ANALISIS FORENSIK APLIKASI INSTANT MESSENGER PADA SMARTPHONE BERBASIS ANDROID

Anton Yudhana[1)], Imam Riadi[2)], Ikhwan Anshori [3)]
Program Studi Teknik Elektro Universitas Ahmad Dahlan[1)]
Program Studi Sistem Informasi Universitas Ahmad Dahlan[2)]
Program Studi Teknik Informatika Universitas Ahmad Dahlan[3)],
Jl. Prof. Dr. Soepomo, S.H. Janturan Yogyakarta 55164
[1)]eyudhana@ee.uad.ac.id, [2)]imam.riadi@is.uad.ac.id, [3)]ikhwananshori93@gmail.com

ABSTRAK

Teknologi smartphone semakin populer dari tahun ke tahun. Salah satu teknologi dengan jumlah pengguna yang banyak adalah smartphone berbasis Android. Sebagai salah satu sistem operasi smartphone, Android cukup kompetitif di pasar smartphone. Jumlah pengguna smartphone Android juga memberi efek pada pengembangan dan penggunaan aplikasi mobile. Meningkatnya jumlah pengguna Facebook Messenger tentu membawa dampak positif dan negatif, salah satu efek negatifnya adalah beberapa orang yang menggunakan Facebook Messenger melakukan kejahatan digital. Jika sebuah smartphone menjadi bukti dalam kasus pidana dan Facebook Messenger dipasang di smartphone itu, maka pada aplikasi ini bukti digital dapat diidentifikasi dan dapat diharapkan menjadi pilihan untuk membantu penegakan hukum dalam mengungkap kejahatan digital. NIST (National Institute of Standards Technology) memiliki panduan kerja baik itu kebijakan dan standar untuk menjamin setiap examiner mengikuti alur kerja yang sama sehingga pekerjaan mereka terdokumentasikan dan hasilnya dapat di ulang (repeatable) dan dapat dipertahankan (defendable). Penelitian ini diharapkan mampu memberikan gambaran umum bagaimana cara atau teknik-teknik yang dapat digunakan untuk mengembalikan bukti digital berupa text dan gambar yang ada pada smartphone android.

Kata Kunci : Digital Forensik, Facebook Mesengger, Android, NIST.

ABSTRACT

Smartphone technology is increasingly popular from year to year. One technology with a large number of users is an Android-based smartphone. As one of the smartphone operating system, Android is quite competitive in the smartphone market. The number of Android smartphone users also has an effect on the development and use of mobile applications. Increasing the number of Facebook Messenger users will bring positive and negative impacts, one of the negative effects is some people who use Facebook Messenger digital crimes. If a smartphone becomes evidence in a criminal case and Facebook Messenger is installed on that smartphone, then in this application digital evidence can be identified and can be expected to be an option to assist law enforcement in uncovering digital crime. NIST (National Institute of Standards Technology) has a guideline for both policy and standards to ensure that every examiner follows the same workflow so that their work is documented and the results are repeatable and defendable. This research is expected to provide an overview of how ways or techniques that can be used to restore digital evidence in the form of text and images that exist on android smartphone.

Keywords: *Digital Forensic, Facebook Messenger, Android, NIST.*

PENDAHULUAN

Perangkat mobile telah menjadi kebutuhan sehari-hari bagi setiap individu. Perangkat mobile yang paling umum digunakan dalam komunikasi sehari-hari adalah smartphone. Ada banyak Sistem Operasi untuk smartphone, salah satunya adalah Android. Smartphone berbasis Android banyak

digunakan untuk melakukan panggilan, mengirim pesan, e-mail, dan komunikasi melalui jejaring sosial dan pesan instan. Salah satu aplikasi media sosial terpopuler adalah Facebook Messenger. Meningkatnya jumlah pengguna Facebook Messenger tentu membawa dampak positif dan negatif, salah satu efek negatifnya adalah beberapa orang yang menggunakan Facebook Messenger melakukan kejahatan digital. Jika sebuah smartphone menjadi bukti dalam kasus pidana dan Facebook Messenger dipasang di smartphone itu, maka pada aplikasi ini bukti digital dapat diidentifikasi dan dapat diharapkan menjadi pilihan untuk membantu penegakan hukum dalam mengungkap kejahatan digital.

