HASIL CEK_60020397_C.1.B.32

by Imam Surat 60020397

Submission date: 21-Mar-2021 05:44AM (UTC+0700)
Submission ID: 1537940062
File name: HASIL_CEK_60020397_C.1.B.32.pdf (1,008.28K)
Word count: 5500
Character count: 32970

Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 5 No. 1 (2021) 45 - 54 ISSN Media Elektronik: 2580-0760

Akuisisi Bukti Digital Viber *Messenger* Android Menggunakan Metode *National Institute of Standards and Technology* (NIST)

Imam Riadi[1], Rusydi Umar[2], Muhammad Irwan Syahib[3]
[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan
[2,3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan
[1]imam.riadi@is.uad.ac.id [2]rusydi@mti.uad.ac.id [3]muhammad1807048014@webmail.uad.ac.id

Abstract

Viber is one of the most popular social media in the Instant Messenger application category that can be used to send text messages, make voice calls, send picture messages and video messages to other users. As many as 260 million people around the world have used this application. Increasing the number of viber users certainly brings positive and negative impacts, one of the negative impacts of this application is the use of digital forensic crime. This research simulates and removes digital crime evidence from the viber application on Android smartphones using the National Institute of Standards Technology (NIST) method, which is a method that has work guidelines on forensic policy and process standards to ensure each investigator follows the workflow the same so that their work is documented and the results can be accounted for. This study uses three forensic tools, MOBILedit Forensic Express, Belkasoft and Autopsy. The results in this study show that MOBILedit Forensic Express gets digital evidence with a percentage of 100% in getting accounts, contacts, pictures and videos. While proof of digital chat is only 50%. Belkasoft gets digital evidence with a percentage of 100% in getting accounts, contacts, pictures and videos. While proof of digital chat is only 50%. For Autopsy does not give the expected results in the extraction process, in other words the Autopsy application gives zero results. It can be concluded that MOBILedit Forensic Express and Belkasoft have a good performance compared to Autopsy and thus this research has been completed and succeeded in accordance with the expected goals.

Keywords: Viber, NIST, Digital Forensic, Mobile forensic, Digital Evidence.

Abstrak

Viber merupakan salah satu media sosial yang popular untuk kategori aplikasi *Instant Messenger* yang dapat digunakan untuk mengirim pesan teks, melakukan panggilan suara, mengirim pesan gambar dan pesan berupa video kepada sesama penggunanya. Sebanyak 260 juta orang di seluruh dunia telah menggunakan aplikasi ini. Peningkatan jumlah pengguna viber tentu membawa dampak positif dan juga negatif, salah satu dampak negative aplikasi ini adalah penggunaan dalam hal melakukan kejahatan forensik digital. Penelitian ini melakukan simulasi dan pengangkatan barang bukti kejahatan digital dari aplikasi viber pada *smartphone* Android dengan menggunakan metode *National Institute of Standards Technology* (NIST) yang merupakan salah satu metode yang memiliki panduan kerja pada kebijakan dan standar proses forensik untuk menjamin setiap investigator mengikuti alur kerja yang sama sehingga pekerjaan mereka terdokumentasikan dan hasilnya dapat dipertanggung jawabkan. Penelitian ini menggunakan tiga alat forensik, MOBILedit Forensic Express, Belkasoft dan Autopsy. Hasil dalam penelitian ini menujukan bahwa MOBILedit Forensic Express mendapatkan hasil bukti digital dengan persentase berupa 100% dalam mendapatkan akun, kontak, gambar dan video. Sedangkan bukti digital *chat* hanya 50%. Belkasoft mendapatkan hasil bukti digital dengan persentase 100% dalam mendapatkan akun, kontak, gambar dan video. Sedangkan bukti digital *chat* hanya 50%. Untuk Autopsy tidak memberikan hasil yang diharapkan dalam poses ekstraksi, dengan kata lain aplikasi Autopsy memberikan hasil nol (*zero result*). Dapat disimpulkan bahwa MOBILedit Forensic Express dan Belkasoft memiliki kinerja yang baik dibandingkan dengan Autopsy dan dengan demikian penelitian ini telah selesai dan berhasil sesuai dengan tujuan yang diharapkan.

Kata kunci: Viber, NIST, Forensik Digital, *Mobile* Forensik, Bukti Digital.

Diterima Redaksi: 13-11-2020 | Selesai Revisi: 10-02-2021 | Diterbitkan Online: 14-02-2021

1. Pendahuluan

Perkembangan teknologi dari waktu ke waktu sangat pesat, salah satunya perkembangan *smartphone* yang selalu mengalami perkembangan dari segi sistem operasi, fitur, spesifikasi, dan aplikasi. Teknologi yang semakin canggih menjadi bagian yang tidak bisa lepas dari kehidupan masyarakat, tidak hanya melakukan kegiatan-kegiatan positif namun kegiatan-kegiatan negatif. Perkembangan teknologi juga sangat berpengaruh terhadap jumlah pengguna internet di dunia. Hal ini memberikan dampak yang sangat signifikan seiring kemudaahan yang didapat di dalam untuk bersosial media. Jumlah pengguna aktif media sosial didunia telah mencapai 2,31 Triliun, yang artinya jumlah tersebut setara dengan 31% dari total seluruh populasi penduduk. Pada Januari 2016 pengguna media sosial yang mengakses *smartphone* sebanyak 1,97 Triliun atau setara dengan 27% populasi penduduk dunia [1].

Indonesia masuk dalam daftar 10 negara terbesar di dunia dalam kategori pengguna internet. Data per maret 2019 menunjukan Indonesia dengan pengguna internet sebanyak 143,26 juta berada di peringkat kelima dunia. Angka ini hanya selisih tipis sebesar 5,8 juta dengan Brasil yang memiliki pengguna internet sebanyak 149,06 juta [2].

Pertumbuhan pengguna internet yang sangat pesat ini juga beriringan dengan banyaknya pengguna media sosial dimana media sosial sangat memudahkan penggunanya untuk berkomunikasi, seperti mengirim pesan taks, pesan gambar, dan video secara gratis [3]. Aplikasi *Instant Messenger* yang banyak digunakan di di Indonesia diantaranya adalah WhatsApp yang diakses sebanyak 1,6 miliar pengguna. Facebook Messenger dan WeChat menyusul dengan masing-masing 1,3 miliar dan 1,09 miliar pengguna. Disisi lain, Viber yang menjadi alternatif pengganti memiliki 260 juta pengguna aktif per bulannya pada tahun 2019. Untuk saat ini alikasi Viber telah didownload sebanyak 500 juta lebih *user* di *playstore* [2].

