Purwarupa Forensik BBM di Telepon Seluler Android Menggunakan IGN-SDK

Dedy Hariyadi[1], Eka Tresna Irawan[2]
Jurusan Teknik Elektro dan Teknologi Informasi FT UGM[1], Woolu Aksara Maya[2]
dedy.h@ugm.ac.id[1], ibnu@aksaramaya.com[2]

Abstract

The growth of mobile phones in 2014 has experienced a high growth in the global market. it affects the growth and development of the use of messaging applications that run on mobile phones. Certainly the use of the Internet or data access on mobile phones is also increasing. It was noted that Internet data usage of mobile phones is quite large when the president election on July 9th 2014. The popular messaging applications in Indonesia are BBM, WhatsApp, LINE, and Yahoo Messenger. The popularity of messaging applications is possible utilizing digital crime as communication media. Application for doing forensic the outcome conversation of mesaging applications required by the investigator or the field of digital forensics expert staff. Therefore it is necessary to design forensics application that has function same as messaging application like blackberry messanger that is widely used in Indonesia. BBM forensics application design using BSD licensed development tools named IGN-SDK.

Keywords: forensics, bbm, ign-sdk, messenger, smart phones

Abstrak

Pada tahun 2014 telepon seluler mengalami pertumbuhan yang tinggi dipasar global. Hal ini mempengaruhi pertumbuhan pengembangan dan penggunaan aplikasi messaging yang berjalan pada telepon seluler. Tentu penggunaan akses internet atau data pada telepon seluler juga meningkat. Tercatat penggunaan data internet cukup besar dari telepon seluler saat pemlihan presiden 9 Juli 2014. Aplikasi messaging populer di Indonesia diantaranya BBM, WhatsApp, LINE, dan Yahoo Messenger. Dengan populernya aplikasi messaging tersebut tidak menutup kemungkinan tindak kejahatan digital memanfaatkan sebagai media komunikasi. Aplikasi untuk memforeksik hasil percakapan aplikasi messaging diperlukan oleh penyidik atau staf ahli bidang forensik digital. Oleh sebab itu perlu dirancang aplikasi forensik aplikasi messaging semisal BBM sebagai aplikasi messaging yang banyak digunakan di Indonesia. Perancangan aplikasi forensik BBM menggunakan piranti pengembangan berlisensi BSD, yaitu IGN-SDK.

Kata kunci: forensik, bbm, ign-sdk, messenger, telepon seluler

1. Pendahuluan

Gartner mencatat pertumbuhan perangkat elektronik seperti telepon seluler (ponsel), tablet ataupun hibrida antara ponsel dan tablet secara global mengalami peningkatan dari tahun 2013 sampai dengan 2015. Masih dalam catatan *Gartner* pertumbuhan sistem operasi pada ponsel seperti *Android*, *iOS* dan *Windows Mobile* juga mengalami peningkatan. Total pertumbuhan mencapai 6,9% di tahun 2014[1].

Pertumbuhan aplikasi hingga saat ini berbanding lurus dengan pertumbuhan ponsel pintar[2]. Aplikasi tersebut diantaranya *Instant Messenger* seperti di *BBM*, *WhatsApp, LINE, Kakao Talk, WeChat*, dan sebagainya. *On Device* melakukan survey kepada pemilik ponsel pintar di beberapa negara seperti Indonesia, Amerika, Tiongkok, Brasil, dan Afrika Selatan bahwa *Instant Messenger* tertinggi yang digunakan adalah *WhatsApp* sebesar 44% disusul *Facebook Messenger* 35%, *WeChat* 28%, *Twitter* 19%, *BBM* 17% , dan *Skype* 16%. Masih dalam catatan *On Device Instant Messenger BBM* ternyata banyak digunakan di Indonesia dengan nilai prosentase 37%, Afrika Selatan 34% dan Amerika 13% [3].

