ANALI SIS DAN I MPLEMENTASI DIGITAL FORENS IC ACQUISITION UNTUK M ENEMUKAN DIGITAL EVIDE NCE AKTIVITAS WIFI DAN BLUETOOTH PADA SMARTPHONE BERBASIS ANDROID

Habib Alkhair[1], Dodi Wisaksono Sudiharto [2], Fazmah Arif Yulianto[3]

[1]Sistem Komputer, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Android s martphone sudah menjadi pilihan pengguna saat ini. Ber a gam aktivitas dilakukan dengan smartphone tersebut. S ehingga beragam informasi yang berhubungan dengan aktivitas pengguna tersimpan pada smartphone . Salah satunya adalah informasi dari aktivitas digital communication yang sering dilakukan para pengguna smartphone . Aktivitas digital communication yang dimaksud adalah aktivitas jaringan wireless yaitu wifi dan b luetooth . Untuk dapat mengumpulkan informasi - informasi tersebut biasanya dilakukan dengan melakukan proses digital forensic . Dalam penyelidikan kasus kriminal, informasi - informasi tersebut dapat dijadikan sebagai digital evidence atau barang bukti digital yang dapat membantu proses investigasi. Pada penelitian ini akan dilakukan proses akuisisi terhadap smartphone android berkaitan dengan aktivitas dari wifi dan b luetooth . untuk melakukan akuisisi dalam penelitian ini , metode yang dipakai memanfaatkan tools yang bersifat open source untuk mendukung proses akuisisi . Pencarian digital evidence dipusatkan kepada dua area , yaitu circular buffer untuk mengakuisi data yang bersifat volatile dan physical image dari fil e system untuk data yang bersifat non - volatile . Pengujian dilakukan kepada tiga macam vendor yang berbeda dengan si stem operasi android v2.3, v4.0 dan v4.1 . kemudian menganalisis efektifitas dari metode akuisisi yang digunakan, pengaruh waktu terhadap digital evidence , dan struktur file tempat tersimpannya informasi atau data yang berpotensi menjadi barang bukti digital

Kata Kunci : digital forensic, digital communication, digital evidence, l ive analysis , c ircular buffer, p hysical image , volotile data & non - volotile data

Abstract

Now a days, a ndroid smartphone has become today's common choice. Some many activities have been done by using android smartphone. Thus, any infor mation which are related to users activit ies can be stored in that smartphone . One of the m is information gathe r ed fro m digital communication activit ies which are done by users. One instance of digital communication is wireless communication which consists of wifi and bluetooth. I n order to gather those information, it is neccessary to implement digital forensic. In regard of criminal investigation, those information can be used as digital evidence which can assist in so lving the case. In this research, the acquisition process of information from android smartphone will be done in regards of wifi and bluetooth activity "s . In order to engage the acqusition process, open source tools will be used to support the entire process. The search of digital evidence will be focused on 2 areas : those are circular buffer to acquire volatile data and physic a l image from filesystem to acquire non volatile data. Testing will be done on 3 different vendors with 3 android versions : v 2.3, v4.0, v4.1. Furthermore, the testing will include analyzing efficiency from the means of acquisition process,the impact of time to digital evidence and file structure where potential evidence is stored

Keywords : digital forensic, digital communicat ion, digital evidence, live analysis, c ircular buffer, p hysical image , volotile data & non - volotile data

`

1. Pendahuluan

1.1 Latar belakang

Perkembangan *Android Smartphone* yang begitu pesat [2] membuat orang-orang melakukan sebagian aktivitasnya menggunakan *Android Smartphone*. Mulai dari berselancar di internet, menggunakan jejaring sosial, penjadwalan, dan aktivitas lainnya. Melihat seringnya aktivitas yang melibatkan *smartphone* dapat dipastikan banyak sekali data atau informasi berharga yang tersimpan di dalamnya. Dalam dunia kepolisian, data-data tersebut dapat berguna sebagai barang bukti maupun sebagai informasi pendukung dalam proses investigasi sebuah kasus kriminal. Untuk menemukan dan mengumpulkan data tersebut, sehingga dapat diterima sebagai barang bukti yang *valid*, maka dilakukan proses *digital forensic*.

