APLIKASI *RAR RECOVERY* UNTUK MEMBUKA BERKAS TERPROTEKSI DENGAN *DIGITAL FORENSICS* BERBASIS *BRUTE FORCE ATTACK* DAN *DICTIONARY ATTACK*

SKRIPSI

Disusun Oleh :

KRISTINA

NPM. 1211010020

FAKULTAS ILMU KOMPUTER

JURUSAN TEKNIK INFORMATIKA

INSTITUT INFORMATIKA & BISNIS DARMAJAYA

BANDAR LAMPUNG

2017

APLIKASI *RAR RECOVERY* UNTUK MEMBUKA BERKAS TERPROTEKSI DENGAN *DIGITAL FORENSICS* BERBASIS *BRUTE FORCE ATTACK* DAN *DICTIONARY ATTACK*

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Mencapai Gelar

SARJANA KOMPUTER

Pada Jurusan Teknik Informatika

IIB Darmajaya Bandar Lampung

Disusun Oleh:

Kristina

1211010020

JURUSAN TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

INSTITUT INFORMATIKA DAN BISNIS DARMAJAYA

BANDAR LAMPUNG

2017

PERNYATAAN

Saya yang bertanda tangan dibawah ini, menyatakan bahwa skripsi yang saya buat ini adalah hasil karya saya sendiri, tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi atau karya yang pernah ditulis atau diterbitkan orang lain kecuali yang secara tertulis dalam naskah ini dan disebutkan dalam daftar pustaka. Karya ini adalah milik saya dan pertanggung jawaban sepenuhnya berada ditangan saya.

Bandar Lampung, 22 Februari 2017

KRISTINA
NPM. 1211010020

HALAMAN PERSETUJUAN

Judul Skripsi	:	APLIKASI *RAR RECOVERY* UNTUK MEMBUKA BERKAS TERPROTEKSI DENGAN *DIGITAL FORENSICS* BERBASIS *BRUTE FORCE ATTACK* DAN *DICTIONARY ATTACK*
Nama	:	Kristina
NPM	:	1211010020
Jurusan	:	S1 Teknik Informatika

Menyetujui :

Pembimbing	Ketua Jurusan, Teknik Informatika
Rionaldi Ali, S.Kom., M.T.I	**Yuni Arkhiansyah.,S.Kom.,M.Kom**
NIK. 12710212	**NIK. 00480802**

HALAMAN PENGESAHAN

Telah diuji dan dipertahankan di depan Tim Penguji Skripsi
Jurusan Teknik Informatika Institut Informatika & Bisnis Darmajaya
Bandar Lampung dan dinyatakan diterima untuk
memenuhi syarat guna memperoleh gelar
Sarjana Komputer

Mengesahkan,

1. Tim Penguji: Tanda Tangan

   Ketua : ……

   Anggota : ……

2. Dekan Fakultas Ilmu Komputer

Dr. RZ. Abdul Aziz, M.T
NIK. 01050904

Tanggal Lulus Ujian Skripsi : 02 Maret 2017

HALAMAN PERSEMBAHAN

Dengan mengucap syukur Alhamdulillah, kupersembahkan karya kecilku untuk :

1. Untuk jagoanku Kenzou Ry Azka Nugroho buah hatiku yang menjadi segalanya untukku.
2. Pasangan hidupku Agung Nugroho, terimakasih untuk semuanya.
3. Untuk kedua orang tuaku yang sangat saya sayangi, Bapak Legiman Dan Ibu Rukini terimakasih yang tak terhingga untuk kalian.
4. Adikku Ujang Sisyono dan kakakku Rugini beserta anaknya Anggie Ayu Aldani yang selalu menjadi penghiburku.
5. Para guru-guru SD, SMP dan SMA serta Dosen yang telah memberikan ilmu dan tauladan kepadaku.
6. Dosen pembimbing Bapak Rionaldi Ali, S.Kom., M.T.I yang sangat sabar membimbingku, menjadi teman curhat sekaligus kujadikan ayah angkatku, memberikan nasehat untuk segala hal dan selalu memberikan motivasi untuk selalu tetap semangat sampai tugas akhir ini selesai.
7. Para saudaraku mbak Vera, Fandy, Keke, Ebil, mbak Novi, Tante Esti, pakde Sunarto, bulek cie, pakde Usman, bude Nur, Bulek Yuli, dan orang tuaku bpk Sumbadi dan ibu Siti, Pamanku tercinta Priyo beserta keluarga, kakak sepupuku tersayang Agus Irawan beserta keluarga, kakek dan nenekku dan semua keluargaku di Palembang.
8. Sahabat-sahabat karibku, Gembul, Sari, Vivi, Via, Heny, mbak Temy, mbak Galuh, Mbak Windul, mbak Tiara, dan seluruh kosan Thamriners, Febry Ayu Budiyanti, Aang Dwi Purnawan, Denis, Zainal Anzori, Bedi Setiawan, Dinar, Ronald, Tri Budiantoro, Kharisma Yudha, Fahrul, Widi Christianto, AdityaSyahril, Ari Setyawan, Ivan, dan seluruh anak DSC pojok.
9. Kampus tercinta IIB Darmajaya sebagai almamaterku.
10. Teman - teman seperjuangan jurusan TI angkatan 2012 yang aku banggakan.

“MOTTO”

“Menjadi diri yang selalu berusaha dan percaya Allah akan menjabahi”

ABSTRAK

APLIKASI *RAR RECOVERY* UNTUK MEMBUKA BERKAS TERPROTEKSI DENGAN *DIGITAL FORENSICS* BERBASIS *BRUTE FORCE ATTACK* DAN *DICTIONARY ATTACK*

Oleh:

KRISTINA

Digital forensics merupakan bagian dari Bareskrim Polda Lampung yang bertugas menangani barang bukti berbentuk digital dan *cybercrime*. Salah satu masalah pada *digital forensics* adalah ketika fase eksaminasi penyidik menemukan *file* yang dilindungi oleh kata kunci *(password).* Sehingga informasi terkait barang bukti suatu kasus tidak lengkap dan tidak dapat dijadikan barang bukti persidangan.

Berdasarkan permasalahan tersebut maka peneliti melakukan penelitian tentang bagaimana cara membuka *file* yang dilindungi oleh kata kunci *(password).* Dengan menggunakan metode *brute force attack* dan *dictionary attack* dapat membuka *file* yang ber-*password*.

Untuk membangun sebuah aplikasi pada penelitian ini, peneliti menggunakan metode *Waterfall* dengan menerapkan fase komunikasi(wawancara), pemodelan(analisis dan perancangan), dan konstruksi (*coding* dan *testing*).

Hasil penelitian ini adalah *file* yang dilindungi *password* dapat dibuka dengan teknik *brute force attack* dan *dictionary attack* meski aplikasi yang dihasilkan baru mampu menangani *file* berformat RAR, namun teknik *brute force attack* mampu menjawab kebutuhan penyidik *digital forensics* dalam pekerjaannya.

Kata kunci : *Password breaking, digital forensics, brute force attack*

ABSTRACT

BRUTE FORCE ATTACK AND DICTIOANARY ATTACT -BASED*RAR RECOVERY* APPLICATION TO OPEN A PROTECTED FILES BY DIGITAL FORENSICS

By

Kristina

Digital forensics is a part of the Criminal Investigation of Lampung Police in charge of handling the evidence in digital form and cybercrime. One of the problems in digital forensics examination phase is when the investigators discovered files protected by keyword (password) so that relevant information on an evidence of the case is incomplete and can not be used as evidence in the trial.

Regarding the problem, then the researcher conducted a study on how to open a file protected by keyword (password), using *brute force* and *dictionary attack*to open the file that berpassword. To build an application on research in, the researcher used *waterfall* method by applying the communication phase (interview), modeling (analysis and design), and construction (coding and testing).

The result of this study was the password protected files can be opened with brute *force attack* and *dictionary attack*techniques despite the resulting application meets the demands of new digital forensics investigator job.
The result of this study was the password protected files can be opened with *bruteforce attack* and *dictionary attack* despite the resulting application capable of handling RAR file format, but*brute force technique* is able to answer the needs of digital forensics investigator job.

Key words: ***Password breaking, digital forensics, brute force attack***

PRAKATA

Assalamu'alaikum Wr.Wb

Puji syukur kehadirat Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyusun dan menyelesaikan Skripsi yang berjudul "APLIKASI *RAR RECOVERY* UNTUK MEMBUKA BERKAS TERPROTEKSI DENGAN *DIGITAL FORENSICS* BERBASIS *BRUTE FORCE ATTACK* DAN *DICTIONARY ATTACK"* dengan baik sesuai dengan kemampuan yang penulis miliki.

Didalam penyelesaian Skripsi ini tidak terlepas dari do'a, bantuan, bimbingan, dorongan, dan saran dari semua pihak yang diberikan kepada penulis. Oleh karena itu penulis mengucapkan terima kasih kepada :

1. Bapak Ir. Firmansyah Y.A., M.B.A., M.Sc, Selaku Rektor Institut Informatika dan Bisnis Darmajaya.
2. Bapak Dr. R.Z. Abdul Aziz, M.T, Selaku Dekan Fakultas Ilmu Komputer Institut Informatika dan Bisnis Darmajaya.
3. Bapak Yuni Arkhiansya.,S.Kom.,M.Kom, Selaku Ketua Jurusan Teknik Informatika
4. Bapak Rio Kurniawan, M.Cs Selaku Wakil Ketua Jurusan Teknik Informatika
5. Bapak Rionaldi Ali, S.Kom.,M.T.I, Selaku Pembimbing Skripsi yang telah membantu memberikan pengarahan kepada penulis dalam penyusunan Skripsi ini hingga selesai.
6. Bapak dan Ibu Dosen khususnya Jurusan Teknik Informatika beserta seluruh Staf Karyawan di IIB Darmajaya yang telah banyak membantu.

Wassalamu'alaikum Wr.Wb.

Bandar Lampung, 24 Februari 2017
Penyusun,

KRISTINA
NPM.1211010020

RIWAYAT HIDUP

1. Identitas

Nama	: Kristina
Tempat & Tanggal Lahir	: Makarti, 10 November 1992
Alamat	: Desa Sumberejo, Kec. Tumijajar, Kab. Tulang Bawang Barat – Lampung RT/RW 002/001
Email	: kristinagung77@gmail.com
No. Telp	: 0822-8013-3698
Orang Tua	: Legiman (Ayah) dan Rukini (Ibu)
Putri ke	: Kedua dari tiga bersaudara

2. Riwayat Hidup

Jenjang pendidikan yang pernah ditempuh, antara lain :

a. Sekolah Dasar (SD) Negeri 1 Sumberejo, Tumijajar – TUBABA tahun 1999.
b. Sekolah Menengah Pertama (SMP) Negeri 2 Tumijajar tahun 2005.
c. Sekolah Menengah Kejuruan (SMK) Muhammadiyah 1 Tumijajar tahun 2008.
d. Pada tahun 2012 Penulis diterima di IIB Darmajaya Jurusan S1 Teknik Informatika.

Dengan ini saya menyatakan bahwa semua keterangan yang saya sampaikan di atas adalah benar.

Penulis,

Kristina

NPM.1211010020

DAFTAR ISI

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

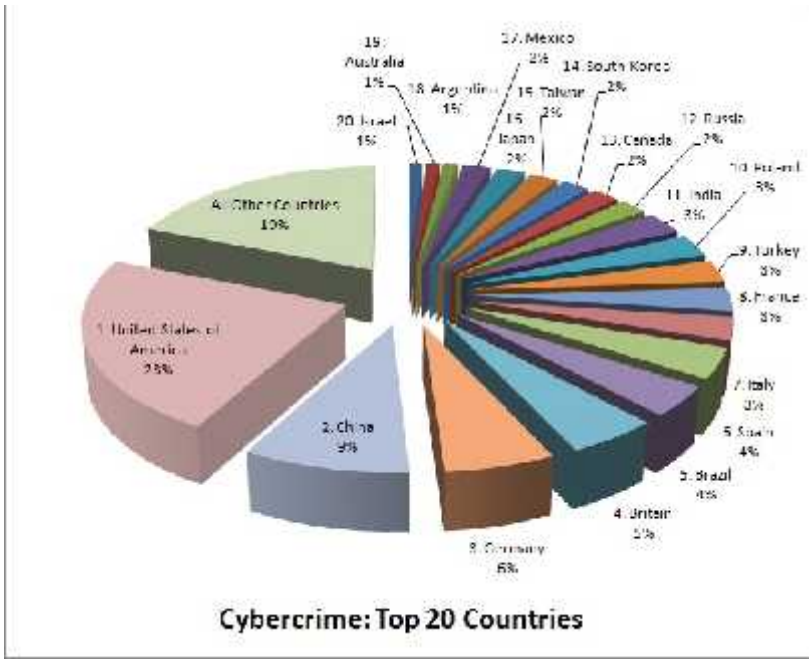
Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini alat digital semakin canggih dan memberikan bantuan kepada manusia dalam segala aktivitasnya sehingga membuat hampir dari semua manusia bergantung pada alat digital. Adapun kegunaan alat digital saat ini sudah banyak digunakan dalam bentuk tindak kejahatan. Sehingga Suatu proses penyidikan sebuah tindak kejahatan memerlukan pembuktian yang berasal dari bukti-bukti dari tempat kejahatan berlangsung ataupun dari tempat-tempat yang dicurigai digunakan atau didatangi oleh baik pelaku maupun korban kejahatan. Bukti suatu kejahatan merupakan aset vital untuk tim penyidik mendapatkan kesimpulan. Bukti kejahatan tidak hanya berupa bukti fisik semata, melainkan juga bukti dalam bentuk digital (non-fisik). Bukti digital pun tersimpan dalam beragam tempat penyimpanan (flashdisk, hard disk, MMC, dll).

