HASIL CEK_60020397_Point-C43-IRD-850GB-Comparative analysis of Forensic Tools on Twitter applications using the DFRWS method

by Imam Riadi 60020397

Submission date: 11-Dec-2020 10:26AM (UTC+0700)
Submission ID: 1471677168
File name: orensic_Tools_on_Twitter_applications_using_the_DFRWS_method.pdf (1.07M)
Word count: 3477
Character count: 21411

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. 5 (2020) 829 - 836 ISSN Media Elektronik: 2580-0760

Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop

Ikhsan Zuhriyanto[1], Anton Yudhana[2] dan Imam Riadi[3]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan
[2]Program Studi Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan
[3]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan
Email: [1]Ikhzann@gmail.com*, [2]eyudhana@ee.uad.ac.id, [3]imam.riadi@is.uad.ac.id

Abstract - *Current crime is increasing, one of which is the crime of using social media, although no crime does not leave digital evidence. Twitter application is a social media that is widely used by its users. Acts of crime such as fraud, insults, hate speech, and other crimes lately use many social media applications, especially Twitter. This research was conducted to find forensic evidence on the social media Twitter application that is accessed using a smartphone application using the Digital Forensics Research Workshop (DFRWS) method. These digital forensic stages include identification, preservation, collection, examination, analysis, and presentation in finding digital evidence of crime using the MOBILedit Forensic Express software and Belkasoft Evidence Center. Digital evidence sought on smartphones can be found using case scenarios and 16 variables that have been created so that digital proof in the form of smartphone specifications, Twitter accounts, application versions, conversations in the way of messages and status. This study's results indicate that MOBILedit Forensic Express digital forensic software is better with an accuracy rate of 85.75% while Belkasoft Evidence Center is 43.75%.*

Keywords: Digital Forensics, DFRWS, Mobile Forensics, Social Media, Twitter

Abstrak - Tindak kejahatan saat ini semakin meningkat salah satunya adalah kejahatan menggunakan media sosial, walaupun tidak ada kejahatan yang tidak meninggalkan bukti digital. Aplikasi Twitter adalah salah satu media sosial yang banyak digunakan oleh penggunanya. Tindakan kejahatan seperti penipuan, penghinaan, ujaran benci dan tindak kejahatan lainnya belakangan ini banyak menggunakan aplikasi sosial media khususnya Twitter. Penelitian ini dilakukan untuk menemukan bukti *forensic* pada aplikasi media sosial Twitter yang diakses menggunakan aplikasi *smartphone* menggukan metode *Digital Forensics Research Workshop* (DFRWS). Tahapan digital forensik ini meliputi *identification, preservation, collection, examination, analysis* dan *presentation* dalam menemukan bukti digital tindak kejahatan dengan menggunakan aplikasi software MOBILedit Forensic Express dan Belkasoft Evidence Center. Bukti digital yang dicari pada *smartphone* dapat ditemukan menggunakan skenario kasus dan 16 variabel yang telah dibuat sehingga didapatkan bukti digital berupa spesifikasi *smartphone*, account Twitter, versi aplikasi, percakapan berupa pesan dan status. Hasil penelitian ini menunjukan *software* digital forensik MOBILedit Forensic Express lebih baik dengan tingkat akurasi 85,75% sedangkan Belkasoft Evidence Center 43,75%.

Kata Kunci: Digital Forensik, DFRWS, Mobile Forensics, Media Sosial, Twitter.

1. Pendahuluan

Salah satu sifat dasar yang dimiliki oleh manusia yaitu saling berkomunikasi dan berinteraksi dengan sesama manusia lainnya. Teknologi yang semakin canggih menjadi bagian yang takbisa lepas dari kehidupan masyarakat [1][2]. Selain memberikan manfaat perkembangan era digital juga memberikan dampak *negative* juga yaitu banyaknya kasus kejahatan meningkat menggunakan aplikasi di internet. Kejahatan dunia maya semakin meningkat setiap tahunnya [3][4]. Internet juga telah merubah gaya hidup masyarakat baik dari sosial, Pendidikan bahkan pemerintah [5]. Dampak buruk yang dihasilkan dari penggunaan teknologi ini adalah penyalahgunaan dalam melakukan kejahatan. Penyalahgunaan penggunaan internet dan sosial media tersebut biasanya dikenal dengan nama *cybercrime*

