CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 5, No. 2, November 2022, hlm. 60-65

IMPLEMENTASI *MOBILE FORENSIC* PADA APLIKASI *MICHAT* DAN *TELEGRAM* DENGAN *FRAMEWORK* NIST 800-101

Nadia Ayu Isroh Maniar[1], Trihastuti Yuniati[2]

[1, 2]Institut Teknologi Telkom Purwokerto
Email: [1]18102242@ittelkom-pwt.ac.id, [2]trihastuti@ittelkom-pwt.ac.id

Abstrak

Sosial media merupakan *platform* untuk saling berkomunikasi secara daring yang memungkinkan orang-orang untuk berinteraksi tanpa dibatasi oleh ruang dan waktu. Salah satu aplikasi yang sering digunakan untuk melakukan kejahatan seperti prostitusi *online* adalah MiChat dan Telegram, karena kedua aplikasi ini mudah diakses dan memungkinkan penggunanya untuk mengirim foto dan video. Barang bukti kejahatan siber dapat berupa barang bukti elektronik dan barang bukti digital. Barang bukti elektronik adalah bentuk fisik dari perangkat elektronik yang terlibat dalam kejahatan, sedangkan barang bukti digital adalah dokumen, riwayat, atau log yang berisi data terkait dengan kejahatan tersebut. Penelitian ini meneliti penerapan teknik forensik pada perangkat *mobile* melalui penggunaan aplikasi MiChat dan Telegram. Ini bertujuan untuk mengumpulkan dan menganalisis data yang dapat digunakan sebagai bukti dalam suatu penyelidikan. Penelitian ini menggunakan kerangka kerja *National Institute of Standards and Technology Special Publication 800-101* Revisi 1 dan menggunakan alat bantu FTK Imager dan MOBILedit Forensic. Hasil penelitian menunjukkan bahwa FTK Imager lebih banyak mendapatkan barang bukti digital dibandingkan MOBILedit Forensic, dan akuisisi bukti digital pada aplikasi Telegram mendapatkan lebih sedikit bukti dibandingkan dengan aplikasi MiChat. Bukti digital yang berhasil didapatkan termasuk pesan percakapan, gambar, video, dan *voice note*.

Kata kunci: forensik digital, kejahatan siber, michat, nist, telegram

IMPLEMENTATION OF MOBILE FORENSIC ON MICHAT AND TELEGRAM APPLICATION WITH NIST 800-101 METHOD

Abstract

Social media is a platform for online communication that allows people to interact without being limited by space and time. One of the commonly used applications for criminal activities such as online prostitution is MiChat and Telegram, because these applications are easily accessible and allow users to send photos and videos. Cybercrime evidence can be in the form of electronic and digital evidence. Electronic evidence is the physical form of electronic devices involved in a crime, while digital evidence is documents, history, or logs containing data related to the crime. This study examines the implementation of forensic techniques on mobile devices using the MiChat and Telegram applications. The aim is to collect and analyze data that can be used as evidence in an investigation. This study uses the framework of the National Institute of Standards and Technology Special Publication 800-101 Revision 1 and uses FTK Imager and MOBILedit Forensic as assistance tools. The results show that FTK Imager obtained more digital evidence compared to MOBILedit Forensic, and the acquisition of digital evidence on the Telegram application obtained fewer evidences compared to the MiChat application. The successfully obtained digital evidence includes conversation messages, images, videos, and voice notes.

Keywords*: cybercrime, digital forensik, michat, nist, telegram*

1. PENDAHULUAN

Bersosialisasi secara daring melalui media sosial memungkinkan orang-orang untuk saling berkomunikasi tanpa terkendala ruang dan waktu (Nimda, 2012). Media sosial sudah diterima oleh masyarakat secara luas bahkan sekarang hampir semua kalangan menggunakan sosial media untuk kepentingan bersekolah seperti mengirim tugas atau berdiskusi dengan teman lainnya, beda halnya dengan yang sudah bekerja sosial media bisa

digunakan untuk mempromosikan barang dagangannya atau mengirimkan laporan kemajuan tugas atau pekerjaan yang sudah dikerjakan, karena adanya pandemi Covid-19 sehingga pekerjaan harus dilakukan secara *Work From Home* (WFH). Situasi tersebut menjadikan penggunaan media sosial semakin meningkat.

