 ISSN : 2338-2899

ANALISIS FORENSIK PADA *PLATFORM* ANDROID

Ilman Zuhri Yadi[1)], **Yesi Novaria Kunang**[2)]

[1), 2)] *Program Studi Sistem Informasi, Ilmu Komputer, Universitas Bina Darma*
Universitas Bina Darma, Jl. Ahmad Yani no. 3 Plaju Palembang
Email : ilmanzuhriyadi@mail.binadarma.ac.id[1)], *yesi_kunang@mail.binadarma.ac.id* [2)]

Abstrak

Teknologi smartphone sangat populer belakangan ini terutama dengan berbagai fitur, fungsi yang sangat mendukung produktivitas. Dengan semakin kompleknya kemampuan yang dimiliki oleh ponsel pintar memberikan tantangan baru di bidang Forensik. Android sebagai salah satu sistem operasi ponsel pintar terkini, muncul sebagai kekuatan yang sangat kompetitif di pasar ponsel pintar. Ponsel Android dapat menyimpan sejumlah besar data yang dapat disimpan baik lokal ataupun remote yang memberikan tantangan bagi analis forensik untuk memperoleh data dan bukti, serta mengumpulkan informasi berharga pada ponsel android. Beberapa tool forensik baik open source dan closed source tersedia untuk mengekstrak data dari perangkat Android.

Tujuan utama dari penelitian adalah untuk mengevaluasi kinerja tool ekstraksi yang mendukung ponsel Android. Dengan menggunakan berbagai literatur di bidang forensik digital dan metode ekstraksi data serta kriteria dan metodologi yang bisa digunakan untuk bisa melakukan evaluasi. Tiga perangkat lunak yang berbeda dievaluasi serta dibandingkan dengan proses ekstraksi manual pada dua perangkat ponsel Android. Data forensik aktual dalam perangkat mobile kemudian diidentifikasi dan dihitung. Kemudian dibandingkan dengan hasil ekstraksi data dari tiga tools forensik android yang diuji serta dievaluasi berdasarkan kelengkapan data yang bisa dikumpulkan serta fitur masing-masing tool.

Hasil dari penelitian ini memberikan gambaran tahapan yang bisa diterapkan di bidang analisis fornsik android serta kriteria evaluasi tool yang bisa digunakan sebagai referensi pemilihan tool forensik android.

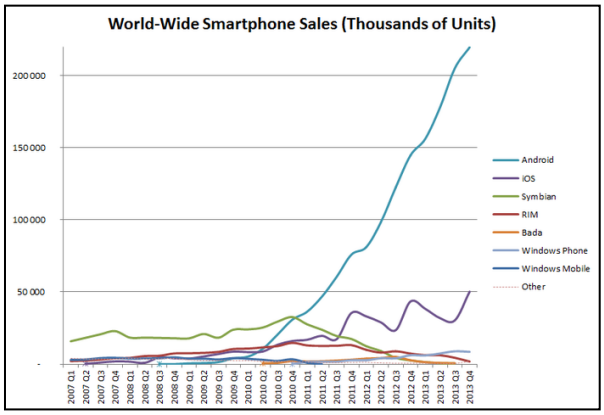
Kata kunci: *Forensic, Mobile Forensic, Android Platform.*

1. Pendahuluan

Dewasa ini Perangkat *mobile* sudah menjadi kebutuhan sehari-hari bagi setiap individu. Dalam komunikasi sehari-hari perangkat *mobile* ini digunakan untuk melakukan panggilan, pengiriman pesan sms, pengiriman *email*, berkomunikasi melalui jejaring sosial atau melalui *instant messaging* dengan teman dan keluarga. Selain itu selain untuk berkomunikasi penggunaan ponsel khususnya untuk *smartphone* juga digunakan dalam berbagai transaksi seperti *mobile banking*, pemesanan dan *check in*, jual beli, lokasi navigasi, menonton video dan film *real time*, tv dan radio *broadcast,* dan berbagai fitur lainnya. Dengan berbagai fitur dan kemampuan yang dimiliki oleh perangkat ponsel *smartphone*, mengakibatkan lonjakan signifikan pertumbuhan penggunaan perangkat *smartphone* pada beberapa tahun terakhir.

Smartphone android sendiri merupakan perangkat *hybrid* yang bisa bekerja sebagai ponsel dan juga bisa bekerja hampir seperti komputer tapi dalam bentuk portabel yang lebih simpel. Dengan meningkatnya penggunaan ponsel cerdas berbasis *platform* android dan IOS memberikan juga tantangan baru penggunaan ponsel cerdas ini dikaitkan dengan kegiatan kriminal. Perangkat ponsel cerdas ini bisa menyimpan data dalam jumlah besar, yang tidak terbatas hanya berupa *log* panggilan atau sms, namun juga informasi lain dari aspek penggunaan, prilaku atau kegiatan lainnya. Sehingga dengan nilai data yang begitu besar yang disimpan dalam ponsel pintar ini meningkatkan juga banyaknya fokus penelitian di bidang perangkat *mobile* forensik.

Untuk penggunaan jenis Sistem Operasi perangkat *mobilephone* ini sendiri bisa dilihat pada gambar 1 di bawah ini. Dari gambar 1 tersebut terlihat perangkat ponsel *mobile* berbasis android mendominasi dengan tingkat penjualan paling tinggi. Hal tersebut menunjukkan penggunaan *smartphone* berbasis android ini sangat luas, hal inilah yang mendasari perlunya mempelajari analisis forensik untuk perangkat berbasis android.



Gambar 1. *Tingkat penjualan perangkat ponsel mobile berbagai sistem Operasi.* [5]

Forensik android sendiri merupakan bagian dari digital forensik yang memberikan kesempatan dan tantangan. Seiring dengan makin beragamnya perangkat android dan penggunaan perangkat tersebut sebagai penunjang kejahatan memberikan tantangan tersendiri bagaimana mengekstrak dan menganalisis data secara efektif pada perangkat ponsel android untuk tujuan forensik. Tersedianya sejumlah *tool* yang bisa dimanfaatkan untuk aktifitas forensik *smartphone* memberikan tantangan tersendiri. Untuk itu pada penelitian ini akan mencoba melakukan analisis forensik pada perangkat smartphone atau tablet yang menggunakan berbagai sistem operasi Android *Platform*. Selain itu juga penelitian ini bertujuan mengevaluasi *tool* forensik yang bisa dimanfaatkan untuk melakukan analisis ponsel android berdasarkan jumlah bukti yang bisa dikumpulkan oleh *tool* forensik tersebut.

