ERA

#DIGITALISATION and #ARTIFICIALINTELLIGENCE in Criminal Justice

Internet Fundamentals, Digital Investigations and AI

Prague, 12-13 June 2025

FACE-TO-FACE

EXCELLENCE IN EUROPEAN LAW

Speakers and chairs

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

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

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

Andrea Cruciani, Judge, Court Martial, Naples

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

Tomáš Gřivna, Lawyer, Advokátní kancelář Gřivna & Šmerda; Professor, Criminal Law, Charles University, Prague

Antonín Mokrý, Lawyer; Chair, International Law Committee; Past President of CCBE, Prague

Serena Quattrocolo, Professor, Italian and European Criminal Procedure, University of Turin

Martin Richter, Lawyer, Richter & Léko advokáti; Assistant Professor, Criminal Law, Charles University, Prague

David Silva Ramalho, Defence Lawyer, Morais Leitão, Galvão Teles, Soares da Silva & Associados; Lecturer, Faculty of Law, University of Lisbon

Co-funded by
the European Union

Key topics

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

Language
English

Event number
324DT07

Organisers
ERA (Laviero Buono) in cooperation with the Czech Bar Association

CZECH BAR
ASSOCIATION

european.law

#DIGITALISATION and #ARTIFICIALINTELLIGENCE in Criminal Justice

Thursday, 12 June 2025

09:00 Arrival and registration of participants

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

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

Chair: Laviero Buono

09:35 **Using open source intelligence to gather evidence online**

- Understanding the Internet and associated technology
- Effective use of the Internet as an investigative investigation tool
- Internet protocols (IPs) and proxy servers
- Search engines, meta browsers and deep web
- Open Source Intelligence (OSINT) links

Philip Anderson

10:30 Discussion

10:45 Break

11:15 **Open source tools, computer forensics in the Cloud**

- Geo-location tools for social media and photos
- Tracing domain name owners, origin of an email and blacklist checks
- Investigating Web 2.0 – social networking, blogs and online gaming
- Protecting your privacy when investigating online

Seanpaul Gilroy

12:15 Discussion

12:30 Lunch

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

Chair: Philip Anderson

13:30 **An overview of the defence rights-related issues regarding the use of e-evidence collected on the internet**
Tomáš Gřivna & Martin Richter

14:15 Discussion

14:30 **Using electronic evidence and artificial intelligence in criminal investigations and presenting it in court**

- The importance of the chain of custody in handling evidence
- Trial considerations: methods of presentation and admissibility tests

Linda Bertram

15:15 Discussion

15:30 Break

16:00 **Digital tech as tool to commit crimes**

- Cyber patrolling and cyber investigations
- Tackling the illegal trade on the darkweb
- Case studies

David Ramalho Silva

Objective

This seminar addresses various challenges linked to digitalisation that judges, prosecutors and lawyers in private practice working in the field of EU criminal justice will have to face in the years ahead. Some of these challenges such as the exchange of electronic evidence, videoconferencing, use of open source intelligence, artificial intelligence, digital technology, etc. are here to stay and will become the new normal.
This event is part of a large-scale project sponsored by the European Commission entitled ‘Judicial training to prepare criminal justice professionals for #digitalisation and #artificialintelligence’. It consists of 12 seminars taking place in various EU cities over the period 2024-2027.

Who should attend?

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

Czech Bar Association
Palác Dunaj, Auditorium 1st floor
Národní 10, 110 Prague

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.

16:30 Discussion

16:45 End of first day

19:30 Dinner offered by the organisers

Friday, 13 June 2025

PART III: VIDEOCONFERENCING AND ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

Chair: David Ramalho Silva

09:30 **Presenting evidence in court: e-files, videoconferences and remote trials**

- Remote trials during and after the pandemic
- E-files
- Witness videoconferencing
- Assessing evidence, the impact of artificial intelligence

Andrea Cruciani

10:15 Discussion

10:30 Break

Chair: Andrea Cruciani

11:00 **The nexus between artificial intelligence and criminal law**
David Ramalho Silva

11:30 **The impact of the AI Act on the applications of AI to criminal justice**
Serena Quattrocolo

12:15 Discussion

12:30 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 93737 323
E-Mail: jreitz@era.int

Apply online for “#Digitalisation and #AI in Criminal Justice”:
www.era.int/?133199&en

This programme has been financed by the European Union

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

Application

#DIGITALISATION and #AI in Criminal Justice

Prague, 12-13 June 2025 / Event number: 325DT07

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), 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 15 March 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. No discounts are applicable.

Travel and Accommodation Expenses

5. Participants will receive a fixed contribution towards their travel expenses and are asked to book their own travel. The condition for payment of this contribution is to sign all attendance sheets at the event. 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.
6. Travel costs from outside the Czech Republic: 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.
7. For inter-Member States return journeys between 50 and 400 km (AT, DE, FR, HR, PL, RO, SI, SK) please consult p.11 on https://era-comm.eu/go/unit-cost-decision-travel
8. For those travelling within the Czech Republic, 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
9. Accommodation costs: international participants travelling more than 50km one-way will receive a fixed contribution of €107 per night for up to two nights' accommodation. National participants travelling more than 50km one way will receive a fixed contribution of €107 per night for max one night accommodation. For more information, please consult p.13 on https://era-comm.eu/go/unit-cost-decision-travel
10. Successful applicants will be sent the relevant claim form and information on how to obtain payment of the contribution to their expenses. Please note that no payment is possible if the registered participant cancels their participation for any reason or does not attend both days of the event.

Participation

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

Accommodation

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

Apply online for "#Digitalisation and #AI in Criminal Justice":
www.era.int/?133199&en

Venue

Czech Bar Association
Palác Dunaj, Auditorium 1st floor
Národní 10, 110 00 Prague

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

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*)

Technical Issues and basic understanding of the Internet architecture and concepts

Using open-source intelligence to gather evidence online

PHILIP ANDERSON

ERA | PRAGUE, 12-13 JUNE 2025

Co-funded by the Justice Programme of the European Union

Outline

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

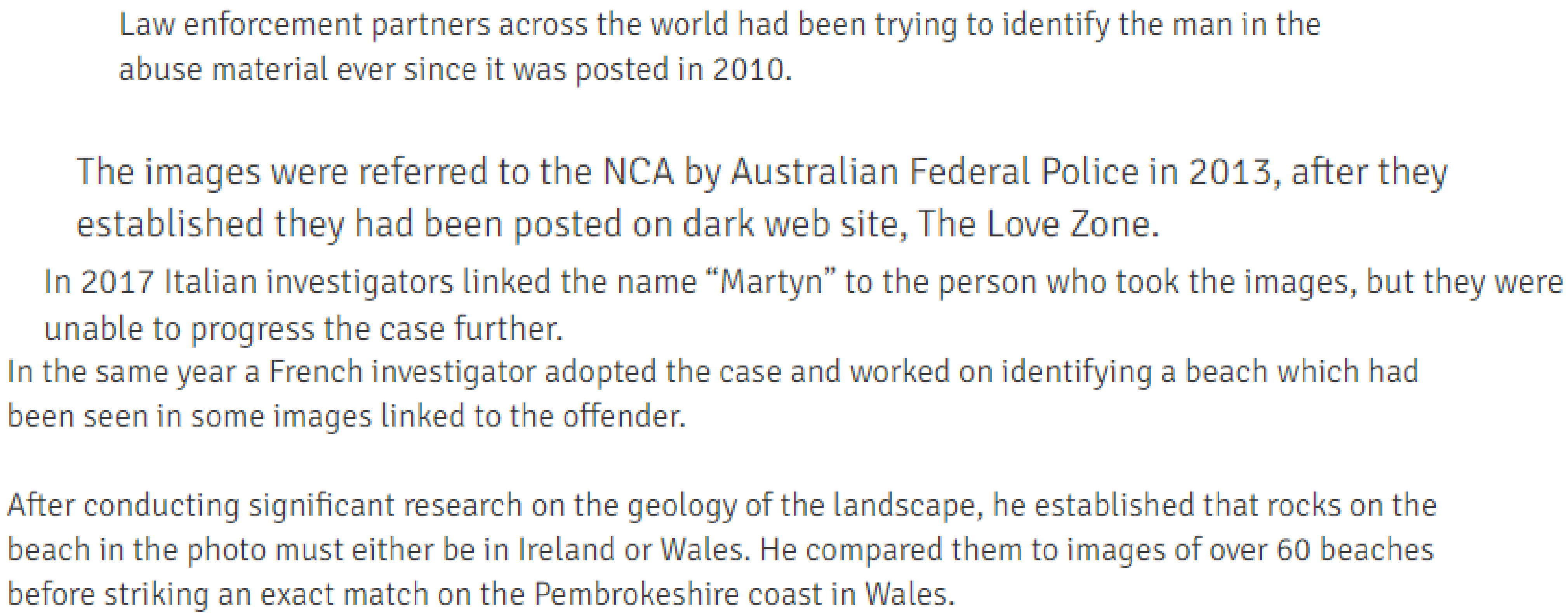
Cybercrime landscape – IOCTA 2024*

- Child Sexual Abuse Material (CSAM)
  - AI-assisted, AI-altered and AI-generated.
  - End-to-end encrypted (E2EE) communication platforms.
- Romance Fraud
- Phishing and social engineering (Phishing as a Service)
  - Phishing kits are widely available, lowering the level of organisation and technical expertise
- Crime as a Service (CaaS) – increasing due to AI tools and services.
- Ransomware as a Service (RaaS) – small to medium sized businesses.
- The dark web an enabler of cybercrime
  - Cryptocurrency favoured – altcoins

* IOCTA 025 out very soon.

Source: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

Example



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

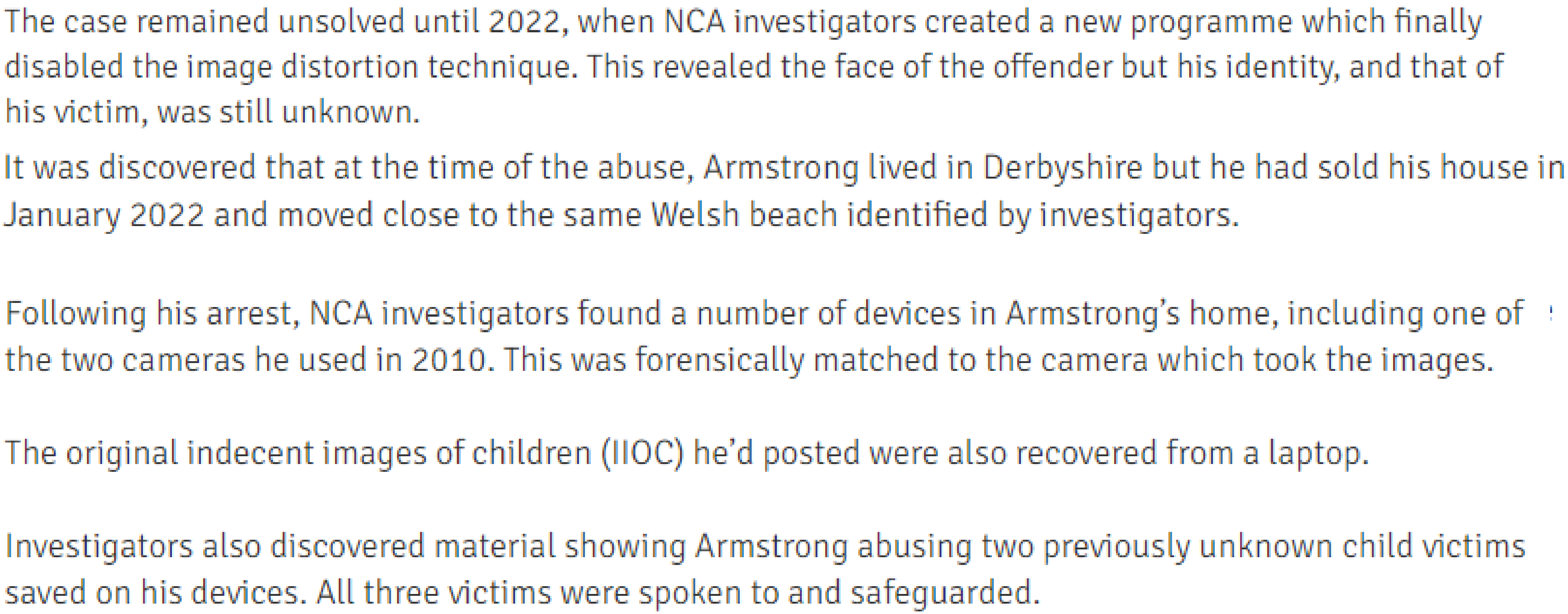
The images were referred to the NCA by Australian Federal Police in 2013, after they established they had been posted on dark web site, The Love Zone.

