ANALISIS DAN INVESTIGASI FORENSIK DIGITAL LIVE MEMORY UNTUK DETEKSI TINGKAH LAKU AGRESI PADA APLIKASI WHATSAPP

Irwansyah Saputra[1], Muhamad Nauval Azhar[2]

STMIK Nusa Mandiri[1], Universitas Kebangsaan[2]
14002085@nusamandiri.ac.id

ABSTRAK

Peningkatan penggunaan internet menciptakan bentuk baru dari serangan yang disebut dengan *cyberagression*. *Cyberagression* menjadi masalah berbahaya karena memiliki dampak yang sangat serius terhadap psikis korban. Fokus penelitian ini adalah fenomena *cyberagression* yang terjadi pada aplikasi olah pesan *WhatsApp Messenger*. Proses pengambilan data pada aplikasi tersebut sulit dilakukan karena adanya fitur *end to end encryption* atau *E2EE*, yaitu setiap pesan yang dikirim langsung dienkripsi secara aman dan hanya bisa dibuka oleh pengirim dan penerima, sehingga harus dilakukan forensik digital untuk mengatasi hal tersebut. Riset ini dimulai dengan proses pengambilan data menggunakan *softwareFTK Imager* dengan metode forensik digital *live memory*. Selanjutnya data diekstraksi kembali dan pengguna *WhatsApp Messenger* dieksplorasi karakteristiknya sesuai dengan konten obrolan dan diberi label menggunakan metode *crowdsourcing*. Kemudian memanfaatkan atribut yang diolah dengan metode mesin pembelajar untuk mendeteksi secara otomatis tingkah laku agresi pada pengguna *WhatsApp Messenger*.
Kata kunci: *cyberagression*, *WhatsApp Messenger*, mesin pembelajar, forensik digital

ABSTRACT

Increased use of the internet creates a new form of attack called cyberagression. Cyberagression becomes a dangerous problem because it has a very serious impact on the victim's psychic. The focus of this research is the cyberagression phenomenon that occurs in the Messaging Messages WhatsAppmessaging application. The data retrieval process in the application is difficult because of the end to end encryption or E2EE feature, ie every message sent is directly encrypted safely and can only be opened by the sender and receiver, so digital forensics has to be done to cover it. This research begins with the data retrieval process using FTK Imager software with digital forensic live memory method. Further data is extracted back and the WhatsApp Messenger user explored its characteristics according to the chat content and labeled using the crowdourcing method. Then take advantage of attributes that are processed by machine learner method to automatically detect aggression behavior on WhatsApp Messenger user.
Keyword: *cyberagression, WhatsApp Messenger, machine learning, digital forensic*

PENDAHULUAN

Pengguna internet di Indonesia saat ini lebih dari 132 juta jiwa[1]. Hal ini berbanding lurus dengan pengguna *smartphone* yang diperkirakan akan meningkat lebih dari 100% dibanding tahun sebelumnya[2]. Aplikasi olah pesan pada *smartphone* seperti *WhatsApp Messenger* pun mengalami peningkatan pengguna yang signifikan yaitu 35,8 juta pengguna dan menjadi aplikasi olah pesan terpopuler di Indonesia[3]. Peningkatan penggunaan aplikasi ini menciptakan bentuk baru dari serangan yang disebut dengan *cyberagression*. *Cyberagression* menjadi masalah berbahaya karena memiliki dampak yang sangat serius terhadap psikis korban[4]. UNICEF merilis laporan tahun 2017 bahwa terdapat 40% anak Indonesia mengalami peristiwa *bully*. Selanjutnya terdapat 32% anak yang melaporkan mendapat kekerasan fisik[5]. Sebagian peneliti bidang ilmu psikologi mengatakan bahwa *bully* termasuk atau memiliki kesamaan perbuatan dengan agresi[6]. Sebagian peneliti lainnya mengatakan bahwa *bullying* adalah bagian dari perilaku agresi[7].*Cyberagression* pada *WhatsApp*rentan dilakukan karena semakin

banyaknya pengguna aplikasi tersebut yang berasal dari berbagai usia[8]. Penyebabnya adalah pembatasan usia minimal 16 tahun untuk pengguna *WhatsApp*tidak ditampilkan saat mendaftardan faktanya *WhatsApp*hanya memerlukan nomor telepon aktif untuk membuat akun[9].

