#DIGITALISATION AND #ARTIFICIALINTELLIGENCE IN CRIMINAL JUSTICE

Open source investigation tools (OSINT), digitalised files, videolinks in justice

Thessaloniki, 9-10 October 2025

FACE-TO-FACE

EXCELLENCE IN EUROPEAN LAW

Speakers

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

Anna Illamaa, Police and Border Guard Board, North Prefecture; Serious Crime Unit, Digital evidence group Special investigator, Tallinn

Julija Kalpokienė, Attorney at Law; Junior Researcher, Vytautas Magnus University, Kaunas

Sabina Klaneček, Counsellor, Supreme State Prosecutor`s Office, Ljubljana

Lilija Mažeikienė, Investigations Manager, EMEA, Binance, The Hague

Joachim Meese, Professor, Criminal Law and Procedure, University of Antwerp; Attorney, Bar of Ghent

Michael Rothärmel, Head of Unit, Fight against Terrorism and Extremism, Bavarian State Ministry, Munich

Bilal Sen, Corporate Investigations and Cybercrime Advisor, 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
- e-Evidence Digital Exchange System (e-EDES)
- Videoconferencing
- Artificial Intelligence (AI)

Language
English

Event number
325DT08

Organiser
ERA (Laviero Buono) in cooperation with the Hellenic School of Judges

Co-financed by the European Union

ΕΣΔΙ
NATIONAL SCHOOL OF THE JUDICIARY

european.law

#DIGITALISATION AND #AI IN CRIMINAL JUSTICE

Thursday, 9 October 2025

09:00 Arrival and registration of participants

09:30 **Welcome and introduction to the programme**
NN Hellenic School of Judges & Laviero Buono

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

Chair: Laviero Buono

09:35 **Open-source tools and computer forensics**
- 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

Bilal Sen

10:45 Discussion

11:00 Break

11:30 **Fighting 2.0 crimes with Web 3.0 possibilities**
- Crypto 101: technology, definitions and more
- (Ab)use of crypto
- Blockchain explorers: understanding transactions, following the money
- Different crypto services: what data to expect?

Lilija Mažeikienė

12:15 Discussion

12:30 Lunch

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

Chair: Bilal Sen

13:30 **Data retention – data protection vs. the risk of systematic impunity**
- Significance of data retention for the investigation and prosecution of crimes committed online and offline
- Jurisprudence of the CJEU
- State of play of legislation on EU and national level

Michael Rothärmel

14:00 Discussion

14:15 **E-evidence in criminal cases: the SkyECC saga**
Joachim Meese

14:45 Discussion

15:00 Break

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 to #digitalisation and #artificialintelligence". It consists of 12 seminars to take place in various EU cities over the period 2024-2027.

Who should attend?

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

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

Venue

National School of Judges
Ikaron str, PC 55102
Kalamaria, Thessaloniki
Greece

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 **8 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.

PART III: VIDEOCONFERENCING AND ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

15:30 **Artificial intelligence and the challenges ahead for legal practitioners**
Joachim Meese

16:00 Discussion

16:30 End of first day

19:30 Dinner offered by the organisers

Friday, 10 October 2025

Chair: Joachim Meese

09:30 **Videoconferencing in the era of artificial intelligence**
- Key success factors for transnational use of videoconferencing in judicial procedures in the EU
- Simplification (or possible complication) in criminal procedures and trials

Sabina Klaneček

10:15 Discussion

10:30 **The nexus between artificial intelligence and digital investigations**
Anna Illamaa

11:00 Discussion

11:15 Break

Chair: Michael Rothärmel

11:45 **"Seeing is believing" no longer stands: deepfake technologies and the evaluation of evidence**
Julija Kalpokienė

12:30 Discussion

12:45 End of seminar and light lunch

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

Apply online for
"#DIGITALISATION AND #ARTIFICIALINTELLIGENCE IN CRIMINAL JUSTICE":

www.era.int/?133190&en

Your contacts

Laviero Buono
Head of Criminal Law Section

Christina Laux
Assistant
Tel.: +49(0)651 93737-324
E-Mail: CLaux@era.int

This programme has been financed by the European Union

Application

#DIGITALISATION AND #ARTIFICIALINTELLIGENCE IN CRIMINAL JUSTICE

Thessaloniki, 9-10 October 2025 / Event number: 325DT08

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, Kosovo* 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).*

   The number of places available is limited (30 places). Participation will be subject to a selection procedure. Selection will be first come first served and according to nationality.

2. Applications should be submitted before **10 June 2025.**
3. A response will be sent to every applicant after this deadline. **We advise you not to book any travel or hotel before you receive our confirmation**.

Registration Fee

4. €135 including documentation, lunches and dinner.

Travel and Accommodation Expenses

5. Participants will receive a fixed contribution towards their travel and accommodation expenses and are asked to book their own travel and accommodation. The condition for payment of this contribution is to sign all attendance sheets at the event. No supporting documents are needed. 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 and accommodation costs.
6. Travel costs from outside Greece: participants can calculate the contribution to which they will be entitled on the European Commission website, Table 2 (https://era-comm.eu/go/calculator). The distance should be calculated from their place of work to the seminar location, *(in case of Bulgarian participants the amounts for Inter-Member States return journeys between 50 and 400 km is fixed at € 37, please consult p.11 on https://era-comm.eu/go/unit-cost-decision-travel).*
7. For those travelling within Greece, the contribution for travel is fixed at €36 (for a distance between 50km and 400km). Please note that no contribution will be paid for travel under 50km. For more information, please consult p.10 on https://era-comm.eu/go/unit-cost-decision-travel
8. Accommodation costs: international participants travelling more than 50km one-way will receive a fixed contribution of €107 per night for up to two nights' accommodation. National participants travelling more than 50km one way will receive a fixed contribution of €107 per night for max one night accommodation. For more information, please consult p.13 on https://era-comm.eu/go/unit-cost-decision-travel.
9. These rules do not apply to representatives of EU Institutions and Agencies who are required to cover their own travel and accommodation.
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 or doesn't attend both days of the event.

Participation

11. Participation in 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 #ARTIFICIALINTELLIGENCE IN CRIMINAL JUSTICE":

Venue

National School of Judges
Ikaron str,
55102 Kalamaria, Thessaloniki
GREECE

Language

English

Contact

Christina Laux
Assistant
Tel.: +49(0)651 9 37 37 324
E-Mail: CLaux@era.int

EMAS
VERIFIED ENVIRONMENTAL MANAGEMENT
DE-176-00031

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)**	

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*)

AI Forensics: Tool and Target of Investigation

The nexus between AI and digital investigation

Anna ILLAMAA, 2025

Introduction

- Definition of AI forensics
- Two perspectives:
    1. AI as a tool for investigation
    2. AI as an object of investigation
- Importance in policing, cybersecurity, law

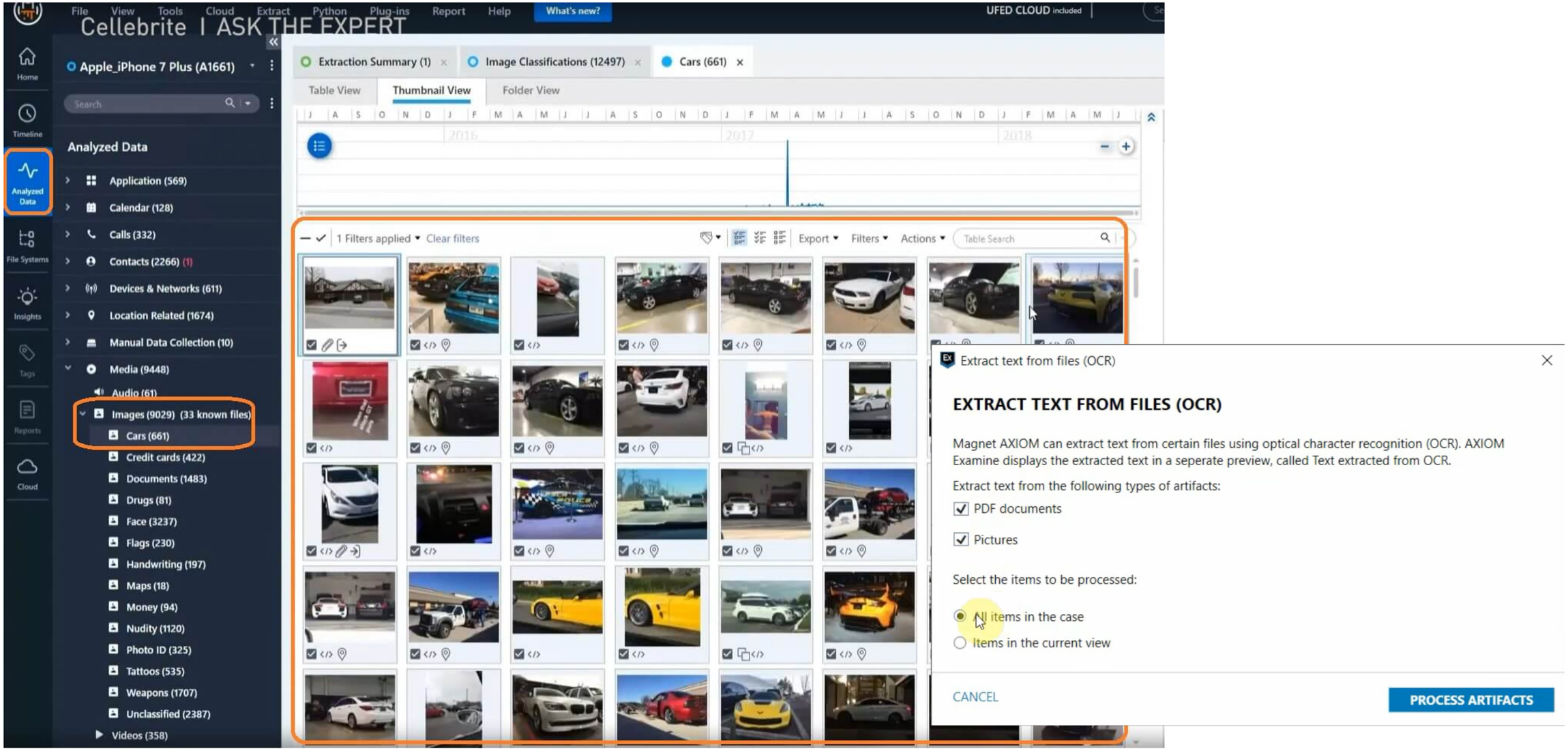
AI refers to systems that display intelligent behaviour by analysing their environment and taking action – with some degree of autonomy – to achieve specific goals.

/EPRS | European Parliamentary Research Service/

How AI is Enhancing Digital Forensics

- Applications:
- - Image/video enhancement
- - Pattern recognition
- - Predictive analytics
- Benefits: faster, more accurate
- Challenges: data quality, bias

Enhanced Image and Video Analysis



https://cellebrite.com/

https://www.magnetforensics.com

AI as a Challenge—New Forms of Digital Evidence

AI-Generated Content and Deepfakes
This is where AI becomes your adversary.

Deepfake audio and video that can convincingly impersonate anyone. Video evidence that appears authentic but is completely fabricated.

AI-generated documents that mimic writing styles perfectly. Imagine a forged email that matches someone's communication patterns so well that traditional authentication methods fail.

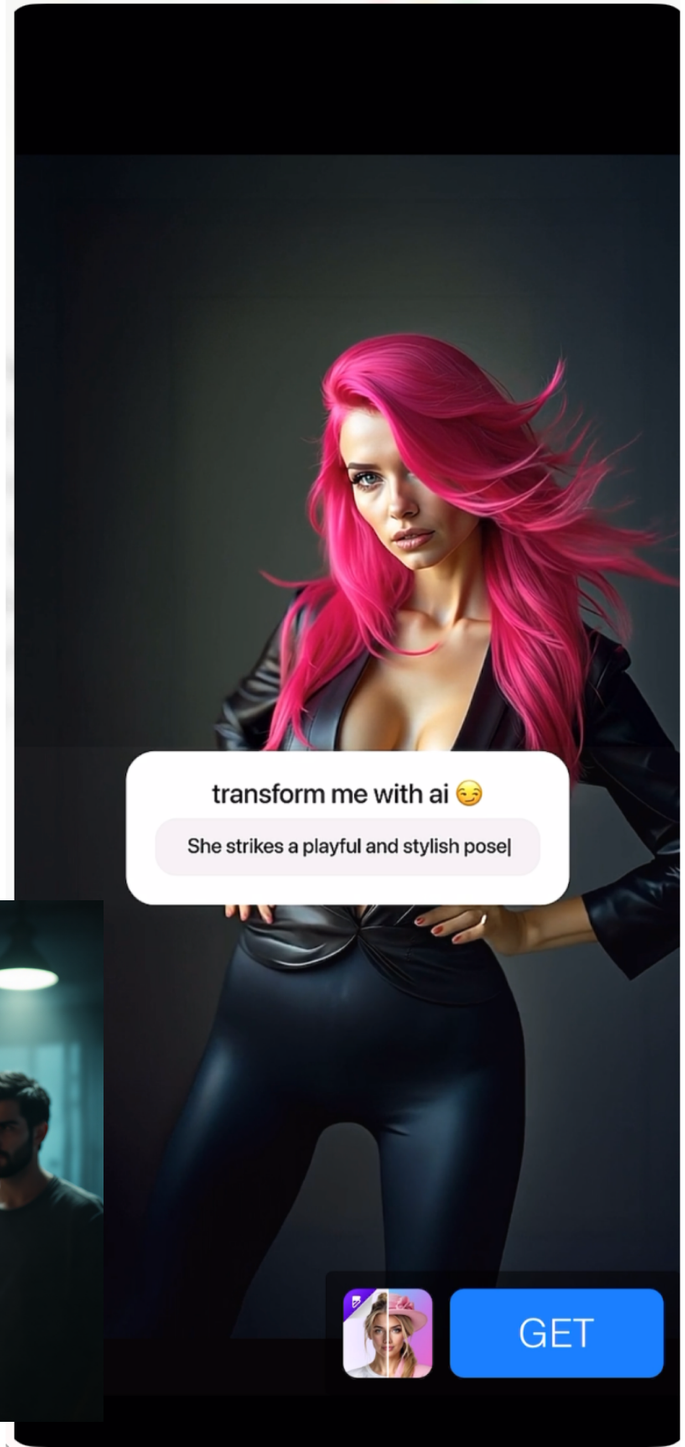
Synthetic identities created by AI for fraud, combining real and fake information in ways that pass conventional verification.

Legal implications for you: The authenticity of digital evidence can no longer be assumed. You must ask: Was this content created by a human or AI? Has it been manipulated? What technical analysis was performed to verify it?

AI: Crime Deepfake

A man had violently assaulted his wife after receiving **explicit images** that appeared to show her with another man. The husband claimed he'd received these images from his wife's ex-boyfriend via messaging app and believed they proved infidelity.

The wife maintained the images were fake—that she had never been in those situations.



AI: crime usage

The technology left fingerprints:

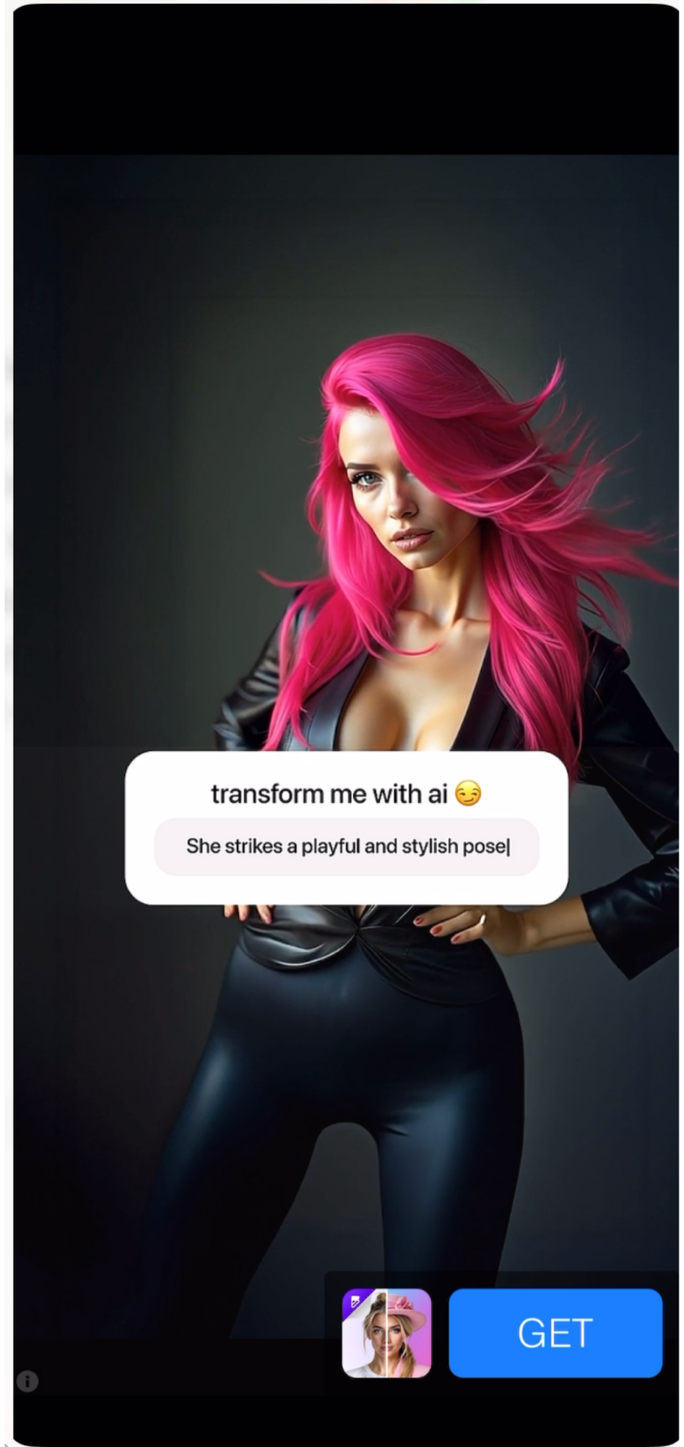
1.Lighting inconsistencies – photo zooming, the face was lit from one direction while the body was lit from another—physically impossible in a single photo.

2. Skin tone mismatches - The facial skin tone didn't precisely match the body, a subtle discrepancy invisible at normal viewing distance.

3. Edge artifacts - There was subtle blurring around the hairline and face boundaries where the AI tried to blend the face onto the body.

4. Digital noise patterns - The noise in the facial area differed from the rest of the image—a telltale sign of manipulation. Error Level Analysis (ELA) which revealed different compression levels between the face and body.

5. Metadata - The EXIF data showed the image was created with photo editing software, not captured by a camera.



AI: crime usage

Seized ex-boyfriend's laptop:

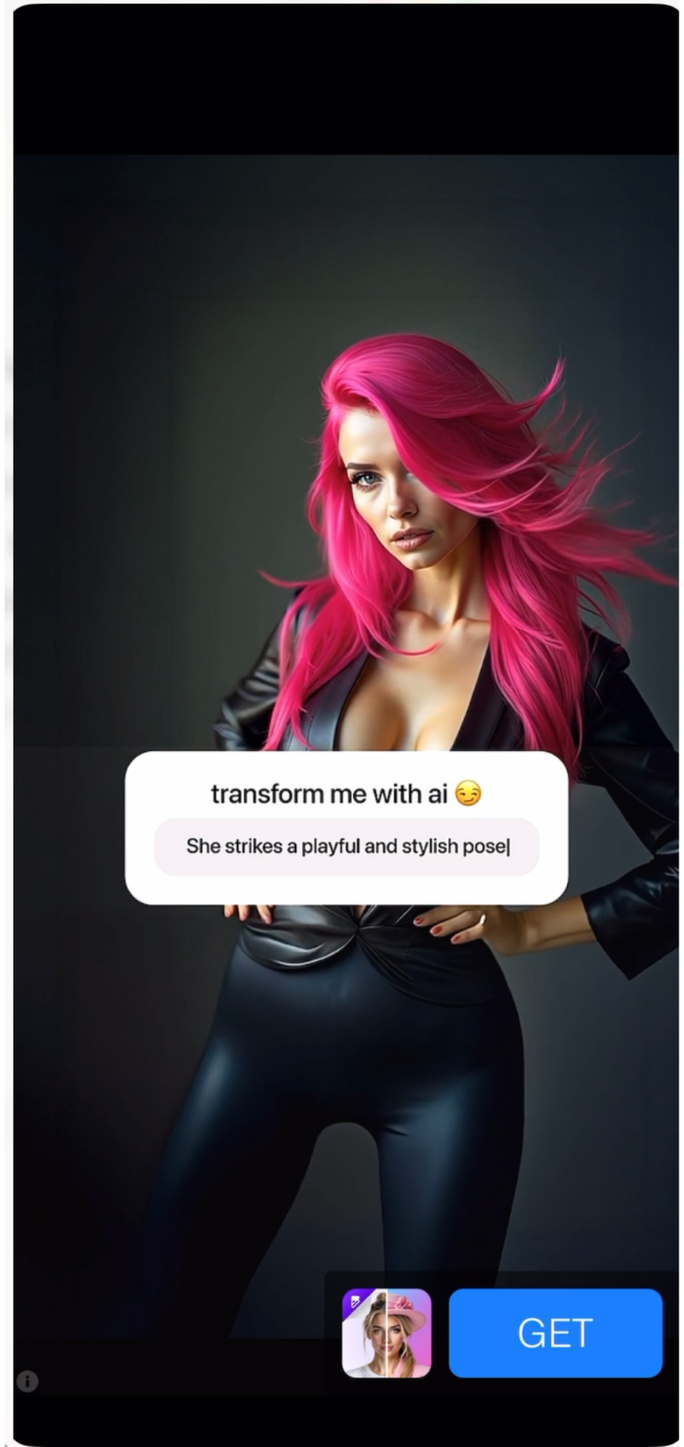
- **The deepfake software**

- **The victim’s source photos** - downloaded from the victim's social media profiles

- **Multiple draft versions** – few attempts showing his trial-and-error process perfecting the forgeries

- **Browser history** - searches for "how to create deepfakes" and tutorial videos

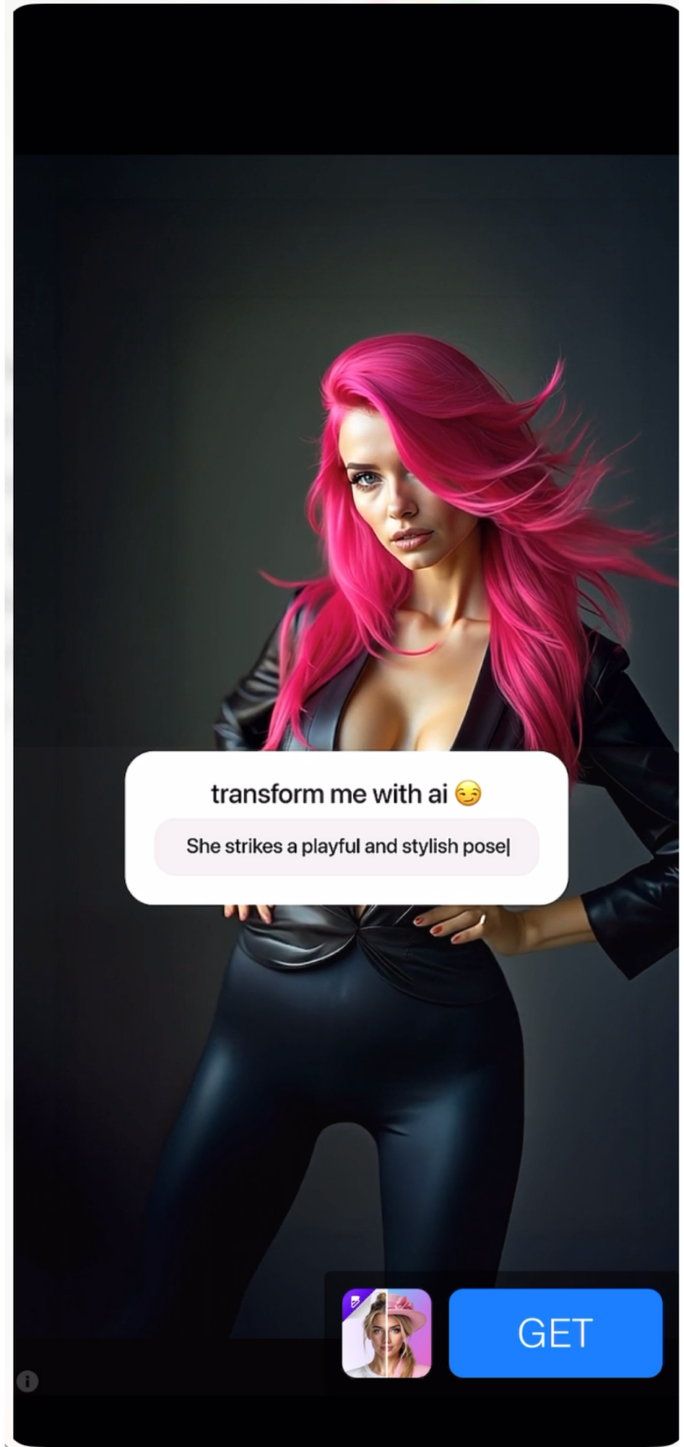
- **Final versions** - images he sent to the husband



AI: crime usage. Why This Case Matters

- How do you prove images are fake beyond reasonable doubt?
- What expert testimony is needed?
- How do you explain deepfake technology to a jury who might not even know what AI is?

Deepfakes have moved from Hollywood special effects to criminal tools accessible to anyone with a computer and malicious intent. They're convincing enough to fool ordinary people and potentially fool courts—unless we have the forensic expertise to detect and prove the manipulation.