Dengan meningkatnya penggunaan aplikasi *instant messaging* tidak menutup kemungkinan aplikasi tersebut digunakan untuk mendukung aksi kejahatan sebagai media komunikasinya. *Digital Analysis Forensics Team (DFAT)* Puslabfor Polri pada tahun 2010 telah memeriksa barang bukti sebanyak 214 jenis yang berasal dari 52 kasus dalam berbagai bentuk kejahatan seperti jaringan narkoba, pornografi, perjudian, korupsi pencemaran nama baik, penipuan, penyuapan, dan lain-lain. Dari jumlah tersebut, sebanyak 118 jenis berupa barang bukti ponsel[4].

2. Prinsip Penanganan Barang Bukti Digital

Asosiasi Kepolisian Inggris atau *Association of Chief Police Officers (ACPO)* bekerja sama dengan konsultan keamanan informasi dan forensik, *7Safe* merumuskan prinsip dasar penanganan barang bukti digital. Adapun prinsip dasar penanganan barang bukti digital dari *ACPO* sebagai berikut[5]:

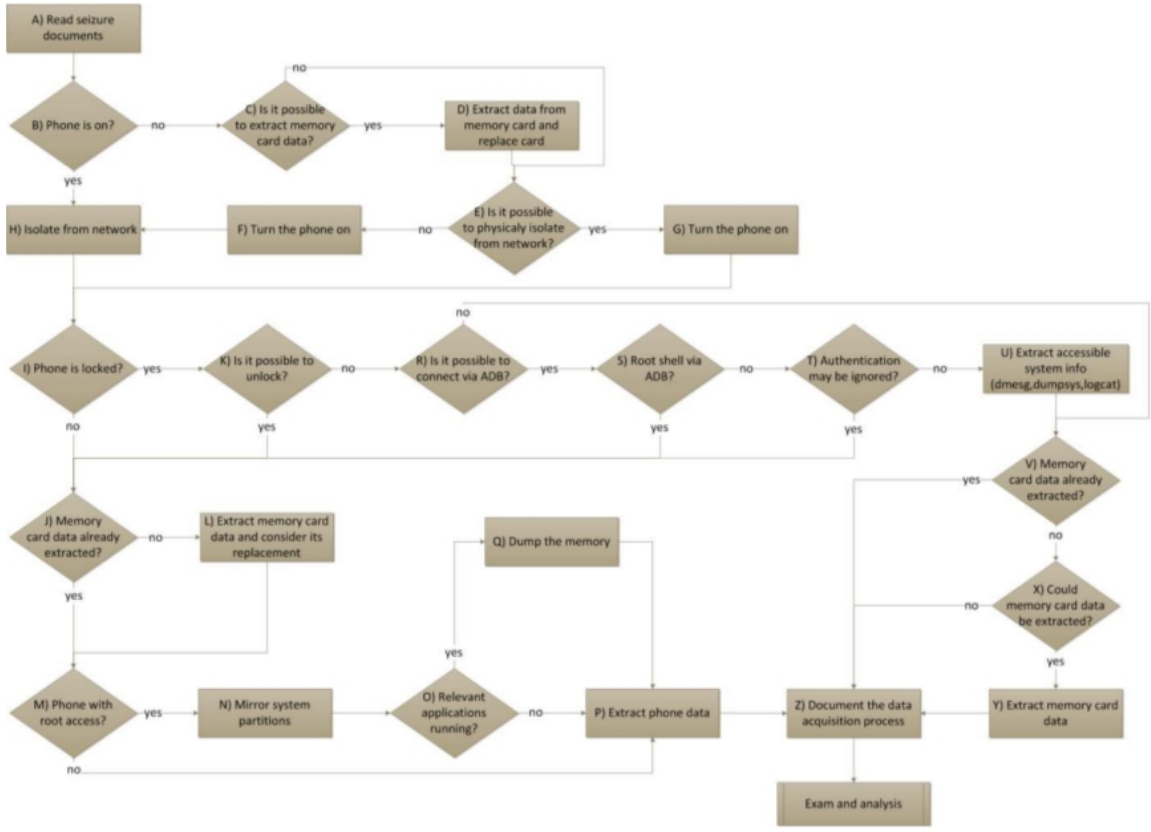
1. *No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.*
2. *In circumtances where a person find it necessary to acces original data held on a computer or storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.*
3. *An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.*
4. *The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.*

