Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 4 No. 4 (2020) 730 - 735 ISSN Media Elektronik: 2580-0760

Investigasi Cyberbullying pada WhatsApp Menggunakan Digital Forensics Research Workshop

Imam Riadi[1], Sunardi[2], Panggah Widiandana[3]
[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan
[3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan
[1]imam.riadi@is.uad.ac.id, [2]sunardi@mti.uad.ac.id, [3]panggah1808048029@webmail.uad.ac.id

Abstract

Cyberbullying in group conversations in one of the instant messaging applications is one of the conflicts that occur due to social media, specifically WhatsApp. This study conducted digital forensics to find evidence of cyberbullying by obtaining work in the Digital Forensic Research Workshop (DFRWS). The evidence was investigated using the MOBILedit Forensic Express tool as an application for evidence submission and the Cosine Similarity method to approve the purchase of cyberbullying cases. This research has been able to conduct procurement to reveal digital evidence on the agreement in the Group's features using text using MOBILedit. Identification using the Cosine method. Similarities have supported actions that lead to cyberbullying with different levels Improved Sqrt-Cosine (ISC) value, the largest 0.05 and the lowest 0.02 based on conversations against requests.

Keywords: Digital Forensic, Instant Messaging, DFRWS, Cosine Similarity, MOBILedit Forensic Express.

Abstrak

Cyberbullying dalam percakapan group pada salah satu aplikasi *instant messaging* merupakan salah satu konflik yang terjadi akibat dampak negatif penggunaan media sosial khususnya WhatsApp. Penelitian ini melakukan forensik digital untuk menemukan barang bukti *cyberbullying* dengan kerangka kerja *Digital Forensics Research Workshop* (DFRWS). Barang bukti dilakukan investigasi menggunakan tools MOBILedit Forensic Express sebagai aplikasi pengangkatan barang bukti dan metode *Cosine Similarity* untuk mengidentifikasi terjadinya kasus *cyberbullying*. Penelitian ini telah dapat melakukan akuisisi untuk mengungkap bukti digital pada pelaku di fitur Group berupa teks menggunakan MOBILedit. Identifikasi menggunakan metode *Cosine Similarity* telah mampu mengidentifikasi tindakan yang mengarah pada *cyberbullying* dengan tingkat yang berbeda, nilai *Improved Sqrt-Cosine* (ISC) terbesar 0,05 dan nilai ISC terendah 0,02 berdasar pada percakapan terhadap *query*.

Kata kunci: *Digital Forensic*, *Instant Messaging*, DFRWS, *Cosine Similarity*, MOBILedit Forensic Express.

1. Pendahuluan

Perkembangan teknologi dan informasi saat ini semakin pesat dan diikuti oleh meningkatnya penggunaan media sosial yang merupakan teknologi yang banyak digunakan terutama perangkat di *platform* android [1]. *Cyberbullying* merupakan salah satu masalah yang sering terjadi [2] terutama percakapan *group* dalam aplikasi *instant messaging*. Berdasarkan survei [3] menyatakan bahwa 97,24% responden menggunakan aplikasi WhatsApp, LINE 88,49%, BBM 85,82%, Facebook 77,26%, dan Telegram 76. Pengguna WhatsApp yang sangat besar tersebut didukung temuan *website* statista [4] yang menunjukkan sebesar 1,6 miliar pengguna mengakses messenger WhatsApp secara bulanan. Hal ini dikarenakan fitur-fitur pada WhatsApp cukup memenuhi kebutuhan manusia untuk mempermudah komunikasi antara satu dengan yang lain dengan jarak yang begitu jauh.

Banyaknya pengguna media sosial khususnya WhatsApp membuka peluang adanya kejahatan siber (*cybercrime*). Kasus-kasus kejahatan di Indonesia yang melibatkan aplikasi WhatsApp banyakmenjadi rujukan dalam forensika digital [5]. *WhatsApp Group* (WAG) merupakan salah satu fitur yang dapat membantu komunitas untuk melakukan komunikasi secara intensif, disisi lain fitur tersebut juga membuka peluang adanya *bully* dalam *group* tersebut.

