Analisis Investigation SIM Card Cloning Terhadap SMS Banking (Studi Kasus Pengguna Telkomsel Dengan Layanan BNI SMS Banking)

Conference Paper · November 2017

CITATIONS
0

READS
1,505

2 authors:

Nuril Anwar
Ahmad Dahlan University
4 PUBLICATIONS **62** CITATIONS
SEE PROFILE

Imam Riadi
Ahmad Dahlan University
240 PUBLICATIONS **1,986** CITATIONS
SEE PROFILE

ANALISIS INVESTIGATION SIMCARD CLONING TERHADAP SMS BANKING (STUDI KASUS PENGGUNA TELKOMSEL DENGAN LAYANAN BNI SMS BANKING)

Nuril Anwar [1], Imam Riadi [2]
[1] Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan
[2] Sistem Informasi, Fakultas Matematika Ilmu Pengetahuan Alam, Universitas Ahmad Dahlan
[1,2] Jalan Prof. Dr. Soepomo, S.H., Warungboto, Umbulharjo, Yogyakarta, 55164

Email [1] : nuril.anwar@tif.uad.ac.id Email [2] : imam.riadi@is.uad.ac.id [2]

Abstrak

Kejahatan dalam sektor telekomunikasi kian marak akhir-akhir ini khususnya disektor perbankan yang melibatkan peran dari provider selullar. Pada sistem keamanan simcard, ditemukan beberapa kelemahan data pelanggan diluar jaringan. Simcard cloning merupakan bagian dari permasalah keamanan yang terdapat pada device simcard. Penyalahgunaan wewenang diantaranya simcard cloning dalam hal mengakses layanan mobile services. Provider Telkomsel sebagai studi kasus dengan layanan BNI SMS Banking menjadi subyek penelitian ini. Authentication algorithm simcard GSM Telkomsel dapat ditembus dengan alat tertentu sehingga seluruh data dalam simcard dapat dipindahkan secara identik ke media simcard kloning lain, konsekuensinya layanan yang melekat didalamnya terkena dampak negatifnya. Fokus penelitian dengan melakukan investigasi digital forensik cloning simcard serta menganalisis dampak yang ditimbulkan dari simcard provider Telkomsel setelah terjadi cloning terhadap layanan BNI SMS Banking. Analisis selanjutnya untuk menguji performansi metode kloning yang meliputi proses registrasi simcard terhadap jaringan selullar, akses layanan BNI (SMS Banking), call setup (Phone Banking), dan akses data (Internet Banking) dengan menggunakan parameter pengujian Due Under Test (DUT) dan Trial and Error. Berdasarkan hasil investigasi cloning simcard dengan layanan perbankkan penelitian ini diperoleh prosentase tingkat kerentanan device simcard khususnya Telkomsel sebagai salah satu provider dengan layanan perbankan BNI SMS Banking. Keberhasilan investigasi digital evidence simcard berdasarkan generasi simcard serta kapasitas memori yang menampung informasi didalamnya. Investigasi forensik terhadap simcard cloning yaitu menitik beratkan pada pencocokan authentication Key (KI) yang terdapat pada simcard asli terhadap KI hasil generate serta penemuan data layanan SMS Banking yang terdapat pada struktur file simcard cloning.

***Kata kunci**: Authentication, BNI SMS Banking, Forensic, Simcard Cloning Telkomsel*

1. PENDAHULUAN

Kartu SIM menyimpan informasi yang berkaitan dengan jaringan yang digunakan untuk otentifikasi *(authentication)* dan identifikasi pengguna. Data yang paling penting adalah nomor identitas kartu (ICCID, *Integrated Circuit Card* ID), nomor pengguna internasional (IMSI, *International Mobile Subscriber Identity*), kunci authentikasi (Ki, *Authentication Key*), kode area (LAI, *Local Area Identity*), dan nomor panggilan darurat operator. SIM juga menyimpan nomor layanan pusat untuk SMS (SMSC, *Short Message Service Center*), nama penyedia layanan (SPN, *Service Provider Name*). (Jansen & Ayers, 2005)

