

Analisis Forensik Digital Aplikasi Michat Menggunakan Metode National Institute of Standards and Technology (NIST)

Cristian Jonathan¹, Novi Safriadi², Fauzan Asrin³

^{1,2,3}Informatika, Fakultas Teknik, Universitas Tanjungpura

Corresponding Author: d1041201039@student.untan.ac.id¹, safriadi@informatics.untan.ac.id²,
asrin@informatika.untan.ac.id³

Published: June, 2025

ABSTRAK

MiChat merupakan salah satu media sosial populer untuk kategori aplikasi Instant Messenger yang memungkinkan penggunaanya mengirim pesan teks, melakukan panggilan suara, serta berbagi gambar, audio, dan video. Popularitas MiChat diiringi dengan potensi penyalahgunaan aplikasi ini untuk aktivitas yang melanggar hukum, termasuk penyebaran konten pornografi. Penelitian ini bertujuan untuk melakukan simulasi dan pengangkatan barang bukti kejahatan digital terkait penyebaran konten pornografi pada aplikasi MiChat menggunakan metode National Institute of Standards and Technology (NIST). Metode ini dipilih karena menyediakan panduan kerja terstandarisasi yang terdokumentasi memastikan proses forensik engan baik dan hasilnya dapat dipertanggungjawabkan. Penelitian ini menggunakan perangkat lunak MOBILedit Forensic Express untuk mengekstraksi data dari aplikasi MiChat yang terpasang pada perangkat Android. Hasil penelitian menunjukkan bahwa MOBILedit Forensic Express berhasil menemukan dan mengekstrak bukti digital berupa 13 gambar, 1 file audio, dan 9 video yang mengindikasikan aktivitas penyebaran konten pornografi melalui aplikasi MiChat. Kesimpulan dari penelitian ini adalah ditemukannya bukti bukti igital yang relevan dan mengindikasikan adanya enyebaran konten pornografi, sehingga dapat digunakan sebagai bahan investigasi lebih lanjut dalam kasus kejahatan digital.

Kata kunci: MiChat, NIST, Forensik Digital, Mobile Forensik, MOBILedit Forensic Express

ABSTRACT

MiChat is one of the most popular social media platforms in the Instant Messenger application category, allowing users to send text messages, make voice calls, and share images, audio, and videos. However, its popularity is accompanied by the potential misuse of the application for illegal activities, including the distribution of pornographic content. This study aims to simulate and collect digital crime evidence related to the distribution of pornographic content on the MiChat application using the National Institute of Standards and Technology (NIST) method. This method was chosen because it provides a standardized and well-documented work guideline that ensures the forensic process is properly conducted and the results are accountable. The study utilizes the MOBILedit Forensic Express software to extract data from the MiChat application installed on an Android device. The results show that MOBILedit Forensic Express successfully identified and extracted digital evidence consisting of 13 images, 1 audio file, and 9 videos indicating the distribution of pornographic content through the MiChat application. The conclusion of this study is that relevant digital evidence was found, indicating the distribution of pornographic content, which can be used for further investigation in digital crime cases.

.Keywords: MiChat, NIST, Digital Forensics, Mobile Forensics, MOBILedit Forensic Express

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0>

PENDAHULUAN

Penggunaan smartphone di Indonesia terus meningkat, dengan lebih dari 211 juta pengguna. Perkembangan ini memicu berbagai aktivitas digital, namun juga meningkatkan risiko kejahatan siber, seperti prostitusi online. Salah satu aplikasi yang sering digunakan dalam kasus ini adalah MiChat, yang memungkinkan pelaku beroperasi

