METODE NIST UNTUK ANALISIS FORENSIK BUKTI DIGITAL PADA PERANGKAT ANDROID

Rusydi Umar[1],Sahiruddin[2]
[1,2]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Ahmad Dahlan
e-mail: [1]rusydi_umar@rocketmail.com, [2]sahiruddinbuton@gmail.com

ABSTRAK

Perangkat seluler mengalami kemajuan yang sangat pesat seiring dengan perkembangan teknologi. Perkembangan teknologi tidak hanya memberikan dampak positif bagi penggunnanya, namun memiliki dampak negatif ketika perkembagan tersebut digunakan sebagai media untuk melakukan tindakan kejahatan. Smartphone saat ini menjadi media terdepan yang mendukung adanya tindakan kejahatan. Bukti digital berupa percakapan yang telah dihapus menjadi kendala untuk membuktikan tindakan kejahatan tersangka dalam persidangan. Penelitian ini menggunakan dua tool forensik Wondershare dr. Fone for Android dan Oxygen Forensics Suite 2014 untuk mendapatkan bukti digital berupa data kontak, log panggilan, dan pesan yang telah dihapus pada smartphone android, dan menggunakan metode National Institute of Standard and Technology (NIST). Hasil penelitian ini adalah Wondershare dr. Fone for Android berhasil mengembalikan data terhapus dengan keberhasilan 30%, sementara Oxygen Forensics Suite 2014 berhasil mengembalikan data terhapus dengan keberhasilan mencapai 73%. Dari hasil yang diperoleh dapat disimpulkan bahwa bukti digital hasil recovery dengan Oxygen Forensics Suite 2014 dapat digunakan sebagai barang bukti dalam persidangan

***Kata Kunci**: Forensik, Smartphone, Android, NIST.*

1. PENDAHULUAN

Perangkat seluler mengalami kemajuan yang sangat pesat seiring dengan perkembangan teknologi [1]. Salah satu bentuk teknologi yang perkembangannya dapat langsung dinikmati dan diaplikasikan dalam kehidupan sehari-hari adalah telepon genggam (*smartphone*). Perangkat *smartphone*kini memiliki fungsi yang sama dengan komputer[2].Situs internetlivestats.com menunjukkan lebih dari 6 juta *smartphone* terjual tiap harinya, hal inimenunjukkan bahwa pengguna *smartphone* terus bertambah, termasuk di dalamnya penggunas*martphone* dengan sistem operasi Android[3]. Perkembangan teknologi tidak hanya memberikan dampak positif bagi penggunanya tetapi, perkembangan teknologi mempunyai sisi negatif ketika perkembangan tersebut dimanfaatkan untuk suatu tindakan kejahatan yang merugikan pihak lain[4].

Saat ini banyak tindakan kejahatan digital yang dilakukan dengan *smartphone* android sebagai mediakomunikasi untuk tujuan kriminal seperti perdagangan narkoba, kegiatan teroris,perencanaan pembunuhan, dan kegiatan kriminal lainnya.Kejahatan yang dilakukan oleh pelaku tentunya akanmeninggalkan barang bukti berupa bukti digital percakapan tentang kejahatan yang dilakukan oleh pelaku[5]. Bukti digital yang telah dihapus oleh pelaku menjadi kendala bagi penegak hukum untuk membuktikan kajatahan tersangka dalam persidangan sehingga, untuk mendapatkan kembali barang bukti tersebut penegak hukum harus melakukan proses forensik digital.Penelitian ini bertujuan untuk mengembalikan data yang telah dihapus berupa data kontak, log panggilan, dan pesan pada perangkat *smartphone* yang menjadi barang bukti untuk menyelesaikan kasus kejahatan penjualan narkoba dalam persidangan. Pengambilan barang bukti digital pada penelitian ini yaitu dengan menggunakan metode yang dikembangkan oleh *National Institute of Standard and Tecnology*(NIST)[6].Pengangkatan barang bukti dapat dilakukan dengan dua cara yaitu*dead forensic* dan *live forensic*. *Dead forensic* merupakan suatu teknik yang membutuhkandata yang disimpan secara permanen dalam perangkat media penyimpanan umumnya*hardisk*. *Live forensic* yaitu suatu teknik analisis menyangkut data yang berjalanpada sistem atau data *volatile* yang umumnya tersimpan pada *Random Access Memory*(RAM) atau transit pada jaringan[7].

