Analisis Artefak Digital Aplikasi Dompet *Cryptocurrency* *Tokocrypto* pada *Android*

Muhammad Nur Adhar

20917025

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2023

Lembar Pengesahan Pembimbing

Analisis Artefak Digital Aplikasi Dompet *Cryptocurrency* Tokocrypto pada *Android*

Muhammad Nur Adhar

20917025

Yogyakarta, September 2023

Pembimbing I	Pembimbing II
Dr. Yudi Prayudi,S.Si., M.Kom.	Erika Ramadhani, ST., M.Eng.

Lembar Pengesahan Penguji

Analisis Artefak Digital Aplikasi Dompet *Cryptocurrency* Tokocrypto pada *Android*

Muhammad Nur Adhar

20917025

Yogyakarta, September 2023

Tim Penguji,

Dr. Yudi Prayudi,S.Si., M.Kom.
Ketua

Dr. Ahmad Luthfi, S.Kom., M.Kom.
Anggota I

Irving Vitra Paputungan, S.T., M.Sc., Ph.D
Anggota II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Universitas Islam Indonesia

Irving Vitra Paputungan, S.T., M.Sc., Ph.D

Abstrak

Analisis Artefak Digital Aplikasi Dompet *Cryptocurrency* Tokocrypto pada *Android*

Dompet *cryptocurrency* merupakan aplikasi yang memungkinkan pengguna *cryptocurrency* untuk menyimpan, penarikan dan transfer berbagai aset digital mata uang *cryptocurrency*. Kasus kejahatan yang dilakukan menggunakan dompet *cryptocurrency* sebagai wadah memainkan peran dalam tantangan untuk membuktikan dan menganalisis artefak atau objek digital yang disimpan di *smartphone*. Oleh karena itu, penelitian ini akan melakukan investigasi forensik terhadap salah satu aplikasi dompet *cryptocurrency* yang legal di negara Indonesia yaitu aplikasi dompet *cryptocurrency* tokocrypto. Penelitian ini berfokus pada penemuan artefak digital dompet *cryptocurrency* tokocrypto dari perangkat *smartphone* berdasarkan fakta dan informasi yang diperoleh dari petunjuk *smartphone*. Untuk menemukan bukti digital dari aplikasi dompet *cryptocurrency* pada *smartphone* menggunakan metode DFRWS dimana metode ini memiliki 6 tahapan yaitu *identification, preservation, collection, examination, analysis* dan *presentation* serta tool forensik yaitu *oxygen forensics* untuk melakukan akuisisi dan anlisis. Berdasarkan hasil penelitian, Penelitian ini bertujuan untuk melakukan analisis artefak dompet digital *cryptocurrency* Tokocrypto pada smartphone Xiaomi Redmi 6A. Hasil analisis menunjukkan bahwa dari sepuluh aktivitas transaksi yang diamati, informasi mengenai tujuh transaksi telah berhasil ditemukan, termasuk deposit fiat, penarikan fiat, penarikan crypto, dan penjualan crypto. Namun, beberapa label transaksi seperti jenis transaksi, Id Pemesanan, Txid, dan alamat dompet tidak tersedia pada beberapa transaksi. Kekurangan label-label ini mengurangi detail dan kelengkapan informasi, menyulitkan pemahaman yang komprehensif tentang aktivitas transaksi.Penelitian ini juga menyoroti pentingnya pendekatan ilmiah dalam analisis forensik digital untuk mengatasi tantangan semacam ini. Ketiadaan label-label transaksi menggarisbawahi perlunya akses ke data yang lebih kaya, termasuk label-label yang relevan, guna memperoleh pemahaman yang lebih lengkap dan akurat. Selain itu, pendekatan lintas disiplin yang mencakup penggunaan bukti metadata tambahan dari sumber eksternal dapat membantu mengisi celah informasi dan memahami transaksi yang kurang lengkap. Hasil penelitian ini memberikan pandangan awal tentang aktivitas transaksi dalam dompet digital Tokocrypto, tetapi juga menekankan perlunya peningkatan dalam metode analisis forensik digital untuk menghadapi tantangan semacam ini dalam masa depan.

Kata kunci

dompet cryptocurrency, mobile forensics, tokocrypto, andorid, dfrws

Abstract

Digital Artifact Analysis of the Tokocrypto Cryptocurrency Wallet Application on Android

Cryptocurrency wallets are applications that enable cryptocurrency users to store, withdraw, and transfer various digital assets of cryptocurrency. Criminal activities involving cryptocurrency wallets as a container play a role in the challenge of proving and analyzing artifacts or digital objects stored on smartphones. Therefore, this research will conduct forensic investigation on one of the legal cryptocurrency wallet applications in Indonesia, namely the Tokocrypto cryptocurrency wallet application. This study focuses on discovering digital artifacts of the Tokocrypto cryptocurrency wallet from smartphone devices based on facts and information obtained from smartphone clues. To find digital evidence from cryptocurrency wallet applications on smartphones, the DFRWS method is used, which consists of six stages: identification, preservation, collection, examination, analysis, and presentation, along with the forensic tool Oxygen Forensics for acquisition and analysis. Based on the research results, this study aims to analyze the artifacts of the Tokocrypto digital cryptocurrency wallet on Xiaomi Redmi 6A smartphones. The analysis results show that out of ten observed transaction activities, information about seven transactions has been successfully identified, including fiat deposits, fiat withdrawals, crypto withdrawals, and crypto sales. However, some transaction labels such as transaction type, Order ID, Txid, and wallet address are not available for certain transactions. The absence of these labels reduces the level of detail and completeness of information, making it challenging to achieve a comprehensive understanding of transaction activities. This research also highlights the importance of a scientific approach in digital forensic analysis to address such challenges. The absence of transaction labels underscores the need for access to richer data, including relevant transaction labels, to obtain a more comprehensive and accurate understanding. Additionally, a multidisciplinary approach that involves the use of additional metadata evidence from external sources can help fill information gaps and understand incomplete transactions. The research results provide initial insights into transaction activities within the Tokocrypto digital wallet but also emphasize the need for improvements in digital forensic analysis methods to address such challenges in the future.

Keywords

cryptocurrency wallet, mobile forensics, tokocrypto, andorid, dfrws

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, 21 September 2023

Muhammad Nur Adhar, S.Kom

Daftar Publikasi

Sitasi publikasi 4

Kontributor	Jenis Kontribusi
Muhammad Nur Adhar	Mendesain eksperimen (60%) Menulis *paper* (70%)
Dr. Yudi Prayudi, S.Si., M.Kom Erika Ramadhani, ST., M.Eng	Mendesain eksperimen (40%) Menulis dan mengedit *paper* (30%)

Halaman Kontribusi

"**Tidak ada kontribusi dari pihak lain**".}

Halaman Persembahan

Alhamdulillah segala puji bagi Allah yang telah memberikan kita semua nikmat dan dengan rahmat dan karunia dari Allah penulis bisa menyelesaikan pendidikan Program Studi Informatika Program Magister di Universitas Islam Indonesia Yogyakarta. Penulis persembahkan penelitian ini kepada kedua orang tua, kakak, adik dan keluarga besar serta calon istri yang telah memberikan do'a, dukungan dan semangat kepada penulis yang tiada hentinya.

Kata Pengantar

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Syukur Alhamdulillah penulis ucapkan atas rahmat dan nikmat Allah sehingga studi Program Magister Informatika ini bisa diselesaikan dengan baik. Shalawat serta salam penulis ucapkan kepada baginda Nabi Muhammad Shallallahu'alaihi wa sallam. Semoga kita semua mendapat syafa'at beliau di hari akhir kelak Aamiin ya rabbal alamin. Penulis juga bersyukur atas selesainya pengerjaan tesis dengan judul "Analisis Artefak Digital Aplikasi Dompet *Cryptocurrency* Tokocrypto pada Android".

Dalam penyususan laporan tesis ini tidak lepas dari bimbingan, dukungan dan bantuan dari berbagai pihak. Oleh karena itu dalam kesempatan ini, dengan kerendahan hati ucapan terima kasih disampaikan dengan setulus-tulusnya kepada:

1. Allah Subhana Wa Ta'ala, yang telah melimpahkan Rahmat dan Karunia-Nya sehingga penulis diberikan kesehatan, kekuatan untunk dapat menyelesaikan laporan tesis ini.
2. Kedua orang tua, kakak, adik dan keluarga besar serta istri yang telah memberikan do'a, dukungan dan semangat kepada penulis yang tiada hentinya.
3. Bapak Rektor dan seluruh jajaran Universitas Islam Indonesia.
4. Dr. Yudi Prayudi, S.Si., M.Kom dan Erika Ramadhani, ST., M.Eng, selaku pembimbing penulisan tesis yang telah memberikan saran, semangat, dan mendorong penulis untuk terus bisa berkembang.
5. Bapak dan Ibu dewan penguji sidang proposal, progres dan pendadaran tesis. Serta Dosen Magister Informatika Universitas Islam Indonesia serta jajaran staf Program Pascasarjana.
6. Seluruh sahabat, teman dan rekan seperjuangan yang selalu bersama-sama dalam menyelesaikan studi jurusan Informatika Program Magister ini.

Penulis berharap semoga Allah membalas semua kebaikan dan kerjasama Bapak/Ibu dan teman-teman. Selanjutnya, penulis juga berharap saran dan kritik dari pembaca tesis ini untuk kesempurnaan penulisan kedepannya.

Yogyakarta, September 2023

Muhammad Nur Adhar

Daftar Isi

Daftar Tabel

Daftar Gambar

Glosarium

UFED - Universal Forensic Extraction Device

BAB 1
Pendahuluan

1.1 Latar Belakang

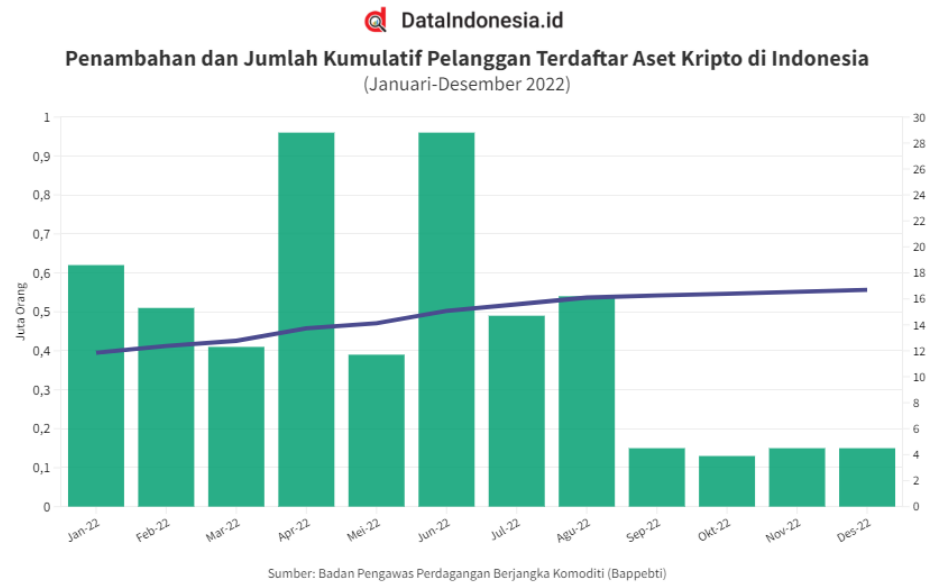
Perkembangan teknologi dari waktu ke waktu sangat pesat, salah satunya perkembangan *smartphone* yang selalu mengalami perkembangan dari segi sistem operasi, fitur, spesifikasi, dan aplikasi. Teknologi yang semakin canggih menjadi bagian yang tidak bisa lepas dari kehidupan masyarakat, tidak hanya melakukan kegiatan-kegiatan positif namun kegiatan-kegiatan negatif. Hal ini dapat dilihat dari banyaknya kejahatan yang dilakukan dengan memanfaatkan teknologi.

Dalam tahun ini dan beberapa tahun terakhir, perdagangan *cryptocurrency* telah meningkat secara signifikan, dan tren ini telah menarik perhatian dunia maya. Mata uang digital ini merupakan hasil dari suatu teknologi melalui sistem kriptografi bertujuan untuk mengamankan, mengatur otoritas tetapi menggunakan sistem terdesentralisasi untuk mencatat transaksi dan mengelola penerbitan unit baru serta memberikan jaminan keamanan dengan tidak bisa gandakan atau ditiru. Kriptografi merupakan salah satu teknik untuk memungkinkan transmisi informasi yang aman (Maha Rani et al., 2021).

Menurut situs Bankrate pada *glossary* mendefinisikan Dompet *cryptocurrency* merupakan aplikasi yang memungkinkan pengguna *cryptocurrency* untuk menyimpan, penarikan dan transfer aset digitat. *Cryptocurrency*, seperti bitcoin, menjadi semakin meningkat serta sangat populer. Bitcoin dapat digunakan secara relatif secara anonim dan itu bisa menantang, atau terkadang tidak mungkin, untuk ditentukan identitas asli pemilik alamat bitcoin. Transaksi Bitcoin relatif lebih murah dan lebih cepat daripada transaksi perbankan biasa. Oleh karena itu, tidak mengherankan bahwa bitcoin juga telah digunakan oleh penjahat dalam kegiatan secara ilegal misalnya membayar obat-obatan terlarang (Zollner et al., 2019), pencucian uang (Maha Rani et al., 2021), pendanaan terorisme (Prasetya et al., 2021), menerima pembayaran dalam kasus pemerasan online dan insiden ransomware yang digunakan dalam pasar darknet (Van Der Horst et al., 2017). Sebab tindakan ini bertujuan untuk menyamarkan transaksi keuangan serta beragam informasi dari transaksi dengan mata uang virtual yaitu *cryptocurrency*, yang merupakan mata uang tanpa bentuk fisik yang dibentuk dari sebuah teknik kriptografi.

Menurut (Chainalysis, 2022) menjelaskan bahwa tindakan pidana pencucian uang *cryptocurrency* mencapai 123 triliun rupiah atau 8,6 miliar dolar amerika pada tahun 2020. Jumlah aset digital ini dihasilkan dari melakukan peretasan atau tindak pidana lainnya, angka kenaikannya mencapai 30 persen dibandingkan pada sebelumya yaitu tahun 2019. Secara umum, tindakan pencucian uang menggunakan aset digital *cryptocurrency* lebih dari 33 miliar dolar amerika atau 473 triliun rupiah dimulai pada tahun 2017. Menurut Chainalysis, pelaku menargetkan pasar bursa terpusat. Sekitar 17 persen dari 8,6 miliar dolar amerika aset digital *cryptocurrency* yang masuk kategori tindak pidana pencucian uang (TPPU) pada tahun 2019, dijalankan di *software* keuangan terdesentralisasi. Naiknya angka dari hanya 2 persen pada 2020. *Chainalysis* menyebut, pencucian uang menggunakan *cryptocurrency* merupakan proses menyamarkan asal usul uang yang diperoleh secara ilegal. Kemudian, pelaku mentransfernya ke bisnis yang sah. Perusahaan mencatat, 8,6 miliar dolar amerika nilai pencucian uang tahun 2020 merupakan dana yang berasal dari kejahatan *cryptocurrency*. Dana tersebut berasal dari penjualan data yang dicuri *darknet* maupun serangan *ransomware*.

