Analisis Keamanan Aplikasi Chat Android Pihak Ketiga Atau Non Playstore Menggunakan Digital Forensics

Novi Krisdayanti[a] , Indra Gunawan[b*]

[ab]Sekolah Tinggi Teknologi Ronggolawe Cepu
[b] Penulis Korespondensi, alamat email igunsttr@gmail.com

Diterima : 19-12-2022 - Direview : 20-12-2022 - Diterbitkan : 31-12-2022

Intisari

Aplikasi pihak ketiga adalah aplikasi yang dibuat oleh pengembang bukan pembuat perangkat yang menjalankan aplikasi atau pemilik situs web yang menawarkannya. Tujuan penelitian ini adalah untuk mengetahui tingkat keamanan dari aplikasi chat GB WhatsApp, Telegram Mod, MiChat Mod, WeChat Mod, dan Line Mod. Analisis digital forensik ini menggunakan 2 metode yaitu statis dengan menggunakan Wireshark sebagai aplikasi perekam aktifitas kinerja jaringan dan dinamis dengan menggunakan Network Miner sebagai aplikasi untuk mengumpulkan data tentang lalu lintas pada jaringan. Hasil penelitian menggunakan metode statis menunjukkan bahwa kelima aplikasi memiliki izin hak akses yang berbahaya, sedangkan menggunakan metode dinamis menunjukkan bukti terdapat kebocoran data pada chat pribadi.

Kata Kunci : ***Aplikasi Pihak Ketiga;Forensika Digital; Analisis Statis; Analisis Dinamis.***

Abstract

Third-party applications are applications that are created by developers not the makers of the devices running the applications or the owners of the websites that offer them. The purpose of this study was to determine the security level of the GB WhatsApp chat application, Telegram Mod, MiChat Mod, WeChat Mod, and Line Mod. This digital forensic analysis uses 2 methods, namely static using Wireshark as an application for recording network performance activities and dynamic using Network Miner as an application to collect data about traffic on the network. The results of the study using the static method showed that the five applications had malicious permissions, while using the dynamic method showed evidence of data leakage in private chats.

Keywords : ***Third-party applications;Digital Forensics;Static Analysis; Dynamic Analysis*.**

1. Pendahuluan

Seiring berkembangnya era globalisasi terutama pada bidang telekomunikasi mendorong seseorang untuk menggunakan teknologi informasi yang akan mempermudah manusia dalam hal berkomunikasi salah satunya yaitu dengan menggunakan Smartphone Android. Salah satu sistem operasi yang banyak digunakan oleh pengguna Smartphone Android adalah aplikasi chatting. Hal ini yang menyebabkan aplikasi chatting mulai marak bermunculan dengan berbagai fitur yang dibuat semenarik mungkin agar dapat memanjakan penggunanya. Banyaknya aplikasi yang ada dan bermunculan modifikasi aplikasi-aplikasi baru membuat seseorang ingin mencoba berbagai fitur baru yang di sajikan oleh berbagai aplikasi modifikasi, salah satunya aplikasi chat dari pihak ketiga.

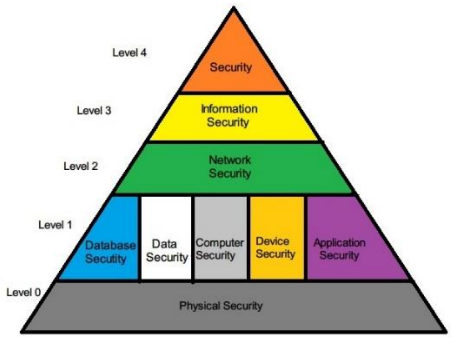
Ancaman pada keamanan aplikasi memiliki beberapa level. Pengamanan computer atau smartphone android dilakukan berdasarkan level dan sistem. Berdasarkan level, pengamanan disusun seperti piramida, yaitu keamanan level 0, level 1, level 2, level 3, dan level 4. Sedangkan berdasarkan sistem pengamanan komputer atau smartphone android dibedakan menjadi network topology, security information management, dan IDS/IPS. Untuk mengatasi masalah ini, pengguna perlu melakukan analisis digital forensik terhadap fitur-fitur yang ada. Analisis digital forensik ini nantinya akan menghasilkan bukti digital yang berisi aman atau tidaknya pada aplikasi – aplikasi tersebut. Analisis ini dibuat agar

