PERBANDINGAN APLIKASI RECOVERY HARD DISK UNTUK KEPENTINGAN FORENSIK

TUGAS AKHIR

Oleh :

Raja Husnul Khatimah **3310801100**

Jesni Herlina **3310801119**

Disusun untuk memenuhi syarat kelulusan Program Diploma III

PROGRAM STUDI TEKNIK INFORMATIKA

POLITEKNIK NEGERI BATAM

BATAM

2011

LEMBAR PENGESAHAN

Batam, 16 Februari 2011

Pembimbing,

Agus Fatulloh

NIK. 107051

LEMBAR PERNYATAAN

Dengan ini, saya:

NIM : 3310801100

Nama : Raja Husnul Khatimah

adalah mahasiswa Teknik Informatika Politeknik Negeri Batamyang menyatakan bahwa tugas akhir dengan judul:

Perbandingan Aplikasi Recovery Hard disk untuk Kepentingan Forensik

disusun dengan:

1. Tidak melakukan plagiat terhadap naskah karya orang lain
2. Tidak melakukan pemalsuan data
3. Tidak menggunakan karya orang lain tanpa menyebut sumber asli atau tanpa ijin pemilik

Jika kemudian terbukti terjadi pelanggaran terhadap pernyataan di atas, maka saya bersedia menerima sanksi apapun termasuk pencabutan gelar akademik.

Lembar pernyataan ini juga memberikan hak kepada Politeknik Negeri Batam untuk mempergunakan, mendistribusikan ataupun memproduksi ulang seluruh hasil Tugas Akhir ini.

Batam, 16 Februari 2011

Raja Husnul Khatimah
3310801100

LEMBAR PERNYATAAN

Dengan ini, saya:

NIM : 3310801119

Nama : Jesni Herlina

adalah mahasiswa Teknik Informatika Politeknik Negeri Batam yang menyatakan bahwa tugas akhir dengan judul:

Perbandingan Aplikasi Recovery Hard disk untuk Kepentingan Forensik

disusun dengan:

1. Tidak melakukan plagiat terhadap naskah karya orang lain
2. Tidak melakukan pemalsuan data
3. Tidak menggunakan karya orang lain tanpa menyebut sumber asli atau tanpa ijin pemilik

Jika kemudian terbukti terjadi pelanggaran terhadap pernyataan di atas, maka saya bersedia menerima sanksi apapun termasuk pencabutan gelar akademik.

Lembar pernyataan ini juga memberikan hak kepada Politeknik Negeri Batam untuk mempergunakan, mendistribusikan ataupun memproduksi ulang seluruh hasil Tugas Akhir ini.

Batam, 16 Februari 2011

Jesni Herlina
3310801119

KATA PENGANTAR

Puji syukur atas kehadirat Tuhan Yang Maha Esa atas karunia-Nya penyusun dapat menyelesaikan Tugas Akhir yang berjudul "Perbandingan Aplikasi Recovery Hard disk untuk Kepentingan Forensik".

Dalam kesempatan ini, penyusun ingin menyampaikan ucapan terima kasih kepada pihak-pihak yang telah membantu proses penyelesaian Tugas Akhir ini yaitu:

1. Allah SWT yang telah memberikan kesehatan dan keselamatan dalam menyelesaikan Tugas Akhir ini.
2. Orangtua dan keluarga yang telah memberikan dukungan baik moral maupun materi.
3. Bapak Dr. Ir. Priyono Eko Santoyo selaku Direktur Politeknik Batam.
4. Bapak Uuf Brajawidagda selaku koordinator Tugas Akhir.
5. Bapak Agus Fatulloh selaku Dosen Pembimbing Tugas Akhir yang telah membimbing penulis dengan baik sehingga penulis bisa menyelesaikan Tugas Akhir ini.
6. Dosen-dosen Teknik Informatika yang telah memberikan kritik dan saran.
7. Sahabat dan teman-teman yang tidak dapat kami sebutkan satu per satu yang telah membantu penyusun dalam menyelesaikan Tugas Akhir ini.

Penyusun juga menyadari bahwa masih terdapat kekurangan dalam penyusunan Tugas Akhir ini. Untuk itu, penyusun mengharapkan kritik dan saran yang membangun dari pihak-pihak lain. Semoga Tugas Akhir ini dapat bermanfaat bagi pembaca, khususnya bagi yang ingin mengembangkan analisis serupa.

Batam, 16 Februari 2011

Penyusun

ABSTRAK

PERBANDINGAN APLIKASI RECOVERY HARD DISK UNTUK KEPENTINGAN FORENSIK

Forensik adalah sebuah ilmu pengetahuan yang ditujukan untuk membantu proses pengadilan, terutama dalam bidang pembuktian. Hal ini diperlukan dalam menganalisa atau menemukan barang bukti, yang bisa dimanfaatkan dalam kasus tertentu. Forensik bukan hanya dikenal di bidang kepolisian dan kedokteran tetapi dapat terjadi juga pada teknologi informasi dan komunikasi. Dengan adanya perkembangan teknologi informasi dan komunikasi dapat menyebabkan terjadinya kejahatan atau penyelewengan di dunia teknologi informasi. Untuk menghindari kejahatan tersebut, maka dibutuhkan komputer forensik dalam menangani penyelewengan pada teknologi informasi.

Kegiatan komputer forensik yaitu sebagai proses mengidentifikasi, memelihara, menganalisa dan mempergunakan bukti digital menurut hukum yang berlaku. Komputer forensik dikelompokkan dalam beberapa bidang diantaranya, Internet Forensik, Network Forensik, Disk Forensik, System Forensik, dan lainnya. Dari berbagai bidang tersebut disk forensik merupakan salah satu bidang yang sering digunakan. Disk forensik adalah ilmu yang membahas tentang bukti fisik meliputi penghapusan data dan kehilangan data yang terjadi pada disk penyimpanan seperti *hard disk.*

Kata kunci :komputer forensik, *hard disk,* aplikasi *recovery*.

ABSTRACT

COMPARISON OF HARD DISK RECOVERY APPLICATIONS FOR FORENSIC INTEREST

Forensics is a science that is intended to assist the court process, particularly in the field of verification. It is necessary to analyze or find the evidence, which can be used in certain cases. Forensics is not just known in the field of police and medicine but can occur also in information and communication technology. With the development of information and communication technology can lead to crime or fraud in the world of information technology. To avoid crime, computer forensics is needed in dealing with fraud on information technology.

Forensic computer activities namely as a process of identifying, maintaining, analyzing and using digital evidence under applicable law. Computer forensics are grouped in several areas including, Internet Forensics, Network Forensics, Forensic Disk, System Forensics, and others. Of the various fields of forensic disk is one area that is often used. Disk forensics is the science which deals with physical evidence includes the deletion of data and data loss that occurs in the disk storage such as hard disks.

Index Terms: computer forensics, hard disk recovery application.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

Bab I Pendahuluan

I.1 Latar Belakang

Forensik adalah sebuah ilmu pengetahuan yang ditujukan untuk membantu proses pengadilan, terutama dalam bidang pembuktian. Hal ini diperlukan dalam menganalisa atau menemukan barang bukti, yang bisa dimanfaatkan dalam kasus tertentu. Forensik bukan hanya dikenal di bidang kepolisian dan kedokteran tetapi dapat terjadi juga pada teknologi informasi dan komunikasi. Dengan adanya perkembangan teknologi informasi dan komunikasi dapat menyebabkan terjadinya kejahatan atau penyelewengan di dunia teknologi informasi.

Pada tahun 2008 terbentuk Undang-Undang ITE yang bertujuan untuk mengatur informasi agar berjalan sesuai dengan etika bertransaksi. Namun, UU ITE ini kurang memberikan arahan dalam proses hukum di Indonesia. Dikarenakan UU ini hanya menjelaskan tentang peraturan perpindahan informasi elektronik secara umum. Selain itu, terdapat juga hal-hal yang bersifat mendalam dari persoalan kasus hukum di Indonesia yang belum diatur dalam UU. Hal yang bersifat mendalam ini dapat dijadikan sebagai acuan dalam teknologi informasi untuk membentuk sistem hukum yang baik dalam komputer forensik.

Kegiatan komputer forensik yaitu sebagai proses mengidentifikasi, memelihara, menganalisa dan mempergunakan bukti digital menurut hukum yang berlaku. Komputer forensik dikelompokkan dalam beberapa bidang diantaranya, Internet Forensik, Network Forensik, Disk Forensik, System Forensik, dan lainnya. Dari berbagai bidang tersebut disk forensik merupakan salah satu bidang yang sering digunakan. Disk forensik adalah ilmu yang membahas tentang bukti fisik meliputi penghapusan data dan kehilangan data yang terjadi pada disk penyimpanan seperti *hard disk.*

I.2 Rumusan Masalah

Rumusan masalah dari Tugas Akhir ini adalah bagaimana menentukan aplikasi *recovery hard disk* untuk kepentingan forensik yang terbaik dalam hal pengembalian data.

I.3 Batasan Masalah

Adapun batasan masalah dari penyelesaian Tugas Akhir ini adalah:

1. Melakukan perbandingan dengan beberapa aplikasi *recovery hard dsik* diantaranya: PC Inspector File Recovey, Pandora Recovery, Data Recovery, Photorec, TestDisk, dan Recuva.
2. Hanya menganalisis data *recovery* yang diakibatkan dari kerusakan non fisik.
3. Hanya menggunakan sistem operasi Windows.

I.4 Tujuan

Tujuan dari Tugas Akhir ini adalah mengetahui aplikasi *recovery* yang terbaik dalam pengembalian data berdasarkan kebutuhan forensik.

I.5 Sistematika Penulisan

Sistematika Penulisan ini terdiri dari 6 (enam) bab dengan rincian sebagai berikut:

Bab 1 Pendahuluan, berisi tentang penjelasan latar belakang analisis, rumusan masalah, batasan masalah, tujuan penelitian serta sistematika penulisan untuk memberikan gambaran isi laporan tugas akhir ini.

Bab 2 Tinjauan Pustaka, berisi tentang teori-teori yang berhubungan dengan Perbandingan Aplikasi *Recovery Hard disk* untuk Kepentingan Forensik.

Bab 3 Analisis Kebutuhan, berisi penjelasan tentang kebutuhan forensik dengan menggunakan aplikasi recovery yang mampu memenuhi kebutuhan forensik tersebut.

Bab 4 Pengujian, hasil dari pengujian yang dilakukan.

Bab 5 Hasil pengujian, berisi tentang hasil yang didapatkan dari pengujian yang telah dilakukan, dengan membandingkan aplikasi yang telah diuji.

Bab 6 Kesimpulan dan Saran, berisi tentang kesimpulan dari analisis perbandingan aplikasi *recovery* dan saran untuk pengembangan analisis tersebut.

Bab II Tinjauan Pustaka

Bab ini membahas tentang kebutuhan dalam analisis Perbandingan Aplikasi *Recovery* untuk Kepentingan Forensik, yang berupa media penyimpanan, yaitu *hard disk* dengan cara menganalisa pengetahuan proses kinerja *hard disk* dan aplikasi yang digunakan dalam melakukan data *recovery*, serta menganalis kegiatan forensik yang menjadi kebutuhan dalam memecahkan sebuah kasus kriminal.

II.1 Komputer Forensik

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. 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 kriteriakriteria, demikian juga dengan proses pembuktian pada bukti yang didapat dari komputer. Di awal tahun 1970-an Kongres Amerika Serikat mulai merealisasikan kelemahan hukum yang ada dan mencari solusi terbaru yang lebih cepat dalam penyelesaian kejahatan komputer. US Federals Rules of Evidence 1976 menyatakan permasalahan tersebut. Hukum lainnya yang menyatakan permasalahan tersebut adalah:

1. Economic Espionage Act 1996, berhubungan dengan pencurian rahasia dagang
2. The Electronic Comunications Privacy Act 1986, berkaitan dengan penyadapan peralatan elektronik.

3. The Computer Security Act 1987 (Public Law 100-235), berkaitan dengan keamanan sistem komputer pemerintah

Forensik adalah suatu proses ilmiah (didasari ilmu pengetahuan) dalam mengumpulkan, menganalisa, dan menghadirkan berbagai bukti dalam sidang pengadilan terkait adanya suatu kasus hukum. Kekuatan dari forensik adalah memungkinkan analisa dan mendapatkan kembali fakta dari kejadian lingkungan. Tentu tidak mudah mendapatkan atau menemukan fakta, karena fakta itu tersembunyi adanya.

Definisi komputer forensik menurut para ahli :

1. Menurut Marcella secara terminologi, komputer forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti komputer dalam kejahatan komputer. Istilah ini relatif baru dalam bidang komputer dan teknologi, tapi telah muncul diluar *term* teknologi (berhubungan dengan investigasi dan investigasi bukti-bukti intelejen dalam penegakan hukum dan militer) sejak pertengahan tahun 1980-an.
2. Menurut Budhisantoso, komputer forensik belum dikenali sebagai suatu disiplin pengetahun yang formal. Dalam hal ini definisi komputer forensik adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sedemikian sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum.
3. Menurut Noblett, yaitu berperan untuk mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer.

4. Menurut Judd Robin, yaitu penerapan secara sederhana dari penyidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin.
5. Menurut Ruby Alamsyah (salah seorang ahli forensik IT Indonesia), digital forensik atau terkadang disebut komputer forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital tersebut termasuk handphone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa.

Definisi komputer forensik dalam arti sederhana yaitu penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan menggunakan *software* dan tool untuk mengambil dan memelihara barang bukti tindakan kriminal.

Berbagai fakta dan bukti tersembunyi yang melingkupi forensik secara umum misalnya, darah, struktur gigi seseorang, riwayat kesehatan, sidik jari dan lainnya harus dianalisa sedemikian rupa sehingga didapatkan fakta yang layak untuk diajukan sebagai barang bukti. Metodologi dalam forensik pasti berubah, mengingat ilmu pengetahuan yang mendasarinya pun berubah. Apapun itu perubahannya, pastinya membawa kepada pembaruan dan metode yang lebih baik dengan dimunculkan bidang keilmuan dan pengetahuan baru.

Bidang forensik sudah berkembang lama, dan ini diawali oleh seorang tabib yang bernama Hi Duan Yu yang dapat mengkategorikan berbagai seseorang didapati meninggal, misalnya saja karena faktor (usia muda, tengelam, akibat benturan, atau bahkan mati dicekik).

Metode forensik pun berkembang sampai pada akhirnya menggunakan DNA. Meskipun DNA menjadi suatu pembuktian yang sangat kuat saat ini dalam forensik, tidak demikian dulu adanya. DNA menjadi bagian dari pembuktian

dalam forensik sudah dipahami lama, dan setelah hamper 20 tahun kemudian baru diterima dalam pengadilan Amerika Serikat, tentunya menjalani proses yang panjang.

Bukan hanya subjek yang berubah dan meluas, prosesnya pun banyak mengalami perubahan. Hal ini pun meluas ke bidang-bidang teknologi baru. bahkan saat ini terdapat istilah komputer forensik yang mulai mencuat akhir-akhir ini. Berbeda dari forensik pada umumnya, komputer forensik adalah pengumpulan dan analisa data dari berbagai sumber daya komputer, seperti: system komputer, jaringan komputer, jalur komunikasi(mencakup secara fisik dan *wireless*) dan juga berbagai berbagai media penyimpanan yang dikatakan layak untuk diajukan dalam sidang pengadilan. komputer forensik menjadi bidang ilmu baru yang terkait dua bidang keilmuan, yaitu hukum dan komputer.

Komputer forensik atau *digital* forensik banyak ditempatkan dalam berbagai keperluan, bukan hanya dalam kasus-kasus criminal yang melibatkan hukum. Secara umum kebutuhan komputer forensik dapat digolongkan sebagai berikut:

1. Keperluan investigasi tindak kriminal dan perkara pelanggaran.
2. Rekontruksi duduk perkara insiden keamanan komputer.
3. Upaya-upaya pemulihan akan kerusakan system.
4. Troubleshooting yang melibatkan *hardware* dan *software*.
5. Keperluan memahami system ataupun berbagai perangkat *digital* dengan lebih baik.

Ilmu forensik yang berkaitan dengan komputer atau disebut dengan komputer forensik. Komputer forensik merupakan cabang ilmu pengetahuan baru yang mengombinasikan antara ilmu komputer dan ilmu hukum. Kegiatan komputer forensik adalah suatu proses mengidentifikasi, memelihara, menganalisa, dan mempergunakan bukti *digital* menurut hukum yang berlaku. Dengan tujuan untuk menjabarkan sebuah system komputer berupa media penyimpanan, salah satunya

ialah *hard disk* dan sebuah dokumen elektronik, seperti dokumen dalam bentuk *image*, teks, *archive*, video, audio dan lain-lain.

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

1. E-mail, alamat e-mail
2. *File*wordprocessor/spreadsheet
3. Source code perangkat lunak
4. *File* berbentuk *image*(.jpeg, .tip, dan sebagainya)
5. Web Browser bookmarks, cookies
6. 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 sehingga bukti *digital* dapat dijamin keasliannya dan dapat dipertanggung jawabkan.

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

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

3. Lengkap, artinya bukti bisa dikatakan bagus dan lengkap jika di dalamnya terdapat banyak petunjuk yang dapat membantu investigasi.
4. 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 pegambilan 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.

Dalam melakukan prosesnya, forensik melibatkan tiga komponen yang dirangkai dan melibatkan tiga komponen yang dirangkai dan dikelola disedemikian rupa menjadi tujuan dengan segala kelayakan dan kualitas.
Tiga komponen ini mencakup:

1. Manusia (*people*)
2. Peralatan (*Equipment*)
3. Aturan (*Protocol*)

Manusia (*People)*, diperlukan kualifikasi untuk mencapai manusia yang berkualitas. Memang mudah untuk belajar komputer forensik, tetapi untuk menjadi ahlinya, dibutuhkan lebih dari sekadar pengetahuan dan pengalaman.
Peralatan (*Equipment*), diperlukan sejumlah perangkat atau alat yang tepat untuk mendapatkan sejumlah bukti (*evidence*) yang dapat dipercaya dan bukan sekadar bukti palsu.
Aturan (Protocol), diperlukan dalam menggali, mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat. Dalam komponen aturan,

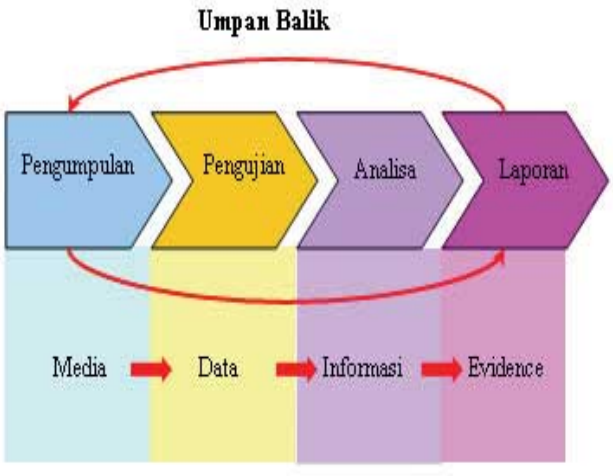
diperlukan pemahaman yang baik dalam segi hukum dan etika, kalau perlu dalam menyelesaikan sebuah kasus perlu melibatkan peran konsultasi yang mencakup pengetahuan akan teknologi informasi.

