Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 170-178
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Akuisisi Bukti Digital Aplikasi *Viber* Menggunakan Metode *National Institute of Standards Technology* (NIST)

Muhammad Irwan Syahib[1], Imam Riadi[2], Rusydi Umar[3]
[1,3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta, Indonesia
[2]Program Studi Sistem Informasi, Universitas Ahmad Dahlan Yogyakarta, Indonesia
Jalan Prof. Dr. Soepomo, S.H., Janturan, Warungboto, Umbulharjo, Yogyakarta, Indonesia
Muhammadirwansyahib13@gmail.com, Imam.riadi@si.uad.ac.id, rusydi@mti.uad.ac.id

Abstract

The rapid development of mobile technology today is directly proportional to the development of mobile applications in it. Making it easier for people to choose and use the application as they want. This has resulted in misuse of negative things, ranging from human trafficking, drug trafficking, as well as online prostitution business. Viber is an Instant Messenger application that makes it easy for users. This application can be used to send messages, call, send photos, audio and video to others. This application has been used by 260 million people worldwide. This is the basis of research to acquire digital evidence in Viber applications. Data obtained after acquiring based on the work steps of NIST are the accounts of the perpetrators, contacts targeted by the perpetrators, call history, text messages, picture messages and videos.

Keywords*: Acquiring, Forensic, Mobile, Instan Mesengger, Viber.*

Abstrak

Pesatnya perkembangan teknologi mobile saat ini berbanding lurus dengan perkembangan aplikasi mobile didalamnya. Sehingga memudahkan orang-orang untuk memilih dan menggunakan aplikasi sesuai yang mereka inginkan. Hal ini mengakibatkan penyalahgunaan untuk hal-hal negative, mulai dari perdagangan manusia, pengedaran narkoba, serta bisnis prostitusi online. Viber adalah salah satu aplikasi Instant Messenger yang memudahkan penggunanya. Aplikasi ini dapat digunakan untuk berkirim pesan, menelepon, mengirim foto, audio maupun video kepada sesama. Aplikasi ini telah digunakan 260 juta orang di seluruh dunia. Hal ini yang menjadikan dasar penelitian untuk mengakuisisi bukti-bukti digital pada aplikasi Viber. Data yang berhasil didapatkan setelah mengakuisisi berdasarkan langkah kerja NIST adalah akun pelaku, kontak yang dijadikan target oleh pelaku, riwayat panggilan, teks percakapan, pesan gambar dan video.

Kata kunci: *Akuisisi, Forensik, Mobile, Instan Mesengger, Viber.*

1. PENDAHULUAN

Perkembangan teknologi lima tahun terakhir sangat pesat, begitu juga perkembangan smartphone yang selalu mengalami kemajuan dari segi sistem operasi, fitur, spesifikasi, dan aplikasi [1]. Data Statista di tahun 2019 menunjukkan sebanyak 95,2 juta *user* internet di Indonesia tumbuh pada tahun 2018, dari 84 juta pengguna tahun 2017 yaitu mencapai 13,3%. Tahun selanjutnya diperkirakan pertumbuhan *user* internet di Indonesia diprediksi akan semakin pesat pada periode 2018-2023 dengan rata-rata tumbuh sebesar 10,2%. Pada tahun 2019 jumlah *user* internet di Indonesia diperkirakan tumbuh sebanyak 12,6% dibandingkan tahun 2018 sekitar 107,2 juta *user*[2].

