ANALISIS ARTEFAK DIGITAL PADA *WHATSAPP WEB* MENGGUNAKAN APLIKASI *INDEXDB*

Dicky Satria Ikhsan Utomo
20917012

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Digital Forensik
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2023

Lembar Pengesahan Pembimbing

ANALISIS ARTEFAK DIGITAL PADA WHATSAPP WEB MENGGUNAKAN APLIKASI INDEXDB

Dicky Satria Ikhsan Utomo

20917012

Yogyakarta, 09 – Oktober -2023

Pembimbing I	Pembimbing II
Dr. Yudi Prayudi, S.Si., M.Kom.	Erika Ramadhani.,S.T.,M.Eng

Lembar Pengesahan Penguji

ANALISIS ARTEFAK DIGITAL PADA WHATSAPP WEB MENGGUNAKAN APLIKASI INDEXDB

Dicky Satria Ikhsan Utomo

20917012

Yogyakarta, Desember, 2023

Tim Penguji,

Dr. Yudi Prayudi, S.S.i., M.Kom. _____

Ketua

Dr. Ahmad Luthfi, S.Kom ., M.Kom _____

Anggota I

Irving Vitra Paputungan, S.T ., M.Sc., Ph.D. _____

Anggota II

Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia

Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Abstrak

ANALISIS ARTEFAK DIGITAL PADA WHATSAPP WEB MENGGUNAKAN APLIKASI INDEXDB

Perkembangan telekomunikasi meningkat sangat pesat semenjak layanan pesan instan berbasis internet merambat cepat ke Indonesia. WhatsApp adalah aplikasi pesan instan paling populer dibanding layanan pesan instan lain. Menurut situs website statista pengguna per Januari 2017 sebanyak 1,2 miliar orang secara aktif menggunakan aplikasi ini. Seiring pembaruan, WhatsApp memiliki berbagai fitur yang disematkan dalam aplikasi ini diantaranya Whatsapp berbasis web untuk komputer. Fitur ini mempermudah pengguna dalam berbagi file tertentu serta dapat tersinkronisasi terhadap smartphone maupun komputer penggunanya. WhatsApp Web adalah ekstensi berbasis komputer dari akun WhatsApp di ponsel pengguna. Pesan yang dikirim dan diterima sepenuhnya disinkronkan antara telepon pengguna dan komputer pengguna, dan pengguna dapat melihat semuanya di kedua perangkat. Semua tindakan yang dilakukan pengguna di ponsel pengguna akan diterapkan juga di WhatsApp Web begitu juga sebaliknya. Saat ini WhatsApp Web hanya tersedia untuk beberapa ponsel Android dan Type IOS saja. Bukti Digital menjadi faktor yang sangat diperlukan dalam sebagian besar kasus hukum. Dalam studi kasus kali ini akan menganalisa apakah aplikasi IndexDB bisa dijadikan pengukuran parameter untuk memberikan analisa karakteristik dari artefak digital serta mengevaluasi alat investigasi forensik yang berspesialisasi dalam ponsel Android untuk membandingkan kinerjanya di forensik WhatsApp Browser. Dalam studi kasus ini juga memberikan informasi mengenai investigasi forensik memakai IndexDB bisa dijadikan alternatif aplikasi sebagai yang paling hemat biaya dan optimal dalam memperoleh artefak.

Kata kunci

forensic, artefak digital , whatsapp messenger web, digital forensics, Analisa forensik , indexeddb.

Abstract

ANALYSIS OF WEB FORENSIC ON WHATSAPP WEB USING INDEXDB APPLICATION

The development of telecommunications has increased very rapidly since internet-based instant messaging services have spread rapidly to Indonesia. WhatsApp is the most popular instant messaging application compared to other instant messaging services, According to the user statistics website as of January 2017 as many as 1.2 billion people actively use this application. Along with WhatsApp updates, various features are embedded in this application, including Web-Based WhatsApp for Computers, This feature makes it easier for users to share certain files and can be synchronized with their smartphones and computers. WhatsApp Web is a computer-based extension of the WhatsApp account on theuser's phone. Messages sent and received are fully synced between the user's phone and the user's computer, and the user can view them all on both devices. All actions that the user takes on the user's phone will be applied also on WhatsApp Web, and vice versa. Currently,WhatsApp Web is only available for some Android and iOS type phones. Digital Evidence has become an indispensable factor in most of the legal cases.. This study shows whether the NIST framework is a parameter measurement for evaluating forensic investigation tools specializing in Android phones to compare its performance in forensic WhatsApp browsers. Nine core assertions, seven optional assertions, six core requirements, and NIST measurement parameter optional feature requirements are used in the scope of work. The research identified WhatsApp Key/DB Extractor as the most cost-effective and best at recovering artifacts.

Keywords

forensic, artifact investigation, WhatsApp web messenger, digital forensics, persistent storage, indexeddb, nist

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Desember 2023

Dicky Satria Ikhsan utomo

Daftar Publikasi

<u>Publikasi yang menjadi bagian dari tesis</u>

Dicky Satria dan Yudi Prayudi (2023). Forensic Web Analysis on The Latest Version of WhatsApp Browser. Article Published in Journal of Computer Networks, Architecture and High-Performance Computing. (CNAPC), Volume 5 No 1, 2023.

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Dicky Satria Ikhsan Utomo	Mendesain eksperimen (60%) Menulis *paper* (70%)
Dr. Yudi Prayudi, S.Si., M.Kom	Mendesain eksperimen (40%) Menulis dan mengedit *paper* (30%)

Halaman Kontribusi

"**Tidak ada kontribusi dari pihak lain**"

Halaman Persembahan

Alhamdulillah segala puji hanya Milik Allah Subhana Wa Ta'ala yang selalu memberikan rahmatnya kepada setiap makhluk yang diciptakan-Nya
Alhamdulillah, hasil dari kerja keras ini saya persembahkan untuk :"Kedua orang tua"
Alm. Bapak Dr. H. Eddy Subrata, MM dan Hj. Surya Insani Ikowati

"Yang terkasih istri dan putri tercinta"

Imaniar Mauliani dan Aluna Kinar Kamilla

"Saudara kandung yang selalu ada dan tak pernah pergi"
Emiria Aulia Devi, Inez Inayah Adelia dan Shinta Almira Amadea

"Keluarga di Balikpapan yang selalu mendoakan dan selalu percaya "
Bapak H. Ambo Anwar, Ibu Hj. Arniati Razak, Bro Lendra & Lia, Kak Ria & Kak Sugi Beserta Kedua Ponakan yang menggemaskan

"Support System selama di Yogjakarta "
Kak Lenvika Meirina dan Kak Nico Marion

"Support System juga waktu di Surabaya "
Tante Uniek, Tante Titiek dan Nabil Azra

"Yayasan Airlangga yang selalu sabar untuk mendanai Pendidikan"
Ibu Hj. Mulia Hayati Deviantie, SE dan Bapak Dr. H.Agung Sakti Pribadi, SH.,MH

"Teman-teman yang sangat istimewa dalam hidup saya"
Asharudin, Riovan Styx Roring, Dedi Genola, Flash Gunawan, Bayu Pratama, Bobby Anand, Fahmi Abdillah, Irfan Ananda, Zona Septa, Salsabilla Suwardi, Nanda Mahardika, Prita Donna, Tasya Ananda, Tito Asmara, Yunas Ramadhan, Yuda Wardhana, Maradona, Mas Wiwit, Erliyani, Annisa Primasari, Khaeriah Insani, Bang Batak, Bang jumbo, Bang Soba, Bang Rivan, Owen, Kak Tasya Klenik, Mas Ican, Mas Rio, Bang Harris, kak Angel dan yang terakhir Mas Hasan (Boss Kost Ryzdin)

Rasanya tidak cukup terima kasih atas rasa bersyukur saya kepada nama-nama diatas untuk segala bentuk kasih sayang, dukungan moril dan materiil, pengalaman, ajaran, dan segala cinta yang kalian berikan kepada saya.
Saya doakan agar apa yang telah kalian berikan kepada saya, akan dibalas oleh Allah S.W.T berkali-kali lipat dan segala keberkahan dalam hidup.

Kata Pengantar

Segala puji syukur penulis panjatkan kepada Allah SWT, karena hanya dengan nikmat dan karunia-Nya sehingga penulis bisa menyelesaikan penulisan Tesis ini. Dan tak lupa pula Shalawat serta salam semoga tetap terlimpahkan kepada junjungan kita Nabi besar Muhammad SAW, sang pembawa kabar gembira dan sebaik-baiknya tauladan bagi yang mengharap Rahmat dan Hidayah-Nya.

Selama proses penulisan Tesis ini, begitu banyak bantuan dan dukungan yang diterima penulis dari berbagai pihak, untuk itu dalam kesempatan ini penulis ingin menyampaikan ucapan terima kasih kepada:

1. Bapak Dr. Yudi Prayudi, S.Si., M.Kom. selaku Dosen Pembimbing Utama, yang telah memberikan bimbingan, tambahan ilmu, serta masukan dan pengarahan dalam penulisan Tesis ini.
2. Ibu Erika Ramadhani, S,T., M.Eng selaku dosen pembimbing Pendamping yang telah meluangkan waktu untuk memberikan bimbingan, masukan, juga tambahan referensi serta ilmunya dalam penulisan Tesis ini.
3. Kedua orang tua, Almarhum bapak Eddi Subrata dan ibunda tercinta Surya Insani, terima kasih atas doa dan dukungannya, baik moril maupun materiil.
4. Kedua orang tua baru, bapak Ambo Anwar dan ibu Arniati Razak terima kasih atas suport kalian selama ini, terima kasih pula atas kasih sayang yang telah diberikan .
5. Orang-orang tersayang, Imaniar Mauliani dan sang rembulan , Aluna Kinar yang telah menemani dan memberikan semangat dan memotivasi untuk tetap bertahan dan tetap bersemangat untuk menggapai cita-cita.

Akhir kata penulis mohon maaf yang sebesar-besarnya atas segala kesalahan yang penulis buat baik sengaja maupun tidak disengaja. Semoga Allah SWT mengampuni segala kesalahan dan menunjukkan jalan yang lurus dan benar kepada kita semua. Amin

Yogjakarta, 09 – Oktober – 2023

Penulis

Daftar Isi

Daftar Tabel

Daftar Gambar

BAB 1
Pendahuluan

1.1 Latar Belakang

Pertumbuhan eksponensial media sosial dan aplikasi pesan instan telah memfasilitasi pengembangan yang berkembang pesat Menurut data statistik website statista menunjukkan jumlah pengguna WhatsApp aktif bulanan di seluruh dunia per-Januari 2017. Pada bulan tersebut, aplikasi perpesanan mobile mengumumkan lebih dari 1,2 miliar pengguna aktif bulanan, naik dari lebih dari 1 miliar pada bulan Februari 2016. Layanan ini salah satu aplikasi seluler terpopuler di seluruh dunia. WhatsApp adalah layanan pesan cepat lintas platform untuk smartphone yang mengandalkan internet untuk pengiriman pesan. Berdasarkan model berlangganan berbiaya rendah, WhatsApp adalah alternatif yang murah untuk mengirim pesan teks melalui SMS, terutama untuk pesan internasional atau grup. Aplikasi perpesanan mobile memungkinkan pengguna berbagi pesan teks, gambar dan video. Di Amerika Serikat, pengguna WhatsApp berjumlah 18,8 juta pengguna pada tahun 2016 dan diperkirakan akan tumbuh menjadi 25,6 juta pengguna pada tahun 2021. WhatsApp adalah aplikasi pesan untuk smartphone yang mampu berjalan lintas platform diantaranya ; Apple iOS, BlackBerry, Android, Symbian Nokia Series 40 dan Windows Phone. WhatsApp Messenger menggunakan paket data internet sama halnya seperti layananan email, browsing web, dan layanan instant messengers lainnya. Aplikasi WhatsApp Messenger menggunakan koneksi data mobile serta WiFi untuk melangsungkan komunikasi data, dengan menggunakan WhatsApp, seseorang dapat melakukan obrolan online, berbagi file, bertukar foto dan fitur lainnya yang menarik penggunanya.

WhatsApp secara resmi mengumumkan peluncuran fitur resmi bernama WhatsApp Web pada tanggal 22 Januari 2015. Fitur ini mencoba memfasilitasi penggunaan aplikasi ini untuk pengguna berbasis komputer. Seperti halnya WhatsApp berbasis smartphone, fitur ini membutuhkan koneksi internet sebagai jalur penyampaikan informasi (Mahajan & Mahender, 2022). WhatsApp bekerja melalui portal online yang disediakan oleh domain.

WhatsApp Web pada prinsipnya berfungsi untuk membuka akun WhatsApp melalui perangkat komputer. Fitur ini pada periode awal lebih mudah digunakan melalui aplikasi browser. Sinkronisasi dibutuhkan untuk membuka akun WhatsApp melalui web. Pengembang menyediakan barcode yang perlu dipindai melalui aplikasi WhatsApp mobile. Pemindaian akan secara langsung membuka aplikasi Whatsapp sesuai dengan akun yang berfungsi pada telepon genggam yang digunakan untuk pemindaian[2]. Percakapan yang terdapat pada aplikasi WhatsApp di telepon seluler akan turut disajikan pada versi web.

Sinkronisasi antar Whatsapp di dalam telepon genggam dengan versi Web dilakukan secara otomatis apabila terjadi perubahan pada salah satu aplikasi yang aktif. Bukti digital telah menjadi kontributor utama dalam pengambilan keputusan dari banyak kasus penting beberapa dekade terakhir. Saat teknologi terus berkembang, lebih banyak kasus akan tergantung pada bukti digital.

