

326DT002

Seminar #Digitalisation and #AI in Criminal Justice

Table of Contents:

- 1) Programme
- 2) Speaker's contributions (PPT)
- 3) Background documentation



#DIGITALISATION and #ARTIFICIALINTELLIGENCE in Criminal Justice

Online investigations and internet
searches in times of AI

Tallinn, 7-8 May 2026



EXCELLENCE IN
EUROPEAN LAW⁷

Speakers and chairs

Sandor Bosch, Court of Appeal Den Bosch, The Netherlands

Laviero Buono, Head of Section for European Criminal Law,
ERA, Trier

Rauno Kiris, State Prosecutor, Office of the Prosecutor General,
Tallinn

Eneli Laurits, State Prosecutor, Office of the Prosecutor General,
Tallinn

Lilija Mažeikienė, Cybercrime Investigations and Digital Evidence,
The Hague

Jordy Mullers, Part-time Judge at Zeeland-West Brabant District
Court, Legal Advisor at the Criminal Investigations Division of the
Dutch National Police, Regional Unit Limburg

Federico Paesano, Training and Investigations, Crystal
Intelligence, Basel

Danijel Sladović, Digital Forensic Consultant, INsig2, Zagreb

Marc Reina Tortosa, Executive Manager, El Paccto 2.0, Madrid

Jaanus Tehver, Criminal Defence Lawyers, Tallinn

George Zlati, Defence Lawyer, Zlati Ionescu Chipari Law Firm, Cluj

Key topics

- Technical issues (internet caches, proxy servers, encryption, deep/dark web, etc.)
- Legal issues (evaluation of the search results, reliability and credibility of authentication, search across jurisdictions)
- Challenges posed by websites, social networks, emails and other computer-generated or stored documents
- Presenting internet searches in court
- Videoconferencing
- Artificial intelligence (AI)

Language
English

Event number
326DT002

Organisers
ERA (Laviero Buono) in cooperation
with the Estonian Prosecutor's
Office



#DIGITALISATION and #AI in Criminal Justice

Thursday, 7 May 2026

09:00 Arrival and registration of participants

09:30 **Welcome and introduction to the programme**
Rauno Kiris & Laviero Buono

PART I: TECHNICAL ISSUES AND BASIC UNDERSTANDING OF THE INTERNET ARCHITECTURE AND CONCEPTS

Chair: Laviero Buono

09:35 **Fighting 2.0 crimes with Web 3.0 possibilities**

- Crypto 101: technology, definitions and more
- (Ab)use of crypto
- Blockchain explorers: understanding transactions, following the money
- Different crypto services: what data can we expect?

Lilija Mažeikienė

10:45 Discussion

11:00 Break

Chair: George Zlati

11:30 **Conducting forensic analysis at the crime scene**

- Triage at the crime scene (search warrant, equipment considerations, protocols, interviewing the suspect)
- Gathering digital evidence from live memory
- Scripts in digital forensic examinations
- Computer and mobile forensics

Danijel Sladović

12:30 Discussion

12:45 Lunch

PART II: LEGAL ISSUES RELATED TO ONLINE INVESTIGATIONS

Chair: Lilija Mažeikienė

13:30 **AI, emerging trends in social network investigations and how technology is changing this landscape**
George Zlati

14:15 Discussion

14:30 **Cross-border access to data and admissibility of evidence**

- Obtaining e-evidence
- Voluntary access to evidence
- Direct access and legal process

Jordy Mullers

15:15 Discussion

15:30 Break

Chair: George Zlati

16:00 **Hunting in the Dark: a prosecutor's experience of the darknet**
Eneli Laurits

16:45 Discussion

17:00 End of the first day (19:30 dinner offered by the organisers)

Objective

This seminar addresses various challenges linked to digitalisation that judges, prosecutors and lawyers in private practice working in the field of EU criminal justice will have to face in the years ahead. Some of these challenges such as the exchange of electronic evidence, videoconferencing, use of open source intelligence, artificial intelligence, digital technology, etc. will become the 'new normal'.

This event is part of a large-scale project sponsored by the European Commission entitled "Judicial training to prepare criminal justice professionals for #digitalisation and #artificialintelligence". It consists of 12 seminars to take place in various EU cities over the period 2024-2027.

Who should attend?

Judges, prosecutors, court staff and lawyers in private practice, who are citizens of eligible EU Member States participating in the EU Justice Programme (Denmark does not participate), Albania, Bosnia and Herzegovina, Kosovo*, Moldova and Ukraine.

* This designation is without prejudice to positions on status and is in line with UNSCR 1244/1999 and the ICJ opinion on the Kosovo declaration of independence.

Venue

Ministry of Justice of Estonia
Suur-Ameerika 1
10122 Tallinn
Estonia

CPD

ERA's programmes meet the standard requirements for recognition as Continuing Professional Development (CPD). Participation in the full programme of this event corresponds to **9 CPD hours**. A certificate of participation for CPD purposes with indication of the number of training hours completed will be issued on request. CPD certificates must be requested at the latest 14 days after the event.

Friday, 8 May 2026

PART III: E-EVIDENCE, CRYPTO, CYBERCRIME AND ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

Chair: Jordy Mullers

- 09:30 **Legal issues/challenges related to the collection of e-evidence in criminal investigations**
Jaanus Tehver
- 10:15 Discussion
- 10:30 **Decentralised finance (DeFi), non-fungible tokens (NFTs), and the broader applications of distributed ledger technology**
Federico Paesano
- 11:15 Discussion
- 11:30 Break
- 12:00 **Evolving definition of crimes:**
- How AI transforms criminal proceedings
 - Cyber crimes 2.0
 - Pretty-Good-Privacy phones: developments in the admissibility of the obtained data
- Sandor Bosch*
- 12:30 **Artificial intelligence and criminal networks: a link that goes beyond Europe**
Marc Reina Tortosa
- 13:00 Discussion
- 13:15 End of the seminar and light lunch

For programme updates: www.era.int.
Programme may be subject to amendment.

Your contacts



Laviero Buono
Head of Section
European Criminal Law



Julia Reitz
Event Coordinator
Tel.: +49 (0) 651 9 37 37 323
E-Mail: jreitz@era.int

**Apply online for
“#Digitalisation and #AI in
Criminal Justice”:
www.era.int/?134019&en**



This programme has been co-financed by the European Union

The content of this programme reflects only ERA's view and the Commission is not responsible for any use that may be made of the information it contains.

Application

#DIGITALISATION and #AI in Criminal Justice

Tallinn, 7-8 May 2026 / Event number: 326DT002



Terms and conditions of participation

Selection

1. Participation is only open to judges, prosecutors, court staff and lawyers in private practice from eligible EU Member States participating in the EU Justice Programme (Denmark does not participate) including Albania and Kosovo* (*this designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ opinion on the Kosovo declaration of independence*). The number of places available is limited (30 places). Participation will be subject to a selection procedure.
2. Applications should be submitted before **20 January 2026**.
3. A response will be sent to every applicant after this deadline. **We advise you not to book any travel before you receive our confirmation.**

Registration Fee

4. €135 including documentation, coffee breaks, lunches and dinner.

Travel and Accommodation Expenses

5. Participants will receive a fixed contribution towards their travel expenses and are asked to book their own travel. The condition for payment of this contribution is to sign all attendance sheets at the event. Participants are required to provide supporting documentation demonstrating that the travel has taken place. The amount of the contribution will be determined by the EU unit cost calculation guidelines, which are based on the distance from the participant's place of work to the seminar location and will not take account of the participant's actual travel costs.
6. Travel costs from outside Estonia: participants can calculate the contribution to which they will be entitled on the European Commission website (<https://era-comm.eu/go/calculator>). The distance should be calculated from their place of work to the seminar location.
7. For inter-Member State return journeys between 50 and 400 km there are fixed rates: Lithuania €22, Latvia €22. Please note that no contribution will be paid for travel under 50km. For more information, please consult <https://era-comm.eu/go/unit-cost-decision-travel> (COM Decision C(2021)35).
8. For those travelling within Estonia the contribution for travel for a distance between 50km and 400km is fixed at €16. Please note that no contribution will be paid for travel under 50km. For more information, please consult <https://era-comm.eu/go/unit-cost-decision-travel> (COM Decision C(2021)35).
9. Accommodation costs: International participants travelling more than 50km one-way will receive a fixed contribution of €214. National participants will receive an overall fixed contribution of €107. For more information, please consult <https://era-comm.eu/go/unit-cost-decision-travel> (COM Decision C(2021)35).
10. Successful applicants will be sent the relevant claim form and information on how to obtain payment of the contribution to their expenses. Please note that no payment is possible if the registered participant cancels their participation for any reason.

Participation

11. Participation at the whole seminar is required and participants' presence will be recorded.
12. A list of participants including each participant's address will be made available to all participants unless ERA receives written objection from the participant no later than one week prior to the beginning of the event.
13. The participant will be asked to give permission for their address and other relevant information to be stored in ERA's database in order to provide information about future ERA events.

Accommodation

14. ERA neither provides nor endorses any accommodation options for this event. Kindly consult your preferred accommodation provider for options.

Apply online for
“#Digitalisation and #AI in
Criminal Justice”:
www.era.int/?134019&en



Venue

Ministry of Justice of Estonia
Suur-Ameerika 1
10122 Tallinn
Estonia

Language

English

Contact:

Julia Reitz
Event Coordinator
Tel.: +49 (0) 651 9 37 37 323
E-Mail: jreitz@era.int

FIGHTING

Web3-Enabled Crimes

with Web2 Technologies & AI

A Practical Guide for Legal Professionals

Prosecutors · Judges · Legal Professionals in Criminal Justice



Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

What We'll Cover Today - 60 Minutes

01

The Web3 Landscape

Blockchain, crypto, key terms & address types

02

Crime Typology

Scams, laundering, ransomware & more

03

How VASPs Work

Exchanges, wallets & the regulated ecosystem

04

Legal Framework

MiCA, global regulation & evidence implications

05

Getting Evidence

MLATs, subpoenas, blockchain tracing

06

AI in the Mix

AI-powered crimes & AI investigative tools

07

Building Your Case

Practical steps, court presentation & tips

01

The Web3 Landscape

Understanding the technology before you can prosecute it

Web2 vs. Web3 — A Simple Distinction

WEB2 (What You Know)

- Centralized platforms (Google, banks, Facebook)
- A company holds your data & your money
- Courts can subpoena those companies
- Account identity is tied to real people
- Transactions can be reversed or frozen

WEB3 (The New Challenge)

- Decentralized networks — no single company owns it
- Users control their own assets via cryptography
- No central server to serve you a search warrant
- Accounts are just math (public/private keys)
- Transactions are final and pseudonymous

Key Insight: Web3 moves the chokepoint from the platform to the exchange (VASP).

Blockchain in Plain English



It's a public ledger

Every transaction ever made is recorded forever and visible to anyone. Bitcoin's entire history since 2009 is public.



Pseudonymous, not anonymous

Transactions show wallet addresses, not names. But addresses can often be linked to real identities through exchanges.



No borders

A wallet in your jurisdiction can send to anywhere instantly. Traditional financial controls don't apply automatically.



This helps investigators

Unlike cash, every crypto transaction leaves a permanent, traceable trail. The blockchain is your evidence.

Key Terms — What You'll See in Evidence

These six terms appear in virtually every crypto case. Know them before you open the exchange records.

Wallet

≈ Bank Account

Software that stores your cryptographic keys and lets you send/receive crypto. Like an app that controls your bank account — except only you hold the keys.

Address

≈ Account Number

A unique string of letters and numbers that identifies where crypto is sent. Public and shareable. Example: bc1qxy2kgd...f59y. One wallet can generate millions of addresses.

Transaction Hash (TXID)

≈ Wire Transfer
Reference

A unique ID for every single transaction on the blockchain. Unchangeable. Paste it into a block explorer to see exactly what was sent, when, and between which addresses.

Hot Wallet

≈ Current Account

A wallet connected to the internet — used for daily transactions. Higher fraud risk. Criminals use hot wallets to move funds quickly. Exchanges hold customer funds in hot wallets.

Cluster

≈ Beneficial Owner
Group

A group of addresses that analysis tools determine are controlled by the same person or entity. Key concept: one criminal may use 200 addresses — a cluster links them all back to one suspect.

Block Explorer

≈ Public Court Record
Search

A free website that lets anyone search the blockchain. Etherscan.io (Ethereum), Blockchain.com (Bitcoin). Paste any address or TXID to see its full history. No subpoena required.

Crypto Address Types — What You'll See in Evidence Files

Addresses look like random text but follow recognisable patterns. Knowing the type tells you which blockchain you're dealing with.

Type / Name	Starts With	Example (truncated)	Blockchain	What It Means for You
Bitcoin Legacy (P2PKH)	1...	1A1zP1eP5QGefi2...	Bitcoin	Oldest Bitcoin address. Still very common. Every tx on Blockchain.com is searchable.
Bitcoin Script (P2SH)	3...	3J98t1WpEZ73CNm...	Bitcoin	Multi-signature or script address. Often used by exchanges & criminal mixing services.
Bitcoin SegWit (Bech32 / P2WPKH)	bc1q...	bc1qxy2kgdygjrsg...	Bitcoin	Modern Bitcoin standard. Lower fees. Increasingly the default for exchanges & wallets.
Ethereum (Account-Based)	0x...	0x742d35Cc6634C...	Ethereum & ERC-20	One address, reused for all transactions. Easier to trace — full history under one ID.
Tron (Account-Based)	T...	TQdMRMG6Bwmk9Q...	Tron (USDT)	Common in Asian crime networks & pig butchering. USDT stablecoin runs on Tron.

Bitcoin (UTXO model — each coin tracked individually)

Account-based (Ethereum / Tron — balance tracked per address)

02

Crime Typology

What crimes look like in the Web3 world

The Web3 Crime Landscape



Investment Scams

Pig butchering, Ponzi schemes, fake exchanges. Victims tricked into depositing crypto that disappears.



Ransomware

Criminals encrypt victims' systems and demand crypto payment. Hospitals, cities, businesses targeted.



Money Laundering

Dirty money converted to crypto, mixed through multiple wallets and exchanges, then cashed out clean.



Dark Market Sales

Drugs, weapons, stolen data sold on darknet markets using crypto as the payment rail.



Fraud & Identity Theft

Stolen card data, hacked accounts converted to crypto for instant, irreversible extraction.



Sanctions Evasion

Sanctioned individuals and states use crypto to move money outside of the regulated financial system.

Case Study: Pig Butchering — The #1 Crypto Fraud

1

Initial Contact

Random text or social media message — 'wrong number' or 'I think we met'

2

Build Trust

Weeks of relationship building. Romantic interest or friendship. Never rushes.

3

Introduce Crypto

Shares 'investment success.' Directs victim to a fake but professional-looking exchange.

4

Small Wins

Victim deposits small amounts. Platform shows huge profits. Victim is hooked.

5

Slaughter

Victim deposits life savings. Suddenly can't withdraw. Platform disappears. Funds gone.

\$3.3B

Lost to pig butchering in 2023 (FBI IC3)

1 in 3

Victims sent ALL savings to these scams

Crypto

Used in nearly 100% of pig butchering cases

03

How VASPs Work

Virtual Asset Service Providers — your key partners in investigation

What is a VASP?

VASP = Virtual Asset Service Provider

Any business that exchanges, transfers, safeguards, or manages virtual assets (crypto) on behalf of others.

Centralized Exchanges



Binance, Coinbase, Kraken

Biggest category. Users trade crypto with a regulated platform. Full KYC required.

Custodial Wallets



Exchange wallets, crypto banks

Platform holds the user's private keys. They control the funds. They have records.

OTC Desks



Brokers, peer-to-peer platforms

Large trades done off-exchange. Often preferred by high-volume movers — including criminals.

Crypto ATMs



Bitcoin ATMs (BTMs)

Physical kiosks that exchange cash for crypto. Heavily used in fraud cases. Operator is the VASP.

What VASPs Know About Their Users (KYC/AML)

Regulated VASPs are required to collect and verify customer identity — just like a bank.

Government ID



Passport, driver's license — tied to real identity

Email & Phone



Verified contact info, often linked to other accounts

IP Address & Device



Login history, device fingerprints, geolocation data

Transaction Records



Full history: amounts, wallets, timestamps, counterparties

Bank Account Linkage



Fiat on/off-ramp records connecting crypto to real money

Beneficial Ownership



For corporate accounts: who actually owns the entity

Key Insight: A regulated VASP is essentially a bank with a blockchain frontend. They have what you need.

Inside a VASP: Who Handles Legal Requests

Legal / Compliance

Handles subpoenas, court orders, MLATs. Primary contact for law enforcement. Has documented processes for responding.

AML / Financial Intelligence / Investigations

Monitors transactions for suspicious patterns. Files SARs/STRs. Has detailed transaction analysis and risk profiles.

Customer Support

(Usually) NOT the right team for legal requests. But can confirm account existence or flag escalation needs.

Law Enforcement Portal

Most major exchanges (Coinbase, Binance, Kraken) have a dedicated LEA portal for formal legal requests. Use it.

3.5

The Legal Framework

How crypto is regulated globally — and what that means for your cases

The Global Regulatory Landscape — Your Evidence Depends on This

Where a VASP is registered determines what legal tools you have. The framework varies dramatically by jurisdiction.

European Union

MiCA (Dec 2024)

- Single CASP licence — one country, valid in all 27
- Mandatory KYC, AML, Travel Rule (TFR) from Dec 2024
- ESMA public CASP register — check if any VASP is licensed
- Non-compliant VASPs must delist or wind down
- For you: Strongest evidence base. Subpoena goes to NCA-licensed CASP.

 **Best jurisdiction for evidence**

United Kingdom

FCA Registration

- Crypto firms must register with FCA for AML purposes
- Full authorisation regime in development (2025–26)
- Similar KYC/AML obligations to EU — good records expected
- UK not bound by MiCA post-Brexit — separate framework
- For you: Strong MLAT/UKCA route. UK courts cooperative.

 **Good jurisdiction — standard process**

United States

FinCEN / SEC / CFTC

- Fragmented: FinCEN (AML), SEC (securities), CFTC (derivatives)
- MSB registration required — KYC/AML via Bank Secrecy Act
- GENIUS Act (July 2025) = first federal stablecoin framework
- Coinbase, Kraken, Gemini: US-based, strong LEA portals
- For you: Use LEA portals. Domestic subpoena or MLAT.

 **Good but complex — know the agency**

Singapore / Hong Kong

MAS PSA / SFC VATP

- Singapore: MAS Payment Services Act — strict licensing
- Hong Kong: SFC VATP regime launched 2023, stablecoin 2025
- Both require KYC/AML, but records harder to access for EU/NL
- MLAT with NL exists but slow; voluntary route often better
- For you: MLAT or direct voluntary request to compliance team.

 **Cooperative but slower — allow weeks**

Offshore / Unregulated

Seychelles / BVI / Anon

- Some exchanges registered in Seychelles, BVI, Marshall Islands
- No mandatory KYC = possibly NO identity records exist
- No regulatory authority to pressure compliance
- Blockchain analysis is your primary tool — trace to next hop
- For you: Focus on blockchain evidence. Find the regulated exit.

 **Limited — lean on blockchain analysis**

MiCA Deep Dive — What Europe's New Framework Means for Prosecutors

MiCA — Markets in Crypto-Assets Regulation

► Fully in force Dec 2024

All 27 EU member states. The first comprehensive crypto law anywhere in the world. Replaces 27 different national frameworks with one unified rulebook.

► VASP → CASP

The old term 'VASP' is replaced by 'CASP' (Crypto-Asset Service Provider) under MiCA. Same entities — stricter obligations. No MiCA licence = illegal to operate.

► Passporting

A CASP licensed in one EU country can serve clients across all 27. Coinbase licensed in Luxembourg. Bitstamp in Luxembourg. This is why they chose it.

► Travel Rule (TFR)

From Dec 2024: every crypto transfer must carry sender and recipient identity data — just like SWIFT wire transfers. A goldmine for investigators.

► Transitional gap

Some firms operate under national grandfathering until July 2026. During this window, pre-MiCA national rules still apply. Check ESMA's register first.

Impact on Criminal Cases — At a Glance

Is the VASP licensed?

Check ESMA interim register (public). If licensed = MiCA obligations apply = they have your data.

Anonymous crypto ATMs?

Banned EU-wide from Sept 2025. All BTM operators must collect KYC. Historical anonymous records = gap.

Travel Rule records?

From Dec 2024 every transfer has sender/recipient data attached. Serves as built-in evidence trail. NOTE — issues with interoperability and implementation, may not be available or credible.

Offshore VASP refuses?

MiCA has no extraterritorial reach. Use blockchain analysis to trace to EU-licensed VASP and subpoena that one.

VASP in grandfathering?

Pre-MiCA national rules still apply — KYC still required. Check which national authority supervises them.

DeFi / unhosted wallets?

Outside MiCA scope (for now). No KYC records exist. Blockchain analysis is your only tool.

04

Getting the Evidence

Legal pathways to obtain crypto account data

Four Ways to Get Evidence from a VASP

1 Domestic Subpoena / Court Order

Speed: Days–Weeks

- VASP operates in your jurisdiction
- Serve legal process to registered agent or LEA portal
- Expect: KYC docs, transaction history, IP logs
- Most major exchanges comply promptly

2 Mutual Legal Assistance Treaty (MLAT)

Speed: Months

- VASP is in a foreign jurisdiction
- Formal government-to-government request
- Slow but legally enforceable
- Parallel voluntary request can speed things up

3 Voluntary Emergency Disclosure

Speed: Hours–Days

- Imminent risk to life or ongoing fraud
- Exchanges can voluntarily share info
- Lower threshold — no court order needed
- Best for freezing live criminal operations

4 Blockchain Analysis (No Warrant Needed)

Speed: Immediate

- Public blockchain data — no legal process required
- Use commercial tools, such as Chainalysis, TRM Labs, Elliptic, Crystal, etc.
- Trace flows, identify clusters, find VASP entry points
- Foundation of most crypto prosecutions today

What to Request From a VASP — Checklist

When drafting your subpoena or legal request, always ask for ALL of the following categories:



Identity Records

- Full legal name, date of birth
- Government ID documents (copies)
- Selfie / liveness verification photos
- Beneficial ownership for entity accounts



Contact & Access

- Email address(es)
- Phone numbers (including 2FA numbers)
- IP login history with timestamps
- Device fingerprints and browser info



Financial Records

- Complete transaction history
- Wallet addresses owned/used by account
- Bank accounts linked for fiat on/off-ramps
- Any holds, flags, or suspicious activity reports filed



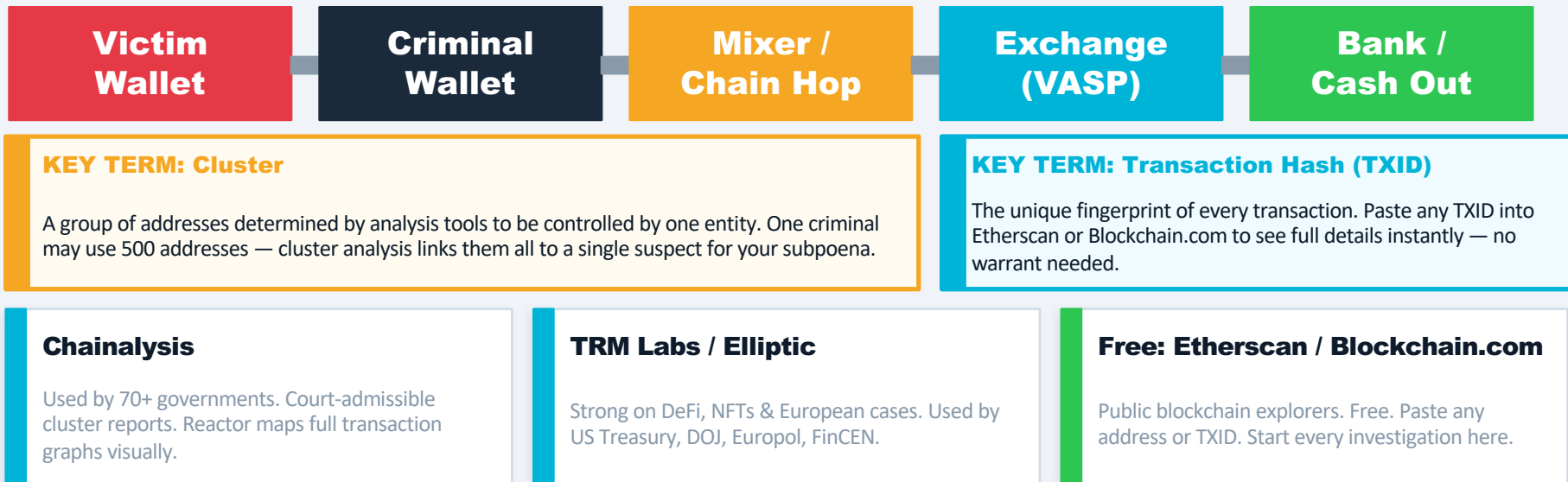
Account Activity

- Account creation date and method
- All linked accounts or referrals
- Any previous name changes or identity updates
- Account status: active, suspended, closed

NOTE: major VASPs follow GDPR framework and alike, hence – be equally prepared to respect data minimization.

Following the Money: Blockchain Tracing

The blockchain is a public record. Anyone can trace transactions — including you, with the right tools.



💡 *Every blockchain address and TXID in your evidence can be verified publicly — before filing any legal process.*

05

AI in the Mix

How AI supercharges both crime and investigation

AI as a Criminal Tool

AI-Generated Scam Personas



ChatGPT-level AI runs hundreds of simultaneous 'pig butchering' conversations. Each victim gets personalized attention. No human scammer required.

Deepfake Identity Fraud



AI swaps faces onto real ID documents, defeating bank selfie-verification. Case: 46 ABN AMRO accounts opened with deepfaked passports (Amsterdam, 2026).

AI-Powered Phishing



Mass personalized phishing emails written by AI, tailored to each victim's LinkedIn/social profile. Dramatically higher success rates than generic phishing.

Automated Laundering Bots



AI scripts automatically split, route, and reassemble crypto through hundreds of wallets and exchanges faster than any human could track.

46 Bank Accounts Opened with AI-Faked Passports

How one fraudster used AI face-swapping to defeat bank identity verification — at scale

1

Harvest Real IDs

Scraped from social media + fake Marktplaats rental ad requesting copies of passports

2

AI Face Swap

Used AI to replace the victim's passport photo with his own face — watermarks & greyscale preserved

3

Bypass KYC Selfie

ABN AMRO's online onboarding asks for ID upload + live selfie. Deepfaked docs passed the check.

4

Open 46 Accounts

Accounts opened in innocent victims' names. Debit cards issued. Fraud undetected for months.

5

Detected by Accident

A woman's passport was submitted with a man's selfie — gender mismatch triggered investigation

46

accounts opened across ABN AMRO

30 months

prison sentence demanded by prosecution

€6,240

compensation ordered to ABN AMRO

Key lesson

Single-layer KYC cannot stop deepfakes

AI as an Investigative Weapon

The same AI capabilities available to criminals are available to law enforcement — often better.



Transaction Graph Analysis

AI can identify wallet clusters, suspicious flow patterns, and likely real identities (if leaked or available in open-source) behind pseudonymous addresses at a speed no human analyst can match.



OSINT & Identity Linking

AI tools can scan social media, forums, leaked databases to link wallet addresses to real people. A careless post or email can unmask an entire criminal ring.



Deepfake Detection

AI-powered forensics tools can detect signs of deepfake manipulation in video and audio evidence — essential as defense attorneys increasingly challenge digital evidence.



Document Analysis

AI can rapidly analyze thousands of exchange records, flagging suspicious transactions, cross-referencing counterparties, and building timeline visualizations.



Natural Language Processing

AI can parse darknet market communications, encrypted chat logs, and financial disclosures to find patterns, codenames, and co-conspirator links.



Asset Recovery Prediction

AI models can assess likelihood of asset recovery, optimal exchange targets for freeze orders, and identifies co-mingled funds in complex laundering chains.

AI Evidence in Court — What You Need to Know



Blockchain Analysis IS admissible

Chainalysis and similar tools have been accepted in federal courts and jurisdictions worldwide. Key: the analyst must be qualified as an expert witness and methodology must be documented. Heuristics CAN be challenged though.



Defense will challenge AI methodology

Expect 'black box' arguments. Your AI vendor must be able to explain how their algorithm works. Always have a human expert who understands the underlying analysis.



Chain of custody for digital evidence

All blockchain evidence and exchange records must have documented, unbroken chain of custody. Hash the records when received. Treat digital evidence like physical evidence.



Deepfake/AI-generated evidence scrutiny

As defense uses AI challenges more aggressively, prosecutors must authenticate digital evidence rigorously. Keep original files, metadata, and platform export documentation.

06

Building Your Case

Practical steps from complaint to conviction

The Crypto Case Investigation Workflow

1 Preserve the Complaint

Collect all victim communications, screenshots, wallet addresses given, platform URLs. Do this before anything disappears.

2 Public Blockchain Recon

Use free explorers (Etherscan, Blockchain.com) to map the transaction flow. Identify which exchange(s) received the funds.

3 Identify Target VASPs

Blockchain analysis tools will cluster addresses to known exchanges. These are your subpoena targets.

4 Legal Process

Issue targeted subpoenas or MLAT requests to identified exchanges. Use emergency disclosure for live/ongoing fraud.

5 Analyze Returns

Exchange records + blockchain data together will identify the criminal. Cross-reference with victim's bank records.

6 Build the Narrative

Visualize the money flow for the court. Blockchain evidence is complex — your job is to make it simple for a jury.

Explaining Crypto to a Jury — Proven Analogies

Wallet Address → Bank Account Number

Every wallet has a public address (like an account number) and a private key (like a PIN). Anyone can send to the address. Only the key holder can spend.

Blockchain → Permanent Bank Statement

Every transaction ever made is recorded publicly and forever. Unlike a bank you can subpoena, this record exists whether the criminal cooperates or not.

Pseudonymous → Numbered Swiss Bank Account

The blockchain shows transactions between numbered accounts, not names — but unlike Swiss banks, the records are fully public and traceable to the exchange.

Private Key → Physical Safe Combination

Whoever has the private key controls the funds. Possession of the key = control. Important for establishing criminal possession and intent.

Mixing / Tumbling → Money Laundering via Casino

Just like breaking up cash at a casino, mixing services try to obscure the origin of funds. Courts recognize this as evidence of criminal intent.

VASP / Exchange → Bank with Extra Steps

Regulated exchanges operate under the same KYC/AML rules as banks. A subpoena to Coinbase is not legally different from a subpoena to Chase.

Key Takeaways

01 **Crypto is traceable.**

The blockchain is a public, permanent ledger. Cash is harder to follow than crypto.

02 **VASPs are your partners.**

Regulated exchanges operate like banks. Use their LEA portals and standard legal process to get KYC and transaction data.

03 **The evidence already exists.**

Before any subpoena, blockchain analysis can tell you where the money went and which exchange received it.

04 **AI doubles both sides.**

Criminals use AI to scale scams. Investigators use AI to trace funds and identify suspects. Know both sides.

05 **Simplify for the court.**

Use banking analogies. Visualize the money flow. The jury doesn't need to understand crypto — they need to understand the story.

Questions?

Remember:

The blockchain never lies.

Crypto criminals leave better trails than cash criminals.

You have more tools than you think.





Co-funded by
the European Union

ERA Tallinn, May 2026

CONDUCTING FORENSIC ANALYSIS AT THE CRIME SCENE



Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not
necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible
for them.



Danijel Sladović

- 🔗 Consultant at INsig2, Department of Digital forensics
 - Training, conducting investigations, consultant for clients
- 🔗 Studied at Faculty of Organization and Informatics
 - Masters degree
- 🔗 Over 8y of experience in Digital forensics
- 🔗 Certificates: CEH, Blackbag, Magnet, Belkasoft, CMFF, CCO, CCPA, Passwords ...
- 🔗 Specialist in Linux, MacOS, Network, Malware, Cloud, Internet forensics, Python, Dark Web, Car ...

www.insig2.com
DanijelS@insig2.com

About INsig2

- Established in 2004, HQ in Zagreb
- 80+ highly educated employees
- Educational & Training centre



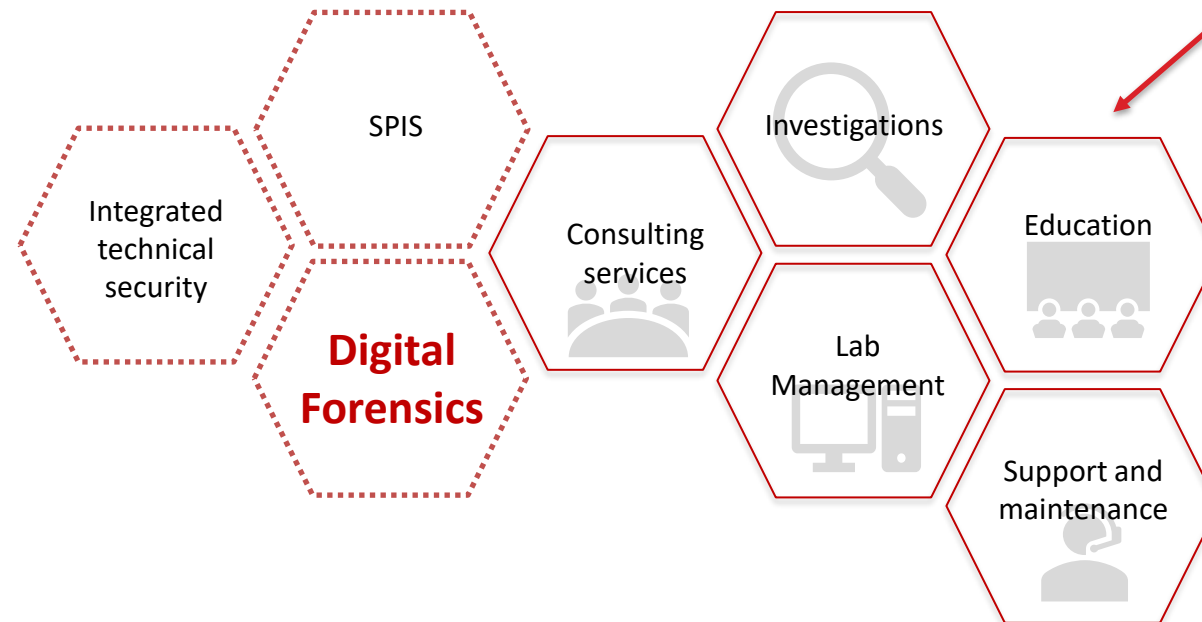
Education & Training Centre in Zagreb, Croatia

- Accommodates up to 15 people per classroom
- Equipment, forensic tools & materials provided

INsig2

- ☞ Three business units
- ☞ „One-stop-shop” in the field of Digital Forensics

We teach what we do!



E-learning platform

- ☞ Customized courses
- ☞ For legal entities, law enforcement, and private sectors
- ☞ Courses on deeper aspects of digital forensics and forensic value of the evidence while collecting, processing, and presenting digital evidence in criminal and administrative proceedings
- ☞ Website: <https://insig2-and-zyberglobal.learnworlds.com/>



Fundamentals of digital forensics for lawyers and judges

This course is intended for lawyers, judges and public prosecutors in order to help them understand the basics of digital forensics.



Fundamentals of digital forensics for private sector

This course is intended for various industry professionals working in private sector such as IT administrators, managers, IT security



Password Management

This course covers different lock security methods, guidelines on securely storing your passwords, various password managers and



Computer and mobile forensics

Computer forensics

- ☞ Branch of digital forensic science, focused on evidence found and recovered from computers and digital storage media, in legally admissible manner
- ☞ Importance of computer forensics today:
 - Supporting legal processes
 - Cybercrime and incident response
 - Complex digital crimes



Mobile forensics

- 🔗 Branch of digital forensics focused on recovering and analyzing data from mobile devices, such as smartphones and tablets
- 🔗 Essential to investigations:
 - Mobile devices contain a wealth of evidence that can be used in any type of investigation
 - This data can be used to track down a suspect, understand a crime
 - Often the only source of evidence and most common one
- 🔗 Constantly evolving



Computer forensics

Then - Now

- 🔗 Data storage
 - GB vs TB + Cloud
- 🔗 OS & File systems
 - VM
- 🔗 Encryption
- 🔗 Anti-forensic tools
- 🔗 Tools & techniques



Mobile phone forensics

Then - Now

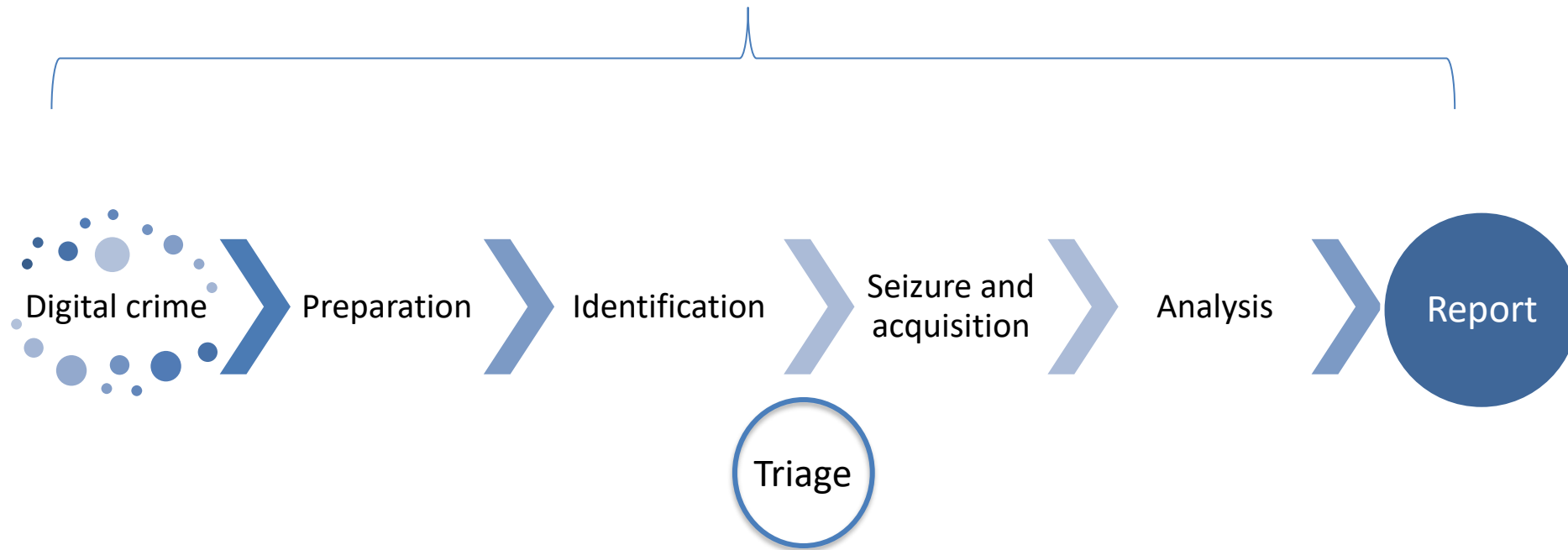
- 🔗 Functions & data
- 🔗 OS
- 🔗 Data storage
 - GB vs TB + Cloud
- 🔗 Encryption
 - Pa\$\$w0rd?
- 🔗 Tools & techniques
- 🔗 Cryptocurrency
- 🔗 IoT + connected devices



E SIM



Digital forensics



Preparation

🔗 Equipment considerations

- Camera, notes, pens, extension cord, cables, Forensic preview and imaging tools, external hard drive, evidence bags, faraday bags, etc.

