JIKO (Jurnal Informatika dan Komputer)
Vol. 6, no. 2, September 2022, hal. 242–250
e-ISSN : 2477-3964 — p-ISSN : 2477-4413

PERBANDINGAN TOOLS FORENSIK PADA APLIKASI DOMPET DIGITAL

Rusydi Umar[1], **Anton Yudhana**[2],dan **Muhammad Noor Fadillah**[3*]
[1,3]Program Studi Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
Email: rusydi@mti.uad.ac.id[1], eyudhana@ee.uad.ac.id[2], muhammad1807048006@webmail.uad.ac.id[3]

Abstrak

Penggunaan smartphone di Indonesia tidak hanya digunakan sebagai alat untuk komunikasi, akan tetapi dengan hadirnya aplikasi dompet digital maka mulai digunakan pula sebagai alat untuk bertransaksi. Proses forensik pada penelitian ini dilakukan pada empat aplikasi dompet digital yang ada di Indonesia dengan mengikuti metode forensik Digital Forensik Research Workshop (DFRWS) yang memiliki beberapa tahapan yaitu identification, preservation, collection, examination, analysis, dan presentation. Proses forensik dilakukan dengan tujuan untuk mencari informasi/dokumen elektronik yang berpotensi menjadi bukti digital yang bisa didapatkan dari aplikasi dompet digital. Tools forensik yang digunakan pada penelitian ini yaitu Autopsy dan Belkasoft Evidence Center. Berdasarkan hasil penelitian, tools forensik autopsy mendapatkan hasil lebih baik untuk mendapatkan data aktivitas transaksi yang ada pada aplikasi dompet digital dengan menemukan 8 dari 17 aktivitas transaksi mendapatkan presentase 47.05%, sedangkan tools Belkasoft Evidence Center mendapatkan 7 aktivitas transaksi dengan presentase 41,17%.
Kata Kunci: *Forensik Mobile, Tools Forensik, Bukti Digital, Aplikasi Dompet Digital, DFRWS*

Abstract

The use of smartphones in Indonesia is not only used as a tool for communication, but with the presence of a digital wallet application, it has also begun to be used as a tool for transactions. The forensic process in this study was carried out on four digital wallet applications in Indonesia by following the Digital Forensic Research Workshop (DFRWS) forensic method which has several stages, namely identification, preservation, collection, examination, analysis, and presentation. The forensic process is carried out with the aim of finding information/electronic documents that have the potential to become digital evidence that can be obtained from digital wallet applications. The forensic tools used in this research are Autopsy and Belkasoft Evidence Center. Based on the research results, forensic autopsy tools get better results for obtaining transaction activity data in digital wallet applications by finding 8 out of 17 transaction activities getting a percentage of 47.05%, while the Belkasoft Evidence Center tools get 7 transaction activities with a percentage of 41.17%.
KeyWords : *Mobile Forensik, Tools Forensik, Digital Evidence, E-wallet Apps, DFRWS.*

