Kumpulan jurnaL Ilmu Komputer (KLIK)
Volume 09 No.02 2022
ISSN: 2406-7857

ANALISIS FORENSIK APLIKASI DOMPET DIGITAL PADA *SMARTPHONE* ANDROID MENGGUNAKAN METODE DFRWS

Muhammad Noor Fadillah[1], Rusydi Umar[2], Anton Yudhana[3]
[1,2]Program Studi Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta
[3] Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
Jalan Prof.Dr.Soepomo, S.H., Janturan, Warungboto, Umbulharjo, Yogyakarta, Indonesia
email : muhammad1807048006@webmail.uad.ac.id[1], rusydi@mti.uad.ac.id[2], eyudhana@ee.uad.ac.id[3]

Abstract

Along with the emergence of app digital wallet in Indonesia, the use of smartphone devices has the function not only as a communication tool, but also began to be used as a tool to perform payment transactions. There are some companies financial technology in Indonesia, which offers a digital wallet service. Behind the ease of that is given of the use of the app a digital wallet, the utilization of the negative-tipped in the case of cybercrime. This research will make the process of forensic on one of the wallet app digital popular in Indonesia, using the tools of forensic Belkasoft Evidence Center and MOBILedit Forensic Express, the process of forensic follow the guidelines on the method of Digital Forensic Research Workshop (DFRWS), which consists of several stages of forensic covers the identification, preservation, collection, examination, analysis and presentation.

This study was conducted to provide an overview of the process of forensic on the application of a digital wallet to search for information, particularly related to transactions conducted on the application of digital wallets, so that the digital evidence obtained from the forensics process can be used as evidence pursuant to the UU ITE about the power of the law of evidence in the digital. From the research that has been done on the application of a digital wallet, managed to get the information in the form of user's data and history transaction activity, with a percentage of data found in the wallet app digital by 100%.

***Keywords**:* Forensic Mobile, Digital Evidence, Digital Wallet Apps, DFRWS

Abstrak

Seiring dengan munculnya aplikasi dompet digital di Indonesia, penggunaan perangkat *smartphone* memiliki fungsi tidak hanya sebagai alat komunikasi, akan tetapi juga mulai digunakan sebagai alat untuk melakukan transaksi pembayaran. Terdapat beberapa perusahaan *financial technology* di Indonesia yang menawarkan layanan dompet digital. Dibalik kemudahan yang diberikan dari penggunaan aplikasi dompet digital, bisa saja terdapat pemanfaatan negatif yang berujung pada kasus *cybercrime*. Penelitian ini akan melakukan proses forensik pada salah satu aplikasi dompet digital yang popular digunakan di Indonesia, menggunakan *tools* forensik Belkasoft Evidence Center dan MOBILedit Forensic Express, proses forensik mengikuti pedoman metode Digital Forensik Research Workshop (DFRWS) yang terdiri dari beberapa tahapan forensik meliputi *identification,*

preservation, collection, examination, analysis dan *presentation*, dilakukan untuk memberikan gambaran proses forensik pada aplikasi dompet digital untuk mencari informasi, khususnya terkait aktivitas transaksi yang dilakukan pada aplikasi dompet digital, sehingga bukti digital yang didapatkan dari proses forensik dapat dijadikan sebagai barang bukti berdasarkan UU ITE tentang kekuatan hukum alat bukti digital. Dari penelitian yang telah dilakukan pada aplikasi dompet digital, berhasil mendapatkan informasi berupa data pengguna dan *history* aktivitas transaksi, dengan presentase data yang ditemukan pada aplikasi dompet digital sebesar 100%.

