ANALISA CAATS (COMPUTER ASSISTED AUDIT TECHNIQUES) UNTUK IDENTIFIKASI DATA LOG FIREWALL

Emilya Ully Artha[1)]

[1)]*Teknik Informatika STMIK AMIKOM Yogyakarta*
Jl Ring road Utara, Condongcatur, Sleman, Yogyakarta 55281
Email : ully@amikom.com[1)]

Abstrak

Internal Audit merupakan salah satu cabang ilmu yang sangat penting sebagai penghubung bisnis di dalam suatu organisasi. Perusahaan atau organisasi pada perkembangannya mempunyai kecendrungan untuk mengadopsi teknologi informasi untuk menjalankan bisnisnya sebagai pendongkrak keuntungan ataupun memperbaiki kinerja. 80% lebih celah keamanan berasal dari dalam suatu organisasi. Kecurangan (fraud) perlu dibedakan dengan kesalahan (error). Kesalahan dapat terjadi pada setiap pengolahan transaksi. Tetapi bila kesalahan sengaja dilakukan maka akan dianggap sebagai kecurangan. Untuk mengurangi fraud dibuatlah sistem yaitu firewall. Dari firewall ini akan dikeluarkan log dari hasil yang dilakukan oleh firewall. Dari log ini akan dianalisa menggunakan Benford's Law analysis menggunakan software audit Picalo. Hasil dari penelitian akan mencari apakah file log yang dianalisa akan memunculkan anomaly data ataukah tidak.

Kata kunci: *internal audit, fraud, error, firewall, log.*

1. Pendahuluan

Perkembangan teknologi mengakibatkan segala sesuatu yang memungkinkan diatur oleh komputer. Dari sistem kerja secara manual perlahan-lahan perlahan-lahan digantikan dengan teknologi. Pergeseran ini juga mengakibatkan pola penyimpanan data yang semakin besar, perubahan terhadap kesediaan informasi, serta perubahan dalam pengambilan keputusan yang cepat. Perubahan yang cepat ini tidak menjamin suatu sistem bebas dari kesalahan atau kecurangan sehingga menimbulkan kerugian, manipulasi data, atau pencurian yang dilakukan oleh pihak luar maupun dalam suatu organisasi.

Kesalahan dapat diartikan sebagai *unintentional mistakes* atau kesalahan yang tidak disengaja. Kesalahan dapat terjadi pada setiap tahapan dalam pengelolaan terjadinya suatu transaksi, dokumentasi, pencatatan dari jurnal, dan sebagainya. Kesalahan dapat pula terjadi dalam bentuk perhitungan matematis atau interpretasi fakta. Apabila kesalahan disengaja, maka kesalahan itu merupakan suatu kecurangan (*fraudelent*). Audit sistem informasi adalah fungsi dari organisasi yang mengevaluasi keamanan aset, integritas data, efektifitas, dan efisiensi sistem dalam sistem informasi berbasis komputer. Fraud auditing adalah upaya untuk mencegah kecurangan dalam transaksi-transaksi komersial.

Kebutuhan audit SI ini disebabkan oleh beberapa faktor [1], yaitu :

a. kemungkinan kehilangan data
b. kemungkinan kesalahan penempatan sumber daya akibat kesalahan pengambilan keputusan yang diakibatkan karena kesalahan pemrosesan data.
c. kemungkinan komputer rusak karena tidak terkontrol
d. harga komputer software/hardware yang mahal
e. biaya operasional yang tinggi apabila komputer rusak
f. kebutuhan privasi dari suatu organisasi/perorangan
g. kebutuhan untuk mengontrol penggunaan komputer

sebagian besar implementasi audit khususnya auditor SI secara khusus berkosentrasi pada efektifitas pengendalian atau kontrol sistem. Kontrol sendiri adalah bentuk dari sistem yang berfungsi untuk mencegah, mendeteksi atau memperbaiki sistem yang tidak teratur. Fungsi kontrol sendiri dibagi menjadi tiga bagian yaitu *Preventive Control,* adalah intruksi yang diletakkan pada dokumen untuk mencegah kesalahan pemasukan data.