Berdasarkan data dari *We are Social* dan *Hootsuite*, terdapat sejumlah 202,6 juta pengguna internet di Indonesia pada Januari 2021. Sementara itu, ada 345,3 juta jaringan seluler yang aktif atau 125,6% dari total populasi, karena ada penduduk yang menggunakan lebih dari satu *smartphone* untuk beraktivitas di internet (Riyanto, 2021). Ini menunjukkan bahwa pengguna internet di Indonesia sangat tinggi dan banyak orang yang memiliki lebih dari satu perangkat untuk mengakses internet. Meskipun media sosial telah berkembang dan banyak orang yang menggunakannya untuk bersosialisasi, beberapa orang juga memanfaatkannya untuk kegiatan kriminal. (Mukti, Masruroh and Khairani, 2018). Hinsa Siburian, Kepala Badan Siber dan Sandi Negara (BSSN), menyatakan bahwa selama Januari hingga Agustus 2021, Indonesia mengalami 888.711.736 serangan siber (cnnindonesia.com, 2021). Maraknya pengguna *smartphone*, media sosial, dan internet di Indonesia saat ini disalahgunakan untuk melakukan kejahatan (*cybercrime*) seperti perdagangan manusia, *cyberbullying*, penipuan, pemerasan, perdagangan barang ilegal, perdagangan narkoba, dan banyak lagi (Sistem *et al.*, 2021). Ini menunjukkan bahwa Indonesia mengalami banyak serangan siber dan perlu meningkatkan keamanan siber untuk mengurangi risiko serangan tersebut. *Smartphone* sering digunakan sebagai alat untuk melakukan kejahatan, seperti mengirim pesan yang mengandung ancaman atau menyebarkan *hoax*. Ini menunjukkan bahwa penggunaan teknologi harus diawasi dan dikelola dengan baik untuk mengurangi risiko kejahatan yang dilakukan melalui teknologi.

Aplikasi *MiChat* dan *Telegram* merupakan dua contoh aplikasi yang disalahgunakan untuk prostitusi *online.* Hal tersebut dikarenakan aplikasi ini mudah diakses dan dapat digunakan untuk mengirim foto dan video. Menurut data dari Komisi Perlindungan Anak Indonesia (KPAI) terdapat 35 kasus eksploitasi seksual, perdagangan manusia, dan pekerja anak yang terjadi antara kurun waktu Januari hingga April 2021. Dari total kasus tersebut sebanyak 60% kasus dilakukan melalui media sosial, dimana 41% kasus menggunakan aplikasi *MiChat* (Jayani, 2021). Pada kasus kejahatan di atas diperlukan adanya barang bukti digital dari kasus kejahatan dengan media sosial tersebut sebagai barang bukti di persidangan (Bintang, Umar and Yudhana, 2020).

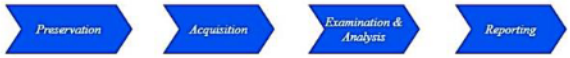
Barang bukti kejahatan siber dapat berupa bentuk fisik perangkat elektronik atau berkas digital yang berisi data-data yang terkait. Barang bukti elektronik dapat berupa perangkat elektronik yang terlibat dalam kejahatan, sedangkan barang bukti digital dapat berupa berkas dokumen, *history*, atau log yang mengandung informasi terkait kejahatan (Riadi, Umar and Nasrulloh, 2018). Penelitian ini menggunakan aplikasi *MOBILedit Forensic Express* dan *tools FTK Imager* sebagai perangkat untuk mencari barang bukti digital.

