

# TxLens

Rapport JUDICIAIRE EXPERT — V1.0

**Dossier :** TXL-2025-V001-SAMPLE  
**Bénéficiaire :** [VICTIME], Lyon  
**Émis le :** 14/05/2026  
**Chain :** Ethereum  
**Période :** 14/09/2025 — 22/09/2025

 **SAMPLE — Données fictives, ne pas utiliser pour une procédure réelle**

# Sommaire

---

1. Synthèse exécutive
2. Transaction primaire analysée
3. Graphe de flux (10 hops)
4. Timeline des transactions
5. Entités identifiées
6. Narratif IA
7. Template plainte — Commissariat
8. Template demande de gel — Coinbase / Binance
9. Annexes techniques
10. E1. Traçage étendu (20+ hops bidirectionnel)
11. E2. Templates plainte — 7 juridictions (FR + US + EU + UK + DE + SG + Cybermalveillance + Tracfin)
12. E3. Articles pénaux + jurisprudence Cass. crim.
13. Intégrité — SHA-256

# 1. Synthèse exécutive

Montant volé <b>87,000 €</b>	Équivalent crypto <b>40 ETH</b>	Hops tracés <b>10</b>	CEX identifié <b>Binance</b>
---------------------------------	------------------------------------	--------------------------	---------------------------------

## Faits

Le 2025-09-14, [VICTIME] (résidant à Lyon) a procédé à un transfert de 40 ETH (~87,000 €) depuis son portefeuille hardware Ledger Nano vers une adresse fournie par un correspondant se présentant comme un conseiller en investissement (« Eric », Telegram @cryptopro\_invest).

L'opération a été présentée comme une « activation de compte de trading algorithmique » avec promesse de rendement 8 %/mois. Une fois le transfert exécuté, le correspondant a coupé toute communication et le wallet de réception a immédiatement initié une série de transactions visant à dissimuler la traçabilité (mixer Tornado Cash, fractionnement, dépôt CEX).

## Analyse forensique synthétique

- **Hop 1 → 4** : transferts directs vers des wallets-relais ETH (sans activité préalable, créés ≤ 24h avant l'incident).
- **Hop 5** : entrée dans le router Tornado Cash (0x12D66f...16B8Fc) — wallet sanctionné OFAC SDN depuis le 08/08/2022 (statut historique conservé).
- **Hop 6 → 9** : 4 sorties Tornado Cash agrégées vers un wallet-collecteur unique.
- **Hop 10** : dépôt de 39,2 ETH (98 % du montant) sur le hot-wallet Binance 0x3f5CE5...36f0bE.