2. TINJAUAN PUSTAKA

2.1. ForensikDigital

Forensik Digital merupakan aplikasi dalam ilmu pengetahuan terutama teknologi komputer yang berguna untuk pembuktian di bidang hukum (*pro justice*), dalam hal ini untuk membuktikan kejahatan dengan smartphone atau kejahatan komputer secara ilmiah sehingga didapatkan bukti-bukti digital yang digunakan untuk menghukum pelaku kejahatan[8]. Digital forensik memiliki banyak bidang, salah satunya adalah *Mobile* Forensik. Digital Forensik pada intinya dapat menemukan bukti digital yang biasa tersimpan pada penyimpanan komputer/*mobile* sementara, penyimpanan permanen, USB, CD, lalu lintas jaringan, dan lainya[9].

2.2. *MobileForensic*

Mobileforensic adalah cabang dari digital forensic yang berhubungan dengan pemulihan barang bukti digital dari perangkat *mobile*atau smartphone. Perangkat mobile dapat dikaitkan dengan perangkat digital yang memiliki memori internal dan kemampuan komunikasi, vatau biasa disebut *smartphone*. Banyak informasi yang diambil dari perangkat *mobile*yang digunakan untuk kejahatan, dan berguna dalam berbagai masalah administrasi,hukum, dan penyelidikan. Contoh masalah penyelidikikan seperti, perceraian dan hukum keluarga, pencurian kekayaan intelektual, penipuanperusahaan, sengketa properti, dan lain-lain.[10]

2.3. Bukti Digital

Bukti digital merupakan data yang dikirimkan atau disimpan memakai perangkat *mobile*atau komputeryang menyangkal atau mendukung suatukejahatan tertentu, atau memberikan petunjuk yang mengarah pada elemen-elemen penting yang berhubungan dengan suatu pelanggaran. Bukti digital memiliki sifat yang mudah rapuh, mudah menguap dan rentan jika tidak ditangani denganbenar. Semua jenis perubahan yang mengandung bukti digital akan mengarah padakesimpulan yang salah, atau bukti digital tidak dapat digunakan kembali. Langkah-langkah pengambilan bukti digital ditentukan dengan memperhatikan, media digital sebagai barang bukti, integritas dan keaslian dari bukti digital,lokasi media penyimpanan digital, dengan memakai WriteProtect, hash, dan lain-lain.Orang tertentu saja yang berhak mengaksws barng bukti digital, dan orang tersebut tidak boleh memakai perangkat elektromagnetik dekatdengan bukti digital, menduplikasi barang bukti digital memakai prosedur dan perangkat di bawah standar akuisisi digital forensik[11].

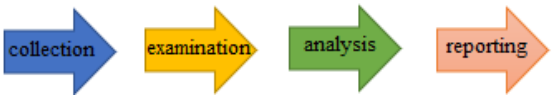
2.4. Smartphone Android

Smartphone adalah telepon selular yang mempunyai mikroprosesor, media peyimpanan, layar dan modem. *Smartphone* merupakan telepon pintar yang menggabungkan fungsionalitas komputer dan perangkat di tangan sehingga menghasilkan *gadget* yang canggih. Smartphone memiliki pesan teks, kamera, pemutar music dan video, game, akses *e-mail*, tv digital, *search engine*, pengelola informasi pribadi, fitur GPS, jasa telepon internet dan bahkan terdapat telepon yang juga berfungsi sebagai kartu kredit

Android dapat didefinisikan sebagai platform perangkat *mobile open source* yang dikembangkan kernel Linux 2.6 dan dikelola oleh *OpenHandset Alliance*, sekelompok operator, produsen, perangkat dan komponen *mobile*, dan vendor perangkat lunak. Sejarah android sebagai platform untuk *smartphone* dimulai pada tahun 2008 setelah *smartphone* pertama kali diperkenalkan[12].