Bukti Digital menjadi faktor yang sangat diperlukan dalam sebagian besar kasus hukum. Namun, kemajuan teknologi yang mengarah pada kompleksitas artefak, memaksa para peneliti untuk membuat hubungan yang canggih antara temuan dan tersangka untuk diterimanya bukti di pengadilan. Tesis ini meneliti apakah IndexedDB, teknologi browser yang muncul, dapat menjadi sumber bukti digital untuk memberikan dukungan tambahan dan berkorelasi untuk tradisional metode investigasi. Ini terutama berfokus pada artefak dari aplikasi populer di seluruh dunia, Eksperimen kuasi pretest-posttest kasus tunggal diterapkan dengan WhatsApp Messenger dan Aplikasi Web untuk mengisi dan menyelidiki artefak dalam penyimpanan IndexedDB Google Chrome. Temuan dicirikan dan disajikan dengan potensinya untuk digunakan dalam penyelidikan forensik verifikasi. Lokasi penyimpanan artefak ditata dan operasi ekstraksi,konversi dan presentasi yang sistematis. Selain itu, alat bukti konsep dikembangkan untuk demonstrasi. Hasilnya menunjukkan bahwa penyimpanan WhatsAppWeb IndexedDB dapat digunakan untuk waktu analisis bingkai, menunjukkan nilainya dalam verifikasi bukti.

Metode yang kuat untuk mendukung kaitan bukti dengan tersangka adalah dengan mendukung klaim dengan mencocokkan informasi dari sumber independen. Misalnya, akses tersangka ke file tertentu, dan catatan pencarian ekstensif yang menunjukkan pemeriksaan

file yang sama di internet dapat dibuat menghubungkan rantai bukti. Garis waktu pembuatan, perubahan, dan akses terakhir dari file sensitive dapat menunjukkan inkonsistensi dalam Windows Registry dan informasi file yang diunduh browser gudang. Selain itu, informasi dari sumber tambahan dapat digunakan untuk memverifikasi kelainan dalam kerangka waktu yang menunjukkan kemungkinan gangguan bukti.

Berdasarkan pernyataan peneliti terdahulu diatas dapat dikembangkan Analisis Investigasi Forensik WhatsApp Messenger smartphone terhadap WhatsApp berbasis Web dengan studi kasus penyadapan percakapan WhatsApp, dengan mempertimbangkan beberapa aspek seperti pernyataan peneliti terdahulu, penelitian lanjutan dihadapkan pada berbagai jenis perangkat smartphone selama penanganan kasus investigasi forensik (Dezfouli, F and Dehghantanha, 2014).

WhatsApp (WA) dan artefak digital memiliki hubungan erat dalam konteks penggunaan aplikasi tersebut. Artefak digital mengacu pada jejak atau bukti elektronik yang dihasilkan oleh aktivitas pengguna pada platform digital, dan WhatsApp sebagai aplikasi pesan instan yang populer menyimpan berbagai jenis artefak digital. Pesan teks, panggilan suara, panggilan video, gambar, video, dan data lainnya yang dihasilkan selama interaksi pengguna dengan WhatsApp semuanya membentuk artefak digital. Analisis terhadap artefak-artefak ini dapat memberikan wawasan yang mendalam tentang perilaku dan aktivitas pengguna, yang dapat digunakan dalam berbagai konteks seperti investigasi forensik, analisis keamanan, dan pemahaman penggunaan aplikasi secara umum. Dengan memahami hubungan antara WhatsApp dan artefak digital, pengembang dan peneliti dapat mengoptimalkan metode analisis untuk menggali informasi yang lebih rinci dan relevan dari jejak digital yang ditinggalkan oleh pengguna WhatsApp.

Teknologi yang baru muncul adalah peluang bagus untuk mendukung bukti tradisional dengan informasi tambahan. Karena teknologi baru bergantung pada teknik penyimpanan dan pemrosesan yang berbeda, mengatasi asal-usulnya membutuhkan usaha ekstra dari pihak tersangka. Oleh karena itu, konfirmasi silang dengan sumber tambahan berfungsi sebagai lapisan tambahan kredibilitas untuk temuan. Kebingungan atau perubahan dalam sumber-sumber tradisional cenderung menciptakan inkonsistensi informasi dengan sumber-

sumber alternatif. IndexedDB adalah sistem database transaksional NoSQL (Not Only SQL) yang baru dikembangkan yang memungkinkan akses cepat ke data persisten melalui objek JSON (JavaScript Object Notation). Bisa dioperasikan melalui kode JavaScript yang membuatnya sangat berguna untuk browser web. Sebuah mendalam keunggulan IndexedDB terletak pada kapasitas penyimpanannya. IndexedDB menawarkan area penyimpanan yang besar mulai dari 50 MB data untuk setiap asal sementara teknologi Penyimpanan Web pesaingnya dapat menyimpan maksimum 5 MB data. Keuntungan ini memungkinkan IndexedDB untuk meningkatkan pemanfaatannya secara drastis di popular website dalam beberapa tahun terakhir. Karena banyak situs web mulai menggunakan IndexedDB, semakin tampak sebagai kandidat untuk menjadi sumber pendukung investigasi digital tradisional (Mendoza et al., 2015).

Penelitian ini menggunakan metode National In Justice karena memiliki tahapan yang lebih baik dibandingkan dengan metode lainnya. NIJ digunakan agar memperoleh atau mendapatkan bukti menurut keilmuan terhadap perawatan, validasi analisis, pengumpulan, identifikasi, dokumentasi, interpretasi, dan presentasi barang bukti dari sumber-sumber digital untuk melanjutkan atau memfasilitasi rekonstruksi kasus didapatkannya kriminalitas dan mendukung mengantisipasi berbagai macam perbuatan yang tidak sah mengindikasikan adanya proses yang diagendakan untuk mengganggu Pengangkatan data dan file dapat menggunakan tools yang sering digunakan dalam investigasi untuk mengekstrak sebagian besar informasi dengan cara yang efisien penelitian ini menyelidiki hipotesis bahwa penyimpanan IndexedDB membawa artefak yang signifikan secara forensik untuk Aplikasi Web WhatsApp. Artefak ini dapat digunakan untuk membuat analisis kerangka waktu dalam investigasi forensik. Bagian berikut membagikan pekerjaan sebelumnya pada forensik dan keamanan IndexedDB, memberikan latar belakang teknologi IndexedDB dan LevelDB, menjelaskan metodologi penelitian ini, menyajikan temuan dengan alat bukti konsep BrowSwEx, dan mengajukan kesimpulan dan kemungkinan pekerjaan di masa depan.

1.2 Rumusan Masalah

Adapun rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana penerapan dan pengembangan framework NIST untuk mendukung proses investigasi forensik pada Whatsapp Browser ?
2. Bagaimana karakteristik artefak digital pada whatsapp browser ?

1.3 Batasan Masalah

Adapun batasan masalah pada penelitian ini adalah sebagai berikut:

1. Penelitian ini hanya fokus dalam penanganan artefak digital pada Whatsapp selular yang dihubungkan dengan Whatsapp Browser.
2. Pengujian framework ini akan dibatasi pada penanganan beberapa artefak dan data-data pada Whatsapp browser untuk sinkronisasi dengan data yang diperoleh dari Whatsapp selular.

1.4 Tujuan Penelitian

Tujuan penelitian merujuk pada hasil yang ingin dicapai atau pertanyaan yang ingin dijawab melalui kegiatan penelitian. Adapun tujuan pada penelitian ini adalah sebagai berikut:

3. Mengenal penerapan framework pada Whatsapp Browser
4. Mengetahui karakteristik artefak digital pada Whatsapp Browser

1.5 Manfaat Penelitian

Manfaat penelitian mencakup dampak positif yang mungkin terjadi sebagai hasil dari penelitian. Adapun manfaat pada penelitian ini adalah sebagai berikut:

1. Memberikan gambaran investigasi forensik aplikasi Whatsapp Browser.
2. Menambah pengetahuan baru bagi dunia forensik untuk penanganan forensik yang terjadi di dalam Whatsapp browser.

BAB 2
Tinjauan Pustaka

2.1 Permasalahan Umum

Hal pertama yang ingin dipastikan adalah penelitian-penelitian yang menelusuri apakah WhatsApp berfungsi di perangkat seluler atau tidak. Pada kasus penelitian sebelumnya banyak ahli forensik menggunakan tools ini sebagai alat bantu mereka untuk menemukan sebuah barang bukti. Tools ini sangat membantu untuk melakukan recovery data yang telah hilang atau rusak, akan tetapi tools ini mempunyai suatu kelemahan tertentu, saat pengembalian data atau recovery data. Data-data yang tersimpan di FlashDrive, HDD, SSD, RAM tersebut ada pada mobile device, komputer bahkan server. Metode recovery data juga berbeda beda tergantung dari storage yang akan di proses. Salah satunya adalah menggunakan tools Autopsy atau FTK imager. Tools ini sangat membantu ahli forensik untuk mencari file data yang hilang, seperti file JPG, MP4, pdf, png, doc, zip, rar dan lain sebagainya. Hanya saja tools Autopsy atau FTK imager ini mempunyai suatu kelemahan tertentu, saat pengembalian data atau recovery data, yaitu data yang hanya bisa di recovery tetapi tidak bisa di buka secara utuh, maka dari itu solusi yang dibutuhkan adalah recovery secara utuh, data yang telah diambil / rusak bisa di recovery dan dibuka di dalam Whatsapp Browser kembali sama seperti sebelumnya.

Untuk mendukung pemecahan masalah maka dari beberapa data yang akan di gunakan adalah beberapa video dan gambar yang berupa file Teks, Log Telepon / SMS, foto, gambar maupun video akan diolah menggunakan beberapa tools forensik seperti Sleuth Kit Autopsy, FTK Imager, IndexedDB. Data ini akan dimasukan ke dalam semua tools tersebut dan akan di proses recovery pada data tersebut. Lalu pada tahap akhir dapat dilihat perbandingan dari beberapa tools forensik, Yang nantinya bisa disimpulkan bahwa ada beberapa tools yang efektif untuk melakukan recovery secara utuh.

2.2 Penelitian Sejenis

Beberapa studi penelitian telah meneliti penerapan teknik dan alat forensic pada aplikasi seluler WhatsApp dan penyelidikan jaringannya, lebih sedikit penelitian yang dilakukan fokus pada forensik Whatsapp Web. Selain itu, beberapa studi penelitian dengan cakupan aplikasi pesan instan yang lebih luas menyentuh analisis forensik WhatsApp Namun, fokus mereka bukan pada investigasi forensik penyimpanan terus-menerus dari IndexedDB, yaitu area subjek yang relatif baru untuk forensik digital.

(Vukadinovic, 2019), melakukan penelitian untuk menemukan artefak WhatsApp di messenger dan web browser. Untuk aplikasi Web WhatsApp dengan sistem operasi Windows dan Mac dengan Peramban Chrome, Firefox, dan Safari tercakup. Studi ini berfokus pada file log WhatsApp Penyimpanan web untuk catatan browser dan artefak yang disajikan seperti gambar profil dan riwayat cache log untuk nilai investigasi forensik. Meskipun artefak dari Penyimpanan Web tertutup secara rinci, tidak ada daftar rinci artefak IndexedDB yang disajikan. Studi tersebut menyatakan fakta bahwa aplikasi web tidak menyimpan pesan teks terkirim di penyimpanan sisi klien. Catatan kapan pesan teks dikirim dan ketika panggilan suara/video aktif tidak tercakup atau diproses untuk tujuan verifikasi untuk penyelidikan teknologi penyimpanan browser tradisional.

Penelitian yang dilakukan oleh Vukadinovic (2019) merupakan sebuah kontribusi penting dalam pemahaman tentang artefak WhatsApp di messenger dan web browser. Penelitian ini mencakup aplikasi WhatsApp Web pada sistem operasi Windows dan Mac, dengan berbagai peramban seperti Chrome, Firefox, dan Safari. Fokus utama dari penelitian ini adalah analisis terhadap file log WhatsApp yang disimpan di Penyimpanan Web, serta artefak yang dapat digunakan dalam investigasi forensik, seperti gambar profil dan riwayat cache log. Meskipun penelitian ini memberikan wawasan yang berharga terkait artefak dari Penyimpanan Web, penting untuk mencatat bahwa tidak ada daftar artefak IndexedDB yang disajikan secara rinci dalam penelitian tersebut.

Vukadinovic (2019) juga mengungkapkan fakta menarik bahwa aplikasi web WhatsApp tidak menyimpan pesan teks terkirim secara langsung di penyimpanan sisi klien. Ini berarti bahwa catatan yang mengidentifikasi kapan pesan teks dikirim dan kapan

panggilan suara/video aktif dilakukan tidak sepenuhnya tercakup atau tidak diproses dengan rinci dalam konteks investigasi teknologi penyimpanan browser tradisional. Dalam penelitian ini, informasi tentang pengiriman pesan dan aktivitas panggilan mungkin bisa digunakan untuk melengkapi temuan penelitian sebelumnya dan memahami lebih lanjut tentang cara WhatsApp Web menyimpan dan mengelola data secara spesifik. Penelitian lanjutan dapat menggabungkan temuan dari kedua penelitian ini untuk memperkaya pemahaman tentang artefak WhatsApp dalam konteks investigasi forensik yang lebih luas.

(Anglano, 2014) menyelidiki artefak yang ditinggalkan di perangkat Android oleh WhatsApp Messenger aplikasi. Penelitian ini mempertimbangkan semua artefak yang ditinggalkan oleh WhatsApp Messenger dan menunjukkan korelasi informasi yang digabungkan dari berbagai artefak. Data yang diperoleh mencerminkan kegiatan penambahan/penghapusan kontak, pengiriman pesan, dan umpan balik pada pengiriman pesan. Ruang lingkup penelitian ini terbatas pada WhatsApp Messenger di perangkat Android, sedangkan WhatsApp Sistem web tidak ditangani.

Penelitian yang dilakukan oleh Anglano (2014) merupakan upaya penting dalam pemahaman terhadap artefak yang ditinggalkan oleh aplikasi WhatsApp Messenger pada perangkat Android. Penelitian ini mengadopsi pendekatan yang sangat inklusif dengan mempertimbangkan seluruh jenis artefak yang dihasilkan oleh WhatsApp Messenger pada perangkat tersebut. Hasil dari penelitian ini mengungkapkan bahwa ada korelasi yang signifikan antara informasi yang terkandung dalam berbagai jenis artefak yang ditemukan. Artefak-artefak tersebut mencakup data terkait penambahan atau penghapusan kontak, pengiriman pesan, serta umpan balik yang berkaitan dengan pengiriman pesan.

