BAB III
METODE PENELITIAN

1. Subyek Penelitian

Subyek penelitian ini yaitu ditekankan pada *Autentication Simcard Cloning* dengan memahami karakteristik dari hasil kloningan untuk selanjutnya dikembangkan ketahap investigasi digital forensik barang bukti berupa skema kasus *simcard cloning*, sedangkan proses investigasi akan dilakukan di Laboratorium IT Centrum Universitas Islam Indonesia dengan alasan utama yaitu laboratorium tersebut merupakan bagian dari Pusat Studi Digital Forensik tentunya dengan dukungan *software* maupun *hardware* yang mampu mencakup tindak lanjut penelitian terkait *simcard cloning* dan segala kebutuhan yang berkaitan dengan investigasi *digital evidence.*

2. Alat dan Bahan Penelitian

Kesiapan sebuah penelitian harus diperhatikan demi keberhasilan yang maksimal meliputi kebutuhan sistem baik *hardware* maupun *software.* Dibawah ini merupakan sebagian besar kebutuhan sistem diantaranya adalah :

2.1 Hardware (Perangkat Keras)

2.1.1 *PC Desktop*

- *Prosesor Intel (R) Core 2 Duo (TM) 5700M CPU @ 3,0 GHz;*
- *RAM 4 GB;*
- *Harddisk 1500GB Sistem Operasi Windows XP Profesional 32 bit.*

2.1.2 *Notebook*

- *Prosesor AMD Apu (TM) 5700M CPU @ 3,0 GHz;*
- *RAM 4 GB;*
- *Harddisk 320GB Sistem Operasi Windows 8 Profesional 32 bit, Virtual : Windows XP Profesional 32 bit. OpenSource BackTrack5*

2.1.3 *Prolifix CardReader data line to a RS232 port Pembaca Simcard*

- *Intended for COMP128v1 based Cloning Support Algoritma A8*
- *Compatible GSM.*
- *USB Connector*
- *Support Connection Compatible GSM (16kb, 32kb dan 64kb)*

Generasi Simcard

2.1.4 *SmartCard PC Serial Reader / Writer (Phoenix)*

- *Intended for COMP32v1 based Cloning Support Algoritma A3*
- *USB Connector*
- *Support Connection Compatible GSM (16kb dan 32kb) Generasi Simcard*

2.1.5 *SuperSIM 16in1(Writer hasil Cloning Simcard)*

- *16 in 1 Super Simcard Writer Cloner Edit Copy Backup GSM (kapasitas write clone Simcard)*
- *Copy different number to one Simcard*
- *Allow 12 different number to one Simcard including phone book, SMS, ring tones etc.*
- *250 set phonebook*
- *40 set SMS*
- *Information safekeeping, set, cancel, manage mobile PIN dan password*

2.1.6 *Simcard Aktivator Converter*

- *Support All Ruim Card (Converter all ruim Simcard mini,micro dan nano Simcard)*

2.2 Software (Perangkat Lunak)

2.2.1 Software Penelitian Cloning Simcard

- *MagicSIM* V25.0
- SIM *Editor* v9.0
- SIM *Scanner* 5.15
- *Woron Scan (Software deteksi algoritma com128)*

2.2.2 Software Analisis Investigasi Simcard Cloning

- Windows Platform
  a) *Paraben Simcard Seizure*
  b) *EnCase*
  c) *Mobiledit*
  d) *SimExplorer*
- BackTrack5 Platform
  a) *AsteRisk* merupakan open source software yang biasanya digunakan untuk membangun suatu sistem layanan komunikasi serta memberikan kemudahan kepada penggunanya untuk mengembangkan layanan telepon sendiri dengan kustomisasi yang seluas-luasnya diberikan kepada

pihak pengguna dengan kata lain asterisk dalam pemanfaatannya sebagai server VoIP sederhana.

b) *Python with PySim* adalah kerangka simulasi diskrit-proses untuk model komponen *simcard*. PySim juga menyediakan fitur diantaranya monitoring kemampuan untuk membantu dalam mengumpulkan statistik tentang proses *cloning simcard*.

3. Metode Penelitian

3.1 Analisis Penelitian

Analisis Penelitian berdasarkan teori agar fokus penelitian sesuai dengan fakta dilapangan terkait penanganan barang bukti *simcard* yang telah dikloning untuk selanjutnya dipaparkan dalam sebuah hipotesis untuk membuktikan bahwa hipotesis yang diangkat sesuai dengan keadaan saat wawancara responden, 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* berdasarkan *log simcard* hasil *cloning* dengan *log simcard* aslinya. Langkah berikutnya yaitu testing atau skenario penelitian terkait *attack* yang ditimbulkan dari *simcard cloning*, serta bagaimana penanganan lebih lanjutnya.