Diterima Redaksi : 12-07-2020 | Selesai Revisi : 26-08-2020 | Diterbitkan Online : 30-10-2020

[6][7]. Pertumbuhan media sosial dan aplikasi pesan instan telah mempermudah pengembangan banyak kejahatan *cyber* dan aktivitas jahat yang serius [8][9]. Penggunaan media sosial Twitter yang semakin mudah, terutama dalam mendaftarkan akun baru membuat memunculkan banyak akun palsu yang selain digunakan untuk berkomunikasi juga digunakan untuk menuliskan berita tidak benar, penipuan dan juga pencemaraan nama baik terhadap seseorang sehingga pada akhirnya merugikan banyak pihak [10][11]. Pada penelitian sebelumnya pernah dilakukan metode *Digital Forensics Research Workshop* (DFRWS) untuk mengambil bukti digital dari *email spoofing* [12]. Hasil penelitian menunjukkan bahwa *email spoofing* dapat di identifikasi dengan melakukan analisis dari kejanggalan pesan.

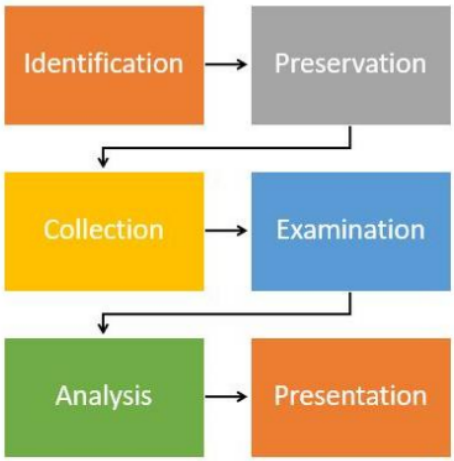
Penelitian yang sudah dilakukan perlunya mencoba menggunakaan metode *Digital Forensics Research Workshop* (DFRWS) untuk diterapkan dalam mencari bukti digital di media sosial. Dikarenakan kejahatan di dunia digital sulit di deteksi secara fisik melainkan harus menggunakan pemrosesan digital, dikarenakan jejak pelaku semakin berkembang menuju kejahatan asimetris [13]. Perkembangan teknologi internet juga di dasari oleh perkembangan *smartphone* yang semakin cepat menggantikan peran computer [14][15]. Fitur dan teknologi yang canggih juga semakin banyak dimanfaatkan untuk melakukan kejahatan [16].

Saat ini banyak orang dalam mengakses informasi dan diikuti oleh pertumbuhan penggunaan media sosial. Data akun yang aktif setara dengan 31% dari jumlah penduduk dunia atau sekitar 2,31 Triliun. Pengguna aplikasi media sosial Twitter sendiri pada bulan juni 2016 telah menembus 310 juta pengguna, dimana kejahatan pada media sosial Twitter semakin meningkat tiap tahunnya [17].

Penelitian ini melakukan perbandingan *tools* forensik dengan menggunakan metode *Digital Forensics Research Workshop* (DFRWS) untuk menentukan akurasi dari masing-masing *tools* forensik dalam mendapatkan barang bukti digital yang dapat diambil di aplikasi media sosial Twitter.

2. Metode Penelitian

Penelitian ini menggunakan metode digital forensik *Digital Forensic Research Workshop* (DFRWS). Metode DFRWS membantu dalam memperoleh barang bukti dan merekam informasi yang dibutuhkan untuk kemudian dikumpulkan menggunakan data mekanisme terpusat [12]. Investigasi forensik digunakan untuk mengetahui bukti digital dan alat bukti menggunakan alat yang berbeda dan merupakan proses yang sulit dan kompleks. Tujuan digital forensik adalah untuk mempertahankan dokumentasi dan mengetahui siapa yang bertanggung jawab sehingga dapat digunakan sebagai bukti di pengadilan [18]. Metode *Digital Forensics Research Workshop* (DFRWS) mempunyai beberapa tahapan untuk melakukan investigasi forensik yaitu seperti pada Gambar 1.



Gambar 1. Alur DFRWS

Identification (Identifikasi), tahap ini merupakan proses identifikasi dalam pencarian barang bukti digital dan menentukan kebutuhan yang diperlukan untuk proses penyelidikan.

Preservation, (Pemeliharaan), tahap ini merupakan tahap pemeliharaan yang diperlukan untuk menjaga bahwa barang bukti digital masih terjaga keasliannya. Barang bukti tidak dilakukan perubahan atau disabotase.