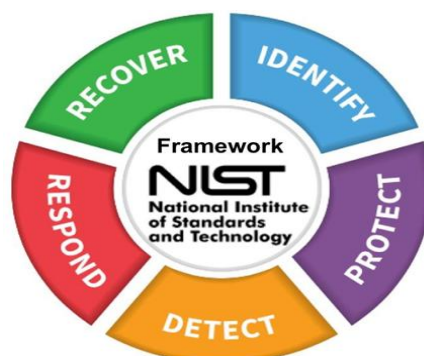
secara anonim. Data KPAI mencatat bahwa dari Januari hingga April 2021, 60% dari 35 kasus eksploitasi seksual anak dilakukan secara online, dan 41% di antaranya melibatkan MiChat. [1]

Untuk mengungkap kasus-kasus tersebut, diperlukan analisis forensik digital yang dapat menelusuri aktivitas dalam aplikasi. Metode National Institute of Standards and Technology (NIST) digunakan karena menyediakan pedoman kerja terstandarisasi dan terdokumentasi. [2] Metode ini telah terbukti efektif dalam berbagai kasus forensik digital lainnya. Penelitian ini bertujuan memperoleh bukti digital dari aplikasi MiChat, seperti pesan, gambar, dan video, menggunakan alat forensik guna mendukung proses hukum secara sah dan efisien. [3]

LANDASAN TEORI

Nist CyberSecurity Framework

NIST Cybersecurity Framework (CSF) adalah kerangka kerja yang dikembangkan oleh National Institute of Standards and Technology (NIST) untuk membantu organisasi manajemen risiko keamanan cyber. CSF ini terdiri dari lima fungsi utama, yaitu Identify, Protect, Detect, Respond, dan Recover.



Gambar 1. Framework Nist

CSF terdiri dari lima fungsi utama yaitu :

1. Identify: Mengidentifikasi aset-aset digital yang relevan dengan organisasi dan menentukan risiko keamanan yang terkait.
2. Protect: Melindungi aset-aset digital dari ancaman keamanan dengan mengimplementasikan kontrol keamanan yang efektif.
3. Detect: Mendeteksi ancaman keamanan yang mungkin terjadi pada aset-aset digital dengan menggunakan sistem deteksi intrusi (IDS) atau sistem monitoring log.
4. Respond: Menanggapi ancaman keamanan yang terdeteksi dengan mengisolasi sistem atau perangkat yang terkena serangan dan melaporkan kepada tim keamanan internal atau eksternal.

5. Recover: Memulihkan sistem atau perangkat yang terkena serangan ke keadaan normal dengan mengembalikan sistem atau perangkat ke keadaan semula dan memastikan bahwa aset-aset digital aman dari ancaman keamanan. [4]

Mobile Forensik

Digital Forensik adalah aplikasi teknologi komputer yang digunakan untuk memperoleh bukti hukum (pro justice) menggunakan teknologi canggih atau komputer untuk membuktikan kejahatan, dan menggunakan bukti digital untuk memerangi Korespondensi : Novi Safriadi penjahat [5]–[10]. Salah satu sub-bidang forensik digital yang sangat relevan adalah Mobile Forensik, yang bertujuan untuk menemukan dan menganalisis bukti digital yang terkait dengan perangkat seluler secara sah. Hasilakhir dari Mobile Forensik adalah bukti elektronik atau file digital. Dalam dunia yang semakin terkoneksi secara digital, pentingnya bukti digital dalam menyelidiki kejahatan siber, pemalsuan, atau pencurian identitas tidak dapat diabaikan. Mobile Forensik memegang peranan sentral dalam memastikan bahwa bukti-bukti yang berasal dari perangkat seluler diproses dengan cara yang sah dan dapat diterima dalam ranah hukum. Ini memerlukan pemahaman yang mendalam tentang teknologi perangkat seluler, perangkat lunak forensik, serta prosedur hukum yang berlaku.