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

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

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

Example



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

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

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

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

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

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

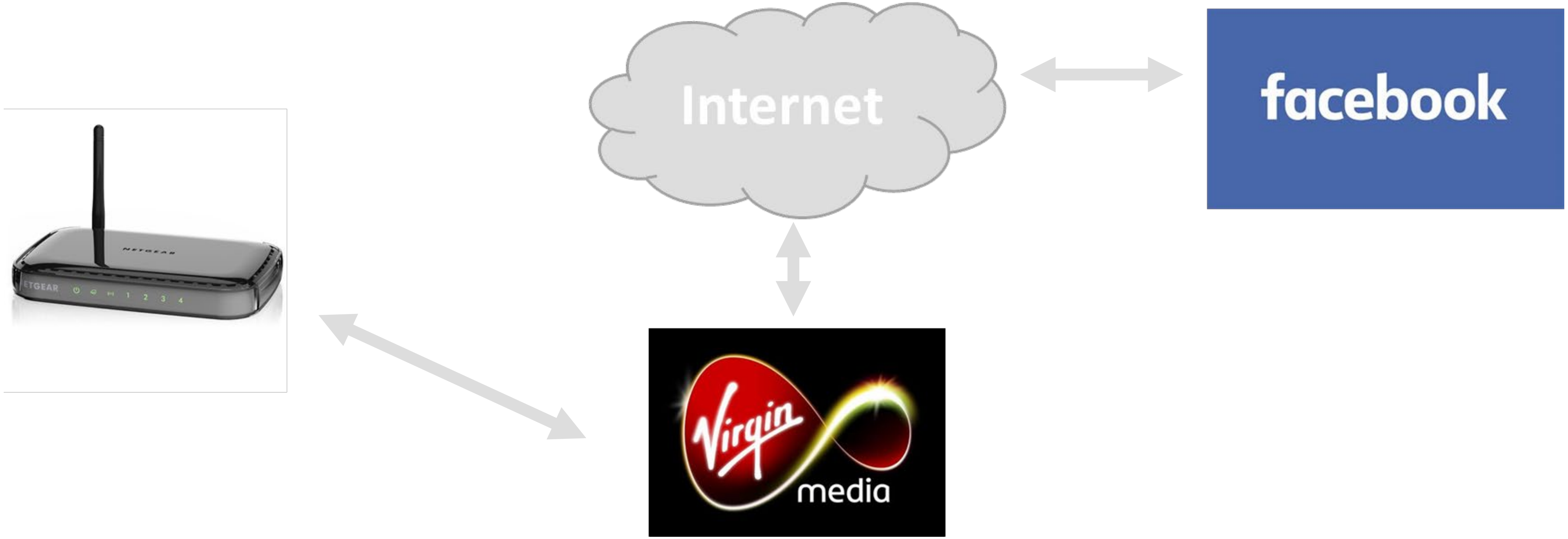
#1

Understanding the Internet and associated technologies

How does it work.

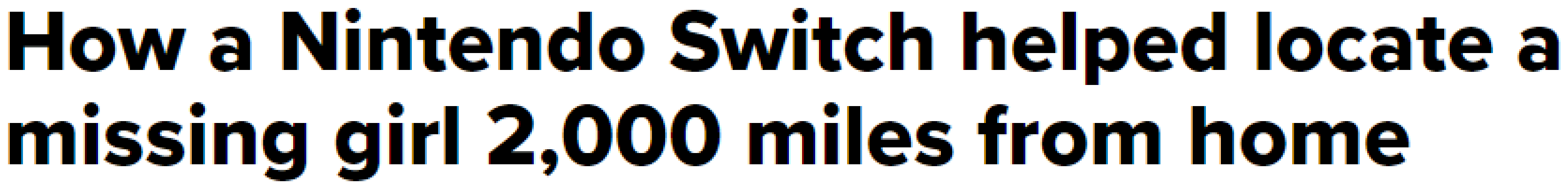
- Every device connected to the Internet is assigned an IP (Internet Protocol) address.
- Every device speaks the same language.
- Every device has a unique IP address.
- To communicate, devices need to exchange addresses.
- This address could be used to trace an online activity back to a device.

How does it work… Infrastructure

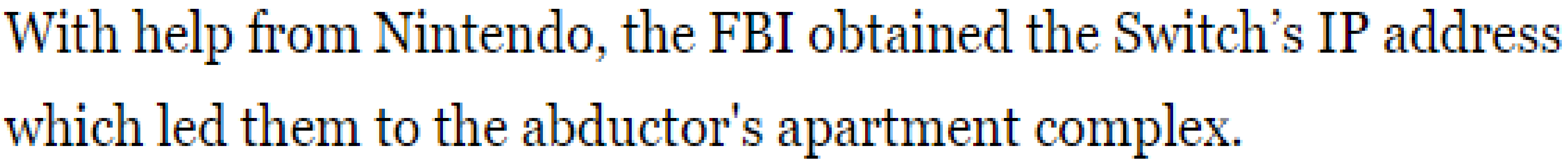


Internet Service Provider (ISP)

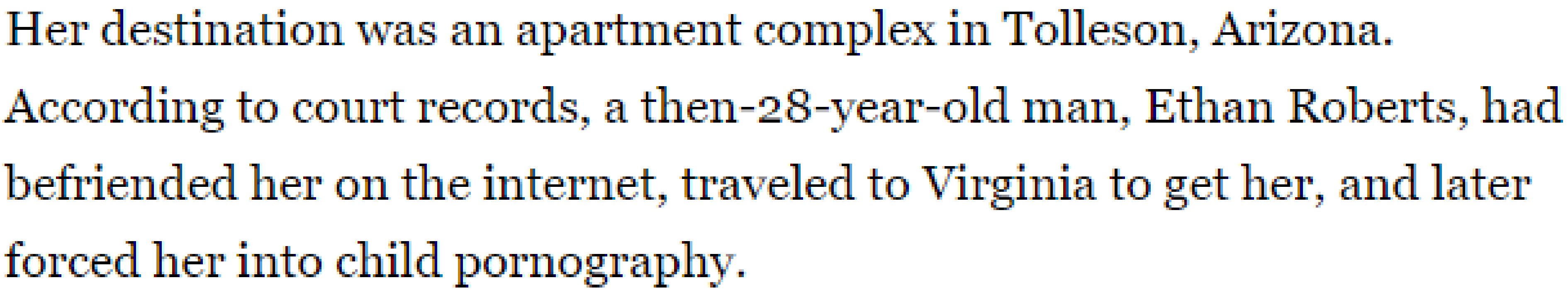
Example



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



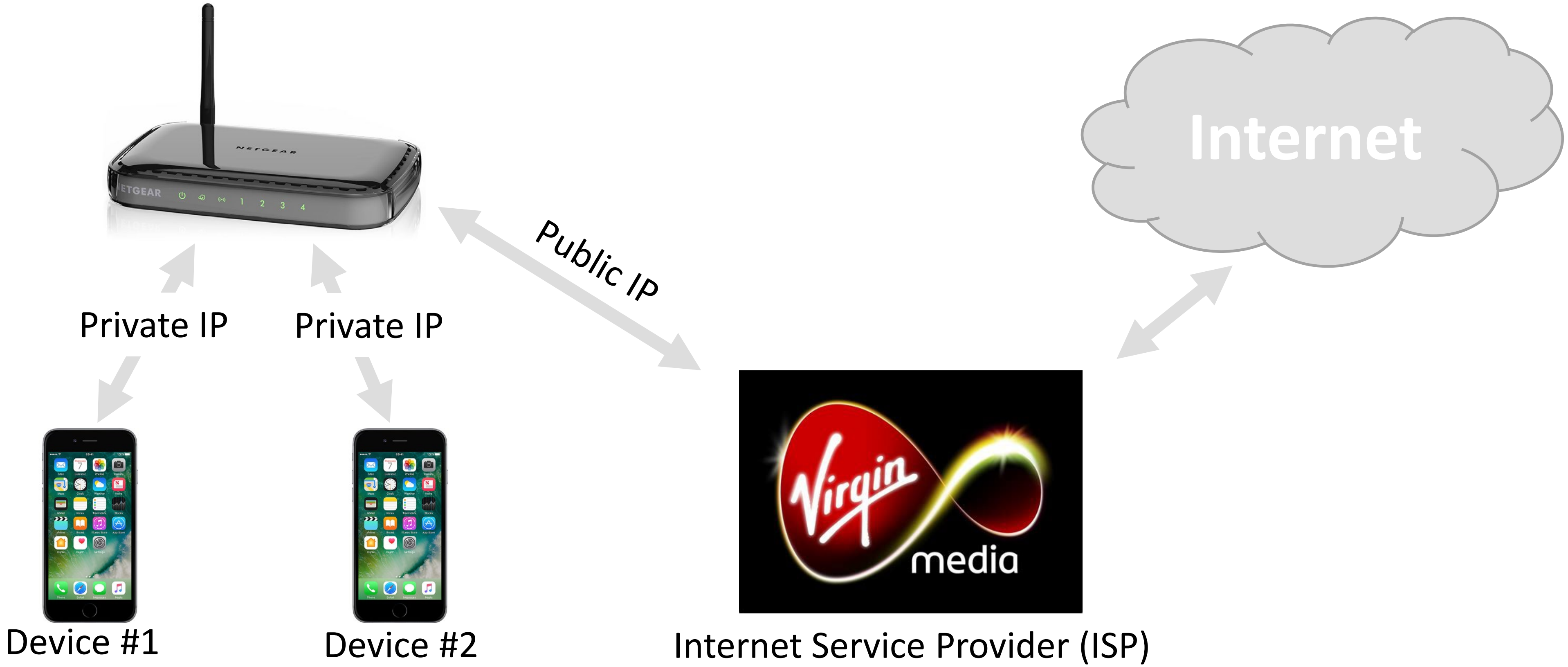
With help from Nintendo, the FBI obtained the Switch's IP address which led them to the abductor's apartment complex.



