326DT004
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

Digital investigations, open source intelligence tools and AI

Budapest, 15-16 October 2026

FACE-TO-FACE

EXCELLENCE IN EUROPEAN LAW

Speakers and chairs

Philip Anderson, Assistant Professor, Computer and Information Sciences Department, Northumbria University, Newcastle

Linda Bertram, Public Prosecutor, Cybercrime Centre, Prosecutor General's Office, Frankfurt

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

Seanpaul Gilroy, Senior Digital Forensic Investigator, Northumbria Police, Newcastle

Krisztina Karsai, Professor, Criminal Law, University of Szeged (Hungary)

Emmanuelle Legrand, Magistrate, Senior Legal Expert, Member of the French Judiciary, Paris

Balázs Rozsnyai, Judge, District Court, Hajdúböszörmény (Hungary)

Bilal Sen, Senior Investigator, Coninsec, Cologne

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
326DT004

Organisers
ERA (Laviero Buono) in cooperation with the National Office for the Judiciary

Co-funded by
the European Union

european.law

#DIGITALISATION and #ARTIFICIALINTELLIGENCE in Criminal Justice

Thursday, 15 October 2026

09:00 Arrival and registration of participants

09:30 **Welcome and introduction to the programme**
Representative of the National Office for the Judiciary & Laviero Buono

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

Chair: Laviero Buono

09:35 **Using open source intelligence to gather evidence online**
- Understanding the Internet and associated technology
- Effective use of the Internet as an investigative investigation tool
- Internet protocols (IPs) and proxy servers
- Search engines, meta browsers and deep web

Philip Anderson

10:30 Discussion

10:45 Break

11:15 **Computer forensics in the cloud**
- Geo-location tools for social media and photos
- Tracing domain name owners, origin of an email and blacklist checks
- Investigating Web 2.0 – social networking, blogs and online gaming
- Protecting your privacy when investigating online

Seanpaul Gilroy

12:15 Discussion

12:30 Lunch

PART II: LEGAL ISSUES RELATED TO THE COLLECTION AND PRESENTATION OF E-EVIDENCE IN COURT

Chair: Philip Anderson

13:45 **Evidence collection, due diligence and online searches**
- Fake generators
- Privacy protection
- Online/delete data

Bilal Sen

14:45 Discussion

15:00 Break

15:30 **Using electronic evidence and artificial intelligence in criminal investigations and presenting them at court**
- The importance of the chain of custody in handling evidence
- Trial considerations: methods of presentation and admissibility tests

Linda Bertram

16:30 Discussion

16:45 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. are here to stay and 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 taking 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

Hungarian Academy of Justice
Tóth Lőrinc street 6
1122 Budapest
Hungary

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, 16 October 2026

PART III: VIDEOCONFERENCING AND ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

Chair: Bilal Sen

09:30 **Presenting evidence at court: e-files, videoconferences and remote trials**
- Remote trials during and after the pandemic
- E-files
- Witness videoconferencing
- Assessing evidence, the impact of artificial intelligence

Balázs Rozsnyai

10:15 Discussion

10:30 Break

11:00 **Digital tech as tool to commit crimes**
- Cyber patrolling and cyber investigations
- Tackling the illegal trade on the darkweb

Emmanuelle Legrand

11:30 **The impact of the AI Act on the applications of AI to criminal justice**
- Deepfakes
- Machine learning
- Prediction and sentencing

Krisztina Karsai

12:15 Discussion

12:30 End of the seminar and light lunch

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

Apply online for
"#Digitalisation and #AI in Criminal Justice":
www.era.int/event-number/326DT004

Your contacts



Laviero Buono
Head of Section
European Criminal Law



Julia Reitz
Event Coordinator
+49(0)651 93737 323
jreitz@era.int

This programme has been 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

Budapest, 15-16 October 2026 / Event number: 326DT004

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, Bosnia and Herzegovina, Moldova, Ukraine 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 **15 July 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 Hungary: 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 States return journeys between 50 and 400 km (Austria €58, Bulgaria €26, Czech Republic €26, Croatia €36, Italy €50, Poland €26, Romania €26, Slovenia €37, Slovakia €26). 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 Hungary the contribution for travel for a distance between 50km and 400km is fixed at €28. 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 €210. National participants will receive an overall fixed contribution of €105. 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/event-number/326DT004**

Venue

Hungarian Academy of Justice
Tóth Lőrinc street 6
1122 Budapest
Hungary

Language

English

Contact

Julia Reitz
Event Coordinator
+49(0)651 9 37 37 323
jreitz@era.int

Technical Issues and basic understanding of the Internet architecture and concepts

Using open-source intelligence to gather evidence online

PHILIP ANDERSON

ERA | BUDAPEST, 15-16 OCTOBER 2026

Co-funded by the European Union

Outline

1. Understanding the Internet and associated technologies.
2. Effective use of the Internet as an investigation tool.
3. Search engines, meta browsers, deep web and people search techniques.
4. Using open-source intelligence to gather evidence online.

Cybercrime landscape – IOCTA 2026

- Online fraud schemes (OFS) – now the fastest-growing area of organised crime
  - Investment fraud, BEC and payment fraud most common; AI personalises social engineering at scale.
- Ransomware – more than 120 active brands observed in 2025
  - Extortion has shifted from decrypting data to threatening to leak it.
- Crime-as-a-Service (CaaS)
  - Increasingly powered by AI and automation, including early agentic tools.
- Child Sexual Abuse Material (CSAM)
  - AI-generated CSAM is rising; sexual extortion reports up roughly 70% year on year.
- The dark web – an enabler of cybercrime
  - Cryptocurrency remains favoured, with growing use of privacy coins resistant to blockchain tracing tools.

Source: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf

Example

Law enforcement partners across the world had been trying to identify the man in the abuse material ever since it was posted in 2010.

The images were referred to the NCA by Australian Federal Police in 2013, after they established they had been posted on dark web site, The Love Zone.

In 2017 Italian investigators linked the name “Martyn” to the person who took the images, but they were unable to progress the case further.

In the same year a French investigator adopted the case and worked on identifying a beach which had been seen in some images linked to the offender.

After conducting significant research on the geology of the landscape, he established that rocks on the beach in the photo must either be in Ireland or Wales. He compared them to images of over 60 beaches before striking an exact match on the Pembrokeshire coast in Wales.



Example

The case remained unsolved until 2022, when NCA investigators created a new programme which finally disabled the image distortion technique. This revealed the face of the offender but his identity, and that of his victim, was still unknown.

It was discovered that at the time of the abuse, Armstrong lived in Derbyshire but he had sold his house in January 2022 and moved close to the same Welsh beach identified by investigators.

Following his arrest, NCA investigators found a number of devices in Armstrong's home, including one of the two cameras he used in 2010. This was forensically matched to the camera which took the images.

The original indecent images of children (IIOC) he'd posted were also recovered from a laptop.

Investigators also discovered material showing Armstrong abusing two previously unknown child victims saved on his devices. All three victims were spoken to and safeguarded.

Source: https://www.nationalcrimeagency.gov.uk/news/nca-develops-new-tool-that-identifies-prolific-child-rapist-after-13-year-international-hunt



Understanding the Internet and associated technologies



How does it work.

- Every device connected to the Internet is assigned an IP (Internet Protocol) address.
- Every device speaks the same language.
- Every device has a unique IP address.
- To communicate, devices need to exchange addresses.
- This address could be used to trace an online activity back to a device.

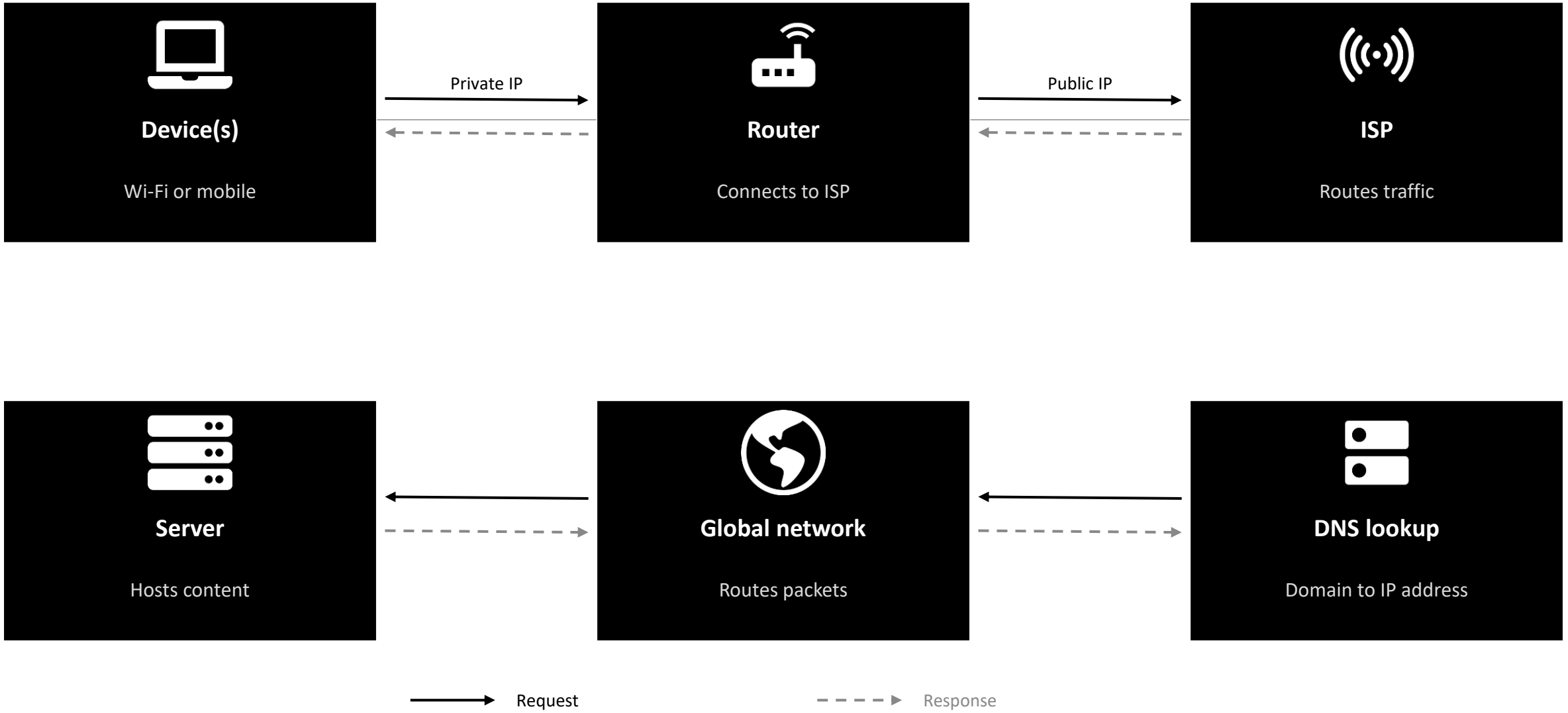
Example

How a Nintendo Switch helped locate a missing girl 2,000 miles from home

With help from Nintendo, the FBI obtained the Switch's IP address which led them to the abductor's apartment complex.

Her destination was an apartment complex in Tolleson, Arizona. According to court records, a then-28-year-old man, Ethan Roberts, had befriended her on the internet, traveled to Virginia to get her, and later forced her into child pornography.

Source: https://www.abc15.com/news/local-news/investigations/how-a-nintendo-switch-helped-locate-a-missing-girl-2-000-miles-from-home


Device(s)
Wi-Fi or mobile
Private IP
Router
Connects to ISP
Public IP
ISP
Routes traffic
Server
Hosts content
Global network
Routes packets
DNS lookup
Domain to IP address
Request
Response

IPv4 vs IPv6

- IPv4
  - 32-bit numbers (2^{32})
  - 4,294,967,296 addresses
  - Range: 0.0.0.0 – 255.255.255.255
- Private ranges
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
- Public IP
  - All addresses outside private and reserved ranges

- IPv6
  - 128-bit numbers (2^{128})
  - 340 undecillion addresses
  - (340,282,366,920,938,463,463,374,607,431,768,211,456)
- Range
  - 0000:0000:0000:0000:0000:0000:0000:0000
  - ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
- Example
  - 2a02:c17c:da4f:2b00:d856:4e43:15ab:7d9f
- Like IPv4, has equivalent private, reserved and public ranges

Attached Devices

help

#	IPv4 Address	Device Name	MAC Address
1	192.168.0.4	Nest-Audio	d8:8c:79:6c:91:3d
2	192.168.0.5	Google-Home-Mini	e4:f0:42:0b:01:87
3	192.168.0.6	SKY+HD	20:47:ed:72:3f:f2
4	192.168.0.11	SkyBooster2	24:a7:dc:21:63:91
5	192.168.0.16	SKY+HD	20:47:ed:c4:d3:ba
6	192.168.0.18	UNKNOWN	d4:a6:51:b9:f1:54
7	192.168.0.19	TY_WR	d4:a6:51:ba:b5:01
8	192.168.0.25	UNKNOWN	58:b0:3e:51:ce:b8
9	192.168.0.34	Chromecast	f4:f5:e8:1e:7e:02
10	192.168.0.37	SKY+HD	d4:52:ee:97:a3:20
11	192.168.0.38	LGwebOSTV	0c:8e:29:a5:72:62
12	192.168.0.95	Google-Nest-Mini	14:c1:4e:4b:e9:8a
13	192.168.0.97	UNKNOWN	82:c0:76:ed:99:aa
14	192.168.0.98	UNKNOWN	ea:d6:68:be:ad:68
15	192.168.0.102	UNKNOWN	08:c2:24:86:1d:30
16	192.168.0.103	UNKNOWN	f0:2f:9e:a4:26:f7
17	192.168.0.104	Nest-Doorbell-Battery	24:e5:0f:dc:2d:97
18	192.168.0.105	SkyBooster4	9c:31:c3:6e:4a:41
19	192.168.0.107	LAPTOP-M9F9TE42	10:63:c8:65:55:39
20	192.168.0.141	DESKTOP-GRL4RV9	48:f1:7f:b4:93:21

How does it work… Public and Private IP

How does it work… Privacy | Anonymity







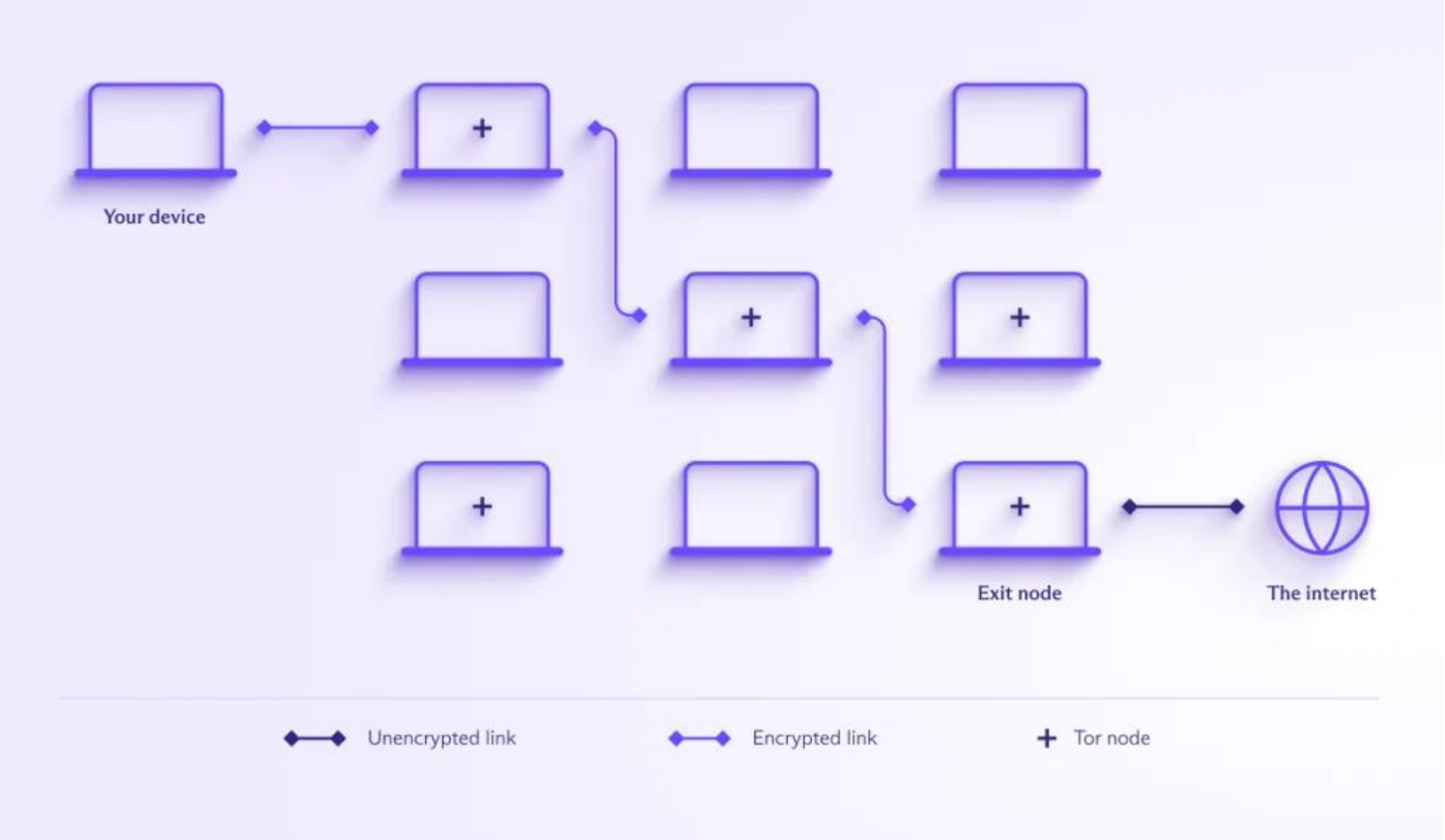
VPN Server

VPN Tunnel

Internet Service Provider (ISP)

VPN IP

How does it work… Onion Routing Network (TOR)



Source: https://protonvpn.com/blog/best-onion-sites?srsltid=AfmBOoq4xMqkfT9NF0kzJqqPmXndDCSWGmaoaSFDCC43FtQg61WHA_gB



Spotlight… Apps - Telegram

- Private 1-2-1 chats (encrypted)
- Private groups (invite-only)
- Public groups (searchable)
- Channels (broadcast platforms)

Source: https://www.osint.industries/post/osint-on-telegram-find-phone-numbers-emails-and-user-details

Spotlight… Telegram

- Anonymous accounts – no phone number required.
- Supports up to 20,000 members in groups.
- Public channels – accessible by everyone.
- 2GB per file sharing limit.
- Supports bots.
- Self-destruct messaging, anonymous forwarding.

- Used by
  - Extremist groups – recruitment and propaganda.
  - Criminals selling malicious software, stolen data and other ‘services’.
  - Drug dealers – encrypted chats and private groups to negotiate deals and public channels advertising drugs.
  - Scammers – promotion.
  - Child exploitation – sharing CSAM material, private ‘discussion’ channels.
  - Million of non-criminals.

- Searching Telegram
  - Telegram usernames – search in the app (@username).
  - Browse the public groups – past messages and user profiles maybe available.
  - Cross-reference usernames with other platforms.
  - Public profiles – personal information.
  - Phone numbers & email lookup.

Source: https://www.osint.industries/post/osint-on-telegram-find-phone-numbers-emails-and-user-details



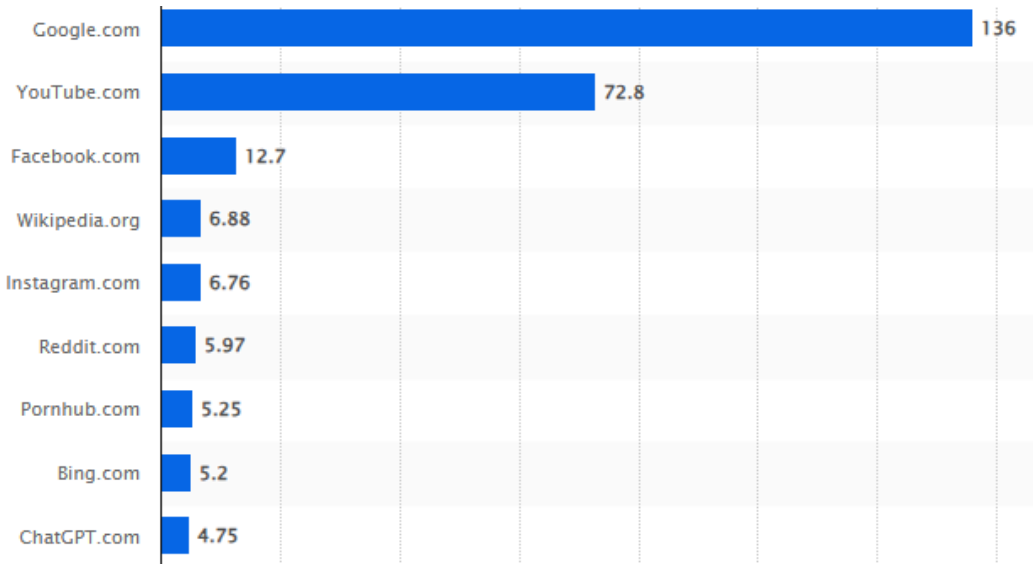
Effective use of the Internet as an investigation tool

Investigations…

- The planning, collection, analysis, interpretation and presentation of materials from sources available to the public, to use as intelligence or evidence within investigations.

Investigations… Social media

- As of February 2025, 5.24 billion social media users from 5.56 billion Internet users[1]
- 4th Q of 2024 – 61.85% of website traffic is from mobile devices[2]

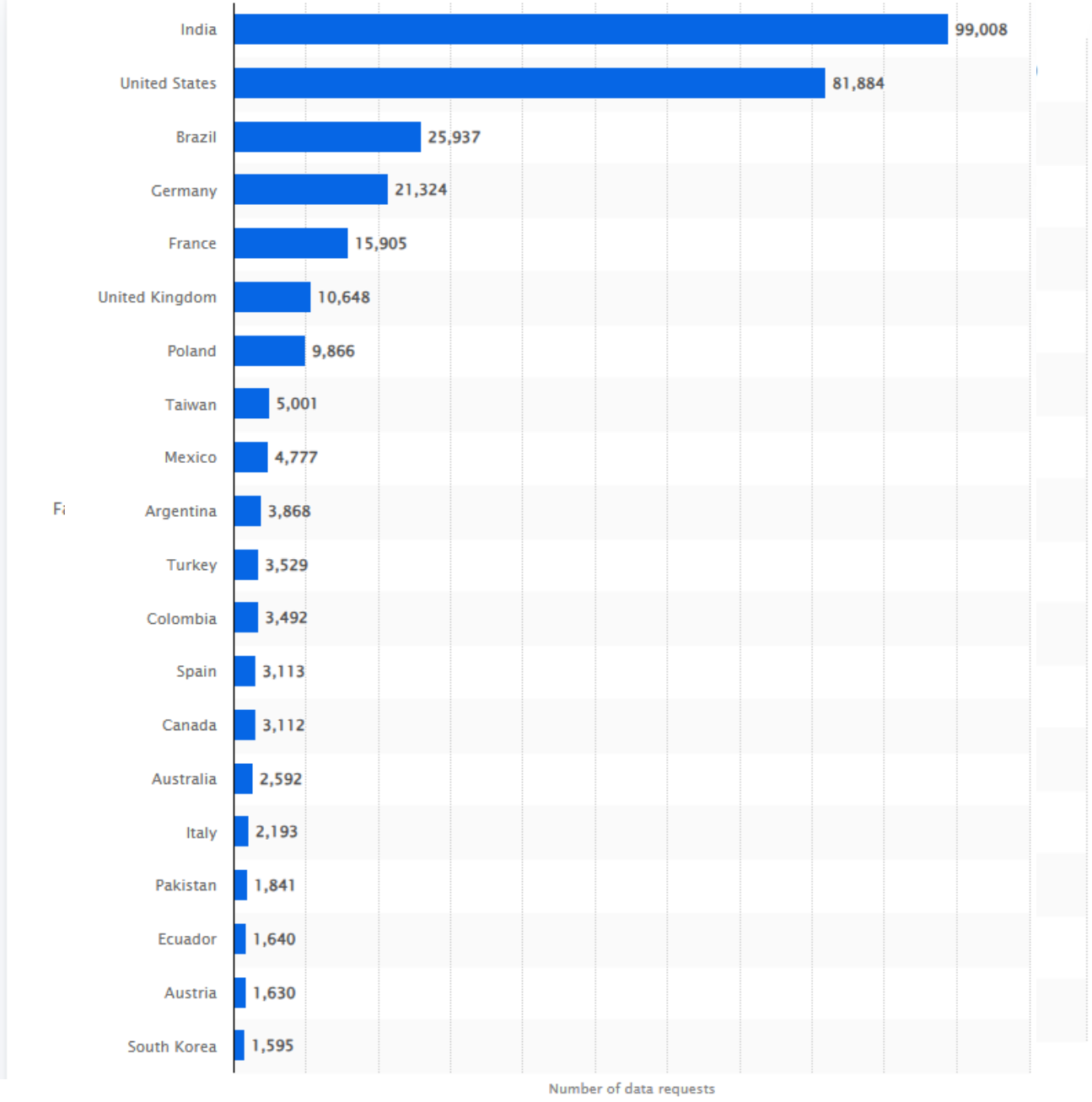


Most popular websites worldwide as of November 2024, by total visits(in billions)

Source - https://www.statista.com/statistics/1201880/most-visited-websites-worldwide/

1. Statista - https://www.statista.com/statistics/617136/digital-population-worldwide/

2. Statista - https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/



#1 Most popular social networks worldwide as of February 2025, ranked by number of monthly active users. Source: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

#2 Number of user data requests issued to Facebook by federal agencies and governments during 1st half 2024, by country). Source: https://www.statista.com/statistics/287845/global-data-requests-from-facebook-by-federal-agencies-and-governments/

Investigations… Social Media Posts



Washington DC shooting suspect accused Israel of 'atrocities' in social media post, Sky News finds

Sky News has uncovered what is believed to be a statement by the shooting suspect posted at 10pm local time, around an hour after the shooting - suggesting it was scheduled.

The letter, signed with Rodriguez's name, was dated 20 May 2025.

In the lengthy essay, Rodriguez criticises Israel's actions in Gaza and attacks the US government's position.

Source: https://news.sky.com/story/washington-shooting-suspect-accused-israel-of-atrocities-in-social-media-post-sky-news-finds-13372548

Other Investigations…

- Detection and prevention
  - Investigating suspicious claims for injury or workers' compensation
- IP theft
- Online defamation
- Due diligence

Investigations… considerations

- Still need to…
- Maintaining evidential integrity – no evidence bags required here.
- Ensuring chain of custody – robust audit trail(s).
- Dates and times are still key when capturing OSINT evidence.
- So is hashing – uniquely identify the evidential items

Investigations… Ethics

- Open source intelligence is the use of **publicly** produced and **publicly** (and legally) available data that can be collected and shared.
- Be aware of the terms and conditions policies on the public data you are trying to collect.
- The collection of open source data and nothing more, shouldn’t be associated with hacking, intrusion testing, or anything similar.



Search engines, meta browsers, deep web and people search techniques

The Internet…

- Surface web
  - The section of the Internet that is being indexed by search engines
  - 2.25 billion pages indexed[1]
  - 175 zettabytes of data[2]
  - Accessed via ‘standard’ browsers - Chrome, Mozilla Firefox, Opera, etc.
- Deep web
  - Not indexed
  - Accessed via username and passwords
  - Some data out of the Deep web may be picked up by search engines in the case of a data breach.
  - Accessed via ‘standard’ browsers - Chrome, Mozilla Firefox, Opera, etc.
- Dark web
  - Challenging environment
  - Anonymous browsing network consists of thousands of relays.
  - Indexing is now happening (proxied TOR sites – TOR2WEB)
  - Accessed via ‘specialist’ browsers – TOR Browser.

1: Source - https://www.ipxo.com/blog/how-big-is-the-internet/
2: Source: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

Example

Like Bake, Yates played a key role in ensuring the site continued to run smoothly. He was responsible for enforcing the rules by promoting or dropping other users, provided access to private and exclusive sections of the site and advised on security measures. He also passed on training to others about the role that he himself had received.

However, Yates was less careful around his own personal security. His username on the site was 'yates704' and in chat logs recovered by the NCA, he also told other users first name, his age and that he lived in Eastbourne.

'yates704' was also found on 'HACKFORUMS.NET, a clear website forum dedicated to discussion relating to hacker culture and cyber security.

Investigators found 6,000 private messages between 'yates704' and other users of The Annex. The conversations varied from fantasy roleplay involving the sexual abuse of children, as well as more official conversations around the moderation of the site, advice on how to post indecent images of children and techniques to evade law enforcement.

NCA officers identified Yates using these details and the email addresses associated to him and he was arrested at his home in Eastbourne in July 2022.



impres

fore be

orcement detection,

Source: https://www.nationalcrimeagency.gov.uk/news/mechanic-who-had-secret-life-running-child-abuse-sites-on-the-dark-web-is-jailed

Open Source… Methods

- Defined as "… is the discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."
  U.S. Director of National Intelligence and the U.S. Department of Defense. Source: US Army FM 2-0 Intelligence March 2010

Methods… Information Sources

- Many websites and tools available that can be used to find publicly available information about an organisation or individual.
- Enable gathering of information about a person that is available on various social networking sites.
- Used to find previous versions of webpages
- Provide access to company information that might otherwise be difficult to obtain.
- Find phone numbers, IP addresses, whois data, geo location, tracing, and more.
- Starting points: OSINT Framework, OSINT Tools and OSINT.Link.

Methods… Information sources

- General search engines
- National search engines
- Meta search engines
  - Results from multiple search engines
- Image, video and document search
- Reverse image search
- Geolocation
- Social Media networks
  - Facebook, Twitter, YouTube, Instagram, Snapchat
  - Weibo (China), VK (Russia)
- Blog search
- Newspaper searches
- Public records
- Business records
  - Government websites
- Transportation
- Doman names
- Internet archives
- People search engines
  - Name, Address, Phone, Email
  - IP Address

Methods… Tools

- Remember
  - Evidential integrity
  - Evidential chain of custody
  - No digital devices have been seized or examined.
- Capturing the (online) evidence
  - Web capture tools
    - Searching
    - Collecting and documenting
      - Timestamps and hashing
    - Audit trail
    - Secure cloud storage
    - Reporting



Using open source intelligence to gather evidence online

Open Source… Case Studies - Bellingcat

- Two Europol StopChildAbuse Images Geolocated - https://www.bellingcat.com/news/2019/12/05/two-europol-stopchildabuse-images-geolocated-part-i-madagascar/
- Google maps photos
- Google Earth imagery
- Geographic and demographic data examined
- Timeline analysis – tropical storms
- Skripal Poisoning Suspect Dr. Alexander Mishkin, Hero of Russia - https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia/
- Passport photos
- Online biographical data
- Locations searches
- Telephone numbers

Open Source…

- Planning
  - Identify potential sources from which information may be gathered from
- Capturing and consolidation
  - Information collected from the chosen sources that may assist in the investigation
- Analysis
  - Data analysis of the processed information
- Presentation
  - Findings are presented/reported

Challenge
Work out the country/region/town





Thank you

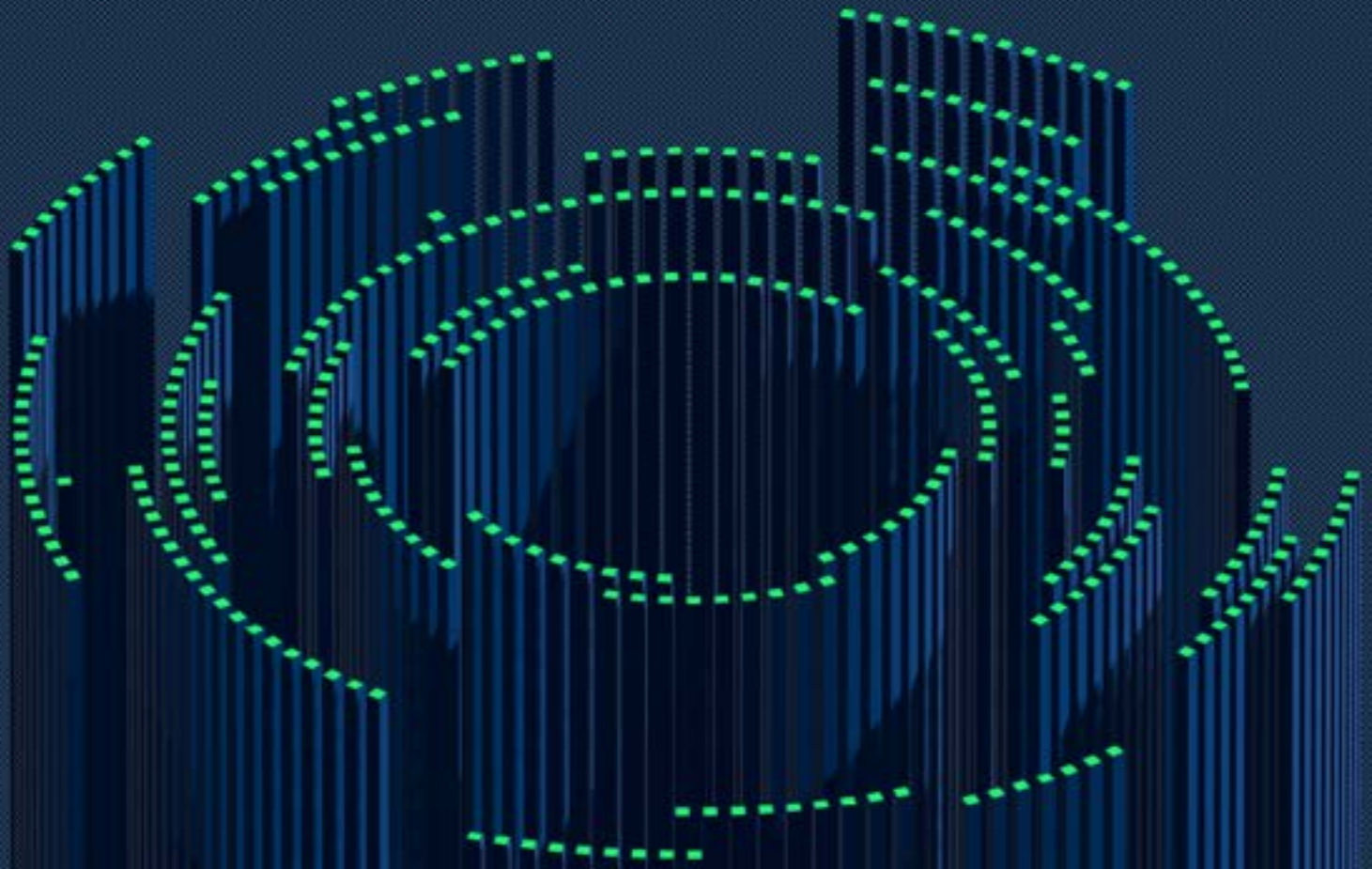
Questions?

Philip Anderson

Assistant Professor

School of Computer Sciences
Northumbria University, UK
Email: philip.anderson@northumbria.ac.uk

EUROPOL



IOCTA 2026

Internet Organised Crime Threat Assessment

The evolving threat landscape

How encryption, proxies and AI are expanding cybercrime



The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime.
Internet Organised Crime Threat Assessment (IOCTA) 2026

PDF WEB

ISBN 978-92-9414-096-8 ISSN 2363-1627 doi: 10.2813/5737847 QL-01-26-004-EN-N

Neither the European Union Agency for Law Enforcement Cooperation (Europol) nor any person acting on behalf of the agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2026

© European Union Agency for Law Enforcement Cooperation, 2026

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the copyright of Europol, permission must be sought directly from the copyright holders.

While best efforts have been made to trace and acknowledge all copyright holders, Europol would like to apologise should there have been any errors or omissions. Please do contact us if you possess any further information relating to the images published or their rights holder.

Cite this publication: Europol, *The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime – Internet Organised Crime Threat Assessment (IOCTA) 2026*, Publications Office of the European Union, Luxembourg, 2026.

This publication and more information on Europol are available on the internet.
www.europol.europa.eu

Your feedback matters.

By clicking on the following link or scanning the embedded QR code you can fill in a short user survey on the received strategic report.

Your input will help us further improve our products.

https://ec.europa.eu/eusurvey/runner/eus_strategic_reports

Contents

Foreword 06

Introduction 07

1

Cybercrime enablers 10

1.1 The dark web ecosystem

1.2 The criminal infrastructure: from residential proxy to proprietary hosting services

1.3 Cryptocurrencies and other financial facilitators

1.4 Automation and AI

2

The criminal infrastructure behind online fraud schemes (OFS) 16

2.1 OFS threat becomes faster and more concealed

2.2 Relay attacks

2.3 Digital asset theft via cryptocurrency drainers

2.4 OFS networks rely on a wide range of enablers

3

Cyber-attacks 22

3.1 An increasingly interwoven ecosystem

3.2 Main developments in the ransomware ecosystem

3.3 New hacking coalitions threaten big tech and customer data

3.4 Infostealers continue to cater for the cybercrime market

3.5 DDoS attacks pose a hybrid threat

4

Online child sexual exploitation 30

4.1 Sexual extortion cases continue to spike

4.2 Shifting offender behaviour: monetisation of CSAM

4.3 E2EE applications for networking and exchange of CSAM

4.4 Production of synthetic CSAM is on the rise

Looking ahead 36

Appendix 38

Abbreviations 39

References 40

Foreword



I am pleased to present Europol's Internet Organised Crime Threat Assessment (IOCTA) 2026, the most comprehensive analysis of the latest threats and trends in cybercrime in the EU. This report also serves as a critical call to action for all stakeholders committed to safeguarding our society in the digital domain and beyond.

The accelerating pace of cybercrime presents progressively sophisticated threats to society, with harmful implications both online and offline. As we release this year's report "How encryption, proxies, and AI are expanding cybercrime", it is clear that law enforcement must step up to address these evolving challenges.

Cybercriminals are rapidly exploiting advanced technologies, particularly AI tools, to enhance the speed, efficiency, and scope of their illicit activities. These tools not only enable automation in criminal processes but also blur the lines between legitimate and malicious uses of technology.

The widespread use of end-to-end encryption platforms and complex jurisdictional barriers create significant investigative challenges, hindering the identification of suspects and the corroboration of evidence. Moreover, restrictive data retention policies often leave law enforcement authorities unable to access crucial data in a timely manner, impeding their ability to track suspects and disrupt criminal operations.

The resilience and adaptability of dark web marketplaces and forums, coupled with the use of cryptocurrencies, further complicate the efforts of policing in the digital domain. The current online fraud epidemic, the threat posed by ransomware intertwining with hybrid threats, and the monetisation of child sexual abuse material underscore the urgent need for more proactive and collaborative efforts.

This call to action resonates deeply, and I am committed to ensuring that Europol leads the way in this critical endeavour. Together, we can build a more secure and resilient digital future for all.

Catherine De Bolle
EXECUTIVE DIRECTOR OF EUROPOL



Introduction

The accelerating pace of cybercrime presents increasingly sophisticated threats for society – with harmful implications both online and offline. In parallel, it introduces additional challenges for law enforcement, which must overcome the widening 'velocity gap'. As AI tools become more accessible, cybercriminals are able to lower the barrier to entry, scale operations more effectively, and increasingly commit crimes without direct involvement in the operations. This evolution means that criminals will likely minimise the time needed to launch attacks, while increasing both their scale and personalisation. Law enforcement authorities (LEAs), therefore, must adopt and integrate AI capabilities proactively to anticipate, understand, and mitigate emerging threats, ensuring society's security in the digital domain while respecting fundamental rights and data protection.

The challenges of investigating and prosecuting cybercrime: Data and jurisdictional barriers

The widespread criminal use of end-to-end encryption (E2EE) platforms, coupled with complex jurisdictional and technical barriers, creates significant investigative blind spots. These obstacles hinder the identification of suspects and the corroboration of evidence, ultimately slowing down investigations and weakening preventive actions against imminent threats. To close this gap and counter the abuse of E2EE applications, LEAs must advocate for regulatory frameworks and expand collaborative initiatives with online service providers (OSPs).

Moreover, LEAs are often hampered by restrictive or inadequate data retention policies. By the time investigators request access to relevant data, it is often no longer available, impairing their ability to track suspects or disrupt criminal operations. The alignment of data retention policies across digital service providers, not just in terms of retention duration but also regarding which data is kept, would significantly enhance LE capabilities.

Cybercrime enablers: Resilient, adaptable, and sophisticated

The resilience of dark web marketplaces and forums plays a critical role in facilitating cybercrime. These platforms are becoming increasingly specialised and fragmented, intertwining more and more with E2EE messaging platforms, in a hybrid ecosystem of anonymity. Despite continuous takedowns by LEAs, these criminal actors show remarkable adaptability, with new platforms emerging rapidly to replace those that are disrupted.

Cryptocurrencies remain the preferred payment method for cybercriminals, particularly in ransomware attacks. The growing use of high-opacity coins and mixing services further complicates LEAs' ability to track illicit financial flows. With the increasing overlap between surface and dark web channels, enabled by E2EE and anonymised services, cybercriminals are conducting near-real-time crypto transactions. This enhances their ability to launder money across both the cybercrime and wider organised crime landscape.

Cybercriminals continue to exploit both commercial

E2EE platforms and decentralised protocols. As these technologies become more accessible, they allow criminals to operate with a larger user base, further complicating LE efforts. The strategic use of bullet-proof hosting, infrastructure spread across multiple jurisdictions, and layered routing schemes via residential proxies make it increasingly difficult for LEAs to detect and track criminal activity.

Online fraud schemes: A growing threat

Fraud schemes represent the fastest-growing area of organised crime. Criminal networks target both individuals and organisations, generating substantial profits from schemes like investment fraud, business email compromise (BEC), and fraud against online payment systems. Investment fraud, particularly related to cryptocurrencies, is especially prevalent.

Online fraud schemes (OFS) networks operate as highly efficient, transnational industries, utilising a range of logistical, technical, and financial operations to perpetrate large-scale fraud. Phishing, the use of SIM boxes, and malicious advertising are common tactics used to steal funds and personal information. With the increasing adoption of generative AI, fraudsters can now personalise social engineering techniques, making them more convincing and dangerous.

The use of crime-as-a-service (CaaS), where fraudsters can outsource criminal activities like cryptocurrency theft, further expands the reach of online fraud. As AI tools become more sophisticated but also mainstream, the threat posed by OFS is set to further escalate, with automated processes enhancing the speed and scale of victimisation.

Ransomware: A complex and evolving landscape

Ransomware remains a dominant threat across the EU, with more than 120 active ransomware brands observed by Europol in 2025. Criminal actors continue to exploit vulnerabilities in the digital supply chain and employ increasingly sophisticated social engineering techniques. The extortion model continues shifting from encrypting data to pressuring victims to pay for their data to not be released.

While financial gain remains the primary driver of cyber-attacks, the relationship between hybrid threat actors and cybercriminals is blurring. Hybrid threat actors are increasingly using cybercriminal networks as proxies for disruptive operations, including DDoS attacks, intrusions, and ransomware attacks. In the growing CaaS economy, hybrid threat actors are simply another customer, further complicating efforts to counter these multifaceted threats.

The ransomware landscape continues to evolve with the expansion of ransomware-as-a-service (RaaS), as criminal actors adapt their platforms and launch new services to attract affiliates. There is also a continuous proliferation of extortion tactics that criminals use to apply psychological pressure on victims, including data exfiltration, DDoS attacks, and cold-calling.

Child sexual abuse material (CSAM): New technologies and monetisation

Child sexual exploitation (CSE) offenders are rapidly adapting to new technologies, expanding their crimes, upscaling abuse opportunities, and making the exchange of CSAM more efficient, while simultaneously complicating law enforcement efforts. The trade in CSAM is growing, with offenders exploiting online platforms for both the production and distribution of illicit material. Live distant child abuse (LDCA) in particular, remains a persistent challenge as the lack of evidence in these crimes makes them difficult to investigate.

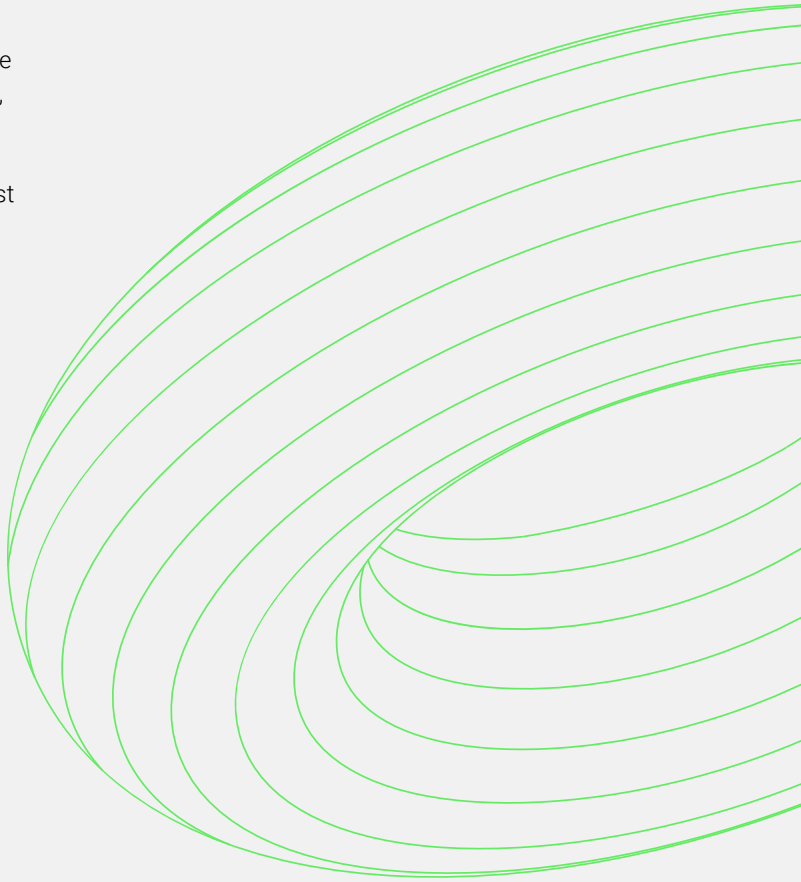
The trade in CSAM for financial gain is increasing, and multi-layered extortion models are also becoming more common, with offenders manipulating victims to produce more content, send money or commit violent acts. The rise of AI-generated CSAM poses additional challenges for victim identification and investigative capabilities. As the trade grows, more platforms selling CSAM also emerge.

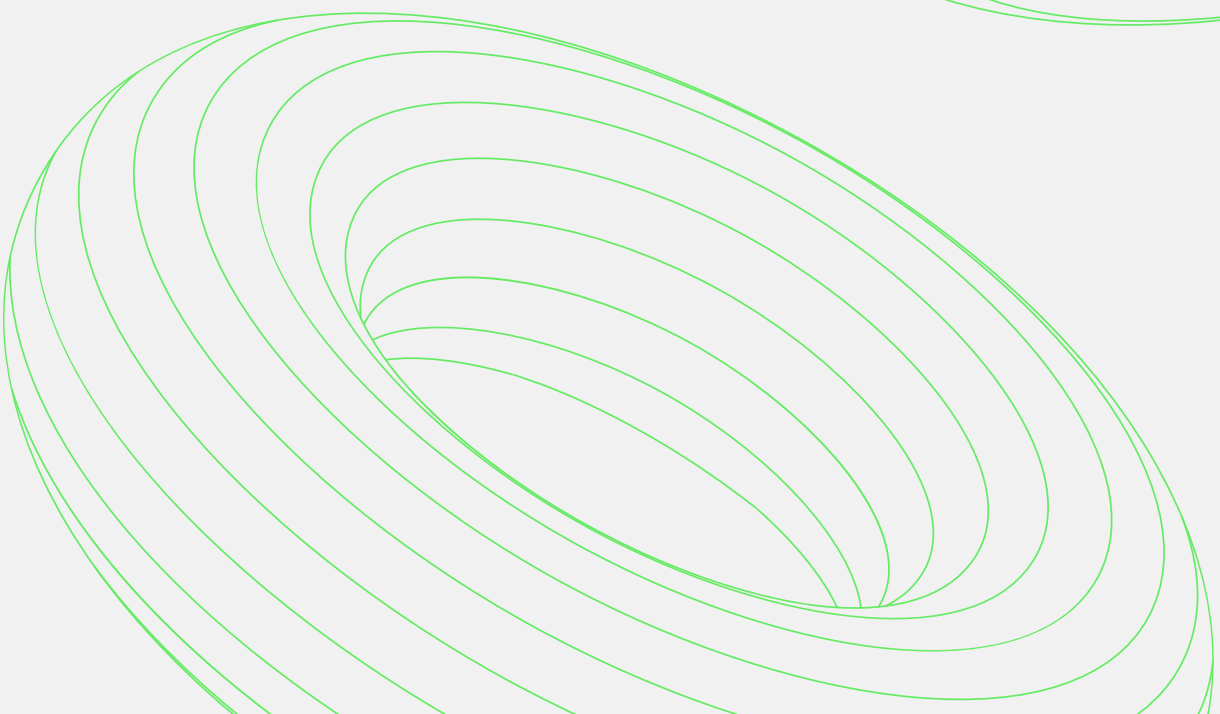
The exploitation of E2EE platforms by CSE offenders and online extortion communities such as The Com network pose extremely serious threats to children and to society, creating a complex criminal landscape where CSE, cyber-attacks, extortion, assault, rape, murder, and violent extremism intertwine.

Looking ahead

The landscape of cybercrime will continue to rapidly evolve, driven by increasingly sophisticated tools and methods. To effectively combat these threats, LEAs must invest in AI capabilities, improve cross-border cooperation, and advocate for stronger data retention and lawful access policies. As criminals exploit new technologies and create complex networks, law enforcement must adapt quickly to ensure the safety and security of the digital world.

In the coming years, law enforcement's ability to tackle cybercrime will depend on its capacity to bridge this 'velocity gap' by harnessing technology. However, the rapid evolution of cybercrime will require more than just technological integration - it will require closer collaboration with the private sector. LEAs must secure access to the vast data held by online service providers (OSPs), in order to identify and apprehend criminals and terrorists effectively.





CYBERCRIME ENABLERS



01

Key Developments

- Dark web marketplaces are increasingly fragmented, moving towards more specialised platforms catering to specific criminal activities. Despite ongoing takedowns and law enforcement efforts, marketplaces demonstrate remarkable resilience, with new ones emerging rapidly to replace those disrupted. Forums function as migration hubs after a prominent market is closed down.
- Cryptocurrencies continue to serve as the preferred payment method for ransomware attacks. A growing trend towards high-opacity coins resistant to blockchain tracing tools poses new challenges to law enforcement authorities. Mixing services frequently located in offshore jurisdictions are making the tracking of illicit transactions even more challenging.
- The distinction between surface and dark web communication channels is becoming increasingly blurred, as E2EE platforms and anonymised services now connect the two realms.
- The abuse of the Domain Name System (DNS) allows criminals to effectively exploit the time period between domain registration and LE intervention.
- Criminals are moving towards more complex operational set-ups, hosted on sub-sub-leased servers or self-deployed infrastructure, routed through multiple obfuscation layers and increasingly masked by residential proxies, which makes them significantly harder for LEAs to trace and dismantle.

In the fast-evolving cybercrime landscape, various enablers facilitate illicit operations, creating a complex environment that challenges LE investigations. The fragmented yet resilient nature of dark web marketplaces and forums serves as primary entry point for cybercriminals. Cybercriminal are implementing more layers in their infrastructures to further challenge their tracing and identification.

Among the facilitators of financial cybercrime, privacy coins and off-shore exchange services play a pivotal role in the laundering of ransomware payments. Besides, the integration of automation and AI in cybercrime operations pose several future threats. Criminal networks also continue to abuse the DNS for both cyber-attacks and online fraud schemes (OFS), where slow reporting mechanisms undermine mitigation and prevention efforts.

1.1 The dark web ecosystem

In 2025, the dark web continued to function as a critical enabler within the global cybercrime ecosystem, providing operational infrastructure, services, and anonymity. While LEAs are able to exert pressure through takedowns, dark web forums continue to shape the underground economy. The dark web continued to demonstrate resilience and dynamism, as marketplaces adapt, user migration becomes easier and faster, and communication platforms diversify.

Marketplaces: fragmentation, specialisation and resilience

General-purpose marketplaces, once the dark web core hubs for illicit trade, have shown signs of contraction. The average lifespan of criminal markets further shortened and administrators appear increasingly risk-averse due to international LEA actions. Following takedowns, users migrate to other marketplaces, moving where the number of listings rapidly increases. Markets do not have enough time to build up large user numbers anymore, leading to a fragmentation, internal instability and widespread mistrust among users.

Smaller, dedicated platforms continued to gain traction[1]. They focus on mediating tools and services for fraud (bank accounts, one-time password (OTP) bypass tools, compromised card data), access brokerage (compromised RDP/VPN credentials), malware services (stealers, droppers, loaders), etc. Smaller communities improve the operational security of the platform by limiting exposure and enable administrators to vet or restrict memberships.

However, dedicated marketplaces also experience instability, with exit scams via sudden shutdowns remaining endemic. Administrators increasingly plan shutdowns, to disappear with users' funds at the first sign of trouble. Shutdown plans involve coordinated deletion, rapid infrastructure turnover, and exit scams. These safeguards reduce the window for asset seizure and hamper digital forensic analysis of seized devices.

EUROPE-WIDE TAKEDOWN HITS LONGEST-STANDING DARK WEB DRUG MARKET

Archetyp Market operated as a drug marketplace since 2020, amassing more than 600 000 users worldwide, with a total transaction volume of at least EUR 250 million. With over 17 000 listings, it was one of the few dark web markets that allowed the sale of fentanyl and other highly potent synthetic opioids, contributing to the growing threat posed by these substances in the EU and beyond. In June 2025, a large-scale LE operation, supported by Europol and Eurojust, led to the dismantlement of the market. Coordinated actions took place across Germany, the Netherlands, Romania, Spain, and Sweden, targeting the platform's administrator, moderators, key vendors, and technical infrastructure. The platform's infrastructure was based in the Netherlands, while its administrator – a 30-year-old German national – was arrested in Barcelona, Spain. Measures were taken in Germany and Sweden against one moderator and six of the marketplace's highest vendors, and assets, worth EUR 7.8 million, were seized[2].

Shortly after the takedown of Archetyp Market, **Abacus Market** (once the largest market in listings) and **MGM Grand** (with more than 15 500 listings) shut down. As the largest remaining Bitcoin-enabled markets, their wide userbase made them vulnerable to heightened LE scrutiny and potential intervention. LE actions potentially prompted administrators to choose self-preservation and exit scamming over risks of seizure.

A new marketplace called **BlackOps** was then launched in July 2025. It immediately listed 41 942 items, and then grew to 63 979 by the end of November 2025. This growth underscores the hypothesis that the shutdown of popular markets triggers user migration and identification of new opportunities for criminal action. Together with **TorZon** and **Nexus Market**, the three quickly became the marketplaces with the largest number of listings by the end of the year.

Forums as the primary entry vector

Forums remain key entry points for aspiring cybercriminals and provide a critical environment to advertise leaked or breached data listed on marketplaces. They also provide onboarding, tutorials, and MO development, trust-based social structures, opportunities for recruitment and vetting, and migration hubs when platforms are dismantled.

The dynamism of forums' is well illustrated by users' migrations from legacy communities – such as **BreachForums** and **XSS**[3] – towards smaller, invitation-only spaces. When forums collapse, user migration is rapid, and new iterations or successor forums emerge within weeks, sometimes backed by the same core actors.

In 2025, **DarkForums** has emerged as the successor of BreachForums (read more in the cyber-attacks chapter), enabling the exchange of leaked data, sale of malware, and distribution of hacking tools across both its surface- and Tor-based platforms.

1.2 The criminal infrastructure: from residential proxy to proprietary hosting services

Modern threat actors rarely confine their operations to the dark web alone. Instead, they increasingly rely on a hybrid ecosystem of anonymity, which includes E2EE messaging platforms and decentralised protocols across both clear and dark web.

Bullet-proof hosting and layered anonymisation as persistent blockers

Cybercriminals continue to rely on BPH providers, which create resilience for their backend infrastructure. These services, sometimes embedded within multi-layered leasing arrangements (sub-sub-leasing) are nested across several jurisdictions, systematically disregarding abuse notifications and judicial takedown requests. Legal measures directed at these hosting providers often result in LEAs obtaining delayed or incomplete electronic evidence, due to limited data retention frameworks or redirection of the judicial requests to intermediaries.

Enhanced anonymisation methods, such as routing traffic through multiple VPN servers (VPN-chaining) and Tor nodes, are also increasingly observed. These techniques introduce successive layers of masked IPs, and possible encryption, before the traffic reaches the hosting environment, complicating source attribution and delaying the investigation due to numerous additional cross-border judicial requests.

Some criminal networks increasingly bypass third-party providers and deploy their own proprietary infrastructure. By owning the hardware, these groups effectively avoid localisation and seizure warrants.

Residential proxy services marketed to cybercriminals

The use of residential proxies in the cybercriminals' attack infrastructure helps camouflage their activity as legitimate traffic, making it harder for LEAs to detect, track and attribute malicious traffic routed through home-user IPs in different countries. Residential proxies act as intermediary servers, with an IP-address assigned to an internet-connected home device. They are widely available and marketed as a way to bypass geo-block or verifications, but these connections can be hijacked or rented by cybercriminals and used to disguise malicious traffic, launch DDoS attacks or scrape data.

Residential proxies can become compromised through vulnerabilities in the unpatched and/or unsecured home appliances or by installing malicious applications that grant access to the device. The proxy networks are easy to maintain - even following a disruption causing a proxy's unavailability, the vulnerability leveraged for the initial compromise is likely still present and may be exploited again, by a different actor, putting it back onto the criminal market.

DNS abuse: a critical delivery infrastructure for cyber-attacks and OFS

DNS abuse effectively bridges the gap between criminal infrastructure and victims of both OFS and cyber-attacks[4]. Technical DNS abuse and website content abuse are tightly intertwined in the criminal process. For instance, criminals register domains to harvest user credentials through imitations of legitimate websites (e.g. financial institutions).

Additionally, ransomware and malware operations abuse DNS for delivery and for Command and Control (C2) of botnets, leveraging residential proxies to anonymise traffic and impersonate legitimate users.

Criminal networks exploit efficiently the time period between domain registration and LE intervention. The absence of automated reporting interfaces and the reliance on slow, cross-border judicial assistance protocols prevent the mitigation (e.g. blocking or take-down of malicious domains) required to stop automated fraud and malware distribution campaigns before they reach scale.

1.3 Cryptocurrencies and other financial facilitators

The use of cryptocurrencies in cybercrime is evolving rapidly, adapting to advancements in blockchain technology, decentralisation, and anonymisation tools. Cryptocurrencies are used to conduct illicit activities through automated tools. They are no longer solely a cybercrime facilitator but now a well-established obfuscation means in the wider SOC landscape.

Privacy coins and off-shore exchange services make ransomware more sophisticated

In 2025, cryptocurrencies served as the preferred payment method for ransomware attacks, mainly due to their relative anonymity and borderless nature. Offenders have been increasingly utilising privacy coins, thanks to their built-in anonymity features, to further obfuscate the origins and destinations of their transactions. This shift highlights a growing trend towards high-opacity coins that are resistant to blockchain tracing tools, posing new challenges to LEAs. Criminals often favour the use of exchange services located in jurisdictions with loose anti-money laundering (AML) protocols or off-shore financial centres.

The growing popularity of cryptocurrencies broadens the target pool

Cryptocurrencies remained largely targeted in cyber-enabled fraud, as they are also becoming increasingly accessible to minors and young adults, also via social media 'get-rich' schemes, and for peer-to-peer trading. Having gained wider acceptance as a form of payment and investment, a sharp rise in crypto assets thefts has been reported in 2025 (read more in the section on cryptocurrency drainers). Minors may unknowingly engage in money laundering by renting out wallets or receiving crypto 'gifts' from cybercriminals.

Mixing-as-a-service for money laundering

One of the most significant trends for cybercriminal usage of cryptocurrencies in 2025 is **the rise of chain-hopping linked to money laundering (ML) operations**. With the advent of blockchain bridges, which facilitate the transfer of assets between blockchains, criminals can move funds rapidly across blockchains, further complicating the process of tracing illicit transactions. Bridging as such is a legitimate and essential technology in the cryptocurrency industry, serving as the 'connective tissue' that enables interoperability between otherwise isolated blockchain networks. Criminals would use a bridge to access opportunities on different chains without selling assets and paying exchange fees. Their speed, liquidity, and relative decentralised nature make them the preferred laundering method for ransomware actors and major dark web marketplace administrators.

The use of privacy coins remains popular among professional money launderers linked to ransomware operations, spoofing services and other forms of cybercrime, despite their declining use on centralised exchanges due to bans.

Especially for vendors on dark web marketplaces, 'coinjoin' services combining multiple coins from multiple users into a single transaction[I] remain a popular mixing solution (even if regulatory and enforcement pressure have increased following the

[I] CoinJoin is a privacy-focused technique used in cryptocurrency transactions to enhance anonymity. It works by combining multiple transactions from different users into a single transaction, making it difficult to trace the origin and destination of the funds. This process helps to break the link between the sender and receiver, thereby increasing privacy.

takedown of **cryptomixer.io**). As coinjoin services are rather 'slow' (a single mixing round can take an hour), users seeking speedy movement of illegal funds to an off-ramp[II] choose faster solutions, such as smart contract-based mixers (also known as 'mixer-as-a-service') and decentralised exchanges (DEXs). These services utilise automated market makers (AMMs) for instant settlement, eliminating the need for manual order book matching, middleman approval, or custodian delays. They operate directly on-chain, allowing for 24/7, peer-to-contract trading. The growing prevalence of such services has made the tracking of illicit transactions even more challenging for investigators, as these platforms bypass traditional financial institutions that enforce know your customer (KYC) and AML regulations.

EUROPOL AND PARTNERS SHUT DOWN CRYPTOMIXER

An illegal cryptocurrency mixing service called 'Cryptomixer' was suspected of facilitating cybercrime and money laundering. Cryptomixer was a hybrid mixing service, accessible via both clear and dark web. It facilitated the obfuscation of criminal funds for ransomware groups, dark web forums and markets. Its software blocked the traceability of funds on the blockchain, making it the platform of choice for cybercriminals seeking to launder illegal proceeds from a variety of criminal activities, such as drug trafficking, weapons trafficking, ransomware, and payment card fraud. Since its creation in 2016, over EUR 1.3 billion in Bitcoin were mixed through the service. In November 2025, Europol supported an action week conducted by LE in Switzerland and Germany in Zurich, Switzerland. Three servers were taken down and seized in Switzerland, along with the cryptomixer.io domain. The operation resulted in the confiscation of over 12 terabytes of data and more than EUR 25 million worth in cryptocurrencies[5].

Other fintech services such as pre-paid cryptocurrency credit cards provide off-ramp services to integrate illicit funds into licit financial flows, bypassing EU AML rules. Cryptocurrency-to-cash desks remain a critical physical service where digital theft is converted into fiat currency. This dual evolution in both physical and digital vectors, the latter all accessible via smartphone, contribute to the further diversification of channels for money laundering and criminal finance, making illicit financial flows increasingly difficult to trace.

