p-ISSN : 2301-8364, e-ISSN : 2685-6131, dapat diakses melalui https://ejournal.unsrat.ac.id/index.php/informatika

Computer Forensics and Cyber Crime Handling

Yuri V. Akay
Teknik Elektro Universitas Sam Ratulangi Manado, Jl. Kampus Bahu-Unsrat Manado, 95115,Indonesia
yuriakay@unsrat.ac.id
Diterima: 14 November 2020 direvisi : 28 November 2020; disetujui : 10 Desember 2020

Abstract - Computer forensics is the science of identifying, extracting, analyzing and presenting digital evidence that has been stored in digital devices. For computer crimes in Indonesia, computer forensics is usually carried out regardless of what is inside the computer. In fact, there is more evidence if the computer forensics is identified. There are two methods commonly used for computer forensics, namely search and seizure and discovery information. This method is also developed with evidence management, including the change of custody and rules of evidence. Emphasis on the methods used and what needs, will be discussed on evidence management. Results and conclusions Search and seizures are the most widely used methods, while information retrieval is to complement the evidence data.

Key words - computer forensics; crm; cyber crime; search and seizure

***Abstrak* — Komputer forensik adalah ilmu mengidentifikasi, ekstraksi, menganalisis dan menyajikan bukti digital yang telah disimpan dalam perangkat digital. Untuk kejahatan komputer di Indonesia, forensik di bidang komputer biasanya dilakukan tanpa melihat apa isi di dalam komputer. Justru lebih banyak bukti jika forensik di dalam komputer itu diindentifikasi. Metode yang umum digunakan untuk forensik pada komputer ada dua, yaitu *search* and seizure dan pencarian informasi (*discovery information*). Metode ini juga dikembangkan dengan manajemen bukti, antara lain the *change of custody* dan *rules of evidence*. Penelitian ini memberikan penekanan pada metode yang digunakan serta apa saja yang perlu dilakukan. Hasil dan kesimpulan *Search dan seizure* merupakan metode yang paling banyak digunakan, sedangkan pencarian informasi sebagai pelengkap data bukti tersebut.**

***Kata kunci* — computer forensic; crm; *cyber crime*; *search* and seizure;**

I. PENDAHULUAN

Munculnya teknologi baru telah meningkatkan jumlah pelaku yang memanfaatkan sumber daya ini untuk menggunakannya secara ilegal untuk keuntungan mereka sendiri [1]. Perkembangan kejahatan pun semakin luas dan beragam. Mulai dari internet *abuse*, *hacking*, *cracking*, *carding*, dan sebagainya. Mulai dari coba-coba sampai dengan ketagihan/*addicted*, kejahatan di internet menjadi momok bagi pengguna internet itu sendiri. Jika pada awalnya hanya coba-coba, kemudian berkembang menjadi kebiasaan dan meningkat sebagai kebutuhan/ketagihan. Teknologi informasi saat ini telah menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia sekaligus menjadi sarana efektif untuk tindak kejahatan. Salah satu bentuk kejahatan yang sangat meresahkan dan mendapat perhatian berbagai kalangan, karena perkembangannya yang pesat dan dampak negatifnya yang luas dan berbahaya adalah masalah *cyber crime*. Pertumbuhan luas *cyber crime* telah mempengaruhi negara – negara dari seluruh dunia. Insiden *cyber crime* telah menyebabkan kerugian yang luas terhadap perekonomian suatu negara [2]. Pada tahun 2008 *Cyber crime* menyebabkan kondisi ekonomi seluruh dunia melemah [3]. Perkembangan kejahatan pun semakin luas dan beragam. Mulai dari internet *abuse*, *hacking*, *cracking*, *carding*, dan sebagainya. Mulai dari coba-coba sampai dengan ketagihan/addicted. *Cyber crime* memanfaatkan beberapa sistem komunikasi publik dan swasta, dari komunikasi satelit ke jaringan sensor nirkabel, jaringan selular, dan internet [4]

kejahatan internet (*cybercrime*) leluasa melawan hukum. KUHP yang notabene warisan Belanda jelas belum menyentuh secara utuh kejahatan di dunia maya ini. Pasal-pasal yang digunakan cenderung tidak membuat jera pelaku kejahatan ini. Pihak berwajib juga masih menunggu hukum cyber yang menurut beberapa pakar hukum merupakan hukum yang tidak begitu mengikat.