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

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

How does it work… Public and Private IP



Internet

Public IP

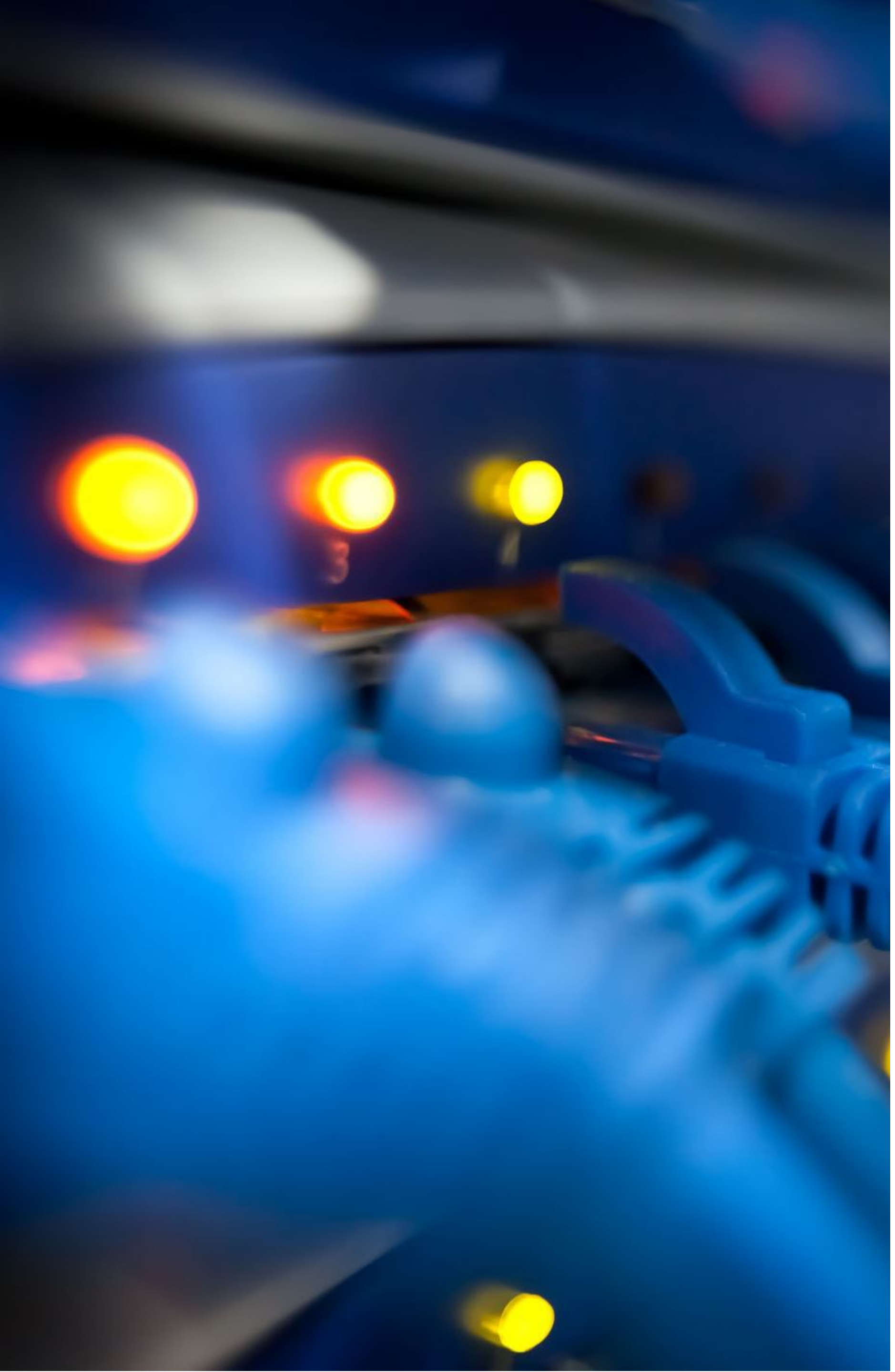
Private IP

Private IP

Device #1

Device #2

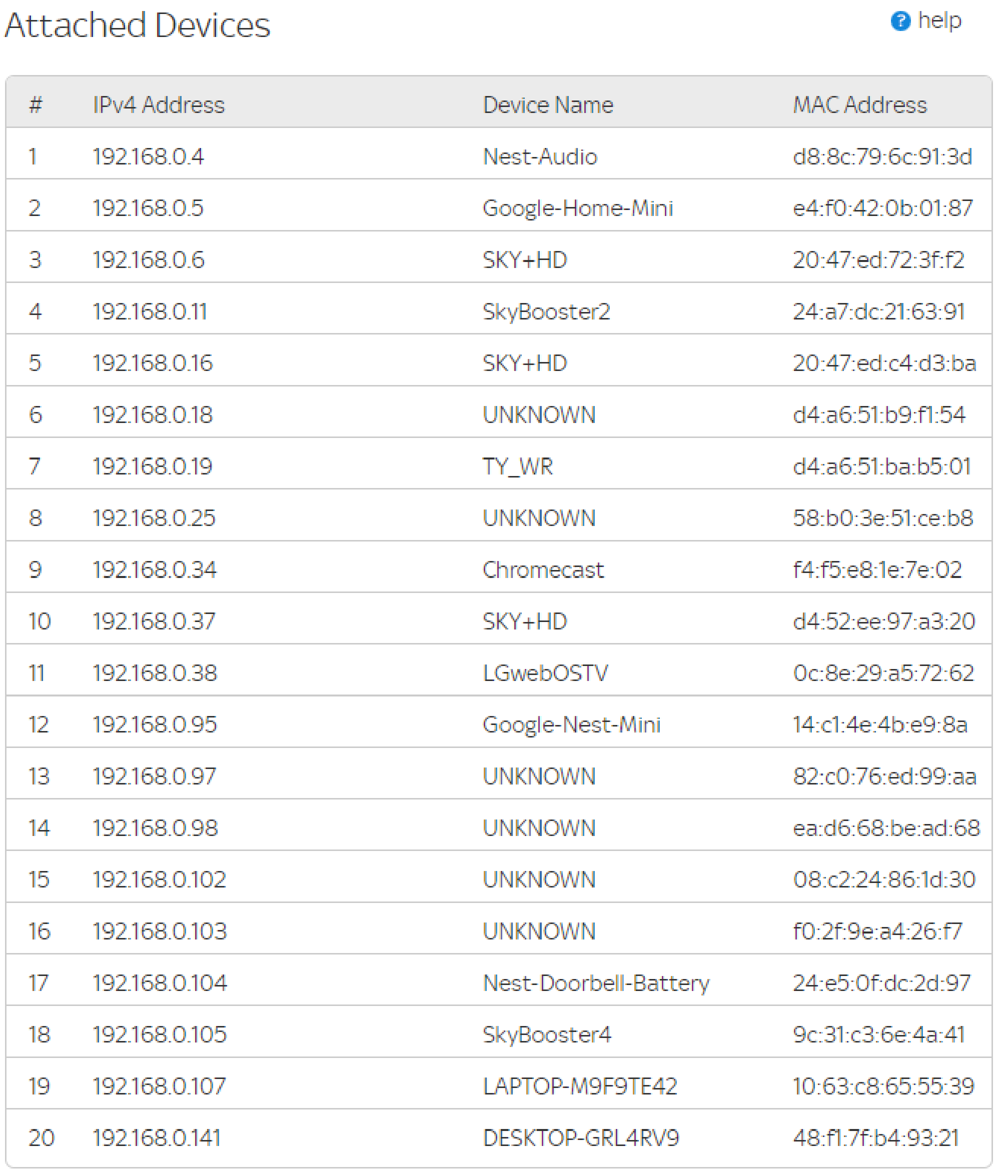
Internet Service Provider (ISP)



How does it work…Public and Private IP.

- Public IP – assigned to the router by the ISP
  - Outward-facing - identifies you to the rest of the Internet
- Private IP – assigned to the device by the router
  - Private network – communicate with other devices on that network

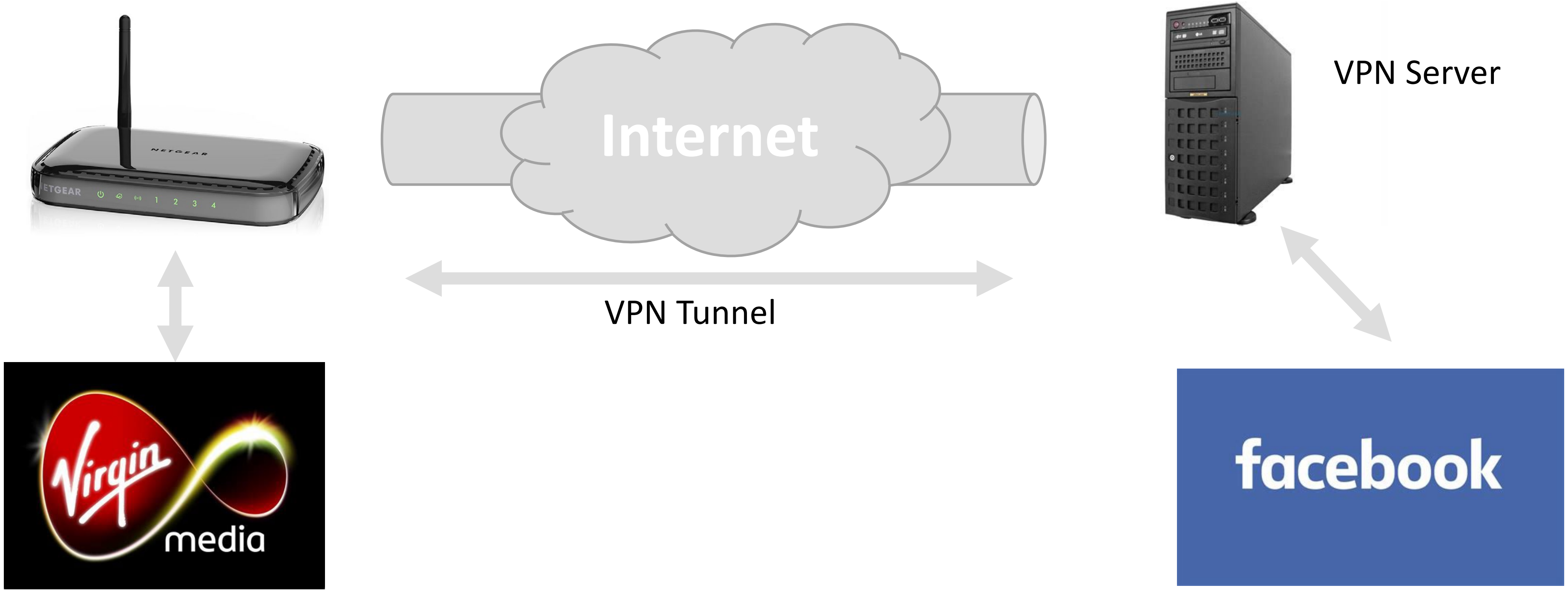
How does it work… Public and Private IP



Attached Devices

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

How does it work… Privacy | Anonymity



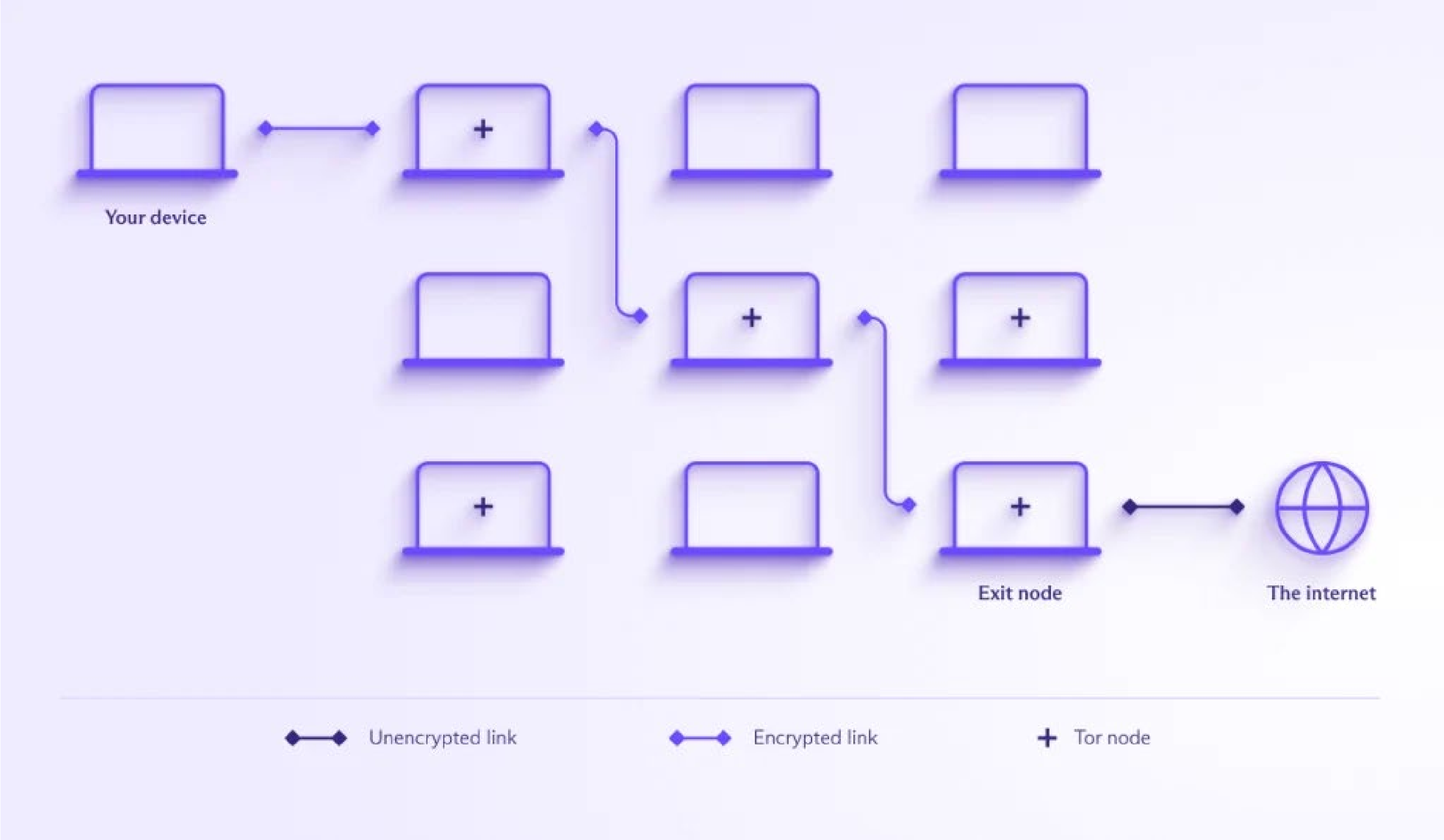
VPN Server

VPN Tunnel

Internet Service Provider (ISP)

VPN IP

How does it work… Onion Routing Network (TOR)



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

Spotlight… Apps - Telegram

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

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

Spotlight… Telegram

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

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

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

Spotlight… Telegram

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

Link to other social media accounts.

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

#2

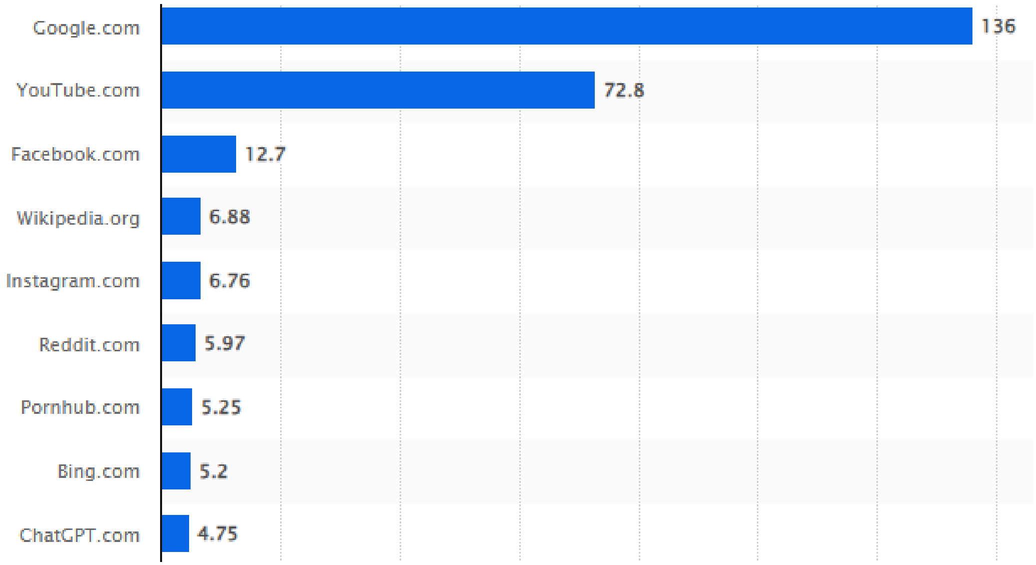
Effective use of the Internet as an investigation tool

