EKSPLORASI BUKTI DIGITAL PADA SIM CARD

Yudi Prayudi [1], Fachreza Rifandi[2]
[1]Pusat Studi Forensika Digital, Jurusan Teknik Informatika
Fakultas Teknologi Industri - Universitas Islam Indonesia
Jalan Kaliurang Km 14.5, Ngaglik Sleman Yogyakarta, 55581
E-mail : prayudi at uii.ac.id[1]

Abstrak

Telepon Selular adalah salah satu teknologi yang sangat populer dikalangan masyarakat saat ini. Setiap telepon selular yang terhubung dengan jaringan telekomunikasi harus memiliki SIM Card. Meningkatnya jumlah telepon selular dan SIM Card berdampak pada meningkatnya potensi cybercrime yang dapat dilakukan oleh seseorang. Karena itu investigator digital harus dapat mengantisipasi kemungkinan adanya kasus kejahatan dengan barang bukti telepon selular ataupun SIM Card. Pada penelitian ini dilakukan upaya eksplorasi karakteristik data dan barang bukti digital pada SIM Card melalui bantuan tools SIMCard Seizure. Hasil yang didapat diharapkan menjadi acuan praktis proses investigasi forensika pada suatu kasus dengan barang bukti SIM Card.

Cellular phone is one of the technologies which are very popular among the people. Any cellular phone that connected to the telecommunications network must have a SIM Card. The increasing number of cellular phone and SIM card have impact on increasingcybercrimethatcan bedone bysomeone. Digital investigators must be able to anticipate the possibility of cases with cellular phone or SIM card as an evidence. This researchtry to explore the characteristics of data and digital evidence using SIM Card Seizure tools. The results are expected to be a practical reference for the forensics investigator on a case with SIM Card as an evidence.

Kata kunci: *SIM Card, Investigasi digital, bukti digital, forensika digital*

1. PENDAHULUAN

1.1 Latar Belakang

Salah satu perlengkapan teknologi yang telah menjadi bagian dari gaya hidup saat ini adalah telepon selular / smartphone. Perubahan telepon selular menjadi smartphone telah mendudukan telepon selular sebagai "*ubiquitous devices*" yang menyatu dalam kehidupan sehari-hari. Karena itu adalah wajar bila World Bank memperkirakan bahwa dalam waktu 1-2 tahun kedepan jumlah telepon selular akan sama dengan jumlah penduduk di dunia ini. Menurut data yang dikeluarkan oleh ITU (*International Communication Union*), pada saat ini jumlah kepemilikan telepon selular pada beberapa negara hampir sama atau bahkan melebihi jumlah penduduk di negara tersebut, Indonesia termasuk ke dalam negara dengan prosentase kepemilikan telepon selular melebihi jumlah penduduknya (109%). Hal ini menunjukkan perkembangan yang pesat dari telepon selular saat ini. Menurut laporan dari RSA, peningkatan pengguna telepon selular / smartphone di seluruh dunia meningkat rata-rata 42%. Dari aspek teknologi, setiap minggu rata-rata terdapat 5 produk / model baru dari telepon selular / smartphone [1].

Meningkatnya jumlah pengguna telepon selular / smartphone telah mengubah kecenderungan orang untuk melakukan tindak kejahatan. Laporan yang dikeluarkan oleh RSA, menunjukkan bahwa diantara 10 trend cybercrime pada tahun 2013 yang pertama adalah kejahatan dengan memanfaatkan fasilitas dan kemampuan peralatan telepon selular / smartphone. Laporan yang dikeluarkan oleh Symantec, untuk wilayah Eropa statistik menunjukkan bahwa 1 dari 10 pengguna telepon selular telah menjadi korban dari cybercrime. [2]

