📖 ChainForensics App Guide

A complete guide to using the ChainForensics blockchain analysis dashboard.

📊 Dashboard Overview

When you first open ChainForensics, you'll see:

- **Header** - Shows connection status (green = connected, red = disconnected)
- **Sidebar** (left) - All input fields and action buttons
- **Stats Grid** (top right) - Real-time network information
- **Results Area** (main) - Where analysis results appear

📈 Stats Grid Explained

Stat	What It Shows
Block Height	Current Bitcoin blockchain height (how many blocks exist)
Network	Which network you're connected to (`main`, `test`, or `regtest`)
Sync Progress	How synced your Bitcoin node is (100% = fully synced)
API Status	Whether the ChainForensics API is responding
Electrs	Connection status to Electrs indexer (enables address lookups)

🔍 Transaction Analysis Section

Input Fields

Transaction ID (TXID)

The 64-character hexadecimal identifier for a Bitcoin transaction.

Example: `4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b`

Where to find it:

- Block explorers (mempool.space, blockstream.info)
- Your wallet's transaction history
- Payment receipts

Output Index (vout)

Every transaction can have multiple outputs (payments). The **vout** number identifies which specific output you want to analyze.

vout	Meaning
0	First output
1	Second output
2	Third output
...	And so on

Example: A transaction sends:

- 0.5 BTC to Address A (vout 0)
- 0.3 BTC to Address B (vout 1)
- 0.1 BTC to Address C (vout 2)

If you want to trace where the 0.3 BTC went, set **vout = 1**.

💡 **Tip:** If unsure, start with vout = 0. You can click "Analyze Transaction" first to see all outputs and their indices.

🔍 **Analyze Transaction Button**

What it does: Fetches complete transaction details from your Bitcoin node.

Output shows:

Field	Description
TXID	The transaction identifier
Block Height	Which block contains this transaction
Confirmations	How many blocks have been mined since (more = more secure)
Size	Transaction size in bytes and virtual bytes (vBytes)
Fee	Mining fee paid (in satoshis)
Total Output	Sum of all outputs in BTC
Inputs	Where the funds came FROM (previous transactions)
Outputs	Where the funds went TO (addresses and amounts)

🔎 UTXO Tracing Section

Direction Setting

Option	What It Does
Forward	Traces where the funds WENT (follows spending)
Backward	Traces where the funds CAME FROM (follows inputs to source)

Use Forward when: "I see coins arrived at this address - where did they go next?"

Use Backward when: "I see coins at this address - where did they originally come from?"

Max Depth Setting

Controls how many "hops" the tracer will follow.

Depth	Meaning
1	Only immediate next/previous transaction
5	Up to 5 transactions deep
10	Up to 10 transactions deep (default)
50	Maximum allowed

Example with Depth = 3:

```
Your TX → Hop 1 → Hop 2 → Hop 3 (stops here)
```

⚠️ WARNING: High Depth Values

Setting Max Depth too high can cause:

Issue	Why It Happens
Slow response	Each hop requires RPC calls to your node
Timeout errors	Request may take longer than allowed
Browser freeze	Too much data to display
Node strain	Heavy load on your Bitcoin node

Recommendations:

Scenario	Suggested Depth
Quick check	3-5
Normal analysis	10 (default)
Deep investigation	15-20
Maximum (use carefully)	30-50

💡 **Tip:** Start with depth 5-10. Only increase if you need to see further and the initial results came back quickly.

🔎 Trace UTXO Button

What it does: Follows the money trail forward or backward through the blockchain.

