INVESTIGASI FORENSIK DIGITAL DAN ANALISIS ARTEFAK DAN JEJAK DIGITAL ASET KRIPTO PADA PLATFORM WINDOWS DAN ANDROID

SEMINAR BIDANG KAJIAN

IZAZI MUBAROK
99222007

PROGRAM DOKTOR TEKNOLOGI INFORMASI

UNIVERSITAS GUNADARMA

JUNI 2024

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Berdasarkan data statistik [Coinmarketcap charts, 2024], saat ini terdapat lebih dari 2,4 juta aset kripto dengan total nilai kapitalisasi pasar sebesar Rp39.949 Triliun. Aset kripto Bitcoin (BTC) memiliki total nilai kapitalisasi pasar tertinggi sebesar Rp21.840 Triliun dan total nilai perdagangan aset kripto dalam 24 jam terakhir mencapai Rp466 Triliun, sedangkan total nilai transaksi terbesar untuk perdagangan aset kripto dalam 24 jam terakhir dicapai oleh Tether (USDT) sebesar Rp970 Triliun sebagaimana Gambar 1.1.1 [Coinmarketcap charts, 2024]. Praktik perdagangan ini menarik perhatian para pelaku kriminal untuk menggunakan aset kripto dengan tujuan pencucian uang, pendanaan terorisme, dan pembelian barang ilegal di pasar *Darknet* [Europol, 2023]. Penelitian [Tziakouris, 2018] mengenai tantangan dan peluang bagi penegak hukum terkait perkembangan aset kripto telah menegaskan bahwa proliferasi aset kripto telah meningkatkan kekhawatiran mengenai penyalahgunaan aset kripto untuk kegiatan terlarang, mencakup pencucian uang, penghindaran pajak, pembelian barang dan jasa ilegal di *Darkweb*, dan pembayaran serangan *ransomware*.

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply
1	Bitcoin BTC	Rp1,1...20.96	0.88%	1.55%	4.08%	Rp 21,840,035,754,189,512	Rp 466,040,996,089,494 422,971 BTC	19,711,209 BTC
2	Ethereum ETH	Rp57,...72.04	0.96%	1.02%	6.42%	Rp 6,960,174,860,714,452	Rp 244,762,815,781,354 4,255,844 ETH	120,154,301 ETH
3	Tether USDT	Rp16,300.26	0.03%	0.06%	0.06%	Rp 1,833,718,602,984,780	Rp 970,868,752,304,032 59,561,933,702 USDT	112,496,265,357 USDT
4	BNB BNB	Rp10,...08.38	0.65%	0.98%	11.59%	Rp 1,484,759,169,006,090	Rp 36,330,289,418,124 3,623,469 BNB	147,584,384 BNB
5	Solana SOL	Rp2,4...80.98	0.66%	0.60%	11.83%	Rp 1,151,251,224,874,455	Rp 40,175,060,054,133 16,197,648 SOL	461,556,349 SOL

Gambar 1.1.1 Kapitalisasi Pasar Aset Kripto Per 12 Juni 2024
Sumber: [Coinmarketcap charts, 2024]

Berbagai jenis dompet kripto telah dirancang untuk menyediakan penyimpanan aset kripto yang aman. Namun demikian, dompet kripto tersebut dapat dieksploitasi oleh individu untuk mencari anonimitas dalam transaksi keuangan mereka. Penyalahgunaan ini menimbulkan tantangan bagi Institusi Penegak Hukum dan Badan Pengawas Perdagangan Aset Kripto dalam memantau dan mencegah kegiatan ilegal [Dyson et al., 2018]. Menurut laporan [ACFE, 2024], terdapat sekitar 76 kasus *fraud* atau sebesar 4% dari 1.921 *fraud* global yang disurvei pada tahun 2023 melibatkan penggunaan aset kripto. Hampir setengah dari kasus tersebut (47%) melibatkan pelaku untuk mengubah aset curiannya menjadi aset kripto, sebesar 33% melibatkan suap atau pembayaran suap kepada rekan konspirator dalam bentuk aset kripto, dan sebesar 29% digunakan untuk pencucian uang hasil *fraud* dengan memanfaatkan aset kripto.

Munculnya aset kripto selama puluhan tahun terakhir telah mendorong para peneliti untuk melakukan penelitian terkait aspek privasi teknologi kripto tersebut. Adanya dampak peningkatan aktivitas ilegal pada aset kripto karena sifatnya yang terdesentralisasi dan penggunaan nama anonim, menimbulkan tantangan baru dalam melacak sumber dana terkait pencucian uang, transaksi *darknet*, serangan *ransomware*, penghindaran pajak, dan penipuan. Hal ini juga yang menyebabkan peningkatan penelitian terkait pendekatan investigasi forensik digitalterhadap pelaku kejahatan yeng melibatkan aset kripto [Dudani et al., 2023].

Terdapat beberapa penelitian yang sudah dilakukan terkait investigasi forensik digital dan analisis terhadap beberapa aset kripto yang tersimpan dalam beberapa jenis dompet kripto pada perangkat komputer Windows dan perangkat seluler Android. Penelitian yang dilakukan oleh [Debono et al, 2024], [Van der Horst et al., 2017], [Zollner et al., 2019], [Thomas, 2020], [Doran, 2015], [Ngwu et al., 2021], dan [Jones, 2014] berfokus pada investigasi forensik digital dan analisis dompet kripto pada perangkat komputer Windows. Penelitian yang dilakukan oleh [Adhar, 2023], [Mirza et al, 2022], [Chang et al., 2022], [Nabi, 2014], [Montanez, 2014] berfokus pada aplikasi dompet kripto pada perangkat seluler Android. Selain itu, terdapat penelitian terkait investigasi dan analisis aset kripto yang terpasang di

perangkat Linux Ubuntu seperti yang dikerjakan oleh [Koerhuis et al., 2020], [Shi et al., 2023], dan [Kovalcik, 2022].

Dari beberapa penelitian tersebut, sebagian besar hanya melakukan investigasi dan analisis terhadap dompet kripto dalam kondisi standar atau normal meliputi instalasi awal di perangkat, pembuatan akun aset kripto, dan aktivitas transaksi aset kripto. Namun demikian, terdapat empat penelitian oleh [Debono et al, 2024], [Mirza et al, 2022], [Montanez, 2014] dan [Ngwu et al., 2021] yang juga melakukan pemeriksaan dan analisis terhadap jejak digital yang masih tersisa di perangkat setelah dompet kripto dilakukan penghapusan. Penelitian tersebut dapat membantu para penegak hukum maupun investigator dalam menghadapi kemungkinan penghapusan dompet kripto saat penanganan kasus kriminal maupun *fraud*. Sebagaimana menurut laporan [ACFE, 2024], bahwa sebesar 89% dari 1.921 kasus *fraud* melibatkan upaya penyembunyian yang antara lain sebesar 19% dengan melakukan penghapusan data elektronik atau *file*.

Meskipun empat penelitian sudah dilakukan untuk menganalisis artefak dan jejak digital dari dompet kripto yang sudah dihapus, hasil penelitian mereka belum menuangkan keseluruhan artefak maupun jejak digital yang potensial seperti *Windows Registry*, *$Recycle.BIN*, dan *Unallocated area*. Selain itu, masih terdapat kekurangan atau kesenjangan dari penelitian-penelitian sebelumnya yang terkait dengan investigasi forensik digital dan analisis terhadap aset kripto, yaitu:

1) Penelitian untuk perangkat komputer Windows baru dilakukan pada versi Windows 7 dan 10 serta penelitian untuk perangkat Android baru dilakukan pada versi Android 4.2.2, 8.0, 8.1.0, dan versi 10.0,
2) Metode akuisisi dompet kripto yang digunakan oleh [Debono et al, 2024] dan [Ngwu et al., 2021] yaitu akuisisi memori RAM melalui memori *virtual machine* dan akuisisi *disk* komputer dengan mengkonversi *disk virtual machine* menjadi *image file* (format forensik) sehingga tidak mencerminkan metode akuisisi yang umumnya bisa dilakukan terhadap sebuah perangkat komputer sesuai dengan kondisi riil di lapangan saat

penanganan kasus atau insiden. Selain itu, beberapa peralatan untuk menangkap memori maupun paket lalu lintas jaringan juga sudah dipasang terlebih dahulu sebelum dilakukan akuisisi padahal dalam praktik yang umum tidak atau jarang ditemukan.