I. PENDAHULUAN

Berdasarkan data laporan hasil survei internet oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2019-2020 Q2, sebanyak 73,7% dari 266,91 juta jiwa penduduk Indonesia sudah menggunakan layanan internet di kehidupan sehari-hari dan sebanyak 95,4% menggunakan smartphone untuk mengaksesnya [1]. Penggunaan *smartphone* sudah semakin berkembang, tidak hanya sebagai alat untuk berkomunikasi, tetapi juga menjadi alat untuk melakukan transaksi pembayaran secara digital. Pembayaran digital dengan menggunakan *smartphone* di Indonesia dimulai sejak tahun 2007 yang pada saat itu masih menggunakan metode *Unstructured Supplementary Service Data* (USSD), dan pada tahun 2016, dengan kemunculan layanan Gopay merubah layanan pembayatan yang sebelumnya masih tradisional menjadi layanan pembayaran digital berbasis aplikasi *mobile* [2]. Layanan pembayaran digital berbasis aplikasi juga dikenal sebagai aplikasi dompet digital, dimana penggunanya dapat melakukan transaksi seperti melakukan pembayaran, mengirim dan menerima uang, dan menyimpan uang pada *smartphone*. Aplikasi dompet digital banyak digunakan karena kemudahaannya yang bisa diakses dimana saja dan kapan saja selama *smartphone* terhubung ke dalam jaringan internet. Pada tahun 2020, jumlah pengguna aplikasi dompet digital di Indonesia sebanyak 51,9 juta orang dan aplikasi dompet digital yang popular digunakan berdasarkan jumlah presentase penggunanya dapat dilihat sebagai berikut : OVO 33,6%, Gopay 29,2%, Link Aja 9,4% dan lainnya 6,3% [3]. Aplikasi dompet digital memberikan penggunanya beragam kemudahan dalam melakukan aktivitas transaksi, akan tetap didalam penggunaannya bisa saja dimanfaatkan ke hal yang berpotensi melanggar hukum. Pada suatu kasus *cybercrime* yang terjadi hampir tidak terlepas dari kontrol penggunanya ketika menggunakan aplikasi *smartphone* [4]. Pada kasus cybercrime yang terjadi banyak ditemukan smartphone digunakan sebagai media suatu tindak kejahatan yang berujung menjadi barang bukti [5]. Pada proses forensik, alat bukti digital bisa didapatkan dari penyimpanan *smartphone* yang menjadi barang bukti [6]. Berdasarkan temuan dari proses forensic memungkinkan mendapatkan informasi terkait aktivitas yang dicurigai dan artefak digital yang bisa menjadi penghubung antara data dan tersangka [7]. Proses forensik untuk mendapatkan barang bukti sangat berberpengaruh terhadap kondisi *smartphone* dan *tools* forensik yang digunakan dalam proses forensik. Proses forensik digital biasa dilakukan pada perangkat komputer, *smartphone* dan perangkat digital lainnya dengan metode *static forensic* atau *live forensic*, dan proses forensik dapat mengikuti beberapa standar seperti *Digital Forensic Research Workshop* (DFRWS), *Association of Chief Police Officers* (ACPO), *National Institute of Standards and Technology* (NIST), *National Intitute of Justice* (NIJ), *Integrated Digital Forensic Investigation Framework* (IDFIF), dan kerangka proses forensik lainnya [8].

Penelitian ini melakukan perbandingan kemampuan *tools* forensik yang digunakan untuk menemukan bukti digital terkait dengan infromasi dan aktivitas transaksi yang dilakukan pada empat aplikasi dompet digital dengan menggunakan metode *Digital Forensic Research Workshop* (DFRWS)

A. Penelitian Sejenis

1) Htar Htar Lwin dan Wai Phyo Aung (2020), melakukan analisis forensik digital dengan menggunakan metode NIST yang berfokus pada pemulihan artefak dan jejak digital pada beberapa aplikasi keuangan yang populer digunakan di Myanmar. Hasil analisis menunjukan terdapat data penting yang tersimpan pada perangkat pengguna dan beberapa aplikasi tidak menyimpan informasi apapun pada perangkat penggunanya [9].
2) Oluwafemi Osho, Uhtman L. Mohammed, Nanfa N. Nimzing, Andrew A. Uduimoh, dan Sanjay Misra (2019), melakukan analisis forensik terhadap aplikasi *mobile banking* berbasis Android yang populer di Nigeria terkait data sensitif yang tersimpan pada *smartphone*. Dari hasil analisis berdasar persyaratan OWASP MASVS-L2, aplikasi berjalan dengan baik dengan tidak menyimpan data sensitif pada perangkat pengguna [10].
3) Rajchada Chanajitt, Wantanee Viriyasitavat, dan Kim-Kwang Raymond Choo (2016), melakukan analisis forensik terhadap aplikasi *mobile banking* berbasis Android yang digunakan di Thailand, hasil penelitian menemukan dengan metode DD dan JTAG beberapa artefak dapat dipulihkan dan juga beberapa aplikasi tidak mengenkripsi data pengguna [11].
4) Yamini konduru, Dr. Nishshol Mishra, dan Dr.Sanjeev Sharma (2018), menganalisis artefak data pribadi pengguna dari aplikasi Android yang dapat tersimpan pada *smartphone*, selain itu juga menganalisis informasi yang dapat dibaca dari artefak dengan menggunakan *forensic tools*. Penelitian menemukan kurangnya fitur keamanan yang tepat pada beberapa aplikasi terutama terkait *commerce* dan *banking* [12].