Detective Control yaitu kontrol yang diletakkan pada program yang berfungsi untuk mendeteksi kesalahan pemasukan data. *Corrective Control* yaitu program yang dibuat khusus untuk memperbaiki kesalahan pada data yang mungkin timbuk akibat gangguan pada jaringan, komputer ataupun kesalahan pengguna (*user*)[2].

Dengan kemajuan TI dan penggunaan software, memberikan manajemen dan dan auditor kemampuan untuk melakukan audit dan monitoring berkelanjutan. Untuk melakukan auditor berkelanjutan, auditor harus mengembangkan program yang secara rutin bekerja pada proses bisnis. Metodelogi audit secara berkelanjutan dapat dibagi menjadi tiga area level data, yang mana merupakan area dasar dari pemeriksaan data[6] :

a. *Keystroke level*. Untuk keberhasilan kebijakan audit berkelanjutan analisis statistic dari setiap

keystroke untuk operasi utilitas database adalah kegiatan yang esensial.

b. *Transaction level*. Secara umum transaksi di validasi pada saat dimasukkan pada software aplikasi
c. *Transaction pattern level*. Memonitor *keystroke* secara dinamika dan menjalankan CAAT (*Computer Assisted Audit Techniques*)

2. Pembahasan

2.1. Digital Analisis dengan Hukum Benford

Benford's Law atau hokum Benfords adalah sebuah hokum yang dapat memperkirakan frekuensi kemunculan sebuah angka dalam serangkaian data numerik. Jika data numerik tersebut dihasilkan tanpa ada unsur kesengajaan, maka frekuensi kemunculan angka tersebut akan sesuai dengan harapan frekuensi dalam *Benford's Law*. Sebaliknya jika ada unsur kesengajaan oleh manusia untuk menciptakan sebuah kombinasi angka dan dimasukkan dalam sebuah data set, maka hasil analisa *Benford's Law* akan menunjukkan bahwa ada angka tertentu yang lebih banyak atau lebih sedikir muncul dari yang diperkirakan[8].

Benford's Law banyak digunakan di berbagai bidang, karena kemampuannya untuk mendeteksi anomaly data pada sebuah data set. Anomali data tersebut, jika ditelusuri lebih lanjut dapat mendeteksi *fraud*. Ada beberapa persyaratan kriteria angka (*data set*) yang harus dipenuhi agar dapat dianlisis dengan menggunakan *Benford's Law*[9] :

a. Data yang dianalisis merupakan merupakan kesatuan utuh dan menggambarkan suatu fenomena yang serupa
b. Data tidak berada dalam batasan maksimum atau minimum (diantara angka tertentu)
c. Data tersebut bukan merupakan angka yang dibentuk secara sengaja atau angka yang disimbolkan
d. Data memiliki ukuran besar (jumlah angkanya lebih banyak)
e. Data adalah milik suatu entitas sehingga dapat dibedakan dengan yang lain dan data juga tidak terduplikasi
f. Data jika diurutkan dari nilai terkecil hingga ke besar membentuk deret geometris
g. Data tersebut memiliki nilai rata-rata (*mean*) lebih besar dari nilai tengah (*median*).
h. Data tersebut memiliku nilai *skewness* positif

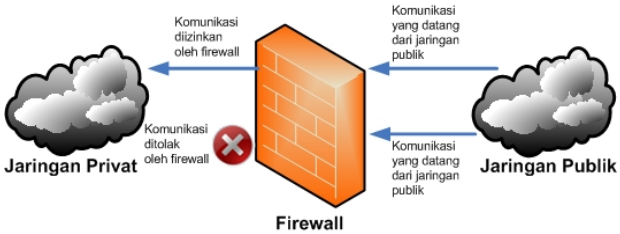
Ada lima tes utama untuk menentukan apakah suatu *set data* kuantitatif dan mengikuti pola *Benford's Law* atau tidak. Uraian lima tes tersebut adalah *First-Digit Tes* (FD), *Second-Digit Tes* (SD), *First-Two Digit Tes* (F2D), *First-Three Digit Tes* (F3D), dan *Last-Two Digit Tes* (L2D).