pengguna bisa lebih berhati-hati dalam mengunakan aplikasi tersebut, dan bisa mengatasi permasalahan yang akan muncul dikemudian hari. Penelitian yang dilakukan ini diharapkan dapat menghasilkan bukti digital. Tujuan penelitian ini adalah untuk mengetahui tingkat keamanan aplikasi chat GB WhatsApp, Telegram Mod, MiChat Mod, WeChat Mod, dan Line Mod dengan menggunakan analisis Digital Forensic

2. Kerangka Teori

2.1. Level Keamanan Smartphone

Keamanan Level 0 merupakan keamanan fisik (physical security) atau keamanan tingkat awal. Apabila keamanan fisik terjaga maka keamanan di dalam smartphone juga akan terjaga. Keamanan Level 1 terdiri dari *database security, data security, dan device security*. Dari pembuatan *database* dapat dilihat apakah digunakan aplikasi yang sudah diakui keamanannya. Selanjutnya adalah memperhatikan *data security* yaitu desain *database*, karena pendesain database harus memikirkan kemungkinan keamanan dari database. Terakhir adalah *device security* yaitu alat yang dipakai untuk keamanan dari *database* tersebut. Keamanan level 2 merupakan keamanan dari segi keamanan jaringan. Keamanan ini merupakan tindak lanjut dari keamanan level 1. Keamanan level 3 merupakan *information security*. Informasi -informasi seperti kata sandi yang dikirimkan kepada teman atau file-file yang penting, karena takut ada orang yang tidak sah mengetahui informasi tersebut. Keamanan Level 4 adalah keseluruhan dari keamanan level 1 sampai level 3. Apabila satu dari keamanan itu tidak terpenuhi maka keamanan level 4 juga tidak terpenuhi. (Mia A,2013).



Gambar 1 Tingkat Keamanan Smartphone

2.2. *GB WhatsApp*

WhatsApp GB merupakan modifikasi dari WhatsApp Plus, yang juga aplikasi hasil modifikasi. WhatsApp Plus sendiri sudah diblokir oleh pihak WhatsApp. Aplikasi tidak resmi ini sejatinya hanya bisa digunakan di platform Android. Namun, WhatsApp GB tidak akan ditemukan di Play Store. Aplikasi ini hanya bisa diunduh lewat APK dari sumber pihak ketiga, seperti situs web. Seperti diketahui, mengunduh aplikasi dari pihak ketiga, lebih berisiko dibanding mengunduh aplikasi lewat Play Store.

2.3 *Telegram*

Telegram adalah sebuah aplikasi layanan pengirim pesan instan multiplatform berbasis awan yang bersifat gratis dan nirlaba. Klien Telegram tersedia untuk perangkat telepon seluler (Android, iOS, Windows Phone, Ubuntu Touch) dan sistem perangkat komputer (Windows, OS X, Linux). Para pengguna dapat mengirim pesan dan bertukar foto, video, stiker, audio, dan tipe berkas lainnya. Telegram juga menyediakan pengiriman pesan enkripsi ujung-ke-ujung opsional.

2.4 *MiChat*

MiChat merupakan aplikasi perpesanan instan gratis yang bikin oleh MiChat PTE. Limited dan bermarkas di Singapura. Aplikasi ini memungkinkan pengguna bisa bertemu dengan teman baru, termasuk di lokasi sekitar pengguna berada. Setelah pengguna mengunduh MiChat, selanjutnya aplikasi akan mendeteksi kontak yang tersimpan di ponsel pengguna, yang mana kontak-kontak tersebut kemudian bisa ditambahkan ke daftar teman.

