IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1658

Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist

Anton Yudhana[1], Imam Riadi[2], Ikhwan Anshori[3]
[1]Program Studi Teknik Elektro ,Universitas Ahmad Dahlan
[2]Program Studi Sistem Informasi,Universitas Ahmad Dahlan
[3]Program Studi Teknik Informatika , Universitas Ahmad Dahlan
[1]eyudhana@ee.uad.ac.id, [2]imamriadi@is.uad.ac.id, [3]ikhwananshoriuad@gmail.com

Abstract

Facebook Messenger became popular social media, both after Whatsapp in the year 2017. The growing number of users Facebook Messenger certainly brings positive and negative impact, its negative effects is the one used for the digital crimes such as drug trafficking. How to catch the perpetrators of the crime required digital evidence at trial. One of the science to get the digital evidence is doing the digital forensics. Digital forensics can be done on a smartphone used the perpetrators of cybercrime. This research will do the adoption of digital crime evidence as much as possible from the Facebook Messenger on your Android smartphone. in this research tool that we use is Oxygen forensic using National Institute of Standards Technology (NIST). NIST has a good employment policy guidelines and standards to ensure every examiner follow the same workflow so that their work is documented and the results can be repeated and can be maintained. The results of this research tool Oxygen forensic get text conversation, conversation time sent messages, audio, images, which is not obtained in the form of a video.

Keywords : *Digital Forensic, Facebook Messenger, Forensic Mobile, NIST*

Abstrak

Facebook Messenger menjadi media sosial yang populer kedua setelah Whatsapp di tahun 2017. Meningkatnya jumlah pengguna Facebook Messenger tentu membawa dampak positif dan negatif, salah satu efek negatifnya adalah digunakan untuk tindak kejahatan digital seperti perdagangan narkoba. Cara menangkap para pelaku kejahatan digital maka diperlukan barang bukti pada persidangan. Salah satu ilmu untuk medapatkan barang bukti digital adalah melakukan forensik digital. Forensik digital dapat dilakukan pada *smartphone* yang digunakan para pelaku kejahatan. Penelitian ini akan melakukan pengangkatan barang bukti kejahatan digital sebanyak mungkin dari facebook Messenger pada *smartphone* Android. Pada penelitian ini *tool* yang kami gunakan adalah *Oxygen Forensic* dengan menggunakan metode *National Institute of Standards Technology* (NIST). NIST 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 dan dapat dipertahankan. Hasil penelitian ini *tool* Oxygen forensic mendapatkan text percakapan, waktu percakapan dikirimkan, pesan audio, gambar, yang tidak didapatkan berupa video.

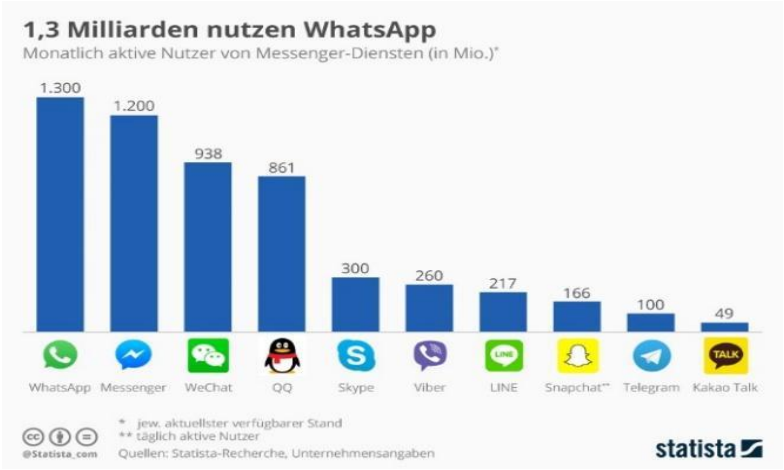
Kata kunci: *Digital* Forensik, Facebook Messenger , *Mobile* Forensik, NIST.