1.1. *Mobile* Forensik

"*Mobile phone* forensik merupakan ilmu yang melakukan proses rekoveri bukti digital dari perangkat *mobile* menggunakan cara yang sesuai dengan kondisi forensik" [11].

Forensik sendiri bisa dilakukan pada berbagai ponsel GSM, akan tetapi pada penelitian ini lebih fokus pada forensik Android. Dengan meningkatnya jumlah ponsel yang kaya fitur membuat sulitnya membuat satu *tool* forensik atau standar khusus untuk satu *platform*. Bukti digital dalam perangkat *mobile* mudah rentan tertimpa dengan data baru atau terhapus. Perangkat *mobile* sendiri menggunakan *flash memory* untuk menyimpan data. Keuntungan menggunakan *flash memory* adalah ketahanannya terhadap suhu dan tekanan yang tinggi sehingga lebih sulit untuk dihancurkan. Dari sudut pandang forensik hal ini menguntungkan *karena flash memory* bisa saja berisi informasi yang sudah dihapus bahkan setelah seseorang berusaha untuk menghancurkan barang bukti. Casey dkk. menjelaskan mengapa perangkat *mobile* merupakan sumber berharga sebagai bukti digital dan berisi informasi penting yang tidak tersedia pada perangkat lain. Selain itu sifat personaliti dari perangkat tersebut membuatnya mudah untuk membuktikan jejak yang mengaitkan perangkat ke individu [4].

Dalam forensik perangkat *mobile* perangkat forensik data yang diambil dari ponsel dengan sendirinya bisa dijadikan sebagai bukti. Bukti-bukti ini bisa menjadi landasan ketika menyelidiki suatu perkara oleh lembaga penegak hukum. Ada sejumlah bukti yang dapat diekstraksi dari ponsel. Jenis barang bukti yang dapat diekstraksi dari ponsel antara lain nomor kontak, log panggilan, pesan sms, file audio, email dan internet history. Artefak ini bisa diekstrak dengan metode logik maupun fisik. Secara Logik adalah mengekstrak data dari file sistem dengan langsung berinteraksi dengan perangkat menggunakan beberapa *tool* khusus. *Software* atau *tool* yang bisa mengekstrak artefak (atau bukti) ini sangat terbatas. Sehingga penyidik forensik akan sulit untuk melaksanakan pekerjaan ini secara tepat waktu [10].

Seorang ahli forensik profesional sering dihadapkan dengan tantangan untuk bisa mengekstrak bukti dari perangkat *mobile* terutama berhadapan dengan fakta faktor bentuk yang kecil yang membuat perangkat *mobile* sangat portabel. *Tool* forensik *mobile* Android dan *toolkit* yang masih tertinggal dibandingkan kemajuan teknologi telepon selular. *Toolkit* tersebut tidak diverifikasi secara independen atau diuji untuk kesiapan forensik secara akurat. Para pengembang *tool* forensik menggunakan metode yang berbeda untuk mendapatkan akses memori pada ponsel *(McCarthy, 2005)*. Karenanya kebanyakan *tool* tersebut memiliki keterbatasan pada jumlah *handset* yang didukung.

Dalam bidang forensik salah satu area profesional forensik adalah mencari bukti di memori. Jika pengguna meng-*upgrade* versi baru ada kemungkinan data di memori akan ditimpa sehingga menghilangkan bukti penting dari ponsel. Tugas utama dari seorang analis forensik adalah membuat salinan yang sama dari perangkat dengan menggunakan kriptografi *hash function*. Akan tetapi dalam kasus ponsel nilai hash (MD5) cenderung berubah sehingga integritas copy sebagai bukti akan dipertanyakan. Nilai-nilai *hash* akan berubah setiap kali ketika ponsel diaktifkan atau dimatikan [7].

Forensik *mobile* juga menggunakan metode yang sama dengan investigasi forensik umum. Ada beberapa teknik yang perlu diikuti, meskipun belum ada format standar penyelidikan di forensik *mobile*. Metode penyelidikan yang digunakan kurang lebih sama dengan investigasi digital. Tahapan proses penyelidikan yang diikuti adalah [11] : (1) *Collection*: merupakan langkah awal dan paling penting dalam penyelidikan. Tujuan utamanya adalah untuk mengumpulkan sumber-sumber bukti potensial seperti ponsel, kartu SIM dan aksesoris lainnya.; (2) *Identification*: lebih difokuskan pada pengenalan sumber barang bukti dengan pelabelan.; (3) *Acquisition*: berkaitan dengan proses ekstraksi data atau bukti potensial bukti dari berbagai sumber yang telah dikumpulkan.

1.2. *Tool* Forensik

Forensik *mobile* merupakan bidang yang relatif baru di area forensik digital, sehingga perangkat lunak dan *tool* yang bisa digunakan untuk mengambil data dari ponsel masih relatif baru. *Tool* ekstraksi bisa berupa *hardware* atau *software* tergantung pada cara data diekstrak dari perangkat *mobile*. Ada banyak *tool* ekstraksi yang tersedia di pasar saat ini dan beberapa alat-alat baru yang muncul dengan beberapa ide inovatif. Kebanyakan *tool* yang ada merupakan *tool* komersil dan ada juga sedikit yang berupa *tool open source*. Akan tetapi pengadaan *tool-tool* ini cukup sulit didapatkan terkait masalah

privasi dan masalah keamanan serta biaya yang dibutuhkan. *Tool* ekstraksi fisik tidak digunakan dalam penelitian ini sehingga *tool* seperti Cellebrite UFED dan XRY tidak digunakan. *Tool* terkemuka lainnya seperti *AccessData Mobile phone Examiner Plus(MPE+)* dan *viaForensics ViaExtract* sulit diperoleh sehingga pada penelitian *tool* yang diuji adalah:

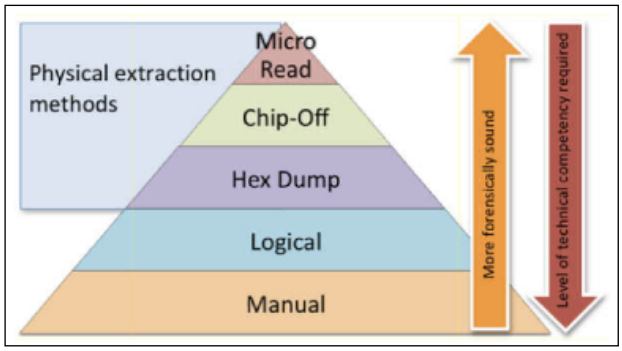
AFLogical
ViaForensic AFLogical OSE merupakan *tool open source* untuk mengekstrak data. *Software* ini sangat ringan dan hanya menggunakan *command line*. *Tool* ini memanfaatkan fitur *adb Android* untuk berkomunikasi dengan komputer.

Oxygen Forensic
Oxygen Forensic adalah *tool* terkemuka di bidang forensik ponsel dengan dukungan berbagai jenis ponsel. Oxygen mengektrak sebagian besar informasi dengan cara yang efisien. *Tool* ini memiliki sistem *reporting* yang baik sehingga pemeriksa bisa membaca rincian detail dari bukti yang didapat.

MOBILedit Forensic
MOBILedit Merupakan *tool* forensik yang memungkinkan penyidik untuk memperoleh secara logik, mencari dan memeriksa perangkat ponsel. *Tool* ini menggunakan beberapa mekanisme konektivitas terutama konektivitas nirkabel dibandingkan *tool* sejenis. *Software* ini cukup baik digunakan untuk memperoleh informasi sistem telepon dan informasi lainnya seperti daftar kontak dan pesan.

1.3. Metode Ekstraksi

Lima fase ekstraksi dari perangkat ponsel (Gambar 2). Seperti terlihat pada gambar secara umum dibagi dua cara dan metode fisik yang lebih dikenal sebagai metoda ektraksi forensik akan tetapi membutuhkan tingkat kompetensi teknis yang lebih tinggi [9].



Gambar 2. *Piramida Analisis Tool Forensic [9]*

Lapisan bawah adalah metode manual dengan cara memeriksa secara manual langsung ke perangkat ponsel dengan proses sederhana. Metode manual ekstraksi ini sangat sederhana dan hampir semua perangkat dapat dianalisis dengan metode ini. Akan tetapi masalah dengan metode ini adalah kemungkinan pemeriksa menghilangkan bagian penting dari bukti seperti item yang dihapus. Hal ini bisa berdampak serius ketika membawa bukti tersebut ke pengadilan. Metode ini hanya cocok dalam situasi di mana integritas data tidak begitu penting dan terbatasnya waktu untuk mencari bukti.
Metode ekstraksi berikutnya adalah metode logik. Metode ini paling direkomendasikan untuk ekstraksi data. Bagian dari teknik ini termasuk mengkopi *tool* aplikasi Forensik Android ke perangkat kemudian menghapusnya dari perangkat. *ViaExtract* adalah salah satu aplikasi yang dikeluarkan oleh perusahaan ViaForensics, *tool* ini mengekstrak informasi berikut : *Browser history, Call Logs, Contact Method, External Image Media (meta data), External Image Thumbnail Media (meta data), External Media, Audio*, dan *Misc. (meta data), External Videos (meta data), MMS, Organizations, People, SMS,* Daftar aplikasi yang diinstal beserta versinya, *Contacts Extensions, Contacts Groups, Contacts Phones* dan *Contacts Settings*" [1].

Ekstraksi logik merupakan cara cepat untuk menganalisis tanpa perlu tingkat keahlian yang tinggi. Metode ini bersifat berulang namun secara forensik belum dikatakan melakukan perubahan data ketika proses pengkopian di perangkat ponsel [6]

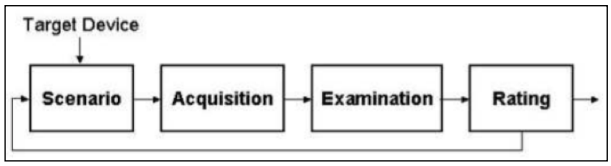
Tiga lapisan berikutnya merupakan metode ekstraksi fisik. Ekstraksi fisik lebih ke proses ektraksi seperti cara forensik pada umumnya. Layer fisik pertama adalah *hex dump*. *Hex dump* melibatkan proses mengupload dan mengganti *boot loader* ke perangkat dan melakukan proses *booting* dari *bootloader* yang baru dimuat. Metode ini hampir serupa dengan membuat *image* forensik. *Hex dumping* perangkat *mobile* mirip dengan *booting* komputer menggunakan *CD boot* untuk memperoleh *image hard disk* saat komputer berjalan. *Hex dumping* membutuhkan tingkat keahlian teknis yang tinggi khususnya saat berinteraksi dengan akses level sistem operasi [9].

Lapisan berikutnya adalah layer *'chip off'* dan teknik melepas *chip flash NAND* fisik dan diperiksa secara eksternal. Teknik ini terutama digunakan bila perangkat rusak dan dalam beberapa kasus untuk menganalisis perangkat yang diproteksi dengan *passcode*. Proses ini termasuk proses yang sangat merusak dan dipilih sebagai pilihan terakhir ketika tidak ada lagi yang bisa dikerjakan selain merusak *chip NAND* selama proses ini [2].

Metode ekstraksi yang terakhir adalah *mikro-read* yang membutuhkan keahlian paling teknis untuk melakukannya. Metode *mikro-read* menggunakan mikroskop elektron untuk melihat keadaan memori pada perangkat. Namun metode ini membutuhkan biaya yang besar dan tidak menggunakan metode standar [3].

1.4. Pengujian dan Validasi

Metodologi sederhana untuk melakukan analisis dari perangkat *mobile [8]*. Langkah-langkah diilustrasikan dalam Gambar 3.