Setiap telepon selular akan terhubung dengan jaringan telekomunikasi melalui ketersediaan SIM Card yang terpasang didalamnya. Dengan kata lain setiap telepon selular akan memiliki SIM Card yang berfungsi sebagai nomor dari telepon selular tersebut. Selain kejahatan umum menggunakan telepon selular, kejahatan yang secara spesifik memanfaatkan karakteristik SIM Card telah mulai bermunculan. Setidaknya sejumlah studi kasus yang dirangkum oleh Casey [1] menjadi contoh beberapa kejahatan memanfaatkan SIM Card. Karakteristik kasus SIM Card umumnya diawali oleh pencurian SIM Card. Pelaku kemudian menggunakan *SIM Card* curian untuk melakukan tindakan illegal yang mengakibatkan adanya lonjakan tagihan pada *SIM Card* curian tersebut. Sementara pada kasus yang lain *SIM Card*curian digunakan untuk menipu pihak bank dengan cara melakukan transaksi palsu.

Salah satu upaya untuk pengungkapan kasus-kasus cybercrime adalah melalui proses investigasi forensika digital. Khususnya untuk kasus *SIM Card,* aktivitas investigasi diperlukan untuk mencari dan menemukan

bukti kejahatan yang tersimpan dalam *SIM Card*. Mengingat potensi terjadinya kejahatan memanfaatkan karakteristik SIM Card diprediksi akan meningkat, maka kajian dan penelitian terkait dengan eksplorasi barang bukti digital berupa SIM Card menjadi sangatlah penting sebagai bagian dari upaya preventif. Penelitian ini akan mencoba untuk melakukan implementasi proses investigasi forensika digital untuk kasus barang bukti SIM Card melalui sebuah studi kasus dan pemanfaatan sejumlah tools yang relevan.

1.2 Review Penelitian

Penelitian umum seputar mobile / cellular forensics antara lain telah dilakukan beberapa peneliti sebelumnya [3][4][5][6]. Karakteristik bukti digital dan implementasi proses forensika pada lingkungan Android dibahas secara lengkap oleh Lee [4]. Sementara itu Thakur et.all [3] membahas secara umum karakteristik jaringan GSM serta potensi kejahatan yang mungkin terjadi beserta dengan solusi pencarian bukti digitalnya melalui beberapa alternative tools. Curran et.all [6] mencoba untuk membuat panduan yang akan menjadi acuan dalam proses forensika untuk mobile phone. Konsep *Proactive Investigation Scheme* dikenalkan oleh Mylonas et al. [5] sebagai sebuah strategi proses investigasi untuk smartphone forensics. Konsep ini adalah sebuah upaya untuk melakukan pengungkapan bukti digital berdasarkan pendekatan aspek legal dari bukti digital yang umumnya terdapat dalam sebuah smartphone.

Penelitian dengan fokus pada SIM Card Forensics antara lain telah dilakukan oleh [7], [8] serta [9]. Dalam hal ini Savoldi [7]mencoba membahas aspek file system dari SIM Card beserta metodologi untuk menemukan bukti digital khususnya untuk katagori hidden file. Sementara Jansen [10] mencoba memetakan sejumlah tools yang dapat digunakan untuk eksplorasi data pada SIM Card. Selain menggunakan tools yang sudah tersedia, salah satu cara untuk melakukan eksplorasi data pada SIM adalah dengan memanfaatkan modul IMP (*Identity Module Programmer*), yaitu sebuah general purpose tools yang dapat digunakan untuk membuat berbagai modul pada SIM Card. Pendekatan XML telah dilakukan oleh Jansen [9] untuk ujicoba eksplorasi data melalui sebuah modul yang dibangun lewat IMP.

Penelitian tentang mobile phone dan atau mobile devices adalah merupakan bagian dari *open problem* dalam bidang forensika digital [11]. Menurut Casey [1], mobile phone / device adalah sebuah sistem dinamis yang menawarkan banyak tantangan dari aspek forensika digital. Selain itu variasi model, vendor, platform OS dan teknologi tidak memungkinkan untuk membangun satu metode / prosedur untuk menangani berbagai aspek dari proses forensika digital mobile phone / devices. Karena itu berbagai variasi kasus dan lingkungan forensika dapat dikembangkan dalam penelitian seputar mobile phone ini. Termasuk didalamnya adalah seputar SIM Card sebagai bagian tak terpisahkan dari sebuah teknologi mobile phone.