Fitur yang dimiliki *WhatsApp*salah satunya adalah *end to end encryption* atau E2EE, yaitu setiap pesan yang dikirim langsung dienkripsi secara aman dan hanya dapat dibuka oleh pengirim dan penerima saja. Artinya, pesan, foto, video, pesan suara, dokumen, pembaruan status dan panggilan telepon hanya dapat dilihat oleh pengirim dan penerima saja. Bahkan *WhatsApp*pun mengklaim tidak dapat melihatnya. Setiap pesan tersebut diamankan menggunakan kunci spesial, hanya penerima dan pengirim saja yang memiliki kunci spesial tersebut. Fitur ini berjalan secara otomatis, pengguna tidak perlu mengaktifkan pengaturan apapun untuk mengaktifkan fitur ini[10]. Selain itu, basis data penyimpanan pesan *WhatsApp*dienkripsi menggunakan encrypt12 yang menyulitkan untuk dibuka dengan metode sederhana sehingga dibutuhkan perangkat lunak tambahan untuk membuka enkripsi basis data tersebut. Forensik digital diperlukan saat hendak mengenkripsi basis data agar keaslian data dan metadatanya terjaga. Perangkat lunak yang dipakai untuk melakukan forensik digital adalah *FTK Imager*.

Riset sebelumnya membahas tentang forensik digital pada *WhatsApp* menggunakan teknik internet *protocol* dengan *tool Wireshark*. Teknik ini bertujuan untuk mendapatkan informasi ketika pengguna sedang melakukan interaksi atau komunikasi dengan orang lain. Kasus yang digunakan pada riset ini adalah mengambil informasi dari dua buah telepon selular dan mengujinya menggunakan teknik internet protokol. Informasi yang didapat adalah berupa pesan yang dikirim, log panggilan, *timestamp* dan atribut lainnya[11].

Gambar 1. Hasil forensik digital menggunakan *tool* Wireshark

Riset kedua melakukan analisis forensik digital pada *WhatsApp*dan *LineMessenger* sebagai rujukan dalam menyediakan barang bukti yang kuat dan valid di Indonesia. Teknik yang digunakan untuk forensik digital pada riset ini adalah *live memory* basis data *WhatsApp*. Tools yang digunakan adalah *FTK Imager* dan *SQLiteBrowser*. Hasil yang didapat yaitu aplikasi *WhatsApp*merupakan aplikasi yang dapat menjadi rujukan dalam forensik digital di Indonesia. Sedangkan Line Messenger merupakan aplikasi yang lebih aman karena sulit dilakukan forensik digital pada aplikasi tersebut[12]. Riset lainnya melakukan deteksi agresi dan *bully* pada twitter berdasarkan fitur konten dan penyematan jaringan profil. Riset ini berfokus pada fenomena yang terjadi di media jejaring sosial *Twitter*. Media jejaring sosial ini memiliki beberapa hambatan untuk mendeteksi prilaku negatif yaitu karena *tweet* yang singkat, banyaknya *spam* dan tata bahasa rumit yang membuat lebih sulit pemprosesan mesin untuk memproses bahasa alami dan mengekstrak atribut berbasis teks dan mengkarakterisasi interaksi pengguna Twitter. Peneliti mengeksplorasi karakteristik pengguna Twitter sehubungan dengan konten dan penyematan jaringan seperti *following*&*follower* dan memanfaatkan

atribut dengan *machine learning* klasifikasi untuk mendeteksi secara otomatis pengguna *Twitter* aggressor dan pengganggu[13].

Fokus penelitian ini adalah mendeteksi *cyberagression* yang terjadi pada aplikasi olah pesan *WhatsApp Messenger*dengan teknik digital *live memory*. *FTK Imager* digunakan sebagai forensik digital untuk menjaga keaslian basis data dan metadatanya. Setelah dilakukan forensik digital, basis data tersebut diekstraksi untuk mendapatkan konten dan atribut yang terdapat di dalamnya. Konten dan atribut yang dimaksud adalah berupa pesan teks. Setelah data didapatkan, pengguna *WhatsApp Messenger* dieksplorasi karakteristiknya sesuai dengan atribut yang terdapat pada konten obrolan dan diberi *label/class*menggunakan metode *crowdsourcing*.

