TEKNIK FORENSIK
UNTUK PEMBUKTIAN HUKUM
KASUS CYBERCRIME (CARDING)

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana
Jurusan Teknik Informatika

DISUSUN OLEH:

Ahmad Fathoni

07 523 142

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA

2012

LEMBAR PENGESAHAN PEMBIMBING

TEKNIK FORENSIK

UNTUK PEMBUKTIAN HUKUM

KASUS CYBERCRIME (CARDING)

TUGAS AKHIR

Oleh :

Nama : Ahmad Fathoni

NIM : 07 523 142

Yogyakarta, Mei 2012

Pembimbing

Yudi Prayudi S.Si., M.Kom.

LEMBAR PENGESAHAN PENGUJI

TEKNIK FORENSIK
UNTUK PEMBUKTIAN HUKUM
KASUS CYBERCRIME (CARDING)

TUGAS AKHIR
Disusun oleh :

Nama : Ahmad Fathoni
NIM : 07 523 142

Telah Dipertahankan di Depan Sidang Penguji Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika
Fakultas Teknologi Indust ri Universitas Islam Indonesia
Yogyakarta, Juni 2012

Tim Penguji,

Yudi Prayudi, S.Si, M.Kom _____
Ketua

Zainudin Zukhri, S.T., MIT _____
Anggota I

Ahmad Munasir Raf'ie Pratama, S.T., MIT _____
Anggota II

Mengetahui,
Ketua Program Studi Teknik Informatika
Universitas Islam Indonesia

Yudi Prayudi, S.Si., M.Kom

PERSEMBAHAN

Alhamdulillahirabbil'alamiin. Rasa puji syukur saya panjatkan kepada Allah SWT atas karunia dan rahmat-Nya saya bisa menyelesaikan tugas akhir ini dengan baik dan semoga akan dapat bermanfaat dikemudian hari
Sholawat dan Salam tak lupa saya panjatkan kepada Nabi Muhammad SAW, karena beliau semoga saya menjadi orang yang selalu benar langkahnya dan diridloi oleh Allah SWT

Buat kedua Orang Tuaku tersyang yang selalu mendukung di setiap hal-hal positif yang aku kerjakan, terima kasih atas bimbingan dan doa nya selama ini.
Kedua saudaraku Mas Wahid dan Rasyid tersayang semoga bisa mendapatkan langkah yang lebih baik dari saudaramu tercinta ini, dan keluarga besar yang selalu membantu mengisi hari yang lebih dari biasanya.

Guru, Pendidik, Pengajar Dosen dan orang – orang yang telah sangat berjasa memeberikan ilmu kepadaku . terimakasih telah mengajarkanku ilmu yang bermanfaat selama ini, semoga tetap ikhlas dan tetap kuat menghadapi kelakuan/sikap anak didik mu yang terkadang aneh.

Untuk teman-teman ngumpul Beben, Umin, M Jet, Ishe, Jeki yang selalu memberikan dukungan serta bantuan moril sehingga tugas akhir ini dapat selesai dibuat.

Untuk sahabat-sahabat kos 37 Yoga, Iwan, Rudi, Ari dan Figar semoga bersabar menghadapi sikap ku yang agak acuh karena skripsi ini, Kelompok Sunyi yang selalu setia menemani hari-hari yang membosankan di depan komputer.

Keluarga besar LPM PROFESI UII yang telah banyak mengahbiskan waktu bersama.
Keluarga besar Include yang tetap rame dan bagi yang belum skripsi jangan malas untuk mengejar kita yang duluan.
Teman-teman Bask keluarga besar KKN Unit 99 angkatan 40.

MOTTO

“Sesungguhnya sesudah kesulitan itu ada kemudahan; Maka apabila kamu telah selesai (dari sesuatu urusan), k*erjakanlah dengan sungguh-sungguh (urusan) yang lain”.*

(Q.S. Alam Nasyrah ayat 6 &7)

“ Semua rahasia akan terungkap suatu saat, ketahuilah rencana-Nya selalu indah”

“Ridho dari orang tua = Ridho ALLAH SWT ”

KATA PENGANTAR

Assalamu'alaikum wr. wb.

Dengan segala hormat, saya panjatkan puji syukur kepada Allah SWT yang senantiasa melimpahkan rahmat dan hidayah-Nya, sehingga saya diberi kesempatan untuk menyelesaikan Tugas Akhir ini, yang diajukan sebagai salah satu syarat untuk meraih gelar sarjana S-1.

Tak lupa, dalam Tugas Akhir ini saya telah dibantu oleh berbagai pihak, baik berupa bimbingan, semangat, maupun kerjasamanya. Oleh karena itu dalam kesempatan ini ijinkanlah saya menyampaikan ucapan terima kasih kepada:

1. Ir. Gumbolo Hadi Susanto, M.Sc., selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.

2. Bapak Yudi Prayudi, S.Si, M.Kom., selaku Ketua Jurusan Teknik Informatika Universitas Islam Indonesia dan selaku Dosen Pembimbing Tugas Akhir.

3. Seluruh staf pengajar Fakultas Teknologi Industri Universitas Islam Indonesia, khususnya dosen-dosen jurusan Teknik Informatika yang telah memberikan bekal ilmu.

4. Orang tua dan keluarga besar saya yang telah memberikan doa, dorongan, fasilitas dan semangat kepada saya.

5. Teman – teman angkatan 2007, khususnya kelas B, teman-teman LPM Profesi serta Bernard, Iwan, Lukman, M. Zulfariansyah, Yoga, Adi dan kawan-kawan atas kebersamaannya

6. Serta semua pihak terkait yang tidak dapat saya sebutkan satu per satu, yang telah membantu dari awal hingga akhir.

Tak ada yang sempurna di dunia ini, oleh karena itu saya menyadari sepenuhnya bahwa masih banyak kekurangan dalam Tugas Akhir ini, sehingga segala kritik dan saran yang membangun akan saya terima dengan rendah hati. Saya sangat berharap semoga Tugas Akhir ini bermanfaat bagi semua pihak.

Yogyakarta, Mei 2012

Hormat Saya

Ahmad Fathoni

SARI

Komputer Forensik adalah penyelidikan dan analisis komputer untuk menentukan potensi bukti legal. Berbeda dari pengertian forensik pada umumnya, komputer forensik dapat diartikan sebagai pengumpulan dan analisis data dari berbagai sumber daya komputer yang mencakup sistem komputer, jaringan komputer, jalur komunikasi, dan berbagai media penyimpanan yang layak untuk diajukan dalam sidang pengadilan.

Komputer Forensik memiliki beberapa tahapan, yaitu : pengumpulan data, pengujian, analisis serta dokumentasi, laporan dan presentasi. Dari tahapan-tahapan tersebut akan diketahui apa, di mana, bagaimana, siapa dan kapan kasus terjadi. Pada tahapan pengumpulan data akan dilakukan suatu proses *image* data, dengan artian mengkloning bukti digital yang telah diperoleh sehingga ketika terjadi suatu kesalahan tidak akan merusak bukti digital atau *barang bukti* yang asli.

Setelah melakukan tahapan imaging, kemudian dilakukan pengecekan atau pengujian terhadap data yang telah di *imaging* menggunakan FTK, untuk mendapat kan data-data yang kemudian dapat dilakukan analisis forensik. Pada tahapan selanjutnya laporan atau dokumentasi. Dari hasil yang telah dianalisis dapat diketahui bahwa FTK dapat menemukan berbagai macam data seperti Log jaringan, *document*, *thumbnail*, email dan lain sebagainya. Pada presentasi, merupakan tahapan akhir dimana dilakukan presentasi temuan yang dilakukan kepada pihak kepolisian dan pengadilan.

Keyword : Komputer Forensik, FTK, Image Data

DAFTAR ISI

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komputer (TIK) telah mengalami kemajuan yang sangat pesat, terutama sekali setelah diketemukannya teknologi yang menghubungkan antar komputer (*networking*) dan Internet. Namun demikian, berbagai kemajuan tersebut ternyata diikuti pula dengan berkembangnya sisi lain dari teknologi yang mengarah pada penggunaan komputer sebagai alat untuk melakukan berbagai modus kejahatan. Istilah ini kemudian dikenal dengan *cybercrim*e.

Permasalahan yang diakibatkan oleh penggunaan komputer untuk kepentingan diatas telah mulai menimbulkan berbagai dampak negatif. Baik secara mikro yang dampaknya hanya pada tingkatan personal/perseorangan, maupun secara makro yang berdampak pada wilayah komunal, publik, serta memiliki efek domino yang luas. Untuk menangani permasalahan ini, maka di beberapa negara telah dibentuk unit khusus kepolisian yang berfungsi sebagai penindak kejahatan yang spesifik terkait dengan permasalahan *cybercrime*.

Komputer forensik merupakan aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti komputer dalam kejahatan komputer. komputer forensik juga merupakan kombinasi ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisis data dari sistem komputer. Dalam suatu kasus hukum merupakan tugas ahli komputer forensik untuk menegakkan hukum dengan mengamankan barang bukti, rekonstruksi kejahatan, dan menjamin jika bukti yang dikumpulkan itu berguna di persidangan.

Di Indonesia kasus-kasus yang dalam penyelesaiannya menggunakan barang bukti digital masih sedikit. Baru satu-dua tahun belakangan ini saja barang bukti digital digunakan, itu pun para ahlinya masih terbatas. Ilmu ini harus benar-benar bisa dipertanggungjawabkan, tidak hanya di laporan saja tapi juga di

pengadilan. Di Indonesia ahlinya masih sangat jarang karena mungkin tidak terlalu banyak pakar teknologi informasi yang ***aware*** di bidang ini. Di Indonesia sendiri mungkin masih banyak pakar teknologi informasi yang takut bila ini dikaitkan dengan hukum. Kasus di Indonesia yang menggunakan barang bukti digital diantaranya adalah kasus pembunuhan Nasrudin (Antasari Azhar), kasus Bank Century, beberapa kasus carding dan penyalahgunaaan ATM (*Skimmer*)

1.2 Rumusan Masalah

Bagaimana menyelesaikan kasus *cybercrime* khususnya *carding* dengan teknik komputer forensik agar nantinya barang bukti dapat diterima sebagai barang bukti yang sah di pengadilan.

1.3 Batasan Masalah

Dalam melaksanakan suatu penelitian diperlukan adanya batasan agar tidak menyimpang dari yang telah direncanakan sehingga tujuan yang sebenarnya dapat tercapai. Batasan masalah dari penelitian ini adalah :

- Menganalisis kasus *cybercrime* dengan studi kasus berupa *carding.*
- Kasus diselesaikan dengan prosedur forensik sampai ke tahapan menjadi barang bukti yang sah.

1.4 Review Penelitian

Tindak kejahatan komputer dan dunia maya yang terjadi saat ini semakin banyak jenisnya. Banyaknya tindak kejahatan dunia maya menyebabkan perlunya peranan seorang ahli dalam menyelesaikan tiap permasalahan yang ada. Dengan demikian topik penelitian ini menjadi sangat penting sebagai upaya untuk memperkenalkan kepada masyarakat ilmiah komputer di Indonesia prosedur-prosedur untuk meyelesaikan tiap kasus kejahatan tersebut. Sejumlah peneliti sudah mengangkat isu-isu tersebut secara umum. (Utdirartatmo, 2001) membahas latar belakang serta metodologi yang digunakan dalam komputer forensik dan cara penggunaan beberapa *tools* komputer forensik terkait kejahatan dunia maya. Sementara (Prayudi & Afrianto, 2007) membahas tentang gambaran singkat

terkait pengertian, metode dan implementasi proses forensik menggunakan sejumlah aplikasi yang tersedia.

Dari sisi keamanan dan pencegahan tindak kejahatan dunia maya, (Dougherty, 2011) Memberikan gambaran bagaimana komputer forensik cocok sebagai elemen strategis dalam keamanan komputer secara keseluruhan organisasi. Sementara (Internet World Into & Life, 2006) Membahas perkembangan identity teft yang merupakan bagian dari cybercrime dan cara memproteksi diri dan mencegah terjadinya tindakan tersebut. Untuk kalangan peneliti yang ada di Indonesia saat ini, isu-isu tentang komputer forensik yang dibahas secara khusus tampaknya belum terlalu banyak disentuh. Untuk itulah maka penelitian ini diajukan untuk mengangkat isu-isu seputar komputer forensik yang penangananya dilakukan secara khusus.

1.5 Tujuan Penelitian

Tujuan Penelitian ini adalah menemukan barang bukti digital yang dapat digunakan sebagai barang bukti yang sah di pengadilan dengan menganalisis kasus *cybercrime* khususnya *carding* sesuai prosedur komputer forensik.

1.6 Manfaat Penelitian

Manfaat Penelitian ini adalah menambah pengetahuan terkait ilmu komputer forensik dan *tools* foresik yang pada nantinya akan bermanfaat untuk bagi orang-orang yang akan menggeluti bidang yang terkait masalah *cybercrime* dan komputer forensik.

1.7 Metodologi Penelitian

Dalam melakuakan penelitian terdapat tahapan-tahapan yang dilakukan agar penelitian tersebut dapat berjalan dengan baik. Dalam penelitian metodologinya berupa :

- Pengumpulan data yang diperlukan menggunakan berbagai macam literatur yang berhubungan dengan *cybercrime* dan komputer forensik. Selain itu juga mencari referensi tambahan di Internet.

- Pembuatan scenario kasus *carding* yang pada nantinya akan dianalisis dengan teknik komputer forensik.
- Melakukan analisis dan identifikasi scenario kasus *carding* yang telah dibuat sesuai tahapan komputer forensik sampai dapat dijadikan barang bukti di pengadilan..

1.8 Sistematika Penulisan

Dalam penyusunan tugas akhir ini, sistematika penulisan dibagi menjadi beberapa bab yaitu sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi pembahasan masalah umum yang meliput latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitan, metodologi penelitian penulisan.

BAB II LANDASAN TEORI

Bagian ini membahas landasan teori yang digunakan dalam penelitian kasus *cybercrime* dengan teknik forensik. Di dalam tugas akhir ini teori-teori yang akan dibahas meliputi hal-hal yang berhubungan dengan *cybercrime* dan komputer forensik.

BAB III METODOLOGI

Bagian ini memuat uraian prosedur dan skenario kasus *carding* dan pembuktiannya.

BAB IV PENGUJIAN DAN PEMBAHASAN

Bab ini membahas tentang analisis penyelesaian kasus *carding* menggunakan teknik komputer forensik yang bertahap sesuai prosedur yang berlaku.

BAB V KESIMPULAN DAN SARAN

Bab ini merupakan rangkuman serta kesimpulan-kesimpulan dari hasil analisis dan saran yang dianggap perlu.

BAB II
LANDASAN TEORI

2.1 Cybercrime

2.1.1 Definisi Cybercrime

*Cybercrim*e merupakan suatu tidakan kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama dan memanfaatkan perkembangan teknologi komputer khususnya Internet. *Cybercrim*e didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi Internet (Fajar, 2010)

Cybercrime adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Hal-hal yang termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara *online*, pemalsuan cek, penipuan kartu kredit/carding, *confidence fraud*, penipuan identitas, pornografi anak, dll.

2.1.2 Karakteristik Cybercrime

Cybercime sendiri memiliki beberapa karakteristik berdasarkan tindakan, sifat dan ruang lingkup kejahatannya. Berbeda dengan kejahatan lainnya, *cybercrime* dikelompokkan sesuai dengan karakteristik dari masing-masing kejahatannya. Dalam perkembangan kejahatan konvensional *cybercrime* dikenal dengan (Lestari, 2008) :

1. Kejahatan kerah biru
2. Kejahatan kerah putih

Kejahatan *cybercrime* sendiri memiliki karakteristik yang unik yaitu (Lestari, 2008) :

1. Ruang lingkup kejahatan

2. Sifat kejahatan
3. Pelaku kejahatan
4. Modus kejahatan
5. Jenis kerugian yang ditimbulkan

Dari karakteristik di atas agar dalam penangannya lebih mudah maka *cybercrime* diklasifikasikan menjadi (Lestari, 2008) :

1. *Cyberpiracy* : Penggunaan teknologi komputer untuk membuat salinan software atau informasi, yang pada nantinya informasi atau software tersebut akan didistribusikan menggunakan teknologi komputer tanpa seijin yang memiliki hak.
2. *Cybertrespass* : Penggunaan teknologi komputer untuk meningkatkan akses pada sistem komputer suatu organisasi ataupun individu
3. *Cybervandalism* : Penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi elektronik yang dapat menghancurkan data yang ada dalam komputer.