Berdasarkan latar belakang tersebut, penulis melakukan penelitian yang berjudul "Implementasi Mobile Forensik Pada Aplikasi *MiChat* dan *Telegram* Dengan Metode Nist 800-101". Aplikasi *MiChat* dan *Telegram* dipilih karena berdasarkan data dari KPAI, aplikasi *MiChat* ini media *online* yang paling banyak digunakan dalam kejahatan eksploitasi seksual dan perdagangan manusia, sedangkan *Telegram* adalah salah satu aplikasi *instant messenger* yang paling sering digunakan oleh orang Indonesia untuk saling bertukar komunikasi. Penelitian ini diharapkan dapat menghasilkan perbandingan banyaknya barang bukti yang didapat antara aplikasi *MiChat* dan *Telegram* dengan menggunakan metode *National Institute of Standards and Technology*.

2. METODE PENELITIAN

2.A. Metode

Metode *National Institute Of Standards Technology* (NIST), merupakan kerangka kerja yang sering digunakan dikarenakan NIST mengatur standar pedoman dan praktek terbaik dalam mengelola resiko terkait segala bentuk yang berkaitan dengan sains dan teknologi informasi (*View of Penerapan Metode NIST untuk Analisis Serangan Denial of Service (DOS) pada Perangkat Internet of Things (IoT)*, *no date*). Metode ini digunakan untuk menjabarkan bagaimana tahapan demi tahapan secara rinci dan sistematis, sehingga dapat menyelesaikan masalah yang ada. Tujuan dari metode ini digunakan untuk mempertahakan hasil yang didapatkan sehingga bisa dijadikan sebagai barang bukti hukum (Ahmadi, Akbar and Mandala Putra, 2021). Tahapan pada metode *National Institute of Standards And Technology* (NIST) *Spesial Publication 800-101 Revision 1* ditunjukkan oleh Gambar 1 (Studi *et al.*, 2021):



Gambar 1. Metode NIST *Spesial Publication 800-101 Revision 1*

1. *Preservation*

Pada tahapan ini yang dilakukan yaitu pengambilan data dari media yang akan dilakukan identifikasi saat penelitian serta pelabelan dengan tetap mengikuti prosedur dalam menjaga keaslian data.

2. *Acquisition*

Pada tahap ini merupakan tahapan pengumpulan data pada saat diproses dengan metode

forensik secara otomatis maupun manual, serta menilai dan mengeluarkan datanya sesuai dengan kebutuhan dan tetap mempertahankan integritas data.

3. *Examination & Analysis*

Pada tahap ini melakukan tahapan pemeriksaan serta analisis terhadap data yang dilakukan sesuai dengan aturan sehingga mendapatkan data untuk dijadikan bukti terkait dengan kasus tersebut.

4. *Reporting*

Pada tahap ini hasil investigasi yang didapatkan dari penyelidikan berisi tentang hasil analisa barang bukti dilaporkan sehingga bukti tersebut dapat membantu dalam proses penyelidikan untuk menemukan tersangka.

2.B. Alat dan Bahan

Perangkat lunak yang digunakan dalam penelitian ini yaitu :

