



ANALISIS FUNGSI BASIS DATA BERBENTUK FILE MSGSTORE.DB.CRYPT DALAM APLIKASI WHATSAPP

Sri Mulyani^a, Syeila Ayu Rizkita^b, Novia Ayu Almawati^c, Dari Dianata Agustin^d, Puteri Marchanda Izzati^e, Mila Puspitasari^f, Rini Junita Manalu^g, Ricky Firmansyah^h

^a Sistem Informasi, 1, Universitas Adhirajasa Reswara Sanjaya

^b Sistem Informasi, syeilaayr30@gmail.com, Universitas Adhirajasa Reswara Sanjaya

^c Sistem Informasi, noviaayualmawati203@gmail.com, Universitas Adhirajasa Reswara Sanjaya

^d Sistem Informasi, daridntaa@gmail.com, Universitas Adhirajasa Reswara Sanjaya

^e Sistem Informasi, putrimarchandaaa@gmail.com, Universitas Adhirajasa Reswara Sanjaya

^f Sistem Informasi, mileuups14@gmail.com, Universitas Adhirajasa Reswara Sanjaya

^g Sistem Informasi, rinijunitamanalu@gmail.com, Universitas Adhirajasa Reswara Sanjaya

^h Sistem Informasi, ricky@ars.ac.id, Universitas Adhirajasa Reswara Sanjaya

ABSTRAK

Now technology is growing rapidly, chat applications are very popular with many parties, one of which is Whatsapp Messenger. WhatsApp can be accessed by Android and iOS users, this application provides facilities not only for sending texts but can also be in the form of videos, photos, files, voice and video calls. WhatsApp has a database called msgstore.db.crypt to back up data used by its users but most people don't understand the purpose of the file. For this reason, this study resulted in several functions of msgstore.db.crypt which were previously unknown to the general public, namely as a data store on WhatsApp, making backing up WhatsApp messages easier, being able to restore deleted message data, being able to synchronize between applications and several other functions. Other things. This database file is useful for running applications, all activities and messages will be directly stored and processed through the database. File types can vary depending on the version of the WhatsApp application of the users if it has not been updated for a long time then it is possible that the crypt used is crypt7, crypt8, crypt10 or crypt12 these are the same file type but with different encryption levels. The msgstore file itself is located in the WhatsApp / Databases folder and opening the database of this file can use the SQLite Browser Database application.

Keywords: Crypt, File, Storage.

Abstrak

Kini teknologi sangat berkembang pesat, aplikasi chatting sangatlah digemari oleh banyak pihak salah satunya WhatsApp Messenger. WhatsApp ini dapat diakses oleh pengguna android dan ios, aplikasi ini menyediakan fasilitas tidak hanya untuk mengirimkan teks namun bisa juga berupa video, foto, file, dan panggilan suara maupun video. WhatsApp memiliki database yang dinamai msgstore.db.crypt untuk membackup data yang digunakan oleh penggunanya namun kebanyakan masyarakat tidak memahami tujuan adanya file tersebut. Dengan menggunakan metodologi pendekatan kualitatif yaitu dengan cara mengumpulkan data studi pustaka dengan menggunakan sumber data berupa buku referensi dan jurnal ilmiah maka pada penelitian ini menghasilkan beberapa fungsi dari msgstore.db.crypt yang sebelumnya tidak diketahui oleh khalayak umum, yaitu sebagai penyimpanan data di whatsapp, mencadangkan pesan whatsapp menjadi lebih mudah, dapat mengembalikan data pesan yang telah terhapus, dapat melakukan sinkronisasi antar aplikasi dan beberapa hal lainnya. File database ini berguna untuk menjalankan aplikasi, semua aktivitas dan pesan akan langsung tersimpan dan diproses melalui database. Jenis file dapat berbeda-beda tergantung dengan versi aplikasi WhatsApp para pengguna jika sudah lama tidak diperbarui maka kemungkinan crypt yang digunakan adalah crypt7, crypt8, crypt10 atau crypt12 ini merupakan jenis file yang sama namun dengan tingkat enkripsi yang berbeda. File msgstore sendiri terletak di dalam folder

WhatsApp / Databases dan membuka database file ini dapat menggunakan aplikasi *SQLite Browser Database*..

Kata Kunci: Crypt, File, Penyimpanan.

1. PENDAHULUAN

Teknologi sangat dibutuhkan di era saat ini, terlebih lagi dengan penyedia komunikasi atau pertukaran informasi yang dapat dilakukan dimana saja tanpa memberatkan para penggunanya, karena itu banyak perusahaan yang meluncurkan aplikasi dengan fasilitas chat, yang dapat digunakan tidak hanya mengirim teks namun bisa juga berupa berkas video, foto, file, dan lain-lain. Salah satu aplikasi yang sedang populer saat ini adalah WhatsApp, aplikasi WhatsApp merupakan aplikasi layanan pesan teks yang diluncurkan untuk pengguna ponsel Android dan iOS. Aplikasi ini banyak digunakan untuk mengirim pesan, melakukan panggilan suara atau video, dan berbagi momen sehari-hari.