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 170-178
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Pertumbuhan pengguna internet di indonesia berbandingan lurus dengan kejahatan siber. Menurut data Kepolisian Republik Indonesia, Pada tahun 2016 kasus *cybercrime* yang ditangani kepolisian adalah 4.931 kasus, pada tahun 2017 meningkat sebanyak 5.061 kasus. Pada tahun 2016 Kepolisian Republik Indonesia penyelesaian sebanyak 1.119 kasus kejahatan *cyber*, dan 1.369 kasus di tahun 2017 [3]. Kasus kejahatan siber di Indonesia sangat banyak, dan yang terbanyak adalah melalui aplikasi *Instant Messenger*. Sebanyak 3.325 kasus kejahatan siber yang telah Polri tangani sejak 2017. Sementara pada 2016, ada 1.829 kasus yang telah ditangani Polri. Kasus kejahatan ini meningkat terus disetiap tahunya, hingga pada tahun 2019 diketahui sebnayak 3.130 laporan kasus kejahatan siber sepanjang Januari-Juli [4]. Kasus-kasus kejahatan siber ini sangat potensial terjadi pada aplikasi *Instant Messenger* apa saja, selama aplikasi tersebut menyediakan fitur untuk mengirim pesan taks, dokumen, gambar, video dan audio [5]. Salah satu aplikasi *Instant Messenger* yang sangat berpotensi dipergunakan untuk kejahatan siber adalah *Viber*. Aplikasi yang dikembangkan oleh *Viber* Media Inc. di tahun 2010 ini dapat dengan mudah digunakan untuk mengirim pesan, menelepon, mengirim foto, maupun pesan video kepada sesama penggunanya. Aktivitas positif maupun *negative* sangat mudah dilakukan pada aplikasi ini karena sangat *simple* dalam penggunaannya. Aplikasi ini telah digunakan 260 juta orang di seluruh dunia [6]. Berdasarkan pernyataan di atas, penelitian ini akan dilakukan proses akuisisi bukti-bukti digital pada aplikasi *Viber* berdasarkan langkah analisis dari *National Institute of Standards Technology* (NIST).

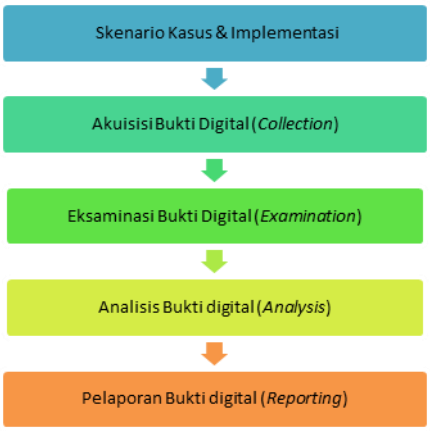
2. METODOLOGI PENELITIAN

Langkah kerja forensik pada penelitian ini mengimplementasikan langkah kerja *forensics* dari *National Institute of Standards Technology* (NIST) [7]. Langkah kerja forensik ini digunakan untuk menjabarkan tahapan-tahapan *forensics* yang akan dilakukan dan dapat diketahui alur-alur penelitian secara terstruktur, dan dapat menjadi acuan dalam menyelesaikan masalah-masalah yang ada[8]. Langkah forensik tersebut dapat dilihat pada Gambar 1.

Gambar 1. Alur Metode NIST

Bukti digital yang digunakan pada penelitian ini peroleh dari hasil scenario kasus dan implementasi pada tahapan awal penelitian [9]. Adapun tahapan forensik mengacu pada 4 tahap standar langkah kerja forensik dari NIST [10]. Dari metode dan langkah kerja tersebut pada penelitian ini terdibagi menjadi 5 tahap penelitian, dan dapat dilihat pada Gambar 2.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 170-178
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti



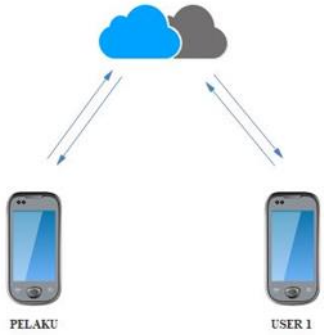
Gambar 2. Tahapan Penelitian.

3. HASIL DAN PEMBAHASAN

Proses akuisisi ini diawali dari menyiapkan 2 *smartphone* untuk membuat percakapan transaksi kemudian percakapan pada *smartphone* pelaku tersebut di hapus. Selanjutkan dimulai proses akuisisi pada *smartphone* pelaku untuk menemukan percakapan yang telah dihapus tersebut yang mengacu pada 4 tahap standar langkah kerja forensik dari NIST.

3.1. Skenario Kasus dan Implementasi

Kasus kejahatan dalam penelitian ini dilakukan berdasarkan skenario kasus dengan tujuan untuk mensimulasikan kasus kejahatan agar didapatkan bukti digital berupa percakapan yang telah dihapus pada aplikasi *Viber*. Pada penelitian ini, skenario kasus yang dibuat berupa mengirim pesan percakapan dari pelaku ke target, diantaranya berupa pesan taks, gambar dan video. Skenario kasus tersebut dapat dilihat pada Gambar 3.



