MEMBANGUN MOBILE FORENSICS INVESTIGATION FRAMEWORK PADA *IOS*

Hikmatyar Insani [(1)], Anton Yudhana [(2)], Sunardi [(3)]
[(1)] Magister Teknik Informatika, Universitas Ahmad Dahlan
[(2)(3)] Teknik Elektro, Universitas Ahmad Dahlan
e-mail : hikmatyar.insani@gmail.com [(1)], eyudhana@ee.uad.ac.id [(2)], sunardi@mti.uad.ac.id [(3)]

Abstrak
Smartphone dengan segala fitur kecanggihannya dapat membantu menyelesaikan masalah yang sedang dihadapi oleh manusia. Disisi lain smartphone dapat disalahgunakan menjadi alat untuk tindak kejahatan oleh manusia yang tidak bertanggung jawab. Kemudahan dalam berkomunikasi dengan orang lain lewat berbagai aplikasi turut membuat persentase tindak kejahatan melalui smartphone semakin tinggi. Hal yang dilakukan dalam penelitian ini adalah mendapatkan informasi-informasi dalam smartphone berbasis iOs yang masih ada maupun yang sudah dihapus. Tahapan yang dilakukan adalah preservation, collection, examination, dan analysis. Tujuan dari penelitian ini adalah untuk mendapatkan barang bukti digital yang dapat membantu para penegak hukum dalam memvonis para pelaku cybercrime sesuai dengan yang dilakukan.

***Kata Kunci** : Cybercrime, iOs, Smartphone*

1. PENDAHULUAN

Perkembangan teknologi yang sangat pesat kini *smartphone* seolah-olah menjadi asisten pribadi hidup manusia. Dalam perkembangan tersebut memiliki berbagai dampak negatif salah satunya adalah sebagai alat untuk tindak kejahatan atau *cybercrime*. Sebagai contoh kasus yaitu masalah *screenshoot* percakapan melalui salah satu media sosial yang membuat resah masyarakat terhadap keaslian dari percakapan tersebut. Hal ini membuat kita berpikir pentingnya ahli digital forensik untuk menganalisa dan membuktikan keaslian dari kasus-kasus tersebut.

Survey Statista pada tahun 2017 menyebutkan bahwa pengguna *Smartphone* berbasis *iOs* dari tahun 2009 sampai dengan 2018 ini berada pada kisaran 10 - 25%, sedangkan di Indonesia pengguna *smartphone* tersebut hanya memiliki persentase sekitar 5% saja. Dari persentase yang sedikit, maka sedikit pula penelitian digital forensik pada *smartphone* berbasis *iOs*. Padahal *smartphone* tersebut merupakan salah satu produk yang menguasai pasar *gadget* di Indonesia. Seperti ponsel pintar lainnya, tidak menutup kemungkinan *smartphone* ini dapat digunakan untuk melakukan tindak kejahatan *cybercrime*.

. Pada esensinya *smartphone* merupakan sebuah komputer kecil, sehingga kita juga dapat menerapkan konsep komputer forensik. Namun data di dalam *smartphone* cenderung cepat berubah jadi seseorang tidak dengan mudah menyalin isi dari memorinya (Engman, 2013). Pelaku kejahatan *cybercrime* biasanya dapat menghilangkan barang bukti kejahatan dengan cara menghapus rekaman atau data yang terdapat pada iphone mereka. Sehingga secara langsung data tersebut tidak dapat terlihat lagi. Oleh karena itu perlu adanya investigasi terhdapat barang bukti berupa iphone yang digunakan untuk tindak kejahatan. Untuk mengatasi masalah diatas, maka dalam penelitian ini menganalisis dan mengembalikan data atau barang bukti di *smartphone* berbasis *iOs* yang sudah dihapus oleh pelaku.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Penelitian ini mengacu pada penelitian-penelitian sebelumnya, dengan adanya penelitian yang sudah pernah dilakukan maka peneliti dapat memiliki gambaran dari hasil yang ingin didapatkan. Proses Investigasi Mobile Forensik pada Smartphone Berbasis *IOS* yang dilakukan oleh Sidik Madiyanto dkk pada tahun 2107, yang berhasil mengembalikan data transaksi penjualan narkoba pada *iphone* 3G dan *iphone* 5 dengan menggunakan *tools* bernama Magnet AXIOM dengan metode Digital Forensik Investigasi *Framework* (DFIF). Peneliti tersebut juga membuat daftar *timeline* proses percakapan dari kedua pelaku yang menyalahgunakan smartphone untuk tindak kejahatan (Mubarok & Widiyasono, 2017).