Kejahatan digital yang bisa dilakukan di Facebook Messenger sebagai media komunikasi untuk tujuan kriminal misalnya seperti perdagangan narkoba, kegiatan teroris, perencanaan pembunuhan, dan kegiatan kriminal lainnya. Pada kondisi seperti itu, perangkat seluler akan digunakan oleh penyidik sebagai barang bukti.Metode yang digunakan untuk melakukan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital yaitu dengan metode NIST (National Institute of Standards Technology). Transformasi pertama terjadi saat data yang dikumpulkan diperiksa, lalu mengekstrak data dari media dan mengubahnya menjadi format yang bisa diproses oleh alat forensik. Kedua, data ditransformasikan menjadi informasi melalui analisis. Akhirnya, transformasi informasi menjadi bukti analogi dengan mentransfer pengetahuan ke dalam tindakan menggunakan informasi yang dihasilkan oleh analisis dalam satu atau beberapa cara selama fase pelaporan.

Forensik Mobile dapat dilakukan pada berbagai smartphone, akan tetapi pada penelitian ini lebih difokuskan pada forensik smartphone ber-platform Android. Seiring meningkatnya jumlah smartphone yang kaya berbagai fitur membuat tantangan dalam membuat tools investigasi forensik atau standar khusus untuk masing-masing platform. Bukti digital dalam perangkat mobile memiliki sifat yang mudah rentan tertimpa dengan data baru atau bahkan terhapus. Perangkat mobile sendiri menggunakan memori internal, meskipun tidak menutup kemungkinan ekternal memori juga dapat dilakukan proses investigasi digital karena melibatkan penyimpanan data satu sama lain. Pertumbuhan eksponensial media sosial dan aplikasi pesan instan telah memfasilitasi pengembangan banyak kejahatan cyber dan aktivitas jahat yang serius [1]. Penjahat dunia maya terus mengubah strategi mereka untuk menargetkan media sosial yang berkembang pesat dan pengguna pesan yang ketat. Penyalahgunaan media sosial dan pesan instan dalam layanan mobile memungkinkan penjahat dunia maya memanfaatkan layanan ini untuk tujuan jahat [2] seperti menyebarkan kode berbahaya, dan mendapatkan dan menyebarkan informasi rahasia. Banyak media sosial dan penyedia pesan instan telah memperluas layanan mereka ke platform empiris, [3] yang memperburuk situasi karena pengguna berada dalam bahaya kehilangan lebih banyak lagi informasi pribadi [4].

Facebook Messenger adalah layanan olahpesan cepat dan aplikasi perangkat lunak. Awalnya dikembangkan sebagai Facebook Chat di tahun 2008, perusahaan tersebut mengubah layanan perpesanannya di tahun 2010, dan kemudian merilis aplikasi iOS dan Android mandiri pada bulan Agustus 2011. Selama bertahun-tahun, Facebook telah merilis aplikasi baru di berbagai sistem operasi yang berbeda, meluncurkan situs web khusus. antarmuka, dan memisahkan fungsi perpesanan dari aplikasi Facebook utama, mengharuskan pengguna untuk menggunakan antarmuka web atau mendownload salah satu aplikasi mandiri. Pengguna dapat mengirim pesan dan bertukar foto, video, stiker, audio, dan file, serta bereaksi terhadap pesan pengguna lain dan berinteraksi dengan bot. Layanan ini juga mendukung panggilan suara dan video. Aplikasi mandiri mendukung penggunaan beberapa akun, percakapan dengan enkripsi end-to-end opsional, dan bermain game. Setelah terpisah dari aplikasi Facebook utama, Messenger memiliki 600 juta pengguna pada bulan April 2015, tumbuh menjadi 900 juta pada bulan Juni 2016, 1

miliar pada bulan Juli 2016, dan 1,2 miliar pada bulan April 2017.[5]

Analisis forensik digital pada line messenger untuk penanganan cybercrime diawali dengan beberapa langkah, yakni preservation, collection, examination, dan pada akhirnya adalah analysis. Analisis yang dihasilkan merupakan gambaran dari semua proses investigasi. Proses investigasi dilakukan pada perangkat pelaku. Hasil yang diharapkan dari penelitian ini adalah proses investigasi yang baik dan terangkatnya bukti digital pada Line messenter di perangkat smartphone Android. Proses collection atau

pengumpulan data diawali dengan rooting menggunakan tool Zenfone RootKit untuk mempermudah pengangkatan data-data yang ada di dalam perangkat Android. Kemudian perangkat Android yang telah di-root, direcovery menggunakan tool Kamas Lite atau AFLogical. Diharapkan data-data yang direcovery dapat menunjukan file percakapan pada aplikasi Line yang berupa teks maupun gambar. [6]

