

# PERBANDINGAN TOOLS FORENSIK PADA APLIKASI DOMPET DIGITAL

Rusydi Umar<sup>1</sup>, Anton Yudhana<sup>2</sup>, dan Muhammad Noor Fadillah<sup>3\*</sup>

<sup>1,3</sup>Program Studi Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta

<sup>2</sup>Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta

Email: rusydi@mti.uad.ac.id<sup>1</sup>, eyudhana@ee.uad.ac.id<sup>2</sup>, muhammad1807048006@webmail.uad.ac.id<sup>3</sup>

## 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 Forensic 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 penggunaanya dapat melakukan transaksi seperti melakukan pembayaran, mengirim dan menerima uang, dan menyimpan uang pada *smartphone*. Aplikasi dompet digital banyak digunakan karena kemudahannya 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 populer digunakan berdasarkan jumlah presentase penggunaanya dapat dilihat sebagai berikut : OVO 33,6%, Gopay 29,2%, Link Aja 9,4% dan lainnya 6,3% [3]. Aplikasi dompet digital memberikan penggunaanya 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 penggunaanya 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 informasi 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 menunjukkan 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 profesional, nama aplikasi dompet digital yang digunakan dalam penelitian ini tidak akan disebutkan.

Tabel I: Alat Penelitian

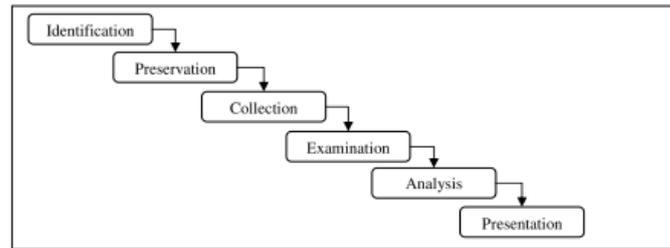
No	Alat penelitian	Deskripsi/spesifikasi
1	<i>Smartphone</i>	Xiaomi Redmi Note 3 MTK Android 5.0.2 Routed
2	Laptop ( <i>workstation</i> )	Toshiba Satellite C40-A Windows 10
3	USB <i>Cable</i>	<i>Type B</i>

Tabel II: Software Pendukung Penelitian

No	<i>software</i>	Nama	Versi
1	Aplikasi Dompet DigitalDompet	Digital A	2.6.0
		Dompet Digital B	4.31.1
		Dompet Digital C	3.47.0
		Dompet Digital D	2.79.09
2	<i>Tools Forensic</i>	Autopsy	4.9.1
		Belkasoft Evidence Center	9.9
3	<i>Tool Hasing</i>	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 bagian 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 <i>smartphone</i>	
<i>Brand</i>	Xiaomi
<i>Model number</i>	Redmi Note 3
<i>Platform</i>	Android (5.0.2)
<i>Serial number</i>	VCS8MVQSYLCMxxxx
<i>Imei</i>	86967702723xxxx
<i>Ram</i>	2GB
<i>Rom</i>	16GB
<i>rooted</i>	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

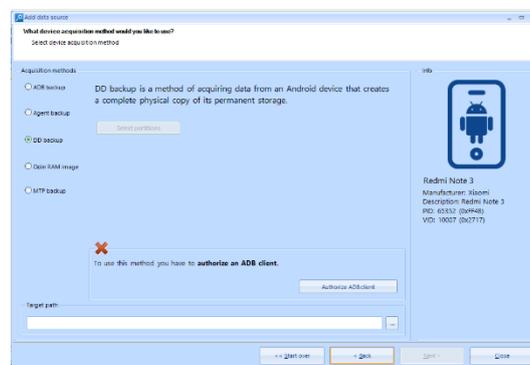
Barang bukti *smartphone* akan disimpan ditempat yang aman dan mengaktifkan *airplane mode* pada *smartphone* untuk mengisolasi barang bukti dari semua jaringan telekomunikasi seperti pada Gambar 2.



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.