Viber adalah aplikasi *Istant Messenger* yang fitur dan fungsinya hampir sama dengan aplikasi-aplikasi *chating* lainnya seperti Whatsapp, MiChat, dan lain-lain . Aplikasi *Instant Messenger* yang satu ini sangat berpotensi dipergunakan untuk kejahatan siber seperti prostitusi online, perdagangan barang illegal, perdagangan manusia, dan lain-lain [4]. Aplikasi ini dikembangkan oleh Viber Media Inc. pada tahun 2010. Aplikasi ini juga dapat dengan mudah digunakan untuk mengirim pesan, menelepon, mengirim foto, maupun pesan video kepada sesama penggunanya. Oleh sebab itu aktivitas positif maupun *negative* sangat mudah dilakukan karena penggunaannya sangat *simple* seperti aplikasi-aplikasi *messenger* lainnya [5].

Perkembangan smartphone, media sosial serta banyaknya pengguna internet didunia khusunya di indonesia saat ini banyak disalahgunakan untuk melakukan tindak kejahatan (*cybercrime*) seperti perdagangan manusia, *cyberbully*, penipuan, pemerasan, perdagangan barang illegal, perdagangan nakoba dan lainya [6]. Pada 2016 kejahatan siber yang ditangani Polri sebanyak 4.931 kasus dengan penyelesaian kasus kejahatan tersebut sebanyak 1.119 kasus. sementara pada tahun 2017 mengalami peningkatan menjadi 5.061 kasus dan sebanyak 1.369 kasus yang diselesaikan. Kasus kejahatan siber yang menonjol adalah ujaran kebencian yaitu sebanyak 1.829 kasus, tetapi pada 2017 meningkat drastis menjadi 3.325 kasus. Kasus kejahatan pada digital forensik sangat rentan pada aplikasi *instant messenger* apa saja, seperti WhatsApp, Facebook Messengger dan lain-lain selama fitur-fitur aplikasi tersebut menyediakan pengiriman pesan taks, gambar, dan video [7].

Referensi penelitian sebelumnya yang dikutip dalam penelitian ini memiliki perbedaan dari segi aplikasi yang digunakan untuk simulasi tindak kejahatan, namun terdapat beberapa kesamaan antara lain metode dan sebagian alat yang digunakan. Rangkuman penelitian terdahulu dapat dilihat pada Tabel 1.

Penelitian-penelitian tersebut merupakan acuan yang menjadi dasar untuk melakukan penelitian ini [8]. Dalam melakukan pengangkatan barang bukti atau akuisisi pada aplikasi *Instant Messenger,* penelitian terdahulu sebagian tidak menerapkan skenario penghilangan atau penghapusan barang bukti terlebih dahulu [9]. Sedangkan penelitian ini akan melakukan akuisisi bukti digital dengan skenario penghilangan atau penghapusan bukti-bukti percakapan pelaku terlebih dahulu. Aplikasi Viber dipilih karena aplikasi ini sedang digandrungi dan telah didownload sebanyak 500 juta kali di *play store* sampai dengan saat ini. Penelitian ini bertujuan untuk membuktikan apakah bukti-bukti digital pelaku kejahatan pengguna aplikasi Viber yang telah dihilangkan atau dihapus dapat di akuisisi kembali dengan menggunakan tools forensik dan kerangka kerja dari metode *National Institute of Standards and Technology* (NIST).

2. Metode Penelitian

Penerapan metode yang tepat dalam mengumpulkan data forensik akan memberikan dampak keberhasilan hingga 100% [10]. Pada penelitian ini, penelitian yang dilakukan untuk pengambilan bukti digital berdasarkan metode *National Institute of Standards and Technology* (NIST) yang dapat dilihat pada Gambar 1. Metode forensik ini memiliki tahapan *Collection, Examination, Analysis,* dan *Reporting* [11]. Kerangka dan metodologi ini diperlukan untuk memastikan integritas barang bukti *video* yang diperoleh. Integritas barang bukti akan terjaga apabila proses-proses forensik yang dilakukan

DOI: https://doi.org/10.29207/resti.v5i1.2626

tidak mempengaruhi atau mengubah data dari hasil proses forensik [12].

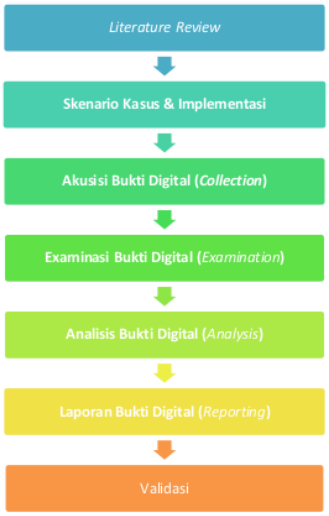
Tabel 1. Rangkuman Hasil Penelitian Terdahulu

Penulis dan Tahun	Judul Penelitian	Hasil Penelitian
Anton Yudhana, Imam Riadi, Ikhwan Anshori (2018)	Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist.	Berhasil mengakuisisi barang bukti pada aplikasi Facebook Messenger menggunkan *tools* Oxygen Forensic dan barang bukti yang didapatkan berupa percakapan, gambar dan audio.
Imam Riadi, Anton Yudhana, Muhamad Caesar Febriansyah Putra (2018)	Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)	Dengan menggunakan tools Oxygen Forensic peneliti berhasil mengagkat barang bukti digital berupa gambar dan *chatting* pada aplikasi Instagram Messenger.
Ikhsan Zuhriyanto, Anton Yudhana, Imam Riadi (2020)	Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop	Barang bukti digital dalam Aplikasi Twitter seperti id user, pesan, gambar, video dan bukti lainnya dapat diambil dengan metode Digital Forensics Research Workshop (DFRWS) dan aplikasi forensik.
Imam Riadi, Rusydi Umar, Muhammad Abdul Aziz (2019)	Forensik Web Layanan Instant Messaging Menggunakan Metode Association Of Chief Police Officers	Dengan menggunakan tools FTK Imager, Peneliti berhasil menemukan barang bukkti digital yang masing-masing tingkat keberhasilannya bervariasi, Whatsapp sebesar 80%, LINE 60% dan Telegram 40%.
Imam Riadi, Rusydi Umar, Arizona Firdonsyah (2017)	Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method	Berdasarkan data yang diperoleh, Andriller hanya mampu memperoleh bukti digital berupa data percakapan, nama pengirim pesan, PIN pengirim dan penerima pesan bersama dengan tanggal percakapan. Sementara data gambar tidak berhasil di dapat.