Collection (Pengumpulan), melakukan proses pengumpulan dan mengidentifikasi bagian yang dibutuhkan untuk melakukan identifikasi dari sumber data berdasarkan barang bukti digital.

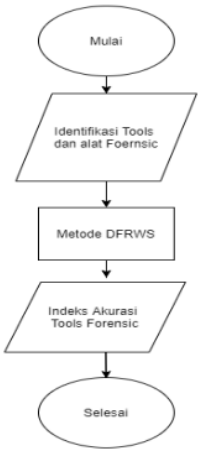
Examination (Pemeriksaan), tahap ini menentukan *filtering* pada salah satu bagian yang berasal dari sumber data, tetapi tetap menjaga keaslian dari isi data tersebut dikarenakan sifat dari keaslian data sangat penting oleh karena itu *filtering* data dilakukan hanya dari sisi perubahan bentuk pada data dengan tetap menjaga keaslian data.

Analysis (Analisis), melakukan penelitian untuk dapat mengetahui dimana, oleh siapa dan bagaimana data dari sebuah kasus tersebut dapat diperoleh.

Presentation (Presentasi), tahapan presentasi dilakukan dengan menampilkan informasi yang diperoleh dari tahap analisis sebelumnya, kemudian dilakukan pendataan data hasil dari analisis yang diperoleh meliputi pelaporan tindakan yang sudah dilakukan. Penjelasan mengenai metode dan *tools* yang di terapkan untuk menentukan tindakan yang dibutuhkan serta memberikan saran dan masukan untuk perbaikan sebuah kebijakan atau hasil yang diperoleh.

2.1. Skenario Kasus

Skenario kasus dibutuhkan untuk melakukan proses digital forensik dengan bantuan beberapa variabel untuk mendapatkan hasil yang maksimal. Skenario kasus dapat dilihat pada Gambar 2.



Gambar 2. *Flowchart* Digital Forensik

Pelaku melakukan tindak kejahatan dengan menggunakan aplikasi Twitter yang ada pada *smartphone*. Setelah smartphone berhasil didapatkan kemudian dilakukan langkah digital forensic untuk mendapatkan bukti tindak kejahatan. Hasil dari bukti tersebut akan di presentasikan sebagai tambahan bukti di persidangan. Dalam memudahkan pencarian barang bukti maka difokuskan untuk pembuatan variabel pencarian bukti digital seperti pada Tabel 1.

Tabel 1. Variabel yang Digunakan

No	Variabel
1.	Application info
2.	Account info
3.	Twitter ID
4.	Friends
5.	User/ Follower/Following
6.	Conversation/Direst Messages
7.	Cached Search
8.	Audio
9.	Video
10.	Text
11.	Picture
12.	Deleted Messages/Tweets
13.	IP Adress
14.	url
15.	Email/Phone Number
16.	Location

Melalui tabel variabel tersebut akan dilakukan proses forensik digital untuk mendapatkan barang bukti yang sesuai.

2.2. MOBILedit Forensic Express

MOBILedit Forensic Express merupakan *tools forensic* yang memungkinkan penyidik memperoleh secara logic. mencari dan memeriksa ponsel menggunakan beberapa mekanisme konektivitas terutama nirkabel, cukup baik digunakan untuk memperoleh informasi sistem telepon dan informasi lain seperti kontak dan pesan [16].

2.3. Belkasoft Evidence Center

Belkasoft Evience Center dapat digunakan untuk mendapatkan, mencari, menganalisa dan menyimpan berbagai bukti digital yang ada pada perangkat komputer atau mobile, tools ini untuk mengekstrak bukti digital dari berbagai sumber dengan menganalisis penyimpanan hard drive, memory dump, iOs BlackBerry dan android backup kemudian secara otomatis menganalisis sumber data dan menyimpannya dalam sebuah laporan [19].

3. Hasil dan Pembahasan

3.1. Tahapan *Identification*

Metode *Digital Forensik Research Workshop* (DFRWS) merupakan salah satu metode yang memiliki tahapan cukup lengkap dalam menjalakan proses *forensic* dan banyak digunakan oleh penyidik dalam mengumpulkan barang bukti. Proses mendapatkan barang bukti pada *smartphone* Android menggunakan *software* forensik Mobiledit Forensic Express dan Belkasoft Evidence Center. Berikut adalah Tabel 2 dan 3 informasi tentang hardware dan software yang diperlukan pada penelitian ini.

