Analisis Forensik *Smartphone* Android Menggunakan Metode *NIST* dan *Tool MOBILedit Forensic Express*

Nasirudin[1], Sunardi[2], Imam Riadi[3]

[1]Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
[3]Program Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta
e-mail: [1]nasir.achink80@gmail.com, [2]sunardi@uad.mti.ac.id, [3]imam.riadi@uad.mti.ac.id

Submitted Date: March 08th, 2020 Reviewed Date: March 09th, 2020
Revised Date: March 29th, 2020 Accepted Date: March 30th, 2020

Abstract

Technological advances are growing rapidly, including mobile device technology, one of which is an Android smartphone that is experiencing rapid progress with a variety of features so that it can spoil its users, with the rapid development of smartphone technology, many users benefit, but many are disadvantaged by the growing smartphone. technology, so that many perpetrators or persons who commit crimes and seek profits with smartphone facilities. Case simulation by securing Samsung Galaxy A8 brand android smartphone evidence using the MOBILedit forensic express forensic tool with the National Institute of Standards and Technology (NIST) method which consists of four stages of collection, examination, analysis and reporting. The results of testing the Samsung Galaxy A8 android smartphone are carried out with the NIST method and the MOBILedit Forensic Express tool obtained by data backup, extraction and analysis so that there are findings sought for investigation and evidence of crimes committed by persons using android smartphone facilities.

Keywords: Analysis; Forensics; NIST; Tool

Abstrak

Kemajuan teknologi semakin berkembang pesat, di antaranya teknologi perangkat handphone salah satunya *smartphone* android yang mengalami kemajuan pesat dengan berbagai fitur sehingga dapat memanjakan penggunanya, dengan semakin berkembang pesatnya teknologi *smartphone* banyak pengguna yang mendapatkan keuntungan akan tetapi banyak pula yang dirugikan dengan adanya *smartphone* yang semakin berkembang teknologi, sehingga banyak pelaku atau oknum yang melakukan tindak kejahatan dan mencari keuntungan dengan fasilitas *smartphone*. Simulasi kasus dengan cara mengamankan barang bukti *smartphone* android merk Samsung galaxy A8 dengan menggunakan *tool forensic* MOBILedit forensic express dengan metode *National Institute of Standard and Technology* (NIST) yang terdiri dari empat tahapan *collection*, e*xamination*, *analysis* dan *reporting*. Hasil pengujian barang bukti *smartphone* android Samsung galaxy A8 yang dilakukan dengan metode NIST dan tool MOBILedit Forensic Express diperoleh *backup* data, dilakukan extraksi dan analisis sehingga terdapat temuan-temuan yang dicari guna penyelidikan dan bukti kejahatan yang dilakukan oleh oknum dengan menggunakan fasilitas *smartphone* android.

Kata Kunci: Analisis; Forensik; NIST; *Tool*

1. Pendahuluan

Indonesia adalah Negara yang sedang berkembang pesat dalam menggunakan teknologi di antaranya teknologi *smartphone* berbasis android yang semakin hari dikembangkan oleh pengembang *system* android guna memanjakan penggunaa dan pelanggan. Dengan semakin berkemajuan tersebut, teknologi tidak jarang pula masih ada yang awam dalam menggunakan *smartphone* android sehingga banyak data atau file yang hilang dan tidak muncul lagi pada *smartphone* android, alhasil pengguna *smartphone* android merasa kebingungan dan bagaimana cara

mengembalikan atau *recovery* data yang hilang baik hilang disengaja ataupun tidak disengaja.

Tidak sedikit pula oknum yang melakukan tindak kejahatan dengan menggunakan fasilitas *smartphone* android dan dengan sengaja membuang *file-file* atau data-data hasil kejahatan, guna menghilangkan barang bukti digital agar terhindar dari jeratan hukum yang memberatkan dakwaan dengan barang bukti digital tersebut (Riadi, Sunardi, & Sahiruddin, 2019).

Smartphone android sendiri merupakan perangkat *hybrid* yang bisa bekerja sebagai ponsel dan juga bisa bekerja hampir seperti komputer tapi dalam bentuk portable yang lebih simpel. Dengan meningkatkan 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 dan disimpan dalam ponsel pintar ini meningkatkan juga banyaknya fokus penelitian di bidang perangkat *mobile* forensik (Yadi & Kunang, 2014).