Gambar 1. Metodologi Penelitian

Agar alur penelitian diketahui secara terstruktur dan dapat menjadi acuan dalam menyelesaikan penelitian yang sistematis, maka berdasarkan metode penelitian pada Gambar 1. dibuatlah sebuah langkah kerja forensik yang digunakan untuk menjabarkan tahapan-tahapan dan langkah-langkah *penelitian* yang akan dilakukan tanpa mengurangi proses yang telah di kemukakan oleh metode NIST [2][13]. Dengan kata lain, langkah kerja forensik pada penelitian ini mengacu pada 4 tahap standar metode forensik dari NIST [14].

Langkah kerja penelitian ini dibagi menjadi 7 tahap penelitian dengan menempatkan langkah dari metode NIST di dalamnya yang dimana dapat dilihat pada Gambar 2. Langkah kerja penelitian dimulai dari *literature review* yaitu dengan cara mengumpulkan beberapa informasi penelitian terdahulu sebagai rujukan dari berbagai sumber [6]. Tahap selanjutnya dilakukan perancangan skenario kasus, menyiapkan alat dan bahan sebagai implementasi untuk simulasi kasus [15]. Selanjutnya masuk pada tahapan metode NIST yaitu proses akuisisi atau tahap *collection* bukti digital yang telah disimulasikan dengan status data-data percakapan telah dihapus terlebih dahulu [16]. kemudian melakukan tahap *examination* yang merupakan tahap pemeriksaan dan pengambilan data dari barang bukti simulasi [17]. Setelah itu melakukan tahap *analysis* yang merupakan tahap menganalisis atau tahap untuk melihat hasil akuisisi secara detil [18].



Gambar 2. Tahapan Penelitian

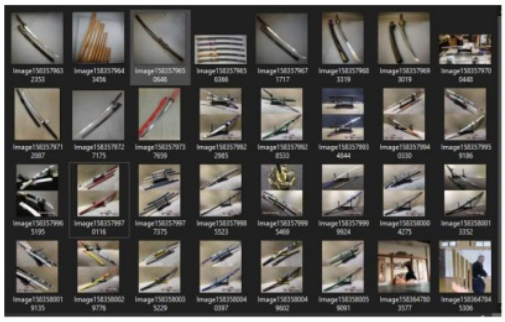
Proses *reporting* yaitu melaporkan hasil analisis barang bukti yang ditemukan pada proses sebelumnya [19]. Terakhir melakukan validasi untuk menguji apakah hasil proses forensik yang diperoleh merupakan hasil yang benar, akurat, kredibel, dan menjaga integritas data sehingga dapat diakui di mata hukum [7].

2.1 Skenario Kasus dan Implementasi

Skenario kasus berupa simulasi penjualan pedang katana asal jepang yang tidak memiliki surat-surat lengkap (ilegal) [20]. Barang bukti dalam penelitian ini berupa 2 *smartphone* android yaitu Evercros B75 dan Samsung Galaxy Grand Duos SM-G318HZ. Kedua *smartphone* ter-*install* aplikasi Viber dan saling melakukan

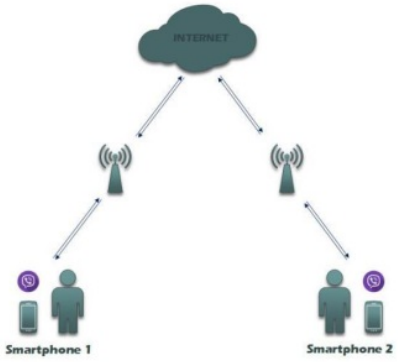
DOI: https://doi.org/10.29207/resti.v5i1.2626

percakapan transaksi barang ilegal tersebut. Percakapan yang dilakukan diantaranya melakukan mengirim dan menerima *chat*, gambar dan *video*. Data awal yang dibuat dalam simulasi kasus berupa 2 akun, 20 *chat*, 30 gambar dan 2 *video*. File gambar dan video ini diambil dari aplikasi instagram dengan hastag #Katana dan #Samurai dan dapat dilihat pada Gambar 3.



Gambar 3. Data Awal 30 Gambar dan 2 Video

Selanjutnya kedua akun dilakukan penghapusan semua pesan teks, gambar dan video percakapan. Hal ini bertujuan menghilangkan barang bukti yang terindikasikan melakukan perdagangan ilegal pedang katana.



Gambar 4. Skenario Kasus Penelitian

Gambar 4. adalah gambaran dari skenario kasus yang dilaukan dimana "Dua orang saling melakukan transaksi jual beli barang illegal berupa pedang katana jepang yang tidak memiliki surat-surat lengkap dengan menggunakan *smartphone* android melalui aplikasi viber. Setelah melakukaan beberapa percakapan dan terjadi transaksi, kedua pelaku terebut menghilangkan jejak dengan menghapus semua isi percakapan mereka".

Alat yang digunakan pada penelitian ini dapat dilihat pada Tabel 2.

Implementasi dari skenario kasus yang sudah disebutkan sebelumnya dilakukan pada dua *smartphone* yang berstatus sebagai barang bukti. Kedua *smartphone* tersebut dapat dilihat pada Gambar 5. Penelitian ini mensimulasikan barang bukti berupa *smartphone* Evercros B75 sebagai *smartphone* 1 dan Samsung Galaxy Grand Duos SM-G318HZ sebagai *smartphone* 2.

Tabel 2. Alat Penelitian

No	Nama Alat	Deskripsi	Ket.
1	Laptop	Lenovo G40, 8 GB DDR 3 Memory, 700 GB HDD	Perangkat keras
2	Windows 10	Windows 10 Pro	Sistem operasi
3	*Smartphone* 1	Evercros B75	Perangkat keras
4	*Smartphone* 2	Samsung Galaxy Grand Duos SM-G318HZ	Perangkat keras
5	Viber	-	Aplikasi Android
6	MOBILedit Forensic Express	Versi 4.1.0	Tool akuisisi
7	Belkasoft	Versi 9.6	Tool akuisisi
8	Autopsy	Versi 4.14.0	Tool akuisisi

Gambar 5. *Smartphone* Barang Bukti

Perangkat *smartphone* yang digunakan pada penelitian ini adalah sebanyak 2 buah, *smartphone* 1 menggunakan *handphone* merek Evercoss dan *smartphone* 2 menggunakan *handphone* merek Samsung dengan masing-masing mempunyai spesifikasi yang berbeda. Spesifikasi kedua *smartphone* tersebut dapat dilihat pada Tabel 3.

