# IMPLEMENTASI TOOLS AUTOPSY DAN BELKASOFT DALAM ANALISIS FORENSIK PADA WHATSAPP MENGGUNAKAN METODE NIST 800-101 Rev.1

1st Mutafaqih Kalam Robbani
Direktorat Universitas Telkom Purwokerto
Universitas Telkom Purwokerto
Purwokerto, Indonesia
20102274@ittelkom-pwt.ac.id

2nd Trihastuti Yuniati, S.Kom., M.T
Direktorat Universitas Telkom Purwokerto
Universitas Telkom Purwokerto
Purwokerto, Indonesia
trihastutiy@telkomuniversity.ac.id

***Abstrak*** **—** Pada tahun 2023 tercatat aktif pengguna *smartphone* pencapai 7,33 miliar pengguna, sebanyak 91,40% populasi manusia terhubung dengan jaringan perangakat seluler. Namun, peningkatan penggunaan smartphone tidak lepas dari risiko kejahatan siber (*cybercrime*). Fenomena ini mendorong munculnya disiplin baru dalam menangani tindak kejahatan , yang disebut sebagai *mobile forensic*. *Mobile forensic* adalah cabang dari keilmuan forensik yang tujuannya untuk memulihkan barang bukti digital pada *smartphone*, mengingat pentingnya barang bukti digital dalam pengungkapan tindak kejahatan. Utamanya dalam kasus ini pada Aplikasi Whatsapp menjadi salah satu tindak kejahatan, yaitu *scammer*, pelaku melakukan penipuan beruba bait dengan iming-iming hadiah undian yang besar. Kasus penipuan tersebuat bisa menjadi barang bukti telah dilakukan perencanaan tindak kejahatan. Barang bukti pada aplikasi Whatsapp bisa berupa dokumen, video, foto, audio dan juga Lokasi GPS. Oleh karena itu, diperlukan aplikasi fonrensik untuk mempermudah mendapatkan bukti digital secara mudah dan efektif. Penelitian ini bertujuan untuk menilai kualitas kerja kedua alat forensik, yaitu Autopsy dan Belkasoft X, dalam analisis forensik aplikasi pesan instan WhatsApp. Metode evaluasi yang digunakan adalah NIST Special Publication 800-101 Revision 1. Akhir investigasi menggambarkan bahwa Belkasoft X memiliki tingkat ketelitian lebih tinggi, dengan indeks agregat sebesar 90,91%, dibandingkan Autopsy yang mencapai 54,55%. Belkasoft X mampu mendeteksi berbagai bukti digital seperti pesan suara, gambar, dokumen, lokasi GPS, dan metadata WhatsApp, yang tidak dapat diakses oleh Autopsy. Melalui investigasi ini, diharapkan mendapati temuan alat forensik yang optimal dan akurat dalam analisis aplikasi pesan instan, khususnya WhatsApp, sehingga penanganan bukti digital pada *smartphone* berbasis Android dapat dilakukan dengan baik dan sesuai dengan standar hukum yang berlaku.

***Kata kunci*— Forensik, Autopsy, Android, Belkasoft, Forensik Digital, NIST, Smartphone**

## I. PENDAHULUAN

Inovasi kian lama berkembang setiap tahunya. Salah satu inovasi teknologi dengan pengoprasian terbesar adalah *smartphone* dengan android dan IOS sebagai sistem pengoperasinya1. Jumlah transaksi pembayaran seluler mencapai $1,7 triliun pada tahun 2021. Pendapatan utama berasal dari biaya pertukaran kecil yang dikenakan oleh setiap vendor per transaksi. Jumlah transaksi pembayaran seluler ini mencatat pertumbuhan tahunan sebesar 27%[1].

Setiap tahun terjadi kenaikan angka pengguna smartphone di tiap negara. Pada tahun 2023 lebih dari 7,33 miliar Pengguna memiliki smartphone dan 91,40% penduduk dunia terhubung via jaringan seluler secara global. Bersamaan dengan meningkatnya penggunaan smartphone berbasis android dan IOS dikaitkan dengan kejahatan siber (*cybercrime*). Pernyataan tersebut membahas meluasnya tindakan kejahatan siber yang melibatkan pengguna ponsel cerdas, yang kemudian mendorong munculnya disiplin baru dalam penanganan kejahatan tersebut, dikenal sebagai *mobile forensic*[2]. *Mobile forensic* adalah cabang dari kajian forensik yang memfokuskan pada Rekonstruksi bukti elektronik (*digital evidence*) dari perangkat seluler[3].