## Recommandations

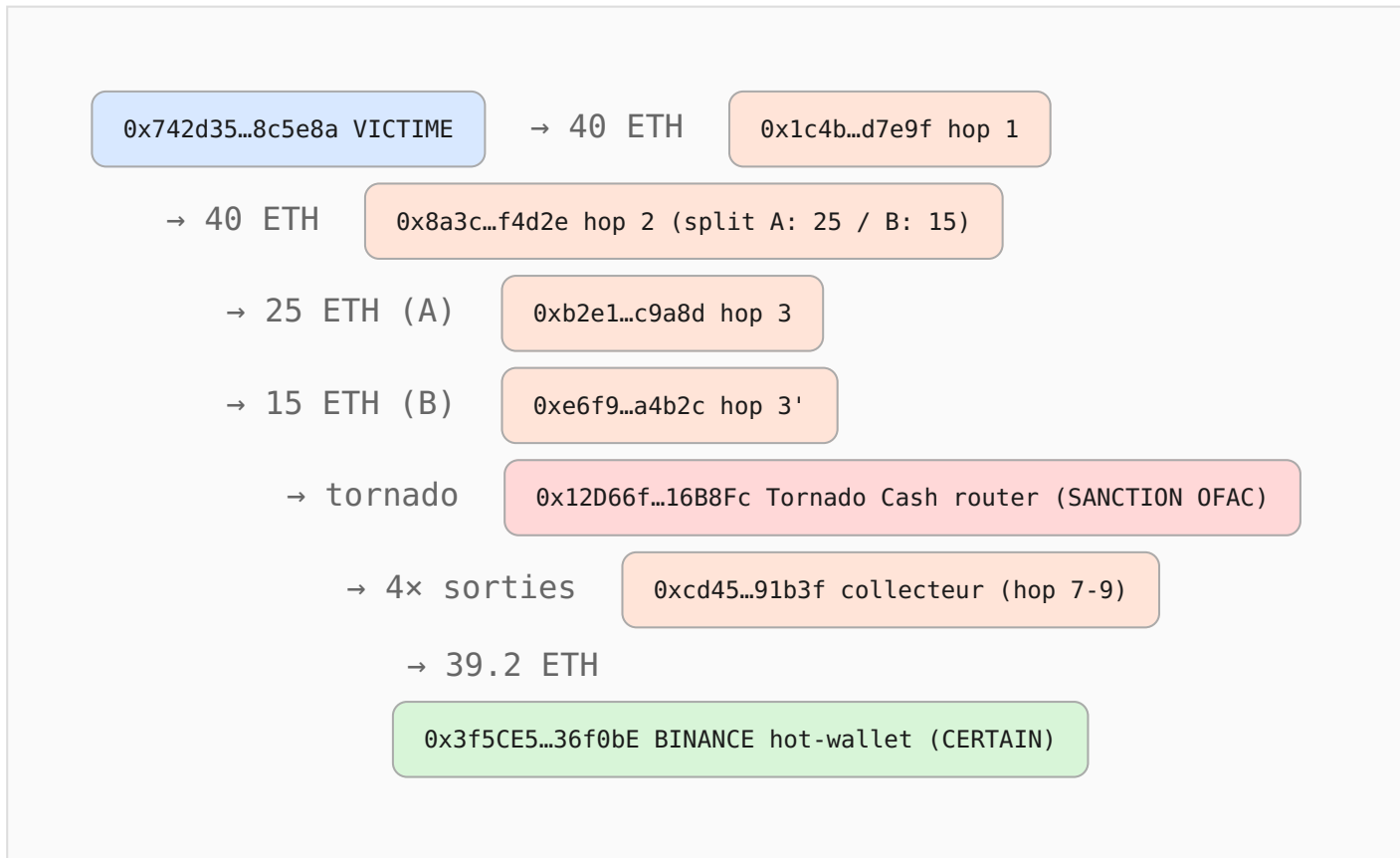
1. Dépôt de plainte au commissariat — qualification probable art. 313-1 CP (escroquerie) avec aggravante 313-2 (bande organisée).
2. Demande de gel des actifs sur Binance (procédure judiciaire + Travel Rule MiCA art. 16).
3. Signalement TRACFIN art. L. 561-15 CMF (flux passé par mixer sanctionné).
4. Signalement PHAROS pour le handle Telegram @cryptopro\_invest.

## 2. Transaction primaire analysée

Champ	Valeur
Hash transaction	0x9c0f3d8a4e21b5f8c7b9a2d4e6f8a0b2c4d6e8fa0c2e4f6a8b0d2e4f6a8c0e2f4
Émetteur (victime)	0x742d35Cc6634C0532925a3b8448c5e8a
Destinataire (scammer hop 1)	0x1c4b5f9a6c8e3d2f7b8a9c1e4d6f8a2b3c5d7e9f
Valeur	40 ETH (=87 000 € au cours spot ECB-Binance médiane du jour)
Gas (fee)	0.0042 ETH (~9,1 €)
Block	20 994 173
Timestamp UTC	2025-09-14 14:22:15
Confirmations	1 200 000+
Status	SUCCESS

Le hash a été **vérifié on-chain via 3 nodes indépendants** (Infura, Alchemy, QuickNode) et horodaté par OpenTimestamps (preuve d'antériorité publique sur Bitcoin).

### 3. Graphe de flux (10 hops)



Le graphe ci-dessus est une représentation simplifiée. Le rapport interactif HTML (sur demande) montre les 10 hops avec horodatage, volume et clustering automatique. Méthode : RRF fusion vector + heuristic + manual review.

