IDENTIFIKASI BUKTI DIGITAL PADA SIM CARD UNTUK MOBILE FORENSIC

DIGITAL EVIDENCE IDENTIFICATION ON SIM CARD FOR MOBILE FORENSIC

Agung Prasetiyo
Prodi S1 Teknik Informatika, Fakultas Teknik, Universitas Telkom
prasetiyoagung00@gmail.com

Abstrak

Sekarang ini, mobile phone sering digunakan dalam kehidupan sehari-hari. Perangkat ini seringkali terlibat dalam kejahatan. Hal tersebut memungkinkan terdapatnya bukti yang dapat menjadi petunjuk terjadinya kejahatan. Karena itu forensik digital pada mobile phone menjadi hal yang penting mengingat semakin banyaknya mobile phone yang digunakan di berbagai tempat kejadian perkara.

Penelitian ini akan melakukan kegiatan forensik yang berfokus pada identifikasi kartu SIM. Penelitian ini melibatkan kegiatan validasi, grouping, analisis timeframe, dan analisis kepemilikan. Investigasi lanjut terhadap kartu SIM ini diharapkan akan membantu proses penyelidikan.

Hasil akuisisi memperlihatkan ada cukup banyak bukti yang bisa didapat. Namun ternyata ada juga jenis bukti yang tidak dapat diambil dari SIM Card sebagaimana disebut dalam daftar jenis bukti potensial yang mungkin didapat dari SIM Card. Berdasarkan hasil grouping dari daftar bukti digital potensial, SMS dan LDN merupakan dua jenis bukti potensial tertinggi yang didapat.
Kata kunci: forensik selular, kartu SIM, bukti digital.

Abstract

Nowadays, mobile phones are often used in everyday life. These devices are often involved in crime. It allows the presence of evidence that can be a clue crime in the mobile phone. Because it is digital forensics on the phone becomes important considering the increasing number of mobile phones that are found in various crime scenes.

This research will implement forensic activities that focus on the identification of the SIM card. This research involves the validation activities, grouping, timeframe analysis, and ownership analysis. Further investigation of the SIM card is expected to help the process of investigation.

Acquisition results showed there was quite a lot of evidence that can be obtained. But there was also the kind of evidence that can not be taken from the SIM Card as mentioned in the list of potential types of evidence which may be obtained from the SIM Card. Based on the results of grouping of the list of potential digital evidence, SMS and LDN are the two types of evidence which has highest potential.
Keyword: mobile phone forensic, SIM card, digital evidence.

1. Pendahuluan

Kartu SIM (*Subscriber Identity Module*) merupakan salah satu elemen terpenting yang terselip di dalam *mobile phone* berbentuk kartu kecil berupa lempeng tembaga yang disajikan oleh penyedia layanan GSM atau CDMA. Kartu ini menyimpan informasi yang berkaitan dengan jaringan yang digunakan untuk *authentification* pengguna. Fungsi utamanya adalah menyimpan informasi sekaligus memudahkan penyedia layanan jaringan untuk mengidentifikasi pemilik kartu SIM.

Dalam penelitian ini, akan dilakukan pengujian terhadap kartu SIM. Kartu SIM yang akan digunakan adalah kartu SIM dengan teknologi GSM, yaitu kartu Simpati dari Telkomsel dan kartu Tri dari PT Hutchison CP Telecommunications. Masalah yang muncul mencakup bukti digital seperti apa yang bisa didapat dari kartu SIM dan juga bagaimana menentukan data sebagai sesuatu yang berpotensi sebagai bukti digital. Dalam forensik, untuk bisa mendapatkan bukti, segalanya sebaiknya dilakukan berdasarkan prosedur atau mengikuti model proses dalam identifikasi. Dalam penelitian ini, akan dibuat sebuah model proses untuk melakukan identifikasi kartu SIM. Dari situ kemudian akan ditelusuri bukti digital yang dapat diambil dari sebuah kartu SIM.