Berdasarkan data dari Badan Pengawas Perdagangan Berjangka Komoditi Republik Indonesia tercatat kenaikan pemodal di semua pedagang aset kripto mencapai 4,2 juta akun per akhir Februari, dibanding setahun sebelumnya yang hanya sekitar 2 juta akun, kenaikan ini merupakan dua kali lipat lebih. Jumlah pemodal aset kripto ini bahkan hampir menyamai total investor di pasar modal yang mencapai 4,5 juta yang hampir setara jumlah investor di pasar modal (saham, obligasi, reksa dana, dan produk lainnya) (Badan Pengawas Perdagangan Berjangka Komoditi, 2021). Jumlah investor kripto di Indonesia bertambah 5,46 juta orang sepanjang tahun 2022. Dengan menambahnya investor kripto, maka terdaftar mencapai 16,55 juta orang hingga akhir Desember 2022 (Bappebti, 2023). Jumlah ini jauh lebih banyak dibandingkan total investor pasar modal yang sebanyak 10,31 juta orang.



Gambar 1.1 Penambahan dan Jumlah Kumulatif Pengguna Aset Kripto di Indonesia

Sekarang Badan Pengawas Perdagangan Berjangka Komoditi Republik Indonesia hanya mengizinkan 229 jenis mata uang kripto untuk diperdagangkan di Indonesia yang di antaranya adalah Bitcoin, Polkadot, Tether, Ethereum dan Litecoin. Hingga tahun 2021, terdapat 13 perusahaan yang sudah memperoleh tanda daftar dari Badan Pengawas Perdagangan Berjangka Komoditi Republik Indonesia sebagai perdagangan fisik aset kripto antara lain PT Crypto Indonesia Berkat (Tokocrypto), PT Zipmex Exchange Indonesia (Zipmex), PT Rekeningku Dotcom Indonesia (Rekeningku.com), PT Indodax Nasional Indonesia (Indodax), PT Pintu Kemana Saja (Pintu), PT Luno Indonesia LTD (Luno), PT Cipta Koin Digital (Koinku), PT Tiga Inti Utama (Triv), PT Indonesia Digital Exchange (Idex), PT Upbit Exchange Indonesia (Upbit), PT Triniti Investama Berkat (Bitocto), PT Plutonext Digital Aset (Plutonext) dan PT Bursa Cripto Prima (Kementerian Perdagangan, 2021).

PT Crypto Indonesia Berkat (Tokocrypto) adalah sebuah startup yeng bergerak di bidang *marketplace* menyediakan layanan untuk masyarakat agar dapat melakukan penyimpanan atau transaksi jual/beli aset *cryptocurrency* (Ladita, 2020). Tokocrypto mencatat 2 juta lebih pengguna terdaftar pada 2021. Mayoritas pengguna berusia 18-34 tahun dengan presentase 66% (Dinas Penanaman Modal Dan Perizinan Terpadu Satu Pintu Provinsi Banten, 2022).

Penelitian sebelumnya melakukan pemeriksaan terhadap aplikasi dompet *cryptocurrency Bitcoin, Litecoin*, dan *Darkcoin* di perangkat seluler untuk mendapatkan artefak digital yang menggunakan *UFED* untuk alat ekstraksi, data yang dihasilkan dari

dompet diekstraksi dari *Android* dan perangkat *iOS* berhasil mendapatkan informasi transaksi dan menunjukan keberadaan dompet *cryptocurrency* pada perangkat *smartphone*. Pengujian pada perangkat Android yang menjalankan versi OS Android yang lebih baru dari 4.4.2. Banyak penelitian yang telah dilakukan, tetapi penyelidikan terhadap dompet *cryptocurrency* masih kurang. Maka diperlukan lebih banyak percobaan dan analisis harus dilakukan untuk pemeriksa forensik secara efektif menanggapi kasus *cybercrime* pada mata uang *cryptocurrency* yang berkembang pesat (Montanez, 2014).

Kasus kejahatan dunia maya yang terjadi pada dompet *cryptocurrency* yang terpasang pada perangkat *smartphone,* untuk mendapatkan informasi yang terletak pada perangkat *smartphone* diperlukan proses forensik yaitu tahap akusisi *storage smartphone* untuk memperoleh bukti digital (Yudhana et al., 2018). Dilakukannya proses forensik pada barang bukti perangkat *smartphone* agar mempeloreh artefak digital terkait aktivitas yang diduga sebagai bagian dari kejahatan dunia maya dan dijadikan sebagai bukti digital (Umar et al., 2018). Keadaan perangkat *smartphone* sangat mempengaruhi bukti digital yang diperoleh pada kondisi *rooted,* lebih handal dalam mempeloreh bukti digital dibandingkan kondisi tanpa *root* dan alat forensik yang digunakan akan berdampak pada saat dilakukan analisis (Riadi et al., 2018). Proses forensik menggunakan tahapan metode forensik *DFRWS* (*Digital Forensic Research Workshop*) yaitu tahapan investigasi forensik meliputi *identification, preservation, collection, examination, analysis* dan *presentation* (Fadillah et al., 2022). Oleh karena itu, penelitian ini akan melakukan investigasi forensik terhadap salah satu aplikasi dompet *cryptocurrency* yang legal di negara Indonesia yaitu aplikasi dompet *cryptocurrency* tokocrypto. Tujuan dari penelitian ini untuk memberikan gambaran karakteristik artefak digital pada aplikasi dompet *cryptocurrency* tokocrypto yang menggunakan perangkat *smartphone* versi *android* yang lebih baru dari versi 4.4.2.

1.2 Rumusan Masalah

Merujuk dari latar belakang di atas maka dalam penelitian merumuskan bagaimana artefak digital dari Aplikasi Dompet *Cryptocurrency* pada *Android*?

1.3 Batasan Masalah

Dalam melaksanakan kegiatan penelitian ini, supaya penelitian akan lebih spesifik dan maksimal maka dibuat batasan masalah. Berikut batasan masalah yang terdapat pada penelitian ini menggunakan Sistem Operasi *Android*

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang dibuat di atas maka tujuan dari penelitian ini mengetahui Artefak digital dari Aplikasi Dompet *Cryptocurrency* Tokocrypto pada *Android*

1.5 Manfaat Penelitian

Manfaat yang didapatkan dalam penelitian ini adalah:

1. Pengetahuan tentang proses investigasi forensik pada aplikasi dompet *cryptocurrency* Tokocrypto pada *Andorid*
2. Sebagai referensi bagi peneliti lain yang mengambil kajian terkait dengan bidang Forensik Aplikasi Dompet *Cryptocurrency* Tokocrypto pada *Android*, atau digunakan untuk memperkaya wawasan untuk pengembangan penelitian selanjutnya

1.6 Sistematika Penulisan

Dalam penyusuan penulisan ini untuk memberikan gambaran terkait dengan penjelasan maka digunakan sebuah sistematika penulisan sebagai berikut:

BAB 1 PENDAHULUAN

Pada Bab ini menjelaskan Pendahuluan yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian dan manfaat penelitian.

BAB II LANDASAN TEORI

Pada Bab ini menjelaskan teori-teori yang terkait yang berhubungan dengan *cryptocurrency*, dompet *cryptocurrency, android,* dan tools forensik yang digunakan.

BAB III METODOLOGI PENELITIAN

Pada Bab ini membahas tentang tahapan penelitian, dari persiapan sistem, simulasi kasus, investigasi, analisis dan laporan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi pembahasan penyelesaian masalah dengan menggunakan metode investigasi forensik dan analisis pengujian yang dilakukan.

BAB V KESIMPULAN DAN SARAN

Kesimpulan dan saran, berisi kesimpulan dari penelitian dan saran yang memerhatikan keterbatasan temuan dalam penelitian dan rekomendasi untuk penelitian selanjutnya.

BAB 2
Tinjauan Pustaka

2.1 Pendahuluan

Pada penelitian ini difokuskan pada analisis artefak digital pada aplikasi dompet *Cryptocurrency* pada *Android*. Pada penelitian sebelumnya (Zollner et al., 2019) melakukan penlitian analisis *cryptowallets* yang diinstal pada sistem windows. Pada penelitian ini menjelaskan cara mengumpulkan data yang diperoleh dari RAM dan Hardisk. Kemudian melakukan analisis untuk mendapatkan catatan transaksi dan mengonfirmasi *cryptowallets.*

Dalam penelitian (Van Der Horst et al., 2017) menjelaskan forensik analisis dilakukan dalam *cryptowallets* yang ditargetkan adalah *Bitcoin Core* dan *Electrum*. Data yang dapat diekstraksi seperti *public keys*, alamat, label, dan catatan transaksi.

Pada penelitian (Montanez, 2014) melakukan pemeriksaan terhadap aplikasi dompet paling populer untuk *cryptocurrency Bitcoin, Litecoin*, dan *Darkcoin* di perangkat seluler untuk mendapatkan artefak digital yang menggunakan *Universal Forensic Extraction Device (UFED)* untuk alat ekstraksi, data yang dihasilkan dari dompet diekstraksi dari *Android* dan perangkat *iOS*, kemudian diuraikan dan dianalisis untuk data yang berpotensi menautkan dompet *cryptocurrency* yang masih di install atau dihapus. Penganalisis Fisik berhasil mengumpulkan data yang menunjukkan adanya aplikasi dompet *cryptocurrency* di perangkat *iOS* dan *Android*, tetapi dompet yang sudah dihapus yang bisa dilakukan ekstraksi hanya untuk perangkat *Android*. Khusus untuk *iOS*, alat *iFunBox* hanya berguna untuk konfirmasi keberadaan aplikasi dompet aktif di perangkat *iOS*. Khusus untuk perangkat *Android*, berhasil mengekstrak banyak informasi transaksi yang berharga untuk aktif aplikasi dompet *cryptocurrency*. Selain data transaksi, mampu mengekstraksi informasi yang menunjukkan keberadaan dompet saat ini dan yang sudah dihapus pada perangkat ponsel, tetapi hanya jika dompet telah dinstal melalui file APK yang diunduh.

Dalam penelitian (Volety et al., 2019) dijelaskan telah melakukan analisis pada dua *cryptowallets* yaitu *Multibit HD* dan *Electrum* yang diinstal di Komputer untuk menemukan kerentanan. Penelitian ini berfokus pada keamanan yang mengamati pentingnya jika *cryptowalllets* dipulihkan dan akses diperoleh, tidak ada jaminan bahwa *cryptocurrency* masih tersimpan dengan aman didompet. Karena dompet dapat diakses dari perangkat lain, jika tersangka memiliki *private key* dan pemulihan frasa.

Pada penelitian (Koerhuis et al., 2020) dijelaskan telah melakukan analisis pada dua *cryptowallets* yaitu *monero* dan *verge* yang diinstal di sistem operasi kali linux. Pada penelitian ini menjelaskan cara mengumpulkan data yang diperoleh dari RAM dan Hardisk. Data yang dapat diekstraksi seperti pemulihan frasa, *public keys*, ID transaksi, direktori *wallet*, dan *private keys* terenskripsi yang dapat di ekstraksi. Para peneliti menyimpulkan bahwa *cryptowallets* dapat dipulihkan dan *cryptocurrency* dapat diperoleh.

Dalam penelitian (Lero et al., 2019) melakukan penelitian mengenai analisis privasi dan keamanan *cryptocurrency* aplikasi seluler. Dalam penelitian ini, melakukan pemeriksaan terhadap profil keamanan umum menggunakan aplikasi *cryptocurrency Android*. Pemeriksaan aplikasi ini untuk kerentanan umum yang digunakan oleh *OWASP* dengan menggunakan 10 besar aplikasi dompet *cryptocurrency*. Menetapkan dasar untuk pengujian dengan mengevaluasi aplikasi perbankan dan perdagangan yang umum digunakan. Melakukan perbandingan hasil dari pengujian dasar dan menetapkan status keamanan yang disediakan oleh aplikasi dompet *cryptocurrency*. Hasil temuan kemungkinan implikasi privasi dari aplikasi seluler. Serta aplikasi layanan keuangan konvensional hanya sedikit lebih baik daripada aplikasi *cryptocurrency* dalam hal keamanan tetapi memberikan privasi yang lebih besar.

Sementara itu, dalam penelitian (Yazdinejad et al., 2020) dalam penelitian ini, menggunakan sebuah Jaringan *Recurrent Neural Network* (RNN) untuk malacak ancaman malware *cryptocurrency*. Tujuan menggunakan RNN untuk menganalisis kode operasi aplikasi Windows (*Opcodes*) sebagai studi kasus. Sampel yang digunakan masing-masing berupa dataset yang terdiri dari 500 *malware cryptocurrency* dan 200 virus jinak (*benign-ware*). Model yang diusulkan dengan lima *Long Short-Term Memory* (LSTM) yang berbeda struktur dan dievaluasi dengan teknik 10-*fold teknik cross-validation* (CV). Hasil yang didapat membuktikan bahwa model konfigurasi 3-lapisan memperoleh 98 persen akurasi deteksi, yang merupakan tingkat tertinggi di antara konfigurasi saat ini dengan yang lainnya. Serta menerapkan pengklasifikasi pembelajaran mesin tradisional untuk menunjukkan penerapan LSTM dengan model tradisional dalam menangani *malware cryptocurrency.*

Tabel 2.1 Lireratur Review

No	Literatur	Tujuan	Metode	Hasil
1	(Zollner et al., 2019)	Mengusulkan cara mengumpulkan data	*Live forensics*	Hasilnya informasi dapat ditemukan dalam artefak

		yang diperoleh dari RAM dan Hardisk pada sistem operasi windows kemudian melakukan analisis untuk mendapatkan catatan transaksi dan mengonfirmasi *cryptowallets.*		browser kecuali untuk brower menggunakan mode privat hanya sebagiannya.
2	(Van Der Horst et al., 2017)	Mengusulkan cara mengidentifikasi sumber potensial dan jenis data potensial yang relevan (misalnya kunci Bitcoin, data transaksi, dan frasa sandi).	Procces Memory	Hasilnya dapat ditemukan berbagai artefak digital yang didapatkan dalam procces memory
3	(Montanez, 2014)	Mengusulkan cara mengestraksi dompet *cryptocurrency* dengan alat UFED pada perangkat *smartphone* yang aktif dan dihapuss	*Live Forensics*	Hasil ekstraksi UFED didapatkan pada perangkat andorid dan iOS dompet *cryptocurrency* yang masih aktif sedangkan dompet *cryptocurrency* yang sudah dihapus hanya didapatkan pada perangkat *android*
4	(Volety et al., 2019)	Mengusulkan untuk meningkatkan keamanan setiap dompet harus menggunakan kombinasi kata sandi dan dompet pemulihan.	*Brute-force password*	Hasilnya kata sandi dompet *cryptocurrency* memungkinkan dapat dipulihkan
5	(Koerhuis et al., 2020)	Mengusulkan cara mengumpulkan data	*Live Forensics*	Hasilnya bahwa *cryptowallets* dapat

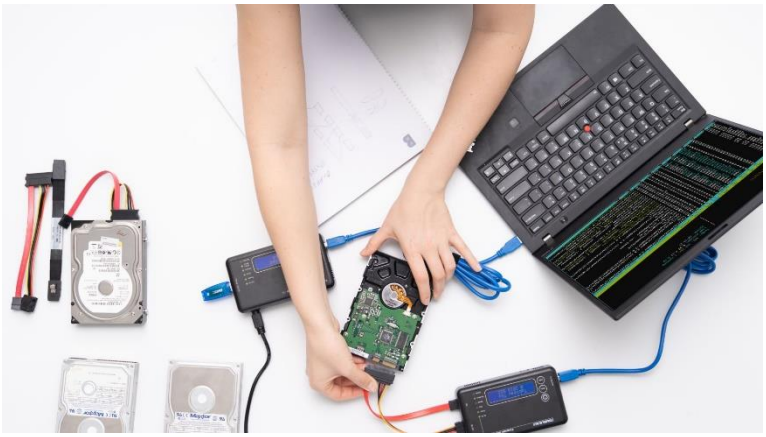
		yang diperoleh dari RAM dan Hardisk pada sistem operasi linux		dipulihkan dan *cryptocurrency* dapat diperoleh
6	(Lero et al., 2019)	Mengusulkan untuk pengujian dengan mengevaluasi aplikasi perbankan dan perdagangan yang umum digunakan. Serta melakukan perbandingan hasil dari pengujian dasar dan menetapkan status keamanan yang disediakan oleh aplikasi dompet *cryptocurrency*.	*OWASP*	Hasilnya didapatkan temuan kemungkinan implikasi privasi dari aplikasi seluler. Serta aplikasi layanan keuangan konvensional hanya sedikit lebih baik daripada aplikasi *cryptocurrency* dalam hal keamanan tetapi memberikan privasi yang kuat.
7	(Yazdinejad et al., 2020)	Mengusulkan cara menggunakan *Recurrent Neural Network* RNN untuk menganalisis kode operasi aplikasi Windows (Opcodes) sebagai studi kasus	*Recurrent Neural Network* (RNN)	Hasil yang diperoleh membuktikan bahwa model konfigurasi 3-*layer* memperoleh 98% akurasi deteksi, yang merupakan tingkat tertinggi di antara konfigurasi saat ini.

