ANALISIS DAN IMPLEMENTASI *MOBILE* FORENSIK PEMULIHAN DATA YANG HILANG PADA *SMARTPHONE* BERBASIS SISTEM OPERASI ANDROID

ANALYSIS AND IMPLEMENTATION OF MOBILE FORENSIC RECOVERY DATA LOST ON ANDROID SMARTPHONE OPERATING SYSTEM

Ahmad Thufail A.[1], Surya Michrandi N.,ST.,MT.[2],Budhi Irawan,SSi.,MT.[3]

[1,2,3]Prodi S1 Sistem Komputer, Fakultas Teknik, Universitas Telkom
[1]thufailagusta@gmail.com , [2] **surya.michrandi@gmail.com**, [3]**budhi.ira1@gmail.com**

Abstrak

Seiring perkembangan jaman, bidang ilmu forensik telah mengalami perkembangan yang pesat. Ilmu forensik ini pun meluas ke bidang-bidang teknologi baru mulai dari digital forensik, komputer forensik dan juga *mobile* forensik. *Mobile* forensik dalam menganalisa dan pengumpulan data didapat dari berbagai sumber daya, misalnya sistem operasi, jalur komunikasi dan juga berbagai media penyimpanan. Sistem operasi pada *mobile* yang sangat popular dimasa ini adalah *smartphone* berbasis sistem operasi android. Dengan kemajuan teknologi, android sudah mendukung media penyimpanan data yang canggih. Dalam perangkat android bisa menyimpan data berupa teks, suara, gambar dan video. Dengan kecanggihan teknologi android tersebut, oleh pelaku kriminal bisa dijadikan media kriminalitas mulai dari menyimpan ide kejahatan, target kejahatan dan skenario kejahatan. dan setelah melakukan kejahatan, data yang ada dalam perangkat android tersebut akan dihapus oleh pelaku.
Pada Tugas Akhir ini telah dibuat aplikasi *mobile* forensik untuk mendapatkan data SMS dan data CDR yang sudah dihapus didalam *smartphone* android menggunakan eclipse dan bahasa java. Pengguna dapat sekedar menampilkan data SMS dan data CDR atau menyimpannya kembali kedalam memori *smartphone*.
Aplikasi ini dapat memulihkan 100% data SMS dan data CDR dalam kondisi sebelum *factory reset*. Setelah dilakukan *factory reset*, dapat dipulihkan 40% data SMS dan 20% data CDR. Tetapi data setelah dilakukan *flash ROM* tidak dapat dipulihkan karena *flash ROM* mengubah ROM lama menjadi ROM baru.

Kata kunci : Forensik, Mobile forensik, Android, Java.

Abstract

In this changing world, forensic studies have developed with rapidly. These studies are used on technological fields with digital forensic, computer forensic and mobile forensic as the examples. Mobile forensic uses various sources like operating system, communication line, and media storages to analyse and gather data. Most popular mobile operating system is Android. With the growing of the technology, android supports modern data storage. Texts, voices, pictures, and videos can be saved by the operating system. Using that ability, evil-doers can save criminal ideas, the targets, and criminal scenarios. After doing criminality, the actor can delete the data on android mobile phone.
In this final project was made a mobile forensic application to get the deleted SMS and CDR data using eclipse and java programming language. Users can show the SMS and CDR or even to save them on to memory storage. This application can restore 100% SMS and CDR data before the factory reset. After factory reset, 40% SMS data and 20% CDR data can be recovered while after flash ROM, no data can be taken back because flash ROM changes previous ROM to the newer one.

Keywords : Forensic, Mobile Forensik, Android, Java.

I. Pendahuluan

Salah satu teknologi yang saat ini menjadi kebutuhan utama manusia adalah ponsel. Salah satu *smartphone* yang populer adalah *smartphone* berbasis sistem operasi android. Namun dengan teknologi ponsel yang canggih tersebut tidak semua digunakan untuk hal yang *positive*, terdapat beberapa oknum yang menggunakannya untuk hal yang *negative* seperti merencanakan tindak kejahatan misalnya pemerasan, penipuan dan transaksi narkoba. Ketika ponsel tersebut sudah digunakan untuk hal *negative*, maka ponsel tersebut bisa dijadikan barang bukti oleh penegak hukum untuk menjerat pelaku kejahatan.