WhatsApp telah menjadi aplikasi populer untuk jejaring sosial dimana orang dapat bertukar informasi pribadi beserta mobilitas yang mereka geluti. Penelitian ini telah menunjukkan bahwa seseorang dapat memperoleh akses lengkap ke semua informasi di WhatsApp baik itu WhatsApp Smartphone maupun WhatsApp Web. Sebagian besar aplikasi chat mengikuti pola sinkronisasi pesan, kontak dan data pengguna yang sama saat syinc dan memperbarui data percakapan secara berkala. Pendekatan yang diambil memberi garis besar umum untuk semua aplikasi serupa yang berjalan di perangkat ber-platform Android maupun Windows seperti Telegram dan sejenisnya. Penelitian ini dapat bermanfaat untuk Mobile Forensic Analysis dan Investigation pada smartphone Android dan aplikasi ganda berbasis web browser. Database QR Code membutuhkan autentikasi terhadap smartphone hanya sekali setiap saat login pertama kali sehingga dibutuhkan kewaspadaan penggunanya seperti penggunaan pattern lock pada smartphone dan login user password pada komputer penggunanya. Proses akuisisi langsung terhadap smartphone korban dan analisis web browser pada komputer. Diharapkan kedepan lebih banyak penelitian yang dapat dilakukan pada interpretasi data percakapan WhatsApp dalam bentuk jurnal atau naskah lain sebagai literatur selanjutnya.[7]

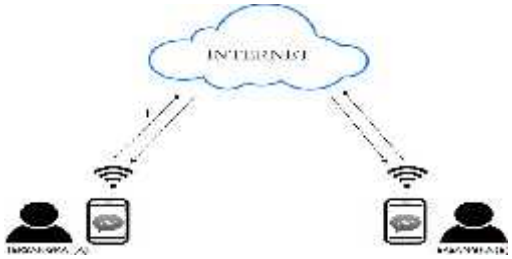
Metode NIST Mobile Forensik dapat diterapkan pada proses perolehan bukti digital dari Blackberry Messenger di smartphone Android dengan menggunakan alat Andriller. Berdasarkan data yang didapat, Andriller hanya bisa memperoleh bukti digital berupa data percakapan, nama pengirim pesan, PIN pengirim dan penerima pesan bersamaan dengan tanggal pembicaraan. Data gambar tidak muncul saat proses perolehan data selesai. Beberapa saran yang dapat diberikan untuk pengembangan dan penelitian lebih lanjut adalah selain metode Forensik Mobile NIST, ada beberapa metode lain yang dapat digunakan dalam proses perolehan dan analisis bukti digital, dengan proses yang lebih rinci dan lengkap. Lebih banyak metode diharapkan bisa memberikan hasil yang lebih akurat. Penggunaan alat dalam memperoleh proses bukti digital juga dapat dikombinasikan dengan alat lain yang memiliki kemampuan berbeda yang dapat memberikan dukungan antar alat untuk menghasilkan laporan yang lebih baik. [8]

Forensik Smartphone adalah bagian dari forensik digital, dan mengacu pada penyelidikan dan perolehan artefak pada smartphone. Ancaman baru terhadap ponsel membuat ilmu forensik menjadi tantangan yang menantang dalam beberapa tahun terakhir. Jumlah pengguna ponsel meningkat di seluruh dunia dan menimbulkan masalah dan tantangan yang luar biasa. Literatur yang relevan dengan forensik smartphone, fokus penelitian ini pada arsitektur sistem operasi smartphone dan teknik anti- forensik. Ini juga membahas bukti digital dari aplikasi smartphone. Dalam penelitian ini, melalui pertimbangan jenis kejahatan yang melibatkan smartphone, sebuah studi kasus nyata dari Negara Kesultanan Oman dipresentasikan. Studi kasus ini melakukan eksperimen praktis terhadap sumber yang teridentifikasi untuk bukti yang nantinya dapat digunakan dalam sistem peradilan [9]