Alat bantu analisis digital seperti *Benford's Law* memang memungkinkan auditor berfokus pada sampel yang dianggap memiliki indikasi kecurangan, namun belum membuktikan bahwa kecurangan itu ada. Oleh karena itu dibutuhkan pendalaman lebih lanjut lewat pengujian. Tes ini digunakan untuk mengetahui apakah data yang dinalisis benar-benar sesuai atau benar-benar berbeda dengan *Benford's Law*. Ada beberapa tes yaitu *Z-Statistic*, *Chi-Square*, *Kolmogorof-Smirnoff*, *Mean Absolute Deviation* (MAD)[9].

2.2. Firewall

Firewall log adalah hasil proses filtering penyimpanan data dari dalam dan luar dari akses kontrol yang telah dibuat[3]. Termasuk record dari proses komunikasi data yang diberi maupun ditolak untuk masuk ke dalam system. Saat ini banyak sekali perangkat lunak yang digunakan untuk melakukan analisa log. Seperti Swatch, Netfilter dan sebagainya.

Firewall adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas data pada jaringan internet dianggap aman untuk dilalui dan mencegah lalu lintas jaringan yang tidak aman. Firewall umumnya diimplementasikan dalam sebuah mesin tersendiri, yang berjalan pada *gateway* antara jaringan lokal dan jaringan lainnya. Firewall juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Fungsi utama dari *firewall* adalah melakukan fungsi inspeksi terhadap paket-paket dan memantau koneksi yang sedang dibuat, lalu melakukan filtering terhadap koneksi berdasarkan hasil inspeksi paket tersebut.



Gambar 1. Firewall

Saat ini firewall merujuk pada system yang mengatur komunikasi antar dua macam jaringan yang berbeda Yng digunakan sebagai perlindungan terhadap perangkat digital perusahaan tersebut dari peretas, ataupun pencurian dara lainnya.

2.1. Cara kerja Firewall

Paket yang datang dari luar jaringan pertamakali akan masuk ke dalam system *firewall*. *Firewall* lalu akan melihat tujuan paket atau sumber dari paket tersebut, protocol yang dibawa, alamat port, juga aplikasi yang diijinkan maupun yang ditolak oleh *firewall*. Contohnya

adalah rules yang digunakan oleh mesin Cisco menggunakan *access-list*.

"access-list 101 permit TCP 137.189.0.0 255.255.0.0 137.1xx.0.0 255.255.0.0 80".

Access-list adalah pengelompokan paket berdasarkan kategori. Statement access-list pada dasarnya adalah paket filter di mana paket dibandingkan terhadap suatu tindakan. List yang telah dibuat bias diterapkan baik kepada lalu lintas *inbound* maupun *outbond* pada interface mana saja[4]. Dari perintah diatas dapat dianalisa bahwa *firewall* melakukan penyaringan menggunakan *access-list* 101. Yang mana 101 merupakan *Extended Access-list* yang dapat mengevaluasi banyak field pada header di layer 3 dan layer 4 pada paket IP. *Permit* berarti *firewall* mengizinkan paket TCP yang dibawa oleh alamat IP Network 137.189.0.0 dan 137.1xx.0.0 untuk menggunakan port 80. Port 80 adalah port yang digunakan pada layer paling atas (*Application Layer*) untuk mengakses halaman web.

