JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 740-749

Analisis Forensik Digital Aplikasi *WhatsApp* pada *Smartphone* Berbasis iOS Berdasarkan ACPO

Febrizky Dwi Restu Rini[1*], Rakha Wilis[1], Reza Aulia Wildana[1]

[1]Fakultas Keamanan Siber, Program Studi Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, Bogor, Indonesia
Email: [1*]febrizky.dwi@student.poltekssn.ac.id, [2]rakha.wilis@student.poltekssn.ac.id, [3]reza.aulia@student.poltekssn.ac.id

Abstrak – Penelitian ini memanfaatkan metode ACPO untuk melakukan analisis forensik digital pada aplikasi WhatsApp yang berjalan pada smartphone berbasis iOS. Tujuan dari penelitian ini adalah untuk menemukan dan menganalisis bukti digital pada aplikasi WhatsApp, yang mencakup file media, log panggilan, dan riwayat obrolan. Metode ACPO digunakan untuk menjamin keandalan dan integritas bukti digital. Studi ini melibatkan penggunaan alat forensik MOBILedit Forensic untuk mengekstrak dan menganalisis data. Hasilnya menunjukkan bahwa metode ACPO efektif dalam menjaga bukti digital, dan alat forensik yang digunakan dapat mengekstrak dan menganalisis data dari aplikasi WhatsApp yang berjalan pada smartphone berbasis iOS. Studi ini juga menunjukkan betapa pentingnya analisis forensik digital untuk menyelidiki tindakan kriminal. Utamanya tindak kejahatan revenge porn.

Kata Kunci: iOS; WhatsApp; ACPO; MOBILedit Forensic, Revenge Porn

Abstract – This research utilizes the ACPO method to conduct digital forensic analysis on the WhatsApp application running on iOS-based smartphones. The aim of this study is to discover and analyze digital evidence within the WhatsApp application, including media files, call logs, and chat histories. The ACPO method is employed to ensure the reliability and integrity of digital evidence. The study involves the use of the forensic tool MOBILedit Forensic for data extraction and analysis. The results indicate the effectiveness of the ACPO method in preserving digital evidence, and the forensic tool used can successfully extract and analyze data from the WhatsApp application running on iOS-based smartphones. This study underscores the significance of digital forensic analysis in investigating criminal activities, particularly in cases of revenge porn.

Keywords: iOS; WhatsApp; ACPO; MOBILedit Forensic; Revenge Porn

1. PENDAHULUAN

Berdasarkan laporan Bussiness for Apps di tahun 2023, Indonesia menjadi pengguna WhatsApp terbanyak ketiga di dunia dengan catatan memiliki pengguna mencapai 112 juta jiwa[1]. Adanya aplikasi ini memang mempermudah banyak pengguna dengan fitur yang ditawarkan. WhatsApp mendukung pengguna dari berbagai sistem operasi, salah satunya iOS. WhatsApp pada iOS memiliki fitur yang sama dengan WhatsApp yang ada di Android, hingga saat ini WhatsApp terus memperbarui fitur - fiturnya demi kemudahan pengguna. iOS memiliki 1,5 milliar pengguna aktif di dunia. Hal ini didukung dengan alasan keamanan dari iOS yang lebih baik dari sistem operasi mobile lain [2]. Pada saat ini versi iOS yang masih tersedia adalah iOS 16 dan 17 dimana iOS 17 untuk seri Iphone 12 ke atas dan 8 - 11 untuk iOS 16. Seri Iphone 8 merupakan Iphone terendah yang dapat mengakses iOS 16 sehingga, hal ini menjadi peluang penelitian terkait keamanan iOS 16 pada Iphone 8.

Memilik banyak pengguna membuat aplikasi WhatsApp menjadi sasaran empuk bagi kejahatan dunia siber. Sebagai aplikasi instant messaging, WhatsApp dengan mudah digunakan sebagai alat komunikasi kejahatan. Salah satunya revenge porn. Revenge porn adalah penyebaran konten pornografi kepada orang yang bersangkutan dengan tujuan melecehkan, mempermalukan, mengintimidasi, hingga menyuap. Penyebaran konten ini sebagai bentuk tidak terima, balas dendam, atau wujud kecemburuan. Revenge porn biasanya disertai dengan ancaman[3]. Menurut Undang Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 5 ayat 1. Informasi Eletkronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Sehingga, semakin banyak data digital yang ada, semakin banyak peluang data tersebut dijadikan bukti digital yang sah[4].

