

IMPLEMENTASI PENGAMANAN BASIS DATA PASSWORD LOGING DENGAN TEKNIK ENKRIPSI PADA POLDA BENGKULU

Jusuf Wahyudi¹, Nugroho Ponco Riyanto², Sapri³

Dosen Tetap Fakultas Ilmu Komputer Universitas Dehasen Bengkulu

ABSTRACT

Bengkulu Police Directorate Reskrimsus using Visual Basic 6.0 programming language. The formulation of the problem is how to design a database encryption software that will help in logging application security and database programs. The purpose of this research is to create a security system logging application program by using encryption and security techniques encryption as a cryptographic security of course.

The place and time of the research conducted at the Office of the Police Directorate Reskrimsus Bhayangkara Bengkulu is in the No. 2 City Road Begkulu. The method used in this study were interviews, observation, and literature. At this stage of encryption on logging applications using the programming language Visual Basic 6.0

From the discussion, it can be concluded that in Bengkulu Police Directorate Reskrimsus evidence in the record necessary for logging in with the password encryption techniques so that not all personnel can open and change it.

Key : Reskrimsus, encryption, cryptographic

INTISARI

Dit Reskrimsus Polda Bengkulu menggunakan bahasa pemograman Visual Basic 6,0. Perumusan masalah adalah bagaimana merancang suatu perangkat lunak pengenkripsian basis data pada loging yang akan membatu keamanan aplikasi program dan database. Tujuan dari penelitian ini adalah untuk membuat system keamanan loging aplikasi program dengan menggunakan enkripsi dan mempelajari teknik pengamanan enkripsi sebagai kriptografi sekuriti.

Tempat dan waktu penelitian dilakukan pada Kantor Dit Reskrimsus Polda Bengkulu berada di Jalan Bhayangkara No 2 Kota Begkulu. Metode yang digunakan dalam penelitian ini adalah metode wawancara, observasi, dan studi pustaka. Pada tahap pengenkripsian pada loging aplikasi menggunakan bahasa pemograman visual basic 6,0

Dari pembahasan dapat disimpulkan bahwa di Dit Reskrimsus Polda Bengkulu dalam mendata barang bukti perlu di buat loging password dengan teknik enkripsi supaya tidak seluruh personel dapat membuka dan merubahnya.

Kunci : Reskrimsus, enkripsi, kriptografi

I. PENDAHULUAN

Perkembangan teknologi informasi yang begitu cepat telah mempengaruhi segala aspek kehidupan manusia, dengan suatu kebutuhan informasi yang tidak bisa lepas dari kehidupan manusia. Ada pihak yang memberi informasi dan ada pula pihak yang menerima informasi. Biasanya proses pengiriman atau pertukaran informasi tersebut saat ini sudah dalam bentuk digital.

Masalah keamanan pada Kantor Dit Reskrimsus Polda Bengkulu merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Masalah keamanan sering berada di urutan terakhir dalam daftar-

daftar yang dianggap penting.. Saat ini, keamanan terhadap data yang tersimpan dalam basis data sudah menjadi persyaratan mutlak. Pengamanan terhadap jaringan komputer yang terhubung dengan basis data sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh “orang dalam” atau pihak – pihak yang langsung berhubungan dengan basis data seperti administrator basis data. Hal ini menyebabkan pengguna basis data harus menemukan cara untuk mengamankan data tanpa campur tangan administrator basis data.

Kemajuan sistem informasi memberikan banyak keuntungan bagi kehidupan manusia. Meski begitu, aspek negatifnya juga banyak, seperti kejahatan komputer yang mencakup pencurian, penipuan, pemerasan, dan

sebagainya. Jatuhnya informasi ke pihak lain, misalnya lawan bisnis, dapat menimbulkan kerugian bagi pemilik informasi. Contohnya informasi sebuah perusahaan hanya boleh diketahui oleh orang-orang tertentu diperusahaan tersebut, misalnya informasi sebuah produk yang sedang dalam pengembangan, algoritma dan teknik yang digunakan untuk menghasilkan produk tersebut harus tejamin keamanan informasinya agar tidak diketahui lawan bisnis perusahaan tersebut.

Pada penelitian ini, rumusan masalah yang diangkat adalah: Bagaimana merancang suatu perangkat lunak pengenkripsian basis data pada data login yang dapat membantu keamanan aplikasi program dan database. Dengan batasan masalah :

1. Perancangan program enkripsi pada login aplikasi program ini menggunakan Bahasa pemrograman visual basic 6.0.
2. Perancangan data login yang diterima adalah tidak ditentukan dan berbentuk karakter tidak numeric. Adapun tujuan dari penelitian ini adalah :
 1. Untuk membuat sistem keamanan login aplikasi program dengan menggunakan enkripsi.
 2. Melakukan teknik pengamanan enkripsi Data pada Kantor Dit Reskrimsus Polda Bengkulu.

II. KAJIAN PUSTAKA

A. Sistem Komputer

Komputer merupakan alat elektronika yang digunakan untuk mengolah data-data yang dimasukkan melalui perangkat input, selanjutnya diproses menggunakan program tertentu oleh *Central Processing Unit* (CPU), sehingga menghasilkan suatu informasi yang diinginkan. Selanjutnya Informasi yang dihasilkan itu dikeluarkan melalui perangkat *output*.

Komputer atau mikrokomputer terdiri atas 3 (tiga) bagian utama yang meliputi *Central Processing Unit* (CPU), *Main Memory*, dan *I/O modul*. Hubungan antara bagian atau elemen dasar yang membentuk sebuah komputer didapat melalui tiga jalur (*Bus*), yaitu Jalur Data (*Data Bus*), Jalur Alamat (*Address Bus*), Jalur Kontrol (*Control Bus*).

Bus alamat terdiri atas 18, 20, 24 atau lebih jalur sinyal paralel. Pada jalur-jalur ini, CPU mengirimkan alamat dari lokasi memori yang akan ditulisi atau dibaca. Jumlah lokasi memori yang dapat dialamati tergantung dari banyaknya

jalur data. Jika CPU mempunyai n jumlah jalur alamat, maka dapat mengalami 2^n lokasi memori. Bus data terdiri dari 8, 16, 32 atau lebih jalur sinyal paralel. Sifat bus data ini adalah dua arah (*bidirectional*), artinya CPU dapat membaca data dari memori atau port pada bus data tersebut. Banyak piranti yang dapat dihubungkan pada bus data ini, tetapi hanya satu peralatan output yang boleh ada pada bus data saat itu.

Bus kontrol berisi 4-10 jalur sinyal paralel. CPU mengirimkan sinyal keluaran pada bus kontrol untuk meng-enablekan output dari memori atau port yang dialamati. Umumnya sinyal-sinyal di bus kontrol adalah memori yang sedang membaca (*read*), menulis (*write*), I/O membaca (*read I/O*), dan I/O menulis (*write I/O*). (Hariyanto.B, *Sistem Operasi Lanjut*, Informatika, Bandung, 2003)

B. Tinjauan Umum Perangkat Lunak

Beberapa definisi perangkat lunak :

1. Instruksi-instruksi dalam program komputer yang bila dieksekusi akan
2. Dokumen-dokumen yang menjelaskan operasi dan pemakaian suatu program.

Jadi perangkat lunak adalah program komputer, struktur data, dan dokumentasi yang berkaitan, yang menyediakan metode logika, prosedur atau kontrol yang diminta.

Berikut ini adalah karakteristik perangkat lunak yang membedakannya dengan perangkat keras. Karakteristik perangkat lunak adalah sebagai berikut :

1. Perangkat lunak dikembangkan dan direkayasa, bukan dirakit seperti perangkat keras. Meskipun ada beberapa kesamaan pengertian antara kedua istilah tersebut, tetapi pada dasarnya berbeda.
2. Perangkat lunak tidak dibuat berdasarkan rakitan komponen yang sudah ada, sedangkan perangkat keras dibuat berdasarkan rakitan komponen yang sudah ada.
3. Perangkat lunak tidak bisa rusak, sedangkan tingkat kerusakan perangkat keras sangat tinggi. Kerusakan yang terjadi pada perangkat keras menandakan perangkat keras itu harus diganti, walaupun terkadang bisa diperbaiki.

C. Implementasi

Implementasi adalah proses untuk memastikan terlaksananya suatu kebijakan dan tercapainya kebijakan tersebut. Implementasi juga dimaksudkan menyediakan sarana untuk membuat sesuatu dan memberikan hasil yang

bersifat praktis terhadap sesama. Van Horn Dan Van Meter mengartikan Implementasi kebijakan sebagai :

"Tindakan-tindakan oleh individu publik dan swasta (atau kelompok) yang diarahkan pada prestasi tujuan yang ditetapkan dalam keputusan kebijakan sebelumnya". (Van Horn Dan Van Meter dalam Subarsono 2006 : 100).

Jadi Implementasi dimaksudkan sebagai tindakan individu publik yang diarahkan pada tujuan serta ditetapkan dalam keputusan dan memastikan terlaksananya dan tercapainya suatu kebijakan serat memberikan hasil yang bersifat praktis terhadap sesama. Sehingga dapat tercapainya sebuah kebijakan yang memeberikan hasil terhadap tindakan tindakan individu publik dan swasta.

Berdasarkan pengertian implementasi yang dikemukakan diatas, dapat dikatakan bahwa implementasi adalah tindakan-tindakan yang dilakukan pihak-pihak yang berwenang atau kepentingan baik pemerintah maupun swasta yang bertujuan untuk mewujudkan cita-cita atau tujuan yang telah ditetapkan, implementasi dengan berbagai tindakan yang dilakukan untuk melaksanakan atau merealisasikan program yang telah disusun demi tercapainya tujuan dari program yang telah direncanakan karena pada dasarnya setiap rencana yang ditetapkan memiliki tujuan atau target yang hendak dicapai.

D. Keamanan Komputer

Pokok masalah keamanan sistem salah satunya disebabkan karena sistem time sharing dan akses jarak jauh, apalagi dengan meningkatnya perkembangan jaringan komputer. Keamanan sistem komputer adalah untuk menjamin sumber daya sistem tidak digunakan / dimodifikasi, diinterupsi dan diganggu oleh orang yang tidak diotorisasi. Pengamanan termasuk masalah teknis, manajerial, legalitas dan politis (wordpress. 2009/01).

3 macam keamanan sistem, yaitu :

1. *external security* (Keamanan eksternal) Berkaitan dengan pengamanan fasilitas komputer dari penyusup dan bencana seperti kebakaran /kebanjiran.
2. *user interface security* (Keamanan interface pemakai) Berkaitan dengan indentifikasi pemakai sebelum pemakai diijinkan mengakses program dan data yang disimpan.
3. *internal security* (Keamanan internal) Berkaitan dengan pengamanan beragam

kendali yang dibangun pada perangkat keras dan sistem operasi yang menjamin operasi yang handal dan tak terkorupsi untuk menjaga integritas program dan data.

Ada 2 masalah penting keamanan, yaitu :

1. data loss (Kehilangan data)
Kehilangan data disebabkan karna adanya kesalahan yang disebabkan oleh pengguna itu sendiri.
2. intruder (Penyusup)
 - a. Penyusup pasif, yaitu yang membaca data yang tidak terotorisasi
 - b. Penyusup aktif, yaitu mengubah data yang tidak terotorisasi.

Sasaran keamanan adalah menghindari, mencegah dan mengatasi ancaman terhadap sistem. 2 aspek kebutuhan keamanan sistem komputer, yaitu :

1. *Secrecy* (Kerahasiaan), diantaranya privasi Keterjaminan bahwa informasi di sistem komputer hanya dapat diakses oleh pihak-pihak yang terotorisasi dan modifikasi tetap menjaga konsistensi dan keutuhan data di sistem
2. *integrity* (Integritas) Keterjaminan bahwa sumber daya sistem komputer hanya dapat dimodifikasi oleh pihak-pihak yang terotorisasi
3. *availability* (Ketersediaan) Keterjaminan bahwa sumber daya sistem komputer bagi pihak-pihak yang diotorisasi saat diperlukan.

Tipe ancaman terhadap keamanan sistem komputer dapat dimodelkan dengan memandang fungsi system komputer sebagai penyedia informasi. Berdasarkan fungsi ini, ancaman terhadap sistem komputer dikategorikan menjadi 4 ancaman, yaitu :

1. *interuption* (Interupsi)
Sumber daya sistem komputer dihancurkan / menjadi tak tersedia / tak berguna. Merupakan ancaman terhadap ketersediaan. Contohnya penghancuran harddisk, pemotongan kabel komunikasi.
2. *interception* (Intersepsi)
Pihak tak diotorisasi dapat mengakses sumber daya. Merupakan ancaman terhadap kerahasiaan. Pihak tak diotorisasi dapat berupa orang / program komputer. Contohnya penyadapan, mengcopy file tanpa diotorisasi.

3. *modification* (Modifikasi)

Pihak tak diotorisasi tidak hanya mengakses tapi juga merusak sumber daya. Merupakan ancaman terhadap integritas. Contohnya mengubah nilai file, mengubah program, memodifikasi pesan.

4. *fabrication* (Fabrikasi)

Pihak tak diotorisasi menyisipkan / memasukkan objek-objek palsu ke sistem. Merupakan ancaman terhadap integritas. Contohnya memasukkan pesan palsu ke jaringan, menambah record file (wordpress. 2009/01.)

E. Sistem Keamanan File / Data

Aspek keamanan data sebenarnya meliputi banyak hal yang saling berkaitan, tetapi khusus dalam tulisan ini penulis akan membahas tentang metoda enkripsi dan keamanan proteksi data pada beberapa program-program aplikasi umum. Hampir semua program aplikasi seperti MS Word, WordPerfect, Excel (Hidayatno, Achmad. 2006.)

F. Password

Menurut Nugroho, Setyo (2004:15), Password adalah kode sandi yang harus dimasukkan ke dalam suatu sistem baik itu sistem komputer yang menggunakan sistem operasi windows atau bukan yang berupa karakter tulisan, suara, atau ciri-ciri khusus yang harus diingat. Kalau sampai lupa, bisa berantakan, ditambah ada hal penting dan harus segera dilakukan atau diketahui. Untuk memberikan keamanan pada Password anda sebaiknya anda mengikuti cara di bawah ini:

1. Gunakan password yang acak dan tidak mudah di terka tapi mudah di ingat untuk anda sendiri contoh: "kr1wul"
2. Gunakan huruf dan angka untuk memberikan kombinasi pada password anda
3. Update password anda 2 minggu sekali
4. Jangan memberitahukan password anda ke saudara / teman anda
5. Jangan melupakan password (sebaiknya anda catat dan disimpan dengan baik)

E. Kriptografi dan Sistem Informasi

Keamanan telah menjadi aspek yang sangat penting dari suatu sistem informasi. Sebuah informasi umumnya hanya ditujukan bagi golongan tertentu. Oleh karena itu sangat

penting untuk mencegahnya jatuh kepada pihak-pihak lain yang tidak berkepentingan. Untuk melaksanakan tujuan tersebutlah dirancang suatu sistem keamanan yang berfungsi melindungi sistem informasi. (Ariyus D, Kriptografi, Keamanan Data dan Komunikasi)

Salah satu upaya pengamanan sistem informasi yang dapat dilakukan adalah kriptografi. Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi, antara lain seperti kerahasiaan, integritas data, otentikasi, dan ketiadaan penyangkalan. Keempat aspek tersebut merupakan tujuan fundamental dari suatu sistem kriptografi.

1. Kerahasiaan (*confidentiality*)

Kerahasiaan adalah layanan yang digunakan untuk menjaga informasi dari setiap pihak yang tidak berwenang untuk mengaksesnya. Dengan demikian informasi hanya akan dapat diakses oleh pihak-pihak yang berhak saja.

2. Integritas data (*data integrity*)

Integritas data merupakan layanan yang bertujuan untuk mencegah terjadinya perubahan informasi oleh pihak-pihak yang tidak berwenang. Untuk meyakinkan integritas data ini harus dipastikan agar sistem informasi mampu mendeteksi terjadinya manipulasi data. Manipulasi data yang dimaksud di sini meliputi penyisipan, penghapusan, maupun penggantian data.

3. Otentikasi (*authentication*)

Otentikasi merupakan layanan yang terkait dengan identifikasi terhadap pihak-pihak yang ingin mengakses sistem informasi (*entity authentication*) maupun keaslian data dari sistem informasi itu sendiri (*data origin authentication*).

4. Ketidadaan penyangkalan (*non-repudiation*)

Ketidadaan penyangkalan adalah layanan yang berfungsi untuk mencegah terjadinya penyangkalan terhadap suatu aksi yang dilakukan oleh pelaku sistem informasi.

F. Mekanisme Kriptografi

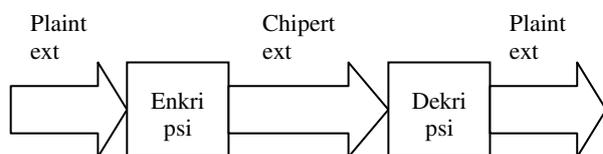
Suatu sistem kriptografi (kriptosistem) bekerja dengan cara menyandikan suatu pesan menjadi suatu kode rahasia yang dimengerti oleh pelaku sistem informasi saja. Pada dasarnya mekanisme kerja semacam ini telah dikenal sejak jaman dahulu. Bangsa Mesir kuno sekitar 4000 tahun yang lalu bahkan telah mempraktekannya dengan cara yang sangat primitif. (R. Munir,

Bahan Kuliah IF5054 Kriptografi, Departemen Teknik Informatika, ITB, 2004.)

Dalam era teknologi informasi sekarang ini, mekanisme yang sama masih digunakan tetapi tentunya implementasi sistemnya berbeda. Sebelum membahas lebih jauh mekanisme kriptografi modern, berikut ini diberikan beberapa istilah yang umum digunakan dalam pembahasan kriptografi.

1. *Plaintext*
Plaintext (message) merupakan pesan asli yang ingin dikirimkan dan dijaga keamanannya. Pesan ini tidak lain dari informasi tersebut.
2. *Chipertext*
Chipertext merupakan pesan yang telah dikodekan (disandikan) sehingga siap untuk dikirimkan.
3. *Chiper*
Chiper merupakan algoritma matematis yang digunakan untuk proses penyandian plaintext menjadi ciphertext.
4. *Enkripsi*
Enkripsi (encryption) merupakan proses yang dilakukan untuk menyandikan plaintext sehingga menjadi chipertext.
5. *Dekripsi*
Dekripsi (decryption) merupakan proses yang dilakukan untuk memperoleh kembali plaintext dari chipertext.
6. *Kriptosistem*
Kriptosistem merupakan sistem yang dirancang untuk mengamankan suatu sistem informasi dengan memanfaatkan kriptografi.