2.1.3 Kasus Cybercrime

Kemajuan teknologi dan informasi saat ini tidak hanya berdampak positif untuk kemajuan serta perkembangan peradaban manusia. Namun perkembangan pesat teknologi itu sendiri juga terlihat memiliki pengaruh negatif. Berbagai permasalahan yang timbul seiring perkembangan teknologi informasi dan komunikasi salah satunya adalah tindak kejahatan *cybercrime*. Jenis *cybercrime* sendiri dapat dibedakan berdasarkan aktivitasnya dan motifnya yaitu (Prasetya, 2008) :

A. Jenis *cybercrime* yang berdasarkan aktivitasnya yaitu (Prasetya, 2008) :

1. *Unauthorized Access to Computer System and Service*

Merupakan tindak kejahatan yang dilakukan dengan cara memasuki / menyusup ke dalam suatu jaringan komputer secara ilegal, tanpa izin atau tanpa sepengetahuan pemilik suatu jaringan komputer tersebut. Biasanya kejahatan ini bermaksud untuk mendapatkan informasi

rahasia dari suatu individu ataupun kelompok yang diserang. Contoh, ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa website milik pemerintah RI dirusak oleh hacker (Kompas, 11/08/1999). Hacker juga telah berhasil menembus masuk ke dalam database berisi data para pengguna jasa America Online (AOL), sebuah perusahaan Amerika Serikat yang bergerak dibidang e-commerce, yang memiliki tingkat kerahasiaan tinggi (Indonesian Observer, 26/06/2000). Situs Federal Bureau of Investigation (FBI) juga tidak luput dari serangan para hacker, yang mengakibatkan tidak berfungsinya situs ini dalam beberapa waktu lamanya.

2. *Illegal Content*

Merupakan tindak kejahatan yang dilakukan dengan memasukkan data atau memberikan informasi ke Internet tentang suatu hal yang tidak benar, tidak layak dan hal-hal yang dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Contoh, menyebarkan berita fitnah yang dapat merusak nama baik orang lain, memasukkan konten pornografi atau konten yang mengandung rahasia negara ataupun propaganda melawan pemerintahan yang sah.

3. *Data Forgery*

Merupakan kejahatan yang dilakukan dengan cara memasukkan data-data palsu pada dokumen penting yang tersimpan sebagai *scriptless* dokumen melalui Internet.

4. *Cyber Espionage*

Merupakan suatu tindak kejahatan dimana pelaku kejahatan memanfaatkan jaringan komputer maupun Internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran.

5. *Cyber Sabotage and Extortion*

Merupakan kejahatan yang dilakukan dengan cara membuat gangguan, penghancuran atau perusakan dari suatu data, program komputer atau

sistem jaringan komputer yang terhubung dengan Internet. Biasanya kejahatan ini dilakukan dengan menyusupkan logic bomb, virus komputer maupun program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan semestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Kejahatan ini juga biasanya disebut sebagai cyber-terrorism.

6. *Offense Againts Intellectual Property*

Kejahatan ini dilakuakn dengan melakukan pelanggaran terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di Internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di Internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

7. *Infringements of Privacy*

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara komputerized, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

8. *Cracking*

Kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak sistem keamanan suatu sistem komputer dan biasanya melakukan pencurian, tindakan anarkis begitu mereka mendapatkan akses. Biasanya masyarakat sering salah menafsirkan antara seorang hacker dan cracker dimana hacker sendiri identetik dengan perbuatan negatif, padahal hacker adalah orang yang senang memprogram dan percaya bahwa informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dapat dipublikasikan dan rahasia.

9. *Carding*

Adalah kejahatan dengan menggunakan teknologi komputer untuk melakukan transaksi dengan menggunakan kartu kredit orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil

B. Jenis *cybercrime* yang berdasarkan motifnya dibagi menjadi dua yaitu (Prasetya, 2008) :

- *Cybercrime* sebagai tindak kejahatan murni

  Merupakan tindak kejahatan yang dilakukan secara disengaja, dimana kejahatan tersebut dilakukan secara sengaja dan terencana untuk melakukan pengerusakan, pencurian, tindakan anarkis, terhadap suatu sistem informasi atau sistem komputer.
- *Cybercrime* sebagai tindak kejahatan abu-abu

  Kejahatan ini tidak dapat terlihat jelas antara kejahatan kriminal atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer tersebut. Selain itu *cybercrime* juga dilakukan berdasarkan motif yang terbagi menjadi :
- *Cybercrime* yang menyerang individu

  Kejahatan yang ditujukan terhadap orang lain secara sengaja dengan motif dendam atau sekedar melakukan hal iseng yang bertujuan untuk merusak nama baik, ataupun mencoba mempermaikan seseorang untuk mendapatkan kepuasan pribadi. Contoh : Pornografi, *cyberstalking*, dll
- *Cybercrime* yang menyerang hak cipta

  Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi/umum ataupun demi materi/nonmateri.
- *Cybercrime* yang menyerang pemerintah

  Kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan teror, membajak ataupun merusak keamanan suatu

pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahan, atau menghancurkan suatu Negara.

2.1.4 Alasan Kemunculan Cybercrime

Semakin berkembang suatu teknologi komunikasi maka semakin meningkat pula tingkat kejahatan di dalamnya. Perkembangan dunia teknologi komunikasi dan Internet menyebabkan semakin banyak orang yang terkoneksi dengan Internet sehingga menimbulkan peluang munculnya berbagai jenis kejahatan komputer dengan beragam variasi kejahatannya. Dalam hal ini menurut Drs. Rusbagio Ishak (Kombes Pol/49120373), terdapat beberapa tendensi dari munculnya berbagai gejala kejahatan komputer :

a. Permasalahan finansial

   C*ybercrime* dapat menjadi alternatif baru untuk mendapatkan uang. Perilaku *carding* (penggunaan hak atas kartu kredit yang dilakukan tanpa seijin pihak yang sebenarnya mempunyai hak*)*, melakuakan pengalihan rekening telepon dan fasilitas lainnya, adalah sebagian bentuk *cybercrime* dengan tendensi finansial.

b. Permasalahan terkait politik, militer dan sentimen nasionalisme

   Teknologi tingkat tinggi yang dimiliki oleh suatu negara pada umumnya menjadi lahan yang menarik bagi tiap negara untuk dijadikan ajang kompetisi dalam mengembangkan peralatan tempurnya, sehingga antar suatu negara terjadi persaingan yang dapat menyebabkan terjadinya tindak *cybercrime* yang digunakan untuk mendapatkan akses informasi antar negara pesaing.

c. Faktor kepuasan pelaku

   Pada tendensi ini terdapat masalah psikologis dari pelakunya. Dimana ada kecenderungan bahwa seseorang dengan kemampuan yang tinggi akan selalu merasa tertantang untuk menerobos berbagai sistem keamanan yang

ketat. Dalam hal ini kepuasan batin menjadi orientasi utama bagi pelaku dibandingkan dengan tujuan finansial ataupun sifat sentimen.

2.2 Komputer Forensik

2.2.1 Definisi Komputer Forensik

Komputer forensik merupakan bagian dari salah satu ilmu yang berkecimpung di dunia forensik, dimana berfungsi untuk mencari informasi dari suatu benda atau kejadian tertentu. Komputer Forensik sebagai cabang Ilmu Forensik memiliki banyak pengertian, antara lain adalah sebagai berikut:

- Pengungkapan, pengolahan, pemeliharaan, dan analisis informasi yang diperoleh dari sistem, jaringan, aplikasi, atau sumber daya komputasi lain, untuk menentukan sumber serangan terhadap sumber-sumber itu **(Weise & Powell, 2005).**

- Cabang ilmu baru dan sedang berkembang yang dijelaskan sebagai pembelajaran terhadap bukti digital yang merupakan hasil dari suatu kejadian. Hal ini memerlukan analisis terhadap data digital. Langkah langkah lain yang sangat penting dalam komputer forensik adalah ***incident preparation***, ***detection***, dan ***recovery***. Semua prosedur ini harus didokumentasikan dengan baik sesuai dengan standart yang berlaku (Haase, 2001).

- Komputer Forensik dapat didefinisikan sebagai penerapan ilmu hukum dalam mencari kebenaran dalam hal perdata, pidana, dan sosial untuk mengakhiri ketidakadilan yang tidak dilakukan untuk setiap anggota masyarakat (EC-Council, 2010).

Dari pengertian di atas dapat disimpulkan bahwa komputer forensik merupakan aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti komputer dalam kejahatan komputer dengan standar yang berlaku. Komputer forensik juga merupakan kombinasi ilmu hukum dan pengetahuan komputer dalam

mengumpulkan dan menganalisis data dari sistem komputer. Selain itu dapat dikatakan pula bahwa komputer forensik merupakan bagian dari keilmuan yang menyelidiki permasalahan tertentu untuk menemukan suatu titik cerah yang pada nantinya dapat digunakan untuk menyelesaikan suatu permasalahan tertentu.

2.2.2 Tujuan Komputer Forensik

Dalam tiap menyelesaikan kasusnya komputer forensik selalu memiliki tujuan-tujuan tertentu yang pada nantinya digunakan untuk mendapatkan hasil yang dapat digunakan oleh penyidik. Komputer forensik dilakukan dengan tujuan (EC-Council, 2010) :

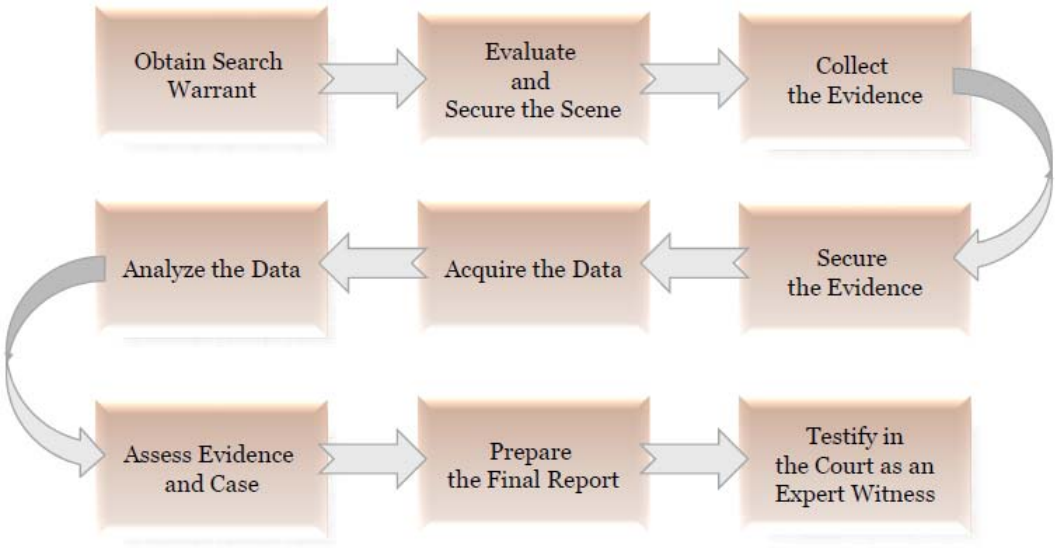
a. Untuk menentukan nilai-nilai bukti dari Tempat Kejadian Perkara (TKP) serta bukti terkait dengan kasus yang bersangkutan.
b. Untuk memulihkan, menganalisis, dan memelihara komputer atau yang hal-hal terkait dengan tindak kejahatan komputer yang kemudian diproses sedemikian rupa hingga dapat disajikan sebagai bukti di pengadilan hukum.
c. Untuk mengidentifikasi bukti dalam waktu singkat, memperkirakan dampak potensial dari aktivitas yang berbahaya bagi korban, dan mengidentifikasi pelaku.

2.2.3 Prosedur Komputer Forensik

Komputer Forensik merupakan ilmu yang menerapkan prosedur-prosedur dalam tiap penyelesaian kasusnya. Agar barang bukti yang ditemukan dapat digunakan sebagai barang bukti yang sah di pengadilan, ahli forensik harus melakukan prosedur yang benar. Prosedur forensik harus dilakukan berdasarkan tahapan-tahapan yang ada secara runtut, hal ini dilakukan untuk mengurangi terjadinya kesalahan dalam menangani sebuah kasus kejahatan. Adapun prosedur dan metodologi forensik yang biasa digunakan seorang ahli forensik yaitu (EC-Council, 2010) :

Gambar 2.1 Prosedur Komputer Forensik

(Sumber : EC-Council, C. (2010). Module)



Gambar 2.2 Metodologi Komputer Forensik

(Sumber : EC-Council, C. (2010). Module)

2.2.4 Investigasi Kasus

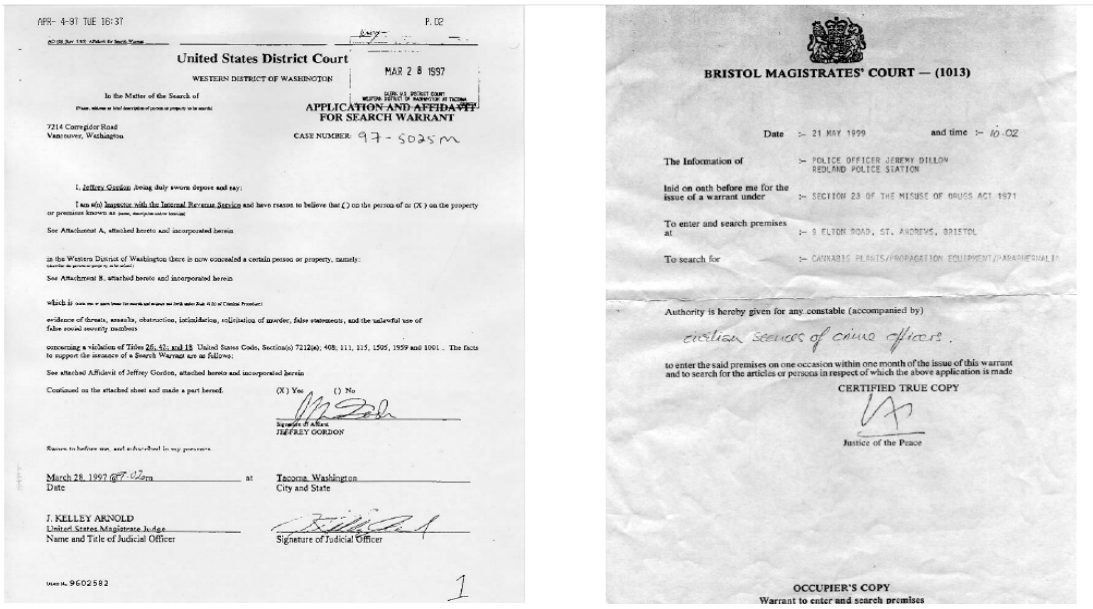
Investigasi kasus merupakan langkah awal dalam prosedur komputer forensik yang menentukan jenis kasus, apakah tergolong sebagai *low level*, *medium level*, atau *high level*. Tahapan investigasi kasus berperan penting untuk mengungkap kasus tersebut. Pada tahapan ini seorang penyidik dituntut untuk

bersikap awas agar tidak salah bertindak yang dapat mengakibatkan terhambatnya pengungkapan kasus. Adapun hal-hal yang dilakukan seorang penyidik dalam investigasi kasus yaitu (EC-Council, 2010) :

a. Menentukan, jenis level kasus telah terjadi
b. Menemukan dan mengintepretasi pentunjuk yang tertinggal.
c. Menyiapkan segala hal yang diperlukan dalam pencarian barang bukti.
d. Mencari dan mengumpulkan perangkat komputer (digital).
e. Mengumpulkan barang bukti yang dapat dipresentasikan di pengadilan.

