan sudah menjadi sebuah masalah yang penuh tantangan dan diperburuk dengan begitu banyaknya data serta terbatasnya alat analisis. Dalam sebuah jaringan yang kecil, analisis manual sangat tidak efisien dan memboroskan banyak waktu (Krasser, 2005).

Berdasarkan asumsi tersebut visualisasi data melalui grafis 3 dimensi menjadi alternatif alat dalam memonitor lalu lintas data dalam sebuah jaringan. Banyak perangkat lunak keamanan menampilkan data secara numerik, hal ini membutuhkan waktu untuk menganalisis data sehingga sangat tidak efisien dan efektif.

Proses Visualisasi Data

Proses visualisasi biasanya terdiri dari tiga komponen yang berbeda tetapi saling terkait seperti terlihat pada gambar 1.



Gambar 1 Tahapan visualisasi, sumber (Akindeinde, 2009).

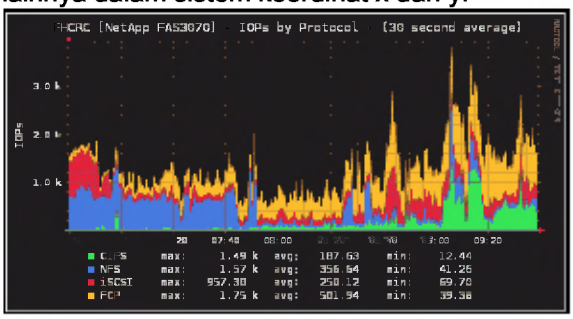
a. *Data Tables;* Data mentah ditransformasikan ke dalam tabel data terstruktur yang memiliki beberapa arti direpresentasikan melalui metadata.
b. *Visual Structures;* Data yang disusun ditransformasikan ke dalam suatu model geometrik dengan memilih bentuk dasar geometris seperti titik, garis dan poligon dan menetapkan data atribut. Sebagai contoh tabel data 3-dimensi dapat ditransformasikan dalam grafik 3-dimensi menggunakan masing-masing kolom yang terkait dengan suatu variabel tertentu. Tabel yang sama dapat digunakan untuk menghasilkan representasi 2-dimensi dengan variabel ketiga direpresentasikan oleh ukuran atau warna dari titik-titik yang ditempatkan di grafik sesuai dengan dua variabel lainnya
c. *Views;* Representasi dapat dilihat dari sudut pandang yang berbeda. Data geometrik

selanjutnya ditransformasikan menjadi gambar. Hal ini dilakukan dengan melihat perubahan skala, *translate*, *zoom* dan representasi grafis.

Data-data tersebut kemudian disajikan dalam bentuk visual grafis. Terdapat berbagai macam cara untuk mempresentasikan data visual. Representasi visual dapat diilustrasikan secara menyeluruh dan dipahami yang dipresentasikan secara nyata secara statistik dengan *tools* representasi data (Mihaly, 2008)

1) *Line Chart*

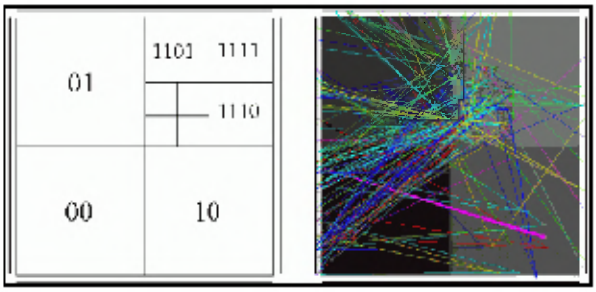
Digunakan untuk mewakili baik dua dimensi dan satu data dimensi. Sekumpulan data titik yang dihubungkan oleh garis, pada umumnya menampilkan nilai dari satu kolom (dimensi data) dibandingkan dengan kolom lainnya dalam sistem koordinat x dan y.



