Makalah Tugas Kuliah EL6115
Operasi Keamanan dan *Incident Handling*

PENERAPAN MODEL PROSES FORENSIK UNTUK MERESPON INSIDEN DAN MENGANALISIS PENGGUNAAN KOMPUTER

Oleh :

FITRIA RIDAYANTI
23214003

Dosen :

Dr. Ir. Budi Rahardjo

SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
PROGRAM MAGISTER TEKNIK ELEKTRO
INSTITUT TEKNOLOGI BANDUNG

2015

ABSTRAK

Metode umum yang biasa digunakan dalam memeriksa komputer tersangka sangatlah rumit, memakan banyak tenaga dan waktu yang lama, serta membutuhkan keahlian khusus dari ahli forensik. Dalam kasus-kasus tertentu, seperti penculikan anak dan orang hilang, waktu menjadi hal yang pokok dan respon insiden yang cepat sangat diperlukan. Namun saat ini kapasitas media penyimpanan semakin meningkat, hal ini membuat metode tersebut memerlukan waktu yang lebih lama. Oleh karena itu, diperlukan model proses forensik baru untuk mengumpulkan bukti-bukti penting dengan cepat dan menyelidiki kasus dengan cepat pula. Dalam makalah ini, diajukan suatu model proses forensik baru untuk memilih data target dan menganalisis bukti-bukti yang relevan saja sehingga proses investigasi menjadi lebih cepat selesai.

Kata kunci: forensik digital; model proses forensik; respon insiden; komputer forensik

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I PENDAHULUAN

Saat ini model yang digunakan dalam melakukan investigasi kejahatan digital masih sangat rumit, memakan tenaga yang banyak dan waktu yang lama, serta memerlukan keahlian khusus dari sang penyelidik. Dengan semakin berkembangnya teknis media penyimpanan, saat ini komputer modern dapat memiliki kapasitas penyimpanan hingga ratusan bahkan ribuan *gigabyte*. Selain itu, investigasi yang besar juga sering melibatkan beberapa sistem komputer sehingga jumlah data yang diproses dapat mencapai puluhan *terabyte* bahkan lebih, sedangkan jumlah waktu yang tersedia untuk memproses data tersebut terbatas [1].

Jenis pengumpulan data yang bergantung pada *images* forensik tentu memiliki keterbatasan. Peningkatan kapasitas media penyimpanan yang masih terus berkembang membuat metode investigasi memakan waktu yang lebih lama. Untuk proses *imaging* dari *hard disk* berkapasitas 250 GB saja memakan waktu lebih dari 90 menit dengan perangkat keras [2]. Hal ini mengakibatkan akan semakin banyak waktu yang diperlukan untuk mencari data yang berkaitan dengan kasus dari bukti-bukti yang dikumpulkan oleh penyidik, dan bukti digital pun menjadi sulit diperoleh [3].

Pada kasus gugatan perdata antar perusahaan, gugatan sering diajukan karena adanya kasus kebocoran rahasia bisnis. Hal ini membuat penyelidik tidak dapat memaksa pemilihan target investigasi, menyita dan menggandakan *hard disk*. Jadi, seperti yang sudah disebutkan sebelumnya, metode-metode untuk penyitaan yang selektif akan data yang berkaitan dengan kasus dan investigasi bukti merupakan hal yang penting [4].

Dalam makalah ini diberikan suatu model forensik baru yang diadaptasi dari model proses umum respon insiden dan komputer forensik, model umum investigasi forensik komputer, dan metodologi investigasi bertahap untuk menelusuri penggunaan komputer. Model proses ini bertujuan untuk memilih dan menyelidiki sistem secara efisien, yang memungkinkan seseorang untuk mengatasi keterbatasan dari model investigasi konvensional. Model ini memberikan identifikasi, akuisisi, dan analisis insiden untuk memilih dan menyelidiki bukti-bukti yang relevan saja. Makalah ini terdiri atas empat bab. Bab I berisi tentang pendahuluan, Bab II berisi tinjuan pustaka mengenai penelitian yang berkaitan dengan topik makalah, Bab III berisi rincian tahapan dari model proses forensik yang diajukan, dan Bab IV berisi kesimpulan dari makalah ini.

BAB II TINJAUAN PUSTAKA

Pada bab ini diberikan tinjauan pustaka mengenai penelitian yang berhubungan dengan topik makalah antara lain: model proses umum respon insiden dan forensik komputer, model umum investigasi forensik komputer, dan metodologi investigasi bertahap untuk menelusuri penggunaan komputer.