Tetapi bukti seperti sms, *call log* dan data lainnya yang dapat menjadi bukti kejahatan sebagian besar sudah dihapus oleh pelaku untuk menghilangkan jejak. Salah satu solusi untuk permasalahan tersebut adalah dengan membuat aplikasi *mobile* forensik untuk mendapatkan data yang sudah dihapus didalam *smartphone* menggunakan eclipse dan bahasa java.

II. Dasar Teori

2.1 Android

Android adalah *software* untuk perangkat *mobile* yang terdiri dari sistem operasi, *middleware*, dan aplikasi inti. Android berbasis pada linux kernel dengan sebuah mesin virtual yang didesain untuk mengoptimalkan penggunaan sumber daya memori dan *hardware* pada perangkat *mobile*. Salah satu keunggulan android yaitu *source code* yang dapat didistribusikan secara terbuka (*open source*).

2.2 SQLite

SQLite merupakan sebuah *library* proses yang menerapkan serverless (mandiri tanpa server), *zero configuration, database SQL* transaksional. *SQLite* saat ini banyak digunakan dalam aplikasi, termasuk dalam beberapa *high - profile project*. *SQLite* juga merupakan mesin *database SQL embedded* yang berbeda dengan kebanyakan *database SQL* lainnya. *SQLite* tidak memiliki proses server yang terpisah. *SQLite* membaca dan menulis secara langsung ke *disk*.

2.3 Eclipse

Eclipse adalah sebuah *IDE (Integrated Development Environment)* untuk mengembangkan perangkat lunak dan dapat dijalankan di semua *platform*. Berikut ini adalah sifat dari *eclipse* :

a. Multi-platform

Target sistem operasi *eclipse* adalah Microsoft Windows, Linux, Solaris, AIX, HP-UX dan Mac OS X.

b. Mulit-language

Eclipse dikembangkan dengan bahasa pemrograman Java, akan tetapi Eclipse mendukung pengembangan aplikasi berbasis bahasa pemrograman lainnya, seperti C/C++, Cobol, Python, Perl, PHP, dan lain sebagainya.

c. Multi-role

Selain sebagai *IDE* untuk pengembangan aplikasi, Eclipse pun bisa digunakan untuk aktivitas dalam siklus pengembangan perangkat lunak, seperti dokumentasi, test perangkat lunak, pengembangan web, dan lain sebagainya.

2.4 Java

Bahasa Java dikembangkan oleh Sun Microsystem tahun 1991 sebagai bagian dari suatu proyek penelitian untuk mengembangkan *software* bagi konsumen barang-barang elektronik seperti televisi, VCR, toaster dan mesin – mesin lainnya yang dapat dibeli di swalayan. Tujuan penciptaan Java pada waktu itu adalah menjadi suatu program yang berukuran kecil, efisien, dan portable di segala jenis *hardware*. Tujuan yang sama ini membuat Java menjadi satu bahasa yang ideal untuk mendistribusikan program-program yang dapat dijalankan melalui *website* dan juga suatu bahasa pemrograman untuk segala tujuan untuk mengembangkan program-program yang dapat digunakan dengan mudah dan portable di berbagai *platform* yang berbeda.

Sekarang, Sun telah mengeluarkan berbagai program Java yang dapat digunakan seperti Java API, atau JDK atau JAVA Developer Kit . Selain itu, banyak juga program-program lain yang dapat digunakan untuk membuat program Java, seperti Eclipse, NetBeans, JBuilder, JCreator, J++, dan sebagainya.

2.5 Digital Forensik

Digital forensik adalah penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti/informasi yang secara magnetis tersimpan/disandikan pada komputer atau media penyimpanan digital sebagai alat bukti dalam mengungkap kasus kejahatan yang dapat dipertanggungjawabkan secara hukum.

Terdapat 5 level akuisisi data yang dapat dilakukan oleh investigator untuk mendapatkan bukti yang akan mendukung investigasi. Kelima level tersebut adalah :

- *Manual Acquisition.* Yaitu melakukan akuisisi data melalui review secara manual terhadap semua dokumentasi dan data yang berhubungan langsung dengan device.

• *Logical Acquisition.* Yaitu akuisisi dengan cara menghubungkan device dengan kabel koneksi ke komputer melalui bantuan berbagai aplikasi untuk mendapatkan data-data yang umumnya tersimpan pada device.
• *Hex Dump Analysis.* Cara ini dilakukan untuk mendapatkan data-data yang hilang/ rusak atau tersembunyi. Komunitas Hacker umumnya banyak memberikan support terhadap teknik-teknik hex dump analysis ini.
• *Chip-Off method.* Yaitu melakukan proses pembacaan memory chip melalui bantuan perangkat lain seperti EEprom Reader. Cara ini umumnya dapat melakukan ekstraksi terhadap semua data yang tersimpan dalam memori.
• *Micro Read.* Cara ini dilakukan bila kondisi device / memori dalam keadaan rusak sehingga harus ditangani secara khusus melalui sejumlah alat bantu forensika lainnya.

