FORENSIK IPOD TOUCH

TUGAS AKHIR

Diajukan sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana
Jurusan Teknik Informatika

OLEH :

NAMA : Muhammad Zulfariansyah
NO. MAHASISWA : 08523120

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA
2012

LEMBAR PENGESAHAN PEMBIMBING

FORENSIK IPOD TOUCH

TUGAS AKHIR

Oleh :

Nama : Muhammad Zulfarianasyah

NIM : 08 523 120

Yogyakarta, April 2012

Pembimbing tunggal,

Yudi Prayudi, S.Si., M.Kom.

LEMBAR PENGESAHAN PENGUJI

FORENSIK IPOD TOUCH

TUGAS AKHIR

Disusun oleh:

Nama : Muhammad Zulfariansyah

NIM : 08 523 120

Telah dipertahankan di Depan Sidang Penguji Sebagai Salah Satu Syarat

Untuk Memperoleh Gelar Sarjana Teknik Informatika

Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, April 2012

Tim Pengaji

Yudi Prayudi, S.Si., M.Kom.
Ketua

Syarif Hidayat, S.Kom., M.I.T.
Anggota I

R. Teduh Dirgahayu, ST., M.Sc., Ph.D.
Anggota II

Mengetahui,

Ketua Program Studi Teknik Informatika

Universitas Islam Indonesia

Yudi Prayudi, S.Si., M.Kom.

LEMBAR PERNYATAAN KEASLIAN
HASIL TUGAS AKHIR

Saya yang bertandatangan dibawah ini,

Nama : Muhammad Zulfariansyah

NIM : 08 523 120

Menyatakan bahwa komponen dan seluruh isi dalam Laporan Tugas Akhir ini adalah hasil karya saya sendiri. Apabila dikemudian hari terbukti bahwa ada beberapa bagian dari karya ini adalah bukan hasil karya saya sendiri, maka saya akan siap menanggung resiko dan konsekuensi apapun.

Demikian pernyataan ini saya buat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, April 2012

Muhammad Zulfariansyah

PERSEMBAHAN

Untuk:

Mama, Papa, adik dan kakak tersayang.

MOTTO

” Ya Allah yang Maha memudahkan yang susah dan Maha menyusahkan yang mudah, maka Mudahkanlah segala urusanku”

“..... sesungguhnya setelah kesulitan tersimpan sebuah kemudahan”

(QS. Al Insyiroh : 6)

KATA PENGANTAR

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيْمِ

Assalamu'alaikum. Wr. Wb

Dengan mengucapkan Alhamdulillah, puji dan syukur ke hadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan tugas akhir ini, yang berjudul "**Forensik iPod Touch"** dengan baik**.**

Laporan tugas akhir ini disusun untuk melengkapi salah satu syarat guna memperoleh gelar Sarjana Teknik Informatika pada Universitas Islam Indonesia dan atas apa yang telah diajarkan selama perkuliahan baik teori maupun praktek, disamping laporan itu sendiri yang merupakan rangkaian kegiatan yang harus dilakukan setelah tugas akhir ini selesai.

Penulisan dan penyelesaian tugas akhir ini tidak lepas dari saran, bimbingan, dukungan serta bantuan dari berbagai pihak. Untuk itu pada kesempatan kali ini penulis menyampaikan ucapan terimakasih kepada :

1. Allah SWT. Atas segala hidayah, barokah dan taufiq-Nya.
2. Kedua orangtua yang selalu melimpahkan kasih sayang yang begitu besar, serta doa dan dukungan yang begitu besar.
3. Bapak Gumbolo selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
4. Bapak Yudi Prayudi, S.Si., M.Kom., selaku Ketua Jurusan Teknik Informatika dan selaku Dosen Pembibimbing Tugas Akhir. Terima kasih atas segala bantuan, dukungan, dan pengetahuan yang telah diberikan kepada penulis dalam penyusunan skripsi ini.
5. Kakak Ria, dan Yanti, dua saudara perempuan tersayang.
6. Mega Ariyanfina, untuk dukungan, doa, dan motivasi yang tiada batas.
7. Bapak Hamid, S.T., M.T., yang telah membantu dan memberikan pencerahan dalam pengerjaan skripsi ini.

8. Mas Citra untuk bantuannya pada langkah awal skripsi ini. Ayo semangat nyekripsi mas!!
9. Teman-teman seperjuangan Tugas Akhir: Gilang Dewantara, Mas Toni, Umin, Juwita, Galuh, Endah, Rif'an, Handika, Uli, Reni, Dwi, dan Lindung.
10. Teman-teman yang telah wisuda lebih dulu, Pak Jeki, Mba Ishe, dan Mas Beben.
11. Teman-teman KP SEIP kelompok 11 angkatan 2.
12. Teman-teman KKN Unit 47, *longlive cutminers!!!*
13. Teman-teman dari LPM Profesi FTI UII.
14. Teman-teman dari Kosmik UII. Spesial untuk *Fold Chair* (2010), *CrossOver and The Fuzzy* (2011), *The Magic Mushroom* (2012). Terimakasih telah mendengar ke-egoisan saya selama dalam masa proyek band.
15. Kakak Kohara Kazamasa, dan Kyuhyun, yang memberikan semangat secara tidak langsung melalui karya.
16. Semua pihak yang telah membantu dalam pembuatan hingga terselesaikannya tugas akhir ini, yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari dalam penulisan laporan tugas akhir ini masih jauh dari sempurna, karena keterbatasan kemampuan dan pengalaman. Penulis mengharapkan saran dan kritik yang bersifat membangun untuk memperbaiki tugas akhir ini semoga dapat bermanfaat bagi penulis khususnya dan pembaca pada umumnya.

Wassalamu'alaikum Wr. Wb

Yogyakarta, April 2012

Muhammad Zulfariansyah

SARI

IPod Touch merupakan sebuah perangkat multimedia yang sangat popular di era digital masa kini. Perannya sebagai media hiburan, kerapkali sering dilupakan bahwa iPod Touch juga berpotensi menyimpan barang bukti pada suatu kasus. Bahkan tidak menutup kemungkinan iPod Touch tersebut menjadi alat dari kejahatan.

Untuk mengungkap permasalah tersebut, diperlukan teknik forensik untuk membuat file *image* dan mengekstraknya. Dari file ekstrak itulah akan disidik iPod Touch dan menemukan barang bukti didalamnya. Proses *imaging* sampai analisis menggunakan berbagai software forensik seperti dd, Oxygen Forensic Suite, Forensic Toolkit, dan Data Rescue 3.

Penyelidikan dimulai dengan membuat *back up* dan *image* pada iPod Touch. Membuat file *back up* bisa dilakukan dengan cara yang umum seperti dengan menggunakan iTunes. Namun, untuk membuat file *image* dari perangkat yang mempunyai struktur file tertutup seperti Apple iPod Touch, harus mempunyai teknik tersendiri untuk membuat dan mengekstraknya. Untuk itulah diperlukan langkah-langkah untuk membuat *back up* dan *image* tersebut.

Hasil akhirnya adalah berupa analisis dan rekapitulasi cara menyidik iPod Touch yang telah diringkas, serta laporan dari penyelidikan. Dari analisis tersebut dapat diketahui iPod Touch dapat berpotensi melakukan kejahatan apa, serta dapat menyimpan barang bukti apa.

Kata kunci : Forensik, *Image, Back Up*

TAKARIR

imaging	membuat salinan data mentah.
forensik	proses ilmiah dalam mengumpulkan, menganalisis, dan menghadirkan berbagai bukti dalam sidang pengadilan terkait adanya suatu kasus hukum
penyidik	orang yang menyidik kasus
backup	membuat cadangan data
write blocking	fitur untuk menghalang penggandaan atau penulisan data.

DAFTAR ISI

BAB III METODOLOGI

BAB IV HASIL DAN PEMBAHASAN

DAFTAR GAMBAR

DAFTAR TABEL

ISLAM
UNIVERSITAS
INDONESIA

BAB I
PENDAHULUAN

1.1 Latar Belakang

Digital Forensik adalah suatu ilmu pengetahuan atau keahlian untuk mengidentifikasi, mengoleksi, menganalisis dan menguji bukti–bukti digital pada saat menangani sebuah kasus sehingga dapat dipertanggungjawabkan di pengadilan (Alamsyah, 2009). Sejauh ini, penerapan digital forensik di Indonesia masih belum luas. Investigasi forensik digital baru diterapkan pada perangkat-perangkat keras yang umum dipakai, seperti *personal computer*, *notebook*, dan *smartphone*. Padahal ada jenis perangkat keras lain yang juga seharusnya tidak luput dari kegiatan forensik digital, salah satunya adalah perangkat pemutar musik seperti Apple iPod Touch.

Apple iPod Touch sebagai perangkat pemutar musik masih kurang diberi perhatian oleh para investigator forensik, dikarenakan fungsinya yang dianggap hanya sebagai pemutar musik. Padahal iPod Touch memiliki kemampuan untuk menyimpan banyak informasi dan data seseorang, sehingga memungkinkan untuk dijadikan barang bukti di persidangan. Sebagai contoh, seperti yang dilaporkan pada BBC News Tahun 2004, di Inggris sekelompok pencuri mobil ditangkap dan bukti yang menyebabkan mereka pada penuntutan adalah iPod Touch. iPod Touch digunakan untuk menyimpan dan menyampaikan informasi tentang mobil yang mereka curi.

Untuk itu perlu dilakukan sebuah analisis forensik pada iPod Touch. Kegunaan dari analisis tersebut adalah untuk mencari bukti dalam iPod Touch dan menjamin bukti itu dapat berguna dipersidangan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disebutkan diatas, maka dapat diambil rumusan masalah, yaitu :

a. Bagaimana menyelidiki barang bukti digital pada iPod Touch agar dapat dijadikan barang bukti hukum yang sah.
b. Bagaimana cara membuat File *Image* dari iPod Touch serta cara mengekstraknya.
c. Bagaimana cara melihat dan meng-*eksplore* struktur file dari iPod Touch agar dapat mengetahui karakteristiknya.
d. Tindakan kriminal apa saja yang dapat dilakukan dengan iPod Touch.
e. Barang bukti apa saja yang terdapat dalam iPod Touch.

1.3 Batasan Masalah

iPod Touch memiliki banyak kemampuan dalam dunia hiburan. Seperti memutar musik dan video, menampilkan gambar, mencatat memo, pengingat kalender, dan sebagainya. Dari banyaknya kemampuan tersebut tentu saja bisa disidik forensik secara keseluruhan. Untuk itu dibutuhkan batasan masalah agar penelitian ini mempunyai ruang dan tidak menyimpang dari apa yang telah direncanakan. Adapun batasan masalah dalam penelitian ini adalah sebagai berikut :

a. *Keypad* iPod Touch yang diforensik dalam keadaan *unlock.*
b. iPod Touch yang diforensik dalam keadaan sudah ter-*jailbreak.*
c. iPod Touch yang diforensik adalah iPod Touch generasi 2, dengan sistem operasi iOS versi 4.2.1 (8C148).

1.4 Review Penelitian

Penelitian yang dilakukan oleh (Finocchiaro, Goldman, Natarajan, & Stanek, 2009) membahas tentang bagaimana struktur file pada sebuah iPod Touch. Selain itu, dalam penelitian ini juga dijelaskan bagaimana cara mendapatkan data yang telah terhapus atau disembunyikan. Hasil akhir dari penelitian yang berjudul "iPod Touch *Forensic Techniques*" ini adalah menampilkan hasil penyelidikan iPod Touch forensik, dari berbagai macam aplikasi atau *tools* investigasi forensik dan juga menampilkan *Forensic Script.* dimana guna dari *forensic script* tersebut adalah untuk mengetahui file yang telah dihapus atau disembunyikan.

Sementara itu, hasil studi dari Purdue University (Marsico & Rogers, 2005) mengatakan bahwa iPod Touch menyimpan catatan yang kuat terkait dengan inisialisasi, seperti *username* dari nama komputer dan nama komputer yang disimpan. Menurut penelitian tersebut, informasi ini dapat terdapat persis dibawah nama perangkat iPod Touch. Penelitian yang berjudul "iPod Touch *Forensic*" tidak hanya menjelaskan tentang bagaimana melakukan kegiatan forensik pada iPod Touch, tapi juga menjelaskan tentang design dan bagian dalam tubuh dari iPod Touch. Serta memberikan gambaran tentang pertimbangan hukum apabila iPod Touch ditemukan dalam Tempat Kejadian Perkara.

Selanjutnya, Penelitian yang berjudul "Analisis *Computer Forensic* Menggunakan Forensic Toolkit" (Rozita, 2011) membahas tentang bagaimana langkah-langkah menyelidiki komputer secara forensik dengan menggunakan *tool* yaitu Forensic Toolkit. Penelitian ini mempunyai skenario kasus terkait terorisme, dan hasil akhir dari penelitian ini adalah berupa tampilan hasil penyelidikan pada skenario kasus tersebut.

Menurut hasil studi yang berjudul "A tool for MAC OS X operating system and application forensic" (Joyce, Powers, & Adelstein, 2008) menyatakan bahwa iPod Touch tidak bisa diabaikan dalam investigasi forensik karena data didalamnya bisa mengandung informasi yang dapat digunakan untuk keperluan bukti hukum. Penelitian ini membahas banyak sekali tools atau aplikasi forensik yang digunakan untuk menyidik Sistem Operasi MAC OS X. Berbagai langkah yang digunakan dalam penelitian ini salah satunya adalah tentang kegiatan forensik pada perangkat MAC yang telah dipasang 2 *Virtual Machines*.

1.5 Tujuan Penelitian

Tujuan penelitian ini adalah :

a. Mengetahui cara penyelidikan barang bukti digital pada iPod Touch agar dapat dijadikan barang bukti hukum yang sah.
b. Memahami cara pembuatan file *image* dari iPod Touch dan cara mengekstraknya.

c. Mengetahui karakteristik iPod Touch dengan meng-*explore* struktur file dari iPod Touch tersebut.
d. Menyelediki iPod Touch dengan *tools* forensik, sehingga dapat diketahui tindakan kriminal apa saja yang bisa dilakukan dengan iPod Touch.
e. Mengetahui barang bukti apa saja yang terdapat pada iPod Touch.

1.6 Manfaat Penelitian

Manfaat penelitian ini adalah :

a. Menambah pengetahuan tentang bagaimana analisis kasus pada proses forensik.
b. Memberikan pemahaman terkait ilmu forensik khususnya iPod Touch forensik serta *tools* yang digunakan untuk analisis forensik.
c. Berguna untuk mengembalikan data pada data iPod Touch yang hilang.

1.7 Metodologi Penelitian

Metode Penelitian yang digunakan dalam penelitian ini adalah sebagai berikut :

1.7.1 Studi dan Pengumpulan data

Sebuah barang bukti dalam suatu kasus akan membutuhkan proses yang sangat panjang untuk bisa menjadi barang bukti yang sah di pengadilan. Dalam sebuah proses forensik, menganalisis *image* dari barang bukti digital merupakan hal yang sangat penting. Karena dari hasil image tersebut akan diperoleh data terkait kasus yang bersangkutan. Namun sebelum melakukan serangkaian proses forensik, maka diperlukan pengumpulan informasi terkait proses penyelidikan forensik ini secara keseluruhan. Informasi tersebut dapat diambil dari buku, jurnal, *paper,* website, atau artikel tentang komputer forensik yang relevan dengan penelitian ini.

1.7.2 Melakukan uji coba, *back up* serta membuat *image* dari iPod Touch

Pada tahapan ini akan dilakukan ujicoba dan implementasi pada iPod Touch. Model ujicoba yang dimaksud adalah praktek simulasi penggunaan iPod Touch sebagai tindak kejahatan. Selanjutnya memproses iPod Touch tersebut

untuk menjadi sebuah barang bukti sebagai penyidik dengan membuat *back up* dan *image data*.

1.7.3 Analisis Data

Pada tahapan ini akan dilakukan analisis terhadap hasil *back up* dan *image* dari iPod Touch tersangka dengan menggunakan *tool* forensik. Sehingga dari proses analisis ini akan diketahui apa saja data-data terkait kasus tersebut serta menyelidiki sejauh mana penggunaan iPod Touch dalam potensi melakukan kejahatan. Dalam tahapan ini juga dilakukan penjelajahan file sistem untuk mengetahui karakteristik dari iPod Touch.

1.8 Sistematika Penulisan

Dalam penyusunan tugas akhir ini, sistematika penulisan dibagi menjadi beberapa bab yaitu sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi pembahasan masalah secara umum yang meliputi LatarBelakang Masalah, Rumusan Masalah, Batasan Masalah, TujuanPenelitian, Manfaat Penelitian, Metodologi Penelitian dan SistematikaPenulisan.

BAB II LANDASAN TEORI

Bab ini memuat landasan teori yang berfungsi sebagai sumber atau alat dalam memahami permasalahan yang terkait dengan iPod Touch Forensik.

BAB III METODOLOGI

Bagian ini berisi studi literature mengenai permodelan uji coba serta langkah-langkah ujicoba proses investigasi forensik.

BAB IV PENGUJIAN DAN PEMBAHASAN

Berisi tentang proses pengujian, berupa print screen serta penjelasan data yang didapat dari hasil forensik. Lalu menganalisis data tersebut.

BAB V KESIMPULAN DAN SARAN

Bab ini merupakan rangkuman serta kesimpulan-kesimpulan dari hasil analisis dan saran yang dianggap perlu.

BAB II
LANDASAN TEORI

2.1 Digital/Komputer Forensik

Digital atau Komputer Forensik berarti melakukan pemeliharaan, identifikasi, ekstraksi, interpretasi, dan dokumentasi bukti komputer,untuk memasukan aturan bukti, proses hukum, integritas bukti, serta pelaporan fakta dari informasi yang ditemukan. Lalu memberikan pendapat sebagai ahli di pengadilan hukum (Computer Hacking Forensic Investigation, 2006).

Komputer Forensik dapat didefinisikan sebagai penerapan ilmu hukum dalam mencari kebenaran dalam hal perdata, pidana, dan sosial untuk mengakhiri ketidakadilan yang tidak dilakukan untuk setiap anggota masyarakat (Ginting, 2008). Dapat juga dikatakan bahwa komputer forensik merupakan serangkaian metode teknik dan prosedur untuk mengumpulkan bukti, dari peralatan komputasi dan berbagai perangkat penyimpanan dan media digital, yang dapat disajikan pada pengadilan dalam format yang mudah dimengerti oleh khalayak umum.

2.1.1 Tujuan Digital Forensik

Tujuan dari digital forensik adalah (Computer Hacking Forensic Investigation, 2006) :

a. Untuk menentukan nilai-nilai bukti dari Tempat Kejadian Perkara (TKP) serta bukti terkait dengan kasus yang bersangkutan.
b. Untuk memulihkan, menganalisis, dan memelihara komputer atau yang terkait dengan itu lalu dip roses sedemikian rupa hingga dapat disajikan sebagai bukti di pengadilan hukum.
c. Untuk mengidentifikasi bukti dalam waktu singkat, memperkirakan dampak potensial dari aktivitas yang berbahaya bagi korban, dan mengidentifikasi pelaku.

2.1.2 Kebutuhan akan Digital Forensik

Seiring pesatnya kemajuan teknologi di dunia, pemanfaatan dari manusia terhadap teknologi itu sendiripun beragam.Ada yang menggunakannya dalam naungan kebaikan, ada juga yang tidak. Penggunaan teknologi seperti komputer, tidak jarang yang menggunakannya untuk kejahatan *cyber*. Namun, untuk mengemukakan bukti dalam suatu kejahatan cyber, diperlukan suatu *skill* untuk dapat menganalisis bukti dari tersangka. *"Komputer forensik dibutuhkan untuk memproses, dan menafsirkan bukti-bukti nyata sehingga membuktikan tindakan penyerang di pengadilan. Dengan analisis komputer forensik, hampir semua kejahatan cyber dapat ditangani, karena komputer forensik dapat melacak pelaku sampai berbagai belahan dunia."* (Sulianta, 2008).

2.2 iPod Touch

iPod Touch adalah merek serangkaian perangkat pemutar media digital yang dirancang dan dijual oleh Apple Computer (Hewlett-Packard juga sempat menjual produk tersebut dengan nama *Apple iPod Touch + HP*). Nama "iPod Touch" juga dahulu merupakan nama salah satu varian pemutar media digital dalam rangkaian tersebut (varian ini kini disebut "iPod Touch classic"). Sebagian besar varian iPod Touch memberikan antarmuka pengguna *(user interface)* yang sederhana dengan menggunakan disain dalam bentuk roda putar *(scroll wheel)*. *iPod Touch classic* menyimpan datanya di dalam sebuah *hard drive*, sementara model lainnya menggunakan *flash memory*. Seperti sebagian besar perangkat pemain musik lainnya, iPod Touch bisa digunakan sebagai *hard drive* eksternal bila disambungkan ke sebuah computer (Yoppie, 2008).

Tony Fadell pertama kali mendapat ilham untuk membuat iPod Touch di luar perusahaan Apple Computer: saat itu ia mengalami kesulitan mencari dana untuk membiayai perangkat pemain musik yang ia ciptakan. Pada waktu ia menunjukkannya kepada Apple Computer, perusahaan tersebut menyewanya sebagai kontraktor mandiri untuk membuahkan hasil dari projek ini. Ia diberikan

tanggung jawab untuk menggalang tim yang akan mengembangkan dua generasi pertama dari perangkat ini. Setelah itu perkembangan iPod Touch yang selanjutnya dilakukan di bawah naungan Jonathan Ive yang merupakan kepala grup disain industri di Apple Computer (Yoppie, 2008).

Sampai bulan Oktober 2004, iPod Touch mendominasi penjualan perangkat pemain musik di Amerika Serikat, dengan meraih 92% dari pasaran perangkat *hard drive* dan lebih dari 65% dari pasaran jenis lainnya. iPod Touch telah berhasil dijual dengan pesat, melebihi sepuluh juta unit dalam tiga tahun terakhir ini. Perangkat tersebut mempunyai pengaruh kebudayaan yang sangat besar di masyarakat bila dibanding dengan saat alat tersebut pertama kali diluncurkan (Yoppie, 2008).

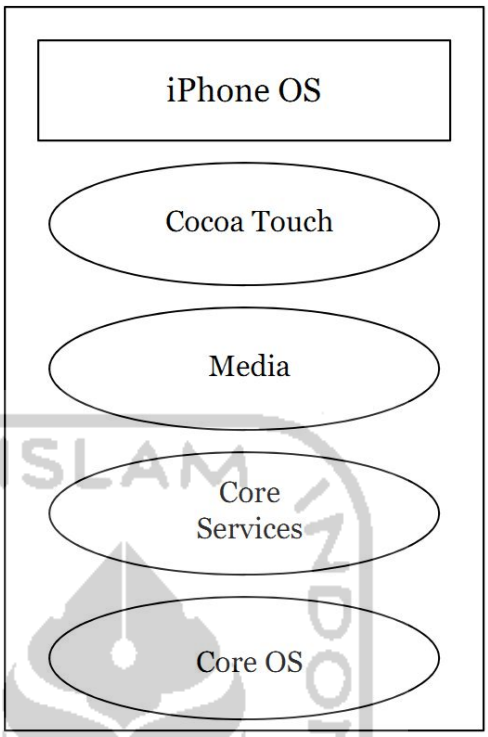
2.2.1 iOS

iOS adalah sistem operasi yang terdapat pada produk-produk yang diciptakan perusahaan Apple Computer. iOS awalnya hanya dikembangkan untuk Iphone. Namun sekarang sudah diperluas untuk perangkat Apple yang lainnya seperti iPod Touch, iPad, dan Apple TV (Saragih, 2011).

iOS merupakan sistem operasi yang berasal dari MAC OS X. iOS mempunyai 4 layer abstraksi, dimana layer abstraksi ini memakan lebih dari setengah Giga Byte (GB) dari total *Memory Storage* (Media Penyimpanan). Layer abstraksi itu adalah (Computer Hacking Forensic Investigation, 2006) :

a. *The core OS layer*
b. *The core services layer*
c. *The media layer*
d. *The cocoa touch layer*

Layer Abstraksi tersebut bisa dilihat pada Gambar 2.1.



Gambar 2.1 *Abstraction Layers*
(Sumber : Modul XXXVII CHFI EC-Council)

2.2.2 iPod Touch *Disc Partition*

Pada dasarnya, iPod Touch memiliki flash memori bertipe Solid State NAND yang terbagi menjadi 2 partisi (Computer Hacking Forensic Investigation, 2006) :

a. *Root Partition.* Partisi ini berukuran 300 MB, didalamnya memuat iOS dan segala aplikasi dasar dari iPod Touch seperti Safari, iTunes, dan lain-lain.Partisi ini telah di-*mount read-only* secara *default.*

b. *User Partition.* Partisi ini memuat data user, seperti musik, gambar, video, dan lain-lain. Partisi ini di-*mount* pada /private/var/ pada iPod Touch.

iPod Touch memiliki 2 jenis sistem file, yaitu HFS+ dan FAT32. iPod Touch akan menggunakan sistem file HFS+ ketika terhubung dengan perangkat MAC OS. iPod Touch akan menggunakan sistem file FAT32 ketika terhubung dengan perangkat PC Windows.

2.2.2.1 HFS+

HFS+ adalah sistem file yang dikembangkan oleh Apple Inc. untuk menggantikan *Hierarchical File System* (HFS) sebagai sistem file utama yang digunakan dalam komputer Machintosh (atau sistem lain yang menjalankan Mac OS). File sistem ini juga salah satu format yang digunakan oleh iPod Touch. HFS+ juga disebut sebagai MAC OS Extended, sebagaimana pendahulunya, HFS disebut sebagai MAC OS Standar (Developer, 2004).