II. METODE

A. Alat dan Bahan Penelitian

Alat dan bahan yang digunakan dalam penelitian ini dapat dilihat pada Tabel I, dan software yang digunakan dalam penelitian dapat dilihat pada Tabel II. Berdasarkan etika professional, nama aplikasi dompet digital yang digunakan dalam penelitian ini tidak akan disebutkan.

Tabel I: Alat Penelitian

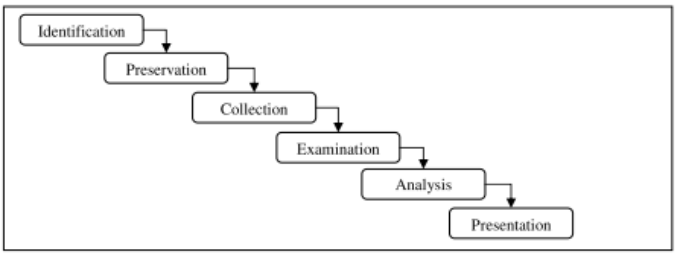
No	Alat penelitian	Deskripsi/spesifikasi
1	*Smartphone*	Xiaomi Redmi Note 3 MTK Android 5.0.2 Rooted
2	Laptop (*workstation*)	Toshiba Satellite C40-A Windows 10
3	USB *Cable*	*Type* B

Tabel II: Software Pendukung Penelitian

No	*software*	Nama	Versi
1	Aplikasi Dompet DigitalDompet	Digital A Dompet Digital B Dompet Digital C Dompet Digital D	2.6.0 4.31.1 3.47.0 2.79.09
2	*Tools Forensic*	Autopsy Belkasoft Evidence Center	4.9.1 9.9
3	*Tool Hasing*	HashMyFiles	2.42

B. Metode Penelitian

Penelitian ini menggunakan metode *Digital Forensic Research Workshop* (DFRWS) terlihat pada Gambar 1, metode ini merupakan metode ilmiah yang digunakan pada *digital forensic* dan telah teruji untuk membantu mendapatkan barang bukti digital [13].



Gambar 1: Model investigasi DFRWS [14]

Berdasarkan Metode *Digital Forensic Research Workshop* (DFRWS), terdapat beberapa tahapan yang harus dilakukan [15], sebagai berikut :

1) **Identification**
   Tahap ini merupakan proses identifikasi dilakukan untuk menentukan kebutuhan yang apa saja yang diperlukan pada penyelidikan dan pencarian barang bukti.
2) **Preservation**
   Tahap ini merupakan tahap pemeliharaan dilakukan untuk menjaga barang bukti digital, memastikan keaslian barang bukti dan menyangkal klaim bahwa barang bukti telah dilakukan sabotase.
3) **Collection**
   Melakukan proses pengumpulan identifikasi bagian yang khusus dari barang bukti digital dan melakukan identifikasi sumber data.
4) **Examination**
   Melakukan tahap menentukan penyaringan data pada begian tertentu dari sumber data, penyaringan data dilakukan dengan melakukan perubahan bentuk data namun Tidak melakukan perubahan pada isi data karena keaslian data merupakan hal yang sangat penting.
5) **Analysis**
   Melakukan melakukan penentuan tentang dimana data tersebut dihasilkan, oleh siapa data tersebut dihasilkan, bagaimana data tersebut dihasilkan dan kenapa data tersebut dihasilkan.
6) **Presentation**
   Presentasi dilakukan dengan menyajikan informasi yang dihasilkan dari tahap analisis. Tahap presentasi dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai *tool*, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, *tool*, atau aspek pendukung lainnya pada proses tindakan forensik digital.

Simulasi Kasus

Disimulasikan sebuah *smartphone* menjadi barang bukti suatu *cybercrime*, didalamnya ditemukan empat aplikasi dompet digital yang diduga digunakan sebagai alat untuk bertransaksi terkait kasus *cybercrime*. setelah barang bukti *smartphone* diamankan, dilakukan proses forensik untuk mendapatkan informasi elektronik yang berpotensi menjadi barang bukti digital. Pencarian bukti digital difokuskan pada aktivitas transaksi yang dilakukan dengan aplikasi dompet digital, yang sebelumnya masing-masing aplikasi dompet digital sudah dilakukan aktivitas transaksi berupa *top up*, mengirim & menerima saldo, dan *transfer* ke rekening bank.

