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

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

Dustin Annisa R.[1], Surya Michrandi N.,ST.,MT.[2],Budhi Irawan,SSi.,MT.[3]

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

Abstrak

Perkembangan teknologi pada telepon genggam di Indonesia sangatlah pesat. Terutama pada tahun 2000-an ini yang merupakan era globalisasi. Salah satunya dengan mulai berdatangannya produsen pengembang telepon genggam. Sejalan dengan perkembangannya, sering kali telepon genggam berindak sebagai sebab maupun akibat dari tindak kriminal. Dengan mulai berkembangnya ilmu forensik dalam bidang teknologi, dampak dari tindak kriminal yang disebabkan oleh telepon genggam dapat diungkap dan diketahui kebenarannya. Salah satunya dengan bidang ke ilmuan mobile forensik. Iphone yang merupakan telepon genggam buatan perusahaan Apple merupakan salah satu telepon genggam yang sedang digemari dalam penggunaanya di Indonesia. Telepon genggam Iphone ini tidak hanya dapat digunakan untuk bertelepon maupun berkirim pesan. Namun, Iphone merupakan salah satu smarphone yang telah dapat menyimpan data suara, gambar maupun video. Telepon genggam ini juga dapat disalah gunakan dalam penggunaannya seperti untuk media merencanakan tindak kriminal atau untuk menghilangkan bukti saat telah melakukan tindak kriminal.
Dalam Tugas Akhir ini telah dibuat aplikasi mobile forensik untuk mendapatkan data SMS dan data CDR yang sudah dihapus didalam iPhone menggunakan xcode dan bahasa Objective-C. Pengguna dapat menampilkan data SMS dan data CDR yang sebelumnya telah terhapus.
Melalui aplikasi mobile forensik ini dapat memulihkan 100% data SMS dan data CDR dalam kondisi iPhone telah ter-jailbreak. Setelah dilakukan factory reset, dapat dipulihkan 5% data SMS dan 10% data CDR.

Kata kunci : iphone, mobile forensics, smartphone, recovery data

Abstract

Mobile phone's development in Indonesia is increasing rapidly, especially in 2000s as globalization era. Mobile phone's producers come to commence their business. As of the growth, sometimes mobile phone becomes the reason of criminality. With the development of forensic studies in technological fields, the effects of criminality caused by mobile phone can be revealed. For example, using mobile forensic study. IPhone, as Apple's product, is one of most popular mobile brands in Indonesia. The iPhone is not only used for making a call or texting message, but also for saving audios, pictures, and videos. This kind of mobile phone can also be used for planning criminal acts or taking criminal proofs away.
In this final project was made an iPhone application to get the deleted SMS and CDR data using xcode and Objective-C programming language. Users can show the deleted SMS and CDR.
By using this mobile forensic application can restore 100% SMS and CDR data on jailbreaked iPhone. After factory reset, 5% SMS data and 10% CDR data can be recovered.

Keywords: iphone, mobile forensics, smartphones, data recovery

I. Pendahuluan

Kemajuan dibidang telekomunikasi sangat pesat, sehingga teknologi telekomunikasi menjadi sangat penting peranannya dalam kehidupan manusia. Salah satu teknologi yang menjadi kebutuhan manusia adalah telpon genggam. Tujuan utama orang menggunakan telpon genggam adalah untuk saling berkomunikasi.

Kini era telpon genggam telah memasuki era smartphone. Salah satu smartphone yang mendominasi pasar Indonesia adalah Iphone. Dengan kecanggihan smartphone beberapa oknum dapat menyalah gunakan penggunaannya seperti untuk media merencanakan tindak kriminal. Smartphone yang telah digunakan untuk tindak kriminal maka smartphone tersebut dapat disita oleh penegak hukum untuk dijadikan sebagai barang bukti. Tetapi sebagian besar pelaku kejahatan telah menghilangkan bukti dalam smartphone tersebut. Oleh karena itu diperlukan aplikasi yang dapat membantu proses investigasi untuk memulihkan data yang dapat dijadikan bukti tindak kriminal dalam smartphone berbasis sistem operasi ios menggunakan bahasa Objective-c.

Untuk mengatasi masalah diatas, maka dalam tugas akhir ini penulis akan merancang sebuah aplikasi mobile forensik untuk memulihkan data yang hilang berbasis sistem operasi ios..