1.4 Automation and AI

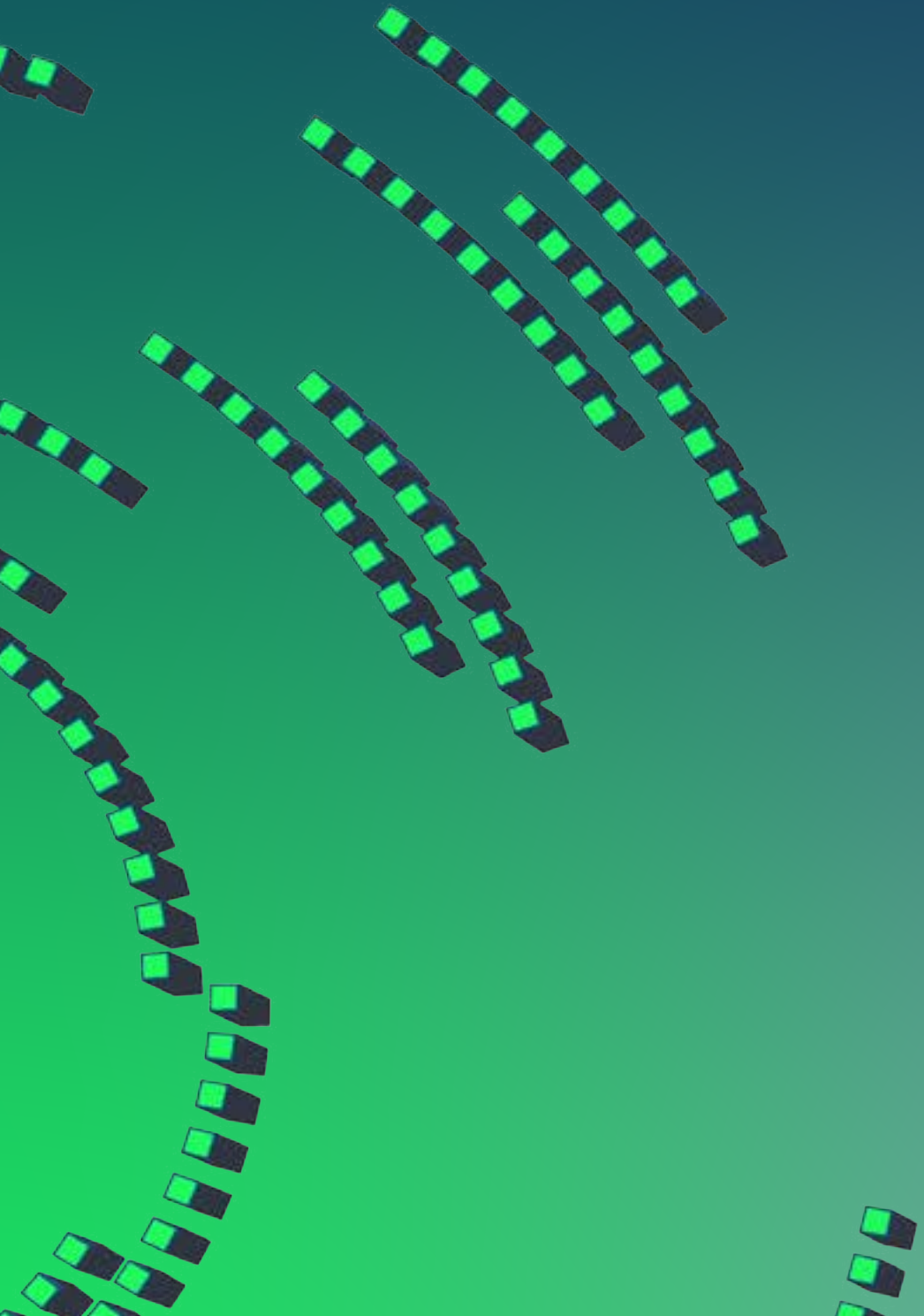
The rapid evolution and accessibility of a wide range of AI tools continuously create opportunities for the whole cybercrime ecosystem to increase efficiency, speed and reach. Criminal networks involved in cybercrime adeptly harness AI and automation to upscale their operations, facilitated by the parallel integration of AI capabilities in legitimate security contexts and business applications, which opens further avenues for exploitation.

Transnational communities of child sexual exploitation (CSE) offenders, fraud networks, and ransomware groups are constantly working to expand their operational capabilities and operational security through the use of generative AI tools and automated bots. Cybercriminals also take advantage of legitimate commercial applications using AI technology.

The dark web remains an important hub for malicious large language models (LLMs), which are built or adapted to remove ethical constraints and filters from legitimate commercial solutions[6]. AI models can also be tailored for criminal purposes by providing inputs that are most relevant and accurate for that application. For example, malware samples, guides on how to carry out OFS or how to set up infrastructure not to be detected and identified can be used to improve the precision and quality of the malicious output of the model.

[II] Crypto on-ramps and crypto off-ramps are services that allow users to exchange fiat currency — government-issued money — for cryptocurrencies, and vice versa. They connect bank accounts, payment cards and digital wallets to crypto exchanges or platforms, so people can buy, sell or spend digital assets securely and easily.

THE CRIMINAL INFRASTRUCTURE BEHIND ONLINE FRAUD SCHEMES



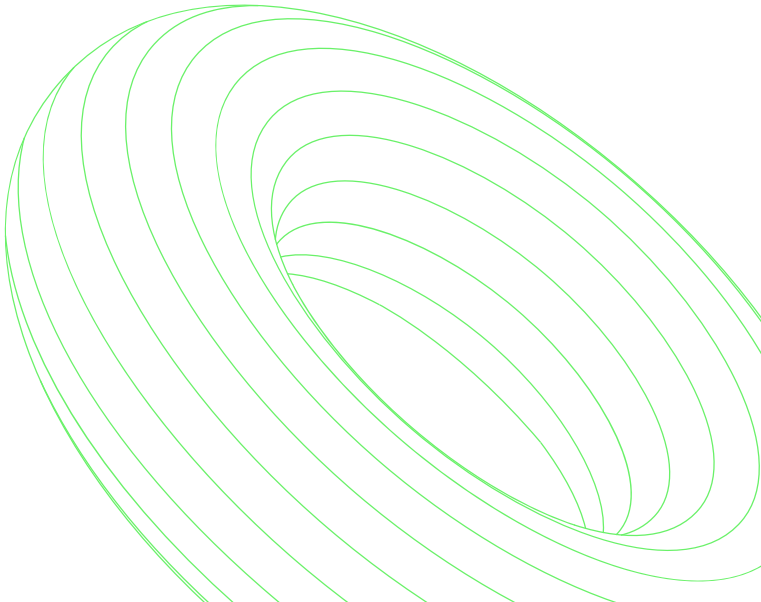
02

Key Developments

- The threat from online fraud schemes continues to grow, supported by a criminal infrastructure enabling speed, industrial-scale victimisation and increased anonymity. Online fraud schemes commonly involve phishing, with malicious advertising as a popular attack vector, enabling the targeting of victims with precision. The abuse of SIM boxes provides hardware for large-scale attacks.
- Certain criminal networks have shifted away from using commercial bulletproof hosting and instead have started to deploy their own infrastructure, so as to bypass KYC protocols and disrupt traditional evidence chains.
- The theft of digital assets via cryptocurrency drainers has matured to a crime-as-a-service (CaaS) system, driven by the uptake of DeFi across the EU, their growing popularity for money laundering purposes, as well as a rising diversity in digital assets available.
- While fraudsters' use of generative AI has improved their ability to personalise social engineering techniques, the criminal adoption of agentic AI to automate parts of the criminal process is set to raise the threat from OFS to unprecedented levels.

Fraud schemes represent the fastest-growing area of organised crime. Fraudsters generate large profits by targeting individuals, public and private sector organisations, and their data. Investment fraud (especially crypto), business email compromise (BEC), romance, tech support and fraud against payment systems are the most common OFS typologies reported by Member States.

While sophistication of techniques and modi operandi vary, cybercriminal networks are particularly active in fraud against payment systems, aimed either at stealing funds or at obtaining personal information[7]. Stolen data are not just used for the fraud scheme but often sold onwards and further exploited by other criminals, via clear and dark web, in a vicious loop where targets are relentlessly re-victimised.



2.1 OFS threat becomes faster and more concealed

Law enforcement reporting throughout 2025 indicated a transition from a threat landscape largely defined by volume and variety of fraud schemes to one also characterised by velocity and more complex operational security.

The adoption of technological advancements allowed OFS to evolve into a high-speed and borderless AI-leveraged criminal activity. Generative AI continued to accelerate online fraud, enabling criminal networks operating from outside the EU to personalise narratives with ease and target EU citizens at high speed and vast scale. This is exemplified in AI-assisted impersonation (e.g. of bank helpdesk or law enforcement personnel), and enhanced realism in business email compromise (BEC) and CEO fraud.

By advertising on very large online platforms (VLOPs)[8], criminal networks can industrialise victims' targeting and bypass geographic or linguistic barriers, a significant enabler especially for crypto investment fraud, now largely happening on VLOPs.

SIM boxes: The industry-like system

The use of SIM boxes to enable fraud has further globalised, with this technology internationally sourced by criminal networks targeting the EU. These farms can provide mass-scale anonymity for phishing campaigns, allowing criminal networks to bypass KYC protocols and subscribe to thousands of services simultaneously – including fraudulent advertising platforms and fake accounts for social media and communication applications. Fraudulent platforms and accounts can be localised to the targeted country, concealing the fraudsters' identity and location.

A **SIM box** is a device that houses hundreds of SIM cards used as part of a voice-over-IP gateway installation. Criminals use them to mask communication data and to make calls or send SMS messages at cheaper rates. A group of SIM boxes is known as **SIM farm**. SIM farms can facilitate the dissemination of thousands of SMS, calls and social media posts to enable large-scale fraud.

Active farms have been identified in the EU and are often utilised remotely by criminal networks based in other jurisdictions. The global reach of these anonymity services illustrates that the SIM box ecosystem is a cohesive, transnational supply chain rather than a localised threat.

Criminal associates travel to jurisdictions where SIM bulk purchasing is possible and registration is either not necessary or less regulated. These assets are then physically trafficked to hosting locations, to populate the industrial-scale SIM farms that nowadays underpin the majority of online fraud operations. This illustrates criminal reliance on a dedicated physical supply chain that law enforcement can intercept.

CAAS NETWORK PROVIDING SIM BOXES FOR TELECOMMUNICATIONS-ENABLED CYBERCRIMES

A network of seven Latvian nationals had set up a SIM farm used to enable crimes against thousands of victims across Europe. The infrastructure comprised at least 1 200 SIM-box devices, operating 40 000 SIM cards linked to telephone numbers registered to people from over 80 countries around the world, offered for criminal abuse. Most fraud schemes using this service involved phishing to gain access to victims' e-mail and banking accounts. While the true scale of this network is still being uncovered, more than 49 million online accounts were created on the basis of the illegal service provided by suspects. Offences facilitated by this criminal service included various forms of online fraud, but also extortion, migrant smuggling and the distribution of child sexual abuse material. The damage caused to victims amounts to millions of Euros. Austrian, Estonian, Latvian, and Finnish authorities, supported by Eurojust and Europol, arrested the group in October 2025[9].



FIGURE 1 - SIM BOXES AND SIM CARDS SEIZED DURING THE OPERATION

IMSI catchers: an interception technology used for OFS

While CaaS and technology advancements continue to lower entry barriers for scammers, the primary operational evolution is the deployment of more sophisticated telecommunications infrastructure, to bypass KYC protocols and disrupt traditional evidence chains, as commonly seen in phishing and account takeover (ATO) campaigns.

A rise in the use of IMSI catchers (and SMS blasters, also enabled to send SMS messages) points to the adoption of interception technology by criminal networks.

An **IMSI catcher** is a device that mimics a cell tower, broadcasting signals to make mobile phones in its range connect to it, thus enabling the harvesting of personal and sensitive data. Devices that also have the capability to send SMS messages, are referred to as **SMS blasters**.

Since the connection is downgraded to 2G, these attacks can occur 'under the radar' of commercial telecommunication providers – effectively bypassing the legitimate network, thus allowing criminals to avoid attribution and disrupt traditional evidence chains.

2.2 Relay attacks

Relay attacks on payment terminals increased in the EU throughout 2025[10], specifically terminal-to-terminal and card-to-terminal vectors (see figure 2). In a terminal-to-terminal relay attack, transaction data is transferred in real-time between a payment card (or digital wallet) and a relay device in possession of the criminal to enable cash-out[11]. In a card-to-terminal relay attack, the victim is deceived into installing a malicious app and insert card details and PIN, which are then used by criminals to cash out.

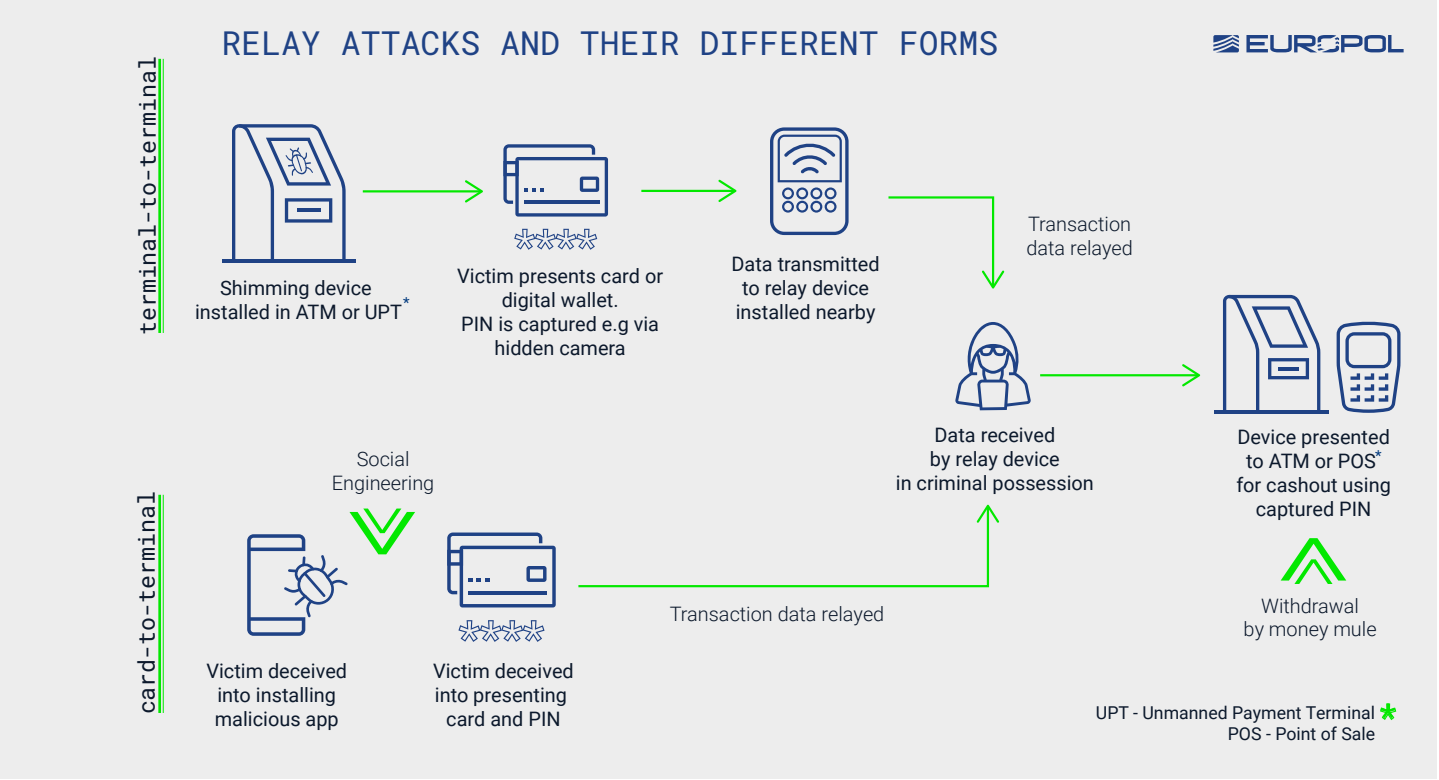


FIGURE 2 - SIMPLIFIED OVERVIEW OF RELAY ATTACKS AND THEIR DIFFERENT FORMS: TERMINAL-TO-TERMINAL AND CARD-TO-TERMINAL [SOURCE: EUROPOL]

2.3 Digital asset theft via cryptocurrency drainers

Theft of digital assets via cryptocurrency drainers kept fluctuating throughout the year, due to a volatile cryptocurrencies market and subsequent user activity, as well changes in the criminal landscape (i.e. the acquisition of a large crypto wallet draining service, Inferno Drainer, by a rival draining-as-a-service provider, Angel Drainer, in October 2024)[12].

Cryptocurrency drainers are specialised malwares that target the Web3 ecosystem[I], designed to grant attackers unauthorised control over victims' wallets. The attack vector relies heavily on phishing and social engineering; victims are manipulated into connecting their wallets to malicious smart contracts and unknowingly approving transactions that authorise the immediate draining of their funds. This threat has matured into a CaaS system.

It is plausible that cryptocurrency drainers are also used by hybrid-actor-linked criminal networks. The threat may continue to expand in line with increasing public uptake of cryptocurrencies and the utility of these assets for laundering criminal proceeds.

[I] Web3, short for Web 3.0, refers to the newer generation of the internet, more decentralised, open, and user-controlled compared to the Web 2.0. Web3 leverages privacy-reducing technologies like blockchain, smart contracts, DeFi, NFTs, etc.

2.4 OFS networks rely on a wide range of enablers

The smartphone is the essential common denominator in modern OFS developments, functioning not merely as a communication tool but as the primary means to circumvent KYC checks. While caller ID spoofing[II] continues to be a major enabler for fraud, online fraudsters have learned to abuse the rapid customer onboarding business model of neo-banks[13]. They enable the fast registration of a continuous stream of new accounts and customers, which places pressure on KYC mechanisms.

Parallel to this increased reliance on mobile identity and financial services, some criminal networks involved in OFS have moved away from commercial bulletproof hosting and are increasingly deploying their own infrastructure[14]. This shift represents a countermeasure against LE access to backend data (read more in the Cybercrime enablers chapter).

Infrastructure for anonymisation via virtual computers has also been incorporated into the extensive CaaS ecosystem supporting online fraud. Criminal marketplaces offering virtual desktop services (VDS)[III] allow fraudsters to enjoy full administrative control and no usage limits, while enhancing anonymisation and enabling location spoofing.

Malicious advertising (also called malvertising) is another primary enabler of high-volume and large-scale fraud, especially relevant in crypto-investment fraud schemes. Criminal affiliate marketeers abuse VLOPs and legitimate marketing platforms to cater to fraudsters huge volumes of victims, behind a façade of legitimacy.

Malvertising ranges from advertisement of fraudulent websites or mobile applications that imitate legitimate banking, investment or trading platforms, to fake accommodation or merchandise listings. Unlike banks, which face license revocation for facilitating financial crime, major tech platforms currently lack comparable penalties to report fraudulent advertising effectively[IV].

The prominence of phishing and smishing campaigns is a direct adaptation to the EU shift towards two-factor authentication (2FA). Despite EU regulations[V] on 2FA[15], and with biometric authentication (e.g. face, fingerprint and iris identification) becoming increasingly commonplace, criminals will continue to seek technical ways to bypass these protocols. However, social engineering and human error will remain the weakest links for fraudsters to exploit.

While the deployment of agentic AI — systems capable of autonomous operational planning and execution — remains a developing driver for crime, criminal networks continue to effectively utilise generative AI to upscale their operations. Artificial Intelligence support includes coding assistance and generation of conversation scripts, to aid call centre operators.

Voice chat bots are also increasingly deployed to pre-screen victims at industrial volume, acting as a filter for human operators, thereby significantly increasing the efficiency of fraud centres. However, industry intelligence reveals that this adoption comes with vulnerabilities; criminals frequently rely on public, jailbroken LLMs.

II Caller ID spoofing is a technique used to falsify the information transmitted to the caller ID display in order to disguise the caller identity. Caller ID spoofing usually happens on traditional landline phones, mobile phones, and Voice over Internet Protocol (VoIP) systems.

III A virtual desktop service, sometimes called Virtual Desktop Infrastructure (VDI) or Desktop-as-a-Service (DaaS), allows users to access a desktop environment and its applications from anywhere, using any device with an internet connection. Instead of running applications on a local device, the applications run on a remote server, and the user interacts with them through a virtual desktop interface.

IV Despite the enforcement framework under the Digital Services Act (DSA), including fines for Very Large Online Platform (VLOP) of up to 6% of the global turnover; European Commission, 2025, The enforcement framework under the Digital Services Act, accessible at https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement.

V Including the eIDAS Regulation and Payment Services Directive 2 (PSD2).

CYBER-ATTACKS



03

Key Developments

- The ransomware landscape remains highly volatile and fragmented due to an increasing number of emerging ransomware brands, driven by competition among criminal actors, the aftermath of LE actions and new available technological resources. In 2025, Europol observed more than 120 active ransomware brands, with ransomware attacks steadily increasing.
- Ransomware-as-a-service (RaaS) groups are increasingly seeking to broaden their service offerings to attract affiliates, including through functionalities leveraging AI tools and more customisable branding.
- There are noticeable overlaps across different ransomware operations and brands and the affiliates and administrators involved, showing their significant role in the ransomware ecosystem.
- Hybrid threat actors leverage cybercriminal networks as proxies for destabilisation purposes, through DDoS or ransomware attacks, for data theft operations and to compromise strategic targets.

3.1 An increasingly interwoven ecosystem

Ransomware persists as a key threat in the EU, with a significant number of ransomware families[I] active throughout 2025. Criminal actors continued leveraging vulnerabilities and targeted the digital supply chain to scale their attacks and deploy increasingly sophisticated social engineering techniques. The focus of the extortion has shifted from releasing (decrypting) the data to pressuring victims to pay for it to not be released (leaked), showing the importance of data in today's digital economy.

While financial gain remains the dominant motivation behind cyber-attacks, the relationships between state hybrid threat and criminal actors have become more and more interwoven. Hybrid threat actors use cybercriminal networks as proxies for interference activities, which include DDoS attacks, intrusions, data theft operations and ransomware attacks. Cybercriminals may serve as proxies unknowingly, others in exchange for protection from prosecution or under coercion[16]. In the prevailing CaaS cybercrime economy, hybrid threat actors just become customers among other customers.

Ransomware: brands fragmentation and short-lived operations

In 2025, Europol observed more than 120 active ransomware brands, with ransomware attacks steadily increasing. The ransomware environment continues to be highly unstable and divided, fuelled by a growing number of new brands, rivalry among criminals, the consequences of LEAs interventions, and the availability of new technological tools.

[I] A ransomware family refers to ransomware samples sharing a common codebase, encryption method, or functional characteristics. A brand is the name adopted by the cybercriminals, like a label chosen to be identified behind attacks/services/tools.

Many **ransomware operations** continue to be short-lived and more likely to rebrand within a shorter timeframe, with a noticeable overlap of administrators and affiliates involved and between different ransomware groups' attack, proxy and money laundering (ML) infrastructure. Ransomware operators can easily pivot their activities, increasingly thanks to the abundance of available leaked ransomware codebases, AI-powered code-assembly tools and RaaS platforms enabling the creation by other criminals of their own malware version.

Initial access is acquired in various ways, with the method of choice usually dependent on the ransomware operator's skills and preferences. Common attack vectors include phishing, infostealers, exploiting unpatched vulnerabilities in public-facing applications, via Initial Access Brokers (IABs), and/or insider threats[17] continued to be deployed.

Multi-layered extortion tactics focus on threat of data release

Most ransomware groups still deploy multi-layered extortion tactics, with data exfiltration as a key element of coercion. Many victims are more willing to pay for their data *not* to be released (publicly leaked), in contrast to the early days of ransomware, when the extortion focused on the need of the victim for the data *to be* released (i.e. decrypted) back to them. Modern enterprises are generally more prepared to deal with the impact of data being lost (encrypted or erased), compared to being published. Simultaneous DDoS attacks, spamming of corporate email addresses and psychological pressure via cold-calling are common in the extortion toolkit of ransomware actors, and are sometimes offered as a service.

3.2 Main developments in the ransomware ecosystem

Ransomware groups vary according to their barrier to entry, their technical sophistication as well as their motivation (i.e. financial, ideological or both). They generally divide in three main groupings: public affiliate programs, semi-closed and closed groups.

Public RaaS affiliate programs

Public RaaS affiliate programs allow almost anyone to sign up and carry out attacks using the different capabilities integrated into their platform. In addition to the malware assembler, these can include botnets for pay-load distribution, tools for persistence and victim monitoring, data exfiltration and ML infrastructure, services for ransom negotiation and leak-site hosting. The administrators of the platform take a percentage of each ransom payment facilitated through their service.

Running exfiltration-focused infrastructure and data leak sites is highly resource-intensive, which is why cybercriminals turn to RaaS platforms. RaaS providers, in turn, are incentivised to offer convenient all-in-one solutions to attract affiliates and establish a reputable and stable brand-identity.

Qilin emerged as a dominant ransomware family in 2025. It offers its affiliates a comprehensive toolkit and have recently included integrated DDoS capabilities to pressure victims[18]. The group seems to be working on automating attack-based vulnerabilities in Fortinet Secure Socket Layer (SSL) VPN devices, thus enabling affiliates to launch attacks on desired targets. The core group appears to be based in Russia, with ties to the defunct Conti group. They present themselves as an ideologically motivated group, although activity appears financially driven and they offer one of the highest affiliate profit-shares in the market (80 % - 85 % of the ransom payment)[II].

[II] A Secure Socket Layer protocol enables remote users to securely access corporate network resources using either a web browser (web mode) or the FortiClient device, which provides full network access.

Akira, also with ties to Conti, is operating since March 2023 and has maintained significant activity in 2025. There are overlaps in the codebase used by both groups as well as the crypto-wallet addresses used by their affiliates. In 2025, Akira also expanded their capabilities to target virtualised infrastructure, likely by leveraging SonicWall[III] vulnerabilities for initial access[19].

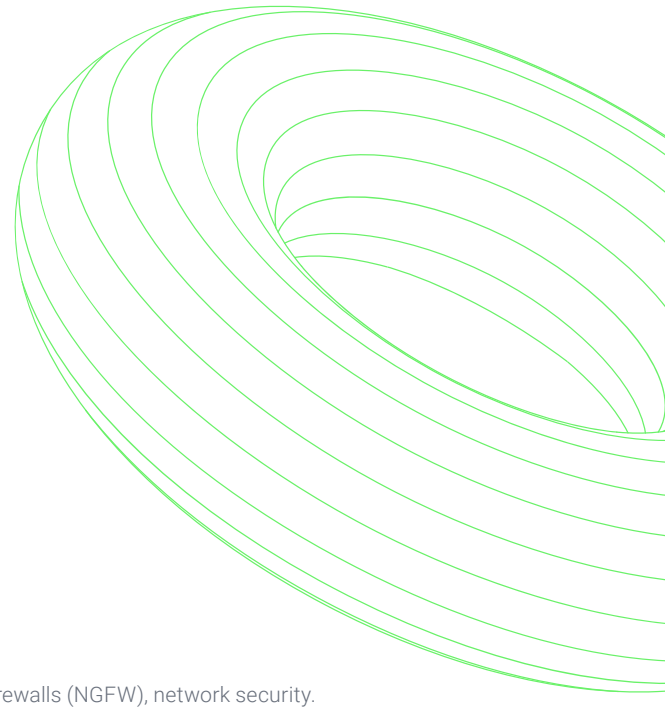
Following its takedown in 2024[20], **LockBit** has made several attempts to rebound in 2025, although with limited success. In May, LockBit suffered a data breach resulting in builds, build configurations and victim negotiation messages being leaked[21]. Since then, its activity dwindled and the number of victims significantly decreased. LockBit 5.0 was released in September, including variants capable of targeting Windows, Linux and VMware. They have updated anti-forensic mechanisms, faster encryption routines, geolocation checks to avoid infecting Russian-language systems, and other features that complicate recovery. The new version is accessible for a little over EUR 400 (USD 500)[22].

DragonForce, a largely Russian-speaking group active since 2023, stood out in 2025 with a novel business model, capabilities and competitive approach[IV]. DragonForce offers different payloads, assembled from Conti and LockBit leaked codebases, and allows affiliates to build different variants for targeting Windows, Linux, VMware and other platforms. In August, a new extortion service was announced, offering exfiltrated data analysis and the creation of tailored extortion materials (e.g. call scripts, draft letters and advice reports), to maximise the pressure on victims. The service fees can be over 20 % of the ransom payment and it is mainly marketed to affiliates targeting high-revenue organisations[23].

In September 2025, a new coalition between DragonForce, LockBit and Qilin was announced on the dark web.

PHOBOS AND 8BASE DISRUPTION[24]

Phobos had been a long-standing RaaS provider with a particularly accessible and adaptable platform, allowing customisation of ransomware campaigns with minimal technical expertise. Taking advantage of the Phobos infrastructure, 8Base developed its own variant. This group had been particularly aggressive in its double extortion tactics, not only encrypting victims' data but also threatening to publish stolen information unless a ransom was paid. Phobos and 8Base declined in activity in 2025, following coordinated international LE actions supported by Europol and the arrests of four individuals of Russian nationality. As a result of this operation, law enforcement was also able to warn more than 400 companies worldwide of ongoing or imminent ransomware attacks.



[III] SonicWall is a cybersecurity company specialised in next-generation firewalls (NGFW), network security.

[IV] Its disputes with the now disbanded RansomHub group saw their leak site being taken out in March 2025 and apparently not having returned by the end of 2025.

Semi-closed groups

Semi-closed affiliate programs are more selective and likely to carry out targeted recruitment on cybercriminal platforms. The core group, made of developers and administrators, seek out skilled, trustworthy and ideologically aligned affiliates to carry out attacks using their platform.

Fog, a ransomware first detected in early 2024, has a modular design, allowing attackers to control the targets and scope of the encryption, content of the ransom note and other aspects of the attack. The group also has a dedicated leaks site and negotiation portal to communicate to victims. Currently it can be classified as a semi-closed group, with operators using shared infrastructure and tactics, techniques, and procedures (TTPs).

BlackBasta was a Russian-speaking group with also roots in Conti[25] that generally used spear-phishing or exploitation of known vulnerabilities to gain access to victims' networks. In 2025, BlackBasta suffered a leak of its internal chat logs, containing a wide range of information, such as phishing templates, cryptocurrency addresses and victims' credentials[26]. The groups leak sites are inactive, but the criminal actors related to BlackBasta are likely to continue their activities under a different brand.

Closed groups

Closed ransomware groups consist of criminal actors who have likely worked together for years and operate with less dependence on CaaS. They develop their own malware and sometimes exploits, use closed communication channels, host much of their own infrastructure, and carry out the attacks themselves. These groups are usually sophisticated and more resilient. As they do not rely on as many commercial criminal services, their identification is more difficult, because their traces are less likely to appear in seized or leaked datasets. They maintain a high level of operational security, and foster stronger trust within their inner circle, further reducing the risk of exposure.

Cl0p is a longstanding closed group known for systematically exploiting zero-day vulnerabilities[27], which resurfaced in February 2025 after a period inactivity.

Play (also known as PlayCrypt) ransomware group continued to be active in 2025. The group has previously targeted critical infrastructure and continues deploying double extortion tactic, with a claimed guarantee on the secrecy of deals[28].

3.3 New hacking coalitions threaten big tech and customer data

In August 2025, the alleged **Scattered LAPSUS$ Hunters (SLSH)** alliance emerged, between Scattered Spider, ShinyHunters and LAPSUS$ hacking collectives. These mostly English-speaking collectives have previously been involved in a range of cybercriminal activities, including online fraud and SIM swapping, high-profile social engineering, insider threat recruitment, data theft and extortion campaigns against major corporations, healthcare and transport providers.

The potential threat of this new coalition is significant, considering the capabilities of the groups' members demonstrated in previous attacks. There are also reports of SLSH members' use of continues harassment and threats, which are not guaranteed to stop even after victims' ransom payments[29]. Some members of the three groups also appear to be tied to E2EE channels used by The Com network, engaged in real-life violence, CSE and violent extremism, which further indicates the fluidity between online criminal communities (read more in the chapter on Child Sexual Exploitation)[30].

Scattered Spider emerged around 2022 and became known for their high-profile social engineering attacks used to infiltrate corporate networks and extorting their victims, as well as online fraud and SIM-swapping activities. In 2023, Scattered Spider members claimed to have acted as an initial access broker (IAB) against UK and US corporations via the ALPHV/BlackCat ransomware affiliate group. The group was also responsible for the cyber-attack against Transport for London in 2024, as well as for extorting many UK retail and US healthcare providers[31].

LAPSUS$ started their activities in 2021 as a small but notorious extortion-focused group that used spear-phishing, SIM-swapping and insider recruitment techniques to breach major tech firms like Microsoft, Samsung NVIDIA, Okta, T-Mobile, Uber, Rockstar Games and many others[32]. In 2022, several members were arrested by the City of London Police in connection to these attacks, which led to the group going dormant.

ShinyHunters is known for their large-scale data theft and extortion campaign against major tech companies. In May 2025, ShinyHunters launched a social engineering campaign that siphoned over a billion Salesforce customer records by tricking victims to connect a malicious app to their organisation's Salesforce portal[33].

3.4 Infostealers continue to cater for the cybercrime market

Infostealers persisted as a key enabler for the entire spectrum of cyber-attacks in 2025. Infostealers cater to a broad illicit market of cybercriminals ranging from IABs and ransomware affiliates to fraudsters[34].

TARGETING CYBERCRIMINAL ENABLERS THROUGH GLOBAL PARTNERSHIPS

Continued iterations of the Europol-coordinated operation Endgame successfully disrupted infrastructure and criminal actors in the CaaS environment. This included the Smokeloader botnet[35], which was run as a pay-per-install service and enabled criminals to access to victims' machines for illicit activities, ranging from keylogging to the deployment of ransomware and cryptominers.

Another action in May, targeting initial access malware services, dismantled Bumblebee, Lactrodectus, Qakbot, Hijackloader, DanaBot, Trickbot and Warmcookie malware strains[36]. Around 300 servers were taken down worldwide, 650 domains neutralised, and international arrest warrants issued against 20 targets.

In November, Endgame targeted infostealers Rhadamantys, VenomRAT and the Elysium botnet. More than 1 000 servers worldwide were taken down or disrupted and the main suspect behind VenomRAT arrested in Greece[37]. The dismantled malware infrastructure consisted of hundreds of thousands of infected computers containing millions of stolen credentials.

The success of LEAs actions against key enablers also relies on contributions from the private sector, providing technical support to the takedown, as well as infrastructure identification and mapping.

3.5 DDoS attacks pose a hybrid threat

Sustained by the wide availability of modular stressor and booter service[V] offerings, DDoS attacks remain a threat. They are often state-sponsored and driven by ideological motivation[38], but also deployed as a means to extort victims or undermine competitors in the criminal ecosystem[39]. Targets include governments, critical infrastructure and high-impact economic sectors. While effective mitigation measures are generally in place and the impact is often low, the relatively minimal effort needed to launch this kind of attacks makes it an effective and sustainable strategy for continuous destabilisation.

DDoS attacks carried out in connection with global events of political significance, such as the June 2025 NATO Summit[VI], contributed to instil a sense of insecurity in society and undermine public confidence in institutions.

[V] Tools designed to test the stress resistance of a network to see if the resources designated to it (e.g. bandwidth, CPU) can withstand additional load.

[VI] During the 2025 NATO Summit, held in The Hague, Netherlands on 24-26 June 2025, several entities experienced DDoS attacks, including websites of summit side events, international organisations, regional transport companies, platforms used for public announcements by regional Dutch authorities and the municipality of The Hague. More information available at https://www.ncsc.nl/waarschuwing/ddos-aanvallen-op-nederlandse-organisaties-rondom-navo-top-0 ; https://www.icc-cpi.int/news/icc-detects-and-contains-new-sophisticated-cyber-security-incident

PRO-RUSSIAN CYBERCRIME NETWORK NONAME057(16)

Mainly Russian-speaking, a network called NoName057(16) known to be targeting governments and corporations, was operating around a core group of individuals based in Russia, with several followers not necessarily technically skilled and located in various countries, including the EU.

In July 2025, as part of Operation Eastwood, coordinated by Europol and Eurojust, and supported by ENISA, the infrastructure of the network was disrupted, followed by a number of international arrests[40]. The countries involved were Belgium, Canada, Czechia, Denmark, Estonia, Finland, France, Germany, Italy, Latvia, Lithuania, Netherlands, Poland, Romania, Spain, Sweden, Switzerland, Ukraine, and the United States.

Following the disruption of the network infrastructure, a decline in activity of the NoName057(16) was initially seen, however capability was quickly recovered and their activity resumed. More recently, the group appears to be moving towards exploring and more impactful attacks, including against industrial control systems.

NONAME057(16) OPERATION **EASTWOOD**

WHAT CRIMINAL ACTIVITIES ARE WE STOPPING?

This operation targeted the criminal network NoName057(16), linked to **73** DDoS attacks per day of Ukrainian private and public actors.

6032 < UNIQUE HOSTS ATTACKED />

674 < PUBLIC WEBSITES ATTACKED />

5358 < PRIVATE WEBSITES ATTACKED />

19 < COUNTRIES INVOLVED />

200 < POLICE OFFICERS INVOLVED />

24 < HOUSE SEARCHES />

+100 < SERVERS DISRUPTED WORLDWIDE />

9 < ARRESTS WARRANTS ISSUED, 2 OF THEM EXECUTED />

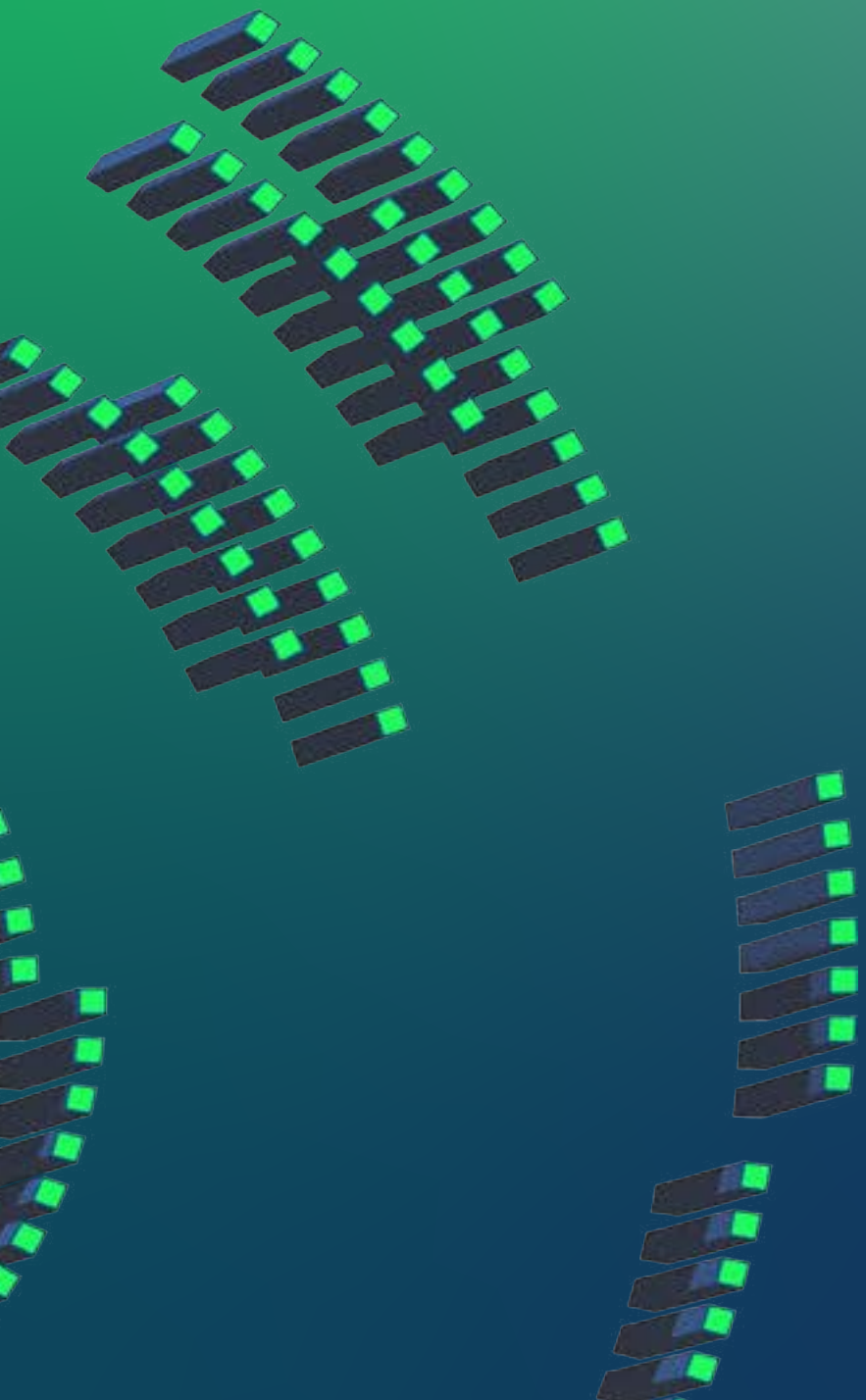
5 < EU MOST WANTED />

13 < INDIVIDUALS QUESTIONED />

+1000 < SUPPORTERS NOTIFIED FOR THEIR LEGAL LIABILITY />

< MAIN INFRASTRUCTURE TAKEN OFFLINE />

ONLINE CHILD SEXUAL EXPLOITATION



04

Key Developments

- Extortion remains a key threat linked to CSE, with child victims manipulated into sending money, producing more sexual content and committing violent acts, including self-harm, to comply to the demands.
- Trade in child sexual abuse material (CSAM) for financial gain is increasing. While live-distant child abuse (LDCA) remains a persistent threat, financial sexual extortion continues to surge. More platforms selling CSAM are identified, along with scam sites related to the sale of CSAM.
- AI-generated CSAM is increasingly being detected, creating additional difficulties in the analysis of CSAM, victim identification, investigative capacity as well as regulatory challenges.
- E2EE messaging applications have become a prominent communication environment for CSE offenders, for grooming, exchange of CSAM, communication and networking, as they are fully aware of the difficulties that LEAs have in obtaining the data exchanged via these applications.

The evolution of the threat posed by CSE continued to be influenced by technological advancements. Offenders show exceptionally quick adaptation to new technologies, both to expand and make more efficient the criminal process, but also as a countermeasure against LE detection.

4.1 Sexual extortion cases continue to spike

Sexual extortion continues to be a major threat linked to CSE. It takes place in many shapes and it is perpetrated by several types of offenders who are moved by different motives, targeting an ever-increasing number of underage victims, with extremely serious consequences.

In 2025, the online distribution of self-generated sexual material from children continued to be a cause of concern. Even when it is not the result of a criminal process of manipulation, it often leads to several forms of CSE. Once the image is shared, the child depicted loses control over it and it can be re-distributed, traded, manipulated or posted on CSE platforms, with the risk to remain online for years. Such images are also often weaponised against the child and used as a leverage for sexual extortion, aiming either at sharing more explicit pictures or at obtaining money (financial extortion).

Both the amount of self-generated sexual images circulating online and the number of sexual extortion cases reported are constantly spiking in volume. Similar to previous years, the number of CyberTips reports related to financial extortion received by NCMEC between January and June 2025 increased by about 70%[I] in comparison with the same period the year before[41]. Such offences have serious consequences in children who are pressured psychologically and financially, with demands in many cases persisting also after demands are met. This process strongly impacts children who feel overwhelmed, ashamed and scared, and often do not seek for help.

[I] The number of reports went from 13 842 in the first six months of 2024 compared to 23 593 in 2025.

PREVENTION AND SUPPORT FOR VICTIMS: HELP4U[42]

Prevention and support for victims are key to mitigate online sexual abuse and CSE. Help4U is a digital platform created by Europol and the research centre CENTRIC to support children and teenagers who are facing online sexual abuse or other harmful online behaviour. It was launched in November 2025 as part of Europol's broader public-awareness and victim-support work on online child sexual exploitation.

Help4U is designed mainly for minors who feel unsafe online, for example because someone is pressuring them for sexual content, sharing their images without consent, or otherwise abusing them. Minors can use it to find local support services, get guidance in private at their own pace, and, in some countries, connect with professionals who can listen and help them move towards safety and recovery. It centralises trusted information on rights, online safety, and practical next steps (such as preserving evidence, blocking/reporting offenders, and seeking help) in clear, age-appropriate language. The platform also provides tailored information for parents, teachers, and other professionals who support young people affected by online sexual exploitation.

Help4U began as a pilot project between Belgium, Germany, Ireland, the Netherlands and Slovenia, and now includes Bulgaria, Croatia, Cyprus, Greece, Hungary, Italy, Portugal, Spain and Romania, with more countries expected to join in 2026.



4.2 Shifting offender behaviour: monetisation of CSAM

Networking, coordination and CSAM exchange among CSE offenders have traditionally relied on trust-based relationships. As a form of countermeasure against LE detection and social stigma, perpetrators tend to form relatively closed, reputation-driven communities where access and exchange are governed by social ties, status, and long-term interaction. This applies mostly for offenders driven by sexual interest towards children, while a minority of perpetrators have been carrying out and/or facilitating CSE offences operating in an opportunistic way, driven by financial gain.

Nevertheless, a significant shift towards CSAM monetisation appears to be influencing also offenders' behaviour, as CSE offenders are not anymore operating only within trusted circles and new types of offences and infrastructure continue to emerge.

Several new platforms selling CSAM have been identified and investigated throughout 2025. Many of the platforms advertised as solely dedicated to the sale of CSAM appear to be OFS sites. Users are able to access only content previews of CSAM or a limited amount of CSAM freely available on the site front page, while an upfront payment (usually in cryptocurrency) supposedly provides access to exclusive content. Once the user pays or submits the CSAM, they do not receive anything or receive access credentials that do not work.

KIDFLIX: A CSAM STREAMING PLATFORM ON THE DARK WEB

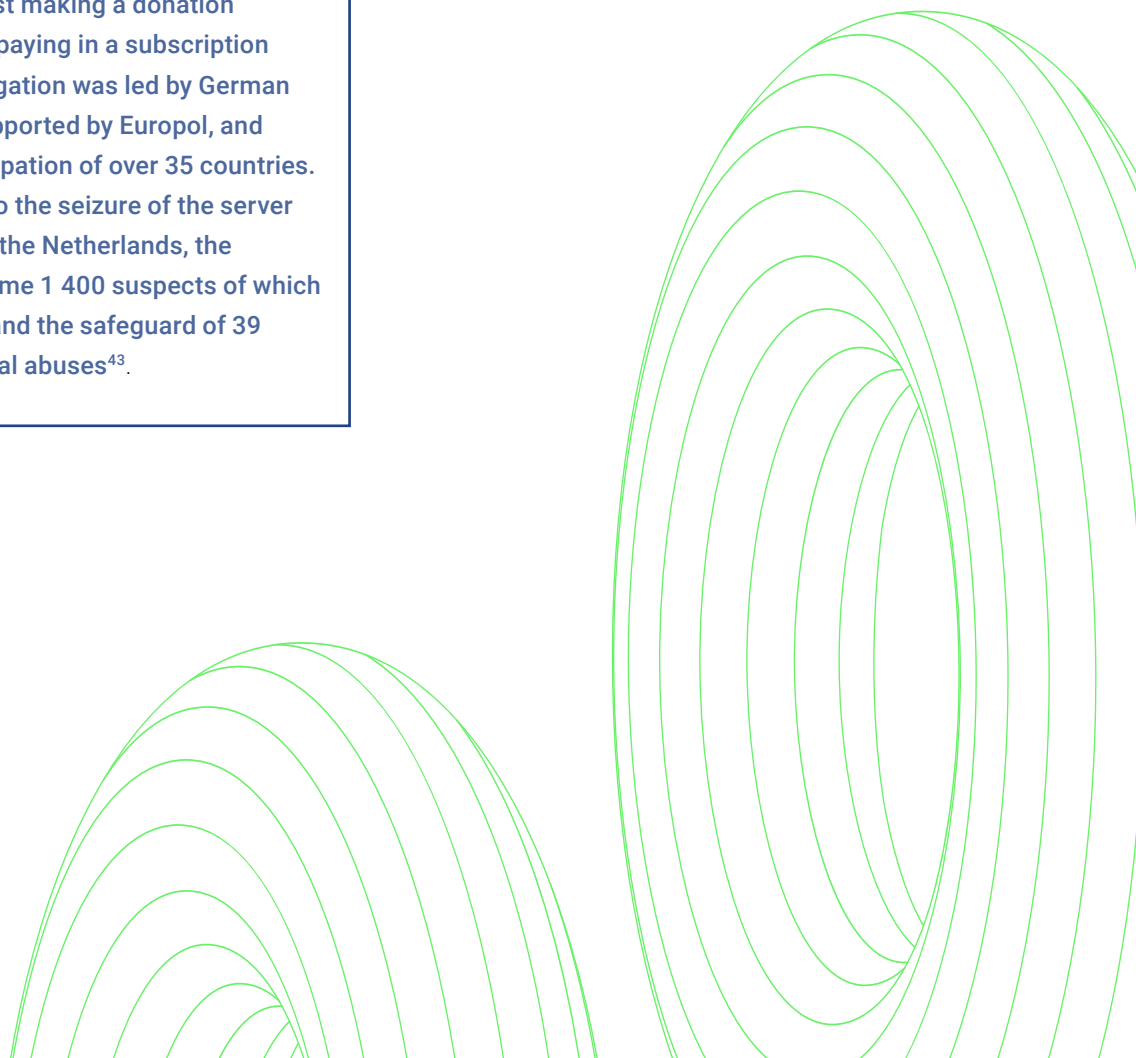
Kidflix was a CSAM streaming platform on the dark web, taken down by LE in 2025. During its activity from 2021 to 2025, the platform had more than 1.8 million users registered and about 80 000 uploaded videos. There were different types of account: basic, premium and admin. With a basic account, users had access only to previews or videos of low quality. Gaining access only required setting up an account with a new username and password. To get full access users needed to obtain a premium account, which could be obtained in exchange for activity on the platform (upload videos, like, rate or comment content). By performing these activities, users would obtain digital coins, called 'candies', and after gaining a certain amount, they would obtain a premium account.

The second possibility was to pay in cryptocurrency, first making a donation and then continue paying in a subscription model. The investigation was led by German authorities and supported by Europol, and involved the participation of over 35 countries. These efforts led to the seizure of the server that was hosted in the Netherlands, the identification of some 1 400 suspects of which 79 were arrested, and the safeguard of 39 children from sexual abuses[43].

Live Distant Child Abuse: a persistent criminal activity in the EU

EU-based consumers mostly purchase live-streamed CSAM of abuses happening in non-EU countries, but cases of CSAM made of victims abused in the EU are also reportedly sold among EU consumers.

The Philippines continues to be a hotspot for LDCA, probably partly influenced by the widespread fluency in English and fast and reliable internet connection in the country. In addition, it is most likely related to established cooperation mechanisms in place and an enhanced national effort in combating CSE. Intelligence suggests that many victims are located in other regions, however these instances remain under-detected. Prices of live-streaming sessions are relatively low, leading to frequent and repeated abuse of victims.



4.3 E2EE applications for networking and exchange of CSAM

An ever-increasing number of group chats dedicated to CSE is hosted on E2EE messaging applications. These applications allow for networking, exchange of CSAM and victims' grooming. A high amount of first-generation CSAM has been identified in investigated groups. E2EE provide high protection from LE scrutiny and given their easy accessibility, they allow for a larger userbase, including offenders who wouldn't have neither the technical capabilities nor will to access the dark web or other environments.

Similar to known patterns in forums in the dark web, these groups operating on E2EE facilitate not only networking and the exchange of CSAM, but also function as 'education' environments, where offenders freely exchange best practices on abuses and countermeasures. In order to avoid LE infiltration, many of these groups have vetting systems for new members who want to join the group. Groups sometimes migrate from one app to another to diversify communication channels, but also if there are suspicions that the hosting application cooperates with the authorities.

THE COM NETWORK AND THE LINKS WITH CSE

Interconnected with the CSE criminal landscape, online communities under the umbrella of **The Com** network pose an extremely serious threat to children and society as a whole. The criminal endeavours carried out by these online communities are multiple, creating a complex landscape where CSE, cyber-attacks, extortion, assault, rape, murder, and violent extremism intertwine. The network is extremely dangerous and combating it is a national priority in several MS and third countries[II].

These networks are largely composed of children, aged between 8 and 17. At the core of their activities lays manipulation and violence, which are a constant feature. There is a full range of individual motivations to join such communities, with some actors engaging in criminal activity for sexual gratification, social reward or a sense of belonging[44]. Some members are driven by a wish to cause fear and chaos, justifying their criminal actions with ideological belief systems. In many cases, the drivers for engagement in the network's criminal activities replicate those that appear in gaming environments.

Offenders often target potential victims on gaming platforms popular among children, and in some cases even on channels used by youth to discuss mental/physical difficulties. Vulnerable children are then groomed on social media and messaging applications with the love-bombing technique. Once sensitive information and compromising images are shared by the victim, the perpetrator uses those to force the child into producing more self-generated sexual material or perform and capture any other violent acts against themselves or others.

The extreme violence, the tremendously high mental and physical health impact on victims, the joining of different criminal activities and actors, and the many investigative challenges linked to data access and E2EE applications, make this online phenomenon particularly threatening. By constantly shifting their activities between different digital spaces and E2EE channels, The Com remains elusive and expands its influence and reach.

[II] For example, in December 2025, Canada formally designated the 764 network (including Maniac Murder Cult and Terrorgram Collective) as a terrorist entity defining it a transnational ideologically motivated violent extremist network. This listing grants law enforcement enhanced powers to counter it. https://www.canada.ca/en/public-safety-canada/news/2025/12/government-of-canada-lists-four-new-terrorist-entities0.html

4.4 Production of synthetic CSAM is on the rise

The rapid evolution of AI tools and the ease of access to them has created more advanced opportunities for offenders, improving the quality of their grooming techniques and scaling up the production of CSAM with the introduction of **AI-generated material.** Investigations on AI-generated material have already emerged, with the identification of platforms made of international communities of offenders dedicated to the production and distribution of synthetic CSAM, where they also exchange of technical skills to improve quality, ready-made prompts, as well as operational security tips.

The accessibility of AI tools has multiplied the volume of CSAM available online, creating additional challenges in the analysis of imagery and identification of offenders. There are two main types of AI-generated CSAM, either fully synthetic or partially synthetic. The latter is usually generated with image-to-image models that are able to modify existing images and produce AI-altered CSAM.

Fully synthetic images are usually generated with text-to-image models, where the user inserts a prompt and obtains the desired image. Text-to-video models have emerged, following the rapid development of text-to-image models. In order to overcome content moderation and obtain accurate results, AI-generated CSAM is often produced in offline models trained with authentic sexual abuse material. Bots editing images to produce synthetic CSAM have also been detected in E2EE groups.

MONTHLY SUBSCRIPTION TO AI-GENERATED CSAM

A subscription business that gave paying customers access to high-quality AI-generated CSAM as well to exclusive communities of AI offenders was created and managed by a 28-year-old suspect, who was also producing AI-generated CSAM and distributing it on the online platform. The exclusive community of AI offenders had around 1 500 members who were exchanging tips on how to best exploit technology to obtain CSAM and how to avoid detection. Customers were from 29 countries worldwide. The platform's administrator was firstly arrested in Denmark in 2024, in an investigation led by Denmark and supported by Europol and the J-CAT, with the involvement of 19 countries. Further coordinated actions in 2025 resulted in the identification of 273 suspects and 25 arrests worldwide[45].

Looking ahead

The cybercrime landscape will continue to present LEAs with an array of evolving challenges, making a proactive and strategic approach more necessary than ever. In the coming years, law enforcement's ability to tackle cybercrime will depend on its capacity to harness innovative technologies, to be able to lawfully access critical data, and to collaborate more closely with the private sector. Below some examples of how the future of cybercrime might look like.

The rise of autonomous cybercrime

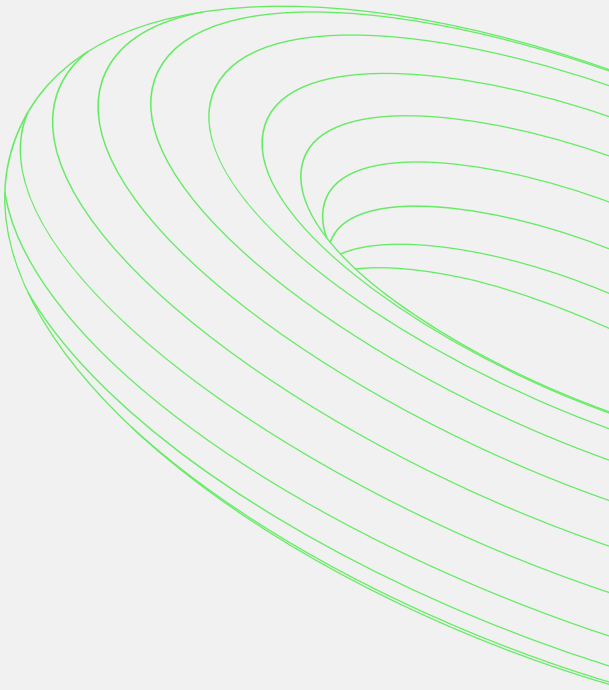
Cybercrime actors have already begun leveraging agentic AI systems capable of autonomously conducting entire criminal workflows with little to no human involvement. As adoption accelerates, these systems will further enable offenders to distance themselves from illicit operations, transforming cybercrime into an increasingly intangible and evasive threat.

Hybrid threats, between ransomware and hacking coalitions

The relationships between state-sponsored hybrid threats and cybercrime actors will continue to pose challenges to society as a whole. DDoS attacks will likely continue to be used as a means to undermine public confidence and trust in governments' ability to protect their citizens and critical infrastructure, instilling insecurity and triggering political instability. The cyber-attacks landscape will likely remain dynamic, with the emergence of hacking coalitions targeting governments, private companies and customers' data, and carrying out cyber-attacks as well as fraud schemes.

More synthetic CSAM and abuse of E2EE

Synthetic CSAM will further expand the variety and severity of child sexual exploitation, exposing victims to deeper and longer-term harms. Social media platforms are likely to remain crucial environments for CSE offenders, and the widespread adoption of E2EE by popular tech companies will continue to thwart swift and effective detection and referral mechanisms. The fight against CSE and online violent extortion networks will be increasingly challenged by the availability of decentralised platforms, which offer high levels of privacy and minimal monitoring.



Online fraud: AI-driven schemes and resilient networks

OFS are expected to continue leveraging AI for various aspects of the criminal process, from sophistication of social engineering to infrastructure management. AI-driven fraud will mean simultaneous multi-tasking, and replacing labour-intensive operations with autonomous digital workforce. On the other hand, the resilience of online fraud networks - especially those relying on CaaS - is based on their ability to legally purchase and activate SIM cards in bulk. As long as bulk purchasing and registration protocols are possible, networks will be able to regenerate their infrastructure indefinitely. Countering the use of SIM boxes requires robust anti-spoofing measures and enhanced identity verification processes in the telecommunications industry.

Cybercrime and financial enablers

Cybercriminals' use of exchange services in non-EU jurisdictions with loose anti-money laundering (AML) standards continues to create barriers to international cooperation. A fragmented regulatory landscape for cryptocurrency oversight impedes authorities' coordination across borders, resulting in enforcement gaps and reduced accountability. In addition, the integration of neo-banks into criminal operations reflects the evolution of criminals' fintech abuse. Strengthening LEAs power of action against services that are non-compliant with current EU AML regulations is therefore paramount.

Appendix

METHODOLOGY

The Internet Organised Crime Threat Assessment (IOCTA) is a strategic analysis report providing an assessment of the latest threats and the impact of cybercrime to the EU. The report provides a law enforcement centric view of the threats and developments related to cybercrime, in order to inform decision-makers at strategic, policy and tactical levels in the fight against cybercrime, and with a view to updating the operational focus for EU law enforcement authorities.

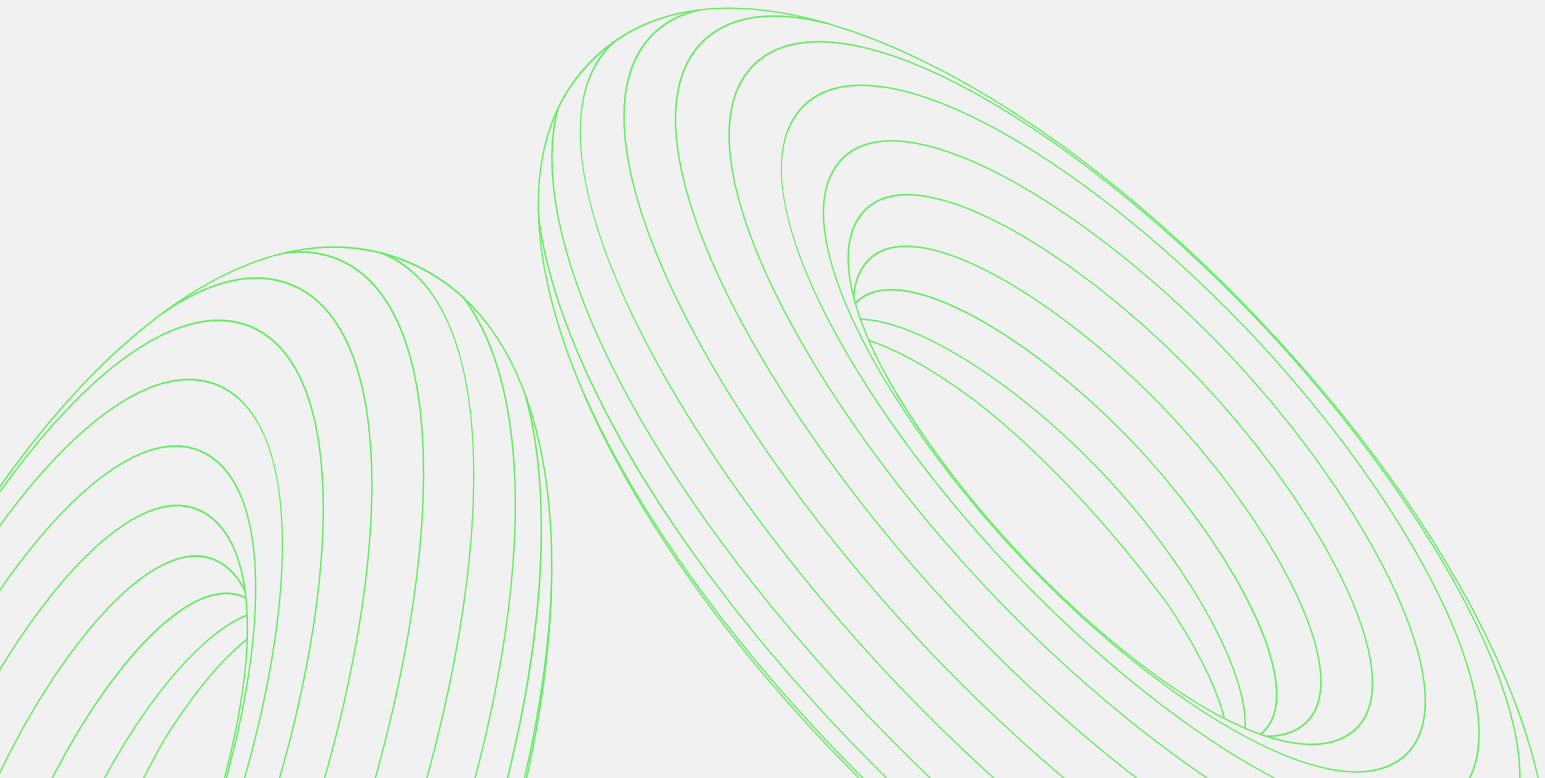
Europol's first threat assessment on Internet Facilitated Organised Crime was published in 2011. Since then, the threat assessment is a regular product issued on a yearly basis.