3. Prosedur Akuisisi Ponsel Android

Menurut Andre Morum de L. Simao dalam mengakuisisi barang bukti berupa ponsel bersistem operasi android memperhatikan beberapa kondisi diantaranya[6]:

1. Apakah ponsel dalam kondisi hidup
2. Apakah layar ponsel dalam kondisi terkunci
3. Apakah memungkinkan terkoneksi melalui ADB
4. Apakah memiliki akses root

Diagram alur proses akuisisi ponsel bersistem operasi Android menurut Andre Morum de L. Simao dapat dilihat pada gambar 1.



Gambar 1 Diagram Alur Akuisisi Ponsel Android

Seorang penyidik forensik digital harus memastikan integritas barang bukti sebelum dan sesudah mengekstraksi menggunakan *hash.* Jika nilai *hash* cocok antara sebelum dan sesudah proses ekstraksi barang bukti baru boleh dianalisis.

Secara umum *hash* terdiri dari 5 langkah proses untuk menghasilkan *message digest*, yaitu[7]:

1. *Messaging padding*
2. Penambahan panjang bit
3. Inisialisasi *buffer*
4. Memproses 16 Subblok 32 bit
5. *Output*

4. IGN Software Development Kit

Distribusi Linux racikan anak bangsa *Indonesia Go Open Source* Nusantara yang bisa dikenal IGN merilis sebuah *Software Development Kit* yang disebut IGN-SDK. Pada awalnya IGN-SDK dirancang khusus untuk sistem operasi Linux IGN. Saat ini IGN-SDK dapat berjalan di beberapa distribusi Linux populer seperti, ArchLinux, Slackware, openSUSE, Ubuntu, Debian. Menggunakan IGN-SDK dapat untuk mengembangkan aplikasi dari kode HTML dan Javascript[8].

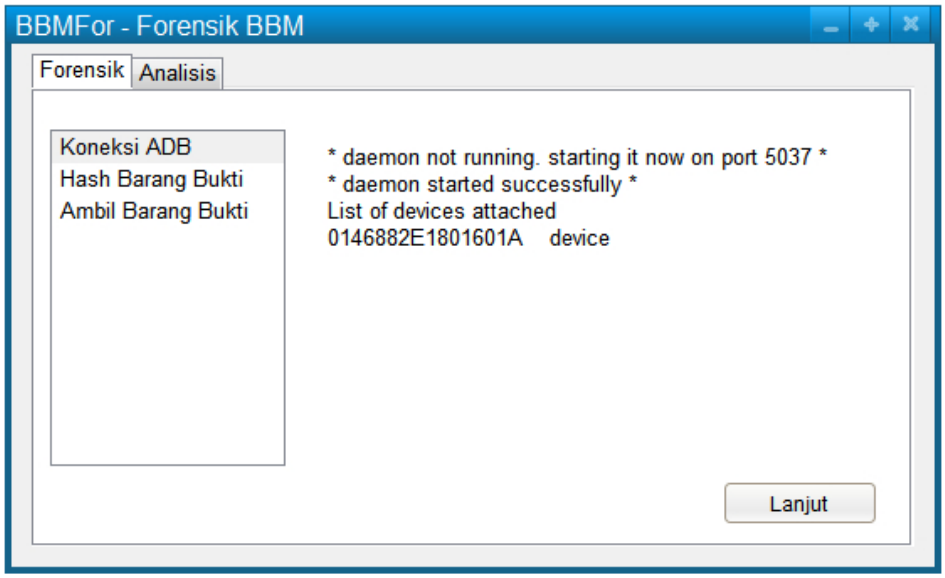
5. Purwarupa Perancangan Forensik BBM

Dalam purwarupa perancangan aplikasi Forensik BBM yang berjalan pada sistem operasi Android dibagi menjadi 2 bagian Forensik dan Analisis. Dalam perancangan aplikasi ini menggunakan prinsip dasar forensik barang bukti digital sesuai ACPO dan proses akuisisi mengikuti prosedur dari Andre Morum de L. Simao. Sedangkan pengembangan aplikasi Forensik BBM menggunakan IGN-SDK.