Urutan-urutan proses kriptografi dapat digambarkan sebagai berikut.



Gambar 2.1. Mekanisme kriptografi

Prosesnya pada dasarnya sangat sederhana. Sebuah plaintext (m) akan dilewatkan pada proses enkripsi (E) sehingga menghasilkan suatu ciphertext (c). Kemudian untuk memperoleh kembali plaintext, maka ciphertext (c) melalui proses dekripsi (D) yang akan menghasilkan

kembali plaintext (m). Secara matematis proses ini dapat dinyatakan sebagai,

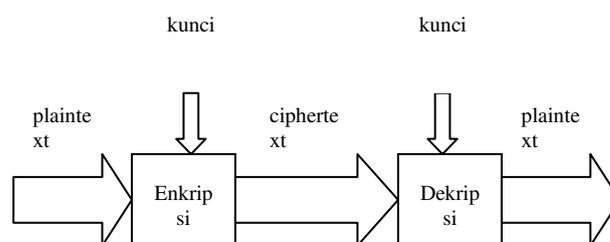
$$E(m) = c$$

$$D(c) = m$$

$$D(E(m)) = m$$

Kriptografi sederhana seperti ini menggunakan algoritma penyandian yang disebut *cipher*. Keamanannya bergantung pada kerahasiaan algoritma penyandian tersebut, karena itu algoritmanya harus dirahasiakan. Pada kelompok dengan jumlah besar dan anggota yang senantiasa berubah, penggunaannya akan menimbulkan masalah. Setiap ada anggota yang meninggalkan kelompok, algoritma harus diganti karena anggota ini dapat saja membocorkan algoritma. (Arnoldus Trio. *Kolaborasi Persandian dan Komunikasi*. <http://www.tni.mil.id>. Tanggal akses: 24 April 2012 pukul 20.45)

Kriptografi modern selain memanfaatkan algoritma juga menggunakan kunci (*key*) untuk memecahkan masalah tersebut. Proses enkripsi dan dekripsi dilakukan dengan menggunakan kunci ini. Setiap anggota memiliki kuncinya masing-masing yang digunakan untuk proses enkripsi dan dekripsi yang akan dilakukannya. Dengan demikian ada sedikit perubahan yang harus dilakukan pada mekanisme yang digambarkan pada gambar 2.1 menjadi seperti gambar 2.2 berikut ini.



Gambar 2.2 Kriptografi berbasis kunci

Mekanisme kriptografi seperti ini dinamakan kriptografi berbasis kunci. Dengan demikian kriptosistemnya akan terdiri atas algoritma dan kunci, beserta segala plaintext dan ciphertextnya. Persamaan matematisnya menjadi seperti berikut,

$$E_e(m) = c$$

$$D_d(c) = m$$

$$D_d(E_e(m)) = m$$

dengan, e = kunci enkripsi
 d = kunci dekripsi

G.Enkripsi

Enkripsi ialah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, namun, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi. Di pertengahan tahun 1970an enkripsi kuat dimanfaatkan untuk pengaman oleh sekretariat agen pemerintah Amerika Serikat pada domain publik, dan saat ini enkripsi telah digunakan pada sistem secara luas, seperti Internet, e-commerce, jaringan telepon bergerak dan ATM pada bank.

Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integrasi dan autentikasi dari sebuah pesan. Untuk menampilkan enkripsi dan kebalikannya dekripsi, digunakan algoritma yang biasa disebut Cipher dengan menggunakan metode serangkaian langkah yang terdefinisi yang diikuti sebagai prosedur. Alternatif lain ialah encipherment. Informasi yang asli disebut sebagai plaintext, dan bentuk yang sudah dienkripsi disebut sebagai ciphertext. Pesan ciphertext berisi seluruh informasi dari pesan plaintext, tetapi tidak dalam format yang didapat dibaca manusia ataupun komputer tanpa menggunakan mekanisme yang tepat untuk melakukan dekripsi.

Cipher pada biasanya memiliki parameter dari sebagian dari informasi utama, disebut sebagai kunci. Prosedur enkripsi sangat bervariasi tergantung pada kunci yang akan mengubah rincian dari operasi algoritma. Tanpa menggunakan kunci, cipher tidak dapat digunakan untuk dienkripsi ataupun didekripsi. (Tops Fari Bima Pratama. Pengertian Enkripsi <http://wartawarga.gunadarma.ac.id/2010/03/pengertian-enkripsi/>)

H.Kriptografi Simetrik dan Asimetrik

Berdasarkan jenis kunci yang digunakan dalam proses enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi dua jenis, yaitu kriptografi simetrik dan kriptografi asimetrik. Perbedaan utama di antara keduanya terletak pada sama dan tidaknya

kunci yang digunakan dalam proses enkripsi dengan kunci yang digunakan pada proses dekripsi. (Ariyus D, Kriptografi, Keamanan Data dan Komunikasi)

I.Kriptografi Simetrik

Kriptografi simetrik (*symmetric cryptography*) atau dikenal pula sebagai kriptografi kunci rahasia (*secret-key cryptography*), merupakan kriptografi yang menggunakan kunci yang sama baik untuk proses enkripsi maupun dekripsi. Secara matematis dapat dinyatakan bahwa :

$$e = d = k$$

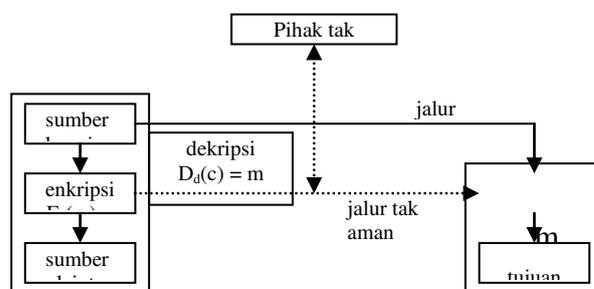
$$E_k(m) = c$$

$$D_k(c) = m$$

Kriptografi simetrik sangat menekankan pada kerahasiaan kunci yang digunakan untuk proses enkripsi dan dekripsi. Oleh karena itulah kriptografi ini dinamakan pula sebagai kriptografi kunci rahasia.

Mekanisme kerja kriptografi simetrik antara dua pelaku sistem informasi, Santi dan Sean, adalah sebagai berikut,

1. Santi dan Sean menyetujui algoritma simetrik yang akan digunakan.
2. Santi dan Sean menyetujui kunci yang akan dipakai.
3. Santi membuat pesan plaintext yang akan dikirimkan kepada Sean, lalu melakukan proses enkripsi dengan menggunakan kunci dan algoritma yang telah disepakati sehingga menghasilkan ciphertext.
4. Santi mengirimkan ciphertext tersebut kepada Sean.
5. Sean menerima ciphertext, lalu melakukan dekripsi dengan menggunakan kunci dan algoritma yang sama sehingga dapat memperoleh plaintext tersebut.



Gambar 2.3 Mekanisme kriptografi simetrik

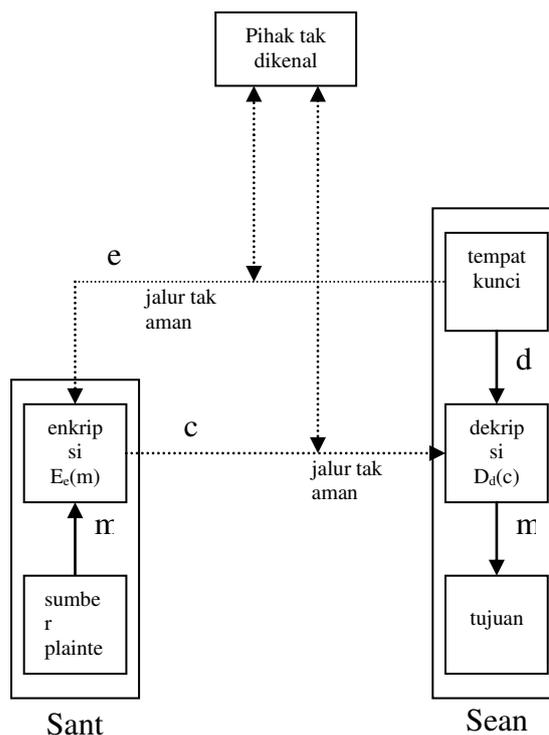
Dari gambar 2.3 dapat dilihat bahwa harus ada jalur aman (*secure channel*) dahulu yang memungkinkan Sean dan Santi melakukan transaksi kunci. Hal ini menjadi masalah karena jika jalur itu memang ada, tentunya kriptografi tidak diperlukan lagi dalam hal ini. Masalah ini dikenal sebagai masalah persebaran kunci (*key distribution problem*). Kelemahan lainnya adalah bahwa untuk tiap pasang pelaku sistem informasi diperlukan sebuah kunci yang berbeda. Dengan demikian bila terdapat n pelaku sistem informasi, maka agar tiap pasang dapat melakukan komunikasi diperlukan kunci sejumlah total $n(n - 1) / 2$ kunci. Untuk jumlah n yang sangat besar, penyediaan kunci ini akan menjadi masalah, yang dikenal sebagai masalah manajemen kunci (*key management problem*). (Ariyus D, Kriptografi, Keamanan Data dan Komunikasi)

Namun di samping kelemahan tersebut, kriptografi simetrik memiliki keuntungan juga. Keuntungan menggunakan kriptografi simetrik ini adalah kecepatan operasinya yang sangat baik. Dibandingkan dengan kriptografi asimetrik, kriptografi simetrik memiliki kecepatan operasi yang jauh lebih cepat.

J.Kriptografi Asimetrik

Kriptografi asimetrik (*asymmetric cryptography*) menggunakan kunci enkripsi dan kunci dekripsi yang berbeda. Kunci enkripsi dapat disebarakan kepada umum dan dinamakan sebagai kunci publik (*public key*) sedangkan kunci dekripsi disimpan untuk digunakan sendiri dan dinamakan sebagai kunci pribadi (*private key*). Oleh karena itulah, kriptografi ini dikenal pula dengan nama kriptografi kunci publik (*public key cryptography*).

Pada kriptosistem asimetrik, setiap pelaku sistem informasi memiliki sepasang kunci, yaitu kunci publik dan kunci pribadi. Kunci publik didistribusikan kepada umum, sedangkan kunci pribadi disimpan untuk diri sendiri. Dengan menggunakan kriptografi asimetrik, mekanisme pengiriman pesan oleh Santi kepada Sean menjadi seperti gambar berikut ini.



Gambar 2.4 Mekanisme kriptografi asimetrik

Langkah-langkahnya adalah sebagai berikut,

1. Santi mengambil kunci publik milik Sean yang didistribusikan kepada umum.
2. Santi melakukan enkripsi terhadap plaintext dengan kunci publik Sean tersebut sehingga menghasilkan ciphertext.
3. Santi mengirimkan ciphertext kepada Sean.
4. Sean yang menerima ciphertext tersebut melakukan proses dekripsi dengan menggunakan kunci pribadi miliknya sehingga mendapatkan plaintext semula.

Dengan cara ini masalah yang dihadapi pada kriptografi simetrik bisa dipecahkan. Sebuah jalur aman untuk distribusi kunci tidak lagi diperlukan. Selain itu manajemen kuncinya lebih mudah. Karena tiap pelaku sistem informasi memiliki sepasang kunci, maka untuk n pelaku dibutuhkan total $2n$ kunci saja. Namun demikian, kriptografi asimetrik memiliki kecepatan operasi yang jauh lebih lambat daripada kriptografi simetrik. (Arnoldus Trio.Kolaborasi

Persandian dan Komunikasi.
<http://www.tni.mil.id>)

Salah satu kriptografi asimetrik yang banyak dipakai sekarang ini adalah RSA. RSA menjadi standar *de facto* kriptografi asimetrik dunia dan banyak dipakai pada transaksi-transaksi data dalam protokol.

K.Kriptografi Gabungan

Kriptografi yang digunakan sekarang ini merupakan kombinasi antara kriptografi simetrik dengan asimetrik. Dengan cara ini, keunggulan dari kedua sistem kriptografi ini dapat dimanfaatkan sementara kekurangannya dapat diminimisasi.

Skenario kriptografi gabungan ini bekerja sebagai berikut,

1. Santi mengambil kunci publik milik Sean yang didistribusikan kepada umum.
2. Santi membangkitkan bilangan acak yang akan digunakan sebagai kunci simetriknya. Bilangan acak ini kemudian dienkripsi dengan menggunakan kunci publik milik Sean.
3. Kunci simetrik yang telah dienkripsi ini dikirimkan kepada Sean.
4. Sean yang menerimanya melakukan proses dekripsi dengan menggunakan kunci pribadi miliknya sehingga mendapatkan kunci simetrik tersebut.
5. Setelah kunci simetrik berhasil ditransfer dengan aman, selanjutnya keduanya berkomunikasi dengan menggunakan kunci simetrik tersebut.

Keuntungan dengan menggunakan kenario gabungan ini tidak lain bahwa kecepatan proses kriptografi simetrik dimanfaatkan secara maksimal, sementara itu masalah ketiadaan jalur aman untuk transfer kunci simetrik diatasi dengan menggunakan kriptografi asimetrik. Dalam implementasi kriptosistem modern, skenario kriptografi gabungan ini sangat populer. (Pengantar Kriptografi. <http://www.kur2003.if.itb.ac.id>)

L.Keamanan Sistem Kriptografi

Keamanan suatu sistem kriptografi merupakan masalah yang paling fundamental. Dengan menggunakan sistem standar terbuka, maka keamanan suatu

sistem kriptografi akan lebih mudah dan lebih cepat dianalisa. Mengingat kenyataan inilah maka sekarang tidak digunakan lagi algoritma rahasia yang tidak diketahui tingkat keamanannya.

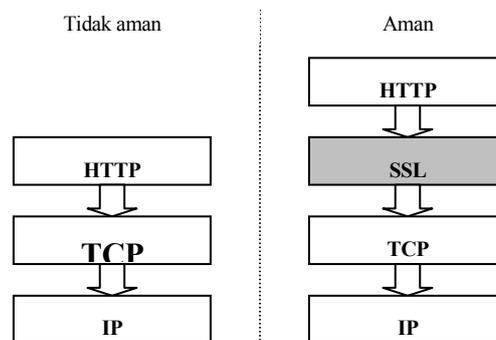
Sebuah sistem kriptografi dirancang untuk menjaga plaintext dari kemungkinan dibaca oleh pihak-pihak yang tidak berwenang, yang secara umum dinamakan sebagai penyerang (*attacker*). Penyerang diasumsikan memiliki akses tak terbatas terhadap jalur tak aman yang digunakan untuk transaksi ciphertext. Oleh karena itu, penyerang dianggap memiliki akses langsung terhadap ciphertext.

Tipe penyerang paling umum terhadap suatu sistem kriptografi adalah serangan kriptanalisis (*cryptanalysis attack*). Kriptanalisis merupakan ilmu yang mempelajari tentang upaya-upaya untuk memperoleh plaintext dari ciphertext tanpa informasi tentang kunci yang digunakan. (Ariyus D, *Kriptografi, Keamanan Data dan Komunikasi*)

M.Penggunaan Sistem Kriptografi

Sistem kriptografi pada era sistem informasi ini telah dimanfaatkan dalam pengamanan suatu sistem informasi. Pada jaringan TCP/IP (*Transfer Control Protocol/Internet Protocol*) misalnya, kriptografi telah dimanfaatkan pada protokol S/HTTP. Protokol S/HTTP (*Secure Hypertext Transfer Protocol*) saat ini digunakan untuk transaksi HTTP dengan memanfaatkan kriptografi sebagai mekanisme untuk menyandikan pesan yang dikirim.

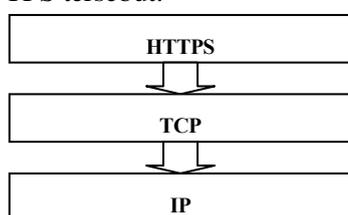
Gambar dibawah ini menunjukkan mekanisme enkapsulasi data pada jaringan TCP/IP tanpa dan dengan kriptografi.



Gambar 2.5 Kriptografi pada TCP/IP

Dapat dilihat bahwa ada penambahan satu layer baru yang dinamakan sebagai SSL (*Secure Socket Layer*). Layer ini berfungsi untuk melaksanakan mekanisme kriptografi terhadap informasi sebelum dilakukan enkapsulasi dan pengiriman data. Penambahan layer SSL ini menyebabkan terbentuknya protokol baru yang dinamakan HTTPS, menggantikan protokol HTTP untuk transaksi HTTP yang aman. Protokol ini digunakan untuk mengamankan transaksi-transaksi data pada web-web *e-commerce*.

Gambar berikut menunjukkan protokol HTTPS tersebut.



Gambar 2.6 Protokol HTTPS

N.Visual Basic

1).Pengenalan Visual Basic

Visual basic adalah salah satu bahasa pemrograman komputer yang digunakan untuk aplikasi windows yang berbasis (GUI Graphical User Interface). Visual basic merupakan *event-driven programming* (Pemrograman terkendali kejadian) artinya program menunggu sampai adanya respon dari pemakai berupa event/kejadian tertentu (tombol diklik, menu dipilih, dan lainlain). Ketika event terdeteksi, kode yang berhubungan dengan event (prosedurevent) akan dijadikan. (Jogiyanto, *HM, Visual Basic Untuk Pemula : 2001*)

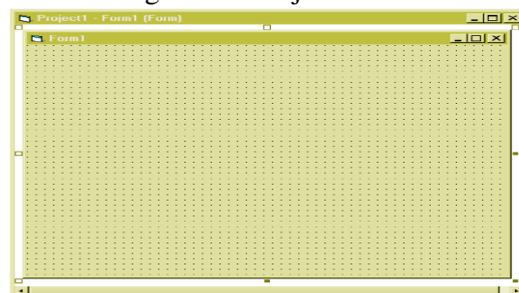
Bahasa pemrograman Visual Basic, yang dikembangkan oleh Microsoft sejak tahun 1991, merupakan pengembangan dari pendahulunya yaitu bahasa pemrograman BASIC (Beginner s All-Purpose Symbolic Instruction Code) yang dikembangkan pada era 1950-an. Visual Basic merupakan salah satu Development Tool yaitu alat bantu untuk membuat berbagai macam program komputer, khususnya yang menggunakan sistem operasi windows. Visual Basic merupakan salah satu bahasa pemrograman

komputer yang mendukung object (Object Oriented Programming = OOP).

