

Akuisisi Bukti Digital Dan Deteksi Keaslian Citra Pada Whatsapp Menggunakan Metode NIST Dan ELA

Ikhwan Wiratama Putra¹, Aries Suharso², Chaerur Rozikin³

^{1,2,3}Teknik Informatika, Universitas Singaperbangsa Karawang, Indonesia

Jl. H.S. Ronggowaluyo Kel. Puseurjaya Kec. Telukjambe Timur Kab. Karawang Prov. Jawa Barat, 0267641177

ikhwan.wiratama17112@student.unsika.ac.id¹, aries.suharso@staff.unsika.ac.id²,
chaerur.rozikin@staff.unsika.ac.id³

Abstract

The growth of technology in the last 3 years has been very rapid, as is the growth of smartphone use. This growth is directly proportional to the crime cases that occur, especially in Indonesia. There were a total of 12,835 case complaints from 2018 to 2020, and the most cases were online fraud cases with 7,560 reports related to fraud on cyber patrol sites. One of the crimes that often occurs is online fraud cases using fictitious transfer receipts. This crime was committed using one of the short messaging applications, namely Whatsapp. After the crime was successfully carried out, the perpetrator then deleted the evidence in the form of the conversation along with a photo of the proof of the transfer using one of the features on WhatsApp. Therefore, this study aims to obtain or acquire evidence on the Whatsapp application using the NIST (National Institute of Standards and Technology) method and applying the ELA (Error Level Analysis) technique to analyze evidence in the form of images obtained to strengthen the evidence in court. In facilitating the investigation process, a forensic tool is needed. The forensic tools used in this research are Magnet Axiom and ForensicallyBeta. The final result obtained is that Magnet Axiom managed to find some evidence, including conversation messages, victim contacts, call history, profile photos of the perpetrators, and pictures. With the help of ForensicallyBeta tools, the obtained receipt image can be analyzed and identified that there has been a modification to the receipt.

Keywords: digital forensic, mobile forensic, fraud, NIST, ELA

Abstrak

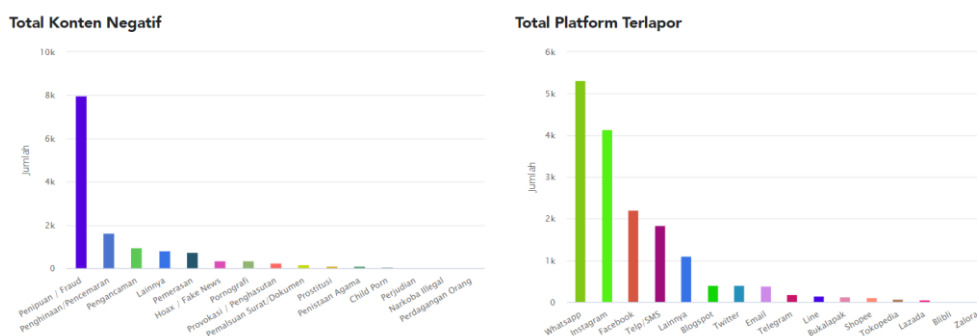
Pertumbuhan teknologi 3 tahun terakhir sangat pesat, begitu pula dengan pertumbuhan penggunaan smartphone. Pertumbuhan itu berbanding lurus dengan kasus kejahatan yang terjadi, terutama di Indonesia. Total ada 12.835 aduan kasus dari 2018 sampai 2020, dan yang terbanyak adalah kasus penipuan online yaitu sebanyak 7.560 laporan terkait penipuan pada situs patroli siber. Salah satu kejahatan yang sering terjadi ialah kasus penipuan online menggunakan bukti struk transfer fiktif. Kejahatan ini dilakukan menggunakan salah satu aplikasi pesan singkat yaitu Whatsapp. Setelah kejahatan tersebut berhasil dilakukan pelaku kemudian menghapus barang bukti berupa percakapannya beserta foto bukti transfernya menggunakan salah satu fitur yang ada pada whatsapp. Oleh karena itu, penelitian ini bertujuan untuk mendapatkan atau mengakuisisi barang bukti pada aplikasi Whatsapp dengan menggunakan metode NIST (National Institute of Standards and Technology) serta menerapkan Teknik ELA (Error Level Analysis) untuk menganalisis barang bukti berupa gambar yang diapatkan guna memperkuat barang bukti di pengadilan. Dalam mempermudah proses investigasi diperlukan adanya sebuah tools forensic. Tools forensic yang digunakan pada penelitian ini adalah Magnet Axiom dan ForensicallyBeta. Hasil akhir yang didapatkan adalah Magnet Axiom berhasil menemukan beberapa barang bukti, diantaranya pesan percakapan, kontak korban, riwayat panggilan, foto profil dari pelaku, serta gambar. Dengan

bantuan tools *ForensicallyBeta* gambar struk yang diperoleh dapat dianalisis dan diidentifikasi bahwa telah terjadi modifikasi pada bukti struk tersebut.