2.2 Konsep Pengetahuan

2.2.1 Forensik Digital

Forensik Digital merupakan keahlian, seni dan keterampilan dalam menganalisa serta memulihkan data dari perangkat digital seperti komputer, *smartphone*, laptop, dan lain-lainnya. Bukti forensik digital berhubungan dengan program perangkat lunak, dokumen komputer, teks, email, foto digital, atau rekaman digital lainnya yang berkaitan dalam hukum pidana, perdata dan penyelidikan pribadi (Periyadi et al., 2017). Dalam buku belajar mengenali forensika digital (Sudyana, 2016) Aspek-aspek yang harus ada termuat

diantaranya cabang ilmu forensik, adanya tahapan-tahapan yang dilakukan, penerapan metode ilmiah, berguna merekonstruksi peristiwa kejahatan yang terjadi, untuk menemukan bukti digital, digunakan untuk kepentingan hukum, dapat diterima dalam pengadilan. Berdasarkan aspek-aspek tersebut, maka dapat diartikan bahwa, Forensik Digital adalah sebuah bidang ilmu forensik dengan penggunaan ilmu dan metode ilmiah dalam menemukan dan mencari barang bukti digital untuk memeriksa peristiwa kejahatan yang terjadi dengan alur yang terstruktur sehingga dapat digunakan untuk penegakkan hukum dan diterima dalam pengadilan.



Gambar 2.1 Barang Bukti Elektronik

2.2.2 *Mobile Forensics*

Mobile Forensics adalah bidang ilmu yang mempelajari proses mencari bukti digital menggunakan cara yang tepat dari perangkat *smartphone* yang biasanya dilakukan di investigasi forensik digital (Şentürk et al., 2020).

Mobile Forensics adalah cabang forensika digital yang menggunakan metode ilmiah untuk mengidentifikasi, mengumpulkan, menganalisis, menguji, menghubungkan, menggunakan, dan mendokumentasikan barang bukti digital dari beberapa sumber digital yang aktif untuk memproses dan mengirimkannya. *Mobile Forensics Tools* (MFT) digunakan untuk membantu investigator dalam mengumpulkan informasi dari perangkat, membuat salinan yang valid dari informasi tersebut untuk dianalisis dan untuk mengekstrak bukti yang dapat diandalkan yang secara hukum (Majed et al., 2020).

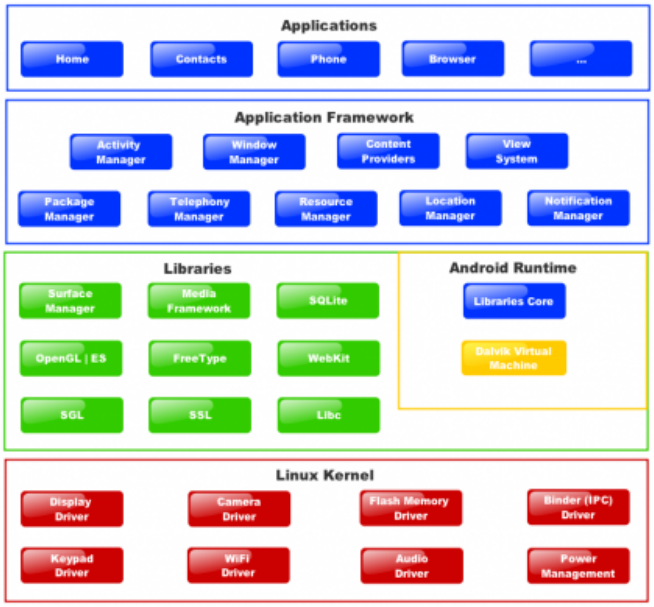
Artefak digital pada *smartphone* dapat diekstrak dengan metode fisik dan logis. Metode logis adalah mengekstrak data dari file sistem dengan langsung berinteraksi dengan perangkat menggunakan tools khusus untuk *mobile device forensics* (Madiyanto et al., 2017).

Gambar 2.2 Proses ekstraksi data pada *smartphone*

2.2.3 *Android*

Android adalah *platform* perangkat lunak dan sistem operasi untuk *smartphone*, berdasarkan *kernel Linux* dan dikembangkan oleh *Google Inc.* dan *Open Handset Alliance*. *Android* di kembangkan dengan pemograman *Java*, mengontrol perangkat melalui Java libraries yang dikembangkan oleh *Google Inc*. *Android* adalah *open source* yang dapat diunduh secara gratis pada perangkat lunak untuk perangkat seluler yang mencakup sistem operasi, *middleware*, dan aplikasi berbasis *Linux* dan *Java*. *Google Inc*. membeli Android pada tahun 2005, dan diresmikan pada tahun 2007. Google membuat *script Android* sebagai *Open source* berlisensi *Apache*. *Android* memiliki banyak pengembang aplikasi di seluruh dunia. Pertama-tama para pengembang menulis skrip di *Java*, lalu unduh aplikasi dari situs pihak ketiga atau toko online (Kirthika et al., 2015).

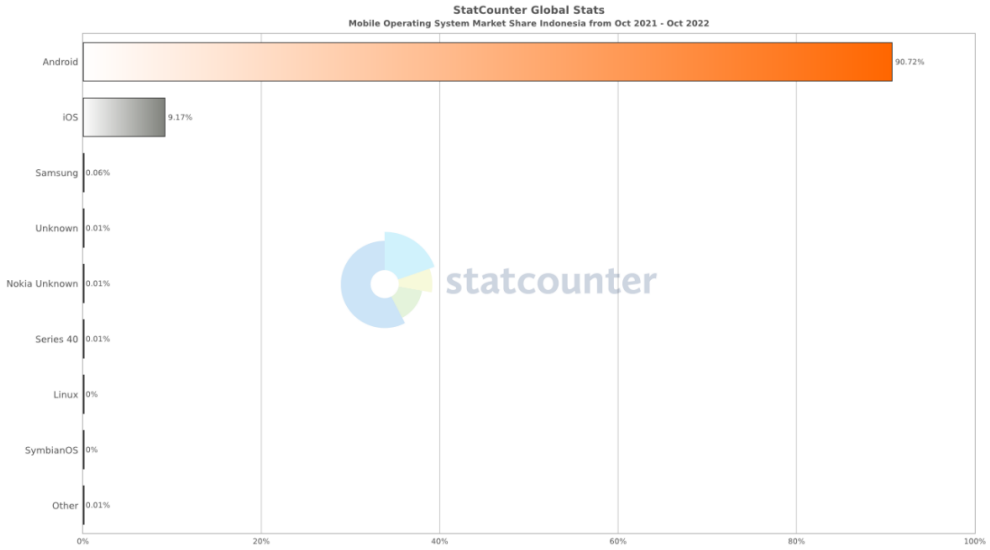
Sistem operasi android memiliki 5 lapisan (layer) yang merupakan komponen sistem android antara lain *application, application framework, library, android runtime,* dan *kernel.*



Gambar 2.3 Arsitektur *Android Operating System*

Menurut (Harahap, 2013) diketahui dalam komponen android terdapat 5 lapisan (Layer) sebagai berikut:

- Kernel
- Library
- Android Runtime
- Application Framework
- Application



Gambar 2.4 Jumlah Pengguna Sistem Operasi Bulan Oktober 2022

Menurut hasil survei yang dilakukan oleh StatCounter 2022 menyebutkan bahwa sistem operasi *smartphone* yang paling banyak digunakan di Indonesia pada tahun 2022 adalah Sistem Operasi *Android*. Pada bulan oktober 2022, *Android* menguasai pangsa pasar hampir 90.72 persen. Sedangkan sistem operasi *smartphone* lainnya berada di bawah 10 persen.

2.2.4 Metode *DFRWS*

Metode DFRWS (Digital Forensics Research Workshop) adalah pendekatan sistematis yang digunakan dalam bidang forensik digital untuk mengumpulkan, menganalisis, dan menginterpretasi bukti digital dari berbagai sumber. Metode ini dikembangkan oleh komunitas forensik digital dengan tujuan untuk menyediakan pendekatan yang lebih terstruktur dan konsisten dalam melakukan investigasi digital. DFRWS telah mengembangkan beberapa prinsip, langkah-langkah, dan panduan umum yang digunakan oleh para profesional forensik dalam menyusun strategi investigasi dan analisis (Garfinkel et al., 2009).

DFRWS memiliki beberapa karakteristik utama:

1. *Open Methodology*: Metode DFRWS dirancang sebagai metodologi terbuka yang dapat diakses oleh seluruh komunitas forensik digital. Hal ini memungkinkan kolaborasi, pengembangan, dan penyesuaian berdasarkan perkembangan teknologi dan tantangan investigasi yang muncul.
2. *Scientific Approach*: Metode DFRWS menekankan pada pendekatan ilmiah dalam melakukan investigasi digital. Ini mencakup penggunaan prinsip-prinsip forensik dan metode analisis yang didukung oleh bukti-bukti yang kuat dan terukur.
3. *Reproducility*: Salah satu prinsip penting dalam metode DFRWS adalah kemampuan untuk mereproduksi hasil investigasi. Ini berarti bahwa langkah-langkah dan teknik yang digunakan harus dapat dijelaskan secara rinci dan dapat direplikasi oleh orang lain.
4. *Holistic Approach*: Metode DFRWS merangkul pendekatan komprehensif dalam analisis bukti digital. Ini mencakup langkah-langkah untuk mengumpulkan bukti, menganalisis bukti dalam konteks yang lebih luas, dan menghasilkan laporan yang komprehensif.
5. *Collaboration*: Metode DFRWS mendorong kolaborasi antara para profesional forensik digital, akademisi, dan peneliti. Ini membantu dalam pengembangan metodologi yang lebih baik dan solusi untuk tantangan forensik terbaru.

Berdasarkan tahapan metode *DFRWS (Digital Forensic Research Workshop)*, terdapat enam tahapan yang harus dilakukan, sebagai berikut:

1. ***Identifiaction***

   Suatu tahapan proses identifikasi untuk menentukan persyaratan yang dibutuhkan selama tahap investigasi, pencarian dan informasi barang bukti elektronik.

2. ***Preservation***

   Suatu tahapan proses menangani barang bukti digital untuk mencegah dan menjamin keaslian barang bukti elektronik dari gangguan.

3. ***Collection***

   Suatu tahapan proses pengumpulan dengan mengidentifikasi bagian-bagian khusus dari barang bukti digital dan menentukan sumber data.

4. ***Examination***

   Suatu tahapan proses melakukan penyaringan data pada begian tertentu dari sumber data. Penyaringan data adalah proses mengubah bentuk data pada bagian tertentu dari sumber data tanpa mengubah isi data, karena keaslian data sangat penting.

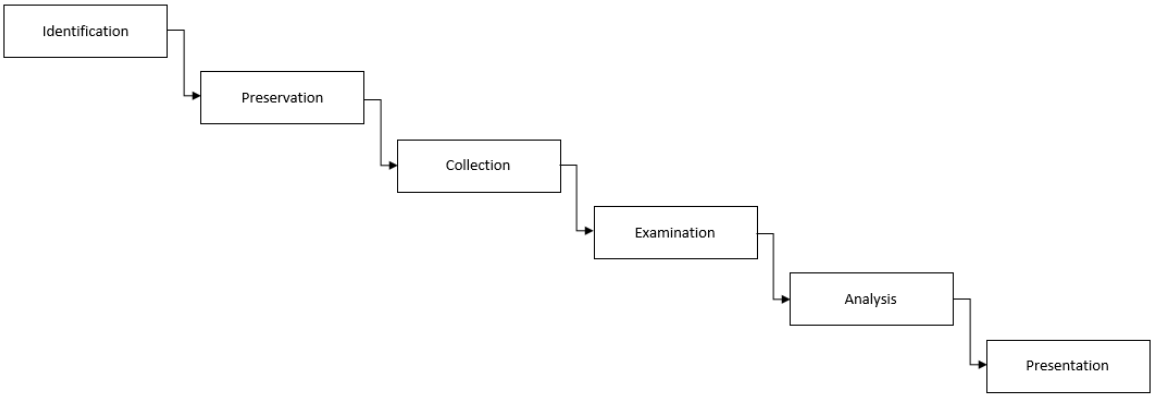
5. ***Analysis***

   Suatu tahapan proses melakukan untuk menentukan asal-usul data, pencipta data, metode penciptaan data, dan tujuan di balik pembuatan data tersebut.

6. ***Presentation***

   Suatu tahapan proses melibatkan tahap penyajian informasi yang dihasilkan dari analisis. Tahap presentasi ini terjadi setelah memperoleh barang bukti digital dari pemeriksaan dan menganalisisnya.

Metode *DFRWS* memiliki beberapa tahapan, seperti pada gambar 3.10.

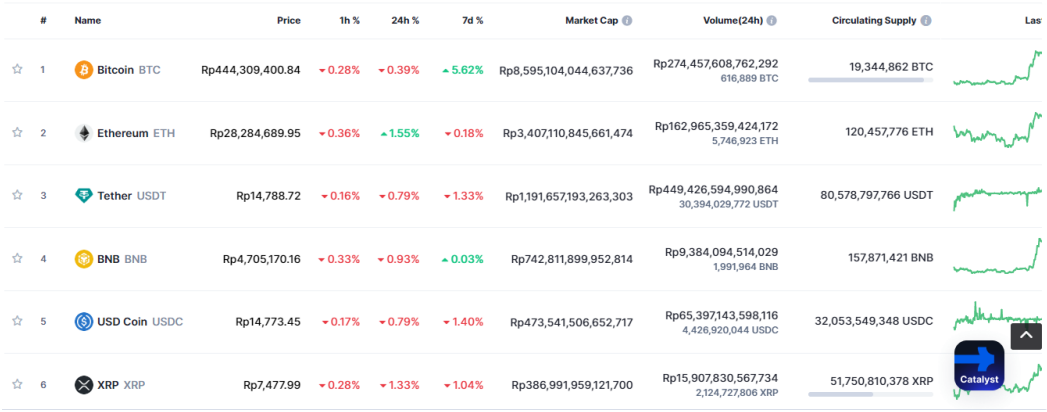


Gambar 2.5 Tahapan Metode DFRWS (Fadillah et al., 2022).