Diterima Redaksi : 15-07-2020 | Selesai Revisi : 12-08-2020 | Diterbitkan Online : 20-08-2020

RSA *Anti Fraud Command Center* [6] menyatakan tahun 2013-2015 terjadi peningkatan aktivitas *cybercrime* sebesar 173% di seluruh dunia dan menyebabkan kerugian sebesar US$ 325 milyar. Transaksi *online* pada tahun 2015 sebesar 45% tetapi menyebabkan peningkatan penipuan sebesar 61%. Dampak negatif media sosial yang sering dialami oleh para remaja adalah tindakan *cyberbullying* [7]. Dalam identifikasi cyberbullying perlu referensi untuk *investigator* untuk mempermudah identifikasinya [8]. Kriteria untuk identifikasi adanya *cyberbullying* dapat dilakukan dengan melihat kandungan kata-kata negatif dalam percakapan [9].

Penelitian tentang Akuisisi Bukti Digital pada Instagram Messenger Berbasis Android Menggunakan Metode *National Institute of Justice* (NIJ) [10] menghasilkan proses akuisisi barang bukti digital yang berhasil didapatkan pada Instagram pada *smartphone* dalam kondisi *root* didapatkan foto dan *chatting*. Penelitian lain yang serupa adalah Analisis Bukti Digital Facebook Messenger Menggunakan Metode *National Institute of Standards and Technology* (NIST) menghasilkan teks percakapan, gambar, dan audio pada aplikasi Facebook Messenger [11].

Penelitian-penelitian sebelumnya tersebut hanya melakukan akuisisi atau pengangkatan barang bukti. Sedangkan penelitian ini setelah melakukan forensik digital untuk mengangkat barang bukti menggunakan tools forensic yaitu MOBILedit dan selanjutnya dilakukan analisis adanya tindakan *cyberbullying*. Penelitian dilakukan pada percakapan WAG menggunakan kerangka kerja *Digital Forensics Research Workshop* (DFRWS). Adanya kasus *cyberbullying* diidentifikasi menggunakan metode *Cosine Similarity* [12].

2. Metode Penelitian

Akuisisi barang bukti dilakukan untuk mendapatkan barang bukti digital. Penelitian melakukan proses akuisisi menggunakan *tools forensic* yaitu MOBILedit yang digunakan untuk mengangkat barang bukti yang kemudian akan dilakukan analisis lebih lanjut mengenai tindakan *cyberbullying*.

2.1. DFRWS

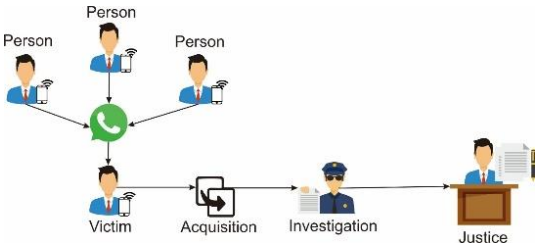
DFRWS merupakan kerangka kerja ilmiah yang memiliki dasar dan terbukti untuk proses investigasi foresik yang meliputi pemeliharaan, pengumpulan, validasi, identifikasi, analisis, interprestasi, dokumentasi, dan presentasi bukti digital yang berasal dari sumber-sumber digital dari tempat perkara atau alat dilakukannya kejadian *cybercrime* untuk tujuan memfasilitasi atau melanjutkan rekonstruksi peristiwa yang melanggar hukum teknologi informasi dan mengandung pidana, atau membantu untuk mengantisipasi tindakan yang merusak keaslian barang bukti sehingga membuat barang bukti yang telah didapatkan menjadi tidak sah di mata hukum dan terbukti mengganggu untuk operasi yang direncanakan dalam proses investigasi [13]. Kerangka kerja DFRWS yang dipakai dalam penelitian dapat dilihat pada Gambar 1.

Gambar 1. Alur tahap DFRWS

Gambar 1 merupakan DFRWS yang terdiri dari beberapa tahapan yaitu tahap identifikasi (*identification*) melakukan perancangan kebutuhan yang diperlukan untuk membantu penyelidikan dalam pencarian bukti, tahap pemeliharaan (*preservation*) menjaga keaslian dan keamanan bukti digital agar sah dibadan hukum, tahap pengumpulan (*collection*) mengumpulkan barang bukti yang memperkuat persidangan kuat, tahap pemeriksaan (*examination*) menentukan apa saja yang akan dianalisis atau filterisasi data, tahap analisis (*analysis*) mencari dan menganalisis barang bukti dalam pengolahan data yang telah didapat, tahap presentasi (*presentation*) melaporkan dan mempresentasikan hasil analisis sehingga dapat dipahami oleh publik dan berlaku dimeja persidangan [14].