5.1. Forensik BBM

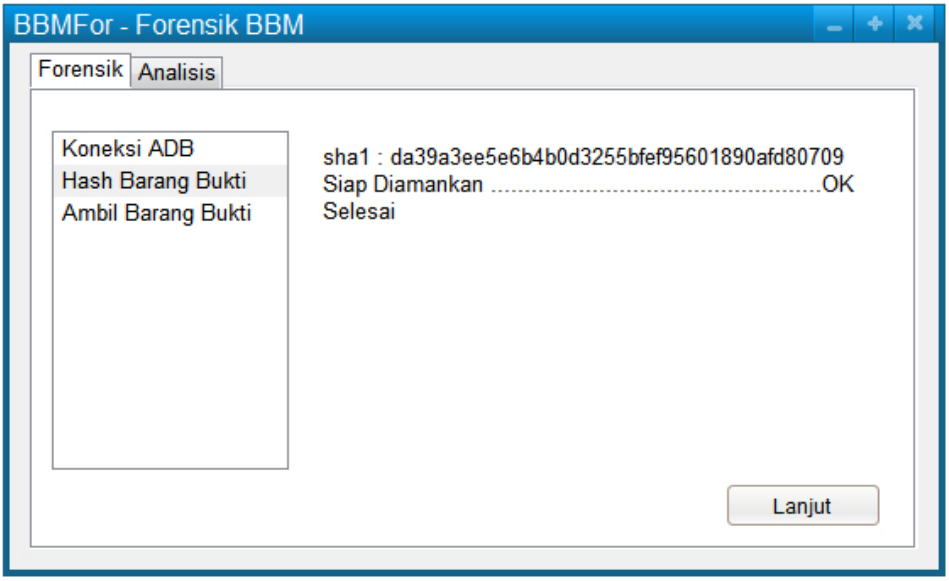
Koneksi untuk tahapan forensik pada ponsel bersistem operasi Android menggunakan ADB. Pada penelitian ini kondisi ponsel sudah ter-*root* dan terinstall *busybox*. Pada tahapan Forensik ini ada 3 tahap, yaitu: Koneksi ADB, Hash Barang Bukti dan Mengambil Barang Bukti.

Mode Development harus diaktifkan untuk memudahkan komunikasi komputer penyidik dengan ponsel bersistem operasi Android. Komputer dan ponsel harus terhubung dengan baik gambar 2 menunjukam proses koneksi berfungsi dengan baik.