Digital forensic adalah bidang keahlian untuk mengidentifikasi, menemukan, mengumpulkan, menganalisa, dan menguji bukti-bukti dalam melakukan investigasi sebuah kasus yang melibatkan barang bukti digital. Ada beberapa tahap yang harus dilakukan saat melakukan *digital forensic*, salah satunya adalah tahap akusisi. Tahap akuisisi adalah tahapan untuk mengambil dan mengumpulkan data digital yang terdapat pada *digital device* seperti *smartphone*. Dalam sudut pandang *digital forensic*, *Android Smartphone* memiliki masalah atau isu tersendiri. Berdasarkan penelitian-penelitian sebelumnya, tidak semua metode efektif diterapkan saat proses akuisisi untuk versi dan *vendor* yang berbeda [10].

Pada penelitian sebelumnya diperkenalkan metode akuisisi dengan menggunakan *open source tools* [4]. Metode tersebut diujikan pada *Android* versi 2 dengan menggunakan *smartphone* dengan *vendor* yang berbeda. Hasilnya metode tersebut efektif digunakan untuk proses akuisisi. Mengacu kepada isu yang dipaparkan sebelumnya, maka pada penelitian kali ini akan diujikan metode akuisisi [4] tersebut kepada *android* dengan versi yang lebih baru dengan seri *smartphone* yang lebih baru. Selain itu, dalam penelitian ini ditambahkan metode untuk *by pass access control* ke dalam metode sebelumnya [4], dengan tujuan untuk menangani kasus dimana terdapat *access control* pada *Smartphone* yang ditemukan di TKP (Tempat Kejadian Perkara). Metode untuk mengakuisisi *digital evidence* dibagi kedalam dua bagian yaitu melakukan *live analysis* pada *circular buffer* menggunakan ADB (*Android Debug Bridge*) kemudian mengambil *physical image* dari partisi data dan sistem dengan menggunakan *dd (Nandump) utility unix*.

Metode tersebut akan diujikan pada *Android* versi 4 dengan 3 buah *vendor smartphone* yang berbeda yaitu Samsung Galaxy Mini, Lenovo A390, dan LG Optimus L9. Untuk pengujian studi kasus yang dipilih adalah jaringan *wireless* pada *smartphone* yaitu *bluetooth* dan *wifi* sesuai dengan penelitian [4]. Kemudian melihat efektifitas penerapan metode akuisisi [4] pada android v2.3, v4.0, dan v4.1 dengan vendor yang berbeda, lalu menganalisis struktur *file* tempat tersimpannya *file* yang berpotensi menjadi barang bukti dan dampak waktu terhadap data atau informasi yang tersimpan pada *circular buffer*.

`

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, berikut adalah rumusan masalah yang dapat dirumuskan:

1. Apakah metode akuisisi [4] efektif diterapkan untuk mendapatkan *digital evindence* terkait dengan aktivitas *wireless networking* pada *Android Smartphone* v2.3, v4.0, dan v4.1 ?
2. Bagaimana dampak waktu terhadap *digital evidence* yang tersimpan pada *circular buffer* terkait aktivitas *user*?
3. Bagaimana struktur *file* yang mengandung informasi terkait dengan jaringan *wireless* pada Samsung Galaxy Mini, LG Optimus L9, dan Lenovo A390 ?

1.3 Tujuan

Tujuan yang ingin dicapai pada penelitian tugas akhir ini adalah sebagai berikut:

1. Menganalisis efektifitas penerapan metode akuisisi [4] kepada *android smartphone* v2.3, v4.0, dan v4.1, untuk mendapatkan *digital evidence* terkait dengan aktivitas jaringan *wireless smartphone.*
2. Menganalisis dampak waktu terhadap *digital evidence* yang tersimpan di *circular buffer* dikaitkan dengan aktivitas *user*.
3. Menganalisis stuktur *file* tempat tersimpannya *file* berisi informasi yang berpotensi menjadi barang bukti digital terkait dengan jaringan *wireless* pada Samsung Galaxy Mini, LG Optimus L9, dan Lenovo A390.

1.4 Hipotesis

Hipotesis dari penelitian ini adalah sebagai berikut :

1. Metode akuisisi yang diperkenalkan pada penelitian sebelumnya [4] dapat diterapkan untuk versi *Android* yang lebih tinggi dengan *vendor* yang berbeda-beda.
2. Aktivitas *user* selama rentang waktu tertentu sangat berpengaruh terhadap informasi atau data yang tersimpan di *circular buffer*. Semakin pendek jarak waktu antara aktivitas kriminal dengan proses akuisisi maka semakin besar kemungkinan untuk menemukan informasi atau data yang berpotensi menjadi barang bukti digital pada *circular buffer*.

