JURNAL FASILKOM
Volume 15 No. 3 | Desember 2025: 533-541

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Analisis Perbandingan *Tools Forensic* Pada Aplikasi Facebook Messenger Menggunakan Metode *National Institute of Standards Technology* (NIST)

Desti Mualfah[1], Febri Israndi[2], Rizdqi Akbar Ramadhan[3]
[1,2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau
[3]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Riau

[1]destimualfah@umri.ac.id, [2]200401013@student.umri.ac.id, [3]rizdqiramadhan@eng.uir.ac.id

Abstract

The rapid development of digital technology has driven a significant increase in internet and social media use across all levels of society. This situation not only facilitates communication and information exchange but also opens up opportunities for various forms of cybercrime. One social media platform frequently exploited in cybercrime activities is Facebook, particularly through its instant messaging feature. Therefore, a systematic and standardized digital forensic investigation process is needed to accurately obtain and analyze digital evidence. This study aims to analyze the application of digital forensic stages using the National Institute of Standards and Technology (NIST) method on the Facebook social media platform. The research method used is a case study with a digital forensic approach based on the NIST framework, which includes the stages of collection, examination, analysis, and reporting. The process of acquiring and analyzing digital evidence was carried out on an Android-based smartphone device using two forensic tools, namely Magnet AXIOM and MOBILedit Forensic. The results of the study indicate that MOBILedit Forensic has better data acquisition capabilities, especially in extracting application artifacts and image data relevant to the case. Meanwhile, Magnet AXIOM demonstrates superiority in aspects of data analysis, result visualization, and integration with other forensic platforms. Based on the results of the comparison, MOBILedit Forensic is recommended as a more effective digital forensic tool for the investigation process on Android devices, especially in handling cybercrime cases involving social media applications.

Keywords: Digital Forensics, Cybercrime, Forensic Tool Comparison, Facebook Messenger, NIST

Abstrak

Perkembangan teknologi digital yang semakin pesat mendorong peningkatan signifikan dalam penggunaan internet dan media sosial di berbagai lapisan masyarakat. Kondisi tersebut tidak hanya memberikan kemudahan dalam komunikasi dan pertukaran informasi, tetapi juga membuka peluang terjadinya berbagai bentuk kejahatan siber. Salah satu platform media sosial yang sering dimanfaatkan dalam aktivitas kejahatan siber adalah Facebook, khususnya melalui fitur pesan instan. Oleh karena itu, diperlukan proses investigasi forensik digital yang sistematis dan terstandar untuk memperoleh dan menganalisis bukti digital secara akurat. Penelitian ini bertujuan untuk menganalisis penerapan tahapan forensik digital menggunakan metode National Institute of Standards and Technology (NIST) pada platform media sosial Facebook. Metode penelitian yang digunakan adalah studi kasus dengan pendekatan forensik digital berdasarkan kerangka kerja NIST yang meliputi tahapan *collection*, *examination*, *analysis*, dan *reporting*. Proses akuisisi dan analisis barang bukti digital dilakukan pada perangkat smartphone berbasis Android dengan memanfaatkan dua tools forensik, yaitu Magnet AXIOM dan MOBILedit Forensic. Hasil penelitian menunjukkan bahwa MOBILedit Forensic memiliki kemampuan akuisisi data yang lebih baik, terutama dalam mengekstraksi artefak aplikasi dan data gambar yang relevan dengan kasus. Sementara itu, Magnet AXIOM menunjukkan keunggulan pada aspek analisis data, visualisasi hasil, serta integrasi dengan platform forensik lainnya. Berdasarkan hasil perbandingan tersebut, MOBILedit Forensic direkomendasikan sebagai tools forensik digital yang lebih efektif untuk proses investigasi pada perangkat Android, khususnya dalam penanganan kasus kejahatan siber yang melibatkan aplikasi media sosial.

Kata kunci: Digital Forensik, *Cybercreime*, *Forensic Tool Comparison*, Facebook Messenger, NIST

1. Pendahuluan

Pesatnya perkembangan era digital, internet dan media sosial kini menjadi elemen yang tidak terpisahkan dari aktivitas masyarakat sehari-hari. Kemajuan teknologi, khususnya dalam beberapa tahun terakhir, menunjukkan peningkatan yang signifikan, baik dari aspek fitur, sistem operasi, maupun ragam aplikasi yang dioperasikan pada perangkat smartphone [1]. Penggunaan internet di Indonesia memperlihatkan tren pertumbuhan yang konsisten dari tahun ke tahun. Berdasarkan laporan Hootsuite dan We Are Social, jumlah pengguna internet meningkat dari 201,6 juta pada 2021 menjadi 204,7 juta pada 2022, dan kembali bertambah hingga 215,6 juta pada 2023.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Peningkatan penggunaan internet ini membuka peluang bagi berbagai bentuk kejahatan siber, termasuk penipuan dan pemerasan di platform media sosial [2]. Salah satu media sosial dengan tingkat penggunaan yang tinggi serta memiliki potensi kerawanan terhadap kejahatan siber adalah Facebook. Menurut data dari [3] Facebook merupakan salah satu platform media sosial terbesar di dunia dengan jumlah pengguna aktif bulanan yang melampaui 2,9 miliar. Di Indonesia, tingginya tingkat penggunaan Facebook menyebabkan platform ini memiliki basis pengguna yang sangat luas, sehingga berpotensi menjadi sasaran utama berbagai bentuk kejahatan siber. Berdasarkan laporan dari [4]. Facebook mencatat jumlah insiden phishing tertinggi di antara platform media sosial lainnya pada tahun 2021, menunjukkan tingginya risiko kejahatan siber pada platform ini. Pemilihan Facebook sebagai objek penelitian dalam studi ini didasarkan pada fakta bahwa Facebook adalah platform media sosial dengan jumlah pengguna terbesar dan memiliki tingkat kejahatan siber yang signifikan dibandingkan dengan platform lain seperti Instagram, WhatsApp, atau Twitter[5]. Data dari berbagai sumber menunjukkan bahwa kasus-kasus penipuan di Facebook mencakup berbagai modus, termasuk penipuan finansial, pencurian identitas, dan penyebaran informasi palsu [6]. Penipuan di Facebook sering kali dilakukan melalui pesan pribadi, postingan di grup, atau bahkan melalui iklan yang tampak sah.