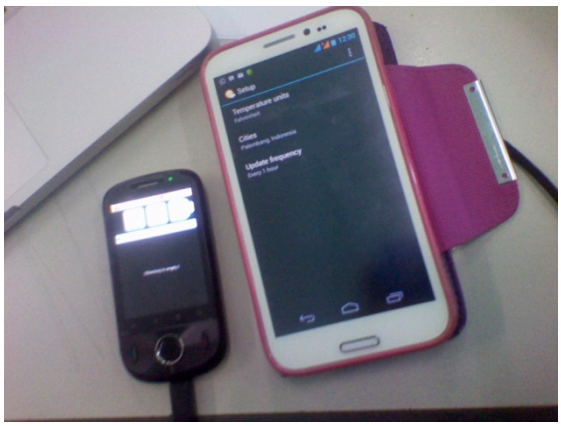


Gambar 3. *Tool Assesmen [8]*

Metode sederhana untuk mengakuisisi satu set target perangkat dan kemudian diikuti serangkaian kegiatan yang ditentukan seperti menempatkan dan menerima panggilan dilakukan pada masing-masing ponsel. Setelah itu isi telepon dan data terkait di SIM dikumpulkan dengan menggunakan alat yang tersedia dan diperiksa untuk menentukan apakah bukti kegiatan tersebut bisa di*recover* seperti yang diharapkan.

2. Pembahasan

Penelitian ini menggunakan tiga *tool* ekstrasi yang digunakan pada dua perangkat android (Gambar 4). Bukti forensik dalam ponsel akan dihitung dan dan setiap *tool* akan dibandingkan berdasarkan bukti yang bisa ditemukan. *Tool* ekstraksi forensik manual juga akan dievaluasi dengan *tool*s yang digunakan. Jenis ponsel Android yang digunakan dalam penelitian yaitu ponsel android AHA Touch huawei ideos c8150 dan perangkat ponsel advan S5F. Kedua ponsel tersebut berkomunikasi dengan komputer menggunakan ADB (*Android Bridge Device)* untuk menyimpan dan mengambil data dari ponsel.



Gambar 4. *Ponsel yang dianalisis*

Tool ekstraksi forensik yang akan diuji dalam penelitian ini antara lain AFLogical, Oxygen Suite Forensik 2014 Suite dan *MOBILedit* Forensik

Selain menggunakan *tool* tersebut pada penelitian ini juga digunakan metode manual ekstraksi data menggunakan FTK imaging lite dan FTK Forensic Toolkit, dan ProDiscover untuk menganalisis *image* yang diambil dari SD Card. *Tool*s yang diuji di sini sebagian besar *open source*. Meskipun dari beberapa acuan referensi tidak semua data bisa diidentifikasi menggunakan *tool* tersebut. Pada penelitian ini akan menghitung membandingkan jumlah barang bukti yang bisa ditemukan. Sebagai acuan barang bukti yang akan dianalisis di penelitian ini adalah berupa: Informasi Sistem, Kontak (no kontak telepon), *Log* panggilan (masuk, keluar dan tidak terjawab), SMS, MMS, Gambar, File Audio (termasuk *ring tones*), Videos, Item kalendar, File (PDF, Word, Excel, dan PowerPoint dan txt, File sistem), Applikasi dan *Browser Bookmarks*

2.1. *Platform* Pengujian

*Tool*s forensik menggunakan banyak resource komputer saat ekstraksi. Komputer forensik yang digunakan menggunakan prosesor Intel i5 dengan RAM 8GB RAM dan hardisk 500GB hard drive. *Tool*s yang digunakan untuk berkomunikasi dengan ponsel Android adalah *tool ADB* yang juga diinstal sebagai bagian dari SDK Android. ADB merupakan *tool* yang memiliki kemampuan mengirim, menarik data, dan juga digunakan untuk mendapatkan akses hingga ke root level dari ponsel. Semua *tool mobile* forensik ponsel diinstal di komputer tersebut.

Model ponsel yang digunakan dalam penelitian memiliki versi sistem operasi Android yang berbeda. Spesifikasi ponsel yang digunakan tercantum pada tabel berikut:

Tabel 1. *Tabel Spesifikasi Ponsel Android yang digunakan*

Spesifikasi	Ponsel 1	Ponsel 2
Handset	AHA Touch	Advan S5-F
Manufacture	Huawei	Advance
Model No	Huawei IDEOS C815	S5-F
Versi OS	2.2	4.2.1
Procsessor	Processor Qualcomm MSM7225-1	quad-core ARM Cortex-A7 1.2 GHz

Ponsel 1 memiliki jumlah barang bukti lebih sedikit dibandingkan ponsel ke-2 yang lebih digunakan secara ekstensif dan menyimpan lebih banyak data termasuk *browser history, cache, email* dll. Tidak ada perubahan yang dibuat pada kedua ponsel setelah dilakukan investigasi awal. Lima kontak baru dan lima pesan teks dibuat pada kedua ponsel dan dihapus setelah beberapa jam. Ponsel kemudian disimpan dan diberlakukan menggunakan pendekatan forensik sehingga jaringan diputus untuk menyimpan data utuh sampai pengujian telah selesai. Bukti yang akan diidentifikasi dari kedua ponsel tercantum pada tabel berikut.

Tabel 2. *Identifikasi bukti yang akan dianalisis*

Ponsel	Sys Info	Kontak	Call Log	SMS/MMS	Gambar
AHA Touch	yes	316	349	53	50
Advan S5-F	yes	386	118	2009	2030

Ponsel	Audio	Video	Kalendar	Aplikasi	File	Bookmark
AHA Touch	1	19	0	34	321	0
Advan S5-F	32	49	6	48	5857	3

2.2. *Tool* yang diuji

*Tool*s yang digunakan dalam penelitian ini dilakukan satu demi satu. Setiap *tool*s memiliki teknik yang berbeda untuk mengekstrak data dari kedua ponsel.