2.2.2.2 FAT32

FAT atau *File Allocation Table* adalah sebuah sistem file yang menggunakan struktur alokasi tabel untuk beroperasi. Sistem file ini sekarang sudah banyak digunakan dalam sistem komputer dan kartu-kartu memori yang digunakan dalam kamera digital atau pemutar media portabel. FAT pertama kali ditemukan oleh Bill Gates dan Marc McDonald pada tahun 1976-1977. Sistem File ini merupakan sistem file utama untuk sistem operasi yang ada pada saat itu (Zeeis, 2008).

Ada beberapa versi dari sistem file FAT, yang dibedakan dari berapa banyak unit alokasi yang didukung. Versi tersebut antara lain FAT 12, FAT16, FAT32, dan exFAT (Zeeis, 2008).

2.2.1 Format Aplikasi

Secara umum, format aplikasi adalah suatu tipe pada file dimana tipe tersebut merupakan sebuah inisialisasi untuk membaca (*read*) atau menulis (*write*) file pada suatu aplikasi. Format aplikasi bersifat unik. File yang tersimpan dengan suatu format aplikasi, dapat dibuka di platform mana saja. Hanya saja, platform tersebut harus mendukung untuk membaca format aplikasi tersebut.

Adapun format aplikasi untuk iPod Touch adalah seperti yang terlihat pada Gambar 2.2 berikut ini.

Feature	Application Format
Contact information	vCard
Calendar entries	vCalendar
Audio	AAC, Protected AAC, MP3, MP3 VBR, Audible (formats 2, 3, and 4), Apple Lossless, AIFF, and WAV
Video	H.264 video, .m4v, .mp4, MPEG-4 video, and .mov

Gambar 2.2 Format Aplikasi pada iPod Touch
(Sumber : Modul XXXVII CHFI EC-Council)

2.3 iPod Touch Forensik

Penyelidikan digital forensik tidak terbatas pada komputer saja. Namun semua barang elektronik yang terdapat dalam TKP juga harus di identifikasi. Terlebih sekarang, *smart device* dapat menggantikan peran komputer dimanapun. Karena ukurannya yang relatif bersahabat dengan genggaman dan saku, membuat orang terkadang lebih mengutamakan menyimpan segala keperluan dalam aktifitasnya secara mobile. Sehingga besar kemungkinannya untuk mendapatkan banyak informasi dari *smart device* ini.

Apple iPod Touch adalah pemutar musik digital yang paling umum sekarang. Setelah menjual lebih dari empat juta unit, iPod Touch terus meroket dalam kesuksesan Thomas (2004). Kombinasi dari iTunes Apple dan iPod Touch telah menjadi gebrakan luar biasa di pasar musik digital dan menjadi kekuatan pendorong bagi revolusi musik digital.

Sebagian besar, orang-orang menggunakan iPod Touch sebagai hiburan. Namun perangkat ini tidak terbatas hanya sebagai media hiburan, fitur-fitur lain dari iPod Touch memungkinkan seseorang untuk mencatat memo, mengirim dan menerima email, menyimpan *to-do list* di kalender, serta *browsing* internet. Dari fitur-fitur ini dapat menyimpan banyak sekali informasi terkait kepemilikan iPod Touch tersebut. Selain itu, fitur-fitur tersebut sangat memungkinkan untuk

digunakan dalam jalur kriminal. Oleh karena itu, iPod Touch tidak bisa diabaikan dalam penyelidikan forensik.

2.4 Jailbreak iOS

Menurut Hoog & Strzempka (2011), *Jailbreak iOS* adalah menggantikan *firmware* asli dari Apple dengan versi *firmware* yang telah di *hack*, yang memungkinkan pengguna mendownload perangkat lunak yang tidak tersedia di *AppStore.* Sedangkan Morrissey (2010) mengumpamakan *Jailbreak iOS* seperti menggandakan film DVD yang memungkinkan membuat salinan illegal dari film tersebut.

Sehingga dapat ditarik kesimpulan bahwa *Jailbreak iOS* merupakan metode untuk melegalkan keterbatasan pada perangkat Apple dengan sistem operasi berbasis iOS. Proses *Jailbreak* ini akan menghilangkan garansi pada perangkat iOS.

Jailbreak ditemukan pertama kali pada tahun 2007 pada iOS versi 1.0. proses *Jailbreak* tersebut dilakukan oleh Iphone Dev Team, sebuah team untuk membangun utilitas untuk memperbolehkan aplikasi yang tidak terotorisasi Apple agar dapat berjalan pada perangkat iOS.

2.5 SSH

Menurut Muhartin (2009), SSH (Secure Shell) merupakan standar yang digunakan untuk login dan mengendalikan komputer dari jarak jauh. Dimana SSH merupakan pengganti aplikasi telnet dan rlogin karena dianggap kurang oleh seorang admin untuk mengontrol komputernya dari jarak jauh. SSH mempunyai kelebihan, yaitu :

a. Enkripsi password dan perintah-perintah, yang mana akan terlindung dari sniffer.
b. Fitur Tunneling, yang mana paket-paket perintah akan di proses dan dikirimkan melalui jaringan yang berbeda.
c. Klien SSH hampir ada di setiap sistem operasi.
d. Menggunakan kode khusus untuk identifikasi klien.

Versi Protokol SSH ada 2, yaitu versi 1 dan 2. Yang membedakannya adalah identifikasi dan enkripsi untuk menghubungkan komputer client dengan server. Protokol ini menggunakan port 22.

Untuk SSH client banyak macamnya. Di lingkungan Windows biasanya menggunakan PuTTY yang merupakan aplikasi client SSH yang portable dan aman. Sedangkan untuk sistem operasi Macintosh menggunakan MacSSH.

2.5.1 Moba SSH

Moba SSH adalah salah satu aplikasi openssh untuk perangkat windows yang memungkinkan untuk menjalankan perintah-perintah dan transfer data ke berbagai sistem operasi.

2.5.2 Open SSH

openSSH merupakan contoh aplikasi server untuk protokol SSH. Konfigurasi openSSH biasanya terdapat di "/etc" dan "/etc/ssh". Open SSH ini merupakan aplikasi *preload* pada perangkat iOS yang telah di *jailbreak.*

2.6 Write Blocking

Write Blocking adalah teknik yang digunakan dalam komputer forensik untuk menjaga integritas data dari perangkat penyimpanan data. Teknik ini dapat digunakan pada komputer bersistem operasi Windows, Linux dan Macintosh. Tiap sistem operasi mempunyai cara yang berbeda dalam melakukan *Write Blocking. Write Blocking* juga bisa memakai Software seperti PDBLOCK atau WiebeTech Forensic SATADock (Computer Hacking Forensic Investigation, 2006).

2.7 FTK

Forensic Toolkit atau FTK adalah software komputer forensik yang di terbitkan oleh Access Data. Software ini dapat mencari berbagai informasi dari suatu perangkat. Dapat mencari file yang telah terhapus atau juga *bad extension.* (Bruce, 2007)

Forensic Toolkit ini juga mencakup program *disk imaging* yang disebut FTK Imager. FTK Imager adalah alat sederhana namun ringkas. FTK Imager

dapat membuat file *image* dari perangkat atau media penyimpanan. Hasilnya adalah file *image* DD baku.

2.8 Oxygen Forensic Suite

Oxygen Forensic Suite adalah sebuah software analisis *mobile* forensik dari ponsel, smartphone dan PDA yang dikembangkan oleh Oxygen Software. Software ini dapat mengekstrak informasi perangkat, kontak, peristiwa kalender, pesan SMS, event log, dan file lainnya. Selain itu, software ini juga dapat mengekstrak metadata yang terkait dengan di atas (Oxygen, 2000).

Pada versi yang terakhir, yaitu OFS 2012, software ini didukung lebih dari 3.500 perangkat, termasuk Nokia, Apple seri iPhone, Apple iPod Touch, Apple iPad, Vertu, Sony Ericsson, Samsung, Motorola, Blackberry, Panasonic, Siemens, HTC, HP, E-Ten, Gigabyte , i-Mate,Ponsel Cina (Mediatek) dan ponsel lainnya. Suite ini juga mendukung perangkat yang menjalankan OS Symbian, Windows Mobile 5/6 dan OS Android (Oxygen, 2000).

2.9 DD

Dalam komputasi, dd adalah program umum pada system operasi Unix yang berfungsi untuk menggandakan atau mengkonversi data mentah. Menurut halaman manual Unix Versi 7, dd berfungsi mengubah dan menyalin file. Hal ini digunakan untuk menyalin sejumlah tertentu byte atau blok (Sam, 2008).

Baris perintah sintaks dd secara signifikan berbeda dari kebanyakan program-program Unix lainnya, karena *ubiquity*-nya rentan terhadap perintah terakhir untuk menegakkan sintaks umum untuk semua alat baris perintah. Umumnya, hh menggunakan option = Format nilai, sedangkan program Unix menggunakan pilihan - pilihan = Format nilai. Selain itu, input ditentukan menggunakan pilihan (dari file input), sedangkan sebagian besar program hanya mengambil nama dengan sendirinya (Sam, 2008) .

Dd tidak memiliki algoritma selain perintah pengguna tentang bagaimana bervariasi pada pilihan run. Seringkali perintah tidak berubah dalam menjalankan dd pada proses multi-langkah untuk memecahkan masalah komputer (Sam, 2008).

BAB III
METODOLOGI

3.1 Studi dan Pengumpulan data

Berbagai kemampuan yang dimiliki oleh Apple iPod Touch dapat digunakan sebagai salah satu cara untuk melakukan kejahatan. Dengan adanya digital forensik akan diketahui siapa, apa, bagaimana, dan kapan waktu kejadian tersebut akan terjadi. Namun, untuk memperoleh bukti-bukti tersebut diperlukan sebuah langkah-langkah tertentu.

iPod Touch sebagai barang bukti tidak boleh diforensik secara langsung. Setelah pengambilan iPod Touch dari Tempat Kejadian Perkara (TKP), iPod Touch di *cloning byte per byte* atau *raw data copy* dengan software dd. Namun, agar iPod Touch dapat dikenali perangkatnya oleh komputer, maka komputer tersebut harus menginstall iTunes terlebih dahulu.

Hasil *cloning* iPod Touch tersebut, kemudian di selidiki menggunakan *tools* forensik. *Tools* yang akan digunakan adalah FTK (Forensic Toolkit) dan Oxygen Forensic Suite. FTK menyidik device secara keseluruhan file, sedangkan Oxygen Forensic Suite menyidik content dari suatu device.

3.1.1 Spesifikasi dan Karakteristik iPod Touch

iPod Touch diproduksi dengan banyak versi, dan setiap versi mempunyai spesifikasi yang berbeda-beda dari model maupun hardware. iPod Touch yang dipakai untuk penelitian ini mempunyai spesifikasi sebagai berikut :

a. iPod Touch *2nd generation.*
b. RAM 128 MB
c. iOS versi 4.2.1 (8C148).
d. Harddisk kapasitas 8GB

iPod Touch generasi kedua mempunyai body yang tipis, dengan *chroom stainless* di bagian belakang. Untuk bagian depan dilapisi dengan fiber dan warna dasar *default* adalah hitam. Selain terdapat *built-in speaker,* iPod Touch *2nd Generation* ini memiliki tombol volume *up* dan *down* di bagian samping kiri dan

memiliki tombol *off* di kiri atas. Jika penampang dari atas, hanya terdapat satu tombol yaitu tombol menu di tengah bagian bawah.

3.1.2 Tahapan pada Komputer Forensik

Pada Gambar 3.1, merupakan gambaran dimana dalam komputer forensik ada 4 tahapan yang dilakukan untuk menginvestigasi suatu kasus pada barang bukti, yaitu pengumpulan, pengujian, analisis, dan laporan (Sulianta, 2008). Ada objek yang dikelola dari proses setiap tahapan, dimulai dari media dan berakhir dengan output *evidence* atau barang bukti.

Gambar 3.1 Tahap-tahap komputer forensik

3.1.2.1 Pengumpulan Data

Ini adalah langkah pertama yang harus dilakukan dalam proses forensik untuk mengidentifikasi sumber dan bagaimana data dari iPod Touch dikumpulkan. Pengumpulan data ini mencakup aktivitas seperti :

a. Identifikasi
b. Penamaan (*labelling*)
c. Perekaman (*recording*)
d. Mendapatkan data

3.1.2.2 Pengujian

Setelah melewati proses pengumpulan data, tahap selanjutnya adalah pengujian. Tahap ini merupakan proses dimana data dari iPod Touch diekstraksi dan dikumpulkan sehingga menghasilkan informasi terkait dengan kasus.

Ada banyak *tools* yang digunakan dalam proses ini. Yaitu *tools* untuk membuat file *back up,* untuk menyidik file *back up* dan untuk membuat *image*

pada struktur file iPod Touch. Pada tahap ini juga diuraikan cara untuk dapat membaca dan menyidik *image* tersebut.

3.1.2.3 Analisis

Tahapan selanjutnya setelah proses pengujian adalah analisis terhadap data yang diperoleh. Begitu data diekstrak, penyidik melakukan analisis terhadap data yang berisi informasi tersebut. Sehingga penyidik dapat merumuskan kesimpulan dalam menggambarkan data.

3.1.2.4 Dokumentasi dan laporan

Dokumentasi dan laporan adalah tahap akhir dari proses komputer forensik. Dalam tahap ini penyidik merepresentasikan informasi yang merupakan hasil dari proses analisis.

3.2 Metodologi Penelitian

Secara umum, metodologi penelitian yang dibuat pada penelitian ini mencakup segala aspek pada Tahapan Komputer Forensik. Metodologi pada penelitian ini bisa dilihat pada Gambar 3.2.

Gambar 3.2 Gambaran Umum Skenario

3.2.1 Skenario Kasus

Asumsi telah ditemukan seorang tersangka *spyer* pada website SMA Negeri 1 Cilacap, dan ditemukan iPod Touch sebagai barang bukti pada TKP ketika dilakukan penyerbuan ke rumah tersangka. iPod Touch ini akan diforensik dan diselidiki untuk melihat apakah ada barang bukti yang tersimpan didalam iPod Touch untuk membantu penyelidikan. Selain itu penyelidikan ini berguna

untuk mengetahui barang bukti apa saja yang berpotensi bisa tersimpan dalam iPod Touch.

3.2.2 Pengumpulan Barang Bukti

Dalam Metodologi Penelitian ini, Pengumpulan Barang Bukti termasuk dalam tahapan Pengumpulan pada tahap-tahap Komputer Forensik menurut Sulianta Feri. Ini adalah langkah pertama dalam proses forensik untuk mengidentifikasi sumber – sumber potensial dan bagaimana kemudian data dikumpulkan. Dalam hal ini, iPod Touch sebagai barang bukti diambil karena merupakan barang digital yang terdapat di area TKP. Selanjutnya iPod Touch tersebut diamankan di laboratorium forensik, agar kemanan data terjaga.

3.2.3 *Write Blocking, Back up* dan *Imaging* iPod Touch

Write Blocking, Back up dan Imaging iPod Touch termasuk dalam tahapan Pengujian dalam tahapan Komputer Forensik menurut Sulianta Feri. Dimana pada tahapan ini adalah tahap dimana data diproses mulai dari proses duplikasi sampai ekstraksi.

3.2.3.1 *Write Blocking*

Write Blocking merupakan teknik untuk mempertahankan keaslian data pada saat pemeriksaan. Pada saat iPod Touch terhubung dengan komputer untuk ditindaklanjuti, sangat memungkinkan pertukaran data terjadi antara iPod Touch dan komputer, baik secara sengaja maupun tidak disengaja. *Write Blocking* berguna untuk menutup akses penulisan data pada media penyimpanan yang terhubung pada komputer melalui USB.

3.2.3.2 *Back up* iPod Touch

iPod Touch merupakan perangkat pemutar multimedia yang memiliki kemampuan menyimpan data personal. Data personal ini meliputi Memo, Kalender, Kontak, Log GPS, serta *cache* dari *Web Browser.* Data personal ini dapat di-*back up* dengan software pemutar musik dari Apple yaitu iTunes. Data *back up* dari iTunes ini, kemudian akan diekstrak serta disidik dengan menggunakan *tools* forensik Oxygen Forensic Suite *2011.*

Data personal memiliki banyak sekali informasi mengenai pemilik *device,* orang-orang dekat atau kerabat dari pemilik, serta keseharian dan lokasi si pemilik *device*. Sehingga menyidik file *back up* dari iPod Touch ini merupakan sesuatu yang perlu.

3.2.3.3 *Imaging* iPod Touch

Proses *Imaging* pada suatu barang bukti digital merupakan keharusan dalam proses forensik. Proses ini menghindari rusaknya data atau barang bukti yang bersifat rapuh. iPod Touch merupakan perangkat Apple dengan akses file yang benar-benar tertutup. Butuh aplikasi pihak ketiga atau dengan menggunakan metode *jailbreak* untuk dapat mendapatkan akses file ke dalam iPod Touch. Berbeda dengan iPod Touch sebelum iPod Touch yang mempunyai fitur *Disc Mode* untuk dapat mengakses file.

Untuk dapat meng-*image* suatu perangkat, perangkat tersebut harus dikenali sebagai media penyimpanan fisik maupun lojik. Pada iPod Touch, perangkat ini akan dikenali sebagai perangkat gambar/perangkat musik sehingga tidak dapat dikenali sebagai media penyimpanan fisik atau lojik.

Cara yang dilakukan untuk dapat meng-*image* iPod Touch adalah dengan menggunakan SSH untuk meremot iPod Touch dari PC, selanjutnya digunakan perintah dd untuk meng-*image* disk dari iPod Touch. Setelah *image* dari iPod Touch berhasil dibuat, selanjutnya *image* tersebut diekstrak dengan menggunakan software Data Rescue.

Setelah data yang telah diekstrak diperoleh, selanjutnya menyidik data tersebut dengan menggunakan *tools Forensic Tool Kit* (FTK).

3.2.4 Analisis Data

Setelah uji coba skenario dan *imaging* serta *back up* dilalui, maka sampai ke tahap analisis data. Analisis data merupakan proses dimana merumuskan data-data yang didapat melalui proses *imaging* dan *back up* tadi menjadi sebuah informasi yang merujuk kepada kasus.

Analisis terhadap barang bukti pada dasarnya bertujuan untuk membentuk dan mengikuti petunjuk yang ada, mengidentifikasi tersangka, format

data, pengembangan barang bukti, merekonstruksi kejahatan yang dilakukan, dan mengumpulkan lebih banyak data. Jadi pada dasarnya data digital hanyalah bagian dari keseluruhan gambaran umum. Dalam melakukan analisis ini akan dihadapkan pada data yang berlimpah. Untuk itu diperlukan proses eliminasi maupun pengalaman dalam melakukan analisis.

3.2.5 Laporan

Tahap ini merupakan tahap dimana semua proses yang diajalani di dokumentasikan dalam sebuah laporan. Laporan ini mencakup ringasan hasil selama masa penyelidikan, serta bukti spesifik untuk membuktikan kesimpulan. Kesimpulan yang diambil harus jelas dan tidak membingungkan.

3.2.6 Presentasi

Tahapan yang terakhir adalah Presentasi. Pada presentasi ini penyidik berperan sebagai *expert witness* atau saksi ahli, dimana presentasi ini menjelaskan semua hasil penyelidikan secara garis besar dan bersifat tidak memihak.

BAB IV
HASIL DAN PEMBAHASAN

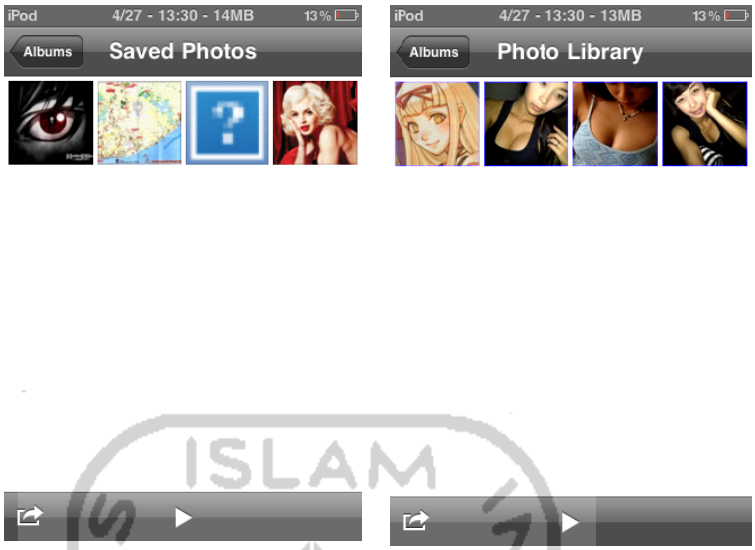
4.1 Skenario Kasus

Ketika dilakukan *maintenance* oleh admin website SMA Negeri 1 Cilacap, terdeteksi adanya *spyer* yang telah masuk sebagai admin pada website tersebut. Sehingga kasus ini diadukan ke polisi karena takut data didalam website disalahgunakan. Setelah itu, kepolisian segera menindak lanjuti si pelaku kejahatan *cyber* tersebut dengan melakukan penyerbuan ke rumah tersangka. Pada TKP (rumah tersangka), terdapat beberapa barang elektronik salah satunya adalah iPod Touch. iPod Touch tersebut milik Toni Ikhwanurahman yang merupakan seorang pelaku *spyer* pada website SMA Negeri 1 Cilacap.

Pada kasus ini, Toni Ikhwanurahman telah melakukan pencurian data, *web hacking* dengan *sql injection,* menyimpan dan mengirimkan informasi dari sekolah tersebut, serta mengirimkan email ancaman. Dengan skenario tersebut akan dilakukan penyelidikan terhadap iPod Touch. Penyelidikan tersebut berguna sebagai pembuktian kepada kejahatan-kejahatan yang telah dilakukan Toni Ikhwanurahman. Selain itu, dengan penyelidikan ini juga dapat diketahui barang bukti apa saja yang bisa terdapat pada iPod Touch.

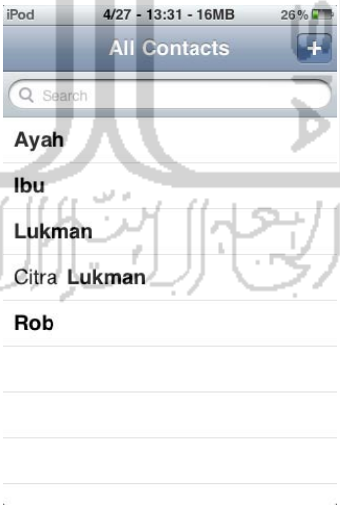
Untuk melakukan pembuktian, maka perlu diperlihatkan *screenshot* pada iPod Touch untuk pembuktian pada saat proses forensik. *Screenshot* ini akan menjadi penjelas dari barang bukti ketika iPod Touch belum diforensik.

Pada Gambar 4.1 terdapat *screenshot* pada folder-folder gambar, yaitu Photo Library dan Saved Photos. Dimana untuk melihat gambar tersebut tidak harus masuk ke dalam system file, tapi masuk ke dalam menu *Photos* pada menu iPod Touch.



Gambar 4.1 *Screenshot* pada folder-folder gambar yaitu *Saved Photos* dan *Photo Library*

Pada Gambar 4.2 adalah merupakan urutan daftar kontak yang terdapat pada barang bukti iPod Touch. Cara masuk ke daftar kontak adalah dengan klik menu *Contact* pada menu iPod Touch.

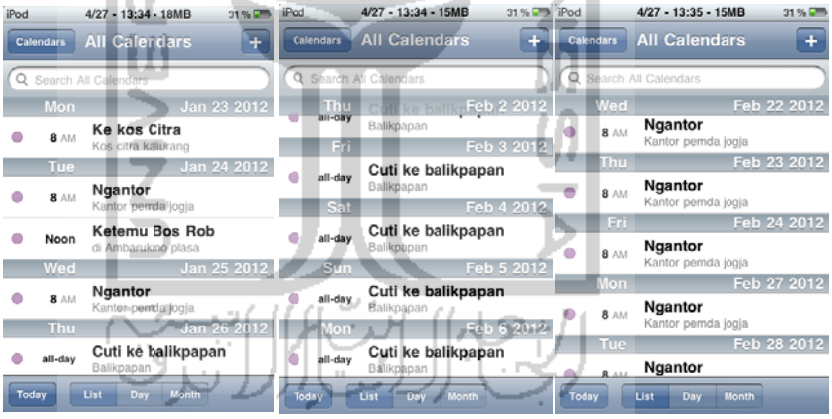


Gambar 4.2 Daftar kontak pada iPod Touch

iPod Touch mempunyai fitur *Map*, dimana ketika membuka aplikasinya yang bernama *Maps*, terlihat hasil pencarian tempat yang telah dicari. Seperti pada Gambar 4.3 merupakan hasil pencarian pada tempat bernama Yaho.

Gambar 4.3 Hasil pencarian pada *Maps*

iPod Touch mempunyai fitur alarm yang dijadikan satu tempat pada *appointment calendar*. Dimana jika melihat alarm tersebut maka harus membuka *Calendar* pada menu iPod Touch seperti yang terlihat pada Gambar 4.4.