Seperti data kejahatan pada alat digital *(cybercrime)* yang terjadi di berbagai Negara, adalah sebagai berikut :



Gambar 1.1 Kasus *Cybercrime* Di 20 Negara

Gambar di atas adalah menerangkan 20 negara teratas yang melakukan tindak kejahatan dengan menggunakan alat digital atau komputer *(cybercrime)* pada tahun 2013. Yang didapat dari sumber https://digital4rainsick.files.wordpress.com/2013/06/cybercrime-top-20-countries-pie-chart.jpg.

Melihat kejadian tersebut membuka mata kita akan pentingnya keahlian dibidang *digital forensics* dalam mendukung investigasi pada kasus kejahatan khususnya kejahatan pada bidang komputer *(cybercrime).*

Adapun kasus yang tengah terjadi pada saat ini yang berhubungan dengan kejahatan pada bidang komputer*(cybercrime)* adalah sebagai berikut:

Gambar 1.2 Ahli *Digital Forensics* Menghadirkan Bukti Digital Dipersidangan

Pada gambar diatas, menjelaskan bahwa sikap Jessica ini seolah memperlihatkan dia terusik dengan keterangan yang disampaikan ahli *Digital Forensics* Puslabfor Mabes Polri, AKBP Muhammad Nuh Al Azhar. Dalam kesaksiannya, Nuh sebagai ahli teknologi informasi (TI) mengupas tiap detik rekaman CCTV Jessica saat berada di Kafe Olivier, Grand Indonesia Mall, Jakarta Pusat, 6 Januari 2016 lalu, saat bertemu Mirna. Yang berlangsung di Pengadilan Negeri Jakarta Pusat, Rabu 10 Agustus. Didapat dari sumber http://m.liputan6.com/news/read/2575129/jessica-terusik-ahli-digital-forensik.

Forensik digital yang merupakan bagian dari unit forensik yang ada di tubuh kepolisian negara Indonesia berperan penting dalam penyidikan yang melibatkan

barang bukti berbentuk digital. Seperti pada peristiwa di atas bahwa suatu kasus kejahatan bisa sangat bergantung pada barang bukti dalam bentuk digital sehingga melibatkan seorang *digital forensics* ikut serta dalam membantu pihak kepolisian dalm mencari bukti nyata. Namun pada saat proses *digital forensics* berlangsung kadang terbentur dengan file yang dilindungi oleh kata kunci. Oleh karena itu, seorang forensik digial memerlukan metode atau alat bantu untuk membuka file yang dilindungi oleh kata kunci yang mungkin saja berguna sebagai barang bukti dalam suatu kasus kejahatan.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah diatas, maka rumusan masalahnya adalah:

1. Memperoleh informasi dari bukti digital terbentur karena proteksi dari file dengan *password.*
2. Salah satu kebutuhan dalam forensik digital di Polda Lampung.

1.3 Batasan Masalah

Penelitian ini akan memfokuskan pada masalah-masalah sebagai berikut:

1. Berkas yang dimaksud dalam penelitian ini ialah berkas yang disimpan pada suatu media penyiman (Flashdisk, Harddisk, MicroSD, dll).
2. Berkas yang akan digunakan dalam penelitian ini ialah berkas dalam format RAR

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk membangun alat bantu guna membantu proses *digital forensics* dalam memperoleh kata kunci (*password*) dengan memanfaatkan metode BFA.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah untuk membantu proses *digital forensics* dalam memperoleh kata kunci *(password)* guna membuka suatu berkas (*file*) dalam suatu media penyimpan yang akan dijadikan barang bukti dalam suatu kasus hukum.

1.6 Sistematika Penulisan

Untuk memberikan gambaran secara menyeluruh masalah yang akan dibahas dalam tugas akhir ini, maka dibuat sistematika penulisan yang terbagi dalam lima bab, penulisan ini akan menjelaskan uraian secara singkat isi tiap bab adalah sebagai berikut:

BAB I PENDAHULUAN

Pada Bab ini berisi tentang latar belakang, masalah, rumusan masalah, batasan masalah, tujuan penelitian dan manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi teori-teori pendukung, pendapat, prinsip dan sumber yang dapat di pertanggung jawabkan dan berhubungan dalam pengetahuan tentang ilmu komputer sehingga menjadi pedoman dan acuan dalam proses pembelajaran.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang metode-metode pendekatan penyelesaian permasalahan yang dinyatakan dalam perumusan masalah.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi penjelasan mengenai hasil dari implementasi dan evaluasi dari hasil praktek yang dibuat.

BAB V SIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil praktek juga berisi saran-saran yang bersifat membangun dan juga untuk perkembangan hasil praktek lebih lanjut.

DAFTAR PUSTAKA

LAMPIRAN

BAB II
LANDASAN TEORI

2.1 Forensik

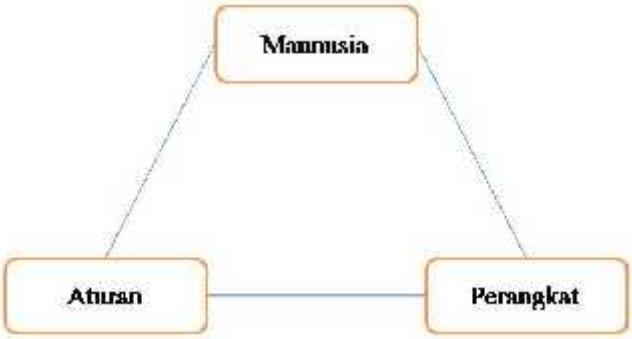
Forensik atau forensik umum merupakan suatu tindakan yang bertujuan untuk membantu proses persidangan kasus hukum yang dilakukan dengan cara menyajikan barang bukti dengan melalui proes analisis dan mendapatkan kembali bukti dari kejadian dan lingkungan tersebut. Tidak mudah untuk mendapatkan atau lebih tepatnya menemukan fakta, karena dalam banyak kasus, fakta sifatnya "tersembunyi", misalnya berkas *(file),* yang dianalisis sedemikian rupa sehingga didapatkan fakta yang benar-benar layak untuk diajukan sebagai pembuktian. Serangkaian proses ini dikenal dengan istilah forensik.

2.2 Forensik Digital

Bagian dari forensik umum yang mulai mendapat perhatian khusus adalah forensik digital. Albert S. (2016) menyatakan bahwa "Forensik digital mengikuti prinsip yang sama dengan forensik umum", yaitu mengumpulkan bukti dan menyajikan laporan analisisnya dari tempat kejadian perkara suatu kasus hukum yang sudah masuk dalam tahap penyidikan sampai dengan pada tahap persidangan. Perbedaan nyata antara forensik umum dengan forensik digital ialah pada objek barang buktinya. Forensik umum mencakup prosedur perlakuan pada barang bukti fisik pada tempat kejadian perkara (TKP), prosedur proses analisis barang bukti, sampai dengan penyajian laporan hasil. Sedang forensik digital mencakup prosedur perlakuan pada barang bukti yang berbentuk digital yang biasanya terdapat pada bukti-bukti elektronik yang memiliki kemampuan menyimpan data digital, prosedur analisis isi (*content*) dari barang bukti digital, sampai dengan proses penyajian laporan hasil pemeriksaan dan analisis isi dari barang bukti digital.

2.2.1 Komponen Forensik Digital

Dalam proses forensik digital terdapat tiga komponen untuk mendapatkan tujuan akhir yaitu bukti atau fakta. Tiga komponen tersebut dapat dilihat pada gambar 2.1:



Gambar 2.1. Komponen Forensik Digital (*Digital Forensics)*

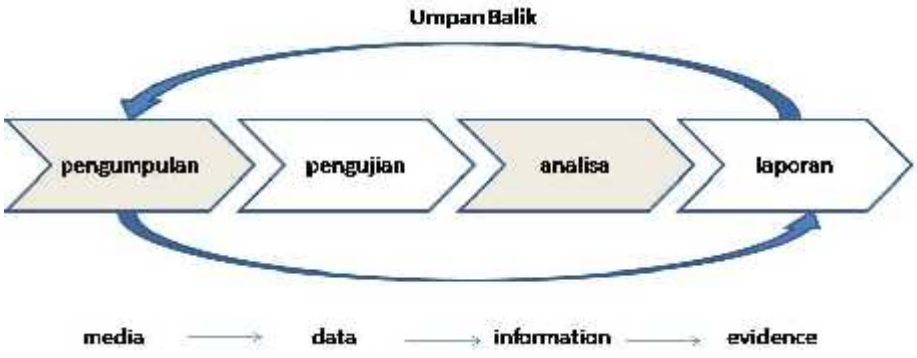
Pada gambar di atas terlihat bahwa semua komponen saling berhubungan, manusia yang diperlukan dalam forensik digital merupakan pelaku utama yang tentunya mempunyai kualifikasi tertentu untuk mencapai kualitas yang diinginkan.

Perangkat untuk kepentingan forensik digital dapat dibedakan pada dua kategori yaitu *hardware* dan *software*.

Aturan merupakan komponen yang paling penting dalam pemodelan forensik digital, didalamnya mencakup prosedur dalam mendapatkan, menggali, menganalisa barang bukti dan akhir bagaimana menyajikan hasil penyelidikan dalam laporan.

2.2.2 Tahapan Forensik Digital

Untuk mendapatkan tujuan akhir tentunya harus mempunyai prosedur atau tahapan dalam melakukan suatu proses forensik digital, diantaranya terdapat empat tahapan yang harus dilakukan, empat tahapan tersebut dapat dilihat pada gambar 2.2:



Gambar 2.2 Tahap-Tahap Forensik Digital (*Digital Forensics)*

a. Pengumpulan Data.

Pada metode ini segala bukti-bukti yang mendukung penyelidikan dikumpulkan. Penyelidikan dimulai dari identifikasi dimana bukti itu berada, dimana disimpan, dan bagaimana penyimpanannya untuk mempermudah penyelidikan.

b. Pengujian.

Pada metode ini menggunakan tool untuk melakukan pengujian seperti *software* yang mampu menentukan secara akurat jenis *file* yang berisi karakteristik data tertentu, misalnya format *file teks, grafik, audio,* atau berbagai *file* kompresi lainnya. Secara mendasar, tahap ini mencakup mengakolasi *file*, mengekstrak *file* (mungkin melalui enskripsi, steografi, *uncompress*, dan lainnya), mugkin melakukan pemeriksaan terhadap metadata, dan lain sebagainya.

c. Analisis.

Analisis dilakukan untuk merumuskan kesimpulan dalam menggambarkan data. Analisis yang dimaksud mengambil pendekatan metodis untuk menghasilkan kesimpulan yang berkualitas didasarkan pada ketersediaan data atau bahkan sebaliknya.

d. Laporan.

Presentasi dilakukan dengan menyajikan dan menguraikan secara detail laporan penyelidikan dengan bukti-bukti yang sudah dianalisa secara mendalam dan dapat dipertanggung jawabkan secara hukum di pengadilan.

2.3 Berkas/File

Dalam menjalankan proses forensik digital tentunya barang bukti yang berkaitan pun juga merupakan barang bukti berupa digital, seperti halnya berkas/*file* yang yang terdapat di dalam komputer dan masing-masing dari *file* memiliki ekstensi tergantung dari jenis *file* itu sendiri. Terdapat dua bagian dari suatu *file* yaitu *header* dan *body*/data. Pada *header* terdapat lokasi penyimpanan, panjang *file*, format *file*(doc, jpg, bmp, dll). Sedangkan *body*/data adalah isi dari suatu *file*. Dua hal tersebut saling bergantung, karena *body*/data tidak dapat berdiri sendiri atau disimpan tanpa terletak dalam *header*, sedang *header* harus memiliki *body/*data jika tidak, *header* tersebut adalah *header* kosong.