Analisis Forensik Digital pada Line Messenger untuk Penanganan *Cybercrime* yang dilakukan oleh Fauzan Ammar, dkk pada tahun 2016 yang membuktikan bahwa terangkatnya bukti digital pada Line messenger di perangkat smartphone Android. Dengan menggunakan *tools* Zenfone Rootkit, KAMAS Lite, dan AFLogical OSE berhasil menemukan bukti dari percakapan lewat *Line Messenger*

yang dilakukan untuk melakukan kasus *Cyberbullying*. Analisis Forensik *Recovery* dengan Keamanan *Fingerprint* pada *Smartphone* Android yang dilakukan oleh Sahirudin, dkk yang dilakukan pada tahun 2017 yang mebuktikan tool atau aplikasi dapat berfungsi untuk mengembalikan data yang hilang meskipun smartphone telah melakukan factory reset (Sahiruddin , Imam Riadi, 2017).

Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial *Facebook* dan *Twitter* pada *Smartphone* Android yang dilakukan oleh Wisnu Ari Mukti, dkk pada tahun 2017 yang membuktikan bahwa bukti forensik lebih banyak ditemukan di dalam aplikasi Facebook (Mukti, Masruroh, & Khairani, 2017). Analisis Forensik pada *Platform* Andorid yang dilakukan oleh Ilman Zuhri Yadi dan Yesi Novaria Kunang pada tahun 2014 yang mebuktikan bahwa beberapa tool yang digunakan untuk mengambil barang bukti dalam smartphone memiliki keunggulan yang berbeda (Yadi & Kunang, 2014).

2.2. Komputer Forensik

Kegunaan istilah forensik adalah untuk membantu pengungkapan bukti-bukti kejahatan cybercrime yang sah menurut undang-undang. Bukti forensik dalam *smartphone* dapat berupa entitas maupun piranti digital, sehingga bukti-bukti tersebut dapat diacari dengan menggunakan metodologi yang terdiri dari teknik dan prosedur yang dinamakan dengan komputer forensik. Jadi bukti tersebut dapat dipergunakan secara sah dalam persidangan (Indrajit, 2011). Manfaat dari komputer forensik diantaranya adalah membantu badan usaha atau organisasi seandainya ada tuntutan hukum yang melanda seperti resiko yang dapat dialami mengenai informasi suatu badan usaha atau organisasi. Ruang gerak para pelaku kejahatan komputer akan semakin sempit dalam menjalankan aksinya terhadap organisasi atau badan hukum yang memiliki kapabilitas forensik komputer.

2.3. *IOs*

IOs merupakan salah satu sistem operasi yang banyak digunakan di dunia khususnya di Indonesia. *iOs* adalah sistem oeprasi buatan *Apple Inc*, sebuah perusahaan teknologi multinasional yang berpusat di Cupertino, California. *IOs* diturunkan dari OS X yang memiliki fondasi Darwin dan karena itu *iOs* merupakan sistem operasi *Unix* (One, 2017). iOs memiliki lingkungan yang tertutup yang berbeda dengan sistem oeprasi lainnya yang relatif terbuka. Fitur-fitur ini mencegah banyak proses duplikasi dan analisis digital forensik tradisional (Hay, Krill, Kuhar, & Peterson, 2011).

2.4. *Cybercrime*

Cybercrime atau kejahatan di dunia komputer memiliki banyak variasi. Secara prinsip kejahatan di dunia komputer dibagi dalam dua jenis yaitu aktivitas dimana komputer atau prianti digital dipergunakan sebagai alat bantu untuk melakukan tindak kejahatan dan, aktivitas dimana komputer atau piranti digital sebagai objek tindak kejahatan dan yang terakhir aktivitas dimana pada saat yang bersamaan komputer atau piranti digital dijadikan alat untuk melakukan kejahatan terhadap target yang merupakan komputer atau piranti digital juga (Indrajit, 2011). Di dalam dunia kriminal dikenal istilah "tidak ada kejahatan yang tidak meninggalkan jejak", ada banyak objek forensik yang bisa didapatkan diantaranya yaitu *log file* atau catatan aktivitas, *file*, rekaman *email* atau percakapan berupa teks atau suara, rekam jejak interaksi dan lain sebagainya.