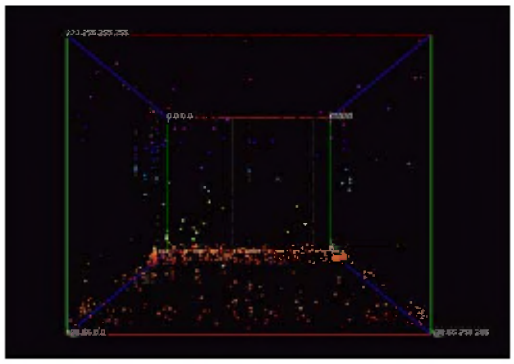
Gambar 2 Contoh dari *Line Chart* *(IOPS alat Jaringan per protokol yang dihasilkan dengan RRDTool)*

2) *Scatterplot*

Scatterplot menggambarkan hubungan antara variabel melalui kemiringan garis. Mudah digunakan tetapi harus diinterpretasikan dengan teliti ketika melihat hubungan antara variabel-variabel, hal ini dikarenakan skala yang digunakan terlalu kecil. Contoh ditunjukkan pada Gambar 3 dan Gambar 4.



Gambar 3 Kiri: *Quadtree* pengkodean *prefix IP*, Kanan: data aktual.

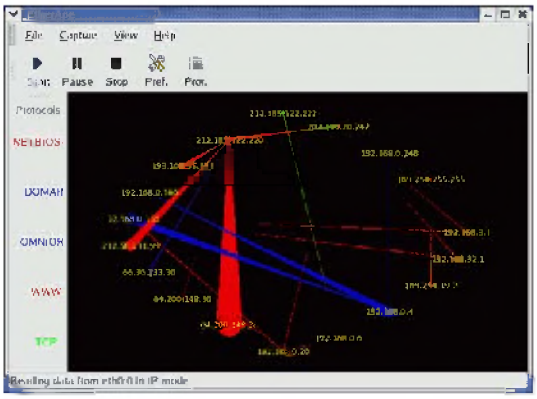


Gambar 4 Contoh lain dari *Scatterplot*

Pada gambar 4 dapat dilihat titik-titik yang menyebar memperlihatkan sejumlah lalu lintas data yang terjadi dalam jaringan.

3) Grafik

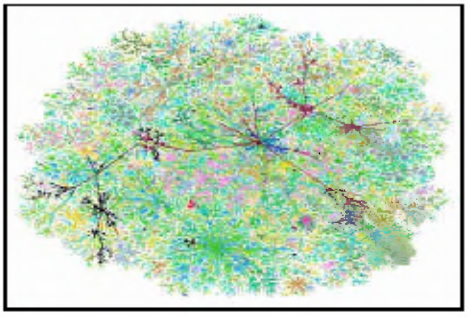
Pada umumnya grafik digunakan untuk mempresentasikan suatu jaringan. Alamat yang unik dari elemen jaringan (misalnya *MAC* untuk lapisan 2 atau *IP* untuk layer 3) direpresentasikan sebagai node dan hubungan antara kedua layer tersebut digunakan untuk mewakili "arus" (aliran *Transmission Control Protocol*/*TCP*).



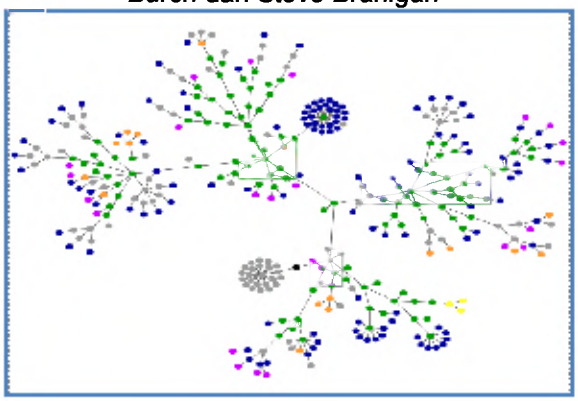
Gambar 5 Contoh dari Grafik menggunakan aplikasi *EtherApe*

Pada gambar 5, node adalah elemen jaringan aktif (*router*, *NIC* dan lain-lain) yang diwakili oleh sebuah alamat. Koneksi antar elemen merupakan lalu lintas data, dengan protokol yang dipresentasikan dengan warna. Ukuran node sebanding dengan jumlah lalu lintas yang dihasilkannya. Contoh lain disajikan kode warna "peta Internet" dari tahun 1998, di mana jarak didasarkan pada jumlah hop yang dilaporkan oleh *traceroute* dari laboratorium *Bell* dan kode wama digunakan

untuk menandai peralatan milik organisasi yang sama (berdasarkan pada dua bagian pertama dari nama *DNS* oleh *reverse-lookup*), terlihat pada gambar 6.



