Bidang Ilmu: Teknik Informatika

LAPORAN

PENELITIAN DOSEN PEMULA

Judul Penelitian

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

Peneliti:

EMILYA ULLY ARTHA

0512128101

JURUSAN TEKNIK INFORMATIKA

STMIK AMIKOM YOGYAKARTA

2015

Halaman Pengesahan

1. Judul Penelitian : Analisa CAATs (Computer Assisted Audit Techniques) Untuk Identifikasi Data Log Firewall
2. Bidang Penelitian : Teknik Informatika
3. Ketua Peneliti
   a. Nama Lengkap dan gelar : Emilya Ully Artha M.Kom
   b. Jenis Kelamin : Laki-laki
   c. NIP/NIDN : 190302223/0512128101
   d. Pangkat / Golongan : -
   e. Jabatan Fungsional : -
   f. Perguruan Tinggi : STMIK AMIKOM Yogyakarta
   g. Program Studi : Teknik Informatika
   h. Status Dosen : Dosen
4. Pembimbing
   a. Nama Lengkap dan gelar : Hanif Al Fatta, M.Kom
   b. Jabatan Fungsional : Lektor
   c. Unit Kerja / PT : STMIK AMIKOM Yogyakarta
5. Jumlah Tim Peneliti : 1 orang
6. Lokasi Penelitian : Lab Jaringan Komputer (Lab 13)
   a. Alamat : Ring Road Utara, Condong Catur, Depok, Sleman
   b. Telepon/Faks : (0274) 884201 / (0274) 884208
7. Jumlah biaya :
   a. Dari P3M STMIK AMIKOM : Rp. 3.000.000,-

      (Tiga Juta Rupiah)

Yogyakarta, 1 Juni 2015

Mengetahui,

Ketua Jurusan D3TI,	Peneliti,
Hanif Al Fatta, M.Kom	Emilya Ully Artha M.Kom
NIP/NIDN : 190302096	NIP/NIDN. 190302223

Menyetujui,

Dosen Pembimbing	Ketua Bagian P3M
Hanif Al Fatta, M.Kom	Heri Sismoro, M.Kom
NIP/NIDN : 190302096	NIP/NIDN.0523057401

DAFTAR ISI

Halaman

RINGKASAN

Perusahaan atau organisasi pada perkembangannya mempunyai kecenderungan untuk mengadopsi Teknologi Informasi untuk menjalankan bisnisnya. Perusahaan atau organisasi cenderung memanfaatkan teknologi untuk meningkatkan efisiensi yang bertujuan untuk mendongkrak pendapatan dan memperbaiki kinerja. Salah satu dampak yang sangat berpengaruh adalah pada proses auditing, adanya pergeseran audit tradisional yang berbasis tugas menuju audit teknologi informasi (TI) berbasis resiko. *Internal Audit* (IA) merupakan salah satu cabang ilmu yang sangat penting sebagai penghubung bisnis di dalam suatu organisasi. Semakin besar suatu organisasi maka semakin kompleks permasalahan (*fraud*) yang muncul. 80% lebih celah keamanan berasal dari dalam suatu organisasi, bukan dari luar. Kecurangan (*fraud*) perlu dibedakan dengan kesalahan (*error*). Kesalahan dapat terjadi pada setiap pengolahan/pengelolaan transaksi data. Tetapi bila kesalahan ini disengaja maka dapat dianggap sebagai kecurangan. Untuk meminimalisir tingkat *fraud* maka dibuatlah sebuah system yang biasa disebut dengan *firewall*. Dari firewall ini akan dikeluarkan sebuah file (*log*) dari hasil inspeksi yan dilakukan oleh system firewall. Menggunakan metodelogi *transaction pattern level* yang mana menggunakan perangkat audit *Computer Assisted Audit Techniques* (CAAT) pada transaksi real time yang mana data diambil dari *log data* dan setiap data diambil menggunakan sumber yang sama.

Kata-kata kunci: *internal audit, CAAT, fraud, firewall, log data, TI*

BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Perkembangan teknologi saat ini mengakibatkan segala sesuatu yang memungkinkan diatur oleh komputer. Dan sistem kerja secara manual perlahan-lahan mulai tergeser dengan adanya teknologi yang semakin canggih. Pergeseran ini mengakibatkan pola penyimpanan data yang semakin besar, perubahan terhadap kesediaan informasi, serta perubahan dalam pengambilan keputusan yang cepat, efisien dan bertanggung jawab. Keuntungan dari perubahan ini adalah semakin cepat dan efisien dalam hal pengambilan keputusan tetapi tidak menjamin suatu system bebas dari kesalahan atau kecurangan sehingga menimbulkan kerugian di satu sisi seperti pemborosan, manipulasi data, atau pencurian yang dilakukan oleh pihak dalam maupun luar 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, pencatatan debit kredit dan sebagainya. Kesalahan dapat pula terjadi dalam bentuk perhitungan matematis, atau interpretasi fakta. Apabila kesalahan adalah disengaja, maka kesalahan itu merupakan suatu kecurangan (*fraudelent*). *Fraud Auditing* adalah upaya untuk mencegah kecurangan dalam transaksi-transaksi komersial.