2).Komponen Komponen Visual Basic

Visual basic selain mempunyai komponen komponen seperti halnya program aplikasi yang berbasis Windows yaitu, baris menu dan toolbar, juga mempunyai komponen komponen yang berfungsi sebagai alat untuk membuat program yaitu :

- 1) Form adalah jendela di mana akan dibuat tampilan, yang bentuknya akan di sesuaikan oleh pembuat, berikut ini adalah gambar dari jendela form :



Gambar 2.7 Form antar muka Visual Basic 6.0

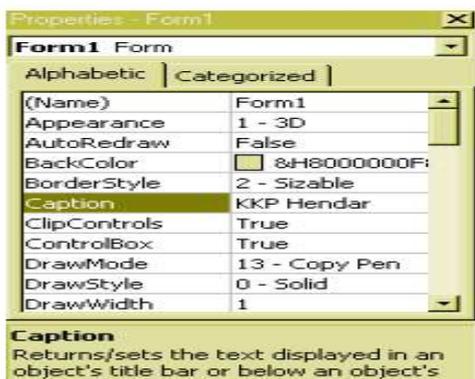
- 2) Toolbox - adalah kumpulan dari objek yang digunakan untuk membuat user interface serta kontrol bagi program aplikasi, berikut ini gambar dari :



Gambar 2.8 Toolbox visual basic 6.0

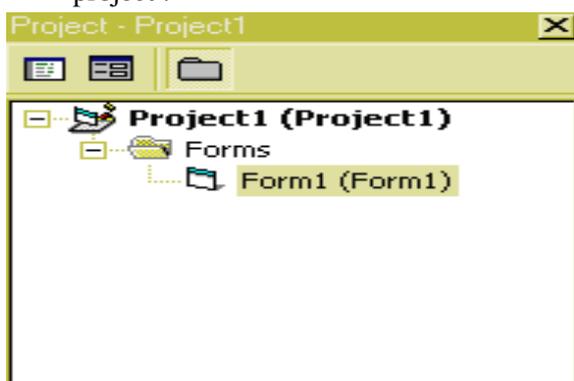
- 3) Jendela Properties adalah nilai / karakteristik yang dimiliki oleh sebuah objek Visual Basic. Visual Basic menerapkan properti default/standart.

Berikut ini adalah gambar dari jendela properties :



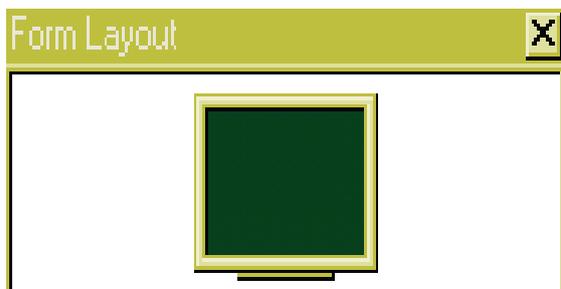
Gambar 2.9 Jendela Properties Visual basic 6.0

4) Jendela Project digunakan untuk menampilkan daftar form dan modul. Project merupakan kumpulan dari modul form, modul class, modul standar, dan file sumber yang membentuk suatu aplikasi. Berikut ini adalah gambar dari jendela project :



Gambar 2.10 Jendela Project Visual Basic 6.0

5) Jendela layout digunakan untuk menampilkan posisi form relative terhadap layar monitor. Berikut ini adalah gambar dari jendela layout :



Gambar 2.11 Jendela Layout Visual Basic 6.0

O. ActiveX Control

ActiveX control merupakan program yang terpisah dari Microsoft visual basic. ActiveX ini digunakan untuk menambahkan kontrol-kontrol standar yang di sediakan visual basic. Dengan menggunakan ActiveX control ini anda bisa lebih mengembangkan aplikasi yang dibuat.

P. Diagram Alur (Flow Chart)

Suatu metode untuk menggambarkan tahap – tahap pemecahan masalah adalah dengan mempresentasikan simbol – simbol tertentu yang mudah di mengerti dan standart. Program flowchart adalah salah satu yang dapat didefinisikan sebagai bagan yang menjelaskan secara rinci langkah – langkah dari proses program (Jogiyanto, *HM : 2001 : 802*).

Simbol	Nama simbol	Keterangan
	Terminal	Untuk menggambarkan awal dan akhir proses aliran dokumen.
	Processing	Dipakai untuk pengolahan aritmatika dan pemindahan data
	Preparation	Dipakai untuk memberikan nilai awal dari suatu variable atau counter
	Decision	Dipakai untuk mewakili operasi perbandingan logika
	Predefined process	Dipakai untuk proses yang detailnya dijelaskan secara terpisah , misalnya dalam bentuk subroutine
	Garis alir	Dipakai untuk menunjukkan aliran dari program
	Penghubung	Menunjukkan penghubung di halaman yang masih sama atau di halaman lainnya
	Input / Output	Mewakili data input atau output

Q.Data Base

Menurut Sutanta Edhie (2004) dalam bukunya yang berjudul *Sistem Basis Data* menjelaskan bahwa: “Basis data dapat dipahami sebagai suatu kumpulan data terhubung (*interrelated data*) yang disimpan secara bersama-sama pada suatu media, tanpa mengatap satu sama lain atau tidak perlu suatu kerangkapan data (kalaupun ada maka kerangkapan data tersebut harus seminimal mungkin dan terkontrol (*controlled redundancy*), data disimpan dengan cara-cara tertentu sehingga mudah untuk digunakan atau ditampilkan kembali, data dapat digunakan satu atau lebih program-program aplikasi secara optimal, data disimpan tanpa mengalami ketergantungan dengan program yang akan menggunakannya, data disimpan sedemikian rupa sehingga proses penambahan, pengambilan dan modifikasi data dapat dilakukan dengan mudah dan terkontrol.” (Hasan: 2004:18)

a. Flasdisk

Penggerak kilat USB (bahasa Inggris: USB flash drive) adalah alat penyimpanan data memori kilat tipe NAND yang memiliki alat penghubung USB yang terintegrasi. Penggerak kilat ini biasanya berukuran kecil, ringan, serta bisa dibaca dan ditulisi dengan mudah. Per November 2006, kapasitas yang tersedia untuk penggerak kilat USB ada dari 64 megabita sampai 512 gigabita. Besarnya kapasitas media ini tergantung dari teknologi memori kilat yang digunakan.

Penggerak kilat USB memiliki banyak kelebihan dibandingkan alat penyimpanan data lainnya, khususnya cakram flopi atau cakram padat. Alat ini lebih cepat, kecil, dengan kapasitas lebih besar, serta lebih dapat diandalkan (karena tidak memiliki bagian yang bergerak) daripada disket.

Namun Penggerak kilat USB juga memiliki umur penyimpanan data yang

singkat, biasanya ketahanan data pada Penggerak kilat USB rata-rata 5 tahun. Ini disebabkan oleh memori kilat yang digunakan tidak bertahan lama. Bandingkan dengan cakram keras yang memiliki ketahanan data hingga 12 tahun, CD/DVD berkualitas (dan bermerek terkenal) selama 15 tahun jika cara penyimpanannya benar. Sumber : [http://id.wikipedia.org/wiki/USB flash drive](http://id.wikipedia.org/wiki/USB_flash_drive)

b. Printer

Printer adalah deffinisi printer adalah pengertian printer adalah apa itu printer adalah - Printer adalah Printer atau pencetak adalah alat yang menampilkan data dalam bentuk cetakan, baik berupa teks maupun gambar maupun grafik, di atas kertas. Printer biasanya terbagi atas beberapa bagian, yaitu picker sebagai alat mengambil kertas dari tray. Tray ialah tempat menaruh kertas.

Tinta atau toner adalah alat pencetak sesungguhnya, karena ada sesuatu yang disebut tinta atau toner yang digunakan untuk menulis atau mencetak pada kertas. Perbedaan toner dan tinta ialah perbedaan sistem; toner atau laser butuh pemanasan, sedangkan tinta atau inkjet tak butuh pemanasan, hanya pembersihan atau cleaning pada print-head printer tersebut.

Ada pula kabel fleksibel untuk pengiriman sinyal dari prosesor printer ke tinta atau toner. Kabel ini tipis dan fleksibel, namun kuat. Pada bagian belakang printer biasanya ada port paralel atau USB untuk penghubung ke komputer. Pencetak modem merupakan alat canggih. Perkakasan elektronik yang terdapat dalam sebuah pencetak sama dengan perkakasan elektronik yang terdapat dalam komputer itu sendiri. Pencetak mempunyai 6 jenis yaitu jenis Dot-Matrix, jenis Daisy Wheel, jenis Ink-Jet atau jenis Bubble Jet, jenis Chain, jenis Drum dan jenis Laser.

tindak pindana khusus. Bagian Reskrimus Kepolisian di Daerah Provinsi Bengkulu berada di Jalan Bhayangkara No. 02 Kota Bengkulu.

Untuk peningkatan mutu keamanan dalam proses penyimpanan data barang

III.ANALISA DAN PERANCANGAN

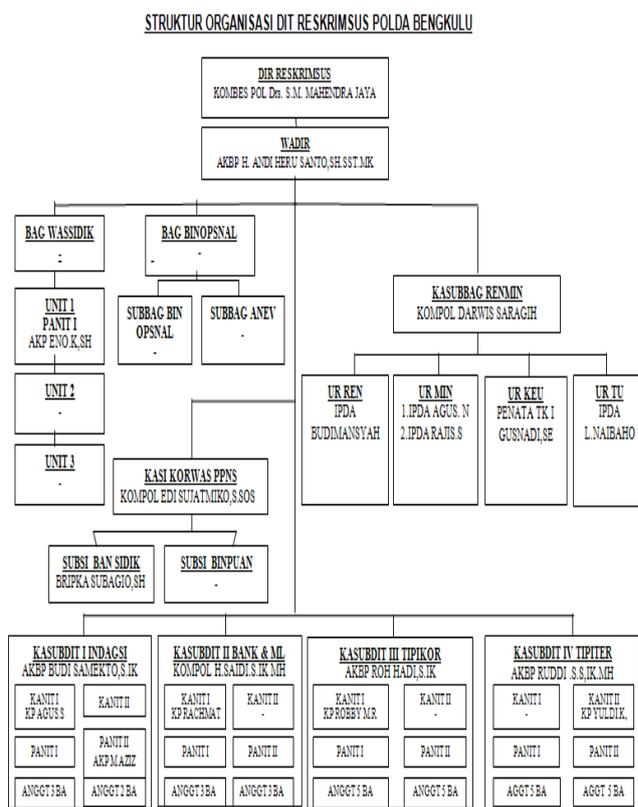
A. Resk.Kepolisian Bengkulu

Direktorat Reserse Kriminal Khusus Kepolisian Daerah Provinsi Bengkulu merupakan bagian yang menangani tentang

bukti kejahatan yang menggunakan program aplikasi tertentu maka perlu di rancang sebuah program khusus yang bisa mengenkripsikan password pada login aplikasi tersebut.

Struktur Organisasi

Struktur Organisasi Direktorat Reserse Kriminal Khusus Kepolisian Daerah Provinsi Bengkulu



Gambar 3.1 Struktur Organisasi Tugas dan Wewenang

- (1) Dit Reskrimsus sebagaimana dimaksud dalam Pasal 10 huruf d merupakan unsur pelaksana tugas pokok yang berada di bawah Kapolda.
- (2) Dit Reskrimsus bertugas menyelenggarakan penyelidikan dan penyidikan tindak pidana khusus, koordinasi, pengawasan operasional, dan administrasi penyidikan PPNS sesuai dengan ketentuan peraturan perundang-undangan.
- (3) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (2), Dit Reskrimsus menyelenggarakan fungsi:

- a. Penyelidikan dan penyidikan tindak pidana khusus, antara lain tindak pidana ekonomi, korupsi, dan tindak pidana tertentu di daerah hukum Polda;
 - b. penganalisisan kasus beserta penanganannya, serta mempelajari dan mengkaji efektivitas pelaksanaan tugas Dit Reskrimsus;
 - c. pembinaan teknis, koordinasi, dan pengawasan operasional, serta administrasi penyidikan oleh PPNS;
 - d. pelaksanaan pengawasan penyidikan tindak pidana khusus di lingkungan Polda; dan
 - e. pengumpulan dan pengolahan data serta menyajikan informasi dan dokumentasi program kegiatan Dit Reskrimsus.
- (4) Dit Reskrimsus dipimpin oleh Dir Reskrimsus yang bertanggungjawab kepada Kapolda, dan dalam pelaksanaan tugas sehari-hari di bawah kendali Waka Polda.
- (5) Dir Reskrimsus dalam melaksanakan tugasnya dibantu oleh Wadir Reskrimsus yang bertanggungjawab kepada Dir Reskrimsus.
- Dit Reskrimsus terdiri dari:

- a. Subbagian Perencanaan dan Administrasi (Subbagrenmin);
- b. Bagian Pembinaan Operasional (Bagbinopsnal);
- c. Bagian Pengawas penyidikan (Bagwassidik);
- d. Seksi Koordinasi dan Pengawasan Penyidik Pegawai Negeri Sipil, disingkat Sikorwas PPNS; dan
- e. Sub Direktorat (Subdit).

A. KASUBBAG RENMIN

- (1) Subbag Renmin sebagaimana dimaksud dalam Pasal 141 huruf a bertugas menyusun perencanaan program kerja dan anggaran, manajemen Sarpras, personel, dan kinerja, serta mengelola keuangan

- dan pelayanan ketata usahaan dan urusan dalam di lingkungan Dit Reskrimsus.
- (2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Subbag Renmin menyelenggarakan fungsi:
- a. Penyusunan perencanaan jangka sedang dan jangka pendek, antara lain Renstra, Rancangan Renja, Renja, kebutuhan sarana prasarana, personel, dan anggaran;
 - b. Pemeliharaan perawatan dan administrasi personel;
 - c. Pengelolaan Sarpras dan penyusunan laporan SIMAK-BMN;
 - d. pelayanan fungsi keuangan yang meliputi pembiayaan, pengendalian, pembukuan, akuntansi, dan penyusunan laporan SAI serta pertanggung-jawaban keuangan;
 - e. pengelolaan dan pelayanan ketatausahaan dan urusan dalam.
 - f. penyusunan LRA dan pembuatan laporan akuntabilitas kinerja Satker dalam bentuk LAKIP meliputi analisis target pencapaian kinerja, program, dan anggaran.
- (3) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Subbag Renmin dibantu oleh:
- a. Urren, yang bertugas membuat Renstra, Rancangan Renja, Renja, RKA-KL, DIPA, Penetapan Kinerja, KAK atau TOR, RAB, dan menyusun LAKIP Satker, serta pemantauan dan evaluasi pelaksanaan program bidang Reskrimsus di lingkungan Polda;
 - b. Urmin, yang bertugas menyelenggarakan kegiatan administrasi umum personel dan materiil logistik;
 - c. Urkeu, yang bertugas menyelenggarakan kegiatan pelayanan keuangan; dan
 - d. Urtu, yang bertugas menyelenggarakan kegiatan ketatausahaan dan urusan dalam.
- B. KABAGBIN OPS**
- (1) Bagbin opsnel sebagaimana dimaksud dalam Pasal 141 huruf b bertugas:
- a. melaksanakan pembinaan Dit Reskrimsus melalui analisis dan gelar perkara beserta penanganannya;
 - b. mempelajari dan mengkaji efektivitas pelaksanaan tugas penyelidikan dan penyidikan;
 - c. melaksanakan atihan fungsi, serta menghimpun dan memelihara berkas perkara yang telah selesai diproses dan bahan literatur yang terkait; dan
 - d. mengumpulkan dan mengolah data, serta menyajikan informasi dan dokumentasi program kegiatan Ditreskrimsus.
- (2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1) Bagbin opsnel menyelenggarakan fungsi:
- a. penganalisisan dan pengevaluasian pelaksanaan tugas Dit Reskrimsus;
 - b. pengkoordinasian pemberian dukungan operasional ke kesatuan kewilayahan;
 - c. pelatihan fungsi dan pengadministrasian kegiatan penyelidikan dan penyidikan, serta pengarsipan berkas perkara;
 - d. pengumpulan dan pengolahan data, serta penyajian informasi dan dokumentasi program kegiatan Dit Reskrimsus; dan
 - e. perencanaan operasi, penyiapan administrasi operasi, dan pelaksanaan Anev operasi.