Output shows:

Field	Description
Transactions Found	Total number of transactions in the trace path
Unspent Outputs	How many endpoints still have unspent coins
CoinJoin Transactions	Number of privacy-mixing transactions detected
Execution Time	How long the trace took
Electrs Enabled	Whether enhanced forward tracing is available

Results Table:

Column	Meaning
Depth	How many hops from your starting transaction
TXID	Transaction identifier (truncated)
Value	Amount in BTC
Status	💰 Unspent, 📤 Spent, or ⛏️ Coinbase
CoinJoin	Probability this is a mixing transaction

Status Icons:

- 💰 **Unspent** - Coins are still at this address (end of trail)
- 📤 **Spent** - Coins moved to another transaction
- ⛏️ **Coinbase** - Mining reward (origin of new coins)

⚡ Quick Actions Section

🔀 Detect CoinJoin Button

What it does: Analyzes a single transaction to determine if it's a CoinJoin (privacy mixing) transaction.

Output shows:

Field	Description
Score	0-100% likelihood of being a CoinJoin
Protocol	Detected type (Whirlpool, Wasabi, JoinMarket, etc.)
Confidence	How certain the detection is
Input/Output Count	Number of participants
Matched Heuristics	Which patterns were detected

Score Interpretation:

Score	Badge	Meaning
70-100%	🔴 High	Almost certainly a CoinJoin
30-70%	🟡 Medium	Possibly a CoinJoin
0-30%	🟢 Low	Probably not a CoinJoin

🛡️ Privacy Score Button

What it does: Calculates an overall privacy rating for a specific UTXO.

Output shows:

Field	Description
Score	0-100 privacy rating
Rating	Good / Moderate / Poor
Summary	Plain English explanation
Privacy Factors	What's helping or hurting privacy
Recommendations	Suggestions to improve privacy

Privacy Factors:

- ✅ **Positive** (green) - Improves privacy (e.g., passed through CoinJoin)
- ❌ **Negative** (red) - Reduces privacy (e.g., address reuse, round amounts)

📊 Timeline View Button

What it does: Creates a visual timeline of how funds flowed over time.

Output shows:

- Chronological list of events
- Visual bars showing relative values
- CoinJoin events highlighted in red
- Total statistics

Event Types:

Icon	Type	Meaning
💰	Receive	Coins arrived and haven't moved
📤	Transfer	Coins moved to another address
🔀	CoinJoin	Passed through a mixing transaction
⛏️	Mining	Coinbase reward (newly created coins)

💼 Address Lookup Section

Input Field

Enter any valid Bitcoin address:

- **Legacy:** Starts with `1` (e.g., `1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2`)
- **P2SH:** Starts with `3` (e.g., `3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy`)
- **Bech32:** Starts with `bc1q` (e.g., `bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq`)
- **Taproot:** Starts with `bc1p` (e.g., `bc1p5d7rjq7g6rdk2yhzks9smlaqtedr4dekq08ge8ztwac72sfr9rusxg3297`)

💰 Get Balance & UTXOs Button

Requires: Electrs connection

What it does: Fetches complete address information including balance and all UTXOs.

Output shows:

Field	Description
Total Balance	Sum of all UTXOs at this address
Confirmed	Balance with at least 1 confirmation
Unconfirmed	Balance still in mempool
Transactions	Total transaction count
UTXOs	Number of unspent outputs
First/Last Seen	Block heights of activity

UTXO List: Each UTXO shows:

- Transaction ID and output index
- Confirmation status
- Value in BTC

🔬 Check Dust Attack Button

Requires: Electrs connection

What it does: Scans for suspicious tiny UTXOs that may be tracking attempts.

What is a Dust Attack? Attackers send tiny amounts (dust) to your address hoping you'll consolidate them with other coins, linking your addresses together.

Output shows:

Field	Description
Total UTXOs	All unspent outputs
Dust UTXOs	Count below threshold (default 1000 sats)
Suspicious Count	UTXOs that look like tracking attempts
Total Dust Value	Sum of all dust in satoshis

Warning Signs:

- ⚠️ Yellow/red warning if suspicious UTXOs found
- ✅ Green checkmark if address looks clean

If Dust is Found:

> ⚠️ **Do NOT consolidate these UTXOs with your other coins!** This will link your addresses together and compromise your privacy.