1.5 Batasan Masalah

Batasan masalah yang hanya akan dibahas dalam penelitian ini adalah:

1. *Android* OS yang digunakan saat pengujian adalah *Android* v2.3, v4.0, dan v4.1. untuk *Android* v3.0 tidak diujikan karena sistem operasi ini hanya untuk *tablet PC*.
2. *Digital evidence* yang dicari berupa *artifact* atau jejak yang membuktikan adanya penggunaan dan aktivitas *bluetooth* maupun *wifi* terkait dengan kasus kriminal yang dijadikan dasar saat pengujian. Proses akuisisi tidak sampai kepada *recovery filesystem* seperti mengembalikan *image* yang telah dihapus.
3. *Tools* yang digunakan saat pengujian adalah *Android Debug Bridge, sqlite, ghex, busybox, vroot, framaroot, super su*.

`

4. *Development machine* yang digunakan dalam pengujian ini berbasis *Linux Ubuntu 12.04 LTE*.
5. Studi kasus yang digunakan adalah aktivitas jaringan *wireless* yaitu *bluetooth* dan *wifi* pada *smartphone*.
6. *Constraint* waktu mengggambarkan aktivitas yang dilakukan dalam rentang terjadinya tindak kejahatan sampai dilakukannya proses akuisisi.
7. Skenario kasus yang digunakan untuk pengujian *by pass access control* sama dengan skenario kasus pengujian untuk jaringan *wireless* pada *smartphone*.
8. Mode akuisisi yang digunakan adalah *Live Acquisition*.

1.6 Metodologi Penyelesaian Masalah

Tahapan-tahapan dalam menyelesaikan tugas akhir ini adalah sebagai berikut :

1. Studi literatur
   Mempelajari dokumentasi cara *Android* mengumpulkan data-data terkait *wireless activity*, *data acquisition*, *tools* terkait yang dapat digunakan untuk melakukan analisis. mempelajari Macam-macam tipe *file system* yang digunakan oleh *vendor smartphone*
2. Perancangan
   Dirancang 3 buah skenario kasus yang dapat memenuhi kondisi penggunaan *smartphone* yang melibatkan aktivitas jaringan *wireless*. kemudiian dilakukan pengujian terhadap masing-masing skenario yang dibuat.
3. Pengujian
   Pengujian dimulai dengan menyiapkan *smartphone* sesuai skenario yang dibuat, kemudian dilakukan proses akusisi pada masing-masing *smartphone* lalu dilakukan analisis.
4. Analisa
   Pada tahap ini dilakukan analisis untuk mengetahui efektivitas dari metode yang digunakan terhadap masing-masing *smartphone*.
5. Pembuatan laporan
   Membuat dokumentasi keseluruhan dari penelitian yang dilakukan

5. Kesimpulan dan saran

5.1 Kesimpulan

Berikut kesimpulan yang didapatkan setelah mengerjakan penelitian ini :

1. Metode akuisisi [4] yang diimplementasikan, efektif mengumpulkan *digital evidence* terkait aktivitas jaringan *wireless* pada *android* versi 2.3, 4.0, dan 4.1 dengan jenis *vendor smartphone* yang berbeda, yaitu LG, *Samsung*, dan Lenovo .
2. Lama rentang waktu terjadinya tindak kejahatan sampai dengan dilakukannya proses akuisisi, sangat mempengaruhi *digital evidence* yangg tersimpan di *circular buffer*. Karena semakin lama rentang waktu tersebut maka kemungkinan aktivitas yang dilakukan *smartphone* juga akan banyak. Sehingga informasi yang tersimpan sebelumnya akan ditimpa kembali oleh *log* yangg baru diikarenakan sifat dasar dari *circular buffer*. Pada dasarnya yang menentukan berapa lamanya informasi bisa tersimpan pada *circular buffer* adalah daya tampung dari circular buffer. Namun dari hasil penggujian, ditemukkan bahwa selain *size*, intensitas penggunaan *smartphone* dan penanganan *hardware* yang berbeda dari masing-masing *vendor* juga sangat mempengaruhi.
3. Struktur *file path* tempat ditemukannya *digital evidence* bisa berbeda-beda pada masing-masing *smartphone* karena penentuan struktur *file path* tersebut bergantung kepada masing-masing *vendor* dari *smartphone* tersebut. Namun merujuk kepada data penelitian sebelumnya [4] dan melihat hasil pengujian pada penelitian ini, bisa diambil sebuah kesimpulan sementara bahwa *smartphone* yang berasal dari *vendor* yang sama memiliki struktur *file* yang sama dalam menyimpan informasi terkait dengan *bluetooth* dan *wifi*, sehingga *filepath* yang ditemukan disini bisa menjadi rujukan untuk menemukan *digital evidence* terkait dengan *bluetooth* dan *wifi*.
4. Analisis yang dilakukan terkait *wifi* pada *physical image* ditemukan informasi mengenai *password* yang digunakan oleh pengguna untuk terkoneksi dengan *access point* yang pernah dikunjunginya. Password terekam dalam bentuk *plain text*, sehingga menjadi sebuah kelemahaan dalam sistem operasi *Android*. Kelemahan ini ditemukan baik pada *Android* versi 2 maupun versi 4.
5. Untuk menemukan *digital evidence* yang lebih akurat bisa ditemukan pada *Physical image* dari partisi data. Partisi data menyimpan informasi yang lebih detail terkait dengan aktivitas komunikasi *wireless* dan aplikasi yang terlibat berdasarkan skenario kasus. Analisis lebih difokuskan kepada *file database* karena pada *file* ini lebih banyak ditemukan informasi yang berguna sebagi barang bukti digital.