Packet inspection merupakan proses yang dilakukan oleh firewall untuk menghadang dan memproses data dalam sebuah paket untuk menentukan bahwa paket tersebut diizinkan atau ditolak, berdasarkan kebijakan akses (access policy) yang diterapkan oleh administrator. Firewall sebelum menentukan keputusan apakah hendak menolak atau menerima komunikasi dari luar, maka harus melakukan inspeksi terhadap paket (baik yang masuk atau keluar) di setiap antarmuka dan membandingkannya dengan melihat elemen-elemen berikut :

a. alamat IP dari komputer sumber
b. Port sumber pada komputer sumber
c. Alamat IP dari komputer tujuan
d. Port tujuan data pada komputer tujuan
e. Protokol IP
f. Informasi header-header yang disimpan dalam paket.

2.3. Data Log

Ketika *firewall* membuat file log, file-file ini akan dikelompokkan menjadi beberapa bagian, seperti koneksi data yang diizinkan masuk ke system, koneksi yang tidak diizinkan masuk ataupun koneksi yang mencoba memaksa masuk ke system. *Log* adalah catatan atau pesan yang tersimpan dalam sebuah file, biasanya mewakili pesan proses pada aplikasi yang berjalan. Terdapat berbagai macam jenis log diantaranya adalah *error log*, *cache log*, *user log* dan *update log*. Log file sendiri dapat merupakan sumber informasi yang penting bagi forensik. Dalam administrasi sistem jaringan, para administrator akan sering berhubungan dengan log. Semisal program web server, database maupun server data. Sebagai contoh adalah program yang digunakan untuk security atau keamanan jaringan, log file dapat menunjukkan usaha penjebolan keamanan yang dilakukan seseorang.

File log yang dihasilkan oleh suatu program dapat berupa file biner atau file teks sederhana (atau keduanya). Sedangkan format file log bisa bermacam-macam, namun file log yang umum ditemukan di dunia Unix atau Windows adalah file log dimana informasi disusun perbaris. Setiap kali program me-log aktivitas, catatan tersebut disusun dalam satu baris dan ditambahkan di baris terakhir (*append*)[5].

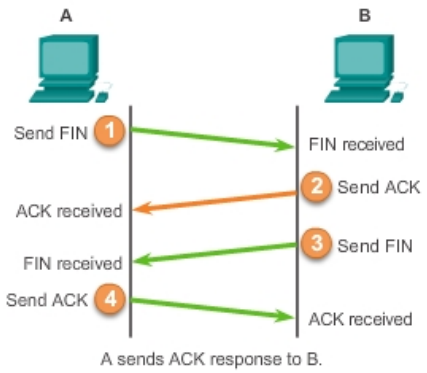
Logging data (data logging) adalah proses otomatis pengumpulan dan perekaman data dari sensor untuk tujuan pengarsipan atau tujuan analisis. Dalam ilmu komputer data adalah informasi yang digunakan oleh komputer yang bukan merupakan kode program namun digunakan dalam komputasi program.

2.4. Protokol TCP/IP

Protocol adalah sebuah standar aturan yang mengatur alat-alat dalam jaringan komputer sehingga dapat berkomunikasi satu sama lain. Dan dapat melakukan perpindahan data. Pada tahun 1981 dibentuk *Transmision Control Protocol* (TCP) dan *Internet Protocol* (IP) sebagai protocol yang digunakan untuk komunikasi dalam jaringan komputer. Setiap komputer dan jaringan terhubung secara langsung maupun tidak langsung ke beberapa jalur utama yang disebut dengan internet *backbone* dan dibedakan satu dengan yang lainnya menggunakan unique name yang biasa disebut dengan alamat IP (*Internet Protocol Address*). Banyak hal yang dapat dilakukan oleh protocol, misalnya :

a. Melakukan deteksi terhadap perangkat fisik
b. Melakukan metode handshaking
c. Melakuka fungsi tes koneksi terhadap berbagai macam koneksi
d. Mengawali dan mengakhiri suatu pesan
e. Mengatur format pesan yang akan dilakukan
f. Mengakhiri suatu koneksi

Port TCP mampu mengindikasikan sebuah lokasi tertentu untuk menyampaikan segmen-segmen TCP yang diidentifikasikan dengan TCP *port number*. Proses pembuatan koneksi TCP dikenal dengan istilah *three-way handshake*. Tujuan metode ini adalah agar dapat melakukan sinkronisasi terhadap nomor urut dan nomor acknowledgement yang dikirimkan oleh kedua belah pihak.