- (3) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1) Bagbin opsional dibantu oleh:
- a. Subbagian Administrasi Operasional (Subbagminops), yang bertugas menyelenggarakan pelatihan fungsi, pengarsipan berkas perkara, dan pengadministrasian kegiatan penyelidikan dan penyidikan; dan
 - b. Subbagian Analisa dan Evaluasi (Subbaganev), yang bertugas menganalisis dan mengevaluasi kegiatan Dit Reskrimsus, serta mengumpulkan dan mengolah data, serta menyajikan informasi dan dokumentasi.
- C. KABAG WASSIDIK**
- (1) Bagwassidik sebagaimana dimaksud dalam Pasal 141 huruf c bertugas melakukan koordinasi dan pengawasan proses penyidikan tindak pidana di lingkungan Dit Reskrimsus, serta menindaklanjuti terhadap pengaduan masyarakat yang terkait dengan proses penyidikan.
- (2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Bagwassidik menyelenggarakan fungsi:
- a. Pengawasan pelaksanaan penyelidikan dan penyidikan tindak pidana yang dilakukan oleh Subdit pada Dit Reskrimsus;
 - b. Pelaksanaan supervisi, koreksi, dan asistensi kegiatan penyelidikan dan penyidikan tindak pidana;
 - c. Pengkajian efektivitas pelaksanaan penyelidikan dan penyidikan tindak pidana melalui penyelenggaraan gelar perkara;
 - d. Pemberian saran masukan kepada Dir Reskrimsus terkait dengan hasil pengawasan penyidikan, termasuk menjawab pengaduan masyarakat; dan
 - e. Pemberian bantuan penyelidikan dan penyidikan tindak pidana khusus yang dilakukan oleh penyidik pada Subdit Dit Reskrimsus dan PPNS.
- D. KASI KORWAS PPNS**
- (1) Sikorwas PPNS sebagaimana dimaksud dalam Pasal 141 huruf d bertugas melaksanakan koordinasi dan pengawasan penyidikan termasuk pemberian bimbingan teknis dan taktis serta bantuan konsultasi penyidikan kepada PPNS.
- (2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Sikorwas PPNS menyelenggarakan fungsi:
- a. Pengkoordinasian dan pengawasan penyidikan kepada PPNS di daerah hukum Polda;
 - b. Pemberian bimbingan teknis dan taktis penyidikan kepada PPNS; dan
 - c. Pemberian bantuan konsultasi penyidikan kepada PPNS.
- (3) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1) Sikorwas PPNS dibantu oleh:
- a. Subseksi Bantuan Penyidikan (Subsibansidik), bertugas memberikan bantuan konsultasi penyidikan kepada PPNS; dan
 - b. Subseksi Pembinaan Kemampuan (Subsibinpuan), bertugas memberikan pembinaan dan bimbingan teknis dan taktis kepada PPNS
- E. SUBDIT**
- (1) Subdit sebagaimana dimaksud dalam Pasal 141 huruf e bertugas melakukan penyelidikan dan penyidikan tindak pidana yang terjadi di daerah hukum Polda.
- (2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Subdit menyelenggarakan fungsi:
- a. Penyelidikan dan penyidikan tindak pidana yang terjadi di daerah hukum Polda;

- b. Pemberkasan dan penyelesaian berkas perkara sesuai dengan ketentuan administrasi penyelidikan dan penyidikan tindak pidana; dan
 - c. Penerapan manajemen anggaran, serta manajemen penyelidikan dan penyidikan tindak pidana.
- (3) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Subdit dibantu oleh sejumlah Unit, yang bertugas membantu pelaksanaan tugas dan fungsi Subdit.

B. Metode Penelitian

Metode pengumpulan data ialah teknik atau cara-cara yang dapat digunakan oleh peneliti untuk mengumpulkan data. Metode (cara atau teknik) menunjuk suatu kata yang abstrak dan tidak diwujudkan dalam benda, tetapi hanya dapat dilihat penggunaannya melalui: *angket, wawancara, pengamatan, ujian (tes), dokumentasi, dan lainnya*. Peneliti dapat menggunakan salah satu atau gabungan tergantung dari masalah yang dihadapi.

Instrumen pengumpulan data adalah alat bantu yang dipilih dan digunakan oleh peneliti dalam kegiatannya mengumpulkan agar kegiatan tersebut menjadi sistematis dan dipermudah olehnya (Suharsimi Arikunto, 1995:134). Selanjutnya instrument yang diartikan sebagai alat bantu merupakan saran yang dapat diwujudkan dalam benda, contohnya: angket (*questionnaire*), pedoman wawancara (*interview guide* atau *interview scheduled*) dan sebagainya.

C. Teknik Pengumpulan Data

1). Observasi

Observasi dilakukan dg cara melakukan pengamatan langsung ke Dit Reskrimsus Polda Bengkulu untuk melihat bagaimana sistem yang sedang berjalan, dari hasil pengamatan penulis maka penulis menyimpulkan perlu adanya perancangan sebuah sistem pengamanan data yang lebih baik lagi.

2). Studi Pustaka

Studi pustaka dilakukan dengan mengumpulkan buku-buku referensi, materi kuliah, diktat, jurnal, artikel-

artikel dari internet serta sumber informasi lainnya yang berkaitan dengan penelitian. Tujuan yang ingin diperoleh dari pengumpulan teori-teori dan prinsip-prinsip yang ada adalah untuk dapat diterapkan dalam pelaksanaan penelitian sehingga dapat menunjang dalam melakukan pemecahan masalah atas masalah yang dihadapi

C. Perangkat Lunak dan Perangkat Keras

Dalam melakukan pemilihan kebutuhan perangkat lunak dan perangkat keras perlu mempertimbangkan beberapa hal sebagai berikut :

- a. Dalam pengadaan hardware dan software harus memperhatikan kebutuhan system sekarang dan akan datang
- b. Dalam pengembangan system pendukung keputusan ini perlu adanya pertimbangan biaya yang minimal dan tetap mendapat hasil optimal

Adapun kebutuhan hardware dan software dapat dikriteriakan sebagai berikut

1. Software (perangkat lunak)
Aplikasi software yang di gunakan yaitu :
 - a. Microsoft Visual Basic 6.0
 - b. Microsoft Access 2007
 - c. Windows XP professional SP 2
 - d. Microsoft Visio 2007
2. Hardware (perangkat keras)
Hardware yang di gunakan adalah sebagai berikut :
 - a. Processor Pentium core i3 3,07 Ghz
 - b. Hardisk 250 Giga byte
 - c. Memory ddr 3 4 Gb
 - d. DVD RW Acer Super multi
 - e. Monitor Panasonic Viera lcd 24"
 - f. Keyboard
 - g. Mouse
 - h. Printer
 - i. UPS (Uninterup Power Supply)
 - j. VGA Ati Radeon Hdd 4690 1 Gb
 - k. PSU Seasonic bronze 512 watt

D. Metode Perancangan Sistem

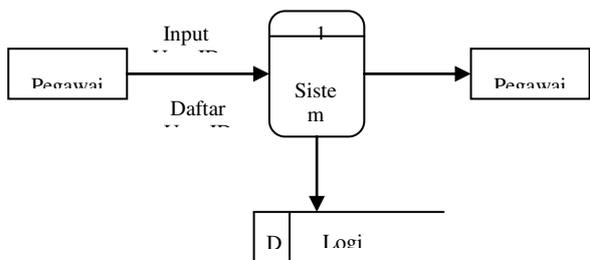
Perancangan Sistem merupakan tahapan untuk menentukan kebutuhan sistem baru yang akan dibuat sehingga menjadi sebuah sistem yang dapat digunakan sesuai dengan tujuan penelitian.

Tahap ini meliputi perancangan diagram konteks, diagram alir data. Perancangan sistem ini sebagai langkah awal untuk pembuatan sistem terkomputerisasi untuk menjawab problema-problema pengamanan data.

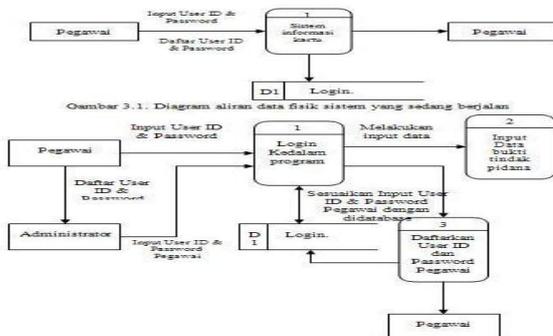
E. Analisis Sistem Aktual

Analisa sistem yang sedang berjalan pada sebuah program pendataan barang bukti kejahatan pada Polda Bengkulu menunjukkan bahwasanya dalam akses keamanan dalam program pendataan barang bukti tindak pidana tersebut sangat tidak terjamin dan semua pengguna ataupun orang lain dapat menggunakan program tersebut sehingga yang nantinya akan mengakibatkan kesalahan data dan kerusakan dalam program kerja dimana laporan-laporan yang akan dihasilkan tidak sesuai dengan fakta yang terjadi di lapangan.

Dari hasil penganalisaan penulis, titik kelemahan dari program pendataan bukti tindak pidana tersebut adalah pada menu login. Pada menu login terlihat user name dan passwordnya tidak terenkripsi sehingga memudahkan orang yang tidak bertanggung jawab mudah masuk menggunakan user name dan password untuk melakukan hal-hal yang merusak kinerja sistem pendataan.



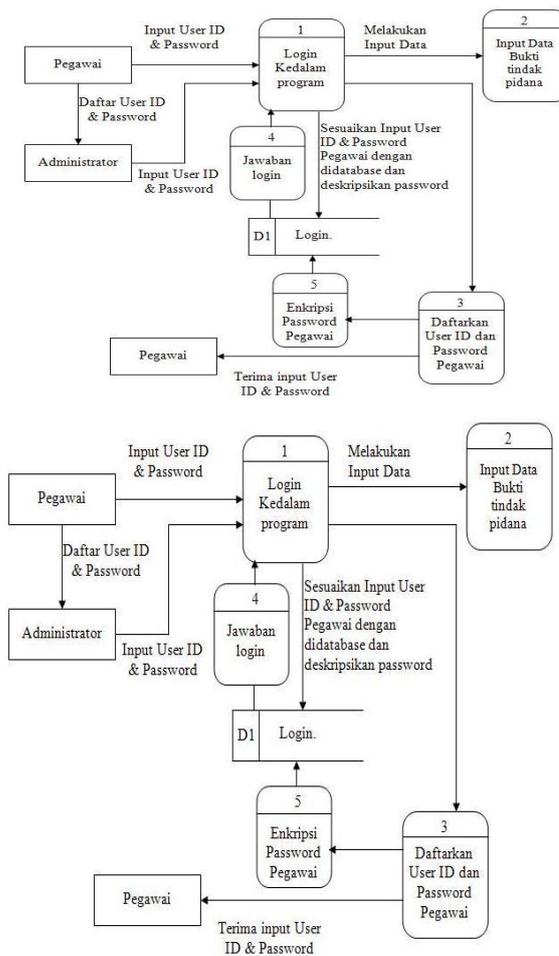
Gambar 3.2. Diagram alir data fisik sistem yang sedang berjalan



Gambar 3.3. DFD sistem yang berjalan

C. Analisa Sistem

Karena lemahnya sistem keamanan dan kerahasiaan data setelah penulis analisis pada sistem yang sedang berjalan, maka sehingga perlu dikembangkan lagi bentuk keamanan dan kerahasiaan data dengan melakukan pengenkripsian menu password tersebut sehingga orang dapat tidak dapat melakukan login dengan menggunakan user id dan password yang terdaftar karena walaupun orang tersebut dapat menembus dan masuk kedalam database login tetapi ketika orang yang dapat menembus database login program ini tetapi dia tidak akan menemukan password dari user-user id dan hanya akan terlihat user id saja karena isi dari passwordnya telah berubah bentuk karena telah terenkripsi pada saat melakukan pendaftaran user id dan password. Bentuk pengenkripsian otomatis pada saat pendaftaran user id dan password pertama sekali.



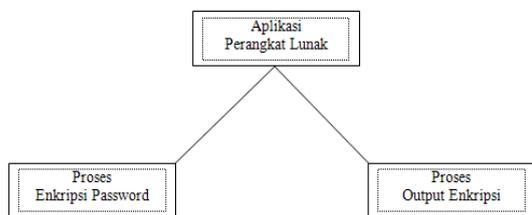
Gambar 3.4. DFD logis sistem diusulkan

Terlihat pada gambar diatas setiap pengguna yang akan melakukan kegiatan menggunakan sistem pendataan bukti tindak pidana harus melakukan input user id dan password. Setelah user id dan password program otomatis akan mengecek apakah user id dan password terdapat didalam database dan mencocokkannya. Saat pengguna selesai mengisi user id dan password dan mengenter ok otomatis program akan mendeskripsikan password didalam database. Jika user id dan password cocok maka pengguna dapat menggunakan program sistem informasi kartu dan jika tidak cocok maka pengguna diharuskan mengulang pengisian user id dan password.

Dan bagi pengguna yang belum memiliki user id dan password harus menghubungi super admin atau meminta kepada yang sudah memiliki user id dan password untuk mendaftarkan user id dan passwordnya kedalam database.

Untuk mendaftar dan mengubah password digunakan menu user account. Pada saat pendaftaran user id dan password program otomatis akan mengenkripsikan password kedalam bentuk enkripsi didalam database login.

F. HIPO



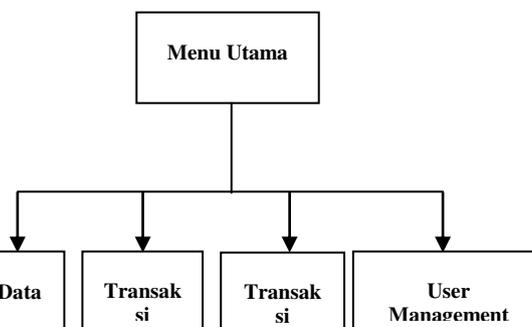
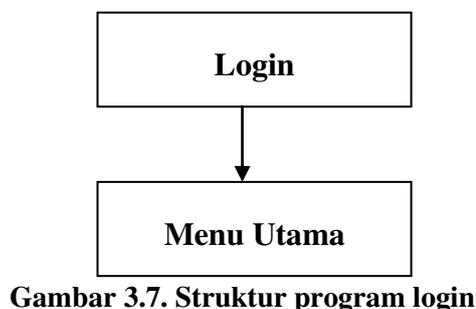
Gambar 3.5 HIPO

G.Perancangan Program Enkripsi

Perancangan program enkripsi ini digunakan untuk membantu pengamanan database login pada program sistem pendataan bukti tindak pidana.

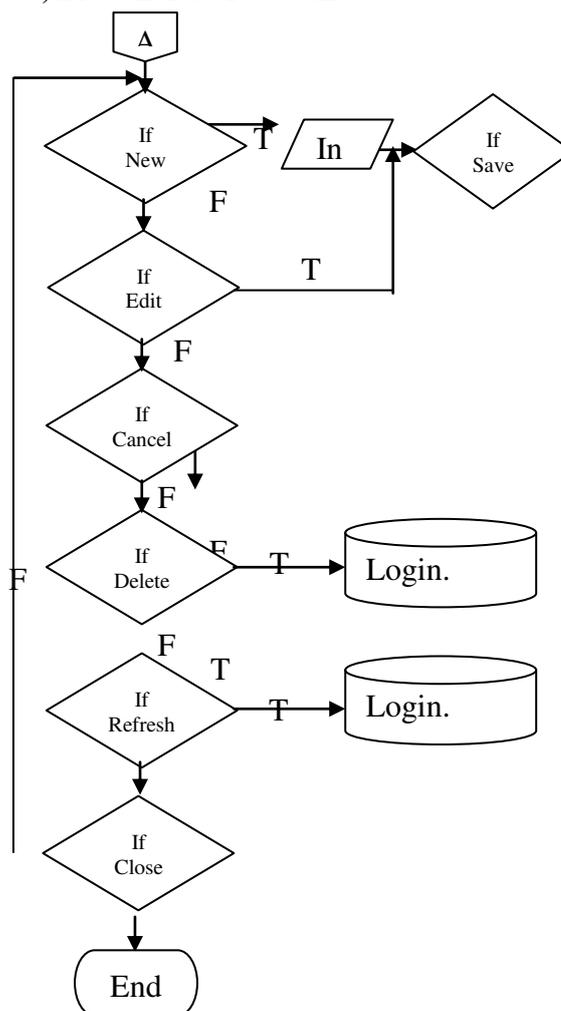
1).Perancangan Struktur Program

Adapun struktur program dari program sistem pendataan bukti tindak pidana adalah sebagai berikut :



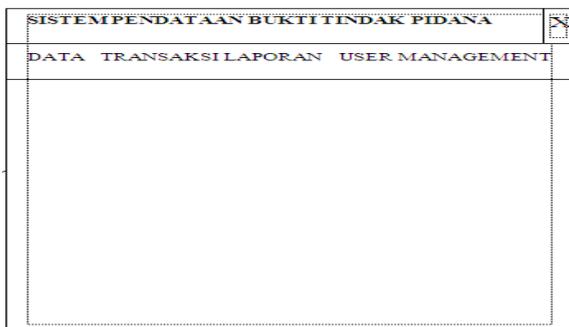
Gambar 3.7. Struktur program login
Gambar 3.8. Struktur program menu utama sistem Informasi bukti pidana

5).Flowchar user account



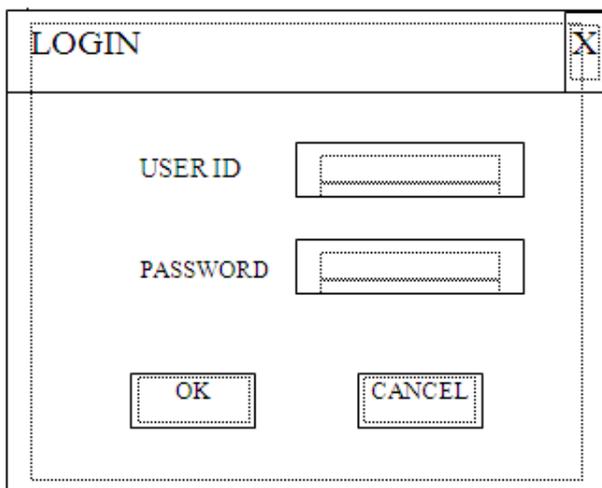
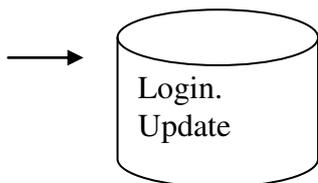
Gambar 3.13. Flowchart user account

6).Perancangan Form



Gambar 3.14. Perancangan form login

Sebelum masuk kedalam program terdapat menu yang pertama yaitu menu login. Jadi setiap pengguna yang akan menggunakan program sistem pendataan bukti tindak pidana ini harus melakukan login. Dalam menu login ini pengguna harus mengisi user id dan password.



Gambar 3.15. Perancangan menu utama sistem pendataan bukti kejahatan

IV.HASIL DAN PEMBAHASAN

A. Hasil dan Pembahasan Program

Aplikasi Implementasi Pengamanan Basis Data Password Login Dengan

Teknik Enkripsi Pada Polda Bengkulu,diberi nama file EnkripsiPasswordLogin.vbp Dimana program ini dapat di aktifkan melalui file aplikasi yang berbentuk Exe. Sedangkan source programnya baru dapat diaktifkan apabila pada sistem komputer telah terpasang Microsoft Visual Basic 6.0.