Antara Manusia (*people*), Peralatan (*Equipment*), Aturan (*Protocol*) akan melebur dan bergabung untuk mengisi setiap fase-fase dalam komputer forensik.

Ada empat fase dalam komputer forensik, antara lain:

1. Pengumpulan
2. Pengujian
3. Analisa
4. 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. Berikut ini merupakan fase-fase yang dilakukan komputer forensik.



Gambar 1 Tahap-Tahap Komputer Forensik

II.2 Kebutuhan Forensik

Pada saat ini jumlah kejahatan yang telah melibatkan komputer sudah berkembang dengan sangat pesat, yang mengakibatkan perusahaan dan institusi berusaha untuk membantu hukum melacak tentang siapa, apa, dimana, kapan dan bagaimana sebuah kejahatan terjadi. Forensik akan mengumpulkan, menganalisa, dan menghadirkan berbagai bukti yang dibutuhkan dalam kasus tertentu. Didalam ilmu forensik terdapat beberapa ilmu forensik lainnya yang dikenal antara lain ilmu fisika forensik, ilmu kimia forensik, ilmu psikologi forensik, ilmu kedokteran forensik, ilmu toksikologi forensik, ilmu psikiatri forensik, komputer forensik, dan sebagainya. Ilmu forensik yang biasa digunakan dalam teknologi informasi dan komunikasi yaitu komputer forensik. Komputer forensik dikelompokkan lagi dalam beberapa bidang diantaranya, Internet Forensik, Network Forensik, Disk Forensik, System Forensik, dan lainnya. Diantara bidang-bidang tersebut disk forensik merupakan bidang yang paling sering digunakan. Disk forensik adalah ilmu yang membahas tentang bukti fisik meliputi penghapusan data dan kehilangan data yang terjadi pada disk penyimpanan seperti hard disk.

Ada empat fase dalam komputer forensik, antara lain:

II.2.1 Pengumpulan Data

Pengumpulan data merupakan langkah pertama dalam proses forensik untuk mengidentifikasi sumber-sumber potensian dan bagaimana kemudian data dikumpulkan. Pengumpulan ini melibatkan proses dan metode yang semakin komplek karena perkrmbangan teknologi yang semakin pesat.

Pengumpulan data ini mencakup aktivitas seperti:

1. Identifikasi
2. Penamaan *(Labeling)*
3. Perekaman *(Recording)*
4. Mendapatkan Data

Setelah melalui proses identifikasi sumber data, langkah selanjutnya yaitu mendapatkan data tersebut. Ada tiga langkah yang dibutuhkan:

1. Membuat Perancangan untuk Mendapatkan Data

   Membuat perancangan untuk mendapatkan data adalah langkah yang paling penting, ada banyak titik-titik sumber data yang potensial, selain itu untuk mendapatkan data dibutuhkan analisa terhadap data yang layak diprioritaskan. Dalam menentukan prioritas ada tiga faktor yang perlu menjadi pertimbangan, antara lain:

   - Kemiripan nilai. Untuk mengacu kepada nilai yang mirip, tentu *Examiner* membutuhkan pemahaman akan situaasi dan kondisi, mungkin berdasarkan pengalaman sebelumnya, perkiraan yang relevan diperlukan untuk menentukan kemiripan nilai.
   - *Volatile*. Data kategori ini tentunya akan hilang begitu saja sewaktu listrik dimatikan, data-data yang menetap dimemori dan ada karena sistem berjalan akan hilang dengan mudahnya jika listrik mati. Karena alasan inilah data tergolong *volatile* mendapatkan prioritas dibandingkan data-data *non-volatile*. Tetapi prioritas demikian tidaklah mutlak, akan didapati banyak kasus yang ternyata data *non-volatile* harus mendapatkan prioritas salah satu ‘penyimpangan’ dalam bentuk lain, misalnya data yang *non-volatile* pun dapat demikian *liquid*, seperti data log transaksi yang demikian dinamis berubah seiring sistem berjalan.
   - Upaya dalam mendapatkan data. Untuk mendapatkan data dari sumber yang ada tidaklah brgitu saja dapat dilakukan, meskipun secara teknik sangat dimungkinkan, belum tentu jika mempertimbangkan melalui pandangan hukum. Misalnya saja akan lebih mudah mendapatkan sumberkan pada *hard disk*.

2. Mendapatkan Data *(Acquire the data)*

   Tidak selalu dibutuhkan kekuatan yang besar dalam mendapatkan data, seandainya data yang diperlukan memang sudah didapatkan dengan *decurity tools, analysis tools*, atau dengan cara lain.

3. Analisa Integritas Data *(Verify the Integrity of the Data)*

   Setelah data didapatkan, verifikasi penting untuk memerisa integritas data. Verifikasi integritas data mencakup penggunaan tool dalam mengkalkulasi informasi yang orisinil dan kemudian meng-*copy*-nya. Selanjutnya dilakukan analisis yang membandingkan apakah data hasil orisinil sama atau identik.

II.2.2 Pengujian

Setelah melalui proses pengumpulan data, langkah lebih lanjut yaitu melakukan pengujian dalam menilai informasi yang relevan dari data-data yang dikumpulkan. Tahapan ini memerlukan meminimalisasi fitur-fitur sistem operasi dan aplikasi yang mengaburkan data, seperti kompresi, enkripsi, dan akses mekanisme kontrol. *Hard disk* berisi ribuan bahkan jutaan *file*, untuk mengidentifikasi data didalamnya akan sangat menghabiskan konsentrasi dan melelahkan. Filtrasi akan mengeliminir sebagian data yang tidak dibutuhkan, misalnya data log minggu lalu yang terdiri dari jutaan *record* dan didapati belasan *record* yang digunakan untuk pemeriksaan lebih lanjut. Ada banyak peralatan dan teknik digunakan dalam melakukan eliminasi terhadap tumpukan data. Pencarian basis teks dan berbagai pola tertentu dapat digunakan untuk mengidentifikasi ketepatan suatu data, seperti pencarian terhadap dokumen yang berhubungan dengan seseorang atau pokok permasalahan tertentu.

II.2.3 Analisis

Begitu informasi diekstrak, *examiner* (pemeriksaan) melakukan kesimpulan dalam menggambarkan data. Analisa yang dimaksud tentunya mengambil pendekatan metodis dalam menghasilkan kesimpulan yang berkualitas didasarkan pasa ketersediaan data. Tugas *examiner* mencakup kegiatan seperti mengidentifikasi *user* atau orang di luar dari pengguna mengidentifikasi lokasi, barang-barang, kejadian dan menentukan bagaimana komponen-komponen tadi terelasi satu dengan yang lain sehingga didapati kesimpulan pada akhirnya, tentunya kompleksitas memunculkan banyak sumber data.

II.2.4 Pelaporan dan Dokumentasi

Reporting adalah tahap akhir dari proses komputer forensik, dalam tahap ini yang dilakukan yaitu mempresentasikan informasi yang merupakan hasil dari proses analisis. Banyak faktor yang mempengaruhi reporting, seperti berikut ini:

1. *Alternative Explanations* (Penjelasan Alternatif)

   Jika informasi yang mengacu pada suatu kasus dikategorikan incomplete, tentunya hasil akhir tidak memadai dan tidak dapat diandalkan untuk menulusuri kejadian. Bahkan jika didapati beberapa penjelasan yang masuk akal akan suatu kejadian, masing-masing harus dipertimbangkan dan diteruskan dalam proses reporting.

   Apapun yang terjadi, analisa harus menggunakan pendekatan dalam menentukan setuju atau menolak setiap penjelasan perkara yang mungkin dilakukan.

2. *Audience Consideration* (Pertimbangan Peserta)

   Menyajikan data atau informasi pada hadirin atau *audience* sangat penting. Kasus yang melibatkan perundangan tentunya membutuhkan laporan *detail*/spesifik berkenaan informasi yang dikumpulkan, dan membutuhkan pula *copy* dari setiap fakta yang diperoleh.

Pertimbangan ini beralasan, misalnya saja administrator sistem mungkin ingin melihat lebih jauh *network traffic* lebih men*detail*.

3. *Actionable Information*

   Proses *reporting* mencakup pula identifikasi *Actionable Information* yang didapat dari data-data terdahulu, dan mendapatkan informasi. Misalnya saja daftar alamat seseorang dapat dikembangkan lebih lanjut, yang kemudian, mengarah pada informasi lain tentang suatu tindak kriminal/kejadian. Keuntungan lain dari *Actionable Information* yaitu informasi yang didapatkan mungkin dapat digunakan dalam keperluan mendatang.

Berdasarkan penjelasan diatas, forensik merupakan suatu pekerjaan identifikasi sampai dengan muncul hasil yang teratur menurut urutan waktu. Sangat tidak mungkin forensik dimulai dengan munculnya hasil tanpa ada penelitian yang mendalam dari bukti-bukti yang ada. Investigator harus mampu menyaring informasi dari bukti yang ada tetapi tanpa merubah keaslian bukti tersebut. Adanya dua istilah dalam manajemen barang bukti, antara lain *The chain of custody* dan rules of *evidence*, jelas akan membantu investigator dalam mengungkap suatu kasus. Dapat dijelaskan seperti berikut:

1. *The chain of custody*

   Satu hal terpenting yang dilakukan investigator untuk melindungi bukti adalah *The chain of custody*. Maksud istilah tersebut adalah pemeliharaan dengan meminimalisir kerusakan yang diakibatkan karena investigasi. Barang bukti harus benar-benar asli atau jika sudah tersentuh investigator, pesan-pesan yang ditimbulkan dari bukti tersebut tidak hilang. Tujuan dari *The chain of custody*, yaitu bukti itu benar-benar masih asli/orisinil dan saat persidangan, bukti masih bisa dikatakan seperti pada saat ditemukan.

2. *Rules of evidence*

   Manajemen bukti kejahatan komputer juga mengenal istilah peraturan barang bukti*(rules of evidence).* Arti istilah ini adalah barang bukti harus memiliki hubungan yang relevan dengan kasus yang ada.

Metodologi yang digunakan dalam menginvestigasi kejahatan dalam teknologi informasi dibagi menjadi dua :

1. *Search & Seizure*

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

2. Pencarian Informasi

   Beberapa tahapan dalam pencarian informasi khususnya dalam bidang teknologi informasi, salah satunya adalah melakukan penyitaan media penyimpanan data*(data storages)* yang dianggap dapat membantu proses penyidikan.

Pada tahun 2008 lahirlah UU ITE yang bertujuan untuk mengatur transfer informasi elektronik agar berjalan sesuai dengan etika bertransaksi informasi elektronik. Berikut ini merupakan isi dari UU ITE :

Undang-Undang ITE (Informasi dan Transaksi Elektonik)

Bab 1 : Ketentuan Umum

Pasal 1:

Dalam Undang-Undang ini yang dimaksud dengan:

(1). Informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (*EDI*), surat elektronik (*electronic mail)*, telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

(2). Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.

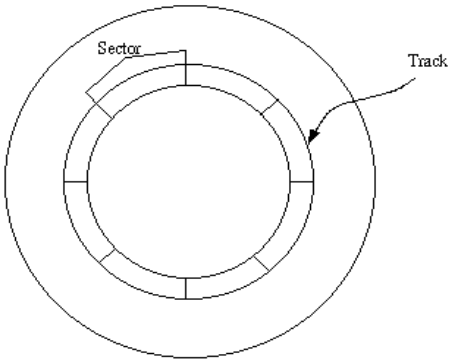
(3). Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.

(4). Dokumen elektronik adalah Isetiap nformasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

(5). Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.

II.3 Hard disk

Hard disk merupakan *hardware* (perangkat keras) yang digunakan sebagai media penyimpanan data pada laptop atau komputer yaitu terdiri dari piringan magnetis yang keras dan berputar, serta komponen-komponen elektronik lainnya. Biasanya piringan magnetis atau *disk* adalah piringan bundar yang terbuat dari bahan tertentu (logam atau plastik) dengan permukaan dilapisi bahan yang dapat di magnetisasi. *Hard disk* bisa disebut juga dengan cakram keras berbentuk piringan hitam terbuat dari alumunium dan dilapisi bahan magnetic.



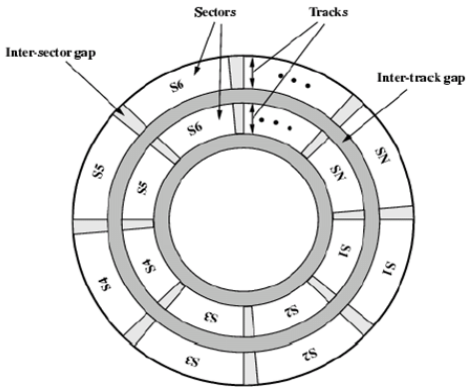
Gambar 2 *Track* dan *Sector*

Gambar di atas merupakan contoh dari sebuah *track* adalah bagian lingkaran *disk*, sedangkan contoh sebuah *sector* adalah bagian dari *track*. Biasanya, sebuah *sector* memiliki jumlah 512 byte. Beberapa *sector* dikelompokkan menjadi sebuah *cluster*. Pengelompokkan tersebut bisa terjadi pada level *drive* ataupun pada level sistem operasi. Ada 3 hal terjadinya pembentukan bagian-bagian pada *disk*, antara lain: format tingkat rendah, partisi dan format tingkat tinggi.

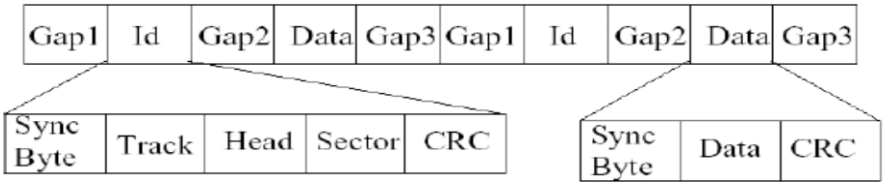
Mekanisme baca/tulis pada *platter* dengan menggunakan kepala baca atau tulis yang disebut *head*, merupakan komparan pengkonduksi (*conducting coil*). Desain fisiknya, *head* bersifat stasioner sedangkan piringan *disk* berputar sesuai kontrolnya. *Layout* data pada *disk* diperlihatkan pada gambar 3. *Disk* diorganisasi

dalam bentuk cincin – cincin konsentris yang disebut *track*. Tiap *track* pada *disk* dipisahkan oleh *gap*. Fungsi gap untuk mencegah atau mengurangi kesalahan pembacaan maupun penulisan yang disebabkan melesetnya *head* atau karena interferensi medan magnet. Sejumlah bit yang sama akan menempati *track – track* yang tersedia. Semakin ke dalam *disk* maka kerapatan (*density*) *disk* akan bertambah besar. Data dikirim ke memori ini dalam bentuk blok, umumnya blok lebih kecil kapasitasnya daripada *track*. Blok – blok data disimpan dalam *disk* yang berukuran blok, yang disebut *sector*. Sehingga *track* biasanya terisi beberapa *sector*, umumnya 10 hingga 100 *sector* tiap *track*nya.

Pada mekanisme membacaan maupun penulisan pada *disk*, *head* harus bisa mengidentifikasi titik awal atau posisi – posisi *sector* maupun *track*. Caranya data yang disimpan akan diberi *head*er data tambahan yang menginformasikan letak *sector* dan *track* suatu data. Tambahan *head*er data ini hanya digunakan oleh sistem *disk drive* saja tanpa bisa diakses oleh pengguna.



Gambar 3 Layout Data *Disk*



Gambar 4 Format Data pada *Track Disk*

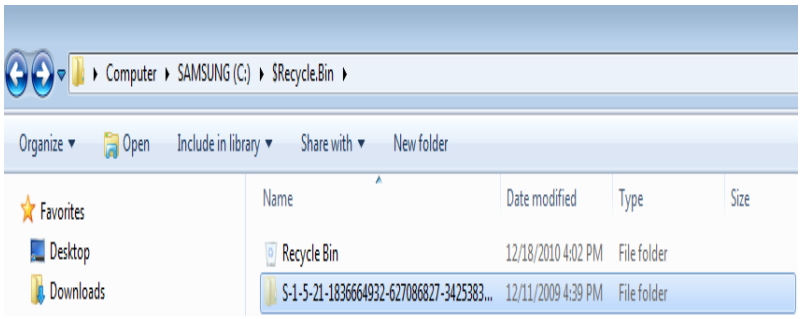
Gambar 4. di atas merupakan gambaran dari pemformatan data pada *disk*. *Field ID* merupakan *head*er data yang digunakan *disk drive* menemukan letak *sector* dan *track*nya. Byte SYNCH adalah pola bit yang menandakan awal field data.

Pada sistem operasi Windows terdapat dua jenis penghapusan sebuah *file*, yaitu:

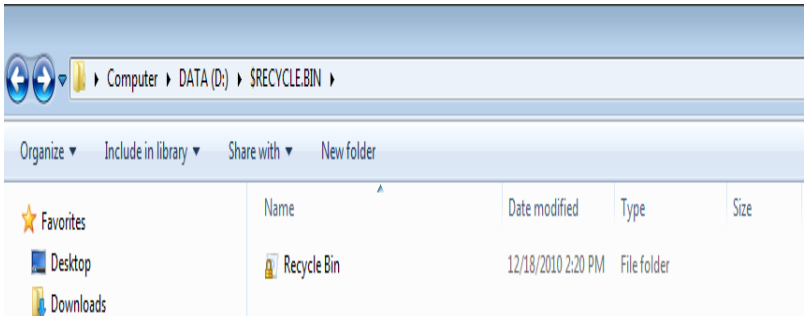
1. Penghapusan Sementara

   Pada saat melakukan penghapusan *file* dengan menggunakan tombol *delete*, sebenarnya *file* tersebut tidak benar-benar terhapus, tetapi *file* tersebut hanya dipindahkan ketempat tertentu, yaitu di Recycle Bin. Tujuannya yaitu agar pada saat *file* tersebut tidak sengaja atau salah menghapus, data tersebut masih bisa mengembalikannya lagi *(restore).*

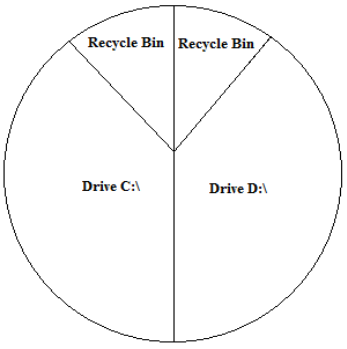
   Ketika Recycle Bin penuh atau kapasitas yang disediakan sudah terisi, maka *file* yang lama akan benar-benar dihapus, sehingga masih tersisa tempat atau ruang untuk menempatkan *file-file* yang baru. Sehingga *file* tersebut hampir tidak bisa dikembalikan lagi kecuali dengan *software* khusus. Recycle Bin yang ada di tampilan desktop merupakan kumpulan dari recycle bin disetiap *drive*. Setiap *drive* memiliki recycle bin. Jika system *file* NTFS, maka folder recycle bin bernama Recycler. Sedangkan *File system* FAT32, maka bernama Recycled. Untuk windows Vista atau Windows 7 dengan nama $Recycle.Bin.