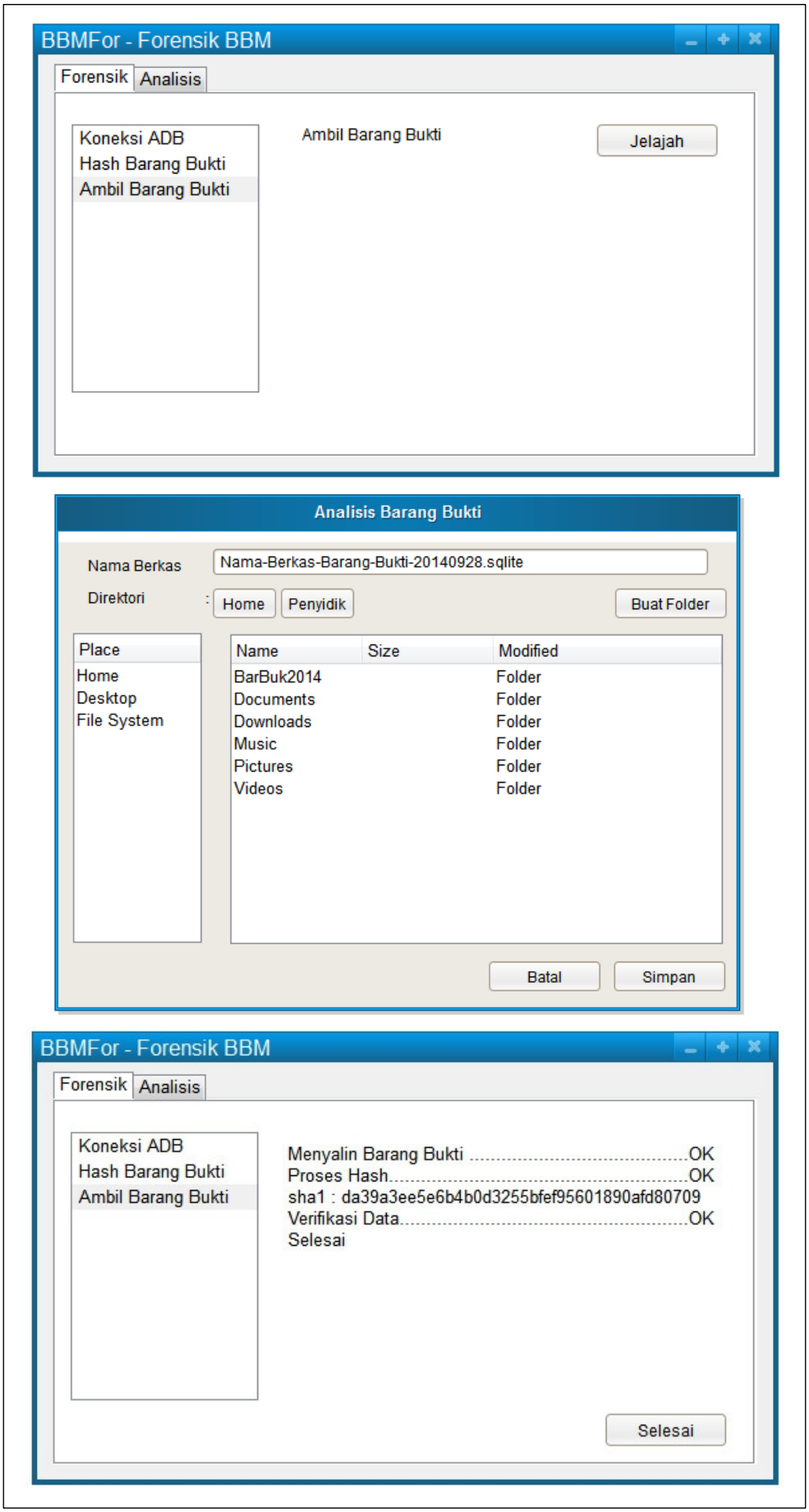
Gambar 2. Koneksi ADB Ponsel

Sebelum barang bukti digital berupa komunikasi BBM disalin ke tempat yang lebih aman harus dilakukan pemeriksaan integritas atau keasliannya menggunakan *sha1sum*. Gambar 3 menunjukan proses hash menggunakan *sha1sum*.