2. KONSEP SIM CARD

Menurut Casey [1], SIM Card adalah gabungan dari tiga komponen yaitu : microprocessor, ROM dan RAM. Ketiga komponen tersebut kemudian dikemas menjadi satu kesatuan yang dikenal dengan ICC-ID (*Integrated Circuit Card Identifier*). Identitas ICC_card ini dikenali lewat MCC (*Mobile Country Code*), MNC (*Mobile Network Code*) dan serial number / no kartu. SIM Card digunakan untuk authentifikasi seseorang pengguna dalam sebuah jaringan GSM. Untuk menghubungkan seseorang pada suatu jaringan GSM, maka SIM Card memuat identitas Ki (istilah untuk *authentication key*), PIN (*Personal Identification Number*) dan nomor yang dikenal dengan MSISDN (*Mobile Subscriber ISDN*). Selain itu SIM Card juga memuat kode negara dari provider yang mengeluarkan SIM Card dalam bentuk IMSI (*International Mobile Subscriber Identity*), jalur radio komunikasi dalam bentuk TMSI (*Temporary Mobile Subscriber Identity*) dan area terakhir pengguna dalam bentuk LAI (Location Area Identity). Data TMSI dan LAI sifatnya adalah dinamis tergantung dari posisi terakhir perlengkapan mobilenya digunakan dalam cakupan infrastuktur jaringan telekomunikasi yang digunakan.

SIM Card memiliki banyak model tergantung dari *provider* yang memakai *SIM Card* tersebut, namun karena menggunakan standar ISO/IEC 7810:2003, ID-000 maka hal ini dipastikan *SIM Card* yang menggunakan standar ini semuanya memiliki panjang, lebar, dan ketebalan yang sama, yaitu panjang 25.00 mm, lebar 15.00 mm dan ketebalan 0.76 mm.

Giesecke [12] menyebutkan bahwa pada awalnya ukuran SIM Card adalah sama dengan kartu kredit, namun karena berkembangnya teknologi yang membuat telepon selular semakin kecil maka ukuran *SIM Card*juga menjadi semakin kecil. Bersamaan dengan keluarnya produk iPad dari Apple, generasi ketiga dari *SIM Card*yang dikenal dengan istilah *Micro-SIM*mulai dikenal di masyarakat. Bahkan saat ini sudah mulai muncul generasi ke empat dari SIM Card yang disebut dengan *Nano-SIM* dengan ukuran 12.3 x 8.8 mm. Nano-SIM 30 persen lebih kecil dibanding dengan *Micro-SIM*. Dengan ketebalan 0.7 mm, berkurang 15 persen dari ketebalan *Micro-SIM*.Dalam [12] juga disebutkan bahwa *Nano-SIM* menawarkan keuntungan bagi manufaktur untuk memberikan ruang lebih untuk komponen telepon selular yang lain seperti *memory card* atau baterai yang lebih besar sehingga membutuhkan ruang lebih. Ukuran

*Nano-SIM*yang lebih kecil juga memberikan dampak lahirnya produk - produk telepon selular / smartphone yang lebih tipis.

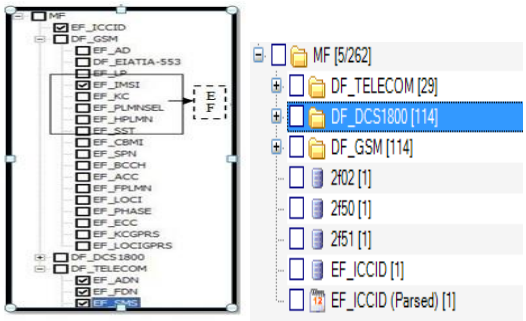
3. KONSEP BUKTI DIGITAL PADA SIM CARD

Salah satu faktor penting dalam proses investigasi adalah hal terkait dengan barang bukti. Dalam hal ini terdapat dua istilah yang hampir sama, yaitu barang bukti elektronik dan barang bukti digital. Barang bukti elektronik adalah bersifat fisik dan dapat dikenali secara visual (komputer, handphone, camera, CD, harddisk dll) sementara barang bukti digital adalah barang bukti yang diekstrak atau di-recover dari barang bukti elektronik (file, email, sms, image, video, log, text). Salah satu definisi sederhana dari bukti digital :*any information of probative value that is either stored or transmitted in digital form*.[1]