Tabel 3. Spesifikasi Barang Bukti

Spesifikasi	*Smartphone* 1	*Smartphone* 2
Merek	Evercoss	Samsung
Seri	B75	Galaxy
IMEI	358441061746***	356803072239***
OS	Android	Android
Versi OS	5.1 (Lollipop)	4.4.4 (KitKat)

3. Hasil dan Pembahasan

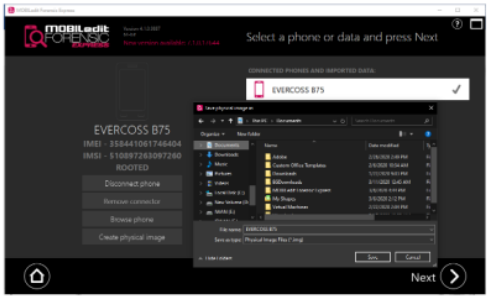
Sebelum melakukan proses akuisisi barang bukti, terlebih dahulu melakukan isolasi perangkat *smartphone* dari komunikasi. Isolasi perlu dilakukan untuk menghindari hal-hal yang dapat merusak bukti digital

DOI: https://doi.org/10.29207/resti.v5i1.2626

atau mempengaruhi integritas data di dalamnya. Langkah pertama adalah merubah status perangkat ke dalam *airplane mode,* selanjutnya mengaktifkan opsi *developer options* untuk proses forensik. *Tools* forensik yang digunakan pada penelitian ini adalah MOBILedit Forensik, Belkasoft dan Autopsy.

3.1 Akuisisi Bukti Digital (*Collection*)

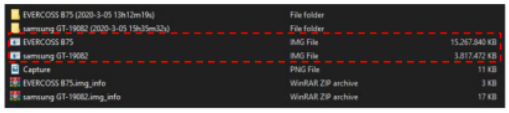
Collection merupakan tahap paling awal dalam metode NIST, tahap ini adalah tindakan untuk pengamanan barang bukti [21]. Tahap ini melakukan koleksi, identifikasi, rekaman atau pengambilan data dari sumber data yang relevan sesuai prosedur untuk menjaga integritas data. Barang bukti yang di usulkan adalah dua buah perangkat *smartphone*. Untuk menjaga barang bukti itu asli dan tidak rusak, maka penjagaan integritas data dapat dilakukan dengan teknik isolasi barang bukti fisik dan pembuatan *backup* berupa *cloning* atau *image file* dari barang bukti tersebut [22]. Tahap pengambilan barang bukti digital ini memiliki risiko yang sangat tinggi, jika terjadi kesalahan fatal, data dan bukti digital yang ada pada *smartphone* dapat hilang atau *corrupted* sehingga tidak terbaca, oleh karena itu perlu dilakukan preservasi barang bukti, yaitu melakukan backup atau imaging *smartphone* yang menjadi barang bukti, proses ini disebut juga *logical acquisition* [23].



Gambar 6. Proses *Backup* Barang Bukti *Smartphone*

Gambar 6. menunjukan proses *backup* barang bukti *smartphone* menggunakan adalah MOBILedit Forensic Express. Kemampuan tool MOBILedit Forensic Express ini dalam membuat sebuah backup sistem *smartphone* cukup baik, MOBILedit Forensic Express mampu membuat backup *smartphone* dengan ekstensi AB (Android *Backup*), img, zip, dan beberapa jenis ekstensi lain sehingga dapat dibuka dalam berbagai tool forensik [7].

Hasil dari proses backup ini berupa dokumen image dari masing-masing *smartphone* Android dengan ekstensi img dengan ukuran dokumen yang bervariasi tergantung pada banyaknya data pada *smartphone* tersebut, seperti terlihat pada Gambar 7.

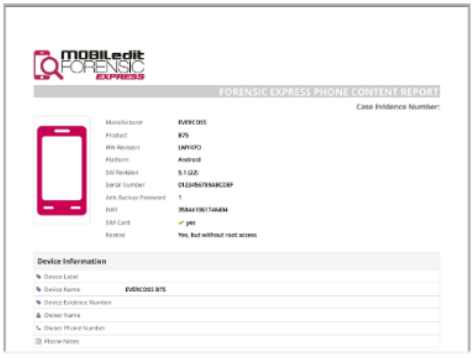


Gambar 7. Hasil Proses *Backup*

3.2 Examinasi Bukti Digital (*Examination*)

Tiga tool forensik yang digunakan sebagai alat akuisisi pada tahap *Examination* ini adalah MOBILedit Forensic Express, Belkasoft dan Autopsy. Hasil dari masing-masing *tools* ini dapat menghasilkan bukti yang sama [24].

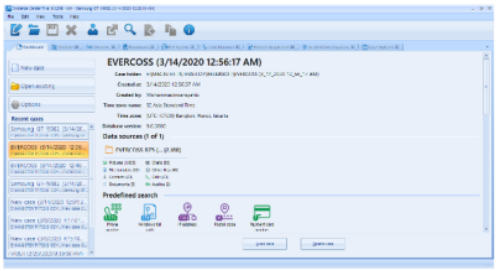
Examination dengan MOBILedit Forensic Express memiliki 2 cara, cara yang pertama yaitu barang bukti harus terkoneksi terlebih dahulu pada komputer atau laptop tempat MOBILedit Forensic Express di-install. Cara yang kedua dengan membuka *file image* dari *smartphone* yang telah dilakukan imaging sebelumnya. Dalam proses *examination* ini dilakukan cara yang kedua. Hasil ekstraksi yang telah dilakukan dengan MOBILedit Forensic Express akan ditampilkan dalam *full report*. Pada penelitian ini, *full Report* yang dipilih adalah dalam bentuk format PDF. Tampilan *full Report* untuk barang bukti *smartphone* seperti ditunjukkan pada Gambar 8.