🔗 Intelligence assessment

🔗 Crime scene

- Secure it, watch for potential threats
- Document everything
- Look for additional source of evidence

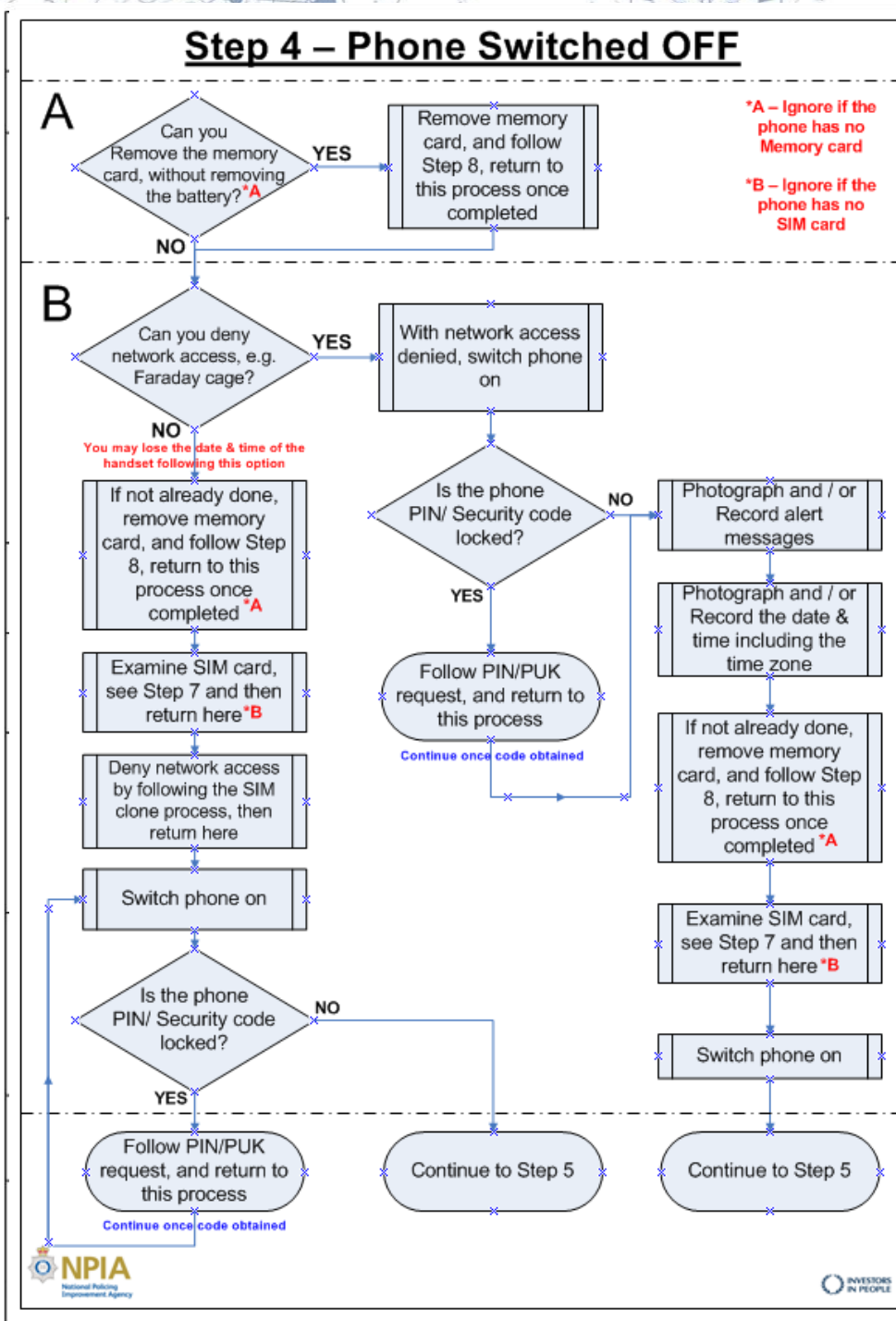


Preparation

- 🔗 Prepare for interviewing the suspect, family members, victims and witness
 - Passcode
 - Any useful information – password dictionary 😊
- 🔗 Prepare questions before getting on crime scene
 - Be good negotiator



- Standardized process
- Chain of Custody
- Rules – ACPO rules
- Best practices – SV
- Standard Operating



cial for maintaining
ble investigations

CHAIN OF CUSTODY	
Received From:	_____
Received By:	_____
Date:	_____ Time: _____ am/pm
Received From:	_____
Received By:	_____
Date:	_____ Time: _____ am/pm
Received From:	_____
Received By:	_____
Date:	_____ Time: _____ am/pm
Received From:	_____
Received By:	_____
Date:	_____ Time: _____ am/pm
Received From:	_____
Received By:	_____
Date:	_____ Time: _____ am/pm

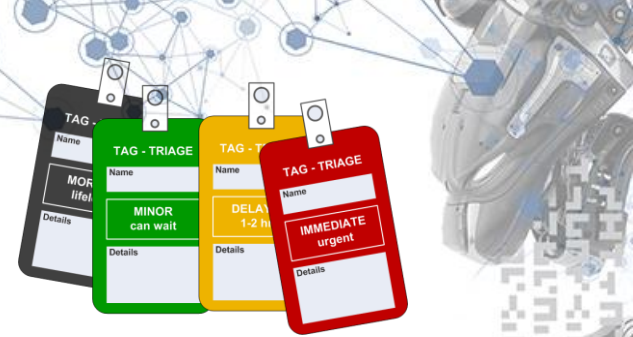
CAT NO. C0C2198





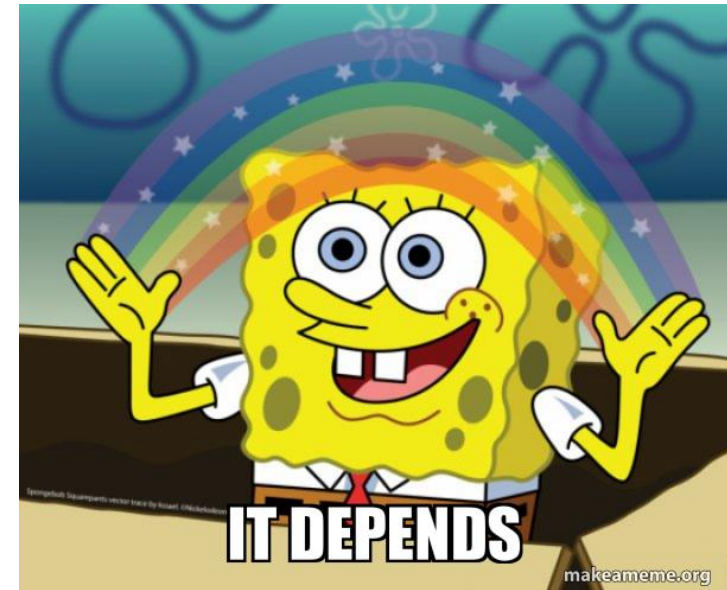
Triage at the crime scene

Triage



- ☞ The process of prioritizing or selecting objects, people, or information according to certain criteria
 - applicable in various areas of digital forensics
 - CO, corporate, Lab or Live scene

- ☞ General procedure
 - If the device is off, leave it off
 - If the device is on, well... it depends...



Computer Triage

When computer is on:

- Harmful process running or system is locked:
 - Turn it off
 - Document, document, document!
 - Pack it and transfer to the lab
 - Time!
- No destructive process observed:
 - Time
 - Document
 - RAM dump
 - Scanning and triage analysis
 - Determining

When computer is off:

- Check attached devices and cables
- Document
- Photo
- Pack it
- Transfer to lab



Computer Triage

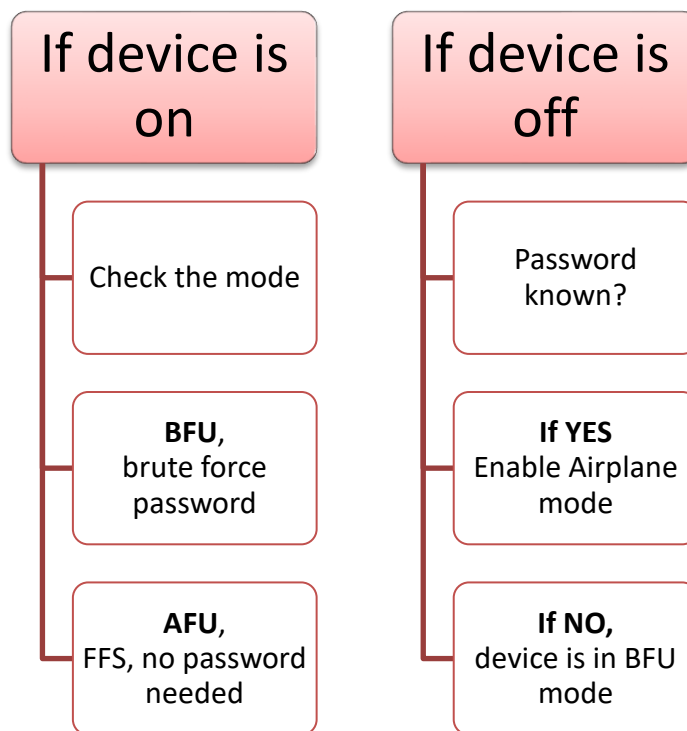
- 🔗 Encryption
- 🔗 Connectivity and rights
- 🔗 Tools:
 - Magnet Outrider
 - ADF Triage
 - Cyacomb Examiner
 - Belkasoft T
 - FTK Imager
 - Scripts
 - Etc.



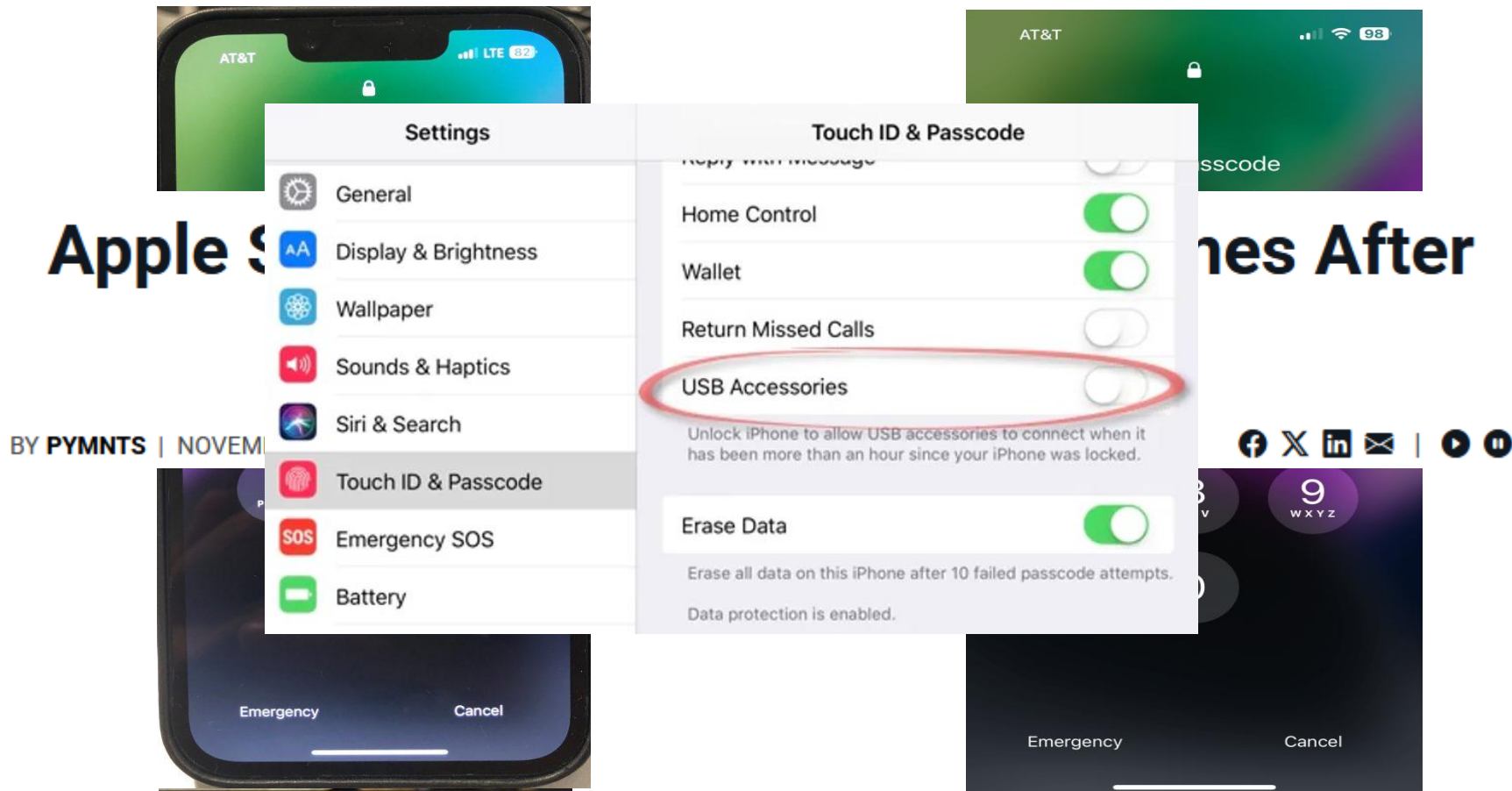
Mobile phone triage

🔗 Mobile phones can be in 2 states

- ON (AFU and BFU)
- OFF (It depends!)



How to identify AFU / BFU ?



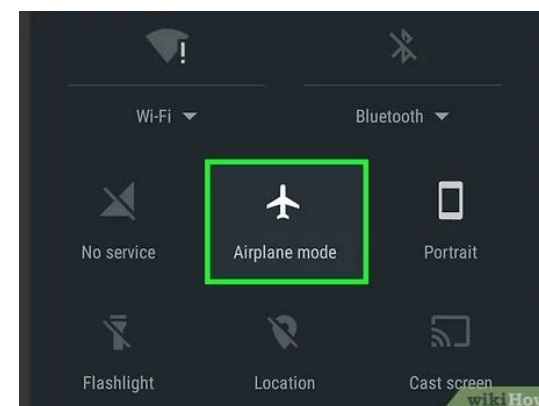
Phone in BFU mode

Phone in AFU mode

Mobile phone triage

☞ When phone is unlocked:

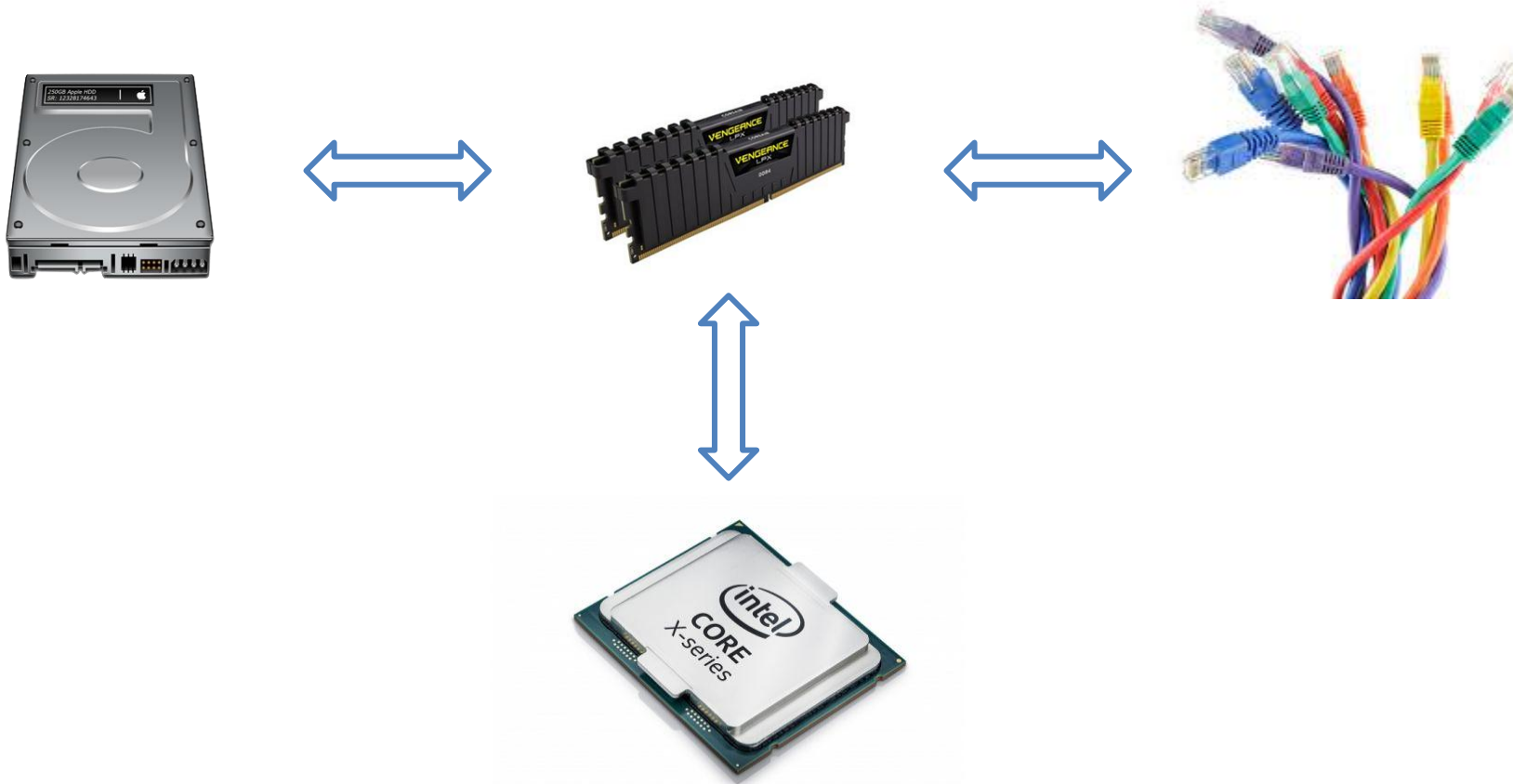
- Airplane mode
- Power source
- Start triage process
- Lock and screen settings
- Additional isolation
- Document
- Pack it
- Transfer to the lab





Gathering digital evidence from live memory

RAM overview



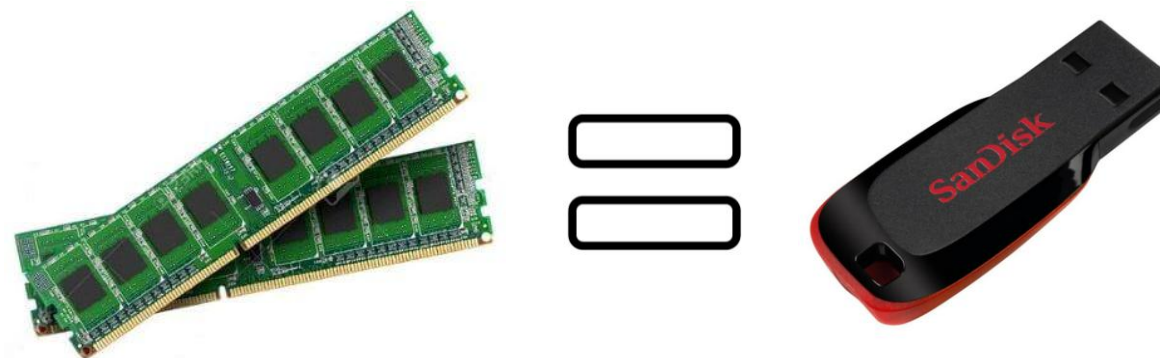
Main memory contains best evidence!!

Why live data is important?

🔗 Some data can only be found in RAM memory

- Volatile data
- Fileless malware
- Portable apps

🔗 Real time insights

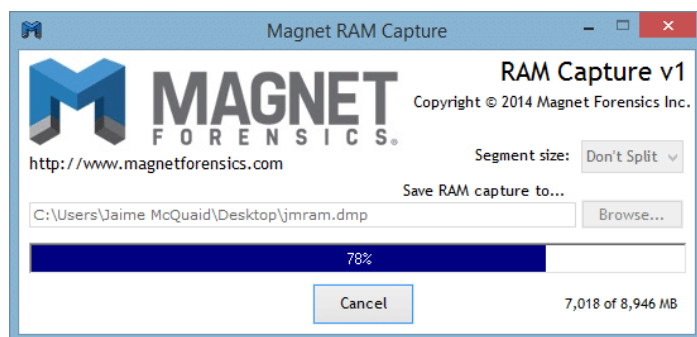


Imaging and analysis of RAM



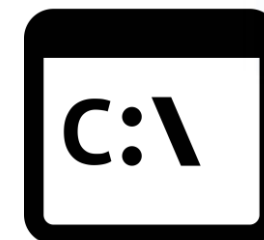
Imaging

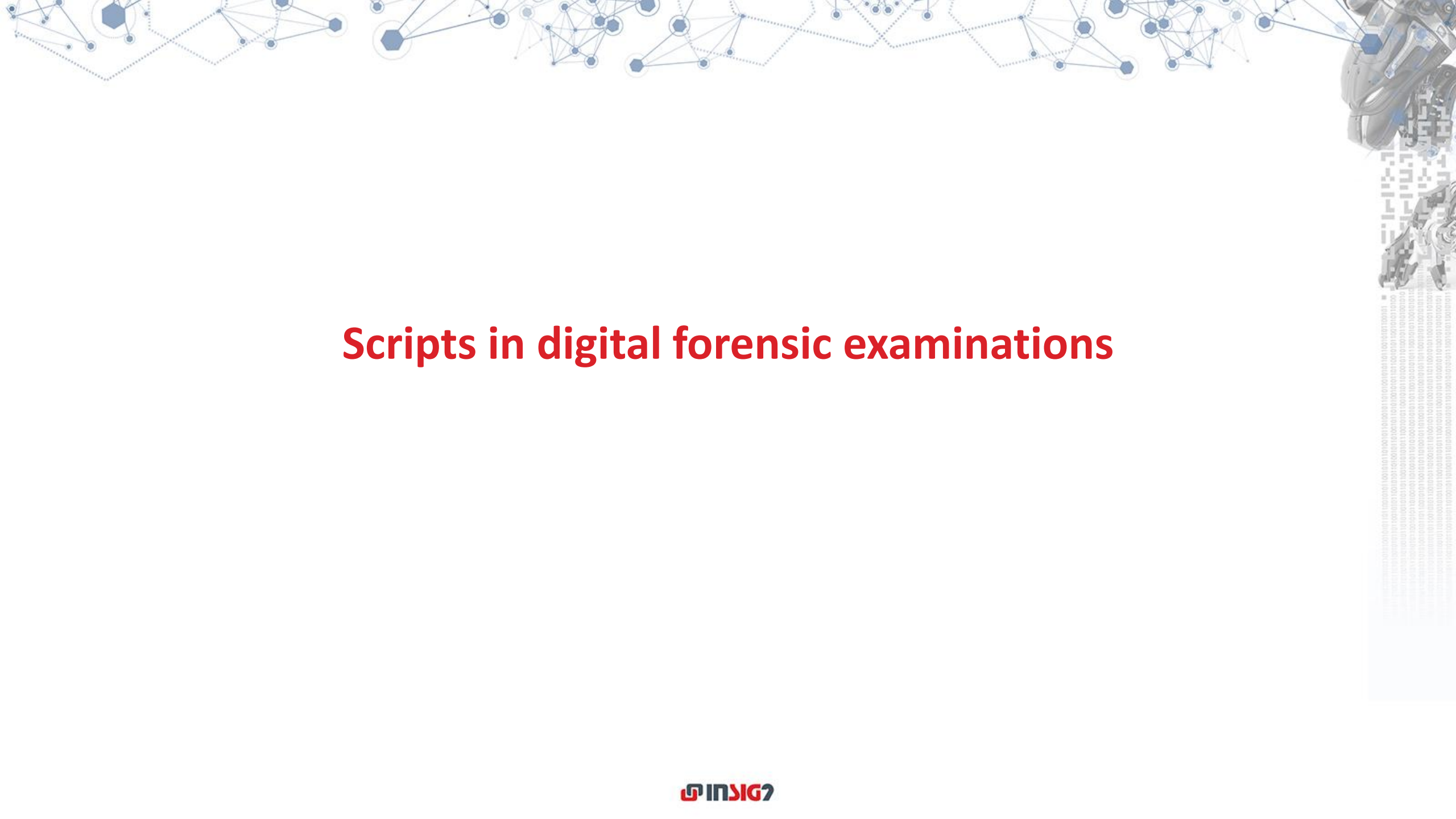
- Which tool to use?
 - Dumpit, Belkasoft RAM capture, Magnet RC
 - Footprint
- Dump entire memory
- External drive
- Fast imaging
- Unlocked PC and admin rights
- Easy to use



Analysis

- Not easy to analyse
 - steep learning curve
- Lack of forensic tools
 - Tools: Volatility, Magnet Axiom, MemProcFS,...
- With analysis we can gather:
 - Malware
 - Passwords
 - Open connections
 - Unsaved files
 - Safe Browsing
 - Email and chat residue files
 - Users and their personal files
 - Pictures
 - Documents





Scripts in digital forensic examinations

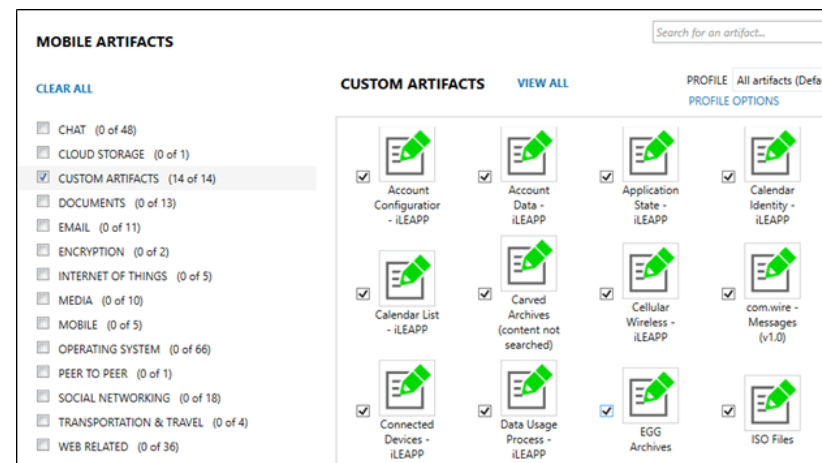
Scripts in digital forensics

☞ Most forensic tools are based on scripts

☞ Why do we need scripting then?

☞ Examples:

- Automating forensic processes – Magnet Automate
- Unsupported artifacts – Magnet Axion
- Malware detection
- OSINT



Scripts in digital forensics

```
$OutFile = "$env:USERPROFILE\Desktop\info.txt"

"=== PC INFO ===" | Out-File $OutFile
hostname | Out-File $OutFile -Append
systeminfo | findstr /B /C:"OS Name" /C:"OS Version" | Out-File $OutFile -Append

"`n=== USER ===" | Out-File $OutFile -Append
whoami | Out-File $OutFile -Append

"`n=== NETWORK ===" | Out-File $OutFile -Append
ipconfig | Out-File $OutFile -Append

"`n=== WIFI PROFILES (NO PASSWORDS) ===" | Out-File $OutFile -Append
netsh wlan show profiles | Out-File $OutFile -Append

Write-Host "Done. File saved to $OutFile"
```



Digital forensic labs

Digital forensic labs

- Facilities dedicated to the identification, acquisition, analysis, and reporting of digital evidence
 - Strict access control
- Key Components:
 - Case Acceptance Area
 - IT Infrastructure
 - Evidence Storage
- ISO 17025
- Specialized divisions: computer forensics, mobile phone forensics, video and audio forensics



Digital forensic labs

Equipment for digital forensic labs

- Forensic workstations
- Forensic duplicators
- Forensic software
 - AI and automation
- Data recovery tools
- Evidence storage
- Soldering station
- Microscope
- Power supply
- Antistatic mat
- Camera
- ...



Computer forensic lab



Mobile phone forensics lab



The image is a collage illustrating a mobile phone forensics laboratory. At the top, a network diagram with blue nodes and lines is visible. Below it, the title "Mobile phone forensics lab" is written in red. The collage includes several photographs: a cluttered workbench with various electronic equipment, a microscope, and a blue device labeled "MOBILE DEVICE (MD-700)"; a black "BLOCK BOX" device; and a clean, organized workstation with a computer monitor displaying a circuit board, a flexible gooseneck lamp, and a vacuum cleaner. The bottom right corner features the "INSIG2" logo.



Conclusion



Digital forensic analysis is a race against time, where investigators must constantly adapt to the ever-accelerating pace of technological change.



danijel.sladovic@insig2.com

Tallinn, 7-8 May 2026

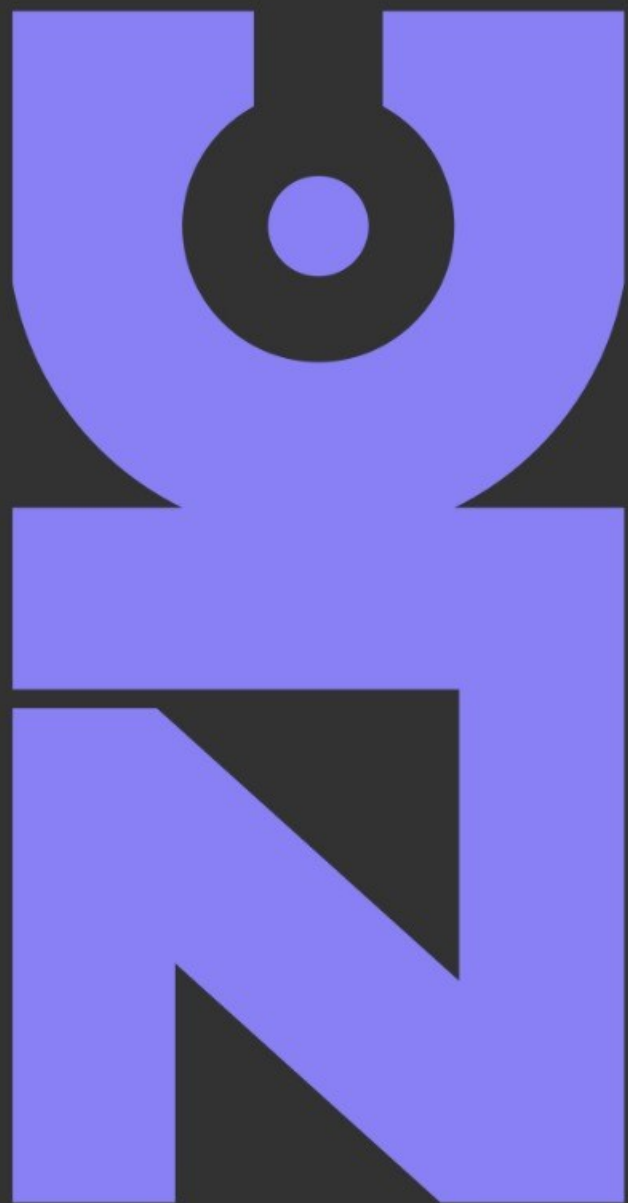
AI, emerging trends in social network investigations and how technology is changing this landscape



George M.R. Zlati



**Not
another
brick in
the law.**



ZLATI IONESCU CHIPERI

**Not
another
brick in
the law.**



Strong focus on

- Cybercrime
- MiCAR compliance
- Cybersecurity



Overview



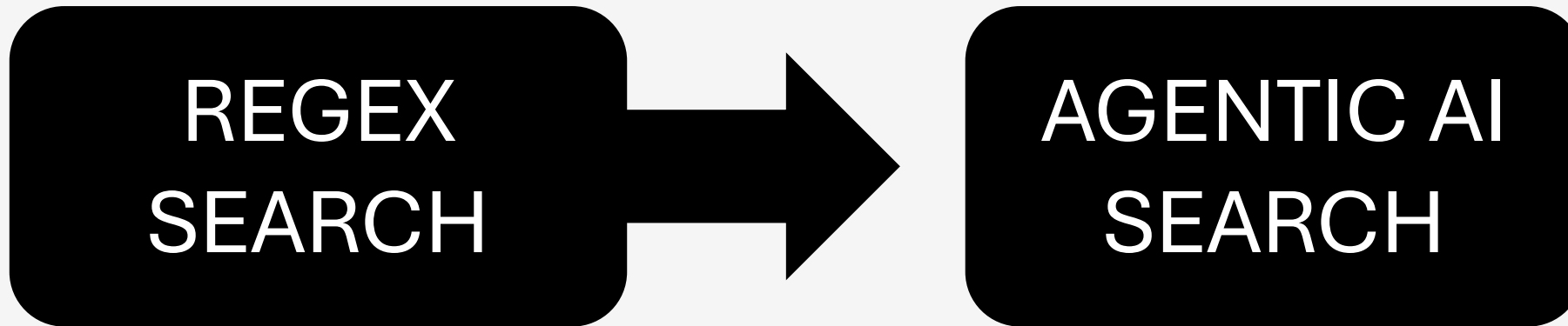
Evidence obtained from social media applications is the new frontier for digital forensics. The plethora of social media applications combined with hundreds of thousands of its users generate large amounts of transmissions daily, yielding a lot of digital evidence for forensic analysis. 4.48 billion people actively used social media applications in 2021, which was a 13.1% increase from 3.69 billion in 2020, indicating the projected increase in these numbers over the years Dean (2021).

2016

- Manual profile review
- Screenshots of the user interface
- Searching for names and usernames
- Single-platform focus (mostly Facebook)

2026

- Open source and commercial **tools for cross-platform investigation**
- OSINT runs as an **automated pipeline**: collection → enrichment → correlation
- **Agentic AI** is used for scraping and data correlation between platforms
- **Pattern detection** across large datasets



Target	Regex
Email	<code>\b[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\b</code>
Credit card (Visa / MC / Amex / Discover)	<code>\b(?:4\d{12}(?:\d{3})? 5[1-5]\d{14} 3[47]\d{13} 6(?:011 5\d{2})\d{12})\b</code>
Bitcoin legacy P2PKH / P2SH	<code>\b[13][a-km-zA-HJ-NP-Z1-9]{25,34}\b</code>
Bitcoin Bech32 (SegWit v0)	<code>\bbc1[ac-hj-np-z02-9]{11,71}\b</code>
Bitcoin Taproot (P2TR, Bech32m)	<code>\bbc1p[ac-hj-np-z02-9]{58}\b</code>
Ethereum / EVM (BSC, Polygon, Arbitrum...)	<code>\b0x[a-fA-F0-9]{40}\b</code>
Monero (XMR)	<code>\b[48][0-9AB][1-9A-HJ-NP-Za-km-z]{93}\b</code>
Litecoin	<code>\b[LM3][a-km-zA-HJ-NP-Z1-9]{25,34}\b</code>
TRON (TRX / TRC-20 — incl. USDT)	<code>\bT[A-HJ-NP-Za-km-z1-9]{33}\b</code>
Solana	<code>\b[1-9A-HJ-NP-Za-km-z]{32,44}\b</code>
Ripple (XRP)	<code>\br[1-9A-HJ-NP-Za-km-z]{24,34}\b</code>
Cardano	<code>\baddr1[ac-hj-np-z02-9]{50,110}\b</code>

Clara était une exploratrice courageuse. Un jour, elle décida de partir à la recherche d'un island mystérieux dont elle avait entendu parler dans de vieux livres. L'océan était agité, mais Clara ne reculerait pas. Avec sa boussole en main et son petit sac rempli d'objets essentiels, comme une apple pour la route, elle se dirigea vers l'inconnu.

Sur cette île, elle découvrit des paysages enchanteurs. Un tigre majestueux traversa son chemin alors qu'elle longeait une rivière sous la lumière de la moon. La forêt était dense et elle trouvait souvent des flowers cachées dans les fourrés. Le bruit constant du river la guidait vers une grotte dissimulée derrière de grands rochers.

En entrant, Clara trouva un vieux livre. Elle alluma sa light pour mieux voir, et en feuilletant, elle découvrit des secrets anciens. Il y était question d'un objet mystérieux, une stone sacrée, cachée quelque part sur l'île. Mais avant de partir, elle devait résoudre une énigme : dans le livre, il était écrit que la solution se trouvait dans les pages du book.

Avec son esprit aiguisé, Clara trouva une clé cachée dans les mots du livre. Elle comprit que tout cela la menait à une wallet oubliée depuis des siècles, un coin de trésor perdu. Elle prit le train de pensées nécessaire pour déchiffrer le mystère, sachant que la key était de se fier à son intuition et aux indices laissés sur son chemin.

Clara était une exploratrice courageuse. Un jour, elle décida de partir à la recherche d'un island mystérieux dont elle avait entendu parler dans de vieux livres. L'ocean était agité, mais Clara ne reculerait pas. Avec sa boussole en main et son petit sac rempli d'objets essentiels, comme une apple pour la route, elle se dirigea vers l'inconnu.

Sur cette île, elle découvrit des paysages enchanteurs. Un tiger majestueux traversa son chemin alors qu'elle longeait une rivière sous la lumière de la moon. La forêt était dense et elle trouvait souvent des flowers cachées dans les fourrés. Le bruit constant du river la guidait vers une grotte dissimulée derrière de grands rochers.

En entrant, Clara trouva un vieux livre. Elle alluma sa light pour mieux voir, et en feuilletant, elle découvrit des secrets anciens. Il y était question d'un objet mystérieux, une stone sacrée, cachée quelque part sur l'île. Mais avant de partir, elle devait résoudre une énigme : dans le livre, il était écrit que la solution se trouvait dans les pages du book.

Avec son esprit aiguisé, Clara trouva une clé cachée dans les mots du livre. Elle comprit que tout cela la menait à une wallet oubliée depuis des siècles, un coin de trésor perdu. Elle prit le train de pensées nécessaire pour déchiffrer le mystère, sachant que la key était de se fier à son intuition et aux indices laissés sur son chemin.

Backup Recovery Phrase

These 12 words are the ONLY way to restore your wallet if you forget your password. Please write them down and store securely offline.

1. liar 2. click 3. merge 4. scan 5. electric 6. early 7. garment
8. urban 9. wall 10. know 11. deliver 12. dinner

Do not save your Recovery Phrase on your computer or share it with anyone - write it down or print it

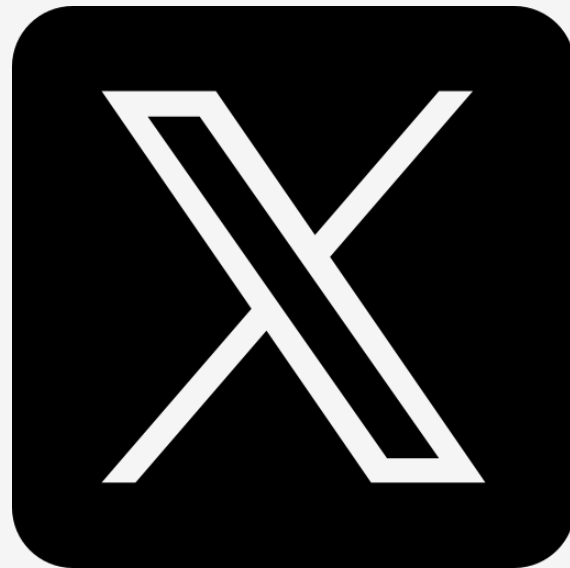
 Print Paper Wallet

I've Written it Down

What are social networks?

Social network

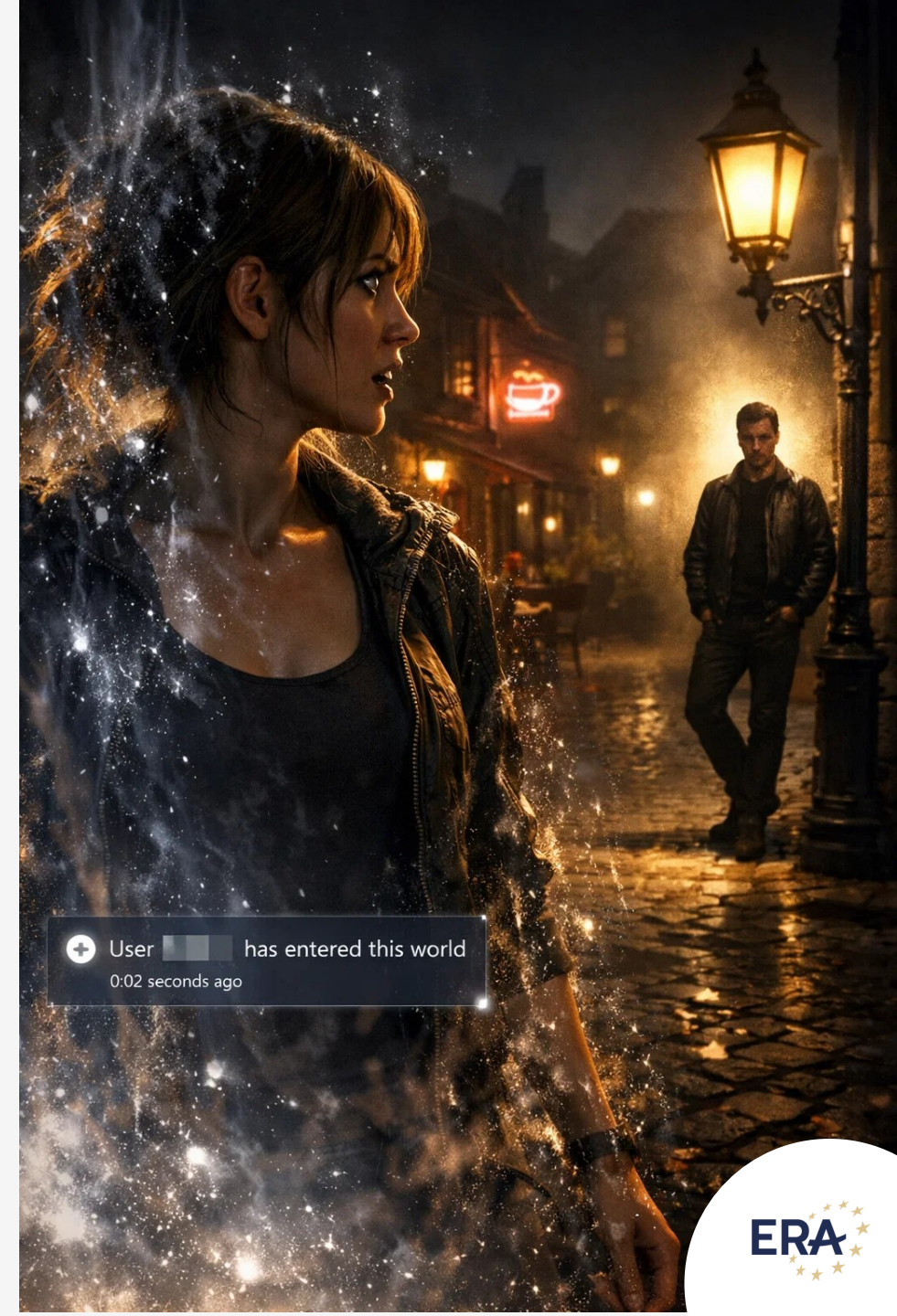
- connects people socially
- facilitates interaction between users
- allows for communication and content sharing
- profiles, posts, timelines are just additional use cases for social networks







Stalking an avatar in the metaverse



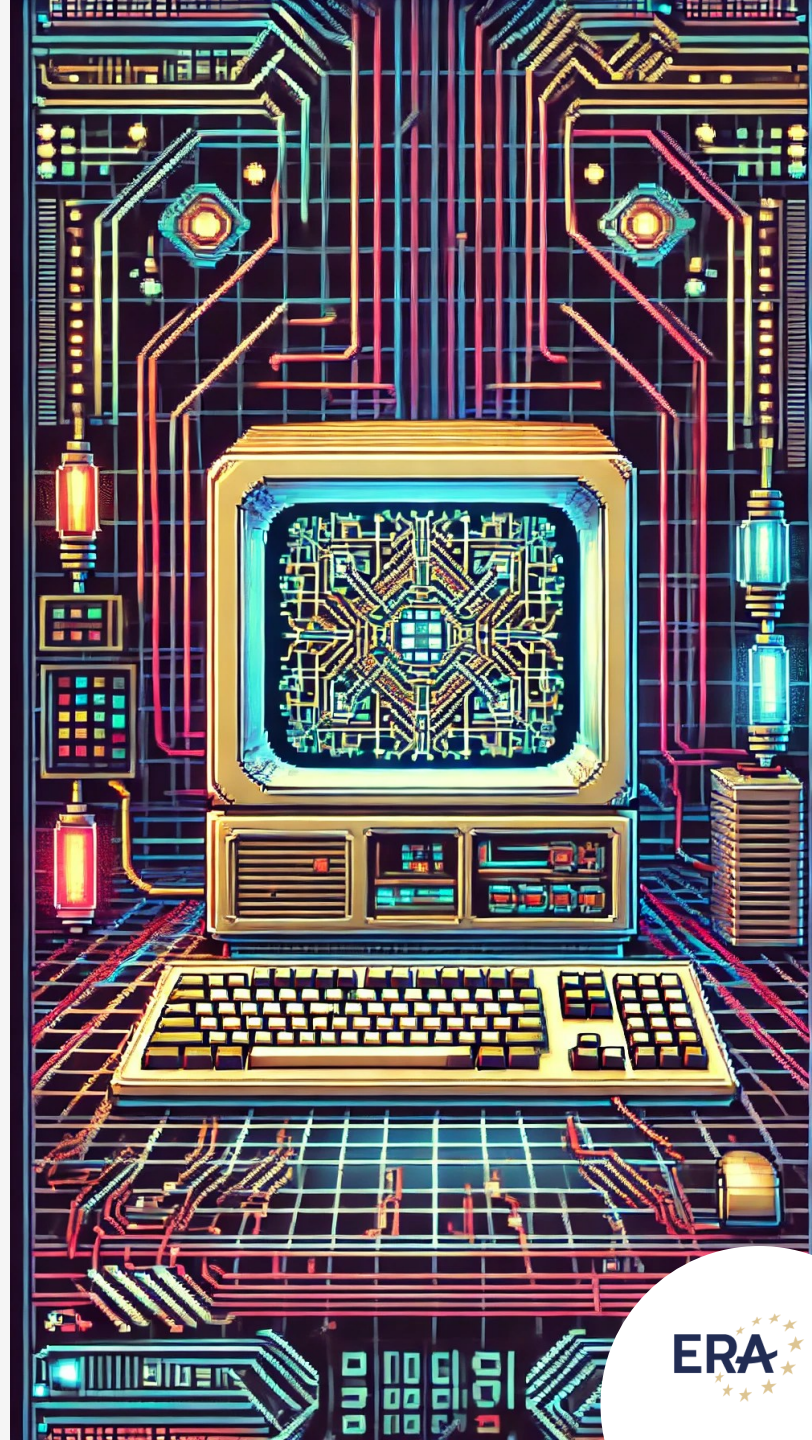
Identity-theft in the metaverse



Interception vs ambient surveillance



Digital search warrant?