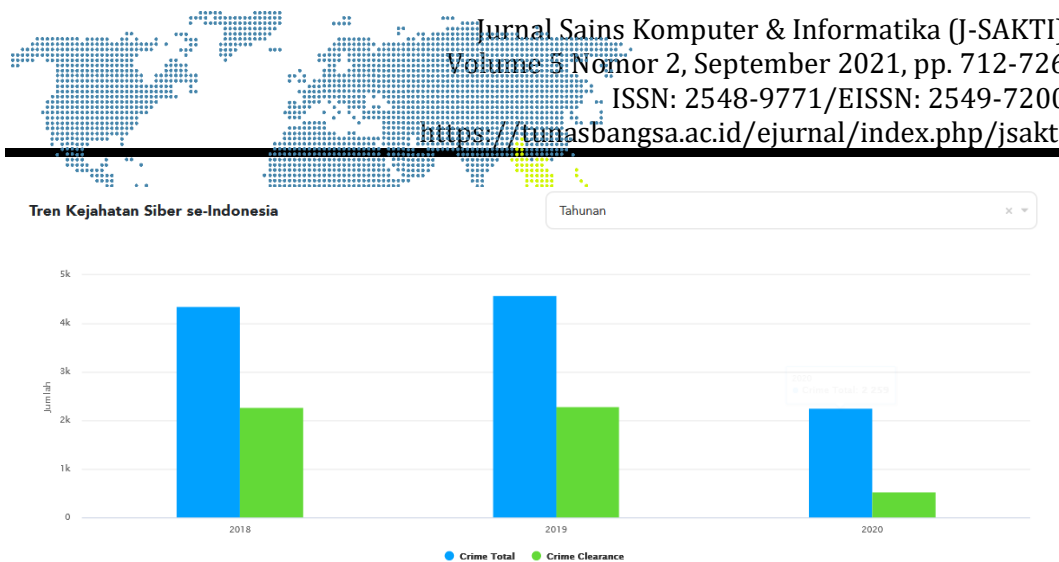
Kata kunci: *digital forensic, mobile forensic, penipuan, NIST, ELA*

1. PENDAHULUAN

Pertumbuhan teknologi 3 tahun terakhir sangatlah pesat, begitu pula dengan pertumbuhan *smartphone* yang senantiasa mengalami kemajuan dari bermacam macam aspek mulai dari segi fitur, sistem operasi, aplikasi, serta pada sisi spesifikasinya yang bermacam-macam [1]. Dari hasil riset salah satu *platform* manajemen media sosial HootSuite beserta salah satu agensi marketing sosial yaitu We Are Social menampilkan bahwa sebanyak 150 juta user internet di Indonesia berkembang pada tahun 2019, yang mana pada tahun 2018 hanya berkisar 132,7 juta pengguna saja. Selanjutnya yaitu pada tahun 2020 pengguna internet yang ada di Indonesia mencapai 175,4 juta [2]. Itu menunjukkan bahwa penggunaan internet di Indonesia semakin tahun semakin meningkat. Pertumbuhan *smartphone* yang semakin meningkat membuka kesempatan kejahatan melalui *smartphone* baik dari pelaku atau korban [3]. Dari informasi yang didapatkan di *website* Patroli Siber Indonesia, di tahun 2018 kasus *cyber crime* yang sukses ditangani kepolisian yakni 4.360 kasus, kemudian pada tahun 2019 bertambah sebanyak 4.586 kasus. Kemudian di tahun 2018 kasus yang bisa dituntaskan cuma sebanyak 2.273 kasus kejahatan siber, serta hanya 2.284 kasus di tahun 2019. Total ada 12.835 aduan kasus dari 2018 sampai 2020, dan yang terbanyak adalah kasus penipuan online yaitu sebanyak 7.560 aduan dan *platform*-nya yang paling banyak di gunakan yaitu melalui Whatsapp. Data tersebut dapat dilihat pada Gambar 1 dan Gambar 2. Permasalahan kejahatan *cyber* ini terus bertambah disetiap tahunnya, sehingga di tahun 2020 diketahui sebanyak 2.259 laporan permasalahan kejahatan siber sepanjang Januari sampai Mei dan yang terselesaikan hanya 527 kasus [4].



Gambar 1. Diagram total konten negatif dan total platform terlapor sepanjang 2018 – 2020 (sumber: patrolisiber.id)



*data ini diperoleh berdasarkan jumlah Laporan Polisi yang masuk dan jumlah kasus selesai yang dilaporkan oleh Subagbinops Ditreskrimsu seluruh Polda

Gambar 2. Diagram Total Jumlah Kasus dan Jumlah Kasus yang terselesaikan sepanjang Januari 2018 – Mei 2020 (sumber: patrolisiber.id)

Berdasarkan diagram pada gambar 1 dan gambar 2 yang bersumber dari *website* patroli siber indonesia Whatsapp menjadi aplikasi yang paling banyak di laporkan. Ada sekitar 4.965 aduan sepanjang Januari 2018 hingga Mei 2020. Ini disebabkan aplikasi tersebut sangat mudah digunakan dalam mengirim pesan, mengirim gambar, menelepon, ataupun video kepada sesama penggunanya. Kegiatan positif ataupun negatif sangatlah mudah untuk digunakan di aplikasi ini sebab penggunaannya yang terbilang mudah.