Gambar 4.4 Fitur *alarm* pada *Calendar*

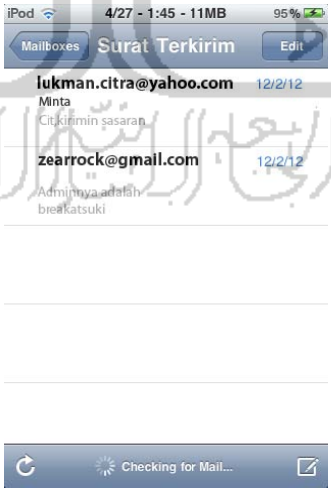
Pada Gambar 4.5, merupakan isi dari *Notes* pada iPod Touch.

Gambar 4.5 Isi Notes dari iPod Touch

Selanjutnya pada Gambar 4.6 menunjukkan bahwa struktur file bisa dilihat dalam aplikasi *iFile* pada iPod Touch. Dimana *iFile* merupakan aplikasi *explorer* bawaan pada iPod Touch. Namun, tidak bisa mengidentifikasi file yang di-*hidden.*

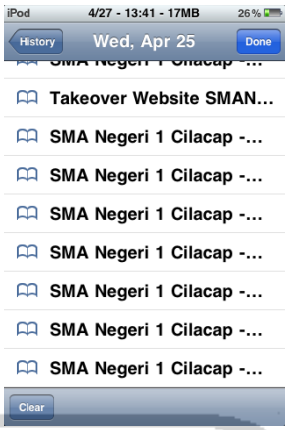
Gambar 4.6 Struktur File pada iPod Touch dalam aplikasi *iFile*

Berikutnya pada Gambar 4.7 merupakan *screenshot* pada E-mail.



Gambar 4.7 Salah satu *screenshot* pada E-mail

Pada Gambar 4.8 merupakan *screenshot* pada history web browser bawaan iPod Touch yaitu Safari.



Gambar 4.8 *Web History* pada Safari

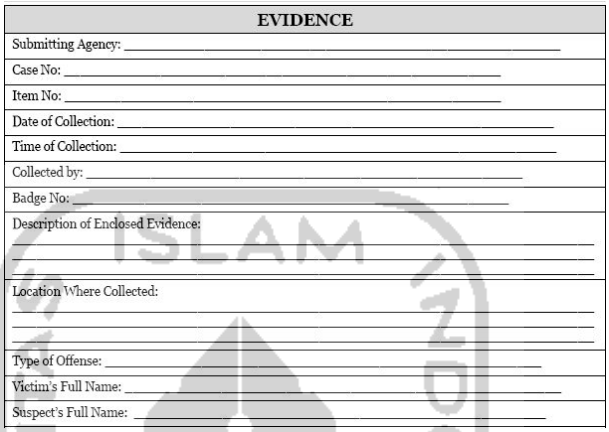
Yang terakhir adalah informasi pada iPod Touch yang bisa dilihat dalam *About* pada *Setting*. Pada *About* tertera informasi-informasi terkait iPod Touch dari versi, model, sampai *MAC Address* dari WiFi dan Bluetooth seperti yang terlihat pada Gambar 4.9.

Gambar 4.9 Informasi iPod Touch pada *About*

4.2 Pengumpulan Barang Bukti

Pada tahap ini, semua barang bukti dikumpulkan untuk mendapatkan suatu petunjuk dari suatu tindak kejahatan. Dalam skenario kasus ini, iPod Touch dikumpulkan untuk menjadi barang bukti pada tahapan ini. Setelah mendapatkan *Search Warrant* sebagai ahli forensik, penyidik harus mengamati dan memahami kejadian di Tempat Kejadian Perkara (TKP) dengan cara mencatat dan mengambil foto pada TKP. Setelah mengamati TKP, lalu penyidik mengumpulkan iPod

Touch sebagai barang bukti. iPod Touch harus diberi *tag* yang menjelaskan informasi detail pada iPod Touch. Setelah iPod Touch diberi *tag,* selanjutnya mengisi *Evidence Form.* Gambar 4.10 merupakan contoh *Evidence Form.*



EVIDENCE
Submitting Agency: _____
Case No: _____
Item No: _____
Date of Collection: _____
Time of Collection: _____
Collected by: _____
Badge No: _____
Description of Enclosed Evidence: _____ _____ _____
Location Where Collected: _____ _____ _____
Type of Offense: _____
Victim's Full Name: _____
Suspect's Full Name: _____

Gambar 4.10 *Evidence Form*
(Sumber : Modul XXXVII CHFI EC-Council)

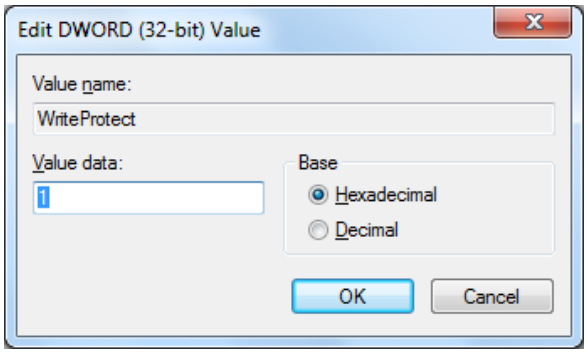
Selanjutnya, iPod Touch dimasukkan kedalam *Stronghold Bag* agar aman dan tidak bisa menangkap sinyal wifi.

4.3 *Write Blocking, Back up* iPod Touch dan Ekstraksi data dari file *Back up*

4.3.1 *Write Blocking*

Sebelum melakukan *back up*, perlu melakukan *write blocking* agar tidak terjadi pertukaran data yang tidak disengaja. Berikut ini merupakan langkah-langkah *Write Blocking* pada Windows :

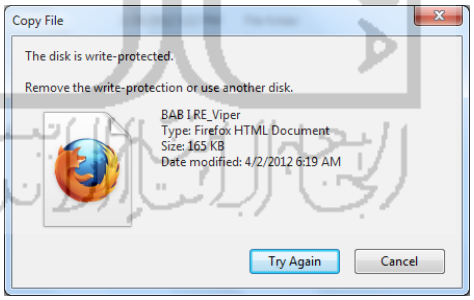
a. Buka *Registry Editor*
b. Arahkan pada HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
c. Buat *key* baru dengan nama *StorageDevicePolicies.*
d. Pada *key* tersebut, buatlah sebuah DWORD (32-bit) *Value* dengan nama *WriteProtect,* seperti yang terlihat pada Gambar 4.11.
e. Klik dua kali pada *WriteProtect* dan atur *ValueData* menjadi 1.



Gambar 4.11 Membuat DWORD (32-bit)

Tanpa di-*restart*, semua *user* pada komputer tidak akan bisa meng-*copy*, transfer, atau menulis data pada media penyimpanan yang terhubung pada USB. Jika hal tersebut dilakukan maka akan muncul peringatan "*The disk is write protected. Remove the write protection or use another disk*". Pada Gambar 4.12 diperlihatkan bahwa peringatan tersebut muncul, maka proses *Write Blocking* berhasil.

Jika ingin mengembalikan atau *write unblocking*, cukup dengan mengganti *value* dengan angka 0.



Gambar 4.12 Peringatan pada *Write Protection*

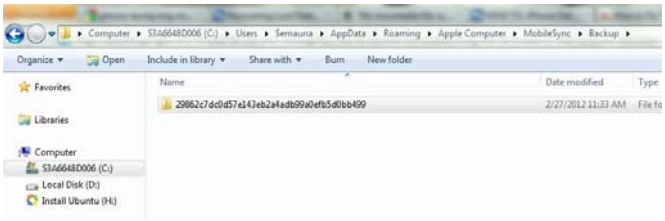
4.3.2 *Back Up* iPod Touch menggunakan iTunes

IPod Touch memiliki kemampuan untuk menyimpan data-data personal, sehingga dalam sisi forensik data personal ini perlu diselidiki. Data personal ini dapat di *back up* melalui software bernama iTunes. Oleh karena itu, perlu untuk menginstall iTunes terlebih dahulu untuk melakukan *back up* dari iPod Touch.

Langkah-langkah untuk melakukan *back up* pada iPod Touch adalah sebagai berikut :

a. Install iTunes pada komputer.
b. Nonaktifkan fitur *auto synchronize* pada iTunes, karena *Auto synchronize* akan menyamakan pengaturan lagu, video dan data lainnya antara iTunes dengan iPod Touch. Klik *edit* pada *menu bar*, lalu pilih *preferences. Check* pilihan *Prevent iPod Touchs, iPhones, and iPads from syncing automatically*. Klik OK.
c. Samakan jam dan tanggal serta *timezone* antara iPod Touch dengan komputer.
d. Sambungkan iPod Touch ke komputer dengan menggunakan kabel USB, setelah itu akan muncul *autorun* dan mengenal iPod Touch sebagai media gambar.
e. Buka iTunes sebagai *administrator* dengan cara klik kanan pada program iTunes, dan pilih *Run as Administrator*. Setelah iTunes terbuka klik kanan pada iPod Touch, lalu pilih *back up.*
f. Maka selanjutnya, iTunes akan membuat *back up* pada iPod Touch. Lokasi penyimpanan *back up* ini adalah C:\Users\[username]\AppData\Roaming\Apple Computer\MobileSync\Backup.

File *back up* ini nantinya akan diforensik menggunakan tool Oxygen Mobile Forensik. File *back up* (Gambar 4.13) ini dilakukan secara manual, agar tidak terjadi persilangan data karena penyamaan data antara komputer dan iPod Touch.

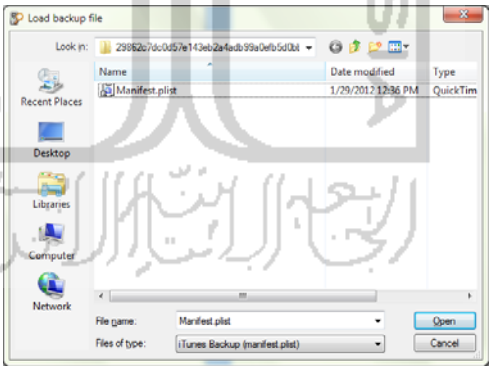


Gambar 4.13 hasil dari iTunes *back up*

4.3.3 Ekstraksi file *back up* Menggunakan Oxygen Forensic Suite

Setelah *back up* iPod Touch, selanjutnya akan mengekstraksi file *back up* tersebut dengan Oxygen Forensic Suite. Langkah-langkah untuk mengekstraksi file *back up* iPod Touch adalah sebagai berikut :

a. Buka program Oxygen Forensic Suite, lalu pilih *Load Back up File* untuk membuat *case* baru berdasarkan pada file *back up*. Dengan menu ini, penyidik dapat memilih beberapa file *back up*. Karena dalam kasus ini akan menyidik file *backup* dari iTunes, maka yang akan dipilih adalah *Load Backup File* lalu *iTunes Backup*. Selanjutnya lokasikan alamat folder ke C:\Users\[username]\AppData\Roaming\Apple Computer\MobileSync\Backup dimana alamat tersebut merupakan alamat *default* file *back up* dari iTunes. Sehingga dalam kasus ini karena memakai komputer dengan *username* "Semauna", alamat *default* menjadi C:\Users\Semauna\AppData\Roaming\Apple Computer\MobileSync\Backup. Seperti yang terlihat pada Gambar 4.14, file *back up* dari iTunes berformat manifest.plist.



Gambar 4.14 File *back up* dari iTunes yang akan disidik mempunyai format manifest.plist

b. Selanjutnya, *Backup Extraction Wizard* akan menampilkan window untuk mengisi informasi dari barang bukti. Informasi yang perlu di isi tersebut antara lain :

   i. *Device Alias* untuk member nama pada barang bukti. Untuk kasus ini, akan diberi nama iPod Touch.

   ii. *Device Owner* adalah pemilik dari barang bukti. Untuk kasus ini, pemilik dari iPod Touch tersebut adalah Toni Ikhwanurahman.

iii. *Case Number* adalah nomor kasus yang akan ditangani. Untuk kasus ini diisi dengan 1.

iv. *Hash Algoritm* adalah pencocokan kode enkripsi antara *device* sebenarnya dan data yang sudah di *extract.*

v. *Evidance Number* adalah nomor barang bukti yang akan disidik. Untuk kasus ini kita isi dengan 1.

vi. *Inspectator* adalah mengisi nama untuk penyidik. Untuk kasus ini di isi dengan Muhammad Zulfariansyah.

vii. *Device Notes* untuk mencatat hal-hal penting lainnya jika diperlukan.

c. Setelah klik *Next,* maka akan ditampilkan window untuk menambah informasi nomor telepon untuk pemilik perangkat. Lewati saja tahap ini dengan klik *Next.*

d. Selanjutnya akan ditampilkan informasi dari pengaturan yang sudah di isi sebelumnya. Lalu Klik *Extract*.

Setelah tahap *extracting data* selesai, maka akan ditampilkan window untuk memilih *Final Action. Final Action* ini diantaranya adalah :

a. *Save to Archieve,* untuk menyimpan file penyelidikan dari data yang sudah di *extract.*

b. *Open Device,* untuk membuka data dari data yang telah di *extract* tanpa disimpan.

c. *Export and Print,* Untuk membuat laporan dan langsung dicetak.

4.3.4 *Cloning* iPod Touch dan Ekstraksi data file *Image*

4.3.4.1 *Cloning* iPod Touch

Cloning merupakan suatu proses yang harus dilalui dalam forensik perangkat digital. Pada umumnya, *cloning* bisa dilakukan melalui *device to device* yaitu dari alat satu ke alat yang serupa, atau dengan menggandakannnya menjadi *disk image* dengan menggunakan *tool. Tool* untuk membuat *cloning image*-pun beragam, contohnya *EnCase* dan FTK *Imager.*

Pada *tools* untuk membuat *image*, media penyimpanan yang dapat di *image* adalah *physical drive* atau *logical image.* Seperti jika ingin membuat *disk image* pada *flashdisk* atau *hardisk external,* bisa dengan menggunakan FTK *Imager* dengan pilihan *physical drive.*

Sementara apabila iPod Touch dihubungkan dengan komputer, maka akan terdeteksi sebagai media gambar. Karena terdeteksi sebagai media gambar, komputer tidak mengenali iPod Touch sebagai *physical drive* dan *logical drive.* Hal ini menyebabkan iPod Touch tidak bisa di-*image* dengan menggunakan tools biasa seperti FTK *Imager* dan *disk image* seperti yang sudah disebutkan diatas. Untuk membuat *disk image* pada iPod Touch adalah dengan mengendalikan iPod Touch dengan menggunakan komputer untuk menggunakan software dd yang sudah terinstall *pre-load* pada iPod Touch.

Setelah melalui proses *imaging,* maka langkah selanjutnya adalah mengekstrak data didalam file *disk image.* Langkah tersebut bisa dengan mengekstrak langsung file *image* ke dalam *tool* forensik agar disidik secara langsung, atau dengan teknik *mounting* sehingga file *image* tersebut dibaca sebagai disk.

Namun, pada file *image* iPod Touch, jika di *mount* atau langsung di ekstrak ke dalam *tool* forensik akan mengalami kegagalan. Menurut Sood (2009), kegagalan ini dikarenakan sistem operasi tidak mendapatkan sistem file dalam format yang tepat untuk melakukan *mounting* pada *image.* Sehingga, untuk mengekstrak data pada hasil *cloning* yang bernama 'iphone-dump.img' tadi harus menggunakan teknik *recovery data.*

Sehingga, secara garis besar langkah pertama untuk menyidik *disk image* pada iPod Touch adalah dengan *cloning* iPod Touch dengan menggunakan program dd, dan selanjutnya adalah melakukan teknik *recovery data* pada hasil *cloning* iPod Touch tersebut.

4.3.4.2 *Cloning* iPod Touch dengan menggunakan dd

Salah satu cara untuk menghasilkan *raw data copy* file dari suatu *device* yang telah di *imaging* adalah dengan menggunakan software dd. Dan cara yang digunakan untuk *cloning* iPod Touch adalah me-*remote* iPod Touch melalui

komputer dengan software putty dan menggunakan perintah ssh lalu menjalankan perintah dd agar iPod Touch mengkloning disknya dan kembali me-*remote* komputer untuk meletakkan hasil *cloning* ke dalam komputer. iPod Touch dengan basis Sistem Operasi UNIX, mempunyai fitur dd secara *preload* tanpa harus diinstal terlebih dahulu.

Langkah-langkah untuk membuat *disk image* pada iPod Touch dengan menggunakan dd adalah sebagai berikut :

a. Pastikan iPod Touch dan komputer Windows terhubung ke dalam satu jaringan WiFi yang sama. Lalu ketahui kedua *address* masing-masing. Asumsi iPod Touch memiliki IP 10.0.0.170 dan komputer memiliki IP 10.0.0.169.

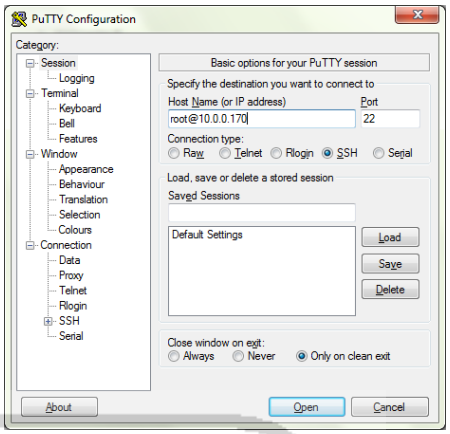
b. Jalankan aplikasi OpenSSH didalam komputer, seperti contoh dalam kasus ini menggunakan Moba SSH versi 1.22. Klik Start untuk menjalankan SSH pada komputer.

c. Siapkan iPod Touch yang telah di *jailbreak* dan pastikan sudah terinstal OpenSSH dalam *package installer*-nya. Umumnya, pada iPod Touch yang telah dijailbreak OpenSSH sudah terinstall didalamnya.

d. Matikan layanan *antivirus* dan *firewall* pada komputer selama kegiatan ini berlangsung, serta non-aktifkan *Auto-Lock* pada iPod Touch dengan Memilih Setting, selanjutnya pilih General, di Tab *Auto-Lock* pilih "Never".

e. Jalankan puTTY sebagai administrator (klik kanan, pilih *Run as Administrator*) untuk kepentingan mengenai hak akses.

f. Remote iPod Touch dengan puTTY dengan cara isi *field Host Name* dengan format namauser@IPaddresslokal. Nama user isi dengan root dan IP addressnya 10.0.0.170. Sehingga yang harus diisi di *field* Host name adalah root@10.0.0.170. Isi *port*-nya dengan 22, *connection type* pilih SSH dan setelah itu pilih open. Untuk lebih jelas, lihat pada Gambar 4.15.

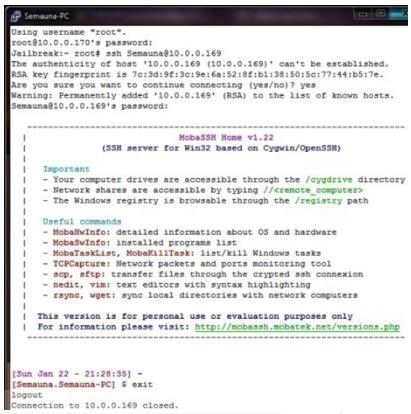


Gambar 4.15 puTTY untuk meremote iPod Touch

g. Jika berhasil, maka akan terbuka window baru berisi *command* yang meminta password root dari iPod Touchnya. ID untuk komputer adalah "Semauna" dan ID untuk iPod Touch adalah "Jailbreak" dan password dari iPod Touch "Jailbreak" adalah *alpine*. Setelah memasukkan password, *command* dari puTTY akan bertindak sebagai iPod Touch dengan hak akses *root.*

h. Selanjutnya ketik perintah "ssh Semauna@10.0.0.169" untuk mendapatkan hak akses *remote* ke komputer. Setelah itu, *command* akan meminta persetujuan untuk melanjutkan koneksi, ketik *yes* lalu enter.

i. Lalu *command* akan meminta password dari komputer. Masukkan password dan akan masuk ke dalam tampilannya Moba SSH. Ketik "exit" untuk keluar. Langkah ini dimaksudkan untuk mencoba apakah SSH sudah berhasil atau belum. Pada Gambar 4.16 menunjukkan bahwa tampilan Moba SSH telah berjalan yang menandakan proses SSH berhasil.



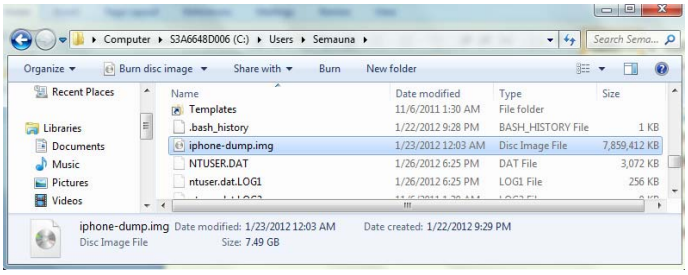
Gambar 4.16 Masuk kedalam tampilan Moba SSH

j. Setelah itu, *command* akan kembali masuk sebagai iPod Touch, lalu ketikkan perintah dd untuk *cloning hard drive* iPod Touch. Sebelumnya, pastikan program dd di komputer berada dalam direktori C:/ agar *command* mengenali bahwa komputer tersebut sudah menginstall program dd.

k. Perintah yang dimasukkan adalah "dd if=/dev/disk0 | ssh Semauna@10.0.0.169 'dd of=iphone-dump.img'". "dd if=/dev/disk0", dimaksudkan 'if' sebagai input yang akan diproses. Karena *command* berjalan sebagai iPod Touch, maka /dev/disk0 adalah direktori atau *harddrive* dari iPod Touch. Sedangkan '|' (*pipeline*) adalah menggabungkan 2 atau lebih perintah dalam satu eksekusi. "ssh Semauna@10.0.0.169" berarti meminta akses SSH ke komputer dengan ID 'Semauna' yang memiliki IP 10.0.0.169. Sedangkan "of=iphone-dump.img" berarti akan menghasilkan output berupa *raw image* dengan nama 'iphone-dump.img' ke direktori default dengan format .img, seperti yang terlihat pada Gambar 4.17. Dalam kasus ini, direktori default adalah C:\Users\Semauna. Lalu *command* akan meminta password komputer.

l. Setelah memasukkan password, maka proses *cloning* akan berjalan.

m. Setelah selesai, hasil *cloning* tersebut akan masuk ke dalam direktori C:\Users\Semauna. Karena pada penelitian ini memakai iPod Touch berkapasitas 8GigaByte, maka *raw data image* atau hasil dari proses *cloning* adalah sebesar 7,8 GB.



Gambar 4.17 Hasil *Cloning* berupa *disk image* berformat .img

4.3.5 Mengekstraksi file *disk image* pada iPod Touch

Menurut Sulianta (2008), tahap pengujian merupakan tahap dimana dilakukannya penilaian dan pengekstrakan informasi yang relevan dari data yang dikumpulkan. Sementara menurut Przibilla (2005), ekstraksi data bisa dari data-data yang telah dipulihkan (*recover*).

Umumnya, *recovery data* bisa dilakukan pada komputer windows. Namun, software-software *recovery data* windows tersebut umumnya me-*recover* data dari media penyimpanan *harddrive*. Kalaupun *support* untuk membaca file *image,* file *image* yang dapat dibaca adalah format yang umum seperti .iso atau format file *image* lain yang mendukung perangkat Windows. Sedangkan file *image* yang dibuat dalam proses *cloning* sebelumnya adalah *image* berformat .img.

Seperti contoh, *recovery tool* pada Windows seperti *'Recuva'* dan *'File Recovery'* tidak bisa mengidentifikasi file sistem dari iphone-dump.img karena alasan diatas.

4.3.5.1 *Recovery Disk Image* menggunakan *Data Rescue*

Pada penelitian ini, untuk proses *recovery* akan memakai *tool* bernama *Data Rescue* versi 3 yang berjalan pada perangkat Apple Macintosh. Karena dengan *Data Rescue*, file-file didalam iphone-dump.img bisa di-*recovery*. Nantinya, file hasil *recovery* inilah yang akan disidik secara forensik.

