

GUMSHOE

BLOCKCHAIN FORENSICS

Blockchain Forensic Investigation Report

Cryptocurrency Tracing, Attribution and Asset Recovery Analysis

SAMPLE

FICTIONAL DATA — NOT A REAL CASE

CASE
GS-2610-0042

MATTER
Ellison / AurexTrade investment fraud

PREPARED FOR
Margaret A. Ellison (victim)

PREPARED BY
GumShoe

REPORT TYPE
Final

VERSION
v1.0 Final

DATE ISSUED
2026-10-16

DATA SNAPSHOT
2026-10-14 00:00 UTC

SAMPLE | CONFIDENTIAL | PREPARED AT THE REQUEST OF VICTIM AND COUNSEL

FRONT MATTER

Document Control

SAMPLE REPORT | FICTIONAL DATA

This is a **sample report**. Every person, case number, address, transaction, website, exchange, and platform in it is fictional and was created to show what a finished GumShoe report looks like. Any resemblance to real people or real blockchain addresses is coincidental. Real protocols and issuers (Tether, Circle, CCTP, Uniswap) are named only to illustrate method. Nothing in this sample should be acted on.

Report ID / Case	RPT-2610-0042-F1 / GS-2610-0042 / Ellison / AurexTrade investment fraud
Type, version, status	Final / v1.0 Final / Issued 2026-10-16
Classification	Confidential / Prepared at the request of the victim and her counsel
Prepared for	Margaret A. Ellison (victim) / Attorney: Dana Whitfield, Whitfield Recovery Law PLLC
Prepared by / reviewed by	GumShoe, License SAMPLE-000000 Peer review: Avery Lin, Senior Analyst, 2026-10-15
Data snapshot	2026-10-14 00:00 UTC / finalized heights: Tron 76,412,880; Ethereum 23,571,204; Arbitrum One 389,114,560
Engine and model	GumShoe 2026.10.2 / narrative model build 2026.10 (see Appendix D)
Evidence packet	PKT-2610-0042 / root hash 56a7b906436736b8 (Appendix C)
Report integrity	SHA-256 `54fabab4d9ed871eaca8d62a63c301b8c3dc2448b1b416090082bf3b0803f060`

Revision History

Version	Date	Author	Description of change	Approved by
v0.1	2026-10-09	Investigator	Initial draft after tracing and CCTP confirmation	
v0.2	2026-10-15	Investigator	Peer review edits; FIFO sensitivity added (7.4)	A. Lin
v1.0	2026-10-16	Investigator	Issued to victim and counsel	Investigator

Distribution

Recipient	Organization	Role	Format	Date provided
Margaret A. Ellison		Victim	PDF + packet	2026-10-16
Dana Whitfield	Whitfield Recovery Law PLLC	Victim's attorney	PDF + packet	2026-10-16
Det. R. Okafor	San Marcos Police Department	Investigating officer	PDF	Pending victim consent

SAMPLE
FICTIONAL DATA · NOT A REAL CASE

Contents

Important Notices 4
0 How to Read This Report 4
1 Executive Summary 6
2 Engagement and Scope 7
3 Background and Reported Incident 8
4 Methodology and Data Integrity 9
5 Subject Addresses and Entities 11
6 Transaction Timeline 13
7 Fund Flow Analysis 14
8 Clustering and Attribution 17
9 Swaps, Bridges and Cross-Chain Movement 17
10 Exchange Exposure 18
11 OSINT and Off-Chain Correlation 18
12 Sanctions Screening and Risk Indicators 19
13 Action Points, Recovery Steps and Monitoring 19
14 Limitations, Assumptions and Alternative Hypotheses 21
15 Conclusions 22
16 Investigator Certification 22
Appendix A: Case Action Log and Chain of Custody 24
Appendix B: Complete Transaction Ledger 25
Appendix C: Evidence Packet and Exhibit Index 27
Appendix D: AI Use Disclosure and Review Record 28
Appendix E: Glossary 29

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

READ FIRST

Important Notices

GumShoe is a donation-funded service that traces cryptocurrency lost to fraud. Its tracing platform is built by GhostKey Development and is not offered for sale. The following notices apply to this report and to every person who receives it.

Notice	Detail
No charge	Ms. Ellison was not charged for this trace, this report, the evidence packet, or the draft documents. GumShoe never charges a fee to "release" funds. Anyone asking for such a fee is not acting for GumShoe.
Your security	GumShoe will never ask for a recovery phrase, private key, password, or remote access to a device.
No guarantee of recovery	Tracing shows where funds went. Freezing or returning them depends on exchanges, stablecoin issuers, courts, and timing, none of which GumShoe controls.
Report to authorities	Reports on file: San Marcos Police Department case SMPD-26-SAMPLE-0193 (filed 2026-09-29); FBI IC3 complaint I26-SAMPLE-4417 (filed 2026-09-30).
Not legal advice	GumShoe is not a law firm. Draft legal documents in this packet are for Ms. Whitfield to review, adapt, and send.
Contact	admin@ghostkey.dev | gumshoe.ghostkey.dev/help

CONFIDENTIALITY NOTICE

This report and its exhibits are confidential. It contains analysis of public blockchain data together with non-public information supplied by the victim. If you received this document in error, notify admin@ghostkey.dev and destroy all copies.

EVIDENTIARY FRAMEWORK

0 How to Read This Report

This report keeps two kinds of statement apart. **Blockchain facts** (amounts, addresses, times, transaction hashes) come from the chain itself and anyone with access to the chain can reproduce them. **Attributed claims** are statements about who controls an address. They are always shown with the named source they came from, and they are never presented as blockchain facts. Every statement carries an evidentiary class, and every attributed claim also carries a confidence level.

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

Evidentiary Classification

Class	Definition	Typical basis
[VERIFIED]	Blockchain fact, or a record independently confirmed against primary data that any qualified examiner can reproduce.	Finalized on-chain data with a stored provider fingerprint.
[CORROBORATED]	Attributed claim supported by two or more independent named sources.	Exchange publication plus observed sweep to that exchange's wallet.
[INFERRED]	Result of applying a stated method to verified data. Open to alternative explanation.	Proportional allocation; single-source behavioral attribution.
[ALLEGED]	Asserted by a party and not yet tested against primary data.	Victim's account; screenshots supplied by the victim.
[UNVERIFIED]	Any claim without a named, assessable source.	Anonymous forum posts.

Attribution Confidence Scale

Level	Meaning
C5 Confirmed	Control established by legal process, self-disclosure, or signed message.
C4 High	Exchange's own published address list, or two independent named sources.
C3 Moderate	One reliable named source or a strong behavioral pattern.
C2 Low	Single heuristic or single unvetted source.
C1 Speculative	Lead only. Not relied on for any conclusion.

Conventions

- Body text uses reference IDs: `A-###` for addresses, `T-###` for transactions, `L-#` for reported losses. Full values are in Appendix B.
- All times are UTC. Block timestamps are authoritative.
- Figures derived from mixed funds carry their accounting method: `[PRO]` proportional (used in this case) or `[FIFO]` (sensitivity only).
- USDT and USDC are valued at $1.00. ETH is valued at $2,800.00, the Provider C one-minute close at the block time of T-005.
- Labels, attributions, classes, findings, actions, and conclusions were decided by the investigator. AI assistance was limited to drafting narrative text (Appendix D).

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

SECTION 1

1 Executive Summary

REPORTED LOSS	VERIFIED ON-CHAIN	AT EXCHANGE (MERIDEX)	FREEZABLE, UNSPENT
$190,000.00	$186,400.00	$86,673.68	$64,115.26

Bottom Line

Between August 4 and September 22, 2026, Ms. Ellison sent four payments worth $186,400.00 to deposit addresses supplied by an online trading platform called AurexTrade. All four payments are confirmed on-chain (F-1). The funds were pooled with payments from two other victims and then moved out in three directions (F-2, F-3).

$150,788.94 of Ms. Ellison's funds is at points where action can still be taken as of 2026-10-14 00:00 UTC: $86,673.68 reached deposit addresses at Meridex Exchange, a custodial exchange that can preserve the account (F-4), and $64,115.26 sits unspent in two addresses holding USDT and USDC, tokens whose issuers can freeze them (F-5). Neither balance had been frozen at the time of the snapshot. A further $35,421.06 was sent to an instant exchange service, where tracing visibility ends (F-6).

