JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 2, Juni 2025, Pp. 1099-1110

PENGEMBANGAN ALAT FORENSIK *WHATSAPP* MENGGUNAKAN ANDROID DEBUG BRIDGE SEBAGAI METODE AKUISISI DATA

Muammar[1)], Imam Riadi*[2)], Rusydi Umar[3)]
1. Universitas Ahmad Dahlan, Yogyakarta, Indonesia
2. Universitas Ahmad Dahlan, Yogyakarta, Indonesia
3. Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Article Info
Kata Kunci: ADB (Android Debug Bridge); Cybercrime; Forensik Digital; Forensics Tools; *WhatsApp*

Keywords: ADB (Android Debug Bridge); Cybercrime; Digital Forensic; Forensics Tools; *WhatsApp*

Article history:
Received 24 Oktober 2024
Revised 19 November 2024
Accepted 28 Desember 2024
Available online 15 March 2025

DOI :
https://doi.org/10.29100/jipi.v10i2.5968

* Corresponding author.
Corresponding Author
E-mail address:
2307048012@webmail.uad.ac.id

ABSTRAK
WhatsApp adalah aplikasi pesan instan yang banyak digunakan yang, selain memudahkan komunikasi, juga menjadi sarana untuk aktivitas kriminal. Oleh karena itu, dibutuhkan alat forensik khusus yang dirancang untuk *WhatsApp* pada smartphone Android untuk menghasilkan bukti digital yang kuat untuk kasus pengadilan. Alat ini dikembangkan melalui proses yang meliputi analisis, desain, pengkodean, pengujian, dan pemeliharaan. Dengan memanfaatkan *Android Debug Bridge* (ADB), aplikasi yang dihasilkan dapat mengakses data forensik penting seperti kunci enkripsi, database msgstore.db yang terenkripsi (versi *crypt12* dan *crypt14*), dan berbagai file media *WhatsApp* seperti audio, video, gambar, catatan suara, dan data stiker. Setelah diuji coba pada sembilan merek *smartphone* yang berbeda, aplikasi ini mencapai tingkat keberhasilan 80%, menunjukkan efektivitasnya sebagai peningkatan yang signifikan dalam alat forensik digital untuk perangkat *Android*. Alat ini memberikan para analis forensik sarana yang kuat untuk memperoleh dan menangani bukti digital dalam kasus tertentu, khususnya meningkatkan kemampuan pemeriksa forensik digital mobile.

ABSTRACT
WhatsApp is a widely used instant messaging app that, while facilitating communication, also becomes a medium for criminal activities. Consequently, there is a need for a specialized forensic tool tailored for *WhatsApp* on Android smartphones to generate strong digital evidence for court cases. This tool is developed through a process that includes analysis, design, coding, testing, and maintenance. Utilizing Android Debug Bridge (ADB), the resulting application can access essential forensic data like encryption keys, encrypted msgstore.db databases (crypt12 and crypt14 versions), and various *WhatsApp* media files such as audio, video, images, voice notes, and sticker data. Upon testing the application across nine different smartphone brands, it achieved an 80% success rate, indicating its efficacy as a significant enhancement in digital forensic tools for Android devices. This tool provides forensic analysts with a powerful means to acquire and handle digital evidence in specific cases, particularly enhancing the capabilities of mobile digital forensic examiners

.

I. PENDAHULUAN

Perkembangan teknologi dan informasi sangatlah cepat, salah satunya adalah perkembangan teknologi *smartphone Android* ditandai dengan banyaknya media sosial dan aplikasi pesan instan yang bermunculan. aplikasi pesan instan *WhatsApp* banyak sekali digunakan untuk berinteraksi sebagai alat komunikasi. Menurut data [1] pada april 2024, *WhatsApp* memiliki 2 miliar lebih pengguna aktif bulanan, jumlah tersebut naik lebih dari 1 miliar terhitung dari 2016. Seiring bertambahnya pengguna *WhatsApp*, secara otomatis aktivitas kriminal yang berkaitan dengan platform ini juga mengalami peningkatan [2]. Menurut penelitian yang dilakukan oleh [3], peningkatan aktivitas pengguna internet media sosial telah menyebabkan peningkatan angka penipuan. Data dari Direktorat Tindak Pidana Siber Bareskrim Polri yang dipublikasikan di situs Patroli Siber menunjukkan bahwa sepanjang tahun 2021 (Januari hingga Desember), terdapat 12.197 laporan kejahatan dari masyarakat. Dari jumlah tersebut, penipuan/fraud menjadi kejahatan yang paling banyak dilaporkan dengan 7.124 laporan. Platform yang

paling sering digunakan untuk melakukan penipuan adalah Whatsapp, dengan 4.888 laporan. Data dari Januari hingga Maret 2021 juga menunjukkan tren yang sama, dengan penipuan/fraud sebagai kejahatan yang paling banyak dilaporkan sebanyak 2.145 dari total 4.453 laporan, dan Whatsapp sebagai platform yang paling banyak digunakan dengan 2.062 laporan. *WhatsApp* dikenal sebagai alat komunikasi tindak kejahatan menurut [3][4][5] pada penelitiannya menjelaskan, banyak oknum yang menyalahgunakan teknologi digital untuk melakukan berbagai kejahatan seperti penipuan, pornografi, korupsi, perjudian ilegal, dan kegiatan jaringan narkoba. Para pelaku kejahatan biasanya memanfaatkan aplikasi pesan instan tersebut sebagai sarana untuk berinteraksi dengan sesama rekan penjahat maupun korban [6]. Menurut [7] pada penelitiannya menjelaskan *WhatsApp* adalah aplikasi pengiriman pesan yang mengimplementasikan enkripsi *end-to-end*, yang memastikan bahwa hanya pengirim dan penerima yang bisa melihat isi pesan. Fitur keamanan ini yang menjadi penyebab, meskipun dirancang untuk melindungi privasi pengguna, sering disalahgunakan oleh individu yang tidak bertanggung jawb untuk kegiatan kriminal. Database *WhatsApp* sendiri dilindungi dengan enkripsi menggunakan format *crypt12*. Jika barang buktinya adalah *smartphone android*, menurut [8][9] Dalam konteks forensik digital, *WhatsApp* dapat digunakan sebagai barang bukti digital dalam persidangan. Upaya untuk mendapatkan barang bukti tersebut melibatkan proses forensik digital yang bertujuan mengumpulkan bukti digital yang sah dan ilmiah untuk membuktikan tindak kejahatan.

Forensik digital adalah bidang pengetahuan yang diterapkan untuk keperluan penyelidikan hukum, dimana tujuannya adalah untuk secara ilmiah mengumpulkan bukti digital yang sah untuk membuktikan tindak kejahatan komputer [10][11]. Laboratorium *Digital Forensics Center* (DFC) Universitas Muhammadiyah Purwokerto (UMP) merupakan salah satu institusi yang bergerak dibidang forensik digital. Laboratorium DFC UMP mengalami kesulitan dalam melakukan analisis forensik pada instan massangger dengan keterbatasan alat atau software yang ada, khususnya analisa pada aplikasi *WhatsApp* dalam mengungkap suatu kasus siber pada smartphone android. Kesulitan yang dialami yaitu alat atau software yang digunakan tidak berfokus pada satu aplikasi sehingga membutuhkan waktu yang lama dalam mengambil data *WhatsApp*.