Langkah yang dilakukan untuk melakukan teknik *recovery* adalah sebagai berikut :

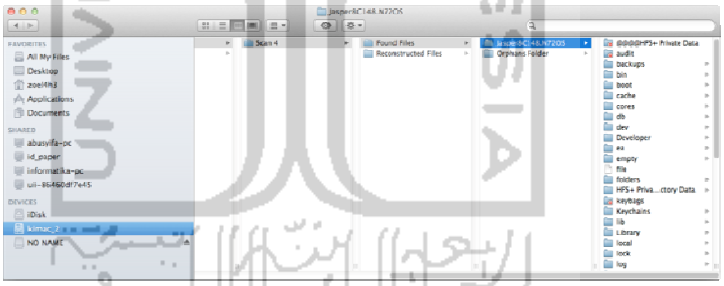
a. Menyediakan *harddrive* dengan kapasitas minimal 9 GB atau *flashdisk* 16GB yang berformat FAT32, karena iphone-dump.img yang berkapasitas 7,8GB tidak akan cukup jika disimpan kedalam *flashdisk* 8GB. *Copy* iphone-dump.img kedalam *flashdisk* tersebut.
b. Install program *Data Rescue* pada Mac PC.
c. *Copy* file iphone-dump.img ke dalam direktori Mac, hal ini bertujuan untuk mempercepat pembacaan data ketika proses *recovery* berlangsung.
d. Klik kanan file iphone-dump.img dan pilih Open With, lalu pilih Disk Utility.
e. Setelah window *Disk Utility* terbuka, klik dua kali pada iphone-dump.img pada kolom sebelah kiri sehingga partisinya terbuka. Dalam penelitian ini partisinya bernama disk2s1.
f. Selanjutnya buka program Data Rescue, pilih Start New Scan.
g. Setelah itu, Data Rescue akan menampilkan partisi-partisi atau *drive* yang ada di dalam komputer tersebut, termasuk iphone-dump.img yang sudah dibuka partisinya. Pilih 'Apple Read:Write (Disk Image)' lalu klik Next untuk melanjutkan.
h. Akan muncul pilihan beberapa tipe *scan. Quick Scan* berguna untuk pencarian file secara dasar. *Deep Scan* berguna untuk pencarian file dalam tingkat sangat rinci. *Deleted File Scan* berguna untuk mencari file file yang sudah terhapus dalam drive. Dalam kasus ini menggunakan *Deep Scan* untuk pencarian data karena pencarian rinci diperlukan untuk mengembalikan seluruh data hasil *cloning* pada iPod Touch. Pilih *Deep Scan* dan klik *Start.*
i. Akan muncul window untuk memilih *workspace. Workspace* ini digunakan untuk menampung data sementara ketika *drive* sedang dalam proses *scanning*.
j. Selanjutnya akan ditampilkan proses *scanning* yang sedang berjalan. Tunggu hingga selesai.

k. Setelah proses *scanning* selesai, Data Rescue akan menampilkan windows untuk memilih folder yang akan di-*recover*. Centang semua folder, lalu klik *recover.*

l. Setelah itu Data Rescue akan menampilkan *Output Folder* yang menjadi tujuan folder tersebut ketika di-*extract.* Pilih folder yang akan menjadi tujuan file atau folder yang akan di-*recover,* selanjutnya klik *Open*.

m. Proses *recover* pun dimulai. Kali ini, file-file yang telah melalui proses *recover* akan masuk kedalam folder yang sudah dipilih sebagai folder tujuan. Tunggu hingga proses *recover* benar-benar selesai.

n. Setelah proses selesai, file yang sudah selesai di *recover* akan terlihat di folder tujuan yang telah dipilih, untuk lebih jelasnya lihat pada Gambar 4.18. Lalu *copy* semua data di folder *Recovered Files* ke *Flashdisk* berformat FAT32 yang dipakai untuk meng-*copy* file iphone-dump.img tadi. Setelah itu, masukkan ke komputer untuk disidik.



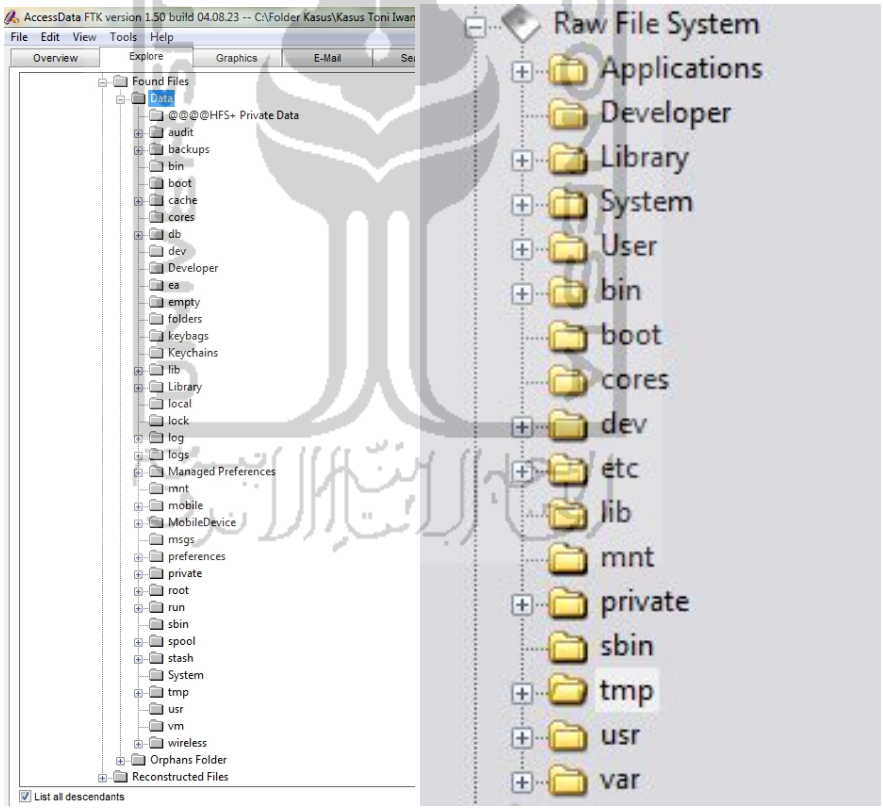
Gambar 4.18 Hasil *recovering* dari iphone-dump.img

4.3.5.2 Mencocokan data *recovery* dengan data asli.

Pencocokan data hasil ekstraksi dengan data asli sangat diperlukan dalam penyidikan untuk validitas data. Dalam iPod Touch forensik, terdapat sedikit perbedaan susunan struktur file. Ada beberapa folder yang ada di hasil *recovery* namun tidak ada di struktur file yang terlihat pada aplikasi pihak ketiga maupun yang terlihat di *iFile* pada Gambar 4.6. Ini dikarenakan ada beberapa file atau folder system yang bahkan tidak bisa dibaca oleh aplikasi pihak ketiga dan *iFile* (*hidden* file), ini membuktikan bahwa teknik *recovery* juga dapat membaca dan mengembalikan *hidden* file. Selain itu,hal ini juga dikarenakan iPod Touch

mempunyai file *link* yang juga bekerja pada aplikasi pihak ketiga namun tidak bekerja pada saat ekstraksi *recovery*. File *link* ini bertujuan untuk meringkas dan menyederhanakan struktur file.

File link yang terdapat pada iPod Touch antara lain adalah *etc*, *User*, *tmp,* dan *var*. Semisal contoh file *link User* untuk mengelompokkan data dalam folder *Mobile.* Sehingga pada aplikasi pihak ketiga folder *Mobile* tidak ada, tapi folder *User* ada dengan data yang sama. Begitu pula sebaliknya pada data hasil *recovery.* Namun, walaupun mempunyai struktur file yang berbeda tapi tetap mempunyai data yang sama. Jadi data *recovery* tersebut adalah data yang valid. Untuk lebih mendapat gambaran, lihat pada Gambar 4.19.



Gambar 4.19 Perbandingan struktur file pada hasil *recovery* (kiri) dan pada aplikasi pihak ketiga (kanan)

4.3.5.3 Mengekstraksi *recovery data* dengan Forensic Toolkit

Setelah pembuatan *image*, maka tahap selanjutnya adalah menganalisis *image* dengan menggunakan Forensic Toolkit. Dalam kasus ini, Forensic Toolkit

berperan melengkapi hasil penyelidikan dengan menggunakan Oxygen Forensic Suite yang tidak bisa menyelidik file dokumen, email dan bagan-bagan dari file sistem Apple iPod Touch. Ketika membuka program sebagai *administrator* (klik kanan dan pilih *Run as Administrator*), maka akan muncul beberapa opsi diantaranya :

a. *Start new case*, digunakan untuk membuat *case* baru dari *image* file yang ada.
b. *Open an existing case*, digunakan untuk membuka kasus yang telah dibuat sebelumnya.
c. *Preview evidence*, digunakan untuk melihat *evidence* yang telah dibuat.

Pilih *Start new case* untuk dapat membuat kasus baru dari *image* yang telah dibuat. Setelah itu Forensic Toolkit akan memberikan *form* isian tentang informasi berkaitan dengan barang bukti yang akan disidik. Mulai dari nama penyidik, nama kasus yang akan diselidiki, serta atribut-atribut lainnya yang berkaitan dengan kasus. *form* ini juga akan menentukan folder yang merupakan tempat menyimpan segala aktivitas penyelidikan.

Untuk kepentingan laporan, selanjutnya akan ditampilkan *form* isian mengenai informasi penyidik. Selama masa penyidikan, FTK akan membuat file bernama FTK.*log* yang akan mencatat aktivitas pada *case.* Kita bisa menentukan *event* apa saja yang akan dicatat dengan member tanda *check* pada opsi yang sudah tertera.

Selanjutnya menentukan *option* untuk pemrosesan *evidence*, pilihlah proses yang relevan dengan *evidence* yang akan ditambah ke *case.* Contoh : jika *case* terutama memuat gambar maka tidak perlu melakukan index pada *evidence*, sedangkan bila kasus tidak memuat gambar maka tidak perlu menyimpan *thumbnail*. *Refine case* memungkinkan kita untuk mengecualikan sejumlah data dari *case*. Tujuannya untuk menghemat waktu dan sumber data, menghilangkan data yang tidak relevan.

Selanjutnya adalah *refine index*, halaman ini membantu menentukan tipe data yang tidak ingin diindeks. Index file dibuat setelah pembuatan suatu *case*, tetapi pembuatan suatu *evidence* item bisa diindex kapan saja. Selanjutnya akan

ditampilkan window *Add Evidence.* Pada halaman ini dapat menambah, mengurangi, mengelola informasi, serta parameter dari barang bukti. Adapun barang bukti yang dimaksud adalah barang bukti yang berhubungan dengan kasus (*case*). Klik tombol *Add Evidence* untuk menambahkan barang bukti.

Karena barang bukti dalam kasus ini merupakan hasil dari *recovery* file *image* dari iPod Touch, maka file yang akan diperiksa adalah isi dari folder *recovery* tersebut. Oleh karena itu dalam kasus ini memilih *Content of a Folder* sebagai barang bukti yang akan dimasukkan. Setelah memilih direktori yang sesuai, maka selanjutnya akan muncul window untuk mengisi *form* informasi dari barang bukti.

Setelah itu, maka pengaturan selesai. Dan siap mengekstrak barang bukti. Lalu akan dilakukan analisis forensik terhadap data-data yang telah diekstrak. Dengan analisis tersebut diharapkan dapat menemukan file-file yang berkaitan dengan kasus. Seperti contoh Dokumen dan E-Mail. Selain itu, dengan Forensic Toolkit dapat juga meng-*explore* bagian dari sistem file iPod Touch yang menjadi karakteristiknya.

4.4 Analisis Kasus

Analisis kasus pada penelitian ini menggunakan dua *tool* yaitu *Oxygen Forensic Suite,* dan *Forensic Toolkit.* Pada setiap *tool* mempunyai langkah-langkah untuk menyidik barang bukti, karena berbeda tool, maka berbeda juga hal yang disidik. Sehingga, langkah pengerjaannya adalah sebagai berikut :

Tabel 4.1 Langkah-langkah penyidikan

Bagian yang disidik	Barang Bukti yang ditemukan	Software	Langkah Penyidikan
File *Back Up*	- *Device Information*	*Oxygen Forensic Suite*	1. Ekstrak file *back up* iTunes ke Oxygen
	- *Phonebook*		
	- *Calendar*		
	- *Notes* (Memo)		
	- Timeline Aplikasi		
	- Log Jaringan		2. Pilih *Section* berkaitan yang berkaitan dengan barang bukti yang ingin diselidiki
	- Struktur file file back		
	- Aplikasi Terinstall		
	- Log Browser		
	- Log chat Skype		
	- Log Yahoo		
File *Recovery Image*	Struktur File	*Forensic ToolKit*	1. Ekstrak file *image* ke FTK (*//Recovery File/Found Files/Data*)
			2. Klik Tab *Explore*
	Aplikasi		*Buka //Recovery Files/Found Files/Data/Mobile/ Application*
	Dokumen hasil dari download		*Buka //Recovery Files/Found Files/Data/Mobile/ Document*
	Email		*Buka //Recovery Files/Found Files/Data/Mobile/Library/ Mail*
	Gambar / Photo / Video / Lagu		*Buka //Recovery Files/Found Files/Data/Media*
	File yang telah terhapus		*Buka //Recovery Files/Reconstructed Files/*

4.4.1 Analisis file *back up* dengan menggunakan Oxygen Forensic Suite

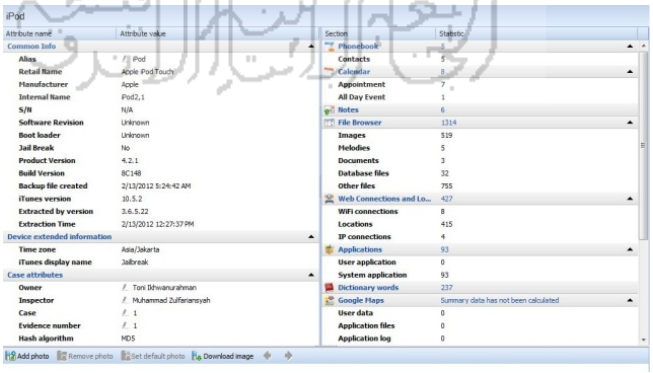
Pada tampilan awal setelah *extracting* file *back up* pada iPod Touch, maka Oxygen akan menampilkan *thumbnail device.* Dari *thumbnail* tersebut terdapat beberapa informasi. Informasi dari iPod Touch seperti *Model, Serial*

Number, dan *Owner*. Selain itu juga menampilkan informasi dari keterangan barang bukti pada kasus serta informasi penyidik.

Selanjutnya ada tab *notes* yang berisikan catatan yang di isi ketika proses *extracting*. Untuk memulai penyelidikan, pada kolom *devices and cases* buka nama *case* yang di isi sebelumnya. Dalam kasus ini karena nama *case* adalah 1, maka klik pada folder 1. Setelah itu akan muncul subfolder yang berisikan nama alias pada *device*, dalam kasus ini nama alias dari *device* adalah iPod Touch. Setelah iPod Touch di klik, maka akan menampilkan beberapa *section* (bagian). Ketika *section* tersebut diklik, maka akan menampilkan informasi yang sesuai dengan *section* tersebut.

4.4.1.1 Hasil dan Pembahasan pada *Device Information*

Device Information akan memuat informasi serta parameter atau statistik lain pada *device*. Terlihat pada Gambar 4.20, menu ini akan menampilkan informasi umum pada *device*,atribut *device* pada kasus yang akan diselidiki, dan juga statistik dari *section* umum pada *device* seperti *phonebook, calendar, notes,* dan lain sebagainya. Berbeda dengan informasi yang tertera pada *About* di Gambar 4.9, yang hanya berisi informasi tentang versi, model, nomor serial, dan *MAC Address* pada Bluetooth dan WiFi.

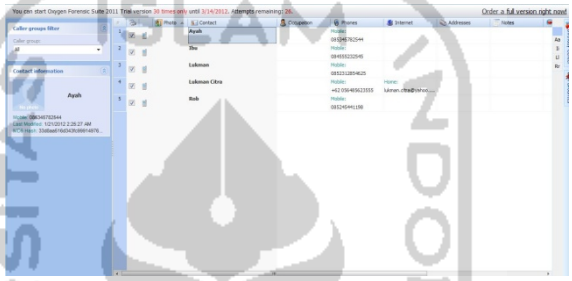


Gambar 4.20 *Device Information* pada iPod Touch

4.4.1.2 Hasil dan Pembahasan pada *Phonebook*

Phonebook adalah media penyimpanan untuk kartu nama. Dalam *phonebook* terdapat informasi terkait rekan atau kerabat dari tersangka seperti

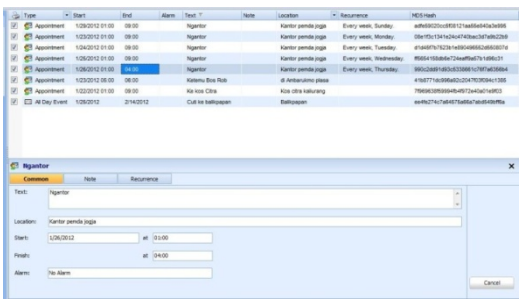
nama, perusahaan, nomor telpon, alamat email, serta alamat rumah. Tidak ada yang berbeda dari isi *Phonebook* jika dilihat dari iPhone seperti yang terlihat pada Gambar 4.2, maupun disidik dengan menggunakan Oxygen Forensic Suite, seperti yang terlihat pada Gambar 4.21. Dari *phonebook* ini bisa membantu penyelidikan dengan cara memanggil orang yang tertera dalam *phonebook* tersebut dan menanyakan secara langsung kepada orang yang bersangkutan sebagai informasi tambahan mengenai tersangka.



Gambar 4.21 Tampilan pada *Phonebook*

4.4.1.3 Hasil dan Pembahasan pada *Calendar*

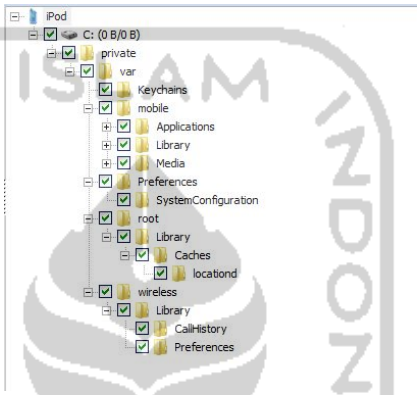
Dalam sebuah *smart device, calendar* berfungsi sebagai pengingat suatu janji penting ataupun rutinitas sehari-hari. Isi Alarm dan *Appointment* dalam *Calendar* di iPod Touch pada Gambar 4.4 sama dengan isi *Calendar* yang disidik dengan Oxygen Forensic Suite pada Gambar 4.22. Dalam keperluan investigasi, melihat isi *calendar* bisa berguna untuk mengetahui rutinitas tersangka. Nantinya urutan waktu tersebut dapat dihubungkan dengan serangkaian bukti yang ditemukan.



Gambar 4.22 Melihat isi *Calendar*

4.4.1.4 Hasil dan Pembahasan pada *File Browser*

File Browser pada dasarnya adalah sebuah *explorer data* dimana berfungsi untuk menjelajah data dari suatu media penyimpanan. Namun, karena dalam kasus ini memakai file *back up* dari iPod Touch sebagai data yang akan di selidiki, maka tidak semua struktur file yang dapat di *back up.* Struktur File pada file *Back Up* bisa dilihat pada Gambar 4.23.



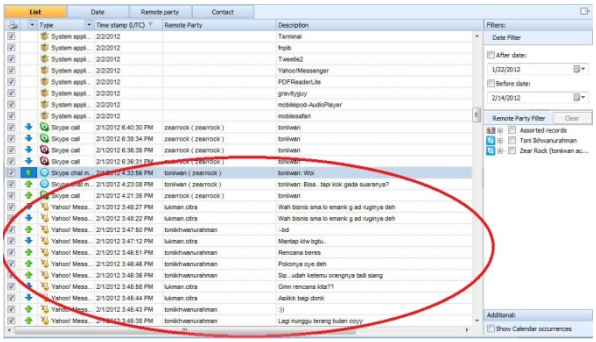
Gambar 4.23 Struktur file pada file *back up* iPod Touch dengan iTunes

Dalam file *back up iTunes,* folder yang di *back up* adalah folder *private/var* dimana didalamnya adalah file-file umum seperti lagu, gambar, dan video hasil produksi dari sebuah aplikasi, *save data* dari konfigurasi pengaturan dan aplikasi, history dari website yang pernah dikunjungi, dan lain-lain.

4.4.1.5 Hasil dan Pembahasan pada *Timeline*

Timeline dalam *Oxygen Mobile Forensic* berguna untuk melihat urutan penggunaan aplikasi pada suatu *device*, sehingga membantu para penyidik dalam menyelidiki suatu kasus. *Entry* dari *timeline* tidak hanya sebatas penggunaan per-aplikasi, namun juga detail dari penggunaannya. Seperti misalnya dalam kasus ini, iPod Touch tersangka di *install* berbagai aplikasi *chating* seperti Yahoo! Messenger, dan Skype, dengan *timeline* bisa terlihat isi dari *chating* tersebut. Namun tidak semua aplikasi bisa dilihat detailnya atau isinya.

Pada kasus ini terlihat aktivitas chating tersangka dengan “lukman.citra” yang terlihat mencurigakan. Penyidik dapat menghubungi “lukman.citra” untuk dimintai keterangan lebih lanjut. Bukti terdapat pada Gambar 4.24.



Gambar 4.24 Tampilan pada *Timeline*

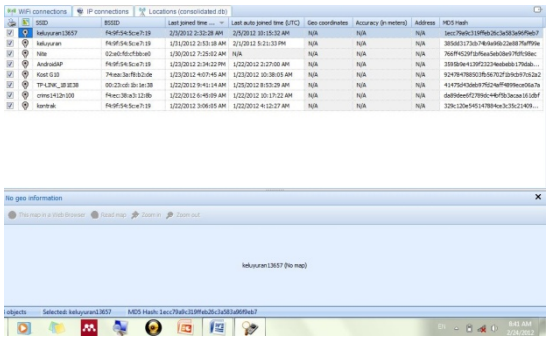
4.4.1.6 Hasil dan Pembahasan pada *Web Connections and Location Services*.

Pada Oxygen Forensic Suite, ada suatu *section* yang bernama *Web Connections and Location Services. Section* ini berguna mengetahui log WiFi yang digunakan *device* untuk dapat terhubung ke internet. Selain itu, *Section* ini juga dapat berguna untuk melihat log GPS pada *device.*

Dalam kasus ini, Apple iPod Touch tidak memiliki fitur GPS. Sehingga jika menggunakan aplikasi GPS seperti *Maps,* yang ditemukan sebagai *my location* adalah lokasi pada *router WiFi* tempat iPod Touch tersambung internet. *Router WiFi* tersebut juga harus *support* GPS tentunya.

Berbeda jika melihat opsi dari *Maps* secara langsung pada iPod. Seperti yang terlihat pada Gambar 4.3, yang tersimpan hanya nama tempat yang telah dicari. Namun, jika disidik dengan menggunakan Oxygen Forensic Suite, maka bisa terlihat *history* tempat yang pernah di *tracking,* dan bahkan bisa melihat *history* penggunaan pada wireless router. *History-history* tersebut dapat dilihat pada Gambar 4.25, 4.26, dan 4.27.

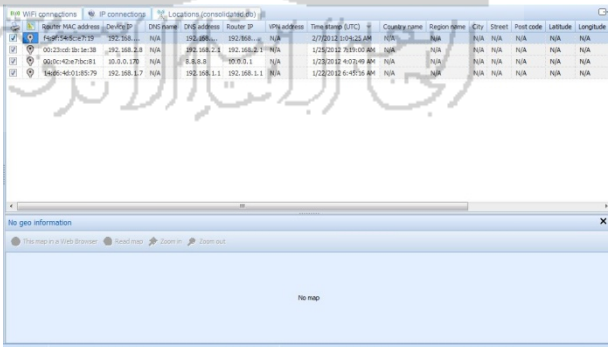
Ada tiga *tab* dalam *section* ini. Yang pertama adalah *WiFi Connections. Tab* ini berguna untuk melihat log jaringan *wireless* yang dipakai pada iPod Touch untuk terhubung pada internet. *Tab* ini akan memperlihatkan SSID, BSSID (Mac Address), *Last joinned time*, *Last auto joined time, Geo Coordinates*, *Accuracy, Address,* serta MD5 *hash.*



Gambar 4.25 *Web Connection and Services* pada WiFi Connections

Pada gambar diatas terlihat bahwa *Geo Coordinates, Accuracy,* serta *Address* tidak dapat dibaca. Hal ini dapat disebabkan oleh beberapa faktor. Semisal koneksi internet yang lemah, atau lokasi yang susah ditangkap koordinatnya.

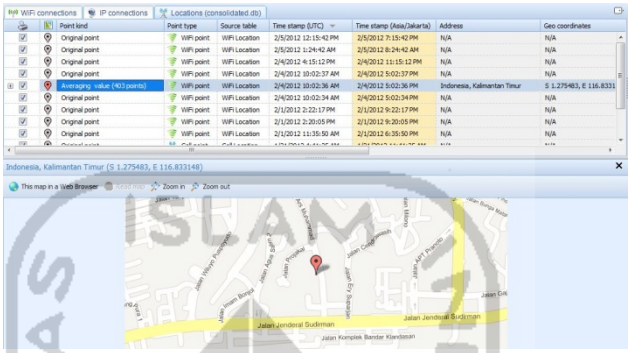
Yang kedua adalah *tab IP Connections. Tab* ini berguna untuk memperlihatkan alamat IP yang didapat oleh iPod Touch. Selain itu, dapat diketahui alamat DNS serta IP dari router yang digunakan untuk terhubung internet. *Tab* ini juga dapat memperlihatkan *Country Name, Region Name, City, Street, Post Code, Latitude, Longitude,* serta *Accuracy* jika koordinat dapat ditangkap oleh GPS.



Gambar 4.26 *Web Connection and Services* pada *IP Connections*

Tab yang terakhir yaitu *Locations. Tab* ini akan memperlihatkan *log* GPS pada *device. Log* ini dibaca melalui file *consolidated.db.* Seperti yang terlihat pada Gambar 4.11, iPod Touch membaca lokasi berdasarkan *WiFi Point* yang berarti titik dimana Router WiFi terhubung. Dapat terlihat juga banyak titik yang

tidak bisa dibaca oleh GPS. Titik yang diberi tanda menunjukkan koordinat tidak bisa dibaca oleh GPS, dan titik yang diberi tanda menunjukkan koordinat bisa dibaca oleh GPS.

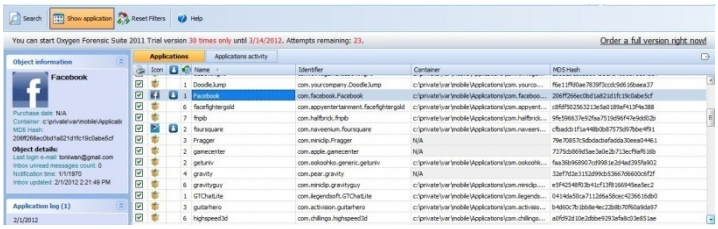


Gambar 4.27 *Web Connection and Service*s pada *Locations*

Dari gambar di atas, *point kind* bertipe *Averaging Value,* ini berarti bahwa titik merupakan hasil koordinat geografis yang dihitung dari beberapa titik dengan waktu yang sama sesuai dengan algoritma mean (*mean algorithm*). Jika dilihat dari log terakhir *WiFi Connection,* iPod Touch terkoneksi dengan router yang tidak mendapat koordinat GPS. Ini menunjukkan titik *Averaging Value* yang didapat merupakan hasil perpindahan router, dimana router tersebut bisa saja sewaktu-waktu menemukan sinyal yang sempurna untuk dapat membaca koordinat GPS.