Ketika *simcard* tersebut berorientasi sebagai *smartcard*, maka membuka kemungkinan keamanan yang beresonansi jauh melampaui dunia yang bersifat *mobile*. Media *simcard cloning* dapat diperoleh dengan mudah oleh para pelaku tindak kejahatan namun, dari berbagai media *cloning simcard* yang dijual dipasaran tidak dapat dipastikan media tersebut dapat digunakan untuk melakukan *cloning simcard*, hanya beberapa produsen yang mempunyai kelebihan serta kemampuan tertentu yang dapat men-generated algoritma A8 atau Ki. Kinerja media *cloning simcard* dapat dipengaruhi dari beberapa faktor dilapangan diantaranya kemampuan baca *simcard reader* serta kapasitas dari media *simcard cloning* itu sendiri. Algoritma A8 sebagai *autentication key* Ki berkaitan erat kaitannya dengan *random challenge* yang mengenerate Ki maka peran algoritma *random number generator*/RAND dapat bertindak sebagai algoritma autentikasi ketika terjadi kloning *simcard*.

Analisis investigasi *simcard cloning* dengan studi kasus penyalahgunaan hak akses pada layanan SMS banking merupakan salah satu metode penanggulangan baik kepada penyedia jasa telekomunikasi maupun pihak perbankkan. *Authentication Simcard* mencakup *Subscriber Based on* IMSI (*Stored on* SIM) dan *Random Number Generator*/RAND, maka akan diteliti lebih lanjut tentang *Authentication Simcard Cloning* dengan mencocokkan respon jaringan pelanggan *login* ke jaringan layanan *mobile. Random Number Generator* (RAND) dengan *Sign Respons* (SRES) yang berisi algoritma A3 *(Provide by Network)* sehingga dalam proses *simcard cloning* RAND berperan serta dalam proses pencocokan algoritma A8 RAND yang terdapat pada *simcard* terhadap algoritma A3 SRES yang terdapat pada jaringan terkait autentikasi data *simcard*. Algoritma tersebut akan digunakan sebagai autentikasi dalam melakukan investigasi dan ekplorasi data *simcard cloning* terkait keberadaan *digital evidence* pada *cloning simcard*.(N Anwar, 2016)

Metode investigasi *simcard* sudah pernah dikembangkan dan dikaji lebih lanjut oleh peneliti terdahulu (Prayudi & Rifandi, 2013) dalam penelitiannya membahas tentang ekplorasi barang bukti *simcard* serta membahas struktur file dari isi dalam *simcard* sedangkan (N Anwar, 2016) meneliti analisis *simcard cloning* beserta algoritma RAND "*Random Number Generator"* beserta simulasi *cloning simcard*. Penelitian selanjutnya akan diterapkan langkah investigasi terhadap kasus *simcard cloning* dengan provider Telkomsel terhadap penyalahgunaan layanan BNI SMS Banking beserta *report* investigasi barang bukti *digital evidence simcard cloning*.

2. METODOLOGI

Metodologi penelitian memuat serangkaian tahapan proses yang diteliti dengan subyek penelitian barang bukti simcard cloning dengan smartphone yang didalamnya terdapat layanan *mobile banking* (SMS *Banking*), selanjutnya mengerucut ke metode pendukung diantaranya :

2.1 Analisis Penelitian

Analisis Penelitian dan fokus penelitian sesuai dengan fakta dilapangan terkait penanganan barang bukti *simcard* yang telah dikloning dan terjadi penyalahgunanan layanan perbankkan yaitu SMS Banking, untuk selanjutnya dipaparkan dalam sebuah hipotesis untuk membuktikan bahwa hipotesis yang diangkat sesuai dengan keadaan dilapangan, responden dalam penelitian ini yaitu peneliti terdahulu terkait explorasi barang bukti *simcard* serta korban dari *simcard cloning*. Tahap akhir dari analisis penelitian *simcard cloning* akan dikemukakan pengaruh *simcard cloning* terhadap layanan sms banking berdasarkan *log simcard* hasil *cloning* dengan *log simcard* aslinya (investigasi device simcard) dan penanganan *incident handler* pada *smartphone* dalam mengakses layanan *mobile banking* (investigasi *devices smartphone*). Langkah berikutnya yaitu testing atau skenario penelitian terkait *attack* yang ditimbulkan dari *simcard cloning*, dalam melibatkan layanan mobile banking (SMS *Banking*) serta bagaimana penanganan lebih lanjutnya.