2.5 *WeChat*

WeChat adalah layanan komunikasi pesan suara dan teks telepon seluler (ponsel) yang dikembangkan oleh Tencent di Tiongkok. Aplikasi ini dapat digunakan pada beberapa sistem operasi, seperti Android, iPhone, BlackBerry, Windows Phone, dan platform Symbian. Bahasa yang didukung termasuk Bahasa Inggris, Hanzi tradisional/disederhanakan, Indonesia, Spany ol, Portugis, Thailand, Vietnam, dan Rusia. WeChat didukung pada Wi-Fi, 3G, dan data 4G jaringan.

2.6 *Line*

LINE adalah sebuah aplikasi pengirim pesan instan gratis yang dapat digunakan pada berbagai platform seperti telepon cerdas, tablet, dan komputer. LINE difungsikan dengan menggunakan jaringan internet sehingga

pengguna LINE dapat melakukan aktivitas seperti mengirim pesan teks, mengirim gambar, video, pesan suara, dan lain lain. LINE diklaim sebagai aplikasi pengirim pesan instan terlaris di 42 negara. LINE dikembangkan oleh perusahaan Jepang bernama NHN Corporation. LINE pertama kali dirilis pada Juni 2011 dan mulanya hanya dapat digunakan pada sistem iOS dan Android

2.7 *Software Wireshark*

Program ini dapat merakam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin, misalnya postingan komentar kamu di blog atau bahkan Username dan Password. Kamu harus bisa menggunakannya dengan bijak. Sebenarnya Wireshark tidak di desain untuk peretasan/hacker. Fungsi aplikasi wireshark utamanya tidak diperuntukkan untuk hacking. Fungsi aplikasi Wireshark yang utama adalah sebagai Administrator Jaringan untuk dapat melacak apa yang terjadi didalam jaringan miliknya atau untuk memastikan jaringannya bekerja dengan baik, serta tidak ada yang melakukan hal-hal buruk pada jaringan itu.

2.8 *Software Network Miner Packet Analizer*

Network Miner Packet Analizer adalah suatu alat yang dapat menganalisis jaringan (Network Forensic Analisys Tool) atau biasa disingkan NFAT untuk system operasi windows. NetworkMiner dapat di gunakan sebagai alat sniffer atau alat untuk menangkap data-data paket dalam hal ini untuk mendeteksi sistem operasi, sesi, nama Host, port yang terbuka (open Ports), dan lain-lain tanpa membebankan sedikitpun traffic pada jaringan. NetworkMiner juga dapat mengurai file PCAP untuk di analisis secara off-line.

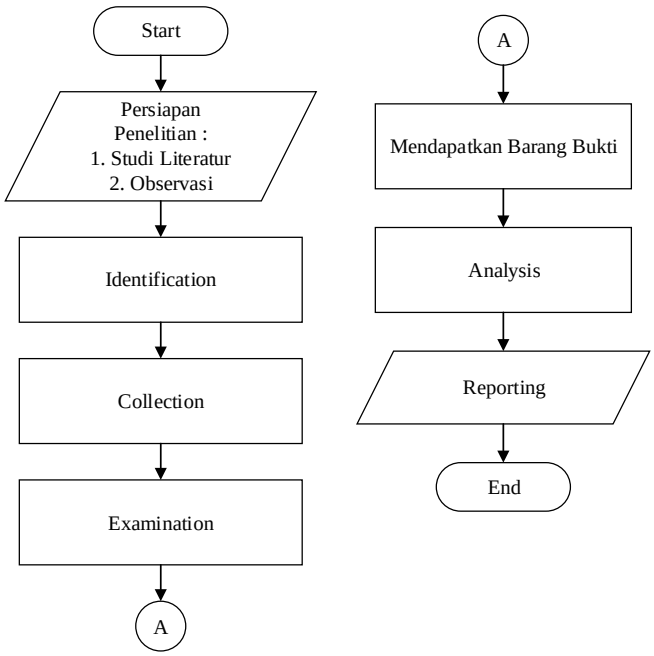
2.9 Digital Forensics

Digital forensic merupakan aktifitas penyelidikan yang dilakukan untuk menemukan bukti digital yang akan memperkuat atau melemahkan bukti fisik dari kasus yang ditangani. Istilah forensik digital pada awalnya identik dengan forensik komputer. tetapi saat ini berkembang menjadi lebih luas yaitu menganalisa semua perangkat yang dapat menyimpan data digital. Forensik digital sendiri diperlukan karena biasanya data di perangkat digital dikunci, diganti, disembunyikan atau bahkan dihapus.