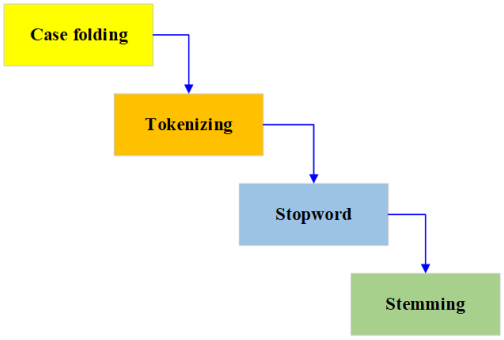
2.2. Simulasi kasus

Simulasi kasus dilakukan dengan membuat WAG yang berisi 4 orang dengan *bullying* dilakukan oleh 3 orang kepada 1 korban seperti pada Gambar 2. *Smartphone* korban akan diakuisisi untuk proses investigasi forensik.



Gambar 2. Simulasi Kasus pada WhatsApp Group

Preprocessing merupakan tahap pertama dari *text mining* yang mencakup semua rutinitas dan mempersiapkan data yang akan digunakan pada operasi *knowledge discovery* sistem *text mining* [15]. *Prepocessing* digunakan untuk mempersingkat dan memperingkas kalimat yang telah diucapkan dalam group dengan cara mengambil kata-kata yang dianggap penting saja untuk mempermudah dan mempercepat proses identifikasi kasus *cyberbullying*. *Prepocessing* terdapat beberapa tahapan untuk mendapatkan kalimat atau kata yang berisi informasi yang diinginkan agar identifikasi dapat lebih akurat. Tahap-tahap *prepocessing* dapat dilihat pada Gambar 3.



Gambar 3. Alur tahapan prepocessing

Gambar 3 merupakan alur tahapan *prepocessing* yang terdiri dari tahap *case folding* melakukan pengubahan huruf kapital menjadi huruf kecil pada percakapan yang ada dan hanya huruf yang diterima untuk proses *text mining* [16], tahap *tokenizing* melakukan pemecahan kalimat menjadi perkata dan menghilangkan tanda baca seperti petik (“), seru (!), tanya (?) [17], tahap *stopword* adalah kosakata yang bukan merupakan ciri (kata unik) dari suatu dokumen. Misalnya “di”, “oleh”, “pada”, “sebuah”, “karena” dan lain sebagainya. *Stopword* didefinisikan sebagai hal yang tidak relevan sehubungan dengan subjek utama dari *database*, meskipun mungkin sering terdapat dalam dokumen *Stopword* termasuk penentu, konjungsi, preposisi dan sejenisnya [18], tahap *stemming* adalah tahapan untuk proses pengembalian kata dari kata berimbuhan menjadi kata asal atau kata dasar [19].

2.3. TF-IDF

Term Frequency (TF) adalah jumlah kata yang terkandung dalam percakapan. Semakin besar kata yang sering muncul maka semakin besar bobotnya seperti dapat dilihat pada Rumus 1.

$$W(d,t) = TF(d,t) \quad (1)$$

Dengan $TF(d,t)$ adalah jumlah kemunculan *term* t pada *teks* d. *Inverse Document Frequency* (IDF) merupakan banyaknya dokumen yang mengandung kata [20] sesuai dengan Rumus 2.

$$idf_t = \log 10\left(\frac{N}{df_t}\right) \quad (2)$$

Dengan *N* adalah jumlah seluruh dokumen di kumpulan dokumen dan df_t adalah jumlah dokumen yang mengandung kata yang menjadi target. Semakin sedikit jumlah dokumen yang mengandung kata target, maka bobot IDF akan semakin besar. TF-IDF perkalian bobot TF dengan IDF dari tiap kata sesuai dengan Rumus 3.

$$w = tf_t \times idf_t \quad (3)$$

Dengan *w* adalah *weight* atau hasil dari perkalian antara *term frequency* dengan *inverse document frequency*. tf_t adalah *term frequency* merupakan jumlah *term* dari setiap dokumen, dan idf_t adalah *term document frequency* merupakan banyak dokumen yang mengandung *term* pada *Query*.