Berdasarkan permasalahan ini, diperlukan pengembangan alat (*Software*) forensik khusus *WhatsApp* dari sebuah perangkat *Android*, yang dapat melakukan akuisisi data *WhatsApp* sehingga dapat mempermudah analisa kasus siber di laboratorium DFC UMP sebagai barang bukti digital yang dapat dipertanggung jawabkan dipersidangan. Dilihat dari penelitian sebelumnya oleh [4] dilakukan sebuah analisis forensik menggunakan metode DFRWS dengan tools MOBILedit Forensic Express dan Hashmyfiles didapatkan hasil kinerja *tools MOBILedit Forensic Express* mempunyai kemampuan akurasi sebesar 84,6%. Sedangkan kemampuan deteksi *HashMyFiles* dapat mendeteksi sebesar 100%. Analisis forensik sebelumnya yang dilakukan [12] dengan *tools Belkasoft Evidence Center*, dan *HashMyfiles* dengan metode ACPO (*Association of Chief Police Officer*) menghasilkan perbandingan kinerja *tools* yang menunjukkan akurasi *tools*, *Belkasoft Evidence Center* sebesar 81,92%, sedangkan *Hashmyfiles* memiliki akurasi sebesar 79,69%. Menunjukkan bahwa hasil yang didapatkan oleh alat forensik berlicensi tidak 100% sempurna, sehingga perlu adanya perancangan alat forensik baru buatan anak bangsa yang dapat bersaing dengan alat forensik lainnya.

Dibutuhkannya Perancangan atau rancang bangun yang menurut [13][14] adalah serangkaian langkah untuk mengubah hasil analisis suatu sistem menjadi kode pemrograman yang merinci implementasi komponen-komponen sistem. Dalam pembangunan *software* dapat memanfaatkan *Android Debugging Bridge (ADB)* untuk mengekstrak data hanya dengan menghubungkan perangkat melalui USB [15]. Metode tersebut dikembangkan menjadi strategi analisis forensik yang umum dengan menggunakan *ADB*[16]. *Android Debug Bridge* adalah bagian dari *Android* SDK, yang mengidentifikasi lokasi, dan nama file. *AndroidDebug Bridge* (ADB) adalah alat baris perintah serbaguna [12][17]. Bahasa pemrograman yang digunakan yaitu *Python*, *Python* merupakan bahasa pemograman untuk jenis pengembangan perangkat lunak. Phyton sangat dikenal dalam bidang pembelajaran mesin, robotika, kecerdasan buatan, dan ilmu data yang merupakan teknologi terkemuka saat [18]. Keunggulan *Python* dalam teknologi ini menjadikannya pilihan utama dalam pengembangan alat forensik *WhatsApp*, memastikan bahwa alat yang dikembangkan tidak hanya efektif tetapi juga mampu beradaptasi dengan kebutuhan teknologi masa kini.

Alat ini memiliki keunggulan unik sebagai alat forensik khusus *WhatsApp* yang mampu mengambil data serta melihat percakapan secara langsung berdasarkan waktu. Selain itu, alat ini juga memungkinkan akses ke media, baik yang tersimpan maupun yang hanya dapat dilihat sekali dalam satu platform, yang merupakan keunggulan dibanding alat forensik lainnya yang biasanya di bedakan platformnya antara akuisisi data dan view data. Dengan ini diharapkan laboratorium *Digital Forensics Center* UMP dapat mengatasi lamanya proses investigasi, memungkinkan pengumpulan dan analisis data lebih cepat dan dapat diandalkan dalam proses penyelidikan forensik digital sehingga dapat meningkatkan efisiensi dan efektivitas proses investigasi bukti digital yang dapat dipertanggungjawabkan secara ilmiah dan hukum di persidangan.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 2, Juni 2025, Pp. 1099-1110

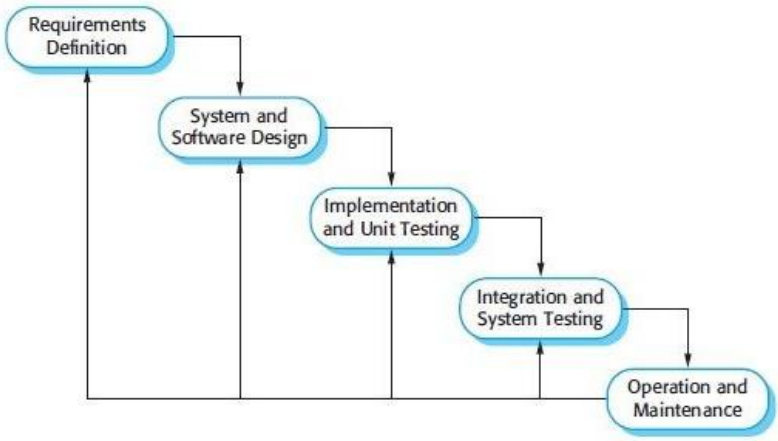
II. METODOLOGI PENELITIAN

Metodologi penelitian adalah rangkaian langkah-langkah, peraturan, dan prosedur yang dipergunakan oleh para peneliti di suatu disiplin ilmu khusus. Dalam konteks penelitian ini, metode *waterfall* diterapkan sebagai pendekatan yang terstruktur dan berurutan, yang umumnya dimanfaatkan dalam pengembangan perangkat lunak serta sistem informasi. Metode ini terdiri dari beberapa tahap yang terstruktur dan terdefinisi dengan baik, seperti analisis kebutuhan, desain sistem, implementasi, pengujian, dan pemeliharaan. Setiap tahap harus diselesaikan sebelum melanjutkan ke tahap berikutnya, memastikan setiap aspek proyek ditangani dengan cermat dan terorganisir. Metode pengembangan perangkat lunak waterfall dipilih dibandingkan metode Agile atau Scrum karena pendekatannya yang linear dan berurutan sangat cocok dengan kebutuhan proses forensik digital yang membutuhkan dokumentasi dan validasi yang ketat di setiap tahap. Waterfall memungkinkan setiap fase pengembangan untuk diselesaikan sepenuhnya sebelum melanjutkan ke fase berikutnya, memastikan bahwa setiap langkah sesuai dengan standar ilmiah dan SNI ISO/IEC 17025:2017. Ini memberikan keuntungan spesifik dalam konteks pengembangan alat forensik, yaitu memastikan bahwa setiap aspek dari perangkat lunak telah melalui proses verifikasi dan validasi yang teliti, mengurangi risiko kesalahan atau inkonsistensi yang dapat mempengaruhi hasil analisis forensik. Selain itu, dokumentasi yang mendetail pada setiap tahap pengembangan mempermudah audit dan memberikan jejak bukti yang jelas, yang sangat penting dalam lingkungan forensik yang menuntut akurasi dan kepatuhan terhadap standar yang tinggi.

A. Tahapan Penelitian

Penelitian yang akan dilakukan untuk mengembangkan aplikasi alat forensik *WhatsApp* pada *smartphone* Android dengan memanfaatkan *Android Debug Bridge* (ADB) memiliki beberapa tahapan untuk melakukan pembuatan. Tahap pertama yaitu melakukan studi pustaka dilakukan dengan membaca studi literatur maupun jurnal-jurnal, wawancara dan observasi langsung, kemudian merancang kebutuhan dan merancang desain aplikasi dengan menggunakan model pengembangan perangkat lunak *waterfall*.

Studi ini menerapkan metode *waterfall* yang bersifat berurutan [19][20]. Ada 5 tahap yang dilakukan dalam metode *waterfall*, yaitu: analisis kebutuhan, desain, implementasi, pengujian, dan pemeliharaan sistem [21]. Sebagaimana dipaparkan dan dijelaskan pada gambar 1 dibawah.