Namun permasalahan yang sering terjadi pelaku tindak kejahatan biasanya mencoba menghapus beberapa atau keseluruhan pesan *messenger* yang dianggap penting dengan tujuan untuk menghilangkan atau membuang barang bukti. Tetapi biasanya seorang penyidik kasus tindak kejahatan akan meminta data pesan Telegram messenger pelaku tindak kejahatan kepada pihak operator telekomunikasi untuk mendapatkan barang bukti. Namun hal ini biasanya memakan proses yang lama untuk mendapatkan data tersebut dari pihak operator Telegram. Bukti digital memiliki peranan yang sangat penting dalam mengungkapkan sebuah tindak kejahatan digital. Terdapat empat tahapan dalam pembuktian bukti digital, yaitu identifikasi bukti digital, penyimpanan bukti digital, analisa bukti digital dan presentasi bukti digital. Keempat tahapan tersebut memiliki tugas dan fungsi masing-masing dalam pengungkapan bukti digital (Riadi, Sunardi, & Sahiruddin, Februari 2020).

Pada banyak kasus penyidik hanya mendapatkan barang bukti sebuah handphone tanpa sim card dan nomor pelaku, di sinilah peranan *mobile forensics* dilakukan untuk mendapatkan barang bukti digital yang akan digunakan dalam menggungkapkan kasus tindak kejahatan dengan menganalisa isi dari handphone tersebut. *Mobile Forensics* merupakan ilmu turunan dari ilmu pengetahuan *digital forensics* atau yang lebih dikenal sebagai komputer forensik. *Digital forensics* merupakan metode ilmiah yang mempelajari tentang cara pemeliharaan, pengumpulan, validasi, analisis, interprestasi, dokumentasi dan presentasi bukti digital yang bersala dari sumber-sumber digital untuk tujuan menfasilitasi rekontruksi peristiwa pidana atau membantu untuk mengantisipasi tindakan yang terbukti melanggar prosedur yang telah ditentukan (Riadi, Umar, & Nasrulloh, May 2018).

Berdasarkan latar belakang tersebut diatas dapat diidentifikasi diantaranya banyaknya kemungkinan tindak kejahatan melalui layanan Telegram *messenger* yang digunakan sehingga perlu dilakukan analisis *forensic* digital untuk menemukan bukti digital yang dapat digunakan dalam proses persidangan, banyaknya yang memanfaatkan oleh pihak oknum yang memusnahkan bukti digital terkait kejahatan yang telah diperbuat. Permasalahan yang akan dibahas dalam penelitian ini bagaimana cara proses *mobile forensic* mampuh mencari informasi dan bukti digital berkaitan dengan kejahatan yang dilakukan oleh oknum pada telegram *messenger* dengan *tool* MOBILedit forensic express, dengan metode *National Institute of Standard and Technology* (NIST) dan bagaimana cara kerja tool tersebut dengan metode NIST.

Adapun tujuan dari penelitian ini adalah melakukan proses investigasi dengan metode NIST pada Telegram *messenger* menggunakan kedua *tool* yang sudah dipersiapkan dan melakukan pengujian untuk mendapatkan data barang bukti digital pada barang bukti handphone *smartphone*. Dengan manfaat yang didapat dalam penelitian ini sebagai referensi penelitiian yang lain dalam membahas *digital forensic* dan membantu penyidik kasus tindak kejahatan dalam mendapatkan barang bukti digital secepat mungkin melalui *digital forensic*.

2. Metode Penelitian

Obyek penelitian dalam kasus ini yaitu *smartphone* android galaxy A8 dan perangkat lunak yang digunakan pada proses pengambilan barang bukti digital, bukti digital dapat berupa profile dari pemilik *smartphone*, kontak, gambar, SMS, whatssApp dan lain-lain. Alat dan bahan yang digunakan dalam melakukan proses pencarian dan pengambilan barang bukti digital membutuhkan sumber daya yang besar, oleh karena itu dibutuhkan perangkat pendukung untuk proses pencarian dan pengambilan bukti digital

dapat berjalan dengan lancar dan tepat, alat dan bahan yang diperlukan dalam investigasi *forensic* digital dapat dilihat pada Tabel 1.