Testing

Testing

Testing

Testing

```
ExifTool Version Number         : 12.76
File Name                       : IMG_2254.heic
Directory                       : .
File Size                       : 1898 kB
File Modification Date/Time     : 2021:08:19 13:50:41+03:00
File Access Date/Time           : 2025:10:07 21:35:42+03:00
File Inode Change Date/Time     : 2025:10:07 21:35:29+03:00
......
File Type                       : HEIC
File Type Extension             : heic
MIME Type                       : image/heic
Major Brand                     : High Efficiency Image Format HEVC still image (.HEIC)
......
Make                            : Apple
Camera Model Name               : iPhone XS Max
......
Software                        : 14.7.1
Modify Date                     : 2021:08:19 12:50:34
Host Computer                   : iPhone XS Max
.......
XMP Toolkit                     : XMP Core 6.0.0
Creator Tool                    : 14.7.1
Date Created                    : 2021:08:19 12:50:34
.......
Device Manufacturer             : Apple Computer Inc.
.......
Profile Copyright               : Copyright Apple Inc., 2017
.......
Create Date                     : 2021:08:19 12:50:34.627+02:00
Date/Time Original              : 2021:08:19 12:50:34.627+02:00
Modify Date                     : 2021:08:19 12:50:34+02:00
GPS Altitude                    : 33 m Above Sea Level
GPS Latitude                    : 48 deg [redacted] N
GPS Longitude                   : 2 deg [redacted] E
Circle Of Confusion             : 0.005 mm
Field Of View                   : 69.4 deg
Focal Length                    : 4.2 mm (35 mm equivalent: 26.0 mm)
GPS Position                    : 48 deg [redacted] N, 2 de[redacted]6" E
Hyperfocal Distance             : 2.04 m
Light Value                     : 13.5
Lens ID                         : iPhone XS Max back dual camera 4.25mm f/1.8
```

Testing

```
parallels@ubuntu-linux-2404:~/Desktop$ exiftool Snapshot2025100701.png
ExifTool Version Number         : 12.76
File Name                       : Snapshot2025100701.png
Directory                       : .
File Size                       : 412 kB
File Modification Date/Time     : 2025:10:07 20:29:08+03:00
File Access Date/Time           : 2025:10:07 21:19:58+03:00
File Inode Change Date/Time     : 2025:10:07 21:19:01+03:00
File Permissions                : -rwx------
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 540
Image Height                    : 720
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Pixels Per Unit X               : 2835
Pixels Per Unit Y               : 2835
Pixel Units                     : meters
Image Size                      : 540x720
Megapixels                      : 0.389
```

Testing

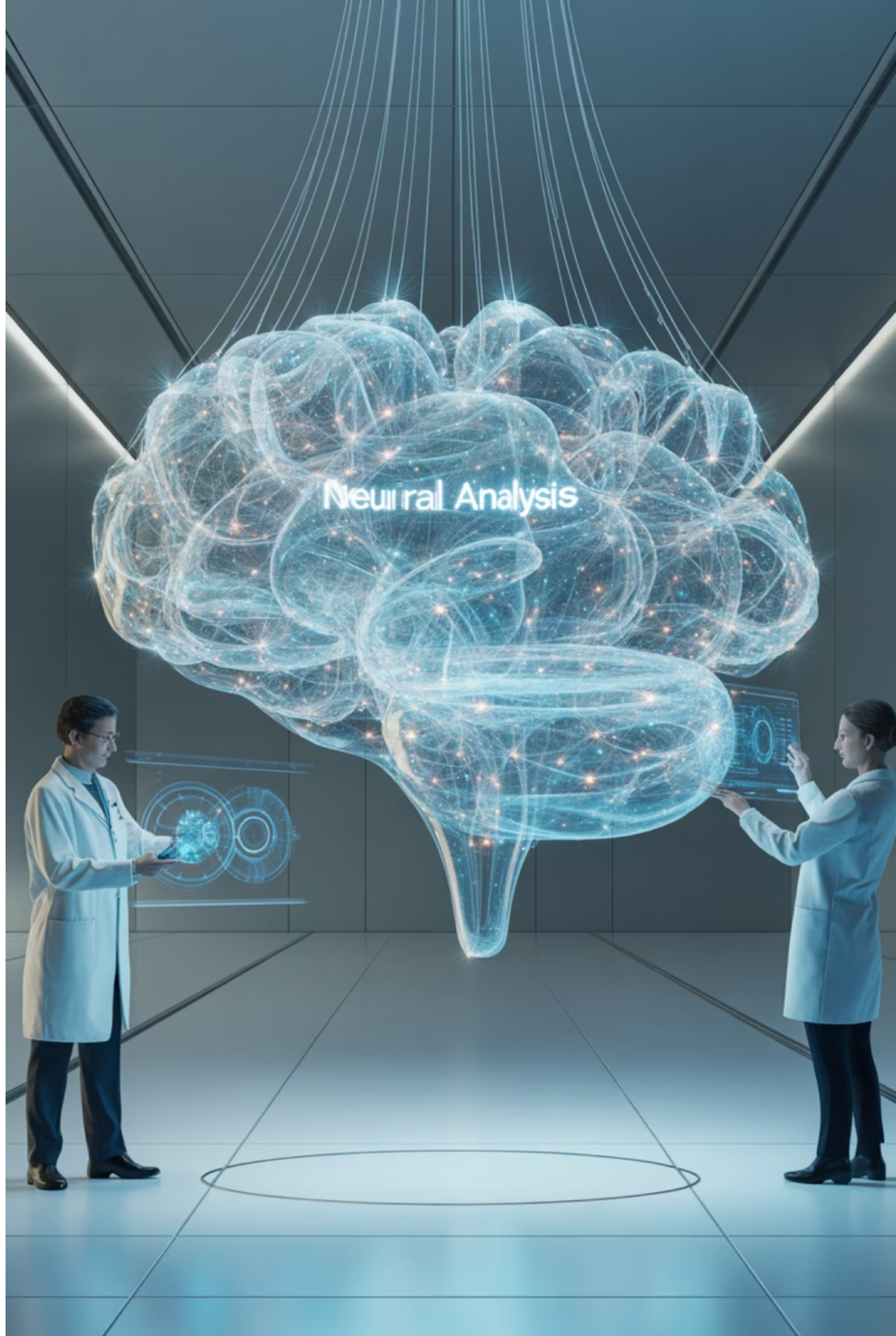
```
ExifTool Version Number         : 12.76
File Name                       : IMG_6294.JPG
....
File Size                       : 169 kB
File Modification Date/Time     : 2025:04:17 09:09:51+03:00
File Access Date/Time           : 2025:10:08 23:01:17+03:00
File Inode Change Date/Time     : 2025:10:07 21:24:37+03:00
....
Compression                     : JPEG (old-style)
....
Thumbnail Length                : 11312
XMP Toolkit                     : XMP Core 6.0.0
Digital Source Type             : http://cv.iptc.org/newscodes/digitalsourcetype/trainedAlgorithmicMedia
.....
Device Manufacturer             : Apple Computer Inc.
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Apple Computer Inc.
.....
Credit                          : Apple Image Playground
.....
Encoding Process                : Baseline DCT, Huffman coding
```

Testing

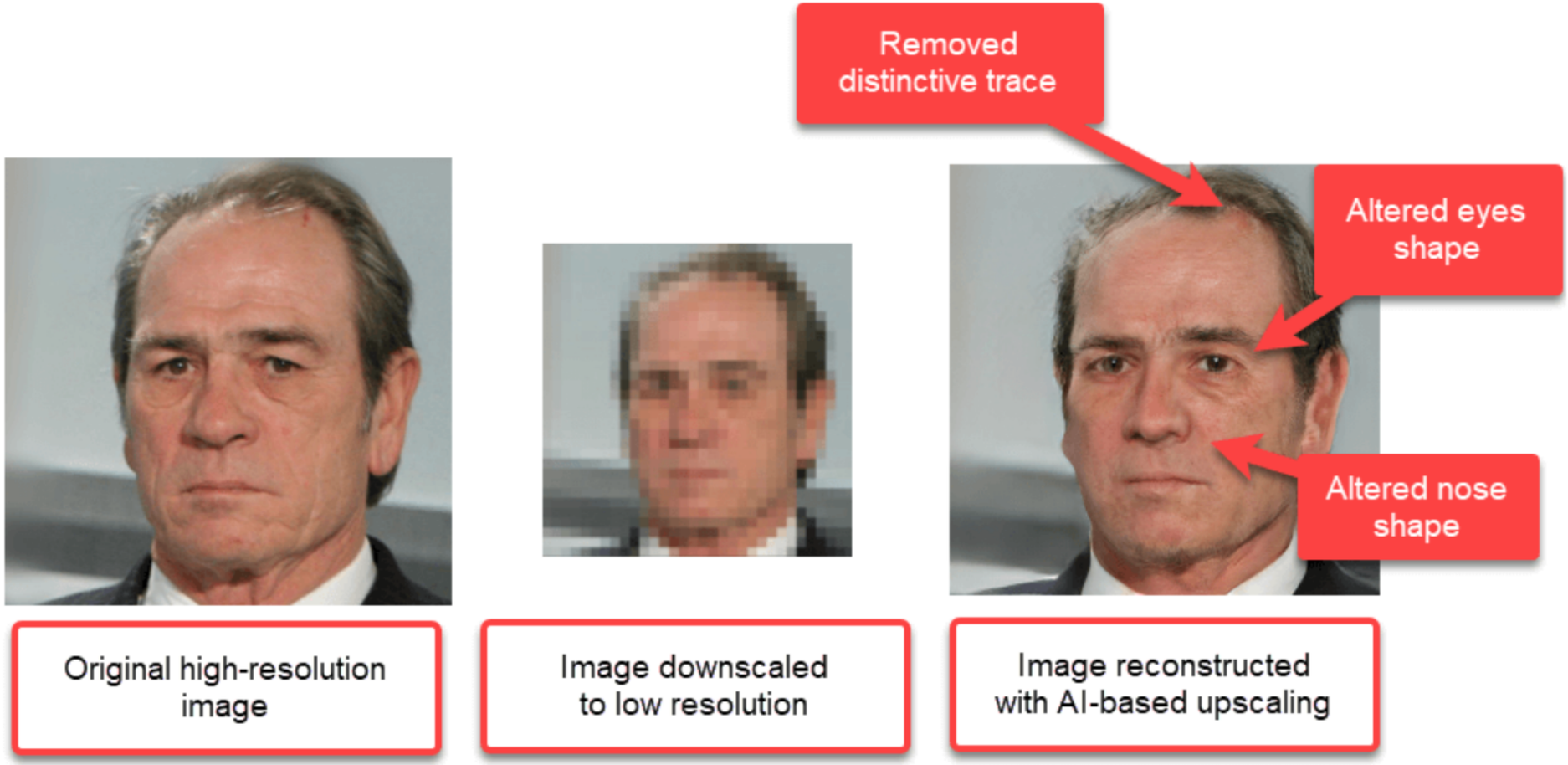
```
ExifTool Version Number         : 12.76
File Name                       : 1.png
Directory                       : /media/
File Size                       : 1048 kB
File Modification Date/Time     : 2025:10:09 00:21:19+03:00
File Access Date/Time           : 2025:10:09 00:25:16+03:00
File Inode Change Date/Time     : 2025:10:09 00:21:19+03:00
File Permissions                : -rwx------
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 864
Image Height                    : 1152
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : Ideogram AI
Modify Date                     : 2025:09:25 18:09:54
Date/Time Original              : 2025:09:25 18:09:54
Create Date                     : 2025:09:25 18:09:54
Image Size                      : 864x1152
Megapixels                      : 0.995
```

AI as a Tool for Investigation

- Can the AI explain HOW it reached its conclusion?
- What data was it trained on?
- Has it been tested for bias?
- Were alternative interpretations considered?
- “Black box”



Understanding the AI 'Brain'



Martino Jerian, CEO and Founder of Amped Software
https://blog.ampedsoftware.com/2024/10/23/how-does-the-ai-act-impact-image-and-video-forensics

Understanding the AI 'Brain'

Martino Jerian, CEO and Founder of Amped Software
https://blog.ampedsoftware.com/2024/10/23/how-does-the-ai-act-impact-image-and-video-forensics

- Biases?
- How it was trained?
- Can we use it as evidence?

Martino Jerian, CEO and Founder of Amped Software
https://blog.ampedsoftware.com/2024/10/23/how-does-the-ai-act-impact-image-and-video-forensics

Reliability in Investigation

- AI shows what it's trained to show
- Behavior based on training data
- Trust and accuracy depend on input quality

	Evidentiary Use 	Investigative Use 
AI-based Enhancement (image -> image) i.e. superresolution	**NO** - Not explainable - Bias from training data	**Yes (with safeguards)** - Disclosure (i.e. not for evidence label) - Education about risks
AI-based Analysis (image -> decision) i.e. face recognition	**Yes (with safeguards)** - Only for decision support - Known reliability - User bias mitigation	**Yes (with safeguards)** - Only for decision support - Known reliability - User bias mitigation

Martino Jerian, CEO and Founder of Amped Software
https://blog.ampedsoftware.com/2024/10/23/how-does-the-ai-act-impact-image-and-video-forensics

Summary

- AI is both a tool and a target
- Accuracy and trust are key
- Laws like the AI Act are shaping the field

Thank you!

Q&A Session

- Open the floor for discussion

Sources

- EPRS | European Parliamentary Research Service, Philip Boucher, 2020
- https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf
- AI Act, 2024, https://artificialintelligenceact.eu/the-act/
- https://cellebrite.com/
- https://www.magnetforensics.com
- *Martino Jerian, Amped Software,* https://blog.ampedsoftware.com/2024/10/23/how-does-the-ai-act-impact-image-and-video-forensics
- Marco Fontani, *Amped Software,* https://blog.ampedsoftware.com/2022/04/27/does-deep-learning-based-super-resolution-help-humans-with-face-recognition

Co-funded by
the European Union

CONINSEC
CONSULTING INVESTIGATION SECURITY

Open Source Tools and Computer Forensics

Bilal Şen

Corporate Investigations and
Cybercrime Advisor

- Cybercrime Centre – Turkish National Police - GOV
- Global Cybercrime Program – UNODC - IO
- Senior Consultant – Industry

- Led tech investigations
- Crafted policies
- Delivered sessions across five continents
- Consulted for international organisations and governments
- Helping businesses, law firms, and more

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 can strengthen your legal practice, uncover the truth, help you win cases.

COMMON OSINT USAGE

It is not hacking

It is not invented by law enforcement

It is not always ‘free’

It is not just the internet

It is not something the Subject/s cant do

It is not as easy as we think it is

It is not only for justice and security

Publicly available? Maybe it was

May require verification

Evidence Collection

Investigation (Crime or Dispute)

Due Diligence (Company Accusation)

Competition (Commercial Intelligence)

Protection (Parents & Juveniles)

Reconnaissance (Hacking)

Pen Test (Cyber Security)

Research (Neighborhood Check)

Verification (CV Verification)

Defense (Military Monitor)

OSINT USAGE FOR LAW PRACTICIONERS

Litigation support: Finding key info on key case factors, opposing parties or witnesses, (social media, press, affiliations, timelines)

Asset tracing: Identifying global assets for collection and discovering hidden wealth, business interests, real estate, vehicles, offshore ties

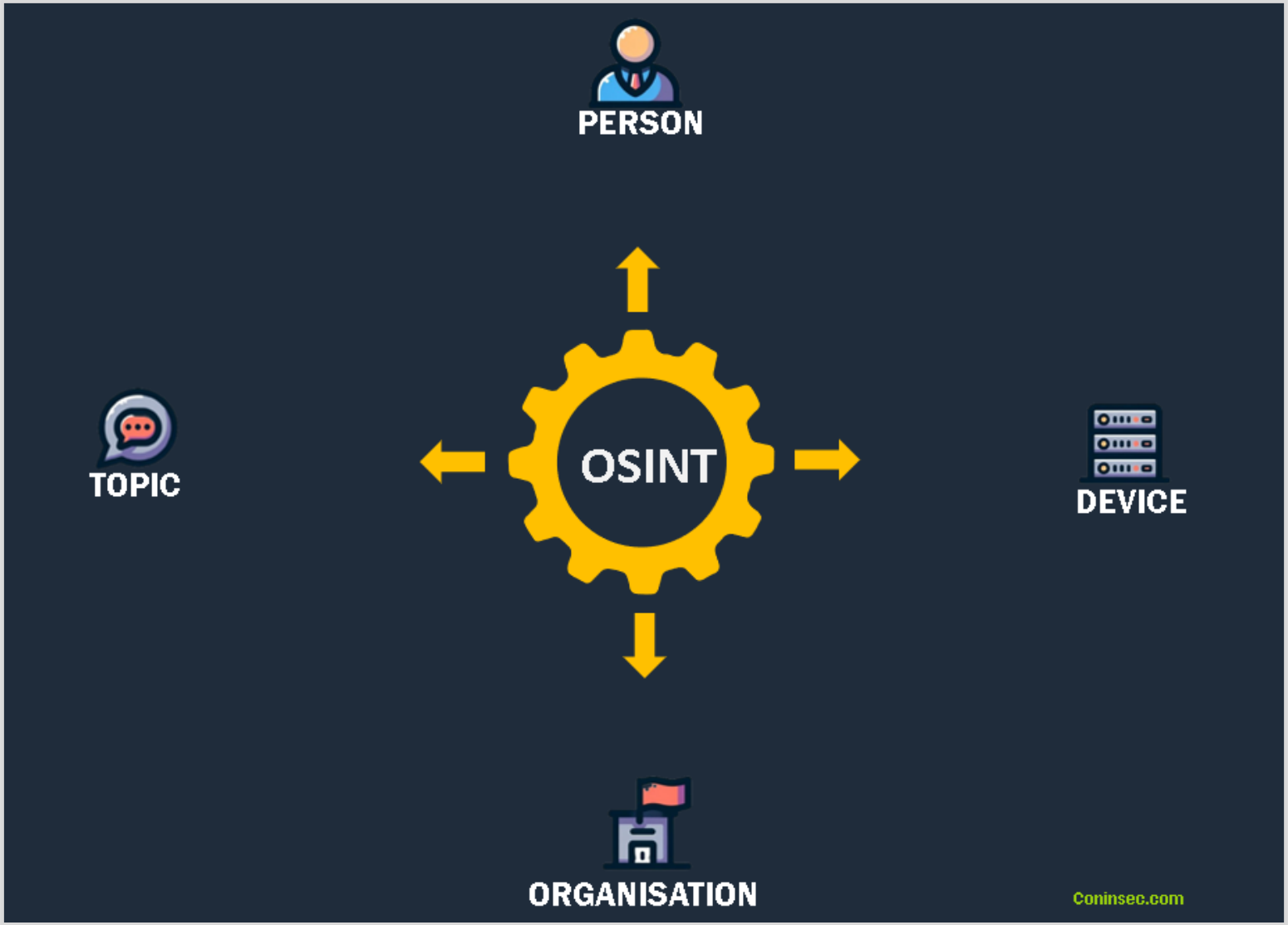
Fraud and forgery: Validating suspicious documents, shell companies, identities

Divorce & child custody : Standard of living, undisclosed relationships, locations

Commercial disputes: Competitor research, IP misuse, contract breaches

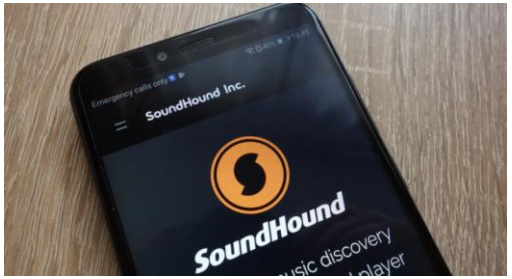
IP & brand protection: Counterfeit detection, web tracking, dark web monitoring

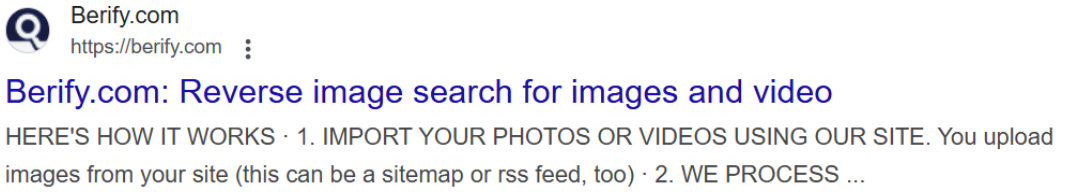
OSINT



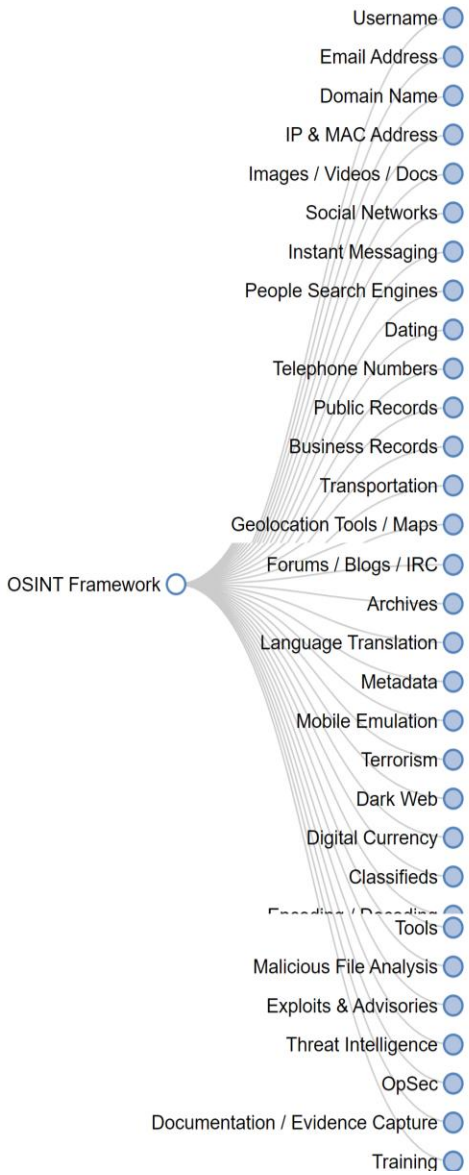
SEARCH POSSIBLE WITH

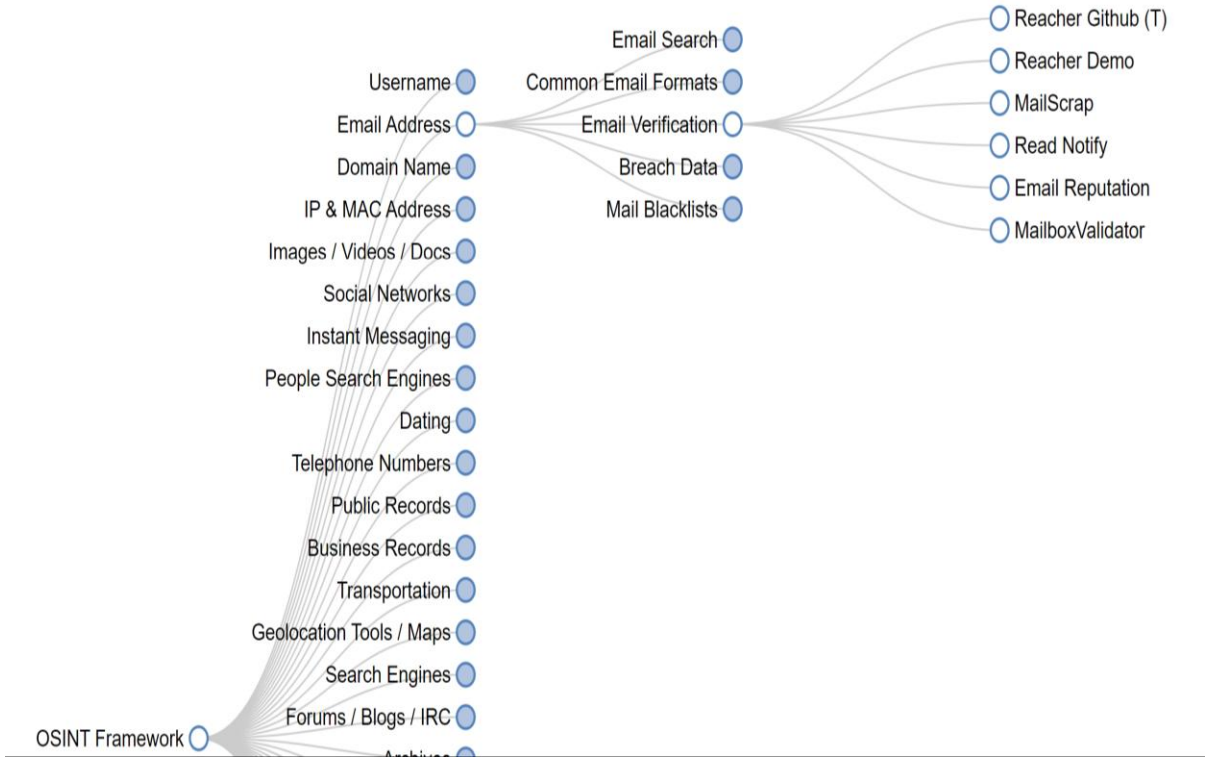
- Text
- Image
- Voice
- Video
- File
- Domain Name or URL





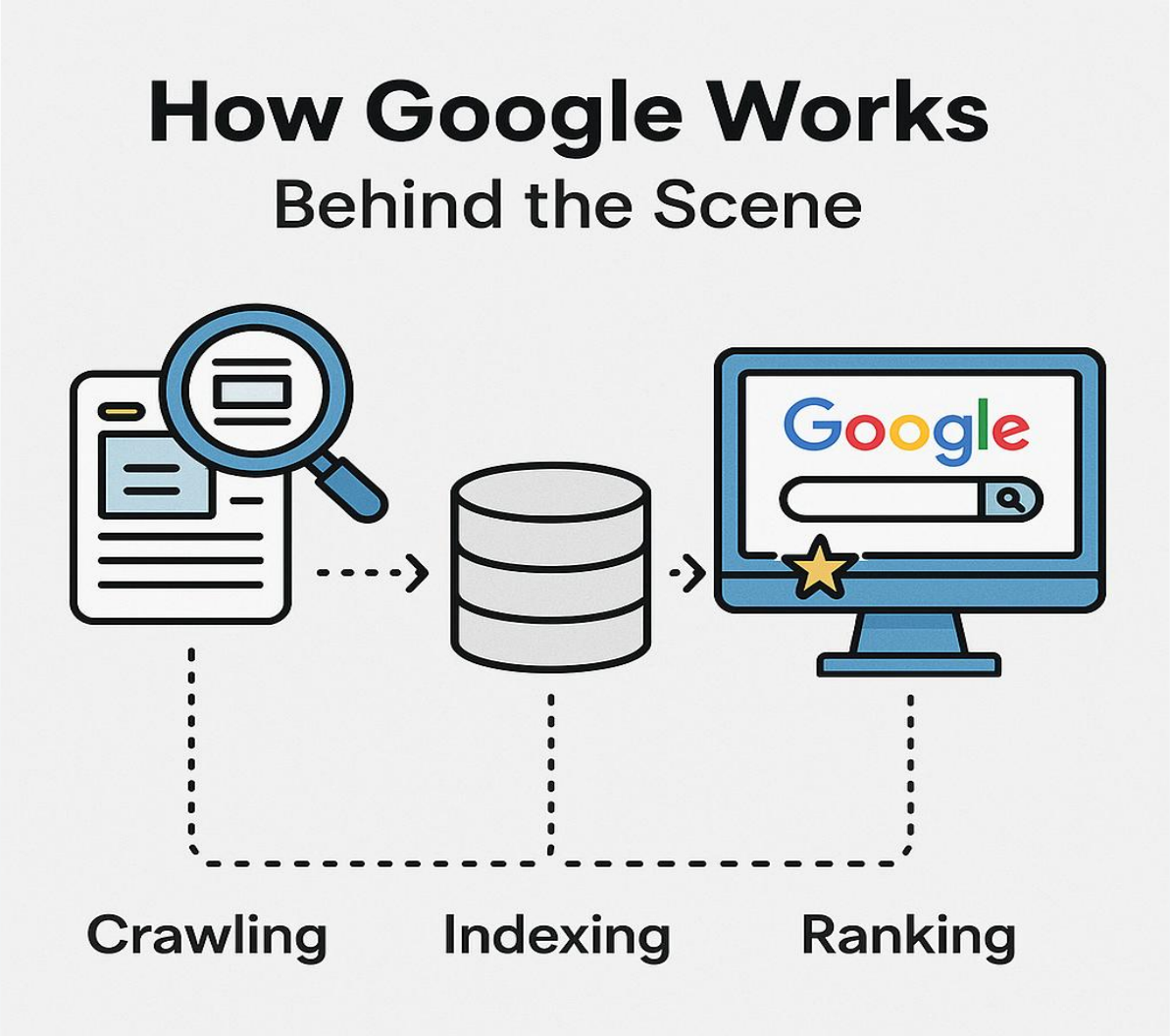
OSINT FRAMEWORK





osintframework.com

GOOGLE SEARCH PROCESS



GOOGLE LOCAL COPY SEARCH TEST

Search Engine Address	Search Term	Amount of Hits	With VPN Connection (Location CA, USA)
Google.de	bilal sen	14.6 M	13.9 M
Google.com.tr	bilal sen	27.7 M	8.8 M
Google.com	bilal sen	7.7 M	13.9 M
Google.com	bilal şen	11.7 M	

isearchfrom.com

I Search From

Google Search from a different location & device

With I Search From you can simulate using Google Search from a different location or device, or perform a search with custom search settings. It's useful for searching Google as if you were somewhere else, as well as for SEO & SEA testing.