2.6 *Mobile* Forensik

merupakan cabang dari digital forensik yang berkaitan dengan pemulihan bukti digital atau data dari perangkat *mobile*, namun juga dapat berhubungan dengan perangkat digital yang memiliki memori internal dan kemampuan komunikasi.

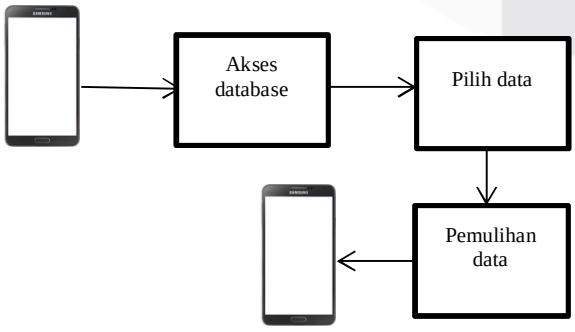
III. Analisis dan Perancangan

3.1 Deskripsi Sistem

Aplikasi *Mobile* forensik berbasis *smartphone* dengan sistem operasi android ini merupakan aplikasi yang mampu menampilkan data SMS, *Call Data Record* dan data Email yang sebelumnya telah dihapus oleh *user*. Kemudian data yang telah dihapus oleh *user* tersebut akan dipulihkan kembali kedalam *smartphone*.

3.2 Gambaran Sistem

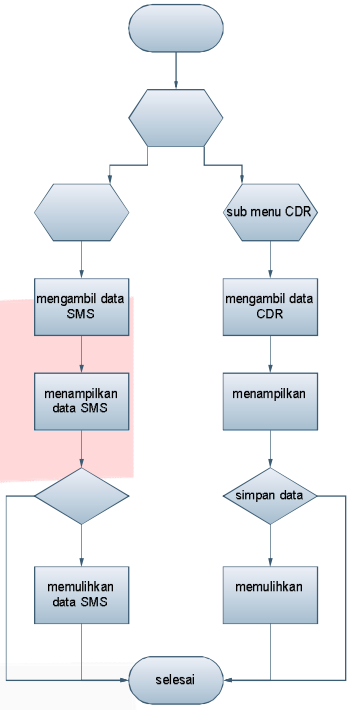
Gambaran umum implementasi sistem dipaparkan sebagai berikut.



Gambar 3.1 gambaran umum sistem

3.3 Diagram Alir

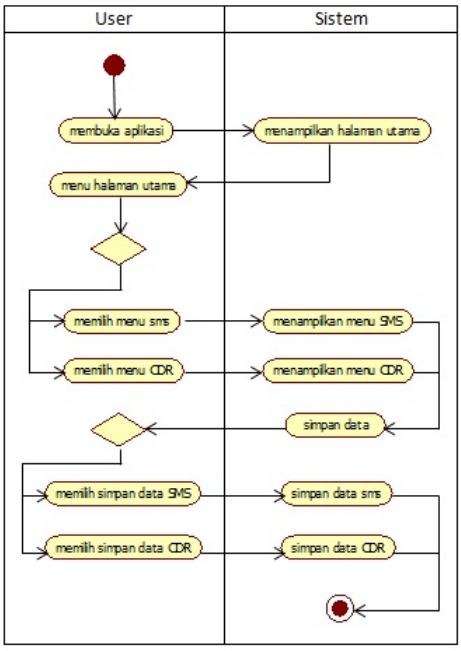
Diagram alir sistem dapat direpresentasikan sebagai berikut.



Gambar 3.2 Diagram Alir

3.3 *Activity* Diagram

Acivity Diagram dari sistem dapat direpresentasikan sebagai berikut.