***Kata kunci**:* Forensik Mobile, Bukti Digital, Aplikasi Dompet Digital, DFRWS

1. PENDAHULUAN

Berdasarkan laporan survei internet oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2019-2020 Q2, 95,4% penduduk Indonesia mengakses internet dengan menggunakan perangkat *smartphone* (Asosiasi Penyelenggara Jasa Internet Indonesia, 2020), dengan sistem operasi *smartphone* yang digunakan terbanyak sebesar 92,3% adalah android (DataReportal, 2021). Pengggunaan perangkat *smartphone* di Indonesia sudah mulai berkembang penggunaannya, tidak hanya sebagai alat untuk berkomunikasi akan tetapi dengan seiring munculnya aplikasi dompet digital, penggunaan *smartphone* juga digunakan sebagai alat untuk melakukan transaksi keuangan (Yadi & Kunang, 2014). Dengan meningkatnya penggunaan *smartphone* dan dukungan layanan *internet* hampir diseluruh wilayah membuat beberapa perusahaan di bidang *financial technology* mengeluarkan layanan pembayaran digital untuk mengurangi transaksi tunai, hal ini sejalan dengan program pemerintah yang mendorong untuk transaksi non tunai dengan Gerakan Nasional Non Tunai (GNNT) pada tahun 2014 (Prayogo, Riadi, & Luthfi, 2017). Berdasarkan presentase jumlah penggunanya, aplikasi dompet digital yang popular digunakan di Indonesia dapat dilihat sebagai berikut : OVO 33.6%, Gopay 29.2%, DANA 14.7%, LinkAja 9.4%, dan lainnya 6.3% (Ipsos, 2020)

Perkembangan teknologi seperti aplikasi dompet digital selain menawarkan beragam kemudahan penggunanya dalam bertransaksi, tetapi juga bisa dimanfaatkan secara negatif. Kasus *cybercrime* tidak terlepas dari kontrol penggunanya ketika menggunakan aplikasi yang dimiliki pada *smartphone* (Yudhana, Riadi, & Zuhriyanto, 2019). Terlebih perangkat *smartphone* sudah menjadi media yang banyak digunakan untuk melakukan suatu tindak kejahatan dan menjadi barang bukti pada kasus *cybercrime* (Umar & Sahiruddin, 2019), maka untuk menangani kasus *cybercrime*, Indonesia memiliki undang-undang tentang ITE (informasi dan Transaksi Elektronik) yang pada UU 11/2018 berisi tentang dasar hukum mengenai alat bukti elektronik dan syarat formil dan materil alat bukti elektronik sebagai kekuatan hukum sehingga dapat diterima di pengadilan (Sitompul, 2012).

Ketika suatu kasus *cybercrime* mendapatkan barang bukti berupa perangkat *smartphone*, maka untuk mendapatkan alat bukti elektronik diperlukan proses forensik, dimana salah satu prosesnya yaitu proses akusisi pada penyimpanan *smartphone* untuk mendapatkan bukti digital (Yudhana, Umar, & Ahmadi, 2018). Dengan melakukan proses forensik pada barang bukti *smartphone*, dimungkinkan

bisa mendapatkan informasi atau artefak digital terkait aktivitas yang dicurigai menjadi bagian *cybercrime*, dan artefak digital yang didapatkan dari proses forensik bisa menjadi bukti digital yang menjadi penghubung antara data dan tersangka (Umar, Yudhana, & Faiz, 2018). Pada proses forensik, kondisi *smartphone* sangat perpengaruh terhadap bukti digital yang didapatkan, *smartphone* dengan kondisi *root* lebih memungkinkan untuk mendapatkan bukti digital dibandingkan dengan *smartphone* dengan kondisi tidak *root* (Riadi, Yudhana, & Putra, 2018a). Selain kondisi *smartphone*, *tools* forensik yang digunakan dalam proses forensik juga mempengaruhi hasil dari bukti digital yang dapat diakusisi (Riadi, Yudhana, & Putra, 2018b).

Penelitian ini akan melakukan proses forensik terhadap salah satu aplikasi dompet digital yang popular digunakan di Indonesia, dengan tujuan untuk memberikan gambaran proses forensik mencari informasi khususnya terkait transaksi yang dilakukan dengan menggunakan aplikasi dompet digital. Berdasarkan aturan forensik digital dan menjaga integritas keaslian bukti digital, proses forensik mengikuti prosedur metode forensik Digital Forensic Research Workshop (DFRWS) yang memiliki beberapa tahapan forensik meliputi *identification, preservation, collection, examination, analysis* dan *presentation.* Dan proses akusisi dan analisis menggunakan *tools* forensik yang sudah diakui dan umum digunakan, yaitu Belkasoft Evidence Center dan MOBILedit Forensic Express.

2. METODOLOGI PENELITIAN

2.1 Alat dan Bahan Penelitian

Alat dan bahan yang digunakan pada penelitian ini dapat dilihat pada tabel 1 dan perangkat lunak *(software)* yang digunakan dapat dilihat pada tabel 2. Berdasarkan etika professional, nama aplikasi dompet digital yang digunakan pada penelitian ini tidak akan disebutkan.