Gambar 1. Model pengembangan perangkat lunak waterfall

1) Requirement

Pada tahap ini, dilakukan analisis untuk mengetahui kebutuhan sistem secara menyeluruh. Proses ini melibatkan identifikasi masalah yang ada dan pencarian solusi yang dapat diimplementasikan untuk mengatasi masalah tersebut. Data dikumpulkan melalui proses pengumpulan data dengan melakukan wawancara terhadap kapala laboratorium DFC UMP dan staf pemeriksa forensik digital (investigator) yang bertugas serta melakukan observasi langsung dengan ikut andil menjadi seorang pemeriksa forensik digital di Labaratorium DFC UMP, mengamati setiap proses dari analisis hingga pelaporan data. Informasi yang diperoleh dari tahap ini dikumpulkan dan didkomuntasikan sehingga dapat menjadi dasar untuk menentukan spesifikasi teknis dan fungsional dari alat forensik *WhatsApp* yang akan dikembangkan. Banyaknya sample test sebanyak 9 unit *smartphone android* dengan merek yang berbeda, dengan data random tanpa rekayasa yang ada dismartphone tersebut sehingga dapat diuji sejauh mana alat ini dapat mengakuisisi data pada *WhatsApp* di *smartphone android*.

2) Design

Setelah kebutuhan sistem teridentifikasi, tahap berikutnya adalah memodelkan kebutuhan tersebut menggunakan unified modeling language (UML). *Flowchart diagram activity* digunakan untuk mendefinisikan fungsi-fungsi sistem secara rinci. Desain ini mencakup alur kerja aplikasi, struktur data, dan antarmuka pengguna. Tujuannya adalah untuk memastikan bahwa semua aspek dari sistem telah dipertimbangkan dan direncanakan dengan baik sebelum memulai tahap implementasi.

3) Implementation

Pada tahap ini, aplikasi dibuat berdasarkan desain yang telah dibuat pada tahap sebelumnya. Pengembangan dilakukan menggunakan bahasa pemrograman *Python*, yang dipilih karena fleksibilitas dan kemampuannya dalam mengelola tugas-tugas yang kompleks dalam pengembangan perangkat lunak. Implementasi melibatkan penulisan kode, pembuatan antarmuka pengguna, dan integrasi fungsi-fungsi yang telah dirancang.

4) Testing

Tahap ini merupakan pengujian sistem yang telah dibangun. Fungsi-fungsi sistem diuji untuk memastikan bahwa semuanya berjalan sesuai dengan spesifikasi yang telah ditentukan. Pengujian dilakukan menggunakan metode *Blackbox Testing*. *Blackbox Testing* adalah metode pengujian perangkat lunak yang berfokus pada fungsi-fungsi eksternal dari aplikasi tanpa memperhatikan struktur internal atau kode sumbernya. Dalam *Blackbox Testing*, penguji mengevaluasi input dan output dari perangkat lunak berdasarkan spesifikasi yang telah ditetapkan untuk memastikan bahwa aplikasi berjalan sesuai dengan yang diharapkan. Skenario pengujian yang dilakukan mencakup validasi fungsi utama aplikasi, uji batas (boundary testing), uji masukan valid dan tidak valid (valid and invalid input testing), serta uji integrasi antar komponen. Penanganan kesalahan diidentifikasi dengan cara memeriksa output yang tidak sesuai dengan ketentuan, kemudian dibuat laporan untuk dianalisis dan diperbaiki. Proses perbaikan melibatkan pemrograman ulang atau penyesuaian modul yang bermasalah sebelum pengujian ulang dilakukan untuk memastikan kesalahan telah diperbaiki. Selain *Blackbox Testing*, jenis pengujian lain yang sering dilakukan adalah *Whitebox Testing*, yang menguji struktur internal aplikasi, dan *Greybox Testing*, yang menggabungkan aspek-aspek dari *Blackbox* dan *Whitebox Testing* untuk memberikan pandangan yang lebih menyeluruh tentang kualitas dan kinerja perangkat lunak. Urgensi memilih *Blackbox Testing* dalam pengembangan alat forensik digital karena *Blackbox Testing* fokus pada validasi fungsionalitas perangkat lunak sesuai dengan spesifikasi pengguna, memastikan alat dapat digunakan dengan benar tanpa memerlukan pengetahuan mendalam tentang kode internal sehingga lebih efisien dalam hal waktu dan sumber daya, serta memungkinkan pengujian dilakukan oleh individu yang tidak terlibat dalam pengembangan, memberikan perspektif objektif dan mengidentifikasi bug yang mungkin terlewat oleh pengembang.

5) Maintenance

Pada tahap ini, sistem yang telah dibuat dipelihara untuk memastikan operasional yang berkelanjutan dan perbaikan jika diperlukan. Jika ditemukan kekurangan atau ada penambahan fungsi yang diperlukan setelah implementasi, perbaikan akan dilakukan. Pemeliharaan lebih lanjut juga akan dilakukan berdasarkan umpan balik dari pengguna dan temuan selama penggunaan aplikasi. Tujuannya adalah untuk memastikan bahwa aplikasi tetap efektif dan sesuai dengan perkembangan kebutuhan di masa mendatang.

III. HASIL DAN PEMBAHASAN

Dalam era digital saat ini, aplikasi pesan instan seperti *WhatsApp* telah menjadi salah satu alat komunikasi yang paling diminati dan digunakan secara meluas di berbagai penjuru dunia.. Penggunaan *WhatsApp* yang meluas ini tidak hanya membawa manfaat dalam komunikasi sehari-hari, tetapi juga menimbulkan tantangan baru dalam bidang forensik digital. Penelitian ini berfokus pada pengembangan alat forensik yang dapat membantu dalam proses akuisisi data dari aplikasi *WhatsApp* menggunakan *Android Debug Bridge* (ADB). Dengan memanfaatkan ADB sebagai metode akuisisi data, penelitian ini bertujuan untuk menyediakan solusi yang efisien dan efektif bagi praktisi forensik dalam mengumpulkan dan menganalisis bukti digital yang relevan dari perangkat *Android*.

Penelitian ini menggunakan pendekatan metode waterfall dalam pengembangan alat forensik tersebut. Metode waterfall melibatkan tahapan yang terstruktur dan berurutan, dimulai dari tahap analisis kebutuhan, desain sistem, implementasi, pengujian, hingga pemeliharaan. Dalam konteks penelitian ini, tahap analisis kebutuhan melibatkan identifikasi spesifikasi teknis dan fungsional yang diperlukan untuk akuisisi data *WhatsApp*. Tahap desain sistem mencakup perancangan arsitektur alat forensik dan alur kerja akuisisi data. Selanjutnya, tahap implementasi berfokus pada pengkodean dan pengembangan perangkat lunak yang mendukung akuisisi data melalui ADB. Pengujian dilakukan untuk memastikan alat yang dikembangkan bekerja sesuai dengan spesifikasi yang diharapkan, dan tahap pemeliharaan melibatkan perbaikan dan pembaruan alat berdasarkan umpan balik dan temuan selama pengujian.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 2, Juni 2025, Pp. 1099-1110

Pada bagian pembahasan ini akan merinci langkah-langkah teknis dari setiap tahap metode *waterfall*, analisis data yang dikumpulkan, serta evaluasi efektivitas alat yang dikembangkan dalam konteks penyelidikan forensik sebagai berikut.

A. Requirment

Sebelum melakukan pembangunan, pengembang melakukan komunikasi langsung kepada pemeriksa forensik digital yang ada di *Digital Forensics Center* UMP dan melakukan observasi langsung dengan ikut andil menjadi seorang pemeriksa forensik digital. Informasi yang didapatkan dianalisis untuk mendapatkan data yang dibutuhkan. Setelah melakukan analisis didapatkan kebutuhan yang diperlukan dalam membuat alat forensik *WhatsApp* yang disajikan dalam tabel 1 dibawah ini.

