ANALISIS RECOVERY KODE POLA DAN KODE KATA SANDI ANDROID

Hendra Kuswanto[1], Rusmin Syafari[2], Timur Dali Purwanto[3]

[1]Universitas Bina Darma
Jalan Jenderal Ahmad Yani No.03 Palembang, 30264
[1]Email:h12142218@gmail.com

[2]Universitas Bina Darma
Jalan Jenderal Ahmad Yani No.03 Palembang, 30264
[2]Email: rusmin.syafari@binadarma.ac.id

[3]Universitas Bina Darma
Jalan Jenderal Ahmad Yani No.03 Palembang, 30264
[3]Email: timoerok@gmail.com

ABSTRAK

Abstrak : *Smartphone* android merupakan ponsel pintar yang pada saat ini berkembang pesat dan digunakan tidak hanya untuk berkomunikasi melalui telepon dan pesan singkat atau sms. Kedudukan smartphone bisa dibilang dapat membantu aktifitas para pengguna-nya baik dalam melakukan pekerjaan kantor, bisnis, *E-Banking* ,maupun untuk berinteraksi dengan pengguna lain nya di media sosial. Oleh karena itu keamanan sebuah smartphone menjadi prioritas utama para pengguna-nya untuk mengamankan data mereka dari orang yang lain. Salah satu keamanan yang sering digunakan oleh pengguna adalah kode keamanan layar dalam mengamankan smartphone, sehingga dapat mempersulit orang lain untuk masuk tanpa izin kedalam layar utama smartphone tersebut. Dibalik keamanan tersebut dapat menjadi tantangan bagi IT forensik dan penegak hukum untuk melakukan penyelidikan terhadap smartphone dari seseorang yang dijadikan tersangka dari sebuah kasus.

Kata kunci: Analysis Forensic *Recovery*, Keamanan Kode, Android.

I. PENDAHULUAN

Dibalik perkembangan *smartphone* tersebut faktor keamanan *smartphone* tersebut merupakan perhatian utama para pengguna-nya. Selain untuk menjaga data pribadi dari resiko pencurian data terhadap smartphone tersebut. Maka hal pertama yang dilakukan oleh pengguna (*user*) adalah dengan mengamankan hak akses ke dalam layar utama *smartphon*e-nya. Baik dengan kode pola, *pin*, kata sandi maupun menggunakan identifikasi muka si pemilik *smartphone*. Hal tersebut dapat meminimalisirkan kemungkinan orang yang tidak bertanggung jawab untuk mengakses *smartphone* tanpa izin dari sang pemilik. Keamanan ini juga menjadi tantangan bagi IT forensik dan penegak hukum untuk melakukan penyelidikan terhadap *smartphone* dari seseorang yang dijadikan tersangka dalam sebuah kasus. Banyak cara untuk menghilangkan kode akses keamanan layar pada *smartphone*, salah satu cara yaitu dengan melakukan *factory data reset* atau mengembalikan smartphone ke kondisi awal dari pabrik. Akan tetapi cara yang dilakukan ini dapat menghapus semua data-data yang tersimpan di *memory internal smartphone* tersebut. Sedangkan untuk melakukan suatu penyidikan, data didalam suatu smartphone yang bisa dijadikan barang bukti digital tidak boleh hilang satu pun selama proses penyidikan dilakukan.

Data yang bisa dijadikan barang bukti seperti sms, telepon, kontak telepon, *history chatting*, dan lain-lain baik yang tersimpan dalam memori smartphone maupun yang ada didalam ram smartphone tersebut, sesuai dengan undang-undang ITE nomor 11 tahun 2008 pasal 5 ayat (1)) UU ITE mengatur bahwa Informasi Eletkronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

II. METODE PENELITIAN

Pada penelitian ini penulis menggunakan metode model proses forensik (*The Forensic Process Model*), dengan langkah-langkah sebagai berikut :

1) Mengidentifikasi Masalah

Tahap ini adalah tahap diamana peneliti melakukan analisis terhadap masalah yang dihadapi yaitu bagaiman cara melewati sistem keamanan layar dengan kode pola ataupun kode kata sandi pada smartphone yang terkunci dengan kode pola dan kode kata sandi serta apakah perangkat android telah diaktifkan usb debuging untuk mempermudah proses untuk menghilangkan sistem keamanan layar android. Hal ini dapat

membantu untuk menentukan teknik apakah yang akan digunakan dalam proses untuk menghapus kunci keamanan layar dengan kode pola dan kode kata sandi pada smartphone android.