3.2 Attack dan Skenario Testing

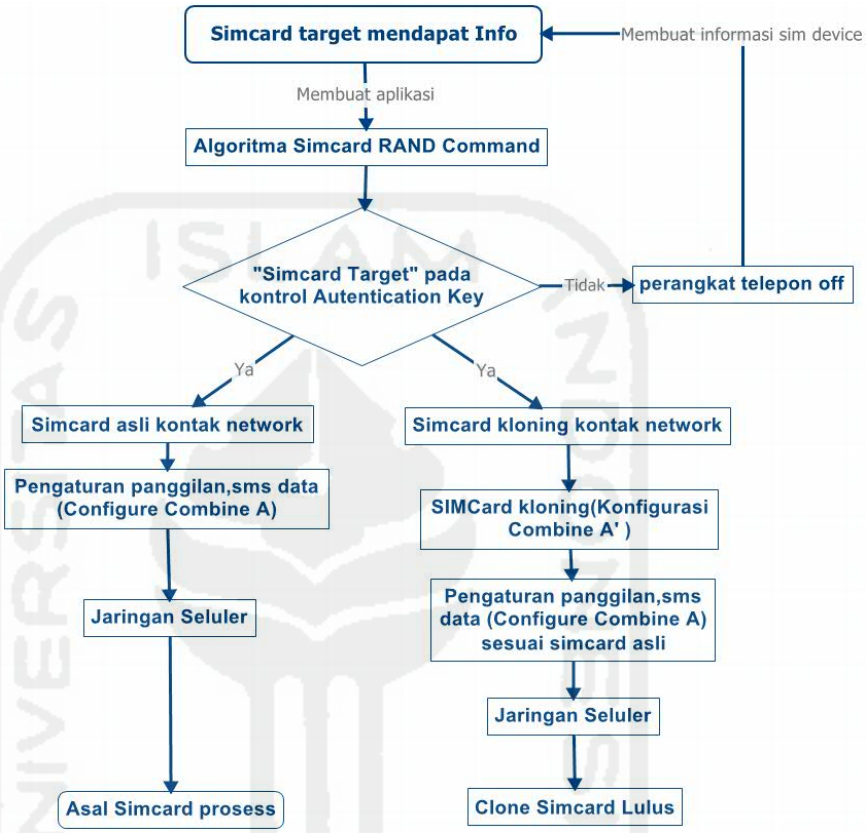
Skenario testing ditekankan pada proses *cloning* dari *simcard* itu sendiri meliputi keberhasilan proses *cloning simcard* asli dan respon terhadap jaringan ketika *simcard cloning* bersinggungan langsung dengan *simcard* asli sedangkan skenario serangan *attack* yang ditimbulkan pasca *simcard* dikloning berupa serangan akses komunikasi seperti sms, *telephone* dan akses data dari *simcard cloning* (korban) beserta efeknya.

1) Attack Simcard Cloning

Hal ini penting bagi penyidik untuk memahami bahwa *Subscriber Identity Module* dapat diserang oleh pihak lain. Dalam konteks

forensik, metode serangan yang paling jelas adalah penghapusan bukti. Karena file pada kartu GSM dapat diakses dalam kondisi tertentu, penyerang dapat menghapus bukti dengan menimpa ruang penyimpanan, dengan kata lain seseorang dapat mengetahui bahwa pesan teks yang dihapus masih dapat diakses pada kartu, dapat menggunakan editor kartu untuk menimpa pesan dengan informasi lainnya. Jika proses ini dilakukan, maka pengkloning *simcard* dapat melakukan penyalahgunaan informasi pada *simcard*. Dalam sistem GSM, identitas pelanggan hanya disimpan di SIM, sehingga perlindungan terhadap *cloning* hanya mengandalkan fitur keamanan SIM. Satu-satunya informasi yang mengidentifikasi pengguna adalah pengguna IMSI dan kunci enkripsi rahasia Ki. Keduanya disimpan di SIM dan di HLR dalam jaringan. Sebagaimana telah dilihat, IMSI dapat dibaca langsung dari kartu SIM jika pengguna mengetahui kode PIN atau PUK. IMSI pelanggan *valid* lain juga dapat diperoleh dengan mendengarkan lalu lintas jaringan terenkripsi pada *interface network*, karena IMSI akan ditransfer terenkripsi seluruh antarmuka jaringan setiap kali register *mobile* dengan jaringan baru. Tindak kriminal *cloning simcard* berupa memperoleh kunci enkripsi Ki, karena Ki disimpan hanya internal dalam kartu SIM, tetapi hanya melalui penggunaan algoritma enkripsi yang disimpan pada kartu. Ki dapat ditemukan jika algoritma mengandung kelemahan yang memungkinkan analisis tersebut umumnya dikenal sebagai serangan Algoritma di GSM. Sebuah alat untuk mengekstrak Ki dari SIM telah diimplementasikan dalam program *Sim-Scan*, tersedia dipasaran seperti *SIMSCAN* dan sebagainya. IMSI dan Ki dapat diperoleh oleh siapa saja dengan akses ke *SIM-card* menggunakan aplikasi bawaan yang dijual bebas yang dapat menghasilkan *SIM-card* baru atau *cloning* dengan IMSI dan Ki yang sama. Alat *cloning* tersebut didistribusikan bersama-sama dengan paket *simcard*. Seorang penyerang juga dapat mendapatkan sebuah *simcard cloning* beserta *programmer Smartcard-*

nya yang identik dengan *simcard* aslinya. Skema *attack* atau serangan *simcard cloning* tampak seperti Gambar 3.1