Penting untuk dicatat bahwa penelitian ini memiliki batasan dalam hal ruang lingkupnya. Fokus utama dari penelitian Anglano adalah pada WhatsApp Messenger yang dijalankan di perangkat Android, sehingga WhatsApp Web System tidak menjadi bagian dari investigasi tersebut. Oleh karena itu, temuan dari penelitian ini memberikan pemahaman yang mendalam tentang artefak yang dihasilkan oleh WhatsApp Messenger di perangkat Android, namun belum secara eksplisit menggambarkan artefak yang mungkin dihasilkan oleh WhatsApp Web System. Dalam konteks investigasi forensik yang lebih luas, penelitian

ini dapat menjadi dasar penting untuk memahami jejak digital yang dihasilkan oleh WhatsApp Messenger, baik pada perangkat Android maupun dalam lingkungan WhatsApp Web.

Menurut (Suhendra et al., 2020) Teknologi komputer pada empat tahun terahir ini mengalami perkembangan yang pesat. Bersamaan dengan itu juga berdampak negatif salah satunya adalah berupa kejahatan komputer. Kejahatan komputer akan meninggalkan jejak aktivitas kejahatan, maka perlu dilakukan analisa dengan ilmu dan metode forensik untuk mendapatkan barang bukti. Bagaimana jika terjadi kejahatan komputer pada media penyimpanan komputer berjenis non-volatile memory dan dilakukan secara live forensik. Pada penelitian ini dilakukan proses forensic digital pada Solid State Drive (SSD) .Langkah kerja forensik mengimplementasikan dari National Institute of Standards Technology (NIST).

Penelitian yang dijelaskan oleh Suhendra et al. (2020) mencerminkan perhatian yang semakin besar terhadap masalah keamanan komputer dan kejahatan digital yang semakin meningkat seiring dengan perkembangan teknologi komputer. Perkembangan teknologi komputer dalam beberapa tahun terakhir telah memberikan peluang baru bagi pelaku kejahatan komputer untuk meninggalkan jejak aktivitas mereka, yang dalam konteks forensik komputer menjadi barang bukti penting dalam mengungkap tindakan kriminal. Penelitian ini memusatkan perhatian pada kasus kejahatan komputer yang terjadi pada media penyimpanan non-volatile memory, khususnya Solid State Drive (SSD).

Pendekatan yang digunakan dalam penelitian ini adalah forensic digital, yang merupakan suatu metode analisis forensik untuk mengumpulkan, memeriksa, dan menganalisis bukti-bukti digital. Proses forensic digital pada SSD ini mengimplementasikan kerangka kerja yang ditetapkan oleh National Institute of Standards and Technology (NIST), yang merupakan panduan terkemuka dalam domain forensik digital. Penelitian semacam ini sangat penting dalam mengembangkan metode dan teknik forensik yang dapat mengungkap bukti-bukti digital dengan tepat dan efektif, terutama dalam menghadapi evolusi teknologi yang terus berlanjut dan berkembang.

Penelitian dengan judul "Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST" (Riadi et al, 2023) bertujuan untuk mengungkap bukti digital dan kinerja dari alat forensik yang digunakan untuk mengembalikan data yang telah dihapus berupa multimedia audio dan video pada perangkat Smartphone berbasis android. Penelitian ini menggunakan metode static forensics dengan kerangka kerja yang dikembangkan oleh National Institute of Standard and Technology (NIST). Alat forensik yang digunakan dalam penelitian ini yaitu Oxygen Forensik Pc Suite 2014, MOBILedit Forensik, Belkasoft evidence, dan Magnet Axiom.

Penelitian dengan judul “Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)” (Yudhana et al, 2022) dilakukan dalam upaya mengumpulkan bukti forensik dari aplikasi media sosial WhatsApp menggunakan metodologi DFRWS. Fase forensik digital meliputi identifikasi, penyimpanan, pengumpulan, penyelidikan, analisis, dan penyajian bukti digital kejahatan dunia maya menggunakan aplikasi perangkat lunak MOBILedit Forensic Express dan HashMyFiles.

Berdasarkan studi penelitian yang telah dijabarkan, dapat disimpulkan beberapa poin kunci. Pertama, terdapat keterbatasan dalam penelitian forensik pada aplikasi seluler WhatsApp dan WhatsApp Web. Meskipun banyak penelitian telah difokuskan pada analisis forensik WhatsApp, terdapat kesenjangan pengetahuan yang signifikan terkait penyelidikan forensik pada WhatsApp Web, khususnya terkait penyimpanan terus-menerus dari IndexedDB. Penelitian Vukadinovic (2019) memberikan kontribusi berharga dengan memfokuskan pada artefak WhatsApp di messenger dan web browser, namun tidak secara rinci membahas artefak IndexedDB, menciptakan peluang bagi penelitian lanjutan.

Kedua, studi Vukadinovic (2019) mengungkapkan bahwa aplikasi web WhatsApp tidak menyimpan pesan teks terkirim secara langsung di penyimpanan sisi klien, mengarah pada pemahaman yang lebih baik tentang cara WhatsApp Web mengelola data. Namun, perlu diingat bahwa catatan kapan pesan teks dikirim dan aktivitas panggilan suara/video tidak sepenuhnya tercakup, memberikan celah untuk penelitian tambahan. Integrasi temuan dari penelitian ini dengan penelitian lain, seperti yang dilakukan oleh Anglano (2014), dapat

membentuk dasar yang lebih komprehensif untuk investigasi forensik WhatsApp dalam berbagai konteks penggunaan.

Selanjutnya, penelitian oleh Anglano (2014) menggambarkan korelasi yang signifikan antara berbagai jenis artefak yang ditinggalkan oleh aplikasi WhatsApp Messenger pada perangkat Android. Namun, perlu diakui bahwa penelitian ini memiliki batasan dalam ruang lingkupnya, khususnya ketidakinklusifan terhadap WhatsApp Web System. Oleh karena itu, sementara hasil penelitian ini memberikan wawasan mendalam tentang artefak di perangkat Android, pemahaman tentang WhatsApp Web dalam konteks forensik masih memerlukan eksplorasi lebih lanjut.

Tabel 2.1 Review Penelitian

No	Paper Utama	Keywords	Isu	Metode	Tools yang digunakan	Target
1	(Khoisyilah, 2013)	Android Forensic; Data Acquisition; phases of computer forensics; Mobile Forensics;Whatsapp	Memeriksa aplikasi WhatsApp seluler untuk akuisisi data	Informasi kontak dipulihkan dari selular dengan Forensik Oksigen.	Oxygen Forensic Suite	Akuisisi data pada storage selular
2	(Umar et al., 2017)	Whatsapp; acquisition; NIST parameters; artifact.	Penelitian mengidentifikasi WhatsApp Key/DB Extractor keluar sebagai yang paling hemat biaya dan efisien	Mengevaluasi alat investigasi forensik yang berspesialisasi dalam selular	Whatsapp Key/DB Extraktor	Ektraksi data dari storage selular

3	(Campos et al., 2016)	Autopsy Forensic Browser; data recovery; phases of computer forensics; storage device	Pengambilan Informasi untuk menganalisis alat forensik komputasi (autopsy forensic)	Memulihkan data penyimpanan pada perangkat	The sleuth kit Autopsy	Storage file pada HHD / SSD
4	(Al-Sabaawi et al., 2019)	Android Forensics; Digital Forensics; Mobile Forensics; Mobile Security	Akuisisi data file pada android	Analisis pengambilan data	AFLogical application, FTK imager, Autopsy	Akuisisi data pada storage android
5	(Karpisek et al., 2015)	WhatsApp, reverse engineering, proprietary protocol, signaling protocols, decryption, mobile forensics, digital forensics,	Pencarian data Log panggilan di perangkat selular	Pengembangan alat Python untuk mengonversi file dump Wireshark	Phyton	Memperoleh artefak log panggilan

6	(Actoriano & Riadi, 2018)	IDFIF Version 2, Scene. Forensic, WhatsApp.	penggalian file penyimpanan pesan terenkripsi dari percakapan WhatsApp	Penggunaan FTK Imager untuk mendapatkan file Database SQLite Google Chrome untuk riwayat, cache, dan sesi web	FTK Imager; SQLite	memberikan kerangka investigasi forensik untuk Whatsapp Selular dan aplikasi Whatsapp Web
7	(Mendoza et al., 2015)	IndexedDB; forensic science; persistent storage; web browser forensics; web storage.	Analisis Artefak indexedDB dari peramban	Penggunaan IndexedDB dan SQ Lite	IndexedDB	Menganalisa dan mencari artefak digital pada peramban

8	(Paligu & Varol, 2020)	digital forensics; persistent storage; web browser forensics	Analisa kerentanan basis data	Penggunaan SQLite untuk melihat Vulnerability data	SQLite;	Mengetahui perbandingan IndexedDB dan Android SQLite
9	(Sistem et al., 2021)	Instant Messaging, Vulnerability, ACPO, FTK Imager, OSForensic.	Analisa komparatif dari nilai vulnerability aplikasi WhatsApp	Menggunakan metode Association of Chief Police Officers (ACPO). Artefak	ACPO	menunjukkan nilai Vulrability dari whatsapp browser
10	(Riadi et al., 2023)	OXYGEN Forensics, Smartphone, Whatsapp Web, NIST	Analisa Framework NIST komparasi dengan Tools OXYGEN Forensic	Analisis komparasi akuisisi data	NIST	Menunjukkan metode NIST dengan Tools OXYGEN

BAB 3
Metodologi

3.1 Metodologi yang Dipakai

Metodologi penelitian adalah langkah-langkah yang harus ditempuh untuk kepentingan penelitian. Langkah-langkah tersebut dibuat supaya menjawab masalah yang muncul secara sistematis dan logis sehingga dilakukan proses ilmiah untuk menyelesaikan masalah yang muncul.

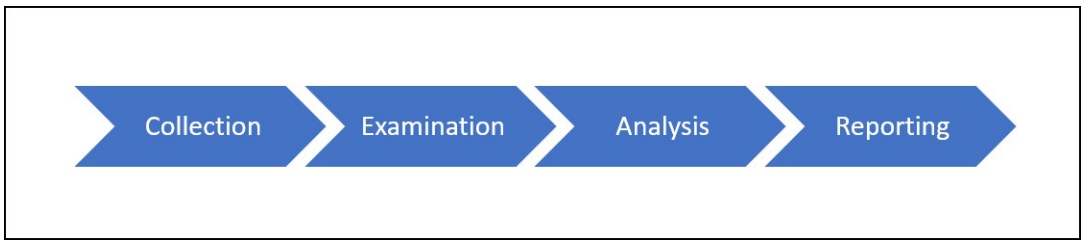
Metodologi penelitian adalah fondasi dari sebuah studi yang memandu peneliti dalam merancang, melaksanakan, dan menganalisis penelitian dengan cara yang terstruktur dan terorganisir. Metodologi penelitian mencakup langkah-langkah dan prosedur yang akan digunakan untuk menjawab pertanyaan penelitian dan mencapai tujuan penelitian yang telah ditetapkan. Metodologi ini juga berperan penting dalam memastikan bahwa penelitian dilakukan dengan cara yang dapat diandalkan dan valid sehingga hasilnya dapat diinterpretasikan secara tepat.

Dalam banyak kasus, metodologi penelitian mencakup pemilihan jenis penelitian, desain penelitian, teknik pengumpulan data, analisis data, serta interpretasi hasil. Peneliti juga harus mempertimbangkan ketersediaan sumber daya, populasi atau sampel yang akan diteliti, dan alat atau instrumen yang akan digunakan. Dengan merencanakan dan mengikuti metodologi penelitian yang tepat, penelitian memiliki dasar yang kuat untuk menghasilkan temuan yang valid dan bermanfaat. Oleh karena itu, pemahaman yang baik tentang metodologi penelitian adalah langkah awal yang penting dalam memulai sebuah penelitian yang berkualitas. Gambar 2.1 menyajikan metodologi penelitian yang digunakan dalam penelitian ini.

Gambar 2.1 Metodologi Penelitian (Riadi et al, 2023)

3.2 Framework yang dipakai

Penelitian ini menggunakan metode yang mengacu pada proses investigasi yang digunakan oleh National Institute of Standard and Technology (NIST). Metode NIST terdiri dari 4 tahapan yaitu Collection, Examination, Analysis, dan Reporting. Metode NIST ini telah terbukti efektif dalam banyak penyelidikan forensik digital karena pendekatan yang sistematis dan akuntabel dalam mengelola dan menganalisis bukti digital. Ini membantu memastikan bahwa temuan yang dihasilkan dapat diandalkan dan dapat digunakan dalam pengadilan atau keperluan investigasi lainnya. Skema metode NIST web forensik disajikan pada Gambar 2.2



Gambar 2.2 Framework NIST (National Institute of Standards and Technology, 2023)

Penjelasan dari skema metode National Institute of Standard and Technology(NIST) adalah sebagai berikut :

1. Collection/Preservation

Tahap ini disebut juga tahap preservasi. Collection merupakan koleksi, atau identifikasi barang bukti yang digunakan berupa perangkat keras yang akan diambil datanya untuk digunakan sebagai bukti digital dari suatu kasus kejahatan digital. Proses ini dilakukan dengan mengikuti langkah pengamanan integritas data.

Proses pengumpulan bukti digital ini harus dilakukan dengan sangat hati-hati dan berdasarkan prinsip-prinsip pengamanan integritas data. Ini berarti bahwa ketika mengambil perangkat keras atau media penyimpanan, perlu diperhatikan agar tidak merusak atau mengubah data yang ada. Dokumentasi yang cermat juga sangat penting untuk mencatat asal usul bukti dan memastikan bahwa rantai bukti tetap utuh dan dapat dipertanggungjawabkan.