3. METODE PENELITIAN

Penelitian ini menerapkan metode yang dikeluarkan oleh *National Institute of Standard and Technology* (NIST) yang banyak diterapkan pada analisis forensik *mobile*. Tahapan metode NIST dapat dilihat pada gambar 1



Gambar 1 Tahapan metode NIST

Penjelasan dari tahapan metode NIST adalah sebagai berikut :

1.*Collection*

Proses *collection* dilakukan untuk proses identifikasi, pelabelan, perekaman, dan pengambilan data dari sumber data yang relevan dengan mengikuti prosedur penjagaan integritas data.

2.*Examination*

Proses *examination* dilakukan untuk pemrosesan data yang dikumpulkan secara forensik menggunakan kombinasi dari berbagai skenario, baik otomatis maupun manual, serta menilai dan mengeluarkan data sesuai dengan kebutuhan dengan tetap mempertahankan integritas data.

3.*Analysis*

Proses analysis dilakukan untuk memeriksa hasil dari proses *examination* dengan menggunakan metode yang dibenarkan secara teknik dan hukum guna mendapatkan informasi yang dapat digunakan untuk menjawab pertayaan-pertayaan yang menjadi pendorong dalam melakukan pemeriksaan.

4.*Reporting*

Pelaporan hasil analisa yang meliputi penggambaran dalam melakukan tindakan yang dilakukan mengenai alat dan prosedur yang dipilih, penentuan tindakan lain yang pelu dilakukan (misalnya melakukan pemeriksaan forensik dari sumber data tambahan, mengamankan celah yang teridentifikasi, atau meningkatkan kontrol kemamanan yang ada dan memberikan rekomendasi untuk perbaikan kebijakan, prosedur, alat dan aspek lain dari proses forensik.Hasil yang diperoleh akan disajikan dalam bentuk persentase dan laporan tertulis untuk keperluan dokumentasi. Perhitungan persentase hasil yang diperoleh yaitu menggunakan rumus persamaan (3.1)

$$Pon = \frac{\sum Pn}{\sum Po} \times 100\%$$

keterangan

P : Persentase (%)

Σn : Data hasil *recovery*

ΣN : Data asli *smartphone*

3.1 Objek Penelitian

Objek yang diteliti dalam penelitian ini adalah proses forensik yang berjalan untuk mendapatkan kembali bukti digital berupa data yang telah dihapus pada smartphone Android menggunakan *tool* Wondershare dr. Fone For Android, Oxygen Forensic Suite 2014 untuk membuktikan kejahatan di persidangan.

3.2. Alat dan Bahan

Penggunaan alat dan bahan akan sangat mendukung dalam proses penelitian yang dilakukan. Terdapat dua jenis alat yang digunakan diantaranya perangkat keras (*hardware*) dan perangkat lunak (*software*). Kebutuhan perangkat keras dan perangkat lunak dapat dilihat pada Tabel 1.

Tabel 1 Kebutuhan perangkat keras dan perangkat lunak

No	Nama Alat dan Bahan	Deskripsi/ Spesifikasi	Keterangan
1.	1 Unit Laptop	Asus SonicMaster X454Y, OS Windows 10 64bit	Perangkat Keras
2.	1 Unit *Smartphone*	Samsung Galaxy J1 Ace	Perangkat Keras
3.	1 unit Kabel Data Mikro USB	Kabel Data yang digunakan untuk menghubungkan *smartphone* dan komputer/laptop	Perangkat Keras
4.	Wondershare dr. Fone for Android	Aplikasi berbasis Windows dan yang dapat digunakan untuk mengangkat bukti digital pada *smartphone*	Perangkat lunak
4.	Oxygen Forensic Suite 2014	Aplikasi berbasis Windows dan yang dapat digunakan untuk mengangkat bukti digital pada *smartphone*	Perangkat Lunak