2) Mengajukan Solusi

Pada tahap ini, peneliti mengajukan solusi yang mungkin untuk dilakukan dalam pemecahan masalah dari hasil identifikasi masalah dan informasi dari hasil tahap pertama. Solusi dalam pemecahan masalah dari hasil tahap pertama adalah membuka keamanan kode pola atau kode kata sandi pada *smartphone.* Hal ini dapat dilakukan dengan menggunakan 3 teknik sebagai berikut.

3) Pengujian

Pada tahapan ini peneliti akan melakukan pengujian pada *smartphone* android dengan menerobos keamanan kunci layar berupa keamanan kode pola maupun keamanan kode kata sandi.

4) Menyelesaikan Prosedur

Pada tahapan terakhir ini peneliti akan menyelesaikan prosedur dengan menggunakan metode deskrptif. Metode deskriptif dapat diartikan sebagai prosedur pemecahan masalah yang diselidiki dengan menggambarkan keadaan subjek atau objek dalam penelitian dapat berupa orang, lembaga, masyarakat dan yang lainnya yang pada saat sekarang berdasarkan fakta-fakta yang tampak atau apa adanya.

Menurut Nazir (1988: 63), metode deskriptif merupakan suatu metode dalam meneliti status sekelompok manusia, suatu objek, suatu set kondisi, suatu sistem pemikiran ataupun suatu kelas peristiwa pada masa sekarang. Tujuan dari penelitian deskriptif ini adalah untuk membuat deskripsi, gambaran, atau lukisan secara sistematis, faktual dan akurat mengenai fakta-fakta, sifat-sifat serta hubungan antarfenomena yang diselidiki.

III HASIL

A. Pengumpulan (*Preservation*)

Pada tahap ini peneliti melakukan pengumpulan dan pendokumentasian barang bukti. Pada penelitian ini yang menjadi barang bukti yaitu berupa smartphone yang diskenariokan sebagai barang bukti dalam kasus kejahatan. Setelah barang bukti dikumpulkan kemudian dilakukan pendokumentasian dengan mencatat merek, model serta hail lain yang berkaitan dengan smartphone tersebut.

B. Mengidentifikasi Masalah

Setelah tahapan pengumpulan (*preservation*) telah dilakukan, maka selanjutnya adalah melakukan tahap mengidentifikasi masalah pada smartphone tersebut. Tahapan ini merupakan tahap awal untuk mengumpulkan data-data yang diperlukan selama proses forensik, serta mendapatkan gambaran secara umum untuk langkah yang harus diambil pada tahap selanjutnya. Masalah yang dihadapi dalam penelitian ini adalah barang bukti berupa smartphone terpasang kunci keamanan layar berupa kode pola dan kode kata sandi dan bagaimana cara melewati sistem keamanan layar dengan kode pola dan kode kata sandi tanpa merusak data-data yang ada didalam smartphone android tersebut untuk mendapatkan bukti lainnya. Berikut merupakan masalah yang dihadapi pada smartphone tersebut.

C. Melakukan Pengujian

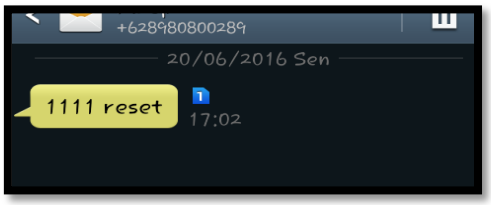
Setelah mengetahui masalah yang dihadapi pada barang bukti, peneliti melakukan pengujian pada barang bukti dengan menerobos keaman kunci layar berupa kode pola dan kode kata sandi tanpa merusak data didalamnya. Ada beberapa cara dalam melakukan pengujian pada barang bukti, seperti menggunakan tool ADB (*Android Debug Bridge*), *SMS Bypass* dan file *Aromafilemanager.zip*