Segala bentuk kejahatan baik di dunia nyata maupun di dunia maya, sering meninggalkan jejak yang tersembunyi ataupun terlihat. Jejak tersebut yang kemudian dapat meningkat statusnya menjadi bukti, menjadi salah satu perangkat/entitas hukum penting.

A. Tinjauan Pustaka

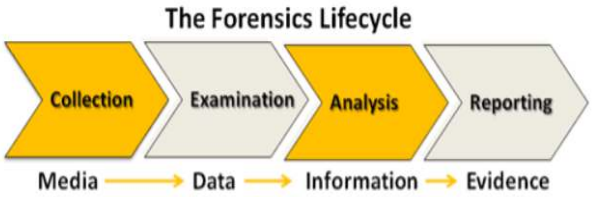
1) Pengertian

Terminologi forensik komputer sendiri adalah suatu proses mengidentifikasi, memelihara, menganalisa, dan mempergunakan bukti digital menurut hukum yang berlaku [5]. Forensik komputer yang kemudian meluas menjadi forensik teknologi informasi masih jarang digunakan oleh pihak berwajib, terutama pihak berwajib di Indonesia.

2) Bukti Digital (Digital Evidence)

Bukti digital adalah informasi dan data dari suatu penyelidikan yang disimpan, diterima, atau dikirimkan oleh perangkat elektronik [6]. Bukti digital ini bisa berupa bukti yang riil maupun abstrak (perlu diolah terlebih dahulu sebelum menjadi bukti yang riil). Beberapa contoh bukti digital antara lain :

E-mail, alamat *e-mail*, *Wordprocessor/spreadsheet files*, *Source code* dari perangkat lunak, Files berbentuk image (*.jpeg*, *.tif*, dan sebagainya), *Web browser bookmarks*, *cookies*, Kalender, *to-do list*



Gambar 1. Tahapan Forensik Komputer

3) Tahapan Dalam Melakukan Forensik Komputer

Gambar 1 merupakan tahapan-tahapan forensin komputer yang dijelaskan sebagaimana berikut ini.

a) Pengumpulan Data (Collection)

Pengumpulan data adalah langkah pertama dalam melakukan proses forensik untuk mengidentifikasi sumber-sumber yang dianggap potensial untuk dijadikan bukti, dan menjelaskan langkah-langkah yang dibutuhkan dalam mengumpulkan data,

Pengumpulan data dalam hal ini mencakup beberapa aktifitas seperti berikut [7]:

Identifikasi, Penamaan (*Labeling*), Perekaman (*Recording*), Mendapatkan data.

Data yang didapatkan haruslah dapat diandalkan dan relevan terhadap kasus yang sedang ditangani, data menjadi barang yang sangat berharga dan merupakan type data yang gampang rapuh, maka dari itu digunakan serangkaian prosedur dalam melakukan penanganan terhadapnya demi menjaga integritas data, setelah melalui proses identifikasi sumber data, langkah selanjutnya tentu mendapatkan data tersebut, ada tiga langkah yang dapat dilakukan dalam mendapatkan data tersebut yaitu:

Membuat perencanaan untuk mendapatkan data (develop a plan to acquire data), Mendapatkan data (Acquire the data), Analisa Integritas data (Verify the integrity of the data)

b) Pengujian (Examination)

Setelah melalui proses pengummpulan data, langkah selanjutnya yaitu dengan melakukan pengujian mencakup didalamnya menilai dan melakukan ekstraksi kepingan informasi yang relevan dari data-data yang dikumpulkan, tahapan ini melibatkan bypassing atau meminimalisasi fitur-fitur sistem operasi dan sistem aplikasi yang akan mengaburkan data , seperti kompresi, enkripsi dan akses mekanisme kontrol.