Bukti elektronik penting dalam upaya penemuan bukti kejahatan, karena merupakan aspek dari barang bukti. Barang bukti merupakan benda yang terkait dengan perilaku kejahatan, dipakai sebagai alat pembukti yang kuat untuk meyakinkan keputusan pengadilan mengenai gugatan tindak kejahatan. Menurut Pasal 5 Undang-Undang Nomor 11 Tahun 2008 (1) tentang "*Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.*"[4]. Menangani bukti elektronik perlu dilaksanakan dengan akurat dan tepat, karena karakteristiknya yang rapuh. Oleh karena itu, diperlukan

aplikasi fonrensik untuk mempermudah mendapatkan bukti digital secara mudah dan optimal.

Penelitian ini bertujuan untuk menilai kinerja Autopsy dan Belkasoft dalam analisis forensik pada aplikasi pesan instan yaitu Whatsapp. Evaluasi ini akan melibatkan Metode *NIST Special Publication 800-101 Revision 1,* yang telah diakui sebagai standar dalam pengujian dan evaluasi alat forensik digital. Metode ini memberikan kerangka kerja yang komprehensif dalam mengukur kehandalan, dan akurasi alat forensik.

## II. KAJIAN TEORI

a) Foresik digital

Proses penerapan wawasan ilmiah dalam merangkai, memeriksa, dan memberlihatkan bukti di dewan hakim. Inti dari forensik adalah keterlibatan dalam penyelamatan dan analisis bukti tersembunyi. Jenis bukti tersembunyi dapat bervariasi, mulai dari jejak *imprint* jari pada jendela, DNA yang diambil dari noda darah, hingga berkas-berkas dalam hard disk computer[5].

b) Forensik mobile

Forensik Mobile didefinisikan sebagai bagian dari forensik digital yang bertujuan untuk mengenali dan mengidentifikasi bukti terkait kejahatan di dunia maya yang melibatkan penggunaan perangkat seluler[6].

c) Bukti Digital

Bukti digital mengutip pada data yang diperoleh digunakan sebagai bukti dalam investigasi hukum atau forensik digital. Ini mencakup berbagai jenis data yang ditemukan pada perangkat elektronik seperti komputer, ponsel, server, dan perangkat penyimpanan lainnya[7].

d) Kejahatan siber

Cybercrime merupakan kejahatan yang dilakukan pada dunia maya dengan memanfaat kan perangkat computer atau seluler yang terhubung dengan internet[8].

e) *Smartphone*

Perangkat yang memungkinkan pengguna untuk berkomunikasi, sambil menyediakan fungsi *Personal Digital Assistant (PDA*) dan kemampuan yang serupa dengan komputer[9].

f) Android

Android dapat diartikan juga sebagai rangkaian perangkat lunak berbasis Linux yang bersifat *open source*, dirancang untuk digunakan pada berbagai perangkat dan beragam bentuk[10].

g) Pesan instant

Layanan komunikasi yang mempermudah individu berkomunikasi secara pribadi dengan pihak lain secara langsung via internet, percakapan melalui pesan instan ini terdiri dari pesan *text*, sekaligus mencakup *voice note* atau rekaman film[11].

h) Whatsapp

Aplikasi perpesanan instan untuk smartphone yang dikenal sebagai WhatsApp Messenger. Dengan menggunakan koneksi internet, aplikasi ini memudahkan *user* mengunggah dan mengirim pesan via jaringan data. Dibentuk pada 24 Februari 2009 dibuat oleh Brian Acton dan Jan Koum[12].

i) Belkasoft X

Belkasoft X (Belkasoft Evidence Center X) adalah alat andalan dari Belkasoft untuk forensik komputer, seluler, dan cloud. Alat ini dapat membantu Anda memperoleh dan menganalisis berbagai perangkat seluler dan komputer, menjalankan berbagai tugas analitis, melakukan pencarian seluruh kasus, menandai artefak, dan membuat laporan[13].

j) Autopsy

*Autopsy* pertama kali dirilis pada tahun 2010 oleh *Basis* Technology. *Basis Technology* adalah perusahaan perangkat lunak forensik digital yang berkantor pusat di Cambridge, Massachusetts, Amerika Serikat. *Autopsy* memiliki fitur-fitur inti yang setara dengan alat forensik *proprietary*, *Autopsy* merupakan solusi investigasi hard drive yang cepat, teliti, dan efisien yang beradaptasi dengan kebutuhan Anda[14].

k) *National Institute of Standards and Technology*

Metode NIST adalah suatu framework yang umum digunakan karena menyediakan standar, panduan, dan praktik unggulan dalam mengelola risiko berkaitan sains dan teknologi informasi[6].

l)

## III. METODE

a) Subjek dan Objek penelitian

1. Subjek penelitian

Autopsy dan Belkasoft adalah subjek dalam penelitian ini. Mereka menjadi fokus utama untuk dievaluasi dalam analisis forensik pada pesan instan menggunakan metode NIST.