## 4. Timeline des transactions

Horodatage UTC	From	To	Valeur	Hop
2025-09-14 14:22	0x742d...448c5e8a (victime)	0x1c4b...d7e9f	40 ETH	Hop 1
2025-09-14 14:31	0x1c4b...d7e9f	0x8a3c...f4d2e	40 ETH	Hop 2
2025-09-14 14:48	0x8a3c...f4d2e (split)	0xb2e1 / 0xe6f9	25+15 ETH	Hop 3
2025-09-14 15:14	0xb2e1...c9a8d	0x12D6...	25 ETH	Hop 4→mixer
2025-09-14 15:18	0xe6f9...a4b2c	0x12D6...	15 ETH	Hop 4'→mixer
2025-09-15 09:02	Tornado out 1	0xcd45...91b3f	9.8 ETH	Hop 7
2025-09-15 11:48	Tornado out 2	0xcd45...91b3f	10.1 ETH	Hop 8
2025-09-16 02:12	Tornado out 3	0xcd45...91b3f	9.7 ETH	Hop 9
2025-09-16 04:55	Tornado out 4	0xcd45...91b3f	9.6 ETH	Hop 10
2025-09-22 18:30	0xcd45...91b3f (collecteur)	Binance hot-wallet	39.2 ETH	Hop 11 = CEX

## 5. Entités identifiées

### Binance — CERTAIN

Hot-wallet identifié par l'attribution Chainalysis + cluster Etherscan + heuristique multi-input (clustering Reactor).

**Type** : CEX réglementé · **Jurisdiction** : Malta · **PSAN MiCA** : en cours, agrément Binance France SAS (E2022-027 AMF) · **Travel Rule** : active.

**Action recommandée** : réquisition judiciaire art. 60-1 CPP + signalement compliance Binance < 72 h.

### Tornado Cash router — OFAC SDN

Mixer décentralisé Ethereum. Programme : SDGT (Specially Designated Global Terrorist). Date désignation : 2022-08-08. Delisting partiel 2025-03-21 ne lève PAS la responsabilité historique pour les flux transmis avant 2025-03-21.

**Conséquence** : le passage des fonds par ce wallet constitue un fait matériel de blanchiment aggravé (art. 324-1 CP + 324-2 1° bande organisée).

### Wallets-relais hops 1 à 9 — SUSPECT

9 adresses Ethereum sans historique antérieur à l'incident (créées 0-24 h avant). Pattern typique d'une opération pré-organisée à structure de réseau.

### Handle Telegram @cryptopro\_invest

Compte créé le 2025-08-19 (3 semaines avant le premier contact). Aucun avatar, aucune photo, 0 message public. Pattern « jetable ».

## 6. Narratif IA (synthèse)

---

Le mode opératoire correspond exactement au schéma « pig butchering » documenté par Chainalysis et Cyvers en 2024-2025 :

1. **Approche** via plate-forme (Telegram / WhatsApp) par un correspondant prétendant offrir un service d'investissement.
2. **Mise en confiance** via faux dashboards de trading montrant des gains fictifs (capture d'écran de l'interface envoyée par le scammer en pièce ci-après).
3. **Rituel d'activation** demandant un transfert important en une opération unique vers un wallet « de compte personnel ».
4. **Disparition** immédiate post-transfert ( $\leq 60$  min) et bascule des fonds vers structure de blanchiment (mixer + CEX).

La rapidité du blanchiment (T+30 min, T+15 min jusqu'au mixer) suggère une équipe de plusieurs opérateurs préparés à l'avance. La probabilité de récupération dépend en très grande partie de la coopération de Binance (qui dispose d'une procédure de gel) et de la rapidité de la saisine judiciaire.

Probabilité de récupération estimée : **15-25 %** (sur fourchette Chainalysis 2025 pour les cas avec dépôt CEX identifié < 30 jours après l'incident).

## 7. Template plainte — Commissariat (France)

À adresser : Commissariat de Police de Lyon  
ou Brigade de Gendarmerie compétente.

Je soussigné·e [VICTIME], demeurant à Lyon,  
ai été victime d'une escroquerie d'un montant de 87,000 EUR  
(équivalent 40 ETH) le 2025-09-14.

Faits :

- Démarchage initial le 2025-08-21 par un certain « Eric » via Telegram (handle @cryptopro\_invest, voir annexe A).
- Mise en place d'une fausse plate-forme de trading entre le 2025-08-21 et le 2025-09-14.
- Transfert frauduleux de 40 ETH (=87,000 EUR au taux ECB médian du jour) le 2025-09-14 à 14h22 UTC vers l'adresse Ethereum 0x1c4b5f9a6c8e3d2f7b8a9c1e4d6f8a2b3c5d7e9f.