2.2.5 *Cryptocurrency*

Cryptocurenncy adalah suatu metode untuk membuat koin virtual dan menyediakan kepemilikan serta transaksi yang aman dengan menggunakan teknik kriptografi. Metode ini dirancang agar mudah diverifikasi tetapi secara komputerisasi sulit untuk dipecahkan kuncinya. Berbagai *cryptocurrency* menggunakan teknik yang berbeda untuk tujuannya, yang paling umum menggunakan nilai hash, dimana hash dihitung sehingga nilai lebih rendah dari nilai tertentu. Dalam kerja komputerisasi dimana metode ini transaksinya diverifikasi sebagai kunci yang unik dan dapat dipercaya. Untuk mendorong partisipasi dalam *cyptocurrency*, transaktor menyertakan biaya transaksi yang masuk ke pengguna pertama yang telah berhasil memverifikasinya. Selain itu, pada proses transaksi jaringan memberikan kepada verifikator sejumlah koin setelah berhasil memverifikasi satu blok transaksi. Proses ini, yang disebut penambangan. Penambangan adalah suatu cara di mana pasokan koin yang beredar pada jaringan diperluas dan kesulitan yang dapat disesuaikan memastikan bahwa kemajuan komputerisasi tidak akan mempengaruhi tingkat ekspansinya. (Harwick, 2016).

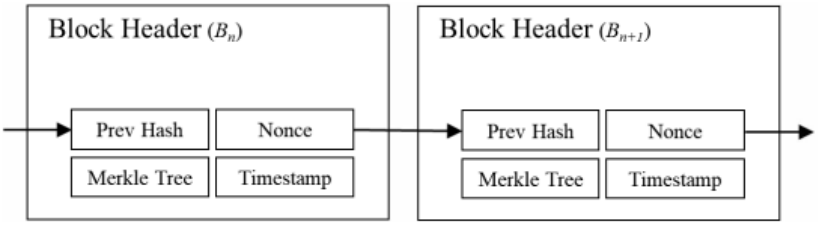
Pada umumnya sistem *cryptocurrency* mengklaim menyediakan pemrosesan transaksi anonim dan terdesentralisasi. Anonimitas ini digunakan sebagai tindakan pencegahan tambahan untuk privasi pengguna dan kerahasiaan. Permintaan dan penerimaan *cryptocurrency* meningkat selama beberapa tahun terakhir. Demikian pula, industri *cryptocurrency* telah berevolusi sejak awal dan sejumlah pemangku kepentingan sekarang telah terhubung dengan perdagangan yang berkembang dan penerimaan mata uang kripto. Saat ini, *cryptocurrency* sudah tersedia di ratusan bursa di seluruh dunia terhadap mata uang fiat (Hameed & Farooq, 2016).



#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Las
1	Bitcoin BTC	Rp444,309,400.84	0.28%	0.39%	5.62%	Rp8,595,104,044,637,736	Rp274,457,608,762,292 616,889 BTC	19,344,862 BTC	
2	Ethereum ETH	Rp28,284,689.95	0.36%	1.55%	0.18%	Rp3,407,110,845,661,474	Rp162,965,359,424,172 5,746,923 ETH	120,457,776 ETH	
3	Tether USDT	Rp14,788.72	0.16%	0.79%	1.33%	Rp1,191,657,193,263,303	Rp449,426,594,990,864 30,394,029,772 USDT	80,578,797,766 USDT	
4	BNB BNB	Rp4,705,170.16	0.33%	0.93%	0.03%	Rp742,811,899,952,814	Rp9,384,094,514,029 1,991,964 BNB	157,871,421 BNB	
5	USD Coin USDC	Rp14,773.45	0.17%	0.79%	1.40%	Rp473,541,506,652,717	Rp65,397,143,598,116 4,426,920,044 USDC	32,053,549,348 USDC	
6	XRP XRP	Rp7,477.99	0.28%	1.33%	1.04%	Rp386,991,959,121,700	Rp15,907,830,567,734 2,124,727,806 XRP	51,750,810,378 XRP	

Gambar 2.6 Mata Uang *Cryptocurrency*

Blockchain berbeda dari kontrak keuangan tradisional, blockchain menghindari perantara pusat tepercaya dan mengandalkan biaya onchain. Setiap blok berisi stempel waktu yang memungkinkannya ditelusuri kembali ke blok sebelumnya saat menggunakan enkripsi data dan infrastruktur kunci publik, seperti yang ditunjukkan pada gambar 2.5



Gambar 2.7 Skema *Blockchain* Dalam *Cryptocurrency* (Baek et al., 2019).

2.2.6 Dompet *Cryptocurrency*

Dompet *cryptocurrency* merupakan sebuah aplikasi dompet digital yang digunakan untuk deposit, menyimpan, penarikan dan melakukan transfer aset digital *cryptocurrency*. Dompet *cryptocurrency* dapat diklasifikasikan menjadi 4 jenis yaitu:

1. *exchange wallets* (pertukaran dompet)
2. *software wallets* (dompet perangkat lunak)
3. *hardware wallets* (dompet perangkat keras)
4. *paper wallets* (dompet kertas).

Pada mekanisme kerjanya dompet *cryptocurrency* dapat diklasifikasikan menjadi dua jenis yaitu:

1. *hot wallets* (dompet panas)
2. *cold wallets* (dompet dingin).

Hot wallet adalah dompet yang terhubung dengan jaringan internet, sedangkan *cold wallet* adalah tidak terhubung jaringan internet. *Exchange wallet* dan S*oftware wallet* adalah h*ot wallet* sedangkan *hardware wallets* dan *paper wallets* adalah *cold wallets*. *Hot wallet* hadir dengan banyak kemudahan sementara *cold wallet* hadir dengan keamanan yang lebih baik (Khan et al., 2019).

2.2.7 Tokocrypto

PT Crypto Indonesia Berkat (Tokocrypto) adalah sebuah startup yeng bergerak di bidang *marketplace* menyediakan layanan untuk masyarakat agar dapat melakukan penyimpanan atau transaksi jual/beli aset *cryptocurrency* yang terdaftar resmi di Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti). Tokocrypto pada awalnya menggunakan web untuk melakukan kegiatan perdagangan, namun sekarang telah bertransisi ke aplikasi mobile. (Ladita, 2020).

Tokocrypto resmi didirikan pada bulan September 2018. Kantor utama tokocrypto Saat ini memusatkan operasi kami di Jakarta, ibu kota Indonesia.

- Visi kami

  Untuk meningkatkan akses aset kripto kepada masyarakat Indonesia. Kami percaya bahwa dengan meningkatkan akses ini, kami dapat membantu masyarakat Indonesia mengambil bagian dalam inovasi kripto yang menarik dan meningkatkan taraf hidup mereka.

- Misi

  Untuk membangun bursa terbaik di Indonesia yang didukung oleh produk yang berpusat pada pengguna, infrastruktur yang kuat, dan kepatuhan terhadap regulator kami.

Gambar 2.8 Logo Tokocrypto

BAB 3
Metodologi

3.1 Pendahuluan

Tahap metodologi ini meliputi beberapa tahapan yang dilakukan secara berurutan untuk menuntun penelitian mulai dari awal hingga akhir. Gambar 3.1 merupakan diagram alir penelitian yang dijalankan.

Gambar 3.1 Tahapan Penelitian

3.2 Kajian Literatur

Merupakan tahap untuk memahami tentang konsep, teori, dan hasil temuan penelitian lain yang serumpun dan akan dijadikan acuan sebagai landasan penelitian. Data yang digunakan dalam penelitian ini adalah data kualitatif. Dimana sumber data penelitian ini dari dokumen-dokumen penelitian atau penemuan sebelumnya, baik bersifat *offline source* maupun *online source* dengan topik terkait.

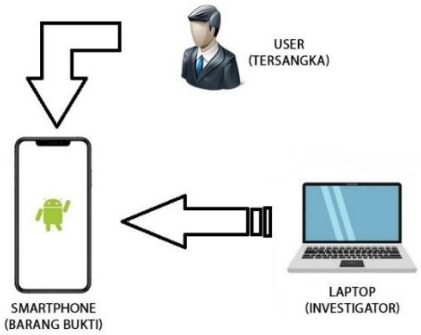
Kajian literatur dilakukan terhadap penelitian yang berkaitan dengan masalah-masalah pada dompet *cryptocurrency*, berikut juga metode-metode yang digunakan untuk melakukan proses investigasi, sehingga dapat menunjang tujuan akhir dilakukannya penelitian ini.

3.3 Persiapan Sistem

Persiapan sistem adalah tahap merancang dan mengimplementasikan aplikasi dompet *cryptocurrency* tokocrypto pada perangkat *smartphone* berbasis *android* sebagai perangkat untuk penelitian. Terdiri dari dua perangkat, yaitu perangkat laptop sebagai investigator dan perangkat *smartphone* sebagai barang bukti.

Pada penelitian sebelumnya tentang Analisis Forensik Pada Platform Android Dari hasil pengujian yang dilakukan tool Oxygen memiliki fitur report yang lebih lengkap dibandingkan tool ektraksi android forensik MOBILedit dan AFLogical. Tool ini hampir bisa mengekstrasi keseluruhan data aktual dari kontak ponsel, call log, sms-mms, kalender file gambar, video, dan file lainnya (Yadi & Kunang, 2014).

Berikut rancangan sistem pada ditunjukan gambar 3.2, rincian perangkat keras pada tabel 3.1 dan rincian perangkat lunak pada tabel 3.2



Gambar 3.2 Rancangan Sistem

Tabel 3.1 Perangkat Keras Penelitian

No.	Perangkat Keras	Deskripsi
1	*Smartphone*	Xiaomi Redmi 6A *Android* versi OS 8.1.0 (*Rooted)*
2	Laptop/Investigator	Acer Aspire E5-475G-Core i5-7200 RAM 12GB DDR4 Windows 10
3	Kabel USB	Tipe B

Tabel 3.2 Perangkat Lunak Penelitian

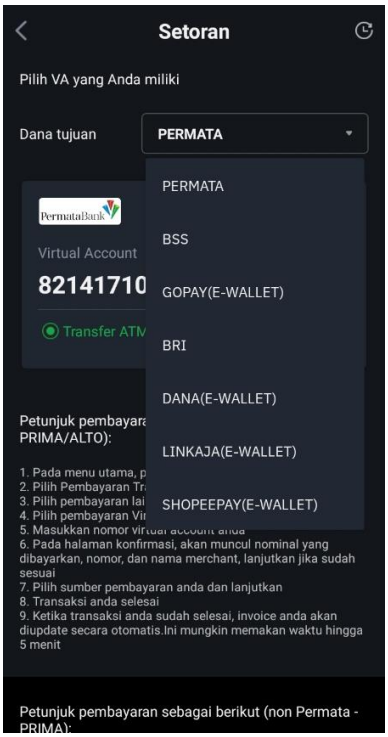
No	Perangkat Lunak	Nama Perangkat Lunak
1	Aplikasi Dompet *Cryptocurrency*	Tokocrypto
2	Alat Forensik	*Oxygen Forensics*
3	Alat *Hashing*	*HashMyFiles*

3.4 Simulasi Kasus

Simulasi kasus adalah tahap dimana aktivitas-aktivitas pada dompet *cryptocurrency tokocrypto* disimulasikan pada perangkat *smartphone* Xiaomi Redmi 6A seperti aktivitas melakukan deposit dan penarikan uang fiat, membeli, mengirim, menerima dan menjual *cryptocurrency*.

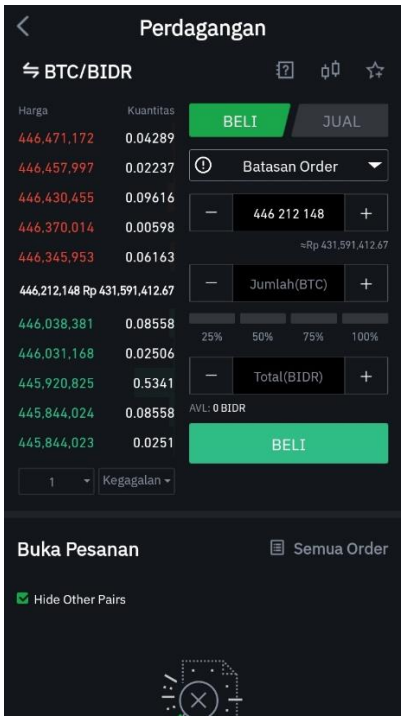
Gambar 3.3 Aktivitas pada Aplikasi Dompet *cryptocurrency*

Tersangka melakukan transaksi deposit uang fiat ke aplikasi dompet *cryptocurrency* tokocrypto dengan beberapa metode seperti pada gambar 3.4



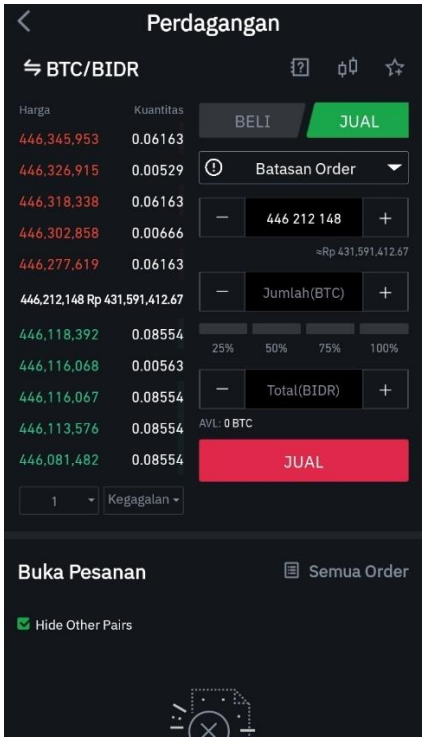
Gambar 3.4 Menu Deposit Uang Fiat *Tokocrypto*

Setelah melakukan transaksi deposit tersangka membeli salah satu *cryptocurrency* seperti pada gambar 3.5



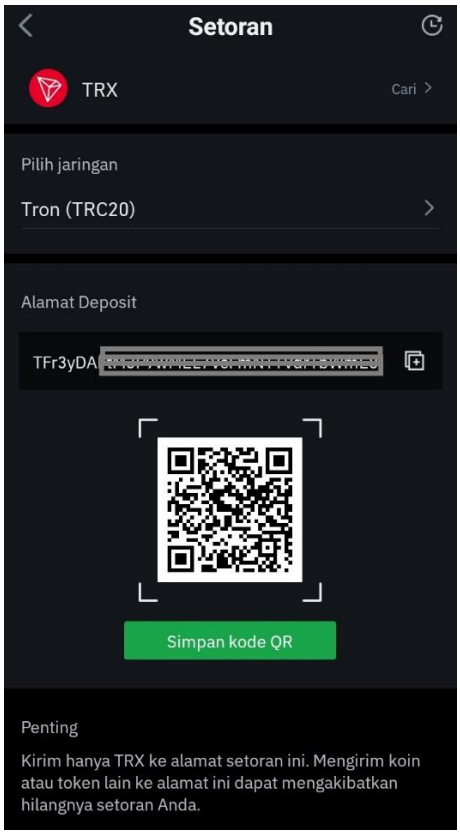
Gambar 3.5 Menu Beli *Tokocrypto*

Setelah melakukan transaksi beli tersangka menjual *cryptocurrency* seperti pada gambar 3.6



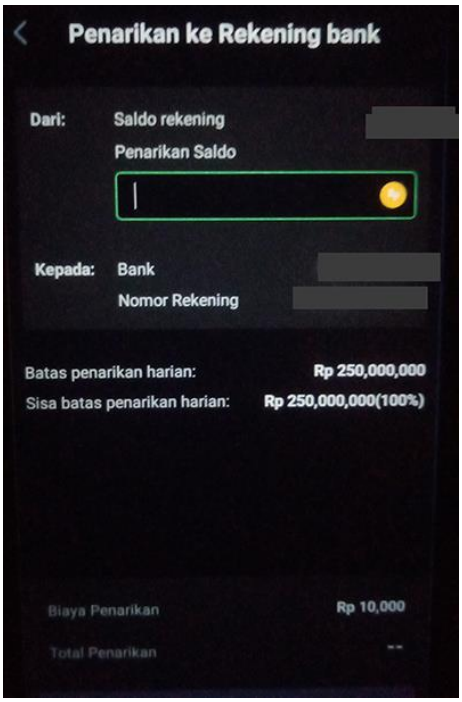
Gambar 3.6 Menu Jual *Tokocrypto*

Berikutnya melakukan transaksi deposit/menerima uang *cryptocurrency* dari teman seperti pada gambar 3.7



