# Aplikasi Graf untuk Mendeteksi Serangan Cyber Secara Real-Time

Erma Safira Nurmasyita (13516072)
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
*13516072@std.stei.itb.ac.id*

***Abstrak*—Kejahatan cyber merupakan kasus kriminal yang berkembang dengan pesat. Kasus ini yang sangat sulit diidentifikasi karena memiliki beberapa faktor, yaitu: pelaku kejahatan dapat berasal dari belahan dunia manapun, besarnya volume log data sebuah jaringan, dan kompleksnya deteksi kerentanan dalam jaringan cyber. Untuk mengurai kerumitan analisis dan pemantauan keamanan cyber, digunakan visualisasi data dengan pemodelan graf jaringan komputer. Pada makalah ini akan dijelaskan mengenai pemodelan jaringan komputer dengan teori graf dan metode analisis graf untuk mendeteksi serangan cyber dan mengatasi kerentanan sistem keamanan jaringan secara real-time.***

***Kata Kunci*—cyber, network, host, traffic, Internet Protocol, phishing**

## I. PENDAHULUAN

Dunia pada masa kini merupakan dunia yang saling terhubung. Terdapat milyaran koneksi yang menghubungkan perangkat dari setiap penjuru dunia. Batas antara dunia nyata dengan dunia maya menjadi semakin tipis. Semakin banyak informasi pribadi pengguna di dunia nyata, bahkan informasi vital, yang disimpan dalam database *online*.

Peningkatan konektivitas berbanding lurus dengan peningkatan kriminalitas di dunia *cyber*. Pada masa kini, kasus kriminal *cyber* membentuk sebuah jaringan yang kompleks dalam mempertemukan orang-orang dari seluruh dunia secara *real-time* untuk melakukan kejahatan dalam skala besar.

Keamanan suatu jaringan komputer merupakan sebuah sistem yang vital. Sistem ini berinteraksi langsung dengan pertahanan terluar komputer, sehingga rentan terhadap berbagai risiko kriminal berupa ancaman dan bahaya serangan *cyber*. Penjahat *cyber* mengerahkan berbagai metode untuk menemukan celah dari sistem pertahanan ini. Mereka mengeksploitasi kerentanan sistem dan mencari jalan masuk untuk mencuri informasi, mengganggu, menghancurkan, atau mengancam penyampaian layanan penting demi keuntungan sepihak. Jaringan serangan *cyber* tersebar luas dan selalu berkeliaran untuk menyerang jaringan organisasi.

Dengan meningkatnya konektivitas dan membesarnya jaringan kriminal *cyber*, data dari jaringan komputer juga semakin kompleks. metode Dibutuhkan analisis yang komperhensif untuk menyeleksi setiap koneksi yang dicurigai melakukan anomali.

Untuk mempermudah analisis data kompleks berukuran besar, dibutuhkan visualisasi data. Visualisasi dapat dimodelkan dengan graf jaringan komputer yang dinamis sesuai *real-time*. Dengan pemodelan graf, aktivitas mencurigakan suatu *host* dapat dengan mudah terdeteksi dan dilacak, menandainya sebagai ancaman, kemudian mengambil tindakan berupa pemblokiran. Dari analisis serangan ini, kerentanan dari sistem keamanan dapat segera ditindaklanjuti.

## II. TEORI DASAR

### *2.1. Teori Graf*

Graf adalah struktur diskrit yang mengandung sekumpulan objek yang dihubungkan dengan busur. Graf digunakan untuk merepresentasikan objek diskrit beserta hubungan antara objek tersebut.

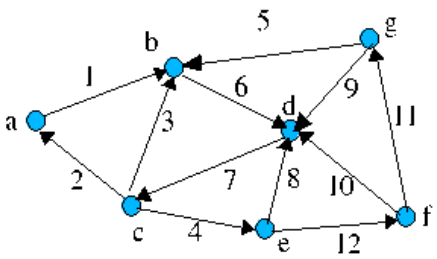
Secara matematis, graf didefinisikan sebagai pasangan himpunan (V,E) dituliskan dengan notasi G = (V,E), yang dalam hal ini:

V adalah himpunan tidak kosong dari simpul (*vertices* atau *nodes*) = {v1, v2, .., vn}, dan

E adalah himpunan sisi (*edges* atau *arcs*) yang menghubungkan sepasang simpul = {e1, e2, .., en}
(Rinaldi Munir, 2006 : VIII – 2).

V dinyatakan tidak boleh kosong, sedangkan E boleh kosong, sehingga sebuah graf dimungkinkan tidak memiliki sisi, tetapi simpulnya harus ada minimal satu. Sebuah graf yang hanya terdiri dari sebuah simpul dinamakan Graf Trivial.