The most time-sensitive step is sending freeze requests to Tether and Circle for the two unspent balances, followed by a preservation request to Meridex. Drafts of all three are ready for Ms. Whitfield's review (Section 13.3). Recovery is not guaranteed, and the balances could move at any time.

Key Findings

ID	Finding	Class	Conf.	Support
F-1	Ms. Ellison's wallets A-001 and A-010 sent four payments totaling $186,400.00 to A-002 and A-011.	[VERIFIED]		T-001, T-003, T-005, T-009
F-2	All $134,600.00 in USDT sent to A-002 was forwarded to A-003, which also received $150,400.00 from two other victims.	[VERIFIED]		T-002, T-004, T-010 to T-014
F-3	A-002 is the AurexTrade deposit address shown to Ms. Ellison, and the same address was given to two other GumShoe intake victims.	[CORROBORATED]	C3	EX-002, EX-001; cases GS-2609-0031, GS-2610-0038
F-4	$86,673.68 of the victim's funds reached Meridex Exchange deposit addresses A-004 and A-013 [PRO].	[CORROBORATED]	C4	T-015, T-016, T-020, T-021; EX-009
F-5	$64,115.26 of the victim's funds remains unspent as USDT at A-005 and USDC at A-012 [PRO]; neither was frozen at snapshot.	[VERIFIED]		T-017, T-008, T-020; issuer status read
F-6	$35,421.06 of the victim's funds was sent through A-006 to a Kestrel Swap deposit address, after which it could not be traced [PRO].	[INFERRED]	C3	T-018, T-019; EX-011
F-7	The victim's ETH was swapped to USDC and bridged to Arbitrum One through Circle CCTP within 41 minutes of receipt.	[VERIFIED]		T-005 to T-008

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

Immediate Actions

1. Freeze request to Tether for A-005. 2. Freeze request to Circle for A-012. 3. Preservation request to Meridex for A-004 and A-013. 4. Provide this report to SMPD and IC3. Detail in Section 13.

SECTION 2

2 Engagement and Scope

2.1 Engagement

Victim / client	Margaret A. Ellison, San Marcos, Texas (victim)
Contact	Phone (512) 555-0147 / m.ellison.sample@example.com (fictional)
Attorney	Dana Whitfield, Whitfield Recovery Law PLLC, Austin, Texas
Case accepted	2026-10-01
Intake channel	gumshoe.ghostkey.dev/help form, submitted 2026-09-30
Secure follow-up	Further details and files collected through a private, encrypted link issued 2026-10-01
Fee	None. GumShoe is donation-funded and victims are not charged.
Purpose	Recovery support and law enforcement referral

2.2 Scope

Chains in scope	Tron, Ethereum, Arbitrum One
Assets in scope	USDT (TRC-20), ETH, USDC (ERC-20 and Arbitrum native)
Time window	2026-08-01 00:00 UTC to 2026-10-14 00:00 UTC
Seeds	2 victim addresses (A-001, A-010) and 4 loss transactions (T-001, T-003, T-005, T-009)
Hop depth limit / threshold	8 hops / $500.00
Victims in scheme	3 known to GumShoe (allocation in Section 7.5)
Out of scope	Victim's Coinvault account activity other than withdrawals; network fees paid in TRX; activity after the snapshot

2.3 Questions Presented

#	Question	Answered in
Q1	Where did the funds Ms. Ellison sent go?	C-1; Sections 6, 7
Q2	Are any of those funds at a point where they can be frozen or preserved?	C-2; Section 13
Q3	What can be said about who received the funds?	C-3; Sections 5, 8
Q4	Is Ms. Ellison's loss connected to other reported victims?	C-4; Sections 7.5, 12

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

SECTION 3

3 Background and Reported Incident

EVIDENTIARY STATUS

Content in this section comes from Ms. Ellison's intake and supplied materials. Unless marked otherwise it is [ALLEGED] and frames the analysis. It is not a finding.

3.1 Intake Summary

Website or app used	AurexTrade, aurextrade-pro.example (archived 2026-10-03, EX-006)
Contact method	Language-exchange app, then WhatsApp with a contact using the name "Daniel Hsu"
Receiving addresses supplied	A-002 (Tron, USDT) and A-011 (Ethereum, ETH), copied from the platform's deposit page
Transaction IDs supplied	4 of 5 payments (L-1 to L-4); none supplied for L-5
First contact / last payment	2026-07-08 / 2026-09-29 (as reported)
Fraud type (investigator)	Investment platform, relationship-initiated

3.2 Incident Narrative

Ms. Ellison reports that in early July 2026 she was contacted on a language-exchange app by a man who called himself Daniel Hsu and said he worked in import logistics. After about two weeks the conversation moved to WhatsApp. She reports that he described profits he was making on a trading platform called AurexTrade and, on July 20, walked her through opening an account.

The victim reports that she bought USDT and ETH on her own Coinvault exchange account, withdrew them to her personal wallets, and sent them to the deposit addresses shown on the AurexTrade site. The AurexTrade dashboard showed her balance growing to more than $410,000. When she asked to withdraw in mid-September, she was told she must first pay an 18% "withdrawal tax." She reports paying this on September 22 (L-4) and then a further $3,600 "account unlock fee" on September 29 (L-5). No withdrawal was ever received. Contact with "Daniel" stopped on October 2.

Ms. Ellison reported the matter to the San Marcos Police Department on September 29 and to the FBI's IC3 on September 30, and contacted GumShoe through the online help form the same day.

3.3 Reported Loss Transactions

Ref	Date (UTC)	Chain / Asset	Amount	Value	Tx	Status
L-1	2026-08-04	Tron / USDT	25,000.00	$25,000.00	T-001	[VERIFIED]
L-2	2026-08-19	Tron / USDT	48,000.00	$48,000.00	T-003	[VERIFIED]
L-3	2026-09-06	Ethereum / ETH	18.50	$51,800.00	T-005	[VERIFIED]
L-4	2026-09-22	Tron / USDT	61,600.00	$61,600.00	T-009	[VERIFIED]
L-5	2026-09-29	Tron / USDT	3,600.00	$3,600.00	Not located	[ALLEGED]

SAMPLE
FICTIONAL DATA — NOT A REAL CASE

Reconciliation: victim-reported total $190,000.00 vs. on-chain verified total $186,400.00. Variance $3,600.00. The variance is L-5. No transfer of that amount left A-001 or A-010 on or near September 29, and Ms. Ellison's Coinvault statement (EX-004) shows a $3,600 USDT purchase on that date withdrawn to an address she does not recognize. She may have pasted an address supplied in the chat directly into Coinvault. A follow-up request for the Coinvault withdrawal record is open; L-5 is excluded from all figures until it is located.

3.4 Materials Received

Exhibit	Description	Provided by	Received	SHA-256
EX-001	Intake form and written statement	Victim	2026-09-30	`ee8d66e0407e...`
EX-002	AurexTrade dashboard and deposit page screenshots (14 images)	Victim	2026-10-01	`b79a9403d15c...`
EX-003	WhatsApp chat export with "Daniel Hsu"	Victim	2026-10-01	`f10e7be924e5...`
EX-004	Coinvault account statements, July to September 2026	Victim	2026-10-02	`92b4d974c980...`
EX-005	SMPD report and IC3 complaint confirmation	Victim	2026-10-02	`c8ab0fa12e5b...`

SECTION 4

4 Methodology and Data Integrity

4.1 Process

- **Intake.** Receiving addresses, transaction IDs, the website used, and Ms. Ellison's account were recorded. Each supplied transaction was confirmed on-chain before use as a seed.
- **Following funds.** Funds were traced from each payment through every address, one token swap, and one bridge until they came to rest or visibility was lost.
- **Identifying action points.** Unspent USDT and USDC balances and deposits to a custodial exchange were flagged (Section 13).
- **Evidence delivery.** This report and a signed, hash-chained evidence packet were produced (Appendix C).
- **Attorney support.** Two freeze requests, one preservation request, and one subpoena exhibit were drafted for attorney review (Section 13.3).