Tabel 1 Daftar alat dan bahan penelitian

Nama Barang	Deskripsi
Laptop	Merk HP Pavilion G series
Kabel USB	Penghubung laptop dan *smartphone*
Smartphone Android	Merk Samsung Galaxy A8
MOBILedit Forensic	*Tool* Forensik

Sistem yang digunakan merupakan kerangka kerja metode *mobile forensic* yang dibuat oleh *National Institute of Standard and Technology* (NIST). NIST merupakan badan yang bertanggung jawab didalam mengembangkan standar, panduan, dan persyaratan minimum untuk menyediakan keamanan informasi yang cukup bagi semua asset dan pihak-pihak yang memiliki kompetensi di bidang digital *forensic*, metode ini dipergunakan oleh para agen pemerintah pusat di Amerika, namun tidak menutup kemungkinan dapat dipergunakan oleh organisasi seperti akademisi, badan penyidik swasta dan lainnya. Metode NIST terdiri dari 4 tahapan, skema dari 4 tahapan NIST dapat dilihat pada Gambar 1.

Gambar 1 Tahapan Metode NIST

1. *Collection* merupakan tahapan paling awal dari metode NIST, hal-hal yang dilakukan dalam tahapan *collection* diantaranya koleksi, pendokumentasian, isolasi, perservasi barang bukti.
2. *Examination* merupakan bagian kedua melanjutkan tahapan *collection* diantaranya *backup* data dan *imaging system* yang mendukung format *image* dan dapat digunakan dengan *tool* format *image*.
3. *Analysis* merupakan tahapan setelah *examination* dengan menggunakan metode yang dibenarkan secara hukum dan tidak merubah teknik untuk mendapatkan suatu informasi yang berguna dan dapat menjawab apa yang dibutuhkan sebagai pendorong untuk melakukan pengumpulan dan pemeriksaan data.
4. *Reporting* merupakan tahapan akhir setelah 3 tahapan dilakukan guna melakukan proses pelaporan dari hasil tahapan yang meliputi penjelasan mengenai alat, dan prosedur yang dipilih, penggambaran tindakan yang dilakukan, memberikan rekomendasi untuk perbaikan kebijakan, prosedur, alat dan aspek lain dalam *forensic*.

3. Hasil dan Pembahasan

Simulasi penelitian ini mengangkat kasus tentang adanya laporan dari salah satu perusahaan PT Rayya Trans yang diindikasikan salah satu karyawan divisi *purchasing* menggelapkan dana belanja *sparepart*. Dengan adanya laporan tersebut peneliti mengambil barang bukti berupa satu buah *smartphone* android milik manajer *purchasing* yang sudah diamankan sebelumnya oleh pimpinan perusahaan dan peneliti melakukan pemeriksaan terhadap *smartphone* yang dijadikan barang bukti untuk diambil bukti digital, peneliti kemudian melakukan langkah-langkah *forensic* untuk mendapatkan bukti digital. Peneliti melakukan tahapan penelitian dengan metode NIST yaitu *collection*, *examination*, *analysis*, *reporting*. Penelitian ini menggunakan barang bukti berupa satu unit *smartphone* yang diskenariokan telah dikoleksi oleh peneliti terlihat pada Gambar 2.

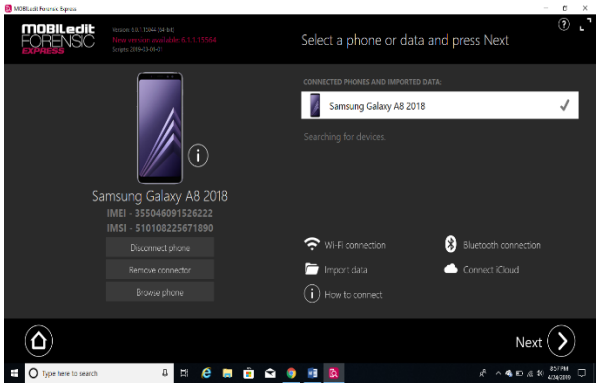
Gambar 2 *Smartphone* Android Samsung

Adapun spesifikasi dari *smartphone* sebagai barang bukti terlihat pada Tabel 2.

Tabel 2 Spesifikasi *Smartphone* Barang Bukti

Detail Perangkat	Spesifikasi
Samsung Galaxy	A8
Nomor Model	SM-A530F/DS
Nomor serial	RR8KC0988DW
Versi Adroid	8.0.0
Processor	Octa-Core2x2.2 GHZ
RAM	6GB
ROM	64GB

Setelah dilakukan koleksi dicatat secara detail dan diamankan dengan cara mematikan saluran data atau diaktifkan mode *airplan* atau mode terbang, kemudian dilakukan pengamanan data dengan cara *backup* data, setelah terdeteksi oleh *tool* MOBILedit Forensic Express dilakukan pemilihan tempat penyimpanan terlihat pada Gambar 3 guna memudahan dalam pencarian hasil data *backup smartphone* guna proses lebih lanjut.