2.1 Model Proses Umum Respon Insiden dan Forensik Komputer

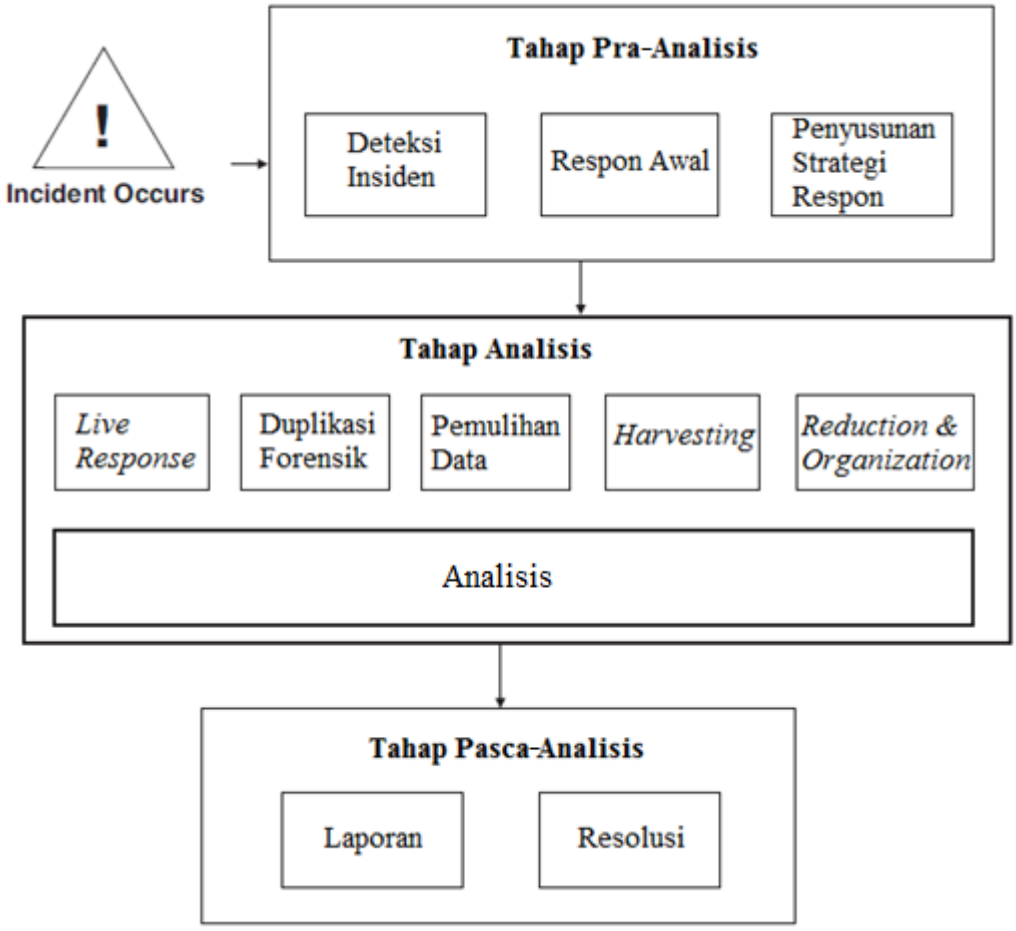
Model proses umum respon insiden dan forensik komputer merupakan model proses baru yang diajukan untuk menginvestigasi insiden keamanan komputer. Model proses ini menggabungkan konsep respon insiden dan forensik komputer untuk meningkatkan keseluruhan proses investigasi. Model proses ini terdiri atas tiga tahap utama, yaitu praanalisis, analisis, dan pascaanalisis. Model proses ini dapat dilihat pada Gambar II-1 [5].

Tahap praanalisis terdiri atas semua langkah dan kegiatan yang dilakukan sebelum memulai analisis yang sesungguhnya. Langkah-langkah yang dimaksud adalah melakukan persiapan pra insiden, mendeteksi insiden, memberi respon awal, dan menyusun strategi respon. Setelah tahap praanalisis selesai dilakukan, tahap selanjutnya adalah tahap analisis. Tahap analisis terdiri atas enam langkah, yaitu:

- *Live response*, yaitu mengumpulkan data dari sistem komputer yang masih hidup sehingga data yang bersifat *volatile* dapat diperoleh
- Duplikasi forensik, yaitu mendapatkan salinan eksak (*image*) dari semua media penyimpanan terkait dengan insiden
- Pemulihan data, yaitu memulihkan data yang telah terhapus, rusak, tersembunyi, atau yang tidak dapat diakses dalam *image* sistem berkas.
- *Harvesting*, yaitu mengumpulkan metadata.
- *Reduction & organization*, yaitu menghapus semua data yang tidak terkait dengan insiden dan mengatur data supaya dicari dengan efisien.

- Analisis, yaitu melakukan analisis yang sesungguhnya terhadap data yang diperoleh dari langkah-langkah sebelumnya.

Setelah tahap analisis selesai dilakukan, investigasi dilanjutkan ke tahap pascaanalisis. Langkah-langkah yang dilakukan pada tahap ini adalah membuat laporan dan memberikan resolusi atas insiden yang terjadi. Laporan berisi rincian insiden dan dokumentasi dari semua langkah yang dilakukan pada tahap praanalisis dan tahap analisis [5].