Selain itu, dalam tahap Collection ini, forensik digital harus mampu mengidentifikasi dengan tepat barang bukti yang relevan, termasuk perangkat keras seperti hard drive, komputer, atau perangkat mobile yang mungkin memiliki informasi yang berharga dalam kasus penyelidikan. Kesalahan dalam mengidentifikasi atau mengumpulkan bukti pada tahap ini dapat berdampak serius pada validitas dan keberlanjutan penyelidikan forensik digital selanjutnya. Oleh karena itu, ketelitian dan metodologi yang cermat sangat diperlukan pada tahap ini.

2. Examination

Merupakan proses pengambilan data menggunakan tool forensik terpercaya sehingga data yang diperoleh memiliki integritas tinggi. Pada tahap Examination dalam metodologi forensik digital yang mengikuti prinsip-prinsip yang diusulkan oleh National Institute of Standards and Technology (NIST), fokusnya bergeser dari pengumpulan bukti menuju pengujian dan pemeriksaan bukti yang telah dikumpulkan. Pada tahap ini, penting untuk menggunakan alat-alat forensik yang terpercaya dan teruji agar data yang diperoleh memiliki tingkat integritas yang tinggi.

Proses pemeriksaan data melibatkan analisis rinci terhadap perangkat keras dan media penyimpanan yang dikumpulkan. Forensik digital akan menggunakan berbagai teknik

dan perangkat lunak forensik untuk menggali informasi yang tersembunyi dalam perangkat tersebut. Proses ini dapat mencakup pemulihan data yang terhapus, identifikasi adanya malware atau jejak aktivitas berbahaya, serta pengecekan integritas data yang dikumpulkan.

Pada tahap Examination ini, dokumentasi yang akurat juga sangat penting. Forensik harus mencatat setiap langkah yang diambil, temuan yang ditemukan, dan metode analisis yang digunakan. Ini penting untuk mempertahankan integritas bukti digital, serta memberikan dasar yang kuat untuk laporan forensik yang akan dibuat pada tahap selanjutnya. Dengan menggunakan alat forensik yang tepercaya dan metodologi yang tepat, tahap examination menjadi kunci dalam menyelidiki dan mengungkap bukti digital yang relevan dalam kasus kejahatan digital.

3. Analysis

Tahap ini adalah proses menganalisis dan mengevaluasi kembali data yang ditemukan dari hasil *examination*. Pada tahap Examination dalam metodologi forensik digital yang mengikuti prinsip-prinsip yang diusulkan oleh National Institute of Standards and Technology (NIST), fokusnya bergeser dari pengumpulan bukti menuju pengujian dan pemeriksaan bukti yang telah dikumpulkan. Pada tahap ini, penting untuk menggunakan alat-alat forensik yang terpercaya dan teruji agar data yang diperoleh memiliki tingkat integritas yang tinggi.

Proses pemeriksaan data melibatkan analisis rinci terhadap perangkat keras dan media penyimpanan yang dikumpulkan. Forensik digital akan menggunakan berbagai teknik dan perangkat lunak forensik untuk menggali informasi yang tersembunyi dalam perangkat tersebut. Proses ini dapat mencakup pemulihan data yang terhapus, identifikasi adanya malware atau jejak aktivitas berbahaya, serta pengecekan integritas data yang dikumpulkan.

Pada tahap ini, dokumentasi yang akurat juga sangat penting. Forensik harus mencatat setiap langkah yang diambil, temuan yang ditemukan, dan metode analisis yang digunakan. Ini penting untuk mempertahankan integritas bukti digital, serta memberikan dasar yang kuat untuk laporan forensik yang akan dibuat pada tahap selanjutnya.

4. Reporting

Tahap reporting merupakan proses pelaporan hasil analisis yang meliputi informasi data yang berhasil ditemukan yang dijadikan sebagai laporan akhir proses forensik yang dilakukan. Pada tahap ini, hasil analisis yang telah ditemukan selama tahap sebelumnya akan dirangkum dan disajikan dalam bentuk laporan forensik yang lengkap. Laporan forensik ini merupakan dokumen penting yang berisi temuan-temuan, kesimpulan, dan rekomendasi yang diperoleh dari analisis data digital.

Laporan forensik harus disusun dengan hati-hati dan sesuai dengan standar forensik yang berlaku. Isinya harus jelas dan rinci, mencakup semua temuan penting yang berkaitan dengan kasus yang sedang diselidiki. Laporan ini juga harus mencantumkan semua langkah-langkah yang telah diambil selama proses forensik, termasuk metode analisis yang digunakan dan alat-alat yang digunakan dalam investigasi.

Selain itu, laporan forensik juga harus mengikuti aturan hukum yang berlaku dan siap digunakan sebagai bukti dalam pengadilan jika diperlukan. Oleh karena itu, penyusunan laporan harus dilakukan secara teliti dan obyektif. Tahap Reporting adalah tahap terakhir yang menentukan sejauh mana kesuksesan investigasi forensik digital ini, dan laporan yang dihasilkan akan menjadi salah satu output utama yang digunakan dalam proses peradilan atau tindakan lebih lanjut yang berkaitan dengan kasus tersebut.

3.2.1 Persiapan Sistem Tools

Merupakan tahapan dalam mempersiapkan spesifikasi hardware dan software yang digunakan dalam penelitian seperti melakukan perancangan dan implementasi analisis perbandingan recovery data dengan menggunakan flashdisk. seperti melakukan instalasi dan konfigurasi sistem, konfigurasi sistem operasi yang ada dalam komputer fisik yaitu microsoft windows 11 Home. Agar implementasi eksperimental dapat berjalan dengan baik, maka perlu adanya hardware dan software komputer fisik sebagai alat dan bahan penelitian.

Pada tahap ini, persiapan perangkat keras (hardware) dan perangkat lunak (software) menjadi sangat penting dalam penelitian forensik digital. Ini mencakup langkah-langkah seperti perancangan dan implementasi analisis pemulihan data menggunakan perangkat penyimpanan seperti flashdisk. Proses ini juga melibatkan instalasi dan konfigurasi sistem

operasi yang akan digunakan dalam penelitian, dalam hal ini, Microsoft Windows 11 Home. Memastikan bahwa perangkat keras dan perangkat lunak terpasang dan dikonfigurasi dengan benar sangat penting agar eksperimen dan analisis berjalan lancar.

Hardware yang diperlukan dapat mencakup komputer fisik atau perangkat penyimpanan tambahan seperti flashdisk yang akan digunakan dalam eksperimen pemulihan data. Proses konfigurasi sistem operasi pada komputer fisik juga merupakan bagian integral dari persiapan ini, karena akan memastikan bahwa lingkungan eksperimental sesuai dengan yang dibutuhkan untuk penelitian. Langkah-langkah persiapan ini menjadi dasar untuk menjalankan eksperimen forensik digital dengan akurat dan dapat diulang sesuai kebutuhan penelitian. Oleh karena itu, perhatian yang cermat terhadap persiapan perangkat keras dan perangkat lunak sangat penting dalam memastikan validitas dan keberhasilan penelitian ini. Berikut ini alat dan bahan yang digunakan dalam melakukan bahan penelitian eksperimen :

1. Laptop Merk HP 15-ef2127 dengan spesifikasi :

   Processor : AMD Ryzen 5500U Hexa-Core Processor
   Memory : 256 GB SSD / 8 GB RAM
   OS : Windows 10 Home Insider 64-bit

2. FlashDisk 8 GB
3. FTK Imager Tool
4. Sleuth Kit Autopsy Tool
5. Testdisk Recover tool
6. Indexed DB Tools
7. Whatsapp Web

3.2.2 Examination

3.2.2.1 Akuisisi Data

IndexedDB adalah database transaksional NoSQL berorientasi objek yang relatif baru. Dengan memanfaatkan kode JavaScript untuk menangani data. Detail implementasinya dibagikan oleh W3C (WorldWideWeb Consortium) yang membuat strukturnya konstan melalui platform yang berbeda.

Eksperimen pretest menyatakan artefak yang secara inheren ada di lokasi penyimpanan. Perbandingan hasil dari pretest dan treatment menunjukkan artefak apa yang diciptakan oleh perawatan. Dengan kata lain, itu merupakan bukti bahwa artefak yang ditemukan adalah hasil dari perlakuan yang diterapkan.

Tentunya, perbandingan antara hasil pretest dan hasil treatment harus dilakukan dengan cermat dan sesuai dengan kerangka waktu investigasi yang telah ditetapkan. Hasil eksperimen pretest bisa memberikan pandangan awal tentang artefak yang ada di lokasi penyimpanan dan mungkin memberikan petunjuk awal tentang potensi perbedaan setelah penerapan treatment. Namun, penelitian forensik yang lebih mendalam diperlukan untuk memastikan bahwa artefak yang ditemukan adalah hasil dari tindakan atau perlakuan yang telah direncanakan.

Selain itu, eksperimen pretest juga dapat membantu dalam mengevaluasi sejauh mana artefak yang diharapkan dapat dihasilkan oleh treatment tertentu. Ini memungkinkan peneliti forensik untuk mengukur efektivitas metode atau teknik yang digunakan dalam menciptakan atau mengidentifikasi artefak tertentu. Dengan kata lain, pretest dapat membantu dalam mengoptimalkan prosedur forensik untuk menghasilkan artefak yang sesuai dengan kebutuhan penyelidikan. Dalam penelitian forensik, pendekatan ini sangat penting untuk memastikan bahwa bukti yang ditemukan dapat digunakan secara efektif dalam pengadilan atau investigasi yang berhubungan. Langkah-langkah berikut telah dilakukan untuk mengatur lingkungan eksperimental sebelumnya:

1. PC1—Laptop Windows 10 diformat dan diinstal dengan browser Google Chrome.
2. Phone1—Ponsel Android 10-Q yang sudah berfungsi telah diinstal whatsapp.
3. Phone1 dan PC1 ditambahkan sebagai kontak satu sama lain dalam buku telepon internal.

Setelah mengatur lingkungan eksperimental seperti yang telah dijelaskan sebelumnya, penelitian kemudian melanjutkan dengan langkah-langkah selanjutnya. Pada tahap ini, perekaman artefak di lokasi penyimpanan IndexedDB dalam browser Google Chrome dan ponsel Android 10-Q dilakukan. Penggunaan PC1 yang diformat dan sudah terinstal Google Chrome serta Phone1 yang telah memiliki WhatsApp memungkinkan untuk merekam artefak yang dihasilkan selama percakapan atau interaksi melalui WhatsApp Web.

Pengadaan Phone1 dan PC1 sebagai kontak satu sama lain dalam buku telepon internal memungkinkan untuk memulai percakapan melalui WhatsApp dan menciptakan lebih banyak artefak yang dapat diamati dan direkam. Langkah ini merupakan langkah

persiapan penting sebelum memasuki fase eksperimental, di mana data dan artefak yang relevan akan dianalisis lebih lanjut. Dengan mengikuti langkah-langkah ini, penelitian memiliki dasar yang kuat untuk merekam artefak yang diperlukan dalam konteks WhatsApp Web dan perangkat Android yang digunakan.

3.2.2.2 Test Awal

Artefak yang secara inheren ditemukan dalam penyimpanan IndexedDB diuji dengan langkah-langkah berikut :

1. WhatsApp Messenger dimulai di Phone1.
2. web.whatsapp.com dicapai melalui PC1
3. Barcode koneksi di browser PC ditampilkan ke pemutaran Phone1 Messenger
4. Koneksi antara Phone1 dan PC1 dibiarkan menganggur
5. Artefak dikumpulkan dari lokasi penyimpanan Chrome IndexedDB di PC1

Pada tahap ini, penelitian menguji artefak yang secara inheren ada dalam penyimpanan IndexedDB melalui serangkaian langkah-langkah eksperimental yang telah dirinci. Pertama, WhatsApp Messenger diinisialisasi di Phone1, yang merupakan langkah awal untuk memulai proses komunikasi melalui WhatsApp. Kemudian, web.whatsapp.com diakses melalui PC1, yang akan menghubungkan aplikasi WhatsApp Web di browser tersebut. Proses koneksi antara Phone1 dan PC1 diinisiasi dengan menampilkan kode barcode di browser PC yang harus dipindai oleh Phone1 Messenger. Setelah koneksi antara perangkat dibuat, langkah selanjutnya adalah membiarkannya menganggur, yang menciptakan artefak yang diperoleh dari lokasi penyimpanan Chrome IndexedDB di PC1.

Eksperimen ini dirancang untuk merekam artefak yang dihasilkan selama proses interaksi antara Phone1 dan PC1 melalui WhatsApp Web. Dengan mengikuti langkah-langkah ini, penelitian dapat memeriksa dan menganalisis artefak yang relevan dalam penyimpanan IndexedDB, yang merupakan langkah penting untuk memahami bagaimana teknologi ini digunakan dalam konteks WhatsApp Web dan bagaimana data dan informasi tersimpan dalam perangkat yang relevan.

3.2.2.3 Treatment

Treatment adalah aktivitas yang dilakukan dengan WhatsApp Messenger dan Web Aplikasi untuk membuat artefak pada penyimpanan IndexedDB. Kegiatan dibuat sesuai dengan pengamatan perilaku umum pengguna dengan browser web dan aplikasi komunikasi messenger.

Ketika informasi aktivitas yang tersimpan diperiksa di WhatsApp Messenger dan Web, aktivitas-aktivitas berikut ini diamati dari semua aktivitas di :

1. Pesan Teks
2. Mengirim pesan media termasuk video dan gambar; gambar termasuk file jpeg dan file, gif, dan menampilkan file yang ditransfer
3. Panggilan suara
4. Panggilan video
5. Memblokir dan membuka blokir kontak
6. Menampilkan info kontak pengguna

Selain itu, dalam penyelidikan dan eksplorasi dilakukan untuk menemukan potensi penelitian, beberapa catatan kehadiran pengguna diamati. Treatment dalam penelitian ini merupakan langkah-langkah yang sengaja diambil untuk menciptakan artefak dalam penyimpanan IndexedDB. Aktivitas-aktivitas yang dilakukan selama treatment dirancang sesuai dengan pengamatan terhadap perilaku umum pengguna dalam penggunaan browser web dan aplikasi komunikasi messenger. Penelitian ini mengamati berbagai aktivitas yang tercatat dalam WhatsApp Messenger dan Web Aplikasi, termasuk pengiriman pesan teks, media seperti gambar dan video, panggilan suara, panggilan video, pengelolaan kontak seperti pemblokiran dan pembukaan blokir, serta informasi kontak pengguna.