2.5. *Autopsy*

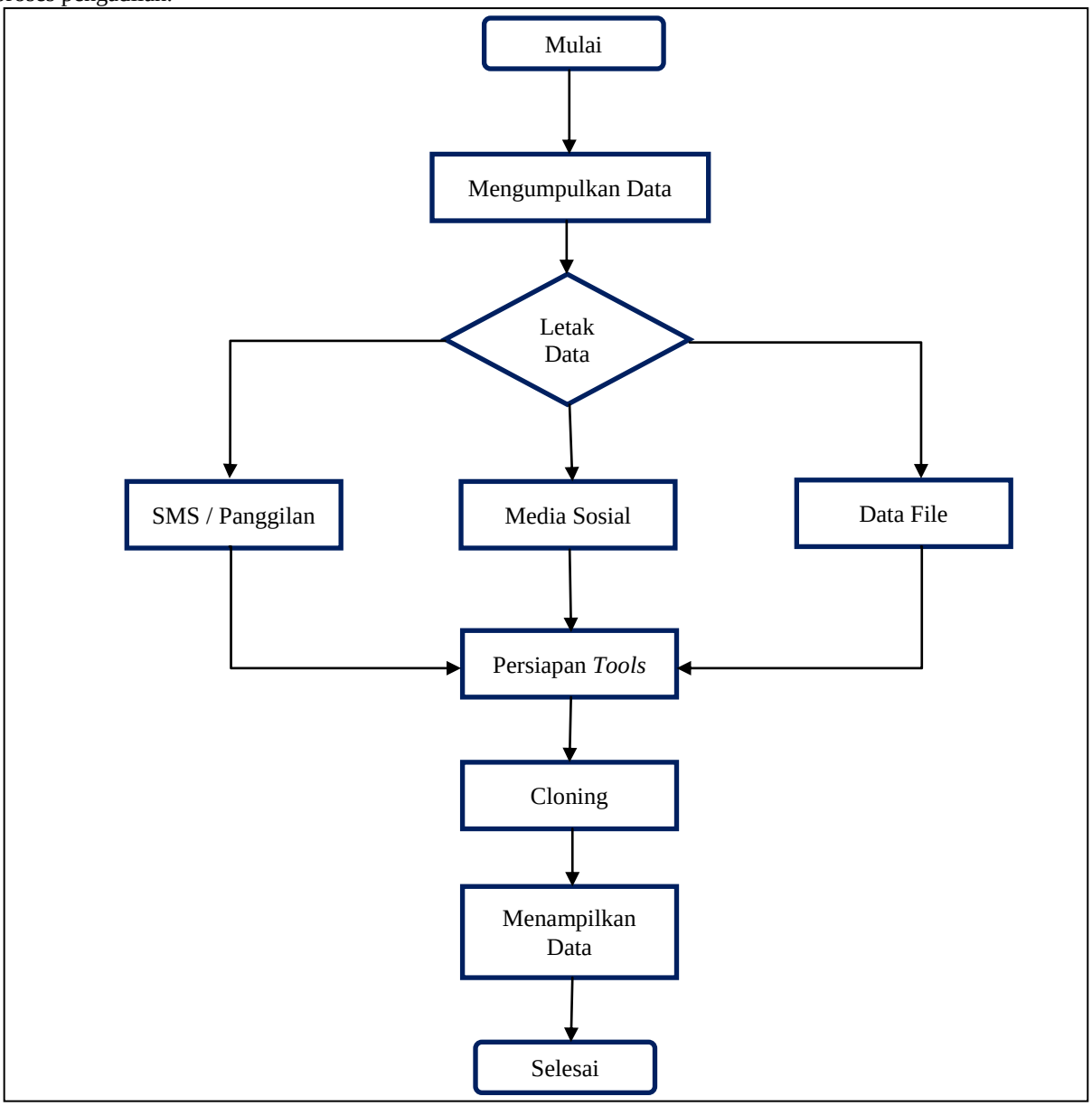
Autopsy merupakan sebauh antarmuka grafis untuk tools di dalam *Sleuth Kit*, yang memudahkan pengguna dalam melakukan investigasi. *Autopsy* sebenarnya adalah sebuah mini web *server* dengan *script* CGI berbasis *perl* dengan tujuan mengubah *file sleuthkit* ke dalam HTML. Sehingga pengguna aplikasi ini membutuhkan web client untuk mengakses manfaat dari *autopsy*. *Autopsy* juga menyediakan fungsi-fungsi administratif tambahan yaitu *logging* (mencatat tindakan/perintah sleuthkit yang telah dijalankan), *notes* (mencatat keterangan tambahan yang diperoleh penyelidik), dan *report* (mencatat hasil analisa). *Autopsy* bersifat opensource yang memberikan banyak fitur untuk menganalisa sistem *Windows* dan *Unix*, tools ini juga dapat menganalisa direktori *file* yang telah dihapus (Vandi Andreas Silalahi, 2017).