2.2 Attack dan Skenario Testing

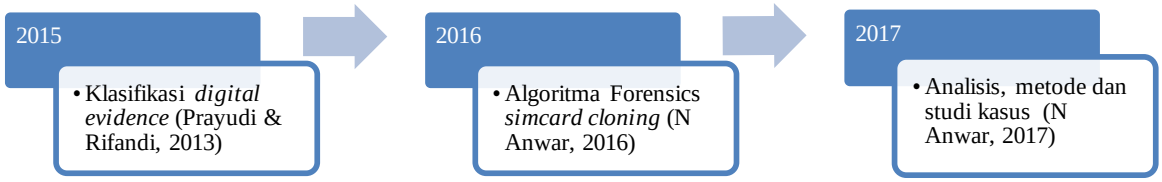
Skenario testing ditekankan pada proses *cloning* dari *simcard* itu sendiri meliputi keberhasilan proses *cloning simcard* asli dan respon terhadap jaringan ketika *simcard cloning* bersinggungan langsung dengan *simcard* asli sedangkan skenario serangan *attack* yang ditimbulkan pasca *simcard* dikloning berupa serangan akses ke layanan mobile banking dalam hal ini SMS Banking serta akses data dari *simcard cloning* (korban) beserta efeknya yang ditimbulkan, sedangkan skenario testing meliputi beberapa komponen testing diantaranya :

a. *Attack Simcard Cloning* terhadap SMS *Banking*
b. *Testing Simcard Cloning* terhadap layanan SMS *Banking*
c. Pengujian *Cloning Simcard* terhadap SMS *Banking*
d. Analisis Forensik *Simcard Cloning* dan SMS *Banking*

Berdasarkan *attack* dan skenario *testing* diharapkan terjalin sebuah luaran framework investigasi dalam penanganan *incident handler* khususnya *simcard* dan *mobile device evidence*.

2.3 Roadmap Penelitian

Penelitian ini merupakan bagian dari *roadmap* penelitian terdahulu yang pernah dilakukan oleh penulis dan mitra riset khususnya di bidang *digital forensics* seperti yang ditunjukkan pada Gambar 2.1. dibawah ini :

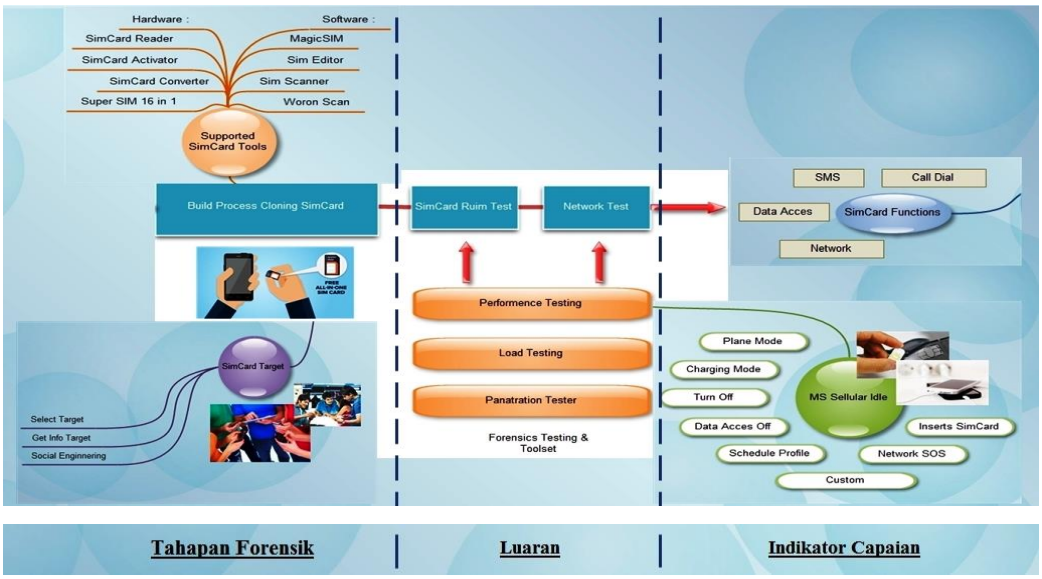


Gambar 2.1. Roadmap Penelitian Bidang Digital Forensics

Berdasarkan *roadmap* penelitian diatas dapat ditunjukkan fokus riset yang akan diteliti terlebih yaitu pada *simcard* untuk selanjutnya diterapkan secara teknis terhadap kasus dilapangan sampai *report investigation forensics*

2.4 Metodologi dan Tahapan Peneliti

Metodologi dan tahapan dalam penelitian terkait simcard cloning dengan layanan SMS banking tersaji dalam peta bagan riset seperti tampak pada gambar 2.2 dibawah ini :