Tabel 2. Alat Penelitian

No	Alat Penelitian	Deskripsi
1.	Laptop	Asus A450L, Windows 10 64 bit
2.	Smartphone	Evercross Y3+, Android Lolipop 5.0.1
3.	Twitter	Aplikasi media sosial
4.	Kabel USB	Konektor dari hp ke laptop

Tabel 3. *Forensic Tools*

No	*Forensic Tools*	Deskripsi
1.	Mobiledit Forensic Express	Berbasis Windows aplikasi yang dapat digunakan untuk memperoleh bukti digital pada smartphone.
2.	Belkasoft Evidence Center	Berbasis Windows aplikasi yang dapat digunakan untuk memperoleh bukti digital pada smartphone

Tahapan pertama yang dilakukan adalah proses identifikasi untuk dijadikan bahan acuan pada pencarian barang bukti berdasarkan kasus yang telah terjadi sebelumnya. Barang bukti yang akan di identifikasi adalah sebuah *smartphone* dengan merk Evercross seperti pada Gambar 3.

Gambar 3. *Smartphone* Penelitian

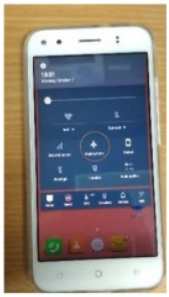
Spesifikasi lebih detail dapat dilihat pada Tabel 4 seperti berikut:

Tabel 4. Spesifikasi *Smartphone*

Spesifikasi	Type
Manufacture	EVERCROSS
Product	B75
HW Revision	LMY47D
Platform	Android
SW Revision	5.1(22)
Serial Number	0123456789ABCDEF
Unlocking Pattern	3452
IMEI	358441061746404
Rooted	Yes
SIM Card	Yes
Operator	3, MCC:510, MNC:89
IMSI	510897263097260
ICCID	89628990007753870152

3.2. *Preservation*

Tahap *preservation*, yaitu tahap pemeliharaan barang bukti digital dan memastikan keadaan barang bukti asli. Proses penjagaan *integritas* dilakukan untuk menjaga barang bukti itu asli dan tidak rusak. Tahap yang dilakukan adalah melakukan isolasi perangkat *smartphone* dari komunikasi data masuk dan keluar. Teknik isolasi perlu dilakukan untuk menghindari hal-hal yang dapat merusak barang bukti digital atau mempengaruhi *integritas* data didalamnya. Kegiatan isolasi barang bukti yang dilakukan adalah merubah status perangkat kedalam mode pesawat seperti pada Gambar 4.

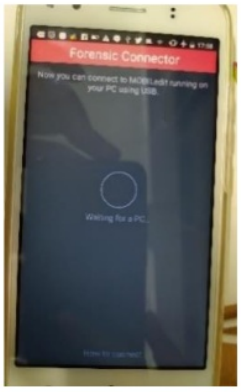


Gambar 4. Isolasi Data dengan Mode Pesawat

Proses isolasi diperlukan untuk mengurangi kemungkinan data pada *smartphone* berubah. Bisa disebabkan oleh penambahan atau pengurangan data dari luar yang menyebabkan barang bukti hilang atau rusak saat dilakukan proses forensik pencarian barang bukti.

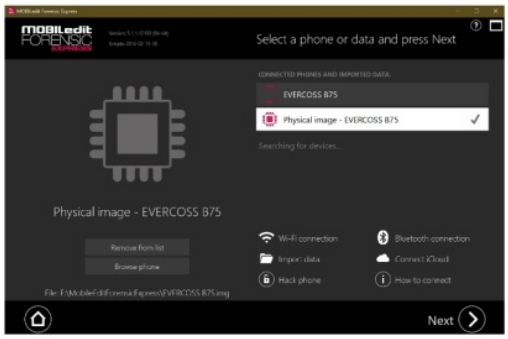
3.3. *Collection*

Tahap pengumpulan barang bukti digital pada *smartphone* memiliki resiko yang tinggi, dikarenakan jika terjadi kesalahan fatal, data dan bukti digital yang ada pada *smartphone* dapat hilang atau *corrupted* sehingga tidak data tidak terbaca. Gambar 5. merupakan proses *collection* data pada *smartphone* dengan MOBILedit Forensic Express sedang berjalan.



