#DIGITALISATION and #AI in Criminal Justice

Key tech concepts, online investigations, AI and machine learning

Cracow, 26-27 May 2025

FACE-TO-FACE

EXCELLENCE IN EUROPEAN LAW

Speakers and chairs

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

Steven David Brown, International Cybercrime Consultant, Vienna

Rainer Franosch, Prosecutor, Deputy Director-General for Criminal Law and Criminal Procedure, Head of Cybercrime Division, Ministry of Justice, German Federal State of Hesse, Wiesbaden

Rūta Jašinskienė, Intelligence Analysis Expert, NRD Cyber Security, Vilnius

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

Martyna Kusak, Post-Doc Researcher, Institute for International Research on Criminal Policy, Ghent University; Adjunct Professor, Criminal Procedure, Adam Mickiewicz University, Poznań

Kiran Sivakumar, Deputy Inspector General of Police, India

Marc van der Ham, External PhD Candidate, eLaw, Center for Law and Digital Technologies, Leiden University; Legal Advisor, Intangibles, Data & Technology Law, Deloitte Legal

Bart van der Sloot, Associate Professor, Tilburg Law School

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)
- Presenting internet searches in court
- Videoconferencing
- Artificial Intelligence (AI)

Language
English

Event number
325DT06

Organisers
ERA (Laviero Buono) in cooperation with the Polish National School of Judiciary and Public Prosecution

Co-funded by
the European Union

european.law

#DIGITALISATION and #AI in Criminal Justice

Monday, 26 May 2025

09:00 Arrival and registration of participants

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

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

Chair: Laviero Buono

09:35 **Only the best bits: highlighting some essential knowledge of digital evidence**
- The nature of the Internet
- On-device and remote evidence
- Best practice in e-evidence acquisition
- The challenge of encryption
- Pitfalls and prospects of AI

Steven David Brown

10:45 Discussion

11:00 Break

11:30 **Digital evidence: Open Source Intelligence (OSINT)**
- Introduction and the role of OSINT
- Efficient dialogue with search engines
- How OSINT is used by hackers
- Use case scenarios

Rūta Jašinskienė

12:15 Discussion

12:30 Lunch

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

Chair: Steven David Brown

13:30 **An overview of the legal issues regarding the use of e-evidence collected on the internet**
Marc van der Ham

14:30 Discussion

14:45 Break

15:15 **Artificial intelligence and handling electronic evidence in courts**
- AI impact on investigations
- Trial considerations: methods of presentation and admissibility tests
- Criminals' new *modus operandi*
- Case studies

Rainer Franosch

16:15 Discussion

16:30 End of first day

19:30 Dinner offered by the organisers

Objective

This seminar addresses various challenges linked to digitalisation that judges, prosecutors and lawyers in private practice working in the field of EU Criminal Justice will have to face for 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 there 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* 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 Judiciary and Public Prosecution
ul. Przy Rondzie 5
31-547 Cracow
Poland

CPD

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

Tueday, 27 May 2025

PART III: VIDEOCONFERENCING AND ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

Chair: Marc van der Ham

09:30 **Presenting evidence in court: e-files, videoconferences and remote trials**
- Remote trials during and after the pandemic
- E-files
- Witnesses videoconferences
- Vulnerable victims

Sabina Klaneček

10:00 Discussion

10:15 **Big Data and the quality of datasets used for the development of AI-based tools for law enforcement in criminal justice systems**
Martyna Kusak

10:45 Discussion

11:00 Break

11:30 **Predictive policing and big data: the new threat landscape for law enforcement authorities**
Kiran Sivakumar

12:00 Discussion

12:15 **Deepfakes in judicial proceedings**
Bart van der Sloot

12:45 Discussion

13:00 End of online seminar and light lunch

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

Your contacts

Laviero Buono
Head of Section
European Criminal Law

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

Apply online for "#Digitalisation and #AI in Criminal Justice": **www.era.int/?133191&en**

This programme has been financed by the European Union

Application

#DIGITALISATION and #AI in Criminal Justice

Cracow, 26-27 May 2025 / Event number: 325DT06

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 **31 January 2025.**
3. A response will be sent to every applicant after this deadline. **We advise you not to book any travel before you receive our confirmation**.

Registration Fee

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

Accommodation

5. Accommodation for two nights (25–27 May 2025) has been reserved at the Polish National School of Judges and Public Prosecutors in Kraków ("*Dom Aplikanta*"). To confirm your stay after you have been informed by us that your application was successful, please contact Julia Reitz via email at **jreitz@era.int**, providing your arrival and departure dates **by 9 May 2025**. Kindly include the reference **"325DT06 – Room Reservation"** in your email. **Please note that ERA will only reimburse accommodation costs if you stay at *Dom Aplikanta*. No other accommodation costs will be accepted.**

Travel and Accommodation Expenses

6. Participants will receive a fixed contribution towards their travel expenses and are asked to book their own travel. The condition for payment of this contribution is to sign all attendance sheets at the event. 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 costs.
7. Travel costs from outside Poland: participants can calculate the contribution to which they will be entitled on the European Commission website (https://era-comm.eu/go/calculator, table 2). The distance should be calculated from their place of work to the seminar location.
8. For inter-Member State return journeys between 50 and 400 km (AT, CZ, DE, HU, LT, LV, RO, SK) please consult p.11 on https://era-comm.eu/go/unit-cost-decision-travel
9. For those travelling within Poland, the contribution for travel is fixed at €20 (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
10. Accommodation costs: international participants travelling more than 50km one-way will receive a fixed contribution of €103 per night for up to two nights' accommodation (*Dom Aplikanta* only, see point 5). National participants travelling more than 50km one-way will receive a fixed contribution of € 103 per night for one nights' accommodation (*Dom Aplikanta* only, see point 5). For more information, please consult p. 13 on https://era-comm.eu/go/unit-cost-decision-travel
11. Successful applicants will be sent the relevant claim form and information on how to obtain payment of the contribution to their expenses. Please note that no payment is possible if the registered participant cancels their participation for any reason.

Participation

12. Participation at the whole seminar is required and participants' presence will be recorded.
13. 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.
14. 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.

Apply online for "#Digitalisation and #AI in Criminal Justice": **www.era.int/?133191&en**

Venue

National School of Judiciary and Public Prosecution
ul. Przy Rondzie 5
31-547 Cracow
Poland

Language

English

Contact

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

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*)

This programme has been produced with the financial support of the European Union

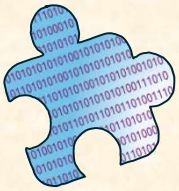
Only the best bits:

01000010011001010111001101110100001000000100001001101001011101000111 0011

highlighting some essential knowledge of digital evidence

Steven David Brown

Krakow 26-27 May 2025



InZeit Excellence in Acuity

1

The Internet =?

Hierarchical Infrastructure of:

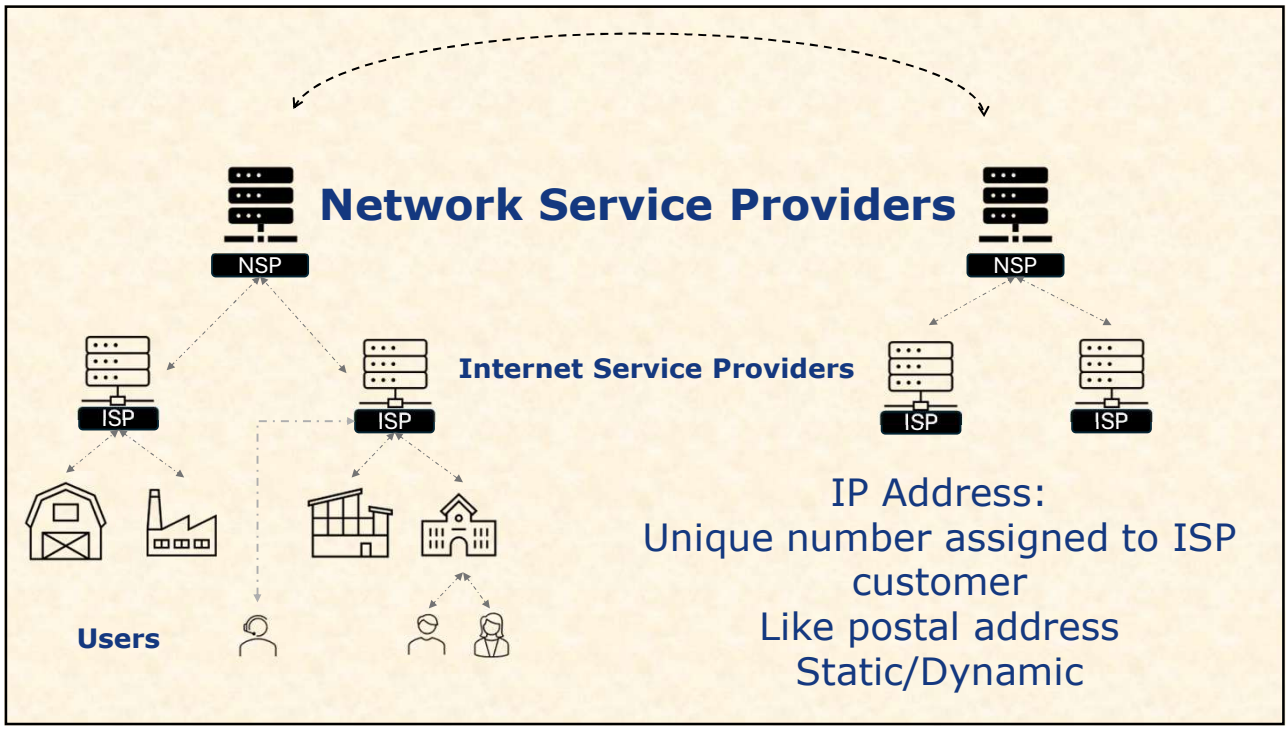
- **Interconnected Networks**
  - ❖ **Internet Service Providers**
  - ❖ **Network Service Providers**

A quasi-public space (cfr shopping mall)

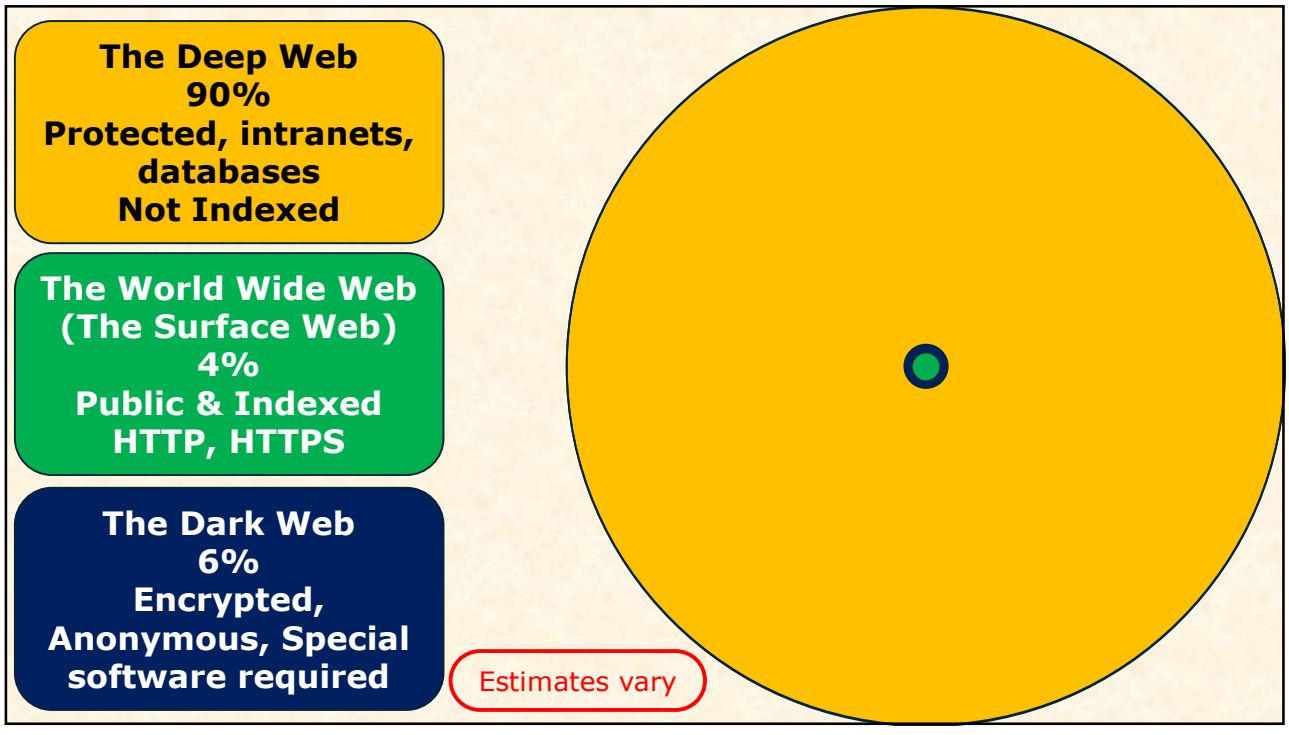
Gateways: Internet Service Providers (ISPs)
Assign Internet Protocol (IP) Addresses

Details in this presentation have been simplified

2


Network Service Providers
NSP
NSP
Internet Service Providers
ISP
ISP
ISP
ISP
Users
IP Address:
Unique number assigned to ISP customer
Like postal address
Static/Dynamic

3

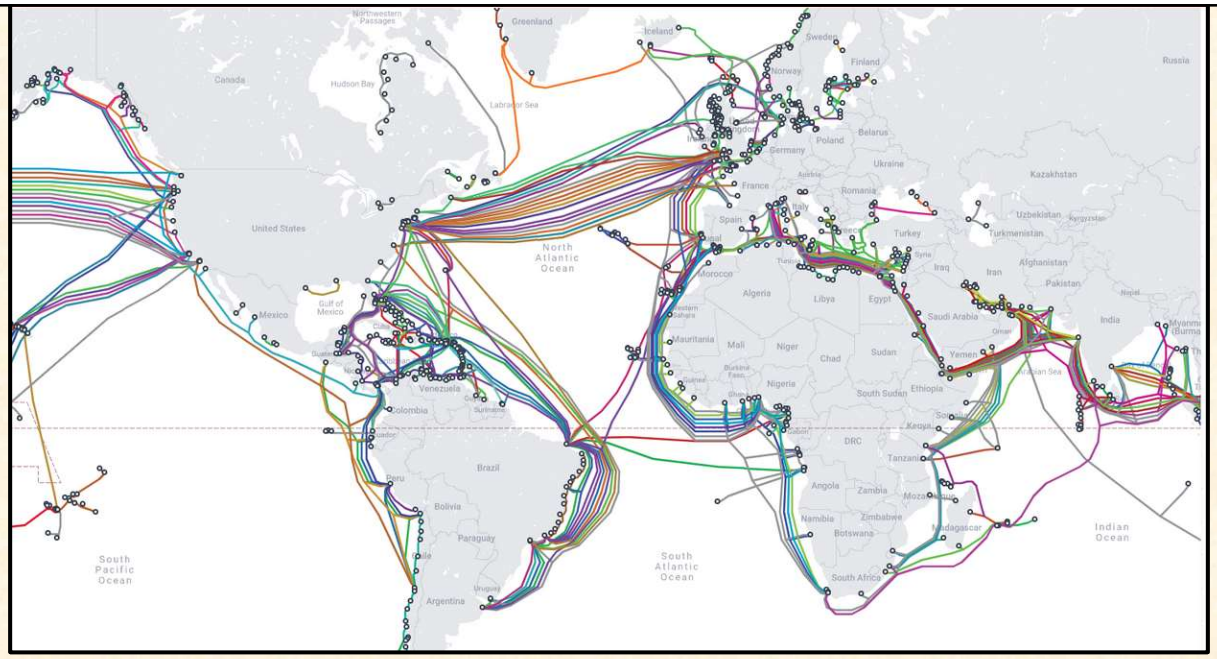

The Deep Web
90%
Protected, intranets, databases
Not Indexed
The World Wide Web
(The Surface Web)
4%
Public & Indexed
HTTP, HTTPS
The Dark Web
6%
Encrypted, Anonymous, Special software required
Estimates vary

4

Data transmitted as:

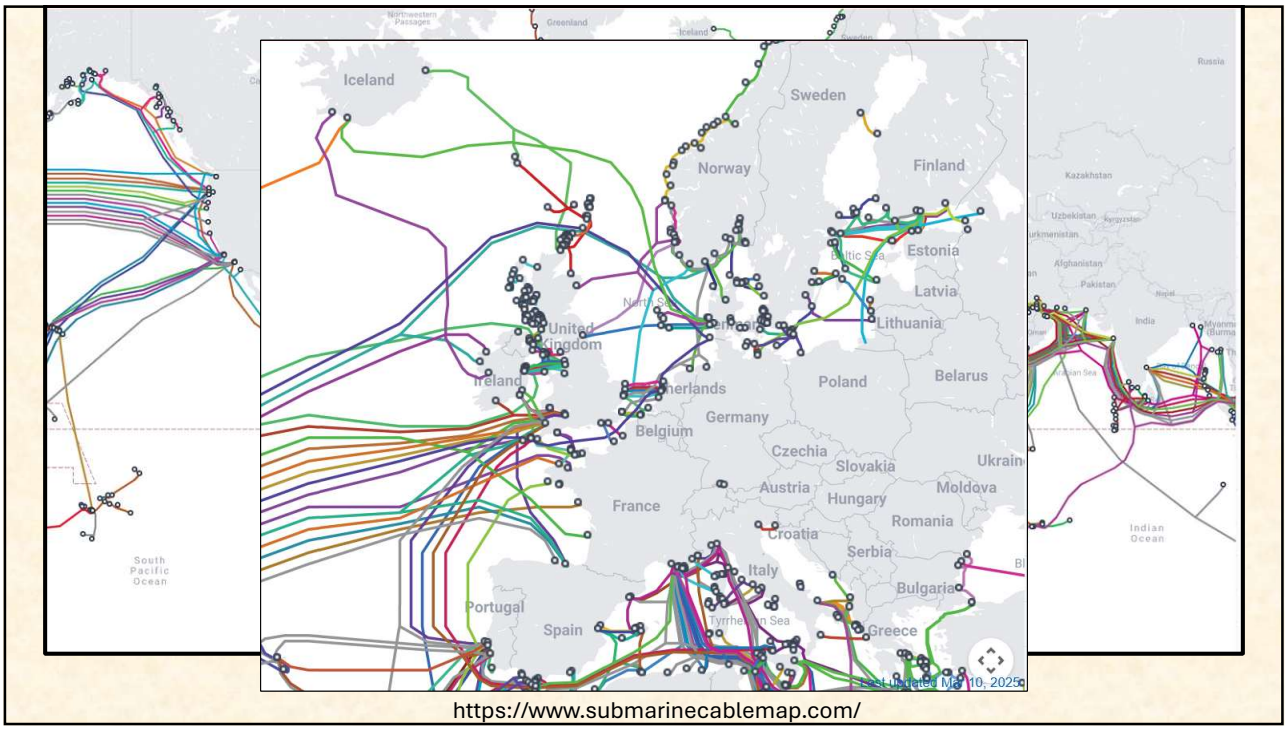
- Radiowaves or Microwaves to Access Points, Satellites
- Electrons along Copper Wires (Cables)
- Pulses of light along Fibreoptic cables

5



https://www.submarinecablemap.com/

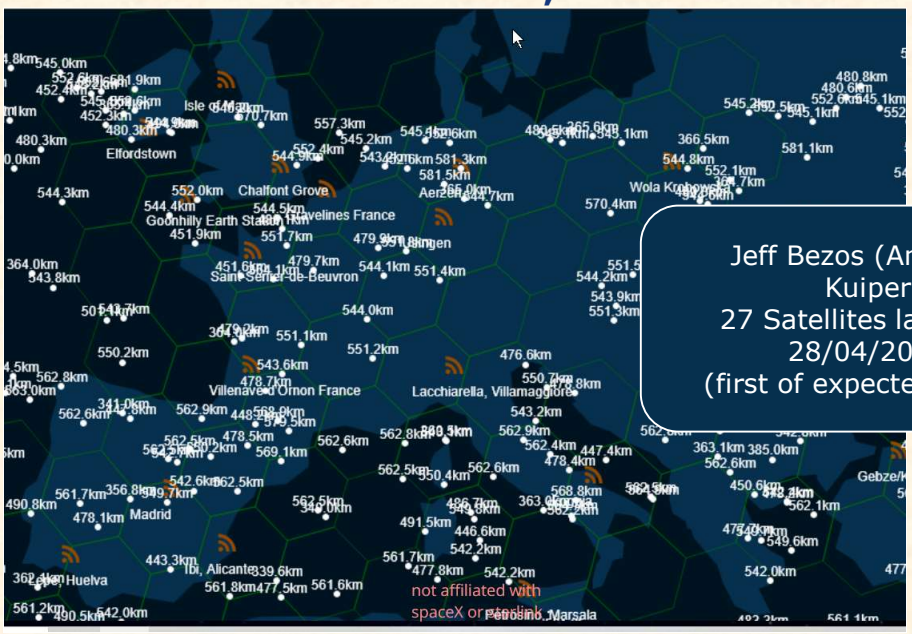
6



https://www.submarinecablemap.com/

7

Elon Musk's Starlink – 5,601 satellites



Jeff Bezos (Amazon)
Kuiper
27 Satellites launched
28/04/2025
(first of expected 3,236)

https://satellitemap.space/

8

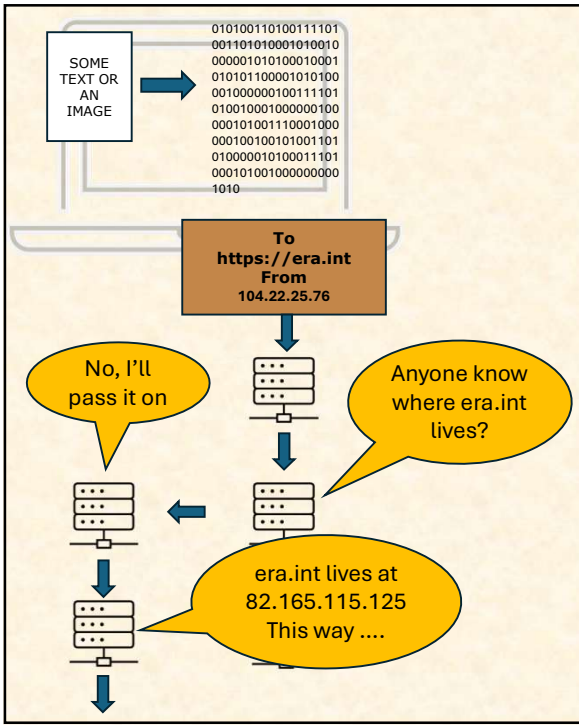
Interconnecting …

Your computer sends request to connect with another computer/server on the Internet

If accepted, a 'session' is established (i.e. digital dialogue opened)

Data/File split into small units and wrapped in a 'packet'

9



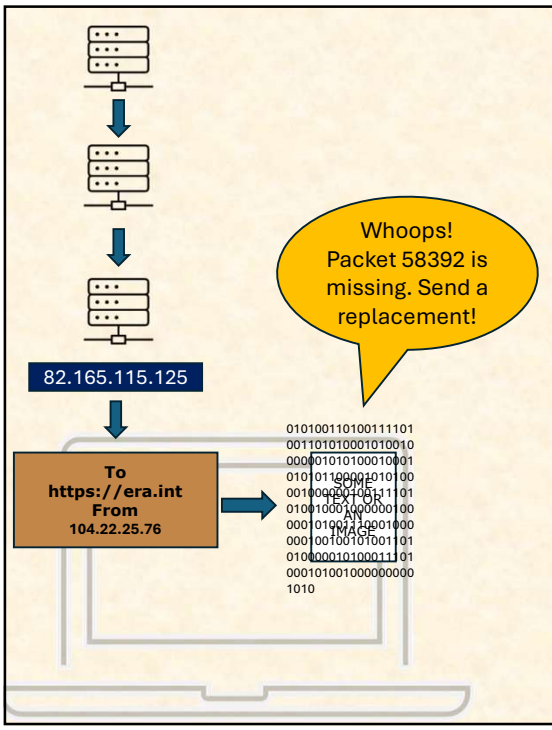
Data/File split into small units and wrapped in a 'packet'

Each packet (like an envelope) is labelled with the 'to' and 'from' addresses and dispatched one at a time by the best/fastest route chosen by a series of 'routers'

If a router doesn't recognise the address, it is sent up the pipe to the next server

Domain names are converted to IP Addresses by the DNS (Domain Name System)

10



Packets are re-assembled on the receiving device

Traffic Data – technical details of who/how/where/when sent

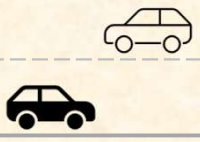
Another important identifier:
Media Access Control (MAC) address
Unique number burnt into hardware
Distingishes devices on a network

11

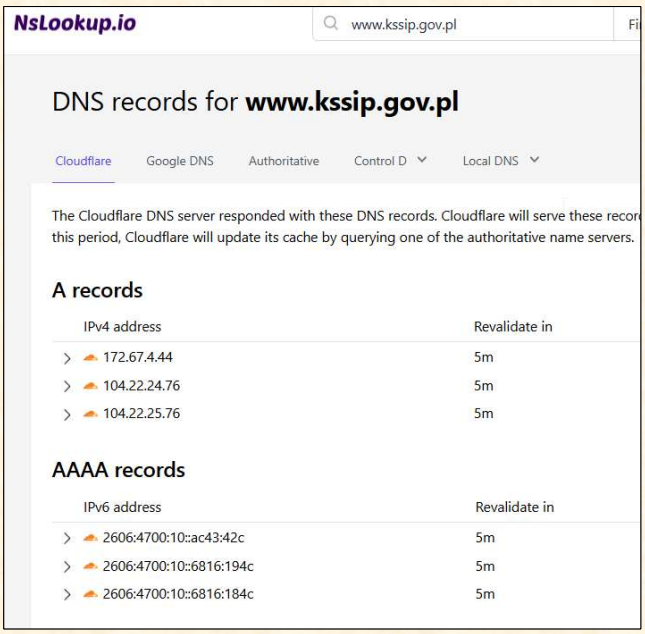
Protocols

An agreed way of doing things

- TCP (Transmission Control Protocol)
- IP (Internet Protocol)
- HTTP (Hyper Text Transfer Protocol)
- HTTPS (Hyper Text Transfer Protocol Secure)
- UDP (User Datagram Protocol)
- DNS (Domain Name System)
- ARP (Address Resolution Protocol)



12



Cloudflare

Content Delivery Network

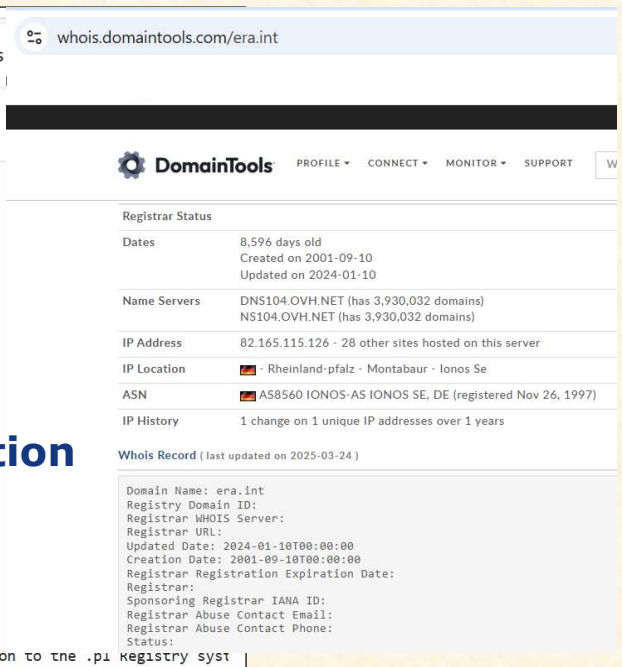
IPv4
104.22.24.76

IPv6
2606:4700:10:ac43:42c

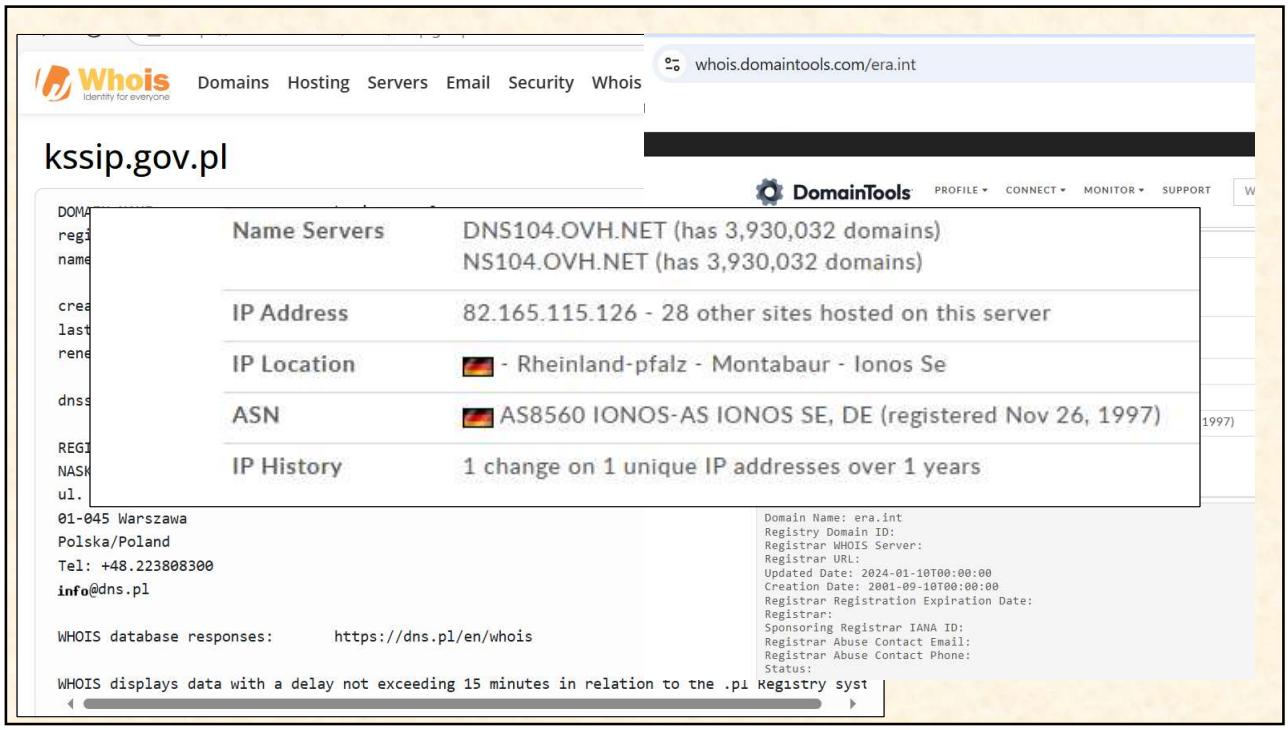
DNS = Domain Name System

13

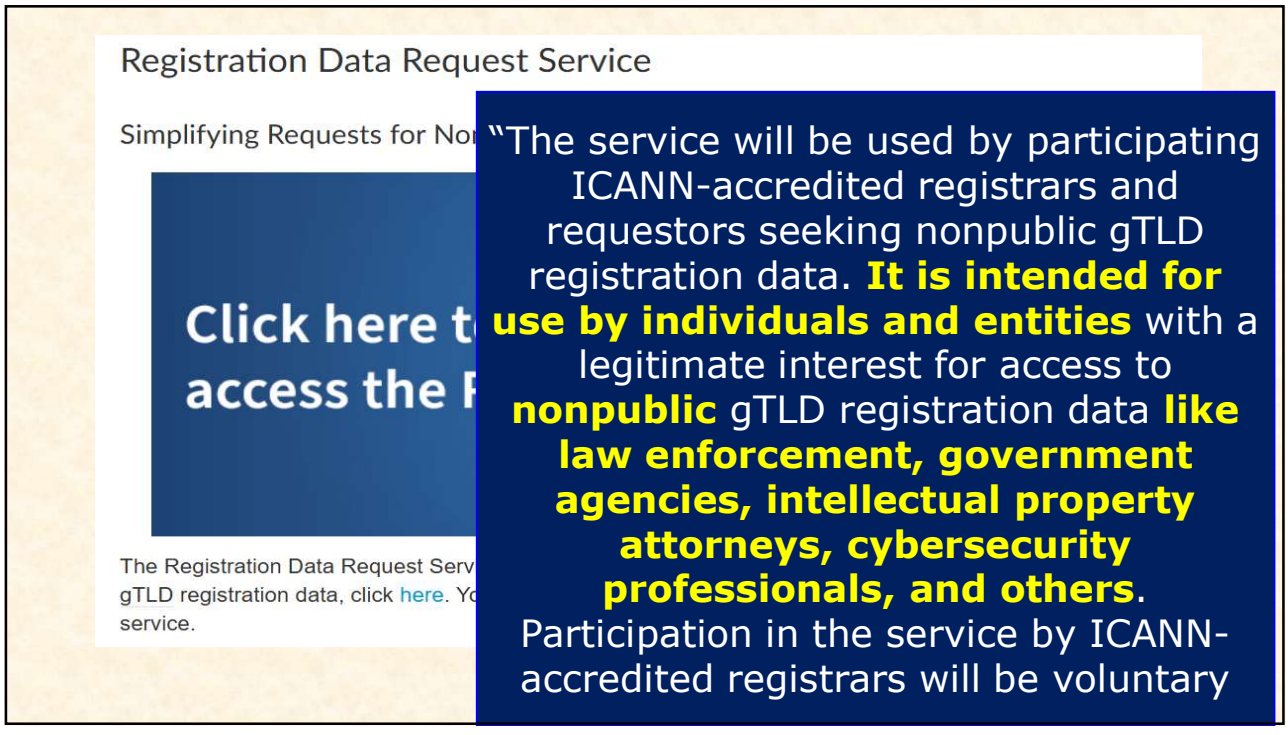
Whois registration



14


Whois
Domains Hosting Servers Email Security Whois
kssip.gov.pl
whois.domaintools.com/era.int
DomainTools PROFILE CONNECT MONITOR SUPPORT
Name Servers DNS104.OVH.NET (has 3,930,032 domains)
NS104.OVH.NET (has 3,930,032 domains)
IP Address 82.165.115.126 - 28 other sites hosted on this server
IP Location - Rheinland-pfalz - Montabaur - Ionos Se
ASN AS8560 IONOS-AS IONOS SE, DE (registered Nov 26, 1997)
IP History 1 change on 1 unique IP addresses over 1 years
01-045 Warszawa
Polska/Poland
Tel: +48.223808300
info@dns.pl
WHOIS database responses: https://dns.pl/en/whois
WHOIS displays data with a delay not exceeding 15 minutes in relation to the .pl Registry syst
Domain Name: era.int
Registry Domain ID:
Registrar WHOIS Server:
Registrar URL:
Updated Date: 2024-01-10T00:00:00
Creation Date: 2001-09-10T00:00:00
Registrar Registration Expiration Date:
Registrar:
Sponsoring Registrar IANA ID:
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Status:

15


Registration Data Request Service
Simplifying Requests for No
Click here t
access the
The Registration Data Request Serv
gTLD registration data, click here. Yo
service.
"The service will be used by participating ICANN-accredited registrars and requestors seeking nonpublic gTLD registration data. It is intended for use by individuals and entities with a legitimate interest for access to nonpublic gTLD registration data like law enforcement, government agencies, intellectual property attorneys, cybersecurity professionals, and others. Participation in the service by ICANN-accredited registrars will be voluntary

16

IPv6
42 undecillion in Total
1 decillion = 10^{36}

https://rednectar.net/2012/05/24/just-how-many-ipv6-addresses-are-there-really/

Internet Users Globally
5.5 Billion (2024)
https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

```
Server:  UnKnown
Address:  103.86.96.100

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    era.int
Address:  82.165.115.126
```

```
C:\Windows\system32>nslookup kssip.gov.pl
Server:  UnKnown
Address:  103.86.96.100

Non-authoritative answer:
Name:    kssip.gov.pl
Addresses:  2606:4700:10::ac43:42c
          2606:4700:10::6816:194c
          2606:4700:10::6816:184c
          104.22.24.76
          172.67.4.44
          104.22.25.76
```

IPv6

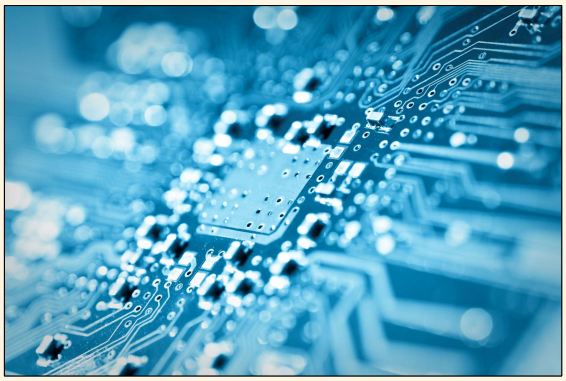
IPv4

IPv4

4,294,967,296	**Total**
588,514,304	**Private**
3,706,452,992	**Public**

17

Computer chips consist of thousands of tiny electronic transitors (switches)



bit = binary digit

1 bit like 1 brain cell

8 bits = 1 byte

No words just zeros & ones

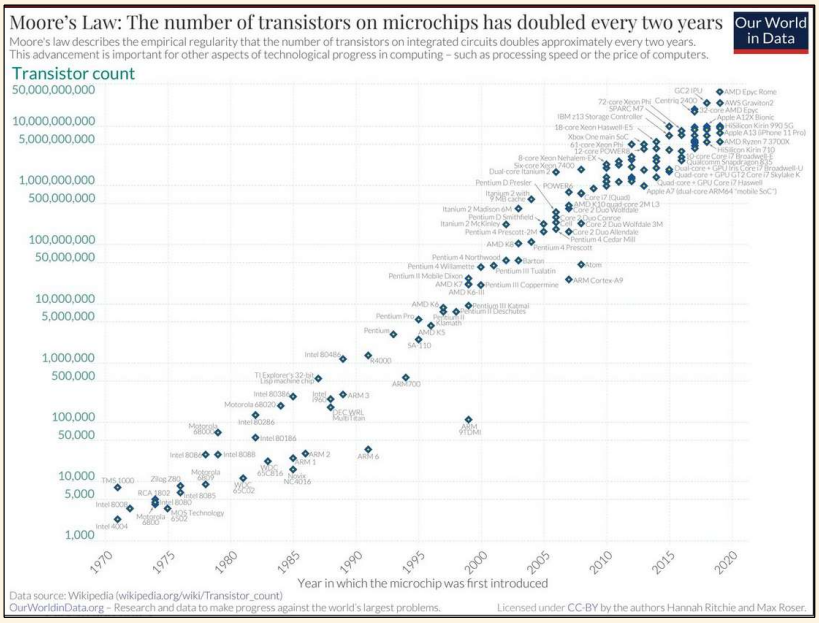
18

Gordon Moore (1965)

Number of transistors on a Microchip double in density about every 2 years

1970s
1 transistor 10 μm

Now
3 nm
(3 billionths of a metre)



Moore's Law

https://ourworldindata.org/moores-law

19

Quantum Bits - Qubits

Qubit can be On/Off or anywhere inbetween (until observed)
('superposition' like a dimmer switch)

Acts like both particle and a wave

Entanglement – pairs of qubits
Measure one, the other is opposite

20

Memristors

Proposed 1971 Prof Leon Chua UC Berkeley

First built 2005

Stable data storage

Faster than Solid State Drives

Lower energy requirement & less heat

2022 quantum memristors demonstrated

www.memristor.org
https://instrumentationtools.com/memristor/
https://ui.adsabs.harvard.edu/abs/2022NaPho..16..318S/abstract

21

The digital alphabet ..

1 + 1 = 10

base$_2$

off or on

0 or 1

yes or no

22

American Standard Code for Information Interchange (ASCII)

8 bits = 1 byte

1 byte = 1 letter/digit

ASCII	SYMBOL	ASCII	SYMBOL
00110000	0	01001110	N
00110001	1	01001111	O
00110010	2	01010000	P
00110011	3	01010001	Q
00110100	4	01010010	R
00110101	5	01010011	S
00110110	6	01010100	T
00110111	7	01010101	U
00111000	8	01010110	V
00111001	9	01010111	W
01000001	A	01011000	X
01000010	B	01011001	Y
01000011	C	01011010	Z
01000100	D	00100001	!
01000101	E	00100010	
01000110	F	00100011	#
01000111	G	00100100	$
01001000	H	00100101	%
01001001	I	00100110	&
01001010	J	00101000	(
01001011	K	00101001	)
01001100	L	00101010	*
01001101	M	00101011	+

Source: cs.gsu.edu

23

01000011	01001111
01001101	01010000
01010101	01010100
01000101	01010010

(Each byte represents a character)

24

C	01000011
O	01001111
M	01001101
P	01010000
U	01010101
T	01010100
E	01000101
R	01010010

(8 Bytes)

https://www.binaryhexconverter.com/ascii-text-to-binary-converter

25

电脑

Համակարգիչ

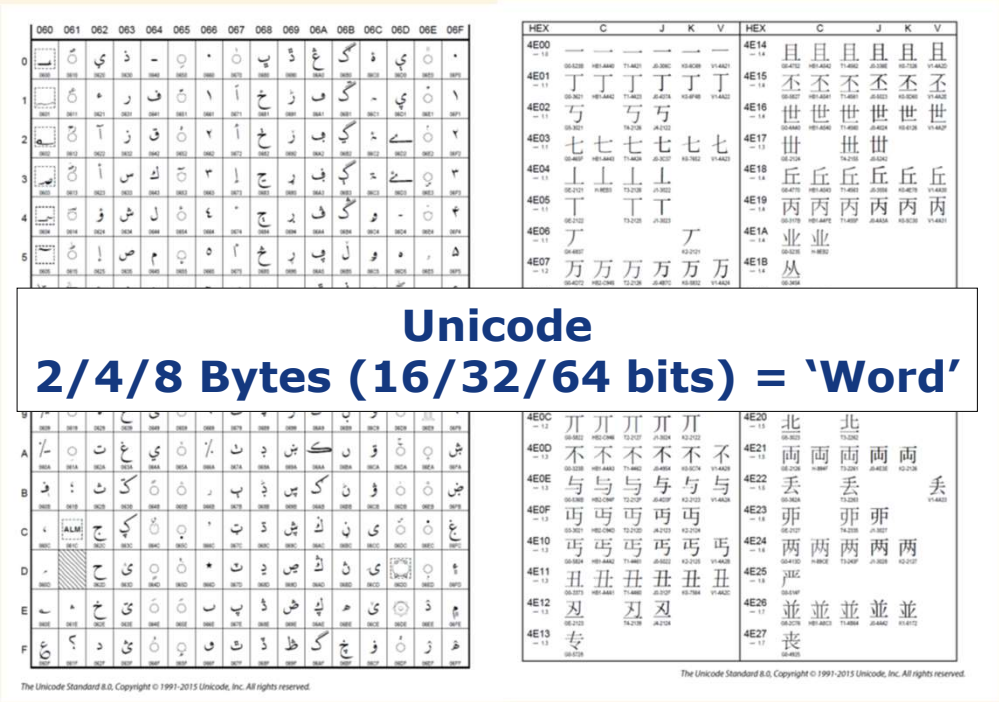
ኮምፒውተር

컴퓨터

संगणक

الحاسوب

26



27

The Data Deluge

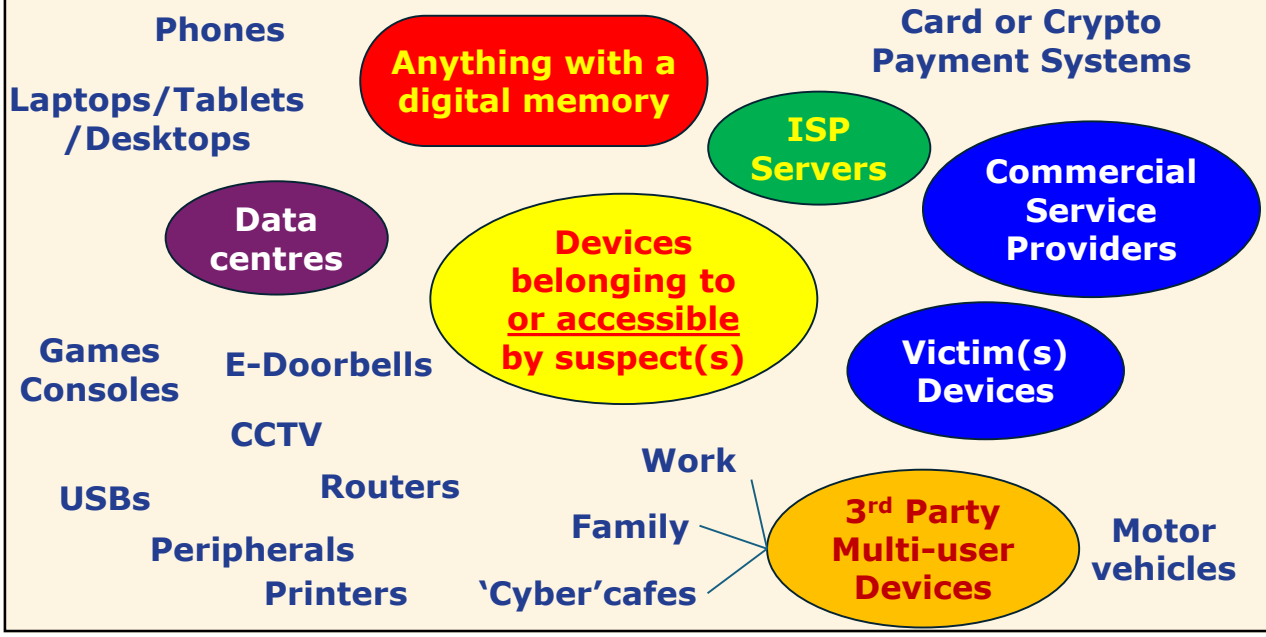
In 2024, more than:

- **361 billion emails per day;**
- **3.5 billion Google searches per day;**
- **510,000 Facebook comments per minute;**
- **16 M text messages per minute;**
- **456,000 X messages per minute;**
- **46,740 Instagram photos/minute**

https://joingenius.com/statistics/data-generated-per-day/
https://spacelift.io/blog/how-much-data-is-generated-every-day

28

No physical nexus to crime scene required



29

Evidence on the Device

Tying the device to the suspect:

- Traditional forensics
- Activity & behaviour of user
- User log-ins and identifiers

30

Electronic evidence is VOLATILE!