Audit Sistem Informasi (SI) adalah fungsi dari organisasi yang mengevaluasi keamanan aset, integritas data, efektifitas, dan efisiensi sistem dalam sistem informasi berbasis komputer. Menurut (Radian, 2005) kebutuhan audit SI ini disebabkan oleh beberapa faktor yaitu :

1. Kemungkinan kehilangan data
2. Kemungkinan kesalahan penempatan sumber daya akibat kesalahan pengambilan keputusan yang diakibatkan karena kesalahan pemrosesan data
3. Kemungkinan komputer rusak karena tidak terkontrol
4. Harga komputer hardware/software yang mahal

5. Biaya operasional yang tinggi apabila komputer rusak
6. Kebutuhan privacy dari suatu organisasi/perorangan
7. Kebutuhan untuk mengontrol penggunaan komputer

Sebagian besar implementasi audit khususnya auditor SI secara khusus berkonsentrasi pada efektifitas pengendalian atau kontrol sistem. Kontrol sendiri adalah sebuah bentuk dari sistem yang berfungsi untuk mencegah, mendeteksi atau memperbaiki situasi yang tidak teratur. Fungsi kontrol sendiri dibagi menjadi tiga bagian yaitu *Preventive Control*, yaitu intruksi yang diletakkan pada dokumen untuk mencegah kesalahan pemasukan data. *Detective Control*, yaitu kontrol yang diletakkan pada program yang berfungsi mendeteksi kesalahan pemasukan data. *Corrective Control*, yaitu program yang dibuat khusus untuk memperbaiki kesalahan pada data yang mungkin timbul akibat gangguan pada jaringan, komputer ataupun kesalahan pengguna (*user*).

Resiko dan pengendalian merupakan dua mata uang yang tidak dapat dipisahkan. Semakin baik pengendalian maka semakin kecil resiko yang harus dihadapi sebuah sistem. Semakin kecil resiko maka semakin baik pula suatu sistem. Baik buruknya suatu sistem sangat mempengaruhi bukti yang dihasilkan dari sistem tersebut. Untuk mengetahuinya dapat dilihat dari pengendalian internal yang dilakukan oleh sistem tersebut. Semakin baik suatu sistem pengendalian internal, sistem dan bukti yang dihasilkan sistem tersebut akan semakin dapat dipercaya (Mahendra, 2011)

Peningkatan kompleksitas kegiatan bisnis mengakibatkan semakin tingginya resiko kesalahan interpretasi dan penyajian laporan keuangan yang mana hal ini menyulitkan para *users* dalam mengevaluasi kualitas laporan. Dalam kenyataannya banyak para auditor tidak banyak para auditor yang bisa memanfaatkan aset dari peranan teknologi informasi dalam mengaudit sistem informasi yang berbasis pada komputerisasi baik pada saat *input*, proses sampai dengan *output*. Mengingat *brainware* dibidang auditor yang mengenal teknologi informasi masih relatif sedikit.

1.2. Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah bagaimana analisa log pada penggunaan internet di STMIK AMIKOM Yogyakarta dapat menjadi masukan bagi bagian pelayanan IT serta sebagai acuan untuk para pengambil kebijakan di kampus STMIK AMIKOM Yogyakarta.

1.3. Tujuan Penelitian

Adapun tujuan yang ingin dicapai adalah sebagai pengendalian aplikasi yang tujuaanya saling melengkapi untuk pengendalian umum, dan dapat digunakan sebagai pengambilan keputusan.

1.4. Manfaat Penelitian

Dari hasil penelitian yang akan dilakukan, untuk menghasilkan beberapa manfaat sebagai berikut :

1. Bagi lembaga pendidikan : yaitu diharapkan dapat membantu bagi pihak pengelola lembaga pendidikan dalam proses kegiatan pendidikan, serta dapat memanfaatkan penggunaan internet secara efektif sebagai bagian dari proses pengembangan keilmuan
2. Bagi para peneliti : dapat lebih memahami cara untuk melakukan fungsi control (audit) serta analisa pada log file.

,

BAB II
KAJIAN PUSTAKA

2.1. Audit Sistem Informasi

Penggunaan teknologi informasi mampu memberikan manfaat yang besar terhadap dunia bisnis yang kompetitif dan dinamis. Perusahaan yang mampu bersaing dalam kompetisi tersebut bisa dikatakan sebagai perusahaan yang mampu untuk menerapkan pengembangan dan pemanfaatan teknologi ke dalam bisnis. Sedangkan sistem informasi adalah suatu kombinasi dari orang-orang, fasilitas, teknologi, media, prosedur-prosedur dan pengendalian yang ditunjukkan untuk mendapatkan jalur komunikasi yang penting, memproses tipe transaksi rutin tertentu, memberi sinyal kepada manajemen dan yang lainnya terhadap kejadian-kejadian internal dan eksternal yang penting dan menyediakan suatu dasar untuk pengambilan keputusan yang cerdik (Moscove dan Simkin, 1984; dalam Jogiyanto, 2007:17).

Keuntungan dari sistem informasi yang sudah terkomputerisasi adalah peningkatan kecepatan, keakuratan dalam pengolahan data informasi. Sistem informasi sebagai suatu sistem yang terbuka (*open system*) tidak bisa menjamin sebagai suatu sistem terbebas dari kesalahan atau kecurangan (Aviana, 2012). Sehingga pengendalian internal yang baik merupakan cara bagi suatu sistem untuk melindungi dirinya dari hal-hal yang merugikan. Pengendalian internal yang memadai diperlukan untuk mengawasi jalannya aktivitas perusahaan. Sistem pengendalian internal diharapkan mampu mengurangi kelemahan, kesalahan, dan kecurangan yang terjadi.