Pada setiap aplikasi terdapat sistem yang berperan sebagai tempat penyimpanan data atau bisa juga disebut basis data atau database. Basis data atau database adalah kumpulan data dan informasi yang tersimpan rapi dalam ruang penyimpanan komputer sehingga dapat dengan mudah diakses oleh program komputer untuk mengetahui keberadaan data tersebut. Dalam dunia komputer saat ini terdapat banyak sekali jenis database seperti MySQL, Microsoft SQL Server, Microsoft Access, Oracle dan masih banyak lagi. Semua memiliki fitur dan spesifikasi yang berbeda [1].

Aplikasi WhatsApp memiliki tabel database yang diperbarui secara berkala dalam sistem operasi Android. Database ini dicadangkan secara otomatis melalui fitur autobackup yang berbeda dengan database utama [2]. File database pada WhatsApp di android tersimpan pada format terenkripsi. Sedangkan pada iOS tidak tersimpan dalam format terenkripsi [3].

Inilah yang menjadi masalah umum kenapa penyimpanan internal menjadi penuh karena WhatsApp menggunakan file crypt untuk mengamankan basis data riwayat pesan bagi para penggunanya. File database crypt ini biasanya terletak di direktori `/sdcard/Whatsapp/database`, pada umumnya WhatsApp dengan manual menamakan filenya sebagai `msgstore.db.crypt` yang tersimpan disetiap penggunaannya, namun file tersebut tidak dapat diakses secara sembarangan.

Yang menjadi masalah khususnya yaitu kebanyakan pengguna aplikasi ini tidak mengetahui apa fungsi dari `msgstore.db.crypt` ini seperti yang telah dijelaskan sebelumnya file ini tidak dapat diakses sembarangan sehingga terkadang membuat para penggunanya kebingungan akan hal ini. Penelitian ini dirumuskan adalah untuk menemukan: apa yang dimaksud dengan Database crypt? apa fungsi dari file `Msgstore.db.crypt` pada aplikasi WhatsApp? dan dimana letak penyimpanan file `Msgstore.db.crypt`?

Adapun tujuan penelitian ini adalah untuk mengetahui apa yang dimaksud dengan database `Msgstore.db.crypt`, apa fungsi dari file database `Msgstore.db.crypt` pada aplikasi WhatsApp. Penelitian ini dibatasi pada fungsionalitas dan penempatan database berupa file `Msgstore.db.crypt` pada aplikasi WhatsApp.

Maka dari itu penulis melihat adanya kebutuhan penelitian terkait dengan fungsi `msgstore.db.crypt` dengan harapan dapat memberikan ilmu yang bermanfaat bagi para pembaca terutama bagi mereka yang merasa penasaran dengan fungsi file database tersebut.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terkait

Penelitian yang dilakukan oleh Muhammad Syarif Hartawan, Amat Damuri, dan Arman Syah Putra pada tahun 2020 dengan judul "Pengolahan Data untuk Menemukan Bukti pada Mobile Forensik" Penelitian ini menggunakan software Sypnote untuk melakukan serangan Remote Access Trojan (RAT) pada smartphone untuk bertukar informasi. Sypnote membentuk software menggunakan ekstensi, software yang mengandung software berbahaya. Serangan itu berhasil menguasai perangkat smartphone, memungkinkannya untuk mengunggah database WhatsApp dari manajemen file smartphone. Dapatkan database WhatsApp, ekstrak menggunakan WhastApp Viewer dan DB.Browser.for.SQLite untuk menghasilkan artefak digital dan memulihkan pesan yang dihapus. Menurut hasil pengujian perangkat lunak enkripsi crypt, bukti Belkasoft dan ekstraktor kunci whatsapp/DB keduanya memenuhi uji verifikasi pengulangan dan reproduktifitas, ekstraktor kunci whatsapp/DB mendominasi dalam kemampuan mengekstrak pesan teks artefak, kemudian belkasoft Memiliki keunggulan dalam mengekstraksi video, gambar dan file [4].