What is social network investigation about?

Social network digital investigations

- Digital forensics on seized devices
 - Network digital investigation via apps and data stored on the device
 - *Post-mortem* digital investigation
- Digital forensics on publicly available accounts
 - Live digital investigation

Social network investigations

- Used by **lawyers**: finding out if a witness is still located in the country; gathering intelligence about an individual; gathering evidence in a civil or criminal case
- Used by **perpetrators**: finding information about the victim useful for scams; associating email accounts with other accounts and scraping the web for credentials
- Used by **investigative bodies**

**Substantive criminal law:
the power of a 👍**

-  **laughter** (approval? sarcasm? mockery? embarrassment?)
-  **enthusiasm** (about the content? the wording? the author?)
-  **affection** (towards the author? the message? the topic?)
-  **thinking** (interest? scepticism? confusion?)

Swiss Federal Tribunal. Bundesgericht, 29.01.2020, BGE 146 IV 23 (6B_1114/2018)



'Unlike the comment function, marking a "Like" or "Share" is, in principle, **evaluatively open** [*wertungsoffen*]. While "Sharing" carries no evaluation at all, **the meaning of the "Like" expression - despite the "thumbs up" - remains diffuse**, that is to say without binding resonance as regards the content concerned. [...] Thus, individual posts not infrequently lead to **(ir)rational herd behaviour** within the social-network collective.'

Swiss Federal Tribunal. Bundesgericht, 29.01.2020, BGE 146 IV 23 (6B_1114/2018)



'Unlike the comment function, however, marking a "Like" or "Share" is fundamentally open to interpretation. **While "sharing" implies no judgment whatsoever, the meaning of a "like," despite the "thumbs up," remains vague and lacks any binding response to the content in question.** Besides expressing appreciation for the content itself, it can also simply be applause for the wording or the author's relationship to it. Thus, individual posts often lead to (ir)rational herd behavior within the social network collective.'

Meiningen Regional Court. *LG Meiningen 6 Qs 146/22*

- After the killing of two police officers near Kusel (Rhineland-Palatinate), one Facebook user posted: *'Not a single second of silence for these creatures.'*
- Another user (the suspect) liked the post

Meiningen Regional Court. *LG Meiningen 6 Qs 146/22*



'That a **fist with the thumb raised upwards signifies approval and endorsement** cannot, in any event, be seriously called into question. The symbolic content of this non-verbal communication - directed at praise, or at least at unqualified approval - would presumably be understood as such even by a recipient of pre-school age. In modern media it has, in any case, become an **outright emblem of advocacy**.'

Article 226 Romanian Criminal Code

(2¹) The disclosure, **dissemination**, presentation or **transmission**, by any means, of an intimate image of an identified person or of a person identifiable from the information provided, without the consent of the person depicted, where this is liable to cause that person psychological suffering or to damage their image, shall be punishable by imprisonment for a term of 6 months to 3 years or by a fine.

(2²) “Intimate image” means any reproduction, irrespective of the medium, of the image of a nude person who exposes, in whole or in part, their genital organs, anus or pubic area or, in the case of women, also their breasts, or who is involved in sexual intercourse or a sexual act.



George M R Zlati is 🕶️ feeling cool with Ulici Vlad and ...



January 25 · 🌐

#workinprogress @ Zlati, Ionescu, Chiperi - SCA

1 În martie... See more



[See insights](#)



257



8



4



Procedural criminal law: surveillance vs. open access



Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

- a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Agentic Artificial intelligence

- Using AI agents to track the activity of the suspect on a social network
- Scraping all data (posts, shares, likes, etc.) generated by the suspect and generating reports

The police use an AI agent to monitor, in real time, the suspect's publicly available activity on X, Telegram and Discord.

The AI agent issues alerts when content of interest appears, aggregates and correlates information, and produces weekly reports.

The agent runs 24/7 for seven months. Its output consists of 14,000 cumulative pages, plus real-time alerts sent to the investigator.

Question: does such an operation amount to **technical surveillance**?

Digital forensics: how to get the data and how to evaluate it

Social network investigations

- Manual investigation
- Investigation using open access or commercial tools
- Investigation using agentic AI and LLMs

Kali Linux + Sherlock OSINT tool

```
(kali㉿kali)-[~]
└─$ sherlock zlati
[*] Checking username zlati on:

[+] 9GAG: https://www.9gag.com/u/zlati
[+] Academia.edu: https://independent.academia.edu/zlati
[+] Anilist: https://anilist.co/user/zlati/
[+] Apple Discussions: https://discussions.apple.com/profile/zlati
[+] Audiojungle: https://audiojungle.net/user/zlati
[+] Behance: https://www.behance.net/zlati
[+] Blogger: https://zlati.blogspot.com
[+] BoardGameGeek: https://boardgamegeek.com/user/zlati
[+] BraveCommunity: https://community.brave.com/u/zlati/
[+] BuzzFeed: https://buzzfeed.com/zlati
[+] CGTrader: https://www.cgtrader.com/zlati
[+] Chess: https://www.chess.com/member/zlati
[+] Clubhouse: https://www.clubhouse.com/@zlati
[+] Codecademy: https://www.codecademy.com/profiles/zlati
[+] Cults3D: https://cults3d.com/en/users/zlati/creations
[+] DailyMotion: https://www.dailymotion.com/zlati
[+] Dealabs: https://www.dealabs.com/profile/zlati
[+] DeviantART: https://zlati.deviantart.com
```

Deep Web Data at Your Fingertips

www.gmail.com

Search

Advanced

 2021 - 2025 @TXT_ALIEN - #01 to #709 (11) [Part 106 of 1328].txt

PRO

2025-03-18 17:01:53

.google.com/signin/v2/challenge/pwd:ha[REDACTED]shka@kpnmail.nl:Foe[REDACTED]
https://accounts.google.com/signin/v2/challenge/pwd:ha[REDACTED]r36@gmail.com:Azer[REDACTED]
https://accounts.google.com/signin/v2/challenge/pwd:ha[REDACTED]r36@gmail.com:dkga[REDACTED]
https://accounts.google.com/signin/v2/challenge/pwd:ha[REDACTED]ta22@guru.sd.belajar.id:sdn011b[REDACTED]
https://accounts.google.com/signin/v2/challenge/pwd:ha[REDACTED]di0@gmail.com:jama[REDACTED]
https://accounts.google.com/signin/v2/challenge/pwd:ha[REDACTED]@gmail.com:hasnzd1[REDACTED]
https://accounts.google.com/signin/v2/challenge/pwd:ha[REDACTED]@outlook.com:hasan[REDACTED]

[View Full Content](#)



This tool allows you to check if an email address is used on several social networks or websites.

Query

[REDACTED]@gmail.com

Found

9

Websites

[academia.edu](#)

[adobe.com](#)

[evernote.com](#)

[github.com](#)

[instagram.com](#)

[myfitnesspal.com](#)

[myspace.com](#)

[pinterest.com](#)

[spotify.com](#)



EPIEOS



Using OSINT

- **Exploiting data breaches from the dark web**
- **Finding social media accounts:** attempt to access an information system?
- **Open access data vs scraping against T&C**
- **Public APIs vs private APIs**



Advanced Search on Twitter



These operators work on [Web](#), [Mobile](#), [Tweetdeck](#).

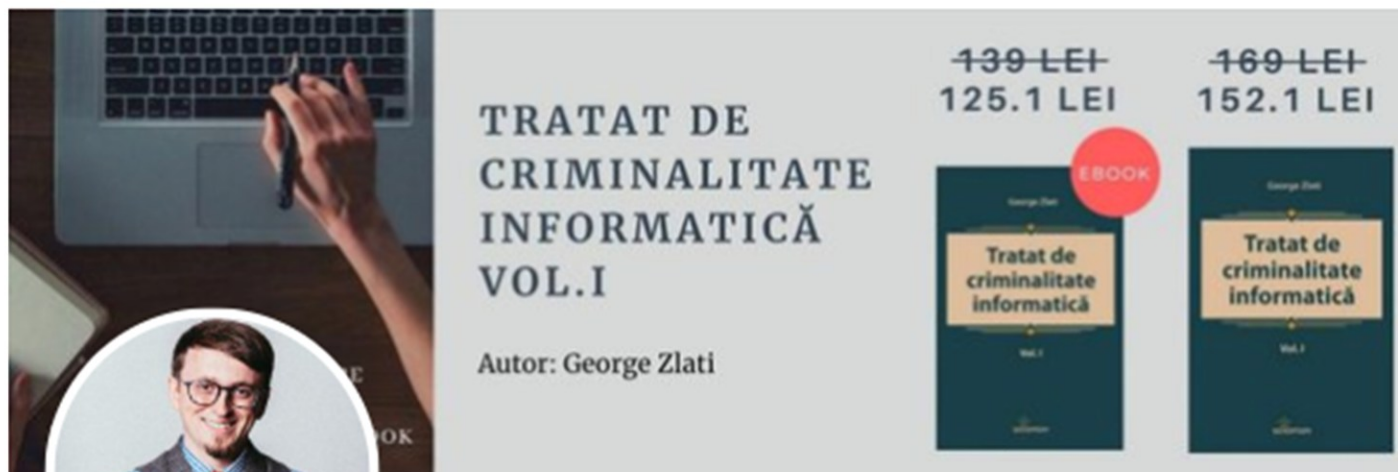
There is some overlap, but largely these will **not work** for [v1.1 Search](#), [Premium Search](#), or [v2 Search](#) APIs.

Adapted from [TweetDeck Help](#), @lucahammer [Guide](#), @eevee [Twitter Manual](#), @pushshift and Twitter / Tweetdeck itself. Contributions / tests, examples welcome!



Time	<code>since:2021-12-31</code>	On or after (inclusive) a specified date. 4 digit year, 2 digit month, 2 digit day separated by - a dash.
	<code>until:2021-12-31</code>	Before (NOT inclusive) a specified date. Combine with a "since" operator for dates between.
	<code>since:2021-12-31_23:59:59_UTC</code>	On or after (inclusive) a specified date and time in the specified timezone. 4 digit year, 2 digit month, 2 digit day separated by - dashes, an _ underscore separating the 24 hour clock format hours:minutes:seconds and timezone abbreviation.
	<code>until:2021-12-31_23:59:59_UTC</code>	Before (NOT inclusive) a specified date and time in the specified timezone. Combine with a "since" operator for dates between.

Users	<code>from:user</code>	Sent by a particular <code>@username</code> e.g. <code>"dogs from:NASA"</code>
	<code>to:user</code>	Replying to a particular <code>@username</code>
	<code>@user</code>	Mentioning a particular <code>@username</code> . Combine with <code>-from:username</code> to get only mentions



**TRATAT DE
CRIMINALITATE
INFORMATICĂ
VOL. I**

Autor: George Zlati

~~139 LEI~~
125.1 LEI

~~169 LEI~~
152.1 LEI

EBOOK

Tratat de
criminalitate
informatică
Vol. I

Tratat de
criminalitate
informatică
Vol. I



Edit profile

George M R Zlati

@GeorgeMRZlati

Criminal Defence Lawyer ⚖️ | Expert and Author on Cybercrime & Blockchain |
Authored Romania's First Treatise on Cybercrime 📖

📍 Romania 🔗 linktr.ee/zlati.george 📅 Joined April 2013

Settings

Q Search Settings

Your account >



Account information

Username
@GeorgeMRZlati



Change username

Username

GeorgeMRZlati

Suggestions

GeorgeR

MrZlati

mr_zlati

GeorgeZlati

george_zlati

Save

TweeterID

X/Twitter ID and Username Converter

Type in any X/Twitter ID or @handle below,
and it will be converted into the respective ID
or username on the right:

Convert

Recent ID Conversions:
@elonmusk => 44196397

A screenshot of a web application titled 'TweeterID' with the subtitle 'X/Twitter ID and Username Converter'. The interface has a dark grey background. On the left, there is a text input field containing '@elonmusk' and a blue 'Convert' button below it. On the right, a box displays 'Recent ID Conversions:' followed by '@elonmusk => 44196397'. Two large red arrows are overlaid on the image: one points from the top right towards the conversion result box, and the other points from the right towards the input field.



What about a screen recording?

39.8K posts



Elon Musk

@elonmusk

Joined June 2009

554 Following 176.1M Followers 145 Subscriptions

Followed by xAI, VirtualBacon, and 140 others you follow

Posts

Replies

Subs

Highlights

Media

Likes

 Pinned

 **Elon Musk** @elonmusk · 1h

This law is not just about TikTok, it is about censorship and government control!

If it were just about TikTok, it would only cite "foreign control" as the issue, but it does not.

 **Thomas Massie** @RepThomasMassie · 2h

The so-called TikTok ban is a trojan horse.

The President will be given the power to ban WEB SITES, not just Apps.

The person breaking the new law is deemed to be the U.S. (or offshore...

Show more

 **Elon Musk** @elonmusk

Analyze Metrics

[How these metrics are calculated](#)

You might like

 **Google** @Google

Follow

 **NASA** @NASA

Follow

 **MrBeast** @MrBeast

Follow

[Show more](#)

Romania trends

1 · Trending

Tate

84.6K posts

2 · Entertainment · Trending

#Oscars2024

191K posts

3 · Technology · Trending

Samsung

46.4K posts

ERA

Forensic capture

- Hunchly / WebPreserver (browser extension)
- Page Vault / Pagefreezer (cloud)
- Social Discovery (enterprise)
- FAW (Forensic Acquisition of Websites)



Michael Saylor ⚡️🔒 @saylor · 4h

#Bitcoin ₿ is the Future.



⚡️ 21 JCLP ⚡️ 13% 🚫

💬 602

↻ 1.1K

❤️ 7.6K

📊 168K



@saylor · 4h



Michael Saylor ⚡🔵 @saylor · 4h

#Bitcoin ₿ is the Future.



⚡ 21 JCLP ⚡ 13% 🚀

💬 602

↻ 1.1K

❤️ 7.6K

📊 168K

🔖 ⬆

```
<time datetime="2024-03-12T12:44:16.000Z">4h</time> == $0
```


EXIF stripping behaviour at upload

Platform / route	Strip?	Notes
Facebook (photos)	YES	Aggressive strip; in place since pre-2016
Instagram	YES	Strip from native re-encode pipeline (pre-2019); originals retained server-side, not public
X (Twitter) — public posts	YES	GPS + most EXIF stripped; ?name=orig restores full resolution only, NOT EXIF
X — DMs / 3rd-party API uploads	partial	DMs sent at 'original quality' may retain GPS
TikTok	YES	Strip; MP4 container-level signatures may persist on video
LinkedIn	YES	Server-side re-encode strips
WhatsApp / Signal	YES	Compression + strip; both E2EE (WhatsApp since 5 Apr 2016)
Snapchat	YES	Strip + ephemeral by default; preservation only via LE portal
Reddit native (i.redd.it)	YES	Strip since native hosting launch (June 2016)
Discord	mixed	JPEG: stripped. PNG, video, XMP/IPTC frequently survive — not just a 'size threshold'
Reddit external link	no	Preserves whatever the 3rd-party host preserves
Telegram 'send as file'	no	Full EXIF retained; 'send as photo' compresses + strips
Email attachment (Gmail, Outlook)	no	Full EXIF preserved — underused OSINT route
Cloud share (Drive, Dropbox, iCloud)	no	Original file with intact EXIF
Flickr	no	EXIF deliberately preserved (privacy override available per setting)

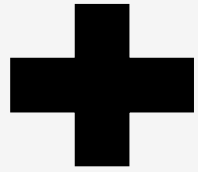
Law-enforcement channels per platform

Platform	Portal	Preservation	Notable
Meta (FB / IG / WA)	facebook.com/records (LERS)	90 days	Messenger E2EE default Dec 2023; WhatsApp metadata server-side
X	legalrequests.x.com	90 days	Cooperation degraded post-Musk; €120M DSA fine 5 Dec 2025 (€45M Art. 25 + €40M Art. 40(12) + €35M Art. 39)
TikTok	tiktok.com/legal/report/lawenforcem entrequest (EEA → TikTok Technology Limited, Dublin)	Yes	Project Clover Ireland operational Sept 2023, Norway live; Irish DPC €530M, 2 May 2025 (EEA-to-China transfers)
Google / YouTube	lers.google.com	Yes	SLA 30-60 days non-emergency; LERS unified for all Google products
Telegram	lawenforcement@telegram.org	Yes	Durov inflexion 24 Aug 2024; Q1 2025 = 22,777 disclosures vs Q1 2024 = 5,826 (3.9× YoY)
Discord	discord.com/safety/360044157931 lawenforcement@discord.com	Yes	Voice not recorded; DMs require warrant; limited audit-log window
Snapchat	lawenforcement.snapchat.com	CRITICAL	Default retention hours-to-days; preservation request must be IMMEDIATE My Eyes Only encrypted client-side, undecryptable
LinkedIn (Microsoft)	microsoft.com/.../law-enforcement-requests	Yes	Predictable cooperator; days for preservation, weeks for content
Reddit	lawenforcement@reddit.com	Yes	H2 2024: ≈ 1,000+ legal requests globally; user-notification on subset



Case study

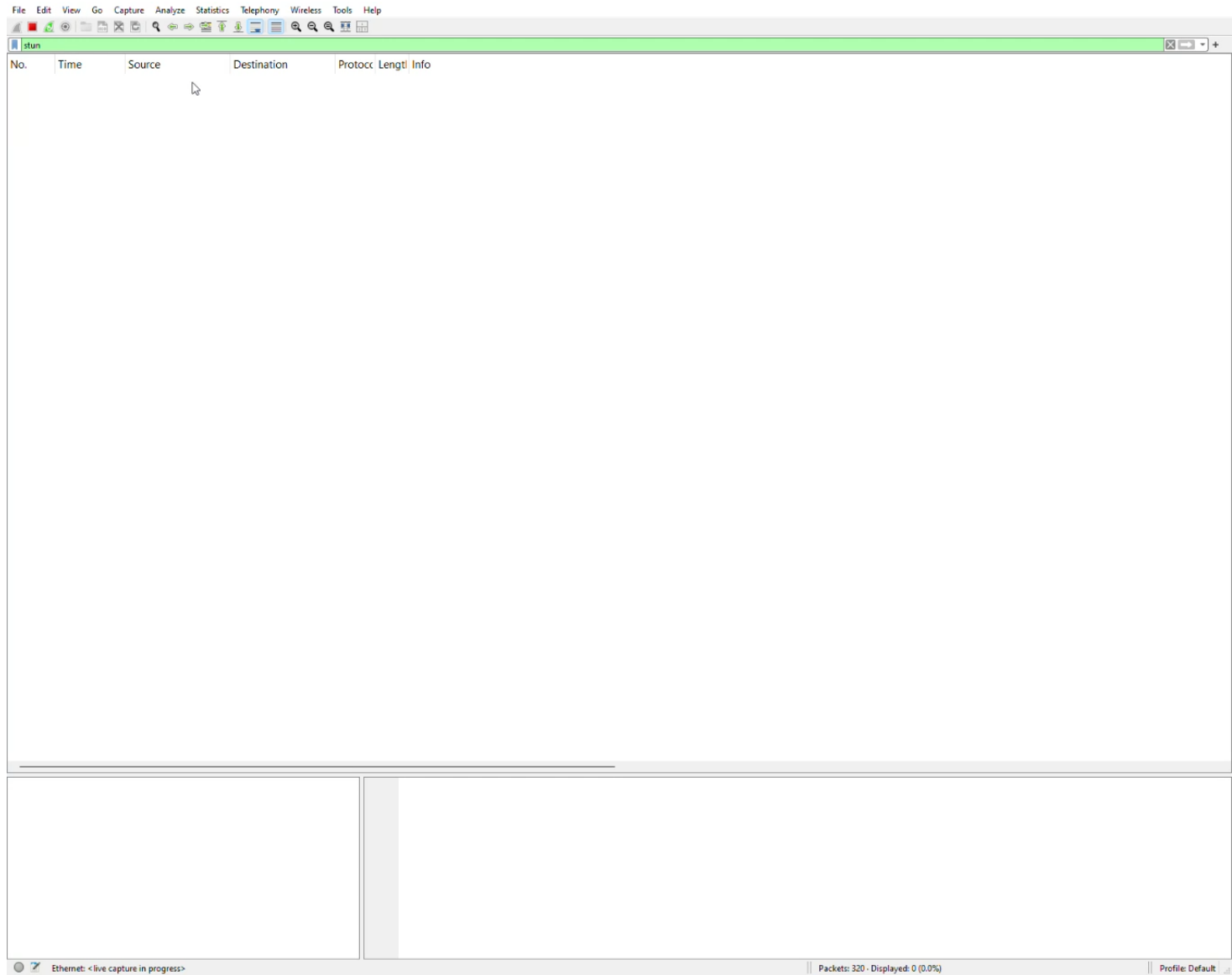
(#1) Discord & VPNs



Case study

(#2) Social networks & P2P

- **A P2P connection creates a direct link between devices**
 - only the content data is being encrypted E2E
- **The target's IP address can be revealed when the devices are being connected**
 - this constitutes data interception
 - you must be on the same network with the device that interacts with the device of the perpetrator



Case study

(#3) From email to

an***1337@gmail.com
d***07@gmail.com și
bo****ss@gmail.com

- Full name of the perpetrator
- Full name of the perpetrator's parents
- Full name of the perpetrator's sister
- Phone number of the perpetrator
- Accounts associated to the perpetrator
- Date and place of birth
- Address of residence

Only for live participants

“NOT ANOTHER BRICK in the law





Cross-border access to data and admissibility of evidence

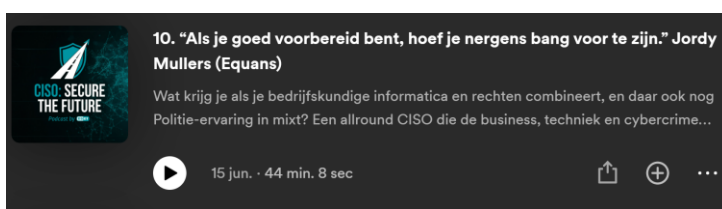
#DIGITALISATION AND #AI IN CRIMINAL JUSTICE

Online investigations and internet searches in times of AI

Tallinn, 7-8 May 2026



Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible for them.



Introduction

Studies:

- Computer Science
- Law School

Professional experience:

- Legal assistant, Lawyer at the Dutch Judiciary
- Legal advisor, Policy Officer cybercrime and digital investigations at the Dutch Police

Current Position, Additional Positions:

- CISO EQUANS Netherlands, Switzerland & ANZ
- Judge at the criminal court of Zeeland West-Brabant & Limburg
- Police volunteer Legal advisor cybercrime and digital investigations



Geografische
spreiding



BOUYGUES GROUP'S



€1,125

MILLION

Net profit attributable to the Group in 2021

81

COUNTRIES

where Bouygues operates

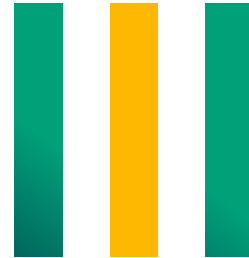
6

SUBSIDIARIES

Bouygues construction, Bouygues Immobilier,
Colas, Equans, TF1, Bouygues Télécom



Life of a CISO



<https://www.youtube.com/watch?v=1RQ2sU5OGUg>



Introduction

Today, I will be discussing a Dutch criminal case with you, highlighting various investigative powers of the police. Additionally, we will explore the topics of cross-border access to data and the admissibility of evidence.

Investigation Phases

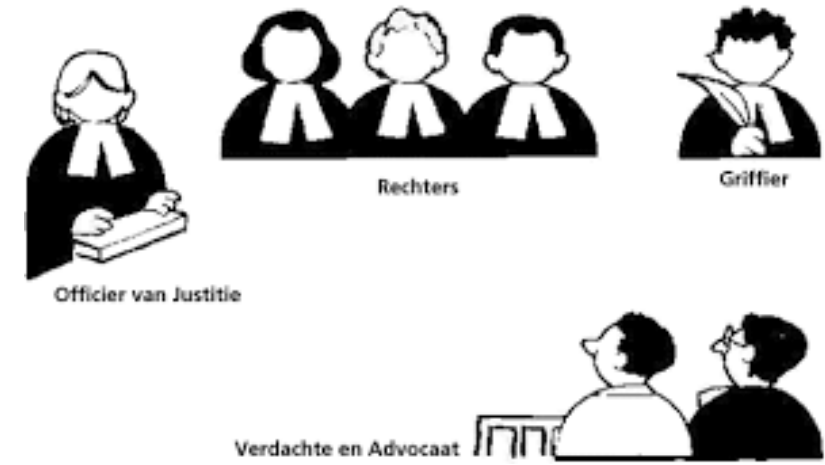
Phase 1: Investigation of a marketplace on the dark web conducted following a legal assistance request

Phase 2: Home search and laptop examination conducted at the suspect's residence. Seizure of two smartphones Occurred when the suspect was apprehended on a public road

Phase 3: Forensic examination of devices and the data on them



The Court











"the indictment" or "the charge."

1. The acquisition of Bots, which are technical tools used to commit criminal offenses such as hacking.
2. Having login credentials in his possession that he knew or should have suspected were stolen.
3. That he hacked a system by logging into internet banking, by using login credentials that were unlawfully obtained.
4. That he had phishing kits on his computer, which are technical tools used to commit criminal offenses such as hacking.



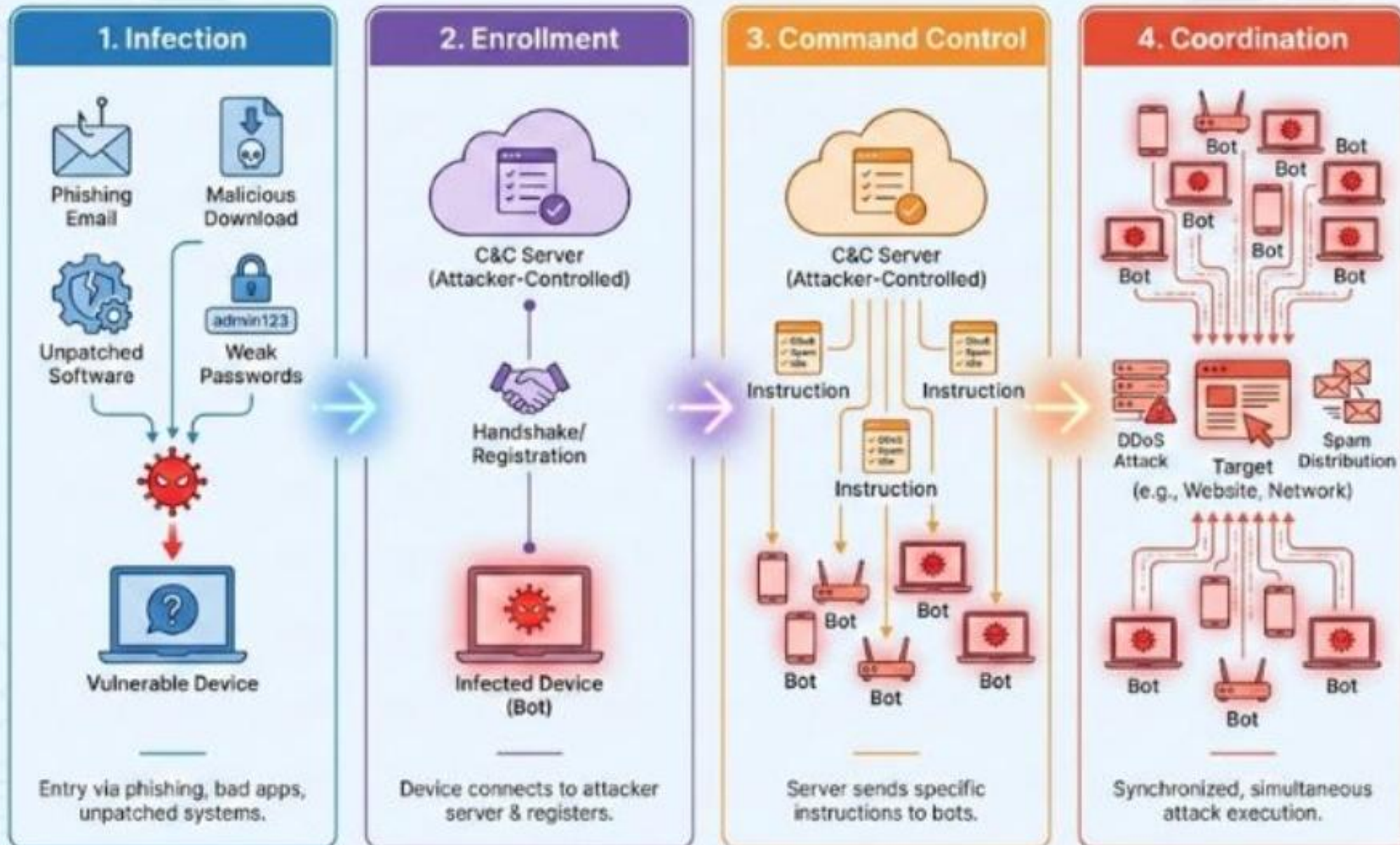


FBI

Start of the investigation.

The investigation started with a request from the FBI to examine a server in the Netherlands as part of a mutual legal assistance request, which contained information about a marketplace for buying bots.

How Botnets Work: A 4-Step Lifecycle





Phase 1

High Tech Crime Team Confirms FBI Intel: Dark Web Marketplace for Bots Uncovered

Investigation by High Tech Crime Team Netherlands

- Conducted thorough analysis of server/webshop on the internet
- Confirmed the accuracy of FBI intelligence findings
- Active marketplace discovered
- Bots available for purchase via the dark web



Phase 1

Spin-Off Investigation from FBI Legal Assistance Request

- Information obtained through FBI's legal assistance request
- Discovery of numerous individuals from the Netherlands purchasing bots

Operation Details

- Marketplace to be taken over for a few days
- Objective: Intercept live data

Outcome

- Identification of a buyer located in the Netherlands

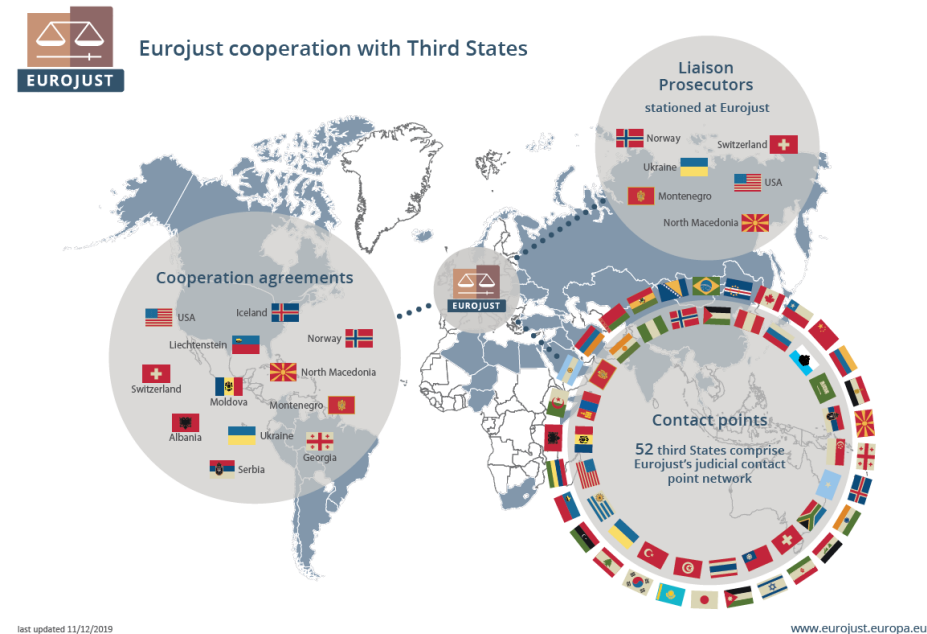
Mutual Legal Assistance

European Convention on Mutual Assistance in Criminal Matters (ETS No. 30)

- Under this Convention, Parties agree to afford each other the widest measure of mutual assistance with a view to gathering evidence, hearing witnesses, experts and prosecuted persons etc.
- National procedures on judicial co-operation in the criminal field.
- Practitioners are urged to consult the lists of signatures and ratifications as well as the declarations and reservations of any convention.
- Treaties create binding obligations on states parties, but actual execution of a request for international cooperation also requires analysis and consideration of the domestic laws of the requesting and requested states

General Principles International Cooperation in Criminal Matters

- Widest Cooperation Possible
- Dual Criminality
- Specialty Principle
- Proportionality



Exceptions

- Article 26 – Spontaneous information
 - within the limits of its domestic law and without prior request,
 - forward information obtained within the framework of its own investigations
 - when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning (cyber)criminal offences or might lead to a request for (cyber)co-operation.
- Article 32 – Trans-border access to stored computer data with consent or where publicly available
 - without the authorization of another Party:
 - a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
 - b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

International Cooperation: Dutch Police and FBI Collaboration Methods

- Mutual Legal Assistance Treaties (MLATs): Facilitate information exchange for criminal investigations.
- Joint Task Forces: Collaborative teams tackling organized crime and cybercrime.(Europol and INTERPOL: Support cross-border investigations and operations.)
- Direct Bilateral Cooperation: Direct collaboration sharing expertise and resources.



Phase 1

Investigation Uncovers Bot Purchaser in the Netherlands

- User with a specific username purchased bots
- Phone number of the user was unregistered
- Bitcoin payments examined
- Wallet provided an address in the Netherlands
- Technical tool installed by the police on the marketplace identified a frequently used IP address
- Telecom provider request revealed an address
- Address linked to a young man in police records
- Prior conviction for fraud

Framework of Investigative Powers of the Dutch Police

General Investigation Power: Police officers can independently exercise certain powers, such as making arrests, conduct searches, seizure of items and gather evidence .

Authorized Powers: More extensive powers, like phone tapping, surveillance, forensic research and (home) searches, require authorization from a public prosecutor or an examining judge





Phase 2

Early Morning Raid Leads to Seizure of Electronics for Forensic Analysis

Early Morning Raid

- Conducted at the suspect's address
- Presence of the examining magistrate during the search

Seized Items

- Laptop (was on but could not be accessed)
- Phone (locked and could not be accessed)

Suspect's Absence

- Suspect was not at home during the search

Forensic Examination

- All items seized and taken for forensic analysis



Phase 2

Suspect Apprehension and Forensic Examination of Seized Smartphone

- Location Tracking: The suspect was located via his phone.
- Arrest and Seizure: Officers arrested the suspect and seized his phone.
- Phone Access: The phone was unlocked by holding it in front of the suspect's face.
- Evidence Found: A Telegram account was discovered on the phone, containing information about login credentials being shared.

Smartphone Seizure and Investigation in the Netherlands

Police Officer

- Limited intrusion into personal privacy.
- General authority of investigative officers is sufficient.
- Applies to consulting a small number of specific data.

Public Prosecutor

- Extensive investigation providing a nearly complete picture of personal life may be unlawful.
- Applies when all data on the device is examined using technical tools.

Investigation Judge

- Foreseeable severe breach of someone's privacy.



Impact of the Landeck Ruling on Smartphone Investigation in the Netherlands

Conclusion:

- The EU Court of Justice's Landeck ruling ([CURIA - List of results](#)).
- Relates to the Dutch Supreme Court's framework in the Smartphone-arrests (e.g., ECLI:NL:HR:2017:584) (8 maart 2025, ECLI:NL:HR:2025:409).

Key Question:

- Whether more cases require investigating judge approval for police investigations of data on seized mobile phones.
- This requirement may be more extensive than previously assumed by the Supreme Court.

Innovation Law in the Netherlands

- Collecting, saving and take notice of data stored on a device after seizure, 556 Sv;
- Investigating data that is stored elsewhere at the time of or after the seizure of a device (network search), 557 Sv
- The forced biometric unlocking of a seized device, 558 Sv.

Collecting and investigation of data stored on a device after seizure, 556 Sv;

- In case of a red-handed felony or a felony that allows pre-trial custody;
- The public prosecutor can order;
- After authorization of the investigation Judge;
- That a police officer can investigate data that is received after seizure;
- If it is needed for the investigation.
- Period 3 days, 3 months or 6 months (severity of the crime and necessary for the investigation)

Synchronization?
Existing
connection?

Investigating data that is stored elsewhere at the time of or after the seizure of a device (network search), 557 Sv

- In case of a red-handed felony or a felony that allows pre-trial custody;
- The public prosecutor can order;
- After authorization of the investigation Judge;
- That a police officer can investigate data that is stored elsewhere during seizure;
- If it is needed for revealing the truth.
- Period 3 days, 3 months or 6 months (severity of the crime and necessary for the investigation)

Territoriality?
Existing
connection?



Phase 3

Rapid Investigation Uncovers Cybercrime Evidence

- Phone Examination: Suspect's phone was quickly examined.
- Password Manager: LastPass password manager found on the phone.
- Laptop Access: Laptop unlocked using credentials from the password manager.
- MFA Confirmation: Suspect compelled to use fingerprint for Multi-Factor Authentication (MFA).

Evidence on Laptop:

- Hacking tools like phishing kits discovered.
- Purchased bots and conversations with victims found.
- Evidence of bank account logins and money transfers.
- Access to various accounts provided additional evidence. (bitcoin wallets)

The Police Officers Hacking in Criminal Investigations

- Effective Date: March 1, 2019 Computer Crime Act III (Wet CCIII)
- Hacking Authority: Allows law enforcement officers to covertly access a suspect's automated system under certain conditions for investigating serious crimes
- Permitted Actions After Access:
 - Identify and record characteristics of the system or user (e.g., identity, location)
 - Execute orders to intercept and record confidential communications
 - Conduct systematic observation
 - Record data stored in the system
 - Make data inaccessible
- Specialized Team: Actions can only be performed by specially designated officers from the National Police's specialized unit.
- Authorization: Can only be executed upon the request of the public prosecutor, with approval from the judge and a positive recommendation from an independent supervisory body

Thanks!

Questions?



Contact:

<https://www.linkedin.com/in/jordy-mullers-5583b829/>
J.mullers@rechtspraak.nl



Digital evidence in criminal procedure

From open source to dark web

ENELI LAURITS

2026, TALLINN



Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not
necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible
for them.



Setting the stage

1. How to collect digital evidence *according to law*?
2. Extending the search within your country;
3. Publicly available data;
4. Remote search with consent;
5. Remote investigative operations without consent.