2.4 Enkripsi File

Pada saat melakukan suatu proses penyidikan dalam kasus forensik digital sering menenmukan suatu *file* yang dikunci. Dalam hal ini *file* yang ditemukan dalam keadaan terkunci harus dienkripsi terlebih dahulu guna untuk mengetahui apakah isi dari *file* tersebut berhubungan dengan kasus yang dipersidangkan di pengadilan atau tidak. Untuk mengetahui hal itu maka *file* harus dienkripsi terlebih dahulu. Seperti yang kita ketahui melakukan enkripsi suatu *file* terlebih dahulu mengenkripsi *header* lalu kemudian *body*/data. Enkripsi dilakukan untuk mengetahui atau dapat membaca keseluruhan dari isi *file*.

2.5 Password (Kata Kunci)

William Stalling (2005) mengatakan bahwa "*Password* adalah kunci kekuatan sebuah algoritma kriptografi". Algoritma kriptografi terbuka dan dipublikasikan untuk umum, sehingga tidak ada rahasia dalam sebuah algoritma kriptografi. Kerahasiaan data dijamin dengan algoritma kriptografi yang standar (misal AES) dan kata kunci yang baik.

2.5.1 Password Strength (Entrophy)

Password dapat dikategorikan menjadi dua yaitu *password* kuat dan *password* lemah. *Password* lemah adalah *password* yang dihasilkan oleh manusia dan *password* yang mengikuti pola. Sedang *password* kuat adalah *password* dengan kombinasi acak. Contoh *password* yang mudah ketebak adalah tanggal lahir, nama peliharaan, penyanyi idola, tim olahraga, nama anak, orang terdekat, 1234567890, event berkesan, *password* bawaan. Alat untuk mengukur kekuatan *password* adalah *GMAIL password strength meter.*

Berikut adalah *measuremen password strength*:

Tabel 2.1 Tabel *Measuremen Password Strength*

Symbol Set	Number Of Symbol	Entropy/Symbol
Digits only (0-9)	10	3,32 bits
Single case letters (a-z)	26	4,7 bits
Single case letters and digits (a-z, 0-9)	36	5,17 bits
Mixed case letters and digits (a-z, A-Z, 0-9)	62	5,95 bits
All standard ASCII keyboard character	94	6,55 bits

2.5.2 Pseudo Random Generator (PRG)

Pseudo Random Generator (PRG) bekerja dengan prinsip *brute force,* yang artinya percobaan menebak diambil dari kombinasi acak seluruh karakter ASCII yang mungkin. Untuk keperluan ini maka diperlukan sebuah prosedur membangkitkan kombinasi acak karakter sebelum percobaan menebak dilakukan. Istilah pembangkitan karakter acak ini disebut *pseudo random generator.*

Dalam sebuah metode untuk membobol suatu *password* melibatkan suatu algoritma yang dibutuhkan, untuk itu digunakan sebuah algoritma untuk menghasilkan urutan-urutan atau *sequence* dari angka-angka sebagai hasil dari perhitungan dengan komputer yang diketahui distribusinya sehingga angka-angka tersebut muncul secara *random* dan digunakan terus-menerus yang disebut sebagai *Pseudo Random Generator* (PRG). Atau lebih singkatnya adalah sebuah algoritma untuk menghasilkan urutan angka yang sifatnya mendekati urutan nomor acak.

2.5.3 Brute Force Attack

Merupakan metode *cracking password* dengan mencoba segala macam variasi yang mungkin. Feri Sulianta (2015) mengatakan bahwa "Metode ini sangat "mujarab" dan populer untuk mendapatkan *password*".

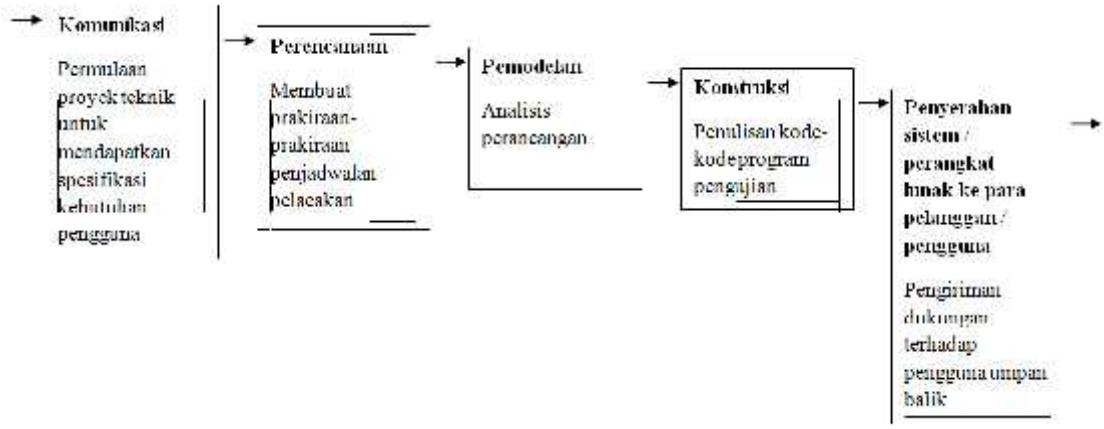
Meski metode ini membutuhkan waktu lama, namun metode ini mampu dan bisa menebak *password* dan dapat diandalkan khususnya untuk *password* pendek. *Brute force* menggunakan aplikasi yang akan menggunakan semua kombinasi. Ada dua jenis *brute force attack* yaitu *online brute force attack* dan *offline brute force attack*. Salah satu aplikasi *online brute force attack* adalah THC-Hydra dan dapat di download "http://www.thc.org/thc-hydra" merupakan salah satu *network logon cracker* tercepat. Sedang *brute force attack offline* adalah program yang akan dibuat dengan mencoba menggunakan satu aplikasi yang dapat membuka file dalam format RAR yang selama ini belum pernah ada.

2.5.4 Dictionary Attack

Dictionary attack adalah metode turunan dari *brute force attack* tetapi hanya mencoba berdasarkan simpanan kamus kata-kata. Sukses atau tidaknya metode ini bergantung pada ukuran simpanan (kamus) 300Kb, 1Mb, 2Mb, 3Mb, 4Mb, 5Mb, 6Mb, 7Mb, 8Mb, 30 Mb, 4 Gb dan seterusnya. Semakin besar ukuran simpanan (kamus) maka kemungkinan sukses juga semakin besar. Umumnya *password* ciptaan manusia sering berupa kata. *Dictionary attack* juga bisa digunakan *online* maupun *offline*. Dan dapat melakukan permutasi A→4, a→@.

2.6 Metode Waterfall

Model *waterfall* (air terjun) menyiratkan pendekatan yang sistematis dan berurutan (skuensial) dari tahap satu ke tahap lain pada pengembangan perangkat lunak dalam model seperti air terjun. Rogers Pressman (2012) mengatakan model ini melingkupi aktivitas-aktivitas seperti yang terlihat pada gambar 2.3:

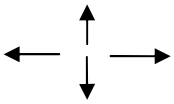
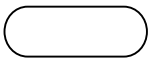
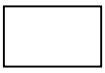
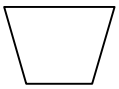


Gambar 2.3 Pengembangan Perangkat Lunak Model *Waterfall*

2.7 Flowchart

Untuk merangkai suatu alur kerja dibutuhkan sebuah flowchat untuk membuat bagan dengan simbol-simbol tertentu yang menggambarkan urutan proses secara mendetail dan hubungan antara suatu proses (instruksi) dengan proses lainnya dalam suatu program. Sehingga flowchart benar dapat meringankan pekerjaan peneliti. Berikut ini adalah beberapa simbol dan fungsinya yang digunakan dalam membuat flowchart:

Tabel 2.2 Tabel Simbol Flowchart

Simbol	Keterangan
	Flow Direction Symbol Yaitu symbol yang digunakan untuk menghubungkan antara simbol yang satu dengan simbol yang lain. Simbol ini disebut juga connecting line
	Terminator Symbol Yaitu simbol untuk permulaan (start) atau akhir (stop) dari suatu kegiatan
	Connector Symbol Yaitu simbol untuk keluar-masuk atau penyambungan proses dalam lembar / halaman yang sama
	Connector Symbol Yaitu simbol untuk keluar-masuk atau penyambungan proses dalam lembar / halaman yang berbeda
	Processing Symbol Simbol yang menunjukkan pengolahan yang dilakukan oleh komputer
	Simbol Manual Operation Simbol yang menunjukkan pengolahan yang tidak dilakukan oleh komputer

Simbol	Keterangan
	Simbol preparation Simbol untuk mempersiapkan penyimpanan yang akan digunakan sebagai tempat pengolahan di dalam storage
	Simbol predefine proses Simbol untuk pelaksanaan suatu bagian (sub-program)/prosedure
	Simbol display Simbol yang menyatakan peralatan output yang digunakan yaitu layar, plotter, printer dan sebagainya.
	Simbol disk and on-line storage Simbol yang menyatakan input yang berasal dari disk atau disimpan ke disk
	Simbol magnetic tape unit Simbol yang menyatakan input berasal dari pita magnetik atau output disimpan ke pita magnetik
	Simbol punch card Simbol yang menyatakan bahwa input berasal dari kartu atau output ditulis ke kartu
	Simbol dokumen Simbol yang menyatakan input berasal dari dokumen dalam bentuk kertas atau output di cetak ke kertas

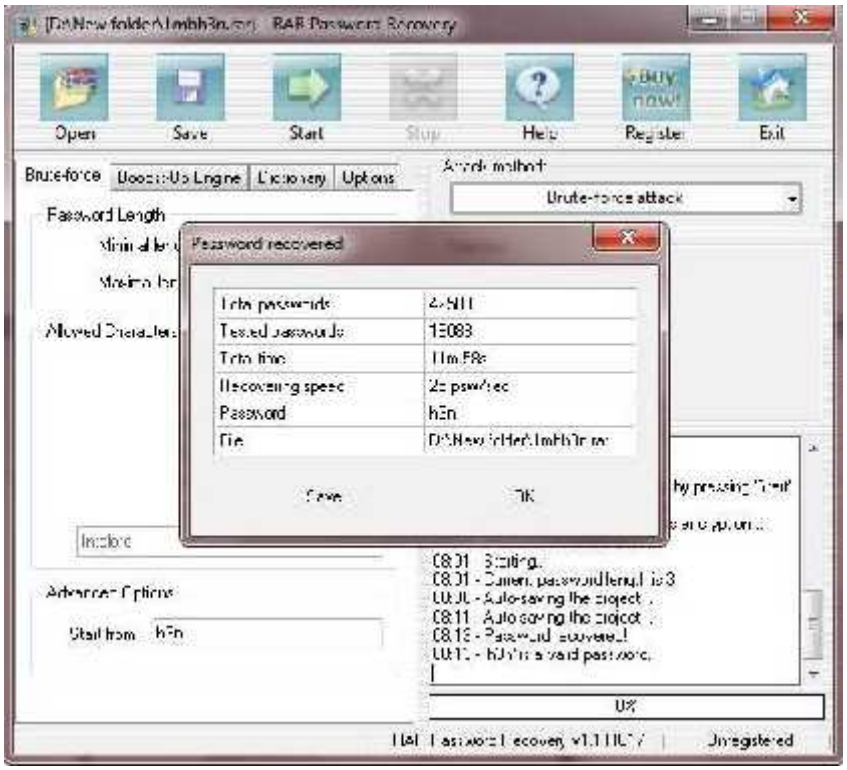
2.8 Black Box Testing

Black box testing atau uji kotak hitam adalah pengujian untuk menentukan prilaku sistem atau bagiannya dalam menanggapi beberapa skenario yang telah dibuat.

Menurut Roger S. Pressman (2010) "pengujian *black box* berusaha menemukan kesalahan dalam kategori sebagai berikut: (1) fungsi-fungsi yang tidak benar atau hilang, (2) kesalahan interface, (3) kesalahan dalam struktur data atau akses database eksternal, (4) kesalahan kinerja, (5) inisialisasi dan kesalahan terminasi".

2.9 Penelitian Terdahulu

Sebelum penelitian ini dilakukan, terdapat penelitian terdahulu dengan tujuan yang sama sehingga hampir dari keseluruhan sistem mempunyai fungsi yang sama dengan aplikasi yang akan dibangun pada Polda Lampung. Untuk menjadikan acuan, peneliti mengusulkan ide sebagaimana program yang akan dibuat mampu mempersingkat waktu dalam proses pencarian *password.* Adapun aplikasi pada penelitian terdahulu dapat dilihat pada gambar 3.8:



Gambar 2.4 Aplikasi Penelitian Terdahulu

Selain penelitian diatas terdapat beberapa penelitian yang diambil dari jurnal-jurnal penelitian terdahulu, jurnal-jurnal ini digunakan untuk panduan dalam proses penulisan karya ilmiah. Jurnal-jurnal tersebut dapat dilihat pada tabel 2.3.