Tabel 1. Alat penelitian

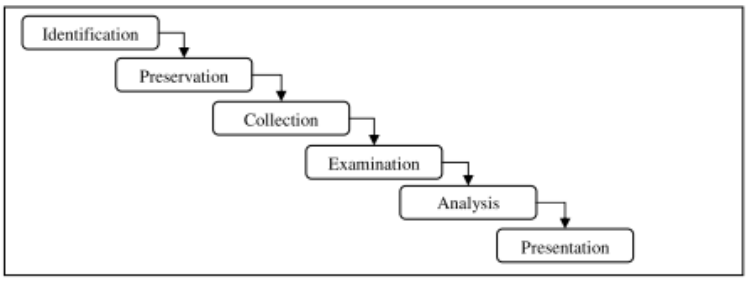
No	Alat penelitian	Deskripsi/spesifikasi
1	*Smartphone*	Xiaomi Redmi Note 3 MTK Android 5.0.2 Rooted
2	Laptop (*workstation*)	Toshiba Satellite C40-A Windows 10
3	USB *Cable*	*Type* B

Tabel 2. *Software* pendukung penelitian

No	*Software*	Nama	Versi
1	Aplikasi Dompet Digital	Dompet Digital X	4.31.1
2	*Tools Forensik*	Belkasoft Evidence Center	9.9
		MOBILedit Forensic Express	7.0.2
3	*Tool Hashing*	HashMyFiles	2.42

2.2 Metode Penelitian

Penelitian ini menggunakan metode Digital Forensic Research Workshop (DFRWS), metode ini merupakan metode ilmiah yang digunakan pada digital forensik dan telah teruji untuk membantu mendapatkan barang bukti digital (Harris, 2006).



Gambar 1. Model investigasi DFRWS (Yusoff, Ismail, & Hassan, 2011)

Berdasarkan Metode Digital Forensic Research Workshop (DFRWS), terdapat beberapa tahapan yang harus dilakukan (Palmer, 2001), sebagai berikut :

a. Identification

Tahap ini merupakan proses identifikasi dilakukan untuk menentukan kebutuhan yang apa saja yang diperlukan pada penyelidikan dan pencarian barang bukti.

b. 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.

c. Collection

Melakukan proses pengumpulan identifikasi bagian yang khusus dari barang bukti digital dan melakukan identifikasi sumber data.

d. 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.

e. Analysis

Melakukan melakukan penentuan tentang dimana data tersebut dihasilkan, oleh siapa data tersebut dihasilkan, bagaimana data tersebut dihasilkan dan kenapa data tersebut dihasilkan.

f. 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.

2.3 Simulasi Kasus

Penelitian ini menggunakan satu buah perangkat *smartphone* Android Xiaomi Redmi Note 3 MTK yang disimulasikan sebagai barang bukti suatu kasus *cybercrime*, dimana pada barang bukti *smartphone* terdapat aplikasi dompet digital yang dicurigai digunakan untuk bertransaksi terkait kasus kejahatan. Pada perangkat *smartphone* sebelumnya sudah di *instal*kan salah satu aplikasi dompet digital yang popular digunakan di Indonesia dan akun yang digunakan adalah akun peneliti yang sudah terverifikasi. Pada aplikasi dompet digital sudah dilakukan aktivitas transaksi dengan rincian pada tabel 3.

Tabel 3. Aktivitas Transaksi yang sudah dilakukan pada Aplikasi Dompet Digital

No	Nama Aplikasi	Waktu Transaksi	Jenis Transaksi	Deskripsi Transaksi
1	Dompet Digital	10 Nov 2021 9:50	*Top Up*	*Top up* Rp.25.000, *Transaction ID* 052021111005058SHD1XjtTNpID
		10 Nov 2021 10:38	*Pay to friends*	*Sent to* Bos Lacoolla xxxxxxxx6656 Rp.10.000, *Transaction ID* 0120211110033807xMQatxQKSYID, *Note:* tempat duit ijo
		10 Nov 2021 10:40	*Pay to friends*	*Sent to* Bos Lacoolla xxxxxxxx6656 Rp.10.000, *Transaction ID* 0520211110034058mSo4JVfo7gID, *Note:* ojek kepala burung
		10 Nov 2021 10:49	*Pay to friends*	*Received from* Bos Lacoolla xxxxxxxx6656 Rp.10.000, *Transaction ID* 0120211110034951TIqL7lmMvQID, *Note:* jaket ijo kepala burung
		10 Nov 2021 10:50	*Pay to friends (request)*	*Received from* Bos Lacoolla xxxxxxxx6656 Rp.10.000, *Transaction ID* 0220211110035042rw09CwXSD8ID, *Note:* (req) jaket ijo kepala burung
		10 Nov 2021 10:57	Bank *Transfer*	*Transfer to* Mandiri xxxx8216 Rp.12.500, *Transaction ID* 0320211110035722lVuh7dKUivID