Investigations…

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

Investigations… Social media

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

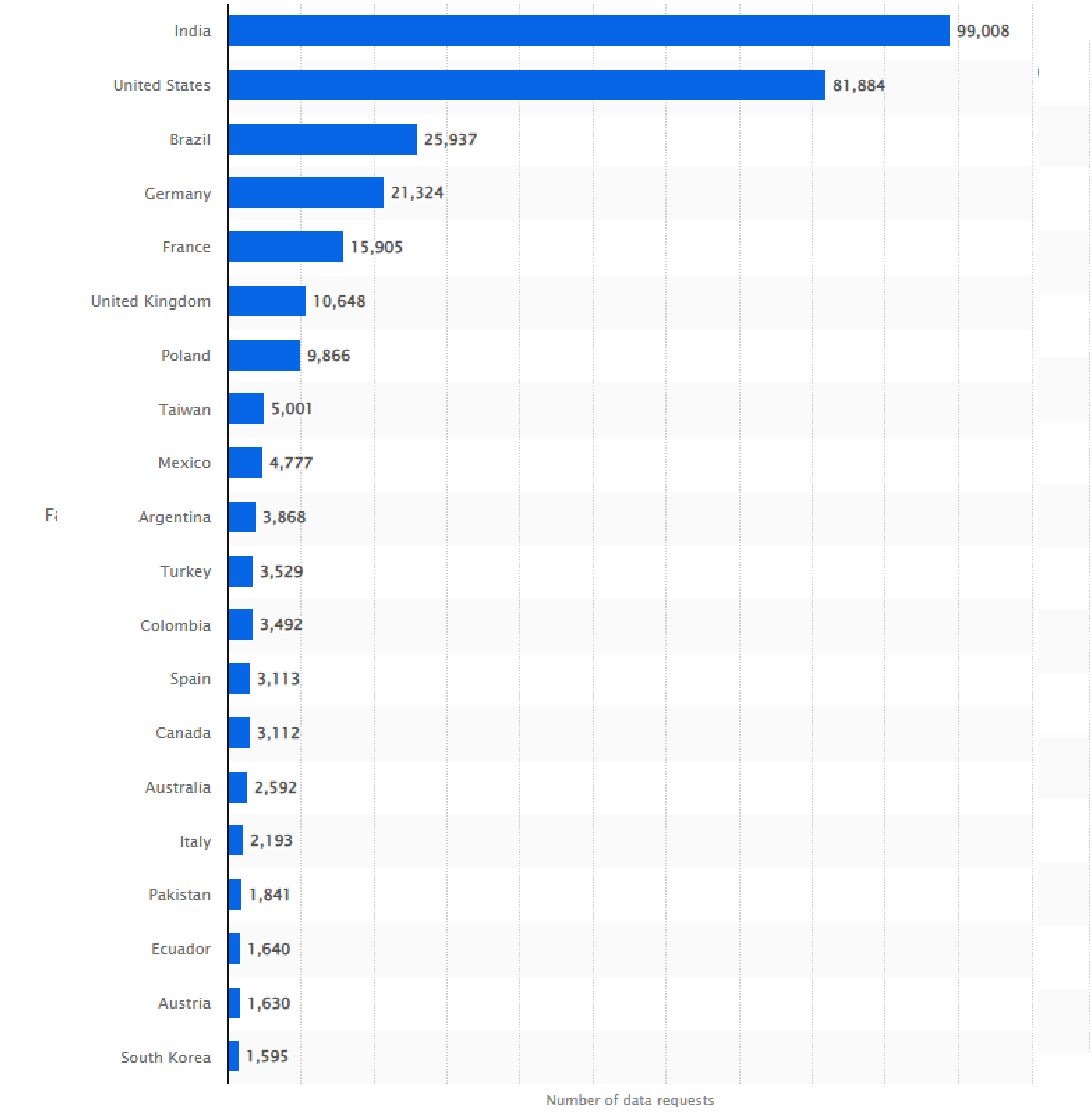


Most popular websites worldwide as of November 2024, by total visits(in billions)

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

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

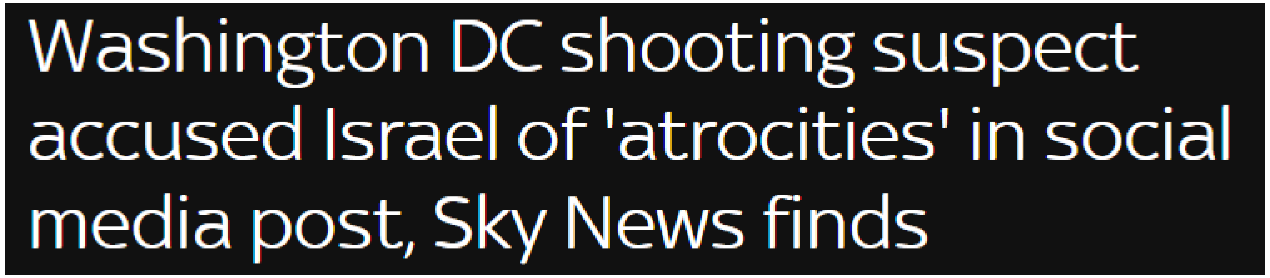
[2] Statista - https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/



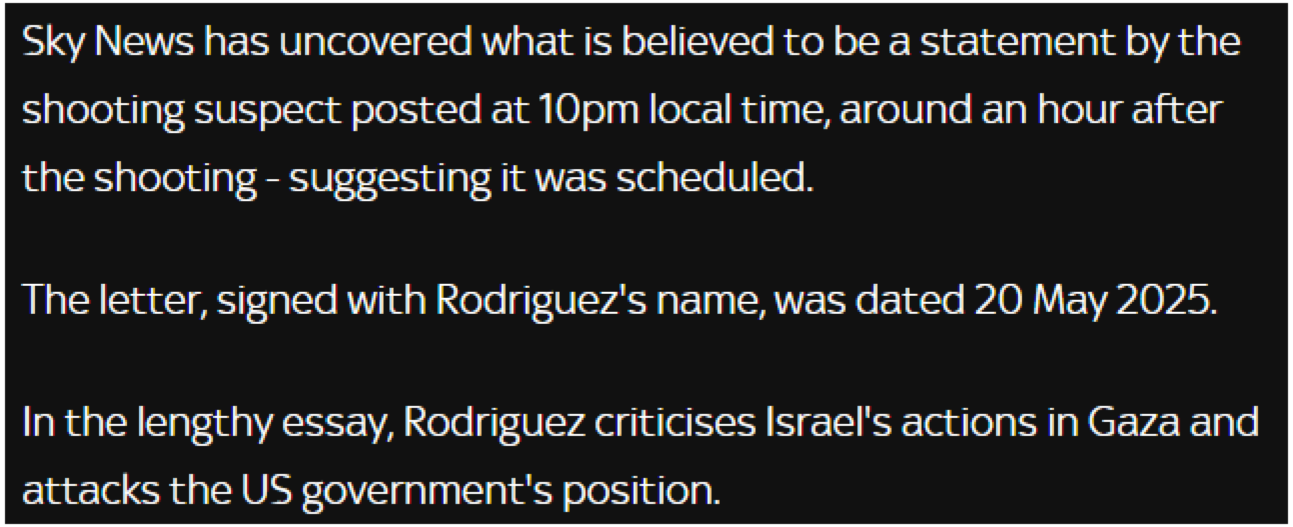
#1 Most popular social networks worldwide as of February 2025, ranked by number of monthly active users. Source: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

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

Investigations… Social Media Posts



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



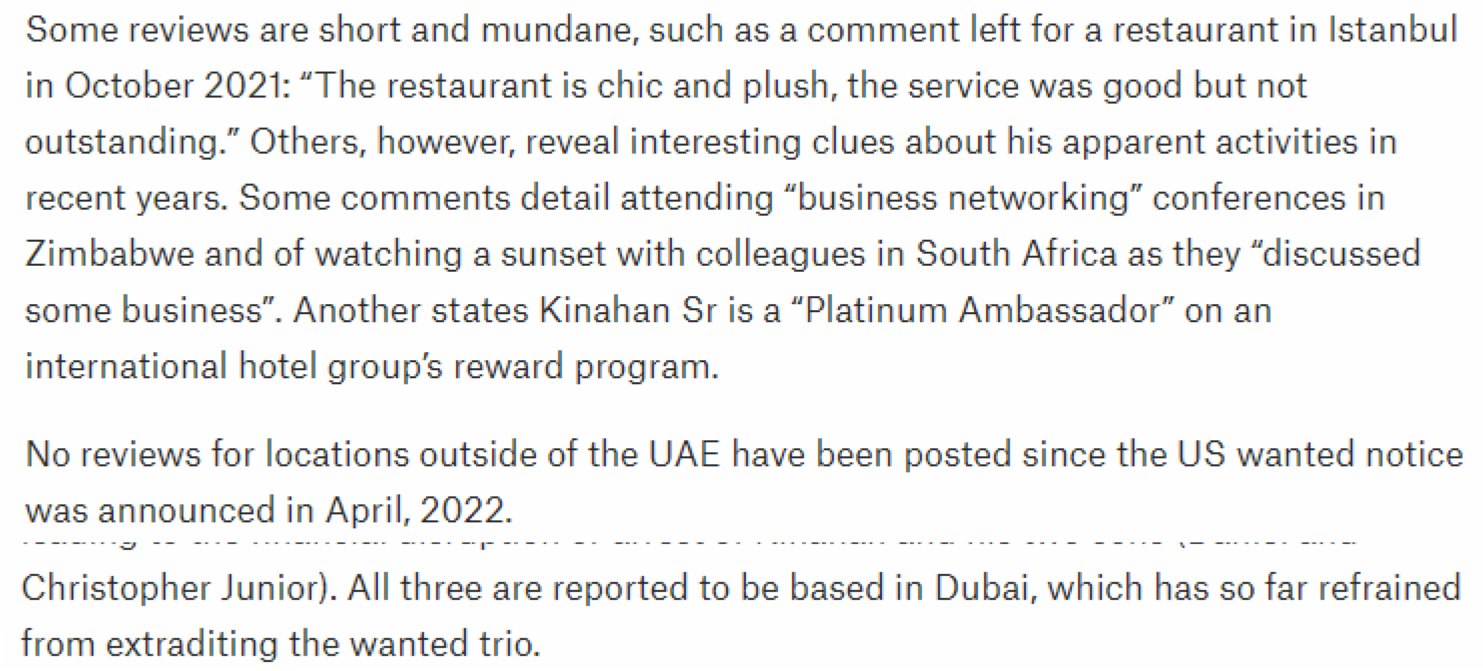
Sky News has uncovered what is believed to be a statement by the shooting suspect posted at 10pm local time, around an hour after the shooting - suggesting it was scheduled.

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

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

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

Investigations… Google Reviews



Some reviews are short and mundane, such as a comment left for a restaurant in Istanbul in October 2021: “The restaurant is chic and plush, the service was good but not outstanding.” Others, however, reveal interesting clues about his apparent activities in recent years. Some comments detail attending “business networking” conferences in Zimbabwe and of watching a sunset with colleagues in South Africa as they “discussed some business”. Another states Kinahan Sr is a “Platinum Ambassador” on an international hotel group’s reward program.

No reviews for locations outside of the UAE have been posted since the US wanted notice was announced in April, 2022.

Christopher Junior). All three are reported to be based in Dubai, which has so far refrained from extraditing the wanted trio.

Source: https://www.bellingcat.com/news/2024/03/30/kinahan-cartel-wanted-narco-boss-exposes-whereabouts-by-posting-google-reviews/

Other Investigations…

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

Investigations… considerations

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

Investigations… Legislation (UK)

- Human Rights Act 1998 (HRA)
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Investigatory Powers Regulations 2018 (IPA)
- Police and Criminal Evidence Act 1984 (PACE)
- Criminal Procedure and Investigations Act 1996 (CPIA)
- Online Safety Act 2023 (OSA)

Investigations… Ethics

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

#3

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

The Internet…

- Surface web
  - The section of the Internet that is being indexed by search engines
  - 2.25 billion pages indexed[1]
  - 175 zettabytes of data[2]
  - Accessed via ‘standard’ browsers - Chrome, Mozilla Firefox, Opera, etc.
- Deep web
  - Not indexed
  - Accessed via username and passwords
  - Some data out of the Deep web may be picked up by search engines in the case of a data breach.
  - Accessed via ‘standard’ browsers - Chrome, Mozilla Firefox, Opera, etc.

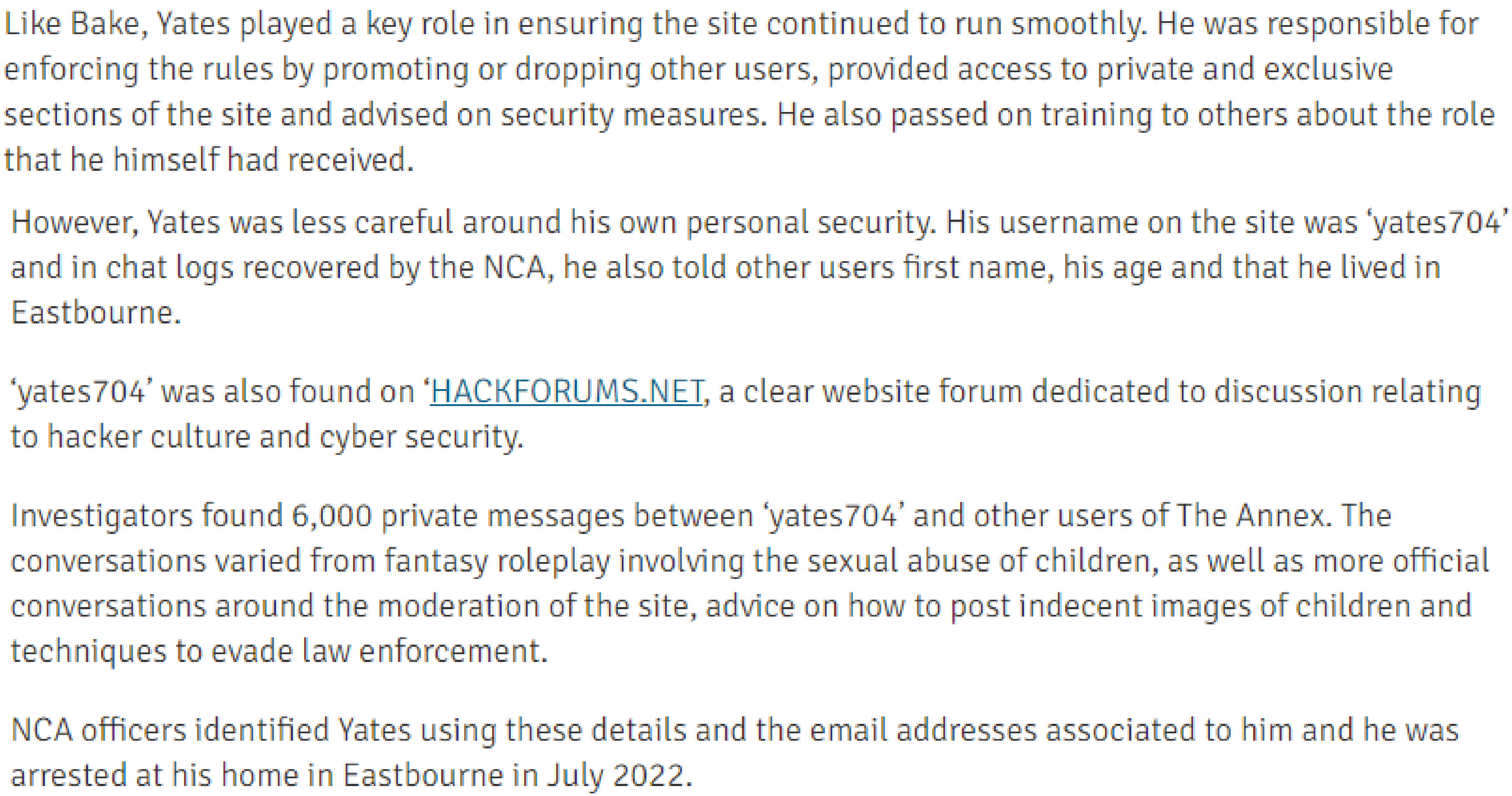
1: Source - https://www.ipxo.com/blog/how-big-is-the-internet/

2: Source: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

The Internet…

- Dark web
  - Challenging environment
  - Anonymous browsing network consists of thousands of relays.
  - Indexing is now happening (proxied TOR sites – TOR2WEB)
  - Accessed via ‘specialist’ browsers – TOR Browser.