Kemudian memanfaatkan atribut tersebut dengan metode *machine learning* klasifikasi untuk mendeteksi secara otomatis tingkah laku agresi pada *WhatsApp Messenger*.

METODE

Metode penelitian yang digunakan pada riset ini menggunakan model *Cross-Standard Industry for Data Mining* (CRISP-DM) yang distandarisasi pendekatan untuk data mining mulai tahun 1999 hasil kerja sama perusahaan otomotif Daimler-Benz, penyedia asuransi OHRA, produsen perangkat keras dan perangkat lunak NCR Corp dan statistik pembuat software SPSS, Inc. Metode penelitan CRISP-DM terdiri dari 6 langkah atau fase[14], yaitu *Business Understanding*, *Data Understanding,Data Preparation, Modeling, Evaluation, Deployment.*

Business Understanding

Data mining dapat menjawab kasus pada eksperimen ini yaitu melalui pendekatan algoritma klasifikasi *NaïveBayes* untuk mendeteksi konten agresi pada *WhatsApp Messenger*.

Data Understanding

Data merupakan bagian penting untuk melakukan tahapan selanjutnya pada siklus sistem. Pemahaman terhadap data dilakukan dimulai dari awal yaitu menganalisis proses pengambilan data, pengetahuan awal dan kemudian mengevaluasi kualitas dari data tersebut. Selanjutnya data diberikan *label* untuk tahap klasifikasi pada *machine learning*.

Data Preparation

Dataset yang digunakan dalam penelitian ini menggunakan basis data obrolan pada *WhatsApp*. Selanjutnya data tersebut diberikan pelabelan menggunakan metode *crowdsourcing* untuk mendapatkan *class* agresi atau normal. Terakhir, data tersebut diklasifikasikan menggunakan algoritma Naïve Bayes untuk dilatih.

Modelling

Model pendekatan riset yang digunakan dapat dilihat pada gambar 2.

Gambar 2. Model Pendekatan Riset

Preservation merupakan tahap awal dari riset ini. Tahap *preservation* melibatkan proses pencarian, pengakuan, dokumentasi dan pengumpulan barang bukti berbasis elektronik. Barang bukti tersebut yaitu sebuah *smartphone* Redmi Note 4.

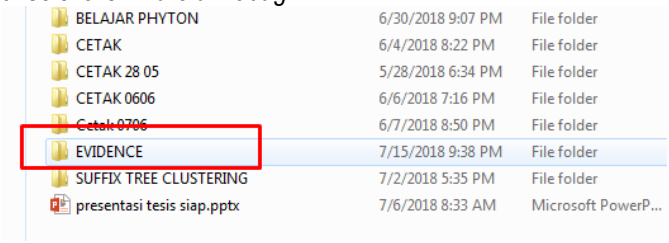
Tabel 2. Data Barang Bukti

No	Evidence	Hardware specification	Software
1	Evidence 1	*Smartphone* Xiaomi Redmi Note 4	Android 7.0 Nougat.

	WhatsApp 2.18.105

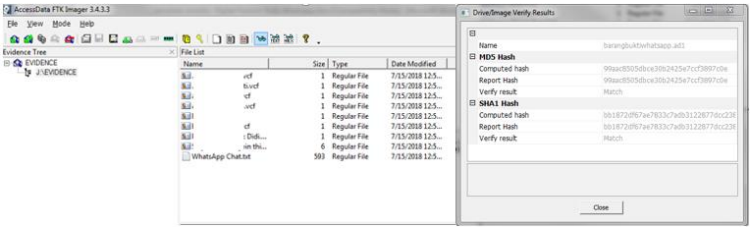
Acquisition merupakan proses yang dilakukan untuk mendapatkan informasi dari *smartphone* atau media lainnya yang terkait. Proses pencarian informasi dilakukan seperti mengidentifikasi perangkat *smartphone*, akusisi memori *smartphone* internal dan eksternal. Kemudian *smartphone* diidentifikasi melalui software *Android Debug Bridge* (ADB) selanjutnya dihubungkan ke *Personal Computer* (PC) menggunakan kabel data *microUSB* 2.0 dengan memilih *transfer file for USB*. Gambar 3 menunjukkan folder yang berisi barang bukti basis data *WhatsApp*.