Untuk konteks mobile phone / smart phone, Casey[1] membuat tabel yang memuat beberapa hal yang berpotensi menjadi barang bukti digital, antara lain adalah : IMEI, Address book, SMS, Calender, memo, to-do list, call register, photo, movie, maps, MMS, GPS, email, history browser, back up, tethering / wifi history, call register, SMS. Secara khusus Mylonas [5] membagi jenis barang bukti yang ada pada perangkat telepon selular menjadi 7 katagori, yaitu : a) *Messaging Data*, yaitu konten dan metadatanya, b) *Device data*, yaitu data yang tersimpan pada storage media yang tidak terkait dengan aplikasi tertentu (misalnya file multimedia), c) *SIM Card Data*, adalah data yang berhubungan langsung dengan identitas SIM, d) *Usage History Data*, yaitu data seputar logs pengguna (misalnya call logs, browsing history), e) *Application Data*, yaitu data permanen atau temporal yang digunakan selama eksekusi aplikasi (misalnya file database), f) *Sensor Data*, yaitu data yang dihasilkan peralatan sensor yang umumnya dimiliki oleh *device* seperti camera, microphone, GPS, *motion sensors* (accelerometer, gyroscope), atau *environment sensors* (magnetometer, proximity, light, temperature, dan g) *User Input Data* yaitu data yang dihasilkan dari input keyboard atau gestures, yang diproses secara fly dan tersimpan dalam *keyboard cache*.

Untuk memahami letak-letak penyimpanan file digital pada SIM Card maka salah satunya adalah memahami konsep sistem file pada SIM Card. Pada prinsipnya sistem file pada SIM Card tersusun dalam suatu struktur hirarki pohon dengan 3 tipe *file* , yaitu: *Master File (MF), Dedicated File (DF), dan Elementary File (EF).*Setiap file yang tersimpan diberikan alamat unik berukuran dua byte hexadecimal, yaitu : 3F untuk master file (MF), 7F untuk dedicated file (DF), 2F untuk elementary file dibawah master file dan 6F untuk elementary file dibawah dedicated file. Beberapa alamat spesifik yang umum adalah 3F00:7F10, yaitu directory DFTELECOM yang memuat informasi terkait dengan layanan system serta data-data yang hasilkan oleh pengguna seperti pesan SMS dan nomor panggilan terakhir. Alamat lainnya adalah 3F00:7F20 untuk directory bernama DFGSM yang memuat informasi jaringan telekomunikasi yang digunakan. Alamat 3F00:2FE2 diberi nama EFICCID yang memuat identitas ICC-ID dan alamat 3F00:7F20:6F07 diberi nama EFIMSI yang memuat data IMSI.

Standar *GSM (Global System for Mobile communication)* membagi beberapa *Dedicated File* yang penting di bawah *Master File* yaitu : *DFGSM*, *DFDCS1800* dan *DFTELECOM*. Untuk file MF dan DF, hanya beberapa EF yang didefinisikan. EF yang berada dibawah DFGSM dan DFDCS1800, mengandung informasi yang terkait dengan jaringan informasi masing-masing untuk GSM 900 MHz dan pengoperasian band *Digital Selular System* (DCS) 1800. Sedangkan pada EF yang berada di bawah DF TELECOM berisikan tentang informasi yang berhubungan dengan *service.*