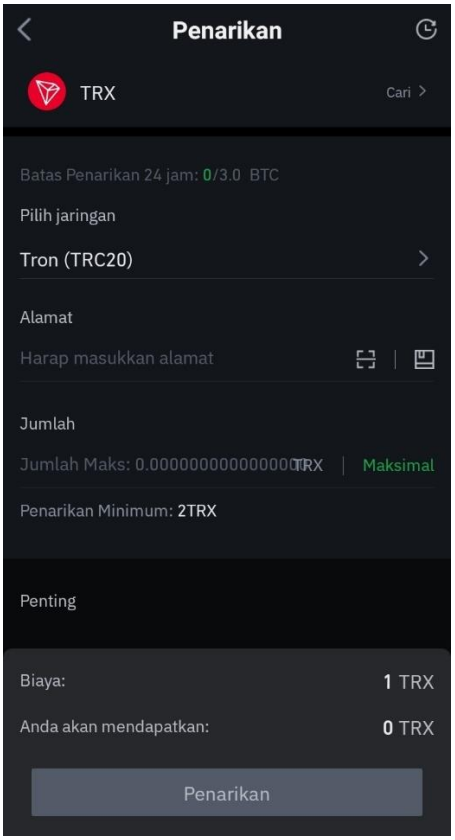
Gambar 3.7 Menu Deposit *Cryptocurrency Tokocrypto*

Berikutnya melakukan transaksi penarikan uang fiat seperti pada gambar 3.8



Gambar 3.8 Menu Penarikan Uang Fiat *Tokocrypto*

Dan terakhir melakukan transaksi mengirim *cryptocurrency* ke teman seperti pada gambar 3.9



Gambar 3.9 Menu untuk Mengirim *Cryptocurrency*

Pada tahap ini, memungkinkan mengidentifikasi skenario kasus yang akan diselesaikan. Dalam aplikasi dompet *cryptocurrency tokocrypto* telah dilakukan aktivitas transaksi sebanyak 10 kali yang telah dirinci pada tabel 3.3

Tabel 3.2 Simulasi Aktivitas Transaksi Pada Aplikasi Dompet *Cryptocurrency Tokocrypto*

No	**Nama *Software***	**Id Pemesanan**	**Txid**	**Waktu Transaksi**	**Jenis Transaksi**	**Deskripsi**
1	Tokocrypto	7866302	f30661e3732f49b0be43964d6a192425	06-04-2023 10:05	Deposit fiat dengan aplikasi dana	Jumlah 49000 BIDR
2		7866310	5a80fad6-f083-47b7-a6ba-22c840350e6a	06-04-2023 10:09	Deposit fiat dengan aplikasi Gopay	Jumlah 49000 BIDR
3		7866384	566fabfb-cae7-42d3-9a97-45b8f3f5818b	06-04-2023 10:23	Deposit fiat pertama dengan aplikasi ShopeePay ke-1	Jumlah 49000 BIDR
4		7866727	904d7618-44f4-4954-921d-d8055eed6ad5	06-04-2023 12:03	Deposit fiat kedua dengan aplikasi ShopeePay ke-2	Jumlah 49000 BIDR
5		[redacted]		06-04-2023 23:27	Pembelian crypto	Jumlah yang dibeli 0.00046 BTC
6				06-04-2023 23:43	Penjualan crypto	Jumlah yang dijual 0.00045 BTC
7		6480141	19396c512b6a49e2853a81a12713ffd9cde	06-04-2023 23:35	Deposit Crypto	Jumlah 35 TRX Ke Alamat dompet TFr3yDAFtM3P9wMEL7VcFmN11Vdr1bWmE8

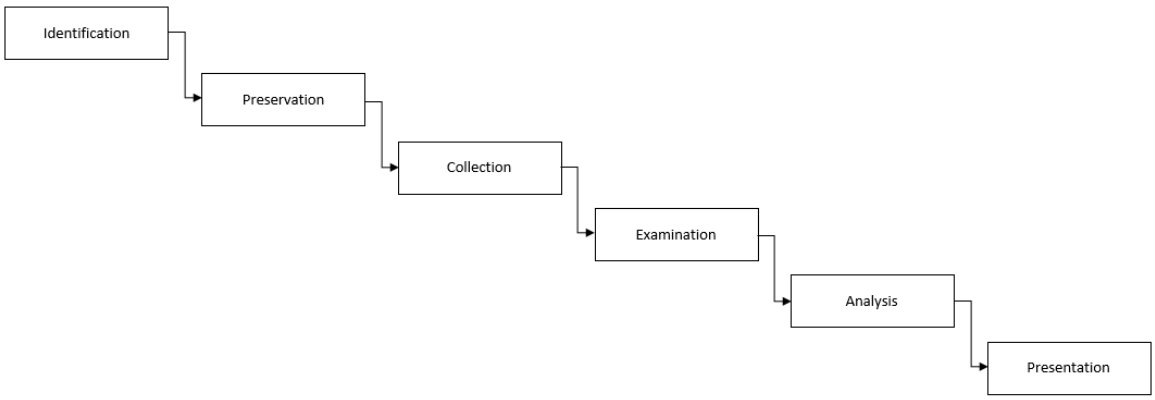
			687382213e67f7429 94c7fc61e79c			
8		5151242	2597835290b9d9585 8e9839b0fa737186cf 31ab4b64fcbd87825b 70f493ca3a3	06-04-2023 23:52	Penarikan Crypto pertama	Jumlah 31 TRX Ke Alamat dompet TGmm6UeGfbsrokadNUR7PM8SwqsdFjFnTG
9		5152799	7e2188e4dc601a1530 773a609976a058b37e 1702518c63bceea093 2064b9e50e	07-04-2023 14:21	Penarikan Crypto kedua	Jumlah 4 TRX Ke Alamat dompet TQAAcLjyvsPzCTrqSUT9HdgAzNMdDgHa3a
10		5075717	642eea2cd129d5cf267 27908	06-04-2023 23:47	Penarikan Fiat	Jumlah 191510 BIDR Ke Bank Mandiri atas nama xxxxxxxxx xxx xxhar dengan nomor rekenign xxxxxxxxx7588

Tujuan dilakukannya simulasi kasus adalah untuk menguji tindakan aktivitas dengan dompet *cryptocurrency* tokocrypto pada perangkat *smartphone* berbasis *android* sehingga dapat dilakukan tahap investigasi forensik.

3.5 Investigasi

Tahap investigasi merupakan tahapan forensik dalam pengujian perangkat *smartphone* untuk menemukan artefak digital atau bukti digital pada aplikasi dompet *cryptocurrency tokocrypto* pada perangkat *smartphone*.

Tahapan dalam forensik digital bisa mengadopsi salah satu dari empat kerangka kerja standar yang digunakan dalam proses investigasi, seperti standar yang ditetapkan oleh *Digital Forensic Research Workshop* (DFRWS), *National Institute of Justice* (NIJ), National *Institute of Standards and Technology* (NIST), *Digital Forensics Integrated Investigation Framework* (IDFIF) dan *Association of Chief Police Officers* (ACPO). Alternatifnya, dapat juga menerapkan pendekatan proses investigasi forensik yang berbeda. Dalam penelitian ini, pendekatan akuisisi yang diterapkan adalah Live Forensics dengan mengadopsi kerangka kerja forensik digital yang mengikuti pedoman yang telah ditetapkan oleh Digital Forensic Research Workshop (DFRWS) sebagai pedoman utama dalam mengarahkan jalannya penelitian ini. Metode DFRWS telah menjadi dasar bagi banyak praktisi dan peneliti dalam melaksanakan investigasi forensik digital yang lebih ilmiah dan efektif. Metode Digital Forensic Research Workshop (DFRWS) memberikan cara untuk mendokumentasikan semua informasi yang diperlukan dengan mekanisme yang sesuai dan secara lengkap akan dibahas hasilnya pada Bab 4. Metode *DFRWS* memiliki beberapa tahapan, seperti pada gambar 3.10.



Gambar 3.10 Tahapan Metode DFRWS (Fadillah et al., 2022).

Berdasarkan tahapan metode *DFRWS (Digital Forensic Research Workshop)*, terdapat enam tahapan yang harus dilakukan, sebagai berikut:

3.5.1 *Identifiaction*

Suatu tahapan proses identifikasi untuk menentukan persyaratan yang dibutuhkan selama tahap investigasi, pencarian dan informasi barang bukti elektronik.

3.5.2 *Preservation*

Suatu tahapan proses menangani barang bukti digital untuk mencegah dan menjamin keaslian barang bukti elektronik dari gangguan.

3.5.3 *Collection*

Suatu tahapan proses pengumpulan dengan melakukan identifikasi bagian yang khusus dari barang bukti digital dan melakukan identifikasi sumber data.

3.5.4 *Examination*

Suatu tahapan proses melakukan penyaringan data pada begian tertentu dari sumber data. Penyaringan data dilakukan dengan perubahan bentuk data namun tidak melakukan perubahan pada isi data karena keaslian data merupakan hal yang sangat penting.

3.5.5 *Analysis*

Suatu tahapan proses melakukan penentuan tentang dimana data tersebut dihasilkan, oleh siapa data tersebut dihasilkan, bagaimana data tersebut dihasilkan dan kenapa data tersebut dihasilkan.

3.5.6 *Presentation*

Suatu tahapan proses dilakukan dengan menyajikan informasi yang dihasilkan dari tahap analisis. Tahap presentasi dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis.

3.6 Laporan

Tahapan laporan merupakan kesimpulan dari keseluruhan penelitian yang telah dilakukan.

BAB 4

Hasil dan Pembahasan

Bab ini membahas secara lengkap dari penelitian yang diangkat tentang analisis artefak digital dompet *cryptocurrency* tokocrypto pada android sebagai metode investigasi forensik mobile. Metode *DFRWS* memiliki 6 tahapan yaitu *Identification, Preservation, Collection, Examination, Analysis* dan *Presentation* yang akan diuraikan secara detail pada bagian pembahasan ini.

4.1 *Indentification*

Tahap indentification merupakan tahap untuk menentukan persyaratan yang dibutuhkan selama tahap investigasi, pencarian dan informasi barang bukti elektronik. Barang bukti yang didapat adalah sebuah perangkat *smartphone android* Xiomi Redmi 6A seperti pada gambar 4.1 dan indentifikasi rincian spesifikasi *smartphone* Xiomi Redmi 6A pada tabel 4.1:

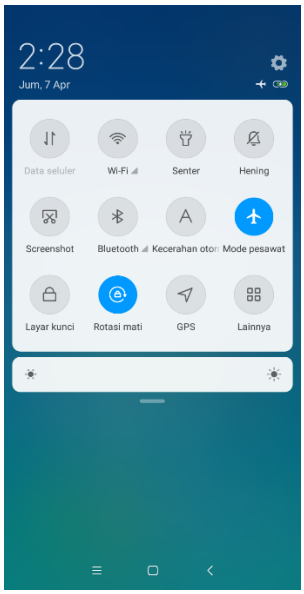
Gambar 4.1 Barang Bukti *Smartphone*

Tabel 4.1 Spesifikasi Barang Bukti *Smartphone*

Spesifikasi	
Merek	Xiomi
Nomor model	Redmi 6A
OS	*Android* (8.1.0)
Nomor seri	35bd9606xxxx
imei	86978804294xxxx
Ram	2GB
ROM	16GB
Rooted	Yes

4.2 *Preservation*

Tahap *preservation* adalah tahap untuk menangani barang bukti digital untuk mencegah dan menjamin keaslian barang bukti elektronik dari gangguan. Maka barang bukti elektroik akan disimpan di tempat aman dan terisolasi berdasarkan segala macam komunikasi, kemudian koneksi jaringan dan internet pada perangkat *smartphone* dinonaktifkan menggunakan mode pesawat pada perangkat *smartphone* Xiomi Redmi 6A seperti pada gambar 4.2:

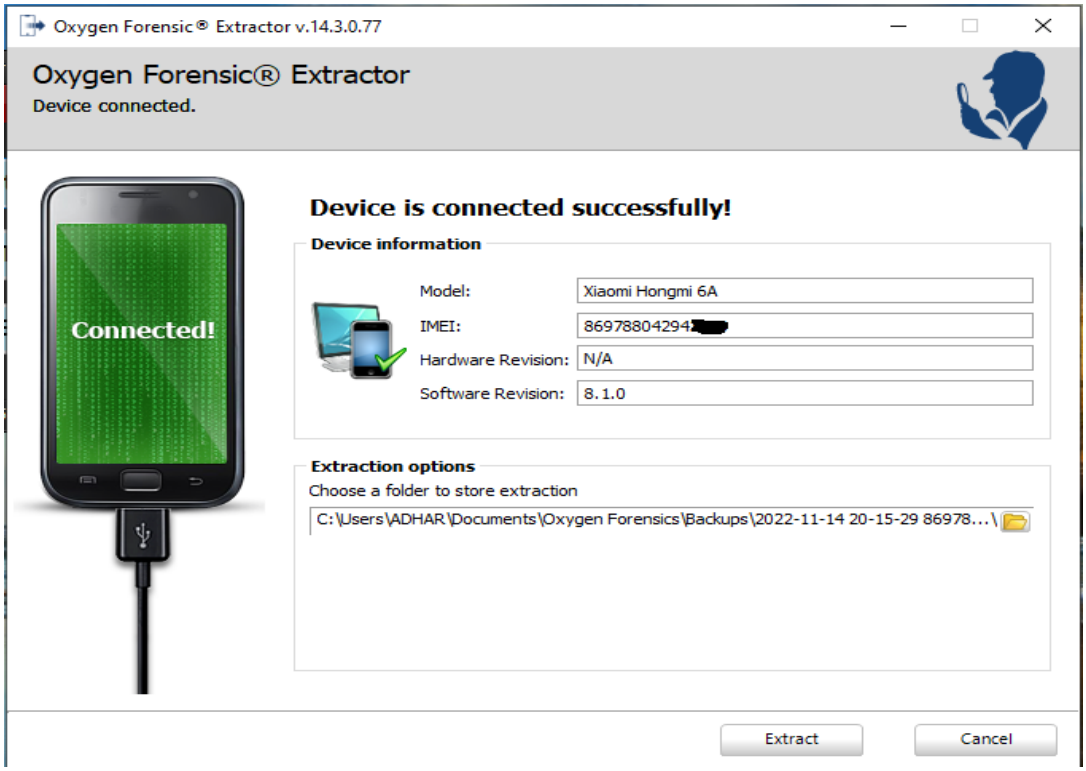


Gambar 4.2 Isolasi barang bukti dengan mode pesawat

4.3 *Collection*

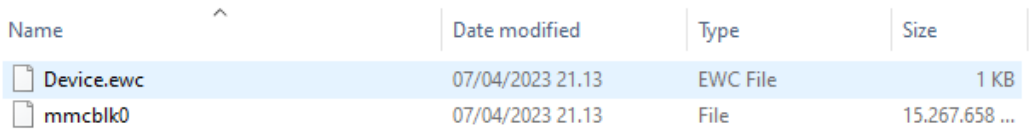
Tahap *colletion menggunakan* alat forensik adalah HashMyFiles untuk menjaga integritas data yang diubah atau dimanipulasi setalah dilakukan tahap akuisisi. Untuk tahap akuisisi menggunakan alat *Oxygen Forensics* yang mampu mengolah data *physical image* pada

perangkat *smartphone* Xiomi Redmi 6A. Tahap akuisisi dilakukan dengan menyambungkan perangkat *smartphone* Xiomi Redmi 6A dengan laptop sebagai perangkat investigator yang sudah terpasang alat *Oxygen Forensics* seperti pada gambar 4.3:



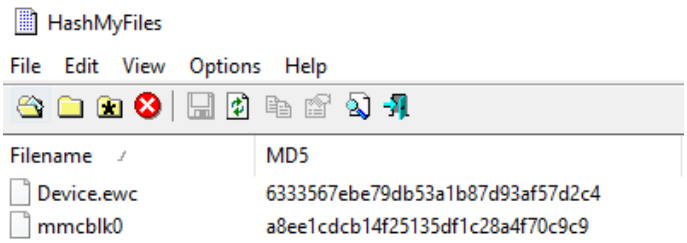
Gambar 4.3 Proses physical image data perangkat *smartphone* dengan alat *Oxygen Forensics*

Setelah tahap *physical image* data *smartphone* dari barang bukti perangkat *smartphone* Xiomi Redmi 6A selesai, maka menghasilkan 2 file seperti pada gambar 4.4:



Gambar 4.4 Hasil Akuisisi

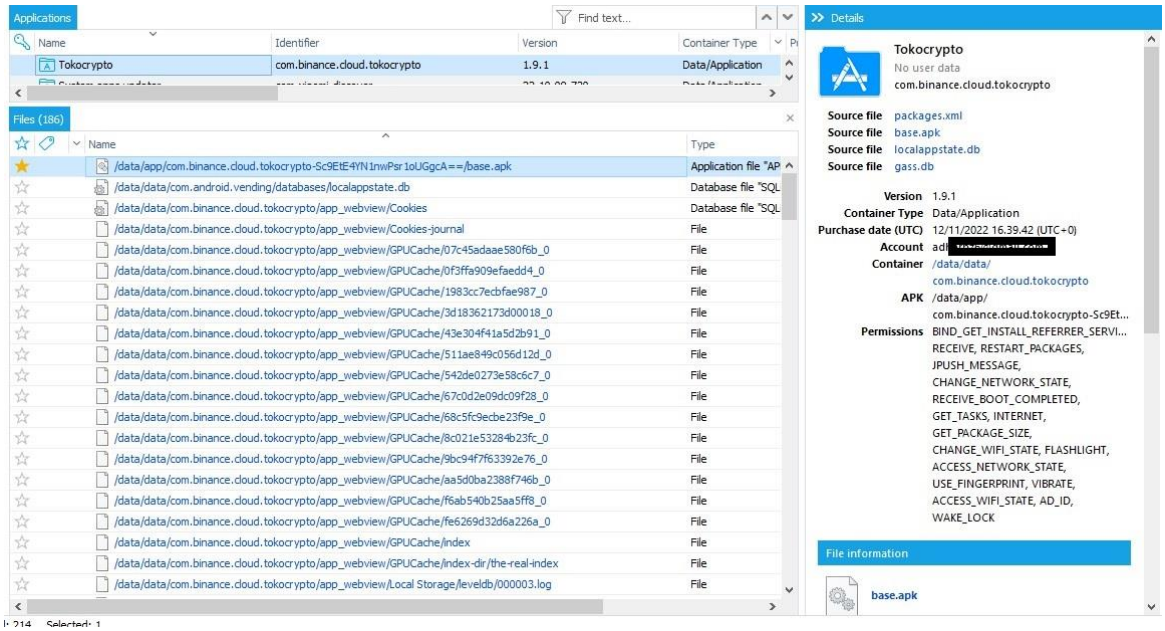
File *physical image* yang dihasilkan dari perangkat *smartphone* Xiomi Redmi 6A pada proses akuisisi dilakukan hashing untuk menjaga validitas bukti digital menggunakan alat *HashMyFiles*, menghasilkan nilai MD5 pada file *Device.ewc* (6333567ebe79db53a1b87d93af57d2c4) dan *mmcblk0* (a8ee1cdcb14f25135df1c28a4f70c9c9) seperti pada gamabar 4.5:



Gambar 4.5 Nilai hash MD5

4.4 *Examination*

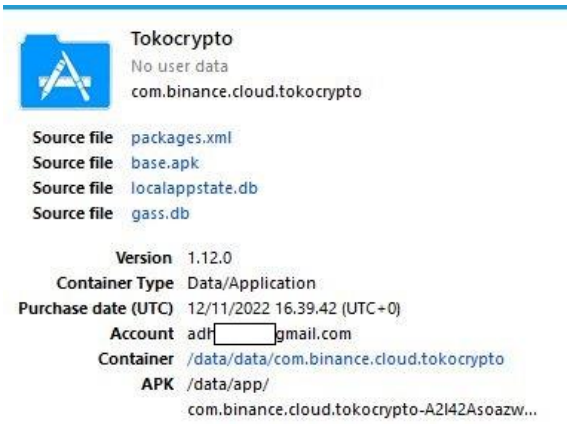
Pada tahap ini, file *physical image* dilakukan ekstraksi agar data-data dapat diekstrak dari file *physical image* perangkat *smartphone* Xiomi Redmi 6A, proses ekstraksi menggunakan alat *Oxygen Forensics* seperti pada gambar 4.6*:*



Gambar 4.6 Hasil ekstraksi file *physical image* menggunakan O*xygen Forensics*

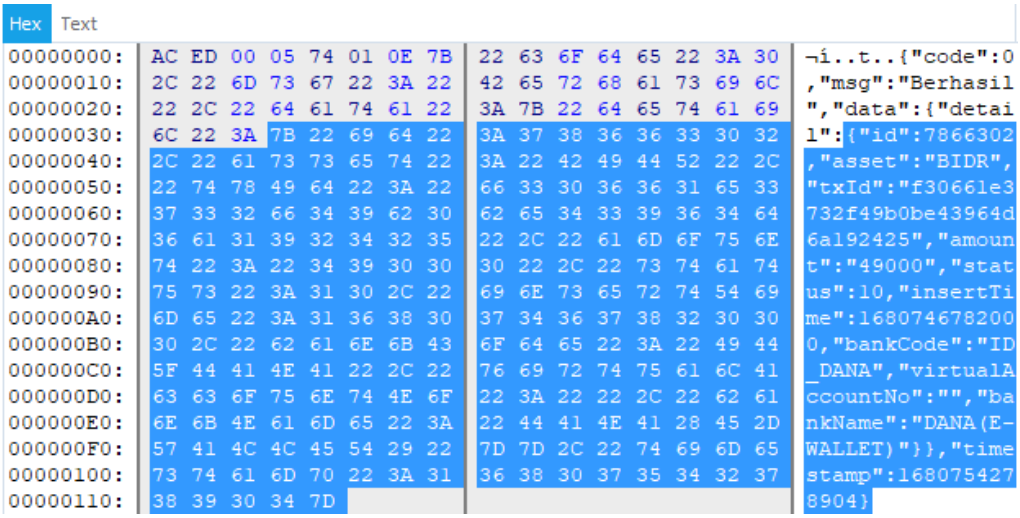
4.5 *Analysis*

Proses analisis menggunakan alat *Oxygen Forensics* dengan data-data yang diekstrak dari file *physical image* perangkat *smartphone android*. Proses analisis akan berfokus pada direktori *data/data/<package_name>* dari aplikasi dompet *cryptocurrency* tokocrypto. Analisis aplikasi dompet *cryptocurrency* tokocrypto ditemukannya informasi akun pengguna dan inforamsi waktu aplikasi di install seperti pada gambar 4.7:



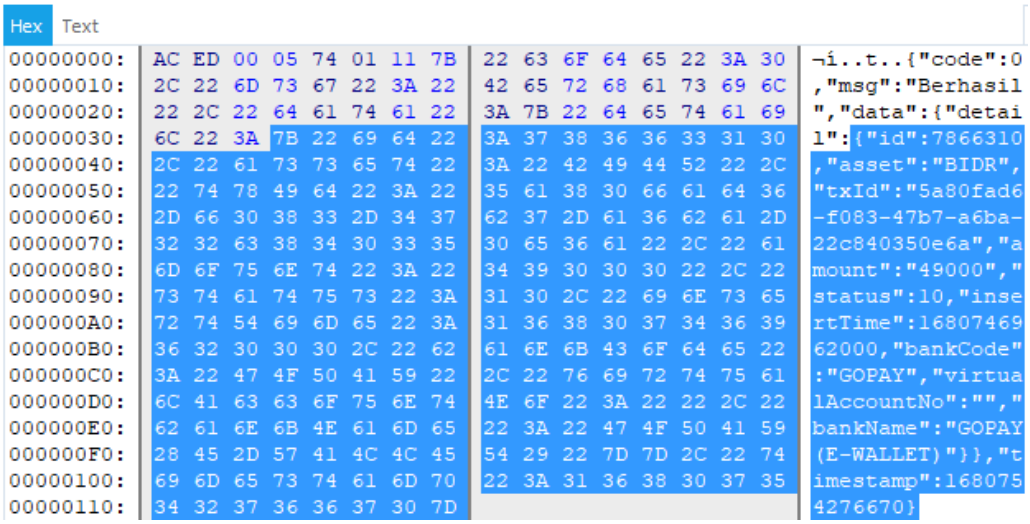
Gambar 4.7 Informasi akun pengguna

Pada file /data/data/com.binance.cloud.tokocrypto/cache/cache/data/fac471429f2b4 88385f87c4429601b26 ditemukan informasi aktivitas transaksi dengan aplikasi *E-Wallet* Dana yang pernah dilakukan dengan id: 7866302, asset: BIDR, txId: f30661e3732f 49b0be43964d6a192425, jumlah: 49000, nama bank: Dana(E-Wallet) dan timestamp: 1680 754278904 seperti pada gambar 4.8.



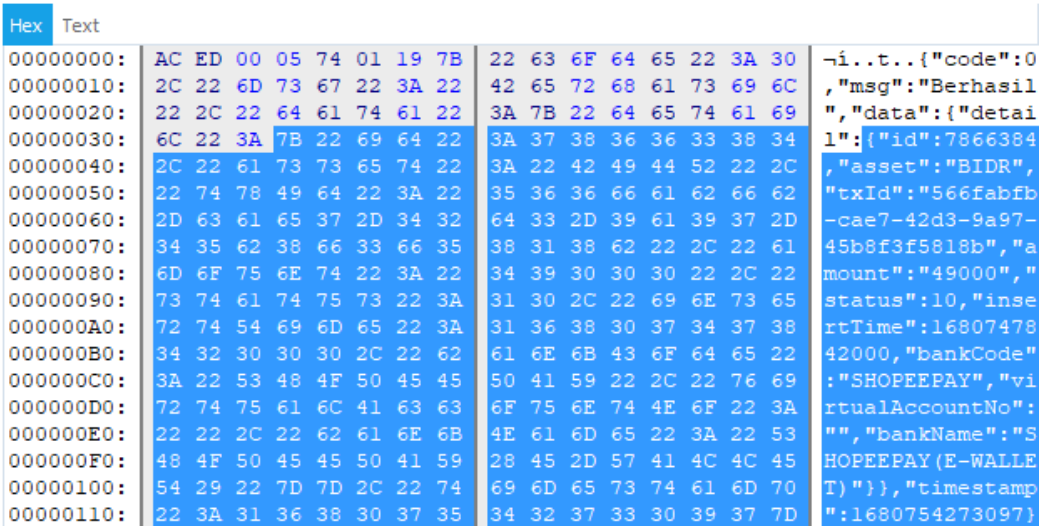
Gambar 4.8 Aktivitas Transaksi dengan Aplikasi *E-Wallet* Dana

Pada file /data/data/com.binance.cloud.tokocrypto/cache/cache/data/e4f8598a0faaa 3e31db48ddcca92c3b1 ditemukan informasi aktivitas transaksi dengan aplikasi *E-Wallet* Gopay yang pernah dilakukan dengan id: 7866310, asset: BIDR, txId: 5a80fad6-f083-47b7-a6ba-22c840350e6a, jumlah: 49000, nama bank: Gopay(E-Wallet) dan timestamp: 1680754278904 seperti pada gambar 4.9.



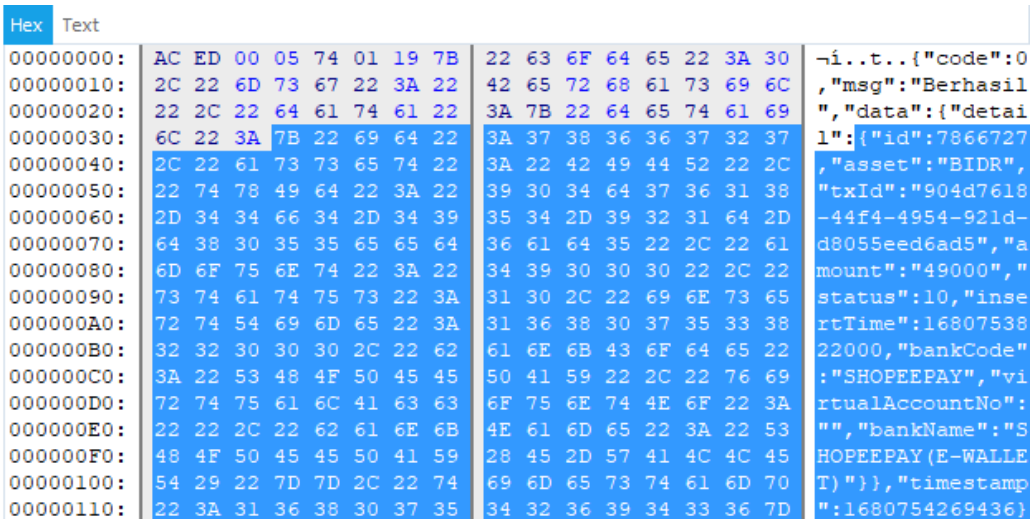
Gambar 4.9 Aktivitas Transaksi dengan Aplikasi *E-Wallet* Gopay

Pada file /data/data/com.binance.cloud.tokocrypto/cache/cache/data/135dc9ff389f9e619a81f77d272a85c9 ditemukan informasi aktivitas transaksi dengan aplikasi *E-Wallet* Shopeepay ke-1 yang pernah dilakukan dengan id: 7866384, asset: BIDR, txId: 566fabfb-cae7-42d3-9a97-45b8f3f5818b, jumlah: 49000, nama bank: Shopeepay(E-Wallet) dan timestamp: 1680754273097 seperti pada gambar 4.10.



