ANALISIS *RECOVERY* BUKTI DIGITAL *INSTAN MESSENGER* PADA *SMARTPHONE* ANDROID MENGGUNAKAN METODE *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)* STUDI KASUS : KASUS PERSELINGKUHAN

Achmad Syauqi[1]
[1]Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Peradaban
okysyauqi@peradaban.ac.id
Jalan Raya Pagojengan Km 3, Paguyangan, Brebes

Kata Kunci:

bukti digital, recovery, mobile, messanger.

Abstrak

Teknologi pada perangkat mobile sangat pesat perkembangannya jika dibandingkan dengan teknologi pada perangkat computer *desktop.* Saat ini hampir setiap orang sudah memiliki perangkat mobile seperti HP dan *Smartphone* khususnya android. Banyak pihak yang memanfaatkan perkembangan teknologi ini baik untuk tindak kejahatan maupun untuk kegiatan positif. Termasuk di dalamnya untuk tindakan perselingkuhan. Beberapa orang memanfaatkan teknologi tersebut agar tidak diketahui oleh pasangannya. Salah satu metode yang sering digunakan yaitu *National Institute Of Standards and Technology (NIST).* Metode ini menjadi dasar dari pengolahan *digital forensics* dari awal sampai dengan akhir. Sedangkan *tools* yang banyak digunakan untuk mengakuisisi bukti digital pada perangkat *smartphone* yaitu *Oxygen Forensics.*

Keywords:

Digital evidence, recovery, mobile, messanger

Abstract

Technology on mobile devices is very rapidly developing when compared to technology on desktop computer devices. Currently, almost everyone already has a mobile device such as cellphones and smartphones, especially Android. Many parties take advantage of this technological development both for crime and for positive activities. This includes the act of adultery. Some people take advantage of this technology so that their partner does not know. One method that is often used is the National Institute of Standards and Technology (NIST). This method forms the basis of digital forensics processing from start to finish. While the tools that are widely used to acquire digital evidence on smartphone devices are Oxygen Forensics.

Pendahuluan

Teknologi pada perangkat *mobile* sangat pesat perkembangannya jika dibandingkan dengan teknologi pada perangkat computer *desktop.* Saat ini hampir setiap orang sudah memiliki perangkat mobile seperti HP dan *Smartphone* khususnya android. Tidak hanya perkembangan *hardware* dan sistemnya saja yang pesat, perkembangan aplikasi di dalamnya pun sangat pesat. Hampir aplikasi apa saja yang dibutuhkan oleh seseorang sudah terdapat di dalam *playstore* maupun *appstore*. Developer aplikasi pun sudah menjamin bahwa aplikasinya sudah aman dan melalui tahap pengujian terlebih dahulu [1]. Banyak pihak yang memanfaatkan perkembangan teknologi ini baik untuk tindak kejahatan maupun untuk kegiatan positif. Termasuk di dalamnya untuk tindakan perselingkuhan. Beberapa orang memanfaatkan teknologi tersebut agar tidak diketahui oleh pasangannya.

Bukti elektronik merupakan barang bukti yang bersifat nyata dan dapat dilihat wujudnya, sedangkan bukti digital merupakan barang bukti yang diambil dari proses akuisisi barang bukti elektronik tersebut. Untuk mendapatkan barang bukti digital tersebut harus melalui proses yang khusus dan legal sehingga bukti digital tersebut dapat diakui. Salah satu bidang ilmu komputer yang mempunyai spesifik ilmu disana yaitu *Digital* forensics. Orang yang melakukan proses pengambilan bukti digital maupun menganalisis file bukti digital juga harus sudah mempunyai kehalian dibidangnya, hal ini dibuktikan dengan sertifikasi yang didapatkan mengingat bukti digital bersifat sangat mudah rusak dan hilang identitasnya.

Salah satu *tools* yang ada dipasaran untuk mengakuisisi data dari *smartphone* yaitu *Oxygen Forensics.* Aplikasi ini dapat mengakuisisi seluruh data yang ada pada *smartphone*. Sehingga data yang dibutuhkan oleh *investigator* dalam menganalisis sebuah kasus dapat tersedia tanpa kekurangan file yang tidak dapat diambil datanya.