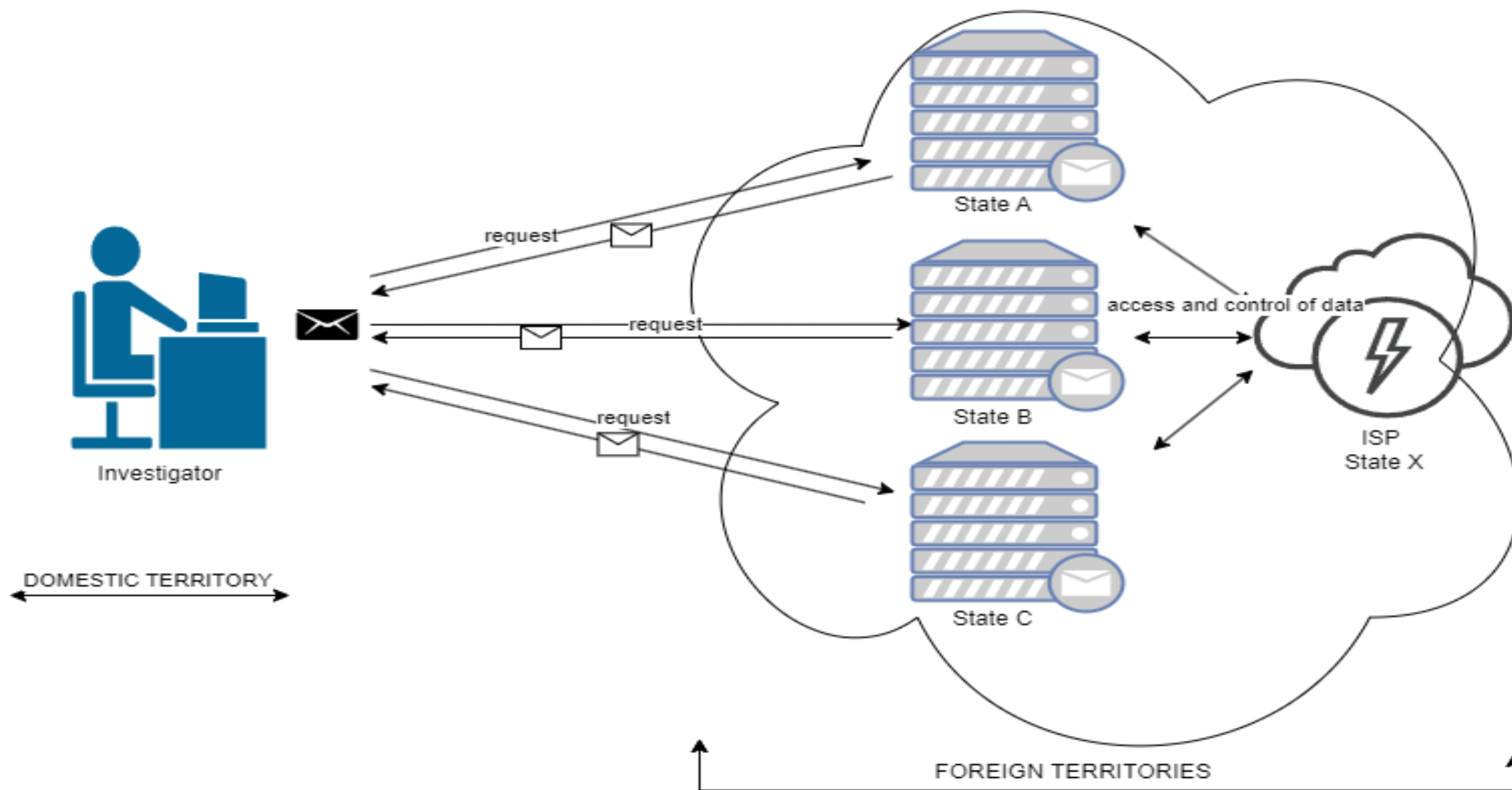
Digital evidence is considered legitimate and lawful when:

- It has been gathered without violating fundamental rights.
- It has been obtained and processed according to the procedure established by law.
- It must be obtained in compliance with best practices to be admissible in court.



Convention on Cybercrime Article 19 – Search or similarly access a computer system or part of it, and computer data stored therein.

Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, and have grounds to believe that the data sought is stored in another computer system or part of it **in its territory**, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.





Enforcement jurisdiction — the power to carry out coercive investigative acts — is presumed to be confined to the State's own territory unless a permissive rule of international law or the consent of another State provides otherwise.

States are in principle not allowed to carry out law-enforcement operations, including criminal investigations, on foreign States' territory.



Article 32 –Trans-border access to stored computer data with consent or where publicly available. A Party may, without the authorization of another Party:

a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.



Publicly available data?



To date there is no globally valid legal definition of public availability - it is often falsely used synonymous with 'not protected in any way'.

- The core of the understanding appears to be that data is publicly available if access to it is not limited to a specified group of persons.
- The key question under EU legislation is if data are related to natural persons and hence fall under the scope of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.
- The mere public availability of data is no feature that can completely disable the protection of a natural person through Articles 7 and 8 EU-CFR.



The US perspective to publicly available data: the reasonable expectation of privacy

In contrast to Article 7 EU-CFR the protection is not automatically granted if data is 'related to a natural person' but rather depends on the reasonable expectation of privacy of the affected person.

It is regularly determined by real considerations whether that expectation exists.



Social media – publicly available?

A sub-section of the surface web is social media (eg Instagram, Snapchat, Facebook, Tinder). Social connections have always been an important investigative approach, with the shift from real-life to electronic communication these connections are often easily accessible and generate valuable insights for law enforcement.

Some of the currently existing networks allow users to limit the reach of their content to certain user groups (everyone, network participants, friends, friends of friends).

The public availability for such restricted data hence often depends on factual barriers that these settings eventually raise.*

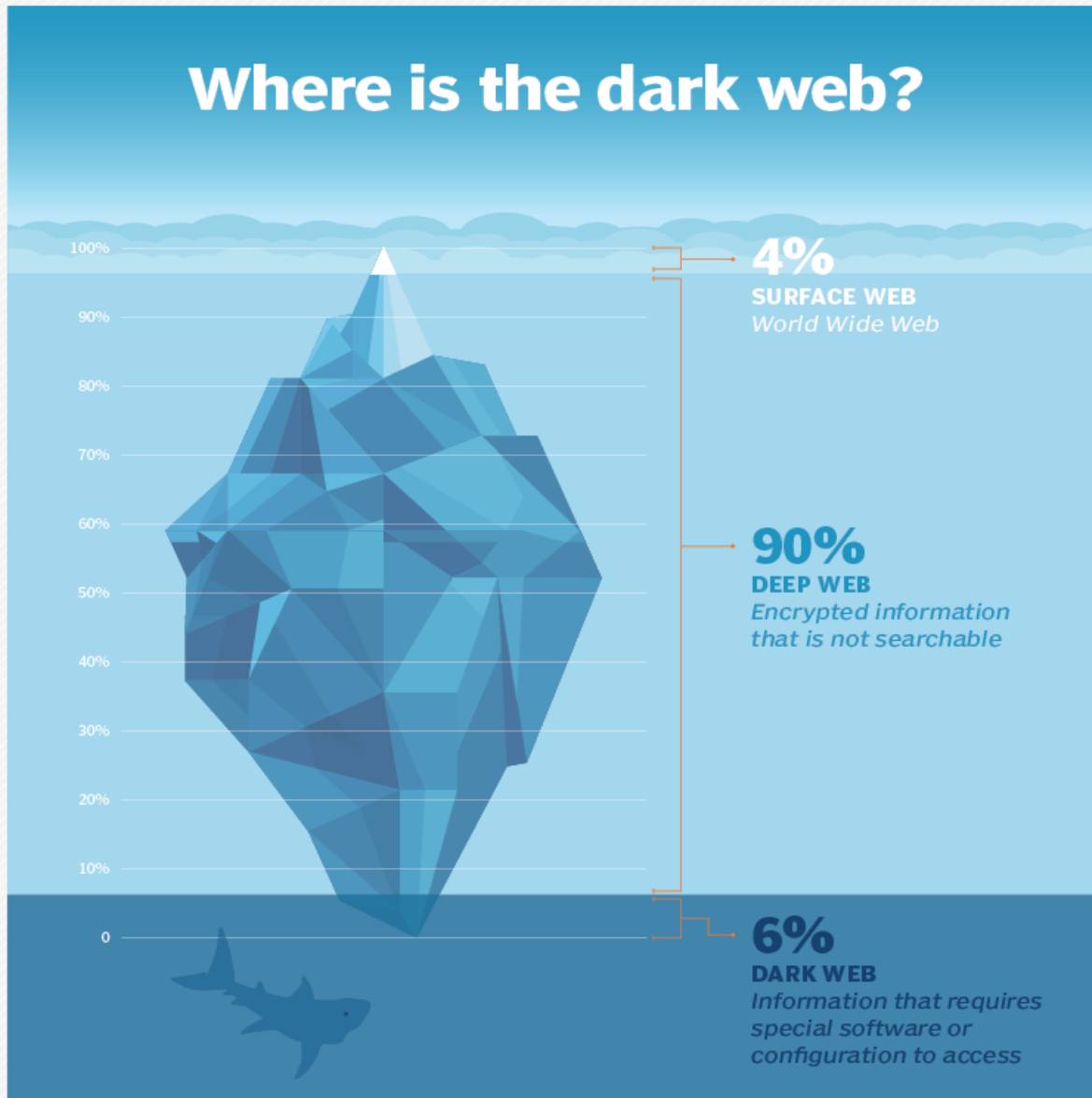
Thilo Gottschalk. „The Data-Laundromat? Public-Private-Partnerships and Publicly Available Data in the Area of Law Enforcement.“



- Data on social networks are easily relatable to natural persons and often give insights in particularly sensitive areas of a persons' life such as religious or political beliefs or sexual preferences.
- Accessing social media data hence bears severe risks to the fundamental rights of the data subject.
- **While data on social media may be manifestly made public, this cannot be re-interpreted as consent or abandoning fundamental rights protection.**



Where is the dark web?



If it's not restricted with a password, is it then publicly available?



- The terms "dark web" and "deep web" are often used interchangeably, but they are not the same. Rather, the dark web is a small, less accessible part of the deep web.
- Both the dark and deep web share one thing in common: neither can be found in search engine results. The difference between them primarily lies in how their content is accessed. Deep web pages can be accessed by anyone with a standard web browser who knows the URL.
- Dark web pages, in contrast, require special software with the correct decryption key, as well as access rights and knowledge of where to find the content.



The Deep web. US v Auernheimer*

- The defendant was convicted of unauthorised access for collecting information from a website of a US telecommunication provider, which was accessible on a hard-to-guess website that was not intended to be accessed.
- Although the data was publicly accessible, the court stated that the data was still protected, analogous to a home where 'the front door is left open or unlocked'.
- The defence argued that the information was made available to everyone and the general public was authorised to view the data.
- Courts increasingly assume that data publication does not necessarily preclude an expectation of privacy.

*Supreme Court of the United States, United States v Andrew Auernheimer (2014) <<https://cite.case.law/f3d/748/525/>>



Access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 32 –Trans-border access to stored computer data with consent or where publicly available.

How about without consent?



Dark web investigations – whose territory is it?

- The term “network investigative technique” [NIT] is a euphemism for law enforcement hacking;
- It describes a law enforcement surveillance method that entails remotely accessing and installing malware on a computer without the permission of its owner or operator.
- Network investigative techniques are especially useful in the pursuit of criminal suspects who use anonymizing software to obscure their location.
- NITs have lead to many cases which have eventually ended up in international cooperation. As Kerr and Murphy* put it: „To date, not only has the most usual response [to discovering a foreign law enforcement agency engaged in the unauthorised access of data stored within its jurisdiction] been one of acquiescence, but, indeed, of providing even more cooperation.“

*Orin S. Kerr & Sean D. Murphy. Essay. **Government Hacking to Light the Dark Web. *Risks to International Relations and International Law?* - *Stanford Law Review*, vol 70, July 2017.**



Could it be lawful to unilaterally access and copy data without consent?

- Discourse and practice increasingly de-emphasize the territoriality of data—its actual location on a server or a device—as a relevant consideration for the valid exercise of enforcement jurisdiction.
- Given the volatile nature of digital data and considering the customary international law of enforcement jurisdiction in cyberspace, there maybe should be rules that allow States' extraterritorial (unilateral) enforcement actions for investigative purposes.



One example: The Norwegian Supreme Court's decision in the Tidal case*

- The Norwegian Supreme Court did not consider it relevant that the data were located outside Norway, instead basing lawfulness of the enforcement action.
- According to the Court, “the search will [not] affect another state to an extent that it constitutes a violation of the principle of sovereignty.”

*Tidal Music AS v. The Public Prosecution Authority, HR-2019-610-A



Concluding thoughts – back to the beginning

It doesn't much matter whether it is the surface web, deep web or dark web as evidence in criminal procedure is considered legitimate and lawful when:

- It has been gathered without violating fundamental rights
- It has been obtained and processed according to the procedure established by law
- It must be obtained in compliance with best practices to be admissible in court



THANK YOU!

Legal issues/challenges related to the collection of e-evidence in criminal investigations

The EU's E-evidence Package as a Trojan Horse

Jaanus Tehver, defence lawyer

ERA's seminar "#Digitalisation and #AI in Criminal Justice", 7-8 May 2026, Tallinn

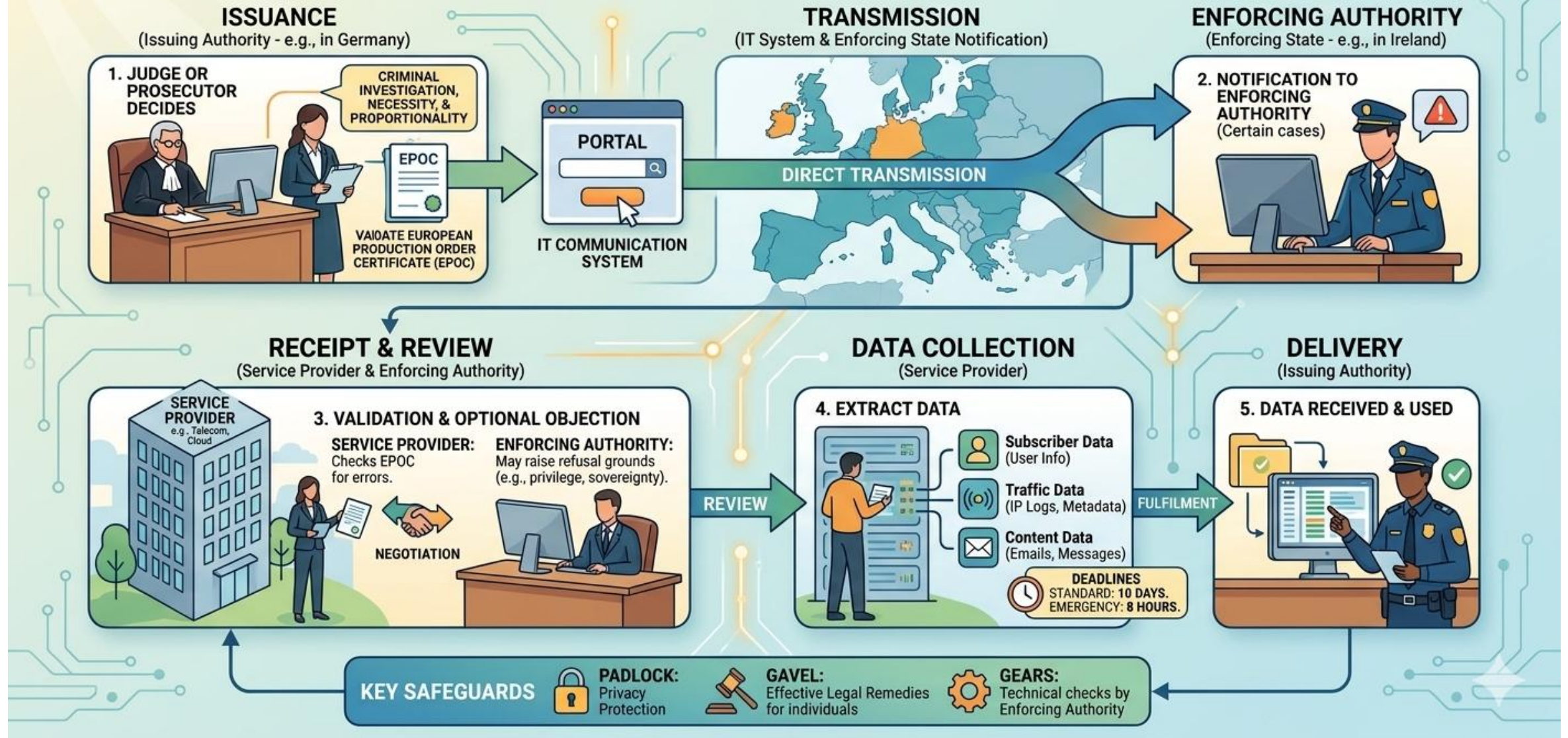


Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

The E-evidence package: basic facts

- E-evidence package = Regulation (EU) 2023/1543 + Directive (EU) 2023/1544
- Directive transposition deadline February 18, 2026
- Regulation directly applicable from August 18, 2026
- Applies to data held by "Service Providers" (not extracted from individual devices)
- Covers 4 categories of data:
 - *Who are you?* (**Subscriber data**: Name, address, billing).
 - *How did you log in?* (**Access data**: IP addresses, timestamps).
 - *Who did you talk to?* (**Traffic data**: Metadata like duration and recipients).
 - *What did you say?* (**Content data**: The actual text of emails, photos, or voice recordings).

E-EVIDENCE PRODUCTION ORDER (REGULATION 2023/1543) PROCESS



A Digression: National Implementation in EE

- No national implementation legislation as of today
- The Ministry of Justice and Digital Affairs published a legislative proposal on **May 4, 2026**
- Stakeholders were invited to express their opinions by **May 6, 2026**
- Official response to ISP's inquiry about the state of readiness of the "decentralized IT system" required by the Regulation (April 2026):

"At this time, the Ministry of Justice and Digital Affairs does not have any additional information to provide regarding the IT system, as the European Commission is still working on its development and the detailed workflows and responsibilities have not yet been finalized. As soon as we receive further and more specific information, we will certainly keep you informed about the next steps and developments on both the European Union and Estonian sides."

Mutual Recognition transformed

- "A new dimension" to mutual recognition: expanding the principle from cooperation between state authorities to private actors (Service Providers)
- What is "mutual" in a situation where Service Providers are only expected to receive and fulfil orders?
- Where is "recognition" when the orders are not subject to be recognised by any judicial authority before actual fulfilment?

Lack of safeguards

- Traditional two levels of protection:
 - the issuing authority assessed legality and proportionality,
 - the executing authority assessed compliance with fundamental rights.
- E-evidence Regulation effectively cancels the second level
- Service Providers are supposed to be guardians of fundamental rights, but there are very limited tools for them in order to fulfil this role, and even less incentives to do so
- Are all Service Providers equally equipped to perform their role as guardians?

Notification requirement : a fig leaf

- Regulation requires that orders for traffic and content data must be notified to a competent authority in the Member State where the Service Provider is established or represented
- That authority has 10 days (4 days in emergency cases) to raise a ground of refusal
- **Is it reasonable to expect that notified authorities choose to intervene, especially when the persons concerned are not usually residing in that Member State?**

Lack of information

- There is general requirement to inform the person whose data are being requested about the production of data on the basis of a EPOC "without undue delay"
- However, the issuing authority may **delay or restrict informing, or omit to inform**, the person whose data are being requested, to the extent that, and for as long as, the conditions in Article 13(3) of Directive (EU) 2016/680 are met
- **This effectively means that in most cases the persons will only be informed after a criminal investigation has been completed (i.e. months and even years after the data was obtained)**

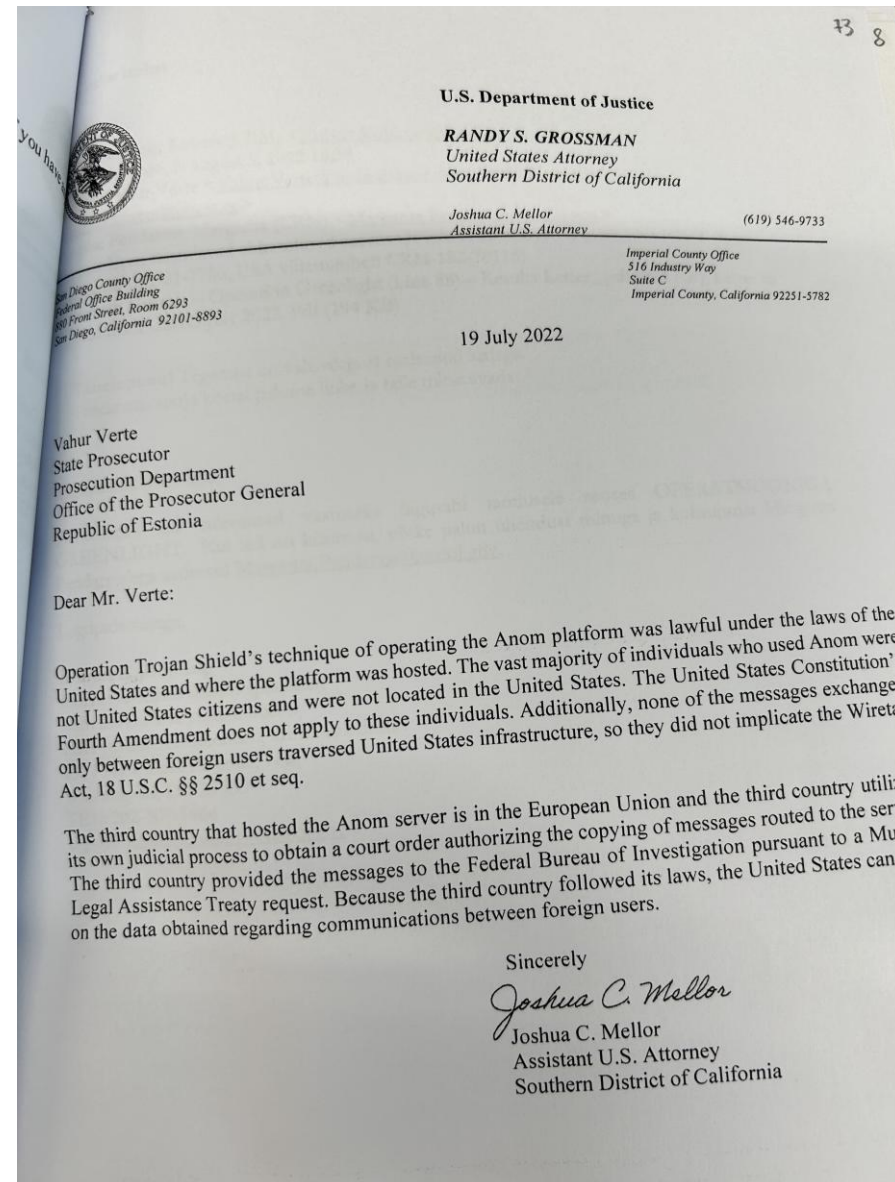
No Effective Remedies

- Extremely limited grounds for refusal
- No possibility to challenge the order and/or seizure of data in the Member State where the order is being fulfilled
- Those concerned can only seek remedies in the Member State where the order was issued
- Without timely notification, a defendant cannot challenge the legality of the seizure (e.g., arguing that the data is privileged or that the warrant was too broad) until after the data has already been integrated into a prosecution file
- No harmonized rules on admissibility of evidence

E-evidence package: a Trojan Horse?

- A structural revolution for EU criminal law
- A strive for efficiency has disabled important fundamental rights safeguards
- Lack of judicial assessment creates risks of abuse
- Citizens are left vulnerable to overbroad and abusive orders
- A blueprint for future measures, not only in criminal law but in other areas?

Discussion #1: Operation "Trojan Shield"



Discussion #2: Access to content data in EE



Decoding the Future

Advanced Analytics and Applications in Crypto

Federico Paesano



Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible for them.



ABOUT ME

Federico Paesano

Senior Investigations Specialist

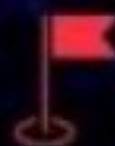
- 1996-2010 Italian Financial Police
- 2009-2010 EUPOL Afghanistan
- 2010-2024 Trainer @ Basel Institute on Governance
- 2024-Now Financial Investigator @ Crystal Intelligence





10th Global Conference on Criminal Finances and Cryptoassets

15+16
SEPTEMBER
2026



EUROPEAN CONVENTION CENTER LUXEMBOURG

How Crystal turns blockchain complexity into clarity



Collate

Multi-blockchain
data collection



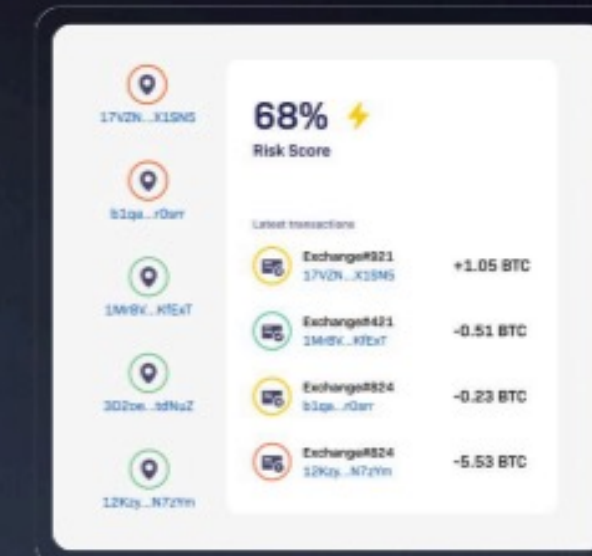
Cluster

Group wallets by
spending patterns and
heuristics



Attribute

Connect clusters to
real-world entities



Score

Apply risk scoring
based on AML/KYC
policies

BUILD PATHS IN SECONDS

One-click path discovery

Automated path building

Between any two entities in seconds

Shortest path or all paths

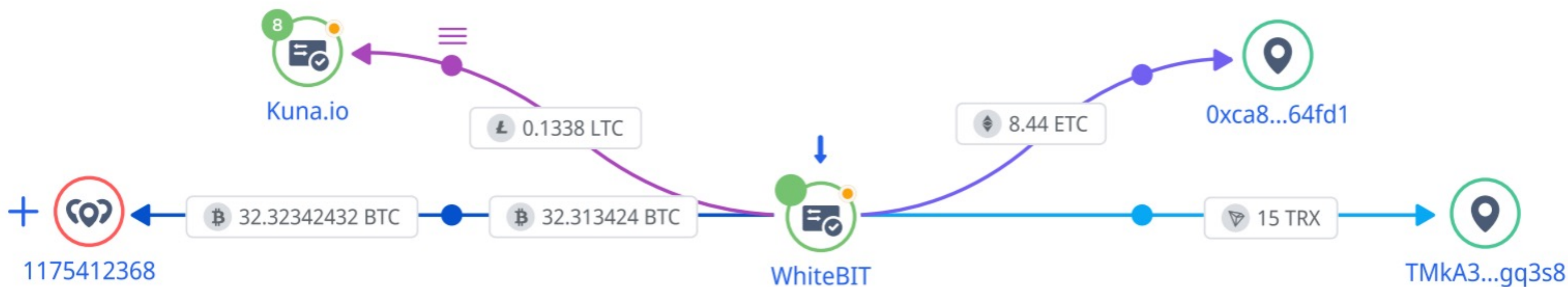
Choose your investigative depth

By owner or by address

Toggles view instantly

Drag and drop customization

For detailed evidence building



Criminal Trends

What criminals will do





Instant Swaps and Cross-chain Bridges



Explorers - THORChain

0xe3de024208aa5d259a9f1dfaeb5710726a90c34f0f545885d36413318...



Swap



20.46365643 ETH.ETH
\$57,439.40



0.59418450 BTC.BTC
\$58,611.52



Inbound ▾

✓ Success

Swap ▾

✓ Success

Outbound ▲

✓ Success

Destination

15CBig...R4wbwF ↑ | [🔗](#)

Hash

B18754...3A1472 ↑ | [🔗](#)

Outbound Stage

Done

Signed

Outbound Fee

0.00002963 BTC.BTC (\$2.47)

Explorers - **Bridgers**



BRIDGERS

Explorer

Status:

✓ Success

Date:

🕒 3 minutes ago (Apr 02, 2025, 11:07:40 AM GMT+2)

From Chain:

ETH

To Chain:

TRX

Deposit Hash:

[0xffe898318fbbf7f414d9b49f13b044d9f1f9e3336a5d766df8bd09e840ab61ad](#) 📋

Destination Hash:

[fc764a387e2319371767ae5dca49e9711f37ae8d3e16728bc87be87efdbad802](#) 📋

From:

[0x843462bc92f4ae1ec8c846f1d9ac4873983dee6a](#) 📋

To:

[TJsbQLHjCYWEtq1gUC8HvJgTQVuWRTbHr2](#) 📋

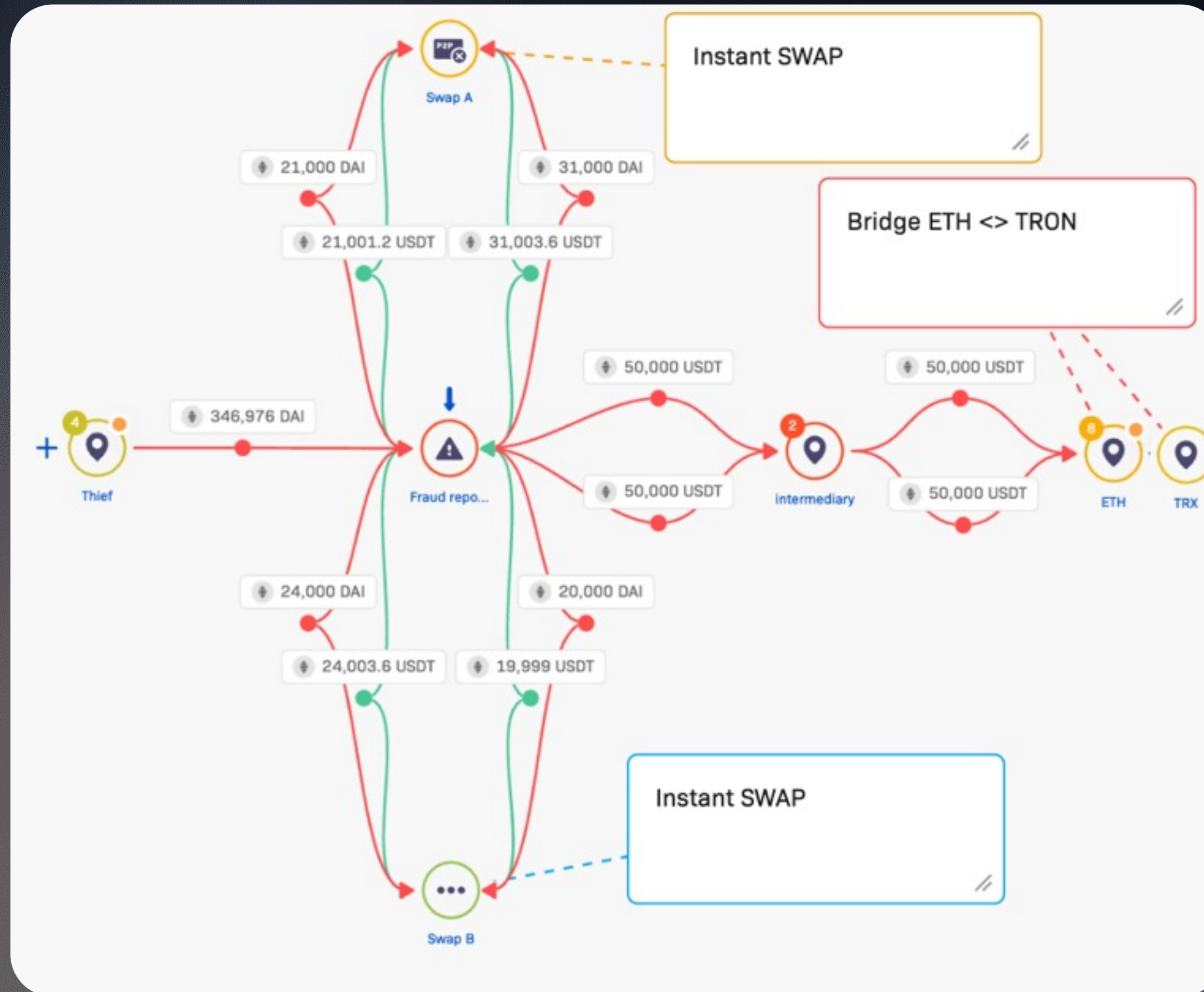
From Value:

30 USDC

To Value:

27.410460 USDT(TRON)

Swaps and cross-chain bridges



Swaps and cross-chain bridges



0xd9e8ca7e4798f56a375ca60a34f652854c4fdb262974f625909fd182772d5bfa 

✓ Success

✓ 20685601

1228898 Block Confirmations

🕒 171 days ago (Sep-05-2024 04:32:47 PM UTC) | ⌚ Confirmed within 3 secs

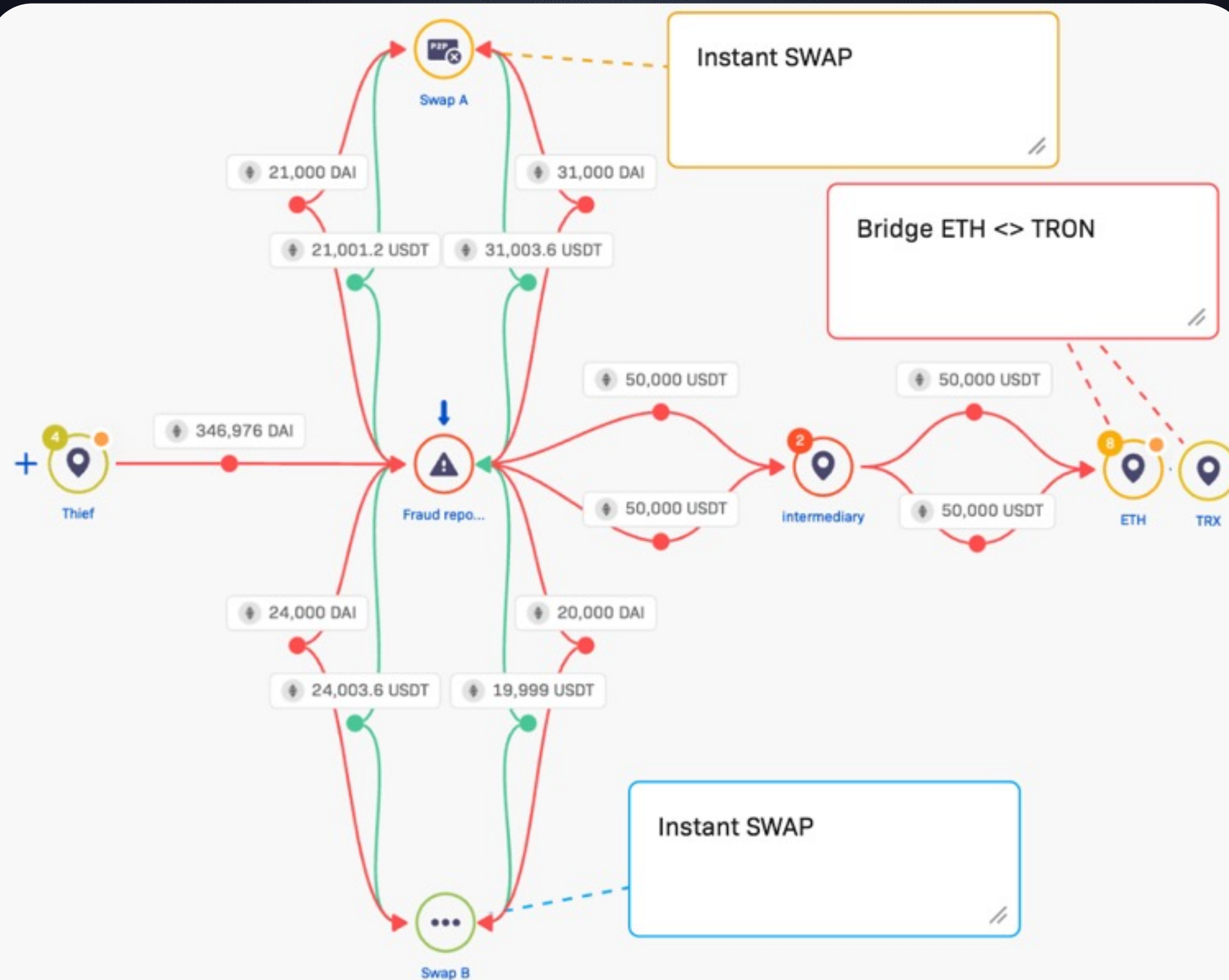
► Call **Bridge To V2** Function by [0x5C68DaEC...D7FBa5ab6](#) on  [OKX: Web3 Proxy](#) 

Swaps and cross-chain bridges

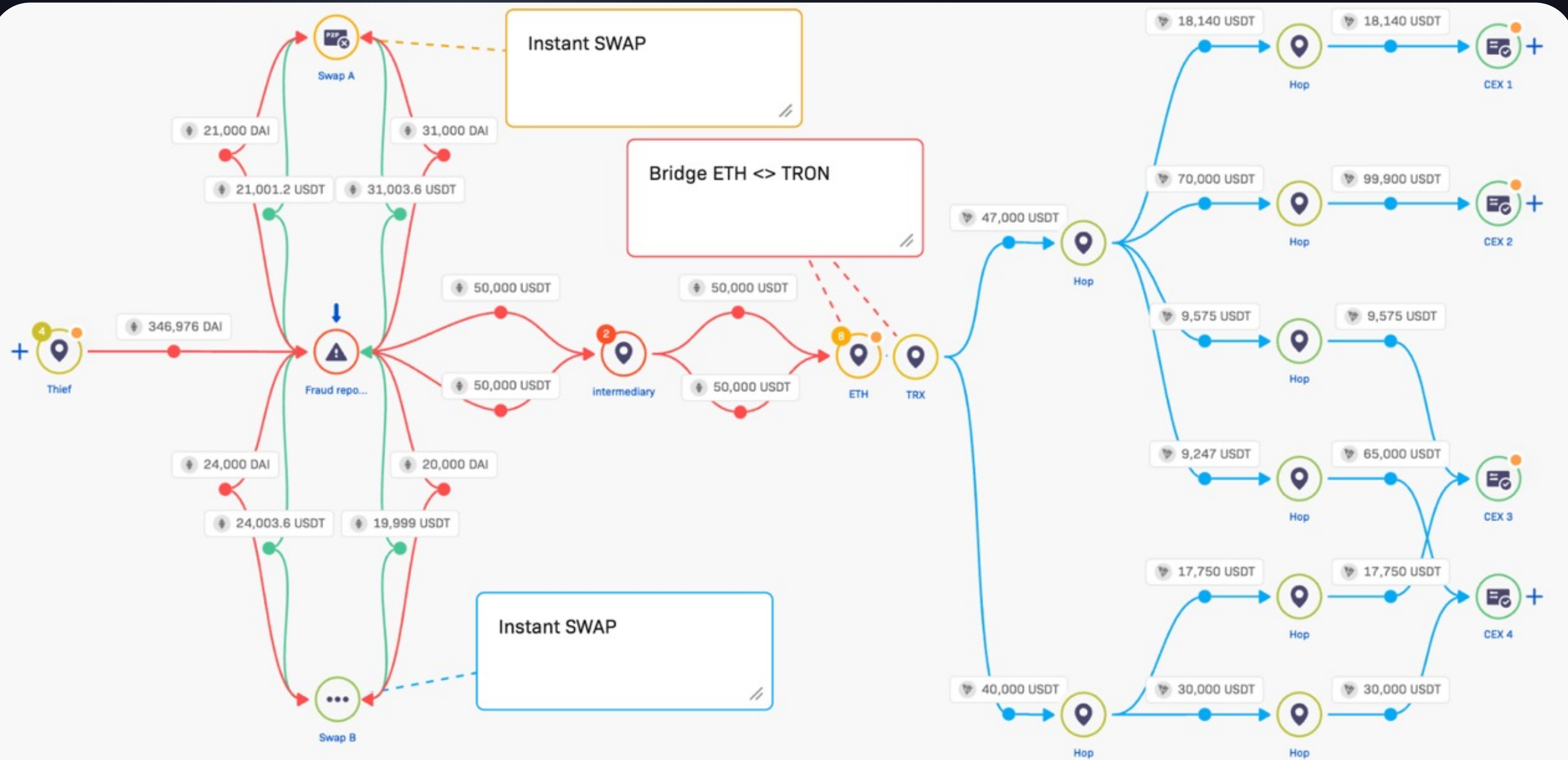


Address	0xb685760ebd368a891f27ae547391f4e2a289895b    
Name	Swap (address fromToken, string toToken, address sender, string destination, minReturnAmount) View Source
Topics	0 0x45f377f845e1cc76ae2c08f990e15d58bcb732db46f92a4852b956580c3a162f
Data	fromToken : 0xdAC17F958D2ee523a2206206994597C13D831ec7 toToken : USDT (TRON) sender : 0xFd6eAd5eAB787Df0dECf409F6B088312e7B38E6b destination : TTNy1SqQ3ZFkT91LtDM4ea6YqGH6Hte1Mu fromAmount : 50000000000 minReturnAmount : 49848000000