1. PENDAHULUAN

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

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1658

bukti digital dapat diidentifikasi dan dapat diharapkan menjadi pilihan untuk membantu penegakan hukum dalam mengungkap kejahatan digital. Pada Gambar 1 merupakan grafik penggunaan Facebook Messenger yang menjadi deretan kedua setelah Whatsapp pada tahun 2017.



Gambar 1. Grafik Pengguna Facebook Messenger

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. Kejahatan tersebut pasti akan meninggalkan barang bukti, barang bukti tersebut sebagai laporan tindak kejahatan di pengadilan.

Metode untuk pengangkatan barang bukti dapat dilakukan dengan dua cara yaitu dead forensic dan live forensic. Dead forensic merupakan suatu teknik yang membutuhkan data yang disimpan secara permanen dalam perangkat media penyimpanan umumnya hardisk. *Live forensic* yaitu suatu teknik analisis dimana menyangkut data yang berjalan pada system atau data volatile yang umumnya tersimpan pada *Random Access Memory* (RAM) atau transit pada jaringan [1].

Mobile dapat diartikan sebagai perpindahan yang mudah dari satu tempat ke tempat yang lain, misalnya telepon mobile berarti bahwa terminal telepon yang dapat berpindah dengan mudah dari satu tempat ke tempat lain tanpa terjadi pemutusan atau terputusnya komunikasi. Sistem aplikasi mobile merupakan aplikasi yang dapat digunakan walaupun pengguna berpindah dengan mudah dari satu tempat ketempat lain lain tanpa terjadi pemutusan atau terputusnya komunikasi. Aplikasi ini dapat diakses melalui perangkat nirkabel seperti pager, seperti telepon seluler dan PDA [2]. Android adalah sistem operasi *Open Source* untuk *smartphone* berbasis Linux Google. Android telah dikembangkan oleh Google sebagai sistem operasi terbuka yang memberikan kebebasan untuk hardware produsen dan operator telepon untuk mengembangkan sistem operasi dan aplikasi[3].

Mobile forensik adalah cabang dari digital forensik berkaitan dengan pemulihan digital bukti atau data dari perangkat mobile di bawah kondisi forensik suara. Perangkat selular biasanya frase mengacu pada ponsel, tetapi juga dapat dikaitkan dengan perangkat digital yang memiliki memori internal dan kemampuan komunikasi. Penggunaan ponsel dalam kejahatan adalah banyak informasi yang diambil dari perangkat mobile dapat berguna dalam berbagai masalah hukum, administrasi dan penyelidikan seperti, Pencurian Kekayaan Intelektual, Perusahaan Penipuan, Penggunaan Properti, Perceraian & Hukum Keluarga, Lokasi geografis kontroversi, Bukti kejahatan [4][5].

IT Journal Research and Development
Vol.3, No.1, Agustus2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1658

Keamanan menjadi tantangan bagi pada teknologi informasi forensik dan penegak hukum untuk melakukan penyelidikan terhadap *smartphone* dari seseorang yang dijadikan tersangka dalam sebuah kasus kejahatan [6]. Banyak cara untuk menghilangkan kode akses keamanan layar pada *smartphone*, salah satu cara yaitu dengan melakukan *factory data reset* atau mengembalikan *smartphone* ke kondisi awal dari pabrik. Akan tetapi, cara yang dilakukan ini dapat menghapus semua data-data yang tersimpan di memori internal *smartphone*. Pada suatu penyidikan, data didalam *smartphone* yang dijadikan barang bukti digital tidak boleh hilang satu pun selama proses penyidikan dilakukan[7] .