Gambar 3. Skenario Kasus

Smartphone pelaku yang digunakan dalam penelitian ini adalah adroid Evercros B75 dengan *system* operasi android 5.1 (lollipop). *Smartphone* yang digunakan telah di *rooting* sebelumnya agar dapat membuka semua akses pada *smartphone* android yang ingin diakuisisi. Barang bukti berupa *smartphone* pelaku dapat dilihat pada gambar 4.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 170-178
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

SIM	Dual SIM
Jaringan	2G, 3G HSDPA, 4G LTE
Layar	IPS 5 inchi 1280 x 720 piksel
Memori	16 GB, Slot micro SD hingga 32 GB
RAM	2 GB
Sistem operasi	Android Lollipop 5.1
Prosesor	Quadcore 64 bit 1.0 GHz

Gambar 4. *Smartphone* Barang Bukti Pelaku

3.2. Akusisi Bukti Digital (*Collection*)

Tahapan *Collection* ini adalah melakukan pengumpulan bukti fisik, mengumpulkan data, dan mendokumentasikan bukti fisik pelaku dalam bentuk *smartphone* seperti yang ditunjukkan pada Gambar 5.

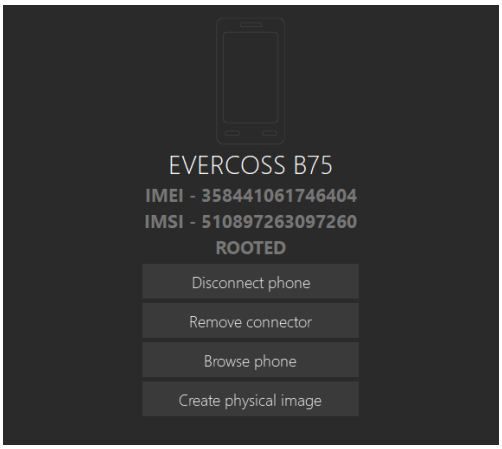
Gambar 5. *Smartphone* Barang Bukti Pelaku

Barang bukti tersebut berupa *smartphone* dengan sistem operasi Android yang telah terinstal aplikasi *viber* yang merupakan alat komunikasi yang digunakan untuk percakapan antara pelaku dan korban. Data yang terdapat pada *smartphone* Android pelaku akan diambil dengan cara dikloning untuk mehindari perubahan data yang akan menjadi barang bukti digital. Untuk melakukan kloning data akan menggunakan aplikasi Mobiledit forensik.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 170-178
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

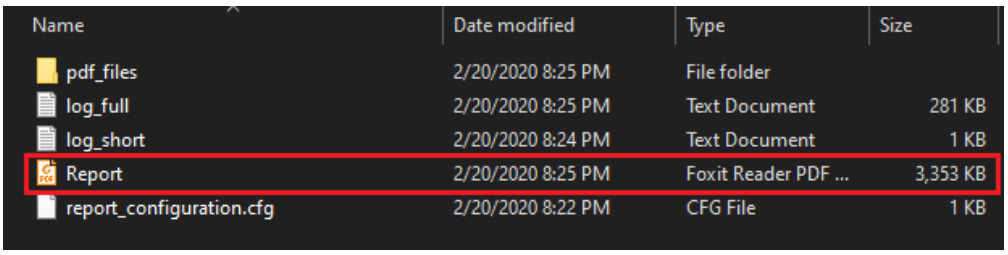
3.3. Examinasi Bukti Digital

Tahap examinasi data yang ada pada barang bukti digital dari percakapan yang telah dihapus antara pelaku dan korban dapat terlaksana dengan melakukan proses akuisisi data-data yang ada pada *smartphone* pelaku tersebut. Proses melakukan akuisisi data yang ada pada *smartphone* Android pelaku dapat dihubungkan ke PC menggunakan kabel data agar terhubung ke apikasi Mobiledit forensik. Tahapan pertama pada proses akuisisi data menggunakan aplikasi Mobiledit forensik *smartphone* Evercros B75 dapat dilihat pada Gambar 6.