Tabel 2.3 Tabel Penelitian Terdahulu

No	Nama	Judul	Tahun Terbit	Keterangan
1	Anggit Dwi Hartanto, Ema Utami, Hanif Al Fatta	Penerapan Teknik Komputer Forensic Untuk Pengembalian Dan Penghapusan Berkas Digital	2011	Penggunaan berkas digital selain banyak kelebihan juga banyak kekurangan antara lain, seingnya dokumen hilang dikarenakan banyak kemungkinan, misalnya menghapus berkas penting secara tidak sengaja. Solusi dari permasalahan itu adalah data yang hilang dikembalikan dengan menggunakan *software recovery file.* Tetapi dengan adanya solusi tentang pengembalian data yang telah hilang tersebut juga menimbulkan masalah baru yaitu bagaimana cara agar data yang dihapus tidak bisa dikembalikan lagi dengan *software recovery file* yang ada. Solusi dari kedua masalah tersebut adalah dengan dilakukan percobaan yang bersifat try and error yaitu dilakukannya tindakan-tindakan terhadap data atau berkas digital. Dengan mengacu pada tindakan tersebut akan diketahui hasil dari penggunaan software testdisk versi 6.11 dalam pengembalian data dan penghapusan data.
2	Eko Suprapto	Peran Komputer Forensik Dalam Penegakan Hukum Untuk Pembuktian Kasus Cyber Crime	2012	The development of information technology so rapidly, was also followed by the development issues surrounding security and computer crime. Various modes of crime emerging computer technology began to be felt by many people. In addition to legal instruments in the form of rules and laws, it is of scientific and technical aspects are also necessary for establishing the crime. In this case the computer forensics is a field that will greatly support the efforts of law enforcement against crime with the help of computer technology. This journal provides a brief overview of computer-related crime in the world of understanding, methods and implementation process of the forensic uses a number of applications available.

BAB III
METODOLOGI PENELITIAN

Penelitian ini ditempuh dengan diawali oleh proses pengumpulan data dan fakta pada tempat penelitian, dilanjutkan dengan melakukan pengembangan perangkat lunak, dan melakukan pengujian perangkat lunak sebagai hasil akhir dari penelitian ini.

3.1 Teknik Pengumpulan Data.

Tahap ini diawali dengan melakukan wawancara di tempat penelitian guna mengumpulkan data, informasi, dan fakta yang diperlukan dalam kaitannya dengan permasalahan dalam penelitian ini serta dengan melakukan studi literatur untuk mendukung penulisan pada saat penelitian.

3.1.1 Wawancara.

Wawancara akan dilakukan di kantor Polda Provinsi Lampung yang bertempat di Jl. W.R Supratman No.1 Teluk Betung dengan objek wawancara yaitu salah seorang personil Polda Lampung berpangkat IPDA yang bernama Sunarto. Wawancara rencananya akan dilaksanakan sebanyak 3 kali mengingat kesibukan objek wawancara dalam posisinya sebagai Panit II di unit Reskum 3 Polda Lampung.

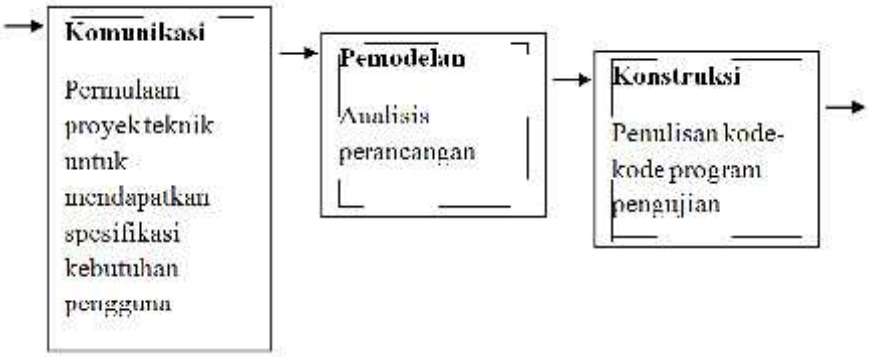
Perihal yang akan menjadi subjek wawancara ialah prosedur yang terkait dengan keseluruhan proses forensik digital yang dijalankan oleh Polda Lampung.

3.1.2 Studi Literatur.

Untuk mendukung proses penelitian perlu adanya pengumpulan data yang diperoleh dari berbagai buku ataupun hasil olahan orang lain. Dalam upaya memperoleh suatu data pendukung penulisan, peneliti menggunakan studi literatur yang didapat dari buku berbagai sumber yang berhubungan dengan forensik digital, program *delphi*, serta jurnal yang terkait dengan penulisan.

3.2 Pengembangan Perangkat Lunak.

Dalam pembuatan perangkat lunak digunakan sebuah metode *waterfall* yang didalamnya terdapat fase-fase yang akan diterapkan dalam menjalani proses pembuatan perangkat lunak. Namun pada pembuatan perangkat lunak ini menerapkan tiga fase utama *waterfall* dari fase-fase yang ada. Menurut Rogers Pressman (2012) berpendapat seperti yang terlihat pada gambar 3.1:



Gambar 3.1 Metode Pengembangan Perangkat Lunak Model *Waterfall*

3.2.1 Komunikasi.

Fase ini adalah tahap awal pengembangan perangkat lunak dengan model *waterfall*, dimana pengguna merupakan faktor utama yang harus diperhatikan sebagai pemakai perangkat lunak yang akan dibangun. Pada fase ini pengembang dan pengguna bertemu dan membahas mengenai perangkat lunak yang akan dikembangkan.

3.2.2 Pemodelan (Analisis Dan Perancangan)

Untuk membangun sebuah sistem tentu adanya tahapan yang harus dikerjakan secara bertahap. Adapun tahapan dalam proses pemodelan dilakukan dengan menganalisis perangkat lunak dan kemudian dilanjutkan dengan perancangan perangkat lunak.

3.2.2.1 Analisis Kebutuhan Perangkat Lunak

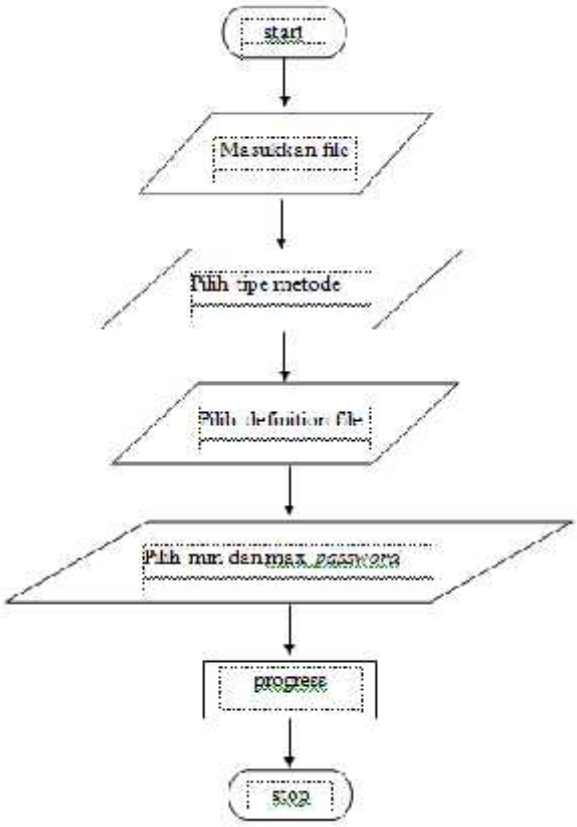
Dalam penelitian ini penyusun menggunakan beberapa perangkat lunak yang dibutuhkan dalam membangun sistem diantanya:

1. Borland delphi 7
2. Command prompt
3. Notepad++

3.2.2.2 Perancangan Perangkat Lunak

Fase ini untuk mengimplementasikan cara kerja sistem forensik digital secara keseluruhan yang akan digunakan di Polda Bandar Lampung. Pada fase ini dilakukan perancangan sistem untuk mempermudah jalannya pembuatan program.

a. Desain Alir Sistem *RAR Recover*

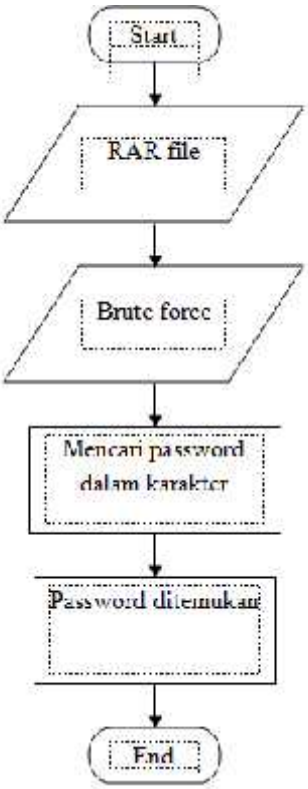


Gambar 3.2 Flowchart Sistem *RAR Recovery*

Gambar diatas menjelaskan untuk *user* menjalanjakan sistem *RAR recovery* pada Polda Lampung yang terdiri dari:

1) 2 (dua) simbol terminator, yang berperan sebagai "start" dan "finish" pada aliran proses flowchart program pada saat *user* menjalankan program.
2) 4 (empat) simbol input dan output, tanpa tergantung jenis peralatannya yang terdiri dari "masukkan file, piih metode, pilih definition file, pilih *min password* dan *max password*, dan *progress*".
3) 1 (satu) simbol processing, yang menunjukkan pengolahan yang dilakukan oleh komputer.

b. Diagram Alir Sistem Mencari Kata Kunci *(Password)* Menggunakan Metode *Brute Force Attack*

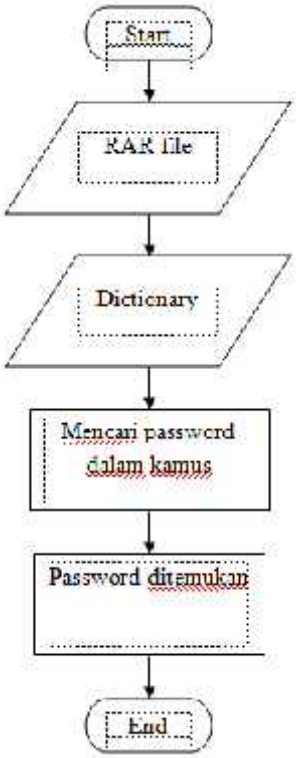


Gambar 3.3 Flowchart Sistem Mencari Kata Kunci Dengan Metode *Brute Force Attack*

Gambar diatas menjelaskan cara kerja sistem pada saat mencari kata kunci pada sistem *RAR recovery* pada Polda Lampung yang terdiri dari:

1) 2 (dua) simbol terminator, yang berperan sebagai "start" dan "finish" pada aliran proses flowchart program pada saat mencari kata kunci *(password).*
2) 2 (dua) simbol simbol input dan output, tanpa tergantung jenis peralatannya yang terdiri dari "RAR file dan *brute force*".
3) 2 (dua) simbol processing, menunjukan pengolahan yang dilakukan oleh komputer, diantaranya "mencari *password* dalam karakter dan *password* ditemukan".

c. Diagram Alir Sistem Mencari Kata Kunci *(Password)* Menggunakan Metode *Dictionary Attack*

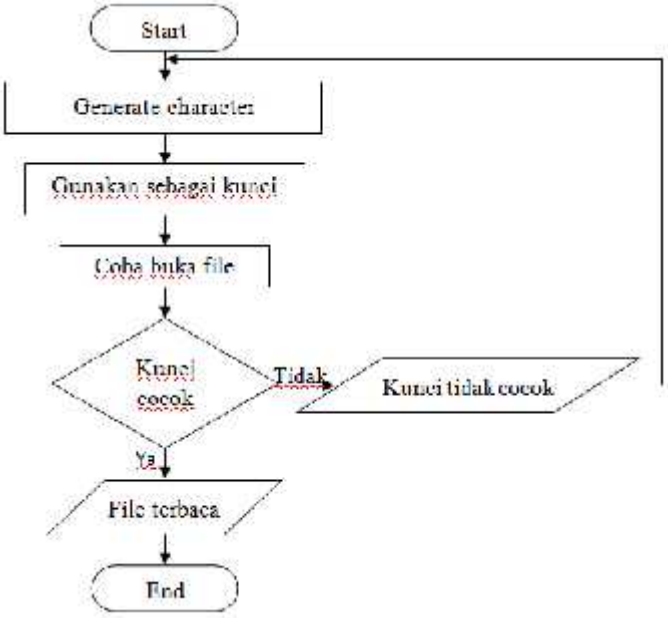


Gambar 3.4 Flowchart Sistem Mencari Kata Kunci Dengan Metode *Dictionary Attack*

Gambar diatas menjelaskan cara kerja sistem pada saat mencari kata kunci pada sistem *RAR recovery* pada Polda Lampung yang terdiri dari:

1) 2 (dua) simbol terminator, yang berperan sebagai “start” dan “finish” pada aliran proses flowchart program pada saat mencari kata kunci *(password).*
2) 2 (dua) simbol simbol input dan output, tanpa tergantung jenis peralatannya yang terdiri dari “RAR file dan *dictionary*”.
3) 2 (dua) simbol processing, menunjukan pengolahan yang dilakukan oleh komputer, diantaranya “mencari *password* dalam karakter dan *password* ditemukan”.

d. Desain *Brute Force Attack* Secara Keseluruhan



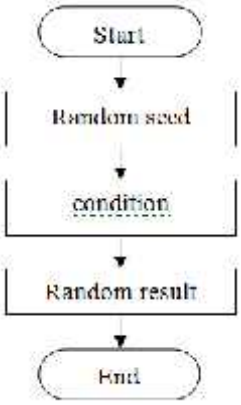
Gambar 3.5 Flowchart *Brute Force Attack*

Gambar diatas menjelaskan untuk *brute force* pada sistem “*RAR recovery* pada Polda Lampung” yang terdiri dari:

1) 2 (dua) simbol terminator, yang berperan sebagai “start” dan “finish” pada aliran proses flowchart program pada saat menjalankan *brute force Attack*

2) 3 (tiga) simbol processing, yang menunjukkan pengolahan yang dilakukan oleh komputer yang terdiri dari: "*generate character*, gunakan sebagai kunci dan coba buka file".
3) 1 (satu) simbol decision, menunjukkan sebuah langkah pengambilan keputusan 'Ya' atau 'Tidak' pada saat pencarian kata kunci.
4) 2 (dua) simbol input dan output, tanpa tergantung jenis peralatannya yang terdiri dari "kata kunci tidak cocok dan file terbaca".

e. Desain *Brute Force (Generate Random)*



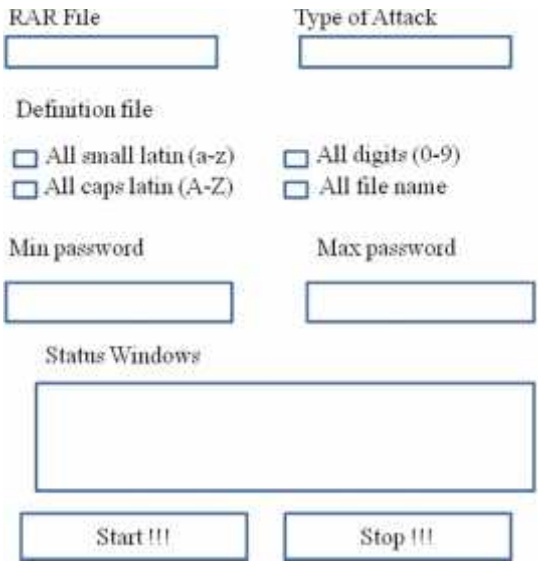
Gambar 3.6 Flowchart *Generate Random*

Gambar diatas menjelaskan untuk *brute force (generate random)* pada sistem "*RAR recovery* pada Polda Lampung" yang terdiri dari:

1) 2 (dua) simbol terminator, yang berperan sebagai "start" dan "finish" pada aliran proses flowchart program pada saat menjalankan *generate random.*
2) 3 (tiga) simbol processing, yang menunjukkan pengolahan yang dilakukan oleh komputer yang terdiri dari: "*random seed, condition, random result*".

f. Rancangan *Interface RAR Recovery*

Rancangan *interface design RAR Recovery* adalah sebagai berikut:



Gambar 3.7 Tampilan Halaman RAR Recovery

Pada tampilan diatas dijelaskan bahwa terdapat parameter-parameter yang masing-masing parameter mempunyai fungsi yang berbeda. Hal pertama yang harus dilakukan oleh user adalah memasukkan file ke dalam aplikasi ini, kemudian pilih metode untuk membuka file, jika yang dipilih adalah *dictionary attack*, maka proses pencarian *password* menggunakan kamus yang sudah disediakan. Jika yang dipilih *brute force attack*, maka harus memilih salah satu atau lebih dari *chexbox* yang terdapat pada *definition* file, kemudian memulai proses dengan cara klik tombol *start*, ketika proses selesai maka akan muncul pada status windows yaitu *password* yang telah ditemukan, banyaknya *password* yang telah dicoba, banyaknya *password* per-detik, dan lama waktu. Ataupun jika ingin berhenti sebelum proses selesai, klik tombol stop.

3.2.3 Konstruksi (Coding Dan Testing)

Untuk membangun suatu sistem dilakukan dua tahapan diantaranya yaitu *coding* dan *testing.*

3.2.3.1 *Coding*

Pada fase ini penulis dituntut untuk melakukan pengkodingan atau penulisan *code-code* pemrograman untuk dijadikan panduan dalam membangun sebuah sistem. Adapun *code-code* pemograman ditulis dalam bentuk *scrypt* dituliskan pada parameter-parameter, diantaranya:

a. Combobox(type of attack)
b. Button(start)
c. Timer
d. Button (stop)

3.2.3.2 *Testing*

Testing dilakukan dengan menggunakan metode *Black Box,* yaitu dengan menggunakan aplikasi dengan berbagai skenario, diantaranya:

Table 3.1 Tabel Skenario Uji Coba Ukuran File Dengan Metode *Brute Force Attack*

Skenario	**Keterangan**
Skenario ukuran file	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 4
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 1Mb dan panjang *password* 4
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 2Mb dan panjang *password* 4
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 3Mb dan panjang *password* 4
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 4Mb dan panjang *password* 4

Skenario	Keterangan
Skenario ukuran file	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 5Mb dan panjang *password* 4
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 6Mb dan panjang *password* 4
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 7Mb dan panjang *password* 4
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 8Mb dan panjang *password* 4
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 9Mb dan panjang *password* 4
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 10Mb dan panjang *password* 4
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100Mb dan panjang *password* 4
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 1Gb dan panjang *password* 4

Table 3.2 Tabel Skenario Uji Coba Ukuran File Dengan Metode *Dictionary Attack*

Skenario	Keterangan
Skenario ukuran file	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 4
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 1Mb dan panjang *password* 4
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 2Mb dan panjang *password* 4
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 3Mb dan panjang *password* 4

Skenario	Keterangan
Skenario ukuran file	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 4Mb dan panjang *password* 4
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 5Mb dan panjang *password* 4
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 6Mb dan panjang *password* 4
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 7Mb dan panjang *password* 4
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 8Mb dan panjang *password* 4
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 9Mb dan panjang *password* 4
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 10Mb dan panjang *password* 4
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 100Mb dan panjang *password* 4
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 1Gb dan panjang *password* 4

Table 3.3 Tabel Skenario Uji Coba Panjang *Password* Dengan Metode *Brute Force Attack*

Skenario	Keterangan
Skenario panjang *password*	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 1
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 2
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 3

Skenario	**Keterangan**
Skenario panjang *password*	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 4
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 5
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 7

Table 3.4 Tabel Skenario Uji Coba Panjang *Password* Dengan Metode *Dictionary Attack*

Skenario	**Keterangan**
Skenario panjang *password*	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 1
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 2
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 3
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 4
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 5
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 6
	Perangkat lunak melakukan *Dictionary* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 7

BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Wawancara

Tahap wawancara merupakan bagian dari komunikasi yang dilakukan dengan melibatkan objek wawancara disertai dengan tanya jawab antara penulis dengan objek. Objek dalam wawancara adalah pihak kepolisian di Polda Lampung. Adapun pihak yang diwawancarai dan tanya jawab dibuat dalam tabel 4.1 dan 4.2:

Tabel 4.1 Tabel Objek Wawancara

Pihak Yang Diwawancarai	
Nama	Ipda Sunarto
Alamat	Jl. W.R Supratman No.1 Teluk Betung Polda Lampung
Jabatan	Panit II di unit Reskum 3 Polda Lampung.
Waktu	1. Pukul 09:00-09:30 (10 agustus 2016) 2. Pukul 09:00-09:30 (14 agustus 2016) 3. Pukul 09:00-09:30 (1 september 2016)

Kemudian terdapat daftar pertanyaan dan jawaban (percakapan) pada saat wawancara di Polda Lampung, lihat tabel 4.2:

Tabel 4.2 Tabel Pertanyaan Dan Jawaban Wawancara

Daftar pertanyaan	Daftar jawaban
1. Apakah selama ini bapak mengetahui bahwa adanya *cybercrime* (kejahatan yang terjadi pada komputer)	Belum
2. Lalu apakah pernah ada kejahatan yang terjadi pada alat komputer *(cybercrime)* sebagai media kejahatan?	Pernah ada beberapa kali
3. Lalu apakah *cybercrime* tersebut langsung ditangani apakah disingkirkan?	Karena memang belum ada petugas yang menangani khusus untuk barang bukti yang berbentuk digital, maka dari beberapa kasus barang bukti tersebut kami gunakan sebagai alat bukti dalam persidangan
4. Selama ini jika menemukan bukti-bukti yang berupa digital apakah benar ditangani sampai pada proses persidangan.	Belum
5. Kenapa barang bukti yang berupa digital tidak menjadi perhatian di Polda Lampung?	Karena tidak ada petugas yang menangani
6. Bagaimana jika saya membantu menerapkan sistem yang berhubungan dengan forensik digital diperbolehkan?	Tentu diperbolehkan jika anda memang berkenan, karena memang selama ini belum ada dari pihak kepolisian yang menangani

4.2 Identifikasi Masalah

Metode yang digunakan pada Polda Lampung khususnya dalam penanganan barang bukti digital masih menggunakan metode manual. Seringkali barang bukti digital yang ditemukan oleh tim penyidik dalam bentuk *file* dan dilindungi oleh kata kunci *(password).* Sehingga tim penyidik pada Polda Lampung membutuhkan alat yang bisa membobol *password* untuk proses penyidikan. Oleh karena itu, dibangun sebuah aplikasi yang diberi nama *RAR Recovery.* Aplikasi ini mampu membobol *password* suatu *file* dalam format RAR.

4.3 Aplikasi RAR *Recovery* dan Pembahasan

Aplikasi *RAR Recovery* adalah aplikasi dengan kemampuan membobol *password* suatu *file* dalam format rar. Aplikasi ini dilengkapi dengan dua pilihan metode diantaranya *brute force attack* dan *dictionary attack.* Metode *brute force attack* adalah teknik membobol *password* dengan semua kemungkinan kunci yang mungkin. Selanjutnya metode *dictionary attack* adalah teknik membobol *password* dengan cara mencari *password* pada ketersediaan kamus.

File dalam format RAR dengan ukuran *file,* panjang *password*, dan kerumitan *password* yang berbeda-beda tentunya akan menghasilkan waktu yang berbeda pula.

Cara pemakaian aplikasi ini di mulai dari memasukkan *file*, pilih metode yang akan dipakai, jika *brute force attack,* maka pilih *chekbox* pada *definition file*, jika *dictionary* yang dipilih, maka proses akan secara otomatis mencari *password* pada kamus yang telah disediakan dalam program *RAR Recovery* ini. Kemudian memulai proses dengan menekan tombol *start* hingga proses berakhir, maka akan muncul pesan validasi yang memberitahukan bahwa proses berhasil, dan klik Ok, lalu pada tampilan status windows muncul keterangan *password* yang telah ditemukan, sudah berapa banyak *password* yang dicoba, banyaknya pencarian *password* per-detik, dan lama waktu.

Gambar 4.1 Tampilan *RAR Recovery*

Pada tampilan aplikasi *RAR Recovery* terdapat beberapa parameter, masing-masing mempunyai fungsi yang berbeda. Berikut penjelasannya:

1) RAR File

   Sebelum memulai proses dalam aplikasi ini terlebih dahulu masukkan file yang ter-*password* ke dalam aplikasi ini, sehingga ketika sudah dimasukkan akan tampil pada kolom rar file

2) Pilih Type Of Attack

   Terdapat pilihan metode apakah yang akan dipakai untuk membobol *password*, terdapat dua pilihan yang tersedia pada aplikasi ini yaitu *brute force* dan *dictionary*.

3) *Definition File*.

