Aplikasi Teori Graf dalam Keamanan Jaringan Komputer

Akmal Fadlurohman,13515074
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13515074@stei.students.itb.ac.id,fadlurohmanakmal@rocketmail.com

***Abstrak*—Salah satu komponen yang harus diperhatikan dalam merancang jaringan komputer yang aman adalah *network monitoring* atau pengawasan terhadap jaringan. Banyak pengguna internet awam yang komputernya tanpa disadari telah terinfeksi *malware-malware* jahat. Aplikasi-aplikasi yang digunakan oleh *user* seringkali menyembunyikan lalu lintas data mereka dengan menggunakan nomor seri *port* yang illegal atau enkripsi-enkripsi yang terspesifik. Dengan *Traffic Dispersion Graph(*TDG), penulis menyajikan suatu cara untuk memonitor lalu lintas data dan mengidentifikasi *malware* pada jaringan internet untuk meningkatakan keamanan jaringan. TDG memodelkan interaksi sosial setiap simpul dengan simpul lainnya diamana sisi-sisi didalamnya mewakili interaksi yang berbeda-beda antar simpul.**

***Kata Kunci*—Keamanan jaringan, Lalu Lintas Data, *Traffic Dispersion Graph(TDG), malware*.**

I. PENDAHULUAN

Kemajuan teknologi dan informasi yang pesat membuat informasi dapat beredar dengan cepat. Informasi-informasi yang kita butuhkan dengan mudah dan cepat bisa kita dapatkan. Beragam penemuan-penemuan muncul berkat kemajuan teknologi informasi.

Salah satu teknologi informasi yang berkembang pesat ialah *interconnected network* atau yang biasa disebut dengan internet. Sekarang ini, internet menjadi kebutuhan dasar manusia. Setiap aktivitas manusia dapat terhubung satu dengan yang lainnya melalui internet.

Orang-orang biasa mengakses internet menggunakan komputer pribadi mereka. Terkadang, pengguna komputer yang awam tidak berhati-hati ketika mereka mengakses internet untuk mengunduh sesuatu seperti musik,gambar,dan film. Tanpa mereka sadari, unduhan mereka seringkali membawa malware dari internet yang dapat membahayakan sistem komputer mereka. Instalasi aplikasi-aplikasi illegal dan bajakan juga dapat menyumbang terhadap jumlah malware yang menginfeksi sistem komputer pengguna. Aplikasi-aplikasi illegal yang diinstal pengguna telah dimodifikasi oleh penyedia aplikasi illegal dengan memasukkan malware-malware yang menguntungkan mereka.

Malware-malware yang telah menginfeksi sistem komputer dapat mengirimkan informasi-informasi yang dimiliki pengguna yang bersifat pribadi ke pihak tidak bertanggung jawab. Malware-malware ini menyamarkan diri menjadi berbagai jenis proses dalam sistem komputer. Komputer yang telah terinfeksi malware memiliki beberapa tanda berikut:

1. Kinerja lambar.
2. Program dan sistem sering mengalami *crash.*
3. Memori penyimpana berkurang drastis.
4. Koneksi internet yang lambat secar terus menerus.
5. Homepage pada browser berganti tanpa kita ketahui.

Gambar 1: Peringatan Bahaya Infeksi Malware saat mengunjungi sebuah situs (sumber: http://www.troublefixers.com/delete-malware-in-windows/)

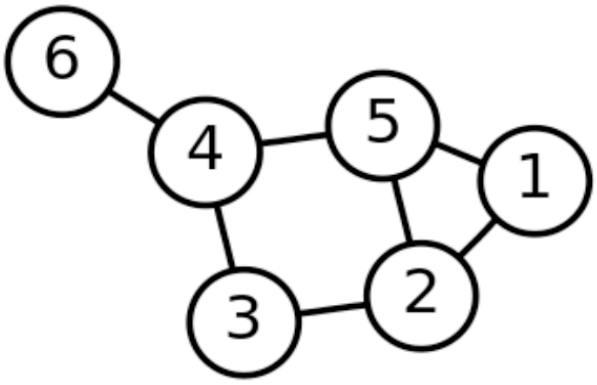
Sebuah cara pendeteksian terhadap malware-malware ini sangat diperlukan. Pada makalah ini, dengan *Traffic Dispersion* Graph (TDG) dan beberapa teori metode identifikasi malware penulis menyajikan cara mengenali malware dalam suatu sistem komputer dengan mengamati lalu lintas data pada jaringan.