Country: Greece

Language: English

Device: (Current)

your search Term

Search

More options

City: (N/A)

Find only pages from the specified country:

Find only pages in the specified language:

Logged in:

Personalized search:

Location:
Greece

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

WHO CREATES ONLINE INFO ABOUT US

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

SOME OF BREACH RECORDS

2016 : 117 M

April 2021 : 700 M

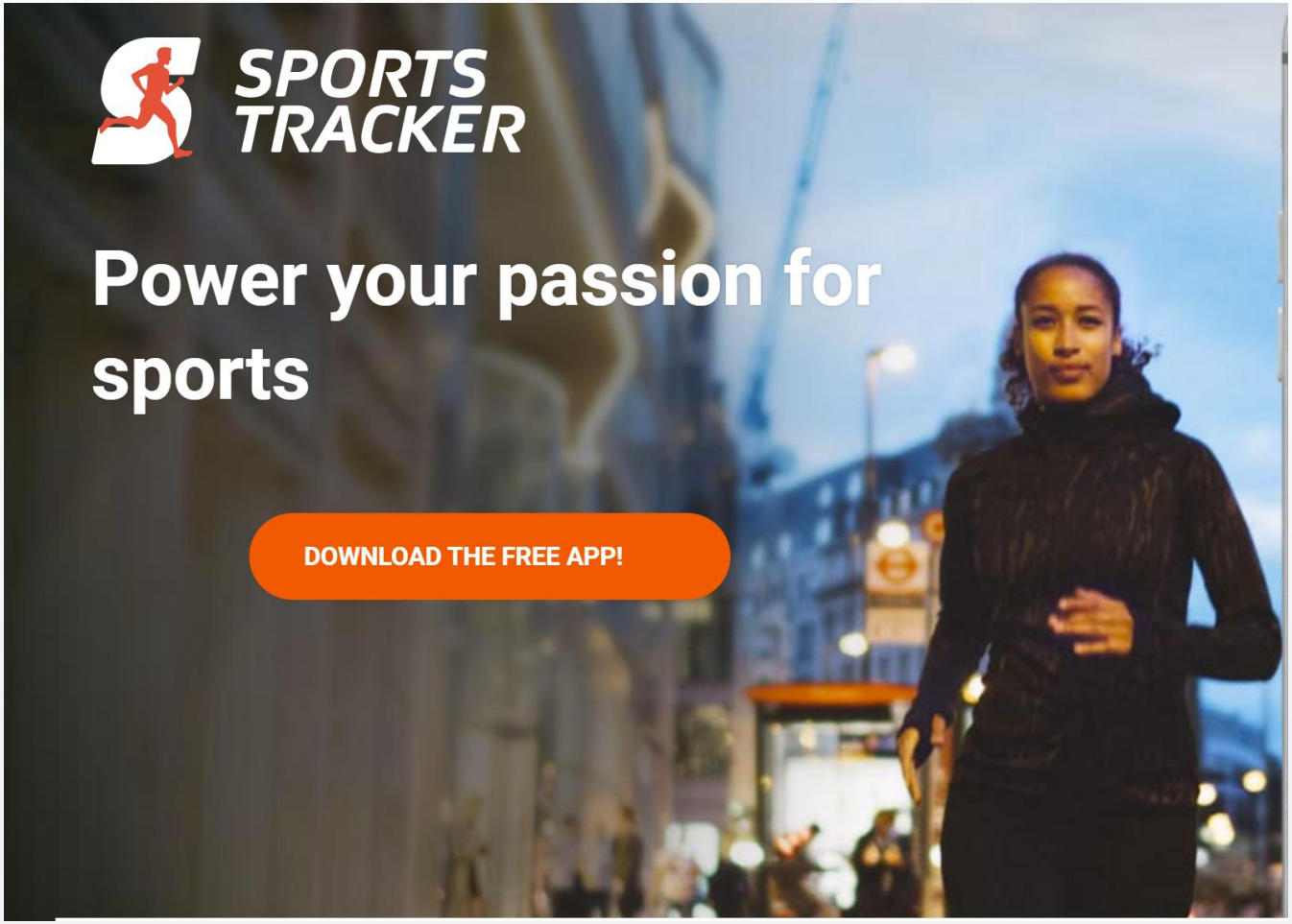
Feb 2023 : 500 M

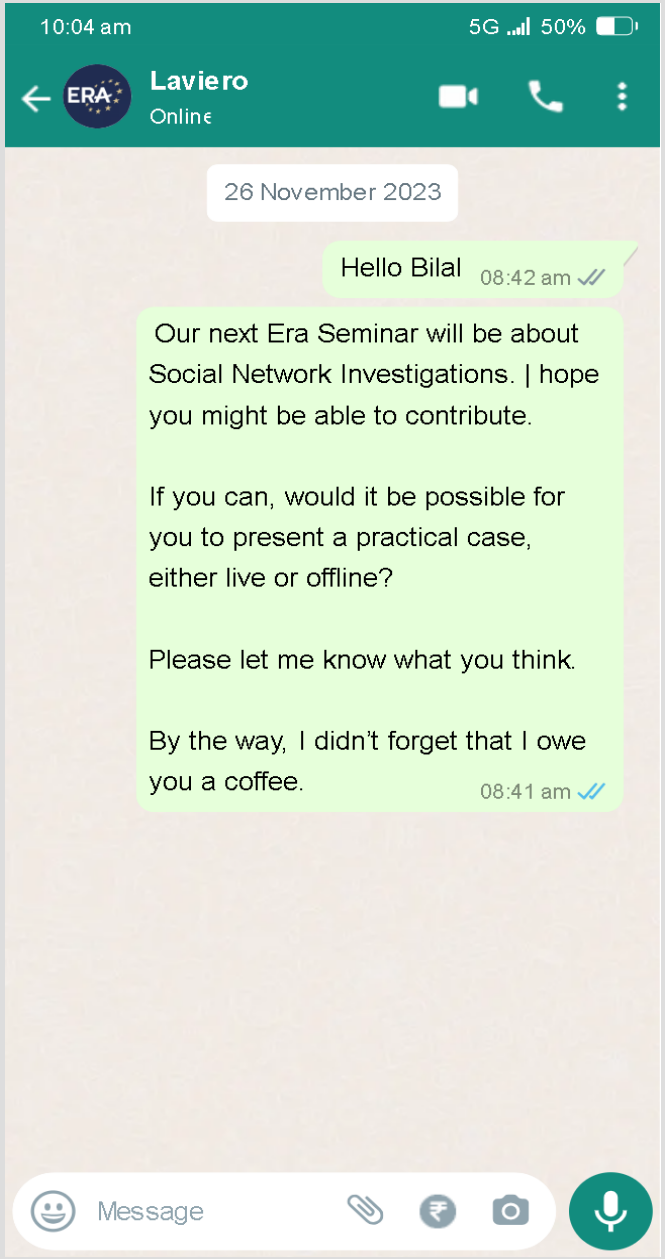
Sep 2019: 700 M

April 2021: 530 M

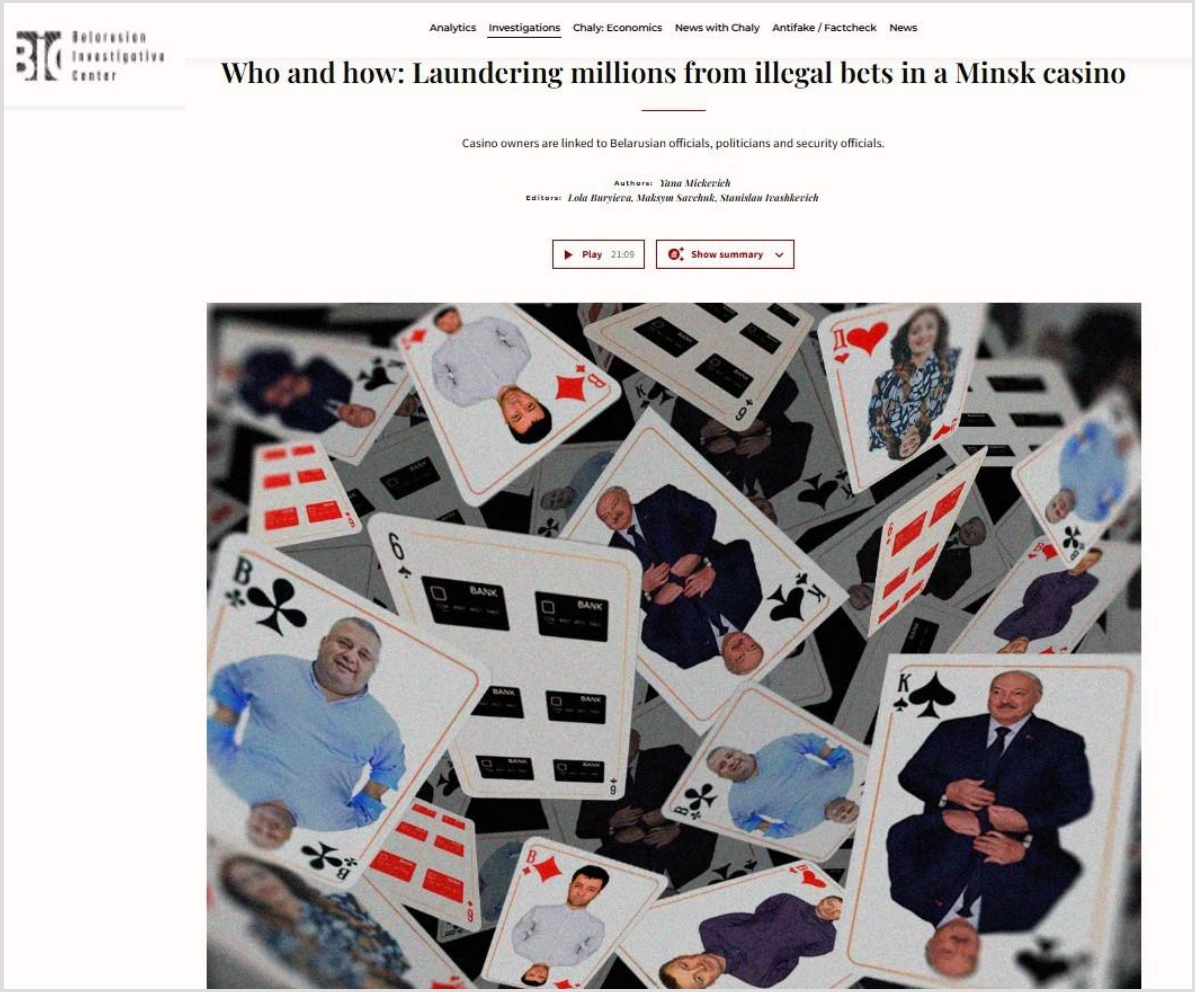
Jan 2021: Unknown

Jan 2023: 200 M


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


10:04 am
5G 50%
Laviero
Online
26 November 2023
Hello Bilal 08:42 am
Our next Era Seminar will be about Social Network Investigations. | hope you might be able to contribute.
If you can, would it be possible for you to present a practical case, either live or offline?
Please let me know what you think.
By the way, I didn't forget that I owe you a coffee. 08:41 am
Message

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*

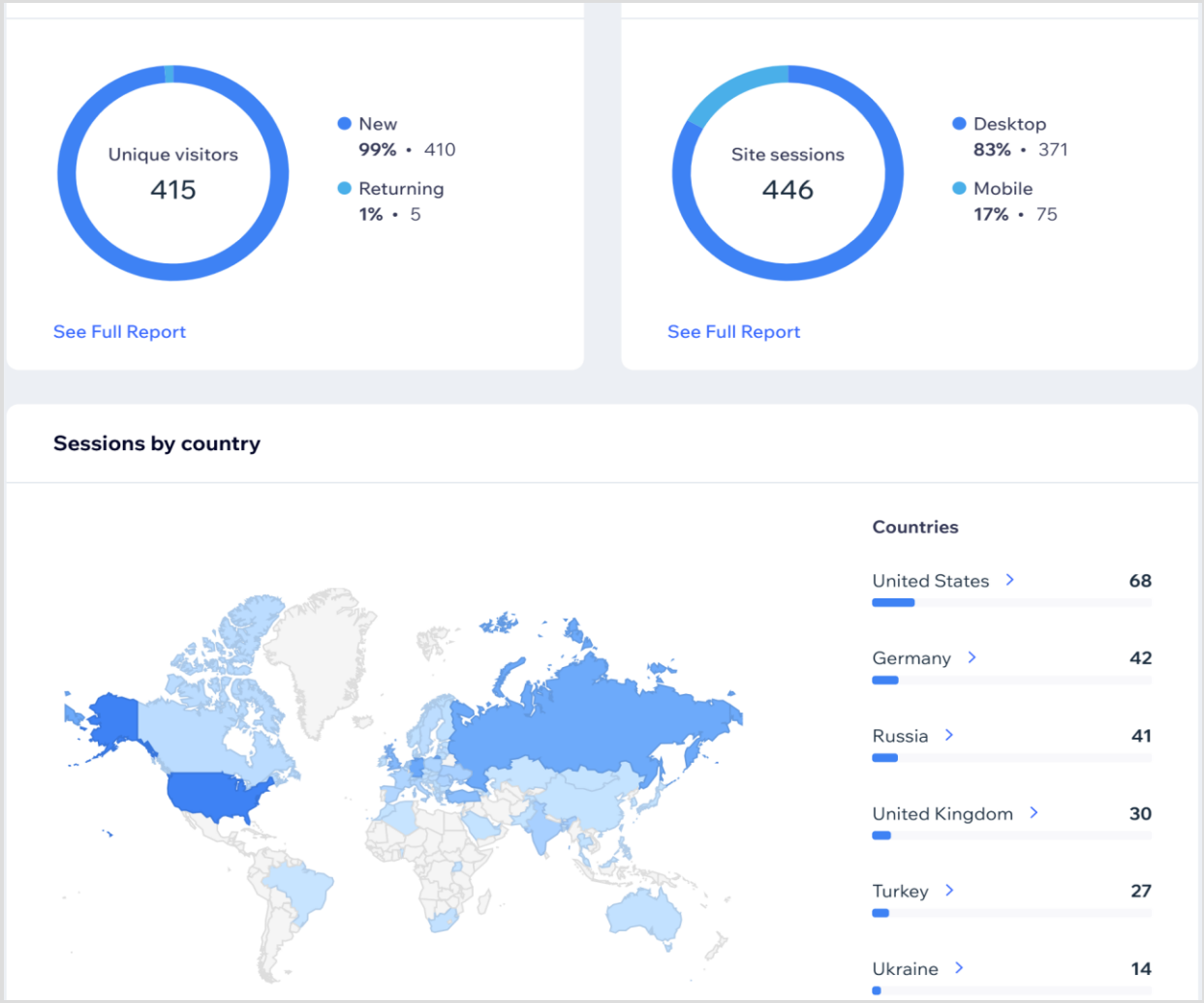
Play 21:09 Show summary

Belarusian Investigative Center

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

Belarusian Investigative Center

PROTECTING YOUR PRIVACY WHEN INVESTIGATING



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.

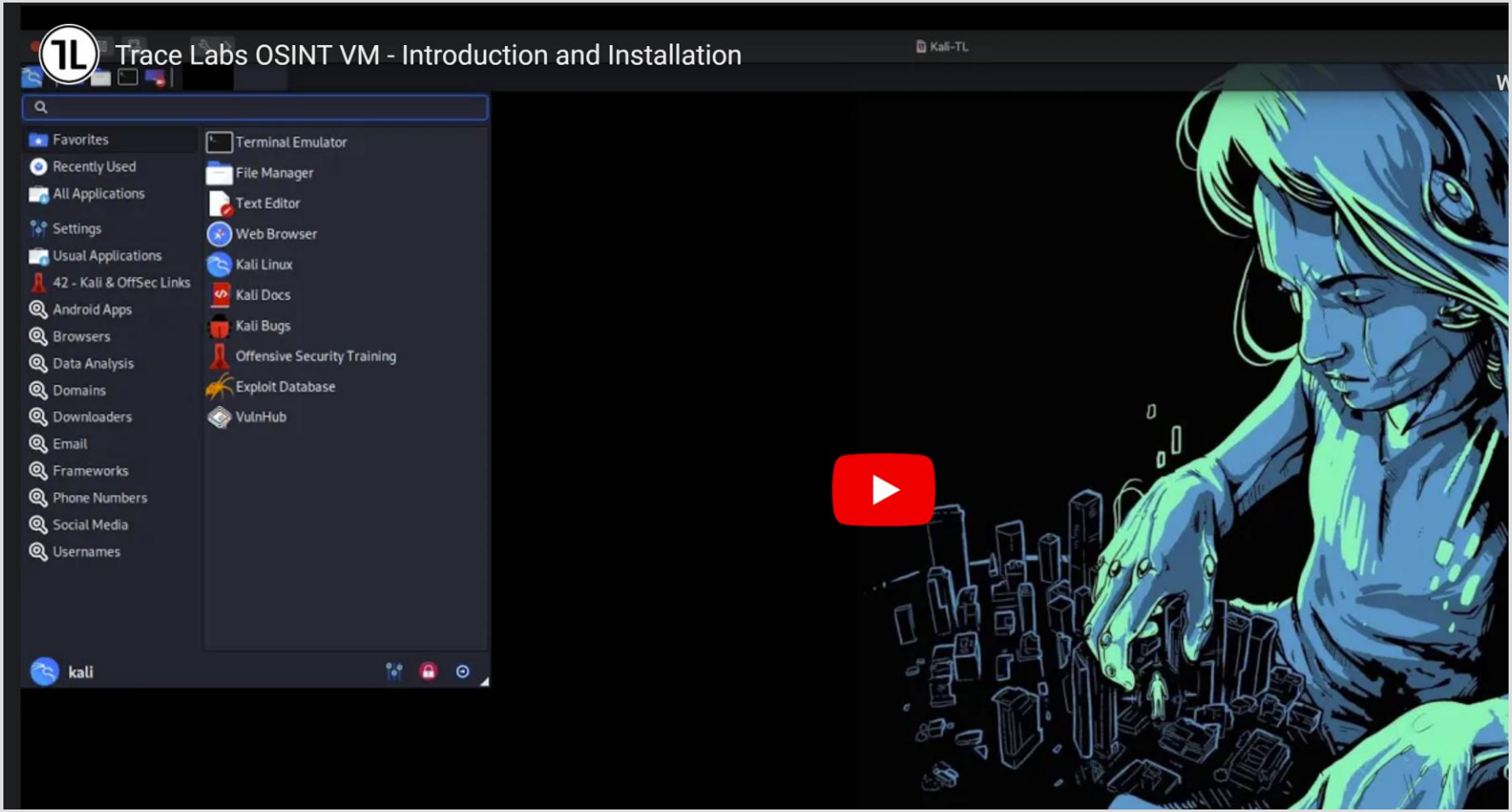
Extension: User Agent Changer

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

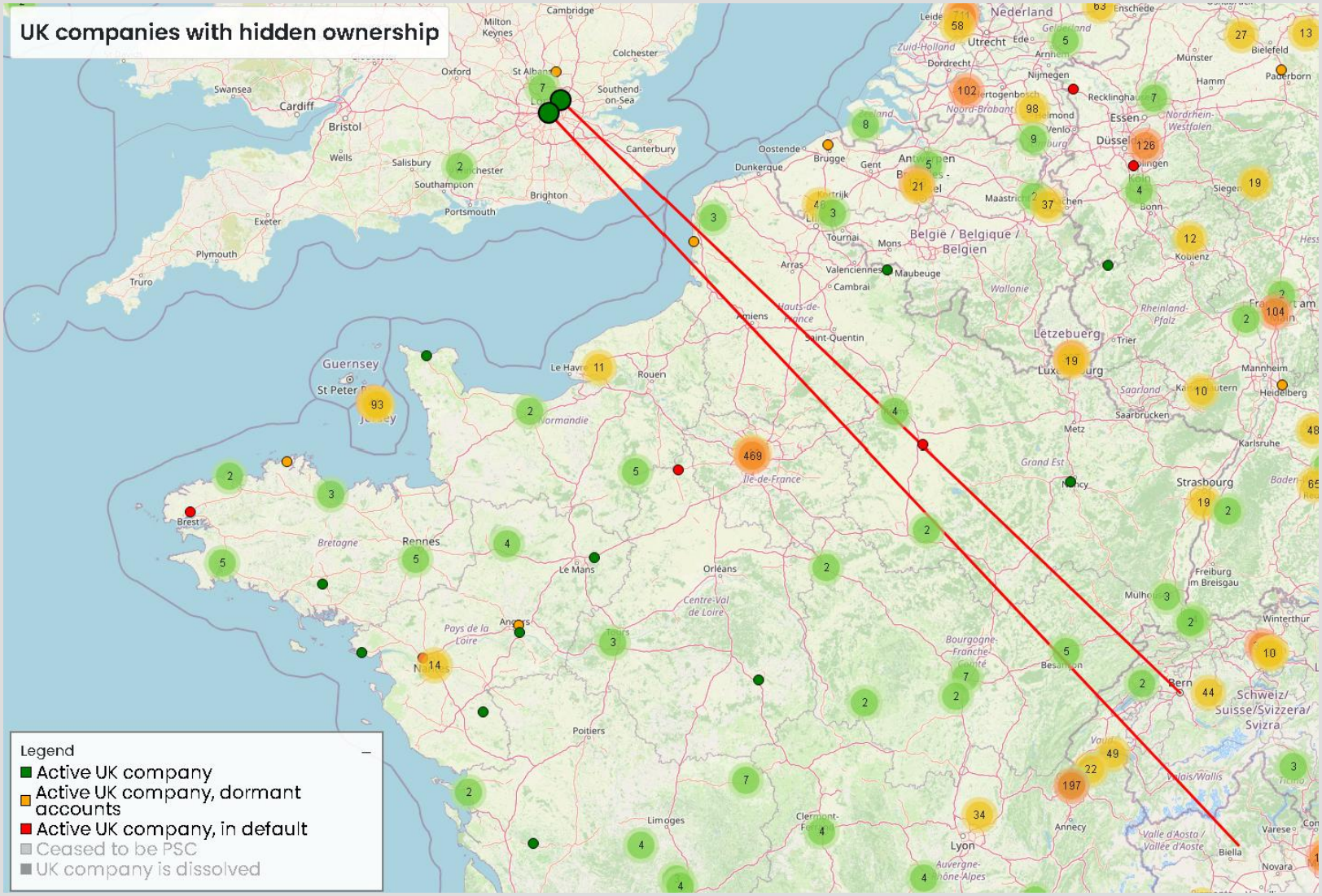
Check Only Through Verified Sources

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

OPERATION SECURITY



HIDDEN BUSINESS OWNERSHIP



ALERT MANAGEMENT

Search alerts are created and managed through an automated process that passively gathers timely and updated information