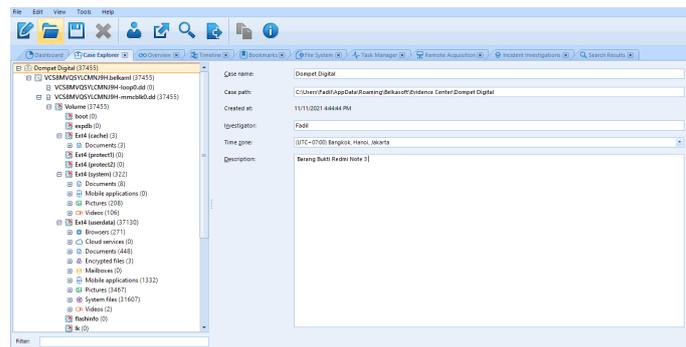
Name	Date modified	Type	Size
VCS8MVQSYLCMNJ9H.belkaml	11/11/2021 6:10 PM	BELKAML File	1 KB
VCS8MVQSYLCMNJ9H-loop0.dd	11/11/2021 4:51 PM	DD File	1,255 KB
VCS8MVQSYLCMNJ9H-mmcbk0.dd	11/11/2021 6:07 PM	DD File	15,388,673 KB
VCS8MVQSYLCMNJ9H-zram0.dd	11/11/2021 6:10 PM	DD File	786,433 KB

Gambar 4: File physical image dari barang bukti smartphone

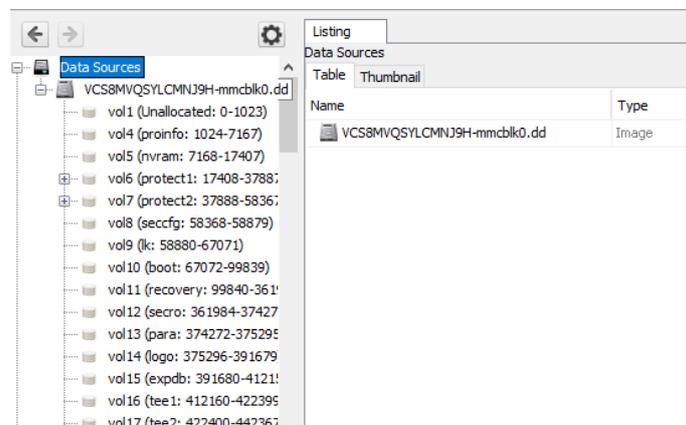
File physical image dari proses akuisisi akan dilakukan hashing dengan tool HashMyFiles untuk menjaga kevalidan barang bukti digital, pada file VCS8MVQSYLCMNJ9H-mmcbk0.dd didapatkan nilai MD5 8b8e63d04c1b222ee8891d46834c3fdc.

#### 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 Dompot 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 memunculkan enam aktivitas transaksi pada folder cache file b23cff29ac58336ad9145a431d4f9925.1 seperti pada Gambar 7 dan tiga aktivitas transaksi ditemukan pada folder database file conversations-database seperti pada Gambar 8.

```

0630 20 20 20 22 6f 72 64 65 72 5f 69 64 22 3a 20 22
0640 30 33 32 30 32 31 31 31 31 30 30 33 35 37 32 32
0650 49 56 75 68 37 64 4b 55 69 76 49 44 22 2c 0a 20
0660 20 20 20 20 20 20 20 20 20 20 20 22 73 65 72 76
0670 69 63 65 5f 74 79 70 65 22 3a 20 22 57 49 54 48
0680 44 52 41 57 41 4c 22 2c 0a 20 20 20 20 20 20 20
0690 20 20 20 20 20 22 73 74 61 74 75 73 22 3a 20 22
06a0 43 4f 4d 50 4c 45 54 45 44 22 2c 0a 20 20 20 20
06b0 20 20 20 20 20 20 20 20 22 64 69 73 70 6c 61 79
06c0 5f 73 74 61 74 75 73 22 3a 20 22 43 6f 6d 70 6c
06d0 65 74 65 64 22 2c 0a 20 20 20 20 20 20 20 20
06e0 20 20 20 22 6f 72 64 65 72 5f 74 69 6d 65 73 74
06f0 61 6d 70 22 3a 20 22 32 30 32 31 2d 31 31 2d 31
0700 30 54 30 33 3a 35 37 3a 32 34 22 2c 0a 20 20 20
0710 20 20 20 20 20 20 20 20 22 6f 72 64 65 72 5f
0720 69 6d 61 67 65 22 3a 20 22 68 74 74 70 73 3a 2f
0730 2f 69 2e 67 6f 6a 65 6b 61 70 69 2e 63 6f 6d 2f
0740 64 61 72 6b 72 6f 6f 6d 2f 6e 65 61 72 62 79 2d
0750 63 6d 73 2d 69 64 2f 76 32 2f 69 6d 61 67 65 73
0760 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 66
0770 69 6c 65 2f 31 38 37 37 2f 33 65 62 35 62 63 61
0780 33 2d 66 30 65 66 2d 34 38 35 39 2d 38 63 64 31
0790 2d 32 39 66 61 33 65 33 33 32 62 38 31 2e 70 6e
07a0 67 22 2c 0a 20 20 20 20 20 20 20 20 20 20 20
07b0 22 64 65 73 63 72 69 70 74 69 6f 6e 22 3a 20 22
07c0 54 72 61 6e 73 66 65 72 20 74 6f 20 4d 61 6e 64
07d0 69 72 69 22 2c 0a 20 20 20 20 20 20 20 20 20
07e0 20 20 22 70 61 79 6d 65 6e 74 5f 74 79 70 65 22
07f0 3a 20 22 44 45 42 49 54 22 2c 0a 20 20 20 20
0800 20 20 20 20 20 20 22 61 6d 6f 75 6e 74 22 3a
0810 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20
0820 20 22 63 75 72 72 65 6e 63 79 22 3a 20 22 49 44
0830 52 22 2c 0a 20 20 20 20 20 20 20 20 20 20 20
0840 20 20 22 76 61 6c 75 65 22 3a 20 31 32 35 30 30
0850 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 20
    
```