Bukti digital yang sah dapat didapatkan melalui proses investigasi. Forensik digital merupakan disiplin ilmu forensik yang erat kaitannya dengan proses yang konsisten, dapat diulang,

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 740-749

dan dapat dipertahankan. Dalam proses investigasi forensik digital, terdapat standar yang digunakan, salah satunya Association of Chief Police Officers (ACPO). Penggunaan ACPO memastikan bahwa bukti digital yang diperoleh dapat diterima di pengadilan. ACPO mencakup standarisasi prosedur, memastikan integrasi bukti, dan menjga jejak audit proses forensik. ACPO juga memberikan rekomendasi terkait pengumpulan, pelestarian, dan analisis bukti digital

Dalam proses forensik digital tentunya dibutuhkan sebuah alat atau tools yang mendukung proses investigasi. MOBILedit Forensic merupakan salah satu tools yang andal, khususnya dalam analisis smartphone. Tools ini digunakan untuk mengekstrasi bukti digital, termasuk Riwayat panggilan, pesan, media, dan data yang tersimpan di perangkat. MOBILedit Forensic menggunakan akuisisi data fisik dan logis dengan interface yang mudah digunakan. Fitur utama dari MOBILedit Forensic antara lain, yakni pengambilan data yang telah dihapus, deteksi malware, ekstraksi bersamaan, pembaruan langsung, dan analisis aplikasi tingkat lanjut[5].

Selumlah penelitian tentang forensik digital yang terkait dengan penelitian ini telah dilakukan sebelumnya. Pada penelitian ini [6], dilakukan forensik digital pada aplikasi IM whatsapp, telegam dan messenger berbasis IOS versi 13.3 berdasarkan metode NIST. Tools yang digunakan meliputi Cellebrite UFED 4PC, Oxygen Forensic Detective, FTK Imager, dan Autopsy. Hasil penelitian tersebut menunjukan temuan bukti digital pada aplikasi Whatsapp dengan presentase sebesar 71.42%. Kemudian, sebuh penelitian [ ] menerapkan forensik digital aplikasi Whatsapp pada system operasi IOS versi 8.3, Android, dan Windows Phone berdasarkan metode ACPO. Tools yang digunakan pada penelitian ini yaitu Cellebrite UFED dan Oxygen Forensic Detective. Hasil penelitian tersebut berupa temuan bukti digital aplikasi Whatsapp pada system operasi IOS versi 8.3, Android, dan Windows Phone. Penelitian selanjutnya [7], forensik digital dilakukan pada aplikasi WHatsapp berbasis android dengan menggunakan tools MOBILedit Forensic Express dan metode Digital Forensic Investigation Workshop (DFRWS). Hasil penelitian ini menunjukkan bahwa terdapat temuan bukti digital menggunakan tools MOBILedit Forensic Express dengan presentase sebesar 84,6%. Selanjtunya, sebuah penelitian [8], mengimplementasiakan forensik digital pada aplikasi skype, whatsapp, dan telegram berbasis Android menggunakan metode Association of Chief Police Officers (ACPO). Tools yang digunakan dalam penelitian adalah FTK Imager, dan OSForensic. Hasil dari penelitian ini menunjukan temuan bukti digital pada aplikasi Whatsapp dengan presentase sebesar 67 %. Penelitian terakhir [9], dilakukan forensic digital pada aplikasi Michat berbasis Android menggunakan tools MOBILedit Forensic Express berdasarkan metode Association of Chief Police Officers (ACPO). Hasil dari penelitian ini berupa temuan bukti digital menggunakan tools MOBILedit Forensic Express dengan presentase sebesar 57,1%.

Studi forensik digital terkait aplikasi WhatsApp pada platform iOS menunjukkan perbedaan dalam pendekatan, metode, alat, dan framework yang digunakan oleh para peneliti. Sebagai contoh, dalam penelitian "iOS Digital Evidence Comparison of Instant Messaging Apps (2022)," [15] menggunakan alat analisis MOBILedit Forensic Express. Di sisi lain, studi sebelumnya pada tahun 2015 menekankan penggunaan metode yang berbeda dengan lebih menitikberatkan pada perangkat keras dan menggunakan alat analisis yang berbeda pula. Selain itu, terdapat perbedaan dalam pemilihan framework, seperti penggunaan metode Digital Forensic Research Workshop (DFRWS) dalam sebuah studi lain. Hal ini menunjukkan variasi dalam pendekatan dan fokus pada platform tertentu, baik iOS maupun Android.