Forensik Android telah berkembang dari waktu ke waktu dengan menawarkan peluang dan tantangan menarik yang signifikan. Di satu sisi, menjadi platform open source Android memberi pengembang kebebasan untuk berkontribusi pada pertumbuhan pasar Android yang pesat, sementara di sisi lain pengguna Android mungkin tidak menyadari implikasi keamanan dan privasi pemasangan aplikasi ini di ponsel mereka. Pengguna mungkin menganggap bahwa perangkat yang terkunci sandi melindungi informasi pribadi mereka, namun aplikasi mungkin menyimpan informasi pribadi pada perangkat, dengan cara yang mungkin tidak diantisipasi pengguna. Dalam penelitian ini akan berkonsentrasi pada satu aplikasi yang disebut 'WhatsApp', aplikasi jejaring sosial yang populer. Penelitia akan membentuk garis besar tentang bagaimana penyidik forensik dapat mengekstrak informasi yang berguna dari WhatsApp dan dari aplikasi serupa yang terpasang di platform Android. Area fokus penelitian adalah ekstraksi dan analisis data pengguna aplikasi dari penyimpanan eksternal non-volatile dan memori volatile (RAM) perangkat Android.[10]

Instant Messaging (IM) merupakan salah satu aplikasi seluler yang sangat popular. Salah satu jenis aplikasi IM adalah WhatsApp (WA). Pengguna WA jumlahnya mencapai 1 Milyar setiap bulannya. WA didukung oleh fitur enkripsi untuk menjamin keamanan data para penggunanya. Kepopuleran dan fitur yang diberikan WA dapat disalahgunakan masyarakat untuk tujuan kriminal, seperti perdagangan

narkoba, kegiatan teroris, perencanaan pembunuhan, dan kegiatan kriminal lainnya melalui fitur- fitur yang tersedia. Pihak berwenang dapat menggunakan data-data dalam WA sebagai barang bukti. Metode forensik diperlukan untuk memastikan keberhasilan proses pengambilan data-data tersebut. Penelitian ini akan menjelaskan langkah-langkah untuk memperoleh data aplikasi WA, dari data yang telah dienkripsi menjadi data yang dapat dibaca dan dianalisis untuk kemudian dapat digunakan sebagai barang bukti.[11] Secara forensik memperoleh dan menganalisis data yang tersimpan perangkat dan lalu lintas jaringan dari 20 aplikasi pesan instan yang populer untuk Android. investigator dapat mengkonstruksikan beberapa atau seluruh isi pesan dari 16 dari 20 aplikasi yang diuji yang mencerminkan keburukan pada tindakan keamanan dan privasi yang digunakan oleh aplikasi ini, namun dapat dianggap positif untuk tujuan pengumpulan bukti digital oleh praktisi forensik digital. Penelitian ini menunjukkan fitur aplikasi pesan instan mana yang meninggalkan jejak pembuktian yang memungkinkan data tersangka direkonstruksi sebagian, dan apakah forensik jaringan atau forensik perangkat memungkinkan dilakukannya rekonstruksi aktivitas tersebut. Peneliti menunjukkan bahwa dalam banyak kasus dapat merekonstruksi data seperti : kata sandi, screenshot yang diambil oleh aplikasi, gambar, video, audio yang dikirim, pesan yang dikirim, sketsa, gambar profil dan lain-lain.[12] Proses skenario kejahatan digital melalui Facebook Messenger seperti terdapat pada gambar 1.1.

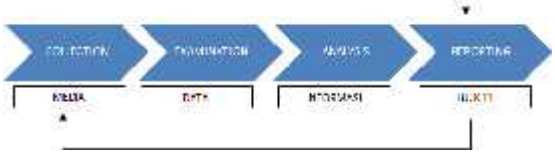


Gambar 1.1. Proses Skenario Kejahatan Digital Melalui Facebook Messenger

METODE PENELITIAN

Penelitian ini menggunakan metode forensik yang dikeluarkan oleh National Institute of Standard and Technology (NIST). [13] Metode yang digunakan untuk melakukan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital yaitu dengan metode NIST (National Institute of Standards Technology). Transformasi pertama terjadi saat data yang dikumpulkan diperiksa, lalu mengekstrak data dari Media dan mengubahnya menjadi format yang bisa diproses oleh alat forensik. Kedua, data ditransformasikan menjadi informasi melalui analisis. Akhirnya, transformasi informasi menjadi bukti analogi

dengan mentransfer pengetahuan ke dalam tindakan menggunakan informasi yang dihasilkan oleh analisis dalam satu atau beberapa cara selama fase pelaporan.[14] Metode tersebut mempunyai beberapa tahap yaitu seperti pada Gambar 2.1.