Gambar 1 Hirarki File pada SIM Card

Menurut Savoldi [7] perbedaan utama dari kedua tipe file (Dedicated File & Elementary File) adalah DF hanya berisi data *Header*, sedangkan file EF berisikan *Header* dan *Body*. *Header* berisi semua informasi yang menghubungkan file dangan struktur dari sistem (sisa kapasitas dibawah DF, jumlah dari EF, dll) dan informasi tentang keamanan (hak akses dari sebuah file). Pada *Body* berisikan informasi yang berhubungan dengan aplikasi untuk kartu yang telah diterbitkan. Terdapat tiga tipe dari EF, adalah :

- Transparent EF : file-file ini diatur sebagai urutan *byte*. dan memungkinkan untuk membaca semua atau hanya sebagian dari isinya dengan menentukan nomer intervalnya.
- Liner Fixed EF : unit kecil yang berada pada bagian *body* tidak disebut dengan *byte* melainkan disebut *record*. Sebuah *Record* adalah kumpulan *Byte*, setiap *record* dari berkas yang sama mewakili jenis informasi yang sama. Pada *Linear-Fixed EF*, semua *record* memliki panjang yang sama.
- Cyclic EF : berkas-berkas ini dimana *record* di susun dalam bentuk melingkar, dan konsep yang sebelumnya berupa pertama dan akhir di ganti menjadi sebelumnya dan setelahnya.

Sementara itu menurut[10], bukti digital dari *SIM* terletak pada tipe file *EF*. Beberapa bukti digital yang terdapat pada tipe *File EF* adalah:

- LOCI - Location Information
- ICCID - Serial Number
- IMSI –Subscriber ID
- MSISDN – Phone Number
- SMS – The Text Messages
- ADN – Short Dialled Numbers
- LND – Last Dialled Numbers

Untuk dapat melakukan eksplorasi data pada SIM card maka SIM Card harus dilepaskan dari telepon selularnya kemudian dibaca terpisah menggunakan alat *SIM Card READER*. SIM Card Reader dapat mengakses sejumlah data pada SIM Card dengan bantuan perangkat lunak yang spesifik untuk itu, diantaranya adalah Sim Card Seizure & MOBILedit. Karakteristik dari kedua tools tersebut adalah :

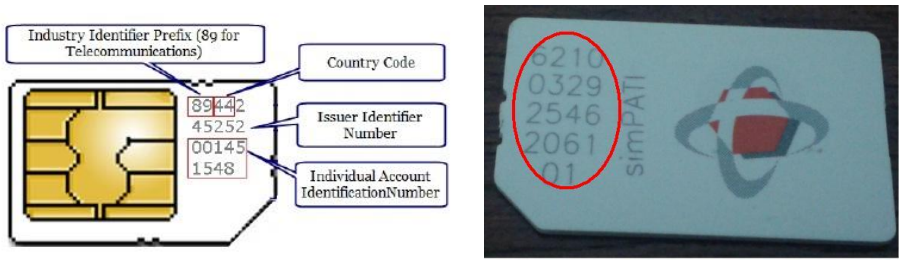
- Sim Card Seizure. *Software forensic* khusus yang di desain untuk mengumpulkan data digital seperti nomer, alamat, tanggal, waktu tanpa mempengaruhi integritas dari kartu sim itu sendiri. Sim card seizure ini juga dapat di gunakan untuk melihat MF dan EF dari sebuah kartu sim yang menyimpan banyak informasi, seperti IMSI, LOCI, dll.
- *MOBILedit* merupakan *software forensic* khusus di buat untuk mengumpulkan data digital dari beberapa *device.* Pengambilan data *SIM Card* merupakan salah satu fitur yang dimiliki oleh *software* ini. *Software* ini juga dapat melihat *IMSI, ICCID, LAI, SMS, LND, AND, Own Numbers*, dan *FDN*.