3. HASIL DAN PEMBAHASAN

Berdasarkan metode DFRWS, berikut tahapan proses forensik pada barang bukti smartphone untuk mencari informasi/dokumen elektronik yang ada pada aplikasi dompet digital.

3.1. *Identification*

Tahapan awal dalam menentukan kebutuhan yang diperlukan pada saat proses penyidikan dan pencarian barang bukti

Perangkat *smartphone*

Berdasarkan barang bukti yang digunakan, yaitu satu buah *smartphone* Android dengan spesifikasi seperti pada tabel 4.

Tabel 4. Spesifikasi barang bukti *smartphone*

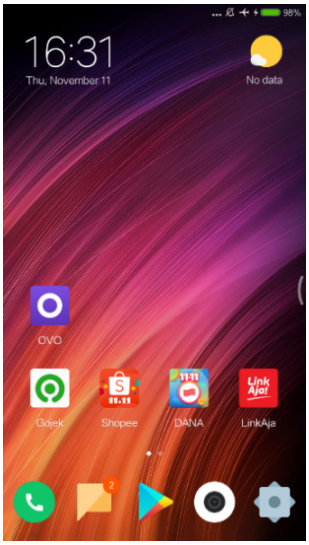
Spesifikasi barang bukti *smartphone*	
Brand	Xiaomi
Model number	Redmi Note 3
Platform	Android (5.0.2)
Serial number	VCS8MVQSYLCMxxxx
Imei	86967702723xxxx
Ram	2GB
Rom	16GB
rooted	Yes

Tools forensic

Tools forensic yang digunakan dalam proses *forensic* berdasarkan tabel, yaitu Belkasoft Evidence Center dan MOBILedit Forensic Express

3.2 *Preservation*

Tahap *preservation* yaitu untuk menjaga barang bukti digital, memastikan keaslian bukti dan menyangkal klaim jika barang bukti telah disabotase. Maka barang bukti perangkat *smartphone* akan di simpan ditempat yang aman dan terisolasi dari semua jenis komunikasi, maka semua koneksi pada *smartphone* akan dimatikan dengan cara mengaktifkan *airplane mode* pada perangkat *smartphone*, seperti pada gambar 2.

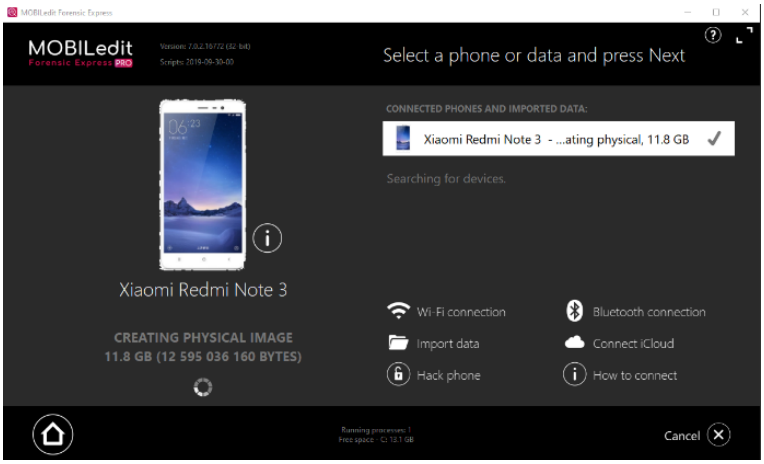


Gambar 2. Mengisolasi barang bukti dari semua jaringan

3.3 Collection

Tahap *collection* dilakukan dengan menggunakan *tools forensik* untuk menjaga integritas sumber data berubah atau rusak. Tahap Collection akan dilakukan dengan menggunakan *tool* forensik MOBILedit Forensic Express, dengan kemampuan dapat melakukan proses membuat *physical image* dari data yang ada pada *smartphone* Android.