2.2.1. Oxygen Forensic

Oxygen forensik diinstal di laptop menggunakan registrasi key. Versi yang diinstal di sini memiliki keterbatasan untuk melihat *timeline, instant messengers* dan *apps.* Oxygen forensik mendukungsejumlah besar USB drivers untuk hampir semua jenis ponsel android. *Software* ini memerlukan kondisi perangkat *mobile* dalam kondis *USB debugging mode* ketika terhubung ke komputer. Kendala pada penggunaan *software* ini adalah perangkat ponsel yang digunakan tidak dikenali oleh Oxygen. Akan tetapi Oxygen memberikan alternatif penggunaan akses melalui *bluetooth*.

Oxygen *software* menginstal aplikasi client yang disebut Oxygen *Agent* dalam memori eksternal ponsel dan *agent* ini akan menarik semua data ke komputer.

Hasil keseluruhan proses akan diekspor ke file PDF. Oxygen juga akan membuat folder yang berisi *images* (termasuk *thumbnails*) dan sebagian kopi dari *SD Card*. Version Oxygen yang diuji pada penelitian tidak dilengkapi fitur *timeline enabled* sehingga tidak bisa dilakukan *timeline analysis*.

2.2.2. *MOBILedit* Forensic

Versi lite *MOBILedit* didownload dari Internet. Installasi *MOBILedit* tidaklah terlampau sulit. Seperti juga Oxygen, *MOBILedit* membutuhkan kondisi *USB debugging mode enabled* di ponsel. Ponsel bisa terkoneksi baik menggunakan kaebl langsung maupun menggunakan koneksi *wireless*. Hal ini memberikan keuntungan untuk jensi ponsel yang tidak bisa didetekesi menggunakan *software* ini bisa diutilisasi menggunakan koneksi *wireless*. *MOBILedit* akan menginstall aplikasi kecil di ponsel untuk menarik data. Data yang iekstrak dibatasi hanya *contacts, call lists, messages* dan file.

2.3.3. AFLogical

Selanjutnya AFLogical OSE yang ada di Santoku diinstal di komputer forensik *workstation. Tool* ini merupakan versi *open source* dari AFLogical. *Full version* hanya digunakan oleh penegak hukum sehingga dalam penelitian hanya menggunakan versi *open source version*. *Tool* ini merupakan *lightweight software* yang tidak memiliki tampilan grafis seperti *tool*s sebelumnya. Ponsel android dikoneksikan ke komputer forensik dengan kondisi *USB debugging mode enabled*. Pada saat dilakukan proses ini *SD card* sebaiknya dilepaskan karena akan tampil pesan ViaForensic yang akan menghapus isi *SD card*. Sehingga sebaiknya dipasang *SD card* kosong ke dalam ponsel. AFLogical membutuhkan ADB untuk berkomunikasi dengan *Android devices*. ADB terdapat pada Android *Software Development (SDK)* di komputer forensik. *Tool* ini merupakan bagian dari SDK kit. Langkah selanjutnya adalah menginstal file *AFLogical package* (file .apk).

AFLogical akan membuat folder yang bernama '*forensics'* pada kartu memori eksternal. Informasi yang diekstrak akan disimpan dalam format *Comma Separated Values (CSV)* dan sebuah file yang bernama info.xml yang berisi informasi detail mengenai informasi sistem ponsel. Semua bukti disimpan dalam format CSV. Versi AFLogical yang digunakan pada penelitian ini menggunakan versi *open source* dan sejumlah bukti tidak bisa dianalisis menggunakan metoda ini.

2.2.4. Ekstrasi Manual

Proses manual ekstraksi juga dilakukan pada penelitian ini. *Physical image* dari SD card untuk kedua ponsel dibuat menggunakan *FTK imager*. Bit demi bit *images* disimpan dalam *forensic workstation hard disk* dalam bentuk file dd.

Tujuan dilakukan proses ini adalah untuk mendapatkan informasi sistem dari images. Untuk menganalisis image digunakan tool FTK-forensic toolkit dan ProDiscover. Dengan teknik ini bisa mencari file yang sudah didelete seperti gambar, files, audio dan video dll.

2.3. Evaluasi Penggunaan *Tool*

Untuk mengevaluasi *tool* forensik yang digunakan maka hasil pengujian yang dilakukan dibandingkan dengan data forensik yang dianalisis dengan cara manual. Data yang disajikan memperlihatkan hasil output setelah pengujian forensik dengan setiap *tool* pada kedua ponsel yang dianalisis. Setiap tahap pengujian dicatat dan disajikan dalam bentuk tabel.

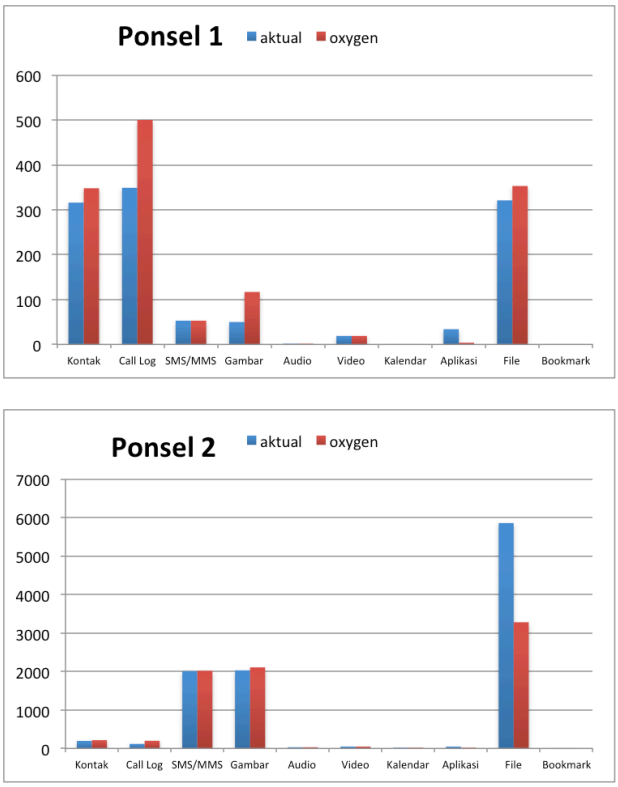
2.3.1. Evaluasi Hasil Ekstraksi menggunakan *Tool* Oxygen Forensic