Gambar 2.1 Tahapan Metode (National Institute of Standards Technology) NIST

1. Collection

Tahap ini merupakan proses identifikasi, pelabelan, perekaman, dan pengambilan data dari sumber data yang relevan dengan mengikuti prosedur penjagaan integritas data.

2. Examination

Tahap ini merupakan tahap pemrosesan data yang dikumpulkan secara forensik menggunakan kombinasi dari berbagai skenario, baik otomatis maupun manual, serta menilai dan mengeluarkan data sesuai kebutuhan dengan tetap mempertahankan integritas data.

3. Analysis

Melakukan analisis pada hasil pemeriksaan dengan menggunakan metode dibenarkan secara teknik dan hukum untuk mendapatkan informasi yang berguna dan menjawab pertanyaan- pertanyaan yang menjadi pendorong untuk melakukan pengumpulan dan pemeriksaan.

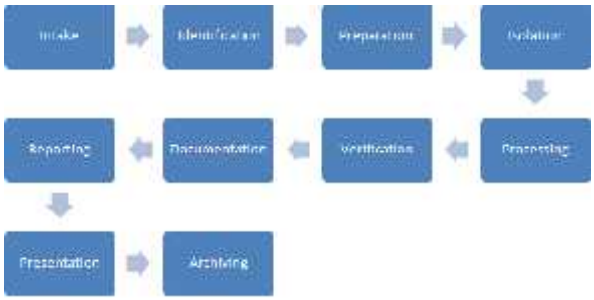
4. Reporting

Melaporkan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai alat dan prosedur yang dipilih, penentuan tindakan lain yang perlu dilakukan (misalnya, pemeriksaan forensik dari sumber data tambahan, mengamankan celah yang teridentifikasi, atau meningkatkan kontrol keamanan yang ada), dan memberikan rekomendasi untuk perbaikan kebijakan, prosedur, alat, dan aspek lain dari proses forensik.

HASIL DAN PEMBAHASAN

Pembahasan

NIST (National Institute of Standards Technology) memiliki panduan kerja baik itu kebijakan dan standar untuk menjamin setiap examiner mengikuti alur kerja yang sama sehingga pekerjaan mereka terdokumentasikan dan hasilnya dapat di ulang (repeatable) dan dapat dipertahankan (defendable).[15] Proses kerja Forensik Mobile dapat dilihat pada Gambar 3.1.



Gambar 3.1 Proses Kerja Forensik Mobile

Keterangan dari gambar diatas adalah sebagai berikut:

1. Intake

Tahapan awal dimana barang bukti diproleh oleh “pemeriksa”, terdapat formulir dokumentasi pendukung lainnya terkait dengan kepemilikan barang bukti dan data informasi-informasi pendukung tentang kasus terkait.

2. Identification

Tahapan selanjutnya melakukan identifikasi, pada tahap ini pemriksa harus mengidentifikasi bebrapa hal antara lain kewenangan, tujuan pemeriksaan, dan identifikasi perangkat.

3. Preparation

Setelah data pendukung sudah didapatkan maka dilakukanlah persiapan mulai dari metode apa yang akan dilakukan dan tools apa saja yang akan digunakan dalam proses ekstraksi dan analisis

4. Isolation

Tahapan Isolation merupakan proses yang penting agar perangkat mobile tidak terhubung dengan jaringan komunikasi

seperti jaringan telepon seluler, bluetooth, infra merah ataupun WiFi.

5. Processing
Setelah proses isolasi dari jaringan komunikasi, maka tahapan selanjutnya adalah memproses barang bukti tersebut. yaitu dengan melakukan ekstraksi dari barang bukti di mana metode ekstraksi sudah ditentukan dalam tahap "Preparation". Setelah itu maka dilakukan analisa terkait temuan-temuan yang didapat dari ekstraksi tersebut.