Berdasarkan penelitian yang telah dilakukan, diketahui bahwa forensik digital menggunakan tools MOBILedit Forensic Express dengan metode ACPO dapat diimplementasikan pada aplikasi Whatsapp berbasi IOS 16. Penelitian ini bertujuan mencari bukti digital pada aplikasi Whatsapp berbasis IOS 16 untuk membuktikan kasus kejahatan revenge porn yang terjadi pada aplikasi tersebut. Forensik digital akan dilakukan berdasarkan metode Association of Chief Police Officers (ACPO) yang mencakup empat tahapan utama yaitu plan, capture, analysis, present. Tools MOBILedit Forensic Express akan digunakan dalam penelitian ini untuk melakukan ekstraksi data pada aplikasi Whatsapp berbasi IOS 16.

2. METODE

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 740-749

Penelitian ini bertujuan utama untuk mendapatkan bukti digital dari aplikasi WhatsApp pada smartphone Android dengan menggunakan kerangka kerja ACPO (*Association of Chief Police Officers*) dan alat forensik MOBILedit Forensic Express selama proses analisis. Pendekatan yang diterapkan dalam penelitian ini melibatkan kombinasi metode kualitatif dan kuantitatif. Metode pengumpulan dan pengolahan data menggunakan pendekatan kualitatif, sementara pendekatan kuantitatif digunakan untuk menguji hasil data forensik digital yang diperoleh dari aplikasi WhatsApp.

Perhitungan indeks digunakan untuk mengevaluasi tingkat kerentanan dari setiap scenario sesuai dengan metode pengujian kuantitatif. Evaluasi ini didasarkan pada hasil akuisisi artefak digital dari masing-masing skenario. Rumus perhitungan nilai kerentanan yang diterapkan adalah persamaan indeks tanpa bobot. Persamaan 1 [6] digunakan untuk mendapatkan nilai kerentanan dari aplikasi perpesanan instan berbasis web.

$$P_{on} = \frac{\sum Pn}{\sum Po} \text{ x } 100 \qquad (1)$$

Keterangan:

Pon : presentase nilai *vulnerability* scenario
$\sum Po$: jumlah data awal artefak digital
$\sum Pn$: jumlah data artefak digital hasil akuisisi

2.1 ACPO (*Association of Chief Police Officers*)

Metode yang diusulkan oleh *Association of Chief Police Officers* (ACPO) merupakan suatu kerangka kerja penelitian yang terdiri dari empat elemen kunci, yaitu identifikasi, pengamanan bukti, analisis, dan penyajian atau presentasi [7]. Skema langkah-langkah penelitian yang diusulkan oleh ACPO dapat ditemukan dalam Gambar 2.

Gambar 2. Tahapan ACPO

Berdasarkan ilustrasi pada Gambar 1, dapat dipahami bahwa metode Association of Chief Police Officers (ACPO) mengikuti beberapa tahapan penelitian yang dapat diuraikan sebagai berikut[8]:

a. Perencanaan (*Plan*): Tahap ini melibatkan penyusunan rencana yang merinci segala aspek yang akan dilakukan dalam proses penelitian sebelumnya. Proses ini meliputi persiapan kondisi device untuk menciptakan simulasi kejahatan serta persiapan device laptop untuk alat forensik digital setelah dilakukan simulasi kejahatan.

b. Penangkapan (Capture): Pada tahap ini, hasil penelitian disimpan untuk memungkinkan kelanjutan analisis dengan menggunakan data yang telah terkumpul. Pada tahap ini dilakukan proses akuisisi menggunakan perangkat forensik MobilEdit Express dengan objek yang telah direncanakan sebelumnya.

c. Analisis (Analysis): Tahap ini fokus pada analisis menggunakan parameter hasil yang diperoleh dari tahap sebelumnya. Setelah proses akuisisi di tahap sebelumnya, dilakukan analisis dengan alat forensik yang sama sehingga menghasilkan laporan atas analisis tersebut.

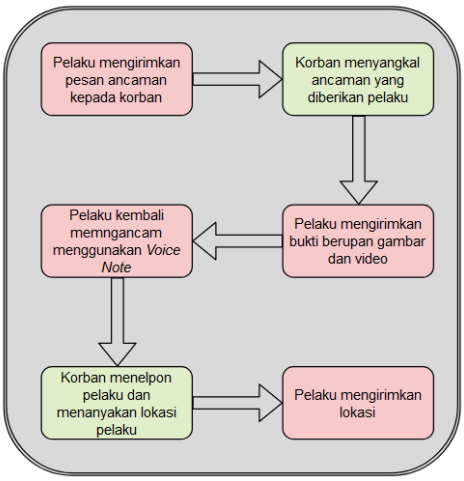
d. Presentasi (Present): Pada tahap presentasi, data hasil analisis dari tahap sebelumnya dipresentasikan untuk dapat diakses oleh publik. Pada tahap ini dilakukan olah kembali terkait laporan hasil analisis agar lebih mudah diterima oleh pembaca.