`

5.2 Saran

Adapun saran untuk penelitian selanjutnya adalah sebagai berikut :

1. Untuk penelitian lebih lanjut diharapkan pengujian dapat dilakukan untuk versi OS yang lebih tinggi. Selain itu *vendor smartphone* yang digunakan juga lebih beragam karena mengingat struktur *file path* yang dimiliki oleh masing-masing *smartphone Android* juga berbeda.
2. Diharapkan Metode *root* yang digunakan lebih mumpuni dan efektif, karena salah satu kendala umum saat melakukan *digital forensic* terhadap *Android smartphone* adalah metode *root* dari kebanyakan *smartphone* saat ini cukup rumit, sehingga resiko kehilangan *digital evidence* lebih besar.

`

Daftar Pustaka

[1] Abdullah, A. G., Andrew, J., Thomas, A. (2012). Forensic Data Acquisition Methods for Mobile Phone. The 7th International Conference for Internet Technology and Secured Transactions (ICITST)

[2] Abdullah, A. G., Andrew, J., Thomas, A. (2012). Guidelines For The Digital Forensic Processing of Smartphone . Perth Western Australia: Edith Cowan University.

[3] ACPO. (2013). Good Practice Guide For Computer Based Electronic Evidence. Retrived from http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf.

[4] Andriotis, P., Oikonomu, G., Thyfonas, T. (2012). Forensic Analysis of Wireless networking Evidence of Android Smartphones. UK : Bristol Cryptography Group, Faculty of Engineering, University of Bristol Queen's Building, University Walk, Bristol, BS8 1TR.

[5] Folloder, A. (2011). Digital forensic *file* carving on *android smartphone*. Retrieved from http://www.utdallas.edu/~anf061000/Digital%20Forensics%20and%20File%20Carving%20on%20the%20Android%20Platform.pdf

[6] Feifan. (2013). Retrieved from http://b*log*.thisisfeifan.com/2012/05/screen-unlock-apk- coming.html.

[7] Goel, A., Tyagi, A., and Agarwal, A. (2012). Smartphone Forensic Investigation Process Model. New Delhi, India: Northern India Engineering College.

[8] Lessing, M., Basie, von S. (2008). Live Forensic Acquisition as Alternative to Traditional Forensic Processes. South Africa : Academy for Information Techno*log*y University of Johannesburg.

[9] Morum, de L., Fabio, C. F., Laerte, P. (2011). Acquisition and Analysis of Digital Evidence in Android Smartphones. IJoFCS.

[10] Mutawa, N., Baggili, I., and Marrington, A. (2012). Forensic Analysis of Social Networking Applications on Mobile Device. Dubai : Zayed University

[11] Vidas, T., Zhang, C., and Christin, N. (2011). Toward a General Collection Methodology For Android Devices. Digital Investigation, vol. 8, no. 1, pp. S14–S24, 2011, 11th Annual DFRWS Conference, New Orleans.

[12] Area man sentence in child porn case (2008). Retrieved from http://www.tulsaworld.com/news/courts/area-man-sentenced-in-child-porn-case/article_cdeaec27-1d98-5570-b481-a4e7343549d3.html?mode=story.

[13] Man post suicide note in *Twitter* before taking his own life. Retrived from http:// thenextweb.com/socialmedia/2010/06/16/man-posts-suicide-note-on-*Twitter*-before-taking-his-own-life.

`

[14] Ariel didakwa memberi kesempatan video porno tersebar. Retrived from http://www.tempo.co/read/news/2010/12/06/063297104/Ariel-Didakwa-Memberi-Kesempatan-Video-Porno-Tersebar