4.2 Supported Chains and Data Finality

Chain	Data providers	Finality rule applied	Finalized height at snapshot
Tron	Provider A (full node); Provider B (indexer)	Solidified block (19 SR confirmations)	76,412,880
Ethereum	Provider A (archive node); Provider B (indexer)	Finalized checkpoint	23,571,204
Arbitrum One	Provider A (archive node); Provider B (indexer)	Batch finalized on Ethereum	389,114,560

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

4.3 Blockchain Facts and Provenance

Each of the 21 transactions in Appendix B carries the SHA-256 fingerprint of the raw provider response it was read from. The responses are stored unmodified in the evidence packet (EX-008).

4.4 Second-Source Cross-Check

Primary / second source	Provider A / Provider B
Transactions cross-checked	21 of 21
Disagreements recorded	1

Tx	Field	Primary value	Second-source value	Resolution	By
T-016	Block time	2026-09-25 09:40:10	2026-09-25 09:40:13	Raw block header confirms primary value; Provider B indexes receipt time.	Investigator

4.5 Accounting Method for Mixed Funds

Ms. Ellison's USDT was mixed at A-003 with payments from two other victims. This case applies the **proportional** method [PRO]: each outflow from A-003 carries her funds in proportion to her share of the pool ($134,600.00 of $285,000.00, 47.23%). The investigator chose this method because all three victims' funds were pooled before any outflow, nothing on-chain indicates an order of use, and the method treats all three victims alike. A FIFO comparison is shown in Section 7.4. Her ETH path was not mixed with other funds and is traced in full.

4.6 Swaps, Bridges and Supporting Heuristics

Technique	How it was handled in this case	Resulting class
Token swap	T-006: ETH to USDC on Uniswap v3, detected from the transaction's own swap event.	VERIFIED
Circle CCTP bridge	T-007 deposit read from the bridge record; arrival T-008 on Arbitrum One proposed by GumShoe and confirmed by the investigator on 2026-10-09 (matching message hash and amount).	VERIFIED
Exchange sweep	A-004 and A-013 each swept to a published Meridex wallet within 25 minutes.	CORROBORATED
Clustering	No common-input heuristics apply (account-model chains). A-003 and A-006 linked by direct transfer only.	INFERRED

4.7 Tools and Data Sources

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

Source	Type	Version / access	Used for
GumShoe	Tracing platform	2026.10.2	Tracing, graph, allocation, report
Provider A	Node RPC	Accessed 2026-10-01 to 10-14	Primary chain data
Provider B	Indexer API	Accessed 2026-10-01 to 10-14	Second-source cross-check
GumShoe exchange address DB	Published deposit addresses	Release 2026.10.1	Exchange identification
OFAC SDN list	Sanctions list	Version dated 2026-10-13	Sanctions screening
Provider C	Price data	One-minute close	ETH valuation

4.8 Standards and Reproducibility

Evidence handling follows ISO/IEC 27037 and NIST SP 800-86, adapted for public ledger data. 102 case actions were written to the append-only, hash-chained case log (Appendix A). Observations are pinned to the finalized heights in Section 4.2.

SECTION 5

5 Subject Addresses and Entities

5.1 Address Register

Ref	Chain	Role	Attributed claim	Named source	Conf. / Class
A-001	Tron	Victim	Ms. Ellison's self-custody wallet	Victim; Coinvault withdrawals (EX-004)	C4 [CORROBORATED]
A-002	Tron	Receiving	AurexTrade deposit address	EX-002; two other victims' intake	C3 [CORROBORATED]
A-003	Tron	Consolidation	Controlled by AurexTrade operators	Direct receipt from A-002 only	C2 [INFERRED]
A-004	Tron	Exchange deposit	Meridex Exchange customer deposit	Meridex publication (EX-009); sweep T-016	C4 [CORROBORATED]
A-005	Tron	Intermediary	None		[VERIFIED] balance
A-006	Tron	Intermediary	Controlled by AurexTrade operators	Direct receipt from A-003 only	C2 [INFERRED]
A-007	Tron	Exchange wallet	Meridex Exchange hot wallet	Meridex publication (EX-009)	C4 [CORROBORATED]
A-008	Tron	Swap / Protocol	Kestrel Swap deposit address	Kestrel deposit page capture (EX-011)	C3 [INFERRED]
A-010	Ethereum	Victim	Ms. Ellison's Ethereum wallet	Victim; Coinvault withdrawals (EX-004)	C4 [CORROBORATED]
A-011	Ethereum	Receiving	AurexTrade ETH deposit address	EX-002 only	C2 [ALLEGED]
A-012	Arbitrum One	Intermediary	None		[VERIFIED] balance

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

Ref	Chain	Role	Attributed claim	Named source	Conf. / Class
A-013	Arbitrum One	Exchange deposit	Meridex Exchange customer deposit	Meridex publication (EX-009); sweep T-021	C4 [CORROBORATED]
A-014	Arbitrum One	Exchange wallet	Meridex Exchange hot wallet	Meridex publication (EX-009)	C4 [CORROBORATED]
A-020	Tron	Victim	Victim V-2 (case GS-2609-0031)	GumShoe intake	C4 [CORROBORATED]
A-021	Tron	Victim	Victim V-3 (case GS-2610-0038)	GumShoe intake	C4 [CORROBORATED]

Full addresses are listed in Appendix B.2. "None" means no attributed claim is made about who controls the address.

5.2 Entity Profiles

Entity	**AurexTrade operators** (Fraudulent trading platform (attributed))
Associated addresses	A-002, A-003, A-006, A-011
Activity window	2026-08-01 to 2026-09-30
Volume	$336,800.00 in / $336,610.00 out
Attribution and source	Deposit addresses shown on the platform (EX-002); same Tron deposit address reported by two other victims
Confidence / class	C3 / [CORROBORATED]
Narrative	The AurexTrade website displayed A-002 and A-011 as deposit addresses for Ms. Ellison's account. Two other victims who contacted GumShoe independently were shown A-002. A-003 and A-006 are included only because they received funds directly from A-002 and A-003; no other link to the operators is claimed. No individual has been identified.

Entity	**Meridex Exchange (fictional)** (Custodial exchange)
Associated addresses	A-004, A-007, A-013, A-014
Activity window	2026-09-09 to 2026-09-25
Volume	$150,000.00 received from subject addresses
Attribution and source	Meridex's own published deposit and wallet address list (EX-009); both deposits swept to published Meridex wallets
Confidence / class	C4 / [CORROBORATED]
Narrative	A-004 and A-013 appear in Meridex's published list of customer deposit addresses, and each forwarded its full balance to a published Meridex hot wallet within 25 minutes. Meridex is treated as a service, not a subject. The account holder behind these deposits is the subject of interest.

SAMPLE
FICTIONAL DATA FOR THIS CASE

Entity	**Kestrel Swap (fictional)** (Instant exchange service)
Associated addresses	A-008
Activity window	2026-09-30
Volume	$75,000.00 received from A-006
Attribution and source	Deposit address shown on Kestrel Swap's public order page (EX-011)
Confidence / class	C3 / [INFERRED]
Narrative	A-008 matches the deposit address format and sweep pattern shown on a captured Kestrel Swap order page. Kestrel Swap publishes no address list and has no known compliance contact. Output of the exchange could not be traced.

SECTION 6

6 Transaction Timeline

Material events across all chains in scope. The complete ledger is in Appendix B.

