# APLIKASI RECOVERY HARD DISK UNTUK KEPENTINGAN FORENSIK

## TUGAS AKHIR

Oleh :


**Ucok Charly Hutagalung 3310801004**

**Bayu Pratama Putra 3310801042**


Disusun untuk memenuhi syarat kelulusan Program Diploma III


**PROGRAM STUDI TEKNIK INFORMATIKA**

**POLITEKNIK NEGERI BATAM**

**BATAM**


**2011**

# LEMBAR PENGESAHAN

Batam, 14 September 2011

**Pembimbing,**

**Agus Fatulloh**

**NIK. 107051**

# LEMBAR PERNYATAAN

Dengan ini, saya:

NIM : 3310801004

Nama : Ucok Charly Hutagalung

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

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, 14 September 2011

**Ucok Charly Hutagalung**
3310801004

# LEMBAR PERNYATAAN

Dengan ini, saya:

NIM : 3310801042

Nama : Bayu Pratama Putra

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

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, 14 September 2011

**Bayu Pratama Putra**
3310801119

# KATA PENGANTAR

Puji syukur atas kehadirat Tuhan Yang Maha Esa atas karunia-Nya penyusun dapat menyelesaikan Tugas Akhir yang berjudul "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. Tuhan Yang Maha Esa 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 mengembangkannya.

Batam, 14 September 2011

Penyusun

# ABSTRAK

## APLIKASI RECOVERY HARD DISK UNTUK KEPENTINGAN FORENSIK

Kegiatan komputer forensik yaitu sebagai proses mengidentifikasi, memelihara, menganalisa dan mempergunakan bukti digital menurut hukum yang berlaku. Komputer forensik dikelompokkan dalam beberapa bidang di antaranya, *Internet* Forensik, *Network* Forensik, *Disk* Forensik dan *System* Forensik. *Disk* forensik adalah ilmu yang membahas tentang bukti fisik meliputi penghapusan data dan kehilangan data yang terjadi pada *disk* penyimpanan seperti *hard disk*. Komputer forensik dalam hal pengembalian data di dalam *hard disk* dilakukan untuk mengembalikan data yang hilang baik disengaja maupun tidak, bahkan setelah *hard disk* diformat atau digunakan orang lain.

Kata kunci: komputer forensik, *hard disk*.

# ABSTRACT

## HARD DISK RECOVERY APPLICATIONS FOR FORENSIC INTEREST

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 and System Forensics. 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. Computer forensics in terms of return data on the hard disk is performed to recover the lost data either intentionally or not, even after the hard disk is formatted or used by others.

Index Terms: computer forensics, hard disk.

# DAFTAR ISI


Bab I Pendahuluan ..... 1
I.1 Latar Belakang ..... 1
I.2 Rumusan Masalah ..... 1
I.3 Batasan Masalah ..... 2
I.4 Tujuan ..... 2
I.5 Sistematika Penulisan ..... 2
Bab II Tinjauan Pustaka ..... 3
II.1 Komputer Forensik ..... 3
II.2 Hard Disk ..... 6
II.3 File Sistem ..... 14
II.4 Open Source ..... 16
II.5 Perbandingan antar Tugas Akhir ..... 19
Bab III Survei Aplikasi ..... 20
III.1 Hasil Survei Aplikasi Recovery Terkait ..... 20
III.2 Aplikasi Recovery yang Tersedia ..... 20
Bab IV Pengujian ..... 23
IV.1 Perbandingan Aplikasi Recovery ..... 23
IV.1.1 Foremost ..... 23
IV.1.2 Scapel ..... 25
IV.1.3 Test Disk ..... 27
IV.1.4 Photorec ..... 28
IV.2 Skenario Pengujian ..... 30
IV.2.1 Kehilangan Dokumen ..... 30
IV.2.2 Kehilangan Gambar ..... 33
IV.2.3 Kehilangan Rekaman ..... 36
IV.2.4 Kehilangan Video ..... 39
IV.3 Identifikasi User Linux ..... 43

Bab V Hasil Pengujian ..... 46
Bab VI Kesimpulan dan Saran ..... 48
VI.1 Kesimpulan ..... 48
VI.2 Saran ..... 48
DAFTAR PUSTAKA ..... 49

# DAFTAR GAMBAR

Gambar 1 Tahap-Tahap Komputer Forensik ..... 5
Gambar 2 Komponen-komponen Hard Disk ..... 11
Gambar 3 Proses scanning data yang dihapus ..... 24
Gambar 4 Proses scanning data yang diformat ..... 24
Gambar 5 Hasil dari scanning Foremost ..... 25
Gambar 6 Hasil pengembalian data yang dihapus ..... 25
Gambar 7 Proses scanning Scalpel ..... 26
Gambar 8 Hasil Pengembalian data yang diformat ..... 26
Gambar 9 Menganalisa Partisi ..... 27
Gambar 10 Proses scanning partisi ..... 28
Gambar 11 Hasil scanning TestDisk ..... 28
Gambar 12 Proses scanning Photorec ..... 29
Gambar 13 Proses scanning Photorec data diformat ..... 29
Gambar 14 LK_juli2011 yang dikembalikan menggunakan Photorec ..... 31
Gambar 15 LK_juli2011 yang dikembalikan menggunakan Foremost ..... 31
Gambar 16 LK_juli2011 yang dikembalikan menggunakan Scalpel ..... 32
Gambar 17 TestDisk ..... 32
Gambar 18 LK_juli2011 ..... 33
Gambar 19 Foto yang dikembalikan menggunakan Photorec ..... 34
Gambar 20 Foto yang dikembalikan menggunakan Foremost ..... 34
Gambar 21 Foto yang dikembalikan menggunakan Scalpel ..... 35
Gambar 22 TestDisk ..... 35
Gambar 23 Foto suap pejabat dengan pengusaha ..... 36
Gambar 24 Rekaman yang dikembalikan menggunakan Photorec ..... 37
Gambar 25 Rekaman yang dikembalikan menggunakan Foremost ..... 37
Gambar 26 Rekaman yang dikembalikan menggunakan Scalpel ..... 38
Gambar 27 TestDisk ..... 38

Gambar 28 Video yang dikembalikan menggunakan Photorec ..... 40
Gambar 29 Video yang dikembalikan menggunakan Foremost ..... 40
Gambar 30 Video yang dikembalikan menggunakan Scalpel ..... 41
Gambar 31 TestDisk ..... 41
Gambar 32 Tersangka di atas motornya ..... 42
Gambar 33 Tersangka mengambil helm ..... 42
Gambar 34 Tersangka meninggalkan area parkir ..... 43
Gambar 35 Pencarian dengan Finger ..... 43
Gambar 36 Pencarian dengan perintah Who ..... 43
Gambar 37 Folder /var/log/ ..... 44
Gambar 38 File auth.log ..... 45

# DAFTAR TABEL

Tabel 1 Ukuran RPM ..... 12
Tabel 2 Perbandingan TA ..... 19
Tabel 3 Spesifikasi File ..... 23
Tabel 4 Hasil Pengujian Aplikasi ..... 46
Tabel 5 Hasil Pengujian Aplikasi ..... 47
Tabel 6 Hasil dari tiap Aplikasi ..... 47

# Bab I Pendahuluan

## I.1 Latar Belakang

Komputer menjadi salah satu perangkat elektronik yang paling banyak digunakan untuk membantu pekerjaan manusia saat ini terutama dalam hal pengolahan data. Data yang tersimpan dalam komputer biasanya terdapat di dalam *hard disk,* yang merupakan salah satu media penyimpanan data. Hal ini membuat data yang tersimpan di dalam *hard disk* bisa saja hilang baik secara disengaja maupun tidak, oleh karena itu komputer forensik dibutuhkan untuk mengamankan dan menganalisis data *digital* tersebut.

Dapat dibayangkan jika sebuah dokumen yang sudah dikerjakan tiba-tiba hilang. Kehilangan data ini bisa disebabkan oleh virus atau mungkin ada yang sengaja menghapusnya. Sebagian besar orang mungkin menganggap bahwa data tersebut benar-benar hilang, namun sebenarnya data tersebut masih ada di dalam *hard disk*. Kejadian seperti ini bisa diatasi dengan menggunakan aplikasi forensik *recovery hard disk* yang berfungsi untuk mengembalikan *file-file* yang telah terhapus.

Aplikasi *recovery* dapat dikategorikan menjadi dua, yaitu aplikasi komersil/ berbayar (*shareware*) dan aplikasi *free*/ *open source.* Seiring dengan maraknya penggunaan aplikasi *open source* saat ini, maka bisa ditentukan aplikasi *recovery hard disk* berbasis *open source* mana yang lebih baik untuk kepentingan forensik. Selain itu, dengan berbagai fitur yang berbeda dari beberapa aplikasi tersebut bisa diteliti apakah di antaranya memiliki kualitas dan keunggulan setara dengan aplikasi *shareware* yang berbayar.

## I.2 Rumusan Masalah

Rumusan masalah dari Tugas Akhir ini adalah bagaimana menentukan aplikasi *recovery hard disk* berbasis *open source* yang terbaik untuk kepentingan forensik.

## I.3 Batasan Masalah

Adapun batasan masalah dari penyelesaian Tugas Akhir ini adalah:

1. Hanya menganalisis data *recovery* yang diakibatkan dari kerusakan non fisik.
2. Hanya menggunakan sistem operasi Linux.

## I.4 Tujuan Penelitian

Tujuan dari analisis ini adalah mengetahui aplikasi *recovery open source* terbaik dalam hal pengembalian data berdasarkan kebutuhan forensik.

## I.5 Sistematika Penulisan

Dalam penulisan suatu laporan perlu adanya Sistematika Penulisan begitu juga pada laporan Tugas Akhir ini, semua isinya disusun secara sistematika. Hal ini sangat penting selain untuk menghindari kekeliruan atau salah tafsir juga memudahkan dalam membaca maupun menganalisa dan memahami secara keseluruhan isinya. Adapun Sistematika Penulisan laporan Tugas Akhir ini adalah sebagai berikut:

BAB I Pendahuluan berisikan latar belakang, rumusan masalah, batasan masalah, tujuan dan sistematika penulisan.

BAB II Landasan teori menerangkan teori dasar yang digunakan untuk mendukung penyelesaian Tugas Akhir ini.

BAB III Survei aplikasi berisi penjelasan pemilihan aplikasi yang digunakan untuk menyelesaikan Tugas Akhir ini.

BAB IV Pengujian aplikasi berisi tentang penggunaan aplikasi dalam menyelesaikan Tugas Akhir ini.

BAB V Hasil pengujian berisi tentang hasil pengujian aplikasi.

BAB VI Kesimpulan dan Saran berisi simpulan-simpulan yang merupakan rangkuman dari hasil analisis kinerja pada bagian sebelumnya dan saran-saran pengembangan dari penelitian yang dibuat dan aspek yang belum terselesaikan.

# Bab II Tinjauan Pustaka

## II.I Komputer Forensik

Dalam kehidupan sehari-hari komputer digunakan untuk mendukung pekerjaan manusia, tapi disisi lain komputer merupakan suatu sarana dan objek dari suatu tindak kriminal. Sebagai sarana komputer dapat digunakan untuk mencuci uang oleh para penjahat. Memanipulasi data penjualan dan keuangan oleh pengemplang pajak, sebagai sarana komunikasi oleh para teroris dan lain-lain.

Sedangkan sebagai objek, komputer digunakan sebagai objek sasaran serangan, pengerusakan data oleh para *hacker* atau *cracker*. Oleh karena itu serangan-serangan seperti ini yang membuat para pengguna komputer merasa tidak nyaman dalam menggunakan komputer. Tindakan ini merupakan salah satu tindak kriminal yang bisa disebut dengan *cyber crime*, sehingga banyak negara yang telah meratifikasi komputer forensik sebagai bukti legal yang diterima oleh hukum.

Bidang komputer forensik memang masih seumur jagung. Namun makin berkembangnya metode-metode baru dalam melakukan *cyber crime*, komputer forensik memang sangat dibutuhkan. Para penyidik menyadari perkembangan ini dan membutuhkan suatu alat yang dapat mengimbangi berkembangnya *cyber crime*. Sehingga penyidik dapat menemukan bukti dari kejahatan yang berhubungan dengan komputer.

Bekerja sama dengan ahli dan praktisi komputer, secara bertahap para penyidik membuat prosedur untuk mendapatkan bukti dari komputer. 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.

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 di luar *term* teknologi (berhubungan dengan investigasi dan investigasi bukti-bukti intelejen dalam penegakan hukum dan militer) sejak pertengahan tahun 1980-an.
2. Menurut Budhi Santoso, 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 menganalisis 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 menganalisis 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 dianalisis.

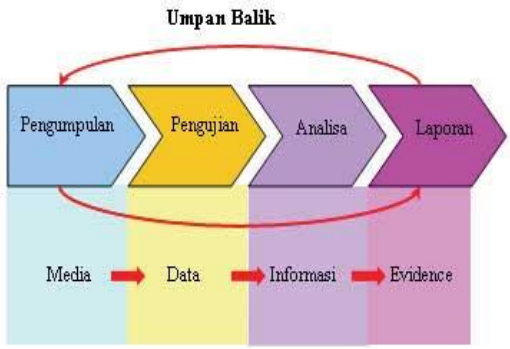
Kegiatan komputer forensik adalah suatu proses mengidentifikasi, memelihara, menganalisis dan mempergunakan bukti *digital* menurut hukum yang berlaku. Dengan tujuan untuk menjabarkan sebuah *system* komputer berupa media

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

Dalam melakukan prosesnya, forensik melibatkan tiga komponen yang dirangkai dan melibatkan tiga komponen yang dirangkai dan dikelola sedemikian rupa menjadi tujuan dengan segala kelayakan dan kualitas.