Gambar 6. Tahapan Pertama Proses Akuisisi

Data-data yang didapatkan dari proses akuisisi terdapat berbagai macam tipe data dari memori penyimpanan *internal* maupun *eksternal* pada *smartphone* Evercros B75. Hasil dari proses akuisisi di *report* menggunakan format .pdf. Hasil proses akuisisi menggunakan Mobiledit forensik dapat membaca *report* aplikasi *Viber*. Hasil akuisisi dapat dilihat pada Gambar 7.

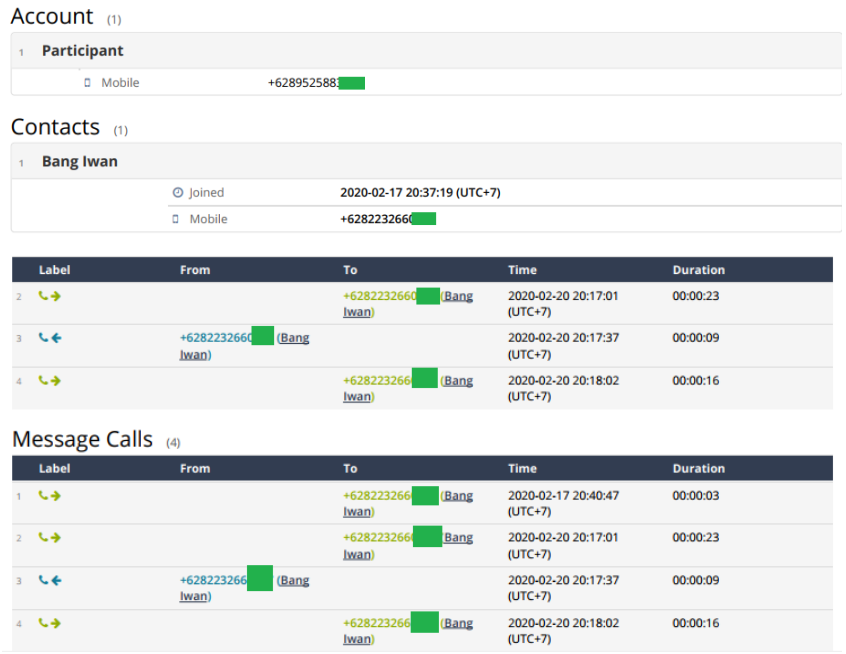


Gambar 7. Hasil Proses Akuisisi

3.4. Analisis Bukti Digital

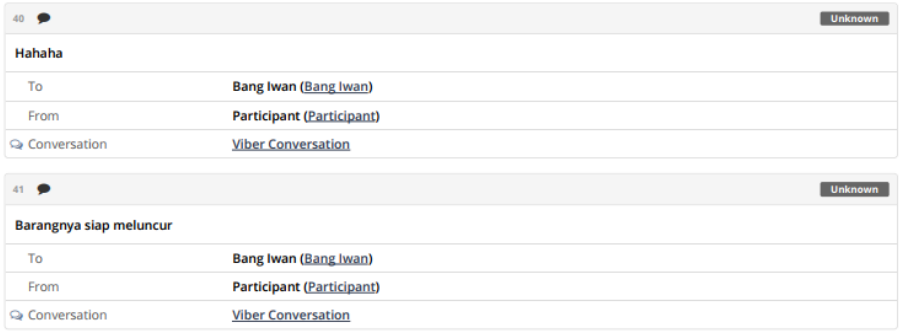
Tahap analisis bukti digital ini adalah melakukan analisis terhadap hasil proses pengambilan data–data dari barang bukti yang telah didapat didalam aplikasi *Viber* pada *smartphone* Evercros B75 yang digunakan oleh pelaku. Data yang dibutuhkan yakni data akun, kontak, pesan taks, riwayat panggilan, gambar dan video. Pada proses analisis menggunakan Mobiledit forensik, berhasil ditemukan beberapa barang bukti.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 170-178
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti



Gambar 8. Bukti Akun, Kontak, dan Riwayat Panggilan

Pada Gambar 8 adalah bukti akun, kontak, dan riwayat panggilan pelaku yang di dapat. Dari hasil analisis dapat diperoleh barang bukti berupa nomor *handphone* pelaku yang dipakai untuk registrasi akun *viber* serta kontak yang dijadikan target untuk melakukan transaksi. Selain itu didapat riwayat panggilan beserta waktu kapan melakukan panggilan dan durasi panggilan berlangsung antara pelaku dan target.

