Criminal Investigations and Network Analysis (CINA): A DHS Center of Excellence

Digital Forensic Investigations Involving Cryptocurrency Wallets Installed on Mobile Devices

Prepared For: CINA
Prepared By: Hexordia

Table of Contents

Acknowledgment: This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 17STCIN00001-08-00.

Executive Summary

This report provides an analysis of twelve iOS and twelve Android cryptocurrency wallet applications, focusing on the identification and location of wallet information, transaction hashes, user identifiers, and app-specific identifiers within these mobile apps. The primary objective of this research is to identify and locate key data elements such as wallet information, transaction hashes, user identifiers, and app-specific identifiers within these mobile apps.

Our findings indicate that wallet addresses and transaction hashes are the most commonly retrievable pieces of information across these applications, providing essential leads for tracking cryptocurrency flows. In a few cases, we also discovered plaintext seed phrases, which are particularly valuable for investigators as they offer potential access to the entire wallet.The mobile apps used for this report include:

iOS	Android
Phantom	Unstoppable
Uniswap	Coinbase
SafePal	Zengo
Exodus	eToro
MetaMask	Guarda
Bither/Bitpie	Phantom
Coinbase	MoonPay
Coin Cola	Rainbow
eToro	MetaMask
Guarda	OKX
MoonPay	Exodus
Rainbow	Gemini

Background

This project addresses the challenges investigators face regarding the effective seizure of cryptocurrencies from software wallet applications and the extraction, preservation, and analysis of related data found on suspects' mobile devices. Law enforcement agencies (LEAs) across the United States currently face a significant gap in both capability and understanding in this area. The traditional days of executing search warrants to recover physical drugs and large sums of fiat currency, such as USD, are dwindling. Many police departments have already observed a shift toward the use of digital currencies, or "cryptocurrencies," which are often perceived as anonymous. These currencies are increasingly prevalent on anonymizing platforms, commonly referred to as darknets, where illicit goods and services are traded internationally. Consequently, LEAs must develop robust digital forensic capabilities and protocols to adapt to this evolving landscape.

This project serves as the continuation of an earlier funded initiative. The original Principal Investigator (PI) transitioned from their university role to a U.S. Government position before the project's conclusion. The completed tasks include updating and finalizing the development of the image and artifact databases, as well as providing a cryptocurrency wallet seizure guide for the mobile apps.

iOS Cryptocurrency Wallets

Phantom

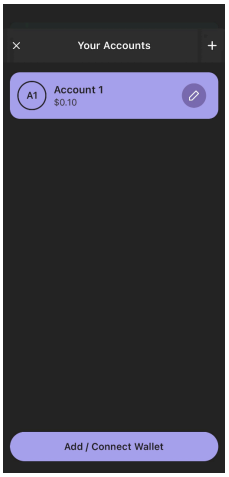
Bundle ID: app.phantom

Wallet Findings:

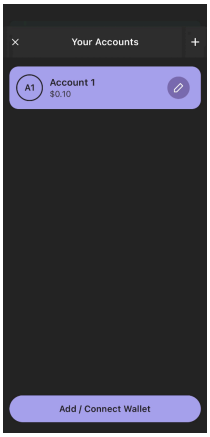
1. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\app.phantom - {DEFAULT GROUP}\3EE53681-0926-4F63-92DF-616141D22310@3x.ktx
    a. Phantom wallpaper

2. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\app.phantom - {DEFAULT GROUP}\downscaled\187DB4AD-AE75-4C63-994C-D0AD0A737E2B@3x.ktx
    a. Phantom Wallpaper

3. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\sceneID:app.phantom-default\BD02ABEC-4527-48BD-B4A0-0E979FF79694@3x.ktx
    a. Wallet account screenshot



4. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\sceneID:app.phantom-default\downscaled\8DABDDE0-3EAF-4A97-8619-62A5644A2FC6@3x.ktx
    a. Wallet account screenshot



5. \private\var\db\diagnostics\logdata.statistics.1.txt
    a. Instances of the Phantom app with the corresponding Application UUID

```
1262616,  11.7, /private/var/containers/Bundle/Application/28741155-AF3D-4567-A67A-3198261143FE/Phantom.app/Phantom ]
```

6. \private\var\mobile\Containers\Shared\AppGroup\<ApplicationUUID>\File Provider Storage\state-log-2024-08-09T12-18-34_PhantomLogs.txt
    a. Phantom logs with the associated addresses associated with each Phantom account.

```
{
  name: "Account 1",
  icon: undefined,
  balance: {
    timestamp: 1723205895394,
    value: 4.9504451616
  },
  identifier: "4683be7e063f4ef86e08b038f1dc2f0527972756acea7fbd3f33c05c44c975ea",
  addresses: [
    {
      networkID: "solana:101",
      addressType: "solana",
      address: "6iwChzVqP2fG8v3RMhf9uu7tPhe8hJ55HCps7oEqCHzB"
    },
    {
      networkID: "eip155:1",
      addressType: "eip155",
      address: "0x961F79a2910cd641Dc6f7eF672561bA021C3b123"
    },
    {
      networkID: "eip155:137",
      addressType: "eip155",
      address: "0x961F79a2910cd641Dc6f7eF672561bA021C3b123"
    },
    {
      networkID: "bip122:000000000019d6689c085ae165831e93",
      addressType: "bip122_p2wpkh",
```


"6iwChzVqP2fG8v3RMhf9uu7tPhe8hJ55HCps7oEqCHzB"
},
{
networkID: "eip155:1",
addressType: "eip155",
address:
"0x961F79a2910cd641Dc6f7eF672561bA021C3b123"

7. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Documents\mmkv\mmkv.default
    a. Wallet address with the corresponding amount
    Description of app
    Recipient address with the corresponding amount
    Solano validator addresses
    Transaction ID. Who sent, received, amount, type, network fee, time, who's paying

```
{
  timestamp: 1723222103,
  owner: "eip155:1/address:0x961f79a2910cd641dc6f7ef672561ba021c3b123",
  id: "eip155:1/tx:0xd40a0319670bdd3a6e8f368e8c71ce71b035c18b0f2f84e48543444d126f0855",
  interactionData: {
    transactionType: "TOKEN_SEND",
    balanceChanges: [
      {
        token: {
          id: "eip155:1/nativeToken:60",
          displayName: "Ethereum",
          logoURI:
          https://cdn.jsdelivr.net/gh/trustwallet/assets@master/blockchains/ethereum/assets/0xC02aaA39b223FE8D0A0e5C4F27eAD
          9083C756Cc2/logo.png,
          tokenType: "Native",
          decimals: 18,
          symbol: "ETH",
          isSpam: false
        },
        amount: "50218256267625",
        to: "eip155:1/address:0xdd0979c7514d3554a72fe9fc6174c98808d09180",
        from: "eip155:1/address:0x961f79a2910cd641dc6f7ef672561ba021c3b123"
      }
    ],
    dapp: null
  },
  chainMeta: {
    networkFee: "76600291593000",
    networkFeePayer: "0x961F79a2910cd641Dc6f7eF672561bA021C3b123",
    status: "success",
    errorMessage: null,
    blockNumber: "20492336",
    chainId: "eip155:1",
    transactionId: "0xd40a0319670bdd3a6e8f368e8c71ce71b035c18b0f2f84e48543444d126f0855"
```

```
state: {
  data: {
    solana:101/nativeToken:501: [
      {
        apy: "0.08095498720030947",
        chainId: "solana:101",
        convertRatio: "1.131423145121606",
        name: "Jito",
        stakePoolAddress: "Jito4APyf642JPZPx3hGc6WWJ8zPKtRbRs4P815Awbb",
        stakePoolTokenMetadata: {
          caip19: "solana:101/address:J1toso1uCk3RLmjorhTtrVwY9HJ7X8V9yYac6Y7kGCPn",
          metadata: {
            address: "J1toso1uCk3RLmjorhTtrVwY9HJ7X8V9yYac6Y7kGCPn",
            chainId: "solana:101",
            decimals: 9,
            logoURI: https://storage.googleapis.com/token-metadata/JitoSOL-256.png,
            name: "Jito Staked SOL",
            symbol: "JitoSOL"
          }
        },
        validators: [
          {
            vote_account: "GFK84uv9cr1d6KnkPERSEYagTvpLKTuwa8W9adx1qMg6"
          },
          {
            vote_account: "B38JgkTi7Fu2Uxk8JzNw4M7aMhVxzGu2fsRqHNScPkCQ"
          },
          {
            vote account: "5cXLZKeTuRm95ng96K2qCdxB2kSU1ajW291HmEkNpXkM"
```

8. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\app.phantom\Cache.db
    a. Wallet addresses


```
"data": {
    "amount": "35211359996770",
    "chain": {
        "id": "eip155:1",
        "imageUrl": "https://dhc7eusqrdwa0.cloudfront.net/assets/
        "name": "Ethereum",
        "symbol": "ETH"
    },
    "coingeckoId": "ethereum",
    "decimals": 18,
    "logoUri": "https://cdn.jsdelivr.net/gh/trustwallet/assets@ma
    "name": "Ethereum",
    "spamStatus": "VERIFIED",
    "symbol": "ETH",
    "walletAddress": "0x961F79a2910cd641Dc6f7eF672561bA021C3b123"
},
"type": "EthereumNative"
```

```
"appVersion": "24.13.0",
"locale": "en",
"platform": "ios",
"identifiers": [
  {
    "type": "ROOT_ID",
    "id": "ad9de006c2ca52adb75e9640e793a531168897c5cda11f7fd54bcbd66c9b1c64"
  }
],
"selectedAccountAddresses": [
  {
    "chainId": "solana:101",
    "address": "6iwChzVqP2fG8v3RMhf9uu7tPhe8hJ55HCps7oEqCHzB",
    "resourceType": "address"
  },
  {
    "chainId": "eip155:1",
    "address": "0x961f79a2910cd641dc6f7ef672561ba021c3b123",
    "resourceType": "address"
  },
  {
    "chainId": "eip155:137",
    "address": "0x961f79a2910cd641dc6f7ef672561ba021c3b123",
    "resourceType": "address"
  },
  {
    "chainId": "bip122:000000000019d6689c085ae165831e93",
    "address": "bc1q09qgar6py3est98y6qr5wfp068j2pezase37zx",
    "resourceType": "address"
  }
],
"isOptedOut": false
```

```
"tokens": [
  {
    "type": "EthereumNative",
    "data": {
      "chain": {
        "id": "eip155:1",
        "name": "Ethereum",
        "symbol": "ETH",
        "imageUrl": "https://dhc7eusqrdwa0.cloudfront.net/assets/ethereum.png"
      },
      "walletAddress": "0x961F79a2910cd641Dc6f7eF672561bA021C3b123",
      "decimals": 18,
      "amount": "35211359996770",
      "logoUri": "https://cdn.jsdelivr.net/gh/trustwallet/assets@master/blockchains/ethereum/assets/0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2/logo.png
      "name": "Ethereum",
      "symbol": "ETH",
      "coingeckoId": "ethereum",
      "spamStatus": "VERIFIED"
    }
```


9. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\rl_persistence.sqlite
    a. Includes wallet address. The “type: seed”, accountID

riginalTimestamp":"2024-08-13T23:04:19.338Z","properti es":{"osName":"iOS","ids":{"Ethereum": [{"id":"0x961F79a2910cd641Dc6f7eF672561bA021C3b123 ","type":"seed","accountId":"4683be7e063f4ef86e08b038 f1dc2f0527972756acea7fbd3f33c05c44c975ea"}],"Po

10. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Documents\SQLite\simpleStorage.db
    a. Contains wallet address

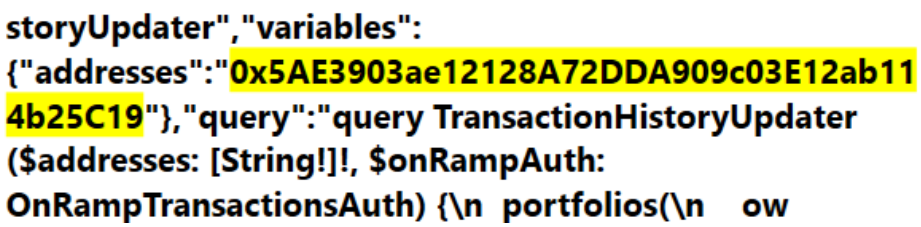
f9uu7tPhe8hJ55HCps7oEqCHzB"},"eip155": {"chainType":"eip155","pathType":"bip44Ethereum","publ icKey":"0x961F79a2910cd641Dc6f7eF672561bA021C3b12 3"}}}]}*O,.phantom-labs.vault.cache.secrets {"version":1,"seedIdentifiers":["ad9de006c2ca52adb75e9

