ANALISIS *COMPUTER FORENSIC* MENGGUNAKAN FTK *(Forensic ToolKit)*

TUGAS AKHIR

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

Oleh :

Nama : ROZITA

NIM : 06 523 054

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA

2011

HALAMAN JUDUL

ANALISIS *COMPUTER FORENSIC* MENGGUNAKAN FTK *(Forensic ToolKit)*

TUGAS AKHIR

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

Oleh :

Nama : ROZITA

NIM : 06 523 054

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA

2011

LEMBAR PENGESAHAN PEMBIMBING

ANALISIS *COMPUTER FORENSIC* MENGGUNAKAN FTK *(Forensic ToolKit)*

TUGAS AKHIR

Oleh :

Nama : ROZITA

NIM : 06 523 054

Yogyakarta, 13 Mei 2011

Pembimbing

(Yudi Prayudi, S.Si, M.Kom)

LEMBAR PENGESAHAN PEMBIMBING

ANALISIS KOMPUTER FORENSIK MENGGUNAKAN
FTK (Forensic ToolKit)

TUGAS AKHIR

Oleh :

Nama : ROZITA
NIM : 06 523 054

Yogyakarta, 13 Mei 2011

Pembimbing

(Yudi Prayudi, S.Si, M.kom)

LEMBAR PENGESAHAN PENGUJI

ANALISIS *COMPUTER FORENSIC* MENGGUNAKAN
FTK (*Forensic ToolKit*)

TUGAS AKHIR

oleh:

Nama : Rozita
No Mahasiswa : 06 523 054

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika
Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 26 Mei 2011

Tim Penguji

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

Syarif Hidayat, S.Kom., M.I.T _____
Anggota I

Hendrik, ST., M.Eng _____
Anggota II

Mengetahui,
Ketua Jurusan Teknik Informatika
Universitas Islam Indonesia

(Yudi Prayudi, S.Si., M.Kom.)

LEMBAR PENGESAHAN PENGUJI

ANALISIS *COMPUTER FORENSIC* MENGGUNAKAN FTK (*Forensic ToolKit*)

TUGAS AKHIR

oleh:

Nama : Rozita

No Mahasiswa : 06 523 054

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 26 Mei 2011

Tim Penguji

Yudi Prayudi, S.Si, M.Kom
Ketua

Syarif Hidayat, S.Kom., M.I.T
Anggota I

Hendrik, ST., M.Eng
Anggota II

Mengetahui,
Ketua Jurusan Teknik Informatika
Universitas Islam Indonesia

(Yudi Prayudi, S.Si., M.Kom.)

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Saya yang bertandatangan dibawah ini,

Nama : Rozita

NIM : 06 523 054

Tugas Akhir dengan Judul :

ANALISIS *COMPUTER FORENSIC* MENGGUNAKAN FTK *(Forensik ToolKit)*

Menyatakan bahwa seluruh komponen dan isi dalam Laporan Tugas Akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini bukan merupakan hasil karya saya sendiri, maka saya siap menanggung resiko dan konsekuen apapun.

Demikian pernyataan ini saya buat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, Mei 2011

(Rozita)

HALAMAN PERSEMBAHAN

Tugas akhir ini ku persembahkan untuk :

1. ***Mak abah***, *yang selalu memberikan dukungan baik secara moral maupun materi, yang tak pernah putus doa untuk Putra - putrinya, terima kasih mak, abah.....I love U.*
2. ***Ulong Q*** *yang selalu cerewet menanyakan kapan lulus, walau demikian itu menjadikan motivasi bagi Q, makasih ya long..* ☺
3. ***Ongah Q , b joko*** *n Kedua jagoan kami (* ***FIFA*** *), makasih juga untuk dukungan nya, walau raga berjauhan namun dihati tetap dekat selalu.*
4. *Untuk adek – adek Q tercinta (* ***Yati, b uber, b oyok n dek kiah*** *) makasih juga untuk motivasinya, terutama buat dek yati yang selalu bertanya " apa kabar skripsi udo " makasih ya sayang..* ☺
5. *Someone special "****izan****" yang selalu ta repotin, kesana kemari mencari sesuatu yang kurang selama mengerjakan tugas akhir ini n selalu ada buat ta,, hehehehe, makasih .....*☺.
6. *Untuk* ***Andong Q*** *tercinta, yang selau bilang "bilo balik habih, tak sayang samo andong do karna kulaih jauh", sekarang ta dah selasai ndong,,,makasih y,,we love u.,,,tak lupa juga terima kasihuntuk* ***mak imus, mak idol, duo ibu ana, ibu ijom, cu ujang, cik ijul*** *dan* ***paman*** *dan* ***ibu2 Q*** *yang tak bisa disebut satu persatu.*

MOTTO

“hiduplah dengan selalu membawa keyakinan dan harapan serta semangat cinta dan perjuangan “

“Seseorang mengalami kegagalan terkadang bukan disebabkan oleh minimnya keahlian yang dia miliki, tetapi justru disebabkan oleh minimnya keteguhan diri”

“ apapun yang kita lakukan akan membuahkan hasil, baik berbuah baik dan buruk berbuah buruk “

“man jadda wa jadda”

“ Ridho dari orang tua = Ridho ALLAH SWT “

“ Innallaha ma’ana ”

KATA PENGANTAR

"*Bissmillahirrohmanirrohim*"

Assalamu'alaikum Wr.Wb.

Allahamdulillahirobbil'alamin, hanya rasa sukur yang sangat mendalam yang dapat penulis panjatkan kehadirat Allah SWT, karena hanya dengan ridho dan hidayahNya penulis dapat menyelesaikan Tugas Akhir yang berjudul " Analisis *Computer forensic* Menggunakan FTK (*Forensic ToolKit*) sebagai prasyarat untuk menyelesaikan masa pembelajaran jenjang Sarjana Strata 1 di jurusan Teknik Informatika Universitas Islam Indonesia.

Ada banyak sekali pembelajaran yang penulis dapatkan selama proses penyelesaian Tugas Akhir ini, dan tak lupa penulis ucapkan banyak terimakasih terhadapat pihak – pihak yang secara langsung maupun tak langsung terlibat dalam penyelesaian Tugas Akhir ini. Untuk itu penulis ingin mengucapkan ucapan terimakasih yang tulus kepada:

1. Allah SWT atas segala karunia, rahmat dan hidayahNya, juga kepada junjungan kita Nabi besar Muhammad SAW.
2. Mak abah yang selalu memberikan dukungan, kasih sayang dan do'a yang tak ternilai harganya.
3. Kakak – kakak dan adik – adikku (ulong, ongah, adek yati, abang juber, abang oyok n bungsu) yang senantiasa memberikan do'a semangat dalam penyelesaian tugas akhir ini.
4. Abangku izan, yang senantiasa mengingatkanku dan selalu memberikan semangat.
5. Bapak Gumbolo Hadi Susanto, Ir., M.Sc selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
6. Bapak Yudi Prayudi, S.Si., M.Kom, selaku Ketua Jurusan Informatika Universitas Islam Indonesia dan selaku dosen pembimbing, terima kasih pak atas segala bantuan, dukungan dan kesabaran yang diberikan.
7. Bapak Dewa dan bapak Hamid. Terima kasih penulis haturkan atas segala bantuan dan kesabaran yang diberikan.

8. Seluruh Dosen Jurusan Teknik Informatika Universitas Islam Indonesia yang telah mengajarkan banyak ilmu, dan semoga ilmu yang diberikan menjadi suatu nilai ibadah.
9. mbak tyas, alias say Q ☺, terimakasih untuk persahabatan dan kesitiakawanan nya, yang tak pernah jemu mengingatkan Q tentang kuliah,,,,makasih bgt...luph u dech pokokke (eh sexan dengan mas Nu nya juga alias mas fajar tigor) ☺.
10. Untuk adek – adek Q (ia, Ukhun "adri", Madu "titin", dan Titi) makasih untuk dukungan nya n persaudaraan yang telah kita bangun, i love u all.
11. Anak – anak Q (Nurul n imul), makasih ya nak, udah memberikan dukungan walau terkadang dengan cara "kita selesai barengkan nyak"...hehehehehe masak nyak n anak selesai bareng.
12. Untuk keluarga baru @jogja (b ujenk, b ichad, adek supri, b bembeng,k gadis,b nawa, vera, b agus, b wawi, aim n b oki) terima kasih atas dukungan nya n kekeluargaan nya.
13. Indah dan Dini makasih ya atas dukungan nya,,,n terima kasih atas persahabatan nya. ☺
14. Keluarga Komoisariat Rokan hilir yang telah mengajarkan banyak hal n kekeluargaan selama dijogja, thanks all. Dan keluarga Komisariat Bengkalis (b nawe, b husni, b hendro, b sandi, boy, fa, safri, b adi, b akmal, b mijack n agung) makasih untuk pembelajarannya dan selalu masak – masaknya,,☺.
15. Aan, mamet, barly n adit yang banyak membantu, thx fren.
16. Semua pihak yang telah membantu dalam menyelasikan Tugas Akhir ini, "*Thanks a lot of all* ".

Semoga Allah SWT senantiasa membalas semua kebaikan dan jasa-jasa yang telah diberikan dengan pahala yang berlimpah, amin. Semoga Tugas Akhir ini bermanfaat untuk kita semua.

Yogyakarta, 26 Mei 2011

Penulis

ABSTRAKSI

Computer forensic adalah penyelidikan dan analisis komputer untuk menentukan potensi bukti legal. Berbeda dari pengertian forensik pada umumnya, *computer forensic* 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.

Ada beberapa tahapan dalam *computer forensic*, yaitu : pengumpulan data, pengujian, analisis serta dokumentasi dan laporan. 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 *evidence* 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.

Kata kunci : *Computer, forensic, toolkit,* FTK, *Image Data*

TAKARIR

Evidence	Informasi atau data (Bukti Digital).
Hash	Ringkasan Pesan
Imaging	Proses menggandakan atau menjadi kan yang copy-an atau yang palsu sama persis dengan yang asli.
Log	Catatan yang merekam segala aktifitas suatu aplikasi dijalankan. terkadang Log juga digunakan untuk menganalisa status suatu aplikasi.
Source	Sumber

DAFTAR ISI

HALAMAN JUDUL i
LEMBAR PENGESAHAN PEMBIMBING ii
LEMBAR PENGESAHAN PENGUJI iii
LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR iv
HALAMAN PERSEMBAHAN v
MOTTO vi
KATA PENGANTAR vii
ABSTRAKSI ix
TAKARIR x
DAFTAR ISI xi
DAFTAR GAMBAR xiv

BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan Penelitian 2
1.5 Manfaat Penelitian 2
1.6 Metode Penelitian 3
1.7. Sistematika Penulisan 3

BAB II LANDASAN TEORI 5

2.1 Latar Belakang dan Sejarah *Computer Forensic* 5

2.2 Kebutuhan Akan Forensik.....6

2.3 Pemodelan Forensik 7

2.4 Tahapan Pada *Computer Forensic* 8

2.5 Metodologi *Forensic* 10

2.6 *Imaging* Data 14

2.7 *FTK* 17

2.8 *Evidence Analyzing* 19

BAB III METODOLOGI 20

3.1 Deskripsi Uji Coba 20

3.2 Gambaran Umum Uji Coba 21

3.2.1 *Imaging Data* Mengunakan *FTK Imager* 21

3.2.2 Pengecekan Data dan Analisis Mengunakan *FTK* 26

BAB IV HASIL DAN PEMBAHASAN 33

4.1 Hasil dan Pembahasan Tombol *Document* 33

4.2 Hasil dan Pembahasan Tombol Folder 34

4.3 Hasil dan Pembahasan Tombol *Other Thumbnail* dan *Graphicks* 35

4.4 Hasil dan Pembahasan *Email Messages* dan *From Email* 37

4.5 Hasil dan Pembahasan *Delated Files* 37

4.6 Hasil dan Pembahasan Log Jaringan.....38

4.7 Hasil dan Pembahasan Tombol-Tombol yang Lainnya 40

BAB V KESIMPULAN DAN SARAN.....42

5.1 Kesimpulan 42

5.2 Saran.....42

DAFTAR PUSAKA.....43

DAFTAR GAMBAR

Gambar 2.1 Tahap – Tahap *Computer Forensic* 8

Gambar 3.1 Gambaran Umum Uji Coba 21

Gambar 3.2 *Create Disk Image* 22

Gambar 3.3 Halaman *Select Source* 23

Gambar 3.4 *Select Drive* 24

Gambar 3.5 *Select Image Type* 25

Gambar 3.6 *Evidence Item Information* 25

Gambar 3.7 *Select Image Destination* 26

Gambar 3.8 IImaging Data Dapat Dimulai 26

Gambar 3.9 Halaman *New Case* 27

Gambar 3.10 Halaman *Case Log Options* 28

Gambar 3.11 *Evidence Processing Options* 28

Gambar 3.12 *Refine Case* 29

Gambar 3.13 *Refine Index* 29

Gambar 3.14 *Add Evidence* 30

Gambar 3.15 *Evidence Informations* 30

Gambar 3.16 *Case Summary* 31

Gambar 4.1 Tampilan *Document* dengan *file htm* 33

Gambar 4.2 Bukti Berbentuk Dokumen 34

Gambar 4.3 Tampilan *Explorer* 35

Gambar 4.4 *Evidence* Pornografi 36

Gambar 4.5 *Evidence* Teroris.....36

Gambar 4.6 Tampilan *Email Messages* 37

Gambar 4.7 Tampilan *Deleted Files* 38

Gambar 4.8 *Log History*.....39

Gambar 4.9 Log Jaringan Berbentuk Aktivitas Ilegal 39

Gambar 4.10 Informasi Keuangan 40

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin pesat menyebabkan perkembangan *computer forensic* juga semakin meningkat. Pada masa dahulu ketika terjadi suatu kasus, bukti yang diamankan hanya lah bukti non digital atau bukti fisik yang berkaitan dengan kasus, namun seiring perkembangan zaman, bukti digital mulai diperhitungkan karena hampir setiap orang menggunakan barang – barang digital seperti notebook, handphone, telpon, ipod, PC, server dan sebagainya, yang mana barang – barang digital tersebut dapat dijadikan sebagai bukti terhadap suatu kasus. Seperti yang terjadi dalam beberapa tahun belakangan, banyak kasus yang dapat dipecahkan melalui *computer forensic* seperti kasus teroris Noordin M.Top dan lain sebagainya.