Gambar 2.2 Tahapan, Luaran dan Indikator Capaian

Desain dan usulan Forensik *simcard cloning* seperti tampak pada Gambar 2.2 dapat ditekankan pada poin diantaranya :

1) *Simcard Cloning Evidence* ; berupa fisik dari *simcard* beserta tindak kriminal beserta penanganannya.
2) *Riset Goal Investigation Methode* ; proses penanganan barang bukti dari memperoleh, akuisisi serta merepresentasikan skema kasus.
3) *Forensics Tools Investigator* ; merupakan *software forensic* dalam hal ekplorasi, eksaminasi dan *reporting* berkenaan terhadap barang bukti *simcard*.
4) *Digital Evidence Risk* ; Resiko yang ditimbulkan pasca kloning berupa layanan SMS *Banking*, *Phone Banking* dan *Internet Banking* serta *simcard* hasil *cloning* memerlukan penanganan yang lebih terkait akuisisi data dari *simcard* tersebut.

3 HASIL DAN PEMBAHASAN

Pada hasil dan pembahasan berisikan detail hasil riset simcard cloning dengan layanan mobile banking dengan barang bukti (digital evidence) device simcard dan smartphone, tersaji pula tabel investigasi yang melibatkan kedua devices evidence. Sub pembahasan hasil riset terdiri dari :

3.1. Hasil Penelitaian

Hasil penelitian menitikberatkan pada penerapan langkah *investigastion* terhadap kasus *simcard cloning* dengan provider Telkomsel terhadap penyalahgunaan layanan BNI SMS Banking dengan motif kejahatan membuat *copy simcard* secara identik dengan *simcard* asli, selanjutnya melakukan tindak kejahatan seolah-olah pelaku sebagai pemilik langsung atau asli pengguna layanan SMS *Banking* yang melakukan transaksi perbankkan tanpa diketahui korban atau pemilik akun tersebut selanjutnya dilakukan langkah prosedur investigasi penanganan atau *incident handler* terhadap barang bukti *simcard cloning* pelaku tindak kejahatan untuk diperoleh serangkaian *report* digital forensik dengan barang bukti *simcard cloning*.

Prosedur forensik mengungkap seluruh isi dari *simcard cloning* yaitu dengan men-*download* seluruh memori SIM dan menghitung nilai *hash* memori sedang untuk melakukan hal ini dibutuhkan alat untuk men-*download* isi biner file individual dan menyimpannya sebagai file individual. alat tersebut adalah *SIMSCAN*. Selain itu dibutuhkan alat untuk menyinkronkan data seperti pesan teks antara kartu SIM dan komputer seperti *Sim Manajer Pro*. Tools forensik saat ini yang paling populer dipenegakan hukum adalah *Simcard Seizure* , yang dikembangkan oleh lembaga forensik *Paraben Corporation*. Alat ini tidak menyimpan salinan digital dari file-SIM dikomputer, melainkan menghasilkan laporan teks pada sebagian besar konten pada kartu SIM. Semua data yang disimpan dapat berpotensi memiliki nilai pembuktian, sedangkan tahapan investigasi simcard cloning yang melibatkan layanan perbankkan akan disajikan dalam bentuk tabel investigasi seperti tampak pada tabel 4.1 dibawah ini :

Tabel Error! No text of specified style in document.**..1. Tabel Investigasi Simcard Cloning dengan Layanan Bank Services**

Identifikasi	Preservasi	Koleksi	Eksaminasi	Analisis	Presentasi
Identifikasi kejahatan Simcard terhadap Layanan Bank Services	Pengolahan Simcard & Layanan Bank Services	Pengamanan barang bukti Simcard & Smartphone	Pelacakan barang bukti Simcard & Smartphone	Kompasrasi data investigasi	Dokumentasi
Profil kejahatan Simcard & SMS Banking	Chain of custody/ kronologis Simcard Cloning & SMS Banking	Teknik investigasi Simcard & Smartphone	Validasi barang bukti Simcard & Smartphone	Pengolahan temuan barang bukti	Klarifikasi invistigator
Audit dan analisa kasus	Manajemen waktu investigasi		Filtering barang bukti		Pernyataan, saran dan tindakan
	Pengolahan kasus Simcard & Smartphone		Pencocokan barang bukti		Interpretasi data Simcard & Smartphone
			Penemuan data tersembunyi		

Tabel 4.1 diatas merupakan prosedur DTR-T001-01, D. F. (2001) atau langkah investigasi yang telah disesuaikan dengan barang bukti digital dalam hal ini devices simcard, simcard hasil cloning dan *smartphone* sebagai media mengakses layanan perbankkan.