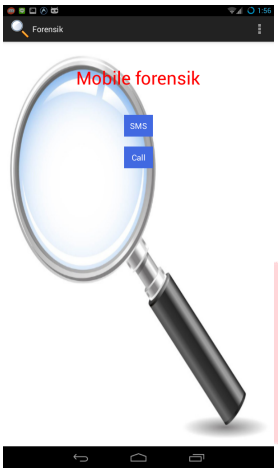


Gambar 3.2 *Activity* Diagram

IV. Implementasi dan Pengujian Sistem

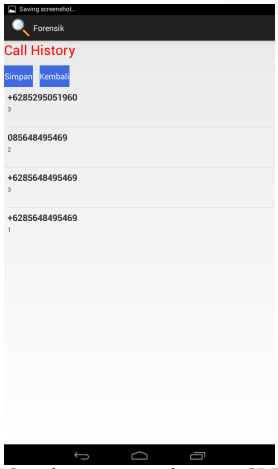
4.1 Implementasi antarmuka

Aplikasi ini diimplementasikan dengan tampilan antarmuka sebagai berikut.



Gambar 4.1 implementasi tampilan awal aplikasi

Gambar 4.2 implementasi tampilan menu sms aplikasi



Gambar 4.3 implementasi tampilan menu CDR aplikasi

4.2 Pengujian Beta

Pengujian beta merupakan pengujian untuk mengetahui apakah aplikasi berjalan sesuai tujuan yang diharapkan. Pengujian Beta dilakukan dengan mengujikan aplikasi ke beberapa orang yang disebut pengguna dan masing-masing pengguna tersebut diberi kuisioner berisi pertanyaan seputar aplikasi.

Pada pengujian ini, jumlah pengguna sebanyak 15 orang. Masing-masing pengguna diminta untuk menggunakan aplikasi kemudian memberikan tanggapan berdasarkan pertanyaan. Berikut ini adalah hasil uji coba yang dilakukan oleh masing-masing 15 orang responden adalah sebagai berikut.

a. Layanan apa yang sering anda gunakan didalam *smartphone ?* *pilih yang paling sering :

   Sebanyak 40% responden memilih SMS dan telp, sedangkan 20% memilih *browser* dan sebanyak 0% memilih Email dan Notes.

b. Sebelumnya apakah anda pernah menggunakan aplikasi sejenis :

   Sebanyak 15 dari 15 orang responden memilih tidak pernah.

c. Seberapa besar kebutuhan anda akan aplikasi ini :

   Sebanyak 67% responden memilih besar, 20% responden memilih cukup dan 13% responden memilih sangat besar

d. Apakah aplikasi ini memfasilitasi kebutuhan anda untuk pemulihan data :

   Sebanyak 64% responden memilih Sangat, 25% responden memilih cukup dan 11% responden memilih kurang.

e. Apakah aplikasi ini mudah digunakan :

   Sebanyak 53% responden memilih mudah, 20% responden memilih sangat mudah dan 27% responden memilih cukup.

4.3 Pengujian Akurasi

Pengujian Akurasi dilakukan untuk mengetahui performa dari aplikasi yang telah dibuat. Pengujian ini dilakukan terhadap hasil dari proses pemulihan data. Pengujian data sms dilakukan dari database berisi 100 sms sampai dengan database 2000 sms sedangkan pengujian data CDR dilakukan dari database berisi 50 *call* log sampai dengan 500 *call log*. Hasil dari pengujian akurasi proses pemulihan data dapat dilihat pada 4able berikut :

Tabel 4.1 pengujian akurasi data SMS

NO	NAMA DATABASE	JENIS PENGUJIAN	HASIL
1	mmssms.db 1	Pemulihan data SMS	Akurat
2	mmssms.db 2	Pemulihan data SMS	Akurat
3	mmssms.db 3	Pemulihan data SMS	Akurat
4	mmssms.db 4	Pemulihan data SMS	Akurat
5	mmssms.db 5	Pemulihan data SMS	Akurat
6	mmssms.db 6	Pemulihan data SMS	Akurat
7	mmssms.db 7	Pemulihan data SMS	Akurat
8	mmssms.db 8	Pemulihan data SMS	Akurat
9	mmssms.db 9	Pemulihan data SMS	Akurat
10	mmssms.db 10	Pemulihan data SMS	Akurat

Tabel 4.2 pengujian akurasi data CDR

NO	NAMA DATABASE	JENIS PENGUJIAN	HASIL
1	contacts2.db 1	Pemulihan data CDR	Akurat
2	contacts2.db 2	Pemulihan data CDR	Akurat
3	contacts2.db 3	Pemulihan data CDR	Akurat
4	contacts2.db 4	Pemulihan data CDR	Akurat
5	contacts2.db 5	Pemulihan data CDR	Akurat
6	contacts2.db 6	Pemulihan data CDR	Akurat
7	contacts2.db 7	Pemulihan data CDR	Akurat
8	contacts2.db 8	Pemulihan data CDR	Akurat
9	contacts2.db 9	Pemulihan data CDR	Akurat
10	contacts2.db 10	Pemulihan data CDR	Akurat

4.4 Pengujian Data

Setelah dilakukan pengujian data, data setelah dilakukan *factory reset* masih dapat dipulihkan tetapi data setelah dilakukan *flash ROM* tidak dapat dipulihkan karena *flash ROM* mengubah ROM lama menjadi ROM baru.