Sebelum *computer forensic* berkembang, ketika terjadi suatu kasus ahli forensik kedokteran amat sangat dibutuhkan, namun sekarang tidak hanya ahli forensik kedokteran saja akan tetapi ahli forensik dibidang teknologi juga sangat dibutuhkan untuk mencari bukti dari suatu kasus sehingga kasus tersebut dapat dipecahkan.

Ketika seorang tersangka menggunakan barang digital maka akan terdapat bukti atau log pada barang tersebut, yang mana barang itu dapat dijadikan bukti kejahatan dihadapan pengadilan, untuk mendapatkan bukti digital dibutuhkan *computer forensic*. Bukti digital yang dapat dianalisa secara forensik harus di *image* terlebih dahulu menggunakan tools forensik, diantaranya adalah FTK *Image*r yang merupakan bagian dari FTK (*Forensc ToolKit*). Setelah proses imaging selesai dilakukan maka akan dilakukan analisis terhadap bukti tersebut, apakah tersangka ada kaitan dengan kasus yang terjadi, dan data apa saja yang akan diperoleh ketika penyelidikan dilakukan dengan menggunakan FTK (*Forensic ToolKit*).

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas dapat dirumuskan permasalahan yang akan diselesaikan yaitu :

a. Bagaimana mengidentifikasi kasus dari suatu disk *image* menggunakan FTK
b. Bagaimana memperoleh bukti digital dan bagaimana membentuk suatu disk *image* menggunakan FTK *imager*.

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 yang diperlukan yaitu :

a. Karakteristik yang dianalisis adalah hasil *imaging* yang berupa *Document, Email Messages, From Email, Deleted Files, Other Thumbnail, Graphics, Folder* serta *Log* Jaringan.
b. Disk *image* menggunakan FTK *image*r.
c. Melakukan penyelidikan terhadap kasus teroris yang mencakup pornografi dan log jaringan.

1.4 Tujuan Penelitian

Tujuan penulisan tugas akhir ini : Menganalisa *computer forensic* dari hasil *imaging* sehingga jenis data atau *log* apa saja yang bisa diketahui jika menggunakan FTK *(Forensic ToolKit*)

1.5 Manfaat Penelitian

Manfaat dari penelitian ini antara lain :

a. Menambah pengetahuan dan lebih memahami ilmu forensik serta tools yang bisa digunakan untuk analisis forensik.
b. Memberikan pemahaman tentang FTK serta *computer forensic* kepada mahasiswa yang lain atau pembaca laporan ini sehingga diharapkan akan lebih mengerti akan tool tersebut.

1.6 Metodologi Penelitian

Dalam suatu penelitian, diperlukan metodologi agar data yang diperlukan dalam penelitian sesuai dengan data yang ada di lapangan. Metodologi penelitian adalah ilmu mengenai jalan yang dilewati untuk mencapai pemahaman. Metodologi penelitian yang akan dilakukan yaitu :

1.6.1 Studi dan Pengumpulan Data

Dalam studi dan pengumpulan data, yang menjadi sasaran pokok adalah hasil *imaging* dari FTK. Pengumpulan informasi data atau *log*, dilakukan menggunakan FTK *imager*. Data yang diperoleh dari Hasil *image* komputer *server* akan dianalisis. Sebelum melakukan *imaging* dan analisis forensik, akan dilakukan pengumpulan informasi yang berkaitan dengan *imaging* dan hal – hal yang berkaitan dengan *computer forensic*, yang diambil dari buku – buku referensi, jurnal, literatur dan internet yang relevan dengan permasalahan yang dihadapi.

1.6.2 Perancangan Sistem Implementasi Pengujian

Pada tahapan ini akan dilakukan ujicoba dan implementasi pengujian dari model ujicoba yang telah dibuat.

1.6.3 Analisis Data

Pada tahapan ini akan dilakukan proses analisis terhadap hasil *imaging* dari FTK sehingga akan diketahui cara kerja dan kemampuan dari tool tersebut.

1.7 Sistematika Penulisan

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

BAB I PENDAHULUAN

Bab ini berisi pembahasan masalah secara umum yang meliputi Latar Belakang Masalah, Rumusan Masalah, Batasan Masalah, Tujuan

Penelitian, Manfaat Penelitian, Metodologi Penelitian dan Sistematika Penulisan.

BAB II LANDASAN TEORI

Bab ini memuat landasan teori yang berfungsi sebagai sumber atau alat, dalam memahami permasalahan yang berkaitan dengan teori *computer forensic*, *Forensic ToolKit* (FTK).

BAB III METODOLOGI

Bagian ini berisi studi literatur mengenai pemodelan uji coba serta langkah langkah – langkah ujicoba.

BAB IV PENGUJIAN DAN PEMBAHASAN

Berisi tentang proses pengujian, berupa print screen dan penjelasan serta hasil analisis forensik dari FTK.

BAB V KESIMPULAN DAN SARAN

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

BAB II

LANDASAN TEORI

2.1 Latar Belakang dan Sejarah *Computer Forensic*

Saat ini teknologi komputer dapat digunakan sebagai alat bagi para pelaku kejahatan komputer : seperti pencurian, penggelapan uang dan lain sebagainya. Barang bukti yang berasal dari komputer, telah muncul dalam persidangan hampir 30 tahun lalu. Awalnya, hakim menerima bukti tersebut tanpa membedakannya dengan bentuk bukti lainnya. Namun seiring dengan kemajuan teknologi komputer, perlakuan tersebut menjadi membingungkan. Bukti yang berasal dari komputer sulit dibedakan antara yang asli ataupun salinannya, karena berdasarkan sifat alaminya, data yang ada dalam komputer sangat mudah dimodifikasi. Proses pembuktian bukti tindak kejahatan tentunya memiliki kriteria, demikian juga dengan proses pembuktian pada bukti yang didapat dari komputer **[YAN10]**.

Computer forensic adalah penyelidikan dan analisis komputer untuk menentukan potensi bukti legal. Berbeda dari pengertian forensik pada umumnya, *computer forensic* 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. Data elektronik bisa muncul dalam bentuk dokumen, informasi keuangan, *e-mail*, *job schedule*, *log*, atau transkripsi *voice-mail* **[UTD05].**

Beberapa definisi *computer forensic* **[UTD05]:**

a. Definisi sederhana “Penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan Software dan tool untuk mengekstrak dan memelihara barang bukti tindakan kriminal”.

b. Menurut Judd Robin, seorang ahli *computer forensic*: “Penerapan secara sederhana dari penyelidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin”.
c. New Technologies memperluas definisi Robin dengan: “*Computer forensic* berkaitan dengan pemeliharaan, identifikasi, ekstraksi dan dokumentasi dari bukti-bukti komputer yang tersimpan dalam wujud informasi magnetik”.

Tujuan dari *computer forensic* adalah untuk melakukan penyelidikan terstruktur dengan tetap mempertahankan rantai dokumentasi bukti untuk mencari tahu persis apa yang terjadi pada komputer dan siapa yang bertanggung jawab untuk itu. Disamping itu penggunaan *computer forensic* misalnya untuk:

a. Mencari bukti penipuan atau korupsi yang dilakukan oleh karyawan.
b. Melakukan analisa atas sistem komputer yang disusupi *hacker*. Bagaimana cara *hacker* tersebut mendapatkan akses dan apa yang dilakukannya.
c. Melakukan *recovery* data yang hilang baik disengaja maupun tidak, bahkan setelah hardisk di-format atau digunakan orang lain.

2.2 Kebutuhan Akan Forensik

Dalam satu dekade terakhir, tingkat kejahatan yang melibatkan komputer semakin meningkat, sehingga semakin banyak perusahaan atau produk yang berusaha membantu penegak hukum dalam proses pembuktian berbasis komputer untuk menentukan siapa, apa, dimana, kapan dan bagaimana kejahatan tersebut terjadi. Teknik dan tool forensik sering kali dikaitkan dengan penyelidikan kriminal dan penanganan insiden keamanan komputer. Hal ini digunakan untuk menyelidiki sistem tersangka, mengumpulkan dan memelihara barang bukti, merekonstruksi kejadian. Selain itu teknik dan tool forensik juga digunakan untuk tugas- tugas lainnya, seperti **[LEO09]** :

a. *Operational Troubleshooting.*

   Banyak tool dan teknik forensik yang dapat digunakan untuk melakukan *troubleshooting* atas masalah-masalah operasional, seperti menemukan

lokasi fisik dan virtual sebuah *host* dengan konfigurasi jaringan yang tidak tepat, mengatasi masalah fungsional dalam sebuah aplikasi.

b. *Log* Monitoring

Beragam tool dan teknik dapat membantu dalam melakukan monitoring *log*, seperti menganalisis entri *log* dan mengkorelasi entri *log* dari beragam sistem. Hal ini dapat membantu dalam penanganan insiden, mengidentifikasi pelanggaran kebijakan, audit, ddan usaha lainnya.

c. Data *Recovery*

Terdapat lusinan tool yang dapat mengembalikan data yang hilang dari sistem, termasuk data yang telah dihapus atau dimodifikasi baik yang disengaja maupun tidak.

d. Data *Acquisition*

Beberapa organisasi menggunakan tool forensik untuk mengambil data dari *host* yang telah dipensiunkan. Sebagai contoh, ketika seorang user meninggalkan organisasi, data dari komputer user tersebut dapat diambil dan disimpan bilamana dibutuhkan di masa mendatang. Media komputer tersebut lalu dapat disanitasi untuk menghapus semua data user tersebut.

e. Regulatory Compliance

Regulasi yang ada dan yang akan muncul mengharuskan organisasi melindungi informasi sensitif dan memelihara beberapa catatan tertentu demi kepentingan audit. ketika informasi yang dilindungi terekspos ke pihak lain, organisasi mungkin diharuskan untuk memberitahu pihak atau individu yang terkena dampaknya. Forensik dapat membantu organisasi melakukan *due diligence* dan mematuhi persyaratan tertentu.

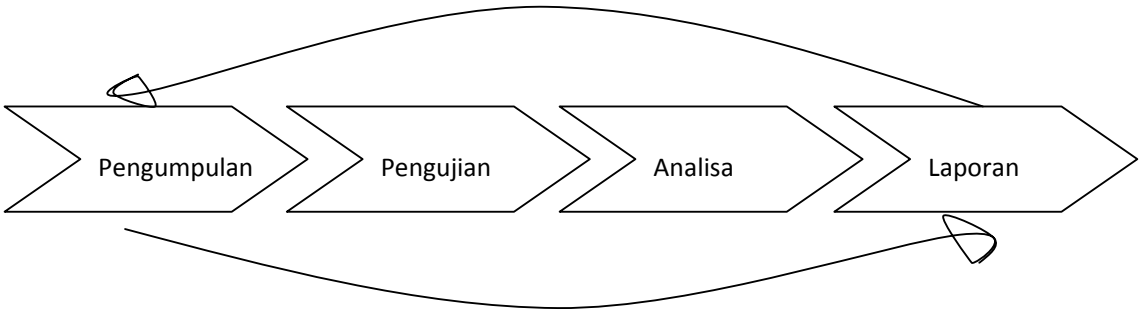
2.3 Permodelan Forensik

Model forensik melibatkan tiga komponen terangkai yang dikelola sedemikian rupa hingga menjadi sebuah tujuan akhir dengan segala kelayakan dan hasil yang berkualitas. Ketiga komponen tersebut adalah **[SUL08]** :

a. Manusia *(People),* diperlukan kualifikasi untuk mencapai manusia yang berkualitas. Memang mudah untuk belajar *computer forensic*, tetapi untuk menjadi ahlinya, dibutuhkan lebih dari sekadar pengetahuan dan pengalaman.
b. Peralatan *(Equipment),* diperlukan sejumlah perangkat atau alat yang tepat untuk mendapatkan sejumlah bukti *(evidence)* yang dapat dipercaya dan bukan sekadar bukti palsu.
c. Aturan *(Protocol),* diperlukan dalam menggali, mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat. Dalam komponen aturan, diperlukan pemahaman yang baik dalam segi hukum dan etika, kalau perlu dalam menyelesaikan sebuah kasus perlu melibatkan peran konsultasi yang mencakup pengetahuan akan teknologi informasi dan ilmu hukum.

2.4 Tahapan Pada *Computer Forensic*

Empat fase dalam *computer forensic* : pengumpulan, pengujian, analisa dan laporan. Ada objek yang dikelola dari proses setiap fase, dimulai dari media dan kemudian didapati *"evidence"* diakhir proses. Tentunya umpan balik diberlakukan untuk menganalisa kembali hasil yang didapat dengan tujuan semula. Konektivitas yang terjalin mencakup proses dan hasil seperti pada gambar 2.1. **[SUL08].**



Gambar 2.1 Tahap – tahap *computer forensic*

2.4.1 Pengumpulan data

Ini adalah langkah pertama dalam proses forensik untuk mengidentifikasi sumber – sumber potensial dan bagaimana kemudian data dikumpulkan. Data yang sering didapat terdapat pada *personal computer* atau *desktop computer*, namun bukan hanya *desktop computer* 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 :

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

Pada kasus ini penulis melakukan pengumpulan data dari sebuah komputer *server* dan kemudian data dikumpulkan dalam satu file *image*.