Committe of Sponsoring Organizations of the Treadway Commision (COSO) mengeluarkan *framework* atau panduan untuk pengendalian internal (*internal control*) sebagai kerangka kerja pengendalian internal yang dirancang dan diimplementasikan oleh manajemen untuk memberikan kepastian yang layak bahwa tujuan pengendalian akan tercapai. Adapun komponen pengendalian internal COSO meliputi hal-hal berikut ini :

1. Lingkungan pengendalian

   Lingkungan penngendalian terdiri atas tindakan, kebijakan dan prosedur yang mencerminkan sikap manajemen puncak, para direktur dan pemilik entitas secara keseluruhan mengenai pengendalian internal serta arti pentingnya bagi intetas tersebut. Faktor lingkungan pengendalian meliputi integritas, nilai etis, gaya operasi manajemen, sistem pelimpahan wewenang, dan proses untuk mengatur dan mengembangkan sumber daya manusia dalam organisasi.

2. Penilaian resiko

   penilaian resiko oleh manajemen untuk menilai resiko sebagai bagian dari perancangan dan pelaksanaan pengendalian internal untuk meminimalkan kekeliruan serta kecurangan yang mungkin akan terjadi. Proses penilaian resiko yaitu mengidentifikasi faktor-faktor yang mempengaruhi resiko, menilai signifikan resiko dan kemungkinan terjadi serta menentukan tindakan yang diperlukan untuk mengelola resiko.

3. Aktivitas pengendalian

   Aktivitas pengendalian adalah kebijakan dan prosedur yang membantu memastikan bahwa tindakan yang diperlukan telah diambil untuk menangani resiko untuk mencapai tujuan entitas. Aktivitas pengendalian umumnya dibagi menjadi 5 jenis yaitu :

   a. Pemisahan tugas yang memadai

   b. Otorisasi yang sesuai atas transaksi dan aktivitas

   c. Dokumen dan catatan yang memadai

   d. Pengendalian fisik atas aktiva dan catatan

   e. Pemeriksaan kinerja secara independen

4. Informasi dan komunikasi

   Tujuan sistem informasi dan komunikasi dari entitas adalah untuk memulai, mencatat, memproses dan melaporkan transaksi yang dilakukan entitas terkait.

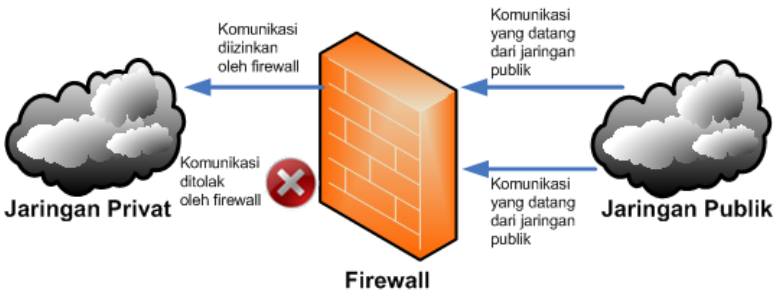
5. Pemantauan

Aktivitas pemantauan berhubungan dengan penilaian mutu pengendalian internal secara berkelanjutan atau periodik oleh manajemen untuk menentukan bahwa pengendalian itu telah beroperasi seperti yang diharapkan dan telah dimodifikasi sesuai dengan perubahan kondisi.

Kegiatan pengendalian adalah kebijakan dan prosedur yang digunakan untuk memastikan bahwa tindakan yang benar diambil untuk menghadapi resiko organisasi yang diidentifikasi. Pengendalian internal dikelompokkan menjadi dua kategori yaitu pengendalian internal komputerisasi dan pengendalian internal tradisional atau manual (Hall, 2001:158-163).

2.2. Firewall

Firewall adalah sebuh 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 terdedikasi, yang berjalan pada pintu gerbang (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 pertama dari firewall adalah adalah firewall harus dapat mengatur dan mengontrol lalu lintas jaringan yang diizinkan untuk mengakses jaringan privat atau komputer yang dilindungi firewall. Firewall melakukan fungsi inspeksi terhadap paket-paket dan memantau koneksi yang sedang dibuat, lalu melakukan filtering terhadap koneksi berdasarkan hasil inspeksi paket tersebut.



Gambar 2.1 *Firewall*

2.3. Protokol

Protokol adalah sebuah standar aturan yang mengatur alat-alat dalam jaringan komputer sehingga dapat berkomunikasi satu sama lain. Dan dapat melakukan perpindahan data. Banyak hal yang dapat dilakukan oleh protokol. Misalnya :

1. Melakukan deteksi terhadap perangkat fisik
2. Melakukan metode handshaking
3. Melakukan fungsi tes koneksi terhadap berbagai macam koneksi
4. Mengawali dan mengakhiri suatu pesan
5. Mengatur format pesan yang akan dilakukan
6. Mengakhiri suatu koneksi

Seiring berjalannya waktu pada tahun 1981 dibentuk *Transmision Control Protocol* (TCP) dan *Internet Protocol* (IP) sebagai protokol yang digunakan untuk komunikasi dalam jaringan komputer. Pada tahun 1983 diresmikan Ipv4 sebagai protokol untuk internet untuk pengalamatan tiap-tiap komputer[1]. *Interconnected-network* atau yang lebih popular sering disebut dengan Internet adalah sebuah sistem komunikasi global yang menghubungkan komputer-komputer dan jaringan-jaringan komputer di seluruh dunia (Fikri Heriyanto, 2006) . Setiap komputer dan jaringan terhubung secara langsung maupun tidak langsung ke beberapa jalur utama yang disebut dengan *internet backbone*[2] dan dibedakan satu dengan yang lainnya menggunakan *unique name* yang biasa disebut dengan alamat IP (*Internet Protokol Address*). Ketika sebuah jaringan komputer yang dikelola semakin besar maka

[1] http://tools.ietf.org/html/rfc791

[2] merupakan teknik pengiriman data dalam bentuk sinyal analog secara kontinyu. Data dikirimkan dalam melalui media pengirim dalam bentuk gelombang elektromagnetik.