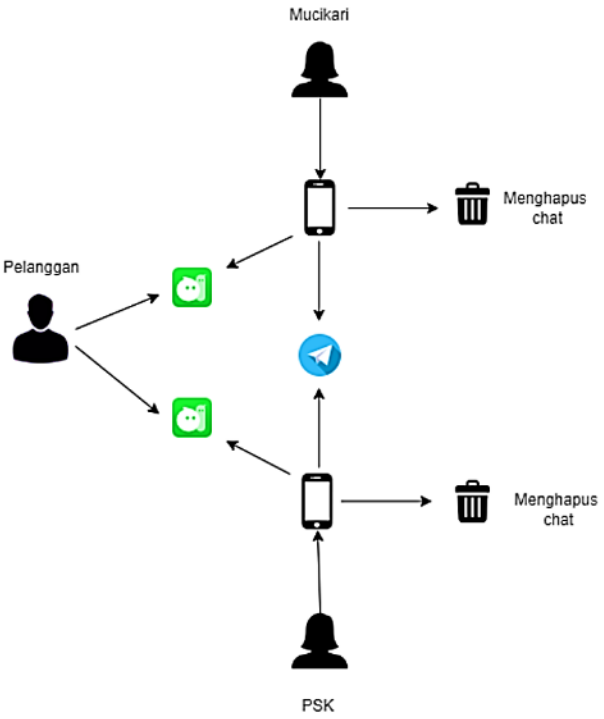
1. *MiChat* versi 1.4.118 dan *Telegram* versi 8.2.7 sebagai aplikasi media sosial yang digunakan untuk transaksi prostitusi *online*
3. *FTK Imager* versi 4.5.0 dan *MOBILedit Forensic Express* versi 7.4.1 (64 bit) sebagai perangkat untuk akuisisi barang bukti digital dengan teknik forensik digital

Untuk dapat menjalankan perangkat lunak yang disebutkan di atas, diperlukan perangkat keras dengan spesifikasi tertentu. Perangkat keras yang digunakan dalam penelitian ini yaitu :

1. Laptop dengan *processor Intel Core i5, OS Windows 64bit,* digunakan untuk *cloning* dan akuisisi barang bukti digital menggunakan *tools FTK Imager* versi 4.5.0 dan *MOBILedit Forensic* versi 7.4.1 (64 bit)
2. Kabel USB digunakan untuk memindahkan data hasil *cloning* ponsel ke laptop
3. *Flashdisk* untuk menyimpan data hasil kloning
4. Ponsel OPPO A37 sebagai perangkat yang digunakan oleh mucikari dalam skenario tindak pidana prostitusi *online* menggunakan aplikasi MiChat dan Telegram
4. Ponsel WIKO HARRY sebagai perangkat yang digunakan oleh PSK dalam skenario tindak pidana prostitusi *online* menggunakan aplikasi MiChat dan Telegram
5. Ponsel OPPO A3S sebagai perangkat yang digunakan oleh pelanggan dalam skenario tindak pidana prostitusi *online* menggunakan aplikasi MiChat dan Telegram

2.C. Pengumpulan data

Sumber data yang digunakan pada penelitian ini adalah data dari dokumentasi simulasi skenario yang sudah dibuat oleh pihak peneliti untuk dijadikan sebagai barang bukti digital. Objek yang akan digunakan pada penelitian ini yaitu riwayat percakapan, *voice note*, gambar, dan video. Data yang akan diambil untuk penelitian ini hanya dilakukan satu kali pengambilan data tetapi apabila data tersebut belum ditemukan maka pengambilan data akan terus berulang hingga ditemukannya bukti digital yang diinginkan. Gambar 2 merupakan skenario yang akan dilakukan dalam penelitian.



Gambar 2. Skenario Simulasi Pengumpulan Data

Penjelasan alur skenario yang ditunjukkan oleh Gambar 2 adalah sebagai berikut:

1. Mucikari melakukan komunikasi dengan pelanggan melalui aplikasi MiChat
2. Mucikari memberikan informasi kepada pelanggan tentang PSK yang akan dipekerjakan
3. Setelah diperoleh kesepakatan antara mucikari dengan pelanggan, mucikari kemudian menginformasikan kepada PSK melalui aplikasi Telegram bahwa aka nada yang menggunakan jasanya
4. Mucikari memberikan kontak pelanggan kepada PSK
5. PSK melakukan komunikasi dengan pelanggan menggunakan aplikasi MiChat
6. Mucikari, PSK dan pelanggan menghapus semua pesan percakapan yang ada di aplikasi MiChat dan Telegram untuk menghilangkan barang bukti
7. Dilakukan penyidikan dan penyelidikan untuk mendapatkan barang bukti digital yang ada pada ponsel mucikari (OPPO A37) di aplikasi MiChat dan Telegram