2. Objek penelitian

Objek penelitian ini menggunakan whatsaap bertujuan untuk mengukur sejauh mana Autopsy dan Belkasoft dapat efektif dan efisien dalam menangani aspek forensik pada pesan instan, dengan menggunakan metode NIST.

b) Alat dan Bahan Penelitian

1. Alat penelitian

*Tabel 3. 1 Perangkat Keras*

| No. | Perangkat Keras | Keterangan |
|---|---|---|
| 1. | Laptop axioo hype 5 | Laptop yag digunakan sebagai media untuk memasang aplikasi forensik, dengan spesifikasi:<br>- AMD Ryzen 5 5500U dengan Radeon Graphics 2.60 GHz<br>- RAM 16gb<br>- Sistem Operasi Windows 11 |

| | | |
|---|---|---|
| 2. | Vivo y30 | Ponsel pintar yang digunakan sebagai media barang bukti, dengan spesifikasi:<br>- Octa-core 2.3GHz<br>- RAM 4gb<br>- Sistem Operasi Android 12 |
| 3. | Veger USB | Kabel data yang digunakan untuk menghubungkan *smartphone* dengan laptop |

*Tabel 3. 2 Perangkat lunak*

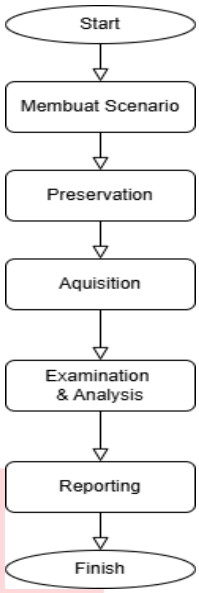
| No | Perangkat lunak | Keterangan |
|---|---|---|
| 1. | Belkasoft X v.2.1.14009 (trial) | Alat forensik |
| 2. | Autopsy 4.2.1.0 | Alat forensik |
| 3. | Whatsapp | Digunakan sebagai barangbukti |

2. Bahan

Penelitian ini menggunakan Whatsapp sebagai bukti digital dalam investigasi penggunaan alat forensik sebagai perbandingannya.

c) Alur Penelitian

Alur penelitian diperlukan sebagai Langkah-langkah dalam melaksanakan penelitian. Alur penelitian ada pada gambar 3.3.




*Gambar 3. 1 Diagram penelitian*

d) Persiapan

Persiapan sebelum pengujian merujuk pada langkah-langkah yang diambil untuk mempersiapkan semua hal yang diperlukan sebelum melakukan pemeriksaan forensic pada telepon. Proses ini melibatkan dua tahapan utama, yaitu *review* literatur dan pengembangan scenario.

1. Studi Literatur

Pencarian referensi, dikumpulkan dari buku, artikel jurnal, dan publikasi ilmiah lainnya guna memperoleh wawasan tentang topik seperti forensik digital, analisis perangkat seluler, dan NIST.

2. Pembuatan sekenario

Penyusunan skenario merupakan langkah dalam merencanakan kegiatan kejahatan di dunia maya. Data yang dihasilkan dari penyusunan skenario ini akan menjadi data awal, yang nantinya akan diungkap melalui proses analisis forensik.

e) Analisa forensik

Berdasarkan metode yang digunakan yaitu *NIST Special Publication 800-101 Revision 1*. Metode ini dipakai sebagai pedoman dalam proses investigasi.

1. *Preservation*

Pada proses preservasi, langkah pertama adalah mengamankan ponsel yang digunakan. Selanjutnya, dilakukan proses pengenalan dan penandaan pada perangkat untuk mengumpulkan data terkait tanpa mengorbankan integritas data.

2. *Acquisition*

Dilakukan penyusunan data secara otomatis maupun

$$I_A = \frac{\sum Q_n}{\sum Q_0} \text{ x } 100 \qquad (3.1)$$

manual menggunakan metode forensic.

3. *Examination & Analysis*

Pada fase pemeriksaan dan analisis, data yang diperoleh dari ponsel akan diselidiki dan dianalisis sesuai dengan tujuan penyelidikan. Fokus utama adalah mengembalikan data seperti riwayat panggilan, kontak

tersimpan, serta media komunikasi dari pesan *text*, foto, audio, dan video dari aplikasi WhatsApp.