Gambar 6 Peta Internet dari "Pemetaan dan Visualisasi Internet" oleh *Bill Cheswick*, *Hal Burch* dan *Steve Branigan*



Gambar 7a *Webpage as Graps* dari http://www.itb.ac.id 22 April 2011 (online dari http://www.aharef.info/static/htmlgraph)

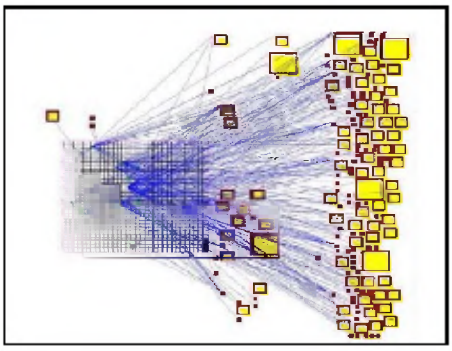
Pada gambar 7a arti dari node warna adalah:

- Biru : *link* untuk teks atau gambar
- Merah : *link* untuk tabel
- Hijau : *link* untuk dokumen *HTML (Hyper Text Markup Languange*)
- Violet : *link* untuk gambar
- Kuning : *link* untuk form (input, teks area, select dan option)
- Orange : *link* untuk linebreaks dan blockquotes
- Hitam : *root node*
- Abu-abu : semua link yang lain

4) Grid Layout

Metode pemetaan alamat *IP* untuk *layout grid* yaitu apabila jumlah alamat *IP* kecil. Contoh dari *Grid Layout* dapat dilihat dari gambar 7, sistem administrator melakukan pemantuan di dalam jaringan internal yang direpresentasikan dengan kotak besar. Eksternal host yang terlibat dalam jaringan dipresentasikan disebelah kanan dengan ukuran yang mempresentasikan jumlah data yang mengalir ke atau dari dirinya sendiri.

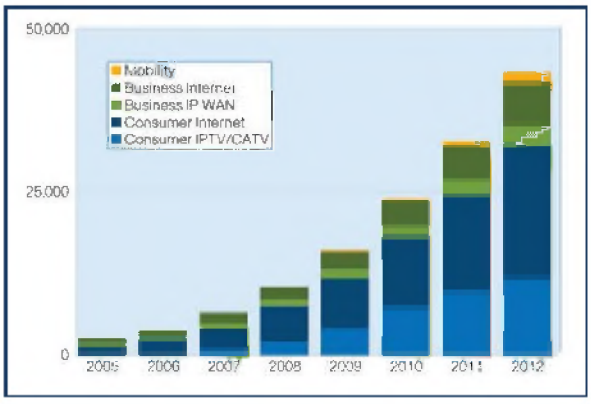
Garis-garis vertikal kecil menggambarkan *TCP/UDP (User Datagram Protocol) port* digunakan selama komunikasi.



Gambar 7b Visualisasi Jaringan *Home-Centric* Administrasi Keamanan Lalu Lintas Jaringan

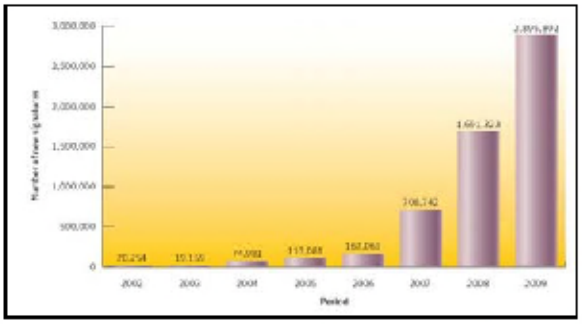
Perkembangan Lalu Lintas Jaringan dan Isu Keamanan

Internet telah berkembang pesat dalam dekade terakhir Schwagele, 2010), seperti yang diilustrasikan pada Gambar 8 menunjukkan bahwa pertumbuhan lalu lintas *Internet Protocol* (*IP*) global diperkirakan akan empat kali lipat pada tahun 2014.



Gambar 8 Grafik perkiraan pertumbuhan lalu lintas *IP* Global (Sumber: *Cisco,* 2010)

Seiring meningkatnya pertumbuhan lalu lintas *IP* memberikan konsekuensi ancaman terhadap jaringan yang meningkat pula, seperti terlihat pada gambar 9. Untuk mencegah dan mengatasi aktivitas berbahaya yang mengancam lalu lintas jaringan tersebut maka diperlukan keamanan jaringan. Keamanan ini bertujuan agar jaringan tidak disusupi oleh orang lain yang tidak memiliki hak akses yang pada akhirnya dapat merusak *performance* jaringan. Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif. Salah satu cara yaitu dengan memonitor lalu lintas jaringan (Schwagele, 2010).