Uniswap

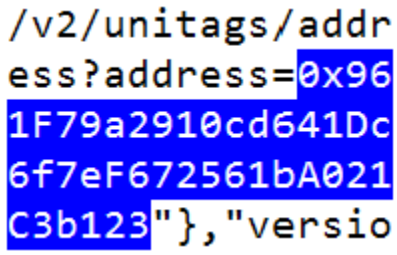
Bundle ID: com.uniswap.mobile

Wallet Findings:

1. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\com.uniswap.mobile\Cache.db
    a. Contains wallet address of Phantom wallet, address funds were transferred to



2. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\com.datadoghq\v2\f5da9c34155155fa15554148a8a2d145170e0a082ddf9cba39ea3a198b2bb947\rum\v2\745365746195
    a. Contains receiving address for Phantom wallet



3. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\io.sentry\99387cfe99a513e350ff41b6ea6377bf986af37b\breadcrumbs.1.state
    a. Contains wallet address

4. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\io.sentry\99387cfe99a513e350ff41b6ea6377bf986af37b\previous.breadcrumbs.1.state

5. Contains transaction notification with wallet address and date time, Device Vendor ID


```
"notifications": {
    "lastTxNotificationUpdate": {
        "0x5AE3903ae12128A72DDA909c03E12ab114b25C19": 1723206738000
```

```
eligibility?address=0x5AE3903ae12128A72DDA909c03E12ab114b25C19&deviceId=13CF7B69-AD63-41F4-9DB9-79BC8DB51F58"
```


6. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\com.uniswap.mobile\fsCachedData\250F9C89-D739-4ECB-AE2C-CBDBFAA37905
    a. Wallet of account that is receiving the money

type":"RECEIVE","hash":"0xcb55d7c79e572cc819a459cb95328c6a27bdd9ce5c954cdce5344a1ad020134b","from":"0x961F79a2910cd641Dc6f7eF672561bA021C3b123","status":"CONFIRMED","application":{"name":null,"address":"0x961F79a2910cd641Dc6f7eF672561bA021C3b

    b. Transaction hashes


```
"id":
"QXNzZXRBY3Rpdml0eTpWSEpoYm5OaFkzUnBiMjVFWlhSaGFXeHpPakI0TkdNeE9HTXhPVEZsTkRRMFlXRTNOekE1Wm1ZeU9UQmxNMkpqTm1Kak56Z3hOMk5rWkdKbE9UazRaRGN6WTJFM04yVTFOVFU0TVdSbFpUZG1PRFUxTWc9PQ==",
```

```
"id":
"AssetActivity:VHJhbnNhY3Rpb25EZXRhaWxzOjB4NGMxOGMxOTFlNDQ0YWE3NzA5ZmYyOTBlM2JjNmJjNzgxN2NkZGJlOTk4ZDczY2E3N2U1NTU4MWRlZTdmODU1Mg==",
```

```
"id":
"AssetActivity:TransactionDetails:0x4c18c191e444aa7709ff290e3bc6bc7817cddbe998d73ca77e55581dee7f8552",
```


7. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\SystemData\com.apple.SafariViewService\Library\WebKit\WebsiteData\NetworkCache\Version 16\Records\29E67EBB1C6F2569C4F72B182605B83B31C7C679\Resource\9A4D4FC2FD3096DA4012BDD24BAF1E6F822C582C-blob

a. Location of wallet that will be receiving the funds. Phantom app

```
md-9">
<div class="d-inline"> <span class="d-inline"><a data-
highlight-value data-highlight-
target="0x961f79a2910cd641dc6f7ef672561ba021c3b123
" href="/
address/0x961f79a2910cd641dc6f7ef672561ba021c3b123
" class="text-break" style="word-break: b
```

Transaction Hash:
0xcb55d7c79e572cc819a459cb95328c6a27bdd9ce5c954cdce5344a1ad020134b
Status:
Success
Block:
204910604 Block Confirmations
Timestamp:
44 secs ago (Aug-09-2024 12:31:47 PM UTC)|Confirmed within 6 secs

---

Transaction Action:
Transfer0.000761881542657748($2.00)ETHTo 0x5AE3903ae12128A72DDA909c03E12ab114b25C19

Sponsored:

From:
0x961F79a2910cd641Dc6f7eF672561bA021C3b123
To:
0x5AE3903ae12128A72DDA909c03E12ab114b25C19

Value:
0.000761881542657748 ETH ($2.00)
Transaction Fee:
0.000087048744552 ETH ($0.23)

8. private\var\mobile\Containers\Shared\AppGroup\<ApplicationUUID>\Library\Preferences\group.com.uniswap.widgets.plist
   a. Wallet address in AppGroup directory

```
<?xml version="1.0" encoding="utf-16"?>
<plist>
  <dict>
    <key>prod.widgets.accounts</key>
    <string>{"accounts":[{"address":"0x5AE3903ae12128A72DDA909c03E12ab114b25C19","name":"Wallet 1","isSigner":true}]}</string>
    <key>prod.widgets.i18n</key>
    <string>{"locale":"en-US","currency":"USD"}</string>
    <key>prod.widgets.favorites</key>
    <string>{"favorites":[{"chain":"ETHEREUM"},{"address":"0x2260fac5e5542a773aa44fbcfedf7c193bc2c599","chain":"ETHEREUM"}]}</string>
  </dict>
</plist>
```

SafePal

Bundle ID: walletapp.safepal.io

Wallet Findings: Describe important findings from the app such as the location of the wallet, transactions found, additional artifacts related to the wallet

1. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Documents\safepal
    a. Found wallet addresses. Tx hash. sender, receiver, and timestamp

txid
0x82090c294e2ec102f451bc52bfadce11e13f20f448cc7862730de6e572d9d9dc
0x4ff6cd14ff899296f62d01b3c5d73d5ac27af4d5e98e5a89efd21eee3d8fbc12

fromAddr	toAddr	value
0x4735d01719de3ed820073a7708262ab36c076b01	0xbcfc52919f1cdcb528801450a7a3460ff9f6725e	666073220519857
0x961f79a2910cd641dc6f7ef672561ba021c3b123	0x4735d01719de3ed820073a7708262ab36c076b01	762253220519857

@a0xbCFC52919f1cDcB528801450A7a3460FF9F6725E<ET
H'N)ŽCETH

0xbCFC52919f1cDcB528801450A7a3460FF9F6725E

ASCII

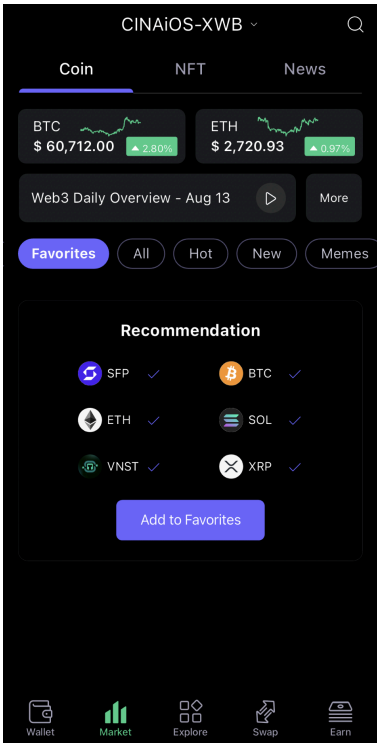
J:\Uniswap.txt

0xbCFC52919f1cDcB528801450A7a3460FF9F6725E

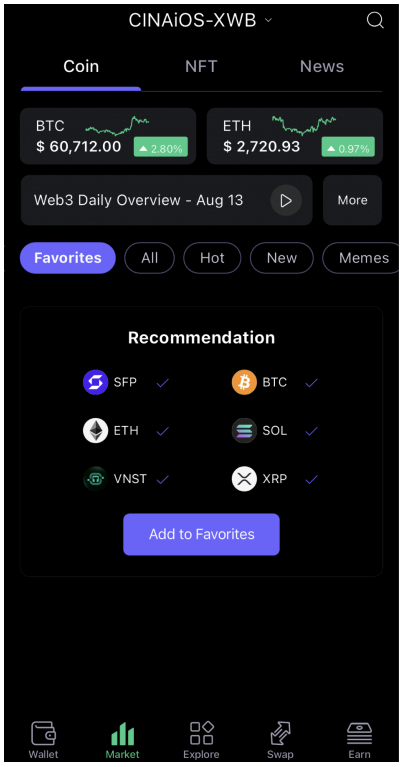
9902610

2. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\sceneID:walletapp.safepal.io-default\AC4D5B78-B626-40A4-BD10-C9830A2B7BA0@3x.ktx
private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\sceneID:walletapp.safepal.io-default\downscaled\63EE6185-9771-4431-8A8A-FCB9AF061A5C@3x.ktx

a. Screenshot of wallet

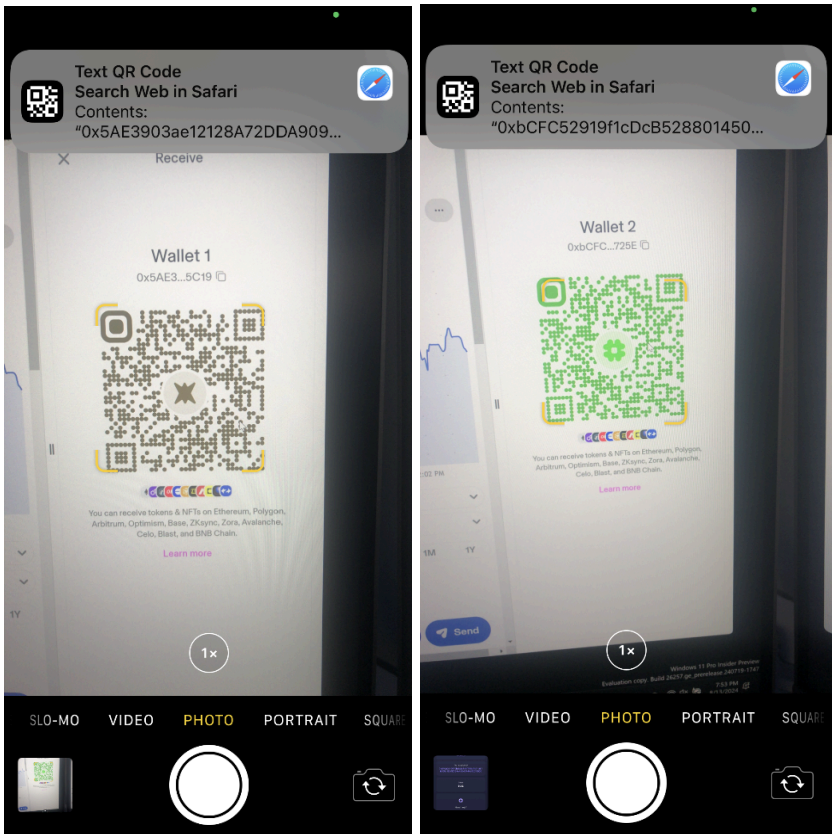


3. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\sceneID:walletapp.safepal.io-default\D97EDE88-FBF2-4246-8D63-BDFF52566BA5@3x.ktx
private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\sceneID:walletapp.safepal.io-default\downscaled\C6B1BA32-0561-44E2-9C45-B647512F9B76@3x.ktx
    a. Screenshot of wallet



4. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\walletapp.safepal.io - {DEFAULT GROUP}\downscaled\D4109B16-7E39-4771-8EEE-575A32F5BC44@3x.ktx
    a. SafePal Wallpaper

5. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\tmp\
    a. Contains wallet addresses


Text QR Code
Search Web in Safari
Contents:
“0x5AE3903ae12128A72DDA909...
Receive
Wallet 1
0x5AE3...5C19
You can receive tokens & NFTs on Ethereum, Polygon, Arbitrum, Optimism, Base, ZKsync, Zora, Avalanche, Celo, Blast, and BNB Chain.
Learn more
1×
SLO-MO
VIDEO
PHOTO
PORTRAIT
Text QR Code
Search Web in Safari
Contents:
“0xbCFC52919f1cDcB528801450...
Wallet 2
0xbCFC...725E
Send
1×
SLO-MO
VIDEO
PHOTO
PORTRAIT

Exodus

Bundle ID: exodus-movement.exodus

Wallet Findings:

1. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Application Support\exodus-movement.exodus\RCTAsyncLocalStorage_V1\manifest.json
    a. Found transaction hash. Sender and amount


```
"txId": "0xd40a0319670bdd3a6e8f368e8c71ce71b035c18b0f2f84e48543444d126f0855",
"date": "2024-08-09T16:48:21Z",
"confirmations": 1,
"dropped": false,
"coinAmount": "0.000050218256267625 ETH",
"coinName": "ethereum",
"from": [
  "0x961f79a2910cd641dc6f7ef672561ba021c3b123"
-
```


2. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\exodus-movement.exodus\Cache.db
    a. Found Phantom Wallet address, address that money is being sent to.


```
0xdD0979C7514d3554A72fE9fC6174C98808D09180&fromTimestamp=1723227521123
```


3. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\exodus-movement.exodus\fsCachedData\
    a. Contains various coins and their value.

```
"AAVE": {
    "USD": 106.54209266082066
},
"AAVEmaticBFDF3C37": {
    "USD": 106.19176129560805
},
"ACHethereumFBAD19A6": {
    "USD": 0.018712045127743868
},
"ADA": {
    "USD": 0.3359599837431608
},
"ADAbscDB5F96AB": {
    "USD": 0.3357795629162 1325
},
```

MetaMask

Bundle ID: io.metamask.MetaMask

Wallet Findings:

1. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Documents\persist Store\persist-root
    a. Wallet addresses

fc711228457f8e63284df422\",
\"0x90ce182e80ac7ddb86d8f39635738929001ddcac\"]},
{\"type\":\"QR Hardware Wallet Device\",\"accounts\":
[]}],\"vault\":\"{\\\"cipher\\\":\\
\"F4mCOAA677PBSSAa1f5y648LYoanNGXAtP7P7xxS

0xE33CAb16Ae3A5cE54698709793Aa6319c9Cd129F\":
0x23E028AdAAa9235BFc711228457F8E63284DF422\":
0x90cE182E80AC7DDB86D8f39635738929001dDCAc\":

2. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\io. metamask.MetaMask\Cache.db
    a. Wallet addresses

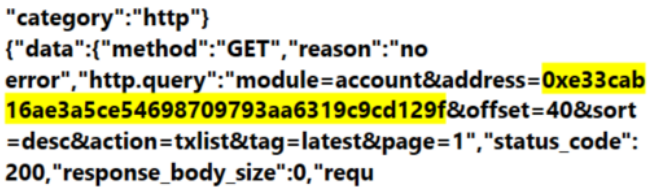
https://api.etherscan.io/api?
module=account&address=0xe33cab16ae3a5ce546
98709793aa6319c9cd129f&offset=40&sort=desc&
action=tokentx&tag=latest&page=1

s.com/?
b=a2EzeEpydGNjNmUxYmkzbTIzYkhiWjo6R2FYczZmNUVi
QVdqZ1lGZW14dkJuOEh1cm4xM3E4cEk=,,#https://
nft.api.cx.metamask.io/
users/0xE33CAb16Ae3A5cE54698709793Aa6319c9Cd129F
/tokens?chainIds=1&limit=50&incl

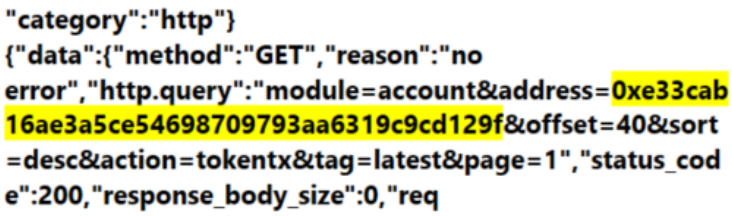
3. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\io.s entry\4e573d0d2511306cf9b3e0c0451da649f4b3e82c\breadcrumbs.1.state
    a. Wallet addresses

true&continuation=","status_code":200,"response_body_s
ize":0,"request_body_size":0,"url":"https:\/\/
nft.api.cx.metamask.io\/users
\/0xE33CAb16Ae3A5cE54698709793Aa6319c9Cd129F\/
tokens"},"timestamp":"2024-0

4. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\io.sentry\4e573d0d2511306cf9b3e0c0451da649f4b3e82c\previous.breadcrumbs.2.state
    a. Wallet addresses



5. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\io.sentry\4e573d0d2511306cf9b3e0c0451da649f4b3e82c\previous.breadcrumbs.1.state
    a. Wallet addresses



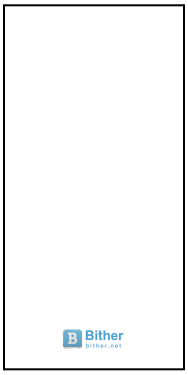
Bither/Bitpie

Bundle ID: net.bither/com.bitpie.wallet

Wallet Findings:

1. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\net.bither - {DEFAULT GROUP}\C6DB610D-F0C5-4726-9799-F3499310B8A9@3x.ktx

   \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\net.bither - {DEFAULT GROUP}\A2CF7054-5B3A-4C41-9F27-5543346B8729@3x.ktx
   a. Bither wallpaper



2. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\bsystemcoins.sqlite
   a. Contains: balance, coin, contract address


```
"balance": "0",
"balance_str": "0",
"coin_code": "TRX-TRC20-USDT",
"coin_name": "Tether USD",
"contract_address": "TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t",
"display_code": "USDT-TRC20",
"is_custom_rpc": false,
"is_fixed": false,
"level": 0,
"p_coin_code": "TRX-TRX",
"price_precision": 4,
"reputation": 0,
"sort_num": 1,
"token_logo": "/token/img/trx-trc20-usdt.png",
"unit_decimal": 6
```

```
"balance": "0",
"balance_str": "0",
"coin_code": "ETH-USDC",
"coin_name": "USD Coin",
"contract_address": "0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48",
"display_code": "USDC-ERC20",
"is_custom_rpc": false,
"is_fixed": false,
"level": 0,
"p_coin_code": "ETH",
"price_precision": 2,
"reputation": 0,
"sort_num": 3,
"token_logo": "/token/img/eth-usdc.jpg",
"unit_decimal": 6
```

```
"balance": "5173752",
"coin_code": "ZEC",
"coin_name": "Zcash",
"is_custom_rpc": false,
"is_fixed": false,
"level": 0,
"price_precision": 2,
"reputation": 0,
"sort_num": 90,
```

3. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\bcoins.sqlite
    a. Shows Zcash balance


```
"balance": "5173752",
"coin_code": "ZEC",
"coin_name": "Zcash",
"is_custom_rpc": false,
"is_fixed": false,
"level": 0,
"price": "299.12",
"price_precision": 2,
"price_prev": "304.41",
"reputation": 0,
"sort_num": 90,
"unit_decimal": 8
```


4. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\buser.sqlite
    a. Transaction hash


```
"ad_pledge_enough": -1,
"address": "t1J92CBFuVL2dTLyivYoChm1FyBoAtnwi16",
"addresses": [],
"balance": "5173752",
"balance_str": "0",
"bbc_split": 1,
"bcc_split": 1,
"bcd_split": 1,
"bcha_split": 1,
"bchsv_split": 1,
"bcx split": 1,
```


5. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\bflowtxs.sqlite
    a. Transaction address, transaction hash, value, transaction date


```
"address": "t1T9kmxog9aTw7TeTC6mct9Moyj4fR2PTS4",
"confirmation": 1703867,
"inputs": [],
"locked": 0,
"multisig_account_id": -1,
"outputs": [],
"tx_at": "2020-07-20T17:57:55",
"tx_hash": "224d36c1fc84d5fb612f9b383ded8b77edd8eb2f5174516f29d386dfcfc69199",
"tx_size": 244,
"tx_type": 0,
"value": "5173752"
```


6. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\com.bitpie.wallet\fsCachedData\D3FFB6B0-54A0-4CF1-B94C-8BE1CC8B87EB
    a. Contract addresses for coin wallets that exist. Coins that don't have existence, have "null" values.

```
coin_code : "TRX-TRC10-BTT"
display_code : "BTTOLD"
token_logo : "/token/img/trx-trc10-btt.jpg"
unit_decimal : "6"
p_coin_code : "TRX-TRX"
sort_num : "225128"
contract_address : "1002000"
coin_name : "BitTorrent"

coin_code : "ETH-USDX-11"
display_code : "USDx"
token_logo : "/token/img/eth-usdx-11.png"
unit_decimal : "18"
p_coin_code : "ETH"
sort_num : "409274"
contract_address : "0xeb269732ab75a6fd61ea60b06fe994cd32a83549"
coin_name : "USDx"
```


7. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Preferences\com.bitpie.wallet.plist
    a. Contains user address, coin information, balance, etc


```
[0] userGenderKey = 0
[1] register_at = 2020-07-20T16:44:08
[2] CoinType = ZEC
[3] kIsBitpieCreate = True
[4] UserAddressesKey = []
[5] kIsUseSystemUnlock = False
[6] CoinsConfigureHash = aefcdf1e9eac47268135fa0054e344db14fa5e51e52fd880622a48f7d5e99807
[7] kAppVerification = False
[8] userAddressKey = t1J92CBFuVL2dTLyivYoChm1FyBoAtnwi16
[9] kUserIsBithdType = 0
[10] seedPhraseEntropyWrittenAgain = True
[11] kHiddenExchangeList
[12] userIdKey = 6777379
[13] KYCLevel = 0
[14] seedPhraseEntropyWritten = True
[15] AdPledgeEnough = 0
[16] kUserAlgoRewardsAmount = 0
[17] KycRealName =
[18] KycRealNames
[19] otcOnLineStatus = False
[20] userAvatarKey =
[21] kUserType = 0
[22] BalanceStrKey = 5173752
[23] TokenInfo = {"coin_name":"Zcash","level":0,"sort_num":90,"reputation":0,"is_fixed":false,"unit_decimal":8,"coin_code":"ZEC","price_precisi
[24] pinCodeKey = 3677630681184600578;12202990137083774525
[25] kOfflineMode = False
[26] receivingAddressIndex = 0
[27] kUserAlgoPendingRewardsAmount = 0
[28] CoinsConfigure = [{"unit_decimal":6,"coin_code":"ALGO","coin_name":"Algorand","sort_num":0},{"sort_num":0,"unit_decimal":18,"coin_na
[29] PinCodeType = sixDigit
[30] kUserAddressesConfigure = [{"index":0,"coin_code":"ZEC","path":0,"address":"t1J92CBFuVL2dTLyivYoChm1FyBoAtnwi16","purpose":44}
```

Coinbase

BundleID: org.toshi.distribution

Wallet Findings:

1. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Documents\default\wallet-rn-v2.sqlite
    a. Contains address and transaction hash, wallet creation date

txHash
Filter
0x5a5135a8fe62429704dba060791836d1a9ad1793e79500c393ff131c6769eec2
0x846bebbe26d58300f548f90ef9ffcc835717a0ae641dde709f8448bd39cfa3e1

fromAddress	fromDomain	amount	fromAmount	toAmount	fee
Filter	Filter	Filter	Filter	Filter	Filter
0xb5d85cbf7cb3ee0d56b3bb207d5fc4b82f…	NULL	194220000000000	NULL	NULL	491089073013000
0xd7f1dd5d49206349cae8b585fcb0ce3d96…	NULL	1	NULL	NULL	1018229329550400

id	primaryAddress	addresses
Filter	Filter	Filter
SOL/SOL/SOLANA_CHAIN:101/false//0/mnemonic/ETH/…	2sWf2kQwVPVQT4AucPgGqDUc2d47ExASFFEz…	[{"type":"Solana","address":"2sWf2
SOL/SOL/SOLANA_CHAIN:101/false//1/mnemonic/ETH/…	6543Ce6QivH1QKER6VZiHqBoXVNQ8AsKs7bJ…	[{"type":"Solana","address":"6543C
SOL/SOL/SOLANA_CHAIN:101/false//2/mnemonic/ETH/…	645bN2gtvWsZgQutViDfSNejARArLrjweDWZ…	[{"type":"Solana","address":"645bN
SOL/SOL/SOLANA_CHAIN:101/false//3/mnemonic/ETH/…	9rQDqLDBR8drf1p3RcLhYusN1LhzPPavDs35…	[{"type":"Solana","address":"9rQDq
SOL/SOL/SOLANA_CHAIN:101/false//4/mnemonic/ETH/…	GAVZ1kj7VRNa2AJZn23MTy6wwPQKLehExUYq…	[{"type":"Solana","address":"GAVZ1
SOL/SOL/SOLANA_CHAIN:101/false//5/mnemonic/ETH/…	F9shbWMqXGWu7wYViuDhPPnNP8KePB98VejR…	[{"type":"Solana","address":"F9shb
SOL/SOL/SOLANA_CHAIN:101/false//6/mnemonic/ETH/…	7wER2oq16EzRARHDWWsrfsqLYJsJABcX2hVu…	[{"type":"Solana","address":"7wER2
SOL/SOL/SOLANA_CHAIN:101/false//7/mnemonic/ETH/…	Doqi34Zza35UozL5yk3LVY7o2BWKTJU4X2p8…	[{"type":"Solana","address":"Doqi3
SOL/SOL/SOLANA_CHAIN:101/false//8/mnemonic/ETH/…	9rYJXeipXL9xLW4CJmPeEEpJY7NsRARaQYEW…	[{"type":"Solana","address":"9rYJX
SOL/SOL/SOLANA_CHAIN:101/false//9/mnemonic/ETH/…	A7bmWzKAAmnBP4ggn9mKjbxfahq5coKa42vC…	[{"type":"Solana","address":"A7bmW
ETH/ETH/ETHEREUM_CHAIN:7777777/false//7/mnemonic/ETH/…	0x47F5897bD059FBd7a193413794e464Ce34…	[{"type":"Ethereum","address":"0x4
ETH/ETH/ETHEREUM_CHAIN:421614/true//7/mnemonic/ETH/…	0x47F5897bD059FBd7a193413794e464Ce34…	[{"type":"Ethereum","address":"0x4
ETH/AVAX/ETHEREUM_CHAIN:43113/true//7/mnemonic/ETH/…	0x47F5897bD059FBd7a193413794e464Ce34…	[{"type":"Ethereum","address":"0x4
ETH/ETH/ETHEREUM_CHAIN:84532/true//7/mnemonic/ETH/…	0x47F5897bD059FBd7a193413794e464Ce34…	[{"type":"Ethereum","address":"0x4
ETH/BNB/ETHEREUM_CHAIN:97/true//7/mnemonic/ETH/…	0x47F5897bD059FBd7a193413794e464Ce34…	[{"type":"Ethereum","address":"0x4
ETH/FTM/ETHEREUM_CHAIN:4002/true//7/mnemonic/ETH/…	0x47F5897bD059FBd7a193413794e464Ce34…	[{"type":"Ethereum","address":"0x4

2. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Documents\mmkv\CBStore.plaintext
    a. Contains primary address
    :userSettingsPrimaryAddress-,"0x886F08C7506058410D3Ed809FfeFd81F581E17C6
3. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Documents\mmkv\mmkv-persistor
    a. Geoavailability checker

```
"state": {
    "data": {
        "country": "US",
        "permitted": true
    },
    "dataUpdateCount": 1,
    "dataUpdatedAt": 1723142971035,
    "error": null,
    "errorUpdateCount": 0,
    "errorUpdatedAt": 0,
    "fetchFailureCount": 0,
    "fetchFailureReason": null,
```


4. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Application Support\com.bugsnag.Bugsnag\org.toshi.distribution\v1\system_state.json
    a. Notes if the device is jailbroken


```
device : {}
    id : "9a926e8d9779480daac0c3109c0f742c9a54bc68"
    osName : "iOS"
    jailbroken : "True"
    simulator : "False"
    osVersion : "15.4"
    locale : "en_US"
```


5. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Application Support\Google\FirebaseInstanceID\g-checkin.plist
    a. Google folder with Firebase Messaging, Android ID


```
[2] GMSInstanceIDGServicesData
    [0] android_id = 4778293050772314181
    [1] device_country = us
    [2] device_registration_time = 1723140000000
    [3] ios device = 1
```

CoinCola

Bundle ID: com.coincola.beta

Wallet Findings:

1. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Saved Application State\com.coincola.beta - {DEFAULT GROUP}\BFE8635E-8C9F-47F9-B53B-B045A3022406@3x.ktx
    a. Coincola wallpaper

2. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Documents\crypto.json
    a. Coins supported

```
otc : {}
  cryptoCoin : [8]
      "BTC"
      "ETH"
      "USDT"
      "EOS"
      "XRP"
      "BCH"
      "LTC"
      "GUSD"
```

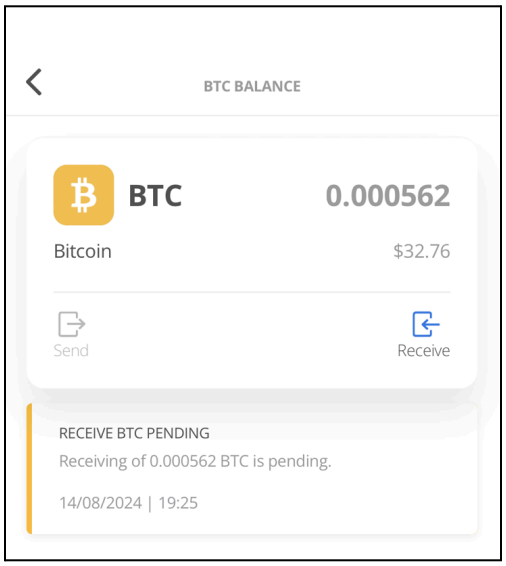
eToro Money

Bundle ID: com.etoro.wallet

Wallet Findings:

1. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\sceneID:com.etoro.wallet-default\40687AE9-B07E-4D36-B8D2-44C1BE3C293E@3x.ktx

   \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\sceneID:com.etoro.wallet-default\B95A947D-0D28-43B8-9841-C3F116C23848@3x.ktx
   a. Screenshot of account balance



2. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\WebKit\NetworkCache\Version 16\Records\0E52D5A5CB46EAB388D4A7A4DA98DF65DDB29539\Resource\B928360B734B602E77E1D25073B0202A1F61D9E7-blob
   a. Different currency comparison

```
InstrumentDisplayDatas : [9057]
  { }
    InstrumentID : "1"
    InstrumentDisplayName : "EUR/USD"
    InstrumentTypeID : "1"
    ExchangeID : "1"
    Images : [6]
      { }
        InstrumentID : "1"
        Width : "35"
        Height : "35"
```

Guarda

Bundle ID: com.crypto.multiwallet

Wallet Findings:

1. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Application Support\com.crypto.multiwallet\RCTAsyncLocalStorage_V1\817e01dfc9ca7287f4e9a0f6a1c6830b
    a. Contains backup phrase. Also contains hidden wallet information, private key information for all wallets


```
"address": "bnb1zt4g8vy9a8wrm0zhtypvl5dxpmd86m83ymkwhk",
"privateKey": "[redacted]8e18317eeb476665bbcad678afbea1ebdf1155820e
"balance": "0",
"currency": "bnb",
"title": "Binance Coin",
"uuid": "-9bvKwgeCeQh",
"derivedFromMnemonicUsing": {
  "accountIndex": 0
,,
"mnemonic": [redacted]jump flash actress weasel grant arena cinnamon bird story",
"last-update-time": 1723681868741,
"version": 50,
"autobackup-setting": 0,
"uuid": "ZR-CH9UWHeQiz_EgabscB7Vsf8pxsmj5XmwT",
"session-timeout": ""
```


2. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Application Support\Google\FirebaseInstanceID\g-checkin.plist
    a. Android ID


```
<dict>
  <key>android_id</key>
  <string>5224914260445558884</string>
  <key>device_country</key>
  <string>us</string>
  <key>device_registration_time</key>
  <string>1723680000000</string>
  <key>ios_device</key>
  <string>1</string>
</dict>
```


3. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\com.crypto.multiwallet\Cache.db

a. Contains wallet address used, total received, total sent, and transaction hash


```
"page": 1,
"totalPages": 1,
"itemsOnPage": 1000,
"addrStr": "1K5PmcEpx5pnMz92oSfMn9fxeqpJ3XZtci",
"balance": "0.00075335",
"totalReceived": "0.00075335",
"totalSent": "0",
"unconfirmedBalance": "0",
"unconfirmedTxApperances": 0,
"txApperances": 1,
"transactions": [
  "4dae50d6e9fe02ea9d5c01fddade1f7abcfb241ced8e926470daaf7bc9d2d938"
```

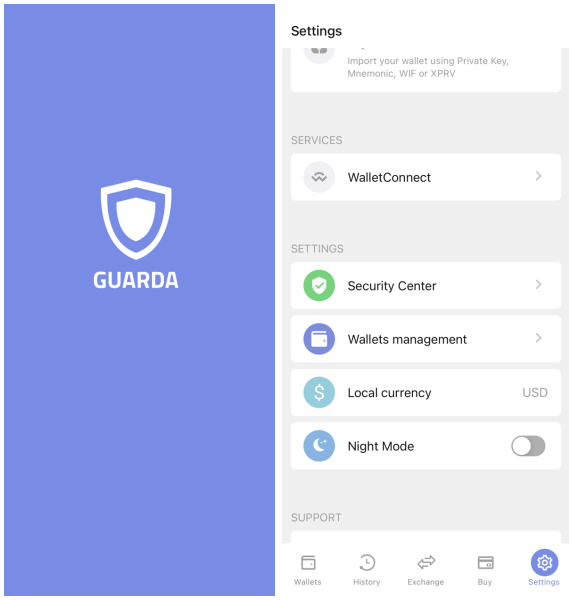
{"page":1,"totalPages":1,"itemsOnPage":100,"addrStr":"1K5PmcEpx5pnMz92oSfMn9fxeqpJ3XZtci","balance"
[{"txid":"4dae50d6e9fe02ea9d5c01fddade1f7abcfb241ced8e926470daaf7bc9d2d938","version":1,"vin":
[{"txid":"bdefbebc467cfe39e857ce2d20199b4862fd04f617e523f32dce3b349c3543d8","vout":10,"sequence":42
{},"addresses":["bc1qjp5ymz5xuymg54k8af89la7w3pzyhn2d6kp335"],"value":"0.00076133"}],"vout":
[{"value":"0.00075335","n":0,"scriptPubKey":
{"hex":"76a914c646ef44838a52571594a45fa18212a81903d67588ac","addresses":
["1K5PmcEpx5pnMz92oSfMn9fxeqpJ3XZtci"]},"spent":false}],"blockhash":"000000000000000000000c8c430f

__CFURLStringType_CFURLString_Phttps://
bitcoinblockexplorers.com/api/
address/1K5PmcEpx5pnMz92oSfMn9fxeqpJ3XZtci#@
$___CFURLRequestNullTokenString__
#ÿÿÿÿÿÿÿÿSGETÔVAccept_Accept

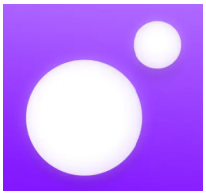
4. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\com.crypto.multiwallet\fsCachedData\
    a. General coin data from exchanges


```
currency : "arv"
extraIdentifier : "0x6679eb24f59dfe111864aec72b443d1da666b360"
family : "bsc"
title : "Ariva"
rates : {}
    usd : "0.00012484823452308338"
changes : {}
    h1h : "-0.1779701"
    h24 : "3.65597835"
    d7 : "-0.37027059"
id : "arv:bsc:0x6679eb24f59dfe111864aec72b443d1da666b360"
```


5. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\
    a. ktx files. Shows app wallpaper and app settings screenshot


GUARDA
Settings
Import your wallet using Private Key, Mnemonic, WIF or XPRV
SERVICES
WalletConnect
SETTINGS
Security Center
Wallets management
Local currency
USD
Night Mode
SUPPORT
Wallets
History
Exchange
Buy
Settings

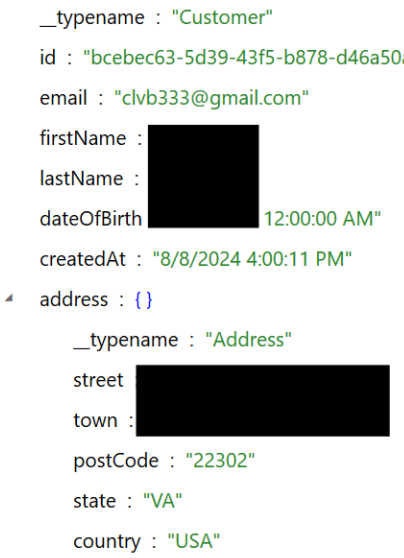
MoonPay



Bundle ID: com.moonpay.app

Wallet Findings:

1. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Application Support\com.moonpay.app\RCTAsyncLocalStorage_V1\91ec1f9324753048c0096d036a694f86
    a. Contains email address, name, creation time



2. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Application Support\com.moonpay.app\RCTAsyncLocalStorage_V1\b6fc409153bed742ecb0853f303fb9f1
    a. Wallet address and balance, location address


```
"bc1qy4mcmduqtf2syfqhts8pjx39fvy6w6u6s720pe": {
  "addressStatus": "supported",
  "totalBalance": "33.6176027366305353",
  "network": "mainnet",
  "chain": "bitcoin",
  "baseCurrency": "USD"
```

```
{
  "state": {
    "data": {
      "alpha2": "US",
      "alpha3": "USA",
      "country": "United States of America",
      "ipAddress": "2607:7e80:1012:d40:b579:6c5:af4d:efd4",
      "isAllowed": true,
      "isBuyAllowed": true,
      "isNftAllowed": true,
      "isSellAllowed": true,
      "isBalanceLedgerWithdrawAllowed": true,
      "isFiatBalanceAllowed": false,
      "isLowLimitEnabled": false,
      "state": "DC"
```


3. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Application Support\com.braze.core.persistence\data\ace60e6\users\bcebec63-5d39-43f5-b878-d46a50a49800_eee4964\session.json
    a. User ID and session date time


```
end : "8/14/2024 11:20:29 PM"
id : "07685BF4-B9F4-41DB-AA42-AD64F94486F2"
messagingStart : "8/14/2024 11:18:10 PM"
start : "8/14/2024 11:18:10 PM"
```