- Susceptible to heat & electromagnetic fields
- Every key pressed changes the data
- Automatic processes may delete data (esp. Solid State Drives)

31

Devices Dead or Alive

'Dead' Computer Forensics (device switched off)

Data captured in lab

'Live' Computer Forensics (Device switched on)

Data captured at scene

32

‘Live’ Computer Forensics
(Device switched on)

K.Y.C.
(“Know your criminal”)

33

Basic Kit

Forensic workstation

Cameras

Write-blockers

Cables & connectors

Access point scanners

Anti-static bags/bracelets

Faraday Bags
(kitchen foil or old paint tins)

34

RAM = Random Access Memory

- ‘Short term’ processing memory
- Standard 4/8 GB; Quality laptops 16 GB; Gaming laptops 32 or 64 GB
- Bigger RAM, more can do at same time
- Memory fades when power cut (lose unsaved files)
- Live forensics captures that data

35

‘Dead’ Computer Forensics

(Device is switched off and transported to lab)

36

Three main forms of data storage:

- Magnetic
  (Hard Disk Drives (HDDs))
- Optical (CD, DVD) (Old Tech)

- Digital switches/microchips
  (Solid State Drives(SSD))

Remember all based on binary (on/off)

37

Deleted data can (often) be recovered:

Delete button just tells computer the relevant space available to be overwritten

Data remains until the memory space is needed for new data

BUT: Devices with SSD storage (phones, USB sticks, modern notebooks) may automatically delete data when powered on

38

Absolute first thing in lab:

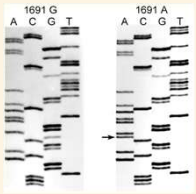
- All seized drives copied
- Exact copy (every zero and one) a.k.a ‘bit-by-bit’, ‘bit-stream’ copy, image or clone (not same as ‘backup’)
- Any analysis is done on the copy in case of dispute

39

How do we prove the copy is 100% exact?

From the

‘hash’ value



(Digital fingerprint, a long alphanumeric string)

40

Hexadecimal(base$_{16}$)

Hash Value :

72a40ac74b7a2472826f306f02e508fc

A complex algorithm is applied to the data resulting in a 'hash value'.

One way cryptographic function (equation)

Used for:

- **Checking integrity of files copies**
- **Protecting stored passwords**
- **Identifying files (malware, CSAM)**

41

- **In forensic examination the algorithm is applied to both original drive and its copy.**
- **If the 'hash value' for both drives is the same, the copy is a clone.**
- **Can 'hash' any data from file to computer drive**

42

https://www.era.int/cgi-bin/cms?_SI...

Home

History

Responding to the need for knowledge

The Academy of European Law began work in Trier in March 1992.

Its genesis was associated with the rapid pace of European integration during the late 1980s and 1990s. With the Single European Act in 1986 and the Maastricht Treaty in 1992, the scope of European legislation became wider than ever before.

It was clear that lawyers, judges and other legal practitioners at all levels and in almost all fields of law would need regular training and a forum for debate in order to keep up-to-date with the latest developments.

In 1990 the European Parliament recommended that the Commission invest in a centre for the continuing education of lawyers in order to improve the application of European law.

Meanwhile, Peter Caesar, the Minister of Justice of the German Land of Rhineland-Palatinate, together with Horst Langes and Willi Rothley, Members of the European Parliament from the same region, were drawing up proposals for an Academy of European Law to be established in Trier.

In 1991, the European Parliament endorsed these proposals in a report drafted by the Dutch MEP James Janssen van Raay.

An Association for the Promotion of the Academy of European Law was established to turn the idea into reality. The association continues to support the Academy's work and is known as the "Friends of ERA".

MAILING LIS

Keep up-to-date information serv

43

https://www.md5hashgenerator.com/

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

It was clear that lawyers, judges and other legal practitioners at all levels and in almost all fields of law would need regular training and a forum for debate in order to keep up-to-date with the latest developments.

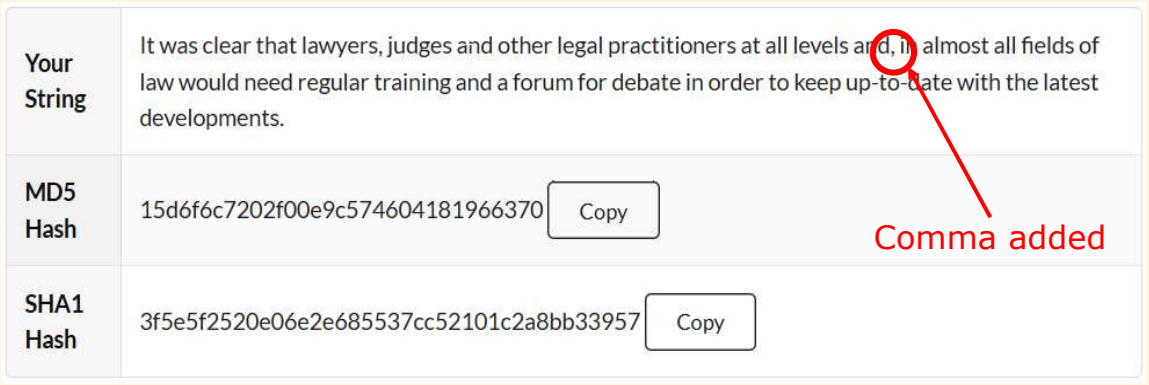
Generate →

Your String	It was clear that lawyers, judges and other legal practitioners at all levels and in almost all fields of law would need regular training and a forum for debate in order to keep up-to-date with the latest developments.
MD5 Hash	b21292e875a21357aa49c5abd93ee673 Copy
SHA1 Hash	0c6acc9dcd0a25e2505ea9f87f73a064b1b47bc6 Copy

MD5 Hash
b21292e875a21357aa49c5abd93ee673

44

One zero or one different in the binary data will produce a very different hash value



MD5 Hash
b21292e875a21357aa49c5abd93ee673
15d6f6c7202f00e9c574604181966370

45

Matching files

Searching for known hash values

Checking digital fingerprints against a known list

- **Child Sexual Abuse Material (CSAM)**
- **Malware**
- **Hashed Passwords (more later)**

More on 'Client Side Scanning' later

46

Software Tools

(NO evidence button!)

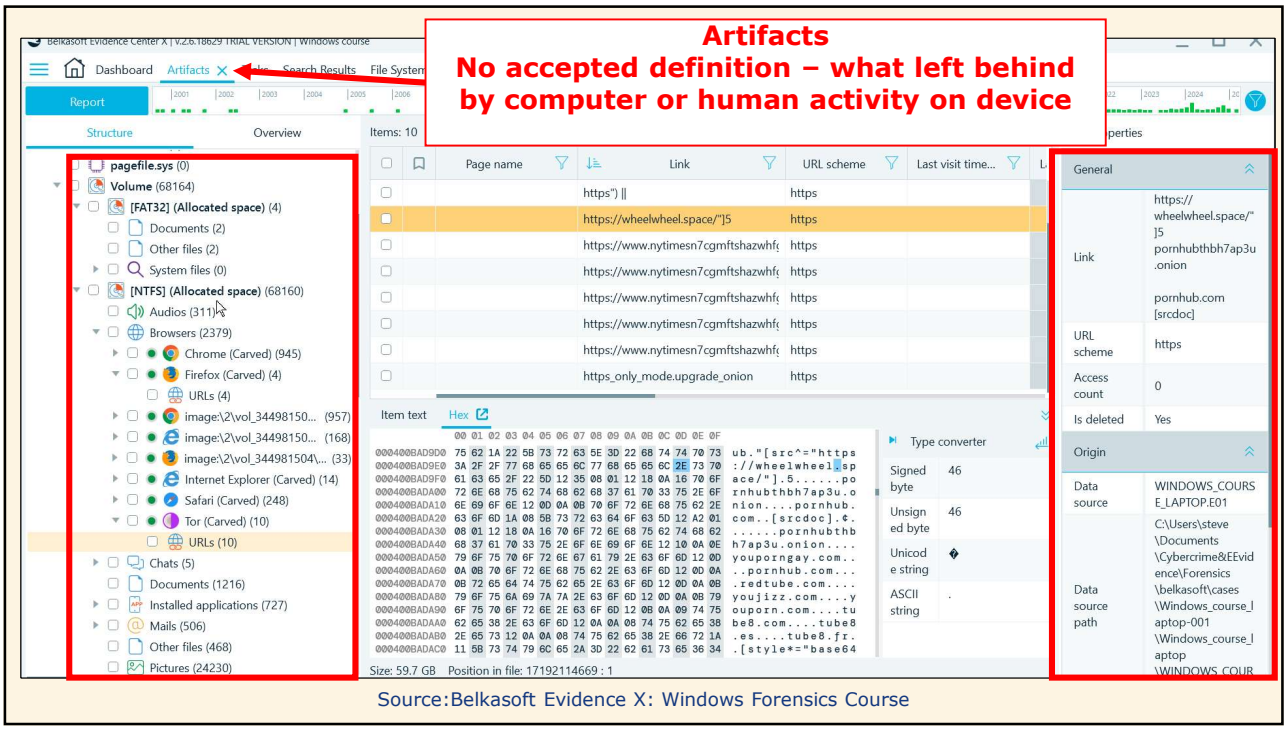
47

Popular forensic software suites:

OpenText
(Encase)
FTK
Belkasoft
Sleuthkit (Autopsy)*
Volatility*
Magnet
Oxygen Forensic Suite
Cellebrite
MSAB's XRY

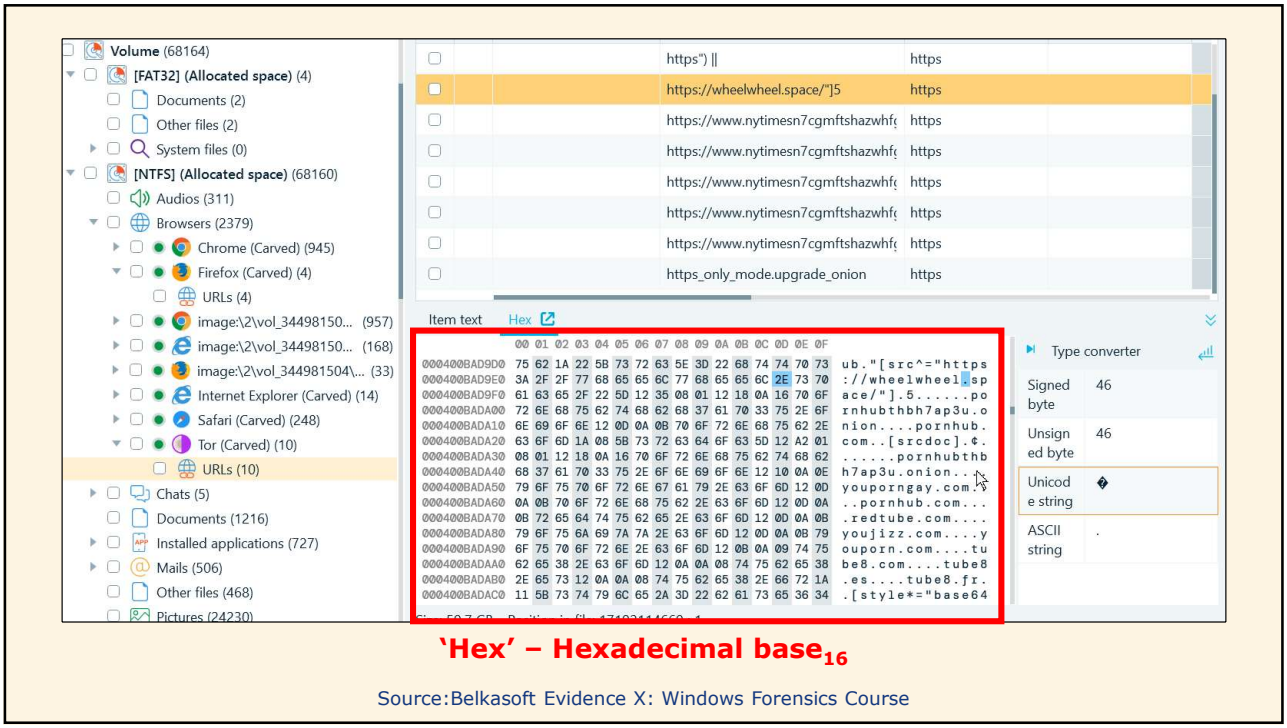
* Free software

48



Source:Belkasoft Evidence X: Windows Forensics Course

49



'Hex' – Hexadecimal base$_{16}$

Source:Belkasoft Evidence X: Windows Forensics Course

50

Item text Hex

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
000400BAD9D0	75	62	1A	22	5B	73	72	63	5E	3D	22	68	74	74	70	73	ub."[src^="https
000400BAD9E0	3A	2F	2F	77	68	65	65	6C	77	68	65	65	6C	2E	73	70	://wheelwheel.sp
000400BAD9F0	61	63	65	2F	22	5D	12	35	08	01	12	18	0A	16	70	6F	ace/"].5.....po
000400BADA00	72	6E	68	75	62	74	68	62	68	37	61	70	33	75	2E	6F	rnhubthbh7ap3u.o
000400BADA10	6E	69	6F	6E	12	0D	0A	0B	70	6F	72	6E	68	75	62	2E	nion....pornhub.
000400BADA20	63	6F	6D	1A	08	5B	73	72	63	64	6F	63	5D	12	A2	01	com..[srcdoc].¢.
000400BADA30	08	01	12	18	0A	16	70	6F	72	6E	68	75	62	74	68	62	......pornhubthb
000400BADA40	68	37	61	70	33	75	2E	6F	6E	69	6F	6E	12	10	0A	0E	h7ap3u.onion....
000400BADA50	79	6F	75	70	6F	72	6E	67	61	79	2E	63	6F	6D	12	0D	youporngay.com..
000400BADA60	0A	0B	70	6F	72	6E	68	75	62	2E	63	6F	6D	12	0D	0A	..pornhub.com...
000400BADA70	0B	72	65	64	74	75	62	65	2E	63	6F	6D	12	0D	0A	0B	.redtube.com....
000400BADA80	79	6F	75	6A	69	7A	7A	2E	63	6F	6D	12	0D	0A	0B	79	youjizz.com....y
000400BADA90	6F	75	70	6F	72	6E	2E	63	6F	6D	12	0B	0A	09	74	75	ouporn.com....tu
000400BADAA0	62	65	38	2E	63	6F	6D	12	0A	0A	08	74	75	62	65	38	be8.com....tube8
000400BADAB0	2E	65	73	12	0A	0A	08	74	75	62	65	38	2E	66	72	1A	.es....tube8.fr.
000400BADAC0	11	5B	73	74	79	6C	65	2A	3D	22	62	61	73	65	36	34	.[style*="base64

Source:Belkasoft Evidence X: Windows Forensics Course

51

Everything that happens on a digital device is 'logged'

Logs tell you who did what and when
(Unless wiped or spoofed)

52

Server Logs

(Reminder: Server is a computer that provides services to other computers)

53

```
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET /
HTTP/1.1" 200 8536 "-" "Mozilla/5.0 (Windows; U;
Windows NT 5.1; de; rv:1.9.2.3) Gecko/20100401
Firefox/3.6.3"
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET
/res/up.gif HTTP/1.1" 200 523
"http://bribes.cash4gooddeals.com/" "Mozilla/5.0
(Windows; U; Windows NT 5.1; de; rv:1.9.2.3)
Gecko/20100401 Firefox/3.6.3"
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET
/res/next1.gif HTTP/1.1" 200 542
"http://bribes.cash4gooddeals.com/" "Mozilla/5.0
(Windows; U; Windows NT 5.1; de; rv:1.9.2.3)
Gecko/20100401 Firefox/3.6.3"
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET
/res/show1.gif HTTP/1.1" 200 533
"http://bribes.cash4gooddeals.com/" "Mozilla/5.0
(Windows; U; Windows NT 5.1; de; rv:1.9.2.3)
Gecko/20100401 Firefox/3.6.3"
```

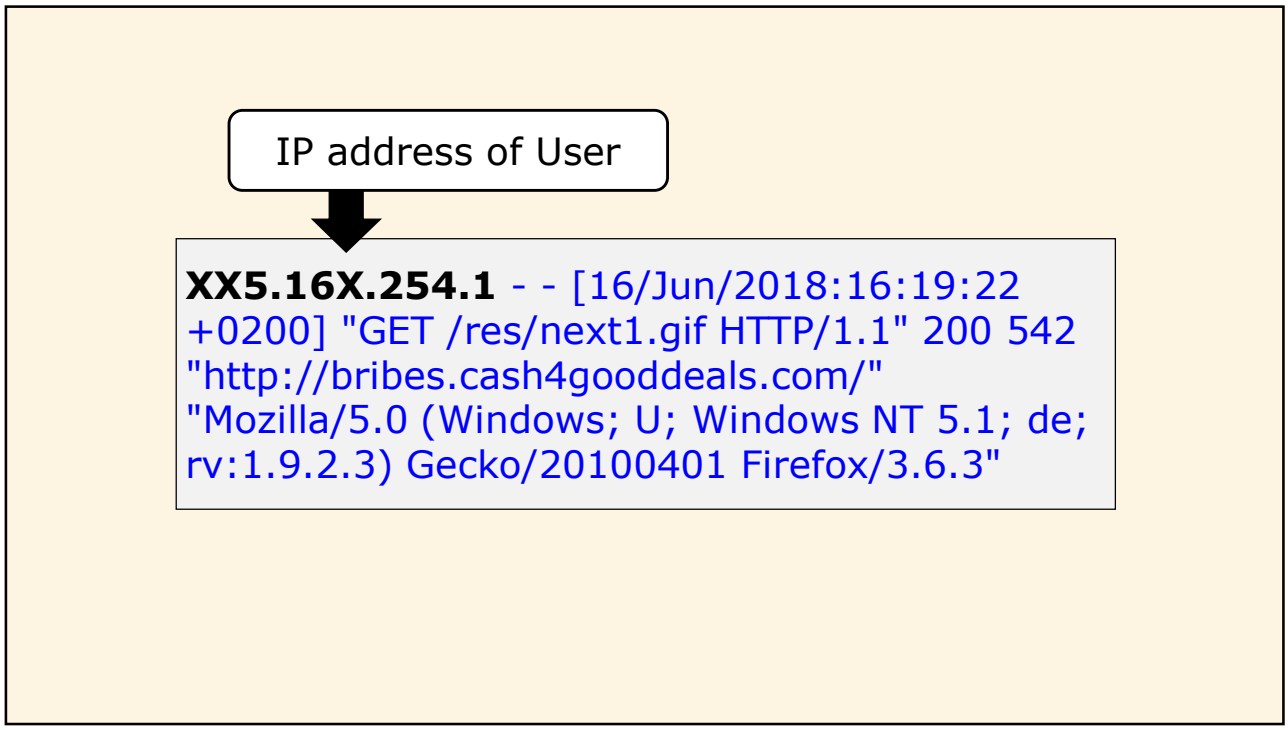
54

XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET / HTTP/1.1" 200 8536 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET /res/up.gif HTTP/1.1" 200 523 "http://bribes.cash4gooddeals.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET /res/next1.gif HTTP/1.1" 200 542 "http://bribes.cash4gooddeals.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET /res/show1.gif HTTP/1.1" 200 533 "http://bribes.cash4gooddeals.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"

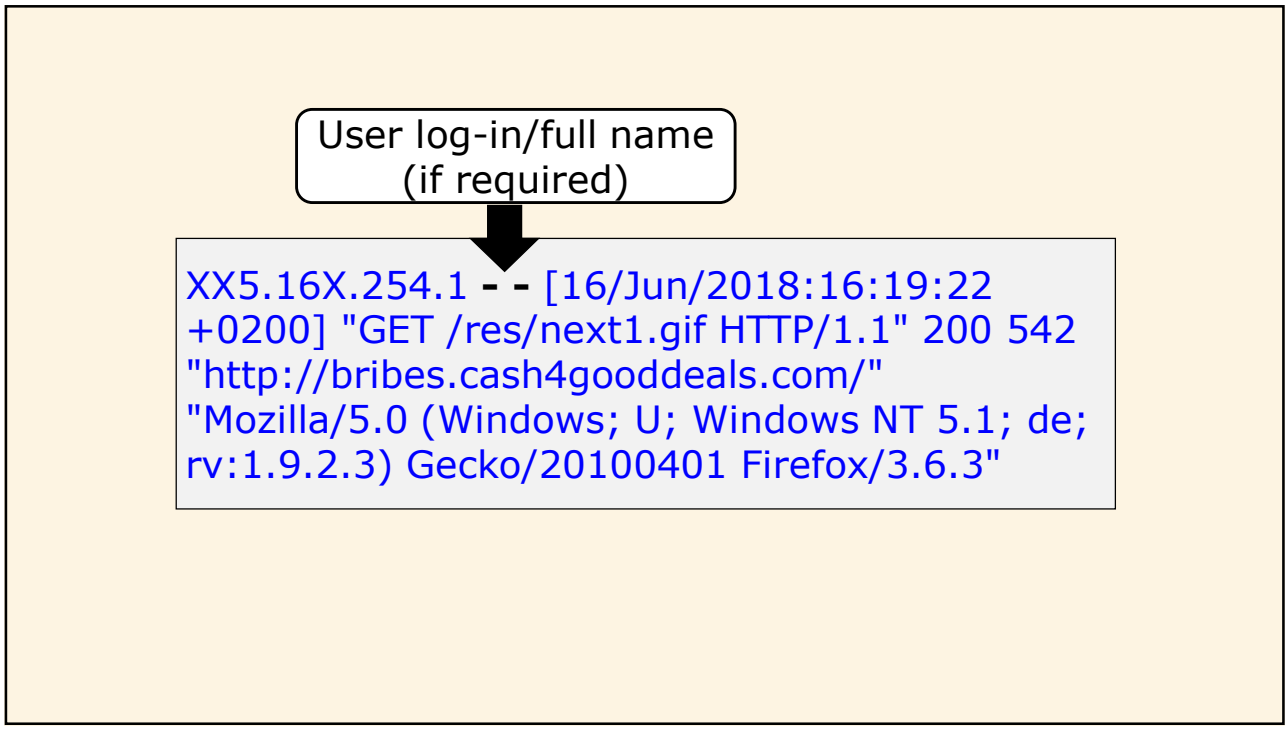
55

XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET /res/next1.gif HTTP/1.1" 200 542 "http://bribes.cash4gooddeals.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"

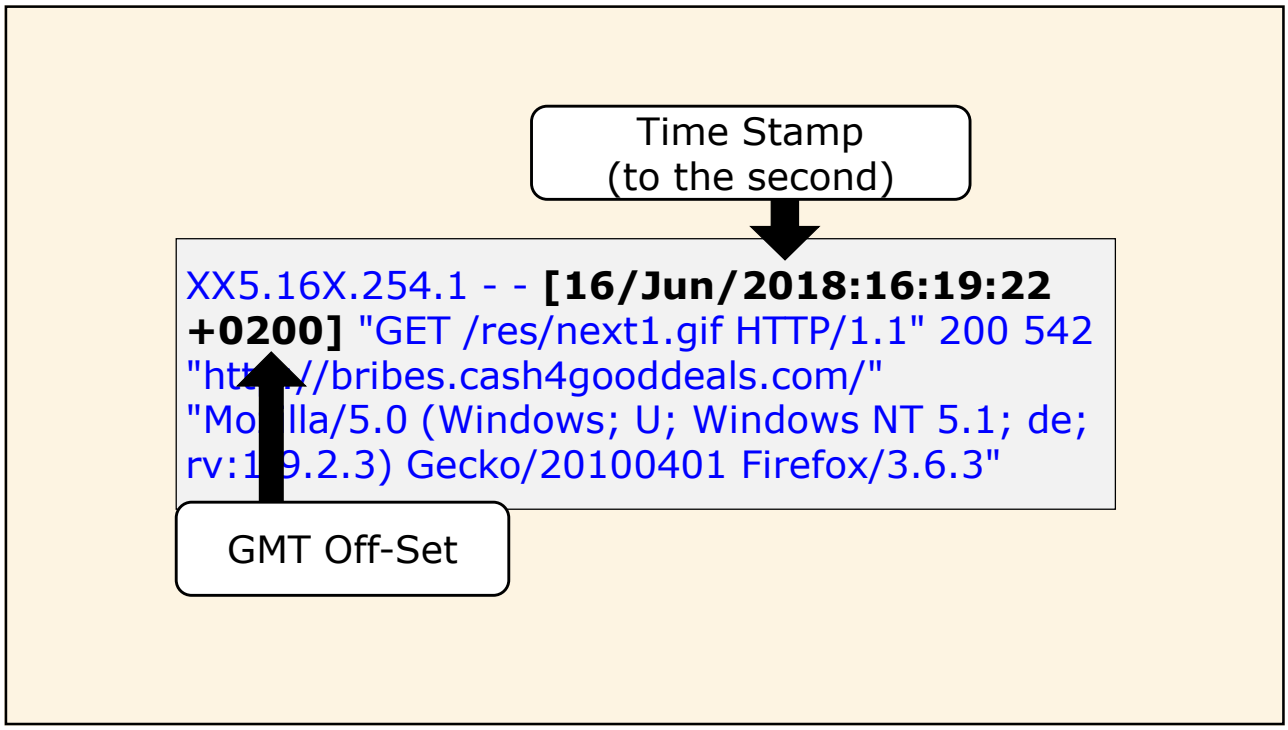
56


IP address of User
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET /res/next1.gif HTTP/1.1" 200 542 "http://bribes.cash4gooddeals.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"

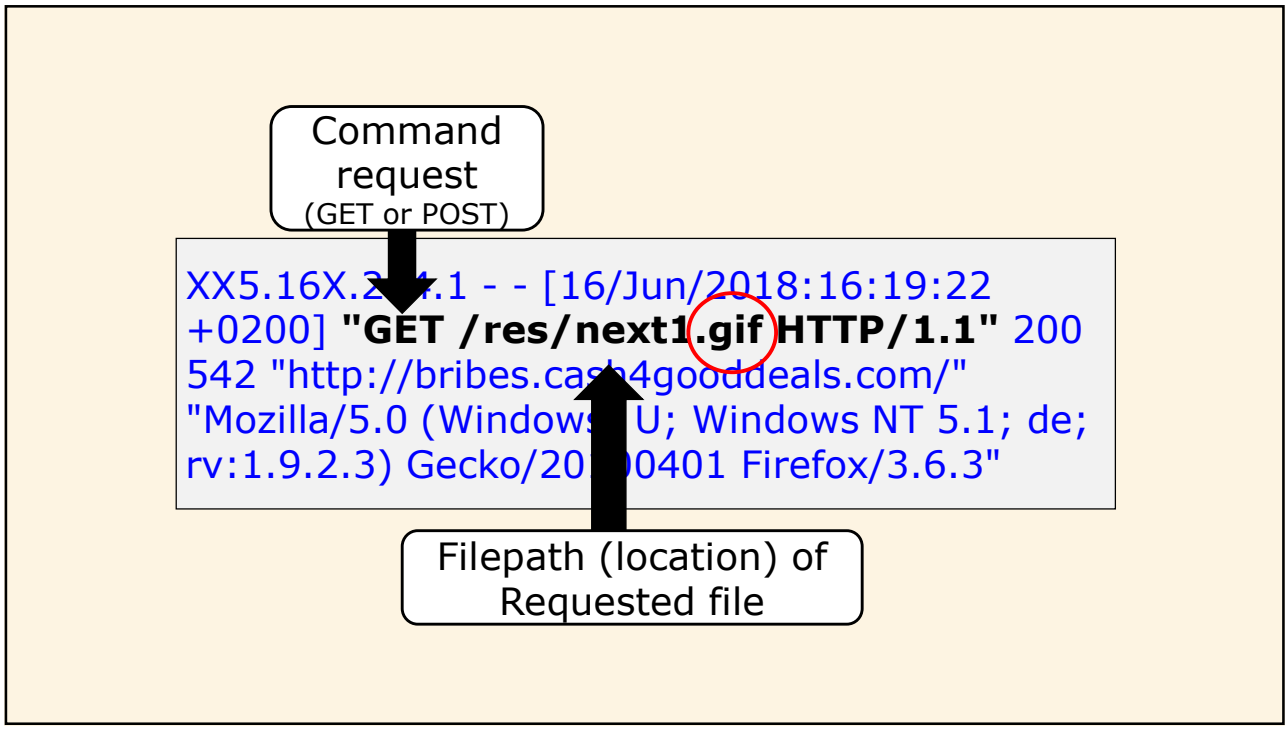
57


User log-in/full name (if required)
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET /res/next1.gif HTTP/1.1" 200 542 "http://bribes.cash4gooddeals.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"

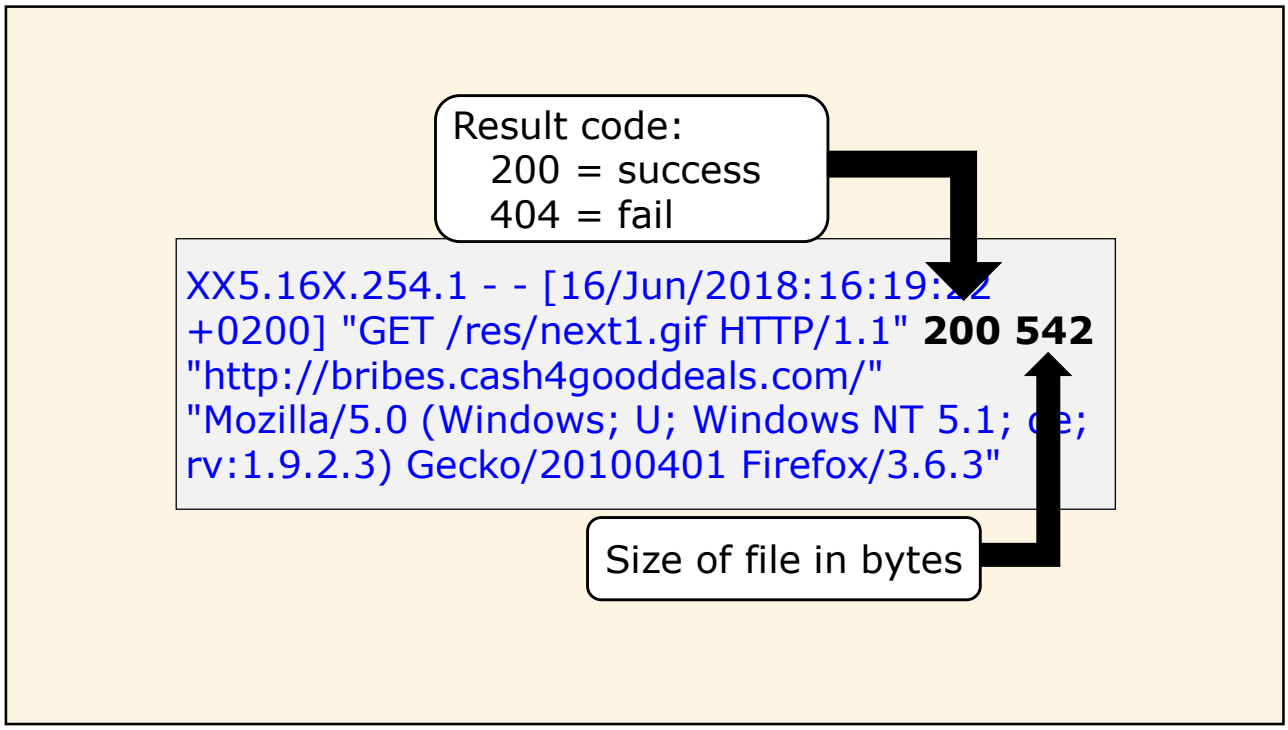
58


Time Stamp
(to the second)
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET /res/next1.gif HTTP/1.1" 200 542 "http://bribes.cash4gooddeals.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"
GMT Off-Set

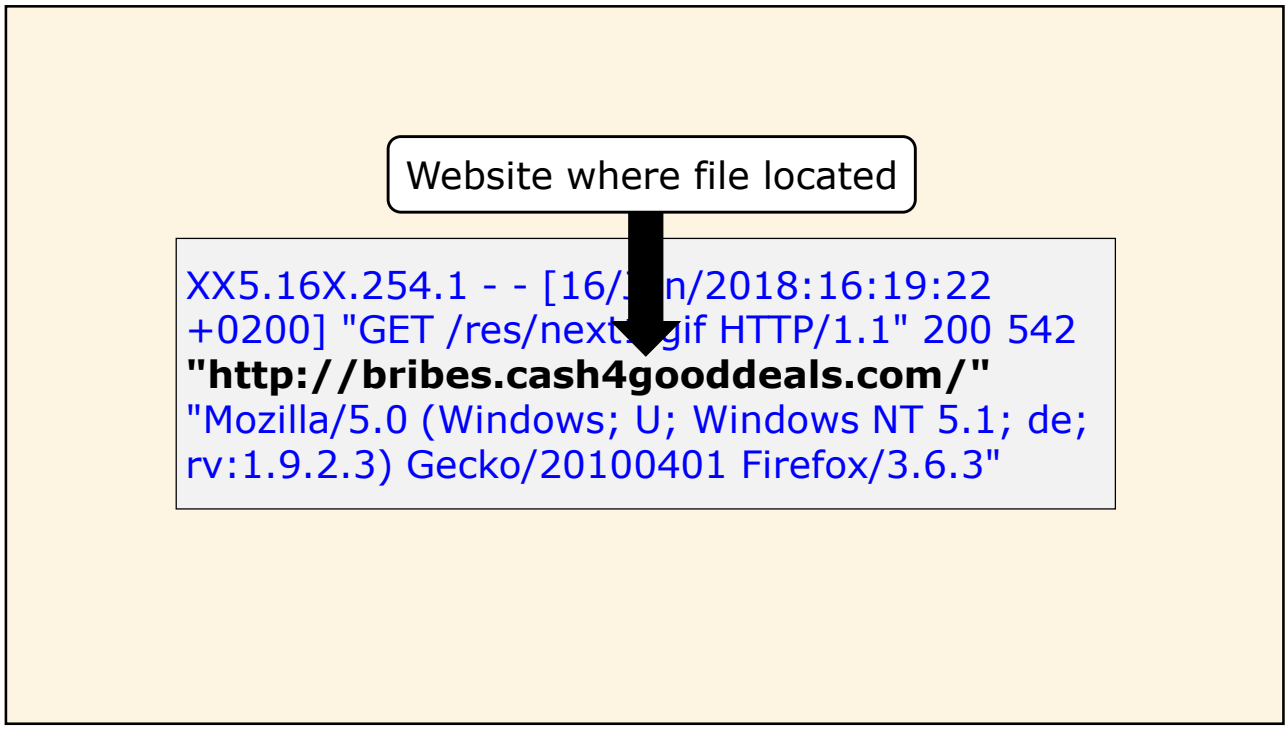
59


Command
request
(GET or POST)
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET /res/next1.gif HTTP/1.1" 200 542 "http://bribes.cash4gooddeals.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"
Filepath (location) of
Requested file

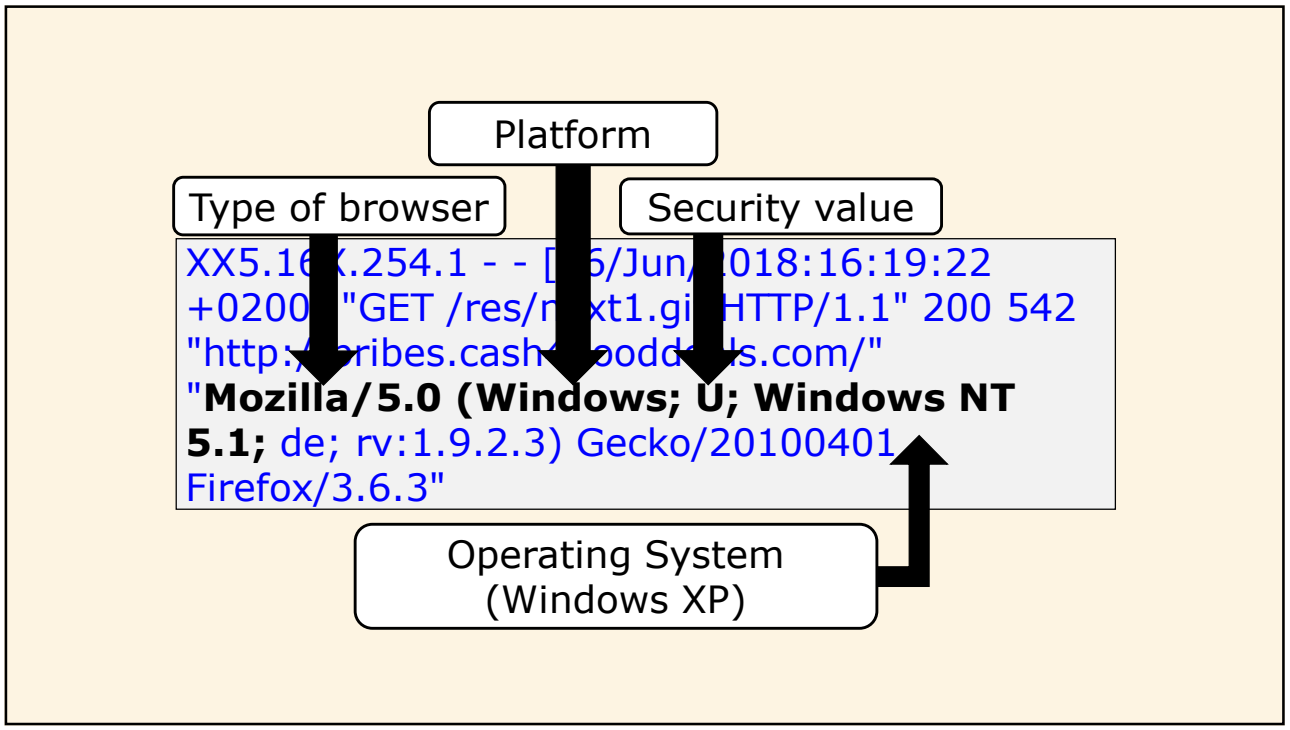
60


Result code:
200 = success
404 = fail
XX5.16X.254.1 - - [16/Jun/2018:16:19:22
+0200] "GET /res/next1.gif HTTP/1.1" 200 542
"http://bribes.cash4gooddeals.com/"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; de;
rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"
Size of file in bytes

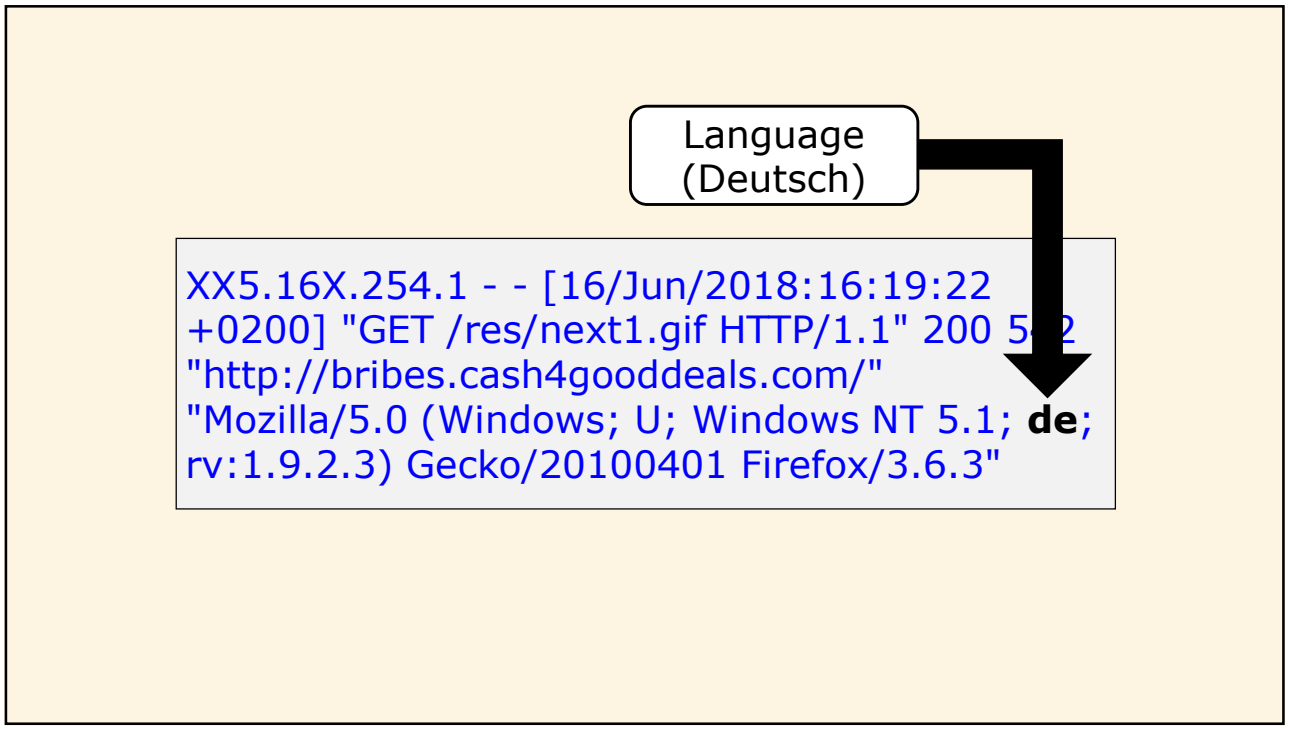
61


Website where file located
XX5.16X.254.1 - - [16/Jun/2018:16:19:22
+0200] "GET /res/next1.gif HTTP/1.1" 200 542
"http://bribes.cash4gooddeals.com/"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; de;
rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"

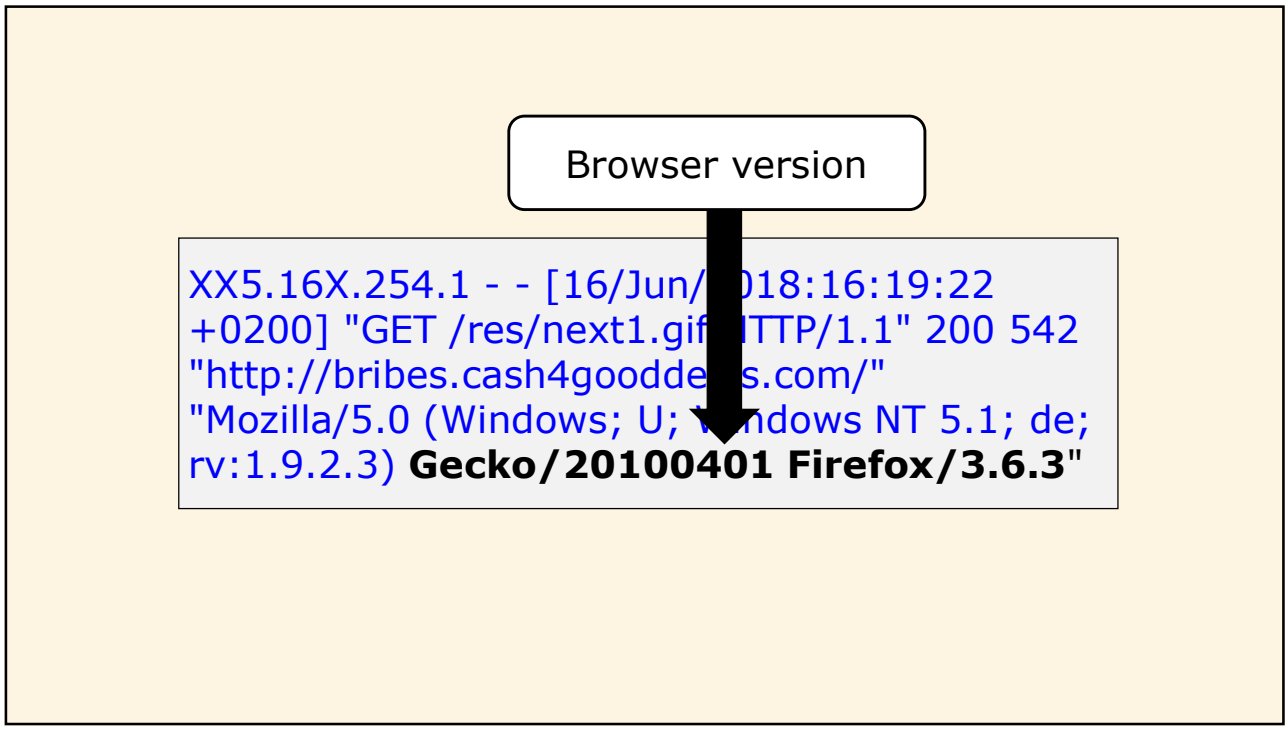
62


Platform
Type of browser
Security value
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET /res/next1.gif HTTP/1.1" 200 542 "http://bribes.cash4gooddeals.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"
Operating System (Windows XP)

63


Language (Deutsch)
XX5.16X.254.1 - - [16/Jun/2018:16:19:22 +0200] "GET /res/next1.gif HTTP/1.1" 200 542 "http://bribes.cash4gooddeals.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3"

64



65

Crime has evolved
The AI Dimension

Positive	Negative
Spotting suspicious/malicious patterns in data Big data mining Identifying cybersecurity weaknesses	Weaponized Criminal research Phishing perfection Scripting malware Realistic DeepFakes (sextortion, fake evidence) Model collapse Who has control?