www.talkwalker.com/alerts

www.google.com/alerts

Site:de “Bilal Sen” OR “Bilal Schen” -Bauingenieurswesens –Gewürze

-(Civil engineering) -Spices

ONLINE DATA IS VOLATILE

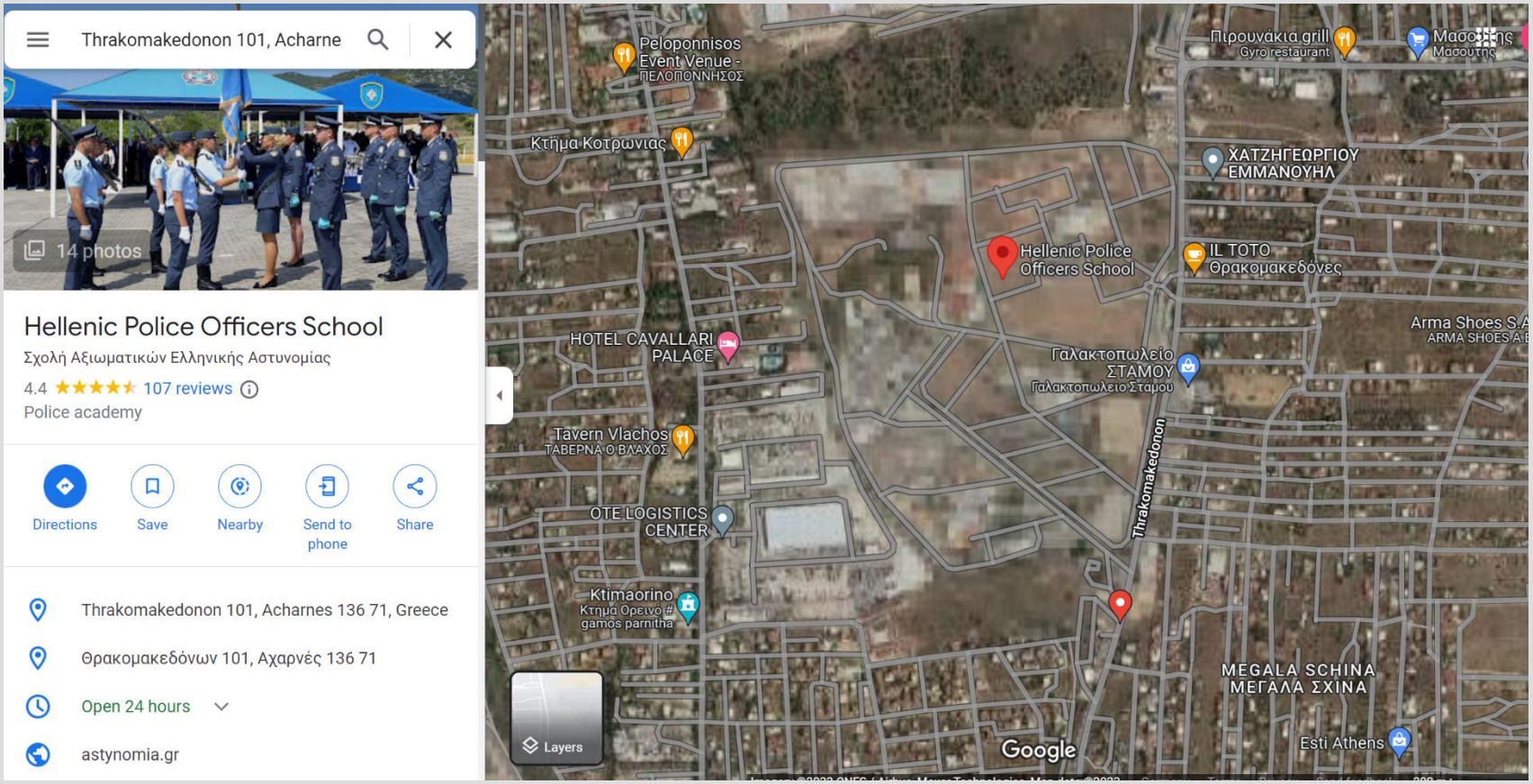
Archive

URL Collection

Freezing The Time

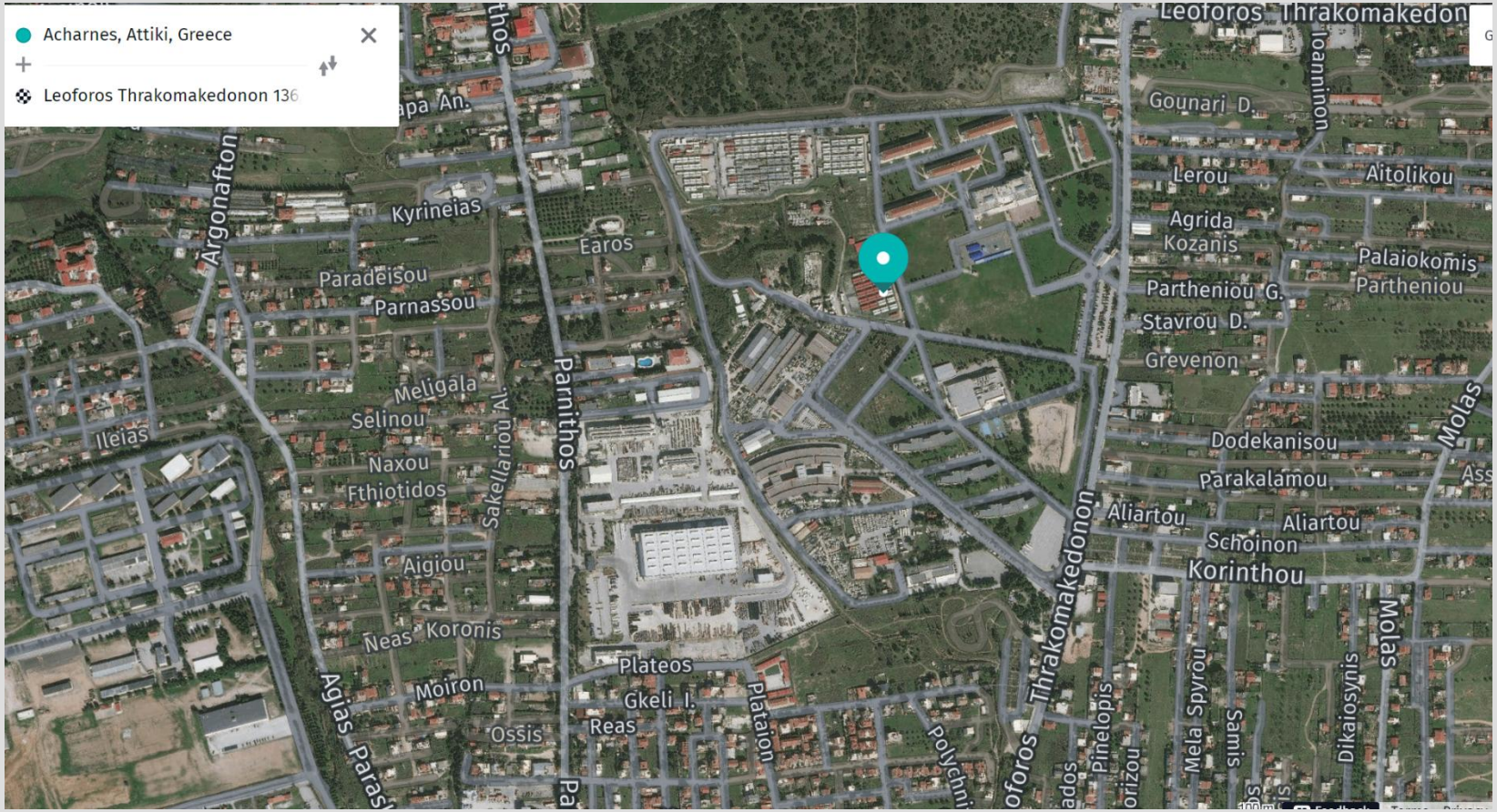
ALTERNATIVE COULD BE BETTER

GOOGLE MAP RESULTS

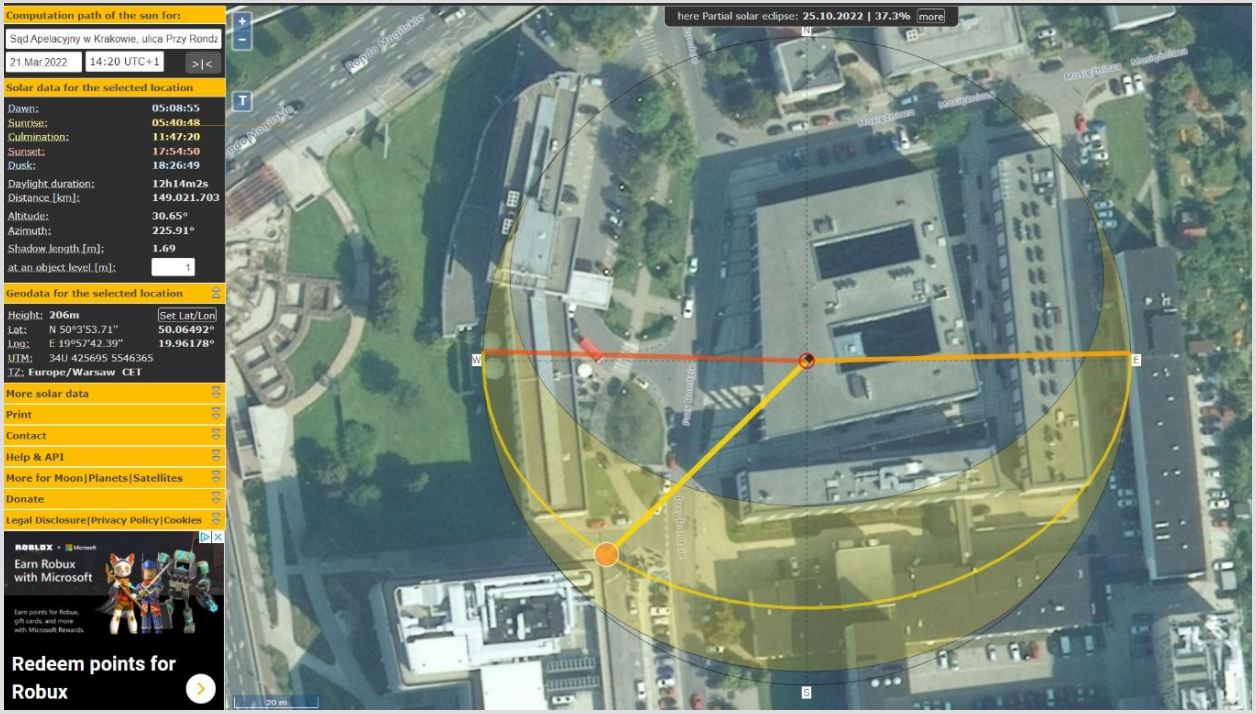


ALTERNATIVE COULD BE BETTER

wego.here.com



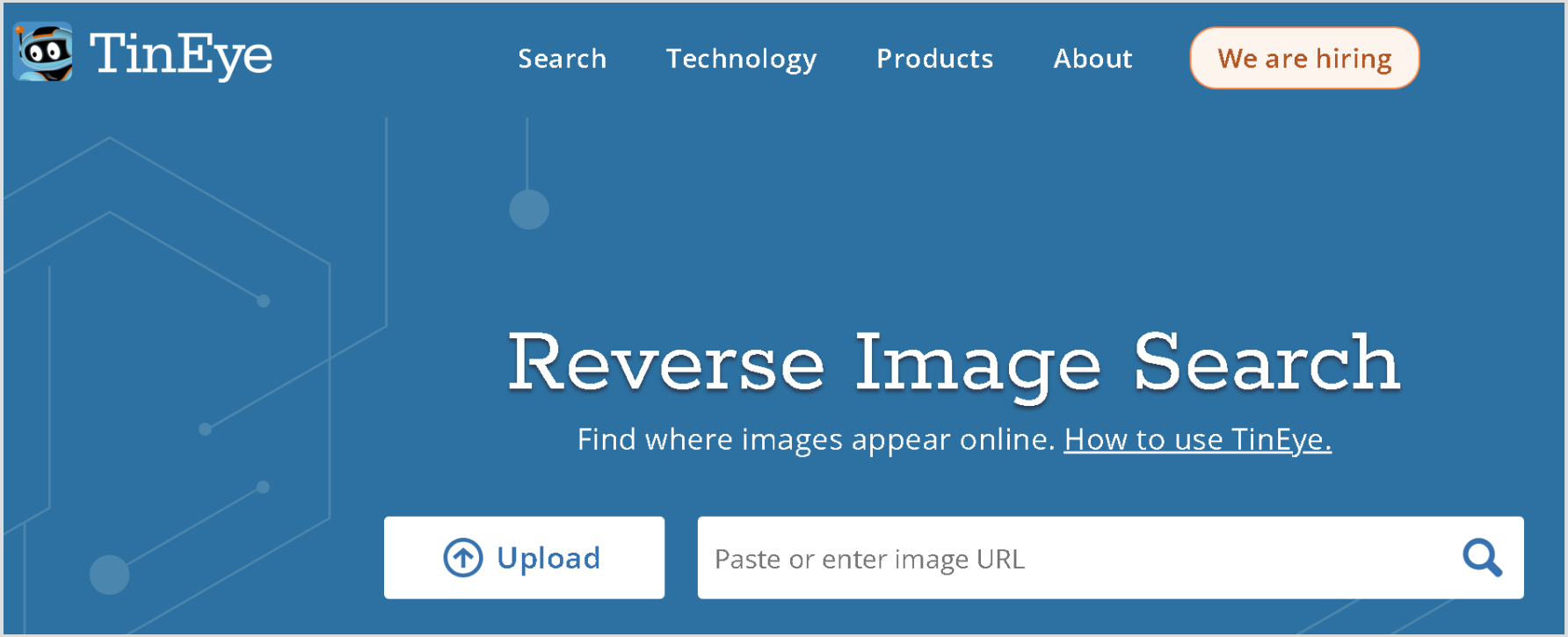
suncalc.org



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

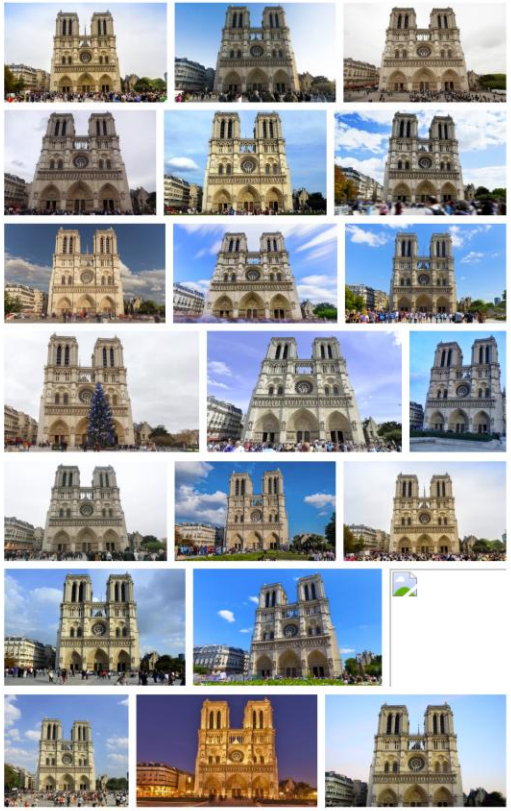
www.alamy.com

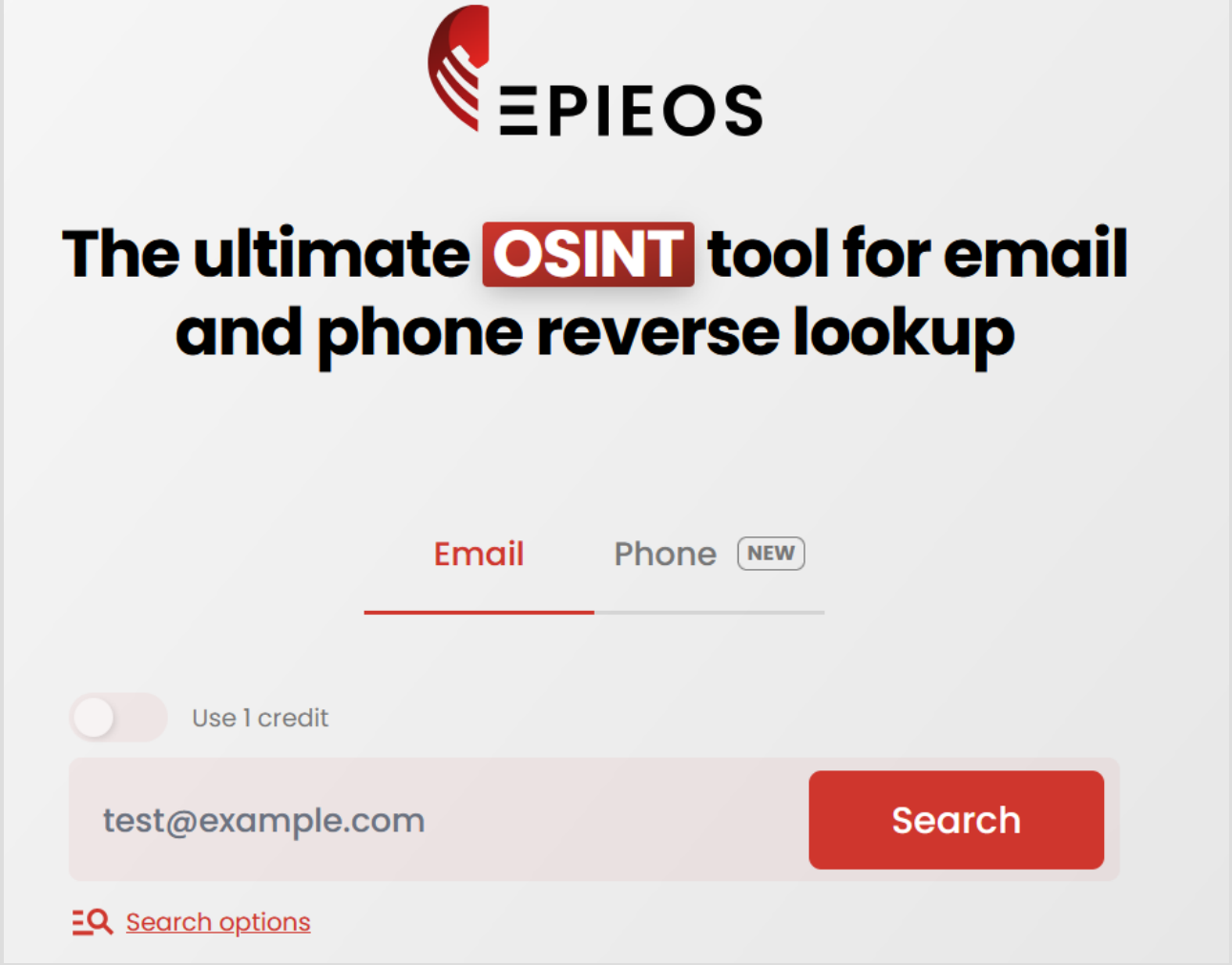
paris-sept-17-2014-the-western-facade-... - First found on Sep 25, 2021

dinneratmidnight.wordpress.com

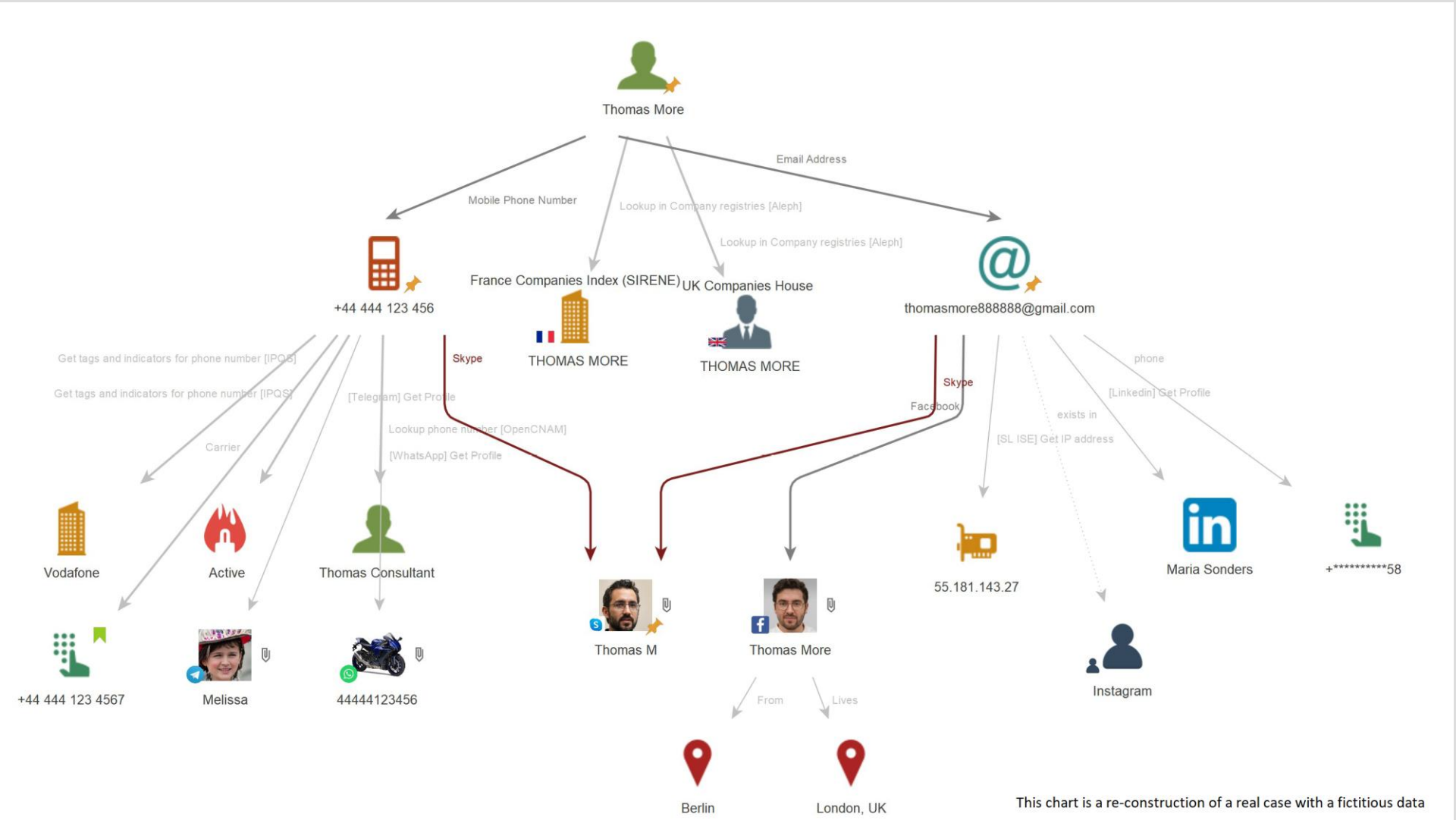
2010/11/14/travels-part-2-paris/ - First found on May 14, 2017
2010/11/14/travels-part-2-paris/ - First found on May 14, 2017
view all 3 matches

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



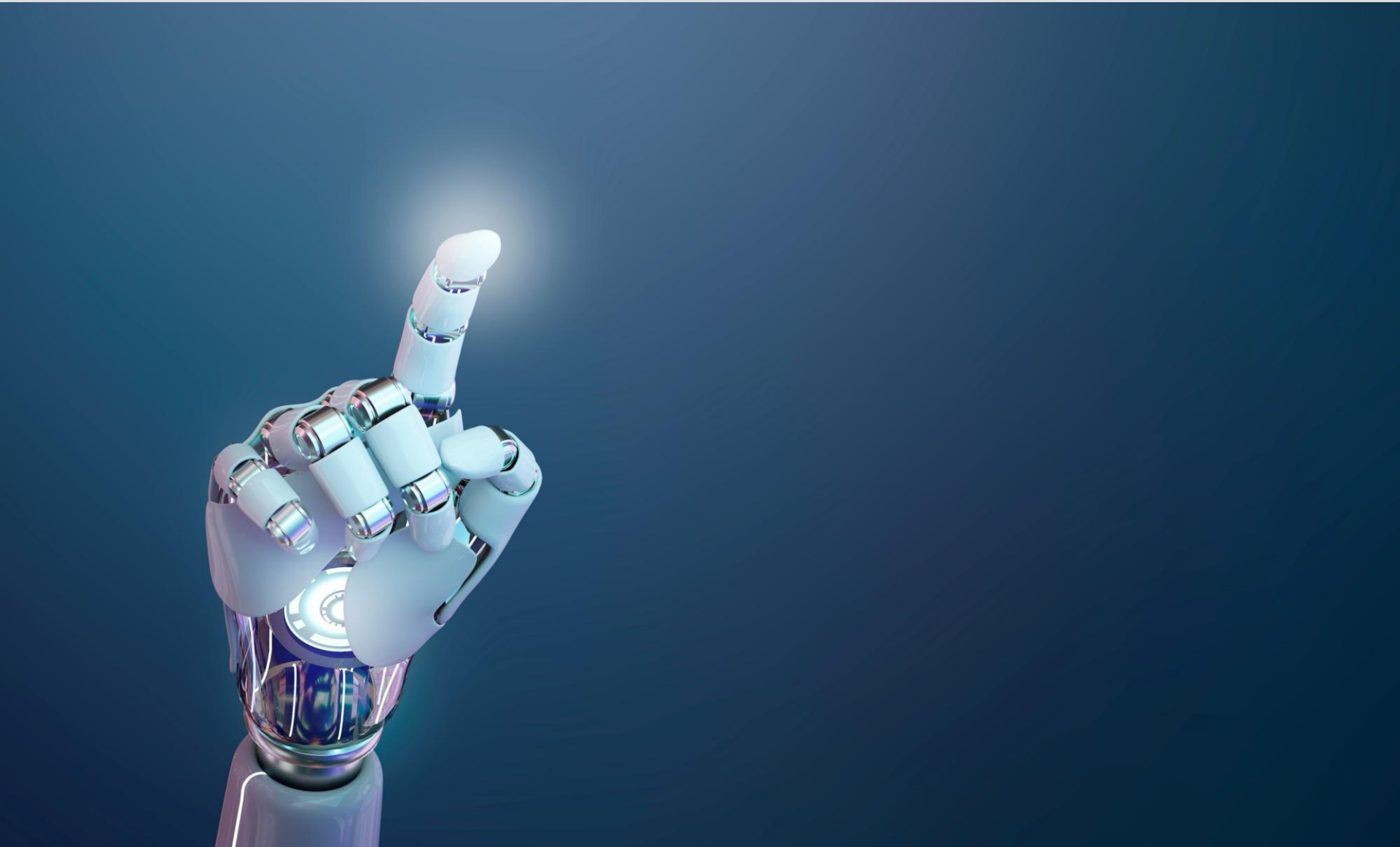

EPIEOS
The ultimate OSINT tool for email and phone reverse lookup
Email
Phone
NEW
Use 1 credit
test@example.com
Search
Search options

SAMPLE SOCMINT CHART



COMPETITOR ANALYSIS

ARTIFICIAL INTELLIGENCE & OSINT



LETS DO PRACTICAL

Your job should you choose to accept it

QUESTIONS & DISCUSSION

Bilal Şen

info@coninsec.com

Co-funded by
the European Union

University of Antwerp
Faculty of Law

E-evidence in criminal cases: the SkyECC saga

Prof. dr. Joachim Meese

associate professor

attorney

The Sky ECC case

- **Sky ECC?**
  - a subscription-based, end-to-end encrypted messaging service on specially modified smartphones, marketed as a tool for maximum anonymity
  - developed by a Canadian company (Sky Global)
  - cf. the (similarly hacked) EncroChat service

The Sky ECC case

- **The investigation**
  - Belgium, France, and the Netherlands initiated the investigation in 2018, creating a Joint Investigation Team (JIT)
  - French authorities created a ‘copy’ or ‘image’ of the Sky ECC servers located in Roubaix, recording and transcribing encrypted communication
  - The operation involved live monitoring and the collection of communications data from thousands of phones
  - it provided a massive dataset of encrypted messages, offering unprecedented insights into the operations of international criminal organisations
  - Sky ECC was officially shut down in March 2021, but hundreds of millions of encrypted messages remain available

The Sky ECC case

- **The use of the data**
  - many prosecutions in many countries rely on data that originates from the operation in France
  - this data was transmitted to other national authorities through European Investigation Orders (EIO)

The Sky ECC case

- **EIO?**

  => principally an instrument for the authorities to gather evidence abroad

  - the EIOD doesn't regulate the position of the defence, e.g. possibility to be present at the execution of specific investigative measures (such as witness examination), or the right for the defence to have a EIO issued

  => inspired by:

  - mutual recognition of judgments and judicial decisions
  - mutual recognition of orders to prevent the destruction, transformation, moving, transfer or disposal of evidence
  - European evidence warrant
  - European arrest warrant

The Sky ECC case

- **EIO: fundamental rights and legal remedies?**
  - EIO is based on mutual confidence and a presumption of compliance by other member States with Union law and, in particular, with fundamental rights
    - however, there can be conflicts between existing regulations in various member States
      - ➢ e.g.: obligation to decrypt vs. privilege against self-incrimination
    - possibility of discussions on admissibility/authenticity of e-evidence in criminal procedures due to different domestic standards
      - ➢ e.g. Cass. Belgium 11 January 2022, P.21.1245.N (https://juportal.be/content/ECLI:BE:CASS:2022:ARR.20220111.2N.1/NL)

The Sky ECC case

- **EIO: fundamental rights and legal remedies?**
  - central question: how can a defendant in another EU country challenge the legality of the underlying operation in France that lead to evidence being used abroad?
    - Cass. fr. 16 September 2025, n° 24-84.262, ECLI:FR:CCASS:2025:CR00936 https://www.courdecassation.fr/decision/export/68c904234f50b651b49423c8/1)
    - person charged in Germany initiated a procedure in France requesting the annulment of evidence obtained in France (art. 694-41 CPP France)
    - see ECHR 24 September 2024, dec., A.L. & E.J v. France, n° 44715/20 and 47930/21:

      "Under French law, this Article provided that a legal challenge, an action for exclusion of evidence or any other type of remedy could be used against a measure taken in French territory pursuant to an EIO, provided that a remedy could have been used against that measure if it had been ordered in domestic proceedings. Where appropriate, the measure taken pursuant to an EIO could be challenged under the same conditions and in accordance with the same procedures as it might have been in a purely internal situation. The Court noted that the provisions of that Article allowed any "person concerned" to pursue the remedies that would have been open to him or her in France if the measure carried out pursuant to the EIO had been so in domestic proceedings. They therefore enabled the applicants to avail themselves of the procedural rights such a status would have conferred on them in a purely internal situation."

The Sky ECC case

- **EIO: fundamental rights and legal remedies?**
  - central question: how can a defendant in another EU country challenge the legality of the underlying operation in France that lead to evidence used abroad?
    - according to the Court de Cassation, the request does not fall under the scope of art. 694-41 CCP France (<-> ECHR)
    - but the next question is: is this procedure compatible with art. 14 EIOD (legal remedies)?
      - ➢ problem for the defendant: if he cannot challenge the legality in the requesting State (Germany) and neither in the executing State (France), what can he do?
      - ➢ 2 prejudicial questions for the Court of Justice of the EU
      - ➢ the Court asked for a speedy decision on the following grounds:

        The interpretation requested is likely to have significant consequences, both in terms of other appeals for annulment brought before the French courts on the same basis and in terms of the numerous proceedings currently underway in various Member States of the European Union, in which individuals are being detained, prosecutions based in particular on the transmission, by European investigation order, of evidence similar to that contested by the applicant in the present appeal, all originating from the same procedure known as 'SkyECC'.

Thank you!

Let’s connect:

@ joachim.meese@uantwerp.be

in www.linkedin.com/in/joachimmeese/

Co-funded by
the European Union

University of Antwerp
Faculty of Law

Artificial intelligence and the challenges ahead for legal practitioners

Prof. dr. Joachim Meese

associate professor

attorney

Artificial intelligence

- what is it and what can we do with it? -

- challenges of using AI -

What is AI?

- **assumption: we can mechanise human thought**
  - can rational thought be made as systematic as algebra or geometry? (e.g. Leibniz, Hobbes, Descartes and the further study of mathematical logic in the 20th century by Russell and Whitehead)
  - the ‘Turing test’ or ‘imitation game’ (1950)

What is AI?

- **expert systems**
  - based on logical rules
  - If <conditions> then <action>, e.g.:
    - IF the person is under 18 THEN the person does not have the ability to sign legal documents
  - these rules can cause problems when certain content can't be structured as a rule ('open-textured problems), e.g.
    - IF the person is mentally incapacitated THEN the person does not have the ability to sign legal documents
      - ➢ the notion mentally incapacitated requires leal knowledge
      - ➢ we need more than rules to interpret law
  - rule-based systems can deliver incorrect output when the rules are poorly designed

What is AI?

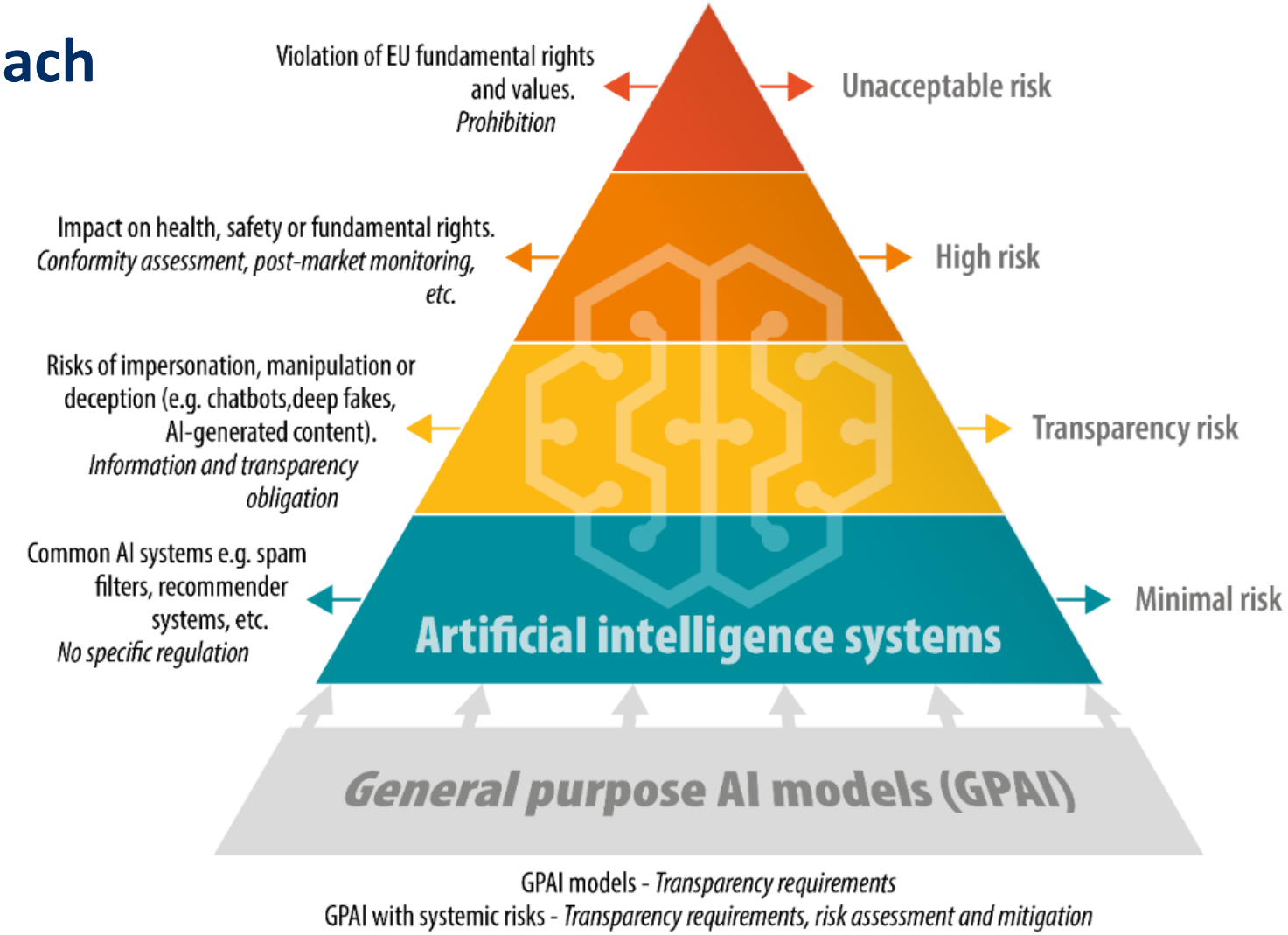
- **datadriven systems**
  - based on the analytics of large amounts of data (machine learning)
    - the system can learn from data, can identify patterns, and can make predictions or decisions with minimal human intervention
    - the system can learn by itself with each new input of information
  - ChatGPT is a large language model (LLM)
    - this is a machine learning model that is trained to generate text that is like human language
    - ‘large’ because it is trained on a large dataset and can generate highly realistic and coherent text

What is AI?

- **Definition of AI in the EU AI Act**
  - Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (http://data.europa.eu/eli/reg/2024/1689/oj)
    - "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" (art. 3.1)
  - entry into force:
    - the regulation will apply from 2 August 2026, however, there are some exceptions:
      - ➢ the prohibitions, definitions and obligations regarding AI literacy have applied since 2 February 2025
      - ➢ some rules took effect on 2 August 2025, including those on governance structure, penalties, and obligations for providers of general-purpose AI models

A quick word on the AI Act

- **Risk-based approach**



A quick word on the AI Act

- **Risk-based approach**
  - is for example prohibited:
    - **criminal risk assessment**, predicting the likelihood of committing a crime solely based on profiling or personality traits, except in objective, fact-based criminal investigations (art. 5.1.d)
    - **Real-time biometric identification in public by law enforcement**, unless strictly necessary for particular situations (e.g. finding missing persons, preventing imminent threats or identifying suspects of serious crimes; see art. 5.1.h)
      - this must follow strict legal procedures, including prior authorisation, a limited scope and safeguards to protect rights and freedoms (see art. 5.3 to 7)
  - are for example considered high risk:
    - AI systems used for assessing the risk of becoming a victim, polygraphs or similar tools, evaluating evidence reliability, predicting recidivism or profiling individuals for criminal investigations (see Annex III, 6)

What can legal practitioners do with AI?

- **preliminary remark**
  - while AI Systems offer the potential to enhance human well-being, productivity, and innovation, they also raise significant concerns regarding their impact on human rights, democracy, and the rule of law
  - every theoretically possible application should be considered in this regard

What can legal practitioners do with AI?

- **as a practical tool for legal practitioners**
  - searching for case law, Q&A, drafting legal documents, predicting case outcomes
  - examples of predictive justice tools
    - in the USA: Supreme Court Forecasting Project (2004):
      - ➢ aimed to predict:
        - ✓ whether the court would affirm or reverse the appeal (1)
        - ✓ how each individual judge would vote (2)
      - ➢ statistical model based on data from precedent cases + parallel analysis by an expert panel
      - ➢ success ratio:
        - ✓ (1): 75% (compared to 59.1% for the expert panel)
        - ✓ (2): 66.7% (compared to 67.9% for the expert panel)
      - ➢ in 2017: machine learning → reliability for (1) *decreased* (70.2%) and increased for (2) (71.9%)

What can legal practitioners do with AI?