Landasan Teori

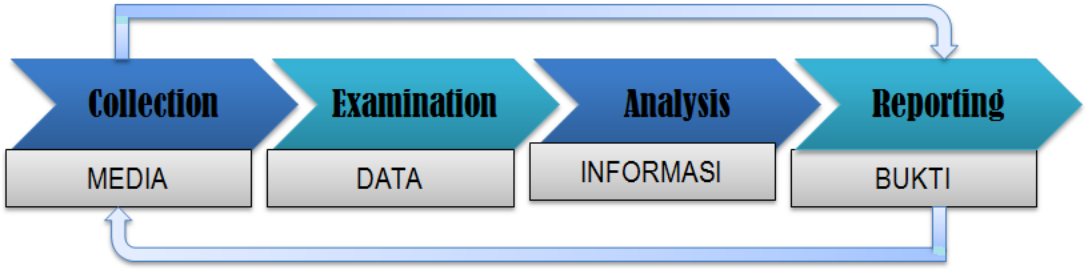
Digital Forensics merupakan bidang ilmu komputer yang mempelajari tentang penemuan dan investigasi data pada perangkat digital [2]. Proses pengambilan data atau bukti digital memerlukan perlakuan yang khusus dan legal, karena *file* digital sangat mudah rusak dan berubah identitasnya. Orang yang melakukannya juga memerlukan keahlian sendiri, dapat dibuktikan dengan mengikuti kelas professional dan sertifikasi.

Banyak metode dan *tools* untuk melakukan proses *imaging* pada perangkat digital baik yang berbayar maupun dapat diunduh secara gratis. Contoh *tools* yang sering digunakan untuk proses ini antara lain *FTK Imager, Encase*. Sedangkan untuk proses *imaging* pada perangkat mobile terdapat *Oxygen Forensics, Mobiledit,* dan lain sebagainya.

Salah satu aplikasi yang diambil datanya yaitu *instan messanger* [3]. Karena aplikasi pesan ini menjadi aplikasi paling dasar dan menjadi aplikasi yang sudah pasti ada di dalam *smartphone.* Karena semua *Smartphone* terdapat aplikasi ini. Selain *instan messanger* sudah ada beberapa penelitian yang melakukan investigasi perangkat android tentang *skype* [4], *gmail* [5], *Instagram* [6], dan masih banyak yang lain.

Metode

Proses untuk mendapatkan bukti digital pada *smartphone* beraneka ragam. Salah satu metode yang baik untuk mengambil bukti digital yaitu *National Institute Of Standards and Technology (NIST)* [7]. Metode ini merupakan rekomendasi dasar pada proses forensika digital. Tahapan pada metode ini antara dapat dilihat pada gambar 1:



Gambar 1. Metode *National Institute Of Standards and Technology (NIST)*

1. *Collection*
   Merupakan tahap pengambilan bukti digital dari bukti elektronik yang sudah ada dengan tata cara khusus dan legal agar bukti digital tersebut dapat diakui.
2. *Examination*
   Merupakan tahap pemeriksaan terhadap bukti digital yang telah diambil, tentunya menggunakan cara khusus dan legal agar bukti digital tersebut tidak rusak atau mengubah identitasnya serta dapat diakui.
3. *Analysis*
   Tahap menganalisis bukti digital tersebut sehingga dapat diambil kesimpulan atau jalan cerita dari kasus yang ada. Tentunya dengan cara yang legal juga.
4. *Reporting*
   Reporting merupakan tahap akhir dari proses pengolahan bukti digial yaitu dengan memberikan laporan sesuai dengan temuan yang ada pada bukti digital tersebut.

Hasil dan Pembahasan

1. *Collection*

   Penelitian ini menggunakan barang bukti berupa *smartphone* dengan merk LG dan type Optimus L3 II (E425). Detail informasi dari perangkat yg dianalsis dapat dilihat pada tabel 1:

Tabel 1. Informasi *Device*

Merk	LG
Model	Optimus L3 II (E45)
IMEI	356071050028340
Software Version	Android OS 4.1.2