Folder tersebut dipindahkan ke PC untuk dilakukan forensik digital dan pelabelan pada obrolan.



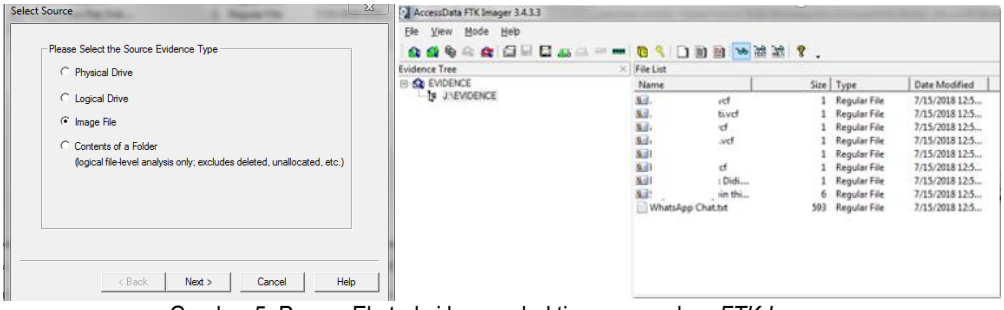
Gambar 3. Folder berisi barang bukti pada kartu memori*smartphone* Redmi Note 4

Alat yang digunakan untuk melakukan akuisi data *smartphone* adalah *FTK Imager*. *FTK Imager* berfungsi untuk *recovery* dan menjaga metadata pada data terkait. Semua hasil data yang diperoleh akan diarsipkan ke dalam satu folder pada PC agar lebih mudah saat proses pemeriksaan analisis data. Keterangan lebih lanjut mengenai akuisisi data menggunakan *FTK Imager* dapat dilihat pada gambar 4.Daftar kontak pada gambar disamarkan untuk menjaga privasi data pihak terkait.



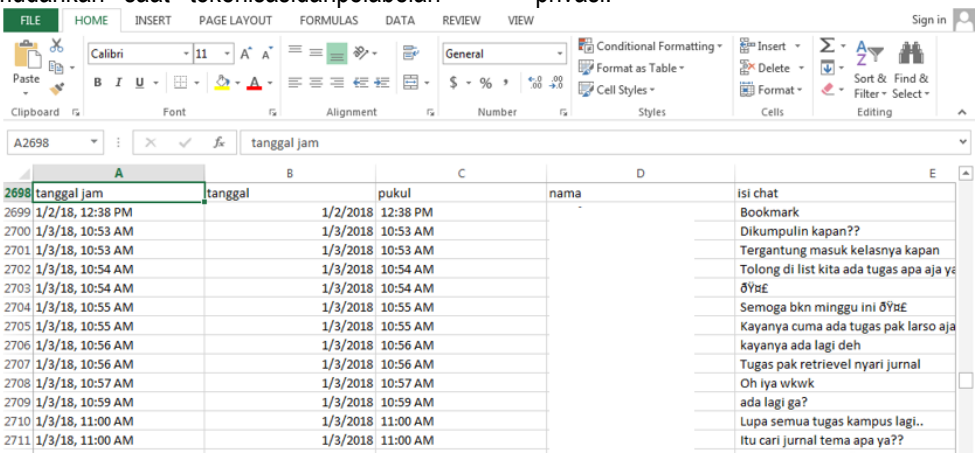
Gambar 4. Proses Akuisisi data menggunakan *FTK Imager*

Examination and *analysis* adalah proses pengungkapan bukti dengan cara menganalisis data berdasarkan hasil *acquisition*. Basis data *WhatsApp*yang dianalisis adalah *WhatsApp*chat.txt. Tahap pertama yang dilakukan adalah mengekstrak data dari image dan dianalisis menggunakan *toolFTK Imager*. Proses tersebut dapat dilakukan melalui menu *file*, pilih *add evidence* dan pilih *Image File*. Selanjutnya *file image* tersebut dimasukkan untuk dilihat isinya.