Tabel 3. *Data yang diekstrak menggunakan tool Oxygen forensic*

Ponsel	Sys Info	Kontak	Call Log	SMS/MMS	Gambar
AHA Touch	yes	348	500	53	117
Advan S5-F	yes	216	200	2020	2108

Ponsel	Audio	Video	Kalendar	Aplikasi	File	Bookmark
AHA Touch	1	19	0	4	353	-
Advan S5-F	32	49	7	22	3281	-

Secara umum *tool* Oxygen forensic yang diuji memberikan laporan standar. Terlihat beberapa perbedaan ketika mengekstrak no kontak dan daftar panggilan yang lebih banyak dibandingkan data aktual. Hasil tersebut memperlihatkan jika Oxygen forensic menampilkan daftar panggilan sejumlah maksimum *log* panggilan yang bisa disimpan di ponsel. Sedangkan untuk nomor kontak analisis manual memperlihatkan jumlah lebih sedikit di kedua ponsel dibandingkan menggunakan *tool* Oxygen, hal tersebut dikarenakan *tool* Oxygen mengekstrak semua situs *social networking Facebook, LinkedIn*, dan *WA*. Hal ini diakibatkan ponsel android melakukan sinkronisasi *account* dengan *phonebook*. Proses sinkronisasi tersebut mengakibatkan perbedaan dikarenakan *tool* Oxygen terkadang menampilkan data *account* yang redundan akan tetapi perbedaan tersebut tidak signifikan. Selain itu juga Oxygen memperlihatkan jumlah gambar yang lebih banyak, hal tersebut dikarenakan Oxygen juga menampilkan *thumbnails* yang tidak dihitung ketika menggunakan cara manual. Gambar 5 memperlihatkan grafik perbandingan analisis menggunakan *tool* forensik Oxygen dengan data aktual



Gambar 5. *Grafik Perbandingan Manual Analisis dan Menggunakan Tool Oxygen Forensic*

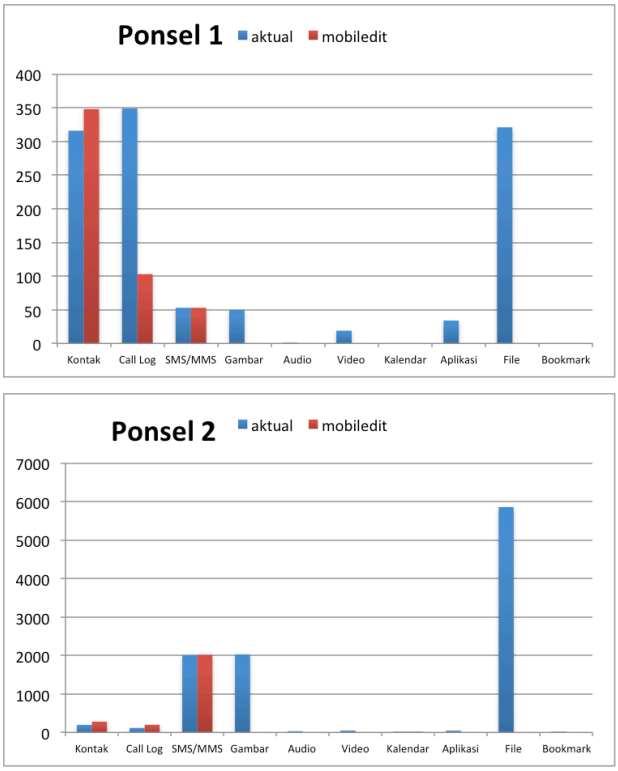
2.3.2. Evaluasi Hasil Ekstraksi menggunakan *Tool MOBILedit*

Hasil analisis yang didapatkan menggunakan *tool MOBILedit* ini sangat terbatas. *Tool* ini hanya menghasilkan *report* berupa kontak, *log* panggilan, pesan dan file. Untuk log sms didapatkan hampir sama dengan nilai aktual untuk *call* khususnya di ponsel 1 yang merupakan ponsel Android versi froyo memperlihatkan sebagian *call log* saja.

Tabel 4. *Data yang diekstrak menggunakan tool MOBILedit*

Ponsel	Sys Info	Kontak	Call Log	SMS/MMS	Gambar
AHA Touch	yes	348	103	53	-
Advan S5-F	yes	281	200	2020	-

Ponsel	Audio	Video	Kalendar	Aplikasi	File	Bookmark
AHA Touch	-	-	0	-	-	-
Advan S5-F	-	-	7	-	-	-



Gambar 6. *Grafik Perbandingan Aktual dan Analisis Menggunakan Tool MOBILedit*

Pada saat melakukan proses analisis dengan menggunakan *tool MOBILedit* terkadang proses ekstraksi terkadang terputus dan gagal dilakukan, selain itu juga pada versi yang digunakan tidak memiliki pilihan untuk mengeksport data. Gambar 6 menampilkan perbandingan data antara data aktual dengan data yang dianalisis dengan *MOBILedit*.

2.3.3. Evaluasi Hasil Ekstraksi menggunakan *Tool* AFLogical

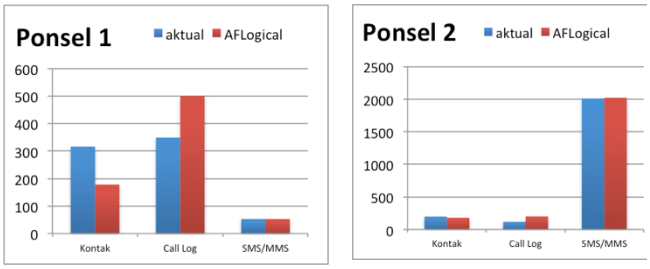
Tool AFLogical merupakan *tool* yang paling simpel dan mudah dalam penggunaannya. *Tool* ini tidak menggunakan tampilan GUI dan bisa diinstal dan dijalankan menggunakan mode terminal. Untuk versi

open source yang digunakan AFLogical hanya mendukung proses ekstraksi kontak contacts, call logs, SMS dan MMS. Data yang diekspor disimpan menggunakan format CSV. Selain itu juga untuk detail sistem informasi disimpan dalam format xml. Pada saat dilakukan proses ekstraksi AFLogical akan remove SD Card dari ponsel yang dianalisis sehingga *tool* ini tidak membaca beberapa informasi lain yang seharusnya bisa diekstrak dari sdcard

Tabel 5. *Data yang diekstrak menggunakan tool AFLogical*

Ponsel	Sys Info	Kontak	Call Log	SMS/MMS	Gambar
AHA Touch	yes	178	500	53	-
Advan S5-F	yes	180	200	2020	-

Ponsel	Audio	Video	Kalendar	Aplikasi	File	Bookmark
AHA Touch	-	-	-	-	-	-
Advan S5-F	-	-	-	-	-	-



Gambar 7. *Grafik Perbandingan Aktual dan Analisis Menggunakan Tool AFLogical OSE*

Gambar 7 memperlihatkan hasil analisis dengan *Tool* AFLogical menghasilkan hanya tiga artefak saja dan beberapa informasi tidak bisa dilihat.