2.4.2 Pengujian

Setelah melalui proses pengumpulan data, langkah lebih lanjut adalah melakukan pengujian, mencakup didalam nya menilai dan mengektrak “kepingan” informasi yang relevan dari data- data yang dikumpulkan. Tahap ini melibatkan bypassing atau meminimalisasi fitur-fitur sistem operasi atau aplikasi yang mengaburkan data, seperti kompresi, enkripsi dan akses mekanisme kontrol.

Ada banyak tools yang digunakan dalam pengujian ini, semisal software yang mampu menentukan secara akurat jenis file yang berisi karakteristik data tertentu, mungkin berupa file teks, grafik, musik, atau berbagai file kompresi lainnya. Secara mendasar tahap ini mencakup mengalokasi file, mengekstrak file (

mungkin melalui *enkripsi, stenografi, uncompress* dan lainnya) atau mungkin melakukan pemeriksaan terhadap metadata dan lain sebagainya.

Setelah data dari file *image* dikumpulkan, maka akan dilakukan pengujian terhadap data, data yang telah diperoleh akan dicek dan dicari data bagian mana yang dibutuhkan untuk kemudian dilakukan pengujian.

2.4.3 Analisis

Setelah pengujian data, selanjutnya akan dilakukan analisa terhadap data yang diperoleh. Begitu informasi diekstrak, *examiner* melakukan analisa untuk merumuskan kesimpulan dalam menggambarkan data. Analisa yang dimaksud tentunya mengambil pendekatan metodis dalam menghasilkan kesimpulan yang berkualitas didasarkan pada ketersediaan data, tugas *examiner* mencakup pula kegiatan seperti mengidentifikasi user atau orang diluar dari pengguna (tetapi terlibat secara tidak langsung), mengidentifikasi lokasi, barang – barang, kejadian, dan menentukan bagaimana komponen – komponen tadi terhubung satu dengan yang lain sehingga didapati kesimpulan pada akhirnya, tentunya kompleksitas memunculkan banyak sumber data.

2.4.4 Dokumentasi dan laporan

Reporting adalah tahap akhir dari proses *computer forensic*, dalam tahap ini kita merepresentasikan informasi yang merupakan hasil dari proses analisis. Banyak faktor yang mempengaruhi proses reporting, Seperti berikut ini :

a. *Alternative Explanations* (penjelasan alternatif).
b. *Audience Consideration* (pertimbangan peserta).
c. *Actionable Information*.

2.5 Metodologi Forensik

Menurut Wright penyelidikan sebaiknya dimulai bila sebuah rencana telah terumuskan dengan baik. Maka landasan metodologi akan memetakan kontruksi ilmiah dalam menyelesaikan sebuah pekerjaan. Demikian juga dalam komputer forensik, metodologi diharapkan akan membantu tercapainya hasil yang dituju.

Walaupun tidak ada standard baku, namun terdapat sejumlah tahapan yang sebaiknya dilakukan dalam proses komputer forensik, yaitu: menentukan tujuan, memproses fakta, mengungkapkan bukti digital. Tujuan diperlukan sebagai pengarah akhir dari sebuah investigasi. Dalam hal ini sebuah tujuan sebaiknya juga dideskripsikan dalam bentuk parameter-parameter kesuksesan dalam menginvestigasi kejadian. Dengan adanya parameter tersebut maka akan diketahui kapan hasil dari inverstigasi telah berakhir.

Bukti digital adalah informasi yang didapat dalam bentuk/ format digital (scientific Working Group on Digital Evidence, 1999). Beberapa contoh bukti digital antara lain :

a. Email-alamat email
b. File wordprocessor/ spreadsheet
c. source code sopwer
d. file berbentuk image
e. webBrowser bookmark, cookies
f. kalender, to-do list

Bukti digital tidak dapat langsung dijadikan barang bukti pada proses peradilan, karena menurut sifat alamiahnya bukti digital sangat tidak konsisten. Untuk menjamin bahwa bukti digital dapat dijadikan barang bukti dalam proses peradilan maka diperlukan sebuah standar data digital yang dapat dijadikan barang bukti dan metode standar dalam pemrosesan barang bukti digital dapat dijamin keasliannya dan dapat dipertanggungjawabkan.

Berikut ini adalah aturan standar agar bukti dapat diterima dalam proses peradilan :

a) Dapat diterima, artinya data harus mampu diterima dan digunakan demi hukum mulai dari kepentingan penyelidikan sampai dengan kepentingan pengadilan.
b) Asli, artinya bukti tersebut harus berhubungan dengan kejadian/ Kasus yang terjadi dan bukan rekayasa.

c) Lengkap, artinya bukti bisa dikatakan bagus dan lengkap jika di dalamnya terdapat banyak petunjuk yang dapat membantu investigasi
d) Dapat dipercaya, artinya bukti dapat mengatakan hal yang terjadi di belakangnya jika bukti tersebut dapat dipercaya, maka proses investigasi akan lebih mudah, syarat dapat dipercaya ini merupakan suatu keharusan dalam penanganan perkara

Untuk itu perlu adanya metode standar dalam pengambilan data atau bukti digital dan pemrosesan barang bukti data digital, untuk menjamin keempat syarat di atas terpenuhi. Sehingga data yang diperoleh dapat dijadikan barang bukti yang legal di pengadilan dan diakui oleh hukum.

2.5.1 Pengungkapan Bukti Digital

Bukti digital (*Digital Evidence*) merupakan salahsatu perangkat vital dalam mengungkap tindak *cybercrime*. Dengan mendapatkan bukti-bukti yang memadai dalam sebuah tindak kejahatan, sebenarnya telah terungkap separuh kebenaran. Langkah berikutnya adalah menindak-lanjuti bukti-bukti yang ada sesuai dengan tujuan yang ingin dicapai. Bukti Digital yang dimaksud dapat berupa adalah : E-mail, file-file wordprocessors, spreadsheet, sourcecode dari perangkat lunak, Image, web browser, bookmark, cookies, Kalender. Menurut Kemmish, terdapat empat elemen forensic yang menjadi kunci pengungkapan bukti digital. Elemen forensic tersebut adalah: identifikasi bukti digital, penyimpanan bukti digital, analisa bukti digital, presentasi bukti digital.

2.5.2 Identifikasi Bukti Digital

Elemen ini merupakan tahapan paling awal dalam komputer forensik. Pada tahapan ini dilakukan identifikasi dimana bukti itu berada, dimana bukti itu disimpan, dan bagaimana penyimpanannya untuk mempermudah penyelidikan. *Network Administrator* merupakan sosok pertama yang umumnya mengetahui keberadaan *cybercrime* sebelum sebuah kasus *cybercrime* diusut oleh fihak yang berwenang. Ketika fihak yang berwenang telah dilibatkan dalam sebuah kasus, maka juga akan melibatkan elemenelemen vital lainnya, antara lain:

a. Petugas Keamanan (Officer/*as a First Responder*), Memiliki kewenangan tugas antara lain : mengidentifikasi peristiwa,mengamankan bukti, pemeliharaan bukti yang temporer dan rawan kerusakan.
b. Penelaah Bukti (Investigator), adalah sosok yang paling berwenang dan memiliki kewenangan tugas antara lain: menetapkan instruksi-instruksi, melakukan pengusutan peristiwa kejahatan, pemeliharaan integritas bukti.
c. Teknisi Khusus, memiliki kewenangan tugas antara lain : memeliharaan bukti yang rentan kerusakan dan menyalin *storage* bukti, mematikan(*shuting down*) sistem yang sedang berjalan, membungkus/memproteksi buktibukti, mengangkut bukti dan memproses bukti. Ketiga elemen vital diatas itulah yang umumnya memiliki *otoritas* penuh dalam penuntasan kasus cybercrime yang terjadi.

2.5.3 Penyimpanan Bukti Digital

Barang bukti digital merupakan barang bukti yang rapuh. Tercemarnya barang bukti digital sangatlah mudah terjadi, baik secara tidak sengaja maupun disengaja. Kesalahan kecil pada penanganan barang bukti digital dapat membuat barang bukti digital tidak diakui di pengadilan. Bentuk, isi, makna dari bukti digital hendaknya disimpan dalam tempat yang *steril*. Hal ini dilakukan untuk benar-benar memastikan tidak ada perubahan-perubahan. Sedikit terjadi perubahan dalam bukti digital, akan merubah hasil penyelidikan. Bukti digital secara alami bersifat sementara (*volatile*), sehingga keberadaannya jika tidak teliti akan sangat mudah sekali rusak, hilang, berubah, mengalami kecelakaan. Langkah pertama untuk menghindarkan dari kondisi-kondisi demikian salah satunya adalah dengan melakukan copy data secara *Bitstream Image* pada tempat yang sudah pasti aman.

Bitstream image adalah metode penyimpanan digital dengan mengkopi setiap bit demi bit dari data orisinil, termasuk File yang tersembunyi (*hidden files*), File temporer (temp file), File yang terdefragmen (*fragmen file*), dan file yang belum ter*overwrite*. Dengan kata lain, setiap biner digit demi digit di-copy secara utuh dalam media baru. Teknik pengkopian ini menggunakan teknik

komputasi CRC**.** Teknik ini umumnya dikenal dengan istilah *cloning disk, image, goshting.*

2.5.4 Analisa Bukti Digital

Barang bukti setelah disimpan, perlu diproses ulang sebelum diserahkan pada pihak yang membutuhkan. Pada proses inilah skema yang diperlukan akan fleksibel sesuai 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 yang telah melakukan, apa yang telah dilakukan (Contoh : penggunaan software apa saja), hasil proses apa yang dihasilkan, waktu melakukan). Secara umum, tiap-tiap data yang ditemukan dalam sebuah sistem komputer sebenarnya adalah potensi informasi yang belum diolah, sehingga keberadaannya memiliki sifat yang cukup penting. Data yang dimaksud antara lain : Alamat URL yang telah dikunjungi, Pesan e-mail 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.

2.5.5 Presentasi Bukti Digital

Kesimpulan akan didapatkan ketika semua tahapan telah dilalui, terlepas dari ukuran *obyektifitas* yang didapatkan, atau standar kebenaran yang diperoleh, minimal bahan-bahan inilah nanti yang akan dijadikan “modal” untuk bukti di pengadilan. Selanjutnya bukti-bukti digital inilah yang akan dipersidangkan, diuji otentifikasi dan dikorelasikan dengan kasus yang ada. Pada tahapan ini semua proses-proses yang telah dilakukan sebelumnya akan diurai kebenarannya serta dibuktikan kepada hakim untuk mengungkap data dan informasi kejadian.

2.6 *Imaging* Data

Proses menciptakan duplikat yang tepat dari media pembuktian keaslian sering disebut Imaging. Dengan menggunakan hard-drive duplikator mandiri atau

perangkat lunak alat pencitraan seperti DCFLdd , IXimager , Guymager , TrueBack, EnCase atau FTK Imager, seluruh hard drive sepenuhnya diduplikasi . Hal ini biasanya dilakukan pada level sektor, membuat salinan bit-stream setiap bagian dari wilayah yang dapat diakses oleh pengguna dari hard drive yang secara fisik dapat menyimpan data, dan bukan duplikasi file sistem. Drive asli kemudian dipindahkan ke tempat penyimpanan yang aman untuk mencegah terjadinya penyalahgunaan. Selama proses imaging data statis, penulisan pada perangkat perlindungan atau aplikasi yang biasanya digunakan untuk mencegah perubahan dari perkenalan kepada media pembuktian pada saat akuisisi citra.

Proses pencitraan diverifikasi dengan menggunakan fungsi hash SHA-1 (dengan program seperti sha1sum) atau lainnya masih layak seperti algoritma MD5 . Pada titik kritis di seluruh analisis, media diverifikasi lagi, yang dikenal sebagai "hashing", untuk memastikan bahwa bukti masih dalam keadaan asli. Dalam lingkungan perusahaan mencari biaya sipil atau internal, seperti langkah-langkah pada umumnya diabaikan karena waktu yang dibutuhkan untuk melakukan itu. Sebaliknya, ketahanan bukti sering bergantung pada proses yang konsisten dan tepatNamun, verifikasi hash adalah penting untuk bukti yang akan dipresentasikan dalam ruang sidang.

Dalam proses *computer forensic*, pengambilan data dikenal dengan istilah '*forensic computer imaging*' dimana hard drive suspect dibuat copy-nya secara persis sama atau klon (termasuk juga data yang sudah dihapus dan area-area teknis hard drive yang tidak terbaca di sistem operasi). Untuk melakukan *imaging* data bisa menggunakan beberapa tools diantaranya adalah FTK *imager*. FTK merupakan *software* yang digunakan untuk membuat salinan yang identik dengan file asli dari data elektronik korban. Proses ini dilakukan agar data awal tidak mengalami perubahan. Hardware dan software yang digunakan pada *computer forensic* dapat menjaga agar data tetap utuh seperti sebelumnya (tidak ada perubahan), bahkan dapat menemukan file yang telah terhapus sehingga akan ditemukan bukti dari kasus yang terjadi.

Bukti-bukti digital dapat dikumpulkan dari berbagai sumber. Sumber - sumber yang nyata terdiri dari komputer, ponsel, kamera digital, hard drive, CD-

ROM, perangkat memori USB, dan sebagainya. Sumber-sumber yang tidak nyata terdiri dari pengaturan dari termometer digital, kotak hitam di dalam mobil, RFID tag, halaman web (yang harus dipertahankan sebagai mereka adalah subjek yang dapat berubah), dan data mengenai perangkat retensi misalnya jaringan selular atau penggunaan internet (biasa di Eropa).