3. Metodologi

3.1 Desain Peneitian

Diagram alir penelitian sangat dibutuhkan untuk melakukan perencanaan proses, analisis proses, dan dokumentasi proses sebagai pedoman untuk melakukan suatu penelitian. Berikut diagram alir penelitian yang ditampilkan pada gambar 3.1.



Gambar 3.1 Desain Penelitian

3.1.1 Metode Pengumpulan Data

Dalam penelitian ini menggunakan metode pengumpulan data meliputi :

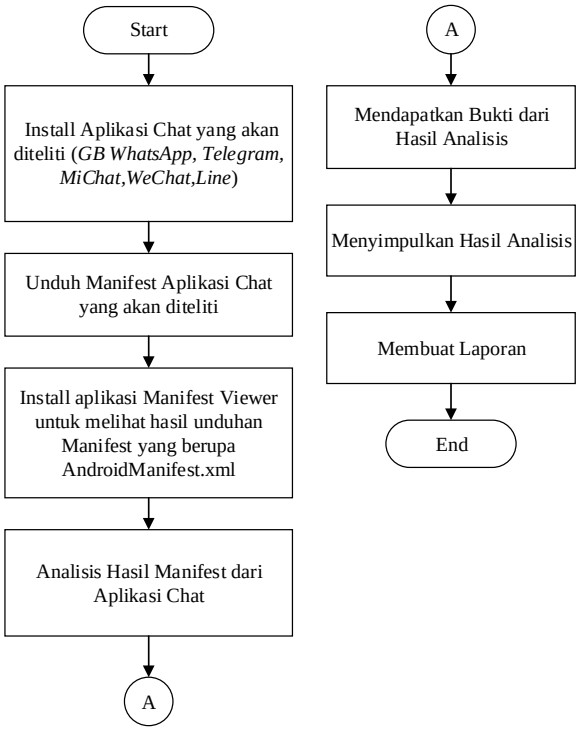
a. Studi Literatur

Studi literatur ini dilakukan oleh penulis untuk mengumpulkan sumber- sumber tertulis, dengan cara membaca, mempelajari dan mencatat hal-hal penting yang berhubungan dengan masalah yang sedang diteliti.

b. Observasi

Observasi yang dilakukan oleh peneliti adalah dengan mengamati secara langsung terhadap objek penelitian. Observasi dilakukan untuk memperoleh informasi secara langsung terhadap permasalahan yang sedang diteliti untuk menentukan system yang benar-benar sesuai.