4. *Reporting*

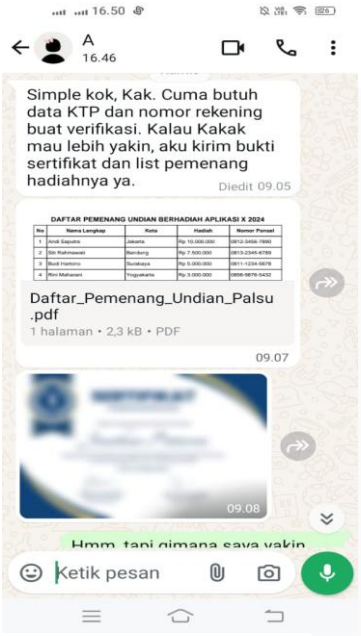
Pada tahap ini, informasi diperoleh dari investigasi termasuk hasil analisis bukti yang dilaporkan. Bukti ini membantu proses penyelidikan untuk mengidentifikasi tersangka. Hasil evaluasi akan dihitung dengan indeks agregatif, untuk menentukan presentase digital *evidance* yang dapat diakses. Indeks agregatif sederhana dapat digunakan untuk menghitung metode perhitungan indeks kuantitas, seperti yang ditunjukkan dalam rumus berikut.

$\sum Q_n$ = Jumlah data Hasil
$\sum Q_0$ = Jumlah data Asli

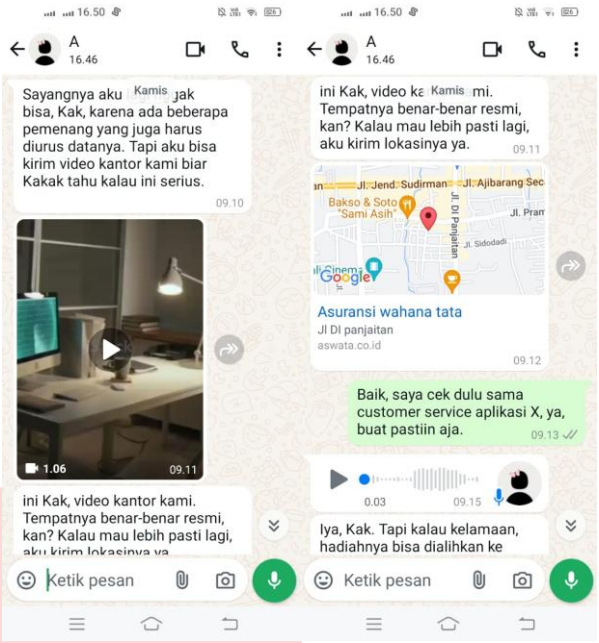
## IV. HASIL DAN PEMBAHASAN

a) Pembuatan Skenario

Skenario telah disusun dengan rinci untuk merencanakan berbagai aktivitas kejahatan digital yang kemungkinan terjadi. Skenario aktivitas kejahatan yang saya buat yaitu Penipuan undian berhadiah dari sebuah aplikasi. Skenario ini mencakup berbagai Tindakan seperti menelpon, membuat dokumen, merekam suara, menghasilkan gambar dan video untuk meyakinkan korban lalu menghapus percakapan.




*Gambar 4. 1 Percakapan memlibatkan gambar dan dokumen*



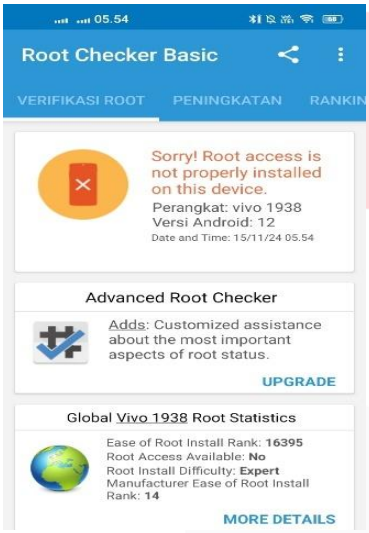

*Gambar 4. 2 Percakapan melibatkan Rekaman video dan audio*


*Gambar 4. 3 Percakapan yang melibatkan Voice note dan panggilan*

b) *Perservation*

Preservation adalah bagian penting dalam forensik digital yang berfokus pada pengumpulan, pelestarian, dan dokumentasi bukti digital dari perangkat, seperti smartphone, untuk mencegah perubahan data. Dalam kasus ini, perangkat yang menjadi objek penelitian adalah Vivo Y30, yang digunakan untuk mensimulasikan skenario penipuan melalui aplikasi pesan instan WhatsApp. Dalam tahapan ini, perangkat Vivo Y30 dibiarkan dalam kondisi normal, tanpa *root*, untuk memastikan data tetap autentik smartphone akan dicek melalui aplikasi *Root checker*.