II. Dasar Teori

2.1 IoS

IOS merupakan sistem operasi yang di buat oleh apple Inc untuk product iPhone saja namun melihat perkembangannya yang sangat pesat maka IOS di kembangkan supaya support dengan perangkat perangkat buatan apple inc lainnya, sistem operasi ios merupakan hasil dari pengembangan Mac OS X, oleh karena itu iOS memiliki ciri khas sebagai mana sistem operasi Unix pada Mac OS X, antar muka IOS menggunakan konsep manipulasi langsung gerakan multi-touch, respon IOS.

2.2 Objective-c

Objective-C adalah bahasa pemrograman yang dikembangkan dari bahasa C digabung dengan gaya bahasa SmallTalk. Dengan kata lain, Objective-C pada OOP-nya bergaya SmallTalk yaitu menggunakan message passing sedangkan C++ menggunakan pemanggilan method. Objective-C saat ini banyak digunakan pada platform Mac OS X dan iOS (iOS adalah sistem operasi untuk iPhone, iPod Touch dan iPad). Dengan adanya framework Cocos2D yang notabene adalah framework untuk membuat game di iPhone, maka Objective-C makin banyak yang mempelajarinya. Catatan Cocos2D merupakan bagian Cocoa Touch API yang dibuat menggunakan Objective-C

Awalnya dikembangkan pada awal tahun 1980, ia dipilih sebagai bahasa utama yang digunakan oleh NeXT untuk sistem operasi NeXTSTEP, dari mana OS X dan iOS berasal . Generik Objective-C program yang tidak menggunakan Kakao Cocoa Touch atau perpustakaan juga dapat dikompilasi untuk sistem yang didukung oleh GCC.

2.3 SQLite

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

2.4 Xcode

Xcode adalah platform native yang dikembangkan langsung oleh Apple untuk mengembangkan OS X dan iOS . Xcode merupakan integrated Development Environment (IDE) yang juga disertakan dalam generasi OS X terkini . dirilis pada tahun 2003 melalui seri 1x ,dan tersedia di seri terkini yakni versi 5.0. Xcode mendukung langsung pengembangan untuk basis smartphone Apple yakni Ipad dan Iphone.

Xcode hadir pertama pada tahun 2003. seri pertama ini dikenal dengan versi 1.x. saat itu platform ini berbasiskan project builder, namun sudah memiliki kemampuan UI,ZeroLink,Fix&Continue,support pengembangan distribusi, dan code sense indexing. setelah itu berturut-turut diikuti versi terbaru yakni 2.x series , 3.x series , 4.x series dan terkini versi 5.0 pada bulan juni 2013. Genartor kode yang digunakan oleh Xcode adalah LLVM,dan LLDB sebagai debugger default (versi 4.3). seri Xcode pertama hadir di OS Mac OS X 10.3 yakni versi 1.x, setelah itu hadir sebagai aplikasi yang dapat digunakan untuk OS Mac generasi selanjut nya.

Pada perkembangan awal, Xcode mendukung distribusi dari beberapa sistem yakni workgroup guild. menariknya xcode juga menyediakan fasilitas untuk membuat Dedicated Network Builds, namun pada versi terbarunya tidak lagi mendukung fasilitas ini.Xcode meruapakan perangkat WebObjects yang mampu menjadi framework pembuatan aplikasi web. tampilan instrumen Xcode adalah GUI dan berjalan di atas Dtrace. Untuk mengembangkan aplikasi pada Iphone dan Ipad disediakan Xcode emulator, namun sebelumnya perlu men-download

iOS yang disesuaikan dengan perangkat pendukungnya.

Platform ini menggunakan bahasa Objective-C sebagai pengembangannya. bahasa pengembangan dari C , yang sekaligus menjadi bahasa native untuk membuat aplikasi mac. salah satu ciri bahasa ini adalah penggunaan style dari Smalltalk. bahasa dari platform ini bersifat objek oriented, namun tetap mendukung bahasa terstruktur. selain itu platform ini juga mendukung bahasa C, C++, Objective-C, Objective-C++, Objective-C++, Java, AppleScript,python dan bahasa pengembangan model dari yang sudah dikenal . pengembang ketiga juga mensupport bahasa seperti Pascal,free pascal , c# ,perl.