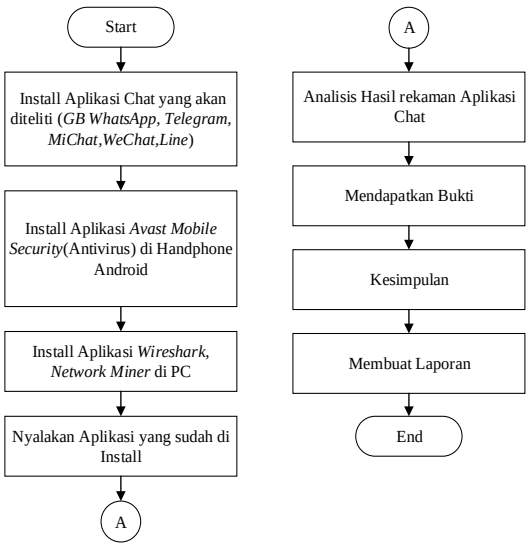
3.2 Digital Forensik Statis



Gambar 2 Diagram Alir Analisis Statis

Analisis Statis merupakan metode analisis aplikasi tanpa menjalankan aplikasi tersebut. Cara kerja metode analisis statis yaitu penulis akan me-review kodingan dari aplikasi untuk menemukan fungsi yang mencurigakan. Fungsi mencurigakan yang dimaksud adalah kode sensitif berupa username default, pin atau password. Keluaran dari proses ini yaitu signature yang dapat digunakan,salah satu fungsinya yaitu untuk mengetahui jenis enkripsi yang digunakan untuk mengamankan aplikasi.

3.2.1 Digital Forensik Dinamis



Gambar 3 Diagram Alir Analisis Dinamis

Analisis Dinamis merupakan metode analisis aplikasi dengan menjalankan aplikasi. Keuntungan dari analisis ini yaitu aplikasi yang diuji diperiksa dan diaktifkan menggunakan mesin virtual untuk selanjutnya dapat dikumpulkan informasi dari analisis yang dilakukan.

4. Hasil dan Pembahasan (Times New Roman, 10 Bold)

4.1 *Static Analysis*

Analisis statis yang dilakukan pada penelitian ini menggunakan aplikasi android Manifest Viewer yang bernama *SQLite Reader/Viewer*. Dimana *SQLite Reader/Viewer* berfungsi sebagai pembaca activity-activity berbentuk *AndroidManifest.xml* yang terdapat pada aplikasi, berupa daftar kelas-kelas java,penggunaan intent untuk pemilihan, dan pemberian label/title pada suatu activity saat mereka aktif.

4.1.1Permissions Analysis

File *AndroidManifest.xml* mengandung informasi yang dibutuhkan oleh sistem Android, seperti version number, metadata, package name, fungsi dan perizinan yang dibutuhkan oleh aplikasi ketika proses pemasangan atau pada saat runtime. Hasil analisis terhadap hak akses file dapat dilihat pada Tabel 1.

Tabel 1 Temuan Hak Akses Berbahaya

No	Nama Aplikasi	Jumlah	Temuan Hak Akses Berbahaya
1	GB WhatsApp	7	read_phone_state, access_coarse_location, access_fine_location, camera, internet, read_contacts, dan read_external_storage
2	Telegram	8	access_coarse_location, access_fine_location, internet, read_contacts, system_alert_window, read_phone_state, camera, dan access_background_location
3	MiChat	10	internet, read_external_storage, read_contacts, read_phone_state, access_coarse_location, access_fine_location, camera, system_alert_window, interact_across_users_full, dan interact_across_users.
4	WeChat	9	access_coarse_location, access_fine_location, camera, system_alert_window,

			download_without_notification, read_phone_state, read_external_storage, dan access_background_location
5	Line	9	camera, read_contacts, internet, read_phone_state, access_coarse_location, access_fine_location, access_location_extra_commands, system_alert_window, dan read_external_storage.

4.2 Dinamic Analysis

Analisis dinamis yang dilakukan pada penelitian ini menggunakan aplikasi NetworkMiner dan *Avast Antivirus (AVG).* Dimana Network Miner berfungsi sebagai alat analisis jaringan (NFAT). Yang dapat digunakan sebagai alat pengintai paket jaringan pasif yang adapat digunakan untuk mendeteksi sistem operasi, sesi,nama host, open port, dan lain-lain tanpa perlu menempatkan lalu lintas di jaringan secara langsung. Sedangkan Avast Antivirus berfungsi sebagai pelindung dan pemindai aplikasi untuk menemukan tanda-tanda adanya bahaya yang mengintai pada smartphone android.

4.2.1 Network Miner

Setelah melakukan rekaman jaringan menggunakan Wireshark, file yang didapat dari rekaman tersebut akan di analisis menggunakan aplikasi Network Miner. Untuk mengetahui adanya file, image, messages yang dapat terdeteksi atau tidak. Hasil analisis paket data pada jaringan dapat dilihat pada tabel 2.