TABEL 1.
KEBUTUHAN FUNGSIONALITAS SISTEM

No	Fungsi	Deskripsi
1	Koneksi	Koneksi data smartphone dan Komputer
2	Akuisisi data	Pengambilan database *WhatsApp*, media dan key
3	Decrypt	Membuka enkripsi database
4	viewer	View chat dan media

Dari hasil analisis dibutuhkan juga *device unit test* berupa *smartphone android* dengan ketentuan dan spesifikasi yang beragam sebagai bahan pengujian alat forensik yang dibangun, yang dimana disekenariokan unit test tersebut akan dilakukan akuisisi data aplikasi *WhatsApp* menggunakan alat forensik *WhatsApp* yang dibangun, terdapat total 9 unit *smartphone android* dengan merek yang berbeda sehingga dapat dilakukan pengujian *sample* yang handal, sebagai mana disajikan *unit test* pada tabel 2.

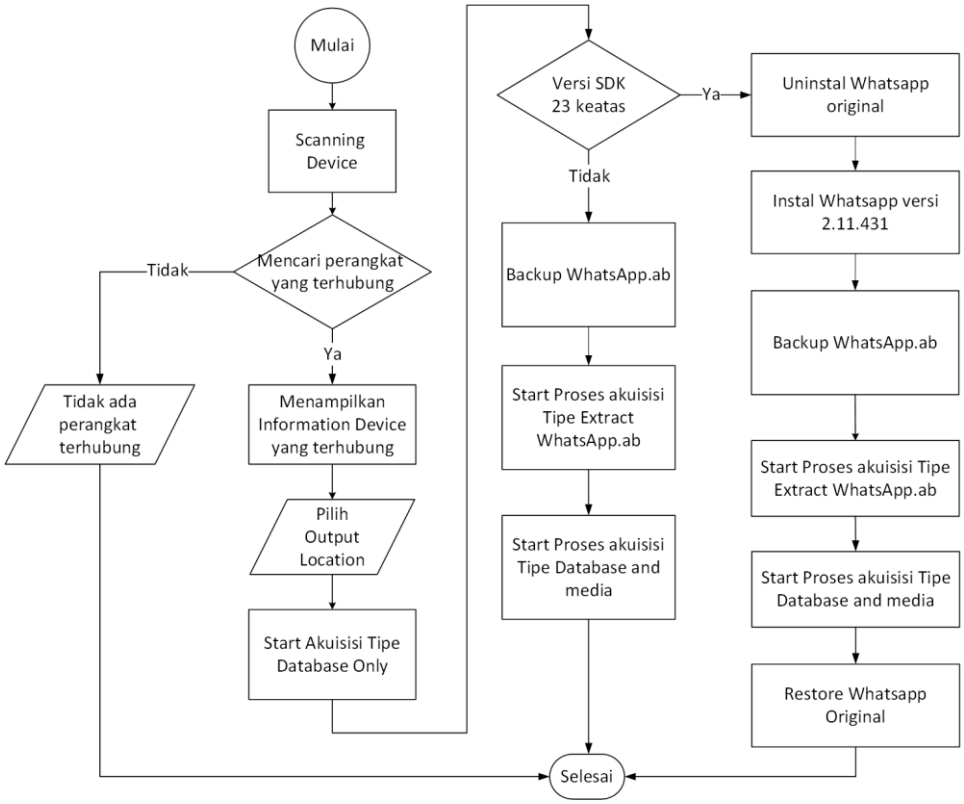
TABEL 2.
UNIT TEST

No	Merek *Smartphone*	*OS Android*	*Storage*
1.	Xiaomi Readmi Not 4x	7.0 nougat	3/32 Gb
2.	Samsung galaxy Y Grand	4.4 lollipop	500 mb/ 4Gb
3.	Vivo Y35	7.0 nougat	3/32 Gb
4.	Lenovo A6000+	7.0 nougat	3/32 Gb
5.	Xioami Readmi Not 8 Pro	10 Q	6/128
6.	Oppo A7	8.1 Oreo	4/64 Gb
7.	Asus zenfone 4 max Pro	8.1 Oreo	3/32 Gb
8.	Xioami Readmi Not 10	*Android* 11	4/64 Gb
9.	Samsung A20	*Android* 11	4/64 Gb

B. Design

Perencanaan desain serta sistem perangkat lunak merupakan aspek krusial dalam pembangunan aplikasi, karena perencanaan yang matang dapat meningkatkan efisiensi dan mempercepat proses pengembangan. Dalam konteks pembangunan aplikasi ini, perencanaan yang teliti mencakup penentuan kebutuhan fungsional dan non-fungsional, yang kemudian dituangkan dalam bentuk desain *flowchart*. Desain *flowchart*, seperti yang ditunjukkan pada Gambar 2 dibawah, menggambarkan alur kerja yang sistematis dan terstruktur, memandu pengembang dalam setiap tahap proses pengembangan. Dengan alur kerja yang jelas, setiap komponen aplikasi dapat diidentifikasi dan diimplementasikan secara tepat, memastikan integrasi yang lancar dan fungsi yang optimal dari aplikasi forensik *WhatsApp* yang dibangun.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 2, Juni 2025, Pp. 1099-1110



Gambar 2. Flowchart rancangan alur kerja aplikasi

Alat forensik *WhatsApp* ini direncanakan dapat berjalan pada *Operating system*(OS) *windows* dan *linux*, minimum requirement *smartphone* mulai dari *Android* Versi 4.4 (*KitKat*) dan SDK *Version* 19 keatas. Aplikasi alat forensik ini dapat melakukan *scanning device* yang terhubung dengan menampilkan informasi *device*, yang kemudian jika sesuai dengan requirement dapat dilakukan akuisisi data, baik database maupun media pada *WhatsApp* dengan memanfaatkan ADB sebagai penghubung untuk mendapatkan data. Setelah proses tersebut dilakukan *decrypt* data yang dienkripsi dengan menggunkan *key* yang diperoleh saat melakukan akuisisi data.

C. Implementation

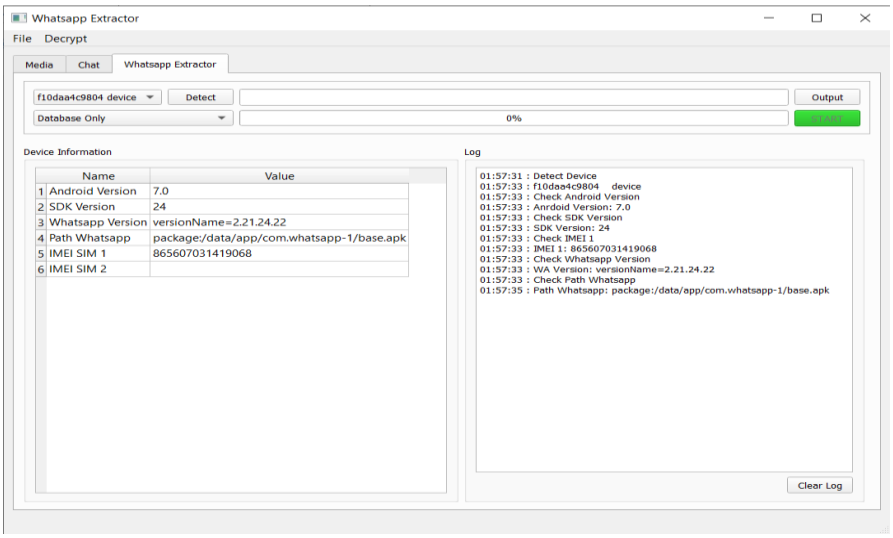
Pada tahap Implementasi, alat forensik *WhatsApp* dikembangkan menggunakan bahasa pemrograman *Python*, mengikuti rancangan desain *flowchart* yang telah dibuat sebelumnya. Aplikasi ini dilengkapi dengan sejumlah fitur penting yang dirancang untuk memfasilitasi proses akuisisi dan analisis data *WhatsApp*. Fitur pertama adalah *WhatsApp Extractor*, yang bertugas mengekstrak data mentah dari perangkat. Setelah data berhasil diekstrak, proses selanjutnya adalah dekripsi (*Decrypt*), yang memastikan bahwa data terenkripsi dapat diubah menjadi format yang dapat dibaca. Setelah tahap dekripsi selesai, pengguna dapat melakukan *review* data chat menggunakan fitur *WhatsApp Viewers*, yang memungkinkan analisis dan visualisasi percakapan secara menyeluruh.