Apabila Program tersebut diaktifkan, maka pada layar akan terlihat tampilan seperti terlihat pada gambar 4.1 berikut :



Gambar 4.1. Tampilan Login Program

Setelah benar memasukan Nama Penggunaan Password pada login program, maka selanjutnya program akan menampilkan tampilan menu utama seperti gambar 4.2 berikut:



Gambar 4.2. Tampilan Menu Utama

Berdasarkan gambar 4.2. di atas dapat diamati bahwa pada menu utama terdapat 4 (Empat) macam pilihan (Submenu), yakni Submenu File, Sub Menu Barang Bukti Submenu Laporan dan Submenu Keluar.

Submenu Input Data terdiri dari 5 (Lima) pilihan lanjutan (Sub-sub menu), yaitu: Sub-submenu Input Data Tambah Admin, Data Korban Kejahatan, Data Saksi Kejahatan, Data Pelaku Kejahatan, dan Exit seperti terlihat pada gambar 4.3. berikut :



Gambar 4.3. Tampilan Sub Menu File

Masing-masing sub menu File tersebut disediakan dengan tujuan untuk memberikan informasi dan pengolahan data Kejahatan.

Sub menu Data Barang Bukti tersebut disediakan untuk memberikan informasi tentang data barang bukti kejahatan.

Sub menu Laporan disediakan dengan tujuan untuk melayani pencetakan hasil persediaan barang, yakni: Laporan Korban Kejahatan, Laporan Saksi Kejahatan, Laporan Pelaku Kejahatan dan Laporan Barang Bukti seperti terlihat panjualan gambar 4.4. berikut:



Gambar 4.4 Tampilan Sub Menu Laporan

Sedangkan sub menu Keluar disediakan untuk melayani pengguna apabila menginginkan keluar dari program, yang mana sub menu ini bersifat tambahan saja, karena untuk menutup program dapat juga melalui fasilitas Windows yang telah ada yakni Close atau dengan shortcut-key (Alt+F4).

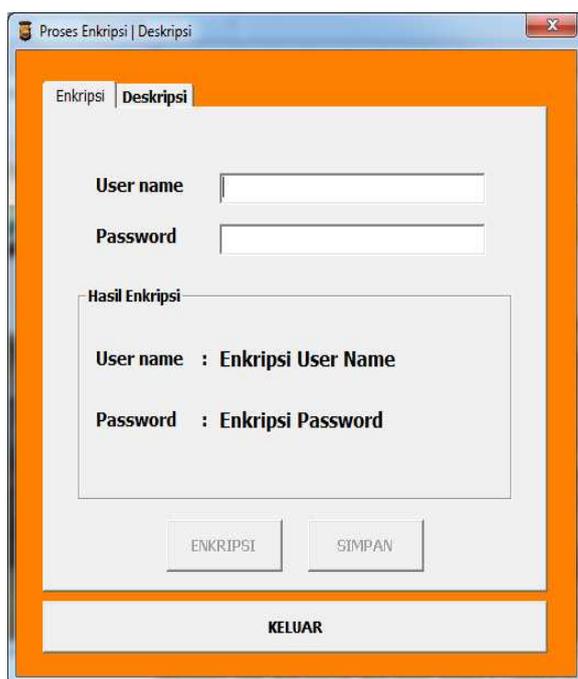
Beikut ini akan diuraikan lebih lanjut dan rinci dari masing-masing submenu sesuai dengan kepentingannya bertujuan untuk mempertegas proses pemakaian program yang sekaligus merupakan panduan penggunaan.

1). Sub Menu Input Data

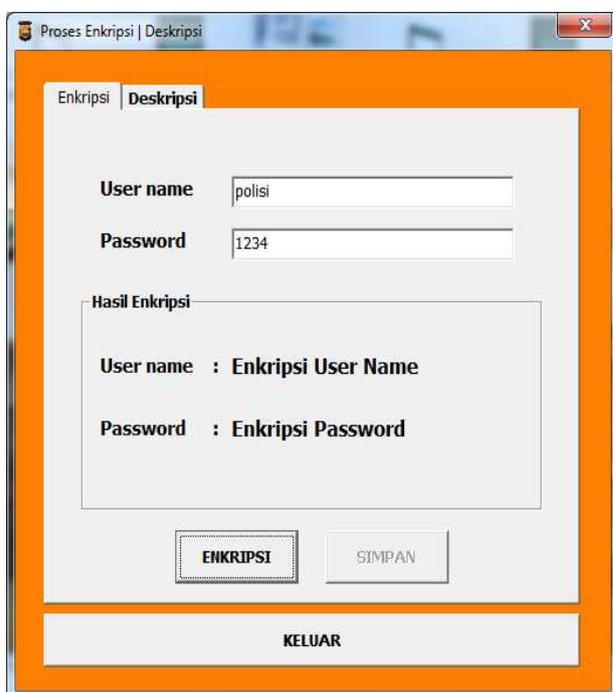
Sub menu Input Data disediakan untuk melayani pengelolaan terhadap data yang akan dikerjakan. Dimana sub menu input data ini memiliki 5 (lima) macam pilihan, yakni Sub-sub menu Input Data Tambah Admin, Data Korban Kejahatan, Data Saksi Kejahatan, Data Pelaku Kejahatan, dan Exit, berikut ini akan dibahas masing-masing pilihan, yaitu :

- a. Input Data Tambah Admin
 Berfungsi untuk menambah data admin dan proses enkripsi dan deskripsi login password, dari Menu Utama diklik Input Data dan dilanjutkan dengan mengklik Tambah Admin, maka program akan

memberikan tampilan program seperti gambar 4.5 berikut :

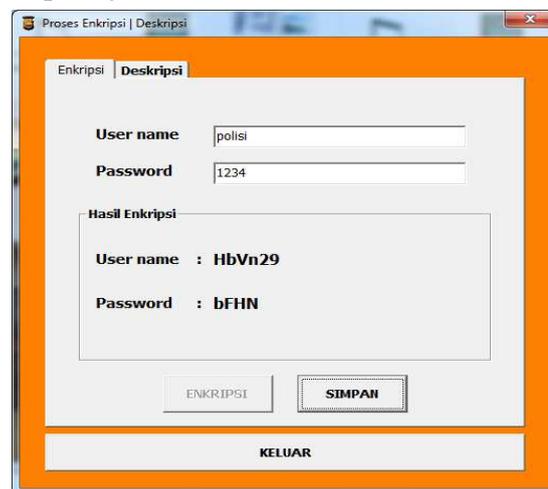


Proses Enkripsi Password Login dapat dilakukan dengan mengisi Username dan Password yang ingin di Enkripsikan seperti gambar 4.6 berikut ini.



Gambar 4.6 Proses Pengisian data Enkripsi

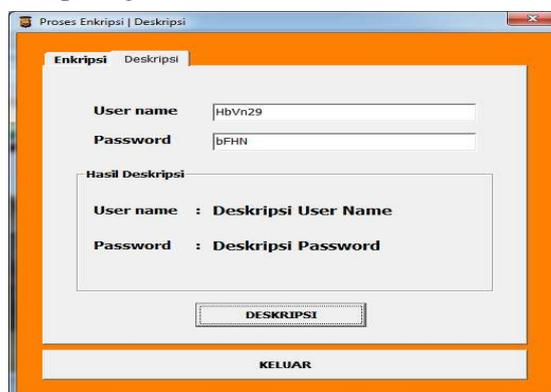
Berdasarkan gambar 4.6 diatas, setelah proses pengisian username dan password dianggap selesai maka dengan menekan tombol enter pada keyboard maka status tombol Enkripsi yang sebelumnya tidak aktif menjadi aktif dan apabila tombol enkripsi diklik maka hasil enkripsi pada Username dan Password akan terenkripsi seperti gambar 4.7 berikut:



Gambar 4.7. Tampilan Hasil Enkripsi

Setelah hasil enkripsi didapat maka status tombol simpan akan menjadi aktif. Selanjutnya dengan mengklik tombol Simpan pada gambar 4.7 diatas maka data Username dan password yang telah dienkripsikan tersebut telah berhasil disimpan ke dalam database.

Proses Deskripsi Password Login
Proses Deskripsi Password Login dapat dilakukan dengan mengisi Username dan Password Yang ingin di Deskripsikan seperti gambar 4.8 berikut ini.



Gambar 4.8 Proses Pengisian Deskripsi

Berdasarkan gambar 4.8 diatas, setelah proses pengisian username dan password

dianggap selesai maka dengan menekan tombol enter pada keyboard maka status tombol Deskripsi yang sebelumnya tidak aktif menjadi aktif dan apabila tombol Deskripsi diklik maka hasil deskripsi pada Username dan Password akan terdeskripsi dan akan menghasilkan data yang sama dengan data pada proses enkripsi seperti gambar 4.9 berikut:

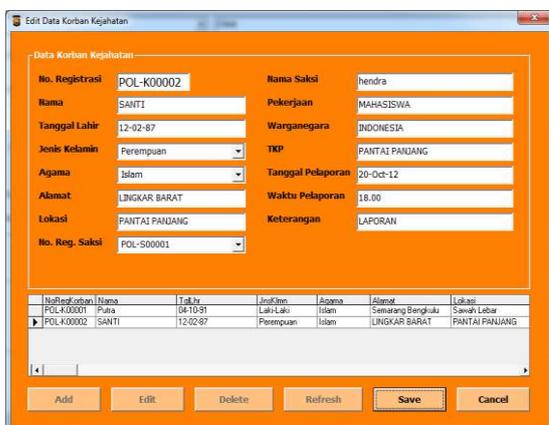


2).Hasil Deskripsi

Berdasarkan hasil deskripsi pada gambar 4.9 diatas membuktikan bahwa hasil deskripsi dan enkripsi tersebut benar.

Data Korban Kejahatan

Untuk menampilkan Data Korban Kejahatan, dari Menu Utama diklik File selanjutnya dengan meng-klik Data Korban Kejahatan maka program akan memberikan tampilan program seperti gambar 4.10 berikut :



Gambar 4.10. Tampilan Data Korban Kejahatan

Berdasarkan gambar 4.10 di atas, dapat dijelaskan bahwa Data Korban Kejahatan berfungsi sebagai tatap muka yang berguna untuk melakukan penambahan data, perbaikan data, dan penghapusan data Korban Kejahatan.

AddData Korban Kejahatan

Untuk melakukan penambahan atau pengisian data baru, dari Data Korban Kejahatan tersebut diklik tombol Tambah dan selanjutnya program akan menampilkan layar seperti gambar 4.11 berikut :



Gambar 4.11 AddData Korban Kejahatan

Pada gambar 4.11. di atas, setelah tombol Tambah diklik, maka status beberapa tombol Add, Edit, Delete, Refresh, Save menjadi tidak aktif. Sedangkan tombol Cancel yang sebelumnya tidak aktif menjadi aktif dengan maksud apabila pengguna ingin mencancel pengisian data.

Setelah mengklik tombol tambah maka secara langsung no registrasi korban akan terisi.

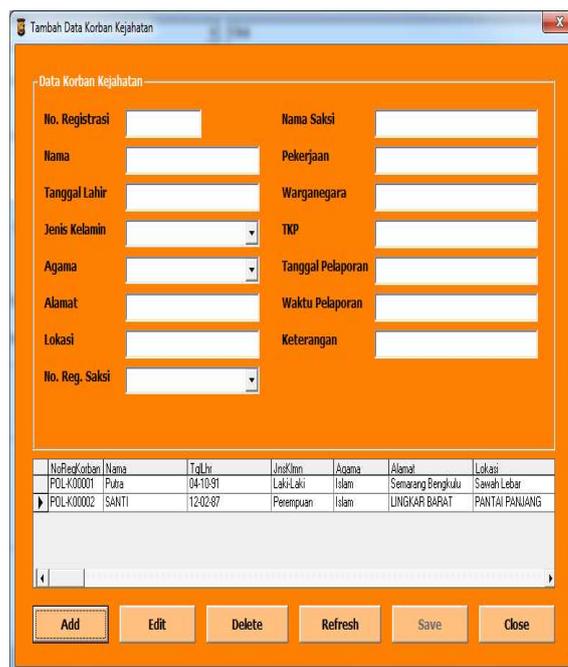
Kemudian setfocus program akan berpindah ke Nama korban, setelah proses pengisian nama selesai maka pengguna diminta untuk mengisi tanggal lahir jenis kelamin, agama, alamat, lokasi, no. registrasi saksi, nama saksi, pekerjaan, warganegara, TKP, tanggal pelaporan, waktu pelaporan, dan Keterangan.

Selanjutnya pengguna diminta menekan tombol Enter untuk mengaktifkan tombol Simpan seperti terlihat pada gambar 4.12 berikut :



Gambar 4.12 Pengisian Data Korban Kejahatan

Berdasarkan gambar 4.12 di atas, apabila tombol Save diklik maka program akan menyimpan seluruh isi data yang telah diisi ke dalam database dan hasilnya terlihat pada DataGridView yang telah bertambah isinya dan tampilan kembali seperti semula seperti terlihat pada gambar 4.13 berikut:

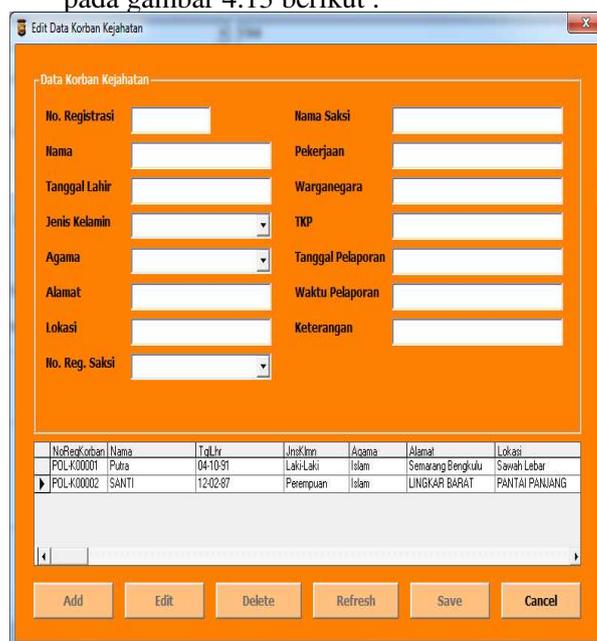


Gambar 4.12 Tampilan Data Korban

Kejahatan Yang Telah diisi

1. Edit Data Korban Kejahatan

Berfungsi Untuk dapat melakukan perbaikan terhadap data yang telah tersimpan dalam database, maka dari Data Korban Kejahatan seperti pada gambar 4.12 di atas diklik tombol Edit maka program akan menampilkan seperti terlihat pada gambar 4.13 berikut :



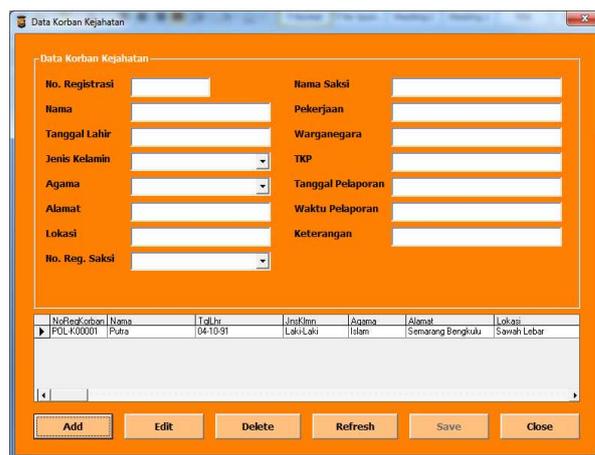
Gambar 4.13 Tampilan Edit Data Korban Kejahatan

Berdasarkan gambar 4.13 di atas, terlihat bahwa untuk melakukan perbaikan terhadap data dilakukan dengan cara menyetik No. Registrasi Korban yang ingin di Edit. Kemudian program akan membandingkan No. Registrasi tersebut dengan data No.Registrasi pada database, jika ditemukan maka ditampilkan isi data lengkapnya. Apabila No. Registrasi yang dipilih tidak ditemukan, kemudian program akan menampilkan pesan data tidak ditemukan, sedangkan apabila ditemukan, program menampilkan ke layar sebagaimana terlihat pada tampilan gambar 4.14 sebagai berikut :



Gambar 4.14 Tampilan Data Korban Kejahatan yang akan diedit

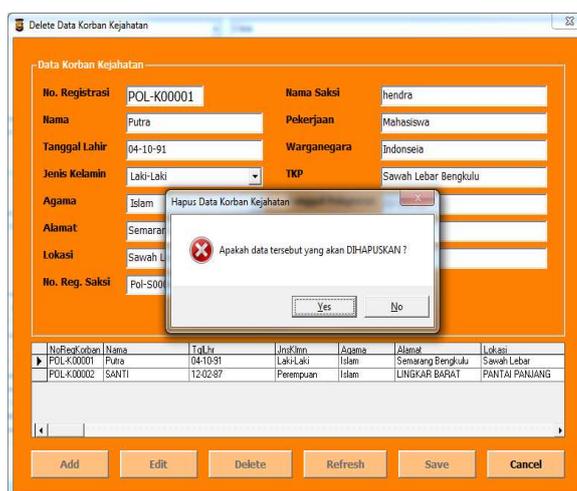
Dari gambar 4.14 di atas, diklik tombol Yes maka program selanjutnya meminta pengguna untuk mengisikan data Korban kejahatan yang lebih benar seperti tampilan gambar 4.15 berikut:



Gambar 4.15 Proses Edit Data Korban Kejahatan

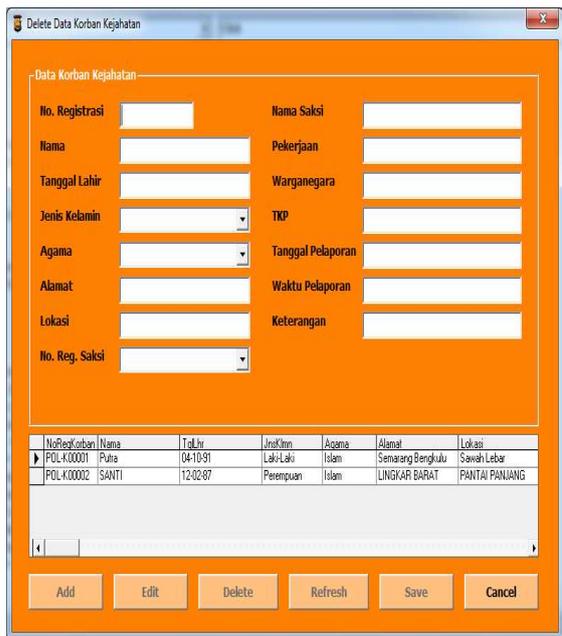
Setelah tombol Simpan pada gambar 4.15 di atas diklik, maka data terbaru dengan No. registrasi telah disimpan dan program kemudian kembali seperti tampilan gambar 4.12 setelah melakukan penyimpanan terhadap data yang telah diedit. Delete Data Korban Kejahatan