2.2.5 Surat Pemeriksaan (*Search Warrant)*

Untuk melakukan suatu investigasi dalam sebuah kasus komputer forensik surat dari pengadilan sangatlah dibutuhkan. Surat dari pengadilan diperlukan sebagai bukti bahwa tindakan yang dilakuakn yaitu berupa pengumpulan barang bukti bersifat legal dan dijamin oleh hukum. Adapun bentuk dari surat pengadilan yaitu (EC-Council, 2010):



APR- 4-97 TUE 16:37 P. 02

United States District Court

WESTERN DISTRICT OF WASHINGTON

MAR 2 8 1997

In the Matter of the Search of

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

7214 Corregidor Road
Vancouver, Washington

CASE NUMBER: 97-5025M

I, Jeffery Gordon being duly sworn depose and say:

I am a(n) Inspector with the Internal Revenue Service and have reason to believe that ( ) on the person of or (X) on the property or premises known as (name, description and/or location)

See Attachment A, attached hereto and incorporated herein

in the Western District of Washington there is now concealed a certain person or property, namely:

See Attachment B, attached hereto and incorporated herein

which is (state one or more bases for search and seizure set forth under Rule 41(b) of Federal Rules)

evidence of threats, assaults, obstruction, intimidation, solicitation of murder, false statements, and the unlawful use of false social security numbers

concerning a violation of Titles 26, 42, and 18 United States Code, Section(s) 7212(a); 408; 111, 115, 1505, 1959 and 1001 . The facts to support the issuance of a Search Warrant are as follows:

See attached Affidavit of Jeffrey Gordon, attached hereto and incorporated herein

Continued on the attached sheet and made a part hereof. (X) Yes ( ) No

Signature of Affiant
JEFFREY GORDON

Sworn to before me, and subscribed in my presence

March 28, 1997 @ 9:02am at Tacoma, Washington
Date City and State

J. KELLEY ARNOLD
United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

Order #: 9602582

1

BRISTOL MAGISTRATES' COURT — (1013)

Date :- 21 MAY 1999 and time :- 10.02

The Information of :- POLICE OFFICER JEREMY DILLON
REDLAND POLICE STATION

laid on oath before me for the issue of a warrant under :- SECTION 23 OF THE MISUSE OF DRUGS ACT 1971

To enter and search premises at :- 9 ELTON ROAD, ST. ANDREWS, BRISTOL

To search for :- CANNABIS PLANTS/PROPAGATION EQUIPMENT/PARAPHERNALIA

Authority is hereby given for any constable (accompanied by)

Civilian Scenes of Crime Officers.

to enter the said premises on one occasion within one month of the issue of this warrant and to search for the articles or persons in respect of which the above application is made

CERTIFIED TRUE COPY

Justice of the Peace

OCCUPIER'S COPY
Warrant to enter and search premises

Gambar 2.2 *Search Warrant*

(Sumber : EC-Council, C. (2010). Module)

2.2.6 Mengumpulkan dan Mengelola Barang Bukti

Ini adalah langkah penting dalam proses forensik untuk mengidentifikasi sumber-sumber potensial dan bagaimana kemudian data dikumpulkan. Data yang sering didapat terdapat pada personal komputer atau desktop komputer, namun bukan hanya desktop komputer saja yang menjadi sumber data, *server* dan mencakup pula media penyimpanan yang dialokasikan pada jaringan komputer (file server, file sharing dan lainnya) menjadi sumber-sumber daya. Selain melibatkan drive untuk mengakses media, ada beberapa perangkat yang mungkin mengintegritasikan media penyimpanan dengan drive (alat pengaksesan nya). Seperti : *CD-ROM Drive, DVD-ROM Drive, USB (Universal Serial Bus) Port, Firewire, PCMCIA (Personal Computer Memory Card Intenational Association)* dan media penyimpanan eksternal lainnya. Pengumpulan data ini mencakup aktivitas seperti (EC-Council, 2010) :

a. Identifikasi.
b. Penamaan (*labeling*).
c. Perekaman (*Recording*).
d. Mendapatkan data.

Untuk mengumpulkan tiap barang bukti yang bersifat fisik investigator harus mengisikan formulir agar barang bukti yang telah dikumpulkan dapat terdata dengan baik. Formulir barang bukti dibuat sebagai bagian dari tindakan penamaan dalam tahapan pengelolaan suatu barang bukti. Formulir barang bukti berisi informasi berupa tanggal dan waktu pengumpulan barang bukti serta deskripsi tentang barang bukti yang telah ditemukan. Adapun bentuk formulir barang bukti yaitu :

EVIDENCE
Submitting Agency: _____
Case No: _____
Item No: _____
Date of Collection: _____
Time of Collection: _____
Collected by: _____
Badge No: _____
Description of Enclosed Evidence: _____ _____ _____
Location Where Collected: _____ _____ _____
Type of Offense: _____
Victim's Full Name: _____
Suspect's Full Name: _____

Gambar 2.4 Formulir Barang Bukti

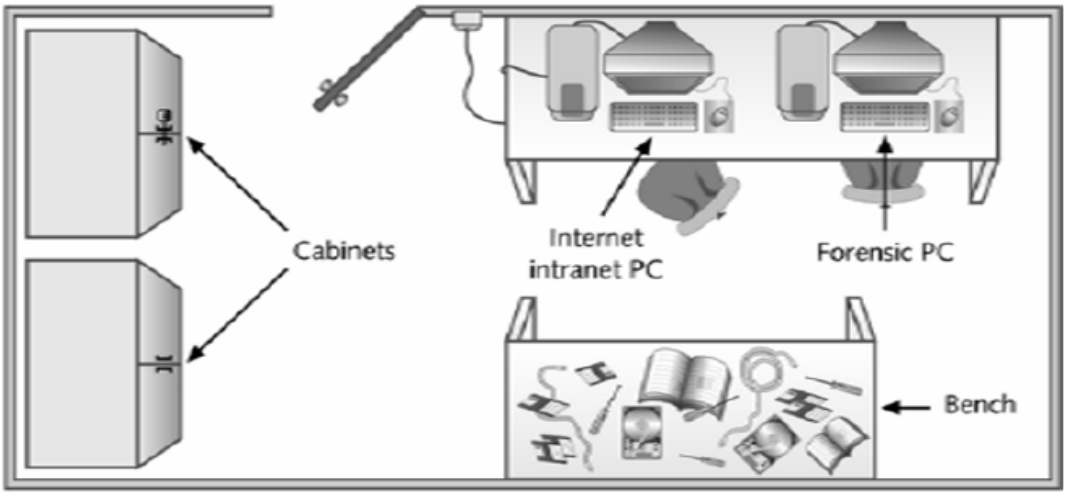
(Sumber : EC-Council, C. (2010). Module)

Untuk mengelola tiap barang bukti yang ada seorang investigator harus memeperhatikan cara dan dimana barang bukti tersebut harus disimpan. Adapun bagian-bagian yang harus diperhatikan dalam melakukan pengelolaan barang bukti yaitu (EC-Council, 2010) :

a. Tempat Penyimpanan Barang Bukti
b. Pendataan Perjalanan Barang Bukti (Chain of Custody)

2.2.7 Ruang Penyimpanan Barang Bukti

Barang bukti yang telah dikumpulkan agar nantinya dapat digunakan dan didata dengan baik haruslah diatur dan diamankan sesuai prosedur yang ada. Untuk tempat penyimpanan barang bukti haruslah ditempat penyimpanan yang telah dibuat khusus untuk menyimpan barang bukti kasus forensik.



Gambar 2.5 Ruangan Penyimpanan Barang Bukti

(Sumber : EC-Council, C. (2010). Module)

Adapun bentuk ruangan tempat penyimpanan barang bukti dapat dilihat pada gambar di atas (gambar 2.5). Dimana terlihat ruangan tersebut minimal harus memiliki dua buah cabinet yang memiliki kunci, sebuah meja, komputer untuk melakukan forensik (tidak terhubung ke jaringan), komputer yang terhubung ke jaringan, serta yang terpenting ruangan tersebut hanya memiliki satu akses keluar masuk.

2.2.8 Chain of Custody

Chain of Custody merupakan rekap perjalanan barang bukti. Tiap-tiap barang bukti yang telah dikumpulkan memiliki masing-masing satu buah *chain of custody*. *Chain of custody* berfungsi sebagai catatan agar barang bukti yang disimpan dapat diketahui keberadaannya, serta mengurangi resiko hilangnya barang bukti tersebut. Adapun formulir dari *chain of custody* yaitu (EC-Council, 2010) :

			efor Case #
			Client Ref. #
Client Item #	Description:		
Make:	Model:	Serial #	Other Identifying #
Client Item #	Description:		
Make:	Model:	Serial #	Other Identifying #
Client Item #	Description:		
Make:	Model:	Serial #	Other Identifying #

CHAIN OF CUSTODY

Client Item #'s	Date/Time	Released By	Received By	Reason
	Date	Name/Client	Name/Client	
	Time	Signature	Signature	

Gambar 2.6 Formulir *Chain of Custody*

(Sumber : EC-Council, C. (2010). Module)

2.2.9 Analisis Barang Bukti

Analisis barang bukti adalah tahapan yang dilakukan untuk memeriksa dan menguji barang bukti yang telah ditemukan untuk mendapatkan hasil yang biasa digunakan dalam persidangan. Analisis ini dilakukan melalui tahapan-tahapan yang ada. Pada tahapan ini penyidik melakukan segala upaya untuk menemukan barang bukti digital. Adapun pada penelitian ini melalui tahapan analisis barang bukti berupa (EC-Council, 2010) :

a. Membuat Image Barang Bukti, tiap item minimal dibuat sebanyak 2 buah *clone.* Image digunakan untuk diperiksa oleh investigator, karena barang bukti asli tidak boleh diselidiki secara langsung.
b. Melakukan Pemeriksaan barang bukti menggunakan tools forensik.
c. Membuat Laporan dan Dokumentasi.

2.2.10 Aturan-aturan Komputer Forensik

Dalam menangani suatu kasus forensik, investigator harus mematuhi aturan-aturan dasar komputer forensik untuk mencegah terjadinya kesalahan dalam penanganan kasus yang dapat menyebabkan kerugian pada diri sendiri

maupun klien. Aturan-aturan ini bersifat wajib dan merupakan batas-batas yang dibuat untuk para penyidik sehingga mengurangi resiko terhambatnya penanganan kasus. Aturan-aturan tersebut yaitu (EC-Council, 2010):

a. Mengurangi kemungkinan untuk menginvestigasi barang bukti secara langsung
b. Mematuhi aturan *barang bukti.*
c. Jangan merusak barang bukti.
d. Selalu menyiapkan *chain of custody.*
e. Menangani barang bukti dengan kepedulian.
f. Tidak pernah melampaui pengetahuan dasar.
g. Mendokumentasikan segala perubahan pada barang bukti.

2.3 Barang Bukti

2.3.1 Definisi Barang Bukti

Barang bukti merupakan bagian terpenting dalam pengungkapan suatu kasus kejahatan. Karena dari barang bukti inilah dapat disimpulkan bahwa suatu kejahatan yang terjadi telah dilakukan oleh tersangka kejahatan tersebut. Pengertian barang bukti dalam Kitab Undang-undang Hukum Acara Pidana (KUHAP) memang tidak dijelaskan secara eksplisit, tetapi dalam KUHAP diatur beberapa ketentuan tentang barang bukti tersebut. Berikut ini pengertian dari barang bukti yaitu :

- Barang bukti merupakan barang yang dipergunakan oleh terdakwa untuk melakukan suatu tindak pidana atau barang sebagai hasil dari suatu tindak pidana. Barang-barang ini disita oleh penyidik untuk dijadikan sebagai bukti dalam sidang pengadilan. Barang ini kemudian diberi nomor sesuai dengan nomor perkaranya, disegel dan hanya dapat dibuka oleh hakim pada waktu sidang pengadilan (Ansori Sabuan, 1990).

- Barang yang merupakan objek, barang yang merupakan produk, barang yang dipergunakan sebagai alat, barang yang terkait dengan peristiwa pidana (Gerson, 1977).

- Benda yang digunakan untuk meyakinkan hakim akan kesalahan terdakwa terhadap perkara pidana yang dituduhkan kepadanya (KBBI, 1994).

- Benda-benda yang dipergunakan untuk memperoleh hal-hal yang benar-benar dapat meyakinkan hakim akan kesalahan terdakwa terhadap perkara pidana yang dituduhkan, benda-benda ini adalah kepunyaan terdakwa, barang-barang yang diperoleh terdakwa dengan kejahatan, barang-barang dengan mana terdakwa melakukan kejahatan (simorangkir, 2002).

2.3.2 Klasifikasi Barang Bukti

Barang bukti yang dihadirkan dalam suatu persidangan tidak hanya berupa barang bukti fisik. Selain barang bukti yang bersifat fisik terdapat pula barang bukti yang tidak dapat dilihat secara fisik atau berupa data. Karena itu barang bukti menurut bentuknya dapat diklasifikasikan menjadi (AKBP Bakti Andriyono, S.Si. M.Si, 2011) :

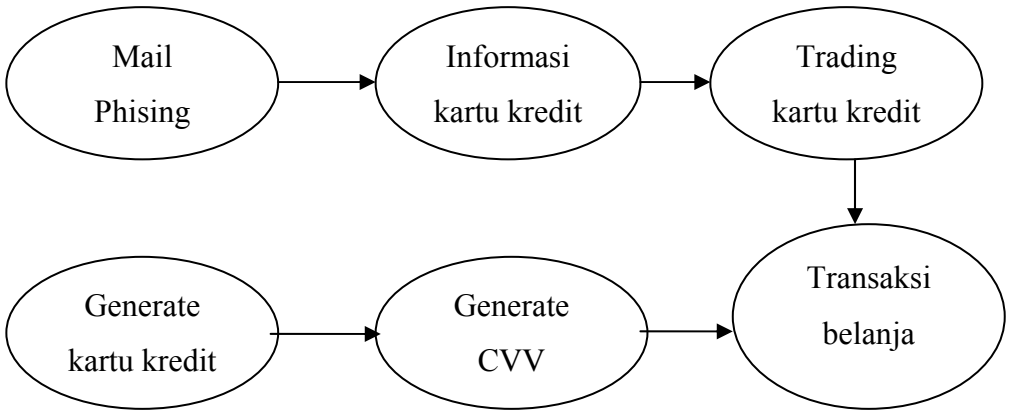
- Barang bukti fisik, merupakan barang bukti yang berbentuk secara fisik, dapat dikenali secara visual dan bersifat nyata. Oleh karena itu penyidik dan forensik analis harus sudah memahami untuk kemudian dapat mengenali masing-masing barang bukti ini ketika sedang melakukan proses searching (pencarian) barang bukti di TKP. Contoh : hardisk, flashdisk, modem, Switch.

- Barang bukti digital, barang bukti ini bersifat digital yang diekstrak atau di-recover dari barang bukti fisik. Barang bukti ini di dalam Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dikenal dengan istilah informasi elektronik dan dokumen elektronik. Jenis barang bukti inilah yang harus dicari oleh forensik analis untuk kemudian dianalisa secara teliti keterkaitan masing-masing file dalam rangka mengungkap kasus kejahatan yang berkaitan dengan barang bukti fisik. Contoh : dokumen *spreadsheet, history web browser,* log percakapan aplikasi *chatting, email.*

BAB III
METODOLOGI

3.1 Skenario Kasus Kejahatan

Meningkatnya populasi orang yang terkoneksi dengan Internet akan menjadi peluang bagi munculnya kejahatan komputer dengan beragam variasi kejahatannya. Di antara sebagian besar kasus yang terjadi terdapat kasus yang memiliki tendensi berupa permasalahan finansial dan kepuasan. Perilaku *carding* merupakan suatu tindakan yang termotivasi terhadap masalah finansial, dimana pelaku menggunakan kemampuannya untuk mengakses secara ilegal terhadap kartu kredit orang lain untuk digunakan secara pribadi. Kasus *carding* dapat dilakukan secara individual maupun berkelompok. Biasanya pelaku yang melakukan secara individual menggunakan *tools* (*card extrapolator*). Sedangkan yang dilakukan secara berkelompok biasanya bekerjasama dengan suatu usaha tertentu yang menggunakan kartu kredit dalam pembayarannya. Dimana pelaku menyimpan hasil inputan dari kartu kredit ke tempat penampungan lain secara ilegal. Adapun bentuk gambaran skenario carding pada kasus ini dapat dilihat pada gambar 3.1.