Michat

Aplikasi Michat, yang menempati urutan ke-7 di Indonesia, seperti yang terlihat dalam Gambar 5.5.1, telah menjadi bagian tak terpisahkan dari kehidupan digital sehari-hari. Namun, dengan semakin banyaknya aplikasi pesan singkat yang tersedia, seringkali tidak diimbangi dengan sistem keamanan yang memadai [11]. Dampak dari kurangnya keamanan ini adalah meningkatnya risiko penyalahgunaan aplikasi pesan singkat untuk tindak kejahatan. Salah satu aplikasi yang seringkali disalahgunakan di Indonesia adalah aplikasi MiChat [12]. Aplikasi MiChat digunakan dalam berbagai kasus cybercrime, seperti perdagangan narkoba, penindasan digital, ekstorsi melalui pesan-pesan yang mengancam, dan yang akan menjadi fokus penelitian , yaitu prostitusi online Kejahatan-kejahatan ini seringkali menggunakan MiChat sebagai platform utama untuk menjalankan aktivitas ilegal mereka. [13].

Forensik Media Sosial

Selain Mobile Forensik, Forensik Media Sosial juga memiliki peran penting dalam dunia investigasi digital. Media sosial sering mengandalkan infrastruktur awan untuk menyimpan data pengguna, yang menciptakan tantangan dalam pengumpulan bukti digital. Forensik digital dalam komputasi awan menjadi semakin relevan dalam menjaga integritas dan keabsahan bukti digital yang berasal dari platform media sosial. Dalam dunia informasi saat ini, media sosial telah menjadi saluran utama untuk berkomunikasi, berbagi informasi, dan berinteraksi secara daring. Oleh karena itu, penelitian dalam

bidang forensik media sosial semakin penting, terutama dalam menangani berbagai jenis tindak kejahatan digital, seperti kejahatan siber, pemalsuan, penyelidikan korupsi, pemantauan terorisme, dan banyak lagi.

MobileEdit Forensic

Peneliti telah menggunakan evaluasi untuk mengukur dan memverifikasi keandalan dan akurasi dua alat forensik seluler yang paling terkemuka, seperti MOBILEdit Forensic dan Oxygen Forensics, berdasarkan pada Spesifikasi Alat Ponsel Cerdas oleh NIST. MobileEdit Forensic merupakan perangkat lunak yang dirancang oleh Compelson Labs, sebuah perusahaan yang berfokus pada pengembangan solusi forensik digital. Perangkat ini telah menjadi alat yang sangat berharga bagi peneliti, forensikwan, dan praktisi keamanan siber dalam menghadapi tantangan analisis perangkat seluler. Dengan MobileEdit Forensic, peneliti dapat mengakses data yang sangat mendalam dari perangkat seluler. Data tersebut mencakup pesan teks, panggilan, email, kontak, foto, video, file aplikasi, catatan, kalender, dan sejumlah data lainnya. Kelebihan utama alat ini adalah kemampuan ekstraksi data yang komprehensif, yang memungkinkan peneliti untuk memeriksa dan menganalisis berbagai jenis bukti digital yang mungkin terkait dengan penyelidikan.

METODE PENELITIAN

Dalam penelitian ini, peneliti menggunakan metode *NIST Cybersecurity Framework (CSF)* adalah kerangka kerja yang dikembangkan oleh *National Institute of Standards and Technology (NIST)* untuk membantu organisasi manajemen risiko keamanan *cyber*. CSF ini terdiri dari lima fungsi utama, *yaitu Identify, Protect, Detect, Respond, dan Recover*. Lokasi penelitian Kota Pontianak, menggunakan aplikasi *Michat*. Data penelitian ini bersifat primer. Teknik pengumpulan data yang digunakan adalah studi lapangan. Analisis data yang digunakan adalah kualitatif.