6. Verification
Setelah memproses barang bukti maka dilakukanlah proses verivikasi, dimana pemeriksa melakukan verivikasi keakuratan data ekstraksi yang didapatkan.
Verifikasi data yang diekstrak dapat dicapai dalam beberapa cara:

a. membandingan data yang telah diekstrak dengan data dalam barang bukti yang didapt
b. memeriksa hex dari data yang diekstraksi
c. menggunakan bebrapa tools untuk membandingkan hasilnya
d. menggunakan hash value untuk membandingkan hasil ekstraksi yang berupa file image

7. Documentation & reporting
Proses Dokumentasi harus dilakukan harus dilakukan dari tahap perolehan sampai pada tahapan- tahapan selanjutnya, setelah itu pelaporan harus dilakukan dengan baik, secara ringkas dan jelas agar mudah dipahami oleh pihak-pihak yang punya otoritas.

8. Presentation
Penyajian harus diberikan seluruh pemeriksaan bagaimana informasi diekstrak dan didokumentasikan dari perangkat mobile dapat dengan jelas disampaikan kepada yang lain penyidik, jaksa dan pengadilan.

9. Archiving
Proses pengarsipan ini juga sangat penting agar seluruh data dari proses pemeriksaan baik data digital atau data dokumentasi dapat disimpan dengan baik guna menjaga data yang diperoleh pada proses-proses sebelumnya.

Hasil Yang Diharapkan
Penelitian ini diharapkan mampu memberikan gambaran umum bagaimana cara atau teknik-teknik yang dapat digunakan untuk mengembalikan bukti digital berupa text dan gambar yang ada pada smartphone android.

PENUTUP
Penelitian ini menggunakan metodologi dan alat-alat penelitian yang diharapkan dapat digunakan untuk analisis forensik aplikasi Facebook Messenger dan memperoleh hasil yang dapat digunakan dalam membantu proses penyelidikan. Dari metode forensik yang telah dikembangkan, tentunya masih perlu pengembangan agar metode ini bisa lebih baik dari sebelumnya. Saran untuk pengembangan selanjutnya menggunakan tool-tool yang teruji keakuratannya agar data-data yang hilang bisa dikembalikan.

DAFTAR PUSTAKA
S. Mohtasebi, A. Dehghantanha, (2011). Defusing the hazards of social network services, Int. J. Digit. Inf. Wirel.Commun. 1 (2011) 504–516

S. Mohtasebi, A. Dehghantanha, H.G. Broujerdi,(2012). Smartphone forensics: a case study with Nokia E5-00 mobilephone, Int. J. Digit. Inf. Wirel. Commun. 1 (2012) 651–655.

F.N. Dezfouli, A. Dehghantanha, B. Eterovic-Soric, K.-K.R. Choo, (2016). Investigating social networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms, Aust. J. Forensic Sci. 46(4) (2016) 469–488, http://dx.doi.org/10.1080/00450618.2015.1066854.

M. Taylor, G. Hughes, J. Haggerty, D. Gresty, P. Almond, (2012). Digital evidence from mobile telephone applications, Comput. Law Secur. Rev. 28 (2012) 335–339, http://dx.doi.org/10.1016/j.clsr.2012.03.006.

https://en.wikipedia.org/wiki/Facebook_Messenger.

A. Fauzan, I. Riadi, and A. Fadlil, "Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime," vol. 2, no. 1, pp. 159–163, 2016.

I. R. Nuril Anwar, "Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web," Anal. Investig. Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbas. Web, vol. 3, no. June, pp. 1–10, 2017.

Arizona Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," Digit. Investig., vol. 15, no.5, SUPPL., pp. 29–36, 2006.

Mubarak Al-Hadadi and Ali AlShidhani. (2013). Smartphone Forensics Analysis: A Case Study International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013

Thakur, Neha S., Forensic Analysis of WhatsApp on Android Smartphones (2013). University of New Orleans Theses and Dissertations. Paper 1706.

Zamroni, G. M., Umar, R., & Riadi, I. (2016). Analisis Forensik Aplikasi Instant Messaging Berbasis Android, 2(1), 102–105.

Daniel Walnycky, Ibrahim Baggili, Andrew Marrington, Jason Moore, Frank Breitinger,(2015). Digital Investigation 14 (2015) S77eS84. DFRWS 2015 USA Network and device forensic analysis of Android social-messaging applications

RSA, "2013:The Current State of Cybercrime, "RSA Anti Fraud Command Center, Canada, 2013 View

K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," 2006.

C. A. Murphy, "Developing Process for Mobile Device Forensics," pp. 1–9, 2012.

ISSN 2302-6227
ISSN *Online* 2580-488X