



Akuisisi bukti digital aplikasi pesan instan “bip” menggunakan metode national institute of Justice (NIJ)

Soni^{*1}, Yulia Fatma², Rizki Anwar³

Email: ¹soni@umri.ac.id, ²yuliafatma@umri.ac.id, ³170401060@student.umri.ac.id

^{1,2,3}Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau

Diterima: 25 Mei 2022 | Direvisi: - | Disetujui: 31 Mei 2022

©2020 Program Studi Teknik Informatika Fakultas Ilmu Komputer,
Universitas Muhammadiyah Riau, Indonesia

Abstrak

Dalam perkembangan revolusi industri 4.0, informasi semakin menunjukkan pengaruh yang besar terhadap kehidupan manusia. Penggunaan teknologi smartphone sering digunakan untuk akses media sosial dan juga internet. Perkembangan smartphone, media sosial, dan jumlah pengguna internet di dunia khususnya di Indonesia saat ini sedang banyak disalahgunakan, salah satunya kejahatan (cybercrime), seperti prostitusi online, perdagangan manusia, cyberbullying, penipuan, pemerasan, perdagangan barang ilegal, perdagangan narkoba. Cyberbullying merupakan tindakan dengan sengaja dan berulang kali menyerang, menghina, atau merugikan orang lain di media sosial, aplikasi instant messenger atau dengan cara lain yang mengarah pada penghinaan terhadap SARA. Metode NIJ merupakan sebuah metode yang bertujuan untuk menjelaskan bagaimana langkah-langkah penelitian yang akan dilakukan sehingga alur dan langkah-langkah penelitian dapat diidentifikasi secara sistematis sehingga dapat dijadikan pedoman untuk memecahkan permasalahan yang ada Metode NIJ dapat diterapkan dalam mengungkap kasus pesan chat yang terhapus. Proses mendapatkan mendapatkan bukti digital pesan yang terhapus dari aplikasi pesan instan “BIP” berhasil didapatkan dengan cara melakukan pengangkatan barang bukti dari smartphone pelaku menggunakan metode National Institute Of Justice (NIJ).

Kata kunci: Bukti Digital, BIP Messenger, Cyberbullying, NIJ, Smartphone

Acquisition of digital evidence “bip” instant messaging application using national institute of justice (NIJ) method

Abstract

In the development of the industrial revolution 4.0, information is increasingly showing a great influence on human life. Smartphone technology is often used to access social media and the internet. The development of smartphones, social media, and the number of internet users in the world, especially in Indonesia, are currently being misused, one of which is crime (cybercrime), such as online prostitution, human trafficking, cyberbullying, fraud, extortion, trafficking in illegal goods, drug trafficking. Cyberbullying is an act of intentionally and repeatedly attacking, insulting, or harming other people on social media, instant messenger applications or in other ways that lead to insulting SARA. The NIJ method is a method that aims to explain how the research steps will be carried out so that the flow and research steps can be identified systematically so that they can be used as guidelines for solving existing problems. The NIJ method can be applied in uncovering cases of deleted chat messages. The process of obtaining digital evidence of deleted messages from the instant messaging application "BIP" was successfully obtained by removing evidence from the perpetrator's smartphone using the National Institute Of Justice (NIJ) method.

Keywords: digital evidence, BIP messenger, cyberbullying, NIJ, smartphone

1. PENDAHULUAN

Perkembangan smartphone, media sosial, dan jumlah pengguna internet di dunia khususnya di Indonesia saat ini sedang banyak disalahgunakan, salah satunya kejahatan (cybercrime), seperti prostitusi online, perdagangan manusia, cyberbullying, penipuan, pemerasan, perdagangan barang ilegal, perdagangan narkoba.