Konsekuensi dengan banyak kejahatan menggunakan tekno*log*i informasi khususnya menggunakan Internet, beberapa kejahatan sering dilakukan dalam bentuk serangan yang terjadi dalam lembaga atau lembaga tertentu. Proses menemukan dan mengidentifikasi jenis serangan, membutuhkan proses panjang yang membutuhkan waktu, sumber daya manusia dan pemanfaatan tekno*log*i informasi untuk memecahkan masalah ini. Proses mengidentifikasi serangan yang terjadi juga membutuhkan dukungan dari perangkat keras dan juga perangkat lunak. Serangan yang terjadi di jaringan Internet umumnya dapat disimpan dalam file *log* yang memiliki format data tertentu. Untuk menyederhanakan proses menganalisis *log*, penggunaan metode ilmiah untuk membantu kelompok beragam data mentah diperlukan. Teknik klaster adalah salah satu metode yang dapat digunakan untuk membantu memfasilitasi proses identifikasi [8][9].

Analisis Forensik akan memberikan rincian yang akan membantu para penyelidik dan lembaga investigasi dalam memecahkan & menghubungkan kasus-kasus dengan kejahatan yang dilaporkan. Makalah ini bertujuan untuk fokus pada pemeriksaan forensik data & Informasi yang disimpan oleh aplikasi di telepon dan teknik ekstraksi data forensik. Dalam pemeriksaan forensik apa pun dari ponsel Android, metodologi forensik yang baik harus diperhatikan. Peralatan, lingkungan dan teknik yang digunakan harus sesuai dengan aturan kardinal forensik komputer. Metodologi forensik yang baik tidak mengubah data apa pun pada perangkat asli juga tidak akan menulis data apa pun di atasnya [10][11].

Forensik jaringan dirasa perlu dilakukan dengan tujuan membantu administrator jaringan untuk mempermudah dalam menemukan serangan yang biasanya di lakukan secara manual. Desain dan implementasi forensik *log* perlu dilakukan dengan tujuan untuk menemukan bukti berdasarkan sumber serangan, waktu kejadian, serta dampak dari serangan pada perangkat jaringan [12].

Hasil analisa struktur dan isi folder serta aplikasi menjadi jawaban untuk mengungkap sebuah kasus kejahatan sesuai skenario percakapan yang telah dibuat pada bagian perancangan dan dilaksanakan pada bagian implementasi. Analisa barang bukti digital meliputi pengumpulan data digital penting dan pembacaan bukti digital[13].

Bukti digital itu rapuh, mudah menguap dan rentan jika tidak ditangani dengan benar. Semua jenis perubahan yang mengandung bukti digital akan mengarah pada kesimpulan yang salah, atau bukti tidak akan berguna. Penentuan langkah-langkah akuisisi bukti digital dilakukan dengan memperhatikan, media digital sebagai bukti, tata letak fisik media penyimpanan digital, integritas dan keaslian dari bukti digital menggunakan Write-Protect, hash, dan banyak lagi, Akses ke bukti digital hanya diberikan untuk siapa yang diberi wewenang dan tidak ada yang menggunakan perangkat elektromagnetik dekat dengan bukti digital, dokumentasi kondisi dan konfigurasi media penyimpanan digital, bukti digital duplikat / pencitraan menggunakan prosedur dan perangkat di bawah standar akuisisi digital forensik [14].

Menurut sebuah studi sebelumnya yang berjudul *Identification Of Digital Evidence On Android's Blackberry* Messenger *Using NIST Mobile Forensic Method* dan diskusi dalam studi ini, ada beberapa hal yang dapat disimpulkan diantaranya: NIST Mobile

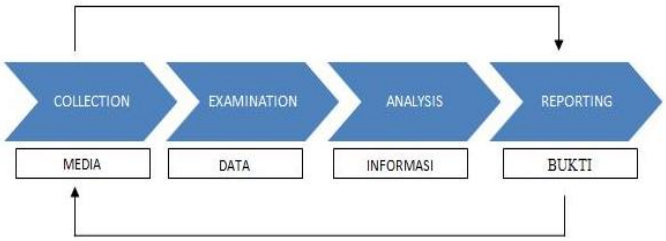
IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1658

Forensik metode dapat diterapkan untuk proses mendapatkan bukti digital Blackberry Messenger pada *smartphone* Android yang menggunakan software *tool* Andriller [15].