4. HASIL DAN PEMBAHASAN

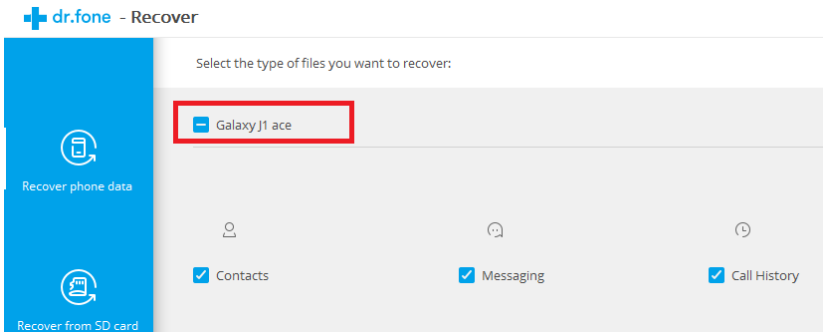
4.1. *Collection*

Tahap *collection* merupakan pengumpulan bukti fisik yaitu barang bukti digital berupa perangkat *smartphone* yang diperlukan untuk melakukan proses penelitian. Penelitian ini menggunakan *smartphone* Samsung galaxy J1 Ace sebagai barang bukti.*Smartphone* yang menjadi barang bukti dapat dilihat pada Gambar 2.

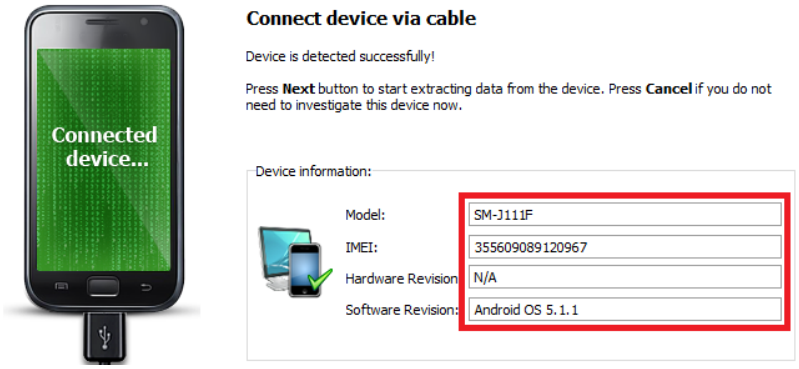
Gambar 2 Smartphone yang menjadi barang bukti

4.2. *Examination*

Tahap ini merupakan tahap pemeriksaan dan pengambilan data dari *smartphone* untuk memperoleh data yang telah dihapus pada barang bukti. Proses ekstraksi data yang dilakukan yaitu *smartphone* yang menjadi barang bukti harus terlebih dahulu terkoneksi pada laptop tempat kedua tool forensik di-install. Gambar 3 menunjukkan *smartphone* yang yang sudahterhubung dengan *tool* Wondershare, dan Gambar 4 menunjukkan *smartphone* yang sudah terhubung dengan Oxygen.