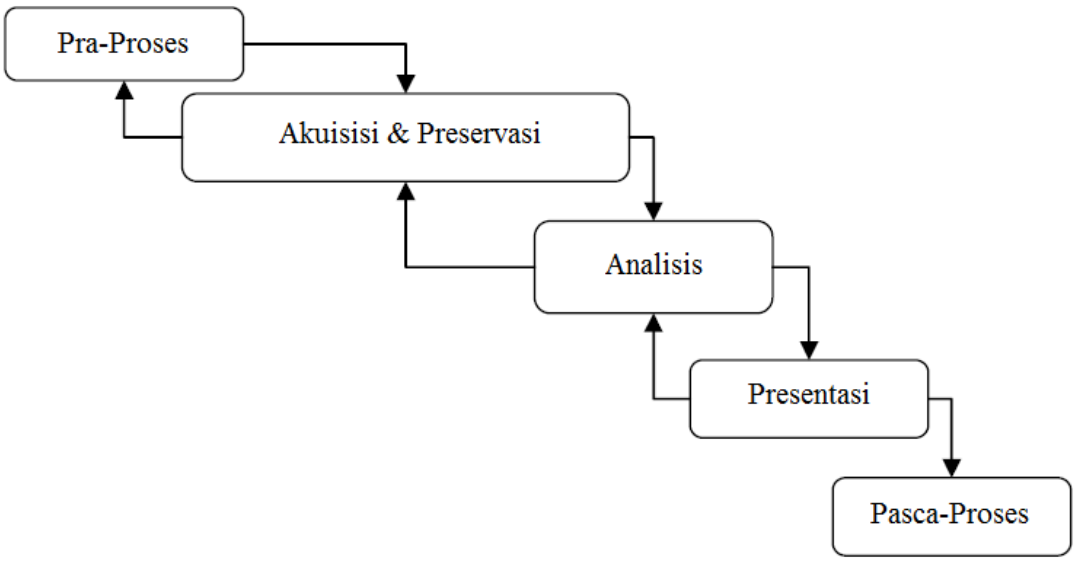


Gambar II-1 Model Proses Umum Respon Insiden dan Forensik Komputer [5]

2.2 Model Umum Investigasi Forensik Komputer

Model umum investigasi forensik komputer, atau dalam bahasa Inggris disebut sebagai *Generic Computer Forensic Investigation Model* (GCFIM), merupakan model yang didapatkan dengan membandingkan beberapa model proses forensik. Model ini terdiri atas lima tahap, yaitu [6]:

- Praproses, yaitu melakukan langkah-langkah yang perlu diselesaikan sebelum investigasi yang sesungguhnya dimulai (seperti mempersiapkan alat investigasi) serta mengumpulkan data resmi.
- Akuisisi dan preservasi, yaitu mengidentifikasi, memperoleh, mengumpulkan, membawa, menyimpan, dan menjaga data terkait insiden.
- Analisis, yaitu menganalisis data yang diperoleh untuk mengidentifikasi sumber kejahatan dan menemukan orang yang bertanggung jawab atas kejahatan tersebut.
- Presentasi, yaitu mendokumentasikan dan menyajikan hasil analisis yang telah dilakukan.
- Pascaproses, yaitu mengembalikan bukti kepada pemilik sebenarnya (jika diperlukan) dan membuat ulasan mengenai proses investigasi yang telah dilakukan sebagai bahan pembelajaran untuk proses investigasi yang akan datang.



Gambar II-2 Model Umum Investigasi Forensik Komputer [6]

Tahapan dalam model ini tidak harus dilakukan secara berurutan. Penyidik dapat kembali ke tahap yang telah dilakukan sebelumnya. Karena tempat kejadian perkara, alat investigasi, alat kejahatan, dan tingkat kemahiran penyidik yang mungkin saja berubah/bertambah, penyidik dapat kembali ke tahap sebelumnya untuk memperbaiki kekurangan dan memperoleh hal/informasi baru [6].

2.3 Metodologi Investigasi Bertahap untuk Menelusuri Penggunaan Komputer

Metodologi investigasi bertahap untuk menelusuri penggunaan komputer, atau dalam bahasa Inggris disebut sebagai *Phased Investigation Methodology (PIM) for tracing computer usage*, berfokus pada pemilihan target investigasi dan menelusuri penggunaan sistem target. Dengan membagi investigasi forensik menjadi beberapa langkah dan menerapkannya secara bertahap, memungkinkan PIM untuk memberi reaksi yang cepat terhadap kasus [4].

2.3.1 Data Target Investigasi

Meskipun *image* forensik telah diperoleh, tetapi jika *image* tersebut belum diinvestigasi dengan teliti maka jawaban dari pertanyaan: data apa yang terdapat dalam komputer tersangka, data telah digunakan untuk apa, dan data mana yang berhubungan dengan kasus belum dapat diketahui. Oleh karena itu, penyidik dapat dengan cepat bereaksi terhadap kasus dengan memperoleh data-data yang hanya memungkinkan penyidik memahami riwayat penggunaan komputer tersangka dari sistem target.

PIM berfokus untuk menelusuri riwayat penggunaan komputer. Sebelum membahas model proses forensik tersebut secara rinci, terlebih dahulu akan dijelaskan mengenai data-data yang tergolong penting yang diperlukan dalam menelusuri riwayat penggunaan komputer. Data-data penting tersebut digolongkan ke dalam lima kategori, yaitu: metadata sistem berkas, berkas *prefetch*, *registry*, berkas peramban web dan berkas dokumen spesifik. Deskripsi dari tiap jenis data target dapat dilihat pada Tabel II-1 [4].

Tabel II-1 Daftar jenis data target [4]

Jenis data	Deskripsi
Metadata sistem berkas	Semua daftar berkas dan folder
Prefetch	Jumlah penggunaan aplikasi dan waktu terakhir aplikasi berjalan
Registry	Daftar dari perintah yang dieksekusi, kata kunci pencarian, folder yang terakhir diakses, berkas yang baru dieksekusi, penggunaan aplikasi terkini
Berkas peramban web	URL yang dikunjungi beserta waktunya, berkas yang diunduh, kata kunci pencarian
Berkas dokumen spesifik	Berkas yang dienkripsi, nama berkas, dan berkas dengan ekstensi yang telah dimodifikasi

a. **Metadata Sistem Berkas**

Metadata sistem berkas mengandung informasi dari seluruh berkas dan direktori yang terdapat pada *hard disk* [7]. Pada sistem berkas NTFS, metadata terdapat pada berkas $MFT. Informasi yang terdapat dalam metadata antara lain: nama berkas dan direktori, ekstensi berkas, waktu pembuatan berkas, waktu modifikasi berkas, waktu berkas diakses, ukuran berkas, lokasi berkas, dan lain-lain. Pada sebagian besar kasus, metadata sistem berkas berukuran sangat kecil sehingga waktu yang diperlukan untuk memperoleh metadata sangat singkat.