Gambar 9 Perkembangan ancaman kejahatan dari *code signature* (Sumber: *Symantec*)

Monitoring Jaringan

Perkembangan jaringan komputer yang semakin pesat memberikan tantangan tersendiri bagi para administrator jaringan dalam menganalisis keamanan jaringannya secara tepat. Monitoring jaringan adalah suatu fungsi pengumpulan informasi dari manajemen jaringan (Wong, 1997). Tujuan dari monitoring jaringan adalah pengumpulan informasi yang berguna dari berbagai macam bagian dari jaringan sehingga jaringan tersebut dapat dikelola dan dikontrol dengan menggunakan informasi yang telah dikumpulkan tersebut. Monitoring jaringan dapat diterapkan dengan membangun sebuah aplikasi monitoring jaringan. Aplikasi inilah yang bertugas mengumpulkan informasi-informasi dari berbagai bagian atau peralatan dalam jaringan. Informasi yang ditampilkan bisa dalam bentuk numerik atau teks bisa juga dalam bentuk visual.

Monitoring koneksi pada jaringan dapat dilakukan setiap hari. Proses *login* merupakan salah satu indikator bahwa koneksi jaringan dalam keadaan baik, akan tetapi hal cara tersebut bukan merupakan cara efisien dalam memantau koneksi jaringan. Tersedia banyak aplikasi sederhana yang dapat digunakan administrator untuk membuat daftar alamat *IP Host* dan dideteksi (*ping*) secara periodik (Wong, 1997).

Jaringan (*network*) merupakan bagian dari sistem komunikasi data yang melibatkan satu atau lebih sistem komputer yang dihubungkan dengan jalur transmisi alat komunikasi membentuk sebuah sistem (Hartono, 2000). Salah satu keuntungan dari penggunaan jaringan komputer adalah kemampuan berbagi pakai sumber daya yang terdapat dan terhubung dalam jaringan komputer tersebut.

Keamanan Jaringan

Keamanan komputer adalah suatu cara untuk mencegah penyerang yang tidak mempunyai hak akses dan pakai terhadap sistem komputer dan jaringan (Howard, 1997). Keamanan ini bertujuan agar pemilik sistem informasi dapat menjaga sistem informasinya tidak disusupi oleh orang lain yang pada akhimya dapat merusak sistem. Adapun tipe dari penyusup ini dapat berupa :

a. *The Curious*
   Penyusup hanya sekedar ingin tahu tentang sistem dan data yang ada.
b. *The Malicious*
   Penyusup hanya merubah bentuk tampilan dan mengacak-acak sistem sehingga menjadi *down*, sehingga pemilik sistem mengeluarkan uang untuk memperbaiki sistemnya.
c. *The High-Profile Intruder*
   Penyusup bertujuan untuk mencari popularitas.
d. *The Competition*
   Penyusup sudah memanfaatkan sistem komputer yang disusupnya untuk keuntungan pribadi.

Dari tujuan penyusup dapat dipahami bahwa sistem keamanan komputer merupakan salah satu aspek penting dari sebuah sistem informasi. Tapi sangat disayangkan masalah ini sering kali kurang mendapat perhatian dari pada pemilik dan pengelola sistem informasi.

Dan seringkali masalah keamanan menjadi urutan yang kedua bahkan terakhir dalam prioritas hal-hal penting pada sistem informasi pada hal sistem informasi sudah menjadi *information-based society* (Howard, 1997). Dengan pemanfaatan perangkat lunak berbasis visual maka pemetaan terhadap lalu lintas jaringan lebih mudah digunakan.

PEMBAHASAN

Analisis

Metodologi yang digunakan dalam pembahasan *paper* ini adalah studi kasus, dalam analisisnya dikaji monitoring jaringan dengan menggunakan cara manual berbasis teks/numerik dan berbasis visual. Untuk monitoring jaringan berbasis teks/numerik digunakan perangkat lunak *Wireshark* sedangkan untuk analisis secara visual digunakan perangkat lunak *Inetvis (Internet Visual)*. *Capture* data dilakukan hari Rabu tanggal 13 April 2011 pukul 13.26 WIB di jaringan internal Institut Teknologi Bandung dengan menggunakan koneksi jaringan *wireless*. Data *IP* sebagai berikut:

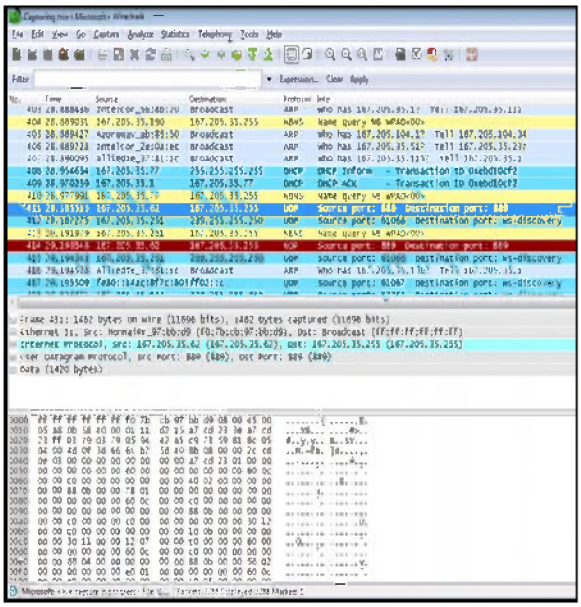
Tabel 1 Data *IP* yang digunakan dalam analisis

Komponen	No IP
IP Address	167.205.35.77
Subnet Mask	255.255.255.0
Defult Gateway	167.205.35.1
DNS Server	167.205.32.2 167.205.22.123

Capture Data Berbasis Teks/Numerik

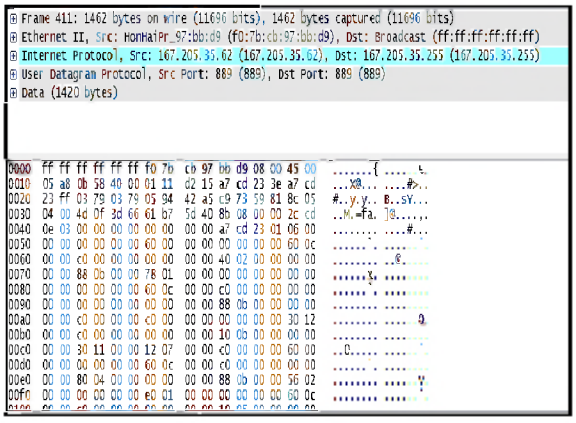
Wireshark merupakan salah satu aplikasi untuk menganalis paket jaringan dan protokol yang banyak digunakan di industri dan institusi pendidikan. Hal ini sangat mirip dengan *tcpdump,* namun memiliki *GUI front-end*, dan informasi lebih banyak dalam memilah dan menyaring pilihan. Selain itu, memungkinkan pengguna untuk melihat semua lalu lintas yang melewati jaringan *ethernet* (Akindeinde, 2009).

Berikut ini adalah analisa hasil dari *capture* berbasis teks/numerik yang dilakukan dengan menggunakan *wireshark*.



Gambar 10 Hasil *capture* berbasis teks/numerik

Hasil *capture* pada gambar 10 memperlihatkan daftar semua *capture* paket dari sumber menuju tujuan yang terjadi di lalu lintas jaringan. Contoh di atas memperlihatkan paket yang berasal dari IP 167.205.35.62 menuju 167.205.35.255 dengan *UDP* (*port* 889) sebagai protokolnya. Gambar 11 merupakan bagian detil dari paket *header IP* 167.205.35.62 dan isi dari paket dalam heksadesimal dan *ASCII*.



Gambar 11 Bagian detil dari paket *header* dan isi dari dari paket dalam heksadesimal dan *ASCII*

Dikarenakan keterbatasan dalam *capture* data teks untuk jaringan yang terinfeksi

malicious di jaringan ITB maka diambil hasil *capture* dari internet sebagai perbandingan.

```
01. GET /serial/index.php HTTP/1.1
02. Accept: */*
03. Accept-Encoding: gzip, deflate
04. User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1;
    Trident/4.0; SLCC2; .NET
05. CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
    Center PC 6.0)
06. Connection: Keep-Alive
07. Host: accord-component.ru
08. HTTP/1.1 200 OK
09. Server: nginx
10. Date: Wed, 30 Nov 2011 23:07:18
11. GMTContent-Type: text/html
12. Transfer-Encoding: chunked
13. Connection: keep-alive
14. X-Powered-By: PHP/5.3.2
15. Content-Encoding: gzip
```