Gambar 5 Recycle Bin pada Drive c:

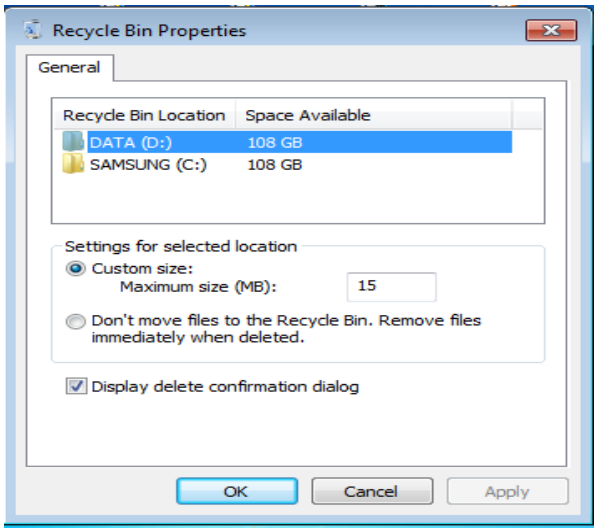


Gambar 6 Recycle Bin pada Drive d:



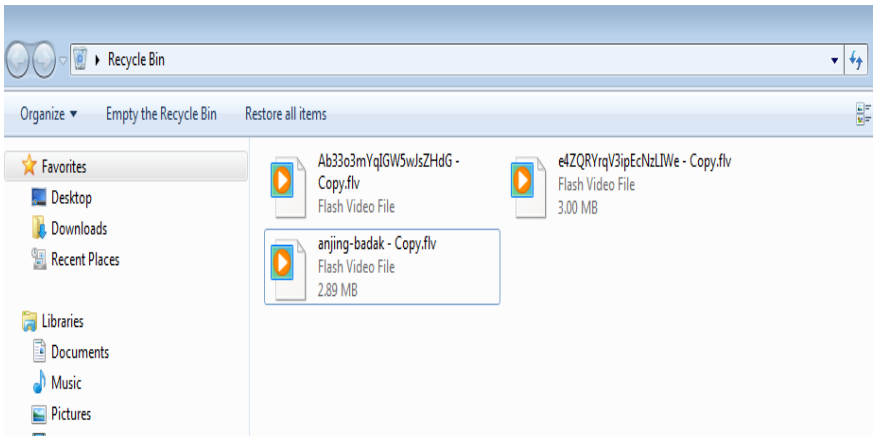
Gambar 7 Pembagian Recycle Bin di Setiap Drive

Saat data dihapus dan kemudian data tersebut pindah ke folder Recycle Bin yang terjadi ialah, ada perubahan *file name* dan *date modified*. Ketika data pindah ke folder recycle bin maka data yang telah dihapus tersebut memiliki nama baru. Jika dibuka maka akan terlihat dimana nama *file* itu berada dan *extention.* Namun, isi data pada recycle bin bisa saja hilang disebabkan melebihi dari batas maksimumnya. Dapat di contohkan, dengan cara melakukan pengaturan ukuran isi Recycle Bin dengan maksimum 15MB.



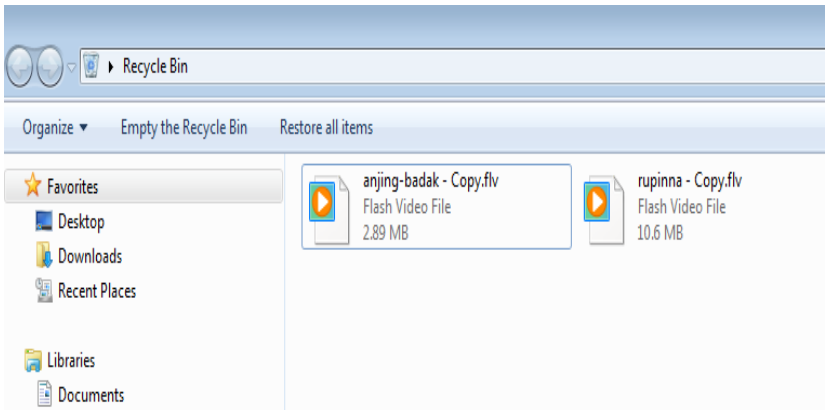
Gambar 8 Pengaturan Maksimum Recycle Bin

Data-data dihapus maka akan berada ke dalam folder Recycle Bin, seperti :



Gambar 9 Isi Folder Recycle Bin Kurang dari Maksimum

Jika Recycle Bin penuh atau melebihi dari ukuran maksimumnya maka data-data tersebut akan terhapus, hasilnya seperti gambar di bawah ini:



Gambar 10 Isi Folder Recycle Bin Melebihi dari Maksimum

Dari penjelasan contoh gambar diatas, maka di perlukan sebuah aplikasi untuk mengembalikan data itu lagi.

2. Penghapusan Permanen

Jika sebuah *file* yang dihapus dengan menekan tombol *delete* di keyboard, maka hanya akan menempatkan *file* itu di folder Recycle Bin. Dengan mudah, *file* itu bisa dikembalikan. Dengan menekan tombol *Shift+Delete* yang menurut Windows akan menghapus *file* secara permanen atau dengan meng-click *Emptying Recycle Bin*, juga tetap bisa dikembalikan. *File* dari hard*disk* yang diformat pun bisa diperoleh kembali. *File* yang memiliki ukuran besar tidak menjamin untuk dapat dikembalikan. Karena sangat mungkin *file* tersebut tersebar di *sector* yang berbeda-beda sehingga memiliki banyak pointer. Pada saat *file* dihapus, seluruh pointernya pun juga dihapus. Ketika *file* itu dikembalikan, ternyata hasil pengembalian tidak sesuai dengan yang diharapkan. *File* yang dikembalikan itu tidak lengkap. Hal ini karena hard*disk* sudah diisi oleh *file* baru. Pada saat *file* baru dimasukkan ke dalam hard*disk* oleh sistem operasi, *file* itu akan diletakkan di *sector* yang dianggap kosong. Bisa saja *sector* itu sesungguhnya berisi bagian dari *file* besar yang tadi

dikembalikan. Itulah yang menyebabkan *file* yang berukuran besar tadi tidak bisa dikembalikan dengan sempurna.

Kehilangan data mungkin pernah dialami oleh setiap pengguna komputer. Beberapa penyebab kehilangan data yaitu kerusakan fisik hard dsik dan kerusakan nonfisik hard disk.

Penyebab kehilangan data yang diakibatkan kerusakan fisik *hard disk* bisa disebabkan, karena:

1. *Hard disk* terjatuh dan merusak mekanik di dalamnya.
2. Terlalu sering dibawa tanpa pengaman membuat *platter hard disk* rusak karena goncangan berlebih.
3. Kondisi *hard disk* yang sudah dalam kondisi yang lama.
4. Sering terjadi pemadaman listrik secara tiba-tiba.

Kehilangan data pada *hard disk* yang bukan karena kerusakan fisik dapat menyebabkan, antara lain:

1. Data terhapus atau hilang.
2. Memiliki banyak nama *letter drive* dan secara tidak sengaja menghilangkan data dengan melakukan *format* pada sebuah *drive letter* sehingga menghapus partisi *hard disk* dan data hilang.
3. Virus melakukan penghapusan data.
4. *Hard disk* mengalami *mulfunction*, hal tersebut dapat terjadi bila *storage* di dalam media terlalu penuh dan *hard disk* mengalami *crash.*

Bisa dibayangkan jika pengguna komputer yang sudah menuliskan dokumen-dokumen penting dan tiba-tiba dokumen tersebut hilang, maka sudah tentu akan terjadi banyak kerugian baik kerugian materiil maupun imateriil. Contoh yang paling dekat jika seorang mahasiswa/i sedang menulis Tugas Akhir (TA) tiba-tiba

ketika sudah hampir selesai dokumen-dokumen tersebut juga raib, tentu hal seperti ini tidak diinginkan.

Sama halnya seperti ilmu forensik di mana penerapannya dari berbagai ilmu pengetahuan untuk menjawab pertanyaan-pertanyaan yang penting dalam sebuah sistem hukum yang mana hal ini mungkin terkait dengan tindak pidana. Namun disamping keterkaitannya dengan sistem hukum, forensik umumnya lebih meliputi sesuatu atau metode-metode yang bersifat ilmiah dan juga aturan-aturan yang dibentuk dari fakta-fakta berbagai kejadian, untuk melakukan pengenalan terhadap bukti-bukti fisik tersebut. Menurut para ahli komputer forensik dapat didefinisikan, yaitu “Ruby Alamsyah (salah seorang ahli forensik IT Indonesia), *digital* forensik atau terkadang disebut komputer forensik adalah ilmu yang menganalisa barang bukti *digital* sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti *digital* tersebut termasuk komputer atau alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa”.

Pada saat di*recovery*, tidak semua data dapat dikembalikan. Terkadang data yang berukuran besar tidak menjamin dapat dikembalikan dengan sempurna seperti pada saat data itu masih ada. Tetapi ada juga data yang dapat dikembalikan dengan sempurna.

1. Penyebab Data Dapat Dikembalikan

   Penyebab data dapat dikembalikan disebabkan karena penempatan data di*sector* tersebut belum terjadi penimpaan data, sehingga data itu dapat dikembalikan, atau bisa saja *hard disk* tersebut belum dilakukan *low format hard disk*. Dimana *low format hard disk* ini merupakan pembentukan *sector* dan *track* pada *platter*. Selain itu pada *hard disk* belum terjadi pembentukan partisi baru pada *sector* yang sama, karena *low*

format hard disk dan partisi itu melakukan pembentukan *sector* dan *track* yang baru.

2. Penyebab Data Tidak Dapat Dikembalikan

   Sebuah data yang berukuran besar tidak menjamin dapat dikembalikan dengan sempurna. Begitu juga dengan program *recovery* data belum tentu dapat seratus persen mampu mengembalikan data yang hilang. Beragam kondisi disyaratkan agar data bisa kembali dengan utuh, misalnya data yang terhapus belum tertimpa (overwritten) oleh data lain. Jika *sector hard disk* yang berisi *file* data yang terhapus oleh tertimpa oleh data lain, maka akan menyulitkan program *recovery* untuk mengembalikan data, atau bila berhasil dikembalikan, kemungkinan *file* akan rusak (*corrupt*). Agar data dapat utuh seratus persen dikembalikan, maka sebelum melakukan *recovery* data, usahakan jangan menambahkan *file* apapun ke dalam *drive* yang akan di-*recovery*, karena kemungkinan *sector hard disk* yang berisi *file* yang akan di-*recovery* akan tertimpa dengan *file* baru.

Bab III Analisis Kebutuhan

Pada bab ini berisi penjelasan tentang analisis dari aplikasi recovery yang banyak tersedia. Analisis tersebut akan digunakan dalam pemilihan aplikasi mana yang terbaik dalam hal pengembalian data.

III.1 Kebutuhan Forensik Terkait Aplikasi Recovery

Didalam kebutuhan forensik, aplikasi recovery harus mampu melakukan hal-hal yang dianggap sebagai kebutuhan forensik, antara lain :

1. Mengumpulkan data yang berbentuk digital dan bisa dijadikan sebagai barang bukti.
2. Mengidentifikasi barang bukti digital tersebut dengan mengetahui lokasi kejadian, dan alat-alat yang digunakan.
3. Melakukan pengujian dari hasil pengumpulan barang bukti.
4. Mengembalikan data yang berada di dalam hard disk yang dianggap penting untuk dijadikan sebagai barang bukti.
5. Menganalisis dari pengujian yang telah dilakukan dan mendapatkan kesimpulan dari hasil pengujian.
6. Membuat laporan dan dokumentasi dari informasi yang merupakan hasil dari proses analisis.

Dalam memenuhi kebutuhan forensik, diperlukan aplikasi recovery hard disk yang mendukung dalam kebutuhan tersebut.

III.2 Aplikasi Recovery yang Tersedia

Aplikasi recovery merupakan software yang digunakan untuk mengembalikan data-data yang terhapus baik yang disengaja ataupun tidak. Banyak aplikasi yang tersedia untuk mendukung pengembalian data yang dibutuhkan dalam komputer forensik. Berikut ini merupakan macam-macam aplikasi recovery :

1. Recuva

   Aplikasi ini dibuat oleh Piriform yang juga merilis aplikasi *free* untuk membersihkan files sampah di sistem Windows, CCleaner. Para pengguna Recuva mempermudah dalam mengelolanya, terlebih dengan tersedianya wisaya (wizard) *recovery* data saat pertama kali program dijalankan. Wisaya tersebut akan memandu untuk menentukan format file apa yang hendak dicari lalu diselamatkan, lokasi tempat files tersebut berada (dengan sejumlah pilihan mulai dari kartu memori, *hard drive*, My Documents, kantong sampah, hingga direktori yang ditentukan sendiri). Proses pengembalian pun bisa dilakukan secara mendalam (deep scan). Proses selanjutnya tentu seperti saat melakukan pencarian lewat fasilitas Find di Windows Explorer. Data yang dicari akan ditampilkan, lalu memilihnya untuk kemudian dikembalikan. Selain, melakukan data hilang lalu mengembalikannya, ada proses estimasi yang bisa dilakukan aplikasi ini. Recuva mampu memperkirakan dan menginformasikannya kepada user apakah sebuah file bisa optimal di-*recovery* atau tidak. Selain *recovery*, Recuva memiliki fungsi tambahan untuk menghapus sebuah data secara penuh, agar kemudian tak bisa diselamatkan kembali.

2. PC Inspector File Recovery

   Program *recovery* buatan Jerman ini termasuk program *recovery* yang menjadi pelopor sebagai freeware *recovery*. Performanya sudah banyak dikenal, meskipun begitu perkembangannya memang terasa sedikit lambat dibanding aplikasi-aplikasi baru sejenis. PC Inspector mampu mendeteksi

partisi data secara otomatis, meskipun berada dalam boot sector. Selain itu kinerja *recovery*-nya juga baik di media-media simpan yang rusak. walaupun, aplikasi berukuran sekitar 6 MB ini mampu mengembalikan data meski header entry (awalan file) tidak lagi ada, termasuk mengembalikan info waktu modifikasi file asli, date stamp, dan juga mendukung *recovery* pada drive simpan dalam jaringan. Tersedia fitur "Special recovery Function" untuk sejumlah format file umum, meliputi sejumlah file dokumen office hingga beragam format file gambar dan aplikasi. Pengelolaan aplikasi ini dirancang agar memudahkan dengan sejumlah pilihan tindakan yang hendak lakukan pada sebuah media simpan. Bentuknya memang tak serupa wizard, namun sudah cukup membantu proses *recovery* dengan cepat. Setelah proses pengembalian data maka pengguna akan diberi pilihan untuk proses *recovery*.

3. TestDisk

   Jika semua aplikasi penyelamat data yang telah dibahas sebelumnya hanya berjalan di atas Windows, maka TestDisk adalah aplikasi yang lebih fleksibel. TestDisk bisa berjalan di hampir semua sistem operasi, mulai dari DOS, Windows (NT4, 2000, XP, 2003, Vista), Linux, FreeBSD, NetBSD, OpenBSD, SunOS, dan juga MacOS. Aplikasi memiliki banyak kegunaan, mulai dari memperbaiki tabel partisi dan juga mengembalikan data partisi yang terhapus. Segala fungsinya berlaku pada format sistem files FAT, NTFS, BeFS, BSD disklabel, HFS, Linux ext, Linux RAID, hingga Sun Solaris i386 disklabel dan masih banyak lagi. Aplikasi ini mampu membangun boot sector yang rusak. Cakupan media simpan yang bisa diatasinya mulai dari karyu memori hingga cakram data seperti CD atau DVD, dan juga Disk Image. Hanya saja tampilan aplikasi ini kurang nyaman untuk dikelola. Untuk format sistem Windows, interface aplikasi ini masih menyerupai tampilan program MS-DOS dengan perintah dalam

bentuk teks. Buat pengguna yang ingin aplikasi komplet dengan cakupan penerapan yang luas, aplikasi boleh dipilih. Bahkan pengunanya bisa mengembangkannya.

4. Data Recovery

   DataRecovery merupakan aplikasi freeware yang dibuat oleh programmer TOKIWA (programmer dari Jepang) untuk me-recovery aplikasi yang telah terhapus, seperti terhapus dari recycle bin. Aplikasi ini hanya single exe, dengan ukuran sekitar 400 KB dan tampilan yang sederhana. Tetapi, pada proses scan juga sangat cepat.

5. Pandora Recovery

   Proses pemulihan data pada aplikasi ini relatif mudah digunakan oleh pengguna, sehingga aplikasi ini diminati oleh pengguna. Hal ini karena kemampuannya dalam menemukan dan mengembalikan data yang hilang. Walaupun tampilannya sangat sederhana, tetapi aplikasi ini dirancang dengan menu yang mudah digunakan.

6. Photorec

   Photorec adalah perangkat lunak yang dirancang untuk memulihkan file yang hilang termasuk video, dokumen dan arsip dari hard disk, CD-ROM dan gambar hilang dari memori digital. Photorec mengabaikan sistem file dan hanya melanjutkan pencarian data hilang, sehingga aplikasi ini bekerja pada berkas yang dihapus dan diformat. Selain itu, aplikasi ini freeware yang bersumber aplikasi multi platform didistribusikan di bawah GNU(General Public Lisence).

Dari bermacam-macam aplikasi yang disediakan, maka akan dilakukan pengujian dari aplikasi tersebut. Pengujian dilakukan agar mendapatkan perbandingan aplikasi mana yang terbaik dalam hal kebutuhan forensik.

Bab IV Pengujian

Pada bab ini berisi tentang perancangan pengujian dari tiap-tiap aplikasi recovery agar mendapatkan perbandingan. Hal ini bertujuan agar mengetahui aplikasi mana yang terbaik dalam pengembalian data untuk kebutuhan forensik.

IV.1 Perbandingan Aplikasi Recovery

Dalam melakukan perbandingan aplikasi recovery dibutuhkan suatu lingkungan pengujian yang dibangun untuk mendapatkan data. Berdasarkan kebutuhan forensik yang harus dipenuhi aplikasi recovery, maka di dalam hard disk terdapat file-file yang akan digunakan untuk melakukan recovery data, berikut spesifikasi file yang digunakan:

Tabel 1 Spesifikasi File

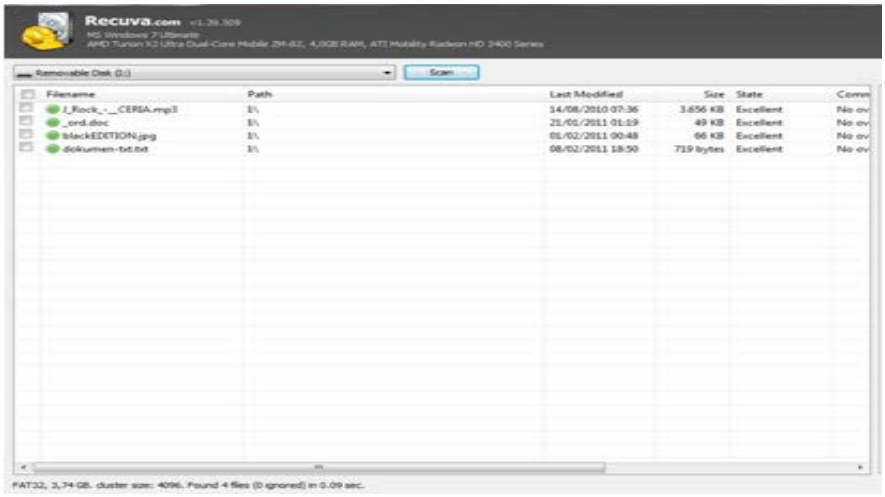
Nama file	Jenis file
LK-Oktober 2010	Doc
0987654321	Jpg
Milik-groupA	Mp3
VD001	Flv

Untuk mendapatkan hasil yang diinginkan, maka dibutuhkan suatu perbandingan aplikasi recovery yang ada untuk melihat proses pengembalian data yang dilihat pada saat penghapusan dan pengformatan, dan dapat menentukan aplikasi mana yang dapat memenuhi dari kebutuhan forensik tersebut.