2. Dasar Teori

2.1. Contoh Bukti Digital

Pada kartu SIM, bukti digital potensial akan dibagi menjadi dua jenis, yaitu jenis bukti potensial yang dapat dikenali secara langsung, dan jenis bukti potensial yang dikenali secara tidak langsung karena harus melibatkan beberapa tahap. Ada cukup banyak bukti digital yang dapat ditemukan dalam kartu SIM. Namun untuk lebih ringkasnya, akan dijelaskan beberapa bukti potensial seperti berikut. [1] [2]

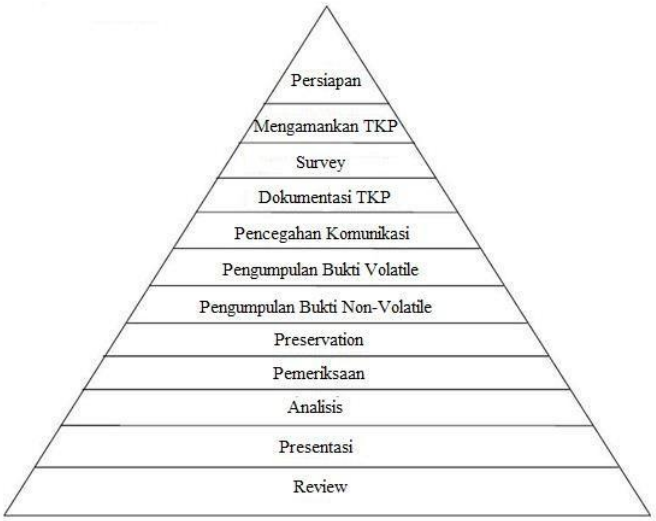
- ICCID (*Integrated Circuit Card Identifier*) adalah angka unik pengenal untuk karti SIM yang dapat memiliki panjang mencapai 20 digit.

- IMSI (*International Mobile Subscriber Identity*) merupakan angka unik sepanjang 15 digit yang diberikan kepada pelanggan. Angka ini memiliki struktur yang mirip dengan ICCID dan terdiri dari MCC, MNC, dan MSIN.
- MCC (*Mobile Country Code*) merupakan 2 atau 3 digit pertama pada IMSI untuk yang mewakili kode negara. Seperti nomor ―302‖ yang mengacu pada Kanada atau ―510‖ yang mengacu pada Indonesia.
- *Country Code / International Direct Dialing (IDD)* merupakan 2 atau 3 digit yang terdapat pada ICCID atau digit pertama pada MSISDN. Berdasarkan kode yang didefinisikan oleh ITU-T rekomendasi E.123 dan E.164 *country code* untuk negara Indonesia adalah 62 atau juga dapat ditulis sebagai +62.
- MNC (*Mobile Network Code*) merupakan digit berikutnya yang digunakan operator. Maksimal digit untuk kode ini adalah 3 digit. Standar untuk negara Eropa adalah 2 digit, sementara untuk Amerika 3 digit.
- MSIN (*Mobile Subscriber Identification Number*) merupakan sisa digit terakhir dalam IMSI setelah MNC. Biasanya jumlah nya akan ada 10 digit, tapi bisa menjadi lebih kecil lagi untuk kasus di negara di mana kode MNC nya terdapat 3 digit.
- ADN (*Abbreviated Dialing Number*), yaitu nomor dan nama yang dipanggil oleh pelanggan disimpan oleh ADN. Fungsi ini bekerja pada nomor-nomor yang biasanya dipanggil oleh pelanggan.
- SMS (*Short Message Service*) merupakan layanan untuk mengirim dan menerima pesan singkat. Atribut dari SMS berisikan informasi lain selain teks itu sendiri, seperti waktu SMS datang, juga waktu SMS terkirim, pengirim atau penerima SMS, alamat SMS center, dan status pengiriman.
- LDN *(Last Dialled Number*) berisikan nomor yang paling terakhir dipanggil oleh pelanggan. Nomor dan nama yang terkait dengan nomor tersebut tersimpan dalam sini.
- FDN *(Fixed Dialled Number)* mirip dengan ADN karena melibatkan nama dan nomor kontak. FDN memiliki cara kerja dengan fungsi ini yang membuat pengguna tidak harus melakukan panggilan dengan menekan seluruh nomor telepon yang dituju; tetapi hanya dengan menahan salah satu tombol pada telepon seluler, mereka dapat mengakses nomor pada kontak.
- TMSI *(Temporary Mobile Subscriber Identity)* adalah identitas yang paling sering dikirim antara ponsel dan jaringan. TMSI secara acak ditugaskan oleh VLR (Visitor Location Register) –sebuah *database* dari pelanggan– ke setiap ponsel di lokasi tersebut saat ponsel itu menyala. TMSI ini diperbarui setiap kali ponsel berpindah tempat.