Tiga komponen ini mencakup 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, yaitu pengumpulan, pengujian, analisis dan laporan. Ada objek yang dikelola dari proses setiap fase, dimulai dari media dan kemudian didapati "*evidence*" diakhir proses. Tentunya umpan balik diberlakukan untuk menganalisis kembali hasil yang didapat dengan tujuan semula. Berikut ini merupakan fase-fase yang dilakukan komputer forensik.




**Gambar 1 Tahap-Tahap Komputer Forensik**

Di dalam 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 kebutuhan tersebut.

## II.2 Hard Disk

Secara umum istilah *hard disk* dikenal sebagai sebuah penyimpanan pada komputer. *Hard disk* (piringan keras) adalah sebuah komponen perangkat keras yang menyimpan data sekunder dan berisi piringan magnetis. 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* berbentuk piringan hitam yang terbuat dari alumunium dan dilapisi bahan magnetic.

Pertama kali, *hard disk* diciptakan oleh Reynold Johnson, salah seorang insinyur IBM pada tahun 1956. Awalnya *hard disk* terdiri dari 50 piringan berukuran 2 kaki (0,6 meter) dengan kecepatan rotasinya mencapai 1.200 rpm *(rotation per minute)* dengan kapasitas penyimpanan 4,4 MB. Dan saat ini *hard disk* dengan lebar 0,6 cm berkapasitas 750 GB, juga secara fisik menjadi semakin tipis dan kecil tetapi dapat menyimpan data berkapasitas besar, serta dapat dipasang dalam

perangkat (internal) dan di luar perangkat (eksternal) dengan menggunakan kabel USB ataupun *FireWire*.

Komponen-komponen *hard disk* yang terdiri dari: *Platter, Head, Actuator Axis, Actuator Arms, Interface, Jumper, Power Connectors, Ribbon Cable* dan *Spindle Motor.*

1. Platter

   Piringan logam hitam (*platter*) yang berfungsi sebagai tempat penyimpanan data. Jumlah piringan ini beragam, mulai 1,2,3 atau lebih. Piringan ini diberi lapisan bahan magnetis yang sangat tipis (ketebalan dalam orde persejuta inci). Pada saat ini digunakan teknologi *thin film* (seperti pada processor) untuk membuat lapisan tersebut.

2. Head

   *Head* berupa kumparan. *Head* pada *hard disk* berbeda dengan *head* pada tape. Pada tape proses baca tulis (rekam) menggunakan dua *head* yang berbeda, sedangkan pada *hard disk* proses baca dan tulis menggunakan *head* yang sama. *Hard disk* biasanya mempunyai *head* untuk setiap sisi-sisi *platter*, untuk *hard disk* dengan dua *platter* dan dapat memiliki 4 *head*, *hard disk* dengan tiga *platter* dapat memiliki sampai enam *head*. Namun, tidak berarti *hard disk* dengan 16 *head* harus memiliki 8 *platter*. Hal ini dikenal dengan istilah translasi.

3. Actuator Axis

   Actuator axis adalah poros untuk menjadi pegangan atau sebagai tangan robot agar *head* dapat membaca sector dari *hard disk.*

4. Actuator Arms

   *Slider* merupakan tempat menempelnya *head*. Dan untuk pergerakannya, *slider* sendiri melekat pada sebuah tangkai yang disebut *actuator arms.*

5. Interface

   Beberapa teknologi *interface hard disk,* sebagai berikut: *Integrated Drive Electronis (IDE), AT Attachment (ATA), Mode PIO, Mode DMA* dan *Block Mode.*

   a. Integrated Drive Electronis (IDE)

      Standar konsumen untuk *interface* kalah jauh dengan SCSI, tetapi jauh lebih murah. *Interface* IDE sekarang ini memiliki dua *channel* yang memungkinkan dua *device* tiap *channel*, apakah itu *hard disk*, CD atau *storage* lain. IDE yang asli dahulu hanya mendukung satu *hard disk* dalam *channel* dan *transfer rate* rata-rata 2-3MB/s. Kebanyakan papan IDE hanya mempunyai satu *channel*, hanya mendukung dua *drive*. *Drive* CD-ROM ketika menggunakan *interface* yang mirip *floopy disk*, dihubungkan pada *sound card.*

   b. AT Attachment (ATA)

      Untuk mendalami ATA perlu memahami tentang dasar-dasar teknologi *hard disk*. Pada prinsipnya ketika suatu sistem operasi akan melakukan operasi baca/ tulis ke *hard disk*, perintah ini diberikan pada BIOS kemudian BIOS yang meneruskannya ke *hard disk.* Sistem operasi lain yang memiliki I/O subsistem sendiri adalah Windows 95, Windows NT dan UNIX, kode-kode pada BIOS dibuat sendiri dalam I/O subsistem tanpa melalui BIOS. Pengaksesan *hard disk* dilakukan dengan menggunakan *register-register* yang dilanjutkan dengan menggunakan sinyal-sinyal. Pembentukan sinyal-sinyal ini dikontrol oleh BIOS, tetapi pengaturan waktu *(timing)* ditentukan oleh *interface hardware*. Spesifikasi ATA menentukan seberapa cepat sinyal-sinyal ini dikirim dan diterima. Saat ini ada beberapa mode PIO *(Programmed Input/ Output)* dan beberapa mode DMA (*Direct Memory Access*). Mode-mode ini menentukan seberapa cepat *transfer rate* yang dihasilkan. Spesifikasinya menentukan seberapa cepat I/O dapat membaca atau menulis.

c. Mode PIO

Mode PIO menentukan seberapa cepat data di*transfer* dari dan ke *hard disk*. Sekarang ini BIOS mendukung penggunaan PIO 0 sampai PIO 4. Biasanya BIOS secara otomatis mendeteksi mode PIO mana yang memaksakan suatu mode PIO yang terlalu tinggi, kemungkinan besar akan ada masalah dalam mengakses *hard disk*.

d. Mode DMA

*Direct Memory Access* (DMA) berarti data *transfer* langsung antara *hard disk* dengan *memory* tanpa menggunakan CPU. Cara ini berlawanan dengan PIO yang menggunakan CPU. Keuntungan menggunakan mode DMA amat terasa pada sistem operasi *multitasking* seperti UNIX karena *transfer* data dengan mode DMA akan menghemat *resource* CPU.

e. Block Mode

*Block mode* biasanya dapat diaktifkan melalui *setup* BIOS. *Block mode* adalah salah satu cara untuk mempercepat *transfer* data. Cara yang digunakan adalah memungkinkan pemberian beberapa perintah baca atau tulis secara bersamaan.

Setiap ada perintah membaca atau menulis maka IRQ akan dibangkitkan sehingga CPU akan melakuan proses *switching*, memeriksa *device* dan melakukan *setup* untuk *transfer* data. Jika setiap ada perintah CPU melakukan ini, tentunya akan menghabiskan waktu. Dengan *block mode*, dalam setiap aksesnya *hard disk* akan memproses beberapa sektor sekaligus tanpa membangkitkan *interrupt* melalui IRQ.

6. Jumper

Setiap *hard disk* memiliki *setting jumper*, fungsinya untuk menentukan kedudukan *hard disk* tersebut. Bila komputer dipasang 2 buah *hard disk*, maka dengan mengatur setting jumper dapat menentukan *hard disk* primer dan *hard disk* sekunder yang biasanya disebut *Master* dan *Slave*. *Master* adalah *hard disk* utama tempat sistem di instal, sedangkan *Slave* adalah *hard*

*disk* ke dua biasanya dibutuhkan untuk tempat penyimpanan dokumen dan data. Bila *jumper setting* tidak di set, maka *hard disk* tersebut tidak akan bekerja.

7. Power connectors

   *Power connectors* adalah sumber arus yang langsung dari *power supply*. *Power supply* pada *hard disk* ada dua bagian :

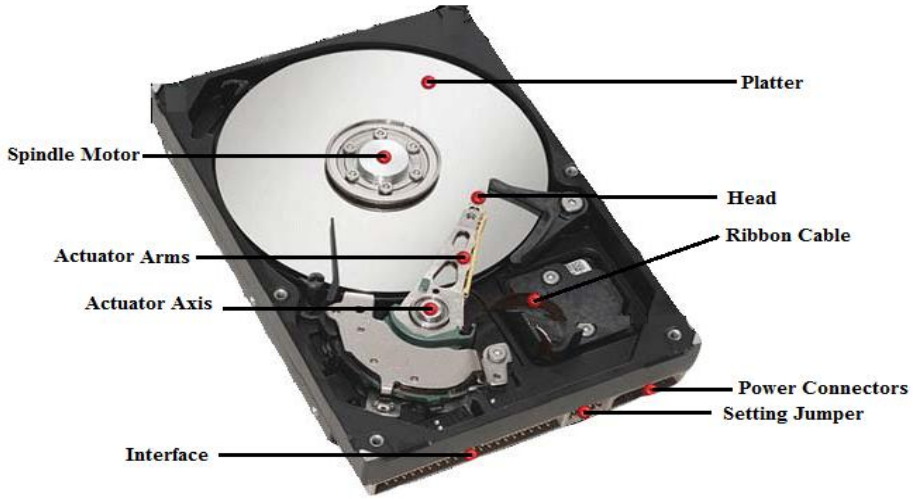
   1. Tegangan 12 Volt, berfungsi untuk menggerakkan mekanik seperti piringan dan *head.*
   2. Tegangan 5 Volt, berfungsi untuk persediaan daya pada *Logic Board* agar dapat bekerja mengirim dan menerima data.

8. Ribbon Cable

   *Ribbon cable* adalah penghubung antara *Head* dengan *Logic Board,* dimana setiap dokumen atau data yang dibaca oleh *Head* akan dikirim ke *Logic Board* untuk selanjutnya di kirim ke *Mother Board* agar *Processor* dapat memproses data tersebut sesuai dengan *input* yang diterima.

9. Spindle Motor

   *Spindle* merupakan suatu poros tempat meletakan *platter*. Poros ini memiliki sebuah penggerak yang berfungsi untuk memutar pelat *hard disk* yang disebut dengan *spindle* motor. *Spindle* inilah yang berperan dalam menentukan kualitas *hard disk* karena semakin cepat putarannya, berarti semakin bagus kualitas *hard disk*nya. Satuan untuk mengukur perputaran adalah *Rotation Per Minutes* atau RPM. Ukuran yang sering didengar untuk kecepatan perputaran ini antara lain 5400 RPM, 7200 RPM atau 10000 RPM.




**Gambar 2 Komponen-Komponen *Hard Disk***

Pada proses baca tulis data pada *hard disk*, saat sebuah sistem operasi mengirimkan data kepada *hard drive* untuk direkam, *drive* tersebut memproses data tersebut menggunakan sebuah formula matematikal yang kompleks yang menambahkan sebuah bit ekstra pada data tersebut. Bit tersebut tidak memakan tempat dan kemudian, saat data diambil bit ekstra tersebut memungkinkan *drive* untuk mendeteksi dan mengkoreksi kesalahan acak yang disebabkan oleh variasi dari medan magnet di dalam *driver* tersebut.

Kemudian, *drive* tersebut menggerakkan *head* melalui *track* yang sesuai dari *platter* tersebut. Waktu untuk menggerakkan *head* tersebut dinamakan "*seek time*". Saat berada di atas *track* yang benar, *drive* menunggu sampai *platter* berputar hingga sector yang diinginkan berada di bawah *head*. Jumlah waktu tersebut dinamakan "*drive latency*". Semakin pendek waktu `*seek*` dan `*latency*`, semakin cepat *drive* tersebut menyelesaikan pekerjaannya. Saat komponen elektronik *drive* menentukan bahwa sebuah *head* berada di atas sector yang tepat untuk menulis data, *drive* mengirimkan pulsa elektrik pada *head* tersebut. Pulsa tersebut menghasilkan sebuah medan magnetik yang mengubah permukaan magnetik pada *platter*. Variasi yang terekam tersebut sekarang mewakili sebuah data.

Membaca data memerlukan beberapa proses perekaman. *Drive* memposisikan bagian pembaca dari *head* di atas track yang sesuai, dan kemudian menunggu sector yang tepat untuk berputar di atasnya. Saat spektrum magnetik tertentu yang mewakili data Anda pada sector dan *track* yang tepat berada tepat di atas *head* pembaca, komponen elektronik *drive* mendeteksi perubahan kecil pada medan magnetik dan mengubahnya menjadi bit. Saat *drive* tersebut selesai mengecek *error* pada bit dan memperbaikinya jika perlu, ia kemudian mengirimkan data tersebut pada sistem operasi. Kinerja *hard disk* berhubungan dengan kecepatannya dalam proses *transfer* data. Berikut ini beberapa parameter yang menentukan kinerja *hard disk*:

1. Untuk *hard disk* dikenal dengan beberapa sistem yang ukuran RPM-nya sebagai berikut:

**Tabel 1 Ukuran RPM**

| | |
|---|---|
| 3600 RPM | (Pre-IDE) |
| 5200 RPM | (IDE) |
| 5400 RPM | (IDE/SCSI) |
| 7200 RPM | (IDE/SCSI) |
| 10000 RPM | (SCSI) |

2. Seek time

   *Seek time* adalah jumlah waktu yang diperlukan oleh lengan penggerak *(actuator arm)* untuk menggerakkan *head* baca/ tulis dari *track* ke *track* lain. Nilai yang diambil adalah nilai rata-ratanya yang dikenal dengan *average seek time*. Penggerakan *head* dapat hanya berupa pergerakan dari satu *track* ke *track* sebelahnya atau mungkin juga digerakan dari *track* terluar menuju ke *track* terdalam. *Seek time* dinyatakan dalam satuan *millisecond* (ms). Nilai *seek time* dari *track* yang bersebelahan sekitar 2 ms, sedangkan *seek* dari ujung ke ujung bisa mencapai 20 ms. *Average seek time* umumnya berkisar antara 8 sampai 14 ms.