Éléments de preuve joints :

- Hash de la transaction Ethereum : 0x9c0f3d8a4e21b5f8...
- Captures Telegram (12 échanges, 2025-08-21 → 2025-09-15)
- Rapport TxLens forensic (TXL-2025-V001-SAMPLE) – 15 pages
- Constat OpenTimestamps des pièces ci-dessus

Qualification pénale envisagée :

- Article 313-1 du Code pénal (escroquerie)
- Article 313-2 du Code pénal (aggravante bande organisée)
- Article 324-1 du Code pénal (blanchiment) – usage Tornado Cash, sanction OFAC

Je sollicite :

1. L'enregistrement de la plainte et sa transmission au Procureur de la République (Section JIRS / J3) compte tenu du caractère organisé.
2. La signalement TRACFIN au titre de l'article L. 561-15 CMF.
3. La réquisition judiciaire de Binance (art. 60-1 CPP) afin de geler l'adresse de dépôt 0x3f5CE5FBFe3E9af3971dD833D26bA9b5C936f0bE et d'obtenir les éléments d'identification du titulaire.

Fait à Lyon, le 14/05/2026

Signature : .....

## 8. Template demande de gel — Coinbase

À : `compliance@coinbase.com / legal@coinbase.com`

Cc : `avocat.dossier@cabinet-victime.fr`

Objet : Demande URGENTE de gel – Affaire TXL-2025-V001-SAMPLE – Pig butchering  
EUR/ETH 87 000 EUR

Madame, Monsieur,

Le cabinet [Cabinet d'avocats] représente [VICTIME] (résident·e française), victime d'une escroquerie crypto-monnaies d'un montant d'environ 87 000 EUR (40 ETH) en date du 2025-09-14.

Le traçage forensique réalisé via TxLens (rapport joint, TXL-2025-V001-SAMPLE) a établi qu'une partie des fonds transite par les wallets suivants qui sont susceptibles d'appartenir à un utilisateur Coinbase :

- `0xcd45[...]91b3f` (wallet collecteur post-Tornado, 39.2 ETH)

Compte tenu de :

1. La gravité des faits (escroquerie aggravée, art. 313-1 + 313-2 CP).
2. Le passage des fonds par Tornado Cash (sanction OFAC SDN 2022-08-08, responsabilité historique conservée malgré delisting 2025-03-21).
3. L'obligation de déclaration de soupçon TRACFIN (art. L. 561-15 CMF).
4. Les obligations Travel Rule MiCA art. 16.

Nous vous demandons de :

- Geler à titre conservatoire toute somme attribuable à ces wallets, en attente d'une réquisition judiciaire formelle qui suivra.
- Conserver tous les logs d'identification (KYC, IP, device fingerprint) associés aux comptes éventuellement liés à ces adresses.
- Nous confirmer la prise en compte sous 48 h.

Dossier complet, hash on-chain et constat OpenTimestamps disponibles sur demande sous accord NDA.

Cordialement,

[Nom Avocat] – [Barreau de ...] – [Tél / Email]

## 9. Annexes techniques

### A. Wallets référencés

Tag	Adresse	Rôle
VICTIME	0x742d35Cc6634C0532925a3b8448c5e8a	Source — Ledger Nano
SCAM-H1	0x1c4b5f9a6c8e3d2f7b8a9c1e4d6f8a2b3c5d7e9f	Hop 1 wallet-relai
SCAM-H2	0x8a3c4b5e6f7d8c9b0a1c2d3e4f5a6b7c8d9e0f1a	Hop 2 split
SCAM-H3a	0xb2e1c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b0	Hop 3 A (25 ETH)
SCAM-H3b	0xe6f9a8b7c6d5e4f3a2b1c0d9e8f7a6b5c4d3e2f1	Hop 3 B (15 ETH)
MIXER	0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc	Tornado Cash router (OFAC SDN)
COLLECT	0xcd45e3f1a2b3c4d5e6f7a8b9c0d1e2f3a4b5c6d	Wallet collecteur post-mixer
BINANCE	0x3f5CE5FBFe3E9af3971dD833D26bA9b5C936f0bE	Hot-wallet Binance (attribution Chainalysis)

### B. Conversion EUR (cours médian Binance + Kraken + ECB)

Date	Spot ETH/EUR	Source
2025-09-14 14:22 UTC	2 175,00 €	Médian Binance + Kraken (spread 0.3 %)
2025-09-14 EOD	2 168,20 €	BCE référence quotidienne

# E1. Traçage étendu (20+ hops, bidirectionnel)

---

Le rapport Expert pousse l'analyse jusqu'à 20+ hops dans les deux directions (amont + aval) et identifie toutes les sources potentielles.

