BLOCKCHAIN FORENSICS REPORT

TRON Mainnet — TRC-20 USDT Fund Flow Analysis

Case Reference: NTI-LEAVITT-2026-001 | April 3, 2026

SCOPE & METHODOLOGY

This report presents the complete on-chain forensic analysis of 14 wallets associated with Case NTI-LEAVITT-2026-001. All data was obtained from the public TRON blockchain via TronScan (tronscan.org) and cross-referenced against known exchange attribution data. Method signatures were analyzed to distinguish USDT transfers (a9059cbb) from TRX energy delegation (9ddf93bb) and approval transactions (095ea7b3).

FUND FLOW — 3-LAYER CASCADE

Layer 1 — Crime Wallets (Fraud Network)

Four wallets constitute the primary fraud layer — the entry point for victim funds and immediate layering chain:

Address	Role	USDT In	USDT Out	Balance	Status
TGf5bSmBBUPAY7bhsGhmafeD...	Primary Collection	$7,080.00	$7,080.00	$0.00	SWEPT
TSt36w9edfNJaCQs433MyUNe...	Primary Sink	$116.94	$0.00	$116.94	FREEZE
TLSptUxetSpjB8xRS6QrnJwu...	Gate.io Exit	$366.94	$0.00	$366.94	FREEZE
TCnJ7ngFdc639YumMhkJ1nR8...	Active Cycling	$6,596.12	$6,596.12	$0.00	ACTIVE

Layer 2 — Exchange & Relay Wallets

Funds flowed through 7 additional intermediate and exchange wallets before reaching the likely cash-out destination:

Address	Label	Exchange	Action Required
TU4vEruvZwLLkSfV9bNw12...	Bybit Hot Wallet	Bybit	KYC Subpoena — compliance@bybit.com
TLSptUxetSpjB8xRS6QrnJ...	Gate.io Exit	Gate.io	Freeze + KYC — compliance@gate.io
TA8rLnJm...kJHkAH7L	Relay #1	Unknown	Tag ChainAbuse
THXLBByJ...JiiFB	Relay #2	Unknown	Tag ChainAbuse

TQn9Y2kh...SLL	Relay #3	Unknown	Tag ChainAbuse
TWd4WrZ9...7h74	Conversion	Unknown	Monitor / Tag
TYukBQZ2...V3h	Terminal Sink	Unknown	Monitor

Layer 3 — Infrastructure & Operators

Two operator wallets supported the fraud infrastructure:

Address	Label	Balance (TRX)	Purpose	Action
TJDENsfBJs4R...	GasFree4uCOM	35.33 TRX	Gas/Energy Operator	Report FinCEN
TCvnWqQ2hFqq...	Dark Energy Market	27,300,000 TRX	Unlicensed MSB	FinCEN Referral

CONTRACT METHOD SIGNATURES OBSERVED

Method Signature	Function	Count in Trace	Significance
a9059cbb	transfer(address,uint256)	29	USDT transfers — direct theft evidence
9ddf93bb	delegateResource(addr,int64,int32)	8	TRX energy delegation to fraud wallet
095ea7b3	approve(address,uint256)	3	Token approval — potential drainer prep

TIMING ANALYSIS — AUTOMATED SWEEPING CONFIRMED

Transaction timing analysis reveals a systematic automated sweeping pattern:

Same-block sweeps	Victim USDT transfers swept from collection wallet within same or next TRX block (~3 seconds)
Gas-before-sweep	TRX energy delegated from operator (TJDENsfBJs4R) BEFORE victim transfer, indicating pre-staged infrastructure
Multi-hop velocity	Funds passed through 3–4 wallets within 30 minutes of initial deposit

Bybit alignment	$480 USDT swept to Bybit-attributed address within 2 hours of same-day victim deposit
Weekend timing	Peak activity September 13-15 (Fri-Sun 2025) — timing typical of cross-border fraud farms

SPAM TOKEN ANALYSIS

The following unauthorized spam tokens were airdropped to the fraud wallet, a common intelligence-gathering and social engineering technique:

Token Name	Amount	Purpose / Notes
HASH8NET	888.8	Phishing lure — redirects to Blockchain hash recovery scam
tron.ink	1,000,000	Mass airdrop spam — associated with Tron phishing campaigns
Pay.bi	8,888.88	Chinese lucky number (88) pattern — targets Chinese-speaking fraud victims
GasFree4uCOM	35.33	Gas service advertisement — operator self-identifying

WARNING: Do NOT interact with spam tokens. Many contain instructions to visit phishing sites that harvest private keys or seed phrases.

FREEZABLE ASSETS — TETHER RECOVERY WINDOW

Total on-chain freezable USDT as of April 3, 2026: **$483.88 USDT**. Tether Limited (issuer of USDT) has technical authority under their terms of service to freeze specific wallet addresses upon verified fraud or law enforcement request. This window remains OPEN. Contact **support@tether.to** or **legal@tether.to** immediately with this case reference.