Secara geometris, graf digambarkan sebagai kumpulan titik (simpul) di dalam sebuah bidang yang dihubungkan dengan sekumpulan garis (sisi).




V = {a,b,c,d,e,f,g}
E = {1,2,3,4,5,6,7,8,9,10,11,12}
Gambar 1: Contoh graf berarah dengan himpunan simpul dan sisinya.[3]

Pasangan simpul dapat dihubungkan oleh dua atau lebih sisi, yang disebut sisi-ganda (*multiple edges* atau *parallel edges*). Sedangkan sisi yang berawal dan berakhir pada simpul yang sama yang membentuk sebuah lingkaran disebut gelang atau kalang (*loop*).

*2.2. Jenis-Jenis Graf*

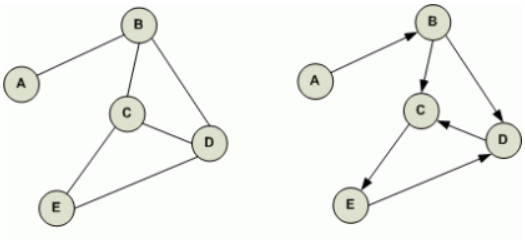
Graf dapat dibedakan menjadi beberapa kategori berdasarkan paradigma pengelompokannya.

Berdasarkan ada tidaknya sisi ganda atau gelang, graf digolongkan menjadi dua jenis, yaitu:

a. Graf sederhana (*simple graph*).
   Graf sederhana merupakan graf yang tidak mengandung gelang maupun sisi-ganda.
b. Graf tak-sederhana (*unsimple-graph*).
   Graf tak-sederhana merupakan graf yang mengandung sisi ganda atau gelang. Graf tak sederhana dapat dibedakan menjadi dua macam, yaitu graf ganda (*multi graph*) dan graf semu *(pseudo graph)*. Graf ganda adalah graf yang mengandung sisi ganda atau lebih yang mengubungkan sepasang simpul, sedangkan graf semu adalah graf yang mengandung gelang *(loop)*.

Berdasarkan orientasi arah sisi pada graf, graf dibedakan menjadi dua jenis, yaitu:

a. Graf tak berarah *(undirected graph)*
   Graf tak berarah merupakan graf yang sisinya tidak mempunyai orientasi arah. Pada graf tak berarah, sisi adalah pasangan tak terurut, dengan definisi G = (V,E), V terdiri dari himpunan tidak kosong simpul dan E adalah himpunan pasangan tak terurut yang berbeda. Sisi (u,v) sama dengan sisi (v,u).
b. Graf berarah *(directed graph)*
   Grak berarah adalah graf yang setiap sisinya memiliki orientasi arah. Sisi yang memiliki arah disebut dengan busur (*arc*). Pada graf berarah, sisi (u,v) tidak sama dengan sisi (v,u). Pada busur (u,v), simpul u dinamakan simpul asal dan v dinamakan simpul terminal.




Gambar 2: Contoh graf tak berarah (kanan) dan graf berarah (kiri)[4]

Dari dua sudut pandang tersebut, jenis graf dapat dikombinasikan sehingga terdapat lima jenis graf menurut [ROS99], yaitu:

| Jenis | Sisi | Sisi ganda | Sisi gelang |
|---|---|---|---|
| Graf sederhana | Tak berarah | Tidak | Tidak |
| Graf ganda | Tak berarah | Ya | Tidak |
| Graf semu | Tak berarah | Ya | Ya |
| Graf berarah | Berarah | Tidak | Ya |
| Graf ganda berarah | Berarah | Ya | Ya |

Tabel 1: Kombinasi jenis graf

*2.3. Terminologi Graf*

Berikut merupakan terminologi atau istilah yang dipakai pada teori graf:

a. Bertetangga *(Adjacent)*
   Sepasang simpul dikatakan bertetangga apabila kedua simpul terhubung langsung dengan sebuah sisi yang sama.
b. Bersisian *(Incident)*
   Sebuah sisi dikatakan bersisian dengan dua buah simpul yang dihubungkan olehnya. Untuk sembarang sisi e = (v1, v2), sisi e bersisian dengan simpul v1 dan v2.
c. Simpul Terpencil *(Isolated Vertex)*
   Sebuah simpul dikatakan terpencil apabila simpul tersebut tidak mempunyai tetangga, yang berarti tidak bersisian dengan sisi manapun.
d. Graf Kosong *(Null Graph)*
   Graf kosong adalah graf yang himpunan sisinya merupakan himpunan kosong, dengan jumlah simpul sebanyak *n*.
e. Derajat *(Degree)*
   Derajat sebuah simpul pada graf tidak berarah merupakan jumlah sisi yang bersisian dengan simpul tersebut.
   Sedangkan pada graf berarah, derajat simpul v dibedakan menjadi menjadi dua sesuai representasi arahnya, yaitu:
   1) Derajat Masuk ($d_{in}(v)$): jumlah busur yang masuk ke dalam simpul *v*.
   2) Derajat Keluar ($d_{out}(v)$): jumlah busur yang keluar dari simpul *v*.
   3) Derajat total simpul (d(v)): jumlah busur masuk dan keluar.
f. Lintasan *(Path)*
   Lintasan adalah barisan selang-seling simpul dengan sisi dimulai dari simpul awal $v_0$ ke simpul tujuan $v_n$.
   Panjang lintasan adalah jumlah sisi dari simpul awal ke simpul tujuan dalam graf G.
g. Siklus *(Cycle)* atau Sirkuit *(Circuit)*
   Siklus adalah lintasan yang berawal dan berakhir pada simpul yang sama.
   Panjang sirkuit adalah jumlah sisi pada sirkuit.
h. Terhubung *(Connected)*
   Graf disebut terhubung apabila setiap pasang $v_i$ dan $v_j$ pada graf mempunyai lintasan yang menuju satu sama lain (terdapat lintasan dari $v_i$ ke $v_j$ dan sebaliknya). Jika tidak, maka graf disebut graf tak terhubung.
   Pada graf berarah, terdapat istilah terhubung kuat dan terhubung lemah. Terhubung kuat berarti apabila terdapat lintasan berarah dari u ke v, maka terdapat lintasan berarah dari v ke u pula. Sedangkn terhubung lemah berarti apabila terdapat busur dari u ke v tetapi tidak terdapat busur v ke u.
i. Upagraf *(Subgraph)* dan Komplemen Upagraf

Upagraf adalah graf yang seluruh anggota simpul dan sisinya merupakan anggota dari himpunan simpul dan sisi graf lainnya.
Komplemen dari sebuah upagraf adalah graf yang anggota himpunan simpul dan sisinya terdiri dari sisi dan simpul yang ada dalam graf G namun tidak dalam upagraf tersebut.

j. Upagraf Merentang *(Spanning Subgraph)*
Sebuah graf merupakan upagraf merentang graf lainnya ketika elemen himpunan simpulnya terdiri dari seluruh elemen himpunan simpul graf lainnya, dengan himpunan sisi yang berbeda.

k. *Cut-set*
*Cut-set* merupakan himpunan sisi dari graf terhubung yang apabila dibuang akan menyebabkan graf tersebut tidak lagi terhubung.

l. Graf Berbobot
Graf berbobot adalah graf yang tiap sisinya memiliki nilai.

*2.4. Representasi Graf*

Dalam bekerja dengan graf, dibutuhkan pilihan representasi yang tepat untuk mempermudah analisis. Berikut merupakan tiga jenis representasi graf:

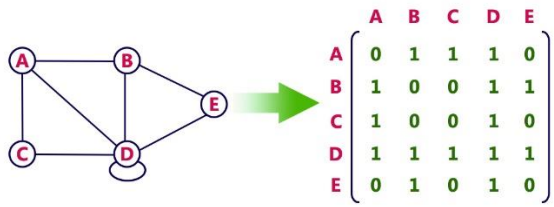
a. Matriks Ketetanggaan (*Adjancency Matrix*)

Matriks ketetanggaan adalah matriks berukuran 2x2 yang menyimpan informasi mengenai keterhubungan antara dua simpul. Jika matriks dinamakan A = [$a_{ij}$], maka:

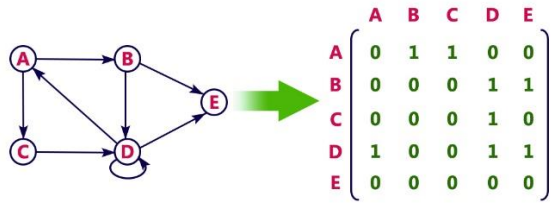
$a_{ij}$ bernilai 1 jika simpul i dan j bertetangga,

$a_{ij}$ bernilai 0 jika simpul i dan j tidak bertetangga.