Namun perkembangan aplikasi Whatsapp tersebut dimanfaatkan oleh beberapa orang dalam melakukan tindakan kejahatan. Salah satu kejahatan yang sering terjadi yaitu penipuan *online*. Pada gambar 1 terlihat bahwa kasus paling banyak terjadi di Indonesia adalah kasus penipuan.

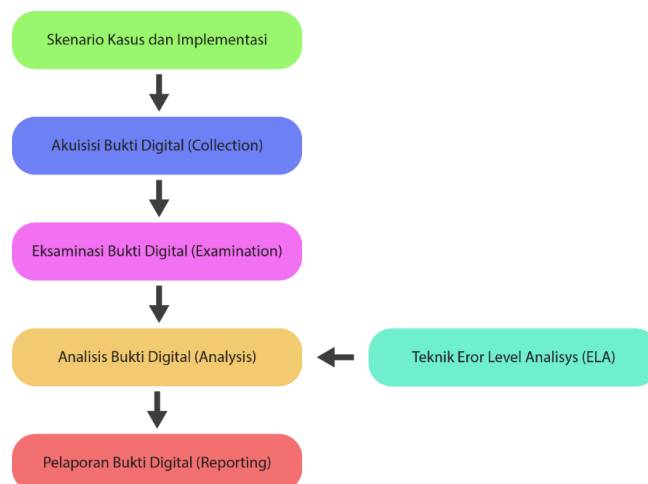
Terdapat penelitian sebelumnya yang dilakukan oleh Muhammad Irwan Syahib, Imam Riadi, Rusydi Umar (2020), pada penelitiannya mereka menggunakan bantuan sebuah *tools* forensik untuk mendapatkan atau mengakuisi barang bukti pada *smartphone* android berdasarkan tahapan NIST. Data yang berhasil di dapatkan merupakan pesan percakapan yang telah oleh pelaku dan juga akun serta riwayat panggilannya [5]. Kemudian pada penelitian yang dilakukan oleh Ikhwan Anshori, Khairina Eka Setya Putri, Umar Ghoni (2020), mereka melakukan penelitian dengan menggunakan beberapa *tools* forensik yaitu Oxygen Forensik, MOBILedit Forensik Express, dan Magnet AXIOM. Hasil yang diperoleh yaitu Oxygen Forensik memiliki kinerja yang kurang baik dalam mendapatkan bukti digital karena hanya berhasil mendapatkan 2 akun, 1 chat dan 26 gambar dengan persentase berupa 100% dalam mendapatkan akun, 5% dalam mendapatkan chat dan 86% dalam mendapatkan gambar. Sedangkan Magnet AXIOM dan MOBILedit Forensik berhasil mendapatkan 2 akun, 11 chat dan 26 gambar dengan persentase berupa 100% dalam mendapatkan akun, 55% dalam mendapatkan chat dan 86% dalam mendapatkan gambar [6].

Berdasarkan dari uraian diatas, maka penelitian ini bertujuan untuk mendapatkan atau mengakuisisi barang bukti digital berupa pesan percakapan pada aplikasi Whatsapp dengan menggunakan metode *National Institute of Standards and Technology* atau disingkat NIST, serta melakukan analisis pada barang bukti gambar dengan menerapkan Teknik *Error Level Analysis* disingkat ELA guna memperkuat barang bukti di pengadilan.

2. METODOLOGI PENELITIAN

Pada penelitian ini peneliti menggunakan skenario sendiri berdasarkan kasus yang sudah terjadi yaitu penipuan online menggunakan bukti struk transfer fiktif melalui aplikasi whatsapp. Dimana si pelaku melakukan penipuannya dengan cara memesan barang kepada korban melalui aplikasi whatsapp, setelah adanya kesepakatan antara korban dengan pelaku, maka pelaku mengirimkan sebuah bukti transfer yang menunjukkan bahwa sudah adanya sebuah pembayaran. Pada penelitian ini bukti struk transfer di manipulasi dengan menggunakan adobe photoshop dan gambar tersebut kemudian dikirim melalau whatsapp web. Bukti pembayaran dan percakapan ini yang nantinya akan dijadikan sebuah barang bukti. Barang bukti didapatkan dari *smartphone* pelaku menggunakan bantuan *tools forensic*. Untuk proses akuisisi bukti-bukti digital tersebut perlu adanya sebuah sistem. Sistem yang akan digunakan ialah kerangka kerja prosedur *mobile forensic* yang dibikin oleh *National Institute of Standard and Technology* atau disingkat NIST [7]. Untuk tahapanya yaitu *Collection, Examination, Analysis, Reporting*.

Berdasarkan pada metodologi yang digunakan yaitu *mobile forensic* dan *image forensic* maka terdapat 5 tahap dalam penelitian ini, yang mana pada tahapan analisis bukti digital terdapat metode ELA untuk mendeteksi keaslian gambar yang diperoleh.