- **as a practical tool for legal practitioners**
  - searching for case law, Q&A, drafting legal documents, predicting case outcomes
  - examples of predictive justice tools
    - in the EU: predictive model on the jurisprudence of the ECtHR
      - data set: decisions on art. 3, 6 and 8 ECHR
      - reliability of the prediction of the decision: about 75%
      - source: Medvedeva, M., Vols, M. & Wieling, M. “Using machine learning to predict decisions of the European Court of Human Rights”, *Artif Intell Law* 28, 237–266 (2020), https://doi.org/10.1007/s10506-019-09255-y

What can legal practitioners do with AI?

- **as a practical tool for legal practitioners**
  - searching for case law, Q&A, drafting legal documents, predicting case outcomes
  - risks?
    - rather low, but be aware of AI hallucinations
      - ➢ https://www.damiencharlotin.com/hallucinations/ (database of examples of hallucinations in legal cases)
    - can lead to cognitive biases
    - accuracy of the output of LLM's is dependent on the quality of the prompting, so training for legal professionals is needed
      - ➢ can be approved by chain-of-thought prompting: not only seeking an answer but also requiring the model to explain its steps to arrive at that answer

What can legal practitioners do with AI?

- **evaluation of the reliability of evidence**
  - China: ‘smart courts’ initiative
    - enables courts to experiment with integrating AI into adjudication in a variety of ways, including by using software that reviews evidence, suggests outcomes, checks the consistency of judgments, and makes recommendations on how to decide cases
    - alerts judges when their judgment falls outside the program’s predicted range of case outcomes
    - source:
      - Rachel E. Stern, Benjamin L. Liebman, Margaret Roberts & Alice Z. Wang, “Automating Fairness? Artificial Intelligence in the Chinese Court”, 59 *COLUM. J. TRANSNAT'L L.* 515 (2021)
      - https://scholarship.law.columbia.edu/faculty_scholarship/2940
  - under the EU AI Act, this is a high-risk system (see art. 6.2 and annex IIII, 6.c)
    - the same goes for polygraphs and similar tools (see art. 6.2 and annex IIII, 6.b)

What can legal practitioners do with AI?

- **predictive policing, profiling and risk assessment, e.g.:**
  - general crime prevention
  - evaluation of the danger levels of the subject
  - determination of the possibility of recidivism

What can legal practitioners do with AI?

- **predictive policing, profiling and risk assessment**
  - under the EU AI Act, these are a high-risk applications (see art. 6.2 and annex IIII, 6.a, d and e), namely:
    - to assess the risk of a natural person becoming the victim of criminal offences
    - for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups
    - for the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of the detection, investigation or prosecution of criminal offences
  - requires an impact assessment to mitigate or eliminate the risks
  - AI as ‘decisional aides’ to human decision makers can lead to cognitive biases

What can legal practitioners do with AI?

- **facial recognition and other biometric surveillance systems**
  - e.g. Clearview AI: software based on data scraping that can produce matches with a photo
    - widely used by US law enforcement
    - some procedures against Clearview AI in Europe (mainly about GDPR)
  - what does the AI Act say?
    - real-time biometric identification in public by law enforcement is prohibited (see above), unless strictly necessary for particular situations (e.g. finding missing persons, preventing imminent threats or identifying suspects of serious crimes; see art. 5.1.h)
    - post-remote biometric identification is considered high-risk (Annex III, 1.a)

What can legal practitioners do with AI?

- **automated decision-making**
  - e.g. COMPAS
    - used by the US courts to aid judges and parole boards in making decisions about sentencing, parole and probation
    - statistical system that includes static and dynamic information (e.g. age, zip code, criminal or family history, the defendant's answers to questions, such as 'does a hungry person has the right to steal?' or 'how old were you when your parents separated?')
      - however, the specific algorithm's design and code are a proprietary trade secret
      - 'black box' problem (lack of transparency)
    - it was shown in 2016 that COMPAS had a bias against black individuals
  - risk of false positives and false negatives

What can legal practitioners do with AI?

- **Why AI can never replace judges**
  - AI judges would never meet the requirement of the right to a fair trial
    - AI can't constitute an independent and impartial tribunal
      - to be a judge requires more than merely applying the law (e.g. being member of a community, to understand that community, its history, its values, and to confer social legitimacy)
      - crime is a social construct, and the social acceptance of a decision, rather than consistency, is the ultimate task of delivering justice
      - respect for a judicial decision and the social legitimacy of the judiciary in general are to be found in the fact that the judgment is rendered by a fellow human being
      - trust in judges is based on public knowledge of the method of appointment, the judge's knowledge and experience, personal reputation, the oath taken, guarantees of independence and impartiality, and other factors that build public confidence in courts and judges; this does not apply to AI
      - judges must not only posses technical competence, but also moral integrity
      - judges apply mercy and compassion and their weighing against justice and use intuition and emotion

What can legal practitioners do with AI?

- **Why AI can never replace judges**
  - AI judges would never meet the requirement of the right to a fair trial
    - AI can't constitute an independent and impartial tribunal
      - algorithms lack a conscience
      - algorithms are dependent on judgments in other cases or on predetermined patterns of behaviour, so the guarantees of judicial independence are undermined
      - the court is not only the body that applies the law to a particular case, but also, or even primarily, the body that controls the legislative and executive powers in relation to individuals
      - judges must do many things (e.g. to assess the credibility of evidence, including witnesses, to interact with people, to manage cases, to provide education, etc.) that can't be done by AI
      - legal norms are rules of conduct expressed in natural language, but enriched with their social and conventional meaning; they have to be applied with understanding of the *ratio legis*
      - the role of the courts is also to develop the law, while AI is backward-looking
      - the dignity of the human person requires a judgment by a human person

Some specific AI challenges

- **transparency issues**
  - black box: how does the system work?
  - delivering the source code is not always a solution: only experts can understand it
  - how much transparency is required?
  - Edmund Burke (1729-1797): “justice ends where mystery begins”
- **evidence manipulation**
  - e.g. deep fakes
  - under the AI Act, there is transparency obligation for deep fakes (see art. 50.4)

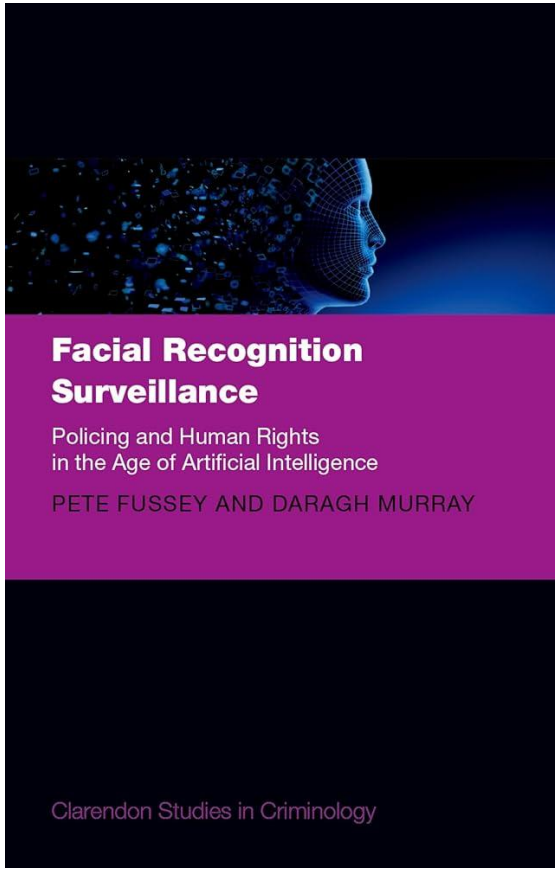
AI: further reading

Books

Digitalization and Artificial Intelligence in Courts: Opportunities and Challenges

- Fernando Esteban de la Rosa, Pablo Cortés & Nuria Marchal Escalona
- https://doi.org/10.1093/9780198918752.001.0001
- Oxford Academic, Oxford
- Published online: 22 August 2025
- Published in print: 25 September 2025

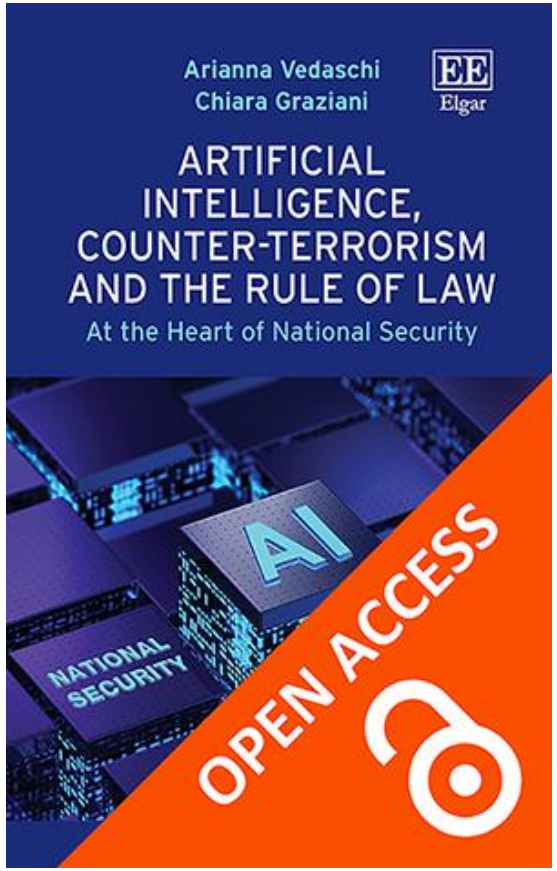
Books



Facial Recognition Surveillance: Policing and Human Rights in the Age of Artificial Intelligence

- Pete Fussey and Daragh Murray
- https://doi.org/10.1093/9780191979927.002.0012
- Clarendon Studies in Criminology, Oxford
- Published online: 19 June 2025
- Published in print: 29 July 2025

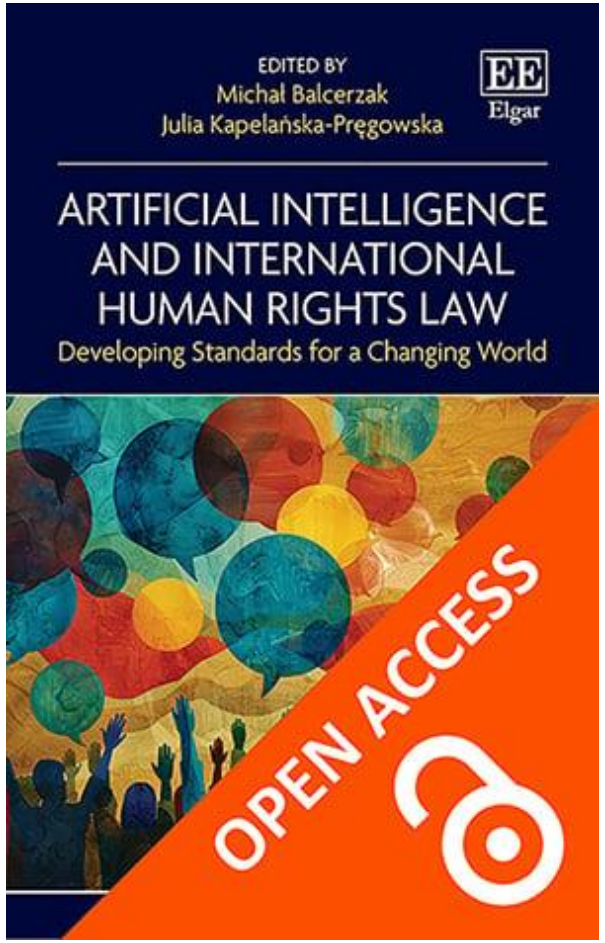
Books



Artificial Intelligence, Counter-Terrorism and the Rule of Law. At the Heart of National Security

- Arianna Vedaschi & Chiara Graziani
- https://doi.org/10.4337/9781803928340
- Open access
- Elgar Online
- Published: 15 May 2025

Books



Artificial Intelligence and International Human Rights Law. Developing Standards for a Changing World

- Michał Balcerzak and Julia Kapelańska-Pręgowska
- https://doi.org/10.4337/9781035337934
- Open access
- Elgar Online
- Published 18 October 2024, 346 p.

Thank you!

Let’s connect:

@ joachim.meese@uantwerp.be

in www.linkedin.com/in/joachimmeese/

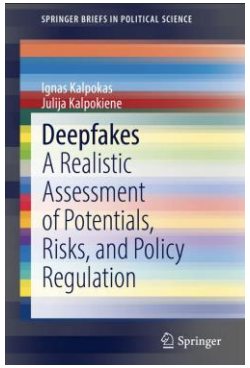
Co-funded by
the European Union

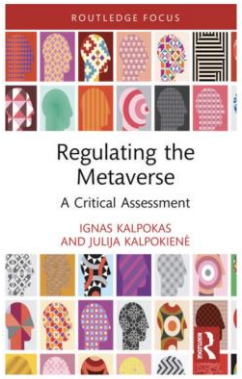
“SEEING IS BELIEVING” NO LONGER STANDS

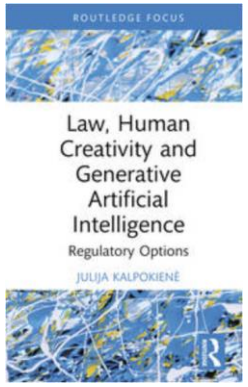
SYNTHETIC TECHNOLOGIES AND THE EVALUATION OF EVIDENCE

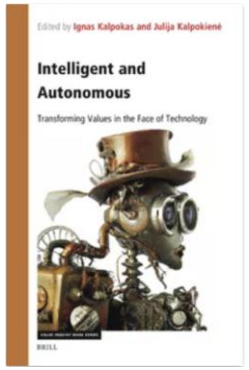
DALL-E “Lawyers having fun in Thessaloniki”

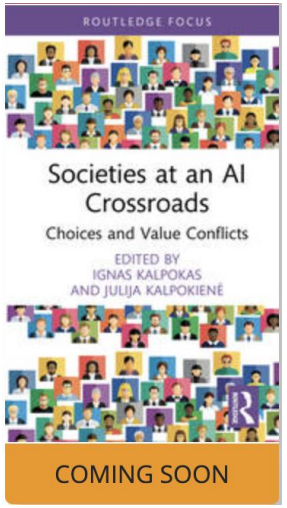
dr. Julija Kalpokienė
10 October 2025 Thessaloniki
ERA: #DIGITALISATION AND #AI IN CRIMINAL JUSTICE











ABOUT ME

www.linkedin.com/in/techlawexpert

- Practicing lawyer (Lithuania)
  www.kalpokiene.lt | advokate@kalpokiene.lt
- Of Counsel (Germany) | www.rickert.law
- Assoc. Prof. & Researcher at Vytautas Magnus University
- Policy Consultant at Internet & Jurisdiction Policy Network

Jon Stone

Deepfakes Surge in 2025, Raising Alarms for Financial Institutions

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

Deepfakes

19 Sep 2025

Friend stole my face for deepfake nudes – now I want tougher laws

The victim of one of the first deepfake prosecutions in Scotland says the law needs to change to protect victims.

19 Aug 2025

Man sent friends nude deepfakes of woman from high school

Callum Brooks was fined for altering the pictures of the woman and sharing them with his friends without her consent.

9 Aug 2025

Elon Musk's AI accused of making explicit AI Taylor Swift videos

Grok Imagine's "spicy" mode made explicit videos of Taylor Swift, according to The Verge and Gizm

Screenshot

AI · ARTIFICIAL INTELLIGENCE

Asia

Finance companies fight back against AI deepfakes, with over 70% of new enrollment attempts to some firms being fake

BY **LIONEL LIM**
ASIA REPORTER

August 13, 2025 at 3:05 AM EDT

CFO

Opinion Library Events Press Releases Topics

92% of companies have experienced financial loss due to a deepfake

Deepfake fraud attempts have taken form in both audio and vide... at an increasing rate, according to new data from Regula.

Published Nov. 6, 2024

Forbes

The Dark Side Of AI: How Deepfakes And Disinformation Are Becoming A Billion-Dollar Business Risk

How deepfakes, nudes and teen misogyny have changed growing up

Follow

...v 6, 2024, 01:43am EST

Gendered misconduct on the rise, female teachers scared of being “deepfaked” and parents protecting badly behaved boys: this is high school in 2024.

By Bri Lee for ABC’s Long Read

Teenagers

Sat 2 Nov

SCRIPPS NEWS

Viral celebrity deepfake ad warns of AI being used 'trick you into not voting'

A video with more than 6 million views on YouTube is warning voters to pay closer attention to what they see and hear online.

abc NEWS Video Live Shows Elections 538 Shop

2024 Election Dashboard Results Map State Results Exit Polls

AI deepfakes a top concern for election officials with voting underway

Artificial intelligence could be weaponized on voters, feds warn

Live Shows ••• CBS NEWS

FBI warns of deepfake videos ahead of Election Day

The Federal Bureau of Investigation is warning the public about two videos falsely claiming to be from the FBI on election security. One mentions the apprehension of groups committing ballot fraud and the other has to do with second gentleman Doug Emhoff. The bureau stresses that the videos are not authentic, are not from the FBI and the content they depict is false. CBS News Homeland Security and Justice reporter Nicole Sganga has more.

NOV 4, 2024

DEEPFAKES – WHAT IS IT?

- Media (image, video, sound):
  - Either created by AI or
  - Manipulated by AI
  - E.g.: face swapping or facial manipulation
- What is required to create a deepfake?
  - Photos / videos (publicly available images may suffices)
  - Text / sound
- Increasingly a mobile device suffices to generate relatively good quality deepfakes:
  - Cheap,
  - Quick to generate,
  - Undetectable without special tools.

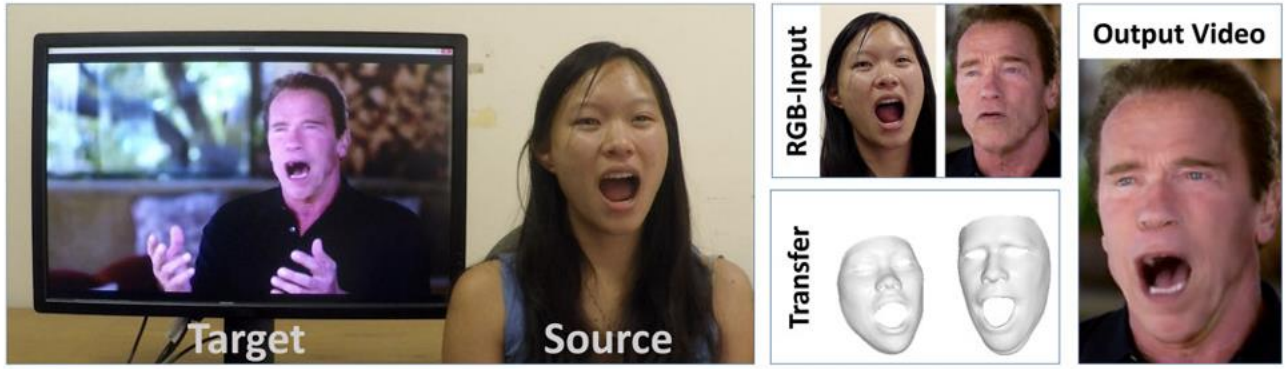
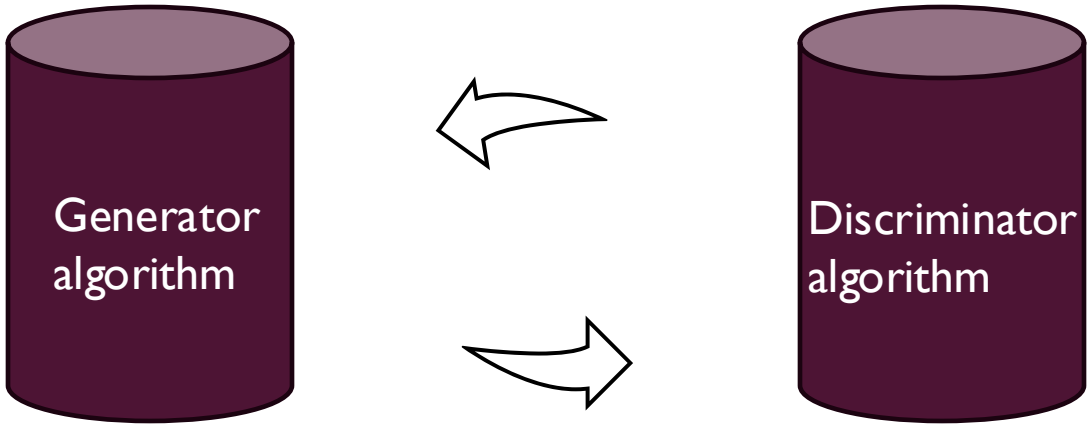


Figure 1. Illustration of Face2Face method. Image credits: Thies and Others.

Edvinas Meskys, Aidas Liaudanskas, Julija Kalpokiene and Paulius Jurcys. "Regulating deep fakes: legal and ethical considerations" Journal of Intellectual Property Law & Practice, 2020, Vol. 15, No. 1

HOW DOES IT WORK?



trained using samples (images, audio, and/or video) &
tasked to create a new piece of media or manipulate an existing one

trained to recognise certain features & points out where the "generator" missed something and has to go back and correct any inconsistencies

DEEPFAKES

- From low-tech and easy to generate to high-tech, expensive and good quality
- Applications range from porn & fraud to films and entertainment

GENERATIVE AI & DEEPFAKES

E. g.: McDonald's commercial in Japan

WHO ARE YOU?










https://thispersondoesnotexist.com/

MYHERITAGE – DEEP NOSTALGIA

Photo by Christopher Campbell on Unsplash

ALSO, FAKE EXPERTS?

- Generated pictures
- Generated video (with or without sound)
- Generated sound / audio / voice

- Who do you trust? How do you check?

SHOW ME YOUR ID // ONLINE VERIFICATION


RZECZPOSPOLITA POLSKA / REPUBLIC OF POLAND / RÉPUBLIQUE DE

PASZPORT
PASSPORT
PASSEPORT

TYPE P
IPYSTYC/CODE POL
N"CATY/PEPRONYSISI-IDE INDŻINAN'E EM 9638245

1. NAZWNO-IM I WIZMENY
MUSIELAK
2. PRITY / NAME / JCRIT / ANNAMES
BORYS ANDRZEJ
3. CKZONBSTWFOCTE D²BIRTH / PEBSONALAS
23 APR/AVR 1984
IVJEDVOZJNET. ID PAR EU PAN IDENTITE
60053482714
5. SEX / PLACE
M/M
AUTHORITKA / MATURTY SIGNATURE
MAZOWIECKI
WOJ. MAZOWECKIE
VOIED.
2. DATA I USZOCU / DATE DESPII / DEEXPIRY
25 STY/JAN 2023
3. DATE D EXPIRY / DATE D EXPIRY / OSSUE
25 STY/JAN 2033

P<POLMUSIELAK<<<BORYS<ANDRZEJ<<<<<<<<<<<<
EM9638245<POL8404238M3301256754<<<<<<<02

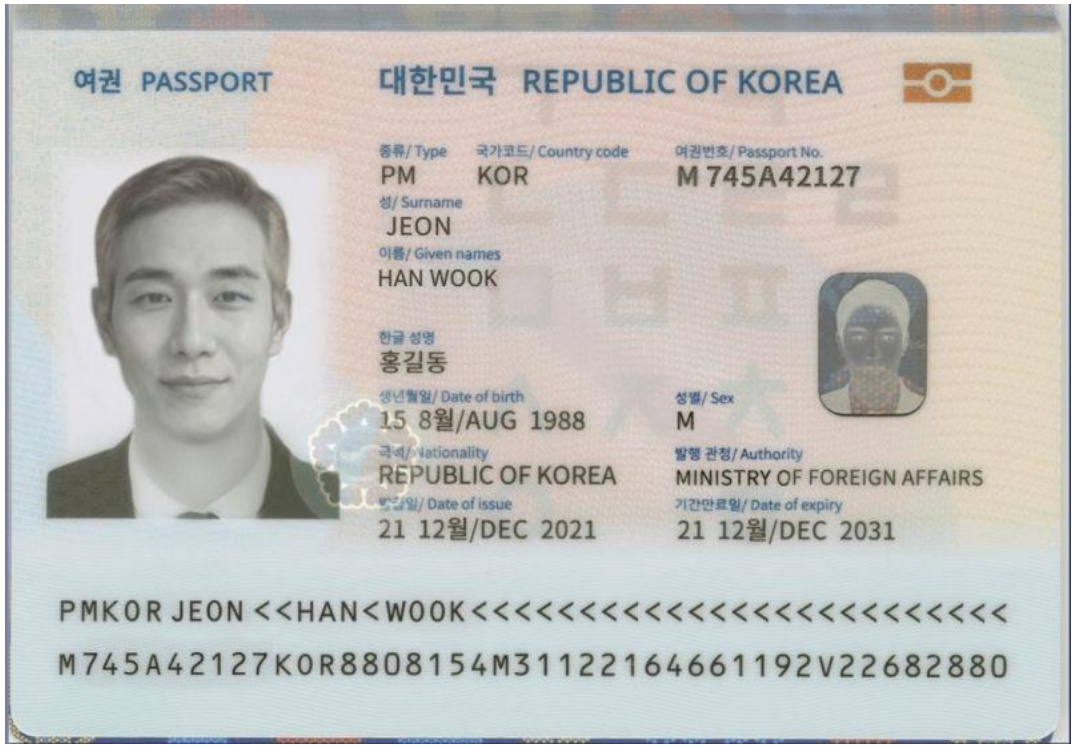
WHAT ARE THE DANGERS? HOW MUCH DO WE RELY ON VERIFICATION?

North Korean hackers use ChatGPT to forge a South Korean military ID

14 Sept. 2025, Bloomberg

How are ID documents used?
What are the verification procedures?
How much do we trust when we see an ID? E.g. a copy of it?

Other use cases: phishing, gaining trust, etc.



WHERE ARE WE HEADING TO?

- Black Mirror: the almond milk and nut allergy scene.
- Who drank the milk? Was it Maria?
- How far off are we?

Turn God Mode on. Meet Human Generator

Create hyperrealistic full-body photos of people in real time

Create human Free

HUMAN GENERATOR New

Description Pose Face upload Hot

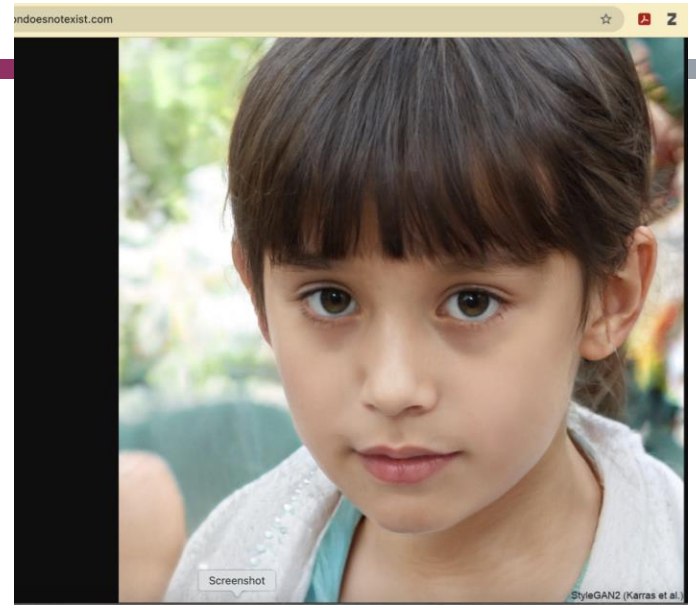
Description Randomize reset

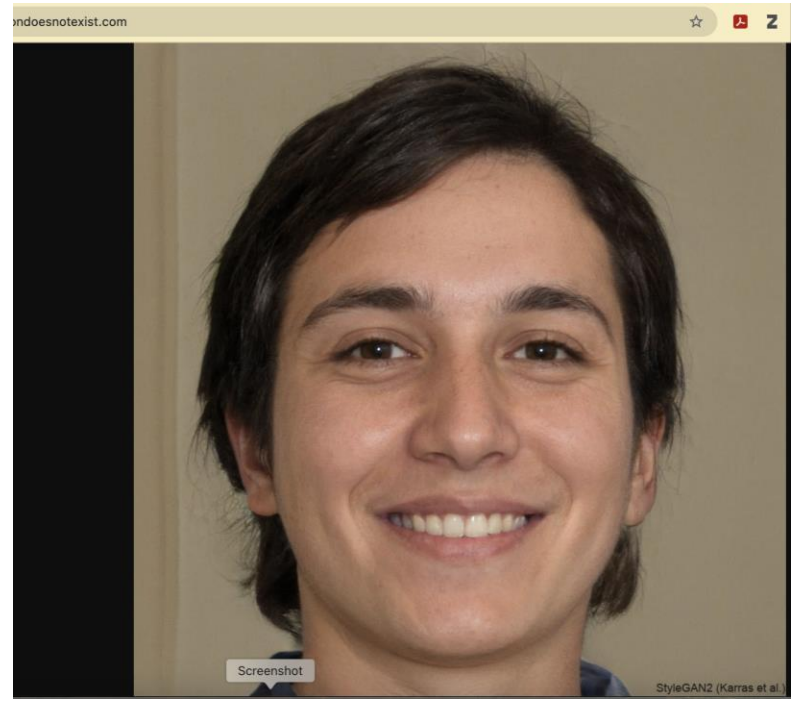
female colombian
average body
young adult sweater
pants shoes
casual clothes
studio backdrop background

Negative prompt

Enter negative prompt...