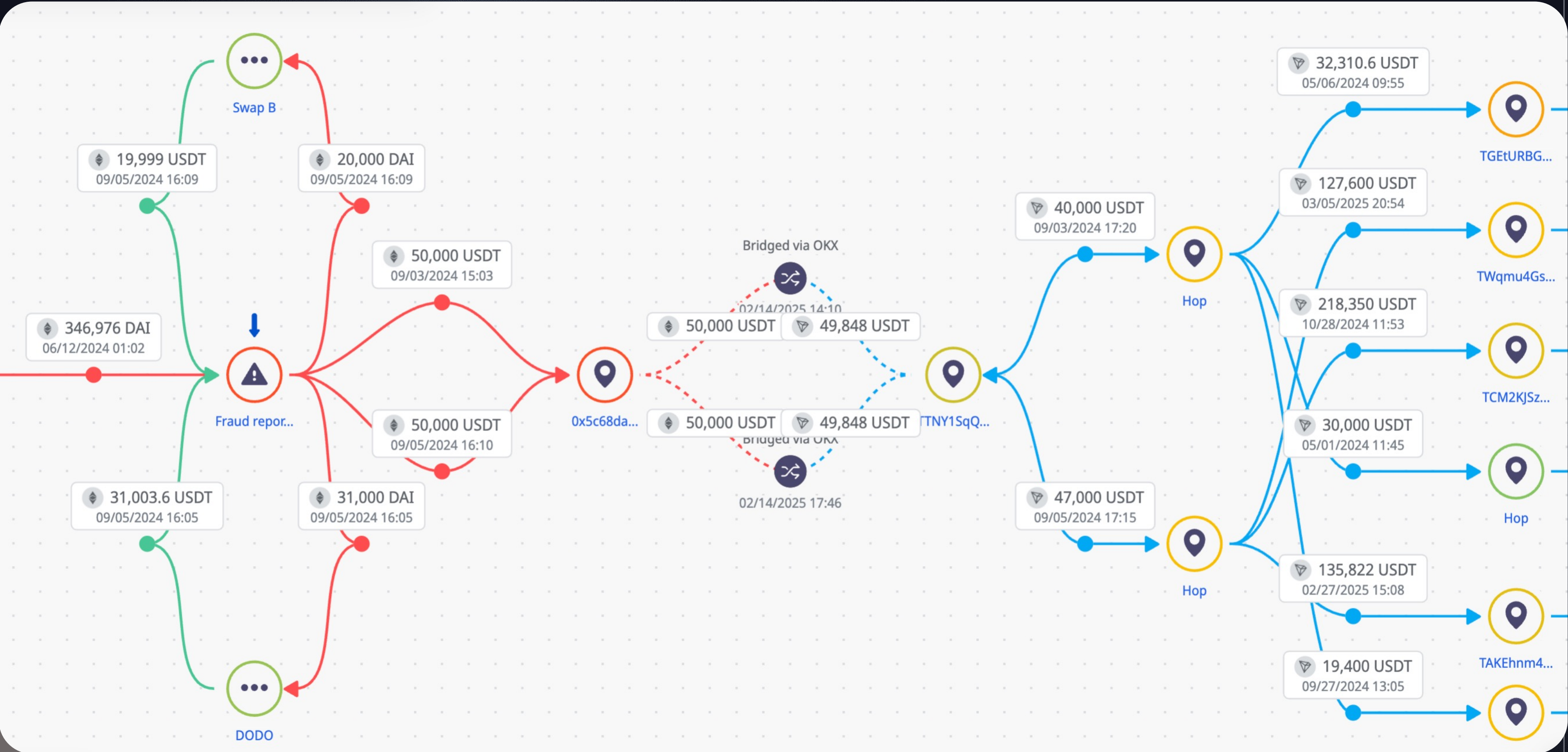
Swaps and cross-chain bridges



Swaps and cross-chain bridges



Swaps and cross-chain bridges



Mixers



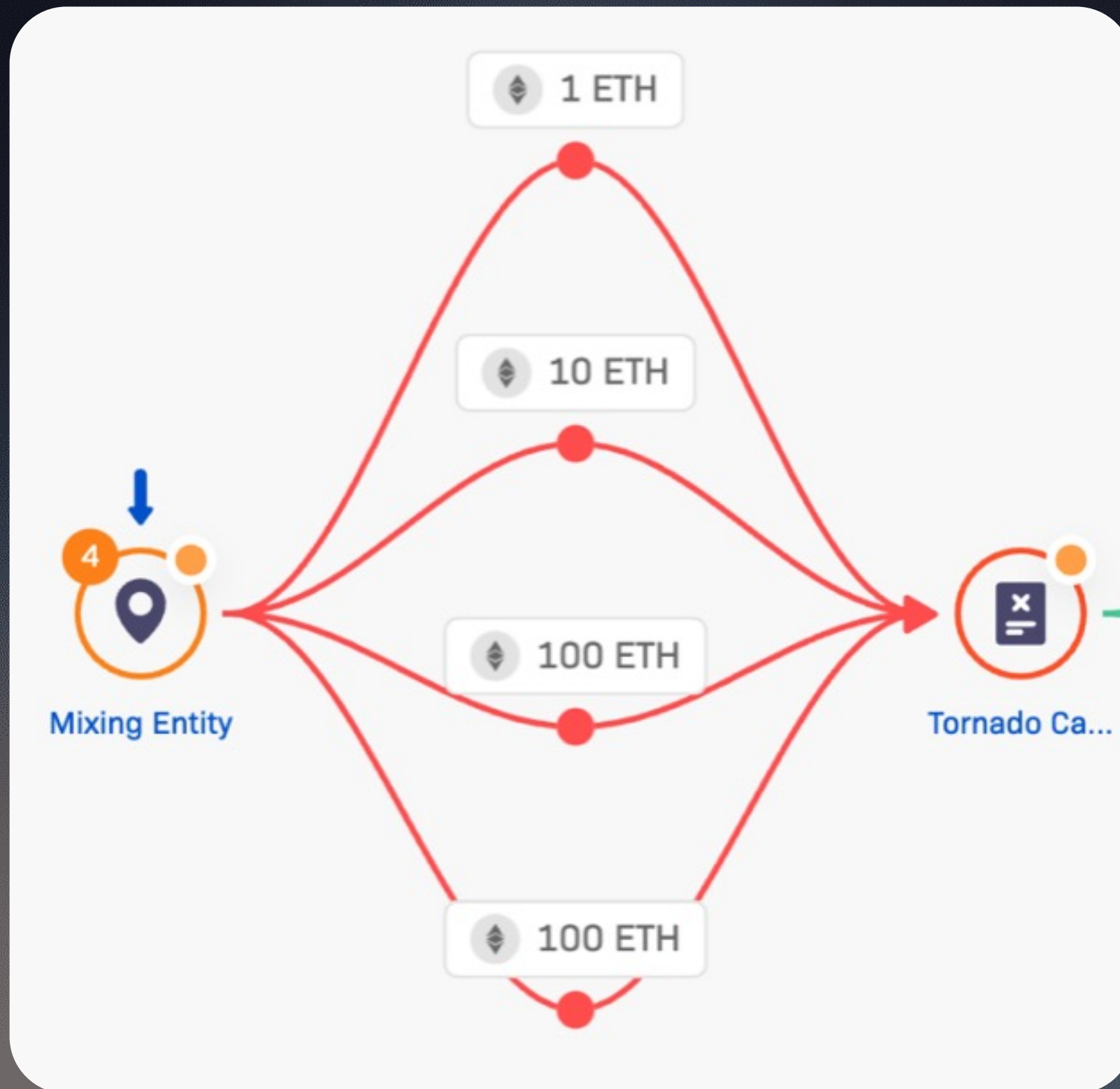


Four Important truths about **Demixing**

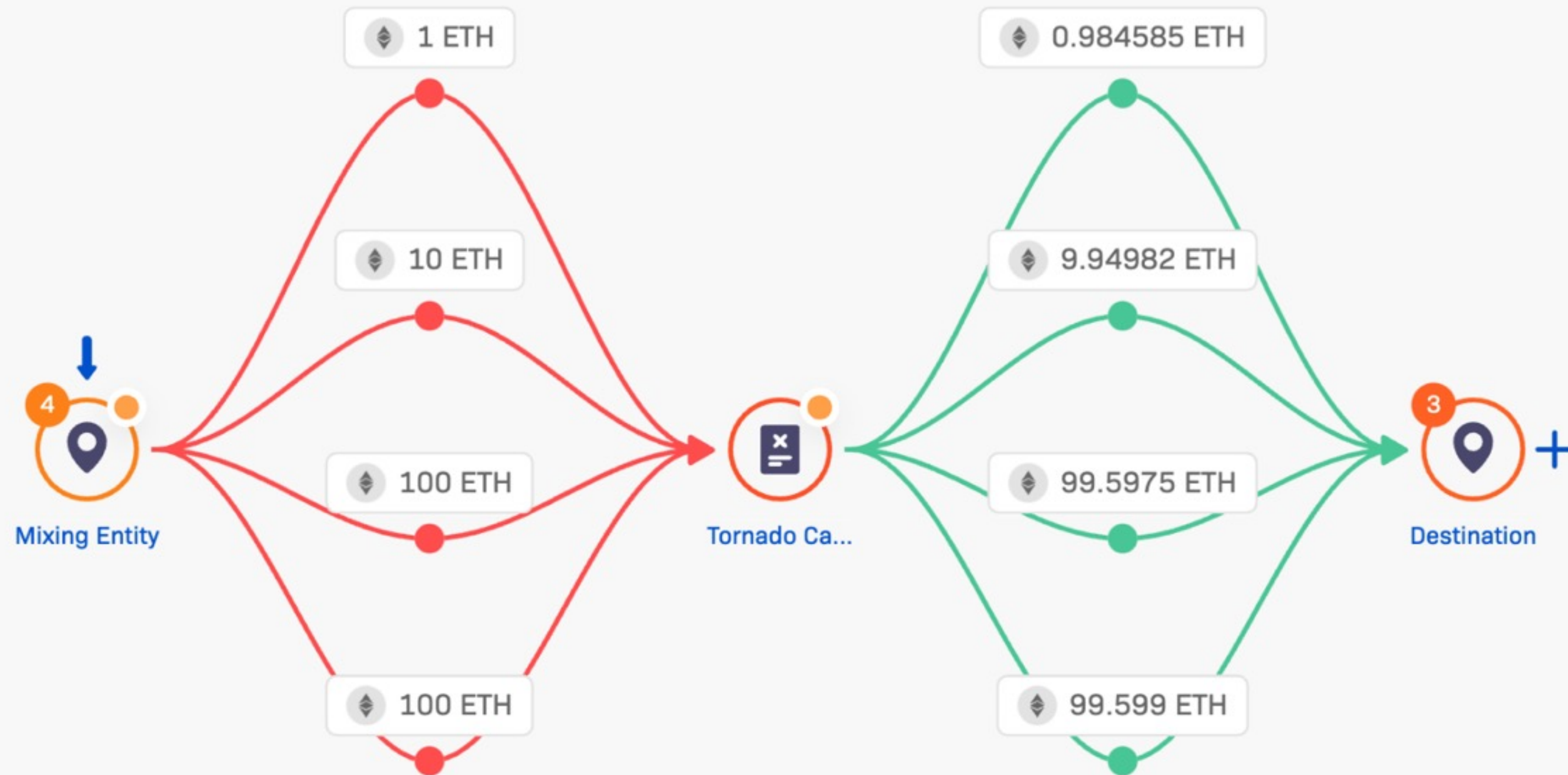
- Demixing is **HARD**
- Demixing is **TIME CONSUMING**
- Demixing is **NOT ALWAYS ACCURATE**
- Demixing is **FRUSTRATING**



- “Why not Just Use a **Mixing Service?**”



- “Why not Just Use a **Mixing Service**?”



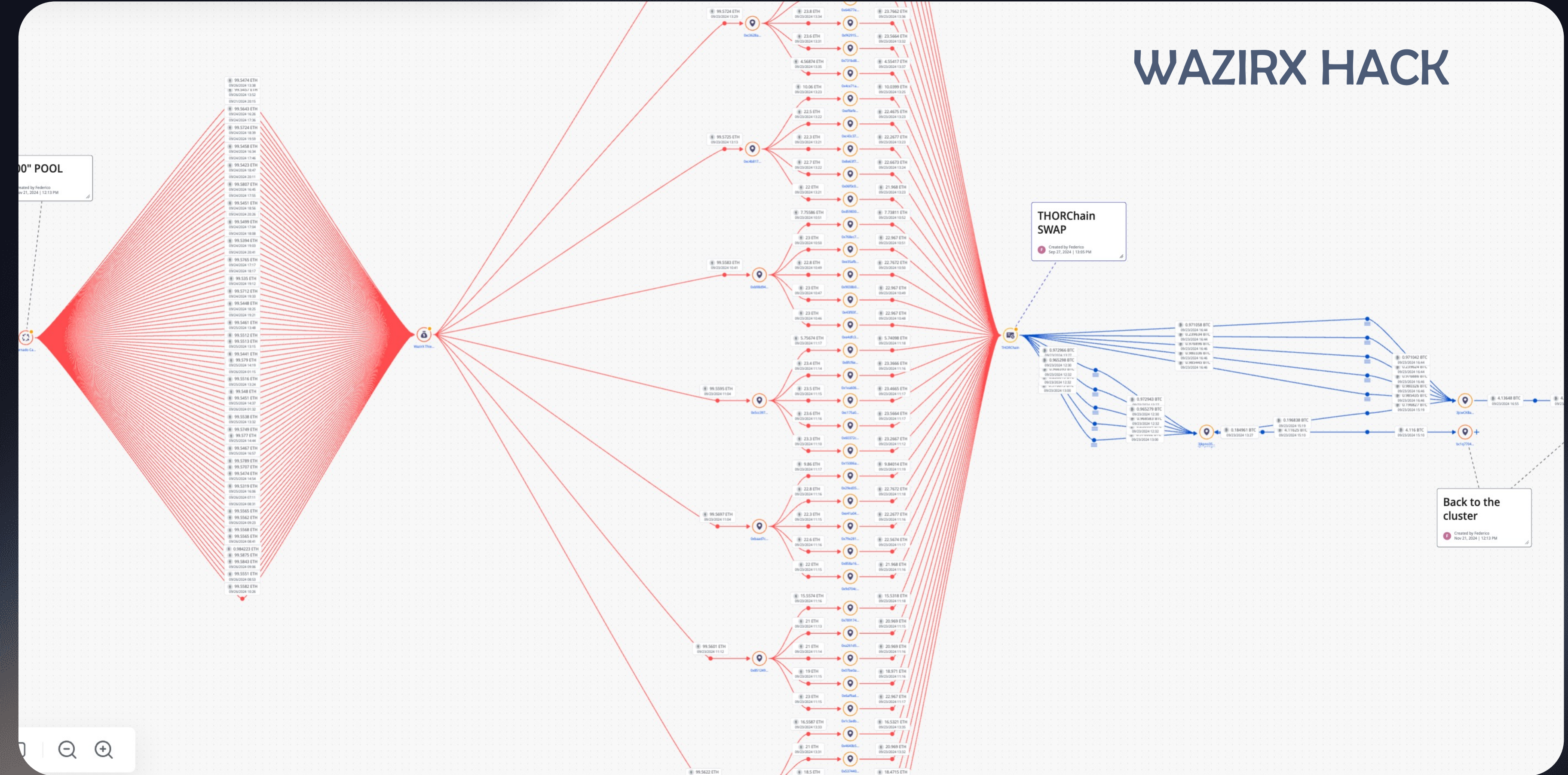


WAZIRX HACK

00" POOL

Created by Federico
Nov 21, 2024 | 12:13 PM

THORChain
Created by Federico
Sep 27, 2024 | 13:05 PM



Back to the
cluster

Created by Federico
Nov 21, 2024 | 12:13 PM

• “Why not Just Use a **Mixing Service?**”



Block Date Apr 02, 2025 11:54 PM

IP 104.248.139.211

Add	INPUT ADDRESS	BTC ↓
	339746885 (26)	63.48159139

Entity/Type

All

Add	OUTPUT ADDRESS	BTC ↓
	Wasabi wallet (1)	63.48140861

Show demixing results

Demix



Navigating self-custody & seed-phrases





THE REALITY

The fundamental problem

"You can seize the person but not the assets, unless you have the keys."

Traditional finance

Assets held by intermediaries →
can be frozen

In crypto

Assets can be held by individuals →
no intermediaries (like cash)



THE PROBLEM

What is self-custody?

“Self-custody is sovereignty, but also a seizure challenge.”



User control

Private keys

Seed phrase



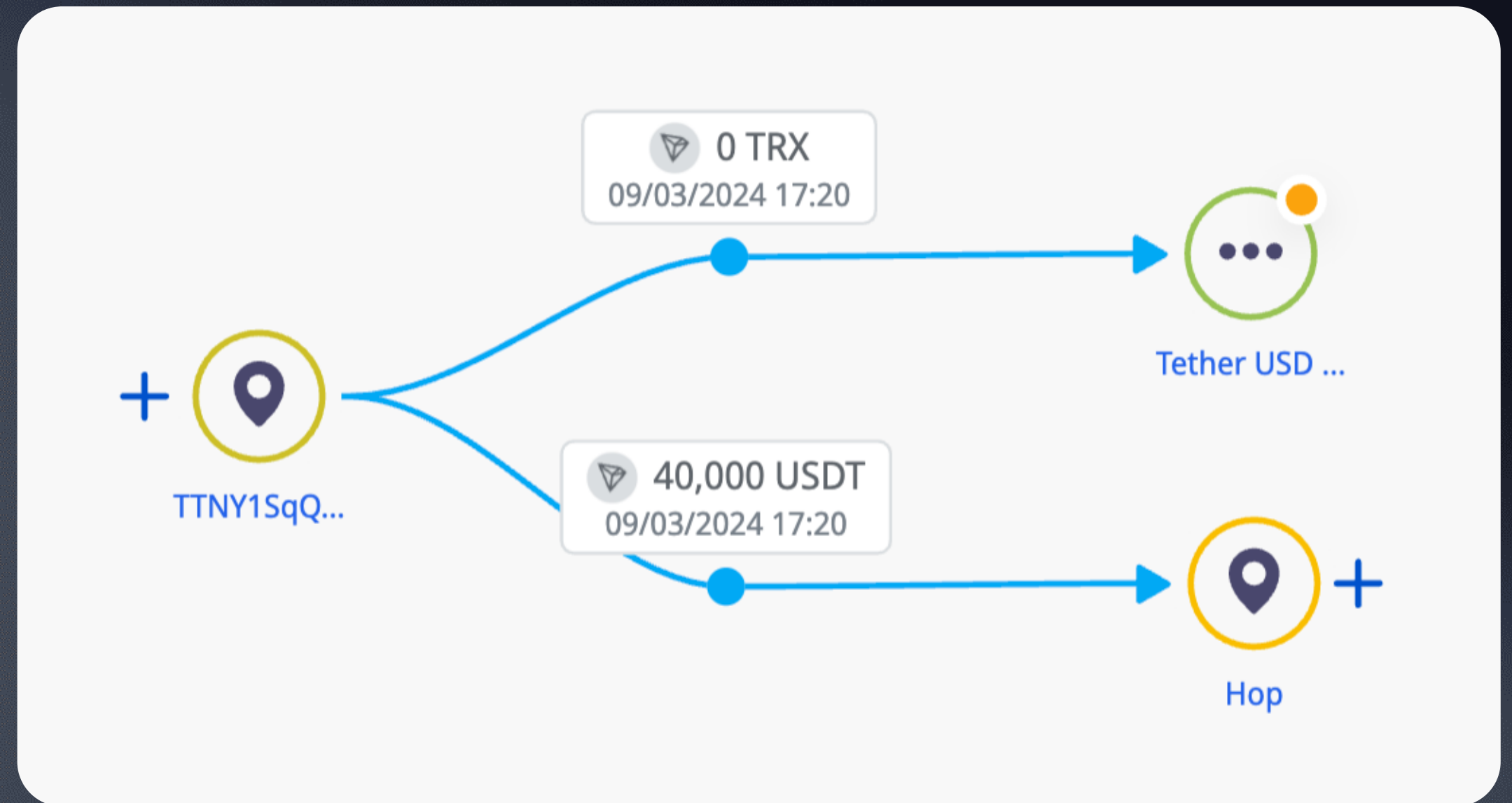
No bank

No custodian

No reset button

THE EXCEPTION

Centralised Stablecoins



Blocklists



World / United Kingdom

Man who lost \$800 million bitcoin in landfill wants to buy the garbage dump

By Issy Ronald, CNN

🕒 3 min read · Updated 10:22 AM EST, Fri February 14, 2025



James Howells accidentally threw away the hard drive that allows him to access his bitcoin.



THE INNOVATION

Hierarchical Deterministic Wallets





THE BARRIER

The seed phrase

*“A seed phrase is not just access,
it’s absolute control.”*

12-24 words

Whoever has it – owns the funds

- No recover mechanism
- No central override
- Instant transfer possible



THE REALITY:

Why seizures are hard

“By the time a court order is issued, the funds may already be gone.”

- No central authority
In crypto you seize through access
- Speed of movement
Crypto doesn't wait warrants
- Anonymity/pseudonymity
We don't start with names. We start with patterns.
- Cross-border jurisdiction issues
Crypto is global. Enforcement is local.
- Use of mixers/DeFi/bridges
Defi removes intermediaries and with them, traditional control points



UNDERRATED INSIGHT

Behavioural reality

“The weakest point is not always the blockchain, it’s human behavior.”

Suspects may:

1

Memorize seed phrases

2

Split phrases (Shamir/partial storage)

3

Use decoy wallets

4

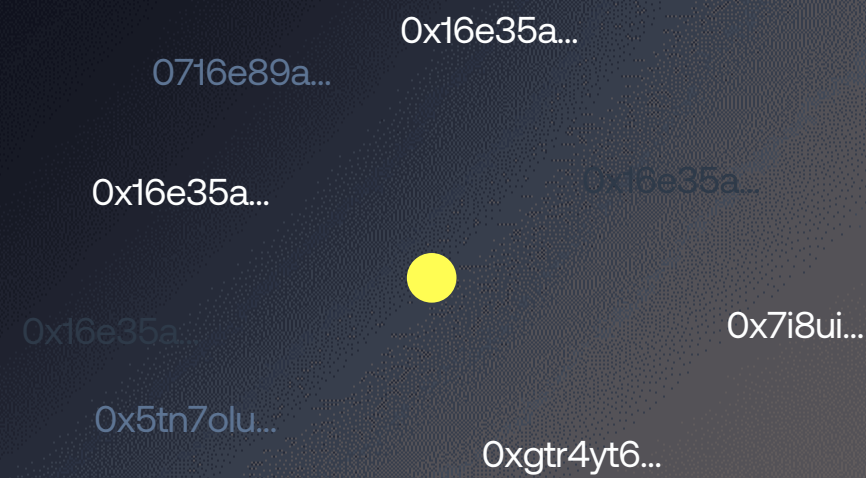
Use hardware wallets hidden physically



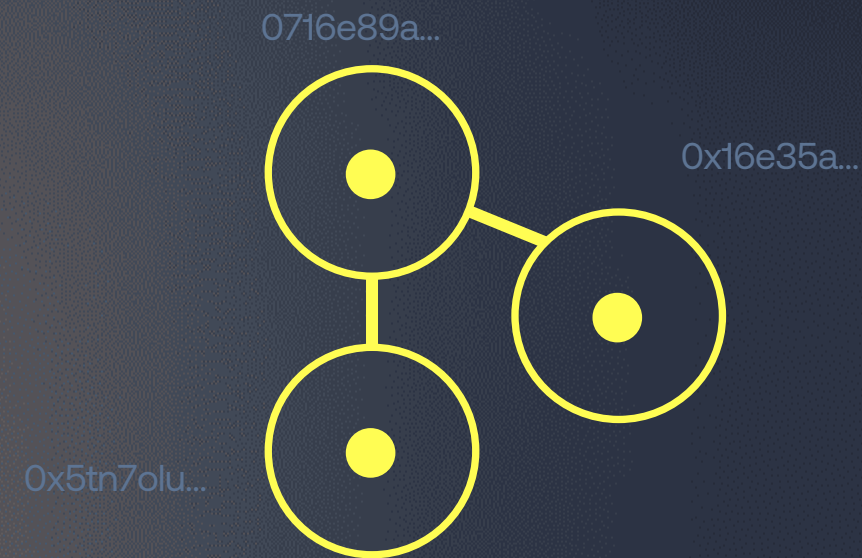
HIDDEN PATHS

One seed $\neq$ one wallet

“Access to the seed does not guarantee access to all funds.”



One seed generates thousands of addresses

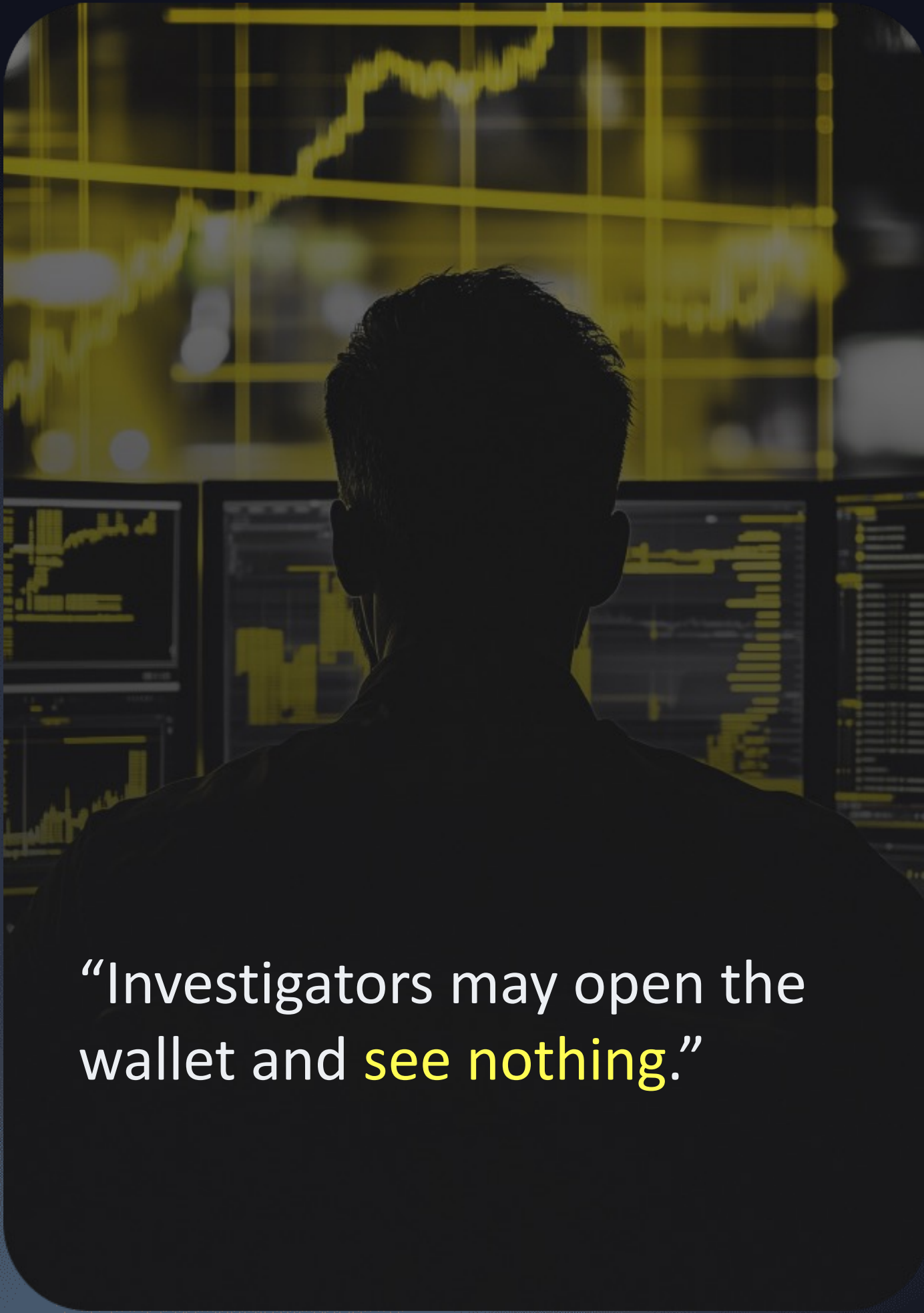


Organized wallets through derivation paths



Wallet apps show only default paths

Derivation paths as an obfuscation tool



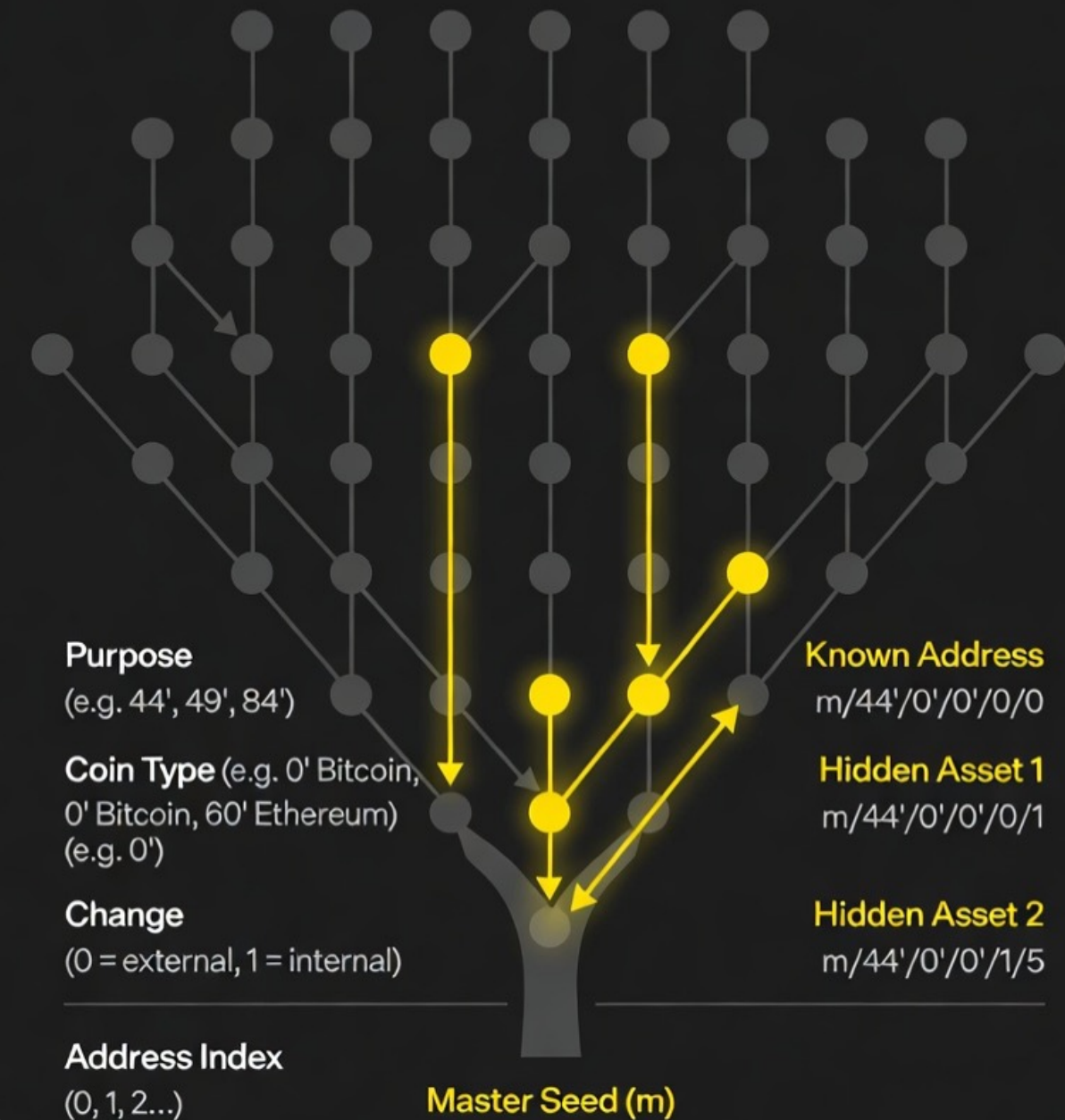
“Investigators may open the wallet and **see nothing**.”



CRIMINAL STRATEGIES

- Use non-standard paths
- Hide funds outside default wallets
- Keep decoy balances in visible paths
- Spread funds across multiple branches

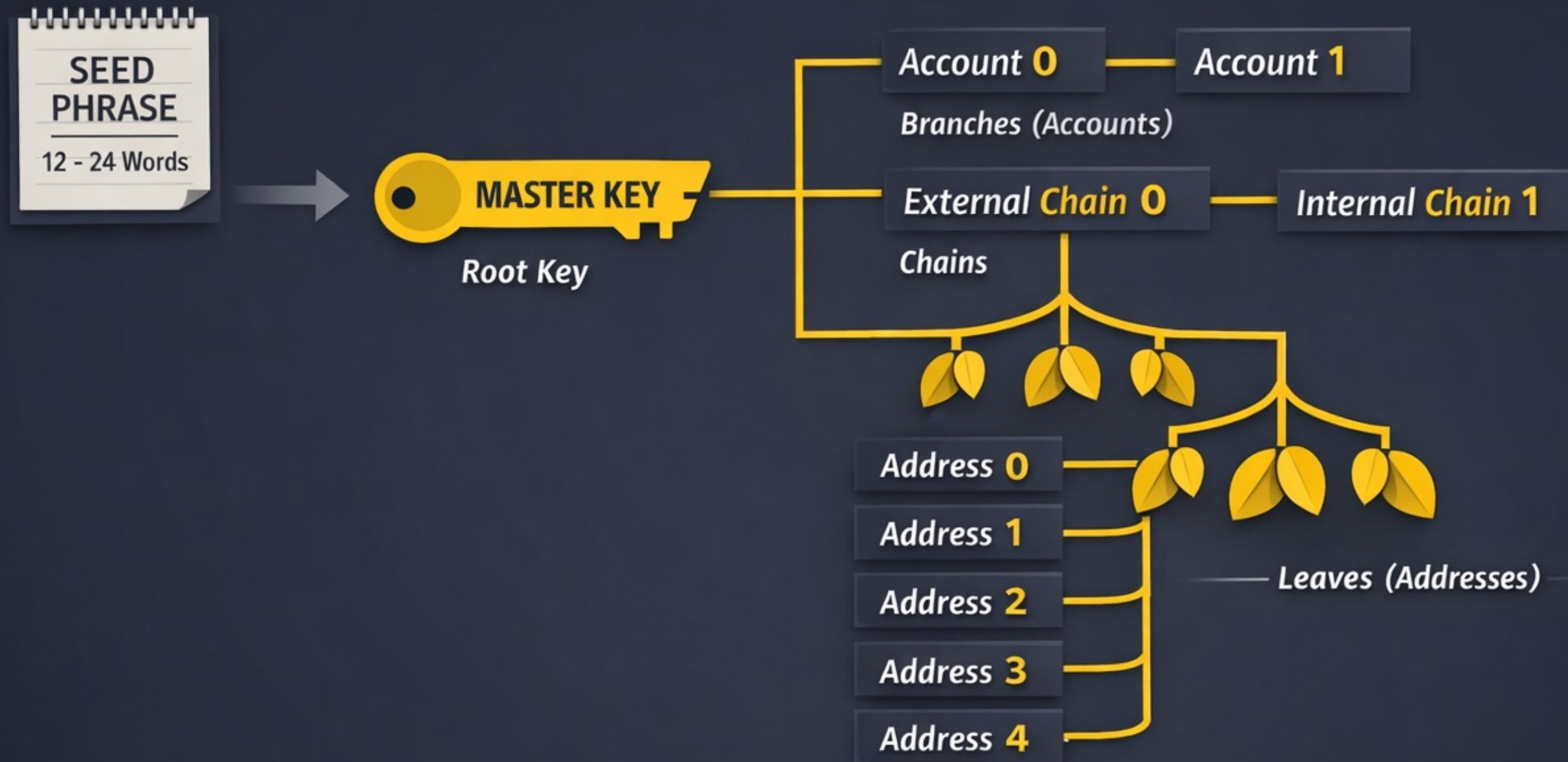
Crypto Derivation Paths: Hiding Assets in HD Wallets





HD WALLET DERIVATION PATHS

From Seed to Addresses



Derivation Path: $m / 44' / 0' / 0 / 2$

“Bitcoin, Account 0, Change, Address 2”

Purpose / Coin Type / Account / Change / Index



HOW THINGS WORK NOW

Current seizure approaches

“Most successful seizures still depend on human or operational errors.”



- Cooperation based
- The suspect reveals keys



- Device-based
- Able to access unlocked phones/laptops



- Custodial choke points
- Exchanges and on/off ramps



- Operational mistakes
- Poor key management by suspect

Cloud Services



Hong Kong Bitcoin Exchange BitFinex Loses Nearly 120,000 Bitcoins in Hack >\$72 million worth of coins stolen, Bitcoin price plummets, individual customer accounts hacked despite multisignature protection

BY MORGEN E. PECK | 03 AUG 2016 | 2 MIN READ | [Bookmark](#)





THE REALITY

Key difficulties



Time sensitivity

Crypto moves instantly



Encryption barriers

Locked devices



Privacy tools

Mixers, privacy coins



Multi-chain complexity

Assets spread across chains



DeFi opacity

Smart contracts, liquidity pools



SOLUTIONS

Strategies

Preparedness

Pre-identified wallets
and real-time alerts

Monitoring

Track long term, even
if not seized today

Seize early

Timing is often more
important than legal
strength

Exploit behavioural weaknesses

- Social engineering
interrogation strategy
- Digital forensics

Multi-agency coordination

Including cross border
cooperation

Target the fiat interface

Exchanges remain
key points



LOOKING FORWARD

Future trends

“Seizures will become less about force and more about intelligence.”



More self-custody
adoption



Better privacy
tools



AI-assisted
laundering



Institutional
involvement

In the world of self-custody,
possession is no longer nine-
tenths of the law, control is.

And control, in crypto,
is defined by keys.

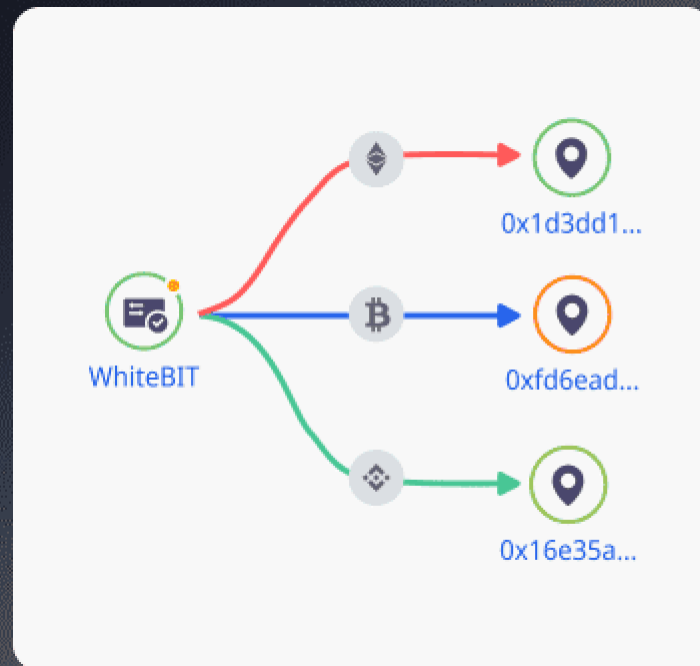




TOOLING

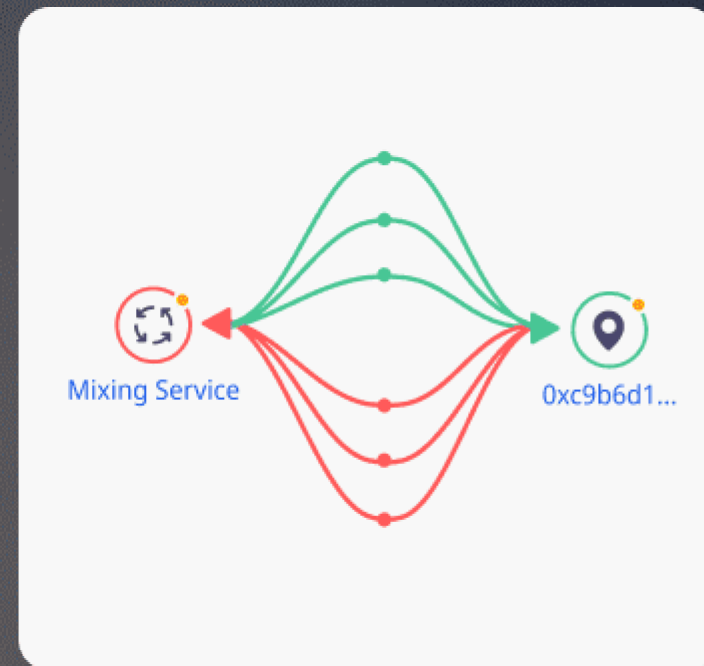
The role of blockchain analytics

Wallet tracking



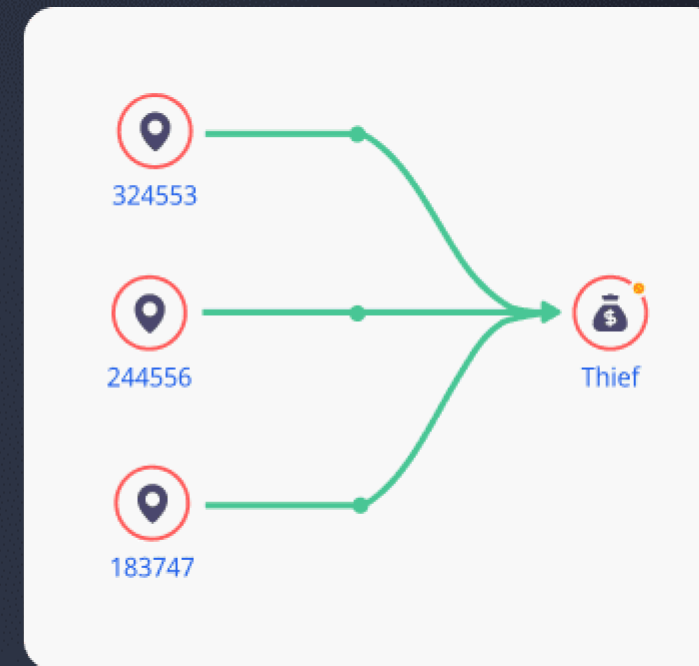
Who has this address transacted with?