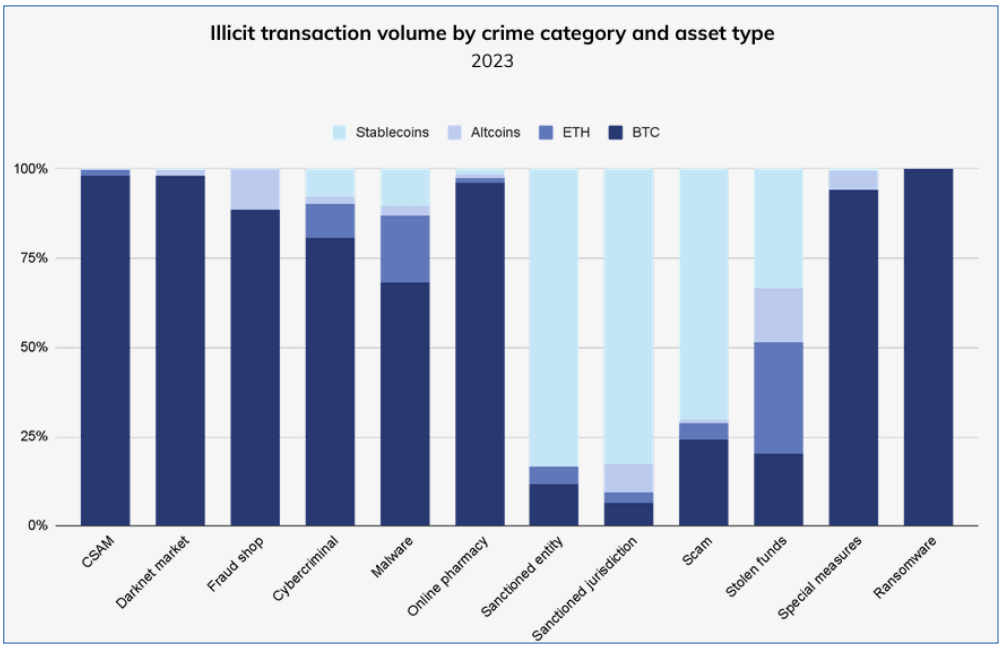
3) Metode akuisisi dompet kripto yang digunakan oleh [Mirza et al, 2022] menggunakan akuisisi secara fisik dengan melakukan *rooting* terlebih dahulu pada perangkat yang dapat menimbulkan isu baru terkait dugaan perusakan perangkat maupun permasalahan integritas data, sedangkan metode akuisisi dompet kripto yang digunakan oleh [Montanez, 2014] menggunakan *adb backup* pada android emulator, dan menggunakan *adb pull* untuk ekstraksi data aplikasi yang sudah dihapus yang memungkinkan tidak akan memperoleh jejak digital lain apabila data aplikasinya juga turut dihapus.
4) Belum ada penelitian yang memberikan analisis komparasi secara komprehensif atas artefak atau jejak digital dompet kripto baik yang kustodian maupun non-kustodian yang terpasang atau digunakan pada perangkat Windows dan perangkat Android.

Mempertimbangkan adanya kekurangan atau kesenjangan tersebut dan perlunya kebutuhan penelitian untuk memberikan pengetahuan (*knowledge*) maupun temuan baru atas penelitian pada bidang investigasi aset kripto ini, maka Penulis akan melakukan penelitian investigasi forensik digital dan analisis artefak dan jejak digital aset kripto pada platform Windows dan Android yang berfokus pada platform sistem operasi yang terbaru (Windows 11 dan Android 11/12), metode forensik digital yang sesuai dengan praktik saat penanganan riil di lapangan dengan menggunakan simulasi penghapusan aplikasi, serta menggunakan 5 dompet kripto non-kustodian dan 5 dompet kustodian dengan jenis aset kripto Bitcoin (BTC) dan Tether (USDT) yang memiliki nilai transaksi perdagangan tertinggi dalam 24 jam terakhir [Coinmarketcap charts, 2024].

1.2 Batasan dan Tujuan

Dalam melakukan penelitian ini, penulis membuat batasan sebagai berikut:

1) Jenis aset kripto yang digunakan dalam penelitian yaitu Bitcoin (BTC) dan Tether (USDT). Bitcoin dan Tether dipilih karena mempunyai volume transaksi paling besar pada saat penelitian dilakukan [Coinmarketcap charts, 2024]. Selain itu, Bitcoin (BTC) dan Tether (USDT) merupakan jenis aset kripto yang paling banyak digunakan dalam kejahatan [Chainalysis, 2024] sebagaimana Gambar 1.2.1.
2) Perangkat yang digunakan berbasis sistem operasi Windows 11 dan Android 11/12.



Gambar 1.2.1 Volume Transaksi Yang Dilarang Berdasarkan Kategori Kejahatan dan Jenis Aset Kripto

Sumber: [Chainalysis, 2024]

3) Jenis dompet kripto yang digunakan dalam penelitian ini dibatasi untuk yang beroperasi di sistem operasi Windows 11 dan Android 11/12. Penulis menggunakan 10 dompet kripto yang terdiri dari 5 dompet kripto non-kustodian dalam bentuk aplikasi *desktop* pada Windows 11 dan aplikasi

Android 11/12 serta 5 dompet kripto kustodian dalam bentuk *web browser* pada windows 11 dan aplikasi Android 11/12. Pemilihan 10 dompet kripto tersebut untuk mendapatkan hasil penelitian yang komprehensif dalam memberikan kontibusi atas beberapa kekurangan dari penelitian terdahulu. Tabel 1.2.1 menggambarkan daftar dompet kripto yang tersedia untuk platform Windows sekaligus platform Android dengan jumlah unduhan di platform Android dan status non-kustodian atau kustodian.

Tabel 1.2.1 Daftar dompet kripto platform Windows dan Android

No	Nama Dompet	Windows		Android		Status
		Browser	*Desktop*	Reviu	Unduhan	
1	Bitcoin Wallet	Tidak	Tersedia	4.3 dari 31 ribu	5 juta	non-kustodian
2	Exodus	Tersedia	Tersedia	4.4 dari 109 ribu	1 juta	non-kustodian
3	Coinomi	Tidak	Tersedia	4.4 dari 40 ribu	1 juta	non-kustodian
4	Electrum	Tidak	Tersedia	4.1 dari 3 ribu	1 juta	non-kustodian
5	Bither	Tidak	Tersedia	4.0 dari 351	50 ribu	non-kustodian
6	Luno	Tersedia	Tidak	3.6 dari 118 ribu	10 juta	kustodian
7	Indodax	Tersedia	Tidak	4.8 dari 166 ribu	5 juta	kustodian
8	Tokocrypto	Tersedia	Tidak	3.7 dari 50 ribu	1 juta	kustodian
9	Reku	Tersedia	Tidak	4.7 dari 33 ribu	500 ribu	Kustodian
10	Digitale xchange.id	Tersedia	Tidak	-	100 ribu	kustodian

4) Artefak dan jejak digital yang dicari yaitu pada memori, *browser*, direktori file (*disk*), jaringan, *email*, *registry*, maupun *$Recycle.BIN* dan/atau *unallocated area* sesuai dengan hasil tinjauan literatur sebagaimana Tabel 1.2.2.