3. METODE PENELITIAN

Digital Forensics Investigation Model (DFIF) sudah berkembang sejak tahun 1995, namun belum ada standart yang digunakan untuk mencarai barang bukti digital (Rahayu & Prayudi, 2014). Jadi peneliti menggunakan metode penelitian yang umum digunakan. Metode penelitian adalah dengan menggunakan pedoman forensik yang dibuat pada umumnya dan memiliki beberapa tahapan dan proses, diantaranya:

Gambar 1. Tahapan Penelitian

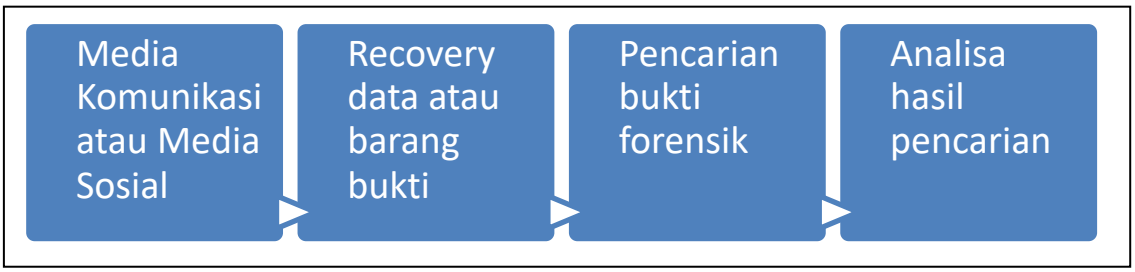
Tahapan pertama dalam proses ini adalah *preservation*, pada tahapan ini yang dilakukan adalah menjaga agar barang bukti dengan data yang ada didalamnya tidak rusak atau hilang. Tahapan ini juga disebut dengan tahap pemeliharaan alat dan bahan sampai pada perjalanan ke laboratorium forensik dan sebelum melakukan tahap selanjutnya yaitu *collecting*. Pada tahap *collecting*, peneliti melakukan pencarian dan mengumpulkan barang bukti dari dalam *smartphone* yang berhubungan dengan kasus atau objek yang sedang diteliti. Setelah semua data sudah didapatkan tahap selanjutanya yaitu *Examination* yaitu mencari data-data yang ada dan membaginya sesuai kategori. Jika ada data dalam *smartphone* yang terindikasi dengan tindak kejahatan maka tiu dapat menjadi barang bukti dan dapat disimpulkan dalam tahap *Analysis* yang dapat membantu pada proses pengadilan.



Gambar 2. Flowchart

Adapun alat dan bahan yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Laptop Lenovo Idepad 310
2. Handphone Iphone 4S
3. USB *connector*
4. *Autopsy*
5. *iRoot*



Gambar 3. Proses Pencarian Barang Bukti

Gambar 2 dan gambar 3 menjelaskan proses pencarian barang bukti digital pada *iphone* 4. Data yang ingin didapat yaitu semua jenis percakapan atau komunikasi yang ada dalam *smartphone* tersebut. Pada tahap *recovery data* ini dimaksudkan untuk mengumpulkan segala macam informasi yang akan dianalisa nantinya. Segala macam informasi bisa berupa hasil percakapan berupa teks, gambar, video dan lain sebagainya yang nantinya akan dilakukan proses pencarian informasi pada tahap selanjutnya menggunakan *tools iRoot* dan *Autopsy*. Pada tahap akhir penelitian yaitu menganalisa hasil pencarian informasi yang sudah didapatkan dari *iphone* 4 kemudian mengklasifikasikan informasi tersebut apakah termasuk pelanggaran atau bukan suatu pelanggaran. Informasi yang didapatkan dapat diperoleh dari aplikasi bawaan iphone 4 seperti pesan dan log panggilan dan diperoleh dari aplikasi media sosial lainnya seperti *Whatsapp, Line, Facebook, Instagram* dan lain sebagainnya. Fokus data yang terpenting adalah log panggilan, kontak, pesan, internet *history*, data dari media sosial yang ada seperti *Facebook, Line, Whatsapp, Instagram* dan sebagainya.