Gambar 5. Proses Ekstraksi barang bukti menggunakan *FTK Imager*

Setelah data berhasil diekstrak, langkah selanjutnya adalah merapikan data secara tabular. Fungsinya adalah agar memudahkan saat tokenisasidanpelabelan data. *Tool* yang digunakan untuk merapikan data secara tabular adalah *MicrosoftExcel*. Nama pengguna disamarkan untuk menjaga privasi.



	A	B	C	D	E
2698	tanggal jam	tanggal	pukul	nama	isi chat
2699	1/2/18, 12:38 PM	1/2/2018	12:38 PM		Bookmark
2700	1/3/18, 10:53 AM	1/3/2018	10:53 AM		Dikumpulin kapan??
2701	1/3/18, 10:53 AM	1/3/2018	10:53 AM		Tergantung masuk kelasnya kapan
2702	1/3/18, 10:54 AM	1/3/2018	10:54 AM		Tolong di list kita ada tugas apa aja ya
2703	1/3/18, 10:54 AM	1/3/2018	10:54 AM		ðŸ¤£
2704	1/3/18, 10:55 AM	1/3/2018	10:55 AM		Semoga bkn minggu ini ðŸ¤£
2705	1/3/18, 10:55 AM	1/3/2018	10:55 AM		Kayanya cuma ada tugas pak larso aja
2706	1/3/18, 10:56 AM	1/3/2018	10:56 AM		kayanya ada lagi deh
2707	1/3/18, 10:56 AM	1/3/2018	10:56 AM		Tugas pak retrievel nyari jurnal
2708	1/3/18, 10:57 AM	1/3/2018	10:57 AM		Oh iya wkwk
2709	1/3/18, 10:59 AM	1/3/2018	10:59 AM		ada lagi ga?
2710	1/3/18, 11:00 AM	1/3/2018	11:00 AM		Lupa semua tugas kampus lagi..
2711	1/3/18, 11:00 AM	1/3/2018	11:00 AM		Itu cari jurnal tema apa ya??

Gambar 6. Proses tabulasi data menggunakan Microsoft Excel

Dataset labelling adalah proses memberikan *label* terhadap *dataset*. Metode yang digunakan untuk memberikan label pada *dataset* adalah *crowdsourcing*. Jumlah *obsever* yang melakukan pelabelan dengan *crowdsourcing*adalah 3 orang.

tanggal jam	isi chat	Tokenization	Bully/Normal	Bully/Normal	Bully/Normal
1/2/18, 12:38 PM	Bookmark			0	
1/3/18, 10:53 AM	Dikumpulin kapan??	kumpul	0	0	0
1/3/18, 10:53 AM	Tergantung masuk kelasnya kapan	gantung jadwal masuk kelas	0	0	0
1/3/18, 10:54 AM	Tolong di list kita ada tugas apa aja ya	tolong data tugas	0	0	0
1/3/18, 10:54 AM			0	0	
1/3/18, 10:55 AM	Semoga bkn minggu ini	semoga minggu	0	0	0
1/3/18, 10:55 AM	Kayanya cuma ada tugas pak larso aja	tugas larso	0	0	0
1/3/18, 10:56 AM	kayanya ada lagi deh	tugas	0	0	0
1/3/18, 10:56 AM	Tugas pak retrievel nyari jurnal	tugas retrievel cari jurnal	0	0	0
1/3/18, 10:57 AM	Oh iya wkwk		0	0	0
1/3/18, 10:59 AM	ada lagi ga?		0	0	0
1/3/18, 11:00 AM	Lupa semua tugas kampus lagi	lupa tugas kampus	0	0	0
1/3/18, 11:00 AM	Itu cari jurnal tema apa ya??	cari jurnal tema	0	0	0
1/3/18, 11:01 AM	Coba di list rum	mohon data	0	0	0
1/3/18, 11:32 AM	Tugas cari jurnal berapa & tema apa?	tugas cari jurnal tema	0	0	0
1/3/18, 11:32 AM	Kelompok or individu	kelompok orang	0	0	0
1/3/18, 11:39 AM	Satu Perorang	orang	0	0	0

Gambar 7. Proses pemberian label terhadap data untuk dilatih

Hasil *obsever* yang berjumlah tiga orang akanmenjadi acuan untuk proses klasifikasi pada tahap selanjutnya.