Gambar 7: Proses ekstraksi menggunakan Autopsy

```

0c1c0 3a 7b 5c 22 72 65 63 65 69 76 65 72 5c 22 3a 7b
0c1d0 5c 22 61 64 64 72 65 73 73 5c 22 3a 5c 22 5c 22
0c1e0 2c 5c 22 70 68 6f 6e 65 5c 22 3a 5c 22 2b 36 32
0c1f0 38 35 31 35 36 36 39 36 36 35 36 5c 22 2c 5c 22
0c200 75 73 65 72 49 64 5c 22 3a 5c 22 31 35 66 33 62
0c210 39 38 35 2d 31 36 64 31 2d 34 64 35 31 2d 39 63
0c220 63 30 2d 38 39 62 66 61 37 65 35 37 38 32 30 5c
0c230 22 2c 5c 22 64 5c 22 3a 66 61 6c 73 65 7d 2c 5c
0c240 22 73 65 6e 64 65 72 5c 22 3a 7b 5c 22 61 64 64
0c250 72 65 73 73 5c 22 3a 5c 22 5c 22 2c 5c 22 70 68
0c260 6f 6e 65 5c 22 3a 5c 22 2b 36 32 38 35 37 35 30
0c270 35 30 31 33 38 30 5c 22 2c 5c 22 75 73 65 72 49
0c280 64 5c 22 3a 5c 22 31 39 65 33 62 63 34 63 2d 62
0c290 30 65 33 2d 34 37 61 35 2d 62 38 64 35 2d 39 62
0c2a0 63 30 30 65 37 65 66 39 37 61 5c 22 2c 5c 22 64
0c2b0 5c 22 3a 66 61 6c 73 65 7d 2c 5c 22 74 72 61 6e
0c2c0 73 61 63 74 69 6f 6e 5f 64 65 74 61 69 6c 73 5c
0c2d0 22 3a 7b 5c 22 61 6d 6f 75 6e 74 5c 22 3a 7b 5c
0c2e0 22 63 75 72 72 65 6e 63 79 5c 22 3a 5c 22 49 44
0c2f0 52 5c 22 2c 5c 22 76 61 6c 75 65 5c 22 3a 31 30
0c300 30 30 30 7d 2c 5c 22 67 6f 50 61 79 54 68 65 6d
0c310 65 49 64 5c 22 3a 5c 22 54 48 45 4d 45 5f 43 4c
0c320 41 53 53 49 43 5c 22 2c 5c 22 6e 6f 74 65 73 5c
0c330 22 3a 5c 22 74 65 6d 70 61 74 20 64 75 69 74 20
0c340 69 6a 6f 5c 22 2c 5c 22 72 65 66 65 72 65 6e 63
0c350 65 5f 69 64 5c 22 3a 5c 22 30 31 32 30 32 31 31
0c360 31 31 30 30 33 33 38 30 37 78 4d 51 61 74 78 51
0c370 4b 53 59 49 44 5c 22 2c 5c 22 73 74 61 74 75 73
0c380 5c 22 3a 5c 22 73 75 63 63 65 73 73 5c 22 2c 5c
    
```