Karena nama, jenis, dan waktu dari berkas yang disimpan pada sistem target dapat didapatkan dengan memperoleh dan menganalisis informasi pada metadata, hal ini membuat metadata dapat digunakan secara efektif dalam memilih sistem target dengan melakukan pencarian berkas atau kata kunci. Cara ini lebih efisien dibanding dengan menelusuri seluruh *disk image*.

b. ***Prefetch***

Berkas *prefetch* adalah berkas *cache* yang digunakan untuk mempersingkat waktu *running* suatu aplikasi [8]. Proses tertentu dari suatu aplikasi menggunakan berkas *prefetch* untuk membuka berkas data yang diperlukan pada memori sebelum

peluncuran aplikasi sehingga kecepatan running pun meningkat. Informasi yang dapat dibaca dari berkas prefetch antara lain: nama berkas, jumlah program yang berjalan, waktu running terakhir, daftar berkas referensi yang dibutuhkan untuk meluncurkan program, dan lain-lain. Informasi ini memberitahu program apa saja yang dijalankan tersangka baru-baru ini dan program apa yang sering ia jalankan [4].

c. ***Registry***

Registry merupakan basis data hierarkis pusat yang digunakan sistem operasi Windows untuk menyimpan informasi yang diperlukan untuk mengkonfigurasi sistem dengan pengguna tunggal atau banyak, aplikasi serta perangkat keras. *Registry* penting dalam dunia forensik karena mempunyai informasi paling banyak mengenai penggunaan komputer dan konfigurasinya. Untuk mempermudah investigasi penelusuran dan tujuan dari penggunaan sistem, informasi dikategorikan berdasarkan perintah yang telah dieksekusi, kata kunci pencarian, folder yang terakhir kali diakses, log aplikasi, dan lain-lain. Tabel II-2 menunjukkan jenis dan deskirpsi informasi yang didapat dari *registry*.

Tabel II-2 Informasi yang diekstrak dari *registry* [9]

Jenis informasi	Deskripsi
Perintah yang telah dieksekusi	Perintah yang dieksekusi dengan "Start + Run"
Kata kunci pencarian	Kata kunci yang digunakan pada pencarian Windows
Folder yang terakhir kali diakses	Folder terakhir yang diakses oleh tiap aplikasi dan waktu yang sesuai
Berkas yang dieksekusi baru-baru ini	Berkas dan folder yang dieksekusi baru-baru ini
Log aplikasi	Waktu terakhir eksekusi aplikasi dan jumlah running

Perintah yang telah dieksekusi merupakan daftar perintah yang digunakan dengan menekan "Start + Run(R)" pada Windows. Kata kunci pencarian menunjukkan daftar kata kunci yang digunakan pada fitur pencarian Windows. Folder yang terakhir kali diakses mengandung berkas yang diakses dengan "Open" dari tiap aplikasi. Berkas yang dieksekusi baru-baru ini menunjukkan berkas dan folder apa saja yang telah

dibuka pengguna baru-baru ini. Log aplikasi memberikan *running path*, waktu eksekusi terakhir, dan jumlah *running* suatu aplikasi [9].

d. **Riwayat Internet**

Peramban web merekam sebagian besar riwayat penggunaan internet dalam berkas log peramban web. Berkas log dari Internet Explorer adalah berkas index.dat, berkas log Firefox2 adalah history.dat, berkas log Firefox3 adalah places.sqlite, sedangkan berkas log Google Chrome terdapat pada basis data sqlite bernama "History". Peramban web tersebut memberikan informasi mengenai alamat situs yang dikunjungi beserta waktu kunjungannya. Informasi kata kunci dapat diekstrak dari URL. Dengan mengekstrak daftar pencarian, riwayat penggunaan web dapat membantu menelusuri riwayat penggunaan komputer [4].

e. **Berkas Dokumen Spesifik**

Dokumen spesifik di sini mengacu pada berkas-berkas dengan nama berkas/ ekstensinya telah dimodifikasi. Tersangka mungkin saja telah mengenkripsi berkas tersebut atau memodifikasi nama berkas/ekstensi untuk menutupi kejahatannya. Jika berkas-berkas dienkripsi, berkas-berkas yang nama berkas/ekstensinya telah dimodifikasi dapat ditemukan dalam sistem komputer tersangka. Berkas-berkas ini dapat menjadi bukti yang sangat penting [4].

Enkripsi berkas dapat dilakukan dengan menggunakan NTFS-EFS (NTFS-*Encrypting File System*), fitur enkripsi dari suatu aplikasi, dan algoritma enkripsi. EFS merupakan fitur Windows yang digunakan untuk menyimpan seluruh informasi pada *hard disk* dalam format terenkripsi. Jika mengenkripsi berkas dengan NTFS_EFS, berkas tersebut akan mempunyai atribut $LOGGED_UTILITY_STREAM di dalam $MFT, yang dapat diperiksa untuk melihat apakah berkas terenkripsi [8]. Selama proses enkripsi, EFS membuat berkas *temporary* bernama "EFS0.TMP" yang kemudian dihapus saat proses enkripsi selesai. Oleh karena itu, jika berkas "EFS0.TMP" dapat

dipulihkan, maka isi berkas yang terenkripsi dapat dilihat tanpa didekripsi terlebih dahulu.