Penelitian yang dilakukan oleh Putu Denny Indra Putra dan Ketut Gede Suhartana pada tahun 2021 dengan judul "Cyberbullying Analysis On WhatsApp Messenger Using The National Institute Of Justice (NIJ) Method". permasalahan dalam penelitian ini ialah akibat dari kemudahan penggunaan media sosial salah satunya ialah aplikasi WhatsApp. tetapi, tidak semua orang memakai media sosial dengan baik dan melakukan kejahatan yang paling umum, cyberbullying. WhatsApp adalah salah satu aplikasi media sosial yang databasenya (msgstore.db) bisa digunakan pada penyelidikan sebagai bukti investasi forensik seluler terkait dengan cyberbullying. pada penelitian ini, metode National Institute of Justice (NIJ) digunakan untuk menyelidiki WhatsApp yang digunakan sebagai platform untuk cyberbullying. saat pemeriksaan lebih lanjut dibutuhkan, diperlukan data krusial yang diklaim "Msgstore.db", yang merupakan tempat penyimpanan data dalam bentuk database yang bisa dibaca oleh software SQLite, dan kemudian ketika pihak berwenang bisa membuka file tersebut, ketika korban melalui jaringan saat melakukan bullying, bukti chatting terungkap [5].

Penelitian ini dilakukan pada tahun 2017 oleh Zulkarnaen akbar dan Iwan Krisnadi dengan judul "Analisis Perbandingan alat Ekstraksi Database Whatsapp Crypt12 menggunakan Metode Ekstraksi Logis". Penelitian ini membandingkan tools untuk menggambarkan file database WhatsApp. hasil penelitian menunjukkan bahwa analisis uji forensik tidak hanya mengandalkan alat yang dibandingkan, melainkan database hasil tertulis. Isi file crypt (backup database) dan arsip asli pada sistem intinya sama, namun yang membedakan ialah WhatsApp hanya mem-backup setiap 24 jam, jadi proses backup tidak diperbarui [2].

2.2. Basis Data

Basis data adalah Kumpulan informasi yang disimpan sistem di komputer sehingga dapat diperiksa menggunakan program komputer untuk mendapatkan informasi dari database. Tujuan utama dari sistem database adalah untuk mengabstraksi data dari mana pengguna dapat membangun tampilan. Ini dirancang untuk menyederhanakan interaksi antara pengguna dan sistem, database dapat menyajikan pandangan yang berbeda kepada pengguna, pemrogram, dan administrator [6]. Database merupakan hal yang sangat penting yang harus diperhatikan. Database itu sendiri digunakan untuk menyimpan informasi atau data yang akan digunakan nantinya.

2.3. WhatsApp

WhatsApp adalah aplikasi layanan pesan singkat untuk pengguna ponsel Android dan iOS. Aplikasi ini banyak digunakan untuk mengirim pesan, melakukan panggilan suara atau video, dan berbagi momen sehari-hari yang sederhana, aman dan terjamin, dan tersedia di berbagai ponsel di seluruh dunia. WhatsApp sendiri mengambil namanya dari frase What's Up yang artinya Ada Apa. Didirikan oleh Jan Koum dan Brian Acton, WhatsApp telah bergabung dengan Facebook sejak 2014 dan terus beroperasi sebagai aplikasi mandiri dengan fokus membangun layanan aplikasi perpesanan yang cepat dan andal di mana pun di dunia.

WhatsApp menggunakan Open Standard Messaging Extensible and Presence Protocol (XMPP) yang telah disesuaikan. XMPP sendiri merupakan teknologi XML terbuka untuk komunikasi waktu nyata dalam sebuah aplikasi obrolan. Saat Aplikasi WhatsApp terinstal di sebuah ponsel maka yang pertama dilakukan adalah membuat akun dengan menggunakan nomor telepon sebagai nama akun. WhatsApp dengan otomatis akan mensinkronisasikan semua nomor telepon yang ada pada ponsel setelah melewati beberapa prosedur perijinan.

WhatsApp sendiri menyimpan semua percakapan dalam database di setiap perangkat pengguna WhatsApp. Aplikasi WhatsApp telah menerapkan enkripsi untuk melindungi file database-nya. Format file database terenkripsi WhatsApp adalah msgstore.db.crypt dan saat ini menggunakan crypt12 [7].

2.4. File Msgstore

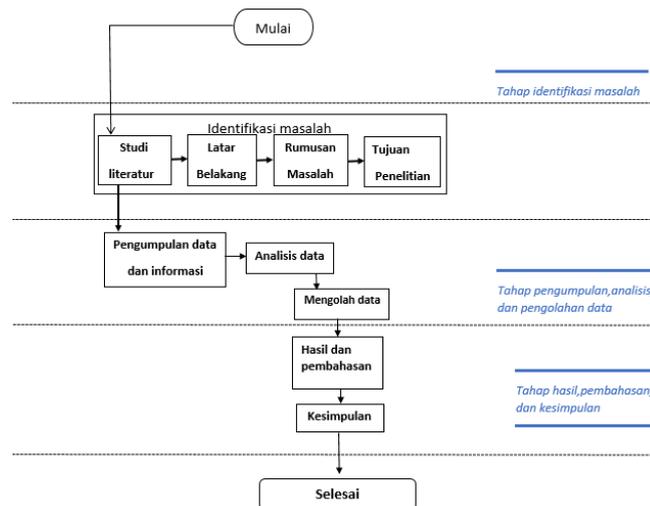
File msgstore adalah file backup otomatis di WhatsApp yang muncul setiap beberapa bulan. Data di WhatsApp, seperti teks, video, gambar, stiker, rekaman, dll, akan dicadangkan ke file msgstore [8].