Time (UTC)	Ref	Event	From	To	Amount	Class
2026-08-01 10:02	T-011	Victim V-2 pays 92,000 USDT to A-002	A-020	A-002	92,000 USDT	[VERIFIED]
2026-08-04 15:22	T-001	**L-1:** Ms. Ellison pays A-002; forwarded to A-003 within 10 minutes (T-002)	A-001	A-002	25,000 USDT	[VERIFIED]
2026-08-19 14:05	T-003	**L-2:** Ms. Ellison pays A-002; forwarded to A-003 (T-004)	A-001	A-002	48,000 USDT	[VERIFIED]
2026-09-02 08:44	T-013	Victim V-3 pays A-002; forwarded to A-003 (T-014)	A-021	A-002	58,400 USDT	[VERIFIED]
2026-09-06 16:40	T-005	**L-3:** Ms. Ellison pays 18.5 ETH to A-011	A-010	A-011	18.5 ETH	[VERIFIED]
2026-09-06 16:52	T-006	A-011 swaps the ETH for USDC on Uniswap v3	A-011	A-011	51,610 USDC	[VERIFIED]
2026-09-06 17:03	T-007/008	USDC bridged to Arbitrum One via CCTP, arriving 17:21	A-011	A-012	51,610 USDC	[VERIFIED]
2026-09-09 11:26	T-020	A-012 sends USDC to a Meridex deposit address; swept 11:48	A-012	A-013	30,000 USDC	[VERIFIED]
2026-09-22 13:47	T-009	**L-4:** Ms. Ellison pays "withdrawal tax"; forwarded (T-010)	A-001	A-002	61,600 USDT	[VERIFIED]
2026-09-25 09:14	T-015	A-003 sends to a Meridex deposit address; swept 09:40	A-003	A-004	120,000 USDT	[VERIFIED]
2026-09-27 22:08	T-017	A-003 sends to A-005, which has not moved since (dormant 16 days at snapshot)	A-003	A-005	90,000 USDT	[VERIFIED]
2026-09-30 03:17	T-018/019	A-003 sends to A-006, which sends to Kestrel Swap 12 minutes later	A-003	A-008	75,000 USDT	[VERIFIED]

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

Activity Chart

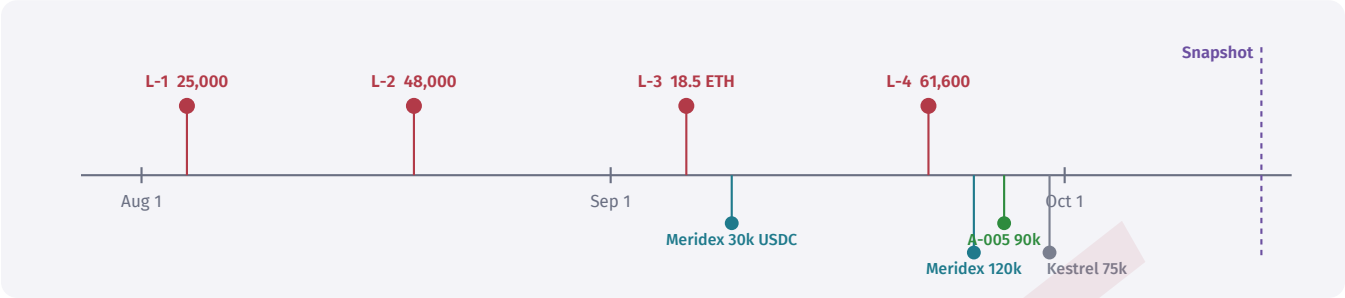

Figure 6.1 Victim payments (above line, red) and onward movements of traced funds (below line), all chains.

SECTION 7

7 Fund Flow Analysis

7.1 Flow Graph

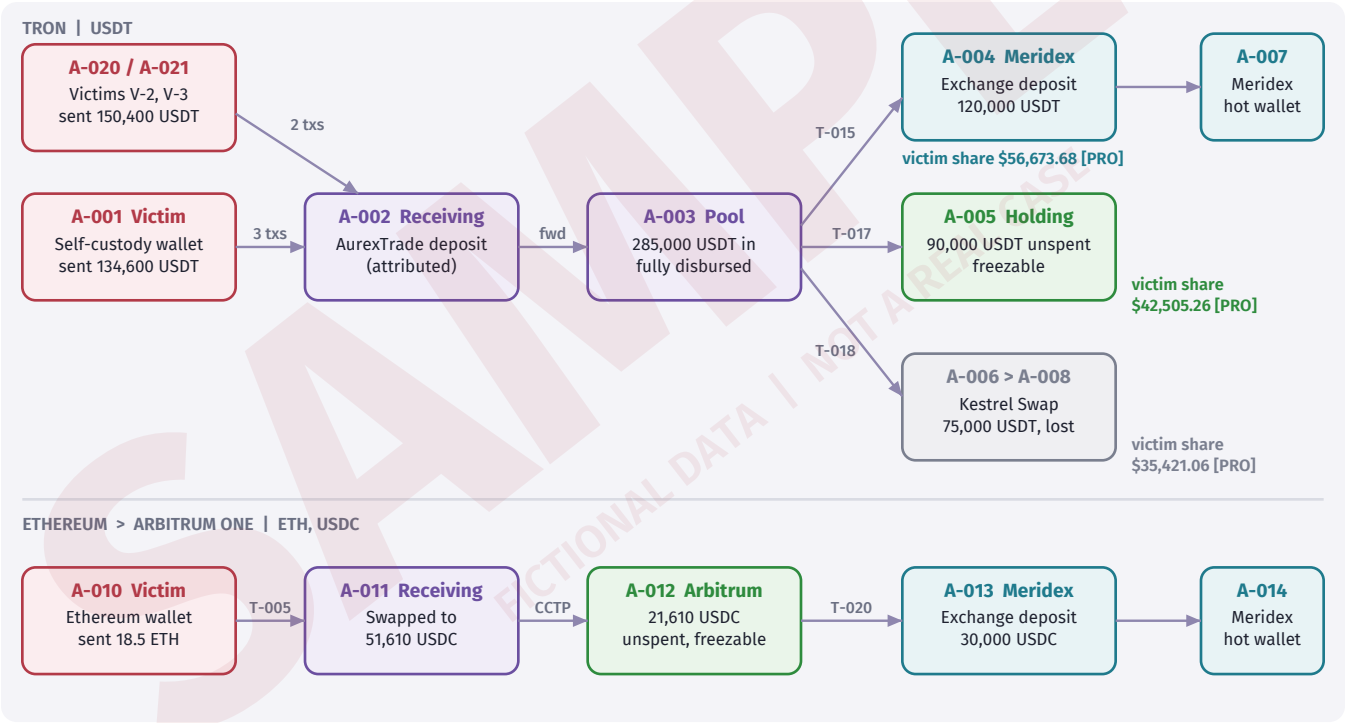

Figure 7.1 Traced fund flow. Red: victims. Purple: subject-controlled (attributed). Teal: exchange. Green: freezable balance. Grey: visibility lost.

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

7.2 Narrative

Payment. Ms. Ellison's three USDT payments ($134,600.00) went to A-002, and each was forwarded in full to A-003 within ten minutes of arrival. A-002 never held a balance for longer than that. A-003 also received $92,000.00 and $58,400.00 that two other victims had paid into A-002, for a pool of $285,000.00.

Movement. Three days after Ms. Ellison's last payment, A-003 emptied the pool in three transfers: $120,000.00 to Meridex deposit address A-004, $90,000.00 to A-005, and $75,000.00 to A-006. Under the proportional method, 47.23% of each transfer is Ms. Ellison's: $56,673.68, $42,505.26, and $35,421.06 [PRO].

Swaps and bridges. Her ETH payment took a separate path. Twelve minutes after it arrived at A-011, the 18.5 ETH was swapped for 51,610.00 USDC (a $190.00 difference from the payment value, attributable to price impact and fees), then moved to Arbitrum One through Circle's CCTP bridge. Three days later 30,000.00 USDC went to Meridex deposit address A-013, and 21,610.00 USDC remains at A-012.

Arrival. Funds came to rest in four places: two Meridex deposit addresses (both swept to Meridex wallets), two unspent stablecoin balances, and one instant exchange service whose output cannot be traced.