Metode ACPO dengan jelas mengartikulasikan langkah-langkah ini sebagai bagian integral dari proses penelitiannya, dimulai dari perencanaan hingga presentasi data yang relevan kepada pihak yang berkepentingan.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 740-749

2.2 Skenario

Sebelum mengujikan skenario, dilakukan simulasi kejahatan dengan memanfaatkan fitur-fitur yang ada dalam aplikasi WhatsApp pada ponsel pelaku. Simulasi akan dilakukan dari ponsel pelaku kepada ponsel korban. Simulasi kejahatan pada WhatsApp mencakup beberapa aksi seperti pengiriman dan penerimaan pesan 10 personal, serta pengiriman dan penerimaan pesan berupa 10 gambar, 10 video, 10 suara, dan 1 lokasi melalui Google Maps.



Gambar 3. Simulasi Kejahatan

Selanjutnya pembuatan skenario dilaksanakan dengan tujuan untuk memperoleh bukti digital tanpa batasan waktu tertentu pada aplikasi WhatsApp, seperti yang terperinci dalam Tabel 1.

Tabel 1. Skenario Penelitian

Skenario	Keterangan
Skenario 1	Data tidak dihapus
Skenario 2	Penarikan pesan pada aplikasi Whatsapp
Skenario 3	Penghapusan semua data melalui pengaturan penggunaan data aplikasi

2.3 Alat Penelitian

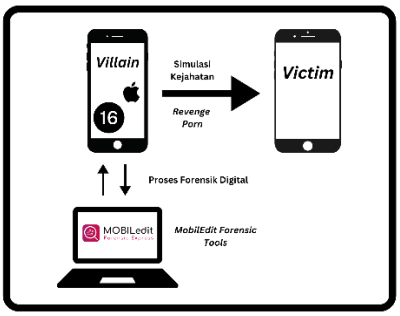
Dalam rangka pelaksanaan penelitian ini, diperlukan alat penelitian yang dapat mendukung jalannya penelitian. Alat penelitian ini melibatkan perangkat keras (hardware) dan perangkat lunak (software). Informasi terperinci mengenai perangkat yang digunakan terdapat dalam Tabel 2.

Tabel 2. Alat Penelitian

No	Alat	Versi
1	Aplikasi Whatsapp	Versi 23.24.73
2	Iphone 8 (Pelaku)	IOS 16
3	Smartphone (korban)	Android 12
3	Laptop Msi GF65 Thin 10SDR	Windows 11 Pro 64bit Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz *with* NVIDIA GeForce GTX 1660 Ti
4	Kabel USB Tipe *Lighting*	Type Lighting
5	MOBILedit Forensic Express	Versi 7.4.0.20393 (64-bit)

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 740-749

Berdasarkan Tabel 2, fokus utama penelitian ini adalah aplikasi WhatsApp pada perangkat iPhone 8 dengan sistem operasi iOS 16. Proses skenario dilakukan dengan menggunakan Whatsapp melalui Iphone 8 dengan IOS 16 sebagai device pelaku yang akan ditujukan ke *smartphone* korban lalu setelah itu dilakukan forensik digital pada sevice pelaku seperti pada gambar 3.



Gambar 3. Skenario Simulasi Kejahatan

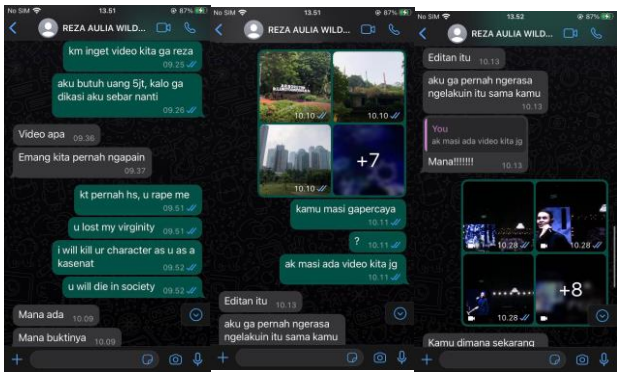
Penggunaan iPhone 8 dan iOS 16 dipilih karena keduanya mendukung pelaksanaan aktivitas komunikasi pada aplikasi WhatsApp. Selain itu, Iphone 8 merupakan Iphone dengan spesifikasi terendah yang dapat mengakses IOS 16, yaitu versi IOS yang hanya dapat diakses oleh Iphone baru[9]. Untuk menjalankan alat forensik yang telah ditentukan, digunakan perangkat laptop Msi GF65 Thin 10SDR. Alat forensik yang diterapkan dalam penelitian ini adalah MOBILedit Forensic. MOBILedit Forensic Express berperan dalam melihat dan mengekstrak data, seperti daftar kontak, riwayat panggilan, pesan, multimedia SMS, file, catatan, pengingat, kalender, data aplikasi mentah, IMEI, sistem operasi perangkat, kartu SIM, ICCID, dan lokasi pada perangkat iPhone 8. Alat ini memiliki kemampuan untuk mengambil data dari memori ponsel dengan cara melewati pengamanan cadangan, serta memberikan dukungan untuk konsumsi fisik perangkat iPhone dan kartu SD[10]. Pada penelitian lain, MOBILedit Forensic Express dinilai lebih superior dibandingkan alat forensik lain, seperti Magnet AXIOM, dengan persentase 22,22% [11].