Example



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

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

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

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

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

impres

fore be

orcement detection,

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

Open Source… Methods

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

Methods… Information Sources

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

Methods… Information Gathering

1. OSINT Framework - http://osintframework.com/
2. OSINT Tools - https://www.osinttechniques.com/osint-tools.html
3. OSINT.Link - https://osint.link/

Methods… Information sources

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

Methods… Tools

- Remember
  - Evidential integrity
  - Evidential chain of custody
  - No digital devices have been seized or examined.

- Capturing the (online) evidence
  - Web capture tools
    - Searching
    - Collecting and documenting
      - Timestamps and hashing
    - Audit trail
    - Secure cloud storage
    - Reporting

#4

Using open source intelligence to gather evidence online

Open Source… Case Studies - Bellingcat

- Two Europol StopChildAbuse Images Geolocated - https://www.bellingcat.com/news/2019/12/05/two-europol-stopchildabuse-images-geolocated-part-i-madagascar/
- Google maps photos
- Google Earth imagery
- Geographic and demographic data examined
- Timeline analysis – tropical storms

- Skripal Poisoning Suspect Dr. Alexander Mishkin, Hero of Russia - https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia/
- Passport photos
- Online biographical data
- Locations searches
- Telephone numbers

Open Source… OpenGuessr

https://openguessr.com/

Open Source…

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

Thank you

Questions?

Philip Anderson

Assistant Professor

Dept. Computer & Information Sciences,
Northumbria University, UK
Email: philip.anderson@northumbria.ac.uk

OPEN SOURCE TOOLS, COMPUTER FORENSICS IN THE "CLOUD"

#DIGITALISATION and #ARTIFICIALINTELLIGENCE in Criminal Justice

Internet Fundamentals, Digital Investigations and AI

Seanpaul Gilroy

Senior Digital Forensic Investigator

Co-funded by

the European Union

About Me

- Senior Digital Forensic Investigator at Northumbria Police
  - Manage a team of Digital Forensic Investigators & technicians
  - Support Investigators with Digital Forensic Strategies
  - Based in Newcastle Upon Tyne, England
  - Worked in the field of Digital Forensics for 11 years
- Deliver training inputs to both new and existing police officers on a regular basis:
  - Seizure of digital evidence and best practice
  - Analysis of digital evidence & digital forensic opportunities

What will we discuss?

🕵️ Overview of open source Investigations

🔏 Protecting your privacy during open source investigations

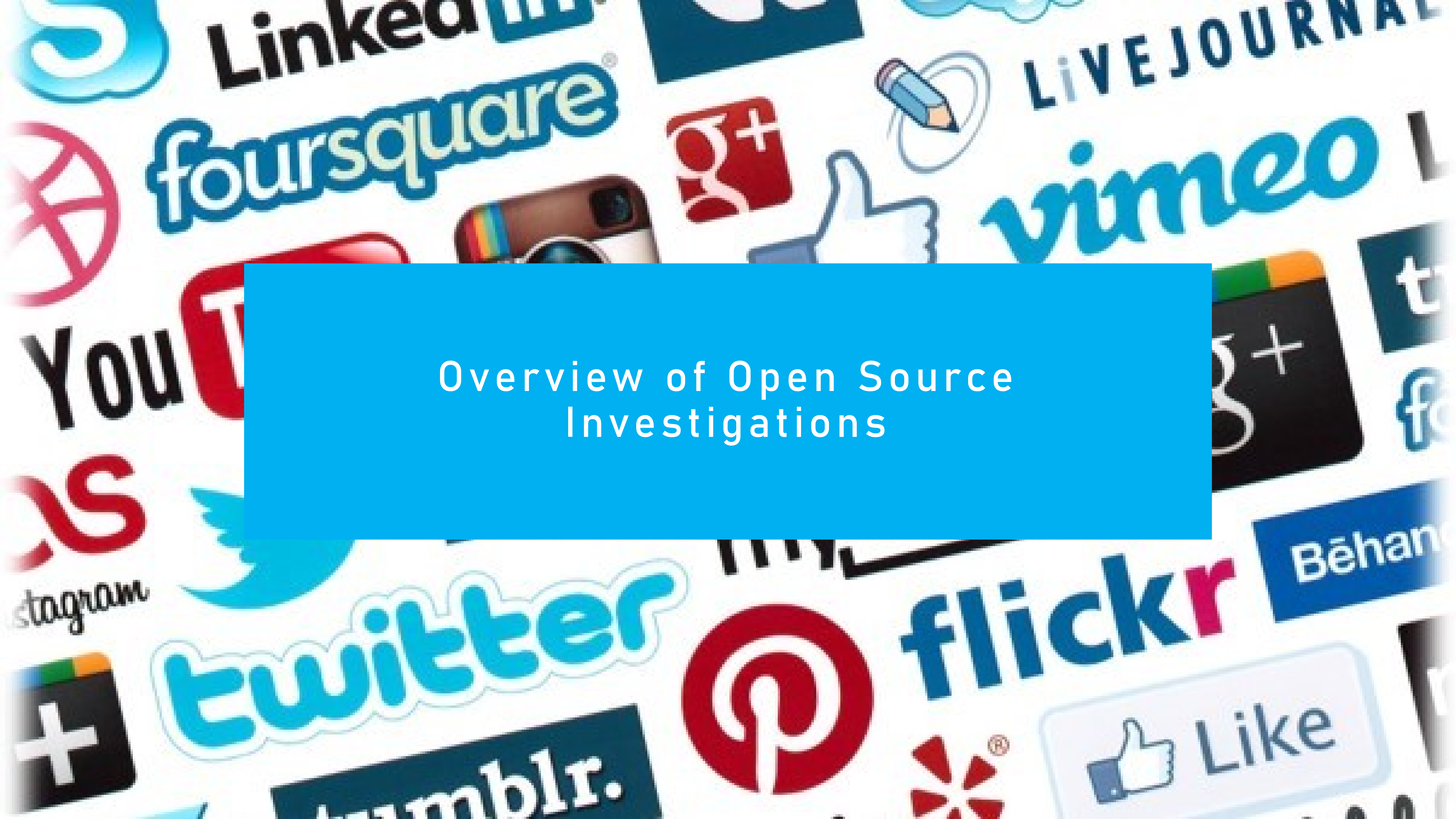
📧 Tracing domain name owners, the origin of an email and email blacklists

🌍 Geo-location tools for open source Investigations

🎮 Investigating Web 2.0 – social networking, blogs and online gaming

REMINDER

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



Overview of Open Source Investigations

WHAT IS OPEN SOURCE?

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

National Police Chiefs Council (NPCC)

DIGITAL FORENSICS

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

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

DIGITAL FORENSIC LIFECYCLE

Seizure

- Device seized
- Advice is to isolate device from the network

Device Pre-Acquired

- Device information recorded, photographs taken of the device
- Checks conducted to ensure device is isolated from the network

Data Extraction

- Data is acquired with the device "isolated from the network" to preserve data integrity. This will also prevent new data being downloaded

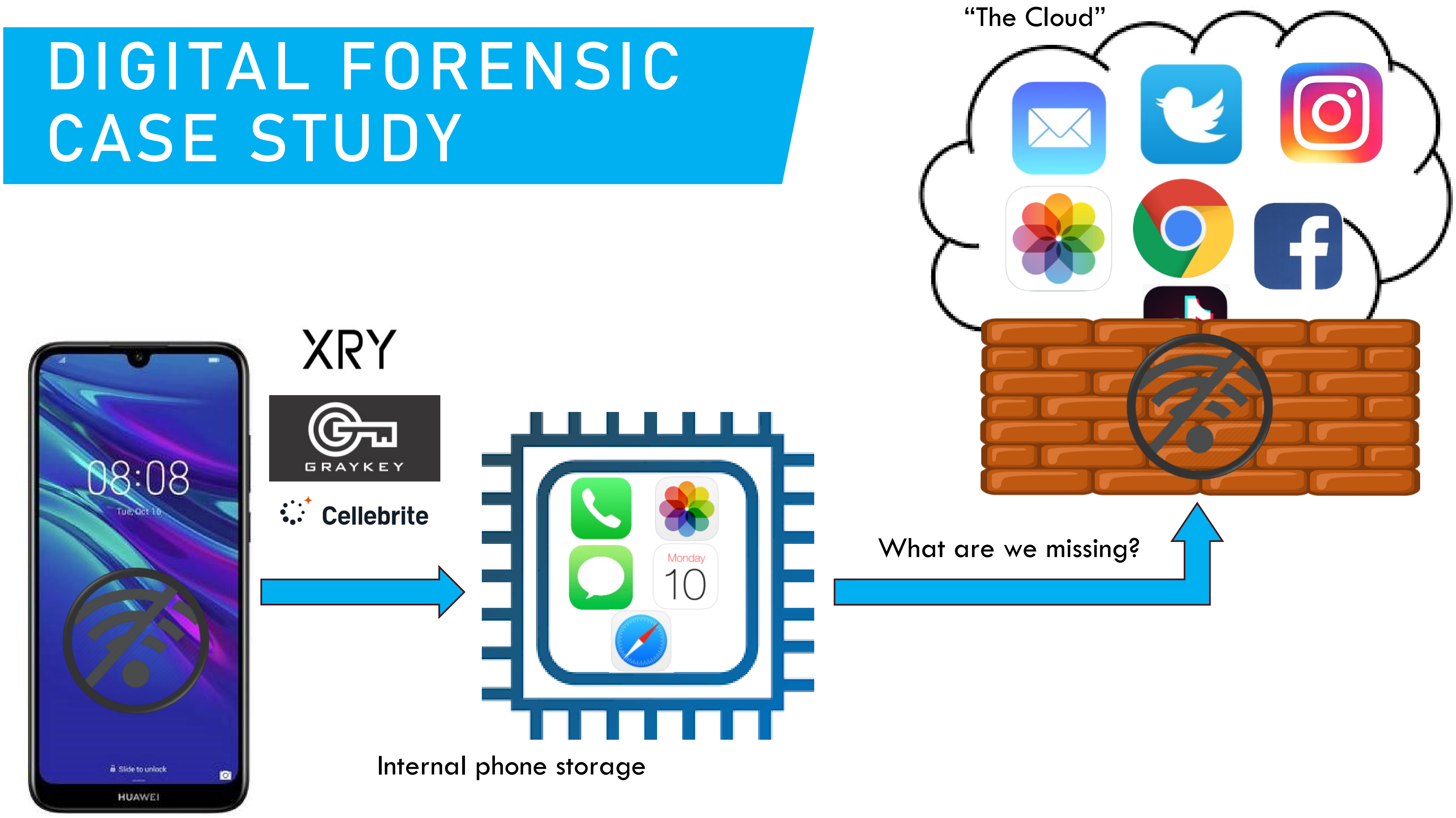
Data Analysis

- Analysis conducted using an array forensic tools
  - In accordance with the supplied Digital Investigative Strategy

Production of Reports

- Reports produced and submitted into the criminal justice system

DIGITAL FORENSIC CASE STUDY



“The Cloud”

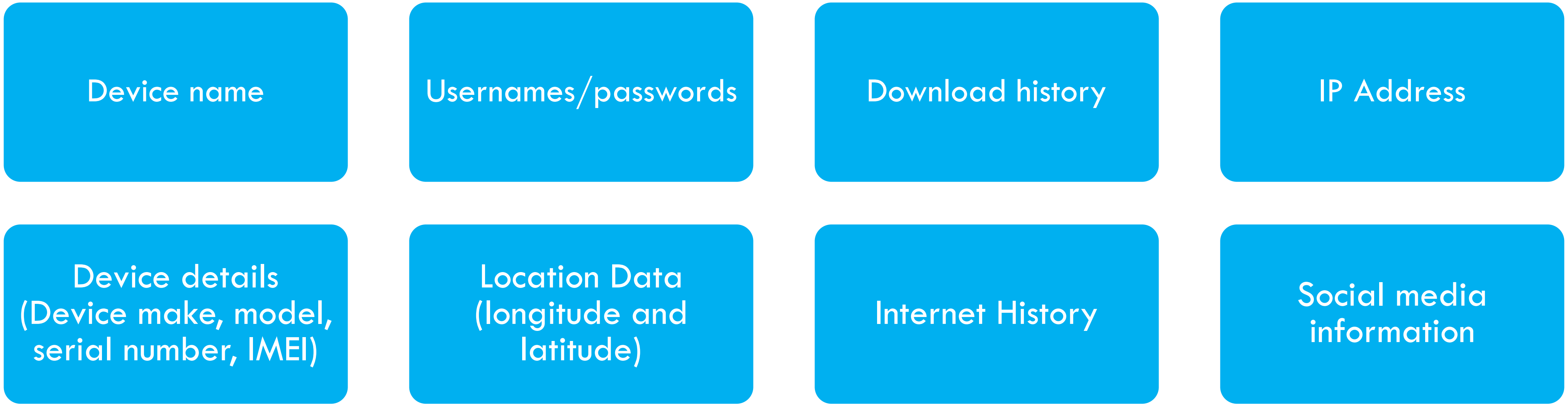
Internal phone storage

What are we missing?