II. TEORI DASAR

2.1. Graf

Graf adalah representasi objek-objek yang dinyatakan dengan noktah dan hubungan antarobjek yang dinyatakan dengan garis. Noktah tersebut disebut "simpul" atau node. Garis tersebut disebut "sisi" atau edge. Graf biasanya dinyatakan dengan G = (V,E), dimana V adalah himpunan tidak kosong dari simpul-

simpul, dan E adalah himpunan sisi.



Gambar 2: Contoh graf dengan 6 simpul dan 7 sisi (Sumber: https://id.wikipedia.org/wiki/Berkas:6n- graf.svg)

2.2. Klasifikasi Graf

Graf dapat diklasifikasi ke dalam beberapa jenis. Berdasarkan ada tidaknya gelang atau sisi ganda, graf dapat dibedakan menjadi graf sederhana dan graf tak-sederhana. Graf sederhana adalah graf yang tidak memiliki sisi ganda dan gelang. Graf tak-sederhana terbagi atas graf ganda dan graf semu. Graf ganda adalah graf yang memiliki sisi ganda. Graf semu adalah graf yang memiliki gelang.

Berdasarkan jumlah simpul suatu graf, graf dapat dibedakan menjadi graf berhingga dan graf tak berhingga. Graf berhingga adalah graf yang jumlah simpulnya berhingga. Graf tak berhingga adalah graf yang jumlah simpulnya tidak berhingga.

Berdasarkan arah sisi, graf dibedakan menjadi graf tak berarah dan graf berarah. Graf tak berarah adalah graf yag sisinya tidak mempunyai orientasi arah. Sementara, graf berarah adalah graf yang sisinya memiliki orientasi arah. Pada suatu sisi di graf berarah, simpul asal busur disebut simpul asal dan simpul yang ditunjuk oleh busur disebut simpul terminal.

2.3. Terminologi Graf

Terdapat beberapa istilah yang digunakan dalam teori graf.

1. Bertetangga

Dua simpul yang dihubungkan dengan sebuah sisi dapat dikatakan bertetangga.

2. Bersisian

Simpul-simpul yang terhubungkan dengan sisi e dapat dikatakan bersisian dengan e

3. Derajat

Pada graf tak berarah, derajat suatu simpul adalah jumlah sisi yang bersisian dengan simpul tersebut.

Pada graf berarah, derajat simpul v dinyatakan dengan:

$d_{in}(v)$ = jumlah busur yang masuk ke v

$d_{out}(v)$ = jumlah busur yang keluar ke v

dan $d(v) = d_{in}(v) + d_{out}(v)$

4. Lintasan

Lintasan adalah barisan selang-seling antara simpul dan sisi dari simpul awal Vo ke simpul tujuan Vn

5. Terhubung

Dua simpul dikatakan terhubung jika ada lintasan dari simpul awal ke simpul akhir.

6. Simpul terpencil

Simpul terpencil adalah simpul yang tidak memiliki sisi yang bersisian dengannya.

7. Graf kosong

Graf kosong adalah graf yang himpunan sisinya adalah himpunan kosong.

8. Siklus atau sirkuit

Siklus atau sirkuit adalah lintasan yang berawal dan berakhir pada sebuah simpul.

2.4. Protokol Pertukaran Data

Jaringan *Internet Protocol* menggunakan dua protokol umum untuk melakukan pertukaran data. Protokol tersebut adalah *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP). Protokol TCP memiliki orientasi terhadap koneksi. Saat sebuah koneksi terbentuk, pertukaran data dapat dilangsungkan dalam dua arah. Protokol ini digunakan dalam HTTP, HTTPS, FTP, dan SMTP. Protokol UDP tidak berorientasi terhadap koneksi. Saat sebuah aplikasi mengharuskan mengirim data ke aplikasi lain, hubugnan anatar kedua aplikasi tersebut berakhir setelah semua data terkirim, dengan kata lain UDP memiliki sifat satu arah.Protokol ini digunakan dalam DNS, DHCP, VOIP, dll.