HASIL DAN PEMBAHASAN

Tabel 1 merupakan informasi tentang alat yang dibutuhkan dalam penelitian ni. Proses untuk memperoleh bukti digital pada perangkat menggunakan alat Mobiledit Forensic Express

TABEL 1. ALAT PENELITIAN

No	Alat Penelitian	Deskripsi
1	Smartphone	Apple
2	Laptop	Asus TUF Gaming A15
3	Michat	Aplikasi Pesan Instan Versi 776

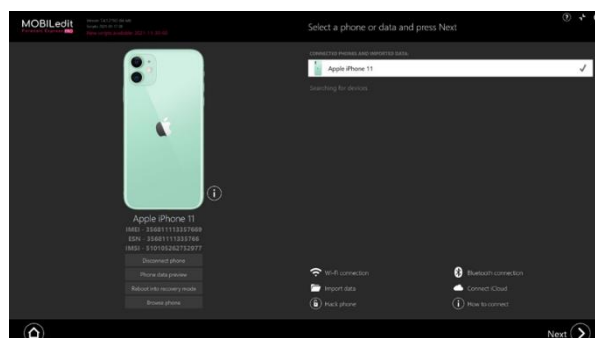
4	USB Connector	Media penghubung smartphone dengan workstation
---	---------------	--

TABEL 2. ALAT FORENSIK

No	Alat Penelitian	Deskripsi
1	Mobiledit Forensic Express	Aplikasi yang digunakan dalam menemukan barang bukti digital pada smartphone yang berbasis pada Windows

Tahap *Identify*

Dalam penelitian ini, proses identifikasi dilakukan untuk memastikan bahwa perangkat yang terhubung dan diakses oleh alat forensik adalah perangkat yang benar-benar sesuai dengan target penelitian. Dalam tool MOBILedit Forensic, proses identifikasi perangkat dilakukan secara langsung melalui aplikasi tanpa memerlukan proses rooting. Proses ini bertujuan untuk mengenali perangkat yang akan menjadi sasaran pengambilan data secara akurat. Identifikasi yang tepat memastikan bahwa data yang diambil berasal dari perangkat yang benar, sehingga mengurangi risiko kesalahan selama proses ekstraksi data. Selain itu, tahap ini juga penting sebagai dokumentasi untuk menjaga validitas dan integritas hasil penelitian, sehingga hasil yang diperoleh dapat dipertanggungjawabkan secara ilmiah

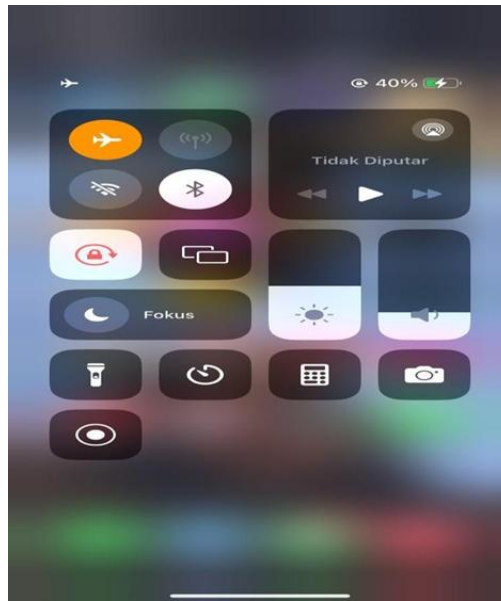


Gambar 2. Proses *Identify* Perangkat

Protect

Setelah proses identifikasi, langkah selanjutnya adalah tahap Protect atau Mengamankan Barang Bukti. Pada tahap ini, bukti-bukti yang telah diidentifikasi akan disimpan secara digital untuk memastikan keaslian dan untuk membantah klaim bahwa bukti telah dihancurkan atau dimanipulasi. Salah satu cara untuk melakukan tahap Protect adalah dengan menggunakan mode pesawat (airplane mode) pada smartphone. Tujuan dari tahap Protect ini adalah untuk memastikan bahwa bukti digital tetap aman

dan tidak dapat diakses oleh pihak yang tidak berwenang. Dengan demikian, keaslian dan keandalan bukti digital dapat dipertahankan.