2.2. Gambaran Umum Model Proses

2.2.1. Model Proses Windows Mobile Forensic

Ada banyak model forensik digital yang diusulkan di berbagai belahan dunia. Namun tidak ada kesimpulan yang telah dicapai sebagai salah satu yang paling tepat. Anup Ramabhradan telah mengusulkan model yang berfokus pada arus informasi terkait dengan penyelidikan forensik pada ponsel Windows [3].



Gambar 1 Model Proses Windows Mobile

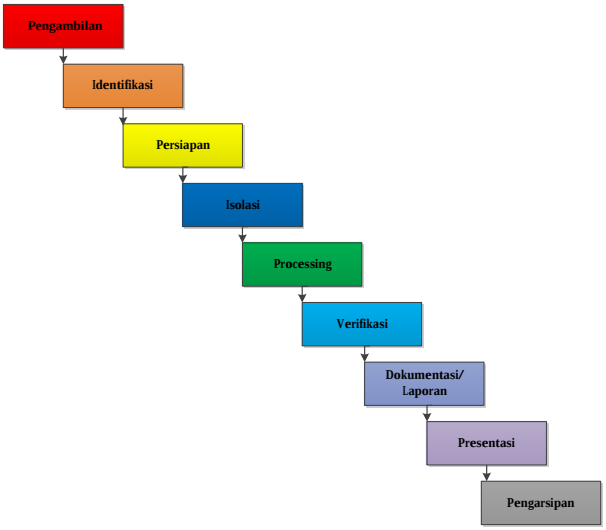
Berdasarkan tulisan yang ditulis Anup dalam pengembangan modelnya [3], terdapat 12 tahap yaitu:

- Persiapan, tahap ini melibatkan pemahaman awal dari kasus kejahatan dan aktivitas seperti persiapan *tools* yang dibutuhkan dan lainnya.
- Mengamankan TKP, tahap ini biasanya berurusan dengan mengamankan TKP dari pihak yang tidak berwenang. Tahap ini membutuhkan protokol formal. Para penyelidik harus mengidentifikasi ruang lingkup kejahatan dan mendirikan garis lingkaran pembatas.

- Survey dan pengenalan, tahap ini melibatkan survey awal yang dilakukan oleh para penyelidik untuk mengevaluasi TKP dan mengidentifikasi sumber-sumber bukti potensial. Dokumentasi TKP
- Dokumentasi TKP, tahap ini melibatkan dokumentasi yang tepat dari TKP termasuk dengan melakukan pemotretan.
- Pencegahan komunikasi, tahap ini terjadi sebelum pengumpulan bukti. Pada tahap ini, semua kemungkinan komunikasi yang dapat dilakukan sebaiknya diblokir.
- Pengumpulan bukti *volatile*, sebagian besar dari bukti yang melibatkan *mobile device* merupakan jenis *volatile*, ditunjukkan dalam RAM. Beberapa contoh *volatile evidence* adalah RAM dan *internal memory*.
- Pengumpulan bukti *non-volatile*, tahap ini melibatkan pengumpulan bukti dari media penyimpanan eksternal seperti MMC, *compact flash, memory sticks, SD memory, micro SD*. *Forensic tool* yang tepat harus digunakan untuk mengumpulkan untuk memastikan diterimanya dalam pengadilan.
- *Preservation*, tahap ini menyangkut bagaimana membungkus, mengangkut, dan menyimpan barang bukti. Prosedur yang baik sebaiknya diikuti dan didokumentasi untuk memastikan barang elektronik yang dikumpulkan tidak mengalami perubahan atau kerusakan.
- Pemeriksaan, tahap ini melibatkan pemeriksaan isi dari barang bukti yang dikumpulkan oleh para spesialis forensik.
- Analisis, tahap ini lebih ke arah teknis seperti melakukan identifikasi hubungan antara bagian data, menganalisa data yang disembunyikan dan lainnya berdasarkan informasi yang dilakukan pada tahap pemeriksaan, merupakan aktivitas yang yang harus dilakukan dalam tahap ini.
- Presentasi, setelah melakukan analisis atas barang bukti yang berhasil dikumpulkan, hasilnya mungkin akan dibutuhkan di depan para penyelidik lainnya, termasuk *technical experts*.
- *Review*, tahap terakhir pada model ini adalah *review*. Tahap ini melibatkan ulasan dari tahap awal sampai akhir. Hasilnya dapat digunakan untuk penyelidikan berikutnya.