III. Analisis dan Perancangan

3.1 Deskripsi Sistem

Deskripsi sistem yang telah dibuat ini adalah aplikasi mobile forensik yang dapat mengembalikan data yang telah hilang untuk membantu proses investigasi berbasis sistem operasi IoS, Data yang telah hilang meliputi data SMS dan data call log.

3.2 Analisa Kebutuhan Sistem

Dalam proses pembuatan aplikasi ini, dibutuhkan penunjang baik dari segi data, software maupun hardware yang mampu menunjang implementasi aplikasi.

3.3.1 Analisis Kebutuhan Data

Data yang diperlukan dalam aplikasi ini adalah data dari database smartphone user berupa data SMS dan data call log. Sebelum menjalankan aplikasi, smartphone user harus dalam keadaan sudah dijailbreak supaya dapat mengakses database smartphone.

3.3.1.1 Data SMS

Data SMS pada Iphone terdapat didalam direktori **/var/mobile/Library/SMS/sms.db.**

3.3.1.2 Data CDR

Untuk data Call Data Record pada Iphone terdapat didalam direktori **/var/wireless/Library/CallHistory/call_history.db.**

3.3.2 Analisa Kebutuhan Proses

Proses yang dibutuhkan dalam aplikasi ini adalah proses menampilkan data sms dan data call log. Setelah ditampilkan data tersebut akan dipulihkan kembali kedalam database smartphone user.

3.3 Analisis Kebutuhan Antarmuka

Perancangan aplikasi memerlukan spesifikasi hardware, software, dan user.

3.3.1 Analisis Kebutuhan Perangkat Lunak

Dalam perancangan sistem, pembuatan program, diperlukan perangkat lunak dengan kebutuhan minimum sebagai berikut :

1. Sistem Operasi MAC OS X 10.10 Yosemite
2. XCode 6

3.3.2 Analisis Kebutuhan Perangkat Keras

Perangkat keras yang dibutuhkan dalam pembuatan program dan simulasi aplikasi adalah sebagai berikut :

Laptop yang digunakan untuk membuat program, melakukan simulasi pada perangkat :

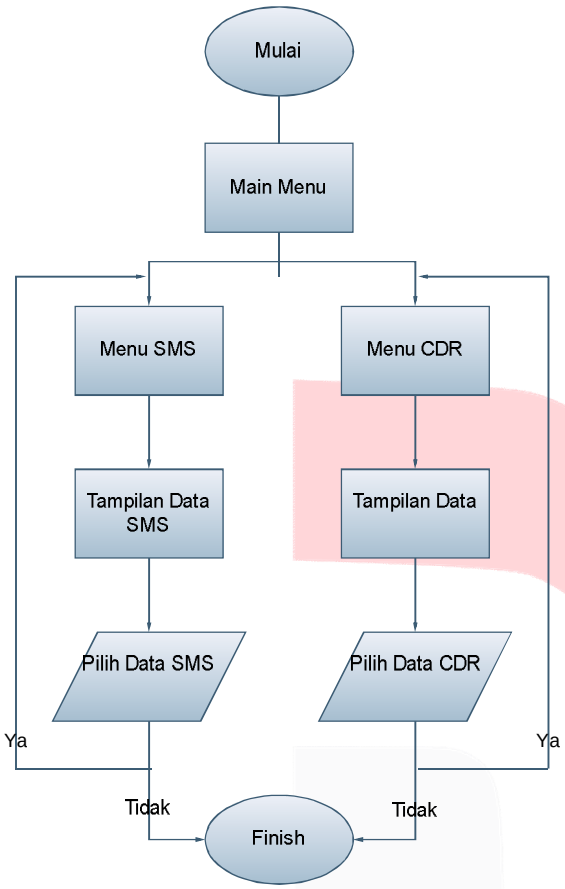
1. Laptop Macbook pro MD101
2. Intel(R) Core(TM) i5 @2.27 GHz
3. RAM 4 GB

Smartphone yang digunakan untuk implementasi aplikasi :

1. Smartphone Iphone 4G
2. 1 GHz Cortex-A8
3. 640 x 960 pixels
4. RAM 512 MB
5. iOS 7.1.1.

3.4 Analisa Sistem

Sistem yang dibuat ini adalah aplikasi mobile forensik yang dapat mengembalikan data yang telah hilang untuk membantu proses investigasi berbasis sistem operasi IoS, Data yang telah hilang meliputi data SMS dan data call log. Sistem dibuat berdasarkan analisis kebutuhan pengguna. Dalam analisis sebuah sistem perlu dilakukan adanya penggambaran alur salah satunya menggunakan diagram alir. Berikut diagram alir untuk sistem aplikasi ini secara keseluruhan :