2.4. *Improved Sqrt-Cosine* (ISC)

Cosine Similarity merupakan metode yang digunakan untuk mengidentifikasi terjadinya kasus *cyberbullying* [21] seperti Rumus 4. Meningkatkan efektifitas untuk deteksi menggunakan pengembangan dari metode *Cosine Similarity* yaitu menggunakan metode *Improved Sqrt-Cosine* (ISC) menggunakan Rumus 4 [22].

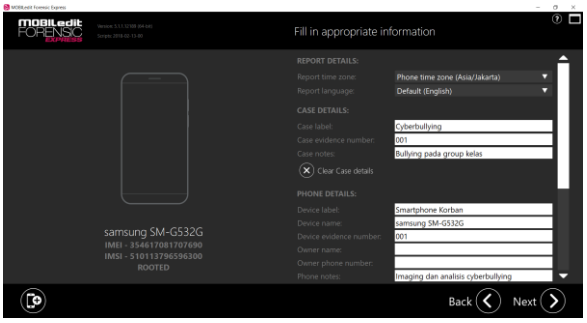
$$ISC\ (d_i, q_i) = \frac{\Sigma_{j=01}^{i}\sqrt{q_{ij} \cdot d_{ij}}}{\sqrt{\Sigma_{j=1}^{t}(q_{ij})}.\sqrt{\Sigma_{j=1}^{t}(d_{ij})}} \quad (4)$$

Dengan q_{ij} adalah bobot istilah j pada *query* i, dan d_{ij} adalah bobot istilah j pada percakapan i.

3. Hasil dan Pembahasan

3.1. *Identification*

Identifikasi dilakukan dengan memberi keterangan pada barang bukti digital yang telah didapatkan seperti pada Gambar 4. Terdapat beberapa form untuk mengidentifikasi barang bukti seperti waktu dilakukan *imaging* dan bahasa yang digunakan. *Case label* merupakan judul dari *case* barang bukti yang akan diinvestigasi sehingga penanganan *case* tidak akan salah sasaran dan *investigator* mengetahui *case* secara singkat dari barang bukti yang akan diinvestigasi. *Case evidence number* merupakan nomor barang bukti yang membantu *investigator* mengetahui *case* yang ditangani merupakan barang bukti *case* yang keberapa karena terkadang dalam satu *case* yang sama terdapat banyak barang bukti yang perlu dianalisis sehingga perlunya *case evidence number* diperlukan untuk mempermudah dalam membedakan barang bukti satu dengan yang lainnya. *Case note* merupakan catatan untuk menandai barang bukti untuk mempermudah dalam melakukan investigasi sehingga lebih mudah melakukan identifikasi barang bukti yang telah ditemukan seperti kapan pengambilan, dimana, siapa saja, dan bagaimana kronologinya sehingga barang bukti yang telah didapatkan dapat benar-benar teridentifikasi dengan jelas.

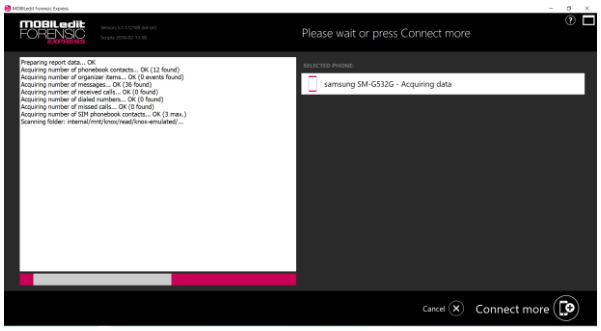


Gambar 4. *Identification* Barang Bukti Digital

3.2. *Preservation*

Preservation seperti pada Gambar 5 dilakukan untuk menjaga keaslian dan keamanan barang bukti untuk itu diperlukan proses *imaging* untuk mengambil barang bukti pada *smartphone* korban yang telah didapat.