Berfungsi untuk dapat melakukan penghapusan terhadap data yang telah tersimpan dalam database. Apabila tombol Delete diklik maka program selanjutnya akan memberikan tampilan seperti terlihat pada gambar 4.16 berikut :



Gambar 4.16 Tampilan Delete Data Korban Kejahatan

Setelah No registrasi diisi dan selanjutnya menekan tombol enter, maka program akan memberikan tampilan seperti gambar 4.17 berikut

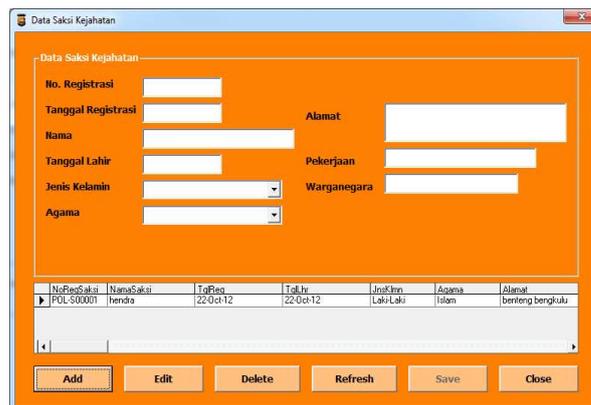
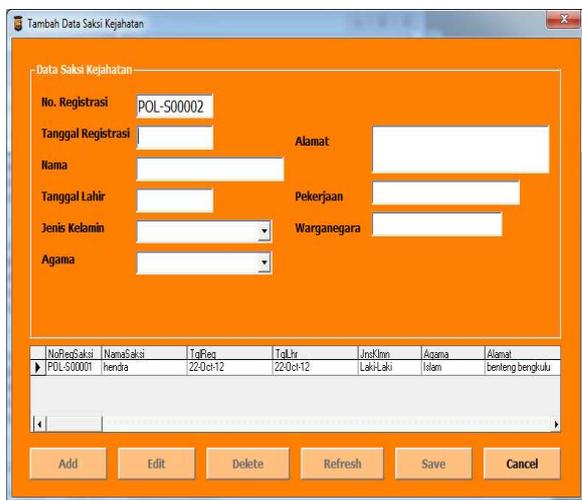


Gambar 4.17 Tampilan Proses delete Data Korban Kejahatan

Berdasarkan gambar 4.17 di atas, apabila tombol Yes diklik maka program selanjutnya akan menghapus data dengan No registrasi yang telah dipilih, baik pada data korban kejahatan maupun pada databasenya.

Refresh Data Korban Kejahatan
 Berfungsi untuk mereshfresh atau mengosongkan penginputan data korban kejahatan.

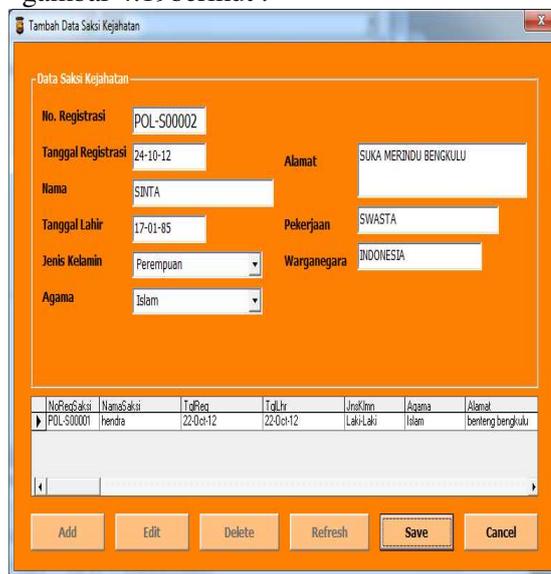
Data Saksi Kejahatan
 Untuk menampilkan Data Saksi Kejahatan, dari Menu Utama diklik File selanjutnya dengan meng-klik Data Saksi Kejahatan, maka program akan memberikan tampilan program seperti gambar 4.18berikut :



Gambar 4.18. Data Saksi Kejahatan

Berdasarkan gambar 4.18 di atas, dapat dijelaskan bahwa Data Saksi Kejahatan berfungsi sebagai tatap muka dengan tujuan untuk melakukan penambahan data, perbaikan data, dan penghapusan data Saksi Kejahatan.

Add Data Saksi Kejahatan
 Untuk melakukan penambahan atau pengisian data baru, dari Data Saksi Kejahatan tersebut diklik tombol Tambah dan selanjutnya program akan menampilkan layar seperti gambar 4.19berikut :

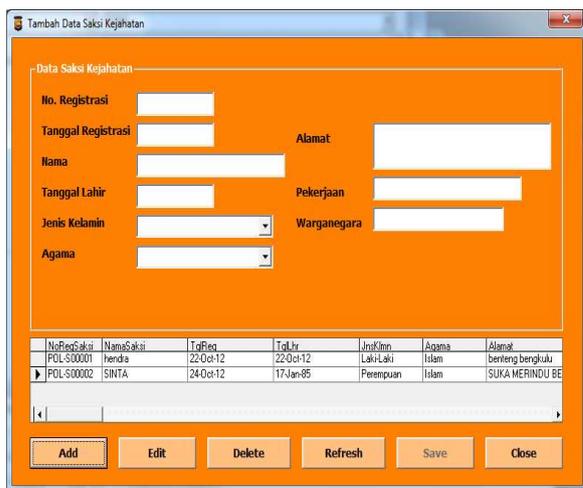


Gambar 4.19 Add Data Saksi Kejahatan

Pada gambar 4.19.di atas, setelah tombol Tambah diklik, maka status beberapa tombol Add, Edit, Delete, Refresh, Save menjadi tidak aktif. Sedangkan tombol Cancel yang sebelumnya tidak aktif menjadi aktif dengan

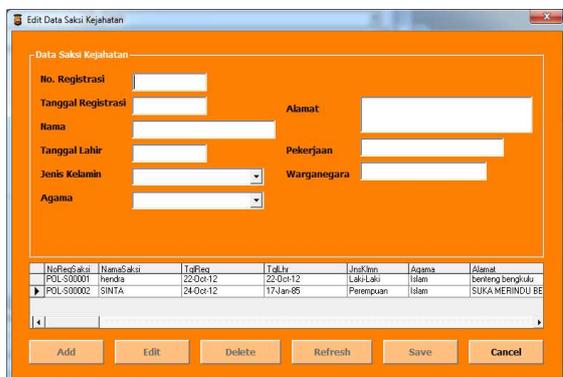
maksud apabila pengguna ingin mencancel pengisian data.

Setelah mengklik tombol tambah maka secara langsung no registrasi korban akan terisi. Kemudian setfocus program akan berpindah ke Tanggal registrasi, setelah proses pengisian Tanggal registrasi selesai maka pengguna diminta untuk mengisih Nama saksi, tanggal lahir jenis kelamin, agama, alamat, pekerjaan dan warganegara. Selanjutnya pengguna diminta menekan tombol Enter untuk mengaktifkan tombol Simpan seperti terlihat pada gambar 4.20berikut :



Gambar 4.20 Pengisian Data Saksi Kejahatan

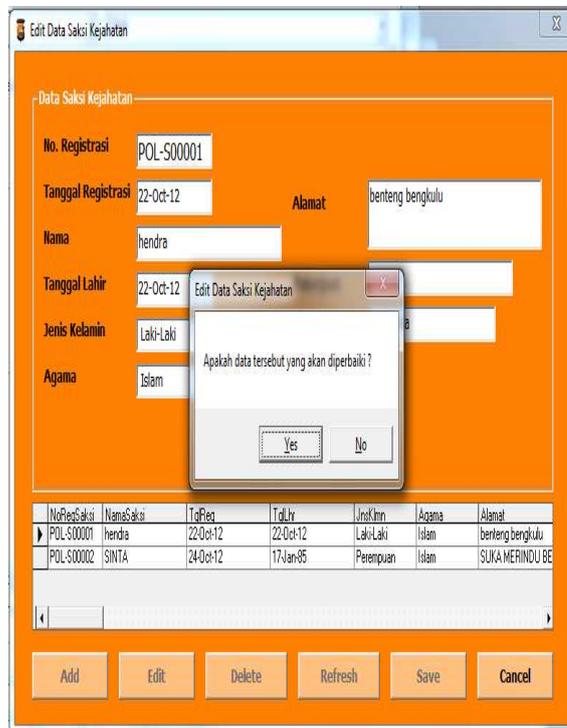
Berdasarkan gambar 4.20 di atas, apabila tombol Save diklik maka program akan menyimpan seluruh isi data yang telah diisi ke dalam database dan hasilnya terlihat pada DataGrid yang telah bertambah isinya dan tampilan kembali seperti semula seperti terlihat pada gambar 4.21 berikut:



Gambar 4.21 Tampilan Data Saksi Kejahatan Yang Telah diisi

Edit Data Saksi Kejahatan

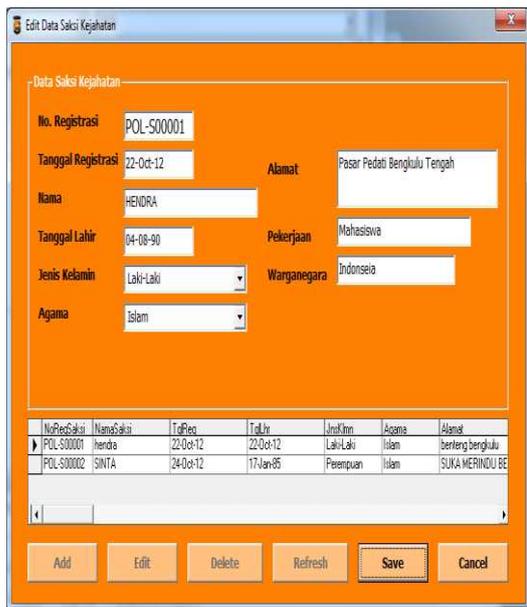
Berfungsi Untuk dapat melakukan perbaikan terhadap data yang telah tersimpan dalam database, maka dari Data Saksi Kejahatan seperti pada gambar 4.21 di atas diklik tombol Edit maka program akan menampilkan seperti terlihat pada gambar 4.22 berikut :



Gambar 4.22 Tampilan Edit Data Saksi Kejahatan

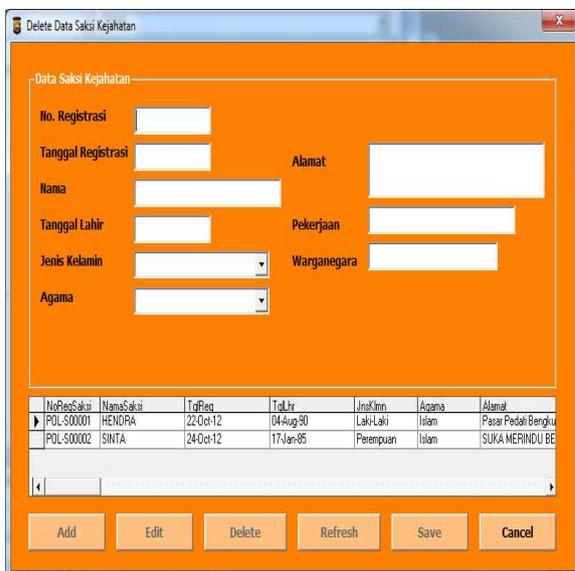
Berdasarkan gambar 4.22 di atas, terlihat bahwa untuk melakukan perbaikan terhadap data dilakukan dengan cara mengetik No. Registrasi Saksi yang ingin di Edit. Kemudian program akan membandingkan No. Registrasi tersebut dengan data No.Registrasi pada database, jika ditemukan maka ditampilkan isi data lengkapnya.

Apabila No. Registrasi yang dipilih tidak ditemukan, kemudian program akan menampilkan pesan data tidak ditemukan, sedangkan apabila ditemukan, program menampilkan ke layar sebagaimana terlihat pada tampilan gambar 4.23 sebagai berikut :



Gambar 4.23 Tampilan Data Saksi Kejahatan yang akan diedit

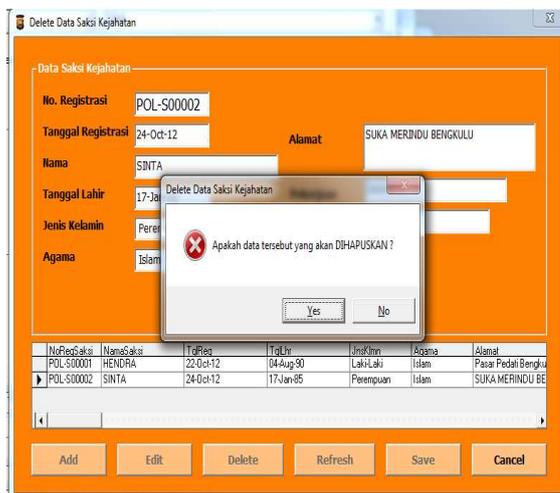
Dari gambar 4.23 di atas, diklik tombol Yes maka program selanjutnya meminta pengguna untuk mengisikan data Saksi kejahatan yang lebih benar seperti tampilan gambar 4.24berikut:



Gambar 4.23 Proses Edit Data Saksi Kejahatan

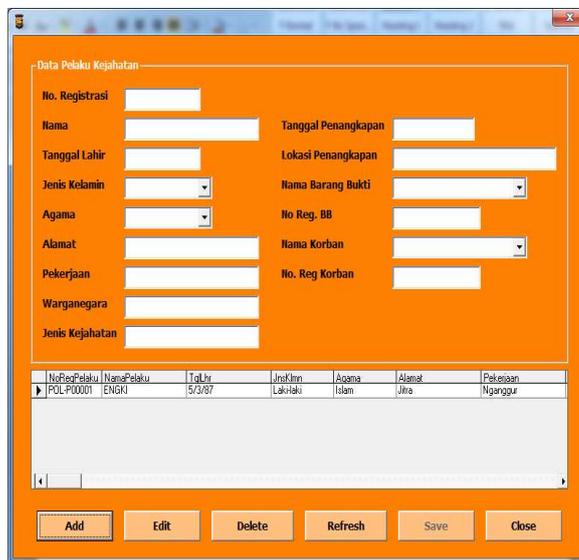
Setelah tombol Simpan pada gambar 4.24 di atas diklik, maka data terbaru dengan No. registrasi telah disimpan dan program kemudian kembali seperti tampilan gambar 4.21 setelah melakukan penyimpanan terhadap data yang telah diedit.

Delete Data Saksi Kejahatan Berfungsi untuk dapat melakukan penghapusan terhadap data yang telah tersimpan dalam database. Apabila tombol Delete diklik maka program selanjutnya akan memberikan tampilan seperti terlihat pada gambar 4.25berikut :



Gambar 4.25 Tampilan Delete Data Saksi Kejahatan

Setelah No registrasi diisi dan selanjutnya menekan tombol enter, maka program akan memberikan tampilan seperti gambar 4.26 berikut



Gambar 4.26 Tampilan Proses delete Data Saksi Kejahatan

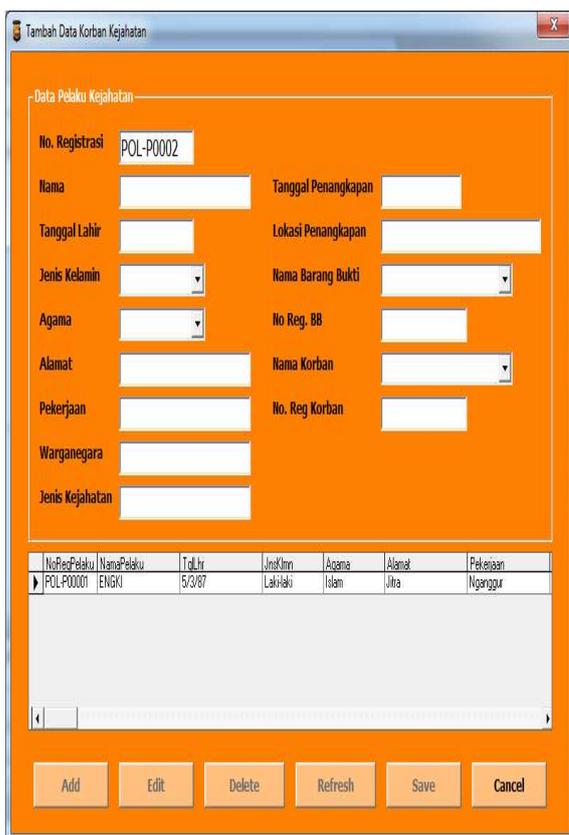
Berdasarkan gambar 4.26 di atas, apabila tombol Yes diklik maka program selanjutnya akan menghapus data dengan No registrasi yang telah dipilih, baik pada data Saksi Kejahatan maupun pada databasenya.

Refresh Data Saksi Kejahatan

Berfungsi untuk mererefresh atau mengosongkan penginputan data Saksi Kejahatan.