The assessment of the threat is based on a set of indicators established by Europol, focusing on developments related to criminal actors and networks, criminal processes, infrastructure used, financial transactions, and the impact on society.

SOURCES

Criminal intelligence stemming from operational activities supported by Europol's European Cybercrime Centre (EC3) constitutes the core dataset for the analysis. EU Member States and operational cooperation partners contribute this information to Europol, which is continuously monitored, thoroughly analysed and enriched by additional sources. The criminal intelligence is related to major investigations supported by Europol in 2025.

Additionally, the assessment draws on the knowledge and expertise of subject matter experts from EC3. The collected data consists primarily of qualitative information complemented by internal and external reports and open-source information.



Abbreviations

2FA Two-factor Authentication

2G Second Generation

AI Artificial Intelligence

AML Anti-Money Laundering

AMM Automated Market Makers

AP Analysis Project

ATO Account Takeover

BEC Business Email Compromise

C2 Control-and-Command

CaaS Crime-as-a-service

CEO Chief Executive Officer

CSAM Child Sexual Abuse Material

CSE Child Sexual Exploitation

CSP Communication Service Provider

DDoS Distributed Denial of Service

DeFI Decentralised Finance

DEX Decentralised Exchange

DNS Domain Name System

E2EE End-to-End Encryption

EC3 European Cybercrime Centre

ENISA European Union Agency for Cybersecurity

EU European Union

EUR Euro

IAB Initial Access Broker

ID Identity Document

IMSI International Mobile Subscriber Identity

IP Internet Protocol

J-CAT Joint Cybercrime Action Taskforce

KYC Know Your Customer

LDCA Live-Distance Child Abuse

LE Law Enforcement

LEA Law Enforcement Agency

LLM Large Language Model

ML Money Laundering

MS Member State

NATO North Atlantic Treaty Organization

NCMEC National Center for Missing & Exploited Children

NFT Non-Fungible Tokens

OFS Online Fraud Scheme

OTP One-Time Password

RaaS Ransomware-as-a-service

RDP Remote Desktop Protocol

SIM Subscriber Identity Module

SMS Short Message Service

SOC Serious and Organised Crime

SSL Secure Socket Layer

TOR The Onion Router

USD United States Dollar

USDT United States Dollar Tether

VLOP Very Large Online Platform

VDS Virtual Desktop Service

VPN Virtual Private Network

References

1 Europol, 2025, Steal, deal and repeat - How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

2 Europol, 16 June 2025, Europe-wide takedown hits longest-standing dark web drug market, accessibile at https://www.europol.europa.eu/media-press/newsroom/news/europe-wide-takedown-hits-longest-standing-dark-web-drug-market

3 Europol, 20 January 2025, Law enforcement takes down two largest cybercrime forums in the world, accessible at https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-takes-down-two-largest-cybercrime-forums-in-world

4 ICANN, November 2025, DNS Abuse Mitigation Program, accessible at: https://www.icann.org/dnsabuse

5 Europol, 1 December 2025, Europol and partners shut down cryptomixer. accessible at: https://www.europol.europa.eu/media-press/newsroom/news/europol-and-partners-shut-down-cryptomixer

6 Unit 42, 25 November 2025, The Dual-Use Dilemma of AI: Malicious LLMs, accessible at https://unit42.paloaltonetworks.com/dilemma-of-ai-malicious-llms/

7 Europol, 2025, European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

8 Digital Service Act, 2025, Very large online platforms and search engines, accessible at: https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops

9 Europol 2025, 17 October 2025, Cybercrime-as-a-service takedown: 7 arrested, accessible at https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested

10 European Association for Secure Transactions (EAST), 2025, European Payment Terminal Crime Report, accessible at https://www.association-secure-transactions.eu/intranet/crime-reports/

11 European Association for Secure Transactions (EAST), 2025, Security Update: Data relay attack, accessible at https://www.association-secure-transactions.eu/wp-content/uploads/secure/EAST-EGAF-and-EPTF-Security-Update-2026-001-Data-Relay-Attack.pdf

12 Binance, 2004, Angel Drainer Absorbs Inferno's Toolkit, Becoming a Larger Threat to Crypto Wallets, accessible at https://www.binance.com/en/square/post/15096207996425

13 Europol, 27 October 2025, Position Paper on Caller ID Spoofing, accessible at https://www.europol.europa.eu/publications-events/publications/position-paper-caller-id-spoofing

14 Europol, 17 October 2025, Cybercrime-as-a-service takedown: 7 arrested, accessible at https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested

15 European Commission, 2025, eIDAS Regulation, accessible at https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation; European Commission, 2025, Implementing and delegated acts - PSD 2, accessible at https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/payment-services-directive_en

16 Europol, 2025, European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

17 Europol, 2025, Steal, deal and repeat - How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

18 Checkpoint, 2025, The State of Ransomware – Q2 2025, accessible at https://research.checkpoint.com/2025/the-state-of-ransomware-q2-2025/

19 CISA, Cybersecurity Advisory, #StopRansomware: Akira Ransomware, accessible at https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

20 Europol, 20 February 2024, Law enforcement disrupt world's biggest ransomware operation, accessible at https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

21 Bleeping Computer, 7 May 2025, LockBit ransomware gang hacked, victim negotiations exposed, accessible at https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-hacked-victim-negotiations-exposed/

22 Trend Micro, 25 September 2025, New LockBit 5.0 Targets Windows, Linux, ESXi, accessible at https://www.trendmicro.com/tr_tr/research/25/i/lockbit-5-targets-windows-linux-esxi.html

23 Trend Micro, 29 October 2025, Ransomware Spotlight DragonForce, accessible at https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-dragonforceI

24 Europol, 11 February 2025, Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown, accessible at https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown

25 Intel471, 28 February 2025, Black Basta exposed: A look at a cybcercrime data leak, accessible at https://www.intel471.com/blog/black-basta-exposed-a-look-at-a-cybercrime-data-leak

26 Bleeping Computer, 7 April 2025, Everest ransomware's dark web leak site defaced, now offline, accessible at https://www.bleepingcomputer.com/news/security/everest-ransomwares-dark-web-leak-site-defaced-now-offline/ ; Bleeping Computer, 20 February 2025, Black Basta ransomware gang's internal chat logs leak online, accessible at https://www.bleepingcomputer.com/news/security/black-basta-ransomware-gang-s-internal-chat-logs-leak-online/

27 Ibid

28 CISA, 4 June 2025, Cybersecurity Advisory, #StopRansomware: Play Ransomware, accessible at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a

29 Krebs on Security, 02 February 2026, Please Don't Feed the Scattered Lapsus ShinyHunters, accessible at https://krebsonsecurity.com/2026/02/please-dont-feed-the-scattered-lapsus-shiny-hunters/

30 Krebs on Security, 24 September 2025, Feds Tie 'Scattered Spider' Duo to $115M in Ransoms, accessible at https://krebsonsecurity.com/2025/09/feds-tie-scattered-spider-duo-to-115m-in-ransoms/

31 Krebs on Security, 24 September 2025, Feds Tie 'Scattered Spider' Duo to $115M in Ransoms, accessible at https://krebsonsecurity.com/2025/09/feds-tie-scattered-spider-duo-to-115m-in-ransoms/

32 MSSP Alert, 22 April 2022, Lapsus$ Cyberattack Victim List: Globant, Microsoft, Nvidia, Okta, Samsung, T-Mobile, accessible at https://www.msspalert.com/news/alleged-lapsus-cyberattack-victim-list-grows-microsoft-nvidia-okta-samsung-more

33 Picus Security, 20 October 2025, Scattered LAPSUS$ Hunters: 2025's Most Dangerous Cybercrime Supergroup, accessible at https://www.picussecurity.com/resource/blog/scattered-lapsus-hunters-2025s-most-dangerous-cybercrime-supergroup ; Krebs on Security, 7 October 2025, ShinyHunters Wage Broad Corporate Extortion Spree, accessible at https://krebsonsecurity.com/2025/10/shinyhunters-wage-broad-corporate-extortion-spree/

34 Europol, 2025, Steal, deal and repeat - How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

35 Europol, 2025, Press Release https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-follow-leads-to-five-detentions-and-interrogations-well-server-takedowns

36 Europol, 2025, Operation ENDGAME strikes again: the ransomware kill chain broken at its source, accessible at https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source

37 Europol, 13 November 2025, End of the game for cybercrime infrastructure: 1025 servers taken down, accessible at https://www.europol.europa.eu/media-press/newsroom/news/end-of-game-for-cybercrime-infrastructure-1025-servers-taken-down

38 Europol, 2025, European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

39 Cloudflare, 15 July 2025, Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS threat report, accessible at https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/

40 Europol, 16 July 2025, Global operation targets NoName057(16) pro-Russian cybercrime network, accessible at https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network?utm

41 National Center for Missing & Exploited Children (NCMEC), 2025, Spike in online crimes against children a "wake-up call", accessible at https://www.missingkids.org/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call

42 Europol, 2025, Help4U: A lifeline for young people facing online sexual abuse, accessible at https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/help4u-lifeline-for-young-people-facing-online-sexual-abuse

43 Europol, 2025, Global crackdown on Kidflix, a major child sexual exploitation platform with almost two million users, accessible at https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users

44 FBI, 2025, Public Service Announcement, Violent Online Networks Target Vulnerable and Underage Populations Across the United States and Around the Globe, accessible at https://www.ic3.gov/PSA/2025/PSA250306

45 Europol, 2025, 25 arrested in global hit against AI-generated child sexual abuse material, accessible at https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material





This publication and more information on Europol are available on the Internet.

www.europol.europa.eu






1897
KT16 LNO

OPEN SOURCE TOOLS, COMPUTER FORENSICS IN THE “CLOUD”

#DIGITALISATION and #ARTIFICIALINTELLIGENCE in Criminal Justice

Internet Fundamentals, Digital Investigations and AI



Seanpaul Gilroy

Senior Digital Forensic Investigator

Co-funded by the European Union

About Me

- Senior Digital Forensic Investigator at Northumbria Police
  - Manage a team of Digital Forensic Investigators & technicians
  - Support Investigators with Digital Forensic Strategies
  - Based in Newcastle Upon Tyne, England
  - Worked in the field of Digital Forensics for 12 years
- Deliver training inputs to both new and existing police officers on a regular basis:
  - Seizure of digital evidence and best practice
  - Analysis of digital evidence & digital forensic opportunities

What will we discuss?

- Overview of open source Investigations
- Protecting your privacy during open source investigations
- Tracing domain name owners, the origin of an email and email blacklists
- Geo-location tools for open source Investigations
- Investigating Web 2.0 – social networking, blogs and online gaming

REMINDER

- All of the techniques shown in this presentation are to demonstrate the ability to locate information during OSINT investigation
- Be aware of local legislation when considering the use of any of these techniques
- I'm not an expert in law
  - As part of my role I work with specialists in legislation (RIPA, DSA, TEI) when considering investigative techniques
- AI Warning – Data may be stored by the AI application to train AI models.





Overview of Open Source Investigations

WHAT IS OPEN SOURCE?

*"The collection, evaluation and analysis of materials from sources **available to the public** whether on payment or otherwise **to use as intelligence or evidence within investigations**"*

National Police Chiefs Council (NPCC)

DIGITAL FORENSICS

- Digital Forensics has developed rapidly over the past few years
- Traditionally, digital forensics has been referred to as "**dead box forensics**"
- A Digital Forensic Investigator will encounter an array of different devices on a case-by-case basis
    - Dynamic field, adapting to new technologies



To understand the importance of opensource investigations, it is beneficial to understand the Digital Forensic Lifecycle

Digital Forensic Investigation Lifecycle

From Device Seizure to Evidential Reporting

PRESERVE
INVESTIGATE
DISCLOSE
ACHIEVE JUSTICE

1 Device Seizure

SECURE AND PRESERVE



- Device secured and documented
- Preservation strategy initiated
- Network isolation considered to protect evidential integrity

2 Pre-Acquisition Assessment

RECORD AND ASSESS



- Device condition documented
- Photographs captured
- Device identifiers recorded (e.g. IMEI, serial number)
- Initial evidential assessment completed

3 Data Acquisition

EXTRACT AND MAINTAIN INTEGRITY



- Forensic extraction performed (logical, file system or physical)
- Data integrity maintained throughout the process (e.g. hashing)
- Device remains isolated from the network to prevent remote data changes

4 Analysis & Review

INTERPRET AND IDENTIFY



- Artefacts examined and interpreted
- Investigative opportunities identified (e.g. timelines, links, patterns)
- Findings assessed against investigative objectives

5 Reporting & Disclosure

PRESENT AND SUPPORT JUSTICE



- Findings documented in a clear, structured report
- Evidential reports produced for disclosure
- Material prepared for judicial processes (e.g. court, disclosure, case files)

1 Device Seizure & Isolation

Mobile device is seized and placed in an isolated state (no network connectivity).

2 Offline Forensic Acquisition

Forensic tools extract data from the device's internal storage while it remains offline.

3 Cloud Services Not Accessible

Network isolation prevents access to cloud-based data and online services.



ISOLATED FROM NETWORK SERVICES

CELLULAR | WI-FI | BLUETOOTH

Recovered Local Evidence

Data successfully extracted from the device's internal storage

- SMS / MMS Messages ✓
- Call History ✓
- Contacts ✓
- Device Photos & Videos ✓
- Local Documents ✓
- Installed Applications and App Data ✓

Potentially Unavailable Evidence

Cloud-based data is not collected during offline acquisition

- Cloud-stored Photos & Videos
- Social Media Activity
- Cloud Backups
- Account Activity Logs
- Location History
- Synced Messages (e.g. email, IM, social media)
- Shared Files & Documents
- Other Cloud-stored Data

KEY MESSAGE

Traditional mobile forensic acquisitions focus on artefacts stored locally on the handset.

When devices are examined in an isolated state, investigators may not identify or preserve potentially valuable cloud-based evidence, including remotely stored communications, media, location history and account activity.

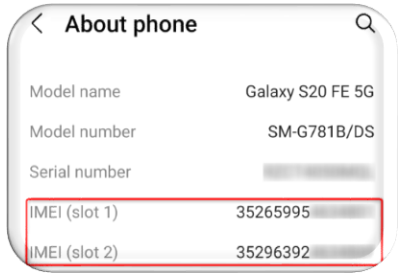
COLLECT
PRESERVE
UNDERSTAND
ACHIEVE JUSTICE



Protecting your privacy during open source investigations

PROTECTING YOUR PRIVACY ONLINE

- The use of technology records a vast amount of information as part of its functionality, primarily to improve the user's experience



Device details (Device make, model, serial number, IMEI)



Device name



Location Data (longitude and latitude)



Usernames/passwords



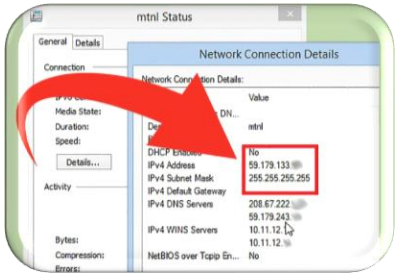
Internet History



Download history



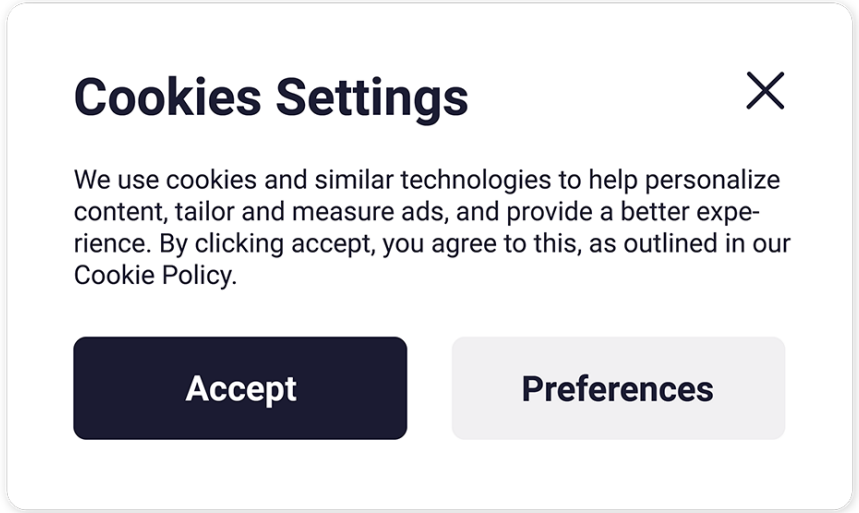
Social media information



IP Address

PROTECTING YOUR PRIVACY ONLINE

- Cookies during OSINT investigations may reveal our identity
  - Cookies are small text files created and stored on your device after visiting a website
  - Used to store information about your use on that website, such as the items in your basket
- It is important that we protect our identity when conducting open source investigations



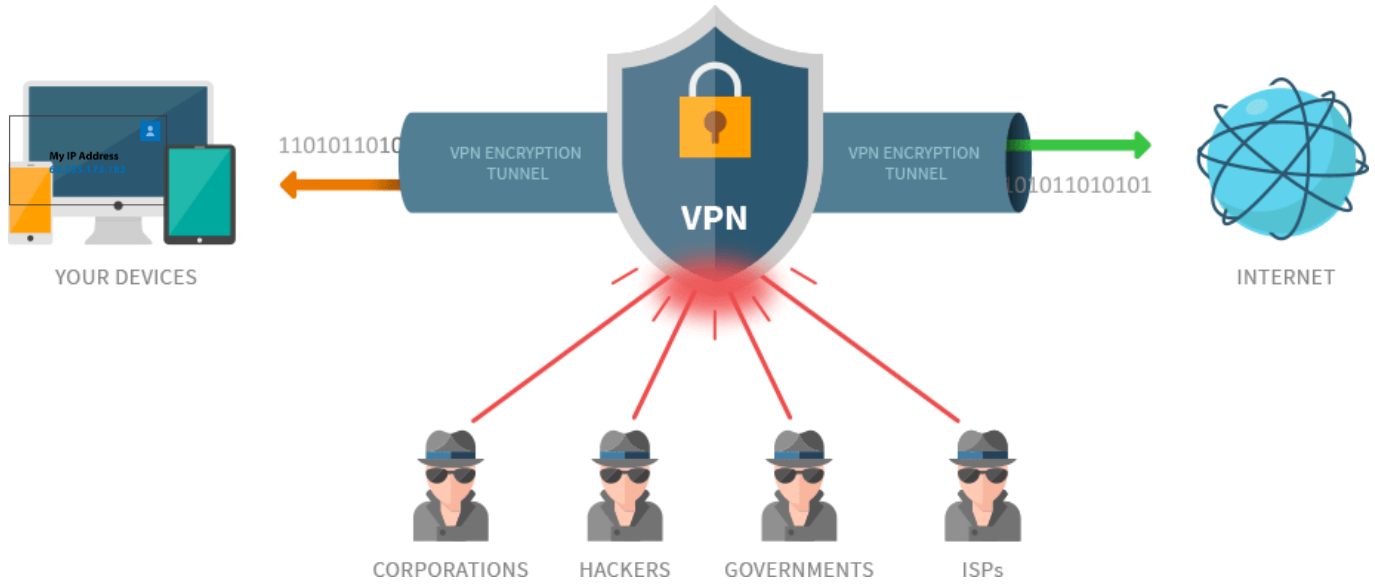
IP ADDRESS EXERCISE

- **Step 1)** Visit Google
- **Step 2)** Search "What's my IP"
  - Google will usually display your IP address, if not it will list a number of free tools which may help
  - https://www.whatismyip.com is one of many tools which are available
  - Make a note of your IP address
- **Step 3)** Visit GeoIP2 Databases Demo | MaxMind
- **Step 4)** Enter your IP address in the GeoIP2 precision service search box and press go

ddress	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain	Connection Type
.53.75	Gateshead, England, United Kingdom (GB), Europe	86.22.52.0/22	NE9	54.9313, -1.5855 (5 km)	Virgin Media	virginm.net	Cable/DSL

VIRTUAL PRIVATE NETWORKS

- VPN stands for **V**irtual **P**rivate **N**etwork
- VPN is an encrypted connection between a device (Computer) and a network (The Internet)
- VPN providers often don't keep logs,
  - preventing requests for information from the police and other organisations
- Using a VPN is an easy way of hiding your IP address (Return address on a letter) from people.



VIRTUAL PRIVATE NETWORKS

- Each VPN will advertise their own benefits:
  - Download Speeds
  - Bandwidth Limits
  - Number of connections
  - Supported Devices
  - Torrent Support
  - Streaming support
- There are numerous VPN providers on the market
  - Some VPN's are free, others charge a subscription fee



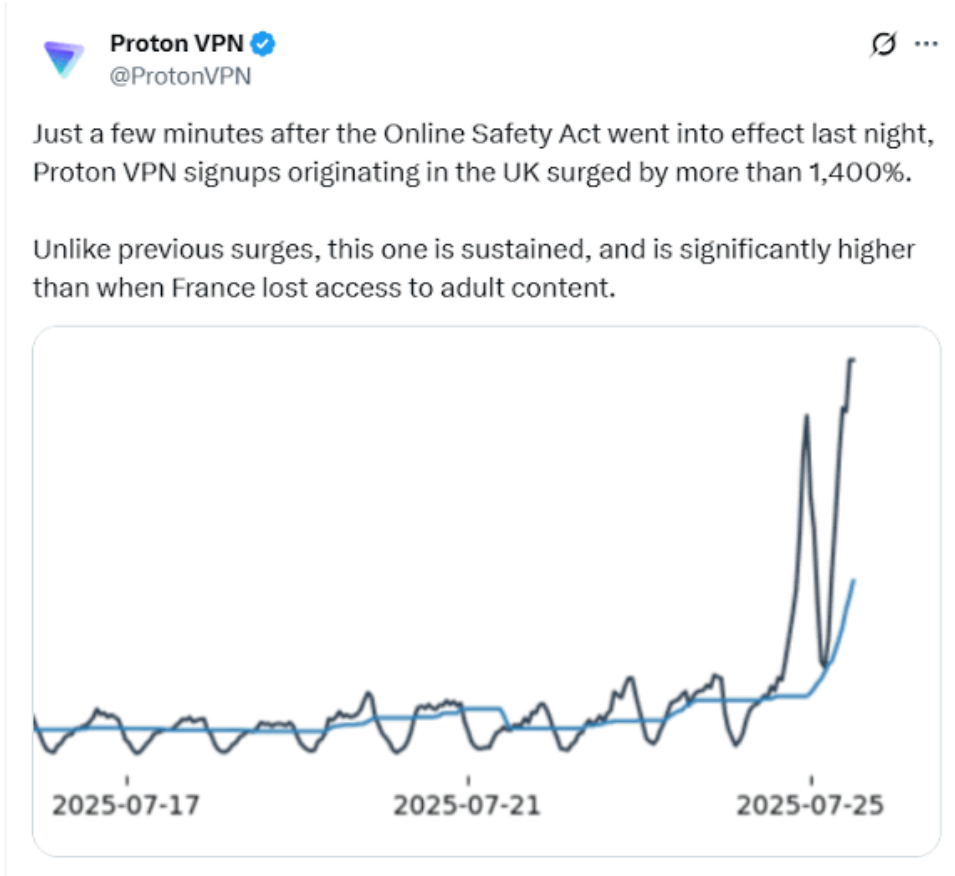




VIRTUAL PRIVATE NETWORKS

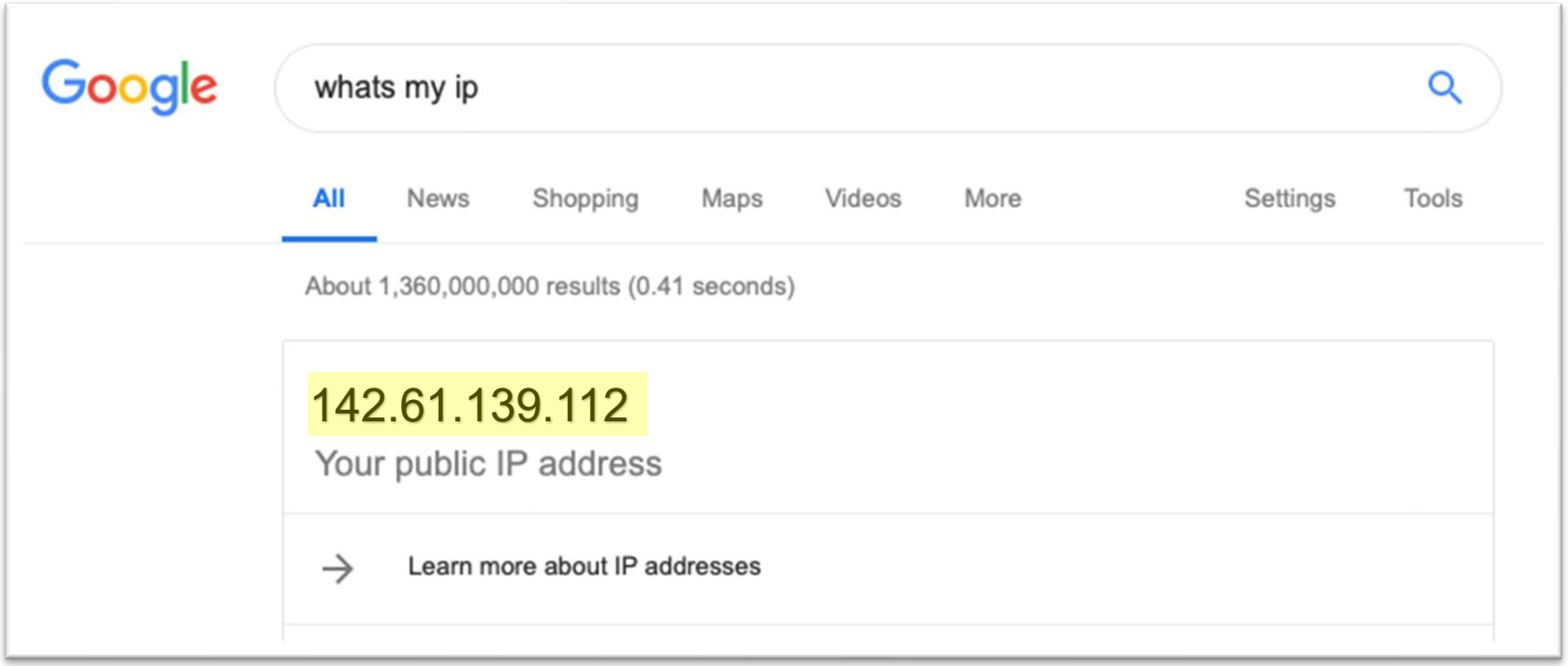
According to Top10VPN's most recent report, **31% of global internet users have a VPN.** Going by Data Reportal's numbers, there are 5.03 billion internet users in the world today. Which amounts to over 1.5 billion VPN users globally





VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 1) Identify your IP address. (Hint: Search “What’s My IP” on Google)



VIRTUAL PRIVATE NETWORKS – EXERCISE

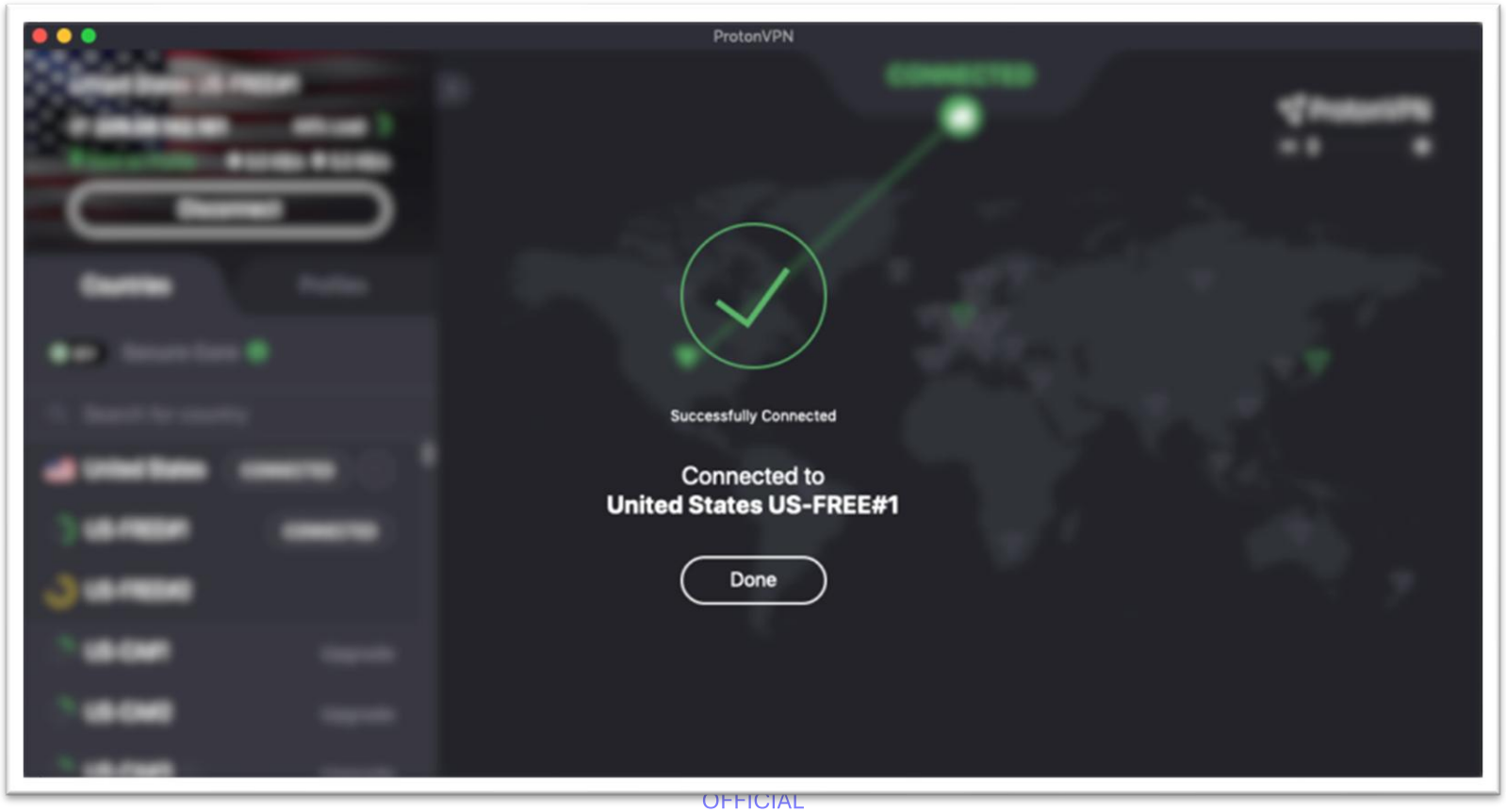
Step 2) Enter your IP into Maxmind

ddress	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain	Connection Type
?.53.75	Gateshead, England, United Kingdom (GB), Europe	86.22.52.0/22	NE9	54.9313, -1.5855 (5 km)	Virgin Media	virginm.net	Cable/DSL

VIRTUAL PRIVATE NETWORKS – EXERCISE

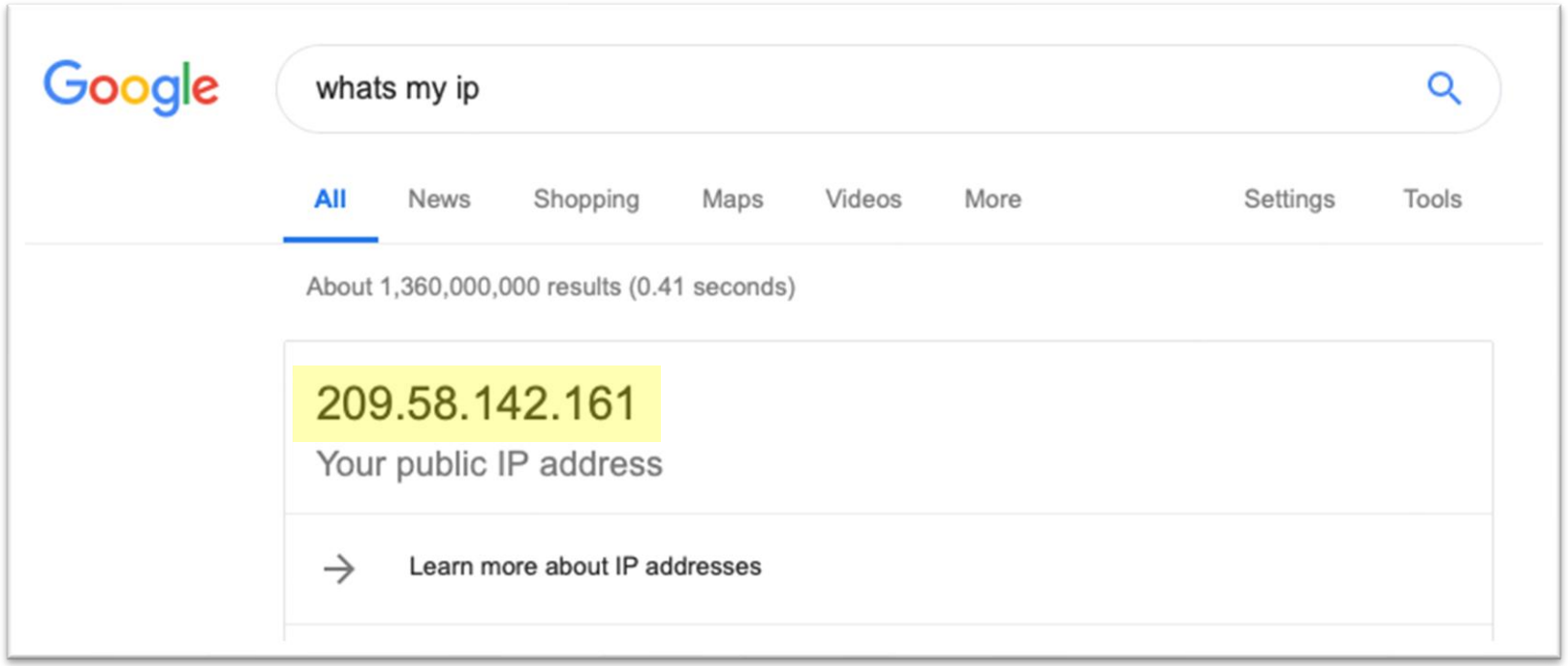
Step 3) Register and Download Proton VPN

Step 4) Login to Proton VPN Connect to a country of your choice



VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 5) Identify your IP address



VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 6) Enter your new IP into Maxmind

Before VPN

ddress	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain	Connection Type
2.53.75	Gateshead, England, United Kingdom (GB), Europe	86.22.52.0/22	NE9	54.9313, -1.5855 (5 km)	Virgin Media	virginm.net	Cable/DSL

After VPN

dress	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain	Connection Type
3.142.161	San Jose, California, United States (US), North America	209.58.136.0/21	95141	37.3388, -121.8916 (1000 km)	Leaseweb San Francisco	-	Corporate

TOR BROWSER

- Tor Browser was developed in the mid 1990's by US Naval Research Laboratory.
- The name "TOR" derived from the original project named
  - **T**he
  - **O**nion
  - **R**outer
- Tor was originally developed to allow anonymous communication
- The TOR Browser directs web traffic through multiple servers, encrypting it each step of the way,
  - As a result, this makes it difficult to trace a user
  - Can be slow due to multiple layers
- Some websites such as Wikipedia limit a users function when using the Tor Browser or an IP address associated the Tor network
  - Wikipedia will not allow you to edit any pages when this is detected
- Could be used during open source in an effort to protect your identity



OFFICIAL

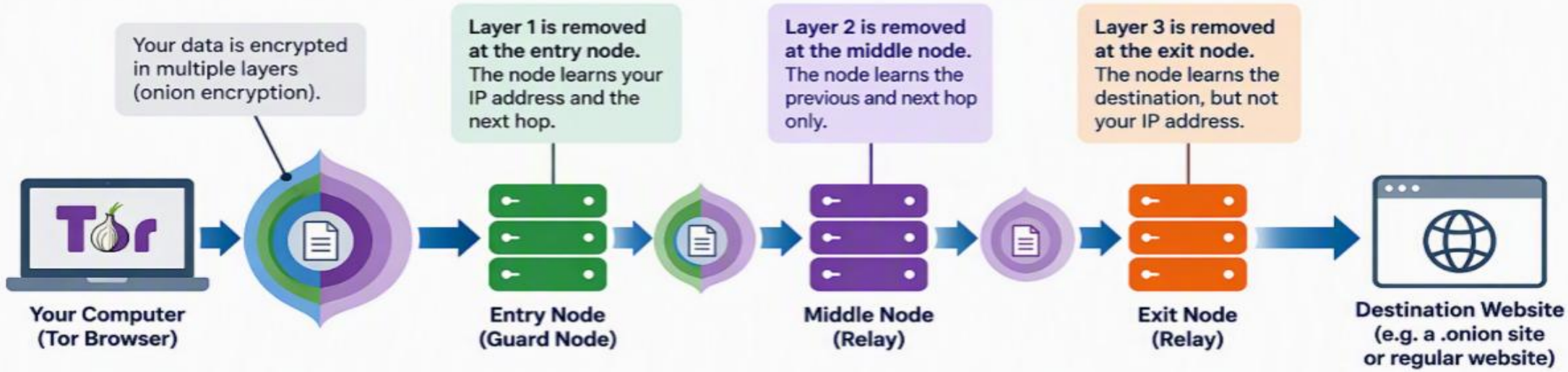
About Tor

Tor Browser | Search or enter address

The Tor Network

How onion routing anonymises internet traffic through layered encryption and multiple relay nodes

No single node knows both the source and destination.



Your Computer

Knows:
- Your IP address
- The entry node (guard)

Entry Node (Guard Node)

Knows:
- Your IP address
- The next hop (middle node)

Middle Node (Relay)

Knows:
- The previous hop (entry node)
- The next hop (exit node)

Exit Node (Relay)

Knows:
- The destination website
- The previous hop (middle node)

Destination Website

Knows:
- The IP address of the exit node (not your IP address)

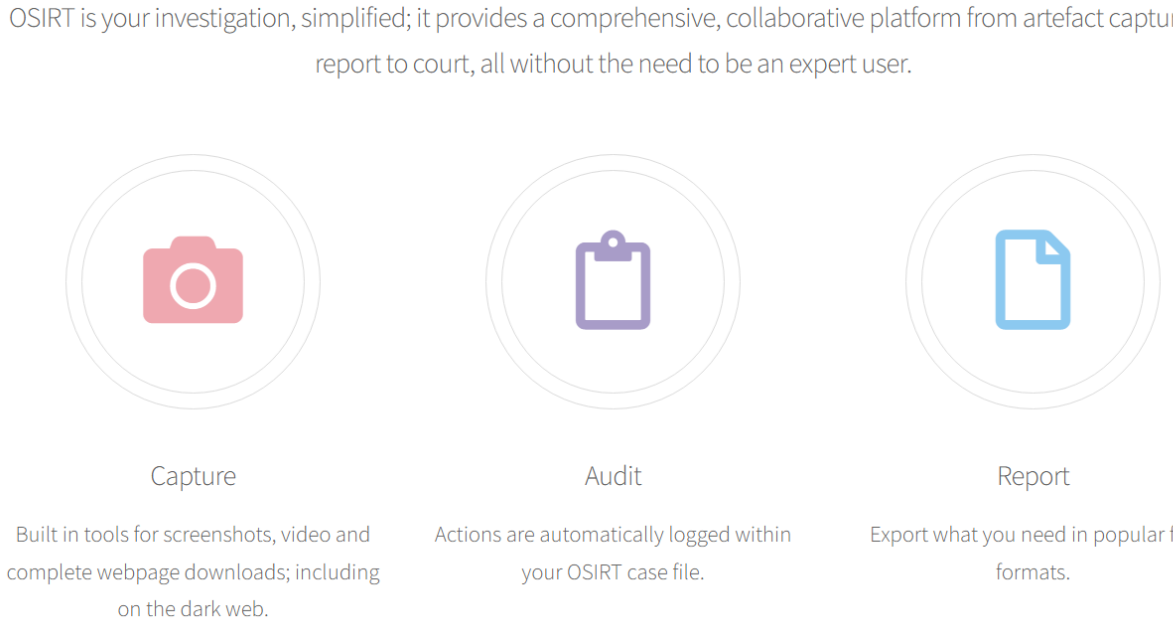
OFFICIAL

Tails


Applications
Places
Mon Apr 13 09:20
en
Type to search...
LibreOffice ...
Onion Circuits
OnionShare
Passwords a...
Pidgin Intern...
Poedit
Power Statis...
Root Terminal
Screenshot
Settings
Simple Scan
Sound Juicer
Sound Recor...
Synaptic Pac...
System Moni...
Tails docum...
Tails Installer
Terminal
Text Editor
Thunderbird
Tor Browser
Unlock Vera...
Unsafe Brow...
Videos
Frequent
All

OSIRT BROWSER

- OSIRT is a web browser which was developed specifically for use in open source investigations
- OSIRT stands for
  - **O**pen
  - **S**ource
  - **I**nternet
  - **R**esearch
  - **T**ool
- OSIRT was a free and open source application:
  - OSIRT have is no longer free, however they do offer a free trial



Screenshots

With just a click, easily capture full page, partial, and specific area screenshots for detailed documentation.

Full Page Capture

Effortlessly capture source code, MHTML, links, and even just the human-readable text on any given webpage.

Download Capture

Capture downloads and save them automatically to your case. Including video downloads.

Page Alerts

Enter the tag you are looking for and working with the OSIRT iii Digital Casebook, it will highlight and alert you to the match.

Dark Web

Advanced investigator? Easily access the Dark Web via Tor in conjunction with our OSIRT iii Digital Casebook.

Fully Auditable

All your captures are automatically logged, hashed, and date and time stamped in the OSIRT iii Digital Casebook.

Reporting

Export your report easily with all your captures in a variety of formats for easy presentation and dissemination.

Privacy By Design

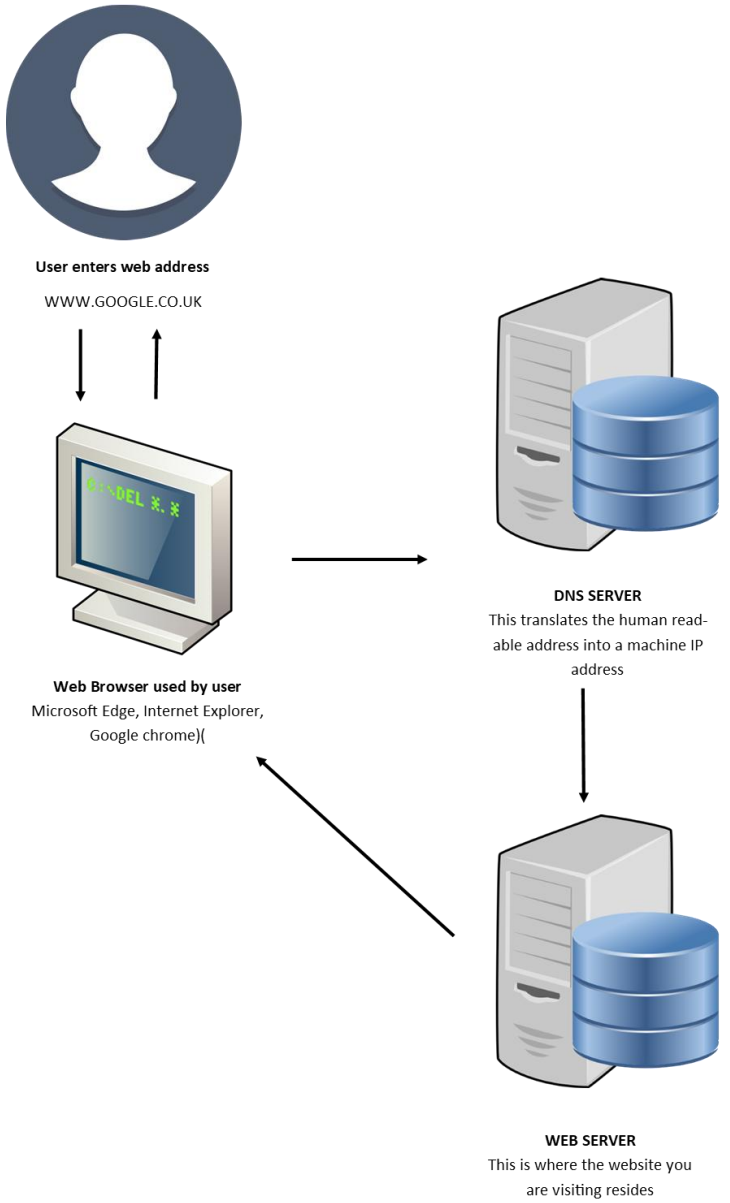
Data captured with OSIRT iii stays only on your machine and never touches our servers, respecting your privacy.


Tracing domain name owners, the origin of an email and email blacklists

DOMAIN NAMES

- A domain name is a unique name for identifying a website
  - 212.58.226.75 > www.bbc.co.uk/news
  - It is a user friendly version of an IP address
- Website developers can purchase a domain name from a number of different companies:
- Like many online purchases, a user is required to provide information when purchasing a domain:





DOMAIN NAMES - WHOIS

- As investigators, this information may help us identify the owner of a website:
  - http://whois.domaintools.com
- WHOIS search conducted for the US Postal Service domain name
  - www.usps.com
- This reveals a number of details
  - Postal address
  - Telephone number
  - Email address
  - IP addresses

```
Registrant:
US Postal Service
   4200 Wake Forest Road
   Raleigh, NC 27668-9000
   US

   Domain Name: USPS.COM

   Administrative Contact, Technical Contact:
      U S Postal Service                    domainadmin@imail.usps.gov
      4200 Wake Forest Rd
      Raleigh, NC 27688
      US
      (919) 501-9100

   Record expires on 09-Jul-2010.
   Record created on 10-Jul-1997.

   Domain servers in listed order:

   DNS100.USPS.COM                56.0.100.25
   DNS141.USPS.COM                56.0.141.25
   DNS082.USPS.COM                56.0.82.25
```

DOMAIN NAMES – PROXY

- Privacy is important part of many peoples lives
  - Think about the latest Apple adverts – all about privacy!
- To assist with privacy, domain name sellers offer a service called Domain Proxy
  - Domain proxy is a paid service which allows you to privately register a domain name
  - The service replaces the domain name owners details with the domain proxy providers details
- What does this mean to an investigator?
  - Enquiries would therefore need to be made with the domain proxy company to identify the “registered owners” details
  - This may prevent its own legislative challenges

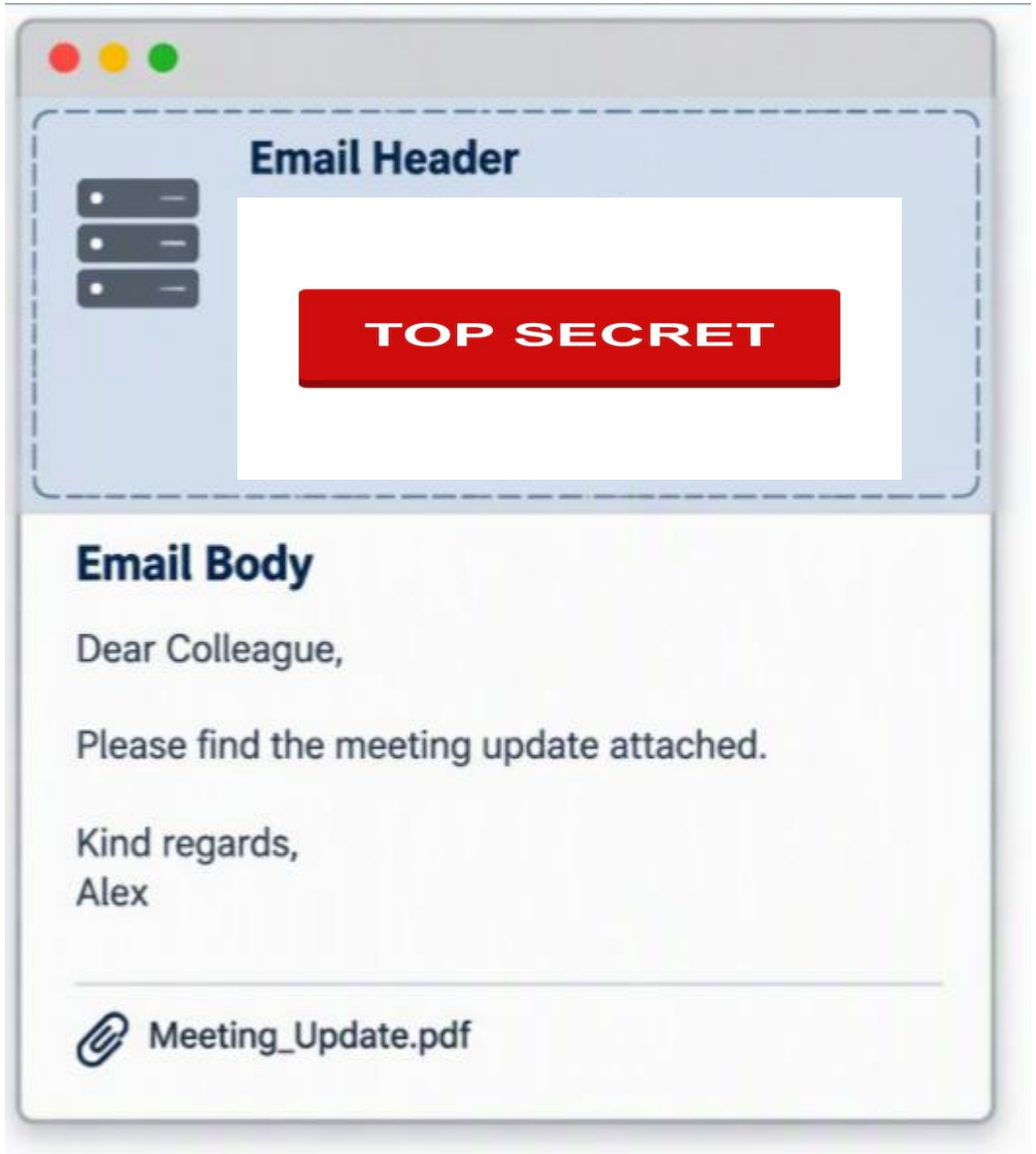
```
Domain name:
        in2locks.co.uk

    Data validation:
        Nominet was able to match the registrant's name and address against a 3rd par
ty data
source on 10-Dec-2012

    Registrar:
        Easily Limited t/a easily.co.uk [Tag = WEBCONSULTANCY]
        URL: http://www.easily.co.uk
```

EMAILS

- Emails can contain hidden information which is useful during an open source investigations
- An email contains two main parts
  - Body
  - Header



EMAIL HEADERS

- Often difficult to interpret, until we understand the different areas of interest
  - **Content-Type:** Notes whether the email is HTML or plain text.
  - **Date:** When the email was written.
  - **Delivery Date:** When the email was received by your mail server.
  - **From:** Who sent the email.
  - **Received:** All of the servers the email has passed through.
  - **Return-Path:** Where a reply to the email will be sent.
  - **Subject:** The email's subject.
  - **To:** Who the email was addressed to
  - **X-Originating-IP:** The IP address from which the email was sent.
  - **X-Spam:** Spam information generated by your email service.

```
Received: from antivirus1.its.rochester.edu (antivirus1.its.rochester.edu
[128.151.57.50])
        by mail.rochester.edu (8.12.8/8.12.4) with ESMTP id h2OGQs9o002563;
        Mon, 24 Mar 2003 11:26:54 -0500 (EST)
Received: from antivirus1.its.rochester.edu (localhost [127.0.0.1])
        by antivirus1.its.rochester.edu (8.12.8/8.12.4) with ESMTP id
h2OGQrQx003450;
        Mon, 24 Mar 2003 11:26:54 -0500 (EST)
Received: from galileo.cc.rochester.edu (galileo.cc.rochester.edu
[128.151.224.6])
        by antivirus1.its.rochester.edu (8.12.8/8.12.4) with SMTP id
h2OGQrDC003447;
        Mon, 24 Mar 2003 11:26:53 -0500 (EST)
Received: (from majord@localhost)
        by galileo.cc.rochester.edu (8.12.8/8.12.4) id h2OGQq91029757;
        Mon, 24 Mar 2003 11:26:52 -0500 (EST)
Date: Mon, 24 Mar 2003 11:26:50 -0500 (EST)
From: somesender@mail.rochester.edu
Message-Id: <200303241626.h2OGQojt002507@mail.rochester.edu>
To: someuser@its.rochester.edu
Subject: My mail message is about:
```

What information may be useful when trying to identify the sender?

EMAIL HEADERS – EXERCISE 1

Good day,

Please, give me your direct email address and co-operation, so that I will introduce to you a business proposal that would benefit both of us immensely.

Await your co-operation.

Yours sincerely,

Wynne Baxter

EMAIL HEADERS – EXERCISE 1

Remember: this could be assigned by a VPN

```
X-Originating-IP: [221.193.216.144]
Authentication-Results: mta1139.mail.ir2.yahoo.com  from=gmail.com; dkim=neutral (no
sig)
Received: from 127.0.0.1  (EHLO ld.cn) (221.193.216.144)
  by mta1139.mail.ir2.yahoo.com with SMTP; Tue, 02 Apr 2019 10:01:46 +0000
Received: from User (unknown [197.242.107.126])
        by ld.cn (CSmail for UNIX) with ESMTP id 8D2935FAA32E;
        Tue,  2 Apr 2019 17:42:36 +0800 (CST)
Reply-To: <wynnebaxtercollp@gmail.com>
From: "Wynne Baxter" <wynnebaxtercollp1@gmail.com>
Subject: Proposal
Date: Tue, 2 Apr 2019 10:55:20 +0100
MIME-Version: 1.0
```

GeoIP2 Precision: City Results

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
221.193.216.144	CN	Handan, Hebei, China, Asia		36.5667, 114.5333	500	China Unicom Hebei	China Unicom Liaoning		

EMAIL HEADERS - EXERCISE 2

Good Day,
Hope you are doing great Today.I have a proposed BUSINESS DEAL that will benefit both parties. This is legitimate,legal and your personality will not be compromised.Please Reply to me ONLY if you are interested and consider your self capable for details.

Sincerely,

Peter OWEN

EMAIL HEADERS – EXERCISE 2

Remember: this could be assigned by a VPN

```
X-Originating-IP: [58.99.32.32]
Authentication-Results: mta1187.mail.ir2.yahoo.com  from=gmail.com; dkim=neutral (no
sig)
Received: from 127.0.0.1  (EHLO tdtv.tinp.net.tw) (58.99.32.32)
  by mta1187.mail.ir2.yahoo.com with SMTP; Wed, 27 Mar 2019 05:52:47 +0000
Received: by tdtv.tinp.net.tw (Postfix, from userid 10734)
        id 83A33364B20; Wed, 27 Mar 2019 13:52:45 +0800 (CST)
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 3.2.4 (2008-01-01) on tdtv.tinp.net.tw
X-Spam-Level: ************
X-Spam-Status: Yes, score=12.8 required=11.0 tests=AWL,BAYES_60,
        DNS_FROM_AHBL_RHSBL,FH_DATE_PAST_20XX,FORGED_MUA_OUTLOOK,MSOE_MID_WRONG_CASE,
        RCVD_IN_BL_SPAMCOP_NET,RCVD_IN_XBL,RDNS_NONE autolearn=spam version=3.2.4
```

GeoIP2 Precision: City Results

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
58.99.32.32	TW	Taichung, Taichung City, Taiwan, Asia		24.1469, 120.6839	100	Taiwan Infrastructure Network Technologies	Taiwan Infrastructure Network Technologie	tinp.net.tw	

EMAIL BLACKLISTS

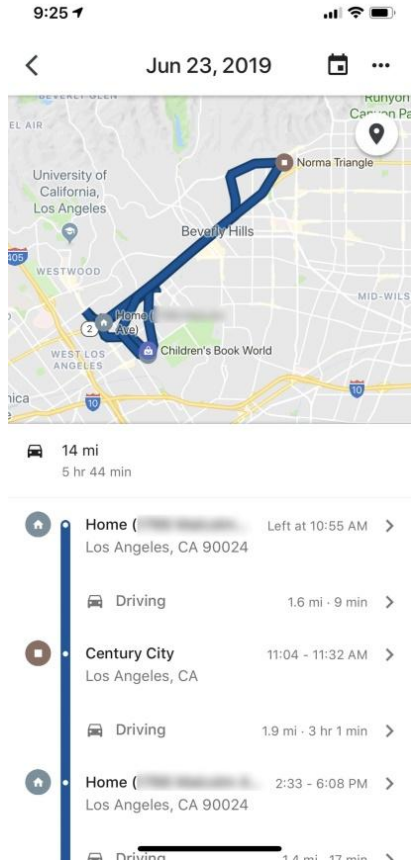
- Email Blacklists were developed in an effort to reduce spam being received by users
- Email Blacklists are a real-time list of IP addresses and domain names which are known to send spam emails
- There are a number of companies who maintain email blacklists
  - Barracuda
  - Spamhaus
- Aggregate blacklist checker mxtoolbox.com is a useful tool which searches around 100 different blacklists
- Email Blacklists are used by a number of people
  - Internet Service Providers (Virgin, Sky and Plusnet etc.)
  - Mailbox providers (Hotmail, Gmail)
  - Organisations

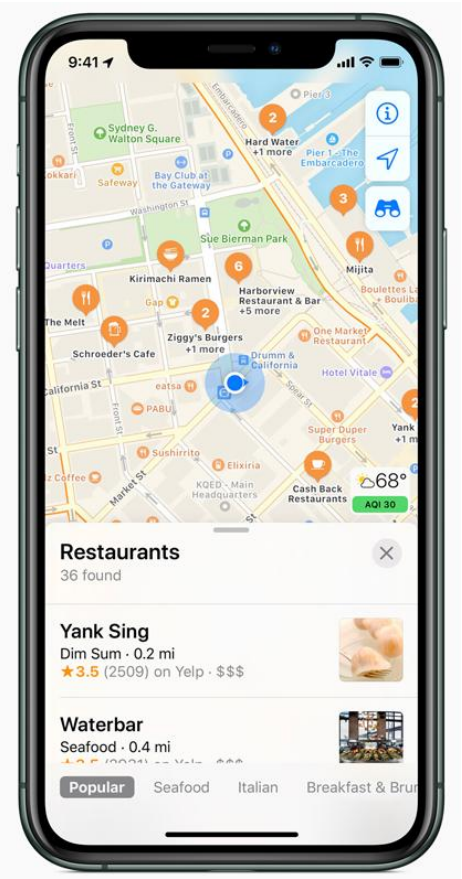



Geo-location tools for Open Source Investigations

GEO-LOCATION

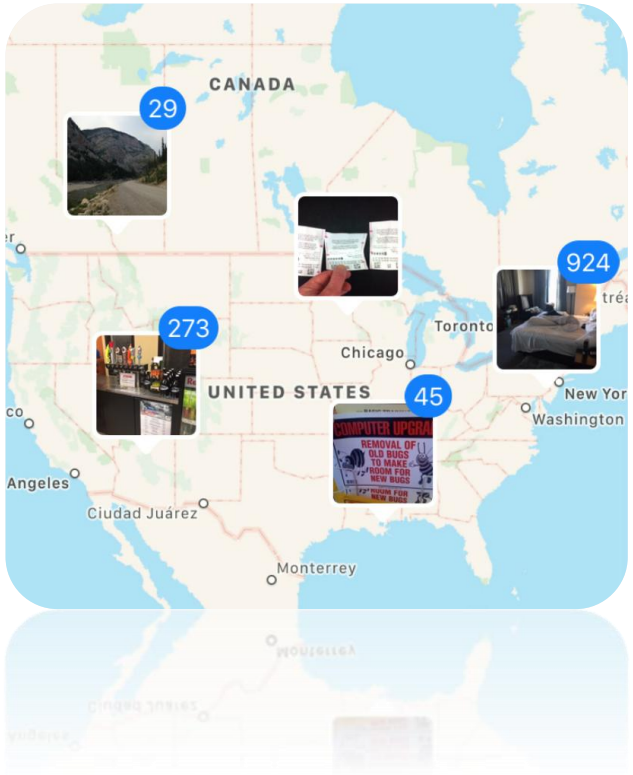
- Geo-location is defined as a technique of identifying the geographical location of a person/device using digital data.
    - Geolocation data can be found within various forms of digital data including:
        - Photographs
        - Social Media
        - Video
        - Posts
- Digital devices record the location for various reasons and in many forms:
    - Record your commonly visited places
    - Booking an Uber
    - Recommendation for a restaurant
    - Location of photographs





GEO-LOCATION

- When taking a photograph on a digital device, the device can often embed metadata (EXIF) within the photograph
  - Settings need to be enabled
  - Many people just press “Accept”
- Metadata is defined as **data about data**, the metadata will vary from the device make/model and the settings enabled.
- Various pieces of EXIF/Metadata can be embedded
- Most paid forensic tools will interpret the image metadata, including plot the geo-location of a photograph on a map.
- Free tools available online which will interpret this data.