Perhatian khusus harus diambil saat memegang bukti komputer: hampir semua informasi digital adalah yang paling mudah berubah, dan sekali berubah biasanya tidak mungkin terdeteksi telah terjadi perubahan (atau mengembalikan data kembali ke keadaan semula) kecuali tindakan lainnya telah diambil . Untuk alasan ini, ini adalah praktek umum untuk menghitung hash kriptografi dari file bukti dan untuk merekam hash yang ada di tempat lain, biasanya dalam notebook milik penyidik, jadi yang satu dapat menetapkan pada titik berikutnya dalam waktu dimana bukti belum diubah sejak hash dihitung.

Spesifik praktek lainnya yang telah diadopsi dalam penanganan bukti digital meliputi:

a. Media Imaging komputer menggunakan alat writeblocking untuk memastikan bahwa tidak ada data / bit yang diubah atau ditambah / dihapus pada perangkat tersangka.
b. Membangun dan menjaga rantai yang jelas.
c. Mendokumentasikan segala sesuatu yang telah dilakukan.
d. Hanya menggunakan alat dan metode yang telah diuji dan dievaluasi untuk memvalidasi akurasi dan reliabilitas.

Ada beberapa mekanisme kerja dari komputer atau digital forensik :

a) Ketika menerima barang bukti digital harus dilakukan proses *imaging* atau bahasa umumnya kloning, yaitu mengcopy secara keseluruhan dengan artian antara file asli dengan kloningan sama persis. Misalnya ada hardisk A yang mau kloning ke hardisk B, maka hardisk itu 1:1 persis sama isinya seperti hardisk A, walaupun di hardisk A sudah tersembunyi ataupun sudah dihapus *(delete).* Semuanya masuk ke hardisk B. Dari hasil kloning tersebut akan dilakukan analisa forensik oleh ahli forensik, Analisa tidak

boleh dilakukan dari barang bukti digital yang asli karena takut mengubah barang bukti. Hal ini bertujuan ketika melakukan penyelidikan terjadi kesalahan dihardisk kloning maka penyelidikan ulang masih bisa dilakukan dari kloningan yang baru dari hardisk aslinya.

b) Menganalisa isi data terutama yang sudah terhapus, tersembunyi, terenkripsi, dan history internet seseorang yang tidak bisa dilihat oleh umum. Misalnya, apa saja situs yang telah dilihat seorang tersangka, kemana saja mengirim email, dan lain-lain. Bisa juga untuk mencari dokumen yang sangat penting sebagai barang bukti di pengadilan. Sehingga *computer forensic* sangat dibutuhkan untuk mengungkap suatu kasus, terutama yang terkait dengan peralatan digital, karena hampir semua orang memiliki peralatan digital.

2.7 *FTK*

FTK (foresic ToolKit) merupakan salah satu tools forensik yang dapat membantu melakukan pengujian forensik yang baik diwindows. *FTK* menyediakan penyaringan file dan fungsi *search* dan juga analisis *email*. Untuk memastikan kalau file yang dipakai bekerja belum berubah, penyidik bisa membandingkan suatu *hash* dari file asal dengan file *image*. *Hashing* ini akan memberikan suatu validitas matematis, sehingga suatu *image* forensik harus sesuai dengan yang aslinya **[UTD05].**

Software dari AccesData ini memiliki kemampuan mencari ribuan file dengan cepat menemukan bukti yang diinginkan. Fitur yang cocok untuk digunakan konsultan *security* untuk menyelesaikan pemeriksaan *Computer forensic*. *FTK* juga dapat membaca berbagai format *digital evidence* data, termasuk yang dibuat oleh *EnCase* **[NEO04].**

Forensic Toolkit Hanya Menganalisa sistem *Windows*, sehingga apabila anda menyidik sistem *Unix* atau *Linux*, anda membutuhkan tool lain seperti *EnCase atau The Coroner's Toolkit.* Setelah instalasi dan memasukkan *KFF Library* ke *direktory* program *FTK* anda dapat memulai penyidikan dengan memilih *Case Options* yang biasanya aktifkan *KFF Lookup* maupun *Full text*

Index. Kedua hal ini yang akan sangat meringankan pekerjaan penyidikan. *FTK* dilengkapi dengan *dtSearch*, suatu *search engin*e yang memungkinkan penyidik melakukan pencarian langsung terhadap suatu informasi berbentuk teks. Langkah-langkah penyidikan *(events*) dicatat secara otomatis dalam *log*, sehingga meringankan pekerjaan membuat catatan audit *trial* terhadap pekerjaan penyidikan **[NEO04].**

FTK bisa menganalisa sistem file : *FAT12/16/32, NTFS, ext2,ext3*. Disamping itu FTK juga bisa membaca format *image* dari : *Encase, Snapback, Safe back 2.0, Expert Witness, dd, ICS, Gosht* (hanya image Forensik) serta *SMART*. Tool ini mampu membuat image dari suatu drive dengan *hash* –nya, melakukan pengujian forensik dan membuat report. FTK menyediakan dua fungsi *hash*, yaitu :

a. *Message Digest 5 (MD5)*
   Suatu *fingerprint* digital 128-bit berdasarkan pada isi file yang dibuat oleh Ron Rivest RSA. *MD5* mengambil input sembarang dari panjang file dan menghasilkan suatu angka dengan panjang fixed yang disebut dengan *hash* atau *digest*, nilai tersebut diturunkan dari input. *MD5 hash* dipakai KFF untuk mengidentifikasi file.
b. *Secure Hash Algorithm (SHA)*
   Suatu *fingerprint* digital 160-bit berdasarkan isi file yang dirancang oleh *National Institude of Standarts and Technology (NIST).*

Option *hash*ing dipilih secara otomatis oleh *FTK* berdasarkan databese *KFF* (*Known File Filter*). *KFF* bertugas membandingkan *hash* file dengan suatu database *hash* dari suatu file, maksud dari *KFF* adalah untuk menghilangkan file yang bisa diabaikan seperti file program dan sistem tertentu, disamping itu ia juga bisa memeriksa file ganda. Dengan *FTK*, Kita bisa melakukan suatu *live search* atau *indexed search.*

a. *Live search* adalah proses pencarian yang memakan waktu lama, dengan membandingkan item – by – item dengan suatu search term. Disini kita

bisa melakukan search karakter non alphanumerik dan melakukan search ekspresi regular.

b. *Indexed search* menggunakan file index untuk menemukan suatu search term. File index memuat string kata yang ditemukan baik pada allocated dan unallocated space pada evidence. FTK menggunakan dtsearch sebagai *engine* untuk *index search*.

FTK membuat case report dan case log untuk mendokumentasikan proses dan hasil, disini terdapat fasilitas *report wizard* untuk membuat dan memodifikasi *report*

2.8 *Evidence Analyzing*

Analisa 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 (smoking gun). 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 anda ke lebih banyak lagi bukti.

Dalam melakukan prosedur ini anda akan dihadapkan pada data yang berlimpah. Untuk itu diperlukan proses eliminasi maupun pengalaman dalam melakukan analisa. Mengidentifikasi Tersangka Data yang anda punyai dapat mengarah ke IP address, nama-nama dalam data file, system name, jenis file dan isinya, teknik yang digunakan, program yang ada, pekerjaan dan keanggotaan sosial tersangka, pengetahuan khusus, cara, motif, dan juga kesempatan.

BAB III

METODOLOGI

3.1 Skenario Pengujian

Semakin banyaknya tindak kriminal menyebabkan semakin dibutuhkan nya ahli forensik. Ketika terjadi suatu kasus, dengan menggunakan komputer forensik akan diketahui apa, siapa, apa, bagaimana dan kapan kejadian tersebut terjadi. Namun untuk memperoleh bukti – bukti yang akurat harus melalui tahapan – tahapan tertentu, untuk mempermudah proses penyelidikan komputer forensik dibutuhkan suatu tool. Salah satu tool forensik yang bisa digunakan adalah FTK (*Forensic ToolKit*), kemudian akan dilakukan uji coba tool untuk lebih mengetahui data apa saja yang ditangkap oleh FTK. Dari tool tersebut apakah akan diketahui siapa melakukan apa, bagaimana tersangka melakukan nya dan sebagainya.

Untuk menemukan *evidence* harus dilakukan suatu tahapan pengumpulan barang bukti dan kemudian akan dilakukan *imaging* data terhadap barang bukti yang diperoleh. Salah satu contoh barang bukti yang dapat di *imaging* adalah notebook, dari notebook tersebut akan dapat dilakukan *imaging* terhadap hardisk dengan beberapa pilihan, seperti *phisical drive* atau *logical drive.* Ketika *examiner* memilih *phisical drive* maka FTK *image*r 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.

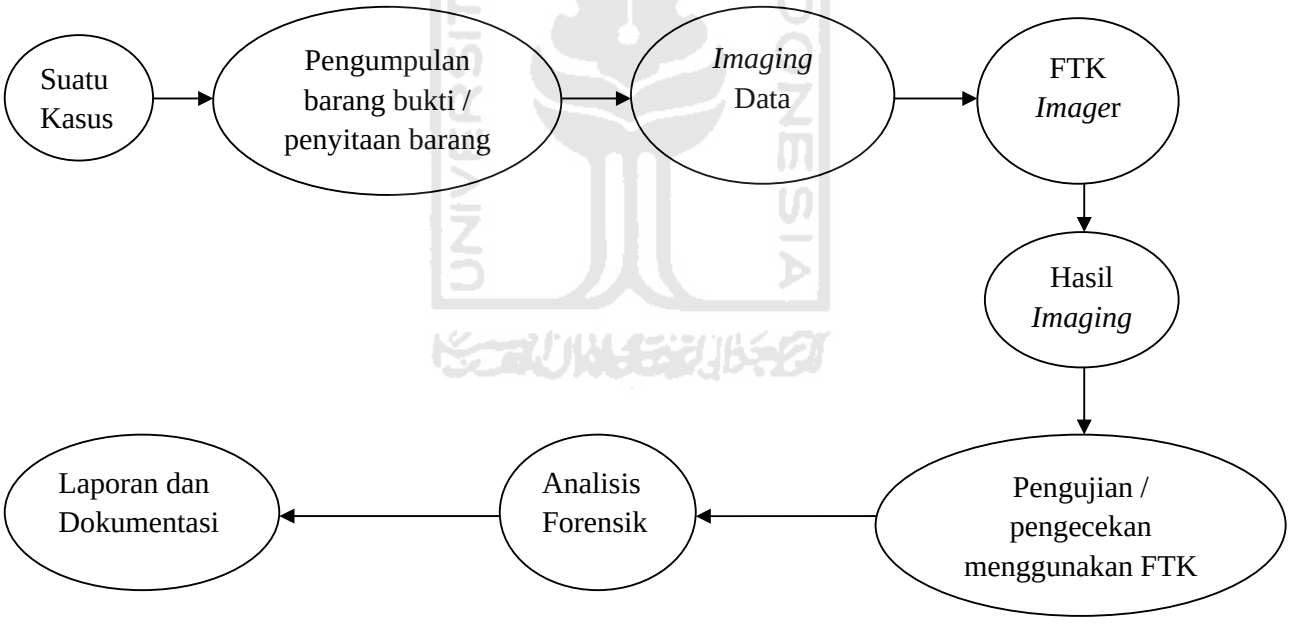
Data yang akan di analisis adalah *Document, Email Messages, From Email, Deleted Files, Other Thumbnail, Graphics, Folder* serta *Log* Jaringan. Dari semua data yang akan dianalisis akan dicari bukti yang berhubungan dengan kasus.

Dalam melakukan *raw data copy* terhadap hard disk atau media penyimpanan lain, berikut adalah prosedur yang disarankan. Perhatikan bahwa

untuk *raw* data copy digunakan perintah dd pada *Unix* (dapat juga rawrite pada DOS). Terhadap Hard Disk.

1. Buat image dengan dd byte demi byte.
2. Lakukan dd dari hard disk ke tape atau media lain Selain data-data yang memang dapat disita, masih ada data yang karena sifatnya tidak dapat disita, seperti misalnya sang tersangka itu sendiri, sumber-sumber berbasis Internet seperti log file dari ISP, catatan telepon, dan lain sebagainya. kita menggunakan sensor untuk mendapatkan bukti lebih jauh seperti menggunakan sniffer ataupun penyadap telepon.

3.2 Gambaran Umum Skenario



Gambar 3.1. Gambaran umum uji coba

3.2.1 *Imaging* data Menggunakan *FTK Imager*

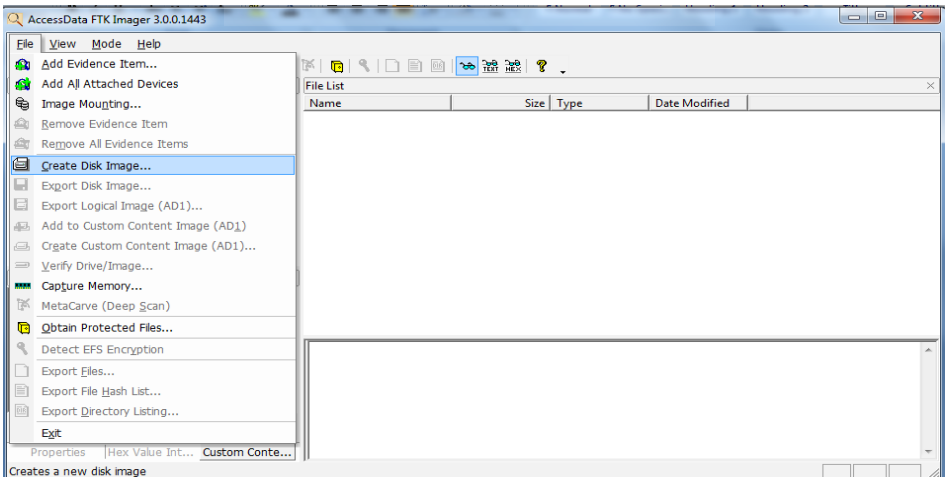
Asumsi ada seseorang diduga terlibat dengan sindikat teroris dan kemudian disita barang bukti dari tersangka berupa sebuah *notebook.* Pada laptop tersebut akan dilakukan pengecekan dengan cara *imaging* data menggunakan *FTK Image*r.