2.2.2. Model Proses Mobile Phone

Selama beberapa tahun terakhir, pemeriksa forensik digital telah melihat peningkatan yang luar biasa dalam permintaan untuk memeriksa data dari telepon seluler dan perangkat *mobile* lainnya. Det.A.Cynthia dalam tulisannya tentang pengembangan model proses untuk *mobile phone* menggambarkan model prosesnya dalam 9 tahap sebagai berikut [4].



Gambar 2 Model Proses Mobile Phone [4]

Penjelasan untuk 9 tahap tersebut yaitu:

- Pengambilan, yaitu tahap pengambilan bukti yang melibatkan prosedur yang meminta untuk pemeriksaan agar ditangani dengan baik. Tahap ini umumnya memerlukan formulir permintaan, informasi kepemilikan dan lainnya.
- Identifikasi, dimana pemeriksa sebaiknya mengidentifikasi hal seperti otoritas hukum, tujuan pemeriksaan, pembuatan model, tempat penyimpanan data, dan sumber bukti potensial lainnya.
- Persiapan, melibatkan persiapan signifikan untuk pemeriksaan *mobile phone*. *Tools* yang tepat dibutuhkan selama persiapan dan pemeriksaan untuk memastikan seluruh barang telah diperiksa dengan tepat.
- Isolasi, yang dapat dicapai melalui penggunaan *Faraday bag* atau atau kain pelindung yang didesain secara spesifik untuk tujuan ini.
- *Processing*, tahap yang dilakukan setelah *cell phone* diisolasi dari jaringan. *Tools* yang tepat digunakan untuk mengekstrak data yang diinginkan dari *mobile device.*

- Verifikasi, dapat ditempuh dalam beberapa cara, yaitu membandingkan data yang diekstrak dengan *handset*, mengecek *underlying hex*, atau menggunakan lebih dari satu jenis *tools*.
- Dokumentasi/laporan, dapat mencakup informasi seperti waktu pemeriksaan dilakukan, kondisi fisik *handset*, foto dari *handset*, status *handset*, *tools* yang digunakan, dan data yang diperiksa.
- Presentasi, yaitu pertimbangan yang diberikan selama pemeriksaan sebagaimana informasi yang diekstrak dan dikomentasikan dari *mobile device* dapat dengan jelas ditunjukkan ke penyelidik lain, atau bahkan ke pengadilan.
- Pengarsipan, yaitu pemeliharaan dari data yang diekstrak dan didokumentasikan dari *mobile device* adalah bagian penting dari keseluruhan proses. Hal ini diperlukan untuk mempertahankan data dalam format yang dapat digunakan saat proses pengadilan, referensi tingkat lanjut, dan untuk kebutuhan arsip.

2.3. Identifikasi Bukti Digital Potensial

Beberapa manufaktur ponsel biasanya menawarkan fitur untuk menangani kumpulan informasi seperti aplikasi Personal Information Management (PIM), fitur pengiriman pesan, *e-mail*, dan juga *Web browsing*. Dengan latar belakang kejadian, pemeriksa dan analis forensik dapat melanjutkan identifikasi dengan melakukan hal sebagai berikut [5]:

- Mengumpulkan informasi tentang individu yang yang terlibat {*who*}
- Menentukan jenis peristiwa yang sebenarnya terjadi {*what*}
- Membangun timeline kejadian {*when*}
- Mengupas informasi yang menjelaskan alasan {*why*}
- Mengupas informasi yang menjelaskan lokasi {*where*}

Mengetahui jenis *tools*, aplikasi, atau fitur yang digunakan {*how*}.