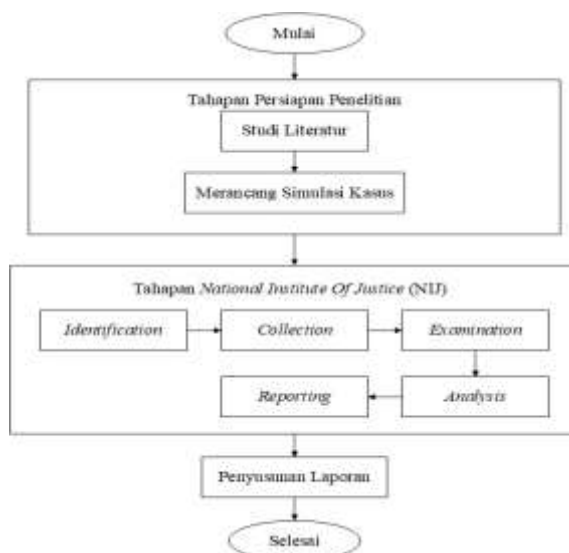
Cyberbullying merupakan tindakan dengan sengaja dan berulang kali menyerang, menghina, atau merugikan orang lain di media sosial, aplikasi instant messenger atau dengan cara lain yang mengarah pada penghinaan terhadap SARA. Beberapa kasus cyberbullying yang pernah terjadi di Indonesia Pemerintah mengumumkan bahwa setidaknya 84% remaja berusia 12 hingga 17 tahun di Indonesia telah ditindas, dan sebagian besar kasus perundungan yang dilaporkan melibatkan cyberbullying (Laksana, 2017). Di Indonesia, cyberbullying menempati urutan ketiga di dunia. Sebanyak 91% laporan cyberbullying terjadi pada anak-anak. Sangat ironis mengingat Indonesia dikenal dengan masyarakatnya yang ramah dan budaya sopan santun (Fauzan et al., 2017). Menurut data dari Komisi Perlindungan Anak Indonesia (KPAI) per tanggal 30 Mei 2018, kasus bullying dan cyberbullying berjumlah 161 kasus, dari jumlah tersebut terungkap data anak korban kasus kekerasan dan bullying mencapai 22,4% dan anak pelaku kekerasan dan bullying mencapai 25,5%. Perilaku bullying dilakukan baik secara langsung ataupun tidak langsung (cyberbullying) (Nazara, 2019). Kasus kejahatan pada forensik digital sangat rentan pada aplikasi instant messenger apa saja, seperti BIP.

BIP merupakan aplikasi instant messenger yang memiliki fitur menyediakan pengiriman pesan, panggilan telepon, panggilan video, taks, gambar, dan video. Aplikasi BIP dikembangkan oleh turkcell pada tahun 2013. Menurut (kompas.com) aplikasi ini tersedia di play store dan IOS, dan telah diunduh di Play Store oleh 50 juta lebih dan 1 juta ulasan dari para penggunanya.

Kejahatan siber pasti akan meninggalkan barang bukti digital, walaupun pelaku menghilangkan barang bukti digital tersebut, dengan cara menghapus barang bukti (chatting) tersebut dari smartphone. Bukti digital yang berada pada perangkat smartphone, seperti data kontak, catatan panggilan, pesan (chatting), video, gambar, dokumen. Tujuan dari penelitian ini untuk melakukan simulasi akuisisi dan mengetahui barang bukti digital (chatting) yang telah dihapus sebelumnya dan barang bukti digital tersebut akan menjadi bukti sebagai laporan tindak kejahatan di pengadilan (Yudhana, Riadi, et al., 2018). Penelitian ini menggunakan metode National Institute Of Justice (NIJ). Metode NIJ dapat diterapkan dalam mengungkap kasus pesan chat yang terhapus. Metode NIJ merupakan sebuah metode yang bertujuan untuk menjelaskan bagaimana langkah-langkah penelitian yang akan dilakukan sehingga alur dan langkah-langkah penelitian dapat diidentifikasi secara sistematis sehingga dapat dijadikan pedoman untuk memecahkan permasalahan yang ada (Riadi, Umar, et al., 2018). Alasan pemilihan metode NIJ, yaitu metode ini lebih efisien untuk diterapkan pada penelitian ini, dikarenakan alur atau tahapan yang digunakan pada metode terurut dan sistematis, yakni dari identification, collection, examination, analysis, reporting (Riadi, Yudhana, et al., 2018).