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

a. Preview *drive* dan *image* tanpa perlu menambahkan nya ke *case (Add Evidence*).
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 :

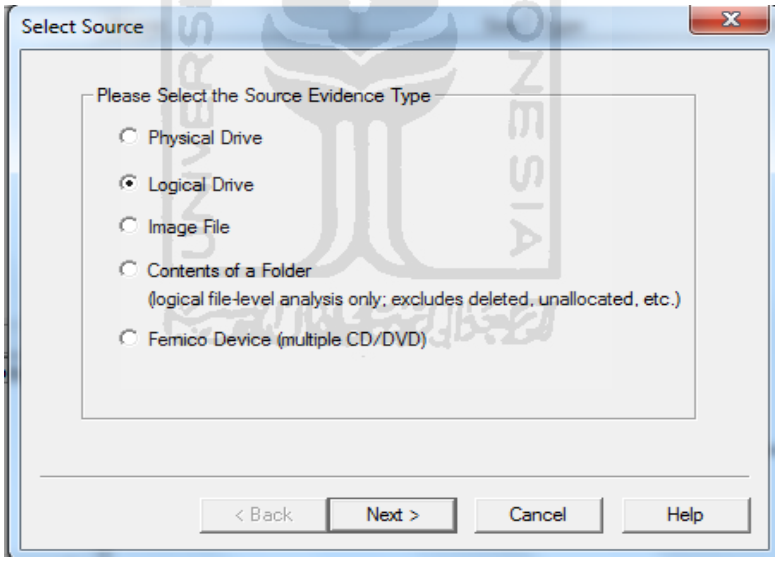
a) Setelah installasi *FTK image*r selesai, maka akan keluar tampilan awal *FTK image*r kemudian klik *file* > *Create Disk Image* > *Next*. Pada kasus ini penulis membuat *image* baru agar bisa dilakukan pengujian data menggunakan *FTK*. Untuk proses pembuatan image baru terdapat pada gambar 3.2.



Gambar 3.2. *Create disk image*

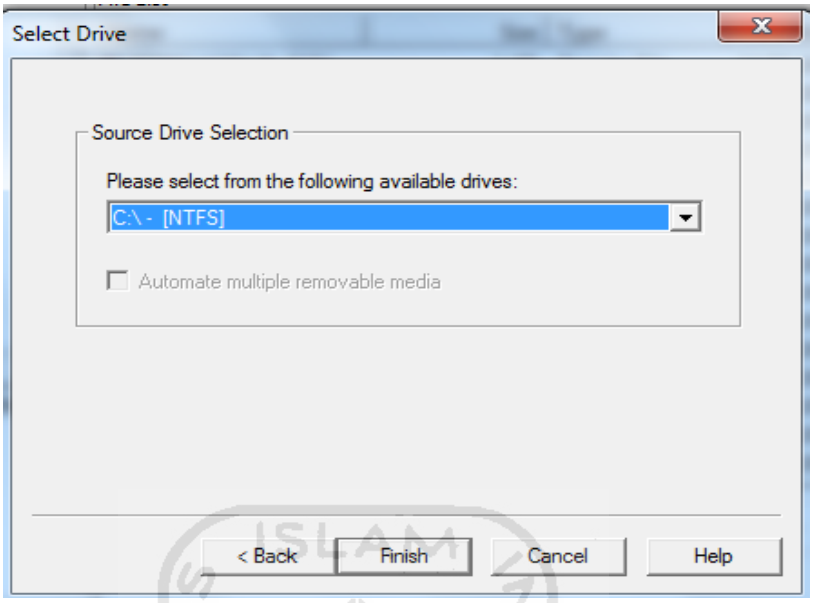
b) Kemudian akan tampil halaman *select source*. Halaman ini penulis dapat memilih untuk melakukan *image* terhadap type apa, pada kasus ini penulis memilih *logical drive* agar lebih mempermudah melakukan pengecekan pada setiap *drive* nya dan waktu yang dibutuhkan relatif lebih singkat. Untuk proses pemilihan source terlihat pada gambar 3.3. Ada beberapa pilihan *source evidence type* yaitu :

a. *Phisical Drive*, digunakan untuk mengimage disk secara keseluruhan.
b. *Logical drive*, pada digunakan unutk memilih partisi yang ingin di*image*.
c. *Image* File, digunakan untuk mengkoversi *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 3.3. Halaman *select source*

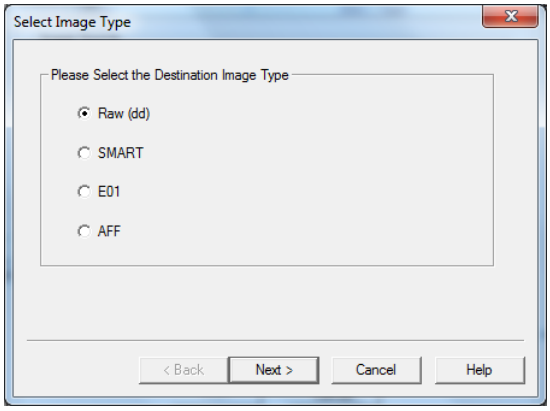
c) Selanjutnya pilih drive mana yang akan di *image* terlebih dahulu, disini penulis memilih C :\[NTFS], yaitu local disk dari sistem operasi. Klik finish untuk mengakhiri. Proses *Select Drive* terlihat pada gambar 3.4 dibawah ini.



Gambar 3.4 *Select drive*

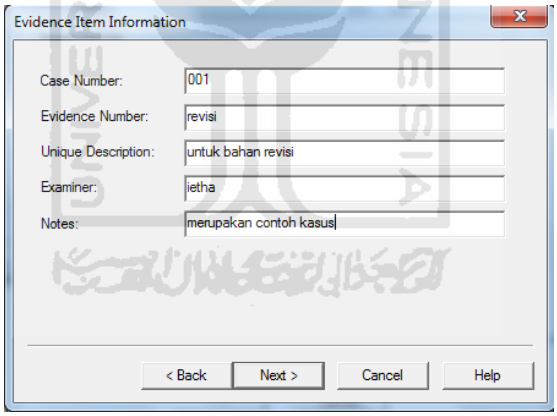
d) Selanjutnya akan diminta untuk menentukan *image destination* atau dimana disk *image* nya akan disimpan, klik *add* sehingga kemudian akan tampil halaman *select image type*, dan klik *next* untuk melanjutkan, untuk lebih jelasna dapat dilihat pada gambar 3.5 *Select Image Type*. Ada beberapa tipe *image* diantaranya :

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



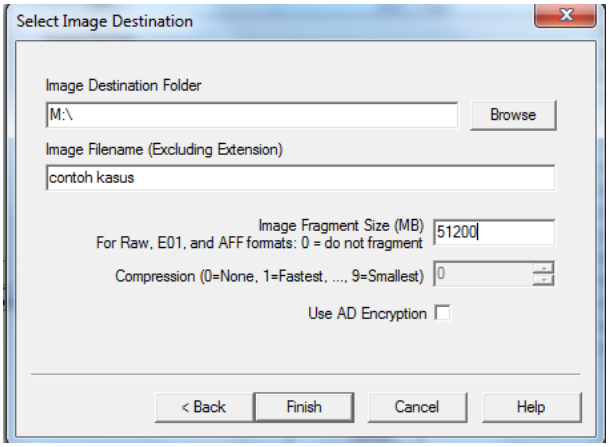
Gambar 3.5 *Select image type*

e) Selanjutnya akan diminta untuk mengisi *evidence item information*, halaman ini digunakan untuk membuat nama file serta informasi mengenai *evidence* yang akan dibuat. Klik *next* untuk melanjutkan. Hal ini digambarkan pada gambar 3.6 berikut ini.



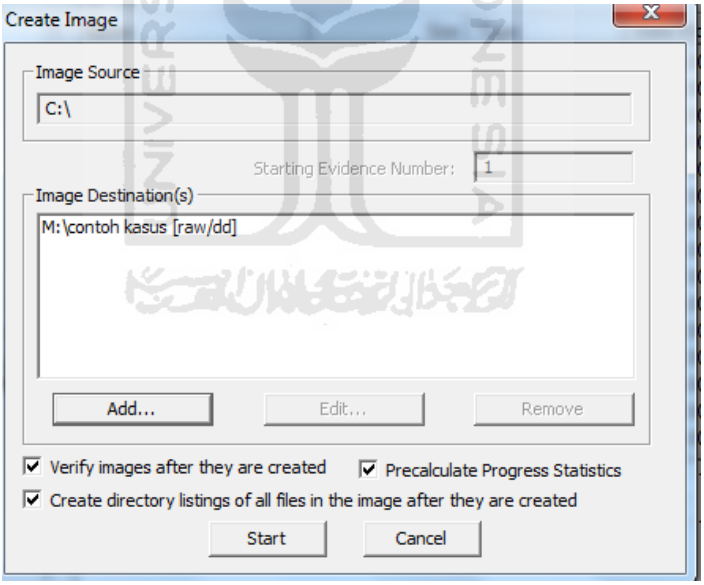
Gambar 3.6. *Evidence item information*

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 3.7 dibawah ini. Klik *finish* untuk mengakhiri.



Gambar 3.7. *Select image destination*

g) Setelah penambahan *image destination* selesai maka akan tampil halaman seperti pada gambar 3.8 berikut ini. Klik *Start* untuk memulai proses *imaging* data dan *cancel* untuk membatalkan.



Gambar 3.8. *Imaging* data dapat dimulai

3.2.2 Pengecekan data dan analisis menggunakan *FTK*

Setelah *imaging* data selesai maka tahapan selanjutnya adalah pengujian atau pengecekan barang bukti agar kemudian dapat dianalisa secara forensik. Pada *FTK* terdapat beberapa opsi diantara nya :

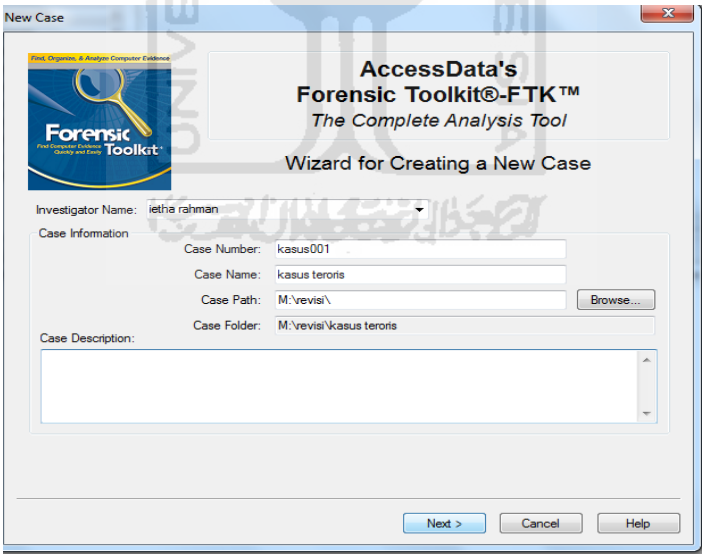
a. *Start new case*, digunakan untuk membuat *case* baru dari *image* file yang ada.

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

c. Preview *evidence*, digunakan untuk melihat *evidence* yang telah dibuat.

Pada kasus ini penulis menggunakan opsi *start new case*, untuk dapat membuat kasus baru dari *image* yang telah dibuat sebelumnya. Setelah *KFF Library Error* dilewati, kita sebaiknya mengisikan informasi berita yang berkaitan dengan kasus ini, misalnya nama penyidik dan nama kasus serta uraian mengenai kasus tersebut. Hal ini berada pada tampilan *new case.*

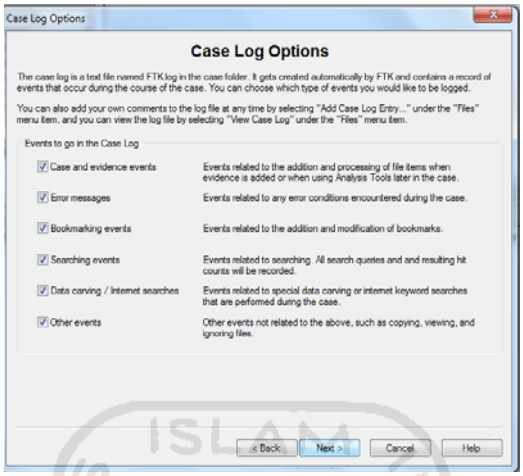
a) Ketika akan membuat *case* baru, maka akan tampil halaman *new case*, pada halaman ini akan diminta untuk mengisi informasi yang berkaitan dengan kasus ini, misal nama penyidik dan nama kasus serta uraian mengenai kasus tersebut. Proses pembuatan case baru terlihat pada gambar 3.9 berikut ini.