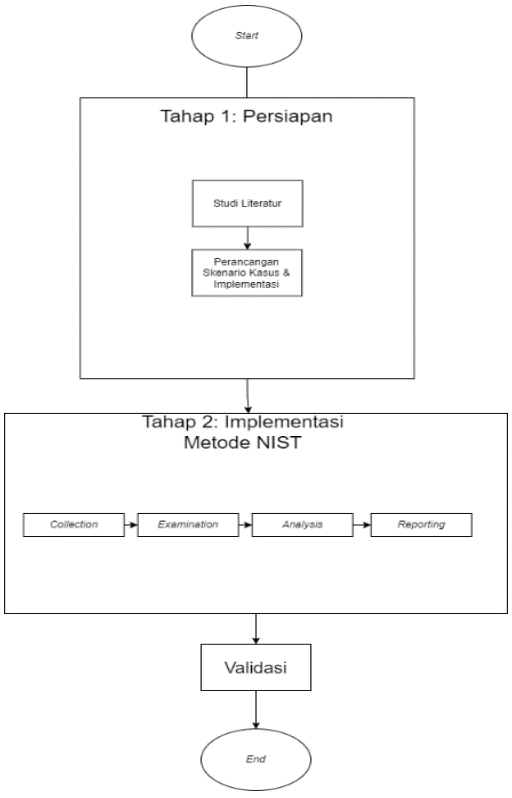
Penggunaan aplikasi mobile untuk mengakses Facebook juga menjadi faktor penting dalam penelitian ini. Berdasarkan data dari[7], [8], [9], lebih dari 98% pengguna Facebook mengakses platform ini melalui perangkat mobile. Hal ini menunjukkan bahwa potensi kejahatan siber tidak hanya terjadi pada aplikasi web tetapi juga pada aplikasi mobile [10]. Oleh karena itu, fokus penelitian ini adalah pada analisis data forensik dari perangkat mobile yang digunakan untuk mengakses Facebook, mengingat tingginya penggunaan perangkat mobile di Indonesia. Dalam konteks forensik digital, analisis dan pengungkapan bukti-bukti digital dari platform Facebook sangat penting untuk mengungkap kasus-kasus kejahatan siber [11], [12], [13] Alat-alat forensik seperti Magnet Axiom dan MOBILedit banyak digunakan dalam proses investigasi digital untuk mengumpulkan dan menganalisis data dari berbagai sumber, termasuk perangkat mobile dan media sosial. Magnet Axiom, misalnya, dapat melakukan analisis mendalam terhadap data dari Facebook, sementara MOBILedit sangat efektif dalam mengekstraksi data dari perangkat mobile [14], [15].

Metode National Institute of Standards and Technology (NIST) [16]digunakan dalam penelitian ini untuk memberikan panduan yang terstruktur dan sistematis dalam melakukan forensik digital. Metode ini terdiri dari empat tahap utama: collection, examination, analysis, dan reporting [17], [18]. Setiap tahap memiliki peran penting dalam memastikan bahwa bukti-bukti digital yang dikumpulkan dapat digunakan secara efektif dalam proses hukum[19][20][21].

Penelitian ini bertujuan untuk mensimulasikan proses forensik digital pada platform Facebook dengan menggunakan metode NIST, serta membandingkan efektivitas dua alat forensik, yaitu Magnet Axiom dan MOBILedit, dalam mengungkap dan menangani kasus-kasus kejahatan siber di Facebook. Diharapkan penelitian ini dapat memberikan kontribusi yang signifikan dalam bidang forensik digital dan membantu penegak hukum dalam mengatasi kejahatan siber di media sosial [22]. Selain itu, penelitian ini juga bertujuan untuk memberikan rekomendasi mengenai alat forensik yang paling efektif dalam mengatasi kejahatan siber [23], [24] pada platform Facebook.

2. Metode Penelitian

Untuk mendukung proses Guna mendukung pelaksanaan analisis dan investigasi forensik pada perangkat smartphone, diperlukan penerapan metode khusus agar proses investigasi dapat berlangsung secara sistematis dan terstruktur. Oleh karena itu, penelitian ini menggunakan metode *National Institute of Standards and Technology* (NIST).



Gambar 1 Metodologi Penelitian

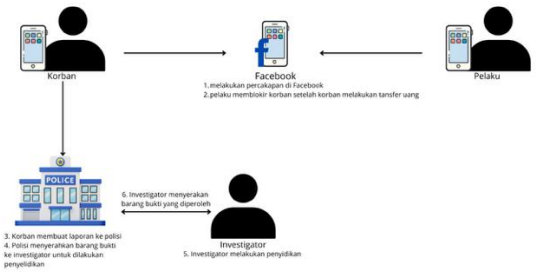
P-ISSN : 2089-3353
E-ISSN : 2808-9162

a. Tahapan Persiapan
Sebelum memulai penelitian, penulis akan melakukan studi literatur untuk memahami penelitian-penelitian sebelumnya yang dapat membantu menyelesaikan penelitian ini, serta menyusun, merancang, dan melakukan simulasi kasus.

b. Studi Literatur
Proses ini mencakup kegiatan penelusuran dan pengkajian terhadap berbagai sumber pustaka yang relevan dengan topik penelitian. Literatur yang digunakan dapat berasal dari jurnal ilmiah, buku, artikel daring, prosiding, dan sumber lainnya. Melalui studi literatur ini, diharapkan peneliti memperoleh pemahaman mengenai metode penelitian pada perangkat smartphone, penggunaan tools forensik mobile, serta tahapan analisis dan investigasi dalam memperoleh bukti digital.

c. Perancangan Skenario
Dalam penyusunan skenario yang dilakukan, kemungkinan terjadinya tindak kejahatan terhadap pengguna smartphone diantisipasi. Skenario ini dirancang untuk mengumpulkan barang bukti sebagai langkah awal menuju proses analisis. Penelitian ini mengacu pada situasi yang sering terjadi dalam kehidupan sehari-hari, di mana kejahatan dilakukan dengan menggunakan aplikasi Facebook Messenger. Proses ini memerlukan investigasi dan penyelidikan untuk mendapatkan barang bukti digital dari aplikasi tersebut.