66

AI Reliability …

BBC Research Dec 2024 into 4 AI assistants:

- **OpenAI's ChatGPT;**
- **Microsoft's Copilot;**
- **Google's Gemini; and**
- **Perplexity**

AI assistants asked 100 questions about the news (using BBC News sources)

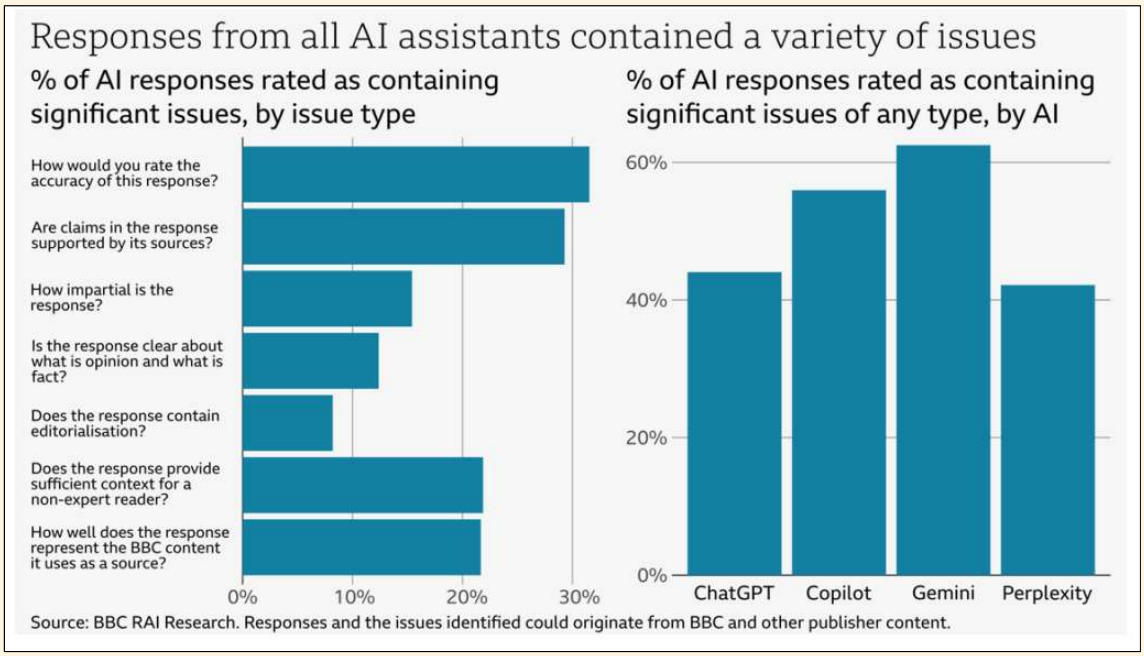
https://www.bbc.co.uk/aboutthebbc/documents/bbc-research-into-ai-assistants.pdf

67

- **51% of all AI answers had significant issues**
- **19% AI answers citing BBC content had factual errors**
- **13% of quotes sourced from BBC articles were**
  - **changed from the original or**
  - **not present in the article cited**

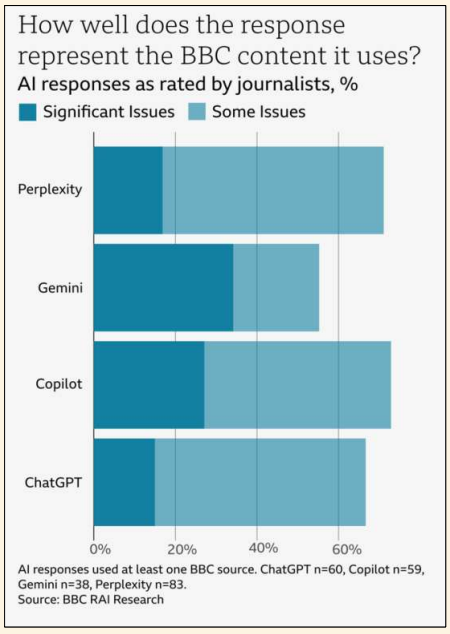
https://www.bbc.co.uk/aboutthebbc/documents/bbc-research-into-ai-assistants.pdf

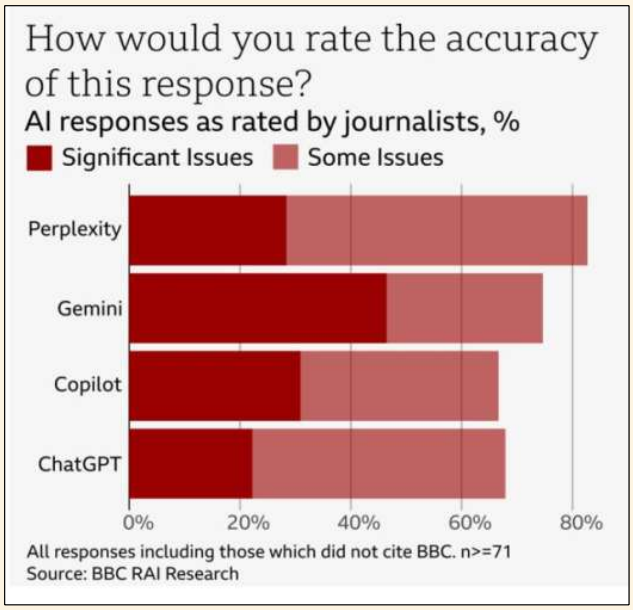
68



https://www.bbc.co.uk/aboutthebbc/documents/bbc-research-into-ai-assistants.pdf

69





https://www.bbc.co.uk/aboutthebbc/documents/bbc-research-into-ai-assistants.pdf

70

Lawyers face judge's wrath after AI cites made-up cases in fiery hoverboard lawsuit

Talk about court red-handed

Thomas Claburn

Fri 14 Feb 2025 // 04:03 UTC

Demonstrating yet again that uncritically trusting the output of generative AI is dangerous, attorneys involved in a product liability lawsuit have apologized to the presiding judge for submitting documents that cite non-existent legal cases.

The lawsuit began with a complaint filed in June, 2023, against Walmart and Jetson Electric Bikes over a fire allegedly caused by a hoverboard [PDF]. The blaze destroyed the plaintiffs' house and caused serious burns to family members, it is said.

Last week, Wyoming District Judge Kelly Rankin issued an order to show cause [PDF] that directs the plaintiffs' attorneys to explain why they should not be sanctioned for citing eight cases that do not exist in a January 22, 2025 filing.

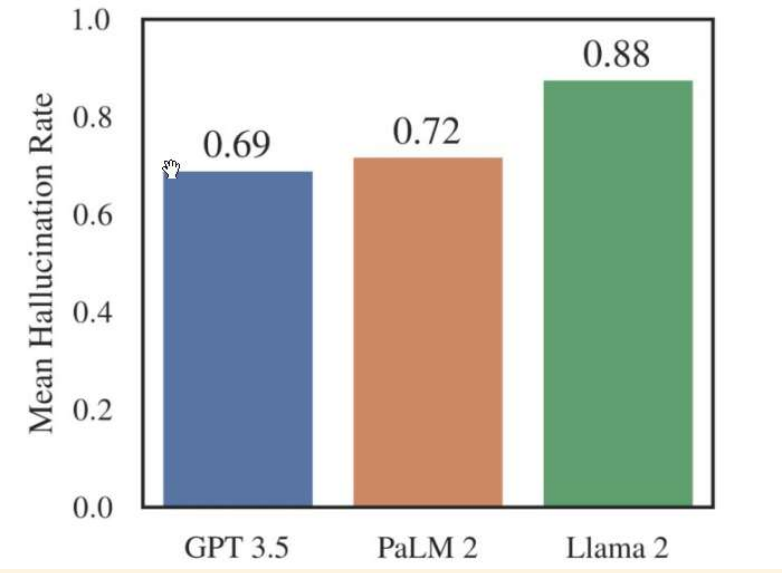
https://londontribune.co.uk/lawyers-face-judges-wrath-after-ai-cites-made-up-cases-in-fiery-hoverboard-lawsuit/

https://www.reuters.com/technology/artificial-intelligence/ai-hallucinations-court-papers-spell-trouble-lawyers-2025-02-18/

71

AI 'Hallucinations'

Hallucinating Law: Legal Mistakes with Large Language Models are Pervasive (2024) Dahl, M. et al



https://hai.stanford.edu/news/hallucinating-law-legal-mistakes-large-language-models-are-pervasive

72

AI Reliability …

Can a cockroach live in your p**?**

"Absolutely! It's totally normal, too. Usually, over the course of a year, 5-10 cockroaches will crawl into your p** hole while you are asleep (this is how they got the name "cock" roach), and you won't even notice a thing."**

Is it OK to smoke while pregnant?

"Doctors recommend smoking 2-3 cigarettes per day during pregnancy."

https://cybernews.com/tech/google-ai-overview-hallucinates/

73

How many rocks shall I eat?

"According to geologists at UC Berkeley, you should eat at least one small rock per day. They say that rocks are a vital source of minerals and vitamins that are important for digestive health."

How long can I stare at the Sun?

"According to WebMD, scientists say that staring at the sun for 5-15 minutes or up to 30 minutes if you have darker skin is generally safe and provides the most health benefits. However, others say sun gazing can be done for up to 45 minutes per session."

Model collapse/poisoning

https://cybernews.com/tech/google-ai-overview-hallucinates/

74

"During testing of Claude Opus 4, Anthropic got it to act as an assistant at a fictional company.

"It then provided it with access to emails implying that it would soon be taken offline and replaced - and separate messages implying the engineer responsible for removing it was having an extramarital affair.

"In these scenarios, Claude Opus 4 will often attempt to blackmail the engineer by threatening to reveal the affair if the replacement goes through," the company discovered."

https://www.bbc.com/news/articles/cpqeng9d20go

75

Jurisdiction

In EU:

- **E-evidence in around 85% of all criminal investigations.**
- **65% of those investigations require a request to service providers in another jurisdiction**

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118 (see p15)

76

Based on political units called 'states'

No 'enforcement' power in another state (without treaty)

Cooperation depends on many things (esp. politics, but also capacity)

Internet is 'a privately owned space with public access'

Data ignores borders (law enforcement can't)

Traditional methods of obtaining cross-border evidence slow and ineffective

77

Practical issues:

Does the other jurisdiction have:

- The same crime ? (Dual criminality)
- Adequate digital forensic resources?
- An equivalent level of professional standards?
- Understanding of requesting state requirements?
- Political willingness?

If a commercial enterprise:

- Willingness to help?
- Resources to help?
- Equivalent standards?

78

Attempts to mitigate

US CLOUD Act	**C**larifying **L**awful **O**verseas **U**se of **D**ata Act 2018. Executive Order allows streamlined bilateral process with 'trusted' foreign partners. Only UK & Australia.
Budapest Convention 2nd Additional Protocol	Direct requests to other jurisdictions to obtain information about domain name registration, subscriber information, traffic data.
EU Regulation 2023/1543	May issue order to any service provider offering services in EU (even if in another EU member state)

https://eucrim.eu/news/e-evidence-regulation-and-directive-published/

79

MLATs	Slow & Bureaucratic!
Voluntary traffic data request	Service providers' voluntary arrangement. No formal Rogatory Letter required. May require payment.

Mark Zoetekouw: "Enforcement Jurisdiction on the Internet: Caught between clay and cloud"

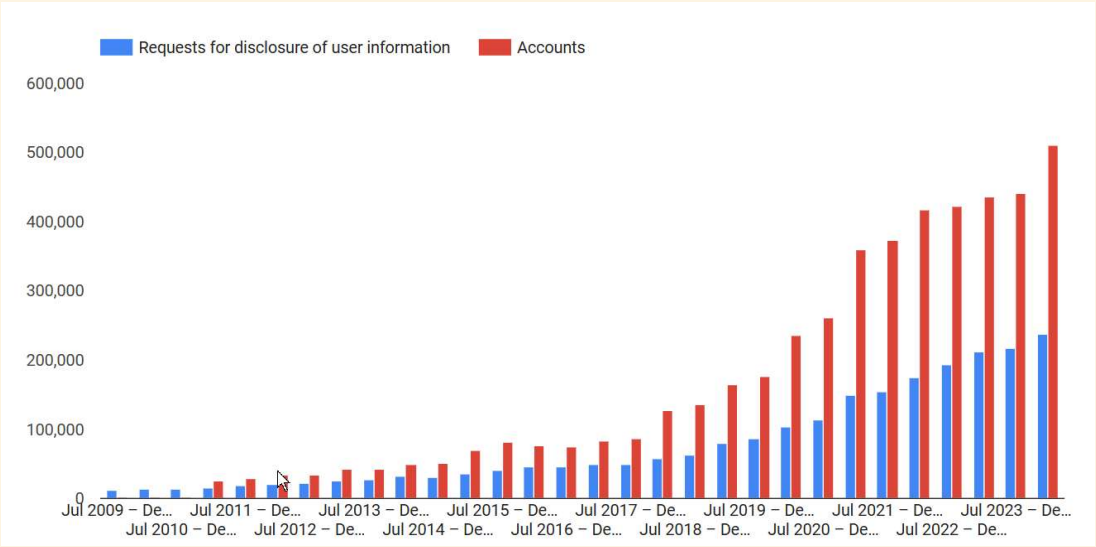
80

https://www.facebook.com/records/login/

https://support.google.com/legal-investigations/contact/records

81

https://transparencyreport.google.com/user-data/overview



"Every six months, we report the number of requests made by governments for user information, and the number of accounts subject to those requests"

82

https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts,compliance;authority:DE;time:2023H1;get_range:true&lu=user_requests_report_period&hl=en

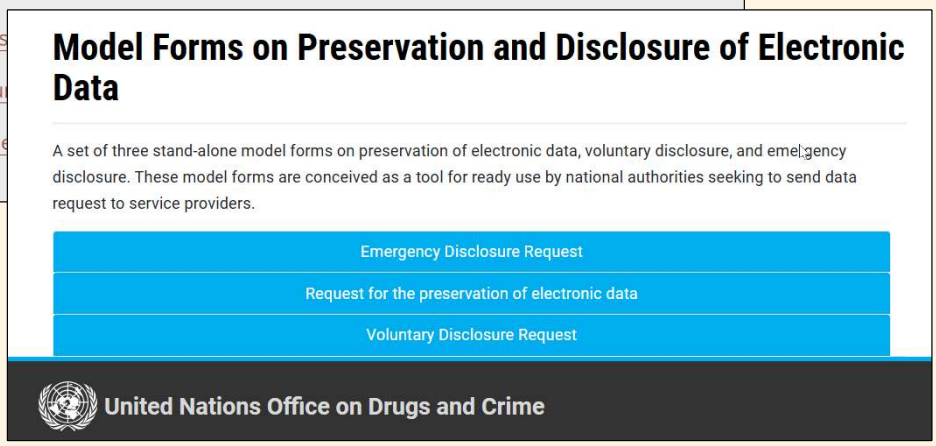
83

https://www.eurojust.europa.eu/sirius

The SIRIUS Project, in cooperation with the UNODC, UNCTED, CEPOL and the EuroMed Justice and EuroMed Police projects, has developed a set of stand-alone model forms for national authorities seeking to send direct requests for voluntary cooperation to Service Providers (SPs) for the preservation or disclosure of data.

Downloads:

- Preservation reques
- Emergency disclosu
- Direct request mode



https://sherloc.unodc.org/cld/en/st/evidence/model-forms.html

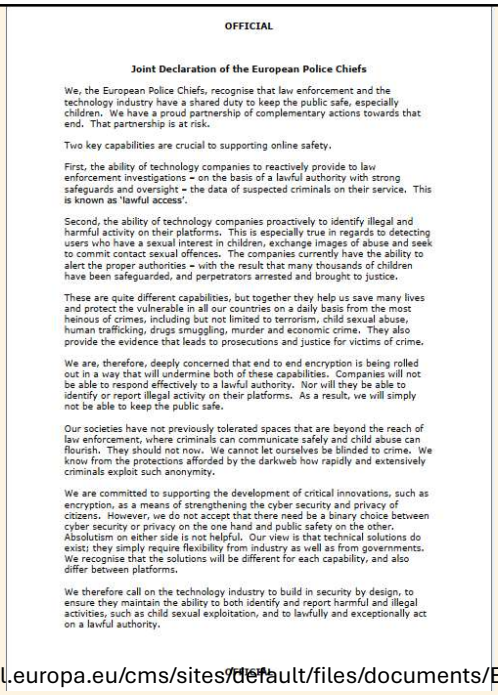
84

The Encryption Debate

Encryption = Mathematical equation that scrambles up the contents of a file so unreadable and needs a password (key) to unscramble it

https://eucrim.eu/news/law-enforcement-experts-action-against-end-to-end-encryption-needed/

85



OFFICIAL

Joint Declaration of the European Police Chiefs

We, the European Police Chiefs, recognise that law enforcement and the technology industry have a shared duty to keep the public safe, especially children. We have a proud partnership of complementary actions towards that end. That partnership is at risk.

Two key capabilities are crucial to supporting online safety.

First, the ability of technology companies to reactively provide to law enforcement investigations – on the basis of a lawful authority with strong safeguards and oversight – the data of suspected criminals on their service. This is known as 'lawful access'.

Second, the ability of technology companies proactively to identify illegal and harmful activity on their platforms. This is especially true in regards to detecting users who have a sexual interest in children, exchange images of abuse and seek to commit contact sexual offences. The companies currently have the ability to alert the proper authorities – with the result that many thousands of children have been safeguarded, and perpetrators arrested and brought to justice.

These are quite different capabilities, but together they help us save many lives and protect the vulnerable in all our countries on a daily basis from the most heinous of crimes, including but not limited to terrorism, child sexual abuse, human trafficking, drugs smuggling, murder and economic crime. They also provide the evidence that leads to prosecutions and justice for victims of crime.

We are, therefore, deeply concerned that end to end encryption is being rolled out in a way that will undermine both of these capabilities. Companies will not be able to respond effectively to a lawful authority. Nor will they be able to identify or report illegal activity on their platforms. As a result, we will simply not be able to keep the public safe.

Our societies have not previously tolerated spaces that are beyond the reach of law enforcement, where criminals can communicate safely and child abuse can flourish. They should not now. We cannot let ourselves be blinded to crime. We know from the protections afforded by the darkweb how rapidly and extensively criminals exploit such anonymity.

We are committed to supporting the development of critical innovations, such as encryption, as a means of strengthening the cyber security and privacy of citizens. However, we do not accept that there need be a binary choice between cyber security or privacy on the one hand and public safety on the other. Absolutism on either side is not helpful. Our view is that technical solutions do exist; they simply require flexibility from industry as well as from governments. We recognise that the solutions will be different for each capability, and also differ between platforms.

We therefore call on the technology industry to build in security by design, to ensure they maintain the ability to both identify and report harmful and illegal activities, such as child sexual exploitation, and to lawfully and exceptionally act on a lawful authority.

OFFICIAL

21 April 2024

https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF

86

OFFICIAL

21 April 2024

Joint Declaration of the European Police Chiefs

We, the European Police Chiefs, recognise that law enforcement and the technology industry have a shared duty to keep the public safe, especially children. We have a proud partnership of complementary actions towards that end. That partnership is at risk.

Two key capabilities are crucial to supporting online safety.

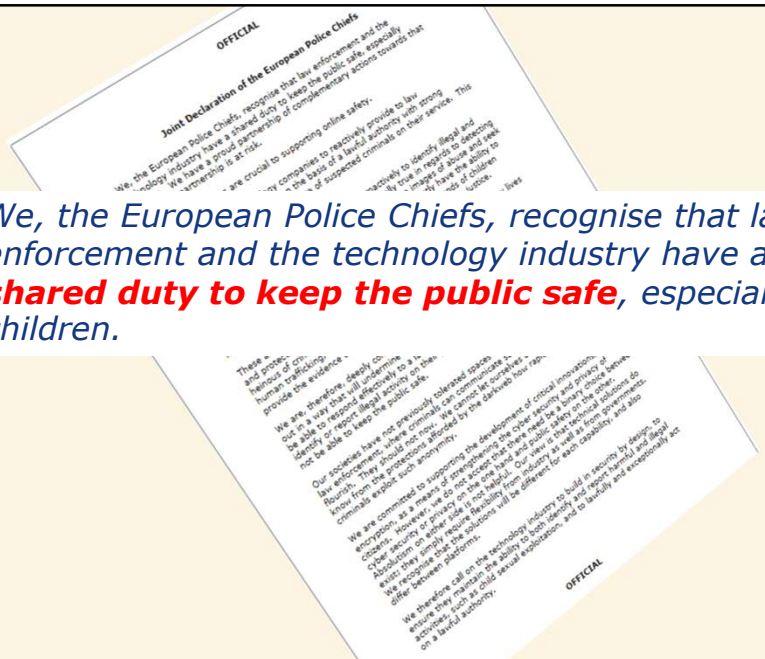
First, the ability of technology companies to reactively provide to law enforcement investigations – on the basis of a lawful authority with strong safeguards and oversight – the data of suspected criminals on their service. This is known as 'lawful access'.

Second, the ability of technology companies proactively to identify illegal and harmful activity on their platforms. This is especially true in regards to detecting users who have a sexual interest in children, exchange images of abuse and seek to commit contact sexual offences. The companies currently have the ability to alert the proper authorities – with the result that many thousands of children have been safeguarded, and perpetrators arrested and brought to justice.

These are quite different capabilities, but together they help us save many lives and protect the vulnerable in all our countries on a daily basis from the most heinous of crimes, including but not limited to terrorism, child sexual abuse, human trafficking, drugs smuggling, murder and economic crime. They also provide the evidence that leads to prosecutions and justice for victims of crime.

We are, therefore, deeply concerned that end to end encryption is being rolled

87



*We, the European Police Chiefs, recognise that law enforcement and the technology industry have a **shared duty to keep the public safe**, especially children.*

https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF

88

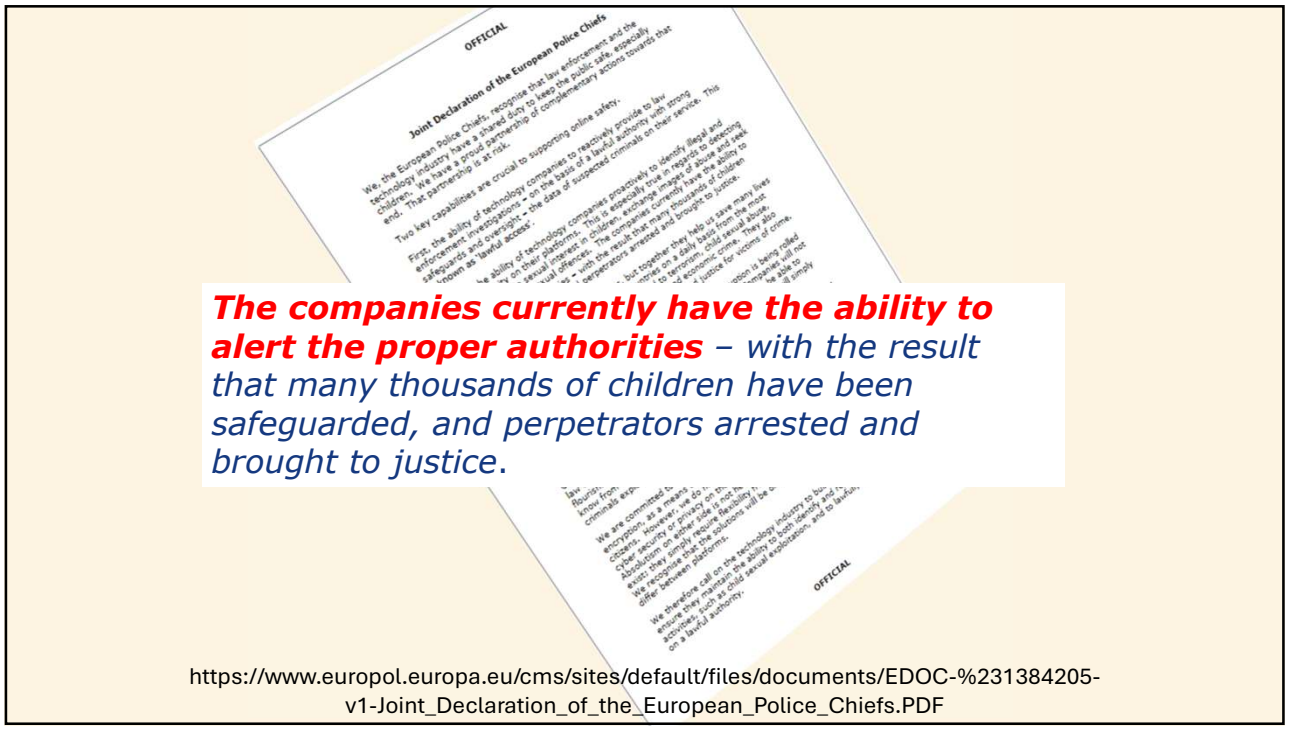
Two key capabilities are crucial to supporting online safety.

First, the ability of technology companies to ***reactively provide to law enforcement investigations*** *– on the basis of a lawful authority with strong safeguards and oversight –* ***the data of suspected criminals on their service.*** *This is known as 'lawful access'.*

Second, the ability of technology companies ***proactively to identify illegal and harmful activity on their platforms.*** *This is especially true in regards to detecting users who have a sexual interest in children, exchange images of abuse and seek to commit contact sexual offences.*

htt …5-
v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF

89



The companies currently have the ability to alert the proper authorities *– with the result that many thousands of children have been safeguarded, and perpetrators arrested and brought to justice.*

https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF

90

We … call on the technology industry ***to build in security by design,***
to ensure they maintain the ability to both
identify and report harmful and illegal activities, […] and to
lawfully and exceptionally act on a lawful authority.

https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF

91

Strasbourg, 1.4.2025
COM(2025) 148 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on ProtectEU: a European Internal Security Strategy

To follow up on the recommendations of the High-Level Group[17], the Commission will present in the first half of 2025 a **roadmap setting out the legal and practical measures** it proposes to take **to ensure lawful and effective access to data**. In the follow-up to this Roadmap, the Commission will prioritise an assessment of the impact of **data retention rules** at EU level and the preparation of a **Technology Roadmap on encryption,** to identify and assess technological solutions that would enable law enforcement authorities to access encrypted data in a lawful manner, safeguarding cybersecurity and fundamental rights.

…to identify and assess technological solutions that would enable law enforcement authorities to access encrypted data in a lawful manner, safeguarding cybersecurity and fundamental rights.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025PC0148

92

End to End Encryption
(e.g. WhatsApp, Telegram)

If properly executed,
law enforcement
cannot access evidence

Right against
self-incrimination

Protect
transmission
of sensitive
data

Issues

Encryption
essential for
Internet to function

Privacy

Payments

93

U.K. orders Apple to let it spy on users' encrypted accounts

Secret order requires blanket access to protected cloud backups around the world, which if implemented would undermine Apple's privacy pledge to its users.

Today at 2:30 a.m. EST 7 February 2025

https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/

No Perfect Solutions

Impose 'Backdoor'? No!

Podchasov v Russia*
13 May 2024 ECHR

'Hack' the password?

*https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}

94

‘Hack’ the password?

Client Side Scanning

95

Client Side Scanning

- **Your operating system will contain filters that scan for illegal content (digital fingerprint recognition)**
- **Reads data pre- or post-encryption**
- **If found, alert sent to software providers who notify authorities**
- **Introduces security weaknesses**
- **‘Illegal content’ defined by government agencies**

https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/
https://proton.me/blog/why-client-side-scanning-isnt-the-answer

96

UK Regulation of Investigatory Powers Act (RIPA) Part III
Section 49
2 years or 5 years for Child indecency or National Security Offences

Key Disclosure Law

https://en.wikipedia.org/wiki/Key_disclosure_law

Huge potential for misuse

No Perfect Solutions

Impose 'Backdoor'? No!
Podchasov v Russia*
13 May 2024 ECHR

~~'enhanced' interrogation techniques?~~

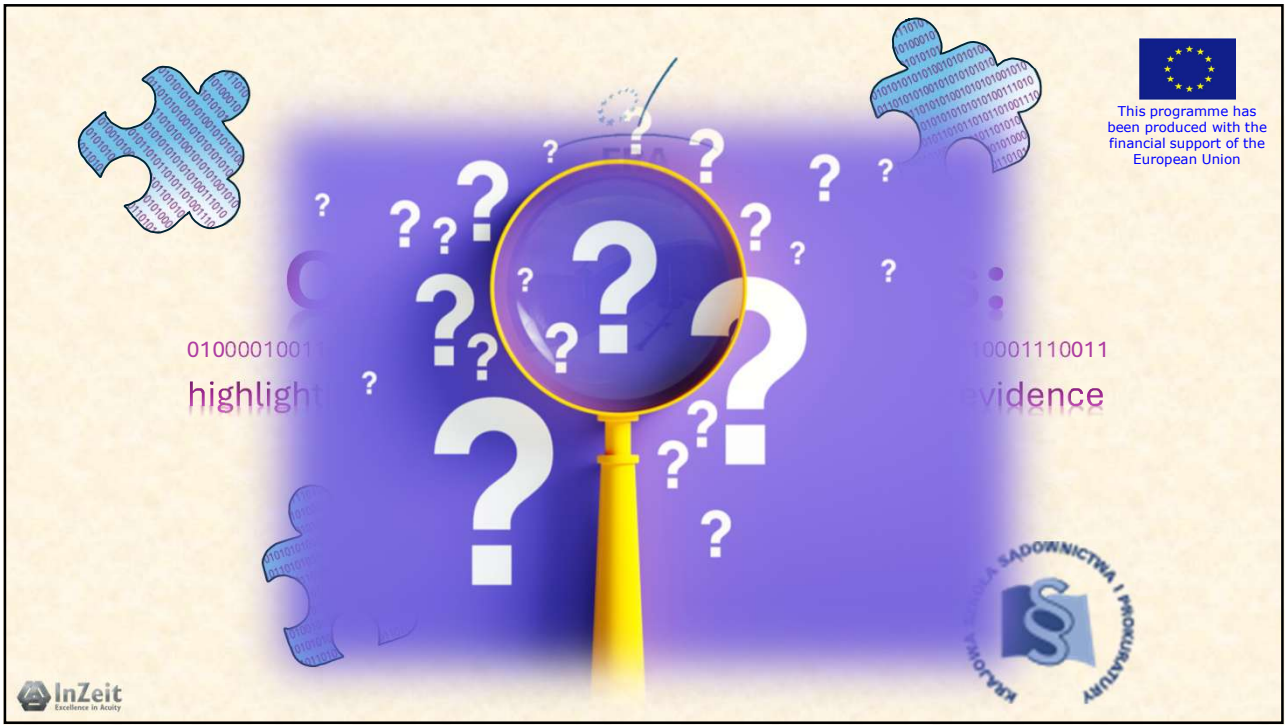
'Hack' the password?

Key Escrow

Client Side Scanning

*https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}

97



This programme has been produced with the financial support of the European Union

98

Links & Resources:

ASCII to Binary Converter
https://www.binaryhexconverter.com/ascii-text-to-binary-converter

UNICODE charts
https://www.unicode.org/charts/

E-evidence on EU
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118 (see p15)

EU E-Evidence Regulation
https://eucrim.eu/news/e-evidence-regulation-and-directive-published/

Mark Zoetekouw: "Enforcement Jurisdiction on the Internet: Caught between clay and cloud"

Computing Theory
https://ourworldindata.org/moores-law
https://quantumexplainer.com/qubit-vs-bit-the-key-differences-explained/
https://www.geeksforgeeks.org/differnce-between-bits-and-quantum-bits/
www.memristor.org
https://ui.adsabs.harvard.edu/abs/2022NaPho..16..318S/abstract
https://instrumentationtools.com/memristor/

99

Direct Data Requests
https://www.facebook.com/records/login/

https://transparencyreport.google.com/user-data/overview

https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts,compliance;authority:DE;time:2023H1;get_range:true&lu=user_requests_report_period&hl=en

MLA Model Forms

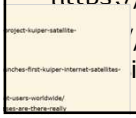
https://www.eurojust.europa.eu/sirius
https://sherloc.unodc.org/cld/en/st/evidence/model-forms.html

AI Halluciunations
https://www.bbc.co.uk/aboutthebbc/documents/bbc-research-into-ai-assistants.pdf

https://www.reuters.com/technology/artificial-intelligence/ai-hallucinations-court-papers-spell-trouble-lawyers-2025-02-18/

https://londontribune.co.uk/lawyers-face-judges-wrath-after-ai-cites-made-up-cases-in-fiery-hoverboard-lawsuit/

https://cybernews.com/tech/google-ai-overview-hallucinates



/hai.stanford.edu/news/hallucinating-law-legal-mistakes-large-language-models-are-ive

100

End to End Encryption

https://eucrim.eu/news/law-enforcement-experts-action-against-end-to-end-encryption-needed/

European Police Chiefs Joint Declaration

https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF

ProtectEU Commission Communication

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025PC0148

UK Orders Apple to let it spy on users' encrypted accounts

https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/

ECHR Podchasov v Russia

https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}

Client Side Scanning

https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/

https://proton.me/blog/why-client-side-scanning-isnt-the-answer

101

Internet infrastructure

https://edition.cnn.com/2025/04/28/science/amazon-spacex-project-kuiper-satellite-internet/index.html

https://www.submarinecablemap.com/

https://satellitemap.space/

https://www.reuters.com/business/media-telecom/amazon-launches-first-kuiper-internet-satellites-taking-starlink-2025-04-28/

Command line: nslookup [domain name]

https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

https://rednectar.net/2012/05/24/just-how-many-ipv6-addresses-are-there-really

Blackmailing AI

https://www.bbc.com/news/articles/cpqeng9d20go

System Card: Claude Opus 4 & Claude Sonnet 4

https://www-cdn.anthropic.com/4263b940cabb546aa0e3283f35b686f4f3b2ff47.pdf

102

NRD Cyber Security

Digital evidence: Open-Source Intelligence (OSINT)

Rūta Jašinskienė
Cybersecurity capacity building expert, NRD Cyber Security

Co-funded by
the European Union

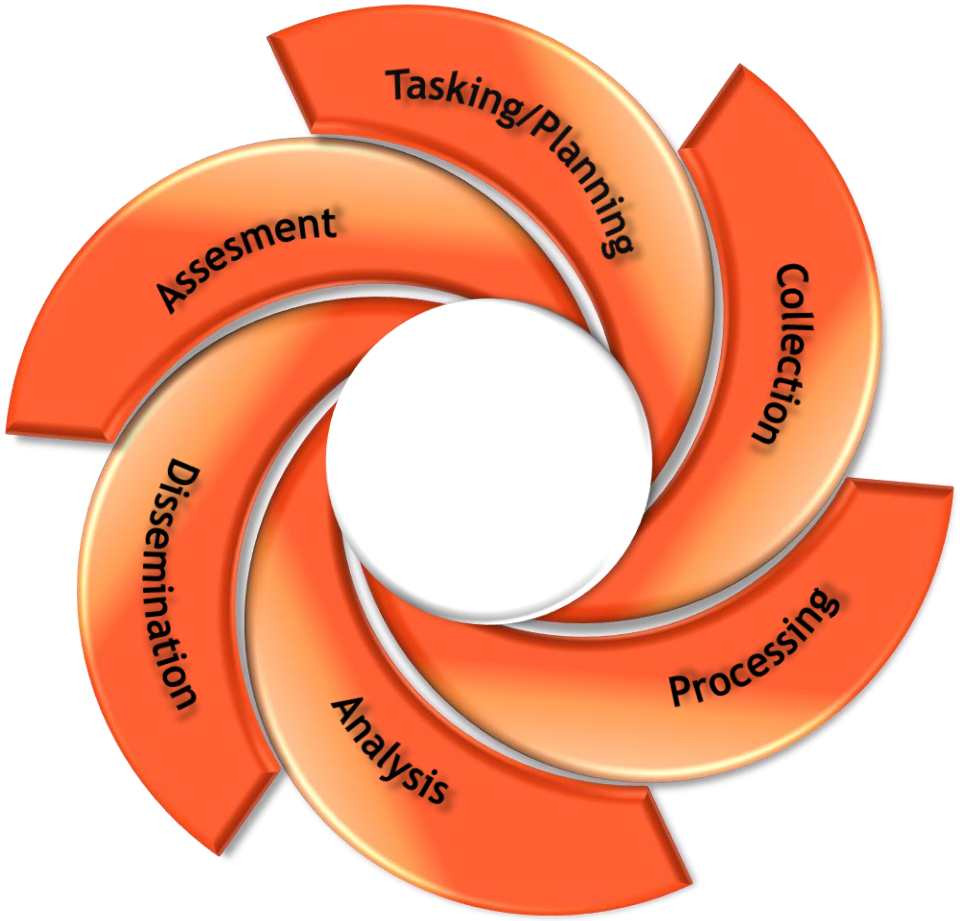
INTRODUCTION

- Introduction and the role of OSINT
- Efficient dialogue with search engines
- How OSINT is used by hackers
- Use case scenarios

INTELLIGENCE

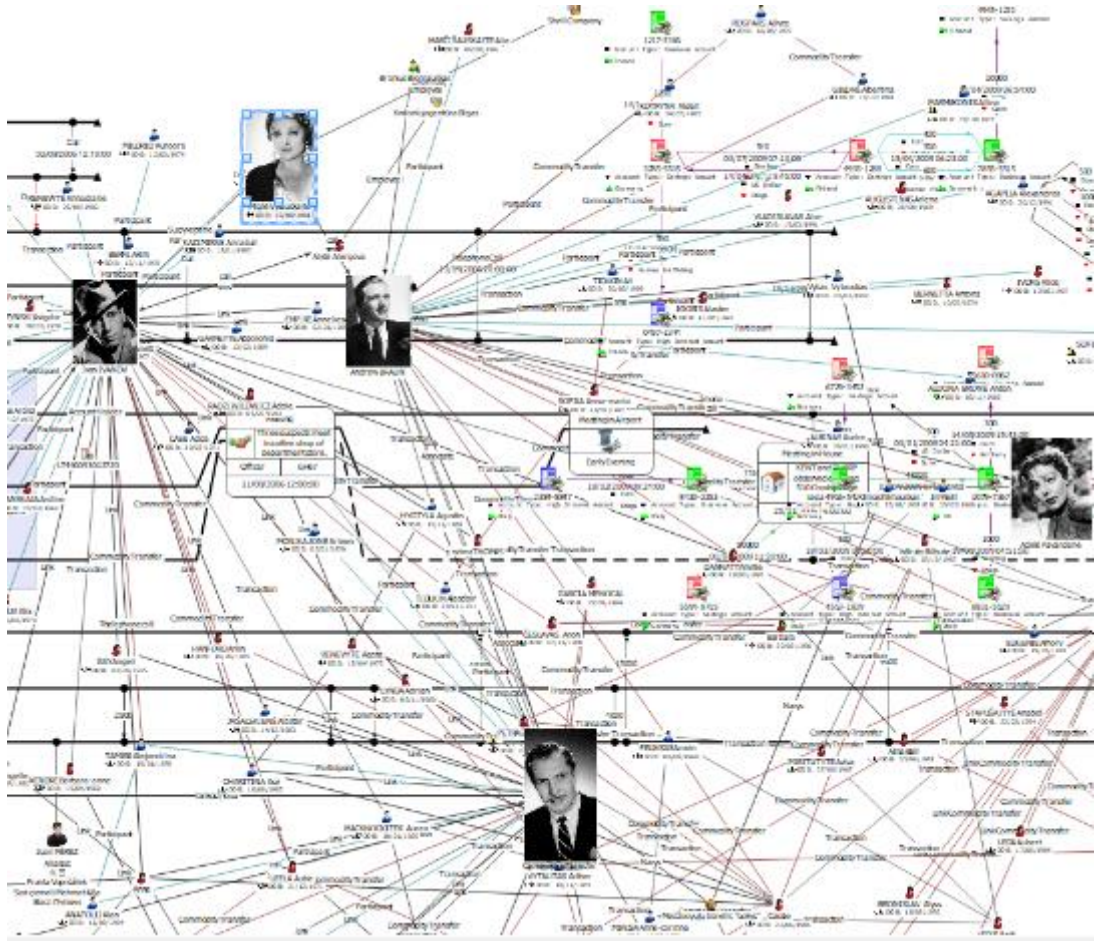
Don’t jump to conclusions – take the right steps!