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 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.

```

068e90 73 61 63 74 69 6f 6e 3f 74 72 61 6e 73 61 63 74
068ea0 69 6f 6e 5f 69 64 3d 33 34 30 39 39 34 35 31
068eb0 31 68 74 74 70 73 3a 2f 2f 77 73 61 2e 77 61 6c
068ec0 6c 65 74 2e 61 69 72 70 61 79 2e 63 6f 2e 69 64
068ed0 2f 77 61 6c 6c 65 74 2f 74 72 61 6e 73 61 63 74
068ee0 69 6f 6e 3f 74 72 61 6e 73 61 63 74 69 6f 6e 5f
068ef0 69 64 3d 33 34 30 39 39 34 35 31 31 3c 62 3e
068f00 66 61 74 6d 61 20 69 72 69 79 61 6e 69 3c 2f 62
068f10 3e 20 6d 65 6e 67 69 72 69 6d 6b 61 6e 20 73 61
068f20 6c 64 6f 20 73 65 62 65 73 61 72 20 3c 62 3e 52
068f30 70 32 30 2e 30 30 30 3c 2f 62 3e 20 6b 65 20 53
068f40 68 6f 70 65 65 50 61 79 2d 6d 75 20 64 65 6e 67
068f50 61 6e 20 6e 6f 2e 20 74 72 61 6e 73 61 6b 73 69
068f60 6c 3c 62 3e 30 33 38 30 31 37 32 38 33 32 39 33
068f70 30 30 38 39 32 30 3c 2f 62 3e 20 43 65 6b 20 64
068f80 69 20 73 69 6e 69 21 58 c5 e8 08 62 63 35 61 36
    
```

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

```

0x00000040: 6D 73 67 22 3A 22 73 75 63 63 65 73 73 22 2C 22 msg: "success",
0x00000050: 74 72 61 6E 73 61 63 74 69 6F 6E 5F 6C 69 73 74 transaction_list
0x00000060: 22 3A 5B 7B 22 74 72 61 6E 73 61 63 74 69 6F 6E [{"transaction
0x00000070: 5F 69 64 22 3A 33 34 30 30 39 39 34 35 31 31 2C _id": "3400994511,
0x00000080: 22 74 72 61 6E 73 61 63 74 69 6F 6E 5F 73 6E 22 "transaction_sn"
0x00000090: 3A 22 30 33 38 30 31 37 32 38 33 32 39 33 30 30 : "03801728329300
0x000000a0: 38 39 32 30 22 2C 22 72 65 66 65 72 65 6E 63 65 8920", "reference
0x000000b0: 5F 69 64 22 3A 22 30 35 38 34 37 38 36 33 31 31 _id": "0584786311
0x000000c0: 34 32 31 33 38 35 38 30 22 2C 22 6D 65 72 63 68 42138580", "merch
0x000000d0: 61 6E 74 5F 69 64 22 3A 31 2C 22 74 72 61 6E 73 ant_id": "1, "trans
0x000000e0: 61 63 74 69 6F 6E 5F 74 79 70 65 22 3A 31 31 2C action_type": "11,
0x000000f0: 22 70 61 72 65 6E 74 5F 69 64 22 3A 33 34 30 30 "parent_id": "3400
0x00000100: 39 39 34 35 30 39 2C 22 73 74 61 74 75 73 22 3A 994509, "status":
0x00000110: 33 2C 22 63 72 65 61 74 65 5F 74 69 6D 65 22 3A 3, "create_time":
0x00000120: 31 36 33 36 35 39 36 33 32 34 2C 22 75 70 64 61 1636596324, "upda
0x00000130: 74 65 5F 74 69 6D 65 22 3A 31 36 33 36 35 39 36 te_time": "1636596
0x00000140: 33 32 34 2C 22 6D 65 74 61 64 61 74 61 22 3A 22 324, "metadata":
0x00000150: 7B 5C 22 63 61 72 64 5F 6F 72 64 65 72 5C 22 3A {"card_order":
0x00000160: 36 2C 5C 22 63 61 72 64 5F 69 6D 61 67 65 5F 75 6, "card_image_u
0x00000170: 72 6C 5C 22 3A 5C 22 68 74 74 70 73 3A 2F 2F 63 rl": "https://c
0x00000180: 66 2E 73 68 6F 70 65 65 2E 63 6F 2E 69 64 2F 66 f.shopee.co.id/f
0x00000190: 69 6C 65 2F 70 71 32 77 6A 68 70 37 33 68 6A 74 ile/pq2vjhp73hjt
0x000001a0: 78 77 77 67 36 69 32 68 33 37 69 79 64 63 6B 76 xwvg6i2h37iydckv
0x000001b0: 31 6A 64 73 2E 6A 70 67 5C 22 2C 5C 22 63 61 72 ljds.jpg", "car
0x000001c0: 64 5F 69 64 5C 22 3A 38 34 2C 5C 22 73 65 6E 64 d_id": "84, "send
0x000001d0: 65 72 5F 75 73 65 72 5F 69 64 5C 22 3A 37 34 30 er_user_id": "740
0x000001e0: 34 30 31 32 2C 5C 22 72 65 63 69 70 69 65 6E 74 4012, "recipient
0x000001f0: 5F 75 73 65 72 5F 69 64 5C 22 3A 35 39 38 37 33 _user_id": "59873
0x00000200: 39 33 2C 5C 22 63 61 74 65 67 6F 72 79 5F 69 64 53, "category_id
0x00000210: 5C 22 3A 36 2C 5C 22 74 72 61 6E 73 66 65 72 5F \": "6, "transfer
0x00000220: 64 65 73 63 72 69 70 74 69 6F 6E 5C 22 3A 5C 22 description": "\
0x00000230: 5C 22 7D 22 2C 22 61 6D 6F 75 6E 74 22 3A 32 30 \": "}, "amount": "20
0x00000240: 30 30 30 30 30 30 30 30 2C 22 66 65 65 22 3A 30 0000000, "fee": "0
0x00000250: 2C 22 75 73 65 72 5F 69 64 22 3A 35 39 38 37 33 , "user_id": "59873
0x00000260: 39 33 2C 22 65 78 74 5F 64 61 74 61 22 3A 7B 22 83, "ext_data": {"
    
```