Transaction tracing



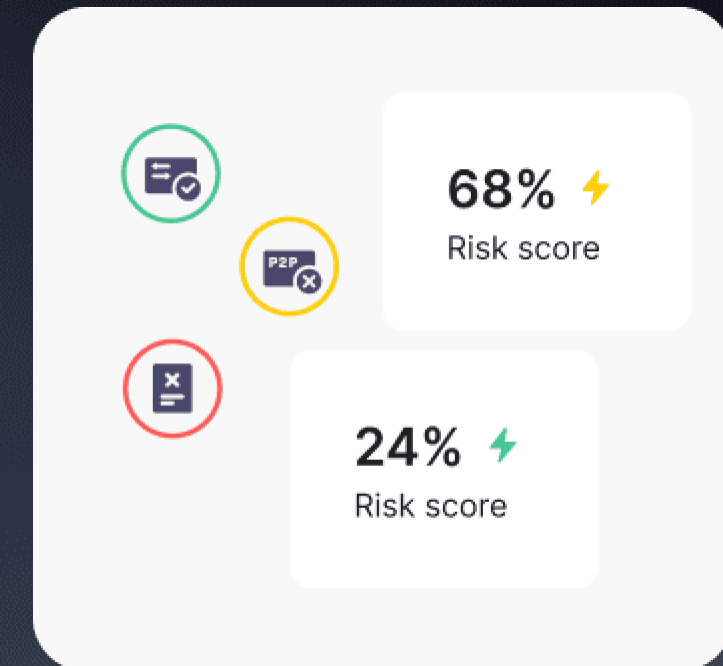
Pattern detection across transactions

Exchange exposure



Real-time sanctions screening

Activity pattern analysis



Behavioral anomalies

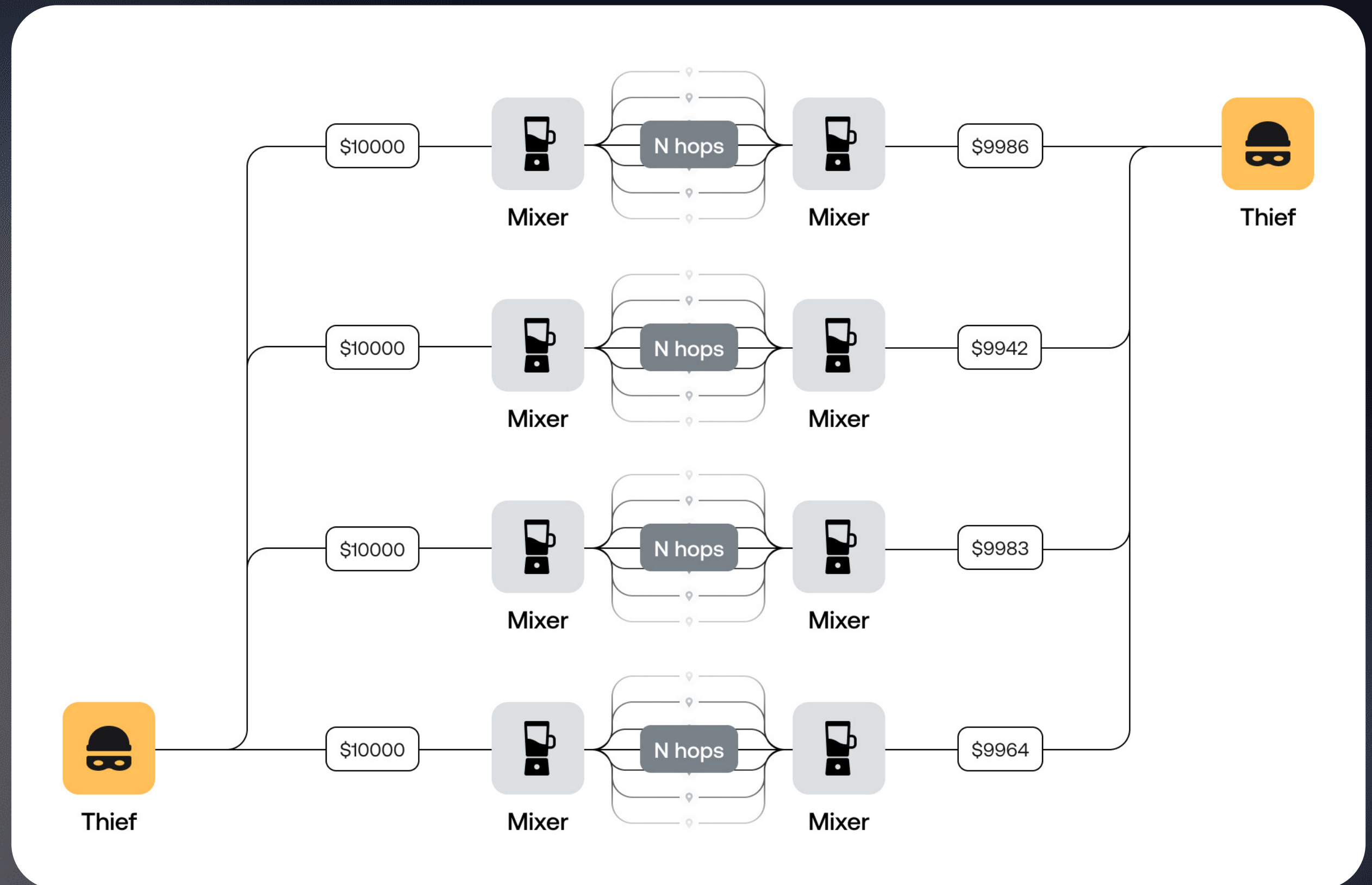
"We don't hold the keys, but we map the battlefield."

The importance of LOGS



Mixer

At first, the assets moved through a mixer. We were able to trace the transactions through the mixer and find their destination.





CHAPTER 2

Exchange



CHAPTER 3

Privacy Coins



Monero (XMR)



Zcash (ZEC)



Verge (XVG)



Beam (BEAM)

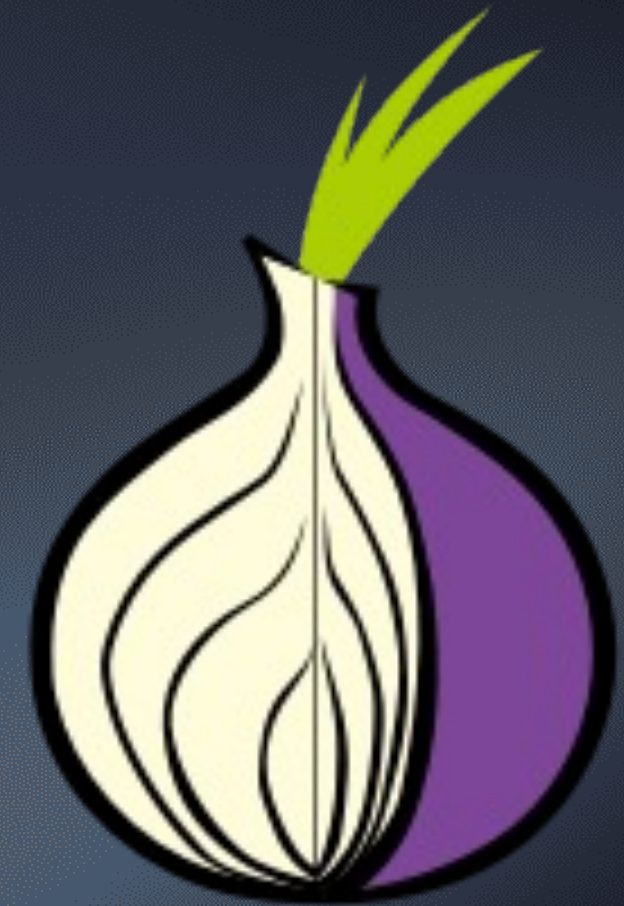


Privacy Coins

LE success usually comes from off-chain mistakes:

- Suspect used a KYC exchange before or after privacy coin usage
- Poor OPSEC (email, IP reuse)
- Undercover buy / controlled delivery
- Seizure of wallets
- Correlating blockchain timing with marketplace logs
- Using a VPN or Tor incorrectly

Even Monero becomes irrelevant if the endpoint is seized.



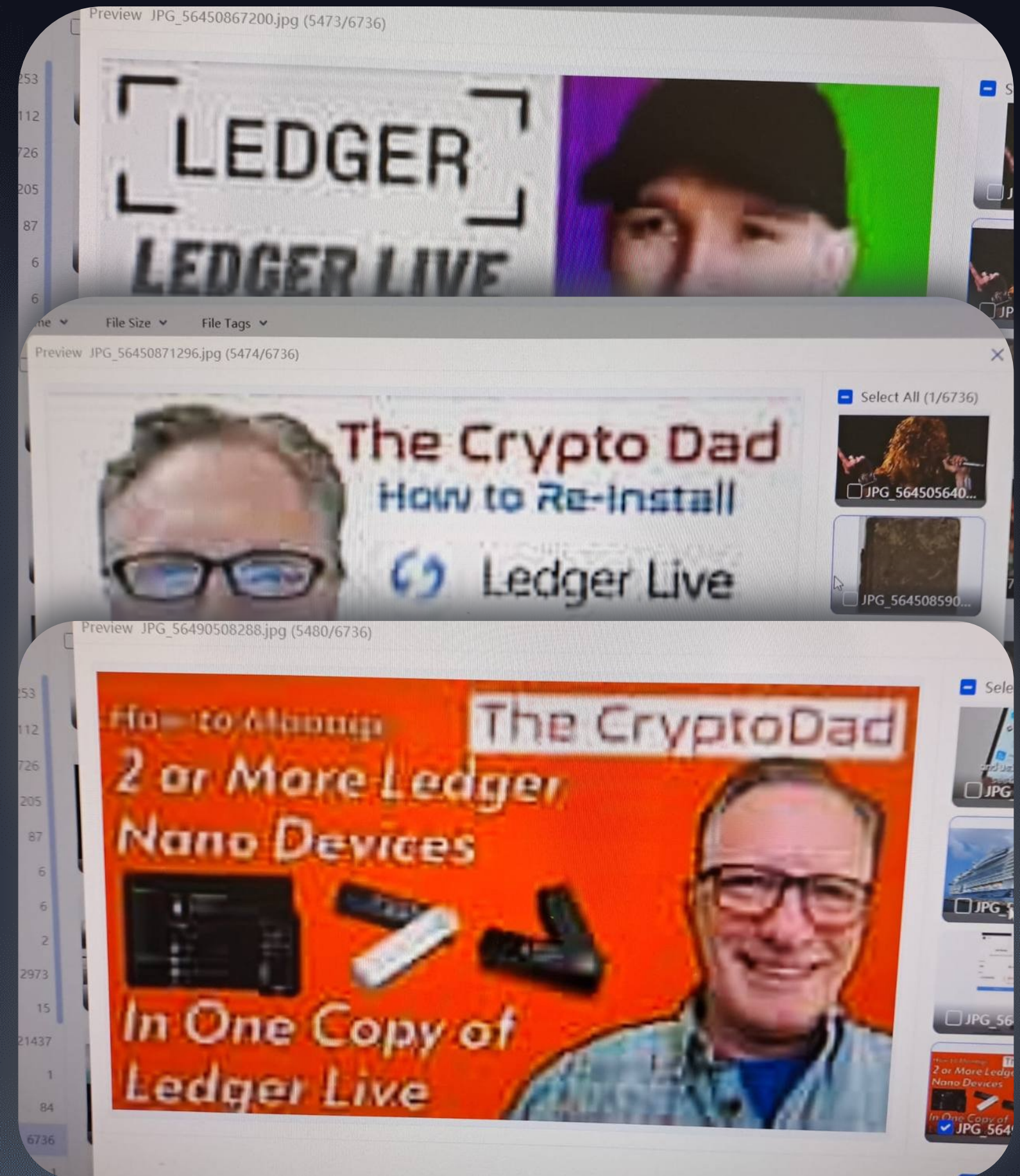
Logs

IP Address	Country	VPN
192.168.1.1	USA	✓
192.168.1.1	Canada	✓
172.16.254.2	Germany	✓
198.51.100.7	Australia	✓
203.1		✗
172.16.254.11	Spain	✓
10.0.0.12	Sweden	✓

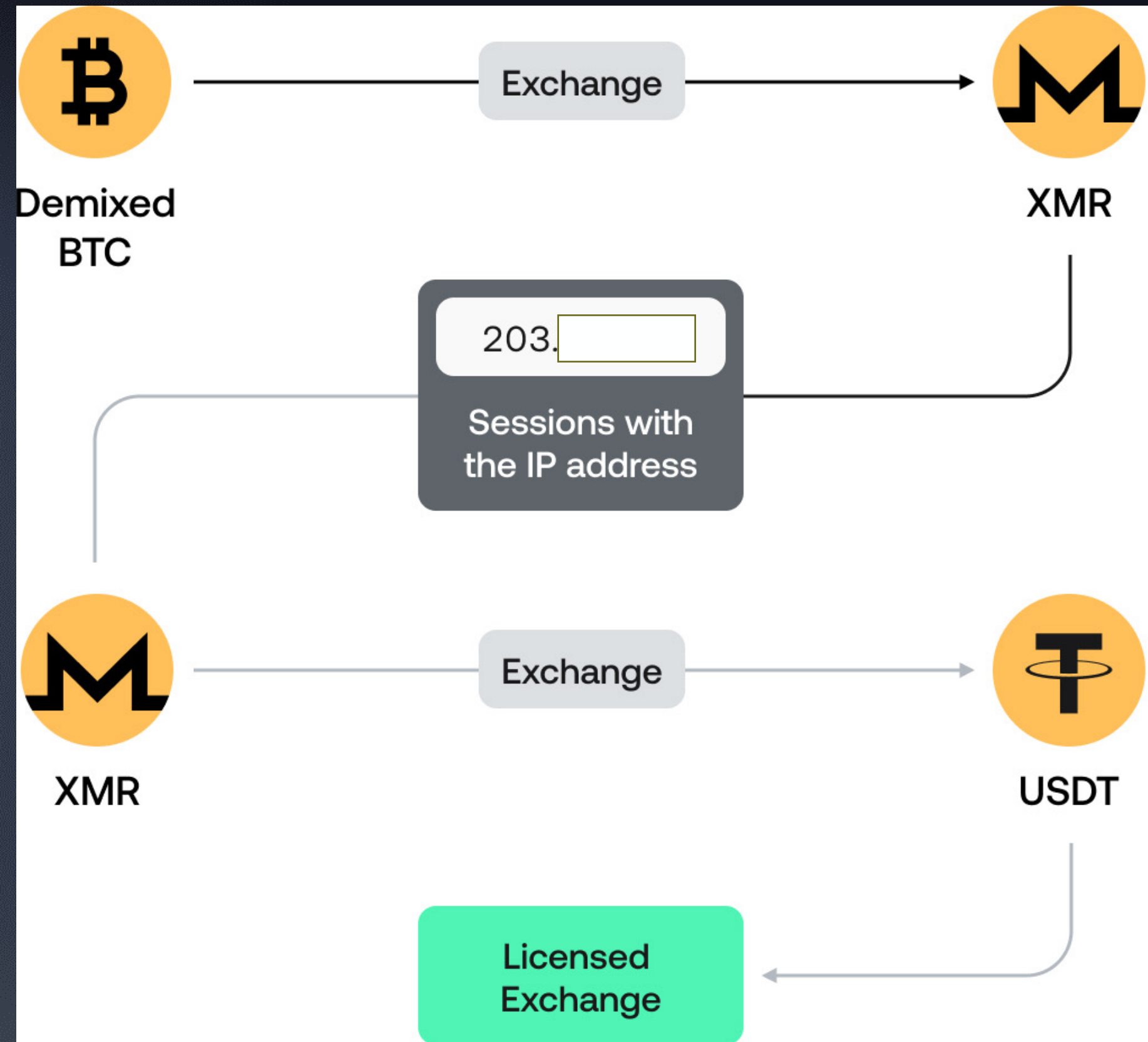
- OS: Windows 10
- Screen Size: 1920x1080
- Timezone: EET (Eastern European Time)
- IP: 203.1
- Browser: Firefox
- Browser Language: en-US
- Session History: 14 transfers in 4 days, BTC to XMR

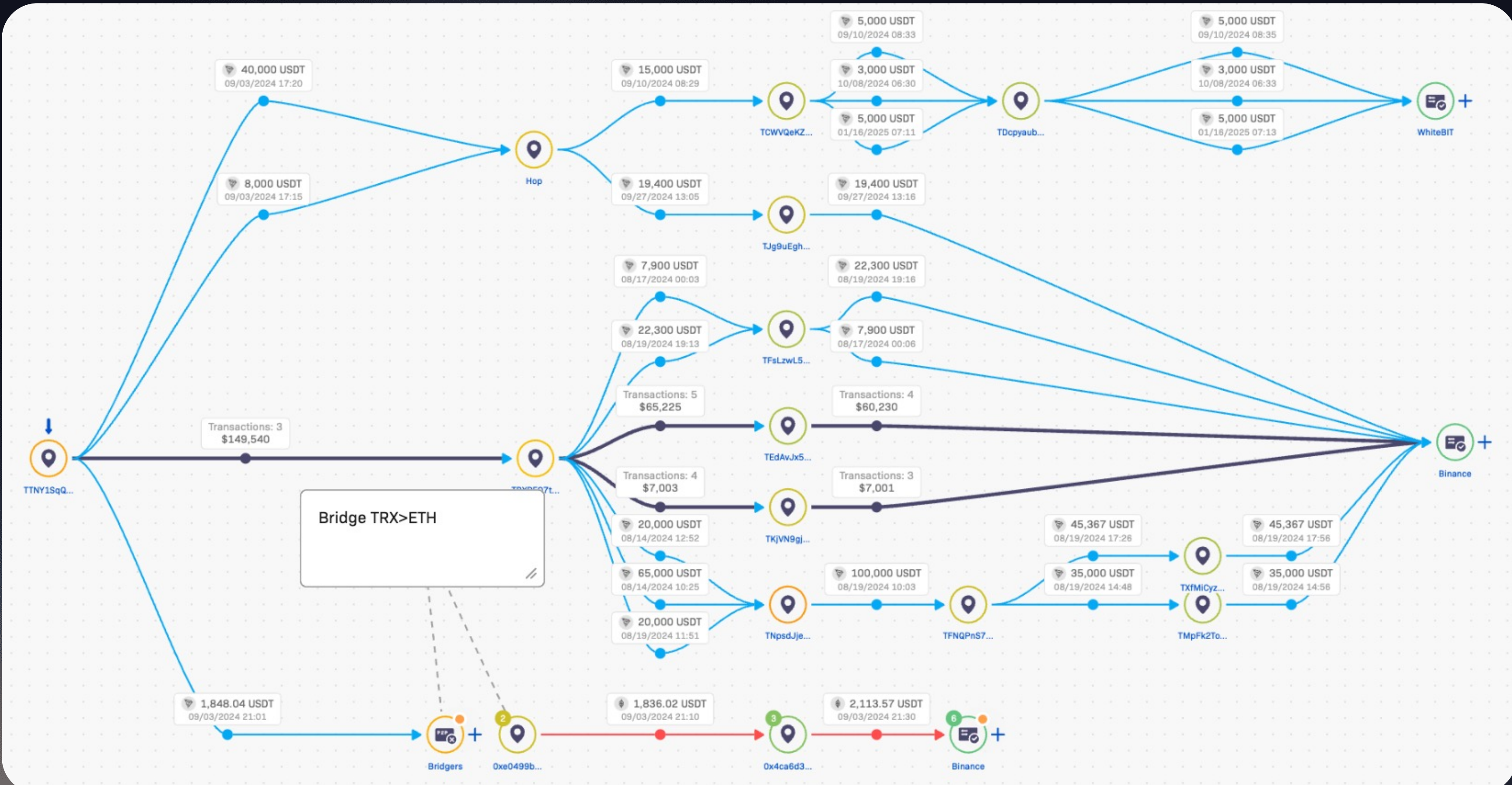
CHAPTER 5:

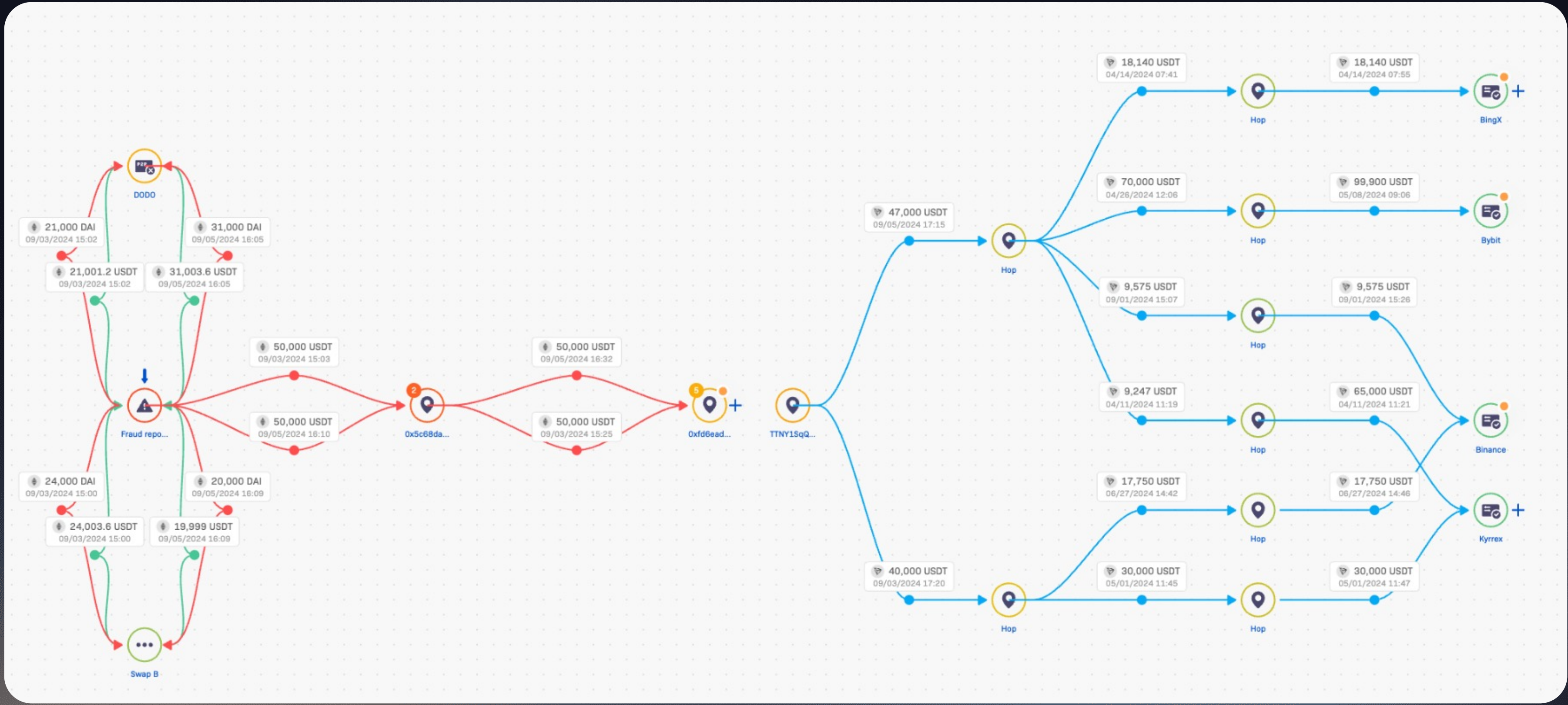
Working with logs

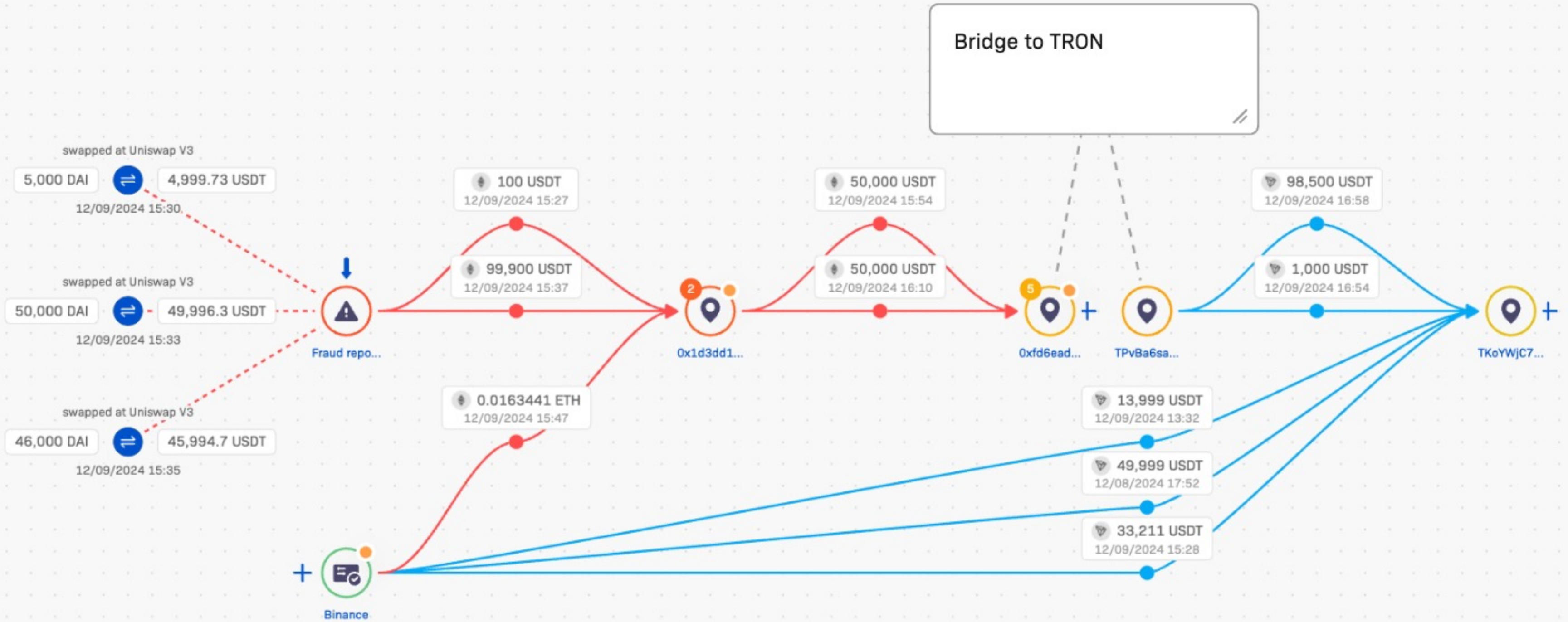


Working with logs









Results

01

Portion of Crypto was
suspended

02

Suspect Identified



03

Collaboration with Law Enforcement

04

Funds traced to
Exchanges

05

Law Enforcement
working on recovery



The solution





Get your
hands dirty!

Use professional
tools





Train
your staff

Enhance
Cooperation





3
Train
your staff

4
Cooperation



Thank you!

Evolving Definition of Crimes

How AI transforms criminal proceedings
Cybercrimes 2.0
Pretty-Good-Privacy phones and admissibility of data



Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not
necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible
for them.

Sandor Bosch

Court of Appeal Den Bosch
The Netherlands

**#Digitalisation and #AI in Criminal
Justice**

**ERA seminar · Tallinn · 7–8 May
2026**

Online investigations and internet searches
in times of AI

Hans Spekman
groeide op in armoede

Joods zijn in steeds
vijandiger klimaat

Algemeen Dagblad, 2 May 2026

► **'Alle 60.000 agenten moeten alert zijn op online misdaad'**

Cybercriminaliteit krijgt bij politie topprioriteit

Meer dan de helft van alle criminaliteit gebeurt online. Het gaat dan om oplichting, bedreiging, fraude, diefstal en afpersing. Daarom moet iedere agent cybercriminaliteit gaan bestrijden.

Wout van Arensbergen
Henk van Gelder

Driebergen

dagelijks onderdeel worden van hun werk."

Dat inzicht zorgt voor een enorme omslag binnen de politie, die de nieuwe werkwijze de komende jaren invoert. De aanpak van online criminaliteit krijgt topprioriteit en moet volgens Duijf ook in het dagelijkse politiewerk een stevig fundament krijgen.

Samenhangend

Aangiften van online criminaliteit waarbij mensen worden opgelicht,

kampen slachtoffers vaak ook met psychische schade. Ze schamen zich en durven niemand meer te vertrouwen. De totale schade van alle cyberincidenten in Nederland zou volgens een onderzoek van het ministerie van Economische Zaken jaarlijks rond de 10 miljard euro bedragen.

Duijf benadrukt dat elke aangifte van belang is. „We kijken als politie

vaak nog te enkelvoudig naar aangiften, te individueel. Vaak zijn er veel meer mensen slachtoffer geworden. De kunst wordt om naar het grotere geheel te kijken. Naar patronen, naar clusters. En dat dan aanpakken. Daarom is elke aangifte belangrijk."

De cyberspecialisten bij de landelijke en regionale teams vormen volgens Duijf het neusje van de zalm en zijn betrokken bij alle grote complexe onderzoeken naar internetcriminelen.

Ook internationaal is de samen-



Toen
nu d
en d

Engel
Diede
Overb



Why this topic matters now

Digitalisation has moved from a specialist issue to the ordinary environment of criminal justice.

The central development is practical: evidence, communication and offending behaviour are increasingly digital, while courts remain responsible for legality, reliability and fairness.

The pressure points

AI is appearing in legal submissions, internal research tools and criminal modus operandi.

Its outputs force courts to ask who is responsible, how quality is verified, and whether the source can carry legal authority.

The courtroom reality

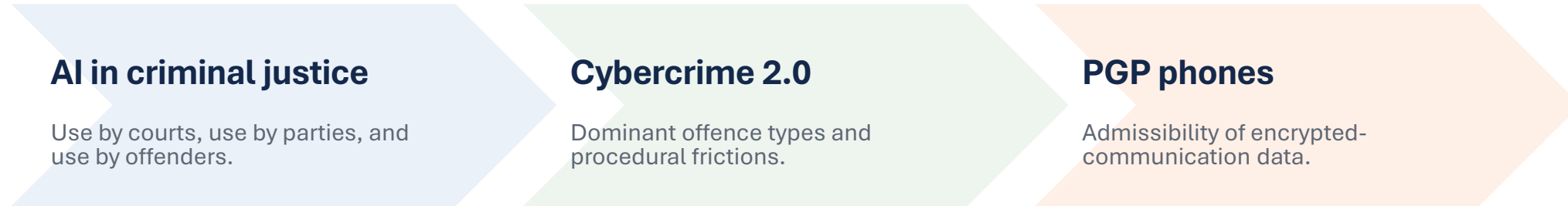
Cybercrime now dominates a significant part of daily practice: bank-helpdesk fraud, phishing, ransomware, doxing and unauthorised access cases require both technical literacy and classic procedural discipline.

The unresolved debate

Encrypted-phone litigation shows how national criminal procedure, cross-border cooperation and European law collide when massive datasets become central to serious organised-crime prosecutions.

Structure of the presentation

Three developments, one underlying question: how criminal justice preserves control over digital power.



The common thread is the same throughout: digital criminal justice is becoming less about isolated computer offences and more about data environments. Courts must assess evidence that is technically complex, legally fragmented and often transnational.

The aim is a concise Dutch case study, with broader relevance for judges, prosecutors and defence lawyers working in EU criminal justice.

AI has entered Dutch criminal justice

AI appears in judicial work, legal submissions and offending methods.

**01**

Courts as users

Internal AI tools such as RechtspraakGPT support the court staff with non-sensitive tasks outside the judiciary domain – writing memos, policy papers, but not meant for tasks related to decision-making.

**02**

Parties as users

Lawyers and litigants increasingly submit AI-generated output as if it has expert value. Courts are developing a cautious response focused on verifiability, accountability and the legitimacy of the source.

**03**

Offenders as users

Deepfakes, automated phishing and synthetic identity fraud lower entry barriers and increase scale. AI changes the evidential landscape and the factual patterns that criminal courts must understand.

The judiciary as AI user

RechtspraakGPT and the EU AI Act make judicial AI a governance question, not merely an efficiency question.

Judiciary introduces RechtspraakGPT for its own employees

AI assistant supports employees with non-sensitive tasks outside the judicial domain

The Hague | December 10, 2025

As of today, all employees of the Judiciary can use RechtspraakGPT. This AI assistant helps with, among other things, creating, improving, and summarizing memos, policy papers, presentations, and other documents. RechtspraakGPT is expressly not intended for tasks related to judicial decisions, human resources, confidential documents, or personal data.

AI Act implications

- AI tools used to assist judicial decision-making fall within the EU AI Act's *high-risk* framework.
- For judicial users, AI literacy therefore means knowing both the tool's possibilities and its boundaries.

Source: <https://www.rechtspraak.nl/organisatie-en-contact/organisatie/raad-voor-de-rechtspraak/nieuws/rechtspraak-introduceert-rechtspraakgpt-voor-eigen-medewerkers>

AI output as evidence: the “synthetic expert” problem

Dutch courts are cautious when parties present AI output as if it were an authoritative source.

- AI-generated output as a claim to expertise without the institutional features that normally justify expert authority
- Courts ask whether the output is substantively reliable, whether a responsible human author can account for it, and whether the legal forum recognises the source as legitimate.
- The [Dutch Bar and the CCBE have both issued guidance](#) on responsible AI use in legal practice, stressing that AI may support lawyers but does not reduce their professional responsibility.

Tools embedded in controlled forensic or institutional workflows receive a different assessment. Hansken, ANPR systems and plagiarism tools are treated more favourably because human verification and institutional accountability surround the technology.

<https://www.njb.nl/auteurs/arnoud-engelfriet/>

Lesson from the prompt-and-temperature case

The procedural failure was deeper than a missing technical setting.

A lawyer submitted ChatGPT output in a dispute concerning a business plan. The court asked which prompt had been used and which **temperature setting** applied. The answers exposed that the production could not be reconstructed or verified.

What made the output fragile?

The wrong version of the document had been assessed, procedural materials had been loaded into the conversation, and the model generated legal conclusions aligned with the user's position.

The reliability problem concerned mandate, source selection and adversarial bias.

The practical lesson for courts

AI-based productions need a reproducible record: the documents used, the prompt sequence, the model context, the intended purpose and the human verification performed before submission.

Without that record, the court cannot test probative value.

AI as an instrument of crime

The same technologies that assist legal work also expand criminal capacity.

Deepfake-enabled bank fraud

A pending Amsterdam case concerns the opening of 47 bank accounts in the Netherlands, Belgium and Italy through deepfake technology.

The significance lies in the attack on Know Your Customer controls: identity verification systems long treated as robust can be manipulated at scale when synthetic faces and documents are combined.

RTL Z.

OM: scammer stuck own head on stolen passport and opened bank accounts

Wouter van Dijke · March 17, 2026 · Modified: March 17, 2026

A 34-year-old Amsterdam resident is suspected of opening almost 50 bank accounts at ABN AMRO using deepfakes. Those accounts could then be used for scams or to launder money. Today the suspect was in court.



[Press release of the court](#)

Cybercrime is now mainstream criminal justice

Dutch data shows online criminality as a central volume problem, with a large hidden figure.

2.4m

victims of online
criminality in 2024

15.7%

of the Dutch population
aged 15+

16%

reported to the police

72%

faced cybercrime
attempts in 2025

- Online fraud increased between 2022 and 2024, phishing remains the most visible entry point, and Dutch organisations reported a sharp rise in attacks during 2025.
- The courtroom sees only a selected part of the problem because reporting rates and attribution rates remain low.

Bank-helpdesk fraud and phishing

The legal analysis often turns on where access occurred and which system was actually entered.

Typical factual pattern

A victim is contacted by someone posing as a bank employee, persuaded to install remote-access software such as AnyDesk or TeamViewer, and then loses control over funds. The charges may include fraud, unauthorised access and identity-related offences.

The charging problem

Dutch cybercrime case law stresses the need to distinguish access to the victim's device from access to the digital banking environment. These are separate technical events.

Installing a tool after deception does not automatically establish unauthorised entry into every later system.

1 Victim device

Remote access request accepted

2 Banking app / portal

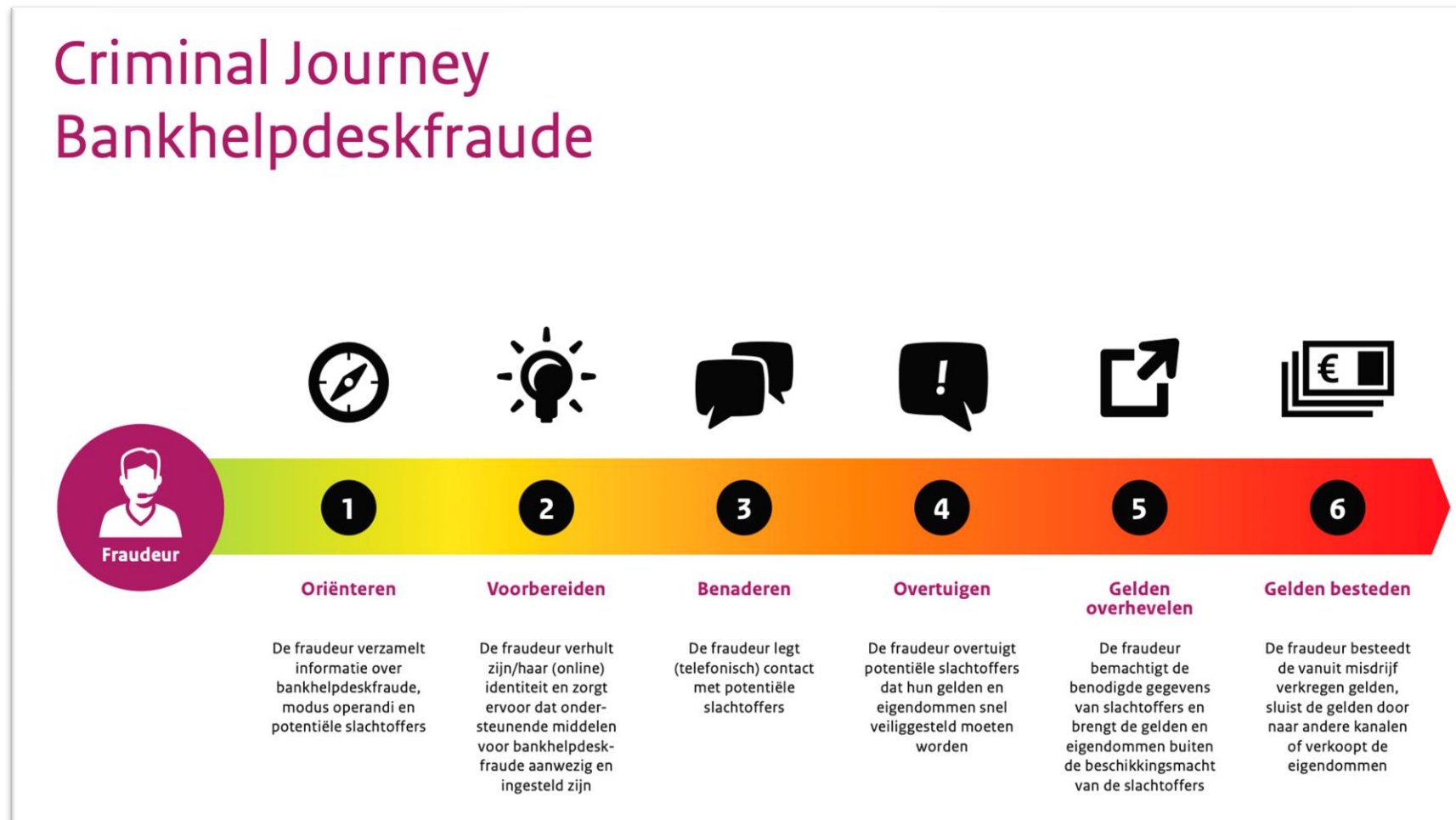
Separate login and transaction layer

3 Funds moved

Fraud loss and laundering trail

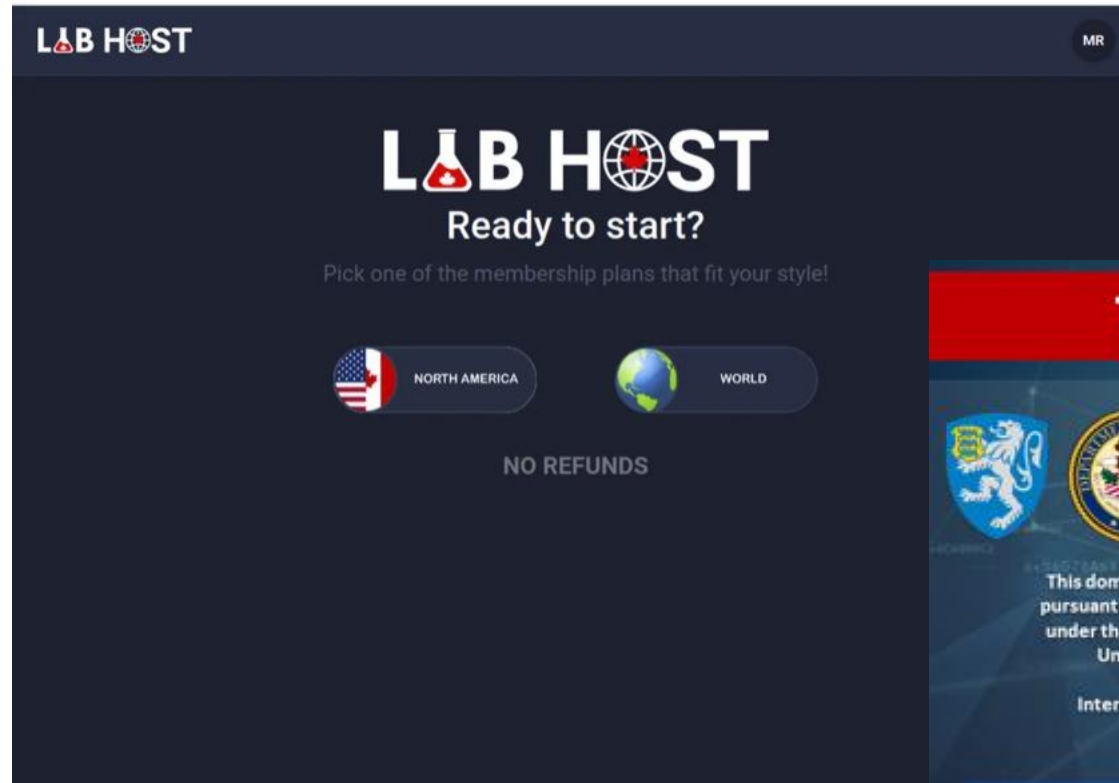
Bank-helpdesk fraud and phishing

The legal analysis often turns on where access occurred and which system was actually entered.