Gambar 3. Tahapan NIST beserta ELA

3. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini merupakan hasil dari penerapan metode NIST terkait dengan kasus penipuan online menggunakan bukti struk transfer fiktif yang mana nantinya akan mengambil atau mengakuisisi barang bukti dari dua buah *smartphone* yaitu dari *smartphone* pelaku dan juga korban sebagai pembanding. Barang bukti digital yang didapatkan berupa pesan percakapan, gambar, dan kontak.

3.1. Skenario Kasus dan Implementasi

Penelitian ini dimulai dengan menggunakan dua buah *smartphone* yang mana nantinya masing-masing *smartphone* ini sudah terinstall aplikasi whatsapp. Setelah kedua akun siap, maka dimulailah skenario percakapan antara akun A dan akun B tentang penipuan menggunakan bukti struk transfer fiktif melalui *smartphone* tersebut. Berikut adalah gambaran dari skenario yang dilakukan :



Gambar 4. Proses Skenario dari Akun A Kepada Akun B melakukan Penipuan Menggunakan Bukti Transfer Fiktif



Gambar 5. Screenshot percakapan dari *smartphone* pelaku bahwa seluruh bukti percakapan telah dihapus

Setelah skenarionya berhasil dilakukan selanjutnya yaitu mencari informasi kemudian menganalisis *smartphone* milik pelaku untuk memperoleh barang bukti dan juga *smartphone* milik korban sebagai pembanding.

3.2. Akuisisi bukti digital

Pada tahapan ini dilakukan pengumpulan barang bukti berupa pemotretan barang, pencatatan jenis dan spesifikasi dari *smartphone* yang digunakan serta mengambil sekaligus menyalin data dari ponsel ke PC. Barang bukti yang digunakan dalam penelitian ini yaitu *smartphone* milik pelaku dan *smartphone* milik korban. *Smartphone* milik pelaku digunakan untuk pencarian dan analisis bukti digital, sedangkan *smartphone* korban digunakan sebagai pembanding bukti digital yang ditemukan dari *smartphone* pelaku. Hasil pemotretan barang bukti dapat dilihat pada gambar 6 yaitu milik pelaku dan pada gambar 7 milik korban.



Gambar 6. Dokumentasi barang bukti pelaku Xiaomi Redmi 4X



Gambar 7. Dokumentasi barang bukti korban Samsung J5

Detail spesifikasi *smartphone* yang di gunakan oleh pelaku dan juga korban dapat dilihat pada table 1 di bawah ini.

Tabel 1. Pencatatan spesifikasi barang bukti

Jenis	Spesifikasi
<i>Smartphone</i> Pelaku	Xiomi Redmi 4X

Jenis	Spesifikasi
	Android Versi 7.1.2
	Ram 4 GB
	CPU Octa-Core Max 1.40Hz
	Qualcom MSM8940 Snapdragon 435
	Internal 64 GB
Smarphone Korban	Samsung Galaxy J5 SM-J500G
	Android Versi 5.1.1
	Ram 1.5 GB
	CPU Quad-Core 1.2Hz
	Qualcom MSM8916 Snapdragon 410
	Internal 8 GB

Selanjutnya dilakukan proses akuisisi bukti digital atau pengambilan barang bukti dari *smartphone* pelaku dan juga korban, yang mana sebelumnya sudah diaktifkan fitur super user-nya atau biasa disebut dengan istilah *root*. *Tools Forensic* yang digunakan pada proses ini yaitu Magnet Axiom.

3.3. Eksaminasi Bukti Digital

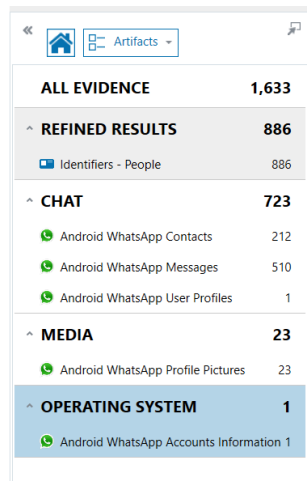
Setelah berhasil melakukan akuisisi, maka terdapat berbagai macam data-data yang berhasil terkumpul. Data-data tersebut dapat dilihat pada laptop yang sebelumnya sudah ditentukan lokasi dari hasil akuisisinya. Dari data-data yang telah didapatkan tersebut, terdapat berbagai macam tipe data dari memori penyimpanan *internal* maupun *eksternal* pada *smartphone*. Hasil dari proses akuisisi terkumpul dalam file bertipe *RAW File*. Hasil akuisisi ini dapat dilihat pada gambar 8.