Data Pelaku Kejahatan

Untuk menampilkan Data Pelaku Kejahatan, dari Menu Utama diklik File selanjutnya dengan meng-klik Data Pelaku Kejahatan maka program akan memberikan tampilan program seperti gambar 4.27berikut :

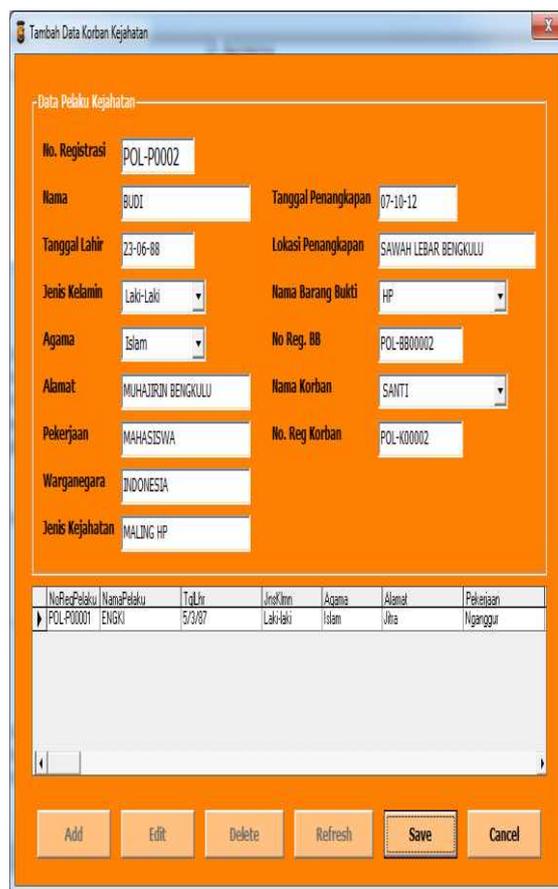


Gambar 4.27. Tampilan Data Pelaku Kejahatan

Berdasarkan gambar 4.27 di atas, dapat dijelaskan bahwa Data pelaku Kejahatan berfungsi sebagai tatap muka yang berguna untuk melakukan penambahan data, perbaikan data, dan penghapusan data pelaku Kejahatan.

Add Data Pelaku Kejahatan

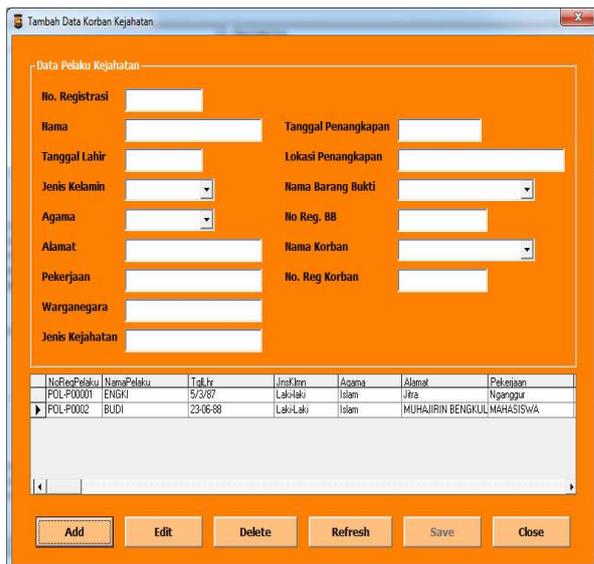
Untuk melakukan penambahan atau pengisian data baru, dari Data pelaku Kejahatan tersebut diklik tombol Tambah dan selanjutnya program akan menampilkan layar seperti gambar 4.28berikut :



Gambar 4.28 Add Data Pelaku Kejahatan

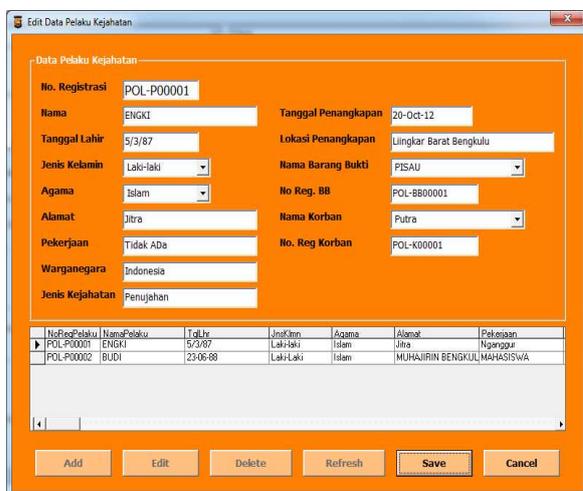
Pada gambar 4.28.di atas, setelah tombol Tambah diklik, maka status beberapa tombol Add, Edit, Delete, Refresh, Save menjadi tidak aktif. Sedangkan tombol Cancel yang sebelumnya tidak aktif menjadi aktif dengan maksud apabila pengguna ingin mengcancel pengisian data.

Setelah mengklik tombol tambah maka secara langsung no registrasi korban akan terisi. Kemudian setfocus program akan berpindah ke Nama korban, setelah proses pengisian nama selesai maka pengguna diminta untuk mengisih tanggal lahir jenis kelamin, agama, alamat, pekerjaan, warganegara, jenis kejahatan, tanggal penangkapan, lokasi penangkapan, nama barang bukti, no. registrasi barang bukti, nama korban, dan no. reg. korban kejahatan. Selanjutnya pengguna diminta menekan tombol Enter untuk mengaktifkan tombol Simpan seperti terlihat pada gambar 4.29berikut :



Gambar 4.29 Pengisian Data Pelaku Kejahatan

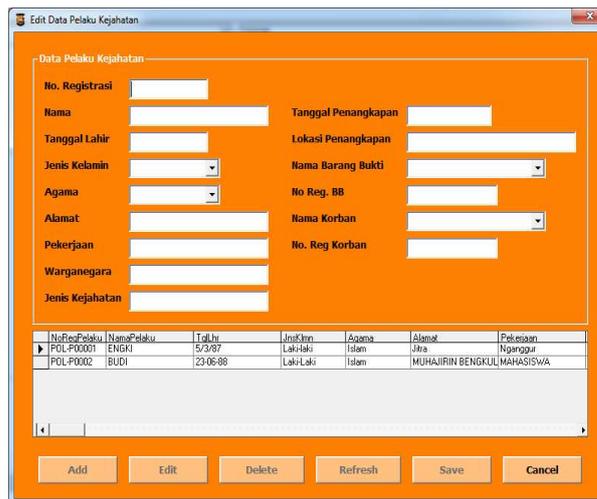
Berdasarkan gambar 4.29 di atas, apabila tombol Save diklik maka program akan menyimpan seluruh isi data yang telah diisi ke dalam database dan hasilnya terlihat pada DataGrid yang telah bertambah isinya dan tampilan kembali seperti semula seperti terlihat pada gambar 4.30 berikut:



Gambar 4.30 Tampilan Data Pelaku Kejahatan Yang Telah diisi

Edit Data Pelaku Kejahatan

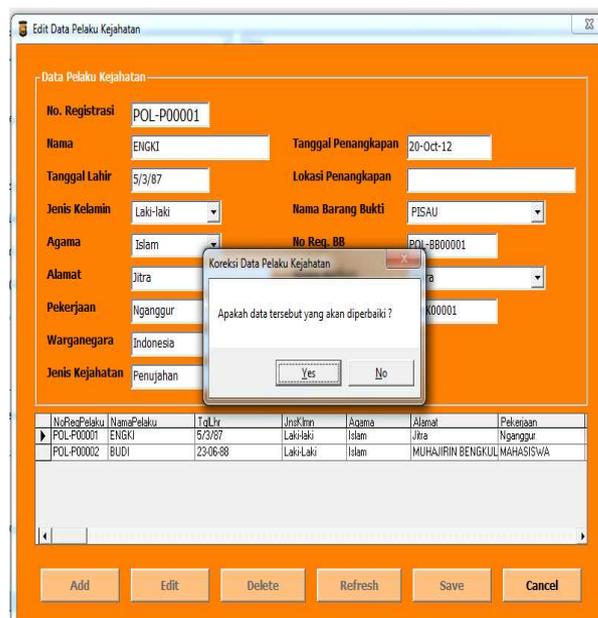
Berfungsi Untuk dapat melakukan perbaikan terhadap data yang telah tersimpan dalam database, maka dari Data Pelaku Kejahatan seperti pada gambar 4.30 di atas diklik tombol Edit maka program akan menampilkan seperti terlihat pada gambar 4.31 berikut :



Gambar 4.31 Tampilan Edit Data Pelaku Kejahatan

Berdasarkan gambar 4.31 di atas, terlihat bahwa untuk melakukan perbaikan terhadap data dilakukan dengan cara mengetik No. Registrasi Pelaku yang ingin di Edit. Kemudian program akan membandingkan No. Registrasi tersebut dengan data No.Registrasi pada database, jika ditemukan maka ditampilkan isi data lengkapnya.

Apabila No. Registrasi yang dipilih tidak ditemukan, kemudian program akan menampilkan pesan data tidak ditemukan, sedangkan apabila ditemukan, program menampilkan ke layar sebagaimana terlihat pada tampilan gambar 4.32 sebagai berikut :



Gambar 4.32 Tampilan Data pelaku Kejahatan yang akan diedit

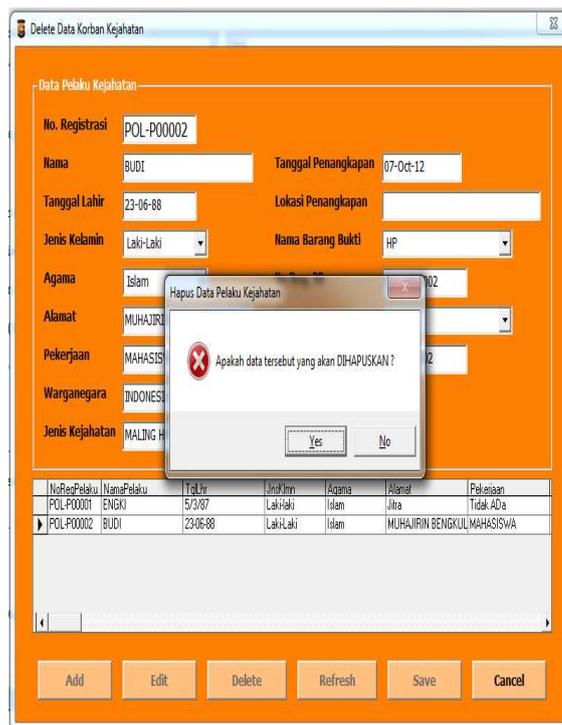
Dari gambar 4.32 di atas, diklik tombol Yes maka program selanjutnya meminta pengguna untuk mengisikan data Pelaku kejahatan yang lebih benar seperti tampilan gambar 4.33 berikut:



Gambar 4.33 Proses Edit Data pelaku Kejahatan

Setelah tombol Simpan pada gambar 4.33 di atas diklik, maka data terbaru dengan No. registrasi telah disimpan dan program kemudian kembali seperti tampilan gambar 4.30 setelah melakukan penyimpanan terhadap data yang telah diedit. Delete Data Pelaku Kejahatan

Berfungsi untuk dapat melakukan penghapusan terhadap data yang telah tersimpan dalam database. Apabila tombol Delete diklik maka program selanjutnya akan memberikan tampilan seperti terlihat pada gambar 4.34berikut :



Gambar 4.34 Tampilan Delete Data Pelaku Kejahatan

Setelah No registrasi diisi dan selanjutnya menekan tombol enter, maka program akan memberikan tampilan seperti gambar 4.35 berikut



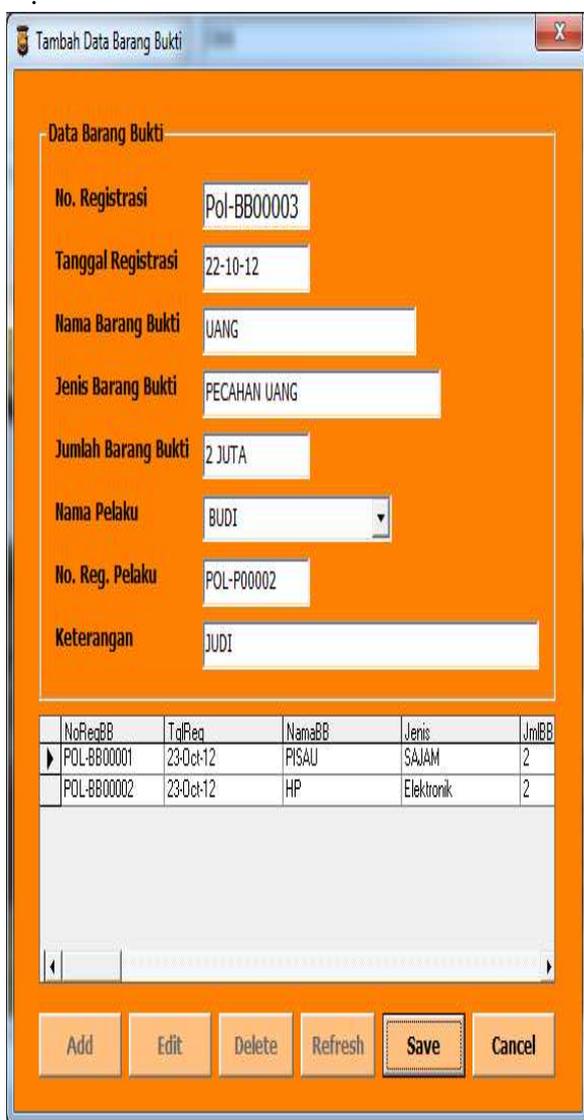
Gambar 4.35 Tampilan Proses delete Data Korban Kejahatan

Berdasarkan gambar 4.35 di atas, apabila tombol Yes diklik maka program selanjutnya akan menghapus data dengan No registrasi yang telah dipilih, baik pada pada data Pelaku kejahatan maupun pada databasenya.

Refresh Data Pelaku Kejahatan Berfungsi untuk merefresh atau mengosongkan penginputan data Pelaku kejahatan.

Sub Menu Data Barang Bukti

Berfungsi untuk menampilkan Data Barang Bukti, dari Menu Utama diklik Data Barang Bukti, maka program akan memberikan tampilan program seperti gambar 4.36berikut :



Gambar 4.36. Data Barang Bukti

Berdasarkan gambar 4.36 di atas, dapat dijelaskan bahwa Data Barang bukti berfungsi sebagai tatap muka dengan tujuan untuk melakukan penambahan data, perbaikan data, dan penghapusan data Barang Bukti.

Add Data Barang Bukti

Untuk melakukan penambahan atau pengisian data baru, dari Barang Bukti tersebut diklik tombol Tambah dan selanjutnya program akan menampilkan layar seperti gambar 4.37berikut :



Gambar 4.37 Add Data Barang Bukti

Pada gambar 4.37.di atas, setelah tombol Tambah diklik, maka status beberapa tombol Add, Edit, Delete, Refresh, Save menjadi tidak aktif. Sedangkan tombol Cancel yang sebelumnya tidak aktif menjadi aktif dengan maksud apabila pengguna ingin mencancel pengisian data.

Setelah mengklik tombol tambah maka secara langsung no registrasi Barang Bukti akan terisi. Kemudian setfocus program akan berpindah ke Tanggal registrasi, setelah proses pengisian Tanggal registrasi selesai maka pengguna diminta untuk mengisih Nama Barang Bukti, Jenis Barang Bukti, Jumlah Barang Bukti, Nama Pelaku, No. Registrasi Pelaku, dan keterangan.Selanjutnya pengguna diminta menekan tombol Enter

untuk mengaktifkan tombol Simpan seperti terlihat pada gambar 4.38 berikut :

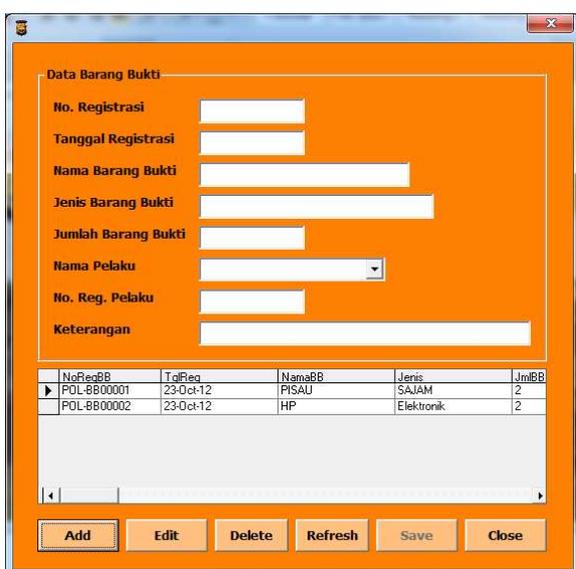


Gambar 4.38 Pengisian Data Barang Bukti

Berdasarkan gambar 4.38 di atas, apabila tombol Save diklik maka program akan menyimpan seluruh isi data yang telah diisi ke dalam database dan hasilnya terlihat pada DataGrid yang telah bertambah isinya dan tampilan kembali seperti semula seperti terlihat pada gambar 4.39 berikut:

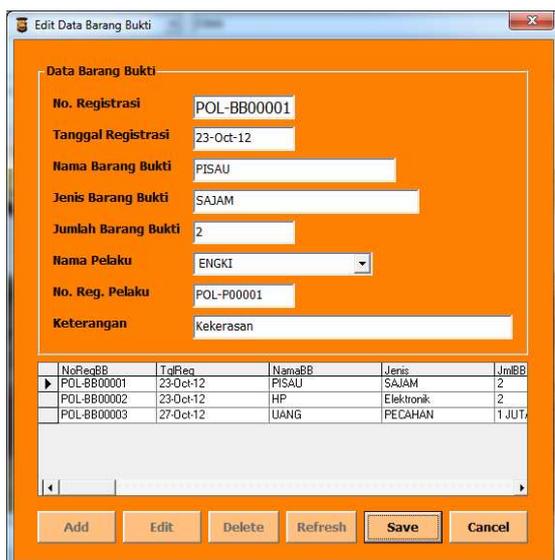


Gambar 4.39 Tampilan Data Barang Bukti Yang Telah diisi



Edit Data Barang Bukti

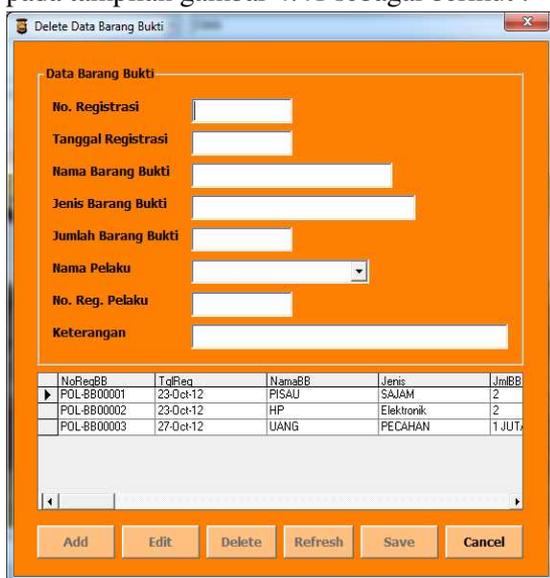
Berfungsi Untuk dapat melakukan perbaikan terhadap data yang telah tersimpan dalam database, maka dari Data Barang Bukti seperti pada gambar 4.39 di atas diklik tombol Edit maka program akan menampilkan seperti terlihat pada gambar 4.40 berikut :



Gambar 4.40 Tampilan Edit Data Barang Bukti

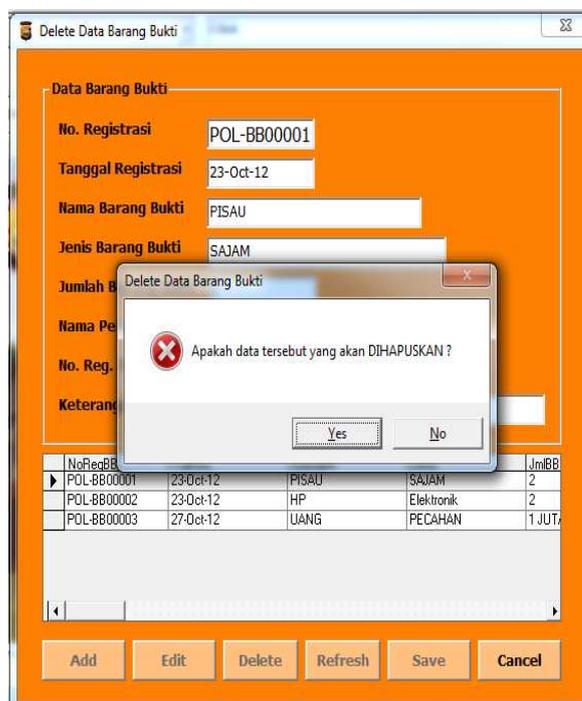
Berdasarkan gambar 4.40 di atas, terlihat bahwa untuk melakukan perbaikan terhadap data dilakukan dengan cara mengetik No. Registrasi yang ingin di Edit. Kemudian program akan membandingkan No. Registrasi tersebut dengan data No.Registrasi pada database, jika ditemukan maka ditampilkan isi data lengkapnya.