III. HASIL

Berdasarkan metode *Digital Forensik Research Workshop* (DFRWS), berikut tahapan proses forensik pada barang bukti smartphone untuk mencari informasi/dokumen elektronik yang ada pada aplikasi dompet digital.

1) ***Identification***
   Smartphone
   Ditemukan barang bukti satu buah smartphone Android dengan spesifikasi pada Tabel III.

Tabel III: Spesifikasi barang bukti *smartphone*

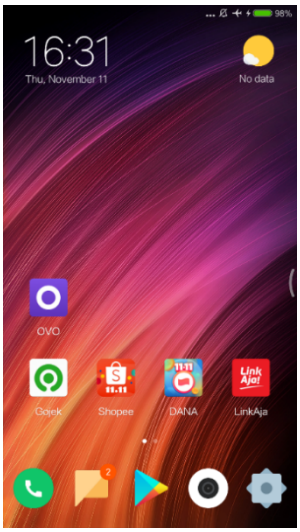
Spesifikasi bukti **smartphone**	
Brand	Xiaomi
Model number	Redmi Note 3
Platform	Android (5.0.2)
Serial number	VCS8MVQSYLCMxxxx
Imei	86967702723xxxx
Ram	2GB
Rom	16GB
rooted	Yes

***Tools* Forensik**

Berdasarkan temuan barang bukti satu buah *smartphone* dengan spesifikasi seperti Tabel IV, maka ditentukan tools forensik yang akan digunakan selama proses penyidikan dan pencarian barang bukti digital yaitu Autopsy dan Belkasoft Evidence Center.

2) ***Preservation***

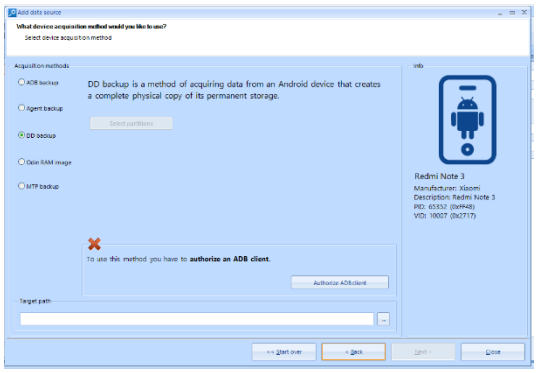
Barang bukti *smartphone* akan disimpan ditempat yang aman dan mengaktifkan *airplane mode* pada *smartphone* untuk mengisolasi barang bukti dari semua jaringan telekomunikasi seperti pada Gambar 2.



Gambar 2: Mengisolasi barangbukti dari semua jaringan

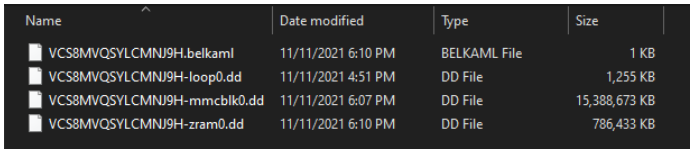
3) ***Collection***

Untuk menjaga integritas sumber data maka proses forensik tidak dilakukan langsung pada barang bukti *smartphone*, maka dilakukan akusisi atau membuat physical image dari barang bukti *smartphone* menggunakan tool Belkasoft Evidence Center dengan metode DD *backup* seperti pada Gambar 3.



Gambar 3: Proses akusisi menggunakan Belkasoft Evidence Center

Dari proses membuat *physical image* didapatkan empat *file* dengan ekstensi .dd seperti pada Gambar 4.