d. Skenario Kasus
langkah pertama adalah membuat 2 buah akun facebook yang satu nya berperan sebagai akun korban penipuan lalu satu nya lagi berperan sebagai akun pelaku, Kemudian keduanya melakukan percakapan di facebook yang mana sipelaku berpura pura sebagai seorang teman lama si korban lalu menawarkan barang untuk dijual, setelah korban setuju dan melakukan pembayaran melalui transfer ke rekening pelaku, selanjutnya pelaku memblokir korban.
Setelah merasa tertipu dan mengalami kerugian materil, korban membuat laporan ke polisi mengenai musibah yang menimpa dirinya, setelah mengumpulkan barang bukti yang ada, lalu pihak kepolisian menemui investigator dan menyerahakn barang bukti yang telah dikumpulkan sebelumnya agar dapat menemukan barang bukti yang valid dari smartphone korban.
Pihak investigator kemudian melakukan invesitagasi nya dan menemukan bukti digital tersebut, kemudian membuat form hasil investigasi, dan setelah itu investigator melaporkan hasil pemeriksaan nya dan menyerahkan form investigasi dan bukti – bukti digital yang didapat dari hasil pemeriksaan smartphone pelaku ke pihak kepolisian. Skenario ini di gambarkan pada scenario berikut:



Gambar 2 Skenario Kasus

e. Pengujian Skenario Kasus
Pada tahap ini, akan dilakukan eksperimen untuk memperoleh bukti digital. Pengujian ini melibatkan contoh-contoh kejahatan yang umum terjadi di media sosial dalam kehidupan sehari-hari, seperti kejahatan atau aktivitas prostitusi online yang dilakukan melalui aplikasi pesan instan. Metode yang digunakan dalam pengujian eksperimen ini melibatkan penggunaan smartphone Android beserta tools Mobiledit, dan Magnet Axiom yang telah diinstal pada laptop.

f. Metode NIST (*National Institute of Standards Technology*)
Sebelum proses akuisisi barang bukti dilakukan, perangkat smartphone terlebih dahulu diisolasi dari seluruh bentuk komunikasi. Tahapan isolasi ini bertujuan untuk mencegah terjadinya perubahan data yang dapat merusak bukti digital atau memengaruhi integritas informasi yang tersimpan di dalam perangkat. Langkah awal dilakukan dengan mengubah status perangkat ke *mode airplane*, kemudian mengaktifkan *developer* options sebagai bagian dari persiapan proses forensik. Dalam penelitian ini, *tools* forensik yang digunakan meliputi MOBILedit Forensic dan Magnet AXIOM. Proses investigasi forensik mengacu pada metode NIST yang terdiri atas empat tahapan, yaitu *collection, examination, analysis, dan reporting.*

3. Hasil dan Pembahasan

Hasil yang diharapkan adalah keberhasilan dalam mengidentifikasi dan mengumpulkan bukti digital yang dapat digunakan untuk mengungkap aktivitas yang terkait dengan kasus yang sedang diselidiki, dengan memastikan bahwa semua langkah investigasi dilakukan secara menyeluruh dan sesuai dengan standar forensik yang berlaku.

Pembahasan merupakan bagian yang menyajikan penjelasan mendasar, keterkaitan, serta generalisasi yang diperoleh dari hasil penelitian. Uraian pada bagian ini bertujuan untuk menjawab rumusan pertanyaan penelitian.

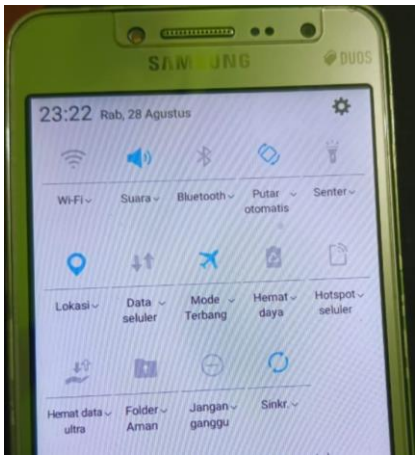
3.1 Tahapan Metode National institute Og Standards Technology (NIST)

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Bagian ini menjelaskan tahapan-tahapan yang digunakan dalam metode National Institute of Standards and Technology (NIST) untuk investigasi forensik digital. Metode NIST terdiri dari empat tahapan utama: *collection* (pengumpulan), *examination* (pemeriksaan), *analysis* (analisis), dan *reporting* (pelaporan).

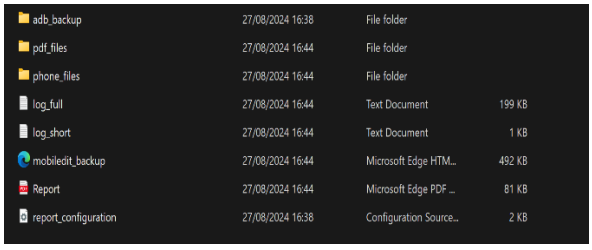
3.2 *Collection*

Pada tahap ini, proses pengumpulan barang bukti dan pencadangan (backup) seluruh data pada perangkat smartphone dilakukan dengan menggunakan alat forensik khusus. Sebelum proses pencadangan dimulai, perangkat smartphone harus di-root terlebih dahulu untuk memastikan bahwa data yang telah dihapus dapat diakses dan dipulihkan. Proses Pencadangan dengan Mode pesawat atau *airplane mode* adalah fitur pada perangkat seluler yang secara otomatis menonaktifkan semua fungsi transmisi nirkabel, termasuk jaringan seluler, Wi-Fi, Bluetooth, dan GPS.