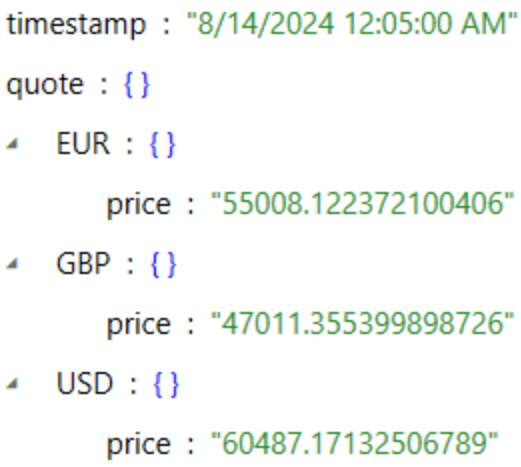

4. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Application Support\Google\FirebaseInstanceID\g-checkin.plist
    a.


```
[2] GMSInstanceIDGServicesData
    [0] android_id = 4738395328126533930
    [1] device_country = us
    [2] device_registration_time = 1723676400000
    [3] ios_device = 1
```


5. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\com.moonpay.app\Cache.db
    a. Wallet addresses: BTC, Ethereum, Solana


```
addresses=3wr7tQwcZpnjEQvmbr2SXzeXLLaUjHN986HRhwtJmmXQ
:bc1qy4mcmduqtf2syfqhts8pjx39fvy6w6u6s720pe%3Abitcoin
:0x20516B44aB56F2c6cE15e26e99485a85CA9A52cb%3Aethereum
```


6. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\com.moonpay.app\fsCachedData\F58FB0D1-D3AB-4DCD-BEDD-25250934E89F
    a. Coin pricing at a date time that exists on the phone



7. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\io.sentry\d1b24b1a17522b6cd8165c795db6b9e4fd3a7b09\breadcrumbs.1.state
    a. Wallet addresses


```
"http.query":
"addresses=Bwr7tQwcZpnjEQvmbr2SXzeXLLaUjHN986HRhwtJmmXQ:solana,bc1qy4mcmduqtf2syfqhts8p
x39fvy6w6u6s720pe:bitcoin,0x20516B44aB56F2c6cE15e26e99485a85CA9A52cb:ethereum&currencyC
de=EUR",
```


8. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Caches\io.sentry\d1b24b1a17522b6cd8165c795db6b9e4fd3a7b09\breadcrumbs.2.state
    a. Wallet addresses

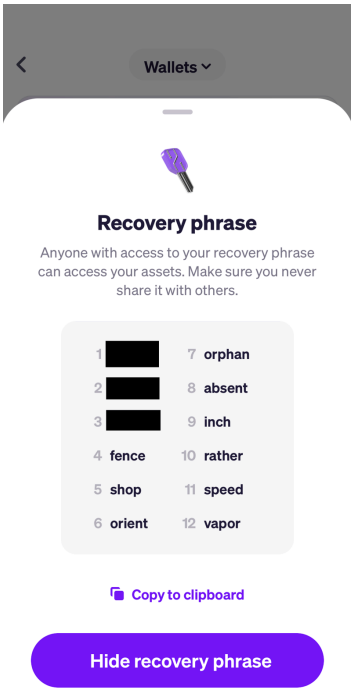

```
"data": {
    "url": "https:\/\/crypto-api.moonpay.com\/api\/v3\/
    balance?addresses=bc1qy4mcmduqtf2syfqhts8pjx39fvy6w6u6s720pc%3Abitcoin%2CBwr7tQwcZpnjEQvmbr2SXzcXLLaU
    jHN986HRhwtJmmXQ%3Asolana%2C0x20516B44aB56F2c6cE15e26e99485a85CA9A52cb%3Aethereum&currencyCode=USD",
```


9. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\sceneID:com.moonpay.app-default\01619737-7D0B-416E-BEA9-1D4AA572918A@3x.ktx

    private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\sceneID:com.moonpay.app-default\93740F62-8CBA-489B-8880-91CED343A5DE@3x.ktx
    a. Recovery phrase

10. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\sceneID:com.moonpay.app-default\downscaled\0FA4BC85-7E96-4735-A303-C6B041E352CA@3x.ktx

    private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\SplashBoard\Snapshots\sceneID:com.moonpay.app-default\downscaled\5581BD44-889D-4454-90E0-9956FD580FC7@3x.ktx
    a. Downscaled versions of recovery phrase screenshot



11. private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\WebKit\WebsiteData\LocalStorage\https_buy.moonpay.com_0.localstorage
    a. User details. Birthday, name, email, nationality, ip country, state


```
"birthday":[redacted]
"createdAt": "2024-08-08T16:00:11.403Z",
"userCreationMonth": "202408",
"email": "clvb333@gmail.com",
"firstName":[redacted],
"lastName": [redacted],
"nationality": "USA",
"ipAddressCountryCode": "USA",
"ipAddressStateCode": "DC",
```

Rainbow

Bundle ID: me.rainbow

Wallet Findings:

1. \private\var\mobile\Containers\Data\Application\<ApplicationUUID>\Library\Application Support\Google\FirebaseInstanceID\g-checkin.plist
    a. Android ID and registration time

Android Cryptocurrency Wallets

Unstoppable

Package Name: io.horizontalsystems.bankwallet

Wallet Findings:

1. \data/user\0\io.horizontalsystems.bankwallet\databases\dbBankWallet
    a. Enabled Wallet

Browse Data | Execute SQL | Edit Pragmas

Table: EnabledWallet | Filter in any column

	tokenQueryId	accountId	walletOrder	coinName	coinCode	coinDecimals
	Filter	Filter	Filter	Filter	Filter	Filter
1	bitcoin|derived:bip84	e25c3f22-107a-4f5a-8d89-f687e3f2810b	0	Bitcoin	BTC	8
2	bitcoin|derived:bip84	813b361c-ab7f-41bc-8c2a-301b36153ee0	0	Bitcoin	BTC	8
3	bitcoin|derived:bip84	b2499dc7-6c4a-4670-960a-fdb9533265d9	0	Bitcoin	BTC	8
4	ethereum|native	e25c3f22-107a-4f5a-8d89-f687e3f2810b	1	Ethereum	ETH	18
5	ethereum|native	813b361c-ab7f-41bc-8c2a-301b36153ee0	1	Ethereum	ETH	18
6	ethereum|native	b2499dc7-6c4a-4670-960a-fdb9533265d9	1	Ethereum	ETH	18
7	binance-smart-chain|native	813b361c-ab7f-41bc-8c2a-301b36153ee0	2	Binance Coin	BNB	18
8	binance-smart-chain|native	b2499dc7-6c4a-4670-960a-fdb9533265d9	2	Binance Coin	BNB	18
9	ethereum|...	813b361c-ab7f-41bc-8c2a-301b36153ee0	3	Tether	USDT	6
10	ethereum|...	b2499dc7-6c4a-4670-960a-fdb9533265d9	3	Tether	USDT	6
11	binance-smart-chain|...	813b361c-ab7f-41bc-8c2a-301b36153ee0	4	Binance USD	BUSD	18
12	binance-smart-chain|...	b2499dc7-6c4a-4670-960a-fdb9533265d9	4	Binance USD	BUSD	18

b. Enabled Wallet Cache

Table EnabledWalletCac... | 15 entries | Page 1 of 1 | Export to CSV

tokenQueryId	accountId	balance	balanceLocked
binance-smart-chain|native	e25c3f22-107a-4f5a-8d89-f687e3f2810b	0	0
binance-smart-chain|eip20:0xe9e7cea3dedca5984780bafc599bd69add087d56	e25c3f22-107a-4f5a-8d89-f687e3f2810b	0	0
ethereum|eip20:0xdac17f958d2ee523a2206206994597c13d831ec7	e25c3f22-107a-4f5a-8d89-f687e3f2810b	0	0
bitcoin|derived:bip84	813b361c-ab7f-41bc-8c2a-301b36153ee0	0.00000000	0.00000000
ethereum|native	813b361c-ab7f-41bc-8c2a-301b36153ee0	0.024056241629289575	0
binance-smart-chain|native	813b361c-ab7f-41bc-8c2a-301b36153ee0	0	0
ethereum|eip20:0xdac17f958d2ee523a2206206994597c13d831ec7	813b361c-ab7f-41bc-8c2a-301b36153ee0	0	0
binance-smart-chain|eip20:0xe9e7cea3dedca5984780bafc599bd69add087d56	813b361c-ab7f-41bc-8c2a-301b36153ee0	0	0
bitcoin|derived:bip84	e25c3f22-107a-4f5a-8d89-f687e3f2810b	0.00000000	0.00000000
ethereum|native	e25c3f22-107a-4f5a-8d89-f687e3f2810b	0	0
bitcoin|derived:bip84	b2499dc7-6c4a-4670-960a-fdb9533265d9	0.00000000	0.00000000
binance-smart-chain|native	b2499dc7-6c4a-4670-960a-fdb9533265d9	0	0
ethereum|eip20:0xdac17f958d2ee523a2206206994597c13d831ec7	b2499dc7-6c4a-4670-960a-fdb9533265d9	0	0
binance-smart-chain|eip20:0xe9e7cea3dedca5984780bafc599bd69add087d56	b2499dc7-6c4a-4670-960a-fdb9533265d9	0	0
ethereum|native	b2499dc7-6c4a-4670-960a-fdb9533265d9	0.024012746159061575	0

c. Account Record:

id	name	type	origin	isBackedUp	isFileBackedUp	words	passphrase
e25c3f22-107a-4f5a-8d89-f687e3f2810b	Wallet 1	mnemonic	Created	1	0	WkPUztS4vEbjNpPuNgowug==] 6hPyjl3Gcue2mQ5AvMrR4uGWpzWnkcLCxy9DBoWNUEgvMPVAFrWcBQ8QSWW2IZu7sHXNxBeQxTqw Oh2EvBrRnV72n8YNkLHNNN7Fps39jem6qr01Xia5KpVqWneOUs0o	iK9LynGC9mZnHNFGxtDr1w==]bqZk/ fuG01G1IGGyAmMUcQ==
813b361c-ab7f-41bc-8c2a-301b36153ee0	Wallet 2	mnemonic	Created	1	0	ITJFJMNIA9fZIIJwaBLEBw==]LxXLijOJ1Estasdj+GqjMB/YcY1BQEIsh2oids +wGXra8wUV4icAvtct0kJTZiqHyYQ9v93Vc3LE toWg2IJwkAKpLskxhQvzJaIxadChSCo=	iWsjktbX1xjfjzOr4Ej6Mw==]OtgqHU5i+V/ pi5WjmjgBNQ==
b2499dc7-6c4a-4670-960a-fdb9533265d9	Wallet 3	mnemonic	Created	1	0	IWBJ+hB8HD/UX331JAKUgw==]O0igS1wQm1xS4eBAWlnP9WKOfL3/jhaTcsNIOGW1IBrM8aI9/fPez/ cBVSFeH3Mz4iJWKcd4W1a9 r94j/l1jaMTFDo6Fy6Nmw8MXohmwdC4=	6bQ3QINzgRMA0iAY39bPLQ==]mDVqhsDaU3ba/8oqqDYB/ A==

2. \data\data\io.horizontalsystems.bankwallet\databases\Ethereum-1-e25c3f22-107a-4f5a-8d89-f687e3f2810b-txs
    a.

Transaction

hash timestamp isFailed blockNumber transactionIndex from to value input nonce gasPrice maxFeePerGas maxPriorityFeePerGas gasLimit gasUsed replacedWith
1723682819 0 20530543 206 24098046603465575 2 1310347801 21000
1723682933 0 24056241629289575 0 1990713056 1990713056 789349450 21000

InternalTransaction

hash blockNumber from to value id

sqlite_sequence

name seq

TransactionTag

name hash
ETH
ETH_incoming
incoming
from_0x8b59d6331efca4e63555e7a4a5ecc045696ce747
ETH
ETH_outgoing
outgoing
to_0x7c0647b5f51780b4d45042504b8eb229c96282b7

3. \data\data\io.horizontalsystems.bankwallet\databases\Ethereum-1-b2499dc7-6c4a-4670-960a-fdb9533265d9-txs
    a.

Transaction

hash timestamp isFailed blockNumber transactionIndex from to value input nonce gasPrice maxFeePerGas maxPriorityFeePerGas gasLimit gasUsed replacedWith
1723682999 0 20530558 183 24012746159061575 0 2047041492 21000

InternalTransaction

hash blockNumber from to value id

sqlite_sequence

name seq

TransactionTag

name hash
ETH
ETH_incoming
incoming
from_0x7c0647b5f51780b4d45042504b8eb229c96282b7

4. \data\data\com.android.vending\databases\library.db
    a.

Table: ownership — Filter in any column

	account	library_id	backend	doc_id	doc_type	offer_type	document_hash	purchase_time
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
108	clvb333@gmail.com	3	3	io.noone.androidwallet	1	1	-870251422448664408 8	1723676473599

Coinbase

Package Name: org.toshi

Wallet Findings: Coinbase wallet provides data including unused wallet addresses, wallet address, transaction history, and application UUID data.