4.4.1.7 Hasil dan Pembahasan pada *Applications*

Ada dua *tab* pada *section* ini. Yang pertama adalah *Applications. Tab Applications* berguna untuk melihat aplikasi apa saja yang terinstall pada iPod Touch. Pada *tab* ini dapat dilihat juga *source* atau *repository* dari suatu aplikasi. Ada beberapa informasi yang dapat diambil dari *section* ini. Seperti akun *social network* yang aplikasinya sudah terinstall pada iPod Touch. Seperti contoh, pada kasus ini dapat diketahui bahwa Facebook milik Toni Ikhwanurahman telah *login* menggunakan email toniiwan@gmail.com. Bukti ada pada Gambar 4.28.



Gambar 4.28 Facebook dan keterangannya pada *section Applications*

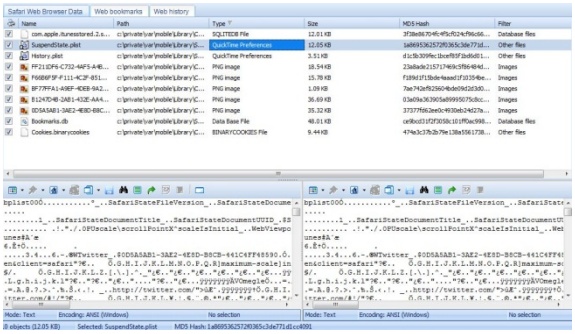
Tab yang kedua adalah *Applications Activity.* Pada *tab Applications Activity*, kegunaannya sama seperti *section Timeline* yaitu melihat penggunaan aplikasi berdasarkan waktu.

4.4.1.8 Hasil dan Pembahasan pada Web Browsers Cache Analyzer

Banyak yang bisa dilakukan oleh iPod Touch hanya dengan menggunakan koneksi *wireless.* Selain mendownload lagu, gambar, dan aplikasi, iPod Touch juga bisa mengakses internet menggunakan *browser default* yaitu Safari. Dalam keperluan penyelidikan, *history* dan *bookmark* browser merupakan data yang sangat penting karena dapat mengetahui napak tilas pengaksesan internet.

Sama seperti yang terlihat pada Gambar 4.8, pada Gambar 4.30 juga menampilkan *Web History* yang dilakukan pada iPod Touch. Namun perbedaannya, pada Gambar 4.30 merupakan *web history* yang disidik menggunakan Oxygen Forensic Suite, sehingga diketahui rincian waktunya. Selain itu, pada Safari iPod Touch tidak bisa menampilkan *Safari Web Browser data* seperti yang terlihat pada Gambar 4.29.

Ada tiga *tab* dalam *section Web Browsers Cache Analyzer.* Yang pertama adalah *Safari Web Browser data. Safari Web Browser data* menyimpan data-data dan sistem yang digunakan oleh Safari.



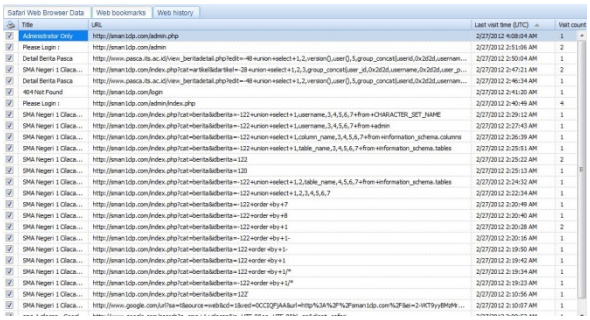
Gambar 4.29 *Safari Web Browsers data*

Data-data tersebut adalah sebagai berikut :

a. *com.apple.itunesstored.2.sqlitedb*, file database ini berisi tentang informasi terkait iTunes Store.

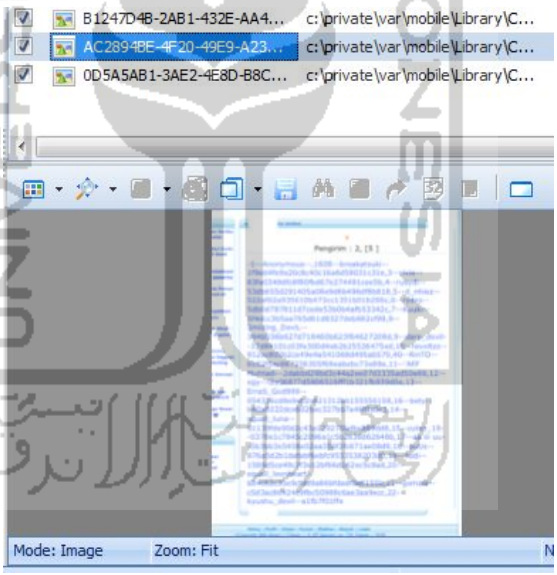
b. *SuspendState.plist*, berisi data tentang halaman terakhir yang diakses pada Safari, sejak terakhir kali pemilik menekan tombol *home*, menekan tombol *off*, atau Safari mengalami *crash.* Data ini berisi daftar *window* dari situs yang terbuka, sehingga iPod Touch dapat membuka kembali halaman tersebut ketika di*resume* dan akan menampilkan *snapshoot* halaman web terakhir yang dilihat.

c. *History.plist,* berisi data *history* dari Safari *Web Browser.* Untuk melihatnya tanpa melalui HexViewer, cukup dengan klik *tab* ketiga yaitu *Web History*. Pada kasus ini, jika dilihat dari *history web page* dan url yang dimasukkan terlihat bahwa Toni Ikhwanurahman melakukan serangan *SQLInjection* ke situs http://sman1clp.com. Ini merupakan pembuktian dari *Web Hacking* dengan *SQL Injection*.

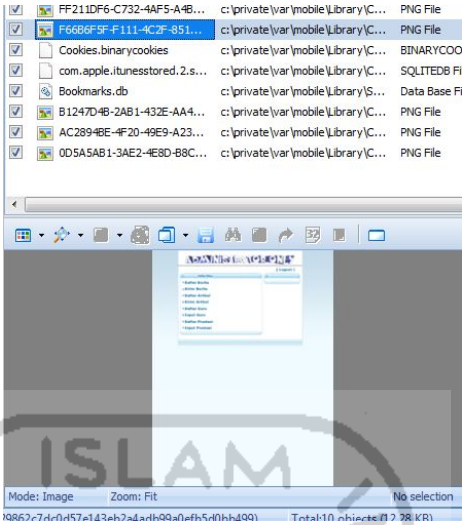


Gambar 4.30 Tampilan *Web History*

d. PNG *Images File,* Gambar berekstensi PNG pada *Safari Web Browser data* merupakan *caches Thumbnail* dari Safari. Dengan kata lain, Gambar PNG tersebut merupakan halaman terakhir yang diakses oleh Safari atau *snapsoot* yang dimaksud pada bagian *SuspendState.plist* sebelumnya. Banyaknya file gambar menunjukkan banyaknya *window* yang dibuka pada safari. Dalam kasus ini terlihat pada Gambar 4.31, ketika terakhir kali mengakses *browser* Toni Ikhwanurahman berhasil mendapatkan *username* dan *password* dari user website SMA Negeri 1 Cilacap, serta berhasil masuk ke halaman admin SMA Negeri 1 CIlacap seperti yang terlihat pada Gambar 4.32. Ini merupakan pembuktian dari kejahatan berupa pencurian data.



Gambar 4.31 Daftar *username* dan *password* yang merupakan bukti pencurian data.

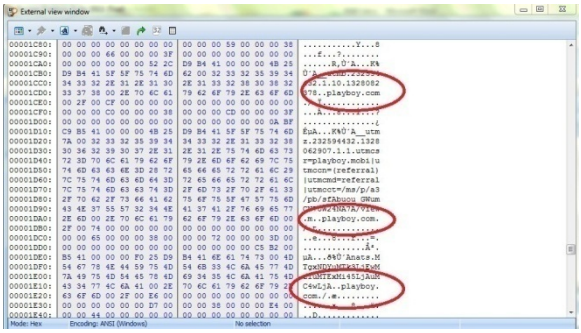


Gambar 4.32 Bukti Toni Ikhwanurahman berhasil masuk sebagai admin

e. *Bookmarks.db*, file database ini akan menyimpan *bookmark* dari Safari. Untuk melihatnya tanpa memakai *HexViewer*, bisa dengan cara klik tab kedua yaitu *Web Bookmarks*. Pada file ini terlihat pada Gambar 4.33, diketahui pemilik juga menyimpan situs dewasa playboy.com sebagai *bookmark*.

Gambar 4.33 Melihat File *Bookmarks.db* dengan *tab Web Bookmarks*

f. *Cookies.binarycookies*, data ini akan menyimpan *cookie* pada kegiatan browser Safari. Walaupun *history* telah dihapus, *cookie* akan mencatat alamat-alamat yang telah dikunjungi. Sehingga file *cookie* ini bisa diselidiki walaupun yang tertera hanya alamat websitenya saja. File *cookie* ini diselidiki menggunakan *HexViewer* dari *Tools* Forensik. Pada kasus ini, setelah diselidiki file *Cookies.binarycookies* ditemukan bahwa pemilik iPod Touch pernah mengunjungi situs dewasa playboy.com seperti yang terlihat pada Gambar 4.34.

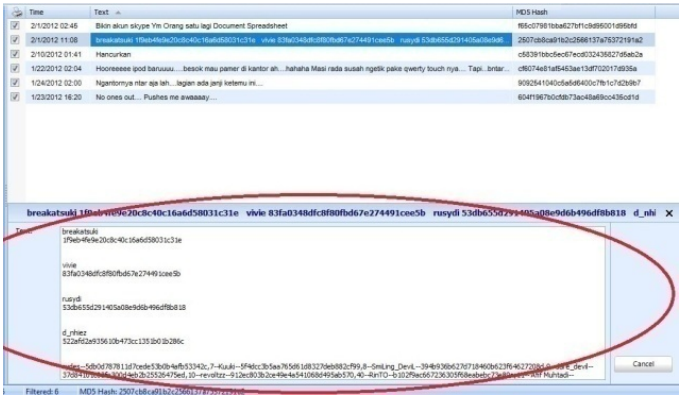


Gambar 4.34 Tampilan *HexViewer* dari *Cookies.binarycookies*

4.4.1.9 Hasil dan Pembahasan pada *Notes*

Pemeriksaan *notes* pada sebuah *smart device* seperti iPod Touch tidak boleh dilewatkan dalam sebuah penyelidikan. Karena dari dalam *notes* tersebut bisa mengandung informasi terkait tersangka. Informasi tersebut dapat berupa catatan alamat rumah seseorang, kode rahasia, pengingat suatu kejadian, dan lain-lain. Tidak ada yang berbeda dari isi Notes sebelum (Gambar 4.5) dan sesudah (Gambar 4.35) diforensik.

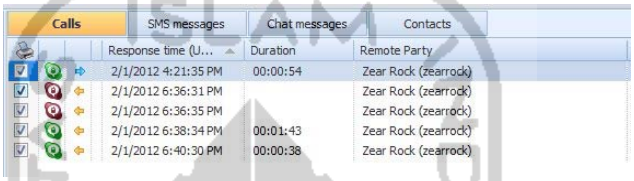
Pada kasus ini, ditemukan catatan yang mencurigakan dari iPod Touch tersangka seperti yang terlihat pada Gambar 4.35. Catatan tersebut berisikan nama orang di ikuti dengan kode atau sandi dibelakang namanya. Isi dari catatan ini sama dengan nama-nama username yang ditemukan pada *web history* sebelumnya. Ini merupakan pembuktian dari penyimpanan informasi sekolah.



Gambar 4.35 Melihat isi *Notes*

4.4.1.10 Hasil dan Pembahasan pada *Skype* Analyzer

Pada *Extra Section* akan ditampilkan beberapa *section* terkait dengan aplikasi yang diinstall. Aplikasi yang muncul biasanya adalah aplikasi sosial seperti Skype dan Yahoo Messenger. Seperti pada barang bukti iPod Touch ini, telah terinstall Skype. *Section* Skype ini dapat memperlihatkan log panggilan seperti yang terlihat pada Gambar 4.36, isi sms, *chat messages*, dan kontak seperti yang terlihat pada Gambar 4.37.



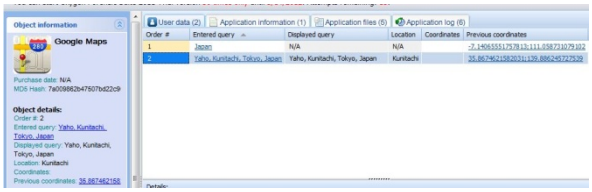
Gambar 4.36 *Log Calls* pada Skype

Gambar 4.37 *Contacts* pada Skype

4.4.1.11 Hasil dan Pembahasan pada *Google Services* (Google Maps)

Google Maps merupakan aplikasi *preload* pada iPod Touch, sehingga tidak perlu menginstallnya lagi. *Section* Google Maps pada iPod Touch ini tidak merekam jejak dari GPS, tetapi merekam dari *search history* yang digunakan untuk mencari tempat, dan tempat dimana Pin dijatuhkan untuk mengetahui alamat.

Seperti yang terlihat pada Gambar 4.38, bahwa pemilik iPod Touch sempat mencari suatu tempat bernama Kunitachi di Jepang. *Section* ini juga akan memperlihatkan titik koordinatnya.

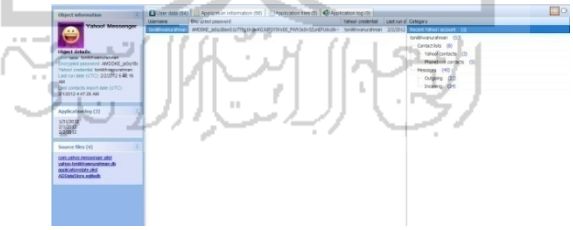


Gambar 4.38 Google Maps pada *Section Google Services*

4.4.1.12 Hasil dan Pembahasan pada Yahoo Messenger

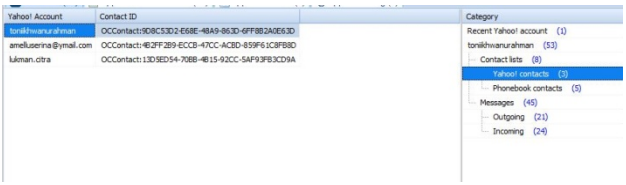
Yahoo Messenger bukan aplikasi *preload* dari iPod Touch. Sehingga untuk memasangnya pada iPod Touch, harus menginstallnya lewat *App Store*. Pada *Section Yahoo Services* (Yahoo Messenger) terdapat beberapa kategori di kolom sebelah kanan untuk penyelidik selidiki terkait akun Yahoo pemilik iPod Touch.

Recent Yahoo! Account akan memberitahukan akun Yahoo! mana yang pernah aktif dengan menggunakan iPod Touch. Disini diketahui bahwa pemilik iPod Touch menggunakan username "toniikhwanurahman", dan password yang terenkripsi seperti yang terlihat pada Gambar 4.39. *Password* yang terenkripsi tersebut bisa kita pecahkan menjadi *plain text* dengan *tools* tertentu atau bisa dengan menanyakannya kepada pemilik iPod Touch secara langsung.



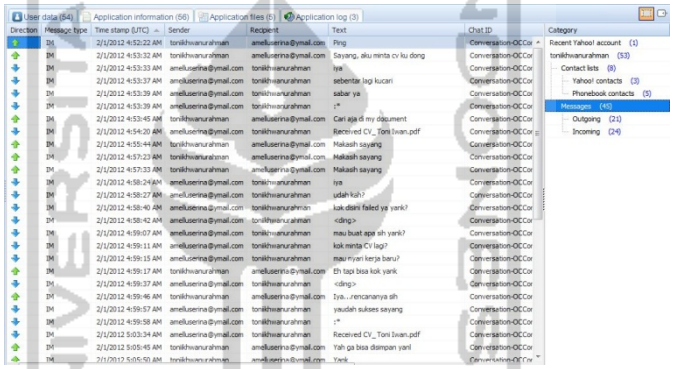
Gambar 4.39 username pada Yahoo Messenger

Selanjutnya, jika dalam *category* memilih username, maka akan terlihat seluruh tampilan log beserta kontak. Untuk melihat Kontak Yahoo Messenger saja, klik pada *Yahoo! Contacts,* maka akan ditampilkan *Yahoo! Account* beserta *Contact ID*-nya (Gambar 4.40)



Gambar 4.40 *Yahoo! Contacts*

Setelah itu, untuk menyelidiki percakapan yang dilakukan pemilik iPod Touch, pilih *Messages* dalam *Category*. Setelah itu klik pada *Time Stamp* untuk mengurutkan percakapan berdasarkan waktu dari yang paling lama ke yang paling baru untuk memudahkan penyelidikan.



Gambar 4.41 *Chat* pada *Yahoo! Messenger*

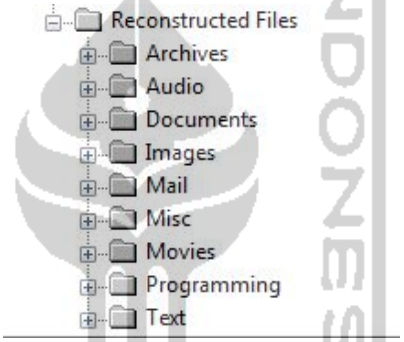
Pada Gambar 4.41 terdapat percakapan mesra antara toniikhwanurahman dengan amelluserina@ymail.com. Untuk langkah penyelidikan selanjutnya, pemilik akun amelluserina@ymail.com bisa dipanggil untuk dimintai keterangan dan informasi terkait pemilik iPod Touch lebih lanjut.

4.4.2 Analisis file *recovery disk image* menggunakan Forensic Toolkit

Setelah mengekstraksi file yang telah di-*recovery* dari file *Image* iPod Touch, selanjutnya menyidik file sistem dari iPod Touch dengan menggunakan *tool* Forensic Toolkit (FTK). Dimana folder yang disidik secara khusus adalah folder *Mobile*, serta mengecek *Reconstructed Files* dimana data-data yang telah dihapus atau hilang dipulihkan kembali dalam folder tersebut. Sedangkan folder lainnya akan disidik secara umum.

Dalam proses *recovery* pada *Data Rescue*, file *Image* yang telah di-*recovery* akan menghasilkan *output* dua bagian. Yang pertama adalah *Found Files* dan yang kedua adalah *Reconstructed Files. Found Files* berisikan struktur file pada iPod Touch.

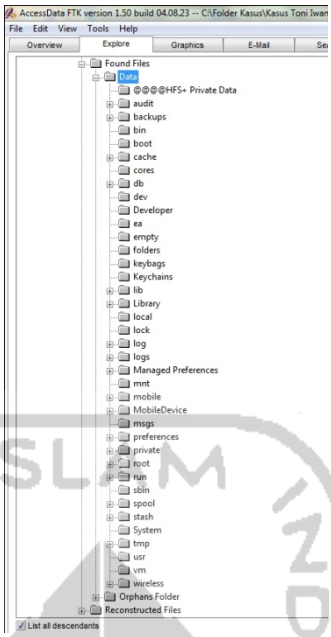
Sedangkan *Reconstructed Files* seperti yang terlihat pada Gambar 4.42, merupakan file yang telah dikonstruksi dan dikelompokkan kedalam beberapa kategori. Setiap jenis file yang telah dikostruksi akan membentuk suatu folder sesuai dengan format file tersebut. File yang telah terhapus atau terformat akan dpulihkan dan disimpan kedalam folder ini.



Gambar 4.42 Struktur File pada *Reconstructed Files*

4.4.2.1 Hasil dan Pembahasan pada Struktur File pada iPod Touch

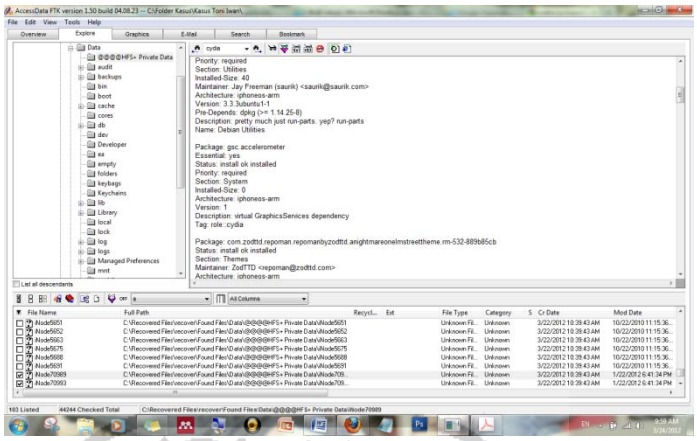
Sama seperti perangkat pintar lainnya, iPod Touch mempunyai struktur file untuk menentukan lokasi ketika instruksi dijalankan. Struktur file pada iPod Touch ini bisa dilihat pada Gambar 4.43. Struktur file ini menjadi salah satu karakteristik dari perangkat Apple iPod Touch.



Gambar 4.43 Struktur file pada iPod Touch

Tiap-tiap folder mempunyai peranan tersendiri dalam integritas pada file sistem. Berikut merupakan kegunaan dan pembahasan dari masing-masing folder tersebut :

a. *@@@HFS+ Private Data*, folder ini merupakan simpanan rahasia file yang berhubungan dengan disk HFS. Folder ini umumnya bersifat tersembunyi (*hidden*), untuk melihatnya membutuhkan suatu utilitas tambahan. Karena bersifat rahasia, folder ini tidak bisa di *copy* atau di *delete.* Bahkan Rixstep, sebuah perusahaan *constellation programmer and support staff,* pada penelitiannya ditahun 2007 menemukan cara untuk mengakses folder tersebut namun tidak dapat disalin seperti pada penelitian ini. Data-data didalam folder ini merekam aktifitas yang terjadi pada disk HFS. Seperti pada penelitian ini menemukan data yang merekam instalasi utilitas umum untuk *jailbreak.* Karena hamper semua aplikasi yang diinstall memuat *tag Cydia. Cydia* merupakan suatu utilitas *jailbreak.* Selain itu, *maintainer* dari aplikasi tersebut merupakan orang-orang *jailbreak developer* yang namanya sudah umum, sepert Joy Freeman dan JodTTD. Rekaman Utilitas *Jailbreak* terlihat pada Gambar 4.44.



Gambar 4.44 Rekaman instalasi utilitas *jailbreak* pada folder HFS+ Private Data

b. *Audit,* folder ini berguna untuk menyimpan konfigurasi umum pada iPod Touch, seperti konfigurasi *font, Keyboard Dictionaries, System Configuration,* dan lain-lain.

c. *Backup,* folder ini menyimpan framework pada aplikasi *pre-load* iPod Touch

d. *Bin,* folder ini berisi perintah-perintah shell dan berisi program-program yang diperlukan *boot script.*

e. *Caches,* folder ini menyimpan data *cache.*

f. *Db,* folder ini berisi file text atau *resource code* untuk bahasa pada iPod Touch

g. *Keybags,* Sebagai *Daemon Sistem* yang akan memuat sistem *keybag* kedalam AppleKeyStore *kernel service* pada waktu *boot.* Selain itu data dalam folder ini juga akan menangani *passcode changes.* (Sigwald, 2009)

h. *KeyChains,* folder ini menyimpan *password user* dari berbagai aplikasi. (Morrissey, 2010)

i. *Library,* folder ini menyimpan file-file dari aplikasi dan sistem yang digunakan pada aplikasi tersebut.

j. *Logs,* berisi informasi iPod Touch, log aktivitas dan *crash repport.*

k. *Managed Preferences,* didalamnya berisi file-file yang diterapkan ke *user, group,* atau aktivitas yang mengubah pengaturan standar dari suatu aplikasi.

l. *Mobile,* penjelasan khusus mengenai folder mobile akan dijelaskan pada Sub-bab 4.5.2.
m. *Preferences,* File untuk *System Configuration.*
n. *Private,* Informasi di dalam folder *Private/var* telah disidik dengan menggunakan *tool* Oxygen Forensic Suite. Sedangkan *Private/etc* memuat konfigurasi aplikasi lain seperti konfigurasi ssh, menyimpan password, konfigurasi profile, dan lain-lain
o. *Root,* informasi dari log GPS, aktivitas Cydia (*jailbreak*) bisa dilihat dari dalam folder ini.
p. *Run,* memuat *System log.* (Morrissey, 2010)
q. *Sbin,* memuat *command line binaries.*
r. *Stash,* didalamnya termasuk aplikasi *pre-load, ringtone default,* dan *wallpaper theme.*
s. *Tmp,* tempat menyimpan *temporary files.*
t. *Wireless,* dalam folder ini terdapat log *wireless.*

Sementara folder yang lain kosong.

4.4.2.2 Hasil dan Pembahasan pada folder *Mobile*

Seperti yang sudah dijelaskan sebelumnya, iPod Touch merupakan perangkat yang sangat tertutup aksesnya. Bahkan untuk melihat struktur filepun harus melakukan suatu metode khusus yang memungkinkan untuk menggunakan aplikasi pihak ketiga.

