Perbandingan Keamanan dan Performa Aplikasi WhatsApp dan Telegram dengan Menggunakan Metode NIJ

Aulyah Zakilah Ifani [1], Andi Mawaddah Sumardi [2], Novera Baytikhalishah [3], Nurlela [4]
[1] Sistem Teknologi Informasi, Institut Teknologi dan Bisnis Nobel Indonesia, Makassar, Indonesia
[2,3,4] Teknik Komputer, Fakultas Teknik, Universitas Negeri Makassar, Makassar, Indonesia
Email: [1*] aulyah@nobel.ac.id, [2] mwddhsmrdi@gmail.com, [3] noveravera3@gmail.com, [4] nurlela28022004@gmail.com
*Corresponding Author

***Abstract*— Dalam era teknologi informasi saat ini, manusia telah merasakan kemudahan dan efisiensi dalam kehidupan mereka berkat adanya media sosial. Berbagai jenis platform media sosial muncul, termasuk *platform* jaringan sosial seperti Facebook dan LinkedIn, *platform* berbagi foto dan video seperti Instagram dan TikTok, serta *platform* pesan instan seperti WhatsApp dan Telegram. Dalam penelitian ini, dilalkukan eksperimen untuk membandingkan kinerja aplikasi WhatsApp dan *Telegram* menggunakan berbagai alat seperti Virtex, *FTK* Imager, Autopsy, dan Metasploit, pada sistem operasi Windows 11, Android 8 dan 11, serta Kali Linux, dengan menggunakan metode NIJ. Tahapan NIJ dimulai dari Identifikasi, Koleksi, Pemeriksaan, Analisis, Pelaporan. Berdasarkan analisis yang dilakukan, semua eksperimen tidak berhasil. Versi terbaru *WhatsApp* dan *Telegram* ditemukan aman terhadap serangan Virtex, FTK Imager tidak efektif dalam memulihkan file yang dihapus, Metasploit tidak terpengaruh oleh serangan pada versi Windows dan Android yang digunakan, dan Autopsy gagal memulihkan file yang dihapus meskipun dapat mengidentifikasinya.**

Keywords—Data Security, Forensics, National Institute of Justice, Telegram, WhatsApp.

I. PENDAHULUAN

Pada era teknologi informasi saat ini, manusia telah merasakan kemudahan dan efisiensi dalam kehidupannya, terutama dengan adanya media sosial. Namun, terdapat Beberapa ancaman yang bisa didapatkan jika tidak mengetahui keamanan dari aplikasi tersebut [1]. Ancaman ini **bisa** menyebabkan data pribadi dari pengguna menjadi rusak atau dimanipulasi [2]. Media sosial menjadi sarana interaksi antar individu yang saling terhubung dan memiliki fungsi yang beragam sesuai dengan kebutuhan masing-masing [3]. Media sosial adalah jenis media *online* yang terhubung dengan jaringan internet. Melalui media sosial, para pengguna dapat terkoneksi, berinteraksi, dan berbagi pesan atau informasi dengan cara yang interaktif tanpa harus berada dalam satu tempat atau bertemu secara langsung [4].

Media sosial adalah suatu rangkaian perangkat baru yang digunakan untuk berkomunikasi dan bekerja sama, yang memberikan kesempatan bagi orang biasa untuk terlibat dalam berbagai jenis interaksi yang sebelumnya tidak mungkin dilakukan [5]. Jenis media sosial yang tersedia sangatlah beragam, tetapi tidak terbatas pada platform jejaring sosial seperti Facebook dan LinkedIn, platform berbagi foto dan video seperti Instagram dan TikTok, serta platform pesan instan seperti WhatsApp dan Telegram [6] [7].

WhatsApp merupakan aplikasi pesan instan yang memiliki tingkat penggunaan paling tinggi dan sangat populer di kalangan pengguna *smartphone* di seluruh dunia, mencapai sekitar 60% dari total pengguna. Di sisi lain, Telegram menempati peringkat ketiga dengan jumlah pengguna terbanyak [8] [9].