Gambar 3 Penyimpanan *Backup* Data

Hasil dari *backup* setelah ditentukan tempat penyimpanan dan dihasilkan data *backup* smartphone android samsung terlihat pada Gambar 4.

adb_backup	5/1/2019 3:13 PM	File folder	
backup_files	4/25/2019 8:54 AM	File folder	
mobiledit_export_files	4/25/2019 9:16 AM	File folder	
pdf_files	4/25/2019 5:46 AM	File folder	
log_full	4/25/2019 7:21 AM	Text Document	4,447 KB
log_short	4/25/2019 3:10 AM	Text Document	156 KB
mobiledit_backup	4/25/2019 3:28 AM	XML Document	10,918 KB
mobiledit_export	4/25/2019 7:17 AM	XML Document	32,599 KB
Report	4/25/2019 6:47 AM	Foxit Reader PDF ...	411,862 KB
report_configuration.cfg	4/24/2019 9:21 PM	CFG File	1 KB
report_html	4/25/2019 5:45 AM	WinRAR ZIP archive	6,856,905 KB

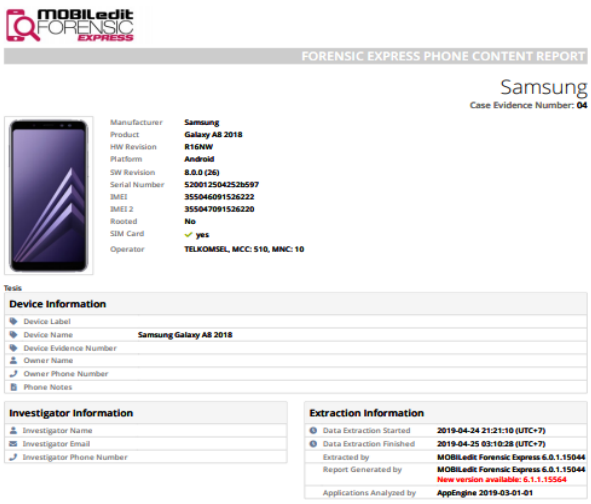
Gambar 4 Hasil *Backup* Data *Smartphone*

Setelah *backup* data selesai kemudian dilanjutkan ketahapan ke dua yaitu *examination* di mana pengambilan dan pemeriksaan data *backup* dan hasil *examination* terlihat pada Gambar 5.

Report	4/25/2019 6:47 AM	Foxit Reader PDF ...	411,862 KB
report_configuration.cfg	4/24/2019 9:21 PM	CFG File	1 KB
report_html	4/25/2019 5:45 AM	WinRAR ZIP archive	6,856,905 KB
xlsxReport	4/25/2019 7:20 AM	Microsoft Excel W...	4,702 KB
xlsxReport_Applications_Adobe Clip	4/25/2019 7:19 AM	Microsoft Excel W...	6 KB
xlsxReport_Applications_Application List	4/25/2019 7:19 AM	Microsoft Excel W...	162 KB
xlsxReport_Applications_Bixby Vision	4/25/2019 7:19 AM	Microsoft Excel W...	3 KB
xlsxReport_Applications_BixbyVision Fra...	4/25/2019 7:19 AM	Microsoft Excel W...	4 KB
xlsxReport_Applications_Halaman Depan ...	4/25/2019 7:19 AM	Microsoft Excel W...	3 KB
xlsxReport_Applications_Hapo	4/25/2019 7:19 AM	Microsoft Excel W...	5 KB
xlsxReport_Applications_iCSee Pro	4/25/2019 7:19 AM	Microsoft Excel W...	4 KB
xlsxReport_Applications_Instagram	4/25/2019 7:19 AM	Microsoft Excel W...	3 KB
xlsxReport_Applications_JOOX	4/25/2019 7:19 AM	Microsoft Excel W...	4 KB
xlsxReport_Applications_Layanan Samsu...	4/25/2019 7:19 AM	Microsoft Excel W...	3 KB
xlsxReport_Applications_LINE	4/25/2019 7:19 AM	Microsoft Excel W...	115 KB
xlsxReport_Applications_Maps	4/25/2019 7:19 AM	Microsoft Excel W...	6 KB
xlsxReport_Applications_OneDrive	4/25/2019 7:19 AM	Microsoft Excel W...	3 KB
xlsxReport_Applications_Penyimpanan ka...	4/25/2019 7:19 AM	Microsoft Excel W...	3 KB