Untuk mendukung hasil penelitian maka dilakukan sebuah simulasi bahwa pemilik iphone 4 telah melakukan jual beli obat terlarang dengan menggunakan aplikasi *Whatsapp* dan juga aplikasi pesan bawaan dari iphone itu sendiri. Setelah itu dilakukan penghapusan data yang terdapat informasi jual beli tersebut yang selanjutnya dapat dicari oleh *tools* yang akan digunakan.

4. HASIL DAN PEMBAHASAN

Setelah dilakukan simulasi menggunakan perangkat iphone 4, diharapkan adanya tindak pidana kejahatan dalam simulasi ini yaitu jual beli obat terlarang dimana pesan dan log panggilan antara pemilik *smartphone* selaku pemakai dan penjual telah dihapus dari *smartphone* tersebut. Dengan demikian informasi yang sudah didapat tadi dapat digunakan sebagai barang bukti yang membantu para penegak hukum dalam memvonis pelaku sesuai pelanggaran yang mereka lakukan.

5. KESIMPULAN

Dengan menggunakan metode forensik dibantu dengan *tools Autopsy* dan *iRoot* diharapkan peneliti dapat menemukan bukti tindak kejahatan yang telah dihapus oleh pelaku.

DAFTAR PUSTAKA

Engman, M. (2013). Forensic investigations of Apple ' s iPhone Kandidatuppsats.

Fauzan, A., Riadi, I., & Fadlil, A. (2017). Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime. *Annual Research Seminar (ARS)*, *2*(1), 159–163. Retrieved from http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752

Hay, A., Krill, D., Kuhar, B., & Peterson, G. (2011). Chapter 20 Evaluating Digital Forensic Options For The Apple iPad, 257–273.

Indrajit, R. E. (2011). Forensik Komputer. *Artikel*, *1*(C), 1–11. Retrieved from http://www.idsirtii.or.id/content/files/IDSIRTII-Artikel-ForensikKomputer.pdf

Mubarok, H., & Widiyasono, N. (2017). Proses Investigasi Mobile Forensik Pada Smartphone Berbasis Ios Investigation Process. *Jurnal Rekayasa Sistem & Industri (JRSI) 4 (01) | Vol: | Issue : | 2017*, *4*(April 2018), 93–98. https://doi.org/10.25124/jrsi.v4i01.149

Mukti, W. A., Masruroh, S. U., & Khairani, D. (2017). Analisa dan Perbandingan Bukti Forensik Apliksai Media Sosial Facebook dan Twitter pada Smartphone Android, *10*(1). https://doi.org/10.15408/jti.v10i1.6820

One, M. (2017). Apple Inc.

Rahayu, Y. D., & Prayudi, Y. (2014). Membangun Integrated Digital Forensics Investigation Frameworks (IDFIF) Menggunakan Metode Sequential Logic. *Seminar Nasional SENTIKA*, *2014*(Sentika).

Sahiruddin , Imam Riadi, S. (2017). Analisis Forensik Recovery dengan Kemanan Fingerprint pada Smartphone Android, 278–282.

Statista. (2017). Mobile OS share in Indonesia 2012-2017 | Statistic. Retrieved from https://www.statista.com/statistics/262205/market-share-held-by-mobile-operating-systems-in-indonesia/

Vandi Andreas Silalahi, I. S. (2017). Analisis Digital Forensics Investigation pada Bukti DIgital Steganography. https://doi.org/10.1111/j.1469-7610.2010.02280.x

Yadi, I. Z., & Kunang, Y. N. (2014). Analisis forensik pada Android. *Konferensi Nasional Ilmu Komputer (KONIK)*, 141–148.

Autopsy Forensik Browser dan SAFFA-NG – Beni Prakoso. (n.d.).