Selain itu, untuk memudahkan pencarian dan peninjauan media yang dikirim dan diterima melalui *WhatsApp*, tersedia fitur *WhatsApp Viewers* Media. Fitur ini memungkinkan pengguna untuk mengakses dan meninjau file media seperti gambar, video, dan audio dengan lebih efisien. Rangkaian fitur ini tidak hanya meningkatkan efektivitas proses investigasi forensik, tetapi juga memastikan bahwa data yang relevan dapat diakses dan dianalisis dengan mudah dan cepat. Dari hasil implementasi dihasilkan sebuah alat forensik *WhatsApp* yang dapat menunjang kebutuhan sebagai berikut.

1) WhatsApp Extraktor

WhatsApp extraktor merupakan fitur dimana pengguna dapat mengakuisisi data *WhatsApp* berupa Database *msgstore.db WhatsApp*, media data yang terdapat pada *WhatsApp*, dan Ekstraksi data *WhatsApp*.ab. Tampilan halaman *WhatsApp extraktor* disajikan pada gambar 3.

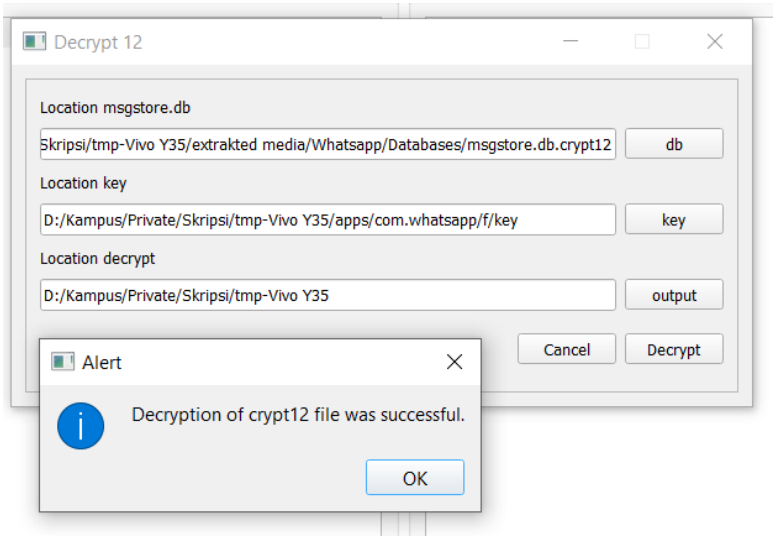
JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 2, Juni 2025, Pp. 1099-1110



Gambar 3. Alat forensik WhatsApp Extraktor

2) Decrypt

Fiture *Decrypt* merupakan proses dimana hasil enkripsi database *WhatsApp* menggunakan *key* dari *WhatsApp* tersebut diubah Kembali ke bentuk asliya sehingga informasi didalamnya dapat dibaca dengan mudah, Proses ini dilakukan setelah proses ektraksi selesai. Pada data *WhatsApp* sekarang terdapat 2 tipe *Decrypt* yaitu *Decrypt12* dan *Decrypt14*. Tampilan halaman *Decrypt* disajikan pada gambar 4.

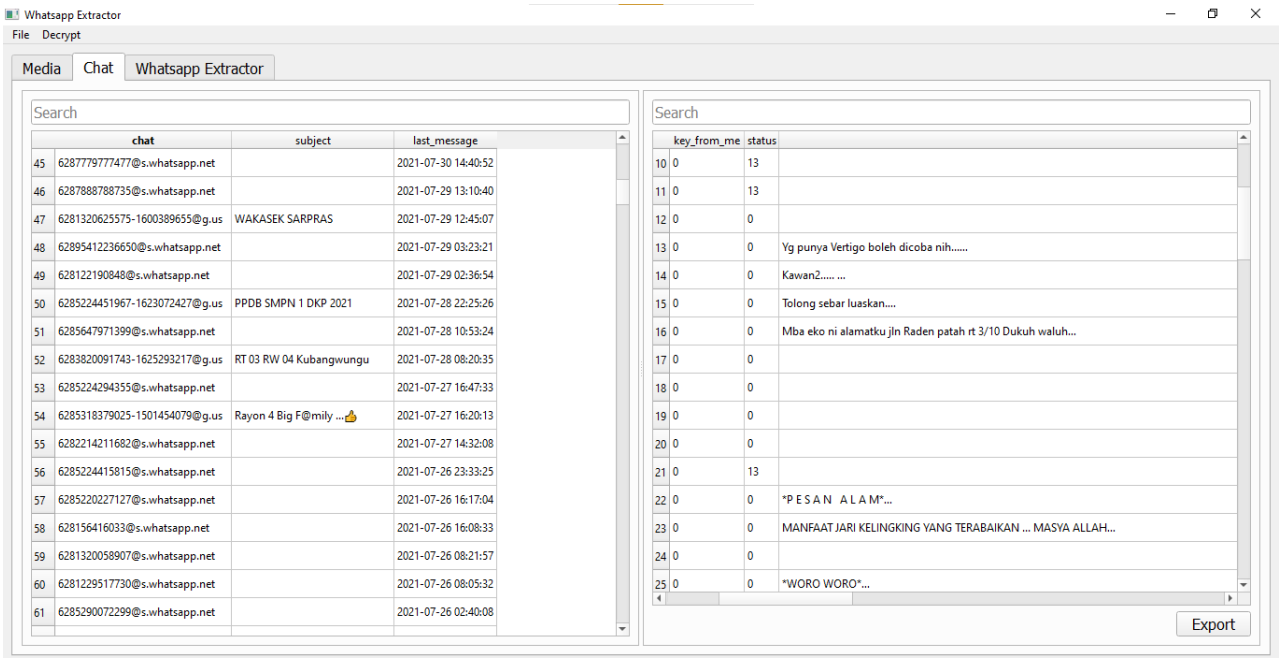


Gambar 4. Tamnpilan fitur decrypt

3) WhatsApp Viewer

Fitur *WhatsApp viewers* merupakan tahap meriview data chating seseorang dengan orang lain dengan data yang bersumber dari *msgstore.db* yang telah di *decrypt* dengan membuka databasenya, secara realdata sesuai dengan urutan data nomor. Fitur *WhatsApp* viewers media merupakan tahap mereview media media berupa foto, video, audio. Berfungsi untuk memudahkan pengguna untuk melakukan pencarian file media berdasarkan nama atau tanggal yang informasinya didapatkan pada fitur *WhatsApp viewers*. Tampilan *WhatsApp viewers* disajikan pada gambar 5.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 2, Juni 2025, Pp. 1099-1110



Gambar 5. Tampilan WhatsApp Viewers

D. Testing

Setelah alat forensik *WhatsApp* selesai dibangun, tahap berikutnya adalah integrasi dan pengujian perangkat lunak yang dilakukan oleh pengembang. Pengujian dilakukan menggunakan metode *Blackbox Testing*, yang berfokus pada pengujian fungsionalitas sistem tanpa melihat struktur internalnya. Pengujian ini mencakup verifikasi fungsi tombol, penanganan kesalahan (*error handling*), dan proses akuisisi data untuk memastikan bahwa alat berfungsi sesuai dengan kebutuhan dan spesifikasi yang telah ditetapkan.

