

Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)

Anton Yudhana¹, Imam Riadi², Riski Yudhi Prasongko³

¹ Program Studi Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta

² Program Studi Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan, Yogyakarta

³ Program Studi Magister Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta

^{1,2} Jl. Ahmad Yani (Ringroad Selatan) Tamanan, Banguntapan, Bantul 55166, Yogyakarta

² Jl. Prof. Dr. Soepomo, S.H., Janturan, Umbulharjo 55166, Yogyakarta

email: ¹ eyudhana@ee.uad.ac.id, ² imam.riadi@is.uad.ac.id, ³ riski1807048022@webmail.uad.ac.id

Abstract — *The more smartphones in the world, the more cybercrimes. WhatsApp is a popular smartphone application used for criminal activities. WhatsApp is a well-known social network in Indonesia, and is used by many people. WhatsApp is a great way to stay safe online, as it protects users from crimes such as hate speech, fraud, and defamation. This investigation was carried out in an effort to collect forensic evidence from the WhatsApp social media application using the DFRWS methodology. Our digital forensics phase includes the identification, storage, collection, investigation, analysis and presentation of digital evidence of cyber crimes using the MOBILedit Forensic Express and HashMyFiles software applications. We searched for digital evidence on smartphones using a case study with 13 parameters. This type of evidence can be found using certain methods. The results of this study indicate that the digital forensic software MOBILedit Forensic Express can detect digital evidence with an accuracy rate of 84.6%, while Hashmyfiles can detect the authenticity of digital evidence by 100%.*

Abstrak — Semakin banyak smartphone di dunia, semakin banyak kejahatan dunia maya. WhatsApp adalah aplikasi smartphone populer yang digunakan untuk kegiatan kriminal. WhatsApp adalah jejaring sosial yang terkenal di Indonesia, dan digunakan oleh banyak orang. WhatsApp adalah cara yang bagus untuk tetap aman saat online, karena melindungi pengguna dari kejahatan seperti ujaran kebencian, penipuan, dan pencemaran nama baik. Penyelidikan ini dilakukan dalam upaya mengumpulkan bukti forensik dari aplikasi media sosial WhatsApp menggunakan metodologi DFRWS. Fase forensik digital kami meliputi identifikasi, penyimpanan, pengumpulan, penyelidikan, analisis, dan penyajian bukti digital kejahatan dunia maya menggunakan aplikasi perangkat lunak MOBILedit Forensic Express dan HashMyFiles. Kami mencari bukti digital pada smartphone menggunakan studi kasus dengan 13 parameter. Jenis bukti ini dapat ditemukan dengan menggunakan metode tertentu. Hasil penelitian ini menunjukkan bahwa perangkat lunak forensik digital MOBILedit Forensic Express dapat mendeteksi barang bukti digital dengan tingkat akurasi sebesar 84,6%, sedangkan Hashmyfiles dapat mendeteksi keaslian barang bukti digital sebesar 100%.

Kata Kunci — WhastApp, Digital Forensik, DFRWS, Komputer Forensiki.

*) penulis korespondensi: Riski Yudhi Prasongko
Email: riski1807048022@webmail.uad.ac.id

I. PENDAHULUAN

Salah satu perkembangan teknologi yang semakin pesat adalah smartphone [1]. Smartphone merupakan perangkat teknologi komunikasi yang digunakan untuk berkomunikasi langsung atau tidak langsung. Smartphone bukan sekedar alat komunikasi, Smartphone juga dapat digunakan sebagai media penyimpan data, mengakses internet dan bertukar pesan. Pada tahun 2019 pengguna smartphone di Indonesia diperkirakan mencapai 92 juta konsemen. Berdasarkan data tersebut, sistem operasi yang digunakan adalah Android sebesar 90,64%, iOS meningkat menjadi 5,34%, Blackberry sebesar 0,38%, Series 40 sebesar 0,37%, Nokia sebesar 0,33% dan lainnya sebesar 2,31%[2][3] .

Smartphone yang berkembang pesat dan mulai populer dibandingkan dengan komputer, dengan tersedianya banyak aplikasi dan fungsi yang terdapat dalam smartphoe, salah satunya adalah aplikasi Instant Messaging (IM). Aplikasi perpesanan yang terkenal dan banyak digunakan oleh para pengguna di Indonesia adalah WhatsApp [5][6].