   Proses *brute force* memerlukan konfigurasi sebelum dijalankan. Konfigurasi ini dibuat dan disimpan dalam apa yang dinamakan *definition file.* Karena luasnya kemungkinan karakter yang mungkin menjadi *password*, maka

definition file digunakan untuk memberikan batasan dan tingkatan *brute force* harus dilaksanakan pada area karakter tersempit terlebih dahulu baru kemudian dilanjutkan ke area yang lebih luas. Umumnya *definition file* dibuat untuk memberikan batasan pada angka saja terlebih dahulu, kemudian dilanjutkan huruf kecil saja, kemudian dilanjutkan huruf besar saja dan seterusnya.

4) Panjang Min.

   Panjang minimum menunjukkan berapa panjang minimum *password* yang akan dipakai untuk menebak *password* dengan kemungkinan-kemungkinan kunci yang mungkin.

5) Panjang Max.

   Panjang maksimum menunjukkan berapa panjang maksimum *password* yang akan dipakai untuk menebak *password* dengan kemungkinan-kemungkinan kunci yang mungkin.

6) Status Windows

   Terdapat kolom kosong untuk mengisi keterangan *password* apakah yang sudah ditemukan, berapa banyak *password* yang telah dicoba, banyaknya pencarian *password* per-detik, dan lama waktu proses.

7) Progress Indicator

   Menunjukkan keaktifan pada saat proses sedang berjalan. Dimulai dari menekan tombol *start* dan berakhir pada saat *password* ditemukan.

8) Start

   Tombol start digunakan pada saat akan memulai proses pencarian *password*.

9) Stop

   Menghentikan proses yang sedang berjalan.

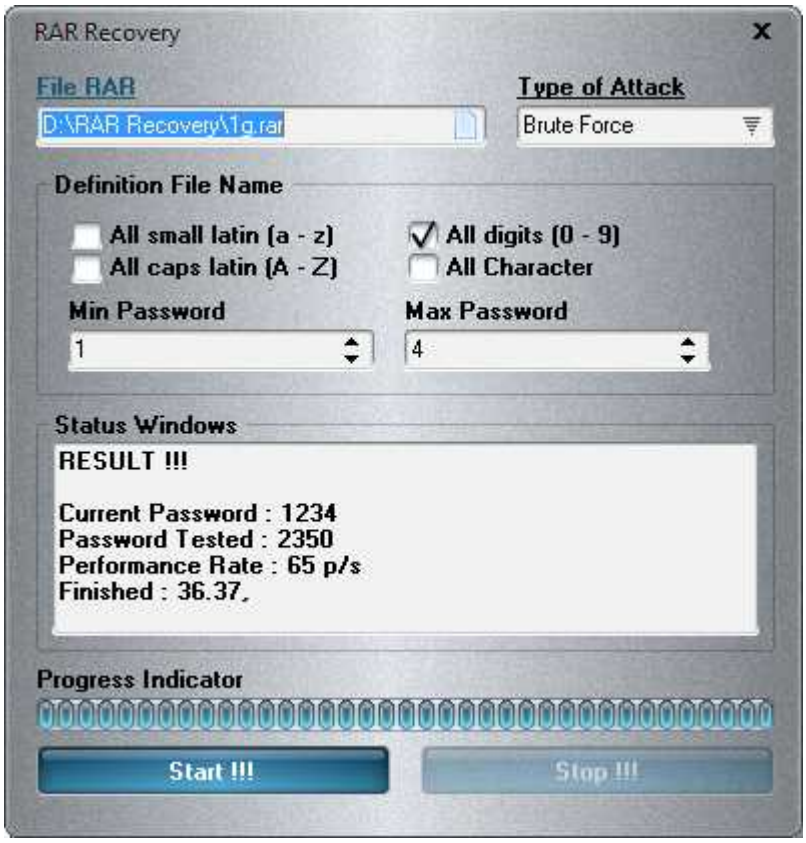
4.3 Pengujian Aplikasi

Pada tahap ini dilakukan pengujian aplikasi *RAR Recovery*, merupakan pengujian program dengan mengutamakan pengujian terhadap penemuan *password.* Pengujian dilakukan dengan menguji beberapa skenario yang ada dan juga pengujian pada sistem interface yang responsive sehingga pengujian mendapat keberhasilan dalam menebak *password.*

Tabel 4.3 Tabel Skenario Uji Coba Ukuran File Dengan Metode *Brute Force Attack*

Skenario	**Keterangan**	**Waktu (hh:mm:ss)**
Skenario ukuran file	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 4	Current Password: 1234 Password tested : 2350 Performance Rate : 140 p/s finished : 00:00:16
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 1Mb dan panjang *password* 4	Current Password: 1234 Password tested : 2350 Performance Rate : 140 p/s finished : 00:00:59
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 2Mb dan panjang *password* 4	Current Password: 1234 Password tested :2350 Performance Rate : 142p/s finished : 00:00:16
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 3Mb dan panjang *password* 4	Current Password: 1234 Password tested :2350 Performance Rate : 142p/s finished : 00:00:16
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 4Mb dan panjang *password* 4	Current Password: 1234 Password tested :2350 Performance Rate :144 p/s finished : 00:00:16

Skenario	Keterangan	Waktu (hh:mm:ss)
Skenario ukuran file	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 5Mb dan panjang *password* 4	Current Password: 1234 Password tested :2350 Performance Rate : 144p/s finished : 00:00:16
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 6Mb dan panjang *password* 4	Current Password: 1234 Password tested :2350 Performance Rate :144 p/s finished : 00:00:16
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 7Mb dan panjang *password* 4	Current Password: 1234 Password tested :2350 Performance Rate : 144p/s finished : 00:00:16
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 8Mb dan panjang *password* 4	Current Password: 1234 Password tested :2350 Performance Rate : 144p/s finished : 00:00:17
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 9Mb dan panjang *password* 4	Current Password: 1234 Password tested :2350 Performance Rate :144 p/s finished : 00:00:17
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 10Mb dan panjang *password* 4	Current Password: 1234 Password tested : 2340 Performance Rate : 144 p/s finished : 00:00:17
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100Mb dan panjang *password* 4	Current Password: 1234 Password tested : 2380 Performance Rate : 144 p/s finished : 00:00:19
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 1Gb dan panjang *password* 4	Current Password: 1234 Password tested : 2380 Performance Rate : 144 p/s finished : 00:00:36



Gambar 4.2 Uji Coba Ukuran File Dengan Metode *Brute Force Attack*

Tabel 4.4 Tabel Skenario Uji Coba Ukuran File Dengan Metode *Dictionary Attack*

Skenario	**Keterangan**	**Waktu (hh:mm:ss)**
Skenario ukuran file	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 4.	Current Password:1234 Password tested : 264 Performance Rate : 132 p/s finished : 00:00:01
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 1Mb dan panjang *password* 4.	Current Password: 1234 Password tested : 164 Performance Rate : 132 p/s finished : 00:00:01

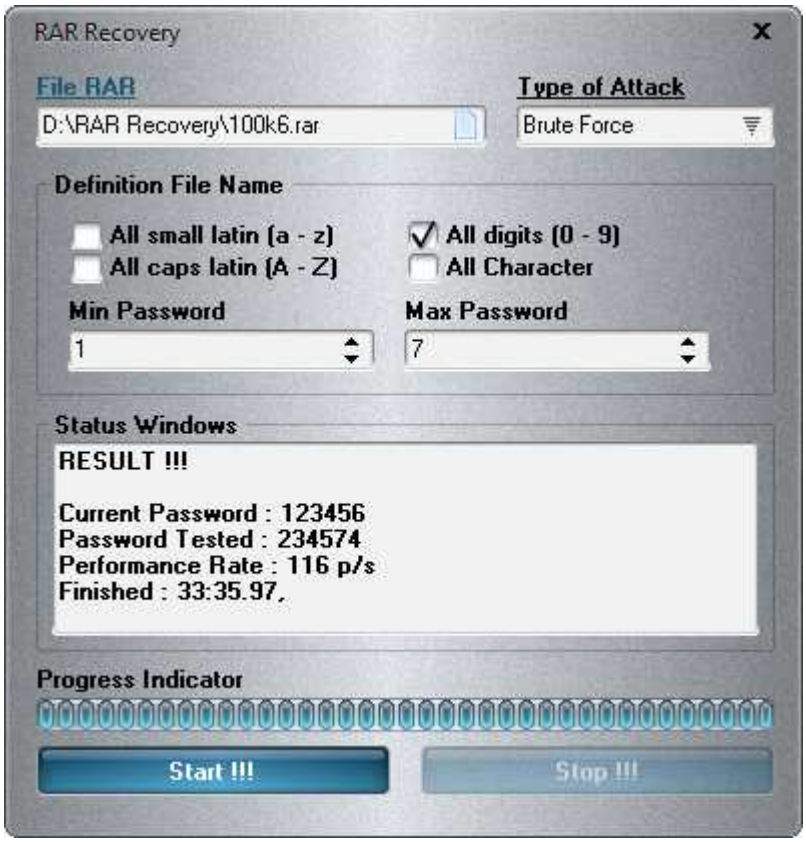
Skenario	Keterangan	Waktu (hh:mm:ss)
Skenario ukuran file	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 9Mb dan panjang *password* 4.	Current Password: 1234 Password tested : 264 Performance Rate : 132 p/s finished : 00:00:04
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 10Mb dan panjang *password* 4.	Current Password: 1234 Password tested : 264 Performance Rate : 132 p/s finished : 00:00:05
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 100Mb dan panjang *password* 4.	Current Password: 1234 Password tested : 264 Performance Rate : 78 p/s finished : 00:00:05
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 1Gb dan panjang *password* 4.	Current Password: 1234 Password tested : 264 Performance Rate : 13 p/s finished : 00:00:19
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 9Mb dan panjang *password* 4.	Current Password: 1234 Password tested : 264 Performance Rate : 132 p/s finished : 00:00:04
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 10Mb dan panjang *password* 4.	Current Password: 1234 Password tested : 264 Performance Rate : 132 p/s finished : 00:00:05
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 100Mb dan panjang *password* 4.	Current Password: 1234 Password tested : 264 Performance Rate : 78 p/s finished : 00:00:05
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 1Gb dan panjang *password* 4.	Current Password: 1234 Password tested : 264 Performance Rate : 13 p/s finished : 00:00:19

Gambar 4.3 Uji Coba Ukuran File Dengan Metode *Dictionary Attack*

Table 4.5 Tabel Skenario Uji Coba Panjang *Password* Dengan Metode *Brute Force Attack*

Skenario	**Keterangan**	**Waktu (hh:mm:ss)**
Skenario panjang *password*	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 1	Current Password: 1 Password tested : 8 Performance Rate : 45 p/s finished : 00:00:00
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 2	Current Password: 12 Password tested : 26 Performance Rate : 118 p/s finished : 00:00:00

Skenario	Keterangan	Waktu (hh:mm:ss)
Skenario panjang *password*	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 3	Current Password: b123 Password tested : 238 Performance Rate : 150 p/s finished : 00:00:01
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 4	Current Password: 1234 Password tested : 2350 Performance Rate : 141 p/s finished : 00:30:16
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 5	Current Password: 12345 Password tested : 23462 Performance Rate : 129 p/s finished : 00:03:02
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 6	Current Password: 123456 Password tested : 234574 Performance Rate : 116 p/s finished :00:33:35
	Perangkat lunak melakukan *Brute Force Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 7	Current Password: 1234567 Password tested : Performance Rate p/s finished : 00:34:48



Gambar 4.4 Uji Coba Panjang *Password* Dengan Metode *Brute Force Attack*

Table 4.6 Tabel Skenario Uji Coba Panjang *Password* Dengan Metode Dictionary Attack

Skenario	**Keterangan**	**Waktu**
Skenario panjang password	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 1.	Current Password: 1 Password tested : 69 Performance Rate : 1165p/s finished : 00:00:00
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 2	Current Password: 12 Password tested : 78 Performance Rate : 116 p/s finished : 00:00:00

Skenario	Keterangan	Waktu
Skenario panjang password	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 3	Current Password: 123 Password tested : 184 Performance Rate : 139 p/s finished : 00:00:01
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 4	Current Password: 1234 Password tested : 264 Performance Rate : 138 p/s finished : 00:00:02
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 5	Current Password: 12345 Password tested : 280 Performance Rate : 126 p/s finished : 00:00:02
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 6	Current Password: 123456 Password tested : 287 Performance Rate : 120 p/s finished : 00:00:02
	Perangkat lunak melakukan *Dictionary Attack* terhadap file (RAR) berkapasitas 100kb dan panjang *password* 7	Current Password: 1234567 Password tested : 288 Performance Rate : 118 p/s finished : 00:00:03

Gambar 4.5 Uji Coba Panjang *Password* Dengan Metode *Dictionary Attack*

BAB V
SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan percobaan yang telah dilakukan, dapat diambil kesimpulan yaitu:

a. Aplikasi RAR *Recovery* bersifat fleksibel karena mudah dalam penggunaannya.
b. Aplikasi RAR *Recovery* mempunyai kemampuan lebih handal dalam hal memproteksi *file* yang ber-*password* karena menngunakan teknologi CUDA untuk mempercepat proses pencarian *password.*
c. Penggunaan Aplikasi RAR *Recovery* diprioritaskan bagi tim penyidik bagian *digital forensics* yang ada di Polda Lampung.
d. Dengan menerapkan Aplikasi RAR *Recovery* ini, mampu menjawab kebutuhan penyidik *digital forensics* dalam pekerjaannya.