Crypt adalah format data yang dienkripsi oleh aplikasi WhatsApp, dan jika dijelaskan, file tersebut menyertakan riwayat tautan, panggilan suara, dan panggilan video. Basis data aplikasi dapat ditemukan menggunakan nama file "msgstore.db". Pada saat yang sama, nama file database cadangan adalah "msgstore.db.cryptX" [9]. Crypt12 adalah versi terbaru dari file database WhatsApp, yang mengklaim sebagai database paling aman, dan sudah memiliki enkripsi ujung ke ujung. WhatsApp menggunakannya untuk melindungi basis data pesan pengguna di perangkat Android-nya. Untuk setiap versi baru aplikasi, WhatsApp menggunakan algoritme yang berbeda untuk mengenkripsi file database. Ekstensi yang ditambahkan ke file DB, seperti .CRYPT6, .CRYPT7, atau .CRYPT8, menunjukkan algoritme yang

digunakan untuk enkripsi [2]. File ini akan berguna bagi pengguna ketika mereka secara tidak sengaja menghapus aplikasi WhatsApp.

3. METODOLOGI PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah pendekatan kualitatif yaitu teknik pengumpulan data studi pustaka dengan menggunakan sumber data berupa buku referensi dan artikel jurnal ilmiah. Jenis data yang digunakan adalah format data sekunder. Prosedur yang dilakukan dalam penelusuran kepustakaan ini yaitu dengan melakukan tahap identifikasi masalah dilanjutkan dengan tahap pengumpulan, analisis dan pengolahan data, lalu yang terakhir tahap pembuatan hasil pembahasan dan kesimpulan.



Sumber : Hasil Penelitian (2022)
Gambar 1. Diagram alur penelitian

4. HASIL DAN PEMBAHASAN

Berdasarkan uraian di atas, maka peneliti bermaksud untuk melakukan penelitian yang berkaitan dengan analisis fungsi basis data berbentuk file (msgstore.db.crypt) dalam aplikasi WhatsApp dengan tujuan untuk mengetahui secara lebih terperinci tentang fungsi dari database WhatsApp tersebut.

Database WhatsApp memiliki fungsi yang sangat penting. Maka dari itu kita harus mengenalnya dan mengetahui fungsi dari database tersebut. Biasanya database ini berada dalam folder bernama file msgstore.db.crypt.

Berikut fungsi-fungsi dari database berbentuk file Msgstore.db.crypt yang ada pada Aplikasi WhatsApp:

4.1.1. Sebagai Penyimpanan Data di WhatsApp

Database berupa file msgstore.db.crypt berfungsi sebagai folder penyimpanan data percakapan WhatsApp. Artinya seluruh aktivitas komunikasi yang dilakukan oleh pengguna akan dimasukkan dan disimpan rapi di dalam file-file tersebut. Data yang tersimpan bersifat permanen. Walaupun kita ganti perangkat, data tidak akan hilang selama nomor yang digunakan sebagai akun WhatsApp baru masih menggunakan nomor yang sama.

Sifat data yang disimpan adalah permanen. Walaupun kita ganti perangkat, data tidak akan hilang selama nomor yang digunakan sebagai akun WhatsApp baru masih menggunakan nomor yang sama.

4.1.2. Mencadangkan Pesan WhatsApp Menjadi Lebih Mudah

Dengan hadirnya database WhatsApp, maka proses back up pesan WhatsApp bisa lebih mudah dan efisien. Ini karena pengguna tidak perlu mengaturnya secara manual, cukup tentukan berapa lama mereka ingin mencadangkan. Saat ini, database masih menerima backup sistem setiap mingguan, bulanan dan tahunan. Artinya jika masih dalam jangka waktu tersebut maka data akan tetap aman walaupun sudah dihapus di aplikasi WhatsApp. File database backup hanya digunakan untuk pencadangan basis data dan dapat digunakan untuk memulihkan data jika sesi dihapus atau aplikasi dihapus.

4.1.3. Dapat Mengembalikan Data Pesan Yang Telah Terhapus

Fungsi database WhatsApp selanjutnya adalah memulihkan pesan atau chat WhatsApp yang terhapus secara tidak sengaja. Pengguna hanya perlu mengakses file berupa msgstore.db.crypt dan kemudian install ulang perangkat sesegera mungkin. Ini adalah fungsi database WhatsApp yang paling banyak digunakan dan fungsi yang harus diketahui oleh pengguna WhatsApp. Walaupun perangkat diganti, data tidak hilang selama nomor yang dipasang dengan WhatsApp baru sama dengan nomor yang lama.