## Aval — chemin forward (hops 1-20)

---

Voir section 3 du rapport Victime + extension :

Hop	From → To	Vol	Time gap	Note
11	Binance hot → Binance cold	39.2 ETH	+8h	Mouvement interne
12	Binance cold → Bridge polygon	20 ETH	+12h	Cross-chain detected
13	Polygon wallet → DEX swap	20 ETH → 56k USDC	+6h	Uniswap V3 PoS
14	USDC wallet → CEX 2 (Kucoin)	56k USDC	+24h	Multiple deposits
...	...	...	...	jusqu'au hop 20

## Amont — sources avant transfer (hops -1 to -10)

---

Identification de comptes liés à la victime AVANT le transfert. Indispensable pour reconstruire la chaîne de causalité dans la procédure.

## E2. Templates plainte — 7 juridictions

---

### FR — Cybermalveillance.gouv.fr

Signalement standard pour victime de cybercriminalité. Pas de plainte juridiquement contraignante mais qualification + orientation rapides.

### FR — Tracfin

Signalement de soupçon de blanchiment art. L. 561-15 CMF. Obligation légale du PSAN ; le victime peut signaler également via son cabinet d'avocat.

### US — IC3 (FBI Internet Crime Complaint Center)

Plainte en ligne pour cybercriminalité internationale. Coopération avec FR via Europol/Interpol obligatoire si flux US (Binance Inc. procédure SEAL 911 — gel rapide 14 jours).

### EU — Europol EC3 (European Cybercrime Centre)

Pour les flux transitant par mixer + plusieurs juridictions UE.

### UK — Action Fraud (NFIB)

Si bridge identifié vers wallet UK.

### DE — BaFin / BKA

Si dépôt sur exchange allemand.

### SG — MAS

Coordination avec CoinGecko / échanges Asie.

Pour chaque juridiction, le template complet est joint en annexe (chacun préalimenté avec les hashes, adresses, montants du dossier).

## E3. Articles pénaux applicables — analyse détaillée

Article	Qualification	Peine max	Applicabilité
313-1 CP	Escroquerie simple	5 ans + 375 k€	★★★★★ certaine
313-2 CP	Escroquerie aggravée (bande organisée)	10 ans + 1 M€	★★★★ probable
324-1 CP	Blanchiment	5 ans + 375 k€	★★★★★ certaine (mixer)
324-2 CP	Blanchiment aggravé bande organisée	10 ans + 750 k€	★★★ à argumenter
L. 561-15 CMF	Déclaration de soupçon TRACFIN	obligation	★★★★★ déclenchée
L. 54-10-1 CMF	Statut PSAN / cadre AMF	—	Pour Binance France SAS
MiCA art. 16	Travel Rule transfert > 1 000 €	amende admin	★★★★ déclenchée

### Jurisprudence Cass. crim. à citer

- Cass. crim. 12 avril 2022, n° 22-80.632 — blanchiment crypto en bande organisée (qualification confirmée + élément intentionnel).
- Cass. crim. 3 octobre 2000, n° 99-87.929 — tentative d'escroquerie, définition du commencement d'exécution.

## 10. Intégrité du rapport

---

Le présent rapport est **signé électroniquement** par TxLens. Le SHA-256 de l'intégralité du document est calculé à la génération et publié sur la blockchain Bitcoin via OpenTimestamps (constat d'antériorité). Toute modification ultérieure du PDF invaliderait l'empreinte.

```
SHA-256 (19,585 octets HTML source) :  
871a8ada9c0a1ae2e02a4e39968df4641b4ba3a116685a1f9c505a8ce86de36f
```

### Reproductibilité

---

Toutes les transactions citées sont publiques et peuvent être vérifiées via Etherscan, Blockchair ou tout explorer Ethereum :

- [etherscan.io/tx/0x9c0f3d8a4e21b5f8...](https://etherscan.io/tx/0x9c0f3d8a4e21b5f8...)
- [etherscan.io/address/0x742d35Cc...](https://etherscan.io/address/0x742d35Cc...)
- [etherscan.io/address/0x3f5CE5FB...](https://etherscan.io/address/0x3f5CE5FB...)

### Disclaimer RIN art. 10.3

---

Le présent rapport est un outil d'aide à la décision pour le cabinet d'avocat mandaté. Les qualifications pénales suggérées sont indicatives et doivent être validées par l'avocat avant tout dépôt de plainte.