Berdasarkan latar belakang di atas, kami akan melakukan penelitian tentang analisis bukti digital pada facebook Messenger berbasis android dengan menggunakan metode *National Institute of Standards Technology* (NIST). Penelitian yang kami lakukan menggunakan *tool* forensic bernama Oxygen forensic.

2. METODE PENELITIAN

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*). Tahapan untuk mendapatkan informasi dari bukti digital yaitu dengan menggunakan metode NIST (*National Institute of Standards Technology*) [16]. 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 ana*log*i dengan mentransfer pengetahuan ke dalam tindakan menggunakan informasi yang dihasilkan oleh analisis dalam satu atau beberapa cara selama fase pelaporan.



Gambar 2. Tahap metode NIST

Berdasarkan gambar 2 hal ini dapat dijelaskan tahap selular Forensik Analisis sebagai berikut:

1. *Collection* adalah pelabelan, identifikasi, rekaman, dan pengambilan data dari sumber data yang relevan dengan prosedur berikut untuk menjaga integritas data.
2. *Examination* adalah pengolahan data yang dikumpulkan dalam penggunaan forensik kombinasi berbagai skenario, baik otomatis atau manual, serta menilai dan mengeluarkan data sesuai kebutuhan Anda sambil mempertahankan integritas data.
3. *Analysis* adalah analisis hasil pemeriksaan dengan menggunakan metode teknis dibenarkan dan hukum
4. *Reporting* adalah melaporkan hasil analisis yang meliputi penggambaran tindakan yang dilakukan,

3. HASIL DAN PEMBAHASAN

Hasil penelitian yang kami melakukan telah mendapatkan hasil. Proses mendapatkan barang bukti pada *smartphone* android menggunakan *software* forensik Oxigen forensic. berikut adalah hasil yang telah didapatkan. Berikut adalah tabel 1 informasi tentang hardware dan software yang diperlukan pada penelitian ini.

IT Journal Research and Development
Vol.3, No.1, Agustus2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1658

Tabel 1. Alat dan Bahan

Nomor	Nama	Spesifikasi	Keterangan
1	Laptop	Acer E14, Windows10	Perangkat Keras
2	*Smartphone*	Samsung Galaxy V+ SM-G318HZ	Perangkat Keras
3	Facebook Messenger	Aplikasi Android	Perangkat Lunak
4	Oxygen Forensic	Aplikasi	Perangkat Lunak

3.1. Collection

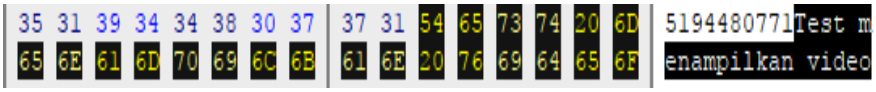
Pada proses *collection* menggunakan android. Android digunakan untuk penelitian ini menggunakan versi kitkat 4.4.4. *Smartphone* yang digunakan adalah Samsung Galaxy V+ SM-G318HZ.

Gambar 3. *Smartphone* yang digunakan

Pada gambar 3 merupakan *smartphone* yang digunakan dalam peneltiian ini. *Smartphone* yang digunakan telah dilakukan proses *Rooting*. *Rooting* adalah proses membuka akses total pada *smartphone* Android. Pada proses *collection* menggunakan Android. Android digunakan untuk penelitian ini menggunakan versi kitkat 4.4.4. *Smartphone* yang digunakan adalah Samsung Galaxy V+ SM-G318HZ.

3.2. Examination

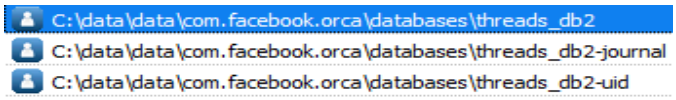
Pada proses *examination* merupakan pengujian pada aplikasi Facebook Messenger menggunakan *tool* Oxygen forensic.