4.1.4. Dapat Melakukan Sinkronisasi Antar Aplikasi

Dengan adanya database aplikasi WhatsApp sinkronisasi antar aplikasi WhatsApp akan tetap terjadi secara otomatis. Hal yang perlu kita lakukan saat mendownload aplikasi tersebut harus tetap menggunakan nomor smartphone yang lama. Nah, apabila nomor smartphone yang digunakan adalah nomor lama pastinya data WhatsApp yang lama juga akan ikut muncul di dalam aplikasi WhatsApp yang baru diinstal ini. Jadi sekalipun smartphone baru, data chat di WhatsApp lama tidak akan hilang dan akan tetap ada.

4.1.5. Perantara Back Up Data Audio Visual WhatsApp

Fungsi database WhatsApp adalah sebagai alat backup data audio visual yang terdapat dalam aplikasi WhatsApp. Dengan adanya fungsi ini tentunya lebih dari sekedar data chat yang di backup. Melainkan juga informasi dari data foto, video serta pesan audio juga dapat tersimpan dengan baik.

4.1.6. Bukti Tambahan Data Forensik

Tidak hanya fungsi umum saja database WhatsApp dapat dimanfaatkan pula dalam sebuah fungsi khusus yaitu membantu kasus kepolisian. Hal ini dapat diterapkan dikarenakan saat ini teknologi sering kali dijadikan sebagai media melakukan kejahatan seperti penipuan, perjudian, pornografi, jaringan narkoba, bahkan pembunuhan. Para pelaku kejahatan biasa sebelum melakukan tindak asusila, ia mengabari korbannya maupun rekan penjahat melalui aplikasi chatting salah satunya WhatsApp.

WhatsApp merupakan media sosial yang menyediakan fasilitas chatting yang datanya tersimpan dalam file database bernama msgstore.db.crypt yang dapat dibaca melalui aplikasi salah satunya SQLite. Dalam hal ini penyelidik membaca file msgstore.db.crypt untuk menemukan bukti terkait yang dapat menjadi tambahan bukti yang mungkin dapat memberatkan pelaku, berkemungkinan saja bahwa pelaku menyusun rencana dengan rekannya di aplikasi WhatsApp.

WhatsApp otomatis akan membackup percakapan setiap harinya pada pukul 04.00 pagi lalu akan disimpan dalam folder WhatsApp bernama msgstore.db.crypt pada ponsel. Folder tersebut biasanya terletak pada memori internal maupun eksternal. Enkripsi yang dipakai WhatsApp ini menggunakan algoritma AES (Advanced Encryption Standard) untuk melindungi data.

Untuk mendapatkan file database, database aplikasi harus terlebih dahulu memerlukan proses rooting untuk memasukkan data. Pada saat yang sama, untuk backup database, karena file database terletak di media penyimpanan, baik internal maupun eksternal tergantung pada pilihan pengguna, sehingga tidak diperlukan proses root. Basis data aplikasi dapat ditemukan menggunakan nama file "msgstore.db". Pada saat yang sama, nama file database cadangan adalah "msgstore.db.crypt". Setiap file database memiliki kegunaannya masing-masing, tergantung dari lokasi file tersebut. Analisis ini bertujuan untuk mendeteksi dan menganalisis hasil dari tahap akuisisi data yang relevan untuk penerapan aplikasi WhatsApp.

Ekstraksi Data WhatsApp dari Data Image Adapun langkah-langkah untuk mengekstrak data adalah sebagai berikut:

4.2.1. Untuk mengambil data gambar dari memori internal dan eksternal kembali, untuk kedua smartphone dengan menggunakan ProDiscover. Cadangan sebagai indikator dalam folder yang menyimpan data berlabel sesuai tanggal. Data yang dicari adalah file data.ext4.tar kemudian diekstrak.

4.2.2. Dengan menggunakan hasil ekstrak perangkat pencitraan ekspor folder WhatsApp folder dan folder com.whatsapp. Jika file tersebut tidak dapat dibuka, maka dalam keadaan terkompresi harus dikompresi terlebih dahulu dengan 7zip.

Database WhatsApp setelah semua data tentang WhatsApp diperoleh dengan dekripsi berikutnya crypt8 dienkripsi WhatsApp untuk menerapkan ke database. Untuk mendekripsinya diperlukan sebuah file key yang terletak pada folder com.whatsapp/files/.

Setelah dekripsi, file database baru msgstore.decrypted.db akan muncul di folder yang sama dengan file database terenkripsi, dan artefak digital yang terkait dengan aplikasi WhatsApp dapat diperoleh. Selain

percakapan dan foto profil, Anda juga bisa mendapatkan file media yang dikirim atau diterima, seperti file audio, video, catatan suara, gambar, dan log panggilan.