dibutuhkan pula sebuah mekanisme teknis mengenai pemetaan routing secara dinamis, karena routing statik sudah tidak bisa diandalkan untuk kondisi jaringan yang kompleks (Achmad Kodar, 2010)

2.4. Log File

Log adalah catatan atau pesan yang tersimpan dalam sebuah file, biasanya mewakili pesan proses aplikasi yang berjalan. Terdapat berbagai macam jenis log diantaranya adalah *error log*, *cache log*, *user log* dan *update log*. Log file dapat merupakan sumber informasi yang penting bagi proses forensik. Dalam administrasi sistem, para administrator akan sering berhubungan dengan file log. Tergantung dari program yang digunakan untuk menghasilkan log. Semisal program web server, log file dapat menunjukkan hit yang diterima oleh suatu situs, browser apa saja yang digunakan oleh pengunjung situs. Contoh yang lain adalah program yang digunakan untuk sekuritas, log file dapat menunjukkan usaha penjebolan keamanan yang dilakukan seseorang.

File log yang dihasilkan oleh suatu program dapat berupa file biner ataupun 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 perbarus. Setiap kali program me-log aktivitas, catatan tersebut disusun dalam satu baris dan ditambahkan di akhir file log (*append*) (Sutabri, 2004).

BAB III

METODELOGI PENELITIAN

3.1. Metode Penelitian

Penelitian ini akan menggunakan metode atau pendekatan studi literature. Yang mana methode literature ini akan membandingkan dua hal. Pertama adalah *treath monitoring*, yaitu data yang muncul akan dibuat tingkatan berdasarkan kebutuhan analisa. Dan yang kedua adalah analisa *audit trails* dari file log ke pembuatan dokumen. *Audit trails* sendiri dapat menggunakan beberapa cara. Antara lain (Peter J Best : 2005)

1. Pengujian dengan data simulasi

   Pemeriksa dapat langsung memeriksa sistem pengolahan dengan menggunakan transaksi simulasi sebagai bahan pengujian. Beberapa program aplikasi diuji kemampuannya dalam memproses data data hingga dapat diketahui apakah program berjalan benar atau ditemukan kesalahan
2. Pemanfaatan fasilitas pengujian secara terpadu

   Teknik ini merupakan perluasan dari teknik pengujian data. Transaksi simulasi digabung dengan transaksi sebenarnya dengan cara memberikan suatu kode khusus. Yang mana kode ini digunakan sebagai error detection.
3. Simulasi pararel

   Pemeriksa membuat simulasi pemrosesan dengan memanfaatkan program yang disusun oleh auditor, yaitu model aplikasi yang dipakai secara rutin. Dari hasil perbandingan ini akan diketahui apakah program/sistem ada penyimpangannya.
4. Pemasangan modul pemeriksaan

   Auditor dapat memasang program pemeriksaan ke dalam program aplikasi untuk memantau secara otomatis sehingga dapat terhimpun data untuk keperluan pemeriksaan sehingga akan muncul catatan log secara berkala.
5. Pemakaian perangkat lunak khusus untuk pemeriksaan

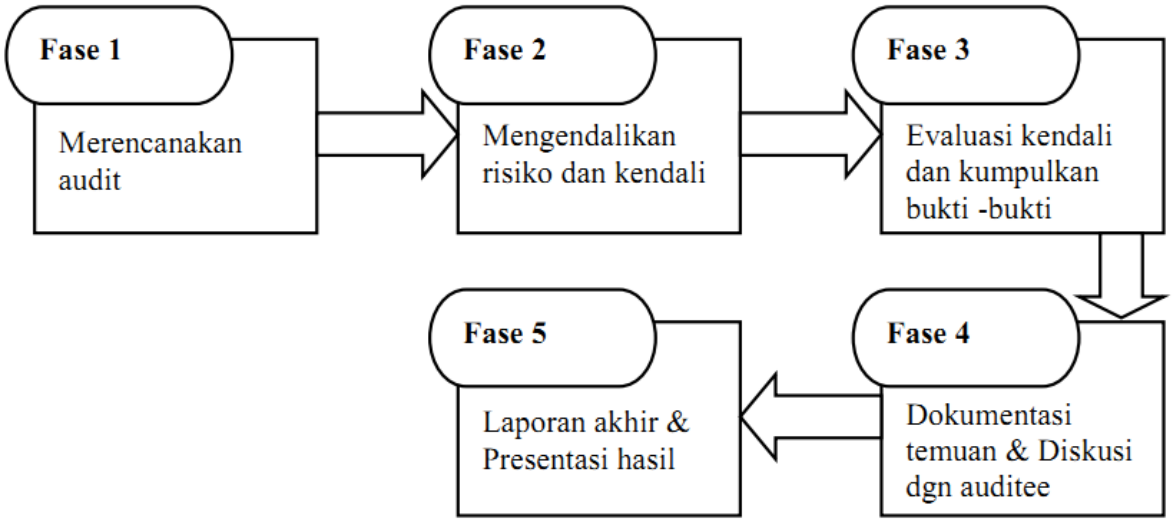
(audit software) pemeriksa dapat menguji keandalan dokumentasi dan berkas suatu objek pemeriksaan. Beberapa software yang sering digunakan yaitu *Generelized Audit Software*, *Audit Command Language* (ACL), *Audasist*, *IDEA-Y*, Picalo.

6. Metode tracing

   Pemeriksa dapat melakukan penelusuran terhadap suatu program/sistem aplikasi untuk menguji keandalan kebenaran data masukan dalam pengujian ketaatan, pemeriksa mencetak daftar instruksi program yang dijalankan sehingga dapat ditelusuri apakah suatu instruksi telah dijalankan selama proses

7. Metode pemetaan (*mapping*)

   Pemeriksa dapat memasukkan kode-kode tertentu yang tidak dikehendaki yang disiapkan ke dalam program untuk kepentingannya. Lalu memilah bagian mana yang akan dikehendaki untuk dianalisa.



