Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 1112-1120
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Analisis Penggunaan Metode ACPO (*Association of Chief Police Officer*) pada Forensik WhatsApp

Riski Yudhi Prasongko[1], Anton Yudhana[2], Imam Riadi[3]
[1,2,3]Megister Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
e-mail: eyudhana@ee.uad.ac.id, imam.riadi@is.uad.ac.id,
riski1807048022@webmail.uad.ac.id

Abstract

The development of smartphone technology is increasing, causing cyber crime to increase from year to year. One of the smartphone applications used by criminals is WhatsApp. The WhatsApp application is one of the most widely used insta messaging applications, especially in Indonesia. Violations such as hate speech, defamation, and fraud are common on the WhatsApp social network. This study was conducted with the aim of finding forensic evidence of cyberbullying behavior on the WhatsApp insta messaging application using the Association of Chiefs of Police (ACPO) method. This forensic phase involves planning, arresting, analyzing and presenting to search for digital evidence of cybercrimes using Belkasoft Evidence Center and HashMyFiles software. Digital evidence on smartphones can be found using case scenarios with 13 parameters that have been generated. The results of this study indicate that the Belkasoft Evidence Center digital forensic software is 81.92%, while HashMyfiles can detect the authenticity of digital evidence 79.96%.

Keywords: *Digital evidence, ACPO, Forensics*

Abstrak

Perkembangan teknologi smartphone yang semakin meningkat menyebabkan kejahatan dunia maya semakin meningkat dari tahun ke tahun. Salah satu aplikasi smartphone yang digunakan oleh para penjahat adalah WhatsApp. Aplikasi WhatsApp adalah salah satu aplikasi perpesanan insta yang paling banyak digunakan terutama di Indonesia. Pelanggaran seperti ujaran kebencian, pencemaran nama baik, dan penipuan sering terjadi di jejaring sosial WhatsApp. Penelitian ini dilakukan dengan tujuan untuk menemukan bukti forensik perilaku cyberbullying pada aplikasi pesan insta WhatsApp menggunakan metode Association of Chiefs of Police (ACPO). Fase forensik ini melibatkan perencanaan, penangkapan, analisis, dan penyajian untuk mencari bukti digital kejahatan dunia maya menggunakan perangkat lunak Belkasoft Evidence Center dan HashMyFiles. Bukti digital pada smartphone dapat ditemukan menggunakan skenario kasus dengan 13 parameter yang telah dihasilkan. Hasil penelitian ini menunjukkan bahwa perangkat lunak forensik digital Belkasoft Evidence Center 81,92%, sedangkan HashMyfiles dapat mendeteksi keaslian bukti digital 79,96%.

Kata kunci: *Bukti digital, ACPO, Forensik*

1. PENDAHULUAN

Perkembangan teknologi saat ini sangat pesat, seperti halnya dengan Evolusi teknologi smartphone dengan sistem operasi Android telah Dilengkapi dengan sejumlah fitur canggih[1]. Semakin banyak fitur dan Aplikasi pesan instan tersedia di smartphone, salah satunya adalah adalah WhatsApp. *Aplikasi pesan instan termasuk dalam perangkat lunak ponsel berbasis Android yang berkembang pesat dengan banyak nama seperti WhatsApp, IMO Messenger, Kakaotalk, Line, WeChat, MiChat, Telegram dan banyak lagi. WhatsApp merupakan salah satu dari sekian banyak aplikasi*

perpesanan lintas platform untuk smartphone dan merupakan aplikasi yang paling banyak digunakan di Indonesia[2].

Peningkatan jumlah pengguna aplikasi WhatsApp akan berdampak pada peningkatan aktivitas kriminal digital menggunakan WhatsApp. Oleh karena itu, analisis forensik digital diperlukan untuk mengumpulkan informasi berharga yang terkandung dalam smartphone Android dan mendapatkan data dan bukti kriminal[3]. WhatsApp adalah aplikasi pesan instan smartphone. Dari fungsinya, WhatsApp hampir sama dengan aplikasi SMS yang biasa digunakan di ponsel lawas. WhatsApp tidak menggunakan pulsa tapi data internet. Selain itu, WhatsApp dapat mengirim pesan teks, suara, gambar, video, dan dokumen secara real time [4]. Teknik pengambilan data akuisisi dilakukan dengan menggunakan metode pencitraan fisik untuk mendapatkan akses penuh ke memori smartphone. Hasil analisis dirangkum dalam bentuk tabel perbandingan. Tabel ini dapat digunakan oleh penyidik forensik saat menyelidiki aplikasi pesan instan yang sedang diselidiki. Analisis mengungkapkan bahwa kami menemukan bukti digital aktivitas berbagi pesan, file media, dan kontak[5].

Proses analisis dilakukan dengan menggunakan alat bukti digital dari penggunaan fitur aplikasi WhatsApp, sehingga proses pendataan didukung dengan simulasi beberapa skenario yang dapat terjadi pada saat terjadinya tindak pidana meningkat. Teknik pengambilan data akuisisi dilakukan dengan menggunakan metode pencitraan fisik untuk mendapatkan akses penuh ke memori smartphone[6]. Hasil analisis dirangkum dalam bentuk tabel perbandingan. Tabel ini dapat digunakan oleh penyidik forensik saat menyelidiki aplikasi pesan instan yang sedang diselidiki. Analisis mengungkapkan bahwa kami menemukan bukti digital aktivitas berbagi pesan, file media, dan kontak[7].

Hasil analisis juga memberikan penjelasan tentang kemungkinan pemulihan barang bukti digital yang terhapus dan cara memulihkannya menggunakan teknik pengukiran data[8]. Penelitian ini berfokus pada pemeriksaan forensik terhadap data dan informasi yang disimpan oleh aplikasi pada telepon dan teknik ekstraksi data forensik. Inspeksi forensik smartphone Android harus mengikuti teknik forensik yang sesuai. Perangkat, lingkungan, dan teknologi yang digunakan harus mematuhi aturan forensik komputer[9].

Cyberbullying merupakan istilah yang ditambahkan ke *Oxford English Dictionary* (OED) pada tahun 2010. Istilah ini mengacu pada penggunaan teknologi informasi untuk menggoda orang dengan mengirim atau memposting teks yang mengancam atau mengintimidasi[10]. Proses investigasi forensik digital pada komputer atau perangkat serupa dapat dilakukan dengan menggunakan dua metode akuisisi, forensik langsung dan forensik statis.

Alur kerja forensik dapat mengimplementasikan salah satu dari beberapa kerangka kerja standar yang digunakan dalam proses forensik. Diantaranya *National Institute of Standards and Technology* (NIST), *National*

Institute of Justice (NIJ), *Integrated Digital ForensicsInvestigation Framework* (IDFIF), *Digital Forensic Research Work Shop* (DFRWS), *Association of Chief Police Officers* (ACPO)) atau Proses forensik lainnya kerangka[11]. Dalam penelitian ini, metode akuisisi yang digunakan adalah metode static forensik yang menggunakan framework ACPO.

2. METODOLOGI PENELITIAN

Metode ACPO digunakan untuk menjabarkan gambaran proses investigasi forensik yang sedang dilakukan sehingga dapat diketahui tahapan-tahapannya secara lebih jelas dan mudah dipahami. Tahapan metode penelitian dapat dilihat pada Gambar 1.

Gambar 1. Skema Metode ACPO

2.1. Plan

Proses perencanaan dimulai dengan menentukan hardware dan software yang diperlukan untuk proses penelitian agar dapat memperoleh hasil penelitian. Proses perencanaan dimulai dari menentukan alat dan bahan penelitian, alat penelitian dapat berupa hardware dan software yang sudah ditentukan sesuai dengan kegunaannya masing-masing.

2.2. Capture

Tahap ini merupakan tahap merekam, menyimpan, menangkap, dan mengumpulkan semua hasil yang di dapat dari proses penelitian. Proses capture pada hasil yang diperoleh dari proses penelitian dapat menggunakan bantuan dari software yang ada atau dapat juga menggunakan bantuan hardware. Penelitian akan melakukan identifikasi data yang dapat dijadikan barang bukti tidak kejahatan.

2.3. Analyze

Tahap ini dilakukan analisis terhadap semua temuan pada proses penelitian dengan membuat perbandingan dari setiap temuan untuk dapat diambil data yang valid tentang proses penelitian. Bukti digital temuan yang sudah diperoleh dianalisis menggunakan tools forensik tertentu untuk kemudian diambil kesimpulan

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 1112-1120
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

2.4. Present

Tahap ini dilakukan penjelasan tentang semua tindakan yang telah dilakukan pada saat penelitian dan menjelaskan secara detail tentang hasil dari penelitian tersebut serta memberikan masukan atau saran yang berhubungan dengan hasil dari penelitian tersebut.

3. HASIL DAN PEMBAHASAN

Pada bagian ini akan membahas mengenai penggunaan metode ACPO dapa Forensik WhatsApp

3.1. Plan

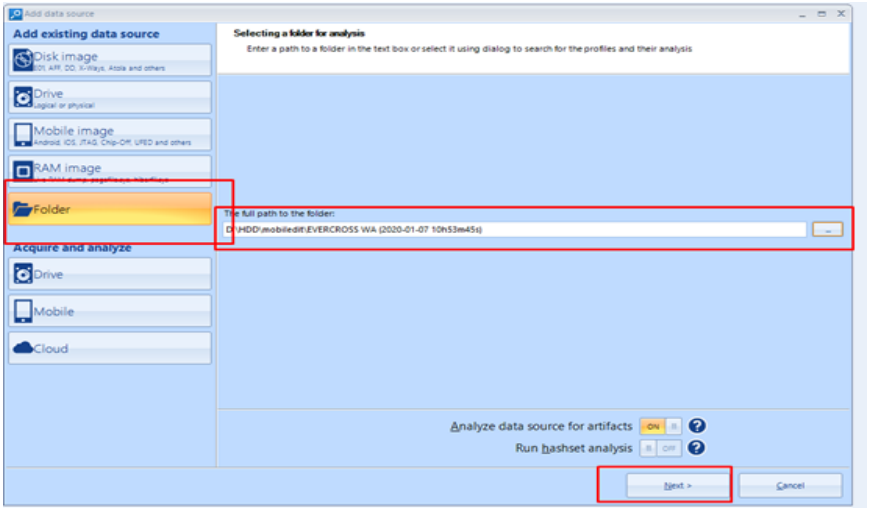
Perencanaan merupakan proses merencanakan software yang digunakan dan tindakan-tindakan yang akan dilakukan pada saat penelitian. Perencanaan diperlukan agar proses penelitian berjalan lancar termasuk dalam menentukan tools yang digunakan pada proses penelitian agar dapat diperoleh hasil penelitian yang valid, selain itu pada tahap ini juga dibuat skema tahap penelitian dan skema simulasi pengujian.

Tabel 1. *Tools* yang digunakan

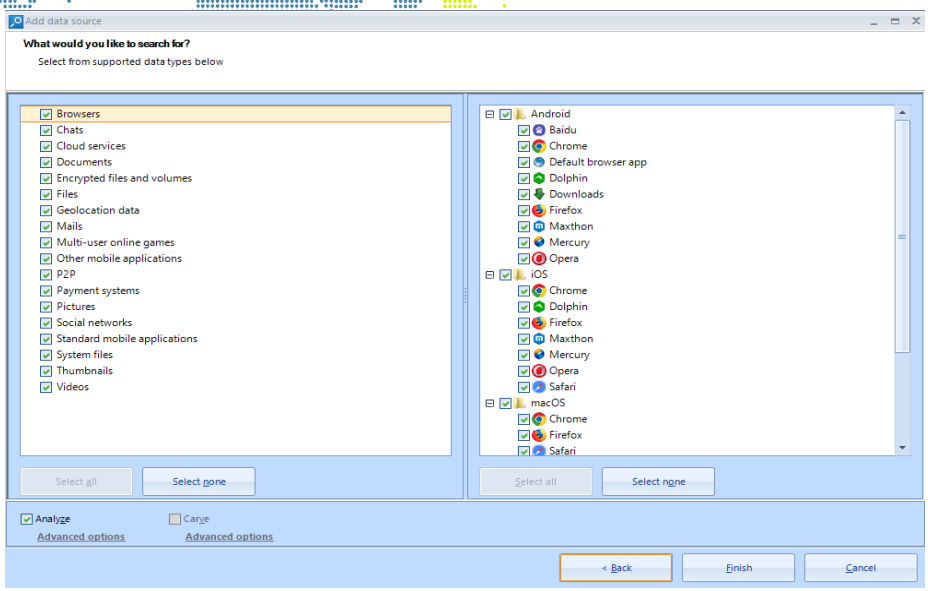
Software	**Kegunaan**
Belkasoft Evidence Center	Menganalisis hasil temuan
Hash my Files	Memvalidasi barang bukti

3.2. Capture

Tahapan pertama yang dilakukan pada proses capture ini adalah tahap pemeliharaan untuk menjaga barang bukti digital, memastikan keaslian barang bukti, dan menyangkal klaim bahwa barang bukti telah dilakukan sabotase. Proses penjagaan integrasi dilakukan untuk menjaga barang bukti itu asli dan tidak rusak, dengan teknik isolasi barang bukti fisik dan pembuatan backup berupa cloning atau proses image file dari barang bukti tersebut.

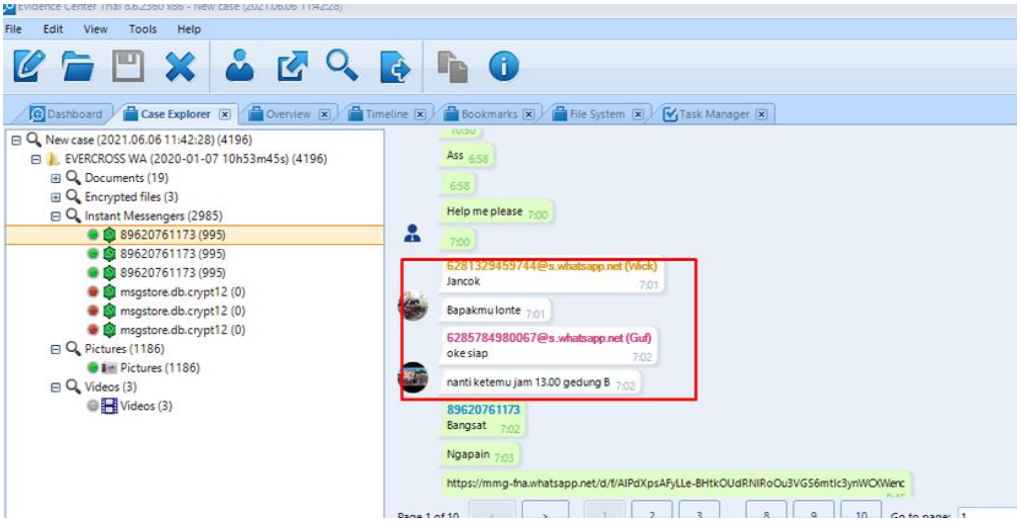


Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 1112-1120
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti



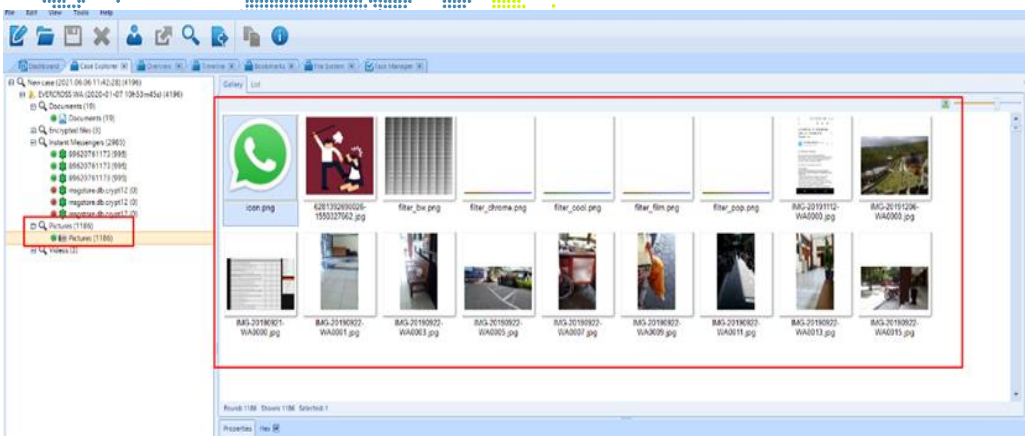
Gambar 1. Proses pada Belkasoft

Gambar 1 merupakan cara menganalisis hasil temuan pada MOBILedit sedangkan gambar kedua terdapat pilihan untuk menganalisis jenis file yang akan diproses. Hasil analisis yang didapat berupa beberapa barang bukti seperti teks, gambar, contact, dan video. Gambar dibawah ini menunjukkan barang bukti yang diperoleh.



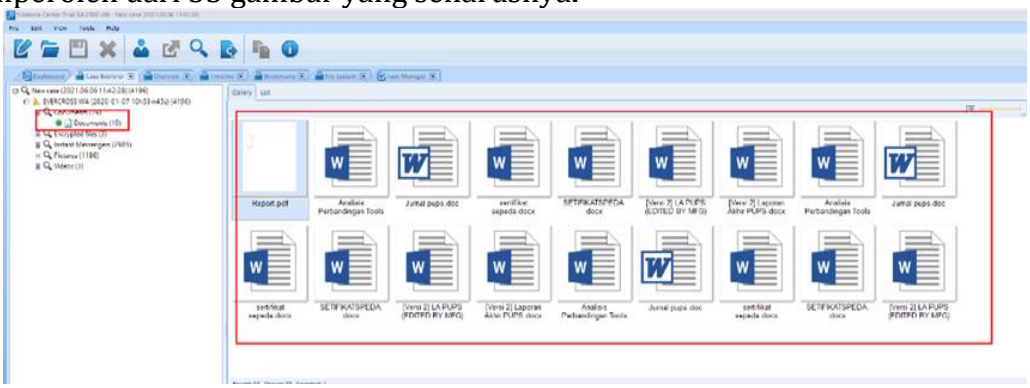
Gambar 2. Barang bukti berupa teks

Gambar 2 menunjukkan barang bukti yang didapat dalam bentuk teks/chat. Pada chat tersebut terdapat indikasi cyberbully karena mengandung kalimat negatif yang berupa hujatan kepada korban.



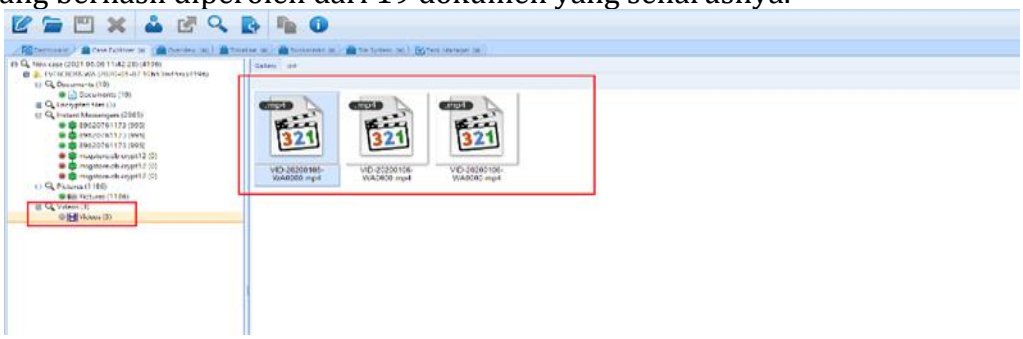
Gambar 3. Barang bukti berupa gambar

Gambar 3. Merupakan hasil gambar yang sudah diperoleh ketika proses ekstraksi. Berdasarkan gambar diatas terdapat 18 gambar yang berhasil diperoleh dari 33 gambar yang seharusnya**.**



Gambar 4. Barang bukti berupa dokumen

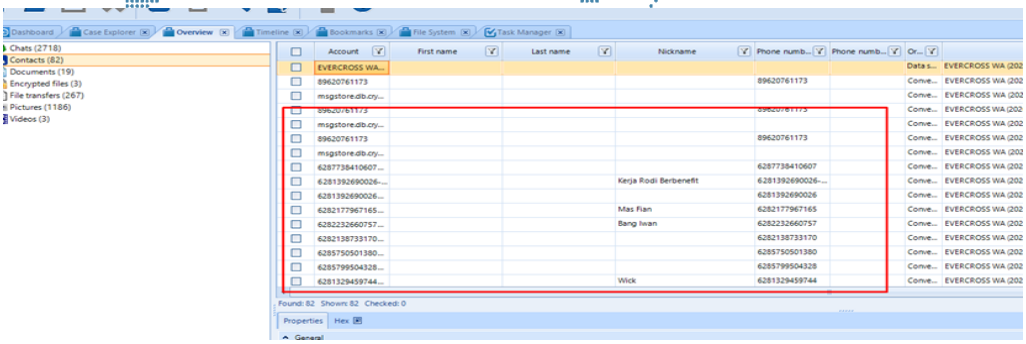
Gambar 4. Merupakan hasil barang bukti dokumen yang sudah diperoleh ketika proses ekstraksi. Dari gambar diatas terdapat 17 dokumen yang berhasil diperoleh dari 19 dokumen yang seharusnya.



Gambar 5. Barang bukti berupa video

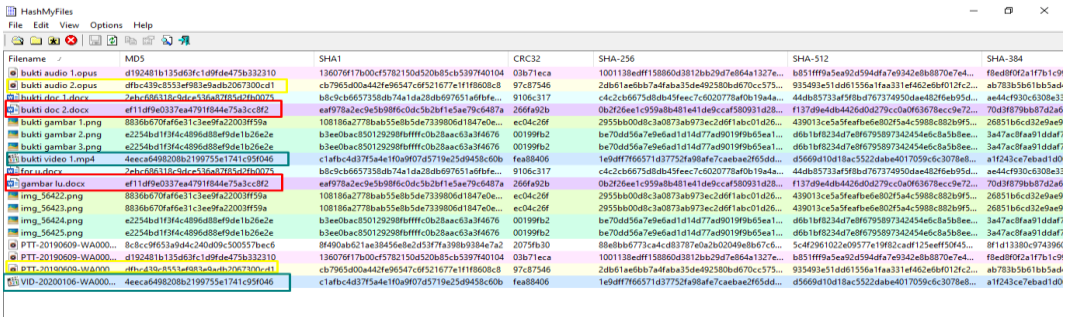
Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 1112-1120
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Gambar 5. Merupakan hasil barang bukti video yang sudah diperoleh ketika proses ekstraksi. Terdapat 3 bukti video yang diperoleh dari 3 video yang seharusnya.



Gambar 6. Barang bukti berupa kontak

Gambar 6. Merupakan hasil barang bukti dari 82 contact yang didapat ketika proses ekstrasi.



Gambar 7. Hasil nilai hashing barang bukti

3.3. Analyze

Analisis tool yang menggunakan Belkasoft Evidence Center, dari jumlah barang bukti yang sudah terlampir pada dibawah ini, setelah dilakukan proses ekstraksi menggunakan Belkasoft didapat beberapa barang bukti yang dapat diekstraksi seperti pada text dan video adalah hasil ekstraksi menggunakan Belkasoft.

Tabel 2. Hasil ekstraksi menggunakan Belkasoft

No	Hasil yang diperoleh	Jumlah	Belkasoft Evidence Center	Presentase
1.	Application info	1	1	81,92 %
2.	Account info	1	1	
3.	Conversation/ Digest Messages	8	8	
4.	Contact	21	21	
5.	Audio	3	0	
6.	Video	1	1	
7.	Text	996	996	
8.	Picture	33	33	
9.	Document	2	2	

No	Hasil yang diperoleh	Jumlah	Belkasoft Evidence Center	Presentase
10.	Deleted Messages	1	1	
11.	IP Adress	1	0	
12.	Email/Phone Number	1	1	
13.	Location	1	0	

Berikutnya alisis tool yang menggunakan HashMyFiles Evidence Center, tool ini digunakan untuk membandingkan hasil file hasil ekstraksi dengan file aslinya. Jika setelah dibandingkan mempunyai nilai hash sama, maka barang bukti tersebut masih asli dan belum termodifikasi. Jenis file yang dapat dibandingkan nilai hash-nya adalah Audio, Video, Picture, dan Document.

Tabel 3. Perbandingan hasil file hasil ekstraksi dengan file aslinya

No	Hasil yang diperoleh	Jumlah	HashMyFiles	presentase
1.	Application info	1	0	79,69 %
2.	Account info	1	0	
3.	Conversation/ Digest Messages	8	0	
4.	Contact	21	0	
5.	Audio	3	3	
6.	Video	1	1	
7.	Text	996	996	
8.	Picture	33	33	
9.	Document	2	2	
10.	Deleted Messages	1	0	
11.	IP Adress	1	0	
12.	Email/Phone Number	1	0	
13.	Location	1	0	

3.4. Present

Tahap Analyze menunjukkan bahwa penggunaan metode ACPO dapat mengakuisisi data barang bukti. Hal ini dibuktikan dengan pendeteksian menggunakan Belkasoft Evidence Center dan HashMyFiles.

Tabel 4. Hasil pendeteksian Belkasoft Evidence Center dan HashMyFiles.

No	Hasil yang diperoleh	Jumlah	Belkasoft Evidence Center	HashMyFiles
1.	Application info	1	1	0
2.	Account info	1	1	0
3.	Conversation/ Digest Messages	8	8	0
4.	Contact	21	21	0
5.	Audio	3	0	3
6.	Video	1	1	1
7.	Text	996	996	996
8.	Picture	33	33	33
9.	Document	2	2	2
10.	Deleted Messages	1	1	0
11.	IP Adress	1	0	0
12.	Email/Phone Number	1	1	0
13.	Location	1	0	0
	Persentase		81,92%	79,69%

4. SIMPULAN

Belkasoft Evidence Center, dan HashMyfiles dapat menghasilkan ekstraksi data pada smartphone serta dapat membuktikan validitas pada barang bukti. Perbandingan kinerja *tools* dapat menunjukkan akurasi *tools*, Belkasoft Evidence Center sebesar 81,92%, sedangkan Hashmyfiles memiliki akurasi sebesar 79,69%.

DAFTAR PUSTAKA

[1] Ali. Ammar Hammad, S. A. M. (2017). Design of Secure Chatting Application with End to End Encryption for Android Platform. Iraqi Journal for Computers and Informatics, 43(1), 22–27.

[2] Asyaky, M. S. (2019). Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android. Jurnal & Penelitian Teknik Informatika, Vol. 3 No(1), 220–231.

[3] Casey, E. (2011). Digital Evidence and Computer Crime, Third Edition. 840.

[4] Fauzan, A., Riadi, I., & Fadlil, A. (2017). Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime. Annual Research Seminar (ARS), 2(1), 159–163.

[5] Hariyadi, D., Winarno, W. W., Luthfi, A., Informatika, M., Teknologi, F., & Indonesia, U. I. (2014). Abstrak. 81–89.

[6] Ikhsani, S., & Hidayanto, C. (2016). Analisa Forensik Whatsapp dan LINE Messenger Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia. Jurnal Teknik ITS, 5(2).

[7] Kunang, Y. N. (2017). Implementasi Prosedur Forensik Untuk Aplikasi Whatsapp Pada Ponsel Android. Jurnal Informatika, 11(1), 21.

[8] Lionnie, R., Kadarina, T. M., & Alaydrus, M. (2018). Analisis Metode SIFT dan SURF untuk Sistem Pendeteksi Gambar Termanipulasi Penyerangan Copy-Move Forgery. Jurnal Telekomunikasi Dan Komputer, 8(3), 183.

[9] Madiyanto, S., Mubarok, H., & Widiyasono, N. (2017). Mobile Forensics Investigation Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS. Jurnal Rekayasa Sistem & Industri, 4(01), 93–98.

[10] Maryanto, B. (2008). Penggunaan Fungsi Hash Satu-Arah Untuk Enkripsi Data. Media Informatika, 7(3), 138–146.

[11] Mukti, W. A., Masruroh, S. U., & Khairani, D. (2017). Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android. Jurnal Teknik Informatika, 10(1), 73–84.