Gambar 3.1 Gambaran Skenario Kasus

Dari gambaran skenario kasus di atas dapat dilihat urutan langkah kejahatan *carding.* Dalam skenario kasus ini detail tindakan pelaku *carding* dapat dilihat sebagai berikut:

a) Pelaku carding menyebarkan mail phising untuk mendapatkan informasi kartu kredit dari pengguna layanan tersebut.

b) Pelaku juga menggunakan aplikasi *Credit Wizard* untuk mengenerate nomer kartu kedit.

c) Dari nomer kartu kredit yang telah didapat dari hasil generate, pelaku kemudian menggunakan aplikasi IRC untuk mendapatkan CVV dari nomer kartu kredit tersebut.

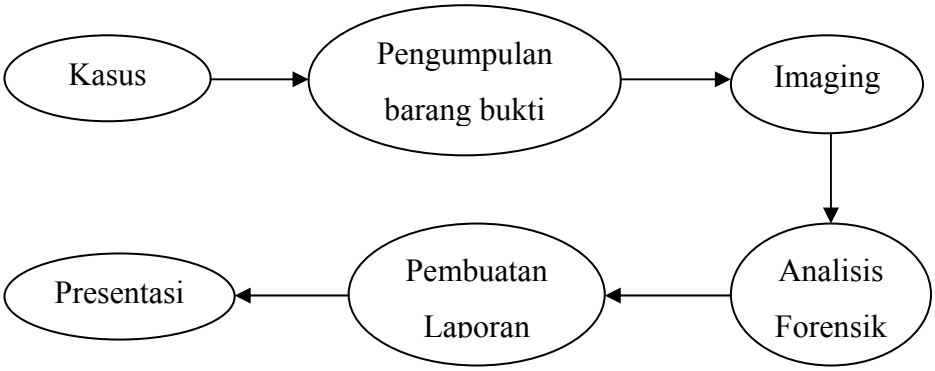
d) Pelaku melakukan transaksi mejual kartu kredit yang telah didapat melalui iRC.

e) Setelah memiliki informasi kartu kredit pelaku menggunakannya secara pribadi untuk belanja online membeli buku di amazon.com dengan menggunakan web browser Mozilla Firefox.

f) Setelah transaksi terjadi pelaku mendapatkan email notifikasi dari amazon.com dan kemudian pelaku menyimpan invoice transaksi pada laptop.

3.2 Skenario Pembuktian

Dalam melakukan suatu penyidikan untuk mengungkap kasus kejahatan komputer seorang penyidik harus mengetahui langkah-langkah yang harus diambila dalam tiap penyidikannya. Hal tersebut dilakukan untuk dapat menemukan bukti-bukti yang akurat. Dalam tiap tahapan penyidikan, tiap langkah harus dilakukan secara seksama dan teliti agar tidak terjadi kesalahan dalam penanganannya. Adapun gambaran skenario pembuktian pada kasus ini yaitu :



Gambar 3.2 Gambaran Skenario Pembuktian

3.2.1 Identifikasi Kasus

Identifikasi Kasus dilakukan untuk mendapatkan informasi dari kasus yang telah terjadi. Pada kasus dalam penelitianini dapat diidentifikasi bahwa kasus merupakan kasus carding yang dilakukan oleh individu. Kasus ini dikategorikan dalam *low level case.* Pada kasus kejahatan ini yang menderita kerugian yaitu pihak pemilik kartu kredit yang terkena phising oleh pelaku.

3.2.2 Pengumpulan barang Bukti

Pengumpulan barang bukti merupakan langkah penting untuk mendapatkan petunjuk-petunjuk yang dapat membuktikan suatu tindak kejahatan. Dimana dalam pengumpulan barang bukti ini seorang penyidik harus mengetahui dan dapat mengidentifikasi semua sumber-sumber potesial dan data yang dikumpulkan. Data yang sering didapat terdapat pada personal komputer atau desktop komputer, namun bukan hanya desktop komputer saja yang menjadi sumber data, *server* dan mencakup pula media penyimpanan yang dialokasikan pada jaringan komputer (file server, file sharing dan lainnya) menjadi sumber-sumber daya.

Dalam tahapan pengumpulan barang bukti ini, pada skenario kasus yang telah disebutkan sebelumnya ditemukan barang bukti berupa sebuah laptop, modem, flashdisk. Untuk memudahkan dalam penyidikan maka barang bukti dikelompokkan menjadi :

- Barang bukti utama, merupakan barang bukti yang pada nantinya akan dianalisis oleh penyidik. Barang bukti utama dalam kasus ini berupa : laptop dan flashdisk.

- Barang bukti tambahan, merupakan barang bukti yang didapat pada saat pengumpulan barang bukti di TKP. Barang bukti tidak dapat dianalisis sehingga hanya disertakan sebagai barang bukti tambahan di persidangan. Barag bukti tambahan dalam kasus ini berupa : modem.

3.2.3 *Imaging* Barang bukti

Untuk menemukan suatu barang bukti maka seorang penyidik harus melakukan suatu pengumpulan barang bukti yang kemudian barang bukti tersebut akan dilakukan *imaging.* Salah satu barang bukti yang dapat di *imaging* adalah sebuah *Hardisk*, dimana dalam melakukan *imaging* terhadap *hardisk* terdapat beberapa pilihan seperti *physical drive* atau *logical drive.* Ketika *examiner* memilih *phisical drive* maka *imager* akan meng*image* hardisk secara keseluruhan tergantung dari kapasitas hardisk itu sendiri, namun ketika *examiner* memilih *logical drive* maka *examiner* dapat memilih partisi mana yang akan di *image*, tergantung dari kebutuhan. Pada skenario kasus ini barang bukti yang akan diimaging berupa hardisk pada laptop, dan flashdisk. Untuk melakukan imaging barang bukti maka diperlukan aplikasi untuk membuat *clone* dari hardisk laptop dan flashdisk pelaku. Untuk itu maka diperlukan perangkat danaplikasi berupa:

- Sebuah PC atau laptop dengan sistem operasi Windows.
- Aplikasi FTK Imager.

3.2.4 Analisis Forensik

Analisis terhadap barang bukti pada dasarnya bertujuan untuk membentuk dan mengikuti petunjuk yang ada, mengidentifikasi tersangka, format data,

pengembangan barang bukti, merekonstruksi kejahatan yang dilakukan, mengumpulkan lebih banyak data, dan bila beruntung mendapatkan barang bukti nyata yang membuat tersangka tidak bisa berkutik. Jadi pada dasarnya data digital hanyalah bagian dari keseluruhan gambaran umum. Membentuk dan Mengikuti Petunjuk File pada komputer dapat mengarah pada website yang dikunjungi tersangka maupun posting yang memberi petunjuk terhadap identitas penggunanya dan dapat membawa ke lebih banyak lagi bukti.

Pada kasus yang telah disebutkan sebelumnya barang bukti yang telah didapat akan dilakukan pemrosesan ulang sebelum nantinya diserahkan pada pihak yang membutuhkan. Pada tahapan inilah skema yang diperlukan akan menjadi lebih fleksibel menyesuaikan dengan kasus-kasus yang dihadapi. Barang bukti yang telah didapatkan perlu di*explore* kembali kedalam sejumlah skenario yang berhubungan dengan tindak pengusutan, antara lain: siapa dan apa yang telah dilakukan (Contoh : penggunaan software apa saja, waktu melakukan, dan hasil proses apa yang dihasilkan). Pada umumnya, semua data yang ditemukan dalam sistem komputermemiliki suatu potensi informasi yang belum diolah atau bersifat mentah, sehingga keberadaannya menjadi sangatlah penting. Data-data yang dimaksud antara lain : Alamat URL yang telah dikunjungi, Pesan email atau kumpulan alamat e-mail yang terdaftar, Program Word processing atau format ekstensi yang dipakai,Dokumen spreedsheat yang dipakai, format gambar yang dipakai apabila ditemukan, Registry Windows, Log Event viewers dan Log Applications, File print spool. Di sini akan digunakan *tools* berupa *Forensic Tool Kit (FTK).*

3.2.5 Pembuatan laporan

Pembuatan Laporan merupakan hal yang sangat penting sekali dalam hasil suatu investigasi. Laporan dibuat untuk dibaca oleh orang umum sehingga haruslah jelas dan ringkas. Dari studi kasus yang ada masing-masing akan dibuatkan sebuah laporan yang pada nantinya akan ditampilkan di sebuah persidangan sebagai hasil analisis komputer forensik sehingga barang bukti yang telah ditemukan dapat menjadi barang bukti yang sah.

3.2.6 Presentasi

Presentasi hasil analisis dilakukan oleh seorang *expert witness*, yaitu orang yang ahli dalam bidangnya yang pada nantinya akan menyampaikan pendapatnya terhadap kasus yang ada kepada orang lain dan membuat orang tersebut percaya apa yang disampaikannya telah sesuai menurut hukum yang sah. Pada penelitian ini akan ditampilkan dua buah jenis presentasi yaitu :

a. Presentasi kepada pihak kepolisian

   Pada tahapan ini penyidik akan menyampaikan informasi-informasi berdasarkan hasil pengamatan dan analisis terhadap kasus yang dibuat. Hal-hal yang akan disampaikan merupakan hal teknis dari analisis serta cara atau metode yang dilakukan pelaku dalam kejahatannya.

b. Presentasi di dalam persidangan

   Pada tahapan ini penyidik akan berprilaku sebagai *expert witness* yang akan menyampaikan pendapatnya terhadap orang-orang umum yang ada di pengadilan. *expert witness* berfungsi sebagai orang yang membantu pengadilan untuk mengerti seluk-beluk barang bukti yang akan ditampilkan.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Imaging Barang Bukti

Dalam skenario kasus yang telah dibuat terdapat beberapa barang bukti yang dapat di*imaging*. Pada tahapan ini akan dilakukan *imaging* terhadap barang bukti yang telah ditemukan yaitu berupa sebuah komputer dan flashdisk. Untuk melakukan *imaging* maka akan digunakan *FTK imager* dan *FTK* untuk membuat *image* hardisk.

4.1.1 FTK Imager

*FTK image*r merupakan *utility* terpisah dari *FTK* yang mendukung:

a. Preview *drive* dan *image* tanpa perlu menambahkan nya ke *case.*

b. Membuat *image* (*Create Disk Image*)

c. Mengkoversi i*mage*.

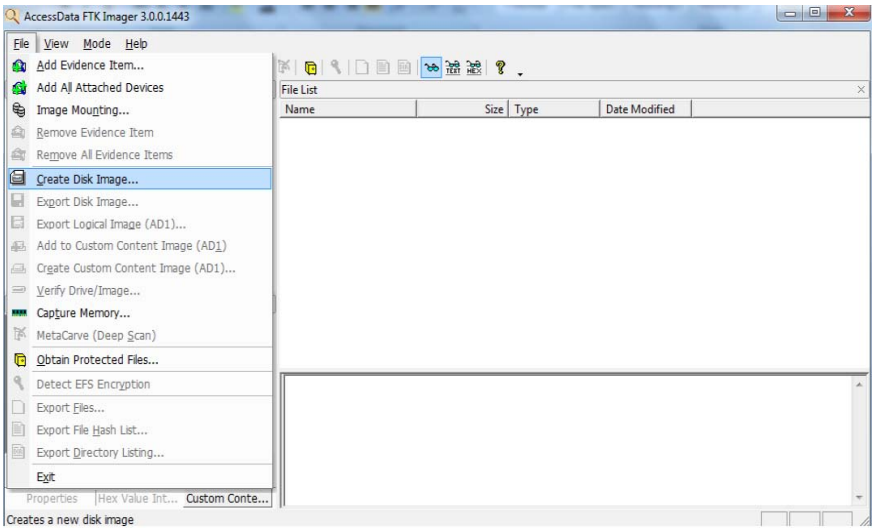
d. Membuat *hash*

e. View properti *image*, Drive, sistem file, file dan folder.

f. View file, *Thumbnail* dan folder yang telah dihapus pada opsi *orphan].*

Untuk membuat *image* tersebut, adapun langkah – langkah pada FTK *Image*r adalah sebagai berikut :

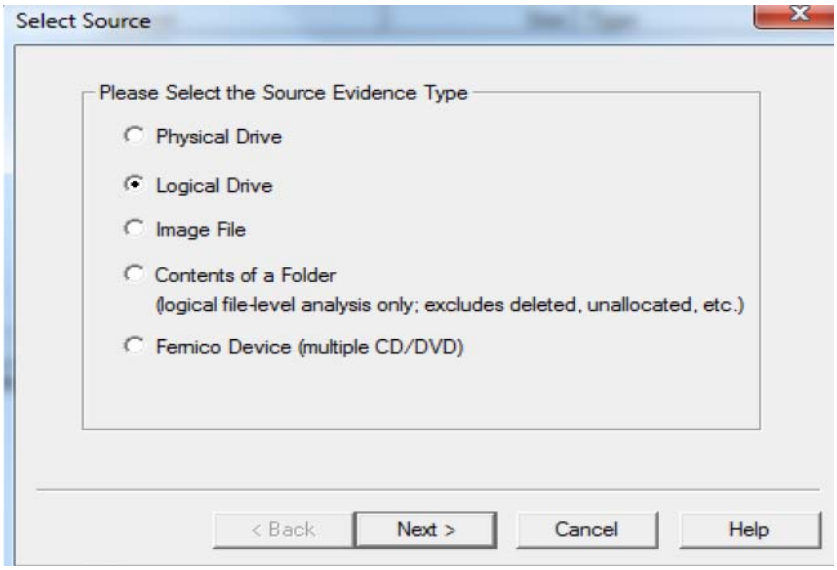
a) Setelah installasi *FTK image*r selesai, maka akan keluar tampilan awal *FTK image*r kemudian klik *file* > *Create Disk Image* > *Next*. Pada kasus ini akan dibuat *image* baru agar bisa dilakukan pengujian data menggunakan *FTK*.