Dari uraian latar belakang penelitian ini, penulis merumuskan beberapa permasalahan yaitu:

1) Bagaimana metode investigasi forensik digital yang komprehensif untuk menemukan artefak dan jejak digital aset kripto Bitcoin (BTC) dan Tether (USDT) pada 5 dompet kripto non-kustodian dalam bentuk aplikasi *desktop* pada Windows 11 dan aplikasi Android 11/12 serta 5 dompet kripto kustodian dalam bentuk *web browser* pada windows 11 dan aplikasi Android 11/12 sesuai Tabel 1.2.1?

Tabel 1.2.2 Hasil Artefak Penelitian Terdahulu

No.	Penelitian	Memori	*Browser*	Direktori File	Jaringan	*Email*	*Registry*	*$Recycle.Bin*	*Unallocated Space*
1	[Debono et al, 2024]	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
2	[Adhar, 2023]	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
3	[Mirza et al, 2022]	Tidak	Ya	Ya	Tidak	Ya	Tidak	Tidak	Ya
4	[Chang et al., 2022]	Tidak	Ya	Ya	Tidak	Ya	Tidak	Tidak	Tidak
5	[Koerhuis et al., 2020]	Ya	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak
6	[Nabi, 2014]	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
7	[Montanez, 2014]	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak	Tidak
8	[Van Horst et al., 2017]	Ya	Tidak	Ya	Tidak	Tidak	Ya	Tidak	Tidak
9	[Shi et al., 2023]	Tidak	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
10	[Zollner et al., 2019]	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
11	[Kovalcik, 2022]	Tidak	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
12	[Thomas, 2020]	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
13	[Doran, 2015]	Ya	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
14	[Ngwu et al., 2021]	Y	Tidak	Ya	Tidak	Tidak	Tidak	Tidak	Tidak
15	[Jones, 2014]	Ya	Ya	Ya	Tidak	Tidak	Tidak	Tidak	Tidak

2) Informasi apa saja terkait aset kripto Bitcoin (BTC) dan Tether (USDT) yang dihasilkan dari analisis terhadap artefak memori, *browser*, direktori file (*disk*), jaringan, *email*, *registry*, maupun *$Recycle.BIN* dan/atau *unallocated area* pada 5 dompet kripto non-kustodian dalam bentuk aplikasi *desktop* pada Windows 11 dan aplikasi Android 11/12 serta dan 5 dompet kripto kustodian dalam bentuk *web browser* pada windows 11 dan aplikasi Android 11/12*?*
3) Apakah masih terdapat jejak digital terkait aset kripto Bitcoin (BTC) dan Tether (USDT) yang tersisa pada perangkat Windows 11 dan aplikasi Android 11/12 setelah 10 dompet kripto tersebut dihapus? Jika iya, mengapa?
4) Bagaimana komparasi maupun keterhubungan artefak dan/atau jejak digital untuk tiap dompet kripto yang dipasang/diakses pada platform Windows dan Android?
5) Dari informasi terkait aset kripto Bitcoin (BTC) dan Tether (USDT) yang dihasilkan artefak memori, *browser*, direktori file (*disk*), jaringan, *email*, *registry*, maupun *$Recycle.BIN* dan/atau *unallocated area* pada setiap dompet

kripto, bagaimana pemanfaatan informasinya dan apakah dapat diperoleh jaringan transaksi aset kripto dengan menggunakan analisis sumber terbuka?

Tujuan penelitian yang diharapkan yaitu:

1) Untuk menggali artefak dan jejak digital dari pada 5 dompet kripto non-kustodian dalam bentuk aplikasi *desktop* pada Windows 11 dan aplikasi Android 11/12 serta 5 dompet kripto kustodian dalam bentuk *web browser* pada windows 11 dan aplikasi Android 11/12,
2) Untuk menggali Informasi apa saja terkait aset kripto Bitcoin (BTC) dan Tether (USDT) dari artefak memori, *browser*, direktori file (*disk*), jaringan, *email*, *registry*, maupun *$Recycle.BIN* dan/atau *unallocated area* pada 5 dompet kripto non-kustodian dalam bentuk aplikasi *desktop* pada Windows 11 dan aplikasi Android 11/12 serta dan 5 dompet kripto kustodian dalam bentuk *web browser* pada windows 11 dan aplikasi Android 11/12,
3) Untuk mengetahui apakah masih terdapat jejak digital terkait aset kripto Bitcoin (BTC) dan Tether (USDT) yang tersisa pada perangkat Windows 11 dan aplikasi Android 11/12 setelah 10 dompet kripto tersebut dihapus.
4) Untuk mendapatkan hasil komparasi maupun keterhubungan artefak dan/atau jejak digital untuk tiap dompet kripto yang dipasang/diakses pada platform Windows dan Android untuk penelitian lebih lanjut.
5) Untuk mendapatkan hasil analisis jaringan transaksi aset kripto Bitcoin (BTC) dan Tether (USDT) yang dapat ditemukan dari 10 dompet kripto.

1.3 Kontribusi

Penelitian ini setidaknya memberikan beberapa kontribusi sebagai berikut:

1) Penulis menyajikan metode forensik digital yang komprehensif untuk melakukan investigasi dan analisis terhadap artefak memori, *browser*, direktori file (*disk*), jaringan, email, *registry*, maupun *$Recycle.BIN* dan/atau *unallocated area* dari *disk* untuk lima aplikasi dompet desktop kripto Bitcoin Core, Exodus, Coinomi, Electrum, dan Bither serta untuk lima aplikasi dompet kripto berbasis web Luno, Indodax, Tokocrypto, Reku, dan digitalexchange.id

yang dipasang dan/atau diakses pada perangkat Windows 11.

2) Penulis menyajikan metode forensik digital yang komprehensif untuk melakukan investigasi dan analisis terhadap artefak yang dibuat oleh 10 aplikasi dompet kripto Bitcoin Wallet/Core, Exodus, Coinomi, Electrum, Bither, Luno, Indodax, Tokocrypto, Reku, dan digitalexchange.id yang dipasang pada perangkat Android 11/12.
3) Penulis menyajikan analisis informasi yang dapat diambil dari artefak yang dibuat oleh 10 dompet kripto Bitcoin Wallet/Core, Exodus, Coinomi, Electrum, Bither, Luno, Indodax, Tokocrypto, Reku, dan digitalexchange.id selama fase yang berbeda, meliputi pasca instalasi dompet kripto, pembuatan akun dompet kripto, dan melakukan transaksi antar dompet kripto, termasuk menyajikan informasi jejak digital yang tersisa pada perangkat Windows 11 maupun Android 11/12 setelah domplet kripto tersebut dilakukan penghapusan yang menyimulasikan skenario kriminal pada umumnya.
4) Penulis menyajikan analisis komparasi maupun keterhubungan artefak dan/atau jejak digital untuk tiap dompet kripto yang dipasang/diakses pada platform Windows dan Android.
5) Penulis menyajikan jaringan transaksi aset kripto Bitcoin (BTC) dan Tether (USDT) yang dapat ditemukan dari 10 dompet kripto.