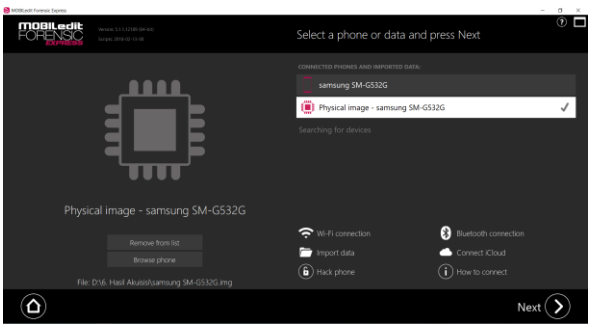
Proses *imaging* dilakukan menggunakan *tools forensic* yaitu MOBILedit Forensic Express untuk pengamanan dan menjaga keaslian barang bukti yang telah didapatkan. Tahap ini sangat mempengaruhi terhadap keaslian barang bukti, apakah barang bukti dapat diterima dipersidangan atau tidak dapat digunakan. Keaslian barang bukti dapat dikatakan sangat sensitif karena jika barang bukti asli berubah maka hasil investigasi yang telah dilakukan tidak dapat diakui didalam persidangan karena sudah dianggap memodifikasi data barang bukti yang telah didapatkan sebelumnya.



Gambar 5. *Create Physical Image*

3.3. Collection

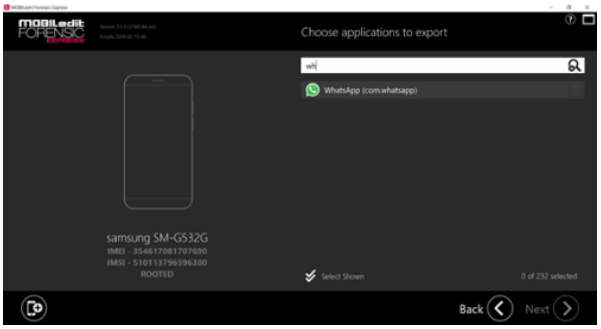
Collection seperti Gambar 6 dilakukan *import* hasil create *physical image* atau *proses imaging* pada *smartphone* korban pada tahap *preservation*. Tahap ini akan membuka barang bukti hasil *cloning* pada tahap *preservation* untuk selanjutnya akan dianalisis oleh *investigator* mengenai *case* yang telah dihadapi. Dengan demikian barang bukti asli tidak akan sedikitpun tersentuh dan merubah data barang bukti asli yang telah didapatkan karena barang bukti yang telah ditemukan harus valid dipersidangan dan salah satu syarat agar barang bukti dapat diterima dipengadilan adalah barang bukti yang asli yang sama seperti saat ditemukannya barang bukti tersebut.



Gambar 6. *Collection* barang bukti digital

3.4. *Examination*

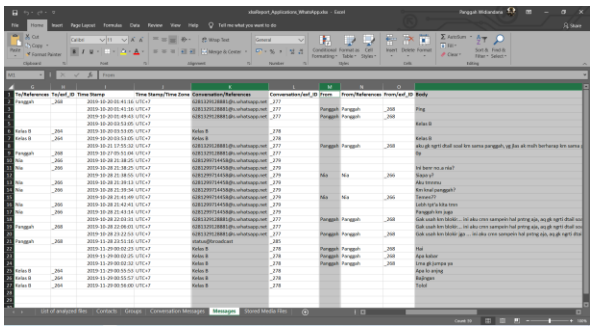
Examination dilakukan seperti pada Gambar 7 dilakukan dengan mencari aplikasi yang akan dilakukan investigasi. Pada penelitian ini aplikasi yang akan dianalisis atau diinvestigasi adalah WhatsApp Messenger. Proses *examination* atau filter barang bukti dilakukan sesuai dengan kebutuhan *investigator* dalam menganalisis barang bukti digital. Tahap ini akan membatasi dalam melakukan penyelidikan barang bukti agar tidak melebihi dari *case* yang telah diinvestigasi, karena dalam hal investigasi forensik *investigator* hanya diperbolehkan menganalisis sesuai perkara yang telah diajukan.



Gambar 7. Proses *examination* barang bukti digital

3.5. *Analysis*

Analisis hasil yang didapat menggunakan aplikasi MOBILedit Forensic Express dan *export* ke dalam bentuk file excel kemudian difilter yang diperlukan untuk proses identifikasi *cyberbullying* sehingga dalam proses analisis identifikasi lebih mudah dan dapat terlihat bagaimana rincian pesan tersebut diteruna mulai dari isi pesan, dari siapa pesan tersebut dikirim, dan dimana proses pesan itu telah berlangsung seperti pada Gambar 8.