Sumber: eBizzAsia, Volume II No 17 - Mei - Juni 2004

Gambar 3.1 *Alur Audit Trail Analisis*

Pada penelitian ini nantinya akan menggunakan perangkat lunak audit yaitu *Audit Command Language* (ACL) untuk melakukan proses analisa data dan dokumentasi.

3.2. Lokasi Penelitian

Lokasi penelitian adalah lingkungan kampus STMIK AMIKOM Yogyakarta dengan mengambil data log dari gateway amikom yogyakarta.

3.3. Pemilihan Informan

Di dalam penelitian ini akan dilakukan pemilihan informan untuk mendukung hasil penelitian, maka pemilihan informan yaitu Bagian/Departemen yang secara langsung berhubungan dengan operasiomal gateway yang ada di STMIK AMIKOM Yogyakarta dalam hal ini adalah Departemen ICT.

3.4. Sumber Data

Adapun data yang diambil adalah data file log penggunaan internet selama 2 bulan dalam rentang kegiatan selama perkuliahan aktif. Pengambilan data sekunder juga akan digunakan baik berupa laporan administrasi atau dokumen yang berhubungan dengan pengendalian dan penyimpanan arsip.

3.5. Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini akan menggunakan teknik sebagai berikut :

1. Observasi atau pengamatan

   Pengumpulan data penelitian ini akan dilakukan melalui pengamatan langsung terhadap objek analisis untuk mengali aspek-aspek yang berhubungan langsung dengan penggunaan internet sebagai dasar dari penelitian.
2. Wawancara

   Wawancara dimaksudkan untuk memperoleh data kuantitatif serta beberapa keterangan atau informasi dari Departemen IT

3.6. Analisis Data

Analisis Data atau Pengolah Data adalah bentuk analisis yang lebih rinci dan mendalam juga membahas suatu tema atau pokok permasalahan. Untuk data

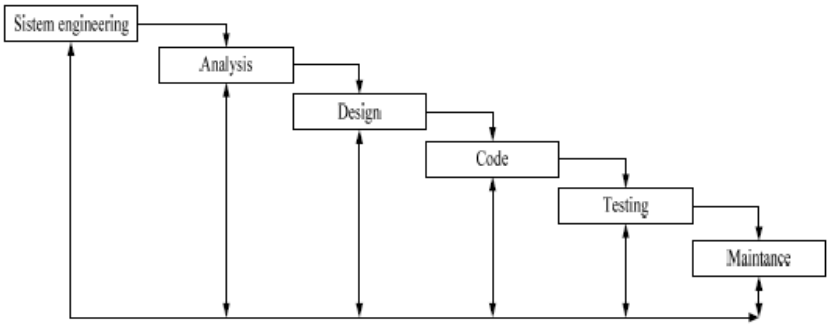
kualitatif yang diperoleh dengan wawancara mendalam, dengan metode analisis *operational component*. Dalam pelaksanaan analsis data kualitatif bertujuan pada penggalian makna, penggambaran, penjelasan dan penempatan data pada konteksnya masing-masing. Uraian data jenis ini berupa kalimat-kalimat.

3.6.1. Tahap Anaisis Sistem

Tahap analisis kebutuhan sistem dilakukan dengan mengidentifikasikan seluruh proses yang telah dipetakan dalam diagram alir proses bisnis. Proses bisnis ini nantinya yang akan digunakan sebagai panduan untuk melakukan audit trails.

3.6.2. Metode Perancangan Sistem

Pada tahapan ini diarahkan terhadap analisis & perancangan sistem yang dibutuhkan untuk meminimalisir kekurangan dari sistem sebelumnya. Pada tahapan ini melakukan pengembangan sistem dengan menggunakan metode *Systems Development Life Cycle* model klasik yang biasa disebut metode *waterfall*. SDLC (*Systems Development Life Cycle*).



Gambar 3.2. Model *Waterfall*

Dalam gambar di atas hanya menggunakan 5 tahapan, menurut Pressman dalam buku Mulyanto (2009). Yang meliputi :

1. Penelitian Sistem

   Tahap untuk meneliti dan mengidentifikasi kebutuhan apa saja yang diperlukan *user*, hal ini berkaitan dengan fasilitas-fasilitas yang ada dalam *website*. Proses

ini meliputi kegiatan studi kelayakan yang mencakup sisi kelayakan teknis, ekonomis, organisasional, dan keperilakuan.

2. Analisis Sistem

   Tahap yang menjelaskan apa yang harus dilakukan sistem untuk mengatasi masalah, sehingga di dalamnya dilakukan kegiatan menganalisis kebutuhan, proses menganalisis fasilitas-fasilitas apa saja yang diinginkan dalam membangun sistem informasi tersebut.

3. Desain Sistem

   Desain sistem terdiri dari beberapa rancangan, yaitu :

   1) Perancangan Proses (menggunakan *flowchart system* dan *data flow chart*/DFD).
   2) Perancangan Tabel Basis Data.
   3) Perancangan Antarmuka (*Interface*)

4. Pengkodean

   Proses pengkodean yaitu mengubah ke dalam bentuk yang dapat dibaca oleh mesin.

5. Pengetesan

   Proses yang memastikan semua kalimat dalam program telah dilakukan pengetesan sehingga memberikan *input* sesuai dengan yang diinginkan.

   Dalam penelitian ini yang akan ditekankan adalah pada bagian analisanya.