<https://integraleaanpakonlinefraude.nl/attachment/entity/4369dac5-dff9-401b-b948-2cc7c79966e4>

LabHost — Phishing-as-a-Service



LabHost — Phishing-as-a-Service

- LabHost was a global phishing-as-a-service platform offering **ready-made fake websites of banks, public bodies and platforms such as Netflix and Amazon.**
- For a monthly crypto fee, users could collect login details, bank data and credit-card information from victims.
- Operation PhishOFF dismantled the platform in April 2024 through cooperation between the UK, Europol, the FBI, the US Secret Service and 18 jurisdictions.
- The seized LabHost database allowed national authorities, including the Netherlands, to identify users and start prosecutions.
- In November 2025, the District Court of Mid-Netherlands issued the first Dutch conviction of a LabHost user, based on digital evidence linking him to phishing panels, servers, crypto payments and victim data.

[ECLI:NL:RBMNE:2025:5658](#)

Ransomware, doxing and unauthorised access

Cybercrime combines social harm, digital infrastructure and classic criminal-law concepts.

Ransomware and system disruption

Ransomware may paralyse airports, public-sector systems or prosecution services. Liability can combine unauthorised access, extortion and participation in organised criminal activity. The hardest practical issues are attribution, jurisdiction and recovery of infrastructure.

Doxing and physical risk

Article 285d of the Dutch Criminal Code covers obtaining and spreading personal data with the intent to cause fear or serious nuisance.

Online publication of photographs and address details can create immediate physical danger.

Unauthorised access as the workhorse provision

Article 138ab of the Dutch Criminal Code remains central across many cybercrime cases. Precision in the indictment matters: what is the “automated work” for evidential purposes? The device, application, server, cloud account, banking environment, or network infrastructure etc.

Procedural control over digital investigations

Searches of devices and datasets require judicial discipline at the front end of the investigation.

The Landeck line – [C-548/21](#), CJEU

When the extraction or analysis of a smartphone or other digital device creates more than a limited interference with privacy, prior authorisation by an investigating judge becomes central.

In its [judgment of 18 March 2025](#), the Dutch Supreme Court revised its case law on searches of electronic devices after **CG/Landeck**, distinguishing between *limited* and *more than limited* privacy intrusions, with prior judicial review required only for the latter.

Encrypted communication platforms



EncroChat and Sky ECC: operational context

The legal debate is inseparable from the scale of the operations.

EncroChat

A European encrypted-communication network with approximately 50,000 users in early 2020, including around 12,000 in the Netherlands. In operation 26Lemont, French and Dutch authorities used a Joint Investigation Team and a Trojan horse to intercept real-time messages over several weeks.

Estimated 115 million messages intercepted

Sky ECC

A Canadian provider of encrypted smartphones and the Sky ECC application, with about 70,000 users worldwide. Belgian and Dutch services gained live access to messages in 2021, followed by raids, arrests and the dismantling of the network.

Hundreds of arrests and major asset seizures followed

EncroChat & Sky ECC — operationele kerngetallen

Stand juni 2023 (EncroChat) en maart 2021 + 2026 (Sky ECC)

	EncroChat	Sky ECC
Operatiennaam (NL)	26Lemont ¹	26Argus ²
Operatiennaam (FR/EU)	Emma 95 ³	—
Operatiennaam (BE)	—	Operatie Sky ²
Periode interceptie	1 apr — 13 jun 2020 ¹	feb — mrt 2021 (3 wkn live) ⁴
JIT-partners	FR, NL ¹	FR, NL, BE ²
Aantal gebruikers	ca. 60.000 wereldwijd ^{3 5} (12.000 NL)	70.000 abonnees ⁴ 171.000 toestellen
Onderschepte berichten	> 115 miljoen ³	ca. 1 miljard ⁶ (≥ 500 mln ontsleuteld)
Aanhoudingen	6.558 ³ (197 High Value Targets)	honderden NL ² + 888 BE ⁴ (eerste jaar)
Inbeslagname / bevroezing	bijna € 900 miljoen ³	€ 4,5 miljard aan drugs (BE) ⁴
Veroordelingen	7.134 jaar gevangenisstraf ³	honderden strafzaken NL ²
Voorkomen moorden	— ³	114 (Europol) ⁴

¹ HR 14 april 2026, ECLI:NL:HR:2026:650 · ² OM, Distributeurs cryptotelefoons Sky ECC aangehouden, 31 jan 2025 · ³ Europol & Eurojust, persconferentie Lille, 27 juni 2023 · ⁴ VRT Nieuws, 5 jaar na 'kraak van de eeuw', 24 feb 2026 · ⁵ Schermer & Oerlemans, NJB 2023/2611 · ⁶ D. Hiroux, VRT Nieuws, 6 april 2021

EncroChat — drie jaar na de hack

Wat is er in beslag genomen?

VERMOGEN

Cash

€ 739,7 mln

Bevroren tegoeden

€ 154,1 mln

Totaal

€ 900 mln

DRUGS

Cocaïne

103,5 ton

Cannabis

163,4 ton

Heroïne

3,3 ton

Synthetische drugs

30,5 mln pillen

WAPENS & TRANSPORT

Vuurwapens

923

Munitie

21.750 stuks

Explosieven

68

Voertuigen

971

Vaartuigen / vliegtuigen

83 / 40

Onroerend goed

271 panden

Encrypted communication platforms

PGP phones created a new evidential category: massive, intercepted, cross-border conversational datasets.

EncroChat and Sky ECC were designed around secrecy: encrypted messaging, modified devices, remote wiping, disabled hardware features and subscription-based access.

Why this became legally explosive

The operations did not produce a few messages from a single suspect. They generated enormous datasets across many users and jurisdictions.

That scale changed the admissibility discussion: defence lawyers requested access to underlying materials, prosecutors relied on international cooperation, and courts had to define the limits of trust in foreign investigative acts.

The core legal question

How far may a Dutch court rely on evidence obtained through foreign authorities, especially where the defence cannot examine every technical step of the interception?

The discussion involves inter-state trust principle, judicial authorization and the right to a fair trial.

The main defence challenges

The recurring arguments focus on access, legality, fair-trial rights and attribution.

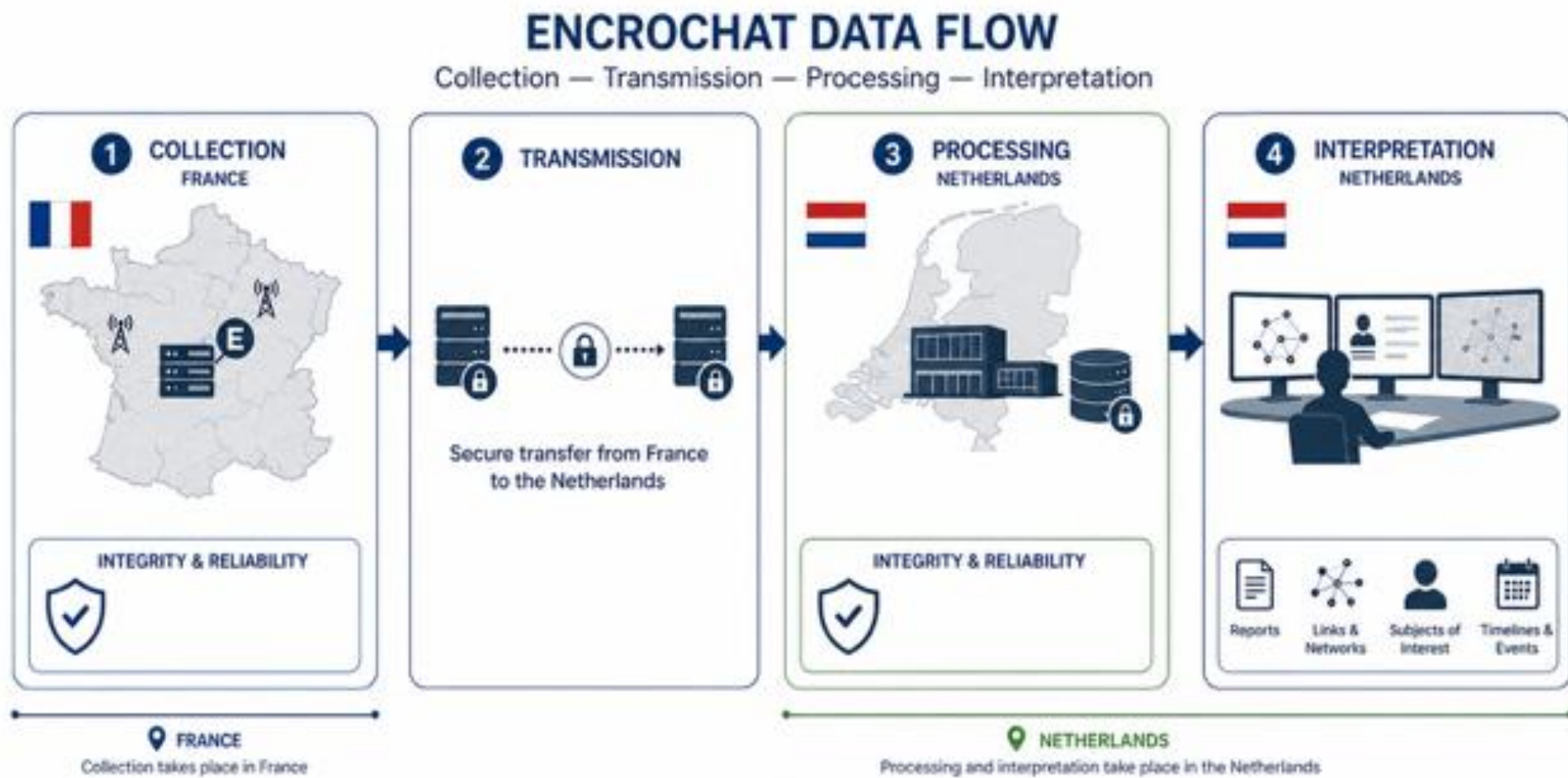
The general defence arguments that EncroChat data should be excluded:

1. it is allegedly **unlawfully obtained and processed**,
2. its **reliability can not be properly verified**, and
3. the defendant lacks **effective legal protection**.

[ECLI:NL:GHSHE:2025:2301](#): the defence wanted the Dutch court to assess the legality and reliability of the data under Dutch law, to clarify whether the interception took place inside or outside the JIT, whether targeted interception was possible, and whether sufficient judicial oversight existed.

[Joint Defense Team – a collaborative network of experienced criminal defence lawyers from several European countries.](#)

Admissibility challenges



Interpretation challenges

Attribution of a specific account to an individual

Interpretation of the content of communications

Identification of communication counterparts and questioning as witnesses

The jurisprudential line

Dutch case law moved from inter-state trust toward a refined EU-law discussion, while preserving the JIT basis.



Hoge Raad 14 April 2026: the central holding

The Supreme Court adjusted the reasoning, yet preserved the admissibility framework for JIT-based EncroChat evidence.

What the defence argued

Relying on the CJEU's 2024 ruling, the defence argued that Article 31 of Directive 2014/41/EU protected individual rights and required further inquiry into the French interception. Requests included raw source data, the Dutch research file and witnesses from the French side, Europol and Eurojust.

What the Supreme Court decided

The Court accepted that Article 31 also protects individuals. It then held that the provision did not govern this evidence because the material was exchanged through a Joint Investigation Team.

Article 3 of the directive excludes JIT exchange from the directive's scope. The March 2020 authorisation by the Dutch investigating judge remained procedurally decisive.

Current position and open issues

The Dutch framework is relatively stable for JIT cases, while other routes remain legally sensitive.

For the majority of Dutch EncroChat cases, the inter-state trust principle, the JIT structure and the investigating judge's authorisation currently sustain admissibility.

Where uncertainty remains

Cases outside the JIT architecture require separate analysis. Where an European Investigation Order was used, the directive applies directly and notification questions under Article 31 may have practical consequences.

Current position and open issues

What to watch

The pending Prudniez reference from the French Cour de cassation may further develop the EU-law dimension. A future CJEU ruling could affect the relationship between notification, individual rights and evidential consequences in encrypted-phone investigations.

C-625/25, Prudniez:

French reference on effective judicial protection in cross-border digital investigations involving Sky ECC.

Pending cases:

Before the CJEU

- **C-564/25, C-565/25 and C-566/25:** Europol liability concerning Sky ECC, EncroChat and Exclu.

Before the ECtHR

- **Silgir vs Germany (no. 27618/21):** Article 5 and Article 8 ECHR issues, concerning liberty and private life.
- **Hoeven vs Netherlands (no. 15038/24) :** Article 6 ECHR issue, concerning the right to a fair trial.

Closing synthesis

Digital criminal justice requires technical literacy, legal precision and visible human responsibility.

1 AI changes authority

Courts must distinguish useful technological assistance from unsupported claims of expertise. Verification and accountability determine legal value.

2 Cybercrime changes volume

Online offending has become a mainstream caseload, with bank fraud, phishing, ransomware, doxing and unauthorised access at the centre of practice.

3 Encrypted-phone cases change procedure

EncroChat and Sky ECC show that admissibility now depends on cross-border cooperation structures, judicial authorisation and control over large datasets.

Questions?



EL PACCTO

2.0

EU-LAC Partnership on
justice and security

ARTIFICIAL INTELLIGENCE AND CRIMINAL NETWORKS: A LINK THAT GOES BEYOND EUROPE

Tallinn, 7-8 May 2026



Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not
necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible
for them.

High Risk Criminal Networks and Artificial Intelligence

ENG

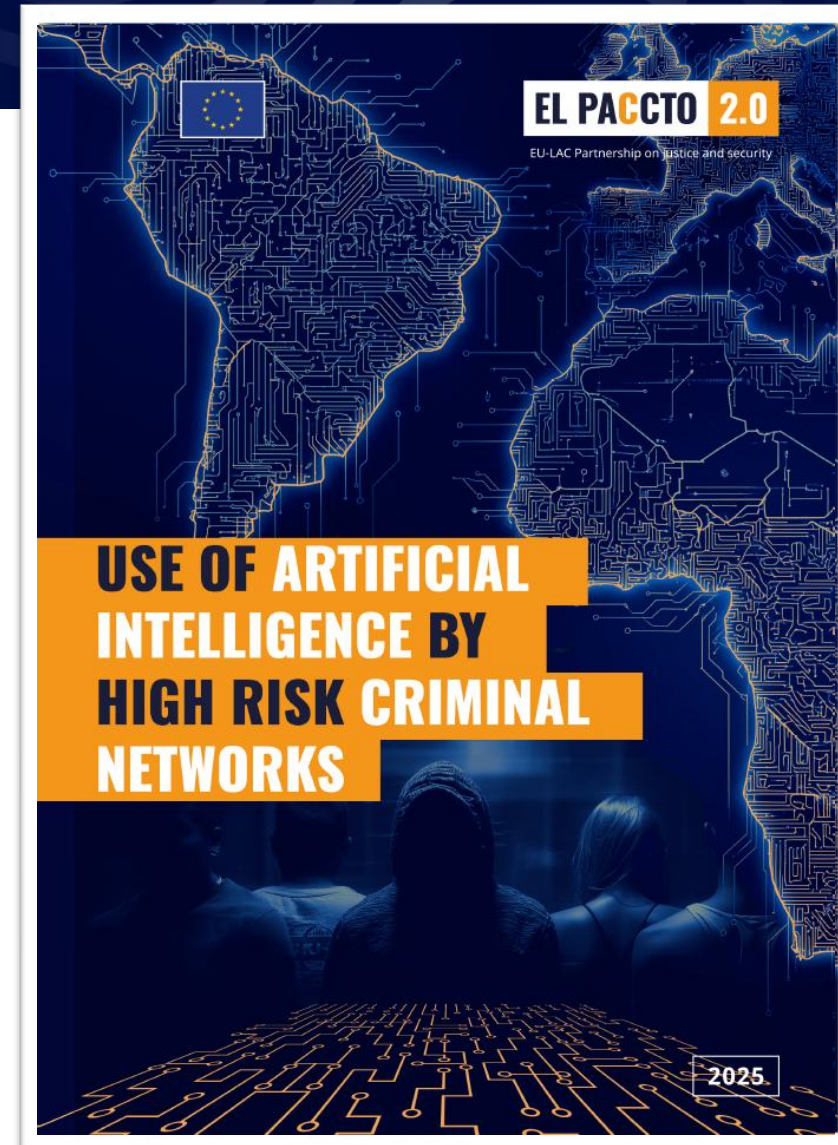


ES



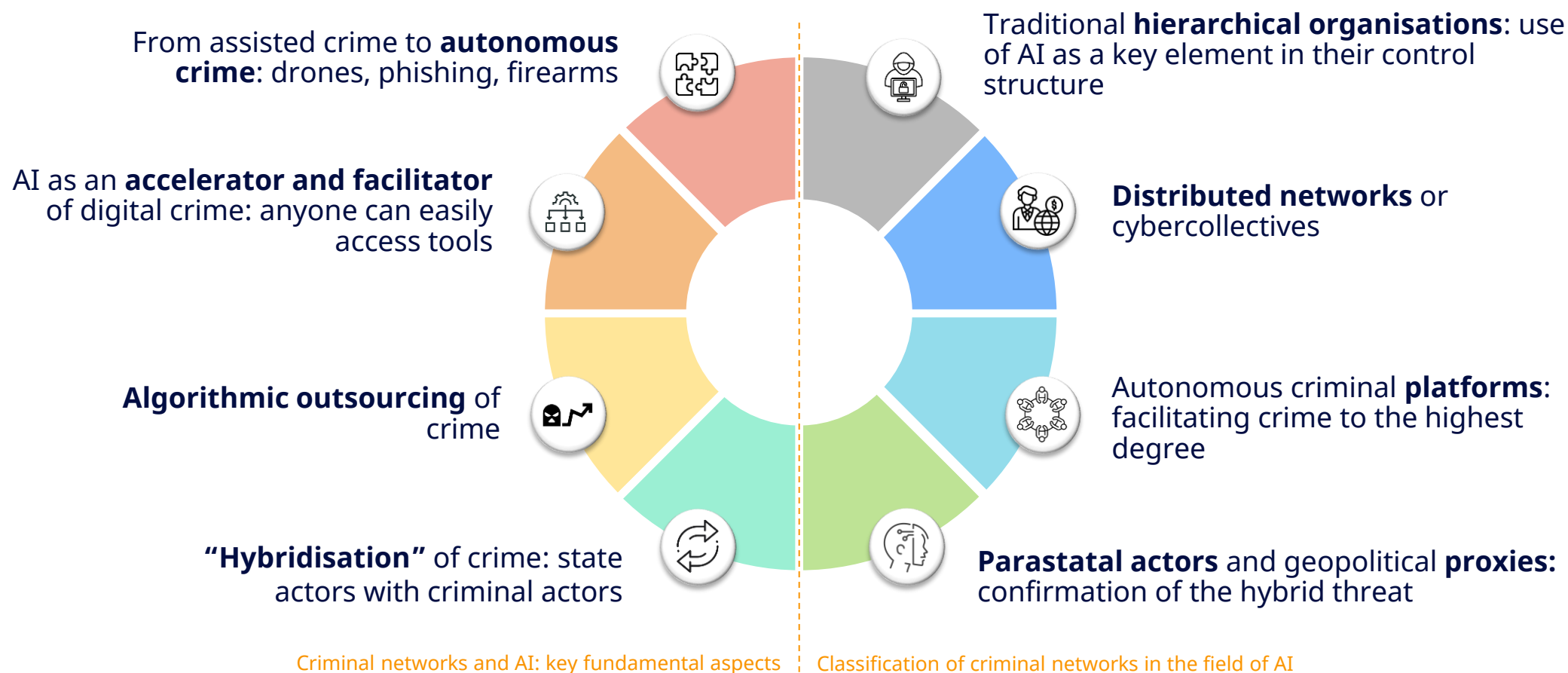
Available at:

<https://doi.org/10.5281/zenodo.16750778>



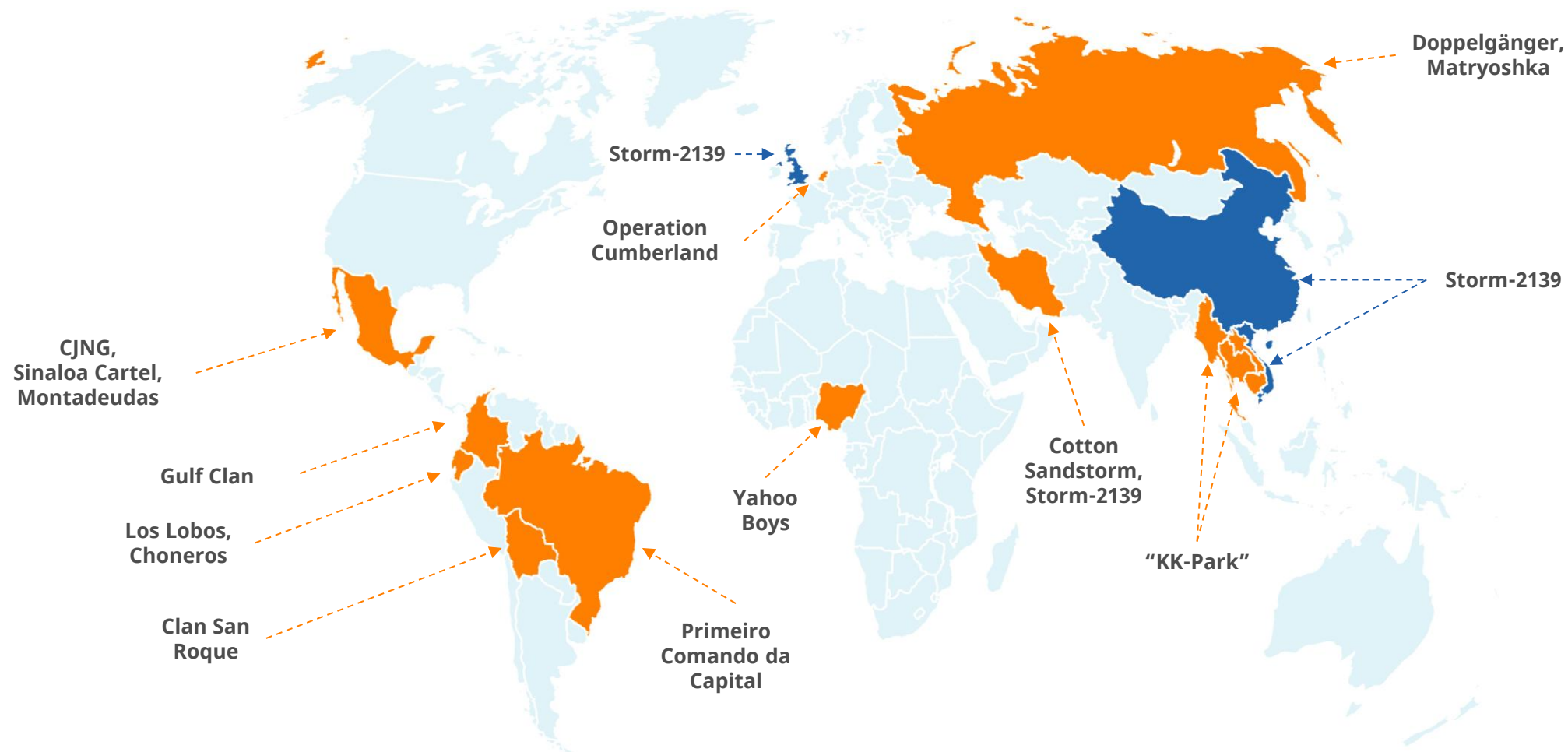


Framework: classification of groups, types of offences





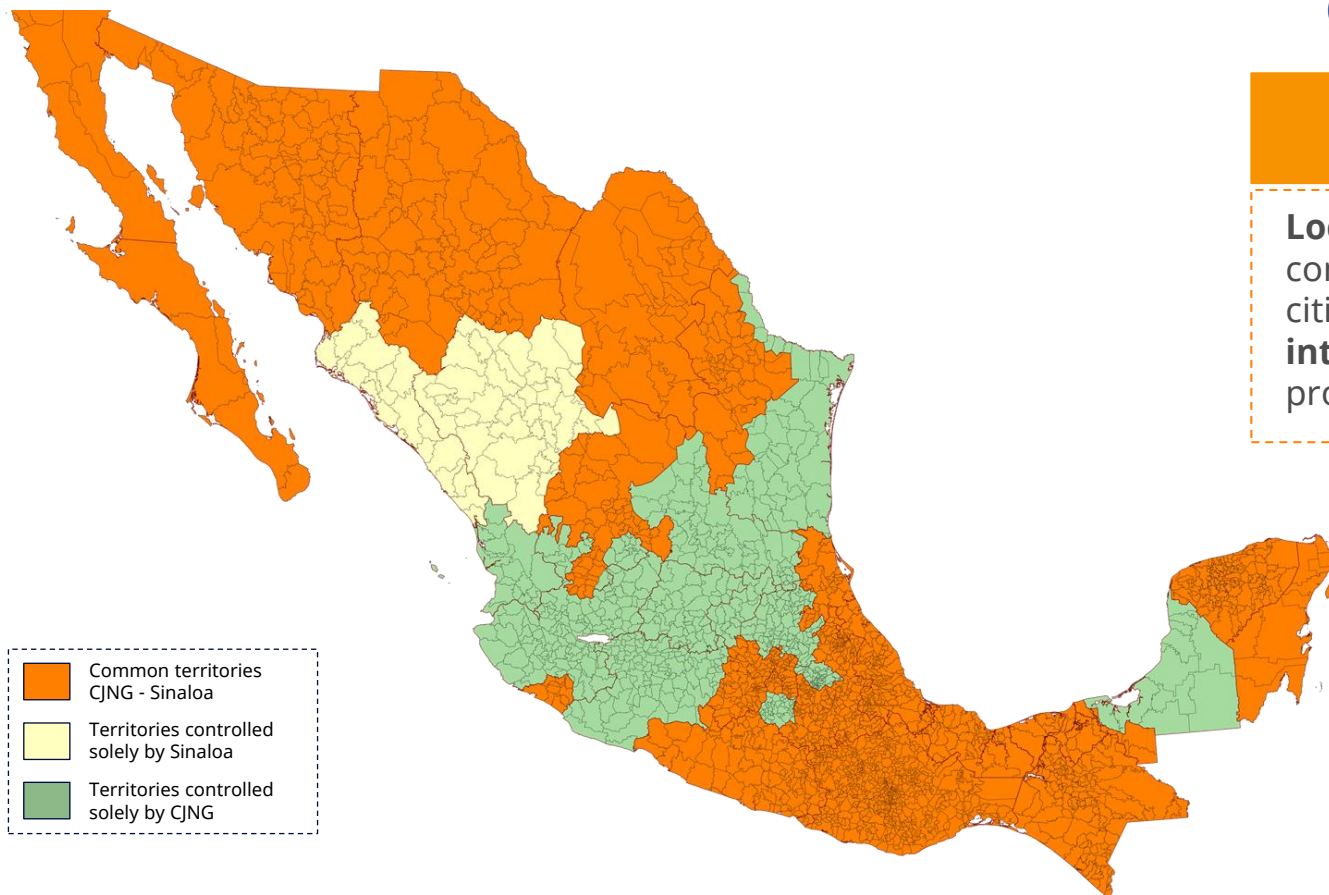
Featured cases: work map





Criminal networks: Traditional hierarchical organisations (I)

Cases: Jalisco New Generation Cartel and Sinaloa Cartel



Special focus

Victims

Local victims (small communities and large cities) and **international**; big profits for cartels

Key features

Technology and crime

Use of **generative AI** for emotional fraud ('pig butchering'), **voice cloning** for extortion and simulated kidnappings, **smishing**, **deepfakes**, and **automated geolocation**

Application of AI in **logistics optimisation** for drug and human trafficking, as well as in **multi-jurisdictional money laundering** schemes

***Los Droneros** (CJNG)



Criminal networks: Traditional hierarchical organisations (II)

Case study: Government action against Jalisco New Generation Cartel boss: Nemesio Oseguera, AKA “El Mencho”



Nemesio Oseguera
alias “El Mencho”

IMPACT

High

CRIMINAL ECONOMIES

- Extortion
- Drug trafficking
- Drug production
- Kidnapping
- Money laundering
- Oil theft

WOMEN IN THEIR RANKS

STATE PENETRATION

CRIMINAL CONNECTIONS WITH EUROPE

AI Uses Technology and crime

Disinformation during his apprehension:

- **200-500 posts** to disinform and create chaos: 25% fully AI-generated, 25% AI-misleading → over 28k times shared
- **Target population:** general population, top Mexican leadership (President Claudia Sheinbaum in hiding)
- Focused on **areas where the cartel holds most of its power**
- **Destabilise the security situation** before the FIFA World Cup
- **Main platforms used:** X, Facebook and WhatsApp and Signal channels

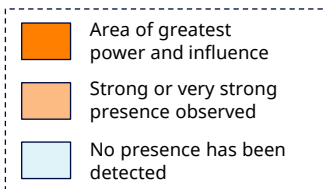
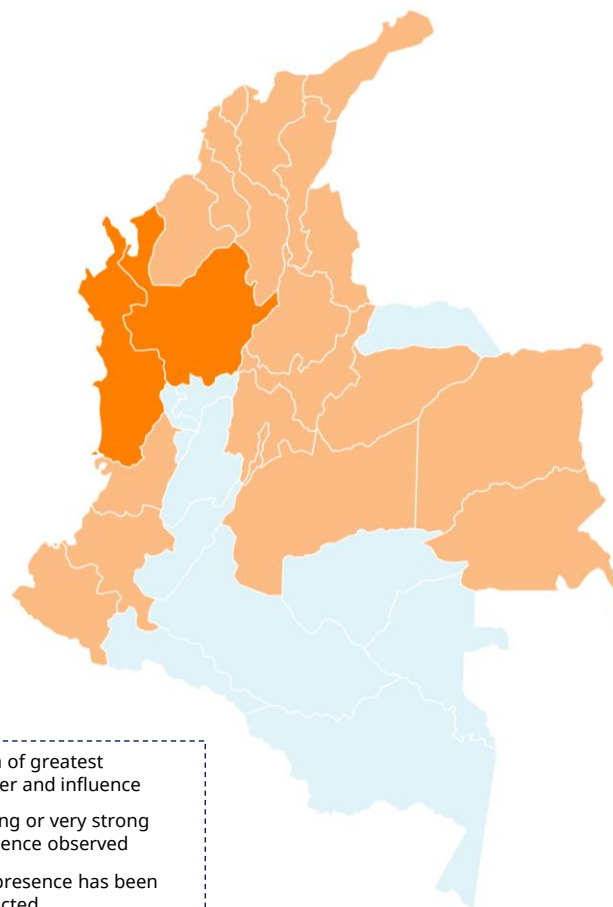




Criminal networks: Traditional hierarchical organisations (III)

Case: Gulf Clan or Gaitanistas

		ORIGIN  Colombia
LEADER (S) Jobanis de Jesús Ávila alias "Chiquito Malo"		
IMPACT High	APPROXIMATE SIZE 7,000 members	
CRIMINAL ECONOMIES - Extortion - Drug trafficking - Illegal mining - Contraband - Migrant smuggling - Loan sharking - Sexual exploitation - Money laundering - Micro trafficking		
 WOMEN IN THEIR RANKS	 STATE PENETRATION	 CRIMINAL CONNECTIONS WITH EUROPE



Key features Technology and crime

Use of **unmanned aerial, aquatic, and underwater autonomous vehicles** for:

- Intelligence, **surveillance** and reconnaissance
- **Drug transport** (air and water/semi-submersible)
- **Explosive launches**, especially in Bolívar and Córdoba
- Between January and August (2025), there were **260 incidents involving explosive drones** (2024 total: 108)

Drones: a **low-cost strategic weapon**

Trends: 1) voice cloning and **synthetic image** production for **extortion** and **fraud**.
2) **Recruitment** (forced or otherwise) of young people and **adolescents**

Criminal networks: Traditional hierarchical organisations (III)

Cases: KK Park “model”

Key features

Technology and crime

Locations: Myanmar, Thailand, Laos, and Cambodia

Industrialised algorithmic fraud complexes: financial scams (*pig butchering*), digital exploitation of victims under modern slavery, transnational deception interfaces

Territorial control, ‘city within a criminal complex’, provision of services, labour and sexual exploitation crimes

Hybrid model of algorithmic criminal governance



Special focus

Victims

Victims deceived around the world;
local and transnational mafias

Victims of **human trafficking** and **smuggling** for labour exploitation



Fuente: Jittrapon Kaicom/The Guardian



Fuente: The Guardian. Google Earth, Aspi



Criminal networks: Distributed networks or cybercollectives



Montadeudas (Mexico)

Networks of fraudulent loan apps that use AI to target victims.

Extortion with deepfakes, automated harassment



Clan San Roque (Bolivia)

Operations centre: the prison system

Crimes: voice cloning (e.g. the Minister of Education) for mass fraud. Use of messaging bots, QR codes for payments, digital mules

Social media to **recruit** victims

Yahoo Boys (Nigeria)

Specialised in **online fraud** powered by **deepfakes** and generative AI, they **simulate identities** for romance and **financial scams**



Op. Cumberland (Netherlands)

Europol investigation into networks producing and distributing **AI-generated child sexual abuse material (CSAM)**. **Decentralised structure**, cryptocurrency payments and exploited legal loopholes



FunkSec (Global)

Cyber collective that combines **hacktivism** and **cybercrime**. Operates **AI-powered** ransomware, reputation sabotage campaigns, and extortion. **No hierarchy:** organised as an AI-based criminal interface



Criminal Networks: Autonomous criminal platforms (Crime-as-a-Service)

Dark LLMs: (WormGPT, FraudGPT, DarkBARD)

Location: worldwide. Exact location unknown

Model based on commercial **jailbreaking** tools

They operate as “services” sold on the **darknet**

Models trained for **fraud, phishing, ransomware, and disinformation**

Darknet users; **criminal clients. Victims** (general or targeted)

Xanthorox AI

Technology, crimes and victims

Location: worldwide. **Private** networks and **servers**

Autonomous cyberattack platform with generative AI. Enables **large-scale targeted attacks** without human intervention. Modular pay-for-use system

Easy purchase of cyberattack **packages and tools.**

Victims: **businesses** and **governments**

Storm-2139

Location, technology, victims

Known locations: China, Iran, United Kingdom and Vietnam

Decentralised autonomous network of cybercriminals producing **real-time deepfakes**, synthetic **CSAM**, and **automated attacks**

Represents the shift towards **autonomous algorithmic crime**



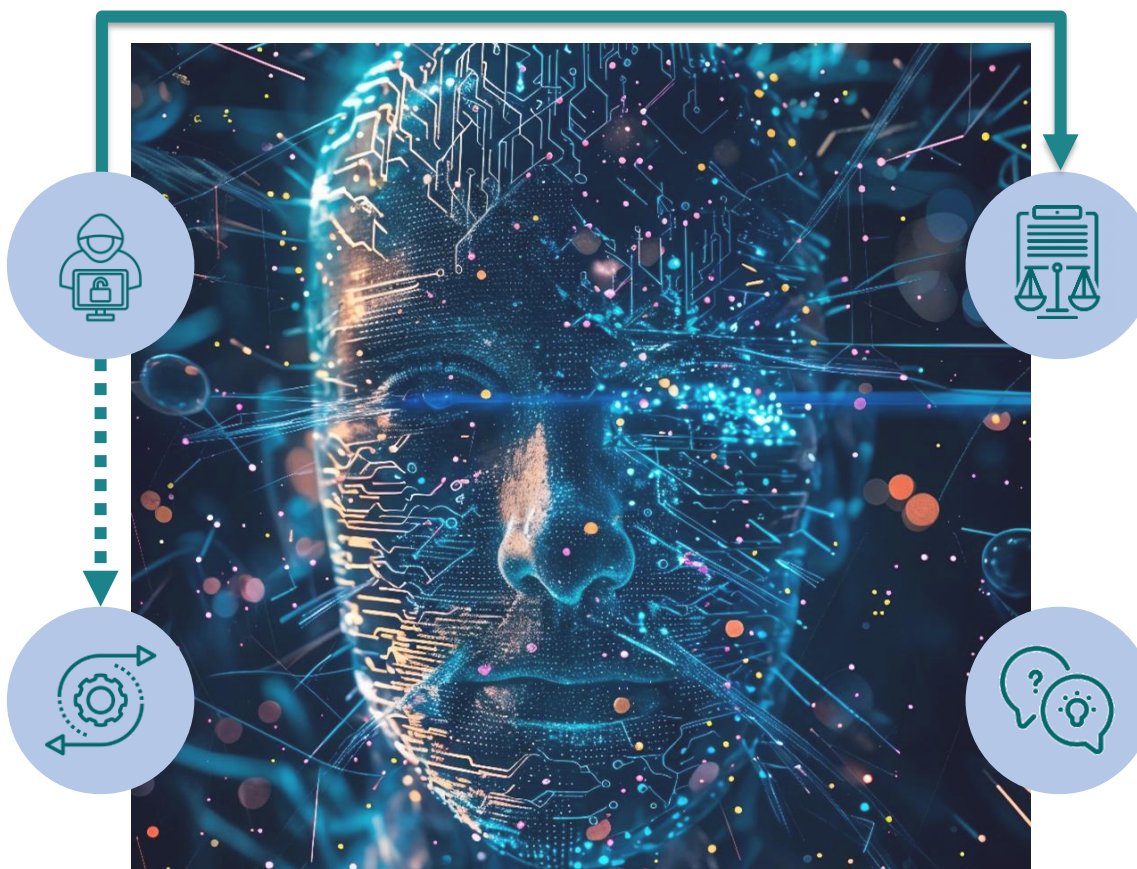
Final considerations and recommendations: AI and HRCN

Criminal groups and networks actively use AI

Sinaloa, CJNG (Operadores Droneros),
Montadeudas, Clan San Roque, Gulf
Cartel-Gaitanistas, PCC, CV

Hybrid threat very much present

Mimicry of technology and ideas seen
in the war in Ukraine in LAC
Crime-as-a-Service: emergence of
multiple tools and offerings to facilitate
crime



Regulatory update: classification and legislation

Clear, specific and evolving regulations. Intelligent regulation. Do we need an international treaty?

International cooperation and institutional support

Raise awareness, train and specialise institutions in the criminal justice system. Promote inter-institutional and international cooperation and collaboration



Funded by
the European Union



EU-LAC Partnership on justice and security

Thank you very
much!

Marc Reina Tortosa
Executive Manager
EL PACCTO 2.0
marc.reina@elpaccto.eu

Implemented by:



Government of the Netherlands

TABLE OF CONTENTS



Co-financed by the European Union

This publication has been produced with the financial support of the Justice Programme of the European Union. The content of this publication reflects only the ERA's view and the Commission is not responsible for any use that may be made of the information it contains.