Gambar 3.9. Halaman *new case*

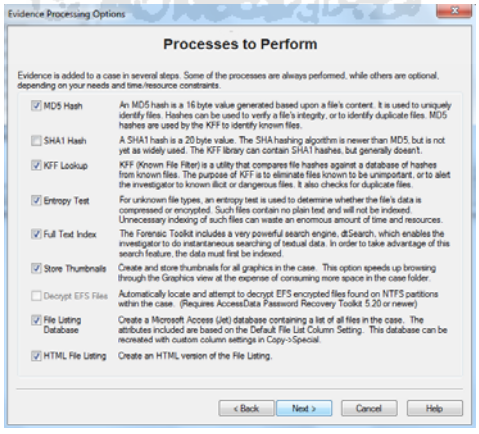
b) Selama masa penyidikan *FTK* akan membaut file bernama *ftk.log* yang mencatat aktivitas yang dilakukan pada *case*. Kita bisa menentukan *event*

apa saja yang akan dicatat. Hal ini akan terdapat pada gambar 3.10 halaman *case log options.*



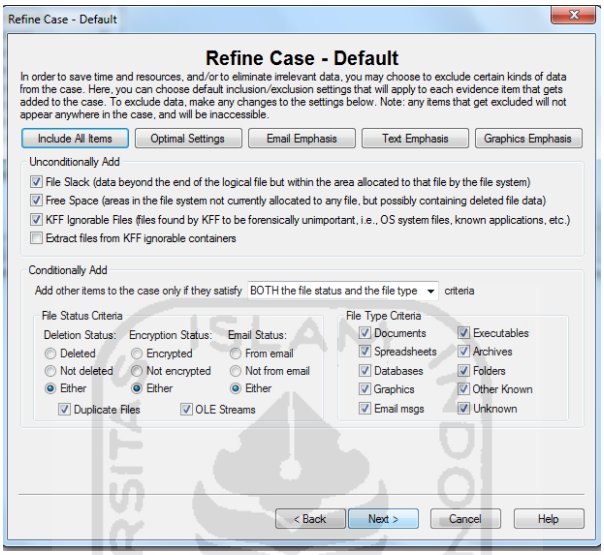
Gambar 3.10. Halaman *case log options*

c) Selanjutnya kita akan menentukan *option* untuk pemrosesan *evidence*, pilihlah proses yang relevan dengan *evidence* yang akan ditambah ke *case*. Contoh : jika *case* terutama memuat gambar maka tidak perlu melakukan index pada *evidence*, sedangkan bila kasus tidak memuat gambar maka tidak perlu menyimpan *thumbnail*. Seperti yang terdapat pada gambar 3.11 *evidence processing options*.



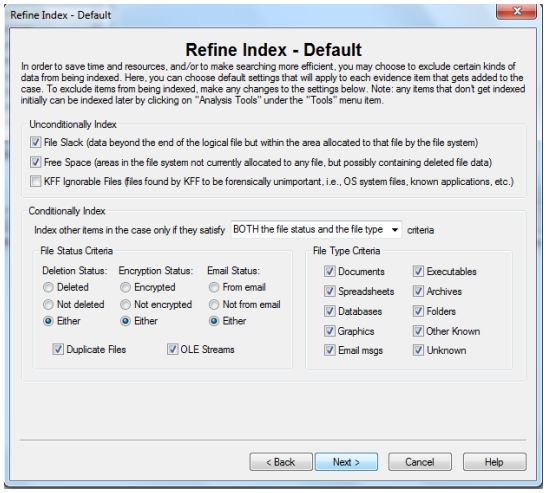
Gambar 3.11. *Evidence processing options*

d) *Refine case* memungkinkan kita untuk mengecualikan sejumlah data dari *case*. Tujuannya untuk menghemat waktu dan sumber data, menghilangkan data yang tidak relevan. terdapat pada gambar 3.12 *refine case*.



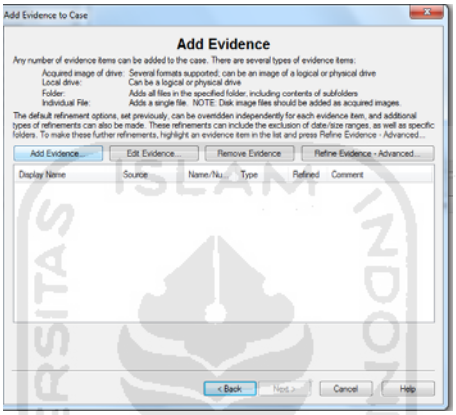
Gamabr 3.12. *Refine case*

e) Selanjutnya adalah *refine index*, halaman ini membantu menentukan tipe data yang tidak ingin diindeks. Index file dibuat setelah pembuatan suatu *case*, tetapi pembuatan suatu *evidence* item bisa diindex kapan saja. Seperti yang terlihat pada gambar 3.13 refine index



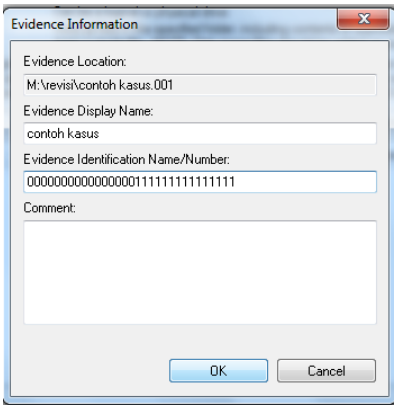
Gambar 3.13. *Refine index*

f) *Add evidence* untuk menambah, mengurangi, mengelola informasi dan parameter *evidence*. *Evidence* yang ditambahkan pada saat *new case wizard* adalah bagian dari *case*. Contoh, kita bisa menambahkan *evidence* dari sejumlah floppy, ZIP disk, dan hardisk. Dan bisa memilih *evidence* dari *image* (bila terdiri dari sejumlah potongan, tempatkan pada suatu direktori), drive, file dan folder. Proses *add evidence* terlihat pada gambar 3.14 berikut ini



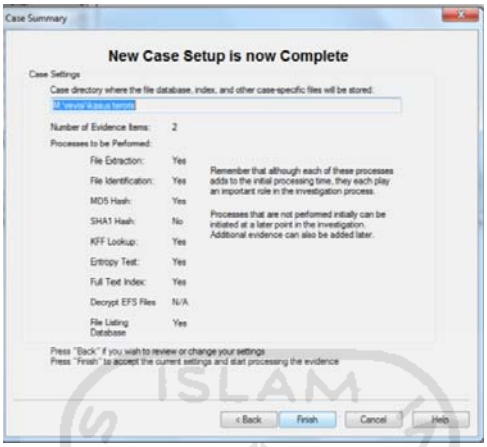
Gambar 3.14. *Add evidence*

g) Selanjutnya dapat memilih file *image* yang ingin kita cek atau kita uji. Contohnya *Contoh Kasus.001*. kemudian perlu menambahkan informasi mengenai *evidence* tersebut, seperti *evidence display name*, *evidence identification name/number serta comment*. Untuk lebih jelasnya dapat melihat gambar 3.15 dibawah ini



Gambar 3.15. *Evidence information*

h) Dan FTK akan memulai melakukan pengumpulan data dari file *image* agar selanjutnya bisa dibaca atau diuji. Seperti yang terdapat pada gambar 3.16 mengenai *case summary.*



Gambar 3.16. *Case summary*

Setelah pengujian *image* selesai dilakukan, selanjutnya akan dilakukan analisis forensik terhadap data yang telah diperoleh. Diantaranya : *Document, Email Messages, From Email, Deleted Files, Data base, Other Thumbnail, Folder* serta Log jaringan.

Dengan melakukan pengecekan terhadap data – data diatas diharapkan akan ditemukan bukti – bukti yang bersangkutan dengan kasus, sebagai contoh file atau data yang telah dihapus atau log dari suatu jaringan, tersangka mengakses situs apa saja, informasi apa saja yang ingin diketahui serta juga bisa mengecek email yang keluar masuk. Setelah data diperoleh baru akan dapat dilakukan analisis apakah tersangka terlibat dengan kasus tersebut atau tidak, selama masa pengujian seorang ahli forensik harus teliti dan jeli dalam melakukan pengecekan terhadap barang bukti agar tidak terjadi kesalahan dan bukti tersebut dapat diajukan kepengadilan.

Ada beberapa tahapan ketika barang bukti ditemukan :

1. *Document* , ketika salah satu file atau document ditemukan maka tahapan pertama adalah mengecek isi dari dokumen tersebut, selanjutnya tanggal

berapa dokumen tersebut terakhir dimofikasi , apakah file tersebut masih ada sehingga dari informasi yang diperoleh akan dapat disimpul kan bahwa file tersebut berhubungan dengan kasus yang telah terjadi.

2. *Deleted files*, akan dilakukan pengecekan satu persatu terhadap file yang telah didelete. Apakah ada file – file tertentu yang sengaja dihapus untuk menutupi sesuatu.
3. *Email message dan from email*, pengecekan terhadap isi email, siapa pengirimnya, kepada siapa dikirimnya serta informasi – informasi yang kira - kira berkaitan dengan kasus.
4. *Other thumbnail*, pengecekan terhadap gambar apa saja yang terdapat dikomputer tersangka, jika kasusnya berkaitan dengan kasus teroris maka akan dicari foto – foto yang yang memungkin kan berkaitan dengan kasus.
5. Log jaringan, akan dilakukan pengecekan apa saja yang pernah di akses oleh orang tersebut, dia pernah melakukan apa saja dijaringan nya sehingga akan diketahui indikasi yang sedang terjadi.

Dari beberapa contoh pilihan diatas dapat diketahui bahwa untuk mendapatkan bukti forensik digital diperlukan pengecekan secara teliti dengan cara pengecekan item – by – item dan juga bisa pengecekan menggunakan *link search* untuk lebih mempermudah penyelidikan, namun penyidik harus tau *keyword* yang akan digunakan untuk pencarian atau *search*.

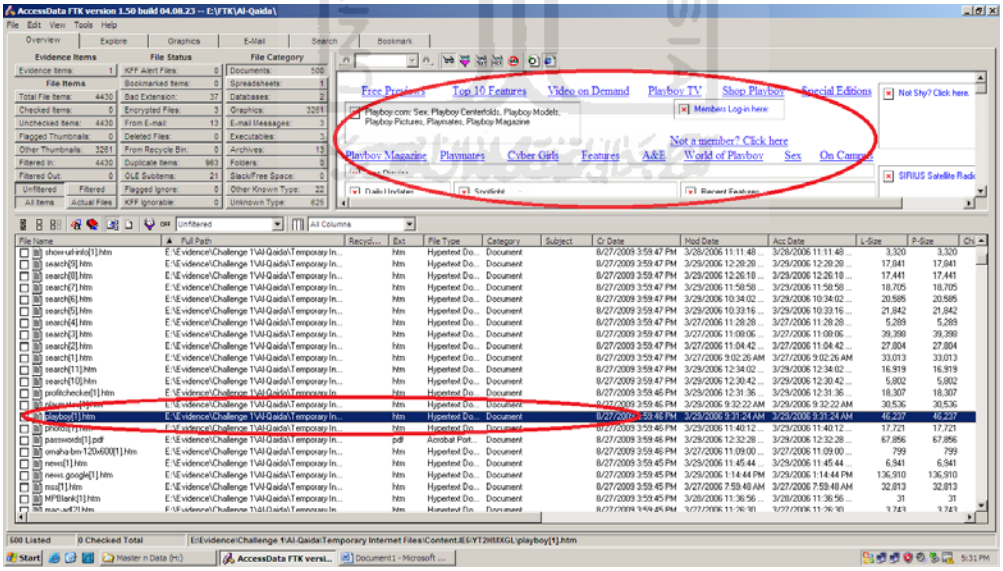
BAB IV

HASIL DAN PEMBAHASAN

Sebelum mendapatkan bukti dari sebuah kasus dibutuhkan untuk melakukan pengecekan terhadap file dari masing – masing tombol yang telah tersedia pada FTK sehingga kemudian akan diperoleh bukti terhadap kasus yang sedang diselidiki.

4.1 Hasil dan Pembahasan Tombol *Document*

Pada tombol *Document* segala informasi yang berkaitan dengan dokumen akan ditemukan,baik itu yang berekstensi doc, txt, pdf serta file html yang pernah diakses dan disimpan. Seperti contoh pada gambar 4.1 terdapat informasi dokumen berekstensi.htm yang mana file tersebut terlihat bahwa file tersebut merupakan halaman daripada salah satu situs dewasa yaitu playboy. Dari gambar tersebut diketahui bahwa tersangka pernah mengakses situs dewasa.

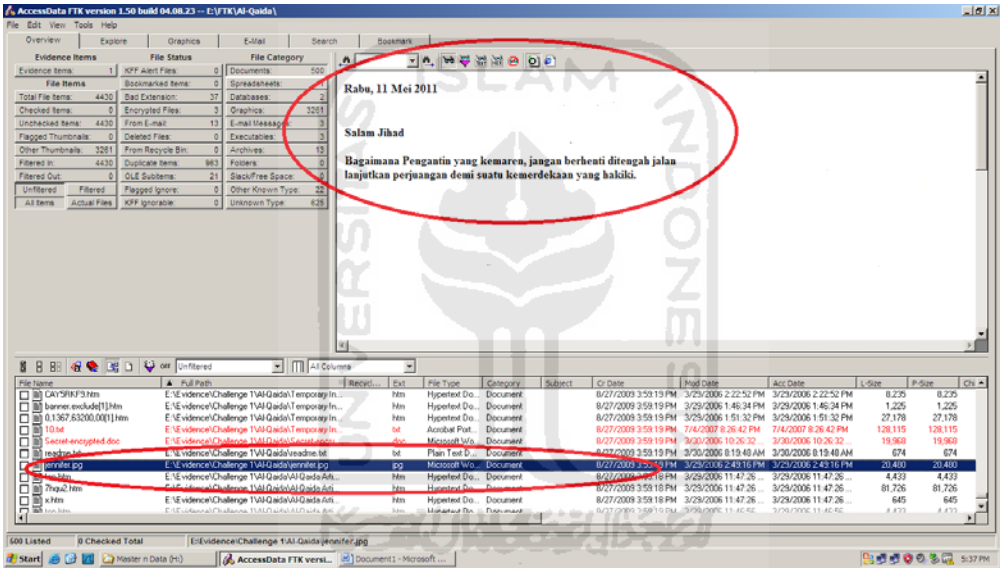


Gambar 4.1. Tampilan *document* dengan *file htm*

Disamping file htm, pada tombol *Document* juga dapat ditemukan file yang terengkripsi seperti .pdf yang diberi password sehingga kita tidak bisa

mengakses file tersebut. Selama masa penyelidikan kita dapat menanyakan password dari file tersebut atau juga bisa menggunakan tools tertentu untuk membuka file tersebut.