4. DESAIN PENELITIAN

Untuk mengetahui lebih mendalam tentang karakteristik data dan bukti digital pada SIM Card, teknik *imaging*, *collecting* dan analisis data pada SIM Card maka diterapkan sebuah aktifitas forensika digital dalam sebuah simulasi kasus. Pada simulasi ini diasumsikan telah terjadi pencurian handphone dan duplikasi SIM Card oleh si pelaku. Selanjutnya untuk mengecoh penyidik maka handphone dan SIM Card asli diletakkan pada satu tempat dan SIM Card hasil *cloning* diaktifkan pada lokasi lain. Melalui SIM Card *cloning* inilah di pelaku melakukan sejumlah tindak kejahatan. Selanjutnya diasumsikan si pelaku dapat ditangkap dan ditemukan dua barang bukti, satu adalah handphone dan SIM Card yang asli dan yang lain adalah handphone dan SIM Card hasil *cloning*. Penyidik diminta untuk melakukan eksplorasi data-data pada SIM Card yang akan akan mendukung upaya pembuktian atas tindak kejahatan yang telah dilakukan. Tahap selanjutnya adalah upaya untuk melakukan proses *imaging* dari SIM Card hasil *cloning* menggunakan bantuan *Card Reader* dan aplikasi SIMCard Seizure dari Paraben. Hasil i*maging* kemudian dilakukan analisis untuk menemukan potensi bukti-bukti digital pada SIM Card. Selain menampilkan sejumlah data hasil analisis, output dari penelitian ini adalah didapatnya gambaran prosedur untuk proses forensika digital pada SIM Card.

5. HASIL DAN ANALISIS

Pada tahap awal, semua barang bukti yang ditemukan akan dikumpulkan. Pada skenario ini, SIM Card yang ada pada handphone dijadikan sebagai salah satu barang bukti.Langkah selanjutnya adalah mengenali terlebih dahulu fisik dari SIM Card yang menjadi barang bukti. Dalam hal ini pada bagian belakang *SIM Card* terdapat nomor ICCID. Nomor ICCID tersebut adalah kumpulan dari berbagai nomor yang berfungsi untuk mengidentifikasi bagian sendiri-sendiri**.**Dua digital awal adalah *Industry Identifier Prefix*, yaitu nomor identifikasi yang khusus untuk bagian telekomunikasi, 2 digit setelahnya adalah kode negara, 6 digit setelahnya adalah nomor operator yang mengeluarkan *SIM Card* tersebut, kemudian 9 digit setelahnya adalah nomor identifikasi kartu itu sendiri.Pada kartu yang dijadikan contoh pada penelitian ini, 2 digit awal adalah kode Negara Indonesia yaitu 62, lalu 6 digit setelahnya adalah kode operator yaitu 100329, kemudian 9 digit setelahnya adalah nomor identifikasi dari kartu itu sendiri yaitu 2546206101.