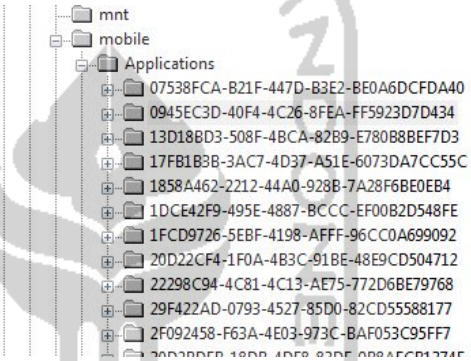
Karena tertutupnya struktur file pada iPod Touch ini, membuat iPod Touch tidak bisa dibuat sebagai *Removable Disk* seperti *flashdisk* pada umumnya untuk menyimpan data-data. Kalaupun untuk menyimpan data, hanya bisa pada satu folder yang terdeteksi pada *explorer* yaitu *DCIM* dimana folder tersebut merupakan folder tempat menyimpan gambar atau video. Pada iPod Touch Generasi 4, folder ini juga sebagai tempat menampung hasil foto pada kamera *built-in.*

Folder *DCIM* ini merupakan subfolder dari folder *Mobile*. Folder *mobile* merupakan folder yang dapat menyimpan banyak sekali informasi. Karena gambar, video, dokument, atau file yang didownload akan tersimpan pada folder

ini. Bagian ini akan menjelaskan subfolder penting yang dapat menyimpan banyak informasi pada folder *mobile.*

a. Folder Application.

Folder *Application* ini adalah tempat untuk menampung aplikasi yang telah diinstall. Aplikasi yang dimaksud bisa aplikasi yang telah didownload di *AppStore*, atau dari penyedia aplikasi jailbreak seperti *Cydia.* Setiap aplikasi akan di letakkan ke dalam suatu folder yang nama foldernya terenkripsi seperti yang terlihat pada Gambar 4.45.



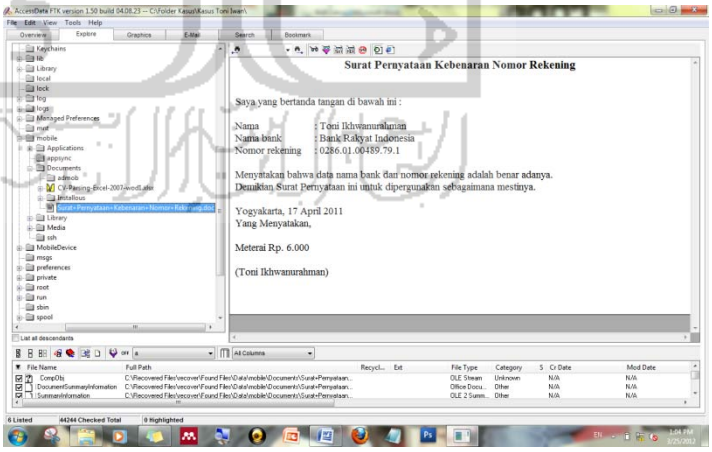
Gambar 4.45 Folder berisi aplikasi yang namanya telah terenkripsi

Setiap folder aplikasi akan ada dua file didalamnya, yaitu *iTunesArtwork* dan *iTunesMetadata.plist. iTunesArtwork* merupakan *icon* dari aplikasi tersebut. Sedangkan *iTunesMetadata.plist* merupakan metadata dari aplikasi tersebut. Penjelasan melalui gambar bisa dilihat pada Gambar 4.46.

Gambar 4.46 Dalam setiap folder aplikasi terdapat file *iTunesMetadata.plist* dan *iTunesArtwork*

b. Hasil dan Pembahasan pada folder *Document*

Folder *Document* ini adalah tempat atau lokasi *default* penyimpanan file yang telah didownload, baik itu dari *browser* atau dari Email. Dalam Gambar 4.47, pada iPod Touch ini ditemukan Surat Pernyataan Kebenaran Nomor Rekening dari Toni Ikhwanurahman. Setiap dokumen akan disimpan dengan tujuan dapat membantu penyelidikan kasus.



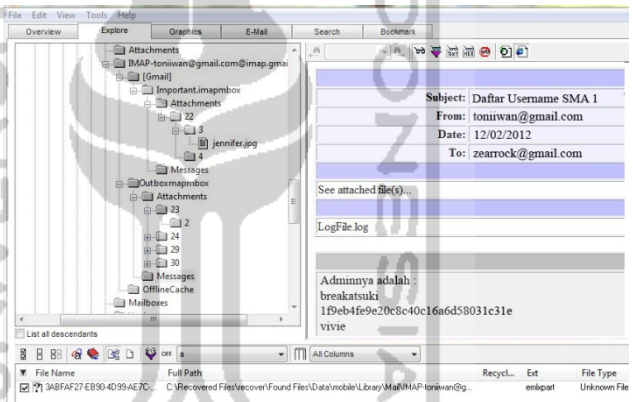
Gambar 4.47 Dokumen yang telah didownload pada folder *Document*

c. Hasil dan Pembahasan pada folder *Library*

Pada umumnya, folder *Library* ini berisi *database* aplikasi umum pada iPod Touch. File *database* ini yang memuat informasi personal dari pemilik iPod Touch. File *Database* inilah yang telah dianalisis pada

subbab 4.4.1 oleh *tool* Oxygen Forensic Suite. Namun, pada *tool* tersebut, tidak dapat menemukan berkas email. Sementara email dapat menyimpan banyak sekali informasi terkait personal.

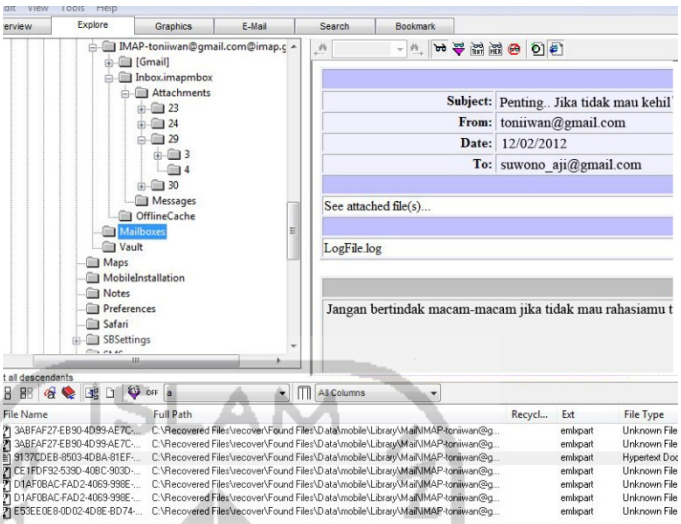
Dalam folder *Library* ini terdapat folder dimana email ditampung yaitu pada *Library/Mail*. Tidak terdapat perbedaan yang besar pada folder Email ketika sebelum disidik (Gambar 4.7) dan sesudah disidik (Gambar 4.32) , Terdapat folder *Attachments* dan *Messages.* Folder *Attachments* adalah folder untuk menyimpan lampiran pada email. Sedangkan folder *Messages* adalah folder untuk menyimpan pesan. Pada Gambar 4.32 merupakan contoh dari email yang dapat dilihat.



Gambar 4.48 Salah satu pesan dari Email

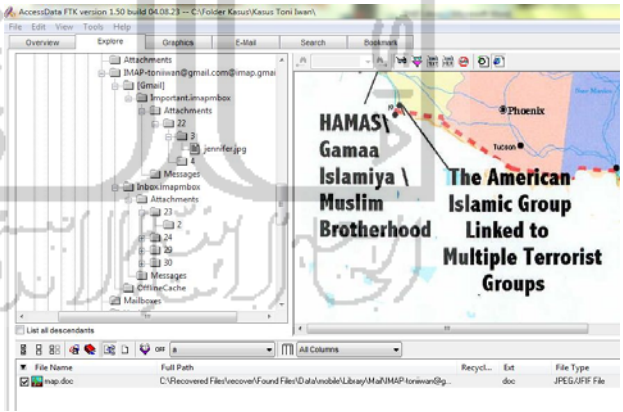
Di email tersebut dapat dilihat bahwa Toni Ikhwanurahman mengirimkan email berisi daftar admin pada SMA Negeri 1 Cilacap ke zearrock@gmail.com. Berhubungan dengan penyelidikan pada *notes* sebelumnya, ini merupakan pembuktian dari penyimpanan dan pengiriman informasi perusahaan (sekolah).

Selain itu, pada email lainnya tepatnya di folder *Mailbox,* terdapat pesan ancaman yang ditujukan kepada suwono_aji@gmail.com seperti yang terlihat pada Gambar 4.40. Ini merupakan pembuktian dari kejahatan berupa pengiriman email ancaman.



Gambar 4.49 Email Ancaman

Sedangkan folder *Attachments* menyimpan lampiran dari email. Gambar 4.50 merupakan contoh lampiran dari email.



Gambar 4.50 Salah satu lampiran pada Email

Pada gambar di atas, lampiran berupa sebuah peta dengan menggunakan kata-kata teroris. Untuk selanjutnya, hal ini bisa ditanyakan langsung kepada pemilik iPod Touch, apakah ada hubungan pemilik iPod Touch dengan terorisme. Selain itu, file tersebut merupakan *bad extention.*Karena file tersebut seharusnya bertipe JPEG/JFIF, sementara ekstensi dari file tersebut .doc atau *document.* Tapi dengan Forensic

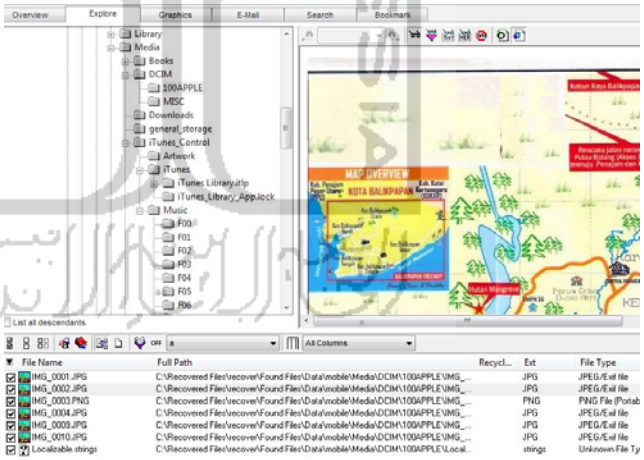
Toolkit, suatu file bisa dibaca atau terlihat jika file tersebut merupakan *bad extension file.*

d. Hasil dan Pembahasan pada Folder *Media*

Didalam folder *Media* terdapat file-file yang berhubungan dengan hiburan. Seperti musik, video, serta foto atau gambar. Kadang-kadang, suatu folder dapat berhubungan dengan folder yang lain, semisal untuk *thumbnail* dari suatu video maka akan disimpan di folder tersendiri terlepas dari folder video.

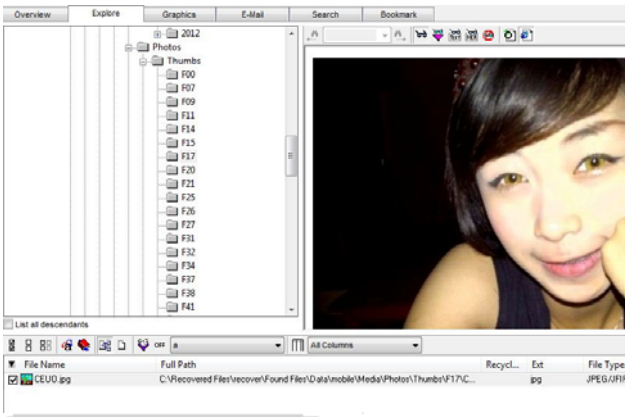
Media foto atau gambar dapat dicari pada folder-folder berikut :

- *DCIM/100APPLE* : Folder ini *default*-nya adalah tempat gambar yang telah didownload dari *Safari Browser*. Pada iPod Touch generasi 4, folder ini menjadi direktori *default* untuk hasil foto kamera. Gambar 4.51 merupakan tampilan folder *DCIM/100APPLE* pada iPod Touch.



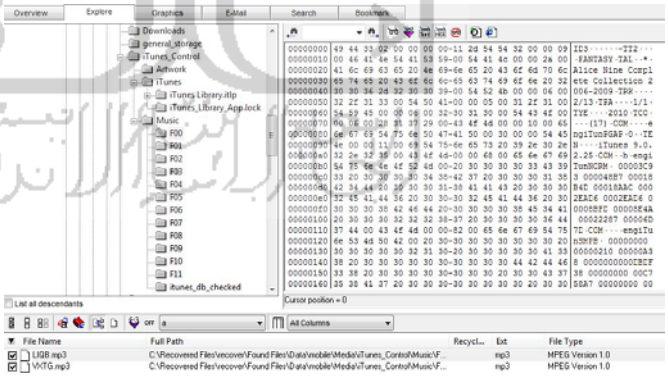
Gambar 4.51 Media foto/gambar di folder *DCIM/100APPLE*

- *Photos/Thumbs* : Folder ini menjadi tempat *thumbnail* (gambar kecil) untuk video, dan juga menjadi tempat penyimpanan foto yang telah di *back up* dari iTunes. Untuk lebih jelasnya, dapat dilihat pada Gambar 4.52.

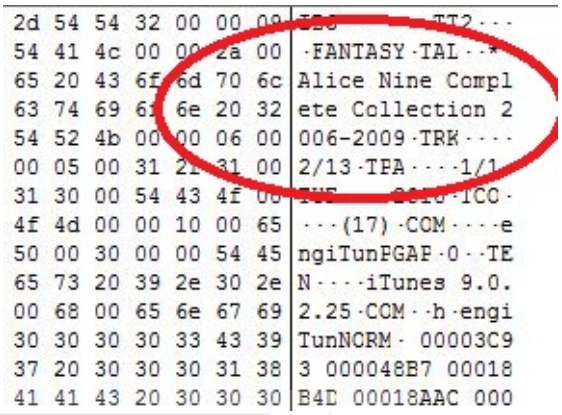


Gambar 4.52 Media foto/gambar di folder *Photos/Thumbs*

- Sedangkan untuk media lagu, dapat dicari pada folder *iTunes_Control/Music* seperti yang terlihat pada Gambar 4.53. Namun nama file telah dienkripsi menjadi 4 huruf acak, tidak seperti file lagu pada umumnya yang bertuliskan judul dan nama artis dari lagu tersebut. Namun, judul lagu dan nama artis tersebut dapat dilihat dengan menggunakan *hexviewer*. Untuk lebih jelasnya, lihat pada Gambar 4.54.

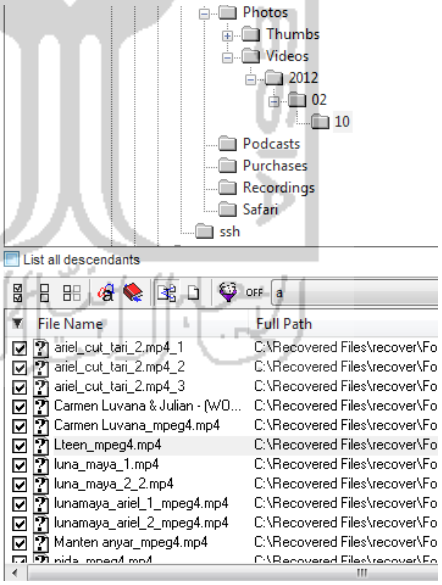


Gambar 4.53 File Musik pada folder *iTunes_Control/Music*



Gambar 4.54 Judul lagu dan artis yang dilihat melalui *hexviewer*

- Untuk media video, dapat dicari pada folder *Photos/Videos.* File video disimpan kedalam subfolder Tahun, Bulan, dan Tanggal dimasukkannya video tersebut dari iTunes. Sebagai contoh, lihat pada Gambar 4.55.



Gambar 4.55 Media Video pada folder *Photos/Videos*

4.4.3 Hasil dan Pembahasan pada *Reconstructed Files*

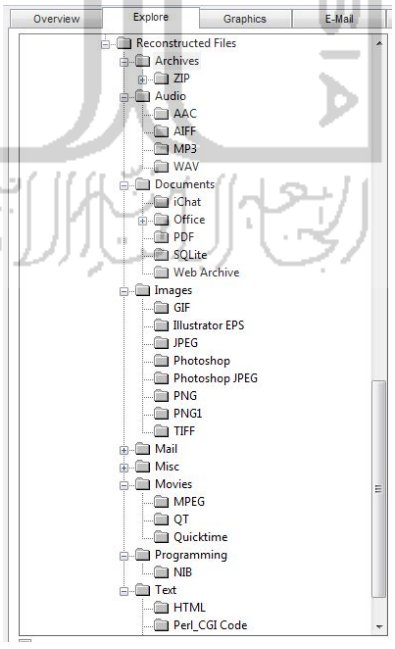
Folder *Reconstructed Files* dibuat pada proses *recovery* dengan menggunakan software *Data Rescue*. Folder ini pada dasarnya adalah untuk mengelompokkan file-file ke dalam masing-masing kategori. Namun, software ini

tidak hanya bertindak sebagai pengelompok file, tapi juga merekonstruksi kembali file-file yang hilang. Kategory file-file yang hilang tersebut tergantung isi dari perangkat yang di *recover.*

Pada iPod Touch ini, kategori yang di *recover* antara lain :

a. *Archives*
b. *Audio*
c. *Documents*
d. *Images*
e. *Mail*
f. *Misc*
g. *Movies*
h. *Programming*
i. *Text*

Didalam Gambar 4.56 terlihat dimana dalam folder kategori ini, terdapat beberapa subfolder yang umumnya sesuai dengan ekstensi file didalamnya.

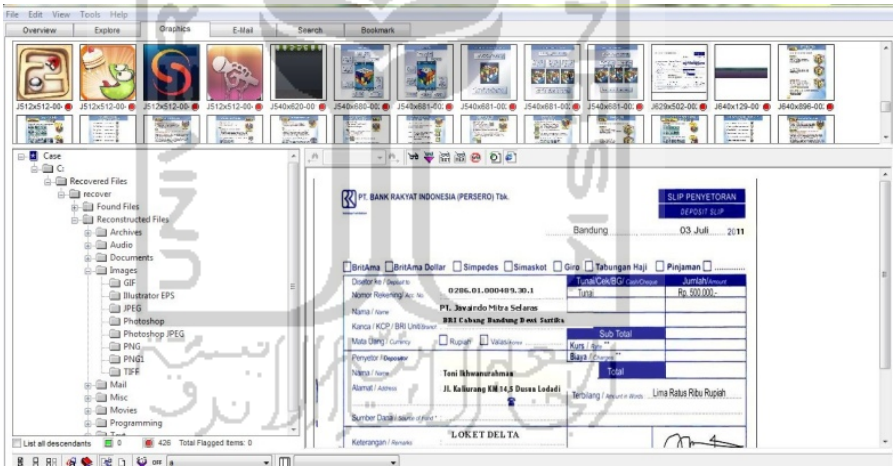


Gambar 4.56 Subsubfolder dari *Reconstructed Files* yang umumnya sesuai dengan ekstensi file didalamnya

Karena pengelompokkan jenis file ini menyeluruh dari suatu iPod Touch, menyebabkan semua file dengan jenis file yang sama akan ikut termasuk di

dalamnya. Semisal contoh, gambar bertipe JPEG yang telah dikelompokkan pada */Reconstructed Files/Images/JPEG* tidak semua gambar JPEG berasal dari folder-folder tempat menyimpan gambar, tapi file JPEG dari aplikasi dan data-data lain juga ikut dikelompokkan.

Dengan banyaknya gambar yang terkumpul, maka diperlukan pengamatan serta ketelitian yang tinggi agar tidak ada gambar yang meleset. Seperti pada kasus ini jika diteliti dan dilihat pada folder *Photos* iPod Touch seperti yang terlihat pada Gambar 4.1, ada beberapa gambar yang tidak ada pada folder-folder penyimpanan gambar setelah disidik dengan Forensic Toolkit. Pada Gambar 4.57 menunjukkan file gambar yang tidak ditemukan pada Menu *Photos* iPod Touch, tapi berhasil ditemukan pada Forensic Toolkit. Ini berarti file tersebut telah dihapus sebelumnya.



Gambar 4.57 Gambar yang tidak ada pada iPod Touch ditemukan didalam folder *Reconstructed Files*

Pada Gambar 4.57 menunjukkan bahwa ada file gambar lain yang ditemukan dalam *Reconstructed Files,* sementara di folder *photos* pada iPod Touch tidak ada gambar tersebut. Ini sebagai salah satu pembuktian bahwa folder *Reconstructed Files* dapat mengembalikan data yang terhapus.

File-file yang terhapus tersebut bisa berisi informasi sehingga harus dianalisis untuk membantu pemecahan suatu kasus. File-file dalam folder *Reconstructed Files* juga harus diamati dengan menggunakan software yang mendukung. Seperti misalnya, file *Document* diperiksa dan dibuka melalui

Microsoft Office, file *Text* bisa dibuka melalui *notepad* atau browser jika filenya bertipe *webpage,* atau file *Movie* dibuka melalui Software Media Player.

4.5 Laporan Hasil Penyelidikan

Laporan hasil penyelidikan dapat dilihat pada lampiran.

4.6 Presentasi

Tahap yang terakhir adalah presentasi. Sebagai penyidik, harus bisa mempertanggungjawabkan hasil penyelidikannya di pengadilan dalam bentuk presentasi. Namun, pada saat presentasi di pengadilan, diperlukan penjelasan yang sederhana dan tidak terlalu menyinggung masalah teknis, sehingga orang yang masih awam terhadap forensik bisa mengerti maksud dari presentasi tersebut. Berbeda pada saat presentasi dengan badan kepolisian yang mengharuskan penjelasan mendetail tentang forensic baik dari segi teknis, maupun non-teknis.

BAB V
KESIMPULAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan , dapat disimpulkan bahwa :

a. Agar dapat dijadikan barang bukti hukum yang sah, penyelidikan barang bukti pada iPod Touch harus melewati tahapan-tahapan komputer forensik, yaitu : Pengumpulan, Pengujian, Analisis, dan Laporan.
b. Proses *imaging* pada iPod Touch tidak bisa dilakukan dengan metode *imaging* media penyimpanan pada umumnya, tapi harus dilakukan dengan cara me-*remote* iPod Touch dari komputer menggunakan PuTTY dan MobaSSH. Selanjutnya iPod Touch me-*remote* komputer kembali agar hasil image disimpan di komputer.
c. Cara melihat struktur file pada iPod Touch bisa dengan aplikasi pihak ketiga *iFuntastic,* atau dengan melakukan *recovery* pada file *data image*pada iPod Touch.
d. Tindakan kriminal yang dapat dilakukan dengan iPod Touch adalah:
    i. Pencurian data.
    ii. *Web Hacking* seperti *Sql Injection*
    iii. Menyimpan dan mengirimkan informasi personal atau perusahaan.
    iv. Mengirimkan e-mail ancaman atau penyerangan.
e. Barang bukti yang dapat ditemukan pada iPod Touch adalah :
    i. *Event* kalender.
    ii. Photo dan video.
    iii. *Caches*.
    iv. Log dari setiap aktivitas.
    v. Peta dan pencitraan satelit.
    vi. Alarm personal.
    vii. Catatan memo.

viii. Musik.
ix. Email.
x. Aktivitas *Web browsing*.
xi. Kontak.
xii. Hal-hal yang menyangkut kepentingan pribadi, seperti Password, akun social network, dll

5.2 Saran

Mengingat keterbatasan yang penulis miliki, maka penulis menyarankan untuk mengembangkan penelitian dimasa mendatang sebagai berikut :

a. Mencari metode baru agar membuat *image* pada iPod Touch jadi lebih mudah.
b. Mencari software *virtual drive* berbasis Windows yang dapat *mounting image* dari iPod Touch secara langsung.

UNIVERSITAS ISLAM INDONESIA

Daftar Pustaka

Alamsyah, R. (2009). Ruby Alamsyah, Teknik Forensik Meneliti Bukti Digital. Retrieved November 15, 2011, from http://www.perspektifbaru.com/wawancara/708 pada 16 Oktober 2009

Bruce, S. (2007). Secure Password Keep You Safer. Retrieved April 10, 2012, from http://www.wired.com/politics/security/commentary/securitymatters/2007/01/72458?currentPage=all

Computer Hacking Forensic Investigation. (2006). Module 37 iPod Touch and iPhone Forensics.

Developer, A. (2004). HFS Plus Basic. Retrieved December 9, 2011, from http://developer.apple.com/legacy/mac/library/#technotes/tn/tn1150.html

Finocchiaro, C., Goldman, E., Natarajan, A., & Stanek, M. (2009). An Investigation into iPod Touch Generation 2. Retrieved December 17, 2011, from http://dl.acm.org/citation.cfm?id=2047470&dl=ACM&coll=DL&CFID=77533652&CFTOKEN=44365781

Ginting, P. (2008). Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana. Retrieved February 7, 2012, from http://eprints.undip.ac.id/17599/1/Philemon_Ginting.pdf

Hoog, A., & Strzempka, K. (2011). *iPhone and iOS Forensics*. (M. Robert, Ed.). Wyman Street, United States of America: Elsevier.

Joyce, A. R., Powers, J., & Adelstein, F. (2008). MEGA A tool for Mac OS X operating system and application forensics.pdf. Retrieved April 2, 2012, from http://www.cpc-ccp.gc.ca/cpclibrary/digital-investigations

Marsico, C., & Rogers, M. (2005). iPod Touch Forensics. Retrieved January 4, 2012, from http://www.utica.edu/academic/institutes/ecii/publications/articles/B4A8B3F3-94D2-F7E5-D32D97CF1539EBB4.pdf

Morrissey, S. (2010). *iOS Forensic Analysis for iPhone , iPad and iPod Touch*. (M. Lowman, Ed.)*Analysis*. New York, United States of America: APRESS.