BAB 2
TINJAUAN PUSTAKA

2.1 Investigasi Forensik Digital Dompet Kripto pada Komputer

[Debono et al., 2024] telah melakukan investigasi dan analisis pada tiga aplikasi dompet kripto yaitu Exodus, Electrum and Bitcoin Core yang dipasang pada komputer dengan sistem operasi Windows. Penelitian dilakukan untuk melihat artefak dan jejak aplikasi dompet kripto pada fase saat aplikasi diunduh dan dipasang, saat pembuatan akun dan digunakan untuk transaksi, dan setelah dihapus dari komputer. Hasil penelitian menunjukkan jejak informasi terkait aplikasi pada browser komputer, memori, dan pada direktori aplikasi di sistem Windows. Sama seperti penelitian yang dilakukan oleh [Van Der Horst et al., 2017] pada dompet kripto berbasis Windows dengan melakukan analisis memori untuk mengidentifikasi ID transaksi/hash di sistem operasi Windows.

[Koerhuis et al., 2020] melakukan investigasi forensik dompet kripto berbasis desktop yang didedikasikan khusus untuk aplikasi perangkat lunak Monero dan Verge. Dengan menggunakan sistem operasi Ubuntu dan MacOS High Sierra, penulis menganalisis serangkaian *snapshot* yang diambil selama berbagai tahapan metodologi mereka. Pengambilan dan analisis lalu lintas jaringan melalui *wireshark*, analisis gambar memori volatil, dan analisis disk.

[Zollner et al., 2019] melakukan penelitian pada dompet kripto dalam bentuk aplikasi yang dipasang dalam komputer Windows dan juga dalam bentuk *website*. Penulis melakukan pemasangan beberapa dompet aset kripto dan melakukan pendaftaran beberapa akun dompet kripto. Analisis aset kripto dilakukan dengan menggunakan *open source* untuk melihat artefak yang tersimpan dalam *random access memory* (RAM), *browser* dan data di *file system.*

[Kovalcik, 2022] membuat alat pemindaian untuk analisis forensik artefak dompet kripto berdasarkan sistem operasi Linux. Penulis memanfaatkan Python 3.8 di Ubuntu 20.04 untuk memperoleh berbagai informasi dari dua dompet berbeda,

yaitu Exodus dan Electrum. Sepanjang temuannya, penulis menjelaskan perbedaan kedua aplikasi satu sama lain.

[Doran, 2015] melakukan penelitian investigasi forensik digital pada komputer Windows yang berfokus pada investigasi memory aset kripto Multibit dan Bitcoin-Qt. Sedangkan penelitian oleh [Ngwu et al., 2021] menyelidiki dan membandingkan enam dompet *desktop* berbeda dalam metodologinya. Dompet yang digunakan adalah MultiBit HD, Electrum, mSIGNA, Bither, Armory dan Bitpay. Penelitian ini menggunakan alat digital "*OS Forensics Tool*" dan "*Magnet RAM capture*".

Terakhir, penelitian yang dilakukan oleh [Jones, 2014] berfokus pada dompet kripto bitcoin versi *web* blockchain.com dan dompet kripto Bitcoin versi aplikasi desktop MultiBit v0.5.17 yang berjalan pada sistem operasi Windows. Penelitian dilakukan dengan berfokus pada penggalian informasi melalui akuisisi RAM dan *disk* perangkat.

2.2 Investigasi Forensik Digital Aplikasi Dompet Kripto pada Telepon Seluler

[Adhar, 2023] melakukan investigasi forensik terhadap salah satu aplikasi dompet kripto yang legal di negara Indonesia yaitu aplikasi dompet kripto tokocrypto. Penelitian ini berfokus pada penemuan artefak digital dompet kripto tokocrypto dari perangkat *smartphone*. Hasil analisis menunjukkan bahwa dari sepuluh aktivitas transaksi yang diamati, informasi mengenai tujuh transaksi telah berhasil ditemukan, termasuk deposit fiat, penarikan fiat, penarikan aset kripto, dan penjualan aset kripto. Namun, beberapa label transaksi seperti jenis transaksi, Id Pemesanan, Txid, dan alamat dompet tidak tersedia pada beberapa transaksi.

[Mirza et al., 2022] melakukan investigasi dan analisis pada dompet aset kripto Web3 yang populer yang tidak memerlukan pengenal pribadi untuk mendaftar yaitu Trust Wallet dan Metamask yang dipasang pada perangkat Android dan iOS. Penelitian dilakukan untuk melihat artefak dan jejak aplikasi dompet aset kripto yang dapat dipulihkan. Hasil penelitian menunjukkan jejak informasi terkait

aplikasi pada direktori file di Android dan iOs.

[Chang et al., 2022] melakukan investigasi dan analisis pada tiga aplikasi dompet aset kripto yaitu Coinomi, Coinbase, dan Atomic yang dipasang pada perangkat seluler dengan sistem operasi Android. Penelitian dilakukan untuk menutupi kesenjangan penelitian sebelumnya yang belum melihat artefak dan jejak transaksi pada *web cookies*, dan protokol *OAuth 2.0* dari aplikasi dompet aset kripto Bitcoin dan Degecoins. Hasil penelitian menunjukkan jejak informasi terkait transaksi, alamat email, informasi pada *web cookies* dan protokol OAuth.

Dalam disertasi yang dibuat oleh [Nabi, 2018], dijelaskan berbagai fitur dari 3 (tiga) jenis dompet kripto yang berbeda untuk mempertimbangkan aspek teknis dan teoritis pada perangkat Android. Secara khusus, penulis mengulas aplikasi dompet Android Coinbase. Sedangkan [Montanez, A., 2014] melakukan penelitian pada aplikasi dompet kripto untuk aset kripto Bitcoin, Litecoin, dan Darkcoin pada perangkat seluler iOS dan Android

2.3 Investigasi Forensik Digital Perangkat Keras Dompet Kripto

[Thomas et al., 2020] melakukan forensik memori pada dompet kripto perangkat keras dengan terlebih dahulu mengunduh klien desktop LIDGer Live dan ada perangkat Windows bersamaan dengan pemasangan dompet Trezor.

2.4 Perbandingan Tinjauan

Dari penelitian terdahulu, dapat diketahui komparasi jenis aset kripto yang digunakan dalam transaksi, berbagai jenis dompet kripto, dan platform penyimpanan aset kripto yang digunakan sebagaimana Tabel 2.4.1.

Tabel 2.4.1 Perbandingan Jenis, Dompet, dan Platform Penyimpanan Aset Kripto

No.	Penelitian	Jenis Kripto	Dompet Kripto	Platform
1	[Debono et al, 2024]	Bitcoin	Exodus, Electrum dan Bitcoin Core	Komputer Windows 10 menggunakan 3 *Virtual Machine*

2	[Adhar, 2023]	Bitcoin	Tokocrypto	Android Redmi 6A versi 8.1.0
3	[Mirza et al, 2022]	Binance Coin, Etherum, NFT	Metamask dan Trust Wallet	Android Samsung M20 dan iOS Iphone 6s
4	[Chang et al., 2022]	Bitcoin dan Dogecoin	Coinomi, Coinbase, dan Atomic	Android Samsung S9+
5	[Koerhuis et al., 2020]	Monero dan Verge	Monero dan Verge	Komputer MacOS High Sierra menggunakan *Virtual Machine* Ubuntu
6	[Nabi, 2014]	Tidak ada	Ethereum, CoinBlesk, BurstCoin, Enjin, Blokchain, Coinbase,	Android
7	[Montanez, 2014]	Bitcoin, Litecoin dan Darkcoin	bitWallet, Coin Pocket, Bitcoin Wallet, Hive, Litecoin Wallet, Darkcoin Wallet	Android Samsung Galaxy S4, iOS iPhone 4, *Virtual Android Device*
8	[Van der Horst et al., 2017]	Bitcoin	Bitcoin Core dan electrum	Komputer Windows 7 menggunakan *Virtual Machine*
9	[Shi et al., 2023]	Tidak ada	253 aplikasi dompet kripto	Komputer Ubuntu Linux dan 2 Android *emulator*
10	[Zollner et al., 2019]	Tidak ada	Aplikasi (Armory, MultibitHD, Electrum, mSIGNA, BitPay, Bither, BitcoinCore, BitcoinKnots); Web (https://blockchain.info/, https://www.bitgo.com/, https://coin.space/, https://greenaddress.it/, https://coinapult.com/,	Komputer Windows 7 dan Windows 10 menggunakan *Virtual Machine*