Gambar 3.1 Flowchart Attack Simcard Cloning

(Tomcsányi, 2013) *Flowchart Attack Simcard Cloning* diatas merupakan modifikasi dari prinsip kerja dari Gambar 2.3 berupa diagram alir dari seluruh proses *Traffic Chanel Attack* untuk selanjutnya dikomparasi dengan keadaan *simcard cloning* sesuai dengan tema penelitian sehingga diperoleh diagram proses baru untuk disesuaikan dengan penelitian terkait *simcard cloning* maka akan tampak diagram proses baru seperti tampak pada Gambar 3.1.

2) Skenario Testing Simcard Cloning

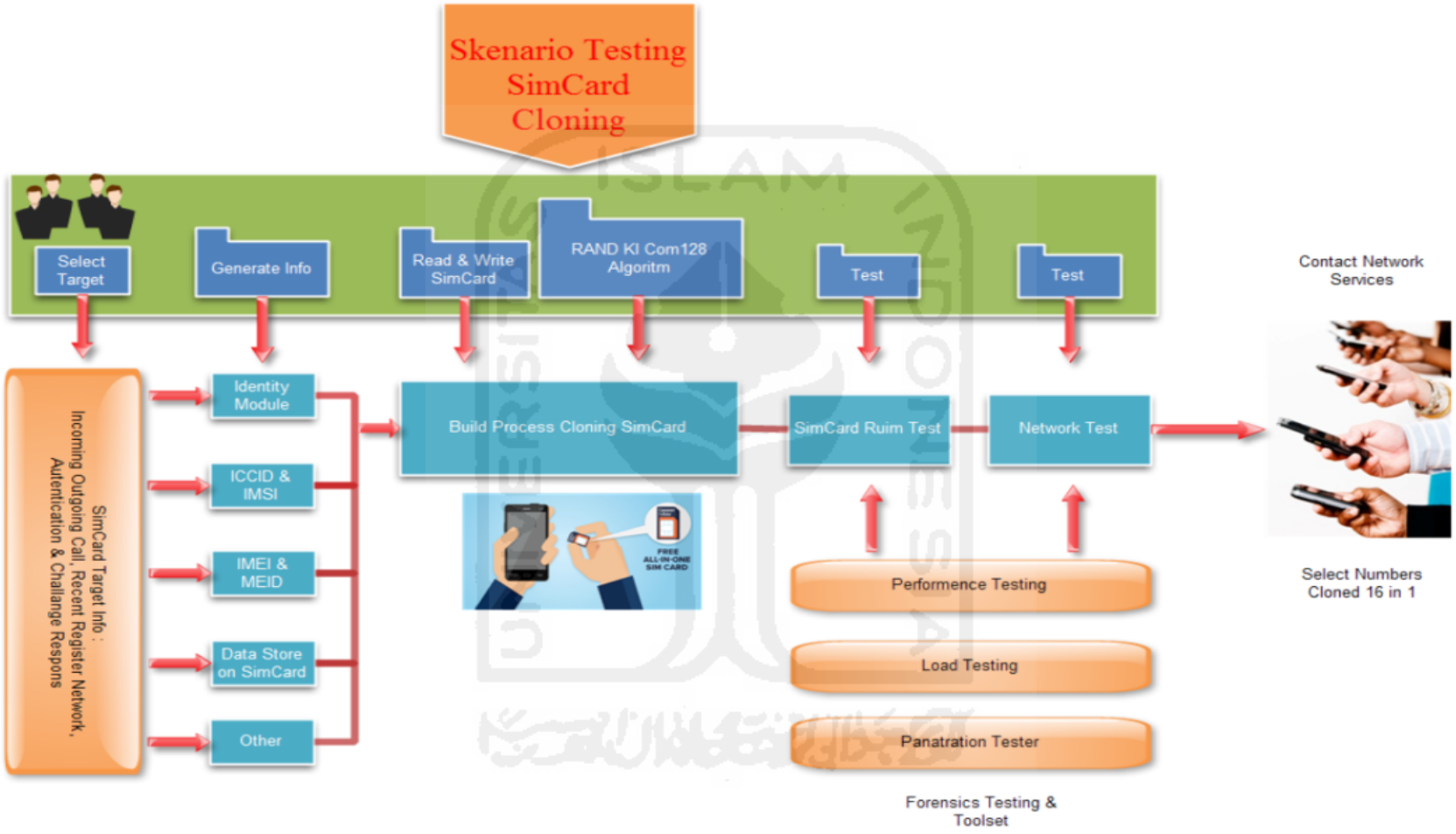
Testing merupakan tugas yang tak dapat dihindari di tiap bagian dari tanggung jawab usaha pengembangan suatu *system* (Howden,