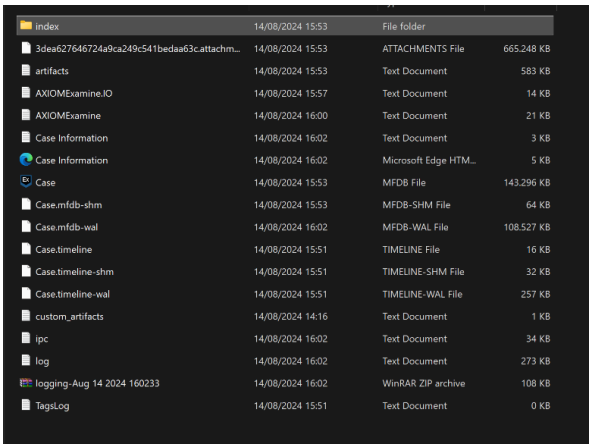


Gambar 3 Konfigurasi Mode Pesawat

Setelah jaringan smartphone dikonfigurasi ke dalam mode pesawat, langkah berikutnya adalah melakukan *backup* data perangkat. Backup ini penting untuk memastikan seluruh data yang ada di dalam perangkat tersalin secara menyeluruh dan tanpa perubahan selama proses berlangsung. Metode yang digunakan dalam backup data adalah dengan menciptakan *physical image*, yaitu salinan lengkap dari memori perangkat, termasuk sistem operasi, file sistem, dan data pengguna.



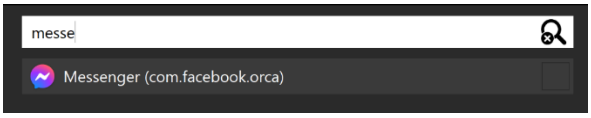
Gambar 4 *Collection* Mobiledit



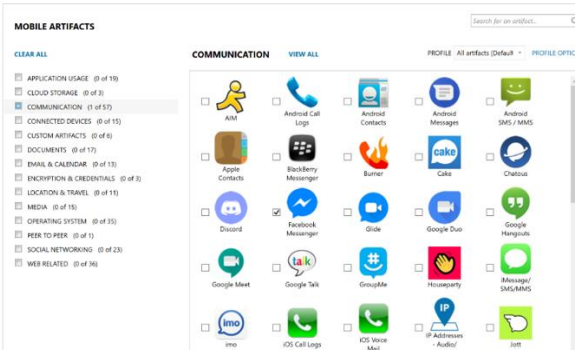
Gambar 5 *Collection* Magnet Axiom

3.2 *Examination*

Pada tahap ini, dilakukan proses investigasi khusus pada aplikasi Messenger di Facebook. Proses investigasi ini bertujuan untuk mengidentifikasi dan mengumpulkan barang bukti digital yang terdapat pada aplikasi Messenger tersebut. Langkah ini merepresentasikan tahap krusial dalam investigasi forensik digital, di mana investigator harus melakukan seleksi strategis terhadap aplikasi-aplikasi yang akan diakuisisi datanya untuk analisis lebih lanjut.



Gambar 6 *Import* data Mobiledit



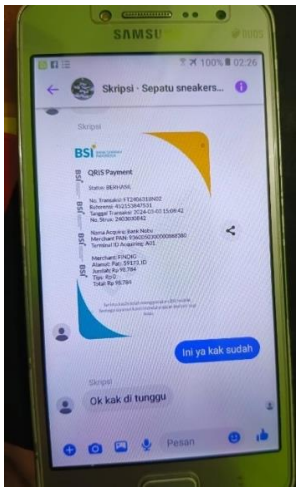
Gambar 7 *Import* Data Magnet Axiom

3.4 Analisis

Pada tahapan ini dilakukan analisis terhadap temuan yang ditemukan pada bukti digital tersebut.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Gambar 8 Bukti Chat Sebelum di Hapus



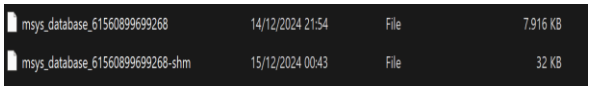
Gambar 9 Bukti Chat Setelah i Hapus

2.4.1 Analisis Hasil dengan Mobiledit Forensic

Setelah dilakukan proses akuisisi data dari perangkat Samsung SM-G532G menggunakan perangkat lunak *Mobiledit Forensic*, struktur folder dan file yang diperoleh menyimpan berbagai informasi penting terkait dengan aplikasi Facebook Messenger. Selain itu, dalam subfolder live_data, terdapat file database bernama inbox_units_db dan inbox_units_db-journal. File ini berisi log percakapan dan informasi lain yang terekam oleh aplikasi Messenger.

Gambar 10 Struktur data Mobiledit

File database ini menyimpan struktur data yang bisa dianalisis lebih lanjut untuk menemukan bukti percakapan yang telah dihapus atau informasi penting lainnya.



Gambar 11 *Database* Hasil Akuisisi Mobiledit

1. Barang Bukti yang ditemukan
   a. Analisis File Database

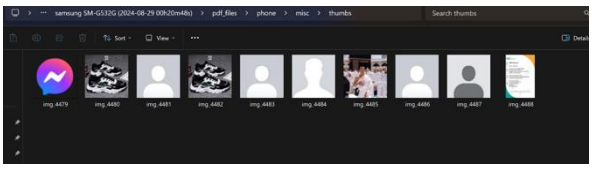
Melalui file inbox_units_db dan inbox_units_db-journal, dilakukan analisis lebih lanjut untuk mengekstrak data yang ada di dalamnya. Dengan bantuan alat seperti Mobiledit, file ini bisa dibuka untuk mengekstrak informasi mengenai percakapan yang mungkin sudah dihapus. Data dalam file database ini disimpan dalam bentuk tabel yang menghubungkan ID pengguna, timestamp percakapan, dan konten pesan. Berikut Verifikasi Data yang telah diakuisis pada menggunkan tools Systool SQLite Viewer:

Tabel 1 Tabel Bukti Chat pada Mobiledit

Isi Bukti Digital	
00736B30 08 08 08 00 00 00 00 5B 87 A8 10 32 18 F1 01 90 .....[.¨.2.ñ.. 00736B40 05 12 E9 9A 6D 69 64 2E 24 67 41 46 75 48 71 42 ..é.mid.$gAFuHqB 00736B50 41 79 47 50 47 57 4E 6C 67 78 6D 6D 51 42 52 4C AyGPGWNlgxmmQBRL 00736B60 68 6D 6F 67 73 43 37 32 30 36 31 31 36 34 33 37 hmogsC7206116437 00736B70 35 35 36 30 37 31 31 37 30 4F 6B 20 6B 6B 20 62 556071170Ok kk b 00736B80 69 73 61 20 6B 69 72 69 6D 20 6E 6F 20 52 65 78 isa kirim no Rex 00736B90 20 6E 79 61 3F 37 FD 47 07 7D F3 50 02 02 03 01 nya?7ýG.}óP.... 00736BA0 90 05 12 E9 9A 02 81 50 3C 52 06 05 51 33 63 05 ...é...P<R..Q3c.	
Keterangan	Korban : Kk bisa kirim no Rex nya?
00736C00 32 18 F1 01 90 05 14 67 57 6D 69 64 2E 24 67 41 2.ñ....gWmid.$gA 00736C10 46 75 48 71 42 41 79 47 50 47 57 4E 6C 6D 76 56 FuHqBAyGPGWNlmvV 00736C20 32 51 42 52 52 6C 44 62 77 6E 2D 37 32 30 36 31 2QBRRlDbwn-72061 00736C30 31 36 38 35 33 35 37 37 33 35 33 37 32 36 31 33 1685357735372613 00736C40 37 38 39 30 30 30 39 0A 49 6E 69 20 79 61 20 6B 7890009.Ini ya k 00736C50 61 6B 0A 41 2E 6E 2E 20 3A 20 72 61 64 69 74 79 ak.A.n. : radity 00736C60 61 20 70 72 61 74 61 6D 61 37 FD 43 8F 02 44 50 a prataMa7ýC..DP 00736C70 02 02 01 90 05 14 67 57 02 81 2B 3B 52 06 05 51 ......gW..+;R..Q 00736C80 33 17 05 00 08 01 01 01 08 00 00 00 00 00 00 00 3.....	
Keterangan	Pelaku : 137890009 Ini ya kak A.n : raditya pratama
00736CD0 87 A8 10 32 18 F1 01 90 05 15 0C 14 6D 69 64 2E .¨.2.ñ.....mid 00736CE0 24 67 41 46 75 48 71 42 41 79 47 50 47 57 4E 6C $gAFuHqBAyGPGWN 00736CF0 70 55 46 47 51 42 52 55 4C 4E 69 50 39 38 37 32 pUFGQBRULNiP987 00736D00 30 36 31 31 37 30 33 31 39 38 37 39 36 39 39 31 0611703198796991 00736D10 36 4F 6B 20 6B 6B 37 FD 47 07 7D F3 50 02 02 03 6Ok kk7ýG.}óP.. 00736D20 01 90 05 15 0C 14 02 81 26 3A 52 06 05 51 33 0D ....&:R..Q3	
Keterangan	Korban : Ok kk
00736D80 10 32 18 F1 01 90 05 17 75 CF 6D 69 64 2E 24 67 .2.ñ....uÏmid.$g 00736D90 41 46 75 48 71 42 41 79 47 50 47 57 4E 6C 79 39 AFuHqBAyGPGWNly9 00736DA0 7A 32 51 42 52 64 72 7A 45 47 4B 58 37 32 30 36 z2QBRdrzEGKX7206 00736DB0 31 31 37 36 38 35 34 35 32 36 32 38 36 33 31 37 1176854526286317 00736DC0 FD 47 07 7D F3 50 02 02 03 01 90 05 17 75 CF 02 ýG.}óP.....uÏ. 00736DD0 81 35 39 52 06 05 51 33 2D 05 00 08 01 01 01 08 .59R..Q3-.....	
Keterangan	Korban mengirimkan bukti transfer
00736E20 08 08 00 00 00 00 5B 87 A8 10 32 18 F1 01 90 05 ......[.¨.2.ñ... 00736E30 18 29 8C 6D 69 64 2E 24 67 41 46 75 48 71 42 41 .).mid.$gAFuHqBA 00736E40 79 47 50 47 57 4E 6C 31 78 6A 47 51 42 52 67 6E yGPGWNl1xjGQBRgn 00736E50 53 53 73 33 59 37 32 30 36 31 31 37 38 38 36 37 SSs3Y72061178867 00736E60 36 36 32 37 31 39 36 30 49 6E 69 20 79 61 20 6B 66271960Ini ya k 00736E70 61 6B 20 73 75 64 61 68 37 FD 43 8F 02 44 50 02 ak sudah7ýC..DP. 00736E80 02 01 90 05 18 29 8C 02 81 3C 38 52 06 05 51 33 .....)...<8R..Q3 00736E90 3B 05 00 08 01 01 01 08 00 00 00 00 00 00 00 00 ;.....	
Keterangan	Korban : Ini ya kak sudah
00736ED0 00 00 08 08 00 00 08 08 08 08 00 00 00 00 5B 87 ....[. 00736EE0 A8 10 32 18 F1 01 90 05 18 3D 9A 6D 69 64 2E 24 ¨.2.ñ....=.mid.$ 00736EF0 67 41 46 75 48 71 42 41 79 47 50 47 57 4E 6C 32 gAFuHqBAyGPGWN12 00736F00 46 6D 6D 51 42 52 67 37 59 5F 4C 77 47 37 32 30 FmmQBRg7Y_LwG720 00736F10 36 31 31 37 39 30 38 33 35 33 34 33 32 35 38 32 6117908353432582 00736F20 53 65 67 65 72 61 20 64 69 20 70 72 6F 73 65 73 Segera di proses 00736F30 20 79 61 20 6B 61 6B 37 FD 43 8F 02 44 50 02 02 ya kak7ýC..DP.. 00736F40 01 90 05 18 3D 9A 02 81 36 37 52 06 05 51 33 2D ....=...67R..Q3-	
eterangan	Korban : Segera di proses ya kak
00736FA0 10 32 18 F1 01 90 05 18 72 D5 6D 69 64 2E 24 67 .2.ñ....rÕmid 00736FB0 41 46 75 48 71 42 41 79 47 50 47 57 4E 6C 32 36 AFuHqBAyGPGWN 00736FC0 31 57 51 42 52 68 78 37 77 4D 51 68 37 32 30 36 1WQBRhx7wMQh7 00736FD0 31 31 37 39 36 36 39 31 38 37 36 33 35 35 33 4F 1179669187635 00736FE0 6B 20 6B 61 6B 20 64 69 20 74 75 6E 67 67 75 37 k kak di tung 00736FF0 FD 47 07 7D F3 50 02 02 03 01 90 05 18 72 D5 02 ýG.}óP.....rÕ.	
Keterangan	Korban : Ok kak ditunggu

b. Analisis file Datbase

Dalam proses analisis forensik digital terhadap perangkat Samsung SM-G532G, dalam folder pdf_files dapat ditemukan kumpulan gambar yang dapat diexsekusi dalam path: D:\Skripsi Febri\Percobaan Mobileedit Samsung\samsung SM-G532G (2024-08-29 00h20m48s)\pdf_files\phone\misc\thumbs.