			https://www.coinbase.com/, and https://xapo.com)	
11	[Kovalcik, 2022]	Bitcoin	Exodus dan Electrum	Komputer Linux Ubuntu
12	[Thomas, 2020]	Bitcoin dan Ethereum	Ledger Nano X (Ledger Live) dan Trezor One (Trezor Wallet)	Komputer Windows 7 menggunakan *Virtual Machine*
13	[Doran, 2015]	Bitcoin	Multibit dan Bitcoin-Qt	Komputer Windows 7
14	[Ngwu et al., 2021]	Bitcoin	MultiBit HD, Electrum, mSIGNA, Bither, Armory dan Bitpay	Komputer Windows 10 menggunakan *Virtual Machine*
15	[Jones, 2014]	Bitcoin	*web* blockchain.com dan aplikasi desktop MultiBit v0.5.17	Komputer Windows 7

Dalam melakukan penelitian, para penulis menggunakan skenario untuk mendapatkan hasil yang diharapkan. Tabel 2.4.2 menggambarkan perbandingan rancangan skenario pengujian investigasi forensik digital yang digunakan oleh para penulis.

Tabel 2.4.2 Perbandingan Rancangan Skenario Investigasi Forensik Digital

No.	Penelitian	Instalasi Dompet Kripto	Pembuatan Akun Aset Kripto	Transaksi Aset Kripto	Penghapusan Dompet Kripto
1	[Debono et al, 2024]	Ya	Ya	Ya	Ya
2	[Adhar, 2023]	Ya	Ya	Ya	Tidak
3	[Mirza et al, 2022]	Ya	Ya	Ya	Ya
4	[Chang et al., 2022]	Ya	Ya	Ya	Tidak
5	[Koerhuis et al., 2020]	Y	Ya	Ya	Tidak
6	[Nabi, 2014]	Tidak	Tidak	Tidak	Tidak
7	[Montanez, 2014]	Ya	Ya	Ya	Ya

8	[Van der Horst et al., 2017]	Ya	Ya	Ya	Tidak
9	[Shi et al., 2023]	Ya	Tidak	Tidak	Tidak
10	[Zollner et al., 2019]	Ya	Ya	Tidak	Tidak
11	[Kovalcik, 2022]	Ya	Ya	Ya	Tidak
12	[Thomas, 2020]	Ya	Ya	Ya	Tidak
13	[Doran, 2015]	Ya	Ya	Ya	Tidak
14	[Ngwu et al., 2021]	Ya	Ya	Ya	Ya
15	[Jones, 2014]	Ya	Ya	Ya	Tidak

Hasil perbandingan atas desain penelitian, kerangka kerja, peralatan, serta metode forensik digital dapat dilihat pada Tabel 2.4.3.

Tabel 2.4.3 Perbandingan Desain Penelitian, Peralatan, Peralatan dan Metode

No.	Penelitian	Desain Penelitian	Kerangka Kerja	Peralatan	Metode
1	[Debono et al, 2024]	Simulasi investigasi dengan 4 fase (fase persiapan sistem, fase instalasi aplikasi ketiga dompet sekaligus peralatan forensik, fase pembuatan akun dan aktivitas transaksi, serta fase penghapusan aplikasi.	Tidak mengacu ke kerangka kerja tertentu. Hanya melakukan akuisisi dan analisis.	Wireshark, Browser History Examiner, Magnet RAM Capture, FTK Imager, Magnet Axiom, Autopsy	*Live forensics*: akuisisi paket jaringan, data *browser*, RAM, dan *virtual machine* secara fisik
2	[Adhar, 2023]	Persiapan sistem, simulasi kasus, investigasi, dan laporan	*Digital Forensic Research Workshop* (DFRWS) [Fadillah et al., 2022]	Oxygen Forensics Detective	*Live forensics*: akuisisi secara fisik (*root*)
3	[Mirza et al, 2022]	Persiapan sistem, populasi data dengan skenario, akuisisi data, pemeriksaan forensik,	*National Institute of Standards and*	Perangkat lunas untuk *Root/Jailbreak*, Magnet	*Live forensics*: akuisisi secara fisik

		analisis dengan OSINT	*Technology* (NIST), publikasi 800-101	Axiom, Autopsy, Exiftool	(*root/ jailbreak*)
4	[Chang et al., 2022]	Persiapan sistem, ekstraksi data, identifikasi, dan analisis	Tidak mengacu ke kerangka kerja tertentu. Hanya melakukan akuisisi dan analisis.	Cellebrite UFED touch, Cellebrite Physical Analyzer, Ciphertrace	*Live forensics*: akuisisi secara logis, *file system*, fisik, dan *cloud (root)*
5	[Koerhuis et al., 2020]	Persiapan sistem, akuisisi *virtual* memori, lalu lintas jaringan, dan *disk image*, serta analisis	Koleksi, Eksaminasi, Analisis, dan Pelaporan [Casey, 2009)	Wireshark, Linux *tools*	*Live forensics*: akuisisi secara fisik, *virtual memory* (vmem), paket jaringan
6	[Nabi, 2014]	Tidak ada	Tidak ada	Tidak ada	Tidak ada
7	[Montanez, 2014]	Persiapan sistem (instalasi, transaksi, penghapusan), ekstraksi data, analisis	Tidak mengacu ke kerangka kerja tertentu. Hanya melakukan akuisisi dan analisis.	Cellebrite UFED Touch Ultimate, Cellebrite UFED Physical Analyzer, iFunBox, Notepad++, DB Browser for SQLite	*Live forensics*: akuisisi logis, *dump*, dan *screenshot*
8	[Van der Horst et al., 2017]	Persiapan sistem, akuisisi *virtual* memori, dan *disk image*, serta analisis *memory*, *disk*, dan *registry*	Tidak mengacu ke kerangka kerja tertentu. Hanya melakukan akuisisi dan	Volatility pada Linux Machine	*Live forensics*: akuisisi memory *virtual machine* dan *disk*

			analisis.		
9	[Shi et al., 2023]]	Persiapan sistem, Analisis	Tidak mengacu ke kerangka kerja tertentu. Hanya analisis.	DB Browser Sqlite	*Live forensics*: akuisisi secara logis
10	[Zollner et al., 2019]	Persiapan sistem, Akuisisi data (aplikasi dan *web* dompet aset kripto), analisis	Tidak mengacu ke kerangka kerja tertentu. Hanya melakukan akuisisi dan analisis	*Open source tool*	*Live data forensics* and *postmortem analysis*
11	[Kovalcik, 2022]	Persiapan sistem, identifikasi dengan aplikasi, akuisisi, analisis	Akuisisi, Verifikasi, Preservasi, Analisis, dan Validasi	Linux *open source*	Akuisisi secara fisik
12	[Thomas, 2020]	Penyusunan skenario, identifikasi struktur data, pengembangan *plugin*, virtualisasi memori fisik	Tidak mengacu ke kerangka kerja tertentu. Hanya akuisisi dan analisis.	Volatility	*Live forensics*: akuisisi fisik *virtual machine*
13	[Doran, 2015]	Penyiapan sistem, akuisisi data, analisis	*Digital Forensic Research Workshop* (DFRWS) [Harrell, 2010]	Tableau Imager, EnCase, Internet Evidence Finder, Winen.exe	*Live forensic:* akuisisi RAM, akuisisi secara fisik
14	[Ngwu et al., 2021]	Penyiapan sistem, akuisisi data, analisis	Tidak mengacu ke kerangka kerja tertentu. Hanya akuisisi dan	OS Forensics, Magnet RAM Capture, HxD	*Live forensic*: akuisisi RAM

			analisis.		
15	[Jones, 2014]	Penyiapan sistem, akuisisi data, analisis	Tidak mengacu ke kerangka kerja tertentu. Hanya akuisisi dan analisis.	FTK Imager Lite, FTK Toolkit	*Live forensic*: akuisisi RAM dan secara fisik

BAB 3
METODOLOGI

3.1 Motivasi

Dalam melakukan penelitian ini, penulis menggunakan metodologi penelitian sebagaimana diuraikan dalam *framework* riset untuk menjadi acuan menjalankan tahapan penelitian agar eksperimen investigasi forensik digital terhadap 10 dompet kripto pada platform Windows dan Android dengan beberapa skenario fase dapat dilakukan secara sistematis, hasilnya valid, dapat dipertanggungjawabkan, dan dapat menjadi pengetahuan dan/atau penemuan baru pada topik penelitian ini.