Gambar 4.1 Membuat Disk Image

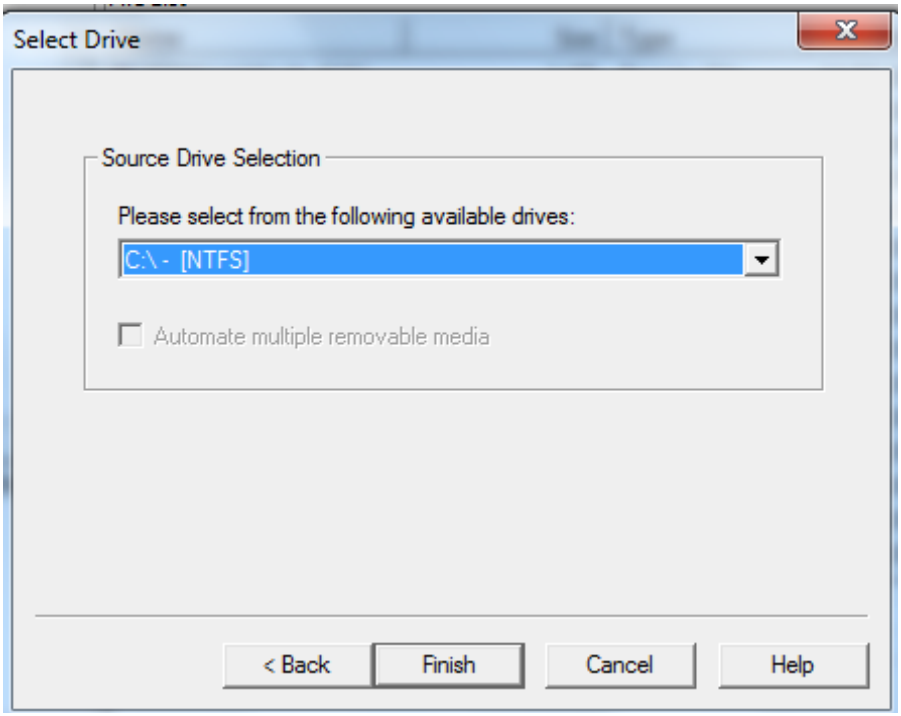
b) Kemudian akan tampil halaman *select source*. Halaman ini dapat memilih untuk melakukan *image* terhadap type apa, pada kasus ini akan dipilih *logical drive* agar lebih mempermudah melakukan pengecekan pada setiap *drive* nya dan waktu yang dibutuhkan relatif lebih singkat. Untuk proses pemilihan source terlihat pada gambar 4.2 Ada beberapa pilihan *source evidence type* yaitu :

   a. *Physical Drive*, digunakan untuk membuat *image* disk secara keseluruhan.
   b. *Logical drive*, digunakan untuk membuat *image* partisi yang ingin dianalisis.
   c. *Image* File, digunakan untuk mengkonversi *image*.
   d. *Content of a folder*, untuk memilih file atau folder tertentu dan hanya untuk kebutuhan analisis saja.
   e. *fernico device*, digunakan untuk mengimage cd / dvd.



Gambar 4.2 Select Source

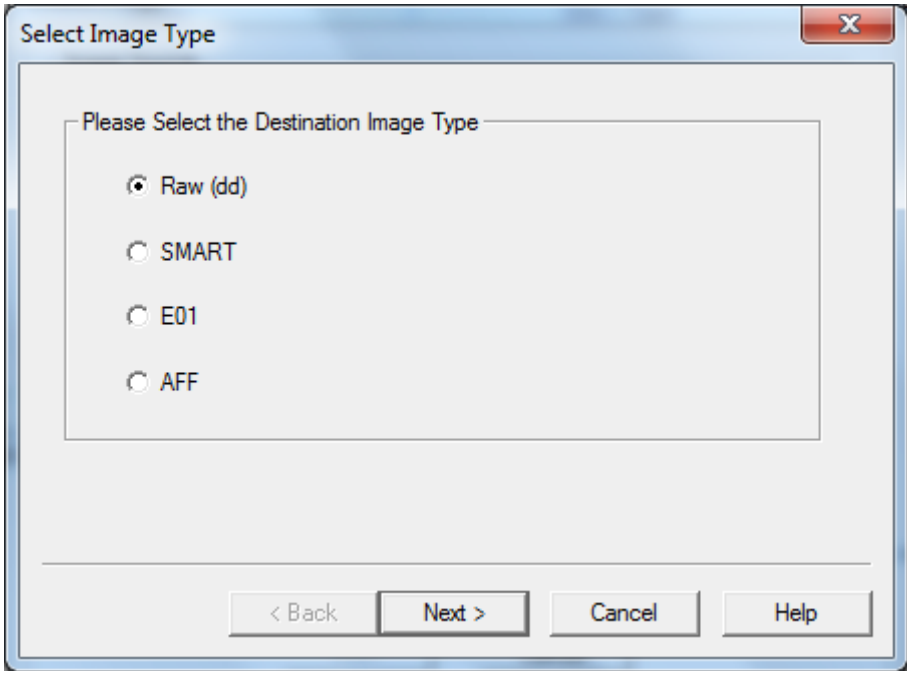
c) Selanjutnya pilih drive mana yang akan di *image* terlebih dahulu, misalnya memilih C :\[NTFS], yaitu local disk dari sistem operasi. Klik finish untuk mengakhiri. Proses *Select Drive* terlihat pada gambar 4.3 dibawah ini.



Gambar 4.3 *Select Drive*

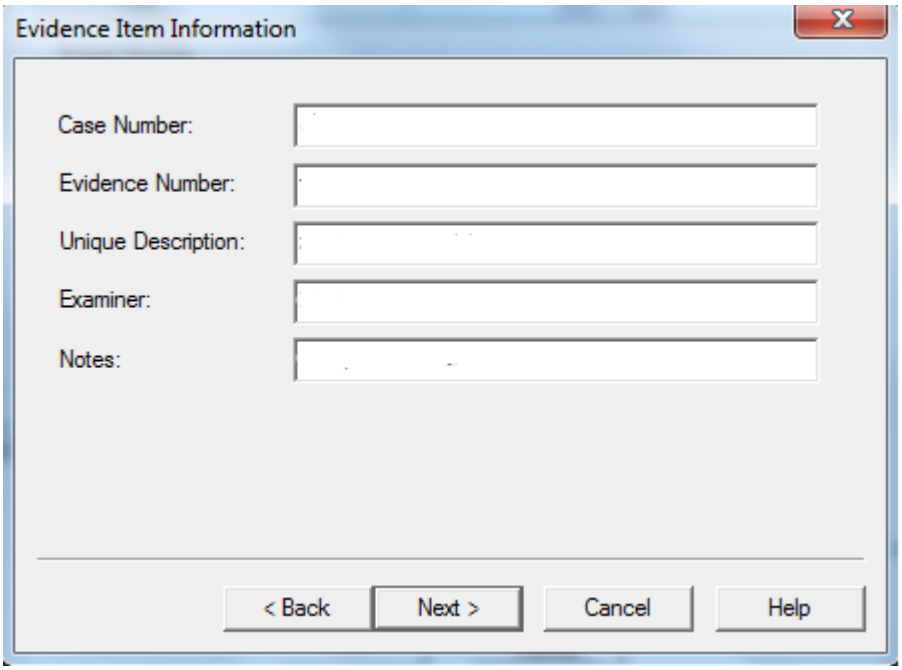
d) Selanjutnya akan diminta untuk menentukan *image destination* atau dimana disk *image* nya akan disimpan, klik *add* sehingga kemudian akan tampil halaman *select image type*, dan klik *next* untuk melanjutkan, untuk lebih jelasna dapat dilihat pada gambar 4.4 *Select Image Type*. Ada beberapa tipe *image* diantaranya :

a. *Raw (dd)*, merupakan data mentah atau yang belum diolah sama sekali.
b. *SMART*
c. *E01*
d. *AFF*



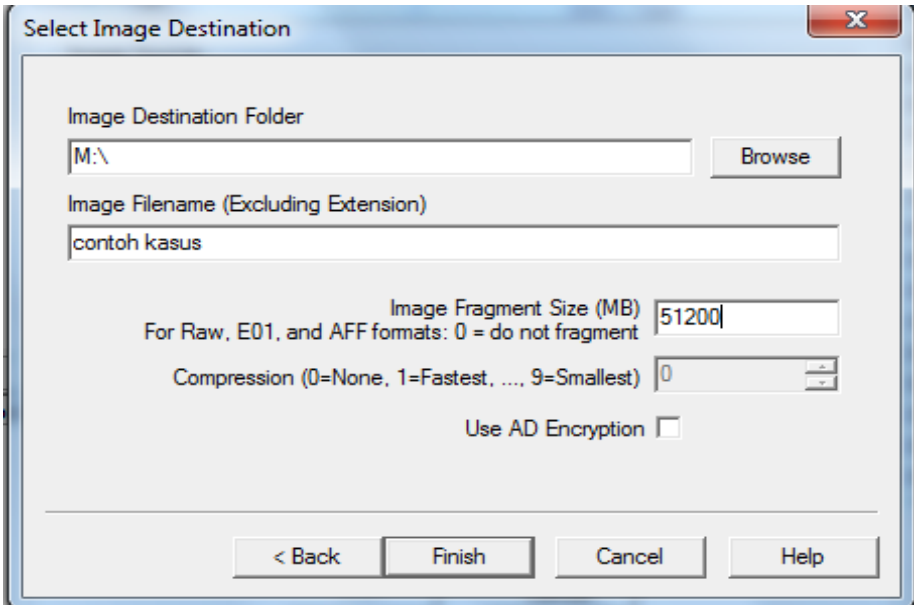
Gambar 4.4 *Select Image Type*

e) Selanjutnya akan diminta untuk mengisi informasi barang bukti, halaman ini digunakan untuk membuat nama file serta informasi mengenai *barang bukti* yang akan dibuat. Klik *next* untuk melanjutkan. Hal ini digambarkan pada gambar 4.5 berikut ini.



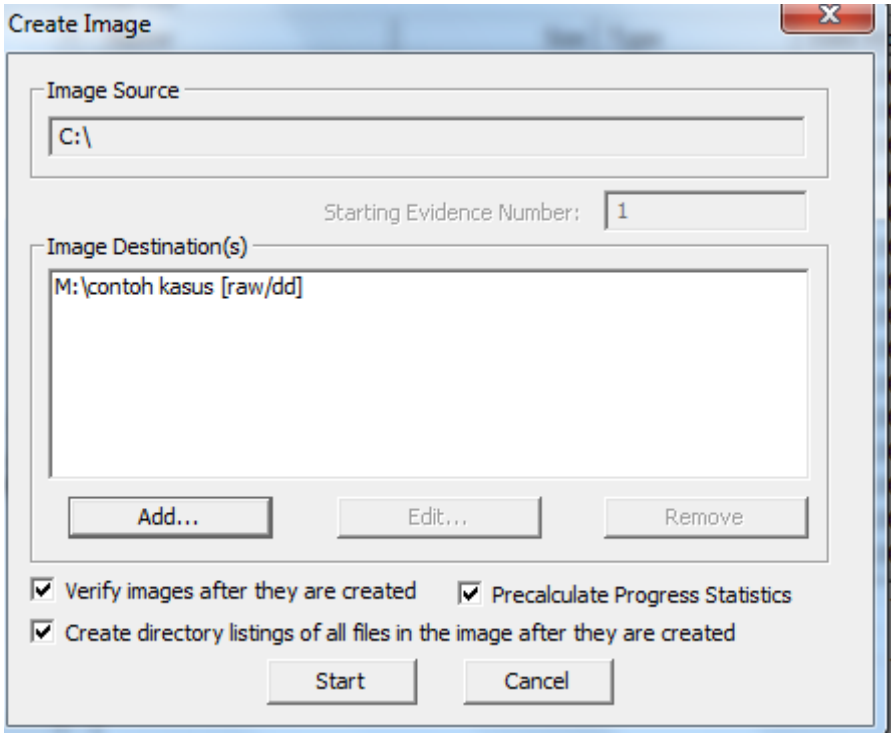
Gambar 4.5 *Evidence Item Information*

f) Selanjutnya akan diminta untuk menentukan dimana *image* akan disimpan, nama file *image* dan *image fragment size* atau ukuran drive yang akan di *image*. Seperti yang terlihat pada gambar 4.6 dibawah ini. Klik *finish* untuk mengakhiri.



Gambar 4.6 *Select Image Destination*

g) Setelah penambahan *image destination* selesai maka akan tampil halaman *Create Image* seperti pada gambar 4.7 berikut ini. Klik *Start* untuk memulai proses *imaging* data dan *cancel* untuk membatalkan.



Gambar 4.7 *Create Image*

4.2 Pengecekan dan Analisis Data

Setelah melalui tahapan imaging selanjutnya barang bukti yang telah dibuat image nya akan dianalisis.

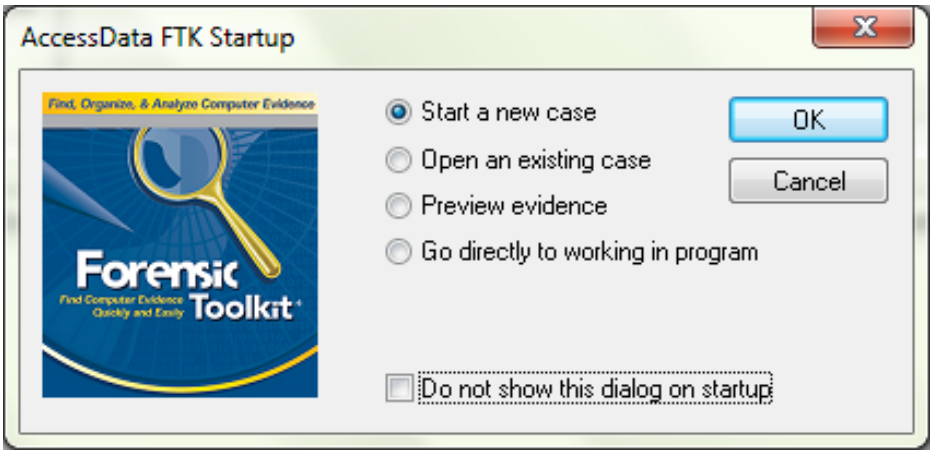
4.2.1 Pembuatan Kasus

Setelah pembuatan *image*, maka tahap selanjutnya adalah menganalisis *image* dengan menggunakan *Forensic Toolkit.* Dalam kasus ini, *Forensic Toolkit* berperan untuk menemukan bukti yang mencakup dokumen, email dan bagan-bagan dari file sistem. Ketika membuka program sebagai *administrator* (klik kanan dan pilih *Run as Administrator*), maka akan muncul beberapa opsi diantaranya :

a. *Start new case*, digunakan untuk membuat *case* baru dari *image* file yang ada.

b. *Open an existing case*, digunakan untuk membuka kasus yang telah dibuat sebelumnya.

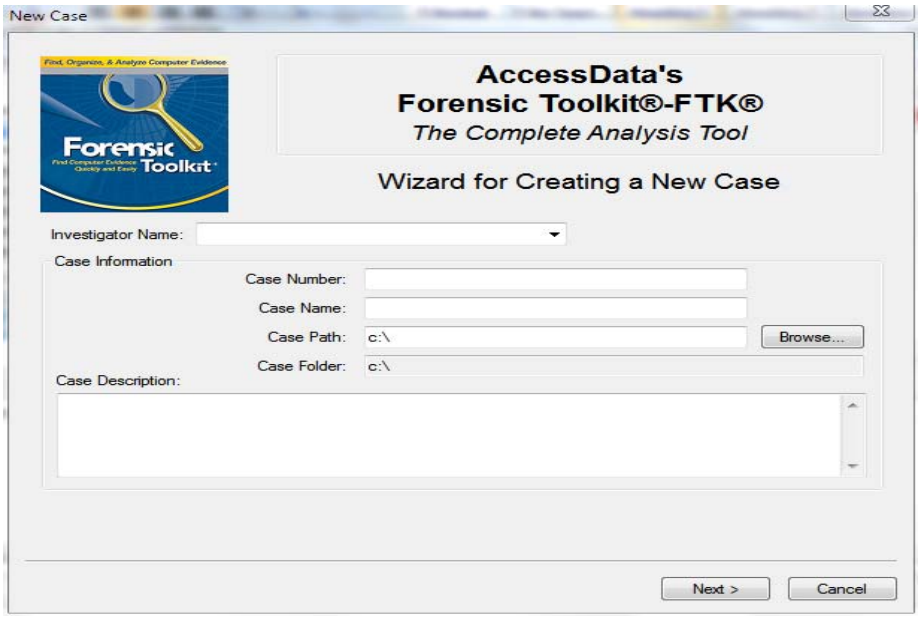
c. *Preview barang bukti*, digunakan untuk melihat *barang bukti* yang telah dibuat.