2. METODE PENELITIAN

Adapun alur penelitian yang direncanakan dalam penelitian ini seperti pada ilustrasi berikut:



Gambar 1. Alur Penelitian

Untuk membantu proses investigasi forensik yang meliputi media elektronik seperti smartphone, maka membutuhkan suatu metode agar pada saat melakukan penyelidikan, proses investigasi menjadi lebih terstruktur. Penelitian ini menggunakan metode NIJ. Kerangka penelitian ini dapat dilihat di pada gambar 1.

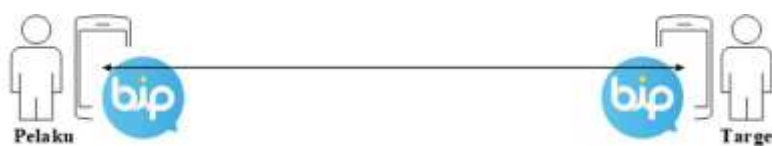
3. HASIL DAN PEMBAHASAN

3.1. Rancangan Skenario Kasus

Pembuatan skenario dan implementasi skenario dijalankan untuk mendapatkan barang bukti digital. Pada penelitian ini penulis menjelaskan apa saja yang akan dilakukan pada aktivitas yang dilakukan pada aplikasi BIP Messenger. Tujuan dari pembuatan simulasi skenario kasus ini agar dapat informasi data percakapan apa saja yang dapat diperoleh dari recovery. Skenario tersebut sebagai berikut :

1. Membuat akun BIP Messenger 082169229331 (Akun Korban).
2. Membuat akun Messenger dua +6281276825306 (Akun Pelaku).
3. Akun pelaku melakukan percakapan (chatting) penipuan bertransaksi melalui aplikasi BIP Messenger dengan korban.
4. Akun pelaku mengirimkan gambar kepada korban.
5. Pada akun pelaku seluruh bukti (percakapan, gambar) merupakan tindakan cyberbullying dan pada perangkat smartphone pelaku buktinya dihilangkan.

Percakapan yang telah dihapus oleh pelaku pada aplikasi BIP Messenger akan diungkap menggunakan tools forensics, guna untuk mendapatkan bukti digital dan menjadikan bukti digital sebagai barang bukti yang sah pada saat dipengadilan. Skenario diatas dijelaskan pada gambar 3.



Gambar 2 Rancangan Skenario

3.2. Investigasi Metode National Institute Of Justice (NIJ)

3.2.1 Identification

Pada penelitian ini barang bukti smartphone yang diperoleh dalam kondisi kondisi normal dan menyala. Dan implementasi dilakukan untuk mendapatkan gambaran tentang mendapatkan barang bukti pada perangkat smartphone. Kondisi smartphone dapat dilihat pada gambar 3.1 yang memperlihatkan kondisi smartphone dalam kondisi menyala.



Gambar 3.1 Barang Bukti Smartphone

Pada gambar 3.1 memperlihatkan kondisi smartphone dalam kondisi menyala. Dan setelah mendapatkan perangkat smartphone milik pelaku maka dilakukan tindakan mendokumentasikan informasi terkait data smartphone.

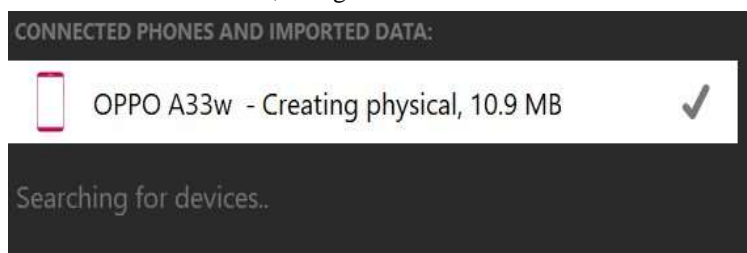
Tabel 3 Spesifikasi Identitas Smartphone

Model	Oppo
Product	Oppo A33w
Platform	Android
IMEI1	861485033878837
IMEI2	861485033878829
Nomor Seri	95AUQKFUFQZDBYJR
Operator	XL

3.2.2 Collection

Melakukan pengumpulan barang bukti dan membackup seluruh data pada perangkat smartphone menggunakan tools forensics, sebelum melakukan backup data perangkat smartphone dilakukan root agar mendapatkan file data yang telah dihapus atau

dihilangkan. Tools forensics yang digunakan untuk membackup data perangkat smartphone menggunakan MOBILedit Forensic. Adapun langkah – langkah dalam melakukan akuisisi, sebagai berikut :