2005). Testing dalam hal ini ditekankan pada pengujian hasil *simcard* pasca dikloning meliputi *performance tesing, load testing* dan *penetration tester* untuk diketahui kemampuan serta *respons* terhadap jaringan atas keberadaan *simcard* lebih dari satu atau ganda. Hasil pengujian berupa tabel *test case* beserta kesimpulan dengan harapan dapat dikemukakan prinsip kerja dari *cloning simcard* itu sendiri beserta efek yang ditimbulkan untuk selanjutnya dilakukan analisis dari cloning simcard. Hasil testing di tampilkan berupa tabel kualifikasi untuk dapat diketahui status proses dari *cloning* hingga tahap proses investigasi yang dihasilkan *reporting* atas barang bukti *simcard cloning*. Skenario *simcard cloning* beserta beserta tahapan prosesnya dapat dilihat pada Gambar 3.2. Sedangkan untuk mengukur tingkat keberhasilan *cloning* terhadap *simcard* dapat berupa serangkaian *testing simcard cloning* antar generasi dan provider selular dapat disajikan dalam bentuk Tabel 3.1

Tabel 3.1 Testing Simcard Cloning (Prosentase Keberhasilan)

No.	Provider Simcard	Generasi 1st	Generasi 2nd	Generasi 3rd
1.	Telkomsel	Th ….. = %	Th ….. = %	Th ….. = %
2.	Indosat	Th ….. = %	Th ….. = %	Th ….. = %
3.	Xl	Th ….. = %	Th ….. = %	Th ….. = %
4.	3	Th ….. = %	Th ….. = %	Th ….. = %
Memori Simcard		32kb	64kb	128kb
Signal Coverage		1G	2G/3G	3G/4G

Berdasarkan Tabel 3.1 diatas dapat diperoleh nilai prosentase tingkat keberhasilan dalam melakukan *simcard cloning* antar sampel *simcard* dari beberapa perusahaan selular serta generasi dan kapasitas memori yang terdapat pada *simcard*.



Gambar 3.2 Skenario Testing Simcard Cloning

Skenario Testing berisi serangkaian proses dari memilih *target cloning,* menghimpun data target untuk selanjutnya proses ekstraksi Ki untuk disalin data-data didalamnya. Ekstraksi Ki menghasilkan algoritma yang identik dengan *simcard* asli maka diperlukan proses testing pasca dilakukan *cloning* data *simcard* yang nantinya akan di *write on simcard* 16 in 1. *Simcard* 16 in 1 ini mempunyai kapasitas *write on* sebanyak 16 kali dalam satu kartu, sehingga mempunyai konsekuensi bilamana slot *simcard* dari 16 itu telah digunakan maka tidak dapat diisi sesi *write on* berikutnya. Tahap akhir dari proses *cloning* ini yaitu memilih nomor mana yang akan diaktifkan ke jaringan secara bergantian tentunya dengan serangkaian testing seperti tampak diatas, sedangkan tabel kualifikasi testing *simcard cloning* tampak seperti beberapa Tabel 3.2

Tabel 3.2 Performance Testing Simcard hasil Cloning

Skenario Pengujian	**Test Case**	**Hasil yang diharapkan**	**Hasil Pengujian**	**Kesimpulan**
Simcard Device Under Test (DUT)	……	Identik dengan Simcard Asli (RAND,Ki)	……	……

Pengujian kloning *simcard* dapat menimbulkan masalah jika penggunaannya tidak dimonitoring sedemikian rupa selain itu dapat menyebabkan hilangnya data dari perangkat yang diuji. *Device simcard* yang memiliki sifat non-volatile memerlukan penanganan yang bersifat khusus sehingga dibutuhkan tahapan atau skema pengujian. Berdasarkan tahapan pengujian yang utama diantaranya dapat disebut dengan tahap *device under test* (DUT), dari tahap tersebut maka diperlukan tahapan berikutnya yaitu *perform test* dengan tabel kualifikasi dan konten yang diuji dapat dilihat pada Tabel 3.2

Tabel 3.3 Load Testing Simcard Cloning

Skenario Pengujian	Test Case	Hasil yang diharapkan	Hasil Pengujian	Kesimpulan
Simcard 'Trial and Error'	……	Sign Respons (SRES)	……	……