Karena keterbatasan *resource* pengujian dilakukan hanya dengan sampai 2000 sms dan 500 *call* log. Dari hasil uji memori penyimpanan, 2000 sms data dan 500 *call log* yang ada semua dapat dipulihkan. Dapat disimpulkan bahwa kapasitas memori penyimpanan data sms dalam android tergantung oleh kapasitas memori *internal* dari *smartphone user*. Semakin besar memori *internal smartphone* semakin besar pula kapasitas memori penyimpanan data sms. Sedangkan data *call log* diandroid terbatas maksimum hanya 500 *call logs.*

V. Penutup

5.1 Kesimpulan

Berdasarkan hasil pengujian dan pembahasan dalam Tugas Akhir dapat disimpulkan bahwa :

1. Aplikasi ini dapat memulihkan data SMS dan data CDR yang telah terhapus kembali ke memori *smartphone*.
2. Berdasarkan hasil *beta*, didapatkan kesimpulan bahwa aplikasi pemulihan data besar dibutuhkan dengan persentase 67%. Dan sebanyak 64% menyatakan aplikasi ini sangat memfasilitasi kebutuhan pengguna untuk memulihkan data.
3. Setelah dilakukan pengujian data, 40% data SMS dan 20% data CDR setelah dilakukan *factory reset* masih dapat dipulihkan Tetapi data setelah dilakukan *flash ROM* tidak dapat dipulihkan karena *flash ROM* mengubah ROM lama menjadi ROM baru.
4. Hasil dari Uji memori penyimpanan, Data SMS tidak ada batas jumlah penyimpanan. Semakin besar memori penyimpanan pada *smartphone* semakin besar pula data SMS yang dapat disimpan. Sedangkan data *call log* mempunyai limit hanya dapat menyimpan 500 data *call log.*

5.2 Saran

Dari aplikasi yang telah dibangun, tentunya masih perlu pengembangan agar aplikasi ini bisa lebih baik dari sebelumnya. Saran untuk pengembangan selanjutnya sebagai berikut.

1. Aplikasi *mobile* forensik ini dapat dikembangkan tidak hanya untuk mengembalikan data SMS dan data *call log* tetapi untuk semua data *user.*
2. Fitur-fitur dalam aplikasi ini disempurnakan lagi. Penambahan fitur baru untuk menunjang kebutuhan *user* yang semakin bertambah dan berkembang.

VI. Daftar Pustaka

[1] Al-Azhar, Muhammad Nuh. 2012. **DIGITAL FORENSIC :Panduan Praktis Investigasi Komputer.** Jakarta : Salemba Infotek.

[2] Hoog, Andrew. 2011. **Android Forensics:Investigation, Analysis,and Mobile Security for Google Android.** USA : Syngress.

[3] Huda, Arif Akbarul. 2012. **24 JAM!! PINTAR PEMROGRAMAN ANDROID.** Yogyakarta : Penerbit Andi.
[4] Safaat H, Nazruddin. 2011. **Android Pemrograman Aplikasi Mobile Smartphone Dan Tablet PC Berbasis Android**. Bandung : Informatika.
[5] C. Racioppo dan N. Murthy. 2012. **Android Forensics: A Case Study of the "HTC Incredible" Phone.** Riset Seidenberg School of CSIS, Pace University, New York.
[6] SQLite Manager http://www.sqlabs.com/sqlitemanager.php Diakses 9 Desember 2014.
[7] Jiang, F., Ku, S., 2010**. *How to display the data from database by ListView on Android***, Journal of technology, Wuhan University of Technology, Wuhan, China.
[8] Elmasri, R., Navathe, S., 2007. ***Fundamentals of Database Systems, 5th edition,* chapter 8**, University of Texas, Virginia, USA.
[9] Andry. 2011. **Android A sampai Z.** Jakarta : PT. Prima Infosarana Media.
[10] What is android? http://developer.android.com/guide/basics/what-is-android.html Diakses 9 Desember 2014.