Gambar 8. *Full Report* MOBILedit *Smartphone*

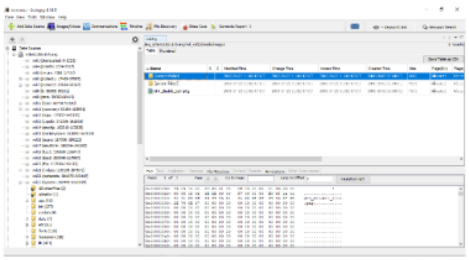
Examination dengan Belkasoft dapat melakukan extraksi langsung dan ekstraksi melaluai *physical image*. *Examination* dengan Belkasoft dilakukan ekstraksi *physical image* yang telah dibuat menggunakan MOBILedit Forensic Express sebelumnya. Hasil extraksi yang didapatkan berupa file-file seperti percakapan text, file gambar, file video, file dokumen, kontak, log panggilan dan lain-lain. Masing-masing file tersebut mempunyai ukuran dan jumlah file yang berbeda-beda sesuai dengan jumlah chat yang terdapat dalam aplikasi viber pada masing-masing *smartphone* tersebut. Tampilan *full Report* untuk barang bukti salah satu *smartphone* yang dilakukan proses extraksi dapat dilihat pada Gambar 9.

DOI: https://doi.org/10.29207/resti.v5i1.2626



Gambar 9. *Full Report* Belkasoft *Smartphone*

Examination dengan Autopsy tidak dapat melakukan extraksi langsung tetapi dapat melakukan ekstraksi melaluai *physical image*. Proses ekstraksi barang bukti pada Autopsy ini dilakukan ekstraksi *physical image* yang telah dibuat menggunakan MOBILedit Forensic Express sebelumnya. Tampilan *full Report* untuk barang bukti *smartphone* dapat dilihat pada Gambar 10.



Gambar 10. *Full Report* Autopsy *Smartphone*

3.3 Analisis Bukti Digital (*Analysis*)

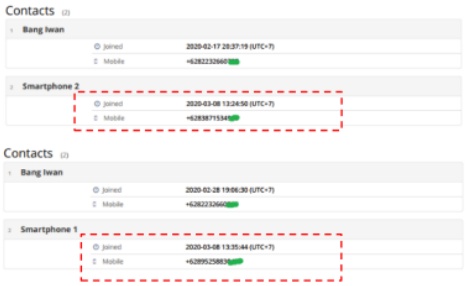
Tahap *Analysis* merupakan tahap menganalisis atau tahap untuk melihat hasil dari tahap *Examination* yang sebelumnya secara detil untuk mendapatkan bukti digital pada barang bukti forensik [25]. Penelitian ini membatasi pencarian bukti digital pada hasil yang didapat dari aplikasi Viber berupa akun, kontak, pesan teks, foto dan video.

Hasil ekstraksi yang didapatkan dari proses *Examination* yang telah dilakukan pada dua *Smartphone* menggunakan tool MOBILedit Forensik Express mendapatkan hasil berupa data akun Viber, nomor *handphone*, daftar kontak, pesan teks, gambar dan video.

Gambar 11. Akun Aplikasi Viber Pada Barang Bukti *Smartphone*

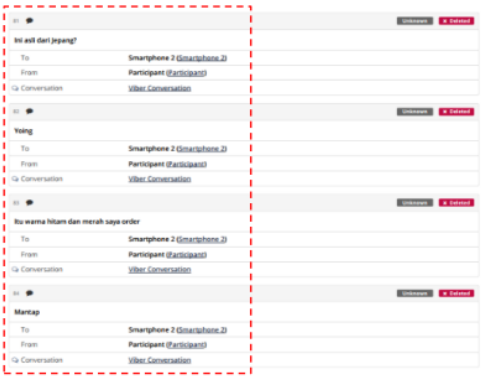
Gambar 11. merupakan bukti digital yang di dapat berupa informasi pemilik akun Viber yang terinstal pada *Smartphone*. Informasi yang didapat berupa nomor *handphone* yang dipakai pelaku untuk mendaftar akun pada proses instalasi aplikasi Viber.

Hasil dari barang bukti yang berhasil di ekstraksi pada perangkat *Smartphone* 1 mendapatkan kontak *Smartphone* 2 yang digunkan untuk transaksi dalam simulasi. Sebaliknya, Hasil dari barang bukti yang berhasil di ekstraksi pada kedua *Smartphone*.



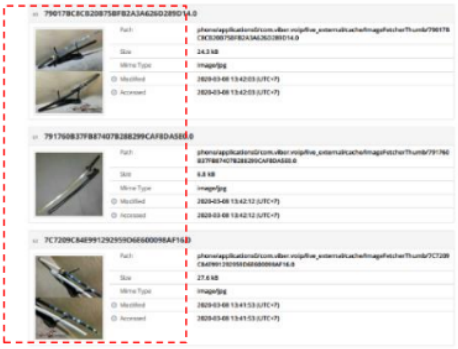
Gambar 12. Informasi Kontak Pada Barang Bukti *Smartphone*

Gambar 12. merupakan bukti digital berupa informasi kontak yang tersimpan di aplikasi Viber yang terinstal pada 2 buah barang bukti *Smartphone*.



Gambar 13. Bukti Percakapan Teks Pada Barang Bukti *Smartphone*

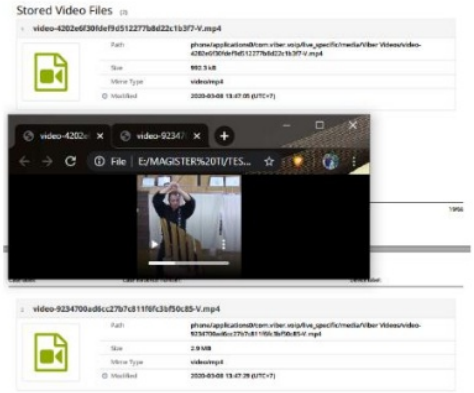
Gambar 13. merupakan hasil ekstraksi yang dilakukan menggunakan MOBILedit Forensic Express. Proses ekstraksi tersebut dapat menampilkan bukti-bukti percakapan yang telah dihapus pada masing-masing perangkat barang bukti *Smartphone*.



Gambar 14. Bukti Pesan Gambar Pada Barang Bukti *Smartphone*

DOI: https://doi.org/10.29207/resti.v5i1.2626

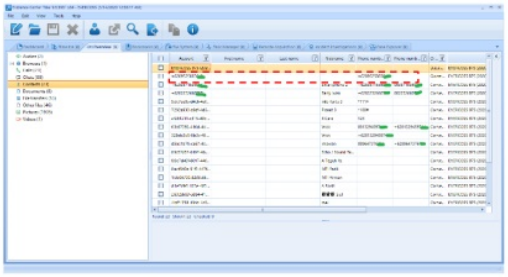
Gambar 14. Bukti percakapan gambar yang merupakan hasil menggunakan MOBILedit Forensic Express.