3.2 *Framework* Riset

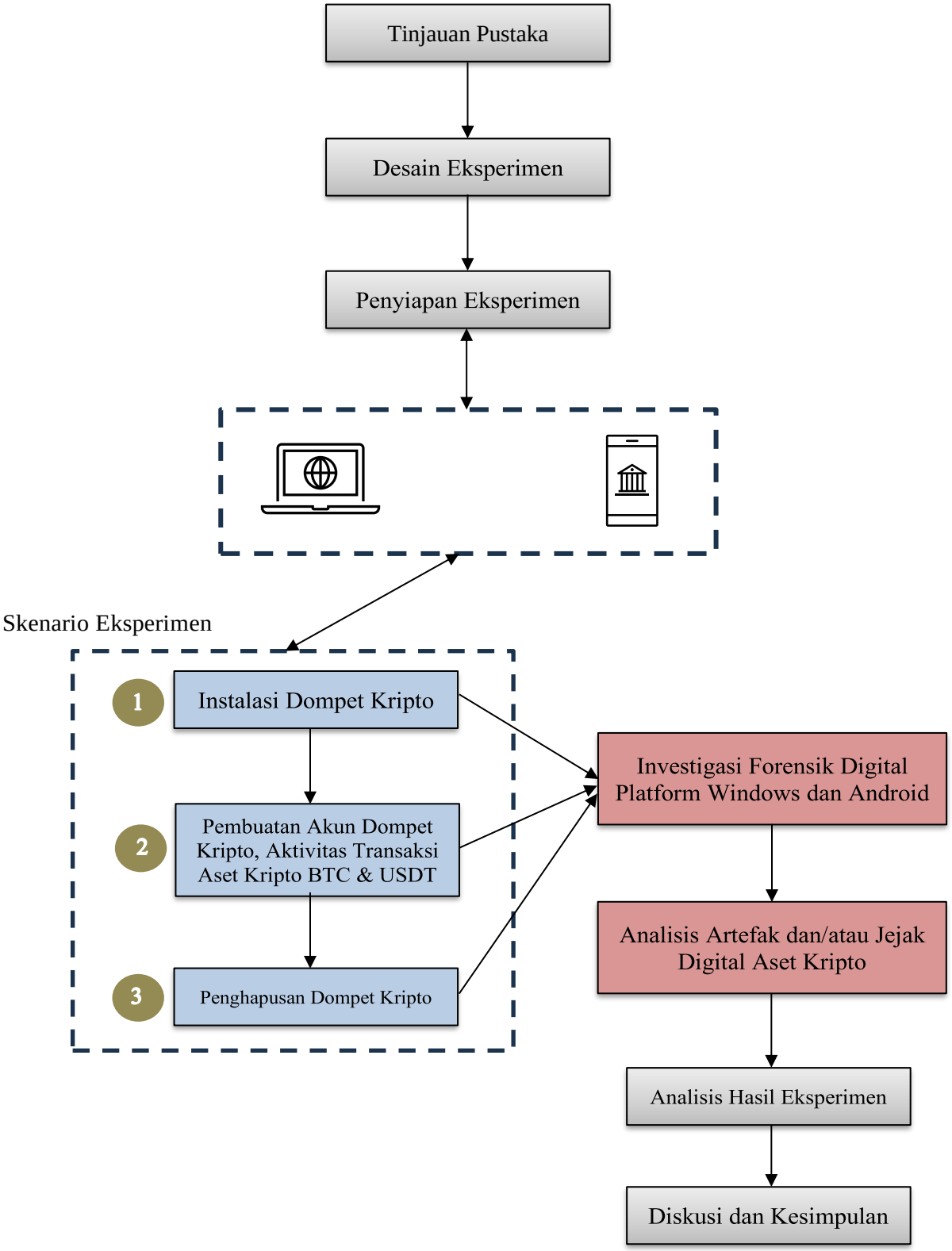
Dalam melakukan penelitian ini, penulis menyusun metodologi penelitian atau *framework* riset sebagaimana Gambar 3.2.1. Secara ringkas, *framework* riset yang digunakan oleh penulis meliputi:

1) Tinjauan Pustaka

Tinjauan Pustaka adalah tahapan penulis melakukan tinjauan pustaka atas penelitian terdahulu yang berkaitan dengan topik penelitian ini. Terdapat 15 penelitian terdahulu yang sudah dilakukan komparasi dan dikaji lebih lanjut untuk menggali kekurangan atau kesenjangan yang selanjutnya menjadi bahan latar belakang, tujuan, serta perumusan masalah dari penelitian ini.

2) Desain Eksperimen

Desain Eksperimen adalah tahapan penulis merancang eksperimen yang dilakukan dalam penelitian ini untuk menjawab permasalahan yang sudah didefinisikan. Desain eksperimen yang dibuat adalah eksperimen melakukan investigasi forensik digital dan analisis atas artefak dan jejak digital aset kripto pada platform Windows 11 dan Android 11/12 . Penulis telah menyusun gambaran desain eksperimen atas penelitian ini sebagaimana Tabel 3.2.1.



Gambar 3.2.1 *Framework* riset

3) Penyiapan Eksperimen

Penyiapan Eksperimen adalah tahapan penulis menyiapkan kebutuhan eksperimen meliputi perangkat komputer dengan sistem operasi Windows 11 dan juga telepon selular Android 11/12 termasuk *virtual machine* Windows 11 dan *emulator* Android 11/12. Daftar kebutuhan perangkat platform Windows dan Android untuk penelitian ini sebagaimana Tabel 3.2.2. Selain itu, penulis juga menyiapkan peralatan forensik digital yang digunakan untuk melakukan investigasi dan analisis atas artefak dan jejak digital aset kripto sebagaimana Tabel 3.2.3.

