FORENSIC SIMCARD CLONING
MENGGUNAKAN ALGORITMA AUTENTIKASI
RANDOM NUMBER GENERATOR (RAND)

Oleh : Nuril Anwar
12917210

ABSTRAK

Kejahatan dalam sektor telekomunikasi merupakan hal yang merugikan baik bagi *customer* maupun *provider* selullar. Pada sistem keamanan jaringan GSM, ditemukan beberapa kelemahan yang terjadi pada pengamanan data diluar jaringan. *Simcard cloning* merupakan bagian dari masalah keamanan yang terdapat pada *device simcard*. Beberapa *authentication algorithm simcard* GSM dapat ditembus dengan alat tertentu sehingga seluruh data dalam *simcard* dapat pula dipindahkan ke media *simcard* kloning lain.

Fokus penelitian dengan melakukan *cloning simcard* serta menganalisis algoritma A3 SRES, dan A8 RAND untuk mendapatkan Ki AUc dan selanjutnya dilakukan proses investigasi forensik hasil *cloning simcard*. Analisis untuk menguji performansi metode kloning yang meliputi proses registrasi *simcard* terhadap jaringan selullar, *call setup*, dan data akses dengan menggunakan parameter pengujian *Due Under Test* (DUT) dan *Trial and Error*.

Berdasarkan hasil proses *cloning simcard* penelitian ini diperoleh analisa *simcard cloning* terkait prosentase tingkat keberhasilan berdasarkan kapasitas memori *simcard* antara 32kb, 64kb dan 128kb dengan tingkat prosentase keberhasilan antara 25% - 100%, serta generasi antar *simcard* berdasarkan tahun produksi. Investigasi forensik terhadap *simcard cloning* yaitu dengan pencocokan algoritma A8 (RAND) yang terdapat pada *simcard* asli terhadap algoritma hasil *generate* RAND yang menghasilkan autentikasi Ki serta penemuan data pendukung investigasi yang terdapat pada struktur *file simcard*.

Kata kunci : *Authentication, Cloning, Forensic,* RAND, *Simcard* dan SRES.