WhatsApp dan Telegram menjadi aplikasi pengganti *Short Message Service* (SMS) dikarenakan platform pesan instan ini murah dan lebih mudah digunakan. Selain itu, memiliki banyak fitur yang berkualitas menjadikannya banyak diminati. Penelitian sebelumnya yang dilakukan oleh [10] dengan jurnal berjudul "*Choosing an Instant Messaging App: Security or Convenience*? *Comparison between Whatsapp and Telegram"* hanya membandingkan keamanan dan performa dengan melihat lalu lintas dengan peneliti sendiri yang bertindak sebagai pelaku yang mengumpulkan dan menafsirkan data-data. Selain itu, penelitian oleh [3] berjudul "Analisis Perbandingan Bukti Digital Forensik pada Instant Messaging Berbasis Smartphone Android menggunakan Framework NIST" membahas tentang perbandingan hasil tingkat kebocoran data pada aplikasi *smartphone*. Hasil yang didapatkan whatsapp memiliki tingkat kebocoran data terbesar.

Jurnal yang akan dibahas ini berjudul "Perbandingan Keamanan dan Performa Aplikasi WhatsApp dan Telegram dengan Menggunakan Metode NIJ". Penelitian ini bertujuan untuk membandingkan keamanan dan performa antara WhatsApp dan Telegram dengan menerapkan sistem Virus Text serta menggunakan beberapa *tools* dengan metode NIJ pada pengiriman pesan teks dan multimedia. Penelitian ini juga membahas perbandingan performa antara WhatsApp dan Telegram pada pengiriman pesan teks dan multimedia. Performa aplikasi ini sangat penting karena dapat mempengaruhi pengalaman pengguna dalam menggunakan aplikasi tersebut.

Penelitian ini diharapkan akan ditemukan hasil yang dapat memberikan pemahaman yang lebih baik tentang keamanan dan performa WhatsApp dan Telegram dengan implementasi Virus Text yang menggunakan beberapa *tools* dan metode NIJ. Selain itu, penelitian ini diharapkan dapat memberikan manfaat bagi pengguna dalam memilih aplikasi

yang tepat dan meningkatkan kesadaran akan pentingnya keamanan dalam penggunaan aplikasi *chat identify them.*

II. METODE PENELITIAN

Penelitian ini memiliki proses berupa eksperimen yang dilakukan dengan cara membandingkan kinerja aplikasi WhatsApp dan Telegram dengan menggunakan *tools* seperti Virtex, FTK Imager, Autopsy, dan Metasploit menggunakan sistem operasi Windows 11, Android 11, dan Kali Linux.

Metode penelitian menggunakan beberapa tinjauan pustaka dan studi literatur. Kedua cara tersebut ditempuh dengan mencari referensi dari artikel, jurnal, paper, dan penemuan sebelumnya serta mengunjungi situs-situs di internet terkait digital forensik, keamanan WhatsApp dan Telegram, dan penggunaan *tools* seperti FTK Imager. Metode pengembangan yang digunakan yaitu *National Institute of Justice* (NIJ) yang digambarkan pada dengan alur Gambar 1.

Gambar 1. Tahapan National Institute of Justice (NIJ).

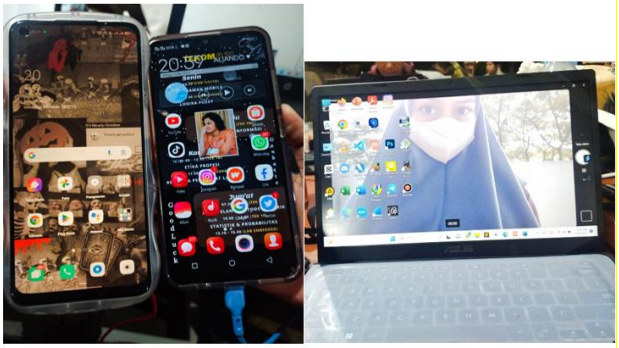
Berikut penjelasan dari tahapan metode *National Institute of Justice* (NIJ) (Nurhairani & Riadi, 2019).