Gambar 3. Proses sha1sum

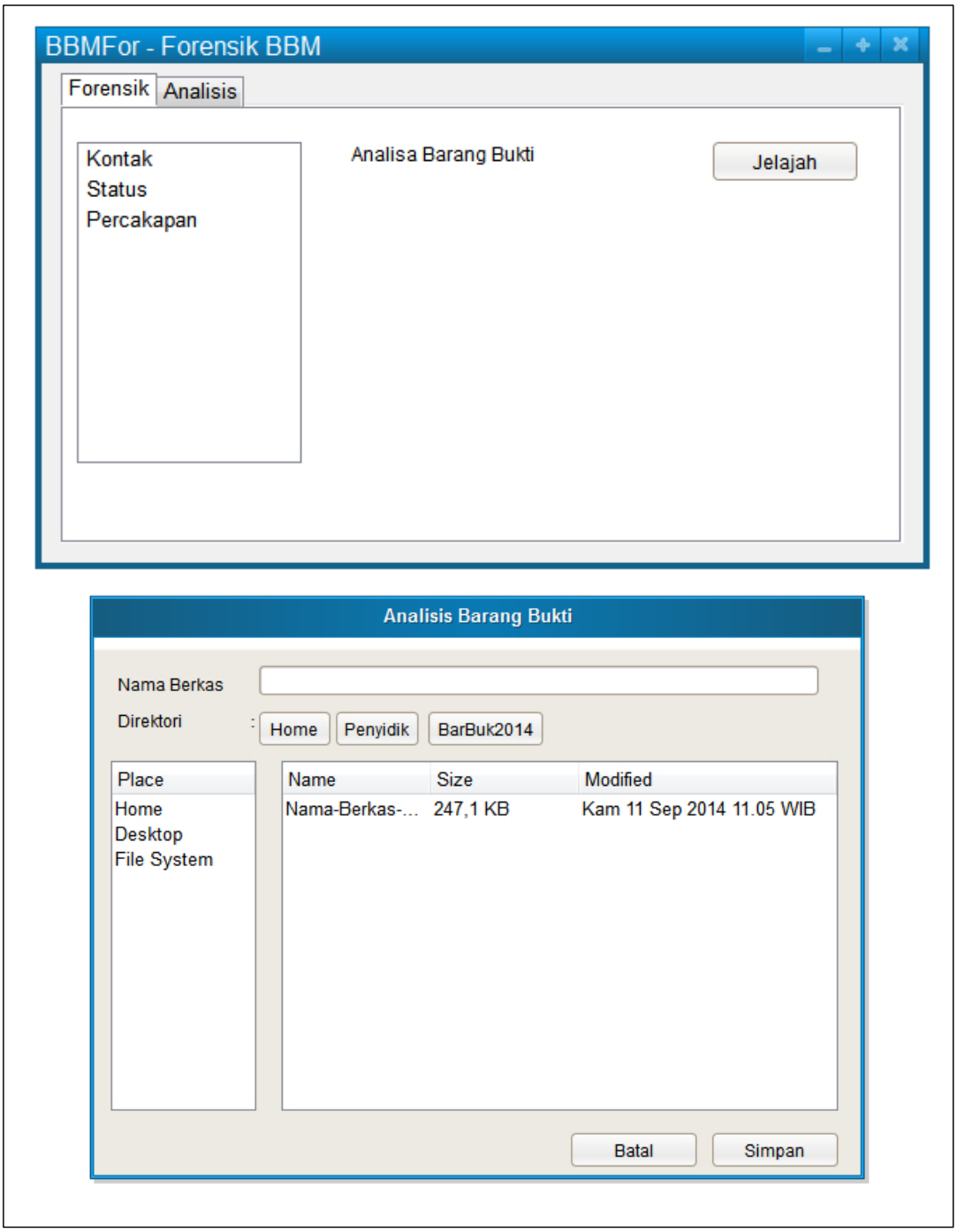
Proses mengambil atau mengamankan barang bukti harus dipastikan bahwa nilai *hash* barang bukti digital komunikasi BBM berupa berkas *sqlite* sebelum disalin dan sesudah salin ke komputer penyidik cocok. Gambar 4 menunjukan proses mengamankan barang bukti digital dan verifikasi terhadap keasliannya.