7.3 Hop Detail

Hop	From	To	Asset / Amount	Tx	Time (UTC)	Basis / method	Class
1	A-001	A-002	25,000.00 USDT	T-001	2026-08-04 15:22	Direct transfer	[VERIFIED]
2	A-002	A-003	25,000.00 USDT	T-002	2026-08-04 15:31	Direct transfer	[VERIFIED]
3	A-001	A-002	48,000.00 USDT	T-003	2026-08-19 14:05	Direct transfer	[VERIFIED]
4	A-002	A-003	48,000.00 USDT	T-004	2026-08-19 14:12	Direct transfer	[VERIFIED]
5	A-001	A-002	61,600.00 USDT	T-009	2026-09-22 13:47	Direct transfer	[VERIFIED]
6	A-002	A-003	61,600.00 USDT	T-010	2026-09-22 13:55	Direct transfer	[VERIFIED]
7	A-003	A-004	120,000.00 USDT	T-015	2026-09-25 09:14	Pool outflow [PRO]	[INFERRED]
8	A-004	A-007	120,000.00 USDT (sweep)	T-016	2026-09-25 09:40	Exchange sweep	[VERIFIED]
9	A-003	A-005	90,000.00 USDT	T-017	2026-09-27 22:08	Pool outflow [PRO]	[INFERRED]
10	A-003	A-006	75,000.00 USDT	T-018	2026-09-30 03:17	Pool outflow [PRO]	[INFERRED]
11	A-006	A-008	75,000.00 USDT	T-019	2026-09-30 03:29	Direct transfer	[VERIFIED]
12	A-010	A-011	18.50 ETH	T-005	2026-09-06 16:40	Direct transfer	[VERIFIED]
13	A-011	A-011	51,610.00 USDC (swap)	T-006	2026-09-06 16:52	Swap event	[VERIFIED]
14	A-011	CCTP	51,610.00 USDC (burn)	T-007	2026-09-06 17:03	CCTP burn	[VERIFIED]
15	CCTP	A-012	51,610.00 USDC (mint)	T-008	2026-09-06 17:21	CCTP mint, confirmed	[VERIFIED]
16	A-012	A-013	30,000.00 USDC	T-020	2026-09-09 11:26	Direct transfer	[VERIFIED]
17	A-013	A-014	30,000.00 USDC (sweep)	T-021	2026-09-09 11:48	Exchange sweep	[VERIFIED]

Pool outflows are marked INFERRED because the victim's share of each is the result of the proportional method; the transfers themselves are VERIFIED.

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

7.4 Where Funds Came to Rest

Destination	Type	Victim value	Method	% of traced	Status at snapshot	Class
Meridex (Tron)	Custodial exchange	$56,673.68	[PRO]	30.44%	Swept to A-007	[CORROBORATED]
Meridex (Arbitrum)	Custodial exchange	$30,000.00	Direct	16.11%	Swept to A-014	[CORROBORATED]
A-005	Unspent USDT	$42,505.26	[PRO]	22.83%	90,000 USDT, not frozen	[VERIFIED]
A-012	Unspent USDC	$21,610.00	Direct	11.61%	21,610 USDC, not frozen	[VERIFIED]
Kestrel Swap	Instant exchanger	$35,421.06	[PRO]	19.02%	Visibility lost	[INFERRED]

Total traced	$186,210.00 ($186,400.00 verified loss less $190.00 swap price impact and fees)
At action points	$150,788.94 [PRO where applicable]
Visibility lost	$35,421.06 (Kestrel Swap, no compliance contact)
FIFO sensitivity	Under FIFO, Ms. Ellison's Tron funds would be $28,000.00 at Meridex, $45,000.00 at A-005, and $61,600.00 at Kestrel Swap. Her amount at Tron action points would fall from $99,178.94 to $73,000.00. The method materially affects her share, which is why it is named beside every figure.

7.5 Multi-Victim Shares

Three victims' funds were pooled at A-003. Each victim's share of the two Tron action points (A-004 and A-005, $210,000.00 in total) is calculated exactly under the proportional method.

Victim	GumShoe case	Contributed	Share of pool	At action points [PRO]	Elsewhere [PRO]
V-1 (this victim)	GS-2610-0042	$134,600.00	47.23%	$99,178.95	$35,421.05
V-2	GS-2609-0031	$92,000.00	32.28%	$67,789.47	$24,210.53
V-3	GS-2610-0038	$58,400.00	20.49%	$43,031.58	$15,368.42

Other victims are identified by reference only. Ms. Ellison's ETH path is not part of the pool and is not shared.

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

SECTION 8

8 Clustering and Attribution

Cluster	Size	Basis	Attributed to	Named source(s)	Conf.	Class
K-1	4	Direct transfers; shared deposit address	AurexTrade operators	EX-002; intake GS-2609-0031, GS-2610-0038	C3	[CORROBORATED]
K-2	4	Exchange publication; sweep pattern	Meridex Exchange	EX-009	C4	[CORROBORATED]
K-3	1	Order page capture	Kestrel Swap	EX-011	C3	[INFERRED]

Competing Explanations

K-1. A-003 and A-006 could belong to a money-moving service used by the operators rather than to the operators themselves. Nothing on-chain distinguishes the two, and the report does not depend on the difference: in either case the funds moved as described. Records from Meridex about the account behind A-004 would help resolve it.

K-3. A-008 could be a look-alike address not operated by Kestrel Swap. The address format and immediate sweep match Kestrel's captured order page, but Kestrel publishes no address list, so the attribution stays at C3.

SECTION 9

9 Swaps, Bridges and Cross-Chain Movement

Ref	Type	Protocol	In (chain / amount)	Out (chain / amount)	Arrival	Class
X-1	Swap	Uniswap v3	Ethereum / 18.5 ETH	Ethereum / 51,610 USDC	Same transaction	[VERIFIED]
X-2	Bridge	Circle CCTP	Ethereum / 51,610 USDC	Arbitrum One / 51,610 USDC	Confirmed by investigator 2026-10-09	[VERIFIED]
X-3	Instant exchanger	Kestrel Swap	Tron / 75,000 USDT	Unknown	Lost	[INFERRED]

Impact on Traceability

X-1 and X-2 did not affect traceability: the swap is recorded in the transaction itself, and the bridge arrival was matched by message hash and amount and confirmed by the investigator. X-3 ended visibility. Kestrel Swap does not publish its output addresses, and no output on any supported chain could be matched to the 75,000 USDT deposit by amount and timing.

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

SECTION 10

10 Exchange Exposure

GumShoe checks every destination against more than 10 million deposit addresses that exchanges have published, plus exchanges' own wallets. Two deposit addresses in this case appear in that data.

Exchange	Deposit refs	Victim value	Window (UTC)	Published source	Custodial	Preservation
Meridex Exchange	A-004, A-013	$86,673.68	09-09 to 09-25	Meridex deposit address list, retrieved 2026-10-02 (EX-009)	Yes	LD-1 drafted, not yet sent
Kestrel Swap	A-008	$35,421.06	09-30	Order page capture (EX-011)	Unknown	Not recommended

Requests to Exchanges

For Meridex, the investigator recommends a preservation request now (LD-1), asking Meridex to keep account records and any remaining balance for the account or accounts credited by A-004 and A-013 between September 9 and September 25, 2026. A subpoena exhibit (LD-4) lists the records to seek later: identity and verification records, login and device records, linked accounts, and withdrawal destinations. Whether and how to send either is for Ms. Whitfield to decide. No request is recommended for Kestrel Swap, which has no known compliance contact.

SECTION 11

11 OSINT and Off-Chain Correlation

Ref	Source	Captured (UTC)	Finding	Archive	Class
O-1	Domain registration record	2026-10-03	aurextrade-pro.example registered 2026-06-02 through a privacy service	EX-006	[VERIFIED]
O-2	Passive DNS; direct resolution	2026-10-03	Site shares a hosting IP with two other trading-platform domains reported to GumShoe	EX-010	[CORROBORATED]
O-3	Victim chat export	2026-10-01	"Daniel" directed support questions to Telegram handle @aurex_support_desk	EX-003	[ALLEGED]
O-4	Public scam-report forum	2026-10-04	Anonymous post lists A-002 as an AurexTrade deposit address	EX-006	[UNVERIFIED]

The off-chain record is consistent with the on-chain findings. The AurexTrade domain was registered about five weeks before Ms. Ellison's first contact, and it shares hosting with two other sites reported to GumShoe as fraudulent platforms (O-2). The forum post naming A-002 (O-4) is anonymous and is not relied on; it agrees with the two victim reports that support F-3.