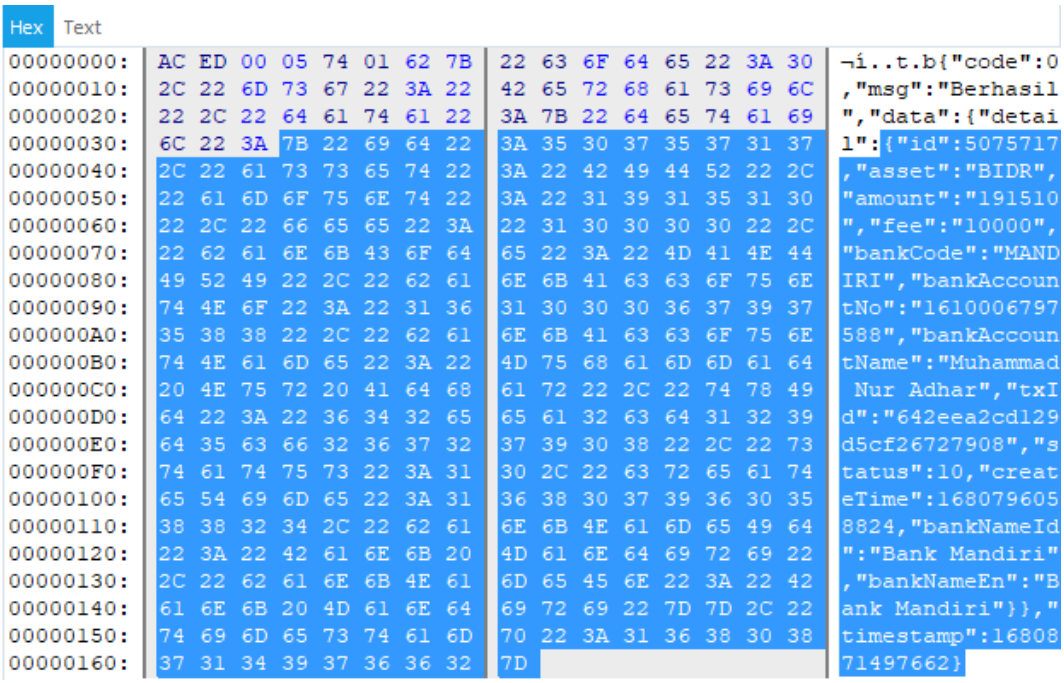
Gambar 4.10 Aktivitas transaksi dengan aplikasi Shopeepay ke-1

Pada file /data/data/com.binance.cloud.tokocrypto/cache/cache/data/70f77b403ed792c423f5c16d5ea3305f ditemukan informasi aktivitas transaksi dengan aplikasi *E-Wallet* Shopeepay ke-2 yang pernah dilakukan dengan id: 7866727, asset: BIDR, txId: 904d7618-44f4-4954-921d-d8055eed6ad5, jumlah: 49000, nama bank: Shopeepay(E-Wallet) dan timestamp: 1680754269436 seperti pada gambar 4.11.



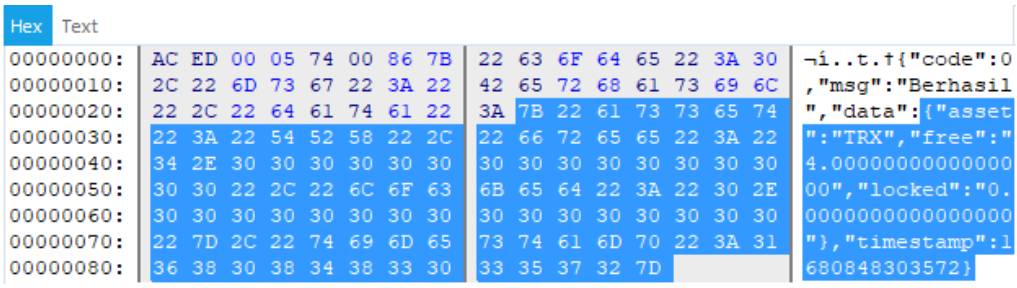
Gambar 4.11 Aktivitas transaksi dengan aplikasi E-Wallet Shopeepay ke-2

Pada file /data/data/com.binance.cloud.tokocrypto/cache/cache/data/e23f22dc4b293139f30e5e6d8a4aefac ditemukan informasi aktivitas transaksi dengan Bank Mandiri yang pernah dilakukan dengan id: 5075717, asset: BIDR, txId: 642eea2cd129d5cf26727908, jumlah: 191510, nama bank: Bank Mandiri, Bank Account No/Nomor Rekening: 161000xxxxxxx dan timestamp: 1680871497662 seperti pada gambar 4.12.



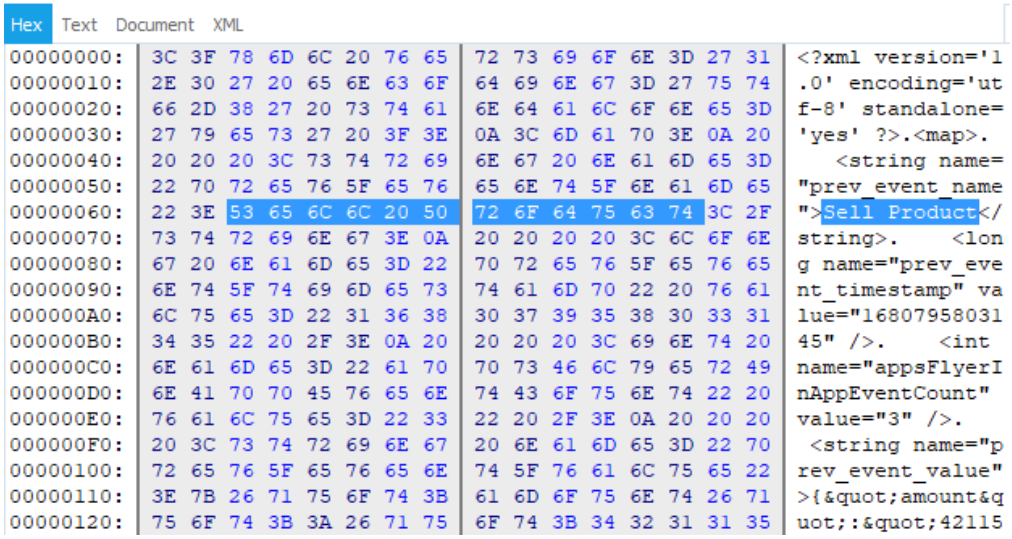
Gambar 4.12 Aktivitas Transaksi dengan Bank Mandiri

Pada file /data/data/com.binance.cloud.tokocrypto/cache/cache/data/fac471429f2b488385f87c4429601b26 ditemukan informasi aktivitas transaksi crypto yang pernah dilakukan dengan nama asset: TRX, jumlah: 4 dan timestamp: 1680848303572 seperti pada gambar 4.13.



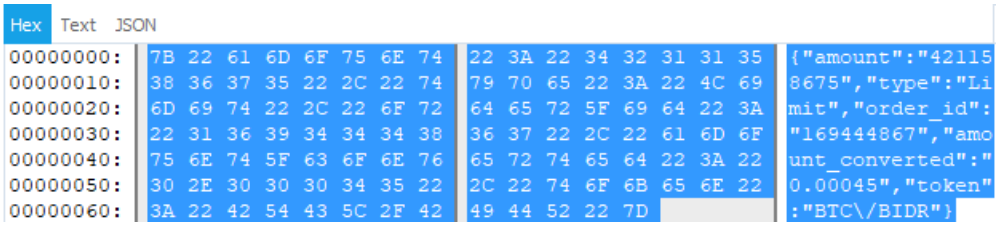
Gambar 4.13 Aktivitas Transaksi Crypto Yang Ditemukan

Pada file /data/data/com.binance.cloud.tokocrypto/shared_prefs/appsflyer-data.xml ditemukan informasi aktivitas transaksi Penjualan Crypto yang pernah dilakukan dengan timestamp: 1680795803145 seperti pada gambar 4.14.



Gambar 4.14 Aktivitas Transaksi Penjualan Crypto

Pada file /data/data/com.binance.cloud.tokocrypto/shared_prefs/appsflyer-data.xml dirubah ke bentuk XML maka didapatkan detail aktivitas transaksi penjualan crypto dengan token: BTC, jumlah: 0.00045



Gambar 4.15 Detail Aktivitas transaksi penjualan crypto

Pada tabel 4.2 di dibawah peneliti melakukan konversi waktu yang dari timestamp merubah ke waktu UTC kemudian merubah ke waktu UTC+8 karena penelitian dilakukan pada waktu indonesia bagian tengah (WITA).

Tabel 4.2 Rincian Aktivitas Transaksi Yang Ditemukan Pada Dompet Tokocrypto

No	Id Pemesanan	Txid	Waktu (UTC +8)	Jenis Transaksi	Jumlah	Keterangan
1	7866302	f30661e3732f49b0be43964d6a192425	1680746782000 (6/4/23 10:06)	-	49000 BIDR	Transaksi menggunakan Aplikasi Dana
2	7866310	5a80fad6-f083-47b7-a6ba-22c840350e6a	1680746962000 (6/4/23 10:09)	-	49000 BIDR	Transaksi menggunakan Aplikasi Gopay
3	7866384	566fabfb-cae7-42d3-9a97-45b8f3f5818b	1680747842000 (6/4/23 10:24)	-	49000 BIDR	Transaksi menggunakan Aplikasi Shopeepay ke-1
4	7866727	904d7618-44f4-4954-921d-d8055eed6ad5	1680753822000 (6/4/23 12:03)	-	49000 BIDR	Transaksi menggunakan Aplikasi Shopeepay ke-2
5	191510	642eea2cd129d5cf26727908	1680796058824 (6/4/23 23.47)	-	191510 BIDR	Transaksi dengan bank mandiri
6	-	-	1680848303572 (7/4/23 14.18)	-	4 TRX	[redacted]
7	169444867	-	1680795803145 (6/4/23 23.43)	Penjualan crypto	0.00045 BTC	-

4.6 *Presentation*

Tahapan ini akan menyajikan semua kegiatan yang dilakukan dari proses sebelumnya dalam presentasi hasil. Dari hasil analisis didapatkan artefak digital atau bukti digital aplikasi dompet *cryptourrency* pada perangkat *smartphone* redmi 6A menggunakan alat *oxygen forensics* yang menghasilkan file *physical image* dengan nama *Device.ewc* dan *mmcblk0*. Kemudian dua file tersebut dilakukan hashing menggunakan alat HashMyFiles yang menghasilkan nilai MD5 untuk file *Device.ewc* (8ac76a48e5b72948e38b1f95eb618245) dan file *mmcblk0* (b9e2fa2a6a20be3857e1aadb711d915d).

Kegiatan simulasi kasus, peneliti melakukan sepuluh aktivitas transaksi pada aplikasi dompet *cryptocurrency* tokocrypto pada perangkat smartphone redmi 6A. Pada proses analisis menggunakan alat *oxygen forensics*, peneliti berhasil memperoleh data aktivitas transaksi yang dilakukan pada aplikasi dompet *cryptocurrency* tokocrypto pada perangkat smartphone redmi 6A sejumlah tujuh aktivitas transaksi serta tiga aktivitas transaksi tidak ditemukan pada aplikasi dompet *cryptocurrency* tokocrypto. Dari tujuh aktivitas transaksi ada beberapa label yang tidak ada pada beberapa transaksi setelah dilihat dari simulasi kasus yang telah dilakukan yaitu:

1. Pada transaksi deposit dengan aplikasi E-Wallet Dana label yang tidak ada yaitu label jenis transaksi
2. Pada transaksi deposit dengan aplikasi E-Wallet Gopay label yang tidak ada yaitu label jenis transaksi
3. Pada transaksi deposit aplikasi E-Wallet Shopeepay ke-1 label yang tidak ada yaitu label jenis transaksi
4. Pada transaksi deposit aplikasi E-Wallet Shopeepay ke-2 label yang tidak ada yaitu label jenis transaksi
5. Pada transaksi penjualan crypto label yang tidak ada yaitu Txid dan untuk label Id Pemesanan pada simulasi kasus tidak ada sedangkan setelah analisis kasus label Id Pemesan ada
6. Pada transaksi penarikan crypto ke-2 label yang tidak ada yaitu label Id Pemesanan, Txid, Jenis Transaksi dan Alamat Dompet
7. Pada transaksi penarikan fiat label yang tidak ada yaitu jenis transaksi

Berikut hasil analisis aktivitas transaksi dengan rincian seperti pada tabel 4.3:

Tabel 4.3 Hasil Analisis Aktivitas Transaksi Yang Ditemukan Pada Aplikasi Dompet Tokocrypto

No.	**Aktivitas Transaksi**	**Id Pemesanan**	**Txid**	**Waktu**	**Jenis Transaksi**	**Jumlah**	**Alamat Dompet**
1	Transaksi Deposit Aplikasi Dana	✓	✓	✓	×	✓	[redacted]
2	Transaksi Deposit Aplikasi Gopay	✓	✓	✓	×	✓	
3	Transaksi Deposit Aplikasi Shopeepay 1	✓	✓	✓	×	✓	
4	Transaksi Deposit Aplikasi Shopeepay 2	✓	✓	✓	×	✓	
5	Transaksi Pembelian crypto	[redacted]	×	×	×	×	
6	Transaksi Penjualan crypto	✓	×	✓	✓	✓	
7	Transaksi Deposit Crypto	×	×	×	×	×	×
8	Penarikan Crypto Pertama	×	×	×	×	×	×
9	Penarikan Crypto Kedua	×	×	✓	×	✓	×
10	Penarikan Fiat	✓	✓	✓	×	✓	[redacted]

4.7 Analisa Hasil

Terdapat dua analisa hasil yang akan dibahas pada bagian ini yaitu analisa hasil individual dan analisa hasil kumulatif

4.7.1 Analisa Hasil Individual

1. Pada transaksi deposit dengan aplikasi E-Wallet Dana, terdapat kekurangan label yang tidak ada, yaitu label jenis transaksi. Ini menunjukkan bahwa dalam proses deposit menggunakan aplikasi E-Wallet Dana, label jenis transaksi tidak tercantum atau tidak diidentifikasi dengan jelas.
2. Pada transaksi deposit dengan aplikasi E-Wallet Gopay, terdapat kekurangan label yang tidak ada, yaitu label jenis transaksi. Sama seperti poin sebelumnya, ini mengindikasikan bahwa dalam transaksi deposit menggunakan aplikasi E-Wallet Gopay, informasi tentang jenis transaksi tidak tercatat.
3. Pada transaksi deposit aplikasi E-Wallet Shopeepay ke-1, terdapat label yang tidak ada, yaitu label jenis transaksi. Ini menunjukkan bahwa pada transaksi deposit pertama menggunakan aplikasi E-Wallet Shopeepay, jenis transaksi tidak diidentifikasi secara jelas.
4. Pada transaksi deposit aplikasi E-Wallet Shopeepay ke-2, terdapat label yang tidak ada, yaitu label jenis transaksi. Sama seperti poin sebelumnya, pada transaksi deposit kedua menggunakan aplikasi E-Wallet Shopeepay, jenis transaksi juga tidak tercantum.
5. Pada transaksi penjualan crypto, terdapat kekurangan label yang tidak ada, seperti Txid. Namun, setelah dilakukan analisis kasus, label Id Pemesanan ditemukan. Ini mengindikasikan bahwa ada kesalahan awal dalam mengidentifikasi label-label yang diperlukan dalam transaksi penjualan crypto, tetapi setelah dilakukan analisis lebih lanjut, beberapa label berhasil diidentifikasi.
6. Pada transaksi penarikan crypto ke-2, terdapat beberapa label yang tidak ada, termasuk label Id Pemesanan, Txid, Jenis Transaksi, dan Alamat Dompet. Hal ini menunjukkan bahwa pada transaksi penarikan crypto kedua, banyak label yang tidak diisi atau tidak teridentifikasi dengan benar, yang dapat mengakibatkan kurangnya informasi penting tentang transaksi tersebut.
7. Pada transaksi penarikan fiat, terdapat kekurangan label yang tidak ada, yaitu jenis transaksi. Ini mengindikasikan bahwa pada transaksi penarikan fiat, informasi tentang jenis transaksi tidak tercantum dengan jelas.

Secara keseluruhan, analisis menunjukkan bahwa terdapat masalah dalam pengelolaan label-label pada berbagai jenis transaksi. Beberapa label tidak terisi, tidak teridentifikasi, atau terlupakan, yang dapat mengakibatkan ketidakjelasan atau kekurangan informasi dalam proses transaksi tersebut. Hal ini dapat berdampak pada pemahaman dan pelacakan transaksi serta keakuratan data yang dikumpulkan.