Berikut merupakan bentuk representasi dari matriks ketetanggaan:




Gambar 3: Matriks ketetanggaan sebuah graf tak berarah.[5]




Gambar 4: Matriks ketetanggaan sebuah graf berarah.[5]

Matriks ketetanggaan untuk graf tak berarah sederhana selalu simetris terhadap diagonalnya, sedangkan untuk graf berarah, matriks ketetanggaannya belum tentu simetris. Selain diagonal utama matriks menunjukkan ada tidaknya kalang pada tiap simpul. Pada graf berarah, tiap kolom menunjukkan simpul terminal, sedangkan tiap barisnya menunjukkan simpul awal.

b. Matriks Bersisian (*Incidency Matrix*)

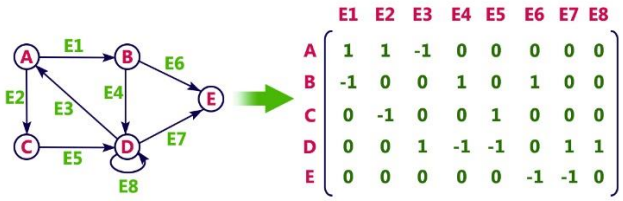
Matriks bersisian merupakan matriks 2x2 yang menyimpan informasi hubungan setiap sisi bersisian atau tidak dengan setiap simpul. Jika matriks dinamakan A = [$a_{ij}$], maka:

$a_{ij}$ bernilai 1 jika simpul i bersisian dengan sisi j,

$a_{ij}$ bernilai 0 jika simpul i tidak bersisian dengan sisi j.

$a_{ij}$ bernilai -1 untuk graf berarah jika terdapat sisi j yang menuju simpul i.

Berikut merupakan bentuk representasi matriks bersisian dari sebuah graf:

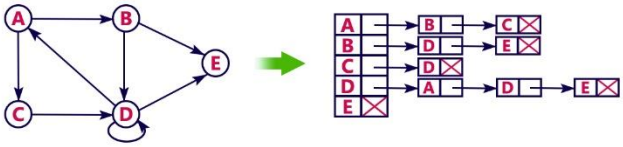



Gambar 5: Matriks bersisian sebuah graf berarah[5]

Tiap kolom matriks menunjukkan sisi atau busur, sedangkan tiap baris menunjukkan simpul graf. Nilai negatif pada graf berarah menunjukkan bahwa sisi e menunjuk kepada simpul yang dituju.

c. Senarai Ketetanggaan (*Adjacency List*)

Senarai ketetanggaan adalah representasi graf yang menyimpan informasi mengenai ketetanggaan antara setiap simpul dengan struktur data bentukan *array of list.* Daftar simpul disimpan dalam *array*. Setiap simpul pada elemen *array* memiliki *pointer* menuju *list* simpul yang bertetangga.



Gambar 6: Senarai ketetanggaan dari sebuah graf.[5]

*2.5. Analisis Graf*

Graf digunakan sebagai wujud visualisasi dari data. Terdapat empat jenis analisis graf, yaitu:

a. Analisis *path*
Jenis analisis ini digunakan untuk menentukan jarak terpendek antara dua simpul pada graf. Contoh dari analisis ini adalah optimasi rute pada pengiriman, suplai, dan rantai distribusi logistic.

b. Analisis konektivitas
Analisis ini dapat diaplikasikan untuk menentukan kelemahan pada suatu jaringan. Analisis ini dapat membandingkan kekuatan antara beberapa konektivitas.

c. Analisis komunitas
Analisis ini digunakan untuk mencari kelompok atau komunitas pada jaringan sosial.

d. Analisis pusat
Analisis ini digunakan untuk mengidentifikasi pemusatan tren pada suatu jaringan. Sebagai contoh yaitu untuk menentukan orang terpopular pada jaringan sosial atau

unuk menemukan halaman web yang paling banyak diakses – penggunaan algoritma PageRank.

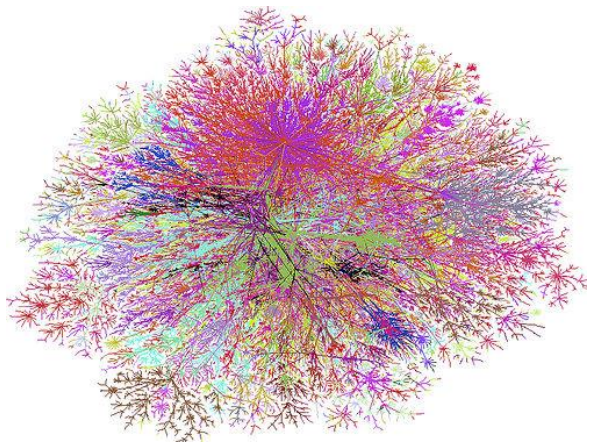
### *2.6. Teori Jaringan Komputer*

*Network* atau jaringan adalah kumpulan dari objek terhubung. *Computer network* atau jaringan komputer adalah kelompok dua atau lebih sistem komputer yang saling terkait. Setiap komputer yang menyambung ke internet merupakan bagian dari *network.* Kelompok ini membentuk jaringan telekomunikasi digital yang memungkinkan tiap perangkat untuk bertukar informasi. Sambungan antar perangkat dibuat menggunakan media kabel atau media nirkabel.