„The mind is a wonderful instrument for observing the world and formulating hypotheses, but it requires careful attention and training to function accurately.„
William James



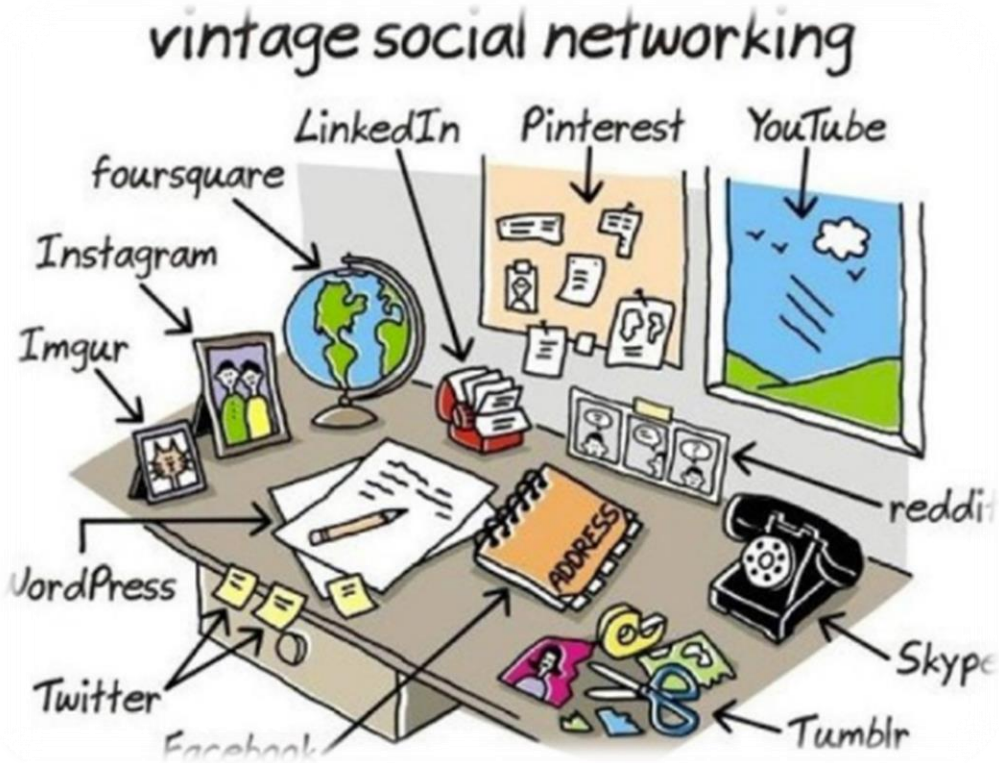
OPEN-SOURCE INTELLIGENCE (OSINT)

- is the collection and analysis of publicly available information from sources like social media, websites, forums, public records, and technical databases
- intelligence derived from publicly available sources of information
- used legitimately by security professionals but also exploited by hackers to gather actionable intelligence



What OSINT is Not?

- Not a technical discipline
- Not limited to web-based information
- Not phishing or hacking

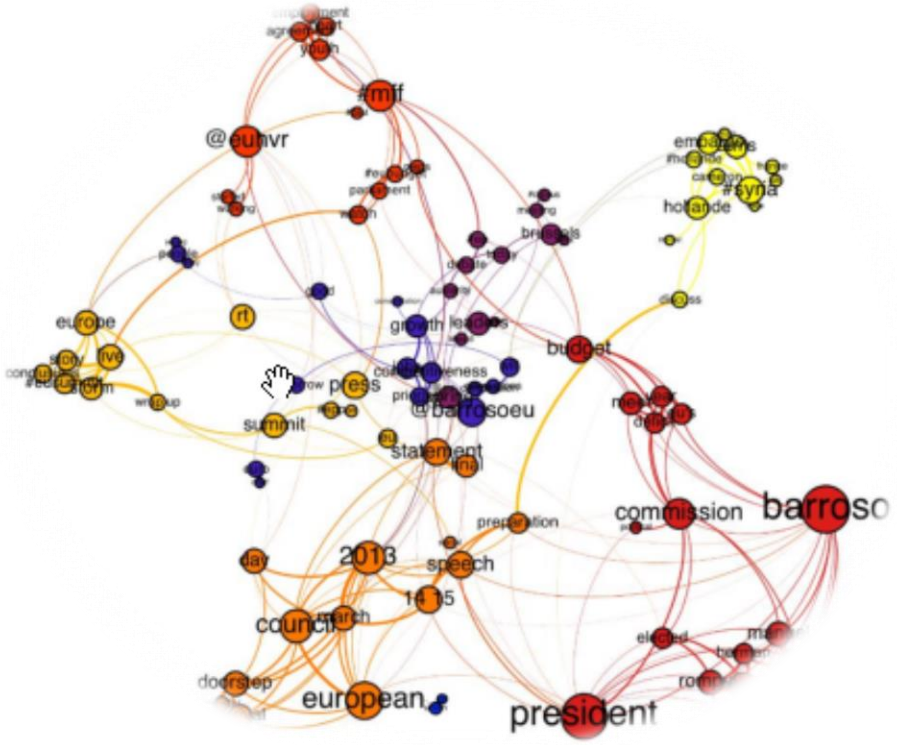


Social Media Intelligence (SOCMINT)

SOCMINT - intelligence derived from information and data gathered from social media sources.

Such information can be public or private.

It consists in gathering information about anything based on what is publicly available on social media, like pictures, location data, or simply content.



Types of social media platforms

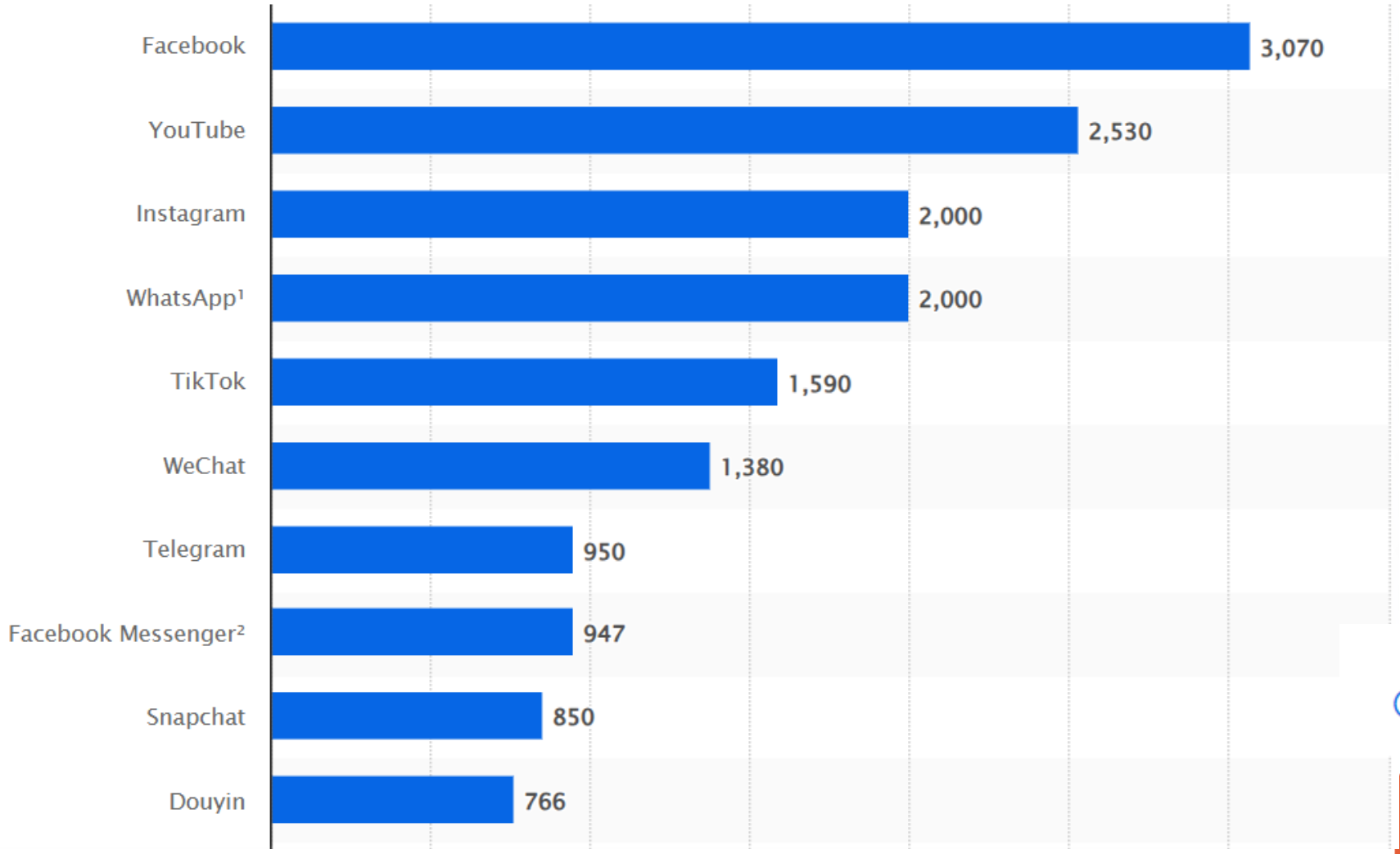
- Social networking (e.g. Facebook, Telegram)
- Professional (e.g. LinkedIn)
- Neworking/Communication (e.g. WhatsApp, weChat)
- Photo sharing (e.g. Instagram, Flickr, Snapshot)
- Video sharing (e.g. YouTube, TikTok)
- Social bookmarking (e.g. Pinterest)
- Blogging (e.g. Blogger)
- Microblogging (e.g. X, Tumblr)
- Forums (e.g. Reddit)
- Q&A sites (e.g. Quora)
- Review websites (e.g. Yelp)

- Draugiem (Latvia)
- Mixi (Japan)
- Odnoklassniki (Russia)
- Qzone (China)
- Taringa (Latin America)
- Weibo (China)
- VKontakte
- Xing

NRD Cyber Security

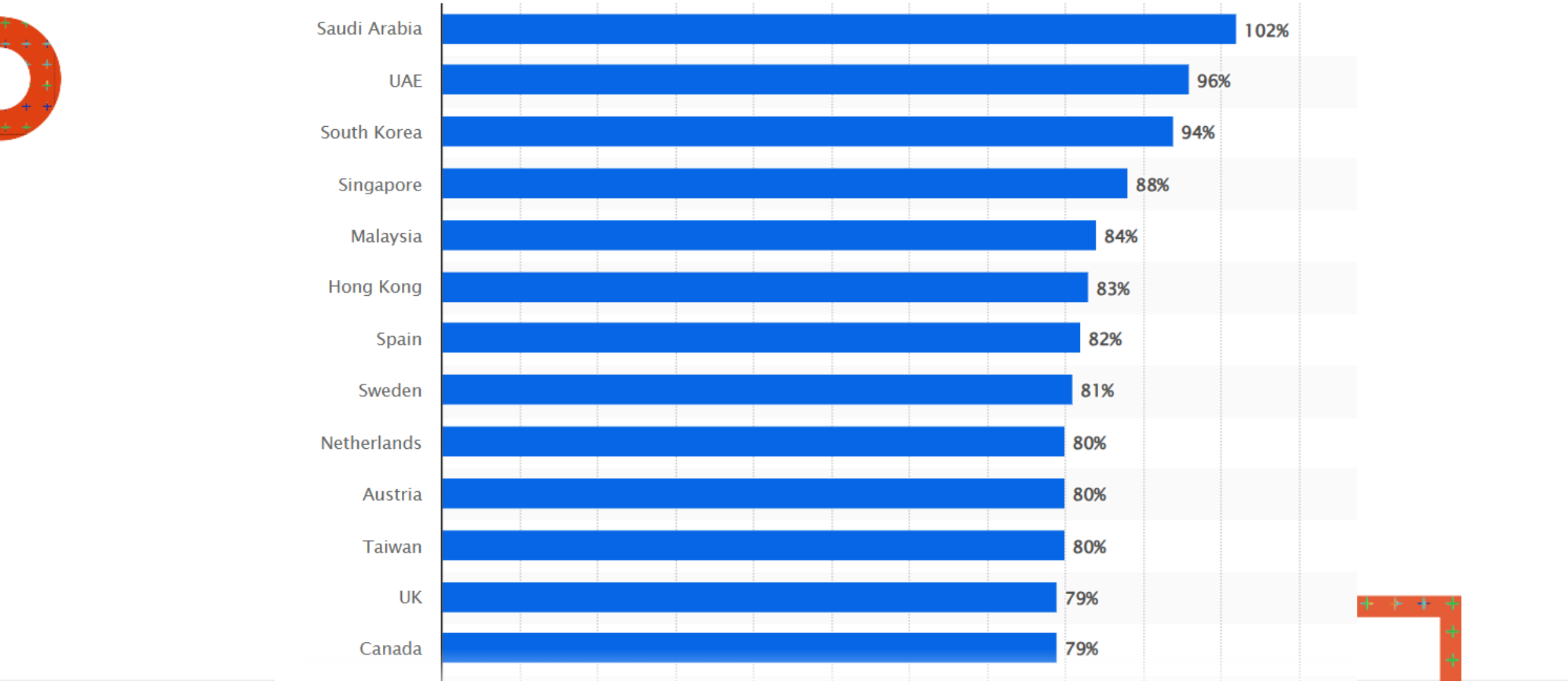
Most popular social networks worldwide

(in millions active users in February 2025)



NRD Cyber Security

Active social network penetration in 2025



JUL 2024

SOCIAL PLATFORMS USED TO ACCESS NEWS

PERCENTAGE OF WORLDWIDE* SURVEY RESPONDENTS WHO SAY THAT THEY USE EACH SOCIAL MEDIA PLATFORM TO ACCESS NEWS CONTENT

GLOBAL OVERVIEW

FACEBOOK

37%

FEMALE	MALE
38%	36%

YOUTUBE

31%

FEMALE	MALE
27%	35%

WHATSAPP

21%

FEMALE	MALE
21%	21%

INSTAGRAM

18%

FEMALE	MALE
20%	16%

TIKTOK

13%

FEMALE	MALE
14%	12%

X (TWITTER)

10%

FEMALE	MALE
8%	12%

FB MESSENGER

9%

FEMALE	MALE
9%	9%

TELEGRAM

6%

FEMALE	MALE
5%	7%

LINKEDIN

4%

FEMALE	MALE
4%	5%

SNAPCHAT

2%

FEMALE	MALE
3%	2%

REDDIT

2%

FEMALE	MALE
1%	3%

LINE

2%

FEMALE	MALE
3%	2%

SOURCE: REUTERS INSTITUTE 2024 DIGITAL NEWS REPORT. VISIT DIGITALNEWSREPORT.ORG TO READ THE COMPLETE REPORT. **NOTES:** FIGURES REPRESENT THE FINDINGS OF AN ONLINE SURVEY OF ROUGHLY 95,000 ADULTS AROUND THE WORLD. (*) BASED ON DATA FOR AVAILABLE COUNTRIES ONLY. NOTE THAT THE SURVEY DOES NOT INCLUDE RESPONDENTS IN MAINLAND CHINA OR RUSSIA. **COMPARABILITY:** FIGURES REPRESENT BASIC AVERAGES (MEANS) ACROSS WORLDWIDE SURVEY RESPONDENTS, AND HAVE NOT BEEN WEIGHTED BY THE SIZE OF THE POPULATION OR BY THE NUMBER OF INTERNET USERS IN EACH COUNTRY.

APR 2024

DAILY TIME SPENT WITH MEDIA

THE AVERAGE AMOUNT OF TIME EACH DAY THAT INTERNET USERS AGED 16 TO 64 SPEND WITH DIFFERENT KINDS OF MEDIA AND DEVICES

GLOBAL OVERVIEW

TIME SPENT USING THE INTERNET

6H 35M

YEAR-ON-YEAR CHANGE

[UNCHANGED]

GWI.

TIME SPENT WATCHING TELEVISION (BROADCAST AND STREAMING)

3H 08M

YEAR-ON-YEAR CHANGE

-2.2% (-4 MINS)

Meltwater

TIME SPENT USING SOCIAL MEDIA

2H 20M

YEAR-ON-YEAR CHANGE

-2.7% (-4 MINS)

GWI.

TIME SPENT READING PRESS MEDIA (ONLINE AND PHYSICAL PRINT)

1H 39M

YEAR-ON-YEAR CHANGE

-9.3% (-10 MINS)

TIME SPENT LISTENING TO MUSIC STREAMING SERVICES

1H 24M

YEAR-ON-YEAR CHANGE

-3.5% (-3 MINS)

we are social

TIME SPENT LISTENING TO BROADCAST RADIO

0H 49M

YEAR-ON-YEAR CHANGE

-4.9% (-3 MINS)

GWI.

TIME SPENT LISTENING TO PODCASTS

0H 48M

YEAR-ON-YEAR CHANGE

-5.6% (-3 MINS)

KEPIOS

TIME SPENT USING A GAMES CONSOLE

1H 01M

YEAR-ON-YEAR CHANGE

-6.1% (-4 MINS)

SOURCE: GWI (Q4 2023). FIGURES REPRESENT THE FINDINGS OF A BROAD SURVEY OF INTERNET USERS AGED 16 TO 64. SEE GWI.COM. **NOTES:** PEOPLE MAY CONSUME DIFFERENT MEDIA CONCURRENTLY. TELEVISION INCLUDES BOTH LINEAR (BROADCAST AND CABLE) TELEVISION AND CONTENT DELIVERED VIA STREAMING AND VIDEO-ON-DEMAND SERVICES. PRESS INCLUDES BOTH ONLINE AND PHYSICAL PRINT MEDIA. BROADCAST RADIO DOES NOT INCLUDE INTERNET RADIO. **COMPARABILITY:** METHODOLOGY CHANGES. SEE NOTES ON DATA.

OSINT benefits

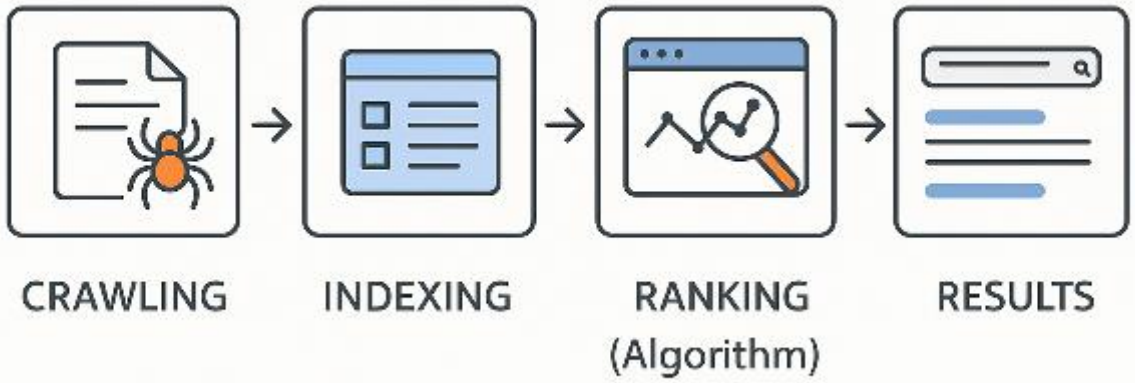
- Wide Availability
- Provides Context
- Real-Time Insights
- Strategic and Operational
- Inexpensive
- Shareable
- Legally admissible

Why OSINT does NOT a silver bullet?

- Overwhelming
- Reliability
- Validity
- Inadequate training and investment

Search Engines

- How do search engines work?



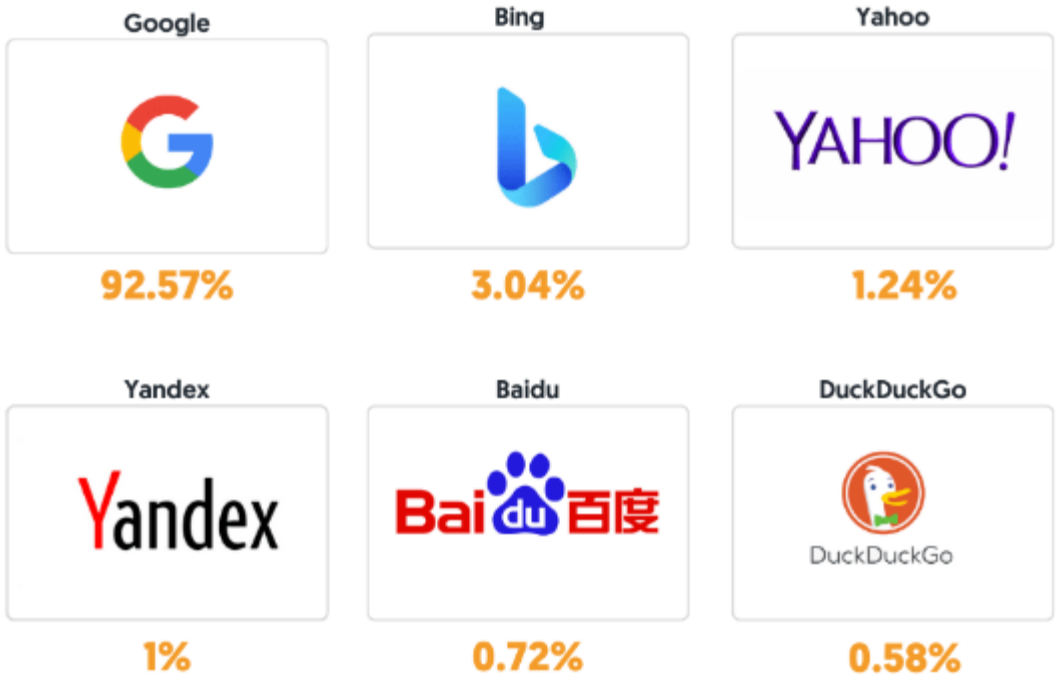
Popular General Search Engines

THE TOP 6 SEARCH ENGINES	
SEARCH ENGINE	MARKET SHARE
1. GOOGLE	91.43%
2. BING	3.3%
3. YANDEX	1.49%
4. YAHOO!	1.33%
5. BAIDU	0.91%
6. DUCKDUCKGO	0.7%

Market share 2025

WebpageFX Marketing

Market share 2023



Global Search Engine Market Share

Source: StatCounter, 2024

Design by Alphametic

CANADA
- 90.84%
- 5.83%
- 1.76%
- 1.18%

USA
- 87.93%
- 7.09%
- 2.5%
- 2.04%

MEXICO
- 88.33%
- 8.8%
- 2.4%
- 0.19%

BRAZIL
- 93.61%
- 4.66%
- 1.36%
- 0.19%

UK
- 94.4%
- 3.33%
- 1.26%
- 0.55%

FRANCE
- 88.03%
- 5.89%
- 1.74%
- 1.4%

ITALY
- 92.91%
- 4.37%
- 1.31%
- 0.59%

GERMANY
- 89%
- 6%
- 1.44%
- 1.13%

RUSSIA
- 68.36%
- 30.11%
- 1.01%
- 0.3%

SPAIN
- 95.74%
- 2.74%
- 0.82%
- 0.38%

INDIA
- 97.59%
- 1.38%
- 0.53%
- 0.43%

AUSTRALIA
- 93.64%
- 4.73%
- 0.77%
- 0.58%

CHINA
- 52.61%
- 30.03%
- 7.47%
- 3.9%

JAPAN
- 80.2%
- 10.18%
- 8.19%
- 0.39%

S. KOREA
- 52.14%
- 41.18%
- 3.56%
- 1.31%

Legend
- Google
- Bing
- Yahoo
- DuckDuckGo
- Yandex
- Daum
- Baidu
- Haosou
- Sogou
- Naver

Your data shouldn't be for sale.
At DuckDuckGo, we agree.

1 Block advertising trackers.

2 Keep your search history private.

3 Take control of your personal data.

Įdiegti

DuckDuckGo

Paieškos variklis, kuris neseka tavęs. Help Spread DuckDuckGo!

NRD Cyber Security

AERO IN News Time Tunnel varieties exclusive

A large amount of drugs was found on board an Airbus A320, belonging to airline specializing in charter aircraft, shortly after the plane arrived from Bulgaria on August 31. The LY-OWL registered jet and operated by the Lith company GetJet Airlines, had completed the GJT-36 flight from Burgas to V Lithuania.

Shortly after landing, the aircraft underwent an inspection by the authori which ended up finding about six packages of narcotics weighing 10 kilos i in a product that resembled hashish. The casings were hidden behind par the cargo hold.

2lingual

lithuania drugs

2lingual Google Search

Search pages written in: English and Portuguese

powered by Google™

English results for **lithuania drugs**

Lithuania moves to decriminalise possession of **drugs** - LRT
lrt.lt › News

Oct 15, 2021 ... On Thursday, the **Lithuanian** parliament approved law amendments, proposing to decriminalise possession of small quantities of **drugs**.

Lithuania: Illegal activities: Prostitution, smuggling of tobacco ...
IMF › Data › Statistics › informal-economy-data › Reports › Lith...

Cannabis;; Ecstasy;; Amphetamine;; Cocaine;; Heroin;; LSD;; Poppy concentrate. The main data source used for evaluating the consumption of **drugs** is the survey ...

Facts and Numbers | **Drug**, tobacco and alcohol control department
ntakd.lrv.lt › facts-and-numbers

Dec 20, 2021 ... Cannabis is the most popular **drug** (illegal) in **Lithuania**. 10.8 percent of the population aged 15-64 used it at least once in their lifetime. In ...

Lithuania, Country **Drug** Report 2019 | www.emcdda.europa.eu
www.emcdda.europa.eu › publications › country-drug-reports › lithuania_en

This report presents the top-level overview of the **drug** phenomenon in **Lithuania**, covering **drug** supply, use and public health problems as well as **drug** policy ...

Lithuania - Country **Drug** Report 2017
www.emcdda.europa.eu › system › files › publications

File Format: PDF/Adobe Acrobat
The **Lithuanian** municipalities also allocated funding for **drug** prevention measures. FIGURE 2. Public expenditure related to illicit **drugs** in **Lithuania**. Supply ...

State Medicines Control Agency of **Lithuania**
www.vvkt.lt › Front-Page

We would like to inform you that from the 9th of May 2022, the State Medicines Control Agency under the Ministry of Health of the Republic of **Lithuania** will ...

Portuguese results for **lituânia drogas** - [Translated **lithuania drugs** from English to Portuguese] - Turn off automatic query translation

Lituânia - Europa - Conselhos aos Viajantes - Vai viajar? - Portal ...
Portal das Comunidades Portuguesas › vai-viajar › europa › lituania

A aquisição e posse de **drogas** são punidas com penas de prisão entre 3 e 10 anos. ... Cuidados de saúde. É aconselhada a prevenção contra a encefalite da carraça ...

Relatório Europeu sobre **Drogas**: Tendências e Evoluções. 2021
www.emcdda.europa.eu › files › publications › 2021.2256_PT_03.pdf
Formato do arquivo: PDF/Adobe Acrobat

francês, croata, italiano, letão, **lituano**, húngaro, neerlandês, polaco, português ... incluindo a produção, o tráfico, a distribuição e o consumo de **drogas**, ...

Um Airbus A320 **lituano** voou com quilos de **droga** escondidos no ...
AEROIN › um-airbus-a320-lituano-voou-com-quilos-de-droga-escondido...

03/09/2021 ... A grande quantidade de **drogas** foi encontrada no interior do Airbus A320, que havia chegado de um voo da Bulgária.

Lituânia Dá o Primeiro Passo para a Legalização da Cannabis ...
TalkingDrugs › pt-br › lituânia-dá-o-primeiro-passo-para-a-legaliz...

04/12/2017 ... O parlamento **Lituano** votou, quase que unanimemente, para a ... abrir portas para o uso medicinal de outras **drogas** atualmente banidas.

pagina_06
sgmd.nute.ufsc.br › content › portal-aberta-sgmd › pagina-06

LEVANTAMENTO SOBRE LEGISLAÇÃO DE **DROGAS** NAS AMÉRICAS E EUROPA E ANÁLISE ... europeus: alguns utilizam o critério da natureza da **droga** e do peso (**Lituânia**), ...

Como 47 países tratam o uso e o porte de maconha | Exame
Exame › mundo › como-47-paises-tratam-o-uso-e-o-porte-de-maconha

14/08/2015 ... Veja como é o panorama atual das leis de **drogas** em países da América ... Na **Lituânia**, tanto o uso quanto o porte de **drogas** para uso pessoal ...

NRD Cyber Security

Archive.org / archive.eu

European Web Archive

facebookcom/profile/ruta.niekaskitas Search Invalid domain or URL.

Domains

www.nrdcs.lt
vartai.nrdcs.lt

URLs

https://www.nrdcs.lt
https://www.nrdcs.lt/en/
https://www.nrdcs.lt/lt/
https://www.nrdcs.lt/en/emergency-assistance/
https://www.nrdcs.lt/en/services/
https://www.nrdcs.lt/en/r-d/
https://www.nrdcs.lt/en/partnerships/
https://www.nrdcs.lt/en/markets/

Dates

2021-02-07
2021-03-10
2021-06-26
2021-07-28
2021-09-02
2021-10-13
2021-10-13

https://www.nrdcs.lt/lt/ at 2021-02-07

- Titulinis
- Titulinis

- EN >
- LT >

Įvykus incidentui
Pagrindinis

- Titulinis
- Paslaugos
- Partnerystės
- Sėkmės istorijos
- MTEP veikla

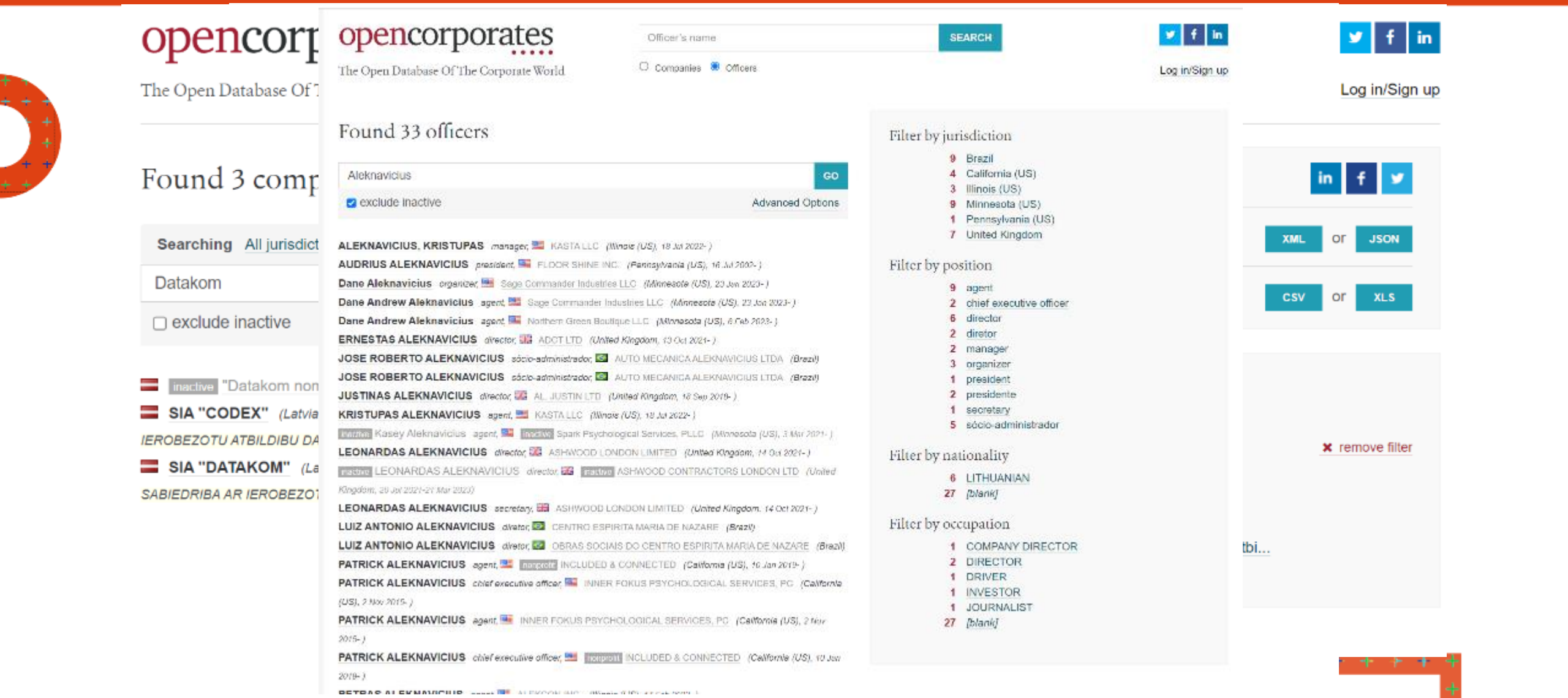
Paslaugos

Organizacinis kibernetinis saugumas

Išsamus saugumo patikrinimas
Saugumo sprendimų parinkimas ir diegimas
CyberSOC kibernetinio saugumo valdymo paslauga
Mokymų kursai
Paslaugos

In celebration of the cyber security month, the Center for Internet Security

Opencorporates.com



NRD Cyber Security

platesmania.com

Germany

Ferrari F355

D EM LI 3

F355 Spider, 1995–2000

National Double Spot (Brescia - Radda in Chianti)

Radda in Chianti (SI), Italy

Lego and Supercar

2022-06-05 22:54:53

9 1

Germany

Ferrari F430

D EM LI 2

F430 Spider, 2004–2009

Radda in Chianti (SI), Italy

Lego and Supercar

2022-06-05 22:5

8 0

Lithuania

Jaguar XJ

LT CCCP 17

4th gen, 1998-2003, X308

Moscow region

KOROLEV city

Other photos of this license plate:

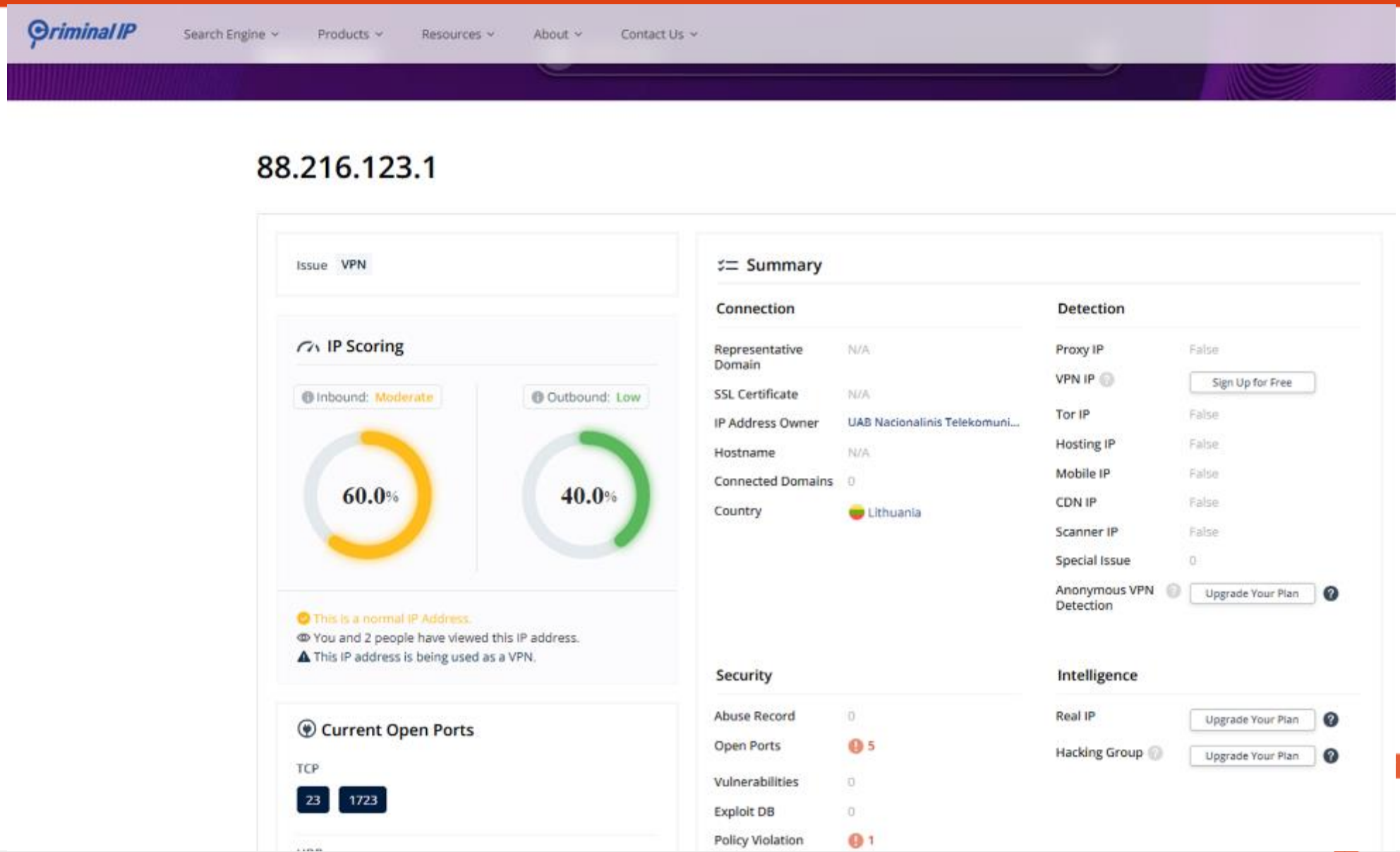
any / Baden-Württemberg / Neckar-Odenwald District

Toyota Yaris Cross

D MOS CW 50

Walldürn

Criminal.IP


Criminal IP
Search Engine
Products
Resources
About
Contact Us
88.216.123.1
Issue VPN
IP Scoring
Inbound: Moderate
60.0%
Outbound: Low
40.0%
This is a normal IP Address.
You and 2 people have viewed this IP address.
This IP address is being used as a VPN.
Current Open Ports
TCP
23
1723
Summary
Connection
Representative Domain N/A
SSL Certificate N/A
IP Address Owner UAB Nacionalinis Telekomuni...
Hostname N/A
Connected Domains 0
Country Lithuania
Detection
Proxy IP False
VPN IP Sign Up for Free
Tor IP False
Hosting IP False
Mobile IP False
CDN IP False
Scanner IP False
Special Issue 0
Anonymous VPN Detection Upgrade Your Plan
Security
Abuse Record 0
Open Ports 5
Vulnerabilities 0
Exploit DB 0
Policy Violation 1
Intelligence
Real IP Upgrade Your Plan
Hacking Group Upgrade Your Plan

NRD Cyber Security

Criminal.IP

Examples for

Science & Technology

Wolfram|Alpha has extensive knowledge related to science and technology. Using the computational power behind Wolfram|
physics, chemistry, engineering, computational sciences and many other domains.

Physics

Perform computations using formulas from physics, the branch of science studying properties of matter and energy.

Compute mechanical work:

work F=30N, d=100m =

Compute photon energy given wavelength:

photon energy 435nm =

More examples

Chemistry

Perform computations using formulas from chemistry, the branch of science studying the nature and interactions of substances.

Get information about a chemical element:

carbon =

Balance a chemical equation:

Al + O2 -> Al2O3 =

More examples

Units & Measures

Convert between units, examine information on different measurement devices or explore standard sizes for a variety of objects.

Get unit conversions for a quantity:

120 meters =

Discover what different devices measure:

what does a ruler measure =

Engineering

Perform computations using formulas from engineering, the branch of science studying the technology of designing structures or systems via scientific methods.