Protecting your privacy during open source investigations

PROTECTING YOUR PRIVACY ONLINE

- The use of technology records a vast amount of information as part of its functionality
  - This is primarily to improve the user's experience
  - Can be used for other purposes
- The end user is often unaware that such information is recorded, often via cookies:



Device name

Usernames/passwords

Download history

IP Address

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

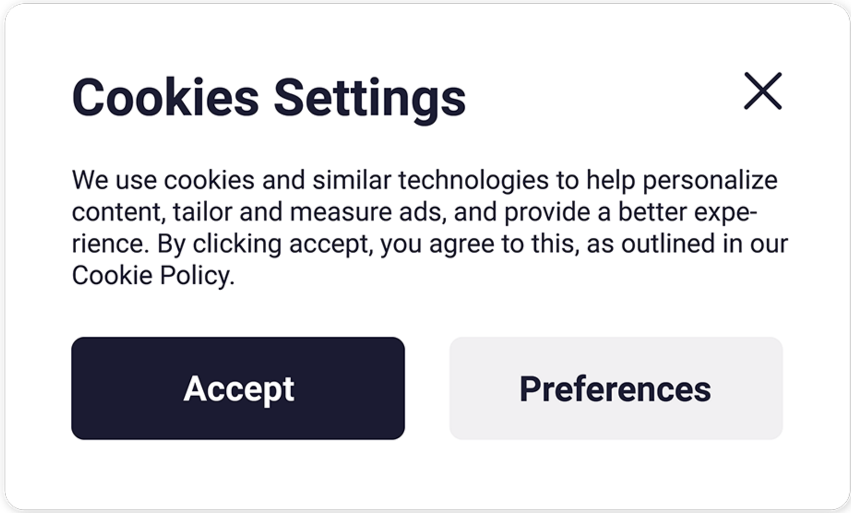
Location Data (longitude and latitude)

Internet History

Social media information

PROTECTING YOUR PRIVACY ONLINE

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

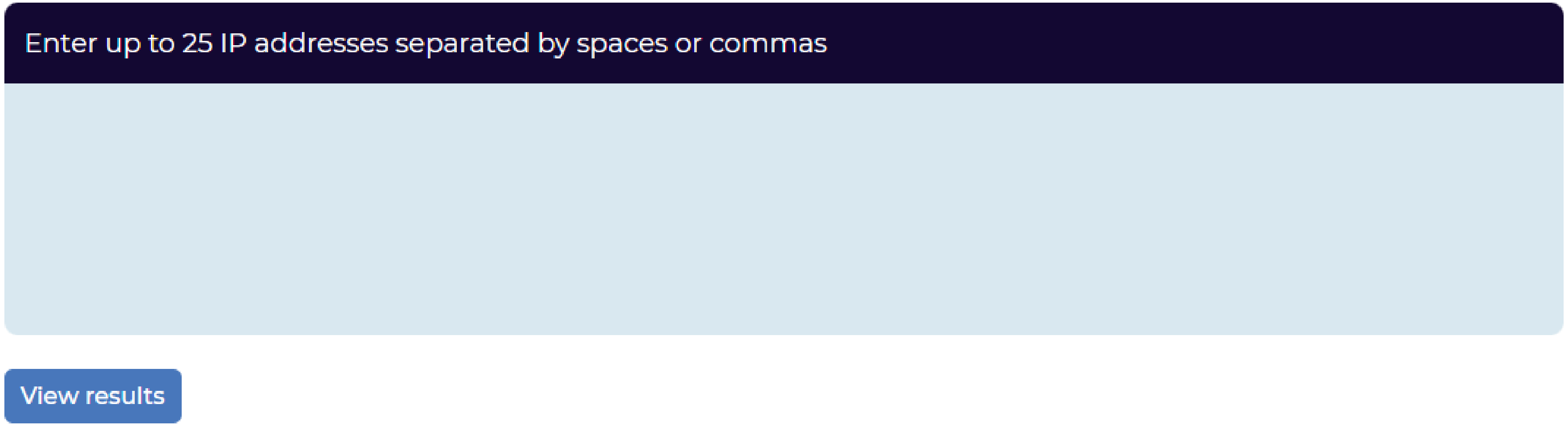


Cookies Settings

We use cookies and similar technologies to help personalize content, tailor and measure ads, and provide a better experience. By clicking accept, you agree to this, as outlined in our Cookie Policy.

IP ADDRESS EXERCISE

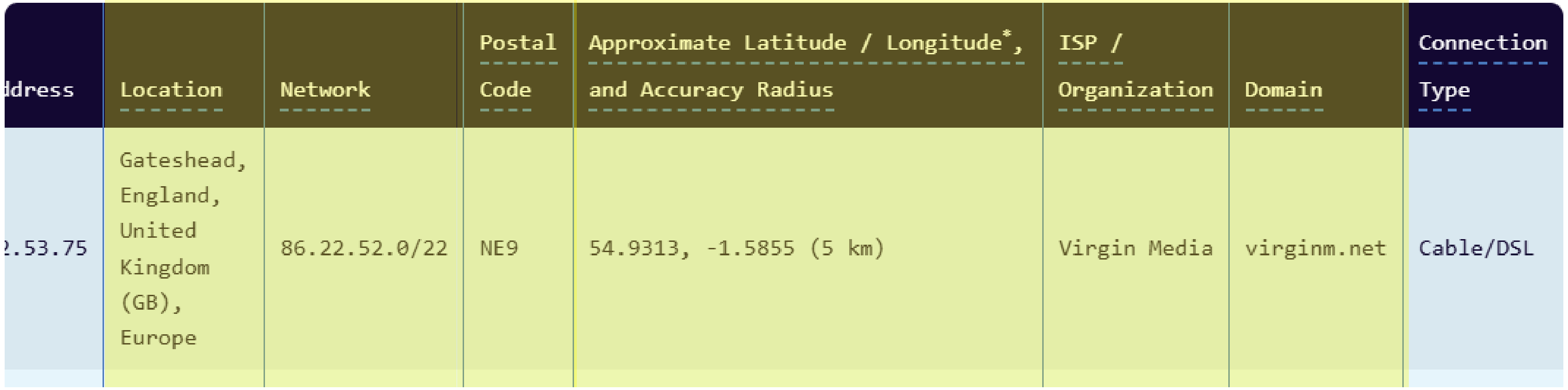
- **Step 1)** Visit Google
- **Step 2)** Search "What's my IP"
  - Google will usually display your IP address, if not it will list a number of free tools which may help
  - https://www.whatismyip.com is one of many tools which are available
  - Make a note of your IP address
- **Step 3)** Visit GeoIP2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



Enter up to 25 IP addresses separated by spaces or commas

IP ADDRESS – EXERCISE

- What information can be obtain from my IP address:

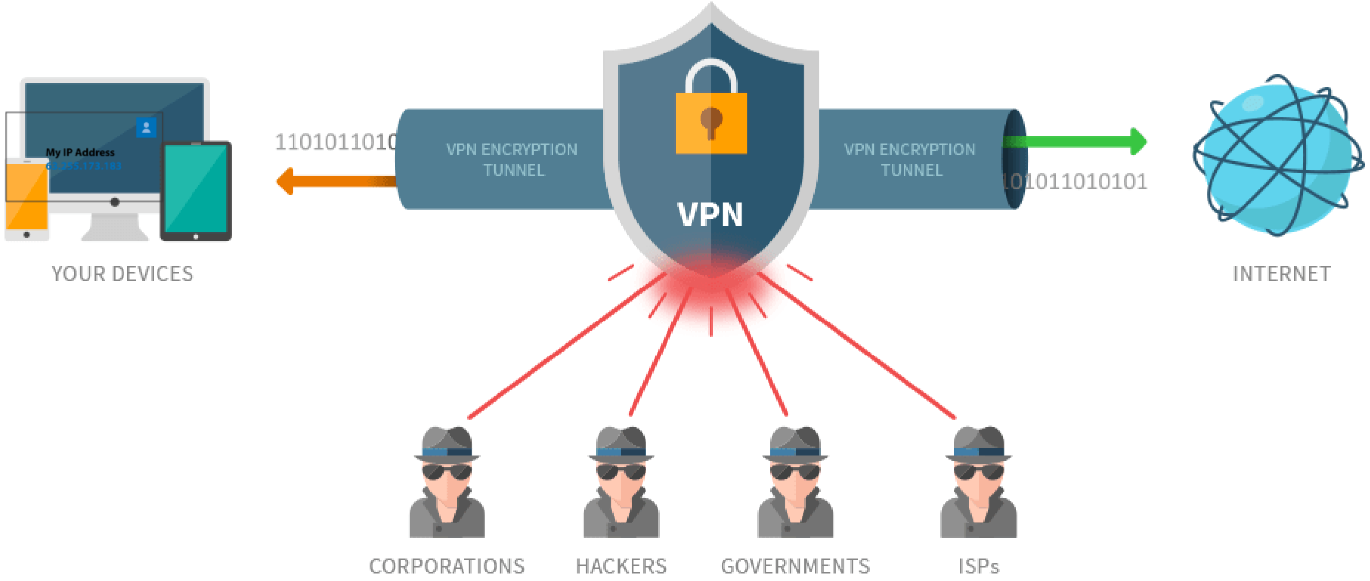


ddress	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain	Connection Type
.53.75	Gateshead, England, United Kingdom (GB), Europe	86.22.52.0/22	NE9	54.9313, -1.5855 (5 km)	Virgin Media	virginm.net	Cable/DSL

- This reveals some key information about my identity online which could be used to assist to identify me as an investigator
- What can we do as investigators to protect our identity online?

VIRTUAL PRIVATE NETWORKS

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



VIRTUAL PRIVATE NETWORKS

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

NordVPN®

ProtonVPN

Mozilla VPN

VIRTUAL PRIVATE NETWORKS

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

There are 1.5 billion VPN users in the world

Protect your online
privacy

Avoid
targeted ads

Enjoy tracker-free
streaming

Improve your
gaming experience

Stay connected
while traveling

Secure your home
network

Bypass oppressive
censorship

Save money
online

Stay safe
on public Wi-Fi

Reduce
ISP throttling

VIRTUAL PRIVATE NETWORKS – EXERCISE

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

Step 2) Enter your IP into Maxmind

Step 3) Register and Download Proton VPN

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

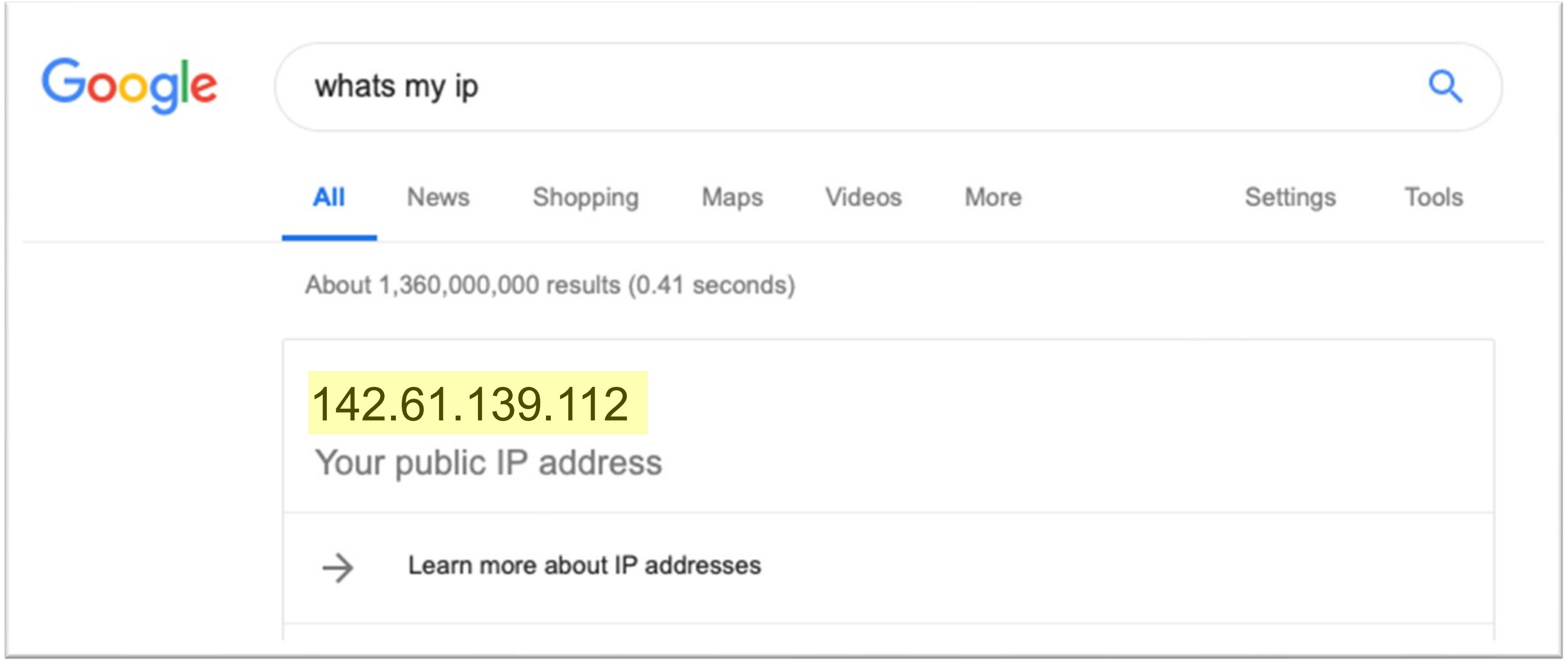
Step 5) Identify your IP address

Step 6) Enter your new IP into Maxmind

What do you notice?