3. ANALISA DAN PEMBAHASAN

Pada bagian ini berisi hasil dari kegiatan penelitian yang sudah dilakukan.

3.1 Plan

Dalam tahapan ini dilakukan pembuatan rencana secara mendetail termasuk pembuatan skenario, persiapan alat dan bahan penelitian, serta melakukan simulasi skenario kejahatan.

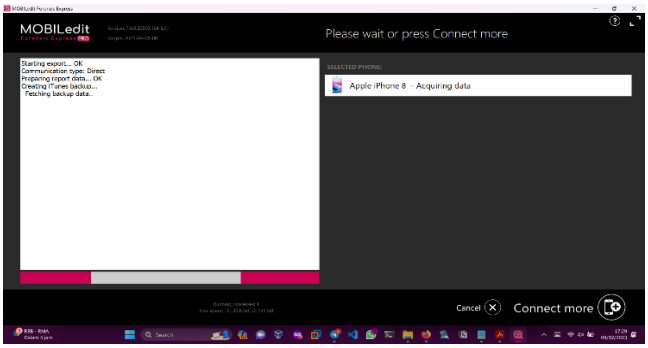


Gambar 4. Simulasi *Chat* Korban

3.2 Capture

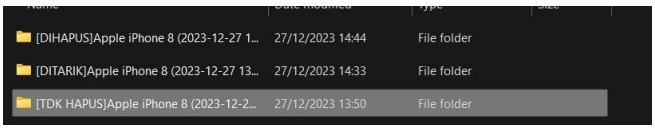
Proses Capture dilakukan untuk mengakusisi, mendokumentasikan, dan menyimpan seluru artefak digital menggunakan *tools* MOBILedit *Forensics* seperti pada Gambar 5.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 740-749



Gambar 5. Proses Akuisisi

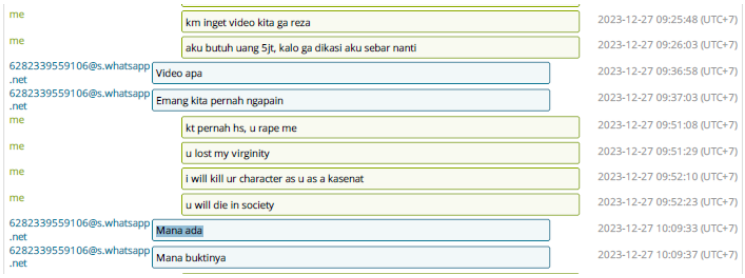
Akuisisi dilakukan pada setiap skenario yang diterapkan sehingga akan didapatkan tiga hasil akuisisi. Hasil dari akuisisi tersrbut berupa direktori yang selanjutnya dapat dianalisis.