4.7.2 Analisa Hasil Kumulatif

1. Konsistensi Label: Masalah yang paling mencolok adalah kurangnya konsistensi dalam penggunaan label pada berbagai jenis transaksi. Label seperti "jenis transaksi" dan "Txid" tampaknya menjadi informasi yang krusial dalam setiap jenis transaksi, namun seringkali label ini tidak tercantum atau tidak terisi dengan benar.
2. Ketidakjelasan Identifikasi: Label "jenis transaksi" tampaknya menjadi elemen yang sering terabaikan. Tanpa label ini, sulit untuk mengidentifikasi dengan jelas apakah transaksi adalah deposit, penarikan, atau penjualan. Ini dapat menyebabkan kebingungan dan kesulitan dalam melacak dan menganalisis data transaksi.
3. Analisis Kasus: Dalam beberapa kasus, ditemukan bahwa label-label yang awalnya tidak ada, seperti "Id Pemesanan", akhirnya ditemukan setelah analisis lebih lanjut. Ini menunjukkan bahwa analisis kasus yang mendalam dapat membantu mengidentifikasi label-label yang mungkin terlewatkan pada tahap awal. Namun, proses ini juga menekankan pentingnya perencanaan yang cermat sebelumnya untuk memastikan label-label yang relevan diidentifikasi dengan benar.
4. Dampak Pada Informasi: Kekurangan label-label ini dapat memiliki dampak serius pada akurasi dan kegunaan informasi yang terkait dengan transaksi. Tanpa label yang tepat, sulit untuk memahami dan menganalisis data dengan benar, yang dapat mempengaruhi pelacakan transaksi, pelaporan, dan pengambilan keputusan.

4.8 Kekurangan dan Kelebihan Solusi Penelitian

4.8.1 Kekurangan Penelitian

1. Keterbatasan dalam mengidentifikasi beberapa aktivitas transaksi yang tidak terdeteksi: Meskipun peneliti berhasil mendapatkan data aktivitas transaksi, terdapat tiga aktivitas transaksi yang tidak ditemukan pada aplikasi dompet cryptocurrency

Tokocrypto. Hal ini menunjukkan keterbatasan alat Oxygen Forensics dalam mengidentifikasi secara menyeluruh semua aktivitas transaksi yang terjadi.

2. Ketidaktersediaan label-label pada beberapa transaksi: Peneliti menemukan bahwa beberapa label penting seperti jenis transaksi, ID Pemesanan, Txid, dan alamat dompet tidak ada pada beberapa transaksi. Hal ini menyulitkan analisis dan pemahaman lebih lanjut tentang transaksi tersebut.

4.8.2 Kelebihan Penelitian

1. Memperoleh data aktivitas transaksi: Alat Oxygen Forensics berhasil memberikan data aktivitas transaksi yang dapat digunakan oleh peneliti. Hal ini dapat menjadi sumber informasi yang berharga dalam melakukan analisis terhadap kegiatan transaksi pada dompet cryptocurrency Tokocrypto.
2. Kemampuan dalam melakukan analisis forensik: Alat Oxygen Forensics memiliki kemampuan analisis forensik yang dapat membantu peneliti untuk memahami aktivitas transaksi secara lebih rinci. Dengan alat ini, peneliti dapat mengidentifikasi pola, tren, dan hubungan antara transaksi yang dapat digunakan dalam investigasi lebih lanjut.
3. Potensi pengembangan solusi: Meskipun terdapat kekurangan dalam hal ketidaktersediaan label penting pada beberapa transaksi, ini juga memberikan peluang bagi peneliti untuk mengembangkan solusi yang lebih baik. Dengan menyadari kekurangan tersebut, peneliti dapat merancang metode tambahan atau menggunakan alat lain untuk melengkapi dan memperoleh informasi yang hilang.
4. Penggunaan alat yang sudah teruji: Oxygen Forensics adalah alat forensik yang telah digunakan secara luas dan teruji keandalannya dalam analisis forensik digital. Dengan menggunakan alat yang terpercaya ini, peneliti dapat memiliki keyakinan bahwa data yang diperoleh dan analisis yang dilakukan memiliki tingkat keandalan yang tinggi.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan proses hasil dan pembahasan dari proses forensik dompet cryptocurrency tokocrypto, maka dapat ditarik kesimpulan yaitu:

1. Bahwa analisis artefak dompet digital cryptocurrency tokocrypto pada smartphone Xiaomi Redmi 6A, berhasil ditemukan informasi mengenai aktivitas transaksi. Dari sepuluh aktivitas transaksi yang dilakukan, berhasil diperoleh informasi tentang tujuh transaksi yang meliputi deposit fiat, penarikan fiat, penarikan crypto, dan penjualan crypto. Namun, beberapa label seperti jenis transaksi, Id Pemesanan, Txid, dan alamat dompet tidak tersedia pada beberapa transaksi. Informasi yang berhasil ditemukan memberikan gambaran tentang transaksi deposit fiat, penarikan fiat, penarikan crypto, dan penjualan crypto yang dilakukan.
2. Penelitian ini juga mengungkapkan kekurangan dalam bentuk label yang tidak tersedia pada beberapa transaksi, seperti jenis transaksi, Id Pemesanan, Txid, dan alamat dompet. Ini menyoroti pentingnya kerangka kerja ilmiah dalam analisis forensik digital untuk mengatasi tantangan semacam itu. Ketiadaan label-label ini menyebabkan tingkat detail dan kelengkapan informasi menjadi terbatas, dan ini mengakibatkan kesulitan dalam pemahaman yang lengkap mengenai aktivitas transaksi. Untuk memperoleh pemahaman yang lebih komprehensif dan akurat, disarankan untuk memiliki akses terhadap data yang lebih kaya, termasuk label-label transaksi yang relevan. Selain itu, pendekatan lintas disiplin yang mencakup penggunaan bukti metadata tambahan dari sumber eksternal dapat membantu dalam mengisi celah informasi dan memahami transaksi yang kurang lengkap.

5.2 Saran

Dalam penelitian ini masih ada keterbatasan karena masih menggunakan salah satu dompet *cryptocurrency* tokocrypto yang digunakan di Indonesia belum melibatkan dompet *cryptocurrency* tokocrypto lainnya dan alat forensik yang digunakan hanya *oxygen forensic.* Untuk peneliti selanjutnya dapat menggunakan dompet *cryptocurrency* lainnya, membandingkan beberapa artefak digital dompet *cryptocurrency* dan membandingkan alat forensik untuk mendapatkan artefak digital.

Daftar Pustaka

Azman, M., & Sharma, K. (2020). HCH DEX: A secure cryptocurrency e-Wallet exchange system with two-way authentication. *Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020*, *Icssit*, 305–310. https://doi.org/10.1109/ICSSIT48917.2020.9214122

Baek, H., Oh, J., Kim, C. Y., & Lee, K. (2019). A Model for Detecting Cryptocurrency Transactions with Discernible Purpose. *International Conference on Ubiquitous and Future Networks, ICUFN*, *2019-July*, 713–717. https://doi.org/10.1109/ICUFN.2019.8806126

Bappebti. (2023). Outlook Bappebti. *Bulletin Bappebti*, *242*, 10–30.

Bappebti. (2021). Bulletin Bappebti Pesona Komoditi Aset Kripto Edisi 226 April. *Bappebti*. http://bappebti.go.id/Bulletin_perdagangan_berjangka/download/bulletin_perdagangan_berjangka_1970_01_01_3embfzwu_id.pdf

Caloyannides, M. A., Memon, N., & Venema, W. (2009). Digital forensics. *IEEE Security and Privacy*, *7*(2), 16–17. https://doi.org/10.1109/MSP.2009.34

Chainalysis. (2022). *The 2022 Crypto Crime Report*. *February*, 1–140. https://go.chainalysis.com/2022-crypto-crime-report.html

Chang, S. E. (2019). Legal Status of Cryptocurrency in Indonesia and Legal Analysis of the Business Activities in Terms of Cryptocurrency. *Brawijaya Law Journal*, *6*(1), 76–93. https://doi.org/10.21776/ub.blj.2019.006.01.06

Dinas Penanaman Modal Dan Perizinan Terpadu Satu Pintu Provinsi Banten. (2022). *Jumlah Pedagang Aset Kripto Akan Terus Bertambah Ketika Industri Semakin Maju | Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu (DPMPTSP) Provinsi Banten*. https://dpmptsp.bantenprov.go.id/Berita/topic/1122

Disemadi, H. S., & Delvin, D. (2021). Kajian Praktik Money Laundering dan Tax Avoidance dalam Transaksi Cryptocurrency di Indonesia. *NUSANTARA : Jurnal Ilmu*

Pengetahuan Sosial, *8*(3), 326–340. http://jurnal.um-tapsel.ac.id/index.php/nusantara/article/view/3201

Fadillah, M. N., Umar, R., Yudhana, A., Studi, P., Informatika, M., Dahlan, U. A., Studi, P., Elektro, T., Dahlan, U. A., & Soepomo, J. P. (2022). *Analisis Forensik Aplikasi Dompet Digital Pada Smartphone Android Menggunakan Metode Dfrws*. *09*(02), 265–278.

Garfinkel, S., Farrell, P., Roussev, V., & Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. *Digital Investigation*, *6*(SUPPL.), 2–11. https://doi.org/10.1016/j.diin.2009.06.016

Hameed, S., & Farooq, S. (2016). The Art of Crypto Currencies. *International Journal of Advanced Computer Science and Applications*, *7*(12). https://doi.org/10.14569/ijacsa.2016.071255

Harwick, C. (2016). Cryptocurrency_and_the_problem.PDF. *Independent Reveiw*, *20*(4), 569–588.

Idrus. (2021). Halal Haram Cryptocurrency. *Al-Tasyree*, *01*(02), 113–123.

Kementerian Perdagangan. (2021). *Perdagangan Aset Kripto Di Indonesia*.

Khan, A. G., Zahid, A. H., Hussain, M., & Riaz, U. (2019). *And QR Code*. *Icic*.

Kirthika, B., Prabhu, S., & Visalakshi, S. (2015). Android Operating System A Review. *International Journal of Trend in Research and Development*, *2*(5), 260–264. www.ijtrd.com

Koerhuis, W., Kechadi, T., & Le-Khac, N. A. (2020). Forensic analysis of privacy-oriented cryptocurrencies. *Forensic Science International: Digital Investigation*, *33*(xxxx), 200891. https://doi.org/10.1016/j.fsidi.2019.200891

Ladita, P. (2020). Analisis Penerapan Aplikasi Android Tokocrypto Menggunakan Pendekatan Design Thinking Dibantu Dengan Platform Design Toolkit V.2. *Analisis Penerapan Aplikasi Android Tokocrypto Menggunakan Pendekatan Design Thinking Dibantu Dengan Platform Design Toolkit V.2* , 1–132.

Lero, A. R. S., Lero, J. B., & Gear, A. Le. (2019). Privacy and security analysis of cryptocurrency mobile applications. *2019 5th International Conference on Mobile and Secure Services, MOBISECSERV 2019*, *1*, 1–6. https://doi.org/10.1109/MOBISECSERV.2019.8686583

Madiyanto, S., Mubarok, H., & Widiyasono, N. (2017). Mobile Forensics Investigation Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS. *Jurnal Rekayasa Sistem & Industri (JRSI)*, *4*(01), 93–98. https://doi.org/10.25124/jrsi.v4i01.149

Maha Rani, D. A., Gede Sugiartha, I. N., & Sukaryati Karma, N. M. (2021). Uang Virtual (Cryptocurrency) Sebagai Sarana Tindak Pidana Pencucian Uang dalam Perdagangan Saham. *Jurnal Konstruksi Hukum*, *2*(1), 19–23. https://doi.org/10.22225/jkh.2.1.2961.19-23

Majed, H., Noura, H. N., & Chehab, A. (2020). Overview of Digital Forensics and Anti-Forensics Techniques. *8th International Symposium on Digital Forensics and Security, ISDFS 2020*. https://doi.org/10.1109/ISDFS49300.2020.9116399

Montanez, A. (2014). Investigation of Cryptocurrency Wallets on iOS and Android Mobile Devices for Potential Forensic Artifacts. *Department of Forensic Science, Marshall University*. http://www.marshall.edu/forensics/files/Montanez-Angelica_Final-Research-Paper.pdf

Periyadi, Mutiara, G. A., & Wijaya, R. (2017). Digital forensics random access memory using live technique based on network attacked. *2017 5th International Conference on Information and Communication Technology, ICoIC7 2017*, *0*(c). https://doi.org/10.1109/ICoICT.2017.8074695

Prasetya, A. Y., Subroto, A., & Nurish, A. (2021). Model Pendanaan Terorisme Melalui Media Cryptocurrency. *Journal of Terrorism Studies*, *3*(1). https://doi.org/10.7454/jts.v3i1.1030

Rafique, M., & Khan, M. N. A. (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools. *International Journal of Scientific & Engineering Research*, *4*(10), 1048–1056. http://www.ijser.org/researchpaper%5CExploring-Static-and-Live-Digital-Forensic-Methods-Practices-and-Tools.pdf

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

Riadi, I., Yudhana, A., Caesar, M., & Putra, F. (2018). 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. https://journal.maranatha.edu/index.php/jutisi/article/view/1490/1162

Sah, A., Riadi, I., & Prayudi, Y. (2018). Deteksi Bukti Digital Online Gambling Menggunakan Live Forensik Pada Smartphone Berbasis Android. In *Cyber Security dan Forensik Digital* (Vol. 1, Issue 1). https://doi.org/10.14421/csecurity.2018.1.1.1237

Sah, A., Riadi, I., & Prayudi, Y. (2018). Deteksi Bukti Digital Online Gambling Menggunakan Live Forensik Pada Smartphone Berbasis Android. *Cyber Security Dan Forensik Digital*, *1*(1), 14–19. https://doi.org/10.14421/csecurity.2018.1.1.1237

Şentürk, Ş., Apaydin, T., & Yaşar, H. (2020). Image and File System Support Framework for a Digital Mobile Forensics Software. *2020 Turkish National Software Engineering Symposium, UYMS 2020 - Proceedings*, 2020–2022. https://doi.org/10.1109/UYMS50627.2020.9247055

Sudyana, D. (2016). *Belajar Mengenali Forensika Digital*. *March 2016*, 130.

Taylor, S. K., Ariffin, A., Zainol Ariffin, K. A., & Sheikh Abdullah, S. N. H. (2021). Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets. *2021 3rd International Cyber Resilience Conference, CRC 2021*. https://doi.org/10.1109/CRC50527.2021.9392446

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

Van Der Horst, L., Choo, K. K. R., & Le-Khac, N. A. (2017). Process Memory Investigation of the Bitcoin Clients Electrum and Bitcoin Core. *IEEE Access*, *5*(c), 22385–22398. https://doi.org/10.1109/ACCESS.2017.2759766

Volety, T., Saini, S., McGhin, T., Liu, C. Z., & Choo, K. K. R. (2019). Cracking Bitcoin wallets: I want what you have in the wallets. *Future Generation Computer Systems*, *91*, 136–143. https://doi.org/10.1016/j.future.2018.08.029

Yadi, I. Z., & Kunang, Y. N. (2014). Analisis forensik pada platform android. *Konferensi Nasional Ilmu Komputer (KONIK)*, 141–148. http://eprints.binadarma.ac.id/2191/

Yazdinejad, A., HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Srivastava, G., & Chen, M. Y. (2020). Cryptocurrency malware hunting: A deep Recurrent Neural Network approach. *Applied Soft Computing Journal*, *96*, 106630. https://doi.org/10.1016/j.asoc.2020.106630

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

Zollner, S., Choo, K. K. R., & Le-Khac, N. A. (2019). An Automated Live Forensic and Postmortem Analysis Tool for Bitcoin on Windows Systems. *IEEE Access*, *7*, 158250–158263. https://doi.org/10.1109/ACCESS.2019.2948774