3.6.3 Hasil Analisis

Dari metode analisis yang telah dilaksanakan, dapat diketahui hasil analisis untuk pembuatan laporan audit. Berikut adalah penjelasan lebih lanjut.

1. Analisis Kebutuhan Masukan

Masukan data pada sistem ini dilakukan oleh 2 pengguna, yaitu:

1. Masukan Admin
2. Masukan dari pengguna internet

2. Analisis Kebutuhan Proses

Kebutuhan proses dari sistem informasi penggunaan internet ini antara lain

1. Proses *login*

   Proses *login* dilakukan oleh semua pengguna sebelum memasuki sistem. Setelah proses *login* berhasil, pengguna dapat mengakses internet.

2. Proses *logout*

   Dilakukan apabila pengguna telah selesai mengakses sistem. Pengguna dapat kembali mengakses sistem dengan melalui proses *login*.

3. Proses ganti *password*

   Proses ini dapat dilakukan oleh administrator yang memegan kendali terhadap para pengguna.

4. Proses pencarian data

   Proses ini dilakukan pada saat file log muncul. Proses pencarian dilakukan dengan memasukkan kata kunci ke dalam sistem.

3. Analisis Kebutuhan Keluaran

Berikut ini adalah beberapa informasi yang dihasilkan, yaitu: informasi pengguna yang login ke system, waktu penggunaan, rata-rata penggunaan bandwith, serta kegiatan yang dilakukan selama melakukan kegiatan di internet

BAB IV

HASIL ANALISA

4.1. Benford's Law

Benford's Law atau hukum 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.

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* :

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).

4.2. 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

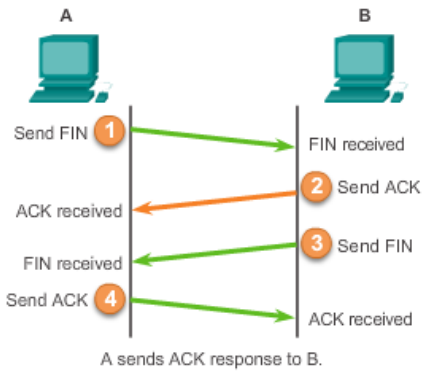
dimana informasi disusun perbaris. Setiap kali program me-log aktivitas, catatan tersebut disusun dalam satu baris dan ditambahkan di baris terakhir (*append*)[5]. Logging data (data logging) adalah proses otomatis pengumpulan dan perekaman data dari sensor untuk tujuan pengarsipan atau tujuan analisis. Dalam ilmu komputer data adalah informasi yang digunakan oleh komputer yang bukan merupakan kode program namun digunakan dalam komputasi program.

4.3. 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 4.1. *TCP Three-way handshake*

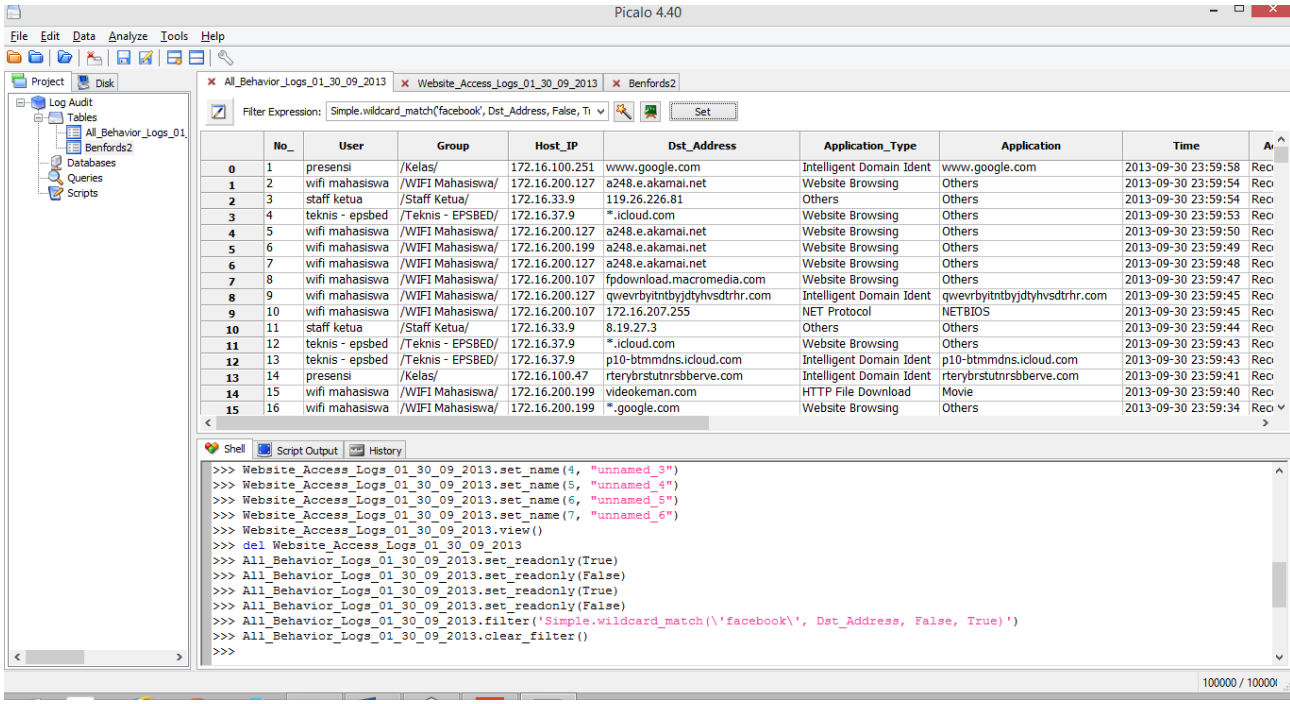
Prosesnya adalah sebagai berikut :

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.