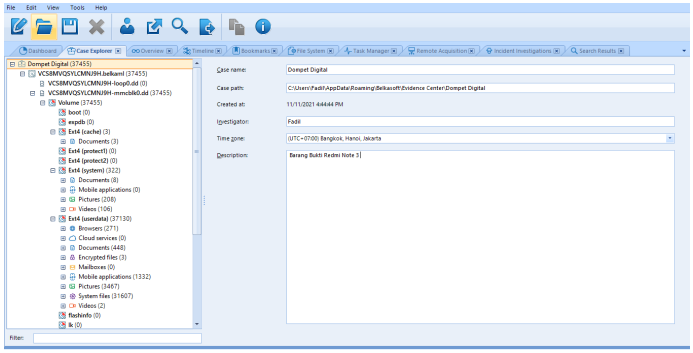


Gambar 4: *File physical image* dari barang bukti *smartphone*

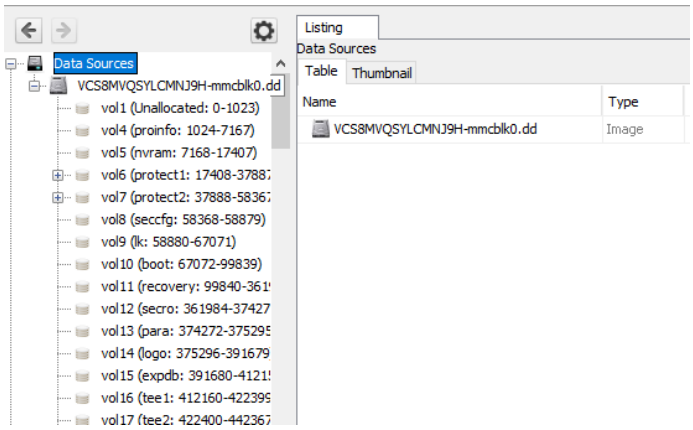
File physical image dari proses akusisi akan dilakukan *hashing* dengan *tool* HashMyFiles untuk menjaga kevalidan barang bukti digital, pada *file* VCS8MVQSYLCMNJ9H-mmcblk0.dd didapatkan nilai MD5 8b8e63d04c1b222ee8891d46834c3fdc.

4) ***Examination***

File physical image dari proses *collection* diekstraksi menggunakan *tools* forensik Belkasoft Evidence Center seperti pada Gambar 5 dan Autopsy seperti pada Gambar 6



Gambar 5: Proses ekstraksi menggunakan Belkasoft Evidence Center



Gambar 6: Proses ekstraksi menggunakan Autopsy

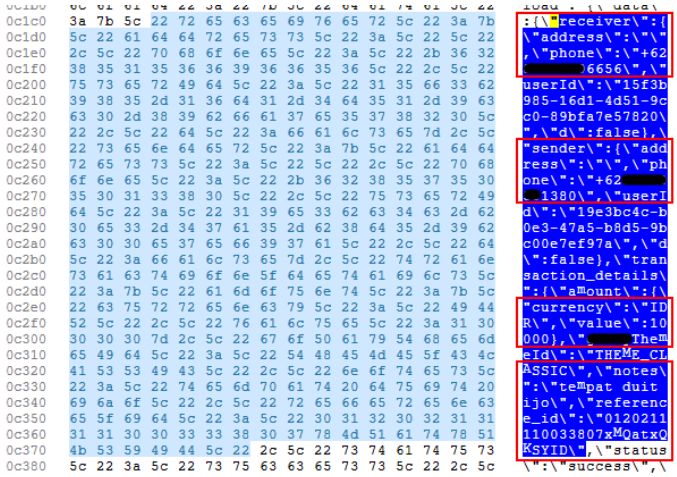
5) ***Analysis***

Selanjutnya dilakukan proses analisis secara manual dengan bantuan *tools* forensik Autopsy dan Belkasoft Evidence Center untuk menemukan informasi yang berpotensi menjadi bukti digital terkait aktivitas yang dilakukan pada masing-masing aplikasi dompet digital. **Aplikasi Dompet Digital A**

Pada aplikasi dompet digital A, *tools* forensik Autopsy dan Belkasoft Evidence Center tidak menemukan data yang relevan terkait aktivitas transaksi yang dilakukan dengan dompet digital A. **Aplikasi dompet digital B**

Pada aplikasi dompet digital B, *tools* Autopsy dan Belkasoft Evidence Center memukan enam aktivitas transaksi pada *folder cache file* b23cff29ac58336ad 9145a431d4f9925.1 seperti pada Gambar 7 dan tiga aktivitas transakasi ditemukan pada *folder database file* conversations-database seperti pada Gambar 8.