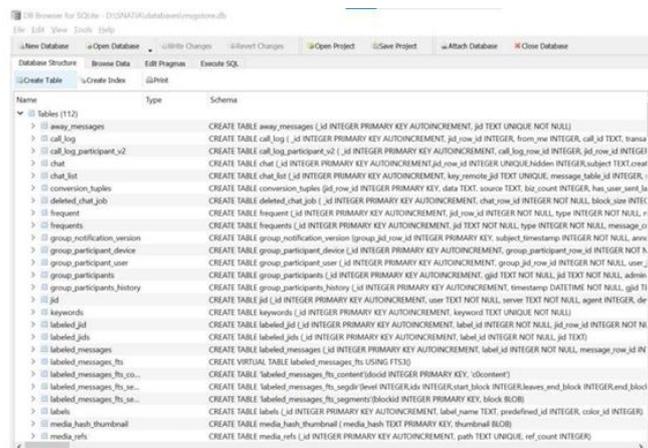
Pada direktori `com.whatsapp/databases/` ada beberapa database yang tidak terenkripsi dan pada direktori `com.whatsapp/avatar/files/` terdapat thumbnails foto profil pengguna dan kontak-kontak pada aplikasi WhatsApp.

Enkripsi pada aplikasi WhatsApp menggunakan AES 256-bit, sehingga sulit untuk didekripsi tanpa file kunci. Teknik dekripsi database aplikasi WhatsApp dapat dilakukan dengan beberapa cara, tergantung dari jenis enkripsi yang digunakan. Dalam jenis enkripsi crypt7 dan crypt8, Anda harus menggunakan kunci file untuk mendekripsi file database, sedangkan dalam jenis enkripsi crypt5, Anda dapat mendekripsi database tanpa file kunci, tetapi hanya alamat email (gmail) yang digunakan untuk mendapatkan kode hash md5nya. Database yang terenkripsi crypt7 dan crypt8 tidak bisa didekripsi menggunakan file key yang ada pada smartphone berbeda, setiap smartphone yang ter-install aplikasi WhatsApp akan membuat sebuah file key yang unik dan hanya bisa digunakan oleh smartphone itu sendiri.

File database aplikasi berguna untuk menjalankan aplikasi. Semua aktivitas dan pesan dalam aplikasi disimpan dan diproses melalui database. Sedangkan file backup database hanya digunakan untuk backup database dan berguna untuk memulihkan data saat percakapan dihapus atau aplikasi di-uninstall. Karena kegunaan yang berbeda, pengembang memperlakukan status setiap file secara terpisah. File database aplikasi tidak dienkripsi sementara database cadangan memerlukan enkripsi.

Hal ini dikarenakan tingkat kerumitan lokasi data dan cara penggunaannya dalam aplikasi. Untuk membuka database, Anda bisa menggunakan aplikasi eksternal untuk membuka keduanya. Untuk database aplikasi, Anda dapat menggunakan aplikasi SQLite Browser Database Processing untuk membuka file secara langsung. Meskipun database backup tidak dapat dibuka langsung menggunakan browser SQLite. Basis data cadangan harus dibuka menggunakan WhatsApp Viewer dan kunci enkripsi harus ditambahkan menggunakan file lisensi yang terletak di folder data aplikasi. Itu sebabnya Anda perlu melakukan root saat membuka kedua database ini.

File crypt ini tidak mudah diakses sebagai msgstore karena database file ini dienkripsi dengan kunci unik pengguna. Setiap pengguna memiliki kunci unik yang dengannya pengguna dapat mendekripsi file database seperti `msgstore.db.crypt`. Kunci unik terletak di penyimpanan internal ponsel yang berada di `Android/data/com.whatsapp/`.



Sumber : <https://bit.ly/3voPOG3> [5].

Gambar 2. Struktur Database “Msgstore.db.crypt”

Tanpa file kunci, file `msgstore.db.crypt` hanya akan menampilkan data kosong. Untuk membuka kunci akses root diperlukan izin ke perangkat. Jika tidak, maka kita tidak akan pernah dapat menggunakan kunci tersebut yang digunakan dalam pecadangan, jadi tidak akan bisa memiliki akses ke conversation yang tersimpan pada salinan tersebut. Untuk membuka file `msgstore.db.crypt` bisa menggunakan aplikasi Whatsapp viewer.

File `msgstore` sendiri terletak di dalam folder `WhatsApp/ Databases` seperti yang tampak pada gambar 3.