Gambar 8. Analysis *cyberbullying*

Gambar 8 merupakan proses analisis *cyberbullying* hasil dari aplikasi MOBILedit Forensic Express. Hasil yang telah ditemukan kemudian dilakukan *filtering* untuk diambil beberapa field seperti *Convertation/Referensi, From*, dan *Body* yang dibutuhkan untuk *text mining* agar dapat mengidentifikasi *cyberbullying*. *Field* yang telah dipilih akan diketahui nama *group*, nama pengirim, dan percakapan yang terjadi pada *group* tersebut. Proses analisis *cyberbullying* pada WhatsApp *Messenger* merupakah hasil pemilihan *field* yang dibutuhkan untuk proses identifikasi *cyberbullying* sehingga dapat dilakukan *preprocessing* dan penerapan metode *cosine similarity* untuk identifikasi *cyberbullying* yang dilakukan pada *group* tersebut. Tahap yang dilakukan untuk mengidentifikasi *cyberbullying* yaitu data yang

diambil dari data simulasi sebuah *group* yang terdiri dari empat orang yang melakukan percakapan dalam *group* tersebut, dialog percakapan dapat dilihat pada Tabel 1.

Tabel 1. Percakapan Group

Pengguna	Isi Percakapan
andi	Leo lo tadi ngomong apa dibelakang kelas?
anto	Iya kenapa guru jadi marah-marah dikelas
nita	Iya ini kayaknya leo ngomong sesuatu deh
leo	aku gak ngomong apa-apa ko
anto	bohong lo pasti ngomongkan kalau kita ngomongin itu guru
nita	gak mungkin lah GOBLOK kalau lo gak ngomong apa-apa, masak tiba2 guru tau masalah julit guru
andi	BEGOK dasar @leo rahasia kita aja ngapain diomongin coba
leo	iya maaf aku tadi sedikit keceplosan kalau lagi ngomongin
anto	ah KAMPRET lo @leo, GOBLOKnya gak ketulungan
andi	apa coba motivasi lo ngomong ke guru, TOLOL
nita	hadeehh punya temen gini amat yak
leo	iya iya maafin aku
anto	TOLOL lo @leo

Data yang telah didapatkan dari pengangkatan barang bukti akan dilakukan pengelompokan sesuai dengan percakapan yang telah dilakukan dalam sebuah *group* dan dilakukan *prepocessing* sebelum diidentifikasi *cyberbullying* menggunakan metode *Cosine similarity*. Hasil *prepocessing* dapat dilihat pada Tabel 2. Hasil *prepocessing* kemudian dilakukan identifikasi dengan metode *Cosine similarity* sehingga mendapatkan TF-IDF seperti Tabel 3, sedangkan Tabel 4 merupakan hasil dari pencarian TF-IDF dari percakapan yang dilakukan oleh pelaku dan korban dalam *group*.

TF yang telah didapat pada percakapan akan dituliskan pada Tabel 3 pada kolom term dengan menggunakan rumus (1). Nilai IDF dalam percakapan dapat dilihat pada Tabel 3 pada kolom IDF dengan menggunakan rumus (2). Hasil perkalian antara rumus (1) dengan rumus (2) maka akan didapatkan rumus (3) atau dapat dikatakan nilai TF-IDF yang dapat dilihat pada Tabel 3 kolom WDt=TF-IDF.

Tabel 2. *Prepocessing* Percakapan

Pengguna	Isi Percakapan
andi	leo, lo, ngomong, belakang, kelas, begok, dasar, leo, rahasia, aja, ngapain, omong, coba, apa, coba, motivasi, lo, omong, guru, tolol
anto	iya, guru, marah, marah, kelas, bohong, lo, omong, omong, guru, ah, kampret, lo, leo, goblok, gak, ketulungan, tolol, lo
nita	iya, kayak, leo, omong, deh, gak, goblok, lo, gak, omong, masak, tiba2, guru, tau, julit, guru, hadeeh, temen
leo	gak, omong, ko, iya, maaf, aku, tadi, ceplos, kalau, lagi, omong, iya, iya, maaf