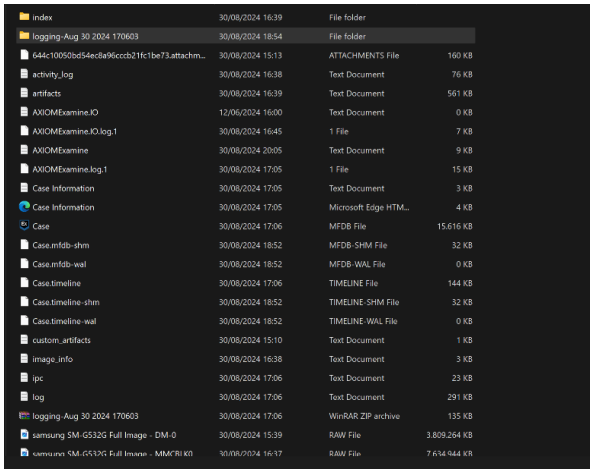


Gambar 12 Bukti Gambar Yang Ditemykan Pada Mobiledit

P-ISSN : 2089-3353
E-ISSN : 2808-9162

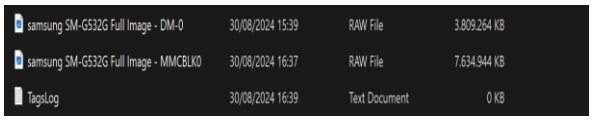
2.4.2 Analisis Hasil Akuisis dengan Mobileedit Forensic

Setelah dilakukan proses akuisisi data dari perangkat Samsung SM-G532G menggunakan perangkat lunak *Magnet Axiom*, struktur folder dan file yang diperoleh menyimpan berbagai informasi penting terkait dengan aplikasi Facebook Messenger.



Gambar 13 Struktur Data Pada Magnet Axiom

Selain itu, terdapat file database bernama samsung SM-G532G Full Image - DM-0. File ini berisi log percakapan dan informasi lain yang terekam oleh perangkat. File database ini menyimpan struktur data yang bisa dianalisis lebih lanjut untuk menemukan bukti percakapan yang telah dihapus atau informasi penting lainnya dalam aplikasi messenger.

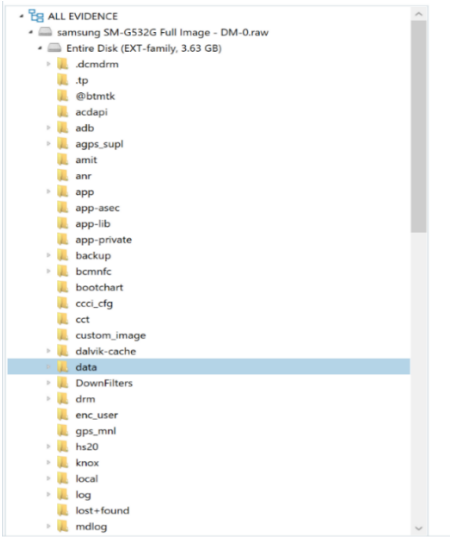


Gambae 14 Bukti Database Magnet Axiom

a. Barang Bukti yang ditemukan

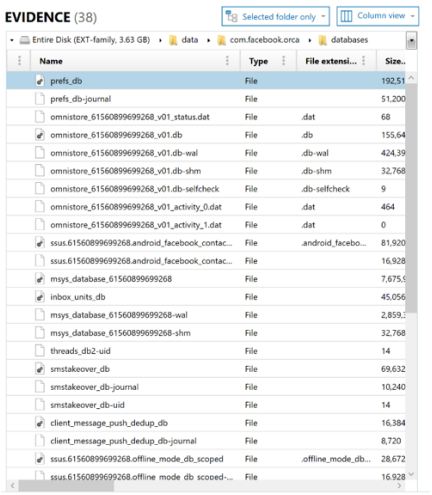
1. Analisis *file Datbase*

Dalam file samsung SM-G532G Full Image - DM-0 dilakukan analisis menggunakan magnet axiom examination ditemukan beberapa folder dan sub-folder bukti bukti yang ditemukan.



Gambar 15 Struktur Folder Bukti Database Magnet Axiom

Dalam Folder data erdapat folder Bernama com.facebook.orca dalam folder tersebut terdapat beberapa folder, dalam folder tersebut ditemukan dalam folder Database ditemukan banyaka file data base.

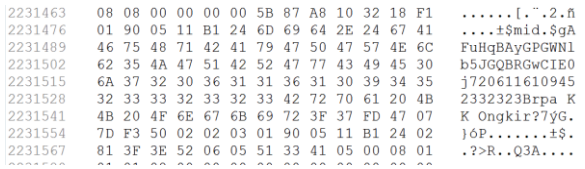


Gambar 16 Bukti Database Magnet Axiom

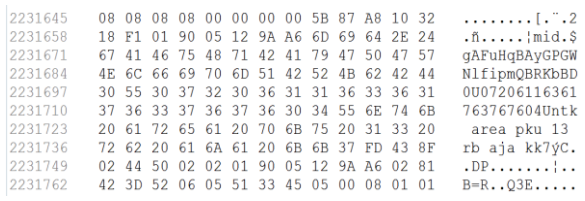
Tabel 2 Bukti Chat pada Magnet Axiom

Isi Bukti Digital
2231268 00 5B 87 A8 10 32 18 F1 01 90 05 10 EF .[.¨.2.ñ....ï
2231281 4D 6D 69 64 2E 24 67 41 46 75 48 71 42 Mmid.$gAFuHqB
2231294 41 79 47 50 47 57 4E 6C 59 33 54 57 51 AyGPGWNlY3TWQ
2231307 42 52 44 76 78 5F 41 48 58 37 32 30 36 BRDvx_AHX7206
2231320 31 31 35 39 30 33 30 32 33 30 38 38 30 1159030230880
2231333 38 37 48 71 72 67 61 20 62 65 6C 75 6D 87Hqrga belum
2231346 20 74 72 6D 61 73 75 6B 20 6F 6E 67 6B trmasuk ongk
2231359 69 72 20 79 61 20 6B 6B 37 FD 43 8F 02 ir ya kk7ýC..
2231372 44 50 02 02 01 90 05 10 EF 4D 02 81 35 DP......ïM..5
2231385 3F 52 06 05 51 33 2B 05 00 08 01 01 01 ?R..Q3+.....
Keterangan Pelaku : Hqrga belum trmasuk ongkir ya kk?	