3. HASIL DAN PEMBAHASAN

3.A. *Preservation*

Pada tahapan NIST 800-101 yang pertama, yaitu tahap *preservation*, ponsel atau barang bukti yang digunakan oleh mucikari, yaitu Ponsel OPPO A37, akan diamankan untuk dilakukan proses identifikasi dan pelabelan. Barang bukti ponsel tersebut kemudian diisolasi dengan cara dibuat mode pesawat dan dimatikan agar tidak dapat diakses dan dimodifikasi oleh pihak yang tidak berhak sebelum dilakukan penyidikan.

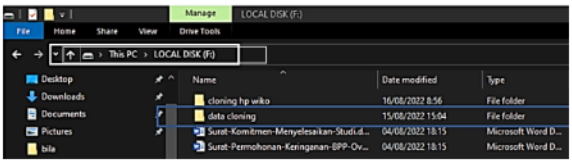
3.B. *Acquisition*

Pada tahap NIST 800-101 berikutnya, yaitu tahap *acquisition*, data yang terdapat pada perangkat ponsel diambil secara forensik menggunakan *tools FTK Imager* versi 4.5.0 dan *MOBILedit Forensic Express* versi 7.4.1. Perangkat ponsel yang menjadi barang bukti dalam kondisi *non-root* untuk menjaga keutuhan barang bukti. Tabel 1 menunjukkan informasi perangkat ponsel OPPO A37 yang digunakan oleh mucikari yang dilakukan akuisisi.

Tabel 1. Informasi Perangkat Ponsel OPPO A37

Informasi Perangkat Ponsel	
Nama Pemilik Perangkat Ponsel	D*** Y******
Nama Perangkat Ponsel	OPPO A37
Nomer Model	A37
Sistem Operasi	Android 10
IMEI	865**********
***Memory* Eksternal**	Ada
Kartu SIM *Card*	Ada
Kata Sandi	Ada

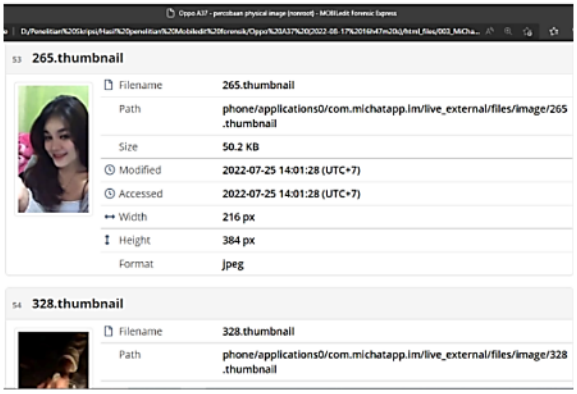
Berdasarkan Tabel 1 diketahui bahwa perangkat yang akan digunakan untuk penyelidikan dalam kondisi *non-root* serta terdapat memori eksternal dan kartu SIM *card*. Agar mendapatkan data pada ponsel dengan kondisi *non-root* maka dilakukan sebuah *cloning* data dimana ponsel mentransferkan datanya melalui USB ke laptop selanjutnya dipindahkan ke *flashdisk*. Gambar 3 merupakan lokasi penyimpanan data *cloning* ponsel OPPO A37 yang disimpan di *LOCAL DISK* (F:), data ini nantinya akan digunakan sebagai bahan pengujian pada kondisi *non-root*.