3. Head switch time

   Seluruh *head* bergerak secara bersamaan. Namun, hanya ada satu *head* saja yang dapat membaca pada saat yang sama. *Head switch time* dinyatakan dalam satuan ms, mempresentasikan berapa lama rata-rata waktu yang diperlukan untuk mengaktifkan suatu *head* setelah menggunakan *head* yang lain.

4. Cylinder Switch Time

   Mirip dengan *head switch time*, *cylinder switch time* berlaku untuk pergerakan silinder dan *track.*

   a. Rotational Latency

      Setelah *head* digerakkan ke suatu *track* yang diminta, *head* akan menunggu piringan berputar sampai *sector* yang akan dibaca berada tepat di bawah *head*. Waktu tunggu inilah yang dikenal dengan *rotational latency. Hard disk* dengan putaran piring yang semakin cepat akan memperkecil *rotational latency.* Namun, makin cepat piringan berputar maka *hard disk* akan lebih cepat panas.

   b. Data Access Time

      Didefinisikan sebagai waktu yang diperlukan untuk menggerakkan *head* dan menemukan *sector* yang dimaksud. Ini merupakan gabungan *seek time*, *head switch time* dengan *rotational latency.* Data *access time* dinyatakan dalam satuan ms.

   c. Transfer Rate

      Didefinisikan sebagai kecepatan *transfer* data antara *hard disk* dengan CPU. Makin tinggi kecepatan *transfer* maka proses pembacaan atau penulisan akan berlangsung lebih cepat. *Transfer rate* dinyatakan dalam Megabyte per detik (MB/s).

d. Data Throughtput Rate

Parameter ini merupakan kombinasi data *access time* dan *transfer rate*. Parameter ini didefinisikan sebagai banyaknya data yang dapat diakses oleh CPU dalam satuan waktu tertentu.

## II.3 File Sistem

*File system* adalah metode pemberian nama *file* dan cara menempatkannya ke dalam media penyimpan, termasuk penempatan *file* pada struktur direktori. Setiap sistem operasi memiliki metode yang berbeda-beda untuk menempatkan *file* dalam struktur hirarki yang disebut dengan istilah *file system.* Berikut ini adalah beberapa jenis-jenis *file system* yang sudah ada:

1. FAT 16 (File Allocation Table 16)

   Pada awalnya sebelum FAT16, telebih dahulu sistem *file* di MS-DOS FAT12 dibuat, tetapi karena memiliki banyak kekurangan maka digantikan dengan FAT16 yang sudah dikenalkan oleh MS-DOS pada tahun 1981. Awalnya, sistem ini didesain untuk mengatur *file* di *floppy disk* dan sudah mengalami beberapa kali perubahan, sehingga digunakan untuk mengatur *file hard disk*. Keuntungan FAT16 yaitu kompatibel hampir di semua sistem operasi, baik Windows 95/98/ME, OS/2, Linux dan bahkan Unix. Namun kekurangan FAT16 adalah ia mempunyai kapasitas tetap jumlah *cluster* dalam partisi, jadi semakin besar *hard disk*, maka ukuran *cluster* akan semakin besar dan juga tidak mendukung kompresi, enkripsi dan kontrol akses dalam partisi.

2. FAT 32 (File Allocation Table 32)

   FAT32 mulai diaplikasikan pada sistem Windows 95 SP2 dan merupakan pengembangan lebih dari FAT16. FAT32 menawarkan kemampuan menampung jumlah *cluster* yang lebih besar dalam partisi. FAT32 menggunakan *cluster address* 32 bit yang memungkinkan untuk membuat partisi hingga 124 GigaByte. Namun, kekurangan FAT32 yaitu hanya beberapa sistem operasi yang mengenalnya.

3. NTFS (New Technology File System)

   NTFS di kenalkan pertama pada Windows NT dan merupakan *file system* yang berbeda dibandingkan dengan teknologi FAT. NTFS adalah *file system* yang digunakan pada Windows berbasis NT (NT, 2000, XP, 2003, Vista). NTFS menawarkan *security*, kompresi *file*, *cluster* dan bahkan *support* enkripsi data yang jauh lebih baik.

4. EXT 2 (2rd Extended)

   Ext2 pertama kali dirilis pada bulan Januari 1993. *File system* ini ditulis oleh Rémy Card, Theodore T. dan Stephen Tweedie, *file system* ini merupakan penulisan ulang besar-besaran dari *extended file system*. Hingga bulan April 2001, *file system* ini masih menjadi *file system* pertama di Linux. *File system* ini juga diimplementasikan di sistem operasi lain seperti: *NetBSD, FreeBSD, GNU HURD, Windows 95/98/NT, OS/2 dan RISC OS*. Ext2 memiliki banyak kemiripan dengan *file system* asli Unix. Ia memiliki konsep *block*, inode, dan *directory*. Serta memiliki ruang kosong untuk Access Control Lists (ACLs), *fragment*, *undeletion* dan *compression* walaupun fungsi-fungsi tersebut belum diimplementasikan (terdapat melalui *patch* terpisah).

5. EXT 3 (3rd Extended)

   EXT3 adalah *file system* yang digunakan pada sebagian besar sistem operasi Linux. Pada *file system* maka setiap *file* akan memiliki suatu *database* mini, yaitu disebut dengan inode. Dimana di dalamnya berisi berbagai informasi seperti jenis *file*, hak akses, pemilik *file*, grup pemilik *file*, besar *file* dan waktu perubahan.

6. EXT 4 (4rd Extended)

   EXT4 dirilis secara komplit dan stabil berawal dari kernel 2.6.28, jadi apabila masih menggunakan *file system* ext3 dapat mengkonversi ke ext4 dengan beberapa langkah yang tidak terlalu rumit. Keuntungan yang bisa didapat dengan meng-*upgrade file system* ke ext4 dibanding ext3 adalah mempunyai

pengalamatan 48-bit block yang artinya ia akan mempunyai 1EB = 1,048,576 TB ukuran maksimum *file system* dengan 16 TB untuk maksimum *file size*nya, *fast* fsck, *journal checksumming* dan *defragmentation support*.

7. Reiser

   Reiser *file system* memiliki jurnal yang cepat. Ciri-cirinya mirip EXT3 *file system*. Reiser *file system* dibuat berdasarkan *balance tree* yang cepat. *Balance tree* unggul dalam hal kinerja, dengan algoritma yang lebih rumit tentunya. Reiser *file syst*em lebih efisien dalam pemanfaatan ruang *disk*. Jika ditulis *file* 100 bytes, hanya ditempatkan dalam satu blok. *File* sistem lain menempatkannya dalam 100 blok. Reiser *file system* tidak memiliki pengalokasian yang tetap untuk inode. Resier *file system* dapat menghemat *disk* sampai dengan 6 persen.

8. Swap

   Swap merupakan *partition* yang boleh dibuat pada *hard disk* dan digunakan sebagai *virtual memory*. Dengan maksud, swap ini digunakan apabila fisikal memory yang ada pada komputer telah digunakan secara maksimum, maka swap akan digunakan untuk menampung memori tambahan. Swap tidak boleh digunakan untuk data.

## II.4 Open Source

*Open source* adalah sistem pengembangan yang tidak dikoordinasi oleh suatu individu/ lembaga pusat, tetapi oleh para pelaku yang bekerja sama dengan memanfaatkan *source code* yang tersebar dan tersedia bebas (biasanya menggunakan fasilitas komunikasi internet). Pola pengembangan ini mengambil model ala bazaar, sehingga pola *open source* ini memiliki ciri bagi komunitasnya yaitu adanya dorongan yang bersumber dari budaya memberi, yang artinya ketika suatu komunitas menggunakan sebuah program *open source* dan telah menerima

sebuah manfaat kemudian akan termotivasi untuk menimbulkan sebuah pertanyaan apa yang bisa pengguna berikan balik kepada orang banyak.

Pola *Open Source* lahir karena kebebasan berkarya, tanpa intervensi berpikir dan mengungkapkan apa yang diinginkan dengan menggunakan pengetahuan dan produk yang cocok. Kebebasan menjadi pertimbangan utama ketika dilepas ke publik. Komunitas yang lain mendapat kebebasan untuk belajar, mengutak-ngatik, merevisi ulang, membenarkan ataupun bahkan menyalahkan, tetapi kebebasan ini juga datang bersama dengan tanggung jawab, bukan bebas tanpa tanggung jawab. Pada intinya konsep *open source* adalah membuka "*source code*" dari sebuah perangkat lunak. Konsep ini terasa aneh pada awalnya dikarenakan *source code* merupakan kunci dari sebuah perangkat lunak. Dengan diketahui logika yang ada di *source code*, maka orang lain semestinya dapat membuat perangkat lunak yang sama fungsinya.

*Open source* tidak hanya berarti bebasnya akses terhadap *source code*. Syarat-syarat distribusi *open source software* harus memenuhi kriteria-kriteria berikut:

1. Distribusi Ulang Gratis

   Lisensi distribusi tidak melarang pihak manapun untuk menjual atau memberikan *software* sebagai bagian dari distribusi *software* terpadu yang memuat program-program dari beberapa sumber yang berbeda. Lisensi seharusnya tidak mensyaratkan royalti atau biaya lain untuk hal tersebut.

2. Kode Sumber (source code)

   Program harus menyertakan kode sumber, dan harus mengizinkan distribusi kode sumber sebagaimana distribusi bentuk terkompilasinya. Jika sebuah produk tidak didistribusikan dengan kode sumbernya, harus ada sarana yang terpublikasi baik untuk mendapatkan kode sumber dengan mudah. Kode sumber harus dalam bentuk yang memudahkan *programmer* untuk memodifikasi program tersebut. Bentuk intermediet, seperti *output preprosesor* atau *translator* tidak diperbolehkan.

3. Kerja Turunan

   Lisensi harus mengizinkan modifikasi dan penerusan hasil kerja oleh orang lain, serta harus mengizinkannya untuk didistribusikan di bawah lisensi yang sama dengan *software* aslinya.

4. Integritas Penulis Kode Sumber

   Lisensi dapat melarang kode sumber untuk didistribusikan ulang dalam bentuk termodifikasi hanya jika lisensi mengizinkan distribusi *file-file* tambahan beserta kode sumber untuk tujuan memodifikasi program pada masa pembangunan. Lisensi harus secara eksplisit mengizinkan distribusi *software* yang dibangun dari modifikasi kode sumber. Lisensi mungkin mensyaratkan hasil kerja turunan untuk menggunakan nama atau versi yang berbeda dari *software* aslinya.

5. Tidak Ada Diskriminasi terhadap Pribadi atau Golongan

   Lisensi tidak boleh mendiskriminasi pribadi atau golongan manapun.

6. Tak Ada Diskriminasi terhadap Bidang atau Usaha Tertentu

   Lisensi tidak boleh melarang siapapun untuk memanfaatkan program dalam bidang atau usaha tertentu. Misalnya, tidak boleh melarang program untuk digunakan di bidang bisnis atau digunakan dalam riset genetika.

7. Distribusi Lisensi

   Hak-hak yang dimiliki oleh program harus dapat diaplikasikan oleh semua orang yang menerima distribusi program tersebut, tanpa perlu penambahan lisensi oleh pihak-pihak yang bersangkutan.

8. Lisensi Tidak Spesifik untuk Satu Produk

   Hak-hak yang dimiliki program bukan karena program tersebut menjadi bagian distribusi *software* tertentu. Jika program tersebut dipisahkan dari distribusi tersebut dan digunakan atau didistribusikan di bawah lisensi program, semua pihak yang menerima distribusi tersebut mempunyai hak yang sama sebagaimana hak yang dipunyai oleh distribusi *software* asal.

9. Lisensi Tidak Membatasi Software Lain

   Lisensi tidak boleh melakukan pembatasan terhadap *software* lain yang didistribusikan bersama dengan *software* yang diberi lisensi. Misanya, lisensi tidak boleh memaksa agar semua program lain yang didistribusikan melalui medium yang sama harus merupakan *open source software*.

10. Lisensi Harus Netral terhadap Teknologi

    Tidak ada syarat lisensi yang merupakan predikat dari suatu teknologi atau gaya antarmuka tertentu.

## II.5 Perbandingan antar Tugas Akhir

Berikut adalah perbandingan Tugas Akhir ini dengan Laporan Tugas Akhir "Perbandingan Aplikasi *Recovery Hard Disk* untuk Kepentingan Forensik" sebelumnya (Tabel 2).