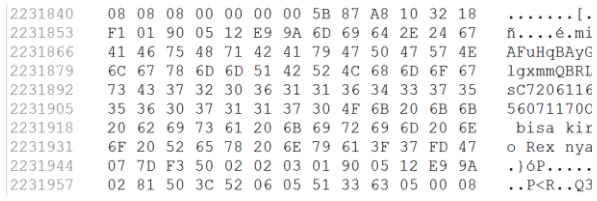
P-ISSN : 2089-3353
E-ISSN : 2808-9162



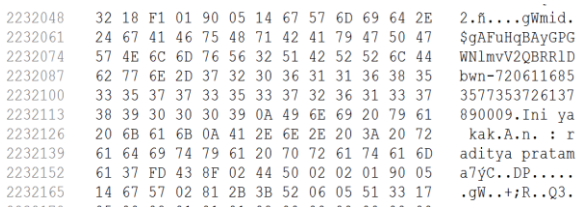
Keterangan	Korban: Brapa kk Ongkirnya?



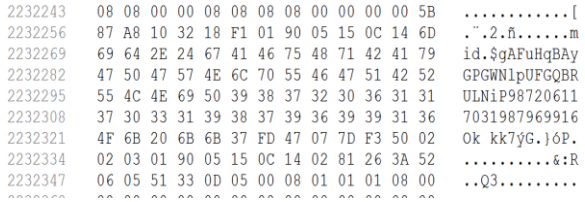
Keterangan	Pelaku: Untk area pku 13 rb aja kk



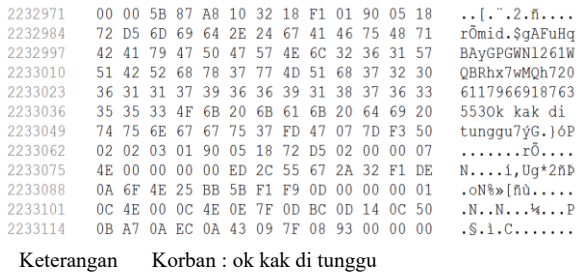
Keterangan	Korban: kk bisa kirim no Rex nya?



Keterangan	pelaku: Ini ya kak a.n. : raditya pratama



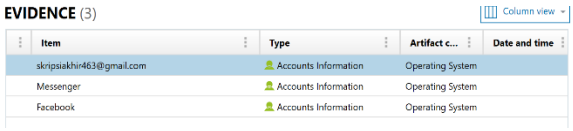
Keterangan	Korban: Ok kk



Keterangan	Korban : ok kak di tunggu

2. Bukti Informasi akun

Selain bukti-bukti percakapan dalam Messenger, Magnet Axiom juga berhasil melakukan akuisisi informasi akun beserta database yang terhubung dengan akun tersebut. Proses akuisisi ini mencakup pengambilan data yang terkait dengan informasi identitas pengguna, aktivitas akun, serta metadata yang penting untuk analisis forensik. Informasi akun meliputi data login, alamat email, riwayat aktivitas, dan interaksi pengguna dengan layanan atau aplikasi tertentu. Di samping itu, database yang terakuisisi memberikan gambaran tentang struktur data yang digunakan oleh sistem, termasuk tabel-tabel yang berisi data pengguna.



Gambae 17 Bukti Informasi Akun Pada Magnet Axiom

3.5 Evaluasi

Proses validasi memiliki peran krusial dalam memastikan bahwa hasil investigasi forensik pada aplikasi Facebook Messenger bersifat benar, akurat, dan kredibel, serta tetap menjaga integritas data sehingga dapat diterima sebagai alat bukti yang sah secara hukum. Hasil pemeriksaan forensik harus memenuhi prinsip *repeatable* dan *reproducible* agar tingkat validitasnya dapat dipertanggungjawabkan dan digunakan sebagai bukti yang kuat. Oleh karena itu, tahapan validasi dalam penelitian ini dibagi menjadi dua, yaitu validasi *repeatability* dan validasi *reproducibility*.

Validasi *repeatability* dilakukan dengan menggunakan beberapa alat forensik seperti MOBILedit Forensic Express, dan Magnet Axiom pada satu perangkat smartphone yang memiliki dua akun Messenger (sebagai korban dan pelaku). Hasil ekstraksi data dengan menggunakan tool Autopsy dilakukan dua kali, namun tidak ditemukan bukti digital yang signifikan. Proses ini memastikan bahwa hasil yang diperoleh konsisten dan dapat diulang dengan menggunakan perangkat yang sama, sehingga kredibilitas hasil dapat dipertahankan dalam konteks investigasi forensik Messenger Facebook.

Tabel 4 Hasil Validasi Repeatibility Mobiledit

Bukti Digital	Mobiledit	
	Ekstraksi 1	Ekstraksi 2
Akun	100%	100%
Kontak	100%	100%
Chatt	100%	100%
Gambar	100%	100%

Tabel 5 Hasil Validasi Repeatibility Magnet Axiom

Bukti Digital	Magnet Axiom	
	Ekstraksi 1	Ekstraksi 2
Akun	100%	100%
Kontak	100%	100%
Chatt	100%	100%
Gambar	0%	0%

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Validasi *reproducibility* dilakukan dengan menguji objek yang sama yaitu satu smartphone dengan dua akun *Messenger Facebook* menggunakan tiga alat forensik berbeda dalam periode waktu yang cukup lama. Proses ini bertujuan untuk memastikan bahwa hasil yang diperoleh dari setiap alat forensik konsisten dan tidak mengalami perubahan, menunjukkan bahwa alat-alat tersebut dapat memproduksi hasil yang sama secara berulang. Dalam validasi reproducibility ini, forensik dilakukan berulang kali dengan menggunakan metode yang sama pada objek penelitian yang identik, namun dengan alat yang berbeda. Proses ini melibatkan penggunaan alat-alat forensik seperti *MOBILedit Forensic Express*, dan *Magnet Axiom* pada smartphone yang sama untuk mengonfirmasi apakah hasil ekstraksi data dari dua akun *Messenger* di perangkat tersebut konsisten di seluruh alat yang digunakan.