IV.1.1 Recuva

a. Delete

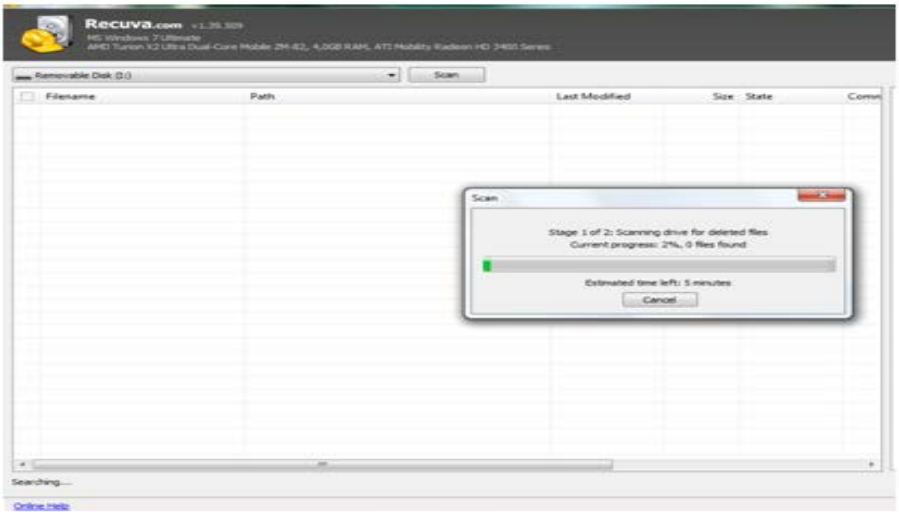
Recuva mampu mengembalikan data hilang yang dihapus. Keterangan hasil pengembalian data seperti pada gambar.



Gambar 11 Hasil Pengembalian Data yang dihapus

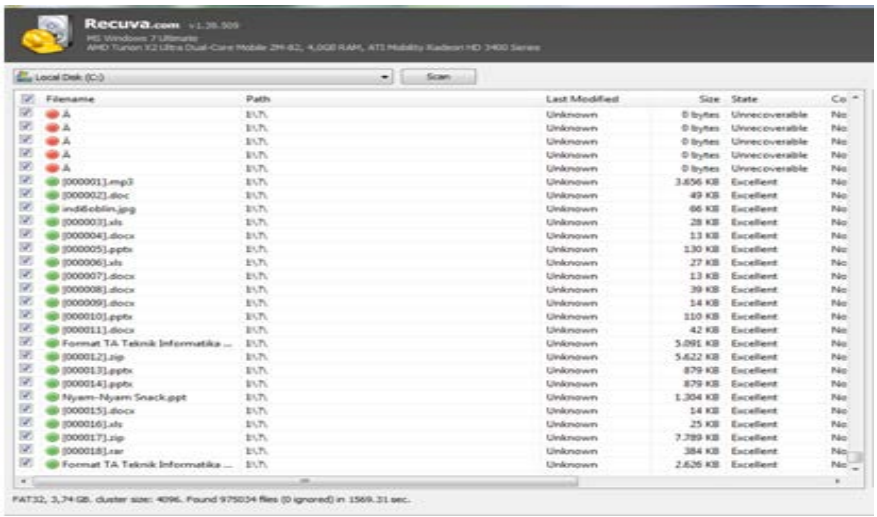
b. Format

Recuva juga mampu mengembalikan data hilang yang diakibatkan partisi diformat. Setelah melakukan proses scanning akhirnya data terdebut bisa dikembalikan.



Gambar 12 Proses Scanning Recuva

Namun, hasil data yang diperoleh masih kurang lengkap dikarenakan file txt tidak dapat dikembalikan.



Gambar 13 hasil Pengembalian Data yang diformat

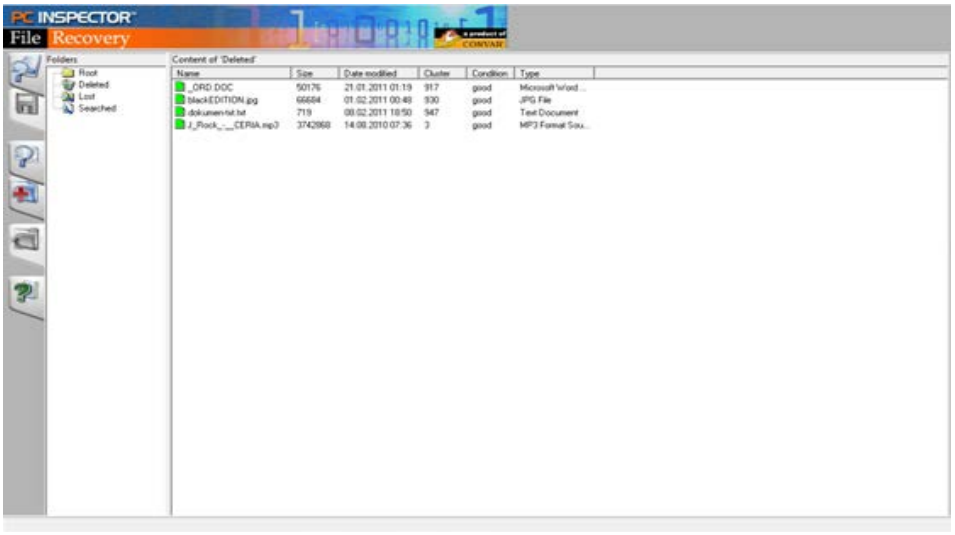
c. Partisi

Pada aplikasi Recuva, tidak ada tools yang mendukung untuk mengembalikan partisi yang hilang.

IV.1.2 PC Inspector File Recovery

a. Delete

PC Inspector File Recovery juga mampu mengembalikan data dihapus dan hasil keakuratan datanya secara utuh. Keterangan hasil pengembalian data dihapus.



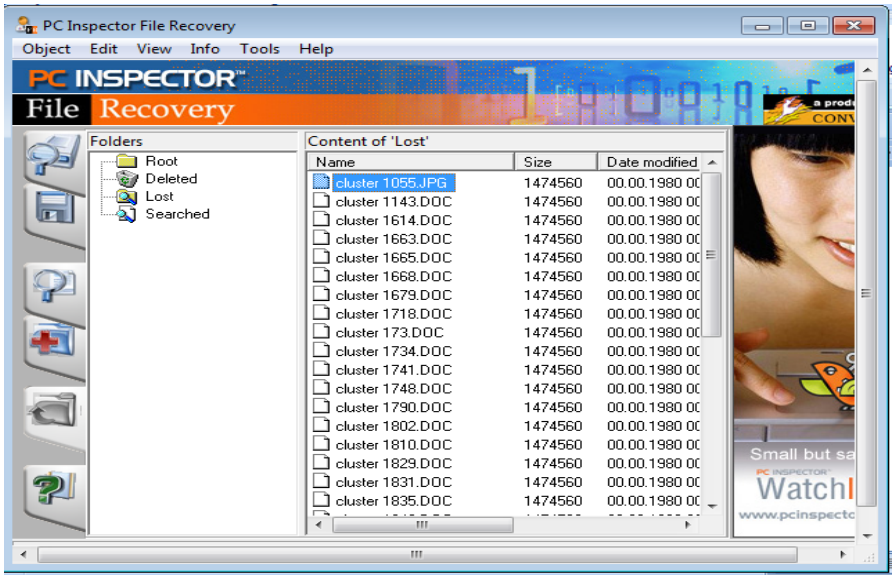
Gambar 14 Hasil Pengembalian Data yang dihapus

b. Format

Ketika partisi diformat PC Inspector File Recovery akan melakukan proses scanning cluster.

Gambar 15 Proses Scanning PC Inspector File Recovery

Setelah proses scaning selesai maka hasil yang diterima masih kurang lengkap. karena hasil scan PC Inspector File Recovery hanya mengembalikan file gambar*(image)*. Keterangan hasil pengembalian data PC Inspector File Recovery.



Gambar 16 Hasil Pengembalian Data yang diformat

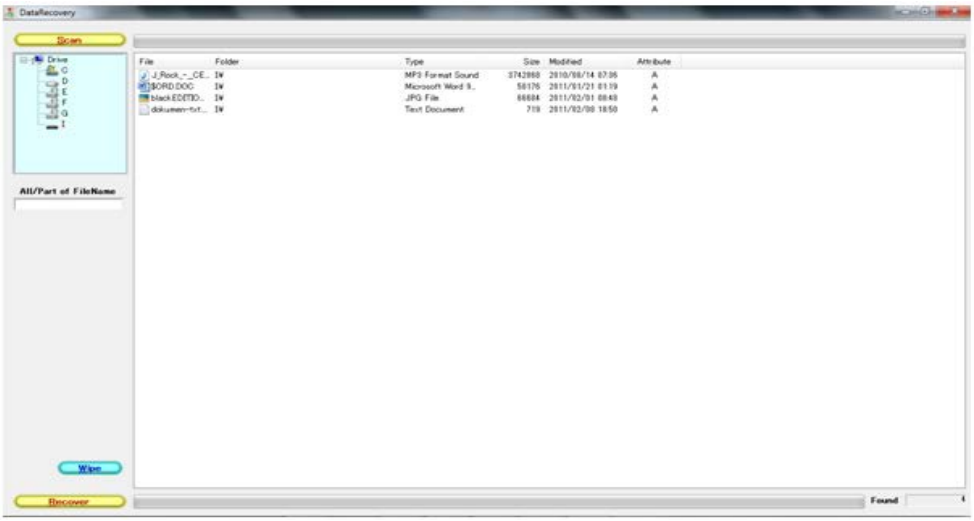
c. Partisi

Pada aplikasi PC Inspector File Recovery, tidak ada tools yang mendukung untuk mengembalikan partisi yang hilang.

IV.1.3 Data Recovery

a. Delete

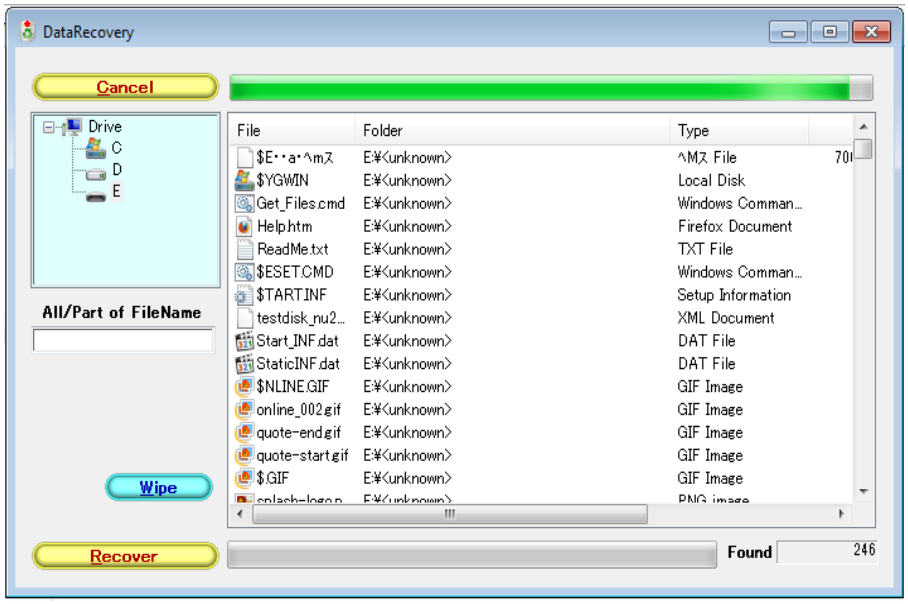
Data recovery mampu mengembalikan data dihapus secara utuh, seperti pada gambar.



Gambar 17 Hasil Data Recovery yang dihapus

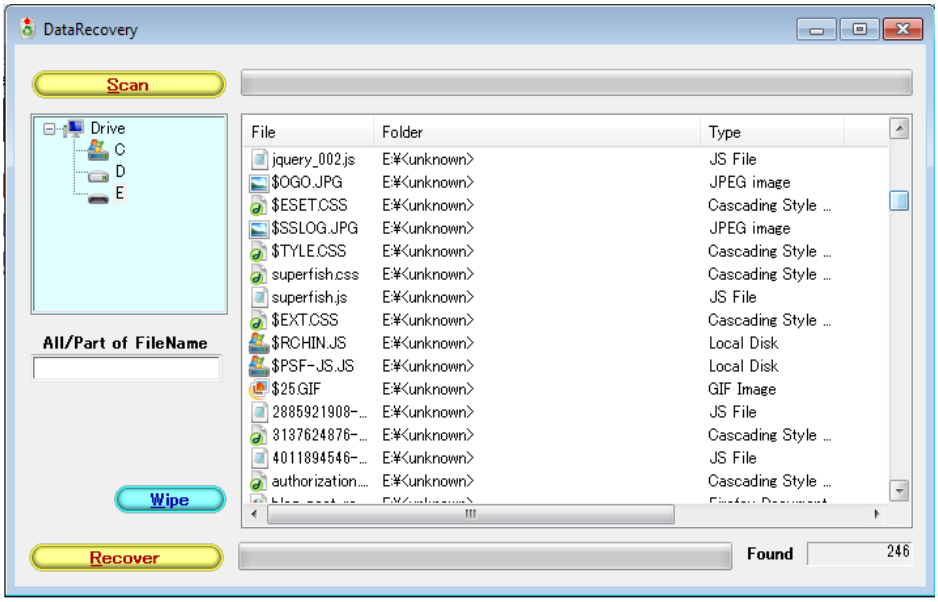
b. Format

Pada saat melakukan pengembalian dari data yang sudah terformat, aplikasi melakukan proses scanning untuk mencari file yang sudah terformat.



Gambar 18 Proses Scanning Data Recovery yang diformat

Setelah melakukan proses scanning, maka hasil yang pengembalian datab yang terformatpun kembali, meskipun tidak semua file dapat dikembalikan.



Gambar 19 Hasil dari Scanning Data Recovery

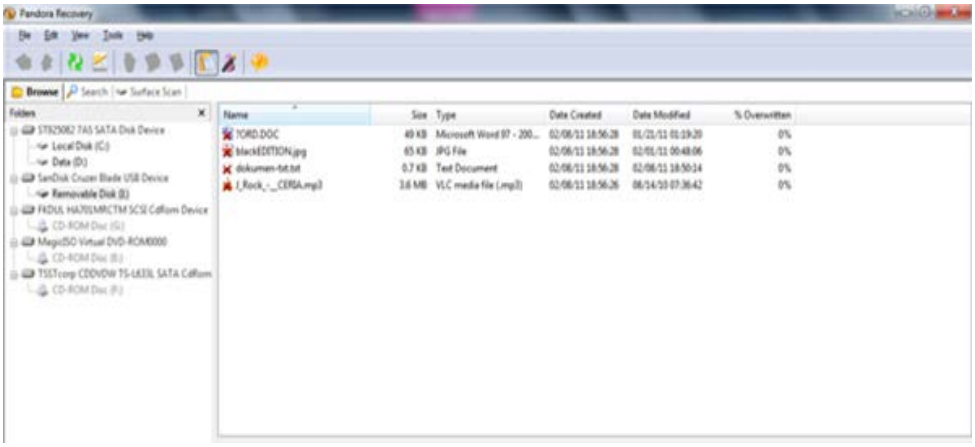
c. Partisi

Pada aplikasi Data Recovery, tidak ada tools yang mendukung untuk mengembalikan partisi yang hilang.

IV.1.4 Pandora Recovery

a. Delete

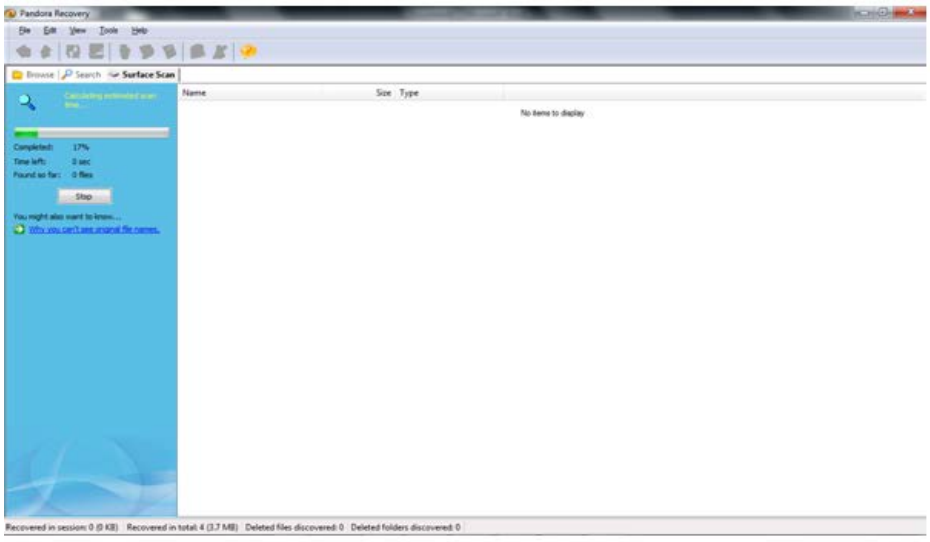
Pandora Recovery mampu mengembalikan data yang dihapus secara utuh tanpa ada kecacatan. Keterangan hasil pengembalian data Pandora Recovery seperti gambar.



Gambar 20 Hasil Pengembalian Data yang dihapus

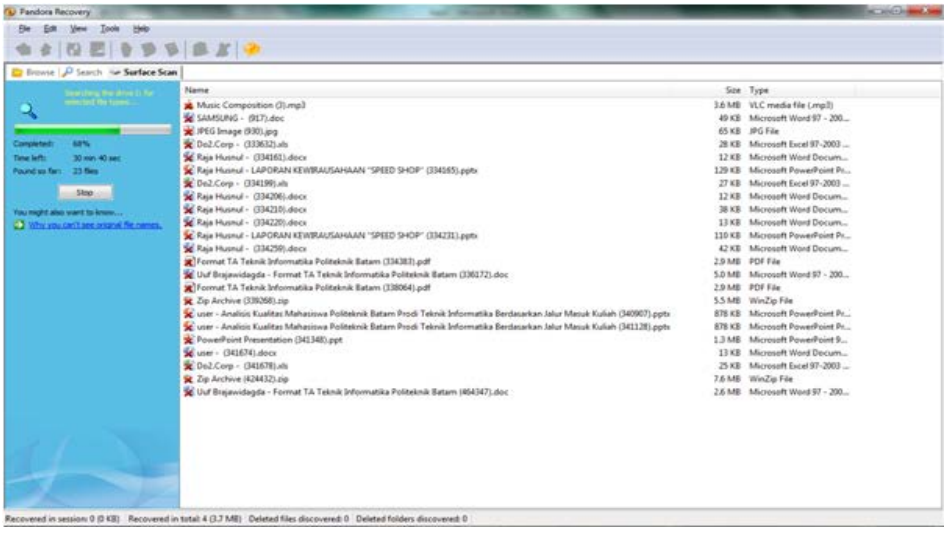
b. Format

Pandora Recovery juga mampu mengembalikan data saat partisi diformat. Keterangan proses scanning Pandora Recovery dan hasil pengembalian data seperti pada gambar.