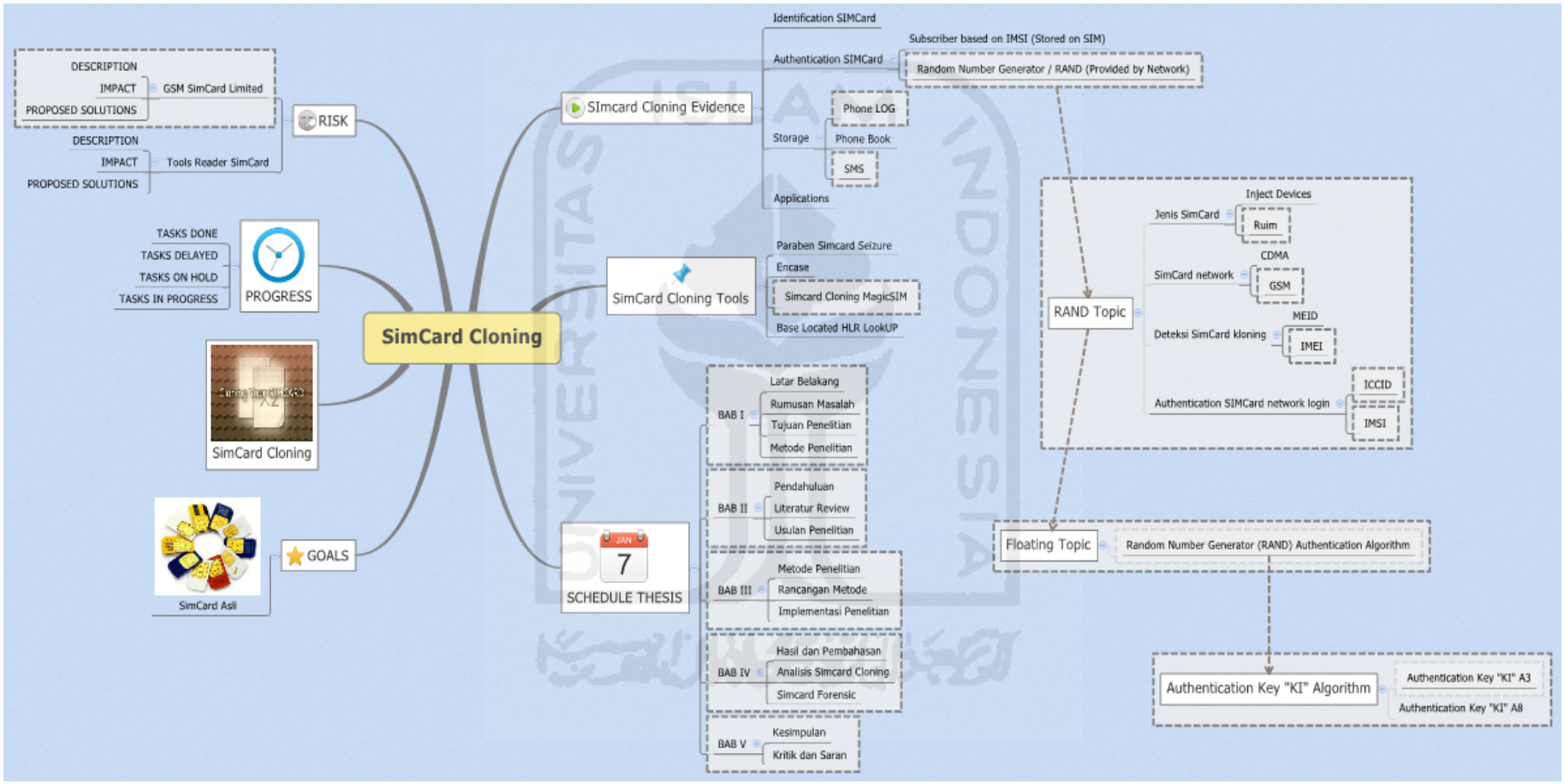
Tujuan dari *Load Testing* yaitu mengetahui respon hasil *simcard cloning* terhadap penyedia jaringan, apakah diterima, ditolak atau berbenturan dengan jaringan *simcard* asli seperti tampak pada Tabel 3.3 diatas, sedangkan *Penetration Tester* merujuk pada hasil akhir dari proses investigasi bukti digital *simcard cloning* beserta pelaporan untuk dapat dikemukakan diranah hukum sesuai kriteria barang bukti. Ditunjukan seperti pada Tabel 3.4

Tabel 3.4 Penetration Tester (Forensics Tools)

Skenario Pengujian	Test Case	Hasil yang diharapkan	Hasil Pengujian	Kesimpulan
Simcard Acquisition and Analysis	……	Explorasi & Repport (Digital Evidence) Simcard Cloning	……	……

Tabel 3.4 merupakan komparasi serta perbandingan performa dari *tools* investigasi, perbandingan tersebut diperlukan dikarenakan tidak ada *tools forensic* yang paling baik tanpa kombinasi penggunaan *tools* saat mengekplorasi barang bukti terutama *simcard cloning*, dengan tujuan akhir yaitu diperoleh banyak bukti digital yang komplek untuk dapat dilanjutkan ke tahap *reporting investigation* sehingga memudahkan investigator dalam memberikan keterangan tindak kejahatan khususnya *simcard cloning*.