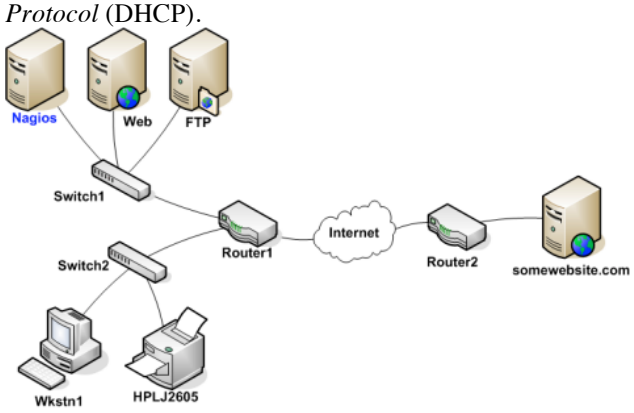
2.5. Nomor Port

Nomor port adalah nomor pengalamatan yang digunakan saat transfer data dalam internet terjadi. Nomor port biasa digunakan untuk memperspesifik alamat tujuan dari data ketika sebuah data masuk. Setiap aplikasi yang bekerja pada suatu komputer memiliki nomor port yang berbeda. Saat data masuk, data ini diteruskan oleh komputer ke aplikasi yang dispesifik oleh pengirim data menggunakan nomor port yang digunakan oleh aplikasi tersebut.Hal ini juga berlaku sama saat sebuah aplikasi dalam komputer mengirim data ke komputer lain.

2.6. Network Host

Network Host atau Host adalah komputer atau perangkat lainnya yang terhubung dengan internet. Host dapat berbagi informasi, servis, dan berbagi penggunaan aplikasi ke host lain. Setiap host dalam jaringan diwakiliki oleh sebuah simpul. Host dapat berperan baik sebagai *server* maupun *client* dalam jaringan. Saat sebuah komputer membuka sebuah situs di internet, komputer tersebut sedang berinteraksi sebagai *client* dengan situs tersebut yang merupakan *client*. Host juga dapat berperan dalam komputasi jaringan *peer to peer* dimana setiap host yang merupakan simpul dalam jaringan memiliki bagian yang sama sebagai anggota jaringan komputer. Setiap host dalam jaringan yang sama memiliki alamat IP yang berbeda dengan host lain yang juga terdapat dalam satu jaringan. Alamat IP dapat di-*assign* ke host secara manual oleh pihak administrator jaringan atau secara otomatis diberikan oleh *Dynamic Host Configuration*

Protocol (DHCP).



Gambar 3 Hubungan antar *host* dalam jaringan komputer (sumber : https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/networkreachability.html)

2.7. Malware

Malware atau *Malicious Software* adalah sebuah program yang didesain untuk merusak atau melakukan hal-hal yang tidak diinginkan terhadap sistem komputer. Virus, *worms*, *trojan horses* , dan *spyware* termasuk kedalam malware. *Spyware* dapat mengumpulkan data yang dimiliki suatu host seperti situs-situs yang biasa dikunjungi dan bahkan informasi rahasia seperti nomor kartu kredit.

III. TRAFFIC DISPERSION GRAPHS

3.1. Definisi

Traffic Dispersion Graph (TDG) adalah graf yang merepresentasikan hubungan interaksi dari sekelompok simpul. Pada jaringan *Internet Protocol* (IP), setiap simpul dalam jaringan memiliki IP address yang berbeda-beda. TDG pada jaringan IP memiliki peran mencatat pertukaran paket data dari satu simpul ke simpul lain. Definisi TDG secara formal adalah graf yang memiliki kemampuan untuk berevolusi terhadap waktu dan ruang seiring berlangsungnya interaksi suatu simpul dalam graf dengan simpul lain yang juga terdapat dalam graf. Sisi yang terbentuk dalam TDG bersifat implisit sementara yang berarti suatu sisi antara 2 simpul dapat terbentuk dalam interval waktu tertentu dan dapat pula hilang bergantung pada waktu pengamatan.