2.4. Karakteristik SIM

SIM Card sebagai bagian terpisah dari *mobile phone* secara teori dapat menyimpan berbagai macam data. Kartu GSM memuat sebuah prosesor dan memori non volatile. Tujuan utama adanya prosesor adalah untuk melakukan implementasi mekanisme akses dan fitur keamanan [6].

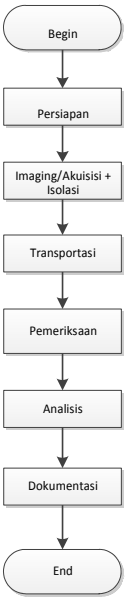
Ukuran kartu SIM secara umum ditetapkan memiliki 2 jenis ukuran. Yang pertama adalah ukuran lebih besar mengacu pada standar ISO 7816. Namun karena menggunakan standar ISO/IEC 7810:2003, maka kartu SIM yang paling sering digunakan sekarang adalah yang berukuran 25mm x 15mm dengan bentuk trapesium sejajar dan memiliki ketebalan 0.76mm. [8]

3. Perancangan dan Pengujian

3.1. Model Proses yang Digunakan

Berdasarkan kedua model proses secara khusus, sekarang akan dibangun sebuah gambaran model proses untuk pemeriksaan kartu SIM. Model proses ini dibangun sejak tahap pengumpulan bukti.

Kemudian ini adalah model proses yang akan ditawarkan dengan fokus pada SIM card yang masih terpasang pada *mobile phone*:



Gambar 3 Model Proses yang Ditawarkan Untuk Identifikasi SIM Card

Penjelasan langkah-langkah pada model proses tersebut yaitu:

- Persiapan, yaitu tahap untuk menyiapkan *tools* yang dibutuhkan untuk melakukan pemeriksaan. Perangkat keras yang biasanya dibutuhkan adalah *SIM Card Reader,* kabel data, dan satu unit komputer. Sementara *software* yang biasanya dibutuhkan untuk pemeriksaan adalah SIM Seizure, MobilEdit, dan XL App.
- Isolasi dapat dilakukan dengan mengubah *handset* ke mode *airplane* atau meletakkan *handset* ke dalam tas Faraday.
- *Imaging*,yaitu tahap yang dilakukan hanya saat terjadi keraguan karena daya baterai lemah saat pertama kali ditemukan di TKP. Tahap ini dilakukan bersamaan dengan *imaging* pada *volatile evidence* atau *mobile device* tempat kartu SIM itu dipasang.
- Akuisisi, yaitu tahap yang melibatkan pengambilan data di dalam *handset,* kartu SIM dan pemeriksaan bukti biologis seperti misalnya sidik jari yang tertinggal di dalam kartu SIM dan juga *handset*.
- Transportasi, yaitu mengemas barang bukti dalam bungkus yang diberi label. Bungkusan tersebut kemudian dimasukkan ke dalam tas Faraday atau kontainer yang dapat menangkal gelombang radio.
- Pemeriksaan dilakukan setelah akuisisi dilakukan. Langkah pertama adalah dengan melakukan validasi yaitu dengan cara membandingkan hasil akuisisi dari beberapa *tools*. Setelah data terbukti konsisten, hal berikutnya yang akan dilakukan adalah dengan melakukan identifikasi dari data tersebut.
- Analisis, tahap ini lebih ke arah teknis seperti melakukan identifikasi hubungan antara bagian data, menganalisa data yang diambil dari *image* atau dari hasil akuisisi.
- Dokumentasi dilakukan untuk mencatat hasil analisis. Dokumen ini berisi informasi dasar seperti nama penyelidik, tanggal, serta lama pengerjaan. Dokumen ini juga berisi hasil analisis secara detail lengkap dengan *copy* rekaman data yang ditemukan.