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	<i>Top up</i>	<i>Top Up</i> Rp.25.000, <i>Transaction ID</i> 2021111010121481030100166312727967228	x	x
		<i>Send Money to Friend</i>	<i>Send Money</i> Rp.10.000 ke Bos Lacoolla xxxxxxxx6656, <i>Transaction ID</i> 20211110121420010100166412727959605, <i>Remarks</i> biru tempat uang	x	x
		<i>Send Money</i>	<i>Receive Money</i> Rp.10.000 from Bos Lacoolla 085156696xxx, <i>Transaction ID</i> 2021111010121420010100166529427788243, <i>Remarks</i> bendera biru	x	x
		<i>Send Money to Bank</i>	<i>Send Money</i> Rp.20.000 to M.NOOR FADILAH Mandiri xxx8216, <i>Transaction ID</i> 202111101021420010100166412727978872, <i>Remarks</i> bendera biru kirim ke livin	x	x
2	Dompet Digital B	<i>Top up</i>	<i>Top up</i> Rp.25.000, <i>Transaction ID</i> 052021111005058SHD1XjtTNpID	✓	✓
		<i>Pay to friends</i>	<i>Sent to</i> Bos Lacoolla xxxxxxxx6656 Rp.10.000, <i>Transaction ID</i> 0120211110033807xMQatxQKSYID, <i>Note:</i> tempat duit ijo	✓	✓

...ke halaman selanjutnya

TabellIV – lanjutan

No	Nama Aplikasi	Jenis Transaksi	Deskripsi Transaksi	Tools Forensik	
				Autopsy	Belkasoft
3	Dompot Digital C	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 0320211110035722IVuh7dKUivID	√	√
	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	
	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 menunjukkan 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].

$$Par = \frac{\sum ar0}{\sum arT} \times 100\% \tag{1}$$

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 Forensic 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* forensik Autopsy berhasil menemukan 8 aktivitas transaksi dengan presentase kemampuan *tools* forensik menemukan data sebesar 47,05%, sedangkan pada *tool* forensik 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.