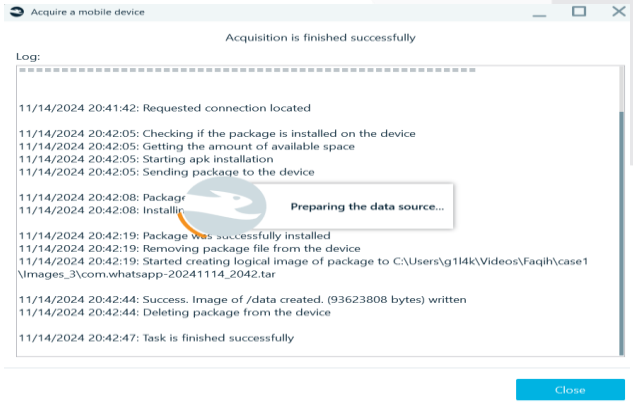

*Gambar 4. 4 Smartphone yang dijadikan bukti*



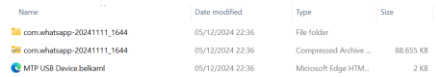

*Gambar 4. 5 Smartphone dalam keadaan Unroot*

c) Acquisition

Pada tahap *Acquisition*, proses imaging dan ekstraksi data dari smartphone ke komputer dilakukan dengan bantuan perangkat lunak forensik Belkasoft X. Dalam metode ini, *Android Debug Bridge* (*ADB*) digunakan untuk memungkinkan akses ke filesystem tanpa harus membuka perangkat secara fisik. ADB juga memungkinkan penggunaan perintah *shell command* untuk mendapatkan data secara mendalam.



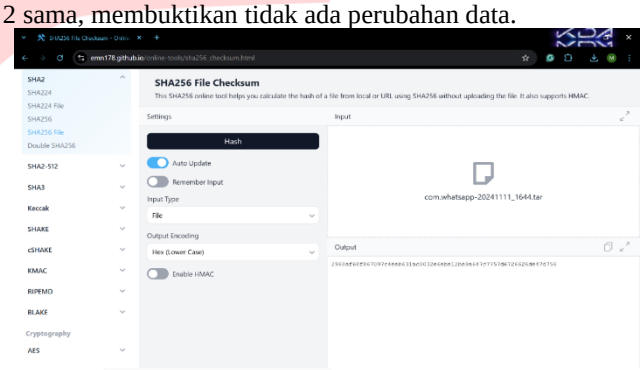

*Gambar 4. 6 proses image data telah berhasil*



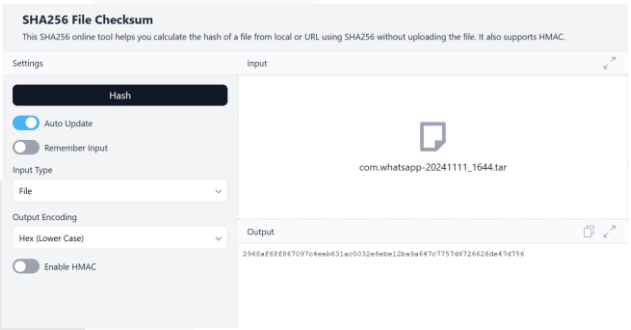

*Gambar 4. 7 Hasil image data telah berhasil*

d) Examination & Analysis

Tahap *Examination & analysis* membuka hasil export data yang sudah dikumpulkan pada tahapan *Acquisition*, Hasil *Acquisition* Data ini kemudian akan diuji pada kedua *tools forensic* berdasarkan parameter penilaian. Sebelum data diuji akan dilakukan pengecekan dengan proses hashing. Proses hashing dilakukan untuk memastikan hasil *image forensic* tidak mengalami perubahan. Pengecekan dilakukan melalui website emn178.github.io/online-tools. Hasil hasing berupa kode SHA2, tergantung opsi pada tools yang digunakan dan akan di lakukan *matching* antara PC 1 dan PC 2. Gambar 4.8 menunjukan hasil hashing antara PC 1 dan PC 2 sama, membuktikan tidak ada perubahan data.