Terdapat beberapa jenis jaringan komputer menurut cakupan wilayahnya, yaitu:

a. *Local Area Network* (LAN): Jaringan komputer yang secara geografis berdekatan (pada bangunan yang sama).
b. *Wide Area Network* (WAN): jaringan antar komputer lebih jauh dan dihubungkan oleh saluran telepon atau gelombang radio.
c. *Campus Area Network* (CAN): Jaringan komputer berada dalam wilayah geografis yang terbatas, seperti kampus atau pangkalan militer.
d. *Metropolitan Area Network* (MAN): Jaringan data yang dirancang pada sebuah kota.
e. *Home Area Network* (HANs): Jaringan pada rumah pengguna yang menghubungkan antar perangkat digital.

Jaringan komputer dapat direpresentasikan ke dalam graf, dengan perangkat sebagai simpul dan koneksi antar perangkat sebagai busur.



Gambar 7: Jaringan koneksi internet antar perangkat pada tahun 2004. [7]

### *2.7. Keamanan Cyber*

Keamanan *cyber* merupakan sistem pertahanan yang dirancang untuk melindungi *network*, perangkat, program, dan data dari serangan, pencurian, kerusakan perangkat keras, perangkat lunak atau informasi, serta akses illegal lainnya dari perangkat asing. Keamanan *cyber* mengontrol akses fisik menuju perangkat keras, serta melindungi sistem dari bahaya yang mungkin terjadi melalui akses jaringan, data, dan injeksi kode.

Kerentanan (*vulnerability*) adalah kelemahan pada implementasi, desain, operasi, dan kontrol pengawasan internal yang dapat menjadi celah masuknya serangan *cyber.* Untuk mengamankan jaringan komputer, penting untuk memahami serangan yang dapat terjadi. Ancaman terhadap jaringan dapat dikelompokkan menjadi beberapa kategori di bawah ini:

*a. Backdoor*, metode gelap untuk melewati otentikasi normal atau kontrol keamanan.

*b.* Serangan *Denial of Service*, serangan koloni komputer yang terkena pengaruh kendali mesin untuk menyerang web yang dituju.

*c.* Serangan *Direct-access*, teknik penetrasi pada komputer atau perangkat pengguna untuk memperoleh akses informasi.

*h. Phishing*, usaha untuk memperoleh informasi sensitif seperti nama pengguna, kata sandi, dan detail kartu kredit dari pengguna.

*j. Clickjacking*, teknik di mana penyerang menipu pengguna agar mengklik tautan jebakan pada halaman web yang sedang dikunjungi pengguna.

## III. PEMBAHASAN

Pemantauan keamanan *cyber* sebuah jaringan komputer terdiri dari kumpulan informasi yang dapat membentuk *big data*. Data tersebut terdiri dari log IP, penggunaan *bandwidth*, log jaringan, dan log komunikasi atau server. *Network* sebuah perusahaan besar menghasilkan sekitar 10-100 miliar log data keamanan setiap hari. Volume dan kompleksitas data tersebut merupakan sebuah permasalahan bagi pemantauan keamanan dengan metode tradisional yang lazim digunakan bernama *Security Information and Event – Management* (SIEM). Metode ini dirancang untuk menganalisis log, arus jaringan, dan deteksi *event* sistem, namun tidak dilengkapi penanganan *big data*. Analisis *network* secara tradisional dapat memakan banyak waktu dalam bekerja dengan database relasional yang menyimpan *big data.*

Untuk mempermudah analisis keamanan, *big data* perlu divisualisasikan dengan pemodelan graf.

### *3.1. Model Graf Network Traffic*

*Network* dapat diabstraksikan sebagai graf G = (V,{VR}). Titik-titik pada graf menotasikan simpul-simpul pada *network* seperti server yang dinotasikan dengan V. VR menotasikan relasi antar dua simpul. Misalkan C dan D menotasikan dua simpul *network.* Terdapat enam jenis koneksi diantaranya sebagai berikut:

K1: C dapat mengakses D sebagai manajer server. C dapat mengendalikan *resource* secara penuh.

K2: C mengakses D sebagai klien umum, terbatas dengan kapasitas *resource* yang dapat dikendalikan.

K3: C mendapatkan atau mendistribusikan informasi pribadi dan publik pada kapasitasnya dari daftar klien pada D.