EXIF DATA EXERCISE

- During an investigation we have recovered two photographs
    - IMG_7300.JPG
    - IMG_3561.JPG
- The investigation team need to understand more information about the images
- Using a free online tool, we will see what other information we can obtain from the photograph
    - For this exercise we will use www.pic2map.com

EXIF DATA EXERCISE

- Filename: IMG_7300.JPG



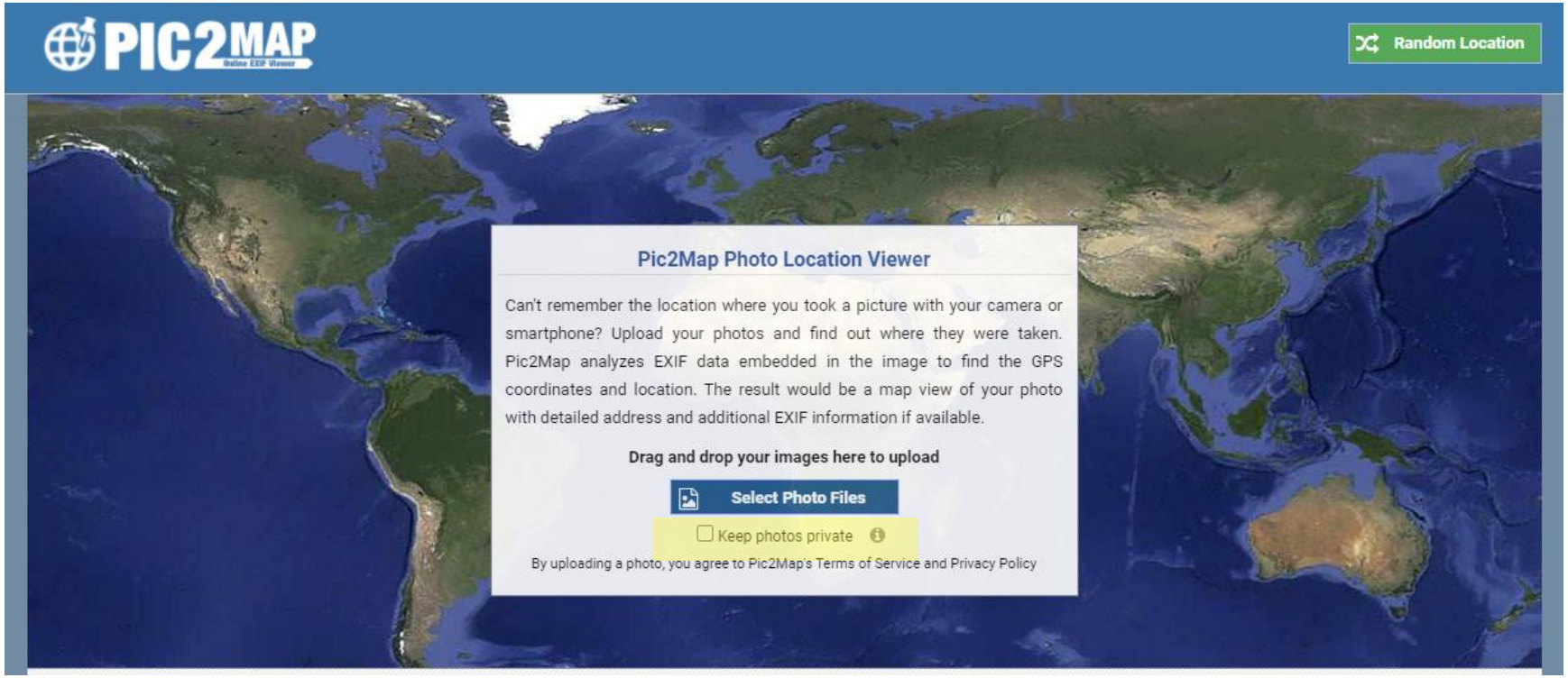
EXIF DATA EXERCISE

- Filename: IMG_3561.JPG



EXIF DATA EXERCISE

- PIC2MAP is one of many free tools available online
  - Can be used to parse EXIF data in photographs



Brand:	Apple	Model:	iPhone 6	Lens Info:	iPhone 6 back camera 4.15mm f...
Shutter:	1/30 (0.0333 seconds)	F Number:	f/2.2	ISO Speed:	ISO 125
Flash:	Not Used	Focal Length:	4.2 mm	Color Space:	sRGB

FILE INFORMATION

File Name:	IMG_7300.JPG	Image Size:	1000 x 750 pixels	Megapixels:	0.8 megapixels
File Size:	202,615 bytes (0.20 MB)	MIME Type:	image/jpeg	Resolution:	72 DPI

DATE & TIME

Date:	2015-06-24	Time:	20:30:13 (GMT -04:00)	Time Zone:	America / Nassau

GPS INFORMATION

Latitude:	28.431397	Longitude:	-81.473206	Lat Ref:	North
Long Ref:	West	Coordinates:	28° 25' 53.03" N , 81° 28' 23.54" W	Altitude:	39m. (Above Sea Level)
Direction Ref:	True North	Direction:	37.21 Degrees	Pointing:	Northeast

LOCATION INFORMATION

City:	State: Florida	Country: USA

Address: Rosen Inn at Pointe Orlando, Samoan Court, Orange County, Florida, 32819-8902, USA

(Location was guessed from coordinates and may not be accurate.)

Brand:	Apple	Model:	iPhone 5	Lens Info:	iPhone 5 back camera 4.12mm f...
Shutter:	1/15 (0.0667 seconds)	F Number:	f/2.4	ISO Speed:	ISO 2000
Flash:	Not Used	Focal Length:	4.1 mm	Color Space:	sRGB

FILE INFORMATION

File Name:	IMG_3561.JPG	Image Size:	1000 x 750 pixels	Megapixels:	0.8 megapixels
File Size:	290,968 bytes (0.29 MB)	MIME Type:	image/jpeg	Resolution:	72 DPI

DATE & TIME

Date:	2014-06-04	Time:	20:56:05 (GMT -05:00)	Time Zone:	America / Cancun

GPS INFORMATION

Latitude:	20.605933	Longitude:	-87.092392	Lat Ref:	North
Long Ref:	West	Coordinates:	20° 36' 21.36" N , 87° 5' 32.61" W	Altitude:	0 (Below Sea Level)
Direction Ref:	True North	Direction:	199.76 Degrees	Pointing:	South

LOCATION INFORMATION

City:	Playa del Carmen	State:	Quintana Roo	Country:	Mexico

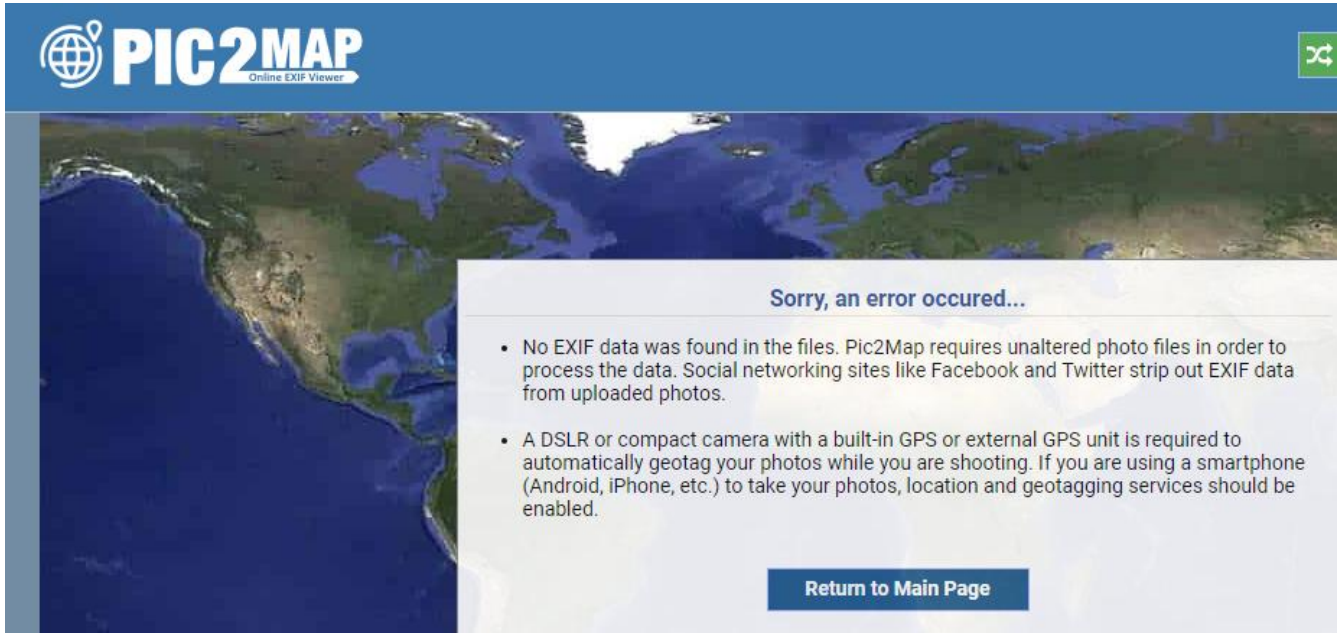
Address: RIU Yucatán, Avenida Paseo Xaman-Ha, Playacar Fase 2, Bosque Real, Playa del Carmen, Solidaridad, Quintana Roo, 777717, Mexico

(Location was guessed from coordinates and may not be accurate.)

EXIF DATA EXERCISE

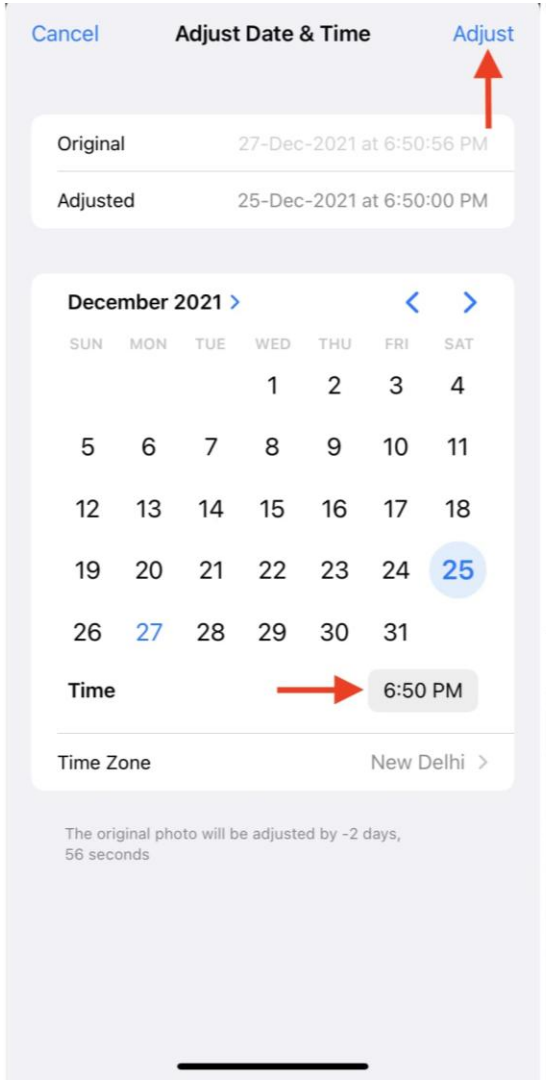
- Not all photographs have EXIF Data

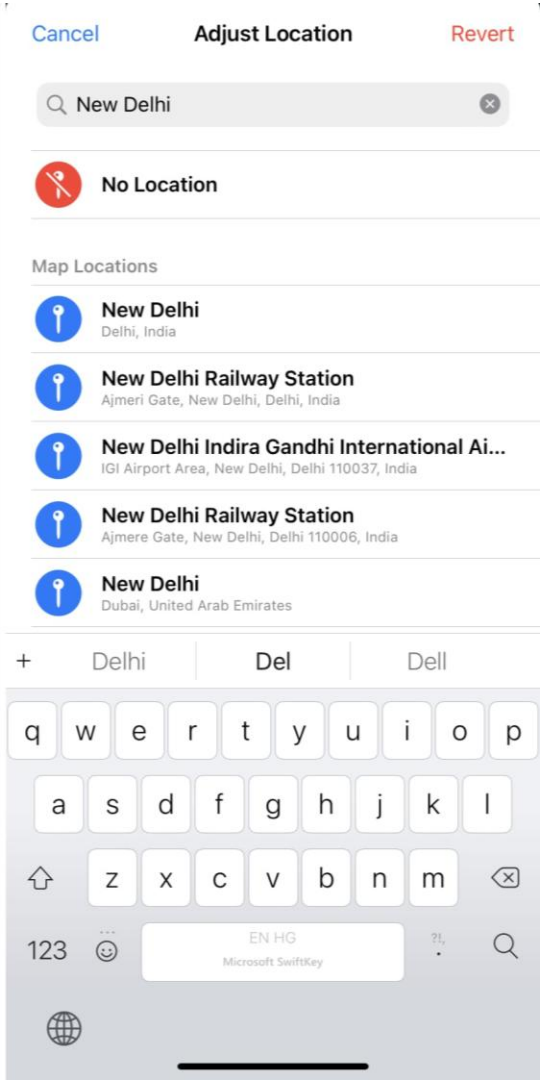




EXIF DATA REMINDER

- There are free tools available online which will allow users to:
  - Edit the metadata embedded within a photograph
  - Remove the metadata embedded within a photograph
- As a result, keep in mind that the metadata, including the geo-location data could be altered!
- In iOS16, Apple implemented a feature which allows users to edit EXIF using the native Photos application:
- WhatsApp or Facebook Messenger often strip the metadata from files
  - To reduce file size for transfer

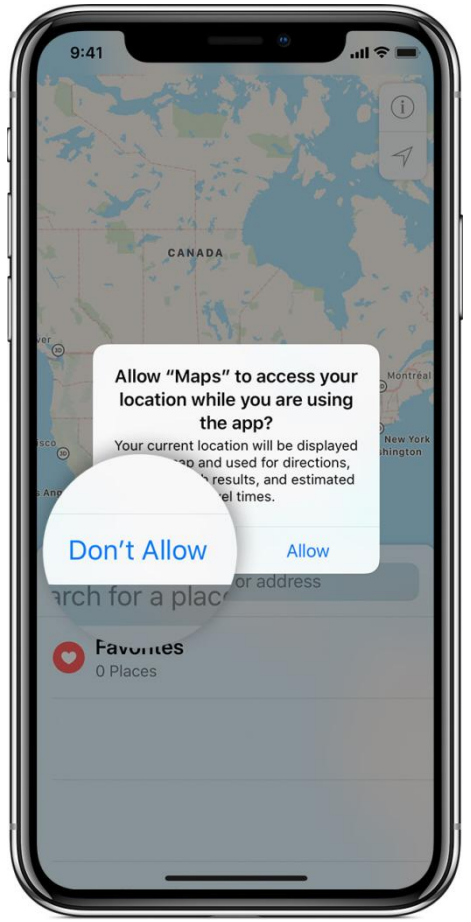




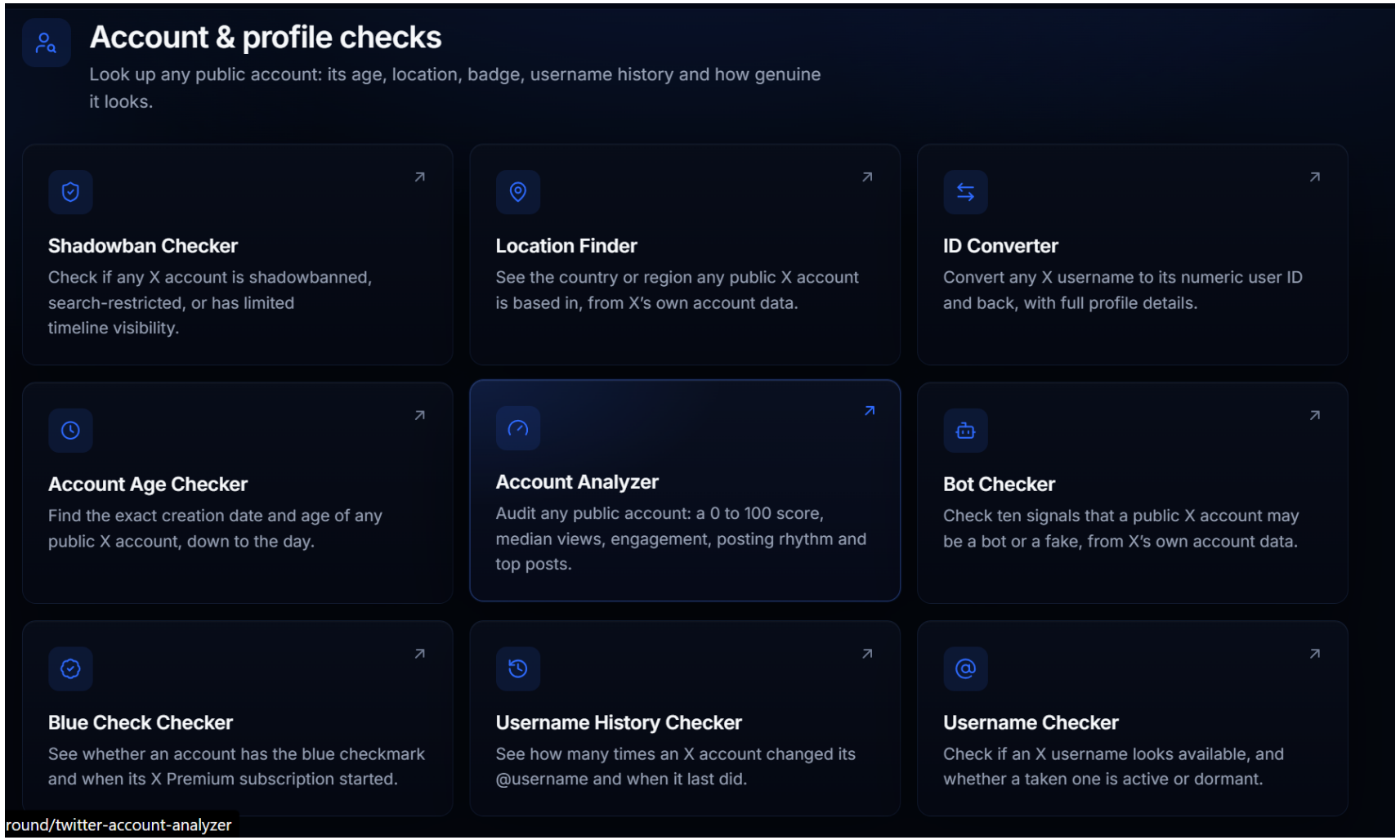
How to Edit the Metadata for Multiple Photos on iPhone on iOS 16 (nerdschalk.com)

X - TWITTER

- In April 2025 X reported they have had 650 million monthly active users
  - UK Population in 2022 was 66 million people
- Users are often unaware that social media tracks lots of data useful to an investigator
  - A lot of people (myself included) just press “Allow” when installing a new application
- X is one of the social media sites which can track the location of tweets
- A number of free tools which are available online which can be used to search tweets containing geo-location data



SORSA API



[Free X (Twitter) Tools — All Sorsa Playground Utilities | Sorsa]

X (TWITTER) API

- Open source tools often rely upon the use of API's(**A**pplication **P**rogramming **I**nterface) to collect data from the website/service
- API's are a mechanism which allows two software components to communicate with one another.
  - For example the weather application on your phone will likely use an API to communicate with the main weather applications computer systems.
- Elon Musk announced from 9th February 2023, the free API service will become a paid service.
- Since February 2023, a large number of Twitter OSINT tools have went offline
  - One of the many challenges associated with OSINT Investigations



BREAKING

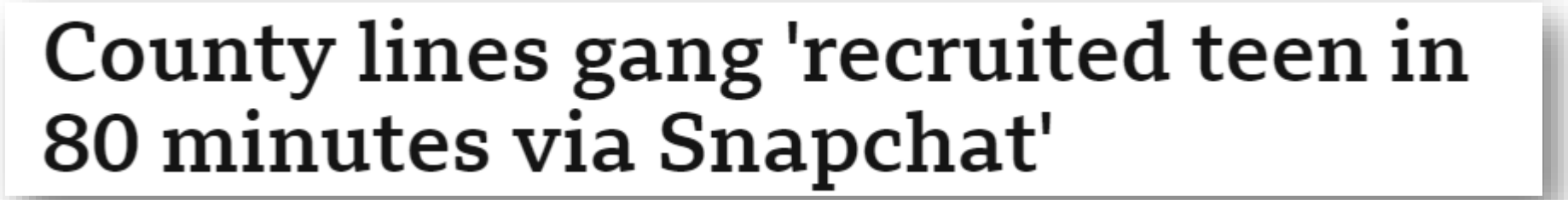
Twitter Ends Its Free API: Here's Who Will Be Affected

Jenae Barnes Former Staff

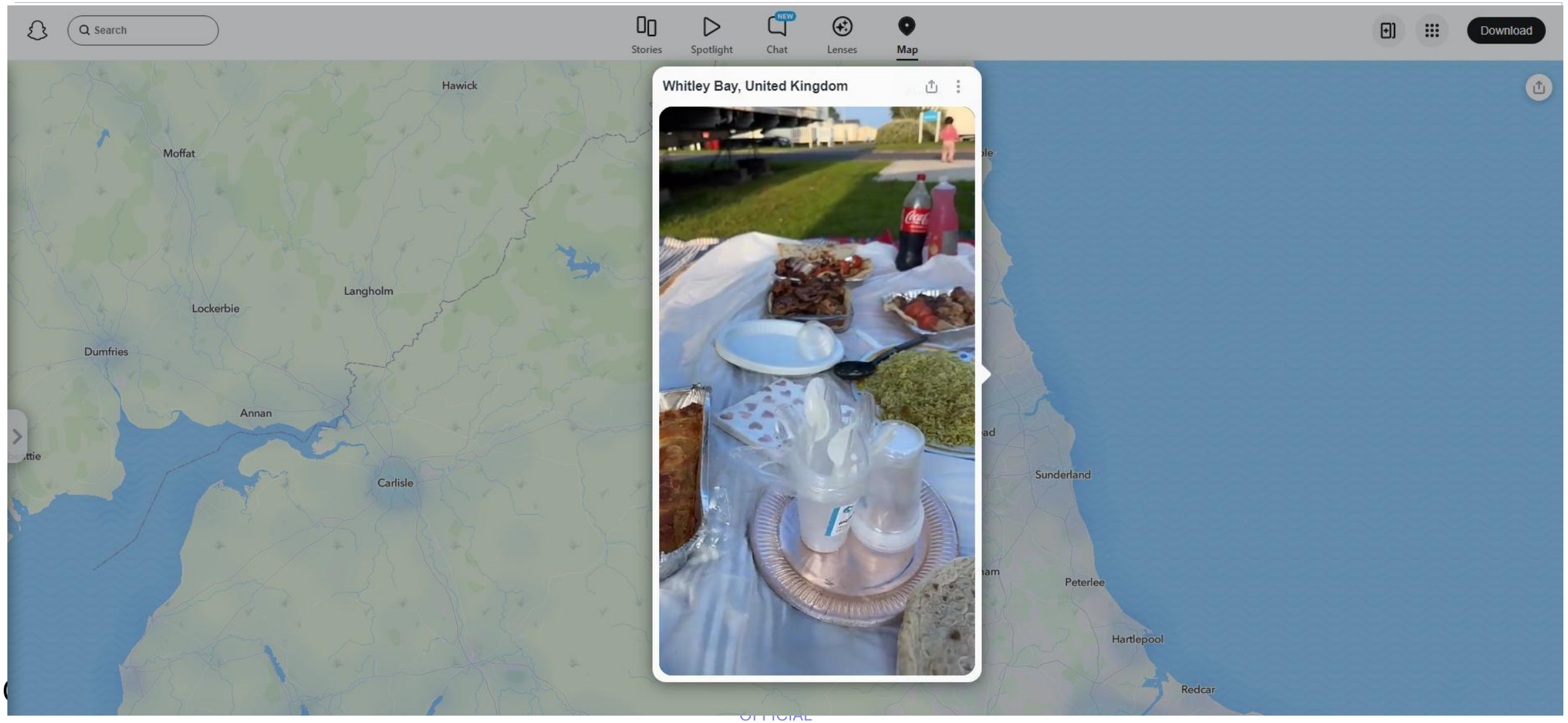
Forbes Staff

SNAPCHAT

- In 2026 Snapchat had around 971 million monthly active users worldwide
- The application was originally developed for person to person sharing,
  - Since evolved to the use of public stories and other sharing features
- Snapchat launched Snap Map in June 2017, it allows users to see the location of their friends
  - It also allows users to view a world map and view publicly available Snaps
- Snap Map can be accessed on the Snapchat Website
  - Snap Map (snapchat.com) **(Now need a Snapchat login to review Snapmap)**
- Users can use Ghost mode to hide their location and choose not to share their Stories to the public Snap Map.


County lines gang 'recruited teen in 80 minutes via Snapchat'

SNAP MAP

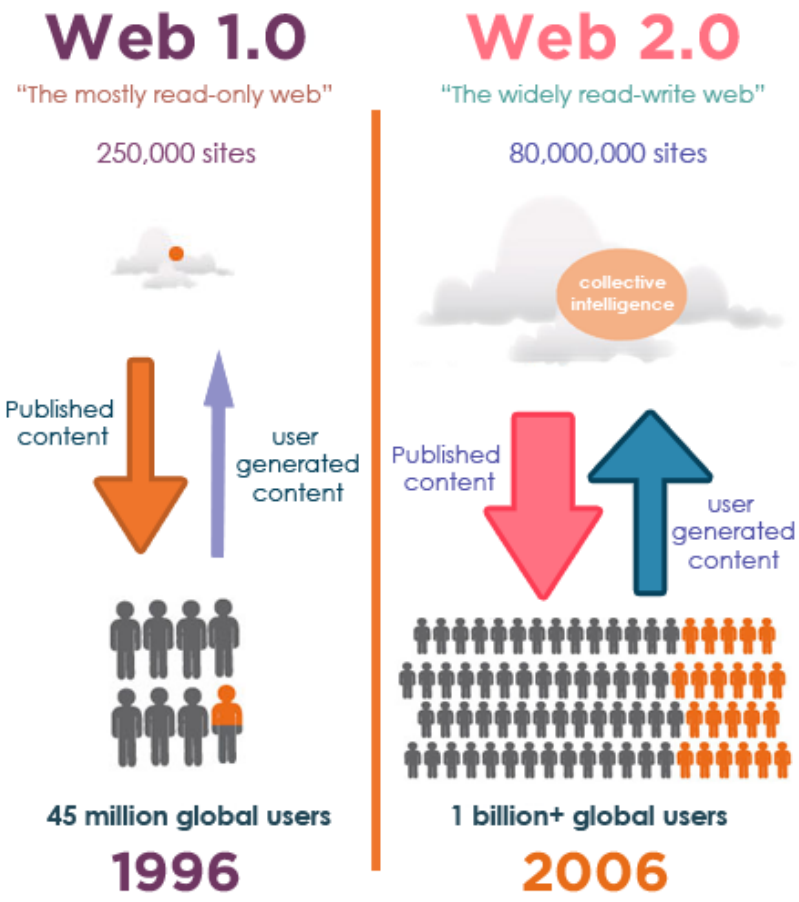

Search
Stories
Spotlight
Chat
NEW
Lenses
Map
Download
Whitley Bay, United Kingdom
Hawick
Moffat
Langholm
Lockerbie
Dumfries
Annan
Carlisle
Sunderland
Peterlee
Hartlepool
Redcar



Investigating Web 2.0 – social networking, blogs and online gaming

WHAT IS WEB 2.0

- Web 2.0 is defined as the second generation of the world wide web
- Originally the internet was relatively static
  - In order to share information, a user would need to have skills such as web design. (HTML/CSS Programming skills)
- The introduction of Web 2.0 made the internet more dynamic
  - This version focused on the ability for people to share information online.
- Web 2.0 websites often utilises information from other websites
  - For example, a website which reviews restaurants such as TripAdvisor may utilise information from a variety of websites including Facebook, Flickr and Google maps.



WEB 2.0 WEBSITES

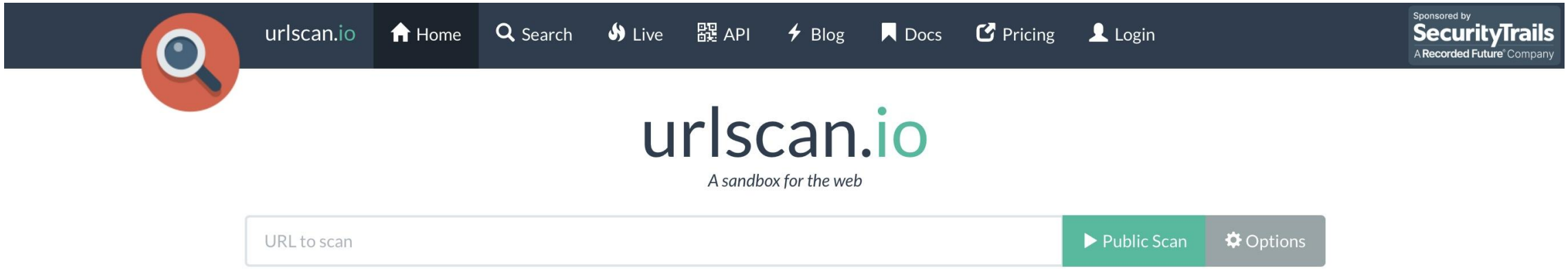
Examples of web 2.0 websites commonly used:

Wikis	Blogs	Social Networking	Content Hosting
• Wikipedia	• Tumblr • WordPress • Blogger	• Facebook • X • TikTok	• YouTube • Flickr

- If there are no tools available specifically for the above websites, consider using the OSIRT browser to record the webpage.

URLSCAN

- URLScan.io provides users with a sandbox environment to review a website
  - A sandbox is an isolated virtual machine in which potentially unsafe software can execute without affecting network resources or local applications.
- Warning: it does show the recent scans on their homepage!
- This is a useful tool if you want to obtain further information about a particular website without visiting the site itself



OFFICIAL

www.bbc.co.uk

151.101.64.81 Public Scan

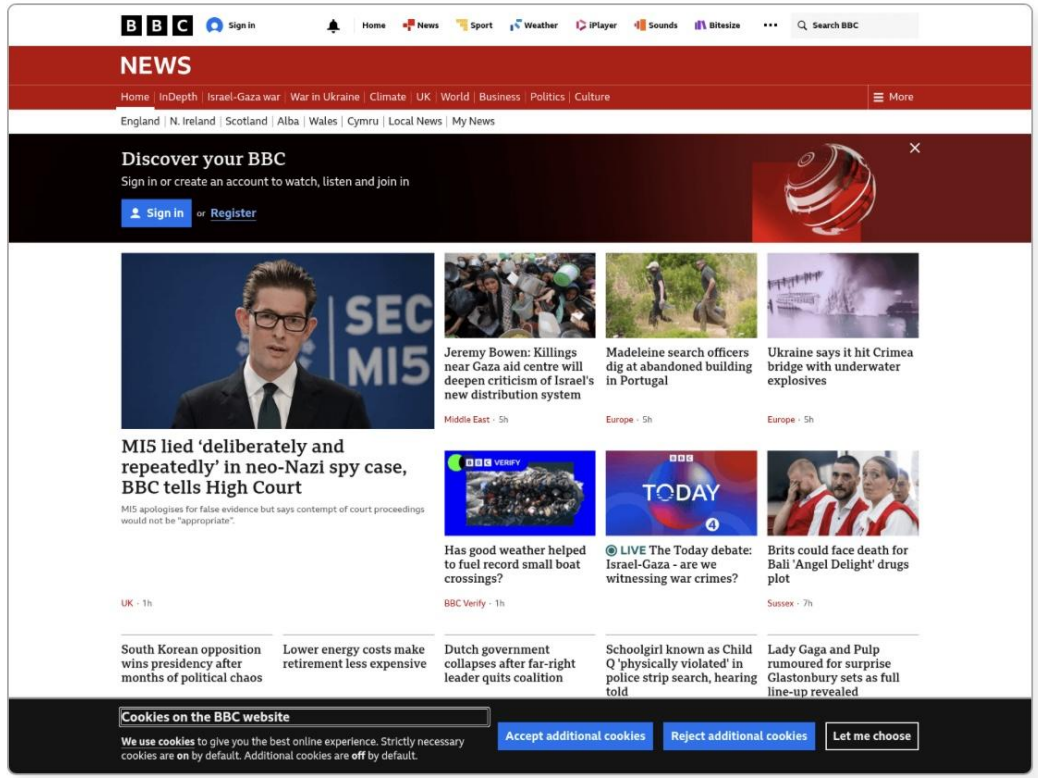
Back to summary

URL: https://www.bbc.co.uk/news

Submission: On June 03 via manual (June 3rd 2025, 7:35:04 pm UTC) from GB — Scanned from UK

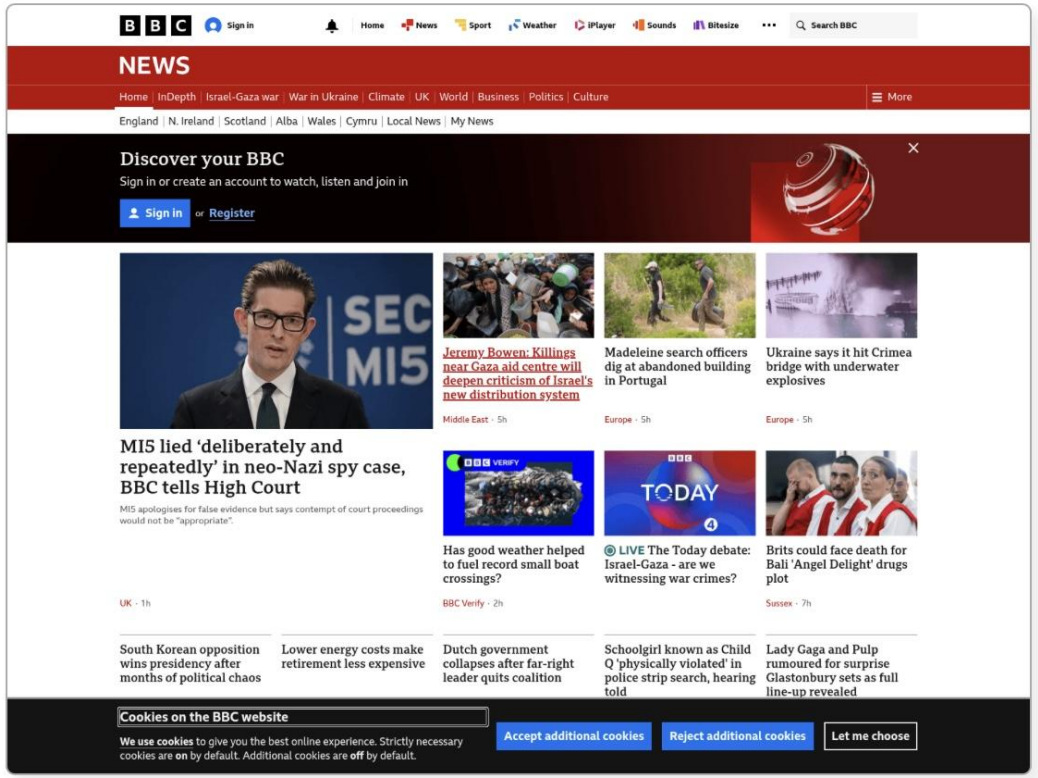
Screenshot during scan

Image



Screenshot now Submitted URL

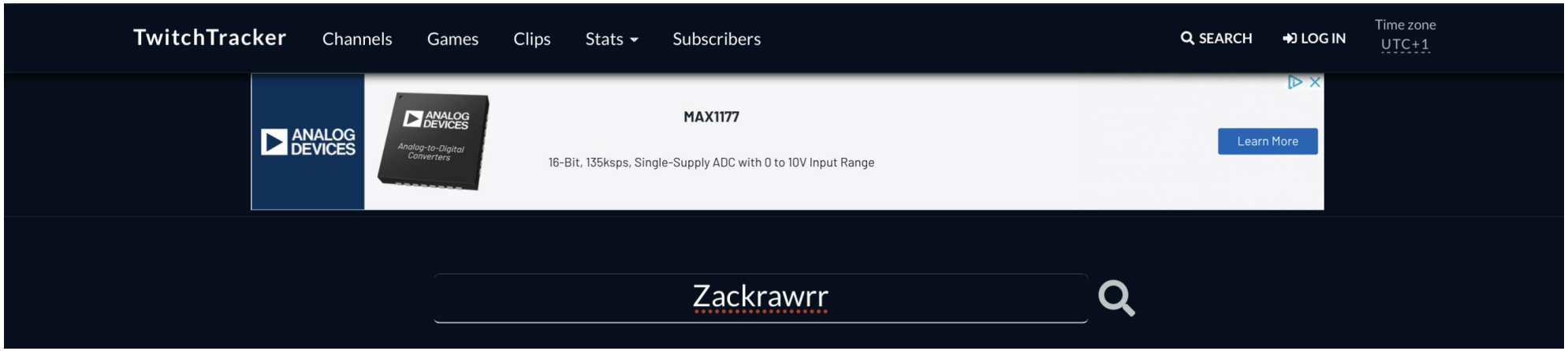
Image



IPs Countries Transfer Size Cookies

TWITCH

- Twitch is a popular American video live streaming service
- Launched in June 2011, in 2025 it was reported that Twitch has 240 million monthly active users
- Various platforms available to interrogate information held on a Twitch account
- TwitchTracker is an OSINT tool which allows you to obtain data sssociated with a particular Twitch account





ZACKRAWRR

Overview | Streams | Games | Subs | Statistics | Clips

RANK 2

PERFORMANCE SUMMARY

7 DAYS | 30 DAYS | 3 MONTHS | ALL TIME

51.1 Hours streamed	49,105 Average viewers	110,355 Peak viewers	2,509,266 Hours watched
5,625 Followers gained	110 Followers / hour	3 Games streamed	7 / 7 Active days

LIFETIME OVERVIEW

8,616 Total hours streamed	#86 309,124 Highest number of viewers Jan 20, 2025	#180 2,095,023 Total followers	168 Total games streamed

INSTAGRAM

- Instagram is a social media platform owned by Meta, designed to share images and movies
- Users can lock down their profiles to allow access to only those who follow them
  - This has an impact on our open source investigation
  - In my experience, there is a significant Increase in users choosing to lock their account to followers only
- In 2025, Instagram reported 2 billion active users each month
- What sort of information can we obtain from a users profile?
  - Posts (Media with captions and tags)
  - Instagram Stories
  - Followers
  - Following
  - Personal bio
  - Tagged posts



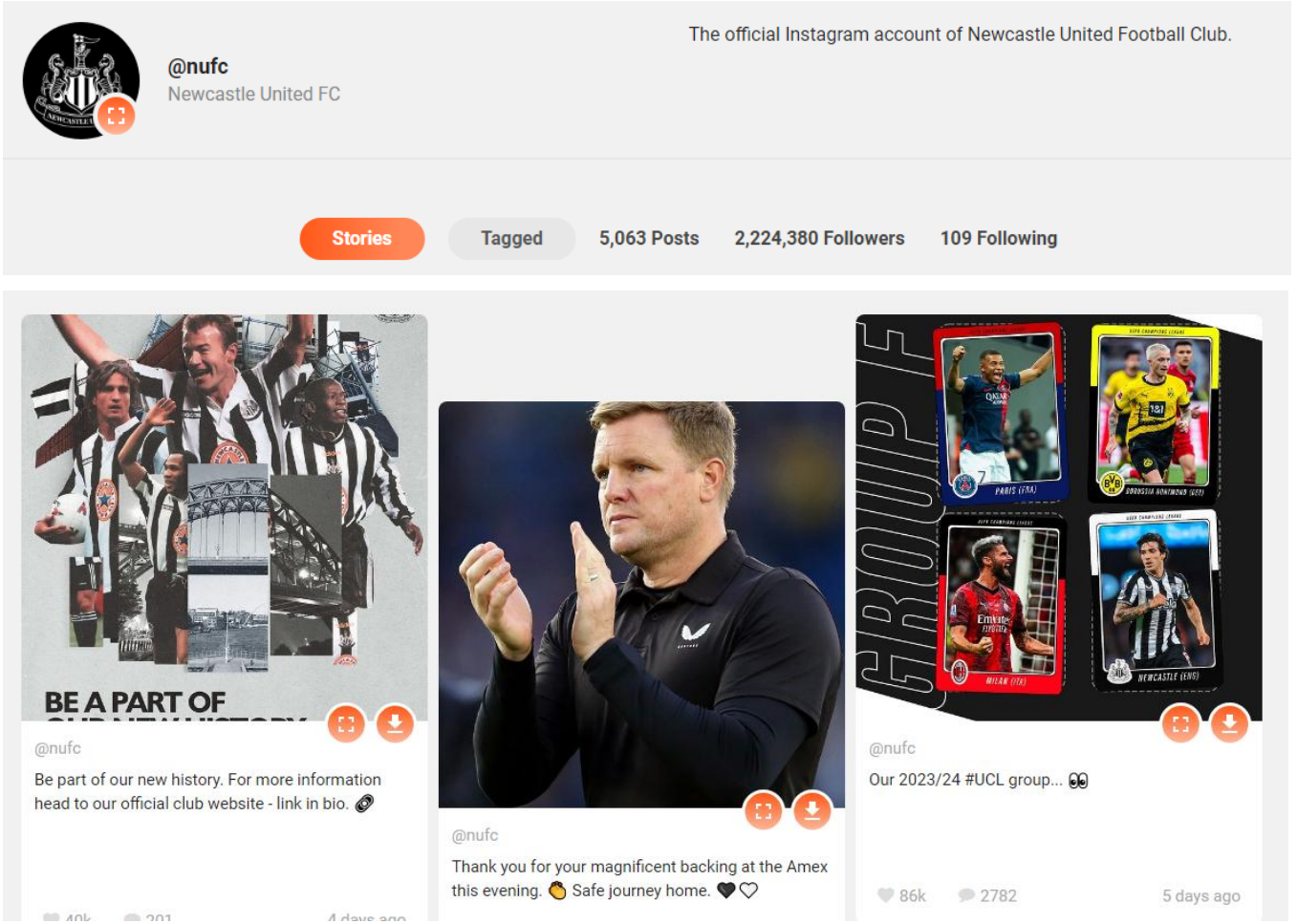
INSTAGRAM EXERCISE

Instagram Exercise 1

Step 1) Visit https://www.inflact.com

Step 2) Enter “nufc” search for the profile

Can we see the profile?



INSTAGRAM EXERCISE

Instagram Exercise 2

If you have an Instagram account, try the following

Step 1) Visit https://www.inflact.com

Step 2) Enter your Instagram name and review your profile

Can we see the profile?

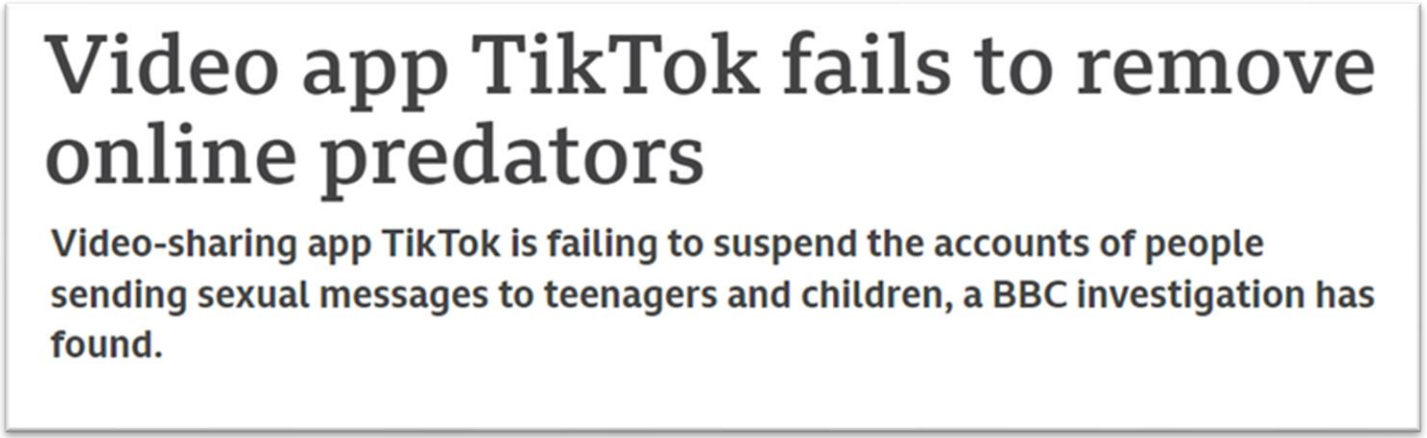


FACEBOOK

- Facebook is another commonly used social network
- In January 2024, Facebook had over 3 billion monthly active users
- Facebook has the ability to record lots of data about a user
  - Friends
  - Employer
  - Photographs
  - Location data
- Over the years Facebook has been under increased scrutiny regarding how they protect a users privacy
  - A large number of accounts are restricted with privacy settings
- Open source with Facebook has become challenging in recent years Although challenging, there are a number of sites which provide tools
  - Inteltechniques.com & Osintframework.com
  - Facebook built in search can be very useful
    - To use this you need an account, this may present legislative challenges

TIKTOK

- TikTok is a social video app that allows users to share short videos.
- Statista reported that TikTok have approximately 1.7 billion users worldwide
  - Up by over 66% when compared to 2020
- The application allows users to comment on videos and also offers private messaging.
- The application is incredibly popular in the UK, as a result as Digital Forensic Investigators we need to understand how the application works and any relevant forensic/open source techniques.
- As the platform is relatively new, techniques are constantly changing

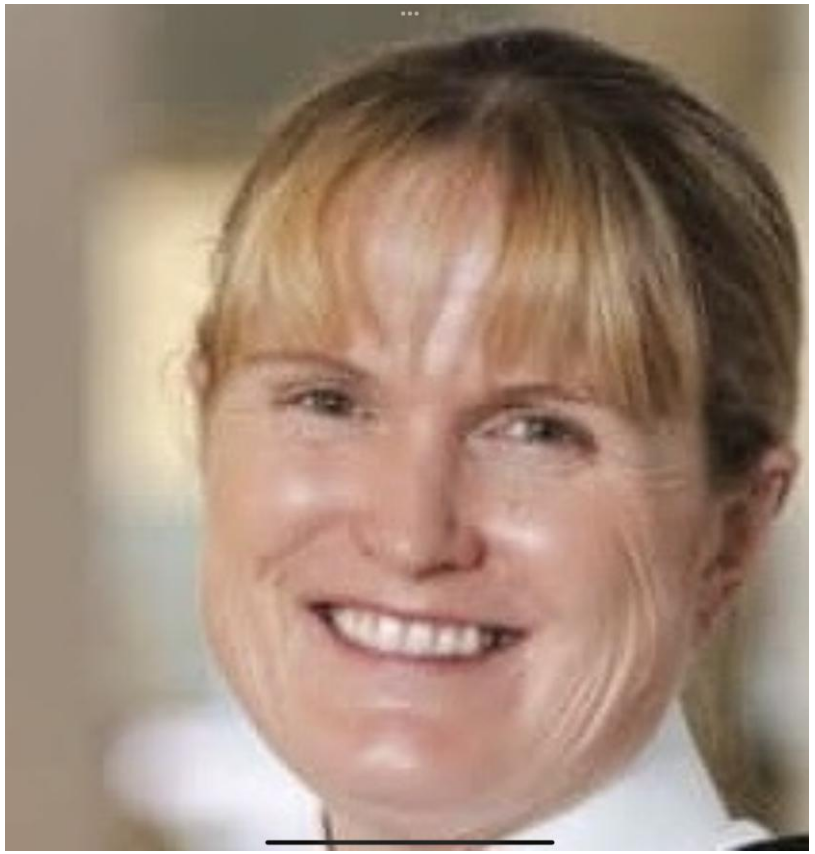


Video app TikTok fails to remove online predators

Video-sharing app TikTok is failing to suspend the accounts of people sending sexual messages to teenagers and children, a BBC investigation has found.

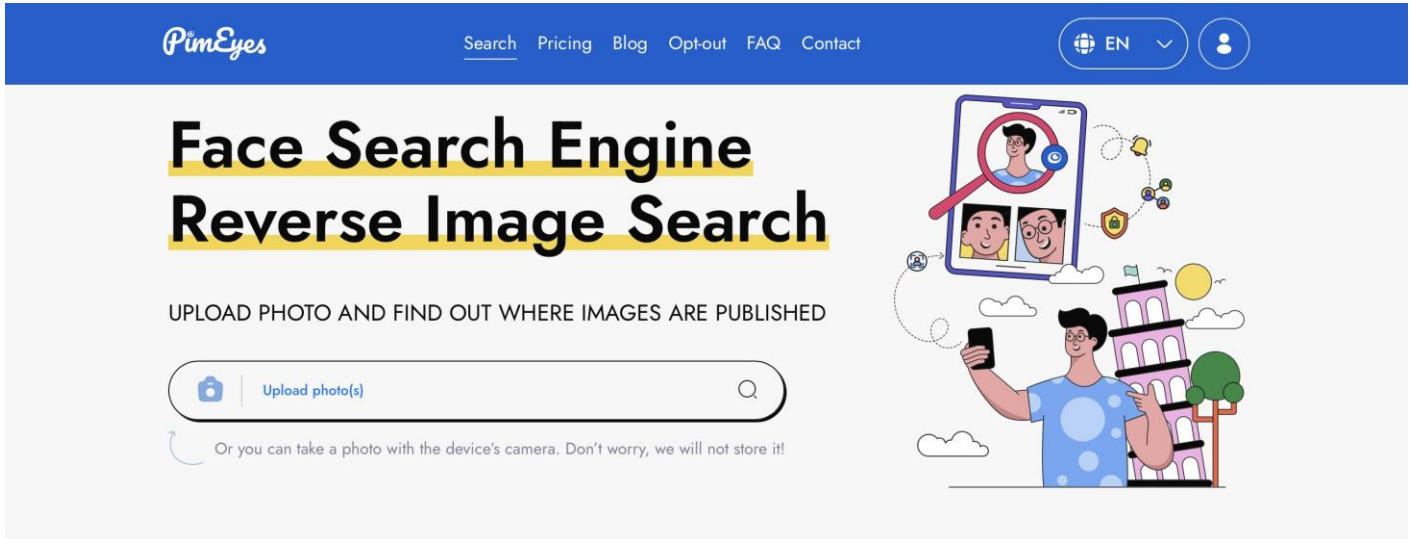
TIKTOK EXERCISE

- There aren't always tools available to assist in open source investigations for a particular website
- Imagine you have been provided with a photo obtained from a TikTok account of interest.
- In this example, the image is low quality to simulate compression which is very common on social media platforms



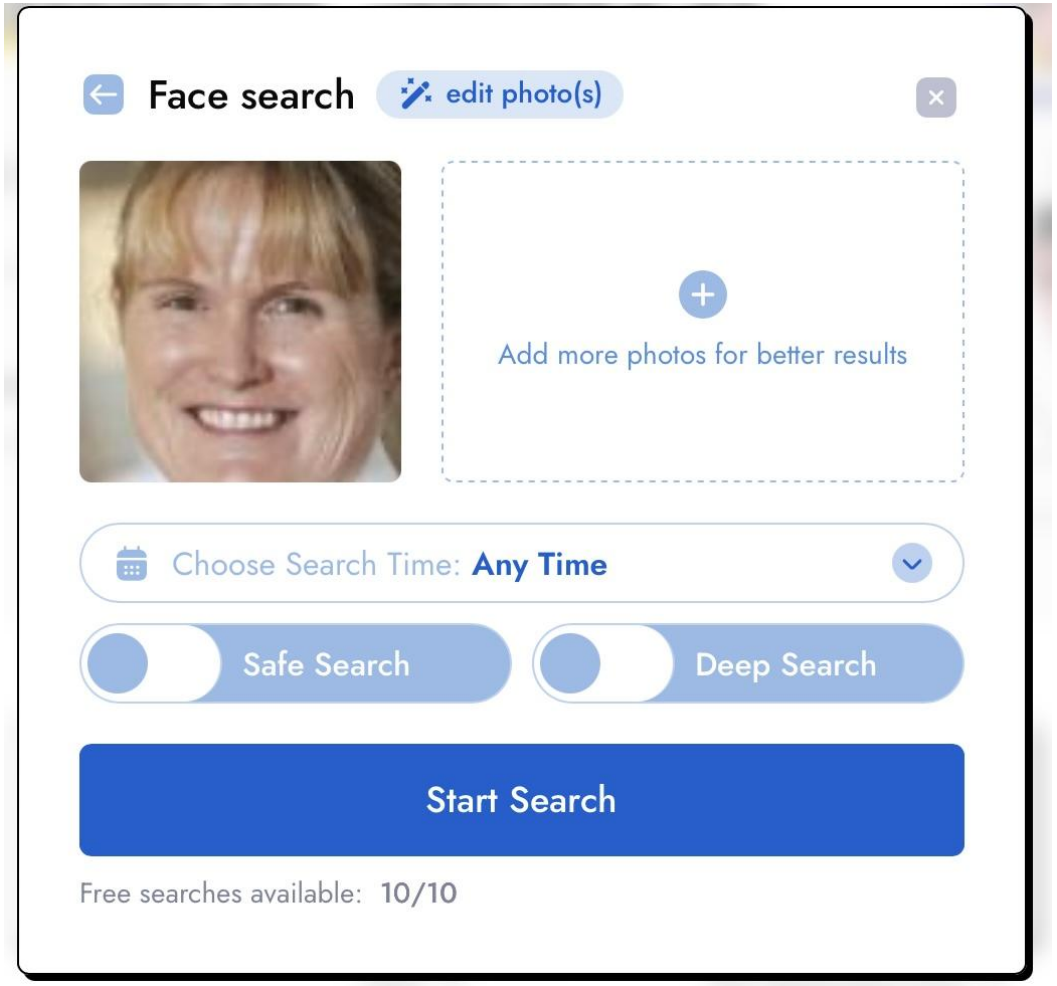
TIKTOK EXERCISE

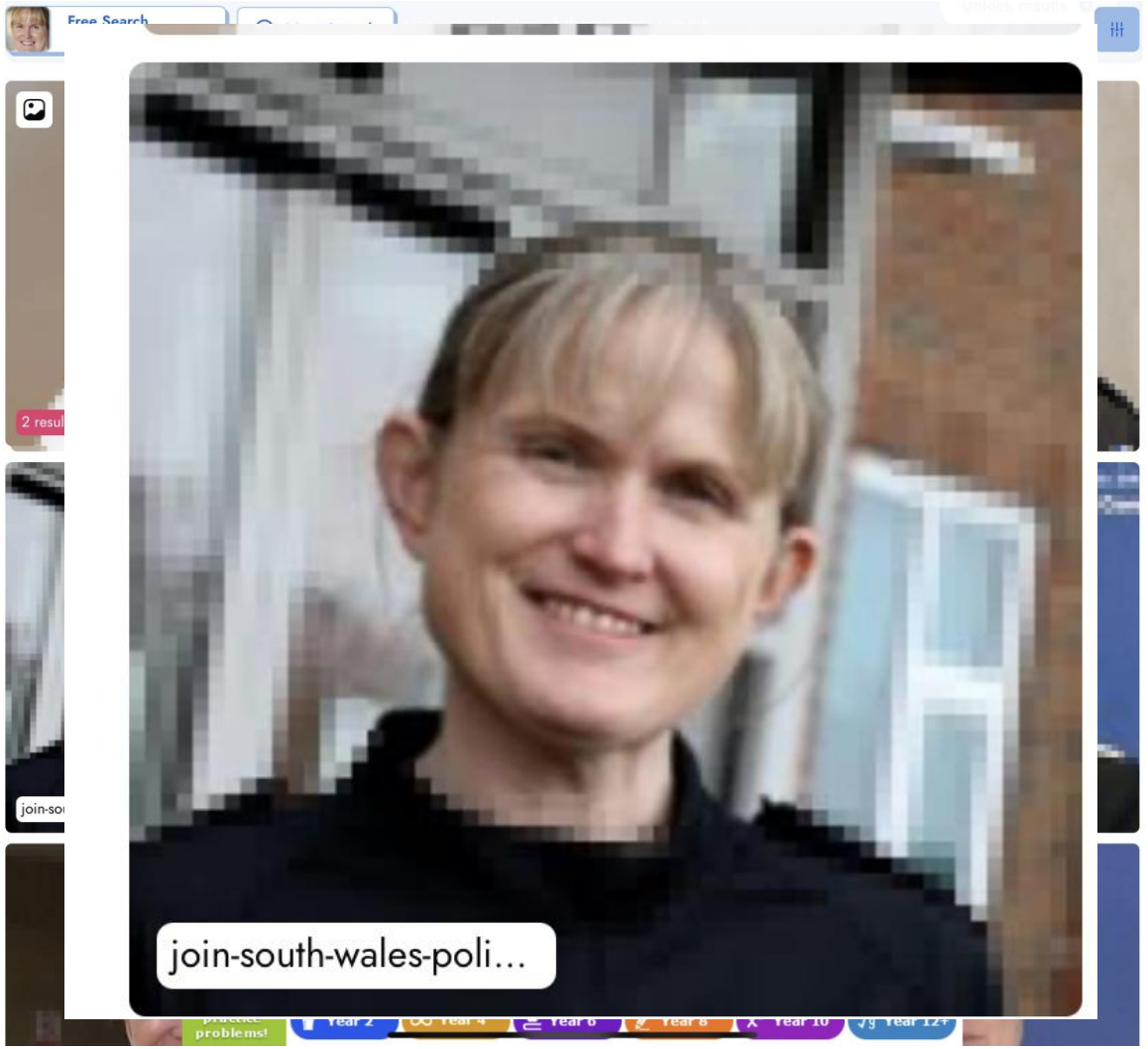
- PimEyes is a free tool which can reverse image search similar to tools such as Google
  - Pimeyes also utilises facial recognition to identify other instances of the same person online
  - It searches the
- Conducting a reverse image search of the TikTok profile picture may assist us



OFFICIAL

TIKTOK EXERCISE

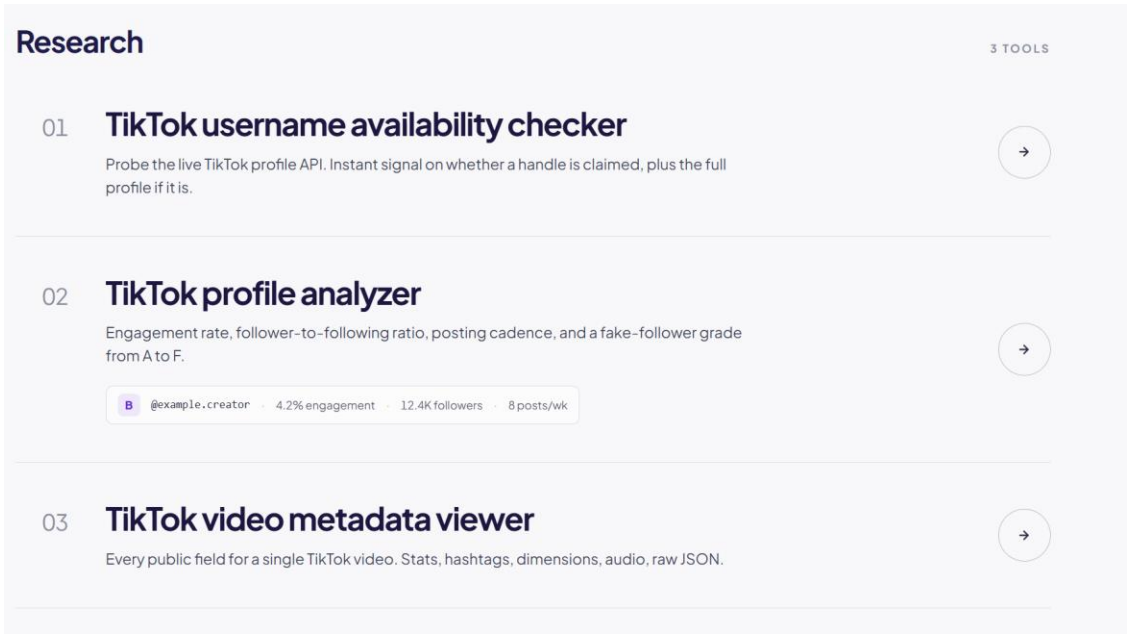


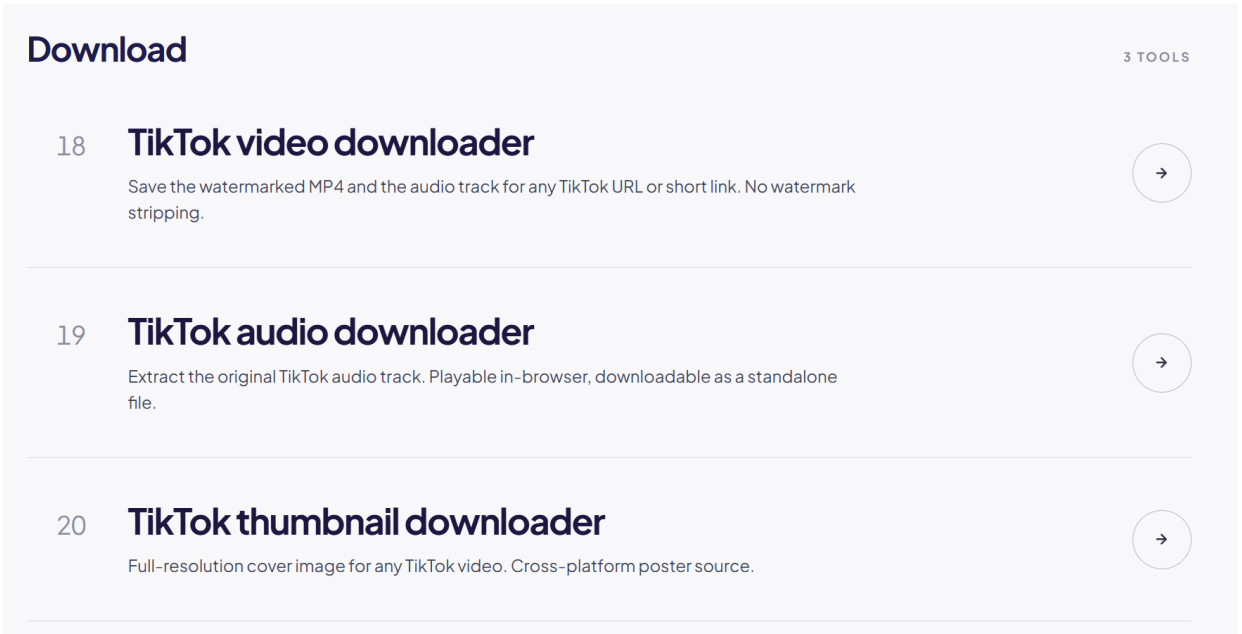


OFFICIAL

TOKTURBO

- TokTurbo is a tool designed to help users grow their channel
- It has various tools useful to use as investigators

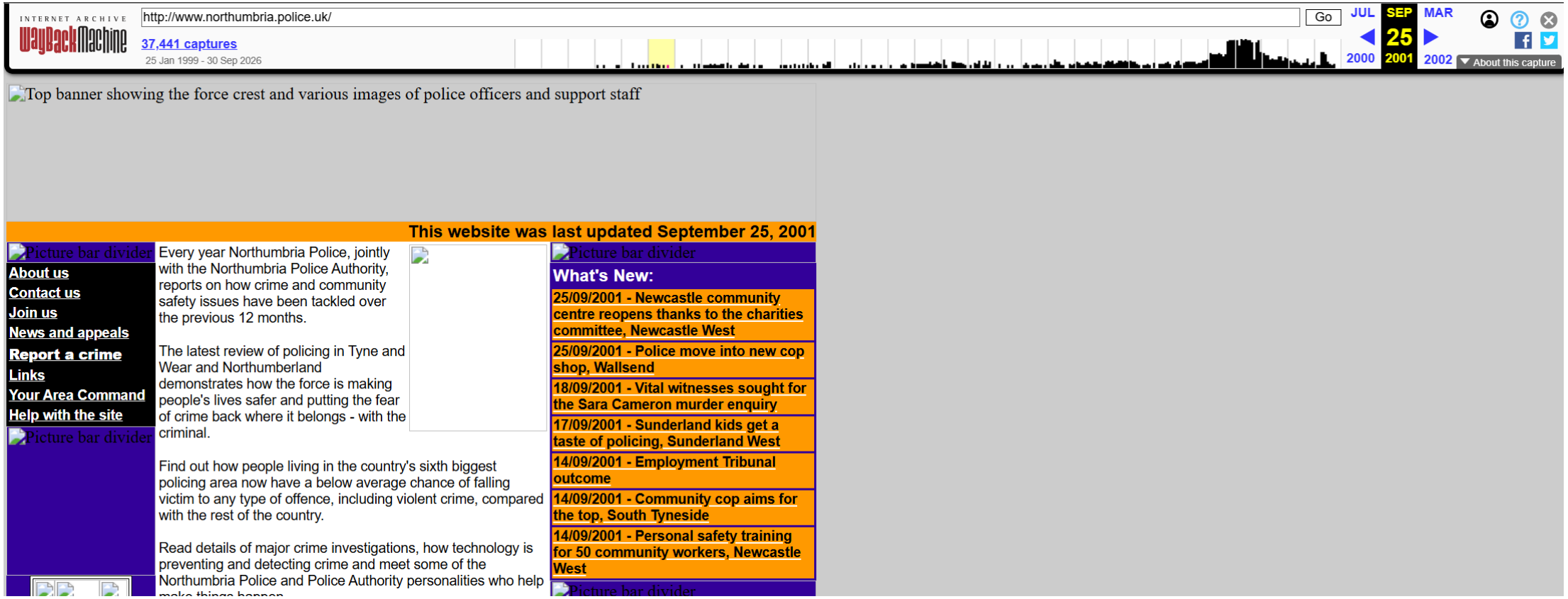




[Free TikTok toolkit · Tokturbo]

WAYBACK MACHINE

- Wayback machine offers a useful tool for capturing web pages, both past and present



GOOGLE

- Google itself can be a very powerful OSINT tool
- Most people are familiar with Google
  - Using advanced filters as part of OSINT
  - Search for:
    - Specific file types
    - Searching for “exact” terms across the internet
    - Finding files created between specific dates
- For example, you could search a website of interest for all PDF files
  - “site:company.website.domain filetype:pdf”
  - More information about Google Search operators can be found at Debugging with Google Search Operators | Google Search Central | Documentation | Google Developers



ONLINE USERNAMES

- Users often use recycle usernames across various platforms
- This is often very useful when trying to identify any other platforms of interest
- There are a number of resources freely available online to identify whether a given username is available on a website
  - Whatsmyname.app
    - Searches 667 online platforms for instances of the username
  - https://checkusernames.com is a useful resource to identify whether the username is used on another website
    - Checkusernames searches 160 social networks

Document Results: these results are document searches with the **first** username in the list used as the search term

Google Search: these results are google searches with the **first** username in the list used as the search term

Found: 38 **Processed:** 6

Show Found | Show False

Bandcamp

Username: Alanshearer
Category: music
Account Found

chatango.com

Username: Alanshearer
Category: social
Account Found

championat

Username: Alanshearer
Category: news
Account Found

eBay

Username: Alanshearer
Category: shopping
Account Found

Garmin connect

All results | PDF | Spreadsheet | Word Document | PowerPoint | Text Files | Python Code | JavaScript Code

About 219,000 results (0.19 seconds) Sort by: Relevance

Did you mean: "***Alan Shearer***"

Alan Shearer (@**alanshearer**) / X
X (formerly Twitter) › alanshearer

260 Premier League goals @BBCMOTD analyst, @premierleague @primevideosport @callawaygolf @hublot @SpeedflexLtd Instagram @**alanshearer**.