3.2 Hasil Investigation

Hasil investigasi digital evidence yang melibatkan devices simcard dan smartphone menjadi representasi hasil utama dalam penelitian ini, maka dari temuan data tersembunyi dari kedua device tersebut dapat di klasifikasikan barang bukti berdasarkan *investigation devices simcard cloning* meliputi :

a. Simcard Evidence

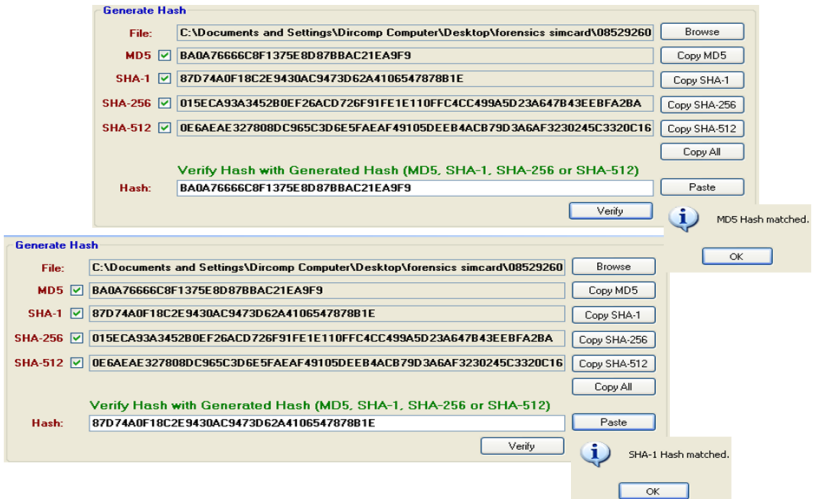
Barang bukti secara visik dapat di klasifikasikan meliputi barang bukti asli sebagai autentikasi dan hasil cloning beserta medianya, seperti tampak pada gambar 3.1 dibawah ini :

Gambar 3.2. Simcard Evidence

Berdasarkan klasifikasi digital *evidence* keduanya memiliki media *storage* yang berbeda secara teknis pemakaian dan fungsi, dalam hal ini *simcard* asli sebagai mediator autentikasi *Ki number* hasil *generated* program *cloning simcard*, sedang media kloning *simcard* sebagai duplikator *simcard* asli korban atau pengguna *(user)*.

b. Validasi barang bukti

Simcard ***Hash Checksum for SIM/USIM/R-UIM*** *Forensic Tool* yang direkayasa sesuai dengan pedoman ACPO untuk memastikan bahwa tidak ada data pada *simcard evidence* yang telah dimodifikasi selama proses membaca. Proses verifikasi *simcard* atau *hash generated* dapat dilihat pada Gambar 3.2 dibawah ini :



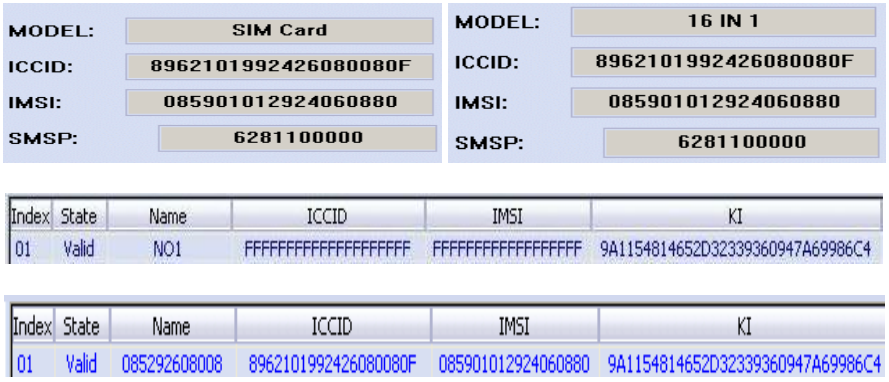
Gambar 3.3. MD5 Hash Check

MD5 check berfungsi sebagai laporan yang secara *digital signature* dengan kedua MD5 dan SHA1/256/512 *hash* untuk memastikan integritas barang bukti tidak terkontaminasi pihak lain (identik dengan *digital evidence* asli).