Screenshot





Create custom faces with the best AI face generator

Worry no more about finding the perfect stock photo with Text to Image on Canva. With the AI person generator, you can make custom, photorealistic faces for your pitch decks, websites, product demos, and more.

Create a face with AI

FACE GENERATOR

Faces

Sign in

Sex

- Male
- Female

Headpose

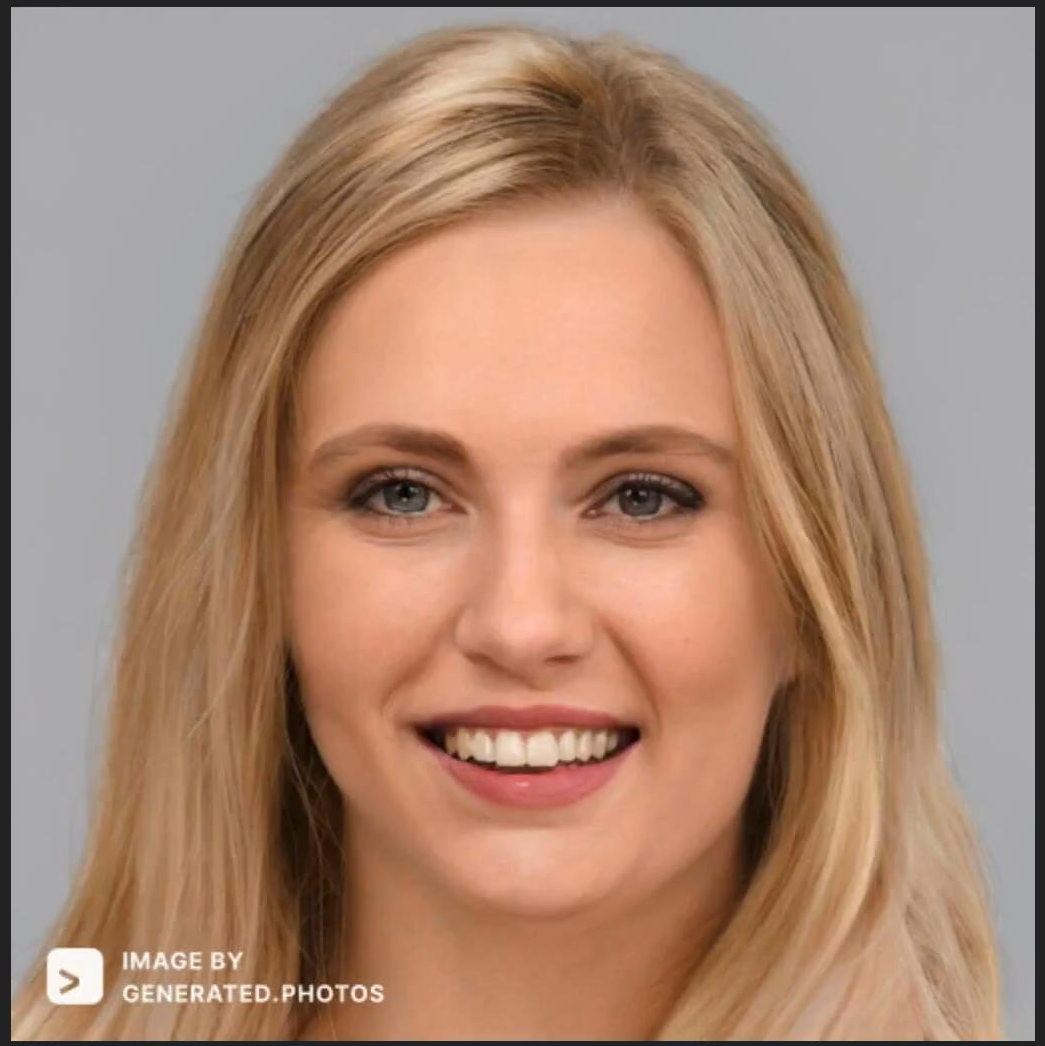
Age

Younger Older

Emotion

- Neutral
- Happy
- Surprised
- Angry
- Contemptuous
- Disgusted
- Frightened
- Sad

Skin Tone Very Fair



Download Add to cart Share

ARE WE VIGILANTE ENOUGH?

SOME EXAMPLES

- Moldovan PM allegedly discussing mobilization or supporting a pro-Russian party
- Ukraine: Deepfakes focusing on a rift between Zelensky and Zaluzhny
- In India, a dead politician endorsing his son, MK Stalin


Bonne année 2024 !
FAKE
MES CHERS COMPATRIOTES.
0:00 / 5:20






- While emphasis is usually on images and video, fake audio is particularly dangerous

  - Less awareness
  - More difficult to spot (both technologically and cognitively)

DO YOU ALWAYS NEED HIGH-TECH?

Sometimes a cheapfake / shallow-fake is enough

Original

Photoshopped

Real Video

Fake Video

Footage of House speaker deliberately slowed down to make her appear drunk or ill

True Claim

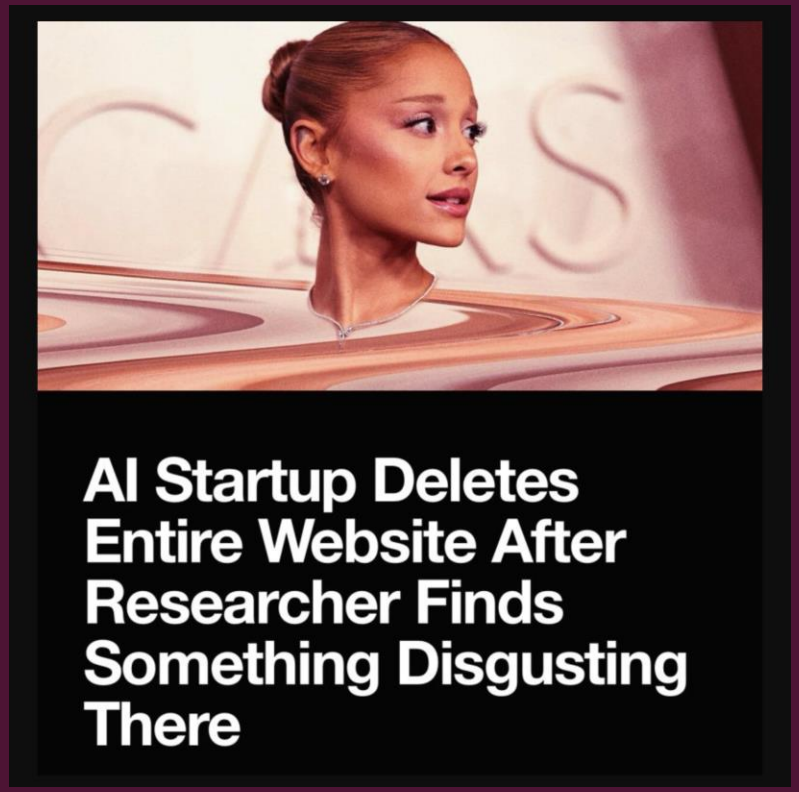
2014 : President Obama and Dr Fauci visiting NIH lab, Maryland in 2014 to learn about Ebola vaccine

False Claim

2020 : President Obama, Dr. Fauci and Melinda Gates and at Wuhan Lab, China in 2015 for 'Bat' project

DOES IT ALSO IMPACT THE LEGAL JUSTICE SYSTEM?

AI as a tool to perpetrate crime
AI as a tool to overwhelm and distract
AI as a tool to help prevent, detect crime



DETECTION

- May not be visible without employing detection tools
- For example, CCTV footage and Zoom calls tend to be low quality, similar as Deepfakes
- Detection tools need to be constantly improved & developed

VIDEO AS A PIECE OF EVIDENCE

- Whose responsibility is it, anyway?
- Education / training – why is it important?
- Detection: how to evaluate? Expertise?
- Expert evidence:
  - Who covers the costs?
  - Who requests?
  - How to ensure that it is detected? Technology, expert knowledge, etc.

DISCUSSION & QUESTIONS

- Let‘s keep in touch
- advokate@kalpokiene.lt
- LinkedIn: www.linkedin.com/in/techlawexpert

ChatGPT “Lawyers having fun in Thessaloniki”

BINANCE

Introduction to Crypto

Lilija Mažeikienė
Investigations Team, EMEA
lilija@binance.com

What to expect?

BINANCE

1 Crypto 101: technology, definitions, blockchain explorers
2 (Ab)use of crypto
3 Crypto services: internal controls, cooperation

BINANCE

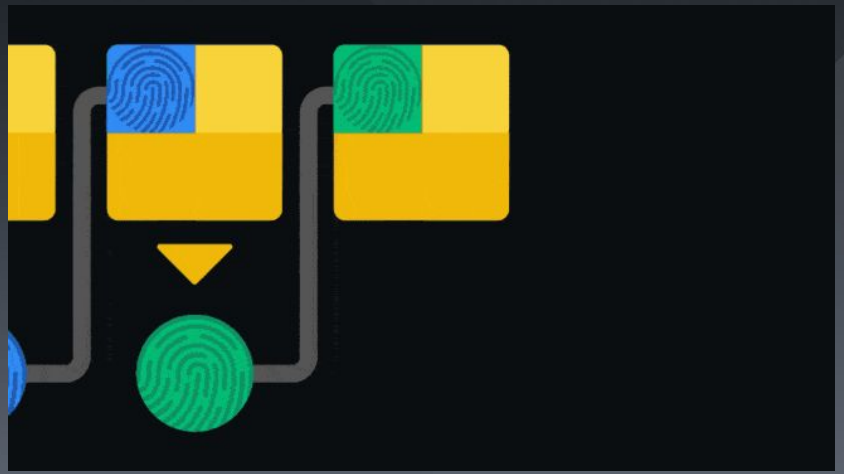
Crypto 101

Crypto 101: Blockchain Technology

BINANCE

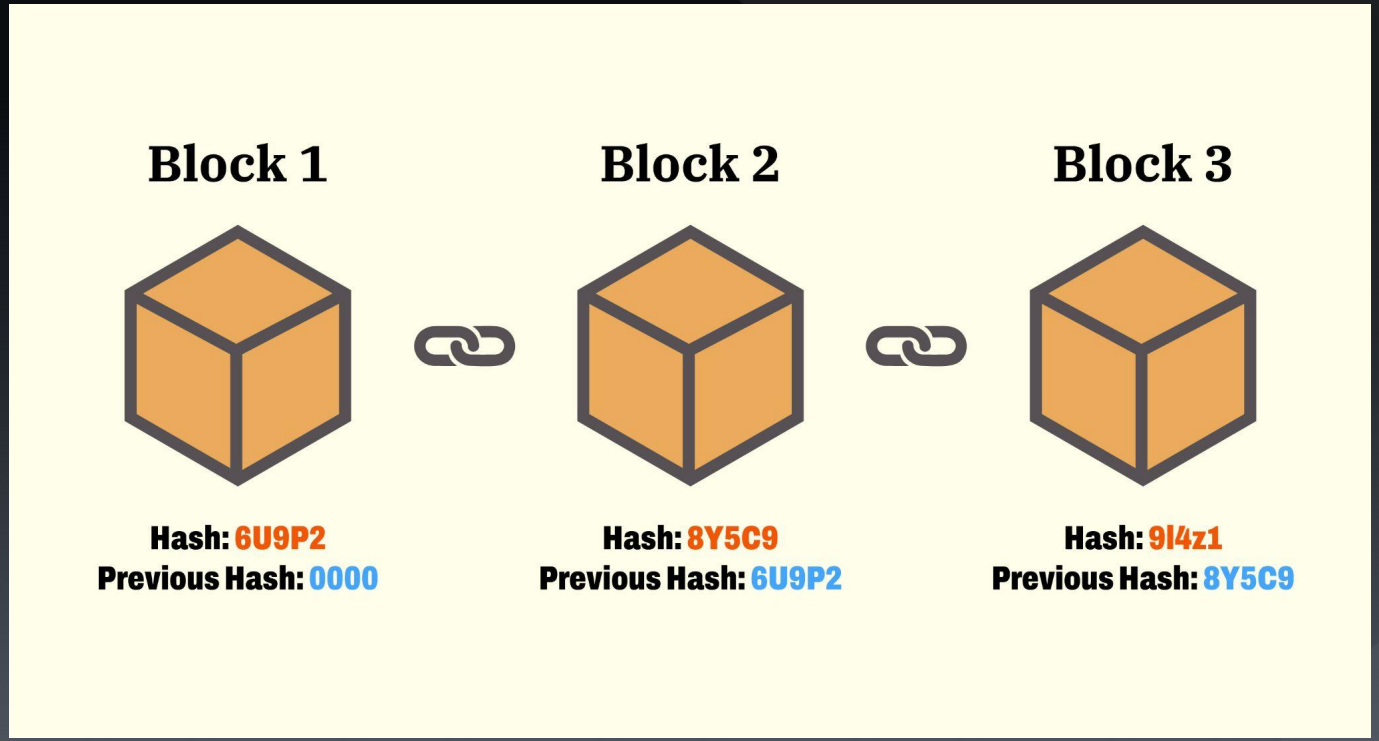
Blockchain - sequence of blocks recorded in a **digital ledger (database)** of transactions that is **distributed on a peer-to-peer network** and **does not require to rely on an external authority to validate the authenticity** and integrity of the data.

To date there is a total of 13,000 coins/tokens and thousands of blockchains!



Crypto 101: Blockchain = Database = Ledger

BINANCE



Crypto 101: Blockchain vs. Cryptocurrency

BINANCE

Blockchain ≠ Cryptocurrency

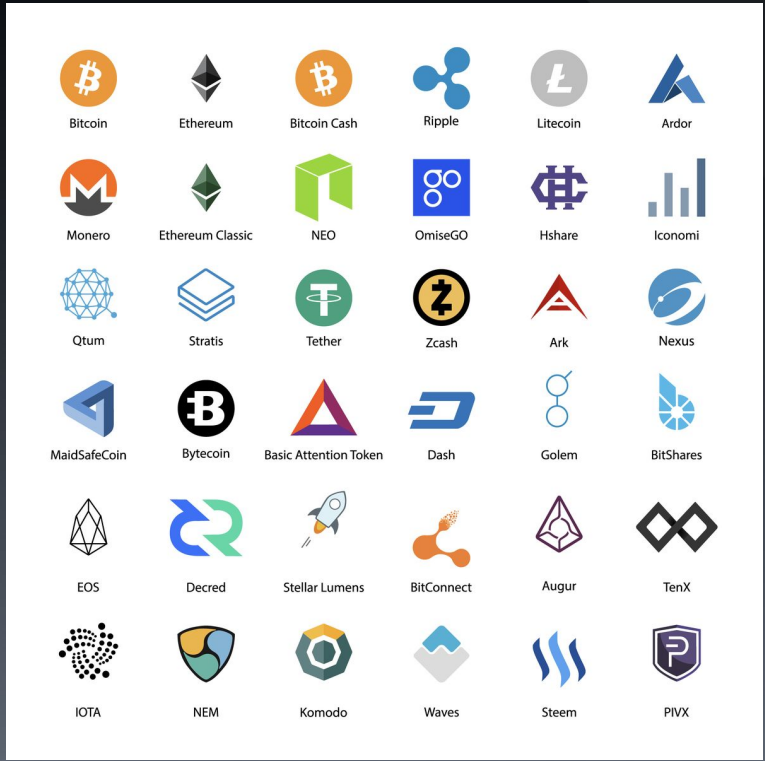
Transactions on a blockchain are usually economic, but any kind of information can be stored and verified in blocks.

Cryptocurrency - **digital currency secured by cryptography** and based on a distributed peer-to-peer network.

Crypto 101: Cryptocurrency

BINANCE

Blockchain ≠ Cryptocurrency



Crypto 101: Definitions

BINANCE

Address - string of alphanumeric text that designates the location of a particular wallet on the blockchain. Often a hashed version of a public key.

Examples:

- Bitcoin address formats:
  - P2PKH - 1..... 26-35 characters
  - P2SH - 3..... 26-35 characters
  - P2WPKH Bech32 – bc1.... (42 characters)
- Other cryptocurrencies have different formats:
  - 0x8bd671ff94fcf7caff7e396a3ac38db2720db3a7 (Ethereum)
  - TU6xb3E3GQaoJyeKLRafGFrZyQHF (Tron)

Crypto 101: Definitions

BINANCE

Transaction Hash / ID - a **unique string of characters given to every transaction** that is verified and added to the blockchain. In other words - it is an **identification number that labels each transaction** on the blockchain.

Examples:

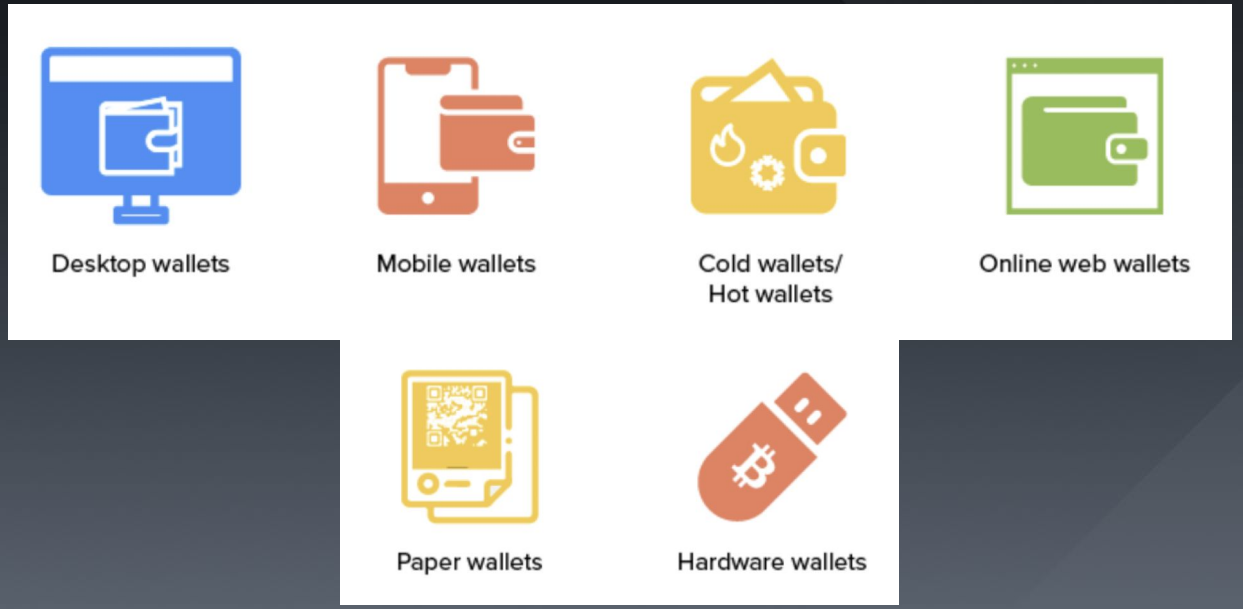
cca7507897abc89628f450e8b1e0c6fca4ec3f7b34cccf55f3f531c659ff4d79

952a44587cfc5b4131570215bb85ce4af160863656c2fc6d1f71e8052d053369

Crypto 101: Definitions

BINANCE

Wallet (≠ Address) - a device, program or other type of storage that stores cryptocurrency keys and allows their owner to access their crypto assets.



Crypto 101: Wallets – many types out there!

BINANCE

Crypto 101: Hardware Wallets

BINANCE

TREZOR

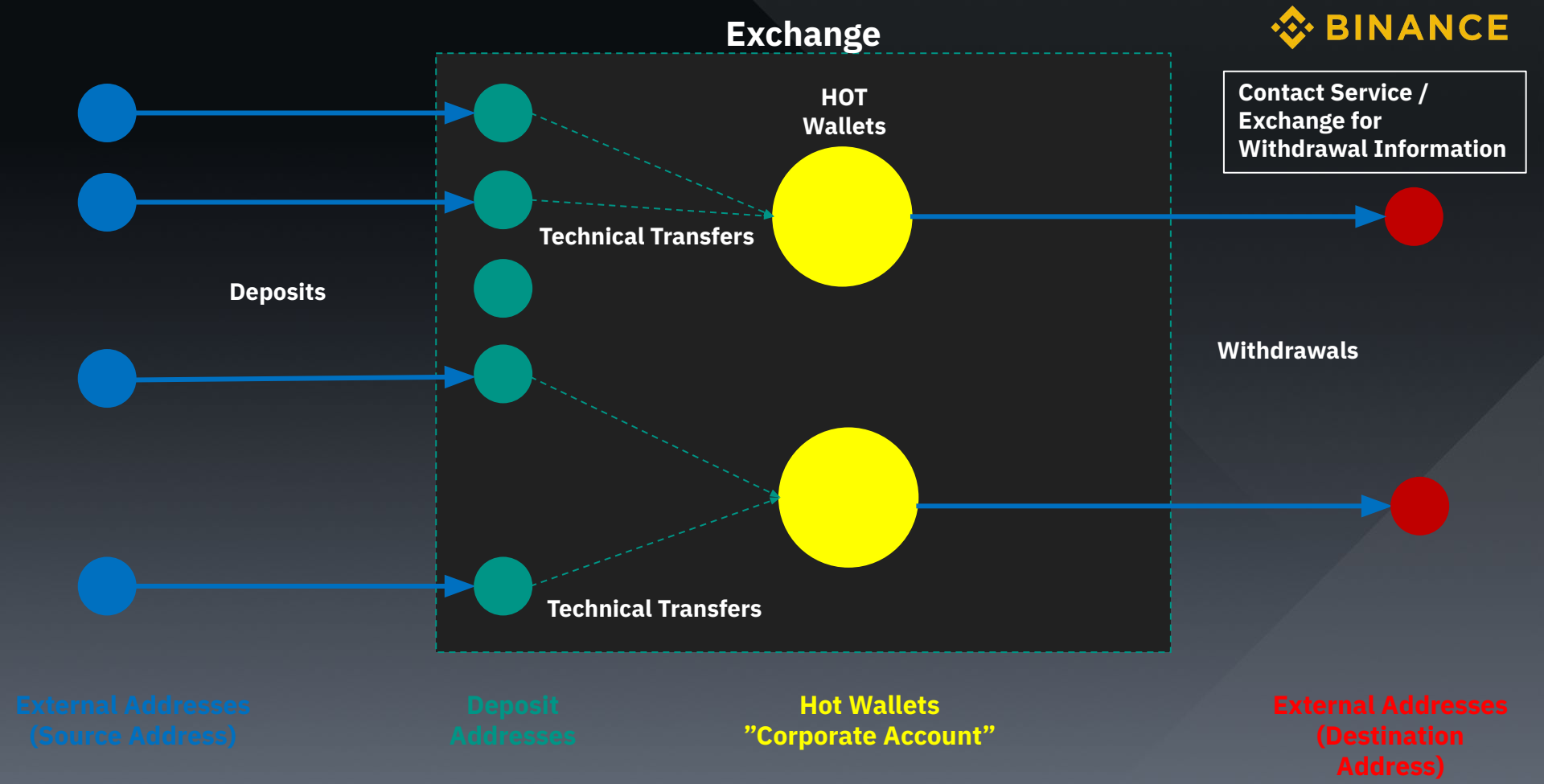
Ledger

keep key

SafePal

Crypto 101: Paper Wallet

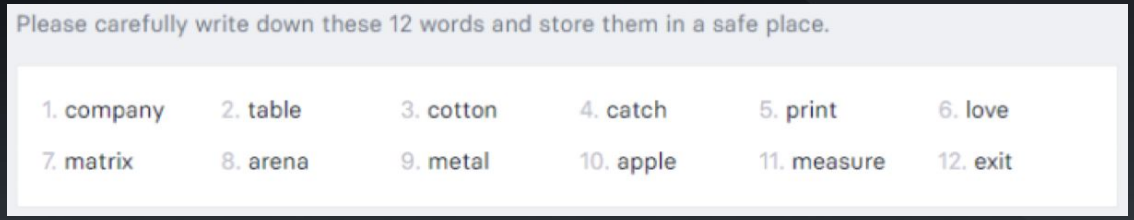
Crypto 101: Hot Wallet



Crypto 101: Definitions

BINANCE

Seed / Recovery Phrase - a sequence of random words that stores the data required to access or recover cryptocurrency on blockchain or crypto wallet.



BINANCE

Blockchain Explorers

Blockchain Explorers: understanding the ledger

BINANCE

{ "ver":1, "inputs":[{ "sequence":4294967295, "witness":"", "prev_out":
{ "spent":true, "tx_index":300978798, "type":0,
"addr":"1MAznqPhDauJLgTw8oP77t3UphrLMuca8d", "value":2092360, "n":1,
"script":"76a914dd46800d249ec587251c7d0b2f72923d26200f6888ac" },
"script":"483045022100e31aadb95978b3bbd1144c9c7beca4b288fe14d5b931891be620dc141856ba8202202
cf912bdc65e0e4891087382534528a0b696db4e795cea09b75df0afc3521c900121028ee0e07a5f37a00a7668a
bbbea1fd14d0b0c3bc8686d342ca9caa72adea0c1f3" }], "weight":896, "block_height":494607, "out":[
{ "spent":false, "tx_index":301707456, "type":0,
"addr":"3CmCP43K1VWQpHwbnAnyVACADUTMLwAnAs", "value":826282, "n":0,
"script":"a9147973c6ce1ff3a792765ba44c3a58a9c19d19b04a87" }, { "spent":true,
"tx_index":301707456, "type":0, "addr":"1Pa6kWj3BqXREosrYGUxuXDRjy1LUrHUc9",
"value":928434, "n":1, "script":"76a914f7954b44e9dab81f6f8bb47aae8f058ceaa59e2f88ac" }],
"lock_time":0, "size":224, "double_spend":false, "time":1510830077, "tx_index":301707456,
"vin_sz":1, "hash":"cbcea30d6ae61d675bc29fbb0ed2a953ee5603562990cab9832833dc4e69a7be",
"vout_sz":2}

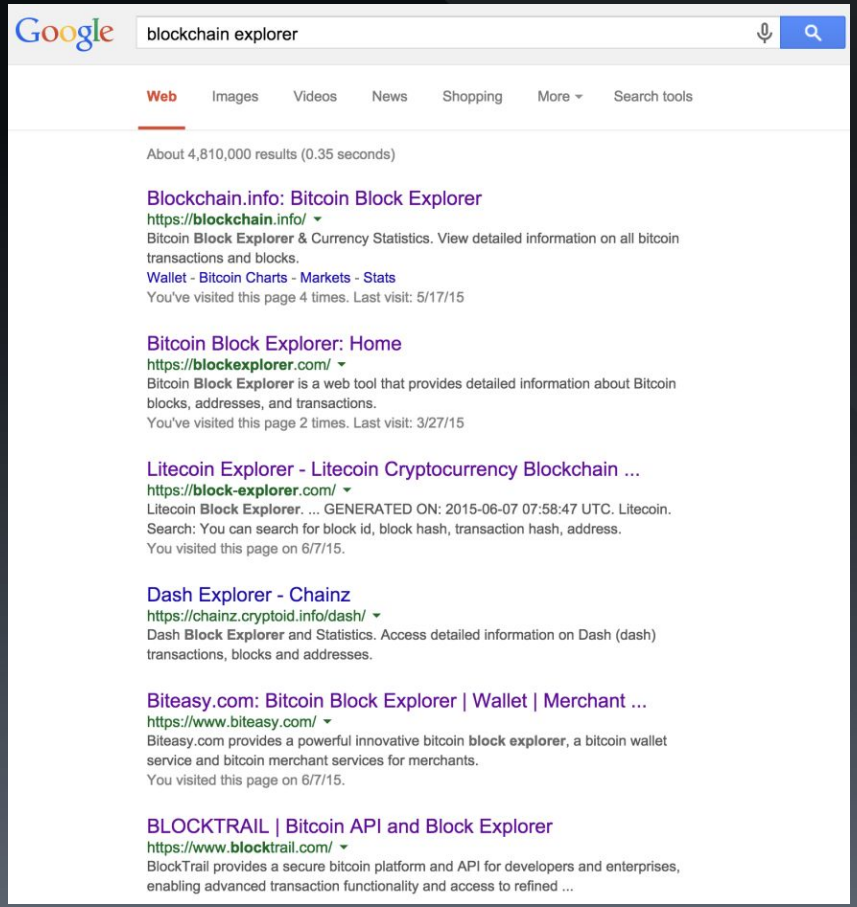
Blockchain Explorers: understanding the ledger

BINANCE

{ "ver":1, "inputs":[{ "sequence":4294967295, "witness":"", "prev_out":
{ "spent":true, "tx_index":300978798, "type":0,
"addr":"1MAznqPhDauJLgTw8oP77t3UphrLMuca8d", "value":2092360, "n":1,
"script":"76a914dd46800d249ec587251c7d0b2f72923d26200f6888ac" },
"script":"483045022100e31aadb95978b3bbd1144c9c7beca4b288fe14d5b931891be620dc141856ba8202202
cf912bdc65e0e4891087382534528a0b696db4e795cea09b75df0afc3521c900121028ee0e07a5f37a00a7668a
bbbea1fd14d0b0c3bc8686d342ca9caa72adea0c1f3" }], "weight":896, "block_height":494607, "out":[
{ "spent":false, "tx_index":301707456, "type":0,
"addr":"3CmCP43K1VWQpHwbnAnyVACADUTMLwAnAs", "value":826282, "n":0,
"script":"a9147973c6ce1ff3a792765ba44c3a58a9c19d19b04a87" }, { "spent":true,
"tx_index":301707456, "type":0, "addr":"1Pa6kWj3BqXREosrYGUxuXDRjy1LUrHUc9",
"value":928434, "n":1, "script":"76a914f7954b44e9dab81f6f8bb47aae8f058ceaa59e2f88ac" }],
"lock_time":0, "size":224, "double_spend":false, "time":1510830077, "tx_index":301707456,
"vin_sz":1, "hash":"cbcea30d6ae61d675bc29fbb0ed2a953ee5603562990cab9832833dc4e69a7be",
"vout_sz":2}

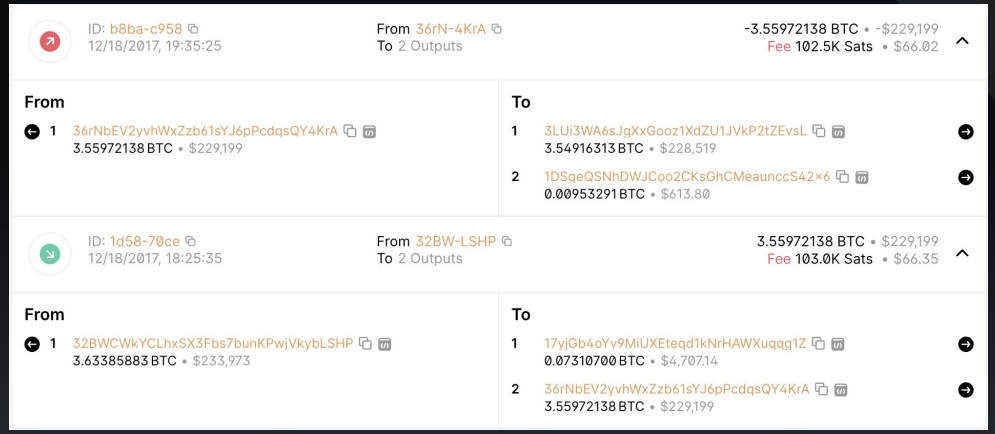
Blockchain Explorers: many possibilities

BINANCE



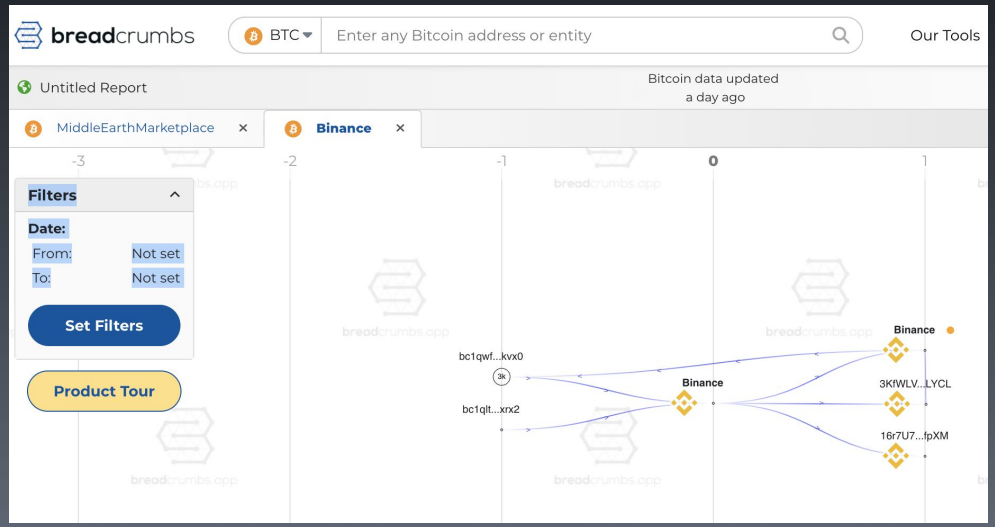
Blockchain Explorers: many possibilities

Blockchain Explorers: what do they show?