3.2. Pengujian Akuisisi

Tahap akuisisi menitikberatkan pada data yang akan diambil dari kartu SIM. Akuisisi akan dilakukan dengan menggunakan *tools* SIMSeizure dari Paraben dan MobilEDIT. Kemudian akan dilakukan analisis terhadap data yang telah dikumpulkan. Analisis dilakukan untuk menentukan data mana yang memiliki potensi untuk dijadikan bukti digital. Analisis juga dilakukan untuk menentukan cara untuk menentukan bukti digital.

4. Implementasi dan Analisis

4.1. Akuisisi

Beberapa bukti digital dari hasil akuisisi yang dapat diraih diantaranya adalah ICCID, ADN, FDN, dan IMSI. Penjelasan mengenai beberapa bukti digital tersebut adalah sebagai berikut:

4.1.1. ICCID

ICCID memiliki format tiga jenis angka yang digabung. Format angka tersebut dapat dituliskan sebagai 89 62 10020254403868, dengan uraian 89 merujuk pada industri telekomunikasi; 62 merujuk pada *country calling code*; 10 merujuk pada MNC; dan 0020254403868 merujuk pada nomor pengenal individu.

Jadi pada ICCID pada kartu SIM ini menunjukkan bahwa kartu SIM ini dikeluarkan di negara Indonesia, dilihat dari *country calling code* nya. Dan jika dilihat dari MNC nya, kartu ini dikeluarkan oleh PT Telekomunikasi Selular. Nomor pengenal individu dapat digunakan untuk melacak kepemilikan dari kartu SIM tersebut.

4.1.2. ADN

Informasi tentang nomor yang tersimpan di dalam SIM:

Tabel 4.1 ADN

Record Number	Name	Phone
1	3 Care	123
2	Bill & TopUp	111
3	Planet 3	333
4	Say It	789
5	Andi	+6282116610308
6	Bos Wahyu	+6289675012221
7	Denny	0812229011888
8	Toro	081384655865

Informasi pada tabel di atas menunjukkan nomor-nomor yang tersimpan di dalam kartu SIM yang telah disederhanakan (ADN). Terdapat total delapan nomor yang tersimpan dengan data binari sebanyak 200 buah. ADN sebenarnya adalah nomor kontak yang tersimpan di dalam kartu SIM. Dalam kartu SIM ini, terdapat lebih dari delapan nomor kontak yang dapat diambil.

4.1.3. IMSI

Sedangkan pada gambar 7 di bawah ini merupakan IMSI. Angka yang ditunjukkan pada IMSI adalah 510 10 2025440386, dengan format sebagai berikut:
510 merujuk pada MCC, artinya kartu SIM tersebut berada di negara Indonesia
10 merujuk pada MNC, artinya kartu SIM tersebut diedarkan oleh penyedia layanan PT Telekomunikasi Seluler.
2025440386 merujuk pada MSIN, yaitu nomor unik yang dapat mengidentifikasi nomor pelanggan pada penyedia layanan.

Gambar 4 IMSI

4.2. Validasi

Berdasarkan hasil akuisisi dari tiga jenis *tools* yang berbeda, dengan *USSD code* atau dengan mengenali fisik dari kartu SIM, maka dapat dibuatlah tabel berikut.

Tabel 4.2 Validasi

Bukti Potensial	SIM Seizure	MobilEDIT	XLApp	USSD	Fisik	Keterangan
ICCID	x	x	-	-	x	*valid*
ADN	x	x	-	-	x	*valid*
FDN	x	x	-	-	-	*valid*
MSISDN	x	x	-	x	-	*valid*
LP	x	-	-	-	x	*valid*
Ciphering Key	x	-	-	-	-	*not yet valid*
SPN	x	x	x	x	x	*valid*
IMSI	x	x	x	x	-	*valid*
TMSI	x	x	-	-	-	*valid*
SMS	x	x	x	-	x	*valid*

4.3. Grouping

Berdasarkan bukti digital yang didapat dari hasil akuisisi, maka dapat dibuat tabel sebagai berikut.