Gambar 3.2 Proses Akuisisi Smartphone

Hasil backup data dari perangkat smartphone dapat dilihat pada gambar 3.3

File Explorer path: C > Fileku (E:) > Simple > Data Skripsi Anwar > OPPO A33w (2022-03-13 23h20m14s)

Name	Date modified	Type	Size
adb_backup	13/03/2022 23:26	File folder	
mobiledit_export_files	14/03/2022 0:38	File folder	
phone_files	14/03/2022 0:37	File folder	
log_full	14/03/2022 0:59	Text Document	3.379 KB
log_short	14/03/2022 0:09	Text Document	2 KB
mobiledit_backup	14/03/2022 0:09	XML Document	8.802 KB
mobiledit_export	14/03/2022 0:37	XML Document	14.275 KB
report.ufdr	14/03/2022 0:59	UFDR File	1.966.031 KB
report_configuration.cfg	13/03/2022 23:20	CFG File	5 KB

Gambar 3.3 Hasil Akuisisi Smartphone

3.2.3 Examination

Setelah pada tahap sebelumnya melakukan pengumpulan data dengan cara backup data. Pada tahap kali ini merupakan tahap investigasi dari hasil backup data tersebut. Proses investigasi dari penelitian ini yaitu pada aplikasi pesan instan BIP Messenger. Merupakan tahap verifikasi data yang terdapat pada smartphone pelaku, namun harus memverifikasi terlebih dahulu apakah smartphone tersebut sudah di root atau belum. Tahap examination juga memastikan bahwa data yang diperoleh dalam bentuk file adalah asli seperti yang diperoleh di tempat kejadian kejahatan dunia maya, karena file digital harus diidentifikasi dan divalidasi dengan teknik hashing.

3.2.4 Analysis

Setelah melakukan pengangkatan barang bukti pada aplikasi BIP dari smartphone. Pada tahap ini menganalisis berupa temuan dari barang bukti digital tersebut. Berikut merupakan tahap melakukan analisis, sebagai berikut:

a. Temuan Barang Bukti

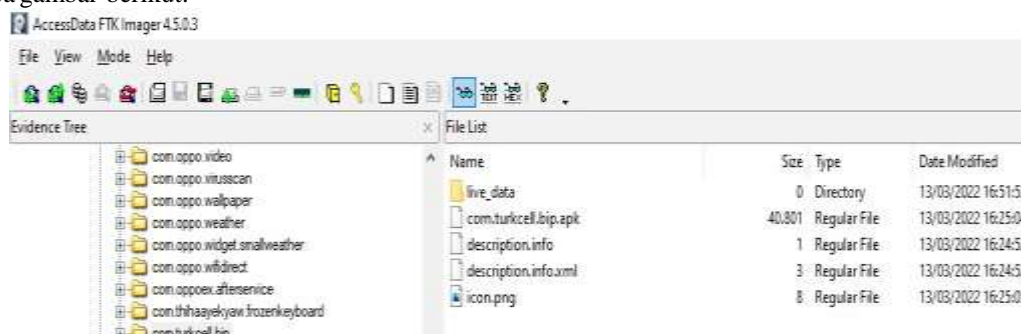
Berikut merupakan tahap melakukan analisis, sebagai berikut :

1. Temuan hasil dari akuisisi merupakan *file* folder dari proses ekstrasi. *File* ekstrasi dapat dilihat pada gambar berikut:

live_data	13/03/2022 23:51	File folder	
com.turkcell.bip.apk	13/03/2022 23:25	APK File	40.801 KB
description.info	13/03/2022 23:24	INFO File	1 KB
description.info	13/03/2022 23:24	XML Document	3 KB
icon	13/03/2022 23:25	PNG File	8 KB

Gambar 3.4 Hasil Ekstraksi Pada Aplikasi BIP Messenger

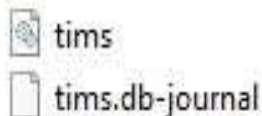
2. Untuk mengetahui struktur dari *folder* pada aplikasi BIP Messenger menggunakan *tools FTK Imager*. Dapat dilihat pada gambar berikut:



Gambar 3.4 Struktur Folder dari BIP Messenger

Struktur folder utama terdapat satu folder utama dalam folder com.turkcell.bip dan ini merupakan hasil proses akuisisi pada barang bukti.