BACKGROUND DOCUMENTATION

***** All documents are hyperlinked *****

Recent work carried out by the European Union on AI and Digitalisation

1	The European AI ACT Regulation (EU) 2024/1689 of the European Parliament and of the Council 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)	
2	Council Decision (EU) 2023/436 of 14 February 2023 authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence	
3	Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings	
4	Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings	
5	<u>Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation</u>	
6	<u>Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)</u>	
7	<u>Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030</u>	
8	<u>Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, OJ L 166, 11.5.2021.</u>	

9	<u>Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2.0), OJ L 30.4.2024.</u>	
10	<u>European e-Justice Strategy 2024–2028, OJ C/2025/437, 16.1.2025 (ELI: C/2025/437)</u>	

Other EU criminal justice documents

A) The institutional framework for criminal justice in the EU

A1) Main treaties and conventions

A1-01	Protocol (No 36) on Transitional Provisions
A1-02	Statewatch Analysis, "The Third Pillar acquis" after the Treaty of Lisbon enters into force, Professor Steve Peers, University of Essex, Second Version, 1 December 2009
A1-03	Consolidated version of the Treaty on the functioning of the European Union, art. 82-86 (<i>OJ C 326/47; 26.10.2012</i>)
A1-04	Consolidated Version of the Treaty on the European Union, art. 9-20 (<i>OJ C326/13; 26.10.2012</i>)
A1-05	Charter of fundamental rights of the European Union (<i>OJ. C 364/1; 18.12.2000</i>)
A1-06	Explanations relating to the Charter of Fundamental Rights (<i>2007/C 303/02</i>)
A1-07	Convention implementing the Schengen Agreement of 14 June 1985 (<i>OJ L 239; 22.9.2000, P. 19</i>)

A2) Court of Justice of the European Union

A2-01	Court of Justice of the European Union: Presentation of the Court
A2-02	European Parliament Fact Sheets on the European Union: Competences of the Court of Justice of the European Union, April 2023
A2-03	Regulation (EU, Euratom) 2019/629 of the European Parliament and of the Council of 17 April 2019 amending Protocol No 3 on the Statute of the Court of Justice of the European Union, OJ L 111, 17 April 2019
A2-04	Consolidated Version of the Statute of the Court of Justice of the European Union (01 August 2016)
A2-05	Consolidated version of the Rules of Procedure of the Court of Justice (25 September 2012)

A3) European Convention on Human Rights (ECHR)

A3-01	Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 together with additional protocols No. 4, 6, 7, 12 and 13, Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11, 14 and 15, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, Council of Europe
-------	--

A3-02	Guide on the case-law of the European Convention on Human Rights: European Union law in the Court's case-law, Council of Europe, updated on 31 August 2022
A3-03	Case of Grzeda v. Poland (Application no. 43572/18), Strasbourg, 15 March 2022
A3-04	Case of Mihalache v. Romania [GC] (Application no. 54012/10), Strasbourg, 08 July 2019
A3-05	Case of Altay v. Turkey (no. 2) (Application no. 11236/09), Strasbourg, 09 April 2019
A3-06	Case Beuze v. Belgium (Application no. 71409/10), Strasbourg, 09 November 2018
A3-07	Case of Vizgirda v. Slovenia (Application no. 59868/08), Strasbourg, 28 August 2018
A3-08	Case of Şahin Alpay v. Turkey (Application no. 16538/17), Strasbourg, 20 March 2018
A3-09	Grand Chamber Hearing, Beuze v. Belgium [GC] (Application no. 71409/10), Strasbourg, 20 December 2017
A3-10	Case of Blokhin v. Russia (Application no. 47152/06), Judgment European Court of Human Rights, Strasbourg, 23 March 2016
A3-11	Case of A.T. v. Luxembourg (Application no. 30460/13), Judgment European Court of Human Rights, Strasbourg, 09 April 2015
A3-12	Case of Blaj v. Romania (Application no. 36259/04), Judgment European Court of Human Rights, Strasbourg, 08 April 2014
A3-13	Case of Boz v. Turkey (Application no. 7906/05), Judgment European Court of Human Rights, Strasbourg, 01 October 2013 (FR)
A3-14	Case of Pishchalnikov v. Russia (Application no. 7025/04), Judgment European Court of Human Rights, Strasbourg, 24 October 2009
A3-15	Case of Salduz v. Turkey (Application no. 36391/02), Judgment, European Court of Human Rights, Strasbourg, 27 November 2008

A4) Brexit

A4-01	Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (<i>OJ L 149</i> , 30.4.2021)
A4-02	Eurojust: Judicial cooperation in criminal matters between the European Union and the United Kingdom from 1 January 2021, 1 January 2021
A4-03	Draft text of the Agreement on the New Partnership between the European Union and the United Kingdom (UKTF 2020-14), 18 March 2020
A4-04	Draft Working Text for an Agreement on Law enforcement and Judicial Cooperation in Criminal Matters
A4-05	The Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 (2019/742), 28th March 2019
A4-06	Brexit next steps: The European Arrest Warrant, House of Commons, 20 February 2020
A4-07	Brexit next steps: The Court of Justice of the EU and the UK, House of Commons, 7 February 2020
A4-08	The Law Society, "Brexit no deal: Criminal Justice Cooperation", London, September 2019
A4-09	European Commission, Factsheet, „A „No-deal“-Brexit: Police and judicial cooperation”, April 2019

A4-10	CEPS: Criminal Justice and Police Cooperation between the EU and the UK after Brexit: Towards a principled and trust-based partnership, 29 August 2018
A4-11	Policy paper: The future relationship between the United Kingdom and the European Union, 12 July 2018
A4-12	House of Lords, Library Briefing, Proposed UK-EU Security Treaty, London, 23 May 2018
A4-13	HM Government, Technical Note: Security, Law Enforcement and Criminal Justice, May 2018
A4-14	LSE-Blog, Why Britain's habit of cherry-picking criminal justice policy cannot survive Brexit, Auke Williams, London School of Economics and Political Science, 29 March 2018
A4-15	House of Commons, Home Affairs Committee, UK-EU Security Cooperation after Brexit, Fourth Report of Session 2017-19, London, 21 March 2018
A4-16	HM Government, Security, Law Enforcement and Criminal Justice, A future partnership paper
A4-17	European Criminal Law after Brexit, Queen Mary University London, Valsamis Mitsilegas, 2017
A4-18	House of Lords, European Union Committee, Brexit: Judicial oversight of the European Arrest Warrant, 6 th Report of Session 2017-19, London, 27 July 2017
A4-19	House of Commons, Brexit: implications for policing and criminal justice cooperation (24 February 2017)
A4-20	Scottish Parliament Information Centre, Briefing, Brexit: Impact on the Justice System in Scotland, Edinburgh, 27 October 2016

B) Mutual legal assistance

B1) Legal framework

B1-01	Council Act of 16 October 2001 establishing in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2001/C 326/01), (OJ C 326/01; 21.11.2001, P. 1)
B1-02	Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 197/1; 12.7.2000, P. 1)
B1-03	Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the surrender procedure between the Member States of the European Union and Iceland and Norway (OJ L 292, 21.10.2006, p. 2–19)
B1-04	Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 8.XI.2001)
B1-05	Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 17.III.1978)
B1-06	European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 20.IV.1959)
B1-07	Third Additional Protocol to the European Convention on Extradition (Strasbourg, 10.XI.2010)
B1-08	Second Additional Protocol to the European Convention on Extradition (Strasbourg, 17.III.1978)
B1-09	Additional Protocol to the European Convention on Extradition (Strasbourg, 15.X.1975)

B1-10	European Convention on Extradition (<i>Strasbourg, 13.XII.1957</i>)
-------	---

B2) Mutual recognition: the European Arrest Warrant

B2-01	Proposal for a Regulation of the European Parliament and of the Council on the transfer of proceedings in criminal matters, COM/2023/185 final, 5 April 2023
B2-02	European Parliament resolution of 20 January 2021 on the implementation of the European Arrest Warrant and the surrender procedures between Member States (2019/2207(INI)), (<i>OJ C 456, 10.11.2021</i>)
B2-03	Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial (<i>OJ L 81/24; 27.3.2009</i>)
B2-04	Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (<i>OJ L 190/1; 18.7.2002, P. 1</i>)
B2-05	Case law by the Court of Justice of the European Union on the European Arrest Warrant – Overview, Eurojust, 15 March 2020
B2-06	Case C-142/22, OE, Judgment of the Court (Second Chamber), 6 July 2023
B2-07	Case C-699/21, E.D.L., Judgment of the Court (Grand Chamber), 18 April 2023
B2-08	Joined Cases C-514/21 and C-515/21, LU and PH, Judgment of the Court (Fourth Chamber), 23 March 2023
B2-09	Case C-158/21, Puig Gordi and Others, Judgment of the Court (Grand Chamber), 31 January 2023
B2-10	Case C-168/21, Procureur général près la cour d'appel d'Angers, Judgment of the Court (Third Chamber), 14 July 2022
B2-11	Joined Cases C-562/21 PPU and C-563/21 PPU, Openbaar Ministerie (Tribunal établi par la loi dans l'État membre d'émission), Judgment of the Court (Grand Chamber), 22 February 2022
B2-12	Case C-649/19, Spetsializirana prokuratura (Déclaration des droits), Judgement of the Court (Fifth Chamber), 28 January 2021
B2-13	Case C-414/20 PPU, MM, Judgment of the Court (Third Chamber), 13 January 2021
B2-14	Joined Cases C-354/20 PPU and C-412/20 PPU, Openbaar Ministerie (Indépendance de l'autorité judiciaire d'émission), Judgement of the Court (Grand Chamber), 17 December 2020
B2-15	Case C-416/20 PPU, Generalstaatsanwaltschaft Hamburg, Judgement of the Court (Fourth Chamber), 17 December 2020
B2-16	Case C-584/19, A and Others, Judgement of the Court (Grand Chamber), 8 December 2020
B2-17	Case C-510/19, AZ, Judgement of the Court (Grand Chamber), 24 November 2020
B2-18	Case C-717/18, X (European arrest warrant – Double criminality) Judgement of the Court of 3 March 2020
B2-19	Case C-314/18, SF Judgement of the Court of 1 March 2020
B2-20	Joined Cases C-566/19 PPU (JR) and C-626/19 PPU (YC), Opinion of AG Campos Sánchez-Bordona, 26 November 2019
B2-21	Case C-489/19 PPU (NJ), Judgement of the Court (Second Chamber) of 09 October 2019

B2-22	Case 509/18 (PF), Judgement of the Court (Grand Chamber), 27 May 2019
B2-23	Joined Cases C-508/18 (OG) and C-82/19 PPU (PI), Judgement of the Court (Grand Chamber), 24 May 2019
B2-24	The Guardian Press Release: Dutch court blocks extradition of man to 'inhumane' UK prisons, 10 May 2019
B2-25	Case 551/18, IK, Judgement of the Court of 06 December 2018 (First Chamber)
B2-26	CJEU Press Release No 141/18, Judgement in Case C-207/16, Ministerio Fiscal, 2 October 2018
B2-27	CJEU Press Release No 135/18, Judgement in Case C-327/18 PPU RO, 19 September 2019
B2-28	Case C-268/17, AY, Judgement of the Court of 25 July 2018 (Fifth Chamber)
B2-29	Case C-220/18 PPU, ML, Judgement of the Court of 25 July 2018 (First Chamber)
B2-30	Case C-216/18 PPU, LM, Judgement of the Court of 25 July 2018 (Grand Chamber)
B2-31	In Absentia EAW, Background Report on the European Arrest Warrant - The Republic of Poland, Magdalena Jacyna, 01 July 2018
B2-32	Case C-571/17 PPU, Samet Ardic, Judgment of the court of 22 December 2017
B2-33	C-270/17 PPU, Tupikas, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-34	Case C-271/17 PPU, Zdiaszek, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-35	Case C-579/15, Popławski, Judgement of the Court (Fifth Chamber), 29 June 2017
B2-36	Case C-640/15, Vilkas, Judgement of the Court (Third Chamber), 25 January 2017
B2-37	Case C-477/16 PPU, Kovalkovas, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-38	Case C-452/16 PPU, Poltorak, Judgement of the Court (Fourth chamber), 10 November 2016
B2-39	Case C-453/16 PPU, Özçelik, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-40	Case C-294/16 PPU, JZ v Śródmieście, Judgement of the Court (Fourth Chamber), 28 July 2016
B2-41	Case C-241/15 Bob-Dogi, Judgment of the Court (Second Chamber) of 1 June 2016
B2-42	C-108/16 PPU Paweł Dworzecki, Judgment of the Court (Fourth Chamber) of 24 May 2016
B2-43	Cases C-404/15 Pál Aranyosi and C-659/15 PPU Robert Căldăraru, Judgment of 5 April 2016
B2-44	Case C-237/15 PPU Lanigan, Judgment of 16 July 2015 (Grand Chamber)
B2-45	Case C-168/13 PPU <i>Jeremy F / Premier ministre</i> , Judgement of the court (Second Chamber), 30 May 2013
B2-46	Case C-399/11 <i>Stefano Melloni v Ministerio Fiscal</i> , Judgment of of 26 February 2013
B2-47	Case C-396/11 Ciprian Vasile Radu, Judgment of 29 January 2013
B2-48	C-261/09 Mantello, Judgement of 16 November 2010
B2-49	C-123/08 Wolzenburg, Judgement of 6 October 2009
B2-50	C-388/08 Leymann and Pustovarov, Judgement of 1 December 2008
B2-51	C-296/08 Goicoechea, Judgement of 12 August 2008
B2-52	C-66/08 Szymon Kozłowski, Judgement of 17 July 2008

B3) Mutual recognition: freezing and confiscation and asset recovery

B3-01	European Judicial Network (for information on mutual recognition of freezing and confiscation orders, including on competent authorities), 14 December 2020, last reviewed on 24 July 2023
B3-02	Moneyval 64th Plenary Meeting report, Strasbourg, 5 January 2023
B3-03	Proposal for a Directive of the European Parliament and of the Council on asset recovery and confiscation (<i>Brussels, 25.5.2022, COM (2022) 245 final</i>)
B3-04	Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010, (<i>Brussels, 20.7.2021 COM(2021) 421 final</i>)
B3-05	FATF, COVID-19-related Money Laundering and Terrorist Financing Risk and Policy Responses, Paris, 4 May 2020
B3-06	Money-Laundering and COVID-19: Profit and Loss, Vienna, 14 April 2020
B3-07	FATF President Statement – COVID-19 and measures to combat illicit financing, Paris 1 April 2020
B3-08	Moneyval Plenary Meeting report, Strasbourg, 31 January 2020
B3-09	Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019, laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA
B3-10	Commission Delegated Regulation (EU) .../... of 13.2.2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, C(2019) 1326 final
B3-11	Regulation 2018/1805 of the European Parliament and of the Council on the mutual recognition of freezing and confiscation orders, L 303/1, Brussels, 14 November 2018
B3-12	Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, L 284/22
B3-13	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), PE/72/2017/REV/1 OJ L 156, p. 43–74, 19 June 2018
B3-14	Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
B3-15	Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies (Text with EEA relevance)
B3-16	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance)
B3-17	Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Text with EEA relevance)

B3-18	Consolidated text: Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union
B3-19	Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community
B3-20	Council Framework Decision of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (2001/500/JHA)
B3-21	Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA)

B4) Mutual recognition: Convictions

B4-01	Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention (<i>OJ L 294/20; 11.11.2009</i>)
B4-02	Council Framework Decision 2008/947/JHA on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions (<i>OJ L 337/102; 16.12.2008</i>)
B4-03	Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union (<i>OJ L 327/27; 5.12.2008</i>)
B4-04	Council Framework Decision 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings (<i>OJ L 220/32; 15.08.2008</i>)
B4-05	Case C-234/18, Judgment of 20 March 2020
B4-06	Case C-390/16, Dániel Bertold Lada, Opinion of AG Bot, delivered on 06 February 2018
B4-07	Case C-171/16, Trayan Beshkov, Judgement of the Court (Fifth Chamber), 21 September 2017
B4-08	Case C-528/15, Policie ČR, Krajské ředitelství policie Ústeckého kraje, odbor cizinecké policie v Salah Al Chodor, Ajlin Al Chodor, Ajvar Al Chodor, Judgement of the Court (Second Chamber), 15 March 2017
B4-09	Case C-554/14, Ognyanov, Judgement of the Court (Grand Chamber), 8 November 2016
B4-10	Case C-439/16 PPU, Milev, Judgement of the Court (Fourth Chamber), 27 October 2016
B4-11	C-294/16 PPU, JZ v Śródmieście, Judgement of the Court (Fourth Chamber), 28 July 2016
B4-12	C-601/15 PPU, J. N. v Staatssecretaris voor Veiligheid en Justitie, Judgement of the Court (Grand Chamber), 15 February 2016
B4-13	C-474/13, Thi Ly Pham v Stadt Schweinfurt, Amt für Meldewesen und Statistik, Judgement of the Court (Grand Chamber), 17 July 2014
B4-14	Joined Cases C-473/13 and C-514/13, Bero and Bouzalmate, Judgement of the Court (Grand Chamber), 17 July 2014
B4-15	C-146/14 PPU, Bashir Mohamed Ali Mahdi, Judgement of the Court (Third Chamber), 5 June 2014
B4-16	Case C-383/13 PPU, M. G., N. R., Judgement of the Court (Second Chamber), 10 September 2013

B5) Mutual recognition in practice: evidence and e-evidence

B5-01	Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, (OJ L 191, 28.7.2023)
B5-02	Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, (OJ L 191, 28.7.2023)
B5-03	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, (Brussels, 20.7.2021, COM(2021) 409 final)
B5-04	The European Law Blog, „E-Evidence: The way forward. Summary of a Workshop held in Brussels on 25 September 2019, Theodore Christakis, 06 November 2019
B5-05	Joint Note of Eurojust and the European Judicial Network on the Practical Application of the European Investigation Order, June 2019
B5-06	European Commission, Press Release, „Security Union: Commission recommends negotiating international rules for obtaining electronic evidence”, Brussels, 05 February 2019
B5-07	EURCRIM, “The European Commission’s Proposal on Cross Border Access to e-Evidence – Overview and Critical Remarks” by Stanislaw Tosza, Issue 4/2018, pp. 212-219
B5-08	Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, Brussels, 05 February 2019
B5-09	Annex to the Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, Brussels, 05 February 2019
B5-10	Fair Trials, Policy Brief, „The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters”, October 2018
B5-11	ECBA Opinion on European Commission Proposals for: (1) A Regulation on European Production and Preservation Orders for electronic evidence & (2) a Directive for harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, Rapporteurs: Stefanie Schott (Germany), Julian Hayes (United Kingdom)
B5-12	Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final, Strasbourg, 17 April 2018
B5-13	Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Strasbourg, 17 April 2018

B5-14	Non-paper from the Commission services: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward (8 June 2017)
B5-15	Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace (7 December 2016)
B5-16	ENISA 2014 - Electronic evidence - a basic guide for First Responders (Good practice material for CERT first responders)
B5-17	Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130/1; 1.5.2014)
B5-18	Guidelines on Digital Forensic Procedures for OLAF Staff" (Ref. Ares(2013)3769761 - 19/12/2013, 1 January 2014
B5-19	ACPO Good Practice Guide for Digital Evidence (March 2012)
B5-20	Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (OJ L, 350/72, 30.12.2008)
B5-21	Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ L 196/45; 2.8.2003)
B5-22	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (Official Journal L 178/1, 17.7.2000)
B5-23	Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions ensuring security and trust in electronic communication - Towards a European Framework for Digital Signatures and Encryption (COM (97) 503), October 1997

B6) Criminal records, Interoperability

B6-01	Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726) (OJ L135/85, 22.05.2019)
B6-02	Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135/85, 22.05.2019)
B6-03	Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135/27, 22.05.2019)
B6-04	Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records

	Information System (ECRIS), and replacing Council Decision 2009/316/JHA, PE-CONS 87/1/18, Strasbourg, 17 April 2019
B6-05	Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States. (COM/2017/0341 final, 29.06.2017)
B6-06	Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93/23; 07.4.2009)
B6-07	Council Decision on the exchange of information extracted from criminal records – Manual of Procedure (6397/5/06 REV 5; 15.1.2007)
B6-08	Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record (OJ L 322/33; 9.12.2005)

B7) Conflicts of jurisdiction – *Ne bis in idem*

B7-01	Case law by the Court of Justice of the European Union on the principle of ne bis in idem in criminal matters, Eurojust, April 2020 Case-law by the Court of Justice of the European Union on the Principle of ne bis in idem in Criminal Matters, Eurojust, December 2021
B7-02	Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (OJ L 328/42; 15.12.2009, P.42)
B7-03	European Convention on the Transfer of Proceedings in Criminal Matters (Strasbourg, 15.V.1972)

C) Procedural guarantees in the EU

C-01	Report from the Commission to the European Parliament and the Council on the implementation of Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, COM/2023/44 final, 1 February 2023
C-02	Commission Recommendation (EU) 2023/681 of 8 December 2022 on procedural rights of suspects and accused persons subject to pre-trial detention and on material detention conditions, (OJ L 86, 24.3.2023)
C-03	FRA Report, Presumption of innocence and related rights – Professional perspectives, Luxembourg, 31 March 2021
C-04	FRA Report, Rights in practice: Access to a lawyer and procedural rights in criminal and European Arrest Warrant proceedings, Luxembourg, 27 September 2019
C-05	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third person informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, COM/2019/560 final, 26 September 2019
C-06	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and

	translation in criminal proceedings, COM/2018/857 final, 18 December 2018
C-07	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, COM/2018/858 final, 18 December 2018
C-08	Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings (OJ L 297/1, 4.11.2016)
C-09	Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings (OJ L 132 1; 21.5.2016)
C-10	Directive 2016/343 of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings (11.3.2016; OJ L 65/1)
C-11	Directive 2013/48/EU of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ L 294/1; 6.11.2013)
C-12	Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (1.6.2012; OJ L 142/1)
C-13	Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings (OJ L 280/1; 26.10.2010)
C-14	C-209/22 - Rayonna prokuratura Lovech, TO Lukovit (Fouille corporelle), 7 September 2023
C-15	C-660/21 - K.B. and F.S. (Relevé d'office dans le domaine pénal), 22 June 2023
C-16	C-430/22, C-468/22 - VB (Information du condamné par défaut), 8 June 2023
C-17	C-608/21 - Politseyski organ pri 02 RU SDVR, 25 May 2023
C-18	C-694/20 - Orde van Vlaamse Balies i in., 8 December 2022
C-19	C-348/21 - HYA and Others (Impossibilité d'interroger les témoins à charge), 8 December 2022
C-20	C-347/21 - DD (Réitération de l'audition d'un témoin), 15 September 2022
C-21	C-242/22 PPU - TL () and de traduction), 1 August 2022
C-22	C-564/19 - IS (Illégalité de l'ordonnance de renvoi), 23 November 2021
C-23	C-282/20 - ZX (Régularisation de l'acte d'accusation), 21 October 2021
C-24	C-649/19 - Spetsializirana prokuratura (Déclaration des droits), 28 January 2021
C-25	Case C-659/18, Judgement of the Court of 2 March 2020
C-26	Case C-688/18, Judgement of the Court of 3 February 2020
C-27	Case C467/18, Rayonna prokuratura Lom, Judgment of the Court of 19 September 2019
C-28	Case C-467/18 on directive 2013/48/EU on the right of access to a lawyer in criminal proceedings, EP, Judgement of the court (Third Chamber), 19. September 2019
C-29	Case C377/18, AH a. o., Judgment of the Court of 05 September 2019

C-30	Case C-646/17 on directive 2012/13/EU on the right to information in criminal proceedings, Gianluca Moro, Judgement of the Court (First Chamber), 13 June 2019
C-31	Case C-8/19 PPU, criminal proceedings against RH (presumption of innocence), Decision of the Court (First Chamber), 12. February 2019
C-32	Case C646/17, Gianluca Moro, Opinion of the AG Bobek, 05 February 2019
C-33	Case C-551/18 PPU, IK, Judgment of the Court (First Chamber), 6 December 2018
C-34	Case C-327/18 PPU, RO, Judgment of 19 September 2018 (First Chamber)
C-35	Case C-268/17, AY, Judgment of the Court (Fifth Chamber), 25 July 2018
C-36	Case C-216/18 PPU, LM, Judgment of 25 July 2018 (Grand Chamber)
C-37	Joined Cases C-124/16, C-188/16 and C-213/16 on Directive 2012/13/EU on the right to information in criminal proceedings Ianos Tranca, Tanja Reiter and Ionel Oprea, Judgment of 22 March 2017 (Fifth Chamber)
C-38	Case C-439/16 PPU, Emil Milev (presumption of innocence), Judgment of the Court (Fourth Chamber), 27 October 2016
C-39	Case C-278/16 Frank Sleutjes ("essential document" under Article 3 of Directive 2010/64), Judgment of 12 October 2017 (Fifth Chamber)
C-40	C-25/15, István Balogh, Judgment of 9 June 2016 (Fifth Chamber)
C-41	Opinion of Advocate General Sharpston, delivered on 10 March 2016, Case C543/14
C-42	C-216/14 Covaci, Judgment of 15 October 2015 (First Chamber)

D) Approximating criminal law and Victims' Rights

D1) Terrorism

D1-01	EU Centre of Expertise for Victims of Terrorism
D1-02	EU's Counter-Terrorism Coordinator
D1-03	Eurojust Meeting on Counter-Terrorism, 16-17 November 2022, Summary of Discussions, 05 April 2023
D1-04	Eurojust Casework on Counter-Terrorism: Insights 2020 – 2021, December 2021
D1-05	Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance), (OJ L 172, 17.5.2021)
D1-06	European Commission, EU Handbook on Victims of Terrorism, January 2021
D1-07	2019 Eurojust Report on Counter- Terrorism, 09 December 2020
D1-08	Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, 9 December 2020, COM(2020) 795 final
D1-09	Report from the Commission to the European Parliament and the Council based on Article 29(1) of Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, COM(2020) 619 final, Brussels, 30 September 2020
D1-10	Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social

	Committee and the Committee of the Regions on the EU Security Union Strategy, 24 July 2020, <i>(COM (2020) 605 final)</i>
D1-11	Council Conclusions on EU External Action on Preventing and Countering Terrorism and Violent Extremism, Brussels, 16 June 2020
D1-12	Terrorism Situation and Trend Report (TE-SAT) 2019
D1-13	Communication from the Commission to the European Parliament, the European Council and the Council, Twentieth Progress Report towards an effective and genuine Security Union, COM(2019) 552 final, Brussels, 30 October 2019
D1-14	Communication from the Commission to the European Parliament, and the Council, Towards better Implementation of the EU's anti-money laundering and countering the financing of terrorism framework, COM(2019) 360 final, Brussels, 24 July 2019
D1-15	Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, L 123/18
D1-16	Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 amending Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries, L 125/4 (Text with EEA relevance)
D1-17	Council Decision (CFSP) 2019/25 of 08 January 2019 updating the list of persons, groups and entities subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism and repealing Decision (CFSP) 2016/1136, Brussels, 08 January 2019
D1-18	Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, 12.9.2018, <i>(COM(2018) 640 final)</i>
D1-19	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), <i>(OJ L 156, 19.6.2018)</i>
D1-20	Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327/20; 9.12.2017)
D1-21	Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88/6)
D1-22	Council Decision (CFSP) 2016/1693 of 20 September 2016 concerning restrictive measures against ISIL (Da'esh) and Al-Qaeda and persons, groups, undertakings and entities associated with them and repealing Common Position 2002/402/CFSP, <i>(OJ L 255, 21.9.2016)</i>

D1-23	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119/132; 4.5.2016)
D1-24	Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism, (OJ L 344, 28.12.2001)

D2) Trafficking in Human Beings, Migrant Smuggling and Sexual Exploitation of Children

D2-01	European Parliament Briefing: Preventing and combating trafficking in human beings, June 2023
D2-02	European Parliament Briefing: Anti-trafficking in human beings, June 2023
D2-03	European Parliament resolution of 15 September 2022 on human rights violations in the context of the forced deportation of Ukrainian civilians to and the forced adoption of Ukrainian children in Russia (2022/2825(RSP)), (OJ C 125, 5.4.2023)
D2-04	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, (COM/2022/732 final, 19 December 2022)
D2-05	Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions report on the progress made in the fight against trafficking in human beings (Fourth Report), (COM/2022/736 final, 19 December 2022)
D2-06	Commission Staff Working Document Impact Assessment Report accompanying the document Proposal for a Directive of the European Parliament and of the Council amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, (SWD/2022/425 final, 19 December 2022)
D2-07	European Parliament resolution of 5 May 2022 on the impact of the war against Ukraine on women (2022/2633(RSP)), (OJ C 465, 6.12.2022)
D2-08	European Parliament At Glance: Russia's war on Ukraine: The risk of trafficking of human beings, May 2022
D2-09	Commission Staff Working Document Evaluation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support, and protection of victims of crime, and replacing Council Framework Decision (2001/220/JHA, SWD/2022/0179 final, 2022)
D2-10	European Migrant Smuggling Centre 6th Annual Report – 2022
D2-11	Europol: The challenges of countering human trafficking in the digital era, As of 6 December 2021
D2-12	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on the application of Directive 2009/52/EC of 18 June 2009 providing for minimum standards on sanctions and measures against employers of illegally staying third-country nationals, (COM/2021/592 final, 29 September 2021)
D2-13	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025, (COM/2021/171 final, 14 April 2021)

D2-14	Eurojust Report on Trafficking in Human Beings, Best practice and issues in judicial cooperation, February 2021
D2-15	Report from the European Commission to the European Parliament and the Council, Third report on the progress made in the fight against trafficking in human beings (2020) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, (COM(2020) 661 final, Brussels, 20 October 2020)
D2-16	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a New Pact on Migration and Asylum, (COM (2020) 609 final, 23 September 2020)
D2-17	European Commission, Study on Data collection on Trafficking in Human Beings in the EU, September 2020
D2-18	Regulation of the European Parliament and of the Council amending Regulation (EC) No 810/2009 establishing a Community Code on Visas (Visa Code), PE-CONS 29/19, Brussels, 15 May 2019
D2-19	European Migrant Smuggling Centre - EMSC
D2-20	European Migrant Smuggling Centre – 4th Annual Activity Report, The Hague, 15 May 2020
D2-21	Report from the European Commission to the European Parliament and the Council, Second report on the progress made in the fight against trafficking in human beings (2018) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, COM(2018) 777 final, Brussels, 03 December 2018
D2-22	European Institute for Gender Equality (EIGE) report: Gender-specific measures in anti-trafficking actions, 17 October 2018
D2-23	UNODC – Global Study on Smuggling of Migrants 2018, Vienna/New York, June 2018
D2-24	Council Conclusions on setting the EU's priorities for the fight against organised and serious international crime between 2018 and 2021, Brussels, 9450/17, 19 May 2017
D2-25	Directive 2011/36/EU of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA

D3) Cybercrime

D3-01	Internet Organised Crime Threat Assessment (IOCTA) 2023
D3-02	European Parliament Legislative Train Schedule: Horizontal cybersecurity requirements for products with digital elements in “A Europe Fit for the Digital Age”, As of 20 September 2023
D3-03	European Parliament Legislative Train Schedule: Review of the Directive on security of network and information systems in “A Europe Fit for the Digital Age”, As of 20 September 2023
D3-04	European Parliament Legislative Train Schedule: Digital operational resilience for the financial sector in “A Europe Fit for the Digital Age”, As of 20 September 2023
D3-05	European Parliament Briefing: EU cyber-resilience act, May 2023
D3-06	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), (OJ L 333, 27.12.2022)
D3-07	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector

	and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance), (<i>OJ L 333, 27.12.2022</i>)
D3-08	Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance), (<i>OJ L 333, 27.12.2022</i>)
D3-09	Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, (<i>COM/2022/454 final, 15 September 2022</i>)
D3-10	Internet Organised Crime Threat Assessment (IOCTA) 2021
D3-11	Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (Text with EEA relevance), (<i>OJ L 274, 30.7.2021</i>)
D3-12	European Commission, Public consultation on Fighting child sexual abuse: detection, removal and reporting of illegal content online, 11 February 2021
D3-13	European Judicial Cybercrime Network 9th Plenary Meeting - 2nd Outcome report 2020, 27 January 2021
D3-14	European Commission, Study on the retention of electronic communications non-content data for law enforcement purposes, Final report, September 2020
D3-15	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: EU strategy for a more effective fight against child sexual abuse, (<i>COM (2020) 607 final, Brussels, 24 July 2020</i>)
D3-16	Internet Organised Crime Threat Assessment (IOCTA) 2020
D3-17	Internet Organised Crime Threat Assessment (IOCTA) 2019
D3-18	Special Eurobarometer 480, Report, "Europeans' Attitudes towards Internet Security", Brussels, March 2019
D3-19	Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Official Journal L 218/8 of 14.08.2013)
D3-20	Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA (<i>OJ L 335; 17.12.2011</i>)
D3-21	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (<i>OJ L 69/67; 16.3.2005</i>)
D3-22	Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography (<i>OJ L 13/44; 20.1.2004</i>)
D3-23	Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Strasbourg, 28.1.2003)
D3-24	Convention on Cybercrime (Budapest, 23.XI.2001)

D4) Protecting Victims' Rights

D4-01	Proposal for a Directive of the European Parliament and of the Council amending Directive 2012/29/EU establishing minimum standards on the rights, support, and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA (<i>COM/2023/424 final, 12 July 2023</i>)
-------	---

D4-02	Commission Staff Working Document: Evaluation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support, and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA (<i>SWD/2022/0179 final, 28 June 2022</i>)
D4-03	FRA Report: "Underpinning victims' rights: support services, reporting and protection", 22 February 2023
D4-04	Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence (<i>COM/2022/105 final, 8 March 2022</i>)
D4-05	D4-01 Victim Support Europe, Paper: Victim Support and Data Protection, 1st March 2021
D4-06	European Union Agency for Fundamental Rights (FRA), Report: Crime, safety, and victims' rights – Fundamental Rights Survey, 19 February 2021
D4-07	European Commission, EU Strategy on victims' rights (2020-2025), COM (2020) 258 final, Brussels, 24 June 2020
D4-08	Factsheet – EU Strategy on Victims' Rights (2020-2025), 24 June 2020
D4-09	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support, and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA (<i>COM/2020/188 final, 11 May 2020</i>)
D4-10	European Commission, Executive Summary of the Report on strengthening Victims' Rights: From Compensation to Reparation – For a new EU Victims' Rights Strategy 2020-2025, Report of the Special Adviser Joëlle Milquet to the President of the European Commission, Brussels, 11 March 2019
D4-11	European Commission Factsheet: The Victims' Rights Directive: What does it bring?, February 2017
D4-12	Regulation (EU) No 606/2013 of the European Parliament and of the Council of 12 June 2013 on mutual recognition of protection measures in civil matters
D4-13	European Commission, DG Justice Guidance Document related to the transposition and implementation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA
D4-14	Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA
D4-15	Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order
D4-16	Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims
D4-17	Website of the European Union Agency for Fundamental Rights (FRA) – Victims' rights
D4-18	Victim Support Europe
D4-19	European Commission: Victims' Rights Platform
D4-20	EC Coordinator for victims' rights

E) Criminal justice bodies and networks

E1) European Judicial Network

E1-01	European Judicial Network, The Report on activities and management 2019-20
E1-02	Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (<i>OJ L 348/130, 24.12.2008, P. 130</i>)

E2) Eurojust

E2-01	Eurojust quarterly newsletter
E2-02	Eurojust Guidelines on Jurisdiction
E2-03	Working Arrangement Between The European Anti-fraud Office And the European Union Agency for Criminal Justice Cooperation, 29 March 2023
E2-04	Eurojust Annual Report 2022
E2-05	Eurojust collection of anniversary essays, 20 years of Eurojust: EU judicial cooperation in the making, 8 August 2022
E2-06	Regulation (EU) 2022/838 of the European Parliament and of the Council of 30 May 2022 amending Regulation (EU) 2018/1727 as regards the preservation, analysis and storage at Eurojust of evidence relating to genocide, crimes against humanity, war crimes and related criminal offences (<i>OJ L 148, 31.5.2022</i>)
E2-07	Guidelines for deciding on competing requests for surrender and extradition, October 2019
E2-08	Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA

E3) Europol

E3-01	Europol Spotlight Series
E3-02	Europol Joint Reports
E3-03	Europol Consolidated Annual Activity Report (CAAR) 2022, 7 June 2023
E3-04	Europol Strategy: DELIVERING SECURITY IN PARTNERSHIP, 6 June 2023
E3-05	The European Union Agency for Law Enforcement Cooperation in Brief, 17 January 2023
E3-06	Europol Programming Document 2023 – 2025, Europol Public Information The Hague, 20 December 2022
E3-07	Case T-578/22: Action brought on 16 September 2022 — EDPS v Parliament and Council, (<i>OJ C 424, 7.11.2022</i>)
E3-08	Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, (<i>OJ L 169, 27.6.2022</i>)
E3-09	Europol Report – Beyond the Pandemic – How COVID-19 will shape the serious and organised crime landscape in the EU, 30 April 2020
E3-10	Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA

E4) European Public Prosecutor's Office

E4-01	EPPO: Internal Rules of Procedure, 29 June 2022
E4-02	Commission Implementing Regulation (EU) 2022/1504 of 6 April 2022 laying down detailed rules for the application of Council Regulation (EU) No 904/2010 as regards the creation of a central electronic system of payment information (CESOP) to combat VAT fraud, (OJ L 235, 12.9.2022)
E4-03	Commission Implementing Decision (EU) 2021/856 of 25 May 2021 determining the date on which the European Public Prosecutor's Office assumes its investigative and prosecutorial tasks, (OJ L 188, 28.5.2021)
E4-04	Working Arrangement between Eurojust and EPPO, 2021/00064, February 2021
E4-05	Working Arrangement establishing cooperative relations between the European Public Prosecutor's Office and the European Union Agency for Law Enforcement Cooperation, January 2021
E4-06	Regulation (EU, Euratom) 2020/2223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013, as regards cooperation with the European Public Prosecutor's Office and the effectiveness of the European Anti-Fraud Office investigations, (OJ L 437, 28.12.2020)
E4-07	Commission Delegated Regulation (EU) 2020/2153 of 14 October 2020 amending Council Regulation (EU) 2017/1939 as regards the categories of operational personal data and the categories of data subjects whose operational personal data may be processed in the index of case files by the European Public Prosecutor's Office, (OJ L 431, 21.12.2020)
E4-08	Council Implementing Decision (EU) 2020/1117 of 27 July 2020 appointing the European Prosecutors of the European Public Prosecutor's Office, (OJ L 244, 29.7.2020)
E4-09	Decision 2019/1798 of the European Parliament and of the Council of 14 October 2019 appointing the European Chief Prosecutor of the European Public Prosecutor's Office (OJ L 274/1, 28.10.2019)
E4-10	Opinion on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 883/2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) as regards cooperation with the European Public Prosecutor's Office and the effectiveness of OLAF investigations Committee on Civil Liberties, Justice and Home Affairs, Rapporteur for opinion: Monica Macovei, 11.1.2019
E4-11	German Judges' Association: Opinion on the European Commission's initiative to extend the jurisdiction of the European Public Prosecutor's Office to include cross-border terrorist offences, December 2018 (only available in German)
E4-12	Communication from the Commission to the European Parliament and the European Council: A Europe that protects: an initiative to extend the competences of the European Public Prosecutor's Office to cross-border terrorist crimes, Brussels, 12.9.2018, COM(2018) 641 final
E4-13	Annex to the Communication from the Commission to the European Parliament and the European Council: A Europe that protects: an initiative to extend the competences of the European Public Prosecutor's Office to cross-border terrorist crimes, Brussels, 12.9.2018, COM (2018) 641 final
E4-14	Council Implementing Decision (EU) 2018/1696 of 13 July 2018 on the operating rules of the selection panel provided for in Article 14(3) of Regulation (EU) 2017/1939 implementing Enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')

E4-15	Annex to the Proposal for a Council Implementing Decision on the operating rules of the selection panel provided for in Article 14(3) of Regulation (EU) 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ("the EPPO"), Brussels, 25.5.2018, COM(2018) 318 final)
E4-16	Csonka P, Juszczak A and Sason E, 'The Establishment of the European Public Prosecutor's Office : The Road from Vision to Reality', Euclid - The European Criminal Law Associations' Forum, 15 January 2018
E4-17	Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')
E4-18	Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law, (OJ L 198, 28.7.2017)

F) Data Protection

F-01	European Data Protection Board (EDPB)
F-02	European Data Protection Supervisor (EDPS)
F-03	Proposal for a Regulation of the European Parliament and of the Council amending Council Decision 2009/917/JHA, as regards its alignment with Union rules on the protection of personal data (COM/2023/244 final, 11.5.2023)
F-04	Directive (EU) 2022/228 of the European Parliament and of the Council of 16 February 2022 amending Directive 2014/41/EU, as regards its alignment with Union rules on the protection of personal data, (OJ L 39, 21.2.2022)
F-05	Directive (EU) 2022/211 of the European Parliament and of the Council of 16 February 2022 amending Council Framework Decision 2002/465/JHA, as regards its alignment with Union rules on the protection of personal data, (OJ L 37, 18.2.2022)
F-06	European Parliament Legislative Observatory, Police cooperation - joint investigation teams: alignment with EU rules on the protection of personal data, 2021/0008(COD)
F-07	EPPO College Decision 009/2020, Rules concerning the processing of personal data by the European Public Prosecutor's Office, 28 October 2020
F-08	Communication from the Commission to the European Parliament and the Council: Way forward on aligning the former third pillar acquis with data protection rules, (COM (2020) 262 final, 24 June 2020)
F-09	Council Decision (EU) 2016/2220 of 2 December 2016 on the conclusion, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, (OJ L 336, 10.12.2016)
F-10	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, (OJ L 119/132; 4.5.2016)
F-11	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such

	data, and repealing Council Framework Decision 2008/977/JHA (4.5.2016; OJ L 119/89)
--	---

G) Police Cooperation in the EU

G1) General

G1-01	Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA, <i>(OJ L 134, 22 May 2023)</i>
G1-02	Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation, <i>(OJ L 158, 13 June 2022)</i>
G1-03	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025 <i>(COM/2021/170 final, 14 April 2022)</i>
G1-04	Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817, and 2019/818 of the European Parliament and of the Council, <i>(COM/2021/784 final, 8 December 2021)</i>
G1-05	European Commission, Press Release, "Police Cooperation Code: Boosting police cooperation across borders for enhanced security", 8 December 2021
G1-06	European Commission, Factsheet, "Reinforcing police cooperation across Europe", 8 December 2021
G1-07	Commission Staff Working Document: Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817, and 2019/818 of the European Parliament and of the Council, <i>(SWD/2021/378 final, Brussels, 8.12.2021)</i>
G1-08	Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol, <i>(COM(2020) 791 final, Brussels, 9 December 2020)</i>
G1-09	European Commission, Inception Impact Assessment on EU Police Cooperation Code (PCC), Ref. Ares(2020)5077685, 28 September 2020
G1-10	Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU Regulation (EU) 2022/1190 of the European Parliament and of the Council of 6 July 2022 amending Regulation (EU) 2018/1862 as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union, <i>(OJ L 185, 12.7.2022)</i>

G1-11	Council Decision 2008/617/JHA of 23 June 2008 on the improvement of cooperation between the special intervention units of the Member States of the European Union in crisis situations, (OJ L 210, 6.8.2008)
G1-12	Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210/12; 06.08.2008)
G1-13	Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210/1; 06.08.2008)
G1-14	Council Framework Decision of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ L 386/89; 29.12.2006, P. 89)
G1-15	Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration of 27. May 2005 (10900/05; 27.5.2005)

G2) Joint Investigation Teams (JITs)

G2-01	Eurojust Information on JITs
G2-02	Europol Information on JITs
G2-03	JIT Evaluation Form
G2-04	Council of Europe: Guidelines on the use of Joint Investigation Teams
G2-05	Riehle, C. "20 years of Joint Investigations Teams (JITs) in the EU": An overview of their development, actors and tools. ERA Forum 24, 163–167, 29 June 2023
G2-06	Checklist for multilateral joint investigation teams, 22 June 2023
G2-07	Latest trends and novelties in JIT operations: first-hand experiences of JIT practitioners and Eurojust Eurojust European Union Agency for Criminal Justice Cooperation (europa.eu) Fourth JITs Evaluation Report, 14 June 2023
G2-08	Regulation (EU) 2023/969 of the European Parliament and of the Council of 10 May 2023 establishing a collaboration platform to support the functioning of joint investigation teams and amending Regulation (EU) 2018/1726, OJ L 132, 17 May 2023
G2-09	Guidelines on the Network of National Experts on Joint Investigation Teams, 2 December 2020
G2-10	Third JIT Evaluation Report, Eurojust, March 2020
G-11	Joint Investigation Teams: Practical Guide, 16 December 2021
G2-12	Council Resolution on a Model Agreement for Setting up a Joint Investigation Team (JIT) – 2017/C18/01, Strasbourg, 19 January 2017
G2-13	Council Document establishing the JITs Network, 08 July 2005
G2-14	Council Framework Decision of 13 June 2002 on joint investigation teams (OJ L 162/1; 20.6.2002)