Gambar 3.4 Diagram Alir Sistem Keseluruhan

Dalam aplikasi ini terbagi dalam beberapa tahap. Yang pertama adalah tahap pemilihan data, seperti data SMS dan data call log. Setelah user memilih data, data yang dipilih user tersebut akan ditampilkan didalam aplikasi. Dilanjutkan dengan proses pemulihan data user kedalam database smartphone.

3.5 Pemodelan Sistem

User yang telah menginstall aplikasi dapat memulihkan data yang telah dihapus dari database smartphone. Proses yang pertama yaitu pemilihan data oleh user, setelah user memilih datanya kemudian data tersebut akan ditampilkan didalam aplikasi dilanjutkan dengan proses pemulihan data user kembali kedalam database smartphone.

IV. Implementasi dan Pengujian

4.1 Implementasi Sistem

Tahap implementasi dilakukan setelah perancangan selesai dilakukan. Selanjutnya di implementasikan pada bahasa pemrograman agar menjadi sebuah aplikasi perangkat lunak yang bertujuan untuk mengkonfirmasi model perancangan, sehingga sistem siap untuk dioperasikan. Kemudian Pengujian dilakukan untuk mengevaluasi hasil dari sistem yang dibuat.

4.2 Pengujian Alpha

Pengujian Alpha (*Black Box)* aplikasi bertujuan untuk menemukan kesalahan sistem sesuai dengan *requirement* yang telah ditetapkan.

4.3 Hasil Pengujian Alpha

Hasil pengujian dari pengujian *alpha* yang telah dilakukan menunjukkan bahwa aplikasi sudah memenuhi rancangan. Secara fungsional, program dapat menghasilkan keluaran yang diharapkan serta dapat diimplementasikan di beberapa perangkat android lainnya.

4.4 Pengujian Akurasi

Pengujian akurasi dilakukan untuk mengetahui performa dari aplikasi yang telah dibuat. Pengujian ini dilakukan terhadap hasil dari proses pemulihan data. Hasil dari pengujian akurasi proses pemulihan data dapat dilihat pada tabel berikut :

Pengujian dilakukan sebanyak 11 kali, dengan database yang sama tetapi jumlah sms yang diuji berbeda dari database dengan 10 sms sampai dengan database 500 sms.

Table 4.1 Hasil Pengujian Akurasi SMS

NO	NAMA DATABASE	JENIS PENGUJIAN	HASIL
1	sms.db (10 SMS)	Pemulihan data SMS	Akurat
2	sms.db (20 SMS)	Pemulihan data SMS	Akurat
3	sms.db (30 SMS)	Pemulihan data SMS	Akurat
4	sms.db (40 SMS)	Pemulihan data SMS	Akurat
5	sms.db (50 SMS)	Pemulihan data SMS	Akurat
6	sms.db (60 SMS)	Pemulihan data SMS	Akurat
7	sms.db (70 SMS)	Pemulihan data SMS	Akurat
8	sms.db (80 SMS)	Pemulihan data SMS	Akurat

9	sms.db (90 SMS)	Pemulihan data SMS	Akurat
10	sms.db (100 SMS)	Pemulihan data SMS	Akurat
11	Sms.db (500 SMS)	Pemulihan data SMS	Akurat

Pengujian dilakukan sebanyak 11 kali, dengan database yang sama tetapi jumlah *call log* yang diuji berbeda, dari database dengan 1 *call log* sampai dengan database 500 *call log*.