Gambar 7: **Proses ekstraksi menggunakan Autopsy**

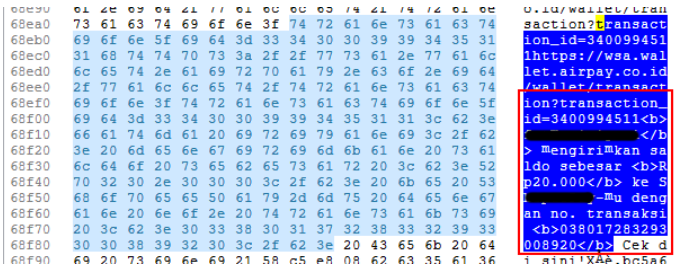


Gambar 8: Aktivitas transaksi yang ditemukan pada chat dompet digital B

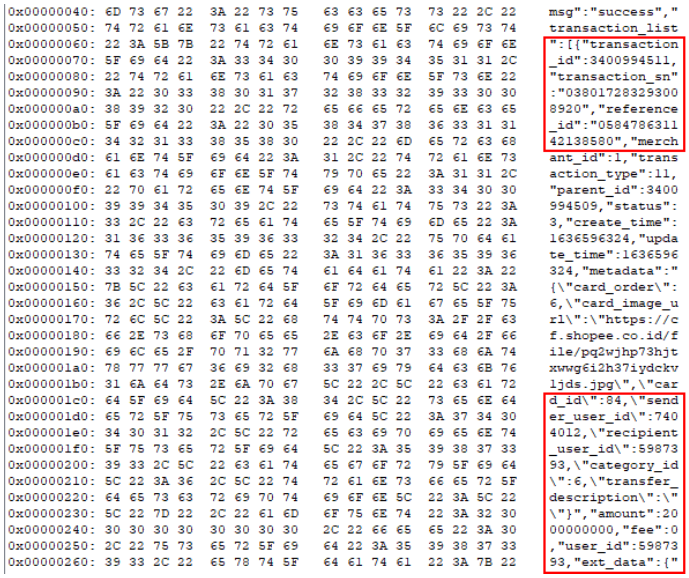
Aplikasi dompet digital C

Pada aplikasi dompetdigital C, *tools* Belkasoft Evidence Center dan Autopsy tidak menemukan data yang relevan dengan aktivitas transaksi yang dilakukan dengan dompet digital C. **Aplikasi dompet digital D**

Pada aplikasi dompet digital D, *tools* Autopsy dan Belkasoft Evidence Center menemukan ditemukan satu aktivitas transaksi pada folder databases file sxxxxx5987393.db seperti pada Gambar 9 dan dua aktivitas transaksi ditemukan oleh *tools* Autopsy pada cache sub folder react_http_cache_networking file 60ceb8918ac55ad7f9057c974dcf2c11.1 seperti pada Gambar 10.



Gambar 9: Aktivitas transaksi yang ditemukan pada chat dompet digital D



Gambar 10: Aktivitas transaksi yang ditemukan pada chat dompet digital D

6) ***Presentation***

Tahapan terakhir yaitu presentasi, dengan memberikan laporan informasi yang didapatkan dari hasil proses analisis forensik. Informasi yang didapatkan dibuatkan laporan berdasarkan metode dan *tools* yang digunakan selama proses forensik.

Berdasarkan pada barang bukti *smartphone*, ditemukan empat aplikasi dompet digital yang selanjutnya dilakukan proses forensik dengan bantuan *tools* Autopsy dan Belkasoft Evidence Center dengan mengikuti kerangka kerja metode *Digital Forensik Research Workshop* (DFRWS). Berhasil menemukan aktivitas transaksi yang tersimpan pada penyimpanan *internal smartphone* dengan rincian seperti pada Tabel IV