Sumber : Hasil Penelitian (2022)
Gambar 3. File WhatsApp

Dalam folder ini kita akan menemukan file dengan format berikut:

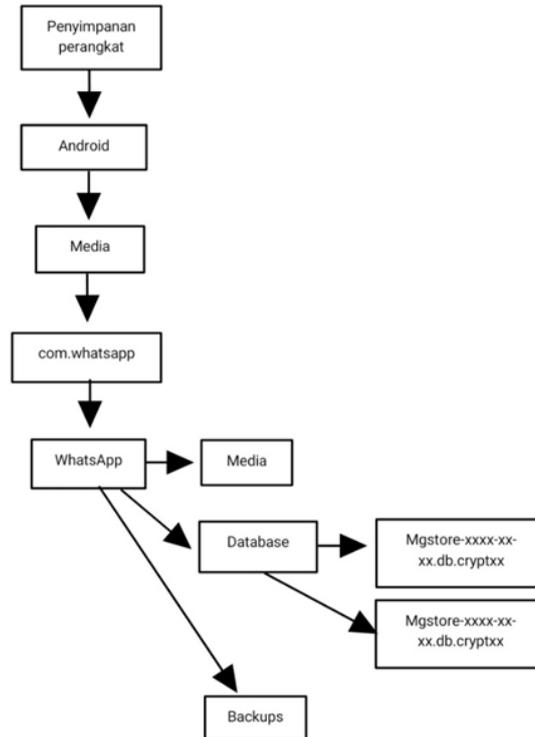
```
msgstore.db.cryptXX
msgstore.db.yyyy-mm-dd.db.cryptXX
msgstore.db.yyy-mm-dd(1).db.cryptXX
yyy-mm-dd
```

Ini akan menampilkan tanggal pembuatan file dalam format tahun-bulan-hari. Jika kami sudah lama tidak memperbarui aplikasi WhatsApp atau menggunakan versi yang sangat lama, kemungkinan besar crypt yang digunakan adalah crypt7, crypt8, crypt10 atau crypt12. Ini adalah jenis file yang sama tetapi dengan tingkat enkripsi yang berbeda. Dengan memiliki tingkat enkripsi yang berbeda, aplikasi yang diizinkan untuk membuka file dengan ekstensi ini (jika belum diperbarui) tidak akan diizinkan untuk mengakses pemeliharaan ini [10].

Berikut adalah cara memulihkan file Whatsapp:

- 4.3.1. Buka aplikasi manager file (file manager)
- 4.3.2. Buka folder/WhatsApp/Databases. Bila tidak ditemukan sesuaikan dengan pengaturan handphone masing-masing dimemori internal atau memori eksternal (kartu SD/XD)

Contoh alur penyimpanan database yang ditunjukkan seperti seperti pada gambar 4.



Sumber : Hasil Penelitian (2022)
Gambar 4. Alur penyimpanan

Contoh file database msgstore pada WhatsApp seperti pada gambar 5.



Sumber : Hasil Penelitian (2022)
Gambar 5. WhatsApp Database

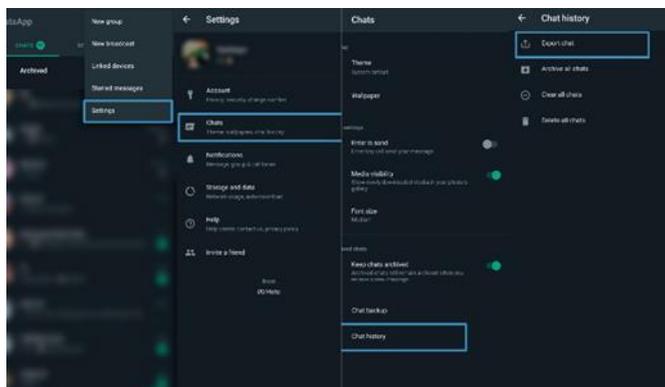
- 4.3.3. Ganti nama file cadangan yang ingin dipulihkan dari msgstore-yyyy-mm-dd.l.db.crypt14 menjadi msgstore.db.crypt.14. Jangan mengubah nomor ekstensi crypt.
- 4.3.4. Uninstall dan Install ulang WhatsApp, kemudian anda memiliki opsi untuk memilih apakah akan memulihkan pesan yang dihapus, jika ingin dipulihkan klik pulihkan.
- 4.3.5. Pesan WhatsApp yang sudah terhapus akan pulih kembali. Perlu diketahui bahwa cara ini hanya dapat digunakan bila pesan terhapus tidak lebih dari 7 hari. Untuk menghindari pesan terhapus lagi, maka kini anda dapat mengaktifkan fitur backup yang ada pada aplikasi WhatsApp.

Adapula cara untuk mengakses obrolan Whatsapp:

*ANALISIS FUNGSI BASIS DATA BERBENTUK FILE MSGSTORE.DB.CRYPT DALAM
APLIKASI WHATSAPP (Sri Mulyani)*

Pertama, Buka aplikasi dan klik tanda titik tiga di sudut kanan atas, lalu klik pengaturan. Dalam pengaturan, ketuk chat, Kemudian klik Riwayat Obrolan lalu masuk Ekspor obrolan.

Setelah itu, pilih chat yang ingin disimpan ke perangkat, lalu kirim ketempat yang diinginkan misalnya Google Drive atau E-mail.