Tabel 4.3 Identifikasi dan Pembagiannya

Bukti Potensial	*What*	*Who*	*Where*	*When*	*Why*	*How*
ICCID		x				
ADN		x				
FDN		x				
LDN		x		x	x	x
MSISDN		x				
LP						x
Ciphering Key						
SPN		x				
IMSI		x				
TMSI			x	x		
SMS	x	x	x	x	x	x

Tabel tersebut menunjukkan bahwa sumber bukti potensial tertinggi adalah SMS karena mencakup semua atribut. Disusul oleh LDN yang memiliki empat atribut, kemudian TMSI (LAI / LOCI) dengan dua atribut. Sayangnya berdasarkan hasil akuisisi, tidak ditemukan *value* pada LDN, sementara informasi yang berhasil

didapat dari SMS pun kebanyakan dikirim oleh provider. Untuk TMSI sendiri, bukti tersebut akan dapat bernilai apabila dicocokkan dengan *database* dari jaringan GSM dan kerja sama dari penyedia layanan.

4.4. Kepemilikan

Dalam *mobile forensic*, analisis kepemilikan dilakukan dengan memeriksa atribut file yang ditemukan. Atribut yang harus diperhatikan adalah atribut user, siapa yang membuat file tersebut, siapa yang mengubahnya, serta kapan terakhir kali diubah. Namun pada kartu SIM, analisis ownership yang lebih efektif dilakukan dengan mengetahui SPN dan ICCID yang tertera di dalam kartu SIM, kemudian menghubungi penyedia layanan untuk mengetahui kepemilikan dari kartu SIM tersebut dengan menyebut ICCID yang tertera di dalamnya.

5. Kesimpulan dan Saran

5.1. Kesimpulan

Berbagai data yang tersimpan pada *mobile phone* memang bisa dijadikan bukti. Pada kartu SIM sendiri, ternyata juga dapat dihasilkan berbagai jenis bukti digital. Dari hasil pengujian awal, tercatat bahwa data berupa jenis SIM, teknologi atau jaringan yang digunakan, nomor unik, MSISDN, ICCID, IMSI dapat dijadikukan bukti.

Ternyata ada beberapa bukti digital yang tidak ditemukan dalam kartu SIM karena kebanyakan *handset* yang digunakan saat ini membuat bukti digital yang dapat dikenali secara langsung seperti ADN, LDN dan SMS secara *default* tersimpan dalam media penyimpanan *handset* tersebut, bukan di dalam kartu SIM. Sayangnya berdasarkan hasil identifikasi, justru ketiga bukti tersebut merupakan bukti digital potensial tertinggi.

5.2. Saran

Karena keterbatasan yang dimiliki, penelitian ini memiliki beberapa kendala. Untuk hasil yang optimal, sebaiknya gunakan *sim card reader* Dekart. Untuk menambah akurasi dalam validasi, sebaiknya gunakan lebih banyak *tools* dan metode. Untuk penelitian berikutnya yang dapat dilakukan adalah penelitian terhadap kartu SIM.

Daftar Pustaka

[1]. Al-Zarouni, Marwan. ―Mobile Handset Forensic Evidence: A Challenge for Law Enforcement,‖ 2006.
[2]. http://www.forensicmag.com/articles/2011/06/sim-forensics-part-2. Accessed on Februrary 13th 2015.
[3]. Ramabhadran, Anup, and others. ―Forensic Investigation Process Model for Windows Mobile Devices.‖ *Tata Elxsi Security Group*, 2007, 1–16.
[4]. Murphy, Det Cynthia A. *Developing Process for Mobile Device Forensics*. Madison, 2009. http://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf.
[5]. ———. ―Guidelines on Cell Phone Forensics.‖ NIST Special Publication 800 (2007): 101.
[6]. Jansen, Wayne A., and Aurelien Delaitre. ―Reference Material for Assessing Forensic SIM Tools.‖ In Security Technology, 2007 41st Annual IEEE International Carnahan Conference on, 227–34. IEEE, 2007. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4373494.
[7]. Ayers, Rick, Sam Brothers, and Wayne Jansen. ―Guidelines on Mobile Device Forensic (Draft),‖ September 2013.
[8]. Casadei, Fabio, Antonio Savoldi, and Paolo Gubian. ―Forensics and SIM Cards: An Overview.‖ International Journal of Digital Evidence 5, no. 1 (2006): 1–21.