Gambar 15. Bukti Pesan Video Pada Barang Bukti *Smartphone*

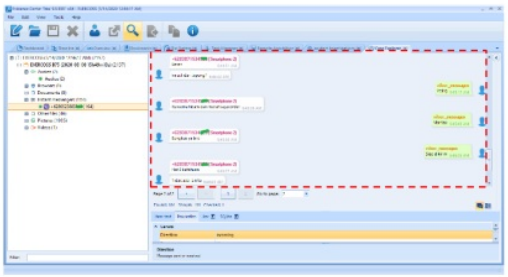
Gambar 15. merupakan barang bukti berupa video yang didapat dari hasil ekstraksi dari kedua *smartphone*.

Hasil ekstraksi yang didapatkan dari proses *examination* yang telah dilakukan pada kedua *Smartphone* menggunakan tool Belkasoft mendapat hasil berupa data akun Viber, daftar kontak, pesan teks, gambar dan video.



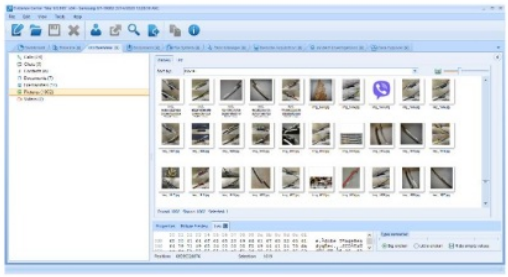
Gambar 16. Hasil Info Akun dan Kontak *Smartphone*

Gambar 16. merupakan bukti digital yang didapat. Bukti digital yang didapat berupa informasi pemilik akun dan informasi kontak aplikasi Viber yang terinstal pada masing-masing *Smartphone*. Informasi yang didapat berupa nomor *handphone* yang dipakai kedua pelaku untuk mendaftar akun pada proses instalasi aplikasi Viber dan informasi kontak yang tersimpan.



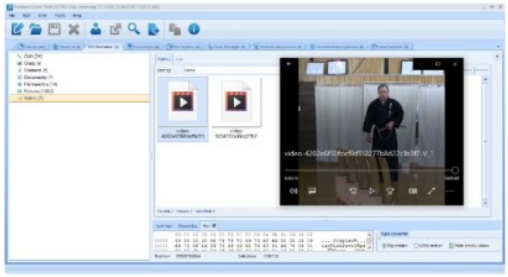
Gambar 17. Bukti Percakapan teks *Smartphone*

Gambar 17. merupakan barang bukti yang berhasil di ekstraksi. Hasil ekstraksi tersebut dapat menampilkan bukti percakapan teks yang telah dihapus pada masing-masing perangkat yaitu *Smartphone* 1 dan *Smartphone* 2.



Gambar 18. Bukti Pesan Gambar pada *Smartphone*

Gambar 18. adalah bukti percakapan gambar berupa foto yang didapat dari hasil ekstraksi pada *Smartphone*.



Gambar 19. Bukti Pesan Video pada *Smartphone*

Gambar 19. merupakan barang bukti berupa video yang didapat dari hasil ekstraksi *Smartphone*.

Analisis yang dilakukan pada hasil ekstraksi kedua barang buki berupa *Smartphone* menggunakan Autopsy tidak memberikan hasil yang diharapkan disebabkan Autopsy tidak memiliki fitur *file decryption* untuk membuka engkripsi *file* database aplikasi Viber, sehingga ekstraksi menggunakan aplikasi Autopsy memberikan hasil nol (*zero result*).

3.4 Laporan Bukti Digital (*Reporting*)

Tahap *Reporting* merupakan tahap pembuatan laporan berupa data-data hasil analisis pada tahap yang dilakukan sebelumnya, yang mencakup deskripsi bukti-bukti apa saja yang berhasil didapat dan presentasi keberhasilan alat forensik dalam melakukan ekstraksi dalam melakukan akuisisi barang bukti [26].

Tabel 4. Bukti Digital yang didapatkan pada *Smartphone* 1

No	Bukti Digital	Alat Forensik		
		MOBILedit	Belkasoft	Autopsy
1	Akun	2	2	Tidak Ada
2	Kontak	Ada	Ada	Tidak Ada
3	*Chat*	10	10	Tidak Ada
4	Gambar	30	16	Tidak Ada
5	Video	2	2	Tidak Ada

DOI: https://doi.org/10.29207/resti.v5i1.2626

Tabel 5. Persentasi Bukti Digital yang didapatkan pada *Smartphone* 1

No	Bukti Digital	Persentasi Keberhasilan (%)		
		MOBILedit	Belkasoft	Autopsy
1	Akun	100	100	Tidak Ada
2	Kontak	100	100	Tidak Ada
3	*Chat*	50	50	Tidak Ada
4	Gambar	100	100	Tidak Ada
5	Video	100	100	Tidak Ada

Bukti digital yang didapat pada aplikasi viber dengan menggunakan MOBILedit Forensic Express, Belkasoft pada *smartphone* 1 dapat dilihat pada Tabel 4. Hasil ekstraksi dari MOBILedit Forensic Express dan Belkasoft sama-sama mendapatkan masing-masing 2 akun, 1 kontak (*Smartphone* 2), 10 *chat*, 30 gambar dan 2 video. Presentasi kinerja kedua alat forensik dapat dilihat pada Tabel 5.

Dalam mengekstraksi bukti percakapan teks, masing-masing hanya medapat 50% dari 20 percakapan teks yang disimulasikan. Untuk hasil pencarian barang bukti di tool Autopsy tidak ditemukan. Seperti yang sudah dijelaskan pada tahap analisis, hal ini dikarenakan Autopsy tidak memiliki fitur *file decryption* untuk membuka engkripsi *file* database aplikasi Viber, sehingga ekstraksi menggunakan aplikasi Autopsy memberikan hasil nol (*zero result*).