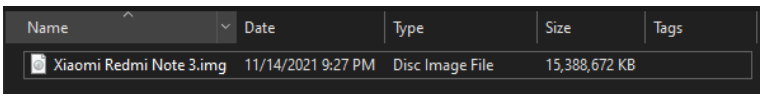
Proses pertama yang dilakukan yaitu menghubungkan perangkat *smartphone android* dengan laptop sebagai *workstation* yang sudah terinstal aplikasi MOBILedit Forensic Express, seperti pada gambar 3.



Gambar 3. Proses membuat *physical image* menggunakan *tool* Forensik MOBILedit Forensik Express

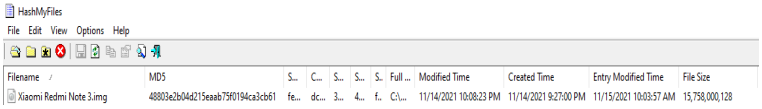
Langkah membuat *physical image* dari barang bukti perangkat *smartphone android* dilakukan untuk menghindari kerusakan pada perangkat asli, proses forensik tidak dilakukan langsung pada perangkat asli, melainkan menggunakan *file physical image smartphone*. Setelah proses membuat *physical image* dari barang

bukti *smartphone* selesai, akan menghasilkan *file* dengan ekstensi *.img*, pada penelitian ini menghasilkan *file* dengan nama Xiaomi Redmi Note 3.img, seperti pada gambar 4.



Gambar 4. *file physical image* dari *smartphone*

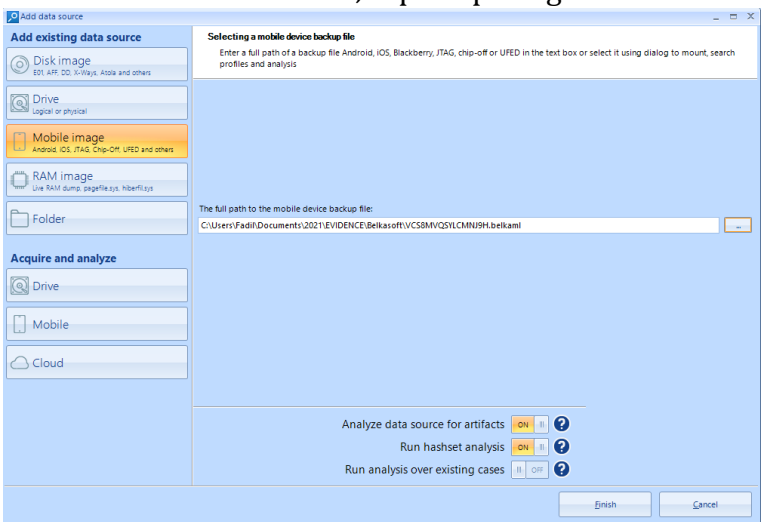
File physical image dari proses diatas dilakukan *hashing* untuk menjaga kevalidan barang bukti digital dengan *tool* HashMyFiles, pada *file* Xiaomi Redmi Note 3.img didapatkan nilai MD5 48803e2b04d215eaab75f0194ca3cb61, seperti pada gambar 5.



Gambar 5. Nilai MD5 dari *file physical image*

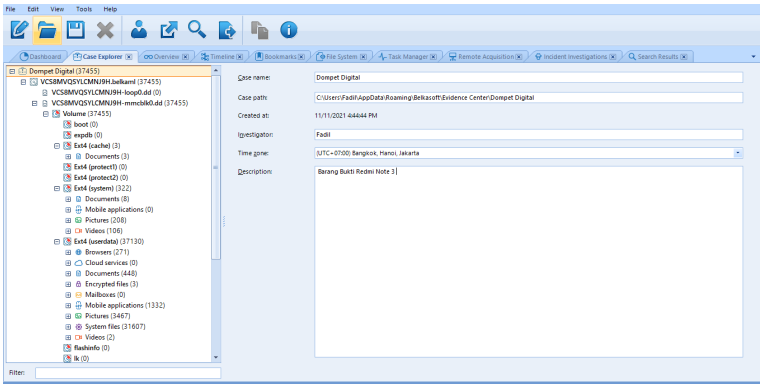
3.4 Examination

Tahap *Examination* dilakukan dengan menggunakan data dari *physical image* barang bukti *smartphone* yang sudah dilakukan sebelumnya. Proses selanjutnya yaitu *extraction* (ekstraksi) dari *file physical image* sehingga semua data pada *physical image* dari *smartphone* akan terekstraksi, proses ekstraksi menggunakan *tool* Forensik Belkasoft Evidence Center, seperti pada gambar 6.