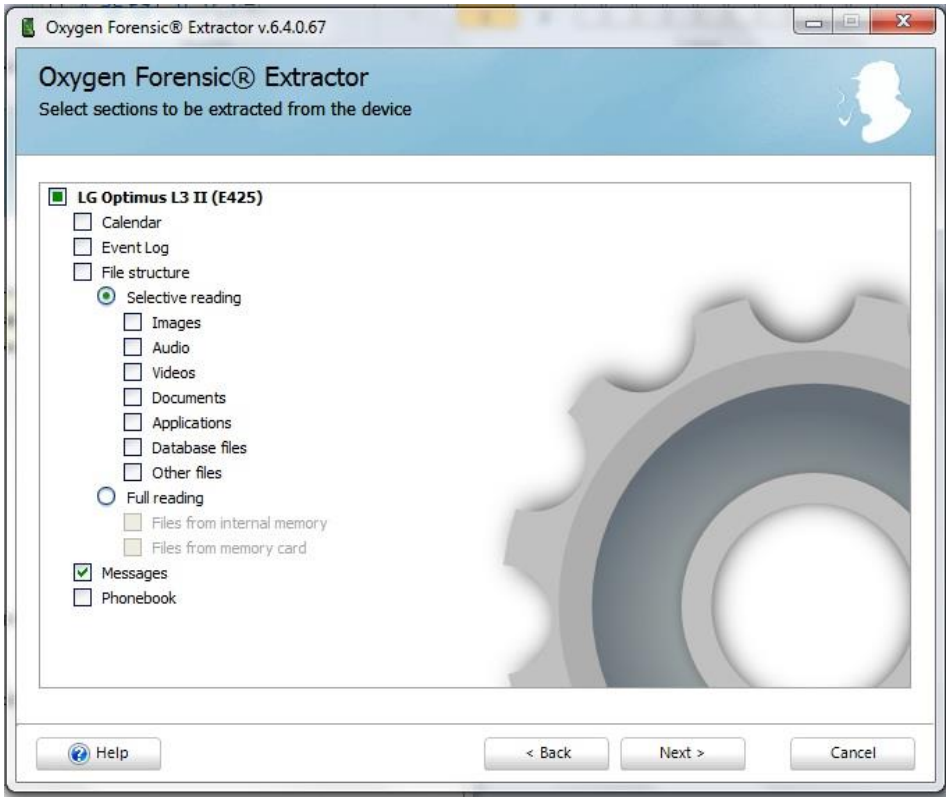
Informasi hardware komputer yang di gunakan untuk proses *collection* atau *imaging* dapat dilihat pada tabel 2:

Tabel 2. Informasi Perangkat Hardware

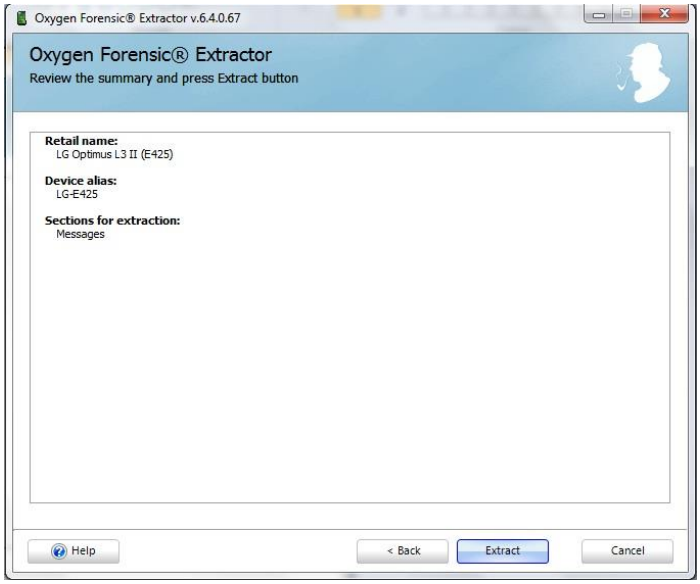
Merk	Lenovo
Processor	Intel Core i5 7200U
RAM	12 Gb
Hardisk	1 Tb
Grafis	Nvidia Geforce 920MX

2. *Examination*

   Tools untuk proses *collection* bukti digital menggunakan software *Oxygen Forensics* dan aplikasi e-root untuk proses rooting device. *Oxygen Forensics* merupakan aplikasi *imaging* atau proses mengambilan bukti digital yang terkenal dan sudah di akui untuk *imaging* pada perangkat *smartphone*. Sudah banyak ahli forensika digital yang menggunakan applikasi ini. Proses *imaging* untuk mengambil data pada *instan messanger* dapat dilihat pada gambar 2 dan gambar 3:



Gambar 2. Proses *Imaging*

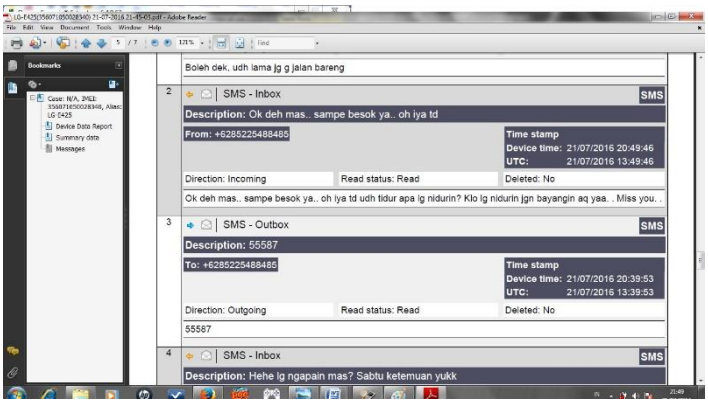


Gambar 3. Proses *Imaging* (Lanjutan)