1) Percobaan menggunakan ADB pada *evidence*

Gambar 1 ADB terhubung pada *evidence*

Setelah smartphone telah terbaca oleh cmd maka selanjutnya menghapus kode kemanan layar pada smartphone dengan cara mengetikan adb shell pada jendela *window command prompt* kemudian ketikan su untuk masuk ke super user pada smartphone setelah itu masuk ke data system pada smartphone dan hapus kode keamanan layar layar seperti dijelaskan pada Gamabr 1, setelah selesai maka dengan sendirinya kode keamanan layar akan hilang, walapun masih terpasang kode pola coba saja sembarang gambar pola dan akan masuk pada perangkat smartphone.

2) Percobaan menggunakan *SMS Bypass* pada *evidence*

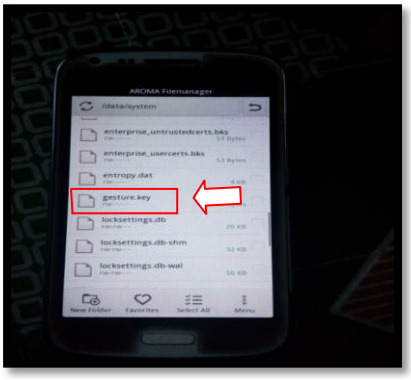


Gambar 2 SMS menggunakan kode reset *sms bypass*

Cara menggunakan *software sms bypass* sangatlah mudah, hanya dengan sms ke nomor target dengan format "1111 reset" maka smartphone target yang disms akan merestart otomatis dan kemanan kunci layar pun hilang.

3) Percobaan menggunakan *Aromafilemanager.zip* pada *evidence*

Setelah masuk pada file aromamanager.zip, sekarang hapus keamanan kunci layar yang berada pada data kemudian system, cari *gesture.key* untuk kode pola dan *password lock* untuk kode kata sandi, hapus file tersebut,



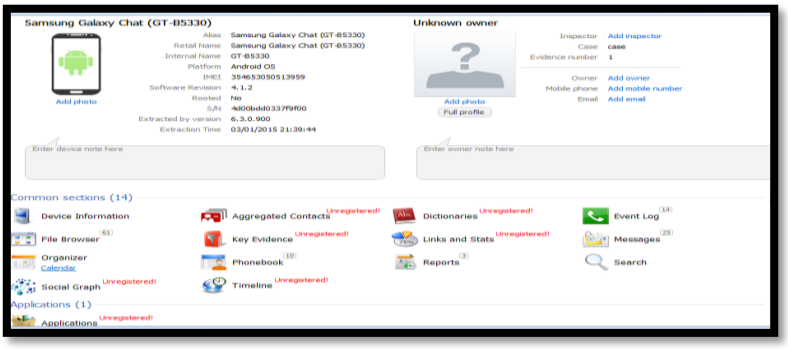
Gambar 3 File kode pola

setelah dihapus, *reboot smartphone* dan otomatis kunci keamnan layar akan hilang apabila msh terpasang kunci layar, coba saja sembarang untuk membukanya.

D. Melakukan Evaluasi

1) Hasil Analisis Menggunakan *Oxygen Forensic*

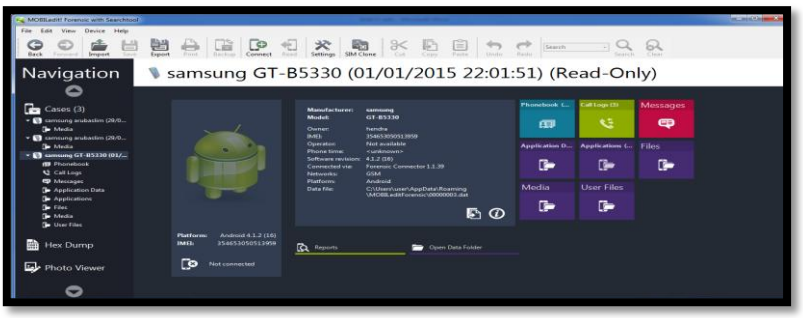
Setelah dilakukan pengujian terhadap *smartphone* yang terpasang kunci keamanan layar berupa kode pola dan kode kata sandi dengan menggunakan teknik yang dilakukan telah mendapatkan hasil bahwa semua data yang ada pada smartphone tersebut tidak ada yang hilang ataupun terhapus, berikut langkah-langkah serta hasil dari *tool oxygen* forensik yang dilakukan sebelum dan sesudah pengujian.