Name	Date modified	Type	Size
42d5dda0a24248f78c71926111fd78db.attachments	5/17/2021 1:04 PM	ATTACHMENTS File	432 KB
activity_log.txt	5/10/2021 1:16 PM	Text Document	1,087 KB
artifacts.log	5/10/2021 1:28 PM	Text Document	4 KB
AXIOMExamine.IO.log	5/6/2021 2:55 AM	Text Document	0 KB
AXIOMExamine.IO.log.1	5/6/2021 2:55 AM	1 File	0 KB
AXIOMExamine.IO.log.2	5/6/2021 2:55 AM	2 File	0 KB
AXIOMExamine.log	5/17/2021 1:04 PM	Text Document	6 KB
AXIOMExamine.log.1	5/10/2021 2:54 PM	1 File	5 KB
AXIOMExamine.log.2	5/15/2021 10:35 PM	2 File	8 KB
Case Information.txt	5/10/2021 1:28 PM	Text Document	2 KB
Case Information.xml	5/10/2021 1:28 PM	XML Document	4 KB
Case.mfdb	5/17/2021 1:04 PM	MFD File	81,312 KB
Case.timeline	5/17/2021 1:04 PM	TIMELINE File	72,400 KB
custom_artifacts.log	5/10/2021 12:25 PM	Text Document	1 KB
image_info.txt	5/10/2021 1:16 PM	Text Document	3 KB
ipc.log	5/10/2021 1:28 PM	Text Document	72 KB
log.txt	5/10/2021 1:28 PM	Text Document	1,567 KB
logging-May 10 2021 133748.zip	5/10/2021 1:37 PM	WinRAR ZIP archive	444 KB
TagsLog.log	5/10/2021 1:16 PM	Text Document	0 KB
Xiaomi Redmi 4X Full Image - MMCBLK0.raw	5/10/2021 1:10 PM	RAW File	30,535,680 ...

Gambar 8. Hasil proses akuisisi

Pada aplikasi Magnet Axiom setiap data yang dipulihkan dari aplikasi ini disajikan sebagai *Artifact* atau dalam bahasa Indonesia disebut sebagai Artefak. Setiap artefak ini berisikan sekumpulan atribut, yang masing-masing

memiliki tipe data dan dapat juga berisikan beberapa bagian data seperti nama, lokasi, serta waktu [8]. Artefak-arterfak ini nantinya akan otomatis dikategorikan sesuai dengan kategorinya. Untuk melihat artefak-arterfaknya diperlukan Axiom Examine untuk membuka file berformat RAW yang didapatkan setelah proses akuisisi. Artefak-arterfak tersebut dapat dilihat pada gambar 9 dibawah ini.



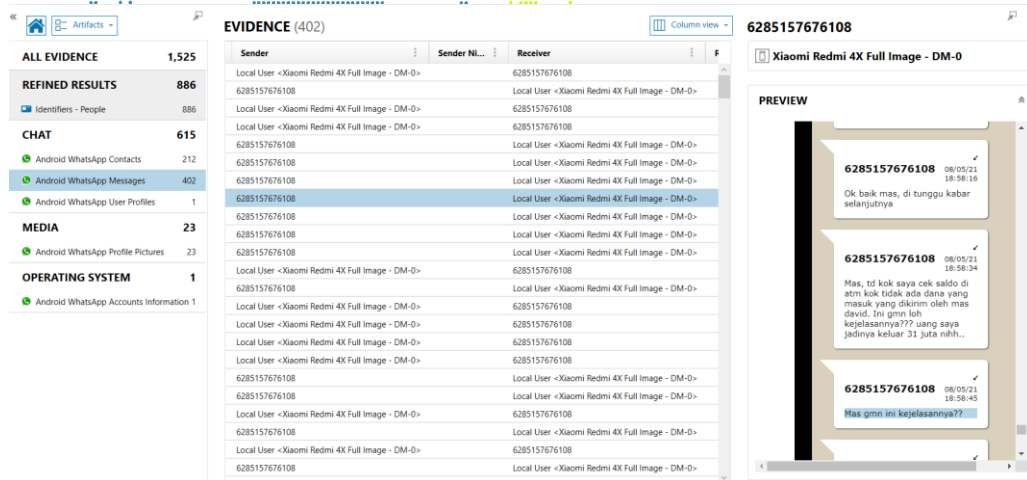
Category	Count
ALL EVIDENCE	1,633
REFINED RESULTS	886
Identifiers - People	886
CHAT	723
Android WhatsApp Contacts	212
Android WhatsApp Messages	510
Android WhatsApp User Profiles	1
MEDIA	23
Android WhatsApp Profile Pictures	23
OPERATING SYSTEM	1
Android WhatsApp Accounts Information	1

Gambar 9. Penemuan barang bukti atau *Artifact* dari whatsapp

3.4. Analisis

Pada tahap analisis ini dilakukan proses analisis terhadap barang bukti yang telah diperoleh yaitu berupa artefak-arterfak yang sudah tersusun rapih sesuai dengan kategorinya. Seperti yang sudah diskenariokan sebelumnya pelaku melakukan penipuan terhadap korban dengan menggunakan bukti struk transfer fiktif. Pada penelitian ini dilakukan pengambilan barang bukti dari *smartphone* dalam waktu 2 hari setelah dilakukannya penghapusan percakapan yang dilakukan oleh pelaku.