Gambar 21 Proses Scanning Pandora Recovery

Namun, hasil pengembalian data yang disebabkan partisi diformat kurang lengkap, karena proses scanning Pandora Recovery hanya mengembalikan file doc, jpg dan mp3.



Gambar 22 Hasil Pengembalian Data yang diformat

c. Partisi

Pada aplikasi Pandora Recovery, tidak ada tools yang mendukung untuk mengembalikan partisi yang hilang.

IV.1.5 TestDisk

a. Delete

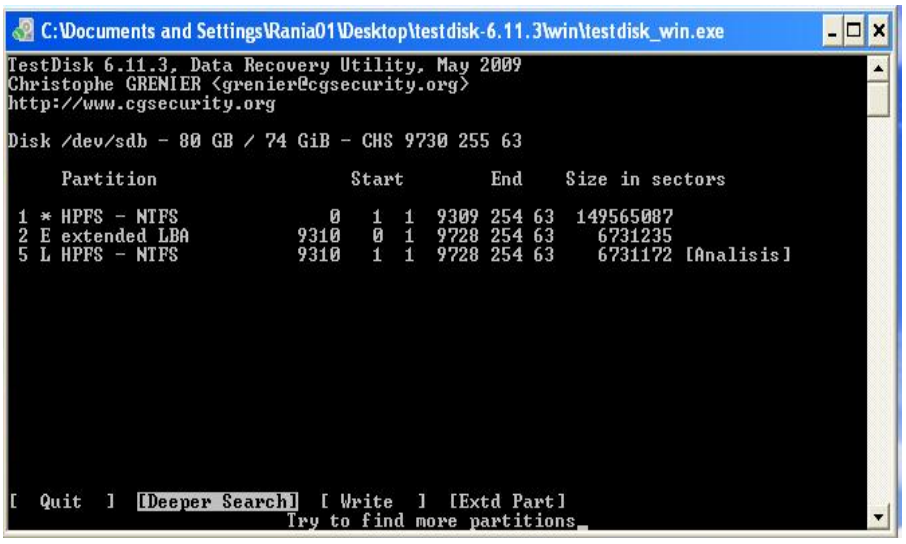
Pada aplikasi TestDisk tidak ada tools yang mendukung proses pengembalian data yang dihapus.

b. Format

Pada aplikasi TestDisk tidak ada tools yang mendukung proses pengembalian data yang diformat.

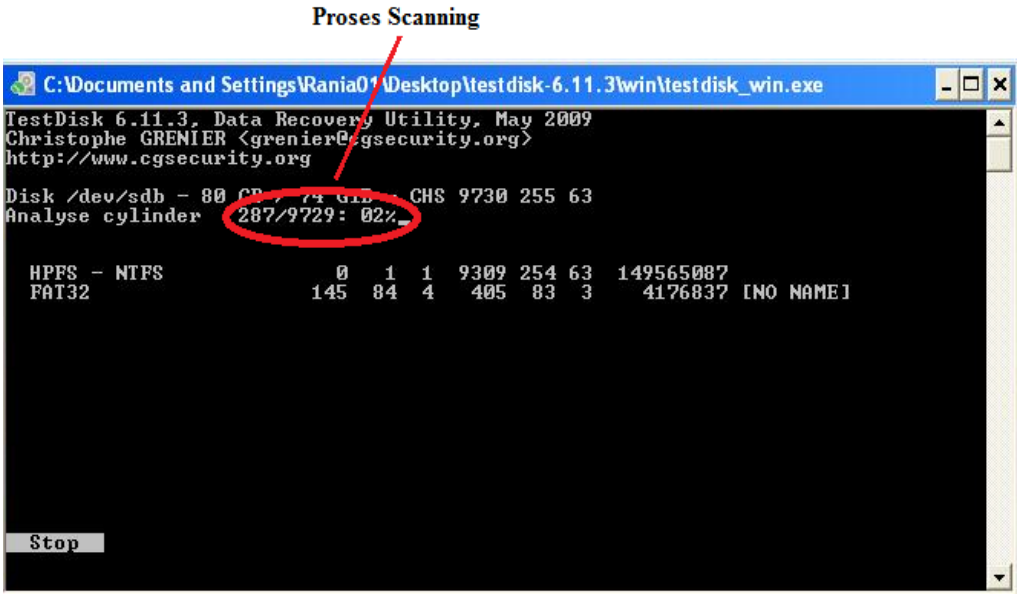
c. Partisi

Dari tampilan struktur *file* sistem NTFS dengan menekan tombol ENTER, maka akan tampil menganalisis partisi. Keterangan gambar sebagai berikut:



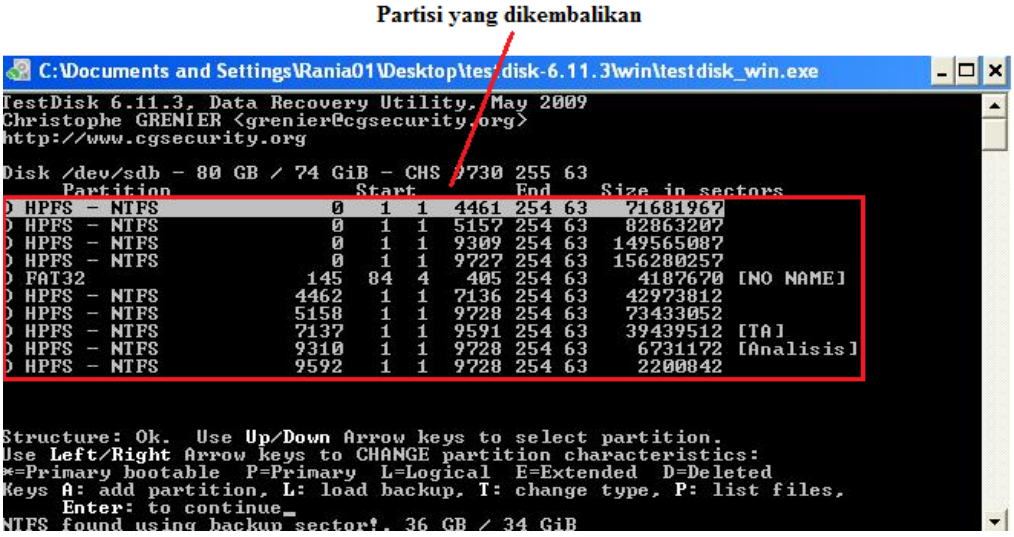
Gambar 23 Menganalisa Partisi

Setelah menganalisis partisi dari gambar di atas dengan memilih Deeper Search, maka akan tampil pencarian dari *Analysis* cylinder. Keterangan gambar sebagai berikut:



Gambar 24 Proses Scanning Partisi

Setelah melakukan pencarian, partisi yang pernah terhapus dari *hard disk* dapat dikembalikan.

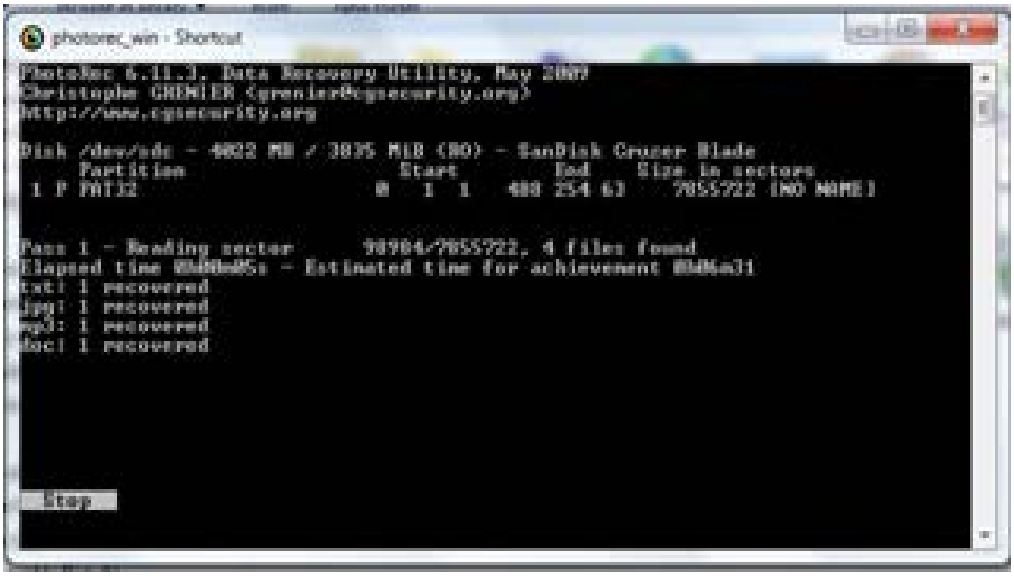


Gambar 25 Hasil Scanning TestDisk

IV.1.6 Photorec

a. Delete

Photorec dapat juga mengembalikan data yang disebabkan data dihapus. Keterangan proses scanning TestDisk.



Gambar 26 Proses Scanning Photorec pada Saat dihapus

b. Format

Selain, pengembalian data dihapus, Photorec juga mampu mengembalikan data saat partisi diformat. Berikut ini merupakn proses scanning dari aplikasi Photorec.

Gambar 27 Proses Scanning Photorec Data diformat

c. Partisi

Pada aplikasi Photorec, tidak ada tools yang mendukung untuk mengembalikan partisi yang hilang.

IV.2 Skenario Pengujian

Didalam proses pengujian, terdapat bermacam-macam kasus kehilangan data yang dapat membuat pihak-pihak tertentu merasa dirugikan. Baik itu kehilangan dokumen, gambar, video bahkan audio yang dianggap penting yang bisa dijadikan sebagai bukti digital untuk kasus hukum.

IV.2.1 Kehilangan Dokumen

Saat ini banyak perusahaan yang mulai memanfaatkan jasa komputer forensik untuk keperluan data audit keuangan, baik yang masih ada atau pun data keuangan yang dicurigai telah dihapus. Dalam hal audit keuangan, perusahaan ABC selalu

melakukan audit pada akhir tahun sehingga memberikan kesempatan kepada karyawan untuk melakukan manipulasi atau menghapus data keuangan perbulan dan menggantinya dengan yang baru.

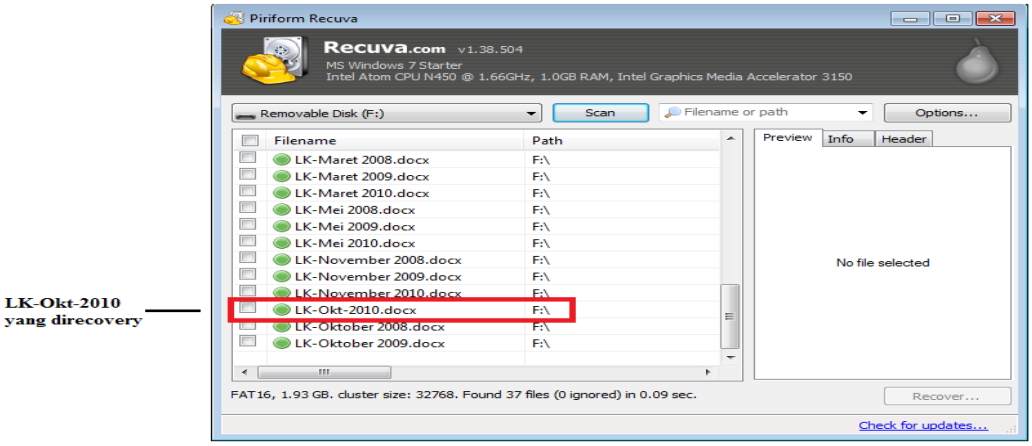
Pada akhir tahun 2010, perusahaan ABC akan melakukan audit keuangan. Namun perusahaan mencurigai adanya ketidaksesuaian terhadap data keuangan perbulan. Perusahaan ABC mencurigai bahwa data keuangan bulan Oktober tidak sesuai, bisa saja data keuangan yang asli telah dihapus sebelumnya dan dibuat pada bulan selanjutnya, sehingga terjadi manipulasi data.

Untuk menyelesaikan masalah, perusahaan ABC mendatangkan ahli komputer forensik guna mengetahui file asli data keuangan pada bulan oktober dan mengembalikannya. Untuk melakukan itu semua, diperlukan tahapan forensik terhadap perusahaan tersebut.

Dalam proses pengembalikan bukti digital, penyidik melakukan pengujian terhadap 6(enam) aplikasi recovery yang telah tersedia. Dari pengujian ini guna mengetahui pengembalian data digital yang terlihat dari keakuratan datanya.

1. Recuva

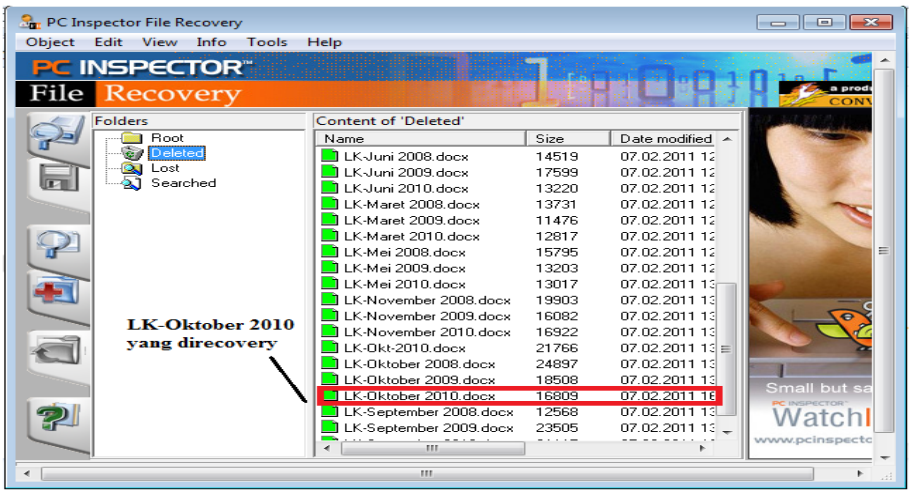
   Ketika menggunakan Recuva, aplikasi ini mampu mengembalikan dokumen Laporan Keuangan pada bulan Oktober tersebut.



Gambar 28 LK-okt-2010 yang direcovery Menggunakan Recuva

2. PC Inspector File Recovery

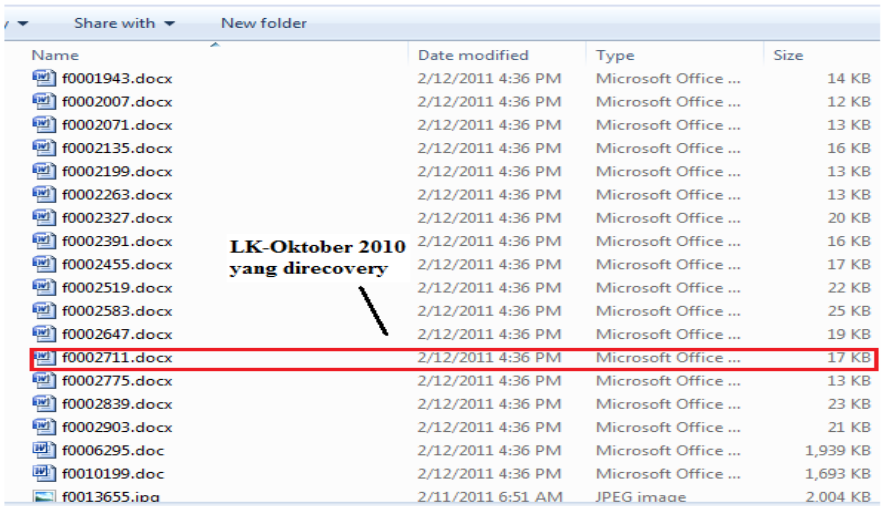
PC Inspector File Recovery mampu juga mengembalikan dokumen yang dihapus, serta mengembalikan modified date data tersebut.



Gambar 29 LK-okt-2010 yang direcovery Menggunakan PC Inspector

3. Photorec

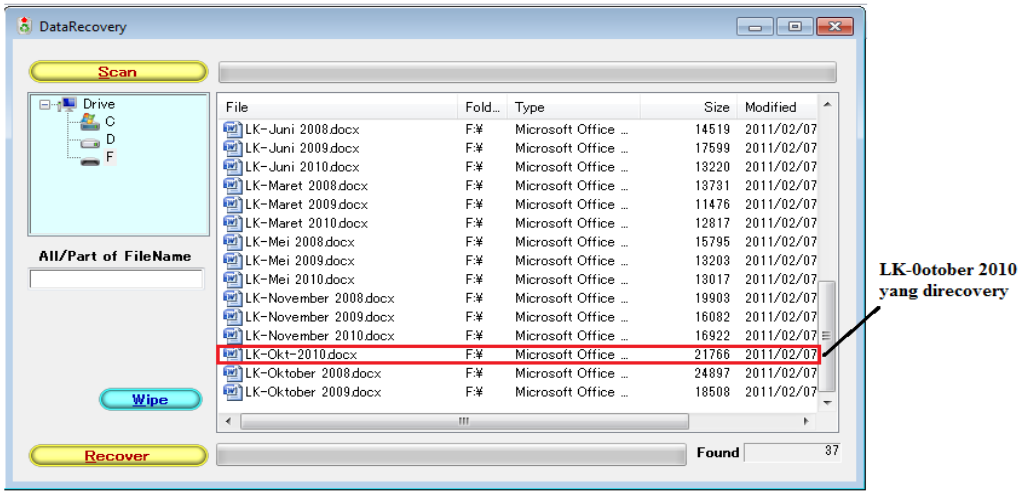
Aplikasi ini dapat mengembalikan dokumen hilang secara utuh, meskipun membutuhkan proses scanning yang lama.



Gambar 30 LK-okt-2010 yang direcovery Menggunakan Photorec

4. Data Recovery

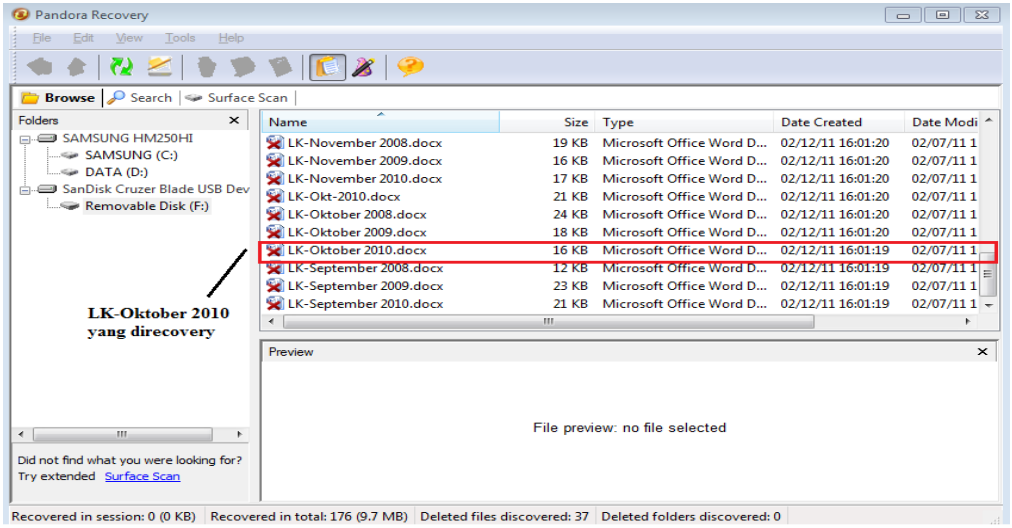
   Data Recovery juga dapat mengembalikan dokumen hilang yang dihapus secara utuh dan juga menampillkan modified date-nya.