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

SECTION 12

12 Sanctions Screening and Risk Indicators

List	United States sanctions list (OFAC SDN, including listed digital currency addresses)
List version used	Dated 2026-10-13 / retrieved 2026-10-14 01:10 UTC
Refresh cadence	Checked daily
Additional lists	None screened for this case

Subject	List	Match type	Result	Screened (UTC)	Class
All 15 case addresses (A-001 to A-021)	OFAC SDN	Exact address	No match	2026-10-14 01:12	[VERIFIED]
AurexTrade, Meridex Exchange, Kestrel Swap	OFAC SDN	Name	No match	2026-10-14 01:12	[VERIFIED]

Risk Indicators Observed

Indicator	Observed	Detail	Refs
Exposure to a sanctioned address	No	No direct or one-hop exposure	
Mixer use	No		
Rapid chain hopping	Yes	ETH received, swapped, and bridged to Arbitrum One within 41 minutes	T-005 to T-008
Structuring below thresholds	No		
Infrastructure shared with other GumShoe cases	Yes	A-002 received payments from victims in GS-2609-0031 and GS-2610-0038	T-011, T-013

SECTION 13

13 Action Points, Recovery Steps and Monitoring

AT CUSTODIAL EXCHANGE	IN FREEZABLE STABLECOINS	ALREADY FROZEN BY ISSUER	WATCHED ADDRESSES
$86,673.68	$64,115.26	$0.00	5

13.1 Action Point Register

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

Point	Type	Address / exchange	Victim amount	Method	Issuer status	Instrument	Draft
AP-1	Freezable stablecoin	A-005 (Tron), 90,000 USDT total	$42,505.26	[PRO]	Not frozen	Freeze request to Tether	LD-2
AP-2	Freezable stablecoin	A-012 (Arbitrum), 21,610 USDC	$21,610.00	Direct	Not frozen	Freeze request to Circle	LD-3
AP-3	Custodial exchange	Meridex via A-004 (Tron)	$56,673.68	[PRO]	n/a	Preservation; subpoena	LD-1, LD-4
AP-4	Custodial exchange	Meridex via A-013 (Arbitrum)	$30,000.00	Direct	n/a	Preservation; subpoena	LD-1, LD-4

Issuer status was read directly from the USDT (Tron) and USDC (Arbitrum One) token contracts at 2026-10-14 06:00 UTC and re-read at 2026-10-16 08:00 UTC before issue. Both unchanged.

13.2 Recommended Actions

Priority	Action	Target	Rationale	Time sensitivity	Owner
1	Send freeze request	Tether, re: A-005	90,000 USDT unspent and not frozen; holds victim's largest reachable balance	Immediate	Attorney
1	Send freeze request	Circle, re: A-012	21,610 USDC unspent and not frozen; entirely the victim's funds	Immediate	Attorney
1	Send preservation request	Meridex Exchange	Preserves records and any remaining balance before account closure	Within days	Attorney
2	Provide report and packet	SMPD, IC3	Law enforcement can make its own freeze and records requests	This week	Victim
2	Seek account records	Meridex Exchange	Identity and withdrawal records for the receiving account (LD-4)	After preservation	Attorney
3	Coordinate with other victims' counsel	Cases GS-2609-0031, -0038	Shared pool; allocation in 7.5 supports a joint approach	Ongoing	Attorney

Recovery is not guaranteed. Both unspent balances can move at any time until frozen.

13.3 Draft Documents for Attorney Review

Draft	Document type	Addressed to	Covers	Exhibit	SHA-256
LD-1	Exchange preservation request	Meridex Exchange compliance	AP-3, AP-4	EX-013	`a497941c887b...`
LD-2	Freeze request	Tether	AP-1	EX-014	`5ab657d7aaaf...`
LD-3	Freeze request	Circle	AP-2	EX-015	`5998b73e9efd...`
LD-4	Subpoena exhibit (records schedule)	Meridex Exchange	AP-3, AP-4	EX-016	`e1f0f0eed818...`

These are drafts for an attorney to review and send. GumShoe is not a law firm and does not give legal advice.

SAMPLE
FICTIONAL DATA · NOT A REAL CASE

13.4 Ongoing Monitoring

Address	Chain	Reason watched	Watching since	Alerts	Last activity (UTC)
A-005	Tron	Unspent USDT (AP-1)	2026-10-03	0	2026-09-27 22:08
A-012	Arbitrum One	Unspent USDC (AP-2)	2026-10-09	0	2026-09-09 11:26
A-002	Tron	Receiving address; may receive new victims	2026-10-03	1	2026-10-11 19:30
A-003	Tron	Consolidation address	2026-10-03	0	2026-09-30 03:17
A-011	Ethereum	Receiving address	2026-10-03	0	2026-09-06 17:03

Alert on A-002 (2026-10-11): a new incoming payment of 8,000 USDT from an address not linked to any GumShoe case. It was forwarded to a new address outside this report's scope and has been referred for intake review. Alerts go to the investigator and Ms. Whitfield.

SECTION 14

14 Limitations, Assumptions and Alternative Hypotheses

14.1 Limitations

- Tracing shows how value moved between addresses. It does not by itself establish the identity, intent, or knowledge of any person.
- Recovery is not guaranteed. Freezing or returning funds depends on Tether, Circle, Meridex, courts, and timing.
- This report supports, and does not replace, the reports already filed with SMPD and IC3.
- Ms. Ellison's share of pooled funds depends on the accounting method. Section 7.4 shows how much.
- Kestrel Swap attribution rests on one captured source. Funds sent there could not be followed further.
- L-5 ($3,600) has not been located on-chain and is excluded from all figures.
- Findings are current as of 2026-10-14 00:00 UTC. Balances and freeze status may have changed since.
- GumShoe is not a law firm. Nothing in this report is legal advice.

14.2 Assumptions

USDT and USDC are valued at $1.00. Network fees paid in TRX and ETH are excluded. Other victims' payments to A-002 are taken from their own GumShoe case files, where each was verified on-chain.

14.3 Alternative Hypotheses Considered

Hypothesis	Evidence for	Evidence against	Assessment
Ms. Ellison controls A-002 or A-011	None	Addresses came from the platform's deposit page; A-002 also received two other victims' payments; no shared activity with A-001 or A-010	Rejected
Meridex is the perpetrator	Received funds	Published exchange address; immediate sweep consistent with ordinary customer deposits	Rejected; Meridex is a service
AurexTrade was a genuine investment	Dashboard showed gains	No funds reached any trading venue; no withdrawal ever paid; fees demanded to withdraw	Rejected

SAMPLE
FICTIONAL DATA · NOT A REAL CASE

SECTION 15

15 Conclusions

Based on the analysis in this report, and subject to the limitations in Section 14, I reach the following conclusions to a reasonable degree of professional certainty:

#	Conclusion	Answers	Basis	Class
C-1	Ms. Ellison's $186,400.00 went to AurexTrade deposit addresses and then to four places: Meridex Exchange ($86,673.68), two unspent stablecoin balances ($64,115.26), and Kestrel Swap ($35,421.06) [PRO].	Q1	F-1, F-2, F-4 to F-7	[VERIFIED] / [INFERRED]
C-2	$150,788.94 of her funds is at points where a freeze or preservation request can be directed. None was frozen at snapshot.	Q2	F-4, F-5; 13.1	[CORROBORATED]
C-3	The receiving addresses are attributed to the operators of AurexTrade. No individual has been identified. Meridex records are the most direct route to identifying the account holder.	Q3	F-3; Section 8	[CORROBORATED]
C-4	Her loss is linked to at least two other victims through the shared receiving address A-002 and pool A-003.	Q4	F-2, F-3; 7.5	[VERIFIED]

SECTION 16

16 Investigator Certification

I certify that I conducted the analysis described in this report; that the facts stated are true to the best of my knowledge; that every label, attribution, classification, finding, and conclusion is my own determination based on the data, methods, and sources disclosed; and that I have reviewed and adopted all narrative text, including text drafted with AI assistance. No fee was charged to the victim for this work, and I have no financial interest in the outcome.

This certification appears in a sample report and is not a sworn statement.

_____

Lead Investigator, GumShoe
Date: 2026-10-16

A. Lin

_____

Avery Lin (fictional)
Senior Analyst, Peer Reviewer
Date: 2026-10-15

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

Investigator Qualifications

In a real report, this section states the license, training, and experience of the investigator who signed it. It is left out of this sample.

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

APPENDICES

Appendix A: Case Action Log and Chain of Custody

Every case action is written to an append-only log. Each entry includes the hash of the previous entry, so any alteration or deletion breaks the chain.