Tabel 2 Temuan Hak Akses Berbahaya

No	Nama Aplikasi	Temuan file
1	GB WhatsApp	-
2	Telegram	-
3	MiChat	Gambar, dokumen, stiker
4	WeChat	Gambar, dokumen
5	Line	-

4.3 Risk Level Aplikasi

Tingkat keamanan ini dapat dibagi dengan beberapa tingkat (level) yaitu : Keamanan Level 0 merupakan keamanan fisik (physical security) atau keamanan tingkat awal. Apabila keamanan fisik terjaga maka keamanan di dalam smartphone juga akan terjaga. Keamanan Level 1 terdiri dari *database security*, *data security*, *dan device security*. Dari pembuatan *database* dapat dilihat apakah digunakan aplikasi yang sudah diakui keamanannya. Selanjutnya adalah memperhatikan *data security* yaitu desain *database*, karena pendesain database harus memikirkan kemungkinan keamanan dari database. Terakhir adalah *device security* yaitu alat yang dipakai untuk keamanan dari *database* tersebut. Keamanan level 2 merupakan keamanan dari segi keamanan jaringan. Keamanan ini merupakan tindak lanjut dari keamanan level 1. Keamanan level 3 merupakan *information security*. Informasi -informasi seperti kata sandi yang dikirimkan kepada teman atau file-file yang penting, karena takut ada orang yang tidak sah mengetahui informasi tersebut. Keamanan Level 4 adalah keseluruhan dari keamanan level 1 sampai level 3. Apabila satu dari keamanan itu tidak terpenuhi maka keamanan level 4 juga tidak terpenuhi. (Mia A,2013). Level Keamanan dari 5 Aplikasi diatas dapat dilihat pada tabel 3.

Tabel 3 Tingkat Keamanan Lima Aplikasi Chat

No	Nama Aplikasi	Tingkat Keamanan
1	GB WhatsApp	*Level 1*
2	Telegram	*Level 1*
3	MiChat	*Level 1*
4	WeChat	*Level 1*
5	Line	*Level 1*

5. Simpulan

Untuk mengetahui tingkat keamanan aplikasi chat GB WhatsApp, Telegram Mod, MiChat Mod, WeChat Mod, dan Line Mod dengan menggunakan analisis Digital Forensic dengan menggunakan metode statis dinamis. Framework yang digunakan memiliki 5 (lima) tahapan yaitu : Identification, Collection, Examination, Analysis, dan Reporting.

Dari penelitian yang dilakukan didapatkan hasil dari tabel risk level menunjukkan bahwa aplikasi chat GB WhatsApp, Telegram Mod, MiChat Mod, WeChat Mod, dan Line Mod memasuki level 1, yang artinya database security,

data security dan device security belum memiliki keamanan yang yang sesuai aplikasi chat resmi pada umumnya.

Manfaat dari penelitian ini adalah diharapkan penelitian ini mampu memberikan pengetahuan untuk masyarakat umum khususnya yang awam akan bahaya aplikasi chat tidak resmi (pihak ketiga) akan adanya kebocoran data dan penyalahgunaan data pribadi. Yang nantinya diharapkan akan lebih selektif dalam memilih aplikasi chat yang aman dan memiliki izin resmi.

Daftar Pustaka

Anshori, I., Putri, K. E., & Ghoni, U. (2021). Analisis Barang Bukti Digital Aplikasi Facebook Pada Smartphone Android Menggunakan Metode Nij. *It Journal Research And Development* (Itjrd), Vol 5, No.2, 11-134.

Anton Yudhana, Imam Riadi, & Ikhsan Zuhriyanto. (2019). Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (Dfrws). Vol.20,No.2, Oktober 2019,125-130.

Anwar, N.,& Imam Riadi (2017). Analisis Investigasi Forensik Whatsapp Messenger Smartphone Terhadap Whatsapp Berbasis Web. Jurnal Ilmu Teknik Elektro Komputer Dan Informatika (Jitek) Vol.3, No. 1, 1-10.