Dalam upaya penyelidikan dan eksplorasi potensial dalam penelitian ini, catatan kehadiran pengguna juga menjadi perhatian. Observasi ini mengambil peran penting dalam memahami bagaimana pengguna berinteraksi dengan aplikasi WhatsApp Web dan bagaimana keberadaan mereka tercatat dalam penyimpanan IndexedDB. Melalui treatment ini, penelitian dapat mengidentifikasi dan merekam artefak-arteafk penting yang dihasilkan oleh aktivitas-aktivitas tersebut, yang akan menjadi dasar bagi analisis dan temuan yang

kemudian akan dipresentasikan dalam penelitian ini. Berdasarkan perilaku yang diamati, langkah-langkah berikut dibangun sebagai treatment :

1. Phone1 WhatsApp Messenger terhubung ke PC1 WhatsApp Web Application melalui kode QR
2. Pesan "Ini adalah pesan 1" dikirim dari PC1 (Telepon1 terhubung) ke Phone1
3. Pesan "Ini adalah balasan 1" dikirim dari Phone1 ke PC1
4. Tautan video sampel dikirim dari PC1 ke Phone1
5. Tautan video sampel diterima dari PC1 ke Phone1
6. Video Sample diputar di Phone1
7. Video Sample diputar di PC1
8. Permintaan panggilan video dikirim dari PC1 ke Phone1. Panggilan dijawab dan berlangsung lebih dari 5 detik
9. Phone1 dibawa sekitar dua puluh meter (diperkirakan kira-kira dengan dua puluh langkah) dari PC1
10. Phone1 dibawa kembali ke PC1
11. Telepon1 terputus dari PC1 dan terhubung kembali setelah 5 detik

Berdasarkan perilaku yang diamati, sejumlah langkah-langkah telah dirancang untuk menjadi bagian dari treatment dalam penelitian ini. Langkah-langkah ini menggambarkan serangkaian aktivitas yang mencerminkan penggunaan WhatsApp Messenger dan Web Application. Treatment dimulai dengan menghubungkan Phone1 WhatsApp Messenger ke PC1 WhatsApp Web Application menggunakan kode QR. Setelah koneksi berhasil, langkah-langkah berikutnya mencakup pengiriman pesan teks antara PC1 dan Phone1, pertukaran tautan video sampel, pemutaran video sampel di kedua perangkat, serta inisiasi panggilan video dari PC1 ke Phone1 yang dijawab dan berlangsung lebih dari 5 detik.

Selanjutnya, treatment juga mencakup adegan di mana Phone1 dibawa sekitar dua puluh meter (sekitar dua puluh langkah) dari PC1, menunjukkan perubahan dalam jarak antara perangkat tersebut, dan kemudian Phone1 dibawa kembali ke dekat PC1. Langkah-langkah ini dirancang untuk menciptakan berbagai situasi yang dapat menghasilkan artefak dalam penyimpanan IndexedDB dan kemudian dianalisis dalam penelitian ini.

BAB 4
Hasil dan Pembahasan

Dalam bab ini, kami akan membahas hasil penelitian kami yang berkaitan dengan penerapan web forensik pada WhatsApp Browser dengan menggunakan Framework NIST (National Institute of Standards and Technology) yang simulasinya terlampir pada lampiran 1.1. Kami akan memulai dengan menjelaskan aspek penting dari teknologi yang digunakan dalam penelitian ini, yakni IndexedDB.

IndexedDB adalah sebuah basis data transaksional NoSQL yang berorientasi objek. Teknologi ini relatif baru dan menggunakan kode JavaScript untuk mengelola data di sisi klien. Detail implementasinya diatur oleh W3C (World Wide Web Consortium), yang membuat strukturnya tetap konsisten di berbagai platform. Salah satu karakteristik penting IndexedDB adalah penggunaan struktur B-tree yang efisien untuk operasi basis data. Google Chrome, Firefox, dan Opera adalah beberapa dari banyak browser yang telah mendukung IndexedDB sejak beberapa tahun terakhir.

Kami juga akan membahas tantangan keamanan yang muncul dalam konteks penggunaan IndexedDB dalam investigasi forensik web. Sistem Kebijakan Asal Sama (Same Origin Policy) yang diterapkan oleh browser membatasi akses dari satu asal (origin) ke asal lain. Meskipun demikian, kami akan menyoroti potensi investigasi lebih lanjut yang terkait dengan penggunaan teknologi LevelDB oleh Google Chrome, yang dapat membuka peluang unik dalam mengungkap informasi tersembunyi.

IndexedDB adalah basis data transaksional NoSQL berorientasi objek yang relatif baru. Ia menggunakan kode JavaScript untuk mengelola data di sisi klien. Detail implementasinya dibagikan oleh W3C (World Wide Web Consortium), yang membuat strukturnya tetap konsisten melalui berbagai platform. Menurut spesifikasi W3C, IndexedDB menggunakan struktur B-tree untuk operasi basis data yang efisien. B-tree adalah struktur data yang memungkinkan manipulasi data secara efisien dalam basis data yang sangat besar. Google Chrome mulai mendukung IndexedDB secara parsial pada tahun

2012 dengan Chrome 11 dan mendukung penuh sejak tahun 2017. Begitu pula dengan browser web utama seperti Firefox dan Opera, mereka telah menyediakan dukungan penuh untuk IndexedDB sejak tahun 2017.

SQLite umumnya digunakan untuk sebagian besar teknologi penyimpanan browser umum seperti riwayat dan bookmark di semua browser web utama. Begitu pula dengan Mozilla Firefox, mereka menggunakan SQLite untuk mendukung IndexedDB. Namun, Google Chrome mengumumkan bahwa mereka mengimplementasikan IndexedDB di atas LevelDB, sebuah teknologi yang dikembangkan oleh Google sejak tahun 2003. Implementasi LevelDB memberikan keuntungan bagi Chrome karena diimplementasikan untuk operasi cepat pasangan kunci-nilai. Studi benchmark pada tahun 2011 yang membandingkan keunggulan LevelDB dibandingkan SQLite v3 menunjukkan bahwa LevelDB lebih cocok untuk pembaruan batch browser web. Karena standar operasi IndexedDB ditetapkan oleh W3C, teknologi LevelDB di Google Chrome mengadopsi penggunaan serupa IndexedDB melalui perintah JavaScript. Penyimpanan LevelDB menyimpan kontennya dalam file .ldb. File ini terkunci untuk melindungi isinya sesuai dengan Kebijakan Asal Sama (Same Origin Policy). Selain itu, file .log dan MANIFEST juga disimpan di lokasi yang sama. Ketika basis data dibuka, informasi dalam file .log dikonversi menjadi titik data (*datapoints*) dan file MANIFEST diperbarui dengan informasi tentang titik data yang diketahui. Titik data dapat dibaca untuk file .ldb, sedangkan file .log berisi informasi yang diencode dalam UTF (Unicode Transformation Format-16) serta entri biner.

Tingkat tertinggi dalam IndexedDB adalah basis data. Oleh karena itu, langkah pertama untuk membuat penyimpanan IndexedDB adalah dengan menetapkan skema basis data. Basis data ditetapkan dengan versi tertentu. Basis data ini pada gilirannya berisi objek toko yang mirip dengan tabel pada basis data tradisional. Jika versi baru basis data didefinisikan dengan indikasi adanya peningkatan pada basis data, maka fungsi *onupgradeneeded* dipanggil untuk membuat kembali objek toko. Jika tidak, fungsi onsuccess dipanggil, di mana objek toko diambil dari penyimpanan yang ada. Begitu pula, dalam percobaan pertama, fungsi *onupgradeneeded* membuat objek toko. Berikut adalah

contoh inisiasi basis data dalam kode JavaScript. Gambar 4.1 menunjukkan inisiasi basis data di IndexedDB menggunakan kode Javascript yang digunakan.

```
// Membentuk basis data dan objectstore
var db;
var request = window.indexedDB.open("newStudyDatabase", 1);

// Jika terjadi kesalahan
request.onerror = function(event) {
  // penanganan kesalahan
}

// Ketika basis data berhasil terbentuk
request.onsuccess = function(event) {
  db = request.result; // jika berhasil, mendapatkan basis data
}

// Jika kita membutuhkan versi baru dari basis data, atau ini adalah panggilan pertama
request.onupgradeneeded = function(event) {
  var db = event.target.result;
  var objectStore = db.createObjectStore("studyObjectStore", {keyPath: "id"});
}
```

Gambar 4.1 Inisiasi Basis Data di IndexedDB

Untuk menambahkan informasi ke objek *store*, kita perlu mendefinisikan transaksi pada basis data dan objek *store* tersebut. Transaksi ini digunakan untuk memanggil fungsi add dan dapat ditangani dengan fungsi *onsuccess* dan *onerror*. Fungsi baca yang serupa dapat dipanggil pada transaksi untuk mengambil data. Gambar 4.2 menunjukkan pembuatan data, penyisipan, dan pengambilan data dari objek *store* yang didefinisikan pada Gambar 4.1.

```
// Penyisipan berhasil
request.onsuccess = function(event) {
  // menangani penyisipan yang berhasil
}

// Kesalahan penyisipan
request.onerror = function(event) {
  // menangani kesalahan penyisipan
}

var request = db.transaction(["studyObjectStore"], "readwrite")
  .objectStore("studyObjectStore")
  .get({"01"});

// Pengambilan berhasil
request.onsuccess = function(event) {
  // melakukan sesuatu dengan data yang diambil, misalnya 'request.result.namaRekaman'
}

// Kesalahan pengambilan
request.onerror = function(event) {
  // menangani kesalahan pengambilan
}
```

Gambar 4.2 Pembuatan, Penyisipan, dan Pengambilan Data

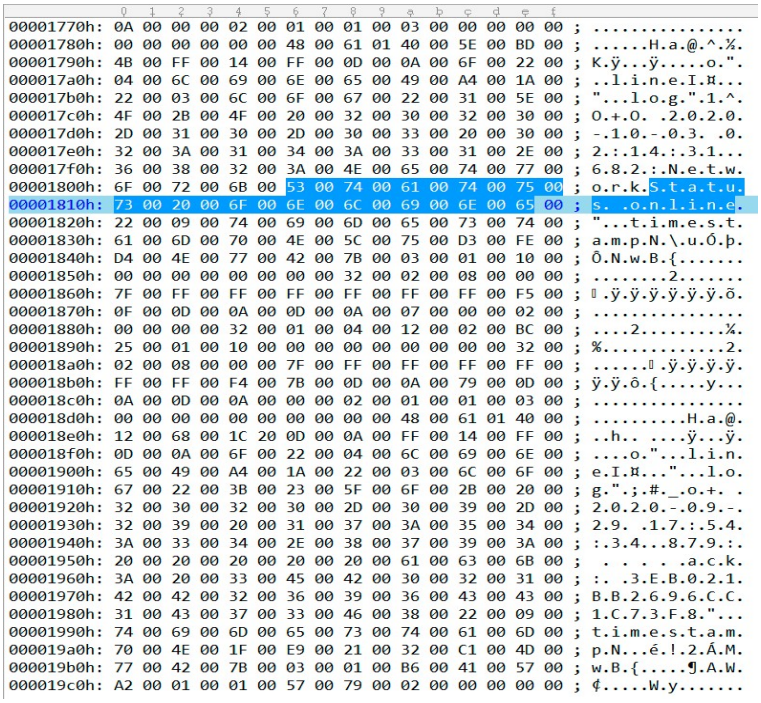
Browser mengamankan konten dari satu asal (origin) dari asal lain dengan menerapkan Kebijakan Asal Sama (Same Origin Policy). Ini berarti informasi yang diperoleh dari satu sumber diisolasi dan hanya dapat diakses oleh sumber yang sama. Dengan cara ini, sebuah situs web yang terbuka dalam tab browser tidak dapat mengakses konten dari situs lain. IndexedDB juga tunduk pada Kebijakan Asal Sama. Oleh karena itu, basis data tidak dapat dibangun dan diakses oleh konten IndexedDB dari situs web lain. Hal ini membuat investigasi forensik relatif lebih sulit karena penyelidik tidak dapat mengakses konten IndexedDB dari suatu asal melalui program web yang dikembangkan dalam JavaScript. Untungnya, LevelDB menyimpan file log yang berisi informasi yang sama dengan yang tercatat dalam basis data. File-file ini diberi nama berdasarkan versi basis data, dan file baru dengan nama versi yang berbeda dibuat ketika terjadi pembaruan pada basis data. Namun, dengan teknik file carving, memungkinkan untuk mengambil kembali file-file tersebut bahkan setelah file-file baru menggantikan yang lama, sehingga potensial tersedia untuk investigasi. Informasi lebih lanjut tentang cara mendapatkan file log dan investigasi forensiknya akan disajikan dalam bagian-bagian berikutnya sesuai dengan alur pada NIST.

4.1 Tahap *Collection*

Sebagai prosedur untuk eksperimen semu, dilakukan pengumpulan data dan uji independen tanpa kegiatan yang dilakukan pada perlakuan. Menggunakan langkah-langkah lengkap dilakukan setelah pengaturan lingkungan eksperimental. Pengumpulan dan pengamatan terhadap artefak yang tercipta dalam file penyimpanan IndexedDB di PC1 disajikan dalam bagian ini.