Gambar 4. Kode Hexa Percakapan pada Facebook Messenger

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1658

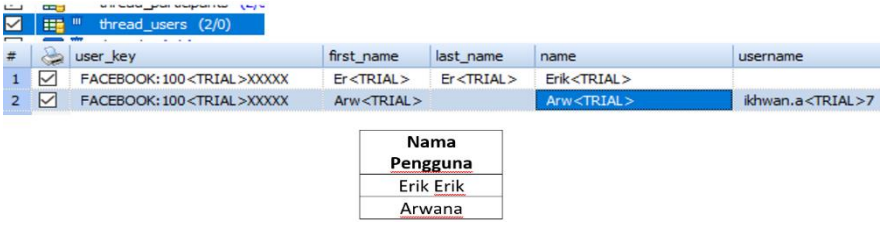
Pada Gambar 4 merupakan tampilan kode hexa dari barang bukti yang didapatkan menggunakan Oxygen forensic dalam percakapan pada facebook Messenger. Didalam kode hexa setelah diterjemahkan mendapatkan hasil text percakapan, isi text pada gambar di atas adalah “Test menampilkan video”.



Gambar 5. Data dari Facebook Messenger

Pada Gambar 5 merupakan data yang ditemukan pada facebook messanger menggunakan *tool*s Oxygen forensic. Data yang ditemukan didalam databases treads_db2, dan di treads_db2_journal.

Data tersebut terletak pada c:\data\data\com.facebook.orca\databases\threads_db2 dan c:\data\data\com.\facebook.orca\databases\threads_db2_journal.

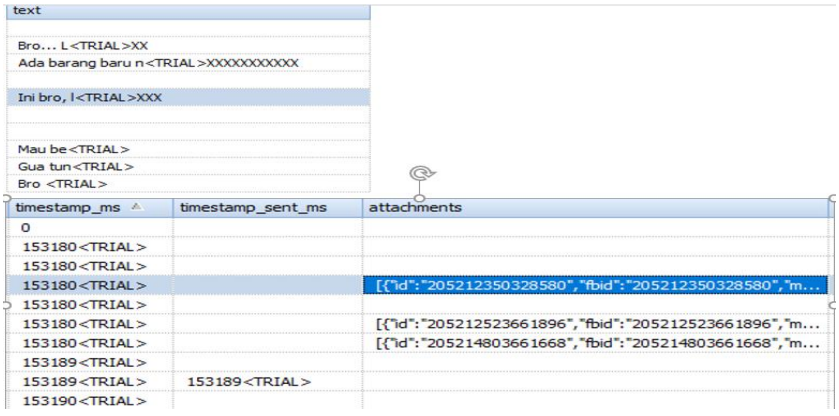


Gambar 6. Hasil akun percakapan pada Facebook Messenger

Pada Gambar 6 merupakan akun percakapan pada facebook messanger yang didapatkan menggunakan *tool*s Oxygen forensic. Data yang didapat pada database treads_db2. Didalammya terdapat akun pengguna facebook messenger pada tread_user. Yang didapatkan bernama “Erik Erik” dan “Arwana”.