- *Identification* adalah tahap persiapan peralatan yang akan digunakan dalam penyelidikan.
- *Collection* adalah tahap mengumpulkan barang yang akan digunakan dalam penyelidikan.
- *Examination* adalah tahap pemeriksaan data pada barang elektronik yang telah dikumpulkan.
- *Analysis* adalah tahap untuk menganalisa hasil pemeriksaan dari barang elektronik menggunakan metode yang telah ditetapkan.
- *Reporting* adalah tahap melaporkan serta menjelaskan apa yang telah dianalisis (Riadi *et al*., 2018).

III. HASIL DAN PEMBAHASAN

A. *Identification*

Pada penelitian ini perangkat atau *device* yang digunakan dalam keadaan normal dan menyala dengan baik. Perangkat yang digunakan dalam penelitian ini adalah *smartphone* dan laptop.



Gambar 2. Kondisi awal perangkat

Gambar 2. Memperlihatkan bahwa perangkat yang digunakan dalam keadaan menyala, kemudian dokumentasi dari spesifikasi perangkat yang digunakan ditampilkan dalam tabel berikut:

TABEL I. SPESIFIKASI IDENTITAS SMARTRPHONE

Perangkat	Model	SO	RAM (GB)	Versi
Smartphone	Oppo	Android	8.00	11
Smartphone	Vivo	Android	2.00	8

TABEL II. SPESIFIKASI IDENTITAS LAPTOP

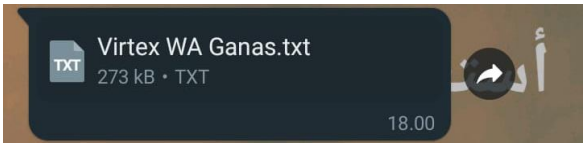
Nama Perangkat	LAPTOP-7R81J37V (ASUS)
Sistem Operasi	Windows
Versi Sistem Operasi	Windows 11
Processor	Intel(R) Core(TM) i3-1005G1 CPU @ 1.20GHz 1.20 GHz
RAM (GB)	4.0

TABEL III. SPESIFIKASI TOOLS

Nama Tools	Versi
Virtex	Video dan Virtex Ganas
FTK Imager	4.7.1.2
Autopsy	4.21.0
Metasploit	6.3.4

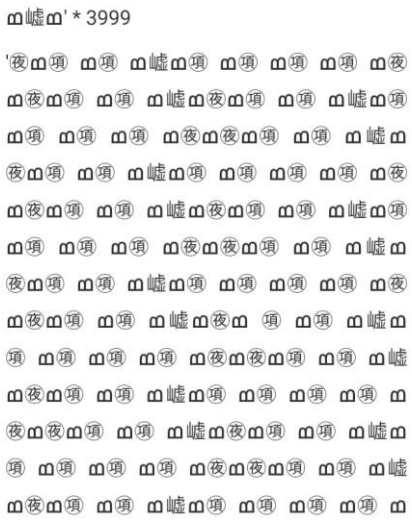
B. *Collection*

Melakukan pengumpulan data kerentanan aplikasi Whatsapp dan Telegram dengan mengirimkan berbagai jenis Virtex melalui aplikasi tersebut, kemudian mengumpulkan data dari folder aplikasi Whatsapp web dan Telegram untuk file yang belum dan telah terhapus. Pengumpulan data tersebut dilakukan pada perangkat laptop dengan menggunakan *tools* FTK Imager. Kemudian uji coba mengumpulkan data dari *smartphone* dengan mengirim file aplikasi Spyware yang dibuat dengan *tools* Metasploit dan dikirimkan melalui aplikasi Whatsapp dan Telegram. Adapun hasil dari pengumpulan data tersebut adalah sebagai berikut:



Gambar 3. Pengiriman File Virtex Melalui Whatsapp

Pada Gambar 4, dapat dilihat dengan jelas isi dari file Virtex yang menjadi fokus penelitian ini dan akan digunakan untuk menyerang aplikasi WhatsApp dan Telegram.