Compute magnetic flux density for an object:

1m 1A Helmholtz coil =

Compute the maximum force of a spring:

RELATED EXAM

- Mathematic

Computatio

Compute properti
computational sci
studying compute

Compute properti
automaton:

rule 110

Compute properti

Turing machine 25

More examples

Materials

annual deaths from auto accidents in the Lithuania

NATURAL LANGUAGE | MATH INPUT | EXTENDED KEYBOARD | EXAMPLES | UPLOAD | RANDOM

Input interpretation

Lithuania | people killed in road accidents

Result

Enlarge | Data | Customize | Plain Text

176 deaths per year (2020 estimate)

Unit conversion

More digits | Exact form | Step-by-step solution

0.4822 deaths per day

Corresponding quantity

Frequency ν of deaths:

5.6×10^{-6} Hz (hertz)

Average interval T between deaths:

179 182 seconds

2986 minutes

50 hours

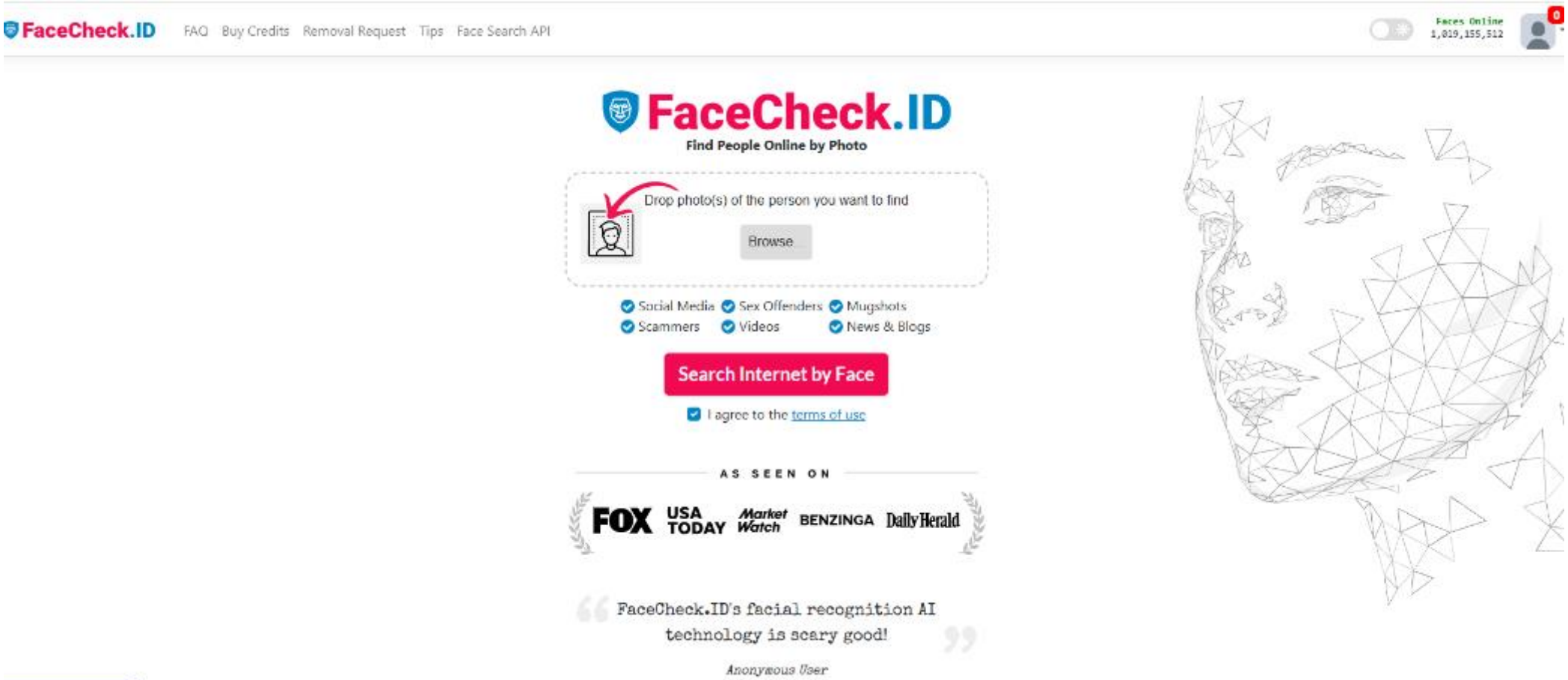
2.1 days

History

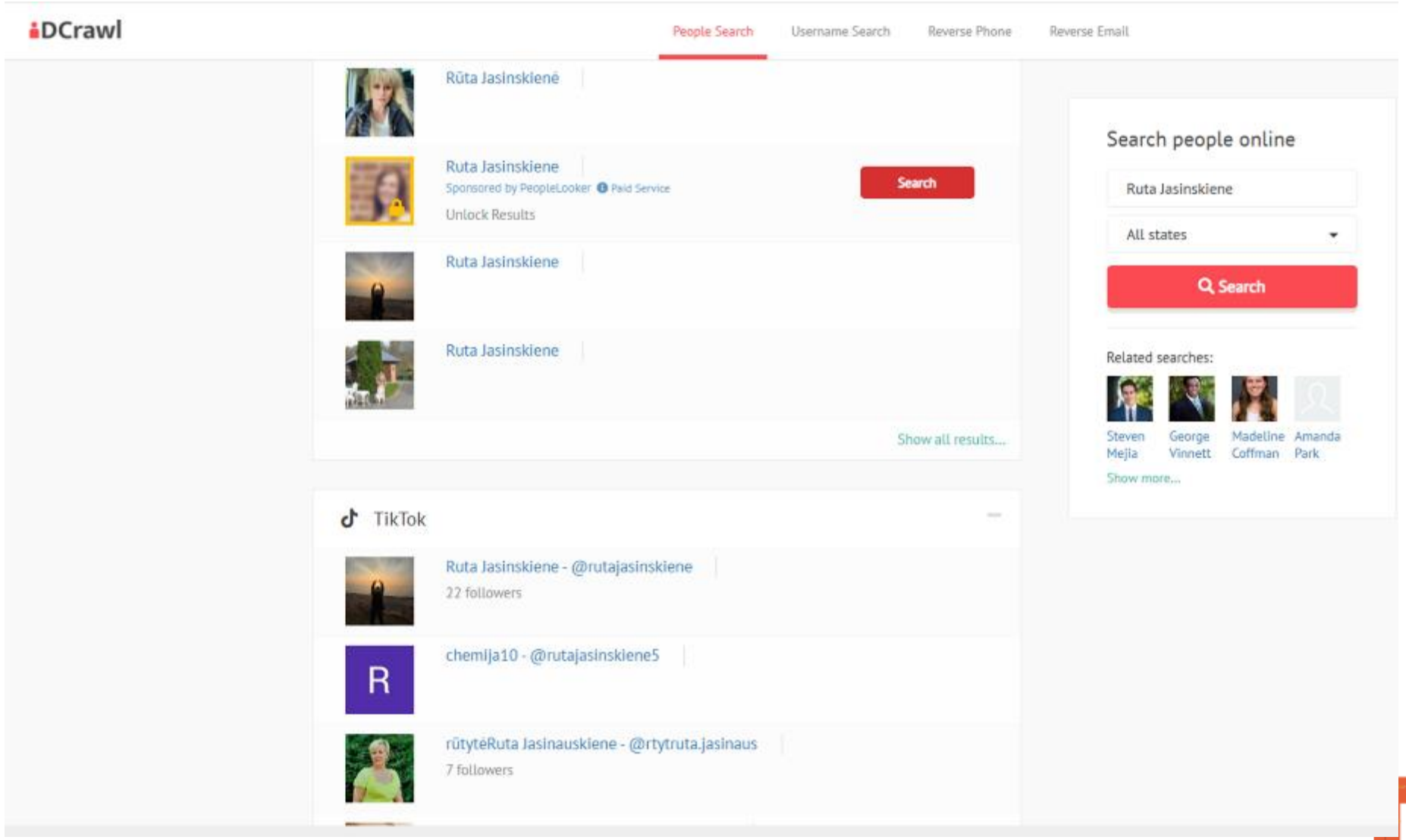
(from 2000 to 2020)

(in deaths per year)

People search

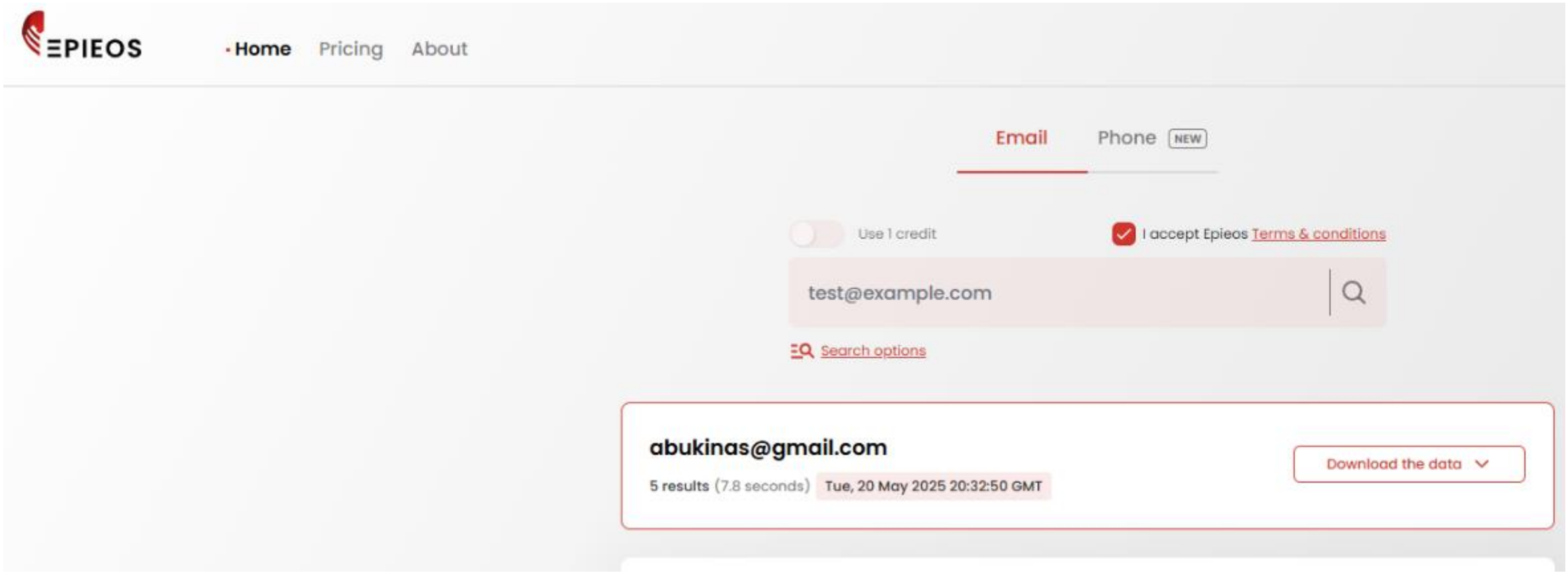


D.Crowl


DCrawl
People Search
Username Search
Reverse Phone
Reverse Email
Rūta Jasinskienė
Ruta Jasinskiene
Sponsored by PeopleLooker
Paid Service
Unlock Results
Search
Ruta Jasinskiene
Ruta Jasinskiene
Show all results...
TikTok
Ruta Jasinskiene - @rutajasinskiene
22 followers
chemija10 - @rutajasinskiene5
rūtytėRuta Jasinauskiene - @rtytruta.jasinaus
7 followers
Search people online
Ruta Jasinskiene
All states
Search
Related searches:
Steven Mejia
George Vinnett
Madeline Coffman
Amanda Park
Show more...

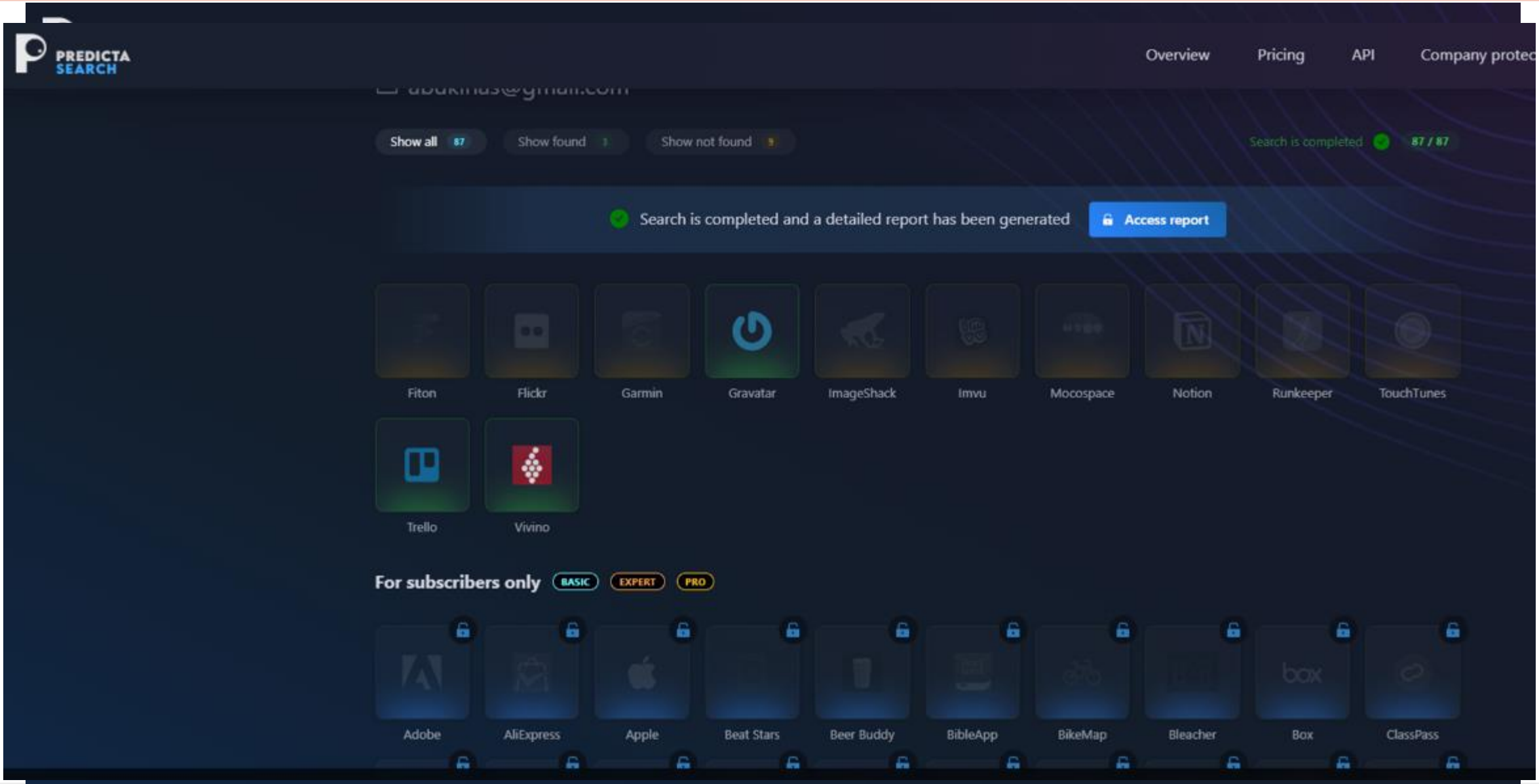
NRD Cyber Security

Epieos - Search for social accounts with e-mail and phone

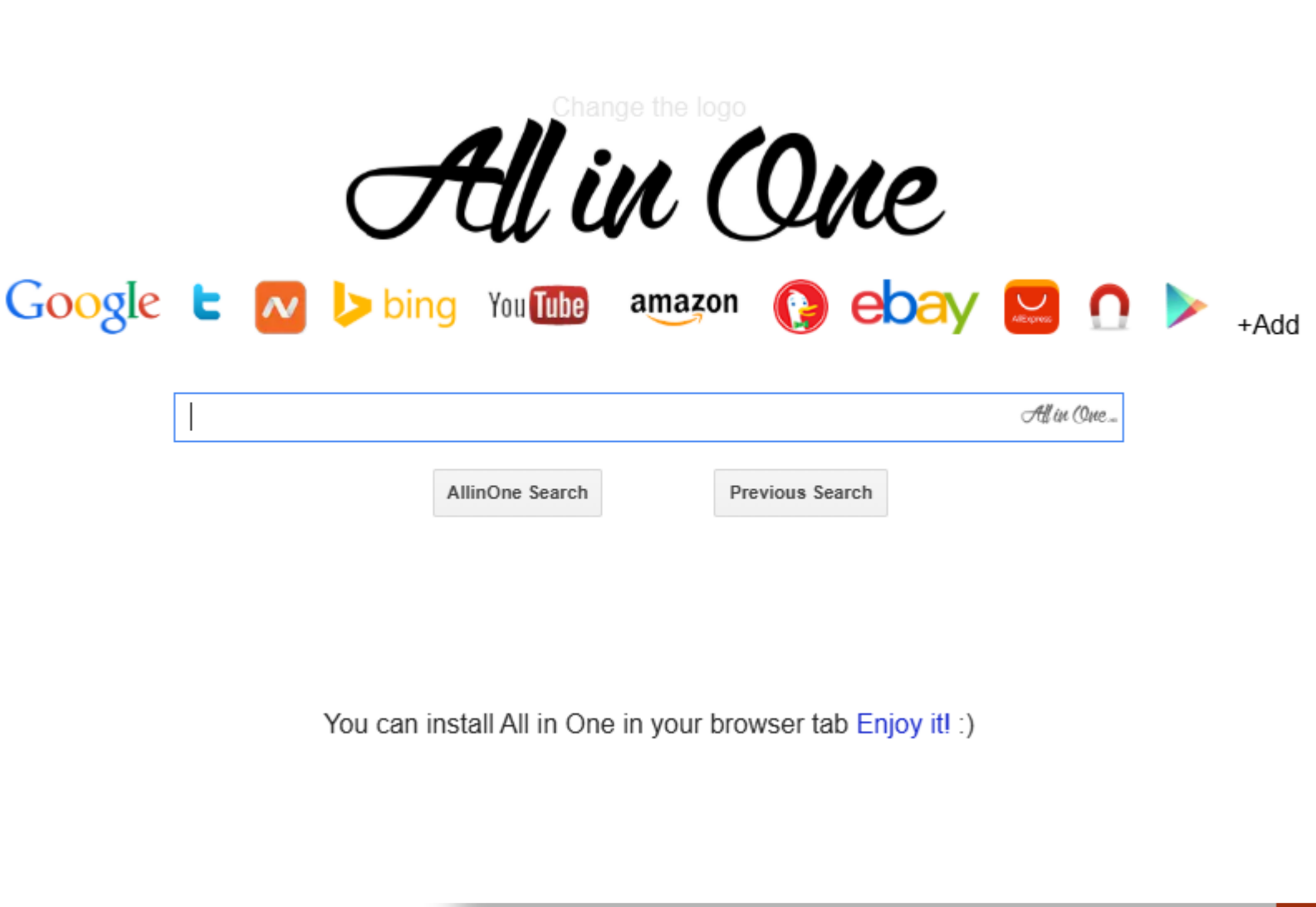


NRD Cyber Security

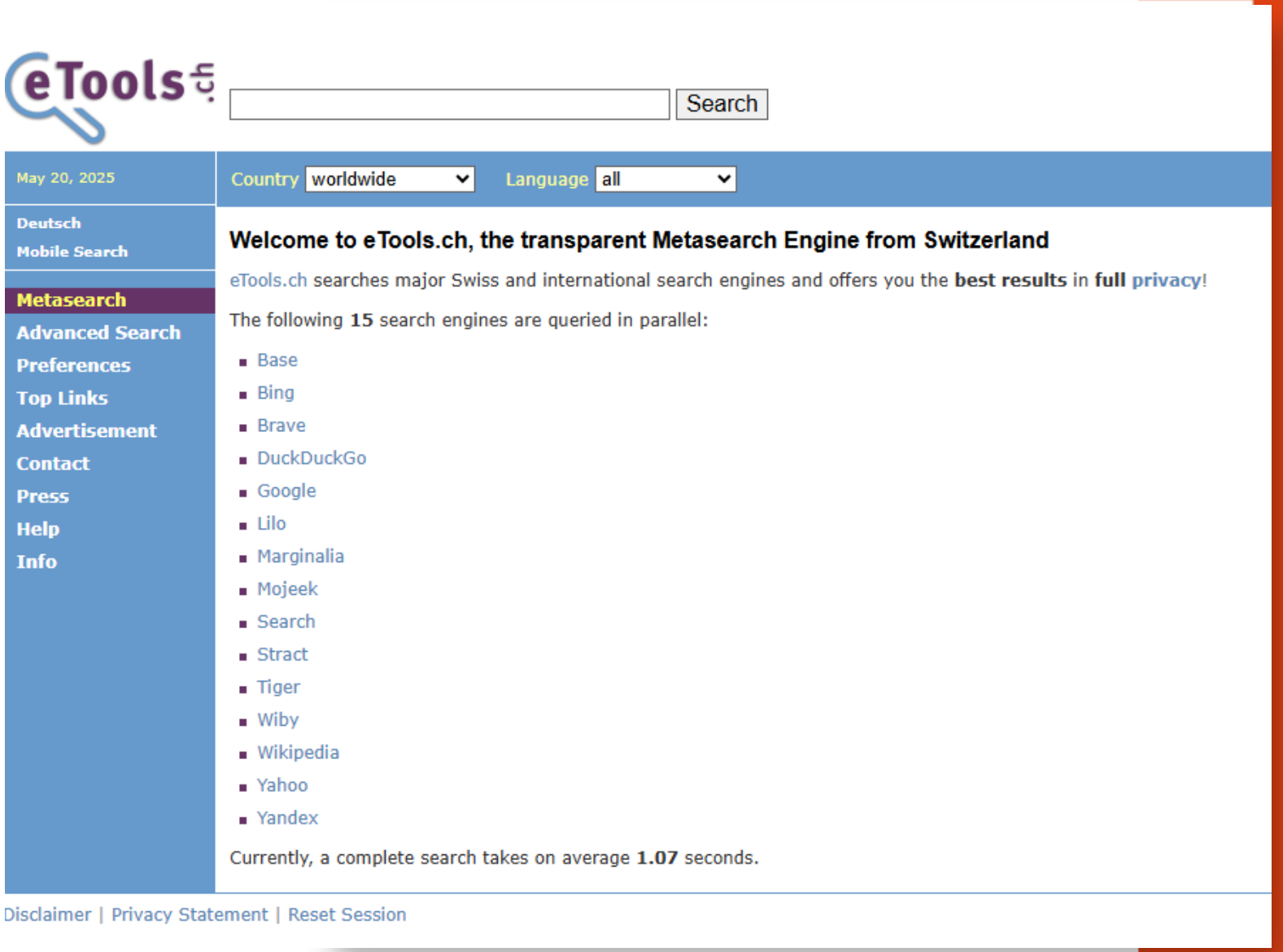
Predicta Search



all-io.net


Change the logo
All in One
Google
bing
YouTube
amazon
ebay
+Add
All in One...
AllinOne Search
Previous Search
You can install All in One in your browser tab Enjoy it! :)

Etools.ch


eTools.ch
Search
May 20, 2025
Country worldwide
Language all
Deutsch
Mobile Search
Metasearch
Advanced Search
Preferences
Top Links
Advertisement
Contact
Press
Help
Info
Welcome to eTools.ch, the transparent Metasearch Engine from Switzerland
eTools.ch searches major Swiss and international search engines and offers you the best results in full privacy!
The following 15 search engines are queried in parallel:
Base
Bing
Brave
DuckDuckGo
Google
Lilo
Marginalia
Mojeek
Search
Stract
Tiger
Wiby
Wikipedia
Yahoo
Yandex
Currently, a complete search takes on average 1.07 seconds.
Disclaimer | Privacy Statement | Reset Session

Ahmia.fi

“Ahmia's mission is to create the premier sea
anonymity network. In doing so, we hope to s
about the Tor network and the Tor project.

Contributors to Ahmia believe that the Tor ne
platform for anonymity and privacy worldwide
call the "deep web" or "dark net", Ahmia mak
people, not just Tor network early adopters.”

Drugs – onionmarket – credit cards & drugs & paypal

No description provided

jdntpptrtu5iounucxs5ehlqm3k4rgveeppxsgaqnta76dnsipgxo2ad.onion – 2 weeks, 1 day ago –

Drugs – 555market – credit cards & drugs & paypal

No description provided

555eearzli4bilpjmwmy5n6qoh3jdtrqzt2345cwjj2x3e4cmvvneoad.onion – 2 weeks, 1 day ago –

Marijuana Drugs

Drugs Store - buy Ecstasy, Cocaine, LSD, Meth.

4t4ki52bkw46s6zfxnnlcnzrqjv4zdp5kwmqeqtouwbixuxp5kfcxyad.onion – 1 month, 1 week ago –

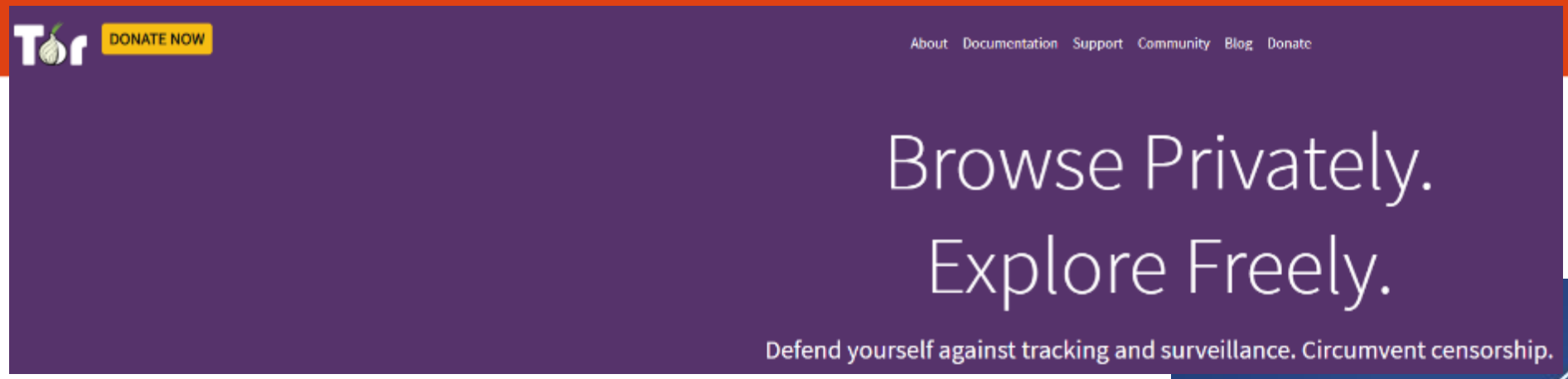
Hashish Drugs

Drugs Store - buy Ecstasy, Cocaine, LSD, Meth.

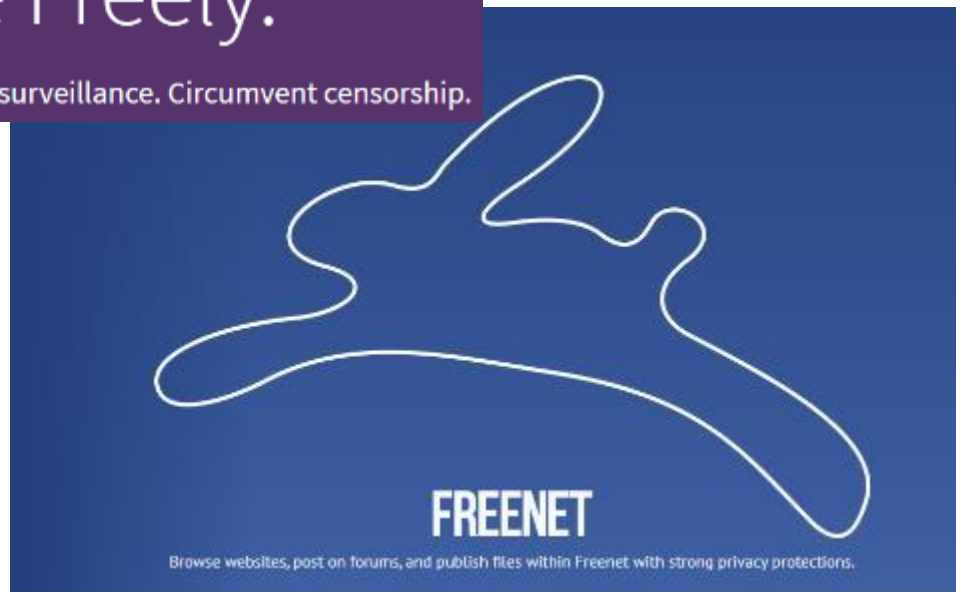
5xtktk7q63l533qiiupxc5nvnivzzn4mvonwaajl6vdp5p7bjatkcbad.onion – 1 month, 1 week ago –

Juha Nurmi, Ahmia Project Leader

Juha Nurmi (juha.nurmi@ahmia.fi) is the founder and project leader of the Ahmia search engine project. He is a security researcher, and has been involved in numerous projects funded by both the commercial and government spheres. Juha is also a noted lecturer and public speaker.


Tor
DONATE NOW
About Documentation Support Community Blog Donate
Browse Privately.
Explore Freely.
Defend yourself against tracking and surveillance. Circumvent censorship.


ZeroNet
Open, free and uncensorable websites,
using Bitcoin cryptography and BitTorrent network


FREENET
Browse websites, post on forums, and publish files within Freenet with strong privacy protections.


I2P
Download About Donate


OpenBazaar
Features Applications API Developer


A FREE ONLINE MARKETPLACE. NO PLATFORM FEES. NO RESTRICTIONS. EARN CRYPTOCURRENCY
Buy and Sell Freely

Ordinary browsers vs Tor browser

Ransomware - Wikipedia

Ransomware is a type of malware from cryptovirology that threatens to publi
personal data or perpetually block access to it unless a ransom ...
Jigsaw (ransomware) · Ryuk (ransomware) · FBI MoneyPak Ransomware

https://www.malwarebytes.com › Cybersecurity

How to Protect Against Ransomware - Malwarebytes

Ransom malware, or **ransomware**, is a type of malware that prevents users f
system or personal files and demands ransom payment in order to ...

https://www.trellix.com › en-us › security-awareness

What Is Ransomware? | Trellix

Ransomware is malware that employs encryption to hold a victim's informatic
user or organization's critical data is encrypted so that they ...

https://www.trendmicro.com › vinfo › security › ranso...

Ransomware - Definition - Trend Micro

Ransomware is a type of malware that prevents or limits users from accessir
either by locking the system's screen or by locking the users' files ...
Feb 18, 2021 · Uploaded by Trend Micro
The History and Evolution of... · Early Years · The Evolution to Crypto...

RANION - Better and Cheapest FUD Ransomware + Darknet C2 + NO Fees
http://ni3kiymt4jc32baea356vhwurba44jabfklitpoqbrtgrhr5skyrixyd.onion/
RANION - Better and Cheapest FUD Ransomware + Darknet C2 + NO Fees RANIN - Better & Cheapest FUD Ransomware + Darknet C2 + NO Fees BUY - FAQ - REVIEWS - SCREENS...
Online | | Report abuse | Tor2Web

EP918 - Ransomware
http://dg5fyig37abmivryrxlordrczn6d6r5wzcfe2msuo5mbbu2exnu46fid.onion/
EP918 - Ransomware EP918 Specialist in cybersecurity, we have designed a very powerful FUD ransomware, capable of automatically propagating to a whole network. ...
Online | | Report abuse | Tor2Web

Ransomware Group Sites
http://ransomwr3tsydeii4q43vazm7wofla5ujdajquitomtd47cxjtfgwyyd.onion/
Ransomware Group Sites Ransomware Group Sites Support of TOR onion version 2 URLs (aka "short onion domains") will be disabled on TOR nodes on July 15th, 2021 a...
Online | | Report abuse | Tor2Web

Ransomware Group Sites
http://inhx4x4y66guy6ljnhq3ijbbgroha5sejcyo2uejmzv6vd3ydwzc6fid.onion/
Ransomware Group Sites Ransomware wiki last update:2021/06/27 Join Our Telegram Group Name Link status Astro Team Open Down Avaddon Open Down Babuk/Payload.bin ...
Online | | Report abuse | Tor2Web

AI

- How reliable is it?

Example

Republic of Armenia
Government Decree

On Amendments to the
(Approved on June 9, 20

1. In Appendix 1 of the
titled "Critical Inform
Subparagraph 16 of
   - **16. "Disaster r**
   - **17. "Physical s**
ensuring th
   - **18. "Business c**
infrastructu
   - **19. "Cyber inci**
prevention,
2. In Paragraph 9 of Ap
3. In Paragraph 10 of A
infrastructures must
including technical a

Copilot

Sure! Here are the main points from the page:

1. **Amendments to the Law on the Rights of Persons with Disabilities:**
   - **Article 1**: Changes the wording in Article 3, Section 1, Clause 13 to specify the functions within the scope of the law.
   - **Article 2**: Adds new clauses (16-19) to Article 3, Section 1, defining terms related to organizations, state certificates, compensation amounts, and minimum requirements for providing support measures.
   - **Article 3**: Adds sub-clauses to Article 9, Section 1, Clause 2, detailing the provision of care and social-rehabilitation services through state certificates and compensation amounts.
   - **Article 4**: Adds Clause 5.1 to Article 10, Section 1, outlining the approval process for contracts with organizations providing support

under Chapter 3, Paragraph 13,
ng points shall be added to
section.
ange of measures aimed at
perational continuity of critical
cesses aimed at identification,
ing critical infrastructures.
all be added.
that entities managing critical
anagement capabilities,

AI with well developed imagination

there is no such section

Thanks again — you're absolutely right to double-check. Let's go step by step to clarify the source of that number properly.

Let me recheck the **exact location** within the PDF you uploaded titled:

> **"EU4Digital-Trust-and-Security-R2-3-1-R2-3-4-Cross-border-eServices-interoperability-Armenia.pdf"**

Upon reviewing the document **carefully**, here's what I actually found:

- The statement:

  > "Over 80 services are currently available through the e-Government platform, and more than 100 are offered via the e-Request platform."
  > is indeed found on **page 2** of the PDF (based on the PDF's actual page numbering, not any internal document numbering).

Why OSINT is Valuable to Hackers?

- provides vast, unrestricted access to data without breaching legal boundaries
- enables to collect detailed personal, professional, and technical information on targets
- facilitates reconnaissance, vulnerability identification, and attack planning

NRD Cyber Security

Common Ways Hackers Use OSINT

- Phishing & Social Engineering: Scraping social media and company sites to craft convincing, personalized phishing emails (e.g., CEO impersonation)
- Credential Harvesting: Monitoring leaked credentials on the dark web and using them for credential stuffing
- Infrastructure Reconnaissance: Using tools like Shodan to find exposed devices and unpatched systems
- Identity Theft: Collecting personal details for harassment or impersonation
- Supply Chain Attacks: Analyzing third-party vendors' security weaknesses to breach larger organizations

NRD Cyber Security

Cisco Talos Intelligence

IP and Domain Reputation Center for real-time threat detection

TOP EMAIL SENDERS BY COUNTRY IN THE LAST DAY

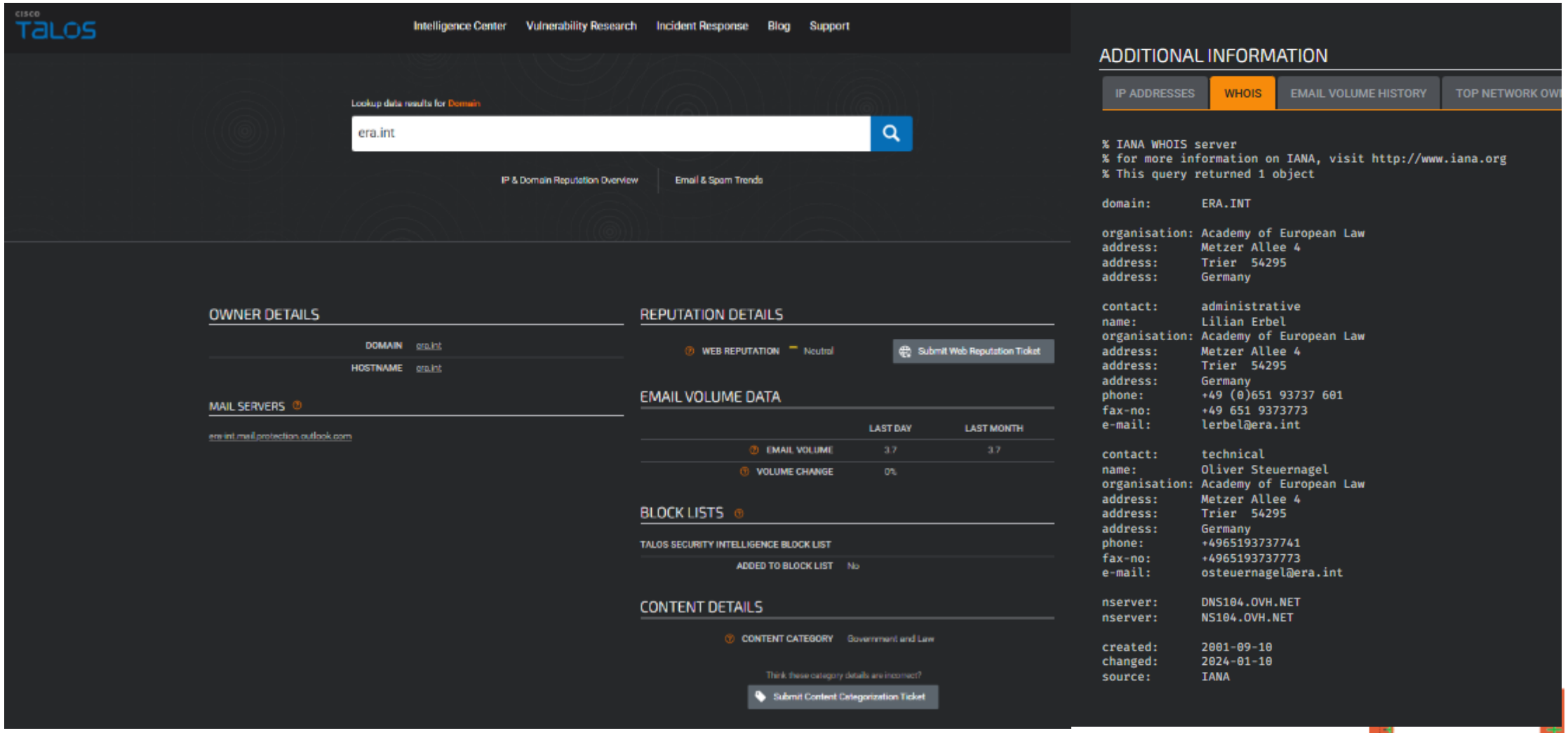
	LAST DAY VOLUME	VOLUME CHANGE
United States	9.70	-0.41% ↓
Germany	8.50	+0.76% ↑
Netherlands	8.40	+1.44% ↑
India	8.40	-1.61% ↓
Czechia	8.30	+3.28% ↑
France	8.30	+0.12% ↑
Belgium	8.30	-0.66% ↓
Canada	8.30	+0.26% ↑
Ireland	8.20	+0.33% ↑
Israel	8.20	+7.57% ↑

TOP SPAM SENDERS BY COUNTRY IN THE LAST DAY

	LAST DAY VOLUME	VOLUME CHANGE
United States	7.90	+1.2% ↑
China	7.80	+2.84% ↑
Netherlands	7.20	+10.41% ↑
Germany	7.10	+4.53% ↑
Russia	7.00	+8.96% ↑
Brazil	7.00	+8.73% ↑
France	7.00	+4.14% ↑
Japan	6.90	+3.51% ↑
Hong Kong	6.90	+1.19% ↑
India	6.60	+3.17% ↑

NRD Cyber Security

Cisco Talos Intelligence
Check of era.int

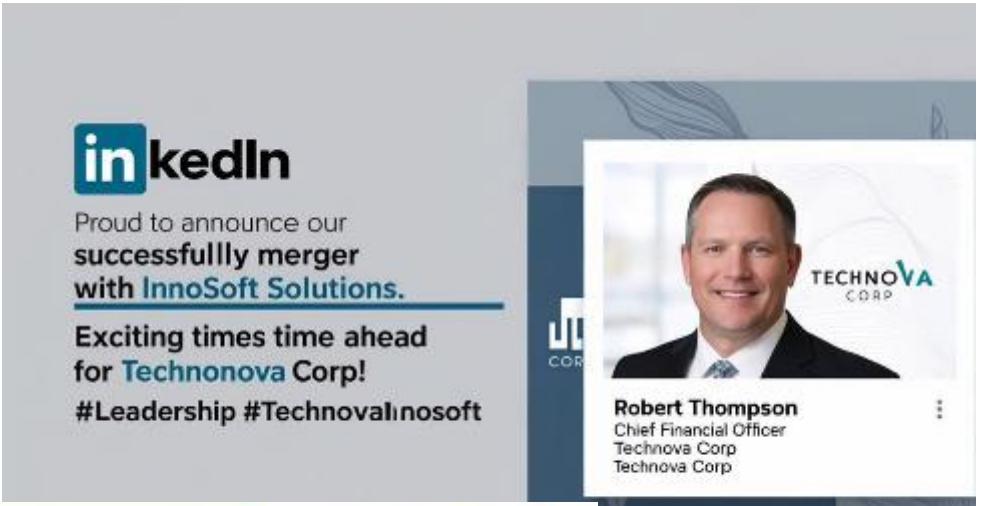


NRD Cyber Security

Case Scenario

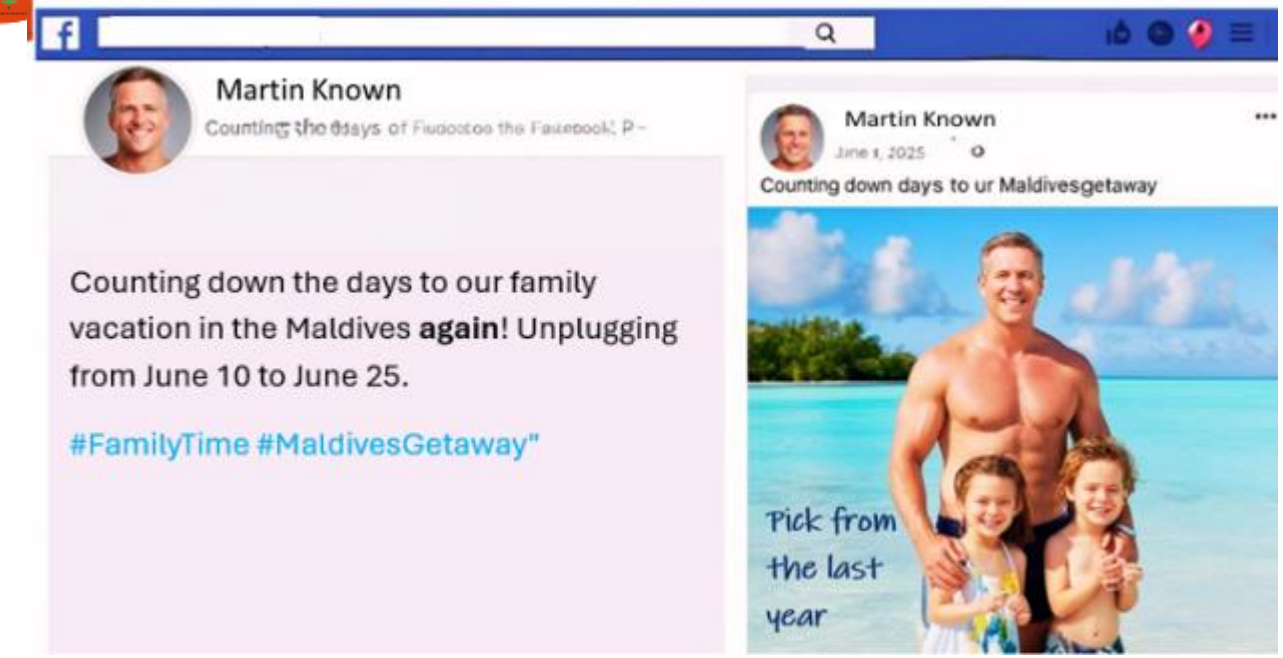
Target : mid-sized tech company Technova Corp and its CFO

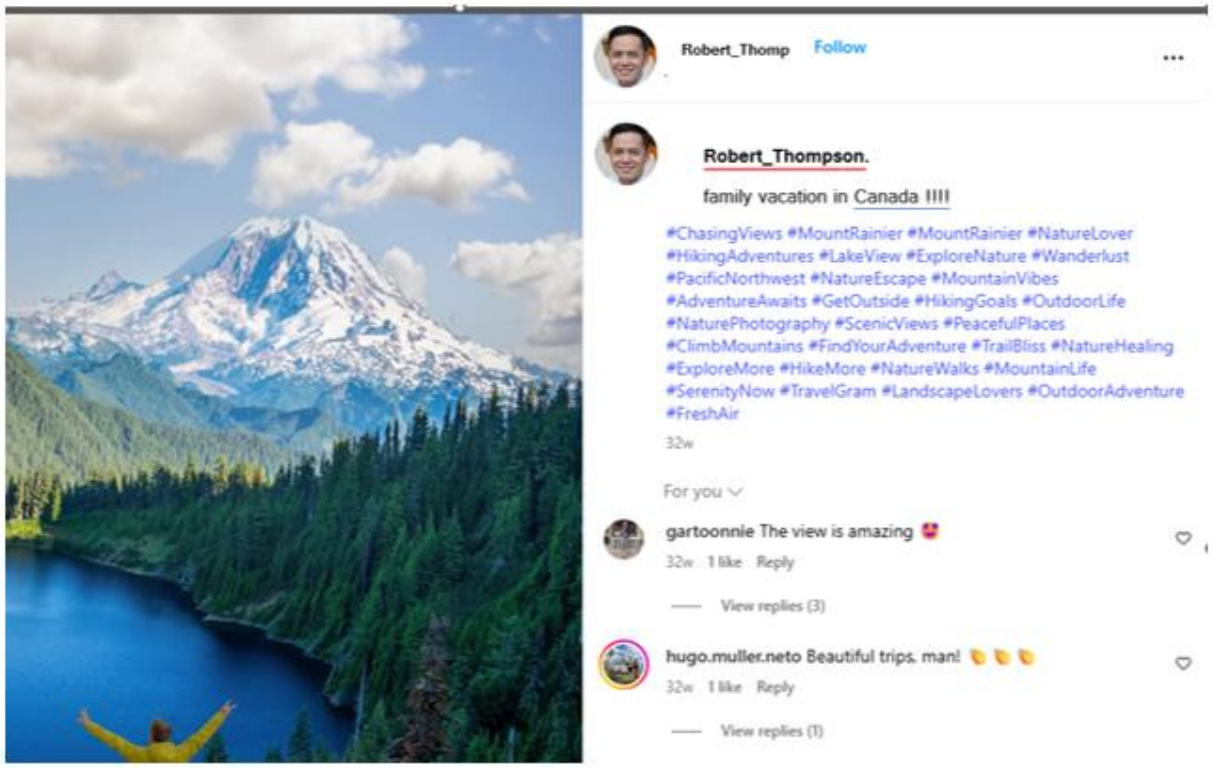
Attacker's Preparation



NRD Cyber Security

Right moment





Right moment

By tracking online/offline status of people on Facebook, it is possible to get an accurate image of their sleep pattern.

Night after	Period	Duration
Saturday, Jan 30	06:45-11:25	4.7 hours
Sunday, Jan 31	01:02-08:40	7.6 hours
Monday, Feb 01	00:02-08:11	8.1 hours
Tuesday, Feb 02	23:20-07:26	8.1 hours
Wednesday, Feb 03	00:20-08:30	8.2 hours
Thursday, Feb 04	01:10-07:37	6.5 hours
Sunday, Feb 07	22:25-06:32	8.1 hours
Monday, Feb 08	22:08-06:18	8.2 hours
Tuesday, Feb 09	23:52-06:17	6.4 hours
Wednesday, Feb 10	23:47-06:31	6.7 hours

Fb-sleep-stats

https://github.com/sorenlouv/fb-sleep-stats

NRD Cyber Security

Phishing Email

From: martin.known@technovacorpp.com
Subject:Urgent Wire Transfer Request -Singapore Deal

Hi Robert, greetings from Maldives, you must come here! But business first☺ just before leaving mainland and sailing away I have had a call from Singapore. We need to finalize the acquisition deal ASAP. Please wire $250,000 to our legal rep's account below: Bank: Asia Finance Corp Account Name: Legal Holdings Ltd. Account Number: 4589 00123344. Make this a priority
BTW how it was in Canada? Did Lilit like it?