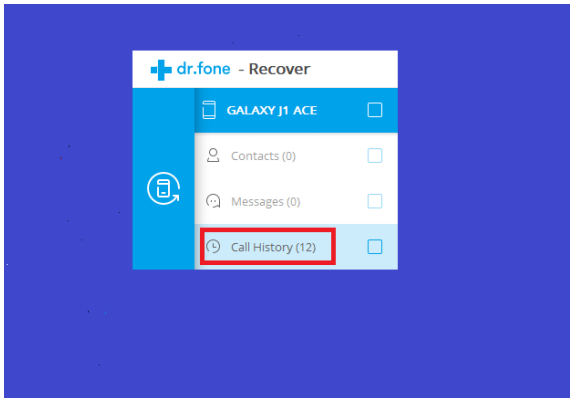


Gambar 3 Smartphone yang sudah terhubung dengan Wondershare



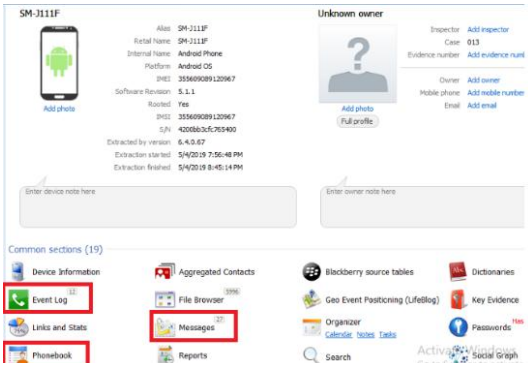
Gambar 4 Smartphone yang telah terhubung dengan Oxygen

Setelah *smartphone* sudah terhubung dengan *tool*Wondershare dan Oxygen, peneliti selanjutnya akan melakukan proses ekstraksi data untuk mengembalikan data yang ada pada perangkat *smarphone*yang telah dihapus oleh tersangka. Proses ekstraksi dengan Wondershare hanya dapat mengembalikan data log panggilan, sementara eksraksi dengan Oxygen dapat mengembalikan data log panggilan dan pesan. Hasil ekstraksi dengan Wondershare dapat dilihat pada Gambar 5, dan hasil ekstraksi dengan Oxygen dapat dilihat pada Gambar 6.



Gambar 5 Hasil ekstraksi dengan Wondershare

Hasil ekstraksi dengan Wondershare hanya berhasil mengembalikan data terhapus berupa 12 log panggilan, sementara data kontak dan pesan tidak dapat dikembalikan.

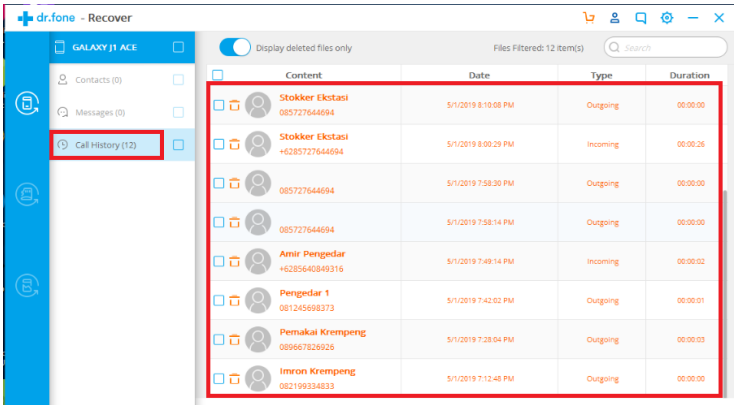


Gambar 6 Hasil ekstraksi dengan Oxygen

Hasil ekstraksi dengan Oxygen berhasil mengembalikan data terhapus berupa 12 log panggilan dan 27 pesan, sementara data kontak tidak dapat dikembalikan.