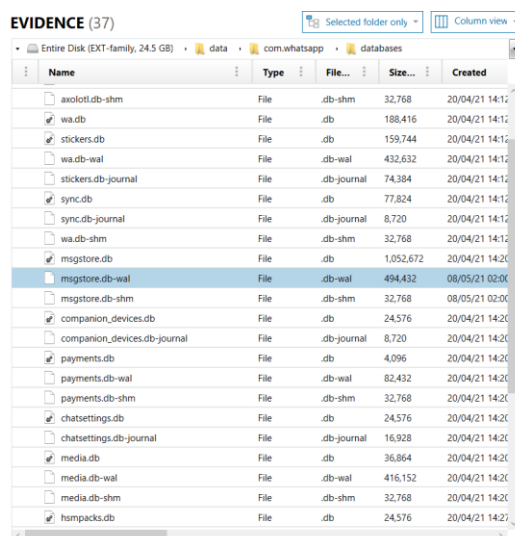
Pada proses analisis menggunakan Magnet Axiom, berhasil ditemukan beberapa barang bukti yang telah dikirim oleh pelaku, diantaranya pesan percakapan, kontak korban, riwayat panggilan, foto profil dari pelaku, serta gambar.



Gambar 10. Tampilan bukti digital pesan whatsapp dari *smartphone* pelaku

Pada gambar 10 adalah bukti percakapan antara pelaku dan korban yang di dapat dari *smartphone* pelaku. Dari hasil analisis terdapat beberapa atribut yang berhasil diperoleh, diantaranya yaitu pengirim dan penerima, waktu pengiriman dan penerimaan pesan, serta text percakapan.

Dari gambar diatas dapat dilihat bahwa percakapan yang sebelumnya telah di hapus oleh pelaku masih dapat di temukan dan masih tersimpan pada database whatsapp tepatnya berada pada file “msgstore.db-wal”. Obrolan yang terjadi pada whatsapp pada umunya disimpan di msgstore.db, akan tetapi setelah dianalisis ditemukan bahwa dengan menghapus bukti percakapannya, percakapan tersebut masih tersimpan di file cache dari msgstore.db yaitu msgstore.db-wal [9]. Untuk filenya dapat dilihat pada gambar 11 dibawah ini.



Gambar 11. Lokasi penyimpanan file barang bukti



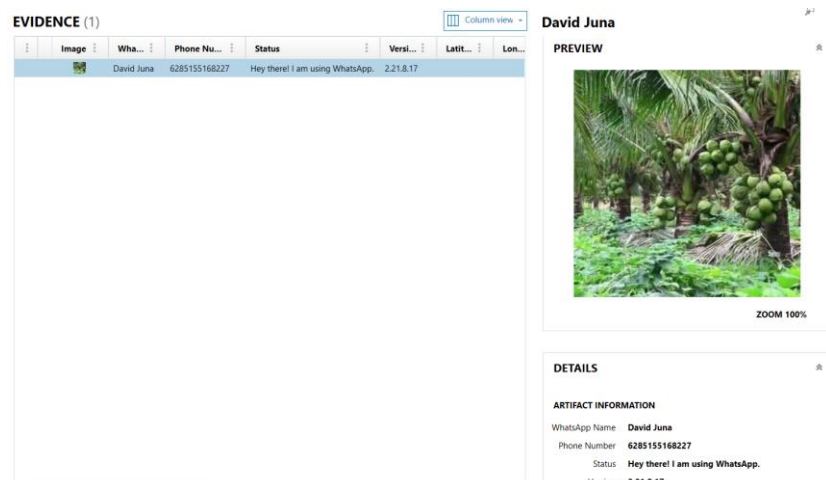
Gambar 12. Tampilan bukti digital kontak korban

Pada gambar 12 adalah tampilan bukti digital dari kontak korban. Dari hasil analisis terdapat beberapa atribut yang berhasil diperoleh, diantaranya yaitu foto profil korban dan nomor telepon.

08/05/21 18:59:08	08/05/21 18:59:10	Local user missed a call
08/05/21 18:59:03	08/05/21 18:59:05	Local user missed a call
08/05/21 18:58:58	08/05/21 18:59:01	Local user missed a call

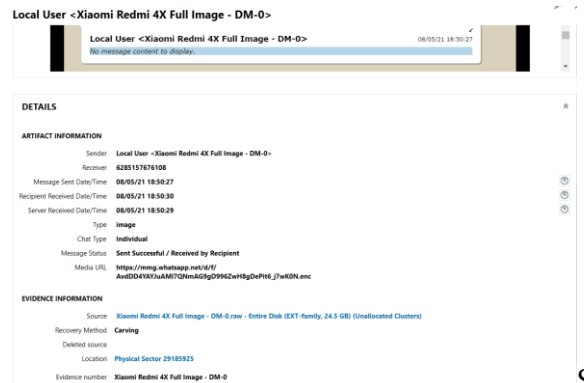
Gambar 13. Tampilan bukti digital riwayat panggilan

Pada gambar 13 adalah tampilan bukti digital dari riwayat panggilan. Dari hasil analisis dapat dilihat bahwa korban sempat melakukan beberap kali panggilan kepada pelaku. Dari hasil analisis ini juga terdapat beberapa atribut yang berhasil diperoleh, diantaranya yaitu tanggal dan waktu korban melakukan panggilan serta status panggilannya apakah dijawab atau tidaknya oleh pelaku.