Gambar 4. Isi dari File Virtex

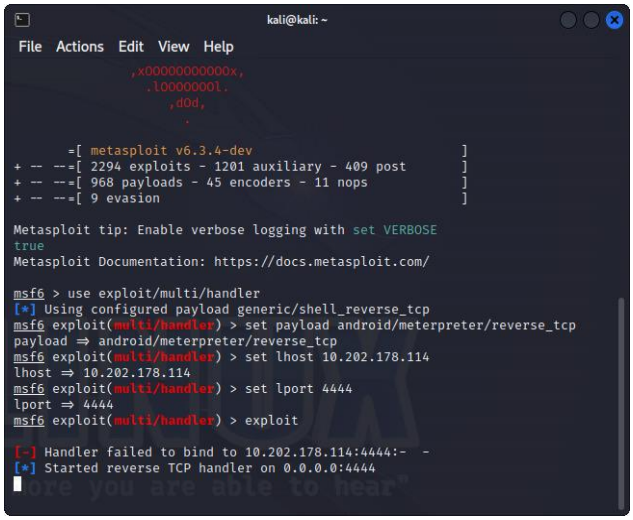
Gambar 5. File Virtex Extensi Video

Pada Gambar 5, terdapat file berekstensi mp4 yang merupakan salah satu jenis format file video yang digunakan dalam penelitian ini. File ini berisi data video yang di dalamnya telah dipasang virtex.

Gambar 6. Pengiriman Video Virtex di Telegram

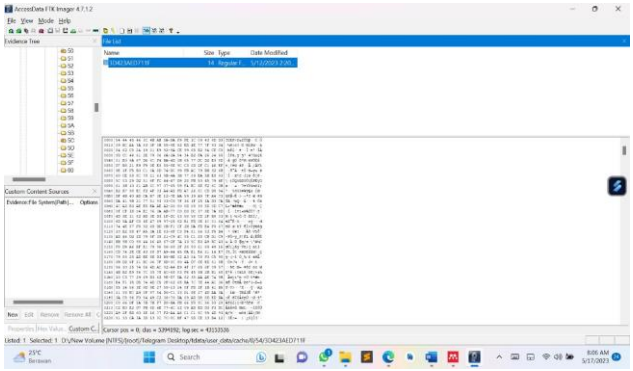
C. *Examination*

Setelah melakukan pengumpulan data pada proses sebelumya, pada tahap ini dilakukan pemeriksaan pada data yang diperoleh. Proses pemeriksaan dilakukan pada perangkat yang dijadikan uji coba. Pada *smartphone* dilihat hasil dari uji coba pengiriman Virtex melalui Whatsapp dan Telegram, kemudian hasil uji coba instalasi aplikasi Spyware pada *smartphone* yang dikirim file aplikasi spyware tersebut. Selanjutnya uji coba pada *tools* FTK Imager untuk melihat keakuratan data yang dapat terbaca dari folder Whatsapp dan Telegram. Berikut adalah beberapa uji coba yang telah dilakukan pada Gambar 7.



Gambar 7. Uji Coba *Tools* Metasploit

Pada Gambar 7, uji coba dilakukan pada sistem operasi Linux menggunakan Metasploit versi 6.3.4. Dilakukan serangkaian eksperimen untuk mengevaluasi kinerja dan keamanan dari WhatsApp dan Telegram pada lingkungan Linux. Uji coba ini melibatkan berbagai skenario dan serangan potensial untuk mengukur efektivitas aplikasi WhatsApp dan Telegram dalam mendeteksi, mencegah, dan mengatasi ancaman keamanan.