BINANCE

Blockchain.com



breadcrumbs

BINANCE

Understanding the transactions

Blockchain Models

BINANCE

BTC and the “UTXO” model - **Like Cash**

- Think of it like physical cash (banknotes)
- When you make a transaction, you don’t just take the exact amount—you spend whole coins and get "change" back.
- Example: If you have two $5 bills and need to pay $8, you give $10 and get $2 back.
- Each transaction creates new "outputs" that can be used in future transactions.

ETH Account-Based Model - **Like a Bank Account**

- Works like a **bank account**—your balance updates directly.
- Transactions just **subtract from one account** and **add to another** without needing to track individual "coins”.
- Example: If you have $100 in your account and send $30, your balance updates to $70.

1 Input, 1 output:

BINANCE

281b0e73b30f2bbb4f1859ed432cceb9e1431418794b27247f72ea834da73268

16Nj2vwbcidN1miG5qFvY2iUSmeZ1cKTzy (0.01098 BTC - Output) → 1KejHZHms744ua6rcFAfo211c3HS71JhyS - (Spent) 0.01097309 BTC

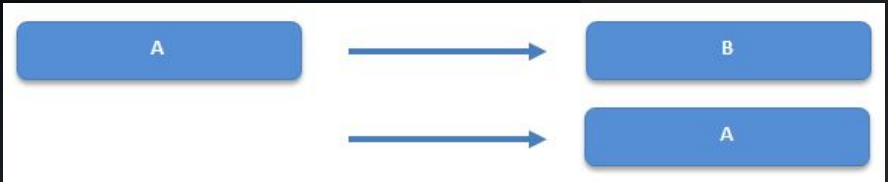
0.01097309 BTC

Summary	
Size	223 (bytes)
Received Time	2016-05-15 20:16:39
Included In Blocks	412153 (2016-05-17 11:38:29 + 2,362 minutes)
Confirmations	8154 Confirmations
Relayed by IP	46.101.15.184 (whois)

Inputs and Outputs	
Total Input	0.01098 BTC
Total Output	0.01097309 BTC
Fees	0.00000691 BTC
Estimated BTC Transacted	0.01097309 BTC
Scripts	Hide scripts & coinbase

1 Input, 2 output:
a) Input address features in the output

BINANCE



Transaction View information about a bitcoin transaction

f157b7335528164a31710798133b7477c4c366f643f045f69d7fcc28f9448e87

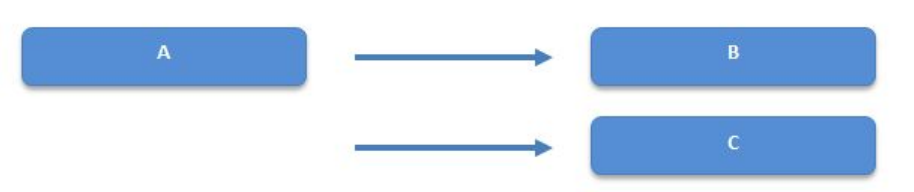
39RwB8D6fg8mA1m7VGAGobKRtZM1vHV99F (0.49299667 BTC - Output)

3H6NEkRy4ukmdhTjS85hERXYRMrkb9Luo2 - (Spent) 0.0416 BTC
39RwB8D6fg8mA1m7VGAGobKRtZM1vHV99F - (Spent) 0.45089667 BTC
0.49249667 BTC

Summary	
Size	333 (bytes)
Received Time	2016-06-26 08:19:11
Included In Blocks	418033 (2016-06-26 08:32:09 + 13 minutes)
Confirmations	2239 Confirmations
Relayed by IP	45.55.170.207 (whois)

Inputs and Outputs	
Total Input	0.49299667 BTC
Total Output	0.49249667 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.0416 BTC
Scripts	Hide scripts & coinbase

1 Input, 2 output:
b) Input address does not feature the output



08ecd5354a0aa3acb5e94f53ebbe2bbbbcc7403899207f27d8572a83b70b0e7f

1KejHZHms744ua6rcFAfo211c3HS71JhyS (0.5 BTC - Output)

1KfrRC4WN9wJJxvCn3Z9vQbpR8xQCFrqYR - (Spent) 0.01 BTC
122PeFgD4MdoCYN9ZEB4z6DxcnzaG8BpWS - (Spent) 0.48999502 BTC

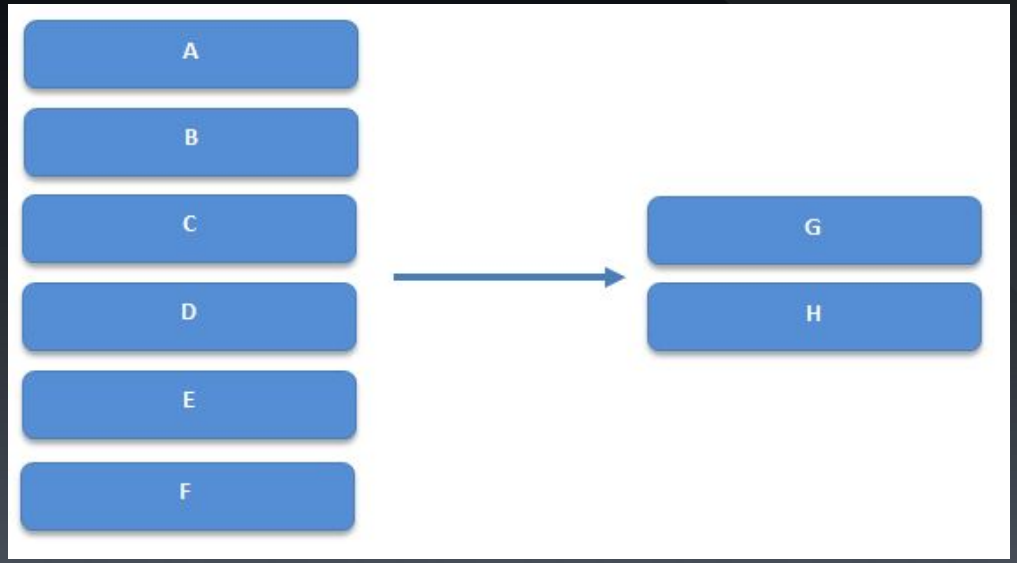
0.49999502 BTC

Summary	
Size	225 (bytes)
Received Time	2016-01-02 14:36:22
Included In Blocks	391442 (2016-01-02 20:52:59 + 377 minutes)
Confirmations	28840 Confirmations
Relayed by IP	192.146.137.1 (whois)

Inputs and Outputs	
Total Input	0.5 BTC
Total Output	0.49999502 BTC
Fees	0.00000498 BTC
Estimated BTC Transacted	0.01 BTC
Scripts	Hide scripts & coinbase

Multi-input Transaction

BINANCE



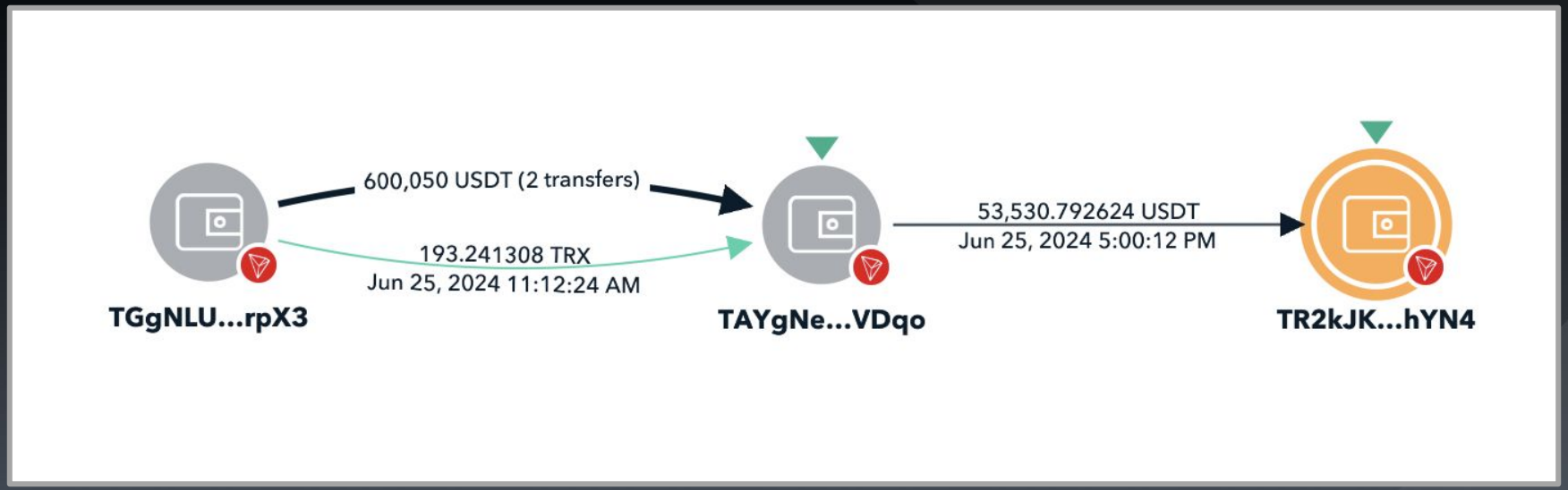
Interpreting Account Based Transactions

BINANCE

Token Movement	- Native tokens - Non-native tokens (e.g., stablecoins, NFTs)
Gas Fees	- Transaction fees that users pay to process transactions or execute smart contracts on a blockchain network
Gas Tokens	- Tokens used to pay for transaction fees - Usually native tokens (e.g., ETH, BNB, SOL)

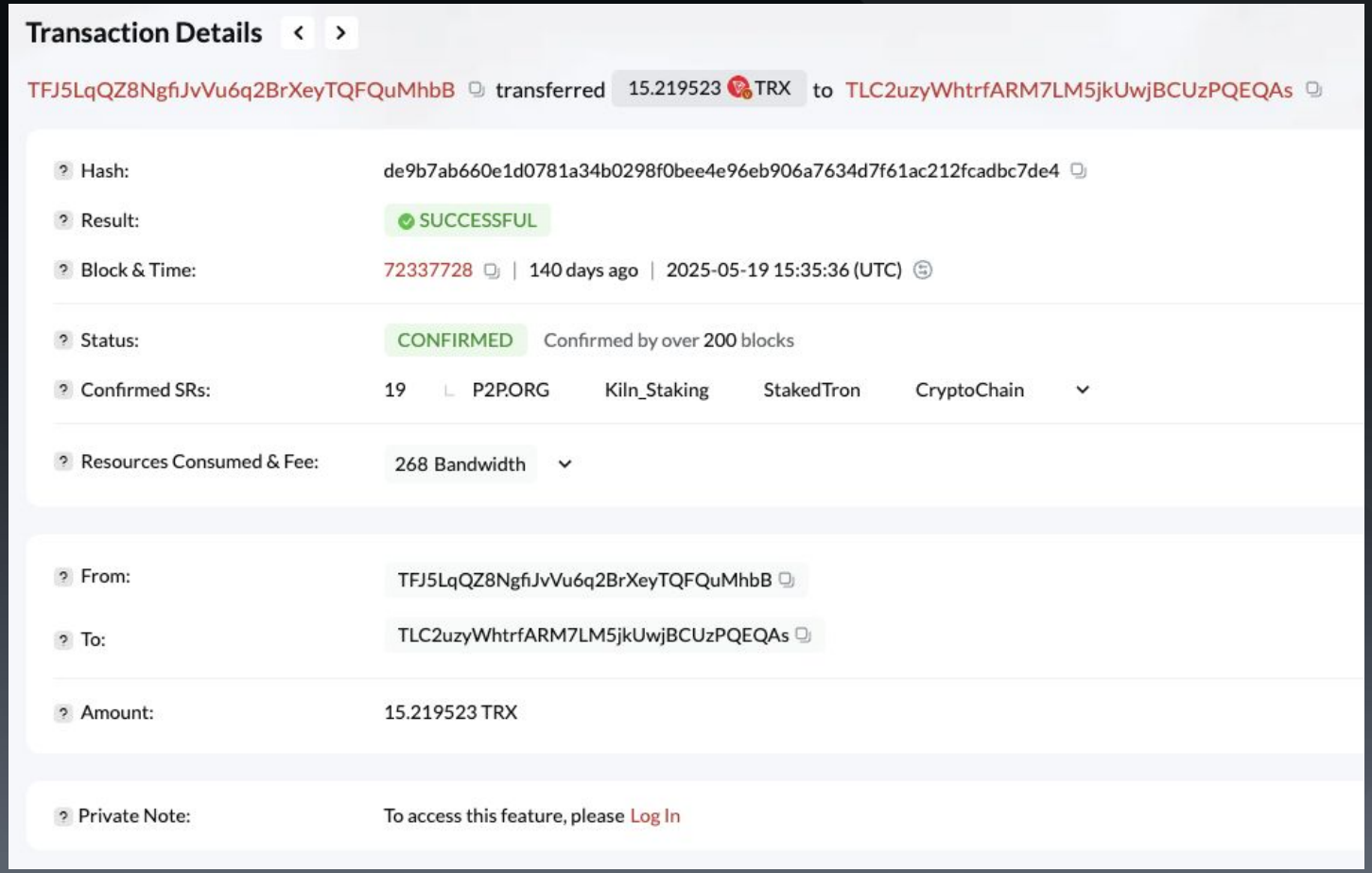
Interpreting Account Based Transactions

BINANCE



Can AI Help Understand Blockchain Transactions?

BINANCE



Explain what happened here.

This is a screenshot of a **TRON (TRX) blockchain transaction** on a TRON explorer. Here's a breakdown of what happened:

🔄 Transaction Summary

- **Sender:** `TFJ5LqQZ8NgfjJvVu6q2BrXeyTQFQuMhbB`
- **Recipient:** `TLC2uzyWhtrfARM7LM5jkUwjBCUzPQEQAs`
- **Amount Transferred:** `15.219523 TRX`
- **Transaction Fee:** 268 Bandwidth (free in TRON's resource system, no TRX was burned)
- **Transaction Result:** ✅ **SUCCESSFUL**
- **Status:** ✅ **CONFIRMED** (Confirmed by over 200 blocks)
- **Block Number:** `72337728`
- **Date & Time:** `2025-05-19 15:35:36 (UTC)`
- **Confirmed Super Representatives (SRs):** 19, including:
  - `P2P.ORG`
  - `Kiln_Staking`
  - `StakedTron`
  - `CryptoChain`

📌 Additional Notes:

- The **transaction hash** is a unique ID:
  `de9b7ab660e1d0781a34b0298f0bee4e96eb906a7634d7f61ac212fcadbc7de4`
- The **bandwidth fee** used (268) means the sender likely had enough bandwidth or staked TRX, so they didn't need to pay TRX as a fee.

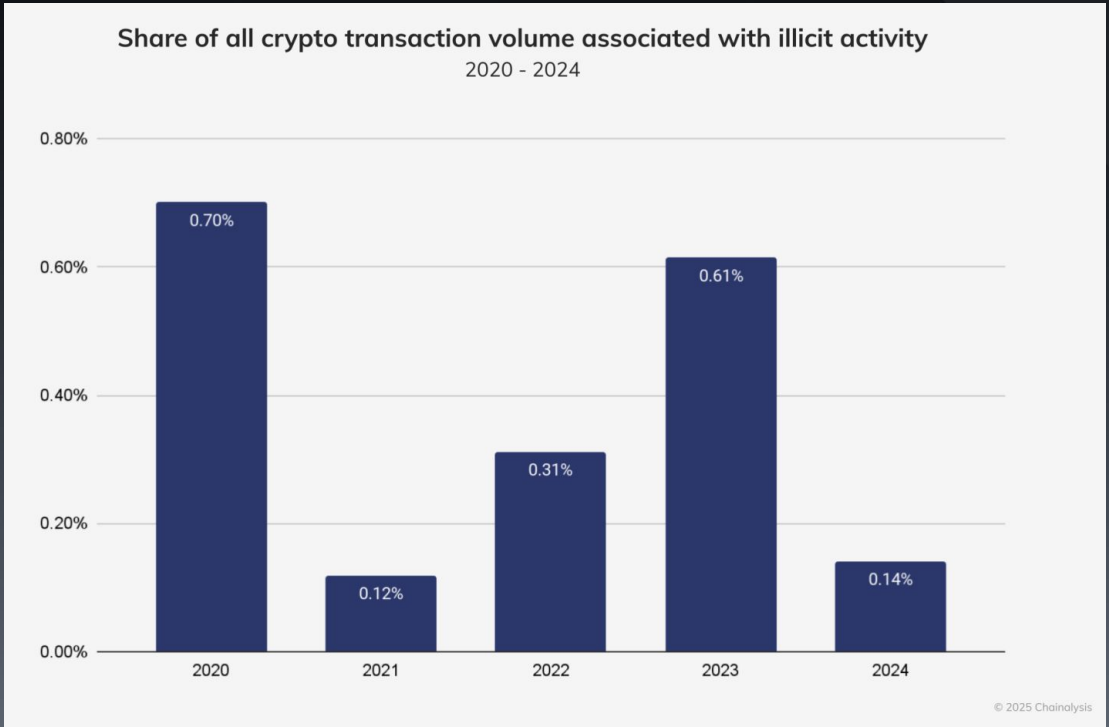
BINANCE

(Ab)use of Crypto

(Ab)use of Crypto

General misconception - crypto is all illicit, but...

- Illicit share of all crypto volume in 2024 - 0.14% (compared to estimated 2-5% of World's GDP, i.e., Traditional Finance)



(Ab)use of Crypto

BINANCE

1 Money Laundering (Dark Economy)

- Financial crime enabler
- Complex layering, use of intermediary services (mixers, online gambling, darknet markets
- Cashing out (high-risk exchanges, abusing compliant exchanges)
- Use of stablecoins to avoid price fluctuations, estimated 63% of all illicit transactions

2 Scams

- Emerging variety of *modi operandi*
- Business-like criminal operation models, call centers
- HuionePay / Huione Guarantee - ML, scam, crime facilitator

(Ab)use of Crypto

BINANCE

3 Hacks / Stolen Funds

- API hacks
- Crypto bridge hacks
- DPRK-attributed actions - estimated 61% of all stolen funds in 2024
- Rise of physical thefts through kidnappings / home invasions

4 Terror-Financing

- Three-way convergence: hawala networks, crypto, traditional finance
- Early technology adopters
- Increasing use of TRX chain and USDT
- Growth in Europe linked to white supremacists and nationalist ideologies

(Ab)use of Crypto

BINANCE

5 CSAM

- Understudied part of crypto crime
- CSAM vendors adopting Monero (privacy-coin)
- CSAM-scams

6 Ransomware

- Overall decrease in ransomware payments
- Attacking bigger targets to collect larger amounts
- Increase of $1M payments
- State-sponsored activity

(Ab)use of Crypto

BINANCE

7 State-Sponsored Attacks

- Complex and elaborate
- Highly tailored, difficult-to-detect social engineering campaigns
- Deployment of malware
- High-scale attacks

Tactics:

- Extensive pre-operational research
- Individualized fake scenarios
- Impersonations

(Ab)use of Crypto

BINANCE

8 Sanctions Evasion

- Increased crypto use to ensure financial lifeline
- Use of ML-networks / mule accounts (accounts for sale)
- Abuse of VASP controls
- Cashing out through OTC / underground banking

9 Rise of Physical / Real-Life Attacks

- Rise of urgent LE requests in crypto-related kidnapping cases
- Correlation between crypto price sures and physical attacks
- Usual victims - individuals with public exposure or presumed direct access to digital assets; crypto investors, executives, professionals, enterpreneurs

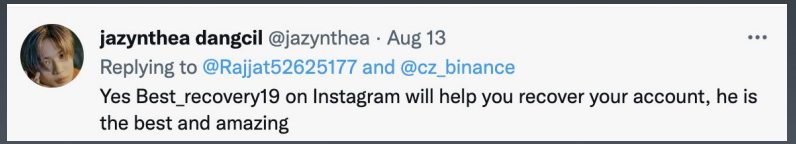
BINANCE

Scam Investigations

Investigating Scam

Modus Operandi - Investment Scam

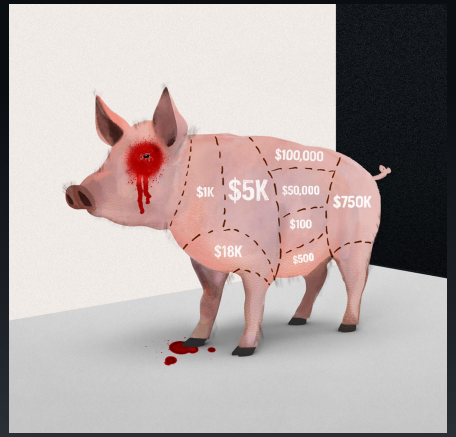
BINANCE

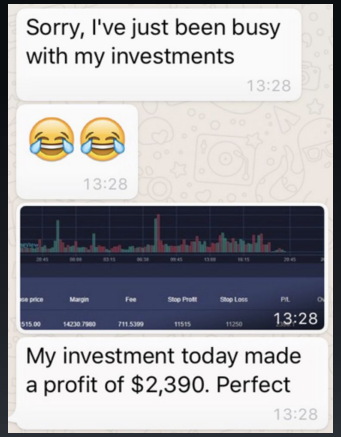


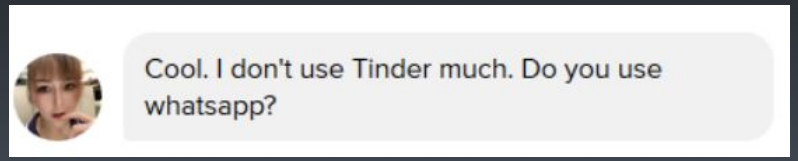
Usual process:
- Receive a call / sign-up online
- Get a personal investment agent
- Graceful offer to take care of all initial steps
- Remote access to victim's computer
- Initial investment → small returns → more investment → attempts to withdraw → fees to process the withdrawal
- **BONUS**: Fund recovery "agents" / companies → even more scams!

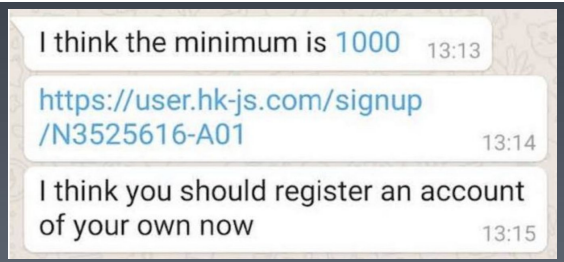
Investigating Scam

Modus Operandi - Pig-Butchering







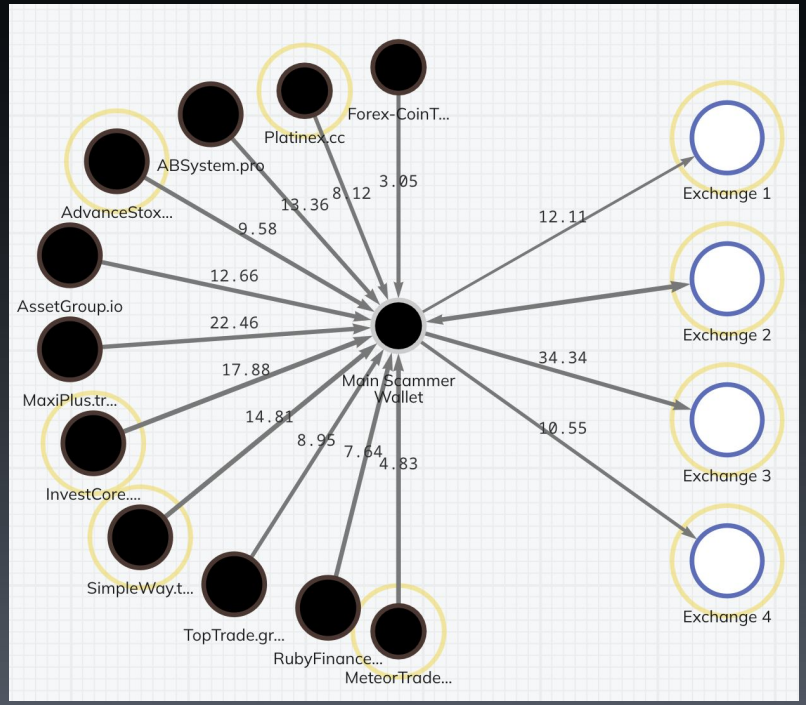


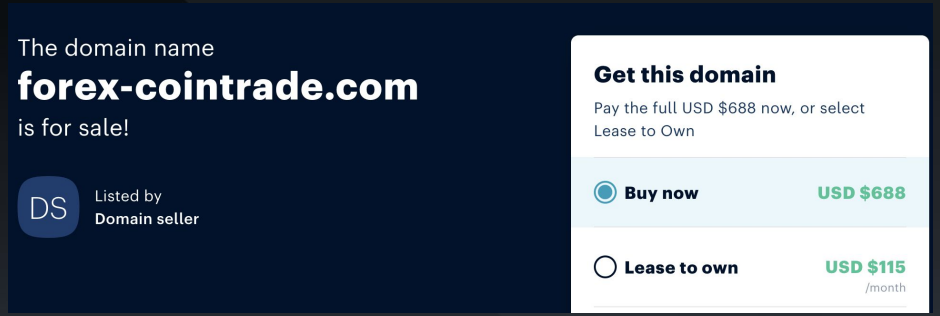
- Finding the victim (social media)
- Building trust
- Convincing to trade crypto
- Fattening "the pig"
- Failure to withdraw funds

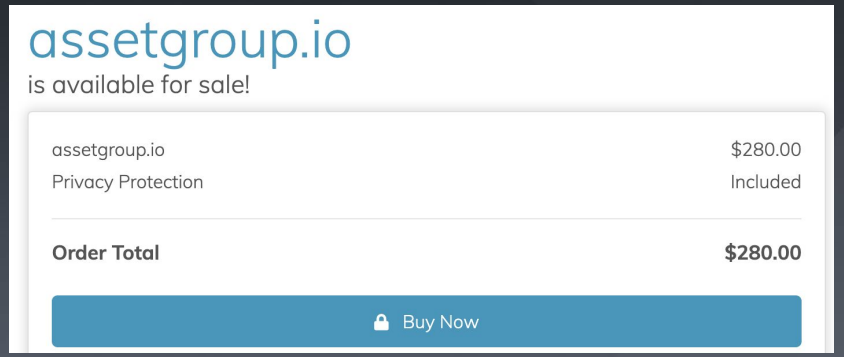
Investigating Scam

One Criminal Group = Multiple Scam Sites?