**Tabel 2 Perbandingan TA**

| Sekarang | Sebelumnya |
|---|---|
| Menggunakan Sistem Operasi Linux (Ubuntu 10.04) | Menggunakan Sistem Operasi Windows (XP/Vista/7) |
| Menggunakan aplikasi *recovery hard disk open source* | Menggunakan aplikasi *recovery hard disk freeware* dan berbayar |

# Bab III Survei Aplikasi

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

## III.1 Hasil Survei Aplikasi Recovery Terkait

Berdasarkan hasil pencarian di internet dari 60 *website*, 44 di antaranya membahas tentang aplikasi testdisk, photorec, foremost dan scalpel dalam hal pengembalian data. Kemudian dari hasil pencarian diatas dapat ditentukan aplikasi mana yang akan dijadikan sebagai aplikasi perbandingan dalam me*recovery* data di dalam *hard disk*. Berikut hasil pencarian yang telah dilakukan:

1. Testdisk : 16 *website*
2. Photorec : 13 *website*
3. Foremost : 12 *website*
4. Scalpel : 11 *website*
5. Lainnya : 16 *website*

## 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. 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 ini memiliki banyak kegunaan, mulai dari memperbaiki tabel partisi dan juga

mengembalikan data partisi yang terhapus. Segala fungsinya berlaku pada format sistem *file*s 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 penggunanya bisa mengembangkannya.

2. 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*).

3. Foremost

   Foremost adalah *tools* untuk *recovery file* berdasarkan *header*, *footer* dan struktur data internal. Oleh karena itu foremost bisa digunakan untuk mencari *file-file* yang sudah terhapus (disengaja atau tidak), bahkan untuk data yang sudah di format sekalipun. Ketika *file* dihapus atau bahkan dibersihkan dari *recycle bin* sekalipun, biasanya data tersebut tetap ada karena yang dihapus hanyalah catatan dimana *file* tersebut berada (*file allocation unit*). Begitu juga ketika *hardisk* diformat sekalipun tetap sama saja, karena yang bisa menghilangkan *file* dengan bersih hanya dengan teknik sanitasi. Keunggulan foremost yaitu bisa melakukan *file recovery*

langsung dari media disk atau *image* tanpa harus di *mount* terlebih dahulu. Foremost merupakan aplikasi berbasis terminal yang mendukung *filesystem* FAT, NTFS, EXT3 dan EXT4. Sebab itu, aplikasi ini tidak membutuhkan banyak memori untuk dapat bekerja.

4. Scalpel

   Scalpel merupakan salah satu aplikasi *recovery* yang membaca data berdasarkan *header*, footer dan kemudian mengekstrak *file* yang serupa atau fragmen data dari sekumpulan *file* gambar atau *file* mentah sebuah perangkat. Scalpel juga mendukung *filesystem* FAT, NTFS, ext2/3, HFS+ dan yang lain sebagainya yang berguna untuk investigasi forensik data digital dan *file recovery.* Selain itu scalpel juga bisa digunakan pada sistem operasi Windows (32 atau 64-bit) dengan menggunakan mingw.

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 3 Spesifikasi File**

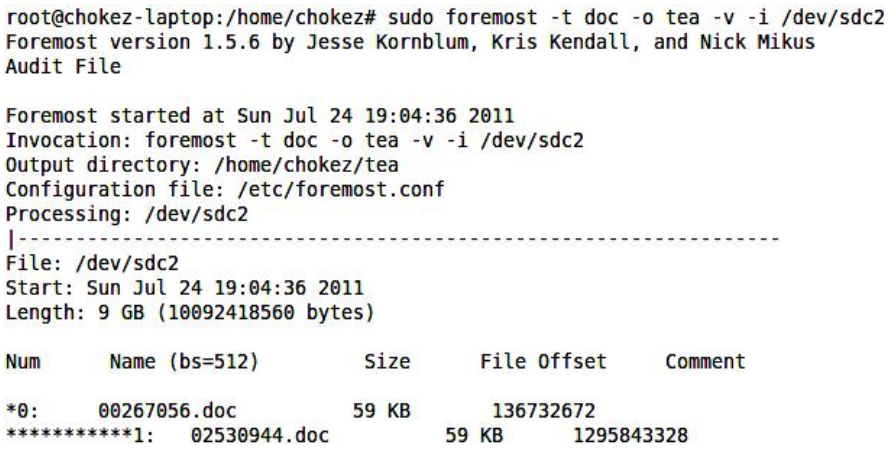
| Nama File | Jenis File |
|---|---|
| LK_juli2011 | Doc |
| 18032011 | Jpg |
| Sound clip 95 | Wav |
| 20110606_ch05 | Mov |

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 Foremost

a. Delete

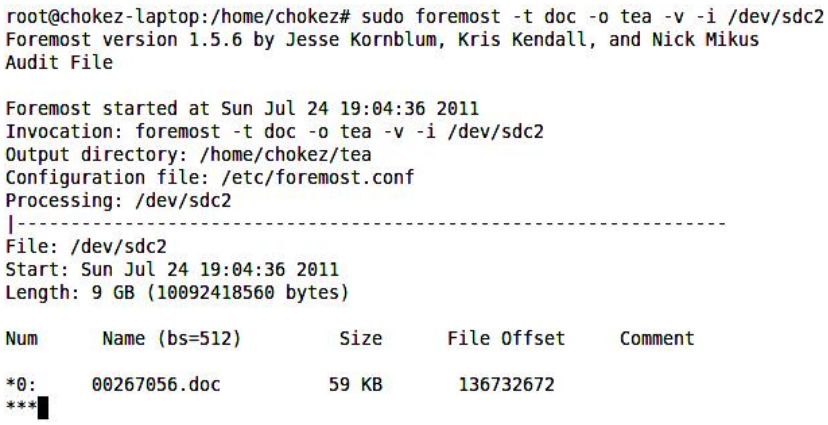
Foremost mampu mengembalikan data dihapus secara utuh, seperti pada gambar 3.




**Gambar 3 Proses Scanning Data yang dihapus**

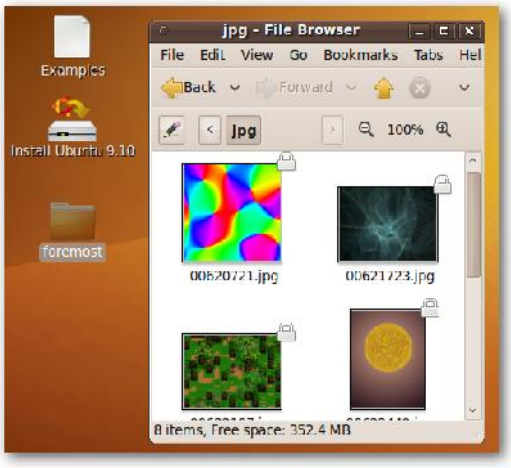
b. Format

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




**Gambar 4 Proses Scanning Data yang diformat**

Setelah melakukan proses *scanning*, maka hasil pengembalian data yang terformat dapat dikembalikan, meskipun tidak semua *file* dapat dikembalikan dengan utuh.




**Gambar 5 Hasil dari Scanning Foremost**

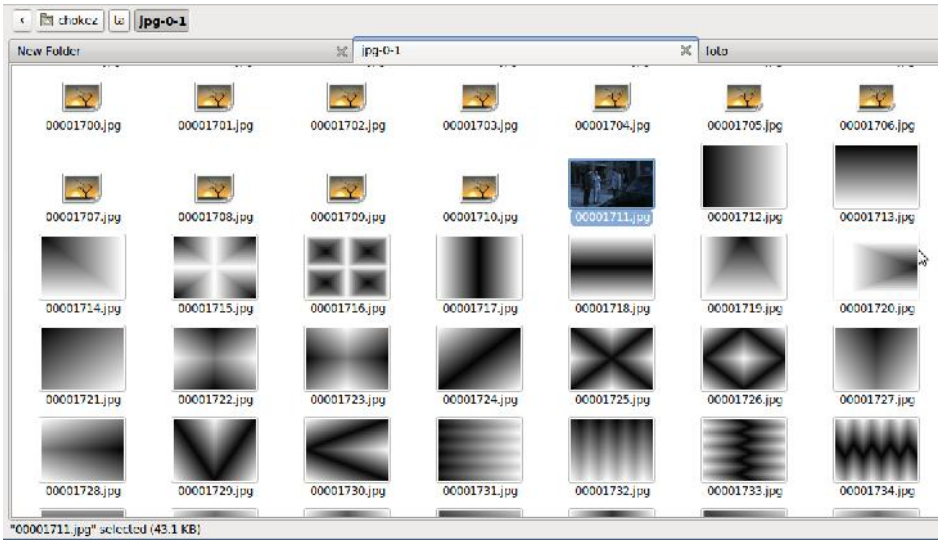
c. Partisi

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

### IV.1.2 Scalpel

a. Delete

Scalpel mampu mengembalikan data yang dihapus secara utuh tanpa ada kecacatan. Keterangan hasil pengembalian Data Scalpel dapat dilihat pada gambar dibawah ini.




**Gambar 6 Hasil Pengembalian Data yang dihapus**

b. Format

Scalpel juga mampu mengembalikan data saat partisi diformat. Keterangan proses *scanning* Scalpel dan hasil pengembalian data seperti pada gambar 7.

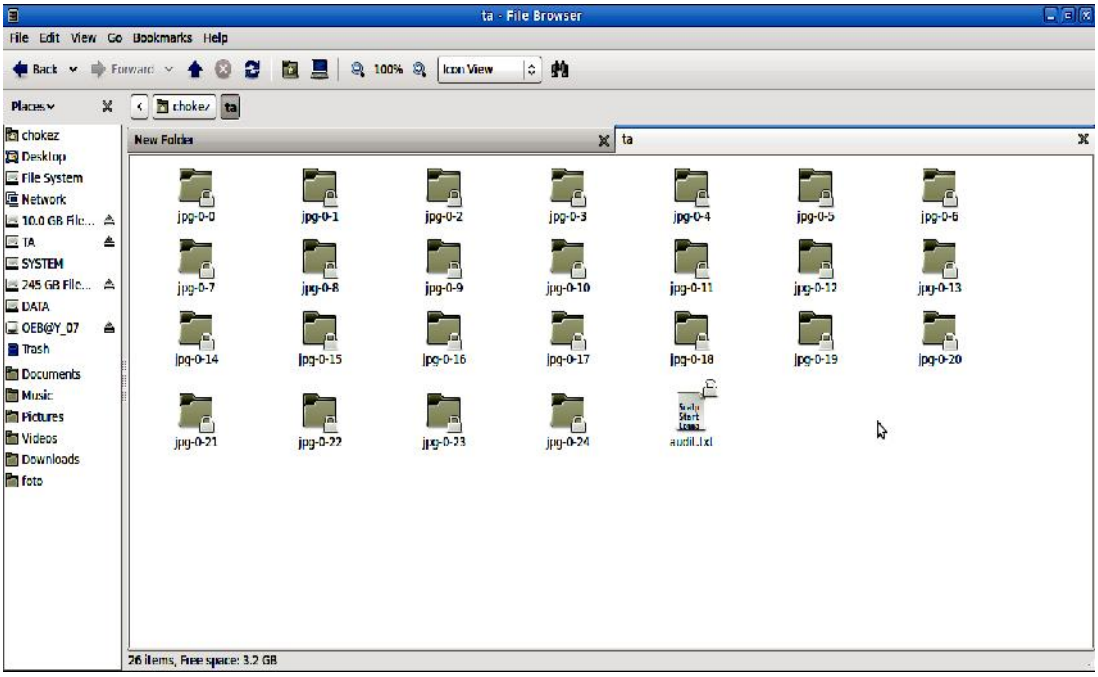
```
root@chokez-laptop:/home/chokez# scalpel /dev/sdc2 -o tea
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/dev/sdc2"

Image file pass 1/2.
/dev/sdc2: 100.0% |*****************************************************************************************************************************| 9.4 GB  00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
doc with header "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" and footer "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" --> 120 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1" and footer "" --> 124 files
Carving files from image.
Image file pass 2/2.
/dev/sdc2: 100.0% |*****************************************************************************************************************************| 9.4 GB  00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 244, elapsed = 544 seconds.
```

**Gambar 7 Proses Scanning Scalpel**

Namun, hasil pengembalian data yang disebabkan partisi diformat kurang sempurna, karena tidak semua *file* bisa dikembalikan secara utuh.