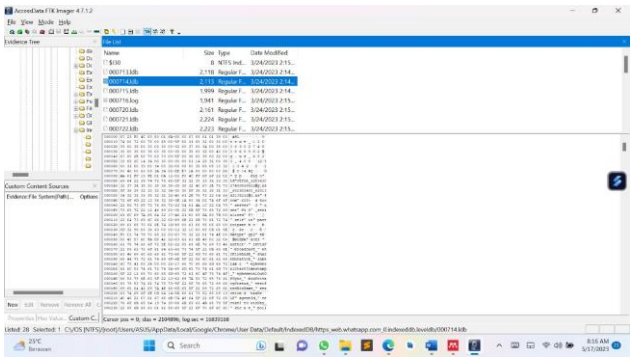


Gambar 8. Uji Coba FTK Imager pada Telegram (File tidak dihapus)

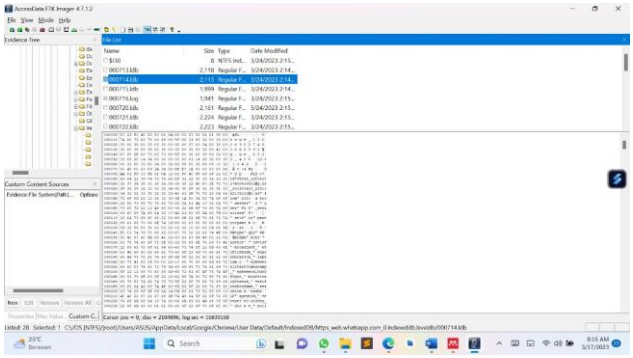
Pada Gambar 8, dilakukan uji coba FTK Imager pada aplikasi Telegram untuk menginvestigasi jejak digital dalam kasus di mana file tidak dihapus. Uji coba ini dirancang untuk menggambarkan kemampuan FTK Imager dalam merekam dan menganalisis data yang ada dalam perangkat komunikasi seperti Telegram ketika pengguna tidak menghapus file atau pesan sehingga memungkinkan untuk memahami lebih dalam jejak-jejak digital yang dapat digunakan dalam investigasi forensik.

Pada Gambar 10, dilakukan uji coba penggunaan FTK Imager untuk melakukan analisis terhadap data yang

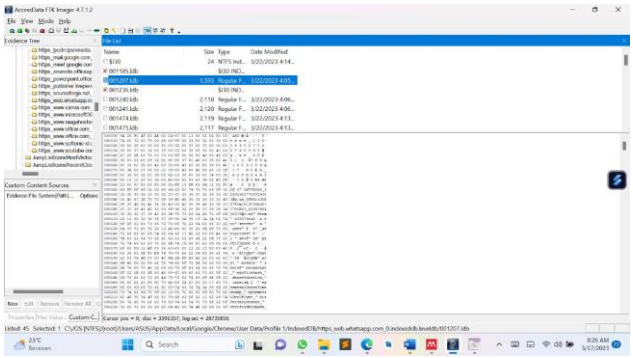
berkaitan dengan Telegram, terutama data yang berkaitan dengan file yang telah dihapus dari platform tersebut. Tujuan dari uji coba ini adalah untuk mengidentifikasi, memulihkan, dan memahami informasi terkait yang mungkin telah dihapus oleh pengguna dalam konteks aplikasi Telegram.



Gambar 10. Uji Coba FTK Imager pada Telegram (File Terhapus)



Gambar 11. Uji Coba FTK Imager pada Whatsapp



Gambar 12. Uji Coba FTK Imager pada Whatsapp

Pada Gambar 11 dan Gambar 12, dilakukan serangkaian uji coba menggunakan FTK Imager untuk menganalisis data dari aplikasi WhatsApp. Dalam uji coba ini, ekstraksi data dilakukan dari perangkat berbasis Android untuk memahami lebih baik tentang penggunaan dan penyimpanan informasi di dalam aplikasi WhatsApp.