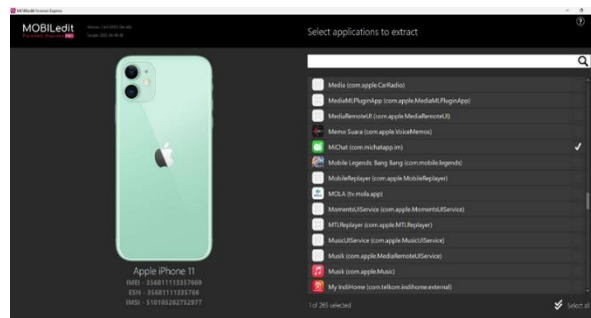


Gambar 3. Proses *Protect*

Mode pesawat dapat mencegah perubahan data pada smartphone, sehingga memastikan bahwa bukti digital tetap asli. Dengan demikian, mengaktifkan mode pesawat adalah langkah yang sangat penting dalam menjaga keaslian dan keandalan bukti digital. Mode pesawat membantu memastikan bahwa bukti digital tidak dapat diubah atau dimanipulasi. Ini sangat penting dalam menjaga integritas bukti digital. Oleh karena itu, mode pesawat harus diaktifkan sebelum melakukan analisis bukti digital.

Detect

Setelah proses identifikasi dan perlindungan selesai dilakukan, langkah selanjutnya adalah melakukan deteksi perangkat untuk mengumpulkan data lebih detail, seperti kontak dan informasi lainnya. Proses deteksi ini bertujuan untuk menggali informasi lebih mendalam mengenai perangkat yang sedang diselidiki, sehingga dapat memberikan pemahaman yang lebih baik mengenai karakteristik, penggunaan, dan konten yang terdapat dalam perangkat tersebut. Deteksi perangkat adalah langkah yang sangat penting dalam proses penyelidikan, karena memungkinkan peneliti untuk mengidentifikasi dan mengumpulkan informasi yang relevan dengan lebih efektif. Dengan demikian, proses ini akan membantu memperkuat bukti dalam penyelidikan yang sedang dilakukan.



Gambar 4. Proses *Detect*

Respond

Respond pada tool MOBILedit Forensic dilakukan dengan cara yang cukup mudah, dengan adanya fitur extract membuat analisis lebih mudah dipahami, dengan hasil akhir berupa folder laporan yang didalamnya berisi kumpulan bukti, adapun beberapa bukti yang didapatkan adalah sebagai berikut

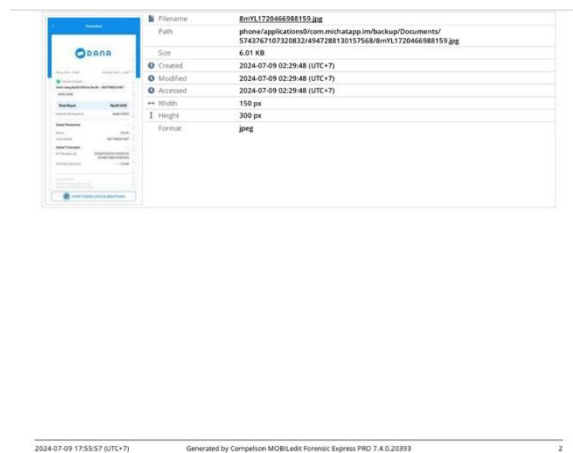
Table of Contents	
Applications	1
MiChat	1
Other Media Files	1
Images	1
Audio	5
Video	5

Gambar 5. *Table Of Contents Hasil Extract Data*

Pada tahap respond, MOBILedit Forensic berhasil mengekstrak data dari perangkat iPhone 11 yang digunakan dalam penelitian ini. Hasil ekstraksi data menunjukkan bahwa terdapat tiga jenis data yang berhasil diambil, yaitu : Gambar, Audio dan Video MOBILedit Forensic berhasil mengekstrak gambar dari perangkat iPhone 11. Gambar-gambar ini mungkin berisi bukti penting yang terkait dengan penggunaan aplikasi Michat. Dalam konteks penelitian ini, gambar gambar ini dapat digunakan sebagai bukti untuk memahami bagaimana aplikasi MiChat digunakan dalam perangkat iPhone 11.