BINANCE







Investigating Scam

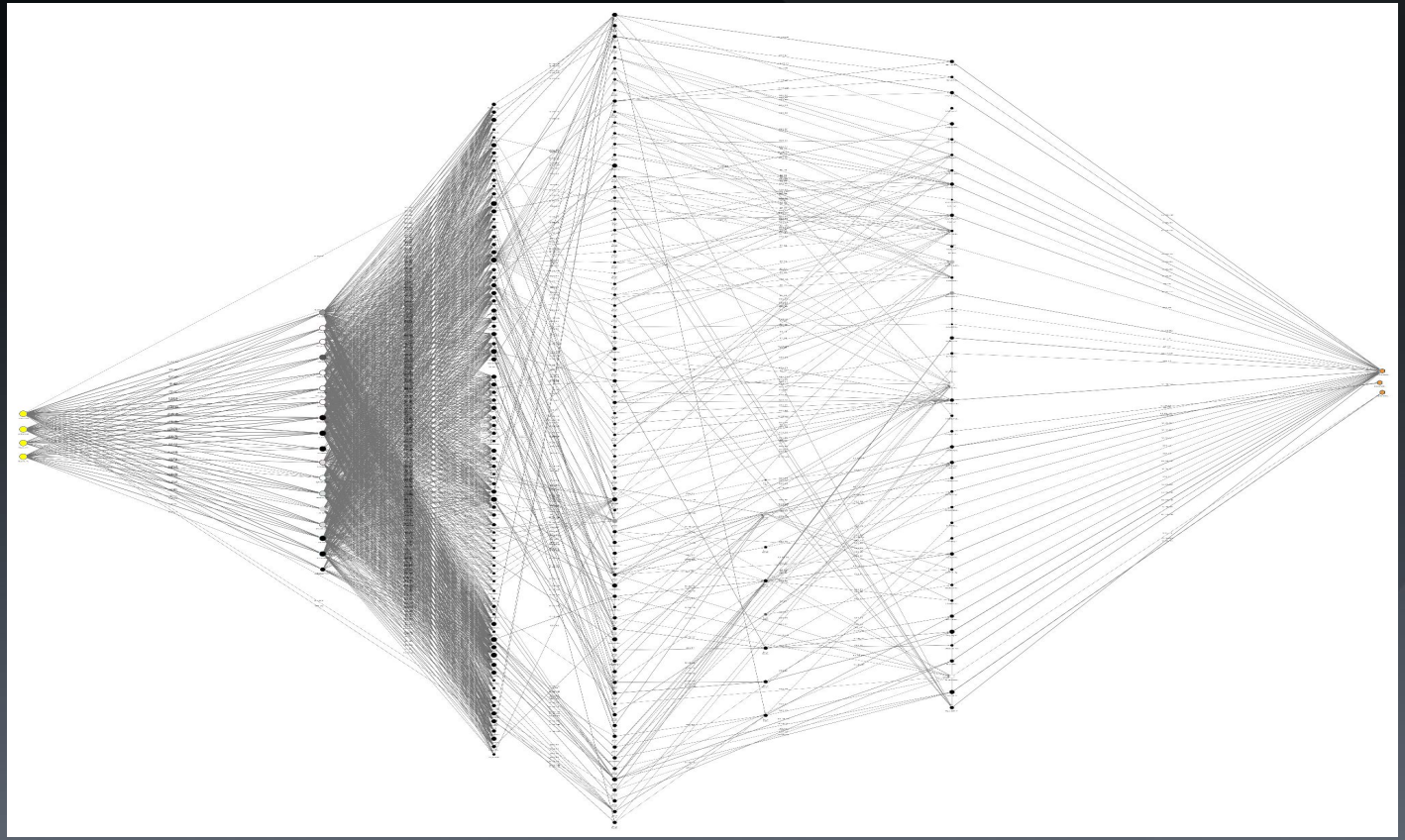
Tip of the Iceberg

BINANCE

Investigating Scam

Flow of Funds

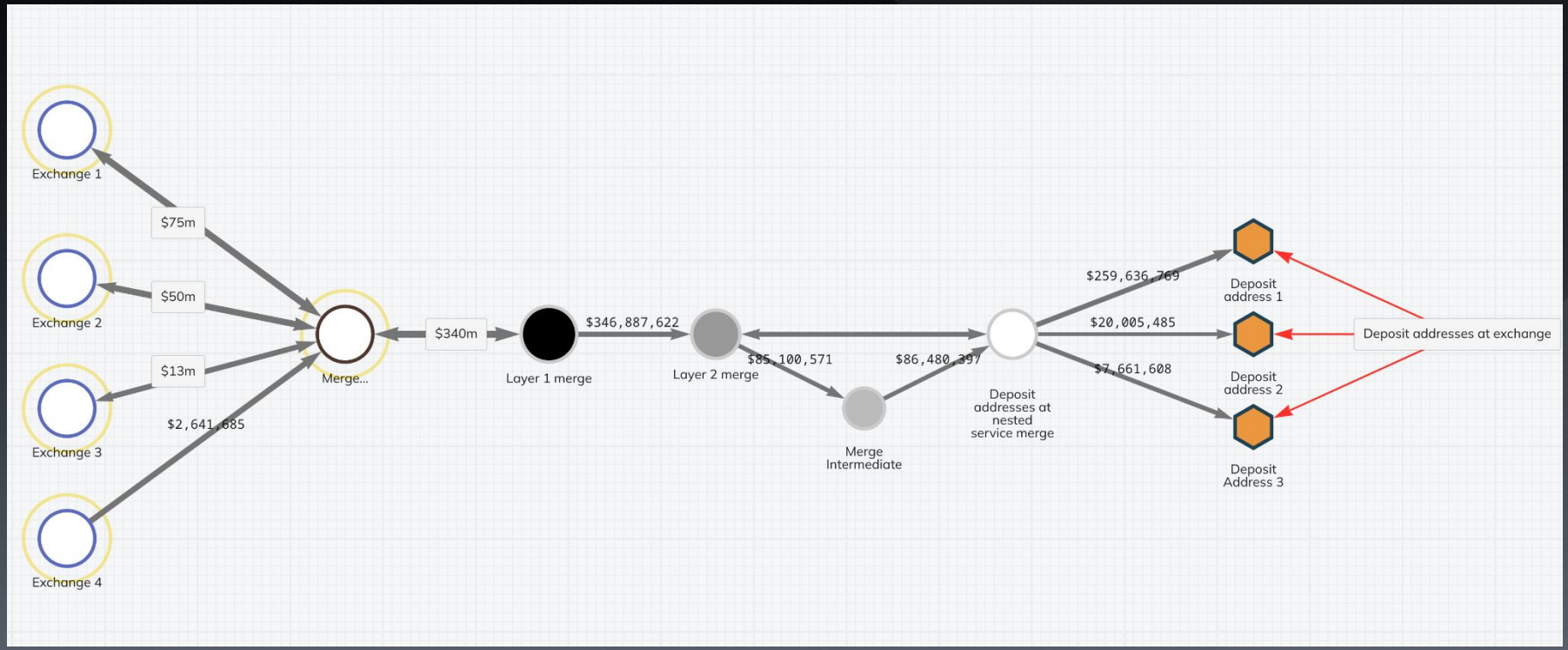
BINANCE



Investigating Scam

Flow of Funds (cleaned-up)

BINANCE



Investigating Scam

Identification

BINANCE

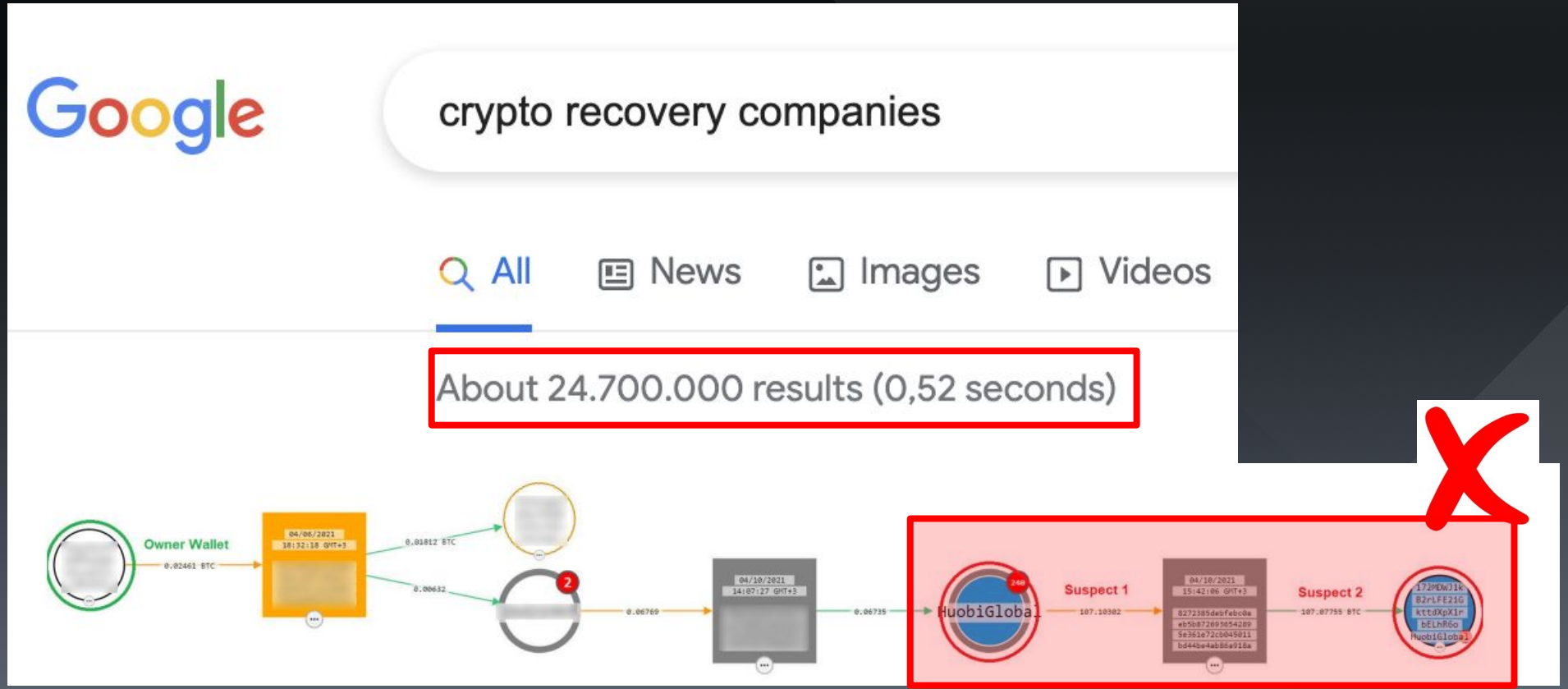
- **Behavioral Analysis**
  - How do scam networks operate?
  - Attack vectors, modi operandi.
  - Developing tactics and techniques to stop the criminals.
- **Predictive Modelling**
  - Scams with similar MO's
  - What addresses will be generated next?
- **Proactive Engagement with Public and Private Sector: Intelligence Sharing**
- **Awareness and Education**

- **Tracing funds**
  - Follow the money (lifo), or trace the source of funds (via gas fees): network analysis
- **Investigations at account level**
  - Linked accounts
  - Investigating User's Behavior at exchange
- **Prevention Measures**
  - Warning Questionnaires & Pop-ups
  - Cool-down periods
  - Withdrawal blacklists

Challenges

Third-party Tracing / Recovery Companies

BINANCE



Anti-Fraud Law Enforcement Support

BINANCE

BINANCE

BINANCE SUPPORTS $47 MILLION FREEZE

In APAC Pig Butchering Scam Investigation

BINANCE

BINANCE AND TOKOCRYPTO COLLABORATE WITH BARESKRIM TO UNCOVER MAJOR CRYPTO FRAUD, SEIZE $200K

BINANCE

INDIA'S ENFORCEMENT DIRECTORATE CRACKS DOWN ON GAMING APP SCAM WITH BINANCE'S SUPPORT

BINANCE

AHMEDABAD POLICE, BINANCE TACKLE $200K SCAM

Cross-border network exposed in South, SEA

Customer Anti-Fraud Protection Levels

CONFIDENTIAL

BINANCE

Wake-Up Call

Chat Dissuasion

24H Cooling-Down

1H Cooling-Down

Freezing Small Amounts of Commission

Global Malicious Address Database Alert

Interactive Risk Assessment Form

Customized Pop-up Notification

Awareness-Raising: Know Your Scam Series

BINANCE

BINANCE

Know Your Scam

A definitive guide to crypto's most prevalent scams

BINANCE

Know Your Scam

*Protect yourself from **Binance** imposter scams*

BINANCE

Know Your Scam

How to Identify and Avoid Ponzi Schemes

BINANCE

Know Your Scam

How to Identify Fake Shopping Websites

BINANCE

Know Your Scam

How to Spot and Protect Yourself From Romance Scams

BINANCE

Know Your Scam

Job Scams to Watch Out For

BINANCE

Know Your Scam

Money Transfer Scams in Crypto

BINANCE

CONFIDENTIAL

BINANCE

Crypto Services: Internal Controls & Cooperation

Crypto Crime Risk Mitigation

BINANCE

1 Internal procedures: KYC/KYB, AML/CFT policies, Transaction Monitoring, Blacklisting

2 Law Enforcement response, proactive investigations

3 Public-private partnership

4 Capacity building + awareness-raising

Abuse of AI Technologies and Deep Fakes

Abuse of AI and Deep Fakes for KYC Verification

BINANCE

Usual Deepfake Techniques used to attempt circumvention of KYC verification controls:

- Mask Attack
- Face Animation
- Image Distortion
- Face Swapping with Similar / Same Background

Law Enforcement Response

Data Production / Freezing / Seizure Considerations

BINANCE

1 Is the request in line with the **GDPR principles and requirements**?

Lawful basis: What are the legal grounds for a request? Are there limitations to exercise domestic powers cross-border?
Necessity: What are the reasons for a request?
Proportionality: What is the scope of data absolutely necessary? Are there other lawful ways to obtain the data?

Data Production / Freezing / Seizure Considerations

BINANCE

2 Is the request addressed to the correct legal entity

For Account Freezes and Seizures - requests need to be addressed to appropriate **operating entity** that handles user assets.

For Account Records Production - requests need to be addressed to appropriate **data controller**.

Tip. Address your request to Nest Services Limited → send through Kodex → You will get guidance.

Data Production / Freezing / Seizure Considerations

BINANCE

3 How confident are you in the tracing that led to Binance?

- Can you account for all hops in between? Any change of ownership of funds? Any unidentified services inbetween?

- Can funds subject to seizure be linked to victim's lost funds? Are there any other victims?

- Was third party-tracing involved? Were findings verified?

Channels of Cooperation

CONFIDENTIAL

BINANCE

Binance accepts requests submitted via

Law Enforcement Request Portal (Kodex) only.

For prior consultation / coordination / flagging exigent requests - investigations@binance.com

Exigent request - immediate threat to life or public safety / TF / CSAM.

Requests: Do's and Don'ts

CONFIDENTIAL

BINANCE

1 Submit requests via Kodex Portal
https://app.kodexglobal.com/binance/signup
- For prior consultation / coordination - investigations@binance.com

2 Always include your full details to expedite the process
- Name, Position, Contact Information

3 Attach a copy of the signed Letterhead / Subpoena / Court Order

4 Include description of suspicious activity / modus operandi

Requests: Do's and Don'ts

BINANCE

5 Provide the starting point

6 Avoid overly broad requests (fishing expeditions)
- Broad requests will get pushed back and additional justification will be requested

7 Provide unique identifiers

8 Add csv/excel or other copyable document
- No bullet-points / numbering

The more precise you are, the better we can assist!

Awareness-raising

BINANCE

Welcome to Crypto

We're on a mission to educate the masses on the transformative potential of cryptocurrency and blockchain technology. On this website, you'll find over 470 articles covering everything from computer security to economics. Oh, and they're in **30 different languages**.

We know it can be a little daunting when you're new. This guide is here to gently introduce you to some of the key concepts you need to kick-start your journey into the world of blockchain tech.

Without further ado, let's dive down the rabbit hole.

BINANCE

Binance Launches Global Law Enforcement Training Program

Questions?

BINANCE

Co-funded by
the European Union

Bavarian State Ministry of Justice

#DIGITALISATION AND #ARTIFICIALINTELLIGENCE IN CRIMINAL JUSTICE

Thessaloniki 9-10 October 2025

Data retention

data protection

vs.

the risk of systemic impunity

Data protection vs. the risk of systemic impunity

EDRi
The CJEU jeopardises essential privacy protections to accommodate false law enforcement claims

BBC Sign in
NEWS
Top EU court rejects EU-wide data retention law
8 April 2014

Structure of presentation

- **Introduction**
  - Definition
  - State of play of legislation
  - Significance for the investigation and prosecution of crimes
- **Case law of the Court of Justice of the EU**
  - Basic considerations of the CJEU
  - State of play
  - Resulting framework for national legislation
- **Current legislative developments**

What does „data retention“ mean?

Obligation for **providers of electronic communications services** to

- **store traffic/location data** (not subscriber/content data) for a certain period of time and to
- **provide access** to authorities under certain conditions

Current legal framework

EU-level:

None (Data Retention Directive 2006/24/EC declared invalid by CJEU decision of 08.04.2014 (C-293/12, C-594/12 Digital Rights Ireland)

Member States:

EUROJUST
European Union Agency for Criminal Justice Cooperation

Fragmentation (Eurojust/EJCN overview of 11/2024 https://www.eurojust.europa.eu/publication/effect-court-justice-european-union-case-law-national-data-retention-regimes-judicial-cooperation): most MSs have law in place, but no recognisable common pattern

Significance for the investigation of crimes

Identification of perpetrators through **subscriber data allocated to dynamic IP-address** (+port number/time stamp), e.g. based on NCMEC (National Center for Missing and Exploited Children)-notifications

BKA- position paper of July 2023:
https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html

success rate for the allocation of IP-addresses to concrete subscribers in NCMEC-cases:

- currently (without any data retention): 41%
- with a hypothetical data retention period of two weeks: 84,5 %

Case law of the CJEU – procedural setting

- **Preliminary rulings on** national data retention law in Member States

- Questions referred to CJEU by national courts concern
  - **interpretation of Article 15(1) of Directive 2002/58/EC** (e-privacy Directive)
  - read in the light of **Charter of fundamental rights**
    - Art. 7 (Respect for private life)
    - Art. 8 (Protection of personal data)
    - Art.11 (Freedom of expression and information)

Case law of the CJEU – procedural setting

Article 15(1) of Directive 2002/58/EC

"Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in (...) this Directive when such restriction constitutes a **necessary, appropriate and proportionate measure** within a democratic society to safeguard **national security** (i.e. State security), **defence, public security, and the prevention, investigation, detection and prosecution of criminal offences** (...). To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. (...)"

Case law of the CJEU – Milestone decisions

- **Digital Rights Ireland** (C-293/12 and C-594/12) 08.04.2014: Data retention Directive is disproportionate and invalid

- **Tele 2 Watson** (C-203/15 and C-698/15) 21.12.2016: general and indiscriminate retention of all traffic and location data for the purpose of fighting serious crime violates EU-law

- **Quadrature du Net** (C-511/18 and C-512/18) 06.10.2020 exception for IP-addresses

- **Hadopi** (C-470/21) 30.04.2024 expansion/clarification of the exception for IP addresses

Case law of the CJEU – Basic considerations

Balance between the various interests and rights at issue:

Rights/interests interfered with by data retention	Rights/interests protected by data retention
Respect for private life	Efficiency of combating crime
Protection of personal data	Obligation to protect (the rights of minors)
Freedom of expression and information	

Case law of the CJEU – Basic considerations

General and indiscriminate retention of all traffic and location data for the purpose of fighting crime

is NOT in line with EU-law

Case law of the CJEU – Key arguments

- As an exception Article 15(1) of Directive 2002/58/EC has to be interpreted narrowly; **the exception mustn´t become the rule**

- **Storage is an interference by itself**, independently of a possible later use of/access to the data

- **Traffic/location data no less sensitive than content** regardless of retention period (provides means to establish profiles of individuals)

Case law of the CJEU – Key arguments

- **Proportionality** requires:
  - Precise rules on **scope of interference and safeguards**
  - **Connection** between the data to be retained and the objective of the legislation

Resulting limits for legislation

Objective of prosecuting serious crime does not justify indiscriminate general data retention; **exceptions:**

- General and indiscriminate retention of **data relating to the civil identity of users**
- **Quick freeze**
- **Targeted retention of traffic and location data** which is limited according to the categories of persons or using a geographical criterion
- General and indiscriminate **retention of IP addresses** assigned to the source of an internet connection

Retention of IP adresses - Hadopi decision

- Retention of (source) IP addresses also for the purpose of combating **general crime (not only serious crime)**

  Precondition: "watertight" separation from other stored data

- **Access by administrative authority** for the sole purpose of identifying perpetrators without prior judicial review

CJEU (C-470/21, par. 119) **"…not to allow such access would carry a real risk of systemic impunity…"**

Current legislative developments

Impact assessment by the European Commission

(https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14680-Data-retention-by-service-providers-for-criminal-proceedings-impact-assessment_en)

Objective:

„(…) ensure the availability of certain categories of non-content data for the purpose of carrying out successful criminal investigations and prosecutions (…)"

Policy options:

- soft law measures
- legislative measures

Thank you for the attention!

Michael Rothärmel
Email: michael.rothaermel@stmj.bayern.de

Co-funded by
the European Union

VIDEOCONFERENCING
IN THE ERA OF ARTIFICIAL INTELLIGENCE

Sabina Klaneček, October, 2025

sabina.klanecek@dt-rs.si


Judge Emily Mis...
D - Amy Stewa...
D - John Stone
Keith Dean
P - Matthew Pe...
21 - Suzy Jones
04 - Tabatha W...
17 - Dwayne Ha...
08 - Emily Tang
09 - Shane Dier...
22- Jeff Bulla
15 - Patty Youn...
19 - Rob Cathri...
14 - Sharyn Cla...
23 - Mary Ann ...
06 - Richard Dia...
18 - Kathleen Li...
07 - Carlos Silv...
28 - Linda Ros...
26 - Kathleen H...
02 - Angela Bar...
27 - Angela Pyl...
24 - Maribel Da...
05 - sheila tho...
10 - Chavda, D...
zoom
DO NOT RECORD


Christopher Tran (Guest)
#MR MEL 11/03 ZR (Seats 10)
Naomi Wootton (Guest)
Judge A Kelly
Participants: 17

VIDEOCONFERENCING - EQUIPMENT

Web applications (Zoom, MS Teams, Webex, …)

- Meetings
- Personal use …

Professional equipment (Cisco, Polycom,…)

- Courts

Mobile units

WHEN

- Witness/Party in a proceeding
- Expert
- Hospital / Social center
- Prison
- Hidden witness (undercover police officer)
- Child victims
- Documents
- Videos/recordings

PREPARATION / TEST

Prepare – book the courtroom/equipment

Exchange information

- Contact data (email, name of the technician, his contact-email, phone…)
- Technical information (VC brand, IP address, link, speed, encrypted or not, recording or not, …)

Document camera

- Exchange of documents

Test

- Test connection, picture - light, sound - any distortion…

Testing the VC connection

- one hour before the court session is too late
- in the break time (Youtube, coffee break…) not wise
- plan it 14 days before the actual hearing (if something goes wrong you still have time to test again)
- include translator
- consider time differences

Technician

- inform them you will have VC
- they should test the connection
- they should be prepared if their help will be needed

„TRUE – TO – LIFE“ PRINCIPLE

Impression as the person is in the same room

At the court everybody needs to see

- Who is speaking,
- What documents are presented through the document camera
- What are the facial expressions of persons

At the court everybody needs to hear

- What the person to be heard is speaking
- What the judge, prosecutor lawyer are saying – no matter where they are

DURING THE HEARING

Eye- contact

- Camera is positioned above the screen

Loudspeakers

- Near the screen, at the side – to provide feeling that the person is really speaking from the direction of the screen

Microphones

- Turned on while speaking, turned off while listening to others

DURING THE HEARING

Mind the Light

- Dark background
- no direct light behind the speaker

Cameras show speakers in 80x80 cm square

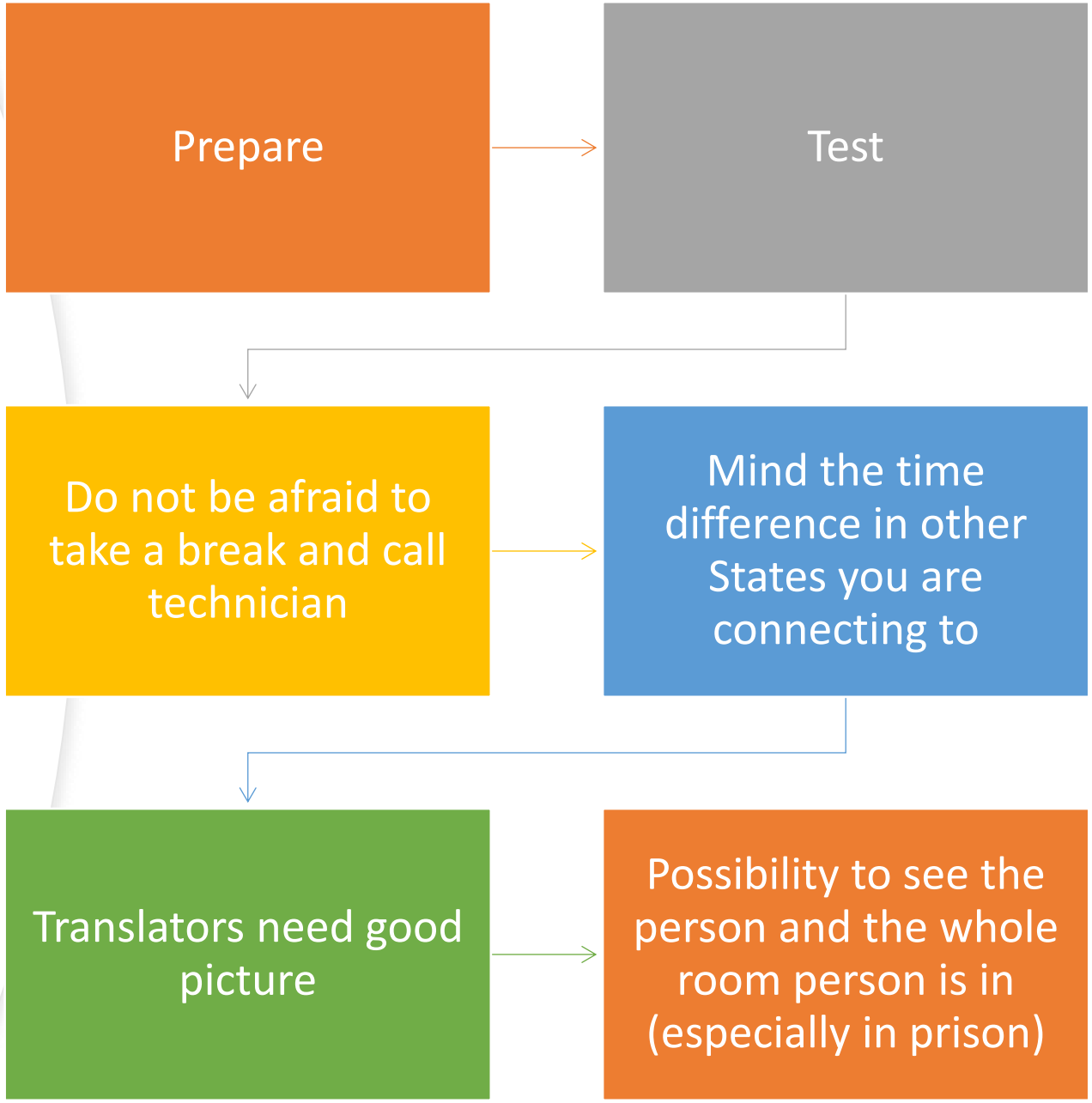
Judge has own camera

Avoid cameras that are connected to microphones/prefer pre-sets of cameras

Microphone is turned on only while the person is speaking (small light sign on)

Mind lawyer-client confidentiality – possibility to turn off all the other microphones and loudspeakers

WRAP UP


Prepare
Test
Do not be afraid to take a break and call technician
Mind the time difference in other States you are connecting to
Translators need good picture
Possibility to see the person and the whole room person is in (especially in prison)

Child victims (Barnahus) Slovenia

Barnahus Model

The use of video-recorded pretrial interviews as evidence helps prevent retraumatization of victims, who no longer need to testify again in court.

Thank you!

Good luck !