1. \data\data\org.toshi\app_webview\Default\Local Storage\leveldb\000003.log
    a. Unused wallet address

18	1	_https://wallet-messaging.coinbase.com unused:Addresses	0x886F08C7506058410D3Ed809FfeFd81F581E17C6
19	1	_https://wallet-messaging.coinbase.com unused:DefaultChainId	1
20	1	https://wallet-messaging.coinbase.com unused:DefaultJsonRpcUrl	https://chain-proxy.wallet.coinbase.com?targetName=ethereum-mainnet

```
0000    01 30 78 38 38 36 46 30  38 43 37 35 30 36 30 35   .0x886F08C750605
0010    38 34 31 30 44 33 45 64  38 30 39 46 66 65 46 64   8410D3Ed809FfeFd
0020    38 31 46 35 38 31 45 31  37 43 36                  81F581E17C6
```

2. \data\data\org.toshi\files/default\wallet-rn-v2.sqlite
    a. Account table>Wallet Address:

id	createdAt	type	primaryAddressChain	primaryAddress	nickname	isDeleted	hasCompletedBackupFlow
mnemonic/ ETH/0x886F08C7506058410D3Ed809FfeFd81F581E17C6	2024-08-08 16:28:29.423	mnemonic	ETH	0x886F08C7506058410D3Ed809FfeFd81F581E17C6		0	1

    b. Transaction history:

Browse Data | Execute SQL | Edit Pragmas

Table: tx_history_v2

	id	createdAt	confirmedAt	ıcyC	feeCurrencyCodeStr	feeCurrencyDecimal	toAddress	fromAddress	fromDomain	amount
1	8eb94125-90b4-4bc...	2024-08-08 16:31:35.000	2024-08-08 16:31:35.000	E...	ETH	18	0x886f08c7506058410d3ed809ffefd81f58...	0xb5d85cbf7cb3ee0d56b3bb207d5fc4b82f...	NULL	194220000000000
2	4fd685e6-...	2024-08-08 16:32:00.000	2024-08-08 16:32:00.000	#...	MATIC	18	0x886f08c7506058410d3ed809ffefd81f58...	0x3c499c542cef5e3811e1192ce70d8cc03d...	NULL	1450000000000000000000
3	dd847a56-114f-48b...	2024-08-08 16:32:50.000	2024-08-08 16:32:50.000	5...	MATIC	18	0x886f08c7506058410d3ed809ffefd81f58...	0x7ceb23fd6bc0add59e62ac25578270cff1...	NULL	5000000000000000000

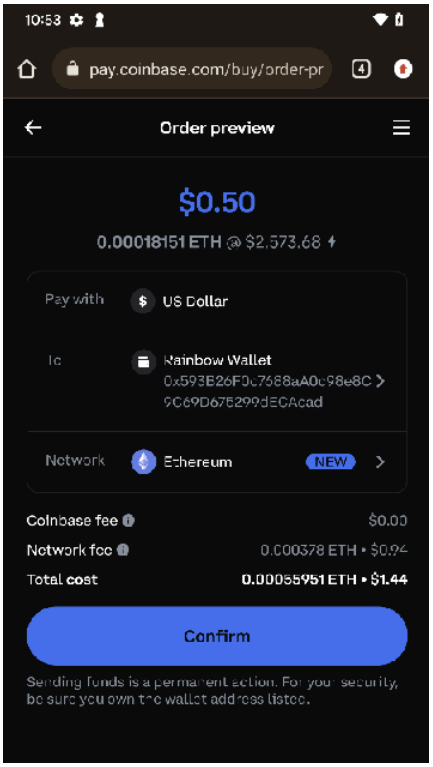
3. Last application usage date: \data\data\org.toshi\app_webview\last-exit-info
    a. {"exitInfoPid":1375,"timestampAtLastRecordingInMillis":1723678686501,"appState":0}
4. \data\data\org.toshi\files\.com.google.firebase.crashlytics.files.v2:org.toshi\open-sessions\66BD3FDD02220001055FF38C5A3A186A\native\app.json
    a. UUID: {"development_platform":"","version_name":"29.6.7","development_platform_version":"","version_code":"290600070","app_identifier":"org.toshi","install_uuid":"5ec9b409c9b446a7b1c8b60632bfc0d3","delivery_mechanism":4}

5. IP addresses: \data\data\org.toshi\files\mmkv\CBStore.plaintext
    a.

Analysis Result 1

Score:	Likely Notable
Type:	Keyword Hits
Configuration:	IP Addresses
Conclusion:	
Keyword:	[redacted]
Keyword Preview:	chnology.network\",\[redacted]",\"carv.pages.dev\"
Keyword Regular Expression:	[illegible]
Keyword Search Type:	2
Set Name:	IP Addresses

b. userSettingsPrimaryAddress-,"0x886F08C7506058410D3Ed809FfeFd81F581E17C6"(CBStore.plaintext:miamiViceFSTODisplayed^^true;CBStore.plaintext:areLowBalanceWalletsHiddenByWalletGroupIdCB{"mnemonic/ETH/0x886F08C7506058410D3Ed809FfeFd81F581E17C6/0":true},CBStore.plaintext:throttleRequestLastUpdated  ^^{"mnemonic/ETH/0x886F08C7506058410D3Ed809FfeFd81F581E17C6-0-BTC":1723678688678,"mnemonic/ETH/0x886F08C7506058410D3Ed809FfeFd81F581E17C6-0-LTC":1723678688808,"mnemonic/ETH/0x886F08C7506058410D3Ed809FfeFd81F581E17C6-0-DOGE":1723678688851}'CBStore.plaintext:lastSyncedBlockheight^^{"mnemonic/ETH/0x886F08C7506058410D3Ed809FfeFd81F581E17C6-0-BTC":856798,"mnemonic/ETH/0x886F08C7506058410D3Ed809FfeFd81F581E17C6-0-LTC":2738308,"mnemonic/ETH/0x886F08C7506058410D3Ed809FfeFd81F581E17C6-0-DOGE":5336375}'CBStore.plaintext:blockchainIsSyncedMap,+"{\"BTC\":true,\"DOGE\":true,\"LTC\":true}"]CBStore.plaintext:mnemonic/ETH/0x886F08C7506058410D3Ed809FfeFd81F581E17C6/isZeroBalanceWallet^^falsefCBStore.plaintext:mnemonic/ETH/0x886F08C7506058410D3Ed809FfeFd81F581E17C6/lastZeroBalanceFireTimeStamp^17236786888950

6. \data\media\0\Pictures\Screenshots\Screenshot_20240808-105351.png
   a. 

7. \data\data\com.android.chrome\cache\Offline Pages\archives\10c56c26-dddf-4943-8605-5cd417e59e24.mhtml
    a. https://pay.coinbase.com/buy/send/success/details?appId=a7ca65d7-6100-4818-bc71-e83ae065885&defaultExperience=buy&defaultNetwork=ethereum&destinationWallets=5B7B address3A0x593B6F0c7688aA0c98e8C9C69D67599dECAcadCblockchains3A5BethereumCoptimismCarbitrumCpolygonCbaseCavalanche-c-chain5DCassets3A5BETHCUSDCCDAICMATICCAVAXCwBTC5D7D5D

8. \data\user\0\org.toshi\cache\http-cache\47b6a1ef6418929850d738acbddfdcae.0
    a. https://chain-proxy.wallet.coinbase.com/api?module=account&action=txlist&address=0x886F08C7506058410D3Ed809FfeFd81F581E17C6&page=1&offset=50&sort=desc&targetName=gnosis-gnosisscan&apikey=7739c80e-684a-40a1-bbc3-977ac36b26fc

9. \data\user\0\org.toshi\cache\http-cache\9daa4498c0c764a6839ddf8e9e56896f.0
    a. https://chain-proxy.wallet.coinbase.com/api?module=account&action=tokentx&address=0x886F08C7506058410D3Ed809FfeFd81F581E17C6&page=1&offset=50&sort=desc&targetName=zetachain-mainnet-etherscan&apikey=GAH6BHW1WXF3TNQ4AH3G44B7BWVVKPKSV5

Zengo

Package Name: com.zengo.wallet

Wallet Findings:

1. \data\data\com.zengo.wallet\databases\RKStorage
   a. User attributes, email address


```
{
  "UserAttributes": [
    {
      "Name": "sub",
      "Value": "f0ed82ef-f933-40df-b3a9-17f36d14c90f"
    },
    {
      "Name": "email_verified",
      "Value": "true"
    },
    {
      "Name": "locale",
      "Value": "en-US"
    },
    {
      "Name": "email",
      "Value": "clvb333@gmail.com"
    }
  ],
  "Username": "f0ed82ef-f933-40df-b3a9-17f36d14c90f"
}
```


   b. User Account Balance

{"userInfo":{"anonymousId":"f90ddd7c-3b29-44bf-99a5-a817221c40a5","userId":"f0ed82ef-f933-40df-b3a9-17f36d14c90f","traits":{"Email":"clvb333@gmail.com","Backup status":"Backed up","Local currency":"USD","Amount Staked":0,"Amount lending":0,"Notification status":"Disabled","Current balance":"0.000000000000000000000000000000"}}}

2. \data\data\com.zengo.wallet\shared_prefs\react-native.xml


```
<map>
  <string name="seenCashbackUnlockedDialog">false</string>
  <string name="hasFaceMap">false</string>
  <string name="hasAdditionalFaceMap">false</string>
  <string name="earnableAssets">[{"symbol":"XTZ","earningMethods":[{"type":"Staking","providers":[{"name":"Figment Network","savingsAddress":"tz1Scdr2HsZiQjc7bHMeBbmDRXYVvdhjJbBh","
  <string name="accountCreationDateForV23AndUpUser">1722980921173</string>
  <string name="isLaunching">true</string>
  <string name="ignoreInitialSupportMessage">false</string>
  <string name="didRequestNotificationPermission">true</string>
  <string name="userReferralCode">"ZENIKPU5"</string>
  <string name="deviceId">3cdaae0b2335bd9278893dd113271fbb1c90d63bbef8974ab7cf70b57e843fa0</string>
  <string name="backupStatus">[["googleDrive",{"fileStatus":"verified","account":"clvb333@gmail.com","lastVerified":"2024-08-08T16:10:36.157Z"}]]</string>
  <string name="backupGoogleDriveFileId">1RgtE0D_6Cq7fnxPJUs68_DRE14mucSPI</string>
  <string name="numReferralPending">0</string>
  <string name="totalReferralEarnings">0</string>
  <string name="backupGooglePendingFileIdSync">false</string>
  <string name="magicLinkEmail">clvb333@gmail.com</string>
  <string name="masterKeyIID">df843eaf-7a08-4a61-baf9-1d2f8af42a99</string>
  <string name="isSignedIn">true</string>
  <string name="totalUserBalanceState">{"totalFiatValue":"0.000000000000000000000000000000","totalFiatValueLocalCurrency":0,"fiatSymbol":"USD","timestamp":1723134340848}</string>
```

3. \data\data\com.zengo.wallet\cache\purchasely\user_attributes.json
    a. [{"key":"registration_date","value":"2024-08-06T21:48:41Z","type":"Date"}]

4. \data\data\com.zengo.wallet\files\AdjustIoActivityState
    a. UUID: 282f2301-b215-4be7-ab56-c1a9f5908a57

5. \data\data\com.zengo.wallet\app_webview/pref_store
    a. {"aw_metrics_app_package_name_logging_rule_last_update":"13367606641798788","uninstall_metrics":{"installation_date2":"1723133041"},"user_experience_metrics":{"client_id2":"cf553be1-fbab-4961-9d9e-39244a8eb585","client_id_timestamp":"1723133041","low_entropy_source3":5289,"session_id":1,"stability":{"launch_count":1,"page_load_count":19,"renderer_launch_count":1}},"variations_country":"us","variations_last_fetch_time":"13367595190674000","variations_permanent_consistency_country":["103.0.5060.71","us"],"variations_seed_date":"13367595190674000"}

6. \data\user\0\com.zengo.wallet\cache\http-cache/b8622c639ae193dbac4f4dda9c94a772.1\b8622c639ae193dbac4f4dda9c94a772.1\0
    a. BEGIN PUBLIC KEY-----\nMFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAESND9gpoSfhOBq4nxb/gghyViiR6yIsoc\nkAJOFFHSo4eOwg5b77iwTPV784aJyZ1VerGDIONzqliPgaKia5hHzg==\n-----END PUBLIC KEY