- Berikut merupakan database dari aplikasi BIP Messenger dapat dilihat pada gambar berikut:



Gambar 3.5 Database Aplikasi BIP Messenger

Pada gambar 3.5 merupakan file database yang berada pada aplikasi BIP Messenger setelah menemukan file database lalu dilakukan investigasi dengan membuka file database aplikasi BIP Messenger menggunakan Oxygen Forensic SQLite Viewer. Dan nilai hash dari file database BIP Messenger dapat dilihat pada tabel 3 berikut:

Tabel 3 Nilai Hash Dari File Image Database

Tipe	Nilai
MD5	2C670337544F760D6D2B764C6A3EAB7A

- Hasil Temuan Barang Bukti Isi Chat Dari Database

Temuan barang bukti chat dengan membuka file database dari aplikasi BIP Messenger menggunakan Oxygen Forensics SQLite Viewer. Temuan barang bukti chatting dapat dilihat pada tabel 3.1.

Tabel 3.1 Barang Bukti Chat

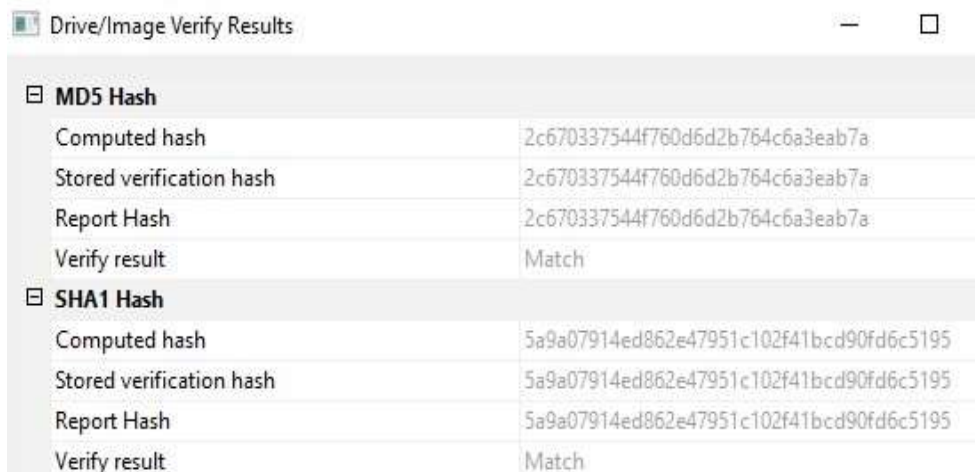
No	Bukti Chat		
1.	4F 79 20 67 61 70 75 61 64 20 6C 75 20 61 70 61 6E 67 61 64 75 20 67 69 72 75 2C 20 20 6D 61 75 6B 61 20 6C 75	6B 2C 20 6D 61 6B 73 75 20 73 61 6D 70 61 69 20 74 75 20 6B 65 20 67 75 20 63 61 72 69 20 6D 75	Oy gapuak, maksu d lu apa sampai ngadu gitu ke gu ru, mau cari mu ka lu Isi pesan pelaku : Oy gapuak, maksud lu apa sampai ngadu gitu ke guru, mau cari mukalu
2.	4F 79 20 67 61 70 75 61 64 20 6C 75 20 61 70 61 6E 67 61 64 75 20 67 69 72 75 2C 20 20 6D 61 75 6B 61 20 6C 75	6B 2C 20 6D 61 6B 73 75 20 73 61 6D 70 61 69 20 74 75 20 6B 65 20 67 75 20 63 61 72 69 20 6D 75	Oy gapuak, maksu d lu apa sampai ngadu gitu ke gu ru, mau cari mu ka lu Isi pesan pelaku : Lu udh gapuak, dekil, hitam, pendek. Tapi tu mulut ember kayak cwe
3.	4E 67 61 70 61 69 6E 20 69 6E 20 6B 65 20 67 75 20 67 75 61 20 63 61 62 20 62 65 6C 61 6B 61 6E 67	6C 75 20 6C 61 70 6F 72 72 75 2C 20 6B 61 6C 6F 75 74 20 6C 65 77 61 74 67 20 73 65 6B 6F 6C 61	Ngapain lu lapor in ke guru, kalo gua cabut lewat belakang sekola g Isi pesan pelaku : Ngapain lu laporin ke guru, kalo gua cabut lewat belakang sekolah
4	4D 61 61 66 2C 73 61 79 6D 61 61 66 20 73 61 79 62 65 72 6D 61 6B 73 75 69 20 69 74 75	61 20 6D 69 6E 74 61 20 61 20 74 69 64 61 6B 20 64 20 73 65 70 65 72 74	Maaf, saya minta maaf saya tidak bermaksud seperti itu Isi pesan korban : Maaf, saya minta maaf saya tidak bermaksud seperti itu
5	4B 61 6C 6F 20 73 61 79 73 61 79 61 20 6D 69 6E 79 61	61 20 73 61 79 61 2C 20 74 61 20 6D 61 61 66 20	Kalo saya saya, saya minta maaf ya Isi pesan korban : Kalo saya salah, saya minta maaf ya