Hard drive berisi ribuan bahkan jutaan file, untuk mengidentifikasi data didalamnya akan sangat menyita waktu dan perhatian serta akan sangat melelahkan, filtrasi akan mengeliminir sebagian data yang tidak dibutuhkan, misalnya data log minggu lalu yang terdiri dari jutaan record dan didapati hanya ratusan record saja yang dinilai penting untuk pemeriksaan lebih lanjut. ada banyak peralatan dan teknik yang digunakan untuk melakukan eliminasi terhadap tumpukan data, pencarian data berbasis teks dan berbagai pola tertentu dapat digunakan untuk mengidentifikasi ketepatan suatu data, seperti pencarian terhadap dokumen yang berhubungan dengan seseorang atau pokok permasalahan tertentu, atau mengidentifikasi pada e-mail log entries untuk mendapatkan email/dan alamat email yang dapat mengarahkan kepada pencerahan kasus.

Terdapat banyak tool yang dapat digunakan dalam pengujian ini, misalnya software yang mampu menentukan secara akurat jenis file yang berisi karakteristik tertentu, mungkin dapat berupa file teks, grafik, audio, atau berbagai file kompresi lainnya, pengetahuan menyeluruh akan jenis dan type file dapat dijadikan acuan dalam menyingkirkan file yang dianggap tidak memiliki kelayakan/nilai lebih.

c) Analisa (Analysis)

Setelah melalui tahapan ekstraksi informasi, *Examiner* (team forensik) akan melakukan analisa untuk merumuskan kesimpulan dalam menggambarkan data. Analisa dimaksud adalah mengambil pendekatan metodis dalam menghasilkan kesimpulan yang berkualitas berdasarkan pada ketersediaan data atau bahkan sebaliknya, dengan menyimpulkan bahwa tidak terdapat kesimpulan/hasil yang diperoleh, dan hal tersebut mungkin saja akan terjadi ketika menghadapi situasi real di lapangan.

Tugas *examiner* mencakup kegiatan seperti:

1. Mengidentifikasi user atau orang di luar dari pengguna tetapi yang tidak terlibat secara langsung.
2. Lokasi (melakukan observasi lokasi kejadian)
3. Barang-barang (menentukan barang-barang yang berhubungan dengan kejadian)
4. Kejadian (menelusuri rangkaian kejadian yang terdapat pada TKP)
5. Menentukan atau mempertimbangkan bagaimana komponen-komponen yang terelasi antara satu sama lainnya, sehingga memungkinkan examiner akan mendapatkan kesimpulan.

Misalnya saja, Network Intrusion Detection System (IDS) log, yang mungkin memiliki link ke banyak host, the host audit logs mungkin berisi banyak link dari aktivitas user dengan account pengguna, dan thost IDS log menjadi history dari aktifitas dan aksi yang dilakukan oleh user.

d) Dokumentasi dan Laporan (Reporting)

Reporting adalah tahapan akhir dari proses computer forensic, dalam tahapan ini kita akan merepresentasikan informasi yang merupakan hasik dari proses analisis, banyak factor yang dapat mempengaruhi reporting seperti yang akan dibahas berikut ini :

(1) Alternative Explanations (penjelasan alternatif)

Jika informasi yang mengacu pada suatu kasus dikategorikan tidak lengkap, maka definisi akhir yang diperoleh tidak memadai, dan tidak dapat diandalkan, untuk mengamati kejadian bahkan jika didapati beberapa penjelasan lain yang masuk akal akan suatu kejadian, masing-masing informasi yang diperoleh haruslah dipertimbangkan dan diteruskan dalam proses reporting.

Apa pun yang terjadi, seorang examiner harus tetap menggunakan pendekatan metodikal dalam menentukan untuk menyetujui atau menolak setiap penjelasan perihal duduk perkara yang mungkin untuk diteruskan/diajukan dihadapan pengadilan.

(2) Audience Consideration (pertimbangan audiensi / pengamat)

Menyajikan data/informasi pada audiensi sangatlah penting kasus yang melibatkan perundangan membutuhkan laporan detail/spesifik berkenaan dengan informasi yang dikumpulkan, dan duplikasi setiap fakta (evidentiary data) yang diperoleh. Pertimbangan ini beralasan, misalnya saja

p-ISSN : 2301-8364, e-ISSN : 2685-6131, dapat diakses melalui https://ejournal.unsrat.ac.id/index.php/informatika

administrator sistem ingin melihat lebih jauh network trafik secara detail.