Tabel 3.2.1 Desain Eksperimen Investigasi Forensik Digital dan Analisis Artefak dan Jejak Digital Aset Kripto pada Platform Windows dan Android

Jenis Aset Kripto	:	Bitcoin (BTC) dan Tether (USDT)
Dompet Kripto	:	10 dompet kripto yang terdiri dari 5 dompet kripto non-kustodian dalam bentuk aplikasi *desktop* pada Windows 11 dan aplikasi Android 11/12 serta 5 dompet kripto kustodian dalam bentuk *web browser* pada windows 11 dan aplikasi Android 11/12. Dompet kripto dimaksud yaitu Bitcoin Wallet/Core, Exodus, Coinomi, Electrum, Bither, Luno, Indodax, Tokocrypto, Reku, dan digitalexchange.id.
Platform	:	Perangkat komputer atau *virtual machine* dengan sistem operasi Windows 11 dan perangkat seluler atau *emulator* Android dengan sistem operasi Android 11/12
Skenario	:	1) Instalasi dompet kripto; 2) Pembuatan akun dompet kripto dan aktivitas transaksi pembelian, penjualan, penerimaan, dan/atau pengiriman aset kripto; 3) Penghapusan dompet kripto
Kerangka kerja	:	Kerangka kerja awal mengadopsi ISO/IEC 27037:2012 dan ISO/IEC 27042:2015 dengan usulan penyesuaian berkaitan dengan objek investigasi dan analisis aset kripto yang punya karakteristik khusus

Metode	:	Beberapa prosedur dan teknik akuisisi untuk mendapatkan artefak dan jejak digital aset kripto yang tersisa di platform Windows dan Android akan digunakan, antara lain akuisisi RAM, akuisisi browser, akuisisi disk, akuisisi email/cloud, akuisisi *protected files*, akuisisi *$Recycle.BIN* dan *Unallocated area*
Peralatan	:	Peralatan Forensik Digital untuk akuisisi perangkat komputer, telepon seluler, dan akun internet/cloud
Artefak dan/atau sisa jejak	:	1) RAM; 2) Browser; 3) Direktori file; 4) Email/cloud; 5) *Windows Registry*; 6) *$Recycle.BIN*; 7) *Unallocated area*

Tabel 3.2.2 Daftar kebutuhan perangkat platform Windows dan Android

Perangkat	Keterangan
Komputer Workstation X1	Platform Windows 11
Samsung M31	Platform Android 12/13
VMware *Virtual Machine*	Virtualisasi sistem operasi Windows 11
Android Studio	Virtualisasi sistem operasi Android 12/13

Tabel 3.2.3 Daftar Peralatan Forensik Digital yang digunakan dalam Penelitian

Nama Peralatan	Kegunaan	Ketersediaan
FTK Imager (versi Windows and Linux)	Akuisisi perangkat Windows (*RAM, Browser, Disk, Protected Files, $Recycle.BIN, dan Unallocated area*)	*Freeware*
Exterro FTK Forensic Toolkit	Analisis perangkat Windows (RAM, Browser, Disk, Protected Files, $Recycle.BIN, dan Unallocated area)	*Proprietary*
Magnet Axiom	Analisis perangkat Windows dan perangkat seluler Android	*Proprietary*
Autopsy	Analisis perangkat Windows dan perangkat seluler Android	*Open-source*
Oxygen Forensics Detective	Ekstraksi (*Physical, File system, Logical*) dan analisis perangkat seluler Android	*Proprietary*
Cellebrite UFED 4PC	Ekstraksi perangkat seluler Android (*Physical, File system,*	*Proprietary*

	Logical)	
Cellebrite Physical Analyzer	Analisis perangkat seluler Android	*Proprietary*
Oxygen Cloud Extractor	Ekstraksi akun internet/cloud	*Proprietary*
Forensics Email Collector	Ekstraksi akun internet/cloud	*Proprietary*
Android Debug Bridge (adb)	Akses sistem operasi Android dan ekstraksi data Android	*Open-source*

4) Skenario Eksperimen

Skenario Eksperimen adalah tahapan penulis melakukan aktivitas sesuai dengan skenario eksperimen yang terdiri dari 3 fase. Fase pertama yaitu instalasi dompet kripto; fase kedua yaitu pembuatan akun dompet kripto dan aktivitas transaksi pembelian, penjualan, penerimaan, dan/atau pengiriman aset kripto; dan fase ketiga yaitu penghapusan dompet kripto. Rincian skenario dapat dilihat pada Gambar 3.2.2 dengan rincian akun pada Tabel 3.2.4.

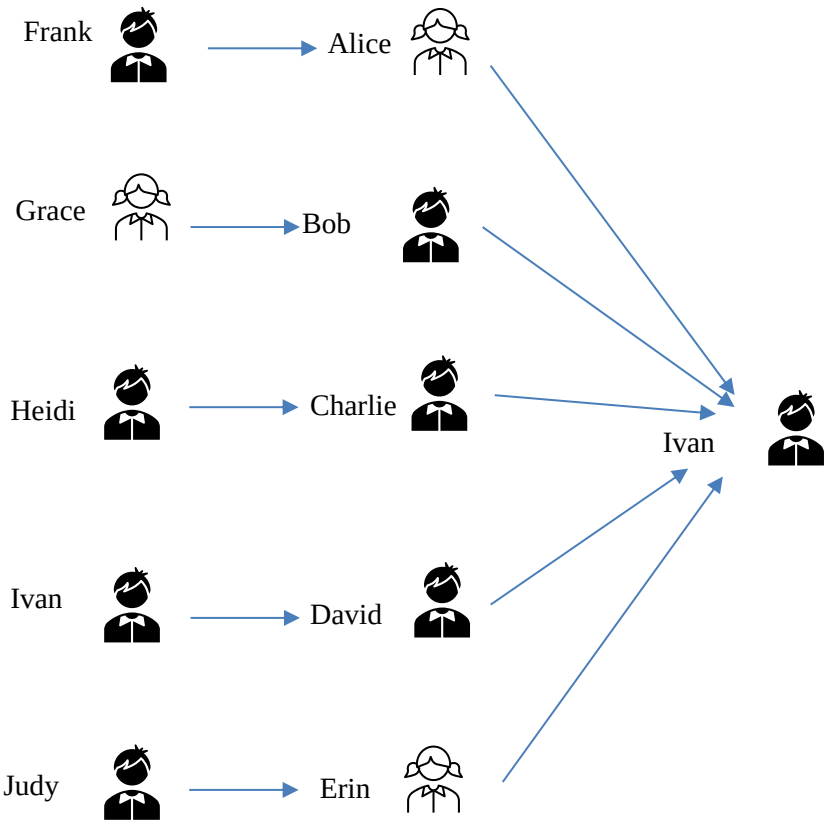
Tabel 3.2.4 Rincian Akun dan Dompet Kripto yang digunakan dalam Penelitian

No	Akun	Email	Dompet	Windows 11	Android 11/12
1	Alice	alice@digitalforensics.asia	Bitcoin Wallet	aplikasi Desktop	Aplikasi Android
2	Bob	bob@digitalforensics.asia	Exodus	aplikasi Desktop	Aplikasi Android
3	Charlie	charlie@digitalforensics.asia	Coinomi	aplikasi Desktop	Aplikasi Android
4	David	david@digitalforensics.asia	Electrum	aplikasi Desktop	Aplikasi Android
5	Erin	erin@digitalforensics.asia	Bither	aplikasi Desktop	Aplikasi Android
6	Frank	frank@digitalforensics.asia	Luno	Website	Aplikasi Android
7	Grace	grace@digitalforensics.asia	Indodax	Website	Aplikasi Android
8	Heidi	heidi@digitalforensics.asia	Tokocrypto	Website	Aplikasi Android
9	Ivan	ivan@digitalforensics.asia	Reku	Website	Aplikasi Android
10	Judy	judy@digitalforensics.asia	Digitale xchange.id	Website	Aplikasi Android

5) Investigasi Forensik Digital Platform Windows dan Android

Investigasi Forensik Digital Platform Windows dan Android adalah tahapan penulis melakukan investigasi forensik digital pada platform Windows

11 dan Android 11/12 untuk setiap fase eksperimen, yaitu 1) akuisisi dan analisis forensik pasca instalasi dompet kripto; 2) akuisisi dan analisis forensik setelah pembuatan akun dompet kripto dan aktivitas transaksi pembelian, penjualan, penerimaan, dan/atau pengiriman aset kripto; dan 3) akuisisi dan analisis forensik pasca penghapusan dompet kripto.