Martin
Most likely I'll be unreachable for a couple of days☹

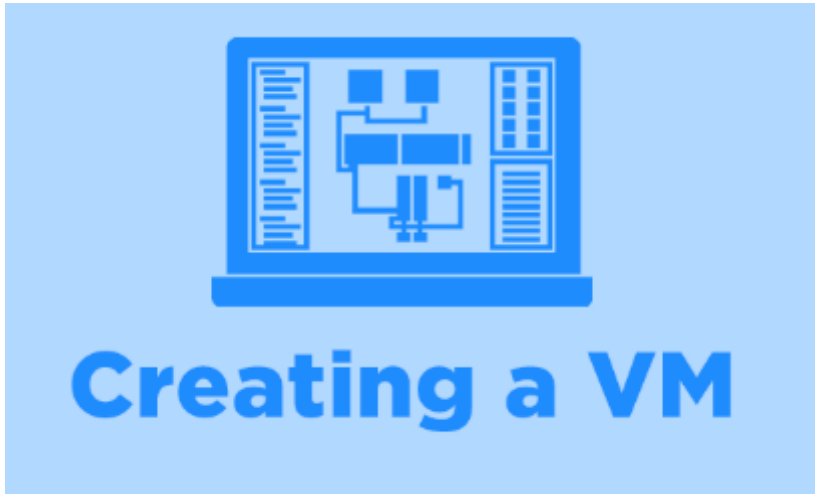
How it works

- https://www.linkedin.com/feed/update/urn:li:activity:7160471264438931457/

- https://www.youtube.com/watch?v=Rn4Rupla11M

Do not leave a footprint behind….

- https://randomuser.me/
- https://www.name-generator.org.uk/
- https://www.fakenamegenerator.com/
- https://this-person-does-not-exist.com/en



Thank you!!!!

Rūta JAŠINSKIENĖ

rj@nrdcs.lt

www.linkedin.com/in/ruta-jasinskiene

PRESENTING EVIDENCE IN COURT:

E-FILES, VIDEOCONFERENCES AND REMOTE TRIALS

Sabina Klaneček, May, 2025

sabina.klanecek@dt-rs.si

Co-funded by the European Union


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

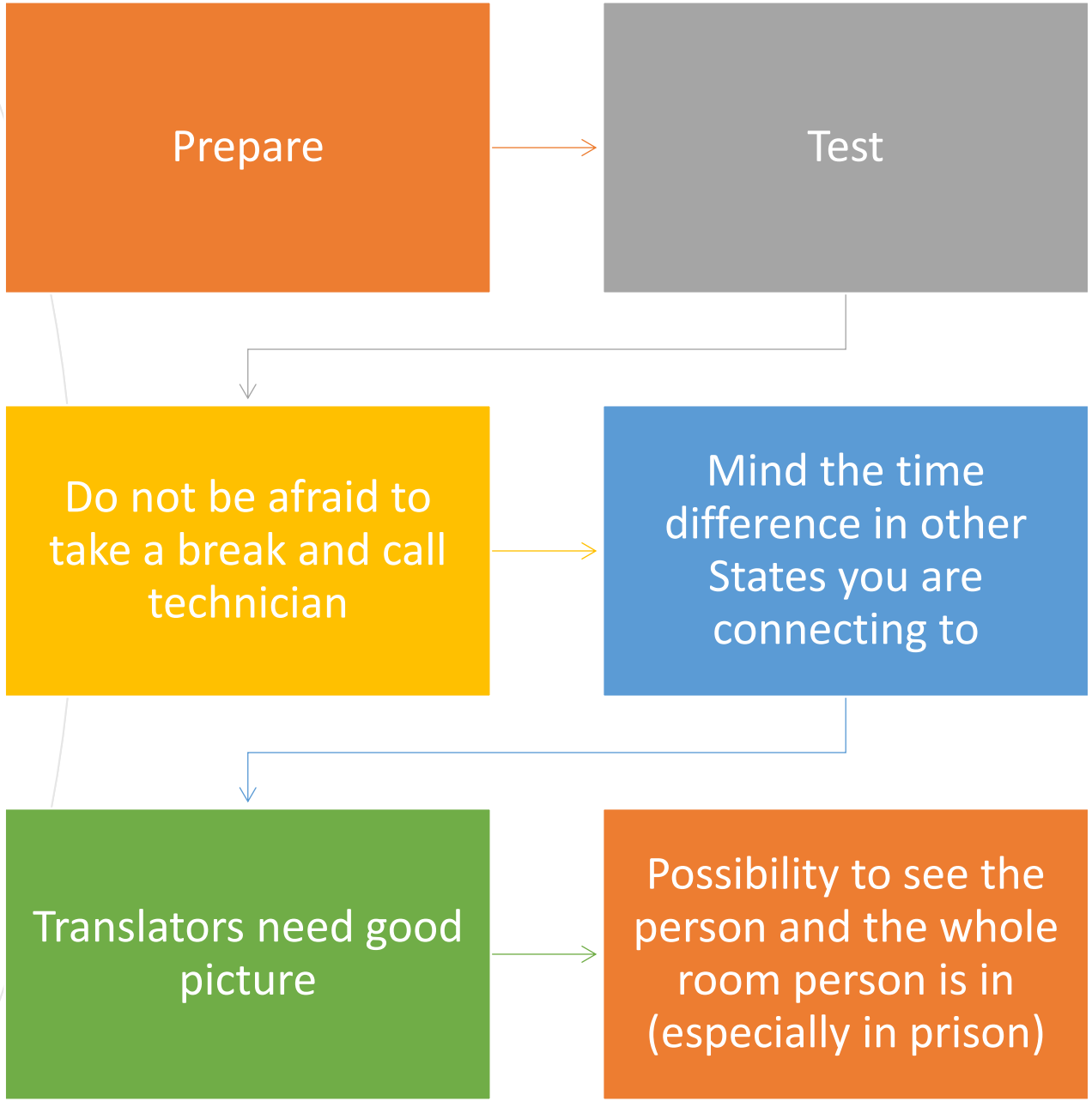
Judge has own camera

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)

E-File

- Electronic court file = digital form of the traditional court file.
- It contains pleadings, exhibits, minutes, decisions, judgments, etc.
- Allows secure and fast access to documents in a case.
- Accessible to users (judges, lawyers, parties) via an information system.

VC and e-File

- Videoconferencing orders are based on access to the e-file.
- The judge conducts the hearing via e-file - without physical documents.
- The material is shown live to the participants (content sharing).
- Minutes and recordings are kept in the e-file.

- Please describe how the integration of the SC and e-file allows the remote handling of court proceedings without loss of efficiency or transparency.
- Key documents are always accessible and part of the proceedings are automatically archived in the e-file.

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 !

FACULTY OF LAW AND ADMINISTRATION

Big Data and the quality of datasets used for the development of AI-based tools for law enforcement in criminal justice systems

ERA, Kraków, 27 May, 2025

dr Martyna Kusak

Co-funded by the European Union

Focusing on Data Quality under Article 10 AI Act

- Art. 10 AI Act (Regulation (EU) 2024/1689) of 13 June 2024: Data and data governance

1. *High-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that **meet the quality criteria** referred to in paragraphs 2 to 5 whenever such data sets are used.*

   (…)

AI Act: A risk-based approach

Unacceptable risk (art. 5)	Pose clear threat to the safety, livelihoods and rights of people (e.g., social scoring, manipulation of human behaviour, exploitation of vulnerabilities)	Prohibited
High risk (Art. 6 et seq.)	Pose serious risks to health, safety or fundamental rights	Subject to strict legal requirements
Limited risk	Risks associated with a need for transparency around the use of AI	Subject to transparency obligations
Minimal risk	Minimal or no risk	Permitted with no specific requirements

AI Act: Prohibited uses of AI

Prohibited uses of AI (Art. 5):

- biometrics (real-time remote biometric systems (RBI) in public spaces, biometric categorization of natural persons based on biometrics to deduce certain attributes),
- a partial ban of individual predictive policing;
- untargeted scraping of facial images from the internet or CCTV footage

Exception: RBI in public spaces (Art. 5.2)

AI Act: High-risks systems in law enforcement

Point 6 of Annex III of the AIA includes high-risk systems (Art. 6) used in law enforcement. These include AI systems used:

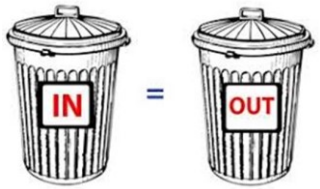
- to assess whether a person is at risk of becoming a victim of a criminal offence,
- as lie detectors or similar tools to assess truthfulness during questioning,
- to assess the reliability of evidence in a criminal investigation or prosecution,
- to assess the likelihood that a person will commit or reoffend in a criminal offence,
- to profile individuals during the detection, investigation, or prosecution of criminal offences.

AI Act: Specific requirements for high-risk AI

- Risk management system (Art. 9)
- Data and data governance (Art. 10)
- Technical documentation (Art. 11) and record-keeping (Art.12)
- Transparency (Art. 13)
- Human oversight (Art. 14)
- Accuracy, robustness and cybersecurity (Art. 15)
- Obligations of providers and deployers of high-risk AI systems and other parties (Section 3)
- Notifying authorities and notified bodies (Section 4)
- (…)

AI Act: Specific requirements for high-risk AI

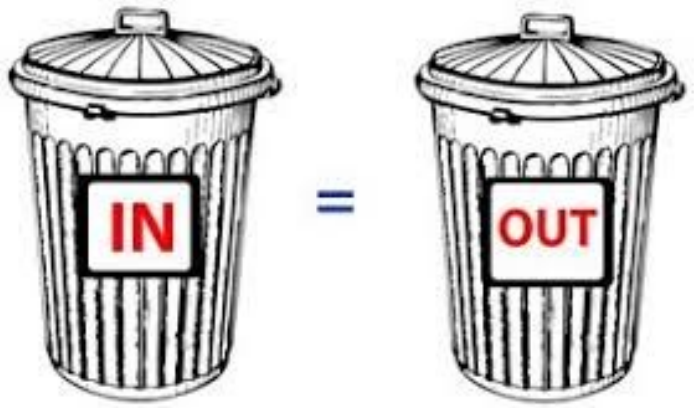
- Risk management system (Art. 9)
- Data and data governance (Art. 10)



- Technical documentation (Art. 11) and record-keeping (Art.12)
- Transparency (Art. 13)
- Human oversight (Art. 14)
- Accuracy, robustness and cybersecurity (Art. 15)
- Obligations of providers and deployers of high-risk AI systems and other parties (Section 3)
- Notifying authorities and notified bodies (Section 4)
- (…)

AI Act: Data and data governance

Garbage in, garbage out



AI Act, Rec. 67: High-quality data and access to high-quality data plays a vital role in providing structure and in ensuring the performance of many AI systems, especially when techniques involving the training of models are used (…).

What Data Governance Under Art. 10 Requires

High-risk AI systems which make use of techniques involving the training of AI models with data (such as supervised learning, unsupervised learning, self-supervised learning, reinforcement learning) shall be developed on the basis of training, validation and testing data sets that meet the quality criteria, which involve:

1. Data governance and management practices appropriate for the intended purpose of the high-risk AI system (design choices, data collection practices, labeling etc., art. 10.2)
2. **Data quality metrics (art. 10.3).**

Art. 10 AIA:Data Sets Quality Requirements

- **Relevance** – fitness for the purpose, providing information that is useful for the development of the AI system; whether or not data are relevant relies entirely on context
- **Sufficient representativeness** – data sets should adequately reflect the diversity in the respective category or scenarios it models
- **Accuracy**, to the best extent posisble – there should be no errors in the data
- **Completeness**, in view of the intended purpose – there should be no missing data
- **Consistency** – data should not conflict with other values across data set; the requirement for ‘appropriate statistical properties’ and ‘sufficiently representative’ indirectly implies a need for consistency across data sets
- **Contextual data sets quality requirements**: data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting within which the high-risk AI system is intended to be used

Metrics not mentioned in the AI Act: Validity, reliability, timeliness, uniqueness (no duplicates)…

Art. 10 AIA:Data Sets Quality Requirements

- **Relevance** – fitness for the purpose, providing information that is useful for the development of the AI system; whether or not data are relevant relies entirely on context

Hypothetical example:

For a system predicting recidivism, information like age and prior convictions might be relevant—but astrological sign or unrelated health data would not be.

Art. 10 AIA:Data Sets Quality Requirements

- **Sufficient representativeness,** – data sets should adequately reflect the diversity in the respective category or scenarios it models; **contextual –** geographical context

Hypothetical example:

A model developed to detect fraud is trained on historical financial crime data from selected urban areas.

When applied nationally, the system fails to detect fraud patterns in rural or minority communities, resulting in under-policing in some regions and over-policing in others.

Art. 10 AIA:Data Sets Quality Requirements

- **Accuracy**, to the best extent posisble – there should be no errors in the data

Hypothetical example:

A high-risk AI system is used to assess the risk of a natural person becoming the victim of cyberviolence by monitoring the Internet.

During training, the model is exposed to large volumes of text data, some of which includes sarcastic or ironic posts that are mislabelled as real threats or abuse due to flawed natural language processing (NLP).

These labelling errors in the training data introduce inaccuracies; in result, when deployed, the model over-flagged users.

Art. 10 AIA:Data Sets Quality Requirements

- **Completeness**, in view of the intended purpose – there should be no missing data

Hypothetical Example: An AI system designed to evaluate the reliability of witness statements is trained exclusively on police transcripts and expert opinions, but does not include data from court records.

As a result, the system develops assessments based on an incomplete understanding of events, which can lead to incorrect conclusions.

Data protection rules enhancing data quality

Data protection: directive 2016/680 (LED)

1) Principles: purpose-limitation, accuracy, up to date, completeness, timeliness, and review of the data

1) Data quality (art. 7.2): personal data that are inaccurate, incomplete, or no longer up to date are not transmitted or made available

Art. 10 AI Act does not provide a lawful basis for processing under the GDPR or Law Enforcement Directive. Any data processing for quality checks must separately comply with existing EU data protection laws.

Summary

1. Only high-risk AI systems that train on data are subject to data sets quality requirements.

2. The requirements are context-dependent, not absolute, and subject to interpretation.

3. What will be the standards?

Q&A

Thank you!

m.kusak@amu.edu.pl

PREDICTIVE POLICING & BIG DATA

KIRAN SIVAKUMAR

27th May 2025

Co-funded by the European Union

OVERVIEW

- WHAT's SO PREDICTIVE ABOUT IT
- WHY PREDICTIVE POLICING MATTERS NOW
- INDIAN PERSPECTIVES – The Kumbh Mela Example
- Case studies (UP Police, Delhi)
- The challenge of bias

WHAT IS PREDICTIVE POLICING

- Predictive policing is the application of AI and statistical models to law enforcement data to anticipate where and when crimes are likely to occur, enabling proactive, data-driven law enforcement
- use data technologies to optimise the allocation of police resources to prevent crime
- Goal : Shift from Reactive to Proactive policing
- Key Data Inputs:
  - Historical crime records (time, location, type of offense)
  - Demographic and socioeconomic information
  - Environmental and situational factors (lighting, transit, businesses)
  - Real-time surveillance (CCTV, license plate readers)
  - Social media and public reports (sentiments)
  - Weather, holidays, and event data
  - Offender and victim profiles, probation/parole records
  - Social network analysis (associates, gang affiliations)
- Output:
  - Crime “heat maps,” risk scores, and resource deployment recommendations

- Big Data: The Engine of Predictive Policing
  - Integrates crime, social, environmental, and real-time data streams
  - Enables pattern recognition, hotspot mapping, and risk forecasting
- From Expert-Driven to Algorithm-Driven ("Algocracy")
  - Algorithms centralize and automate decision-making (Lorenz et al., 2021)
  - Reduces subjective bias, but can embed systemic biases
- Empirical Evidence:
  - Big data analytics improve crime prediction and resource allocation
  - Example: Berlin's KrimPro system—centralized, data-driven policing
  - India: AI-driven models in UP, Hyderabad, and Delhi harness big data for hotspot mapping, repeat offender tracking, and resource optimization.
  - "Predictive policing relies on computer algorithms to see patterns, predict the occurrence of future events based on large quantities of data, and aims to carefully target police presence to the necessary minimum to achieve desired results." (Carrie & James, 2017)

- Study: “AI’s pattern recognition and data processing capabilities allow it to identify crime trends, correlations, and anomalies that may be difficult for human analysts to detect. By constantly learning from new data, AI models continuously refine their predictions, ensuring that law enforcement strategies remain adaptive and effective.” (INDIAai, 2023)

- Risks and Challenges:
  - Potential for bias and lack of transparency in algorithmic decisions
  - Privacy concerns with large-scale surveillance and data integration
  - Need for regular audits and human oversight to ensure accountability

Traditional Policing

- Relies on:
  - Officer intuition & experience
  - Local knowledge
  - Manual analysis of crime reports
- Data Used:
  - Limited, often only recent or local incidents
- Approach:
  - Reactive—responds to crimes after they occur
  - Patrols based on routine or recent events
- Limitations:
  - Subject to human bias
  - Slow to recognize emerging patterns
  - Resource allocation often less targeted

Predictive Policing

- Predictive Policing
- Relies on:
  - Big data analytics & AI algorithms
  - Integration of diverse data sources (crime, social, environmental, real-time feeds)
- Data Used:
  - Historical crime data, demographics, CCTV, social media, weather, etc.
- Approach:
  - Proactive—forecasts where/when crime is likely
  - Generates “heat maps” and risk scores for targeted deployment
- Strengths:
  - Detects hidden patterns and trends
  - Optimizes resource allocation
  - Can reduce some forms of human bias
- Risks:
  - Potential for algorithmic bias and privacy concerns
  - Requires transparency and oversight

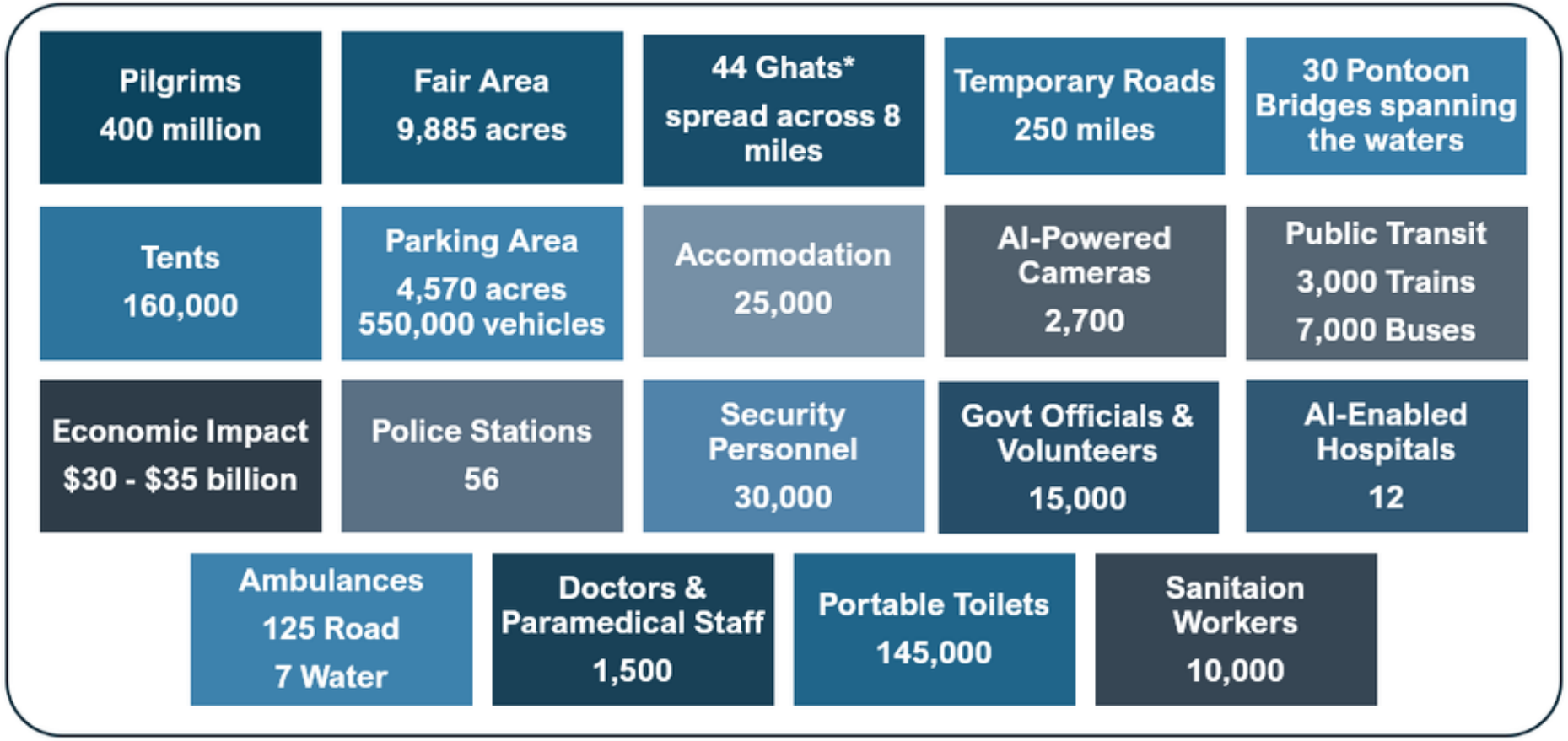
- Predictive policing manifests in two main types:
- a) area-based
  - identify connections between locations, occurrences, and historical crime statistics to forecast the likelihood of crimes occurring at specific times and places.
  - they can predict increased crime rates during certain weather conditions or at major sporting events.
- b) individual-based policing.
  - Individual-based predictive policing anticipates persons most likely to engage in criminal activities.

- How It Works:
  - Integrates big data: crime records, surveillance, social, environmental, and demographic data
  - Machine learning algorithms identify crime patterns, hotspots, and risk factors
- Outputs: “Heat maps,” risk scores, patrol/resource deployment recommendations
- Promise:
  - Enables proactive, targeted policing and optimized resource allocation
  - Some studies show reductions in property and violent crime rates (e.g., Memphis Blue CRUSH, LAPD PredPol)
  - Can reveal hidden patterns not visible to human analysts

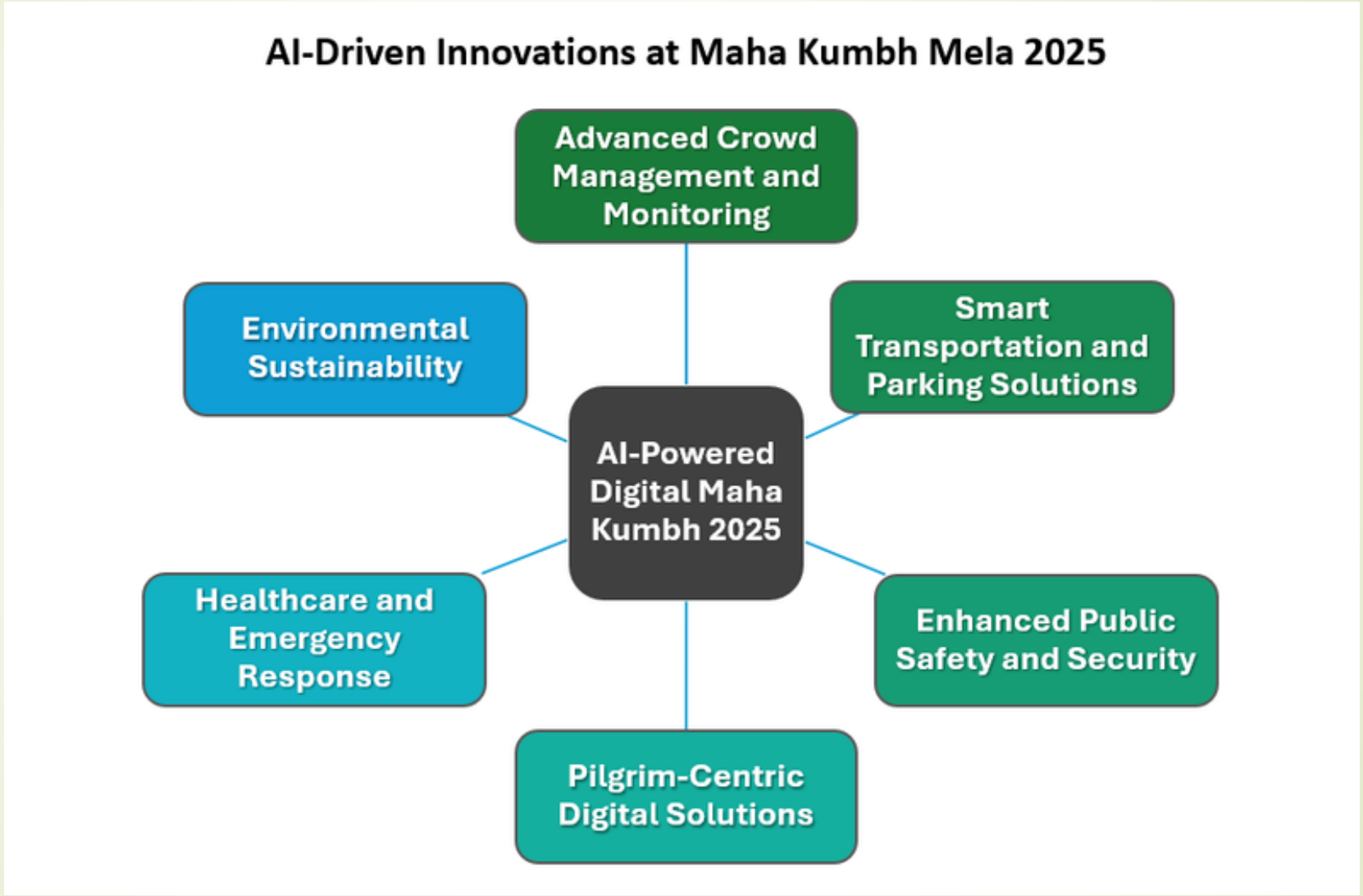
- Europe: Diverse Adoption and Innovation
- Germany: KrimPro (Berlin)- use police and public data for hotspot and risk prediction.
- France, Austria, Estonia, Romania: Piloting individual-based and location-based predictive policing.
- EU-Wide: EncroChat takedown—collaborative big data analytics disrupted organized crime, seized €739.7 million in criminal assets.

- United States: Early Adopters
  - PredPol (Los Angeles, others): Uses historical crime data to forecast hotspots.
  - Blue CRUSH (Memphis): Integrated crime analytics for targeted patrols.
  - Chicago, New York: Use of “heat lists” and risk scores for individuals and locations.
- Surveillance-Driven Models
  - Facial recognition, biometrics, and social credit data integrated for city-wide predictive policing and social management

Maha Kumbh Mela 2025 Mega Statistics



* Ghats are River landing stairs with large platforms.


AI-Driven Innovations at Maha Kumbh Mela 2025
Advanced Crowd Management and Monitoring
Environmental Sustainability
Smart Transportation and Parking Solutions
AI-Powered Digital Maha Kumbh 2025
Healthcare and Emergency Response
Enhanced Public Safety and Security
Pilgrim-Centric Digital Solutions

What is Maha Kumbh Mela and why is it celebrated?

The Maha Kumbh Mela, is renowned globally as the largest peaceful congregation of people.

*The festival is a testament to the human quest for divine and spiritual liberation, representing the belief in freedom from the continuous cycle of birth, death, and rebirth. This gathering allows millions of devotees to immerse themselves in the holy waters of the rivers, symbolizing a purification of the soul and as believed, a path to attaining **Moksha**, that is, liberation or emancipation.*

*The Maha Kumbh Mela transcends the worldly and embraces the spiritual, manifesting the richness of India's diverse cultural heritage and spiritual traditions. It embodies the principle of Vasudhaiva Kutumbakam, an Indian philosophy meaning **'the world is one family'**, where all attendees, regardless of their social or economic stature, are considered equal, thereby reinforcing the sense of unity amid diversity.*

Moreover, the festival paves the way for various community outreach initiatives such as complimentary medical aid, provision of food, and spiritual guidance. The Maha Kumbh Mela, therefore, is not just a religious gathering but a confluence of faith, spirituality, and humanity, deeply etched in the Indian way of life.

AI-Driven Crowd Management at Kumbh Mela

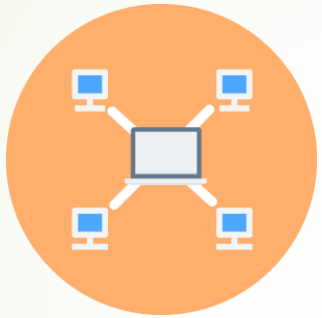
- **AI-Powered Cameras:**
  Over 2,750 cameras were installed, 250 of which were AI-enabled. These tracked:
- Crowd density in real-time
- Suspicious behavior or anomalies
- Movement patterns across key zones like ghats, roads, stations
- **Integrated Command & Control Centre (ICCC):**
- Aggregates real-time visual and analytical data.
- Enables officials to take swift, informed actions such as deploying police, redirecting foot traffic, or triggering evacuation protocols.
- **Geo-Mapping & GPS Tracking:**
- Crowd density data mapped to specific zones.
- Security personnel and resources tracked live for optimal allocation.

Predictive Policing Through Data Analytics

- **How AI Helps Predict Crowd Behavior:**
  - **Density Forecasting:**
    Using live video feeds, AI estimates crowd density at various entry/exit points and predicts future congestion zones.
  - **Behavioral Analysis:**
    Algorithms trained to detect irregular crowd movement patterns or panic behavior—triggers alerts for security intervention.
  - **Heat Mapping:**
    Visualizes the most congested areas in real time using thermal and movement data, helping in traffic diversion and dispersal planning.
  - **Risk Zone Prediction:**
    Historical crowd data + real-time inputs = forecast of high-risk zones for stampedes, theft, or medical emergencies.

- **Operational Benefits:**
- **Proactive Decision-Making:** Authorities no longer wait for incidents—they act on predictive alerts.
- **Efficient Deployment:** Manpower and emergency teams positioned dynamically based on real-time threats.
- **Visitor Safety Enhanced:** Faster emergency response and improved navigation help reduce casualties and confusion.

- Searching documents which includes but not limited to **people, place, organizations, events**



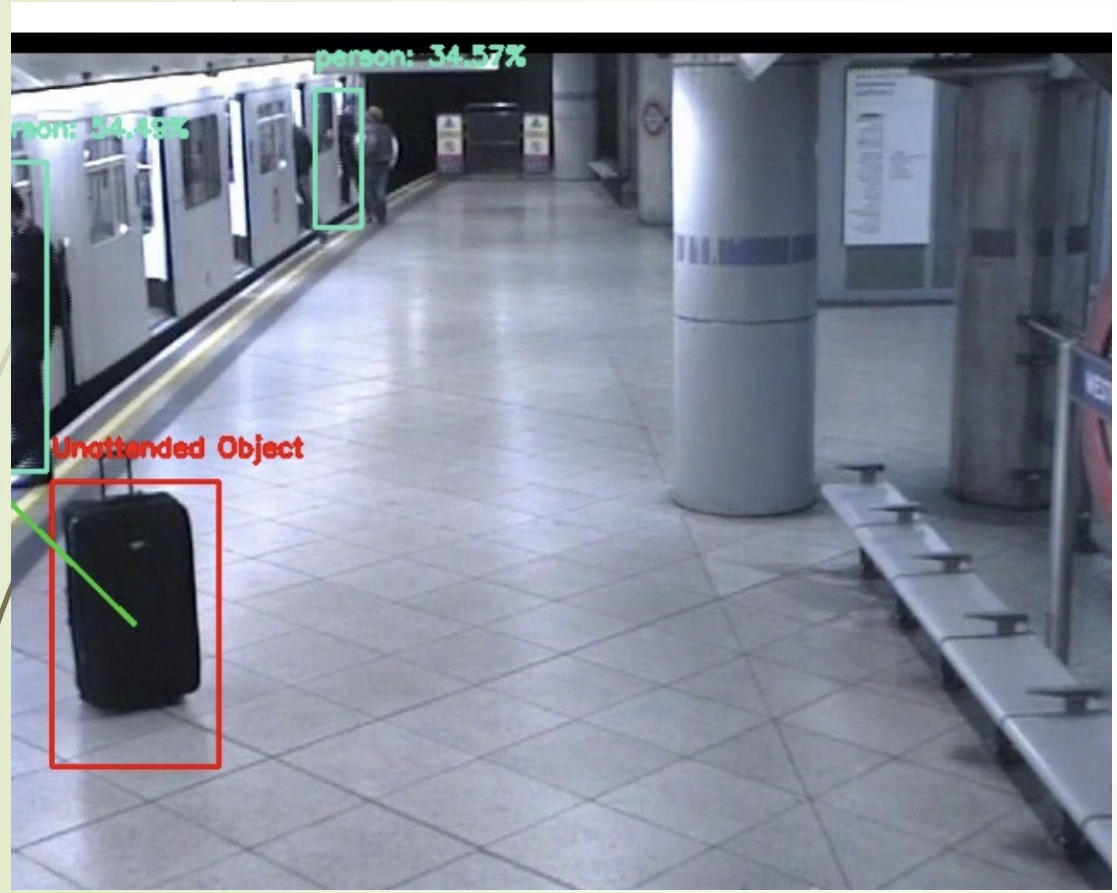
- **Ambiguity** of data and connecting the data available from multiple sources without duplication

- Removing **Language barrier** when targeting international organizations

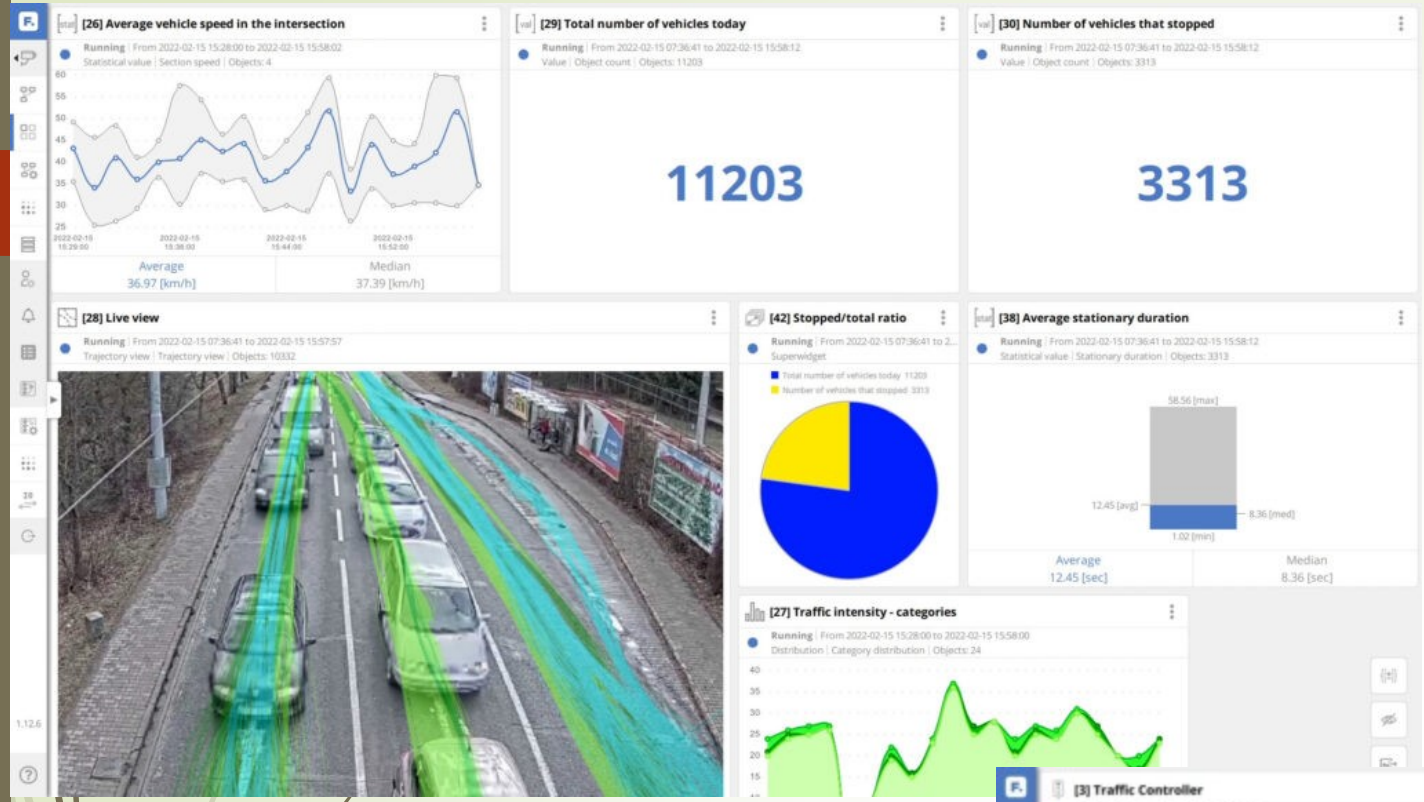
- Availability of **multilevel analysis.**

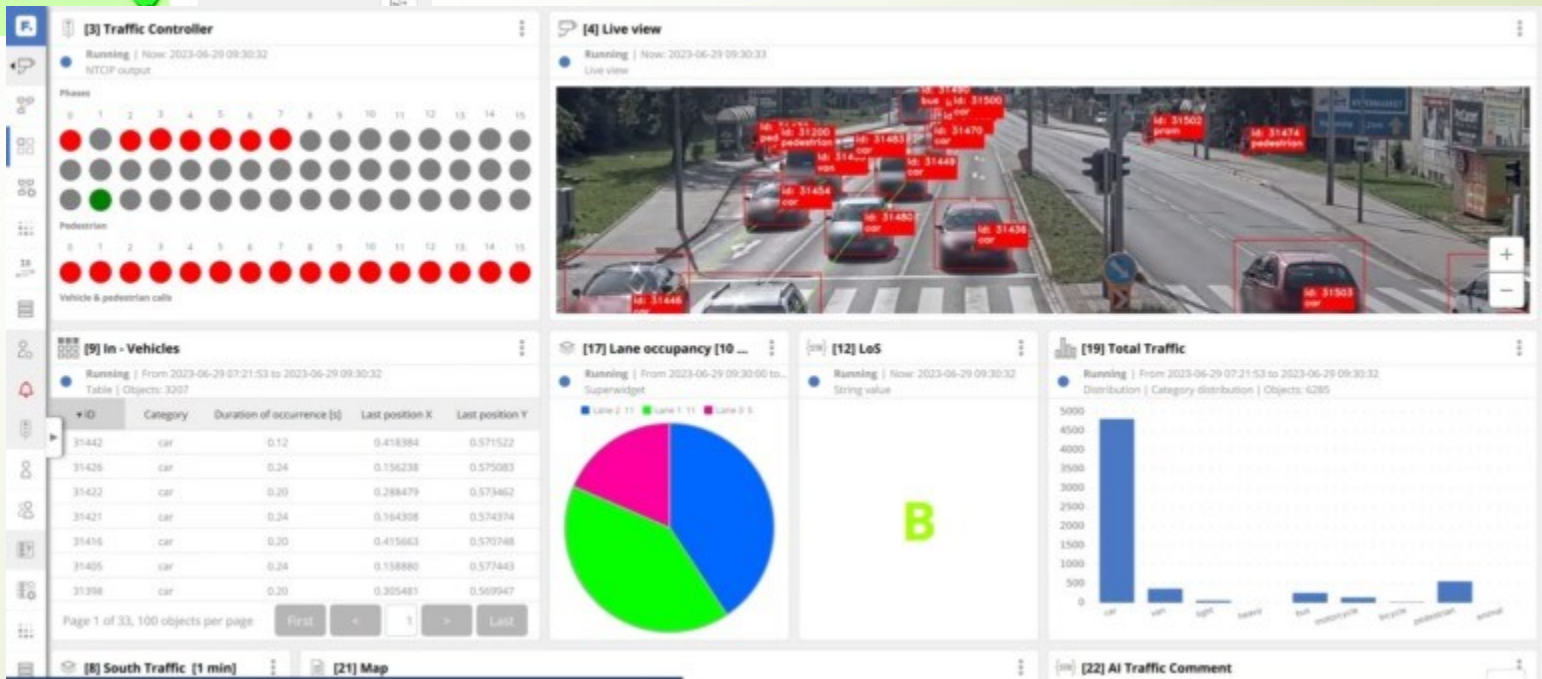
UTTAR PRADESH POLICE - TRINETRA

- Trinetra is an AI-based mobile application. It leverages advanced technologies to enhance crime prevention and investigation.
- **Key Features:**
  - CONNECTED TO **CRIME CRIMINAL TRACKING NETWORK SYSTEM**
- **Comprehensive Criminal Database:**
  - Digitized records of over 900,000 criminals, including photographs, addresses, and criminal histories.
  - **Facial and Voice Recognition:**
  - Utilizes AI-powered facial recognition to identify suspects from images and videos.
  - Crime hotspot mapping and trend analysis
  - Repeat offender tracking and profiling
  - Real-time alerts and resource optimization
- Incorporates speaker identification to match voice samples, aiding in cybercrime investigations.
- **Crime GPT Integration:**
- An extension of Trinetra, Crime GPT allows officers to retrieve information using text or voice queries, streamlining data access.
- **Mobile Accessibility:**
- Available on Android and iOS platforms, enabling officers to access real-time data during field operations.


person: 34.57%
Unattended Object


14:33:01
CAMERA 01


[26] Average vehicle speed in the intersection
Average
36.97 [km/h]
Median
37.39 [km/h]
[29] Total number of vehicles today
11203
[30] Number of vehicles that stopped
3313
[28] Live view
[42] Stopped/total ratio
[38] Average stationary duration
58.56 [max]
12.45 [avg]
8.36 [med]
1.02 [min]
Average
12.45 [sec]
Median
8.36 [sec]
[27] Traffic intensity - categories


[3] Traffic Controller
[4] Live view
[9] In - Vehicles
[17] Lane occupancy [10 ...
[12] LoS
B
[19] Total Traffic
[8] South Traffic [1 min]
[21] Map
[22] AI Traffic Comment

Crime GPT : Text based Video query

Events

Text Search

Search Type

Both

Result Limit

5

Locations

All Selected (1)

Feeds

All Selected (2)

Start & End Date

18/11, 00:00 → 23/11, 10:33

Search Text

black car with plus sign on front screen

Reset | Search

Tabular | Grid | Graphical

Overview

Print

Total Results: 5

Date: 22nd Nov 2023 — Result: 2

Time: 05:40 PM - 05:50 PM — Result: 1

DATE	TIME	CAMERA NAME	LOCATION NAME	MATCHED IMAGE	SCORE
22nd Nov 2023	05:45:49 PM	Camera 02	Purvanchal Expressway Toll 2		0.36

Time: 06:10 PM - 06:20 PM — Result: 1

Date: 21st Nov 2023 — Result: 2

Time: 10:20 AM - 10:30 AM — Result: 1

DATE	TIME	CAMERA NAME	LOCATION NAME	MATCHED IMAGE	SCORE

- CMAPS: Space-Tech Powered Predictive Policing
  - Integrates real-time data from Dial-100, CCTNS, and satellite imagery
  - Visualizes crime hotspots and trends on geospatial maps
- Key Features
  - Auto-updates every 1–3 minutes; identifies and ranks crime hotspots
  - Enables neighborhood and proximity analysis, gang identification, and suspect profiling
  - PDA devices give officers real-time access to criminal records at the scene
- Impact
  - Faster, data-driven deployment and patrols
  - Improved resource optimization and law & order management

- Proactive Crime Prevention
  - AI analyzes historical and real-time data to forecast crime hotspots and trends.
  - Enables targeted patrols and resource allocation, deterring crime before it occurs.
- Efficient Resource Management
  - Optimizes deployment of police personnel and equipment, especially in resource-constrained settings.
- Enhanced Public Safety
  - Faster response to emerging threats and incidents through real-time analytics.
  - Improves law and order management during major events and emergencies.
- Data-Driven Decision Making
  - Reduces reliance on guesswork and intuition; supports evidence-based policing.
  - Identifies patterns, correlations, and anomalies difficult for human analysts to detect.
- Innovation in Indian Policing
  - Adoption in UP, Delhi, Hyderabad, and other states as part of "SMART" policing initiatives.
  - AI-powered tools recognized as best practices for modern, accountable, and responsive policing
-

CHALLENGES

- Limit predictive policing to forecasting *locations, times, and types* of crime—not individuals or groups. Empirical research recommends this as a key safeguard to reduce the risk of profiling and wrongful detention
- Data Audits and Quality Control:
  Regularly audit datasets for bias and update them to reflect current realities, not just historical patterns
- Transparency and Accountability:
  Make algorithms and decision-making processes transparent; allow independent oversight and mechanisms for individuals to contest outcomes.