**Gambar 8 Hasil Pengembalian Data yang diformat**

c. Partisi

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

### IV.1.3 TestDisk

a. Delete

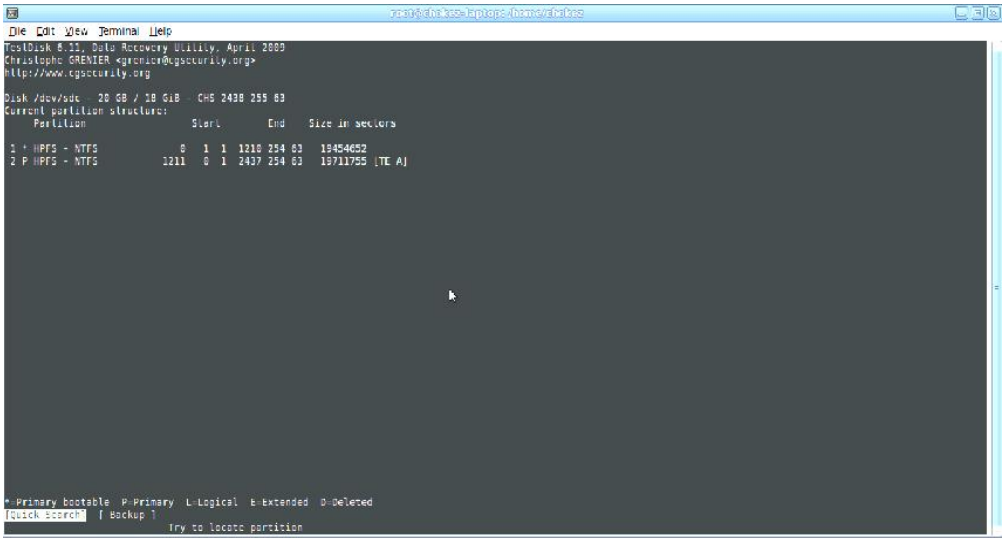
Pada aplikasi TestDisk tidak ada *tools* yang mendukung proses pengembalian data yang dihapus.

b. Format

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

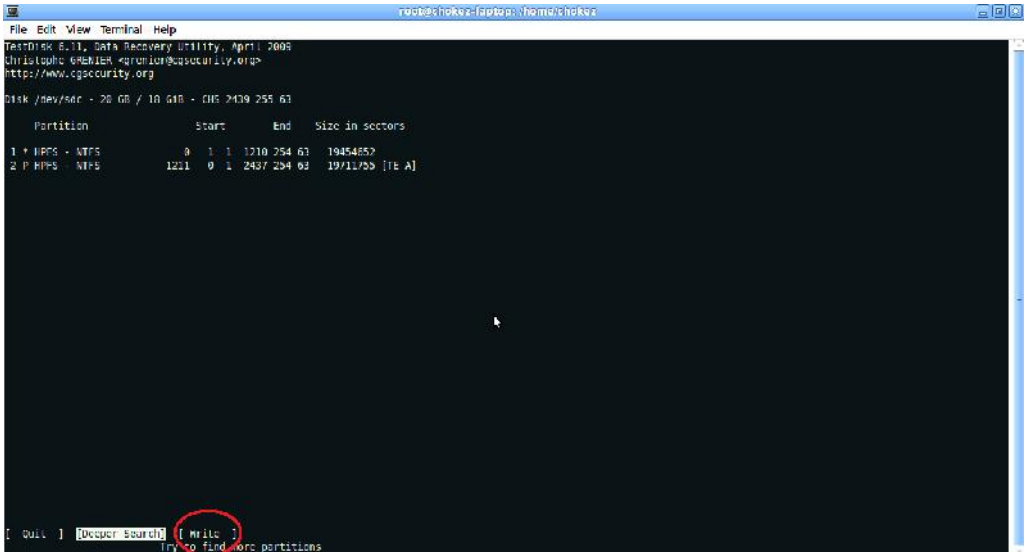
c. Partisi

Pada tampilan struktur *file* sistem NTFS tekan tombol ENTER pada *Quick Search*. Keterangan gambar sebagai berikut:



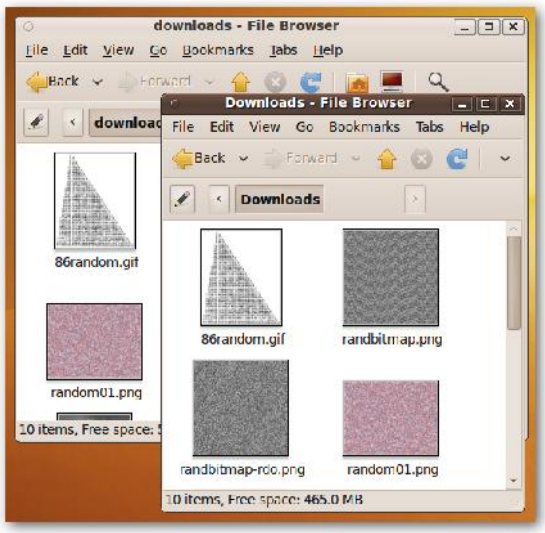

**Gambar 9 Menganalisa Partisi**

Setelah menganalisis partisi dari gambar di atas dengan memilih *Write*, maka TestDisk akan meminta *reboot*. Keterangan gambar sebagai berikut:




**Gambar 10 Proses Scanning Partisi**

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

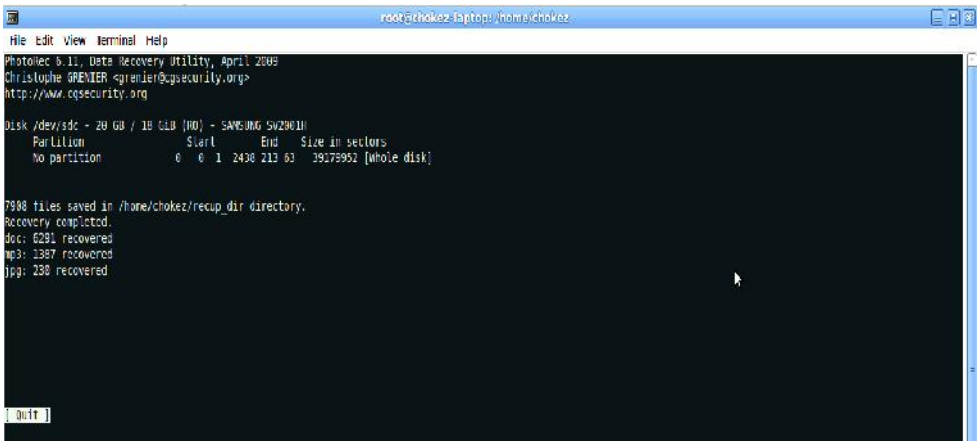



**Gambar 11 Hasil Scanning TestDisk**

### IV.1.4 Photorec

a. Delete

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




**Gambar 12 Proses Scanning Photorec**

b. Format

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


**Gambar 13 Proses Scanning Photorec Data diformat**

c. Partisi

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

## IV.2 Skenario Pengujian

Dalam 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

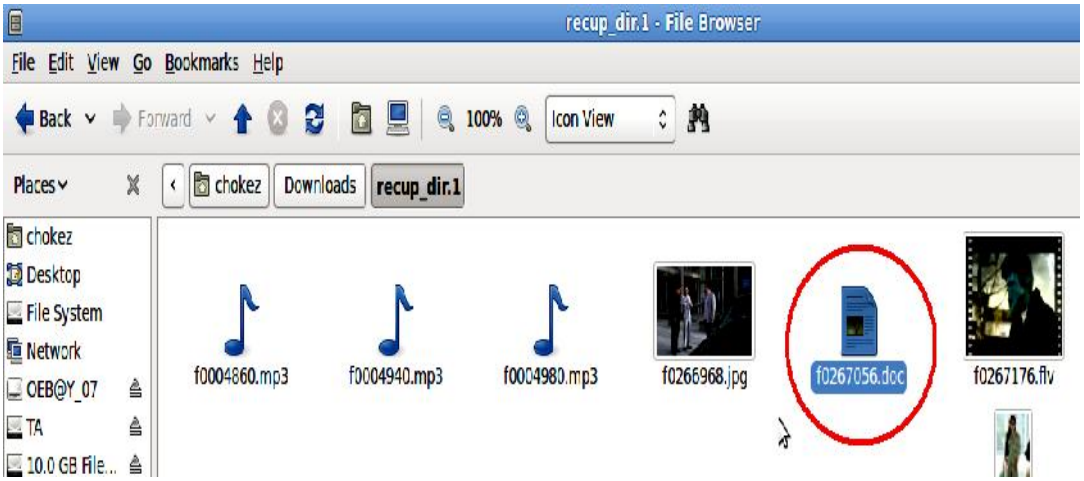
Sekelompok mahasiswa mendapatkan tugas untuk menjual berbagai macam aksesoris pada mata kuliah kewirausahaan. Mereka diberi waktu selama 3 bulan untuk menjual semua barang tersebut dan membuat laporan keuangan dari hasil penjualan. Setelah berhasil menjual semua barang, salah seorang mahasiswa yang merupakan anggota dari kelompok tersebut membuat laporan keuangan sederhana yang kemudian akan diserahkan kepada dosen untuk nilai tugas mata kuliah kewirausahaan.

Mahasiswa tersebut kemudian membuat laporan itu dan setelah selesai ia meminjamkan laptopnya kepada kakaknya yang juga ingin membuat tugas. Keesokan harinya ketika mau mencetak laporan tersebut data yang dicari ternyata hilang. Setelah ditanya kepada kakaknya, kakaknyapun mengaku telah menghapus data tersebut karena menganggap data tersebut tidak penting. Kemudian mahasiswa itu memberitahu kepada temannya bahwa laporan yang dibuat olehnya telah hilang. Salah seorang anggota kelompoknya ada yang menyarankan untuk mencoba mengembalikan data yang hilang dengan menggunakan aplikasi *recovery hard disk*.

Dalam proses pengembalikan data, mereka melakukan pengujian terhadap 4 (empat) aplikasi *recovery* yang telah tersedia. Dari pengujian ini guna mengetahui pengembalian data digital yang terlihat dari keakuratan datanya.

1. Photorec

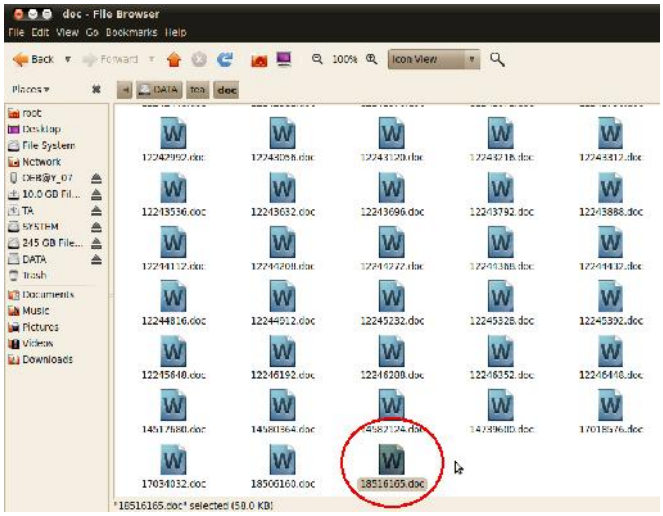
   Aplikasi ini dapat mengembalikan dokumen hilang secara utuh, meskipun membutuhkan proses *scanning* yang cukup lama.




**Gambar 14 LK_juli2011yang dikembalikan Menggunakan Photorec**

2. Foremost

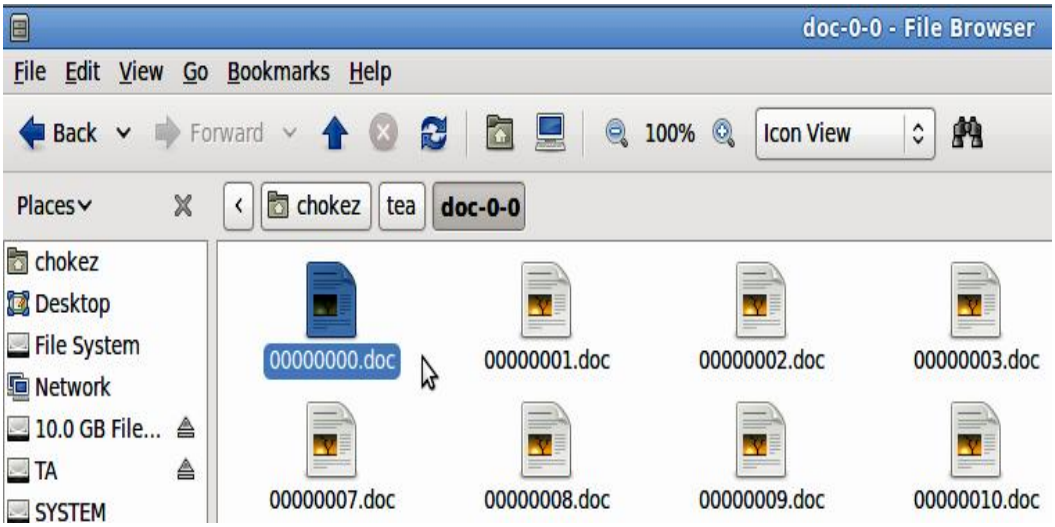
   Foremost juga dapat mengembalikan dokumen hilang yang dihapus secara utuh.