Lokasi penyimpanan file IndexedDB untuk WhatsApp Web pada peramban Chrome yang digunakan dalam sistem operasi Windows 10 Single Language adalah "C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\IndexedDB". File-file tersebut memiliki format .ldb yang berbeda dengan format .sqlite pada Firefox dan .dat pada Internet Explorer. Setiap asal situs web memiliki satu file .ldb untuk penyimpanan IndexedDB. Umumnya, file-file .ldb bisa dibaca sebagian oleh manusia [6]. Namun, file-file yang dibuat untuk WhatsApp Web tampaknya hampir sepenuhnya dapat dimengerti oleh

pembaca manusia. Kejelasan file-file penyimpanan IndexedDB WhatsApp Web membuat teknologi IndexedDB sangat cocok untuk investigasi forensik WhatsApp. Selain itu, diperhatikan bahwa file .log dibuat dari file .ldb selama operasi. Lokasi file .log sama dengan file .ldb. File-file ini berisi baris-baris dengan karakter yang tidak dapat dibaca oleh manusia karena berisi data biner untuk seluruh koleksi objek toko dari asal situs web dalam basis data. Namun, catatan-catatan yang terlihat berharga untuk investigasi forensik terlihat hadir dalam bentuk yang dapat dibaca oleh manusia yang diencode dalam UTF-16 di file log yang sama. Gambar 4.3 menunjukkan contoh file .log yang disimpan di lokasi penyimpanan file IndexedDB. Bagian yang di-highlight menunjukkan Catatan Status Jaringan Online tepat setelah cap waktu dalam format yang dapat dibaca oleh manusia.



Gambar 4.3 File .log dari lokasi penyimpanan file IndexedDB Google Chrome

4.2 Tahap *Examination*

Selanjutnya, data yang dikumpulkan di uji dalam bentuk treatment. *Treatment* yang diberikan kepada subjek telah menghasilkan pembentukan artefak pada file penyimpanan IndexedDB pada peramban Chrome. Diperhatikan bahwa sejumlah besar artefak terbentuk

dengan perlakuan tersebut. Aplikasi ini mencatat operasi teknis, seperti sinkronisasi dan asinkronisasi perangkat, pengakuan dari server tentang ketersediaan kontak, dll. Kami mencoba mempersempitnya menjadi catatan-catatan yang dapat menjadi bukti penting untuk investigasi. Artefak-artefak yang kami anggap signifikan tercantum dalam bagian ini dengan perlakuan yang memicunya. Artefak-artefak yang terbentuk berikut ini menunjukkan tindakan pengguna dalam Aplikasi WhatsApp Web. Ringkasan artefak yang terbentuk tercantum dalam Tabel 4.1 dengan tindakan perlakuan yang sesuai.

Tabel 4.1 Hasil *Treatment* dan Artefak Beserta Perbandingannya

Treatment	Artefak	Perbandingan dengan SQLite
Pesan "Ini adalah pesan 1" dikirim dari PC1 ke Phone2	Rekaman Chat Tindakan Kirim Pesan	SQLite: Query untuk melihat log pesan yang dikirim
Pesan "Ini adalah balasan 1" dikirim dari Phone2 ke PC1	Rekaman Chat Tindakan Terima Pesan	SQLite: Query untuk melihat log pesan yang diterima
Video "Sample" diputar di Phone1	Rekaman Media Load pada Data yang Dimuat	SQLite: Query untuk melihat log pemutaran video di Phone1
Video "Sample" diputar di PC1	Rekaman Media Load pada Data yang Dimuat	SQLite: Query untuk melihat log pemutaran video di PC1
Video "Sample" diputar di Phone2	Rekaman Media Load pada Data yang Dimuat	SQLite: Query untuk melihat log pemutaran video di Phone2
Permintaan panggilan video dikirim dari Phone2 ke Phone1. Panggilan tidak dijawab.	Recv: s<Number> [Call, ...]	SQLite: Query untuk melihat log panggilan video tidak dijawab
Permintaan panggilan video dikirim dari Phone2 ke Phone1. Panggilan dijawab dan berlangsung lebih dari 5 detik.	Recv: s<Number> [Call, ...]	SQLite: Query untuk melihat log panggilan video yang dijawab dan berlangsung lebih dari 5 detik
Phone1 dibawa sekitar dua puluh meter dari PC1	Tindakan Rekaman Tidak Tersedia	SQLite: Query untuk melihat apakah ada catatan ketika perangkat terputus
Phone1 dibawa kembali ke dekat PC1	Tindakan Rekaman Tersedia	SQLite: Query untuk melihat apakah ada catatan ketika perangkat terhubung kembali
Phone1 terputus dari PC1 dan terhubung kembali setelah 5 detik.	Stream:rememberMe: true Record	SQLite: Query untuk melihat catatan status jaringan online dan offline
Aplikasi WhatsApp Messenger pada Phone1 terhubung ke Aplikasi WhatsApp Web pada PC1 melalui kode QR.	Network Status Online Record	SQLite: Query untuk melihat catatan status jaringan online saat koneksi antara aplikasi WhatsApp di Phone1 dan WhatsApp Web di PC1 terhubung

Adapun tindakan-tindakan yang tidak menghasilkan artefak yang bermakna tidak tercantum dalam tabel ini. Ketika tab pengguna pada browser yang mengandung Aplikasi

WhatsApp Web aktif, rekaman "Network Status Online" dibuat dalam penyimpanan IndexedDB. Rekaman ini berisi informasi yang berulang mengenai label rekaman dan waktu pembuatan pada tubuh rekaman tersebut. Contoh dari rekaman ini dapat ditemukan pada Tabel 4.2.

Tabel 4.2 Rekaman *Network Status Online*

Rekaman	***Output***
Network Status Online	*{line: 2011, log: "*O=? 2022-11-19 21:10:42.044:NetworkStatus online", timestamp: 1598763047703.76} line: 2011, log: "*O=? 2022-11-19 21:10:42.044:NetworkStatus online", timestamp: 1598763047703.76} timestamp: 1598763047703.21*

"*Network Status Online*" memiliki nilai forensik yang signifikan karena menjadi indikator waktu ketika pengguna berinteraksi dengan aplikasi. Dalam penyelidikan, dakwaan terhadap seorang tersangka sering kali bergantung pada timestamp bukti. Kesesuaian pengaturan waktu antara timestamp bukti dan interaksi pengguna dengan komputer dapat menjadi indikator yang kuat bahwa seorang tersangka bertanggung jawab atas bukti tersebut.

Rekaman "Stream:rememberMe" dibuat ketika pengguna menghubungkan *browser* komputer yang menjalankan aplikasi WhatsApp Web dengan ponsel menggunakan WhatsApp Messenger. Rekaman ini berisi informasi tentang label record dan timestamp di dalamnya. Contoh dari rekaman ini dapat dilihat pada tabel 4.3.

Tabel 4.3 Rekaman Stream:rememberMe

Rekaman	***Output***
Stream:rememberMe	*{line: 2012, log: "*O=? 2022-11-19 21:10:42.059:Stream:rememberMe: true", timestamp: 1598763047704.23} line: 2012 log: "*O=? 2022-11-19 23:50:47.059:Stream:rememberMe: true" timestamp: 1598763047704.44*

Rekaman "Stream:rememberMe" digunakan ketika tersangka menginginkan WhatsApp Messenger untuk mengingat komputer tersebut. Preferensi ini dapat menunjukkan penggunaan berulang komputer oleh tersangka. Laporan investigasi forensik digital berisi informasi mengenai perilaku tersangka, yang kemudian dipresentasikan di

pengadilan untuk memahami motif tersangka dengan lebih baik. Interaksi yang sering dilakukan oleh tersangka dengan komputer yang menjadi bukti penting karena memberikan wawasan tentang karakteristik perilaku tersangka.

Sejumlah rekaman yang disebut "MediaLoad:video.onloadeddata" dibuat ketika sebuah file media, seperti video, dibuka baik pada aplikasi messenger maupun aplikasi web. Rekaman ini berisi penanda waktu yang menunjukkan waktu pembukaan file media tersebut, beserta labelnya. Contoh rekaman media load dapat dilihat pada Tabel 4.4.

Tabel 4.4 Rekaman MediaLoad:video.onloadeddata

Rekaman	***Output***
MediaLoad:video.onloadeddata	*{line: 2330, log: "*O=? 2022-11-19 21:10:42.768:MediaLoad:video.onloadeddata #1", timestamp: 1598763200175.39}* *Line: 2330* *log: "*O=? 2022-11-19 21:10:42.768:MediaLoad:video.onloadeddata #1"* *timestamp: 1598763200175.39*

Banyak kasus yang melibatkan bukti digital terkait dengan gambar dan video ilegal tentang anak di bawah umur. Selain itu, terdapat juga kasus yang berkaitan dengan masalah privasi antara pasangan yang melibatkan distribusi dan eksposisi media pribadi. Dalam kasus-kasus ini, informasi mengenai kapan media diakses dan seberapa sering diakses menjadi sangat penting dalam penyelidikan.

Tabel 4.5 Rekaman Recv: s<Number> [Call, ...]

Rekaman	***Output***
Recv: s<Number> [Call, ...]	*{line: 2345, log: "*O=? 2022-11-19 21:10:42.325: recv: s29 [Call, ...]", timestamp: 1598763231721.61}* *Line: 2345* *log: "*O=? 2022-11-19 21:10:42.325: recv: s29 [Call, ...]"* *timestamp: 1598763231721.61*

Rekaman "Recv: s<Number> [Call, ...]" dibuat ketika terjadi panggilan video atau suara melalui messenger atau aplikasi web. Informasi timestamp mengenai durasi panggilan aktif disertakan dalam data dengan label rekaman tersebut. Aplikasi ini mencatat log ini beberapa kali selama panggilan berlangsung. Selain itu, teramati bahwa panggilan yang tidak

terjawab juga dapat menghasilkan rekaman "Recv: s<Number> [Call, ...]". Sebagai contoh, panggilan suara yang tidak dijawab dan berdering selama 1 menit dapat menghasilkan lebih dari sembilan contoh rekaman tersebut. Tabel 4.5 menunjukkan contoh dari jenis rekaman ini.

Mengetahui rentang waktu panggilan video atau suara yang aktif dapat memberikan informasi mengenai kapan panggilan penting dilakukan. Hal ini dapat menjadi sangat berguna terutama dalam kasus-kasus di mana penyelidikan dilakukan dengan melibatkan kedua pihak yang melakukan panggilan tersebut.

Rekaman dengan label "action, presence, unavailable" dibuat ketika aplikasi klien mengirimkan informasi kehadirannya ke server WhatsApp. Catatan ini menunjukkan bahwa pengguna sedang offline atau tidak aktif menggunakan aplikasi. Namun, kami telah mengamati bahwa ketika pengguna menjauh dari komputer dengan telepon terhubung melalui WhatsApp Messenger, kedua perangkat menjadi tidak aktif dalam penggunaan aplikasi dan menciptakan catatan "action, presence, unavailable". Hal ini terjadi bahkan jika tab aplikasi web tetap terbuka.

Koneksi antara perangkat tidak bergantung pada jarak. Hal ini terbukti dari tidak terputusnya koneksi ketika terdapat jarak antara perangkat. Selain itu, koneksi dapat terbentuk ketika komputer terhubung melalui Wi-Fi dan perangkat Android terhubung melalui penyedia layanan. Bukti awal menunjukkan adanya mekanisme timeout untuk pembuatan catatan ini. Hal ini didukung oleh fakta bahwa catatan ini dibuat dalam waktu delapan hingga sebelas detik. Namun, informasi lebih lanjut dapat diperoleh dengan memeriksa lalu lintas jaringan yang dihasilkan oleh perangkat selama koneksi. Dalam penelitian ini, fokus kami adalah pada penyimpanan IndexedDB di komputer tersangka dan artefak yang tercipta di dalamnya melalui perlakuan eksperimen yang diberikan.

Waktu awal ketika pengguna menjauh dari komputer dicatat dengan timestamp pada label catatan. Namun, ketepatannya tidak terlalu akurat karena catatan tersebut dibuat setelah delapan hingga sebelas detik. Perlu dicatat bahwa ketika koneksi antara telepon dan komputer bermasalah, catatan "action, presence, unavailable" kadang-kadang ditambahkan dengan durasi singkat antara sepuluh hingga dua puluh detik sebelum catatan "action,

presence, available" ditambahkan kembali. Selama percobaan, kami telah mengamati catatan seperti itu. Penting juga untuk mencatat bahwa ketika durasi ketiadaan pengguna cukup lama, beberapa catatan ditambahkan. Demikian pula, catatan "presence, available" kadang-kadang ditambahkan tanpa pengguna benar-benar offline atau menjauh dari komputer. Tabel 4.6 menunjukkan contoh dari jenis catatan ini.

Tabel 4.6 Rekaman Action, Presence, Unavailable

Rekaman	***Output***
action, presence, unavailable	*{line: 2406, log: "*O=? 2022-11-19 21:10:42.199:sending: 1598763310.–44, action, presence, unavailable", timestamp: 1598763310592.405}* *Line: 2406* *log: "*O=? 2022-11-19 21:10:42.199:sending: 1598763310.--44, action, presence, unavailable"* *timestamp: 1598763310592.405*

Dalam kasus yang melibatkan bukti digital, salah satu pembelaan yang sering diajukan adalah klaim bahwa tersangka bukanlah orang yang menggunakan komputer pada saat terjadinya pelanggaran. Perangkat pribadi seperti ponsel cenderung digunakan oleh satu individu. Sementara komputer dapat digunakan oleh lebih dari satu pengguna, hal ini lebih umum terjadi dalam bisnis dengan komputer cetak, *database*, dan tujuan umum. Catatan yang menunjukkan kapan tersangka menjauh dari komputer merupakan informasi yang berpotensi penting untuk mendukung atau menentang pembelaan bahwa mereka tidak hadir pada saat pelanggaran terjadi.

"Send<code>, action, message, chat" dan "recv<code>, action, msg, relay, chat" adalah rekaman yang dibuat ketika sebuah pesan teks dikirim dari satu akun ke akun lainnya. Aplikasi ini mencatat informasi yang lebih detail mengenai proses pengiriman pesan dan rincian pengirimannya. Namun, pesan-pesan ini dapat bervariasi dalam hal keterlambatan jaringan dan status server. Dalam analisis periode waktu, terbukti bahwa rekaman *Send-Receive* Sederhana sudah cukup untuk menandai aktivitas pengiriman pesan. Rekaman *Send-Receive* ini mencakup timestamp dan label rekaman. Selain itu, terdapat kode identifikasi seperti 3EB0A2F3697 . . . 6B3365 dalam rekaman tersebut. Kode ini tampaknya berisi informasi tentang akun yang menerima pesan atau akun yang mengirim pesan. Oleh karena

itu, kode ini dapat digunakan untuk memisahkan percakapan antara berbagai akun. Namun, tidak ada cara yang dapat diidentifikasi untuk mengetahui akun mana yang sesuai dengan kode tersebut.