Selain dai bukti diatas juga ditemukan sebuah *email* yang mungkin di attachdan kemudian disimpan menggunakan ekstensi.jpeg sehingga jika dilihat secara langsung tidak akan kelihatan bahwa file tersebut adalah file word. Hal ini menimbulkan kecurigaan karena kata – kata pada surat tersebut mengandung kata – kata yang lazim digunakan oleh teroris. Seperti pada gambar 4.2

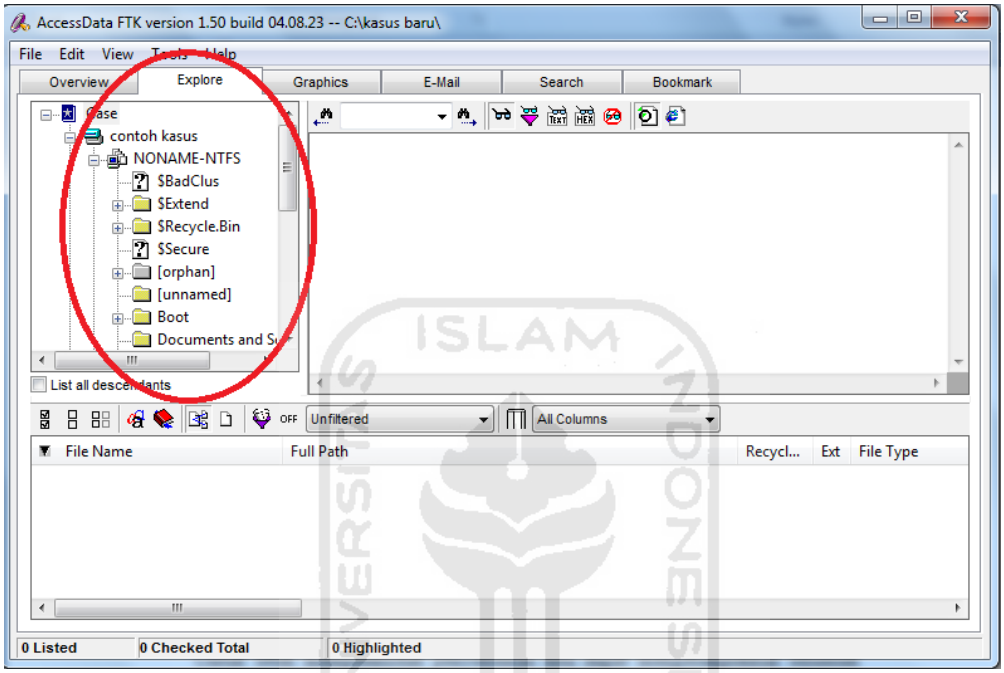


Gambar 4.2. Bukti berbentuk dokumen

4.2 Hasil dan Pembahasan Tombol Folder

Dari case yang telah dibuat, setiap *button* bisa memunculkan informasi yang di inginkan, kita bisa klik *button* folders untuk melihat semua folder yang ada. Tanda silang menyatakan direktori tersebut telah dihapus. Untuk melihat properties suatu direktori, klik kanan lalu pilih File properties, maka infomrasi yang akan tampil adalah informasi semacam ukuran file, posisi sector dan cluster, hashing dan enkripsi serta yang berkaitan dengan case. Disamping itu untuk melihat folder – folder yang terdapat pada sistem dapat menggunakan tombol

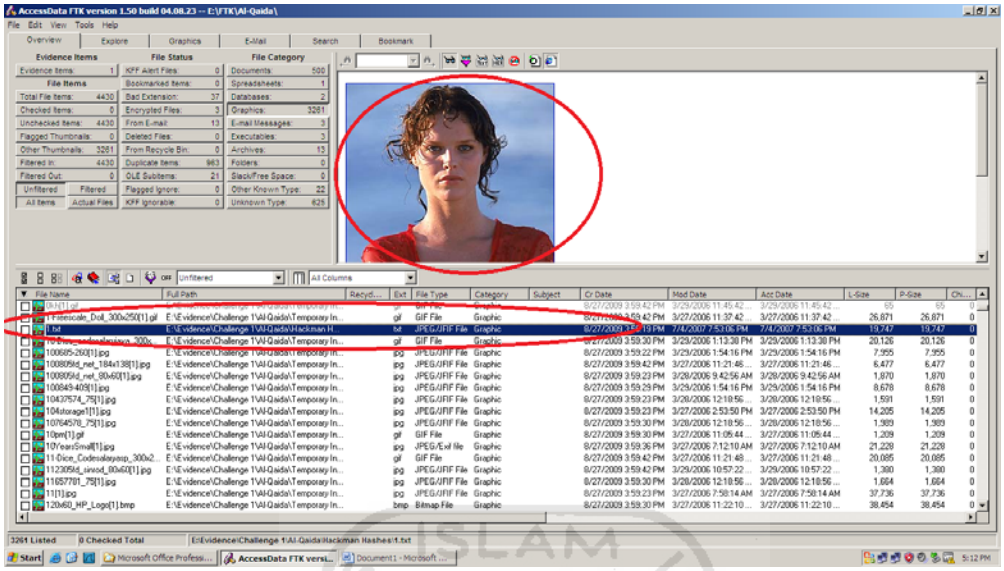
explore yang mana pada tombol ini berisi tentang semua yang terdapat disistem seperti my documnet, program file, windows serta file – file [*orphan*] atau yang telah dihapus. Seperti yang terdapat pada gambar 4.2 berikut ini.



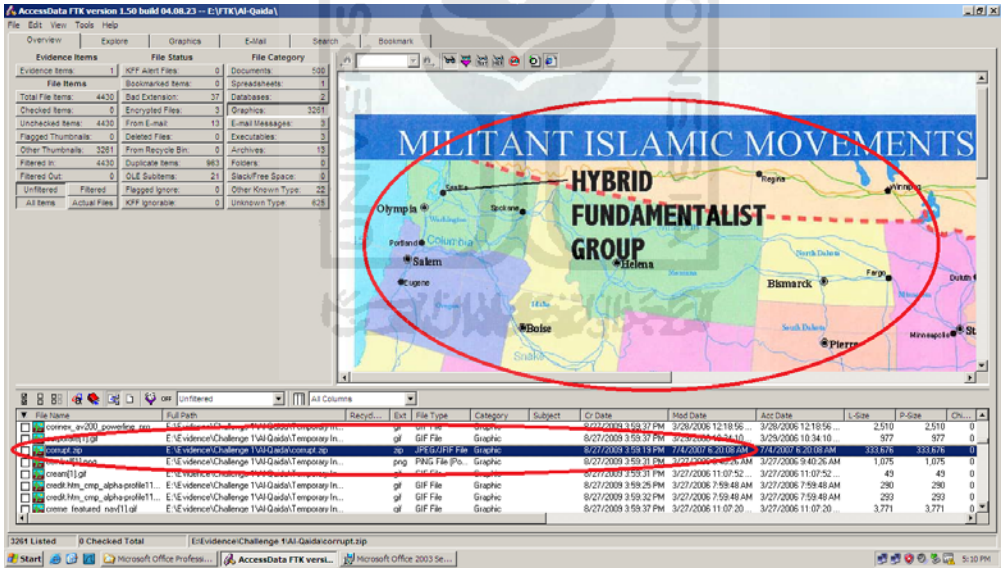
Gambar 4.3. Tampilan *explore*

4.3 Hasil dan Pembahasan Tombol *Other Thumbnail* dan *Graphics*

Tombol *other thumbnail* dan *graphics* memiliki persamaan yaitu sama – sama menampilkan bukti berbentuk grapik atau thumbnaill yang berekstensi jpeg, gif dan sebagainya. dari case yang telah dibuat ditemukan beberapa foto yang mengarah terhadap kasus yaitu indikasi teroris dan pornografi dan foto tersebut telah diubah ekstensinya menjadi .txt untuk salah satu bukti pornografi dan .zip untuk salah satu bukti teroris seperti yang terdapat pada gambar 4.3 sebagai bukti dari pornografi dan gambar 4.4 sebagai bukti teroris dibawah ini.



Gambar 4.4. *Evidence* pornografi



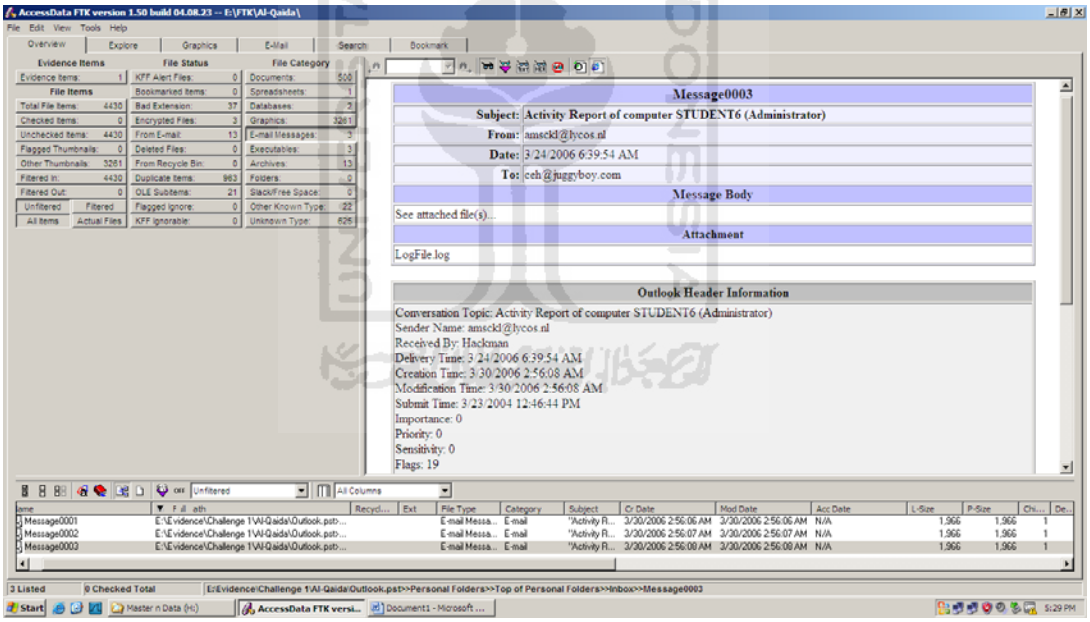
Gambar 4.5. *Evidence* teroris

Dari kedua gambar diatas, dikatakan bahwa gambar tersebut bisa dijadikan bukti dikarenakan ada kesengajaan perubahan ekstensi pada kedua gambar yang semula berektensi .jpeg diganti menjadi .txt dan .zip. Hal ini menyebab kan

kecurigaan bahwa gambar tersebut sengaja diedit untuk menutupi bukti yang ada namun jika kita menggunakan FTK perubahan pada file tersebut menjadi terlihat. Karena file yang telah di ubah ekstensinya dan tidak sesuai dengan ekstensi asli maka link file tersebut akan berubah warna menjadi warna merah dan standart dari file – file yang ada berwarna hitam.

4.4 Hasil dan Pembahasan *Email Messages* dan *From Email*

Pada tombol *Email messages* dan *from email* terdapat persamaan yaitu sama- sama berisi pesan email yang masuk dan keluar namun beda nya pada from email akan terlihat inbox, outbox, dan sebagainya. dihalaman email message akan terlihat siapa pengirim email, siapa yang menerima email serta kapan email tersebut dikirim. Seperti yang terdapat pada gambar 4.6 dibawah ini.