Gashi, E. (2018). Pemission-Based Privacy Analysis For Android Applications. *Ubt Knowledge Center*.

Gunawan, I. &. (2017). Analisis Keamanan Jaringan Wifi Pendekatan Blackbox Dan Whitebox (Studi Kasus Ibnu Sina Batam). *In Sisiti: Seminar Ilmiah Sistem Informasi Dan Teknologi Informasi, (Vol.5, No.1).*

Gunawan, I. (2021). Analisis Malware Botnet Proteus Pendekatan Static Dan Dinamic. *Simetris, 15(1)*, 12-17.

Gunawan, I. (2021). Keamanan Data: Teori Dan Implementasi. Jejak.

Imam Riadi, Sunardi, & Muhamad Ermansyah Rauli. (2018). Identifikasi Bukti Digital Whatsapp Pada Sistem Operasi Proprietary Menggunakan Live Forensics. *Jurnal Teknik Elektro Vol. 10 No. 1*, 18-22.

Imam Riadi, Rusdy Umar, & Dora Bernadisman. (2019). Analisis Forensik Database Menggunakan Metode Forensik Statis. *Jurnal Sistem Informasi Bisnis 01 (2019)*, 9-1

Karuniawan, M. I. (2018). Penerapan Analisis Dinamis Untuk Pengujian Aplikasi Sia Umj Mobile. *Jurusan Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Jember*, 1-9.

Melania, D., & Gunawan, I. (2021). Analisis Keamanan Aplikasi Android Non Playstore Dengan Metode Digital Forensik Pendekatan Statis Dan Dinamis. *Simetris, 15(2)*, 29-34.

Muhammad Abdul Aziz, Imam Riadi, & Rusydi Umar. (2018). Analisis Forensik Line Messenger Berbasis Web Menggunakan Framework National Institute Of Justice (Nij). *Upn "Veteran" Yogyakarta, 24 November 2018*, 51-57.

Palallo, E., & Dr. Irwan Sembiring,S.T.,M.Kom. (2017). Analisis Dan Investigasi Mobile Forensik Pada Aplikasi Whatsapp . *Universitas Kristen Satya Wacana*, 7-25.

Prasongko, R. Y., Yudhana, A., & Fadil, A. (2018). Analisa Forensik Aplikasi Kakaotalk Menggunakan Metode National Institute Standard Technology. *Seminar Nasional Informatika*, 129-133.

Qibriya, M. R., Ambarwati, A., & Susilo, K. E. (2021). Analisis Forensik Digital Pada Aplikasi Instant Messaging Di Smartphone Berbasis Android Untuk Bukti Digital. *Jurnal Teknologi Informasi*, 112-121.

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (Nij). Elinvo(Electronics, Informatics, And Vocational Education), 70-82.

Riskiyadi, M. (2020). Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime. *Cybersecurity Dan Forensik Digital Vol. 3, No. 2, November 2020*, 12-21.

Sunardi, Imam Riadi, & Muh. Hajar Akbar. (2020). Penerapan Metode Static Forensics Untuk Ekstraksi File Steganografi Pada Bukti Digital Menggunakan Frameworks Dfrws. *Jurnal Resti (Rekayasa Sistem Dan Teknologi Informasi) Vol. 4 No.3*, 2-9.

Syukur Ikhsani, & Bekti Cahyo Hidayanto. (2016). Analisa Forensik Whatsapp Dan Line Messenger Pada Smartphone Android Sebagai Rujukan Dalam Menyediakan Barang Bukti Yang Kuat Dan Valid Di Indonesia. *Jurnal Teknik Its Vol. 5, No. 2, (2016)*, 728-736.

Triawan Adi Cahyanto, Victor Wahanggara, & Darmawan Ramadana. (2017). Analisis Dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis Dan Malware Analisis Statis. *Jurnal Sistem & Teknologi Informasi Indonesia, Vol. 2, No. 1, Februari 2017*, 19-30.