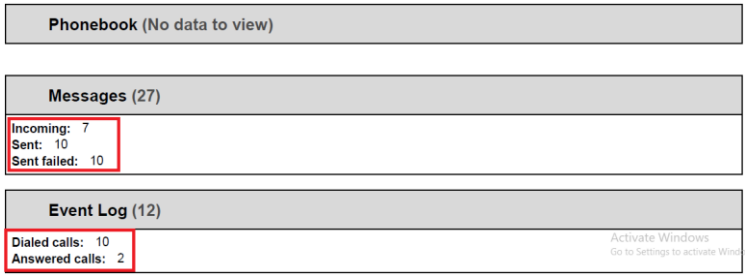
4.3. *Analysis*

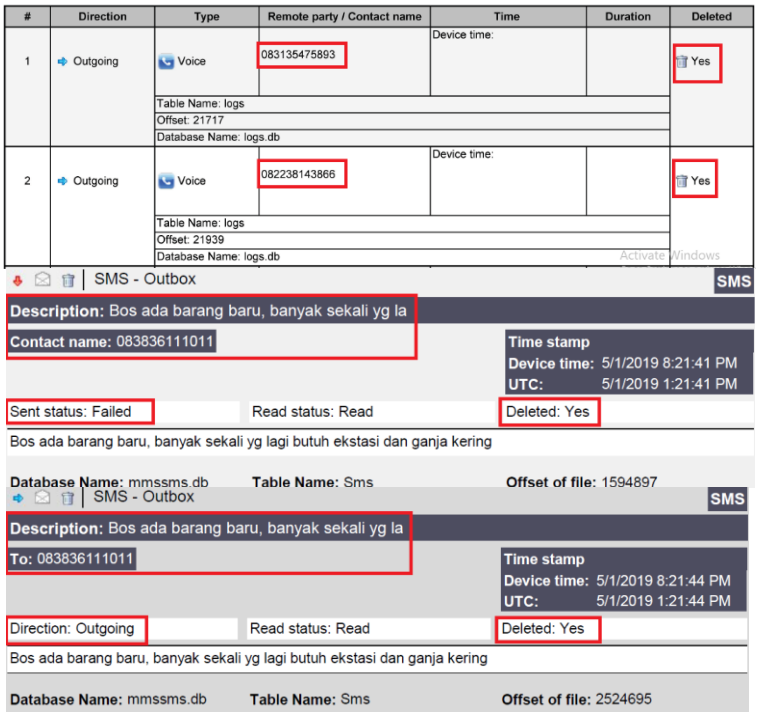
Hasil yang diperoleh dari proses *examination* menggunakan *tool* Wondeshare dan Oxygen yaitu dengan tool Wondershare, data terhapus yang dapat dikembalikan hanya berupa log panggilan, sementara data kontak dan pesan terhapus tidak dapat dikembalikan. Berbeda dengan hasil menggunakan tool Wondershare, proses *examination* dengan Oxygen memberikan hasil yang lebih signifikan yaitu data terhapus yang berhasil dikembalikanyaitu berupa log panggilan dan pesan.Gambar 7 menunjukan data terhapus yang berhasil dikembalikan oleh Wondershare, dan Gambar 8 menunjukkan data terhapus yang berhasil dikembalikan Oxygen.



Gambar 7 Data terhapus yang berhasil dikembalikan oleh Wondershare

Jumlah data terhapus yang berhasil dikembalikan berupa log panggilan oleh Wondersharememiliki jumlah yang sama dengan data yang dihapus pada smartphone yang menjadi barang bukti yaitu sebanyak 12 log panggilan, sementatara data kontak dan pesan tidak memberikan hasil apapun.





Gambar 8 Data terhapus yang berhasil dikembalikan oleh Oxygen

Hasil *examination* dengan *tool* Oxygen adalah data terhapus yang berhasil dikembalikan yaitu sebanyak 12 log panggilan, data tersebut memiliki jumlah yang sama dengan data yang dihapus pada *smartphone* yang menjadi barang bukti. Data berbeda ditunjukkan oleh data pesan yang berhasil dikembalikan yaitu sebanyak 27 pesan dari 17 data yang dihapus pada *smartphone* yang menjadi barang bukti. Hasil analisis menunjukkan bahwa tambahan data sebanyak 10 pesan merupakan pesan yang sama atau pesan gagal yang dianggap sebagai satu data temuan oleh Oxygen.

4.4. Reporting

Berdasarkan bukti digital yang diperoleh menggunakan *tool* Wondershare dan Oxygen forensik, data terhapus yang bisa dikembalikan hanya berupa data log panggilan dan pesan, sementara data terhapus berupa data kontak tidak bisa dikembalikan. Hasil *recovery*menggunakan 2 *tool* forensik dapat dilihat pada Tabel 2.