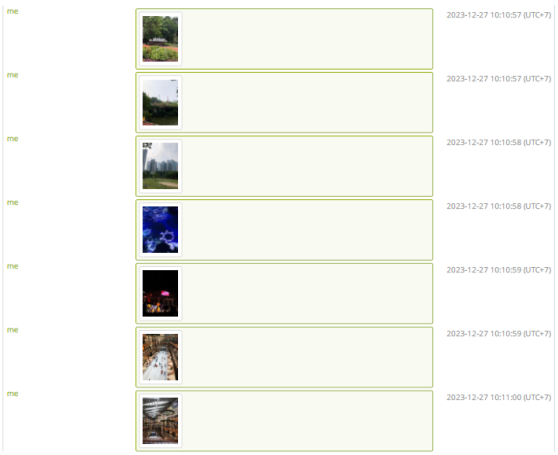
Gambar 6. Direktori Hasil Akuisisi

3.3 Analysis

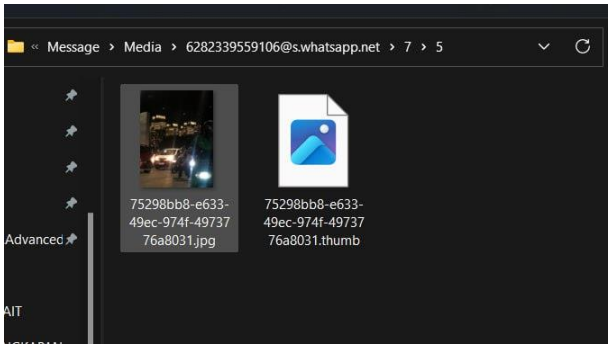
Tahap analisis dilakukan pada direktori hasil proses *Capture* untuk menemukan bukti digital pada aplikasi *Whatsapp*. Dari hasil analisis ditemukan bahwa ketiga skenario yang telah diterapkan memiliki hasil yang berbeda. Pada skenario 1 seluruh bukti digital aplikasi Whatsapp terkait dengan kejahatan yang terjadi dapat ditemukan.