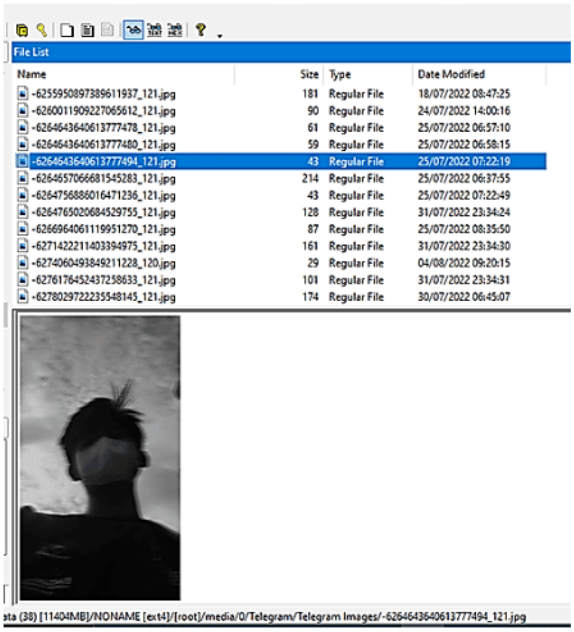
Gambar 3. Data *Cloning* pada *Flashdisk*

3.C. *Examination & Analysis*

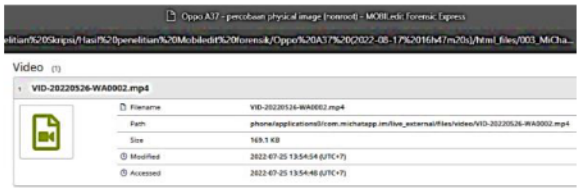
Pada tahapan NIST 800-101 yang ketiga, yaitu *Examination & Analysis*, dilakukan pencarian barang bukti digital dengan teknik forensik menggunakan dua *tools, MOBILedit Forensic Express* dan *FTK Imager*. Barang bukti digital yang dimaksud adalah pesan percakapan antara mucikari dengan pelanggan dan pesan percakapan PSK dengan pelanggan dari skenario yang telah dibuat sebelumnya. Barang bukti digital yang berhasil atau tidak berhasil diperoleh dengan teknik forensik menggunakan kedua *tools* kemudian dicatat, untuk selanjutnya dapat diketahui barang bukti apa sajakah yang berhasil diperoleh dari aplikasi Telegram dan MiChat menggunakan *MOBILedit Forensic Express* dan *FTK Imager*. Gambar 4 sampai dengan Gambar 9 merupakan contoh sebagian bukti digital yang berhasil ditemukan pada aplikasi *Michat* dengan *tools MOBILedit Forensic Express* dan *FTK Imager* berupa foto, video, dan pesan suara.



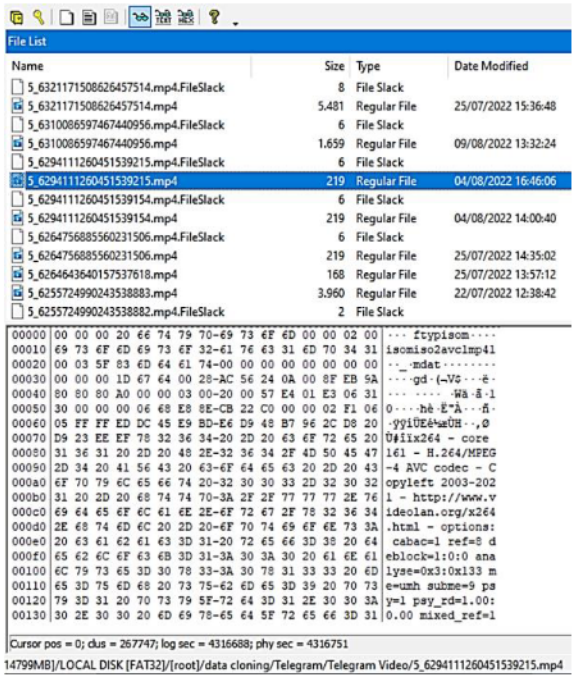
Gambar 4. Bukti digital berupa foto pada *tools MOBILedit Forensic*