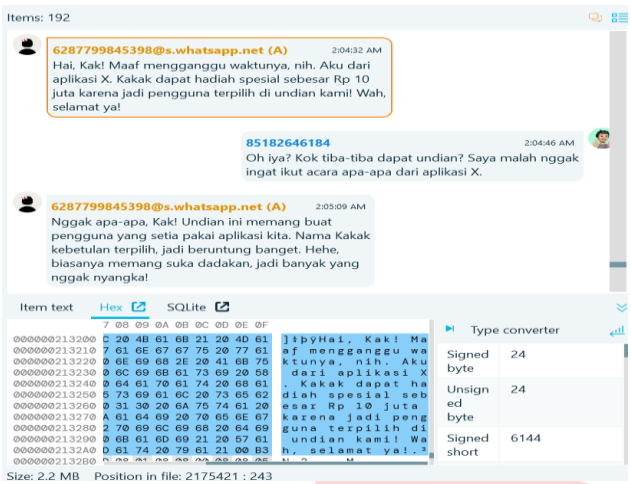



*Gambar 4. 8 kode hash pc 1*

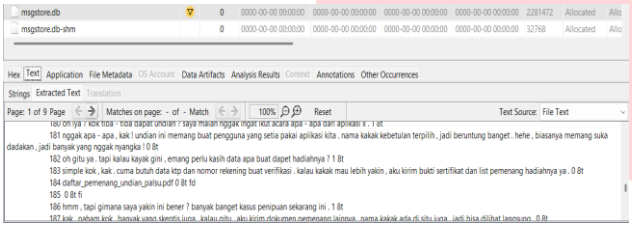



*Gambar 4. 9 hasil kode hash pc 2*

Pada hasil *export* data ditemukan beberapa ditemukan bukti percakapan whatsapp pada kedua aplikasi tersebut yang tersimpan di database whatsapp mgstore.db. hasil percakapan whatsapp pada Gambar 4.10 dan 4.11.



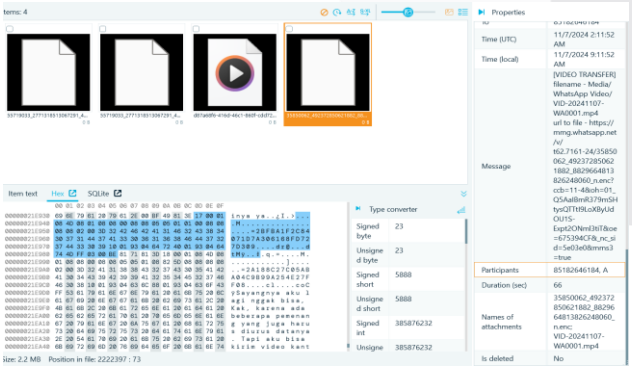

*Gambar 4. 10 Percakapan text pada Belkasoft*



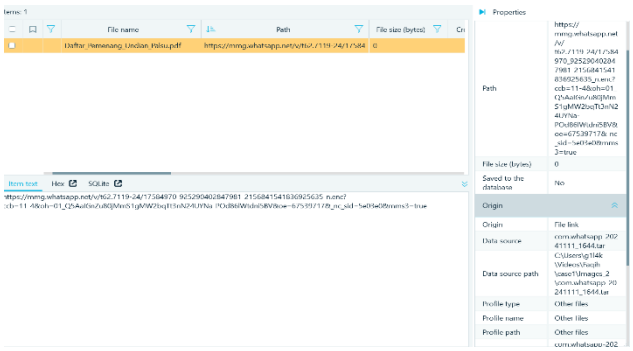

*Gambar 4. 11 Peercakapan text pada autopsy*

Ditemukan bukti berupa: gambar, video, audio, lokasi gps dan dokumen pdf yang dikirimkan oleh pelaku untuk meyakinkan korban. Bukti terdapat pada gambar dibawah.