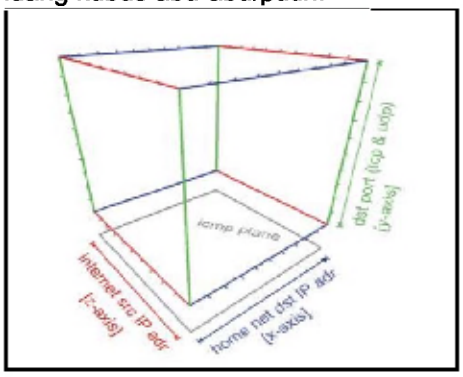
Gambar 12 Hasil capture berbasis teks yang mengindikasikan adanya *malicious*. Sumber: (Tasevski, 2012)

Pada gambar 12 melalui situs *accord-component.ru*, menunjukkan bahwa pengguna telah mengunjungi situs yang berbahaya. *Wiresharsk* dapat mengidentifikasi situs atau lalu lintas mana saja yang telah teridentifikasi oleh situs berbahaya tersebut. Kekurangan dari *tools* berbasis teks ini adalah *user* harus terlebih dahulu mengetahui nama domain atau alamat *IP* dari situs yang dianggap berbahaya. Diperlukan *tools* tambahan seperti *Netresec's Network Miner 2.1* untuk mendapatkan *file* yang akan dianalisis sehingga dalam hal ini monitoring keamanan jaringan menjadi tidak efektif. Selain itu dikarenakan informasi yang ditampilkan dalam bentuk teks/numerik, sulit dipahami terutama bagi *user* yang bukan ahli dalam jaringan. Hal ini sangat berbeda apabila menggunakan *tools* berbasis visual, *user* hanya tinggal melihat representasi gambar anomali berupa titik-titik padat berbentuk persegi atau garis diagonal yang mengidentifikasikan adanya *malicious*.

Capture Data Berbasis Visual

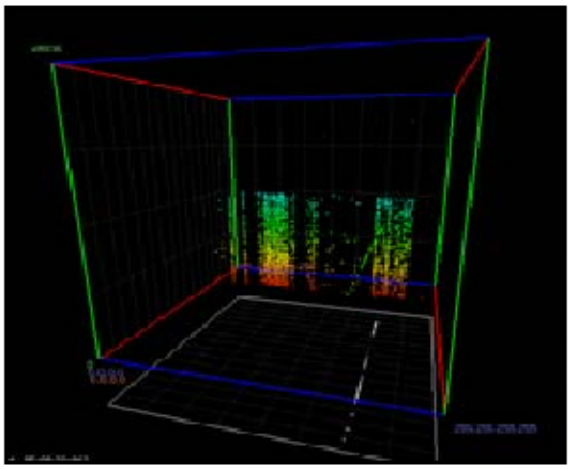
InetVis adalah sebuah visualisasi *scatter-plot 3-D* untuk lalu lintas jaringan. *InetVis* diadopsi dari *Cube Stephen Lau*, *Spinning Cube of Potential Doom*. Representasi *InetVis* sebagai berikut

- Alamat tujuan (*home network*) diplot sepanjang sumbu x berwarna biru (horizontal)
- Sumber alamat (*external Internet range*) diplot sepanjang sumbu z berwarna merah (kedalaman)
- Port (*TCP dan UDP*) diplot sepanjang sumbu y berwarna hijau(vertikal)
- Lalu lintas *Internet Control Message Protocol (*ICMP*)* diplot di bawah *TCP/UDP* bidang kubus abu-abu/putih.



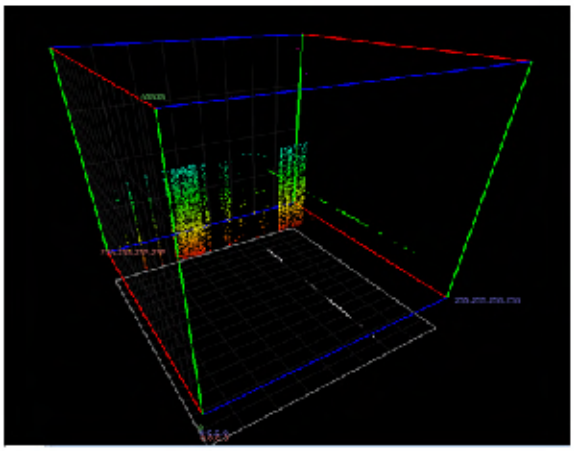
Gambar 13 Representasi grafis *InetVis*

Hasil *capture* berbasis visual menggunakan *InetVis* pada pukul 13.17 WIB.