5.2 Saran

Berdasarkan analisa kesimpulan diatas, ada beberapa saran yang penulis coba cermati yaitu:

a. Pengembangan konsep dapat diperluas dengan tambahan parameter yang lebih baik. Dengan penambahan *symbol* dan *space* mampu menjadikan konsep ini menjadi lebih lengkap untuk digunakan.
b. Dalam pengembangan selanjutnya dimungkinkan akan ada paket yang lebih baik sehingga lebih mudah diimplementasikan.
c. Implementasi paket-paket dengan Delphi sebaiknya menggunakan Delphi terbaru. Saat ini Delphi yang digunakan Borland Delphi 7.

DAFTAR PUSTAKA

Dwi Hartanto, Anggit., Utami, Ema., Al Fatta, Hanif. 2011. Penerapan Teknik Komputer Forensic Untuk Pengembalian Dan Penghapusan Berkas Digital. Yogyakarta. STMIK AMIKOM

Kadir, Abdul. 2004. Pemrograman Database Dengan Delphi 7 Menggunakan Access Dan Ado. Unit Penerbit dan Percetakan Andi, Yogyakarta.

Pressman, Rogers S. 2012. Rekayasa Perangkat Lunak buku 1. (Alih Bahasa Adi Nugroho; George John Leopold Nikijuluw; Theresia Herlina Rachadiani; Ike Kurniawati Wijaya,ST,MT). Penerbit Andi, Yogyakarta.

Pressman, Rogers S. 2010. Software Engineering: A Practitioner's Approach (8rd ed). Publisher, McGraw-Hill.

Stalling, Williams 2005. Cryptography And Network Security. Publisher, Prentice Hall.

Sulianta, Feri. 2015. Menjebol Sekaligus Mengamankan Password. Unit Penerbit dan Percetakan Andi, Yogyakarta.

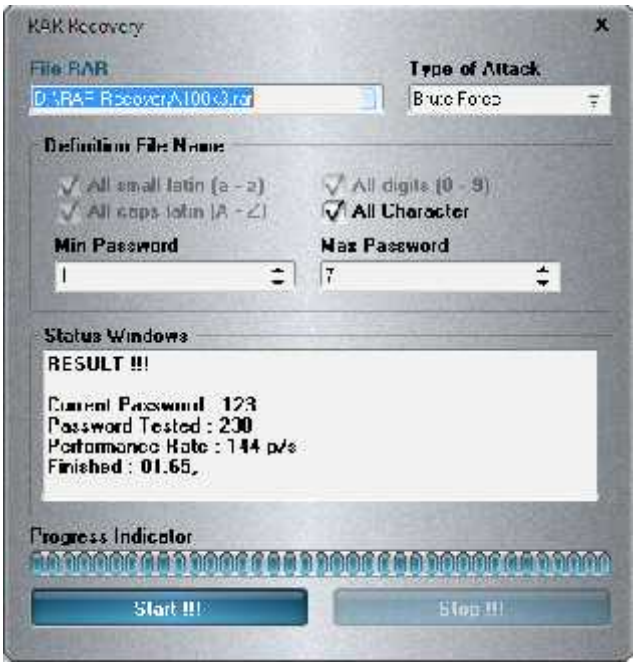
Suprapto, Eko. 2012. Peran Komputer Forensik Dalam Penegakan Hukum Untuk Pembuktian Kasus Cyber Crime. Jambi. Batanghari.

LAMPIRAN

Lampiran A Uji Coba Ukuran File

Gambar L.1 Uji Coba Ukuran File Dengan Metode *Brute Force Attack* Panjang *Password* 1

Gambar L.2 Uji Coba Ukuran File Dengan Metode *Brute Force Attack* Panjang *Password* 2

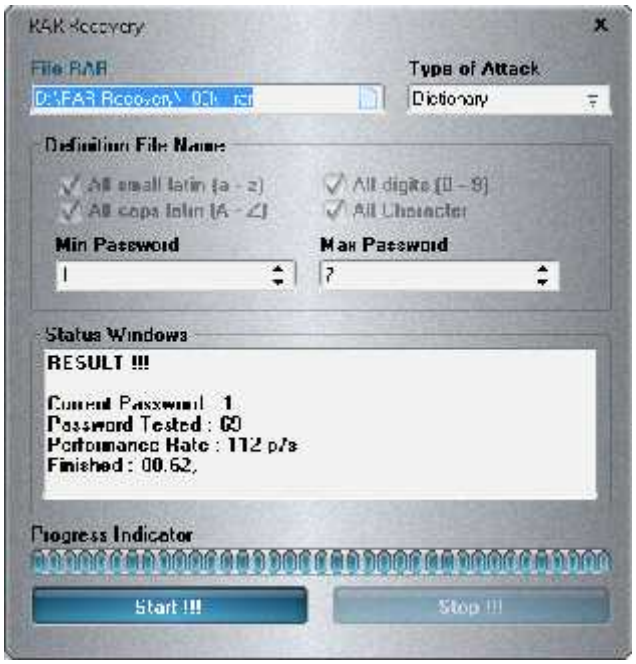


Gambar L.3 Uji Coba Ukuran File Dengan Metode *Brute Force Attack* Panjang *Password* 3

Gambar L.4 Uji Coba Ukuran File Dengan Metode *Brute Force Attack* Panjang *Password* 4

Gambar L.5 Uji Coba Ukuran File Dengan Metode *Brute Force Attack* Panjang *Password* 5

Gambar L.6 Uji Coba Ukuran File Dengan Metode *Brute Force Attack* Panjang *Password* 7

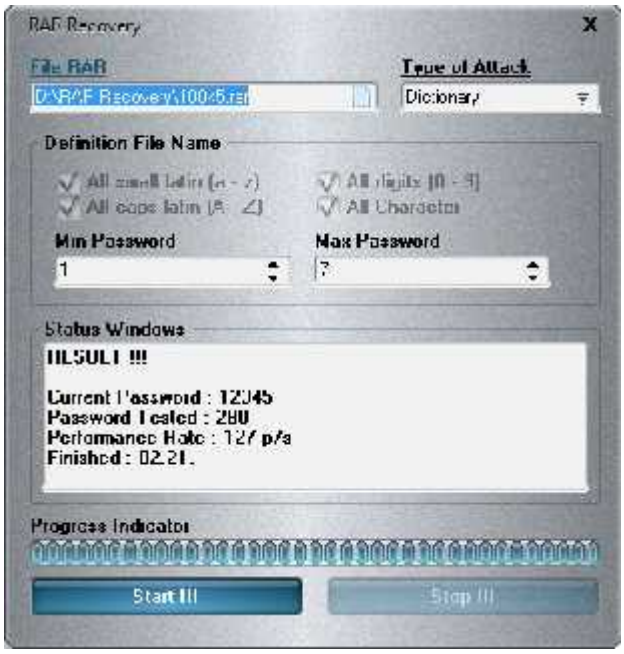


Gambar L.7 Uji Coba Ukuran File Dengan Metode *Dictionary Attack* Panjang *Password* 1

Gambar L.8 Uji Coba Ukuran File Dengan Metode *Dictionary Attack* Panjang *Password* 2

Gambar L.9 Uji Coba Ukuran File Dengan Metode *Dictionary Attack* Panjang *Password* 3

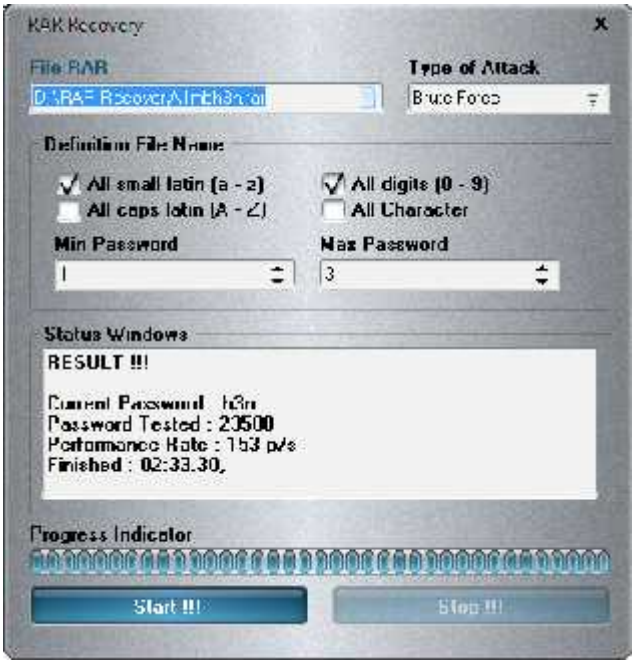
Gambar L.10 Uji Coba Ukuran File Dengan Metode *Dictionary Attack* Panjang *Password* 4



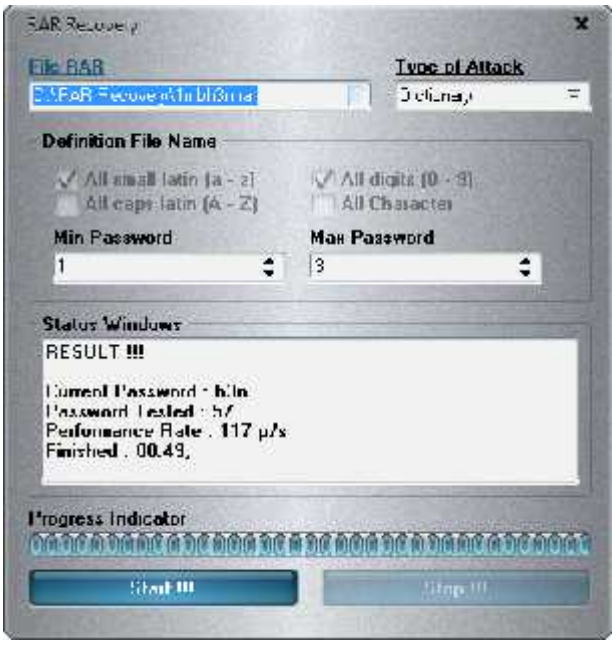
Gambar L.11 Uji Coba Ukuran File Dengan Metode *Dictionary Attack* Panjang *Password* 5

Gambar L.12 Uji Coba Ukuran File Dengan Metode *Dictionary Attack* Panjang *Password* 6

Gambar L.13 Uji Coba Ukuran File Dengan Metode *Dictionary Attack* Panjang *Password* 7



Gambar L.14 Uji Coba Ukuran File Dengan Metode *Brute Force Attack* Panjang *Password* 3(acak)



Gambar L.15 Uji Coba Ukuran File Dengan Metode *Dictionary Attack* Panjang *Password* 3(acak)

Lampiran B Laporan Kasus Pada Polda

KEPOLISIAN NEGARA REPUBLIK INDONESIA
DAERAH LAMPUNG
SENTRA PELAYANAN KEPOLISIAN TERPADU

" PRO JUSTITIA "

Kejahatan >
Pelanggaran >Yang dilaporkan
Lain-lain >

LAPORAN POLISI
Nomor:LP / B-501 / V / 2016 / Lpg / SPKT

YANG MELAPOR	
N A M A	: EDY YANTO
TEMPAT / TGL LAHIR	: MENGGALA, 15 OKTOBER 1970
JENIS KELAMIN	: LAKI LAKI
PEKERJAAN	: WIRASWASTA
ALAMAT	: P. KARUNIA INDAH BLOKE E4 NO 9 DESA/KEL SUKABUMI INDAH KEC. SUKABUMI KOTA BANDAR LAMPUNG
TELP/FAX/EMAIL	: 085377057511
AGAMA	: ISLAM
KEWARGANEGARAAN	: INDONESIA
PERKARA	: PENIPUAN
1. WAKTU KEJADIAN	: PADA BULAN MARET 2016
2. TEMPAT KEJADIAN	: DI SHOWROOM JAPANESE ANTASARI BANDAR LAMPUNG
3. APA YANG TERJADI	: PENIPUAN
4. BAGAIMANA TERJADI	: PELAPOR MEMBELI MOBIL DARI SHOWROOM JAPANESE ANTASARI DENGAN CARA DIANGSUR, KEMUDIAN MOBIL TERSEBUT DISITA OLEH POLISI KARENA DIDUGA HASIL KEJAHATAN.
5. DILAPORKAN	: PADA HARI KAMIS, 12 MEI 2016
6. SIAPA	
a. KORBAN	: PELAPOR
b. TERLAPOR	: SHOWROOM JAPANESE
7. SAKSI-SAKSI	
1.NAMA	: SANDRI
JENISKELAMIN	: LAKI LAKI
UMUR	: 31 TAHUN
PEKERJAAN	: SWASTA
ALAMAT	: BRABASAN RT/RW 03/06 KEC. TANJUNG RAYA KAB.] MESUJI
2.NAMA	: -
JENISKELAMIN	: -