Alan Shearer (@**alanshearer**) / X
X (formerly Twitter) › alanshearer

260 Premier League goals @BBCMOTD analyst, @premierleague @primevideosport @callawaygolf @hublot @SpeedflexLtd Instagram @**alanshearer**.

Alan Shearer (@**alanshearer**) • Instagram photos and videos
www.instagram.com › alanshearer
946K followers · 711 following · 1683 posts · @**alanshearer**: "@bbcfootball analyst. Former @england captain. 260 @premierleague goals.

Alan Shearer (@**alanshearer**) • Instagram photos and videos
www.instagram.com › AlanShearer
944K Followers, 711 Following, 1682 Posts - Alan Shearer (@**AlanShearer**) on Instagram: "@bbcfootball analyst. Former @england captain.

Alan Shearer | RIP Boss. I owe you so much. You were amazing ...
Instagram › ...
Nov 26, 2023 ... 58K likes, 224 comments - **alanshearer** on November 26, 2023: "RIP Boss. I owe you so much. You were amazing. ❤️".

Alan Shearer | An amazing day playing RCD. The course is ...
Instagram › ...
May 20, 2025 ... 7582 likes, 64 comments - **alanshearer** on May 20, 2025: "An amazing day playing RCD. The course is sensational. Even a lesson from Butch ...

Alan Shearer | What a great day @goswickgolfclub with lovely lads ...
Instagram › ...
Apr 11, 2025 ... 4027 likes, 26 comments - **alanshearer** on April 11, 2025: "What a great day @goswickgolfclub with lovely lads!!!! Great weather and course in ...

Alan Shearer | Oh what a night that was !!! Ryan and the Jersey Boys ...
Instagram › reel
Mar 9, 2025 ... 1385 likes, 22 comments - **alanshearer** on March 9, 2025: "Oh what a night that was !!! Ryan and the Jersey Boys were bloody amazing.

Alan Shearer | Cheers @theowalcott Come on ...
Instagram › ...
Jul 6, 2024 ... 40K likes, 293 comments - **alanshearer** on July 6, 2024: "Cheers @theowalcott Come on Pressure is for tyres ".

Alan Shearer | Good luck today @willshearer9 running the ...

Web | Image

About 219,000 results (0.21 seconds) Sort by: Date

Team ACL | Find your Team ACL and Info | | Which player came ...
Instagram › reel › DKXmucRsUJV
2 days ago ... ... **alanshearer** @rvnistelrooij @robybaggio_official @kendrickperkins @iambarondavis And some other icons such as R9, Ricky Rubio, Jamal Murray ...

Amazon Prime Video Sport | @WayneRooney and @**AlanShearer** ...
Instagram › ...
5 days ago ... 572 likes, 4 comments - primevideosport on May 29, 2025: "@WayneRooney and @**AlanShearer** make their #UCL final predictions…".

Jack McNamara on X: "Thanks for coming @**alanshearer**" / X
X (formerly Twitter) › JackMcNamara81 › status

5 days ago ... @**alanshearer**. ·. 5h. Had a great night with my friend #PaulFerris at the @LiveTheatre to celebrate the launch of his new book 'Once Upon a Toon'.

Alan Shearer (@**alanshearer**) • Instagram photos and videos
www.instagram.com › AlanShearer
7 days ago ... 944K Followers, 711 Following, 1682 Posts - Alan Shearer (@**AlanShearer**) on Instagram: "@bbcfootball analyst. Former @england captain.

Baller League UK | A Bakary Sako hat-trick in an absolute goalfest ...
Instagram › ballerleagueuk › DKIPOpUMzib
8 days ago ... ... League UK in Copper Box Arena with @johnterry.26, @. johnterry.26 · micahrichards · garylineker · **alanshearer** · _26ers · deportriofc · 1,141 ...

Alan Shearer | From then to now @garylineker!!! It has been an ...
Instagram › ...
May 24, 2025 ... 77K likes, 444 comments - **alanshearer** on May 25, 2025: "From then to now @garylineker!!! It has been an honour to share the MOTD studio with ...

Gary Lineker on X: "RT @**alanshearer**: It has been an honour to ...
X (formerly Twitter) › GaryLineker › status

May 24, 2025 ... RT @**alanshearer**: It has been an honour to share the MOTD studio with you @GaryLineker THANK YOU for everything over the years. You are an…

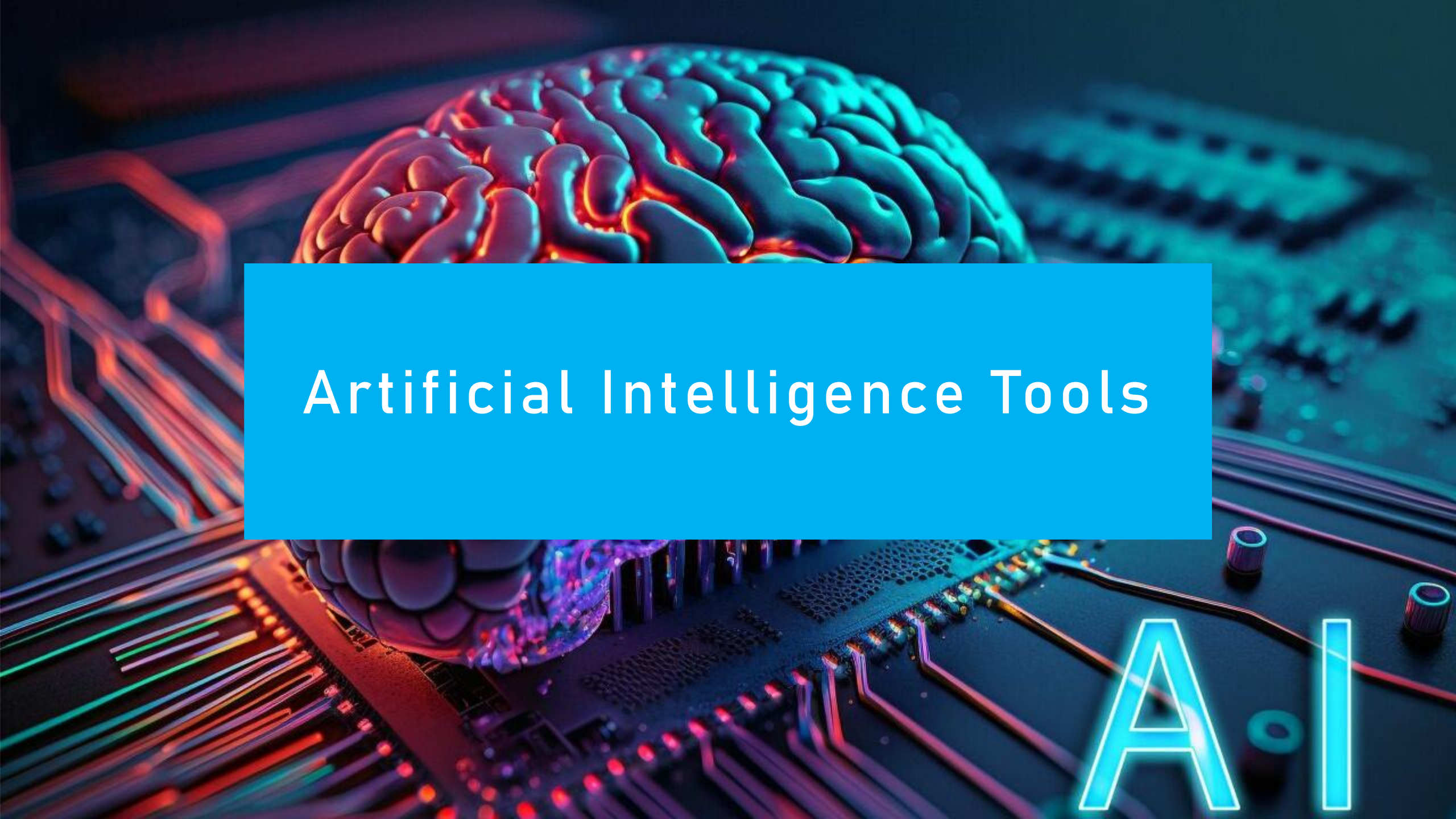
Premier League on X: "Read more about @**alanshearer's** picks here ...
X (formerly Twitter) › premierleague › status

May 20, 2025 ... Read more about @**alanshearer's** picks here ⬇️ https://t.co/vtMCbgh8rN.

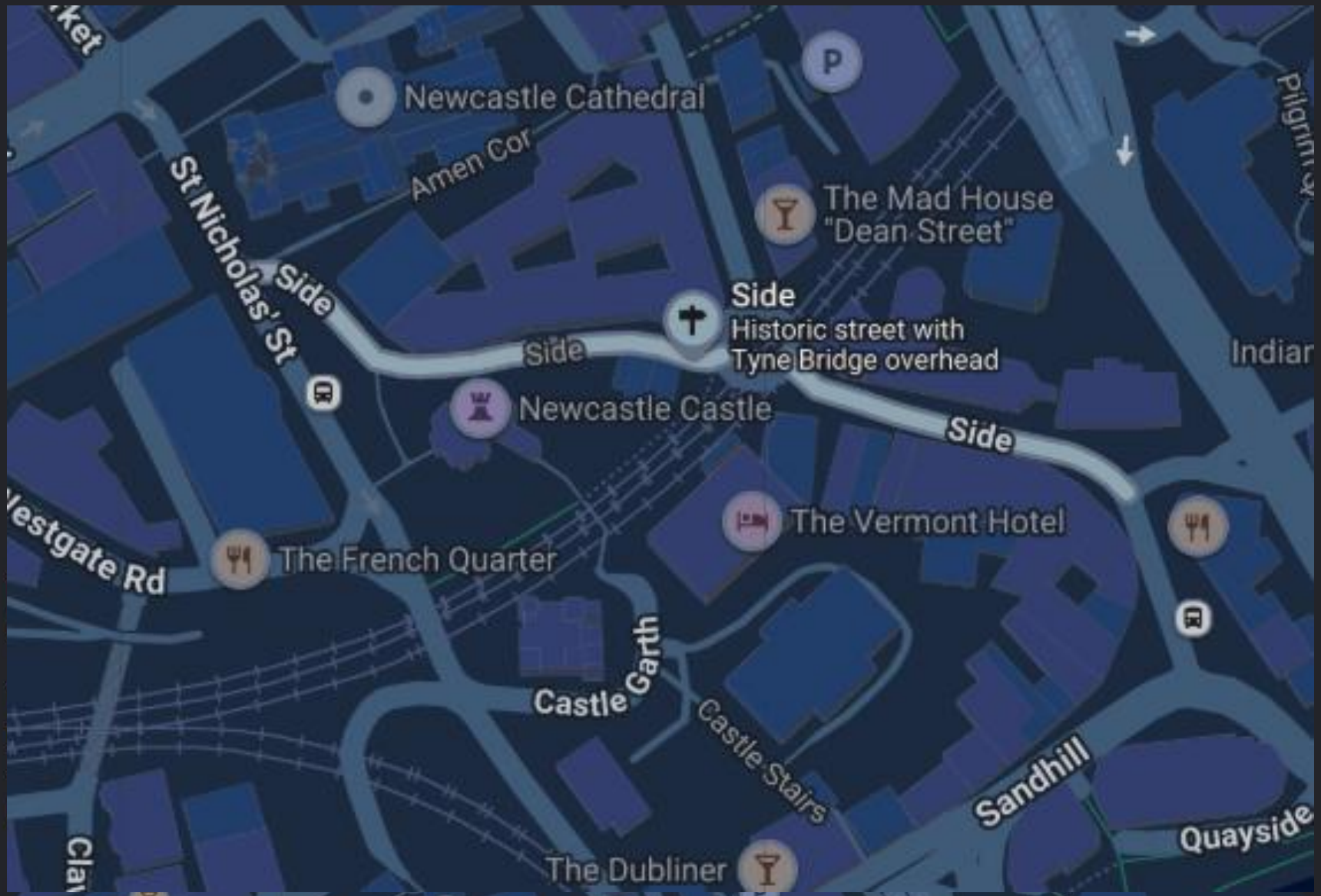
Graeme Bandeira on X: "Brilliant to hear @**alanshearer** on ...
X (formerly Twitter) › GraemeBandeira › status

May 19, 2025 ... Brilliant to hear @**alanshearer** on @RestIsFootball going on about wingers not putting balls into the box!

Alan Shearer | An amazing day playing RCD. The course is ...


Artificial Intelligence Tools
AI

AI Mode All Visual matches






Search Google Maps
11 Side
Newcastle upon Tyne, England
Google Street View
Mar 2026
See more dates
Share
AKENSIDE TRADERS
Castle
Tyne Bridge
Google Maps



here Partial solar eclipse: **29.03.2025 | 37.1%** more

Computation path of the sun for:

River Drive, South Tyneside, South Shields, Tyne

03.Jun.2025 | 21:47 UTC+1 | LIVE

Solar data for the selected location

Dawn:	03:37:24
Sunrise:	04:31:40
Culmination:	13:03:55
Sunset:	21:36:54
Dusk:	22:31:31
Daylight duration:	17h5m14s
Distance [km]:	151,754,158
Altitude:	-1.18°
Azimuth:	315.52°
Shadow length [m]:	n/a
at an object level [m]:	1

Reverse Calculation

Geodata for the selected location

Height: 0m — Set Lat/Lon

Lat:	N 55°0'16.71"	55.00464°
Lng:	W 1°25'30.68"	-1.42519°
UTM:	30U 600722 6096442	

TZ: Europe/London DST BST

More solar data & Photovoltaic

Print

Contact

Help

More for Moon|Planets|Satellites

Donate

Legal Disclosure|Privacy Policy|Cookies

Ads by Google
Stop seeing this ad
Why this ad?

SunCalc - sunrise, sunset, shadow length, solar eclipse, sun position, sun phase, sun height, sun calculator, sun movement, map, sunlight phases, elevation, Photovoltaic system, Photovoltaic

SunCalc.org ©Torsten Hoffmann 2015-2025

GeoHints

Search...









GeoHints















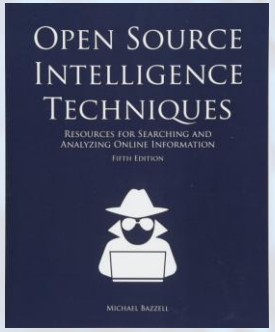


THANK YOU
ANY QUESTIONS?

Seanpaul Gilroy

Useful Resources

- The Ultimate OSINT Collection - start.me
- OSINT Framework
- Open Source Intelligence Techniques – Book
- UK-OSINT
- Inteltechniques.com
- bellingcat - the home of online investigations



ChatGPT

CONINSEC
CONSULTING INVESTIGATION SECURITY

Digital Investigations, Open-Source Intelligence Tools and AI

15 October 2026 Budapest

Evidence Collection, Due Diligence and Online Searches

Bilal Şen

Corporate Investigations and Cybercrime Advisor

Co-funded by the European Union



- Cybercrime Centre – Turkish National Police
- Manager, Global Program on Cybercrime Program – UNODC
- Senior Consultant – Industry

- Led Tech Investigations
- Consulted International Organisation
- Delivered sessions in five continents
- Currently Helping Businesses and Law Firms

Please Ask Me

- OSINT
- Cybercrime
- Electronic Data from ISPs
- Case Discussions
- Digital Forensics

OSINT

Open-Source Intelligence (OSINT) is the practice of collecting and analysing publicly available information such as websites, social media, news, breach data repositories, archive records and official records to uncover valuable insights.

It supports legal, investigative, and business decisions by revealing hidden connections, verifying facts, and identifying risks, all through ethical and legal means.

Open source intelligence systematic can strengthen your legal practice, uncover the truth.

OSINT USAGE FOR JUDICIAL AUTHORITIES

Evidence validation: Authenticity, timelines, source reliability, digital evidence assessment.

Investigative support: Identifying persons, entities, locations, affiliations, and relevant facts.

Asset identification: Real estate, vehicles, business interests, beneficial ownership, cross border assets.

Fraud and forgery: False identities, forged documents, shell companies, deception indicators.

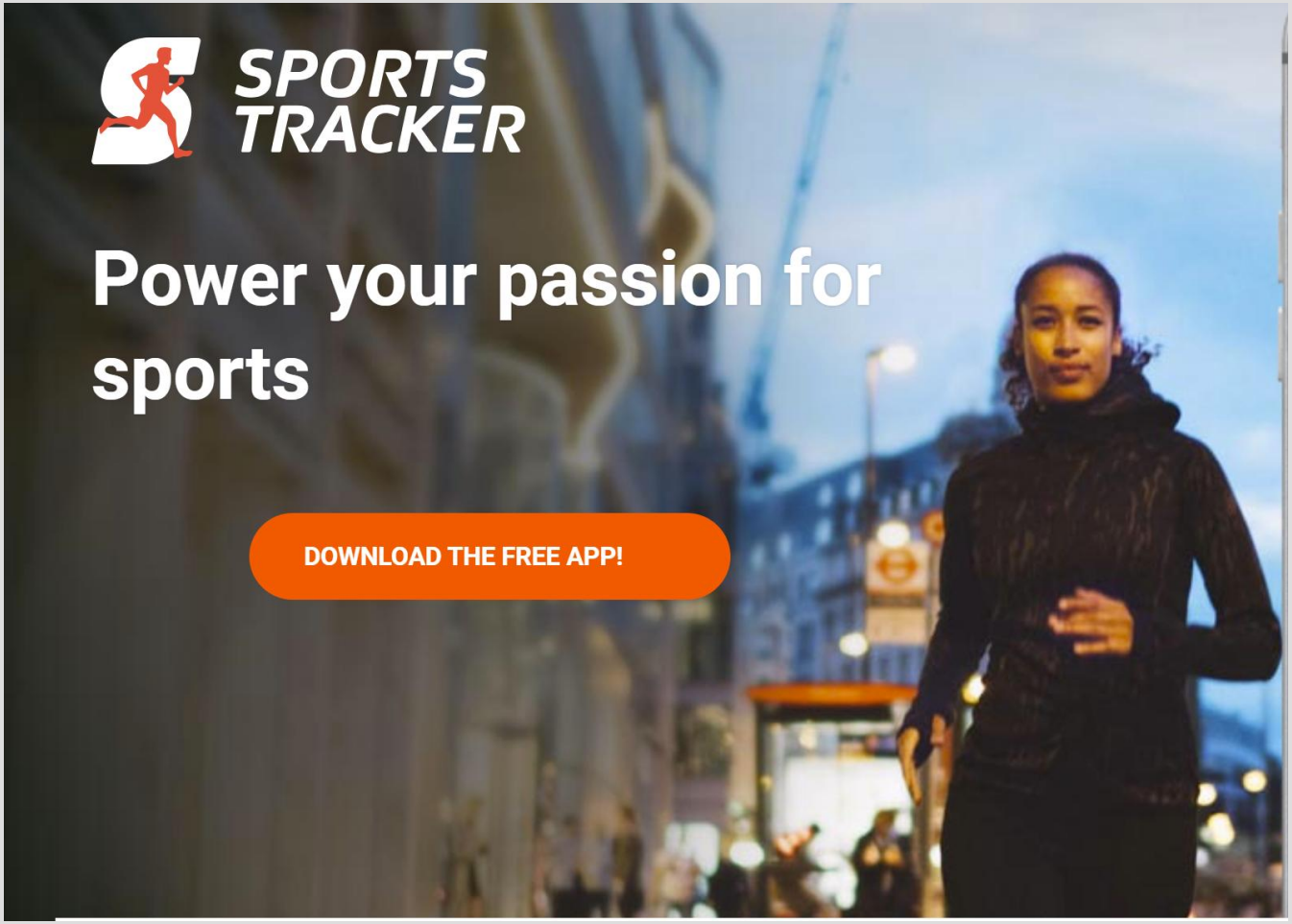
Network analysis: Relationships between individuals, companies, organizations, and criminal groups.

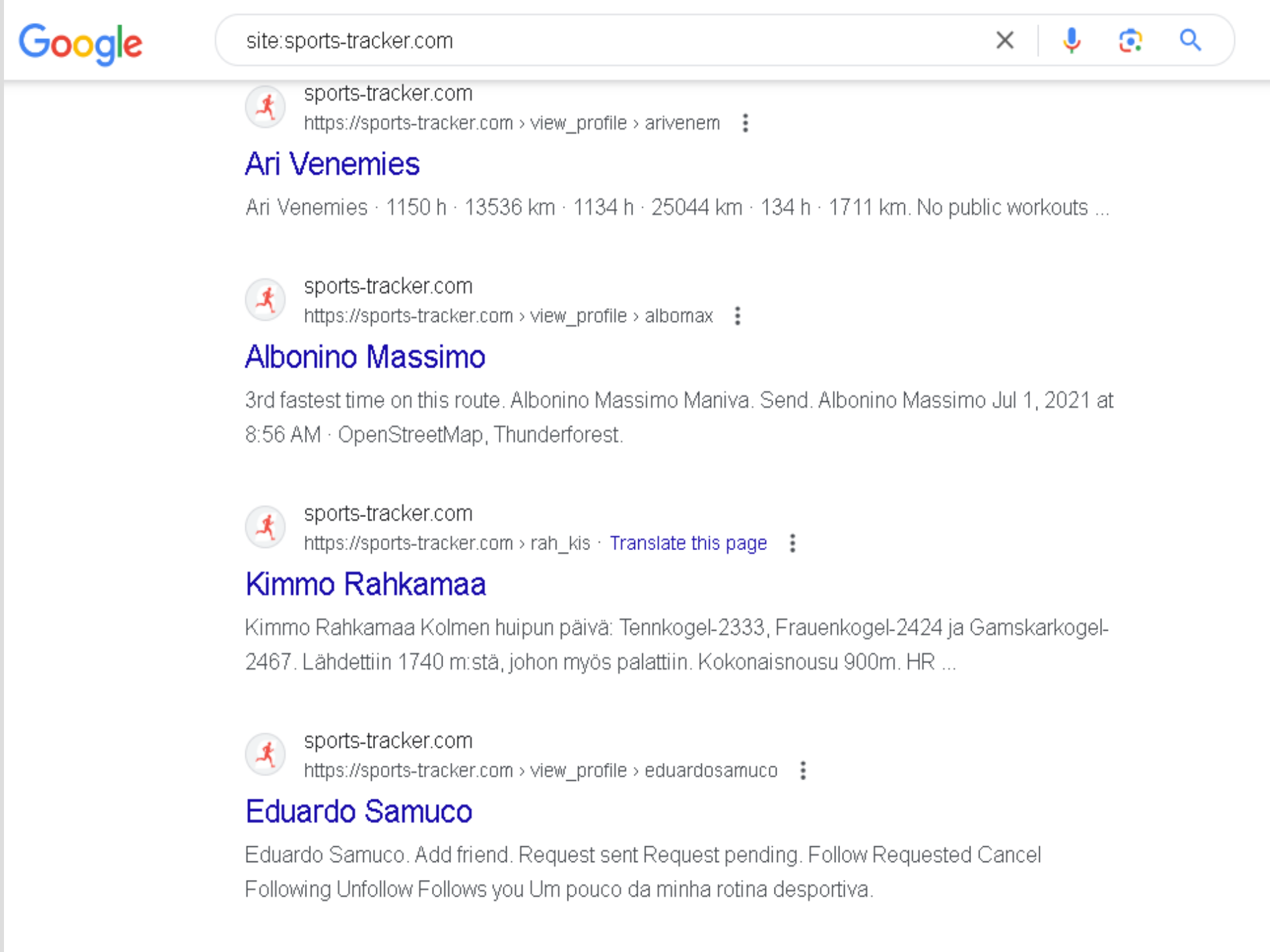
Cybercrime investigations: Social media, digital footprints, online threats, and internet based offences.

Public safety & corruption: Organized crime, corruption risks, emerging threats, and public interest concerns.

WHO CREATES ONLINE INFO ABOUT US

- **We**
- Our Private And Professional Contacts
- Competitors
- Professionals
- Institutions / Companies
- Machines
- **Breach Records**


SPORTS TRACKER
Power your passion for sports
DOWNLOAD THE FREE APP!


Google
site:sports-tracker.com
sports-tracker.com
https://sports-tracker.com › view_profile › arivenem
Ari Venemies
Ari Venemies · 1150 h · 13536 km · 1134 h · 25044 km · 134 h · 1711 km. No public workouts ...
sports-tracker.com
https://sports-tracker.com › view_profile › albomax
Albonino Massimo
3rd fastest time on this route. Albonino Massimo Maniva. Send. Albonino Massimo Jul 1, 2021 at 8:56 AM · OpenStreetMap, Thunderforest.
sports-tracker.com
https://sports-tracker.com › rah_kis · Translate this page
Kimmo Rahkamaa
Kimmo Rahkamaa Kolmen huipun päivä: Tennkogel-2333, Frauenkogel-2424 ja Gamskarkogel-2467. Lähdettiin 1740 m:stä, johon myös palattiin. Kokonaisnousu 900m. HR ...
sports-tracker.com
https://sports-tracker.com › view_profile › eduardosamuco
Eduardo Samuco
Eduardo Samuco. Add friend. Request sent Request pending. Follow Requested Cancel Following Unfollow Follows you Um pouco da minha rotina desportiva.

SOME OF COMMON BREACH RECORDS







Platform	Year	Records
LinkedIn	2016	117 M
LinkedIn	2021	700 M
LinkedIn	2023	500 M
Facebook	2019	419 M
Facebook	2021	533 M
X (Twitter)	2023	235 M+

MOST HELPFUL INFO TO START

PERSON

Full Name

Date of Birth

Email Address

Mobile Phone Number

Headshot Photo

Profession or Position

ENTITY

Full Name

Website

Tax Number

Email Addresses

Business Addresses

Shareholders/Managers

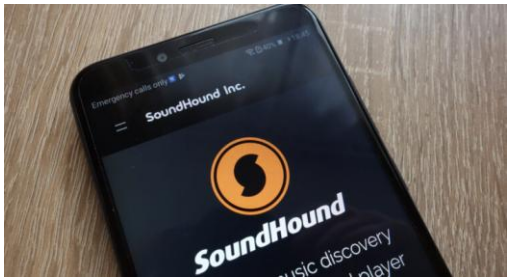
SEARCH POSSIBLE WITH

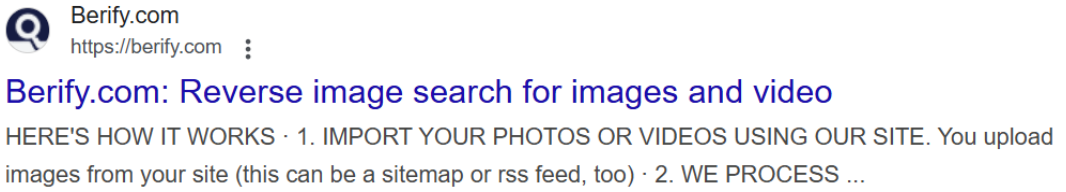
- Text
- Image/ Live Photo
- Voice
- Video
- File
- Domain Name or URL



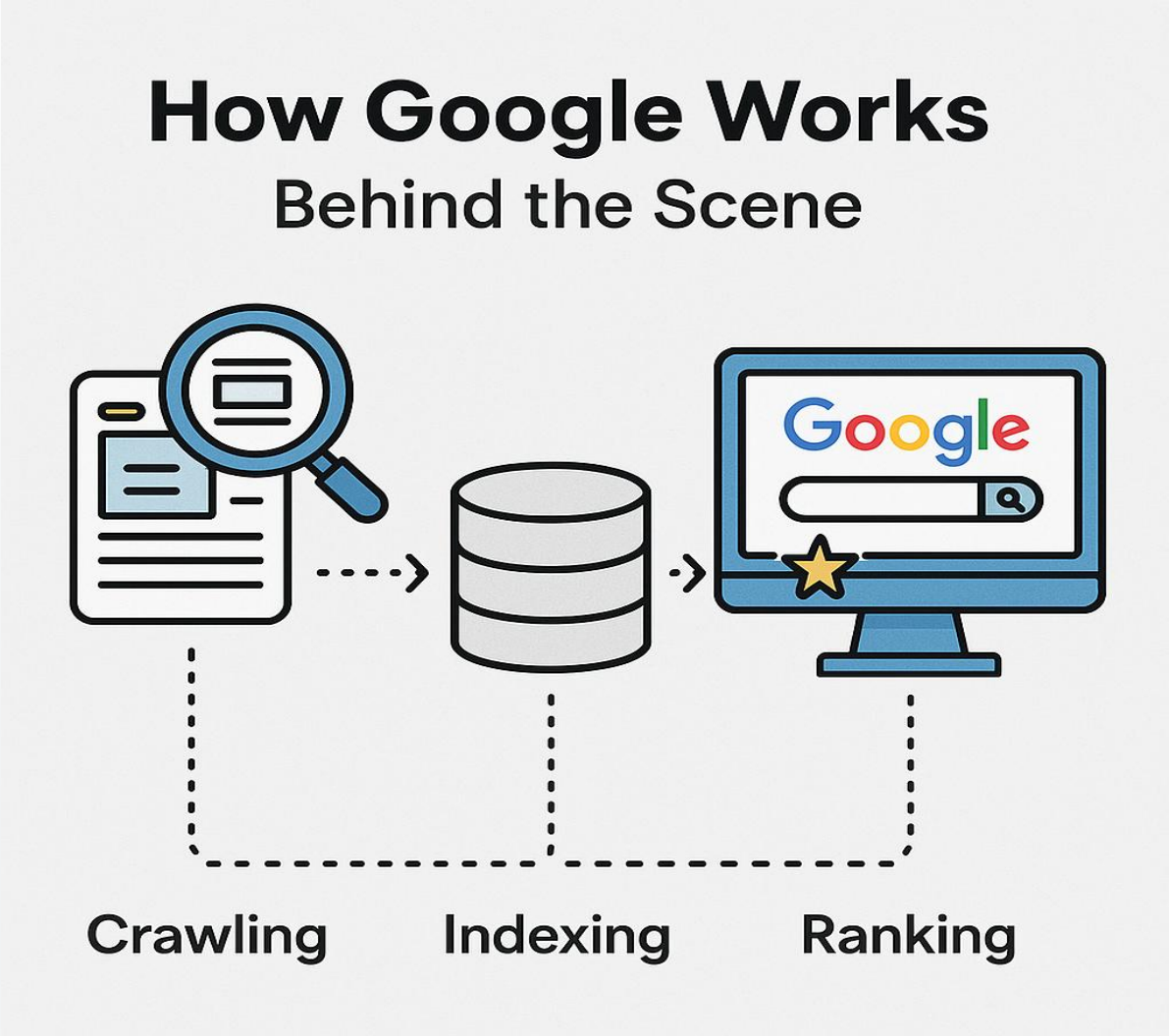




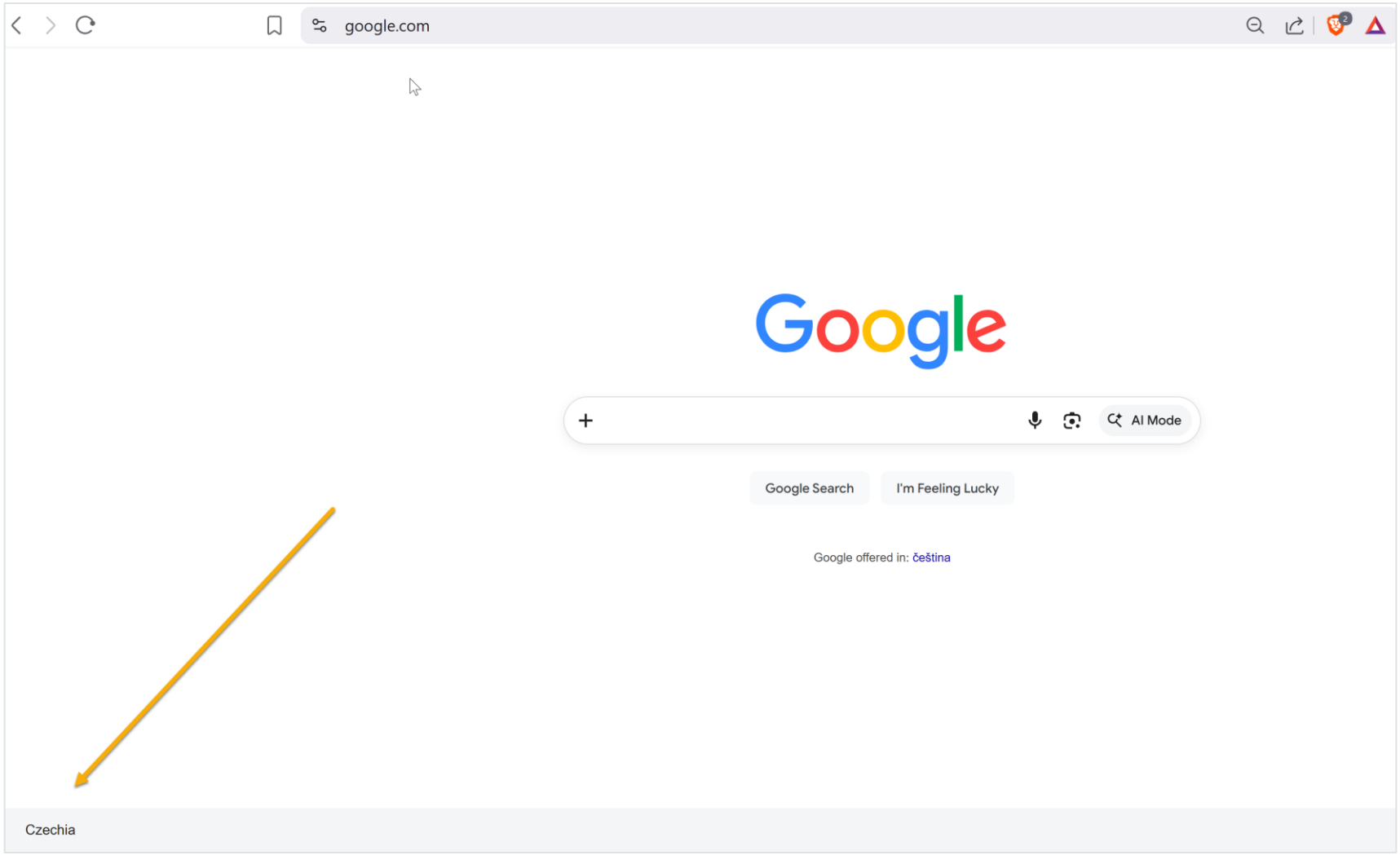




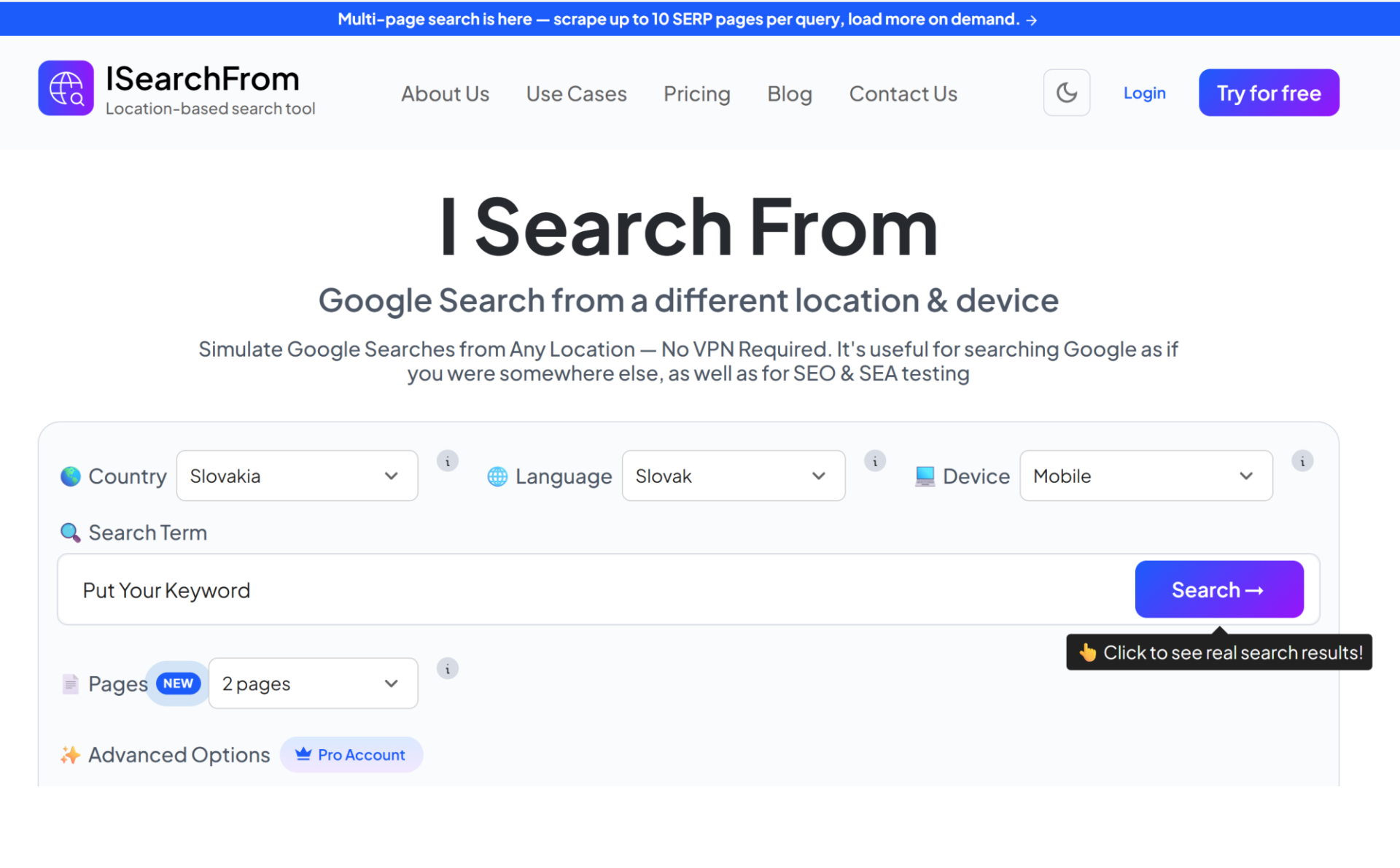
GOOGLE SEARCH PROCESS



GOOGLE LOCAL COPY SEARCH TEST



isearchfrom.com



OSINT TOOLS



OSINT

OPEN SOURCE INTELLIGENCE

Collect. Analyze. Understand.
Intelligence from open sources.



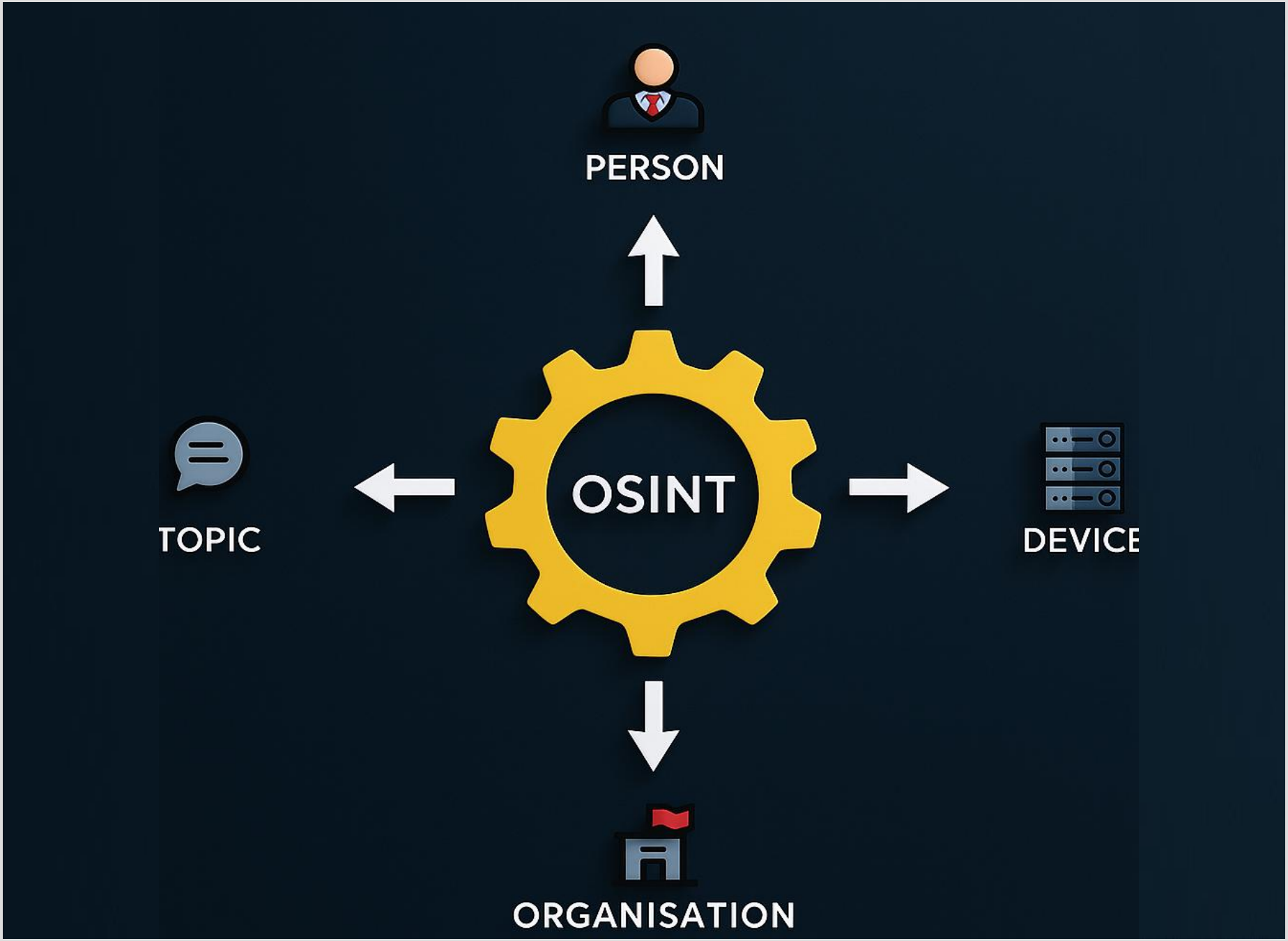
FIND
Discover relevant information

FILTER
Remove noise, focus on what matters

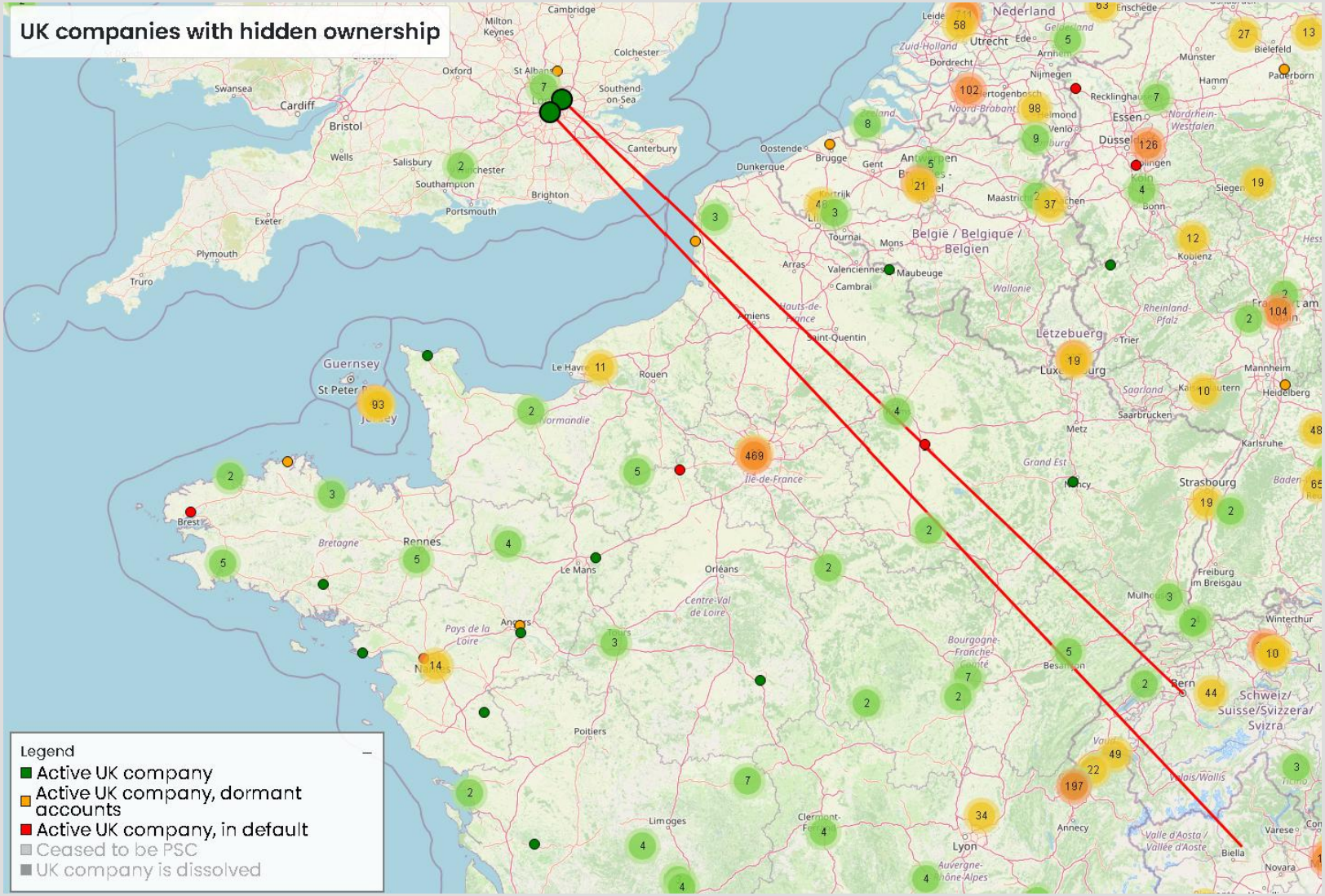
ANALYZE
Extract insights and patterns

VERIFY
Validate and cross-check information

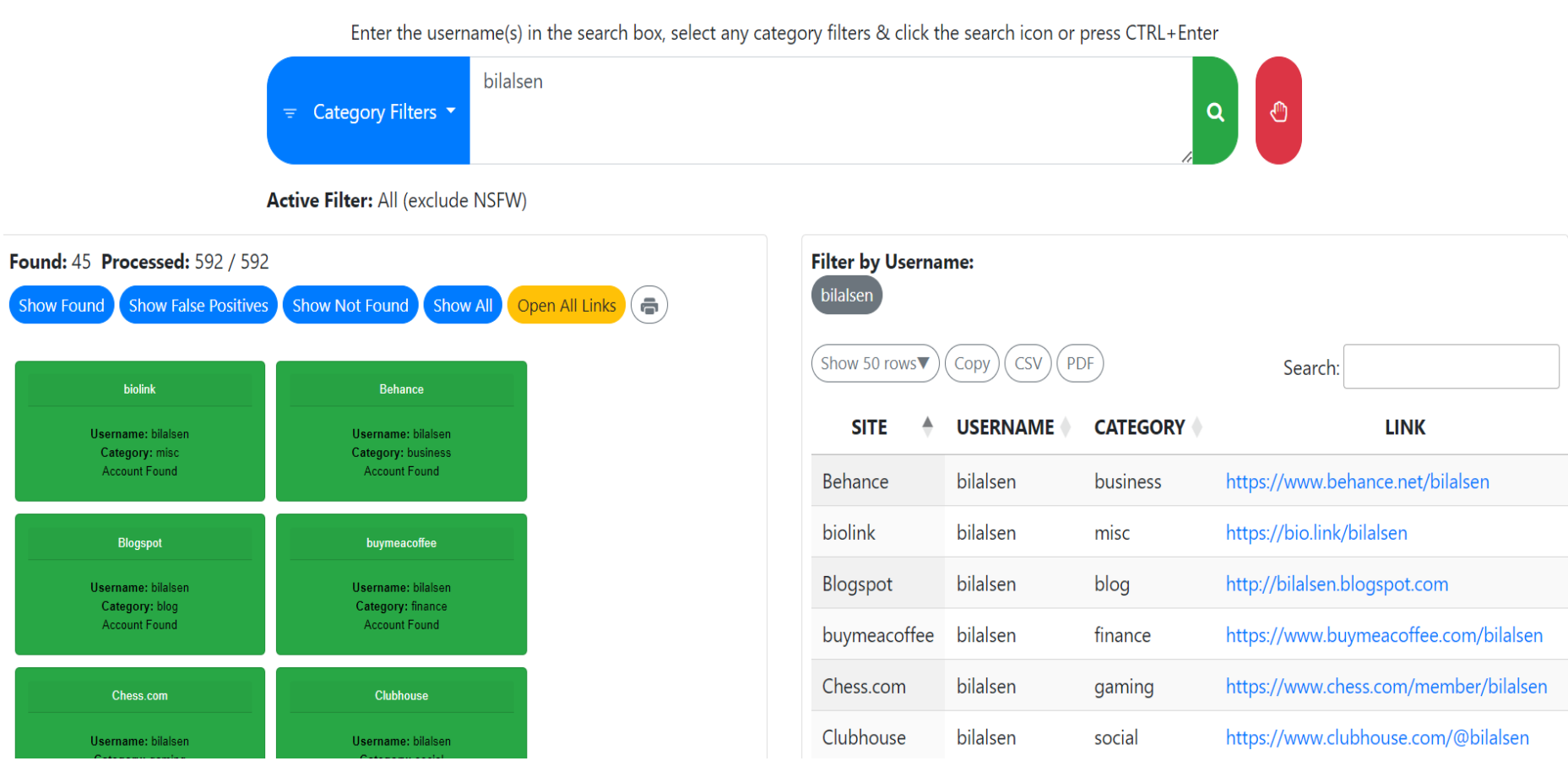
UNDERSTAND
Turn information into intelligence


PERSON
TOPIC
OSINT
DEVICE
ORGANISATION

HIDDEN BUSINESS OWNERSHIP



USERNAME SOLUTION WHATSAPPMYNAME



paypal.com/paypalme/bilalsen

Privatkunden KMU Großunternehmen Developer Hilfe Einloggen Neu anmelden



Bilal Sen
@BilalSen
Lommel

Senden

Diesen Link melden

chess.com/member/bilalsen

Chess.com

Play

Puzzles

Learn

Watch

News

Social

More

Search

Sign Up



bilalsen

Bilal Şen

Jan 3, 2024

Jan 2, 2018

8

12

Gift

Challenge

Message

More

Current Games (0)

No games in progress

site:drive.google.com limited payment

All Images News Videos Maps More Tools

Life insurance | Visa | Policy | Solutions | SumUp | Wise | SWIFT | Depop

google.com
https://drive.google.com › viewerng › viewer › custom...

customer-information-sheet-for-inward-payments-to-hong ...

Please instruct remitting banks to send the **payment** instruction to us (HSBCHKHHHKH) by SWIFT MT103 with *the ... HSBC Bank Australia **Limited**, Sydney HSBC Bank ...

google.com
https://drive.google.com › viewerng › viewer › 3.-term...

3.-terms-of-sale.pdf

Paid Content. means purchase of **Paid** Content on our website as a. one-off transaction;. "Sale Confirmation" means our acceptance and confirmation of your.

google.com
https://drive.google.com › drive › my-drive

Google Drive: Sign-in

Sign in. to continue to Google Drive. Email or phone. Forgot email? CAPTCHA image of text used to distinguish humans from robots.

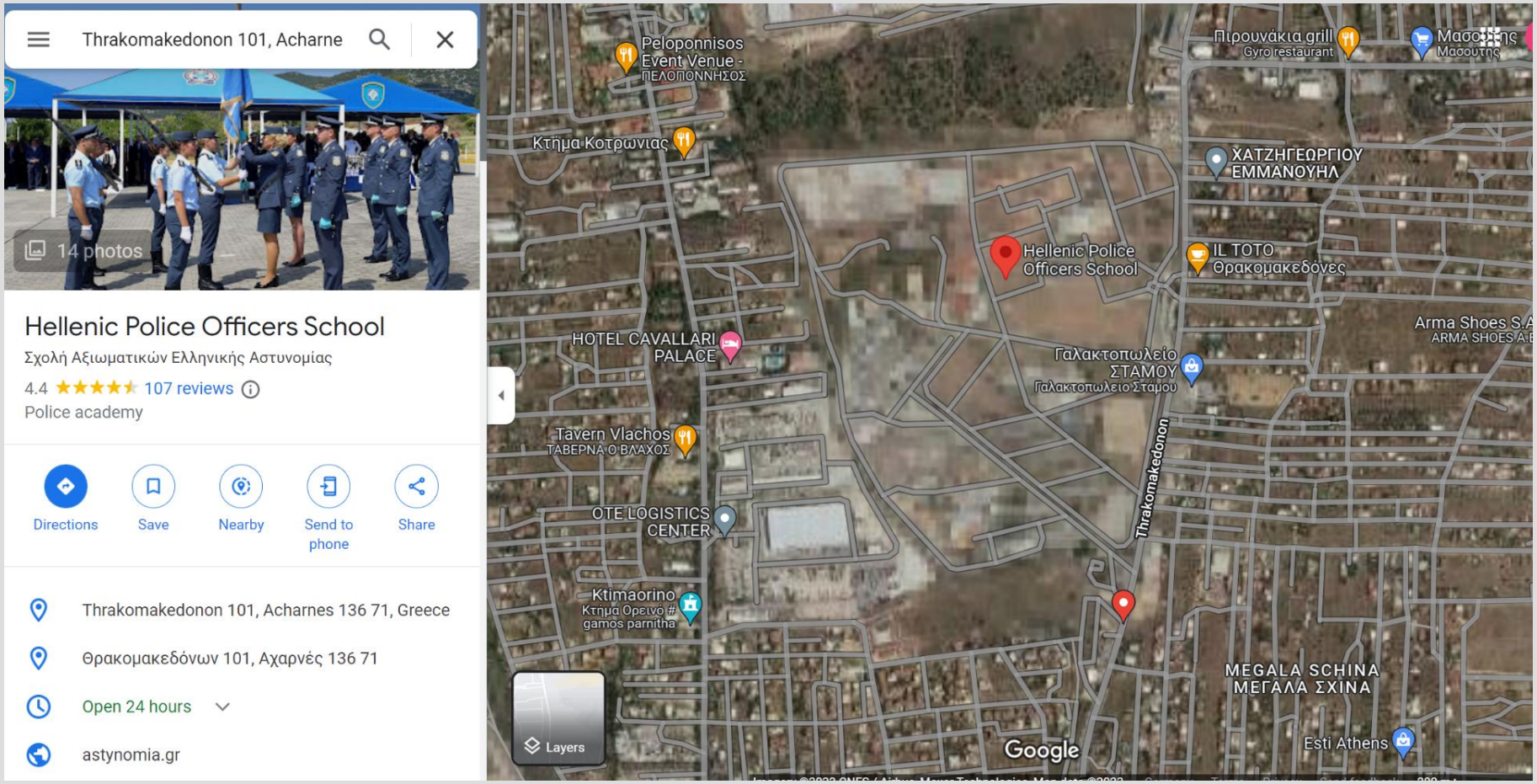
google.com
https://drive.google.com › viewerng › viewer › year_ro...

year_round_e.pdf

– The above offers are valid from 1 January to 31 December 2020. – Customer must settle the **payment** with enJoy Card to enjoy the above offers (Some offers must ...