✓ Validate Address Button

What it does: Checks if an address is valid and identifies its type.

Output shows:

Field	Description
Valid	✓ or ✗
Type	P2PKH, P2SH, P2WPKH, P2WSH, P2TR
Network	mainnet, testnet, or regtest
SegWit	Whether it's a SegWit address
Witness Version	0 (SegWit v0) or 1 (Taproot)

Address Types Explained:

Type	Prefix	Description
P2PKH	1...	Legacy (oldest type)
P2SH	3...	Script hash (often multisig or wrapped SegWit)
P2WPKH	bc1q...	Native SegWit (recommended)
P2WSH	bc1q... (longer)	SegWit script hash
P2TR	bc1p...	Taproot (newest, best privacy)

🍺 Buy Me a Drink Button

Shows a popup with:

- QR code for Bitcoin donations
- Copyable Bitcoin address

- Thank you message

Your support helps development continue!

🔌 Electrs Features

Some features require Electrs to be connected:

Feature	Without Electrs	With Electrs
Transaction Analysis	✅ Works	✅ Works
Backward Tracing	✅ Works	✅ Works
Forward Tracing	⚠️ Limited (can't follow spent outputs)	✅ Full (follows spending chain)
Address Balance	❌ Not available	✅ Works
Address UTXOs	❌ Not available	✅ Works
Dust Attack Check	❌ Not available	✅ Works
Address Validation	✅ Works	✅ Works

Check Electrs Status: Look at the "Electrs" stat in the top grid.

💡 Tips & Best Practices

For Transaction Analysis

1. Always start by analyzing the transaction to understand its structure
2. Note which output (vout) contains the funds you want to trace
3. Check the CoinJoin score before deep tracing - CoinJoins break the trail

For Tracing

1. Start with low depth (5-10) and increase if needed
2. If you hit a CoinJoin, the trail becomes unreliable
3. Look for "Unspent" status to find where funds currently sit
4. Use backward tracing to find the original source

For Address Lookup

1. Validate addresses before sending funds
2. Check dust attacks periodically on addresses you publish
3. Prefer Taproot (bc1p) or Native SegWit (bc1q) addresses

For Privacy Analysis

1. Higher privacy scores are better
2. Multiple CoinJoin passes improve privacy
3. Avoid address reuse
4. Be cautious of round number amounts (they stand out)

⚠️ Common Errors

Error	Cause	Solution
"Transaction not found"	Invalid TXID or not in your node's index	Verify TXID, ensure `txindex=1` is enabled
"Connection refused"	API server not running	Run `docker compose up -d`
"Timeout"	Depth too high or node busy	Reduce Max Depth, wait and retry
"Electrs not available"	Electrs not configured or offline	Check Electrs settings in `.env`
"Invalid address"	Typo or wrong network	Double-check address, ensure correct network

---

🔐 Privacy Note

All analysis happens **locally on your network**:

- No data sent to external servers
- No tracking or logging
- Your queries are private
- Only your Bitcoin node is contacted

📚 Glossary

Term	Definition
UTXO	Unspent Transaction Output - a chunk of Bitcoin that hasn't been spent yet
TXID	Transaction Identifier - unique 64-character hash identifying a transaction
vout	Output index - which output in a transaction (0, 1, 2, etc.)
CoinJoin	Privacy technique that mixes coins from multiple users
Dust	Tiny amounts of Bitcoin (usually under 546-1000 satoshis)
Satoshi	Smallest Bitcoin unit (0.00000001 BTC = 1 satoshi)
Mempool	Waiting area for unconfirmed transactions
Confirmations	Number of blocks mined after a transaction's block
SegWit	Segregated Witness - newer transaction format, lower fees
Taproot	Latest Bitcoin upgrade - better privacy and efficiency

---

Happy tracing! 🔍