Gambar 2. TCP Three-way handshake

Prosesnya adalah sebagai berikut :

a. Host pertama akan mengirimkan sebuah segmen TCP dengan flag SYN diaktifkan kepada host kedua

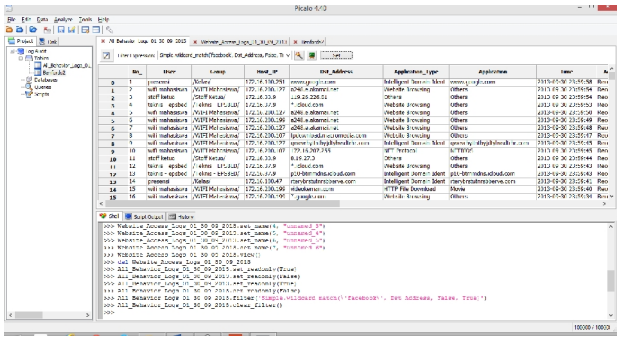
b. Host kedua akan meresponnya dengan mengirimkan segmen dengan acknowledgment dan juga SYN kepada host pertama

c. Host pertama selanjutnya akan mulai saling bertukar informasi data dengan host kedua

Protocol IP merupakan salah satu protocol kunci dalam kumpulan protocol TCP/IP. Sebuah paket IP akan membawa data actual yang dikirimkan melalui jaringan dari satu titik ke titik lainnya. Metode yang digunakan adalah connectionless yang berarti tidak perlu membuat dab memelihara sesi koneksi. Selain itu protocol ini juga tidak menjamin penyampaian data.

2.5. Analisa Log Firewall

Pada penelitian ini file log yang digunakan adalah file log yang diambil pada bulan September tahun 2013. Pada file log yang diambil masih dalam bentuk format ASCII yang mana setiap record akan disimpan dalam baris baru. Menggunakan software CAAT dari picalo[7] untuk melakukan konversi file dari ASCII ke dalam table sehingga mudah untuk dilakukan analisa data nantinya.



Gambar 2. Hasil analisa firewall log

Setelah dilakukan analisa dengan memasukkan script berdasarkan table yang sudah ada, maka didapatkan hasil analisanya sebagai berikut. Di bawah ini adalah script yang digunakan untuk melihat trend alamat apa saja yang sering digunakan pada tanggal 9 september 2013.

```
facebook =
Trending.handshake_slope(All_Behavior_Logs_01
_30_09_2013, "Dst_Address")

facebook =
Trending.handshake_slope(All_Behavior_Logs_01
_30_09_2013, "Dst_Address")

facebook =
Grouping.summarize_by_value(All_Behavior_Logs
_01_30_09_2013, "User", "Host_IP",
"Dst_Address", facebook="facebook")

facebook.view()
```

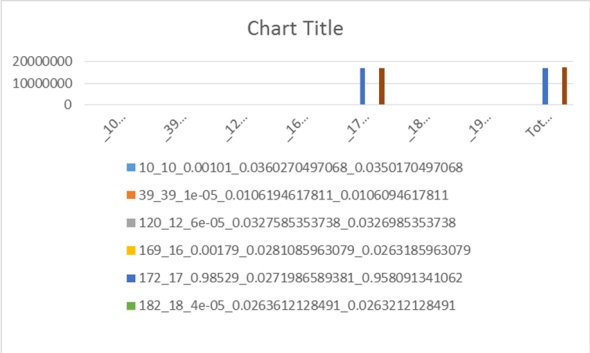
2.6. Uji Metode Benford's Law

Untuk menguji temuan audit maka dibuat pola frekuensi dari nilai log yang yang diharapkan oleh Benford's Law. Perbedaan tersebut meliputi perbedaan pada digit pertama (First Digit/FD) dan digit kedua (Second Digit/SD).