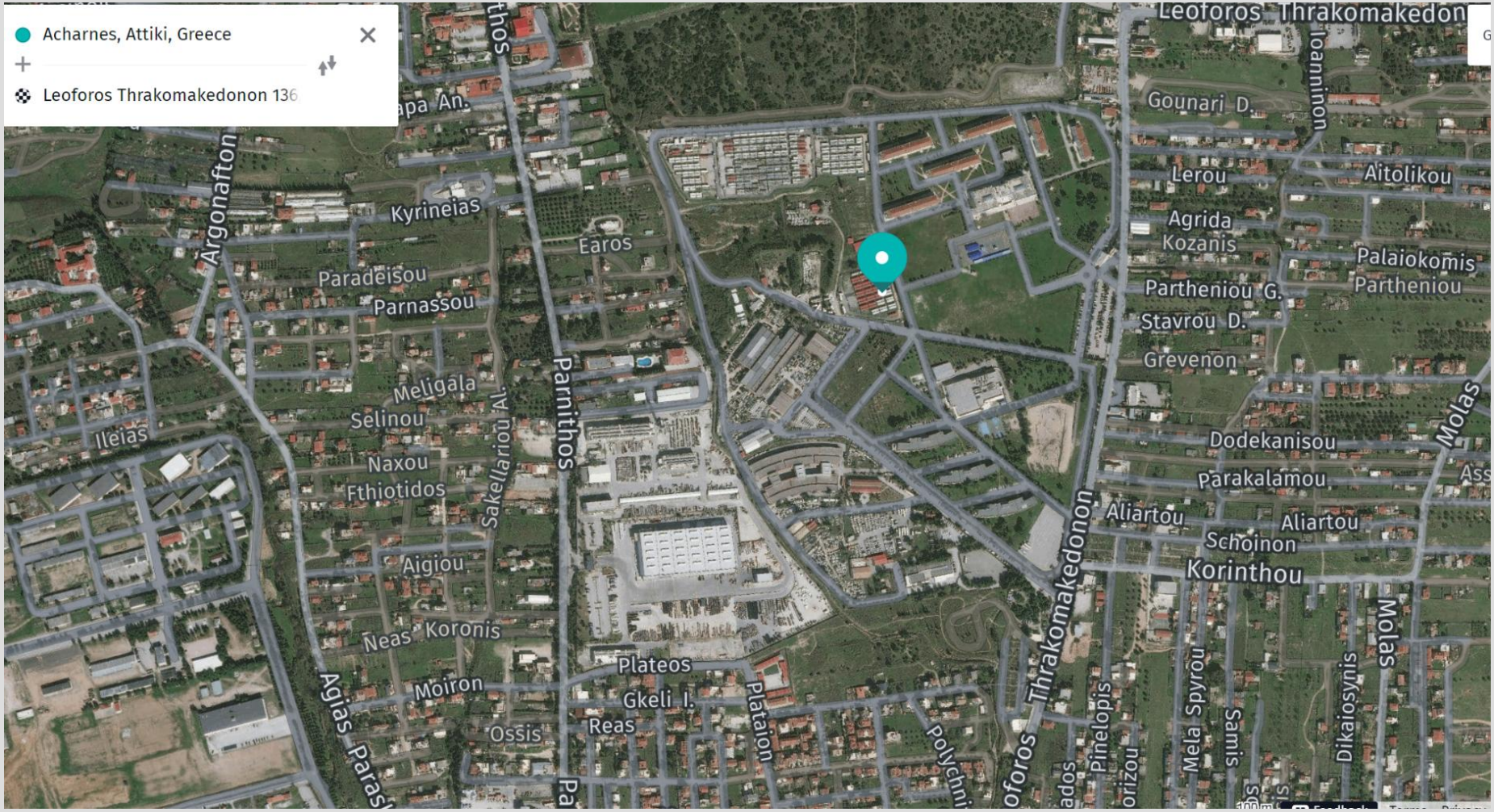
ALTERNATIVE COULD BE BETTER

GOOGLE MAP RESULTS

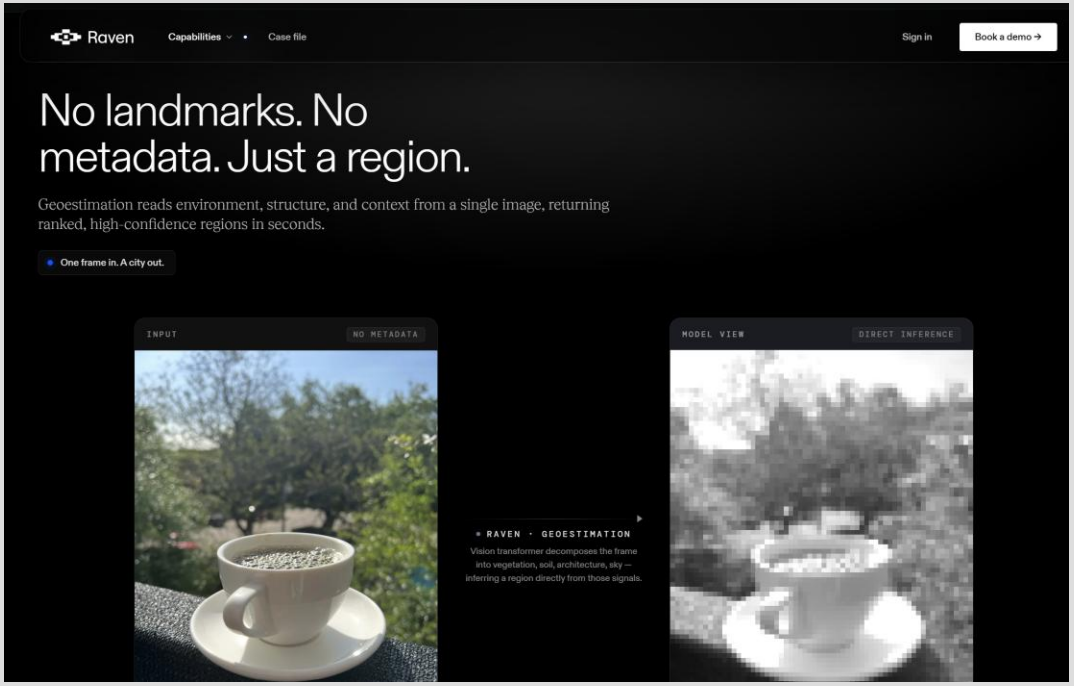


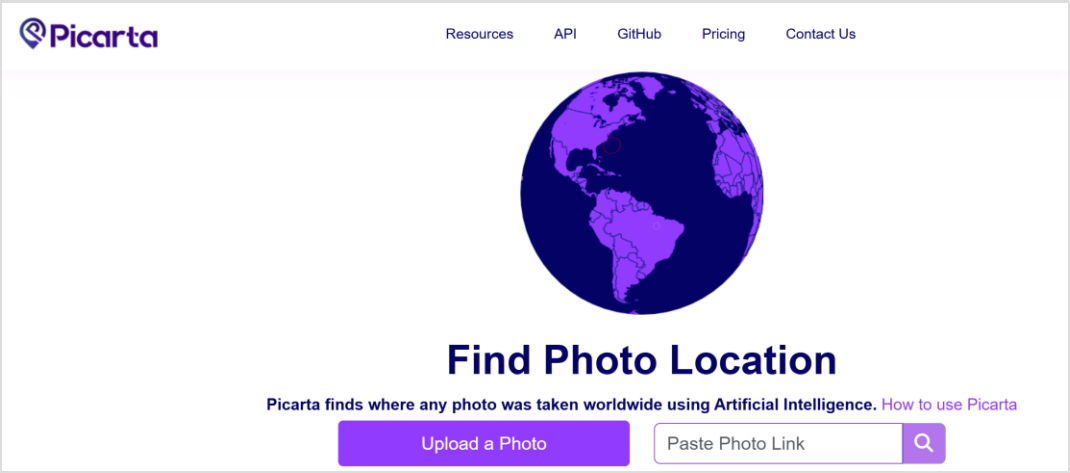
ALTERNATIVE COULD BE BETTER

wego.here.com

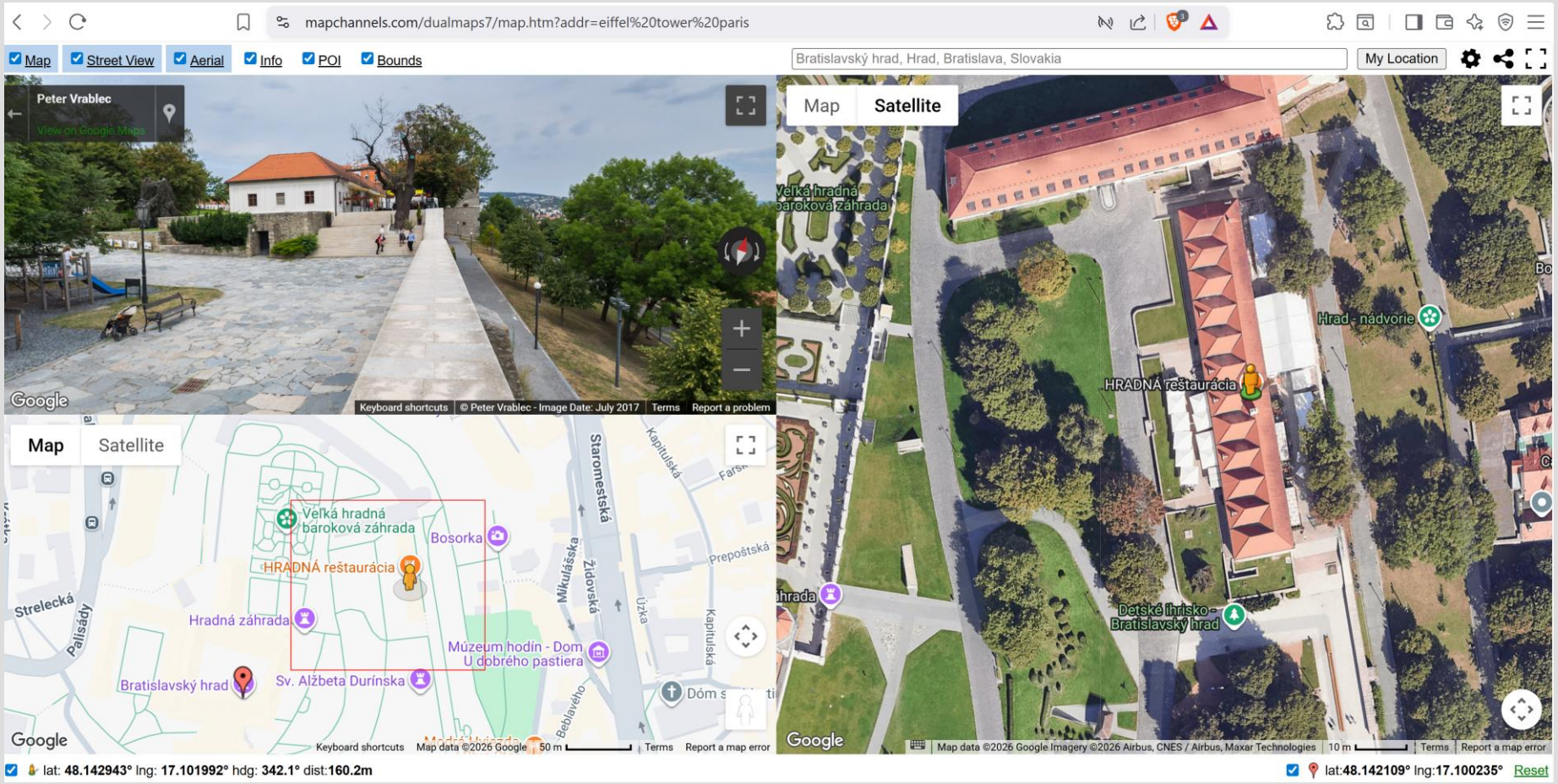


GEOLOCATION – RAVEN & PICARTA

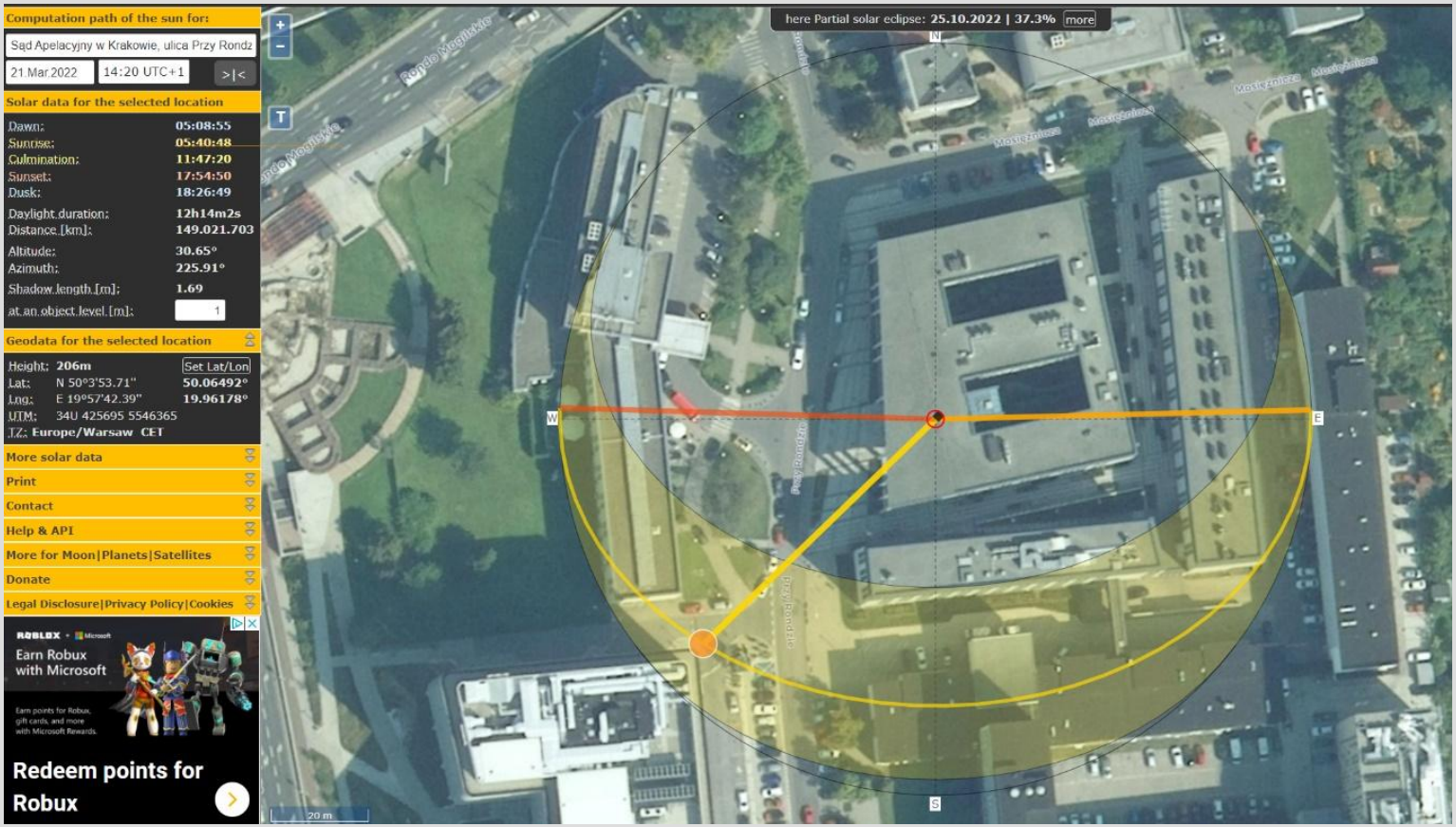




GEOLOCATION - DUALMAP



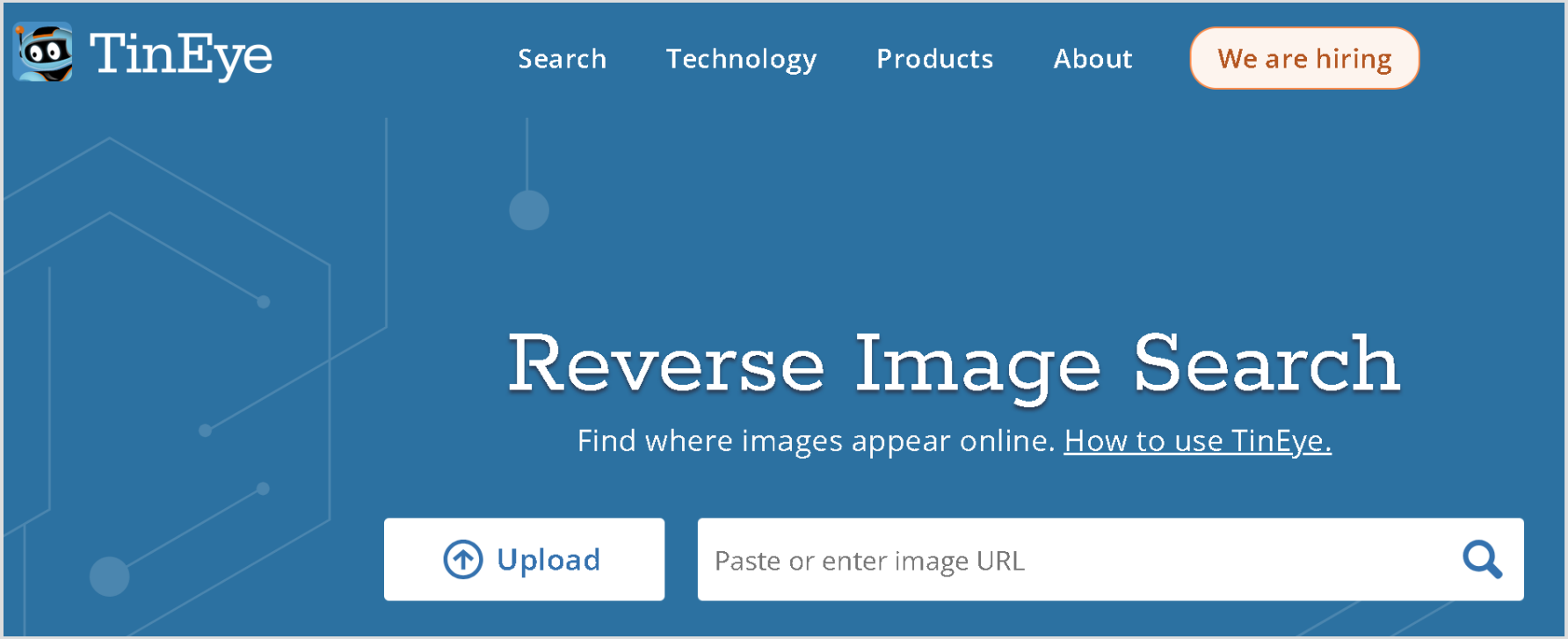
suncalc.org



SunCalc is a sunlight calculator that helps determine the time and date based on the sun's movement and sunlight analysis for a given day and location.

www.suncalc.org/#/50.0649,19.9618,19/2022.03.21/14:20/1/1

tineye.com


TinEye
Search
Technology
Products
About
We are hiring
Reverse Image Search
Find where images appear online. How to use TinEye.
Upload
Paste or enter image URL

Tineye Test



tineye.com



STOCK · SPONSORED

ENJOY 15% OFF. Use TINEYE15 on Shutterstock.

www.shutterstock.com

image-photo/paris-sept-17-2014-wester... - First found on Jun 11, 2022



STOCK · SPONSORED

stock.adobe.com

images/Prospetto-di-Notre-Dame-a-Par... - First found on Oct 25, 2021



STOCK · SPONSORED

www.alamy.com

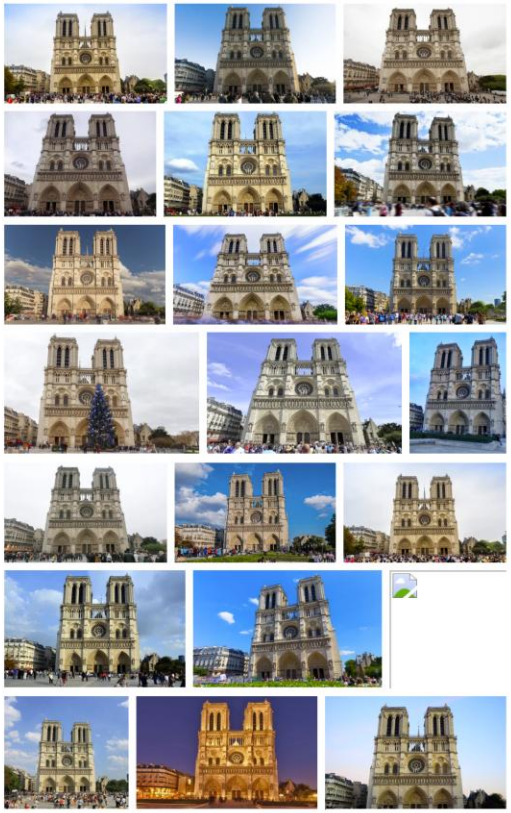
paris-sept-17-2014-the-western-facade-... - First found on Sep 25, 2021



dinneratmidnight.wordpress.com

2010/11/14/travels-part-2-paris/ - First found on May 14, 2017
2010/11/14/travels-part-2-paris/ - First found on May 14, 2017
view all 3 matches

Filename: **paris-29.jpg** (1963 x 3081, 558.4 kB)



shutterstock | GET 10 FREE



The ultimate OSINT tool for email and phone reverse lookup

Email | Phone NEW

Use 1 credit

test@example.com

Search

Search options

ALERT MANAGEMENT

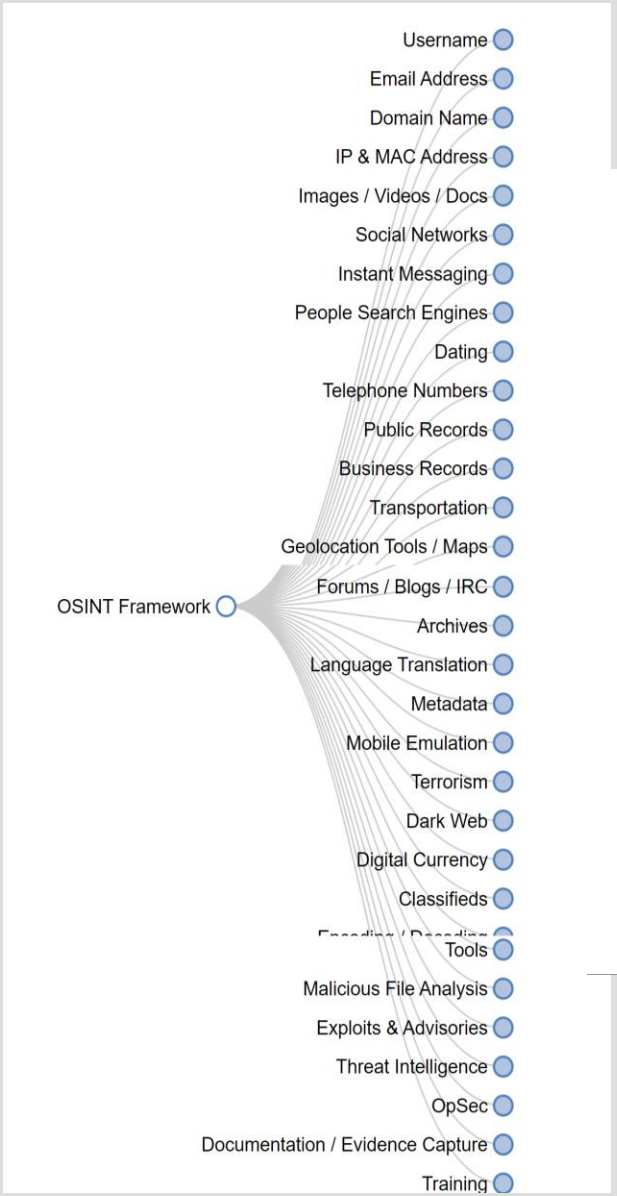


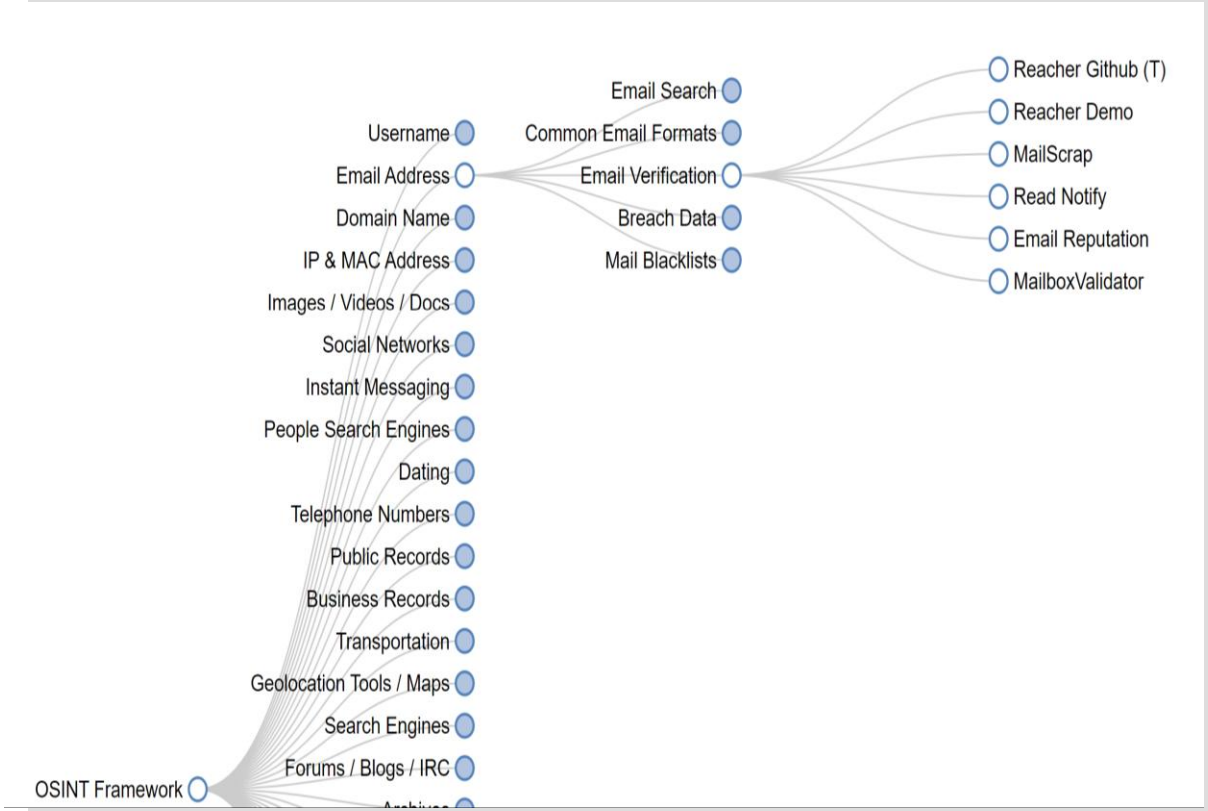
Search alerts are created and managed through an automated process that passively collects timely and up to date information.

www.talkwalker.com/alerts

www.google.com/alerts

OSINT FRAMEWORK





osintframework.com

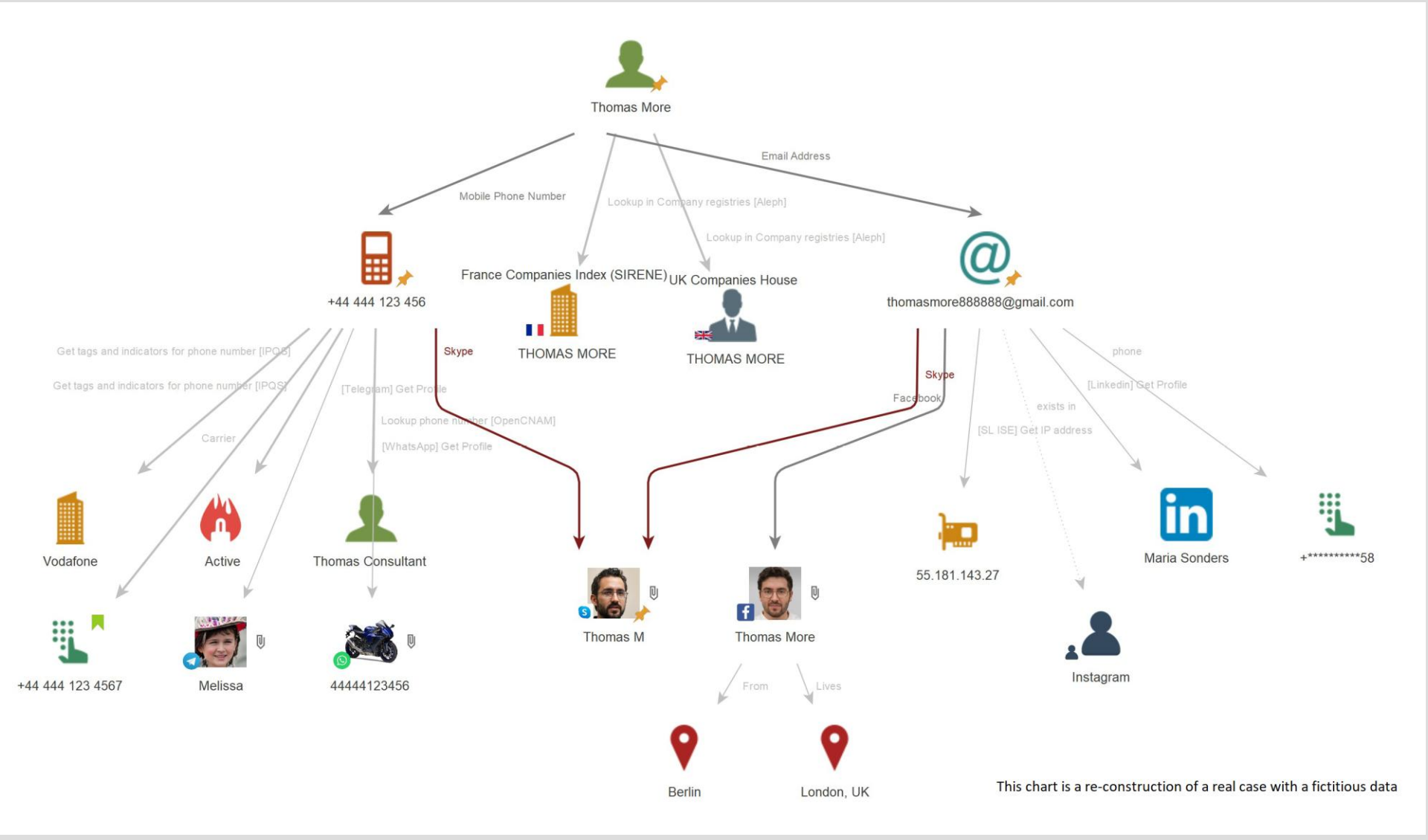
ONLINE DATA IS VOLATILE

Archive

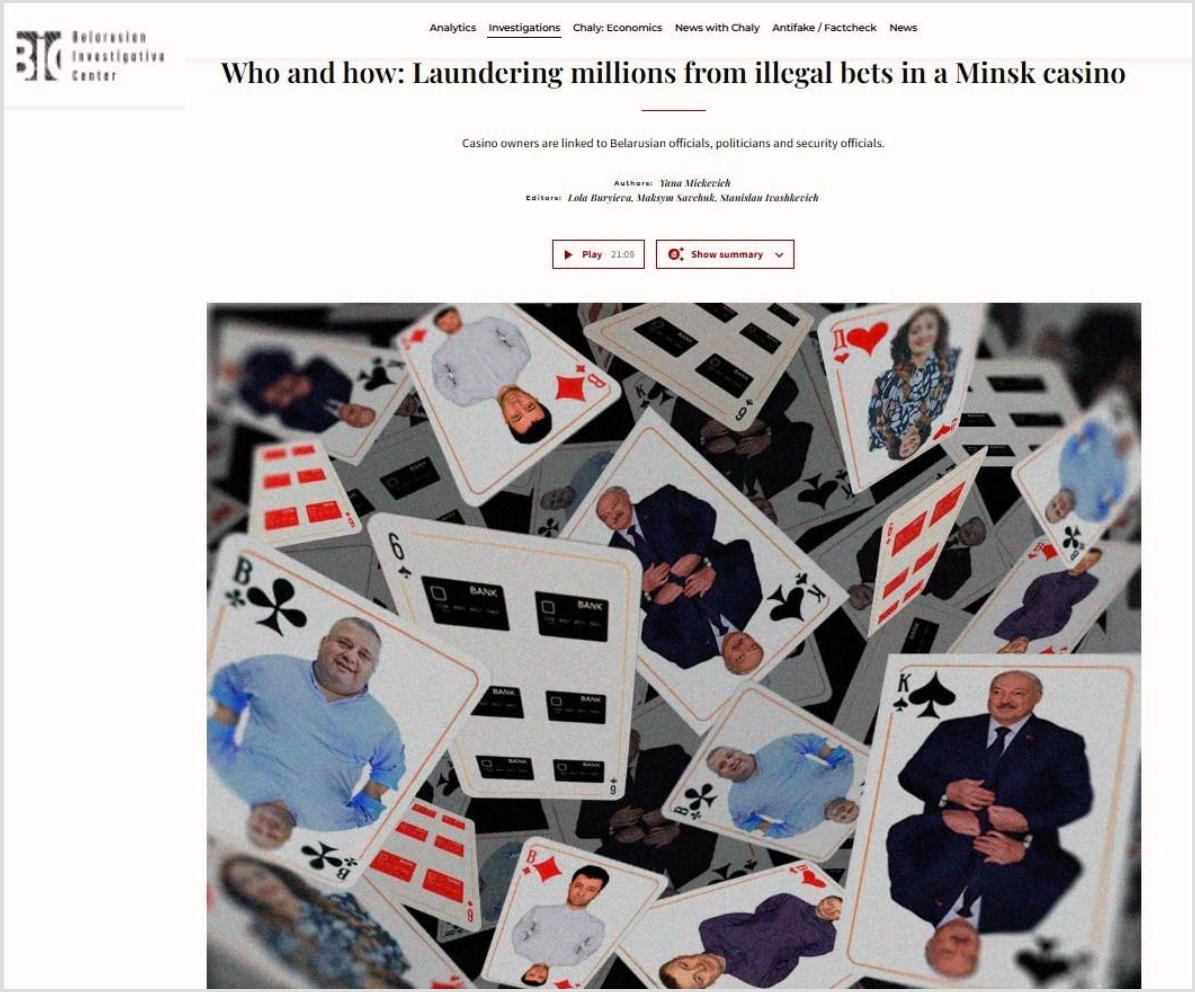
URL Collection

Freezing The Time

SAMPLE SOCMINT CHART



VERIFICATION & ADMISSIBILITY



Belarusian Investigative Center

Analytics Investigations Chaly: Economics News with Chaly Antifake / Factcheck News

Who and how: Laundering millions from illegal bets in a Minsk casino

Casino owners are linked to Belarusian officials, politicians and security officials.

Authors: *Yana Mickevich*
Editors: *Lola Buryieva, Maksym Savchuk, Stanislau Iwashkevich*

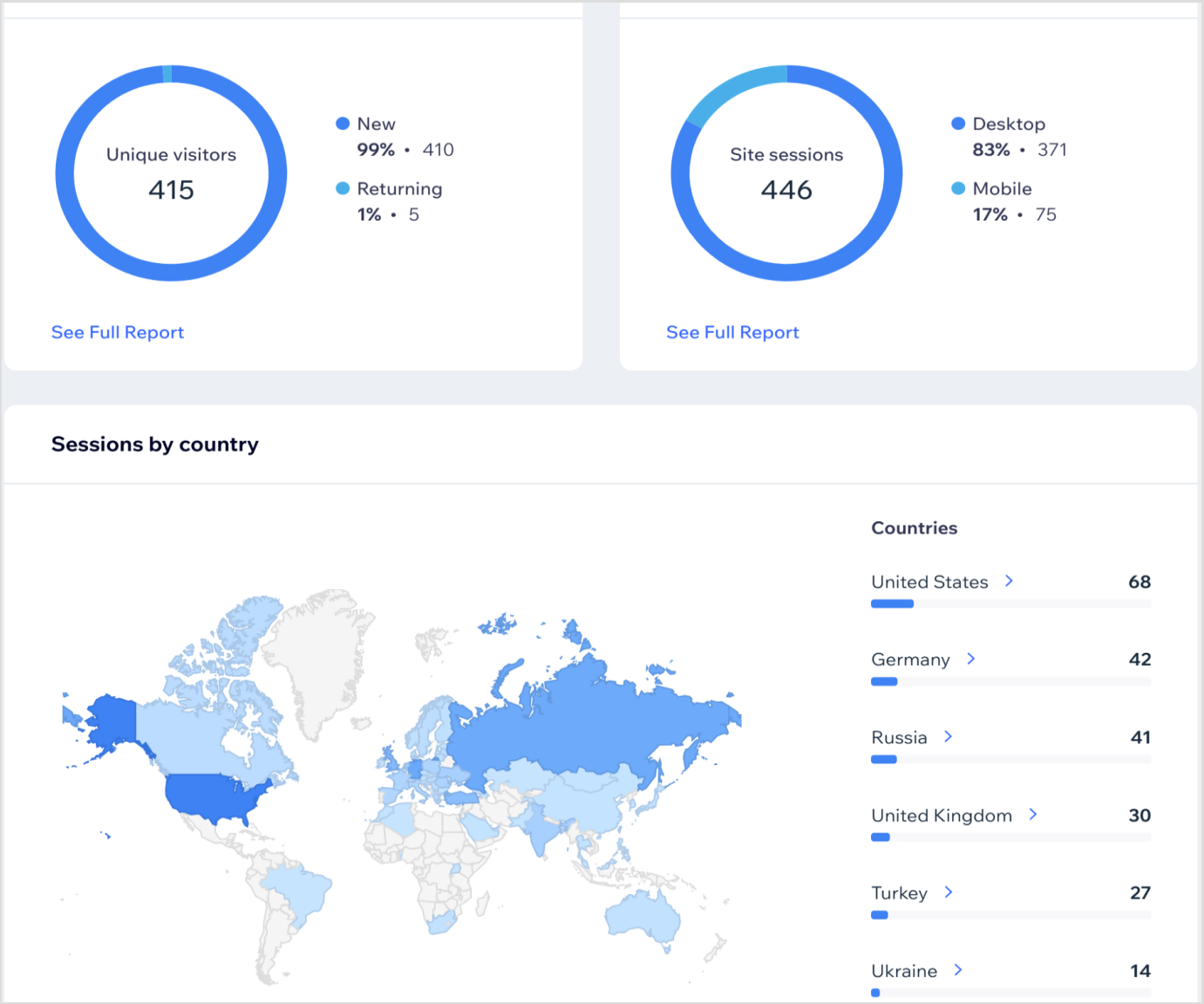
Play 21:09 Show summary

Belarusian Investigative Center

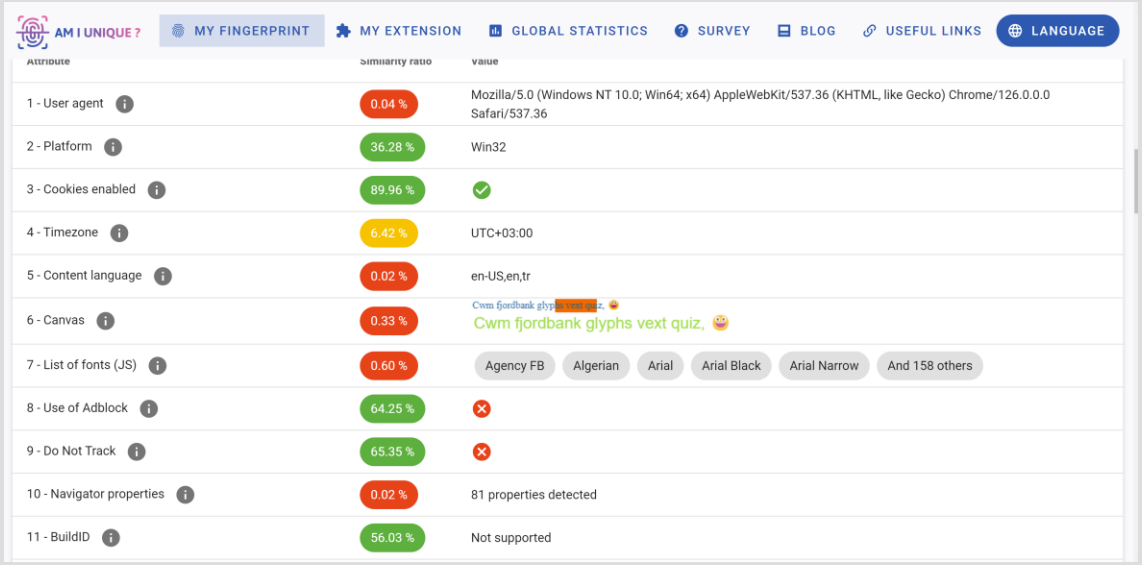
Analytics Investigations Chaly: Economics News with Chaly News Donate BY RU EN

Belarusian Investigative Center

PROTECTING YOUR PRIVACY WHEN INVESTIGATING



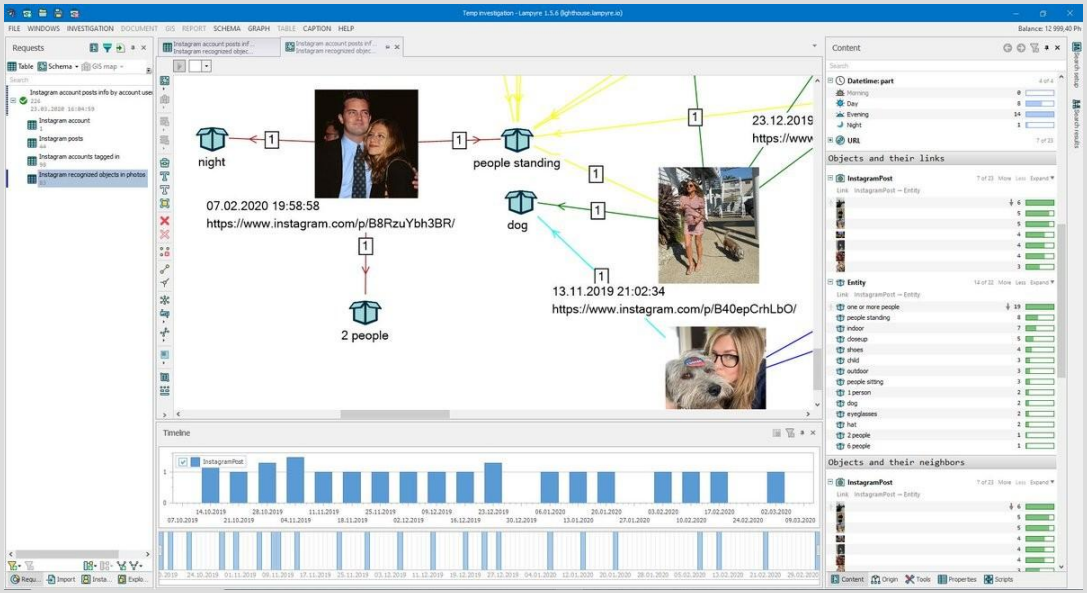
PROTECTING YOUR PRIVACY WHEN INVESTIGATING





PROTECTING YOUR PRIVACY WHEN INVESTIGATING

lampyre



Matthias Wilson • 3rd+
Intelligence & Investigations Professional / Intelligence Trainer /...
1yr •

+ Follow ···

Just a friendly reminder: the company behind the #OSINT tool Lampyre is actually Norsi Trans. And they're on the U.S. Department of the Treasury OFAC sanctions list.

Be careful what you OSINT with
keyfindings.blog

OPERATION SECURITY

VPN (Virtual Private Network)

Encrypts your connection, hides your IP/location, and ensures anonymity.

VM (Virtual Machines)

Separates your investigation from your main system, protects against threats, and supports secure OS/configuration use.

Extension: User Agent Changer

Spoofs browser/device info to avoid detection. Tools: User-Agent Switcher and Manager.

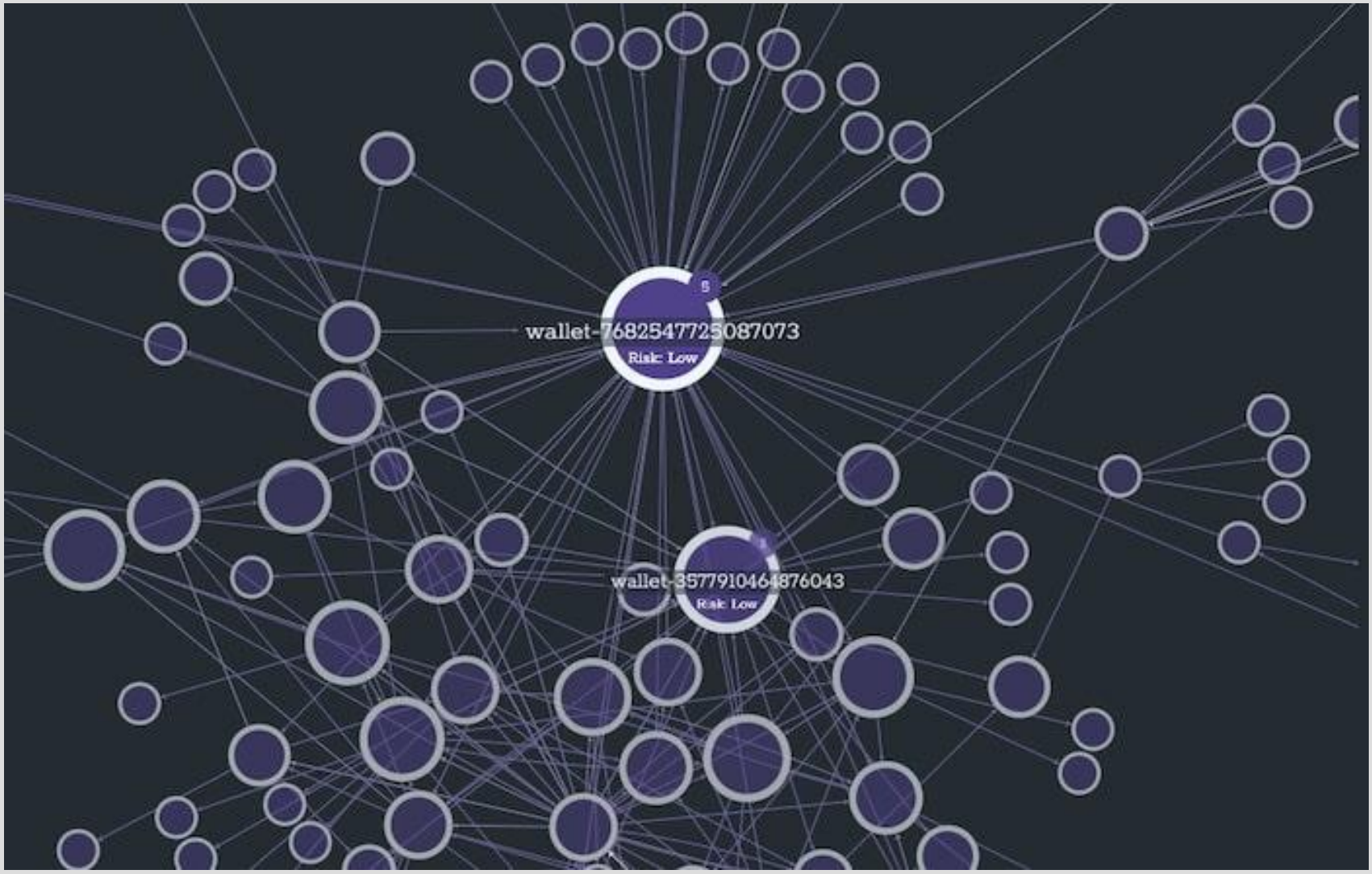
Check Only Through Verified Sources

Always verify the origin of tools, extensions, and data sources. Using unverified sources can lead to exposure, malware infection, or misinformation.

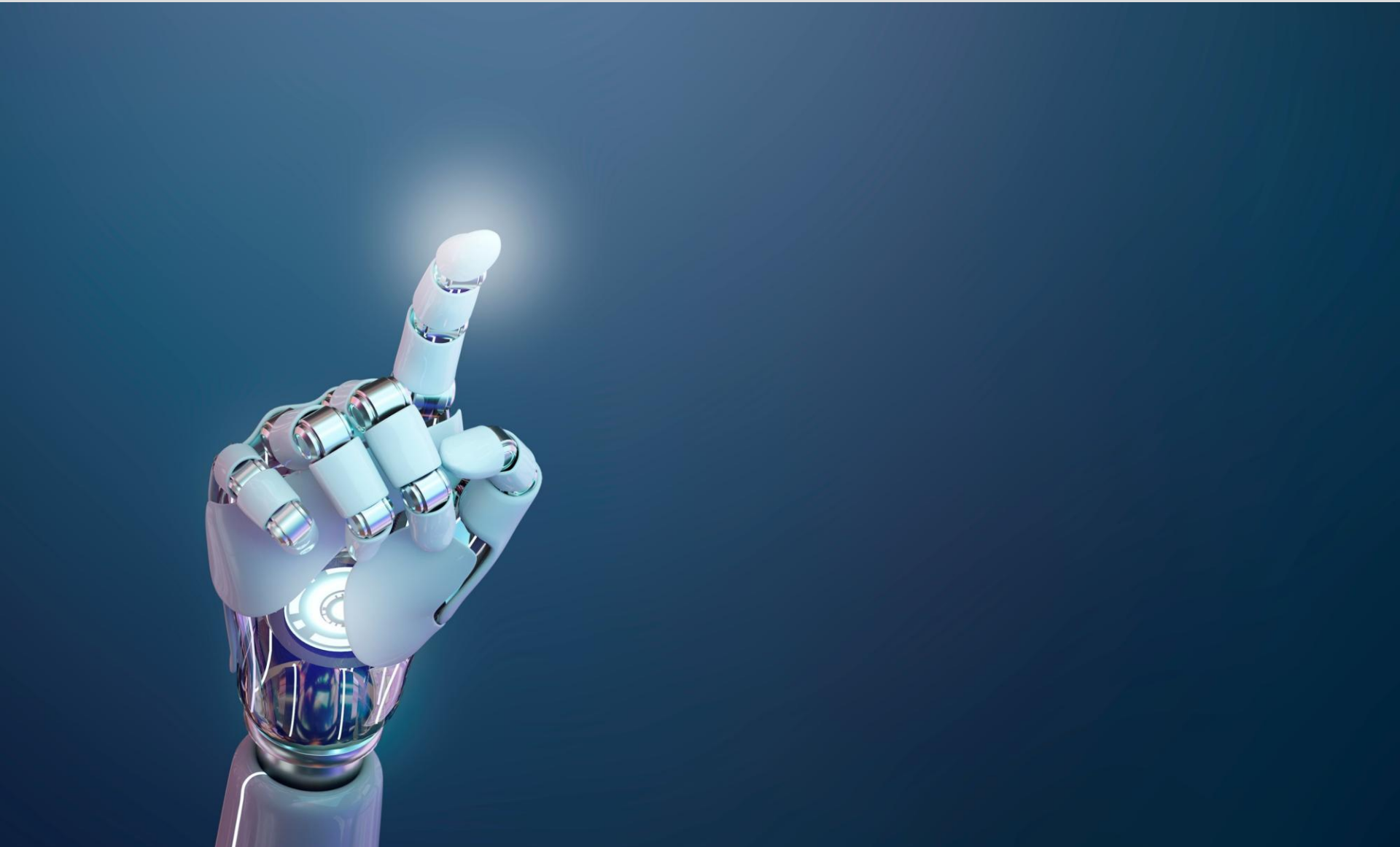
COMPETITOR ANALYSIS



BLOCKCHAIN ANALYSIS



Large Language Model (LLM) & OSINT



Before hiring OSINT expert Bilal Sen, I'd like to verify whether he has a strong track record in cyber capabilities. Please assist me in researching his background.

I was unable to find verifiable evidence of someone named *Bilal Sen* who matches the description "OSINT expert" with a strong, documented track record in cyber/intelligence work. Here's what I found (and what I couldn't), plus suggestions for how you might dig deeper to verify for yourself.

What I *could* find

- There is a GitHub account under the name **bilalseen** (or "Bilal Şen"). GitHub
  - It identifies itself as a *Frontend Developer / Computer Engineering Graduate*. GitHub
  - The public repos are mostly front-end / UI work (React Native, etc.) and general app / JS projects. GitHub
  - I didn't see evidence in those repos of OSINT, threat intelligence, or incident response tools or research.
- There's a Linktree and "Read CV" link associated with Bilal Sen via Instagram. Linktree
  - But the Instagram/Linktree page doesn't clearly show a verified cybersecurity portfolio or specific OSINT-projects. Linktree

---

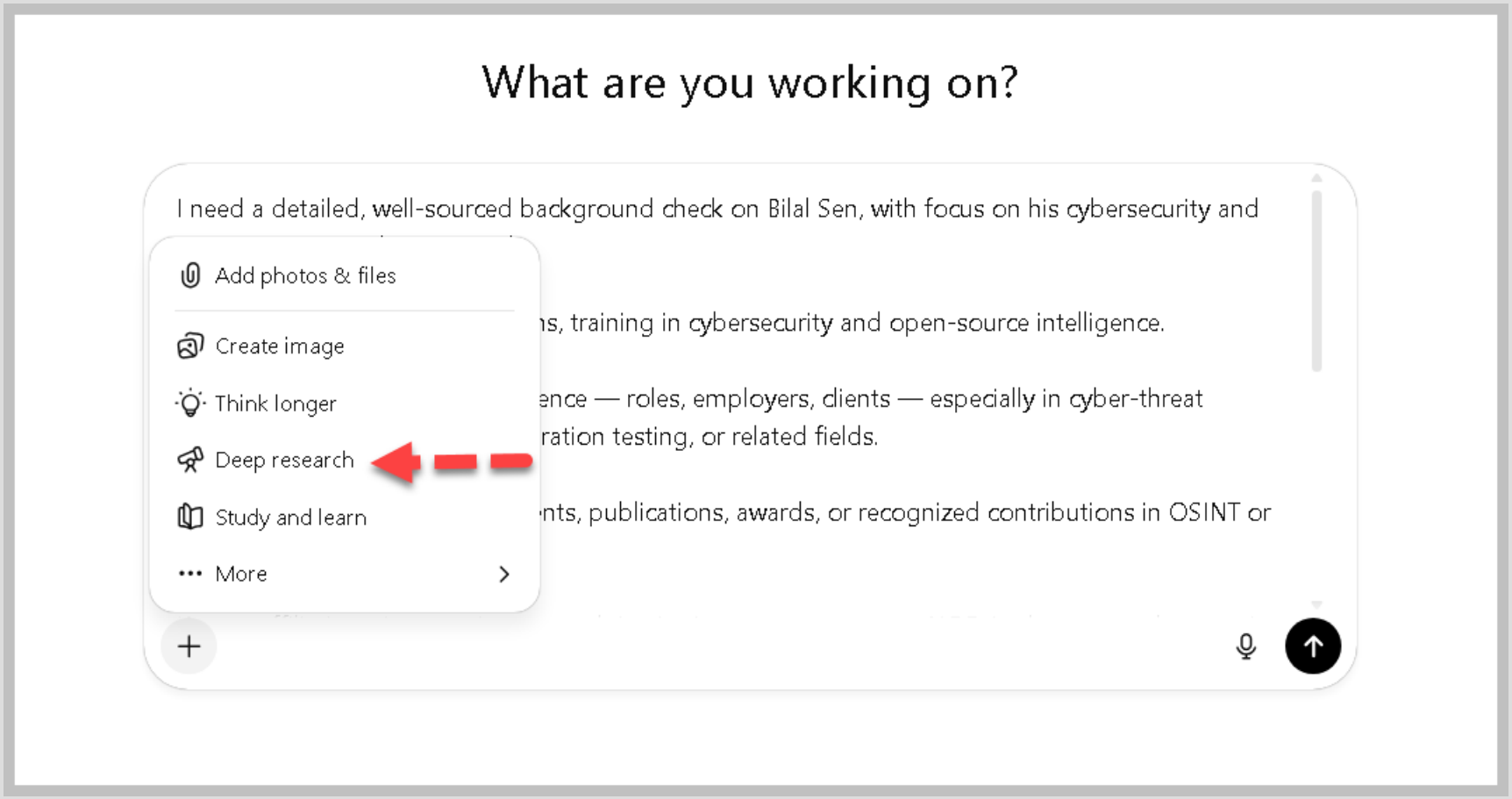
What I *couldn't* (but tried to) find

- Any credible publications, reports, or whitepapers authored by *Bilal Sen* in OSINT / threat intelligence / cyber investigations (peer reviewed or otherwise).

Here's a more formalized prompt you can use with ChatGPT (or other AI assistants) to ensure you receive detailed, well-sourced information — including only from verified or government sources (including Turkish government sources) — about Bilal Sen's cybersecurity / OSINT credentials:

Prompt:

> "I need a detailed, well-sourced background check on **Bilal Sen**, with focus on his cybersecurity and OSINT expertise. Please provide:
>
> 1. **"Official qualifications, certifications, training in cybersecurity and open-source intelligence."**
> 2. **"Documented professional experience — roles, employers, clients — especially in cyber-threat intelligence, investigations, penetration testing, or related fields."**
> 3. **"Any publicly verifiable achievements, publications, awards, or recognized contributions in OSINT or cybersecurity."**
> 4. **"Known affiliations (companies, research institutions, government or NGOs) relevant to cybersecurity."**
> 5. **"Any controversies, security incidents, or credible negative reports, if available."**
>
> **Important requirements:**
> • Use only credible, verifiable sources: official government websites, court or regulatory filings, well-established institutions or universities, recognized industry publications.
> • For Turkish sources, include documents or statements from Turkish government agencies, Turkish courts, regulatory bodies, or other official Turkish institutions.
> • For each claim, provide the source (URL) and date.
> • Clearly distinguish between confirmed facts and unverified or speculative claims.
>
> If you cannot find substantial publicly verified information on Bilal Sen's cybersecurity/OSINT track record, state that explicitly."


What are you working on?
I need a detailed, well-sourced background check on Bilal Sen, with focus on his cybersecurity and
Add photos & files
Create image
Think longer
Deep research
Study and learn
More
ns, training in cybersecurity and open-source intelligence.
ence — roles, employers, clients — especially in cyber-threat
ration testing, or related fields.
nts, publications, awards, or recognized contributions in OSINT or

LETS DO PRACTICAL

Your job should you choose to accept it



QUESTIONS & DISCUSSION

Bilal Şen

info@coninsec.com

DIGITAL EVIDENCE AND AI IN CRIMINAL JUSTICE



Using electronic evidence and AI in criminal investigations and presenting them at court

Senior Public Prosecutor Linda Bertram

ERA – ACADEMY OF EUROPEAN LAW | BUDAPEST, 15–16 OCTOBER 2026
#DIGITALISATION AND #ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

Co-funded by the European Union

SETTING THE SCENE

Introduction to AI in Criminal Proceedings

Definition

Artificial intelligence refers to computer systems capable of performing tasks that ordinarily require human intelligence.

RELEVANCE IN CRIMINAL JUSTICE

Enhanced data analysis
Greatly enhances the capacity to analyse large and complex datasets.

Forensic & prognostic support
Assists in forensic investigations, judicial prognostic assessments in criminal law and predictive policing.

Legal assistance
Supports legal work - e.g. analysis & summarization of case law.

New legal questions
Raises questions about evidence admissibility and defendants' rights.

AI IN CRIMINAL INVESTIGATIONS AND PROCEEDINGS

Where AI Enters the Investigation

General preliminary investigations

- Threat analysis & prioritization (cybercrime, money laundering...)
- AI-generated criminal complaints (fraud prevention...)
- Situation & sentiment assessment (media analysis...)
- Data analysis & pattern recognition (serial-offence detection...)

Technical support in investigations

- Speech recognition, analysis & translation (encrypted chats...)
- Image & video analysis (facial recognition, deepfakes...)
- Social-media monitoring & OSINT analysis (web crawlers, bots...)
- Generation of images & voice imitation (undercover operations...)
- Integration of relevant data (HessenData...)
- Use of third-party AI results (e.g. Klette case...)

AI IN CRIMINAL INVESTIGATIONS AND PROCEEDINGS

Analysing Data & Assessing Risk

Analysis of large data volumes

- Detection & categorization of files (IT forensics...)
- Pre-evaluation of images and videos (child-abuse imagery, juvenile pornography...)
- Communication & network data analysis (chats, emails...)
- Financial data & transaction analysis (account data, blockchain...)

Judicial prognostic assessments

(as distinct from predictive policing)

- Risk of violence by individuals & overall threat assessment (police...)
- Criminal liability of statements & preliminary evaluation (hate speech...)
- Risk of flight & reoffending (grounds for detention...)
- Risk of recidivism (probation, preventive detention...)

AI IN CRIMINAL INVESTIGATIONS AND PROCEEDINGS

AI as Legal Assistance

Speech recognition & translation

Legal assistance and complaint chatbots.

Analysis & summarization of case law

Research support such as Beck-chat.

Document analysis & information integration

Form-filling and “robo-judge” drafting support.

Deadline tracking & statistics

Automated reminders and case statistics.

CASE STUDY

Predictive Policing in Germany



Implementation

Deployed across various German federal states.



Challenges

Data-protection compliance and concerns about algorithmic bias.

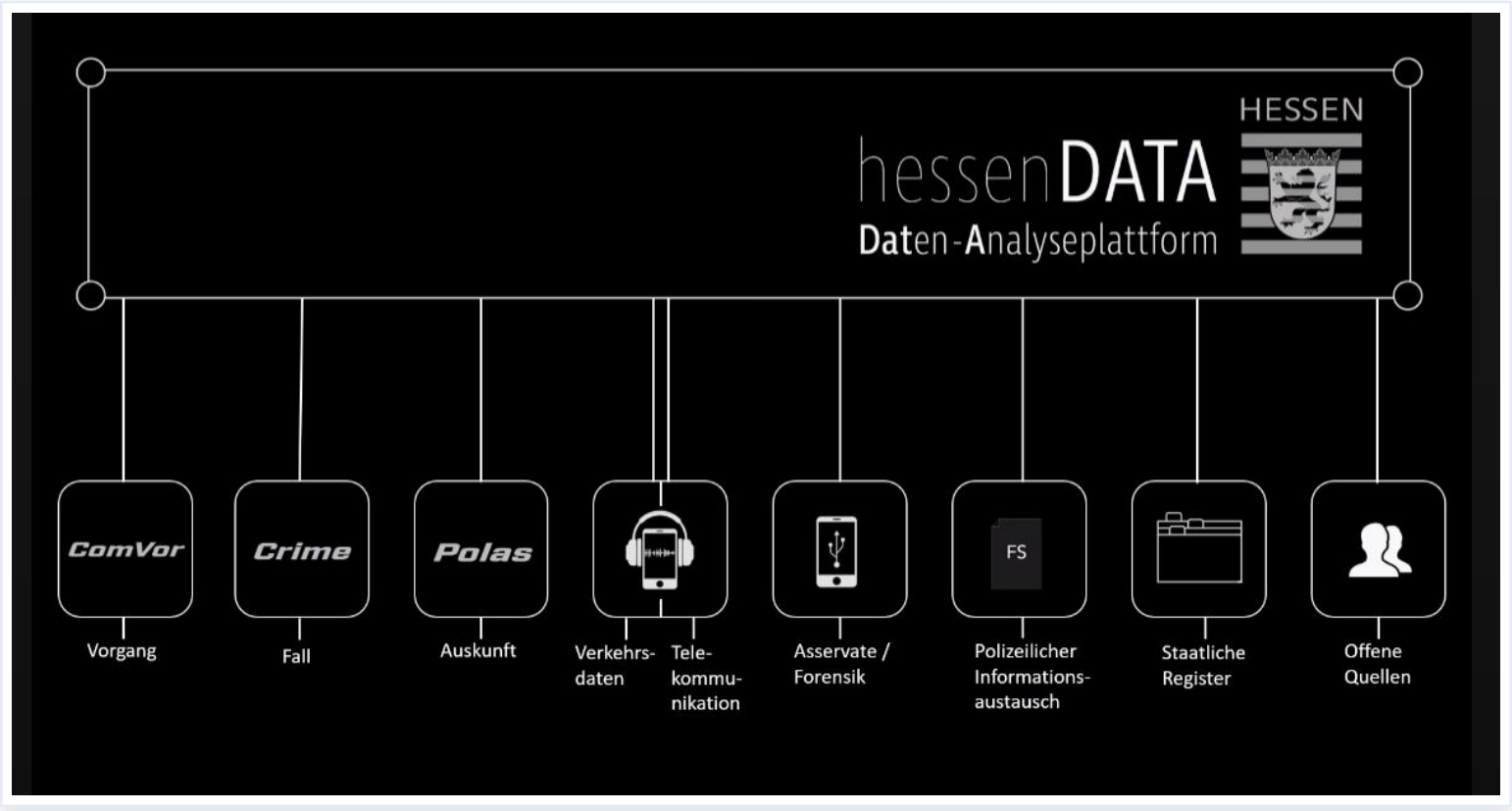


Open debate

Effectiveness and legality remain actively contested.

CASE STUDY · HESSENDATA (PALANTIR) - 1 / 7

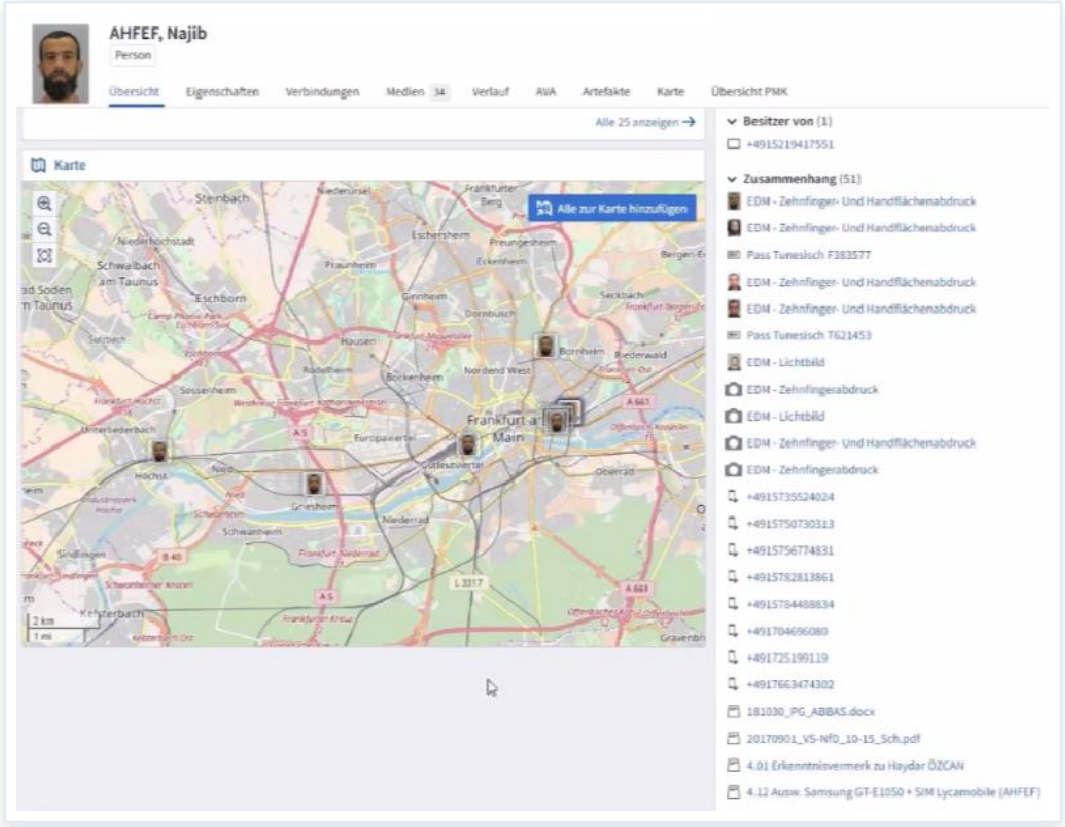
Cross-Database Analysis in Practice



Central analysis dashboard - the HessenDATA platform (built on Palantir).

CASE STUDY · HESSENDATA (PALANTIR) - 2 / 7

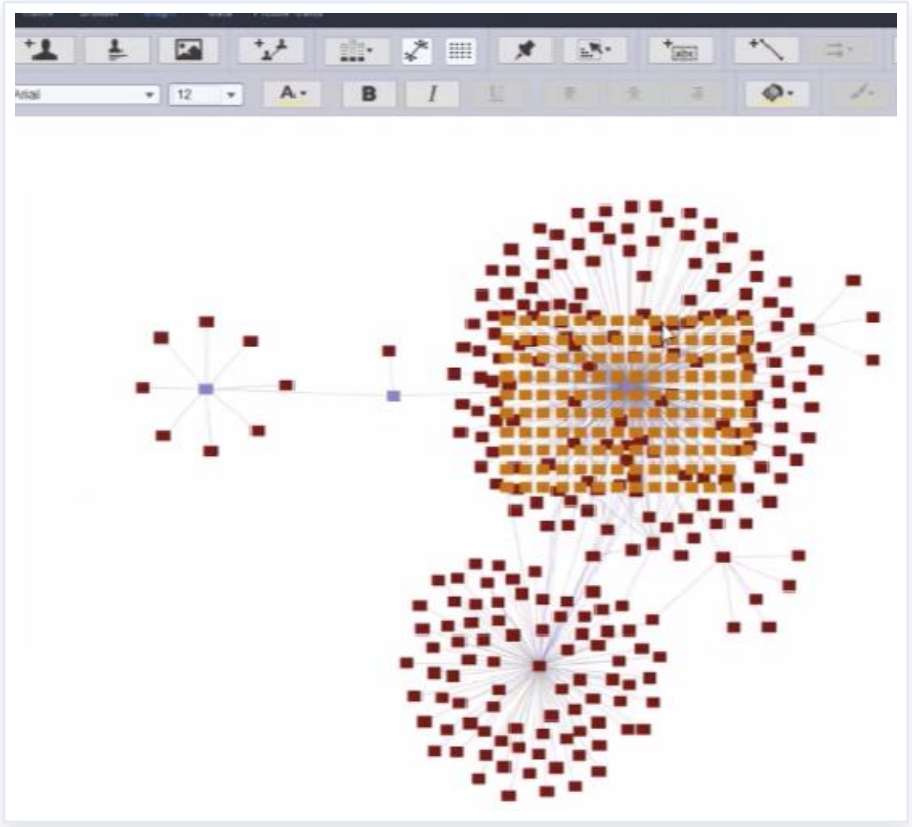
Cross-Database Analysis in Practice



Geospatial view: case locations linked on an interactive map.