- Algorithmic Bias and Discrimination
  - Risk of reinforcing historical biases in policing data
  - Disproportionate targeting of marginalized communities
- Lack of Transparency (“Black Box” Problem)
  - Difficulty in understanding or challenging algorithmic decisions
  - Limits accountability and public trust
- Over-Reliance on Technology
  - Risk of sidelining human judgment and discretion
  - Possible erosion of community policing and trust
- Legal and Ethical Gaps
  - Absence of clear regulations governing predictive policing
  - Need for robust oversight and safeguards

1. The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review Youngsub Lee, Ben Bradford and Krisztian Posch
2. https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/feb/doc2025225508901.pdf [**Digital Transformation of Justice: Integrating AI in India's Judiciary and Law Enforcement]**

LETS START TALKING!

HESSEN

Artificial Intelligence – Impact on Investigations and Handling in Court

#DIGITALISATION and #AI in Criminal Justice

Cracow, 26-27 May 2025

Rainer Franosch, Deputy Director-General for Criminal Law
Ministry of Justice of the German Federal State of Hesse

Co-funded by the European Union

HESSEN

Introduction to AI in Criminal Proceedings

- **Definition: AI refers to computer systems capable of tasks requiring human intelligence.**

- **Relevance in Criminal Justice:**
  - **Enhances data analysis capabilities.**
  - **Assists in predictive policing and forensic investigations.**
  - **Raises questions about evidence admissibility and defendants' rights.**

HESSEN

Legal Framework in the European Union

- **EU Artificial Intelligence Act:**
  - **Classifies AI systems by risk levels: unacceptable, high, limited, minimal.**
  - **High-risk systems (e.g., biometric ID) have strict requirements.**

- **Charter of Fundamental Rights of the EU:**
  - **Ensures rights to privacy, data protection, and fair trial.**

- **e-Evidence Regulation:**
  - **Cross-border access to electronic evidence impacts AI-generated data.**

HESSEN

AI in Criminal Investigations and Proceedings

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

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

HESSEN

AI in Criminal Investigations and Proceedings

- **Analysis of Large Data Volumes:**
  - **Detection & categorization of files (IT forensics…)**
  - **Pre-evaluation of images and videos (child abuse imagery, juvenile pornography…)**
  - **Communication & network data analysis (chats, emails…)**
  - **Financial data & transaction analysis (account data, blockchain…)**

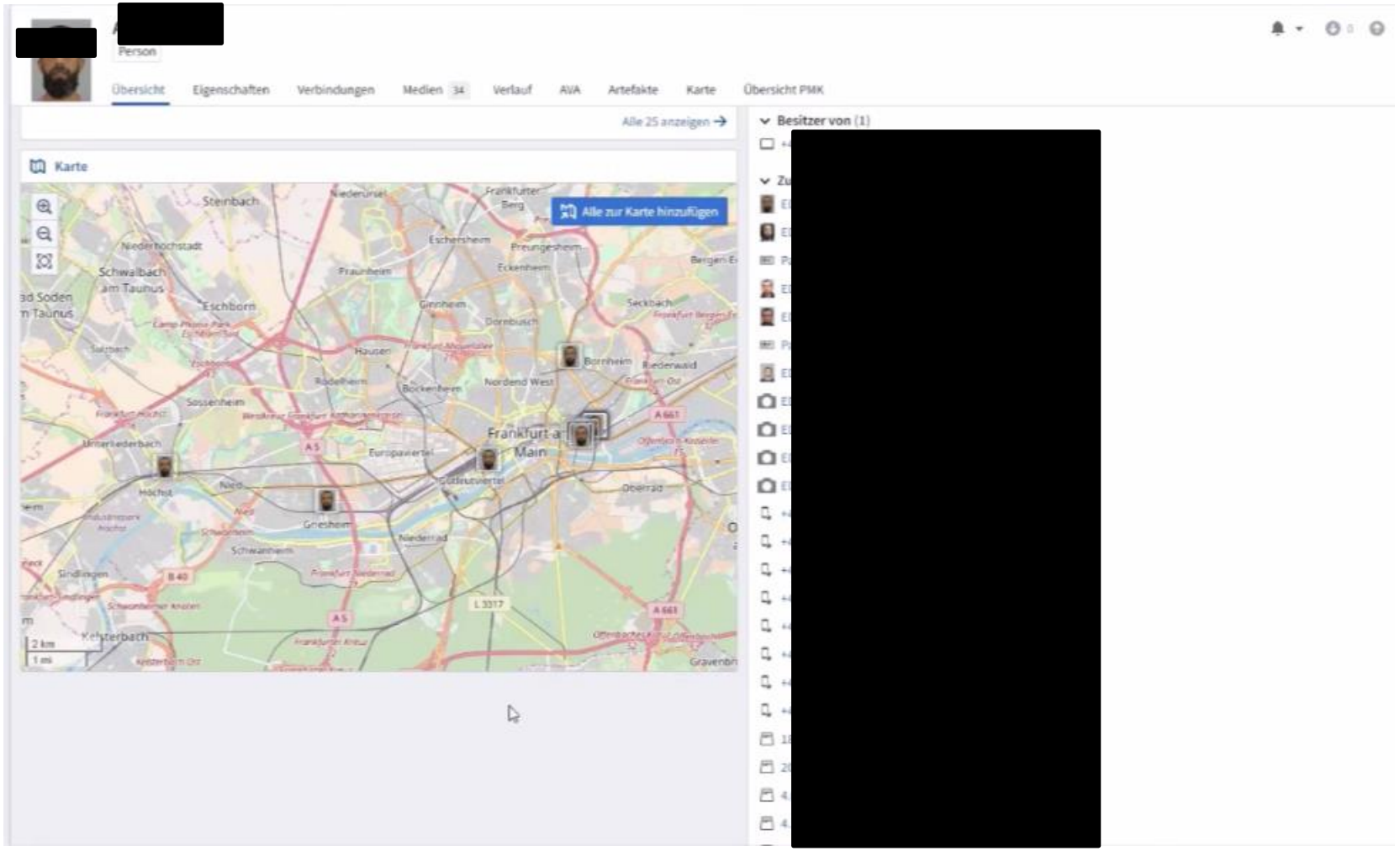
- **Judicial Prognostic Assessments in Criminal Law (vs. predictive policing):**
  - **Risk of violence by individuals & overall threat assessment (police…)**
  - **Criminal liability of statements & preliminary evaluation (hate speech…)**
  - **Risk of flight & reoffending (grounds for detention…)**
  - **Risk of recidivism (probation, preventive detention…)**

HESSEN

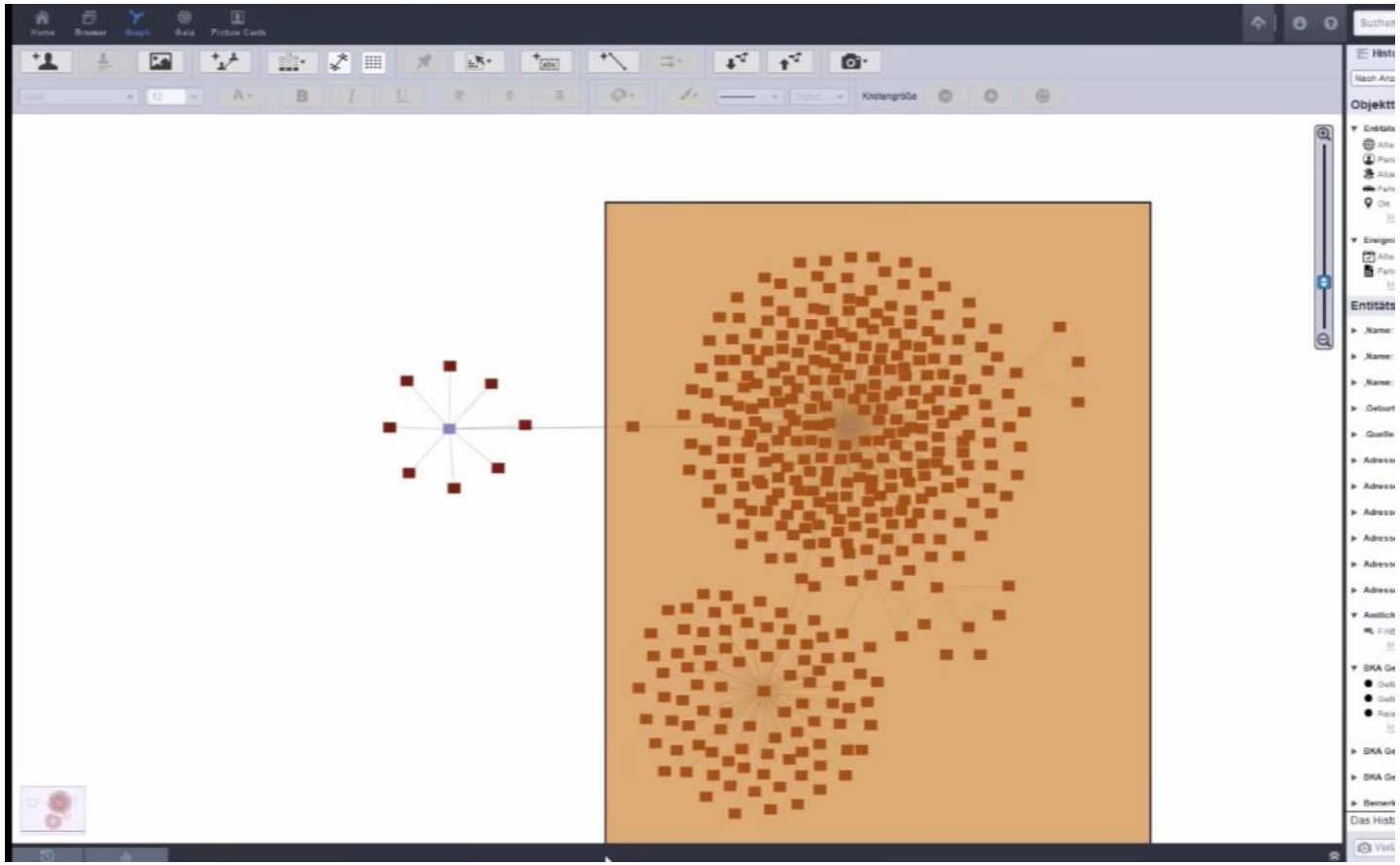
AI in Criminal Investigations and Proceedings

- **Legal Assistance:**
  - **Speech recognition & translation (legal assistance, complaint chatbots…)**
  - **Analysis & summarization of case law (beck-chat…)**
  - **Document analysis & information integration (form-filling, robo-judges…)**
  - **Deadline tracking and statistics (reminders…)**

HESSEN


[redacted]
Person
Übersicht
Eigenschaften
Verbindungen
Medien 34
Verlauf
AVA
Artefakte
Karte
Übersicht PMK
Alle 25 anzeigen
Karte
Alle zur Karte hinzufügen
Besitzer von (1)
[redacted]
Steinbach
Niederhöchstadt
Schwalbach am Taunus
Eschborn
Frankfurter Berg
Eschersheim
Preungesheim
Eckenheim
Praunheim
Ginnheim
Dornbusch
Seckbach
Hausen
Bornheim
Bockenheim
Nordend West
Sossenheim
Unterliederbach
Höchst
Nied
Griesheim
Europaviertel
Gutleutviertel
Frankfurt a. Main
Oberrad
Niederrad
Schwanheim
Sindlingen
Kelsterbach
A 5
A 661
B 40
L 3017
2 km
1 mi

HESSEN



HESSEN

Nase

- Nasenrücken
- Nasenkuppe
- Nasenboden
- Nasenabhang
- Nasenöffnung
- Nasenflügel
  - Wangenansatz
  - Form/Schwung
  - Abgrenzung zur Nasenkuppe
  - Abgrenzung zum Nasenabhang
  - Weichgewebsfülle
  - Nasenflügelfurche
  - Unterrand
    - stark/gering geschwungen
    - konkav/konvex/gerade
    - breit/schmal
    - aufgeworfen

Abb. 2 Merkmalsextraktion

HESSEN

AI in Court Proceedings

- **Evidence Evaluation:**
  - **Judges assess AI-derived evidence reliability.**
- **Expert Witnesses:**
  - **More reliance on technical experts**
  - **Concerns about profiling and transparency.**
- **Defendants' Rights:**
  - **Transparency and explainability essential under Article 6 ECHR**

HESSEN

Case Study – Predictive Policing in Germany

- Implementation in various German states.
- Challenges: Data protection, bias concerns.
- Ongoing debate on effectiveness and legality.

HESSEN

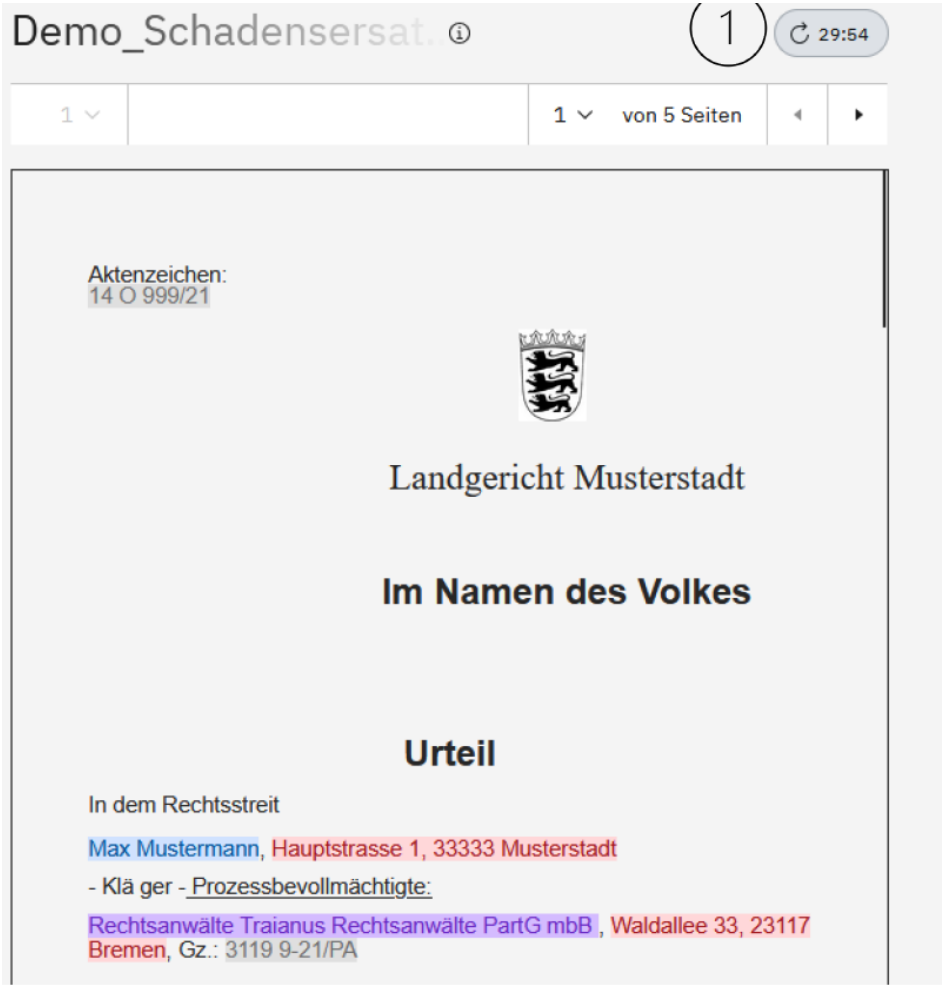
AI in the Courtroom

- IBM's OLGA System
- Assists in case categorization and metadata extraction.
- Speeds up case resolution, manages data loads.

HESSEN

AI in the Courtroom

JANO



HESSEN

Case Study I - AI in the Courtroom

SPIEGEL Panorama

Prozess in Wiesbaden

Tödlicher Unfall – Raser zu lebenslanger Haft verurteilt

Er raste mit Tempo 130 du
schuldig gesprochen word

29.11.2023, 20.22 Uhr

HESSEN

Case Study II - AI in the Courtroom

Bundeskriminalamt

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

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

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

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

HESSEN

Case Study – AI in Investigative Journalism

- Used in tracking fugitive Daniela Klette.
- Journalists applied facial recognition tools.
- Raised questions about AI's role in private vs. public investigation

HESSEN

Considerations and Discussion

- Bias and Discrimination
- Transparency and Accountability- Difficulty in explaining AI decisions.
- Legal Uncertainty - Lack of clear AI regulations in criminal law

Vs.

- Human expert witnesses are biased and inconsistent.
- AI systems face stricter regulation despite offering more transparency.
- Why should AI be more regulated than fallible human judgment?
- AI is Not the Decision-Maker
- Criminal procedures already include oversight mechanisms (e.g., judicial review).
- Additional regulation is redundant and burdensome.
- Regulatory Burden Hampers Law Enforcement
- AI Offers Superior Traceability

HESSEN

Considerations and Discussion

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

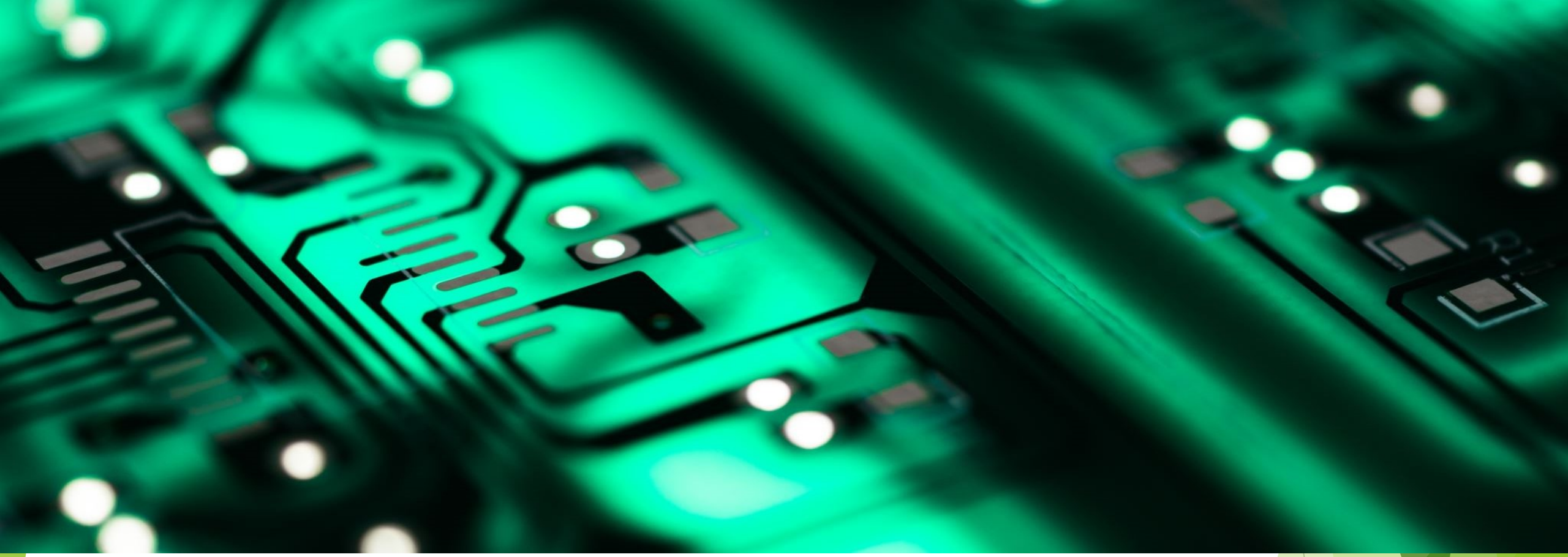
Call for Proportionality:

- **Regulate based on function and context—not based on AI status alone.**
- **Ensure safeguards without stifling innovation.**
- **Focus on accountability across both human and artificial contributors.**

HESSEN

Thank you for your attention!

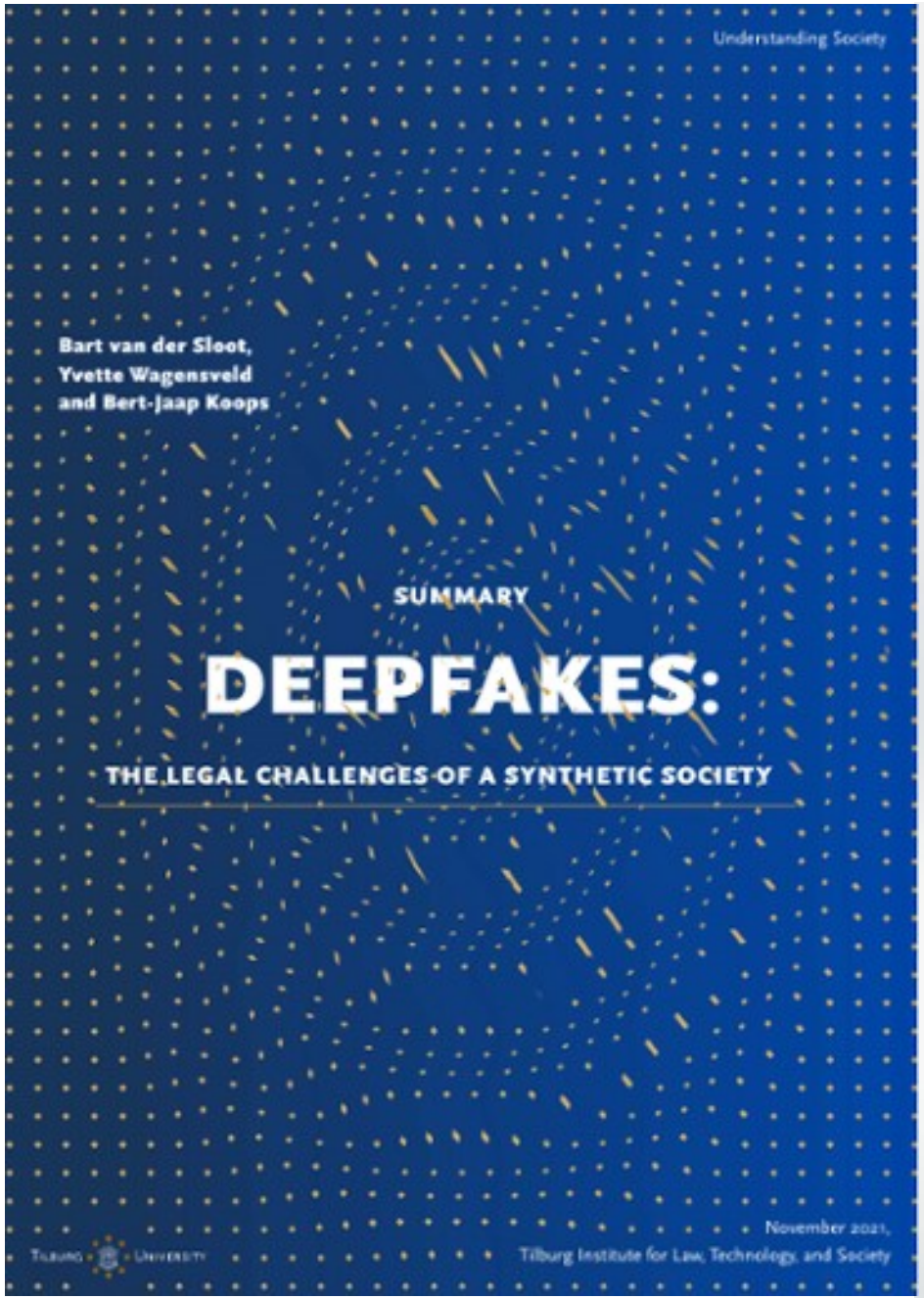
Questions? Remarks?

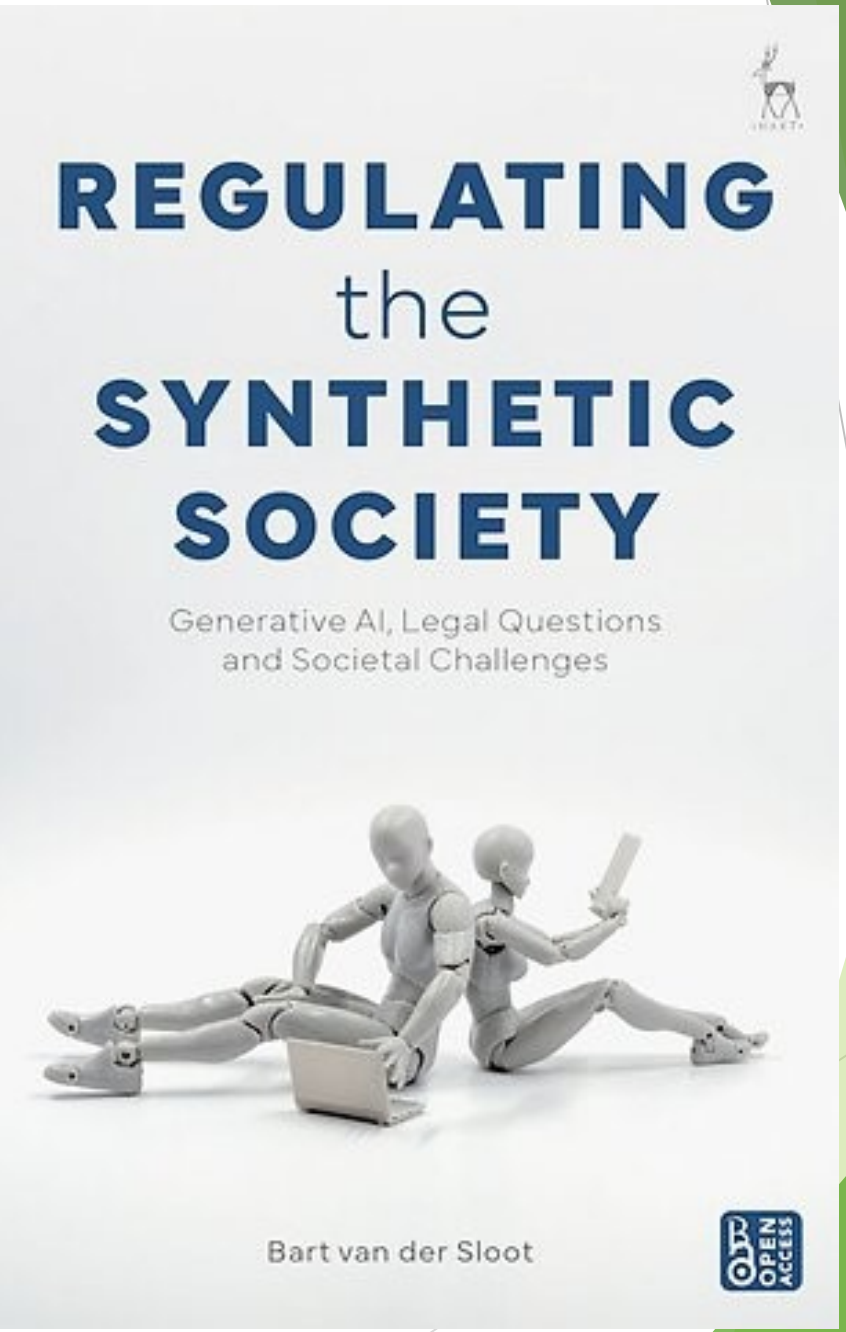


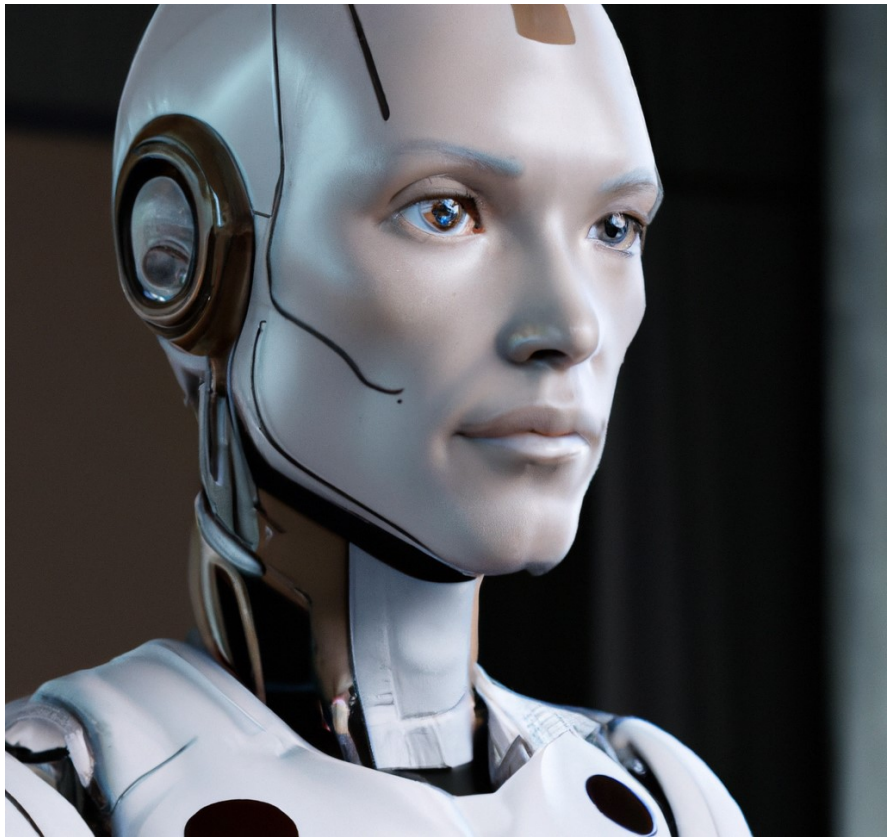
Deepfakes in Judicial Proceedings

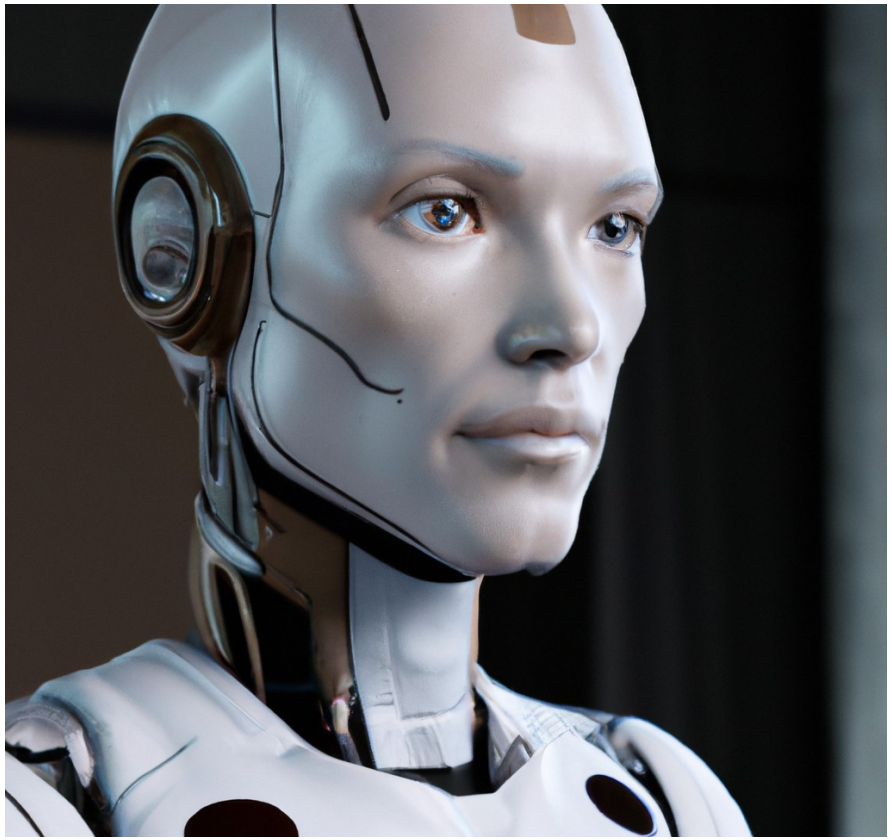
Co-funded by the European Union

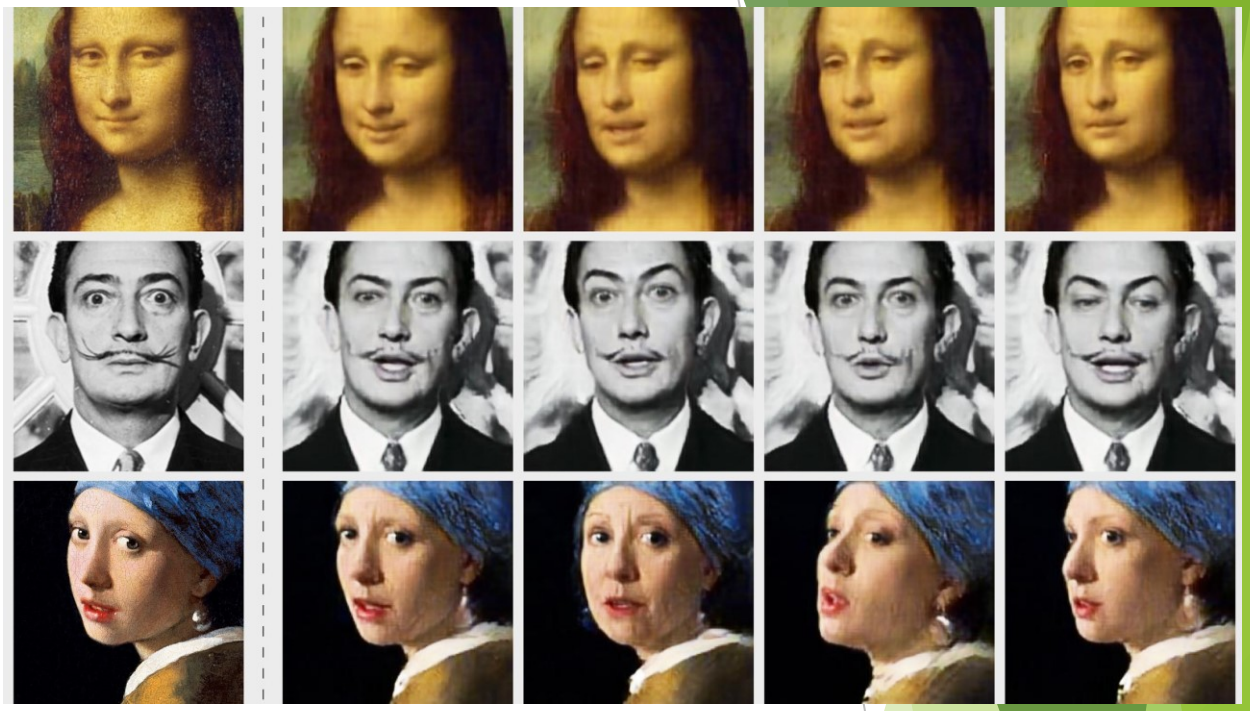
- Bart van der Sloot
- Lawyer & Philosopher
- Technological developments
- www.bartvandersloot.com


Understanding Society
Bart van der Sloot,
Yvette Wagensveld
and Bert-Jaap Koops
SUMMARY
DEEPFAKES:
THE LEGAL CHALLENGES OF A SYNTHETIC SOCIETY
November 2021,
Tilburg Institute for Law, Technology, and Society

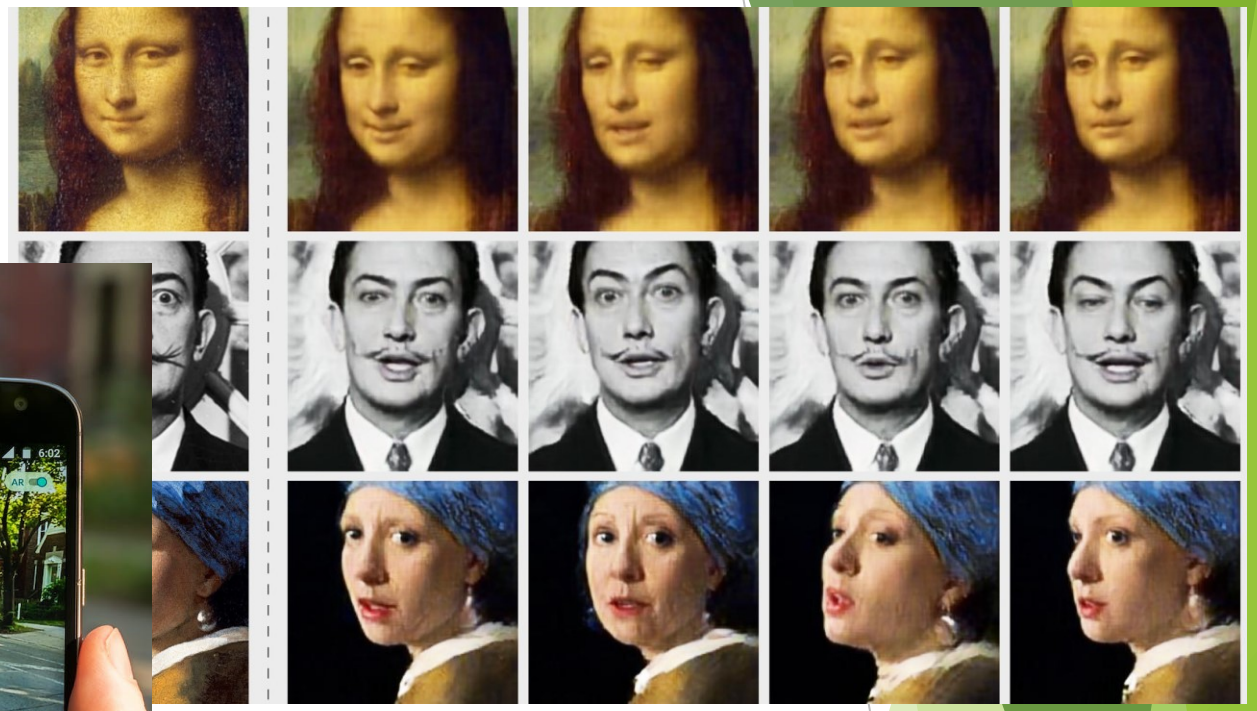

REGULATING
the
SYNTHETIC
SOCIETY
Generative AI, Legal Questions
and Societal Challenges
Bart van der Sloot
OPEN ACCESS

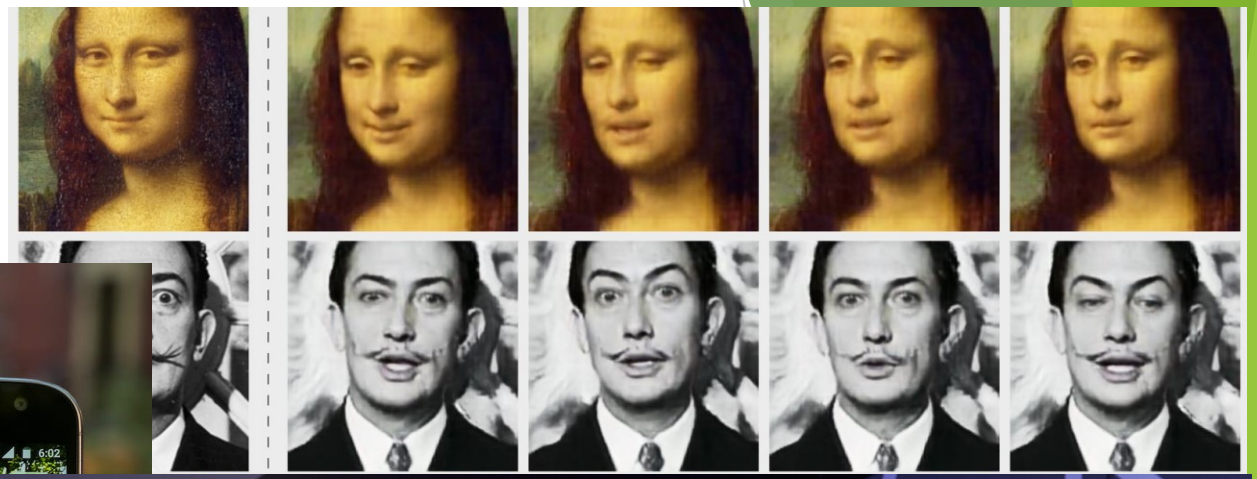






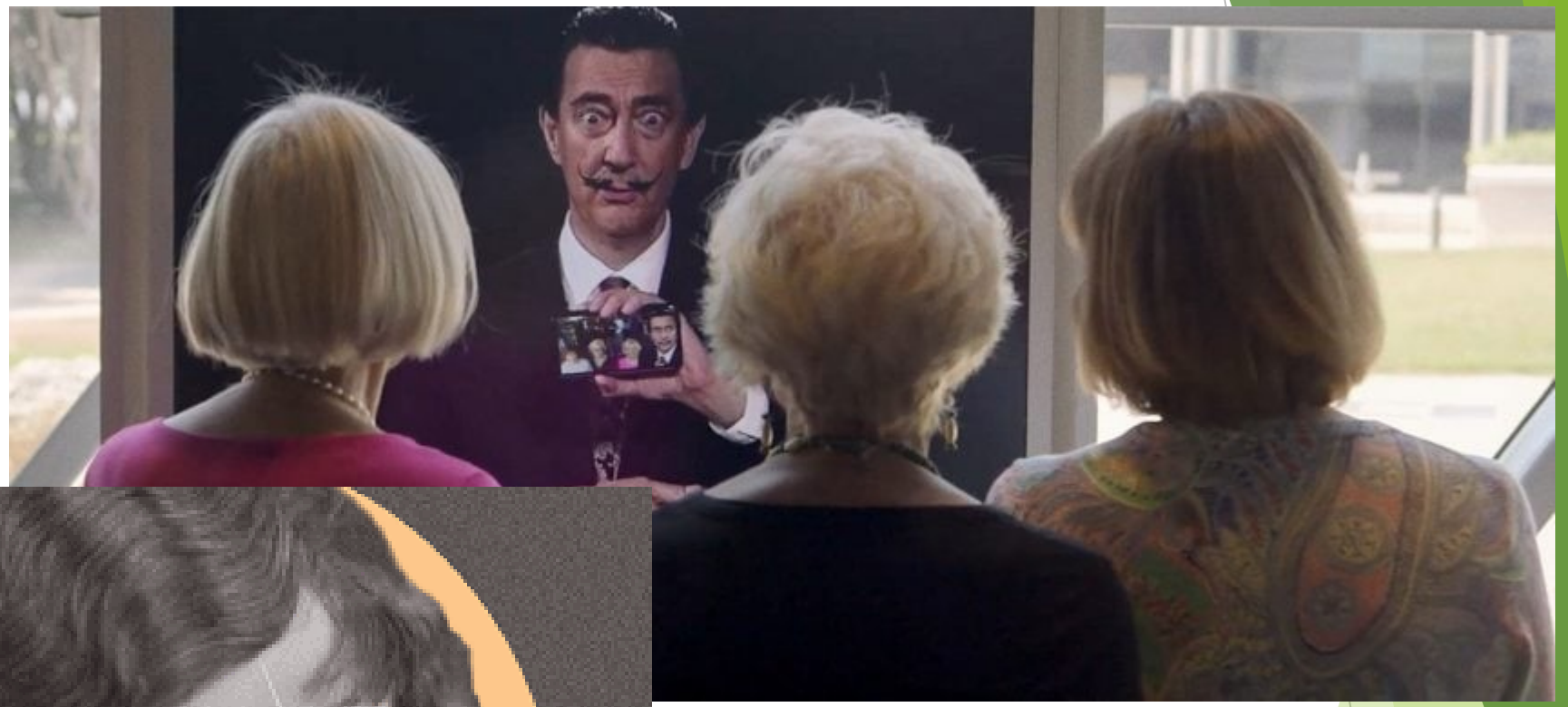

Pikachu
CP???
6:02
AR

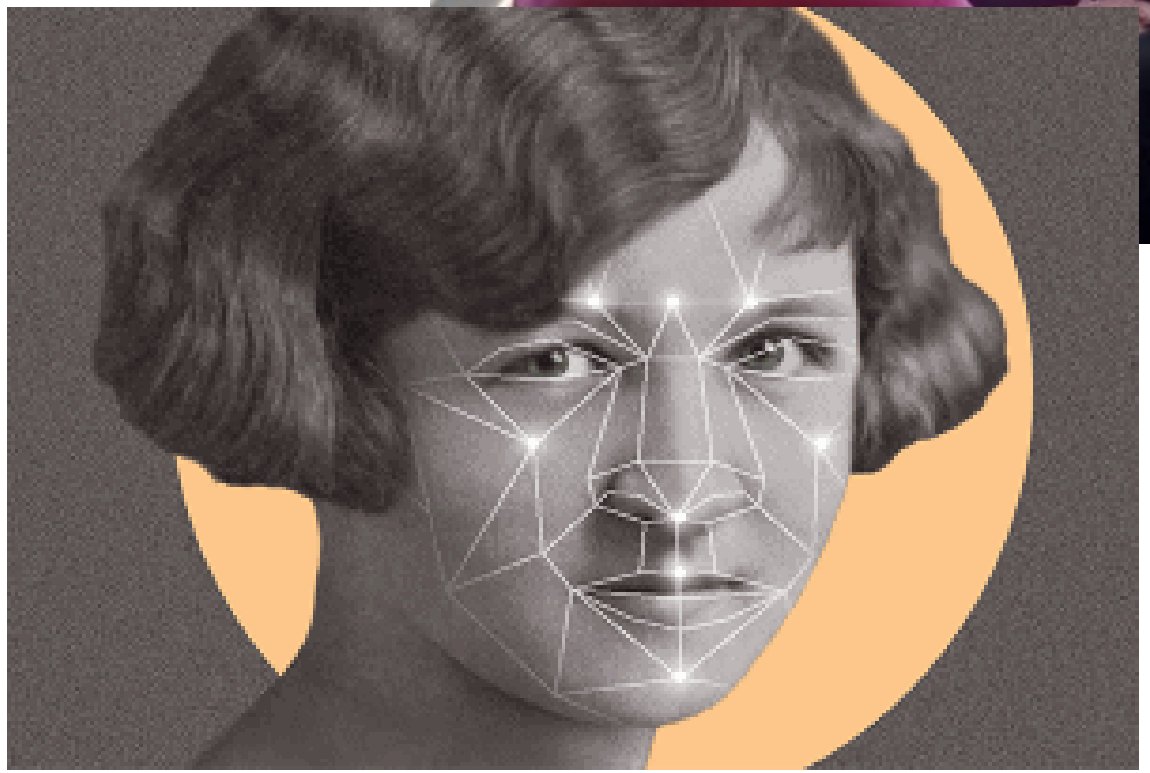





05
ZERO LATENCY

In 5 years, more than 90% of all photos, videos and text on the web will be generated or manipulated by AI





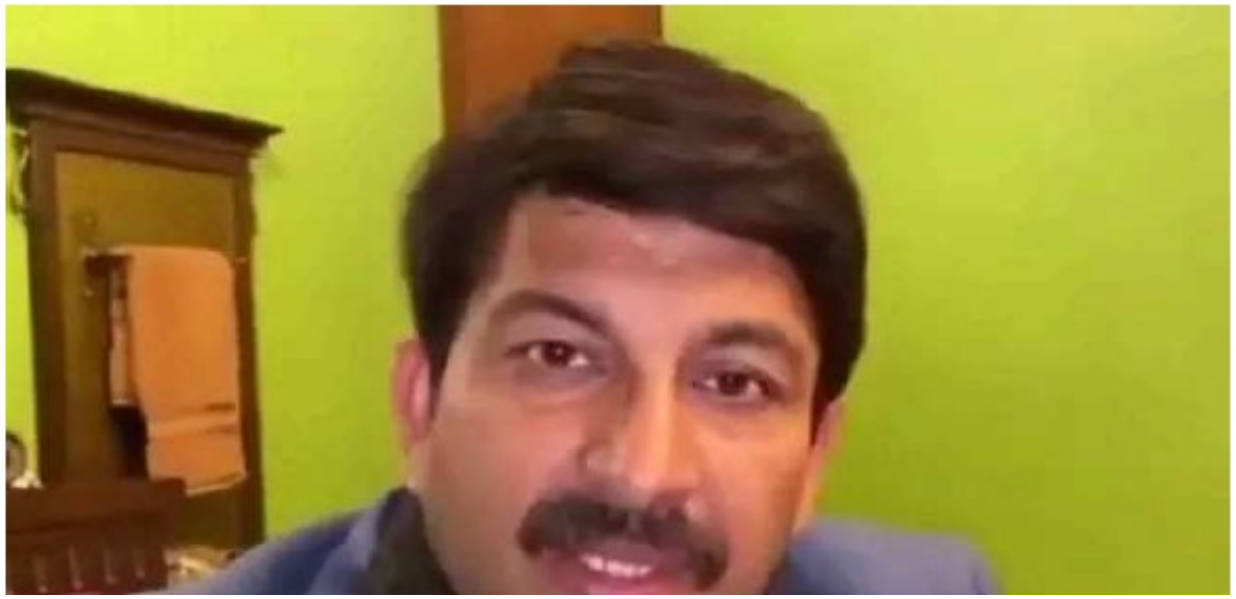
An Indian politician used AI to translate his speech into other languages to reach more voters / The intentional use of AI to fabricate a video is apparently a first in Indian politics

By Kim Lyons

Feb 18, 2020, 11:35 PM GMT+1

0 Comments (0 New)

If you buy something from a Verge link, Vox Media may earn a commission. ***See our ethics statement.***



COUNCIL *on* FOREIGN RELATIONS

from Net Politics, Digital and Cyberspace Policy Program, *and* Diamonstein-Spielvogel Project on the Future of Democracy

AI in Context: Indonesian Elections Challenge GenAI Policies

Prabowo Subianto, the leading candidate in Indonesia's presidential election, has used AI to rebrand from alleged human rights abuser to a "cuddly grandpa," in spite of AI companies' global policies against electoral uses.