Tabel IV: Aktivitas transaksi yang berhasil ditemukan tools forensik

No	Nama Aplikasi	Jenis Transaksi	Deskripsi Transaksi	*Tools* Forensik	
				Autopsy	Belkasoft
1	Dompet Digital A	*Top up*	*Top Up* Rp.25.000, *Transaction ID* 202111101012148103010016631272796722 8	x	x
		Send Money to Friend	*Send Money* Rp.10.000 ke Bos Lacoolla xxxxxxxx6656, *Transaction ID* 202111101214200101001664127279596 05, *Remarks* biru tempat uang	x	x
		Send Money	*Receive Money* Rp.10.000 from Bos Lacoolla 085156696xxx, *Transaction ID* 202111101012142001010016652942778824 3, *Remarks* bendera biru	x	x
		Send Money to Bank	*Send Money* Rp.20.000 *to* M.NOOR FADILAH Mandiri xxxx8216, *Transaction ID* 202111101021420010100166412727978872, *Remarks* bendera biru kirim ke livin	x	x
2	Dompet Digital B	*Top up*	*Top up* Rp.25.000, *Transaction ID* 052021111005058SHD1XjtTNpID	√	√
		Pay to friends	*Sent to* Bos Lacoolla xxxxxxxx6656 Rp.10.000, *Transaction ID* 0120211110033807xMQatxQKSYID, *Note:* tempat duit ijo	√	√

...ke halalaman selanjutnya

TabelIV – lanjutan

No	Nama Aplikasi	Jenis Transaksi	Deskripsi Transaksi	*Tools* Forensik	
				Autopsy	Belkasoft
		Pay to friends	*Sent to* Bos Lacoolla xxxxxxxx6656 Rp.10.000, *Transaction ID* 0520211110034058mSo4JVfo7gID, *Note:* ojek kepala burung	√	√
		Pay to friends	*Received from* Bos Lacoolla xxxxxxxx6656 Rp.10.000, *Transaction ID* 0120211110034951TIqL7lmMvQID, *Note:* jaket ijo kepala burung	√	√
		Pay to friends (request)	*Received from* Bos Lacoolla xxxxxxxx6656 Rp.10.000, *Transaction ID* 0220211110035042rw09CwXSD8ID, *Note:* (req) jaket ijo kepala burung	√	√
		Bank Transfer	*Transfer to* Mandiri xxxx8216 Rp.12.500, *Transaction ID* 0320211110035722lVuh7dKUivID	√	√
3	Dompet Digital C	*Top up*	*Top Up* Rp.25.000, *No.referensi* 210000-20211110094712-114188-00000IM-00000middleware	x	x
		Transfer ke Sesama	Transfer ke Bos Lacoolla Rp.10.000, No.Referensi SPR-9925802037, Pesan: tempat uang ungu bulat	x	x
		Transfer ke Sesama	Transfer dari Bos Lacoolla Rp.10.000, No.Referensi SPR-99258859735, Pesan: ok, plastic hitam	x	x
		Transfer ke Rekening Bank	*Outgoing Transfer to* BANK MANDIRI-M.NOOR FADILLAH, No.Referensi 217937532f5e6c15dac4cf67488b70f611127216, Pesan: ungu kirim ke livin	x	x
4	Dompet Digital D	*Top up*	*Top Up* Rp.40.000, No.Transaksi 050752362906422223, No.Referensi 3094496467962200207	x	x
		Transfer	Transfer ke Bos Lacoolla xxxxxxxx6656, No.Transaksi 005199470250955041, No.Referensi 000374450245364866 t	√	x
		Transfer	Transfer dari Bos Lacoolla xxxxxxxx6656, No.Transaksi 038017283293008920, No.Referensi 058478631142138580	√	√

Pada Tabel IV menunjukan perbandingan data yang berhasil ditemukan pada masing-masing *tools* forensik, dari 17 data aktivitas transaksi yang ditemukan dengan menggunakan tiga tools forensik dapat dihitung indeks kemampuan dari masing-masing *tools* forensik dengan menggunakan Rumus 1. sebagai berikut.
Perhitungan angka indeks yang digunakan ditunjukkan pada Rumus 1 [16].

$$Par = \frac{\sum ar0}{\sum arT} \times 100\% \quad (1)$$

Par = angka index
ar0 = jumlah yang terdeteksi *tools* forensik
arT = jumlah total keseluruhan bahan

$Autopsy\ Par = \frac{\sum ar0}{\sum arT} \times 100\% = \frac{8}{17} \times 100\% = 47,05\%$

$Belkasoft\ Evidence\ Center\ Par = \frac{\sum ar0}{\sum arT} \times 100\% = \frac{7}{17} \times 100\% = 41,17\%$

Berdasarkan perhitungan indeks kemampuan dari masing-masing *tools* forensik dalam menemukan informasi terkait aktivitas transaksi pada aplikasi dompet digital, didapatkan hasil bahwa *tool* forensik Autopsy berhasil mendapatkan 8 data transaksi dengan indeks presentase sebesar 47,05%, sedangkan *tool* forensik Belkasoft Evidence Center mendapatkan 7 data aktivitas transaksi dengan presentase sebesar 41.17%.