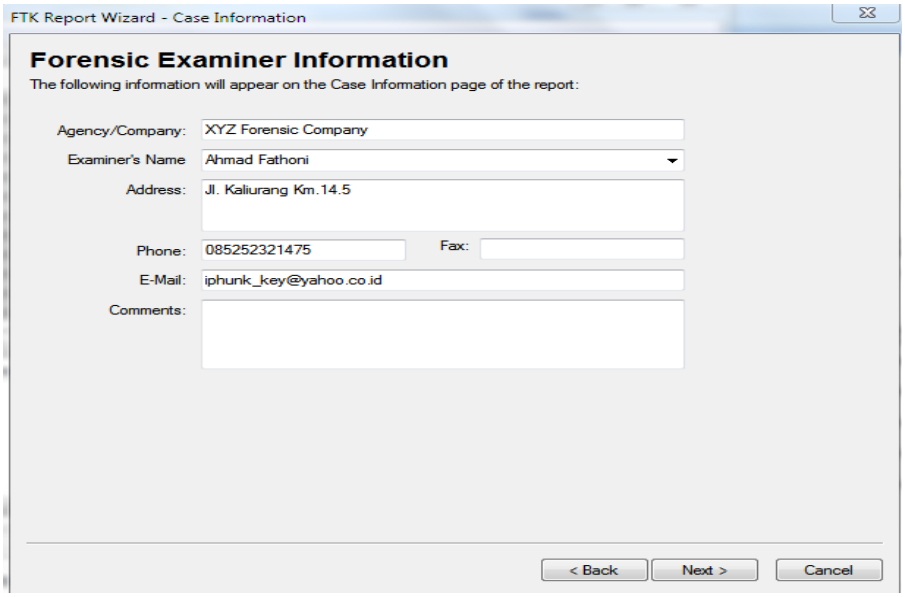
Gambar 4.8 FTK startup

Di sini akan dipilih *Start new case* untuk dapat membuat kasus baru dari *image* yang telah dibuat.

a. Ketika akan membuat *case* baru, maka akan tampil halaman *new case*, pada halaman ini akan diminta untuk mengisi informasi yang berkaitan dengan kasus ini, misal nama penyidik, nama kasus yang akan diselidiki, atribut-atribut lainnya mengenai kasus serta menentukan tempat yang akan menjadi folder penyimpanan kasus dan segala aktivitas yang berkaitan dengan penyidikan. Proses pembuatan case baru terlihat pada gambar 4.8 berikut ini. Untuk informasi dalam penulisan laporan penyidikan FTK juga menyediakan form mengenai informasi penyidik, form informasi penyidik dapat dilihat pada gambar 4.10.

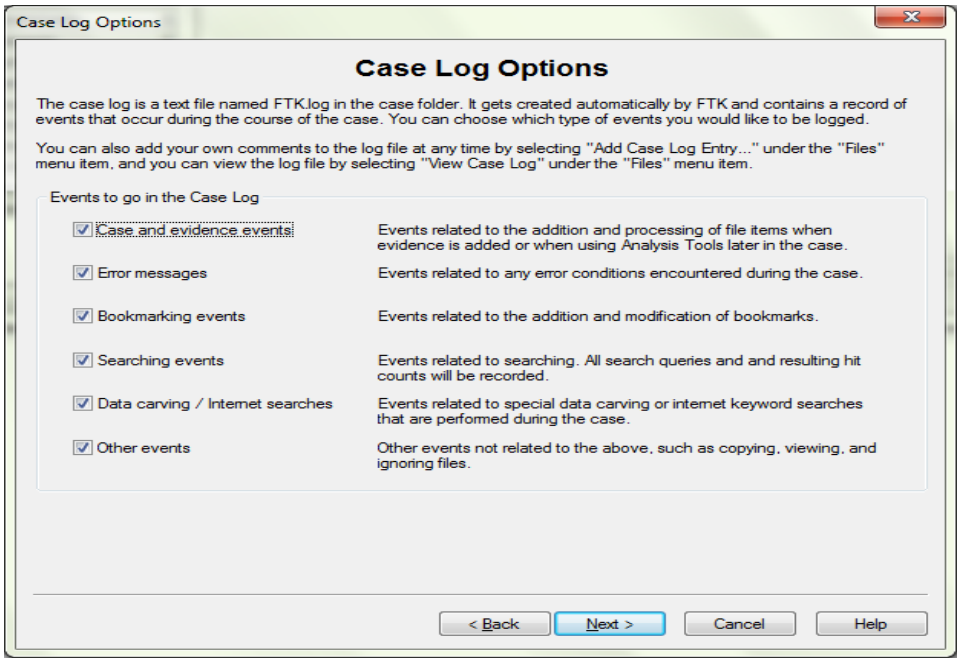


Gambar 4.9 *Form New Case*



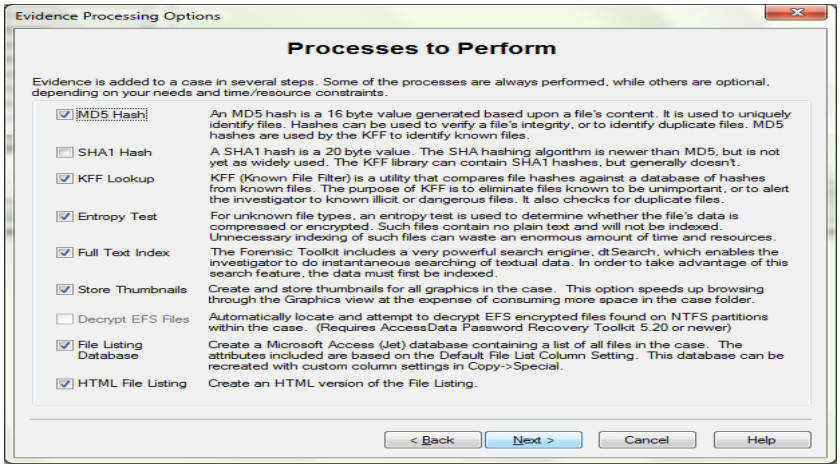
Gambar 4.10 *Form FTK Examiner Information*

b. Selama masa penyidikan yang menggunakan FTK, FTK akan membuat file bernama *ftk.log* yang akan mencatat aktivitas pada *case*. Dari log ini bisa menentukan *event* apa saja yang akan dicatat dengan member tanda *check* pada opsi yang sudah tertera seperti Gambar 4.11.



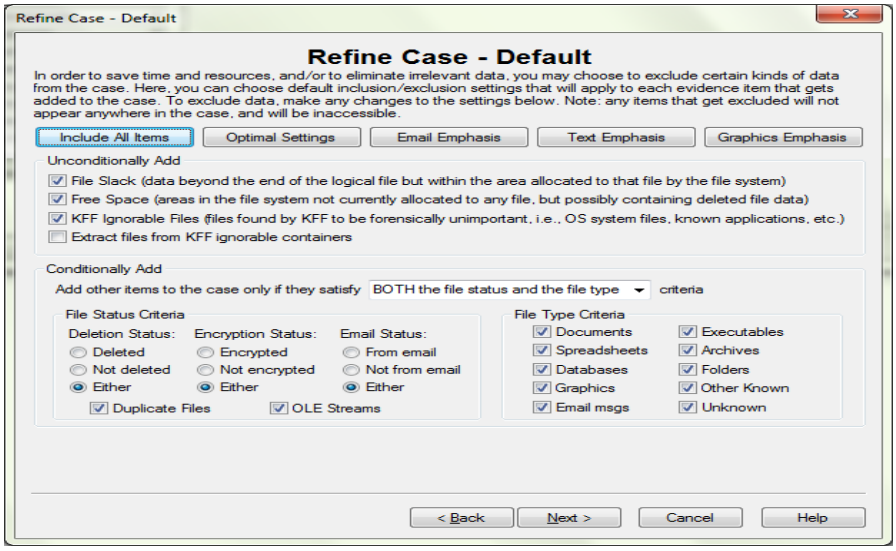
Gambar 4.11 *Case Log Option*

c. Selanjutnya akan menentukan *option* untuk pemrosesan *barang bukti*, pilihlah proses yang relevan dengan *barang bukti* yang akan ditambah ke *case*. Contoh : jika *case* terutama memuat gambar maka tidak perlu melakukan index pada *barang bukti*, sedangkan bila kasus tidak memuat gambar maka tidak perlu menyimpan *thumbnail*. Seperti yang terdapat pada gambar 4.12.



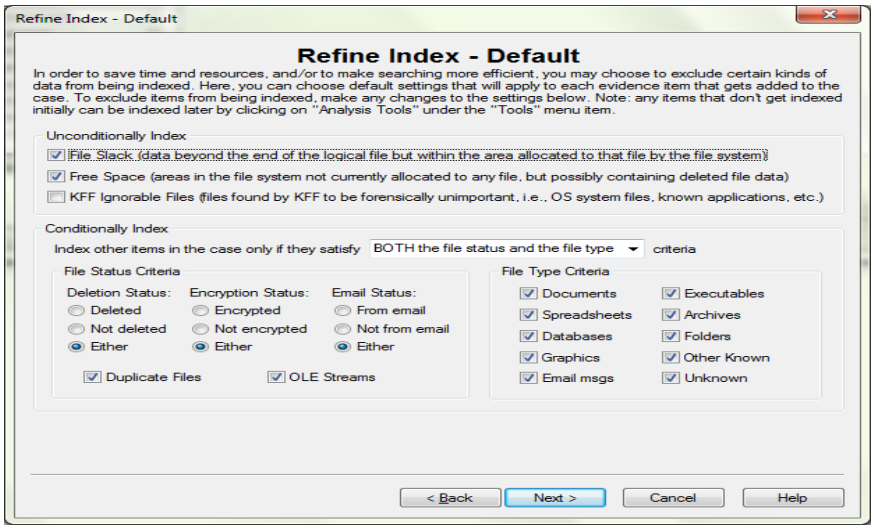
Gambar 4.12 *Evidence Processing Option*

d. *Refine case* memungkinkan untuk meng*eliminate* sejumlah data yang tidak terkait dari *case*. Tujuannya untuk menghemat waktu dan sumber data, *Refine case* dapat dilihat pada gambar 4.13.



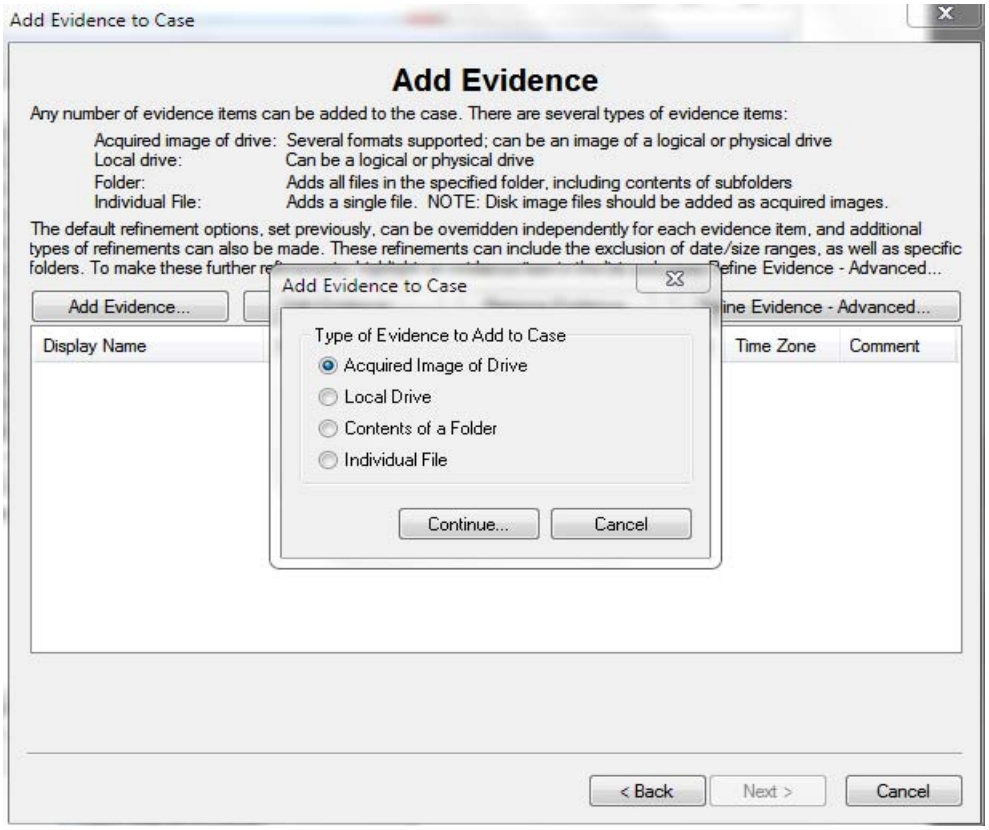
Gambar 4.13 *Refine Case*

e. *refine index* membantu menentukan tipe data yang tidak ingin diindeks. Index file dibuat setelah pembuatan suatu *case*, tetapi pembuatan suatu bagian dari barang bukti bisa diindex kapan saja. Seperti yang terlihat pada gambar 4.14.



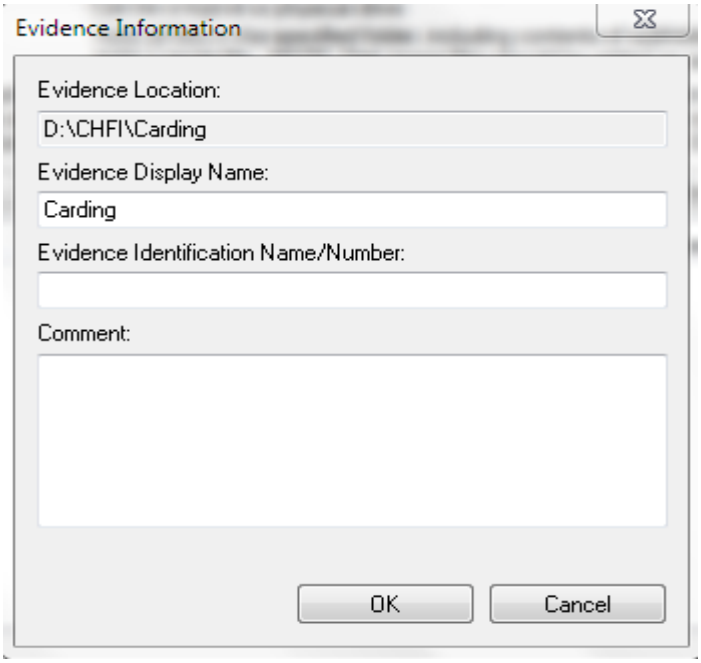
Gambar 4.14 *Refine Index*

f. Selanjutnya akan ditampilkan window *Add Evidence.* Pada halaman ini dapat menambah, mengurangi, mengelola informasi, serta parameter dari barang bukti. Adapun barang bukti yang dimaksud adalah barang bukti yang berhubungan dengan kasus (*case*). Klik tombol *Add Evidence* untuk menambahkan barang bukti.



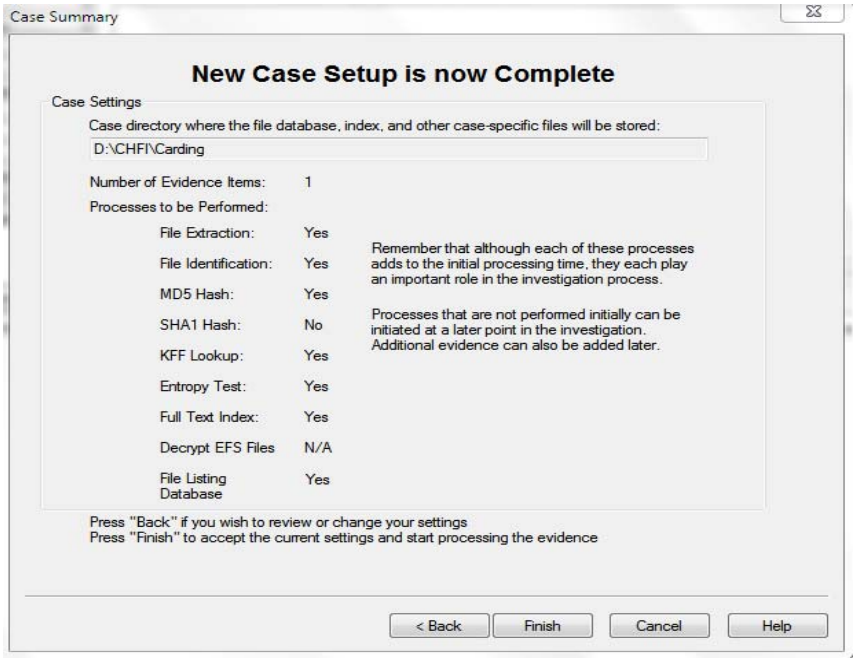
Gambar 4.15 *Add Evidence*

g. Selanjutnya dapat memilih file *image* yang ingin dicek atau diuji. kemudian perlu ditambahkan informasi mengenai *barang bukti* tersebut, seperti *evidence display name*, *evidence identification name/number serta comment*. Untuk lebih jelasnya dapat melihat gambar 4.16.