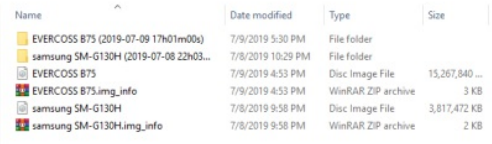
Gambar 5. Proses *Collection* Data pada *Smartphone*

Kemampuan *tools* MOBILedit Forensic Express adalah dapat membuat sebuah backup sistem dan *collection* data pada *smartphone* kemudian mengekstraksinya seperti pada Gambar 6.



Gambar 6. Backup dan *Collection* Data

Hasil dari proses *backup data* ini berupa dokumen *image* dari *smartphone* dengan ekstensi .img dengan ukuran dokumen yang bervariasi tergantung banyaknya data yang disimpan pada *smartphone* tersebut. Gambar 7 merupakan hasil dari proses *backup* dan *collection* yang sudah selesai dilakukan.

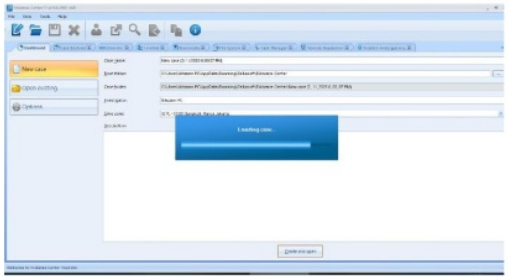


Gambar 7. *Physical Image*

Setelah dilakukan *backup* dan *collection* data, langkah selanjutnya adalah melakukan ekstraksi data dengan menggunakan *tools* MOBILedit Forensic Express yang

ditunjukkan pada Gambar 8 dan proses ekstraksi Belkasoft Evidence Center yang ditunjukan pada Gambar 9.

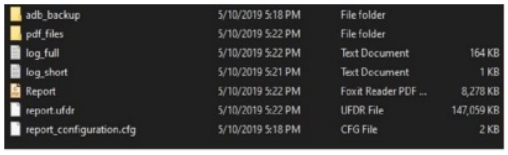
Gambar 8. Proses *Extraction* MOBILedit Forensic Express



Gambar 9. Proses *Extraction* Belkasoft Evidence Center

3.4. *Examination*

Hasil dari ekstraksi yang telah dilakukan akan tampil dalam bentuk Full *report* bentuk format.pdf. Tampilan file data hasil ekstraksi seperti yang ditunjukan pada Gambar 10.



adb_backup	5/10/2019 5:18 PM	File folder	
pdf_files	5/10/2019 5:22 PM	File folder	
log_full	5/10/2019 5:22 PM	Text Document	164 KB
log_short	5/10/2019 5:21 PM	Text Document	1 KB
Report	5/10/2019 5:22 PM	Foxit Reader PDF ...	8,278 KB
report.ufdr	5/10/2019 5:22 PM	UFDR File	147,059 KB
report_configuration.cfg	5/10/2019 5:18 PM	CFG File	2 KB

Gambar 10. Hasil Extraction

Hasil dari laporan Report.pdf dapat menunjukan bahwa *smartphone* yang digunakan adalah bermerk Evercross dan spesifikasinya secara lebih detail, Selain spesifikasi didapat juga informasi lain seperti *time zone*, IMEI, Storage dan lainnya, sesuai dengan yang di tunjukkan pada Gambar 11.

Device Properties

Manufacturer	EVERCOSS
Product	B75
HW Revision	LMY47D
Platform	Android
SW Revision	5.1 (22)
Android ID	63858a211302353a
Serial Number	0123456789ABCDEF
Adb Backup Password	1
Unlocking Pattern	3452
Device Time	2019-09-29 16:07:43 (UTC+7)
Manual Time	✓ Yes
Time Zone	Asia/Jakarta
Manual Time Zone	✗ No
Device Storage Encrypted	✓ Yes
IMEI	354441061746404
LACCID	LAC: 12901, CID: 84642657
Rooted	Yes
SIM Card	✓ Yes
IMSI	510897263097260
SIM Card Country	Indonesia
ICCID	89628990007753870152
Total Storage	11.4 GB
Used Storage	11.3 GB
Total SD Card Storage	11.3 GB
Used SD Card Storage	11.3 GB

Gambar 11. *Report Smartphone*

3.5. *Analysis*

Hasil dari analisa aplikasi Twitter yang di dapat dari report.pdf adalah informasi yang menunjukan version aplikasi yang dipakai adalah 8.13.0, data size 10.3 Mb, dan permission yang digunakan untuk mengakses *smartphone* sesuai dengan Gambar 12.