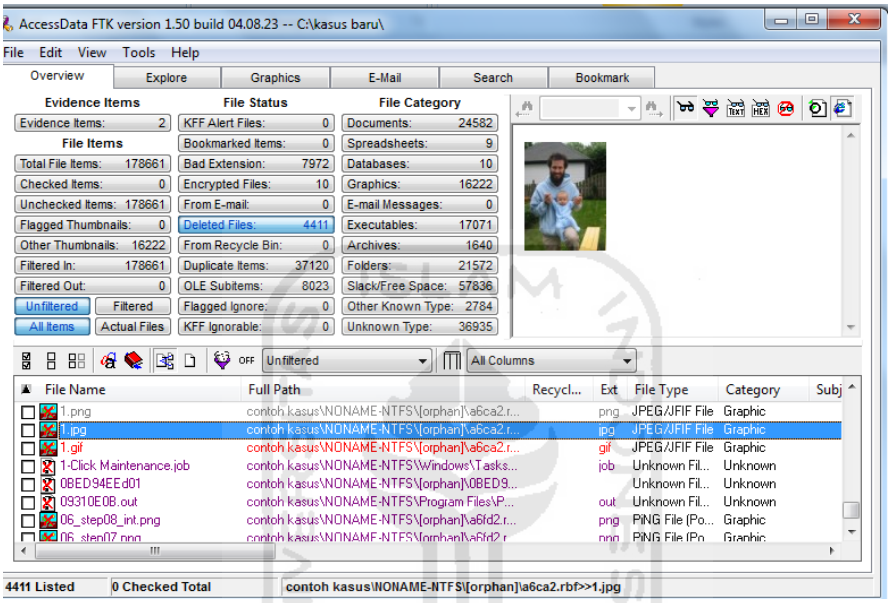


Gambar 4.6. Tampilan *email messages*

4.5 Hasil dan Pembahasan *Deleted Files*

Dihalaman ini akan menampilkan file – file yangtelah terhapus, sebagian dari file tersebut masih bisa dibuka namun sebagian ya lagi sudah tidak bisa dibuka, jika terdapat suatu file yang dicurigai berkaitan dengan kasus dan file

tersebut telah dihapus maka kita masih dapat memperoleh file tersebut kembali, baik yan secara langsung bisa diakses ataupun harus menggunakan tools tertentu untuk recovey data yang telah dihapus tersebut. Ketika suatu file telah dihapus atau terhapus maka file yang akan tampil berwarna merah dan ungu dan ada tanda silang pada file tersebut, seperti yang terdapat pada gambar 4.7 berikut ini

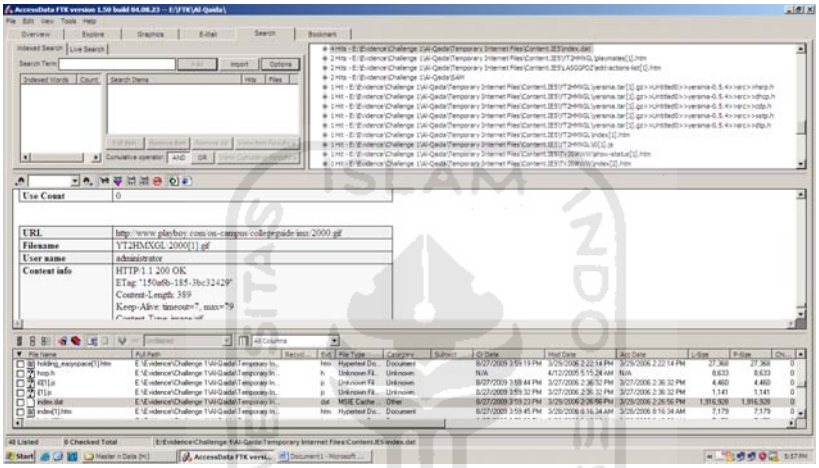


Gambar 4.7. Tampilan *deleted files*

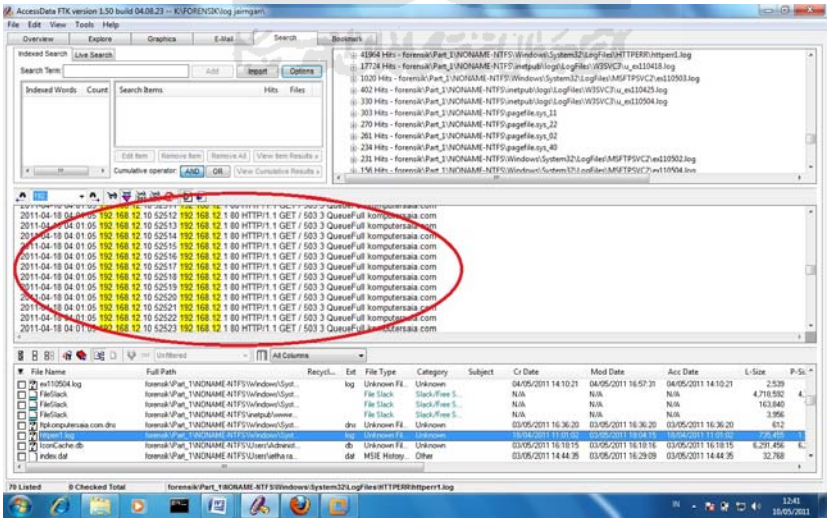
4.6 Hasil dan Pembahasan Log Jaringan

Ada beberapa cara untuk mendapatkan bukti log jaringan, bisa menggunakan from email, *ole subitems* serta bisa menggunakan tombol seacrh. Untuk lebih mempermudah pencarian log tersebut bisa mengunakan index seacrch dengan cara memasuk kan *keyword* yang diinginkan. Jika ingin mengecek history browsingnya bisa menggunakan key word http dan *keyword* ini juga bisa digunakan untuk pencarian Ip address dari suatu sistem yang pernah terkoneksi dengan sistem tersangka. Disamping itu juga bisa menggunakan *keyword* log, namun dengan menggunakan *keyword* – *keyword* tersebut akan membutuhkan ketelitian terhadap pengecekan data karena dari file yang telah terfilter harus dicek satu persatu.

Untuk mengetahui ada aktivitas ilegal yang pernah dilakukan oleh tersangka kita harus mencari tau dahulu ip yang digunakan oleh tersangka atau yang pernah digunakannya, setelah ip tersebut diketahui bisa dijadikan *keyword* untuk mencari aktivitas apa saja yang telah dilakukan oleh orang tersebut. Pada kasus ini diketahui situs apa saja yang pernah diakses oleh tersangka seperti pada gambar 4.8, serta aktivitas ilegal yang terekam disistem sepeti yang terdapat pada gambar 4.9.



Gambar 4.8. Log *history*

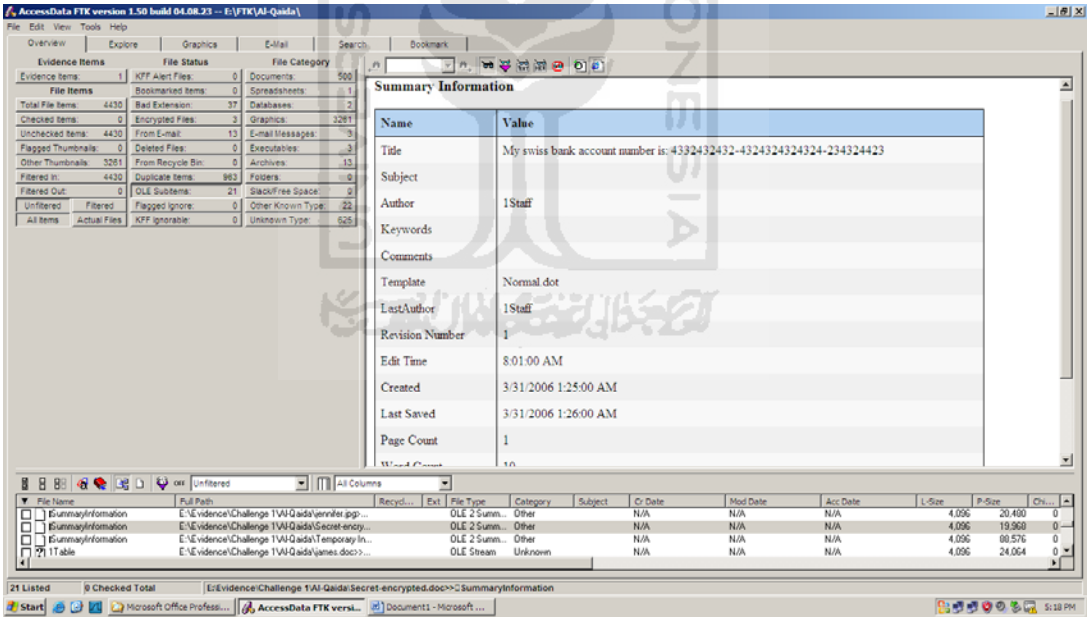


Gambar 4.9. Log jaringan berbentuk aktivitas ilegal

Dari gambar 4.8 diperoleh bukti bahwa tersangka pernah mengakses situs www.playboy .com, sedangkan untuk gambar 4.9 diasumsikan tersangka pernah mencoba melakukan serangan terhadap sistem dengan ip 192.168.12.1 yang kemungkinan besar aktivitas tersebut adalah DoS atau DdoS.

4.7 Hasil dan Pembahasan Tombol – Tombol yang Lainnya

Selain tombol – tombol yang telah dijelaskan diatas ada beberapa tombol lain yang mendukung untuk pencarian brang bukti, seperti *ole subitems*. Pada tombol ini ditemukan beberapa file yang indikasinya berkaitan dengan kasus yaitu *summary information* yang berisi informasi keuangan yang berkaitan dengan nomor rekening bank swiss, sehingga dapat diasumskan bahwa terjadi suatu transaksi keuangan diantara tersangka dengan rekannya, seperti yang terdapat pada gambar 4.10. berikut ini



Gambar 4.10. Informasi keuangan

Selain tombol *ole subitems* juga terdapat tombol *bad extention* dan *encrypted files*. Tombol *bad extention* berisi file – file yang tidak sesuai ekstensinya atau file – file yang telah diubah ekstensinya. Misal, dari .jpeg diganti menjadi .txt dan file – file yang telah terhapus. Sedangkan *encrypted files* berisi

file – file yang terenkripsi atau dilindungi password sehingga harus dimasuk kan password dahulu baru file tersebut bisa diakses.

Untuk lebih mempermudah penyelidikan kita dapat mengelompokkan sejumlah file. Seperti namanya, bookmark bisa membantu untuk dengan cepat mengamati sejumlah bukti. Untuk membuat bookmark file yang akan ditambahkan ke *bookmark* perlu ditandai atau dicheck terlebih dahulu pada tab overview.

Untuk memeriksa kemungkinan image mengalami kerusakan, misal hardisk yang dipakai untuk menyidik mengalami error, maka kita bisa menggunakan fitur dari *tools* > *Verify Image Integrity*. Namun pengujian ini memakan waktu yang lama. Bila ada *evidence* yang pernah ditambah ke case tetapi belum dianalisa secara lengkap, maka dengan memanfaatkan menu tools > Analysis Tools, dan kemudian dapat membuat serta index file. Sederhananya *searching* bisa dilakukan secara live atau dengan memanfaatkan index. *Live search* lebih fleksibel tetapi memakan waktu yang lebih lama. Dukungan ekspresi reguler akan lebih mempermudah untuk menemukan data dengan pola yang di inginkan.

Untuk mendapatkan bukti – bukti diatas diperlukan nya kejelian dan ketelitian dari *examiner* dalam mencari bukti dan menganalisanya. Karena unutk mendapatkan *evidence* tersebut harus dicek satu persatu dan itu membutuhkan waktu yang lama serta pemahaman terhadap kasus dan sistem itu sendiri, sebagai contoh untuk dapat menyimpulkan suatu file tersebut merupakan salah satu bukti yang bisa diajukan kepengadilan seorang *examiner* harus paham akan konsep bukti itu sendiri seperti log jaringan tentang aktivitas ilegal yang telah dilakukan oleh tersangka, jika kita tidak paham akan konsep aktivitas ilegal maka bukti yang berkaitan dengan hal tersebut tidak akan ditemukan.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah melakukan implementasi dan pengujian, dapat diambil kesimpulan:

a. Sebelum hasil *imaging* dapat dianalisa secara forensik, maka harus dilakukan pengecekan satu persatu terhadap file yang telah *dimage* sehingga akan diketahui file mana saja yang berkaitan dengan kasus.
b. Dengan menggunakan FTK akan diketahui file – file yang telah dirubah ekstensinya sehingga akan lebih mempermudah pencarian terhadap data yang telah dimanipulasi serta yang telah dihapus.
c. Untuk dapat menganalisa suatu *evidence*, seorang penyidik bukti digital harus paham akan konsep bukti itu sendiri, sistem operasi yang akan di cek serta paham akan konsep jaringan dan serangan.
d. Bukti digital yang akan di image dapat berupa phisical drive dan bisa berupa logical drive.

5.2 Saran

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

a. Tombol – tombol yang ada pada FTK kurang maksimal karena ada beberapa tombol yang memiliki fungsi hampir sama sehingga ketika harus dicek satu persatu maka akan memakan waktu yang cukup lama.
b. Ketika akan menggunakan FTK alangkah lebih baiknya jika kita pahami terlebih dahulu kasus yang akan diselidiki dan dianalisis.

DAFTAR PUSTAKA

[BEL07] *Pengenalan Jaringan, 2007*. Diakses dari : http://belajarit.um.ac.id/index.php/jaringan/18-pengenalan-jaringan-komputer/48-ftp-server.html. Pada 5 mei 2011, pukul 15.20

[GIR10] Girin Digdo. 2010. *DoS, Flooding dan DdoS*. Diakses Dari : http://10108262.blog.unikom.ac.id/dos-*flooding*-dan.g9. Pada 17 januari 2011, 22:17

[INF09] *[info] Cara Dan Langkah Hacking sebuah Situs, 2009* . Diakses dari : http://bansurya.blogspot.com/p/info.html. Pada 21 januari 2011, 11:35

[NEO04] Neotek. Vol.IV No.6. *Computer Forensics Menjadi Cyber Detectives.* Jakarta: NeoTek Maju Mandiri.

[SUL08] Sulianta, Feri. 2008. *Computer forensic*. Jakarta : Alex Media Komputindo.

[UTD05] Utdrartatmo, Fiffar. 2005. *Cara Mudah Menguasai Computer forensic dan Aplikasinya*. Yogyakarta : Graha Ilmu.

[WOR10] *Digital Forensic untuk Tangkap Maling Internet, 2010.* diakses dari : http://worldfriend.web.id/digital-forensic-untuk-tangkap-maling-internet-. Pada 19 januari 2011, 22:51

[YAN10] Yanto,S,Si. 2010. *Computer forensic*. Diakses Dari : http://yanto-ssi.blogspot.com/2010/05/komputer-forensik.html. Pada 10 januari 2011, 22:57