4.4. 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 4.2. *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()
```

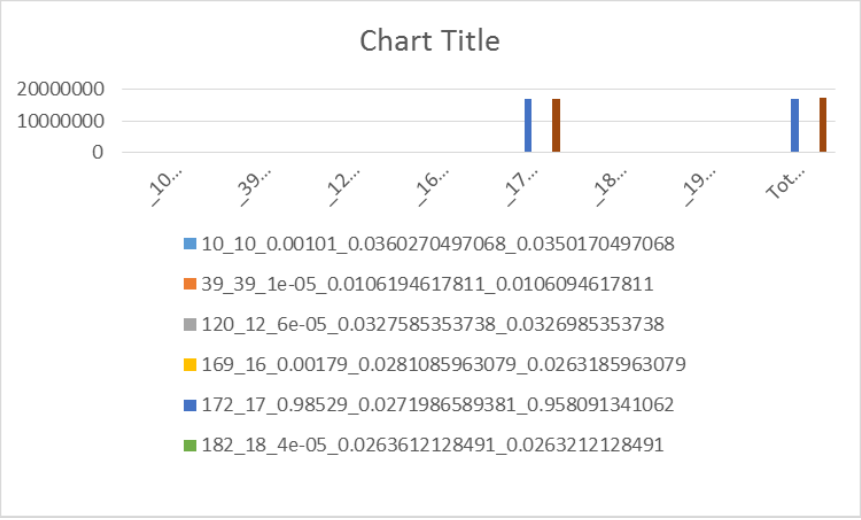
4.5. Uji Metode Benford's Law

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 4.3. 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.

BAB V
PENUTUP

5.1. 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.

5.2. Saran

Keterbatasan pengujian disebabkan karena data yang diambil sangat minim, serta perangkat keras yang kurang memadai untuk melakukan tracking log. Penelitian berikutnya dapat menggunakan perangkat keras yang memadai seperti server dan database yang dapat diakses untuk pencarian data log.

DAFTAR PUSTAKA

Fitri Annisa : Lutfi Haris, 2011, *Deteksi Indikasi Fraud Dengan Teknologi Audit*, Seminar Nasional Aplikasi Teknologi Informasi (SNATI), ISSN : 1907-5022

Isworo Nugroho, 2009, *Peranan Teknologi Informasi Dalam Audit Sistem Informasi Komputerisasi Akuntansi*, Dinamika Informatika Vol 1 No 2, ISSN : 2085-3343

Peter J Best, *Continous Fraud Detection In Enterprise Systems Trough Audit Trail Analysis, Journal of Digital Forensics*, Security and Law Vol 4 (1)

Putu Mega Selvya Aviana, 2012, *Penerapan Pengendalian Internal Dalam Sistem Informasi Akuntansi Berbasis Komputer*, Jurnal Ilmiah Mahasiswa Akuntansi Vol 1 No 4

Radian Victor Imbar, 2005, *Pelaksanaan Kontrol dan Audit Sistem Informasi Pada Organisasi*, Jurnal Informatika UKM, Vol 1 No 1

Sutabri, 2004, *Analisa Sistem Informasi*, Yogyakarta, Andi

Mahendra Adi Nugroho, 2011, *Audit Lingkungan TI : Perspektif dan dampak pada proses auditing secara komprehensif*, Jurnal Pendidikan Akuntansi Indonesia, Vol IX No 1 Tahun 2011, Hal 24-42

Lampiran 1

Rincian Biaya Penelitian

1. Honor				
Pelaksana	Honor/jam (Rp)	Waktu (jam/minggu)	Minggu	Honor per tahun (Rp) Tahun I
Ketua	Rp. 10.000	5	12	Rp. 600.000
			Sub total (Rp)	Rp. 2.800.000

2. Peralatan penunjang

Material	Justifikasi Pemakaian	Kuantitas	Harga Satuan (Rp)	Harga Peralatan Penunjang (Rp)
				Tahun I
Hard Disk Eksternal 1 terabyte	Digunakan untuk menyimpan data laporan dan log file	1	Rp. 1.200.000	Rp. 1.200.000
Akses Internet	Digunakan untuk mencari data	1	Rp. 100.000	Rp. 100.000
			Sub total (Rp)	Rp. 1.300.000

3. Bahan Habis Pakai

Material	Justifikasi Pemakaian	Kuantitas	Harga Satuan (Rp)	Biaya per Tahun (Rp)
				Tahun I
Kertas	Digunakan untuk media laporan mencetak penelitian (Selama 3 Bulan)	1	Rp. 50.000	Rp. 50.000
Tinta Printer/Catridge	Digunakan sebagai tinta printer untuk proses pencetakan laporan (3 Bulan)	1	Rp. 300.000	Rp. 300.000
			Sub total (Rp)	Rp. 350.000

4. Perjalanan

Perjalanan	Justifikasi Perjalanan	Kuantitas	Harga Satuan (Rp)	Biaya per Tahun (Rp) Tahun I
Biaya Transportasi survey dan pengumpulan data log	Digunakan sebagai akomodasi perjalanan untuk survey dan pengambilan data (selama 3 bulan)	1	Rp. 450.000	Rp. 450.000
			Sub total (Rp)	Rp. 450.000

5. Lain-lain

Kegiatan	Justifikasi	Kuantitas	Harga Satuan (Rp)	Biaya per Tahun (Rp) Tahun I
Penyususnan Laporan	Untuk menyusun Laporan penelitian dalam bentuk jilid (Selama 3 bulan)	2	Rp. 50.000	Rp. 100.000
Publikasi Journal	Untuk menerbitkan laporan penelitian dalam journal nasional	1	Rp. 200.000	Rp. 200.000
			Sub total (Rp)	Rp. 300.000
TOTAL ANGGARAN YANG DIPERLUKAN SETIAP TAHUN (Rp)				Tahun I Rp. 3.000.000

TOTAL ANGGARAN YANG DIPERLUKAN SELURUH TAHUN (Rp)	Rp. 3.000.000

LAMPIRAN 2