3.3. Analysis

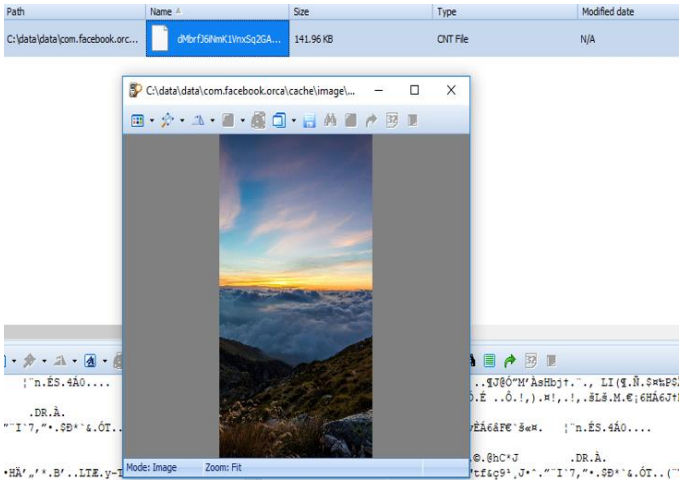
Pada proses analysis ditemukan beberapa barang bukti dari *tool*s forensic Oxygen. Berikut adalah barang bukti yang ditemukan.



Gambar 7. Hasil percakapan dari Oxygen Forensic

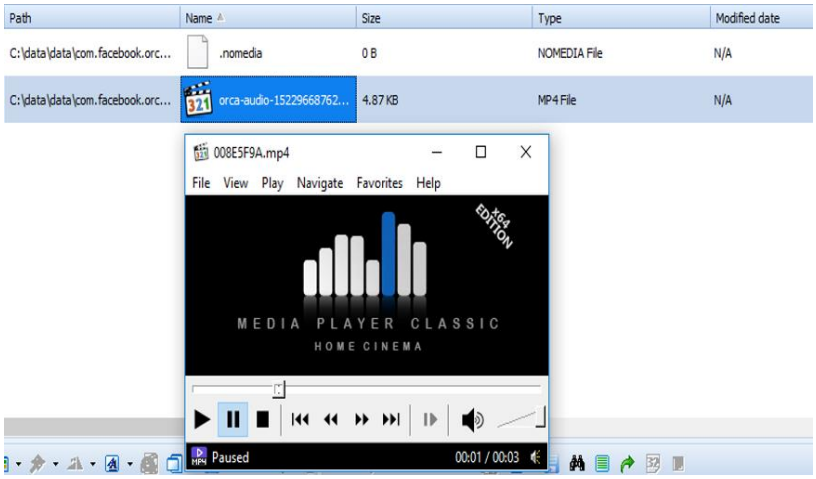
IT Journal Research and Development
Vol.3, No.1, Agustus2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1658

Pada Gambar 7 menunjukkan hasil text percakapan berupa enam kalimat dan didapatkan juga waktu saat percakapan itu dikirimkan. Pada proses analysis ditemukan beberapa barang bukti dari *tool*s Oxygen Forensic. Pada timestamp_ms terdapat angka-angka yang harus dikonversi dapat menggunakan website seperti freeformatter. Hasil konversi menggunakan freeformatter didapatkan timestamp **1531900638372** menjadi **7/18/2018, 12:57:18 AM**.



Gambar 8. Hasil Gambar dari Oxygen Forensic

Pada Gambar 8 merupakan hasil Oxygen forensic berupa gambar. Pada c:\data\data\com.facebook.orca\cache\image ditemukan sebuah gambar dengan nama file pemandangan dengan tipe file jpeg.



Gambar 9. Hasil Audio dari Oxygen Forensic

Pada Gambar 9 Menunjukkan barang bukti data berupa audio. Pada data c:\data\data\com.facebook.orca\cache\audio ditemukan sebuah file audio bernama 008E5f9A berformat mp4..

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1658

3.4. Reporting

Pada tahap reporting merupakan hasil analisis yang telah dilakukan, berikut hasil dari *tool* forensik yang telah ditemukan pada Tabel 2.

Tabel 2. Hasil *tool* Oxigen Forensic

Data	Oxygen Forensic
Akun	Ya
Percakapan	Ya
Gambar	Ya
Audio	Ya
Video	Tidak

Pada tahap ini telah melakukan skenario yaitu data pesan dihapus dan tidak dihapus, pada saat ketika data pesan dihapus, tidak ada satupun data yang didapat dan pada waktu tidak dihapus, dapat menampilkan berupa text percakapan, gambar dan audio pada saat menggunakan tool Oxigen forensic.