Gambar 31 LK-okt-2010 yang direcovery Menggunakan Data Recovery

5. Pandora Recovery

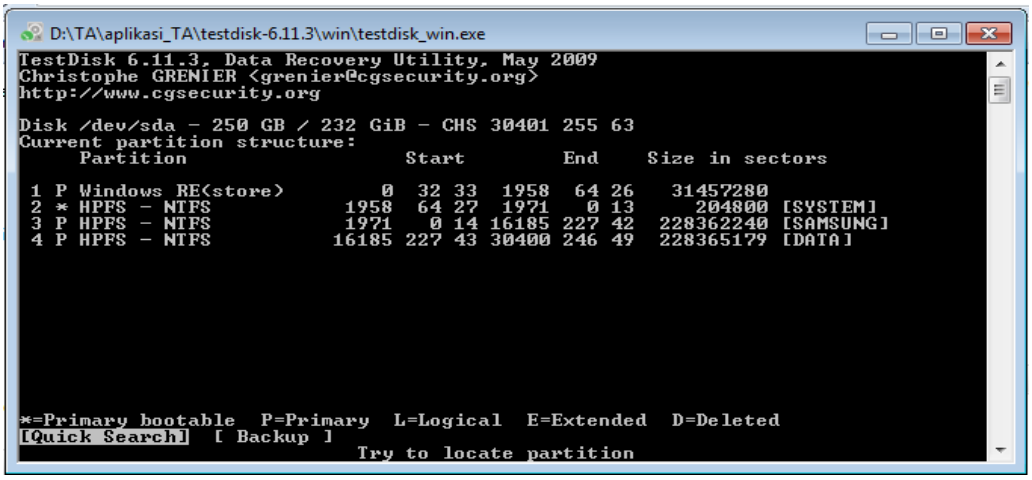
   Aplikasi ini mampu mengembalian dokumen hilang yang dihapus secara utuh, serta juga menampilkan created date dan modified date.



Gambar 32 LK-okt-2010 yang direcovery Menggunakan Pandora

6. TestDisk

   Aplikasi ini tidak mendukung pengembalian data hilang yang diakibatkan dihapus.



Gambar 33 LK-okt-2010 yang direcovery Menggunakan TestDisk

PERUSAHAAN ABC
LAPORAN KEUANGAN
OKTOBER 2010

Tanggal	Ket	Debit	Kredit
04-Oktober-2010	Penjualan Jilbab	1500000	
05-Oktober-2010	Penjualan Kaos Kaki	1000000	
05-Oktober-2010	Penjualan Kaos Kaki	1000000	
06-Oktober-2010	pngeluaran		3000000
07-Oktober-2010	Penjualan Jilbab	3000000	
09-Oktober-2010	Penjualan Pin	1000000	
10-Oktober-2010	Penjualan Sarung Tangan	2000000	
10-Oktober-2010	Penjualan Jilbab	2500000	
13-Oktober-2010	Penjualan Sarung Tangan	1000000	
13-Oktober-2010	Penjualan Kaos Kaki	5000000	
15-Oktober-2010	Pembelian Barang	1000000	
09-Oktober-2010	Penjualan Pin	3000000	
10-Oktober-2010	Penjualan Jilbab	3000000	
10-Oktober-2010	Penjualan Kaos Kaki	1000000	
13-Oktober-2010	Penjualan Pin	2000000	
13-Oktober-2010	Penjualan Jilbab	4500000	
17-Oktober-2010	Penjualan Kaos Kaki	5000000	
20-Oktober-2010	Penjualan Kaos Kaki	2000000	
23-Oktober-2010	Penjualan Pin	3000000	
23-Oktober-2010	Penjualan Jilbab	1500000	
26-Oktober-2010	Penjualan Sarung Tangan	1000000	
26-Oktober-2010	Penjualan Jilbab	3000000	
26-Oktober-2010	Penjualan Kaos Kaki	5000000	
26-Oktober-2010	Penjualan Pin	2000000	
27-Oktober-2010	Maintenance Warnet 1	1800000	
28-Oktober-2010	Maintenance Warnet 2	1150000	
29-Oktober-2010	Maintenance Warnet 3	1200000	
Total		Rp 55650000	Rp 3000000
		Rp 52.650.000	

Gambar 34 Laporan Keuangan Bulan Oktober 2010

Tetapi, menurut laporan keuangan tahun 2010 yang diberikan karyawan keuangan, bahwa laporan pada bulan Oktober berbeda dengan hasil laporan yang berhasil dikembalikan. Seperti pada gambar dibawah ini :

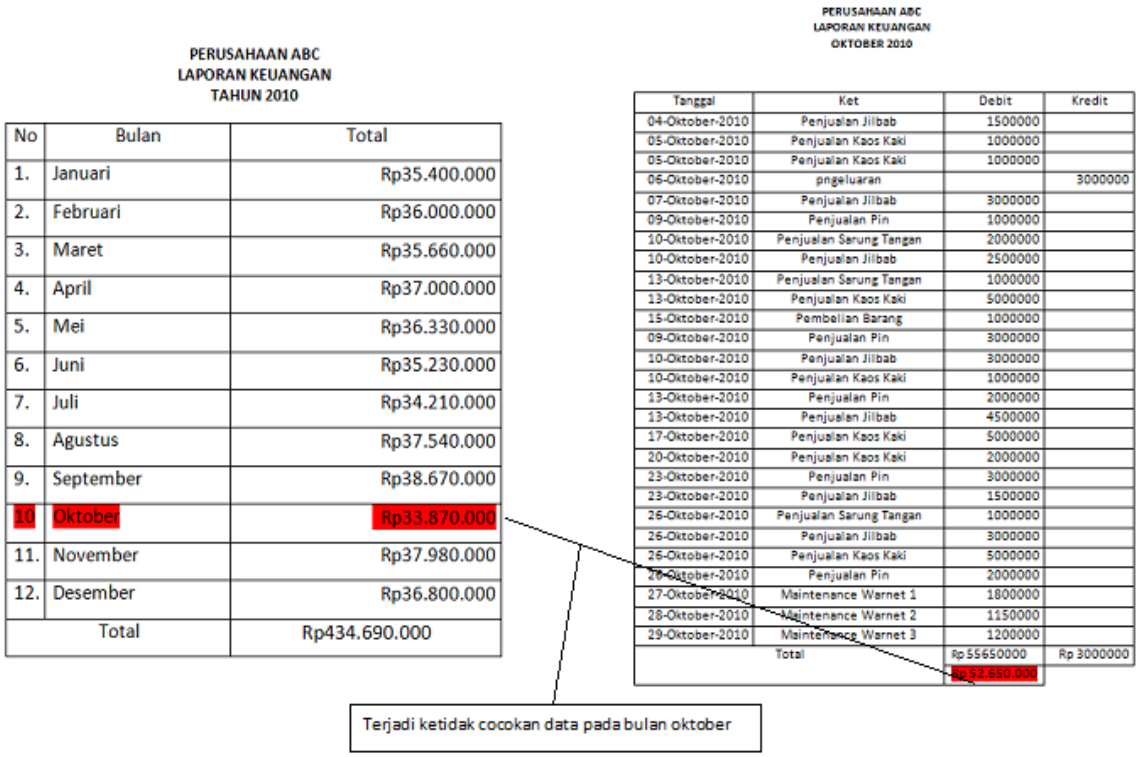
PERUSAHAAN ABC
LAPORAN KEUANGAN
TAHUN 2010

No	Bulan	Total
1.	Januari	Rp35.400.000
2.	Februari	Rp36.000.000
3.	Maret	Rp35.660.000
4.	April	Rp37.000.000
5.	Mei	Rp36.330.000
6.	Juni	Rp35.230.000
7.	Juli	Rp34.210.000
8.	Agustus	Rp37.540.000
9.	September	Rp38.670.000
10	Oktober	Rp33.870.000
11.	November	Rp37.980.000
12.	Desember	Rp36.800.000
Total		Rp434.690.000

LK-Oktober 2010

Gambar 35 Laporan Keuangan 2010

Setelah dianalisis, ternyata terjadi ketidakcocokan data pada bulan Oktober 2010 yaitu:



PERUSAHAAN ABC
LAPORAN KEUANGAN
TAHUN 2010

No	Bulan	Total
1.	Januari	Rp35.400.000
2.	Februari	Rp36.000.000
3.	Maret	Rp35.660.000
4.	April	Rp37.000.000
5.	Mei	Rp36.330.000
6.	Juni	Rp35.230.000
7.	Juli	Rp34.210.000
8.	Agustus	Rp37.540.000
9.	September	Rp38.670.000
10	Oktober	Rp33.870.000
11.	November	Rp37.980.000
12.	Desember	Rp36.800.000
Total		Rp434.690.000

Gambar 36 Perbandingan LK_Oktober 2010

Setelah perbandingan laporan keuangan yang diberikan oleh karyawan keuangan dengan laporan keuangan yang direcovery, akhirnya pihak perusahaan mengetahui bahwa sudah terjadi sabotase pada lapo5an keuangan bulan Oktober 2010.

IV.2.2 Kehilangan Gambar

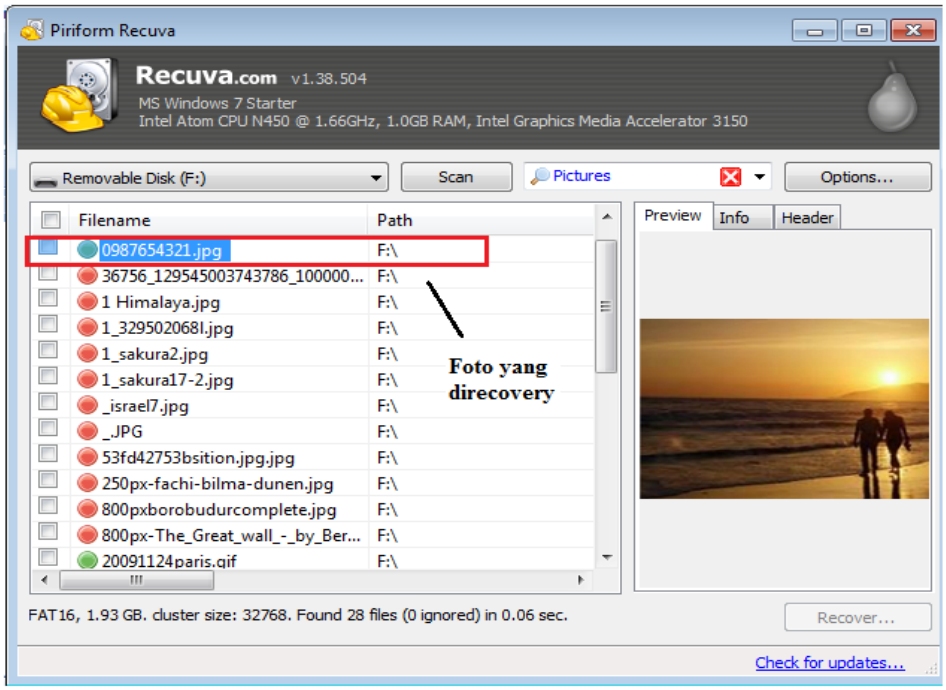
Seorang pejabat negara diberitakan telah berfoto mesra dengan perempuan yang dikenal sebagai rekan kerjanya di DPR. Berita tersebut diketahui oleh istrinya dengan media handphone yang dikirim oleh seseorang yang tidak diketahui nomor identitiasnya. Orang itu mengirimkan sms yang berisi bahwa dilaptop suaminya terdapat foto mesra dengan rekan kerjanya. Hal ini membuat sang istri merasa

penasaran, apakah benar suaminya berfoto mesra dengan seorang wanita. Tetapi pada saat istrinya melihat isi didalam laptop suaminya, foto tersebut sudah tidak ada. Ini membuat sang istri tambah merasa penasaran. Lalu sang istri memutuskan untuk mengundang pihak forensik untuk melacak apakah benar didalam laptop tersebut terdapat foto mesra suaminya bersama rekan kerjanya.

Dalam proses pengembalian data digital, penyidik melakukan pengujian terhadap 6(enam) aplikasi recovery yang telah tersedia. Pengujian ini dilakukan guna membuktikan kebenaran yang terlihat dari keakuratan data dalam pengembalian data tersebut.

1. Recuva

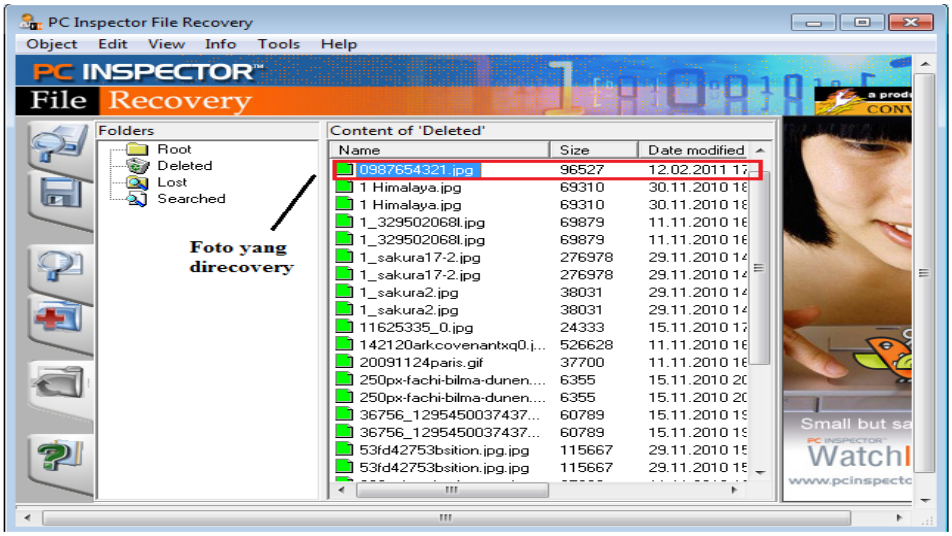
   Dalam pengujian pertama, penyidik melakukan pengembalian data menggunakan aplikasi Recuva. Dan aplikasi ini dapat mengembalikan data tersebut.



Gambar 37 Foto yang direcovery Menggunakan Recuva

2. PC Inspector File Recovery

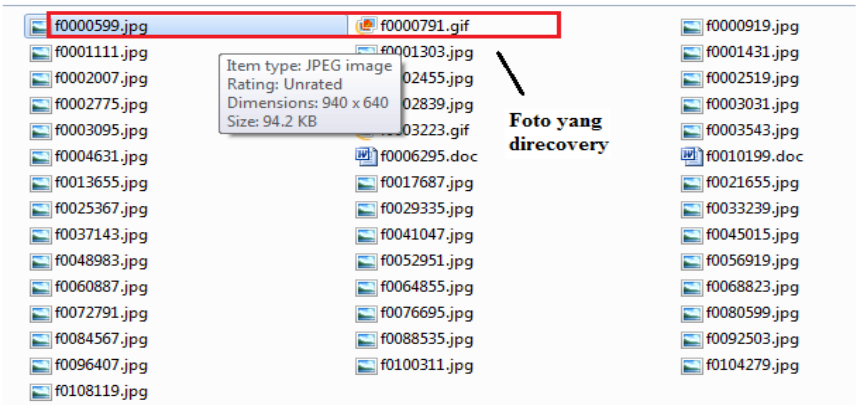
Tahap berikutnya, penyidik melakukan kembali menggunakan aplikasi PC Inspector File Recovery. Aplikasi ini mampu mengembalikan data dan juga modified date-nya.



Gambar 38 Foto yang direcovery Menggunakan PC Inspector

3. Photorec

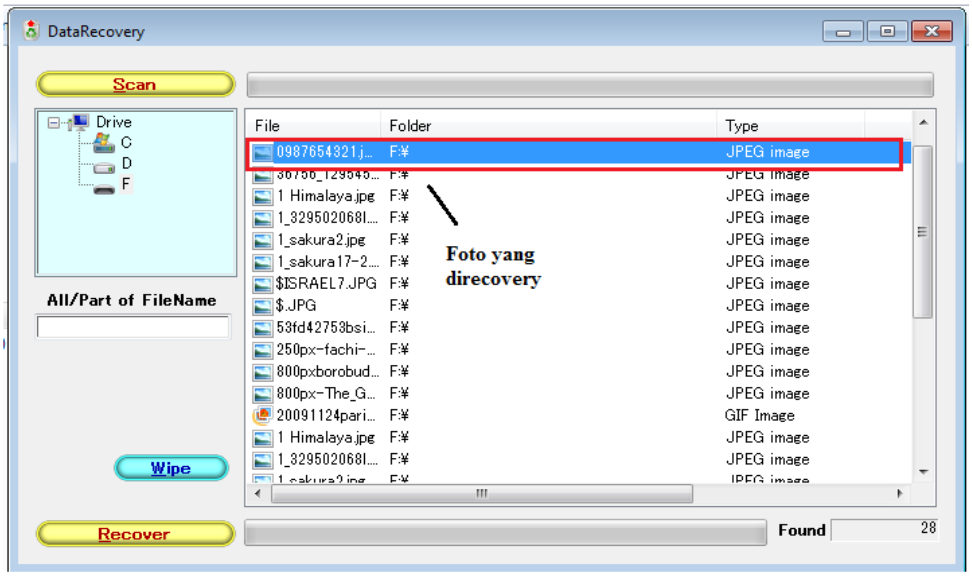
Untuk menyakinkan kebenaran data tersebut, penyidik melakukan pengembalian data menggunakan aplikasi Photorec. Aplikasi ini dapat mengembalikan data tersebut.



Gambar 39 Foto yang direcovery Menggunakan Photorec

4. Data Recovery

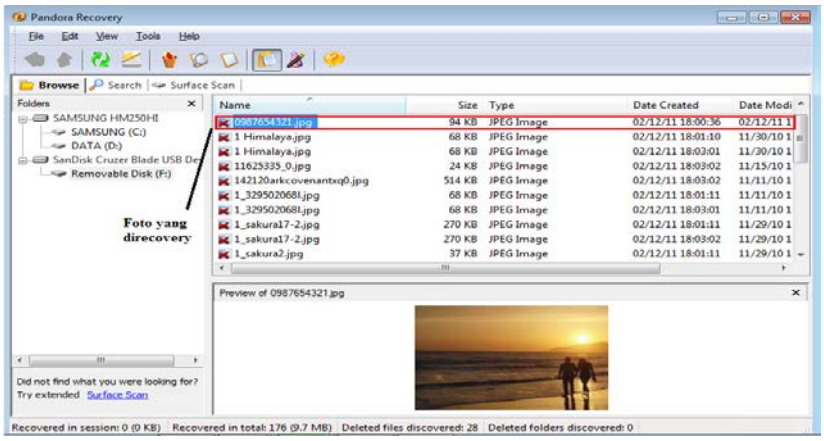
Aplikasi berikutnya yakni Data Recovery, aplikasi ini juga mengembalikan gambar tersebut.