Gambar 5 Hasil Tahapan *Examination*

Setelah dilakukan tahapan *examination* kemudian dilanjutkan ke tahapan *analysis* yaitu tahapan melihat hasil dari tahapan *examination* secara rinci untuk didapatkan bukti digital dari barang bukti yang sudah dilakukan tahapan-tahapan sebelum *analysis*, dalam tahapan ini dapat dilakukan secara manual maupun dengan tambahan bantuan perangkat lunak yang beredar di dunia *forensic* digital. Di sini peneliti melakukan tahapan *analysis* secara manual dan hasil *analysis* yang didapatkan terlihat pada Gambar 6.



Gambar 6 Hasil *Analysis* Manual

Gambar 7 menunjukan hasil *analysis* secara manual yang telah dipisah atau dipilih-pilih satu persatu untuk mencari bukti digital setelah dilakukan tahapan *collection* dan *examination.*

2019-04-25 05:46:42 (UTC+7) Generated by Compelson MOBILedit Forensic Express 6.0.1.15044 II

Case Label: Samsung Case Evidence Number: 04 Device Label:

Table of Contents

2019-04-25 05:46:42 (UTC+7) Generated by Compelson MOBILedit Forensic Express 6.0.1.15044 III

Gambar 7 Hasil *Analysis* Manual

Setelah dilakukan tahapan *analysis* tahapan terakhir yaitu tahapan *reporting* merupakan tahapan akhir dari metode NIST yang akan melaporkan hasil *analysis* mencakup deskripsi kasus yang terjadi, teknik *tool* yang digunakan, ada atau tidaknya tindakan, pedoman, prosedur, perangkat dan aspek lain yang berkaitan dengan penelitian tahapan *reporting* pada penelitian ini. Adapun informasi bukti fisik dalam penelitian ini yaitu berupa *smartphone* berbasis android, dengan bukti digital profile pengguna, kontak, email, *chat*, dan gambar yang terdeteksi keseluruhan 75% dari data yang ada pada *smartphone*. Tabel *reporting* terlihat pada Tabel 3.

Tabel 3 *Reporting* NIST

Deskripsi	Total
Contact	1527
Messages	149
Email	278
Call	500
Photos	38
Images File	2038

4. Diskusi

Dalam penelitian ini masih banyak kekurangan karena itu untuk para pembaca koreksi dan saran sangat dibutuhkan guna penyempurnaan penulisan jurnal ini, oleh karena itu ke depannya akan terus dikembangkan penelitian ini dengan perpaduan *tool forensic* dan literatur yang ada.

5. Kesimpulan

Hasil *forensic smartphone* berbasis android merk samsung galaxy A8 dihasilkan beberapa dari target yang diinginkan guna dianalisa dan dikembangkan untuk mendapatkan bukti digital dengan metode *National Institut of Standard and Technology* dan menggunakan *tool* MOBILedit.

Forensic Express dan dianalisa secara manual sehingga hasil yang didapat belum terpenuhi, ke depannya penulis akan mengembangkan cara menganalisa agar terdapat hasil bukti digital yang diharapkan guna kepentingan penyidikan kasus kejahatan digital.

Daftar Pustaka

Riadi, I., Sunardi, & Sahiruddin. (2019). Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ). *JURTI, 3*(1), 2579-8790.

Riadi, I., Sunardi, & Sahiruddin. (Februari 2020). Perbandingan Tool Forensik Data Recovery Berbasis Android MenggunakanMetode NIST. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 7*(1), 2355-7699.

Riadi, I., Umar, R., & Nasrulloh, I. M. (May 2018). Analisis Forensik Digital Pada Frozen Solid State Drive dengan Metode National Institute Of Justice (NIJ)J). *ELINVO(Electronics, Informatics, and Vocational Education), 3*(1), 2580-6424.

Yadi, I. Z., & Kunang, Y. N. (2014). Analisis Forensik pada Platform Android. *Konferensi Nasional Ilmu Komputer (KONIK)*, 2338-2899.