Table 4.2 Hasil Pengujian *call log*

NO	NAMA DATABASE	JENIS PENGUJIAN	HASIL
1	call_history.db (10 *call log*)	Pemulihan data CDR	Akurat
2	call_history.db (20 *call log*)	Pemulihan data CDR	Akurat
3	call_history.db (30 *call log*)	Pemulihan data CDR	Akurat
4	call_history.db (40 *call log*)	Pemulihan data CDR	Akurat
5	call_history.db (50 *call log*)	Pemulihan data CDR	Akurat
6	call_history.db (60 *call log*)	Pemulihan data CDR	Akurat
7	call_history.db (70 *call log*)	Pemulihan data CDR	Akurat
8	call_history.db (80 *call log*)	Pemulihan data CDR	Akurat
9	call_history.db (90 *call log*)	Pemulihan data CDR	Akurat
10	call_history.db (100 *call log*)	Pemulihan data CDR	Akurat
11	call_history.db (500 *call log*)	Pemulihan data CDR	Akurat

4.5 Pengujian Data

Pengujian dilakukan untuk mengetahui data yang akan dipulihkan apakah berbatas waktu atau berbatas memori penyimpanan.

Table 4.3 Hasil Pengujian data setelah *factory reset*

NO	DATABASE	PENGUJIAN	HASIL
1	sms.db	Pemulihan data sms setelah factory reset	Data tidak dapat dipulihkan
2	call_history.db	Pemulihan data CDR setelah factory reset	Data tidak dapat dipulihkan

Table 4.4 Hasil Pengujian *setelah* jailbreak

NO	DATABASE	PENGUJIAN	HASIL
1	sms.db	Pemulihan data sms setelah Jailbreak	Data dapat dipulihkan
2	call_history.db	Pemulihan data CDR setelah Jailbreak	Data dapat dipulihkan

Table 4.5 Hasil Pengujian data memori

NO	DATABASE	PENGUJIAN	HASIL
1	sms.db	Pemulihan data sms (500 SMS)	Data dapat dipulihkan
2	call_history.db	Pemulihan data CDR (500 *call log*)	Data dapat dipulihkan

Setelah dilakukan pengujian data, data setelah dilakukan *factory reset* tidak dapat dipulihkan tetapi data setelah dilakukan *Jailbreak* dapat dipulihkan. Hasil dari Uji memori penyimpanan, data SMS dan data CDR tidak ada batas jumlah penyimpanan. Data SMS dan data CDR dapat

menyimpan data dalam jumlah yang tergantung dari besaran memori dari *smartphone*, jadi semakin besar memori penyimpanan pada *smartphone* semakin besar pula data SMS dan data CDR yang dapat disimpan.

V. Penutup

5.1 Kesimpulan

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

1. Pembuatan aplikasi mobile forensik berbasis sistem operasi IoS dengan basis kode objective-c dapat memulihkan data SMS dan CDR yang telah terhapus.
2. Setelah dilakukan pengujian data, data setelah dilakukan jailbreak masih dapat dipulihkan tetapi data setelah dilakukan factory reset dapat dipulihkan sebagian.
3. Hasil dari Uji memori penyimpanan, data SMS dan data CDR tidak ada batas jumlah penyimpanan. Semakin besar memori penyimpanan pada smartphone semakin besar pula data SMS dan data CDR yang dapat disimpan.
4. Setelah dilakukan pengujian data, 5% data SMS dan 10% data CDR setelah dilakukan factory reset dapat dipulihkan.
5. 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. Agar meningkatnya kualitas aplikasi ini saran untuk pengembangan selanjutnya untuk dipertimbangkan sebagai berikut :

1. Untuk membuat aplikasi pada *smartphone* iPhone yang lebih sesuai sebaiknya terdaftar sebagai IoS *Developer Program.*
2. Aplikasi *mobile* forensik ini dapat dikembangkan lagi untuk mengembalikan data yang terdapat dalam *smartphone*, seperti data *email, notes* dan lainnya.

.

VI. Daftar Pustaka

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

[2] S. Morrissey, M. Lowman, Ed. 2010. **iOS Forensic Analysis for iPhone, iPad and iPod touch**. USA: Apress.

[3] iOS Developer Library. http://developer.apple.com/library/ios/navigation/ Diakses 9 Desember 2014

[4] SQLite Manager http://www.sqlabs.com/sqlitemanager.php Diakses 9 Desember 2014

[5] Hoog, Andrew. 2011. **iPHONE AND iOS FORENSICS, investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices.** USA : Syngress.

[6] Altheide, Cory and Carvey, Harlan. 2011. **DIGITAL FORENSICS WITH OPEN SOURCE TOOLS.** USA : Syngress.

[7] Wentk, Richard. 2012. **iOS App Development Portable Genius.** Wiley.

[8] Xcode. https://developer.apple.com/xcode/ Diakses 9 Desember 2014