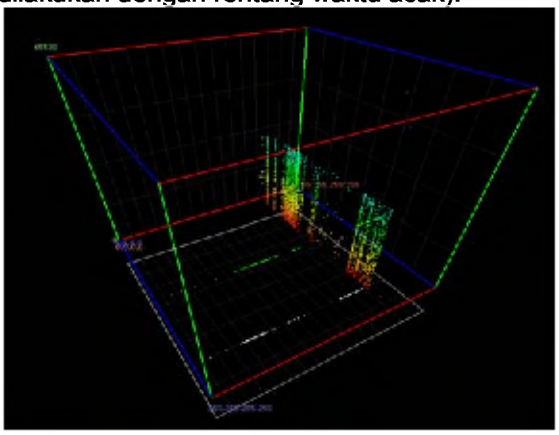
Gambar 14 Hasil *capture* berbasis visual (1)

Hasil *capture* berbasis visual menggunakan *InetVis* pada pukul 13.18 WIB (selang waktu 60 detik dari hasil pengamatan pertama).



Gambar 15 Hasil *capture* berbasis visual (2)

Hasil *capture* berbasis visual menggunakan *InetVis* pada pukul 13.32 WIB (pengamatan dilakukan dengan rentang waktu acak).

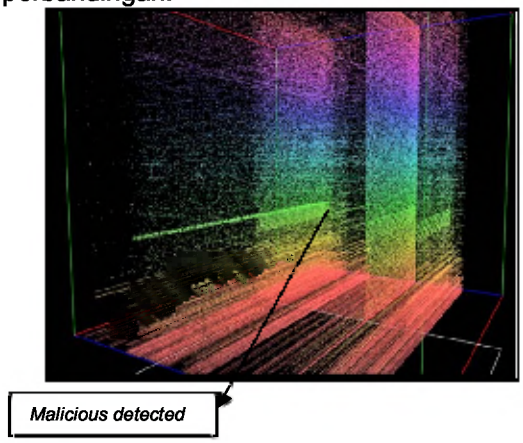


Gambar 16 Hasil *capture* berbasis visual (3)

Hasil *capture* paket pada gambar 14 sampai 16 memperlihatkan lalu lintas paket yang terjadi di jaringan. IP *range* tidak ditentukan, jadi semua IP pada jaringan tersebut di *capture*. Jangkauan *port* dari 0-65535 (*default*). Berdasarkan hasil pengamatan pertama dan kedua dapat dianalisis bahwa dalam waktu 60 detik lalu lintas jaringan dapat dimonitoring dengan cepat karena informasi disajikan secara visual. Lalu lintas paket dalam jaringan dibedakan hanya dengan melihat tampilan warna pada hasil *capture*.

Gambar 14 sampai dengan 16 menggambarkan pola *plotting InetVis*. Proses paket data dalam jaringan dibaca dengan bantuan *libpcap* sebagai *file library* dari *InetVis*. Lalu lintas data yang diplot mencakup *TCP*, *UDP* dan *ICMP* yang terdapat pada *IP layer*. *ICMP* digambarkan pada bagian bawah kubus (*ICMP plane*) sementara *TCP* dan *UDP* digambarkan dengan gambar 3 dimensi dalam kubus. Lalu lintas data dipresentasikan dengan warna titik dalam kubus yang menggambarkan port tujuan dari sebuah paket, *port* sumber atau jenis protokol, alamat tujuan atau sumber dari paket. *ICMP* dipresentasikan dengan tititk-titik berwarna putih/abu-abu yang terlihat pada bagian bawah kubus, *UDP* atau *TCP* berwarna hijau sebagai port tujuan. *IP* tujuan dipresentasikan dengan warna biru sementara *IP* sumber berwarna merah. Warna dan ukuran masing-masing titik dapat dirubah berdasarkan kebutuhan visualisasi.

Dikarenakan keterbatasan dalam *capture* data visual untuk jaringan yang terinfeksi *malicious* di jaringan ITB maka diambil hasil *capture* dari internet sebagai perbandingan.