Alat forensik ini diuji melalui serangkaian *unit test* yang telah disebutkan sebelumnya, dengan skenario pengujian yang mencakup semua fitur yang ada. Pengujian *Blackbox* memastikan bahwa setiap komponen alat beroperasi dengan benar dan efektif, termasuk ekstraksi data, dekripsi, peninjauan chat, dan peninjauan media.

Pengujian **pertama** di skenariokan dengan membuka Software alat forensik apakah berjalan atau tidak. Pengujian **kedua** dilakukan pengujian koneksi antara software dan smartphone android dengan cara menghubungkan smartphone dengan laptop menggunakan kabel USB dimana keberhasilan ditandai dengan box alert bertuliskan "*detect device*", jika tidak periksa kabel maupun spesifikasi android dengan minimal android 4.4 (kitkat). Pengujian **ketiga** dilakukan dengan mengetest tombol "*Aquicition type*" , "*Location output*", "*Start*", "*Decrypt*", apakah berjalan sebagai mana mestinya sesuai fungsi masing-masing. Pengujian ke **empat** dilakukan proses akuisisi data dengan menekan tombol start dimana seharusnya sistem akan menampilkan device information dan sistem melanjutkan proses akuisisi data *WhatsApp* yang ditandai dengan progres bar persentase sesuai dengan alur proses yang sedang berjalan. Jika proses ini tidak berjalan maka akan dilakukan pengecekan ulang dari langkah awal pada saat *detect device.* Pengujian ke **lima** yaitu mengetahui proses *decrypt* pada data yang dienkripsi apakah berhasil di *decrypt* atau tidak. Kemungkinan pada proses ini gagal hanyalah jika proses akuisisi gagal dilakukan. Pengujian ke **enam** dilakukan dengan membuka menu "*chat"*, hasil yang dihapkan pada menu ini adalah menampilkan data percakapan yang bersumber dari database *WhatsApp,* data percakapan sesuai dengan nomor dan isi dari percakapan tersebut dipaparkan. Ketidakberhasilan menu ini hanya jika proses decrypt tidak berhasil. Pengujian ke **tujuh** dilakukan dengan menguji menu "media", hasil yang diharapkan adalah dapat menampilkan list media yang berupa video, gambar, dan suara. Ketidakberhasilan menu ini tampil hanya jika proses akuisisi data WhatsApp gagal dilakukan, yang menjadi unggulan dapat menampilkan data media yang sudah terhapus dan media sekali lihat, dengan catatan media tersebut diterima maksimal 3 sebelumnya.

Hasil pengujian ini disajikan secara rinci dalam Tabel 3 dibawah, yang menunjukkan kinerja alat terhadap berbagai parameter uji dan validasi semua fitur dengan menggunakan 9 unit test berfungsi sesuai harapan.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 2, Juni 2025, Pp. 1099-1110

TABEL 3.
HASIL PENGUJIAN ALAT FORENSIK

No	Kriteria pengujian	Data masukan	Hasil yang diharapkan	Hasil pengamatan	Status
1.	*Interface*	Buka Aplikasi pada menu *WhatsApp extraktor*	Menampilkan halaman *WhatsApp extraktor*	Tampil halaman *WhatsApp extraktor*	Berhasil
2.	Fungsional	*Detect device*	Menampilkan *device connected*	Tampil pada box *list device*	Berhasil
3.	Fungsional	*Aquicition type*	*Input type Aquicition*	Tampil *type aquicition*	Berhasil
4.	Fungsional	*Location output*	Menampilkan *Input location output*	Tampil data *Location output*	Berhasil
5.	Fungsional	*Start Aquicition*	Menjalankan Proses Aquicition	Proses berjalan	Berhasil
6.	Fungsional	*Device information*	Menampilkan device information	Tidak semua *Device information* yang diharapkan tampil	Berhasil
7.	Fungsional	*Log status*	Menampilkan log yang sedang berjalann	Tampil detail log	Berhasil
8.	Fungsional	*Decrypt 12*	Fitur *decrypt* berjalan	Fitur *decrypt* berjalan	Berhasil
9.	Fungsional	*Decrypt 14*	Fitur *decrypt* berjalan	Fitur *decrypt* belum berjalan	Berhasil
10.	*Interface*	Buka Aplikasi pada menu *Chat*	Menampilkan halaman *WhatsApp viewer chat*	Tampil halaman *WhatsApp viewer chat*	Berhasil
11.	Fungsioal	Membuka database *WhatsApp*	Menampilkan data *chat* dari database *WhatsApp*	Tampilkan data *chat* dari database *WhatsApp*	Berhasil
12.	*Interface*	Buka Aplikasi pada menu media	Menampilkan halaman *WhatsApp viewer media*	Tampil halaman *WhatsApp viewer media*	Berhasil
13.	Fungsional	*List* media	Menampilkan *list* media	Tampil list media	Berhasil
14.	Fungsional	*Find* media	Menampilkan hasil *find* media	Tampilkan media	Berhasil

Dalam forensik digital, nilai hash digunakan untuk memastikan keaslian dan integritas data dengan cara verifikasi integritas dimana nilai hash dari data asli dicatat saat pengambilan bukti. Kesamaan nilai hash dengan salinan atau data yang diakses kemudian membuktikan bahwa data tidak diubah. Kemudia pada pelaporan *Chain of Custody* dimana nilai hash dicatat pada setiap transfer atau akses data, memastikan bahwa integritasnya terjaga dan tidak dimanipulasi. Lalu identifikasi data dimana nilai hash digunakan untuk membandingkan data yang ditemukan dengan data yang dikenali, memastikan keasliannya dalam proses penyidikan.

Kesamaan nilai hash penting karena menjamin bahwa data tidak berubah sejak pertama kali diakses, memvalidasi keabsahan bukti dalam pengadilan dan mencegah manipulasi atau kesalahan. Adapun perolehan nilai hash sebagai

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 2, Juni 2025, Pp. 1099-1110

pendukung keaslian dari hasil akuisisi data yang telah dilakukan menggunakan alat forensik *WhatsApp*, dari pengujian ini terhadapt 9 unit test 100% hasil dinyatakan sama untuk pengujian integrasi data, dengan melakukan perbandingan nilai hash. Diambil beberapa sampling dari salah satu *smartphone* yaitu Samsung A20 dapat disajikan bahwa memiliki nilai hash yang dihasilkan dinyatakan sama, tidak berubah setelah dilakukan akuisisi, dapat dilihat pada tabel 4.