(3) Actionable Information

Proses reporting mencakup pula identifikasi actionable information yang diperoleh dari data-data terdahulu, darinnya kita bias mendapatkann informasi baru.
Misalnya saja, daftar alamat seseorang dapat dikembangkan lebih lanjut yang kemudian akan mengarahkan pada informasi lain terkait dengan kejadian tindak kriminal tersebut.

Keuntungan lain dari actionable information, informasi yang diperoleh akan dapat mungkin dapat digunakan untuk keperluan mendatang, misalnya tujuan pengamanan seperti backdoor yang mungki bias dieksploitasi, maka dibutuhkan penanganan segera. Dalam prosesnya, mungkin didapati mesalah yang harus diperbaiki sesegera mungkin seperti policy shortcomings atau procedural errors formal review dapat membantu dalam mengidentifikasi dan meningkatkan kualitas.

Presentasi Bukti Digital Adalah proses persidangan di mana bukti digital akan diuji otentifikasi dan korelasi dengan kasus yang ada. Presentasi di sini berupa penunjukan bukti digital yang berhubungan dengan kasus yang disidangkan. Karena proses penyidikan sampai dengan proses persidangan memakan waktu yang cukup lama, maka sedapat mungkin bukti digital masih asli dan sama pada saat diidentifikasi oleh investigator untuk pertama kalinya.

4) Manajemen Bukti

Manajemen bukti harus dilakukan secara sistematis, formal, dan terstruktur untuk menjamin keabsahan bukti [8].Adanya dua istilah dalam manajemen (barang) bukti antara lain the chain of custody dan rules of evidence, jelas akan membantu investigator dalam mengungkap suatu kasus.

a) The Chain of Custody

Definisi dari U.S. National of Justice (NIJ) adalah pemeliharaan dengan meminimalisir kerusakan yang diakibatkan karena investigasi. Barang bukti harus benar-benar asli atau jika sudah tersentuh investigator, pesan-pesan yang ditimbulkan dari bukti tersebut tidak hilang. Tujuan dari the chain of custody adalah :
1. Bukti itu benar-benar masih asli/orisinil
2. Pada saat persidangan, bukti masih bisa dikatakan seperti pada saat ditemukan. (biasanya jarak antara penyidikan dan persidangan relatif lama).
Beberapa pertanyaan yang dapat membantu the chain of custody ini adalah :
1. Siapa yang mengumpulkan bukti ?
2. Bagaimana dan di mana ?
3. Siapa yang memiliki bukti tersebut ?
4. Bagaimana penyimpanan dan pemeliharaan selama penyimpanan bukti itu ?
5. Siapa yang mengambil dari penyimpanan dan mengapa ?
Untuk menjaga bukti itu dalam mekanisme the chain of custody ini, dilakukan beberapa cara :
1. Gunakan catatan yang lengkap mengenai keluar-masuk bukti dari penyimpanan
2. Simpan di tempat yang dianggap aman.
3. Akses yang terbatas dalam tempat penyimpanan.
4. Catat siapa saja yang dapat mengakses bukti tersebut.

b) Rules of Evidence

"Peraturan Barang Bukti" atau Rules of Evidence. Arti istilah ini adalah barang bukti harus memiliki hubungan yang relevan dengan kasus yang ada [9]. Dalam rules of evidence, terdapat empat persyaratan yang harus dipenuhi, antara lain :
1. Dapat Diterima (Admissible)
Harus mampu diterima dan digunakan demi hukum, mulai dari kepentingan penyidikan sampai dengan kepentingan pengadilan.
2. Asli (Authentic)
Bukti tersebut harus berhubungan dengan kejadian/kasus yang terjadi dan bukan rekayasa.
3. Lengkap (Complete)
Bukti bisa dikatakan bagus dan lengkap jika di dalamnya terdapat banyak petunjuk yang dapat membantu proses investigasi.
4. Dapat Dipercaya (Believable & Reliable)
Bukti dapat mengatakan hal yang terjadi di belakangnya. Jika bukti tersebut dapat dipercaya, maka proses investigasi akan lebih mudah. Walau relatif, dapat dipercaya ini merupakan suatu keharusan dalam penanganan perkara.