IV. Simpulan

Berdasarkan hasil forensik pada empat aplikasi dompet digital dengan menggunakan *tools* forensik Autopsy dan Belkasoft Evidence Center menggunakan metode *Digital Forensik Research Workshop* (DFRWS), berhasil menemukan bukti digital terkait informasi aktivitas transaksi yang dilakukan pada beberapa aplikasi dompet digital. Dari total 17 data aktivitas transaksi yang dilakukan, *tools* forensic Autopsy berhasil menemukan 8 aktivitas transaksi dengan presentase kemampuan *tools* forensic menemukan data sebesar 47,05%, sedangkan pada tool forensic Belkasoft Evidence Center mendapatkan 7 aktivitas transaksi dengan sebesar 41,17%.

Ucapan Terima Kasih

Terima Kasih kepada segenap akademisi Fakultas Magister Teknik Informatika Universitas Ahmad Dahlan Yogyakarta atas bantuan secara moral sehingga dapat menyelesaikan karya ilmiah ini.

Pustaka

[1] Asosiasi Penyelenggara Jasa Internet Indonesia, “Laporan Survei Internet APJII 2019 – 2020,” Asos. Penyelenggara Jasa Internet Indones., vol. 2020, pp. 1–146, 2020.
[2] J. W. N. Agusta, “Mobile Payments in Indonesia: Race to Big Data Domination,” 2018.
[3] Ipsos, “Indonesia ‘The Next Cashless Society,’” 2020.
[4] I. Zuhriyanto, A. Yudhana, and I. Riadi, “Perancangan Digital Forensik pada Aplikasi Twitter Menggunakan Metode Live Forensics,” in Seminar Nasional Informatika 2008 (semnasIF 2008), 2018, vol. 2018, no. November, pp. 86–91.
[5] R. Umar and Sahiruddin, “Metode Nist Untuk Analisis Forensik Bukti Digital Pada Perangkat Android,” in Prosiding SENDU_U_2019, 2019, pp. 978–979.
[6] A. Yudhana, R. Umar, and A.- Ahmadi, “Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ),” J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf., vol. 4, no. 1, p. 8, 2018.
[7] 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.
[8] A. Yudhana, I. Riadi, and I. Anshori, “Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist,” It J. Res. Dev., vol. 3, no. 1, pp. 13–21, 2018.
[9] H. H. Lwin and W. P. Aung, “Forensics Analysis of Mobile Financial Applications Used in Myanmar,” Proc. First Univ. Res. Conf. Sci. Eng., vol. 1, pp. 19–24, 2020.
[10] O. Osho, U. L. Mohammed, N. N. Nimzing, A. A. Uduimoh, and S. Misra, “Forensic Analysis of Mobile Banking Apps,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 11623 LNCS, pp. 613–626, 2019.
[11] R. Chanajitt, W. Viriyasitavat, and K. K. R. Choo, “Forensic analysis and security assessment of Android m-banking apps,” Aust. J. Forensic Sci., vol. 50, no. 1, pp. 3–19, 2018.
[12] Y. Konduru, N. Mishra, and S. Sharma, “Acquisition and analysis of forensic data artefacts of some popular apps in android smartphone,” Proc. - IEEE 16th Int. Conf. Dependable, Auton. Secur. Comput. IEEE 16th Int. Conf. Pervasive Intell. Comput. IEEE 4th Int. Conf. Big Data Intell. Comput. IEEE 3, pp. 94–99, 2018.
[13] R. Harris, “Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem,” Digit. Investig., vol. 3, no. SUPPL., pp. 44–49, 2006.
[14] Y. Yusoff, R. Ismail, and Z. Hassan, “Common Phases of Computer Forensics Investigation Models,” Int. J. Comput. Sci. Inf. Technol., vol. 3, no. 3, pp. 17–31, 2011.
[15] G. Palmer, “A Road Map for Digital Forensic Research,” in The Digital Forensic Research Conference, 2001.
[16] 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.