3.3 Desain dan Usulan Forensik Simcard Cloning



Gambar 3.3 Usulan Forensik Simcard Cloning

Desain dan usulan Forensik *simcard cloning* seperti tampak pada Gambar 3.3 dapat ditekankan pada poin diantaranya :

1) *Simcard Cloning Evidence* ; berupa fisik dari *simcard* beserta tindak penanganannya.
2) *Random Number Generator*
   a. RAND ; proses penentuan algoritma autentikasi
   b. *Autentication Key* (KI) ; proses mendapatkan KI original untuk selanjutnya di *write* atau *clone* ke *blank simcard*
3) *Forensics Tools Investigator* ; merupakan *software forensic* terkait barang bukti *simcard* dengan tipe *opensources* dan resmi
4) *Digital Evidence Risk* ; *Simcard* hasil *cloning* memerlukan penanganan yang lebih terkait akuisisi data dari *simcard* tersebut

3.4 Pengujian Cloning Simcard

Autentication Cloning Simcard dalam scenario pengujian mengacu pada *Autentication key* (disebut sebagai Ki dalam terminologi *simcard* GSM), merupakan bagian dari IMSI dan nomor ESN Dari hal ini, hanya private key dan 'Ki' dilindungi serta terdapat pada kartu SIM. Sedangkan *Private Key* melekat pada *simcard*. A3-algoritma yang digunakan sebagai algoritma *checksum*, dikenal sebagai COMP128. Dengan test *trial-and-error*, dengan memberi inputan yang berbeda untuk *simcard* dan mengamati respon. A3 COM128 adalah algoritma dalam *simcard* yang digunakan untuk mengenkripsi *simcard* terhadap piranti selullar keduanya algoritma *checksum* hasil dari perhitungan KI A3 COM 128 diharapkan dapat

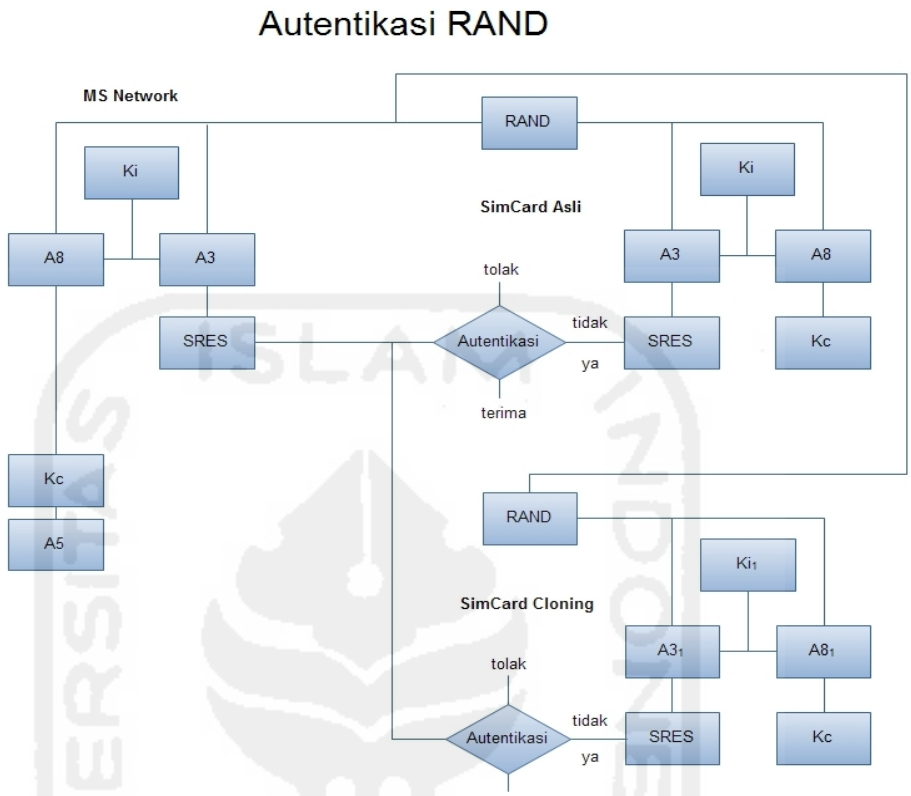
1) Mengetahui respon terhadap jaringan selullar pasca *simcard* dikloning.
2) Mengakumulasi autentikasi respon dan menghitung kunci enkripsi KI.
3) A3 COM128 dan A8 COM128. Kemungkinan memodifikasi algoritma atau hanya mendistribusikan kartu SIM diubah serta memodifikasi AUCs *(Authentication Center).*

4) Pengaruh lalu lintas dari ponsel pengguna ke *base station simcard* yang telah dikloning terhadap *simcard* yang masih terenkripsi.