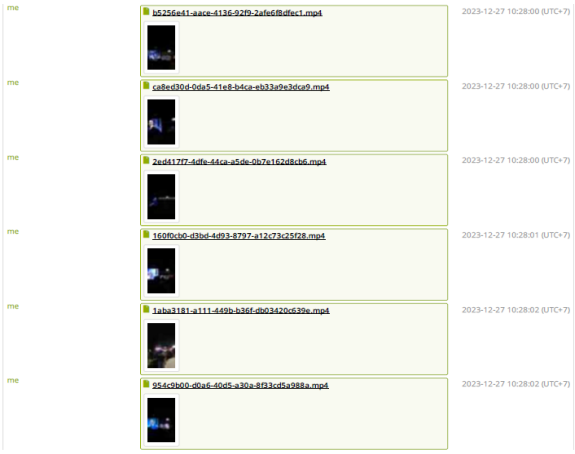
Gambar 7. Bukti Digital Pesan

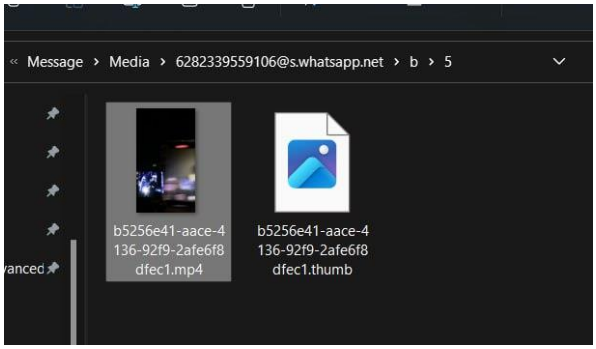


JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 740-749

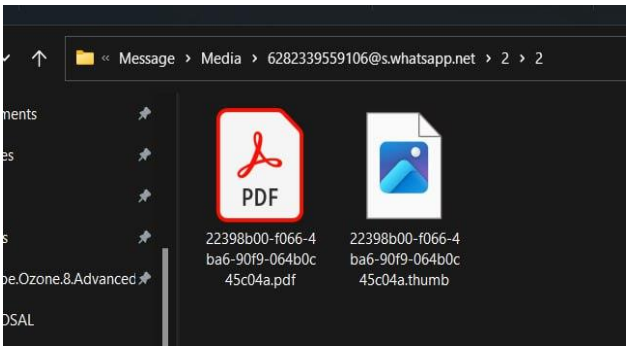


Gambar 8. Bukti Gambar



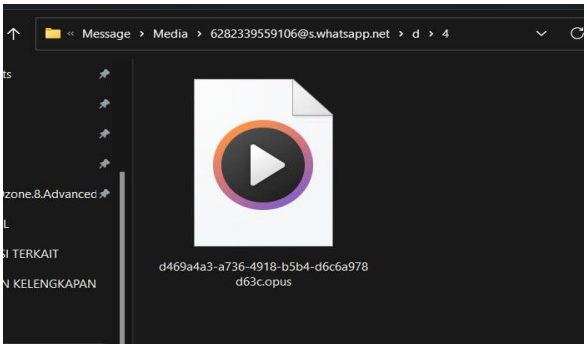


Gambar 9. Bukti Video

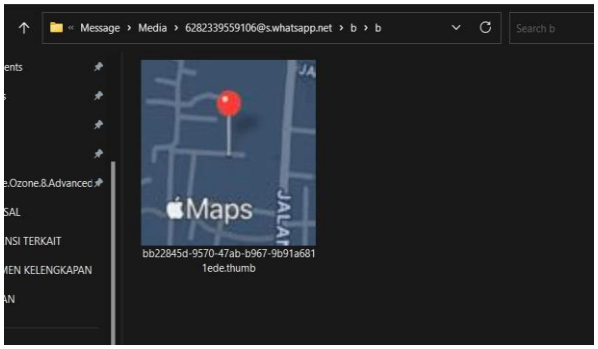


Gambar 10. Bukti File PDF

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 740-749

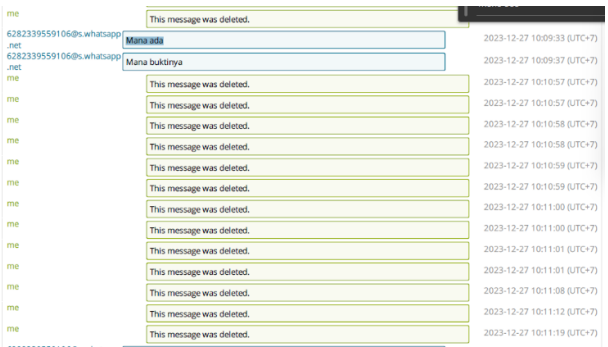


Gambar 11. Bukti *Voice Massege*



Gambar 12. Bukti Lokasi

Selanjutnya pada skenario kedua yaitu penarikan pesan, tidak terdapat bukti digital yang dapat ditemukan. Namun, bukti pelaku melakukan penarikan pesan dapat terlihat.



Gambar 13. Bukti Ditariknya Pesan

Pada skenario ketiga yaitu dilakukan penghapusan data aplikasi, tidak terdapat bukti digital yang berhasil ditemukan. Berdasarkan hasil analisis yang telah dilakukan,bukti digital yang ditemukan dapat dilihat pada Tabel 3.1

Tabel 3. Bukti Digital yang diemukan

Skenario	Data Hasil Akuisisi					
	Pesan Teks	Pesan Gambar	Pesan Video	Pesan Suara	Pesan File	Pesan Lokasi
1	18	10	10	1	1	1
2	-	-	-	-	-	-
3	-	-	-	-	-	-

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 740-749

Bukti digital yang berhasil diakuisisi selanjutnya akan digunakan untuk menentukan nilai presentase perolehan bukti digital dari masing masing skenario yang telah diterapkan. Nilai presentase perolehan tersebut ditentukan berdasarkan perbandingan jumlah bukti digital yang ditemukan dengan data digital yang dikirimkan. Dalam hal ini melalui aplikasi *Whatsapp.*

3.4 Preparation

Nilai hasil presentase perolehan bukti digital dari sekenario 1 hingga scenario 3.

Tabel 4. Hasil Skenario 1

Jenis	Jumlah Data Awal	Jumlah Hasil Akuisisi
Pesan Teks	18	18
Pesan Gambar	10	10
Pesan Video	10	10
Pesan Suara	1	1
Pesan File	1	1
Pesan Lokasi	1	1
Jumlah	**41**	**41**

Berdasarkan hasil pada Tabel 3.2, diperoleh hasil nilai presentase bukti digital sebesar 100%. Presentase tersebut diperoleh dari perhitungan perbandingan nilai sebgai berikut:

Nilai resentase perolehan skenario 1 = $\frac{41}{41} \times 100\% = 100\%$

Tabel 5. Hasil Skenario 2

Jenis	Jumlah Data Awal	Jumlah Hasil Akuisisi
Pesan Teks	18	0
Pesan Gambar	10	0
Pesan Video	10	0
Pesan Suara	1	0
Pesan File	1	0
Pesan Lokasi	1	0
Jumlah	**41**	**0**

Berdasarkan hasil pada Tabel 3.3, diperoleh hasil nilai presentase bukti digital sebesar 0%. Presentase tersebut diperoleh dari perhitungan perbandingan nilai sebgai berikut:

Nilai presentase perolehan skenario 2 = $\frac{0}{41} \times 100\% = 0\%$

Tabel 6. Hasil Skenario 3

Jenis	Jumlah Data Awal	Jumlah Hasil Akuisisi
Pesan Teks	18	0
Pesan Gambar	10	0
Pesan Video	10	0
Pesan Suara	1	0
Pesan File	1	0
Pesan Lokasi	1	0
Jumlah	**41**	**0**