Tabel 4.7 Rekaman Send Action Message

Rekaman	***Output***
Send<code>, action, message, chat *recv<code>, action, msg, relay, chat*	*{line: 2267, log: "*O=? 2022-11-19 21:10:42.554: send: 3EB00698747 . . . 00B6AB,* *action, message, chat,,3EB0069874767200B6AB", timestamp: 1598763101996.04}* *line: 2267* *log: "*O=? 2022-11-19 21:10:42.554: send: 3EB0069874767200B6AB,* *action, message, chat,,3EB0069874767200B6AB"* *timestamp: 1598763101996.04*

Dalam penyelidikan digital di mana pemeriksa tidak memiliki akses ke kredensial WhatsApp tersangka, informasi tentang kapan tersangka mengirim dan menerima pesan dapat berguna untuk menentukan tindakan yang dilakukannya pada waktu tertentu.

4.3 Tahap *Analysis*

Informasi yang tercatat dalam IndexedDB storage oleh WhatsApp Web Application memberikan informasi yang luas tentang tindakan seorang pengguna. Informasi ini direkam dalam format yang mencakup waktu tindakan dalam format UNIX epoch time, selain format yang dapat dibaca oleh manusia. UNIX epoch time adalah jumlah detik sejak 1 Januari 1970 (tengah malam UTC/GMT). Oleh karena itu, waktu ini berada dalam zona waktu yang berbeda dengan waktu yang dapat dibaca oleh manusia dalam catatan. Misalnya, 1598763047703.76 dari Tabel 4.2 sesuai dengan "Sabtu, 19 November 2022 13:10:42 GMT". Pada rekaman yang sama, waktu terlihat sebagai "2022-11-19 21:10:42.044" karena komputer subjek berada di zona waktu (GMT+8). Rekaman-rekaman ini dibagi dengan penomoran yang memudahkan penguraian. Dapat diamati dalam Tabel 4.2 hingga 4.7 bahwa informasi tersebut berulang dalam format yang berbeda. Set pertama dari catatan-catatan ini mencantumkan informasi dalam tanda kurung, sedangkan rekaman selanjutnya memisahkan waktu, label, dan nomor baris ke dalam baris yang berbeda. Hal ini mengindikasikan desain yang bermaksud untuk mendukung berbagai metode pengumpulan informasi.

Diamati bahwa tindakan yang dilakukan dengan WhatsApp Messenger Application di ponsel direkam dalam WhatsApp Web IndexedDB storage selama koneksi aktif. Jika seorang pengguna menjawab panggilan video atau menonton video melalui aplikasi dari ponsel, rekamannya akan ditemukan di komputer.

Karena tindakan yang dilakukan oleh pengguna dalam WhatsApp Messenger dan Web Applications disimpan dalam file LevelDB yang dapat dengan mudah diuraikan dan dimanipulasi oleh tersangka, dapat timbul kekhawatiran tentang privasi. Meskipun tidak ada percakapan yang disimpan langsung dalam file ini, jadwal seseorang dalam melihat file media dan informasi tentang waktu yang mereka habiskan dengan komputer mereka dapat dengan mudah dihitung.

Pentingnya temuan ini adalah bahwa tindakan yang dilakukan oleh pengguna dalam WhatsApp Messenger Application di ponsel mereka terekam dengan rinci dalam WhatsApp Web IndexedDB storage selama koneksi aktif. Dengan kata lain, jika seorang pengguna menjawab panggilan video atau menonton video melalui aplikasi dari ponsel mereka, jejak aktivitas ini akan terekam dan dapat diakses dari komputer. Meskipun percakapan tidak tersimpan secara langsung dalam file ini, penelitian ini menggarisbawahi bahwa informasi mengenai kapan seseorang melihat file media dan berapa banyak waktu yang dihabiskan di depan komputer dapat dengan mudah diidentifikasi melalui analisis data ini. Hal ini menunjukkan pentingnya melindungi privasi dalam penggunaan aplikasi seperti WhatsApp Messenger dan menjaga keamanan data pribadi pengguna dari potensi penyalahgunaan.

4.3.1 Implementasi IndexedDB pada Teknologi Browser yang Berbeda

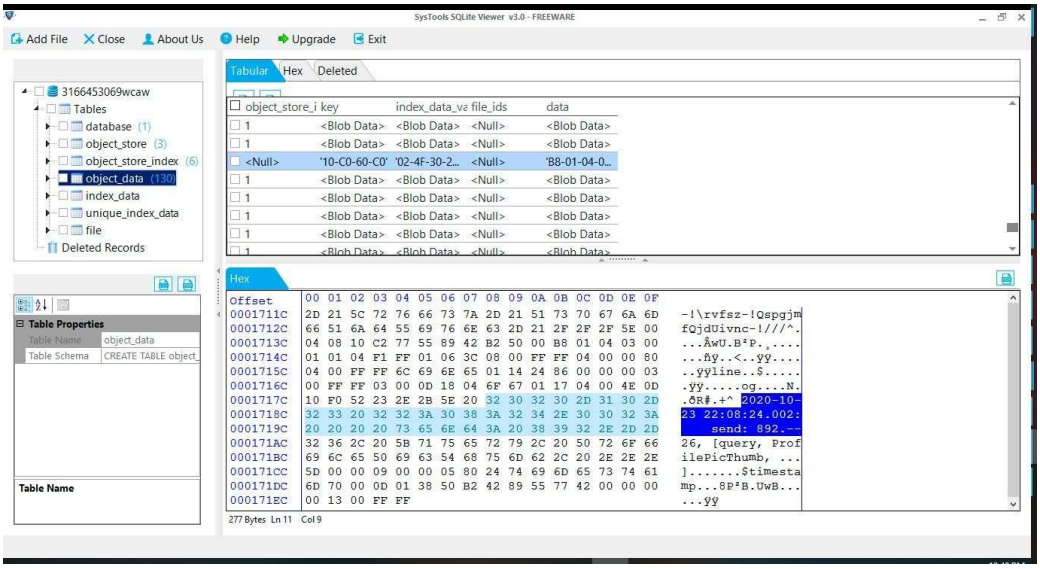
Penelitian ini berfokus pada penyimpanan artefak WhatsApp Web dalam Google Chrome pada IndexedDB yang diimplementasikan dalam LevelDB. Namun, terdapat berbagai implementasi yang berbeda di berbagai browser.

Tabel 4.8 Teknologi IndexedDB pada Berbagai Browser

Browser	Teknologi
Google Chrome	LevelDB
Microsoft Edge	LevelDB
Opera	LevelDB
Mozilla Firefox	SQLite
Internet Explorer	File .dat

Tabel 4.8 merangkum teknologi di balik IndexedDB untuk browser utama. Microsoft Edge dan Opera menggunakan LevelDB untuk IndexedDB seperti Google Chrome. Oleh karena itu, konsep-konsep yang dijelaskan dalam penelitian ini juga berlaku untuk browser-browser ini.

Mozilla Firefox menggunakan file SQLite untuk IndexedDB, yang mudah diakses dengan peramban SQLite. Gambar 4.4 menampilkan file penyimpanan IndexedDB WhatsApp Web yang ditampilkan di peramban SQLite. Penting untuk mencatat bahwa tidak ada mekanisme keamanan yang menghalangi akses ke file SQLite IndexedDB yang digunakan oleh Mozilla Firefox. Internet Explorer menggunakan file .dat untuk seluruh penyimpanan perambannya. File-file ini khusus untuk Internet Explorer dan dapat diakses oleh editor teks mana pun.



Gambar 4.4 Tampilan File SQLite IndexedDB (Paligu & Varol, 2020)

4.3.2 Analisis Menggunakan BrowSwEx

IndexedDB dapat dioperasikan melalui kode JavaScript. Namun, Same Origin Policy mencegah sebuah database yang dibuat oleh localhost atau origin lainnya untuk mengakses konten WhatsApp Web yang disimpan di browser. Oleh karena itu, satu-satunya cara untuk mengakses catatan-catatan tersebut adalah melalui akses langsung ke file yang terdapat di lokasi file IndexedDB Google Chrome. Ketika WhatsApp Web dijalankan di browser

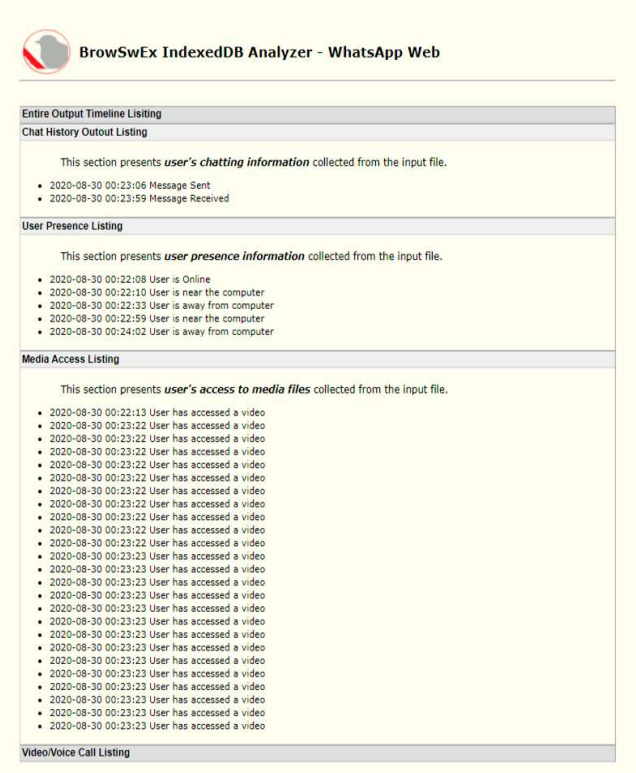
Chrome, sebuah file .ldb dibuat untuk mengandung semua informasi tentang interaksi saat ini maupun sebelumnya dengan aplikasi tersebut. Google Chrome menggunakan LevelDB untuk penyimpanan IndexedDB. LevelDB dikembangkan dengan teknologi C/C++. Oleh karena itu, akses langsung ke file .ldb hanya dapat dicapai menggunakan program C/C++. Namun, seperti yang dibahas dalam bagian latar belakang dan hasil penelitian, file .ldb meninggalkan informasi di file .log yang disimpan di lokasi file yang sama dengan file .ldb. Oleh karena itu, ada dua cara untuk mengumpulkan catatan-catatan IndexedDB WhatsApp Web dari Google Chrome. Cara pertama adalah menggunakan kompiler C dengan library LevelDB. Cara kedua adalah dengan memproses file .log dengan mengurai informasi teks mentah dalam format log. Sebagai bukti konsep, BrowSwEx dikembangkan menggunakan program PHP yang secara sistematis mengurai file .log yang dihasilkan oleh file .ldb. Pseudocode yang digunakan oleh BrowSwEx untuk memproses file .log dapat dilihat pada Tabel 4.9.

Tabel 4.9 Pseudocode Untuk Memproses .log

Pseudocode	***Input***
Memproses file .log	*Jika file input.log tidak ada* *Ekstrak file <numberpattern>.log dari lokasi file Chrome IndexedDB* *Ganti nama file <numberpattern>.log menjadi input.log* *While baris yang harus dibaca di input.log* *Baca sebuah baris* *Jika baris tersebut berisi entri waktu* *While tipe catatan kunci yang harus diperiksa* *Ambil sebuah tipe record* *Jika baris cocok dengan tipe record tersebut* *Konversi tipe record menjadi deskripsi* *Tambahkan waktu dan deskripsi record ke hasil* *else* *continue*

Setelah file .log diproses, hasil yang diperoleh digunakan dalam berbagai fungsi untuk menyajikan informasi yang ditentukan. Alat ini menggunakan fungsi preg_match dan lima fungsi khusus: EntireOutputList(), ChatOutputList(), PresenceOutputList(), MediaAccessOutputList(), dan VideoCallOutputList() untuk menyusun daftar informasi dan mencapai format catatan yang diinginkan yang tercantum dalam bagian sebelumnya.

Gambar alat yang menyajikan informasi dalam rentang waktu dapat dilihat pada Gambar 4.5.



Gambar 4.5 Daftar Rekaman Whatsapp Web di BrowSwEx

4.3.3 Verifikasi Menggunakan BrowSwEx

Hasil pengujian dari Single Case Pretest–Posttest Quasi Experiment berhasil dideteksi oleh BrowSwEx. Namun, jumlah entri yang sangat banyak dan variasi jenis log yang serupa menunjukkan potensi kesalahan. Oleh karena itu, verifikasi lebih lanjut tampaknya diperlukan. BrowSwEx diuji dengan menggunakan Google Chrome Developer Tools. Google Chrome Developer Tools mencantumkan setiap rekaman penyimpanan persisten untuk situs web aktif. Informasi ditampilkan dalam format mentah dengan detail yang sangat lengkap dan tidak ada opsi untuk mencari atau mengurutkan. Agar Google Chrome Developer Tools dapat beroperasi di situs web tersebut, komputer harus aktif dan situs web harus diautentikasi oleh telepon pengguna.

BrowSwEx memparsing file .log yang direkam dari folder penyimpanan file Chrome IndexedDB. Dengan kata lain, analisis dapat dilakukan secara offline tanpa keberadaan kredensial pengguna untuk autentikasi. Pendekatan verifikasi informasi yang ditampilkan oleh BrowSwEx dilakukan dalam dua bagian:

1. Keberadaan catatan yang ditampilkan diperiksa kembali dengan menggunakan Google Chrome Developer Tools.
2. Waktu penggunaan untuk menciptakan artefak diperiksa berdasarkan waktu yang ditampilkan dalam antarmuka pengguna alat tersebut.