3.5 RAND Autentication

(Isomäki, November 29, 1999) SIM dan AuC. Jika AuC terganggu, identitas semua pelanggan dapat dipalsukan. Telah dilaporkan bahwa kloning kartu SIM mungkin terjadi, dan dengan metode ini identitas pengguna dari pelanggan tunggal dapat dipalsukan atau digandakan, hal ini membutuhkan akses ke kartu dan jika kedua nyata dan *simcard* kloning dapat digunakan secara bersamaan, hal tersebut dapat terjadi dikarenakan sistem deteksi penipuan operator hanya berupa sinyal peringatan. Aspek penting lain dari otentikasi GSM adalah kekuatan algoritma A3. Pada prinsipnya A3 dimiliki operator selular tertentu, akan tetapi penggunaan mungkin sebagian operator algoritma yang sama. Berdasarkan pernyataan Isomaki diatas selanjutnya dikomparasi antara algoritma autentikasi *Random Number Generator* (RAND) dan Sign Respon (SRES), jika *key* (Ki) dapat diekstraksi dari *simcard* asli maka pengguna atau pihak ketiga diluar operator akan mampu membuat duplikat *simcard*. Algoritma A3 dan A8 menentukan *inpu*t (RAND dan Ki) dan *output* (SRES dan Kc) dari masing-masing algoritma. COMP128 adalah sering dikenal sebagai fungsi *hash*, (RAND dan Ki) menghasilkan nilai 32-bit (SRES). Karena terdapat banyak kemungkinan nilai-nilai RAND dan Ki dapat diubah maka, ada kemungkinan bahwa lebih dari satu nilai RAND akan menghasilkan SRES yang sama. Hal ini dikenal sebagai *cloning simcard*, dan dalam kasus COMP128 cenderung menduplikasi informasi tentang Ki. *Autentication* berdasarkan keamanan GSM pada kerahasia *autentication key* (Ki) dapat dilihat pada Gambar 3.4

.



Gambar 3.4 Flowchart RAND Autentication

Pelaku *cloning* melalui proses pemilihan nilai-nilai yang tepat dari RAND, pengkloning akhirnya dapat menentukan nilai Auc Ki dengan memeriksa kebocoran SRES. Serangan ini dengan mengeluarkan kunci rahasia Ki dan mengeksekusi algoritma otentikasi COMP128 serta memeriksa hasil bersama nilai Ki, selanjutnya kunci rahasia Ki disalin ke kartu SIM lain dan secara efektif terjadilah kloning *simcard* seperti Gambar 3.4 diatas.

3.6 Analisis Forensik Simcard Cloning

Kartu SIM adalah kartu pintar, yang berisi prosesor dan memori *non-volatile*. Di GSM, kartu SIM yang digunakan sebagai perangkat penyimpanan data pelanggan terkait. Satu-satunya tujuan dari prosedur ini adalah untuk menerapkan mekanisme akses dan fitur keamanan. Kartu SIM dapat diakses dengan me-*mount* kartu dengan pembaca *Smartcard Reader* standar. Untuk mengakses kartu diperlukan perangkat lunak

sebagai pembaca atau akses GSM SIM. Isi kartu SIM merupakan sebagian dari rangkaian file yang berisi data biner yang dapat di-*download* sesekali pengguna telah dikonfirmasi dirinya dengan atau tanpa kode PIN atau PUK. Prosedur forensik terbaik akan gambaran seluruh isi 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 uantuk menyinkronkan data seperti pesan teks antara kartu SIM dan computer seperti *Sim Manajer Pro*. Alat tersebut harus dihindari dalam analisis forensik, karena isi dari kartu akan terkontaminasi. Alat saat ini yang paling populer dimasyarakat penegakan 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.

Tabel 3.5 Tabel Proses Investigasi Simcard Cloning(Gubian, 2011)

Indentifikasi	**Preservasi**	**Collection**	**Examination**	**Analisis**	**Presentasi**
Identifikasi kejahatan Simcard	Pengolahan kasus Simcard	Pengamanan barang bukti Simcard	Pelacakan barang bukti Simcard	Kompasrasi data investigasi	Dokumentasi
Profil kejahatan Simcard	Chain of custody/ kronologis Simcard Cloning	Teknik investigasi Simcard	Validasi barang bukti Simcard	Pengolahan temuan barang bukti	Klarifikasi invistigator

Tabel 3.5 Tabel Proses Investigasi Simcard Cloning (Lanjutan)

Audit dan analisa kasus	Manajemen waktu investigasi		Filtering barang bukti		Pernyataan, saran dan tindakan
	Pengolahan kasus Simcard		Pencocokan barang bukti		Interpretasi data Simcard
			Penemuan data tersembunyi		

Tabel 3.5 bersumber dari tabel *Investigative process for Digital Forensic Science* DFRWS (DTR-T001-01, 2001). Berdasarkan tabel proses diatas kemudian dikondisikan dengan proses penanganan *digital evidence* terkait *simcard cloning* maka dapat diperoleh tabel investigasi pengembangan *Digital Evidence Subscriber Identity Module SIM* yang berisikan informasi yang dapat dinilai sebagai bukti digital meliputi nama penyedia jaringan atau *provider* selullar yang dicetak pada *device simcard*, bersamaan dengan nomor identifikasi serta dapat digunakan untuk mendapatkan informasi dari penyedia berupa nama pelanggan, alamat dan nomor telepon yang dikaitkan dengan *simcard*, selain itu catatan telepon juga dapat diambil dari nomor ini sebagaimana dijelaskan dibawah ini :