TABEL 4.
HASIL HASH

No	Parameter	File Asli	Hasil Akuisisi
1	Nilai Hash	93dd9b4aa0f2c62a59eebaeba71431a0	93dd9b4aa0f2c62a59eebaeba71431a0
	Directori	*./Backups/chatsettingsbackup.db.crypt14	*D:/Kampus/Private/Skripsi/Tools/dfc-whatsapp-extractor-and-viewer/Samsung/extracted/Whatsapp/Backups/chatsettingsbackup.db.crypt14
2	Nilai Hash	0a8fdcd78ea9a946f9630caf793361ba	0a8fdcd78ea9a946f9630caf793361ba
	Directori	*./Databases/msgstore.db.crypt14	*D:/Kampus/Private/Skripsi/Tools/dfc-whatsapp-extractor-and-viewer/Samsung/extracted/Whatsapp/Databases/msgstore.db.crypt14
3	Nilai Hash	47bcf8d735351e2730ac1bcd3a58eebb	47bcf8d735351e2730ac1bcd3a58eebb
	Directori	*./Backups/stickers.db.crypt14	*D:/Kampus/Private/Skripsi/Tools/dfc-whatsapp-extractor-and-viewer/Samsung/extracted/Whatsapp/Backups/stickers.db.crypt14
4	Nilai Hash	26fe9f12c14305c3c4c1039bf0549bec	26fe9f12c14305c3c4c1039bf0549bec
	Directori	*./Backups/wallpapers.backup.crypt14	*D:/Kampus/Private/Skripsi/Tools/dfc-whatsapp-extractor-and-viewer/Samsung/extracted/Whatsapp/Backups/wallpapers.backup.crypt14
5	Nilai Hash	293dca45a926f6b78db2d79e81634de4	293dca45a926f6b78db2d79e81634de4
	Directori	*./Media/WhatsApp Images/IMG-20210615-WA0000.jpg	*D:/Kampus/Private/Skripsi/Tools/dfc-whatsapp-extractor-and-viewer/Samsung/extracted/Whatsapp/Media/WhatsApp Images/IMG-20210615-WA0000.jpg

Berhasilnya akuisisi data pada *WhatsApp* dibuktikan dengan adanya hasil akhir *extraksi* data *WhatsApp*, menggunakan Tools Forensik *WhatsApp* yang dilakukan terhadap 9 unit test, didapatkan sebagiamana berikut pada tabel 5.

TABEL 5.
HASIL AKUISISI DATA YANG BERHASIL DIDAPATKAN

No	Merek Smartphone	Key DB*	Msgstore.db.*crypt14*	Media	chat_list	group_ participants	deleted_ chat_jobs	message_thumbnails : message_vcard, message_links, media_streaming_sidecar
1.	Xiaomi Readmi Not 4x	✓	✓	✓	✓	✓		✓
2.	Samsung galaxy Y Grand Duos	✓	✓	✓	✓	✓	✓	
3.	Vivo y35	✓	✓	✓	✓	✓	✓	✓
4.	Lenovo A6000+	✓	✓	✓	✓	✓	✓	✓
5.	Xioami Readmi not 8 Pro,	✓	✓	✓	✓	✓		
6.	Oppo A7	✓	✓	✓	✓	✓	✓	✓
7.	Asus zenfone 4 max pro			✓				

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 2, Juni 2025, Pp. 1099-1110

No	Merek Smartphone	Key DB*	Msgstore.db.*crypt14*	Media	chat_list	group_ participants	deleted_ chat_jobs	message_thumbnails : message_vcard, message_links, media_streaming_sidecar
8.	Xioami Readmi not 10	✓	✓	✓	✓	✓	✓	✓
9.	Samsung A20	✓	✓	✓	✓	✓	✓	✓

Alat forensik khusus untuk aplikasi *WhatsApp* menjadi sangat penting mengingat banyaknya kasus siber di masyarakat yang melibatkan penggunaan *WhatsApp*. Kelebihan Alat ini menunjukkan efektivitas tinggi dalam ekstraksi data, mampu mengekstraksi pesan, media, dan log panggilan dengan akurasi tinggi, termasuk pesan yang dihapus dan media sekali lihat, dengan syarat media tersebut diterima smartphone maksiamal 3 hari sebelummnya. Alat ini juga menyediakan antarmuka yang ramah pengguna dan proses yang terotomatisasi, sehingga memudahkan penggunaannya. Dukungan perangkatnya mencakup perangkat Android dengan minimal versi Android 4 KitKat sebagai batasan. Keberhasilan akuisisi data terbukti dengan suksesnya pengujian pada 9 unit test, menunjukkan hasil yang baik dalam kondisi pengujian spesifik. Selain itu, alat ini menawarkan kemudahan analisis dengan fitur analisis lanjutan dan pelaporan yang komprehensif, serta dianggap lebih ekonomis dan dapat disesuaikan dengan kebutuhan spesifik lembaga atau pengguna. Namun, kekurangan alat ini mungkin memerlukan lebih banyak pengujian dan validasi di berbagai situasi dan perangkat yang berbeda untuk mencapai tingkat kepercayaan yang sama dengan alat komersial yang sudah ada. Dukungan perangkat belum mencakup perangkat IOS.

Dari hasil akuisisi data *WhatsApp* diatas dinyatakan keberhasilan 87% dapat diambil dari 9 unit test yang menjadi bahan pengujian, hasil ini dapat dikatakan alat forensik *WhatsApp* ini dapat bersaing dengan alat forensik yang ada dipasaran seperti yang dijelaskan pada penelitian [22] yang melakukan Analisis Penggunaan Metode ACPO (Association of Chief Police Officer) pada Forensik WhatsApp menggunakan *tools Belkasoft Evidence Center* menunjukkan akurasi tools, Belkasoft Evidence Center sebesar 81,92% . sedangkan pada penelitian [4] dilakukan analisis pada Aplikasi *WhatsApp* diperoleh dan dideteksi menggunakan metode *DFRWS* dengan *tools MOBILedit Forensic Express* menunjukkan akurasi pada tools MOBILedit Forensic Express mempunyai kemampuan akurasi sebesar 84,6%. Dengan hasil ini dapat dilihat perbedaan keunggulan dari hasil yang didapatkan.

E. Maintenance

Pemeliharaan dilakukan setelah penerapan dan penggunaan aplikasi, terutama jika sistem mengalami masalah yang tidak terdeteksi selama pengujian atau jika ada permintaan pengguna untuk meningkatkan fungsionalitas sistem. Selama tahap pemeliharaan, pengembangan akan melakukan analisis ulang dari setiap tahap pengembangan sistem, tanpa membuat sistem baru.

IV. KESIMPULAN

Kesimpulan yang dapat diambil dari pembangunan alat forensik *WhatsApp* pada *smartphone* Android yaitu dengan memanfaatkan *Android Debug Bridge* aplikasi ini dapat memperoleh data *WhatsApp* yang di ambil dari beberapa *device* yang di sebutkan pada *unit test* berisikan **Database *msgstore.db*, *Key* WhatsApp* untuk membuka *decrypt* database, Media *WhatsApp* baik video, gambar maupun audio.**

Berdasarkan hasil Uji *Blackbox* yang telah dilakukan keberhasilan dinyatakan 87% dari setiap elemen dan fitur yang ada pada aplikasi, selain itu berdasarkan pengujian didapatkan nilai hash yang sama sesuai dengan aturan yang ada bahawasannya hasil akuisisi diharuskan memeproleh data yang sama dengan aslinya pada *device* barang bukti. Selain data yang didapatkan dapat dikonvert dalam bentuk *chat WhatsApp viewer* dan media viewer untuk membantu memudahkan seorang analis forensik digital mobile dalam melakukan akuisisi khususnya seorang *examiner* di laboratorium Digital Forensik . Hal tersebut menjadi sebuah hasil pengembangan terbaru pada sebuah alat forensik khusus aplikasi *WhatsApp*, sehingga alat ini dapat dikatakan pembaruan yang spesifik pada forensik digital *smartphone android* pada aplikasi *instan massangger WhatsApp*.