Twitter

Label	Twitter
Package	com.twitter.android
Version	8.13.0-release.00
Application Type	User Application
Application Size	50.1 MB
Data Size	10.3 MB
Cache Size	10.0 MB
APK File Extracted	✓ Yes
APK Verification Result	APK verification successful
APK Verification Message	Verification scheme used v2 Best certificate found: Cert 40f3166bb567d3144bca7da466bb948b782270ea, valid from 2010-04-27T23:01:34Z to 2048-08-25T23:01:34Z, Subject: C=US, ST=CA, L=San Francisco, O=Twitter, Inc., OU=Mobile, CN=Leland Rechis, Issuer: C=US, ST=CA, L=San Francisco, O=Twitter, Inc., OU=Mobile, CN=Leland Rechis
	com.twitter.android.permission.RESTRICTED, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.INTERNET, android.permission.VIBRATE, android.permission.READ_PROFILE, android.permission.READ_CONTACTS, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, com.twitter.android.permission.READ_DATA, com.google.android.providers.gsf.permission.READ_GSERVICES , com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.READ_PHONE_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.GET_ACCOUNTS, android.permission.ACCESS_NETWORK_STATE,

Gambar 12. Aplikasi Twitter

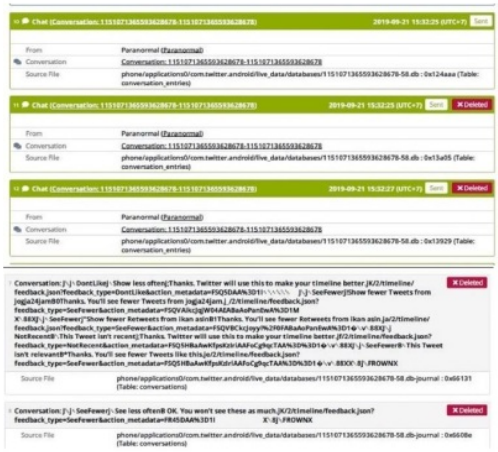
File *report* juga menampilkan nama *account* yang digunakan dalam aplikasi Twitter di *smartphone*, disini munjukan dengan nama *nickname* @Wicakson8 dengan nama *account* Paranormal, sesuai Gambar 13.

Gambar 13. Informasi *Account* Twitter

Selain nama *account* yang digunakan juga dapat ditemukan status Twitter yang sudah di hapus dari *timeline* media sosial Twitter sepeti yang di tunjukkan pada Gambar 14.

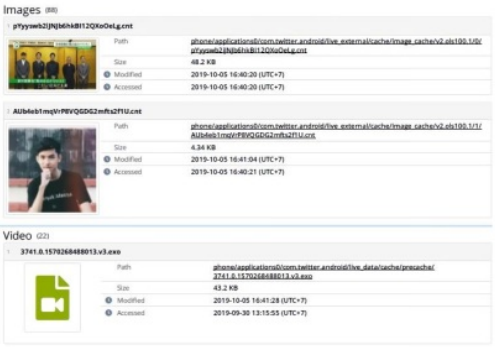
Gambar 14. Status Twitter yang dihapus

Bukti data *chatting* atau percakapan yang sudah di hapus juga dapat diketahui dan ditampilkan kembali sehingga memudahkan untuk menemukan barang bukti yang sudah terhapus sebelumnya. Gambar bukti chat percakapan yang sudah terhapus dapat terdapat pada Gambar 15.



Gambar 15. Percakapan di Twitter

Hasil dari analisa juga menemukan media berupa gambar dan video pada akun Twitter @wicakson8. Bukti media yang ditemukan pada aplikasi Twitter ini adalah 88 gambar dan 22 video seperti yang ditunjukan pada Gambar 16.



Gambar 16. Media Twitter

3.6. *Presentation*

Tahapan akhir adalah tahapan presentasi, tahapan ini dilakukan dengan menampilkan kembali informasi yang dihasilkan dari tahap sebelumnya setelah memperoleh barang bukti dari proses pemeriksaan. Informasi yang diperoleh kemudian dibuatkan laporkan berdasarkan tahapan metode dan *tools* yang digunakan. Gambar 17 menjelasan mengenai jumlah barang bukti yang berhasil diperoleh menggunakan aplikasi Belkasoft Evidence Center dimana untuk pelaporannya akan di lakukan perbandingan dengan aplikasi MOBILedit Forensic Express.