Log entries	102
First entry	2026-09-30 21:14:02 UTC
Head hash at issue	`b895b2f467c6ad8c4a893e8db3cd07a7dfb4905ff37bf7161cc69a9f99cf8171`

Seq	Time (UTC)	Actor	Action	Entry hash	Previous
1	2026-09-30 21:14	System	Intake form received; case opened	`1fedebed2a7b`	`d72146bdfbf7`
9	2026-10-01 15:02	Investigator	Case accepted; secure link issued	`9deac0c724ff`	`1fedebed2a7b`
17	2026-10-01 18:40	Investigator	Seeds T-001, T-003, T-005, T-009 confirmed on-chain	`36127cdad91e`	`9deac0c724ff`
38	2026-10-03 02:11	System	Trace run 1 complete; 21 transactions fingerprinted	`e78eaa0ea7cc`	`36127cdad91e`
52	2026-10-04 16:25	Investigator	A-002 class ALLEGED to CORROBORATED	`e6fa7dd0f78e`	`e78eaa0ea7cc`
71	2026-10-09 14:03	Investigator	CCTP arrival T-008 confirmed	`c39d2a6aab6d`	`e6fa7dd0f78e`
88	2026-10-14 06:00	System	Issuer freeze status read: AP-1, AP-2 not frozen	`fd5cd46c9f53`	`c39d2a6aab6d`
102	2026-10-16 09:31	Investigator	Report v1.0 approved; packet sealed	`6c8f65d3638c`	`fd5cd46c9f53`

Excerpt. The full log (102 entries) is EX-017.

Classification Changes

Item	From	To	New supporting source	By	Log seq
A-002	ALLEGED	CORROBORATED	Same deposit address in intake for GS-2609-0031 and GS-2610-0038	Investigator	52
X-2	INFERRED	VERIFIED	CCTP message hash and amount match; investigator confirmation	Investigator	71

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

APPENDICES

Appendix B: Complete Transaction Ledger

B.1 Transactions

Ref	Chain	Tx hash (full)	Block	Time (UTC)	From	To	Amount	Provider fingerprint	2nd src
T-011	Tron	609edb05fae93f0631e616e8b1133d3fff56a34a5773b30c7704586780af10b8	74,288,419	2026-08-01 10:02:17	A-020	A-002	92,000.00 USDT	1bc3bc84da7e1f	Match
T-012	Tron	98025d4eb0d424d92d953c6bb9a4d048c4fc087fc58f9a8ddc579841227ceb96	74,288,566	2026-08-01 10:09:40	A-002	A-003	92,000.00 USDT	891c307e0c133a	Match
T-001	Tron	c48556f5231a59f7cf235219f3b00c773603ece744cde8e19e24d2d0304fe2f5	74,381,207	2026-08-04 15:22:08	A-001	A-002	25,000.00 USDT	99a73c7c41a597	Match
T-002	Tron	2fb371ae7bea3f668a57a3fe55ff4281e2967b34cab1bfd74f3adf608ccf2e03	74,381,399	2026-08-04 15:31:44	A-002	A-003	25,000.00 USDT	bfd1c8b78bf3e3	Match
T-003	Tron	0c7254b9bf3e1847bc65ca75212ed3d1d7b0caa7c3d2fb626ae7eca74fc09ea0	74,811,032	2026-08-19 14:05:51	A-001	A-002	48,000.00 USDT	0f0396857326d6	Match
T-004	Tron	a68a0b79af33100f28a164deac54ce14f4fabbae675ac772a213c57c2ef350ad	74,811,161	2026-08-19 14:12:20	A-002	A-003	48,000.00 USDT	fa9b724b1bdd07	Match
T-013	Tron	c2b2ed23d49a559aef9a4417f0b42851bcaf5153ccb96e662e598dbbc71d38a5	75,213,870	2026-09-02 08:44:05	A-021	A-002	58,400.00 USDT	f3d77c4f82c3ba	Match
T-014	Tron	95c83f06c31bf4e26dccb09d22ed6f1035535b4e50fbda4bb7f1ff68b2b39898	75,213,999	2026-09-02 08:50:31	A-002	A-003	58,400.00 USDT	819b513c0ae9c7	Match
T-005	Ethereum	0x1423669ed8b32235d51a1de942281f4f1fe41553ee2ddbf4d7a9b330db4bc544	23,312,904	2026-09-06 16:40:12	A-010	A-011	18.50 ETH	7d9a74daa8c9e9	Match
T-006	Ethereum	0x0bc8a7a149f98c9e9beb9f0fcc46c4a7afd724affffeb51eb61761df62ee626	23,312,966	2026-09-06 16:52:37	A-011	A-011	51,610.00 USDC (swap)	94bdb6797499fc	Match
T-007	Ethereum	0xe2c4fd468c6c53248bf68851ea99c16ce9e3615e445ffb53fb352180a2f4745e	23,313,018	2026-09-06 17:03:09	A-011	CCTP	51,610.00 USDC (burn)	0a0830f939288a	Match
T-008	Arbitrum One	0xbaad0c435d3053ebbb9d4c8fa2c80368d0ad1a58d1ab1d18365f1af1a3c37e63	381,226,410	2026-09-06 17:21:46	CCTP	A-012	51,610.00 USDC (mint)	e84c8386bd05b4	Match
T-020	Arbitrum One	0x3cbbeed9e33f061d4cc9a0511dd1a38c95868406a27534ccfec1dfbbcc1f2e6b	382,170,522	2026-09-09 11:26:40	A-012	A-013	30,000.00 USDC	df75dd289f23d3	Match

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

Ref	Chain	Tx hash (full)	Block	Time (UTC)	From	To	Amount	Provider fingerprint	2nd src
T-021	Arbitrum One	0x6acd37e8d1c8a29789681e1068d8c80c60b130336b96b7f2d4de3db78c61758f	382,175,630	2026-09-09 11:48:02	A-013	A-014	30,000.00 USDC (sweep)	1c51efe5a9070b	Match
T-009	Tron	d27a965b5cbbdc085c32b501680eb9468bacc99eb076236cf08184d5b4562787	75,789,544	2026-09-22 13:47:30	A-001	A-002	61,600.00 USDT	26a08cd2704097	Match
T-010	Tron	502a5d3403bbf1e79f68fa71c112711ae66db44903660372e04e97494f3eea64	75,789,694	2026-09-22 13:55:02	A-002	A-003	61,600.00 USDT	bd43cc3a1b17f0	Match
T-015	Tron	9570a0d78efeaf66fed1ae80b5676f7dc9c6d64d8325e68d2a35c8ce1cea7ba7	75,870,329	2026-09-25 09:14:33	A-003	A-004	120,000.00 USDT	1d4b348f3bad68	Match
T-016	Tron	6f4cd7e20a19a77a8cde982dadae64ddaffacf6a40f29a277c3625d77e2ba46f	75,870,841	2026-09-25 09:40:10	A-004	A-007	120,000.00 USDT (sweep)	a938a66d410c10	Time diff.
T-017	Tron	09e1c384b21353c4f17f09cdbf5b4148f89f5b70710513b0d2d5dd00960efcc5	75,943,882	2026-09-27 22:08:51	A-003	A-005	90,000.00 USDT	1359dd44922927	Match
T-018	Tron	494f546c8a36757bc76d1e1a4b19a4bc29f0bb2af3a186f4d13d498614c6527f	76,007,215	2026-09-30 03:17:26	A-003	A-006	75,000.00 USDT	0a4bcb2eed46bc	Match
T-019	Tron	97fcae7c60a2f24bb5f56f39e50a8a009bb3831a7643eadd4492fe1f3899dc68	76,007,465	2026-09-30 03:29:58	A-006	A-008	75,000.00 USDT	8d1a5c46d032cd	Match