7. \data\data\com.zengo.wallet\cache\http-cache\dc90777a02e1edeb49602568cf060b64.1\dc90777a02e1edeb49602568cf060b64.1\0
    a. [0, "https://buy.moonpay.com?apiKey=pk_live_dvi5zCdeC76Jrnhk7usngGhU3mC39Nk&externalCustomerId=f0ed82ef-f933-40df-b3a9-17f36d14c90f&colorCode=%2335c4ba&currencyCode=doge&walletAddress=DLqNST7bWzvMPERsKvYFrJQdEHbmJgEPf3&feeBreakdown=false&enabledPaymentMethods=credit_debit_card%2Capple_pay%2Cgoogle_pay%2Csamsung_pay%2Csepa_bank_transfer%2Cgbp_bank_transfer%2Cgbp_open_banking_payment&email=clvb333%40gmail.com&signature=YWyi3VVCiPVDrimbkTKu%2BOCcJDzDPFT3FpYADTKHttY%3D"
    b. [0, "https://buy.moonpay.com?apiKey=pk_live_dvi5zCdeC76Jrnhk7usngGhU3mC39Nk&externalCustomerId=f0ed82ef-f933-40df-b3a9-17f36d14c90f&colorCode=%2335c4ba&currencyCode=btc&walletAddress=36J27V2E3Dw8gksn7zarUj1Qu6ymAkhpfj&feeBreakdown=false&enabledPaymentMethods=credit_debit_card%2Capple_pay%2Cgoogle_pay%2Csamsung_pay%2Csepa_bank_transfer%2Cgbp_bank_transfer%2Cgbp_open_banking_payment&email=clvb333%40gmail.com&signature=CWsh%2FkbDUmRfxddl4UAUk5eGgivfz6oUw2x2yOkUOzQ%3D"

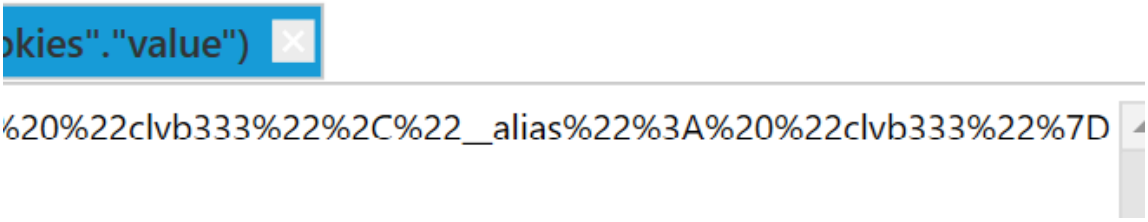
8. \data\data\com.zengo.wallet\cache\WebView\Default\HTTP Cache\Cache_Data\0f418e80fb6f11ba_0
    a. https://buy.moonpay.com/?apiKey=pk_live_dvi5zCdeC76Jrnhk7usngGhU3mC39Nk&externalCustomerId=f0ed82ef-f933-40df-b3a9-17f36d14c90f&colorCode=%2335c4ba&currencyCode=doge&walletAddress=DLqNST7bWzvMPERsKvYFrJQdEHbmJgEPf3&feeBreakdown=false&enabledPaymentMethods=credit_debit_card%2Capple_pay%2Cgoogle_pay%2Csamsung_pay%2Csepa_bank_transfer%2Cgbp_bank_transfer%2Cgbp_open_banking_payment&email=clvb333%40gmail.com&signature=YWyi3VVCiPVDrimbkTKu%2BOCcJDzDPFT3FpYADTKHttY%3D

eToro

Package Name: com.etoro.wallet

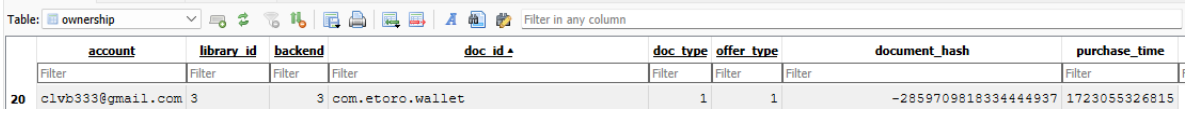
Wallet Findings:

1. \data\data\com.etoro.wallet\app_webview\Default\Cookies
   a. user email address



2. Username: \data\user\0\com.etoro.wallet\app_webview\Default\Local Storage\leveldb\000003.log
   a. 

3. Last application login timestamp: \data\data\com.etoro.wallet\app_webview\last-exit-info
   a. {"exitInfoPid":32314,"timestampAtLastRecordingInMillis":1723677961996,"app State":2}
   b. $initial_referrer":"$direct","$initial_referring_domain":"$direct","$user_id":"clvb 333","Application":" walletAndroid","AppVersion":"77.0.1","page":"/create-wallet","token":"dbbd7bd9566da85f012f7ca5d8c6c944"}}}](_https://www.etoro. com

4. Installed date: \data\data\com.android.vending\databases\library.db
   a. 

5. \data\user\0\com.etoro.wallet\cache\WebView\Default\HTTP Cache\Cache_Data\7014620de1d761c3_0
    a. https://www.etoro.com/api/wallet/v1/cryptos/metadata?includeErc20=true&client_request_id=cd51735d-e583-442e-b417-5c4d8e455534&session_guid=7e632041-54fa-4bb9-817a-79d18f00700d&user_session=48485b38-3440-4374-b6b5-8d4aec3718d8

Guarda

Package Name: com.crypto.multiwallet

Wallet Findings:

1. \data\data\com.crypto.multiwallet\databases\RKStorage
    a. Password, wallet, private key, seed phrase


```
"mnemonic": "soda wheat black jump flash actress weasel grant arena cinnamon bird story",
"last-update-time": 1723682099108,
"version": 50,
"autobackup-setting": 0,
"uuid": "0GX7M5eN9opkRgroEpbLU7sMIvVpZx9IK1hi",
"session-timeout": ""
```


    b. {\"address\":\"1K5PmcEpx5pnMz92oSfMn9fxeqpJ3XZtci\",\"privateKey\":\"KxJFhoEFfCP91BBPTzxG4LFfGV5CSHfYbpzTFo6MmT49Jj5eufSJ\",\"publicKey\":\"033e32b612071d3937a3fe64ae58dbe703952f7208714b7339293b6320aa17d36a\",\"balance\":\"0\",\"currency\":\"btc\",\"title\":\"Bitcoin\",\"uuid\":\"sok2zZqErH8b\",\"derivedFromMnemonicUsing\":{\"accountIndex\":0}

    c. backup": "{\"type\":\"decrypted\",\"masterPassword\":\"0fdca547cab0e9535f466fdd50d7cc59(tXntTbJFzh]4EuQVmjzM9GXHCth8\",\"data\":{\"walletsByUuids\":{\"8_wzAqrwWJXT\":{\"address\":\"bnb1zt4g8vy9a8wrm0zhtypvl5dxpmd86m83ymkwhk\",\"privateKey\":\"61f816ef20b60f78e18317eeb476665bbcad678afbea1ebdf1155820e1e18389\",\"balance\":\"0\",\"currency\":\"bnb\",\"title\":\"Binance Coin\",\"uuid\":\"8_wzAqrwWJXT\",\"derivedFromMnemonicUsing\":{\"accountIndex\":0},\"subWallets\":[{\"isFakeToken\":true,\"uuid\":\"BwDt3aFN2qMC\",\"currency\":\"ava-645\",\"address\":\"bnb1zt4g8vy9a8wrm0zhtypvl5dxpmd86m83ymkwhk\",\"precision\":8,\"title\":\"Travala\",\"family\":\"bnb\",\"privateKey\":\"61f816ef20b60f78e18317eeb476665bbcad678afbea1ebdf1155820e1e18389\",\"parentUuid\":\"8_wzAqrwWJXT\",\"smartContract\":\"ava-645\",\"balance\":\"0\",\"subWallets\":[]},{\"isFakeToken\":true,\"uuid\":\"nVr_lSwgYZ5v\",\"currency\":\"now\",\"address\":\"bnb1zt4g8vy9a8wrm0zhtypvl5dxpmd86m83ymkwhk\",\"precision\":8,\"title\":\"ChangeNOW Token\",\"family\":\"bnb\",\"privateKey\":\"61f816ef20b60f78e18317eeb476665bbcad678afbea1ebdf1155820e1e18389

2. Application UUID \data\data\com.crypto.multiwallet\files\.com.google.firebase.crashlytics.files.v2:com.cryp

to.multiwallet\open-sessions\66BD4CF1013700012FDD8A14E11ADBFF\native\app.json

   a. 6f7bb0743c164ce7941265206160eedb

3. \data\data\com.crypto.multiwallet\files/mmkv\mmkv.default
   a. mmkv-cache--440166755'&{"state":"loading","previous":"empty"}^mmkv-cache-209358152{"state":"cached","ttl":86400000,"createdAt":1723682101607,"data":{"data":{"lastUpdate":88915,"list":[{"id":"btc","ticker":"btc","family":"","contract":"","title":"Bitcoin","rate":58847.77454575762,"rank":1,"decimals":8},{"id":"eth","ticker":"eth","family":"","contract":"","title":"Ethereum","rate":2659.8265987122068,"rank":2,"decimals":18},{"id":"usdt:eth:0xdac17f958d2ee523a2206206994597c13d831ec7","ticker":"usdt","family":"eth","contract":"0xdac17f958d2ee523a2206206994597c13d831ec7","title":"Tether USDt","rate":1.0002533994769067,"rank":3,"decimals":6}

4. \data\data\com.crypto.multiwallet\cache\http-cache\0cd6ccf47c92ac61c87bd640e1efdd16.0
   a. https://tron.guarda.com/api/account?address=TA7khtsXLXVV8wATdmRGyPizxzL3yBr3wX

5. \data\user\0\com.crypto.multiwallet\cache\http-cache\5489863c42bdbee239d991d8a0cf3335.0
   a. https://ethbook.guarda.co/api/address/0xacd0fa3f01e5ce9d4d15809c78abb9252ec7a655

6. \data\data\com.crypto.multiwallet\cache\http-cache\9f14ac65cf54fb29b6252af5edfdd2ce.0
   a. https://bscbook.guarda.com/api/address/0xacd0fa3f01e5ce9d4d15809c78abb9252ec7a655?details=txs&pageSize=100&noHex=true

Phantom

Package Name: app.phantom

Wallet Findings:

1. Transaction data: \data\data\app.phantom\files\mmkv\mmkv.default
    a. ETH","imageUrl":"https://dhc7eusqrdwa0.cloudfront.net/assets/ethereum.png"},"decimals":18,"logoUri":"https://cdn.jsdelivr.net/gh/trustwallet/assets@master/blockchains/ethereum/assets/0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2/logo.png","name":"Ethereum","symbol":"ETH","coingeckoId":"ethereum","spamStatus":"VERIFIED","walletAddress":"0x961F79a2910cd641Dc6f7eF672561bA021C3b123","amount":"12351433857000"}},{"type":"BitcoinNative","data":{"chain":{"id":"bip122:000000000019d6689c085ae165831e93","name":"Bitcoin","symbol":"BTC","
    b. https://dhc7eusqrdwa0.cloudfront.net/assets/ethereum.png"},"decimals":18,"logoUri":"https://cdn.jsdelivr.net/gh/trustwallet/assets@master/blockchains/ethereum/assets/0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2/logo.png","name":"Ethereum","symbol":"ETH","coingeckoId":"ethereum","spamStatus":"VERIFIED","walletAddress":"0x961F79a2910cd641Dc6f7eF672561bA021C3b123","amount":"12351433857000"}},{"type":"BitcoinNative","data":{"chain":{"id":"bip122:000000000019d6689c085ae165831e93","name":"Bitcoin","symbol":"BTC","imageUrl":"https://dhc7eusqrdwa0.cloudfront.net/assets/bitcoin.png"},"decimals":8,"logoUri":"https://dhc7eusqrdwa0.cloudfront.net/assets/bitcoin.png","name":"Bitcoin","symbol":"BTC","coingeckoId":"bitcoin","spamStatus":"VERIFIED","walletAddress":"bc1q09qgar6py3est98y6qr5wfp068j2pezase37zx","amount":"0"}}

2. data\data\app.phantom\files\SQLite\simpleStorage.db

a. Wallet addresses

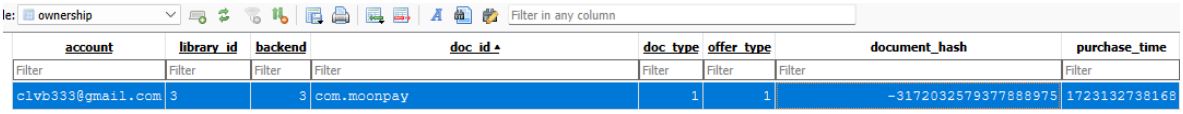

```
"version": 1,
"accounts": [
  {
    "version": 1,
    "type": "seed",
    "identifier": "4683be7e063f4ef86e08b038f1dc2f0527972756acea7fbd3f33c05c44c975ea",
    "seedIdentifier": "ad9de006c2ca52adb75e9640e793a531168897c5cda11f7fd54bcbd66c9b1c64",
    "derivationIndex": 0,
    "chains": {
      "solana": {
        "chainType": "solana",
        "pathType": "bip44Change",
        "publicKey": "6iwChzVqP2fG8v3RMhf9uu7tPhe8hJ55HCps7oEqCHzB"
      },
      "eip155": {
        "chainType": "eip155",
        "pathType": "bip44Ethereum",
        "publicKey": "0x961F79a2910cd641Dc6f7eF672561bA021C3b123"
      },
      "bip122_p2tr": {
        "chainType": "bip122_p2tr",
        "pathType": "bitcoinTaproot",
        "publicKey": {
          "type": "Buffer",
```


3. /LogicalFileSet1/AndroidFullyLoggedinCrypto-001.tar/data/data/app.phantom/no_backup/expo_installation_uuid.txt
    a. 6073c5bb-a803-4a1c-ab00-87d652260d51

MoonPay

Package name: com.moonpay

Wallet findings: Moonpay data is primarily found within the web cache data.