Gambar 17. Aplikasi Belkasoft Evidence Center

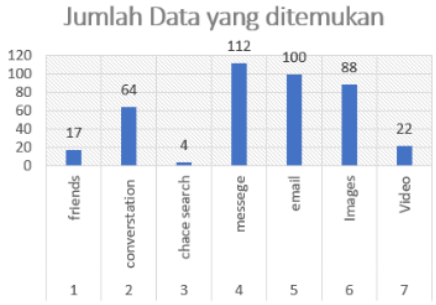
Penggunaan aplikasi *tools forensic* Belkasoft Evidence Center ini digunakan untuk membaca *image* data yang sudah dianalisis sehingga menampilkan informasi yang lebih detail untuk barang bukti yang berhasil ditemukan.

Perbandingan hasil dari penemuan barang bukti pada aplikasi Belkasoft Evidence Center dan MOBILedit Forensic Express dengan menggunakan variabel yang digunakan dapat dilihat pada Tabel 5.

Gambar 18 menunjukkan jumlah data barang bukti digital yang diperoleh menggunakan *tools* MOBILedit Forensic Express dan Belkasoft Evidence Center.

Tabel 5. Hasil Variabel

No	Hasil yang diperoleh	Tools	
		MOBILedit Forensic Express	Belkasoft Evidence Center
1.	Application info	√	×
2.	Account info	√	×
3.	Twitter ID	√	√
4.	Friends	√	×
5.	User/Follower/Following	√	√
6.	Conversation/Direst Messages	√	√
7.	Cached Search	√	×
8.	Audio	×	×
9.	Video	√	×
10.	Text	√	√
11.	Picture	√	√
12.	Deleted Messages/Tweets	√	√
13.	IP Adress	×	×
14.	url	√	√
15.	Email/Phone Number	√	×
16.	Location	√	×
	Index Score	14	7



Gambar 18. Jumlah Data Yang Diperoleh

Keseluruhan hasil tersebut diperoleh berdasarkan pengujian dari pendeteksian dengan menggunakan *tools*, skenario dan variabel yang telah ditentukan pada tahap perencanaan. Indeks akurasi untuk mengukur kemampuan masing-masing pendeteksian dapat dihitung menggunakan rumus [20].

$$Par = \frac{\sum ar0}{\sum arT} x100\% \quad (1)$$

Par adalah angka indeks akurasi alat forensik
ar0 adalah jumlah variabel yang terdeteksi.
arT adalah jumlah keseluruhan variabel yang digunakan.

Perhitungan indeks akurasi untuk mengukur kemampuan masing-masing pendeteksian *tools forensic* dapat dihitung seperti pada berikut.

MOBILedit Forensic Express:

$$Par = \frac{14}{16} x100\% = 85{,}75\%$$

Belkasoft Evidence Center :

$$Par = \frac{7}{16} x100\% = 43{,}75\%$$

Berdasarkan perhitungan indeks kemampuan akurasi alat-alat dan teknik forensik dengan variabel yang digunakan maka mendapatkan hasil MOBILedit Forensic Express akurasi sebesar 85,75% dan Belkasoft Evidance Center akurasi sebesar 43,75%.

4. Kesimpulan

Kesimpulan yang didapat setelah dilakukan forensik digital pada aplikasi Twitter menggunakan *smartphone* Evercross B75 adalah barang bukti digital seperti *id user*, pesan, gambar, video dan bukti lainnya dapat di ambil dengan menggunakan metode *Digital Forensics Research Workshop* (DFRWS) dan aplikasi forensik. Aplikasi MOBILedit Forensic Express mendapatkan akurasi yang lebih tinggi yaitu 85,75% dengan 14 variabel yang berhasil diperoleh dari 16 variabel sedangkan Belkasoft Evidence Center mendapatkan akurasi 43,75% dengan 7 variabel yang diperoleh dari 16 variabel.

Daftar Rujukan

[1] M. I. Syahib *et al.*, "Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan Cybercrime Menggunakan Metode Nist," *Semin. Nas. Inform. 2018 (semnasIF 2018)*, vol. 2018, no. November, pp. 134–139, 2018.