Tabel 2 Hasil *recovery* menggunakan 2 tool forensik

Tool Forensik	Bukti Digital	Data Asli smartphone	Data Recovery *Tool* Forensik
Wondershare	Kontak	11	0
	Log panggilan	12	12
	Pesan	17	0
Oxygen	Kontak	11	0
	Log panggilan	12	12
	Pesan	17	17

Data tabel 2 diperoleh dari hasil analisis jumlah data yang berhasil dikembalikan pada *smartphone* yang menjadi barang bukti. Hasil yang diperoleh dengan menggunakan *tool* Wondershare adalah 30% data terhapus bisa dikembalikan, sedangakan hasil yang diperoleh dengan Oxygen forensik adalah 73%. Hasil ini diperoleh menggunakan perhitungan angka indeks tidak tertimbang sebagai berikut :

Perhitungan hasil *recovery* data terhapus menggunakan Wondershare

Hasil $recoverytool = \frac{12}{40} x100\% = 30\%$

Perhitungan hasil *recovery* menggunakan Oxygen

Hasil $recoverytool = \frac{29}{40} \times 100\% = 73\%$.

5. KESIMPULAN

Berdasarkan hasil Penelitian tentang analisis bukti digital pada *smartphone* android menggunakan *National Institute Standard and Technology* (NIST) untuk menemukan bukti digital berupa data kontak, log panggilan, dan pesan yang telah dihapus pada *smartphone* samsung galaxy J1 Ace maka dapat disimpulkan bahwa *recovery* dengan *tool* Wondershare hanya mencapai 30%, sedangkan hasil *recovery* dengan Oxygen forensik mencapai 73% data terhapus bisa dikembalikan.Dengan demikian data hasil *recovery* bukti digital dengan *tool* Oxygen sangat direkomendasikan sebagai barang bukti dalam membuktikan kasus kejahatan dalam persidangan.

DAFTAR PUSTAKA

[1] Z. M. Guntur , U. Rusydi and R. Imam ,2017, Analisis Forensik Aplikasi Instant Messaging Berbasis Android," in *Annual Research Seminar (ARS)*, Karawang.

[2] Ruuhwan, R. Imam and P. Yudi, 2017, Evaluation of Integrated Digital Forensics Investigation of Smartphone Using Soft System Methodology, *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, pp. 2806-2817.

[3] F. Arizona, R. Imam and Sunardi, 2016,Analisis Forensik Bukti Digital Blackberry Pada Android," in *Cyber Learning & IT Computer Karawang (ClicK)*, Karawang.

[4] Sahiruddin, Sunardi and R. Imam, 2018, Data Recovery Dengan Keamanan Fingerprint Pada Smarphone Android," in *Seminar Nasional Multi Disiplin Ilmu (SENDI_U)*, Semarang.

[5] Y. Anton, R. Imam and A. Ikhwan, 2018, Analisis Bukti Digital Facebook Messenger Menggunakan Metode NIST," *IT Journal Research and Development*, vol. 3, pp. 13-21.

[6] Y. Anton, R. Imam and F. P. C. Muhamad, 2018, Forensic Tool Comparison on Instagram Digital Evidence Based on Android with NIST Method," *Scientific Journal Informatics*, vol. 5, pp. 235-247.

[7] U. Rusydi, . Y. Anton and F. Muhammad , 2017 Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary.

[8] Al-Azhar and N. Muhammad, 2012, Digital Forensic,Panduan Praktis Investigasi Komputer, Salamba Infotech, Jakarta.

[9] R. Imam, U. Rusydi and F. Arizona, 2017, Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensics Method," *International Journal of Computer Science and Information Security (IJSSIC)*, vol. 15, pp. 155-160,.

[10] R. Imam, F. Abdul and F. Ammar , 2018, Evidence Gathering and Identification of LINE Messenger on Android Devices," *IJCSIS*, vol. 16, pp. 1-6.

[11] A. Faiz and R. Imam , 2017, Forensic Analysis of Frozen Hard Drive Using Static Forensics Method," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, 173-178.

[12] H. Andrew, 2011, Mobile Analysis Kung Fu, San Francisco.