Gambar 6. Proses ekstraksi *file physical image* menggunakan Belkasoft Evidence Center

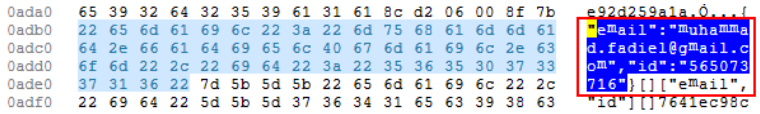
Hasil ekstraksi dari *file physical image* dengan menggunakan *tool* forensik Belkasoft Evidence Center ditampilkan pada *menu case* seperti pada gambar 7.



Gambar 7. Hasil ekstraksi pada *tool* forensik Belkasoft Evidence Center

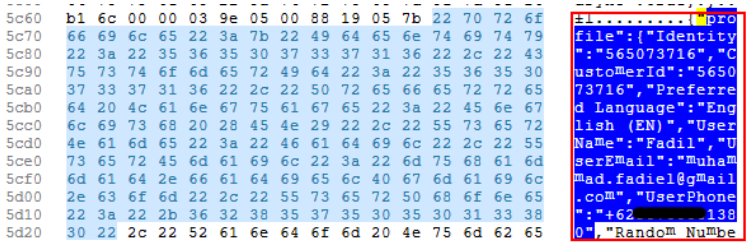
3.5 Analysis

Proses analysis dilakukan secara manual dengan *tool* forensik Belkasoft Evidence Center, menggunakan data dari hasil ekstraksi *file physical image* perangkat *smartphone android* yang dijadikan barang bukti. Proses analisis akan berfokus pada direktori *data/data/<package_name>* dari aplikasi dompet digital. Pada proses analisis terhadap aplikasi dompet digital didapatkan informasi data pengguna pada *folder database file instabug.db* berupa *email* dan *userid* pengguna, seperti pada Gambar 8.



Gambar 8. Informasi data pengguna yang ditemukan pada *file instabug.db*

Pada *folder database file clevertap* ditemukan informasi berupa *userid, username, email,* dan nomor kontak pengguna, seperti yang ditampilkan pada gambar 9.



Gambar 9. Informasi data pengguna yang ditemukan pada *file clevertap*

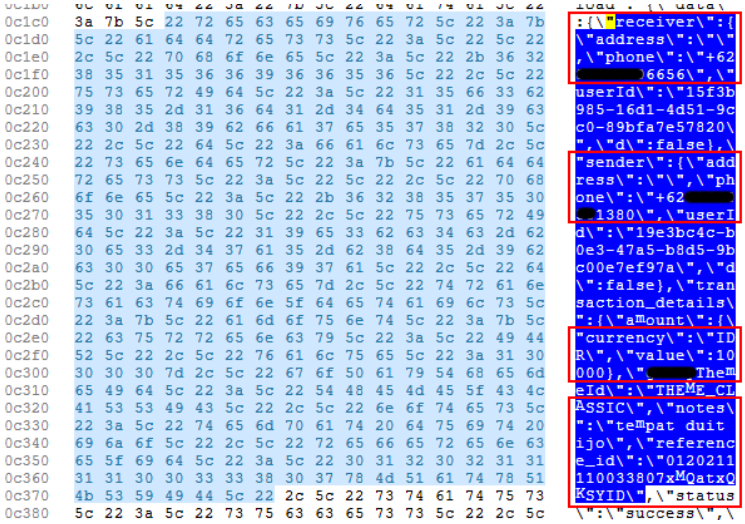
Informasi terkait aktivitas transaksi yang dilakukan dengan aplikasi dompet digital ditemukan pada *folder cache file* b23cff29ac58336ad 9145a431d4f9925.1. Pada *file* tersebut ditemukan enam aktivitas transaksi yang pernah dilakukan dan salah satunya ditampilkan pada gambar 10, dengan rincian aktivitas transaksi ditampilkan pada tabel 5.