3.2. Sisi pada TDG

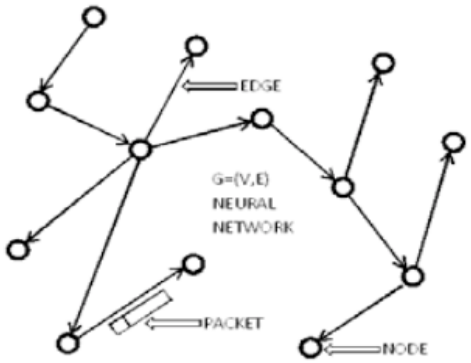
Sisi-sisi pada *Traffic Dispersion Graph* (TDG) merupakan sisi yang berarah. Arah setiap sisi ini menunjukkan arah komunikasi yang sedang berlangsung diantara dua simpul dengan satu simpul sebagai pengirim paket data dan simpul lainnya sebagai penerima. Setiap simpul dalam TDG mewakili interaksi yang berbeda diantara dua simpul. Saat sebuah simpul u mengirim paket data ke simpul v dalam suatu waktu pengamatan maka sebuah sisi (u,v) terbentuk dalam kurun waktu pengamatan tersebut. Sisi yang terbentuk ini memiliki jenis *Edge on First Packet* (EFP). EFP digunakan dalam transfer data antara dua buah simpul yang menggunakan protokol UDP. Transfer data dengan protokol TCP menggunakan prinsip "*3-Way Handshake"*(SYN,SYN-ACK,ACK). Saat sebuah simpul u mengirimkan paket data ke simpul v menggunakan protokol TCP, maka sebuah sisi berarah (u,v) terbentuk. Sisi berarah (u,v) ini memiliki jenis *Edge on First SYN Packet (EFSP)*. Dalam makalah ini, sisi-sisi yang terbentuk dalam TDG bergantung pada jenis nomor port yang digunakan sebuah simpul dimana simpul tersebut mewakili sebuah aplikasi .

3.3. Pembentukan TDG

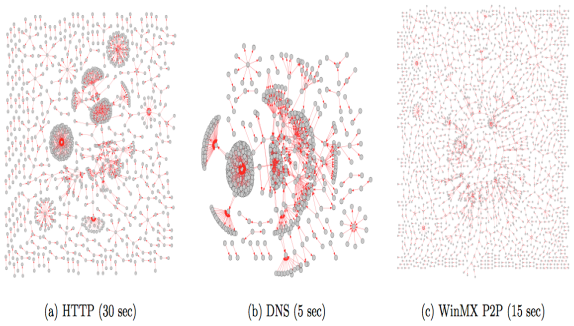
Saat sebuah aplikasi menggunakan protokol TCP dengan nomor port tertentu mengirimkan data ke aplikasi lain atau host lain dengan nomor port berbeda, maka terbentuk simpul berjenis EFSP. Saat aplikasi menggunakan protokol UDP, maka terbentuk simpul berjenis EFP. Jenis simpul yang digunakan ini membantu TDG "merekam" semua ciri-ciri dari aplikasi yang menggunakan nomor port tertentu. Jika didapati ciri-ciri dari suatu aplikasi berbeda dengan ciri-ciri aplikasi tersebut yang sebelumnya pernah dicatat oleh TDG, dapat dimungkinkan aplikasi tersebut terinfeksi *malware.*

3.4. Visualisasi TDG

Visualisasi TDG dibatasi oleh besar volume lalu lintas data dalam satu aliran. Dalam gambar, setiap simpul memiliki derajat yang berbeda-beda. Arah sisi dari satu simpul ke simpul lain juga berbeda. Sisi ini menunjukkan komunikasi antara satu aplikasi dengan aplikasi lainnya melalui nomor port yang berbeda. Perbedaan derajat dan arah sisi setiap simpul ini menunjukkan sifat aplikasi yang berbeda-beda. Aplikasi yang menggunakan interaksi *client-server* memiliki derajat keluar besar untuk sisi *client* dan derajat 0 untuk sisi server. Aplikasi yang menggunakan protokol *peer to peer* (P2P) memiliki jumlah derajat setiap simpul sama.



Gambar 4: *Traffic Dispersion Graph*
(Sumber: A.S. Cheema, J. Kohli, K. Arora, S. Gupta, S.S. Ahmed. Network Security Using Graph Theory. In International Journal of Innovations in Engineering and Technology (IJIET), pages 131-138,2013)



Gambar 5 : Visualisasi TDG
(Sumber: M. Iliofotou, P. Pappu, M. Faloutsos, M. Mitzenmacher, S. Singh, and G. Varghese. Network monitoring using traffic dispersion graphs (tdgs). In In ACM Internet Measurement Conference (IMC), pages 315–320, 2007)