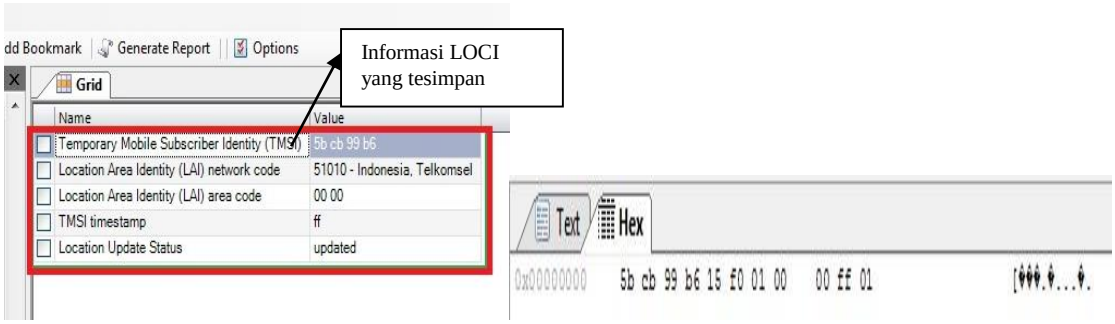


Gambar 2 Nomor ICCID Fisik SIM Card

Langkah selanjutnya sebelum melakukan analisis adalah melakukan *cloning* dari SIM Card itu sendiri. Terdapat beberapa cara untuk melakukan *cloning* dari *SIM Card*, diantaranya adalah menggunakan produk Paraben Corp yaitu *Device Seizure*, atau *SIMMAX USB GSM SIM Card Cloner*. Proses*Cloning* SIM Card akan berhasil bila digunakan software dan hardware yang mendukung. Selain itu, diperlukan pula SIM Card kosong yang berfungsi untuk menyimpan hasil *Cloning* dari SIM Card. Pada penelitian ini, untuk kepentingan *Cloning* SIM Card digunakan *Device Seizure*.*Tool* ini dipilih karena memiliki spesifikasi yang cukup untuk melakukan *cloning* dan ketersediaannya di Indonesia melalui *reseller*.

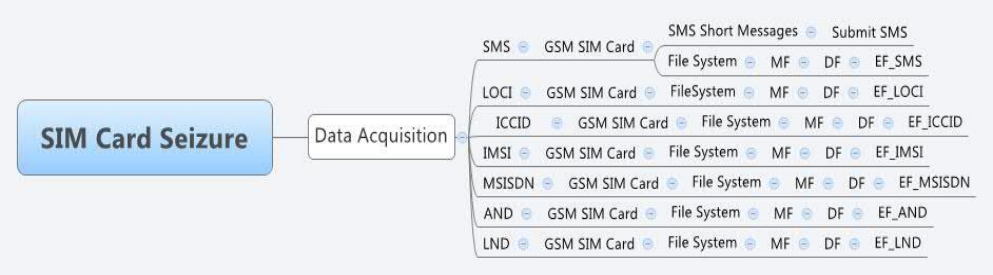
Langkah berikutnya adalah melakukan analisis data untuk proses pencarian bukti-bukti digital. Dalam hal ini bukti digital yang didahulukan adalah bukti-bukti yang memuat aktivitas dari SIM Card melalui identifikasi data pada bagian LOCI (Location Information), ICCID (Serial Number), IMSI (Subscriber ID), MSISDN (Phone Number), SMS (Text Message), AND (Dialled Numbers), LND(Last Dialled Number). Pada prinsipnya tools yang digunakan telah secara sistematis memfasilitasi investigator untuk dapat dengan mudah menemukan data-data yang diperlukan melalui pilihan sejumlah menu. Sebagai contoh untuk mengetahui informasi LOCI didapat dengan memilih salah satu sub menu sehingga akan muncul informasi sebagaimana pada Gambar 6. Selain melalui sub menu, informasi LOCI dapat pula diketahui melalui informasi heksa yang tersedia.

Pada Gambar 3 dapat diketahui bahwa *Temporary Mobile Subscriber Identity(TMSI)* adalah 5b cb 99 b6, Location Area Identity 51010 – Indonesia, Telkomsel, maksudnya adalah kode lokasi saat telepon genggam pelaku dalam keadaan hidup adalah 51010, pada negara Indonesia. Cara lain adalah mengenali LOCI dari informasi hex dari EF_LOCI , yaitu 5b cb 99 b6 15 f0 01 00 00 ff 01



Gambar 3. Informasi LOCI dalam bentuk Tabel dan Heksa

Hal yang sama juga dapat dengan mudah dilakukan untuk mengetahui informasi ICCID (Serial Number), IMSI (Subscriber ID), MSISDN (Phone Number), SMS (Text Message), AND (Dialled Numbers), LND(Last Dialled Number). Dengan demikian gambaran umum dari proses pencarian bukti digital pada SIM Card menggunakan Sim Card Seizure dapat dirangkum sebagaimana pada Gambar 4.