Gambar 10. Aktivitas transaksi yang ditemukan pada aplikasi dompet digital

Tabel 5. Rincian aktivitas transaksi yang ditemukan pada aplikasi dompet digital

No	Id transaksi	Waktu	Deskripsi	Jumlah	Catatan
1	0320211110035722IV uh7dKUivID	10-11-2021 10:57:24	Transfer ke Bank Mandiri xxxx8216	Rp.12.500	
2	0220211110035042rw 09CwXSD8ID	10-11-2021 10:50:42	Received from Bos Lacoolla xxxxxxxx6656	Rp.10.000	(req) jaket ijo kepala burung
3	0120211110034951Tl qL7ImMvQID	10-11-2021 10:49:51	Received from Bos Lacoolla xxxxxxxx6656	Rp.10.000	jaket ijo kepala burung
4	0520211110034058mS o4JVfo7gID	10-11-2021 10:40:59	Sent to Bos Lacoolla xxxxxxxx6656	Rp.10.000	ojek kepala burung
5	0120211110033807xM QatxQKSYID	10-11-2021 10:38:07	Sent to Bos Lacoolla xxxxxxxx6656	Rp.10.000	tempat duit ijo
6	052021111005058SHD 1XjtTNpID	10-11-2021 09:50:58	Top Up	Rp.25.000	Mandiri

Pada *folder database file conversations-database*, ditemukan tiga aktivitas transaksi, salah satunya ditampilkan pada gambar 11 dengan rincian aktivitas transaksi ditampilkan pada tabel 6.



Gambar 11. Aktivitas transaksi yang ditemukan pada *file conversations-database*

Tabel 6. Rincian aktivitas transaksi pada *file conversations-database*

No	*Id reference*	Penerima	Pengirim	Jumlah	Catatan
1	0120211110033807xMQatxQKSYID	+62xxxxxxx6656	+62xxxxxxx1380	Rp.10.000	tempat duit ijo
2	0520211110034058mSo4JVfo7gID	+62xxxxxxx6656	+62xxxxxxx1380	Rp.10.000	ojek kepala burung
3	0220211110035042rw09CwXSD8ID	+62xxxxxxx1380	+62xxxxxxx6656	Rp.10.000	(req) jaket ijo kepala burung

3.6 Presentation

Tahap *presentation* yaitu menjelaskan *tools* forensik dan metode yang digunakan pada proses forensik dan menyampaikan informasi dari hasil analisis berdasarkan barang bukti yang didapatkan. Berdasarkan barang bukti pada penelitian ini, yaitu satu buah *smartphone android* Redmi Note 3 MTK. Telah dilakukan proses forensik mengikuti prosedur metode forensik Digital Forensic Research Workshop (DFRWS) menggunakan *tool* Forensik MOBILedit Forensik Express pada tahap akusisi dengan menghasilkan *file physical image* dengan nama *file* Xiaomi Redmi Note 3.img dan nilai MD5 48803e2b04d215eaab75f0194ca3cb61. pada tahap analisis dilakukan dengan menggunakan *tool* forensik Belkasoft Evidence Center. Dari proses forensic yang dilakukan berhasil ditemukan data terkait aktivitas transaksi yang pernah dilakukan pada aplikasi dompet digital sebanyak enam aktivitas transaksi dengan rincian seperti pada tabel 7.

Tabel 7. Enam aktivitas transaksi yang berhasil ditemukan pada aplikasi dompet digital

No	Nama Aplikasi	Jenis Transaksi	Deskripsi Transaksi	*Tool* Forensik Belkasoft
1	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	√
		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	√

Berdasarkan Tabel 7, dapat dihitung indeks aktivitas transaksi yang berhasil ditemukan pada aplikasi dompet digital. Perhitungan angka indeks menggunakan rumus 1 (Riadi, Umar, & Firdonsyah, 2018).

$$Par = \frac{\sum ar0}{\sum arT} \text{ x } 100\% \qquad (1)$$

Par = angka indeks
$ar0$ = jumlah yang terdeteksi tools forensik
arT = jumlah total keseluruhan aktivitas transaksi yang dilakukan

Indeks aktivitas transaksi yang ditemukan pada dompet digital

$$Par = \frac{\sum ar0}{\sum arT} \text{ x } 100\% = \frac{6}{6} \text{ x } 100\% = 100\%$$

Berdasarkan perhitungan indeks aktivitas transaksi yang ditemukan pada proses forensik dengan menggunakan *tools* forensik MOBILedit Forensik Express dan Belkasoft Evidence Center, didapatkan hasil bahwa aktivitas transaksi yang dapat ditemukan pada aplikasi dompet digital yang digunakan pada barang bukti *smartphone android* Redmi Note 3 MTK memiliki indeks sebesar 100%.