Gambar L.16 Laporan Halaman Pertama Kasus Pada Polda Lampung

-2-

URAIAN KEJADIAN

—— Pada Bulan Maret 2016 telah terjadi tindak pidana Penipuan yang dilakukan oleh terlapor. bahwa pelapor membeli 1 unit mobi Honda Jazz berwarna Merah dengan nomor polisi BG 2826 NG, nomor rangka MRHGD37804P011303 dan nomor mesin L15A41703238 dari sebuah Showroom yang beralamat di Jl. Pangeran Antasari Bandar Lampung. mobil tersebut dibeli dengan cara kredit melalui jasa pembiayaan PT. CIMB Niaga Auto Finance yang beralamat di jl. Wolter Monginsidi Bandar Lampung selama 4 (empat) tahun dengan DP sebesar Rp. 30.000.000,- (tiga puluh juta rupiah). Pelapor sudah membayar angsuran tersebut selama 30 bulan. Kemudian datang pihak leasing lain yaitu PT. Batavia Prosperindo Finance cabang Bandar Lampung akan mengambil mobil tersebut karena angsuran mobil tersebut tidak dibayar. Kemudian pada tanggal 07 November 2015 oleh Polsek Terbanggi Besar Resor Lampung Tengah melakukan penyitaan mobil tersebut berdasarkan Laporan Polisi Nomor :LP/775-A/XI/2015/Res LT/ Sek Tebas karena diduga mobil tersebut dalam keadaan bermasalah. Akibat kejadian tersebut pelapor melaporkan terlapor ke Polda Lampung guna dilakukan penyelidikan lebih lanjut.

Pelapor atau Pengadu memberikan keterangannya, kemudian membubuhkan tanda tangannya dibawah ini.

Pelapor

EDY YANTO

CATATAN KEPOLISIAN :

TINDAKAN YANG DIAMBIL:

a. Membuat Laporan Polisi
b. Membuat tanda bukti lapor
c. Menerima Barang bukti

TINDAK PIDANA APA : PENIPUAN
BARANG BUKTI : Terlampir.

MENGETAHUI
A.n. KEPALA KEPOLISIAN DAERAH LAMPUNG
KA SPKT
U.b
KA SIAGA SPKT I

M. LUMBAN GAOL
KOMPOL NRP 62040869

Bandar Lampung, 12 Mei 2016
Yang Menerima Laporan
BA YANMAS I

JHON E.J SITUMORANG
BRIPKA NRP 83090074

Gambar L.17 Laporan Halaman Kedua Kasus Pada Polda Lampung

Lampiran C Listen Program

```
//coding type of attack
unit uRAR;
interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, StdCtrls, Mask, sMaskEdit, sCustomComboEdit, sTooledit, XPMan,
  sLabel, sComboEdit, sCheckBox, ExtCtrls, sPanel, sGroupBox, sComboBox,
  sEdit, sSpinEdit, sMemo,shellapi, sButton, ComCtrls, acProgressBar,TlHelp32,
  sSkinManager;

type
  TfrmRAR = class(TForm)
    sWebLabel1: TsWebLabel;
    XPManifest1: TXPManifest;
    edFile: TsFilenameEdit;
    sGroupBox1: TsGroupBox;
    cbLatinkecil: TsCheckBox;
    cbLatinbesar: TsCheckBox;
    cbDigit: TsCheckBox;
    sLabel1: TsLabel;
    cbAttack: TsComboBox;
    sLabel2: TsLabel;
    cbPilihsemua: TsCheckBox;
    sLabel3: TsLabel;
    sGroupBox2: TsGroupBox;
    mmStatus: TsMemo;
```

```
    bStart: TsButton;
    edMinpass: TsDecimalSpinEdit;
    edMaxpass: TsDecimalSpinEdit;
    Timer1: TTimer;
    sProgressBar1: TsProgressBar;
    sLabel4: TsLabel;
    bStop: TsButton;
    sSkinManager1: TsSkinManager;
    procedure FormCreate(Sender: TObject);
    procedure cbPilihsemuaClick(Sender: TObject);
    procedure cbAttackChange(Sender: TObject);
    procedure bStartClick(Sender: TObject);
    procedure Timer1Timer(Sender: TObject);
    procedure bStopClick(Sender: TObject);

private
    { Private declarations }
 procedure brute;
    procedure createFile(s: String);
    procedure createRAR(s,namaFile: String);
  public
    { Public declarations }
  end;
var
  frmRAR: TfrmRAR;

implementation
```

```
{$R *.dfm}

function KillTask(ExeFileName: string): Integer;
const
  PROCESS_TERMINATE = $0001;
var
  ContinueLoop: BOOL;
  FSnapshotHandle: THandle;
  FProcessEntry32: TProcessEntry32;

procedure TfrmRAR.brute;
begin
  edFile.Clear;
  cbAttack.Text := 'Pilih Type Attack';

  cbLatinkecil.Checked := false;
  cbLatinbesar.Checked := false;
  cbDigit.Checked := false;
  cbPilihsemua.Checked := false;

  mmStatus.Lines.Clear;

  cbLatinkecil.Enabled := false;
  cbLatinbesar.Enabled := false;
  cbDigit.Enabled := false;
  cbPilihsemua.Enabled := false;

  edMinpass.Enabled := false;
```

```
  edMaxpass.Enabled := false;
  mmStatus.Enabled := false;
  sProgressBar1.Min := 0;

 sProgressBar1.Max := 0;
  sProgressBar1.Position := 0;

  Timer1.Interval := 0;
  Timer1.Enabled := false;

  bStart.Enabled := true;
  bStop.Enabled := false;

end;

procedure TfrmRAR.FormCreate(Sender: TObject);
begin
  brute;
end;

procedure TfrmRAR.cbPilihsemuaClick(Sender: TObject);
begin
  if cbPilihsemua.Checked = true then
  begin
    cbLatinkecil.Enabled := false;
    cbLatinbesar.Enabled := false;
    cbDigit.Enabled := false;
```

```
    cbLatinkecil.Checked := true;
    cbLatinbesar.Checked := true;
    cbDigit.Checked := true;
    exit;
  end;

  if cbPilihsemua.Checked = false then
  begin
    cbLatinkecil.Enabled := true;
    cbLatinbesar.Enabled := true;
    cbDigit.Enabled := true;

    cbLatinkecil.Checked := false;
    cbLatinbesar.Checked := false;
    cbDigit.Checked := false;
    exit;
  end;
end;
procedure TfrmRAR.cbAttackChange(Sender: TObject);
begin

  if cbAttack.Text = 'Brute Force' then
  begin
    cbLatinkecil.Enabled := true;
    cbLatinbesar.Enabled := true;
    cbDigit.Enabled := true;
    cbPilihsemua.Enabled := true;
    edMinpass.Enabled := true;
```

```
    edMaxpass.Enabled := true;
    mmStatus.Enabled := true;
    exit;
  end;
  if cbAttack.Text = 'Dictionary' then
  begin
    cbLatinkecil.Enabled := false;
    cbLatinbesar.Enabled := false;
    cbDigit.Enabled := false;
    cbPilihsemua.Enabled := false;
    edMinpass.Enabled := true;
    edMaxpass.Enabled := true;
    mmStatus.Enabled := true;
    exit;
  end;
end;

procedure TfrmRAR.bStartClick(Sender: TObject);
var
  stat,currentDir: String;
begin
  currentDir := ExtractFilePath(Application.ExeName);
  if (edFile.Text = '') then
  begin
    MessageDlg('File RAR Masih Kosong !!', mtWarning, [mbYes],0);
    edFile.SetFocus;
    exit;
  end;
```

```
 if (cbAttack.Text = 'Pilih Type Attack') then
 begin
   MessageDlg('Pilih Type Attack !!', mtWarning, [mbYes],0);
   cbAttack.SetFocus;
exit;
 end;
 if (cbAttack.Text = 'Brute Force') then
 begin
   if (cbLatinbesar.Checked = false)and(cbLatinkecil.Checked = false)and
       (cbDigit.Checked = false) and (cbDigit.Checked = false) then
   begin
     MessageDlg('Destination File Name Kosong !!',mtWarning,[mbYes],0);
     exit;
   end;
   if (cbLatinkecil.Checked = True) then stat := 'huruf_kecil.def';
   if (cbLatinbesar.Checked = True) then stat := 'huruf_besar.def';
   if (cbLatinbesar.Checked = True)and(cbLatinkecil.Checked = True) then stat :=
'huruf_kecil_besar.def';
   if (cbDigit.Checked = True) then stat := 'angka.def';
   if (cbDigit.Checked = True)and(cbLatinbesar.Checked = True) then stat := 'angka_huruf_besar.def';
   if (cbDigit.Checked = True)and(cbLatinkecil.Checked = True) then stat := 'angka_huruf_kecil.def';
   if (cbPilihsemua.Checked = True) then stat := 'angka_huruf_kecil_besar.def';
   if (edMinpass.Text = '' )or(edMaxpass.Text = '') then
   begin
     MessageDlg('Min/Max Password Kosong !!',mtWarning,[mbYes],0);
     exit;
   end;
   createFile(stat);
```

```
    exit;
  end;
  if (cbAttack.Text = 'Dictionary') then
  begin
    if (edMinpass.Text = '' )or(edMaxpass.Text = '') then
    begin
      MessageDlg('Min/Max Password Kosong !!',mtWarning,[mbYes],0);
      exit;
    end;
    createFile('kamus.def');
    exit;
  end;
end;

procedure TfrmRAR.Timer1Timer(Sender: TObject);
begin
  sProgressBar1.Position :=  sProgressBar1.Position + 1;
end;
procedure TfrmRAR.createFile(s: String);
var
  getSTR, maxL,minL: String;
  Lines: TStringList;
FileName,currentDir,hasil,msg: String;
Begin
  KillTask('crark.exe');
  KillTask('cmd.exe');
  currentDir := ExtractFilePath(Application.ExeName);
  FileName := 'cek.bat';
```

```
  hasil := PChar(''+currentDir+'hasil.txt'+'');
  msg := PChar(''+currentDir+'msg.txt'+'');

  minL := IntToStr(StrToInt(edMinpass.Text));
  maxL := IntToStr(StrToInt(edMaxpass.Text));
 end;
end;

procedure TfrmRAR.createRAR(s,namaFile: String);
var
  seinfo: tshellexecuteinfo;
  exitcode: dword;
  executefile: string;
  startinstring: string;
begin
  bStart.Enabled := false;
  sProgressBar1.Position := 0;
  mmStatus.Enabled := true;
  mmStatus.Lines.Clear;

  fillchar(seinfo, sizeof(seinfo),0);
  seinfo.cbSize :=sizeof(tshellexecuteinfo);
  bStop.Enabled := true;
  with seinfo do
  begin
    fMask := see_mask_nocloseprocess;
    wnd := application.Handle;
    executefile:=pChar(s);
```

```
    lpfile:=pchar(executefile);
    lpdirectory:=pchar(startinstring);
    nshow:=SW_HIDE;



  end;
  if shellexecuteex(@seinfo) then
  begin
   repeat
      sProgressBar1.Min := 0;
  sProgressBar1.Max := 100;
      Timer1.Interval := 1000;


      Timer1.Enabled := true;
      application.ProcessMessages;
      getexitcodeprocess(seinfo.hProcess, exitcode);
    until (exitcode <> still_active) or application.Terminated;
      sProgressBar1.Position := 100;
      MessageDlg('Sukses !!',mtInformation,[mbYes],0);
      Timer1.Interval := 0;
      Timer1.Enabled := false;
      mmStatus.Lines.LoadFromFile(namaFile);
      bStart.Enabled := true;
      bStop.Enabled := false;
    end
  else
    MessageDlg('Terjadi Kesalahan !!',mtError,[mbYes],0);
end;
```

```
//coding start
procedure TfrmRAR.bStopClick(Sender: TObject);
begin
  KillTask('crark.exe');
  KillTask('cmd.exe');
  FormCreate(sender);
end;

end.

//coding timer
procedure TfrmRAR.Timer1Timer(Sender: TObject);
begin
  sProgressBar1.Position :=  sProgressBar1.Position + 1;
end;
```