4.3.4 Pembatasan BrowSwEx

Untuk mengakses file <numberpattern>.log, lokasi <userprofile> (berbeda untuk setiap nama pengguna) dalam file "WhatsAppWebIDB.php" harus diperbarui. Karena setiap lingkungan berbeda. Dalam beberapa kasus, pengguna perlu secara manual mendapatkan file <numberpattern>.log dari lokasi penyimpanan file IndexedDB, mengganti namanya menjadi input.log, dan menempatkannya di direktori server web. Selain itu, beberapa catatan tampaknya bersifat berulang, misalnya, ketika pengguna memulai panggilan video, catatan "Recv: s<Number> [Call, ...]" dimasukkan ke file IndexedDB beberapa kali untuk entri waktu yang sama. Setelah pertimbangan yang matang, entri berulang ini tidak dihilangkan. Hal ini dikarenakan log yang berbeda mengandung identifikasi yang berbeda yang dapat penting dalam pembuatan kembali hasil investigasi. Meskipun demikian, BrowSwEx adalah alat sumber terbuka dan dapat ditingkatkan oleh pengguna sesuai dengan kebutuhan mereka.

Pengguna perlu memiliki server yang berfungsi untuk memparsing PHP, dan mentransfer file-file alat tersebut ke direktori www mereka agar alat tersebut berfungsi. Peneliti telah menggunakan server WAMP (Windows, Apache, MySQL, dan PHP) dengan PHP dan Apache Server bawaan selama pengembangan BrowSwEx.

4.4 Tahap *Reporting*

Tahap pelaporan dalam kerangka kerja forensik NIST (National Institute of Standards and Technology) adalah langkah penting yang melibatkan dokumentasi temuan dan kesimpulan yang dihasilkan dari analisis data forensik. Berbagai jenis data yang ditemukan diidentifikasi, dianalisis, dan selanjutnya dilaporkan untuk menyajikan temuan dan

kesimpulan kepada pihak berwenang. Tabel 4.2 merangkum temuan dan kesimpulan untuk berbagai jenis data yang ditemukan selama investigasi.

Tabel 4.10 Temuan dan Kesimpulan Investigasi Data WhatsApp Browser

No	Jenis Data	Sumber Data	Temuan	Kesimpulan
1	Teks Pesan	WhatsApp Web IndexedDB	Riwayat pesan terhapus	Pesan telah dihapus
2	Gambar Profil Pengguna	WhatsApp Web IndexedDB	Profil pengguna tidak ada	Profil pengguna tidak aktif
3	Riwayat Panggilan Suara	WhatsApp Web IndexedDB	Riwayat panggilan ada	Aktivitas panggilan terjadi
4	Riwayat Panggilan Video	WhatsApp Web IndexedDB	Riwayat panggilan ada	Aktivitas panggilan terjadi
5	Kontak Diblokir	WhatsApp Web IndexedDB	Kontak yang diblokir ada	Kontak telah diblokir
6	Info Kontak Pengguna	WhatsApp Web IndexedDB	Informasi kontak ada	Info kontak tersedia
7	Log Aktivitas	WhatsApp Web IndexedDB	Log aktivitas ditemukan	Aktivitas pengguna tercatat
8	Lokasi Pengguna	GPS Device Log	Data lokasi ditemukan	Lokasi pengguna teridentifikasi
9	Riwayat Penjelajahan Web	WhatsApp Web IndexedDB	Riwayat penjelajahan ada	Penggunaan web tercatat
10	File Media (Foto, Video)	WhatsApp Web IndexedDB	File media ditemukan	Media tersimpan

Setiap jenis data dalam tabel ini mencerminkan temuan dari analisis forensik dan kesimpulan yang dapat diambil dari temuan tersebut menggunakan metode eksperimental untuk proses ektrasi data (Paligu & Varol, 2020). Laporan forensik lengkap akan menguraikan temuan ini lebih lanjut, menyajikan konteks investigasi, dan memberikan informasi yang relevan untuk pihak berwenang dalam proses investigasi WhatsApp Browser. Dengan adanya dokumentasi yang tepat, keseluruhan proses investigasi forensik menjadi lebih transparan dan dapat digunakan sebagai dasar untuk tindakan lebih lanjut sesuai dengan hukum yang berlaku.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Penelitian ini mengkaji penerapan teknik forensik digital pada aplikasi WhatsApp Web menggunakan kerangka kerja National Institute of Standards and Technology (NIST). Dalam konteks ini, langkah-langkah investigasi forensik, mulai dari inisiasi, pengumpulan data, analisis, hingga pelaporan, telah diuraikan dan diterapkan secara detail.

Hasil penelitian menunjukkan bahwa WhatsApp Web dapat menjadi sumber informasi yang berharga dalam investigasi forensik. Berbagai jenis data, termasuk pesan teks, riwayat panggilan suara dan video, informasi kontak pengguna, dan banyak lagi, dapat ditemukan dalam penyimpanan IndexedDB aplikasi. Data ini dapat digunakan untuk membangun kronologi peristiwa, mengidentifikasi kontak yang relevan, dan mendukung proses investigasi forensik.

Selain itu, penelitian ini juga mengilustrasikan pentingnya penggunaan kerangka kerja NIST dalam melaksanakan investigasi forensik. Pendekatan ini memberikan struktur yang jelas dan metodologi yang dapat diandalkan untuk mengumpulkan, menganalisis, dan melaporkan data forensik dengan integritas yang tinggi.

Dalam rangka meningkatkan efektivitas investigasi forensik di masa mendatang, penelitian ini menekankan perlunya upaya yang berkelanjutan dalam mengembangkan alat-alat forensik yang dapat secara efisien mengakses, menganalisis, dan melaporkan data dari aplikasi WhatsApp Web. Dengan perkembangan teknologi yang terus berlanjut, penelitian semacam ini akan menjadi semakin penting dalam menjaga keamanan dan keadilan dalam dunia digital yang terus berkembang.

5.2 Saran

Berdasarkan hasil penelitian ini, beberapa saran dapat diajukan untuk pengembangan lebih lanjut dalam bidang investigasi forensik digital terutama pada aplikasi WhatsApp Web:

1. Untuk memfasilitasi investigasi forensik pada WhatsApp Web, disarankan untuk mengembangkan alat forensik khusus yang dapat secara efisien mengakses dan menganalisis data dalam penyimpanan IndexedDB. Alat ini harus mematuhi kerangka kerja NIST untuk memastikan akurasi dan integritas data yang tinggi.
2. Penting bagi para profesional forensik digital untuk menerima pelatihan yang tepat dalam menghadapi aplikasi web seperti WhatsApp Web. Ini akan membantu mereka memahami teknik-teknik investigasi yang diperlukan dan memastikan bahwa proses investigasi berjalan sesuai dengan pedoman forensik yang benar.
3. Kolaborasi antara lembaga penelitian, penyidik forensik, dan industri pengembang aplikasi seperti WhatsApp dapat meningkatkan pemahaman tentang cara aplikasi ini menyimpan data dan memfasilitasi pengembangan alat forensik yang lebih baik.
4. Dalam pengembangan alat forensik dan selama proses investigasi, perlu ditekankan perlunya melindungi privasi pengguna. Penerapan etika dan hukum yang ketat dalam mengakses dan menggunakan data pribadi pengguna adalah suatu keharusan.
5. Penelitian lebih lanjut dalam bidang ini diperlukan untuk mengikuti perkembangan teknologi dan aplikasi baru. Hal ini juga dapat mencakup pengembangan teknik analisis yang lebih canggih dan adaptasi terhadap perubahan dalam aplikasi dan perangkat yang digunakan oleh pengguna.

Dengan mengikuti saran-saran ini, diharapkan akan ada peningkatan dalam kemampuan untuk melakukan investigasi forensik yang efektif pada aplikasi WhatsApp Web dan aplikasi serupa, sambil memastikan perlindungan privasi yang tepat bagi pengguna.

Daftar Pustaka

Actoriano, B., & Riadi, I. (2023). *Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2*. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 7(4), 410–419. http://sdiwc.net/digital-library/forensic-investigation-on-whatsapp-web-using-framework-integrated-digital-forensic-investigation-framework-version-2

Al-Sabaawi, A., Foo, E., & Au, E. (2019). *A Comparison Study of Android Mobile Forensics for Retrieving Files System Handprint Recognition Technique Based in Image Segmentation for Recognize View project A Comparison Study of Android Mobile Forensics for Retrieving Files System*. International Journal of Computer Science and Security (IJCSS), 13, 2019–2148. https://www.researchgate.net/publication/335422366

Anglano, C. (2014). *Forensic analysis of whats app messenger on Android smartphones.* Digital Investigation, 11(3), 201–213. https://doi.org/10.1016/j.diin.2014.04.003

Campos, L. M. O., Gomes, E., & Martins, H. P. (2016). *Forensic Expertise in Storage Device USB Flash Drive: Procedures and Techniques for Evidence*. IEEE Latin America Transactions, 14(7), 3427–3433. https://doi.org/10.1109/TLA.2016.7587651

Dezfouli, F and Dehghantanha, A. (2014). *Digital forensics trends and future*.

Karpisek, F., Baggili, I., & Breitinger, F. (2015). *WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages*. Digital Investigation, 15(October), 110–118. https://doi.org/10.1016/j.diin.2015.09.002

Khoisyilah, U. (2013). Universiti Putra Malaysia Universiti Putra Malaysia. *Factors Influencing Continuance Intention Towards On- Demand Ridesharing Services*, M, 2–3.

Mahajan, D.A., Mahender, C.N. (2022). A Study on Impact of WhatsApp on College Students. In: Zhang, YD., Senjyu, T., So-In, C., Joshi, A. (eds) Smart Trends in Computing and Communications. Lecture Notes in Networks and Systems, vol 286. Springer, Singapore. https://doi.org/10.1007/978-981-16-4016-2_58

Mendoza, A., Kumar, A., Midcap, D., Cho, H., & Varol, C. (2015). *BrowStEx: A tool to aggregate browser storage artifacts for forensic analysis. Digital Investigation*, 14(September), 63–75. https://doi.org/10.1016/j.diin.2015.08.001

National Institute of Standards and Technology. (2023). Cybersecurity Framework. Diakses dari https://www.nist.gov

Paligu, F., & Varol, C. (2020). *Browser forensic investigations of whatsapp web utilizing indexeddb persistent storage*. Future Internet, 12(11), 1–17. https://doi.org/10.3390/fi12110184

Riadi, I., Yudhana, A., Caesar, M., & Putra, F. (2018). *Akuisisi Bukti Digital Pada Whatsapp Web Berbasis Android Menggunakan Metode National Institute Of Justice (. Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)*, 4, 219–227.

Sistem, R., Riadi, I., Umar, R., Aziz, M. A., Informatika, S. T., & Dahlan, U. A. (2021). *Komparatif Web-based Instant Messaging Vulnerability Menggunakan*. 1(10), 813–819. https://doi.org/10.29207/resti.v4i5

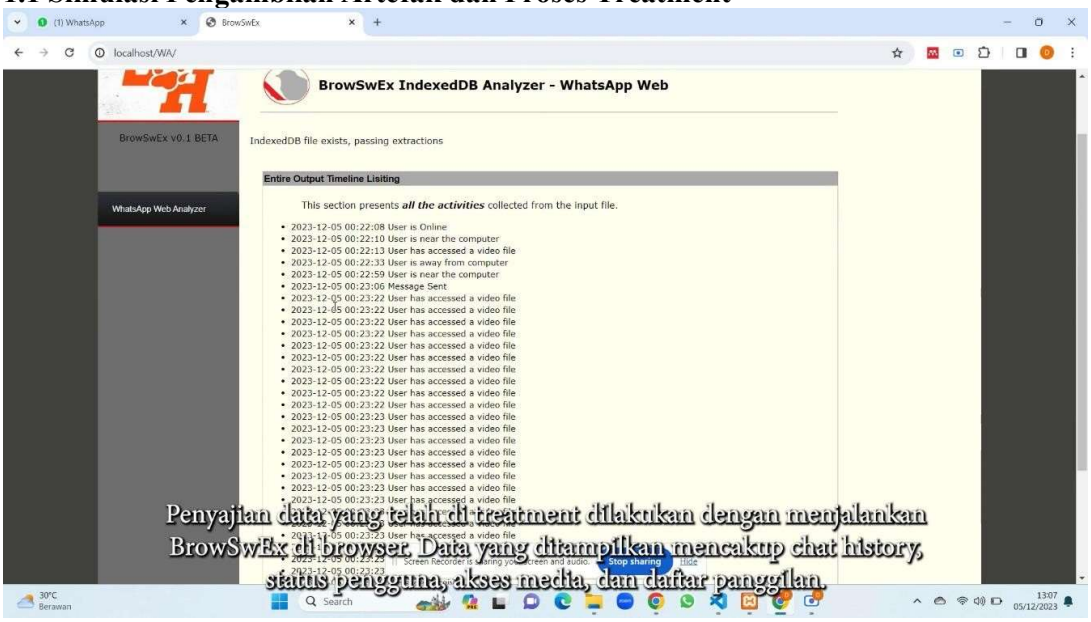
Suhendra, A. D., Asworowati, R. D., & Ismawati, T. (2020). *Perbandingan Analisis Forensik Digital Aplikasi Whatsapp Messenger menggunakan Metode NIST*. Akrab Juara, 5(1), 43–54. http://www.akrabjuara.com/index.php/akrabjuara/article/view/919

Umar, R., Riadi, I., & Maulana, G. (2017). *A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements*. International Journal of Advanced Computer Science and Applications, 8(12). https://doi.org/10.14569/ijacsa.2017.081210

Vukadinovic, N. V. (2019). WhatsApp Forensics: Locating Artifacts in Web and Desktop Clients. Master's Thesis, Purdue University Graduate School, M

LAMPIRAN

1.1 Simulasi Pengambilan Artefak dan Proses Treatment



Link:https://drive.google.com/file/d/1mKJbl4gIyHG3JWMBPyTHFt-ew17GAYuK/view?usp=drive_link