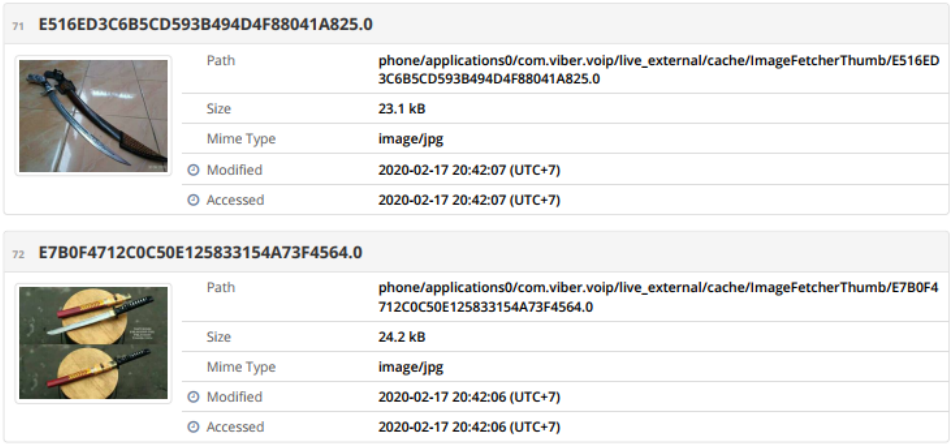


Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 170-178
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Participant (Participant)	Yang hitam boleh bang	(no message time)
Participant (Participant)	Oke	(no message time)
Participant (Participant)		(no message time)
Participant (Participant)	Apaan tuh	(no message time)
Participant (Participant)	Wkwkwk	(no message time)
Participant (Participant)	Canda bang	(no message time)
Participant (Participant)	Hahaha	(no message time)
Participant (Participant)	Barangnya siap meluncur	(no message time)
Participant (Participant)	Oke	(no message time)
Participant (Participant)	Di tunggu	(no message time)
Participant (Participant)	Jangan sampai ketahuan	(no message time)
Participant (Participant)	Siap	(no message time)

Gambar 9. Pesan Teks Yang Telah Di Hapus

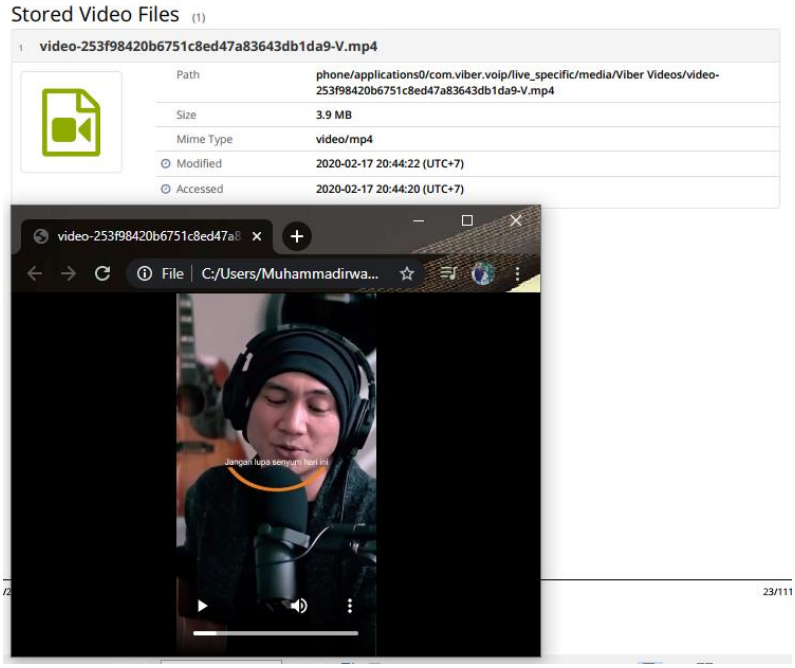
Pada Gambar 9 menunjukkan hasil text percakapan antara pelaku dan target yang telah di hapus di *smartphone* pelaku, dimana pelaku mencoba menawarkan barang yang ingin dijual serta target yang mengorder barang tersebut.