Tabel 3. TF-IDF

Term	DF	IDF	WDt = TF-IDF				
			Q	Andi	Anto	Nita	Leo
begok	2	0,48	0,48	0,48	0	0	0
bohong	2	0,48	0,48	0	0,48	0	0
kampret	2	0,48	0,48	0	0,48	0	0
tolol	3	0,30	0,30	0,30	0,30	0	0
goblok	3	0,30	0,30	0	0,30	0,30	0

Tabel 4. TF-IDF dengan *Query*

WDt*WDq				
Q	Andi	Anto	Nita	Leo
0,30	0,23	0	0	0
0,48	0	0,23	0	0
0,48	0	0,23	0	0
0,48	0,09	0,09	0	0
0,30	0	0,09	0,09	0

Pada rumus (4) di bagian pembilang yaitu $\Sigma_{j=01}^{i}(q_{ij}.d_{ij})$ dilakukan penambahan dari hasil perkalian antara TF-IDF percakapan yang dilakukan oleh seseorang dengan TF-IDF *query*. Cara mendapatkan $\Sigma_{j=01}^{i}\sqrt{q_2 \cdot d_i}$ pada bagian penyebut Rumus (5) merupakan hasil akar dari penjumlahan Tabel 4 pada setiap *user*. Hasil untuk mendapatkan $\sqrt{\Sigma_{j=1}^{t}(q_{ij})}.\sqrt{\Sigma_{j=1}^{t}(d_{ij})}$ pada pembilang pada rumus (5) dengan hasil penjumlahan TF-IDF pada Tabel 3 dan dilakukan akar. Hasil ISC untuk efektifitas metode *Cosine similarity* menggunakan rumus (5) dapat dilihat sebagai berikut:

$$ISC(d_{andi}, q_i) = \frac{0,6}{2,03 \times 10,29} = 0,03$$

$$ISC(d_{anto}, q_i) = \frac{0,8}{2,03 \times 7,91} = 0,05$$

$$ISC(d_{nita}, q_i) = \frac{0,3}{2,03 \times 8,99} = 0,02$$

$$ISC(d_{leo}, q_i) = \frac{0}{2,03 \times 7,78} = 0$$

Hasil perhitungan ISC mendapatkan kesimpulan bahwa nilai ISC terbesar adalah anto sebesar (0,05), yang kedua adalah andi sebesar (0,03), yang ketiga adalah nita sebesar (0,02), dan terakhir adalah leo (0).

3.6. *Presentation*

Data yang didapat dalam penelitian ini adalah aplikasi forensik MOBILedit Forensic Express dapat mengambil data berupa percakapan dalam group WhatsApp kemudian dianalisis dan mendapatkan nilai *Cosine Similarity* pelaku yang melakukan *cyberbullying* beserta tingkat *cyberbullying* yang dilakukan.

4. Kesimpulan

Hasil yang didapat menggunakan metode DFRWS membantu proses akuisisi untuk mengungkap bukti digital pada pelaku di fitur *Group* berupa teks. Hasil identifikasi tindakan yang mengarah pada *cyberbullying* didapatkan dengan nilai hasil tertinggi memiliki tingkat *cyberbullying* sebesar 0,05 dan nilai hasil terendah memiliki tingkat *cyberbullying* dengan nilai ISC sebesar 0,02 dari persentase tersebut didapat nilai kata

cyberbulying pada percakapan terhadap *query*. Data tersebut membuktikan bahwa metode *forensics* DFRWS dapat mengangkat barang bukti berupa teks dalam group dan metode *Improved Sqrt-Cosine* dapat mengidentifikasi *cyberbullying* sesorang yang akan melakukan tindakan *cyberbullying* dengan tingkat yang berbeda-beda.

Daftar Rujukan

[1] R. Umar, I. Riadi, and B. F. Muthohirin, "Live forensics of tools on android devices for email forensics," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 4, pp. 1803–1809, 2019, doi: 10.12928/TELKOMNIKA.v17i4.11748.

[2] S. Wang, "Standing up or standing by: Bystander intervention in cyberbullying on social media," *New Media Soc.*, p. 1461444820902541, Jan. 2020, doi: 10.1177/1461444820902541.

[3] F. Zebua, "Laporan DailySocial: Survey Instant Messaging 2017," *dailysocial.id*, 2017. https://dailysocial.id/post/laporan-dailysocial-survey-instant-messaging-2017.

[4] J. Clement, "WhatsApp - Statistics & Facts," *statista*, 2019. https://www.statista.com/topics/2018/whatsapp/.