Clasifier merupakan tahapan untuk mengklasifikasikan *dataset* yang sudah diberi *label* untuk mendapatkan keputusan kepada data baru berdasarkan *dataset* yang sudah dilatih menggunakan algoritma *Naïve Bayes Clasifier* (NBC).Data uji yang digunakan pada riset ini diambil dari data latih nomor 18, 19, 20, 307, 348, 309, 310.

Proses model algoritma NBC yang digunakan untuk menghitung data pada riset ini dapat dilihat pada gambar 7.

KATA KUNCI	YES	NO	JUMLAH TOKEN (YES)	JUMLAH TOKEN (NO)	JUMLAH SELURUH KATA UNIK	YES	NO	DATA UJI NOMOR	19
semester	2	4	109	624	387	0,006	0,005	YES	0,0000000000000042
libur	2	6	109	624	387	0,006	0,007	NO	0,0000000000000040
semester	2	4	109	624	387	0,006	0,005		
temu	1	2	109	624	387	0,004	0,003		
selesai	2	2	109	624	387	0,006	0,003		
buat	3	2	109	624	387	0,008	0,003		

Gambar 8. Proses perhitungan model algoritma Naïve Bayes Clasifier

Result adalah hasil dari perhitungan klasifikasi yang terdiri dari akurasi, *precision*, *recall* dan metode KAPPAyang digunakan untuk menilai tingkat realibitas antara data training dan data uji.

HASIL

Perhitungan hasil pada riset ini menggunakan nilai akurasi, *precision*, *recall* dan KAPPA. Metode KAPPA berfungsi untuk menilai tingkat reliabilitas antar *rater/obsever* atau antar *class/prediction*. Menurut Landis & Koch yang dikutip oleh Bhisma membagi nilai KAPPA menjadi tiga kategori seperti yang tercantum pada tabel 3[15].

Tabel 3. Interpretasi nilai KAPPA

Nilai K	Kekuatan Kesepakatan
≤0.40	Buruk
0.41 - ≤0.75	Sedang
0.76 - 1.00	Baik

Hasil akurasi yang didapatkan berdasarkan perhitungan dari 7 data uji adalah sebesar 71%. Kemudian hasil *precision* didapatkan nilai 100%.Terakhir, hasil *recall* didapatkan nilai 33%. Gambaran lebih detail hasil perhitungan akurasi, *precision* dan *recall* dapat dilihat pada gambar 8.

		CLASS	
Confusion Table	Predicted ↓	YES	NO
	YES	*1*	*0*
	NO	*2*	*4*

AKURASI	71%
PRECISION	100%
RECALL	33%

Gambar 9. Hasil perhitungan akurasi, *precision* dan *recall*

Hasil perhitungan KAPPA adalah sebesar 0.36. Jika dilihat dari tabel interpretasi, hasil ini bernilai buruk. Hal ini terjadi karena perhitungan KAPPA hanya dilakukan untuk 7 data uji. Hasil dapat berbeda tergantung dari jumlah data yang diujikan. Hasil perrhitungan tersebut dapat dilihat pada gambar 9.

	CLASS			
Predicted ↓	YES	NO	Jumlah	%
YES	1	0	1	14%
NO	2	4	6	86%
Jumlah	3	4	7	
%	43%	57%		

Pr(a)	0,7
Pr€	0,6
KAPPA	0,36

Gambar 10. Hasil perhitungan KAPPA

SIMPULAN

Peningkatan penggunaan internet menciptakan bentuk baru dari serangan yang disebut dengan *cyberagression*. *Cyberagression* menjadi masalah berbahaya karena memiliki dampak yang sangat serius terhadap psikis korban. Fokus penelitian ini adalah fenomena *cyberagression* yang terjadi pada aplikasi olah pesan *WhatsApp Messenger*. Proses pengambilan data pada aplikasi tersebut sulit dilakukan karena adanya fitur *end to end encryption* atau E2EE, yaitu setiap pesan yang dikirim langsung dienkripsi secara aman dan hanya bisa dibuka oleh pengirim dan penerima, sehingga harus dilakukan forensik digital untuk mengatasi hal tersebut. Riset ini dimulai dengan proses pengambilan data menggunakan software *FTK Imager* dengan metode forensik digital *live memory*. Selanjutnya data diekstraksi kembali dan pengguna *WhatsApp Messenger* dieksplorasi karakteristiknya sesuai dengan konten obrolan dan diberi label menggunakan metode *crowdsourcing*. Kemudian atribut diolah dengan metode *Naïve Bayes Clasifier*untuk mendeteksi secara otomatis tingkah laku agresi pada pengguna *WhatsApp Messenger*. Hasil akurasi yang didapatkan berdasarkan perhitungan dari 7 data uji adalah sebesar 71%. Kemudian hasil masing-masing dari *precision*, *recall* dan KAPPA adalah 100%, 33% dan 0.36.