IV. IDENTIFIKASI MALWARE

4.1. DNS *Sinkhole*

Fitur *firewall* pada sebuah komputer telah diatur agar dapat meneruskan semua lalu lintas data yang keluar dari sistem dam membatasi lalu lintas data yang masuk. Malware-malware memanfaatkan pengaturan pada sistem *firewall* komputer inang ini dengan menginisiasi lalu lintas data keluar agar dapat terhubung dengan *Command Center* (CC) penyerang atau dalam istilah lain "Pemilik Asli Malware". Strategi ini lebih memungkinkan untuk diterapkan karena jika pihak penyerang yang menginisiasi koneksi dengan komputer inang atau mengirim subuah paket internet ke pakket internet, sistem *firewall* komputer inang akan dapat dengan mudah mendeteksi serangan ini. Pengguna komputer yang dijadikan inang oleh malware kebanyakan tidak memiliki *static* IP address sehingga mekanisme pengiriman paket data oleh malware dapat dilakukan dengan lebih mudah. Untuk menginisiasi koneksi dengan CC, malware mencari *domain* dari IP address yang telah terdaftar sebagai milik CC dengan melakukan query *domain* tersebut melalui server DNS. Ketika IP address dari *domain* telah ditemukan, malware kemudian membangun koneksi ke CC dengan menjalankan program yang telah diatur pada dirinya. Malware lebih menyukai sistem pencarian *domain* daripada pencarian IP address secara langsung karena beberapa alasan berikut:

1. Malware meniru kebiasaan manusia saat mengakses sebuah situs menggunakan *Uniform Resource Locator* (URL).
2. Penggunaan registrasi DNS secara dinamik untuk mengihindari pendeteksian IP address penyerang.
3. Untuk mempermudah mendapatkan IP address baru CC setelah kurun waktu tertentu dikarenakan IP address CC atau penyerang yang dapat berubah-ubah.

DNS *sinkhole* adalah sistem dimana DNS service komputer pengguna yang terhubung ke suatu server DNS menyelesaikan query-query DNS. Server DNS tidak akan memberikan IP address dari domain yang diquerikan jika domain tersebut terdaftar dalam *blacklist* penyedia DNS. Saat sebuah malware mengquerikan sebuah *domain,* sistem DNS telah dikonfigurasi untuk mengatur ulang queri malware (*redirect*) ke sebuah IP address yang memungkinkan pakar-pakar analisis malware menggunakan IP address tersebut sebagai *sinkhole* untuk mengisolasi dan mencegah malware mendapatkan IP address dari CC. Saat sebuah malware berhasil diisolasi, semua lalu lintas data yang masuk dan keluar dari komputer inang dapat diamati dan dianalisis oleh para pakar. Saat pengguna tidak sedang menggunakan komputer mereka tetapi di komputer mereka terdapat lalu lintas data, dapat diperkirakan sebuah malware sedang bekerja di komputer tersebut.

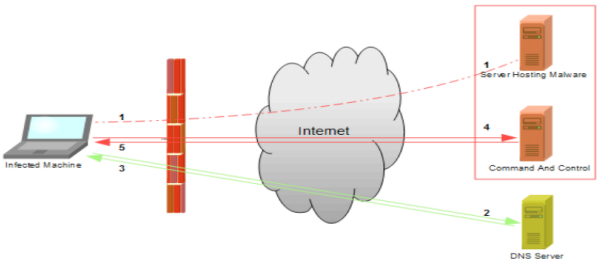
Sistem DNS *sinkhole* juga sering disebut sebagai sistem DNS *redirection* karena cara kerjanya yang mengatur ulang arah lalu lintas data yang mencurigakan ke subuah IP address yang berfungsi sebagai *sinkhole*. Sistem DNS *sinkhole* juga sering disebut sebagai *Blackhole server, internet sinkhole,* atau *sinkhole server*.

4.2. *Live Traffic Analysis*

Live Traffic Analysis (LTA) adalah analisis secara *real-time* terhadap lalu lintas data yang dibuat oleh malware baik itu untuk menerima paket data atau mengirim paket data ke CC. Analisis terhadap lalu lintas data ini dapat digunakan terhadap malware yang menggunakan *Secure-Socket Layer* (SSL) dalam menerima dan mengirimkan data. Sistem yang digunakan dalam LTA dapat meneruskan paket data yang dikirim malware ke CC dan juga meneruskan paket data dan perintah yang dikirimkan CC ke malware. Sistem LTA bekerja seperti *proxy* sehingga tidak mengganggu koneksi malware ke CC. Sistem ini dapat membantu para pakar malware mempelajari jenis data-data yang dirimkan malware dari komputer inang dan diterima malware dari CC tanpa diketahui pihak CC.