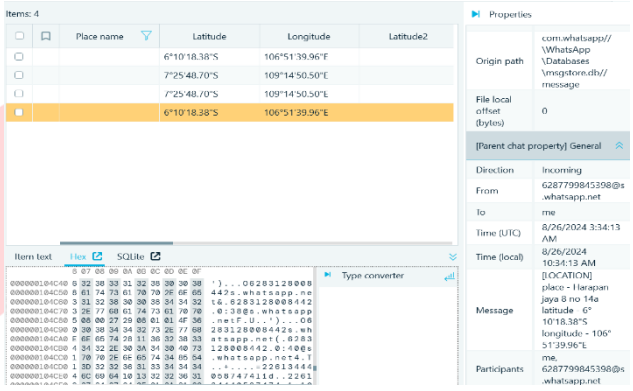

*Gambar 4. 12 Bukti foto sertifikat palsu di belkasoft*



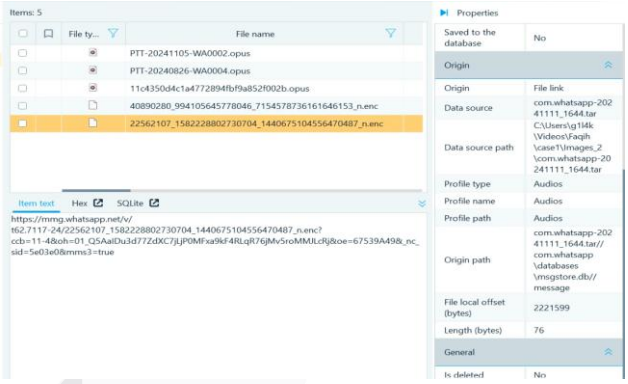

*Gambar 4. 13 Bukti Video terkirim di belkasoft*




*Gambar 4. 14 Bukti dokumen pdf terkirim di belkasoft*

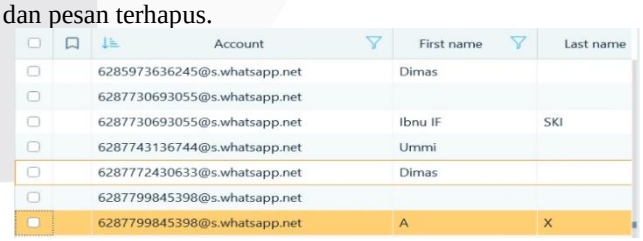



*Gambar 4. 15 Bukti Lokasi terkirim belkasoft*



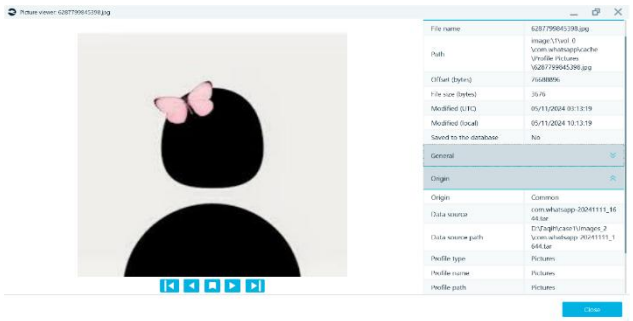

*Gambar 4. 16 voice note ditemukan di belkasoft*

Ditemukan kontak pelaku, foto profile, Riwayat penggilan dan pesan terhapus.

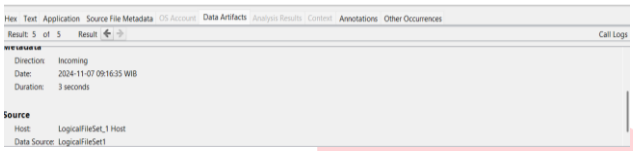



*Gambar 4. 17 Menemukan kontak di belkasoft*

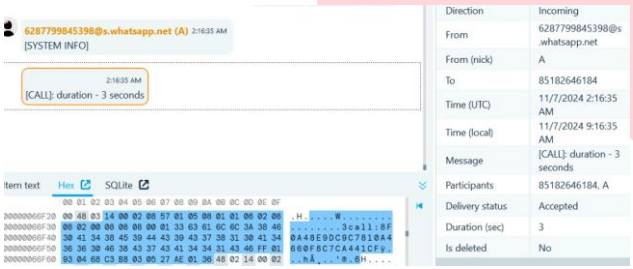

*Gambar 4. 18 Menemukan kontak pelaku di autopsy*



*Gambar 4. 19 foto profile di belkasoft*



*Gambar 4. 20 Riwayat panggilan di autopsy*



*Gambar 4. 21 Riwayat panggilan belkasoft*

Untuk pesan yang terhapus pada gambar 4.22 dibawah. dibandingkan dengan chat yang tidak terhapus, pada hex dump hanya ada kode ID dan tidak diikuti isi *chat*. Membuktikan bahwa isi *chat* benar - benar hilang dan tidak bisa di pulihkan, ini berarti belkasoft hanya bisa menemukan indikasi chat yang terhapus tetapi tidak bisa merecovery isi dari percakapan yang terhapus.


*Gambar 4. 22 bukti percakapan terhapus di belkasoft*

e) Reporting

Tahap akhir dalam penelitian ini adalah reporting, yaitu menyusun hasil dari proses examination dan analysis yang dilakukan menggunakan tools Belkasoft dan Autopsy. Tahapan ini bertujuan untuk mengevaluasi kinerja kedua tools berdasarkan kemampuan mereka dalam mengidentifikasi dan menganalisis data. Penilaian kinerja dilakukan menggunakan parameter tertentu yang relevan dengan konteks investigasi digital.