Gambar 6. Barang Bukti Foto (1)



Gambar 7. Barang Bukti Foto (2)

Gambar ini adalah tangkapan layar dari halaman salah satu platform pembayaran atau dompet digital.

MOBILedit Forensic berhasil mengekstrak file video dari perangkat iPhone 11, Video-Video ini mungkin berisi bukti penting yang terkait dengan penggunaan aplikasi.



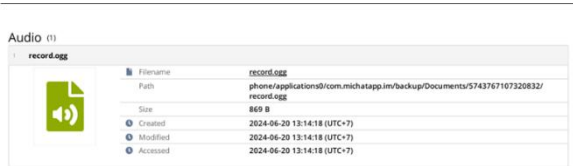
Gambar 8. Barang Bukti Video (1)



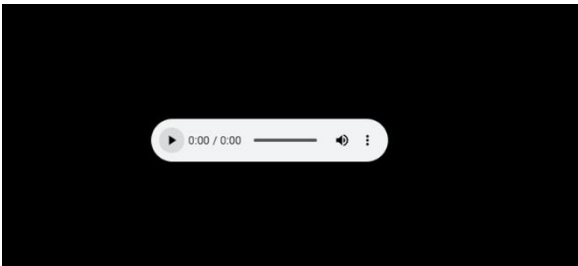
Gambar 9. Barang Bukti Video (2)

Recover

Pada tahap ini, Penulis menggunakan MOBILedit Forensic untuk mengembalikan data yang telah dihapus secara permanen dari perangkat mobile yang digunakan. Hasil dari tahap recover ini adalah didapatkan jejak bukti digital berupa audio dan video, Contoh dari jejak bukti digital yang didapatkan adalah seperti pada gambar dibawah, yang menunjukkan adanya rekaman audio dan video



Gambar 10. File Audio Yang Diperoleh



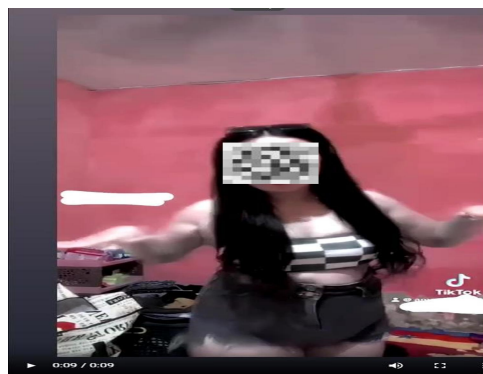
Gambar 11. Barang Bukti Audio



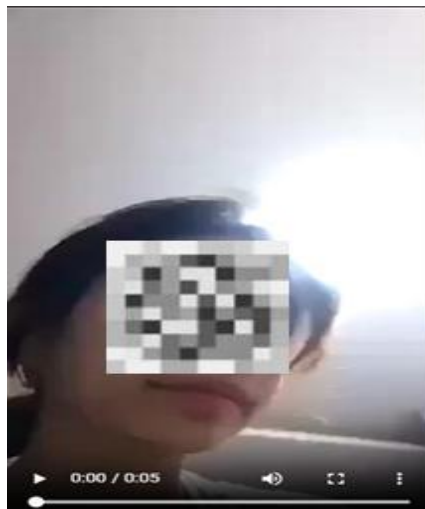
Gambar 12. Barang Bukti Video Yang Terhapus (1)