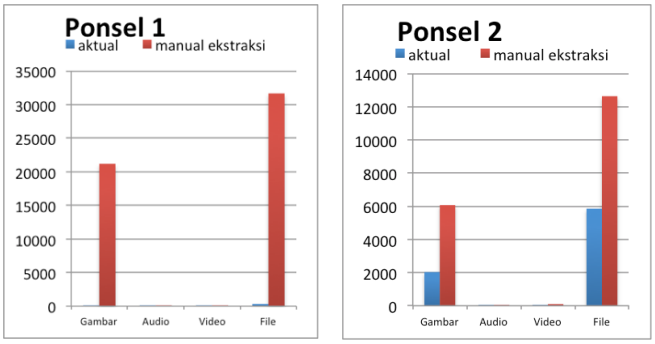
2.3.4. Evaluasi Hasil Ekstraksi dengan Cara Forensik Manual Ekstraksi

Proses manual ekstraksi berbeda dengan mengekstrak data menggunakan *tool*. Proses ini dilakukan dengan membuat *image* (DD) dari *SD card* maupun memori internal ponsel dengan menggunakan *tool* FTK Imager kemudian dianalisis dengan menggunakan *tool* Forensik Access Data FTK light, ProDiscover dan EnCase. Proses ini sangat penting untuk mencari gambar dan file yang bisa dijadikan bukti.

Tabel 6. *Data yang diekstrak secara Manual*

Ponsel	Sys Info	Kontak	Call Log	SMS/MMS	Gambar
AHA Touch	-	-	-	-	21196
Advan S5F	-	-	-	-	6069

Ponsel	Audio	Video	Kalendar	Aplikasi	File	Bookmark
AHA Touch	28	19	-	-	31670	-
Advan S5-F	7	103	-	-	12639	-



Gambar 8. *Grafik Perbandingan Aktual dan Analisis Ekstraksi Manual*

Untuk proses membuat *image* menggunakan *tool* FTK Imager, untuk Ponsel 1 yang masih menggunakan android Froyo 2.2 yang hanya bisa dibuat *image* adalah *SDCARD* nya sedangkan memori internal ponsel tidak bisa dideteksi di *tool* tersebut. Untuk Ponsel 2 yang menggunakan android Jelly Bean *tool* bisa mendeteksi *memori internal* dan bisa dibuat *image* baik *memori internal* yang berukuran 8 G maupun SDCARDnya. Proses ekstraksi ini bisa mendapatkan jumlah file yang lebih banyak dibandingkan file aktual, hal tersebut dikarenakan dengan cara ini file yang bisa dianalisis bukan saja file aktual akan tetapi juga file yang sudah dihapus masih bisa didteksi dan sebagian masih bisa direcover. Proses ini sangat penting jika barang bukti sudah dihilangkan atau dihapus sebelumnya. Selain itu juga di ponsel 1 *SDCARD* terdeteksi lebih banyak file dibandingkan ponsel 2, padahal data aktual file di ponsel 2 lebih banyak.

2.4. Perbandingan Keseluruhan

Tabel 7. *Keseluruhan Hasil ekstraksi ponsel 1*

Tool	Kontak	Call Log	SMS/MMS	Gambar	Audio	Video	Kalendar	Aplikasi	File	Bookmark
aktual	316	349	53	50	1	19	0	**34**	321	0
oxygen	**348**	**500**	**53**	**117**	**1**	**19**	0	4	**353**	-
mobiledit	**348**	103	**53**	-	-	-	-	-	-	-
AFLogical	178	**500**	**53**	-	-	-	-	-	-	-
manual ekstraksi	-	-	-	**21196**	**28**	**19**	-	-	**31670**	-

Tabel 8. *Keseluruhan Hasil ekstraksi ponsel 2*

Tool	Kontak	Call Log	SMS/MMS	Gambar	Audio	Video	Kalendar	Aplikasi	File	Bookmark
aktual	197	118	2009	2030	32	49	6	**48**	5857	3
oxygen	**216**	**200**	**2020**	**2108**	**32**	**49**	**7**	**22**	3281	-
mobiledit	**281**	**200**	**2020**	-	-	-	**7**	-	-	-
AFLogical	180	**200**	**2020**	-	-	-	-	-	-	-
manual ekstraksi	-	-	-	**6069**	7	**103**	-	-	**12639**	-

Tabel 7 dan 8 memperlihatkan hasil keseluruhan dari *tool*s yang digunakan untuk mengeketraksi data. Jika dilihat di tabel tersebut angka yang ditebalkan memperlihatkan bahwa *tool* bisa menampilkan seluruh data aktual. Untuk data kontak ponsel memperlihatkan *tool* Oxygen dan *MOBILedit* cukup baik membaca data kontak ponsel. Untuk data call log terlihat *tool* Oxygen, dan AFLogical cukup baik membaca call log, sedangkan untuk *mobile*edit untuk ponsel 1 untuk android versi froyo terlihat *MOBIL*edit gagal mendeteksi semua *call log*.

Untuk data pesan berupa *SMS* dan *MMS* ketiga *tool* tersebut Oxygen, AFLogical dan *mobile*Edit bisa membaca sms dengan baik. Sedangkan untuk pembacaan file, gambar, audio dan video dari ketiga *tool* yang digunakan terlihat memiliki fitur pembacaan file dan hampir bisa mendeteksi dan membaca keseluruhan file, sedangkan *tool*s *mobile*edit dan AFLogical versi free yang digunakan tidak memberikan akses tersebut.