Gambar 40 Foto yang direcovery Menggunakan Data Recovery

5. Pandora Recovery

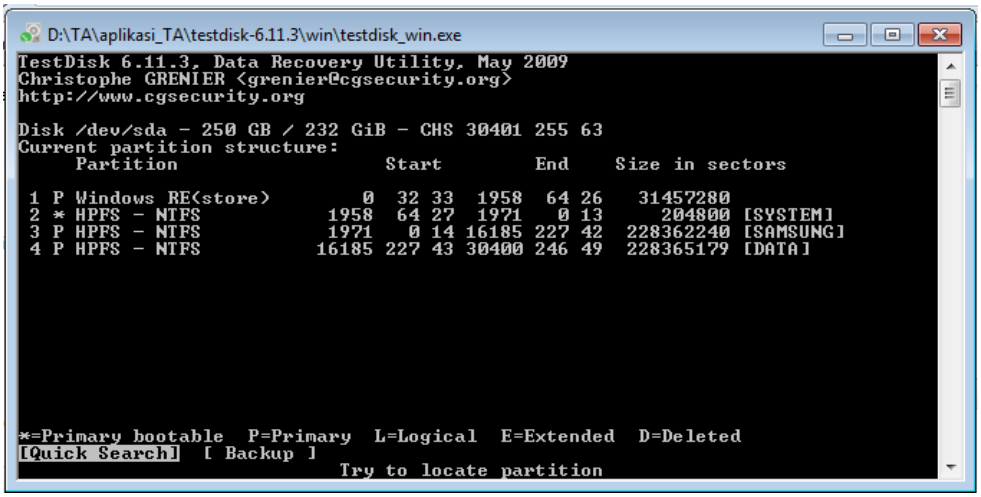
Kemudian menggunakan aplikasi Pandora Recovery, aplikasi ini mampu mengembalikan gambar tersebut, juga menampilkan date created dan date modified.



Gambar 41 Foto yang direcovery Menggunakan Pandora Recovery

6. TestDisk

   Aplikasi ini tidak mendukung dalam proses pengembalian data hilang yang diakibatkan penghapusan data.



Gambar 42 Foto yang direcovery Menggunakan TestDisk

Setelah proses recovery dilakukan, maka foto yang sudah dihapus oleh suaminya itu dapat dikembalikan lagi. Istrinyapun dapat melihat langsung foto yang dimaksud orang yang sms istrinya itu. Setelah dilihat, ternyata benar bahwa suaminya yang berfoto mesra dengan rekan kerjanya di DPR. Berikut ini merupakan gambar foto yang berhasil dikembalikan.

Gambar 43 Foto Mesra Anggota DPR dan Rekan Kerjanya

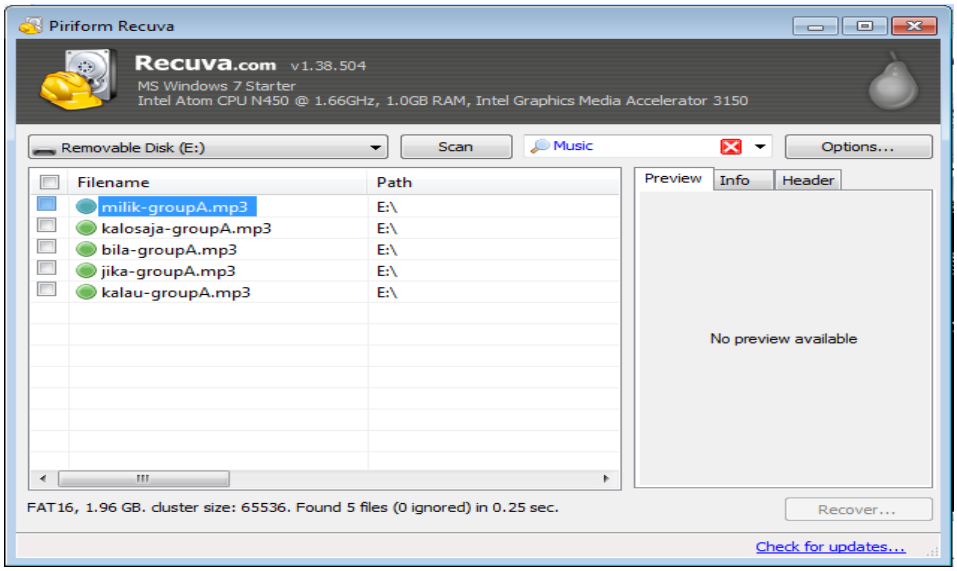
IV.3 Kehilangan MP3

Group Band A melapor kepada pihak berwajib mengenai lagu ciptaannya berjudul Bila yang diplagiat oleh group band B. Lagu ini tersimpan dalam komputer pribadi miliki group band A. Namun karena terkena virus, data lagu tersebut hilang dari hard disk komputer. Tanpa disangka lagu tersebut di klaim sebagai lagu ciptaan group band B. Untuk mengusut laporan ini, pihak polisi meminta bantuan ahli digital forensik untuk menganalisa kebenaran hal tersebut. Ahli digital forensik melakukan recovery hard disk pada komputer group band A untuk menganalisa lagu tersebut.

Dari kasus kehilangan mp3, penyidik melakukan pengujian terhadap 6(enam) aplikasi recovery yang telah tersedia. Pengujian dilakukan guna membuktikan kebenaran data digital yang dilihat dari keakuratan data dalam proses pengembalian data.

1. Recuva

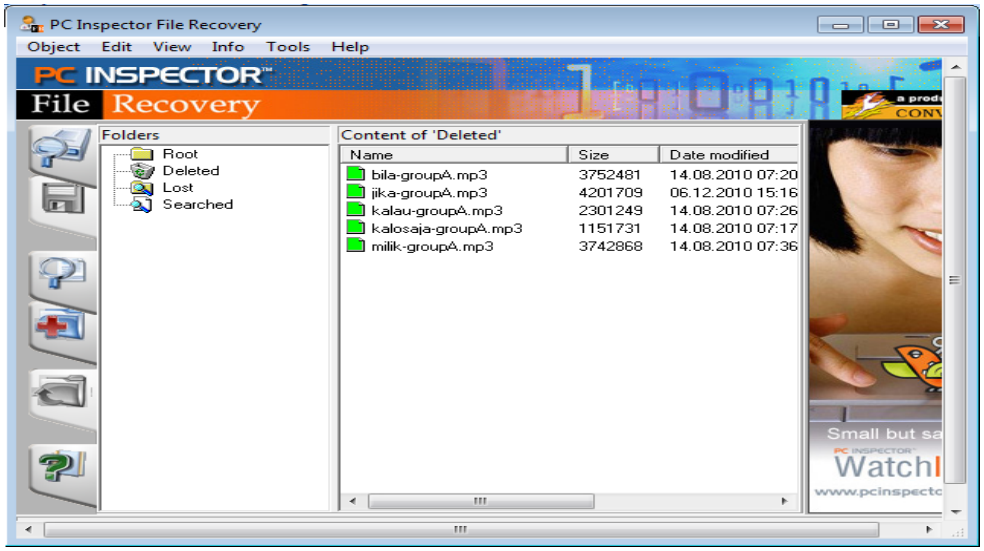
   Pengujian pertama dilakukan pada aplikasi Recuva, aplikasi ini mampu mengembalikan mp3 tersebut. keterangan gambar terlihat di bawah ini:



Gambar 44 Lagu yang direcovery Menggunakan Recuva

2. PC Inspector File Recovery

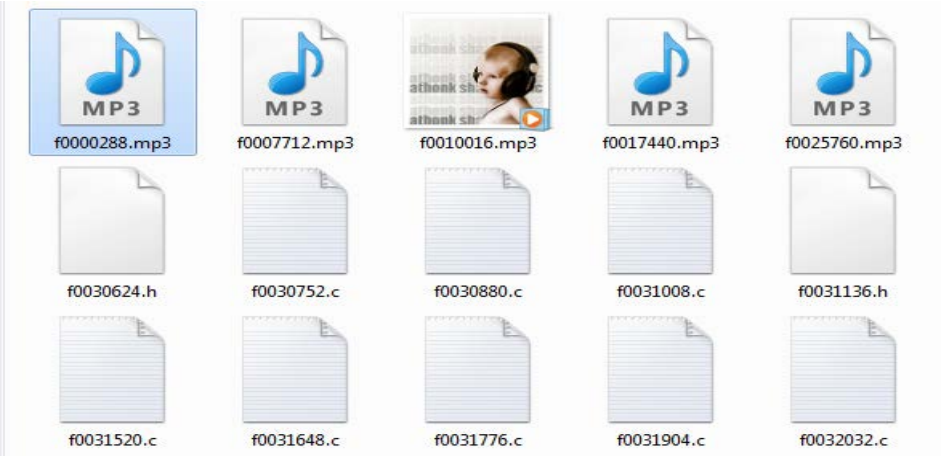
Pengujian kedua dilakukan menggunakan aplikasi PC Inspector File Recovery. Aplikasi ini juga mengembalikan mp3 dan juga menampilkan date modified data tersebut. keterangan gambar terlihat di bawah ini:



Gambar 45 Lagu yang direcovery Menggunakan PC Inspector

3. Photorec

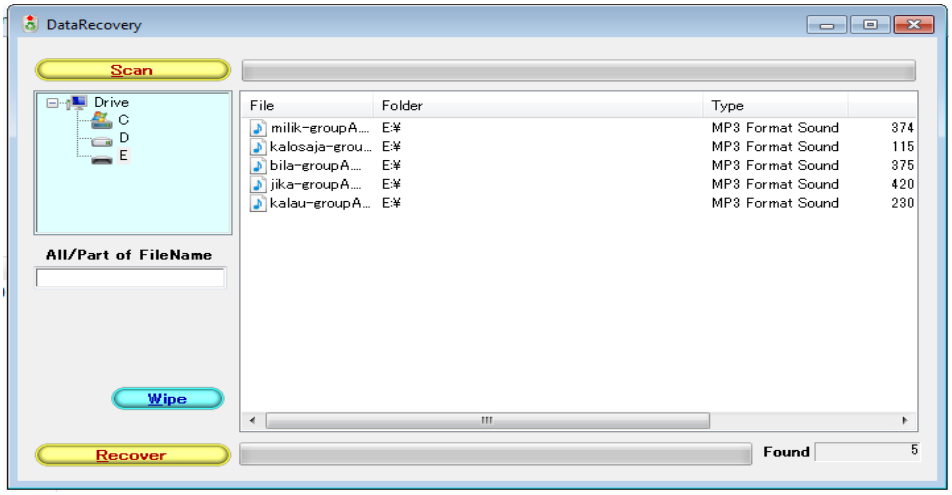
Pengujian aplikasi ketiga yakni Photorec, aplikasi ini mampu mengembalikan mp3 tersebut. keterangan gambar terlihat di bawah ini:



Gambar 46 Lagu yang direcovery Menggunakan Photorec

4. Data Recovery

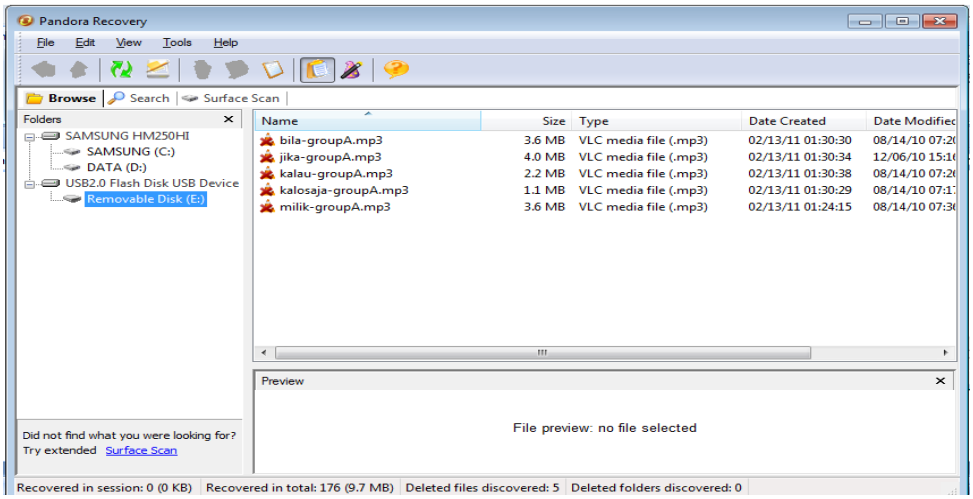
Pengujian keempat dilakukan pada aplikasi Data Recovery, aplikasi ini juga dapat mengembalikan mp3 tersebut. keterangan gambar terlihat di bawah ini:



Gambar 47 Lagu yang direcovery Menggunakan Data Recovery

5. Pandora Recovery

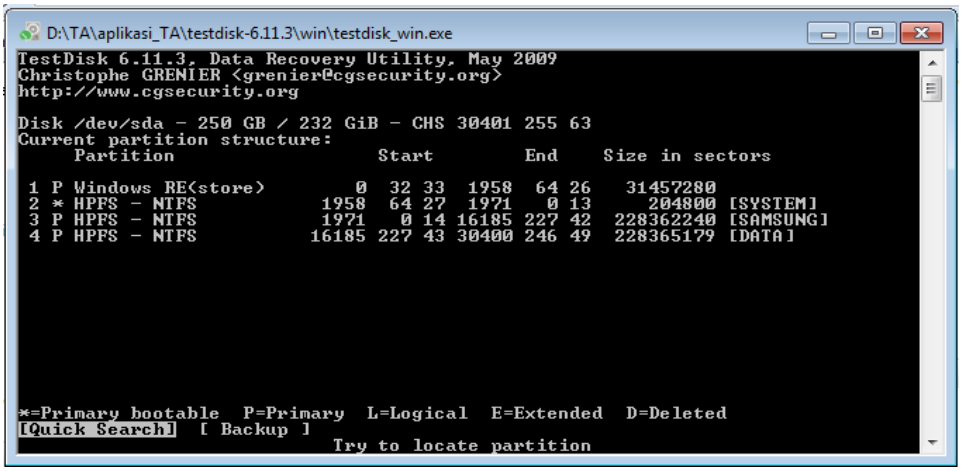
Kemudian aplikasi berikutnya yaitu Pandora Recovery, aplikasi ini mampu mengembalikan mp3 tersebut. keterangan gambar terlihat di bawah ini:



Gambar 48 Lagu yang direcovery Menggunakan Pandora Recovery

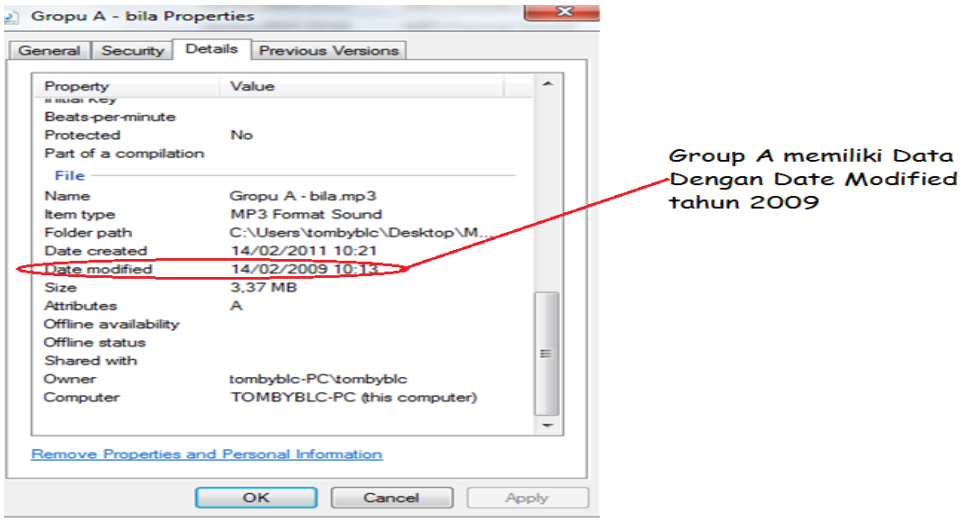
6. TestDisk

Aplkasi ini tidak mendukung proses mengembalian data hilang yang diakibatkan penghapusan data. keterangan gambar terlihat di bawah ini:

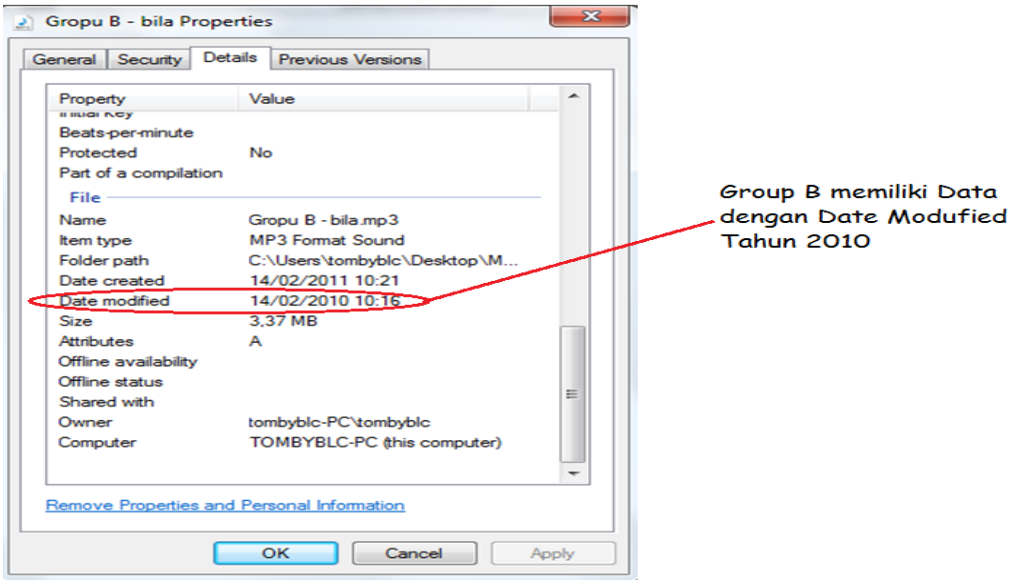


Gambar 49 Lagu yang direcovery Menggunakan TestDisk

Setelah melakukan proses recovery terhadap lagu group A, ternyata benar bahwa lagu group A yang hilang tersebut diplagiat oleh group B. Gambarnya seperti pada gambar.