Tabel 6. Bukti Digital yang didapatkan pada *Smartphone* 2

No	Bukti Digital	Alat Forensik		
		MOBILedit	Belkasoft	Autopsy
1	Akun	2	2	Tidak Ada
2	Kontak	Ada	Ada	Tidak Ada
3	*Chat*	10	10	Tidak Ada
4	Gambar	30	30	Tidak Ada
5	Video	2	2	Tidak Ada

Tabel 7. Persentasi Bukti Digital yang didapatkan pada *Smartphone* 2

No	Bukti Digital	Persentasi Keberhasilan (%)		
		MOBILedit	Belkasoft	Autopsy
1	Akun	100	100	Tidak Ada
2	Kontak	100	100	Tidak Ada
3	*Chat*	50	50	Tidak Ada
4	Gambar	100	100	Tidak Ada
5	Video	100	100	Tidak Ada

Bukti digital yang didapat pada *smartphone* 2 sama dengan bukti digital pada *smartphone* 1 dimana hasil ekstraksi dari MOBILedit Forensic Express dan Belkasoft sama-sama mendapatkan masing-masing 2 akun, 1 kontak (*Smartphone* 2), 10 *chat*, 30 gambar dan 2 video. Bukti digital dapat dilihat pada Tabel 6. Dalam mengekstraksi bukti percakapan teks, kedua alat forensik masing-masing hanya medapat 50% dari 20 percakapan teks yang disimulasikan. Presentasi kinerja kedua alat forensik dapat dilihat pada Tabel 7.

Untuk hasil pencarian barang bukti di tool Autopsy lagi-lagi tidak ditemukan apapun. Seperti yang sudah dijelaskan pada tahap analisis, hal ini dikarenakan Autopsy tidak memiliki fitur *file decryption* untuk membuka engkripsi *file* database aplikasi Viber, sehingga ekstraksi menggunakan aplikasi Autopsy memberikan hasil nol (*zero result*).

3.5 Validasi

Proses validasi diperlukan untuk menguji apakah hasil proses forensik yang diperoleh merupakan hasil yang benar, akurat, kredibel, dan menjaga integritas data sehingga dapat diakui di mata hukum. Hasil tes forensik setidaknya harus *repeatable* (dapat diulang kembali) dan *reproducible* (dapat diproduksi kembali) untuk menguji validitas hasil forensik dan dapat digunakan sebagai barang bukti [27]. Maka dari itu, proses validasi terdiri dari dua proses yaitu validasi *repeatability* dan validasi *reproducibility*. Proses validasi *repeatability* dilakukan pada *Smartphone* 1 dan *Smartphone* 2 menggunakan MOBILedit Forensic Express, Belkasoft dan Autopsy. Untuk hasil ekstraksi menggunakan tool Autopsy dilakukan dua kali ekstraksi dan tidak ditemukan hasil barang bukti digital apapun.

Tabel 8. Hasil Validasi *Repeatability*

Bukti Digital	MOBILedit Forensic Express	
	Ekstraksi 1	Ekstraksi 1
Akun	2	2
Kontak	Ada	Ada
Chat	10	10
Gambar	30	30
Video	2	2
Bukti Digital	Belkasoft	
	Ekstraksi 1	Ekstraksi 1
Akun	2	2
Kontak	Ada	Ada
Chat	10	10
Gambar	30	30
Video	2	2
Bukti Digital	Autopsy	
	Ekstraksi 1	Ekstraksi 1
Akun	Tidak Ada	Tidak Ada
Kontak	Tidak Ada	Tidak Ada
Chat	Tidak Ada	Tidak Ada
Gambar	Tidak Ada	Tidak Ada
Video	Tidak Ada	Tidak Ada

Tabel 8. merupakan hasil validasi *repeatability* yang dilakukan pada 2 alat forensik. validasi *repeatability* memberikan hasil yang positif. Kinerja alat forensik tersebut dinilai layak melakukan proses forensik pada aplikasi Viber yang terpasang pada *Smartphone* 1 dan *Smartphone* 2.

Validasi *reproducibility* dilakukan dengan pengujian objek yang sama dengan tiga alat forensik dalam waktu yang relatif lama. Alat forensik yang digunakan dinyatakan telah memenuhi pengujian validasi *reproducibility* apabila hasil yang didapat dari masing–masing alat forensik memiliki kesamaan dan tidak mengalami perubahan. Proses forensik dilakukan secara berulang dalam waktu yang sangat berdekatan menggunakan metode dan objek penelitian yang sama dengan alat penelitian yang berbeda. Proses validasi *reproducibility* dilakukan pada dua perangkat yaitu *smartphone* 1 dan *smartphone* 2 dengan tool

DOI: https://doi.org/10.29207/resti.v5i1.2626

menggunakan MOBILedit Forensic Express, Belkasoft dan Autopsy.

Tabel 9. Hasil Validasi *reproducibility*

Bukti Digital	MOBILedit Forensic Express	
	Ekstraksi 1	Ekstraksi 1
Akun	2	2
Kontak	Ada	Ada
Chat	10	10
Gambar	30	30
Video	2	2
Bukti Digital	Belkasoft	
	Ekstraksi 1	Ekstraksi 1
Akun	2	2
Kontak	Ada	Ada
Chat	10	10
Gambar	30	30
Video	2	2
Bukti Digital	Autopsy	
	Ekstraksi 1	Ekstraksi 1
Akun	Tidak Ada	Tidak Ada
Kontak	Tidak Ada	Tidak Ada
Chat	Tidak Ada	Tidak Ada
Gambar	Tidak Ada	Tidak Ada
Video	Tidak Ada	Tidak Ada

Tabel 9. merupakan hasil validasi *reproducibility* yang dilakukan pada 2 alat forensik memberikan hasil yang positif. Sama seperti validasi *repeatability*, kinerja alat forensik tersebut dinilai layak melakukan proses forensik pada aplikasi Viber yang terpasang pada *Smartphone* 1 dan *Smartphone* 2.

4. Kesimpulan

Berdasarkan hasil yang diperoleh dari proses akuisisi 2 barang bukti, yang terdapat pada Tabel 4 dan Tabel 6 yang menggunakan 3 tool forensik dapat disimpulkan bahwa: Proses analisis menggunakan MOBILedit Forensic Express di masing-masing *smartphone* berhasil mendapatkan bukti digital berupa 2 akun yang digunakan untuk saling berinteraksi, 1 kontak di masing-masing *Smartphone*, 10 *chat*, 30 gambar dan 2 video. Proses analisis menggunakan Belkasoft berhasil mendapatkan bukti digital berupa 2 akun, masing-masing 1 kontak, 10 chat, 30 gambar dan 2 video. Sedangkan proses analisis menggunakan Autopsy tidak memberikan hasil yang diharapkan, dengan kata lain aplikasi Autopsy memberikan hasil nol (zero result), hal ini disebabkan Autopsy tidak memiliki fitur *file decryption* untuk membuka engkripsi *file* database aplikasi Viber.