4. KESIMPULAN

Berdasarkan hasil dari proses penelitian ini, dalam penelitian ini telah melakukan skenario penelitian yang dilakukan adalah menggunakan *Smartphone* Galaxy V+ SM-G31HZ, melakukan proses *Rooting*, install aplikasi Facebook Messenger , pembuatan pesan, melakukan infestigasi menggunakan tool forensic yang bernama Oxigen forensic, kemudian melakukan analisis pada ketiga alat perangkat lunak forensik tersebut, hasil dari analisis akan dilaporkan 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*). Hasil yang telah didapatkan adalah text percakapan, gambar dan audio.

5. SARAN

Saran-saran untuk penelitian lebih lanjut membandingkan alat lebih banyak lagi dengan metode yang berbeda.

DAFTAR PUSTAKA

[1] R. Umar, A. Yudhana, and M. Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary," no. April, 2017.

[2] A. Yulianti, M. Zulhelmi, D. Suryani, "Aplikasi Legalitas Surat Izin Mengemudi (SIM) Berbasis Mobile (Studi Kasus : Polisi Resort Rengat)," *IT Journal Research and Development*, vol. 2, no. 2, pp. 34–44, 2018.

[3] I. Riadi and R. Umar, "*Identification Of Digital Evidence On Android's Blackberry* Messenger *Using NIST Mobile Forensic Method*" *International Journal of Computer Science and Information Security (IJCSIS).*, vol. 15, no. 5, pp. 3–8, 2017.

[4] C. Anglano, "Forensic analysis of WhatsApp Messenger on Android smartphones," *Digit. Investig.*, vol. 11, no. 3, pp. 1–13, 2014.

[5] I. Riadi, A. Fadlil, and A. Fauzan, "Evidence Gathering and Identification of LINE Messenger on Android Device," *IJCSIS*, vol. 16 no. 5 May, pp. 1–6, 2018.

IT Journal Research and Development
Vol.3, No.1, Agustus2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1658

[6] I. R. Nuril Anwar, "*Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web*,", *JITEKI*, vol. 3, no. June, pp. 1–10, 2017.
[7] R. Umar, I. Riadi, and G. maulana Zamroni, "*A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements*," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, pp. 69–75, 2017.
[8] I. Riadi, J. Eko, A. Ashari, and S. Subanar, "*Internet Forensics Framework Based-on Clustering*," *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 12, pp. 115–123, 2013.
[9] M. A. Zulkifli and U. A. Dahlan, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard," *Int. J. Comput. Appl.*, vol. 180, no. 35, pp. 23–30, 2018.
[10] A. Mahajan, M. S. Dahiya, and H. P. Sanghvi, "*Forensic Analysis of Instant Messenger Applications on Android Devices*," *Int. J. Comput. Appl.*, vol. 68, no. 8, pp. 38–44, 2013.
[11] M. Kukuh, I. Riadi, and Y. Prayudi, "Forensics Acquisition and Analysis Method of IMO Messenger," *Int. J. Comput. Appl.*, vol. 179, no. 47, pp. 9–14, 2018.
[12] J. Fahana, R. Umar, and F. Ridho, "Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan," *Query J. Inf. Syst.*, vol. 1, no. 2, pp. 6–14, 2017.
[13] R. A. Putra, A. Fadlil, and I. Riadi, "Forensik Mobile Pada Smartwach Berbasis Android," *JURTI*, vol. 1, no. 1. pp. 41–47, 2017.
[14] Faiz Albanna, Imam Riadi, "Forensic Analysis of Frozen Hard Drive Using Static Forensics Method", International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 1, January 2017.
[15] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android ' s," *IJCSIS*, vol. 15, no. 5, pp. 3–8, 2017.
[16] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile forensic tools evaluation for digital crime investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, 2018.