D. Analisis

Berikut merupakan tabel analisis hasil pemeriksaan dari uji coba yang telah dilakukan.

TABEL IV. SPESIFIKASI IDENTITAS LAPTOP

	Whatsapp	**Telegram**	**Keterangan**
Virtex	Tidak Berhasil	Tidak Berhasil	Whatsapp dan Telegram versi terbaru yang digunakan saat ini, telah aman dari serangan Virtex.
FTK Imager	Tidak Berhasil	Tidak Berhasil	File yang sudah terhapus tidak dapat teridentifikasi dan tidak terbaca kode hashnya, *signature* mengalami kerusakan.
Metasploit	Tidak Berhasil	Tidak Berhasil	Versi dari perangkat yang digunakan yaitu Windows 11 dan versi Android 8 dan 11 tidak terpengaruh oleh serangan ini dikarenakan sistem keamanan yang ketat.
Autopsy	Tidak Berhasil	Tidak Berhasil	File yang terhapus dapat teridentifikasi, namun file tersebut tidak dapat dibuka atau diakses kembali.

E. Reporting

Berikut ini adalah tahap-tahap pelaporan dari analisis yang telah dilakukan:

1) WhatsApp:
   a) Status: Tidak Berhasil
   b) Keterangan: WhatsApp versi terbaru yang digunakan saat ini telah aman dari serangan Virtex. Ini berarti bahwa tidak ditemukan indikasi adanya kerentanan keamanan atau serangan yang berhasil terhadap aplikasi WhatsApp dalam analisis yang dilakukan.
2) Telegram:
   a) Status: Tidak Berhasil
   b) Keterangan: Telegram versi terbaru yang digunakan saat ini telah aman dari serangan Virtex. Hal ini menunjukkan bahwa aplikasi Telegram tidak menunjukkan kerentanan atau adanya serangan yang berhasil dalam analisis yang dilakukan.
3) FTK Imager:

a) Status: Tidak Berhasil
b) Keterangan: File yang sudah terhapus tidak dapat teridentifikasi dan tidak terbaca kode hashnya. Signature (tanda tangan) dari file juga mengalami kerusakan. Hal ini mengindikasikan bahwa FTK Imager tidak dapat mengambil atau memulihkan file yang sudah terhapus secara efektif.

4) Metasploit:
   a) Status: Tidak Berhasil
   b) Keterangan: Versi perangkat yang digunakan (Windows 11 dan Android 8 dan 11) tidak terpengaruh oleh serangan yang sedang dianalisis. Ini menunjukkan bahwa sistem keamanan yang ketat pada versi Windows dan Android tersebut telah melindungi perangkat dari serangan yang ditargetkan oleh analisis tersebut.
5) Autopsy: (jaraknya dengan atas)
   a) Status: Tidak Berhasil
   b) Keterangan: Dalam analisis yang dilakukan, file yang terhapus dapat teridentifikasi, namun tidak dapat dibuka atau diakses kembali. Ini mengindikasikan bahwa Autopsy tidak dapat memulihkan file yang terhapus dengan berhasil, meskipun mampu mengenali keberadaan file tersebut

Berdasarkan pelaporan dari analisis yang telah dilakukan, seluruhnya berstatus tidak berhasil. WhatsApp dan Telegram versi terbaru aman dari serangan Virtex, FTK Imager tidak dapat efektif memulihkan file yang terhapus, Metasploit tidak terpengaruh oleh serangan pada versi Windows dan Android yang digunakan, dan Autopsy tidak berhasil memulihkan file yang terhapus meskipun dapat mengidentifikasinya.