Sumber : Hasil Penelitian (2022)

Gambar 6. Tutorial akses obrolan WhatsApp

Cara ini berguna ketika kita ingin berbagi percakapan yang kita pertahankan dengan orang lain tanpa mengambil tangkapan layar.

Kelebihan dan keunikan dari jurnal ini adalah terletak pada ide dan gagasannya, dengan menggunakan dasar teori yang beragam sesuai dengan permasalahan yang diambil dalam jurnal ini, selain itu penulis dengan cermat memilih pembahasan yang sering ditanyakan oleh khalayak umum dan juga tersusun dengan sistematis dengan bahasa yang mudah dipahami

5. KESIMPULAN

File msgstore merupakan file backup otomatis data-data pada WhatsApp, seperti teks, video, gambar, stiker, rekaman suara, dan lain-lain. Dari hasil analisis dapat disimpulkan bahwa fungsi-fungsi dari database berbentuk file Msgstore.db.crypt yang ada pada Aplikasi WhatsApp adalah sebagai berikut:

1. Sebagai penyimpanan data di WhatsApp, dimana seluruh aktivitas komunikasi yang dilakukan oleh penggunaan akan dimasukkan dan disimpan rapi di dalam file-file tersebut dan data yang tersimpan bersifat permanen.
2. Mencadangkan pesan WhatsApp menjadi lebih mudah, karena pengguna tidak perlu mengaturnya secara manual, cukup tentukan berapa lama mereka ingin mencadangkan.
3. Dapat mengembalikan data pesan yang telah terhapus, dengan cara mengakses file berupa msgstore.db.crypt dan kemudian install ulang perangkat sesegera mungkin.
4. Dapat melakukan sinkronisasi antar aplikasi WhatsApp, hal yang perlu dilakukan saat mendownload aplikasi terbaru harus tetap menggunakan nomor smartphone yang lama sehingga data WhatsApp yang lama juga akan ikut muncul di dalam aplikasi WhatsApp yang baru diinstal.
5. Perantara back up data audio visual WhatsApp, dimana informasi dari data foto, video serta pesan audio dapat tersimpan dengan baik.
6. Membantu kasus kepolisian karena dapat menemukan bukti tambahan data forensik yang dapat memberatkan pelaku kejahatan yang menggunakan aplikasi WhatsApp saat melakukan perbuatannya.

6. DAFTAR PUSTAKA

- [1] E. O. Choiri, "Fungsi Penting Database Yang Perlu Anda Ketahui," *Qwords*, Nov. 18, 2019. <https://qwords.com/blog/fungsi-database/> (accessed Jul. 03, 2022).
- [2] Z. Akbar and I. Krisnadi, "Analisa Perbandingan Tools Ekstaktor Whatsapp Database Crypt12 Menggunakan Metoda Logical Extraction," *J. Telekomun. dan Komput.*, vol. 8, no. 1, p. 43, Dec. 2017, doi: 10.22441/incomtech.v8i1.2144.
- [3] A. Raf'ie Pratama, "WHATSAPP FORENSICS: EKSPLORASI SISTEM BERKAS DAN BASIS

- DATA PADA APLIKASI ANDROID DAN IOS,” 2014.
- [4] M. S. Hartawan, A. Damuri, and A. S. Putra, *PENGOLAHAN DATA UNTUK MENEMUKAN BUKTI PADA MOBILE FORENSIK*. 2020.
- [5] J. Elektronik, I. K. Udayana, I. P. Denny, I. Putra, I. Ketut, and G. Suhartana, “Cyberbullying Analysis On WhatsApp Messenger Using The National Institute Of Justice (NIJ) Method,” 2021.
- [6] A. Andaru, “Fakultas Komputer Andry Andaru Section Class Content PENGERTIAN DATABASE SECARA UMUM,” p. 1, 2018.
- [7] A. Wirara, B. Hardiawan, and M. Salman, “Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan ‘WhatsApp,’” *Teknoin*, vol. 26, no. 1, pp. 66–74, Mar. 2020, doi: 10.20885/teknoin.vol26.iss1.art7.
- [8] A. F. I. Sani, “Memori Ponsel Penuh? Hapus Saja File Msgstore di WhatsApp,” *tempo.co*, Aug. 03, 2021. <https://tekno.tempo.co/read/1490261/memori-ponsel-penuh-hapus-saja-file-msgstore-di-whatsapp#> (accessed Jul. 03, 2022).
- [9] S. Ikhsani and B. C. Hidayanto, “Analisa Forensik Whatsapp dan LINE Messenger pada Smartphone Android sebagai Rujukan dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia,” 2016.
- [10] I. Sala, “Apa itu msgstore dan untuk apa,” *androidguias.com*, Oct. 15, 2021. <https://androidguias.com/id/que-es-msgstore-y-para-que-sirve/> (accessed Jul. 03, 2022).