Dampak perkembangan smartphone ini memiliki dampak negatif yaitu berupa banyaknya kejahatan digital atau mampu dianggap menggunakan cybercrime. Pelaku cybercrime memanfaatkan smartphone menjadi indera komunikasi buat membantu melakukan kejahatan, hal ini termasuk ke pada cybercrime lantaran memakai media elektro smartphone pada melakukan kejahatan sinkron menggunakan UUIE

(Informasi dan Transaksi Elektronik) no. 11 tahun 2008 [7]. Forensik digital secara teknis dapat membantu dalam pengumpulan bukti digital untuk disajikan di pengadilan berdasarkan hukum yang berlaku [8].

Analisis forensik digital adalah alat penting untuk penegakan hukum yang dapat membantu mengidentifikasi kejahatan yang mungkin dilakukan dengan informasi digital. Spesialis forensik digital adalah ahli dalam mengekstrak informasi dari perangkat digital. Teknik forensik seluler adalah salah satu dari banyak spesifikasi yang mereka patuhi [9]. Dalam forensik digital terdapat banyak spesifikasi, salah satunya yaitu mobile forensik [10]. Mobile forensik merupakan ilmu untuk melakukan pengembalian barang bukti digital yang terdapat dalam perangkat mobile dengan data yang sesuai dengan forensik [11].

Metode penghilangan jejak digital dalam forensik digital dipecah menjadi dua teknik yaitu forensik hidup dan forensik statis [12]. Forensik statis menggunakan teknik dan pendekatan tradisional yang memproses bukti elektronik menggunakan gambar bit-by-bit untuk melakukan proses forensik di mana sistem yang berjalan tidak dihidupkan. Forensik langsung digunakan untuk menutupi beberapa kekurangan forensik statis; metode ini dijalankan ketika sistem berada dalam keadaan menyala untuk mengumpulkan bukti digital [13] [14]. Penyelidikan ini menggunakan aplikasi WhatsApp dalam mencari barang bukti dan menggunakan metode DFRWS dalam proses forensiknya.

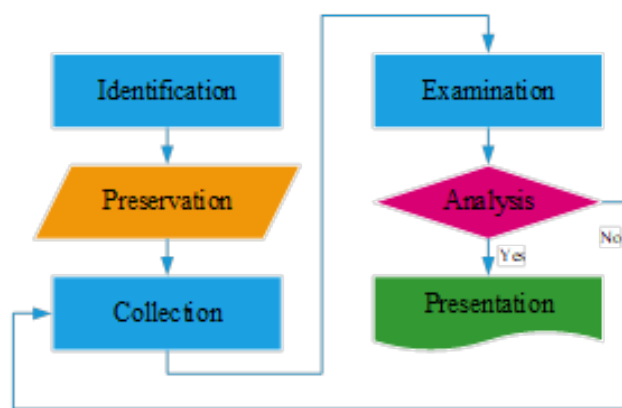
II. PENELITIAN YANG TERKAIT

Langkah-langkah forensik dapat mengimplementasikan salah satu dari 4 struktur beberapa standar yang digunakan dalam proses forensik seperti standar National Institute of Standards and Technology (NIST), National Institute of Justice (NIJ), Digital Forensics Integrated Investigation Framework (IDFIF), Digital Forensic Research Workshop (DFRWS), dan Association of Chief Police Officers (ACPO) atau langkah kerja proses dari forensik yang lain [15]. Pada penelitian ini metode akuisisi yang digunakan adalah metode Live Forensics dengan kerangka kerja forensik mengacu pada standar dari Digital Forensic Research Workshop (DFRWS).

Penelitian sebelumnya tentang Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist [16]. Penelitian ini menunjukkan proses pengambilan bukti digital pada aplikasi pesan Messenger Facebook. Barang bukti digital yang diperoleh berupa pesan teks, audio dan gambar. Penelitian lainnya yang berhubungan tentang mobile forensic adalah Analisis Bukti Digital Instagram Menggunakan Metode Nist [17]. Penelitian ini dapat memperoleh barang bukti pada Instagram berupa pesan teks, gambar, audio dan video.

III. METODE PENELITIAN

Penelitian yang dilakukan dengan menggunakan metode forensik digital yang dikembangkan oleh Digital Forensic Investigation Workshop (DFRWS). Metode DFRWS ini memberikan bukti mekanisme untuk merekam segala informasi yang dibutuhkan. Tahapan DFRWS memiliki beberapa tahapan sebagaimana yang ditunjukkan pada Gambar 1[18].