**Gambar 15 LK_juli2011yang dikembalikan Menggunakan Foremost**

3. Scalpel

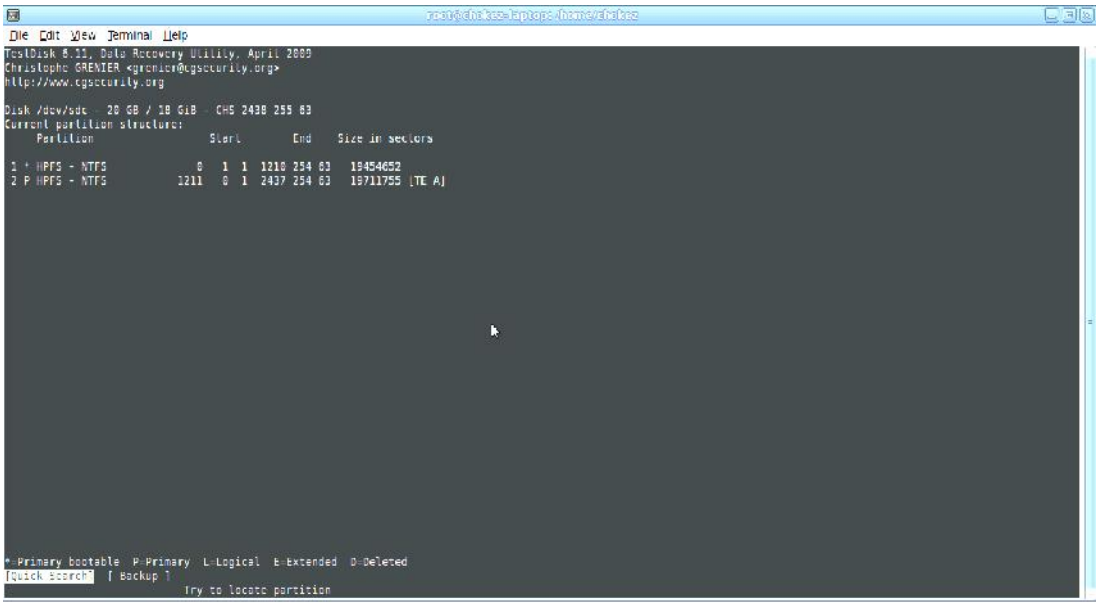
   Aplikasi ini mampu mengembalikan dokumen hilang yang dihapus secara utuh.




**Gambar 16 LK_juli2011yang dikembalikan Menggunakan Scalpel**

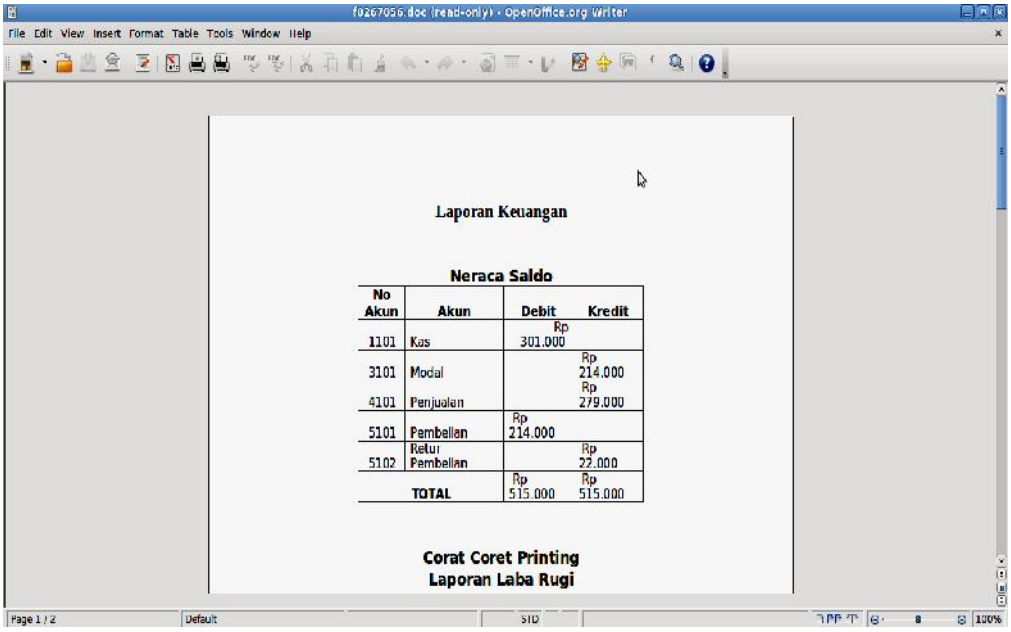
4. TestDisk

   Aplikasi ini tidak mendukung pengembalian data hilang yang diakibatkan dihapus.




**Gambar 17 TestDisk**

Setelah diperiksa ternyata data yang berhasil dikembalikan sama persis seperti laporan yang telah dibuat sebelumnya. Hasil pengembalian data seperti gambar di bawah ini.




**Gambar 18 LK_juli2011**

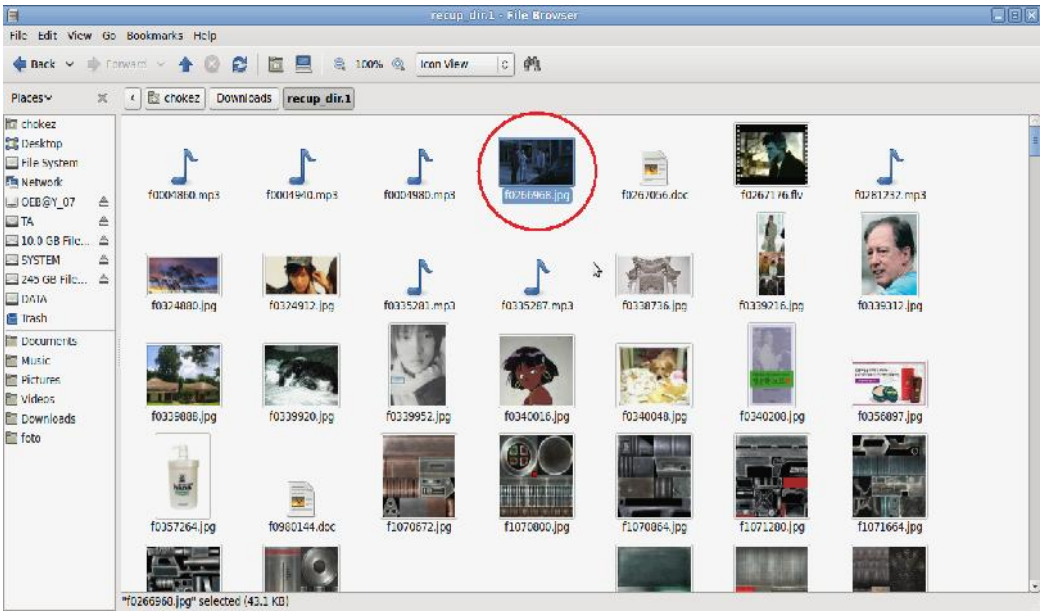
### IV.2.2 Kehilangan Gambar

Seorang pejabat negara dicurigai telah menerima suap dalam proyek pembangunan daerah. Kemudian seorang fotografer secara tidak sengaja berhasil memotret peristiwa dimana pejabat tersebut menerima uang dari seorang pengusaha. Setelah foto tersebut ia simpan di laptopnya, pada keesokan harinya ia mendapati ruang kerjanya berantakan dan seseorang telah mengakses komputernya dan foto yang kemarin didapatnya juga telah hilang. Fotografer tersebut kemudian memutuskan untuk mengundang pihak forensik untuk melacak apakah benar semua foto di dalam komputernya hilang.

Dalam proses pengembalian data digital, penyidik melakukan pengujian terhadap 4 (empat) aplikasi *recovery* yang telah tersedia. Pengujian ini dilakukan guna membuktikan kebenaran yang terlihat dari keakuratan data dalam pengembalian data tersebut.

1. Photorec

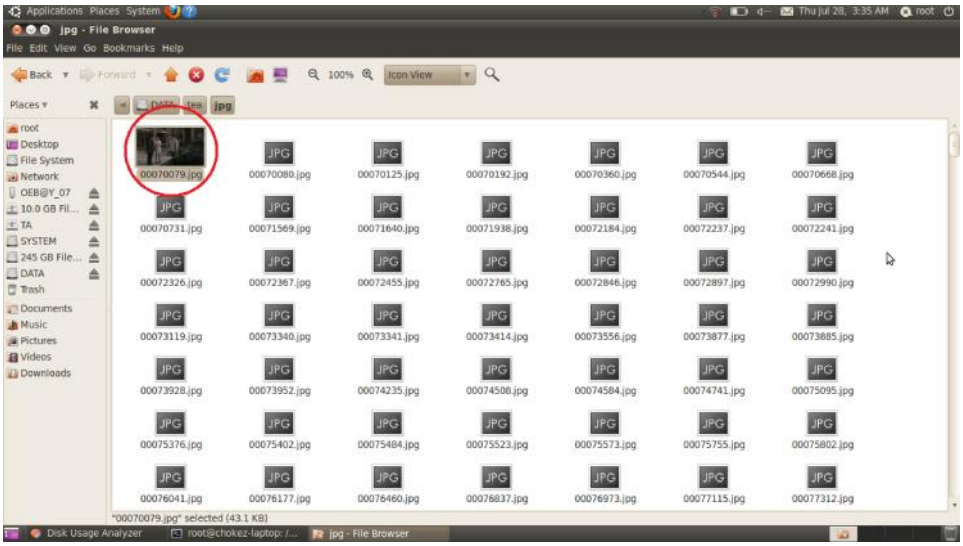
Untuk meyakinkan kebenaran data tersebut, penyidik melakukan pengembalian data menggunakan aplikasi Photorec. Aplikasi ini dapat mengembalikan data tersebut.




**Gambar 19 Foto yang dikembalikan Menggunakan Photorec**

2. Foremost

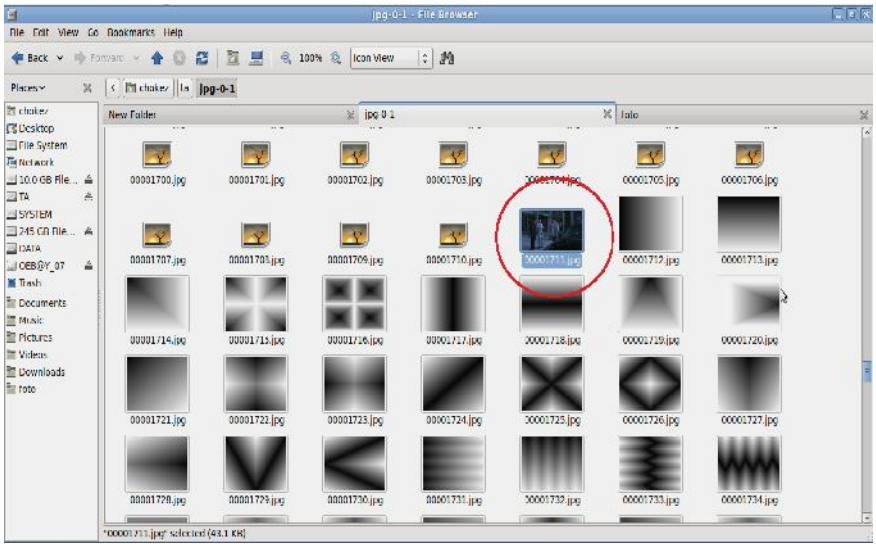
Aplikasi berikutnya yakni Foremost, aplikasi ini juga mengembalikan gambar tersebut.




**Gambar 20 Foto yang dikembalikan Menggunakan Foremost**

3. Scalpel

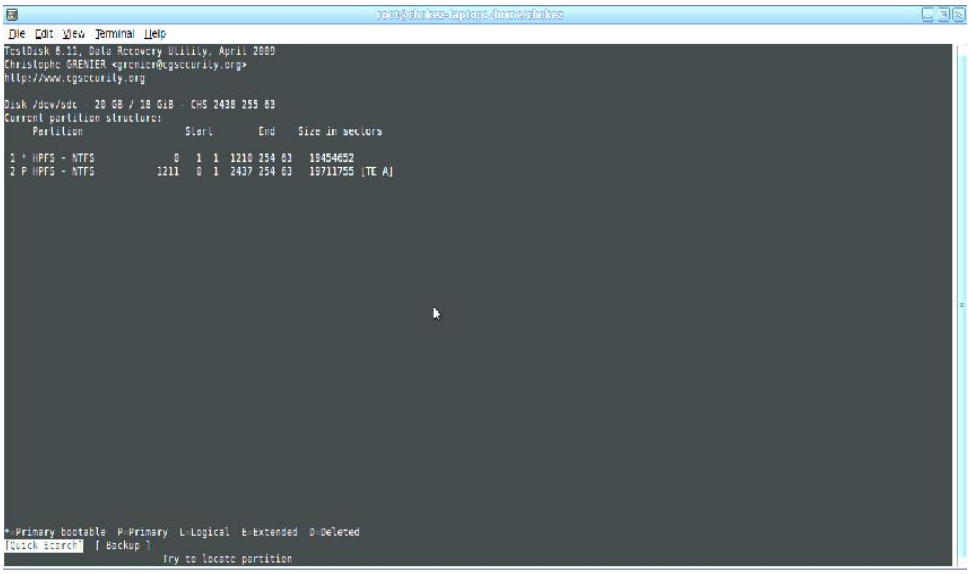
Kemudian menggunakan aplikasi Scalpel, aplikasi ini mampu mengembalikan gambar tersebut.



**Gambar 21 Foto yang dikembalikan Menggunakan Scalpel**

4. TestDisk

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




**Gambar 22 TestDisk**

Setelah proses *recovery* dilakukan, maka foto-foto yang sudah dihapus oleh seseorang yang masuk ke ruang kerjanya berhasil ia dapatkan kembali. Berikut ini merupakan gambar foto yang berhasil dikembalikan.