Tabel 1. Definisi Operasional Variabel

Var	Keterangan	Jenis	Penjelasan
X1	MAD FD	Independen	Nilai perbedaan antara proporsi angka actual pada digit pertama yang diharapkan menurut Benford's Law
X2	MAD SD	Independen	Nilai perbedaan antara proporsi angka actual pada digit kedua yang diharapkan menurut Benford's Law

Dalam menganalisa pola frekuensi, digunakan perangkat lunak Picalo dan Micosoft Excel. Analisa ini digunakan untuk melihat apakah pola frekuensi angka actual pada data ini sama ataukah berbeda dengan frekuensi yang diharapkan menurut *Benford's Law*. Pengujian dilakukan dengan dua tes yaitu First-Digit Tes dan Second-Digit Tes.



Gambar 3. Hasil analisa Benford's Law

Berdasarkan diagram pada gambar diatas diketahui bahwa model *First-Digit* (warna biru) mempunyai nilai yang sama dengan model *Second-Digit* (warna merah) atau bias dikataka bahwa data tersebut tidak memiliki anomaly data. Anomaly data adalah nilai yang berbeda dari data sebenarnya. Nilai anomaly bias lebih besar atau bias juga lebih kecil dari data sesungguhnya.

3. Kesimpulan

Log termasuk di dalam bagian forensik audit untuk membantu dalam melakukan analisa. Dengan menggunakan software, fungsi analisis semakin cepat dan dapat digunakan untuk melakukan kebijakan yang berhubungan dengan perkembangan atau kebutuhan dari suatu organisasi.

Dari hasil penelitian ini, disimpulkan bahwa pada file log firewall ini tidak terdapat kegiatan yang mencurigakan, yang dapat merugikan sebuah organisasi atau perusahaan. Perbedaan antara dua model fist-digit dan second-digit dapat menghasilkan angka yang signifikan. Jika nilai perbedaan angka actual digit pertama dan digit kedua berbeda maka kemungkinan temuan fraud pada audit semakin besar.

Daftar Pustaka

[1] Radian Victor Imbar, "Pelaksanaan kontrol dan audit sistem informasi pada organisasi", Jurnal informatika UKM, Vol 1 No 1 2005
[2] Peter J Best, "Detection of anomalous computer session activity" Security and Privacy, Proceedings., 1989 IEEE Symposium
[3] Tongshen, Xiamin, Qingzhang, "Design and implementing of Firewall-log-based Online Attack Detection System" Proceedings of the 3rd International Conference on Information Security, Page 146-149, 2004
[4] Todd Lammie, "CCNA Cisco Certified Network Accociate Study Guide", Elex Media Komputindo, 2005.
[5] Sutabri, *Analisa Sistem Informasi*, Yogyakarta, Andi, 2004
[6] Mahendra Adi Nugroho "Audit Lingkungan TI : Perspektif dan dampak pada proses auditing secara komprehensif", Jurnal Pendidikan Akuntansi Indonesia, 2011
[7] picalo.org
[8] Muhammad Mufti Arkan, "Analisis penggunaan Benford dalam perencanaan audit pada Direktorat Jenderal Bea dan Cukai", Simposium Nasional Akuntansi XIII, 2010
[9] Nigrini, Mark J, "Digital Analysis Using Benford's Law : test and statictic for auditors", Global Audit Publication, 2000

Biodata Penulis

Emilya Ully Artha M.Kom, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta, lulus tahun 2005. Memperoleh gelar Magister Komputer (M.Kom) Program Pasca Sarjana Magister Teknik Informatika STMIK AMIKOM Yogyakarta, lulus tahun 2012. Saat ini menjadi Dosen di STMIK AMIKOM Yogyakarta.

ISSN : 2302-3805