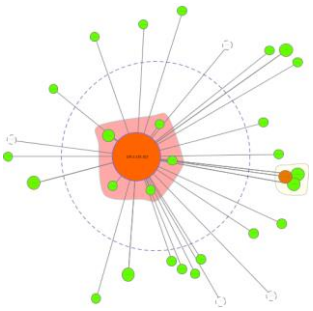
K4: C mendapatkan atau mendistribusikan informasi pribadi dan publik pada kapasitasnya dari klien anonim pada D. Konektivitas dapat dilambangkan seperti halnya koneksi layanan *firewall.*

K5: C mengunjungi D pada lapisan jaringan IP, hubungan ini terjalin konektivitas lapisan IP.

K6: C mengunjungi D pada *link layer*, relasi menunjukkan konektivitas dari *link layer*.

Sehingga relasi antara simpul C dan D dinotasikan sebagai (C, D) ∈ VR, dengan VR = {K1, K2, K3, K4, K5, K6}.

Untuk menampilkan visualisasi *network* secara *real-time*, pada analisis ini digunakan alat pembuat graf bernama *Linkurious*, platform pemodelan graf yang dikembangkan oleh sebuah startup dari Perancis. Visualisasi menampilkan informasi data IP *host* dan koneksi antar *host.*

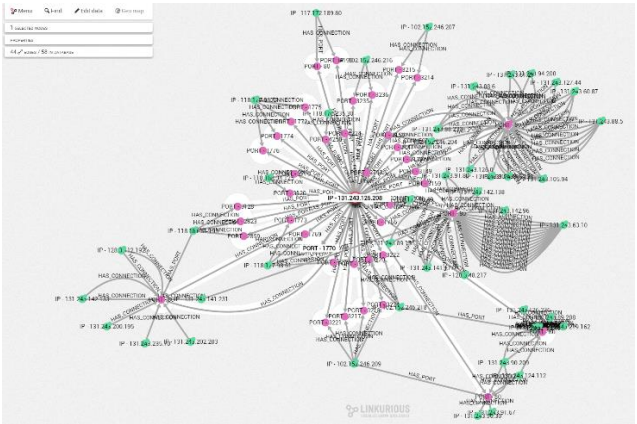


Gambar 8: Pemodelan graf *network* secara *real-time* dengan NetGrok.[11]

Pemodelan sederhana di atas dibuat dengan platform bernama NetGrok, *software* untuk memvisualisasikan jaringan yang dikembangkan oleh *University of Maryland*. Simpul di dalam garis putus-putus melambangkan *host* lokal, sedangkan simpul-simpul di luar garis putus-putus melambangkan *host* asing. Garis-garis busur menunjukkan koneksi *host* asing dengan *host* lokal.

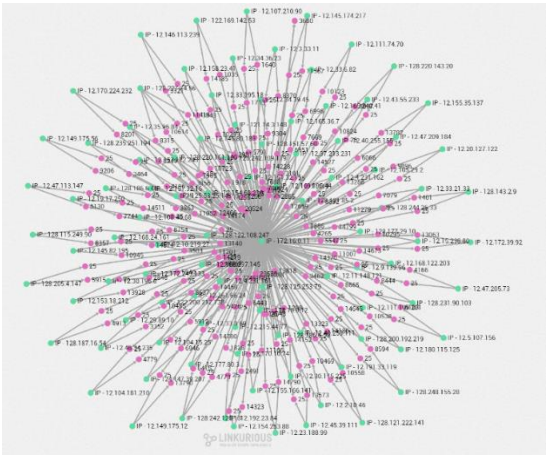
*3.2. Analisis Aktivitas Jaringan Komputer*

Mengetahui kondisi normal suatu *network traffic* merupakan langkah awal dalam mendeteksi aktivitas mencurigakan dari *host* asing. Sebagai contoh, visualisasi berikut menunjukkan aktivitas normal pada sebuah *network*, dimana *host* melakukan koneksi dengan IP 131.243.125.208 menggunakan port layanan yang berbeda.



Gambar 9: Graf aktivitas normal sebuah *network.*[12]

Di sisi lain, berikut merupakan pola aktivitas abnormal. Sebagian besar *host* yang terhubung ke IP 172.16.0.11 menggunakan port yang sama dan tidak menghasilkan *traffic* lain. Mereka melakukan operasi yang sama dengan teratur secara bersamaan. Pola aktivitas ini mengindikasikan kumpulan *botnet* yang melakukan serangan UDP *storm*. Serangan ini pada dasarnya merupakan *Denial of Service* (DoS).