Jika berkas dienkripsi dengan menggunakan suatu aplikasi, sebagian besar berkas mempunyai suatu *flag* yang dapat memberitahu apakah berkas terenkripsi. *Flag* ini dapat digunakan untuk mengekstrak berkas-berkas yang terenkripsi. Jika berkas dienkripsi dengan algoritma enkripsi, uji frekueni dapat digunakan untuk mendeteksi enkripsi [10].

Nama berkas/ekstensi dapat diasumsikan dimodifikasi jika waktu pembuatan, waktu modifikasi terakhir, waktu akses terakhir, waktu modifikasi entri dari atribut $FILE_NAME dalam $MFT berbeda. Khusus modifikasi ekstensi dapat dideteksi dengan membandingkan *signature* dari format berkas umum dan kode heksadesimal aktual [8].

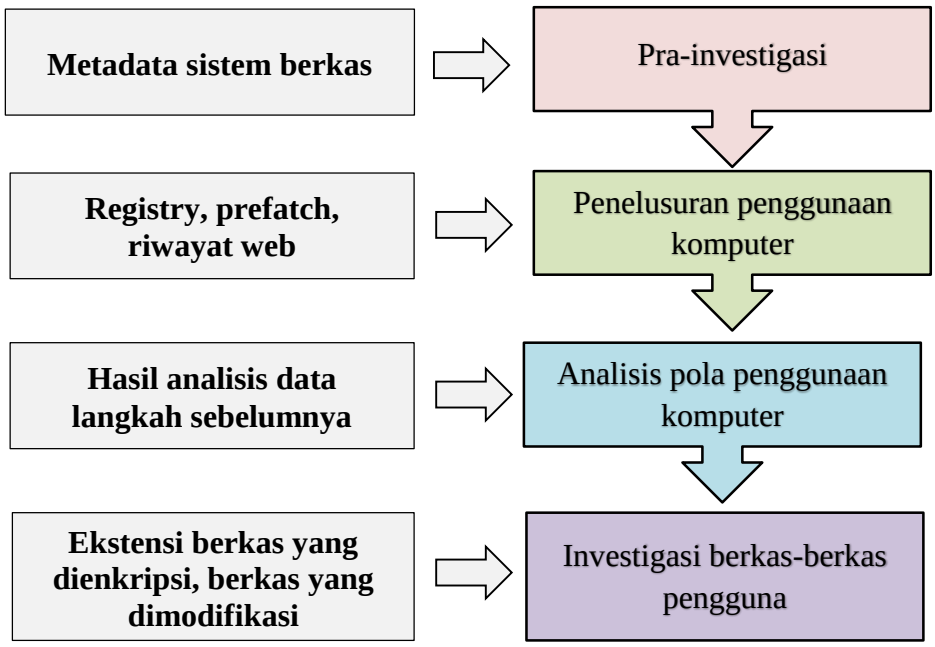
2.3.2 Tahapan dalam Metodologi Investigasi Bertahap

PIM dibagi menjadi empat langkah, yaitu pemilihan target dari sistem dan pra-investigasi, menelusuri penggunaan komputer terkini, analisis pola penggunaan komputer dan investigasi konten-konten berkas pengguna. Analisis data dilakukan hanya pada data-data yang diperlukan dalam setiap langkah. Prosedur keseluruhan dari PIM dapat dilihat pada Gambar II-3 [4].

Pada langkah pertama, metadata sistem berkas diperoleh dan dianalisis untuk menilai apakah sistem perlu diinvestigasi. Selain itu, metadata dianalisis supaya dapat ditentukan mana yang menjadi sistem target. Dalam kata lain, kata kunci yang berkaitan dengan kasus dapat digunakan untuk menginvestigasi daftar berkas dan menilai hubungan-hubungannya [4].

Pada langkah kedua, informasi *task* terkini dari *registry*, berkas *cache* aplikasi, berkas peramban web diinvestigasi untuk menentukan apakah tersangka melakukan *task* yang berkaitan dengan kasus atau untuk menentukan apakah komputer digunakan dalam kasus. Walaupun sistem target telah dipilih pada langkah pertama, namun sistem tersebut dapat temasuk bukan target jika tidak ada *task* terkini [4].