**Gambar 23 Foto suap pejabat dengan pengusaha**

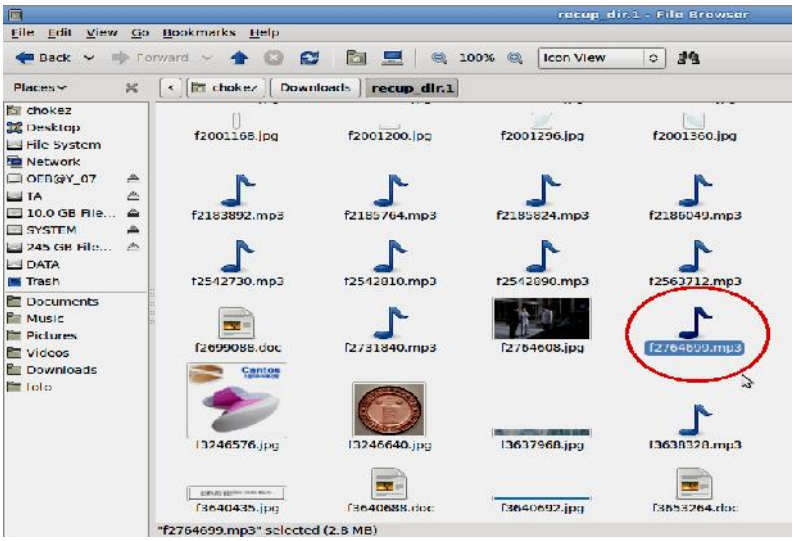
### IV.2.3 Kehilangan Rekaman

Seorang wartawan sebuah surat kabar mendapat tugas untuk mewawancarai kepala dinas kota setempat. Setelah menyelesaikan tugasnya ia pun segera menyimpan *file* rekaman tersebut di dalam komputernya. Keesokan harinya ketika ia akan menulis laporan dari hasil wawancaranya dengan menggunakan hasil rekaman yang berada di komputernya, tiba-tiba komputernya tidak bisa menyala dan data yang berada di dalamnya hilang. Disebabkan ia sangat membutuhkan *file* tersebut kemudian dia memanggil ahli digital forensik melakukan *recovery hard disk* pada komputernya untuk menganalisa rekaman tersebut.

Dari kasus kehilangan ini, penyidik melakukan pengujian terhadap 4 (empat) aplikasi *recovery* yang telah tersedia. Pengujian dilakukan guna membuktikan kebenaran data digital yang dilihat dari keakuratan data dalam proses pengembalian data.

1. Photorec

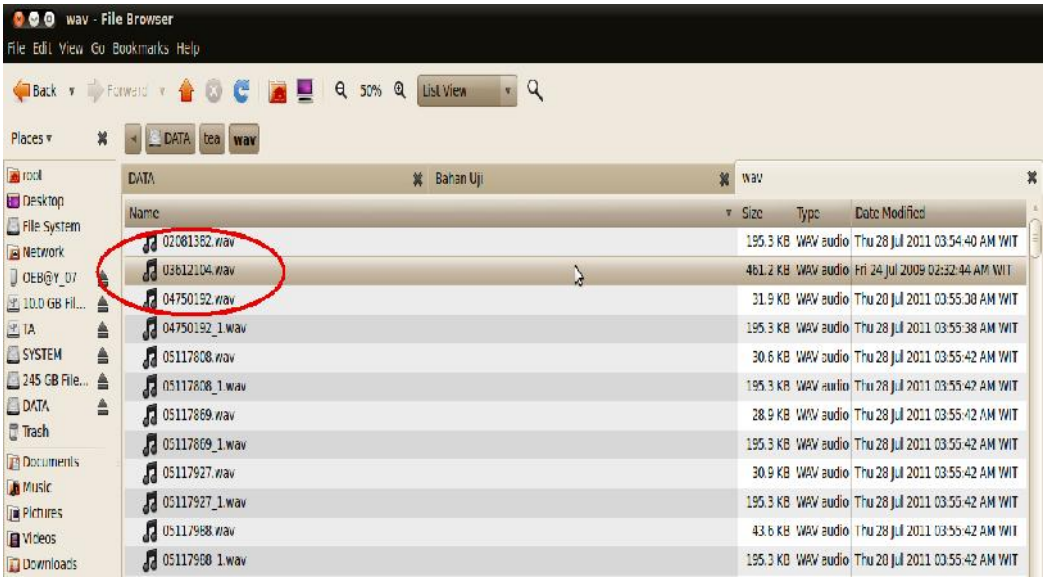
   Pengujian aplikasi Photorec, aplikasi ini ridak bisa memulihkan *file* dengan ekstensi wav, namun bisa mengembalikan tipe *file* mp3. Contoh gambar terlihat di bawah ini:




**Gambar 24 Rekaman yang dikembalikan Menggunakan Photorec**

2. Foremost

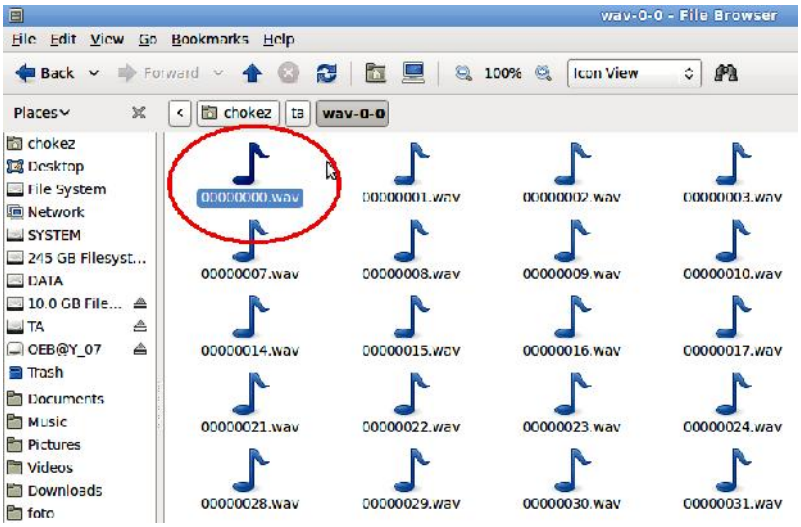
   Pengujian kedua dilakukan pada aplikasi Foremost, aplikasi ini juga dapat mengembalikan rekaman tersebut. Keterangan gambar terlihat di bawah ini:




**Gambar 25 Rekaman yang dikembalikan Menggunakan Foremost**

3. Scalpel

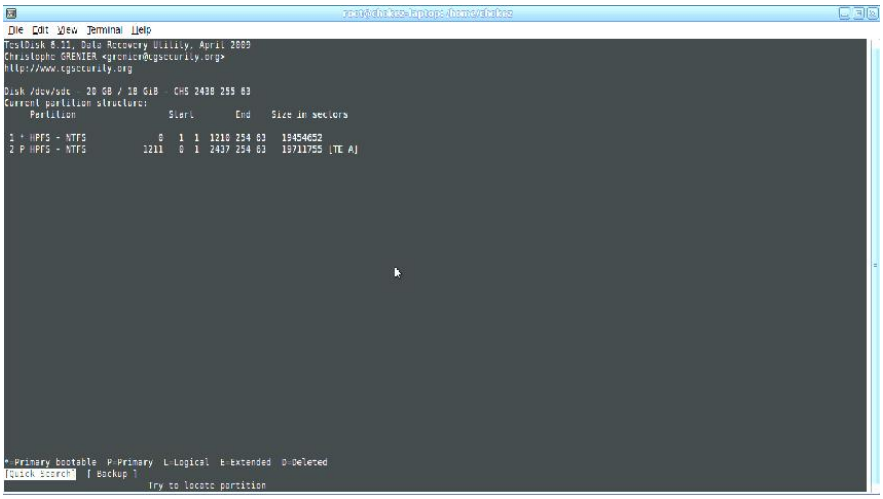
   Kemudian aplikasi berikutnya yaitu Scalpel, aplikasi ini mampu mengembalikan rekaman tersebut. Keterangan gambar terlihat di bawah ini:




**Gambar 26 Rekaman yang dikembalikan Menggunakan Scalpel**

4. TestDisk

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




**Gambar 27 TestDisk**

Setelah melakukan proses *recovery*, akhirnya rekaman tersebut bisa dikembalikan.

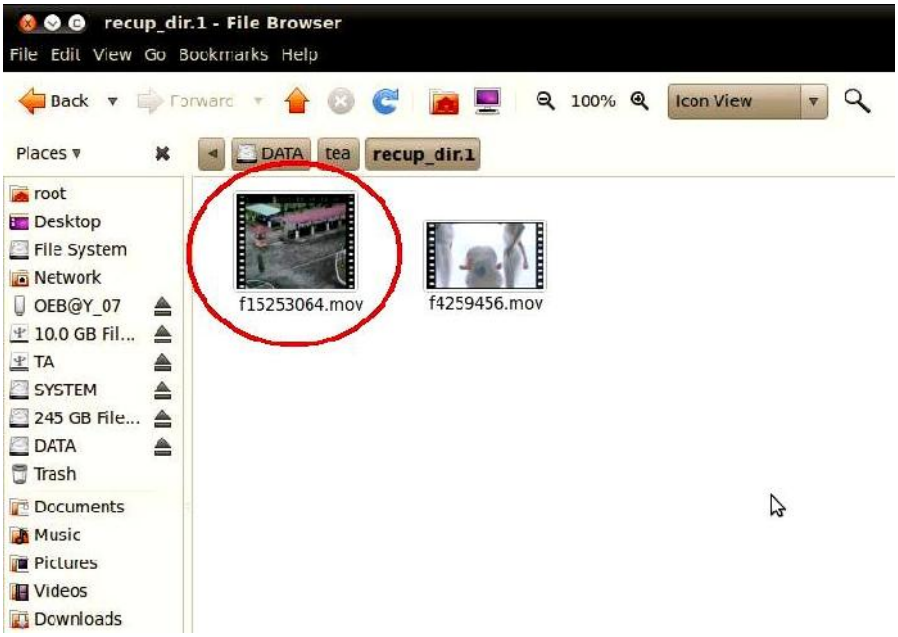
### IV.2.4 Kehilangan Video

Pada saat jam pulang kerja Doni dikejutkan dengan helm motornya yang hilang, padahal ia sudah menggantungnya di jok motor miliknya. Karena mengira sulit untuk mengetahui pelakunya maka ia melanjutkan untuk pulang ke rumah. Keesokan harinya karyawan lain melihat rekaman CCTV dan di dalam video, terlihat jelas seorang karyawan lain telah membuka paksa helm tersebut dari jok motornya. Karena pada hari itu Doni tidak bekerja, maka karyawan tersebut tidak bisa memberitahukan hal itu kepadanya. Oleh karena itu, video tersebut disimpan di dalam komputer karyawan itu. Mengetahui video itu tersimpan, tersangka itupun menghapus video tersebut. Pada keesokan harinya, ketika karyawan itu ingin menunjukkan video tersebut kepada Doni, tiba-tiba video tersebut sudah tidak ada. Kerena penasaran dengan isi video tersebut, akhirnya Doni itu meminta bantuan seorang temannya untuk melacak, menganalisa atau mengembalikan video tersebut dari komputer karyawan itu.

Dari kasus kehilangan video, penyidik melakukan pengujian terhadap 4 (empat) aplikasi *recovery*. Pengujian dilakukan guna membuktikan kebenaran data digital yang dilihat dari keakuratan dalam proses pengembalian data.

1. Photorec

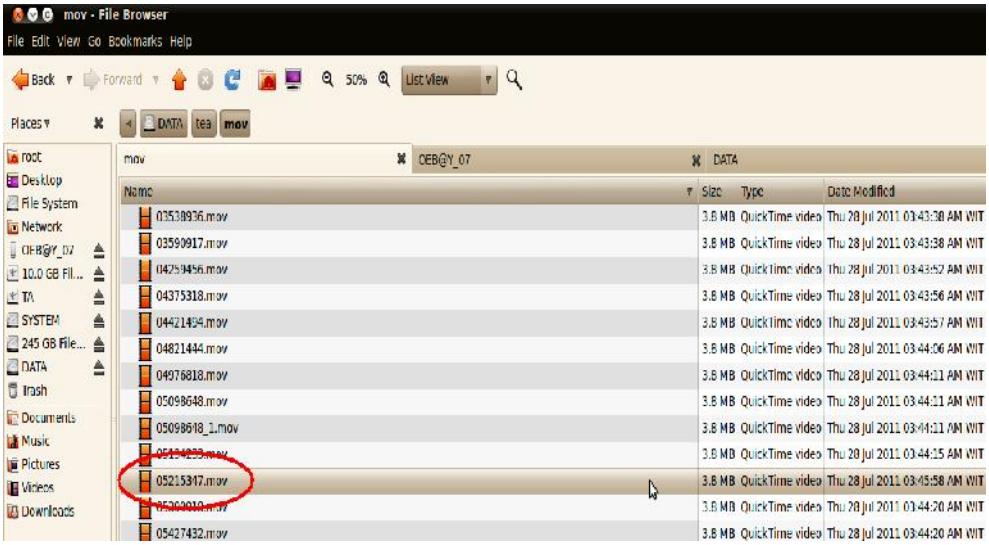
   Pengujian dilakukan pada aplikasi Photorec. Aplikasi ini dapat mengembalikan video tersebut. Keterangan dapat dilihat pada gambar 28.