Proses ini akan mengambil seluruh data *instan messanger* yang ada pada *smartphone* tersebut. Dan hasil bukti digital yang didapatkan dapat dipertanggungjawabkan keasliannya karena semua langkah sudah menggunakan cara yang tepat dan didokumentasi dengan baik serta user yang melakukan proses tersebut sudah memiliki sertifikat keahlian sesuai dengan bidangnya dan diakui.

3. *Analysis*

Hasil dari proses *collection* pada aplikasi *instan messanger* dapat dilihat pada gambar 3:



Gambar 3. Hasil

Berdasarkan analisis data pada hasil ekstraksi *instan messanger* tersebut, setelah proses pemeriksaan bukti digital pada *instan messanger* terdapat temuan pesan percakapan yang diduga sebagai kasus perselingkuhan dengan nomor dan pesan yang diduga sebagai nomor tersangka perselingkuhan. Temuan ini nantinya akan dibuat laporannya pada tahap *reporting* dan diserahkan kepada pihak yang berwenang untuk diproses lebih lanjut.

4. *Reporting*

Tahap ini menuliskan semua hasil temuan yang didapat dari proses investigasi, dalam penulisan laporan tidak ada yang dikurangi dan dilebihkan. Semua hasil temuan dituliskan secara lengkap dan rinci sesuai dengan prosedur yang ada. Dan hasil laporan ini kemudian diserahkan kepada pihak berwenang.

Kesimpulan dan Saran

Ilmu *Digital Forensics* dapat digunakan untuk mencari bukti digital dari kasus kejahatan komputer yang terjadi di dunia ini. Karena file bukti digital sangat rentan terjadi kerusakan, untuk mengambilnya diperlukan tata cara yang khusus serta legal agar file tersebut dapat diakui keasliannya. Salah satu kasus kejahatan komputer yang terjadi menggunakan *smartphone*. Berdasarkan hasil investigasi dari kasus ini ditemukan bukti percakapan tentang perselingkuhan. Penelitian ini telah berhasil mengakuisisi bukti digital pada aplikasi *instan messanger* sehingga bukti digital tersebut dapat dianalisis dan diperoleh

hasilnya. Tentunya semua proses yang dilakukan dengan tata cara yang legal sehingga bukti digital tersebut nantinya dapat dipertanggungjawabkan. Saran dari penulis, proses recovery bukti digital pada *smartphone* ini dapat dikembangkan lagi untuk aplikasi-aplikasi lain seperti sosial media, *e-commerce,* karena rawan untuk disalahgunakan.

Referensi

[1] A. Syauqi, I. Riadi and Y. Prayudi, "Validation Policy Statement on the Digital Evidence Storage using First Applicable Algorithm," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 10 no 10, 2019.

[2] B. Raharjo, "SEKILAS MENGENAI FORENSIK DIGITAL," *Jurnal Sosioteknologi,* vol. 29, 2013.

[3] M. Unik, V. G. Larenda and H. Mukhtar, "ANALISIS INVESTIGASI ANDROID FORENSIK SHORT MESSAGE SERVICE (SMS) PADA SMARTPHONE," *JOISIE Jurnal Of Information SystemAnd Informatics Engineering,* vol. 3 no 1, 2019.

[4] M. R. Setyawan, A. Yudhana and A. Fadlil, "IDENTIFIKASI BUKTI DIGITAL SKYPE DI SMARTPHONE ANDROID DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)," *Seminar Nasional Teknologi Fakultas Teknik Universitas Krisnadwipayana,* 2019.

[5] H. "ANALISIS KEAMANAN APLIKASI EMAIL BAWAAN ANDROID DAN GMAIL PADA JARINGAN NIRKABEL," *Teknoin,* 2017.

[6] I. Riadi, A. Yudhana and M. C. F. Putra, "ANALISIS RECOVERY BUKTI DIGITAL INSTAGRAM MESSANGERS MENGGUNAKAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)," 2017.

[7] I. Riadi, A. Yudhana and M. C. F. Putra, "ANALISIS RECOVERY BUKTI DIGITAL INSTAGRAM MESSANGERS MENGGUNAKAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)," *Seminar Nasional Teknologi Informasi dan Komunikasi - SEMANTIKOM,* 2017.