Gambar 10: Graf *network* pada saat terjadi serangan DoS.[12]

Representasi *network* dengan graf memungkinkan pemantauan koneksi dan penemuan aktivitas abnormal yang tidak terlihat secara eksplisit dengan menggunakan kemampuan manusia dalam mengenali pola secara visual. Mengombinasikan kemampuan manusia dengan mesin pemroses data memungkinkan penemuan anomali suatu *network* dengan tepat. Pendekatan deteksi anomali ini dapat mencegah akses ilegal dari *host* asing, menemukan titik masuk *malware*, memprediksi serangan *cyber*, dan menemukan kerentanan pada sistem keamanan *cyber*.

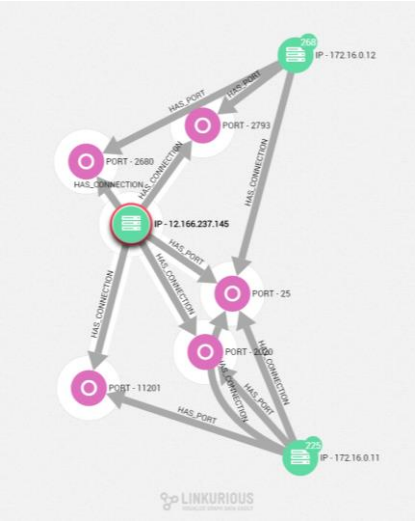
*3.3. Pelacakan Aktivitas Abnormal*

Seperti halnya domain web, domain yang digunakan serangan *phishing* terkait dengan beberapa infomasi, yaitu:

a. Alamat IP: label numerik yang dimiliki setiap perangkat yang berpartisipasi pada suatu *network* yang menggunakan *Internet Protocol* untuk berkomunikasi.
b. Nama server: perangkat keras dan lunak server yang mengimplementasikan layanan *network* untuk memberikan respon atas *request* layanan direktori.
c. Registrar: organisasi atau entitas komersial yang mengelola reservasi nama domain.

Ketika anomali terdeteksi, pelacakan dapat dilakukan pada alamat IP. Dengan menyalakan layanan geospasial untuk mengintegrasikan alamat IP dengan koordinat GPS, lokasi dari penyerang atau botnet dapat ditampilkan.

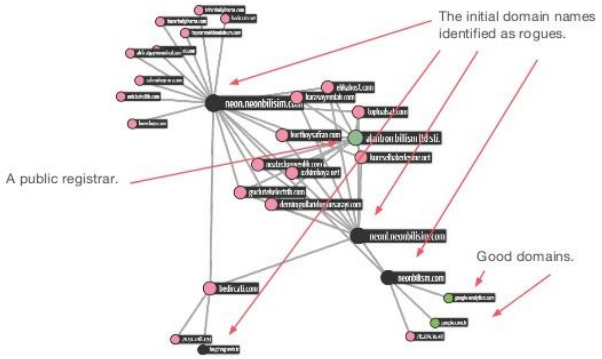
Kemudian aktivitas dari alamat IP tertentu juga dapat dieksplorasi untuk meninjau jaringan yang terkait oleh sebuah *host* yang melakukan aktivitas abnormal beserta jenis koneksinya. Misalnya pada kasus DoS pada gambar ( ), apabila ditinjau, alamat IP 12.166.237.145 memiliki tautan lain. Secara terpisah, semua koneksi yang dilakukan alamat IP tersebut dapat ditampilkan. Dengan cara ini, dapat dilacak bahwa IP ini berkait dengan alamat IP lainnya, yaitu 172.16.0.12. Pelacakan dapat merambat menuju alamat IP dari sumber *phishing*.




Gambar 11: Pelacakan aktivitas *botnet* IP 12.166.237.145.[12]

Berikut merupakan metode analisis yang dilakukan Cisco, perusahaan teknologi multinasional Amerika, dalam melacak serangan *phishing*. Sebagai penyedia keamanan *cyber*, Cisco melakukan *follow-up* terhadap domain-domain yang memiliki reputasi baik hingga domain yang tingkat keamanannya rendah. Cisco mengenali informasi dari 25-30 juta domain internet. Tetapi masih terdapat 180 juta domain yang belum diidentifikasi.

Ketika Cisco mendeteksi koneksi mencurigakan dari sebuah *host*, dilakukan analisis untuk menemukan registrar dan domain yang terlibat dengan melacak domain yang terhubung sebelumnya pada penyerang. Untuk meenemukan koneksi dataset besar, dapat ditinjau dari graf jaringan koneksi domain tersangka.