c. Simcard Info

Berdasarkan Gambar 4.3 dibawah dapat diketahui status proses *cloning* dengan komponen

diantaranya ICCID, IMSI, SMSP dan yang paling uama yaitu Ki dapat disalin secara identik terhadap *simcard* asli

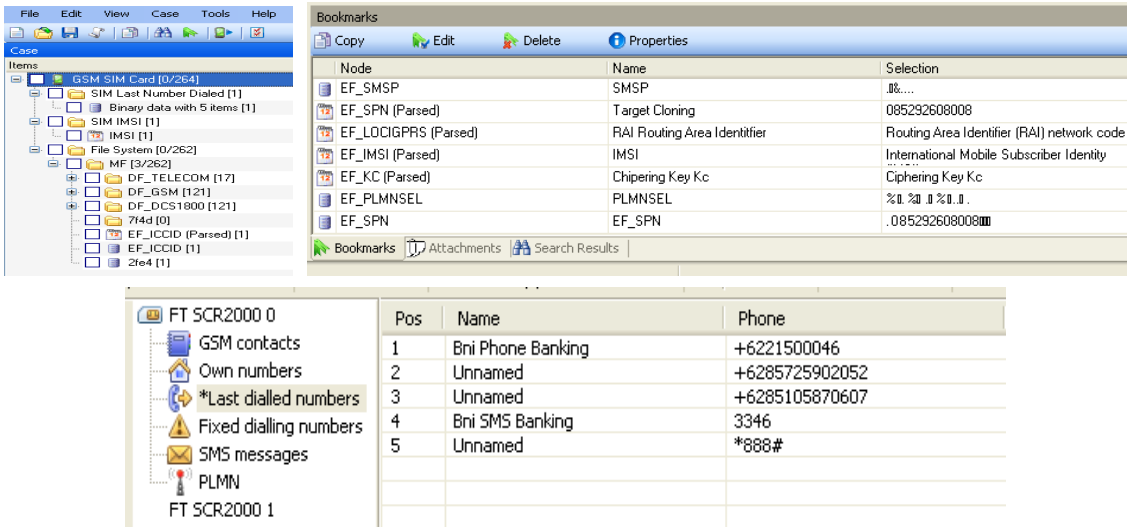


Gambar 3.4. Simcard Info

Berdasarkan gambar 3.3 diatas dapat diketahui bahwa identitas simcard asli dan hasil kloning *match* ditunjukkan dengan ICCID IMSI dan SMSP dengan hasil generated Ki number seperti tampak pada gambar.

d. Filtering barang bukti

Paraben's SIM-Card Seizure *Forensic Tool* yang dapat menampilkan *file system* beserta struktur file pada *simcard*, selain itu *software forensic* ini mampu melakukan akuisisi data *simcard* tanpa harus melakukan *scan device evidence* secara berulang. Kemampuan lain yaitu mampu melakukan analisis yang komprehensif dari data kartu SIM. File struktur temuan pada barang bukti *simcard* dapat dilihat pada Gambar 3.4 :



Gambar 3.5. Simcard File Structure

Berdasarkan struktur *simcard* diatas dapat diketahui jenis barang bukti digital dalam hal ini *simcard* sebagai *digital evidence* yang memuat serangkaian penguatan bahwa *simcard* telah dikloning, dengan sejumlah nomor-nomor layanan perbankkan BNI SMS *Banking*.

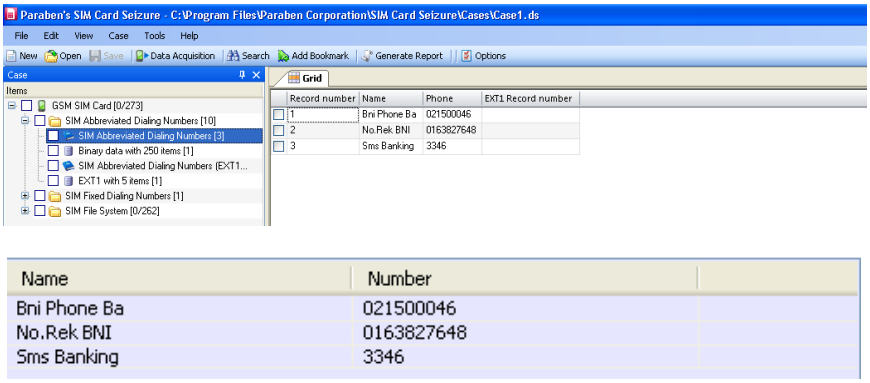
e. SIMQuery

Forensic Tool merupakan alat command line yang mengambil ICCID dan IMSI dari kartu SIM GSM. Sebuah *smart cardreader* yang kompatibel dengan subsistem *smartcard*. (http://vidstrom.net/otools/simquery/). Seperti tampak pada gambar 3.5 :