Secara umum dari ketiga *tool*s ekstraksi yang digunakan Oxygen, *MOBILedit* dan AFLogical , Oxygen dan *MOBILedit*, Oxygen memperlihatkan memiliki keunggulan dari kelengkapan dan kemampuan melakukan ekstraksi data. Selain itu juga *Tool* Oxygen Forensic juga memberikan *report* yang cukup lengkap dalam bentuk format pdf, yang bisa digunakan sebagai bukti di pengadilan. *Tool* AFLogical OSE memiliki kelebihan di sisi fleksibilitas dalam proses ekstraksi data yang cukup cepat, dan juga kemudahan mendeteksi *device* karena kelengkapan *library* adb yang dimiliki, sehingga dari pengujian yang dilakukan dengan dua ponsel tersebut, tidak perlu dilakukan proses instalasi adb device. Sedangkan untuk *tool* Oxygen dan *mobile*edit, peneliti harus men*download* dan menginstal *library device android*. Semua *tool*s tersebut kecuali proses ekstraksi manual menggunakan aplikasi *agent* untuk mengambil data dari ponsel Android. Kesulitan utama dari proses analisis forensik dengan *platform* android ini adalah dukungan aplikasi *agent (adb driver*) masing-masing *tool* untuk semua jenis ponsel android yang tidak semuanya bisa dikenali.

Masing-masing *tool* yang diuji menggunakan methodology yang berbeda untuk mengekstrak data. Misalnya pada *MOBILedit* tidak mendukung ekstraksi data dari *SD card* sementara *tool*s lain bisa. Sedangan untuk android versi froyo tidak bisa dilakukan ekstraksi data untuk memori internal ponsel menggunakan FTK imager.

Dari ketiga *tool* yang digunakan untuk ekstraksi tersebut tidak dilengkapi fitur kemampuan mengekstraksi data yang sudah dihapus atau di delete dari ponsel. Untuk menganalisis atau mencari file bukti yang sudah dihapus dari ponsel, proses ektraksi secara manual dengan membuat image ponsel dan *sdcard* dilanjutkan dengan menganalisis *image* dengan *tool* forensik merupakan satu-satunya cara yang bisa digunakan. Terbukti dari pengujian yang dilakukan untuk *tool* versi evaluasi yang digunakan, *tool* seperti Oxygen hanya bisa mengenali data aktual yang tersimpan di ponsel, sedangkan untuk data yang sudah dihapus dari ponsel hanya bisa dianalisis dengan *tool* ekstraksi manual.

3. Kesimpulan

Kesimpulan dari penelitian ini memperlihatkan keberhasilan implementasi pada *platform Tool* pengujian. Lingkungan forensik testing dibangun sebelum menguji *tool*s. *Benchmark* diidentifikasi dengan cara mengumpulkan informasi bukti secara manual dari ponsel. Kemudian hasil awal ini diuji kembali dengan mengekstrak data menggunakan forensic *tool*s untuk kedua ponsel yang berbeda versi sistem operasi Android. Dari hasil yang diperoleh bisa didapatkan kesimpulan sebagai berikut:

1. Masing-masing *tool* yang diuji menggunakan methodology yang berbeda untuk mengekstrak data. Misalnya pada *MOBILedit* tidak mendukung ekstraksi data dari SD card sementara *tool*s lain bisa. Sedangan untuk android versi froyo tidak bisa dilakukan ekstraksi data untuk memori internal ponsel menggunakan FTK imager.

2. Semua *tool*s tersebut kecuali proses ekstraksi manual menggunakan aplikasi agent untuk mengambil data dari ponsel Android. Kesulitan utama dari proses analisis forensik dengan *platform* android ini adalah dukungan aplikasi *agent (adb driver*) masing-masing *tool* untuk semua jenis ponsel android yang tidak semuanya bisa dikenali.

3. Dari hasil pengujian yang dilakukan *tool* Oxygen memiliki fitur report yang lebih lengkap dibandingkan *tool* ektraksi android forensik *MOBIL*edit dan AFLogical. *Tool* ini hampir bisa mengekstrasi keseluruhan data aktual dari kontak ponsel, call log, sms-mms, kalender file gambar, video, dan file lainnya.

4. Untuk ekstraksi file barang bukti yang sudah dihapus atau diformat, proses analisis ponsel menggunakan cara ekstraksi manual dengan proses pembuatan image merupakan cara terbaik yang bisa dilakukan.

Daftar Pustaka

[1] A. Hoog, *"Introduction to Android forensic"*, DFI, April 30 2010.

[2] A. Hoog,. "Android Forensics (Vol. 1st Ed)", Waltham, MA, USA: Syngress, 2011.

[3] B. Knight, *"Mobile Devices: iPhone Risks and Forensic Tool Capability",* Auckland, NZ: AUT University, 2010

[4] E.C., Turnbull, *"Digital Evidence on Mobile Devices"*,In E. Casey, Digital Evidence and Computer Crime (3rd Edition ed.), Academic Press, 2011.

[5] Gartner, Inc, "Gartner Smart Phone Marketshare 2013 Q4".. Retrieved 2014-01-13.

[6] M. Westman, *"Complete Mobile Phones Forensic Examination: Why we need both Logical & Physical Extractions* ", E-Evidence Info, May, 2009.

[7] P. Owen, *"An Analysis of the Digital Forensic Examination of Mobile Phones"*, International Conference on Next Generation Mobile Applications, Services and Technologies (pp. 25-29). Amman: IEEE , 2010.

[8] R. Ayers, R, "Mobile Device Forensics - Tool Testing" , Mobile Device Forensics . NIST, 2008

[9] S. Brothers, *"Cell Phone and GPS Forensic Tool Classification System"*, 2009.

[10] S.G. Punja, *"Mobile Device Analysis"*. Small Scale Digital Device Forensics Journal , 2 (1), 2008

[11] W. Jansen,.*"Guidelines on Cell Phone Forensics"*, NIST, May, 2007.