Tantangan bagi setiap penyidik forensik adalah terus berkembangnya teknologi enkripsi yang dipakai pada *WhatsApp* sehingga akan semakin menyulitkan dalam proses forensik digital. Selain itu, hasil akurasi dengan nilai kurang dari 80% masih memberikan peluang bagi

para peneliti untuk menerapkan algoritma lain pada kasus ini sehingga dapat menghasilkantingkat akurasi yang lebih baik.

DAFTAR RUJUKAN

[1] A. Prabowo, "Pengguna Ponsel Indonesia Mencapai 142% dari Populasi," 2017. [Online]. Available: https://databoks.katadata.co.id/datapublish/2017/08/29/pengguna-ponsel-indonesia-mencapai-142-dari-populasi.

[2] I. Rahmayani, "Indonesia Raksasa Teknologi Digital Asia," 2015. [Online]. Available: https://www.kominfo.go.id/content/detail/6095/indonesia-raksasa-teknologi-digital-asia/0/sorotan_media.

[3] A. Hadi Pratama, "Laporan comScore: *WhatsApp*Adalah Aplikasi Mobile Terpopuler di Indonesia," 2017. [Online]. Available: https://id.techinasia.com/comscore-*WhatsApp*-adalah-aplikasi-terpopuler-di-indonesia.

[4] N. C.L. Jacobs, L. Goossens, F. Dehue, T. Völlink, and L. Lechner, "Cyber*bully*ing: Where Are We Now? A Cross-National Understanding," *Dutch Cyberbullying Vict. Exp. Perceptions, Attitudes Motiv. Relat. to (Coping with) Cyberbullying Focus Gr. Interviews*, p. 133, 2017.

[5] UNICEF, "Laporan Tahunan Indonesia 2015," *UNICEF Lap. Tah. Indones. 2015*, pp. 1–19, 2015.

[6] S. J. Parault, H. A. Davis, and A. D. Pellegrini, "The Social Contexts of *Bully*ing and Victimization," *J. Early Adolesc.*, vol. 27, no. 2, pp. 145–174, 2007.

[7] Keith Sullivan, *The Anti-bullying Handbook*. Oxford University Press, 2000.

[8] A. Pingit, "*WhatsApp*Naikkan Batas Usia Pengguna Menjadi 16 Tahun," 2018. [Online]. Available: https://katadata.co.id/berita/2018/04/27/*WhatsApp*-naikkan-batas-usia-pengguna-dari-menjadi-16-tahun.

[9] *WhatsApp*Inc., "Verifikasi Akun," 2018. [Online]. Available: https://faq.*WhatsApp*.com/id/iphone/20902747.

[10] *WhatsApp*Inc., "Enkripsi end-to-end," 2018. [Online]. Available: https://faq.*WhatsApp*.com/en/android/28030015/?lang=id.

[11] F. Karpisek, I. Baggili, and F. Breitinger, "*WhatsApp*network forensics: Decrypting and understanding the *WhatsApp*call signaling messages," *Digit. Investig.*, vol. 15, pp. 110–118, 2015.

[12] S. Ikhsani and C. Hidayanto, "Analisa Forensik *WhatsApp*dan LINE Messenger Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia," *J. Tek. ITS*, vol. 5, no. 2, pp. 728–736, 2016.

[13] D. Chatzakou, N. Kourtellis, J. Blackburn, E. De Cristofaro, G. Stringhini, and A. Vakali, "Detecting Aggressors and Bullies on Twitter," pp. 767–768.

[14] S. Colin, "The CRISP - DM Model: The New Blueprint for DataMining," *J. Data Warehous.*, vol. 5, p. 14, 2000.

[15] B. Murti, "Validitas dan reliabilitas pengukuran," pp. 1–19, 2011.