Tabel 6. Hasil Validasi *Reproducibility* Mobiledit

Bukti Digital	Mobiledit	
	Ekstraksi 1	Ekstraksi 2
Akun	100%	100%
Kontak	100%	100%
Chat	100%	100%
Gambar	100%	100%

Tabel 7 Hasil Validasi Reproducibility Magnet Axiom

Bukti Digital	Magnet Axiom	
	Ekstraksi 1	Ekstraksi 2
Akun	100%	100%
Kontak	100%	100%
Chat	100%	100%
Gambar	0%	0%

Hasil dari validasi *reproducibility* yang dilakukan pada dua alat forensik untuk aplikasi *Messenger*

Daftar Rujukan

[1] L. H. Wei, O. C. Huat, and R. Thurasamy, "The impact of social media communication on consumer-based brand equity and purchasing intent in a pandemic," *International Marketing Review*, vol. 40, no. 5, pp. 1213–1244, Dec. 2023, doi: 10.1108/IMR-12-2021-0353.

[2] "1114-Other-2419-1-10-20210530".

[3] W. Presthus and D. M. Vatne, "A Survey on Facebook Users and Information Privacy," in *Procedia Computer Science*, Elsevier B.V., 2019, pp. 39–47. doi: 10.1016/j.procs.2019.12.152.

[4] "IT Security Economics 2022 Executive summary."

[5] Soni, E. Ramadhan, and D. Mualfah, "Investigasi Bukti Digital Aplikasi WeChat Menggunakan Framework Integrated Digital Forensics Proses Model (IDFPM) Berbasis SNI 27037 : 2014," *Jurnal INTEK*, vol. 4, no. 1, pp. 25–31, 2021.

[6] V. U. Sameer, I. Dali, and R. Naskar, "A deep learning based digital forensic solution to blind source identification of Facebook images," *... on Information Systems Security*, 2018, doi: 10.1007/978-3-030-05171-6_15.

[7] Statista, "Average consumer spend on mobile apps per smartphone as of 3rd quarter 2023.pdf," 2023.

[8] L. A. Arram and M. Moreb, "Cyber Security In Mobile Apps And User CIA," *2021 International Conference on ...*, 2021, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9491657/

[9] M. Kambar, A. Esmaeilzadeh, Y. Kim, and ..., "A survey on mobile malware detection methods using machine learning," *2022 IEEE 12th ...*, 2022, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9720753/

[10] N. Atanassov and M. M. Chowdhury, "Mobile Device Threat: Malware," *2021 IEEE International ...*, 2021, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9491845/

[11] M. I. Syahib, I. Riadi, and R. Umar, "Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST)," *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, vol. 4, no. 1, p. 170, 2020, doi: 10.30645/j-sakti.v4i1.196.

[12] R. Hayami, I. Komputer, U. M. Riau, and M. Forensik, "Jurnal Computer Science and Information Technology (CoSciTech) Akuisisi Bukti Digital Pada Aplikasi Michat di Smartphone Menggunakan Metode National Acquisition of Digital Evidence on the MiChat Application on Smartphones Using the National Institute of," vol. 3, no. 3, pp. 283–290, 2022.

[13] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "1490-Article Text-2859-1-10-20190413," *Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)*, vol. 4, pp. 219–227, 2018.

[14] M. Schofield, "Comparison of malware classification methods using convolutional neural network based on api call stream," *International Journal of Network Security &Its ...*, 2021, [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3822934

[15] A. A. Baso, P. Ariani, and A. Astuti, "The 5 th International Conference on Entrepreneurship Wired to Change: The Role of Digital Messaging in Boosting EV Awareness Among Indonesian Millennials."

[16] D. Mualfah, Muhammad Iqbal Syam, and Baidarus, "Analisis perbandingan tools mobile forensic menggunakan metode national institute of justice (NIJ)," *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 4, no. 1, pp. 283–292, May 2023, doi: 10.37859/coscitech.v4i1.4767.

[17] D. A. Ramadhan and R. A. Arrasyid, "Implementation of Live Forensic Method on Fusion Hard Disk Drive (HDD) and Solid State Drive (SSD) RAID 0 Configuration TRIM Features," 2024.

[18] D. Mualfah and I. Riadi, "Network Forensics For Detecting Flooding Attack On Web Server," 2017. [Online]. Available: https://sites.google.com/site/ijcsis/

[19] D. Mualfah and R. A. Ramadhan, "Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology)," *IT Journal Research and Development*, vol. 5, no. 2, pp. 171–182, 2020, doi: 10.25299/itjrd.2021.vol5(2).5731.

[20] R. A. Ramadhan, D. Mualfah, and D. Hariyadi, "Digital Forensics: Acquisition and Analysis on CCTV Digital Evidence using Static Forensic Method based on ISO /IEC 27037:2014," no. ICoSET 2019, pp. 85–89, 2020, doi: 10.5220/0009120400850089.

[21] F. T. Admojo, S. Risnanto, A. W. Windiawati, M. Innuddin, and D. Mualfah, "Comparison of Naïve Bayes and Random Forest Algorithm in Webtoon Application Sentiment Analysis," *Innovation in Research of Informatics (INNOVATICS)*, vol. 6, no. 1, pp. 23–28, 2024, doi: 10.37058/innovatics.v6i1.10636.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

[22] D. Mualfah, Y. Fatma, and R. A. Ramadhan, "Anti-forensics: The image asymmetry key and single layer perceptron for digital data security," in *Journal of Physics: Conference Series*, Institute of Physics Publishing, May 2020. doi: 10.1088/1742-6596/1517/1/012106.

[23] R. R. Hanaputra *et al.*, "Identifikasi Digital Evidence dalam Transaction Fraud pada WhatsApp Desktop berdasarkan NIST SP 800-86: Studi Kasus Bisnis Properti".

[24] I. Riadi and T. Ruslan, "Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST".