Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 8, Nomor 1, Februari 2023, pp 1-8
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Forensic Analysis Of Dana Applications Using The ACPO Framework

Ermin[1], Muhammad Rizki Setyawan[2*], Fitriyani Tella[3]
[1,2,3] Universitas Muhammadiyah Sorong, Sorong, Indonesia
Email: ermin@um-sorong.ac.id[1], muhammadrizkisetyawan@gmail.com[2], fitriyanitella@um-sorong.ac.id[3]*

Abstract

The DANA application is a digital wallet platform designed to make all transactions easier, faster and safer, both online and offline. However, apart from the benefits provided, digital wallet applications can also cause harm to their users, namely negative use which can lead to cybercrime cases. Digital forensics is a branch of forensic science that focuses on investigating and finding digital evidence in cybercrime cases. This study aims to conduct a forensic analysis of the DANA application to identify artifacts that have the potential to be used as digital evidence of cybercrime by using the ACPO framework with the assistance of forensic tools such as the Belkasoft Evidence Center and MobilEdit Forensic Express Pro. Based on the research that has been done, it can be concluded that the use of the ACPO Framework to find out the artifacts obtained can be used properly and forensic analysis of the results obtained using two forensic tools, namely the Belkasoft Evidence Center failed to find artifacts that can be used as digital evidence, while the MobilEdit Forensic tool Express Pro only managed to find artifacts in the form of user photos and screenshots of transactions made..

Keywords*: ACPO, Digital Forensics, Digital Wallet, DANA*

Abstrak

Aplikasi DANA adalah platform dompet digital yang dirancang untuk membuat semua transaksi menjadi lebih mudah, cepat, dan aman, baik online maupun offline. Namun selain manfaat yang diberikan, aplikasi dompet digital juga dapat menimbulkan kerugian bagi penggunanya yaitu pemanfaatan secara negatif yang dapat berujung pada kasus kejahatan dunia maya. Forensik digital adalah salah satu cabang ilmu forensik yang berfokus pada penyelidikan dan penemuan bukti digital dalam kasus kejahatan dunia maya. Penelitian ini bertujuan untuk melakukan analisis forensik terhadap aplikasi DANA untuk mengetahui artefak-artefak yang berpotensi untuk dijadikan bukti digital atas tindakan cybercri,me dengan menggunakan framework ACPO dengan bantuan tool forensik berupa Belkasoft Evidence Center, dan MobilEdit Forensic Express Pro. Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa penggunaan ACPO Framework untuk mengetahui artefak yang diperoleh dapat digunakan dengan baik dengan hasil analisis forensik hasil yang diperoleh dengan menggunakan dua tool forensik yaitu Belkasoft Bukti Pusat gagal menemukan artefak yang dapat digunakan sebagai bukti digital, sedangkan tool Forensik MobilEdit Express Pro hanya berhasil menemukan artefak berupa foto pengguna dan tangkapan layar dari transaksi yang dilakukan.

Kata kunci*: ACPO, Digital Forensik, Digital Wallet, DANA*

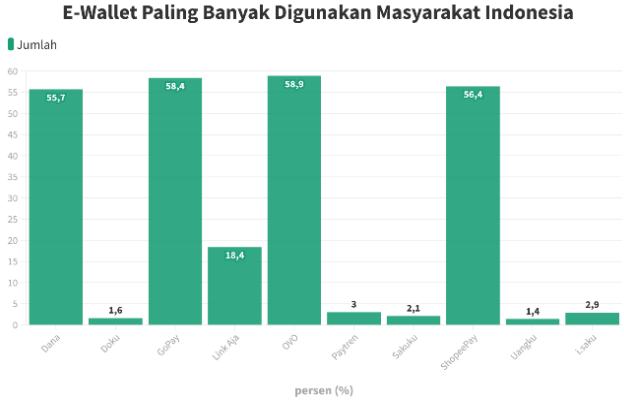
1. PENDAHULUAN

Perkembangan teknologi telah memberikan kita kemudahan dalam melakukan berbagai aktivitas, salah satunya dengan memanfaat aplikasi E-wallet. Dompet digital atau yang lebih dikenal dengan e-wallet merupakan sebuah aplikasi yang dapat digunakan untuk menyimpan uang secara digital dan melakukan transaksi baik online maupun offline[1]. Kemunculan dompet digital ini memiliki banyak manfaat seperti dapat mengurangi resiko penipuan dengan uang palsu dan memiliki pengaruh positif terhadap inflasi [2]. Ada banyak aplikasi dompet digital

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 8, Nomor 1, Februari 2023, pp 1-8
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

yang dapat digunakan saat ini antara lain OVO, DANA, GoPay, ShopeePay dan lainnya[3].

DANA merupakan aplikasi dompet digital yang dirancang untuk membuat semua transaksi lebih mudah, cepat, dan aman, baik online maupun offline. Aplikasi ini dikembangkan oleh Emtek Group dan Alibaba. Di Indonesia, nama resminya adalah PT Espay Debit Indonesia. Aplikasi ini memiliki banyak fitur yang ditawarkan kepada penggunanya seperti DANA wallet, kirim dan minta DANA, DANA Bisnis, DANA Enterprise dan masih banyak lainnya. Menurut survei yang dilakukan oleh DailySocial, aplikasi DANA menempati urutan keempat pada aplikasi dompet digital yang paling banyak digunakan oleh masyarakat Indonesia, mencapai 55,7% pengguna.



Gambar 1. *Statistik Pengguna* E-wallet *(Sumber: DailySocial)*

Namun, selain manfaat yang ditawarkan aplikasi dompet digital, juga dapat menimbulkan kerugian bagi pengguna yaitu pemanfaatan negatif yang dapat berujung pada kasus *cybercrime* [4]. Barang bukti digital dari kasus *cybercrime* bersifat rapuh, rentan akan kerusahan dan mudah hilang sehingga diperlukan metode yang tepat dalam menangani kasus *cybercrime* [5].

Forensik digital merupakan cabang dari ilmu forensik yang berfokus pada penyelidikan dan penemuan barang bukti dalam kasus kejahatan dunia maya [6]. Barang bukti yang ditemukan dapat berupa bukti elektronik yaitu bukti yang bersifat fisik dan dapat kenali secara visual seperti komputer, router, CCTV, flashdisk, dan handphone, dan lainnya. Sedangkan untuk bukti digital adalah bersiftal digital yang yang didapatkan dari hasil proses ekstrak atau recovery dari bukti elektronik seperti file audio, file video, dokumen, user id dan password, dan masih banyak lainnya.

Terdapat dua metode yang umumnya digunakan pada digital forensik yaitu *static* forensik dan *live* forenisk. *Static* forensik merupakan proses forensik yang dilakukan pada sistem yang sedang tidak berjalan atau *not running* dimana data telah dikloning atau membuat *physical image* terlebih dahulu. Sedangkan *live* forensik adalah proses forensik yang dilkaukan pada sistem yang sedang berjalan (*running*) atau teknik untuk menemukan bukti digital pada data volatile [7].

Penelitian dengan topik yang sama dilakukan oleh M.M.J. Sianipar et al [8], di mana peneliti melakukan analisis forensik digital terhadap aplikasi OVO

menggunakan framework NIST SP 800-86. Hasil dari penelitian tersebut adalah metode NIST dapat digunakan sebagai acuan untuk mengalisis bukti digital yang terdapat pada database aplikasi OVO dengan bantuan tools Notepad dan SQL DB Browser. Penelitian selanjutnya dilakukan oleh Rusdi Umar et al [9] yaitu membandingkan dua *tools* forensik yaitu Belkasoft Evidence Center dan Autopsy untuk menemukan barang bukti dari aplikasi *e-wallet* menggunakan kerangka kerja DFRWS. Dari hasil penelitiannya, *tool* forensik Autopsy memiliki tingkat keberhasilan 47,5% dalam memperoleh bukti digital, lebih baik dibandingkan dengan Belkasoft evidence Center yang memiliki tingkat keberhasilan 41,17%.

Penelitian lainnya dilakukan oleh M.N. Fadillah et al [10], bertujuan melakukan proses forensik pada aplikasi dompet digital yang populer di indonesia menggunakan metode DFRWS dan tools forensik berupa Belkasoft Evidence Center dan Autopsy. Hasil yang didapatkan adalah penulis berhasil mendapatkan barang bukti berupa data pengguna dan aktivitas transaksi yang ditersimpan pada perangkat *smartphone* dengan angka indeks keberhasilan yaitu sebesar 100%.

Penelitian lainnya dilakukan oleh Andrew A Uduimoh et al [11], menentukan berapa banyak data pengguna yang dihasilkan dan disimpan oleh aplikasi Mobile Banking setelah registrasi dan melakukan transaksi, dan apakah data tersebut dapat digunakan untuk mengidentifikasi tindakan atau transaksi yang dilakukan oleh pengguna. Hasil penelitian menunjukkan aplikasi mobile banking masih menyimpan data pengguna yang berharga, termasuk kredensial login pengguna dan detail transaksi.

Dari permasalahan di atas, penelitian ini bertujuan untuk mengetahui artefak-artefak dari aplikasi DANA yang berpotensi untuk dijadikan bukti digital.

2. METODOLOGI PENELITIAN

Tahapan penelitian ini dimulai dengan meninjau literatur dari penelitian sebelumnya, kemudian membuat transaksi menggunakan aplikasi DANA, selanjutnya melakukan pemeriksaan dan analisis untuk menemukan artefak yang dapat menjadi potensi barang bukti, dan terakhir memberikan kesimpulan. Tahapan penelitian dapat dilihat pada Gambar 2.

Gambar 2. Tahapan Penelitian

Pada tahapan pemeriksaan dan analisis menggunakan metode static forensik dengan *framework* dari *Association of Chief Police Officers* (ACPO). Penggunaan *framework* dimaksudkan untuk menggambarkan proses forensik yang akan dilakukan dengan lebih jelas dan mudah dipahami [8]. Langah-langkah *framework* ACPO dapat dilihat di Gambar 3.

Gambar 3. Langkah-langkah ACPO

Adapun penjelasan langkah-langkah *framework* dari ACPO adalah sebagai berikut:

a) *Plan*
Tahap ini membuat rencana serta mempersiapkan tool dan software yang akan dipakai dalam penelitian.

b) *Capture*
Tahap ini melakukan akuisisi atau membuat kloning data dari *smartphone* yang digunakan menggunakan *tools* forensik.

c) *Analysis*
Tahap ini menganalisis data yang telah di akuisisi untuk mengetahui artefak apa saja yang bisa di jadikan sebagai barang bukti digital.

d) *Present*
Pada tahap ini membuat laporan serta menampilkan hasil dari analisis yang telah dilakukan secara rinci, jelas dan informatif.

3. HASIL DAN PEMBAHASAN

Penelitian ini menggunakan *framework* dari *Association of Chief Police Officers* yang memiliki empat tahapan yang terdiri dari *Plan, Capture, Analysis, dan Present*.

3.1. Plan

Pada tahap ini mempersiapkan tool dan perangkat lunak yang digunakan. Adapun tool dan perangkat lunak yang dalam penelitian ini seperti yang dipaparkan pada Tabel 1.

Tabel 1. Tool Dan Perangkat Lunak

No.	Name	Keterangan
1.	Laptop Asus VivoBook 14	Sebagai *workstation.*
2.	Redmi S2	Sebagai objek penelitian
3.	Kabel USB	Sebagai konektor dengan laptop
4.	Belkasoft Evidence Center versi 9.9	*Tool* forensik
5.	Mobil Forensic Express Pro versi 7.4.0	*Tool* forensik
6.	Aplikasi DANA versi 2.24.1	Sebagai objek penelitian

Tampilan dan spesifikasi dari *smartphone* yang digunakan dapat dilihat di Gambar 4 dan Tabel 2.

Gambar 4. Redmi S2

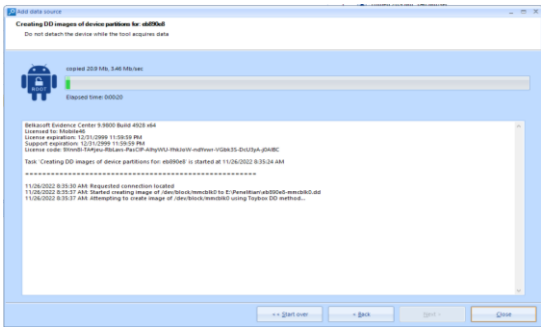
Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 8, Nomor 1, Februari 2023, pp 1-8
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Tabel 2. Spesifikasi Redmi 2

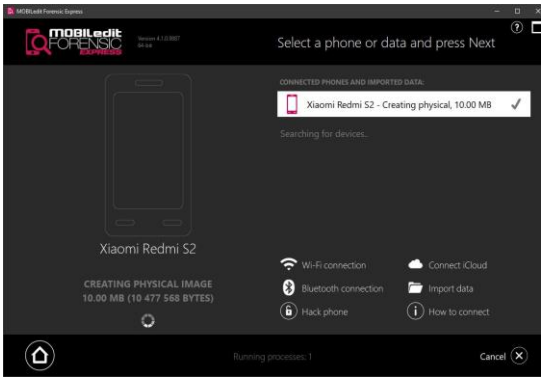
Merek	**Xiaomi**
Model	Redmi S2
MUI	Versi 12.0.0.1
Android	Versi 9 (Pie)
RAM	4 GB
ROM	64 GB
Rooted	Yes

3.2. Capture

Pada tahap ini melakukan akuisisi data dari *smartphone* menggunakan *tools* yang telah disiapkan. Proses ini tidak dilakukan secara langsung pada *smartphone* yang dijadikan barang bukti melainkan membuat *physical image* atau kloning dari *smartphone* Redmi S2 yang digunakan, tujuannya untuk menjaga keaslian data agar barang bukti digital tidak rusah dan terjadi manipulasi data. Gambar 5 dan Gambar 6 merupakan tampilan dari proses akuisisi menggunakan dua *tools* forensik.

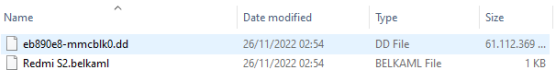


Gambar 5. Proses akuisisi menggunakan tool Belkasoft



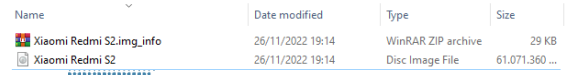
Gambar 6. Proses akuisisi menggunakan tool MobilEdit

Adapun untuk hasil akuisisi yang telah dilakukan menggunakan dua *tools* forensik seperti yang ditampilkan Gambar 7 dan Gambar 8.



Gambar 7. Hasil akuisisi menggunakan *tool* Belkasoft

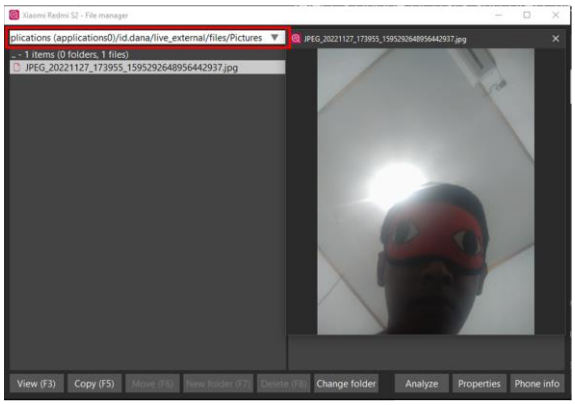
Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 8, Nomor 1, Februari 2023, pp 1-8
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik



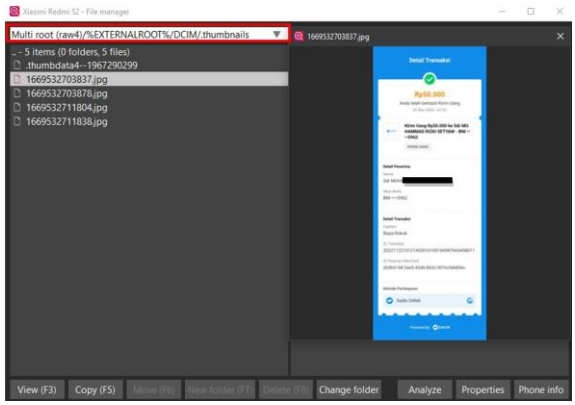
Gambar 8. Hasil akuisisi menggunakan *tool* MobilEdit

3.3. Analysis

Setelah dilakukan akuisisi, tahap selanjutnya melakukan analisis terhadap file *physical image* tersebut. Tujuan analisis yaitu untuk menemukan artefak apa saja yang bisa dijadikan barang bukti dari aplikasi DANA. Hasil dari analisis yang dilakukan menggunakan tool forensik Belkasoft Evidence Center peneliti tidak berhasil menemukan bukti digital apapun. Sedangkan untuk MobilEdit Forensic Express Pro hanya bisa mendapatkan foto pengguna yang tersimpan pada folder **application/id.dana/live_external/files/pictures** dan *screenshoot* transaksi yang disimpan untuk yang tersimpan pada folder **Multi Root/%ExternalRoot%/DCIM/.thumbnails** seperti yang dipaparkan di Gambar 9 dan Gambar 10.



Gambar 9. Foto Profil



Gambar 10. *Screenshoot* transaksi yang disimpan

Kemudian untuk informasi akun, saldo, riwayat transaksi seperti Top Up, Kirim DANA ke Teman ataupun ke Bank, dan nomor rekening tidak berhasil ditemukan.

3.4. Present

Pada bagian ini merupakan pembuatan dan menampilkan hasil analisis dan menjelaskan artefak apa saja yang diperoleh dari kegiatan forensik yang telah dilakukan. Tabel 3 merupakan ringkasan laporan yang telah dibuat.

Tabel 3. Ringkasan Laporan *Tools Forensic*

Artefak	*Tools* Forensik	
	Belkasoft Evidence Center	**MobilEdit Forensic Express Pro**
Informasi Akun	-	-
Informasi Saldo	-	-
Foto Profil	-	✓
Screenshoot Transaksi	-	✓
Riwayat Transaksi	-	-

Berdasarkan Tabel 3 dapat dilihat bahwa *tool* Belkasoft tidak berhasil menemukan artefak yang berpotensi menjadi bukti digital, sedangkan *tool* MobilEdit Forensic Express Pro hanya berhasil menemukan foto profil dan *screenshoot* transaksi yang dapat sebagai barang bukti digital.

4. SIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa penggunaan *Framework* ACPO untuk mengetahui artefak yang diperoleh dapat digunakan dengan baik dengan hasil hasil analisis forensik yang diperoleh dengan menggunakan dua *tools* forensik yaitu Belkasoft Evidence Cneter gagal menemukan artefak yang dapat digunakan sebagai bukti digital, sedangkan *tool* forensik MobilEdit Express Pro hanya berhasil menemukan artefak berupa foto pengguna dan *screenshoot* dari transaksi yang telah dilakukan.

DAFTAR PUSTAKA

[1] H. H. Nawawi, "Penggunaan E-wallet di Kalangan Mahasiswa," *Emik*, vol. 3, no. 2, pp. 189–205, 2020, doi: 10.46918/emik.v3i2.697.

[2] E. Zunaitin, R. Niken W, and F. Wahyu P, "Pengaruh E-money terhadap Inflasi di Indonesia," *J. Ekuilibrium*, vol. 2, no. 1, pp. 18–23, 2017, [Online]. Available: https://jurnal.unej.ac.id/index.php/JEK/article/download/13920/7264

[3] M. N. Fadillah, R. Umar, and A. Yudhana, "Rancangan Metode Nist Untuk Forensik Aplikasi Mobile Payment Berbasis Android," *Semin. Nas. Inform. 2018 (semnasIF 2018)*, vol. 2018, no. November, pp. 115–119, 2018, [Online]. Available: http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/2626

[4] Anton Yudhana, Abdul Fadlil, and M. R. Setyawan, "Analysis of Skype Digital Evidence Recovery based on Android Smartphones Using the NIST Framework," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 682–690, 2020, doi: 10.29207/resti.v4i4.2093.

[5] M. R. Setyawan, A. Yudhana, and A. Fadlil, "Akuisisi Data Pada Skype Messenger Menggunakan Metode National Institute Of Justice," *Syst. Inf. Syst. Informatics Journal.*, vol. 5, no. 2, pp. 13–18, 2019, doi: 10.29080/systemic.v5i2.724.

[6] M. R. Setyawan, A. Yudhana, and A. Fadlil, "Identifikasi Bukti Digital Skype Di

Smartphone Android Dengan Metode National Institute Of Justice (NIJ)," in *Seminar Nasional Teknologi Fakultas Teknik Universitas Krisnadwipayana (semnastek)*, 2019, pp. 565–570.

[7] M. Rizki Setyawan, H. Hermansa, and M. Fadli Hasa, "Analisis Forensik Digital Pada Skype Berbasis Windows 10 Menggunakan Framework ACPO," *J. Ilm. Betrik*, vol. 13, no. 2, pp. 111–119, 2022, doi: 10.36050/betrik.v13i2.469.

[8] M. M. J. Sianipar, S. Juli, I. Ismail, and G. B. Satrya, "Analisis Digital Forensik Aplikasi OVO Pada Android," *e-Proceeding Appl. Sci.*, vol. 7, no. 6, pp. 2745–2749, 2021.

[9] R. Umar, A. Yudhana, and M. N. Fadillah, "Perbandingan Tools Forensik Pada Aplikasi Dompet Digital," *JIKO (Jurnal Inform. dan Komputer)*, vol. 6, no. 2, p. 242, 2022, doi: 10.26798/jiko.v6i2.621.

[10] M. N. Fadillah, U. Rusydi, and A. Yudhana, "Analisis Forensik Aplikasi Dompet Digital Pada Smartphone Android Menggunakan Metode DFRWS," *Kumpul. J. Ilmu Komput.*, vol. 09, no. 02, pp. 265–278, 2022.

[11] Andrew A. Uduimoh, Oluwafemi Osho, Idris Ismaila, and Shafi'i M. Abdulhamid, "Forensic Analysis of Mobile Banking Applications in Nigeria," *i-manager's J. Mob. Appl. Technol.*, vol. 6, no. 1, p. 9, 2019, doi: 10.26634/jmt.6.1.15704.