Gambar 1. Alur proses DFRWS

A. Identification

Tahap ini dilakukan untuk menentukan apa saja yang dibutuhkan dalam melakukan penyidikan dan pencarian barang bukti.

B. Preservation

Fase ini dilakukan untuk melindungi barang bukti digital, memastikan keaslian barang bukti, dan menyanggah klaim bahwa barang bukti tersebut dipalsukan.

C. Collection

Menyelesaikan proses menangkap mengidentifikasi potongan-potongan file atau data dari bukti dan mengidentifikasi sebagai sumber data.

D. Examination

Dengan melakukan langkah penentuan seleksi data pada bagian-bagian dari beberapa sumber data tertentu, seleksi data dilakukan dengan mengasumsikan bentuk dari data tetapi tanpa mengubah isi data karena keaslian data itu penting.

E. Analysis

Melakukan penentuan tentang di mana data tersebut dihasilkan, siapa yang membuatnya, bagaimana data tersebut dibuat, dan mengapa data dibuat.

F. Presentation

Penyajian dilakukan dengan menyajikan informasi yang dihasilkan dengan tahap analisis. Tahap penyajian terjadi setelah diperolehnya bukti tersebut dari proses investigasi kemudian analisis. Selain itu, fase ini menjelaskan alat dan metode yang digunakan, menentukan langkah-langkah dukungan yang diterapkan, dan membuat rekomendasi guna meningkatkan kebijakan atau perintah, metode, alat, atau aspek pendukung lainnya.

Untuk memudahkan pencarian bukti, fokusnya adalah pada pembuatan parameter pencarian bukti seperti yang ditunjukkan pada Tabel 1.

TABEL 1. PARAMETER YANG DIGUNAKAN

No	Parameter
1.	Application info
2.	Account info
3.	Conversation/Direct Messages
4.	Contact
5.	Audio
6.	Video
7.	Text
8.	Picture
9.	Document
10.	Deleted Messages
11.	IP Address
12.	Email/Phone Number
13.	Location

IV. HASIL DAN PEMBAHASAN

A. Identificaion

Tahap Plan ini disebut juga tahap perencanaan. Pada tahap ini, perangkat keras dan perangkat lunak yang akan digunakan dan tindakan yang akan diambil selama investigasi direncanakan. Perencanaan diperlukan agar proses penelitian dapat berjalan dengan lancar, termasuk menentukan alat-alat yang akan digunakan dalam proses penelitian sehingga dapat diperoleh hasil penelitian yang valid, selain memiliki rancangan tahap investigasi dan rencana simulasi uji pada tahap ini. Tabel 2 menunjukkan alat yang akan digunakan.

TABEL 2. SOFTWARE YANG DIGUNAKAN

Software	Kegunaan
<i>MOBILedit Forensic Express</i>	Mengekstrak data pada <i>smartphone</i>
<i>Hash my Files</i>	Memvalidasi barang bukti

Tabel 2 merupakan daftar *tools* yang digunakan dalam penelitian ini beserta penjelasan kegunaan masing-masing. Sedangkan spesifikasi perangkat keras yang digunakan untuk penelitian ini seperti pada Tabel 3.

TABEL 2. HARDWARE YANG DIGUNAKAN

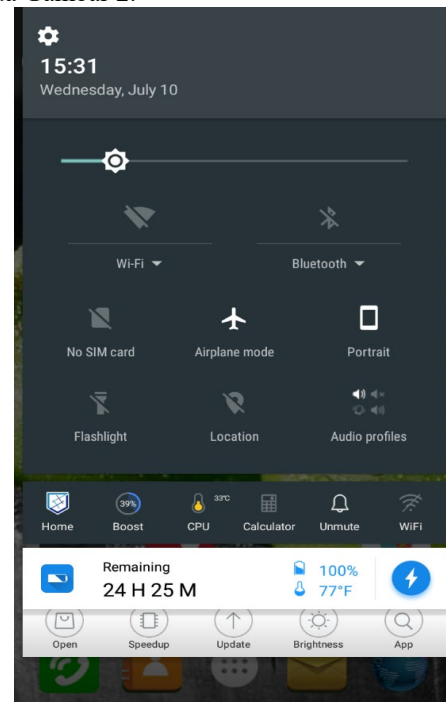
Jenis Spesifikasi	Spesifikasi
Laptop	Merk ASUS A45V
Smartphone	Manufacture Evercross
	Productt B75
	HW Revision LMY47D
	Platform Android
	SW Revision 5.1(22)
	Serial Number 0123456789ABCD EF
	Unlocking Pattern 3452
	IMEII 358441061746401