Muhartin. (2009). SSH. Retrieved March 12, 2012, from http://muhartin.wordpress.com/author/muhartin/page/3

Oxygen, F. (2000). Oxygen Forensic Suite. Retrieved April 10, 2012, from http://www.oxygen-forensic.com/

Przibilla, A. (2005). IPOD TOUCH FORENSICS : FORENSICALLY SOUND EXAMINATION OF AN APPLE IPOD TOUCH. Retrieved December 9, 2011, from http://www.computer.org/comp/proceedings/hicss/2007/2755/00/27550267c.pdf

Rozita. (2011). *Analisis Computer Forensic Menggunakan FTK (Forensic Toolkit)*. Univesitas Islam Indonesia.

Sam, C. (2008). How and When to Use the dd command. Retrieved December 4, 2011, from http://www.codecoffee.com/tipsforlinux/articles/036/html

Saragih, S. (2011). Sistem Operasi iOS. Retrieved December 9, 2011, from https://shidiksaragih.wordpress.com/tag/apa-itu-ios/

Sigwald, J. (2009). iPhone data protection in depth. *Agenda*. Retrieved April 2, 2012, from http://esec-lab.sogeti.com/dotclear/public/publications/11-hitbamsterdam-iphonedataprotection.pdf

Sood, A. (2009). How To Fix "No Mountable File System" Error. Retrieved December 9, 2011, from http://ezinearticles.com/?How-to-Fix-No-Mountable-File-System-Error-in-Mac-OS-X&id=3452027

Sulianta, F. (2008). *Komputer Forensik*. (W. Yoevestian, Ed.). Jakarta, Indonesia: PT. Elex Media Komputindo.

Yoppie. (2008). Apa Itu iPod Touch ?! Retrieved December 6, 2011, from http://aishiterunippon.multiply.com/journal/item/2?&show_interstitial=1&u=/journal/item

Zeeis. (2008). FAT File System - Embedded FAT12, FAT16 & FAT32 File System. Retrieved December 9, 2011, from http://www.zeeis.com/fat-file-system/

LAMPIRAN

Device Data Report

Device details	
Device alias	iTunes Backup (29862c7dc0d57e143eb2a4adb99a0efb5d0bb499)
Retail name	Apple iPod Touch
Manufacturer	Apple
Model	iPod Touch
S/N	N/A
SW revision	Unknown
Boot loader	Unknown
Wi-Fi MAC address	N/A
Bluetooth MAC address	N/A
iTunes display name	Jailbreak
Phone number	N/A
IMSI	N/A
ICCID	N/A
Device model	N/A
Time zone	Asia/Jakarta
Serial number	N/A
Identificator	N/A
Sim status	N/A
Jail Break	No
Device owner numbers	N/A
Case details	
Extracted by version	3.6.5.22
Case assigned	1
Evidence Number	1
Device notes	N/A
Extraction date	4/11/2012
Extraction time	2:58:01 PM
Device owner	Toni Ikhwanurahman
Extraction made by	Muhammad Zulfariansyah
Report details	
Generation date	4/11/2012
Generation time	3:05:57 PM
Extraction made by	Muhammad Zulfariansyah

Phonebook

Ayah

Mobile	085345782544
First name	Ayah
Last Modified Date	1/21/2012 2:25:27 AM
Storage	Device
SHA-2 Hash	a818883fd1ef1915895eff14e6b7571ac42f0367f613a044c8557e7a1bfad001

Ibu

Mobile	084555232545
First name	Ibu
Last Modified Date	1/21/2012 2:25:43 AM
Storage	Device
SHA-2 Hash	0f005272e8e398d8fb39d8ed75e972ad48378f728b7fd7ade13f1ab627459e8f

Lukman

Mobile	0852312854625
First name	Lukman
Last Modified Date	1/21/2012 2:26:28 AM
Storage	Device
SHA-2 Hash	f3bc0a95ae83588af479708f26dcf5bbbeae1bd0560eb5a80b3ecdc2a0a52488

Lukman Citra

Home	lukman.citra@yahoo.com
Mobile	+62 056485623555
Last name	Lukman
First name	Citra
Last Modified Date	1/31/2012 3:51:11 AM
Storage	Device
SHA-2 Hash	1dc62a4937742c209d3f3a9adc2eecbf3c2a748802adbebbaac158be95aeada4

Rob

Mobile	085245441198
First name	Rob
Last Modified Date	1/21/2012 2:26:00 AM
Storage	Device
SHA-2 Hash	b9257bc8b95804f38952670baf49081c613e681f2580b83a4effc1c68e1c1c41

Calendar

Ke kos Citra

Type: Appointment
Ke kos Citra
Location: Kos citra kalijurang
Event start: 1/22/2012 01:00; Event end: 09:00
SHA-2 Hash: 14c465239c07f8db435ce6b4b7f5bfc984e3b8d092461e1496dee24d2aca0cc4

Ngantor

Type: Appointment
Ngantor
Location: Kantor pemda jogja
Event start: 1/23/2012 01:00; Event end: 09:00
SHA-2 Hash: 3b76fc1d0220c33534d6f5f19e8005636a8494c0f71533c566481d2df80d2393

Recurrence: weekly
recurrence end date: 1/23/2013

Ngantor

Type: Appointment
Ngantor
Location: Kantor pemda jogja
Event start: 1/24/2012 01:00; Event end: 09:00
SHA-2 Hash: 6d3f255ae6969fc82721002c17b610970303da63e8db7e45657c7a2c6ef78963

Recurrence: weekly
recurrence end date: 2/24/2013

Ngantor

Type: Appointment
Ngantor
Location: Kantor pemda jogja
Event start: 1/25/2012 01:00; Event end: 09:00
SHA-2 Hash: 512e81be84033dd91bc7e53a279e8352b9ef15982e39884e353271991c587070

Recurrence: weekly
recurrence end date: 2/25/2013

Ngantor

Type: Appointment
Ngantor
Location: Kantor pemda jogja
Event start: 1/26/2012 01:00; Event end: 04:00
SHA-2 Hash: 765e488d525242b1bff11f50e5b0125110608da8ffab72539dc68ab805be7048

Recurrence: weekly
recurrence end date: 2/26/2013

Ngantor

Type: Appointment
Ngantor
Location: Kantor pemda jogja
Event start: 1/29/2012 01:00; Event end: 09:00
SHA-2 Hash: 8707451dd1e72338973b2db04bc7cc3b1e5d241267f0bb915a03796d96e02a47

Recurrence: weekly

Cuti ke balikpapan

Type: All day
Cuti ke balikpapan
Location: Balikpapan
Event start: 1/25/2012; Event end: 2/14/2012
SHA-2 Hash: 39adc295b53c435171729e2c4faea3bbe59d651d05e6ac151927a94dc7b08a00

Ketemu Bos Rob

Type: Appointment
Ketemu Bos Rob
Location: di Ambarukmo plasa
Event start: 1/23/2012 05:00; Event end: 06:00
SHA-2 Hash: 8685e1296a244154265e182a74135cfbe69ba82cdc5a1ce4d6be90430c90649c

Notes

Note	No ones out.... Pushes me awaaaay....
Time stamp	1/23/2012 4:20:00 PM
SHA-2 Hash	e09a0aceb3fb810ab8c701e68b02c805eeda878fcd1b31ff3647e0c8ac00b3eb

Note	Ngantornya ntar aja lah....lagian ada janji ketemu ini....
Time stamp	1/24/2012 2:00:00 AM
SHA-2 Hash	2b78b008381d31ee2f2c8fe03769a0fb80b0805d95bff7d0d7fce78b36378a3e

Note	Hooreeeee ipod baruuuu.....besok mau pamer di kantor ah....hahaha Masi rada susah ngetik pake qwerty touch nya.... Tapi...bntar lagi juga terbiasa ^^
Time stamp	1/22/2012 2:04:00 AM
SHA-2 Hash	11961e9e3c80670bac8ba62f466771442401a55e38f7e1abd676da6ae2977042

Note	Bikin akun skype Ym Orang satu lagi Document Spreadsheet
Time stamp	2/1/2012 2:45:00 AM
SHA-2 Hash	8ec8366ffdb3eeed731cefa4e4dfb11e8f58e49e21203be27fd477eb259c40cc

Note	breakatsuki 1f9eb4fe9e20c8c40c16a6d58031c31e vivie 83fa0348dfc8f80fbd67e274491cee5b rusydi 53db655d291405a08e9d6b496df8b818 d_nhiez 522afd2a935610b473cc1351b01b286c rydes--5db0d787811d7cede53b0b4afb53342c,7--Kuuki--5f4dcc3b5aa765d61d8327deb882cf99,8--SmiLing_DeviL--394b936b627d718460b623f64627208d,9--dare_devil--37d84101c03fe300d4eb2b25526475ed,10--revoltzz--912ec803b2ce49e4a541068d495ab570,40--RinTO--b102f9ac667236305f68eabebc73e89e,11--'Afif Muhtadi--2dabbd29bd3c44a2ee07d3335ad50e69,12--egy--f2a06877d5806516fff1b321fb939d0e,13--ErraS_God999--054316cd8e9eb2c621312bb155556158,16--bety--b40a9222dce602bec327bb7a46f0a0c1,14--squall_luna--91139fde90d2c43a129275bdbc889dd8,15--cutez_19--0378e1c7845c2096a1c5b2636d62648b,17--aa iii uu--5b3bb3e5458e02aa356f2fc671ae08d9,18--puUs--876a5d2b1dafabf6ebfc9553538203d0,19--Yudi--1588d5ce49c2f3e12bf66d162ec5c8ad,20--squall_leonheart--b84c62c35e9cfdd9a86bfdadf0a8155b,21--gemala--c5d3ac86424e9fbc50988c6ae3aa9ecc,22--kyushu_devil--a1fb7f01ffe
Time stamp	2/1/2012 11:08:00 AM
SHA-2 Hash	6da80e77be0d420b6c1b9d4a20bc7a21698f82ebed365c0e8301315aff128e58

Note	Hancurkan
Time stamp	2/10/2012 1:41:00 AM
SHA-2 Hash	07a1b00d255f77532ff62fdc3d9c4dd4188d170630cdedf091a2bc79aac27bd3

File manager

C:\	
c:\private	
c:\private\var	
c:\private\var\mobile	
c:\private\var\mobile\Library	
c:\private\var\mobile\Library\Preferences	

File name	com.apple.apsd.plist
Time stamp	N/A
Size (bytes)	156
SHA-2 Hash	daaf968df4f7dbf4399b974b351063583714147d8aea25dd058d1ba9dc1648bf
EXIF	No EXIF information

File name	com.apple.gamecenter.plist
Time stamp	N/A
Size (bytes)	69
SHA-2 Hash	c01c3ab07e2b6c275d85617fc5410d1369826afae07ddbb77982f5ec45037a37
EXIF	No EXIF information

File name	com.apple.gamed.plist
Time stamp	N/A
Size (bytes)	1006
SHA-2 Hash	3d0b098f423dac6614588b35ba6e52e5ab36713136398e6587fa3b5daee1bd5a
EXIF	No EXIF information

File name	com.apple.preferences.network.plist
Time stamp	N/A
Size (bytes)	60
SHA-2 Hash	1f530b76f6d22068a9bc72b9dedb0cad33e71507b34da3aac59fc536243101a5
EXIF	No EXIF information

File name	com.apple.stocks.plist
Time stamp	N/A
Size (bytes)	1001
SHA-2 Hash	7752c025aca9f3d7edb628a1c2e123d6f0414de49c400345eb273695ba7eb93a
EXIF	No EXIF information

c:\private\var\mobile\Library\SpringBoard	
c:\private\var\mobile\Library\Caches	
c:\private\var\mobile\Library\Caches\Safari	
c:\private\var\mobile\Library\Caches\Safari\Thumbnails	

Timeline

Type:	Appointment
Direction	Unknown
Time stamp:	1/22/2012 1:00:00 AM
Phone Number:	
Text/Description	Ke kos Citra
Remote party:	
Item details	
Start:	1/22/2012 01:00
Finish:	1/22/2012 09:00
Location:	Kos citra kaliurang

Type:	Note
Direction	Unknown
Time stamp:	1/22/2012 2:04:00 AM
Phone Number:	
Text/Description	Hooreeeee ipod baruuuu.....besok mau pamer di kantor ah....hahaha Masi rada susah ngetik pake qwerty touch nya.... Tapi...bntar lagi juga terbiasa ^^
Remote party:	
Item details	
Time stamp:	1/22/2012 2:04:00 AM

Type:	WiFi point
Direction	Unknown
Time stamp:	1/22/2012 2:28:23 AM
Phone Number:	
Text/Description	94:0c:6d:ef:70:28
Remote party:	
Item details	
Point kind:	Original point
Source table:	WiFi Location
MAC address:	94:0c:6d:ef:70:28
Time stamp:	1/22/2012 2:28:23 AM
Time stamp (Asia/Jakarta):	1/22/2012 9:28:23 AM

Type:	WiFi connection
Direction	Unknown
Time stamp:	1/22/2012 3:06:05 AM
Phone Number:	kontrak (f4:9f:54:5c:e7:19)
Text/Description	
Remote party:	
Item details	
Address:	N/A
SSID:	kontrak
BSSID:	f4:9f:54:5c:e7:19
RSSI (in dBm):	-10
Channel:	6
Last joined time (UTC):	1/22/2012 3:06:05 AM
Last auto joined time (UTC):	1/22/2012 4:12:27 AM
Geo coordinates:	N/A
Accuracy (in meters):	N/A

Type:	WiFi connection
Direction	Unknown
Time stamp:	1/22/2012 6:45:09 AM
Phone Number:	crims1412n100 (f4:ec:38:a3:12:8b)
Text/Description	
Remote party:	
Item details	
Address:	N/A
SSID:	crims1412n100
BSSID:	f4:ec:38:a3:12:8b
RSSI (in dBm):	-59
Channel:	4
Last joined time (UTC):	1/22/2012 6:45:09 AM
Last auto joined time (UTC):	1/22/2012 10:17:22 AM
Geo coordinates:	N/A
Accuracy (in meters):	N/A

Type:	IP connection
Direction	Unknown
Time stamp:	1/22/2012 6:45:16 AM
Phone Number:	
Text/Description	14:d6:4d:01:85:79
Remote party:	
Item details	
Router MAC address:	14:d6:4d:01:85:79
Device IP address:	192.168.1.7
DNS address:	192.168.1.1
Time Stamp (UTC):	1/22/2012 6:45:17 AM
Router IP:	192.168.1.1

Type:	WiFi connection
Direction	Unknown
Time stamp:	1/22/2012 9:41:14 AM
Phone Number:	TP-LINK_1B1E38 (00:23:cd:1b:1e:38)
Text/Description	
Remote party:	
Item details	
Address:	N/A
SSID:	TP-LINK_1B1E38
BSSID:	00:23:cd:1b:1e:38
RSSI (in dBm):	-42
Channel:	1
Last joined time (UTC):	1/22/2012 9:41:14 AM
Last auto joined time (UTC):	3/25/2012 2:01:39 PM
Geo coordinates:	N/A
Accuracy (in meters):	N/A

Type:	Appointment
Direction	Unknown
Time stamp:	1/23/2012 1:00:00 AM
Phone Number:	
Text/Description	Ngantor
Remote party:	
Item details	
Start:	1/23/2012 01:00

Finish:	1/23/2012 09:00
Recurrence:	Every week, Monday.
Location:	Kantor pemda jogja

Type:	WiFi connection
Direction	Unknown
Time stamp:	1/23/2012 4:07:45 AM
Phone Number:	Kost G10 (74:ea:3a:f8:b2:de)
Text/Description	
Remote party:	
Item details	
Address:	N/A
SSID:	Kost G10
BSSID:	74:ea:3a:f8:b2:de
RSSI (in dBm):	-55
Channel:	1
Last joined time (UTC):	1/23/2012 4:07:45 AM
Last auto joined time (UTC):	1/23/2012 10:38:05 AM
Geo coordinates:	N/A
Accuracy (in meters):	N/A

Type:	IP connection
Direction	Unknown
Time stamp:	1/23/2012 4:07:49 AM
Phone Number:	
Text/Description	00:0c:42:e7:bc:81
Remote party:	
Item details	
Router MAC address:	00:0c:42:e7:bc:81
Device IP address:	10.0.0.170
DNS address:	8.8.8.8
Time Stamp (UTC):	1/23/2012 4:07:50 AM
Router IP:	10.0.0.1

WiFi Connections

SSID	Zear Hotspot
BSSID	f4:9f:54:5c:e7:19
RSSI (dbm)	-54
Channel	6
Last joined time (UTC)	3/26/2012 4:30:42 AM
Last auto joined time (UTC)	3/29/2012 9:07:28 AM
Geo coordinates (from Google server)	N/A
Accuracy (in meters) (from Google server)	N/A
Address(from Google server)	N/A
SHA-2 Hash	529b776795b113e1028a20d20cbf056ae758cb8098bd4b52390f7fcf5323f79a
SSID	perpus UG
BSSID	00:15:6d:9e:d0:21
RSSI (dbm)	-83
Channel	2
Last joined time (UTC)	3/21/2012 2:38:57 AM
Last auto joined time (UTC)	3/29/2012 6:12:33 AM
Geo coordinates (from Google server)	N/A
Accuracy (in meters) (from Google server)	N/A
Address(from Google server)	N/A
SHA-2 Hash	458c6121a88084999af3cfeea09a7e31830f2790181080f163592de23533c604
SSID	TP-LINK_1B1E38
BSSID	00:23:cd:1b:1e:38
RSSI (dbm)	-42
Channel	1
Last joined time (UTC)	1/22/2012 9:41:14 AM
Last auto joined time (UTC)	3/25/2012 2:01:39 PM
Geo coordinates (from Google server)	N/A
Accuracy (in meters) (from Google server)	N/A
Address(from Google server)	N/A
SHA-2 Hash	eaacc5fd3b652e01a1f3cb275ecee4189193839846aedb789b074aa1ee29fa3a
SSID	KANAYAKAN BARU 40
BSSID	00:26:5a:37:0e:64
RSSI (dbm)	-72
Channel	10
Last joined time (UTC)	2/28/2012 3:36:43 AM
Last auto joined time (UTC)	3/9/2012 5:40:29 AM
Geo coordinates (from Google server)	N/A
Accuracy (in meters) (from Google server)	N/A
Address(from Google server)	N/A
SHA-2 Hash	c184e97b8bb5181a830314a9e865cf59c94e1d5dd13d1a10627cf5d6f83a1559

SSID	AndroidAP
BSSID	f4:9f:54:5c:e7:19
RSSI (dbm)	-49
Channel	6
Last joined time (UTC)	1/23/2012 2:34:22 PM
Last auto joined time (UTC)	3/4/2012 11:49:58 AM
Geo coordinates (from Google server)	N/A
Accuracy (in meters) (from Google server)	N/A
Address(from Google server)	N/A
SHA-2 Hash	796f66b6306217b19c78486bb299ab5e2a5bf63f28566bb41f42447b60db6ce2
SSID	keluyuran13657
BSSID	f4:9f:54:5c:e7:19
RSSI (dbm)	-11
Channel	6
Last joined time (UTC)	2/3/2012 2:32:28 AM
Last auto joined time (UTC)	2/5/2012 10:15:32 AM
Geo coordinates (from Google server)	N/A
Accuracy (in meters) (from Google server)	N/A
Address(from Google server)	N/A
SHA-2 Hash	f962e57fb8d6fecf4d9274818c608fac3a62a0df90837f978db30428808bbce7
SSID	keluyuran
BSSID	f4:9f:54:5c:e7:19
RSSI (dbm)	-40
Channel	6
Last joined time (UTC)	1/31/2012 2:53:18 AM
Last auto joined time (UTC)	2/1/2012 5:21:33 PM
Geo coordinates (from Google server)	N/A
Accuracy (in meters) (from Google server)	N/A
Address(from Google server)	N/A
SHA-2 Hash	2e03b5893df0f4a5c808cde76d27f73c1b1ae5725344670157bc04cc98004887
SSID	Nite
BSSID	02:e0:fd:cf:bb:e0
RSSI (dbm)	-30
Channel	10
Last joined time (UTC)	1/30/2012 7:25:02 AM
Last auto joined time (UTC)	N/A
Geo coordinates (from Google server)	N/A
Accuracy (in meters) (from Google server)	N/A
Address(from Google server)	N/A
SHA-2 Hash	60f3417ca685b495791632beaee511828775452ea17491e0a92b8179ddd67f30

SSID	kontrak
BSSID	f4:9f:54:5c:e7:19
RSSI (dbm)	-10
Channel	6
Last joined time (UTC)	1/22/2012 3:06:05 AM
Last auto joined time (UTC)	1/22/2012 4:12:27 AM
Geo coordinates (from Google server)	N/A
Accuracy (in meters) (from Google server)	N/A
Address(from Google server)	N/A
SHA-2 Hash	fabee26c0668f75757b36b92f275db22cd1e3ebe98b126bed6dc4aaf4cc460f9
SSID	Kost G10
BSSID	74:ea:3a:f8:b2:de
RSSI (dbm)	-55
Channel	1
Last joined time (UTC)	1/23/2012 4:07:45 AM
Last auto joined time (UTC)	1/23/2012 10:38:05 AM
Geo coordinates (from Google server)	N/A
Accuracy (in meters) (from Google server)	N/A
Address(from Google server)	N/A
SHA-2 Hash	bc30269699a70b216986e7ab2c1e6e4d5f2d02e8ab6efd3dc7ddc35df86a8c35

IP connections

Router MAC address	00:10:4b:0e:52:97
Device IP address	192.168.111.201
DNS address	192.168.111.1
Time Stamp (UTC)	3/29/2012 6:06:06 AM
Router IP	1.1.1.1
SHA-2 Hash	8190021235cbdd63e56b98143c62bc83b166db225ca3868938d8aeab137b318d

Router MAC address	00:10:4b:0e:52:97
Device IP address	192.168.111.86
DNS address	192.168.111.1
Time Stamp (UTC)	3/29/2012 6:06:06 AM
Router IP	1.1.1.1
SHA-2 Hash	10599a579870ca1f98a5f7bc7e2758fd79e09f2546eb1a432c865fd5f80f1aa4

Router MAC address	00:10:4b:0e:52:97
Device IP address	192.168.111.243
DNS address	192.168.111.1
Time Stamp (UTC)	3/29/2012 6:06:06 AM
Router IP	1.1.1.1
SHA-2 Hash	809887de9a9ad9b0ca4792b023e20e4fa82aae72e943eea0f7c3bd398b30a53e

Router MAC address	00:10:4b:0e:52:97
Device IP address	192.168.111.155
DNS address	192.168.111.1
Time Stamp (UTC)	3/29/2012 6:06:06 AM
Router IP	1.1.1.1
SHA-2 Hash	589511be4fc0a4de44133e74c11e9db7993c649680d732db63c276bbe3864f58

Router MAC address	00:10:4b:0e:52:97
Device IP address	192.168.111.114
DNS address	192.168.111.1
Time Stamp (UTC)	3/29/2012 6:06:06 AM
Router IP	1.1.1.1
SHA-2 Hash	7854fc6445cc6ec2946f17e63f8cd3bbd4557c753a5fe25150f91e3da8eb7dae

Router MAC address	f4:9f:54:5c:e7:19
Device IP address	192.168.43.150
DNS address	192.168.43.1
Time Stamp (UTC)	3/28/2012 5:24:15 PM
Router IP	192.168.43.1
SHA-2 Hash	07e63360228751fee734a44ec9064f2d4e6663494233d98f55a969ac56267e02

Router MAC address	00:23:cd:1b:1e:38
Device IP address	192.168.2.5
DNS address	192.168.2.1
Time Stamp (UTC)	3/25/2012 2:01:43 PM
Router IP	192.168.2.1
SHA-2 Hash	99d08820b1d21c3c2cdd4a1e7b70825208fba47dce310b58c6860c0c54254642

Router MAC address	00:23:cd:1b:1e:38
Device IP address	192.168.2.8
DNS address	192.168.2.1
Time Stamp (UTC)	3/25/2012 2:01:43 PM
Router IP	192.168.2.1
SHA-2 Hash	d896a01c63cdf0d1ec7a5ce476cd15defb0d666273e42324811844542101d34a

Router MAC address	00:26:5a:37:0e:63
Device IP address	192.168.1.9
DNS address	192.168.1.1
Time Stamp (UTC)	3/9/2012 4:33:51 AM
Router IP	192.168.1.1
SHA-2 Hash	bc620c024a03c50057a926f221656b9354eae08247db3ef78fdd6a81a2aab448

Router MAC address	00:26:5a:37:0e:63
Device IP address	192.168.1.13
DNS address	192.168.1.1
Time Stamp (UTC)	3/9/2012 4:33:51 AM
Router IP	192.168.1.1
SHA-2 Hash	32a7d0a71855f4575bd2235631a431243fb66daf773e076870e52217a9491bf2

Locations

Time stamp (UTC)	2/27/2012 4:10:06 AM
Time stamp (Region)	2/27/2012 11:10:06 AM
Coordinates	N/A
Address	N/A
Speed	N/A
Point kind	Original point
Point type	Cell point
Source table	Cell Location
Vertical accuracy	N/A
Horizontal accuracy	N/A
SHA-2 Hash	224d84d7f3f519d82a5c6305a04838b6f0b88616f78eac71e0f7451451da8b0c