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 1) Identify your IP address. (Hint: Search "What's My IP" on Google)



whats my ip

About 1,360,000,000 results (0.41 seconds)

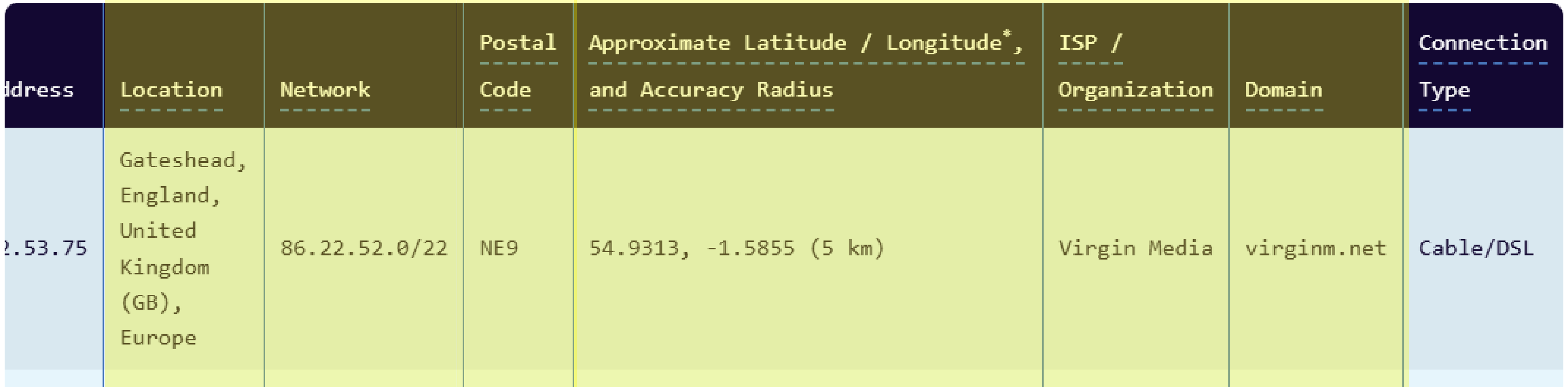
142.61.139.112

Your public IP address

Learn more about IP addresses

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 2) Enter your IP into Maxmind

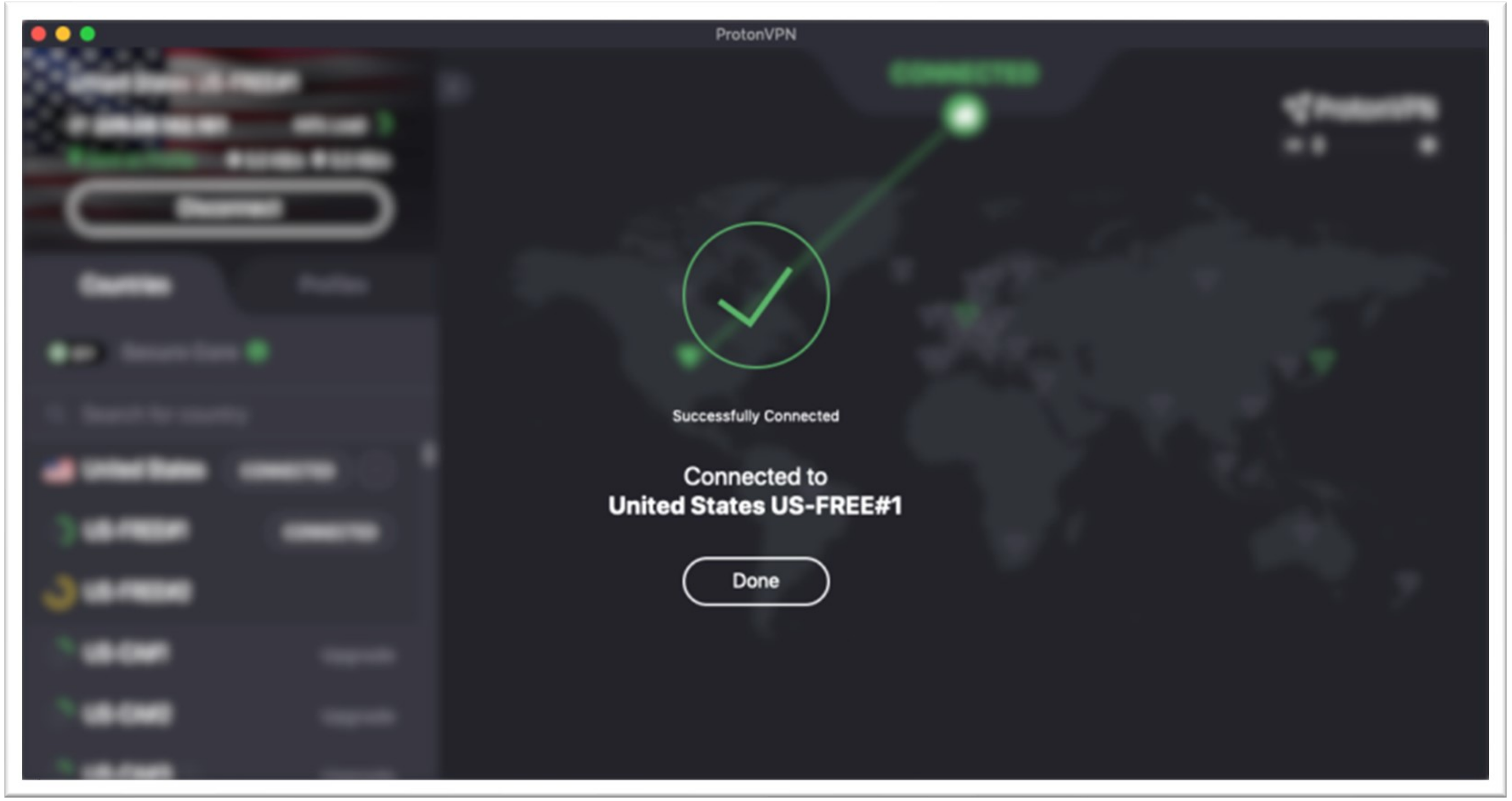


ddress	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain	Connection Type
2.53.75	Gateshead, England, United Kingdom (GB), Europe	86.22.52.0/22	NE9	54.9313, -1.5855 (5 km)	Virgin Media	virginm.net	Cable/DSL

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 3) Register and Download Proton VPN

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

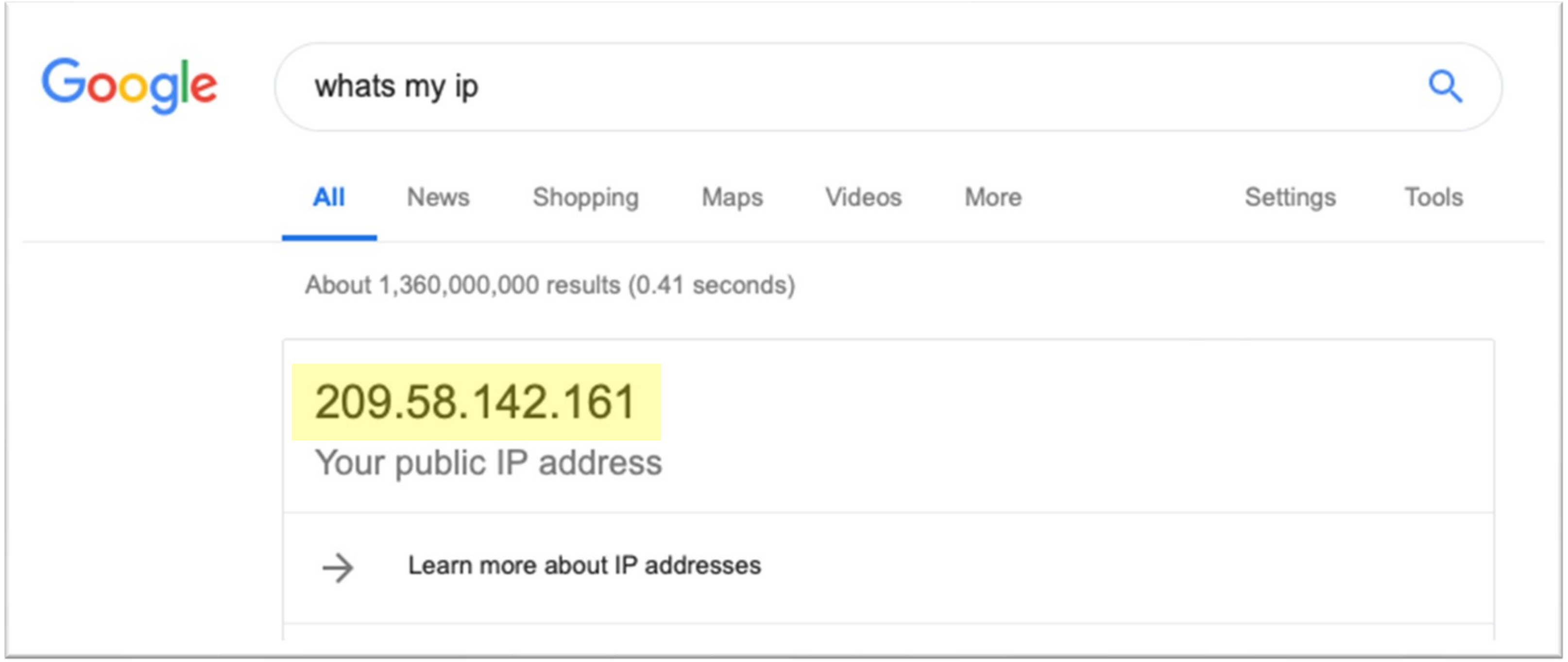


Successfully Connected

Connected to
United States US-FREE#1

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 5) Identify your IP address



whats my ip

About 1,360,000,000 results (0.41 seconds)

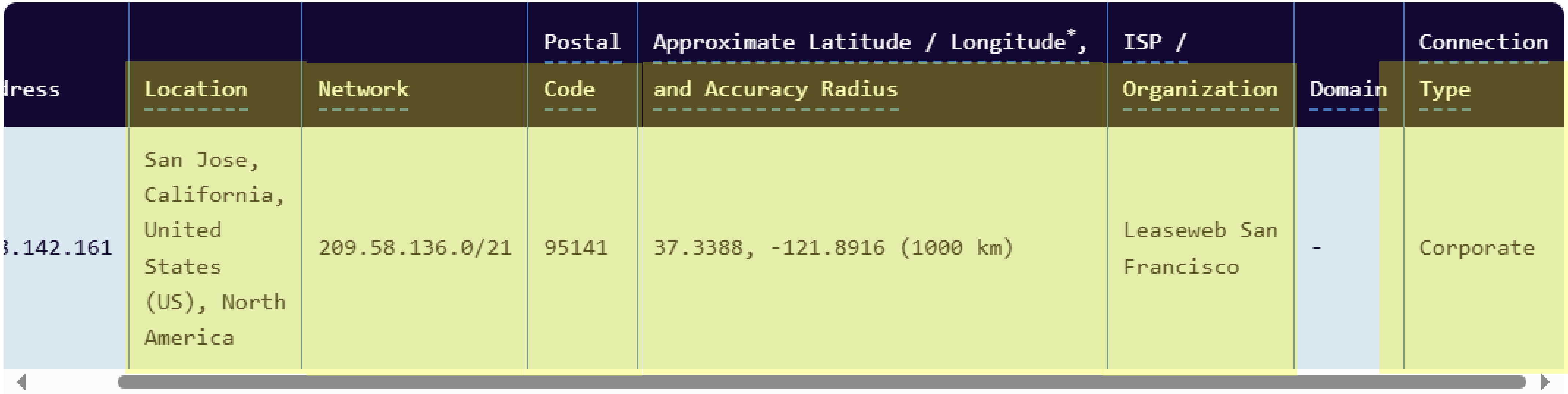
209.58.142.161

Your public IP address

→ Learn more about IP addresses

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 6) Enter your new IP into Maxmind