Gambar 4 Hasil *tool Oxygen Forensic*

Pada gambar diatas adalah tampilan hasil dari tool oxygen forensik dimana pada hasil tersebut mendapatkan beberapa file berupa *Device Information, File Browser, Organizer, Social Graph, Aggregated contacts, Key Evidence, Phonebook, Timeline, Dictionaries, Links and State, Reports, Event log, Message*s dan *Search.*

2) Hasil Analisis Menggunakan *MOBILedit*



Gambar 5 Hasil analisis menggunakan *tool MOBILedit*

E. Tabel Perbandingan

Tools	***Call Log***	***SMS***	***Phonebook***	***Aplikasi***	***File Browser***
Oxygen	✓	✓	✓	×	✓
MOBILedit	✓	✓	✓	✓	×

Pada tabel perbandingan menjelaskan bahwa aplikasi yang digunakan berupa aplikasi *oxygen forensic* dan aplikasi *MOBILedit* dari kedua aplikasi yang digunakan mendapatkan hasil yang berbeda. *Pada oxygen* data yang didapatkan berupa *call log*, sms, *phonebook* dan *file browser* sedangkan pada *aplikasi MOBILedit* data yang didapatkan berupa *call log*, sms, *phonebook* dan aplikasi. Hasil yang tidak didapatkan menggunakan *oxygen forensic* berupa aplikasi sedangkan menggunakan *MOBILedit* data yang tidak didapatkan berupa *file browser*.

IV. SIMPULAN

Setelah melakukan uji coba dan analisis *recovery* kode pola dan kode kata sandi pada perangkat *Smartphone* (*Android*), maka disimpulkan :

1) Semua teknik yang digunakan menggunakan ADB (*Android Debug Bridge*), *SMS Bypass* dan *Aromafilemanager.zip* semuanya berhasil, tidak ada yang hilang maupun rusak. Pada teknik yang digunakan menggunakan *Aromafilemanager.zip* terdapat kesulitan karena untuk menggunakan file tersebut harus terlebih dahulu terpasang *CWM* atau *TWRP* pada *smartphone.*
2) *Tool oxygen forensic* yang digunakan untuk evaluasi hasil pengujian pada smartphone, bisa dikatakan kurang bagus karena banyak hasil yang tidak bisa diakses dikerenakan lisensi yang terbatas.
3) Berdasarkan hasil yang didapat menggunakan aplikasi *oxygen forensic* dan aplikasi *MOBILedit* terdapat perbedaan karena pada *oxygen forensic* tidak mendapatkan data aplikasi sedangkan *MOBILedit* tidak mendapatkan data *file browser.*

DAFTAR PUSTAKA

Gogolin, G. 2013. *Digital Forensics Explained*. USA: Taylor & Francis Group.

Hukum pidana narkotika. http://www.resnarkoba-metro.org

Salbino, S. 2014. *Buku Pintar Gadget Android untuk Pemula*. Jakarta: Kunci Komunikasi.

Riandy, O. 2015. *Analisis Forensic Recovery dengan Keamanan Kode Pola pada Smartphone Android*, di Student Colloquium Sistem Informasi & Teknik Informatika (SC-SITI), Palembang, 21-22 Agustus 2015.

Yadi, I. Z. & Kunang, Y. N. 2014. *Analisis Forensik pada Platform Android*, di Konferensi Nasional Ilmu Komputer (KONIK2014), Makassar, 2014

Palembang, 3 September 2016

Penulis,

(Hendra Kuswanto)

Menyetujui,

Pembimbing Utama,	Pembimbing Pendamping,
(Rusmin Syafari)	(Timur Dali Purwanto)