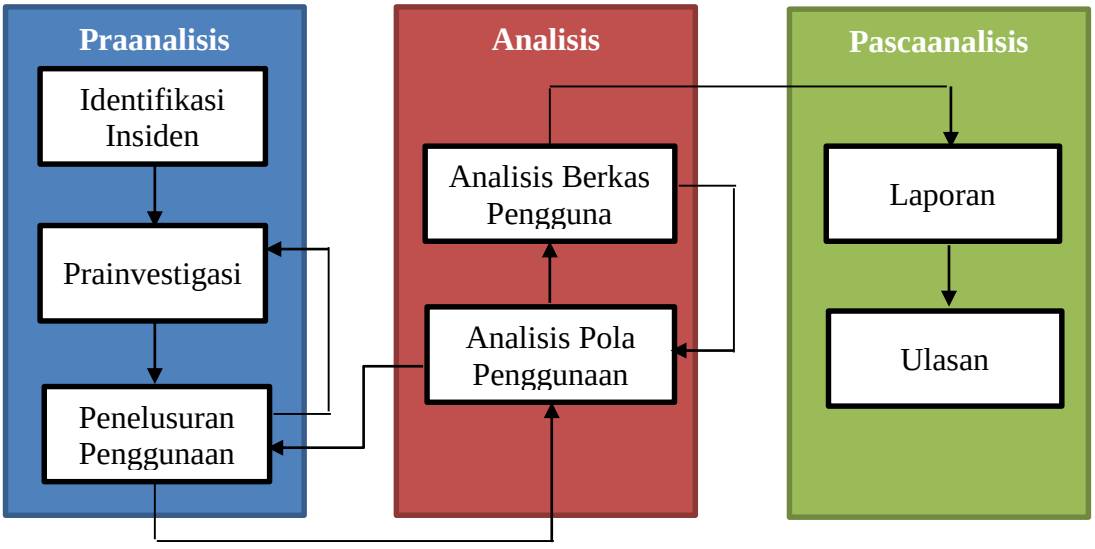
Pada langkah ketiga, statistik dari koneksi internet, penggunaan berkas dan aplikasi digunakan untuk menganalisis pola penggunaan komputer dan menginvestigasi informasi *task* per jam dan per hari. Pada langkah keempat, berkas yang sesungguhnya diperoleh berdasarkan hasil analisis informasi sebelumnya untuk menginvestigasi konten-kontennya dan untuk mendapatkan berkas yang dapat dijadikan sebagai bukti. Secara singkat, PIM memungkinkan untuk melakukan pemilihan sistem target investigasi dengan cepat serta melakukan penelusuran yang efektif akan penggunaan komputer [4].



Gambar II-3 Bagan keseluruhan langkah PIM [4]

BAB III PEMBAHASAN

Model proses forensik yang diajukan dalam makalah ini diambil dari model proses umum respon insiden dan forensik komputer, model umum investigasi forensik komputer (GCFIM), dan metodologi investigasi bertahap untuk menelusuri penggunaan komputer (PIM). Model proses ini memberikan model investigasi baru dalam memilih sistem target dan menganalisis bukti-bukti yang relevan saja. Model proses ini terdiri atas tiga tahapan utama yaitu tahap praanalisis, tahap analisis, dan tahap pascaanalisis. Ketiga tahapan ini ditunjukkan pada Gambar III-1.



Gambar III-1 Model Proses Forensik yang Diajukan

3.1 Tahap Praanalisis

Tahap pertama dari model proses forensik yang diusulkan adalah tahap praanalisis. Tahap ini terdiri atas tiga langkah, yaitu identifikasi insiden, prainvestigasi, dan penelusuran penggunaan.

3.1.1 Identifikasi Insiden

Langkah pertama pada tahap praanalisis adalah mengidentifikasi insiden/kasus. Kepala penyidik harus memilih jenis kasus tertentu dan mengenali kemungkinan-kemungkinan pasti dari tempat kejadian perkara (TKP). Kepala penyidik memastikan waktu insiden terjadi, lokasi kasus, sistem apa yang harus diinvestigasi berdasarkan jenis kasus. Dengan begitu, tahap identifikasi kasus ini membantu dalam memahami karakteristik kasus, termasuk untuk kasus dengan jumlah sistem yang sangat banyak. Tahap ini dapat memberikan cara yang efektif dalam menanggapi suatu insiden/kasus dengan mempersingkat waktu keseluruhan investigasi.

3.1.2 Prainvestigasi

Pada langkah ini, *live data* dan metadata sistem berkas diperoleh dan dianalisis. *Live data* terdapat di dalam *random access memory* (RAM), bukan di dalam *hard disk* sistem. Untuk mengumpulkan informasi *live data*, sistem target tentunya masih aktif. *Live data* memberikan informasi penting dari sistem target seperti "Snap shot" pada waktu respon insiden awal. Dengan adanya informasi penggunaan sistem dalam *live data*, informasi mengenai sistem dasar seperti nama komputer, pengguna yang baru *log-on*, waktu *booting* dan *uptime* pun dapat diidentifikasi. Dengan menggunakan informasi tesebut, tahap perencanaan Informasi tersebut dapat membantu untuk merespon insiden secara efektif.

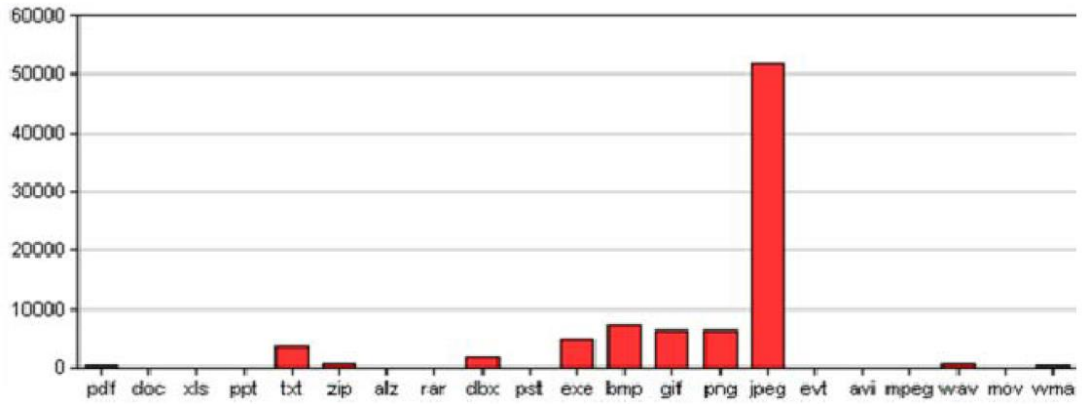
Seperti yang sudah disebutkan pada Subbab 2.3.1, metadata berisi nama, atribut, dan lokasi dari semua berkas yang disimpan di dalam sistem berkas *hard disk*. Penyidik dapat menggunakan beberapa informasi dari metadata untuk melakukan analisis forensik. Seluruh daftar berkas dapat dibaca dari metadata. Dari nama berkas dan ekstensi, penyidik dapat menginvestigasi keberadaan berkas-berkas yang berhubungan dengan kasus melalui pencarian atau *filtering* kata kunci.