**Gambar 28 Video yang dikembalikan Menggunakan Photorec**

2. Foremost

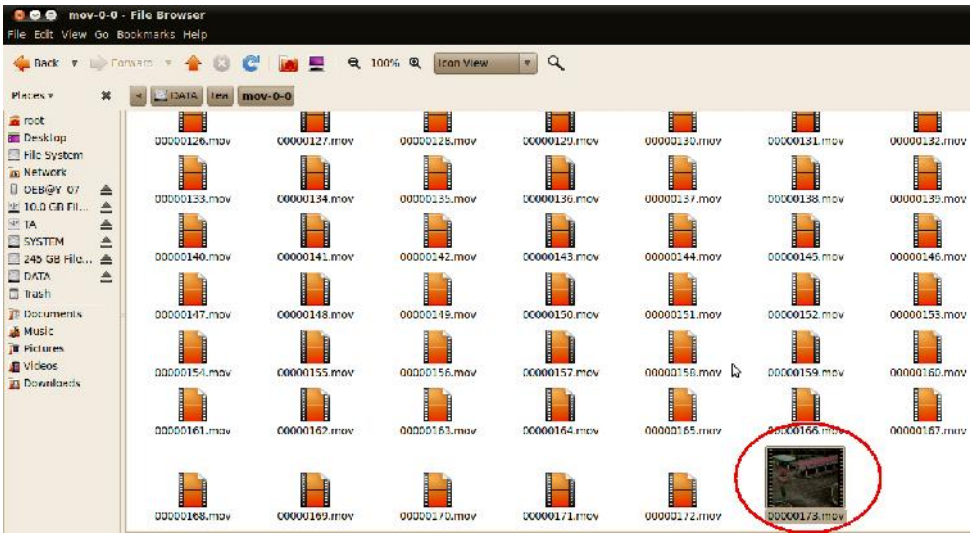
Setelah melakukan pengujian pada aplikasi Photorec, maka penyidik melakukan lagi pengujian pada aplikasi Foremost. Aplikasi ini juga dapat mengembalikan video tersebut walaupun tidak sempurna. Keterangan gambar terlihat di bawah ini:




**Gambar 29 Video yang dikembalikan Menggunakan Foremost**

3. Scalpel

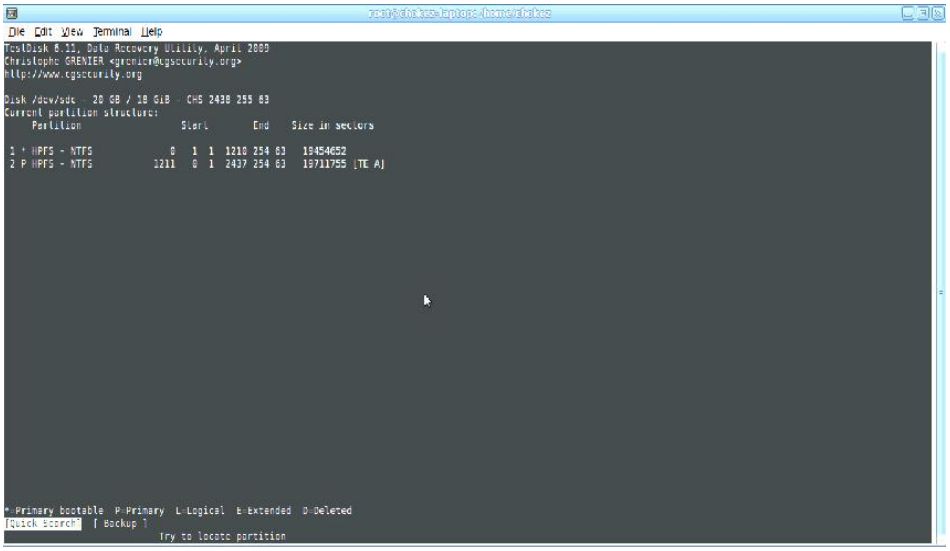
Tahap pengujian selanjutnya yakni menggunakan aplikasi Scalpel. Aplikasi ini dapat juga mengembalikan video tersebut. Keterangan gambar terlihat di bawah ini:




**Gambar 30 Video yang dikembalikan Menggunakan Scalpel**

4. TestDisk

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




**Gambar 31 Testdisk**

Setelah dikembalikan, akhirnya video itu membuktikan bahwa karyawan yang mengambil helm Doni adalah Rio yang merupakan rekan kerjanya. Berikut ini merupakan gambar  yang di *print screen* dari video tersebut.


**Gambar 32 Tersangka di atas motornya**


**Gambar 33 Tersangka mengambil helm**


**Gambar 34 Tersangka meninggalkan area parkir**

## IV.3 Identifikasi User Linux

Sebuah perusahaan memiliki *server* linux yang memantau semua kegiatan dan arus data di perusahaan tersebut. Pada suatu hari data-data yang terdapat di dalam *server* ditemukan tidak beraturan seperti ada yang sengaja mengacaknya. Kemudian *administrator* mencoba menelusuri siapa yang terakhir kali mengakses *server* karena sebelumnya data yang ada baik-baik saja. *Administrator* dengan menggunakan terminal linux mencari *user* yang login ke komputer *server*.

```
root@chokez-laptop:/home/chokez# finger
Login     Name       Tty      Idle  Login Time   Office     Office Phone
bayu                 pts/1          Jul 28 18:05 (localhost)
chokez    Chokez    *tty1        9  Jul 28 17:56
chokez    Chokez     pts/0         Jul 28 18:04 (:0.0)
```

**Gambar 35 Pencarian dengan Finger**

```
root@chokez-laptop:/home/chokez# who
chokez   tty1         2011-07-28 17:56
chokez   pts/0        2011-07-28 18:04 (:0.0)
bayu     pts/1        2011-07-28 18:05 (localhost)
```

**Gambar 36 Pencarian dengan perintah Who**

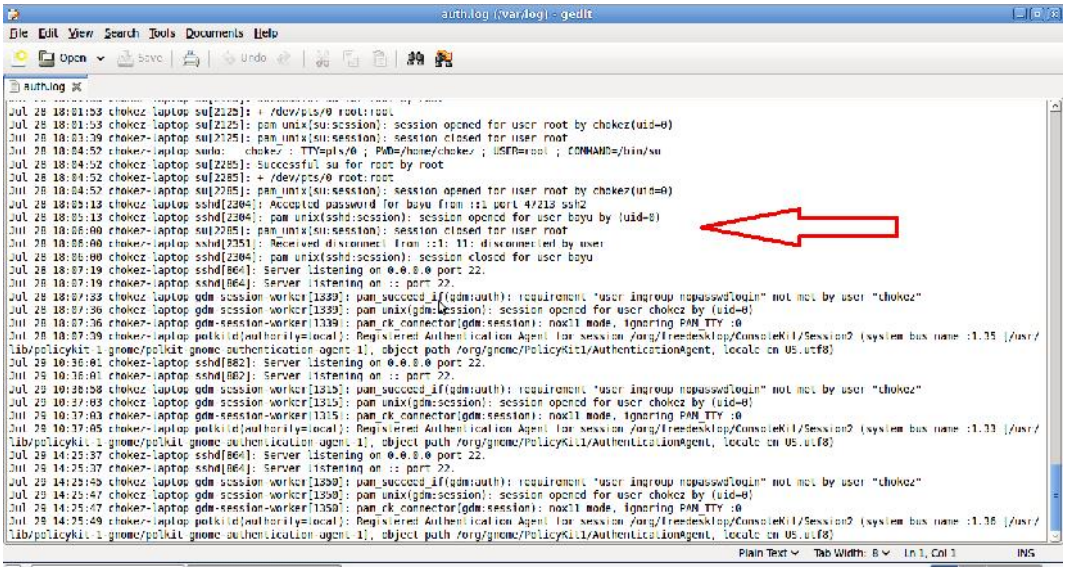
Hasil pencarian menunjukkan tidak hanya *user* yang tampil namun beserta dengan tanggal dan jam aksesnya. Linux memiliki mekanisme untuk mencatat kejadian-kejadian penting yang dicatat ke *file-file* log tertentu. Pada kebanyakan distribusi Linux, biasanya *file* log disimpan di dalam direktori /var/log atau /var/adm. Fasilitas pencatatan tidak menulis kejadian pada sebuah *file*, tapi ke beberapa *file* sesuai dengan kategorinya. Sebagai contoh pada distribusi RedHat atau Mandrake terdapat *file-file* di bawah ini:

1. /var/log/cron, mencatat semua kegiatan *cron* (utilitas untuk menjalankan program secara periodik).
2. /var/log/httpd/*, mencatat akses ke web *server*.
3. /var/log/maillog, mencatat segala hal yang berhubungan dengan *email*.
4. /var/log/messages, mencatat segala hal yang tidak termasuk pada *file* log lainnya.
5. /var/log/news/*, mencatat segala hal yang berhubungan dengan *news server*.
6. /var/log/samba/*, mencatat hal-hal yang berhubungan dengan *file server* samba.
7. /var/log/secure, mencatat hal-hal yang berhubungan dengan keamanan *system*.
8. /var/log/spooler, mencatat hal-hal yang berhubungan dengan pencetakan.
9. /var/log/xferlog, mencatat *transfer file* melalui FTP.

*File-file* yang penulis sebutkan di atas adalah *file* teks biasa, dan dapat dilihat dengan menggunakan utilitas teks biasa, misalnya gunakan perintah tail -f /var/log/messages untuk melihat perkembangan pada sistem.


**Gambar 37 Folder /var/log/**

Informasi mengenai kegiatan *user* yang mengakses *server* bisa dilihat di *file* auth.log di folder /var/log.




**Gambar 38 *File* auth.log**

# 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 4 Hasil Pengujian Aplikasi**

| Jenis File | Aplikasi Recovery | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PhotoRec | | | Scalpel | | | Foremost | | | TestDisk | | |
| | Ext2 | Ext3 | Ext4 | Ext2 | Ext3 | Ext4 | Ext2 | Ext3 | Ext4 | Ext2 | Ext3 | Ext4 |
| 7z | √ | √ | √ | X | X | X | X | X | X | √ | √ | √ |
| Avi | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Bmp | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Doc | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Exe | √ | √ | √ | X | X | X | X | X | X | √ | √ | √ |
| Flv | √ | √ | √ | X | X | X | X | X | X | √ | √ | √ |
| Gif | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Gz | √ | √ | √ | X | X | X | X | X | X | √ | √ | √ |
| Htm | X | X | X | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Ico | √ | √ | √ | X | X | X | X | X | X | √ | √ | √ |
| Iso | √ | √ | √ | X | X | X | X | X | X | √ | √ | √ |
| Jpg | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Mkv | √ | √ | √ | X | X | X | X | X | X | √ | √ | √ |
| Mov | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| mp3 | √ | √ | √ | X | X | X | √ | √ | √ | √ | √ | √ |
| Mpg | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Pdf | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Png | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Psd | √ | √ | √ | X | X | X | X | X | X | √ | √ | √ |
| Rar | √ | √ | √ | X | X | X | X | X | X | √ | √ | √ |
| Rm | √ | √ | √ | X | X | X | X | X | X | √ | √ | √ |
| Swf | √ | √ | √ | X | X | X | X | X | X | √ | √ | √ |
| Tif | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Txt | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Wav | X | X | X | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Wmv | X | X | X | X | X | X | √ | √ | √ | √ | √ | √ |
| Zip | √ | √ | √ | √ | √ | √ | X | X | X | √ | √ | √ |

Keterangan : √ = Baik (Poin 10)

X = Buruk (Poin 0)

**Tabel 5 Hasil Pengujian Aplikasi**

| Kegiatan | Ukuran File | File Sistem | | |
|---|---|---|---|---|
| | | Ext2 | Ext3 | Ext4 |
| Format *File* | 23,7 MB (7 tipe *file*) | 202,1 MB | 25,1 MB | 22 MB |

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

**Tabel 6 Hasil dari tiap aplikasi**

| File Sistem | Foremost | Scalpel | TestDisk | Photorec |
|---|---|---|---|---|
| Ext2 | 150 | 140 | 270 | 240 |
| Ext3 | 150 | 140 | 270 | 240 |
| Ext4 | 150 | 140 | 270 | 240 |

Pada keterangan tabel nilai pengujian di atas, maka akan terlihat bahwa aplikasi mana yang banyak memiliki keunggulan dari segi pengembalian data pada berbagai *file* sistem Linux.

# Bab VI Kesimpulan dan Saran

## VI.1 Kesimpulan

Dari hasil analisis dan pengujian yang dilakukan, Photorec merupakan aplikasi yang paling banyak memenuhi kebutuhan forensik yaitu, mengumpulkan data, melakukan pengujian dan mengembalikan bukti digital dengan baik. Sedangkan Testdisk menjadi aplikasi yang tepat untuk pengembalian data di dalam partisi *hard disk* yang hilang, dibandingkan dengan dua aplikasi yang lain yang proses pengembalian bukti digitalnya kurang baik, karena hanya dapat mengembalikan beberapa *file* tertentu saja.

## VI.2 Saran

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

1. Melakukan perbandingan aplikasi *recovery* lainnya yaitu, Guymaker, Sleuthkit dan gddrescue.
2. Pengembang selanjutnya diharapkan dapat membuat aplikasi yang berkaitan dengan *recovery hard disk.*
3. Penelitian selanjutnya diharapkan mampu menjelaskan secara rinci proses baca tulis *hard disk* dengan formula matematika yang terdapat di dalamnya.

# DAFTAR PUSTAKA


[1] "Foremost". Tersedia: http://foremost.sourceforge.net/

[2] "Photorec" Tersedia : http://www.cgsecurity.org/wiki/PhotoRec

[3] *"TestDisk"*. Tersedia : http//www.cgsecurity.org/wiki/Test*Disk*

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

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

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

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

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

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

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

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

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

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

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

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

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

[17] Scalpel”. Tersedia: http://www.digitalforensicssolutions.com/Scalpel/

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

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

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