CASE STUDY · HESSENDATA (PALANTIR) - 3 / 7

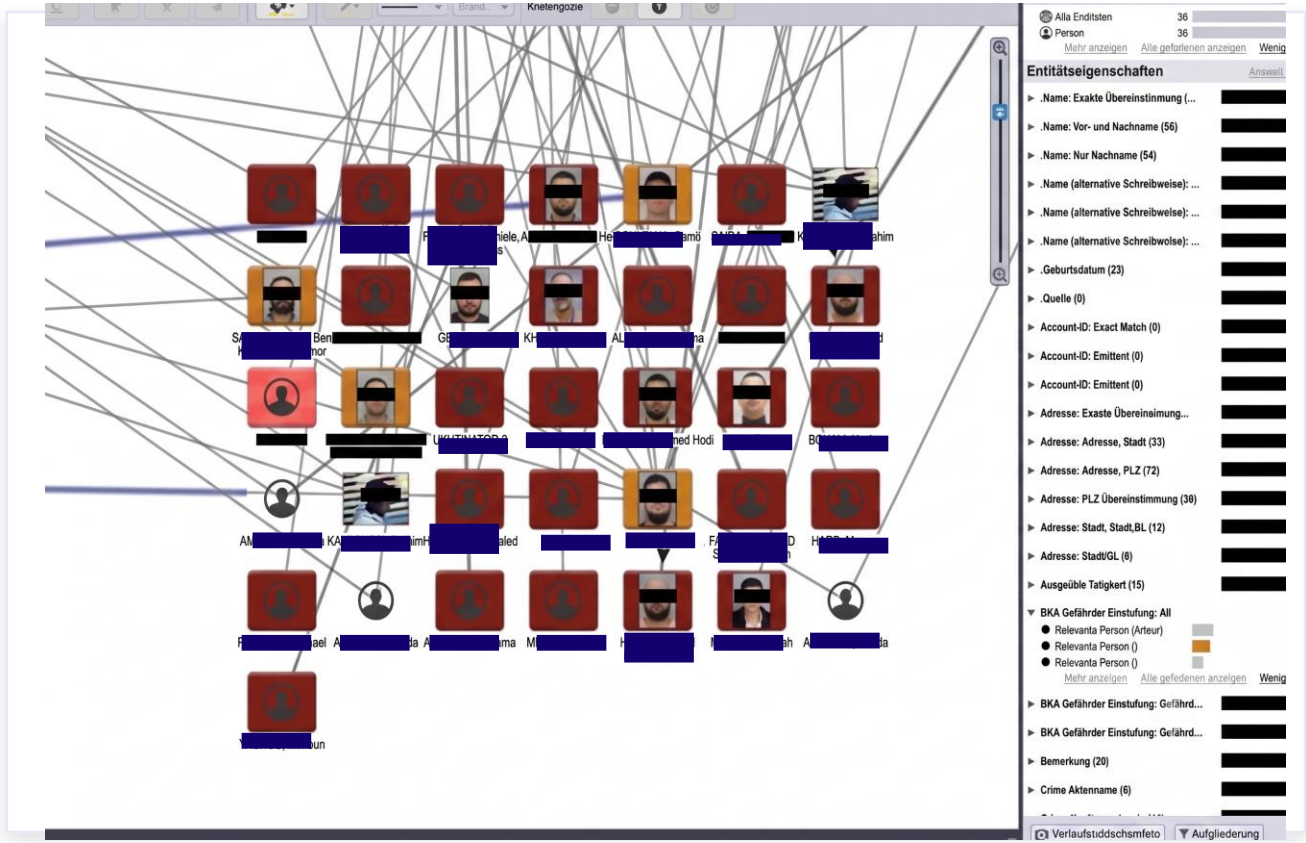
Cross-Database Analysis in Practice



Link analysis: entity-relationship network across data sources.

CASE STUDY · HESSENDATA (PALANTIR) - 4 / 7

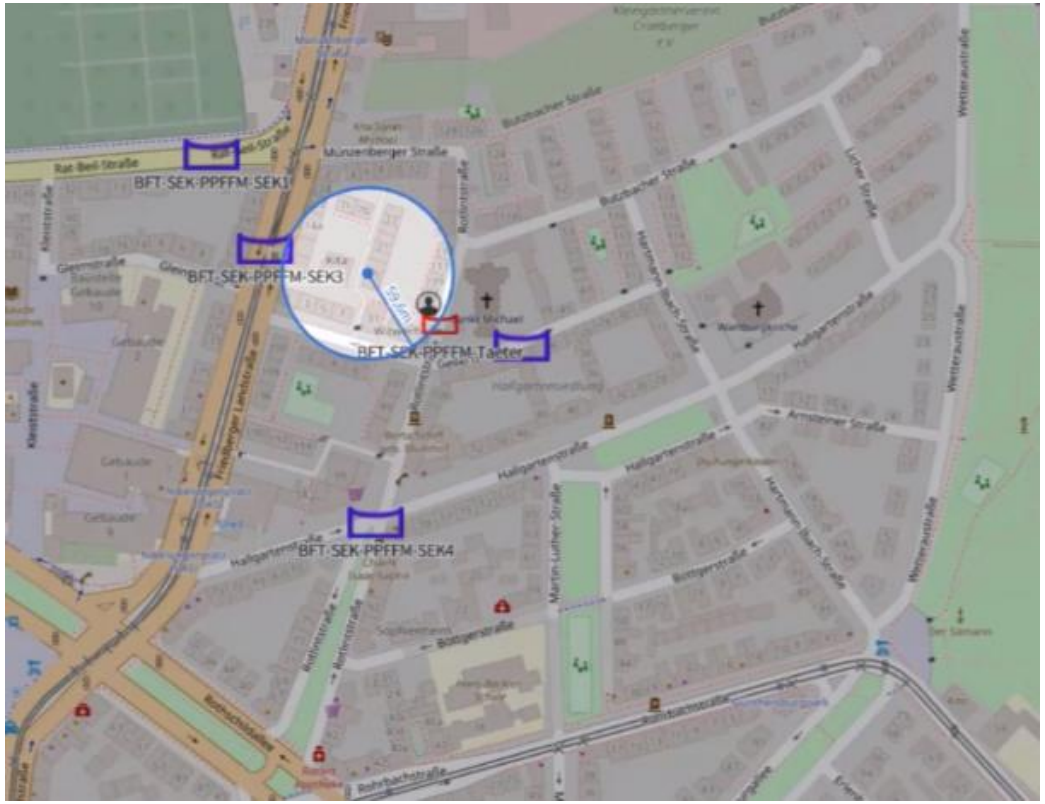
Cross-Database Analysis in Practice



Combined media grid and relationship analysis.

CASE STUDY · HESSENDATA (PALANTIR) - 5 / 7

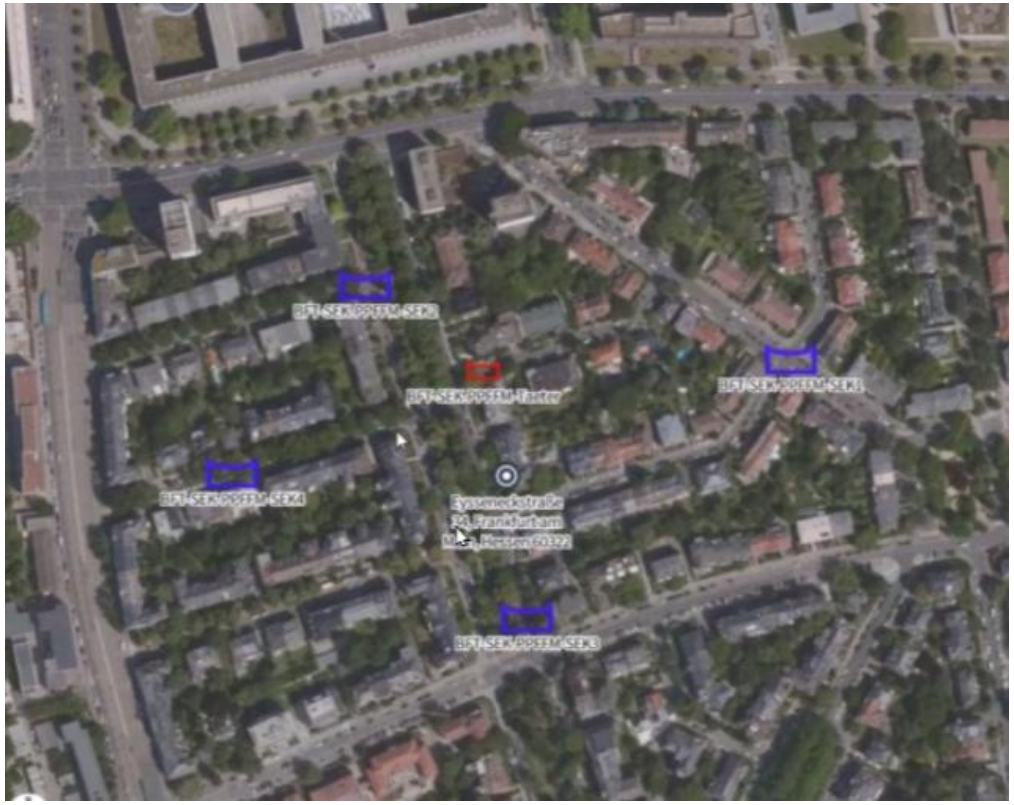
Cross-Database Analysis in Practice



Location radius and geofencing around points of interest.

CASE STUDY · HESSENDATA (PALANTIR) - 6 / 7

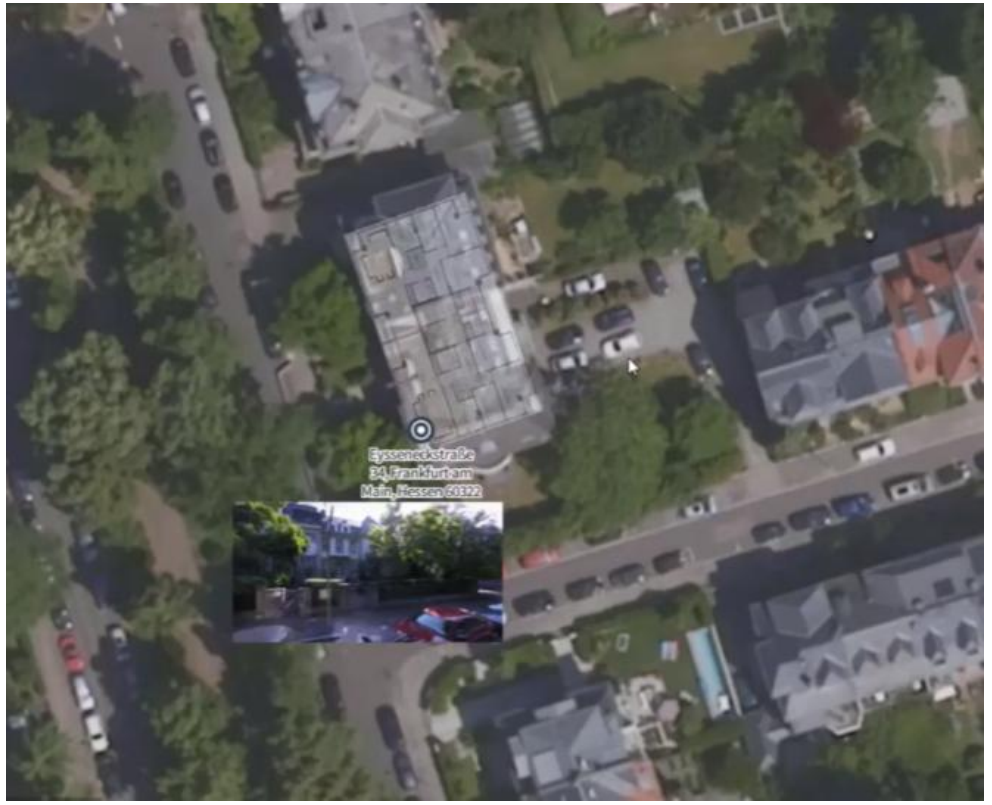
Cross-Database Analysis in Practice



Connected locations plotted across the city.

CASE STUDY · HESSENDATA (PALANTIR) - 7 / 7

Cross-Database Analysis in Practice



Aerial / satellite view of a location of interest.

CASE STUDY - WIESBADEN RECKLESS-DRIVING CASE

VR and AI Used in a Murder Trial

SPIEGEL Panorama

Prozess in Wiesbaden

Tödlicher Unfall – Raser zu lebenslanger Haft verurteilt

Er raste mit Tempo 130 durch die Innenstadt: Ein 25-Jähriger ist in Hessen des Mordes schuldig gesprochen worden. Vor Gericht hatte der Mann Reue gezeigt.

29.11.2023, 20.22 Uhr



Scene of the fatal collision, Wiesbaden

WIESBADEN RECKLESS-DRIVING CASE

VR and AI Used in a Murder Trial

The facts of the case

- October 2022: a 24-year-old drove at 120 km/h in a 50 km/h zone in Wiesbaden.
- He ignored a red light and fatally crashed into another vehicle.
- The victim was a 55-year-old woman.
- The driver had a prior history of traffic violations.
- Trial held in 2023 at Wiesbaden Regional Court.
- Charged with murder under **§ 211 StGB**.
- The court found he acted with conditional intent (bedingter Vorsatz).

120 / 50

km/h driven in a 50 km/h zone

§ 211

Murder - German Criminal Code

Life

Outcome: life imprisonment

WIESBADEN RECKLESS-DRIVING CASE

How VR and AI Shaped the Verdict

AI-assisted VR reconstruction

The court rebuilt the crime scene in 3D, enabling an immersive view of:

- Driving path and speed
- Visibility and timing
- The possibility to prevent the crash

Assessing intent
AI-assisted VR helped the court weigh intent and foreseeability.

A German first
Pioneering use of VR in German criminal justice.

Evidentiary clarity
Enhanced spatial understanding and clarity of the evidence.

Legal classification
Reinforced classifying extreme speeding as murder.

Precedent
Sentencing set a strong precedent for reckless-driving cases.

WIESBADEN CASE - FROM THE WRITTEN JUDGMENT

“Getting into the Car”: VR in the Verdict

> In the second step, according to witness “police officer 6 (PHK 6)”, it was necessary to select the correct technology to capture the images so that a realistic rendering of the perspectives could be achieved. A problem was that ordinary cameras have a **static viewing angle**, which cannot be changed afterward and thus only allows a limited representation of the actual perspective. It was crucial to create the possibility of virtually "getting into the car" and seeing the actual positions. The solution was the use of **"virtual reality" (VR)**, which here essentially meant recording with **360° cameras**, so that one could subsequently select the respective viewing angle oneself. (...) To obtain an even more realistic impression of the visibility conditions, the court could follow in real time on a screen what witness PHK 6 saw in the VR headset he was wearing. First, the view from the perspective of the Mercedes driver was shown - initially at **70 km/h** (original speed), and then at **140 km/h** (double playback speed), viewed multiple times. Witness PHK 6 moved his gaze on the court's instructions and at the request of other parties, thereby steering the perspective displayed on the screen. This confirmed the impression already gained from the VLC version, while conveying a more realistic perception.
>
> *- Excerpt from the court's written judgment*

CASE STUDY · AI IN THE COURTROOM

“Im Namen des Volkes” - The Written Judgment

Landgericht Darmstadt

Geschäftsnummer

3 KLs 200 Js 2761/24
(2/24)

Zur Geschäftsstelle
gekommen am: 23. Jan. 2025

IM NAMEN DES VOLKES
URTEIL

In der Strafsache

g e g e n [redacted]
zuletzt ohne festen Wohnsitz,
z. Zt. JVA Weiterstadt,
ledig (verlobt), deutscher Staatsangehöriger

w e g e n sexuellen Missbrauchs von Kindern

Excerpt from the court's written judgment (“In the name of the people - Judgment”).

CASE STUDY · AI IN THE COURTROOM

Forensic & Investigative Documentation

Bundeskriminalamt

Bundeskriminalamt (Federal Criminal Police Office)

BETREFF Ermittlungen wegen schweren sexuellen Missbrauchs von Kindern
Hier: Authentifizierung von Bild- und Videodaten

BEZUG Untersuchungsanträge des PP Darmstadt vom 02.04.2024 und 26.04.2024, Az. ST/0044172/2024

Tabelle 8: Liste der relevanten Metadaten der eingereichten Bilddateien Nr. 4-7, sowie für ein Referenzbild (IMG_20240429_110034.jpg), welches mit dem eingereichten Mobiltelefon A aufgenommen wurde.

Beschreibung	IMG_20220618_215537_291.jpg	IMG_20220618_215537_404.jpg	IMG_20220618_215537_573.jpg	IMG_20220618_215537_751.jpg	IMG_20240429_110034.jpg
ImageWidth	6560				
ImageHeight	3028				
EncodingProcess	Baseline DCT, Huffman coding				
BitsPerSample	8				
ColorComponents	3				
YCbCrSubSampling	YCbCr4:2:0 (2 2)				
Model	Mi Note 10 Pro				
Orientation: Rotate	180	180	270 CW	90 CW	Horizontal
ModifyDate [MESZ]	2022:06:18 21:44:26	2022:06:18 21:49:27	2022:06:18 21:45:51	2022:06:18 21:40:00	2024:04:29 11:00:37
YCbCrPositioning	Centered				
ISO	2458	2642	2382	2385	148
ExposureProgram	Program AE				
Fnumber	2.0				
ExposureTime	1/11	1/10	1/10	1/13	1/60
Exif_0x9999	"mirror":true,"sensor_type":"front","Hdr":"off"				
SensingMethod	Not defined				
SubSecTime	266879	480441	272532	804955	833845

CASE STUDY · AUTHENTIC EVIDENCE CHALLENGED

“The Video Was AI-Generated” - A Defendant's Claim



The case

Criminal proceedings concerning the sexual abuse of a child.

THE DEFENDANT'S CLAIM

An incriminating video - found on his mobile phone and showing him engaging in sexual acts with his three-year-old biological daughter - had, he claimed, been **artificially generated using AI**. **He asserted that the video did not depict a real event.**

CHILD-ABUSE CASE - FROM THE WRITTEN JUDGMENT

Why the Court Rejected the “Deepfake” Claim

> The fact that video file no. 1 was **not artificially generated using AI** follows, in the court's view, from **expert witness K's convincing statements**, according to which the **metadata of video file no. 1 rules out artificial generation**. Furthermore, the recording position of the video - and the fact that it was recorded only **47 minutes** before video files no. 2 and no. 3, likewise found on the defendant's mobile phone - indicate that this video must also have been recorded by the defendant.
>
> *- Excerpt from the court's written judgment*

CHILD-ABUSE CASE - THE SENTENCE

The Outcome

7 years

Total term of imprisonment

Convictions

The defendant was sentenced to a total term of imprisonment of seven years for aggravated sexual abuse of children with child-pornography intent in two cases - each in conjunction with sexual abuse of wards and with the production of child-pornography content - and, in one further case each, for third-party possession of child-pornography content and possession of child-pornography content.

CHILD-ABUSE CASE - THE EXPERT'S REASONING

Why the Video Could Not Have Been AI-Generated

> When asked whether it would theoretically be possible to create the videos using AI, the expert explained that, in theory, it is possible to generate a video synthetically - but this would require **suitable training material: images of a person with a similar appearance**. Here, a particularly notable feature is the penis shown in the videos, due to implants located beneath the glans; this **distinctive feature makes synthetic generation even harder without corresponding original image material**. The real crux, however, is that the AI-generated video would have needed to be compressed into the file format of the device - specifically the **Xiaomi Mi Note 10 Pro** - which would require an extremely high level of IT expertise; the expert stated that even he himself would not be capable of doing this. Moreover, an AI-generated video would only produce **random noise, not the systematic noise** present in the examined files. The expert therefore concluded that the videos **could not have been generated using AI**.
>
> *- Expert witness, as recorded in the judgment*

LESSONS LEARNED

The “Liar's Dividend”

The liar's dividend

Casting doubt on authentic evidence is as serious a courtroom threat as fabrication itself.

Authentic, dismissed as fake

Defendants increasingly try to dismiss authentic recordings as possible deepfakes.

Demand a factual foundation

Courts should require a factual basis before entertaining such challenges - yet in this case questioning was allowed though the defence offered no support for its AI-manipulation theory.

Detection is contested

Expert evidence is the pivot point, but deepfake detection is genuinely unreliable - with documented performance collapse on unseen, real-world fakes.

WHEN GENUINE EVIDENCE IS CALLED A "DEEPFAKE"

United States v. Reffitt

D.D.C., No. 21-cr-00032 - the first January 6 trial and an early appearance of the deepfake defense

WHAT HAPPENED AT TRIAL

1. A genuine 360° helmet-camera video of the defendant at the Capitol was admitted on direct examination - with no defence objection.
2. On cross-examination, defence counsel asked the FBI analyst about deepfakes and suggested the footage could have been AI-manipulated.
3. The prosecution objected; the court asked for a good-faith basis. Counsel offered none beyond an intention to ask whether exhibits were altered - and was allowed to continue.
4. The analyst confirmed no reason to think the video was fake. Defence argued "deepfake" at closing anyway. The jury convicted on all five counts.

THE CAUTIONARY POINT

0

items of evidence ever offered to support the AI-manipulation theory

5 / 5

counts of conviction

Real evidence was put in doubt at no cost - the essence of the "liar's dividend."

Source: A. Mitchell, "Deepfaked Evidence," Berkeley Technology Law Journal (2025); trial transcript, U.S. v. Reffitt, No. 21-cr-00032 (D.D.C.).

FROM AN EARLY DEEPFAKE-DEFENSE CASE TO COURTROOM PRACTICE

Five Takeaways for Bench and Prosecution

1 Low bar, big gap

Sufficiency-level authentication lets manipulation be raised without any showing that it occurred.

2 Good faith needs teeth

Requiring a basis helps only if a bare intention to ask is not treated as enough to proceed.

3 Ready the examiner

Forensic witnesses should affirm that media shows no indicia of synthesis - not merely describe it.

4 A graduated burden

Proposed U.S. FRE 901(c): an objection needs a plausible basis; then authenticity is proven to a higher bar.

5 AI literacy first

No rule works unless judges and counsel grasp what generative AI can and cannot do.

⚠ The bottom line

As fakes grow familiar, the guilty can discredit real evidence by merely invoking the possibility.

Sources: Berkeley Technology Law Journal (2025); R. Chesney & D. Citron, 107 Calif. L. Rev. 1753 (2019); U.S. FRE Advisory Committee (proposed Rule 901(c)).

EUROPOL IOCTA 2026

The Rise of Synthetic CSAM

Für das Bild *ph_02054_.png* wurden folgende Prompts eingesetzt:

POSITIVE PROMPT	pre teen child girl walking up a beach carrying a surfboard under her arm, long wavy brunette hair blows in the wind, wearing a wetsuit unzipped and showing a bit of cleavage, long sleeves, morning sunlight reflects off the water, heavy surf
NEGATIVE PROMPT	((censored)), ((Asian)), ((bad anatomy)), bad hands, three hands, three legs, bad arms, missing legs, missing arms, poorly drawn face, bad face, fused face, cloned face, worst face, three crus, extra crus, fused crus, worst feet, three feet, fused feet, fused thigh, three thigh, fused thigh, extra thigh, worst thigh, missing fingers, extra fingers, ugly fingers, long fingers, horn, extra eyes, huge eyes, amputation, disconnected limbs, cartoon, cg, 3d, unreal, animate bad anatomy, bad hands, breasts, three hands, three legs, bad arms, missing legs, missing arms, poorly drawn face, bad face, fused face, cloned face, worst face, three crus, extra crus, fused crus, worst feet, three feet, fused feet, fused thigh, three thighs, fused thigh, extra thigh, worst thigh, missing fingers, extra fingers, ugly fingers, long fingers, horn, extra

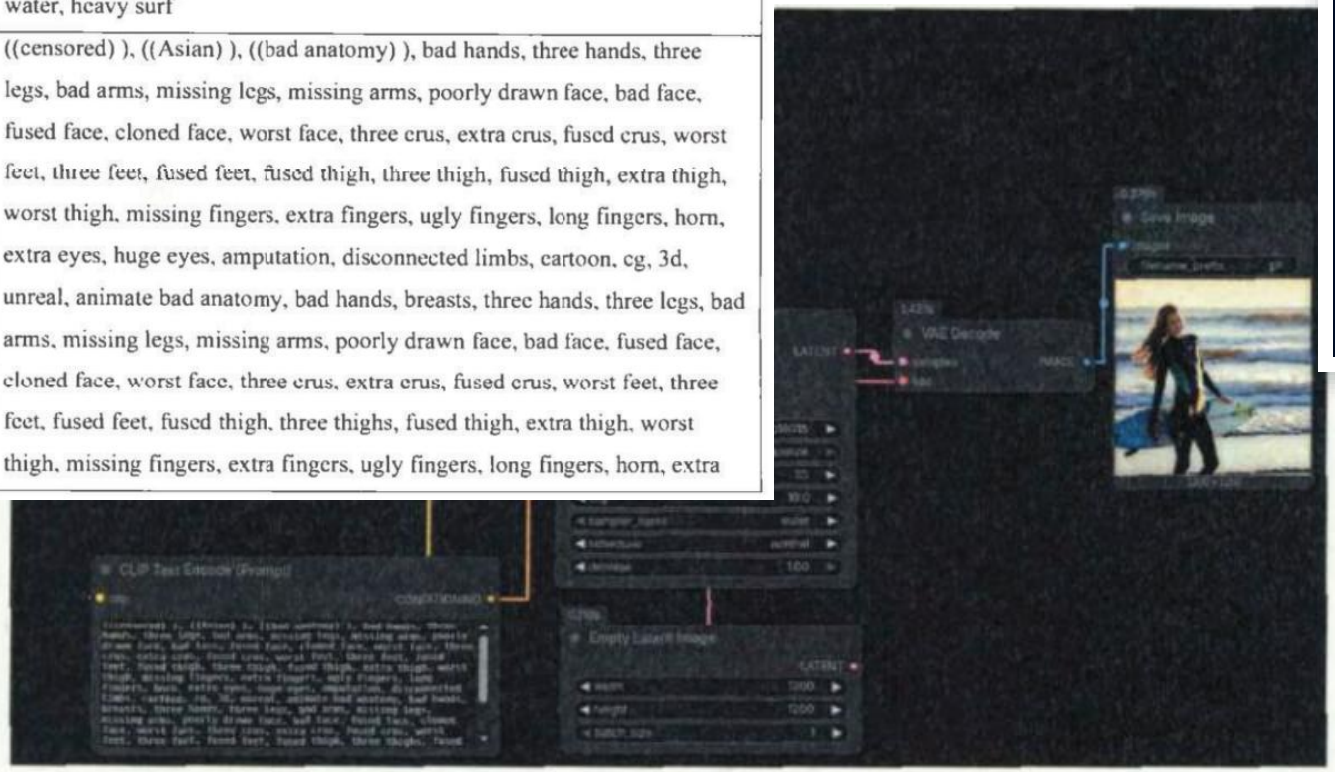


Abbildung 3 – Workflow aus Abb. 2 nach Verarbeitung durch ComfyUI



EUROPOL IOCTA 2026

The Rise of Synthetic CSAM

Production at scale

The rapid evolution and accessibility of AI tools have drastically scaled up the production of Child Sexual Abuse Material (CSAM) and sophisticated offender grooming techniques.

Organised exchange

Investigations reveal international platforms where offenders exchange technical skills, ready-made prompts, and OPSEC tips to refine synthetic production.

Unprecedented challenge

This multiplied volume of highly realistic AI-generated material poses severe, unprecedented challenges for imagery analysis and the identification of offenders.

EUROPOL IOCTA 2026

AI Generation & Evasion Tactics

Fully vs. partially synthetic

Image-to-image models alter existing photos to create partially synthetic CSAM. In parallel, advancing text-to-image and text-to-video models generate entirely new, fully synthetic material from offender prompts alone.

Offline models

To bypass online content moderation and safety guardrails, offenders use offline AI models - deliberately trained on authentic abuse material for accurate, unmoderated generation.

Bots in E2EE groups

Automated generation bots operate within encrypted communications. Bots capable of editing images to produce synthetic CSAM on demand have been detected inside end-to-end-encrypted groups.

CASE STUDY

AI in Investigative Journalism



Tracking a fugitive

Used to help track fugitive terrorist Daniela Klette.

Facial recognition

Journalists applied facial-recognition tools to public images.

Public vs. private

Raised questions about AI's role in private versus public investigation.

DANIELA KLETTE CASE

How Facial Recognition Reopened the Hunt



- **Daniela Klette**: former RAF (Red Army Faction) member.
- Suspected of involvement in serious crimes from the 1980s and 1990s.
- Went underground in 1993 and lived undetected for **over 30 years**.
- One of Germany's most-wanted fugitives.
- In 2024, investigative journalists used the facial-recognition tool **PimEyes**.
- PimEyes compared public images to online sources using AI algorithms.
- A match was found between old RAF photos and a woman in Berlin.
- This led to a reactivation of law-enforcement efforts.

DANIELA KLETTE CASE - THE VERDICT

Sentenced in Verden, May 2026

13 years

Prison sentence (Verden court, 27 May 2026)

- Arrested in early 2024 in Berlin after the renewed investigation.
- Convicted of **aggravated armed robbery, attempted kidnapping, and possession of military weapons**.
- The ruling rested on a series of heists on supermarkets and cash-transport vehicles between 1999 and 2016, committed to finance her life underground after the RAF disbanded.
- The verdict focused strictly on these criminal acts - separate from any politically motivated terrorism charges from her earlier RAF years.
- Alleged accomplices Burkhard Garweg and Ernst-Volker Staub, both ex-RAF members, **remain at large**.

LEGAL PERSPECTIVES ON BIOMETRIC SCRAPING & DIGITAL IDENTIFICATION

AI Biometrics in Criminal Procedure

Legality of biometric scraping

GDPR Article 9 constraints and the impact of the EU AI Act on mass-scale facial harvesting.

Private vs. public surveillance

A shift of investigative tasks to private-sector databases - and the resulting challenges for public oversight.

Evidentiary value & standards

The weight of AI-generated matches in court, and the procedural fairness of algorithmic evidence.

LEGAL FRAMEWORK

The European Union's Rules

EU Artificial Intelligence Act

Regulation (EU) 2024/1689 classifies AI by risk - unacceptable, high, limited, minimal. High-risk systems (e.g. biometric ID) face strict requirements.

Charter of Fundamental Rights

Guarantees the rights to privacy, data protection, and a fair trial.

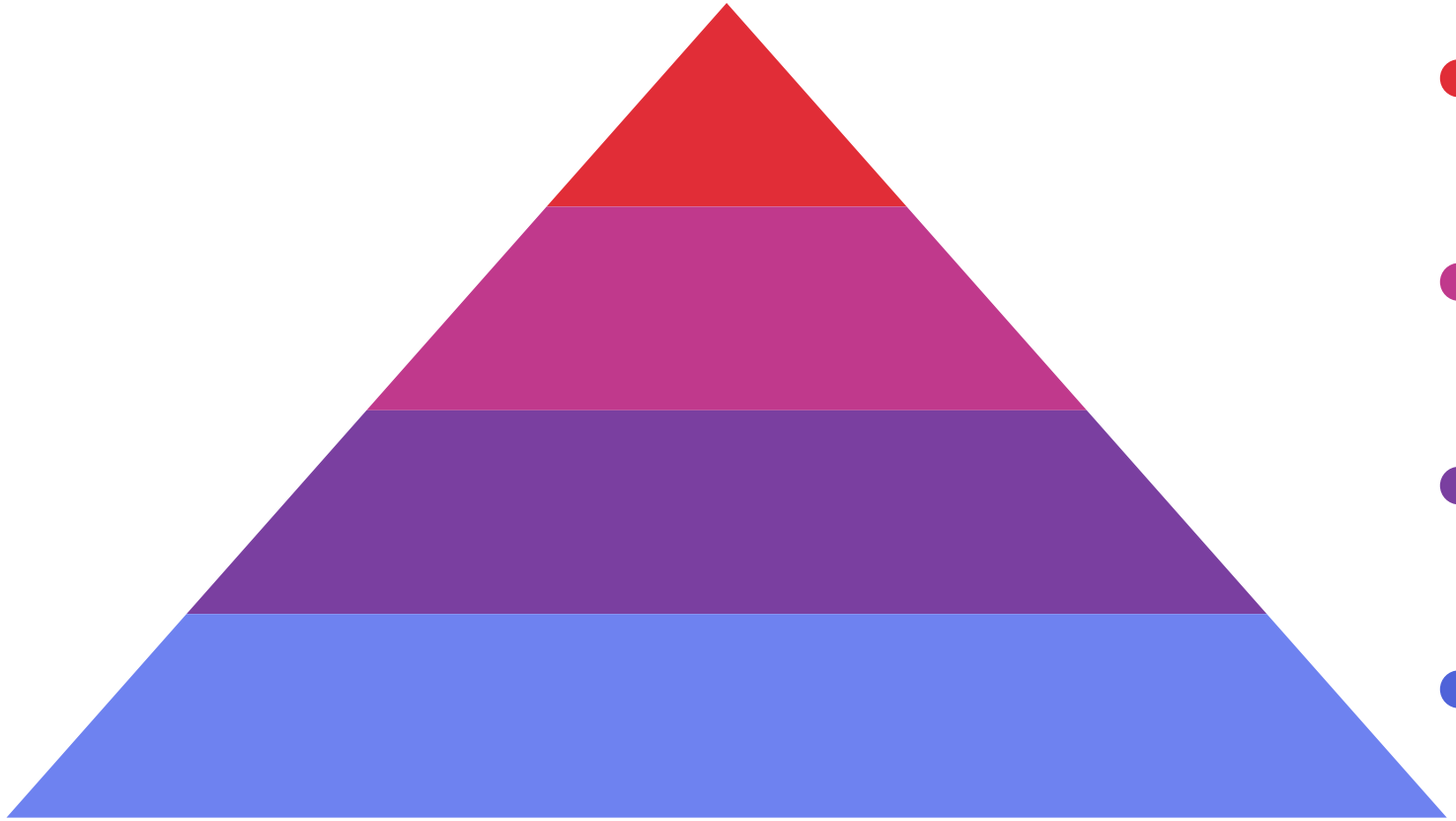
e-Evidence Regulation

Cross-border access to electronic evidence - directly affecting AI-generated data.

EU ARTIFICIAL INTELLIGENCE ACT

A Risk-Based Approach

The AI Act defines four levels of risk for AI systems:



Unacceptable risk

Prohibited AI practices

High risk

Strict requirements (e.g. biometric ID)

Limited risk

Specific transparency obligations

Minimal risk

Most AI - no specific obligations

PROHIBITED AI SYSTEMS · CHAPTER II, ART. 5

Real-Time Biometric ID: Banned - Except...

Real-time remote biometric identification (RBI) in publicly accessible spaces for law enforcement is **prohibited** - except in three situations:

Finding victims

Searching for missing persons, abduction victims, and people who have been human-trafficked or sexually exploited.

Preventing grave threats

Preventing a substantial and imminent threat to life, or a foreseeable terrorist attack.

Serious-crime suspects

Identifying suspects in serious crimes - e.g. murder, rape, armed robbery, drug and illegal-weapons trafficking, organised crime, environmental crime, etc.

PROHIBITED AI SYSTEMS · CHAPTER II, ART. 5

The Safeguards on Real-Time RBI

1

Strict necessity

Permitted only where not using the tool would cause considerable harm - and always weighing the rights and freedoms of affected persons.

2

Assessment & registration

Before deployment: a fundamental-rights impact assessment and registration in the EU database. In duly justified urgency, deployment may start before registration, provided it is registered later without undue delay.

3

Judicial authorisation

Prior authorisation from a judicial or independent administrative authority. In urgency it may begin first, but authorisation must be requested within 24 hours - and if refused, deployment must cease immediately, deleting all data, results and outputs.

EUROPEAN COMMISSION

Guidelines on Prohibited AI Practices



European Commission

Brussels, 4.2.2025 - C(2025) 884 final

Annex: Guidelines on prohibited AI practices established by the AI Act.

ANNEX

to the

Communication to the Commission

Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)

PROHIBITED AI SYSTEMS · ART. 5 - EXAMPLE 1

Festival: Untargeted Facial Recognition

> During a busy festival, police deploy live facial recognition to monitor the area and identify wanted individuals with outstanding arrest warrants for illegal drug trafficking and sexual offences. At the entrances, live video of passers-by is compared against a watchlist. **Concerning the offence types, RBI can be used for illegal drug trafficking. However, sexual offences are not on the list** - unless they relate to the sexual exploitation of children, child sexual abuse material, or rape. The police are **not allowed** to deploy real-time facial recognition in a broad, untargeted manner, in the hope of finding wanted criminals and taking them off the streets.
>
> *- European Commission, Guidelines on prohibited AI practices*



ASSESSMENT

Not permitted

Broad, untargeted use - and most of the cited offences fall outside Art. 5.

PROHIBITED AI SYSTEMS · ART. 5 - EXAMPLE 2

Festival: A Targeted Search

> The case is different if the police have received a **physical description with a photograph** of a wanted individual who is subject to a **European Arrest Warrant for drug trafficking**, and they have reason to believe he will be present at the festival. In those circumstances, deploying real-time facial recognition to identify a **targeted individual** may be covered by Article 5(1)(h)(iii) AI Act.
>
> *- European Commission, Guidelines on prohibited AI practices*



ASSESSMENT

May be permitted

A targeted search for one identified person, on a qualifying offence.

PROHIBITED AI SYSTEMS · ART. 5 - EXAMPLE 3

After a Terror Attack

> After a serious terror attack at a Christmas market with **12 deaths**, the police use real-time facial recognition to identify the offender and track where he is escaping. They also use the real-time facial recognition of the nearby train station and at the destination stations of trains leaving shortly after the attack. In the case of a **terror attack**, such use can be permitted under Article 5(1)(h)(iii) AI Act.
>
> *- European Commission, Guidelines on prohibited AI practices*



ASSESSMENT

Can be permitted

A foreseeable / actual terrorist attack is an express exception.

CONSIDERATIONS AND DISCUSSION

Concerns and Counterpoints

COMMON CONCERNS

- Bias and discrimination.
- Transparency and accountability - the difficulty of explaining AI decisions.
- Legal uncertainty - the lack of clear AI rules in criminal law.

COUNTERPOINTS

- **Human expert witnesses are themselves biased and inconsistent** - why should AI be regulated more than fallible human judgment, despite offering more transparency?
- **AI is not the decision-maker** - criminal procedure already has oversight (e.g. judicial review), so extra regulation is redundant and burdensome.
- **Regulatory burden hampers law enforcement** - while AI offers superior traceability.

CONSIDERATIONS AND DISCUSSION

A Call for Proportionality

THESIS

The EU AI Act overregulates AI tools in criminal justice - placing an undue burden on investigations without equivalent scrutiny of human actors.

Regulate by function

Regulate based on function and context - not on AI status alone.

Safeguard, don't stifle

Ensure safeguards without stifling innovation.

Hold everyone to account

Focus on accountability across both human and artificial contributors.

LEGAL FRAMEWORK

AI Act timeline – updated October 2026

1 Aug 2024	AI Act (Regulation (EU) 2024/1689) entered into force
2 Feb 2025	Prohibited practices (Art. 5) and AI literacy obligations apply
2 Aug 2025	Governance rules and obligations for general-purpose AI models apply
2 Aug 2026	General date of application, incl. transparency obligations for deepfakes (Art. 50)
2 Dec 2026	**NEW: bans on AI systems generating non-consensual intimate imagery and CSAM**
2 Dec 2027	**NEW DATE: high-risk systems under Annex III (incl. law enforcement, justice) – previously 2 Aug 2026**
2 Aug 2028	**NEW DATE: high-risk AI in regulated products (Annex I) – previously 2 Aug 2027**

Changes introduced by the Digital Omnibus on AI, Regulation (EU) 2026/1744 (OJ 24 July 2026, in force since 27 July 2026)

Source: Regulation (EU) 2024/1689; Regulation (EU) 2026/1744 – eur-lex.europa.eu

AI IN PRACTICE

Beck-Noxtua – a legal AI workspace

- **Launched on 26 November 2025** by the legal publisher C.H.Beck and the Berlin-based legal AI company Noxtua
- **Combines the beck-online database** with legal AI – answers are based on curated legal sources, not on the open internet
- **Functions:** legal research with verifiable citations, analysis of several documents in parallel, first drafts of documents, also in Microsoft Word
- **Transparency:** agentic workflows show each work step and the AI's reasoning
- **Target groups** incl. law firms, the public sector and the judiciary

60m+

documents in the beck-online database

26 Nov 2025

market launch

Source: Noxtua press release "Launch of Beck-Noxtua", 26 Nov 2025 – noxtua.com; beck-noxtua.de/produkt

AI IN PRACTICE

Beck-Noxtua – data security and our test

- **Hosting in Germany:** processing in data centres of IONOS and Open Telekom Cloud; according to the provider compliant with GDPR and § 203 StGB
- **Open-weights model ("Athena")** runs as an encapsulated copy on European infrastructure
- **Certifications stated by the provider:** BSI C5, ISO/IEC 27001 and ISO/IEC 42001
- **We are currently testing Beck-Noxtua in our office:** quality of research and citations, data protection, fit with prosecutorial workflows
- **Keep in mind:** AI assisting judicial authorities in researching and interpreting facts and law is high-risk under Annex III AI Act

Test

currently running in our office

Human

review of every result remains mandatory

Source: noxtua.com, 26 Nov 2025; beck-noxtua.de/produkt (provider information); Annex III no. 8 Regulation (EU) 2024/1689

DANKE

Linda Bertram
Oberstaatsanwältin/
Senior Public Prosecutor

Generalstaatsanwaltschaft Frankfurt am Main
- Zentralstelle zur Bekämpfung der Internetkriminalität- /
Prosecutor General's Office
– Cyber Crime Center –

International Legal Assistance

Konrad-Adenauer-Straße 15
60313 Frankfurt am Main

Mail: linda.bertram@gsta.justiz.hessen.de

HESSEN

ERA

Presenting evidence in court: e-files, videoconferences and remote trials

Balázs Rozsnyai

16 October 2026, Budapest

Co-funded by
the European Union

Overview

1

Remote trials

During and after the pandemic — the Hungarian experience, the numbers, immediacy, and the safeguards on screen

2

E-files

The image and audio recording as part of the case file — storage, protection, access

3

Videoconferencing practice

The legal framework and the practical rules of cross-border hearings

4

Assessing evidence & AI

Authenticity of recordings — when must expert evidence be ordered if manipulation is alleged?

1

Remote trials

During and after the pandemic

The Hungarian remote-hearing project

A nationwide system for electronic court administration

- *Goal:* **widespread, efficient electronic court administration**
  - The judiciary joined the project in 2018
- *Endpoints:* **courts, government offices, customer-service points, police, prisons, expert institutes**
- *Who can join:* **anyone (authorised), from anywhere**
  - Call / content: end-to-end encrypted

Frequency of use during the pandemic

216 **(20% of all courtrooms)**

courtrooms equipped

Non-stop

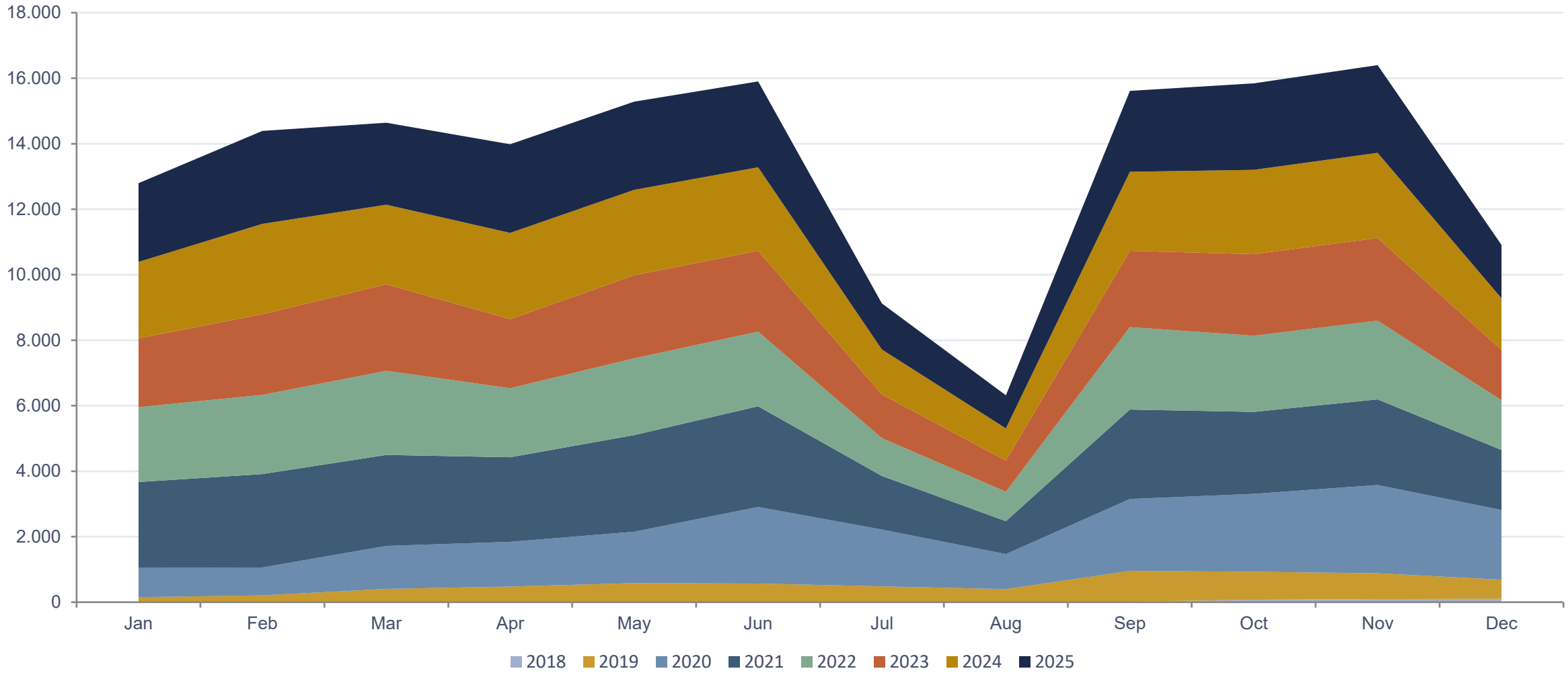
the judiciary kept operating during the pandemic

~ 3 x

rise in the number of remote hearings

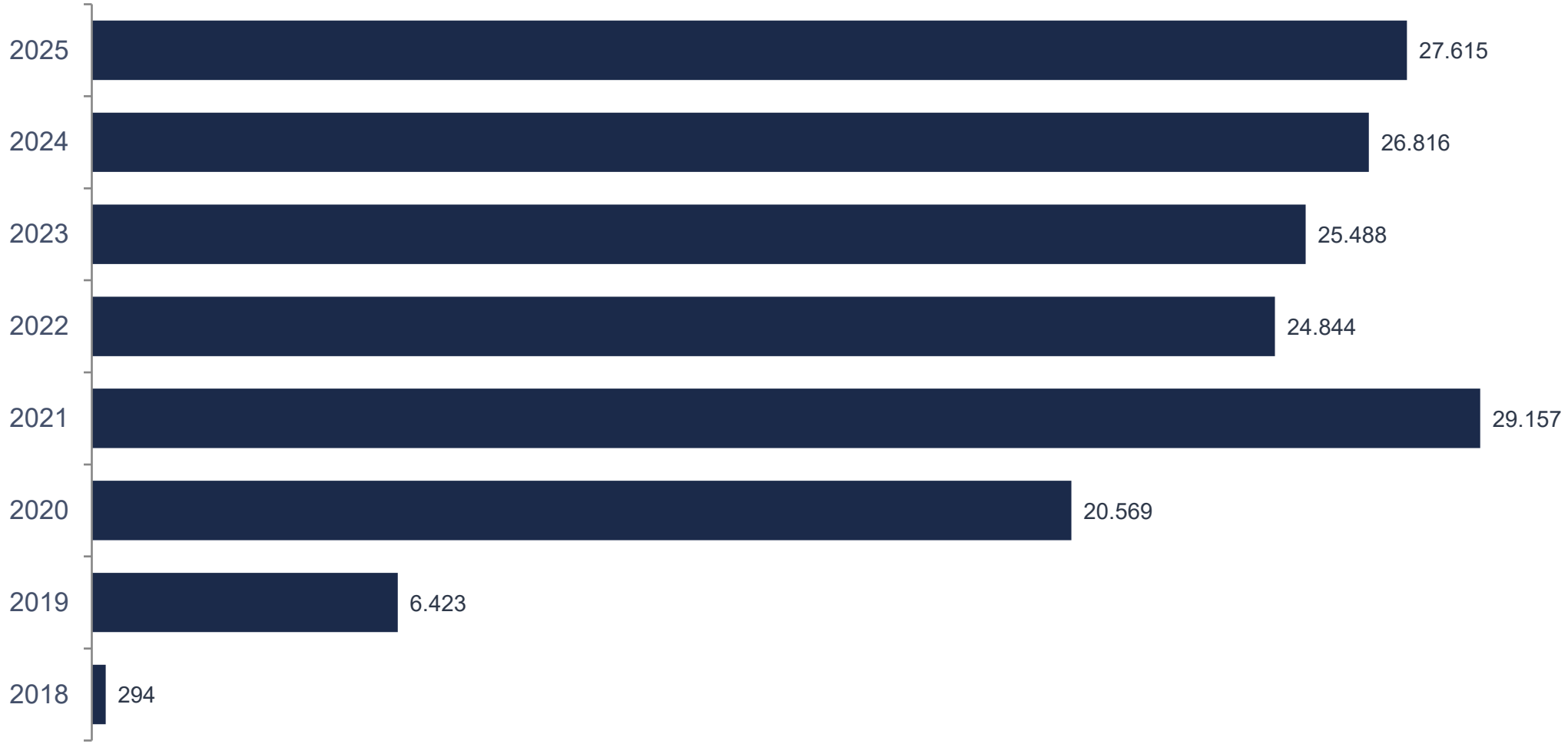
Remote hearings / videoconferences I.

January 2018 – December 2025



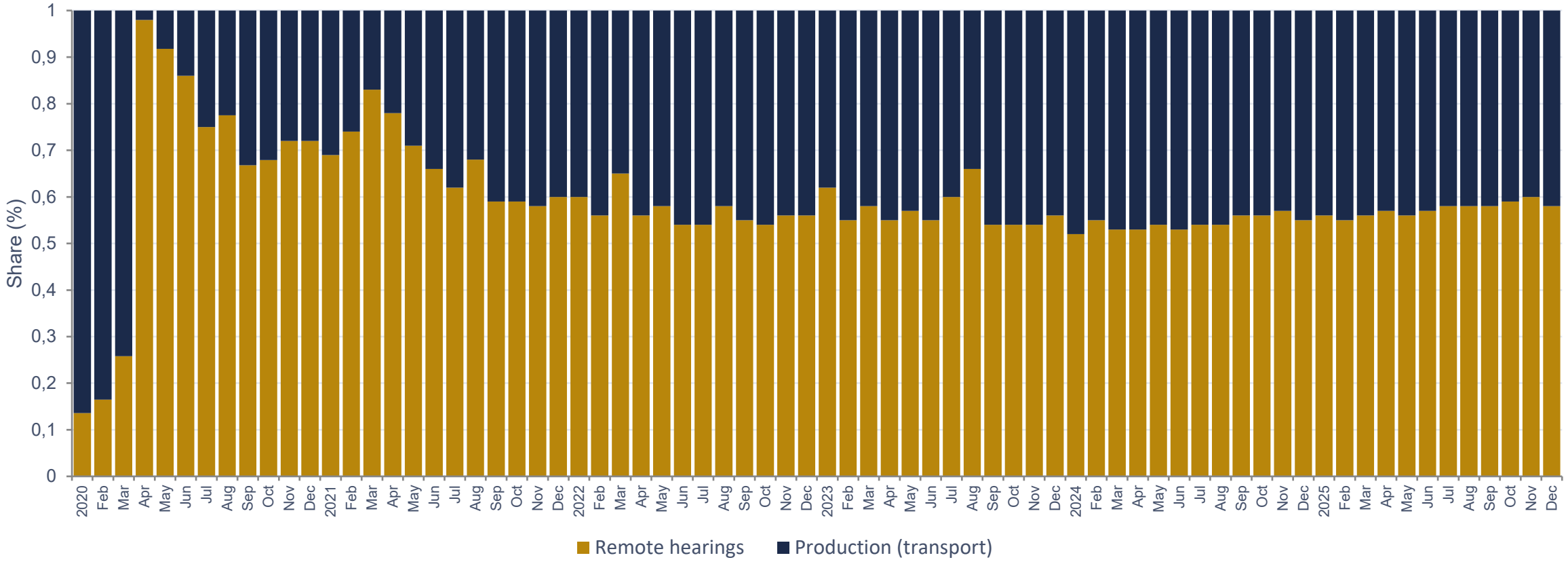
Remote hearings / videoconferences II.

January 2018 – December 2025



Hearing of persons in detention

Share of remote hearings vs. production (court-ordered transport), 2020–2025



Key point: during COVID up to **80%** of in-person appearances were replaced by remote hearings

Immediacy and the fair trial

The constitutional tension behind every remote format

- **Immediacy principle — direct, first-hand perception of evidence**

- **The defendant's right to presence and effective participation (ECHR Art. 6)**
  - Marcello Viola v. Italy (2006) – *"Videoconference participation is compatible with Article 6, provided it pursues legitimate aims and the defence rights are safeguarded."*
  - Khodorkovskiy and Lebedev v. Russia (2020)

- **Ensuring the publicity of the hearing**

Practical experience I.

1) **No more reluctance to use**
2) The right to **ask and initiate questions**, to **make comments and observations**, even cross-examination, can be easily exercised
3) **The participants** — witnesses, the accused, lawyers, experts — **are in favour of** the system too
4) **safety of protected victims and witnesses**

Practical experience II.

5) Less trouble with **keeping order** during the trial
6) Recordings as **trial minutes**
7) **„issues”** might occur **with weblinks** / / direct dialing
8) hearing witnesses abroad via **weblink - C-255/23 and C-285/23** *(suveregnity issues?!)*
9) **Judges are skilful** at using the system

Hearing a witness on screen: risks and safeguards

- **Credibility on screen** — fewer non-verbal cues
- **Is the witness alone? — who is off-camera?**
  - Highlighting / speaker view — controlled by the judge
  - Mute-all (forced mute)
- **Protected-witness mode — image/voice masking**
- **Every safeguard feeds into one recording**

2

E-files

The image and audio recording as part of the case file

The recording is part of the file — by law

- **The remote hearing is always recorded (recording on by default)**
  - *reason:* legal compliance (Cp. § 125(2); Decree 12/2018. (VI. 12.) MoJ, § 52–53)
  - recording and streaming each appear as a separate “participant”
  - the recording must be released on the parties’ request
- **Recordings as trial minutes**

Why integrity matters: three safeguards

Encrypted

The recorded image and audio are stored encrypted

Access-controlled

Not reachable through the organiser interface — only the institution can retrieve it

Chain of custody

Per-session files and full logs (who, what, when) make it traceable

3

Witness (and defendant) videoconferencing

EIO - Rules & experiences I.

Specific grounds for refusal

- **No consent of the defendant (Art. 24.2 (a))**
  - in writing or recorded in the minutes
- **No consent of the witness**
- **Execution contrary to the fundamental principles of the executing State's law (Art. 24.2 (b))**
  - C-325/24 - Bissilli

EIO - Rules & experiences II

Procedural rules

- **„forum regit actum”** — but also **„locus regit actum”**
- **A member of the executing court should be present**
  - verifies identity + ensures enforcement of national rules
- **Minutes of the hearing:**
  - issuing court — minutes on the merits
  - executing court - records who is present and compliance / sends recording without delay

EIO - Rules & experiences III.

Interpretation

- **Interpreter as mediator** → criminal cost
- **Contact language** to be agreed (form A, section K)
- **Appointment** → not regulated, but: the issuing state (reasonable for criminal costs)
- **In the executing MS** — may be needed **to follow the proceedings** → own costs (Art. 21(1))
- **Too high costs** → negotiation (Art. 21(2))

Background rule: Directive on Interpretation (2010/64/EU)

Videoconference with non-EU States

- **Art. 9 — Second Additional Protocol (2001) to the European Convention on Mutual Assistance in Criminal Matters (Strasbourg Convention)**
- **Main difference:**
  - as a general rule — only witnesses and experts
  - defendants only by special agreement, or not at all
  - reservations and declarations (CoE Treaty No. 182)

https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=182

If addressed to Hungary: consent of witness and expert required

4

Assessing evidence and artificial intelligence

Authenticity of image and audio recordings — when must the court order expert evidence if a party alleges AI manipulation?

Comparative supreme-court practice

on the authenticity of digital recordings

FRANCE

Cour de cassation

1re civ., 2021.02.11., 19-23.501

Free proof, but a credibly contested digital exhibit may be set aside. **On serious doubt (doute sérieux)** the judge must order the necessary examination (expert).

GERMANY

Bundesgerichtshof

„objektiv tragfähige Tatsachengrundlage"; StPO 244(2), 261, 267. §

Free evaluation of evidence is **limited by the duty of investigation**: the court must clarify the authenticity of multimedia evidence. However, it examines **only the obvious** (naheliegende) alternatives, that rest on concrete indications.

POLAND

Sąd Najwyższy

Ministry of Justice & Ombudsman (RPO), 2024

Not a substantive "doubt threshold", but a **procedural burden**: the expert motion must be filed by the party **contesting authenticity** — the court does not examine every file ex officio.

HUNGARY

Kúria

Be. §§ 167, 188(1), 520 — no dedicated Curia ruling

Free evaluation; **expert is mandatory** where a fact requires special expertise — a recording's authenticity is such. **On well-founded doubt** expert evidence is due.

International context and the common principle

ECHR — Strasbourg

Lisica v. Croatia (20100/06, 25 Feb 2010)

Under **Article 6**, what matters is not the objective genuineness of the recording, but whether **the defence had a real opportunity** to challenge its authenticity. Admissibility itself is a matter of national law.

USA — the burden-shifting model

Proposed FRE 901(c); (*Rittenhouse (2021); State v. Puloka (2024))*

1) The contesting party must first make a **threshold showing** that the evidence is a deepfake.
2) The proponent must prove genuineness by the **higher ("preponderance") standard**.

The common principle

The court need not subject every recording to an authenticity check, and a bare allegation is not enough. **The duty to order expert evidence arises on a concrete, objective indication (well-founded doubt) — and then the burden of proving authenticity (partly) shifts to the party submitting the recording.**

Can the forensic expert give certainty?

- **No method can categorically prove — genuine or AI**
- **Structural reason: detection and generation share the same basis**
  - a detector spots a flaw → the generator is trained to remove it
- **The expert opinion is probability, not certainty**
  - chain of custody, device, metadata, witnesses, circumstances

There is no foolproof way today to classify … as authentic or AI-generated.

Linna, Grimm, Grossman, Tunheim et al., „Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases", 2024 University of Chicago Legal Forum 75.

Huang v. Tesla, 2023— “deepfake defence” rejected

Superior Court of Santa Clara County, California (Judge Evette Pennypacker)

- 2018 fatal crash — Autopilot engaged ⟹ **wrongful death lawsuit**
  - *Plaintiffs: Autopilot failed; E. Musk on a 2016 statement (self-driving “safer than a human”)*
  - *Tesla: Musk is often a target of deepfakes*
- The court rejected the deepfake argument based on mere possibility

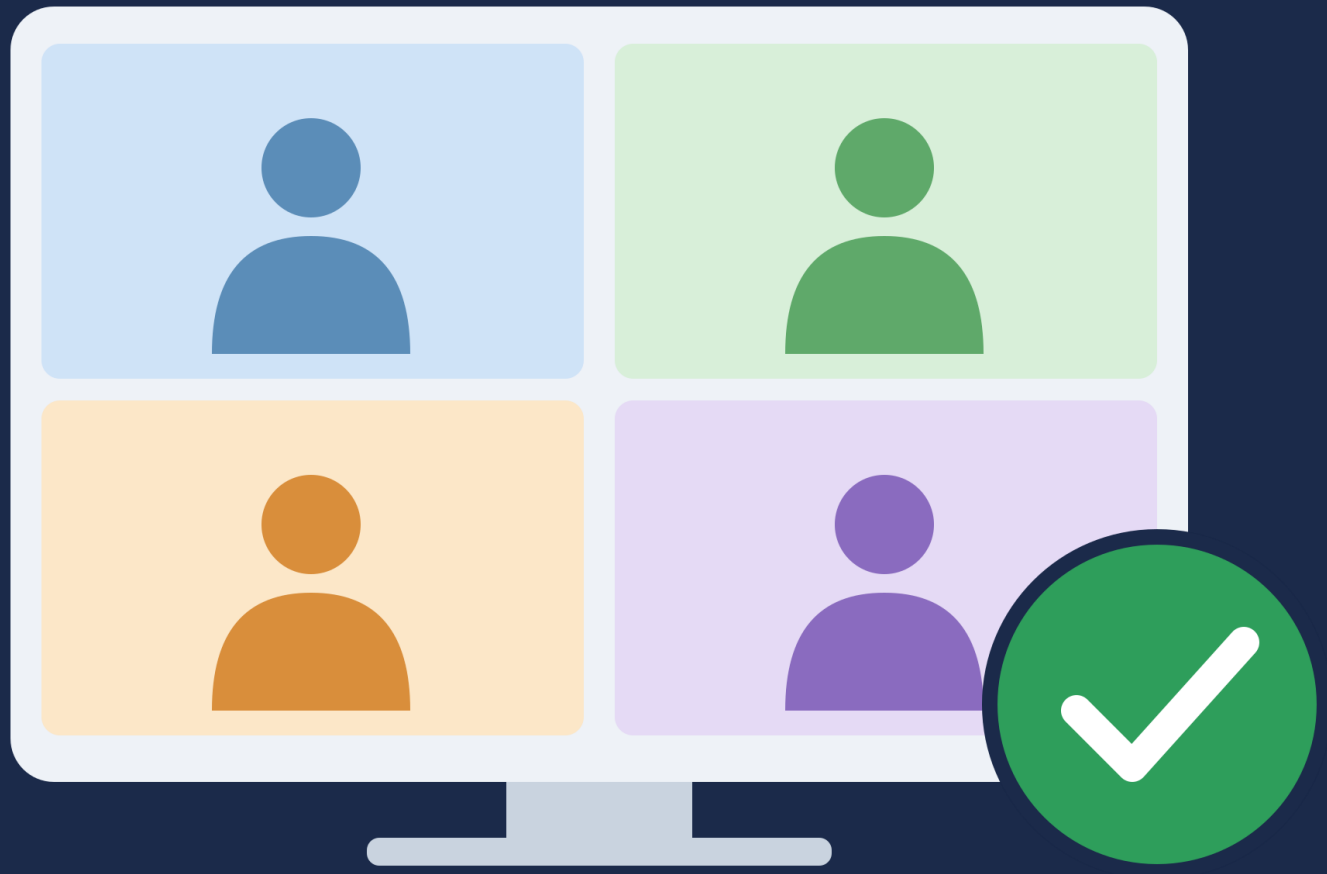
The deeper lesson

- ***Irony:* the "most objective" evidence undermines itself**
  - authenticating and deceiving systems share the same basis — no independent check

- ***Proof of origin* (C2PA, cryptographic origin) — only if built in at capture**
  - Kúria, BH 2015.2.38. — judging a recording's value as evidence: how was it made, and could it have been manipulated?