Gambar 4. Proses Mengamankan dan Verifikasi Barang Bukti

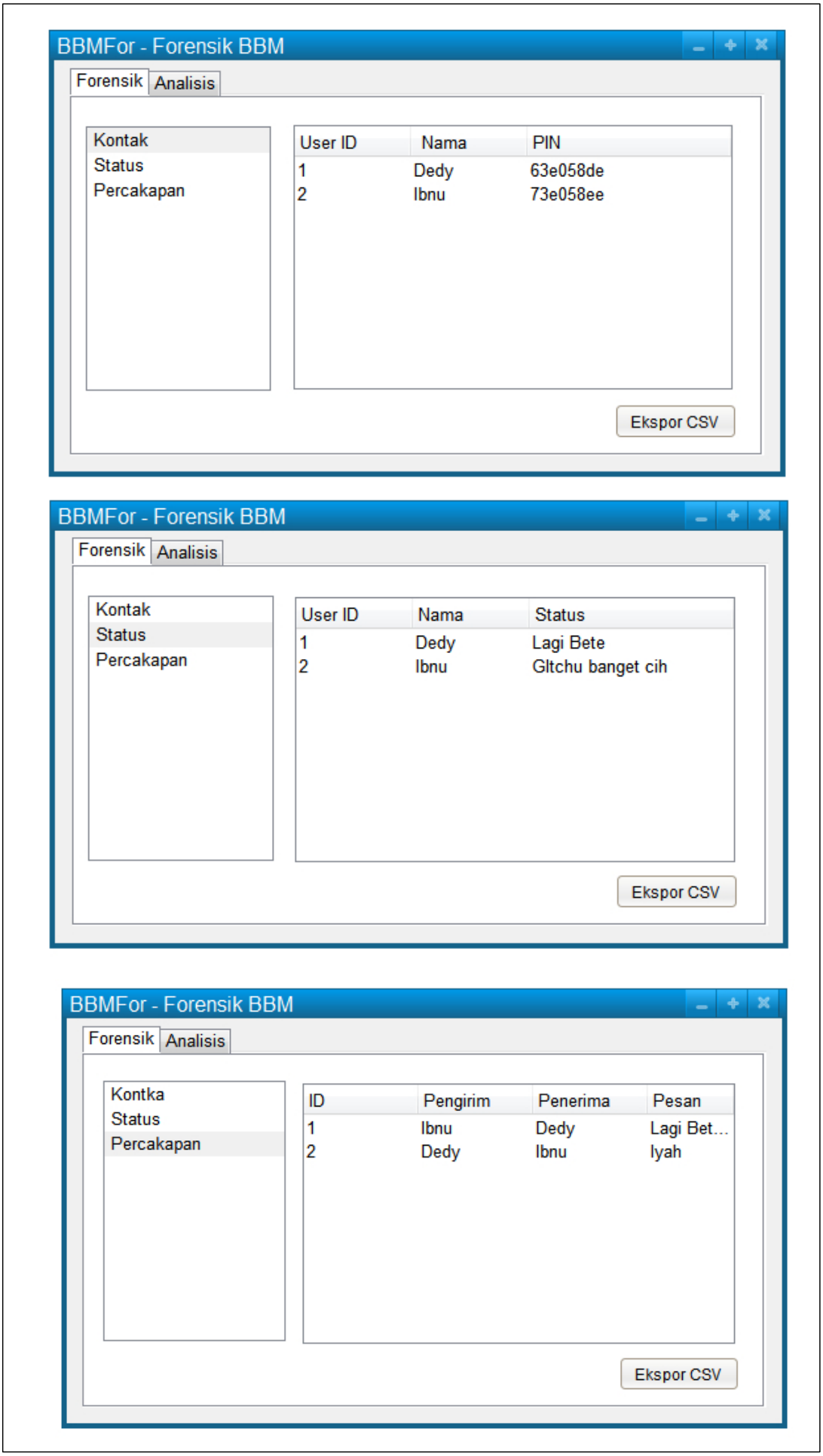
5.2. Analisis BBM

Setelah proses Olah Tempat Kejadian Perkara (TKP), barang bukti dianalisis oleh penyidik atau staf ahli yang ditunjuk. Aplikasi Forensik BBM dapat melakukan analisis barang bukti digital berupa berkas .sqlite. Gambar 5 menunjukan proses awal mengambil barang bukti untuk dianalisis.