Sebagai contoh, dalam kasus pornografi anak, yang menjadi data relevan adalah berkas gambar dan video. Dengan begitu, kepala penyidik menyusun rencana untuk

mencari berkas gambar dan video menggunakan metadata sistem berkas. Penyidik dapat mencari ekstensi dari jenis berkas tersebut atau kata kunci yang relevan untuk menemukan berkas-berkas tersebut. Dengan menggunakan metadata sistem berkas, investigasi dengan teknik ini tentu lebih cepat daripada investigasi keseluruhan *disk image*.

Selain itu, statistik dari informasi ekstensi dan waktu berkas dapat memberikan petunjuk untuk mengetahui tujuan utama penggunaan komputer [4]. Jika ekstensi seperti .xls dan .doc paling menonjol, dapat diasumsikan bahwa komputer tersebut biasa digunakan untuk *word processing*. Berkas *temporary* dari peramban web dan berkas bawaan yang terpasang pada sistem harus dikeluarkan dari statistik karena berkas-berkas tersebut berisi banyak berkas gambar, berkas HTML dan berkas *executable* yang dapat membuat statistic menjadi kurang akurat.

Gambar III-2 menunjukkan contoh statistik dari informasi ekstensi berkas yang terdapat dalam metadata sistem berkas tersangka. Dari gambar tersebut dapat diketahui bahwa dalam komputer tersangka terdapat banyak berkas JPEG. Setelah melakukan pencarian ekstensi pada metadata, banyak ditemukan berkas-berkas yang dicurigai sebagai berkas dengan konten dewasa. Dengan begitu, tujuan utama penggunaan komputer tersangka pun dapat diketahui.



Gambar III-2 Contoh grafik statistik dari ekstensi berkas [4]

3.1.3 Penelusuran Penggunaan Komputer

Data target yang diperoleh pada tahap ini adalah *registry*, *prefetch* dan aktivitas internet seperti berkas riwayat web, penggunaan *messenger*, dan arsip surel. Semua data tersebut dianalisis untuk menentukan apakah tersangka melakukan *task* yang berkaitan dengan kasus atau untuk menentukan apakah komputer digunakan dalam kasus.

Registry dapat memberikan informasi seperti perintah-perintah yang telah dieksekusi, kata kunci pencarian, folder yang terakhir diakses, berkas yang terakhir dieksekusi, log aplikasi, dan lain-lain. Penyidik dapat melakukan analisis *registry* untuk mengekstrak berkas dan data yang berkaitan. Sebagai contoh, jika tersangka sering menggunakan program MS Office, penyidik dapat mengekstrak berkas dengan nama program, ekstensi yang dibuat program, berkas yang dibuat, modifikasi dan akses pada eksekusi terakhir program MS Office, dan hal lainnya dari daftar berkas yang dibuat dari hasil analisis metadata sistem berkas.

Berkas *prefetch* dapat digunakan untuk menentukan aplikasi mana yang sering digunakan akhir-akhir ini. Daftar berkas yang diakses tersebut dapat digunakan untuk melihat apakah *task* yang berkaitan dengan kasus baru dilakukan akhir-akhir ini. Jika berkas yang baru diakses tersebut tidak ditemukan dalam sistem berkas, dapat diasumsikan bahwa tersangka telah menghapusnya untuk menghilangkan bukti [4].

Berkas peramban web merupakan alat bantu yang ampuh untuk menelusuri penggunaan internet tersangka. Informasi waktu dapat menunjukkan alamat-alamat URL dan waktu kunjungan situs yang dilakukan tersangka. Analisis URL memungkinkan untuk melacak berkas unduhan, lokasi sumber unduhan, dan hasil-hasil pencarian. Berkas *temporary*-nya bahkan dapat menunjukkan isi dari surel.

3.2 Tahap Analisis

Setelah semua langkah pada tahap praanalisis selesai dilakukan, tahap selanjutnya tahap analisis. Pada tahap ini dilakukan dua macam analisis, yaitu analisis pola penggunaan komputer dan analisis berkas pengguna.

3.2.1 Analisis Pola Penggunaan Komputer

Langkah pertama pada tahap analisis adalah menganalisis pola penggunaan komputer. Dari hasil analisis data yang telah dilakukan pada tahap praanalisis, penyidik dapat menganalisis pola penggunaan komputer tersangka. Analisis pola penggunaan komputer dapat memberikan petunjuk tentang kapan tersangka sering menggunakan komputer dan jenis berkas atau aplikasi apa saja yang digunakan. *MAC time* pada metadata sistem berkas dapat digunakan untuk melihat kapan tersangka membuat, memodifikasi, mengakses berkas [4].