Saran yang diberikan untuk penelitian selanjutnya agar perlu dilakukan pengembangan dengan menggunakan aplikasi forensik, metode-metode dan kasus-kasus forensik lain serta perlu dilakukan pengangkatan bukti digital pada *smartphone* berbasis iPhone atau yang lainnya.

Daftar Rujukan

[1] W. A. Mukti, S. U. Masruroh, and D. Khairani, "Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android," *J. Tek. Inform.*, vol. 10, no. 1, pp. 73–84, 2018, doi: 10.15408/jti.v10i1.6820.

[2] M. I. Syahib, I. Riadi, and R. Umar, "Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST)," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 4, no. 1, p. 170, 2020, doi: 10.30645/j-sakti.v4i1.196.

[3] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 1, 2016, doi: 10.26418/jp.v2i1.14369.

[4] D. Hariyadi, W. W. Winarno, A. Luthfi, M. Informatika, F. Teknologi, and U. I. Indonesia, "Analisis Konten Dugaan Tindak Kejahatan Dengan Barang Bukti Digital Blackberry Messenger," pp. 81–89, 2014.

[5] A. P. Utama Siahaan, "Pelanggaran Cybercrime Dan Kekuatan Yurisdiksi Di Indonesia," *J. Tek. dan Inform.*, vol. 5, no. 1, pp. 6–9, 2018.

[6] A. Fauzan, I. Riadi, and A. Fadlil, "Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime," *Annu. Res. Semin.*, vol. 2, no. 1, pp. 159–163, 2017.

[7] M. D. K. Perdani, W. Widyawan, and P. I. Santosa, "Blockchain untuk Keamanan Transaksi Elektronik Perusahaan Financial Technology (Studi Kasus pada PT XYZ)," *Semnasteknomedia*, vol. 6, no. 1, pp. 7–12, 2018.

[8] Z. Akbar, B. Nugraha, and M. Alaydrus, "Whatsapp Forensics Pada Android Smartphone : a Survey," *Sinergi*, vol. 20, no. 3, p. 7, 2016, doi: 10.22441/sinergi.2016.3.006.

[9] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *It J. Res. Dev.*, vol. 3, no. 1, p. 13, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[10] A. Tanner and D. Dampier, "Concept mapping for digital forensic investigations," *IFIP Adv. Inf. Commun. Technol.*, vol. 306, pp. 291–300, 2009, doi: 10.1007/978-3-642-04155-6_22.

[11] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," *Natl. Inst. Stand. Technol. Inf. Technol. Lab.*, vol. 145, p. 7, 2011, doi: 10.1136/emj.2010.096966.

[12] I. Riadi and I. M. Nasrulloh, "Analisis Forensik Solid State Drive (Ssd) Menggunakan Framework Grr Rapid Response Forensic Analysis Of Solid State Drives (Ssd) Using The Grr Rapid Response Framework," vol. 6, no. 5, pp. 509–518, 2019, doi: 10.25126/jtiik.201961516.

[13] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3991–4003, 2018, doi: 10.11591/ijece.v8i5.pp3991-4003.

[14] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.

[15] M. H. A. Sunardi, Imam Riadi, "Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi," vol. 1, no. 10, pp. 2–6, 2020.

[16] M. N. Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," vol. 1, no. 3, pp. 108–114, 2017.

[17] I. Riadi and R. Umar, "Identification Of Digital Evidence On Android ' s," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 3–8, 2017.

[18] Nasirudin, "Analisis Telegram mengggunakan Metode NIST," 2019.

[19] R. Umar, I. Riadi, and Z. Guntur Malulana, "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, doi: 10.14569/IJACSA.2017.081210.

[20] C. Anglano, M. Canonico, and M. Guazzone, "Computers & Security The Android Forensics Automator (AnForA): A tool for the Automated Forensic Analysis of Android Applications,"

vol. 88, 2020, doi: 10.1016/j.cose.2019.101650.
[21] I. Riadi, R. Umar, and I. M. Nasrulloh, "Experimental Investigation of Frozen Solid State Drive on Digital Evidence with Static Forensic Methods," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 9, no. 3, p. 169, 2018, doi: 10.24843/lkjiti.2018.v09.i03.p06.
[22] R. A. K. N. Bintang, R. Umar, and U. Yudhana, "Perancangan perbandingan live forensics pada keamanan media sosial Instagram, Facebook dan Twitter di Windows 10," *Pros. SNST ke-9 Tahun 2018 Fak. Tek. Univ. Wahid Hasyim*, pp. 125–128, 2018.
[23] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)," vol. 4, pp. 219–227, 2018.
[24] I. Riyadi, A. Yudhana, and M. C. F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute of Justice (Nij)," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 219–227, 2018, doi: 10.28932/jutisi.v4i2.769.
[25] M. S. Chang and C. Y. Chang, "Forensic analysis of LINE messenger on android," *J. Comput.*, vol. 29, no. 1, pp. 11–20, 2018, doi: 10.3966/199115992018012901002.
[26] S. Madiyanto, H. Mubarok, and N. Widiyasono, "Mobile Forensics Investigation Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS," *J. Rekayasa Sist. Ind.*, vol. 4, no. 01, 2017, doi: 10.25124/jrsi.v4i01.149.
[27] G. M. Zamroni, "Analisis Forensik Instant Messaging (WhatsApp) Berbasis Android," 2018.

DOI: https://doi.org/10.29207/resti.v5i1.2626

HASIL CEK_60020397_C.1.B.32

ORIGINALITY REPORT

7%	8%	5%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	jurnal.iaii.or.id Internet Source	2%
2	doaj.org Internet Source	1%
3	www.ejournal.unkhair.ac.id Internet Source	1%
4	ejournal.unira.ac.id Internet Source	1%
5	Khairunnisak Khairunnisak, Hamid Ashari, Adam Prayogo Kuncoro. "ANALISIS FORENSIK UNTUK MENDETEKSI KEASLIAN CITRA DIGITAL MENGGUNAKAN METODE NIST", Jurnal RESISTOR (Rekayasa Sistem Komputer), 2020 Publication	1%
6	id.scribd.com Internet Source	1%
7	ojs.umrah.ac.id Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		