Gambar 16 Hasil capture berbasis visual yang mengindikasikan adanya *malicious*.
Sumber: (Schwagele, 2009)

Gambar 16 memperlihatkan sejumlah paket yang ada di jaringan. Screenshot menampilkan 8.200.000 paket. Berbagai tanda berbahaya dapat dilihat pada gambar. *Malicious* dapat dideteksi pada garis hijau berbentuk persegi panjang dengan plot padat. Pada gambar nampak garis hijau tebal yang menandakan adanya penyusupan antar host dalam jaringan yang terjadi secara intensif dalam interval waktu tertentu. Hal ini ditunjukkan oleh kepadatan (*density*) atau ukuran dari titik-titik berwarna warna hijau pada sumbu-x.

Monitoring jaringan dengan visual dapat mendeteksi kegiatan yang membahayakan jaringan dengan cepat, hal ini berbeda dengan

cara manual (teks/numerik) yang hanya dapat memonitoring lalu lintas jaringan saja.

Sehubungan banyaknya data mengalir melalui jaringan yang digunakan dan jika data tersebut dapat dilihat dalam bentuk visualisasi, akan memudahkan melihat sebuah lalu lintas jaringan yang saling mempengaruhi satu dengan lainnya sebagaimana yang dijelaskan pada analisis di atas bahwa sebuah penyusupan dalam jaringan dapat dideteksi dalam waktu yang sangat cepat.

Masa depan visualisasi data merupakan sesuatu hal yang menjanjikan mengingat begitu banyak upaya yang dilakukan dalam mengembangkan perangkat lunak monitoring lalu lintas jaringan seperti berbagai perangkat lunak yang disebutkan di awal. Tantangan dalam mengembangkan perangkat monitoring jaringan adalah membuatnya lebih interaktif dan dinamis sama halnya dengan display *platform* yang tentunya dapat meningkatkan kualitas visualisasi data itu sendiri.

KESIMPULAN

Setelah dilakukan penelitian tentang analisis visualisasi data keamanan jaringan, ternyata dapat diambil kesimpulan sebagai berikut:

1. Monitoring jaringan berbasis visual berkembang dilatar belakangi oleh jumlah data yang besar yang harus diamati dalam lalu lintas jaringan.
2. Hasil pengamatan dengan menggunakan visual dapat memeriksa lalu lintas jaringan dan mendeteksi *anomali* jauh lebih cepat dari pada dengan cara manual (berbasis teks/numerik).
3. Melalui visualisasi, data dapat direpresentasikan dalam bentuk visual sedemikian rupa sehingga memungkinkan *user* lebih mudah untuk mengidentifikasi aktivitas berbahaya yang terjadi dalam jaringan.

DAFTAR PUSTAKA

Akindeinde, Olu, 2009, *Security Analysis And Data Visualization,* Lagos, Nigeria.

Howard, John D.,1997, An Analysis of Security Incidents on the Internet 1989-1995, PhD thesis, Carnegie Mellon University.

Hartono, 2000, Pengenalan Komputer, Yogyakarta, Andi.

Krasser, Sven; Conti Gregory, et.al. (2005): Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization, in Workshop on Information Assurance, New York

Mihaly, Balazs Attila. (2008): Visualization techniques for networking data, [Online], Tersedia: http://hype-free.blogspot.com/2008/05/visualization-techniques-for-networking.html, Akses 18 April 2011, 23.00 WIB

Schwagele, Chris., 2010, *dotNetVis: An enhancement and.NET re-implementation of the InetVis Data*, Thesis, Rhodes University, Grahamstown, South Africa.

Schwagele, 2009. dotNetVis: A re-implementation and enhancement of InetVis, [Online], Tersedia: http://www.cs.ru.ac.za/research/g07s3491/index-1.html Akses 27 April 2011, 22.00 WIB.

Tasevski, 2012, Identify Possible Infection of Malware Into the Wireshark Capture File, [Online], Tersedia: http://predragtasevski.com/malware/malware-wireshark-capture/ Akses 10 Februari 2012, 22.00 WIB

Tri, Dang T. et al, Security Visualization For Peer To Peer Resource , *International Journal on Computer Science and Engineering*, Vol.1, No.2, 2009, pp. 47-55.

Wong, 1997, Network Monitoring Fundamentals and Standards, [Online], Tersedia: http://www.cse.ohio-state.edu/~jain/cis788-97/ftp/net_monitoring/Network Monitoring.htm. Akses 16 April 2011, 13.00 W IB