Dari data yang didapat melalui survei oleh FBI dan The Computer Security Institute, pada tahun 1999 mengatakan bahwa 51% responden mengakui bahwa mereka telah menderita kerugian terutama dalam bidang finansial akibat kejahatan komputer. Survei yang sama juga dilakukan pada tahun 2000, terjadi peningkatan menjadi 74% dari responden yang mengatakan bahwa mereka menderita kerugian finansial akibat kejahatan komputer. Pemaparan data di atas memberikan gambaran bahwa terjadi kecenderungan peningkatan kerugian finansial dari pihak pemilik komputer karena kejahatan komputer.

Cyber crime dibagi menjadi dua, yaitu computer fraud dan computer crime. Computer fraud meliputi kejahatan/pelanggaran dari segi sistem organisasi komputer. Sedang computer crime merupakan kegiatan berbahaya di mana menggunakan media komputer dalam melakukan pelanggaran hukum (computer as a tool). Untuk menginvestigasi dan menganalisa kedua kejahatan di atas, maka digunakan forensik dalam teknologi informasi.

II. METODE

Metode yang digunakan dalam menginvestigasi kejahatan dalam teknologi informasi dibagi menjadi dua :
1. *Search* & Seizure
2. Pencarian informasi

1. *Search* and *Seizure*

Investigator harus terjun langsung ke dalam kasus yang dihadapi, dalam hal ini kasus teknologi informasi [10]. Diharapkan investigator mampu mengidentifikasi, menganalisa, dan memproses bukti yang berupa fisik. Investigator juga berwenang untuk melakukan penyitaan terhadap bukti yang dapat membantu proses penyidikan, tentunya di bawah koridor hukum yang berlaku.

2. *Pencarian Informasi*

Beberapa tahapan dalam pencarian informasi khususnya dalam bidang teknologi informasi :

1) Menemukan lokasi tempat kejadian perkara
2) Investigator menggali informasi dari aktivitas yang tercatat dalam log di komputer
3) Penyitaan media penyimpanan data (data storages) yang dianggap dapat membantu proses penyidikan.

Walaupun terlihat sangat mudah, tetapi dalam praktek di lapangan, ketiga tahapan tersebut sangat sulit dilakukan. Investigator yang lebih biasa ditempatkan pada kasus kriminal non-teknis, lebih terkesan terburu-buru mengambil barang bukti dan terkadang barang bukti yang dianggap penting ditinggalkan begitu saja.

Dalam menggali informasi yang berkaitan dengan kasus teknologi informasi, peran investigator dituntut lebih cakap dan teliti dalam menyidik kasus tersebut. Celah yang banyak tersedia di media komputer menjadikan investigator harus mengerti trik-trik kasus teknologi informasi.

Kedua metodologi di atas setidaknya menjadi acuan pihak yang berwenang dalam menyidik kasus kejahatan dalam bidang teknologi informasi.

III. HASIL DAN PEMBAHASAN

A. Prosedur forensik yang umum digunakan

Beberapa literatur menyebutkan bahwa prosedur yang perlu dilakukan oleh investigator dapat dijelaskan sebagai berikut :

1. Membuat copies dari keseluruhan log data, files, dan lain-lain yang dianggap perlu pada suatu media yang terpisah
2. Membuat fingerprint dari data secara matematis (contoh hashing algorithm, MD5)
3. Membuat fingerprint dari copies secara matematis
4. Membuat suatu hashes masterlist
5. Dokumentasi yang baik dari segala sesuatu yang telah dikerjakan

Bukti yang biasanya digunakan dalam forensik komputer adalah berupa :

1. Logs
2. Stand alone system
3. Networked system
4. Harddisk
5. Floppy disk atau media lain yang bersifat removable

Selain itu, perlu dilakukan investigasi lanjutan di mana digunakan dua metodologi yang telah disebut sebelumnya. Dari kedua metode tersebut, metode *search* and seizure lebih banyak digunakan dari pada pencarian informasi. Walaupun di sisi lain, tidak ada salahnya jika metode *search dan seizure* tersebut dilengkapi dengan pencarian informasi yang lebih rinci.