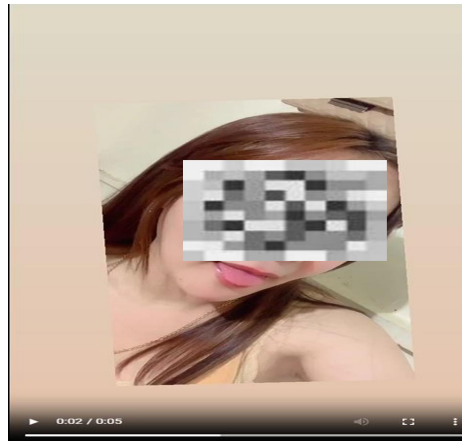
Gambar13. Barang Bukti Video Yang Terhapus (2)



Gambar 14. Barang Bukti Video Yang Terhapus (3)



Gambar 15. Barang Bukti Video Yang Terhapus (4)



Gambar 16. Barang Bukti Video Yang Terhapus (5)

KESIMPULAN

Berdasarkan hasil penelitian berhasil mengidentifikasi Barang bukti digital. Data yang diperoleh dari aplikasi menunjukkan bukti berupa gambar, audio, dan video. Penelitian ini juga menunjukkan bahwa penggunaan Kerangka Keamanan Siber NIST efektif dalam menganalisis keamanan perangkat mobile dan mengidentifikasi risiko keamanan potensial. Lima tahapan kerangka ini, yaitu Identify, Protect, Detect, Respons, dan Recover, menyajikan pendekatan komprehensif untuk mengatasi insiden keamanan dan memulihkan dari kehilangan data.

DAFTAR PUSTAKA

- APJII, "Survey Penetrasi & Perilaku Internet 2023," Tahun 2023.
- Dasmen dan F. Kurniawan, "Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial," *Techno. Com*, vol. 20, no. 4, pp. 527-539, 2021.
- Yudhana,I. Riadi, andI. Anshori, "Analisis Bukti DigitalFacebookMessengerMenggunakanMetodeNist," *It J. Res. Dev.*, vol. 3, no. 1, doi:10.25299/itjrd.2018.vol3(1).1658 pp. 13–21, 2018.
- National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*
- M. Marzuki and T. Sutabri, "ANALISIS FORENSIK MEDIA SOSIAL MICHAT METODE DIGITAL FORENSIK INTEGRATED INVESTIGATION FRAMEWORK (IDFIF)," *Blantika: Multidisciplinary Journal*, vol. 2, no. 1, pp. 56-70, 2023.
- I. Riadi, R. Umar, and M. Fauzan Gustafi, "Audio Forensics on Smartphone with Digital Forensics Research Workshop (DFRWS) Method," 2021.
- A. W. Laksana, "Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif," *Jurnal Hukum*, vol. 35, no. 1, hal. 52-76, 2019.

- M. J. C. Purba, "TINDAK PIDANA KOMPUTER DAN UPAYA PEMBUKTIAN," Lex Crimen, vol. 10, no. 4, 2021.*
- I. Riadi, Sunardi, and P. Widiandana, "Investigasi Cyberbullying pada WhatsApp Menggunakan Digital Forensics Research Workshop," *masa berlaku mulai*, vol. 1, no. 3, pp. 730–735, 2017.
- M. K. Anam, "Eksistensi Perundang-Undangan Terhadap Digital Forensik Dalam Sistem Pembuktian Pidana," 2022.
- J. J. Siregar, "Analisis Explotasi Keamanan ... (Junita Juwita Siregar) ANALISIS EXPLOTASI KEAMANAN WEB DENIAL OF SERVICE ATTACK."
- T. A. Zahra, "ASPEK HUKUM PENGGUNAAN APLIKASI MICHAT SEBAGAI SARANA TINDAK PIDANA PROSTITUSI ONLINE Studi Putusan Pengadilan Nomor 393/Pid. Sus/2021/PN. Bjm," Bachelor's thesis, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah Jakarta.*
- G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *J. Media Informatika Budidarma*, vol. 6, no. 2, pp. 1263-1271, 2022.