Apabila No. Registrasi yang dipilih tidak ditemukan, kemudian program akan menampilkan pesan data tidak ditemukan, sedangkan apabila ditemukan, program menampilkan ke layar sebagaimana terlihat pada tampilan gambar 4.41 sebagai berikut :



Gambar 4.41 Tampilan Data Barang Bukti yang akan diedit

Dari gambar 4.41 di atas, diklik tombol Yes maka program selanjutnya meminta pengguna untuk mengisikan data Barang Bukti yang lebih benar seperti tampilan gambar 4.42 berikut:



Gambar 4.42 Proses Edit Data Barang Bukti

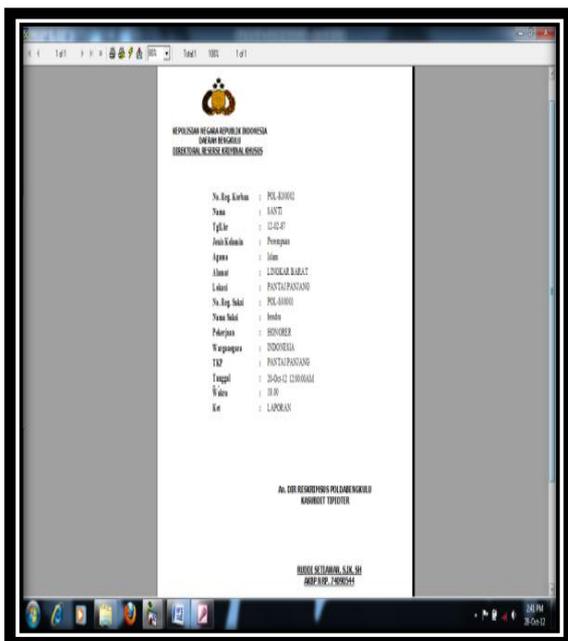
Setelah tombol Simpan pada gambar 4.42 di atas diklik, maka data terbaru dengan No. registrasi telah disimpan dan program kemudian kembali seperti tampilan gambar 4.39 setelah melakukan penyimpanan terhadap data yang telah diedit.

3).MenuLaporan

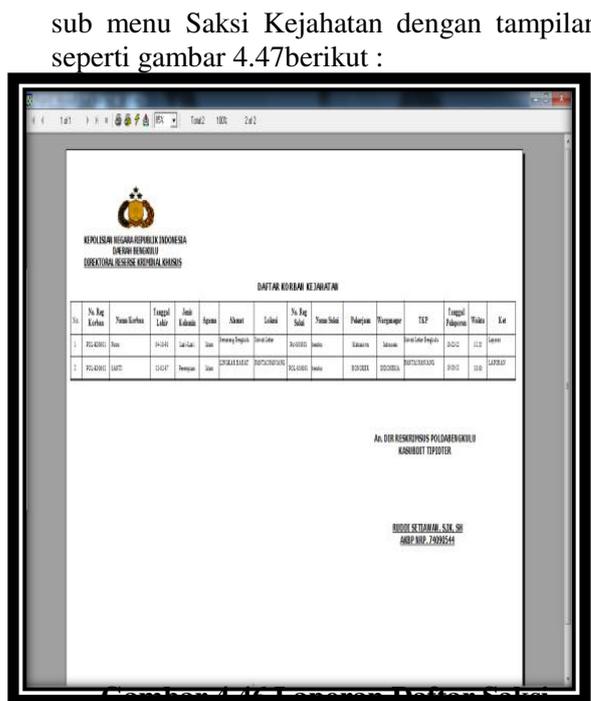
Seperti telah disinggung pada awal bab ini, submenuLaporan terdiri atas 4 (empat) buah pilihan sub-submenu, yakni sub menuLaporan Korban Kejahatan, Laporan Saksi Kejahatan, Laporan Pelaku Kejahatan dan Laporan Barang Bukti, yaitu :

Sub-sub Menu Laporan Korban Kejahatan

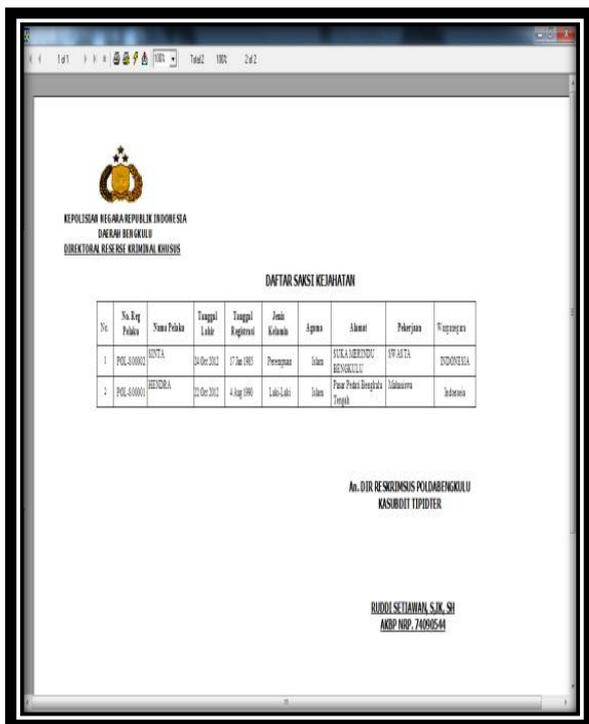
Berfungsi untuk dapat menampilkan Informasi Korban Kejahatan, dari menu utama pilih sub menuLaporan kemudian pilih sub-sub menu Korban Kejahatan, dengan tampilan seperti gambar 4.45berikut :



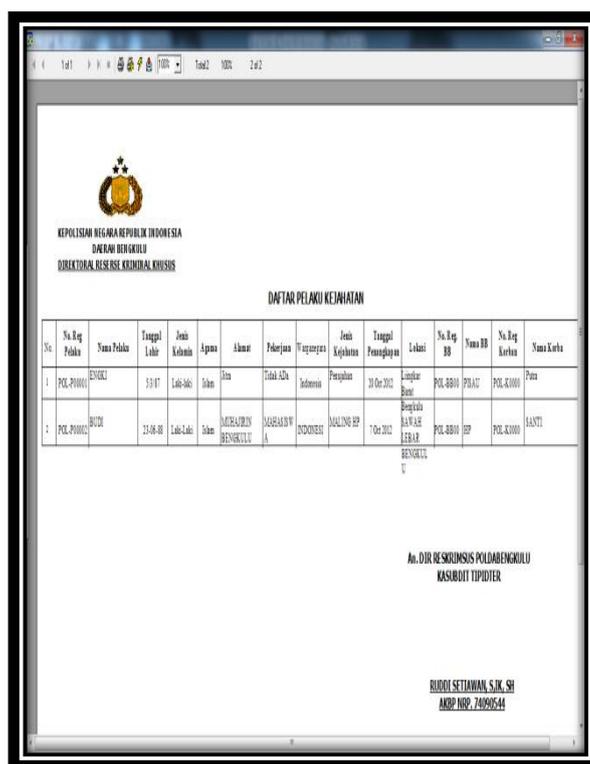
Gambar 4.45 Laporan Daftar Korban Kejahatan



Gambar 4.46 Laporan Daftar Saksi Kejahatan



Gambar 4.46 Laporan Data Korban Kejahatan

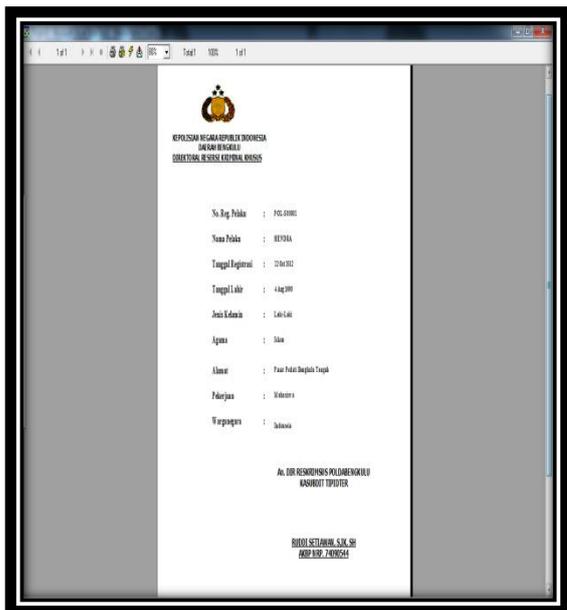


Gambar 4.47 Laporan Data Saksi Kejahatan

Sub-sub Menu Laporan Saksi Kejahatan Berfungsi untuk dapat menampilkan Informasi Saksi Kejahatan. Dari menu utama pilih sub menu laporan kemudian pilih sub-

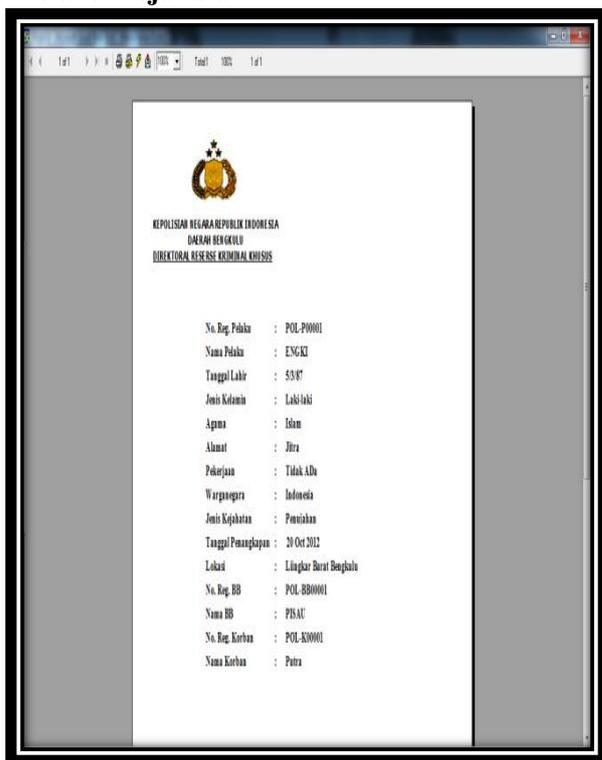
Sub-sub Menu Laporan Pelaku Kejahatan Berfungsi untuk dapat menampilkan Informasi Pelaku Kejahatan. Dari menu utama pilih sub menu laporan kemudian pilih

sub-sub menu Laporan Pelaku Kejahatandengan tampilan seperti gambar 4.48berikut :



Gambar 4.48.Lapoaran Daftar

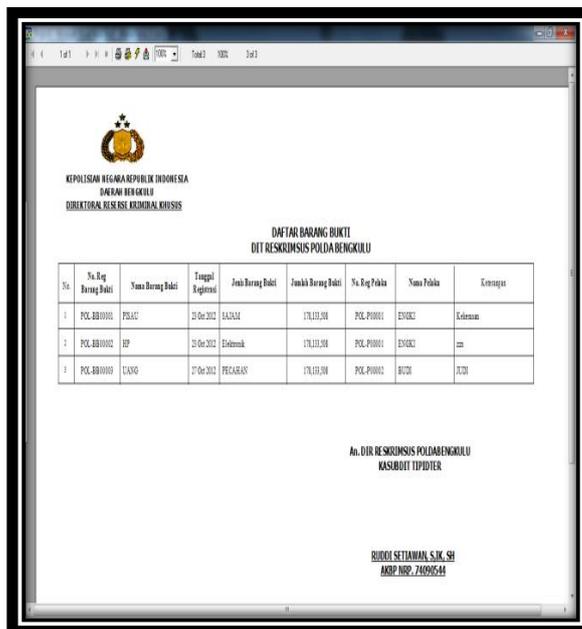
Pelaku Kejahatan



Gambar 4.49 laporan Data pelaku kejahatan

Sub-sub Menu Laporan Barang Bukti Berfungsi untuk dapat menampilkan Informasi Barang Bukti. Dari menu utama

pilih sub menu laporan kemudian pilih sub-sub menu Laporan Barang Bukti dengan tampilan seperti gambar 4.50berikut :



Gambar 4.50 Laporan Daftar Barang Bukti

MenuKeluar

Berfungsi untuk keluar dari program dan saat tombol keluar pada menu Keluar Apabila Ya diklik maka keluar dari aplikasi dan jika tombol No diklik maka batal keluar dari program danakan tampil seperti gambar 4.51 berikut;



Gambar 4.51 Tampilan keluar dari program

4).Pengujian Sistem

Proses pengujian sistem yang telah dibangun selanjutnya diimplementasi pada tempat penelitian dan diuji coba. Dalam proses implementasi yang dilakukan, program dipasang pada sistem operasi MS Windows dengan spesifikasi perangkat keras yang sesuai dengan terdahulu.

Pengujian sistem baru inidilaksanakan pada Polda Bengkulu. Proses pengimplementasian ini dilakukan langsung oleh Kausdit Tipidter Polda Bengkulu. Penulis juga menerangkan dan menjelaskan tata cara menjalankan program ini. Agar tidak terjadi kesalahan dlm menjalankannya.

Selama perancangan penyusun program banyak meminta masukan dari pihak Polda Bengkulu. Dengan demikian program hasil yang telah dibangunpun diharapkan memberikan informasi yang dibutuhkan oleh pihak Polda Bengkulu maupun konsumen.

Perbandingan Sistem Lama dan Sistem Baru

Adapun jenis keuntungan penggunaan sistem baru dibandingkan sistem lama yang dimaksud dapat dijelaskan sebagai berikut :

Table 4.1 Perbandingan Sistem Lama dan Sistem Baru

Jenis	Sistem Lama	Sistem Baru
Keamanan Data	Sangat terbuka kemung-kinan terjadi kehilangan data	Sangat aman karena data hasil proses tercakup dalam database.
Kebutuhan Media Simpan	Sangat besar dalam bentuk map-map dan perleng-kapan administrasi kantor lainnya	Simpel dan hanya memerlukan ruang simpan yang kecil (Flash Disk, Hard Disk)
Ketelitian	Ketelitian sangat rendah karena menyangkut daya ingat bagian pembukuan dan tidak otomatis	Ketelitian tinggi karena sistem telah terintegrasi antar tabel yang terkoneksi

V.KESIMPULAN DAN SARAN

A.Kesimpulan

Berdasarkan hasil pengamatan yang telah dilakukan melalui implementasi dan penerapan pemakaian program pada Polda Bengkulu dan sekaligus pendapat dari pihak Polda Bengkulu, dapat disimpulkan sebagai berikut :

1. Keberadaan program sebagai alat bantu memberikan informasi tentang Korban Kejahatan, Saksi Kejahatan, Pelaku Kejahatan, dan Barang Bukti
2. Program ini banyak memberikan kemudahan dan ketelitian baik dalam hal pengelolaan data.
3. Keberadaan program ini, dapat memberikan efektifitas dan efisiensi dalam pekerjaan di Polda Bengkulu

B.Saran

Berdasarkan pembahasan dan kesimpulan yang telah diuraikan di atas, saran yang dapat diberikan adalah :

1. Agar Aplikasi ini dapat dikenal secara luas maka diharapkan di lakukan melalui web pribadi Polda Bengkulu.
2. Untuk kemudian hari diharapkan dapat memberikan tampilan program yang lebih menarik.

DAFTAR PUSTAKA

Ariyus D, *Kriptografi, Keamanan Data dan Komunikasi*, Edisi Pertama, Graha Ilmu.,2006

Arnoldus Trio.*Kolaborasi Persandian dan Komunikasi.* <http://www.tni.mil.id>. Tanggal akses: 24 April 2012 pukul 20.45

A. Rahmani, *Implementasi Teknik Kriptografi Blowfish untuk Pengamanan Basis Data*, Tesis Magister Departemen Teknik Informatika, ITB, 2003.

A. Silberschatz, H. F. Korth. Dan S. Sudarshan, *Database System Concepts, 4th Edition*, McGraw – Hill, 2002.

B. Trower, *Crypt Data Packaging*, Trantor Standard Systems Inc. 2005

Hariyanto.B, *Sistem Operasi Lanjut*, Informatika, Bandung, 2003

Jogiyanto, *HM, Visual Basic Untuk Pemula : 2001*

Kurniadi, A., *Pemrograman MS. Visual Basic 6*, PT. Elex Media Komputindo, Jakarta, 2001.