Gambar 3.2.2 Skenario Eksperimen

6) Analisis Artefak dan/atau Jejak Digital Aset Kripto

Analisis Artefak dan/atau Jejak Digital Aset Kripto adalah tahapan penulis melakukan analisis informasi yang diperoleh dari proses investigasi sebelumnya dengan sumber terbuka seperti website https://metasleuth.io/, https://www.blockchain.com/explorer untuk menemukan riwayat transaksi atau menggali siapa saja yang terkait dengan alamat aset kripto guna pengembangan kasus.

7) Analisis Hasil Eksperimen

Analisis Hasil Eksperimen adalah tahapan penulis melakukan analisis atas seluruh temuan yang diperoleh selama penelitian dilakukan. Penulis akan mengaitkan hasil analisis investigasi dengan permasalahan yang diangkat dalam penelitian ini.

8) Diskusi dan Kesimpulan

Diskusi dan Kesimpulan adalah tahapan penulis untuk membahas hasil penelitian lebih lanjut dan menyusun kesimpulan terkait penelitian ini. Hasil penelitian dievaluasi dan dibandingkan dengan tinjauan pustaka atas beberapa penelitian terdahulu yang sudah dilakukan. Selain itu, penulis juga menyajikan rumusan kontribusi yang dapat diberikan termasuk kontribusi hasil penelitian sebagai pengetahuan dan/atau penemuan baru pada topik penelitian ini.

3.3 Pendekatan

Dalam penelitian ini, penulis menggunakan pendekatan penelitian kualitatif melalui jenis penelitian eksperimen. Penelitian eksperimen digunakan untuk menangkap dan memperoleh informasi yang mendalam mengenai suatu peristiwa atau kejadian dalam hal ini proses investigasi dan analisis pada artefak dan/atau jejak digital pada platform Windows dan Android sesuai dengan desain eksperimen yang dikembangkan agar hasil selanjutnya bisa disandingkan dengan tinjauan pustaka atas penelitian-penelitian terdahulu, apakah penelitian ini dapat menutup kekurangan atau kesenjangan yang ada dari penelitian yang sudah dilakukan atau tidak.

DAFTAR PUSTAKA

[ACFE, 2024] ACFE. (2024). Occupational Fraud 2024: A Report to the Nations. Association of Certified Fraud Examiners. Austin, USA. https://legacy.acfe.com/report-to-the-nations/2024/

[Adhar, 2023) Adhar, M., N. (2023). Analisis Artefak Digital Aplikasi Dompet Cryptocurrency Tokocrypto pada Android. Tesis. Universitas Islam Indonesia.

[Caestecker, 2024] Caestecker, K. (2024). Crypto Assets. *OECD Internasional Academy for Tax Crime Investigation: Conducting Finansial Investigations*. National Tax Academy

[Chainalysis, 2024] Chainalysis. (2024). The 2024 Crypto Crime Report: The Latest Trends in Ransomware, Scams, Hacking, and More. https://go.chainalysis.com/crypto-crime-2024.html

[Coinmarketcap charts, 2024] Coinmarketcap charts. https://coinmarketcap.com/. (diakses pada tanggal 12 Juni 2024 pukul 17:04 WIB)

[Casey, 2009] Casey, E. (2009). Handbook of Digital Forensics and Investigation. Academic Press. October 2009.

[Chang et al., 2022] Chang, D., Darcy, P. , Choo, K. R., and Nhien-An Le-Khac, N. (2022). Forensic Artefact Discovery and Attribution from Android Cryptocurrency Wallet Applications. https://doi.org/10.48550/arXiv.2205.14611.

[Debono et al., 2024] Debono, D. and Sultana, A. (2024). Desktop Crypto Wallets: A Digital Forensic Investigation and Analysis of Remnants and Traces on end-User Machines. *The 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 350-357. https://doi.org/10.5220/0012313000003648.

[Doran, 2015] Doran (2015). A Forensic Look at Bitcoin Cryptocurrency. SANS

Institute. https://www.sans.org/white-papers/36437/.

[Dudani et al., 2023] Dudani, S., Baggili, I., Raymond, D., and Marchany, R. (2023). The current state of cryptocurrency forensics. *Forensic Science International: Digital Investigation*. https://doi.org/10.1016/j.fsidi.2023.301576

[Dyson et al., 2018] Dyson, S., Buchanan, W. J., and Bell, L. (2018). The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime. *The Journal of The British Blockchain Association*, 1(2), 5779. https://doi.org/10.48550/ arXiv.1907.12221.

[Europol, 2023] Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA) 2023. Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf

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

[Hirwani, 2012] Hirwani, Y., Pan, B., Stackpole, D., J. (2012). Forensic Acquisition and Analysis of VMware Virtual Hard Disks, https://scholarworks.rit.edu/cgi/ viewcontent.cgi?article=1300&context=other.

[Jones, 2014] Jones, L., D. (2014). Examining the forensic artifacts produced by use of bitcoin currency. Utica College ProQuest Dissertations & Theses.

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

[Kovalcik, 2022] Kovalcik. (2022). Digital forensics of cryptocurrency wallets. Dissertation. https://www.diva-

portal.org/smash/get/diva2:1671204/FULLTEXT02.

[Li et al., 2020] Li, X., and Whinston, A. B. (2020). Analyzing cryptocurrencies. *Information Systems Frontiers*, 22(1), 17–22. https://doi.org/10.1007/s10796-019-09966-2 p.19.

[Mirza et al., 2022] Mirza, M., M., Ozer, A., and Karabiyik, U. (2022). Mobile Cyber Forensic Investigations of Web3 Wallets on Android and iOS. *Appl. Sci.*, 12, 11180. https://doi.org/10.3390/app122111180.

[Montanez, 2014] Montanez, A. (2014). Investigation of cryptocurrency wallets on iOS and Android mobile devices for potential forensic artifacts. Dissertation, Huntington, United States.

[Nabi, 2018] Nabi, A. G. (2018). Analytic Study on Android-based Crypto-Currency Wallets. Dissertation, University of Zurich.

[Ngwu et al., 2021] Ngwu, C., R., Amah, N., L., and Ede, C., C. (2021). Digital Forensic Investigation and Analysis of Bitcoin Wallets: Data Remnants and Traces on User Machines. *Umudike Journal of Engineering and Technology (UJET)*, Vol. 7, No. 1, pp. 79 – 89; Michael Okpara University. https://doi.org/10.33922/j.ujet_v7i1_12.

[Shi et al., 2023] Shi, C. and Guan, Y. (2023). Forensic Analysis of Android Cryptocurrency Wallet Applications. Advances in Digital Forensics XIX: 19th IFIP WG 11.9 International Conference, ICDF. Virginia, USA.

[Thomas et al., 2020] Thomas, T., Piscitelli, M., Shavrov, I., and Baggili, I. (2020). Memory FORESHADOW: Memory FOREnSics of HArDware CryptOcurrency wallets – A Tool and Visualization Framework. *Forensic Science Internasional: Digital Investigation, Volume 33, Supplement*, 2020, 301002, ISSN 2666-2817, https://doi.org/10.1016/j.fsidi.2020.301002.

[Tziakouris, 2018] Tziakouris. (2018). Cryptocurrencies - A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective. *IEEE Security & Privacy*, vol. 16, no. 4, pp. 92-94. https://doi.org/10.1109/MSP.2018.3111243.

[Van der Horst et al., 2017] Van der Horst L., Choo, K-K. R. Choo, Le-Khac, N-A. (2017). Process memory investigation of the Bitcoin Clients Electrum and Bitcoin Core. *IEEE Access* Vol.5(1). https://doi.org/10.1109/ACCESS.2017.2759766.

[Zollner et al., 2019] 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*, volume 7, page 158250 158263. https://doi.org/10.1109/ ACCESS.2019.2948774.