1. User data: Path \data\user\0\com.android.vending\databases\library.db
   a. 

account	library_id	backend	doc_id	doc_type	offer_type	document_hash	purchase_time
clvb333@gmail.com	3	3	com.moonpay	1	1	-3172032579377888975	1723132738168

2. User profile data: \data\data\com.android.chrome\app_chrome\Default\Local Storage\leveldb\000006.log
   a.

{"birthday":"[redacted]","createdAt":"2024-08-08T16:00:11.403Z","userCreationMonth":"202408","email":"clvb333@gmail.com","firstName":"[redacted]","lastName":"[redacted]","nationality":"USA","ipAddressCountryCode":"USA","ipAddressStateCode":"DC","accountId":"66b7fa3c-596c-4835-bea5-2a7d88b551e3","partner":"Phantom","partnerId":"66b7fa3c-596c-4835-bea5-2a7d88b551e3","partnerName":"Phantom","organizationId":"0aee56b8-49aa-4d5a-9239-28e444e07f6c","organizationName":"Phantom","branch":"master","platform":"Widget","Release":"0.1.0-bda09a9.202408141228","iframeParent":"Iframe not detected","subflow":"BuyPrincipal","flow":"buy","transactionType":"Buy","anonymousId":"e85f733a-fcc8-416e-83d3-6efc8efe3bfa","screenName":"Login Form (Enter email verification code)","baseCurrencyCode":"usd","quoteCurrencyCode":"btc","baseCurrencyAmount":39.55,"quoteCurrencyAmount":0.00065,"totalAmount":40,"networkFeeAmount":0.15,"feeAmount":0,"extraFeeAmount":0.3,"emailVerificationRequired":false,"isReturningCustomer":true}

3. Web History Artifact
   a. Date Accessed : 2024-08-14 23:05:07 EDT
      URL :
      https://buy.moonpay.com/?apiKey=pk_live_g3KLHBinccCUh1j2eXWng19TFuqcItWC&enabledPayments=credit_debit_card%2Capple_pay%2Cgoogle_pay%2C

samsung_pay%2Csepa_bank_transfer%2Cgbp_bank_transfer%2Cgbp_open_banking_payment&colorCode=%234E44CE&
walletAddresses=%7B%22btc%22%3A%22bc1qae8r5zcel2k4gyjetcps70tfg3qqn2e3z5qqtg%22%7D&defaultCurrencyCode=btc&baseCurrencyAmount=40&signature=yBChLx%2B5ng9cWAoV8m1jvdepiOZo8%2Bj%2FGKLv5g0f2Ag%3D
Title : MoonPay
Comment : Chrome History

Rainbow

Package Name: me.rainbow

Wallet Findings:

1. Wallet address and balance:
   Path: \data\data\me.rainbow\files\mmkv\rainbowKeychainLocalStorage

   a. "version":1,"wallets":{"wallet_1723127327795":{"addresses":[{"address":"0x593B26F0c7688aA0c98e8C9C69D675299dECAcad","

      {"state":{"associatedWalletAddress":"0x593B26F0c7688aA0c98e8C9C69D675299dECAcad","chainBalances":[[1,0.4510614255],[8453,0],[10,0],[42161,0],[137,0],[7777777,0],[81457,0],[666666666,0],[43114,0],[56,0]],"idsByChain":[[1,["eth_1"]],[8453,[]],[10,[]],[42161,[]],[137,[]],[7777777,[]],[81457,[]],[666666666,[]],[43114,[]],[56,[]],["all",["eth_1"]]],"userAssets":[["eth_1",{"address":"eth","uniqueId":"eth_1","chainId":1,"chainName":"mainnet","mainnetAddress":"eth","isNativeAsset":true,"native":{"price":{"change":"3.61%","amount":2485.05,"display":"$2,485.05"},"balance":{"amount":"0.4510614255","display":"$0.45"}},"name":"Ethereum","price":{"value":2485.05,"changed_at":1723130115,"relative_change_24h":3.614121257353964},"symbol":"ETH","type":"native","decimals":18,"icon_url":"https://rainbowme-res.cloudinary.

2. \data\data\me.rainbow\files\mmkv\mmkv.default
   a. [ÿÿÿ
      hidden-coins-obj-null{}pinned-coins-obj-null{}7pinned-coins-0x593B26F0c7688aA0c98e8C9C69D675299dECAcad["undefined_mainnet"]7hidden-coins-0x593B26F0c7688aA0c98e8C9C69D675299dECAcad[];hidden-coins-obj-0x593B26F0c7688aA0c98e8C9C69D675299dECAcad{};pinned-coins-obj-0x593B26F0c7688aA0c98e8C9C69D675299dECAcad{"undefined_mainnet":true}

3. data\data\me.rainbow\files\.com.google.firebase.crashlytics.files.v2:me.rainbow\open-sessions\66B4DB73010200013B7AA1E868FB8F26\native\app.json
   a. UUID: 8baf70600ede4cc9ada3093e9c6e6796
   b. \data\data\me.rainbow\app_webview\pref_store

Uninstall_metrics":{"installation_date2":"1723127155"},"user_experience_metrics":{"client_id2":"3e66970c-e339-4d75-83e4-217ed93b0428","client_id_timestamp":"1723127155","low_entropy_source3":6875,"session_id":1,"stability":{"launch_count":1,"page_load_count":0,"renderer_launch_count":0}},"variations_country":"us"

4. \data\data\me.rainbow\cache\sentry\401bcfcb4f16aaa63549e26396ff61f3422791db\.scope-cache\user.json
    a. {"id":"7vGOUuV0OaLGDmBqLn3-C","data":{"currentWalletAddress":"0x5f9a3e90f06794b93a9e16e4777a24ffedc6cd2bdc40ed76df82d3ce78b1dccc"}}

5. \data\misc\keystore\persistent.sqlite
    a.

rainbowAddressKey
rainbowAllWalletsKey
rainbowPinKey
rainbowSelectedWalletKey
reboot_escrow_key_store_encryption_key
signature_0x593B26F0c7688aA0c98e8C9C69D675299dECAcad

MetaMask

Package Name: io.metamask

Wallet Findings:

1. Wallet: \data\data\io.metamask\cache\WebView\Default\HTTP Cache\Cache_Data\35197e4d9453e19e_0
    a. https://account.api.cx.metamask.io/accounts/ 0xe33cab16ae3a5ce54698709793aa6319c9cd129f

2. \data\user\0\io.metamask\cache\WebView\Default\HTTP Cache\Cache_Data\0872b6e62e813712_0
    a. https://staking.api.cx.metamask.io/v1/staking/any-directly-staking/1? addresses=0xe33cab16ae3a5ce54698709793aa6319c9cd129f

3. \data\data\io.metamask\cache\WebView\Default\HTTP Cache\Cache_Data\2ad33e353f29b3bb_0
    a. https://staking.api.cx.metamask.io/v1/staking/any-directly-staking/1? addresses=0x23e028adaaa9235bfc711228457f8e63284df422,0xe33cab16ae3a5ce 54698709793aa6319c9cd129f

4. Wallet's: \data\data\io.metamask\app_webview\Default\LocalStorage\leveldb\000005.ldb
    a.

__type":"Map","value":[["e6aac86a63d",{"accoue7
["
0x23E028AdAAa9235BFc711228457F8E63284DF422"],"chainId":1,
id":
,"nam
etek
,injected","u
}}]]},6f
urrent":6)
,"va&(on":2},
E33CAb16Ae3A5cE54698709793Aa6319c9Cd129F"
'j3N_https://portfolio.metamask.io

5. Wallet addresses and balance: \data\user\0\io.metamask\files\persistStore\persist-root
    a.

Analysis Result 4,104
Score:
Likely Notable
Type:
Keyword Hits
Configuration:

Conclusion:

Keyword:
0xe33cab16ae3a5ce54698709793aa6319c9cd129f
Keyword Preview:
\":{\"accounts\":{\"«0xe33cab16ae3a5ce54698709793aa6319c9cd129f«\":{\"balance\":\"0x
Keyword Regular Expression:
0xE33CAb16Ae3A5cE54698709793Aa6319c9Cd129F
Keyword Search Type:
1
Analysis Result 4,105
Score:
Likely Notable
Type:
Keyword Hits
Configuration:

Conclusion:

Keyword:
0x23e028adaaa9235bfc711228457f8e63284df422
Keyword Preview:
"0x9b3f3e3f980\"},\"«0x23e028adaaa9235bfc711228457f8e63284df422«\":{\"balance\":\"0x
Keyword Regular Expression:
0x23E028AdAAa9235BFc711228457F8E63284DF422
Keyword Search Type:
1
Analysis Result 4,106
Score:
Likely Notable
Type:
Keyword Hits
Configuration:

Conclusion:

Keyword:
0x90ce182e80ac7ddb86d8f39635738929001ddcac
Keyword Preview:
55ee3a45cf044f\"},\"«0x90ce182e80ac7ddb86d8f39635738929001ddcac«\":{\"balance\":\"0x
Keyword Regular Expression:
0x90cE182E80AC7DDB86D8f39635738929001dDCAc
Keyword Search Type:

6. \data\data\io.metamask\cache\http-cache\45f004a609ad9b374b009282fd83e560.0
    a. https://api.etherscan.io/api?module=account&address=0x23e028adaaa9235bfc711228457f8e63284df422

7. \data\user\0\com.android.chrome\cache\Cache\Cache_Data\7db98ccfaee8fba6_0
    a. https://mercuryo.io https://exchange.mercuryo.io/?country_code=US&currency=ETH&fiat_currency=USD&fiat_amount=28&address=0xE33CAb16Ae3A5cE54698709793Aa6319c9Cd129F&merchant_transaction_id=0c6f730aa462a8635&redirect_url=metamask%3A%2F%2Fon-ramp%2Fproviders%2Fmercuryo&widget_id=b42c13c6-e5f9-4649-be86-f9cfd071ba34&payment_method=google&type=buy&fix_fiat_currency=true&fix_currency=true&fix_fiat_amount=true&fix_amount=true&fix_payment_method=true&network

=ETHEREUM&fix_network=ETHEREUM&partner_flow=metamask&signature
=e81135399916079443091008afee167924c25918e0187281cbbdaf006a8c3cb37c
138f72cd78f8657922a2308abdceec8d9da45ab974b0365626d03e63c1cf14&
hide_address=true

OKX

Package name: com.okinc.okex.gp

Wallet Findings:

1. \data\user\0\com.android.vending\databases\library.db
   a. clvb333@gmail.com | 3 | 3 | com.okinc.okex.gp

2. \data\data\io.horizontalsystems.bankwallet\databases\dbBankWallet
   a. > 0x6cc5f688a315f3dc28a7781717a9a798a59fda7b | OKEx

Gemini

Package name: com.gemini.android.app

Wallet Findings:

1. User data: \data\user\0\com.android.vending\databases\library.db
   a.

clvb333@gmail.com	3	3	com.gemini.android.app
clvb333@gmail.com	licensing	3	com.gemini.android.app

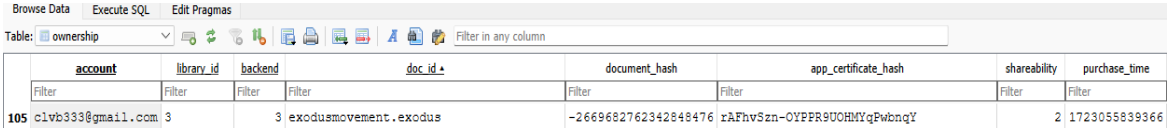
2. \data\data\io.horizontalsystems.bankwallet\databases\dbBankWallet
   a.

>	0x5f65f7b609678448494de4c87521cdf6cef1e932	Gemini

Exodus

Package Name: exodusmovement.exodus

Wallet Findings:

1. \data\data\com.android.vending\databases\library.db
   a. 

Browse Data | Execute SQL | Edit Pragmas

Table: ownership — Filter in any column

	account	library_id	backend	doc_id	document_hash	app_certificate_hash	shareability	purchase_time
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
105	clvb333@gmail.com	3	3	exodusmovement.exodus	-2669682762342848476	rAFhvSzn-OYPPR9UOHMYqPwbnqY	2	1723055839366