[5] T. D. Larasati and B. C. Hidayanto, "Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10," *Sesindo*, vol. 6, no. November, pp. 456–256, 2017.

[6] RSA, "Current State of Cybercrime," 2016. https://www.rsa.com/content/dam/rsa/PDF/2016/05/2016-current-stateof-cybercrime.pdf.

[7] J. P. S. A. Kusumadewi, "Polisi usut percakapan 'jessica-mirna' yang beredar di sosmed," *CNN Indonesia*, 2016. http://www.cnnindonesia.com/nasional/20160121080758-12-105715/polisi-usut-percakapan-jessica-mirna-yang-beredar-di-sosmed/.

[8] I. Riadi and P. Widiandana, "Mobile Forensics for Cyberbullying Detection using Term Frequency - Inverse Document Frequency (TF-IDF)," vol. 5, no. 2, pp. 68–76, 2020, doi: 10.26555/jiteki.v5i2.14510.

[9] P. Widiandana, I. Riadi, and Sunardi, "Analisis investigasi forensik cyberbullying pada Whatsapp Messenger menggunakan metode NIST," *Semin. Nas. Teknol. Fak. Tekinik Univ. Krisnadwipayana*, pp. 488–493, 2019, [Online]. Available: https://jurnal.teknikunkris.ac.id/index.php/semnastek2019/article/view/308.

[10] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Tek. Inform. dan Sist. Inf. Vol. 4 Nomor 2 Agustus 2018*, vol. 4, pp. 219–227, 2018, [Online]. Available: https://www.researchgate.net/profile/Imam_Riadi/publication/327779438_Akuisisi_Bukti_Digital_Pada_Instagram_Messenger_Berbasis_Android_Menggunakan_Metode_National_Institute_Of_Justice_Institute_Of_Justice_Institute_of_Justice_NIJ/links/5ba3e1bf92851ca9ed1.

[11] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *It J. Res. Dev.*, vol. 3, no. 1, p. 13, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[12] D. Van Bruwaene, Q. Huang, and D. Inkpen, "A multi-platform dataset for detecting cyberbullying in social media," *Lang. Resour. Eval.*, 2020, doi: 10.1007/s10579-020-09488-3.

[13] Brian Carrier, "Defining Digital Forensic Examination and Analysis Tools Using \nAbstraction Layers," *Int. J. Digit. Evid.*, vol. 1, no. 4, pp. 1–12, 2013, doi: 10.1017/CBO9781107415324.004.

[14] A. L. Suryana, R. El Akbar, and N. Widiyasono, "Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS)," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, pp. 111–117, 2016, doi: 10.26418/jp.v2i2.16821.

[15] J. Feldman, R., & Sanger, "The Text Mining HandBook," New York: Cambridge University Press, 2007.

[16] C. Triawati, "Metode Pembobotan Statistical Concept Based untuk Klastering dan Kategorisasi Dokumen Berbahasa Indonesia," *Univ. Telkom*, 2009.

[17] F. J. Weiss, S. M., Indurkhya, N., Zhang, T., & Damerau, *Text Mining: Predictive Methods fo Analyzing UnstructeredInformation*. New York: Springer, 2005.

[18] W. Dragut, E., Fang, F., Sistla, P., Yu, C., & Meng, *Stop Word and Related Problems in Web Interface*. Chicago: Computer Science Department University of Illinois, 2009.

[19] F. Z. Tala, *A Study Of Stemming Effects On Information Retrieval in Bahasa Indonesia*. The Netherlands: Universiteitvan Amsterdam, 2003.

[20] F. A. H. and D. A. Zuhdi, "Aplikasi Sistem Temu Kembali Dokumen dengan Metode Vector Space Model," *KONVERGENSI*, vol. 5, no, pp. 38–49, 2009.

[21] G. A. Pradnyana dan N. A. Sanjaya, "Perancangan Dan Implementasi Automated Document Integration Dengan Menggunakan Algoritma Complete Linkage Agglomerative Hierarchical Clustering," vol. 5, (2, pp. 1–10, 2012.

[22] S. Sohangir and D. Wang, "Improved sqrt-cosine similarity measurement," *J. Big Data*, vol. 4, no. 1, 2017, doi: 10.1186/s40537-017-0083