No	Bukti Chat
6	 <p>Sebelum di recovery terdapat dua pesan yang dihapus</p>
7	 <p>Isi pesan pelaku setelah di recovery : Awas lu, ketemu gua sama lu. Abis lu gua buat</p>
8	 <p>Isi pesan pelaku setelah di recovery : Mau lu gua buat kayak gini ha puak</p>
9	 <p>Hasil dari gambar yang dikirim pelaku</p>

b. Verifikasi Akuisisi

Pada tahap ini merupakan membandingkan nilai hash dari file hasil ekstraksi pada saat melakukan forensik dan sesudah selesai mendapatkan barang bukti. Berikut adalah merupakan nilai hash pada Database BIP.

- Hash Image Database BIP
Nilai hash pada file database BIP setelah melakukan akuisisi



Gambar 3.6 Nilai Hash Database BIP

Pada gambar 4.11 memperlihatkan bahwasannya tidak adanya perubahan nilai hash yang eksekusi atau imaging dengan nilai hash awal dari barang bukti.

- aa

3.2.5 Reporting

Tahap reporting merupakan tahap akhir dari proses investigasi, tahap ini merupakan tahap membuat laporan hasil dari penemuan barang bukti yang didapat selama proses penyelidikan pada saat pengangkatan bukti digital pada smartphone. Untuk tabel reporting dapat dilihat pada tabel 3.2

Tabel 3.2 Hasil *Reporting* Forensik Digital FORM

	<p align="center">REPORTING HASIL INVESTIGASI</p> <p align="center">INFORMATIC ENGINEERING LABORATORY</p> <p align="center">UNIVERSITAS MUHAMMADIYAH RIAU</p> <p align="center">Tuanku Tambusai Street Pekanbaru City</p>
	INFORMASI KASUS
Nomor Laporan	001045
Nama Kasus	Pengangkatan bukti digital pada aplikasi BIP kasus <i>cyberbullying</i>
Waktu dan Tanggal	Senin, 16 Maret 2022
Nomor Kasus	01
PIHAK PENANGGUNG JAWAB	
Investigator	Rizki Anwar
Nomor Petugas Investigator	170401060
Email Investigator	170401060@student.umri.ac.id
Petunjuk Investigator	Melakukan akuisisi bukti digital pada perangkat <i>smartphone</i> pada aplikasi <i>instant messenger</i> BIP
DESKRIPSI BUKTI	
Tipe Barang Bukti	<i>Smartphone</i>
Nama Perangkat	Oppo
Nama Pemilik	Samson

Peralatan Yang Digunakan	1. Satu unit laptop 2. Kabel USB 3. FTK Imager 4. Mobiledit Forensic 5. Oxygen Forensic SQLite Viewer
Nomor Model	Oppo A33
Kondisi	Bagus
IMEI	861485033878837
Catatan	Melakukan pengangkatan bukti digital pada <i>smartphone</i>
Temuan Barang Bukti	1. Temuan data <i>chatting</i> yang dihapus pada perangkat <i>smartphone</i> pelaku 2. Temuan gambar pada perangkat <i>smartphone</i> pelaku
Deskripsi Kasus	Tindak <i>cyberbullying</i> melalui aplikasi BIP Messenger