B.2 Address Directory

Ref	Chain	Address (full)	Role
A-001	Tron	TpUR5Nc8RZ41sABxTLzxLoFkMVwn7KGWQC	Victim
A-002	Tron	T5hecDQ8aesgsv2jDWGfiptv7nPadWCMBh	Receiving
A-003	Tron	TTDugH83BUMbo7UL4p7jqqBcS38VvZtTQq	Consolidation
A-004	Tron	ThkC6hmZfS7gHVFLzJCBFa4Ze75eFgkPPX	Exchange deposit
A-005	Tron	TSNY4k4We1ugECvunNjNjUzkTra6BG32Rj	Intermediary
A-006	Tron	TWVKAGaQBD9kkxeR8eyC8ubGCCCJW54RpC	Intermediary
A-007	Tron	TppRBzteY6cw4dkoQVJHNBdYWP3hLJkq4R	Exchange wallet
A-008	Tron	Tg3NJK71Yzwqz9MJr62ohSTc9LnCeuAWC3	Swap / Protocol
A-010	Ethereum	0x0ad9c20dcb2ea23a46cb7126be7dcea28a01946e	Victim
A-011	Ethereum	0x63cb5666d3cd34f65f480a0d83016e1898302ed3	Receiving
A-012	Arbitrum One	0x7d077d9aac830ff6609b34e86dc56eb8283332e3	Intermediary
A-013	Arbitrum One	0x2f3ee67f9c66838520d768ebe06e2bef863b114f	Exchange deposit

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

Ref	Chain	Address (full)	Role
A-014	Arbitrum One	0x63fa066a836ba8fb3c9c9c145a5d8d3c4039e068	Exchange wallet
A-020	Tron	TWGoYDX3ncTGF1hhbkMQWGygZpVD43JUSJ	Victim
A-021	Tron	TbWqDs624Js1qvUFKDKi6wKYsW5BZ6aNKA	Victim

APPENDICES

Appendix C: Evidence Packet and Exhibit Index

The evidence packet contains this report, every exhibit, the raw provider responses behind each transfer, and the case action log. It is hash-chained, timestamped by an outside authority, and signed twice: once with a conventional signature and once with a signature designed to resist quantum computers. Anyone can verify it offline with GumShoe's standalone verifier.

Packet ID	PKT-2610-0042
Root hash	56a7b906436736b846400effe0fe98792cfbb4ddf9ffc7cd9bc37e56c14ba8f7
External timestamp	Timestamp authority (sample) / 2026-10-16 09:33:41 UTC / token TSR-0042
Signature 1 (conventional)	Ed25519 / key gk-sig-2026-01
Signature 2 (quantum-resistant)	ML-DSA-65 / key gk-pq-2026-01
Verifier	gumshoe-verify 1.0.0 (SHA-256 e429b4e5287cd81e)
Public keys published at	gumshoe.ghostkey.dev/keys (sample)

Verifying the Packet Offline

- Obtain the verifier and confirm its SHA-256 matches the value above.
- With no network connection, run: `gumshoe-verify PKT-2610-0042.gspkt --offline`
- The verifier recomputes every file hash and the hash chain, checks the timestamp, and checks both signatures.
- A pass means no file has changed since sealing. Any failure means the packet must not be relied on.

Exhibit Index

Exhibit	Title	Type	Size	SHA-256
EX-001	Intake form and written statement	PDF	4 pp	918729dccf9766de85744f6e...
EX-002	AurexTrade screenshots	PNG set	14 images	2c8032d53fc4b32d0a689e10...
EX-003	WhatsApp chat export	TXT + media	2.1 MB	64e50ec09cf20654b33fda89...
EX-004	Coinvault statements, Jul to Sep 2026	PDF	9 pp	29498c5c90e5f6ddbd1ebbd7...
EX-005	SMPD report; IC3 confirmation	PDF	3 pp	f79ef45ce0cf462d1dbe3046...
EX-006	Domain record, site archive, forum capture	WARC + PDF	18.4 MB	cba2bbae017ef0a12843306e...
EX-007	GumShoe trace graph export	SVG + JSON	412 KB	b676fbcd17a320bd767cde01...
EX-008	Raw provider responses (21 tx, 2 sources)	JSON	1.3 MB	4120df37c5e0b7763fbe2f29...

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

Exhibit	Title	Type	Size	SHA-256
EX-009	Meridex published address list capture	PDF + CSV	6.8 MB	bc12749438ed2636ce56593c...
EX-010	Passive DNS and hosting capture	PDF	5 pp	8c577f3de2db7b1cacc680ea...
EX-011	Kestrel Swap order page capture	WARC	3.2 MB	7e8c144b07219c329efea19c...
EX-012	OFAC SDN list snapshot, 2026-10-13	XML	28 MB	ab375d65a4171d6e4ae53198...
EX-013	LD-1 Meridex preservation request (draft)	DOCX	3 pp	c4cb9c331a94376335ad0c90...
EX-014	LD-2 Tether freeze request (draft)	DOCX	2 pp	a8a7581639da75913e95fc0f...
EX-015	LD-3 Circle freeze request (draft)	DOCX	2 pp	bfc59965857a6777cc90bf54...
EX-016	LD-4 Subpoena exhibit (draft)	DOCX	4 pp	41fd30aa8cd439f31caae22e...
EX-017	Case action log export	JSONL	88 KB	db1b80b9d99c6e527ece442f...

APPENDICES

Appendix D: AI Use Disclosure and Review Record

GumShoe's narrative model drafted prose in the sections listed below. A person decided everything else. AI output did not become any label, attribution, classification, finding, action, or conclusion. The model had access only to data already entered in this case, and the investigator reviewed and adopted every drafted passage.

Model	GumShoe narrative model, build 2026.10 (sample entry)
Generation run ID	GEN-2610-0042-03
Prompt template version	rpt-tmpl 2.1 (SHA-256 81942e9d9a67378a)
Data supplied to model	Case data model for GS-2610-0042 only; no external access
Generated (UTC)	2026-10-15 17:20

Section	AI-drafted	Human edits	Reviewed by	Approved (UTC)
1 Bottom Line	Yes	Moderate	Investigator	2026-10-16 09:10
3.2 Incident Narrative	Yes	Minor	Investigator	2026-10-16 09:10
5.2 Entity narratives	Yes	Moderate	Investigator	2026-10-16 09:12
7.2 Fund flow narrative	Yes	Minor	Investigator	2026-10-16 09:14
8, 9, 10, 11 narratives	Yes	Minor	Investigator	2026-10-16 09:18
14.2 Assumptions	Yes	None	Investigator	2026-10-16 09:19
All other sections	No	n/a	Investigator	2026-10-16 09:25

SAMPLE
FICTIONAL DATA | NOT A REAL CASE

Pre-Issue Review Checklist

Check	Status
Every transaction hash and address resolves at the finalized height, with a stored provider fingerprint	Pass
Second-source disagreements recorded; none relied on unresolved	Pass
Every finding and conclusion carries a class and cites a source	Pass
Every attributed claim names its source; unsourced claims marked UNVERIFIED	Pass
No AI output appears as a label, attribution, classification, finding, action, or conclusion	Pass
Accounting method tag shown beside every mixed-funds figure	Pass
Totals reconcile across Sections 1, 3, 7, and 13, including multi-victim shares	Pass
USDT / USDC issuer freeze status re-read within 24 hours of issue	Pass
Bridge arrivals marked confirmed only where the investigator confirmed them	Pass
Sanctions screening used the current daily list	Pass
Evidence packet passes the offline verifier	Pass
Victim notices present and no fee language anywhere	Pass

APPENDICES

Appendix E: Glossary

Term	Definition
Action point	A place where traced funds can be reached: a freezable stablecoin balance or a custodial exchange account.
Attributed claim	A statement about who controls an address, always shown with its named source. Not a blockchain fact.
CCTP	Circle's Cross-Chain Transfer Protocol. Burns USDC on one chain and mints it on another.
Custodial exchange	An exchange that holds funds for its customers and can therefore freeze or preserve them.
Evidence packet	The sealed, signed, hash-chained bundle of this report, its exhibits, and raw data, verifiable offline.
Finality	The point after which a blockchain record can no longer change.
Freeze request	A request to a stablecoin issuer (Tether for USDT, Circle for USDC) to block tokens at an address.
Instant exchanger	A service that swaps one asset for another without an account, often with little record keeping.
Pig butchering	A fraud in which a relationship is built over weeks before the victim is drawn into a fake investment.
Preservation request	A request asking an exchange to keep account records and funds pending legal process.
Proportional [PRO]	Accounting method in which each outflow from a mixed address carries traced funds in proportion to their share.
Provider fingerprint	The SHA-256 hash of the raw data response a transfer was read from.
Sweep	An exchange moving a customer deposit from its deposit address into its own main wallet.

SAMPLE
FICTIONAL DATA | NOT A REAL CASE