Gambar 4.16 *Evidence Information*

h. FTK akan memulai melakukan pengumpulan data dari file *image* agar selanjutnya bisa dibaca atau diuji. Seperti yang terdapat pada gambar 4.17 mengenai *case summary.*

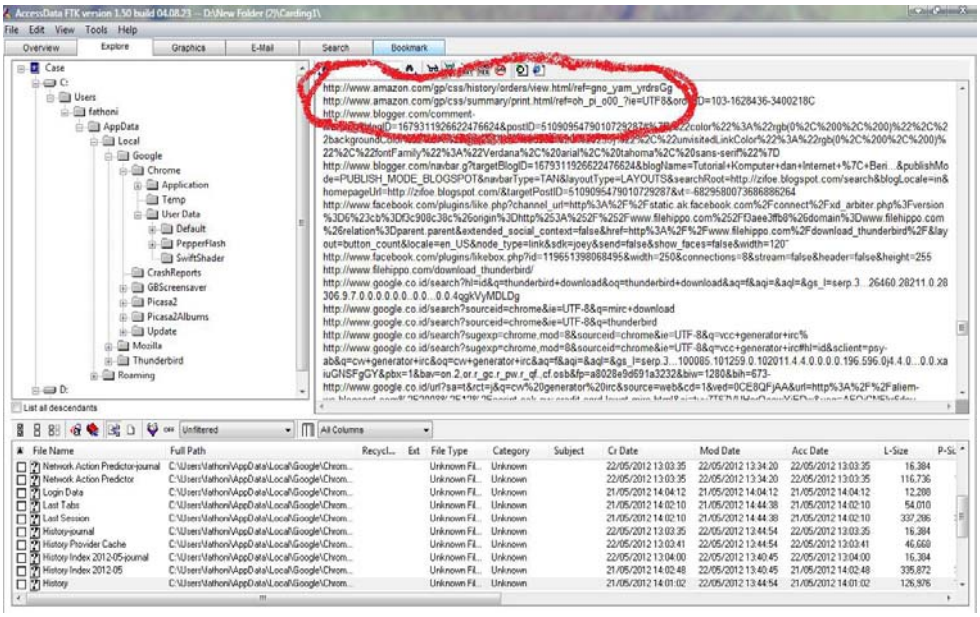


Gambar 4.17 *Case Summary*

4.2.2 Pengecekan dan Analisis Kasus

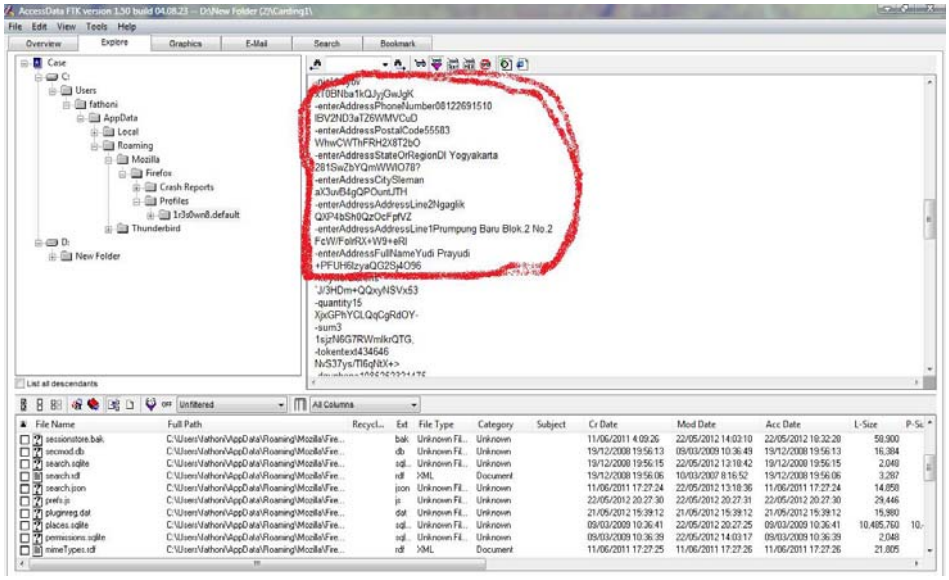
Setelah pembuatan kasus berhasil dilakukan selanjutnya akan dilakukan analisis forensik terhadap data-data yang telah di *ekstract.* Dengan analisis tersebut diharapkan dapat menemukan file-file yang berkaitan dengan kasus. Untuk menemukan barang bukti dari kasus yang sedang diselidiki seorang penyidik haruslah memahami konsep bukti yang dicari serta jenis dan tipe dari kejahatan yang sedang diselidiki. Untuk skenario kasus yang dibuat pada penelitian ini penyidikan berfokus untuk mencari barang bukti yang terkait berupa *Document, Email, Deleted Files, Data base, Other Thumbnail, Folder, Log History*, Log jaringan serta aplikasi yang mungkin digunakan oleh pelaku.

a. Pada tahapan ini akan dimulai dari pencarian berupa log history pada web browser yang dilakukan oleh pelaku menggunakan komputernya. Log history web browser dapat ditemukan pada drive tertentu tempat instalasi aplikasi tersebut. Web browser yang sering digunakan antara lain google chrome dan mozilla firefox, pada chrome log history, cache dan bookmark dapat ditemukan pada bagian direktori C:\Users\fathoni\AppData\Local\Google\Chrome\User Data\Default. Sedangkan pada mozilla firefox data-data yang berisi log history, bookmark dan cache dapat ditemukan pada direktori C:\Users\fathoni\AppData\Roaming\Mozilla\Firefox\Profiles\1r3s0wn8.default. seperti yang terlihat pada gambar di 4.18.



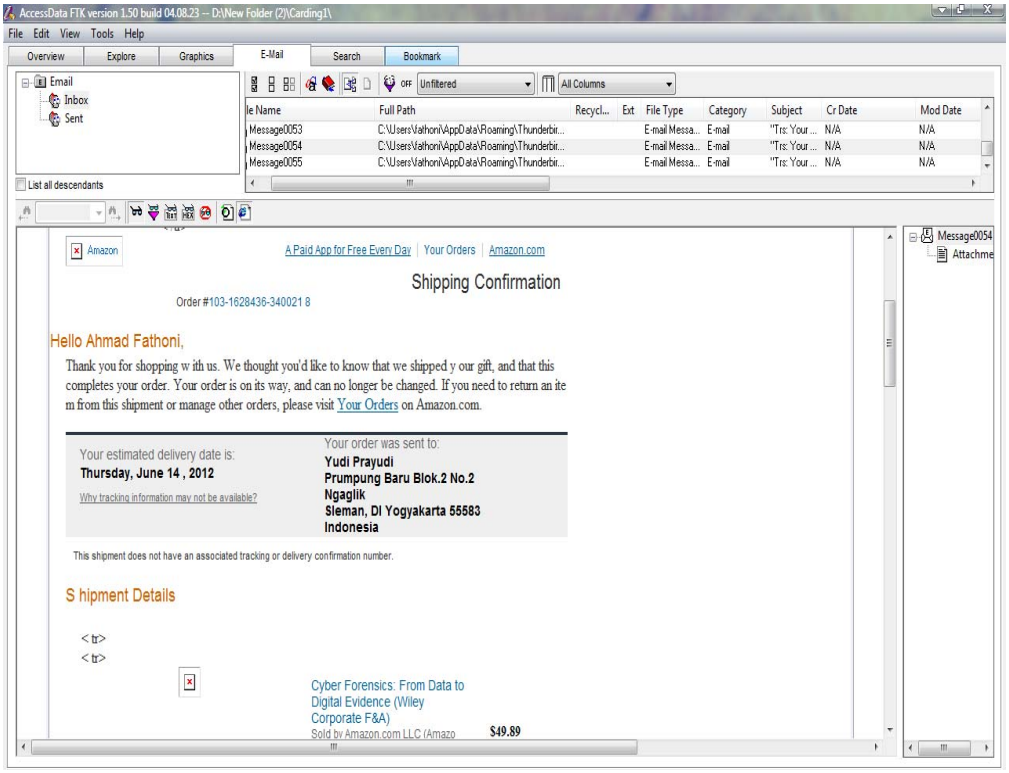
Gambar 4.18 Tampilan History pada Web Browser

b. Dari Temuan sebelumnya yang berupa History dari web browser selanjutnya akan dilakukan pencarian informasi dari web browser tersebut. Pada kasus ini ditemukan beberapa inputan yang dilakukan oleh pelaku berupa session web browser yang terdapat pada direktori C:\Users\fathoni\AppData\Roaming\Mozilla\Firefox\Profiles\Ir3s0wn8.default\Sessionstore.bak. hasil temuan dapat dilihat pada gambar 4.19.

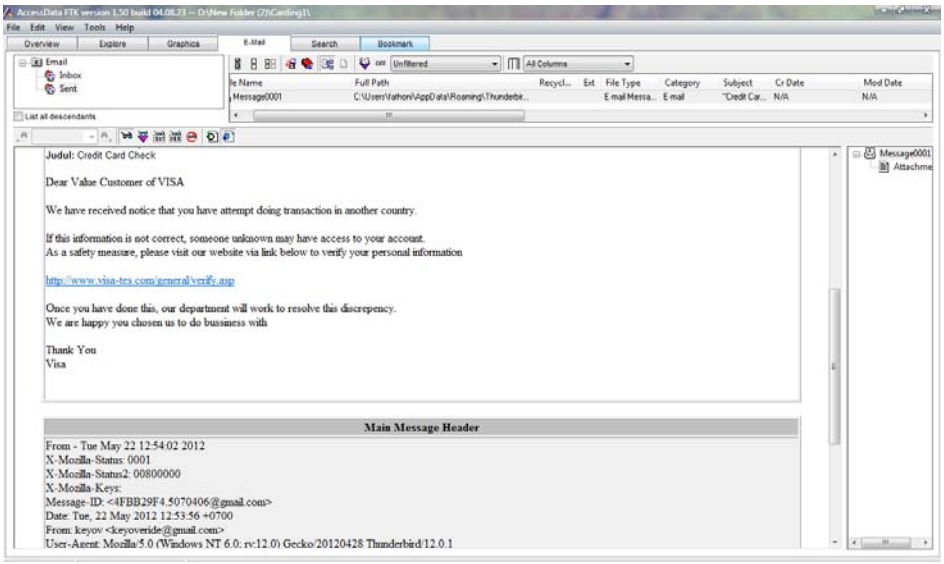


Gambar 4.19 Tampilan *Session*

c. Setelah mendapatkan data-data dan informasi dari web browser pelaku, selanjutnya akan diselidiki bagian yang memuat informasi berupa E-mail. Untuk melakukan pencarian berupa E-mail agar lebih mudah dapat dilakukan pencarian menggunakan tab E-mail. Pada tab *E-mail* dapat menemukan semua pesan masuk maupun keluar. Dari sini penyidik dapat melihat siapa pengirim email, siapa yang menerima email, kapan email tersebut dikirim serta header lengkap dari email tersebut. Pada kasus ini ditemukan bukti berupa email invoice hasil transaksi pelaku dan email yang digunakan pelaku untuk mendapatkan kartu kredit berupa email phising. Seperti yang terlihat pada gambar 4.20 dan gambar 4.21.

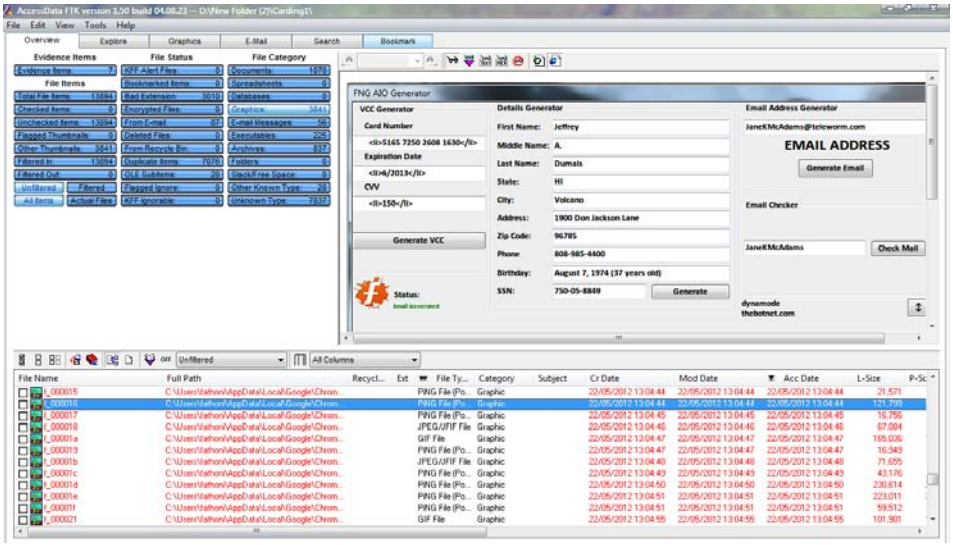


Gambar 4.20 Tampilan *E-mail* Masuk berupa Invoice



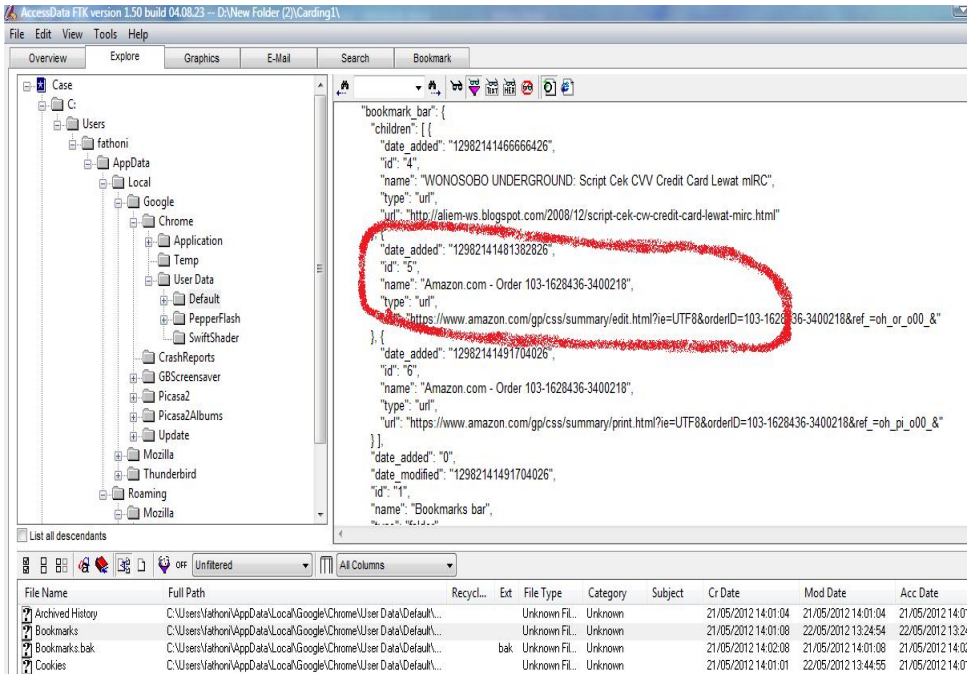
Gambar 4.21 Tampilan *E-mail* Keluar berupa *Phising Mail*

d. Selanjutnya penyidik dapat melakukan pencarian informasi berupa gambar. Untuk memudahkan pencarian maka terdapat tombol *Graphic* dan *Other Thumbnail*. Pada tombol tersebut penyidik dapat menemukan file-file yang telah disortir berupa image yang berekstensi jpeg, gif, png dan sebagainya. Pada kasus ini ditemukan screen shot hasil generate cvv yang dilakukan oleh pelaku menggunakan aplikasi *FNG AIO Geerator*. Seperti yang terlihat pada gambar 4.22