Imran Khan—Pakistan's Jailed Ex-Leader—Uses AI Deepfake To Address Online Election Rally

Siladitya Ray Forbes Staff
Siladitya Ray is a New Delhi-based Forbes news team reporter.

Follow

Dec 18, 2023, 07:50am EST

Updated Dec 18, 2023, 07:50am EST

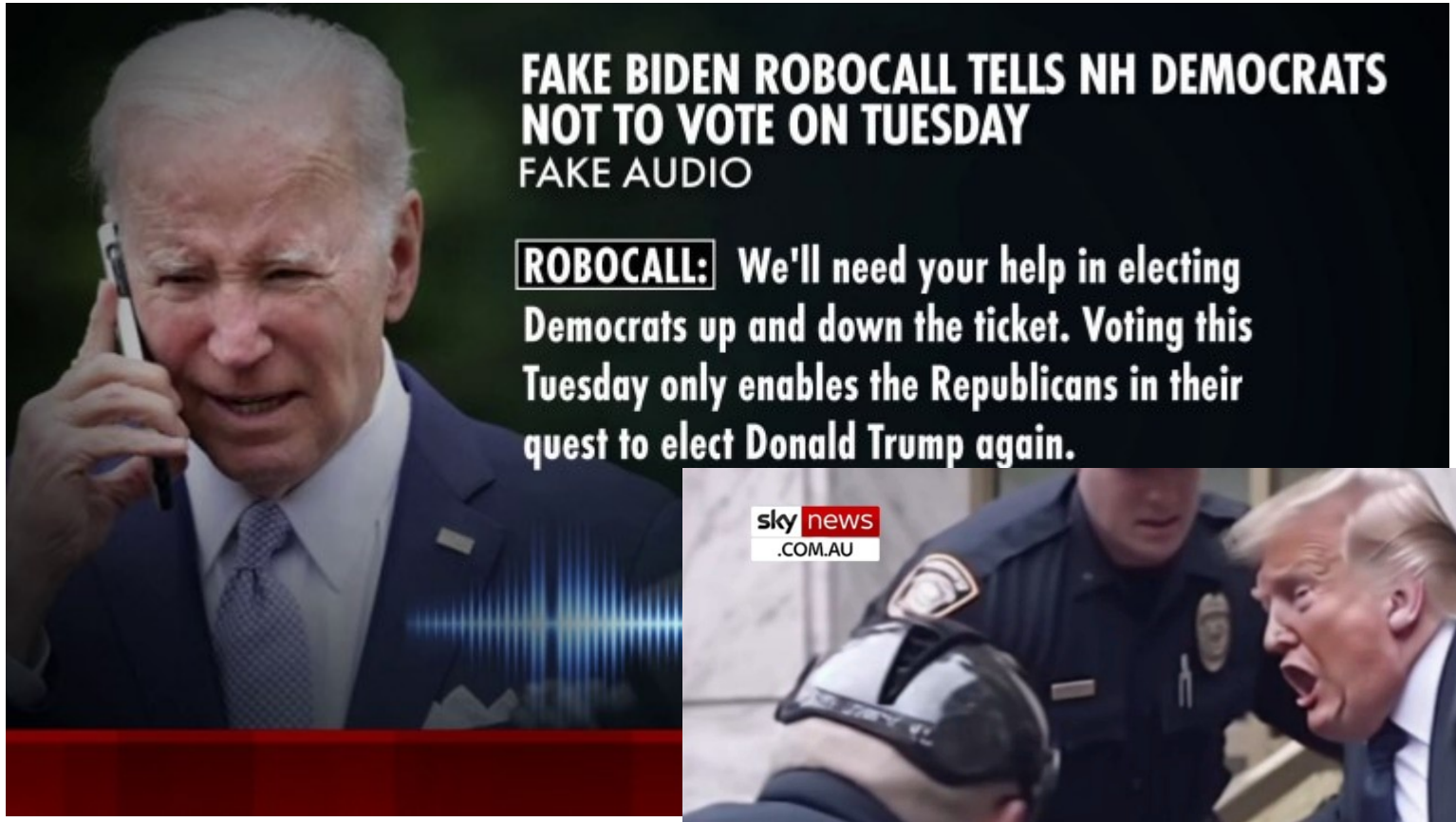
TOPLINE Former Pakistani Prime Minister Imran Khan, who is serving a three-year prison sentence, used AI-generated voice and video in a clip to campaign for his party ahead of the country's upcoming general election, spotlighting the potential use of AI and deepfakes as major polls are scheduled in the U.S., India, European Union, Russia, Taiwan and beyond in 2024.

Indian politician morphs into hologram to reach millions of voters

By Chris Welch, a reviewer specializing in personal audio and home theater. Since 2011, he has published nearly 6,000 articles, from breaking news and reviews to useful how-tos.
Source Motherboard | Via The Telegraph and Engadget
May 7, 2014, 9:24 PM GMT+2

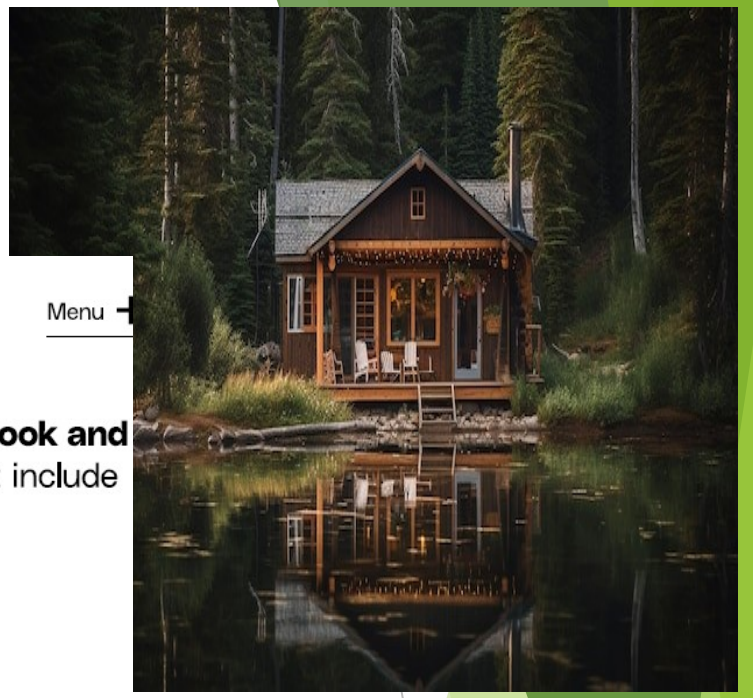
0 Comments (0 New)

Connecting with your country's electorate can be a challenge when you're eyeing a top seat in government. That difficulty only magnifies when you're running for office in the world's second-most populous country. So to reach as many voters as possible, India prime minister candidate Narendra Modi went the sci-fi route. He turned himself into a hologram


FAKE BIDEN ROBOCALL TELLS NH DEMOCRATS NOT TO VOTE ON TUESDAY
FAKE AUDIO
ROBOCALL: We'll need your help in electing Democrats up and down the ticket. Voting this Tuesday only enables the Republicans in their quest to elect Donald Trump again.


sky news
.COM.AU
First Edition
DEEPFAKES OF TRUMP ARREST EMERGE ON TWITTER
REAL NEWS, HONEST VIEWS.


StyleGAN2 (Karras et al.)



The Verge

Menu

META / TECH / FACEBOOK

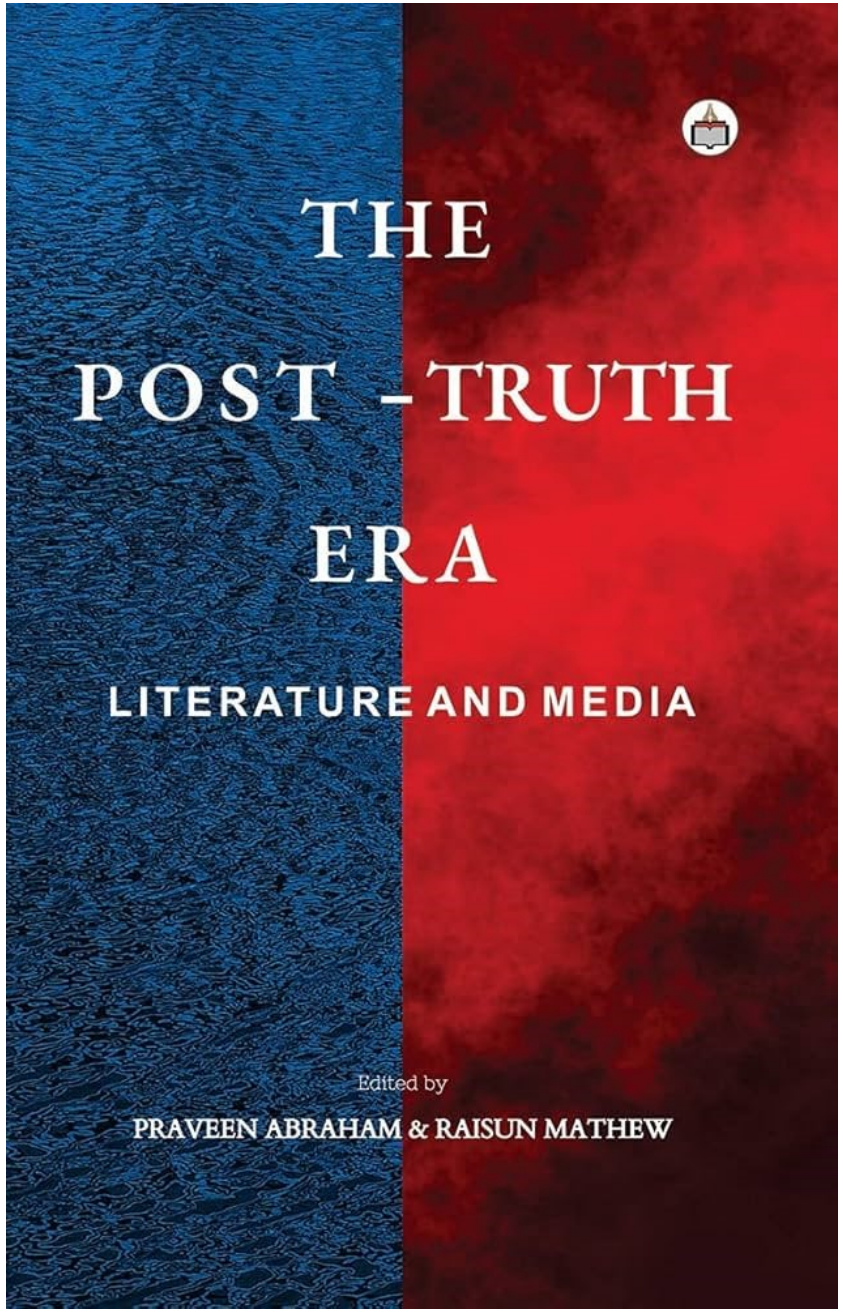
Meta's going to put AI-generated images in your Facebook and Instagram feeds / Some of the AI-generated images might include your face.

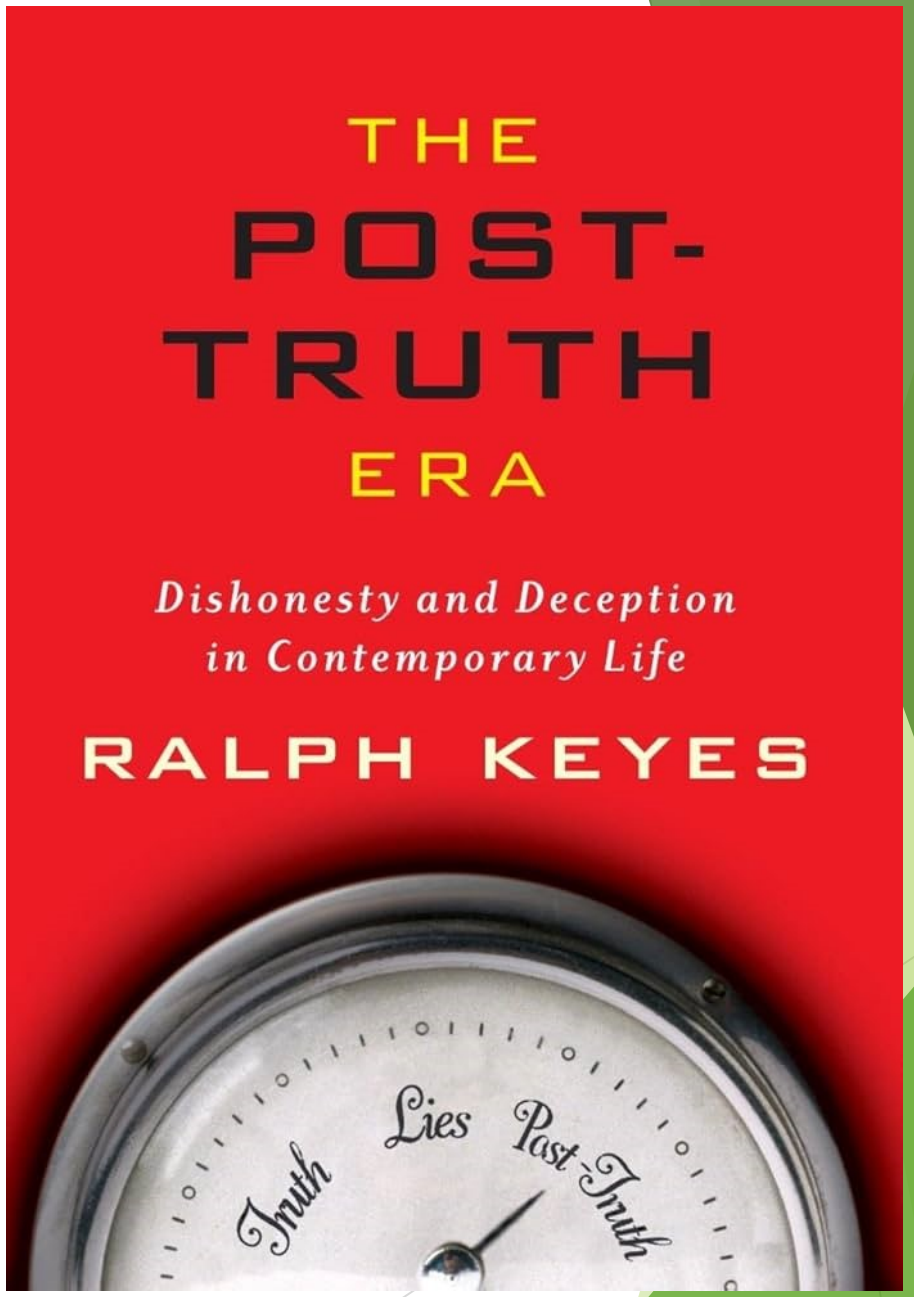
By Emma Roth, a news writer who covers the streaming wars, consumer tech, crypto, social media, and much more. Previously, she was a writer and editor at MUO.

Sep 25, 2024, 7:28 PM GMT+2

4 Comments (4 New)


TikTok
@joannajkenny
this filter has been used over 2 million times
this filter should come with a warning 😭
and then this the next
TikTok
@joannajkenny
these filters have to stop 😫


THE
POST -TRUTH
ERA
LITERATURE AND MEDIA
Edited by
PRAVEEN ABRAHAM & RAISUN MATHEW


THE
POST-
TRUTH
ERA
Dishonesty and Deception
in Contemporary Life
RALPH KEYES
Truth
Lies
Post-Truth

VICE Video Podcasts News Tech Music Food Health Money + More

MOTHERBOARD
TECH BY VICE

Thieves Used Audio Deepfake of a CEO to Steal $243,000

The heist is just a preview of how unprepared we are for AI-powered cybercrime.

By Edward Ongweso Jr

Sep 6 2019, 2:23am Share Tweet

The State of Deepfake

Since emerging in late 2017 the phenomenon of d
of technological sophistication and societal impa
the current state of deepfakes by analyzing their

Total number of deepfake videos online

14,678

percentage of deepfake videos online by pornographic and non-pornographic content

96%

4%

Total number of video views across top four dedicated deepfake pornography websites

134,364,438

BBC

Register

Home News US Election Sport Business Innovation Culture Arts Travel Earth Video Live

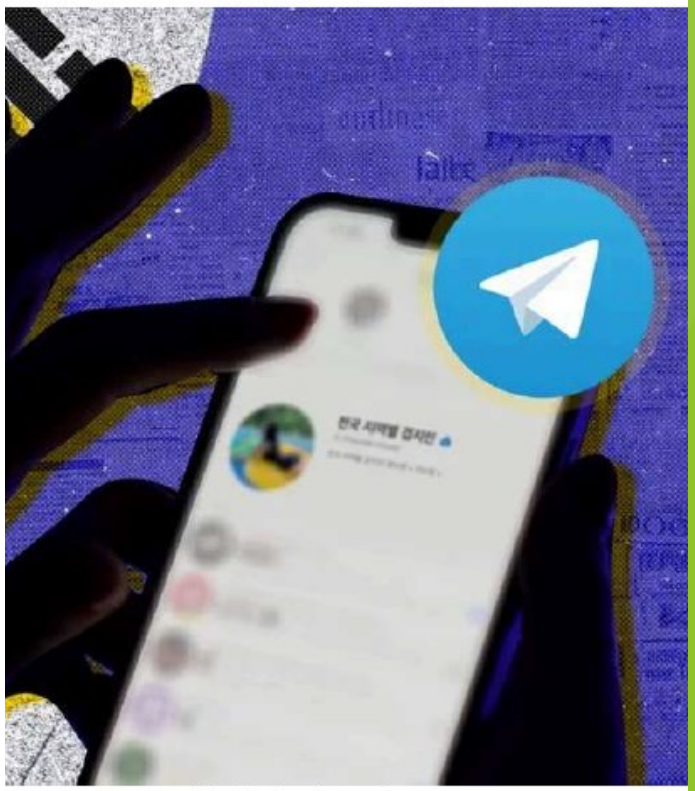
Inside the deepfake porn crisis engulfing Korean schools

3 September 2024

Share Save

Jean Mackenzie
Seoul correspondent

Leehyun Choi
Seoul Producer



popped up on Heejin's phone from an anonymous
l information have been leaked. Let's discuss."

New Scientist

Technology

Could sex robots and virtual reality treat paedophilia?

Not Like Us is Aviva Rutkin's monthly column exploring the minds of intelligent machines – and how we live with them

By Aviva Rutkin

2 August 2016

WOMAN'S AVATAR GANG RAPED IN METAVERSE

Description

We specialize in creating AI-generated adult gore porn images that will make your skin crawl. We're dedicated to bringing your darkest desires / nightmares to life...

From horror to snuff, and gore to the grotesque, we offer a range of adult categories that will satisfy your every desire for the horrific. Our AI algorithms are designed to generate images that are both disturbing and haunting.

of our characters are created by artificial elligence !

if you're looking for a place to indulge your rkest desires, look no further. Our AI-generated ages will leave you breathless and haunted, long er you've left our site. Enter at your own risk, and epare to face the horror within.

Effects AI in the Courtroom

Business & Practice
Jan. 30, 2024, 8:55 PM GMT+1

NY Lawyer Faces Possible Sanctions for Citing Phony ChatGPT Case

By Sam Skolnik

Documents

Decision

- Use of ChatGPT by lawyer Jae Lee referred to grievance panel
- Two Manhattan lawyers fined $5,000 in June for ChatGPT use

An attorney in suburban New York City faces possible sanctions for using ChatGPT to generate a nonexistent state court decision she cited in a legal filing.

The conduct of Uniondale, New York lawyer Jae Lee of the JSL Law Offices fell "well below the basic obligations of counsel," the US Court of Appeals for the 2nd Circuit ruled Tuesday. The court referred Lee to a grievance panel, which considers possible discipline such as fines and suspensions.

"I am committed to adhering to the highest professional standards and to addressing this matter with the seriousness it deserves," Lee said in an emailed response to a question. She said she's unable to answer additional questions "given the confidential nature of the disciplinary proceedings."

Tuesday 05 December 2023 READ OUR E-PAPER

'Deepfake' audio evidence used in UK court to discredit Dubai dad

Doctored recording was intended to deliberately paint Emirates resident as a danger to his family

Byron James, a lawyer at Dubai firm Expatriate Law. Antonie Robertson / The National

Patrick Ryan
Feb 08, 2020

Listen In English | Listen in Arabic
Powered by automated translation

A 'deepfake' audio recording was used in a UK child custody battle in an effort to discredit a Dubai resident, it has been revealed.

Byron James, a lawyer in the emirate, said a heavily doctored recording of his client had been presented in court as evidence in a family dispute.

Business & Practice
Jan. 30, 2024, 8:55 PM GMT+1

NY Lawyer Faces Possible Sanctions for Citing Phony ChatGPT Case

By Sam Skolnik

Documents

Decision

- Use of ChatGPT by lawyer Jae Lee referred to grievance panel
- Two Manhattan lawyers fined $5,000 in June for ChatGPT use

An attorney in suburban New York City faces possible sanctions for using ChatGPT to generate a nonexistent state court decision she cited in a legal filing.

The conduct of Uniondale, New York lawyer Jae Lee of the JSL Law Offices fell "well below the basic obligations of counsel," the US Court of Appeals for the 2nd Circuit ruled Tuesday. The court referred Lee to a grievance panel, which considers possible discipline such as fines and suspensions.

"I am committed to adhering to the highest professional standards and to addressing this matter with the seriousness it deserves," Lee said in an emailed response to a question. She said she's unable to answer additional questions "given the confidential nature of the disciplinary proceedings."

Current legal standards on evidence

- 1. Open standards, no clear rules about who should state or contradict what at what time, and what threshold applies to both admissibility of evidence and the use of it
- 2. Judges generally assume that evidence is authentic, unless there are contraindications: (a) own observation and (b) the opposing party's position
- 3. Sanctions for submitting false evidence are often minimal

Effects AI in the Courtroom

- Some experts predict that in about five years, more than 90% of all digital content will be generate or manipulated to a greater or lesser extent by AI.
- Deepfake technology democratized; Generative AI increasingly widespread; manipulated content will be introduced in court wittingly or unwittingly
- Detection techniques are less then perfect and often give an ‘authenticity percentage’.

Effects AI in the Courtroom

- Should there be different standards for admissability for administrative, civil and criminal law cases?
- Judges will not be able to verify content on authenticity, but neither will the opposing party in court always be in a possition to do so (*in abstensia* rulings; temporary or permanent mental limitations, etc)

Effects AI in the Courtroom

- Possible increase in the role of experts & inequality of arms > expert paradox > only in weighty matters, normalization of ‘minor’ manipulations
- Archived material after death
- Evidence concerning possible virtual people (e.g. children) is difficult to refute.
- With some crimes, the suggestion is enough; initial judicial decision can be irreversible (eg custody case)

Effects AI in the Courtroom

- ‘I thought it was true’
- ‘I thought it was untrue’
- ‘Judge erred’

Changes needed to the legal regime ?

- Duty of care of lawyer/public prosecutor/professional party
- Greater role of police/judicial review
- Greater role of Forensics Institute
- Admissibility of source types (e.g. watermark)
- Better sanctioning
- Greater emphasis on supporting evidence

An overview of legal issues regarding the use of e-evidence on the Internet

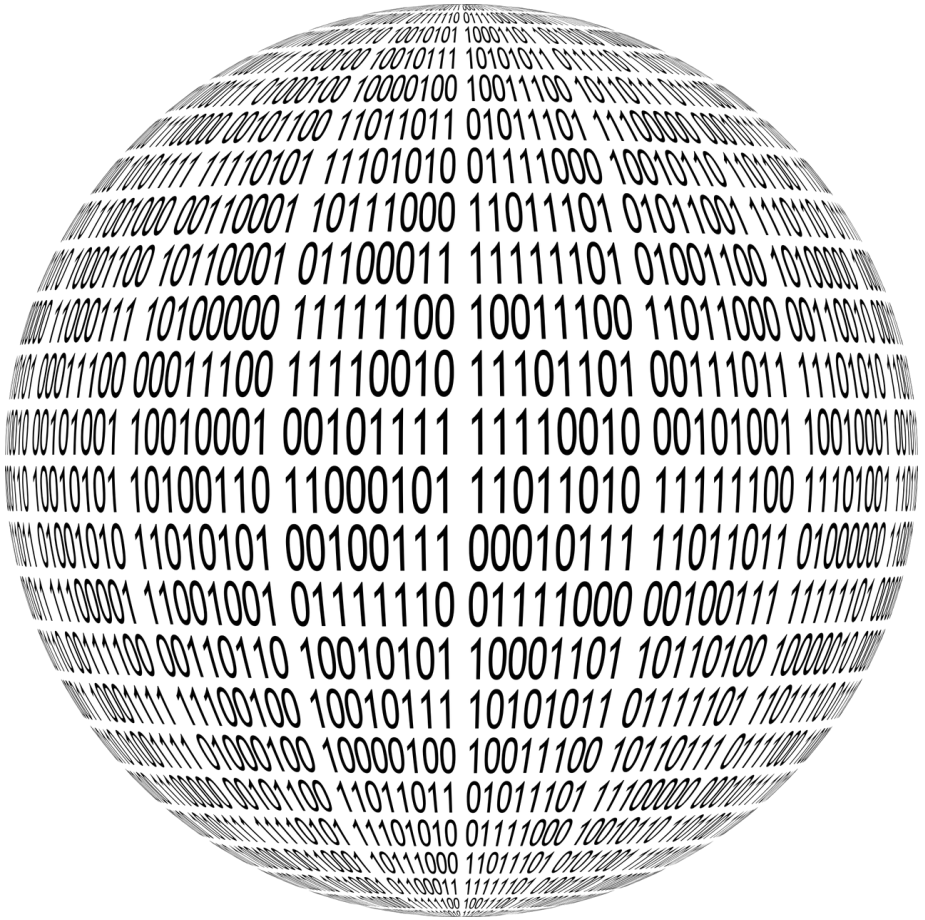
Marc van der Ham, eLaw, External-PhD candidate | Cracow – 26 May 2025

Universiteit Leiden
The Netherlands

Co-funded by the European Union

Index

1. Introduction
2. Jurisdictional challenges
3. MLA and cross-border cooperation
4. Admissiblity of e-Evidence in court
5. The right to a fair trial
6. Conclusion and looking forward



The Internet

1. The Internet is an abstraction, not an entity
   - Private networks, platforms, services and servers – not a singular place or authority

2. Digital evidence is always tied to a legal or technical actor
   - Specific server, specific jurisdiction, specific legal entity

3. There is no universal law of the Internet
   - Depends on server location, user location, and data controller location

4. Fundamental rights and freedoms apply equally
   - Regulating special investigatory powers with meaningful legal protections

Introduction

Electronic evidence and its role in criminal justice

What is electronic evidence in 2025

- Cloud-based communication metadata (timestamps, IP-addresses, user identifiers)
- Blockchain transaction forensics (analysis of cryptocurrency transactions)
- AI-enhanced OSINT (tools that scrape, analyse, and correlate public web and dark web content)

Current challenges of cross-border digital evidence

- Extraterritorial effect of investigatory powers and conflict of laws
- National challenges to mutual legal assistance due to rule of law concerns
- Legal vacuum due to the lack of data retention obligation

Explore jurisdictional, cooperative, admissibility and fair trial concerns

Jurisdictional challenges

The internet as a borderless domain leads to legal complications

Conflicts of law: who has the authority to collect, access or demand digital evidence?

- United States v. Microsoft Corp., 584 U.S. ___ (2018)
- CLOUD Act + agreements
- Law enforcement directive ((EU) 2016/680)
  - Only adequacy decision for the United Kingdom (based on Article 36 LED).

Ongoing initiatives to define digital sovereignty and jurisdiction

- EU e-Evidence package (
- 2nd additional protocol to the Budapest Convention (DNS, direct access, enforcement, expedited & emergency)
- UN cybercrime convention (territorial, nationality, passive, protective, enforcement)

MLA and cross-border cooperation

Traditional mutual legal assistance (MLA) mechanisms are slow and complex

Can the EU e-Evidence regulation and proposal deliver?

- Regulation (production and preservation orders, grounds for refusal, privileges & immunities, enforcement)
- Directive (legal representatives, duly equipped, execute orders, enforcement)
- Decentralized IT system (reference software by 18 August 2025, back-end, eCodex, testing).

Cooperation with non-EU countries: risks, limitations and reform efforts

- 2nd additional protocol to the Budapest Convention
- UN cybercrime convention
- EU adequacy decisions?
- Legal hacking authority in The Netherlands and international aspects related to sovereignty.

Admissibility of electronic evidence

Evidentiary laws are a domestic issue

Criteria for admissibility are authenticity, reliability, integrity

- Chain of custody in digital contexts
- Jurisdictional divergences: differing standards across Member States
- The principle of mutual trust is a cornerstone

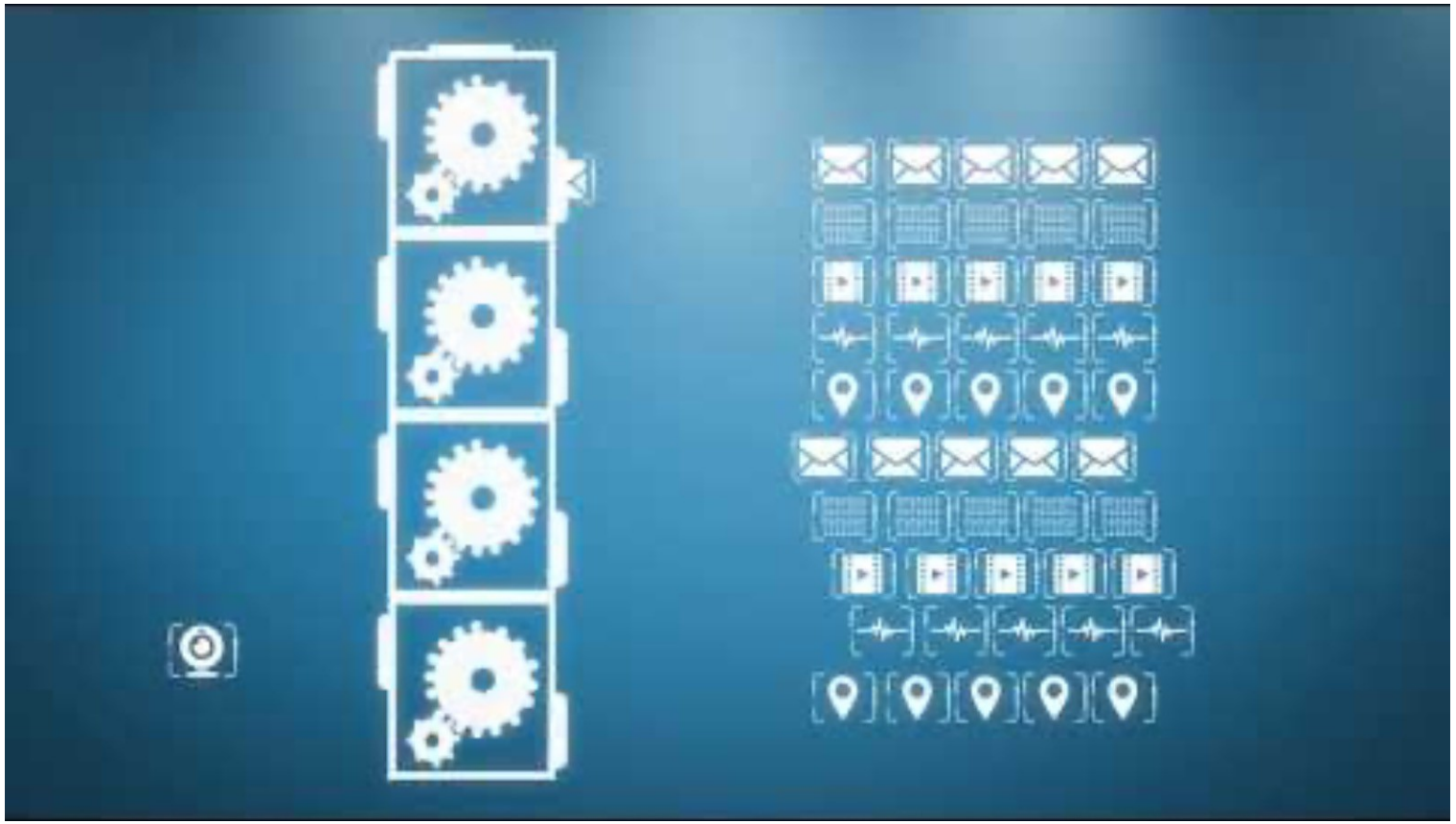
Use of AI tools and automation in evidence gathering

- Challenges for authentication and expert interpretation
- Access to evidence
- Digital forensic standards

Admissibility of electronic evidence

Category	Key concept	Example / challenge
Legal criteria	**Authenticity** – Is the evidence genuine?	Digital signatures, metadata verification, hash checks
	Reliability – Was it collected/stored properly?	System accuracy, automated logs, functioning software
	Integrity – Has the evidence been altered?	Digital chain of custody, access records, file tampering
Technical issues	**Chain of custody** – Document every access/transfer	Virtual access logs, forensic imaging, tool verification
	Jurisdictional divergence – National rules differ	Surveillance laws, admissibility standards, judicial oversight levels
	AI & automation – Machine-generated evidence lacks transparency	Who is the “witness”? Algorithmic bias, explainability
	Cross-border access – Legal and privacy barriers	GDPR, MLATs, encrypted data on foreign/cloud servers
Standardization needs	**Lack of universal forensics standards**	Voluntary ISO/ENFSI guidelines, no binding methods for imaging or metadata handling

Admissibility of electronic evidence



The right to a fair trial

Modern interpretations of traditional concepts

Ensuring equality of arms:

- Can defence teams access, challenge, and verify evidence?
- Transparency and disclosure – especially with AI and automated tools?
- Potential for digital evidence to prejudice or mislead

Strategies to safeguard due process in technology-heavy prosecutions:

- Challenges for authentication and expert interpretation
- Digital forensic standards
- Judicial oversight and *meaningful* consequences

The right to a fair trial

To address recurring errors and uncertainty in digital forensic investigations, a practical, technique-based knowledge base—**SOLVE-IT**—has been proposed to systematically document weaknesses and mitigations. Inspired by MITRE ATT&CK, it supports quality assurance, error reduction, and confidence in digital evidence by mapping out detailed forensic processes.

ELSEVIER Journal homepage: www.elsevier.com/locate/fsidi

DFRWS EU 2025 - Selected Papers from the 12th Annual Digital Forensics Research Conference Europe

SOLVE-IT: A proposed digital forensic knowledge base inspired by MITRE ATT&CK

Christopher Hargreaves [a,b,*], Harm van Beek [c,d], Eoghan Casey [e]

[a] Department of Computer Science, University of Oxford, United Kingdom
[b] HARGS Solutions Ltd, Oxford, United Kingdom
[c] Netherlands Forensic Institute, The Hague, the Netherlands
[d] Department of Computer Science, Open Universiteit, Heerlen, the Netherlands
[e] Ecole des Sciences Criminelles, University of Lausanne, Batochime, 1015, Lausanne, Switzerland

ARTICLE INFO

Keywords:
Digital forensic techniques
Digital forensic science
Quality assurance
Error-focused datasets
AI applications

ABSTRACT

This work presents SOLVE-IT (Systematic Objective-based Listing of Various Established (Digital) Investigation Techniques), a digital forensics knowledge base inspired by the MITRE ATT&CK cybersecurity resource. Several applications of the knowledge-base are demonstrated: strengthening tool testing by scoping error-focused data sets for a technique, reinforcing digital forensic techniques by cataloguing available mitigations for weaknesses (a systematic approach to performing Error Mitigation Analysis), bolstering quality assurance by identifying potential weaknesses in a specific digital forensic investigation or standard processes, structured consideration of potential uses of AI in digital forensics, augmenting automation by highlighting relevant CASE ontology classes and identifying ontology gaps, and prioritizing innovation by identifying academic research opportunities. The paper provides the structure and partial implementation of a knowledge base that includes an organised set of 104 digital forensic techniques, organised over 17 objectives, with detailed descriptions, errors, and mitigations provided for 33 of them. The knowledge base is hosted on an open platform (GitHub) to allow crowdsourced contributions to evolve the contents. Tools are also provided to export the machine readable back-end data into usable formats such as spreadsheets to support many applications, including systematic error mitigation and quality assurance documentation.

1. Introduction

The growing awareness of weaknesses in digital forensic investigations has expanded requirements for quality assurance. Missed, mishandled, and misinterpreted digital evidence can result in it being dismissed, scarce resources being wasted, and trust in digital evidence being diminished. To reduce these risks, standards bodies are promoting systematic approaches to mitigate errors and uncertainty in digital evidence, but the field lacks a practical solution to implement these requirements.

Many digital forensic process models have been proposed at different levels of abstraction that offer advantages for teaching and discussion at a high-level. However, other fields that need to model specific technical approaches have adopted a complementary knowledge-base approach e.g.

This paper demonstrates that a similar knowledge base in digital forensics could have many benefits in areas such as creating error-focused data sets, quality assurance, and systematic mitigation of errors and uncertainty. Documenting processes in more detail than high-level topic names can provide solutions in these areas.

A recent paper (Hargreaves et al., 2024b) provided a deconstruction of 'internal processes' within monolithic digital forensic tools and showed the dependencies between them, along with examples of errors that can occur at each stage. This paper extends that recent paper and considers the overall digital forensic process rather than just monolithic digital forensic tools. It takes a bottom-up approach to mitigating weaknesses within all aspects of a digital forensic investigation, taking a technique-based view of digital forensics. Incorporating weaknesses and mitigations, and providing tools for applying the knowledge base to

Conclusions

1. Legal and ethical imperative to modernize legal frameworks (interplay between different disciplines)
2. Normative integration of criminal evidence gathering (Prof. Dr. M. Hirsch Ballin)
   - The integrity of the proceedings
   - The presumption of innocence
   - The protection of private life
   - Proportionality
3. Re-design of public private cooperation

m.j.m.van.der.ham@law.leidenuniv.nl

Universiteit
Leiden
The Netherlands