1) Metode Search dan Seizure

Proses *search dan seizure* sendiri dimulai dari perumusan suatu rencana. Cara yang paling sering digunakan adalah membuat software khusus untuk mencari bukti. Selain merupakan cara yang tepat untuk melakukan forensik teknologi informasi, pembuatan software khusus ini juga membuktikan adanya metodologi penelitian yang ilmiah.

Tahapan dalam *search* dan seizure1 ini dapat dijabarkan sebagai berikut :

1. Identifikasi dan penelitian permasalahan Dalam hal ini identifikasi adalah identifikasi permasalahan yang sedang dihadapi, apakah memerlukan respon yang cepat atau tidak. Jika tidak, maka dilanjutkan dalam penelitian permasalahan secara mendalam.
2. Membuat hipotesa Pembuatan hipotesa setelah melalui proses identifikasi dan penelitian permasalahan yang timbul, sehingga data yang didapat selama kedua proses di atas dapat dihasilkan hipotesa.
3. Uji hipotesa secara konsep dan empiris Hipotesa diuji secara konsep dan empiris, apakah hipotesa itu sudah dapat dijadikan kesimpulan atau tidak.
4. Evaluasi hipotesa berdasarkan hasil pengujian dan pengujian ulang jika hipotesa tersebut jauh dari apa yang diharapkan
5. Evaluasi hipotesa terhadap dampak yang lain jika hipotesa tersebut dapat diterima.

Tahapan-tahapan di atas bukan merupakan tahapan yang baku, disesuaikan dengan kondisi di lapangan. Kondisi keadaan yang berubah-ubah memaksa investigator lebih cermat mengamati data sehingga hipotesa yang diambil tidak jauh dari kesimpulan akhir.

Search dan seizure sendiri meliputi pemulihan dan pemrosesan dari bukti komputer secara fisik. Walaupun banyak hal yang positif, metode ini juga memberikan penekanan dan batas-batas untuk investigator agar hipotesa yang dihasilkan sangat akurat. Adapun penekanan dan batas-batas untuk investigator tersebut adalah :

1. Jangan merubah bukti asli
2. Jangan mengeksekusi program pada bukti (komputer) terutama Operating System-nya
3. Tidak mengizinkan tersangka untuk berinteraksi dengan bukti (komputer)
4. Segera mungkin mem-backup bukti yang ada di dalam komputer tersangka. Jika pada saat diidentifikasi komputer masih nyala, jangan dimatikan sampai seluruh data termasuk temporary selesai dianalisa dan disimpan
5. Rekam seluruh aktifitas investigasi
6. Jika perlu, pindahkan bukti ke tempat penyimpanan yang lebih aman.

Penekanan ini sangat berguna dalam pengumpulan, penanganan, dan penyimpana bukti agar dalam jangka waktu yang lama (sejak proses penyidikan sampai proses persidangan) bukti tersebut tidak berubah.

Untuk seizure ini, terdapat guidance dari Manageworx Infosystem Inc sebagai berikut :

1. Perencanaan / Planning
   a. Identifikasi sistem komputer yang dihadapi
   b. Identifikasi komputer tersebut terhubung dengan jaringan atau tidak
   c. Identifikasi kebutuhan lain yang diperlukan oleh sistem administrator untuk menggunakannya
   d. Tunjuk satu orang yang bertanggung jawab terhadap bukti tersebut
   e. Buat dokumentasi apa saja yang akan dan sudah dikerjakan
2. Pemeliharaan, Pengumpulan, dan Dokumentasi
   a. Tunjuk bukti utama
   b. Buat dokumentasi berupa gambar dan video
   c. Berikan catatan pada dokumen gambar dan video tersebut
   d. Beri label pada seluruh bukti
3. Seizing Electronic Evidence

a. Jika memiliki jaringan, ambil bukti tersebut supaya tidak diremote
b. Gunakan disk yang bootable dan cek apakah ada virus
c. Kunci media penyimpanan (harddisk) agar tidak ditulis/dihapus ulang

4. Catat waktu investigasi
5. Membuat gambaran arus bit dari bukti ke dalam media baru
6. Kalkulasi dan catat kriptografi checksum dari media penyimpanan yang asli dan image-nya md5sum menyediakan 32 bit signature yang sensitif terhadap perubahan
7. Tidak mungkin 2 file berbeda membuat hash yang sama

Managework membuat checklist ini selain untuk mempermudah, Manageworx juga sudah memiliki software forensik yang dapat diimplementasikan dalam sistem UNIX atau non-UNIX.