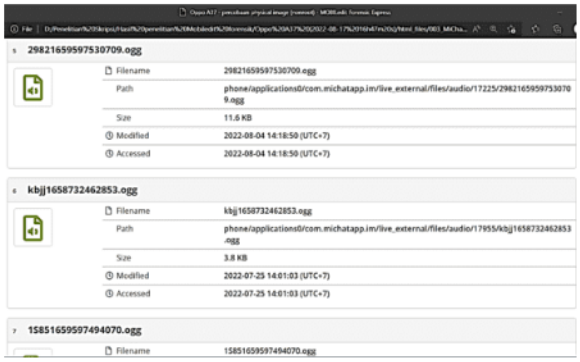
Gambar 5. Bukti digital berupa gambar pada *tools FTK Imager*



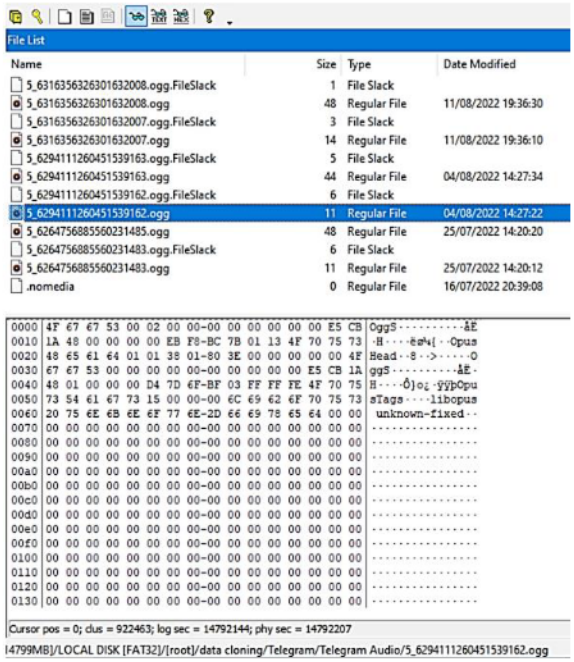
Gambar 6. Bukti digital berupa video pada *tools MOBILedit Forensic*



Gambar 7. Bukti digital berupa video pada *tools FTK Imager*



Gambar 8. Bukti digital berupa pesan suara pada *tools MOBILedit Forensic*



Gambar 9. Bukti digital berupa pesan suara pada *tools FTK Imager*

3.D. *Reporting*

Reporting merupakan tahapan yang terakhir dari NIST 800-101. Setelah melakukan pemeriksaan dan akuisisi bukti digital menggunakan *tools MOBILedit Forensic Express* dan *FTK Imager* maka langkah selanjutnya adalah menyusun laporan hasil dari analisis yang sudah ditemukan secara keseluruhan. Secara garis besar, hasil akuisisi barang bukti digital pada aplikasi MiChat dan Telegram menggunakan *tools MOBILedit Forensic Express* dan *FTK Imager* ditunjukkan oleh Tabel 2.

Tabel 2. Hasil akuisisi barang bukti digital pada aplikasi MiChat dan Telegram dengan *tools MOBILedit Forensic Express* dan *FTK Imager*

Barang bukti	FTK Imager		MOBILedit Forensic Express	
	MiChat	Telegram	MiChat	Telegram
Teks	X	X	X	X
Gambar	V	V	V	V
Video	V	V	V	X
Voice note	V	V	V	X

Keterangan:

X = tidak ditemukan

V = berhasil ditemukan

4. KESIMPULAN DAN SARAN

4.A. Kesimpulan

Berdasarkan hasil penelitian forensik digital yang telah dilakukan dengan menerapkan kerangka kerja *National Institute of Standards And Technology* (NIST) *Spesial Publication 800-101 Revision 1* menggunakan *tools MOBILedit* Forensik

dan *FTK Imager* terhadap aplikasi *MiChat* dan *Telegram* dapat disimpulkan bahwa :

1. Hasil akuisisi baik menggunakan *tools MOBILedit Forensic* maupun *FTK Imager* hanya berhasil ditemukan barang bukti digital berupa gambar, video, dan *voice note* sedangkan pesan berupa teks percakapan tidak berhasil ditemukan.
2. Dari kedua *tools* yang digunakan dalam penelitian ini, secara keseluruhan *tools FTK Imager* mampu mendapatkan hasil barang bukti digital lebih banyak dibandingkan *MOBILedit Forensic*.