[2] A. Eleyan and M. S. Anwar, "Multiresolution Edge Detection Using Particle Swarm Optimization," *Int. J. Eng. Sci. Appl.*, vol. 1, no. 1, pp. 11–17, 2017, doi: 10.1109/CCAA.2017.8229843.

[3] A. A. Agus and Riskawati, "PENANGANAN KASUS CYBER CRIME DI KOTA MAKASSAR (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)," vol. XI, no. April, pp. 20–29, 2016.

[4] T. D. Larasati and B. C. Hidayanto, "Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10," *Semin. Nas. Sist. Inf. Indones. 6 Novemb.* 2017, no. November, 2017.

[5] T. Rochmadi, I. Riadi, and Y. Prayudi, "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," *Int. J. Comput. Appl.*, vol. 164, no. 8, pp. 31–37, 2017, doi: 10.5120/ijca2017913717.

[6] I. Riadi, A. Yudhana, and W. Y. Sulistyo, "Analisis Perbandingan Nilai Kualitas Citra pada Metode Deteksi Tepi," *Rekayasa Sist. dan Teknol. Inf.*, vol. 4, no. 2, pp. 345–351, 2020.

[7] Handrizal, "Analisis Perbandingan Toolkit Puran File Recovery , Glary Undelete Dan Recovery Untuk Digital Forensik," *J. sains Komput. Inform.*, no. 1, pp. 84–94, 2017.

[8] M. R. Wankhade and N. M. Wagdarikar, "Feature Extraction of Edge Detected Images," *Int. J. Comput. Sci. Mob. Comput.*, vol. no. 6, pp. 336–345, 2017.

[9] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilmu Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, 2017, doi: 10.26555/jiteki.v3i1.6643.

[10] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Perancangan Digital Forensik Pada Aplikasi Twitter Menggunakan Metode Live Forensics," vol. 2018, no. November, pp. 86–91, 2018.

[11] 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.

[12] A. L. Suryana, R. 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.

[13] A. C. K. Wardana, R. Pedrason, and T. B. Prasetyo, "Implementasi Digital Forensik Brunei Darussalam Dalam

Membangun Keamanan Siber," pp. 1–22, 2017.
[14] A. Yudhana, R. Umar, and F. M. Ayudewi, "The Monitoring of Corn Sprouts Growth Using the Region Growing Methods," *J. Phys. Conf. Ser.*, vol. 1373, no. 1, 2019, doi: 10.1088/1742-6596/1373/1/012054.
[15] 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.
[16] Y. N. Kunang and A. Khristian, "Implementasi Prosedur Forensik untuk Analisis Artefak Whatsapp pada Ponsel Android," *Annu. Semin. 2016*, vol. 2, no. 1, pp. 59–68, 2016.
[17] A. Mukti, S. U. Masruroh, and D. Khairani, "Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial," *J. Tek. Inform.*, vol. 10, no. 1, pp. 73–84, 2017, doi: 10.15408/JTI.V10I1.5617.
[18] F. G. Hikmatyar, "Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases," vol. 7, no. 2, pp. 19–22, 2018.
[19] M. Parekh and S. Jani, "Memory Forensic : Acquisition And Analysis Of Memory And Its Tools Comparison," *Communiacation, Integr. Networks Signal Process. 2018*, vol. 5, no. 2: SE : February 2018, pp. 90–95, 2018, doi: 10.5281/zenodo.1198968.
[20] 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.

HASIL CEK_60020397_Point-C43-IRD-850GB-Comparative analysis of Forensic Tools on Twitter applications using the DFRWS method

ORIGINALITY REPORT

10%	8%	6%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to President University Student Paper	4%
2	index.pkp.sfu.ca Internet Source	2%
3	Muhammad Irwan Syahib, Imam Riadi, Rusydi Umar. "Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST)", J-SAKTI (Jurnal Sains Komputer dan Informatika), 2020 Publication	1%
4	Irfan Fathur Rohman, Nur Widiyasono, Rohmat Gunawan. "Simulasi Analisis Bukti Digital Aplikasi Skype Berbasis Android menggunakan NIST SP 800-101 R1", Jurnal Sustainable: Jurnal Hasil Penelitian dan Industri Terapan, 2019 Publication	1%
5	dev.kinetik.umm.ac.id	

Internet Source

1%

6 onesearch.id

Internet Source

1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		