2) Pencarian Informasi

Metode pencarian informasi yang dilakukan oleh investigator merupakan pencarian bukti tambahan dengan mengandalkan saksi baik secara langsung maupun tidak langsung terlibat dengan kasus ini. Pencarian informasi didukung bukti yang sudah ada menjadikan hipotesa yang diambil semakin akurat.

Pada intinya, pencarian ini merupakan bukti tambahan, dengan memperhatikan hal-hal sebagai berikut :

1. Jika melakukan penggalian informasi lebih dalam ke saksi, maka gunakan metode wawancara interaktif, sehingga bukti yang sudah ada dapat di-cross check agar keberadaan bukti tersebut diakui oleh saksi.
2. Jika memungkinkan, rekonstruksi dilakukan dengan/tanpa tersangka sehingga apa yang masih belum jelas dapat tergambar dalam rekonstruksi.

B. Data Recovery

Data recovery merupakan bagian dari analisa forensik di mana hal ini merupakan komponen penting di dalam mengetahui apa yang telah terjadi, rekaman data, korespondensi, dan petunjuk lannya. Banyak orang tidak menggunakan informasi yang berasal dari data recovery karena dianggap tidak murni/asli/orisinil.

Untuk melihat seberapa jauh data sudah dihapus atau belum, perlu memperhatikan segala sesuatu yang ada dalam raw disk. Jika data yang digunakan untuk kejahatan ternyata masih ada, maka cara yang termudah adalah menguji data dengan pemanfaatan tool yang ada pada standar UNIX, seperti strings, grep, text pagers, dan sebagainya. Sayangnya, tools yang ada tidak menunjukkan data tersebut dialokasikan di mana.

Melalui investigasi dari sistem yang dirusak oleh intruder, sistem files UNIX yang modern tidak menyebar contents dari suatu file secara acak dalam disk. Sebagai gantinya, sistem files dapat mencegah fragmentasi file, meskipun setelah digunakan beberapa tahun.

File content dengan sedikit fragmentasi akan lebih mudah untuk proses recover dari pada file content yang menyebar dalam disk (media penyimpanan). Tetapi sistem file yang baik memiliki beberapa keuntungan lain, salah satunya mampu untuk menghapus informasi untuk bertahan lebih lama dari yang diharapkan.

C. Pengelompokan Analisa Media

Pengelompokan ini bertujuan untuk mengetahui aliran dan proses dalam media yang digunakan dalam kejahatan. Dari pengelompokan ini dapat disimpan informasi penting yang didukung oleh sistem yang ada. Pengelompokan dalam bentuk laporan ini diisi dengan keadaan fakta di lapangan.

D. Pembuatan Laporan dalam Analisa Media

Beberapa hal penting yang perlu dimasukkan dalam laporan analisa media adalah sebagai berikut :

1. Tanggal dan waktu terjadinya pelanggaran hukum pada CPU
2. Tanggal dan waktu pada saat investigasi
3. Permasalahan yang signifikan terjadi
4. Masa berlaku analisa laporan
5. Penemuan yang berharga (bukti) Pada laporan akhir, penemuan ini sangat ditekankan sebagai bukti penting sebagai pendukung proses penyidikan.
6. Teknik khusus yang dibutuhkan atau digunakan (contoh : password cracker)
7. Bantuan pihak yang lain (pihak ketiga)

Pada saat penyidikan, pelaporan dalam bentuk worksheet ini dicross check dengan saksi yang ada, baik saksi terlibat langsung maupun tidak langsung.