Gambar 50 Lagu Group A dengan Date Modufied



Gambar 51 Lagu Group B dengan Date Modufied

IV.4 Kehilangan Video

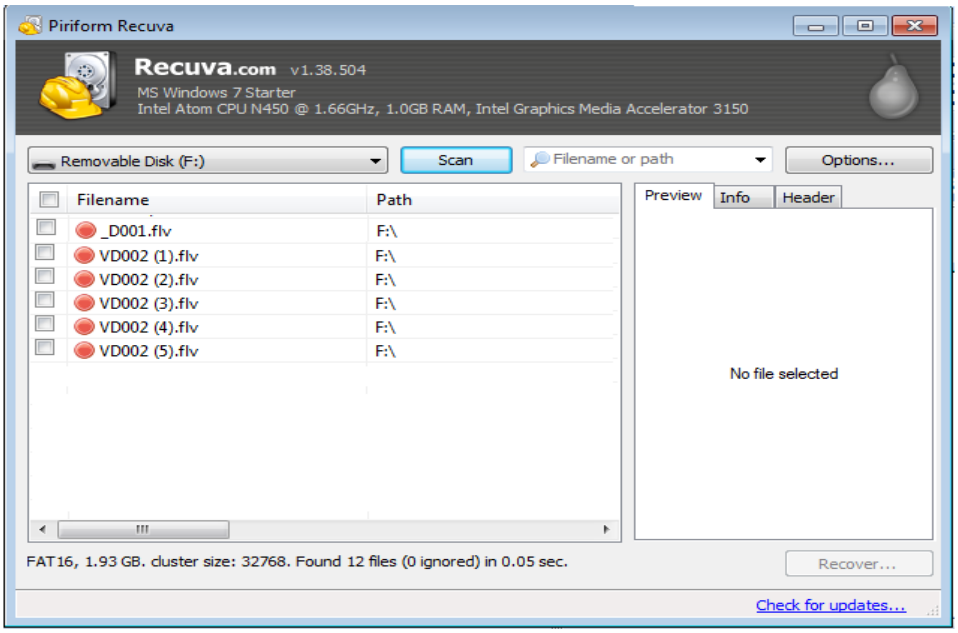
Pada suatu hari direktur perusahaan terkejut karena berangkasnya terbuka dan isinya kosong. Ternyata seorang karyawan perusahaan telah mengetahui video tentang pencurian uang sebesar Rp 150.000.000,- yang terekam di CCTV dalam ruangan direktur perusahaan tersebut. Didalam video, terlihat jelas seorang CS (Cleaning Service) telah membuka paksa berangkas yang berisi uang tersebut. Karena pada hari itu direktur tidak berada dikantor, maka karyawan tersebut tidak bisa memberitahukan hal itu kedirektur perusahaan. Oleh karena itu, video tersebut disimpan di dalam komputer karyawan itu. Seperti mengetahui penyimpanan yang terjadi, CS itupun menghapus video tersebut. Pada keesokan harinya, karyawan itu ingin memberitahukan video tersebut kepada direktur, tetapi setelah dilihat video tersebut sudah tidak ada. Lalu karyawan itu langsung memberitahukan kepada direktur atas kejadian itu. Tetapi sang direktur tidak mempercayai apa yang dikatakan karyawan, karena CS yang dikatakan melakukan pencurian tersebut adalah CS kepercayaan sang direktur. Karena sang direktur marah terhadap karyawan tersebut karena sudah memfitnah CS itu, akhirnya

karyawan itu mendatangkan pihak forensik untuk melacak, menganalisa, atau mengembalikan video tersebut dari komputer karyawan itu.

Dari kasus kehilangan video, penyidik melakukan pengujian terhadap 6(enam) aplikasi recovery. Pengujian dilakukan guna membuktikan kebenaran data digital yang dilihat dari keakuratan dalam proses pengembalian data.

1. Recuva

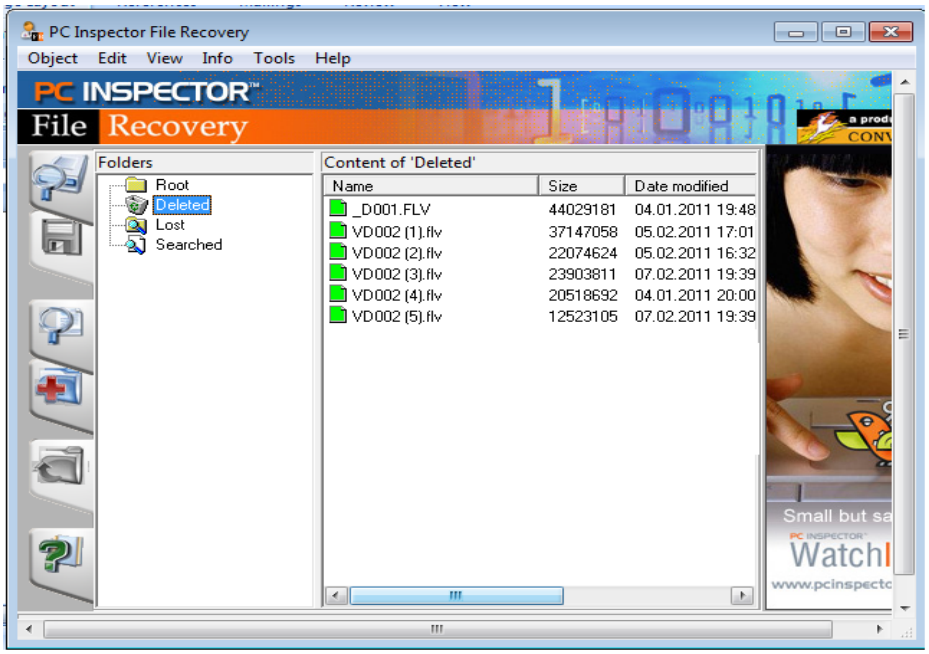
   Pengujian pertama menggunakan aplikasi Recuva, aplikasi ini mampu mengembalikan video tersebut. keterangan gambar terlihat di bawah ini:



Gambar 52 Video yang direcovery Menggunakan Recuva

2. PC Inspector File Recovery

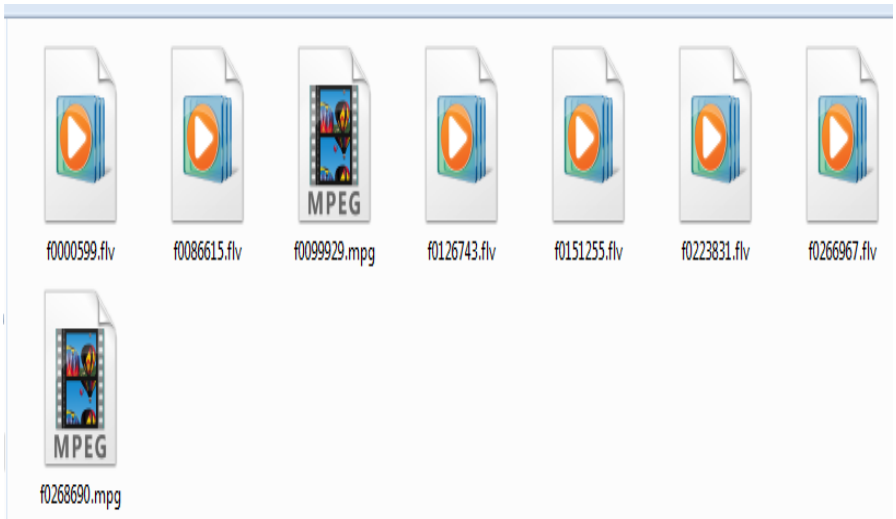
   Pengujian selanjutnya mnggunakan aplikasi PC Inspector File Recovery. Aplikasi ini mampu mengembalikan video tersebut. keterangan gambar terlihat di bawah ini:



Gambar 53 Video yang direcovery Menggunakan Recuva

3. Photorec

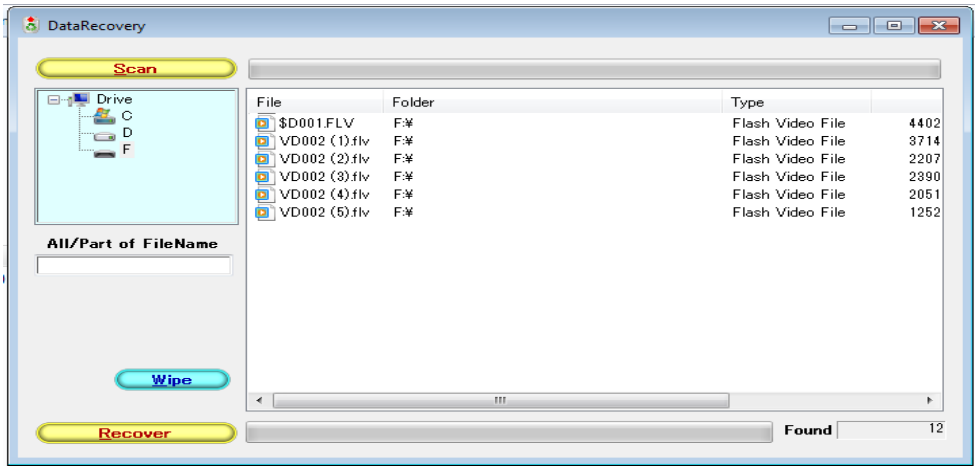
Kemudian, pengujian dilakukan lagi pada aplikasi Photorec. Aplikasi ini juga dapat mengembalikan video tersebut. keterangan gambar terlihat di bawah ini:



Gambar 54 Video yang direcovery Menggunakan Recuva

4. Data Recovery

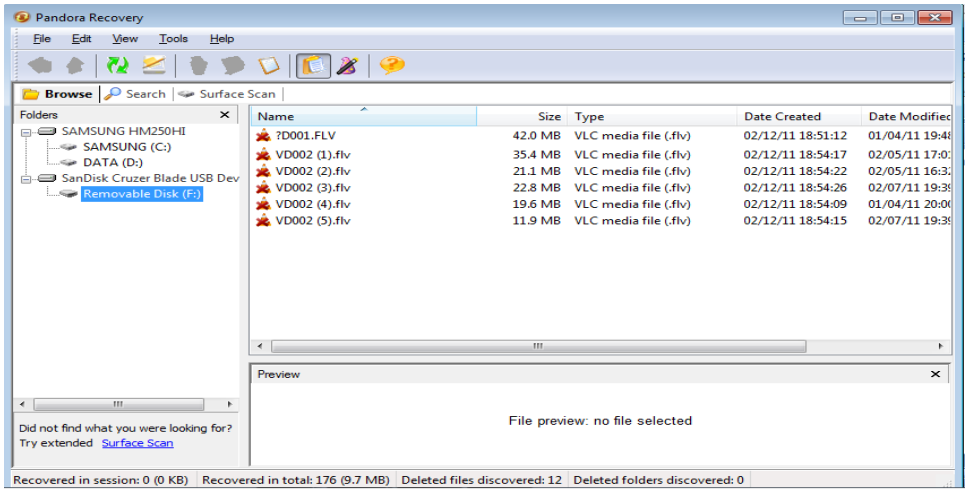
Setelah melakukan pengujian pada aplikasi Photorec, maka penyidik melakukan lagi pengujian pada aplikasi Data Recovery. Aplikasi ini juga dapat mengembalikan video tersebut. keterangan gambar terlihat di bawah ini:



Gambar 55 Video yang direcovery Menggunakan Recuva

5. Pandora Recovery

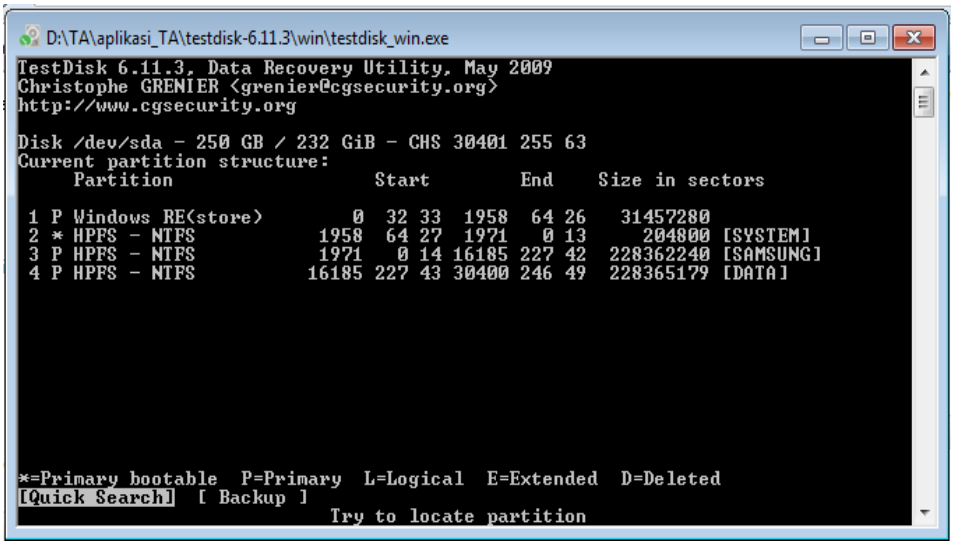
Tahap pengujian selanjutnya yakni menggunakan aplikasi Pandora Recovery. Aplikasi ini dapat juga mengembalikan video tersebut. Keterangan gambar terlihat di bawah ini:



Gambar 56 Video yang direcovery Menggunakan Recuva

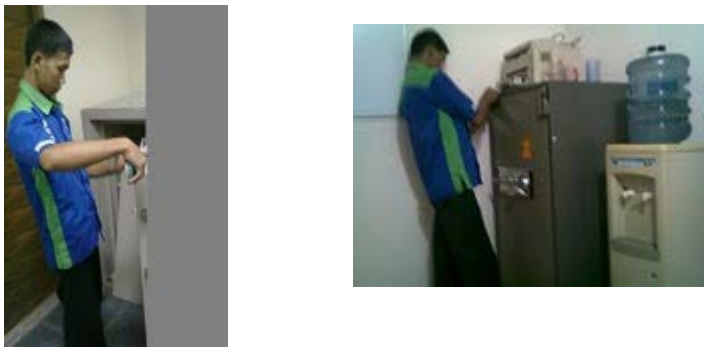
6. TestDisk

   Aplikasi ini tidak mendukung dalam proses pengembalian data hilang yang diakibatkan penghapusan data. keterangn gambar terlihat di bawah ini:



Gambar 57 Video yang direcovery Menggunakan Recuva

Setelah direcovery, akhirnya video yang membuktikan bahwa CS (Cleaning Service) kepercayaan direktur tersebut benar yang membuka dan mengambil uang direktur di dalam berangkas. Hal ini langsung diberitahukan kepada direktur. Berikut ini merupakan gambar yang di *print screen* dari video tersebut.



Gambar 58 CS (Cleaning Service) yang Membuka Berangkas

Bab V Hasil Pengujian

Bab ini berisikan tentang hasil dari pengujian yang telah dilakukan, dengan melihat hasil perbandingan tersebut maka akan dapat terlihat aplikasi mana yang mempunyai banyak keunggulan dalam pengembalian data.

Tabel 2 Hasil Pengujian Aplikasi

Aplikasi Recovery	Proses											
	Delete				Format				Partisi			
	Dokumen	Audio	Gambar	Video	Dokumen	Audio	Gambar	Video	Dokumen	Audio	Gambar	Video
	Doc	MP3	Jpg	Flv	Doc	MP3	Jpg	Flv	Doc	MP3	Jpg	Flv
Recuva	√	√	√	√	√	√	√	√	X	X	X	X
PC Inspector File Recovery	√	√	√	√	X	X	√	X	X	X	X	X
Data Recovery	√	√	√	√	√	X	X	X	X	X	X	X
Pandora Recovery	√	√	√	√	X	X	√	X	X	X	X	X
TestDisk	X	X	X	X	X	X	X	X	√	√	√	√
Photorec	√	√	√	√	√	√	√	√	X	X	X	X

Keterangan : √ = Baik (Poin 100)

X = Buruk (Poin 0)

Setiap 1 file bernilai 25

100 = Sangat Baik

75 = Baik

50 = Sedang

25 = Buruk

0 = Sangat Buruk

Setelah melakukan pengujian dengan menggunakan kasus-kasus yang ada, selanjutnya membuat hasil dari tiap-tiap aplikasi yang sudah dilakukan pengujian.

Tabel 3 Hasil dari tiap aplikasi

Proses	Recuva	PC Inspector File Recovery	Data Recovery	Pandora Recovery	TestDisk	Photorec
Delete	100	100	100	100	0	100
Format	100	25	25	25	0	100
Partisi	0	0	0	0	100	0

Pada keterangan tabel nilai pengujian diatas, maka akan terlihat bahwa aplikasi mana yang banyak memiliki keunggulan dari segi pengembalian data pada saat dihapus ataupun diformat.

Bab VI Kesimpulan dan Saran

VI.1 Kesimpulan

Dari hasil analisis dan pengujian yang dilakukan, Photorec dan TestDisk merupakan aplikasi yang paling banyak memenuhi kebutuhan forensik yaitu, mengumpulkan data, melakukan pengujian, dan mengembalikan bukti digital dengan baik. Sedangkan ke empat aplikasi yang lain, proses pengembalian bukti digitalnya kurang baik, karena dapat mengembalikan file-file tertentu seperti dokumen ,gambar, video dan audio.

VI.2 Saran

Adapun saran yang diberikan sebagai bahan pertimbangan demi meningkatkan kualitas komputer forensik dalam pengembalian data adalah:

1. Mampu melakukan perbandingan aplikasi *recovery* lainnya yaitu, ADRC Data Recovery Software Tools, Avira UnErase Personal, FreeUndelete, Glary Undelete, SoftPerfect File Recovery, dan free wipe wizard.
2. Diharapkan pengembang selanjutnya dapat melakukan uji coba selain sistem operasi Windows yaitu, Linux dan MacOS.

DAFTAR PUSTAKA

[1] Wikipedia bahasa Indonesia, "*Forensik*", (2010, Juni 24). Tersedia : http://wikipwedia.org/wiki/forensik

[2] Kang Deden, "*Mengenal Teknologi Hard disk*", (2007, Agustus 14). Tersedia : http://dedenthea.wordpress.com

[3] *Disk* doktor,"*Download Demo*".Tersedia: http://translate.*user*googlecontent.com

[4] Izirock, "*Adu Jago Software Recovery* ", (2010, Maret 27). Tersedia : http://izirock.blogspot.com

[5] Rantarou Ryoku-Uchi, "*All About Hard disk*". Tersedia : http:// www.kazoku-community.com

[6] *Paulus Joko Purwanto*, "Mengapa Komputer Perlu *Hard disk*", (2009, April 04) Tersedia :http://pointeruksw.blogspot.com

[7] Agustin Nurul Fahmi, "Me*recovery* Partisi Yang Hilang atau Rusak Menggunakan Test*Disk*", (2010, Juli 10). Tersedia http://palinukan.org

[8] Simarmata Janner, "*Pengenalan Teknologi Komputer dan Informasi*". ANDI : Yogyakarta,2007, pp.130-141.

[9] "*Menginstal dan memakai PC Inspector File Recovery*" (2009, Juli 22).Tersedia http://4.bp.blogspot.com

[10] GNU FDL Free Doc License "*TestDisk, Data Recovery*", (2009, April 19). Tersedia: http://www.cgsecurity.org

[11] Jason Brightman "*Free Hard disk Utilities: Recover Deleted Files and Lost Data*", (1998-2007). Tersedia: http://www.pcworld.com

[12] Freebyte.com"*Free Data Recovery Tools*", (1995-2010). Tersedia:http://ultrahosting.com

[13] Kasku.as, ”Bagian-bagian dalam dari *hard disk*”, (2010, juli 12). Tersedia: http://www.t-w-t.co.cc

[14] Shinta Dewi, *“bagian dalam hard disk”*, (2010, Juni 12). Tersedia: http://ruangberita.com

[15] Lukman, *” Cara Menghitung Kapasitas Hard disk Yang Benar”*, (2009, Oktober 10).Tersedia :http://cyberkios.com

[16] *“PC Inspector File Recovery”*. Tersedia: http://www.pcinspector.de/*file_recovery*/welcome.htm

[17] *“TestDisk”*. Tersedia : http//www.cgsecurity.org/wiki/Test*Disk*

[18] Anders Svensson. *“Computer Forensik Apllied to Windows NTFS Computer”*.3 Januari 2008. http:/www.dsv.su.se/research/seclab/pages/pdf-*file*s/2005-x-268.pdf>

[19]. Budhisantoso, Nugroho, Personal Site, alamat: www.forensik-komputer.inf0

[20]. Budiman, Rahmadi, 2003, *Makalah Tugas Keamanan Sistem Lanjut, Komputer Forensik Apa Dan Bagaimana***,** Magister Teknik Elektro Option Teknologi Informasi, Institut Teknologi Bandung.2003