Gambar 4. Bagan penggunaan SIM Card Seizure

6. SIMPULAN DAN SARAN

6.1 Simpulan

SIM Card merupakan sebuah perangkat komunikasi yang sangat di butuhkan di era digital ini. Dibalik perannya sebagai media komunikasi, *SIM Card* ternyatajuga berpotensi untuk menyimpan barang bukti pada suatu kasus kejahatan atau bahkan *SIM Card* tersebut adalah juga berfungsi sebagai alat kejahatan. Pada penelitian ini telah dilakukan sejumlah langkah serta ekplorasi terhadap SIM Card menggunakan SIM Card Seizure. Analisis dilakukan untuk mengetahui beberapa karakteristik data digital yang dapat disimpan dalam SIM Card serta teknik untuk melakukan analisisnya. Untuk barang bukti SIM Card, data digital standar yang dapat dijadikan sebagai inisiasi proses investigasi adalah pada informasi ICCID (Serial Number), IMSI (Subscriber ID), MSISDN (Phone Number), SMS (Text Message), AND (Dialled Numbers) dan LND(Last Dialled Number). Informasi tersebut dapat dilihat dengan mengenali karakteristik struktur file dan nilai heksa decimal pada SIM Card yang terbagi menjadi *Master File (MF), Dedicated File (DF),* dan *Elementary File (EF).* Bagan yang dihasilkan dari penelitian ini dapat dijadikan sebagai panduan danpengetahuan praktis bagi investigator digital untuk mengungkapkan kasus-kasus kejahatan yang melibatkan barang bukti SIM Card.

6.2 Saran

Mengingat keterbatasan yang di miliki, maka untuk penelitian berikutnya yang dapat dilakukan adalah memperluas studi kasus sehingga semua potensi bukti digital pada telepon selular dan SIM Card dapat dianalisis bersamaan. Sementara khusus untuk mengenali lebih lanjut karakteristik SIM Card, penelitian berikutnya dapat diarahkan pada eksplorasi IMP (*Identity Module Programmer*) pada SIM Card sebagai cara lain untuk melakukan eksplorasi data digital.

DAFTAR PUSTAKA

[1] E. Casey and B. Turnbull, "Digital Evidence on Mobile Devices," in *Digital Evidence and Computer Crime*, Third Edition., Elsevier Inc., 2011.

[2] "Prospective Analysis On Trend In Cybercrime From 2011 to 2020," National Gendarmerie, France.

[3] R. S. Thakur, K. Chourasia, and B. Singh, "Cellular Phone Forensics," *Int. J. Sci. Res. Publ.*, vol. 2, no. 8, 2012.

[4] X. Lee, C. Yang, S. Chen, and J. Wu, "Design and Implementation of Forensic System in Android Smart Phone," presented at the JWIS, 2010.

[5] A. Mylonas, V. Meletiadis, and B. Tsoumas, "Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition," *IFIP Adv. Inf. Commun. Technol.*, vol. 376, pp. 249–260, 2012.

[6] K. Curran, A. Robinson, and S. Peacocke, "Mobile Phone Forensic Analysis," *Int. J. Digit. Crime Forensics*, vol. 2, no. 2, May 2010.

[7] A. Savoldi and P. Gubian, "SIM and USIM Filesystem: a Forensics Perspective," presented at the SAC, Seoul Korea, 2007.

[8] Wayne Jansen and R. Ayers, "Forensic Software Tools for Cell Phone Subscriber Identity Modules," presented at the Conference on Digital Forensics, Association of Digital Forensics, Security, and Law (ADFSL), Las Vegas Nevada USA, 2006.

[9] W. A. Jansen and A. Delaitre, "Reference Material For Assesing Forensics SIM Tools," NIST, NIST IR-7617, Oct. 2009.

[10] W. Jansen and R. Ayers, "Guidelines on Cell Phone Forensics," National Institute Of Standard and Technology Department Of Commerce USA, 800-101, May 2007.

[11] S. Garfinkel, "Digital Forensics Research: The Next 10 Years," 2010, vol. 7, pp. 64–73.

[12] Giesecke & Devrient, "Giesecke & Devrient: Creating Confidence.," 2012. [Online]. Available: http://www.gi-de.com/en/index.jsp. [Accessed: 25-Feb-2013].