Time stamp (UTC)	1/23/2012 8:22:42 AM
Time stamp (Region)	1/23/2012 3:22:42 PM
Coordinates	N/A
Address	N/A
Speed	N/A
Point kind	Original point
Point type	WiFi point
Source table	WiFi Location
MAC	74:ea:3a:f8:b2:de
Vertical accuracy	N/A
Horizontal accuracy	N/A
SHA-2 Hash	77d41471d5205c32c55395801776c5ee02536d0dee02d371d27464b12af2adc2

Time stamp (UTC)	1/23/2012 8:36:26 AM
Time stamp (Region)	1/23/2012 3:36:26 PM
Coordinates	N/A
Address	N/A
Speed	N/A
Point kind	Original point
Point type	WiFi point
Source table	WiFi Location
MAC	00:1e:64:16:40:03
Vertical accuracy	N/A
Horizontal accuracy	N/A
SHA-2 Hash	f20c55b56a83e3c534fa66b00b3963a4c9c567db4c2e76b11d110a24999292ee

Time stamp (UTC)	1/22/2012 2:28:23 AM
Time stamp (Region)	1/22/2012 9:28:23 AM
Coordinates	N/A
Address	N/A
Speed	N/A
Point kind	Original point
Point type	WiFi point
Source table	WiFi Location
MAC	94:0c:6d:ef:70:28
Vertical accuracy	N/A
Horizontal accuracy	N/A
SHA-2 Hash	9d242a87e1c726d6acf6be0235b0058644a6b82c4ec2692ce38c1c7780072eda

Time stamp (UTC)	2/1/2012 11:35:50 AM
Time stamp (Region)	2/1/2012 6:35:50 PM
Coordinates	N/A
Address	N/A
Speed	N/A
Point kind	Original point
Point type	WiFi point
Source table	WiFi Location
MAC	00:02:6f:5d:da:ab
Vertical accuracy	N/A
Horizontal accuracy	N/A
SHA-2 Hash	5b7ae2fed5e97d9b513acf60898e508a54079280cb2e1b9d2435235fcb2ac168

Time stamp (UTC)	2/1/2012 2:20:05 PM
Time stamp (Region)	2/1/2012 9:20:05 PM
Coordinates	N/A
Address	N/A
Speed	N/A
Point kind	Original point
Point type	WiFi point
Source table	WiFi Location
MAC	00:4f:62:1c:f8:90
Vertical accuracy	N/A
Horizontal accuracy	N/A
SHA-2 Hash	2ce64e43afe24ea422206a6b143d306186ee01f508493140b6d2f6eb944afecf

Time stamp (UTC)	2/1/2012 2:22:17 PM
Time stamp (Region)	2/1/2012 9:22:17 PM
Coordinates	N/A
Address	N/A
Speed	N/A
Point kind	Original point
Point type	WiFi point
Source table	WiFi Location
MAC	b0:48:7a:b7:2f:67
Vertical accuracy	N/A
Horizontal accuracy	N/A
SHA-2 Hash	5d79a2c94ada8f30b57da1fae962fa8aa0e725684fc54bf4667c83c82a60e7aa

Time stamp (UTC)	2/4/2012 10:02:34 AM
Time stamp (Region)	2/4/2012 5:02:34 PM
Coordinates	N/A
Address	N/A
Speed	N/A
Point kind	Original point
Point type	WiFi point
Source table	WiFi Location
MAC	1c:7e:e5:fd:1c:68
Vertical accuracy	N/A
Horizontal accuracy	N/A
SHA-2 Hash	0a0a29f5a11a8e85083c7c85c0e1e60557e139a9fdf7790b32f9af9f588b1c55

Time stamp (UTC)	2/4/2012 10:02:36 AM
Time stamp (Region)	2/4/2012 5:02:36 PM
Coordinates	S 1.27707451, E 116.83251583
Address	N/A

Speed	N/A
Point kind	Original point
Point type	WiFi point
Source table	WiFi Location
MAC	00:20:a6:92:b8:72
Vertical accuracy	12
Horizontal accuracy	53
SHA-2 Hash	d1b2ecc123af854ff96164c33b1c99f36ecddb3d9e75bd48c0ce2a98e2153acd

Time stamp (UTC)	2/4/2012 10:02:36 AM
Time stamp (Region)	2/4/2012 5:02:36 PM
Coordinates	S 1.2770701, E 116.83139181
Address	N/A
Speed	N/A
Point kind	Original point
Point type	WiFi point
Source table	WiFi Location
MAC	00:25:9c:d5:bf:16
Vertical accuracy	12
Horizontal accuracy	60
SHA-2 Hash	e43ce28a92136d3f9b79dbc71d1da4634f0ad89b45414e3c4f6875285b110812

Web cache

Safari (C:\private\var\mobile\Library\Safari\)	
File name	c:\private\var\mobile\Library\Safari\SuspendState.plist
Size (bytes)	12502
SHA-2 Hash	eea36d1c33bf7ae0e520006e21d9ef04a0d64da27b3a03643911c753d1b4f455

File name	c:\private\var\mobile\Library\Safari\Bookmarks.db
Size (bytes)	49152
SHA-2 Hash	527e03bab66d67ca0d652b8c4ff081e2559f207b82eb686cbeec369ecbdb8d5c

File name	c:\private\var\mobile\Library\Safari\History.plist
Size (bytes)	0
SHA-2 Hash	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

File name	c:\private\var\mobile\Library\Caches\Safari\Thumbnails\B1247D4B-2AB1-432E-AA40-66CC52024CE0.png
Size (bytes)	37561
SHA-2 Hash	41a755d2289235f59a6de3090f71cf08b2efc880763c97e8ce30b99bc7715201

File name	c:\private\var\mobile\Library\Caches\Safari\Thumbnails\FF211DF6-C732-4AF5-A4B9-C19664B3F4B9.png
Size (bytes)	18984
SHA-2 Hash	1e6e895e718a6cbc0ac91c7fa5237827dff2c432568cceedc5b44a7df416b4c7

File name	c:\private\var\mobile\Library\Caches\Safari\Thumbnails\F66B6F5F-F111-4C2F-851C-968B5B69FEF1.png
Size (bytes)	1120
SHA-2 Hash	c78d5d0009c6998fb6ee2784cdaffcc40f33d34b967a12fc65a0235372630a3f

File name	c:\private\var\mobile\Library\Caches\Safari\Thumbnails\0D5A5AB1-3AE2-4E8D-B8CB-441C4FF48590.png
Size (bytes)	36170
SHA-2 Hash	b765315e7d8fbfea88da4a895b9c2be53f4bcf24b1df7d30421e7e0fac57f120

File name	c:\private\var\mobile\Library\Cookies\Cookies.binarycookies
Size (bytes)	9657
SHA-2 Hash	7fa0c2d8abb6b217d44b1efc6dced16037fcbc758b298d8b1af0257775635c4e

File name	c:\private\var\mobile\Library\Cookies\com.apple.itunesstored.2.sqlitedb
Size (bytes)	12288
SHA-2 Hash	d0c5f7c47a2e499978ea8efc577459a20f5e3b2d64289d038e93ff21cf543ed1

Bookmarks	
URL	http://www.playboy.mobi/ms/p/a3/pb/sfAbuou_GWumCN7UW24NA7A/view.
Path	Playboy | Lindsay Lohan
SHA-2 Hash	34a0cf145808b27e4fb7c2e038dd9842

URL	http://www.sman1clp.com/index.php?cat=artikel&idartikel=-28%20union%20
Path	SMA Negeri 1 Cilacap - The Favourite school in Cilacap
SHA-2 Hash	24e4fe175b82838001475e49827859e2

Dictionaries

Original Order	2
Word	ping
Frequency	N/A
SHA-2 Hash	970c3e11acf1be38f06285cb9136692d

Original Order	4
Word	sudd
Frequency	N/A
SHA-2 Hash	1d54e8465ed5b9e1cb3a6b2dd81a61e9

Original Order	6
Word	iphone
Frequency	N/A
SHA-2 Hash	0a2b7dbfc851909382c57223065c9a73

Original Order	8
Word	if
Frequency	N/A
SHA-2 Hash	797135c403479d0c5e3d21dba01db4ad

Original Order	10
Word	iphone
Frequency	N/A
SHA-2 Hash	719829cd70f5c7a7b62abeda76467398

Original Order	12
Word	if
Frequency	N/A
SHA-2 Hash	2e25692dbe17e489c264a7a4df19ba24

Original Order	14
Word	iphone
Frequency	N/A
SHA-2 Hash	d36faa33944b27c5059ca52f40f9c2a7

Original Order	16
Word	ssh
Frequency	N/A
SHA-2 Hash	21b4923c847c843e5677e8aa803b2a4d

Original Order	18
Word	ump
Frequency	N/A
SHA-2 Hash	2cb4f802c4711d05e9c55946a2e069bf

Original Order	20
Word	if
Frequency	N/A
SHA-2 Hash	e46b01ac2bc450c65e05df7248d74000

Skype Analyzer

Account

Toni Ikhwanurahman (toniiwan)

No photo

Account name	toniiwan
Display name	Toni Ikhwanurahman
Language (ISO)	en
Country (ISO)	id
City	Jogjakarta
Email	toniiwan@gmail.com
Birthday	10/10/1985
Balance	0
Time zone	+07:00
Chat Messages Count	13
Calls Count	5
SHA-2 Hash	07216d0f6514a6ffeeafe7a0e7908128a435480616b3833db7eaa2ae72863eee

Account calls (toniiwan)

Remote party	Zear Rock (zearrock)
Duration	00:00:00
Call type	Skype call
Call direction	Incoming call
Is missed	Yes
Cost	0
Time stamp	2/1/2012 6:36:31 PM
Response time stamp	2/1/2012 6:36:31 PM
Online number	
SHA-2 Hash	c9d6c0fea8cbae768247ec8c94b2a12b0b5ef7d7783ca8f8992c3fa3363eb14c

Remote party	Zear Rock (zearrock)
Duration	00:01:43
Call type	Skype call
Call direction	Incoming call
Is missed	No
Cost	0
Time stamp	2/1/2012 6:38:34 PM
Response time stamp	2/1/2012 6:38:34 PM
Online number	
SHA-2 Hash	81c747024235cf4e9d6c213a8b3b8c724badc90eea8cf0dcfd0415f7f224c914

Remote party	Zear Rock (zearrock)
Duration	00:00:38
Call type	Skype call
Call direction	Incoming call
Is missed	No
Cost	0
Time stamp	2/1/2012 6:40:30 PM
Response time stamp	2/1/2012 6:40:30 PM
Online number	

Account calls (toniiwan)

SHA-2 Hash	348c027d8de47a5f8b7b4c11c0a374dd7d9bc5821ef7304ac3b68e2e789d3baf

Remote party	Zear Rock (zearrock)
Duration	00:00:00
Call type	Skype call
Call direction	Incoming call
Is missed	Yes
Cost	0
Time stamp	2/1/2012 6:36:35 PM
Response time stamp	2/1/2012 6:36:35 PM
Online number	
SHA-2 Hash	50d8fefb03a7e976c2cf473acf9118bfd916ca91a3e40b3d142d2c1fc7c5bbc6

Remote party	Zear Rock (zearrock)
Duration	00:00:54
Call type	Skype call
Call direction	Outgoing call
Is missed	No
Cost	0
Time stamp	2/1/2012 4:21:35 PM
Response time stamp	2/1/2012 4:21:35 PM
Online number	
SHA-2 Hash	db8f60a099e1d997b7c5522569bfede233ebd571bb96e5352f5a1a6c3bba7dd0

Account chat messages (toniiwan)

Remote party	zearrock
Direction	Outgoing
Time stamp	2/1/2012 4:23:08 PM
Message kind	Private message
SHA-2 Hash	b978677b6bcb434c905c7488a3ae92a4e3bdab8e3618ad82e59ffcc1c94c3d98
Bisa...tapi kok gada suaranya?	

Remote party	zearrock
Direction	Outgoing
Time stamp	2/1/2012 4:33:56 PM
Message kind	Private message
SHA-2 Hash	30ab79b737a35bac1284a4c6397bc4322e96df21643218c3d5247014aa1e627d
Woi	

Account contacts (toniiwan)

Echo / Sound Test Service (echo123)

Account name	echo123
Display name	Echo / Sound Test Service
Language (ISO)	en
Web address	http://www.skype.com/go/help
Note	Hi, this is Skype automatic sound test service. Add me to your contact list and give me a call to test your sound setup. See http://www.skype.com/go/help for more assistance. Thank you.
Time zone	-00:00
SHA-2 Hash	56bae69342aa4eeaf79d42d865faac85eb6c393109ae7135d2b213595180300d

Account contacts (toniiwan)

fahrian nur (ryan.guanteng)

Account name	ryan.guanteng
Display name	fahrian nur
Country (ISO)	id
Region	East Borneo
City	Balikpapan
Time zone	-00:00
SHA-2 Hash	212bb3e716fdf4db2c84481a0d068e13878dd31 [illegible] 5f76ffb4657478f039663

Zear Rock (zearrock)

Account name	zearrock
Display name	Zear Rock
Language (ISO)	id
Country (ISO)	id
City	Balikpapan-Yogyakarta
Web address	http://criticalnote.blogspot.com
Note	Yeah....
Birthday	6/19/1990
Time zone	-10:35
SHA-2 Hash	55a606665df7c287cc1a517c787238b27d70713ed1293edfd09999c3421d38f9

End of report

Signed by _____

FTK CASE REPORT

Case Information

Apr 11, 2012

FTK Version	Version 1.50, build 04.08.23
Case Number	1
Case Location	c:\Kasus iPod\
Case Description	
Report Created	Apr 11, 2012 4:29pm

Forensic Examiner	Muhammad Zulfariansyah
Agency	Zear Forensic Investigation
Address	Jl. Kaliurang KM 10, Aji Soko Kost
Phone	08995482864
Fax	
Email	zearrock@gmail.com
Comments	

Investigator	Muhammad Zulfariansyah
Agency	Zear Forensic Investigation
Address	Jl. Kaliurang, KM 10
Phone	08995482864
Fax	
Email	zearrock@gmail.com
Comments	iPod Milik Toni Ikhwanurahman

AccessData Forensic Toolkit

FTK CASE REPORT

File Overview

Apr 11, 2012

Evidence Items

Evidence Items: 1

File Items

Total File Items: 92707
Flagged Thumbnails: 0
Other Thumbnails: 38853

File Status

KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 1398
Encrypted Files: 84
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 47735
OLE Subitems: 92
Flagged Ignore: 0
KFF Ignorable: 0

File Category

Documents: 3502
Spreadsheets: 5
Databases: 0
Graphics: 38853
E-mail Messages: 0
Executables: 56
Archives: 86
Folders: 0
Slack/Free Space: 0
Other Known Type: 4088
Unknown Type: 46117

FTK CASE REPORT

Evidence List

Apr 11, 2012
Display Name: Recovered Files
Evidence File Name: Recovered Files
Evidence Path: D:\C
Identification Name/Number: iPod Touch
Evidence Type: Contents of a folder
Added: 4/11/2012 3:16:52 PM
Children:
Descendants: 92707
Investigator's Name: Muhammad Zulfariansyah
Comment: Milik Toni Ikhwanurahman

AccessData Forensic Toolkit

FTK CASE REPORT

Case Summary

Case Audit Files

List by File Path

- None -

MS Access database

List File Properties

- None -

Bookmarks

- None -

Graphic Thumbnails

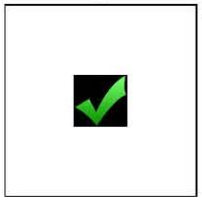

```
4/11/2012 3:16:52 PM -- FTK Version 1.50 build 04.08.23
        Examiner's Machine:
        Phys Mem:  Total: 2,147,483,647  Available: 2,147,483,647  Used: 0
        Virt Mem:  Total: 2,147,352,576  Available: 1,913,188,352  Used: 234,164,224
        Page File Available: 4,294,967,295
        ----------------------------------------------------
4/11/2012 3:16:52 PM -- AccessData PRTK5 EFS integration unavailable: AccessData PRTK 5 is n
4/11/2012 3:16:52 PM -- New case started by investigator Muhammad Zulfariansyah using FTK ve
        Case Name: Kasus iPod
        Case Number: 1
        Case Folder: c:\Kasus iPod
        Description:
        Case Log Options (NOT Case Agent Logging Options):
          Log case and evidence events: Yes
          Log error messages: Yes
          Log bookmarking events: Yes
          Log searching events: Yes
          Log special searching events: Yes
          Log other events: Yes
          Log extended information: No
        Processes to be performed:
          File Extraction: Yes
          File Identification: Yes
          MD5 Hash: Yes
          SHA1 Hash: No
          KFF (Known File Filter): Yes
          Entropy Test: Yes
          Full Text Index: Yes
          Prerender Thumbnails: Yes
          File Listing Database: Yes
          HTML File Listing: Yes
          Decrypt EFS Files: Unavailable
        Default Case Refinement Settings:
          Add files only if they satisfy BOTH the file status and the file type criteria as
            File Status Criteria:
              Deletion status: any
              Encryption status: any
              From email status: any
              Duplicate status: any
              OLE stream status: any
            File Type Criteria:
              documents: yes
              spreadsheets: yes
              databases: yes
              graphics: yes
              email messages: yes
              executables: yes
              archives: yes
              folders: yes
```

FTK CASE REPORT

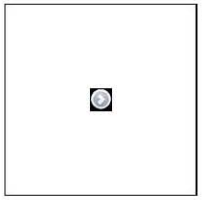
All Graphics

Apr 11, 2012

1 D:\C\Recovered Files\recover\Found Files\Data\audit\Audio\UISounds\ct-error.caf



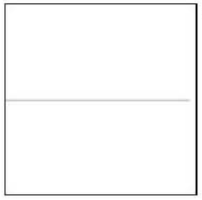
2 D:\C\Recovered Files\recover\Found Files\Data\audit\CoreServices\MobileStorageMounter.app\it.lproj\Localizable.strings



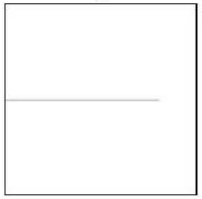
3 D:\C\Recovered Files\recover\Found Files\Data\audit\CoreServices\MobileStorageMounter.app\ja.lproj\Localizable.strings

Thumbnail Unavailable

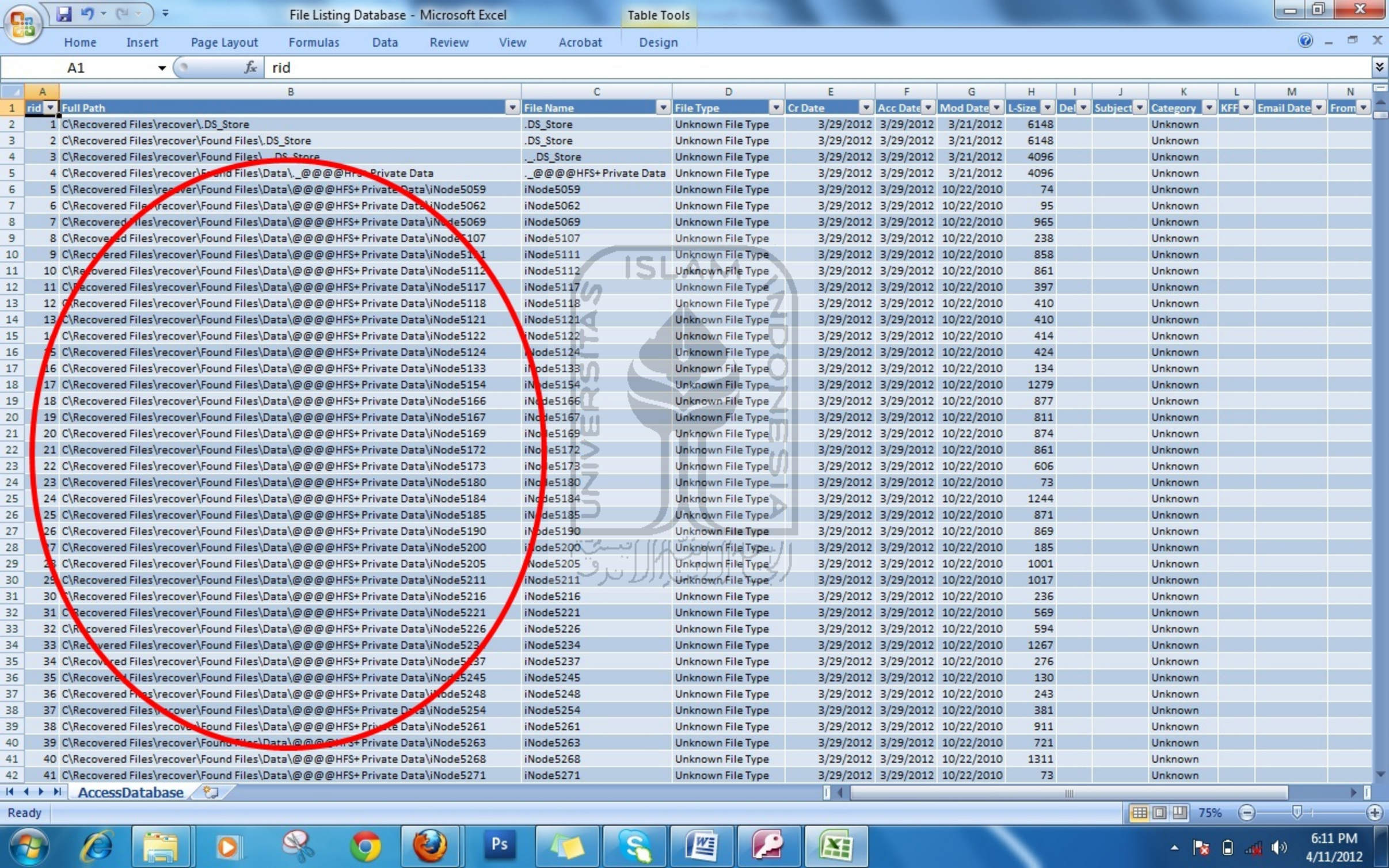
4 D:\C\Recovered Files\recover\Found Files\Data\audit\CoreServices\MobileStorageMounter.app\ko.lproj\Localizable.strings



5 D:\C\Recovered Files\recover\Found Files\Data\audit\CoreServices\MobileStorageMounter.app\ms.lproj\Localizable.strings



6 D:\C\Recovered Files\recover\Found Files\Data\audit\CoreServices\MobileStorageMounter.app\no.lproj\Localizable.strings



File Listing Database - Microsoft Excel

Table Tools

Home Insert Page Layout Formulas Data Review View Acrobat Design

A1 rid

rid	Full Path	File Name	File Type	Cr Date	Acc Date	Mod Date	L-Size	Del	Subject	Category	KFF	Email Date	From
1	C\Recovered Files\recover\.DS_Store	.DS_Store	Unknown File Type	3/29/2012	3/29/2012	3/21/2012	6148			Unknown			
2	C\Recovered Files\recover\Found Files\.DS_Store	.DS_Store	Unknown File Type	3/29/2012	3/29/2012	3/21/2012	6148			Unknown			
3	C\Recovered Files\recover\Found Files\._.DS_Store	._.DS_Store	Unknown File Type	3/29/2012	3/29/2012	3/21/2012	4096			Unknown			
4	C\Recovered Files\recover\Found Files\Data\._@@@@HFS+ Private Data	._@@@@HFS+ Private Data	Unknown File Type	3/29/2012	3/29/2012	3/21/2012	4096			Unknown			
5	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5059	iNode5059	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	74			Unknown			
6	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5062	iNode5062	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	95			Unknown			
7	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5069	iNode5069	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	965			Unknown			
8	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5107	iNode5107	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	238			Unknown			
9	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5111	iNode5111	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	858			Unknown			
10	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5112	iNode5112	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	861			Unknown			
11	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5117	iNode5117	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	397			Unknown			
12	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5118	iNode5118	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	410			Unknown			
13	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5121	iNode5121	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	410			Unknown			
14	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5122	iNode5122	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	414			Unknown			
15	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5124	iNode5124	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	424			Unknown			
16	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5133	iNode5133	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	134			Unknown			
17	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5154	iNode5154	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	1279			Unknown			
18	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5166	iNode5166	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	877			Unknown			
19	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5167	iNode5167	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	811			Unknown			
20	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5169	iNode5169	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	874			Unknown			
21	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5172	iNode5172	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	861			Unknown			
22	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5173	iNode5173	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	606			Unknown			
23	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5180	iNode5180	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	73			Unknown			
24	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5184	iNode5184	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	1244			Unknown			
25	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5185	iNode5185	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	871			Unknown			
26	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5190	iNode5190	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	869			Unknown			
27	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5200	iNode5200	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	185			Unknown			
28	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5205	iNode5205	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	1001			Unknown			
29	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5211	iNode5211	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	1017			Unknown			
30	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5216	iNode5216	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	236			Unknown			
31	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5221	iNode5221	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	569			Unknown			
32	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5226	iNode5226	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	594			Unknown			
33	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5234	iNode5234	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	1267			Unknown			
34	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5237	iNode5237	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	276			Unknown			
35	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5245	iNode5245	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	130			Unknown			
36	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5248	iNode5248	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	243			Unknown			
37	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5254	iNode5254	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	381			Unknown			
38	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5261	iNode5261	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	911			Unknown			
39	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5263	iNode5263	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	721			Unknown			
40	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5268	iNode5268	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	1311			Unknown			
41	C\Recovered Files\recover\Found Files\Data\@@@@HFS+ Private Data\iNode5271	iNode5271	Unknown File Type	3/29/2012	3/29/2012	10/22/2010	73			Unknown			

AccessDatabase

Ready 75%

6:11 PM 4/11/2012