1) Location Register

   Location Register (VLR). VLR dapat dikaitkan dengan satu atau beberapa MSC. Data ini diperbarui dengan meng-*update* dari *Mobile Station* MS melalui MSC, atau langsung dari pelanggan *Home Location Register* (HLR). HLR adalah data register pelanggan. Informasi *subscribtion*, layanan diperkenankan, informasi otentikasi dan lokalisasi pelanggan yang setiap saat disimpan dalam HLR. Informasi ini dapat diperoleh oleh VLR / MSC bila diperlukan seketika

pelanggan menjelajah ke daerah lokasi VLR lain / MSC, maka HLR secara otomatis memperbaharuinya.

2) Equipment Identity Register

Equipment Identity Register (EIR). Tujuannya adalah untuk mendaftar Imei dari mobile station yang digunakan. Dengan menerapkan EIR penyedia jaringan dapat mem-*blacklist* nomor *simcard* yang dicuri, hilang atau rusak, sehingga penggunaannya tidak diperbolehkan mengakses jaringan dalam waktu tertentu.

3) Akses ke SIM

PIN-kode *(Personal Identification Number)* biasanya diperlukan untuk mengakses SIM. Jumlah ini merupakan kode empat digit yang harus dimasukkan untuk mendapatkan akses. Karena ponsel tidak dapat digunakan tanpa akses ke SIM. PIN-kode untuk kartu dapat diubah dan dinonaktifkan oleh pengguna. PUK-kode yang tetap dan tidak dapat diubah. Karena PUK-kode adalah tetap, operator jaringan biasanya melacak PUK-kode untuk semua penggunanya. Oleh karena itu, penyidik dapat hampir selalu mendapatkan akses untuk *simcard* dengan meminta operator jaringan untuk kode PUK. Dengan demikian, memungkinkan bagi penyidik untuk menentukan dimana lokasi di area ponsel ini terletak ketika terakhir beroperasi. Operator jaringan dapat membantu penyidik dalam mengidentifikasi daerah lokasi.

4) Pesan teks atau Short Message Service (SMS)

Layanan dasarnya memungkinkan jenis pengguna dalam pesan teks singkat dan mengirimkannya ke pengguna lain melalui *Short Message Service Centre* pusat (SMSC). SIM menyediakan ruang penyimpanan untuk pesan teks. Kebanyakan SIM-card memiliki 12 slot untuk teks-pesan. Selain itu, sebagian telepon modern juga membiarkan pesan teks user menyimpan dalam memori ponsel maupun *simcard*.

5) Number Short Dial

Untuk membantu pengguna dalam mengingat angka, kebanyakan ponsel memiliki kemampuan untuk menyimpan nomor telepon yang

biasa dipanggil. Kebanyakan *SIM-card* memiliki sekitar 100 slot untuk menyimpan nomor panggilan singkat. Dalam SIM, nomor pendek disimpan dalam format biner, yang berisi nama dan nomor disetiap slot. Program seperti *Simcard Seizure* akan men-*decode* format nomor tertentu. Ketika nomor dihapus, informasi dalam slot ditimpa dengan nilai *hex* FF. Dengan demikian, kemungkinan untuk memulihkan nomor yang dihapus. Slot nomor biasanya akan dialokasikan secara berurutan, sehingga mengidentifikasi slot kosong diantara slot yang digunakan biasanya akan menunjukkan bahwa nomor yang tersimpan telah dihapus.

6) Recent Call atau Log Panggilan

   SIM juga memiliki kemampuan untuk menyimpan nomor keluar terakhir. Kebanyakan kartu hanya terdapat 5 slot. Angka-angka yang disimpan dalam biner dikodekan format yang dapat diinterpretasikan oleh program *Simcard Seizure*. Penyidik dalam hal ini diperlukan untuk mengetahui *log* panggilan keluar ketika *simcard* telah dikloning.

7) Simcard File System

   Kartu SIM berisi sistem file hirarki yang berada di EEPROM. Struktur file terdiri dari *Master File* (MF), yang merupakan akar dari sistem file, *Dedicated File* (DF), dan SD *Elementary Files* (EF). File *Dedicated* direktori bawahan di bawah MF, isinya dan fungsi yang didefinisikan oleh standar GSM. *Dedicated file* atau DF terdiri dari DF (DCS1800), DF (GSM), dan DF (Telecom). Sedangkan dalam MF berisikan EF (ICCID). Sementara semua file memiliki *header*, hanya EF berisi data. *Byte* pertama dari header mengidentifikasi jenis file. *Header* mengandung keamanan dan informasi yang berkaitan dengan struktur dan atribut *file*. Struktur EF berisi informasi yang berkaitan dengan aplikasi *file* yang dapat berupa aplikasi tertentu dan akses ke data yang tersimpan dikendalikan oleh sistem operasi.