Tabel 3 merupakan spesifikasi *hardware* yang digunakan sehingga dapat menunjang kinerja dalam proses identifikasi forensik. Skenario penelitian yang digunakan sebagai parameter pengujian sudah dibuat pada tahap ini, pada skenario tersebut pelaku mengirim pesan kepada korbannya, kemudian bukti pesan yang didapat dianalisis untuk membuktikan keaslian barang bukti tersebut ketika diajukan sebagai barang bukti di pengadilan. Tujuan dibuatnya skenario penelitian ini selain sebagai parameter pengujian juga digunakan untuk menentukan tindakan-tindakan yang diperlukan pada proses penelitian.

B. Preservation

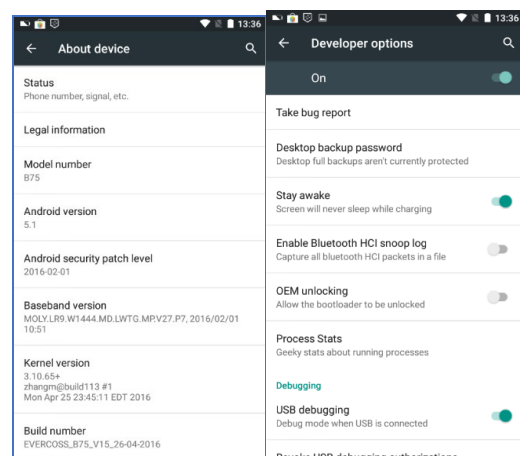
Tahap kedua adalah tahap untuk melindungi barang bukti berupa digital, guna untuk memastikan keaslian bukti dan klaim barang bukti yang telah dirusak. Proses proteksi integrasi dilakukan untuk menjaga keutuhan barang bukti dengan cara mengisolasi barang bukti berupa fisik dan membuat salinan cadangan kloning atau pemrosesan file citra tersebut. Tahaan selanjutnya yaitu mengisolasi perangkat dari koneksi internet.

Isolasi diperlukan untuk mencegah dari sesuatu yang bisa merusak bukti atau membahayakan keaslian data yang dikandungnya. Kegiatan yang dilakukan untuk isolasi yaitu mengubah status perangkat ke mode tanpa internet / pesawat seperti ada Gambar 2.



Gambar 1. Menonaktifkan mode pesawat

Aktifkan *Developer Option* untuk proses forensik, untuk mengaktifkannya dengan menekan tulisan *Build Number* pada *smartphone* sebanyak 7 kali. Apabila proses aktivasi sudah berhasil, maka langkah selanjutnya pada menu *Developer Options* adalah mengaktifkan opsi *Stay Awake* dan *USB Debugging* untuk proses forensik. *Stay Awake* diperlukan supaya perangkat *smartphone* tidak dalam mode *sleep* apabila tidak digunakan beberapa saat ketika melakukan proses forensik karena dapat mengaktifkan system pengamanan perangkat *smartphone*. *USB Debugging* digunakan untuk memberi izin kepada perangkat *smartphone* untuk melakukan komunikasi dengan *workstation* menggunakan kabel USB dan ADB. Gambar 3 merupakan cara mengaktifkan mode *developer* dan *stay awake*.

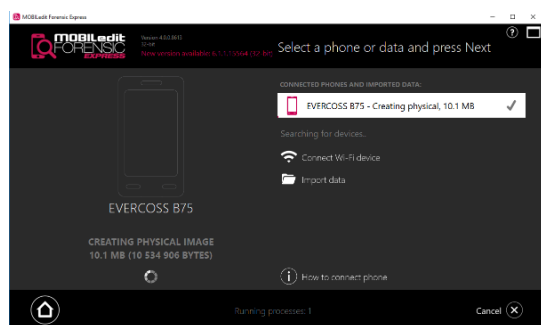


Gambar 2. Mengaktifkan mode *developer* dan *stay awake*

C. Collection

Fase perekaman barang bukti digital di smartphone dikaitkan dengan tingkat risiko tinggi. Apabila terdapat kesalahan, data dan bukti digital pada smartphone dapat hilang atau rusak dan mengakibatkan data tidak terbaca. Maka barang bukti itu harus dijaga. Artinya, membuat salinan cadangan atau gambar yang menjadi bukti.