E. Log Out Evidence – Visual Inspection and Inventory

Tahapan yang dilalui dalam inspeksi komputer secara visual adalah :

1. Log out seluruh komputer untuk dianalisa lebih lanjut
2. Jika ada media penyimpanan lain (CD/disket), diberi label khusus agar bukti tersebut tetap utuh
3. Inspeksi visual dilakukan dengan melakukan physical makeup
4. Buka casing CPU, identifikasi dan analisa sirkuit internal, buat catatan apa saja yang ada di dalam CPU tersebut. Catat juga kartu tambahan (expansion cards) jika ada.
5. Beri rekomendasi apakah CPU tersebut bisa dijadikan sebagai barang bukti fisik atau tidak
6. Catat keseluruhan letak perangkat keras (harddisk, CD ROM, RAM, dan sebagainya)
7. Dokumentasikan dalam bentuk gambar sebelum dan sesudah identifikasi dan analisa

F. Pengumpulan Bukti Akhir

Dari keseluruhan proses investigasi, dibuat dalam worksheet yang digunakan untuk tahapan analisa dan proses lebih lanjut ke tingkat selanjutnya. Dalam proses ini, bukti yang digunakan tidak boleh berubah sejak digunakan sebagai alat bukti pertama kali.

IV. KESIMPULAN DAN SARAN

Metode yang banyak digunakan dalam forensik komputer adalah *search dan seizure* dan pencarian informasi. *Search dan seizure* merupakan metode yang paling banyak digunakan, sedangkan pencarian informasi (information *search*) sebagai pelengkap data bukti tersebut.

Tinjauan dari sisi software maupun hardware dalam forensik ini lebih mencerminkan bahwa kedua komponen komputer itu memang tidak dapat dipisahkan, karena adanya saling ketergantungan satu sama lain. Dalam

menginvestigasi suatu kasus, digunakan tools untuk menganalisa komputer baik secara software maupun hardware.

Forensik komputer adalah bidang baru di Indonesia, di mana keberadaan forensik ini sangat dibutuhkan untuk memecahkan kasus tertentu. Jika lebih dikembangkan, maka forensik akan menjadi cabang keamanan dari komputer/jaringan dan bagian yang tidak terpisahkan dalam Labkrim Mabes Polri.

V.KUTIPAN

[1] M. M. Kamal, I. A. Chowdhury, N. Haque, M. I. Chowdhury, and M. N. Islam, "Nature of *cyber crime* and its impacts on young people: A case from Bangladesh," Asian Soc. Sci., vol. 8, no. 15, pp. 171–183, 2012.

[2] J. Požár, "Modelling of the investigation of *cybercrime*," Sci. Mil., pp. 63–70, 2014.

[3] L. a Ionescu, V. Mirea, and A. Blajan, "Fraud , Corruption and *Cyber Crime* in a Global Digital Network," Econ. Manag. Financ. Mark., vol. 6, no. 2, pp. 373–380, 2011.

[4] G. Loukas, D. Gan, and T. Vuong, "A Review of Cyber Threats and Defence Approaches in Emergency Management," Futur. Internet, vol. 5, pp. 205–236, 2013.

[5] K. K. Sindhu, "Digital Forensics and *Cyber Crime* Datamining," J. Inf. Secur., vol. 03, no. July, pp. 196–201, 2012.

[6] S. Tripathi, "Digital Evidence for Database Tamper Detection," J. Inf. Secur., vol. 03, no. April, pp. 113–121, 2012.

[7] F. Sulianta., "Teknik Forensik: Cara Jitu Mengatasi Problema Komputer," .,

[8] G. Giova, "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems," J. Comput. Sci., vol. 11, no. 1, pp. 1–9, 2011.

[9] and D. J. C. Saltzburg, Stephen A., Michael M. Martin, "Federal rules of evidence manual: a complete guide to the Federal rules of evidence," 1998.

[10] W. R. LaFave, "*Search* and seizure: a treatise on the Fourth Amendment," West Gr. Publ., vol. 4, 2004.

.

Author, Yuri Vanli Akay Bachelor of Education in Network Computer Engineering, Universitas Negeri Manado Indonesia, Master of Engineering in Enterprise Information System Atmajaya University Yogyakarta, Indonesia. Research in last view Years, Metode User Centered Design (UCD) Dalam Perancangan Sistem Informasi Geografis Pemetaan Tindak Kriminalitas (Studi Kasus: Kota Manado), Analisis Sentimen Twitter Pasca Pengumuman Hasil Pilpres 2019 Menggunakan Metode Lexicon Analysis, Web Performance Analytics: WebQEM In Academic Portal.