IV. KESIMPULAN

Berdasarkan hasil dan pembahasan, dapat diketahui bahwa Virtex tidak dapat lagi menyerang keamanan maupun performa WhatsApp dan Telegram. Selain itu, digunakan pula *tools* seperti FTK Imager, Autopsy, dan Metasploit dan didapatkan hasil bahwa file Whatsapp dan Telegram versi terbaru aman dari serangan yang diberikan. Saran untuk peneliti selanjutnya agar bisa mencoba serangan lainnya agar lebih mengoptimalkan lagi Whatsapp dan Telegram. Selain itu, peneliti juga dapat menggunakan media sosial lainnya untuk diuji keamanannya dari berbagai jenis serangan.

REFERENSI

[1] I. Riadi, A. Ifani, and R. Kusuma, "Optimization and Evaluation of Authentication System using Blockchain Technology," *Emerging Science Journal*, vol. 4, pp. 225–240, Feb. 2022, doi: 10.28991/esj-2021-SP1-015.

[2] I. Riadi, Herman, and A. Z. Ifani, "Optimasi Keamanan Web Server terhadap Serangan Broken Authentication Menggunakan Teknologi Blockchain," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 6, no. 3, Art. no. 3, Sep. 2021, doi: 10.14421/jiska.2021.6.3.139-148.

[3] R. B. Kusumadewa and S. Syaifuddin, "Analisis Perbandingan Bukti Digial Forensik pada Instant Messaging Berbasis Smartphone Android menggunakan Framework NIST," *Seminar Keinsinyuran Program Studi Program Profesi Insinyur*, vol. 2, no. 1, Art. no. 1, Aug. 2022, doi: 10.22219/skpsppi.v3i1.5061.

[4] M. S. Alif and A. R. Pratama, "Analisis Kesadaran Keamanan di Kalangan Pengguna E-Wallet di Indonesia," *AUTOMATA*, vol. 2, no. 1, Art. no. 1, Jan. 2021, Accessed: Jul. 03, 2023. [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/view/17279

[5] D. Perwita, "Literasi Media Digital Mahasiswa Universitas Jenderal Soedirman," *EQUILIBRIUM : Jurnal Ilmiah Ekonomi dan Pembelajarannya*, vol. 9, no. 1, Art. no. 1, Jan. 2021, doi: 10.25273/equilibrium.v9i1.8515.

[6] M. B. Yel and M. K. Nasution, "KEAMANAN INFORMASI DATA PRIBADI PADA MEDIA SOSIAL," *Jurnal Informatika Kaputama (JIK)*, vol. 6, no. 1, Art. no. 1, Jan. 2022.

[7] M. A. Alaby, "Media Sosial Whatsapp Sebagai Media Pembelajaran Jarak Jauh Mata Kuliah Ilmu Sosial Budaya Dasar (ISBD)," *Ganaya : Jurnal Ilmu Sosial dan Humaniora*, vol. 3, no. 2, Art. no. 2, Sep. 2020.

[8] F. Fahurian, H. Yunita, K. Zuhri, and Y. Yuniarthe, "Prototipe Sistem Keamanan Ganda Pada Kendaraan Roda Dua Berbasis Android dan WhatsApp Messenger," *IJEIS (Indonesian Journal of Electronics and Instrumentation Systems)*, vol. 11, p. 201, Oct. 2021, doi: 10.22146/ijeis.69189.

[9] R. Normadhoni, S. P. Dewanti, W. C. Namaskara, D. Y. Akhadi, and R. Fauzi, "Penggunaan Bot Telegram sebagai Announcemnt System dalam Dunia Parenting," *Journal of Education and Technology*, vol. 1, no. 1, Art. no. 1, Jun. 2021.

[10] A. Shahrul and A. Wibawa, "Choosing an Instant Messaging App: Security or Convenience? Comparison between Whatsapp and Telegram," *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 3, pp. 115–121, Sep. 2021, doi: 10.12928/biste.v3i2.2784.