Kemudian pada peneliatian ini disarankan pada penelitian selanjutnya alat forensik *WhatsApp* yang dibuat dapat dikembangkan lagi bedasarkan pengujian yang dilakukan yaitu aplikasi ini belum berhasil mendapatkan *device information* secara lengkap, tidak semua *device support* disarankan untuk dapat membuat *device bypass* agar semua *device Android support*. Sekaligus melakukan penelitian perbandingan *tools* forensik *WhatsApp* dibangun dengan alat forensik yang ada dipasaran.

V. KESIMPULAN

Bagian kesimpulan tidak harus ada. Meskipun kesimpulan mungkin merangkum poin utama di dalam artikel, jangan menyalin abstrak sebagai kesimpulan. Sebuah kesimpulan mungkin saja menegaskan dalam pentingnya hasil pekerjaan ataupun saran untuk pengembangan lebih lanjut.

UCAPAN TERIMA KASIH

Terima kasih kepada Laboratorium *Digital Forensics Center* Universitas Muhammadiyah Purwokerto atas data dan unit testing yang diberikan serta terima kasih kepada program studi Magister Informatika Universitas Ahmad Dahlan atas dukungan yang esensial dalam penelitian ini. Penghargaan juga disampaikan kepada ahli forensik yang telah memberikan wawasan dan kerjasama serta dukungan dari semua pihak pada penelitian ini.

Penelitian ini didukung oleh Direktorat Riset, Teknologi, dan Pengabdian Masyarakat (DRTPM) Direktorat Jenderal Pendidikan Tinggi, Riset, dan Teknologi, Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi di bawah Penelitian Tesis Magister dengan nomor hibah: 069/PTM/LPPM UAD/VI/2024 (15 Juni 2024).

DAFTAR PUSTAKA

[1] Statista, "Most popular social networks worldwide as of April 2024, ranked by number of monthly active users," Statista. Accessed: Apr. 01, 2024. [Online]. Available: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[2] F. F. Febrian and J. Sidabutar, "Comparative Analysis of Forensic for Whatsapp Desktop on Mac OS and Windows Using IDFIF V2," *Proc. - 2023 IEEE Int. Conf. Cryptogr. Informatics, Cybersecurity Cryptogr. Cybersecurity Roles, Prospect. Challenges, ICoCICs 2023*, pp. 327–331, 2023, doi: 10.1109/ICoCICs58778.2023.10276727.

[3] S. D. Utami, C. Carudin, and A. A. Ridha, "Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 24–32, 2021, doi: 10.14421/csecurity.2021.4.1.2416.

[4] A. Yudhana, I. Riadi, and R. Y. Prasongko, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," *J. Inform. J. Pengemb. IT*, vol. 7, no. 1, pp. 43–48, 2022, doi: 10.30591/jpit.v7i1.3639.

[5] R. Novrianda, Y. N. Kunang, and P. . Shaksono, "Analisis Forensik Malware Pada Platform Android," *Konf. Nas. ilmu Komput.*, pp. 141–148, 2014, [Online]. Available: http://if.binadarma.ac.id/sipi/jurnal/Jurnal-Paper - Anggie Khristian 12142057.pdf

[6] Fitria, "Pengaruh Orientasi Kewirausahaan dan Penggunaan E-Commerce Terhadap Kinerja Usaha," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2017.

[7] M. P. Aji and K. Oktaviani, "Database forensik msgstore.db.crypt12 pada aplikasi whatsapp," *J. Media Pratama*, vol. 12, no. April 2019, pp. 25–32, 2018.

[8] I. A. Plianda and R. Indrayani, "Analisa dan Perbandingan Performa Tools Forensik Digital pada Smartphone Android menggunakan Instant Messaging Whatsapp," *J. Media Inform. Budidarma*, vol. 6, no. 1, p. 500, 2022, doi: 10.30865/mib.v6i1.3487.

[9] 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, pp. 949–955, 2018, doi: 10.18517/ijaseit.8.3.3591.

[10] 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, [Online]. Available: https://www.researchgate.net/profile/Imam_Riadi/publication/317620078_Identification_Of_Digital_Evidence_On_Android's_Blackberry_Messenger_Using_NIST_Mobile_Forensic_Method/links/5943f0cd0f7e9b6910ee2624/Identification-Of-Digital-Evidence-On-Androids-Blac

[11] M. N. Al Jumah, B. Sugiantoro, and Y. Prayudi, "Penerapan Metode Composite Logic Untuk Perancangan Framework Pengumpulan Bukti Digital Pada Media Sosial," *Ilk. J. Ilm.*, vol. 11, no. 2, pp. 135–142, 2019, doi: 10.33096/ilkom.v11i2.442.135-142.

[12] D. Hariyadi *et al.*, "Analisis Barang Bukti Digital Aplikasi Paziim Pada Ponsel Paziim Digital Evidence Analysis Application on Android," *CyberSecurity dan Forensik Digit.*, vol. 2, no. 2, pp. 52–56, 2019.

[13] S. Patil, K. Sharma, M. Sharma, G. Chhaparwal, and K. Chowdhari, "Data Extraction Techniques for Android Based Devices," *Int. J. Comput. Sci. Trends Technol.*, vol. 5, no. 2, pp. 355–358, 2017.

[14] T. F. Efendi, R. Rahmadi, and Y. Prayudi, "Rancang Bangun Sistem Untuk Manajemen Barang Bukti Fisik dan Chain of Custody (CoC) pada Penyimpananan Laboratorium Forensika Digital," *J. Teknol. dan Manaj. Inform.*, vol. 6, no. 2, pp. 53–63, 2020, doi: 10.26905/jtmi.v6i2.4177.

[15] J. A. M. Jeyaseeli and C. Shanthi, "Physical Data Extraction from Android mobile using Apeaksoft Android toolkit and Android Debug Bridge," vol. 8, no. 5, pp. 1913–1922, 2021, [Online]. Available: http://nveo.org/index.php/journal/article/view/739/669

[16] C. Easttom, D. Sc, and W. Sanders, "On the Efficacy of Using Android Debugging Bridge for Android Device Forensics," pp. 730–735, 2019.

[17] A. Wiki, "Android Debug Bridge." Accessed: Jun. 07, 2021. [Online]. Available: https://en.droidwiki.org/w/index.php?title=Android_Debug_Bridge&oldid=387

[18] J. Shovic, *Phthon*, 1st ed. Canada: John Wiley & Sons, Inc., 2019.

[19] Nurjannah, M. H. Dar, and B. Bangun, "Sistem Pelacakan Kontak COVID-19 Menggunakan Teknologi QR Code Berbasis Web," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 7, no. 3, pp. 283–292, 2021, [Online]. Available: https://jurnal.stmikroyal.ac.id/index.php/jurteksi/article/view/1180

[20] N. Hidayati and S. Sismadi, "Application of Waterfall Model In Development of Work Training Acceptance System," *INTENSIF J. Ilm. Penelit. dan Penerapan Teknol. Sist. Inf.*, vol. 4, no. 1, pp. 75–89, 2020, doi: 10.29407/intensif.v4i1.13575.

[21] M. Al Fajar, M. H. Dar, and R. Rohani, "Application of Waterfall model in development of family planning participants information system," *Sinkron*, vol. 7, no. 2, pp. 679–686, 2022, doi: 10.33395/sinkron.v7i2.11387.

[22] R. Y. Prasongko, A. Yudhana, and I. Riadi, "Analisis Penggunaan Metode ACPO (Association of Chief Police Officer) pada Forensik WhatsApp," *J. Sains Komput. Inform.*, vol. 6, no. 2, pp. 1112–1120, 2022.