- ***The focus shifts:* expert opinion → overall weighing of evidence**
  - the expert opinion is one factor, not the last word

Conclusion



Thank you for your attention!

DIGITAL TECH AS TOOL TO COMMIT CRIME

ERA SEMINAR, BUDAPEST

OCTOBER 16, 2026

Emmanuelle Legrand
French judge (seconded), former public prosecutor and liaison prosecutor
Criminal, cyber, digital, and AI law

Co-funded by the European Union

WHY AND HOW IS TECH CHANGING « TRADITIONAL » CRIMINAL INVESTIGATION?

COMMISSION OF CRIME	INVESTIGATION ABOUT CRIME/ PROSECUTION
Fast to commit crime – Fast to disappear	Takes time to investigate, identify, find, and prosecute
No rules and no ethics	Procedural rules and human rights
Catch me if you can ! I do not know borders! « Low cost » compared to other types of crime	Jurisdiction according to the law, international mutual legal assistance tools
Electronic evidence easy to erase	Electronic evidence not easy to obtain, read and interpret
Creative methods but not-so-complicated tools available on the internet/darknet/market	Not using any kind of tools without guarantees and need to respect the law and people's rights
Technology keeps evolving everyday / « AI revolution »	Criminal procedural law and investigative techniques sometimes take a long time to keep up with tech/real world developments

AI and cybersecurity: the new threat

CYBER POLICY BY CYBER PEOPLE: The dominance of the AI perspective in cybersecurity is leading people to focus on the wrong issues, Marcus Hutchins told Morning Cyber in an interview. Hutchins is a cyber threat researcher and former hacker best known for stopping the huge WannaCry ransomware attack in 2017.

Context: Since Anthropic unveiled Mythos back in April, the cybersecurity world has become overwhelmed by fear, uncertainty and doubt about the capabilities of frontier AI models. Incidents like OpenAI's accidental intrusion into Hugging Face have hit the highest political level, the musings of top AI voices like Dario Amodei and warnings from former employee Jacob Coxon have made front page news.

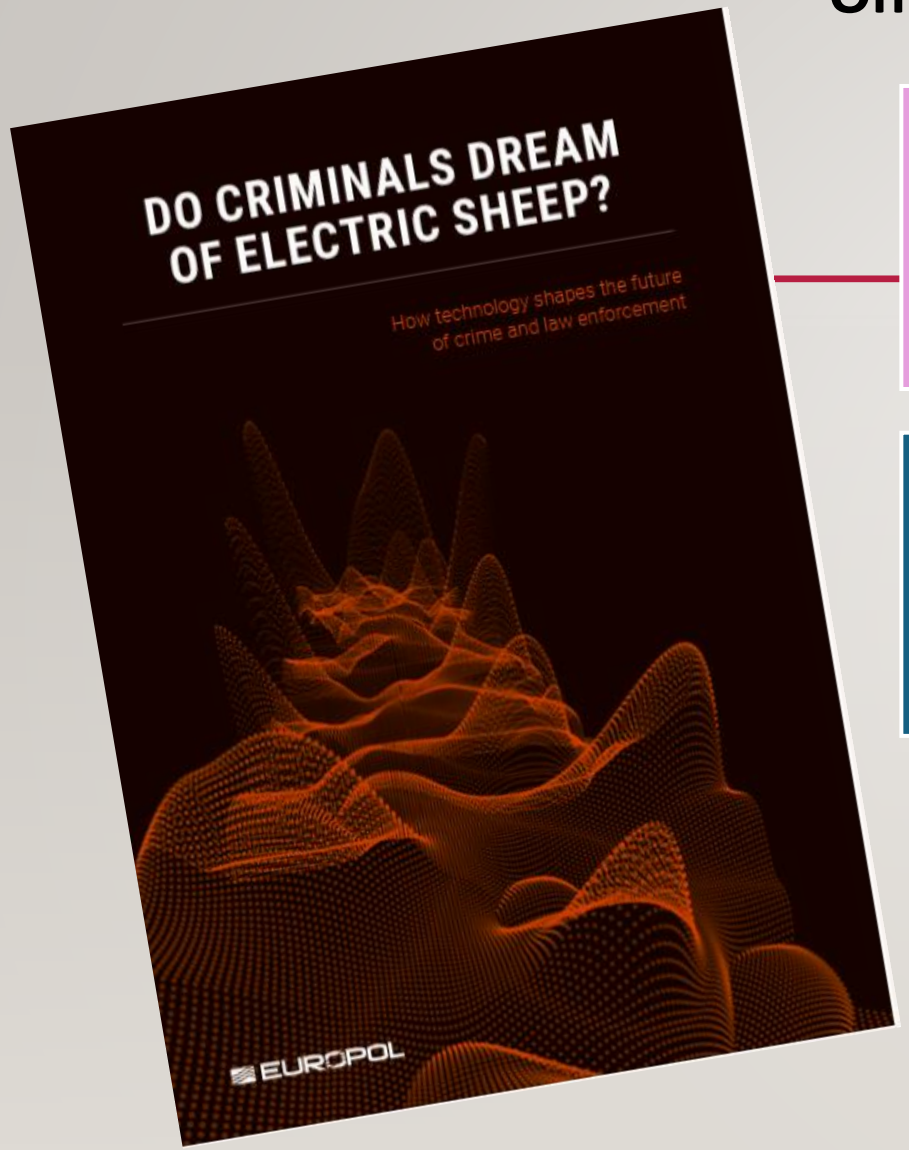
Unhelpful: Not only does the focus on outlandish or unlikely outcomes mean potentially more pressing concerns are sidelined, it is actively unhelpful, Hutchins argued. "The doomer stuff is very counterproductive," he said, adding that it leads people to disengage and causes "disaster fatigue," in turn disincentivising them from taking steps like doing security updates that could actually help them.

The vulnerability obsession: Hutchins acknowledged that AI systems are good at finding software bugs, known as vulnerabilities. But it's more common for hackers to break into systems through other means, like phishing. EU cyber agency ENISA said in a key report last year that hackers got into systems by exploiting vulnerabilities in only 21.3% of cases. Hutchins put that number at about 30%.

Looking in the wrong places: That means that even if an AI model was invented that could find and fix every single vulnerability — an extremely unlikely outcome — it still wouldn't stop the majority of attacks, Hutchins argued. In any case, in that scenario, hackers would just try a different method, he said. "This hyper fixation with software vulnerabilities has kind of sucked all the air out of the room."

Politico, October 2nd, 2026

On the crime side …



AI

Botnets, cyber attacks

QUANTUM

5G

Darkweb/ Cryptocurrencies

IoT

3D-printing

Biotech

« OLD » TECHNIQUES, LIKE PHISHING, STILL WORK

CYBERSECURITY

EUROPE'S INBOX PROBLEM: Three out of every four EU employees have encountered suspicious emails, messages or links at work, according to a new Eurobarometer survey released this week.

Phishing wins: Phishing remains the most common workplace cyber threat, with 39% of workers reporting fraudulent messages or websites designed to steal information or gain access to systems. Other common threats include attempts to steal personal data, at 18%, malware attacks, 17%, and efforts to compromise passwords, 16%.

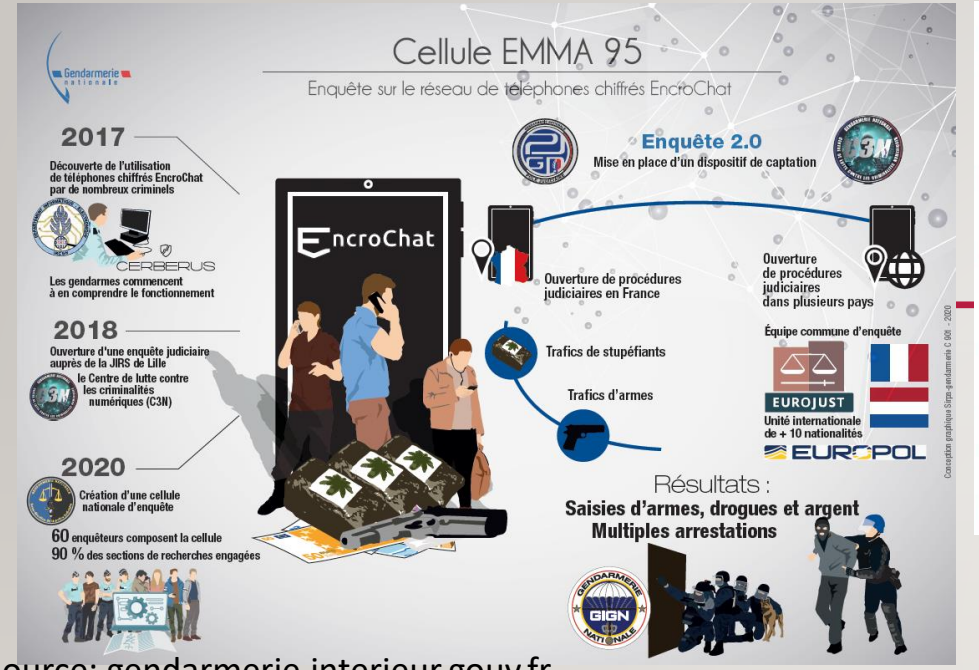
Enter AI: Another 15% reported encountering AI-generated scams. But spotting them remains tricky — 83% of workers could understand that cyberattacks have serious consequences, but only 48% said they could recognize an AI-generated fake video.

Politico, October 2026

EXAMPLES OF MORE « SOPHISTICATED » CYBERCRIME

- Malware/ransomware
- Encrypted criminal communications/criminal networks
- Darkweb markets/ Cryptocurrencies- financial infrastructure – money laundering
- Crime-as-a-service: phishing tools, personal data, botnet services…
- 3-D printing for firearms… and more to come?
- AI for biocrime/bioterrorism?

Encrypted criminal network (Encrochat)



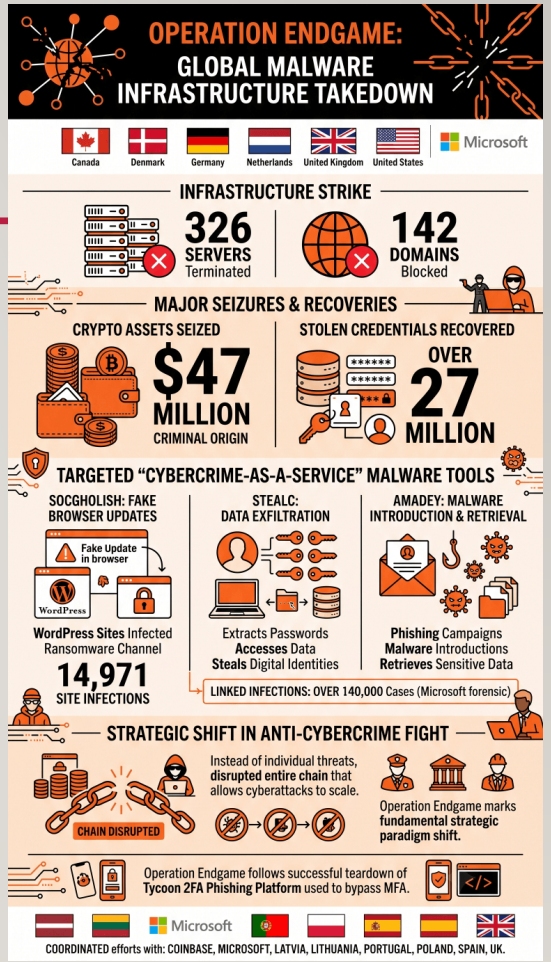
Source: gendarmerie.interieur.gouv.fr

Ransomware (Lockbit)



Source: National Crime Agency UK

Malware-as-a-service



Source: news.bitcoin.com

Darknet (Silkroad)



Source: ice.gov

Phishing-as-a-service (Labhost)

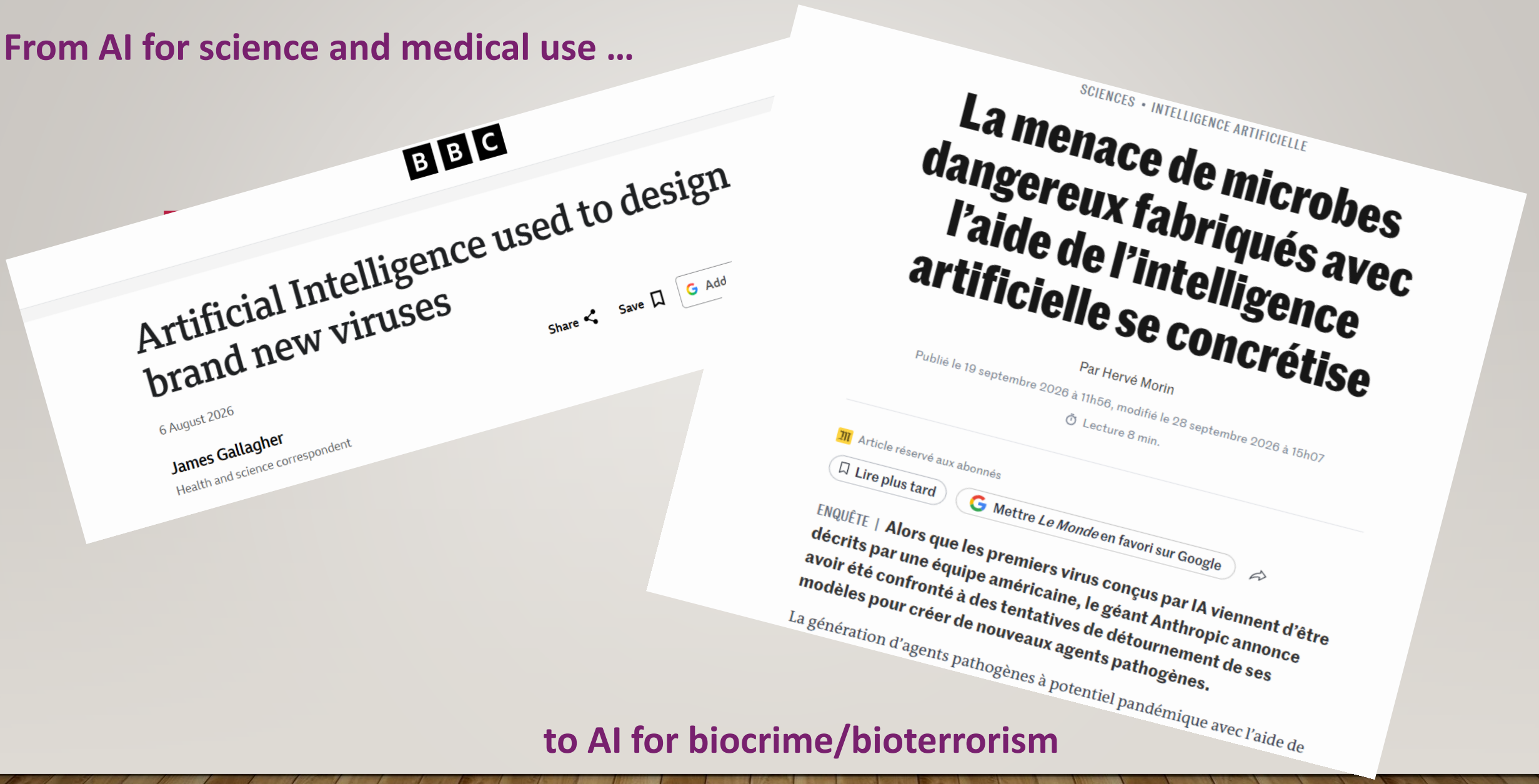


3-D PRINTING - CRIMINAL CASES EXAMPLES – from firearms to ATM skimming devices and counterfeiting?

AI Overview (Google's reply): **« Notable Recent Cases**

- **Robert Adamski (London, UK — January 2026):**
  - **Offenses:** Jailed for 17 years total (15 years imprisonment, 2 years on licence) at the Old Bailey after counter-terrorism police caught him manufacturing an FGC-9 Mk2 9mm semi-automatic firearm, alongside terrorism and weapon possession charges.
  - Counter Terrorism Policing +1
- **David Boylett (Telford, Shropshire, UK — August 2026):**
  - **Offenses:** Sentenced to 4.5 years in jail following a National Crime Agency (NCA) investigation. Officers found him 15 minutes away from finishing a 3D-printed firearm, along with two 3D printers and instructional videos.
  - National Crime Agency +1
- **Roy Tucker (Edmonton, Canada — September 2026):**
  - **Offenses:** Sentenced to 3 years in prison after being found guilty of multiple weapons charges involving a commercial-grade 3D printer, 16 privately made Glock-style handguns, and thousands of rounds of ammunition.
  - YouTube·CityNews
- **Ammani Justino (Jacksonville, Florida, USA — September 2026):**
  - **Offenses:** Charged with federal weapons offenses for using a 3D printer to mass-produce and sell roughly 50 "Glock switches" (devices that convert handguns into machine guns) at a time.
  - YouTube·News4JAX The Local Station
- **Marquel D. Payne (Evansville, Indiana, USA):**
  - **Offenses:** Sentenced to 7 years in federal prison for possessing a 3D-printed ghost gun, a 3D-printed silencer, and about 60 3D-printed Glock switches as a convicted felon.
  - Department of Justice (.gov)
- **Demetrio Daga (Albany, New York, USA — October 2026):**
  - **Offenses:** Convicted on all 15 counts after a 15-month investigation into an arsenal that included dozens of 3D-printed ghost-gun handguns and AR-style rifle frames, facing up to 40 years in prison.
  - WRGB »

From AI for science and medical use …



BBC

Artificial Intelligence used to design brand new viruses

Share Save Add

6 August 2026

James Gallagher

Health and science correspondent

SCIENCES • INTELLIGENCE ARTIFICIELLE

La menace de microbes dangereux fabriqués avec l'aide de l'intelligence artificielle se concrétise

Par Hervé Morin

Publié le 19 septembre 2026 à 11h56, modifié le 28 septembre 2026 à 15h07

Lecture 8 min.

Article réservé aux abonnés

Lire plus tard

Mettre *Le Monde* en favori sur Google

ENQUÊTE | **Alors que les premiers virus conçus par IA viennent d'être décrits par une équipe américaine, le géant Anthropic annonce avoir été confronté à des tentatives de détournement de ses modèles pour créer de nouveaux agents pathogènes.**

La génération d'agents pathogènes à potentiel pandémique avec l'aide de

to AI for biocrime/bioterrorism

… and on the investigation/prosecution side …

Jurisdiction/ Cross-border evidence	Public/private cooperation	Collection of electronic evidence/ Chain of custody	Smartphone data extraction
Encryption/ « going dark » phenomenon	OSINT/big data investigation (regulated?)	Undercover/ Cyberpatrols	Expertise in cyber
Privacy rights	Biometrics/facial recognition?	Fake news/ Deepfakes	« Legal hacking »?

Different laws, different rules, different limits, different court decisions, different capacities, different results…
But quite the same challenges (legally and technically)

TOWARD AI-POWERED CRIMINAL INVESTIGATION?

PRO Article | Cybersecurity and Data Protection | + 2 more

Europe's AI policing plan stokes privacy concerns

The EU police ... have to contend with both cybercriminals and privacy ...

PRO Newsletter | Cybersecurity and Data Protection

Cyber's AI panic has a hacker problem

by Antoaneta Roussi · OCT 2 · 7 MINUTES READ

PRO Newsletter | Cybersecurity and Data Protection

Europe wants an AI-powered Europol

by Antoaneta Roussi · OCT 5 · 10 MINUTES READ



Faster, at scale

Jürgen Ebner, the agency's deputy executive director, who was named last month to take its helm, said that crimefighting today requires equipping your organization with the full powers of artificial intelligence.

"AI is transforming how crime is committed across a broad range of criminal activities," Ebner said a week after being selected by national representatives to take the top job, pending a review by the European Parliament. "AI makes criminal activities faster, more sophisticated and easier to carry out at scale. This is a significant challenge for law enforcement."

Politico, October 5th, 2026

Wiewiórowski's EDPS has previously reprimanded Europol for its data-gathering practices, and has pushed back against a previous proposal to expand Europol's remit.

He has cautioned that the proposal to revamp Europol poses serious privacy risks, and would allow the agency to retain data on a "vast" number of people with no links to criminal activity "for an extensive and unspecified period of time."

Furthermore, Stéphane Duguin, a former Europol Cybercrime officer who now leads Protect.ngo, says law enforcement also finds it challenging to keep up with adversaries' technological and strategic advances. Beyond the challenges of their technical capacity, he argues that Europe's policing network must also overcome its own longstanding structure.

Criminals aren't "only doing cybercrime or foreign interference or information manipulation, but that's how police forces operate. And that's a problem," Duguin said. "If you look at Europol in a vacuum, it doesn't make any sense because it's the whole value chain of justice that needs to be evolving. If you have more capacity to investigate online crimes but, at the end of the day, it doesn't stand in front of a court because of national legislation, then it doesn't make any sense."

THANK YOU FOR YOUR ATTENTION!



Krisztina Karsai

The impact of the AI Act on the applications of AI to criminal justice

#DIGITALISATION and #ARTIFICIALINTELLIGENCE in Criminal Justice

Digital investigations, open source intelligence tools and AI

Budapest, 15-16 October 2026

FACE-TO-FACE

EXCELLENCE IN EUROPEAN LAW

University of Szeged, Hungary

(Artificial Intelligence and Legal Order Research Group)



Artificial Intelligence and the Legal Order

SZTE UNIVERSITY OF SZEGED

Co-funded by the European Union

Interdiszciplináris Kutatásfejlesztési és Innovációs Kiválósági Központ

For centuries, criminal justice has asked what happened.

AI increasingly asks what will happen next.



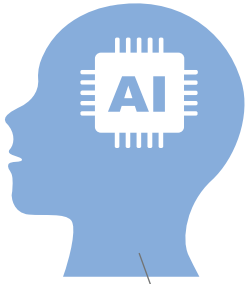
At what point does technological assistance begin to transform the nature of criminal justice decision-making itself?

When AI creates reality (?)
When AI learns reality (?)
When AI predicts reality (?)
When AI recommends reality (?)

A_L_E_A_I_A_C_T_A_E_S_T



AI ACT



Legal fitness

2024/1689 Regulation

AI system' means a machine-based system that is designed to operate **with varying levels of autonomy and that may exhibit adaptiveness after deployment**, and that, for explicit or implicit objectives, **infers**, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments (Article 3, 1)

PROHIBITED | HIGH-RISK | OTHER

Article 6 (2) and Annex III Section 8 - Administration of justice and democratic processes:

(a) AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and **in applying the law to a concrete set of facts**, or to be used in a similar way in alternative dispute resolution;

APPLICATION by the authorities

APPLICATION by the parties

But not by the criminals if…

AI & AI Act & Criminal Justice

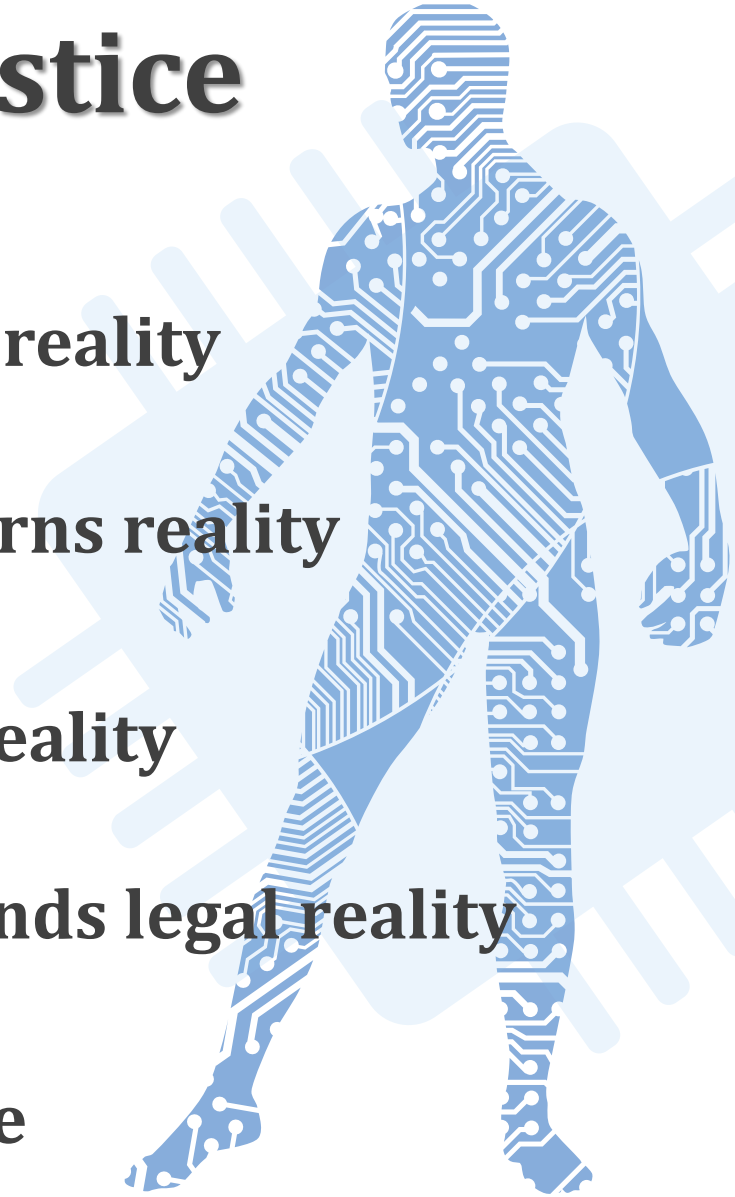
01 Deepfake - When AI creates the reality

02 Machine learning – When AI learns reality

03 Prediction – When AI predicts reality

04 Sentencing – When AI recommends legal reality

05 AI Literacy in the criminal justice



DEEPFAKE – AI creates reality

a fundamental assumption of criminal evidence – seeing or hearing something provides at least some basis for believing that it actually happened

false evidence
→ synthetic material presented as authentic

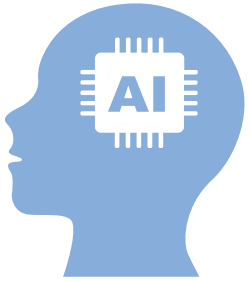
false denial
→ authentic material challenged as AI-generated

AI ACT Art 50, 2; Art 50, 4
Transparency obligations

outputs shall be marked in a machine-readable format and are detectable as artificial; must be disclosed that the content has been artificially generated or manipulated

AI ACT does not determine its admissibility or evidential value in criminal proceedings

DEEPFAKE



OR HARMONISATION/UNIFICATION ON EU LEVEL?

AI ACT Art 50, 2; Art 50, 4
Transparency obligations

outputs shall be marked in a machine-readable format and are detectable as artificial; must be disclosed that the content has been artificially generated or manipulated

AI ACT does not determine its admissibility or evidential value in criminal proceedings

NATIONAL LEGAL SYSTEMS

Who bears the burden of establishing its authenticity?

What degree of authentication should be required?

When should the court appoint an expert?

How should the chain of custody of digital material be documented?

Does uncertainty affect the assessment of reasonable doubt?

DEEPFAKE … AI detecting AI



https://factcheck.afp.com/doc.afp.com.C8V34NQ

„96% probability that the recording has been manipulated."

?

AI ACT Annex III 6, c

High risk AI – evaluation the reliability of evidence!

„AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies, in support of law enforcement authorities to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences"

AI & AI Act & Criminal Justice

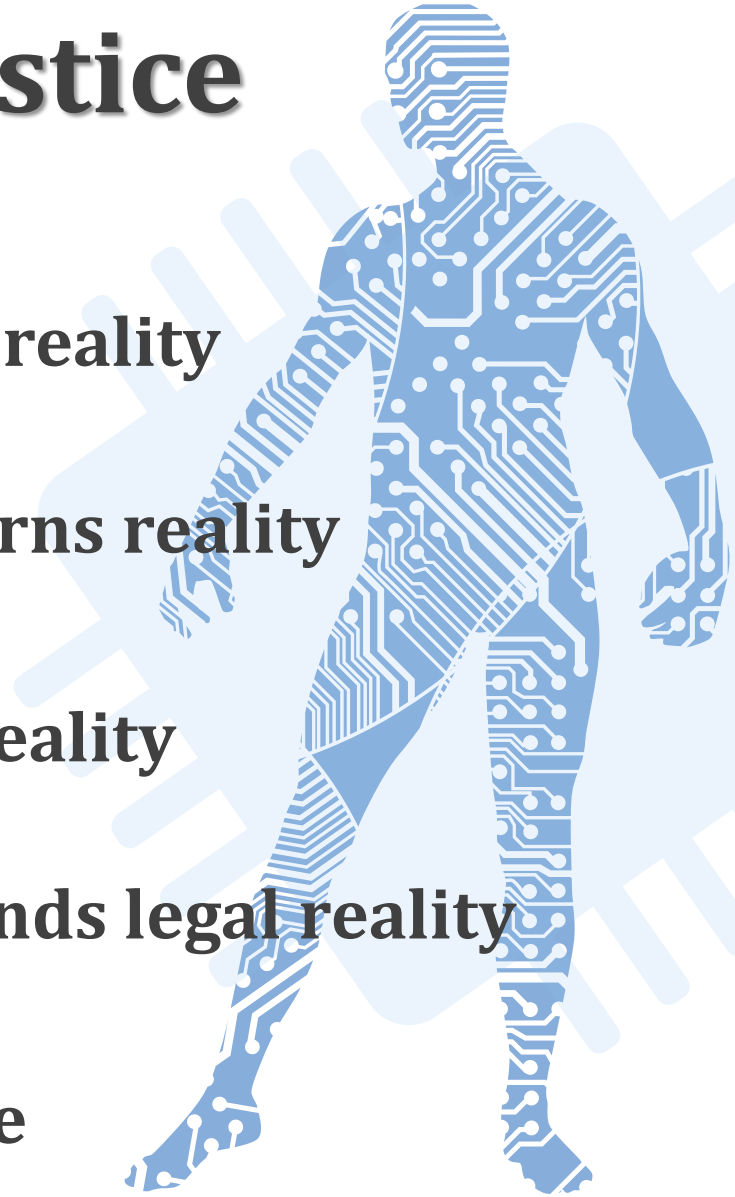
01 Deepfake - When AI creates the reality

02 Machine learning – When AI learns reality

03 Prediction – When AI predicts reality

04 Sentencing – When AI recommends legal reality

05 AI Literacy in the criminal justice



Machine Learning



Machine Learning

Traditional programming

RULES + DATA → OUTPUT

Rules
(written by a human)

```
IF ears are large
and upright
AND muzzle is short
AND fur is short
THEN classify as
chihuahua.

ELSE IF round shape
AND dark colour
AND texture is rough
THEN classify as
chocolate muffin.
```

\+

New image
(to be classified)



→

Output
(apply the rule)



Chihuahua

Machine learning

DATA + OUTCOMES → PATTERNS → PREDICTION

Training data
(with known labels)



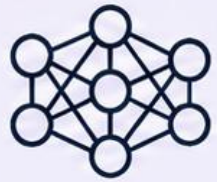
Chihuahua



Chocolate muffin

→

Learning patterns
(from many examples)



The system learns which visual features (e.g. shape, texture, colour, ears, eyes) are associated with each label.

→

New image
(to be classified)



↓

Prediction
(based on learned patterns)

Chihuahua	96%
Chocolate muffin	4%

Key legal difference: In traditional programming, the rule is explicitly formulated by a human decision-maker. In machine learning, the rule is inferred from data: the system learns which features are associated

Machine Learning (2)

example

Traditional programming

RULES + DATA → OUTPUT

Rules
(written by a human)



```
IF previous
convictions > 2
THEN classify as
high risk.
```

+

Data



→

Output



High risk
/ Low risk

Machine learning

DATA + OUTCOMES → PATTERNS → PREDICTION

Data
(with known outcomes)



e.g. previous offenders and whether they reoffended

→

Learning patterns



The system identifies statistical patterns in the data.

→

Prediction



Estimated risk of reoffending



Key legal difference: In traditional programming, the rule is explicitly formulated by a human decision-maker. In machine learning, the relevant rule may no longer have been explicitly formulated by a human. It has been inferred from data.

Machine Learning (3)

inference

AI ACT does not regulate it separately as „special" technology

AI ACT technology-neutral

AI ACT – AI definition

„inference"

An AI system uses inputs to infer how to generate outputs such as predictions, recommendations or decisions. In machine-learning systems, these rules are typically not written explicitly by a human programmer; they are inferred from data.

high risk AI system (function)
+
WITH machine learning

= inference

Machine Learning (3)

Inference: the AI applies patterns learned from past data to this new person (object)

Prediction: „68% risk of reoffending"
Classification: "high-risk / low-risk offender"
Recommendation: "consider pre-trial detention"
Decision support: "similar cases typically resulted in 24–36 months' imprisonment"
Content: a summary of evidence, argumentation etc.

high risk AI system (function)
+
WITH machine learning

= inference

AI & AI Act & Criminal Justice

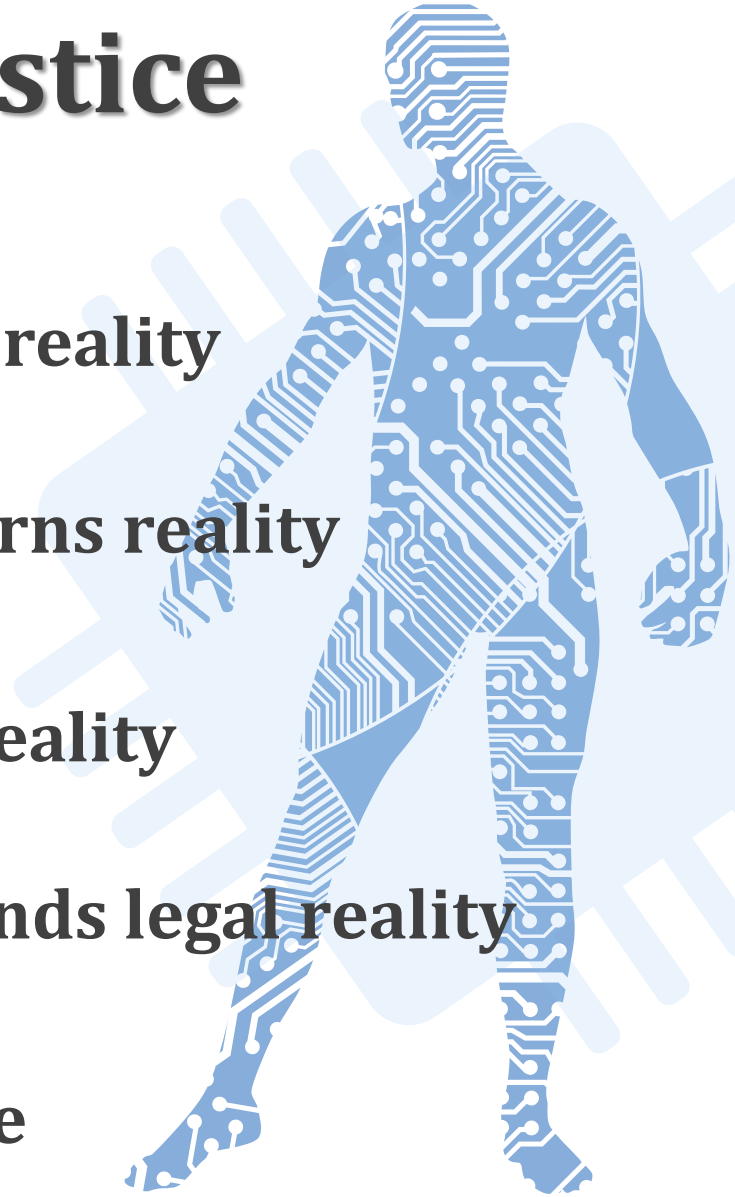
01 Deepfake - When AI creates the reality

02 Machine learning – When AI learns reality

03 Prediction – When AI predicts reality

04 Sentencing – When AI recommends legal reality

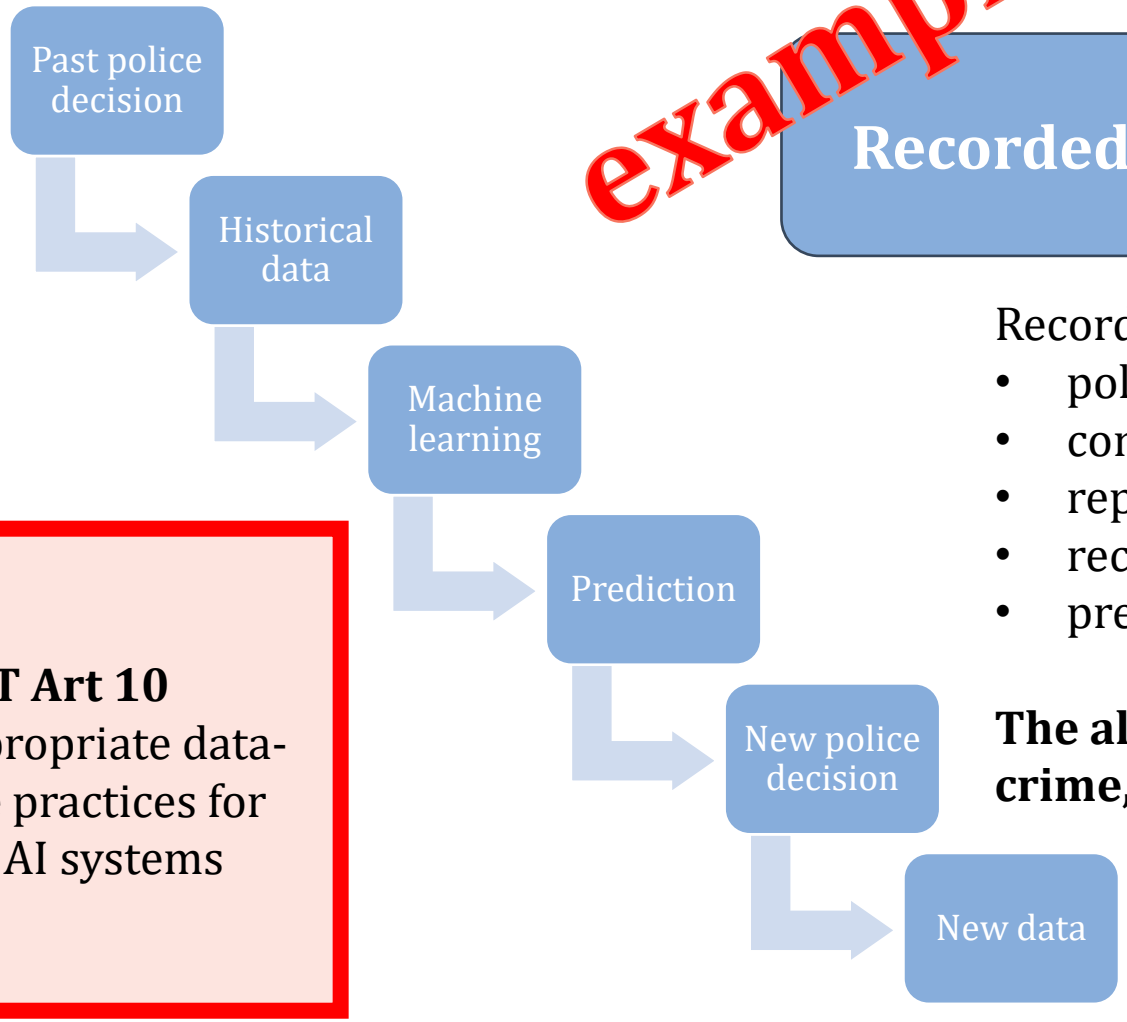
05 AI Literacy in the criminal justice



ML and Prediction

example

Recorded crime v Actual crime



Recorded crime reflects:

- police presence
- control and stop practices
- reporting patterns
- recording practices
- previous risk classifications

The algorithm may learn the institutional record of crime, not crime itself.

AI ACT Art 10
requires appropriate data-governance practices for high-risk AI systems

Prediction

prohibited AI practice:

AI ACT Art 5 (1) (d) the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of **a natural person committing a criminal offence,** based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity;

WHO YOU ARE

profiling
personality traits
predicted personal characteristics

WHAT YOU HAVE DONE

objective conduct
verifiable facts
facts directly linked to criminal activity

PROHIBITED
Art. 5(1)(d) AI Act

HIGH-RISK / PERMITTED
(subject to safeguards)
Art. 5 (exception) and Annex III (6d) AI Act

Example: Person A



Age: 21
Unemployed
Personality score: impulsive
Social profile: high-risk
Neighbourhood: X

AI output
Probability of future offending:
72%

→ PROHIBITED

Example: Person B


CCTV at the scene


Fingerprint on the weapon

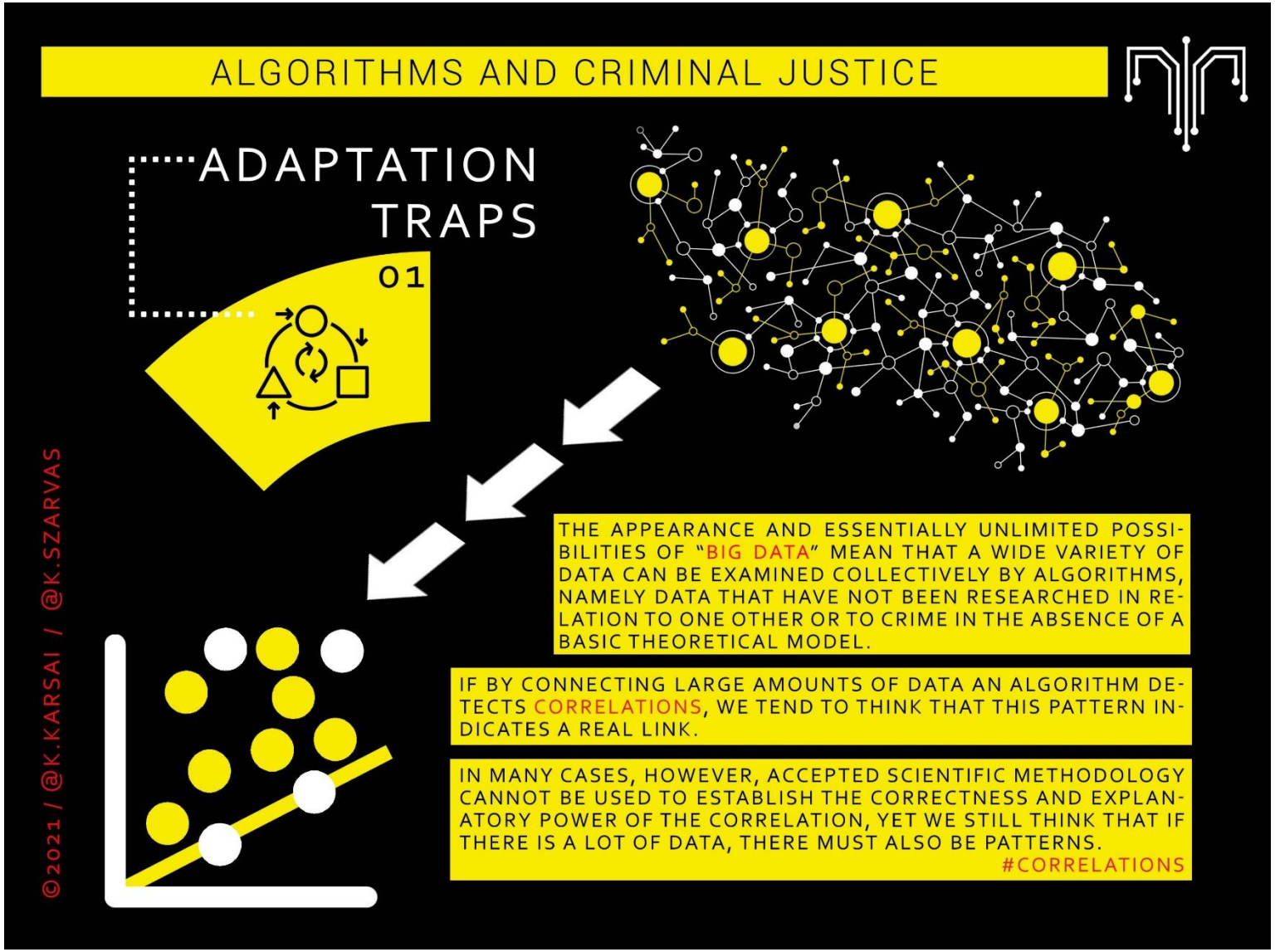

Phone location at the time


Previous convictions for similar offences

AI output
Probability of reoffending:
68%

→ HIGH-RISK / PERMITTED
(subject to safeguards)

ML and Correlations



INFOGRAPHS

PAPER

ML and Correlations

a newly discovered statistical relationship can legitimately support an inference about a fact that matters in the proceedings?

how should a court interpret and evaluate a probabilistic output produced by such a system?

Probabilistic evidence

Established forms of evidence that express uncertainty in statistical terms.

DNA evidence



"The probability of observing this DNA profile if it came from an unrelated person is **1 in 1 billion.**"

Fingerprint comparison



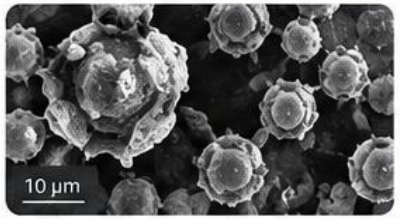
A system or expert provides a similarity score or probability of a match (e.g. 99.7%).

Voice comparison



"The observed features are much more likely if the questioned and known voice come from the same speaker."

Gunshot residue



Statistical analysis indicates how likely a particular trace would be under different hypotheses.

Cell-site / location evidence



Statistical analysis may be used to estimate the likelihood that a phone was in a particular area at a given time.

Machine-learning evidence

Outputs generated by a model that has learned patterns from data.

Facial recognition



A machine-learning system compares a face captured on CCTV with a suspect's image and generates a similarity or confidence score.

Deepfake detection



The system concludes, for example, that there is a 96% probability that a video has been manipulated.

Voice recognition



A machine-learning model analyses speech characteristics and estimates whether two recordings belong to the same speaker.

Gait recognition



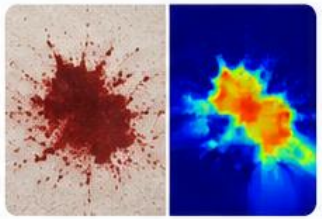
The system analyses a person's walking pattern and estimates whether the person in the video is the accused.

Object / activity recognition



AI may identify a weapon, a vehicle, a violent act or another relevant event in CCTV footage.

Forensic image classification



Machine learning may classify patterns in bloodstains, injuries or tool marks.

Probabilistic evidence expresses uncertainty numerically.
Machine-learning evidence generates an evidential conclusion by applying patterns learned from data.

The two categories can overlap (e.g. a facial-recognition score may be both probabilistic and machine-learning based).

ML and Probability

a newly discovered statistical relationship can legitimately support an inference about a fact that matters in the proceedings?

To what extent the evidence supports a given conclusion;
What the probability of error is;
And **how reliable** the system is that produced the probabilistic result

how should a court interpret and evaluate a probabilistic output produced by such a system?

AI & AI Act & Criminal Justice

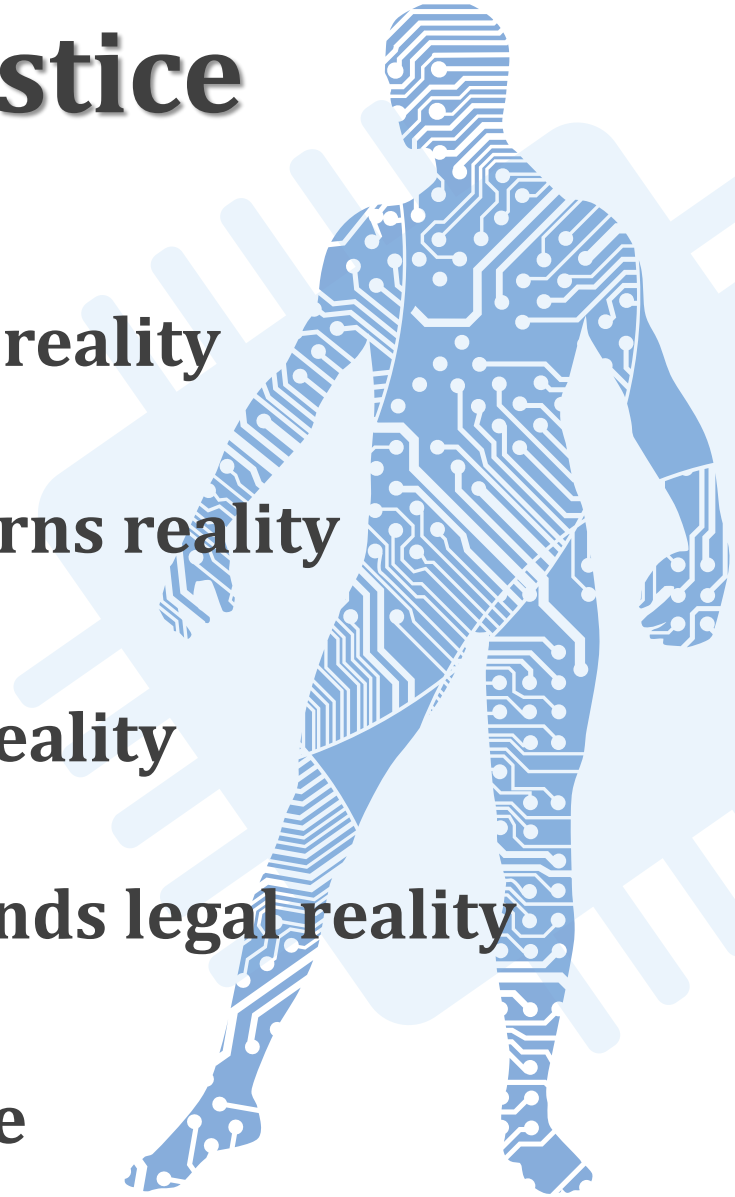
01 Deepfake - When AI creates the reality

02 Machine learning – When AI learns reality

03 Prediction – When AI predicts reality

04 Sentencing – When AI recommends legal reality

05 AI Literacy in the criminal justice



Sentencing



Here are 200 comparable judgments.

The median sentence in 1,420 comparable cases was 28 months.

In comparable cases, imprisonment was imposed in 82% of cases.

Recommended sentence: 32 months.

Sentence: 32 months' imprisonment.

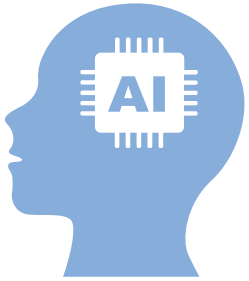
AI Act does not contain a separate category called a "sentencing algorithm"

Annex III, point 8(a) - high-risk AI system if intended to be used by a judicial authority, or on its behalf, to assist in **researching and interpreting facts and law and in applying the law to a concrete set of facts**

At which point does information become influence, and influence become decision-making?

AI Act Recital 61: AI may support judicial decision-making, but should not replace it

Sentencing (2)



Automation bias

AI Act Art 14 (4) b)
to remain aware of the possible tendency of **automatically relying or over-relying** on the output produced by a high-risk AI system (automation bias), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons

Paradox of consistency

Similar cases should receive similar sentences. AI can analyse thousands of judgments, detect sentencing patterns and potentially reduce unjustified variation between judges.
But: What if past sentencing practice itself contains unjustified disparities? A machine-learning system trained on historical sentences may not correct those disparities. **It may learn them.**

Summary

Application	AI Act response	Key provisions
Deepfakes	Transparency	Art. 50(2), (4)
Machine Learning	Data quality, bias control, accuracy & robustness	Arts. 10, 15
Prediction	Prohibition or high-risk regulation	Art. 5(1)(d); Annex III 6
Sentencing / Judicial AI	High-risk safeguards	Annex III 8(a); Arts. 14, 27, 86



The AI Act does not regulate all uses of AI in criminal justice in the same way.

The AI Act regulates the AI system.
It does not replace criminal procedure.

Key takeaway

AI ACT	CRIMINAL PROCEDURE
Risk classification	Admissibility of evidence
Data governance	Evidential value
Documentation	Standard of proof
Accuracy & robustness	Presumption of innocence
Human oversight	Equality of arms
Transparency	Defence access
Fundamental Rights Impact Assessment	Judicial reasoning
	Individualised sentencing



A compliant AI system does not automatically produce a lawful criminal justice decision.

The AI Act regulates the AI system.
It does not replace criminal procedure.

AI & AI Act & Criminal Justice

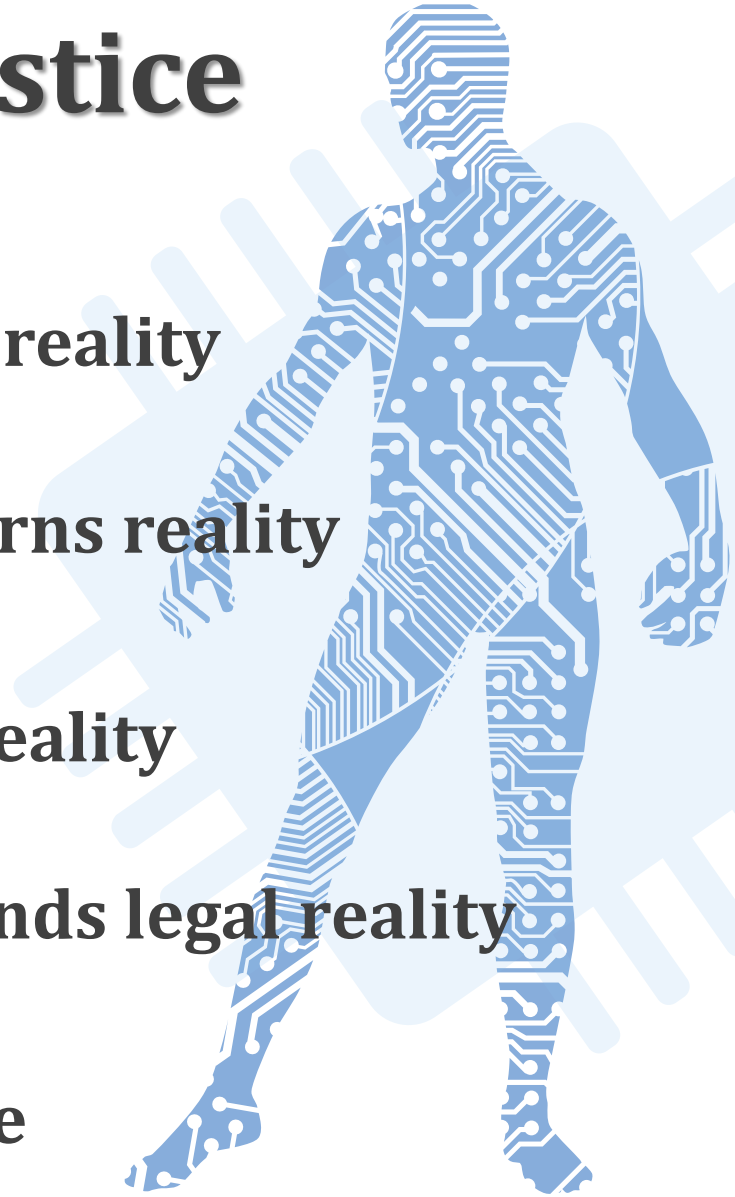
01 Deepfake - When AI creates the reality

02 Machine learning – When AI learns reality

03 Prediction – When AI predicts reality

04 Sentencing – When AI recommends legal reality

05 AI Literacy in the criminal justice



AI Literacy – AI ACT

AI Literacy: the final safeguard

AI literacy is not technical expertise



It is the ability to understand:

- what the system can and cannot do;
- what data and assumptions its outputs depend on;
- what uncertainty and error rates mean;
- when an output may reflect bias or weak correlations;
- when human judgment must override the system.

AI Literacy – AI ACT



Article 3 (56) ‘AI literacy’ means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

Article 4 - **Providers and deployers of AI systems shall take measures** to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Article 95 – (1) The AI Office and the Member States shall encourage and facilitate the drawing up of **codes of conduct**…

AI Literacy

AI ACT Regulation 2024/1689

Article 3 (56) … „**providers, deployers and affected persons**" … „informed deployment" „gain awareness about the opportunities and risks… possible harm it can cause"
Article 4, 95

Role	When can a court act in this role?	Relevance of AI literacy
Provider	When the court develops or commissions its own AI system	Ensures legal compliance, transparency, and accountability
Deployer	When the court uses an AI system in its operations or procedures	Requires awareness of proper use, safeguards, and limitations
‚Affected Person"	When an external AI system influences proceedings or evidence	Requires critical evaluation of AI impact and potential misuse



When the parties are using AI…

Summary

AI in criminal justice can create, learn, predict and recommend



The AI Act tells us when these systems are prohibited, high-risk or subject to transparency obligations

Final question: what role are we willing to let statistical and algorithmic reasoning play in decisions about individual liberty and responsibility?

Brodowski, Dominik (2023); Hartmann, Markus; Sorge, Christoph; Automatisierung in der Strafrechtspflege, NJW 2023, 583-588
Gülteki-Várkonyi, Gizem (2025): AI Literacy for Legal AI Systems: A practical approach SSRN, 2025
Gless, Sabine / Wohlers, Wolfgang (2019), Subsumtionsautomat 2.0 - Künstliche Intelligenz statt menschlicher Richter? in: Martin Böse / Kay H. Schumann / Friedrich Toepel (Hrsg.), Festschrift für Urs Kindhäuser zum 70. Geburtstag, Nomos Verlag 2019, S. 147-165.
REED C. LAWLOR(1963) : What computers can do: analysis and prediction of judicial decisions. American Bar Association Journal 1963, 49 337–344
SOLON BAROCAS – SOPHIE HOOD – MALTE ZIEWITZ (2013), Governing Algorithms: A Provocation Piece (March 29, 2013)
AMBER MARKS / BEN BOWLING / COLMAN KEENAN (2015): Automatic Justice? Technology, Crime, and Social Control. (October 19, 2015).
VEALE et al. (2019): Algorithms in the Criminal Justice System. The Law Society of England and Wales, 2019
Aleš Završnik (2019): Algorithmic justice: Algorithms and big data in criminal justice settings. European Journal of Criminology 2019
van Dijck, Gijs (2022) Predicting Recidivism Risk Meets AI Act. European Journal on Criminal Policy and Research, 28, 407–423.
DOI: 10.1007/s10610-022-09516-8.
Ryberg, Jesper (2024) Criminal Justice and Artificial Intelligence: How Should We Assess the Performance of Sentencing Algorithms? Philosophy & Technology.
DOI: 10.1007/s13347-024-00694-3.
Ryberg, Jesper (2024) Artificial intelligence at sentencing: when do algorithms perform well enough to replace humans? AI and Ethics.
DOI: 10.1007/s43681-024-00442-5.
Közvetlenül human versus algorithmic decision-making; recidivism prediction és sentencing összevetése
Ryberg, Jesper (2026) AI in criminal sentencing: mapping the ethical terrain. AI and Ethics, 6, Article 225.
Sandoval, Maria-Paz et al. (2024) Threat of deepfakes to the criminal justice system: a systematic review. Crime Science, 13, Article 41.
DOI: 10.1186/s40163-024-00239-1.
Herke Csongor (2024) A bizonyítékok újraértékelése: a deepfake technológia hatása a büntető igazságszolgáltatásra. Magyar Jog, 71(6), 321–332.
Capra, Daniel J. (2024): Deepfakes Reach the Advisory Committee on Evidence Rules, Fordham Law Review 92, 2491

https://www.linkedin.com/in/krisztina-karsai-106aa66b/

Thank you for your kind attention!

karsai.krisztina@szte.hu

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	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	
6	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)**	
7	Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030	
8	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.	

9	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.	
10	European e-Justice Strategy 2024–2028, OJ C/2025/437, 16.1.2025 (ELI: C/2025/437)	

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 *(OJ C 326/47; 26.10.2012)*
A1-04	Consolidated Version of the Treaty on the European Union, art. 9-20 *(OJ C326/13;, 26.10.2012)*
A1-05	Charter of fundamental rights of the European Union *(OJ. C 364/1; 18.12.2000)*
A1-06	Explanations relating to the Charter of Fundamental Rights *(2007/C 303/02)*
A1-07	Convention implementing the Schengen Agreement of 14 June 1985 *(OJ L 239; 22.9.2000, P. 19)*

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 *(OJ L 149, 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, 6th 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.195*9)
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 (*Strasbourg, 13.XII.1957*)

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)), *(OJ C 456, 10.11.2021)*
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 *(OJ L 81/24; 27.3.2009)*
B2-04	Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States *(OJ L 190/1; 18.7.2002, P. 1)*
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	InAbsentiEAW, 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, Zdziaszek, 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 C241/15 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 *Jeremy F / Premier ministre*, Judgement of the court (Second Chamber), 30 May 2013
B2-46	Case C-399/11 *Stefano Melloni v Ministerio Fiscal*, 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 Kozlowski, 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 *(Brussels, 25.5.2022, COM (2022) 245 final)*
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, *(Brussels, 20.7.2021 COM(2021) 421 final)*
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 *(OJ L 294/20; 11.11.2009)*
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 *(OJ L 337/102; 16.12.2008)*
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 *(OJ L 327/27; 5.12.2008)*
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 *(OJ L 220/32; 15.08.2008*)
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 Opria, 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, *(COM (2020) 605 final)*
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, *(COM(2018) 640 final)*
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), *(OJ L 156, 19.6.2018)*
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, *(OJ L 255, 21.9.2016)*

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), *(OJ L 333, 27.12.2022)*
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), *(OJ L 333, 27.12.2022)*
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, *(COM/2022/454 final, 15 September 2022)*
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), *(OJ L 274, 30.7.2021)*
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, *(COM (2020) 607 final, Brussels, 24 July 2020)*
D3-16	Internet Organised Crime Threat Assessment (IOCTA) 2020
D3-17	Internet Organised Crime Threat Assement (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 *(OJ L 335/; 17.12.2011*)
D3-21	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems *(OJ L 69/67; 16.3.2005*)
D3-22	Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography (*OJ L 13/44; 20.1.2004*)
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.I.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 *(COM/2023/424 final, 12 July 2023)*

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 *(SWD/2022/0179 final, 28 June 2022)*
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 *(COM/2022/105 final, 8 March 2022)*
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 *(COM/2020/188 final, 11 May 2020)*
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 (*OJ L 348/130, 24.12.2008, P. 130*)

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 *(OJ L 148, 31.5.2022)*
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, *(OJ C 424, 7.11.2022)*
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, *(OJ L 169, 27.6.2022)*
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', Eucrim - 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, *(OJ L 134, 22 May 2023)*
G1-02	Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation, *(OJ L 158, 13 June 2022)*
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 *(COM/2021/170 final, 14 April 2022)*
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, *(COM/2021/784 final, 8 December 2021)*
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, *(SWD/2021/378 final, Brussels, 8.12.2021)*
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, *(COM(2020) 791 final, Brussels, 9 December 2020)*
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, *(OJ L 185, 12.7.2022)*

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*)