Berdasarkan pada tabel 3.2 polisi mendapatkan laporan tindak cyberbullying melalui aplikasi BIP Messenger pada tanggal Rabu, 16 Maret 2022, lalu pihak penyidik melakukan penyidikan dan menahan barang bukti perangkat *smartphone* milik pelaku. Untuk mendapatkan bukti digital setelah melakukan pengecekan pelaku menghilangkan barang bukti lalu pihak kepolisian menyerahkan *smartphone* pelaku kepada investigator. Untuk melakukan proses forensic mobile guna mendapatkan bukti digital, temuan bukti digital pada perangkat *smartphone* seperti data *chatting*, dan gambar barang bukti temuan yang telah didapatkan dapat menjadikan barang bukti yang sah untuk dipersidangan

4. KESIMPULAN

Berdasarkan hasil dari penelitian yang telah dilakukan dapat dibuat kesimpulan bahwa metode national institute of justice dalam proses identifikasi barang bukti dari aplikasi BIP Messenger pada *smartphone* android berhasil didapatkan dan semua tools yang digunakan berjalan baik dan tools yang digunakan dapat memenuhi kebutuhan tools lainnya. Kemudian proses mendapatkan bukti digital pesan yang terhapus dari aplikasi pesan instan “BIP” berhasil didapatkan dengan cara melakukan pengangkatan barang bukti dari *smartphone* pelaku.

DAFTAR PUSTAKA

- [1] Bhosale, S. T., Patil, T., & Patil, P. (2015). SQLite: Light Database System. *International Journal of Computer Science and Mobile Computing*, 44(4), 882–885.
- [2] D. Mualfah, & Riadi, I. (2017). Network Forensics For Detecting Flooding Attack On Web Server. *International Journal of Computer Science and Information Security*, 15(2), 430–436.
- [3] Fauzan, A., Riadi, I., & Fadlil, A. (2017). Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime. *Annual Research Seminar (ARS)*, 2(1), 159–163. <http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752>
- [4] Iqbal, M. T. (2018). Alat Bukti Elektronik Dalam Hukum Acara Di Indonesia. *Jurnal Ius Civile*, 2(1), 89–97.
- [5] Madiyanto, S., Mubarak, H., & Widiyasono, N. (2017). Mobile Forensics Investigation Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS. *Jurnal Rekayasa Sistem & Industri (JRSI)*, 4(01), 93–98. <https://doi.org/10.25124/jrsi.v4i01.149>
- [6] Muhammad Kukuh Tri Haryanto. (2018). Analisa Forensics Terhadap Database Sqlite pada Aplikasi IMO Berbasis Android. Universitas Islam Indonesia.
- [7] Nazara, K. (2019). Analisis Perilaku Cyberbullying Remaja di Jejaring Sosial Instagram di Sekolah Madrasah Aliyah Islamiyah Sunggal. In Universitas Medan Area. Universitas Medan Area.
- [8] Prasetyo, B. Y., & Riadi, I. (2021). Investigat ion Cyberbullying on Kik Messenger using National Institute of Standards Technology Method. *International Journal of Computer Applications*, 174(17), 34–41. <https://doi.org/10.5120/ijca2021921060>
- [9] Putra, I. P. D. I., & Suhartana, I. K. G. (2021). Cyberbullying Analysis on WhatsApp Messenger Using the National Institute of Justice (NIJ) Method. *JELIKU (Jurnal Elektronik Ilmu Komputer Udayana)*, 9(4), 501. <https://doi.org/10.24843/jlk.2021.v09.i04.p07>
- [10] Soni, Prayudi, Y., & Sugiantoro, B. (2017). Teknik Akuisisi Virtualisasi Server Menggunakan Metode Live Forensic. *Teknomatika*, 9(2).
- [11] Riadi, I., Sunardi, S., & Sahiruddin, S. (2019). Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ). *Jurnal Rekayasa Teknologi Informasi (JURTI)*, 3(1), 87. <https://doi.org/10.30872/jurti.v3i1.2292>
- [12] 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)*, 3(1), 70–82. <https://doi.org/10.21831/elinvo.v3i1.19308>
- [13] Riadi, I., Yudhana, A., & Barra, M. Al. (2021). Forensik Mobile pada Layanan Media Sosial LinkedIn. *JISKA (Jurnal Informatika Sunan Kalijaga)*, 6(1), 9–20. <https://doi.org/10.14421/jiska.2021.61-02>
- [14] Riadi, I., Yudhana, A., & Putra, M. C. F. (2017). Analisis Recovery Bukti Digital Instagram Messengers Menggunakan Metode National Institute of Standards and Technology (NIST). *Seminar Nasional Teknologi Informasi Dan Komunikasi - SEMANTIKOM*, 161–166.
- [15] Riadi, I., Yudhana, A., & Putra, M. C. F. (2018). Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ). *Jurnal Teknik Informatika Dan Sistem Informasi*, 4(2), 219–227.
- [16] Rohman, I. F., Widiyasono, N., & Gunawan, R. (2019). Simulasi Analisis Bukti Digital Aplikasi Skype Berbasis Android menggunakan NIST SP 800-101 R1. *Jurnal Sustainable: Jurnal Hasil Penelitian Dan Industri Terapan*, 08(01).
- [17] Ruuhwan, R., Riadi, I., & Prayudi, Y. (2016). Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, 2(1). <https://doi.org/10.26418/jp.v2i1.14369>
- [18] Soni, Ramadhan, E., & Mualfah, D. (2021). Investigasi Bukti Digital Aplikasi WeChat Menggunakan Framework Integrated Digital Forensics Proses Model (IDFPM) Berbasis SNI 27037 : 2014. *Jurnal INTEK*, 4(1).
- [19] Widiandana, P., Riadi, I., & Sunardi. (2020). Implementasi Metode Jaccard pada Analisis Investigasi Cyberbullying WhatsApp Messenger Menggunakan Kerangka Kerja National Institute of Standards and Technology. *JURNAL RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 4(6), 1046–1051.