Berdasarkan hasil pada Tabel 3.4, diperoleh hasil nilai presentase bukti digital sebesar 0%. Presentase tersebut diperoleh dari perhitungan perbandingan nilai sebgai berikut:

Nilai presentase perolehan skenario 3 = $\frac{0}{41} \times 100\% = 0\%$

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 740-749

4. KESIMPULAN

Dari keseluruhan skenario yang dikejakan, didapatkan hasil bahwa bukti digital hanya ditemukan pada skneario 1, sedangkan pada skenario 2 dan 3, bukti digital tidak dapat ditemukan. Pada skenario 2, hanya jejak penarikan pesan oleh pelaku yan berhasil terlihat. Dalam penelitian ini, ACPO digunakan sebagai panduan untuk melakukan analisis forensik digital pada aplikasi *WhatsApp* berbasis iOS. Hasil penelitian menunjukkan bahwa ACPO dapat digunakan untuk mengidentifikasi dan memulihkan data yang terhapus dari aplikasi *WhatsApp* berbasis iOS. Namun, hasil menunjukkan tidak ditemukan apapun pada skenario 2 dan 3.iOS yang dirasa lebih aman dari Android pun ketika dilakukan forensik menggunakan skenario 1, tetap ditemukan adanya bukti digital tersebut. Namun, penelitian ini memiliki keterbatasan dalam hal jumlah sampel yang digunakan dan perlu dilakukan penelitian lebih lanjut.

REFERENCES

60 Statistik iPhone untuk 2024: Penggunaan, Penjualan & Pangsa Pasar. 2023. https://mspoweruser.com/id/iphone.statistics/

Apa Itu Revenge Porn, Dampak, dan Hukumnya di Indonesia. 2023. Pramborsfm. https://www.pramborsfm.com/news/apa-itu-revenge-porn-dampak-dan-hukumnya-di-indonesia

Cunningham, A. 2023. *iOS 16.7 arrives for older iPhones and people who don't want to upgrade*. Ars Technica. https://arstechnica.com/gadgets/2023/09/ios-16-7-arrives-for-older-iphones-and-people-who-dont-want-to-upgrade/

D. Hariyadi, F. Nastiti, and F. Aini. 2018. *Framework for Acquisition of CCTV Evidence Based on ACPO and SNI ISO/IEC Framework for Acquisition of CCTV Evidence Based on ACPO and SNI ISO/IEC 27037:2014 Dedy Hariyadi Farida Nur Aini*.

I. Riadi, R. Umar, and M. Abdul Aziz. 2020. Komparatif Web-based Instant Messaging Vulnerability Menggunakan Metode Association of Chief Police Officers. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(5). https://doi.org/10.29207/resti.v4i5

Imam Riadi, Herman, H., & Nur Hamida Siregar. 2022. Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework. *Matrik: Jurnal Manajemen, Teknik Informatika, Dan Rekayasa Komputer*, *21*(3), 489–502. https://doi.org/10.30812/matrik.v21i3.1620

Imam Riadi, Yudhana, A., & Galih Fanani. 2023. Comparative Analysis of Forensic Software on Android-based MiChat using ACPO and DFRWS Framework. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *7*(2), 286–292. https://doi.org/10.29207/resti.v7i2.4547

K. Dwi, O. Mahendra, I. Komang, and A. Mogi. 2021. *Digital Forensic Analysis of Michat Applications on Android as Digital Proof in Handling Online Prostitution Cases*.

M. Aziz, W. Sulistyo, and R. Astari. 2021. *Komparatif Anti Forensik Aplikasi Instant Messaging Berbasis Web Menggunakan Metode Association of Chief Police Officers (ACPO)*.

MOBILedit. (n.d.). *MOBILedit Forensic*. MOBILedit. https://www.mobiledit.com/mobiledit-forensic

Muhammad Syihaab Al-Faaruuq, & Dimas Febriyan Priambodo. 2022. *iOS Digital Evidence Comparison of Instant Messaging Apps*. https://doi.org/10.1109/icsintesa56431.2022.10041620

Negara Dengan Jumlah Pengguna WhatsApp Terbanyak. 2024. Validnews.id. https://validnews.id/catatan-valid/negara-dengan-jumlah-pengguna-whatsapp-terbanyak

Otto Cornelis Kaligis. 2012. *Penerapan Undang-Undang nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik dalam prakteknya*.

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

Yudhana, A., Imam Riadi, & Riski Yudhi Prasongko. 2022. Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS). *Jurnal Informatika: Jurnal Pengembangan IT*, *7*(1), 43–48. https://doi.org/10.30591/jpit.v7i1.3639