Gambar 4.22 Tampilan *Graphics* dan *Thumbnail*

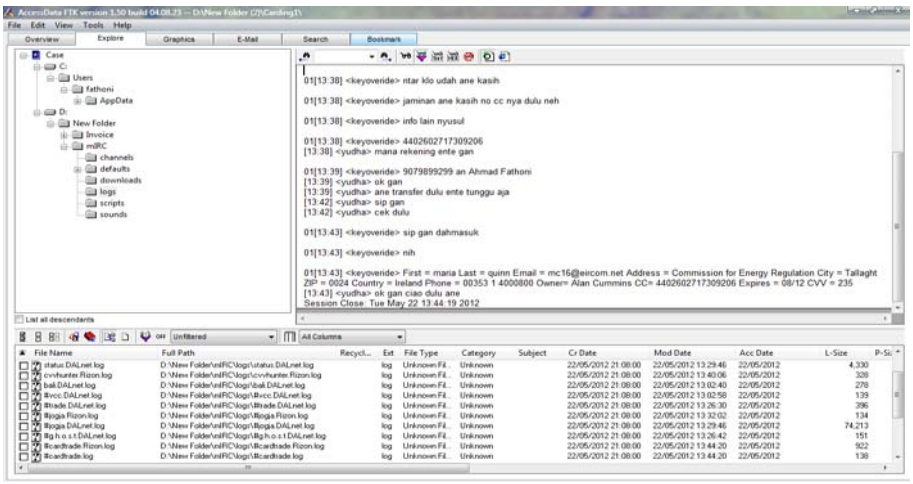
e. Untuk menemukan file-file lain yang sulit dilihat di halaman *Overview* penyidik dapat mencoba untuk mencarinya pada tab explore. Pada halaman ini penyidik dapat melihat direktori pada barang bukti. Untuk mencari dokumen-dokumen terkait seperti history, bookmark, cookies dan sebagainya dapat dilakukan dengan mudah dengan cara mengakses direktori Web Browser yang digunakan pelaku. Dari sana dapat ditemukan situs apa saja yang pernah dikunjungi dan yang di *bookmark* oleh pelaku. Dari situ dapat dicari hal-hal terkait kasus misal, halaman situs jual beli online yang diakses pelaku untuk menggunakan kartu kredit yang ia punya. Atau situs phising yang digunakan pelaku untuk mendapatkan informasi kartu kredit, serta dokumen yang tersimpan pada direktori pridadi pelaku. Tab Explore dapat dilihat pada gambar 4.23.



Gambar 4.23 Tampilan Explore *Bookmark*

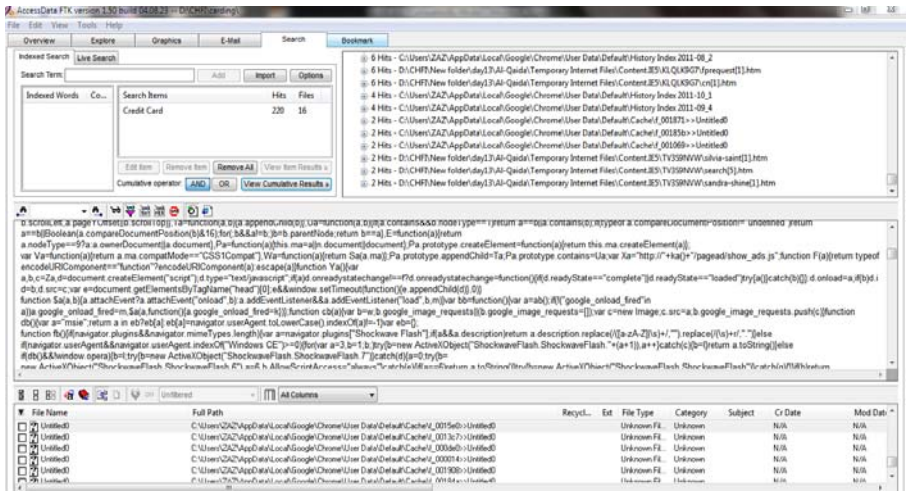
f. Untuk menemukan informasi berupa log percakapan yang dilakukan menggunakan IRC penyidik dapat melakukan pencarian pada direktori tempat instalasi aplikasi yang digunakan untuk melakukan *Relay*

Chatting seperti aplikasi mIRC. Pada kasus ini ditemukan hasil percakapan pelaku berupa transaksi jual beli kartu kredit dan hasil generate CVV menggunakan mIRC. Hasil temuan terdapat pada direktori D:\New Folder\mIRC\log. Seperti yang terlihat pada gambar 4.24.



Gambar 4.24 Log IRC

g. Jika telah memiliki gambaran apa saja yang ingin dicari penyidik dapat menggunakan tab search untuk menyeleksi file-file yang dibutuhkan. Pada halaman ini penyidik akan memasukkan beberapa kata kunci yang diinginkan dan terdapat indikator or atau and. Tab search dapat dilihat pada gambar 4.25



Gambar 4.25 Gambar *Tab Search*

4.3 Laporan Hasil Forensik

Setelah melakukan analisis dan pengecekan pada barang bukti yang telah ditemukan dan telah didapatkan hasil maka penyidik harus membuat laporan untuk kepentingan penyidikan di pengadilan. Laporan berisi rangkuman dari hasil investigasi, menyebutkan barang bukti secara spesifik dan pembuktiannya, dan kesimpulan yang jelas dan tidak bersifat ambigu. Adapun laporan dari analisis kasus yang dibuat yaitu :

REPORT OF MEDIA ANALYSIS

MEMORANDUM FOR	**:**	Kepala Polisi Investigator Fathoni Jakal Street
SUBJECT	**:**	XYZ Forensics Analysis Report SUBJECT : Lukman Case Number : 001

1. Status : Closed

2. Summary of Finding :

- Ditemukan 1 file *spreadsheet* berisi daftar kartu kredit dan status jual beli.
- Ditemukan aplikasi card extrapolator.
- Ditemukan e-mail transaksi jual beli kartu kredit.
- Ditemukan ScreenShot Invoice yang diduga merupakan hasil dari transaksi pembelian online menggunakan kartu kredit.
- Ditemukan history dan bookmark situs phising yang digunakan untuk mendapatkan informasi kartu kredit.
- Ditemukan Log IRC berupa percakapan transaksi dan generate cvv.

3. Item Analyzed :

TAG NUMBER	**ITEM DESCRIPTION**
012345	Sebuah Laptop

4. Details of Findings :

- Temuan yang ada pada paragrap ini terkait Hard Drive, Model ABCD, Serial #1234, ditemukan dari Tag Number #012345, Sebuah Laptop.
- Pemeriksaan pada hard drive ditemukan menggunakan Sistem Operasi Microsoft Windows Vista.
- Direktori D:\New Folder\Invoice ditemukan Invoice transaksi.
- Direktori D:\Dokumen\Daftar\ ditemukan sebuah file spreadsheet yang berisi list informasi kartu kredit. File dibuat : 5 November 2011 antara pukul 11.33 p.m dan 11.45 p.m. dan last access terhadap file : 30 Maret 2012.
- Direktori D:\Dokumen\App\ ditemukan aplikasi card extrapolator berupa : cardpro versi 2.0.3 , cardwizard 2.2.1.
- Direktori D:\New Folder\mIRC\log ditemukan log transaksi jual beli yang dilakukan oleh pelaku melalui IRC.
- DirektoriC:\Users\fathoni\AppData\Roaming\Mozilla\Firefox\Profiles\Ir3s0wn8.default\Sessionstore.bak ditemukan history berupa session dari aktivitas transaksi pelaku.
- Ditemukan e-mail transaksi dan phising pada ThunderBird pada direktori . C:\Users\fathoni\AppData\Roaming\ThunderBirds\

5. Glossary

Card Extrapolator : Aplikasi untuk mengenerate CVV kartu kredit.

6. Item Provided:

Sebagai lampiran dari laporan hardcopy, satu buah DVD yang menyampaikan laporan ini dalam bentuk softcopy. Laporan dalam DVD berisi hyperlink dari file dan direktori yang disebutkan di atas.

4.4 Presentasi

Presentasi hasil dari analisis kasus dilakukan di pengadilan dan di depan kepolisian. Presentasi yang pertama kali dilakukan adalah presentasi di depan kepolisian. presentasi di depan kepolisian berisi temuan-temuan dari analisis dan informasi tentang teknik yang digunakan oleh pelaku dalam melakukan kejahatannya. Sedangkan presentasi yang dilakukan di depan pengadilan berisi

temuan-temuan yang bias dijadikan bukti yang sah dan informasi-informasi yang besifat umum yang dapat dengan mudah ditangkap oleh orang secara umum.

4.4.1 Presentasi Kepolisian

Pada kasus yang telah dibuat akan dipresentasikan teknik dan temuan apa saja yang telah didapatkan selama proses investigasi. Adapun bentuk presentasinya berupa :

Kasus : Carding
Pelaku **:** Lukman
Kejadian : Yogyakarta
Barang Bukti :

- Flashdisk
- Modem
- Sebuah Laptop :
  - OS : Windows Vista
  - File system : FAT 32
  - Hard Drive : 120 Gb

Teknik :

- Pelaku melakukan aktivitas penipuan untuk mendapatkan kartu kredit melalui IRC
- Pelaku juga melakukan aktivitas phising dengan berpura-pura sebagai perusahaan kartu kredit tersebut.
- Dari kartu kredit yang telah didapat pelaku mengenerate CVV dengan menggunakan cardwizard dan cardpro.
- CVV degenerate dengan menggunakan mIRC, cardwizard dan cardpro yang menggunakan MOD 10 Algorithm atau Luhn Algorithm.
- Kartu kredit digunakan pelaku untuk melakukan belanja secara online.

- Kartu kredit yang didapat diperjual belikan oleh pelaku.

Temuan :

- Ditemukan daftar kartu kredit yang dikumpulkan pelaku pada komputer yang menjadi barang bukti.
- Ditemukan aplikasi card extrapolator berupa : master4, cardpro, cardwizard.
- Ditemukan screenshot berupa invoice hasil transaksi.
- Ditemukan e-mail transaksi dan phising.
- Ditemukan history dan bookmark berupa situs phising dan situ belanja online.

4.4.2 Presentasi Pengadilan

Pada bagian presentasi ini akan dilakukan pemberian informasi secara umum mengenai barang-barang bukti yang telah ditemukan beserta temuan-temuannya. Adapun bentuk presentasinya berupa laporan dari examiner :

Kasus : Carding

Pelaku : Lukman

Kejadian : Yogyakarta

Waktu : Maret 2012

Temuan :

- Pemeriksaan pada hard drive ditemukan menggunakan Sistem Operasi Microsoft Windows Vista.
- Direktori D:\New Folder\Invoice ditemukan Invoice transaksi.
- Direktori D:\Dokumen\Daftar\ ditemukan sebuah file spreadsheet yang berisi list informasi kartu kredit. File dibuat : 5 November 2011 antara pukul 11.33 p.m dan 11.45 p.m. dan last access terhadap file : 30 Maret 2012.
- Direktori D:\Dokumen\App\ ditemukan aplikasi card extrapolator berupa : cardpro versi 2.0.3 , cardwizard 2.2.1.

- Direktori D:\New Folder\mIRC\log ditemukan log transaksi jual beli yang dilakukan oleh pelaku melalui IRC.
- DirektoriC:\Users\fathoni\AppData\Roaming\Mozilla\Firefox\Profiles\Ir3s0wn8.default\Sessionstore.bak ditemukan history berupa session dari aktivitas transaksi pelaku.
- Ditemukan e-mail transaksi dan phising pada ThunderBird pada direktori . C:\Users\fathoni\AppData\Roaming\ThunderBirds\
- Ditemukan modem yang digunakan pelaku untuk terhubung ke jaringan Internet.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah melakukan implementasi dan pengujian, dapat diambil kesimpulan:

a. Untuk dapat menganalisis suatu barang bukti, seorang penyidik bukti digital harus paham akan konsep bukti itu sendiri, sistem operasi yang akan dicek serta paham akan konsep jaringan dan serangan.
b. Dalam penelitian ini barang bukti yang ditemukan dibagi menjadi dua yaitu, barang bukti utama berupa laptop dan flashdisk serta barang bukti tambahan berupa modem.
c. Dalam skenario kasus ini *carding* dilakukan dengan cara *phising* dan melakukan *generate* kartu kredit. Sehingga dalam pembuktiannya kita harus fokus untuk mencari bukti berupa tools dan *phising mail.*
d. Barang bukti *carding* yang ditemukan dalam penelitian ini berupa *phising email*, *invoice* transaksi kartu kredit, percakapan IRC, log history, bookmark, aplikasi terkait, dan sebagainya.
e. Untuk pencarian barang bukti *carding,* pada awalnya dapat difokuskan pencarian log aktivitas pada *web browser*.
f. Pencarian barang bukti *carding* berupa email dapat dengan mudah dilakukan jika pelaku menggunakan fasilitas mail client pada komputernya. Jika pelaku tidak menggunakan mail client, email dapat ditemukan pada tempat penyimapanan sementara (*temporary file)* pada web browser.
g. Dengan menggunakan FTK akan menampilkan hampir seluruh data sehingga akan lebih mempermudah pencarian terhadap data yang telah dimanipulasi serta yang telah dihapus.
h. Analisis dalam kasus ini dapat mengalami kesulitan jika pelaku melakukan penghapusan log dari setiap aktivitasnya. Jika log telah terhapus kita dapat

mengembalikannya dengan cara mengambil kembali data yang telah terhapus menggunakan tools tertentu.

i. Laporan hasil pembuktian kasus harus dapat mudah dipahami oleh masyarakat umum.
j. Presentasi laporan kasus yang dilakukan ke pihak kepolisian berupa teknik yang dilakukan pelaku disertai temuan barang buktinya, sedangkan presentasi ke pihak pengadilan berupa seluruh hasil temuan yang dijadikan barang bukti sehingga pelaku dapat dijadikan terdakwa dalam kasus tersebut.

5.2 Saran

Dari hasil pengujian dan implementasi yang telah dilakukan terdapat beberapa saran yang perlu disampaikan :

a. Ketika akan menyelidiki sebuah kasus alangkah lebih baiknya jika penyidik memahami segala kemungkinan teknik yang digunakan oleh pelaku sehingga memudahkan dalam penyidikan.
b. Laporan harus dibuat dengan bahasa yang mudah dipahami dan isinya harus jelas.

DAFTAR PUSTAKA

Dougherty, J. J. (2011). Interested in learning more Institu Authrensfrig. *Style (DeKalb, IL)*, (Security 401).

EC-Council, C. (2010). Module I - Computer Forensics in Today's World Scenario. *Reproduction*.

EC-Council, C. (2010). Module 2 - Computer Forensics Investigation Process Scenario. *Reproduction*.

Casey, Eoghan, (2010). Handbook of Digital Forensic and Investigation. Elsevier Academic Press

Fajar. (2010). Cybercrime Tugas Besar Dunia TI Indonesia. Retrieved from Http://yogyacarding.tvheaven.com

Haase, N. (2001). InfoSec Reading Room Computer Forensics : Introduction to Incident tu , A ho ll r igh ts. *Information Security*.

Internet, T., World, O., Into, H., & Life, Y. (2006). Identity Theft : Evolving with Technology.

Prayudi, Y., & Afrianto, D. S. (2007). Antisipasi Cybercrime Menggunakan Teknik Komputer Forensik. *Seminar*, *2007*(Snati).

Rozita. (2011). Analisis Komputer Forensik Menggunakan FTK.

Utdirartatmo, F. (2001). Tinjauan Analisis Forensik Dan Kontribusinya Pada Keamanan Sistem Komputer.

Weise, J., & Powell, B. (2005). Using Computer Forensics When Investigating System Attacks. C*omputer*, (819).