Gambar 12: Graf informasi domain yang diindikasikan sebagai tindakan *phishing*.[15]

Pada gambar di atas, simpul berwarna merah muda merepresentasikan domain-domain yang terhubung dengan penyerang sebelumnya. Nama domain yang mencurigakan dapat dipantau sehingga tidak dapat digunakan dalam serangan lainnya. Kemudian dengan sigap Cisco memblokir nama domain sebelum digunakan oleh para *hacker*.

## IV. KESIMPULAN

Salah satu aplikasi teori graf adalah sebagai visualisasi jaringan komputer. Dengan graf, analisis *network* dapat dilakukan dengan cepat. Secara visual manusia dapat mengidentifikasi pola koneksi dan asosiasi yang tidak secara langsung ditemukan dalam analisis *network* secara tradisional dengan database relasional. Selain itu, graf meningkatkan visibilitas data. Representasi dengan graf mempermudah interpretasi *network* dalam mendeteksi aktivitas abnormal sehingga apabila terjadi indikasi serangan *cyber*, kasus dapat dilacak dan ditindaklanjuti dengan cepat.

## V. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa yang telah memberikan petunjuk dan kelancaran dalam menulis makalah ini. Penulis juga berterima kasih kepada kedua orangtua Penulis yang telah mendukung Penulis hingga sejauh ini Penulis berkuliah di Teknik Informatika. Tak lupa Penulis ucapkan terima kasih kepada Bapak Dr.Ir. Rinaldi Munir, MT. yang telah memberikan tantangan bagi Penulis untuk mengembangkan kemampuan menulis karya ilmiah dan juga Bapak Dr. Judhi Santoso M.Sc. sebagai dosen mata kuliah Matematika Diskrit yang telah mengajar dan membimbing Penulis pada semester ini.

## REFERENSI

[1] Munir, Rinaldi, Matematika Diskrit, Bandung: Penerbit Informatika Bandung.
[2] Rosen, Kenneth H. Discrete Mathematics and Its Applications, 7th Edition. The McGraw-Hill Companies.2012.
[3] Anonim, "Graph Theory", http://www.aber.ac.uk/~dcswww/Research/bio/robotsci/data/model/graph_theory.html, diakses 2 Desember 2017.
[4] Anonim, "Build An Adjacency Matrix of a Graph", https://www.codediesel.com/algorithms/building-a-adjacency-matrix-of-a-graph/, diakses 2 Desember 2017.
[5] Anonim, "Graph Representation", http://btechsmartclass.com/DS/U3_T9.html, diakses 2 Desember 2017.
[6] Nykamp DQ, "An introduction to networks." dari Math Insight. http://mathinsight.org/network_introduction, diakses 1 Desember 2017.
[7] Internet Map 2004. https://www.flickr.com/photos/jurvetson/916142/, diakses 1 Desember 2017.
[8] Ferguson, Mike. "What is graph analytics?" http://www.ibmbigdatahub.com/blog/what-graph-analytics, diakses 1 Desember 2017.
[9] Lord, Nate. "What is Cyber Security?". https://digitalguardian.com/blog/what-cyber-security, diakses 2 Desember 2017.
[10] Rampat, Adesh. "Vulnerabilities in Network System". http://searchsecurity.techtarget.com/tip/Vulnerabilities-in-network-systems, diakses 2 Desember 2017.
[11] Blue R., Dunne C., Fuchs A., King K., Schulman A. (2008) Visualizing Real-Time Network Resource Usage. In: Goodall J.R., Conti G., Ma KL. (eds) Visualization for Computer Security. Lecture Notes in Computer Science, vol 5210. Springer, Berlin, Heidelberg
[12] Villedieu, Jean. "Cyber Security : How to Use Graphs to Do an Attack Analysis" dari blog Linkurious. https://linkurio.us/blog/cyber-security-use-graphs-attack-analysis/, diakses 2 Desember 2017.
[13] Department of Homeland Security, "Cyber Security", https://www.dhs.gov/topic/cybersecurity, diakses 2 Desember 2017.
[14] Harith A. Dawood, "Graph Theory and Cyber Security", 2014 3rd International Conference on Advanced Computer Science Applications and Technologies (ACSAT), vol. 00, no. , pp. 90-96, 2014, doi:10.1109/ACSAT.2014.23
[15] Gundert, Levi. "Attack Analysis with a Fast Graph" https://blogs.cisco.com/security/attack-analysis-with-a-fast-graph, diakses 2 Desember 2017

[16] Ming-zhong M. (2012) Network Security Analysis Based on Graph Theory Model with Neutral Network. In: Zhang Y. (eds) Future Communication, Computing, Control and Management. Lecture Notes in Electrical Engineering, vol 141. Springer, Berlin, Heidelberg

## 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, 3 Desember 2017

Erma Safira Nurmasyita (13516072)