Gambar 5. Proses Menambil Barang Bukti

Aplikasi Forensik BBM ini memiliki fitur analisis standar yaitu untuk mengetahui **Kontak** yang berisi Nama dan PIN, **Status** yang biasanya digunakan media eksistensi atau kode tertentu dan **Percakapan** yang berisi data percakapan yang dikelompokan per-pesan. Aplikasi yang diberi nama BBMPork memiliki fitur analisis yang dapat dikonversi ke dalam bentuk berkas *Comma Separated Values* (CSV) seperti pada Gambar 6. Menggunakan CSV untuk mempermudah dalam pertukaran data yang dapat dibuka diberbagai aplikasi *Spreadsheet*, seperti *MS Excel, OpenOffice Calc, LibreOffice Calc, Kingsoft Calc*, dan sebagainya[9].



Gambar 6. Analisis Aplikasi BBMPork

6. Kesimpulan dan Saran

6.1. Kesimpulan

Purwarupa dari perancangan aplikasi BBMPork dapat membantu penyidik atau staf ahli bidang keamanan informasi atau forensik digital untuk menganalisis komunikasi melalui BBM. Fokus perancangan aplikasi forensik dari komunikasi BBM pada ponsel bersistem operasi Android. Proses akuisisi masih bersifat *logical forensics* namun dapat melakukan analisis berkas *sqlite* yang dihasilkan dari proses akuisisi bersifat *physical forensics*.

BBMPork merupakan aplikasi *logical forensics* berlisensi MIT yang dikembangkan menggunakan IGN-SDK dengan fungsi utama untuk melakukan analisis percakapan *BlackBerry Messenger* yang berjalan di ponsel bersistem operasi Android.

6.2. Saran

Pengembangan aplikasi BBMPork masih banyak kekurangan, oleh sebab itu diharapkan kedepan dapat dikembangkan yang mendukung kinerja penyidik atau staff ahli bidang keamanan informasi dan forensik digital. Adapaun saran pengembangan sebagai berikut:

1. Proses Forensik dapat dengan mudah mengenali telepon seluler yang belum ter-*root*.
2. Proses Analisis dapat menampilkan grafik statistika komunikasi BBM.
3. Akhir dari proses Analisis dapat membuat laporan dari proses forensik komunikasi BBM.
4. Penambahan fitur injeksi *busybox* pada proses akuisisi.

7. Daftar Pustaka

[1] Gartner Inc., "Gartner Says Worldwide Traditional PC, Tablet, Ultramobile and Mobile Phone Shipments Are On Pace to Grow 6.9 Percent in 2014," 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2692318. [Accessed: 16-Jul-2014].

[2] "Genjot Industri Kreatif Digital Lokal, Telkomsel Gelar Kompetisi - Liputan6.com," 2013. [Online]. Available: http://tekno.liputan6.com/read/676361/genjot-industri-kreatif-digital-lokal-telkomsel-gelar-kompetisi. [Accessed: 20-Sep-2014].

[3] On Device Research, "Messenger Wars: How Facebook lost its lead," 2013. [Online]. Available: https://ondeviceresearch.com/blog/messenger-wars-how-facebook-lost-its-lead. [Accessed: 20-Sep-2014].

[4] M. N. Al-Azhar, *Digital Forensic: Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek, 2012.

[5] Association of Chief Police Officer, "ACPO Good Practice Guide for Digital Evidence," 2012.

[6] Andre Morum de L. Simao, Fabio Caus Sicoli, Laerte Peotta de Melo, and Rafael Timoteo de Sousa Junior, "Acquisition of digital evidence in android smartphones," *Australian Digital Forensics Conference*, no. December, 2011.

[7] M. Prasetiya, "Perbandingan Algoritma Message Digest 5 (MD5) dan Secure Hash Algorithm 1 (SHA1) untuk Autentikasi," Institut Pertanian Bogor, 2001.

[8] "IGOS Nusantara SDK." [Online]. Available: http://ignsdk.web.id/. [Accessed: 05-Dec-2013].

[9] Y. Shafranovich, "Common Format and MIME Type for Comma-Separated Values (CSV) Files." [Online]. Available: https://tools.ietf.org/html/rfc4180. [Accessed: 30-Sep-2014].