Susunan Organisasi Tim Peneliti Dan Pembagian Tugas

No	Nama / NIDN	Instansi Asal	Bidang Ilmu	Alokasi Waktu (jam/minggu)	Uraian Tugas
1.	Emilya Ully Artha/ 0512128101	STMIK AMIKOM YOGYAKARTA	Teknik Informatika	5 jam	1. Pembuatan analisa dan konsep 2. Survey dan observasi 3. Metodologi penelitian 4. Pengembangan dan analisis kebutuhan sistem 5. Analisa Data 6. Pembuatan laporan

LAMPIRAN 3

Format Biodata Ketua/Anggota Tim Peneliti/Pelaksana

KETUA PENELITIAN

A. Identitas Diri

1	Nama Lengkap (dengan gelar)	Emilya Ully Artha, M. Kom
2	Jenis Kelamin	L
3	Jabatan Fungsional	On progress
4	NIP/NIK/Identitas lainnya	190302223

5	NIDN	0512128101
6	Tempat, Tanggal Lahir	Pontianak, 12 Desember 1981
7	E-mail	ully@amikom.ac.id
8	Nomor Telepon/HP	081328747192
9	Alamat Kantor	STMIK AMIKOM Jl. Ringroad utara condongcatur, sleman, Yogyakarta
10	Nomor Telepon/Faks	(0274) 884201/(0274) 884208
11	Lulusan yang Telah Dihasilkan	S-1 = … orang; S-2 = … orang; S-3 = … orang
12	Nomor Telepon/Faks	
13	Mata Kuliah yang Diampu	1 Jaringan Komputer
		2 Pengantar Jaringan Komputer
		3 Sistem Operasi
		-
		-
		-

B. Riwayat Pendidikan

	S-1	S-2	S-3
Nama Perguruan Tinggi	STMIK AMIKOM	MTI STMIK AMIKOM	
Bidang Ilmu	Teknik Informatika	CIO	
Tahun Masuk-Lulus	2003-2005	2010-2012	

Judul Skripsi/Tesis/Disertasi	Tunnelling IPv6 menggunakan Zebra	Implementasi metoda fishbone pada Bagian Umum KanReg BKN Yogyakarta	
Nama Pembimbing/Promotor			

C. Pengalaman Penelitian Dalam 5 Tahun Terakhir

(Bukan Skripsi, Tesis, maupun Disertasi)

No.	Tahun	Judul Penelitian	Pendanaan	
			Sumber*	Jml (Juta Rp)
1				
2				
3				
dst				

* Tuliskan sumber pendanaan baik dari skema penelitian DIKTI maupun dari sumber lainnya.

D. Pengalaman Pengabdian Kepada Masyarakat dalam 5 Tahun Terakhir

No.	Tahun	Judul Pengabdian Kepada Masyarakat	Pendanaan	
			Sumber*	Jml (Juta Rp)
1				
2				
3				
dst				

* Tuliskan sumber pendanaan baik dari skema pengabdian kepada masyarakat DIKTI maupun dari sumber lainnya.

E. Publikasi Artikel Ilmiah Dalam Jurnal dalam 5 Tahun Terakhir

No.	Judul Artikel Ilmiah	Nama Jurnal	Volume/Nomor/Tahun
1	Pengembangan Sistem Pendukung Keputusan Untuk Penilaian Ujian Tugas Skripsi (Studi kasus pada STMIK AMIKOM Yogyakarta)	Journal DASI STMIK AMIKOM YOGYAKARTA	Jurnal Dasi Maret 2009
2			
3			
dst			

F. Pemakalah Seminar Ilmiah (*Oral Presentation*) dalam 5 Tahun Terakhir

No.	Nama Pertemuan Ilmiah / Seminar	Judul Artikel Ilmiah	Waktu dan Tempat
1			
2			
3			
dst			

G. Karya Buku dalam 5 Tahun Terakhir

No.	Judul Buku	Tahun	Jumlah Halaman	Penerbit
1				
2				
3				

H. Perolehan HKI dalam 5–10 Tahun Terakhir

No.	Judul/Tema HKI	Tahun	Jenis	Nomor P/ID

1				
2				
3				
dst				

I. Pengalaman Merumuskan Kebijakan Publik/Rekayasa Sosial Lainnya dalam 5 Tahun Terakhir

No.	Judul/Tema/Jenis Rekayasa Sosial Lainnya yang Telah Diterapkan	Tahun	Tempat Penerapan	Respon Masyarakat
1				
2				
3				
dst				

J. Penghargaan dalam 10 tahun Terakhir (dari pemerintah, asosiasi atau institusi lainnya)

No.	Jenis Penghargaan	Institusi Pemberi Penghargaan	Tahun
1	Juara 2 IPTEK	KEMENRISTEK	2011
2	Juara 2 Penggunaan Rekayasa Teknologi	Bupati Sleman	2011
3			
dst			

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidak-sesuaian dengan kenyataan, saya sanggup menerima sanksi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan Hibah Penelitian Dosen Pemula

Yogyakarta, 29 September 2014
Ketua Peneliti

(Emilya Ully Artha M.Kom)
NIP/NIK 190302223