Gambar 14. Tampilan bukti digital kontak pelaku

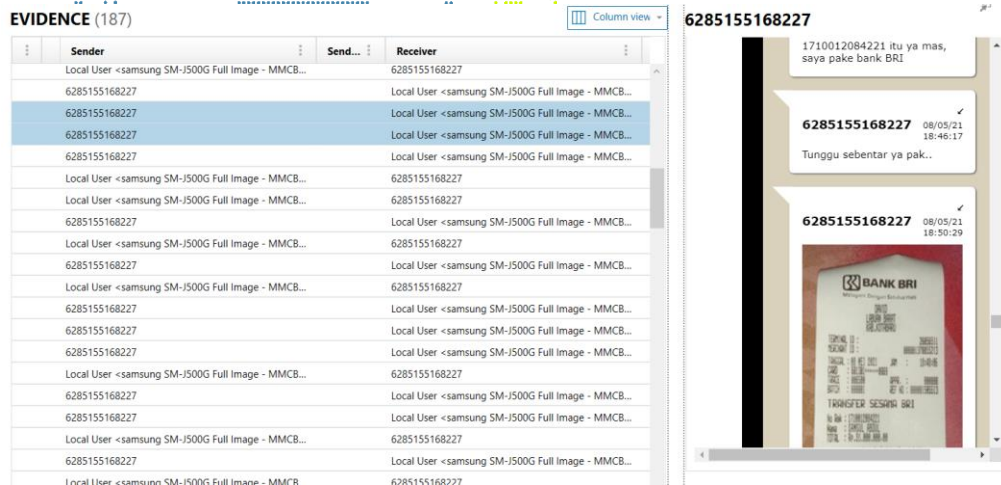
Pada gambar 14 adalah tampilan bukti digital mengenai informasi kontak pelaku. Dari hasil analisis ini terdapat beberapa atribut yang berhasil diperoleh, diantaranya yaitu foto profil yang digunakan oleh pelaku, nama yang digunakan pelaku, nomor telfon, serta versi whatsapp yang digunakan.



Gambar 15. Tampilan bukti digital gambar tidak ditemukan dari *smartphone* pelaku

Pada gambar 15 menunjukkan bahwa gambar yang dikirimkan oleh pelaku maupun korban yang telah dihapus tidak dapat dimunculkan kembali. Maka dari itu diperlukan cara lain untuk mendapatkan bukti transfernya, yaitu melalui *smartphone* korban. Karena pada whatsapp terdapat fitur "delete for everyone" yang memungkinkan pengguna untuk menghapus percakapan maupun file pada pengguna whatsapp lainnya. Cara ini dapat digunakan jika pelaku menghapus percakapannya lebih dari 1 jam [10]. Cara lainnya jika memang gambar yang dikirim oleh pelaku dihapus kurang dari 1 jam, maka diperlukan akuisisi dan analisis yang lebih luas lagi terkait penyimpanan internal maupun eksternal pada *smartphone* pelaku.

Pada penelitian ini pelaku menghapus percakapan pada *smartphone*-nya lebih dari 1 jam sehingga pesan dan gambar yang ada *smartphone* pelaku masih tersedia. Walaupun gambar yang sudah dihapus tidak dapat dimunculkan kembali, akan tetapi masih terdapat beberapa atribut yang dapat membantu untuk mencocokkannya dengan *smartphone* pembanding, seperti waktu pengiriman dan penerimaan pesan, serta nomor telepon pengirim dan penerimanya.



Gambar 16. Tampilan bukti digital gambar ditemukan dari *smartphone* korban

Pada gambar 16 berhasil dilakukan pengambilan barang bukti digital berupa pesan percakapan dan juga gambar dari *smartphone* korban. Gambar tersebut kemudian diambil dan dianalisis lebih lanjut untuk dilihat apakah itu gambar fiktif atau bukan.



Gambar 17. Bukti struk transfer yang berhasil diambil dari *smartphone* korban

Selanjutnya pada tahap analisis bukti struk transfer, teknik atau metode yang digunakan yaitu teknik *error level analysis* atau disingkat dengan ELA. Sedangkan untuk *tools* yang digunakan yaitu ForensicallyBeta. Bukti digital gambar yang telah didapatkan seperti gambar 17, gambar yang telah didapatkan tersebut kemudian dimasukkan kedalam ForensicallyBeta untuk dianalisis.



Gambar 18. Analisis gambar

Hasil analisisnya yaitu dengan *error level analysis* dapat diketahui daerah mana yang direkayasa atau diedit dari gambar tersebut, karena pada *error level analysis* apabila terdapat daerah yang berbeda dari yang lain, seperti tekstur, garis tepi, dan warnanya itu terjadi karena adanya level kompresi yang berbeda. Hasil analisis yang diperoleh yaitu gambar struk transfer tersebut telah dimanipulasi sehingga dapat terlihat pada bagian nama pengirim, lokasi, tanggal dan waktu pengiriman, serta di bagian nomor rekening dan juga total biaya pengirimannya terdapat bintik-bintik yang tidak merata atau tidak seimbang serta terlihat adanya perbedaan kontras warnanya. Maka dapat disimpulkan bahwa gambar tersebut telah dimanipulasi [11].