Gambar 10. Bukti Pesan Gambar Yang Dihapus

Pada Gambar 10 menunjukkan hasil pesan gambar antara pelaku dan target. Selain itu didapat pula waktu pesan gambar itu dikirim ke target.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 170-178
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti



Gambar 11. Bukti Video Yang Dihapus

Pada Gambar 11 menunjukkan hasil pesan video yang dikirim pelaku ke target. Terlihat pula ukuran video dan waktu video tersebut dikirim.

3.5. Laporan Bukti Digital

Pada tahap laporan adalah *reporting* data-data yang telah didapatkan baik yang berhasil ataupun yang gagal di akuisisi yang merupakan data hasil analisis yang dilakukan menggunakan tool Mobiledit forensik. Data yang telah berhasil didapatkan akan menjadi barang bukti digital dari tindak kejahatan yang dilakukan oleh pelaku. Data-data bukti digital yang berhasil ditemukan dapat dilihat pada Tabel 1.

Tabel 1. Bukti digital yang berhasil didapat

Data	Berhasil (Ya/Tidak)
Akun & Kontak	Ya
Riwayat panggilan	Ya
Pesan teks	Ya
Foto	Ya
Video	Ya

4. SIMPULAN

Berdasarkan proses yang telah dilakukan dalam penelitian ini, yang dimulai dari membuat skenario percakapan dengan mengirim berbagai macam jenis yaitu pesan teks, pesan video dan gambar dan selanjutnya pesan percakapan tersebut dihapus. Kemudian melakukan proses *rooting* agar

memiliki akses *full* ke perangkat android. Setelah itu melakukan infestigasi dan analisis pada barang bukti berupa *smartphone* pelaku menggunakan tool Mobiledit forensik berdasarkan tahapan metode *National Institute of Standards Technology* (NIST). Data berupa pesan percakapan yang telah dihapus oleh pelaku beserta akun dan riwayat panggilan berhasil didapat.

DAFTAR PUSTAKA

[1] Z. Akbar, B. Nugraha, and M. Alaydrus, "Whatsapp Forensics Pada Android Smartphone : a Survey," *Sinergi*, vol. 20, no. 3, p. 207, 2016, doi: 10.22441/sinergi.2016.3.006.

[2] D. H. Jayani, "Berapa Pengguna Internet di Indonesia?," 2019. [Online]. Available: https://databoks.katadata.co.id/datapublish/2019/09/09/berapa-pengguna-internet-di-indonesia.

[3] M. I. Syahib, I. Riadi, and R. Umar, "Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan," *Semin. Nas. Inform. 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 Novemb. 2018*, vol. 2018, no. November, p. 134, 2018.

[4] E. Chintia, R. Nadiah, H. N. Ramadhani, Z. F. Haedar, A. Febriansyah, and N. A. Rakhmawati S.Kom., M.Sc.Eng, "Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya," *J. Inf. Eng. Educ. Technol.*, vol. 2, no. 2, p. 65, 2019, doi: 10.26740/jieet.v2n2.p65-69.

[5] R. A. K. N. Bintang, R. Umar, and U. Yudhana, "Perancangan perbandingan live forensics pada keamanan media sosial Instagram, Facebook dan Twitter di Windows 10," *Pros. SNST ke-9 Tahun 2018 Fak. Tek. Univ. Wahid Hasyim*, pp. 125–128, 2018.

[6] Digo, "7 Aplikasi Chat Populer di Indonesia dan 17 Alternatif lainnya," 2020. [Online]. Available: https://bukugue.com/aplikasi-chatting/.

[7] Mustafa, I. Riadi, and R. Umar, "Rancangan Investigasi Forensik E-mail dengan Metode National Institute of Standards and Technology (NIST)," *Pros. SNST*, vol. 9, pp. 121–124, 2018.

[8] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3991–4003, 2018, doi: 10.11591/ijece.v8i5.pp3991-4003.

[9] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)," vol. 4, pp. 219–227, 2018.

[10] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.