Tools yang digunakan dalam melakukan *backup* adalah MOBILedit Forensic Express. Kemampuan alat ini adalah dapat membuat cadangan sistem *smartphone* dan mengekstraknya. Gambar 4. merupakan proses *backup* pada *smartphone*.



Gambar 3. Proses *backup* *smartphone*

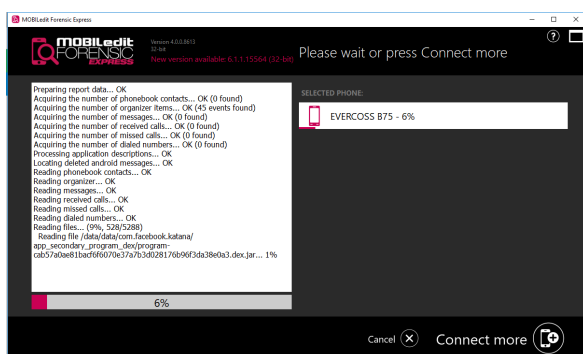
Hasil proses backup adalah dokumen gambar *smartphone* dengan format file *.img* dan dokumen yang bervariasi bergantung jumlah data dalam *smartphone*. Gambar 5. adalah hasil dari proses backup.

Name	Date modified	Type	Size
EVERCOSS B75 (2019-07-09 17h01m00s)	7/9/2019 5:30 PM	File folder	
samsung SM-G130H (2019-07-08 22h03...)	7/8/2019 10:29 PM	File folder	
EVERCOSS B75	7/9/2019 4:53 PM	Disc Image File	15,267,840 ...
EVERCOSS B75.img_info	7/9/2019 4:53 PM	WinRAR ZIP archive	3 KB
samsung SM-G130H	7/8/2019 9:58 PM	Disc Image File	3,817,472 KB
samsung SM-G130H.img_info	7/8/2019 9:58 PM	WinRAR ZIP archive	2 KB

Gambar 4. Hasil proses *backup*

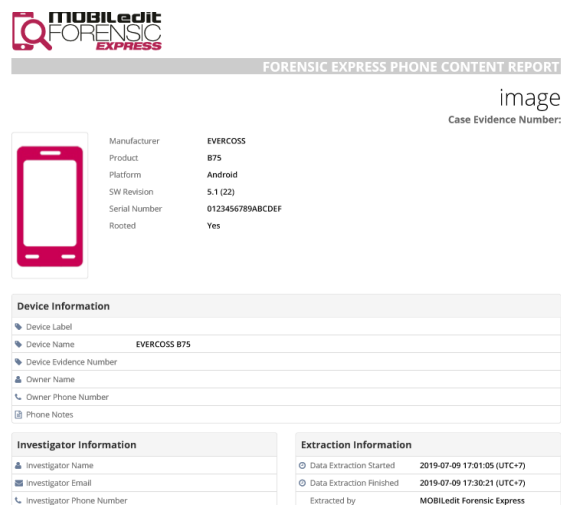
Setelah backup selesai, kemudian mengekstrak data dengan alat MOBILedit Forensic Express. Pada tahap ini, Anda harus terlebih dahulu menghubungkan barang bukti atau *smartphone* ke komputer tempat MOBILedit Forensic Express diinstal.

D. Examination



Gambar 5. Proses ekstraksi data *smartphone*

Hasil ekstraksi yang dilakukan disajikan dalam laporan lengkap dalam penelitian ini. Laporan lengkap yang dipilih dalam format *.pdf*, melihat laporan lengkap untuk tujuan bukti adalah seperti yang ditunjukkan pada Gambar 7.



Gambar 6. Full report pada MOBILedit

E. Analysis

Hasil ekstraksi yang sudah didapat dari *file image* dilakukan proses *hashing* untuk mengecek keaslian barang bukti digital. Gambar 8. Ekstraksi merupakan contoh barang bukti yang didapat berjenis audio.

Name	Date modified	Type	Size
PTT-20190609-WA0001	6/9/2019 12:49 PM	AIMP: Opus Audio	8 KB
PTT-20190609-WA0002	6/9/2019 4:26 PM	AIMP: Opus Audio	10 KB
PTT-20190609-WA0003	6/9/2019 5:14 PM	AIMP: Opus Audio	19 KB
PTT-20190609-WA0004	6/9/2019 5:19 PM	AIMP: Opus Audio	3 KB
PTT-20190609-WA0005	6/9/2019 5:33 PM	AIMP: Opus Audio	21 KB
PTT-20190609-WA0006	6/9/2019 5:33 PM	AIMP: Opus Audio	8 KB

Gambar 7. Hasil ekstraksi

Hasil ekstraksi yang telah disimpan kemudian proses *hashing* dilakukan untuk menentukan nilai *hash* dalam *file*. Gambar 9 merupakan perbandingan nilai *hashing* pada *file* audio hasil ekstraksi *image* dengan *file* asli pada *smartphone*.

Filename	MD5	SHA1
PTT-20190609-WA0001	96746007c56086570a3e92a378d49a44	373a5319c5d9dd66ab6b8e60256cd3881f32a...
PTT-20190609-WA0002	6b7483e1c6e40c71891d41e870474f0b	beedd44ca25638e5c8531d623d44cc359cb273...
PTT-20190609-WA0003	020a40f2b5d7123c03b66894be9549f9	78ed15ed694af6a0453adcb6c3fab1996f28...
PTT-20190609-WA0004	8c8cc9f653a94dc240d09c500557bec6	8f490ab621ae38456e8a2d53f7a398b938f...
PTT-20190609-WA0005	d192481b135d63f1d9fde475b332310	136076f17b00cf5782150d520b85cb539740104...
PTT-20190609-WA0006	dfbc439c8553ef983e9adb2067300cd1	cb7965d00a442ef96547c6f521677e1f118608c8

Gambar 8. Proses *hashing*

Gambar 9 menunjukkan hasil perbandingan dari kedua barang bukti asli dari *smartphone* dengan hasil ekstraksi *image*. Terdapat persamaan warna pada gambar sehingga dapat dikatakan barang bukti tersebut tervalidasi masih asli.

F. Presentation

Tahap *Analyze* menunjukkan bahwa penggunaan metode DFRWS dapat membuktikan keaslian barang bukti. Hal ini dibuktikan dengan pendeteksian menggunakan tools *MOBILedit Forensic Express* dan *HashmyFiles*. Tabel 4 menunjukkan hasil keseluruhan yang diperoleh dari penelitian menggunakan tools tersebut.

TABEL 3. HASIL PENGAMBILAN BARANG BUKTI

No	Hasil yang diperoleh	MOBILedit Forensic Express
1.	Application info	√
2.	Account info	√
3.	Conversation/Direct Messages	√
4.	Contact	√
5.	Audio	√
6.	Video	√
7.	Text	√
8.	Picture	√
9.	Document	√
10.	Deleted Messages	√
11.	IP Address	x
12.	Email/Phone Number	√
13.	Location	x

Tabel 4 menunjukkan bahwa keseluruhan hasil forensik dapat mendeteksi adanya barang bukti digital. *MOBILedit* dapat mengambil data *WhatsApp* pada *smartphone*, sedangkan *HashMyFiles* dapat mendeteksi keaslian barang bukti. Indeks akurasi dalam pengukuran setiap pengenalan dapat dihitung dengan Persamaan 1 untuk akurasi [19].

$$Par = \frac{\sum ar0}{\sum arT} \times 100\%$$

(1)

dengan *Par* merupakan nomor indeks tools forensik yang digunakan, *ar0* merupakan jumlah bahan terdeteksi oleh alat forensik, dan *arT* merupakan jumlah total bahan digunakan.

Maka perhitungan indeks untuk mengukur kemungkinan setiap deteksi dapat dihitung sebagai berikut.

MOBILedit Forensic Express,

$$Par = \frac{11}{13} \times 100\% = 84,6\%$$

Hashmyfile,

$$Par = \frac{13}{13} \times 100\% = 100\%$$

Berdasarkan perhitungan akurasi alat dan teknik forensik yang digunakan, maka diperoleh bahwa *MOBILedit Forensic Express* memiliki akurasi sebesar 84,6%. Sedangkan

kemampuan deteksi *HashMyFiles* dapat mendeteksi sebesar 100%

V. KESIMPULAN

Barang bukti digital pada kasus cybercrime menggunakan aplikasi *WhatsApp* dapat diperoleh dan dideteksi menggunakan metode DFRWS dengan tools *MOBILedit Forensic Express* dan *Hashmyfiles*. Perbandingan kinerja tools dapat menghasilkan analisa yang membuktikan dengan menunjukkan akurasi pada tools *MOBILedit Forensic Express* mempunyai kemampuan akurasi sebesar 84,6%. Sedangkan kemampuan deteksi *HashMyFiles* dapat mendeteksi sebesar 100%. Hasil dari barang bukti dapat digunakan untuk keperluan pengadilan

UCAPAN TERIMA KASIH

Terimakasih kepada Allah SWT yang telah melimpahkan Kesehatan dan keberkahan dalam hidup, terimakasih juga saya sampaikan kepada para dosen pembimbing yang telah membimbing saya dengan penuh rasa sabar. Serta istri saya yang sebentar lagi akan melahirkan anak kita yang pertama, semoga lancar selalu.

DAFTAR PUSTAKA

- [1] W. A. Mukti, S. U. Masruroh, and D. Khairani, "Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android," *J. Tek. Inform.*, vol. 10, no. 1, pp. 73–84, 2017, doi: 10.15408/jti.v10i1.6820.
- [2] M. Zaini and S. Soenarto, "Persepsi Orangtua Terhadap Hadirnya Era Teknologi Digital di Kalangan Anak Usia Dini," *J. Obs. J. Pendidik. Anak Usia Dini*, vol. 3, no. 1, p. 254, 2019, doi: 10.31004/obsesi.v3i1.127.
- [3] Ramalia, Armaita, and P. Vandelis, "Hubungan Ketergantungan Smartphone dengan Kecemasan (Nomophobia)," *J. Kesehat.*, vol. 10, no. 2, pp. 89–93, 2019.
- [4] G. M. Zamroni, R. Umar, and I. Riadi, "Analisis Forensik Aplikasi Instant Messaging Berbasis Android," *Pros. Ilmu Komput.*, vol. 2, no. 1, pp. 102–105, 2016.
- [5] 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, 2016.
- [6] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 1, 2017, doi: 10.26555/jiteki.v3i1.6643.
- [7] S. Madiyanto, H. Mubarak, and N. Widiyasono, "Mobile Forensics Investigation Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS," *J. Rekayasa Sist. Ind.*, vol. 4, no. 01, pp. 93–98, 2017,

doi: 10.25124/jrsi.v4i01.149.

- [8] A. Febriyanto and I. Sembiring, "Uji Perbandingan Tools Mobile Forensic Pada Platform Java, Blackberry dan Android," Universitas Kristen Satya Wacana, 2016.
- [9] A. T. A., S. Michrandi, and B. Irawan, "Analisis dan Implementasi Mobile Forensik Pemulihan Data yang Hilang pada Smartphone Berbasis Sistem Operasi Android," *J. Eproc*, vol. 60, no. 507, pp. 499–500, 2015.
- [10] I. Riadi, Sunardi, and Sahiruddin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, pp. 87–95, 2019.
- [11] I. Riadi, A. Yudhana, and I. Anshori, "Analisis Forensik Aplikasi Instant Messenger pada Smartphone Berbasis Android," *J. Insa. Comtech*, vol. 2, no. 2, pp. 25–32, 2017.
- [12] R. Umar, A. Yudhana, and M. N. Faiz, "Experimental Analysis of Web Browser Sessions Using Live Forensics Method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 2951–2958, 2018, doi: 10.11591/ijece.v8i5.pp.2951-2958.
- [13] R. A. Ramadhan, Y. Prayudi, and B. Sugiantoro, "Implementasi dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive (SSD)," *Teknomatika*, vol. 9, no. 2, pp. 1–13, 2017, [Online]. Available: <http://teknomatika.stmikayani.ac.id/wp-content/uploads/2017/07/1.pdf>.
- [14] I. Riadi and E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *J. Tek. Elektro*, vol. 10, no. 1, pp. 18–22, 2018.
- [15] I. Ansori, "Identifikasi dan Analisis Bukti Digital Facebook Messenger Menggunakan Metode National Institute of Standards Technology (NIST)," Universitas Ahmad Dahlan, 2019.
- [16] 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.
- [17] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," vol. 5, no. 2, pp. 235–247, 2018.
- [18] 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.
- [19] 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.