List Command SIMQuery Python with PySim :

```
./pySim-read.py
ICCID          : 89621019924260800080F
IMSI           : 085901012924060880
SMSP           :fffdfffffffff62811000000fffffffffff
Generated card parameters :
> Name         : Magic SIM 16 in 1
> SMSP         : 62811000000
> ICCID        : 89621019924260800080F
> MCC/MNC      : 501/10
> IMSI         : 085901012924060880
> Ki           : 9A1154814652D323-
                 39360947A69986C4
> OPC          : None
> ACC          : None
```

Script diatas berfungsi sebagai autentikasi identias *simcard* dengan parameter hasil seperti tampak pada list *tools SIMQuery (Python with PySim),* sehingga dapat dihasilkan sotware investigasi kombinasi dengan *Parabens SIM Card Software* diketemukan *log* transaksi *simcard* seperti tampak pada gambar 3.5 :



Gambar 3.6. Log Simcard

Berdasarkan hasil ekplorasi *digital evidence* berupa *simcard device* diperoleh kuat dugaan akan *simcard cloning* telah mengakses serangkaian layanan perbankkan ditunjukkan dengan *log* transaksi SMS *Banking.*

4.2.1 Device Smartphone

Pada proses investigasi yang melibatkan *digital evidence* berupa *smartphone* pelaku *cloning simcard* pembahasan terbatas hanya pada *device simcard* saja *(incident handler),* sedangkan proses investigasi *forensics mobilephone* akan dilakukan ke tahap penelitian selanjutnya.

4 KESIMPULAN

Penelitian Analisis *Investigation Simcard Cloning* terhadap SMS *Banking* dengan Studi Kasus Pengguna Telkomsel dengan Layanan BNI SMS *Banking* telah dilalui dengan beberapa tahapan sehingga dapat ditarik kesimpulan diantaranya ; telah dilakukan langkah pendeteksian *simcard*, bilamana simcard asli (korban) telah mengalami serangkaian proses kloning sehingga terdapat kesamaan akan data yang melekat sesuai dengan *simcard* aslinya. Penanganan barang bukti *simcard cloning* dengan kasus SMS *banking* melibatkan beberapa komponen diantaranya :

a. Investigasi *devices Simcard,*

b. Investigasi *devices Smartphone*

Berdasarkan kedua komponen diatas dapat dihasilkan hasil investigasi yang berbeda secara *devices* maupun langkah penanganannya *(incident handler)*.

Report Investigation berupa *bookmark* dari temuan-temuan sebagai penguat barang bukti *digital*, untuk lebih *detail report investigation* tersaji dalam *general report* hasil dari *software forensics mobile device simcard parabens simcard seizure*.

5 DAFTAR PUSTAKA

DTR-T001-01, D. F. (2001). *A roadmap for digital forensic research.*

Hayat, C. (2014). *Analisis SIM Card Clone Pada IM3 Smart Serta Penggunaan Ellptic Curve Cryptosystem Untuk Meningkatkan Keamanan Jaringan GSM.* Depok, Indonesia: Jurusan Sistem Informasi, Universitas Gunadarma.

Jansen, W., & Ayers, R. (2005). National Institute of Standards and Technology. *Forensic Software Tools for Cell Phone Subscriber Identity Modul* .

N Anwar, I. R. (2016). Forensic SIM Card Cloning Using Authentication. *Int. J. of Electronics and Information Engineering Vol.4, No.2, PP.71-81, June 2016* , 71-81.

N Anwar, I Riadi, A Luthfi. (2016). Analisis SIM Card Cloning Terhadap Algoritma Random Number Generator. *Jurnal Nasional Buana Informatika Universitas Atma Jaya Yogyakarta Vol 7, No 2 (2016)*

Prayudi, Y., & Rifandi, F. (2013). Ekplorasi Bukti Digital pada SIMCard. *Pusat Studi Forensika Digital, SESINDO FTI - Universitas Islam Indonesia* .