- [20] Soni, S., Hafid, A., & Sudyana, D. (2019). Analysis of Security Awareness in using Technology and Social Media at Muhammadiyah University of Riau. 177(18), 20–25.
- [21] Yudhana, A., Riadi, I., & Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. *It Journal Research and Development*, 3(1), 13–21. [https://doi.org/10.25299/itjrd.2018.vol3\(1\).1658](https://doi.org/10.25299/itjrd.2018.vol3(1).1658)
- [22] Yudhana, A., Umar, R., & Ahmadi, A. (2018). Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ). *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi*, 4(1), 8. <https://doi.org/10.24014/coreit.v4i1.5803>
- [23] Fitriatus, N.S. (2021). "Mengenal Aplikasi BiP yang Dilirik Pengguna WhatsApp Selain Telegram". <https://www.kompas.com/tren/read/2021/01/20/170500665/mengenal-aplikasi-bip-yang-dilirik-pengguna-whatsapp-selain-telegram?page=all>. Diakses pada tanggal 10 Januari 2022.
- [24] Purnama, E.P. (2021). "Khawatir Kebijakan WhatsApp, Masyarakat Gunakan Aplikasi BIP". [https://www.republika.co.id/berita/qn7jqc484/khaw atir- kebijakan-whatsapp-masyarakat-gunakan-aplikasi-bip](https://www.republika.co.id/berita/qn7jqc484/khaw%20atir-kebijakan-whatsapp-masyarakat-gunakan-aplikasi-bip). Diakses pada tanggal 22 Maret 2022.
- [25] Soni, Prayudi, Y., Sugiantoro, B., Sudyana, D., & Mukhtar, H. (2019). Server Virtualization Acquisition Using Live Forensics Method. 190, 18–23. <https://doi.org/10.2991/iccelst-st-19.2019.4>
- [26] Sudyana, D., Putra, R. T., & Soni, S. (2019). Digital Forensics Investigation on Proxmox Server Virtualization Using SNI 27037:2014. *Sinkron*, 3(2), 67–72. <https://doi.org/10.33395/sinkron.v3i2.10029>