Parameter yang digunakan untuk menilai kinerja tools dalam proses investigasi digital dirangkum dalam Tabel 4.1 berikut:

| No | Parameter | Belkasoft | Autopsy |
|---|---|---|---|
| 1 | Pesan *text* | ✓ | ✓ |
| 2 | *Voice note* | ✓ | × |
| 3 | Pesan gambar | ✓ | × |
| 4 | Histori panggilan | ✓ | ✓ |
| 5 | Kontak | ✓ | ✓ |
| 6 | Whatsapp log | ✓ | × |
| 7 | Pesan terhapus | × | × |
| 8 | Dokumen | ✓ | × |
| 9 | Lokasi GPS | ✓ | × |
| 10 | Database | ✓ | ✓ |
| 11 | Foto profile | ✓ | ✓ |

Berdasarkan parameter penilaian, maka kinerja kedua *tools* dapat diukur dengan menggunakan rumus agregat :

Belkasoft $X\ (I_A) = \frac{10}{11}$ x $100\% = 90{,}91\%$ Tingkat keberhasilan

Autopy $(I)_{A)} = \frac{6}{11}$ x $100\% = 54{,}55\%$ Tingkat keberhasilan

Hasil perhitungan tersebut menunjukkan Tingkat akurasi kinerja tools Belkasoft X sebesar 90,91% lebih akurat dari Autopsy sebesar 54,55%. Dapat disimpulkan berdasarkan hasil indeks Agregat kinerja Belkasoft X lebih baik dalam menginvestigasi evident case pada whatsapp dibandingkan dengan Autopsy.

## V. KESIMPULAN

Belkasoft X terbukti memiliki kinerja yang lebih unggul dibandingkan Autopsy, dengan tingkat akurasi 90,91% dalam mengidentifikasi dan menganalisis bukti digital, termasuk pesan teks, pesan suara, gambar, video, dokumen, lokasi GPS, dan pesan terhapus yang berasal dari platform WhatsApp. Sebaliknya, Autopsy hanya mampu mengidentifikasi sebagian bukti dengan akurasi 54,55%, terbatas pada analisis pesan teks, kontak, histori panggilan, database, dan foto profil. Oleh karena itu, Belkasoft X

## REFERENSI


[1] N. Setiawan, "Kasus Kejahatan Siber Pada Telepon Seluler Android," *Cyber Secur. dan Forensik Digit.*, vol. 2, no. 1, pp. 24–29, 2019, doi: 10.14421/csecurity.2019.2.1.1420.

[2] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.

[3] I. Z. Yadi and Y. N. Kunang, "Analisis forensik pada platform android," *Konf. Nas. Ilmu Komput.*, pp.

141–148, 2014, [Online]. Available: http://eprints.binadarma.ac.id/2191/

[4] *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Indonesia, 2008.

[5] D. N. P. Sari, "Analisis Digital Forensik Perilaku Plagiarisme Pembuatan Makalah Mahasiswa Kurikulum dan Teknologi Pendidikan Angkatan 2018 Menggunakan SmallSEOTool.," p. 70, 2020.

[6] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *J. Media Inform. Budidarma*, vol. 6, no. 2, p. 1263, 2022, doi: 10.30865/mib.v6i2.3946.

[7] D. R. Rahadi, "Perilaku Pengguna Dan Informasi Hoax Di Media Sosial," *J. Manaj. Dan Kewirausahaan*, vol. 5, no. 1, pp. 58–70, 2017, doi: 10.26905/jmdk.v5i1.1342.

[8] E. Casey, *Digital Evidence and Computer Crime*. 2011. doi: 10.4018/978-1-59904-379-1.ch015.

[9] G. F. Mandias, "Analisis Pengaruh Pemanfaatan Smartphone Terhadap Prestasi Akademik Mahasiswa Fakultas Ilmu Komputer Universitas Klabat," *CogITo Smart J.*, vol. 3, no. 1, pp. 83–90, 2017, doi: 10.31154/cogito.v3i1.47.83-90.

[10] F. Ikrar Gama Raditya, "Architecture of android," Binus University. Accessed: Jan. 15, 2024. [Online]. Available: https://sis.binus.ac.id/2022/04/18/architecture-of-android/#:~:text=Arsitektur Android adalah lapisan komponen,Android Framework

[11] A. Karhendana, "Keamanan pada Layanan Instant Messaging : Studi Kasus Yahoo Messenger , Windows Live Messenger , dan Google Talk," *J. Inform.*, 2006.

[12] N. Hannani, "Pengertian WhatsApp Beserta Sejarah, Manfaat, Kelebihan dan Kekurangan WhatsApp," Nesabamedia. [Online]. Available: https://www.nesabamedia.com/pengertian-whatsapp/

[13] "Belkasoft evidence center x," Belkasoft. [Online]. Available: https://belkasoft.com/x

[14] "Autopsy Digital Forensics Software," BasisTech. [Online]. Available: https://www.basistech.com/autopsy/