Log penggunaan berkas dan aplikasi dapat digunakan untuk menelusuri kapan berkas dan aplikasi tersebut digunakan. Secara khusus, *MAC time* dapat digunakan untuk memperkirakan pola penggunaan aplikasi. Berkas peramban web dapat digunakan untuk menginvestigasi kapan tersangka mengakses suatu situs web. Hal ini didukung dengan pemeriksaan tambahan pencarian kata kunci pada *webmail* untuk mengetahui kepentingan utama tersangka [4].

3.2.2 Analisis Berkas Pengguna

Pada tahap ini, berkas-berkas dan data yang relevan diambil. Selain itu, berkas-berkas bukti diinvestigasi berdasarkan hasil analisis data dan pemahaman kasus secara keseluruhan. Berkas-berkas yang diambil adalah berkas yang didapat dari metadata sistem berkas pada langkah prainvestigasi. Berkas-berkas ini dianalisis untuk memutuskan apakah tersangka benar melakukan kejahatan [4].

Pada tahap ini secara khusus lebih berfokus pada investigasi mengenai apakah tersangka menghapus, mengenkripsi, atau memodifikasi nama/ekstensi berkas untuk

merusak bukti. Jika tersangka menyadari akan adanya investigasi, kemungkinan ia akan mencoba cara-cara tersebut. Karena upaya merusak bukti mungkin saja dari hasil persekongkolan, analisis yang lebih rinci menjadi penting [4].

3.3 Tahap Pascaanalisis

Tahap terakhir dari model proses yang diajukan adalah tahap pascaanalisis. Tahap ini terdiri atas dua langkah, yaitu pembuatan laporan dan pembuatan ulasan. Laporan tersebut berisi rincian insiden dan dokumentasi dari semua langkah yang dilakukan pada tahap praanalisis dan tahap analisis. Ulasan mengenai proses investigasi yang telah dilakukan dibuat sebagai bahan pembelajaran dan perbaikan untuk proses investigasi yang akan datang.

BAB IV KESIMPULAN

Dalam makalah ini, diajukan suatu model proses forensik yang bertujuan untuk memilih dan menginvestigasi sistem secara selektif. Model proses ini memungkinkan untuk mengatasi keterbatasan model proses forensik konvensional yang memforensik seluruh data dalam *hard disk* di mana waktu yang diperlukan ntuk memperoleh seluruh *image* dari *hard disk* tersebut sangat lama. Oleh karena itu, diusulkan suatu model proses forensik baru untuk menelusuri penggunaan komputer.

Model proses forensik ini terdiri atas tiga tahap, yaitu tahap praanalisis, tahap analisis, dan tahap pascaanalisis, di mana setiap tahap terdiri atas beberapa langkah. Data target yang dikumpulkan pada model proses forensik ini adalah *live data*, metadata sistem berkas, berkas *registry*, berkas *prefetch*, berkas riwayat web, dan berkas dokumen spesifik. Kemudian data target tersebut dianalisis secara bertahap. Model proses forensik ini sangat berguna dalam menelusuri penggunaan sistem oleh tersangka dan mengambil berkas-berkas dan data yang berhubungan dengan kasus.

Jika terlalu banyak sistem yang harus diinvestigasi, sebagian sistem dapat dikeluarkan dari target atau dapat juga diberi prioritas di atas *task* lainnya supaya investigasi dapat dilakukan dengan cepat dan efektif.

DAFTAR PUSTAKA

[1] K. Lim, S. Lee, J. Park, and S. Lee "XFRAME:XML-based Framework for Efficient Acquiring Digital Evidence on Windows Live System", proceedings of *4th Annual IFIP WG11.9 International Conference on Digital Forensics*, Kyoto, Japan, 2008.

[2] J. Riley, D. Dampier and R. Vaughn, "Time Analysis of Hard Drive Imaging Tools", *Advances in Digital Forensics IV Springer*, pp. 335-344, 2008.

[3] G. Palmer, " A Road Map for Digital Forensic Research. Technical Report DTR-T0010-01", Report from *The First Digital Forensic Research Workshop*, November 2001.

[4] S. Lee, J. Bang, K. Lim, J. Kim, and S. Lee, "A Stepwise Forensic Methodology for Tracing Computer Usage", *The Fifth International Joint Conference on INC, IMS and IDC*, 2009.

[5] F. C. Freiling and B. Schwittay, "A Common Process Model for Incident Response and Computer Forensics", *3rd International Conference on IT –Incident Management & IT-Forensics*, Stuttgart, Germany, 2007.

[6] Y. Yusoff, R. Ismail, and Z. Hassan, "Common Phases of Computer Forensics Investigation Models", *International Journal of Computer Science & Information Technology (IJCSIT)*, Volume 3, No.3, June 2011.

[7] B. Carrier, "File System Forensic Analysis", Addison-Wesly, pp.186-198, 2005

[8] H. Carvey, "Windows Forensic Analysis", *Syngress*, pp. 226-229, 2007

[9] Microsoft Corporation "Windows Registry, Information for Advanced User", [Online]. Available: http://support.microsoft.com/kb/256986, 2008

[10] B. Park and S. Lee, "Determinant Whether the Data Fragment in Unallocated Space is Compress or Not Decompressing of Compressed Data Fragement", *Journal of The Korea Institute of Information Security & Cryptology*, Volume 18, Issue 4, pp. 175-186, August 2008.