4. SIMPULAN

Berdasarkan penelitian yang telah dilakukan pada salah satu aplikasi dompet digital telah berhasil dilakukan proses forensik dengan mengikuti prosedur metode forensik Digital Forensic Research Workshop (DFRWS) yang memiliki beberapa tahapan forensik meliputi *identification, preservation, collection, examination, analysis* dan *presentation.* Menggunakan *tools* forensik Belkasoft Evidence Center dan MOBILedit Forensic Express. Pada proses forensik berhasil mendapatkan informasi berupa data pengguna dan aktivitas transaksi yang ditersimpan pada perangkat *smartphone*. Dari perhitungan angka indeks data aktivitas yang dilakukan pada saat simulasi dan data yang berhasil ditemukan dengan *tools* forensik yaitu sebesar 100%

DAFTAR PUSTAKA

[1] Asosiasi Penyelenggara Jasa Internet Indonesia. (2020). Laporan Survei InternetAPJII 2019 – 2020. *Asosiasi Penyelenggara Jasa Internet Indonesia*, *2020*, 1–146. Retrieved from https://apjii.or.id/survei

[2] DataReportal. (2021). Digital 2021 Indonesia. Retrieved from https://datareportal.com/reports/digital-2021-indonesia

[3] Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation*, *3*(SUPPL.), 44–49. https://doi.org/10.1016/j.diin.2006.06.005

[4] Ipsos. (2020). Indonesia "The Next Cashless Society."

[5] Palmer, G. (2001). A Road Map for Digital Forensic Research. In *The Digital Forensic Research Conference*. https://doi.org/10.1016/0032-3950(82)90064-8

[6] Prayogo, A., Riadi, I., & Luthfi, A. (2017). Mobile Forensics Development of Mobile Banking Application using Static Forensic. *International Journal of Computer Applications*, *160*(1), 5–10. https://doi.org/10.5120/ijca2017912925

[7] Riadi, I., Umar, R., & Firdonsyah, A. (2018). Forensic tools performance analysis on android-based blackberry messenger using NIST measurements. *International Journal of Electrical and Computer Engineering*, *8*(5), 3991–4003. https://doi.org/10.11591/ijece.v8i5.pp3991-4003

[8] Riadi, I., Yudhana, A., & Putra, M. C. F. (2018a). Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ). *Jurnal Teknik Informatika Dan Sistem Informasi*, *4*(2), 219–227.

[9] Riadi, I., Yudhana, A., & Putra, M. C. F. (2018b). Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method. *Scientific Journal of Informatics*, *5*(2), 235–247. https://doi.org/10.15294/sji.v5i2.16545

[10] Sitompul, J. (2012). *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*. (Tatanusa, Ed.), *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*. Jakarta.

[11] Umar, R., & Sahiruddin. (2019). Metode Nist Untuk Analisis Forensik Bukti Digital Pada Perangkat Android. In *Prosiding SENDU_U_2019* (pp. 978–979).

[12] Umar, R., Yudhana, A., & Faiz, M. N. (2018). Experimental analysis of web browser sessions using live forensics method. *International Journal of Electrical and Computer Engineering*, *8*(5), 2951–2958. https://doi.org/10.11591/ijece.v8i5.pp2951-2958

[13] Yadi, I. Z., & Kunang, Y. N. (2014). Forensik Pada Platform Android. *Konferensi Nasional Ilmu Komputer (KONIK)*, 141–148. Retrieved from http://eprints.binadarma.ac.id/2191/

[14] Yudhana, A., Riadi, I., & Zuhriyanto, I. (2019). Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS). *Jurnal TECHNO*, *20*(2), 125–130.

[15] Yudhana, A., Umar, R., & Ahmadi, A.-. (2018). Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ). *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi*, *4*(1), 8. https://doi.org/10.24014/coreit.v4i1.5803

[16] Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, *3*(3), 17–31. https://doi.org/10.5121/ijcsit.2011.3302