3.4. Reporting

Setelah berhasil melakukan beberapa tahapan seperti *Collection*, *Examination* dan *Analysis*, maka selanjutnya yaitu *Reporting*. Dimana pada tahapan ini akan membahas serta menyajikan barang bukti yang berhasil diperoleh yang berkaitan dengan aplikasi WhatsApp untuk mengungkapkan sebuah kasus kejahatan yang mana telah diskenariokan sebelumnya. Data-data bukti digital tersebut dapat dilihat pada tabel 2 dan tabel 3.

Tabel 2. Bukti digital yang berhasil didapatkan dari *smartphone* pelaku

Data	Berhasil (Ya/Tidak)
Akun & Kontak	Ya
Riwayat Panggilan	Ya
Pesan Teks	Ya
Gambar	Tidak

Tabel 3. Bukti digital yang berhasil didapatkan dari *smartphone* pembanding atau korban

Data	Berhasil (Ya/Tidak)
Akun & Kontak	Ya
Riwayat Panggilan	Ya
Pesan Teks	Ya
Gambar	Ya

4. SIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa untuk mendapatkan bukti-bukti digital perlu dilakukannya *root* kepada kedua *smartphone* agar memiliki akses full ke perangkat android, yang mana nantinya dilakukan akuisisi dan analisis bukti digital.

- 1) Berdasarkan tahapan dari NIST (*National Institute of Standards and Technology*) penelitian ini dimulai dari pembuatan skenario dan dilakukannya sebuah simulasi kasus, kemudian dilanjut dengan pengumpulan bukti-bukti digital atau *collection*, setelah itu dilakukan proses ekstraksi bukti-bukti digital atau *examination* yang disajikan dalam bentuk artefak (sekumpulan atribut), dilanjut dengan proses analisis bukti digital yang didapatkan berupa pesan percakapan dan juga bukti digital struk transfer atau *analysis*, dan yang terakhir yaitu pelaporan bukti-bukti digital yang telah di peroleh atau *reporting*, yang memperoleh temuan berupa akun dan kontak, riwayat panggilan, pesan teks, serta gambar yang didapatkan dari *smartphone* pembanding.
- 2) Analisis gambar bukti struk transfer ini dilakukan dengan menggunakan bantuan *tools* ForensicallyBeta dengan menerapkan teknik ELA (*Error Level Analysis*). Dengan *error level analysis* dapat diketahui daerah mana yang direkayasa atau diedit dari gambar tersebut, karena pada *error level analysis* apabila terdapat daerah yang berbeda dari yang lain, seperti tekstur, garis tepi, dan warnanya itu terjadi karena adanya level kompresi yang berbeda. Hasil analisis yang diperoleh yaitu gambar struk transfer tersebut telah dimanipulasi sehingga dapat terlihat pada bagian nama pengirim, lokasi, tanggal dan waktu pengiriman, serta di bagian nomor rekening dan juga total biaya pengirimannya terdapat bintik-bintik yang tidak merata atau tidak seimbang serta terlihat adanya perbedaan kontras warnanya. Maka dapat disimpulkan bahwa gambar tersebut telah dimanipulasi.

DAFTAR PUSTAKA

- [1] Z. Akbar, B. Nugraha, and M. Alaydrus, "Whatsapp Forensics Pada Android Smartphone : a Survey," *Sinergi*, vol. 20, no. 3, p. 207, 2016, doi: 10.22441/sinergi.2016.3.006.
- [2] Kemp, S. (2020, February 18). *reports*. Retrieved from datareportal.com: <https://datareportal.com/reports/digital-2020-indonesia>.
- [3] Hariyadi, D., & Pasa, I. Y. "Identifikasi Barang Bukti Percakapan Aplikasi Dual Apps Whatsapp Pada Ponsel Xiaomi Menggunakan Metode Nist Mobile Forensics", *INTEK*, Vol.1, No.1, 1-7, Mei 2018.
- [4] Muhammad, I. S., Imam, R., & Rusydi, U. "Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology

- (NIST)", *Jurnal Sains Komputer & Informatika (J-SAKTI)*, Vol.4, No.1, 170-178, Maret 2020.
- [5] Ikhwan, A., Khairina, E. S., & G, U. "Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ", *IT Journal Research and Development (ITJRD)*, Vol.5, No.2, 118-134, Maret 2021.
- [6] Nasirudin, Sunardi, & Riadi, I. "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express", *Jurnal Informatika Universitas Pamulang*, Vol.5, No.1, 89-94, Maret 2020.
- [7] Forensics, Magnet. (2020). *Magnet Axiom User Guide*. Waterloo: Magnet Forensics.
- [8] Xiaolvyantech. (2018). *ProgrammerSought*. Retrieved from Article: <https://www.programmersought.com/article/61453200964/>.
- [9] Whatsapp. (2021). *Pusat Bantuan*. Retrieved from Whatsapp: <https://faq.whatsapp.com/android/chats/how-to-delete-messages/>.
- [10] Irwansyah, & Yudiastuti, H. "Analisis Digital Forensik Rekayasa Image Menggunakan Jpegsnoop Dan Forensically Beta", *Jurnal Ilmiah MATRIK*, Vol.21, No.1, 54-63, April 2019.