4.B. Saran

Saran untuk penelitian selanjutnya yaitu :

1. Melakukan akuisisi barang bukti digital pada aplikasi selain *MiChat* dan *Telegram* agar dapat diketahui tingkat keamanan pada masing-masing aplikasi.
2. Menggunakan *tools* selain *MOBILedit Forensic* dan *FTK Imager* untuk mengetahui tingkat akuisisi yang mampu didapatkan oleh masing-masing *tools*.

DAFTAR PUSTAKA

AHMADI, AHWAN, AKBAR, T. AND MANDALA PUTRA, H. 2021. Perbandingan Hasil Tool Forensik Pada File Image *Smartphone* Android Menggunakan Metode Nist, *JIKO (Jurnal Informatika dan Komputer)*, 4(2), pp. 92–97. doi: 10.33387/jiko.v4i2.2812.

BINTANG, R. A., UMAR, R. AND YUDHANA, A. 2020. Analisis Media Sosial Facebook Lite dengan *tools* Forensik menggunakan Metode NIST, *Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto)*, 21(2), p. 125. doi: 10.30595/techno.v21i2. 8494.

CNNINDONESIA.COM. 2021. *BSSN: Ada 888 Juta Serangan Siber Sepanjang 2021*, *www.cnnindonesia.com*. Available at: https://www.cnnindonesia.com/nasional/20210913131225-12-693494/bssn-ada-888-juta-serangan-siber-sepanjang-2021 (Accessed: 12 November 2021).

JAYANI, D. H. 2021. *Kasus Prostitusi Anak Paling* Banyak *Terjadi lewat Aplikasi MiChat*, *databoks.katadata.co.id*. Available at: https://databoks.katadata.co.id/datapublish/2021/06/03/kasus-prostitusi-anak-paling-banyak-terjadi-lewat-aplikasi-michat (Accessed: 7 November 2021).

MUKTI, W. A., MASRUROH, S. U. AND KHAIRANI, D. 2018. Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada *Smartphone* Android, *Jurnal Teknik Informatika*, 10(1), pp. 73–84. doi: 10.15408/jti.v10i1.6820.

NIMDA. 2012. *Apa itu Sosial Media*, *http://www.unpas.ac.id/*. Available at: http://www.unpas.ac.id/apa-itu-sosial-media/ (Accessed: 7 November 2021).

RIADI, I., UMAR, R. AND 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)*, 3(1), pp. 70–82. doi: 10.21831/elinvo.v3i1.19308.

RIYANTO, A. D. 2021. *Hootsuite (We are Social): Indonesian Digital Report 2021*, *andi.link*. Available at: https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2021/ (Accessed: 7 November 2021).

RIADI, I., UMAR, R. AND SYAHIB, M. I. 2021. Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode Nasional Institute of Standards and Technology (NIST), *Jurnal Resti*, 1(10), pp. 45–54.

MUSHLICH, M.M.A.S., IZZUDDIN, M.A., AND RIDWAN., M. 2021. Analisis Kinerja Aplikasi Forensik Open-Source Pada Ponsel Cerdas Berbasis Android Dalam Mendapatkan Bukti Digital, *Jurnal Inovasi Informatika Universitas Pradita (JII)*, 6(2), pp. 86-97. doi: https://doi.org/10.51170/jii.v6i2.175

ARSADA. L., AND MUSLIM. A. 2021. Penerapan Metode NIST untuk Analisis Serangan Denial of Service (DOS) pada Perangkat Internet of Things (IoT), *Jurnal Ilmiah KOMPUTASI*, 20(2), pp. 275-281.