Tujuan dari menganalisis perilaku malware dalam membentuk lalu lintas datanya secara *real-time* adalah untuk memahami dampak-dampak yang timbul saat sebuah komputer terinfeksi malware, cara memperbaiki komputer yang terinfeksi, cara membersihkan malware dari komputer inang, dan mengidentifikasi *vulnerability* atau kelemahan dari sistem komputer sehingga kedepannya tingkat keamanan sistem dapat ditingkatkan.
Sistem *Live Analysis Traffic* (LTA) dapat membantu meningkatkan keamanan jaringan dengan berbegai alasan sebagai berikut:

1. Organisasi yang menjadi korban serangan malware dapat mengetahui aktivitas penyerang dan menemukan penyerangnya melalui alamat IP.
2. Pakar dan analis dapat menilai perintah dan program yang digunakan penyerang untuk menjalankan malware.
3. Mengetahui persebaran malware di komputer-komputer lain
4. Mengamati perilaku malware yang menggunakan koneksi SSL dalam koneksi dengan penyerang

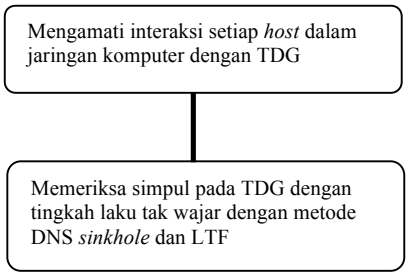


Gambar 5 Lalu Lintas Data Malware (Sumber: Sourabh Saxena. *Demystifying Malware Traffic*. SANS Institute InfoSec Reading Room, page 8, 2016)

V. KESIMPULAN

Aplikasi teori graf dalam *Traffic Dispersion Graph* (TDG) sangat berguna untuk membuat sistem pengawasan lalu lintas data dalam suatu jaringan. TDG mencatat interaksi host dengan host lainnya dalam jaringan komputer dimana setiap host adalah simpul dan sisi-sisinya adalah interaksi-interaksi yang terjadi. TDG membantu dalam mendeteksi keberadaan malware dalam sebuah sistem komputer dengan mengamati simpul-simpul dengan perilaku tak wajar.

Simpul-simpul tak wajar yang telah ditemukan dengan TDG kemudian diperiksa secara teliti menggunakan metode DNS *sinkhole* dan *Live Traffic Analysis* (LTF) untuk menentukan apakah suatu simpul benar-benar terinfeksi oleh malware dan jenis malware yang menginfeksi. Setelah malware teridentifikasi, solusi perbaikan terhadap kerusakan-kerusakan yang ditimbulkan oleh malware dapat ditentukan. Dalam diagram, proses kerja sistem pendeteksi malware adalah sebagai berikut:



REFERENCES

[1] Rinaldi Munir, *Diktat Kuliah IF1220: Matematika Diskrit*. Bandung: Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung,2006.

[2] M. Iliofotou, P. Pappu, M. Faloutsos, M. Mitzenmacher, S. Singh, and G. Varghese. *Network monitoring using traffic dispersion graphs* (tdgs). In In ACM Internet Measurement Conference (IMC), pages 315–320, 2007.

[3] A.S. Cheema, J. Kohli, K. Arora, S. Gupta, S.S. Ahmed. *Network Security Using Graph Theory*. In International Journal of Innovations in Engineering and Technology (IJIET), pages 131-138,2013.

[4] Sourabh Saxena. *Demystifying Malware Traffic*. SANS Institute InfoSec Reading Room, pages 1-8, 2016.

[5] E. Garrison Walters, *Essential Guide to Computing*, page 149, Prentice Hall PTR, 2001.

[6] http://www.diffen.com/difference/TCP_vs_UDP Waktu akses: 9 Desember 2016 pukul 09.15 WIB

[7] http://techterms.com/definition/malware Waktu akses: 9 Desember 2016 pukul 10.00 WIB

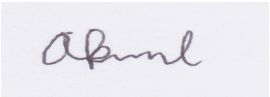
[8] https://www.lifewire.com/port-numbers-on-computer-networks-817939 Waktu akses: 9 Desember 2016 pukul 10.30 WIB

[9] https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/ Waktu akses : 9 Desember 2016 pukul 13.00 WIB

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 8 Desember 2016



Akmal Fadlurohman 13515074