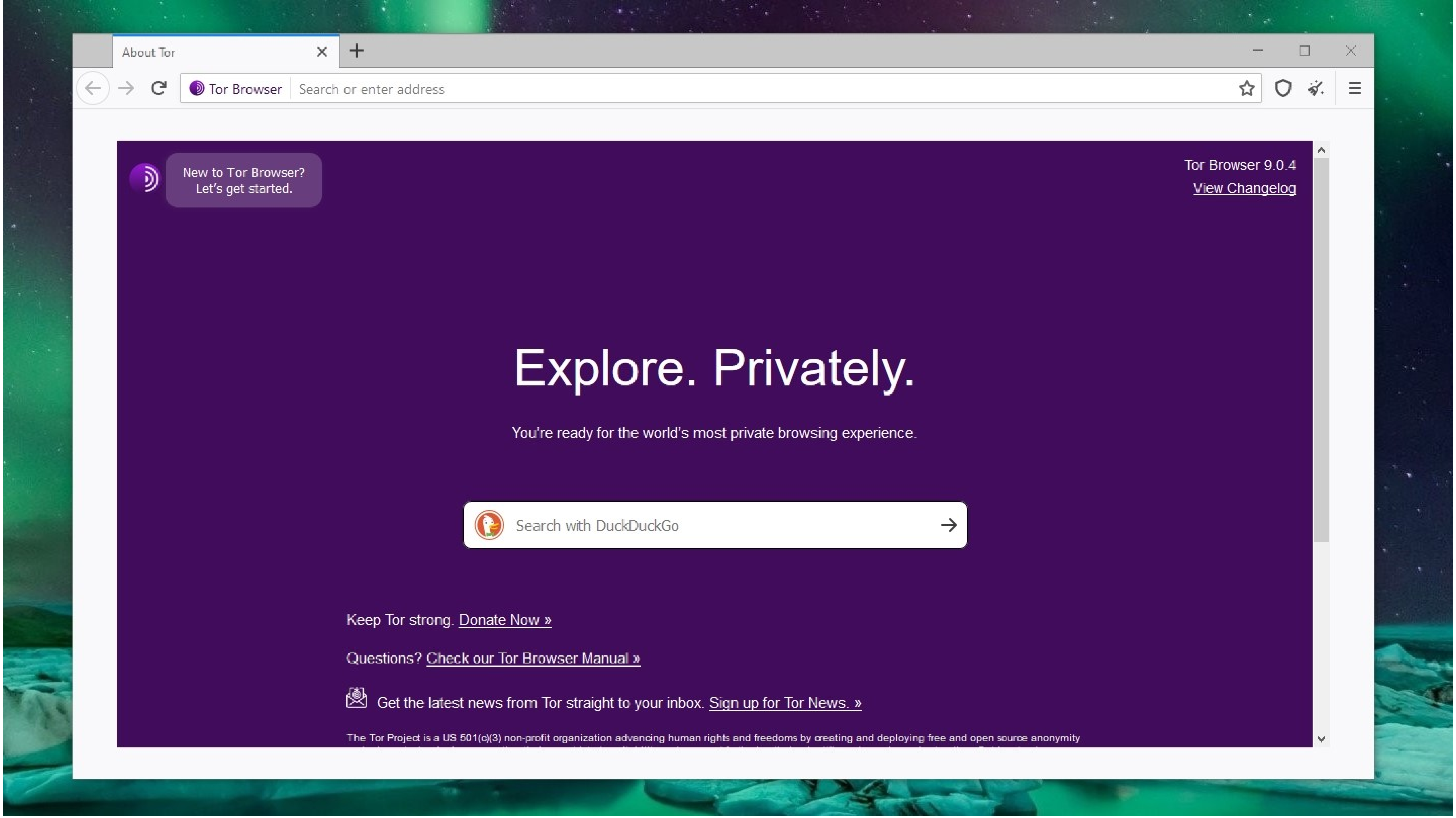


dress	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain	Connection Type
.142.161	San Jose, California, United States (US), North America	209.58.136.0/21	95141	37.3388, -121.8916 (1000 km)	Leaseweb San Francisco	-	Corporate

What do you notice?

TOR BROWSER

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



New to Tor Browser? Let's get started.

Tor Browser 9.0.4
View Changelog

Explore. Privately.

You're ready for the world's most private browsing experience.

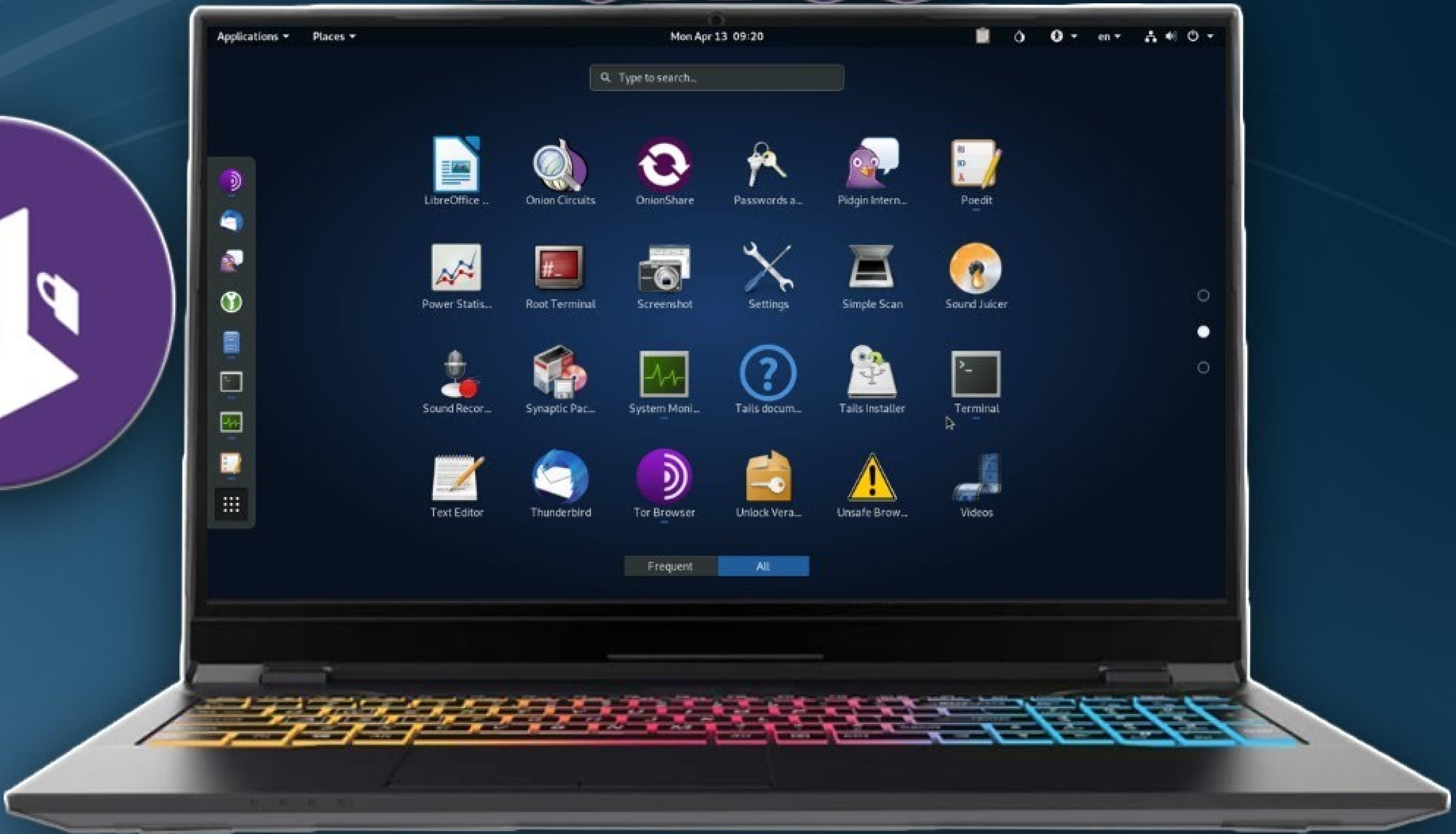
Keep Tor strong. Donate Now »

Questions? Check our Tor Browser Manual »

Get the latest news from Tor straight to your inbox. Sign up for Tor News. »

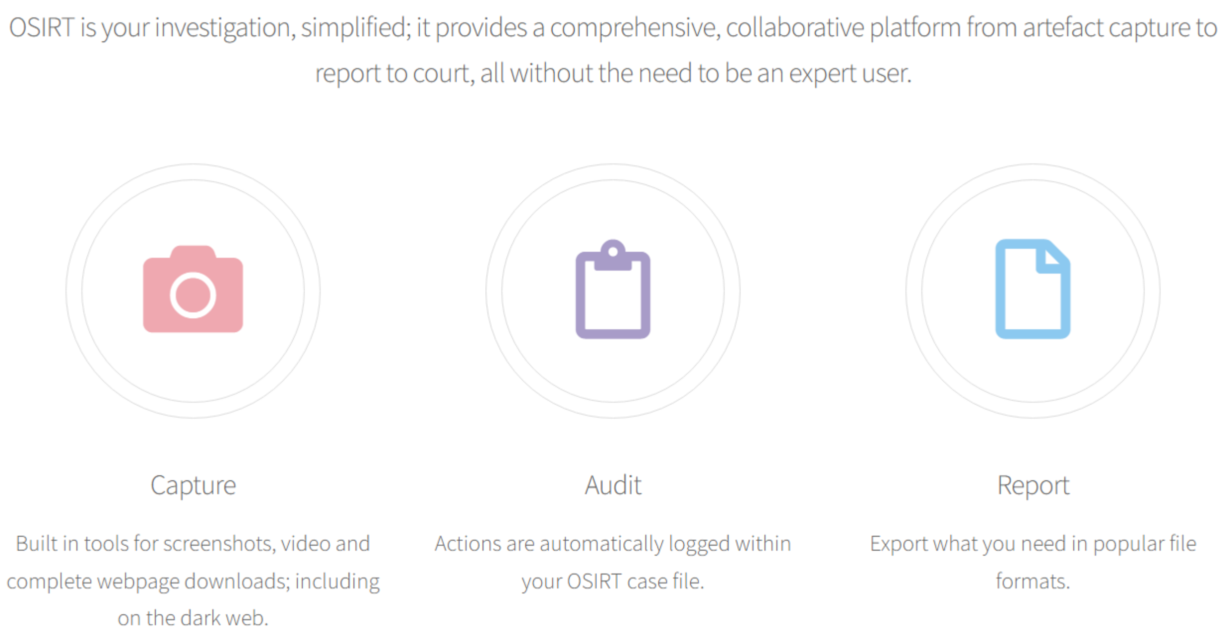
The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity

Tails


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

OSIRT BROWSER

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



OSIRT is your investigation, simplified; it provides a comprehensive, collaborative platform from artefact capture to report to court, all without the need to be an expert user.

Capture

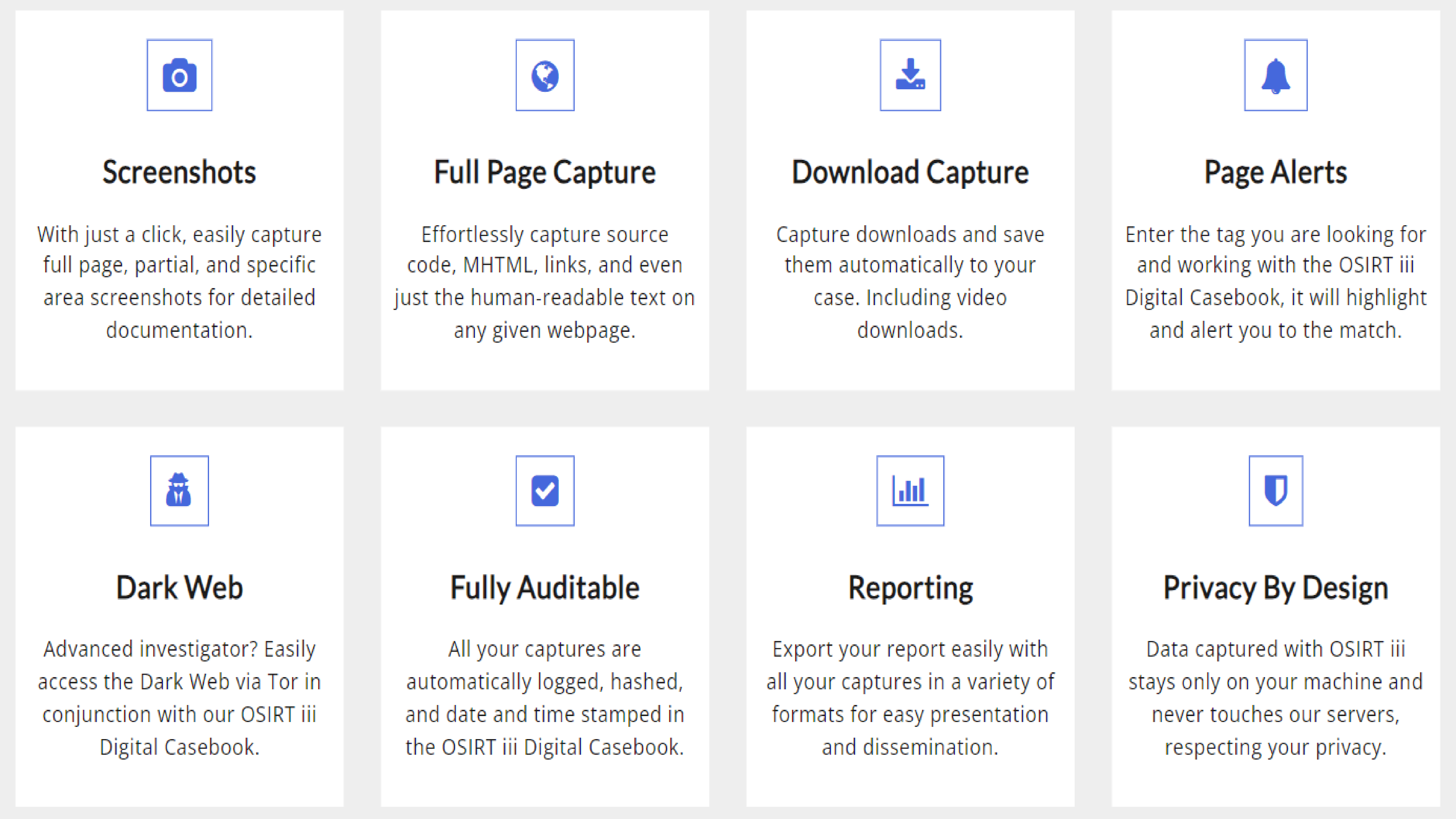
Built in tools for screenshots, video and complete webpage downloads; including on the dark web.

Audit

Actions are automatically logged within your OSIRT case file.

Report

Export what you need in popular file formats.



Screenshots

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

Full Page Capture

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

Download Capture

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

Page Alerts

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

Dark Web

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

Fully Auditable

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

Reporting

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

Privacy By Design

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

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

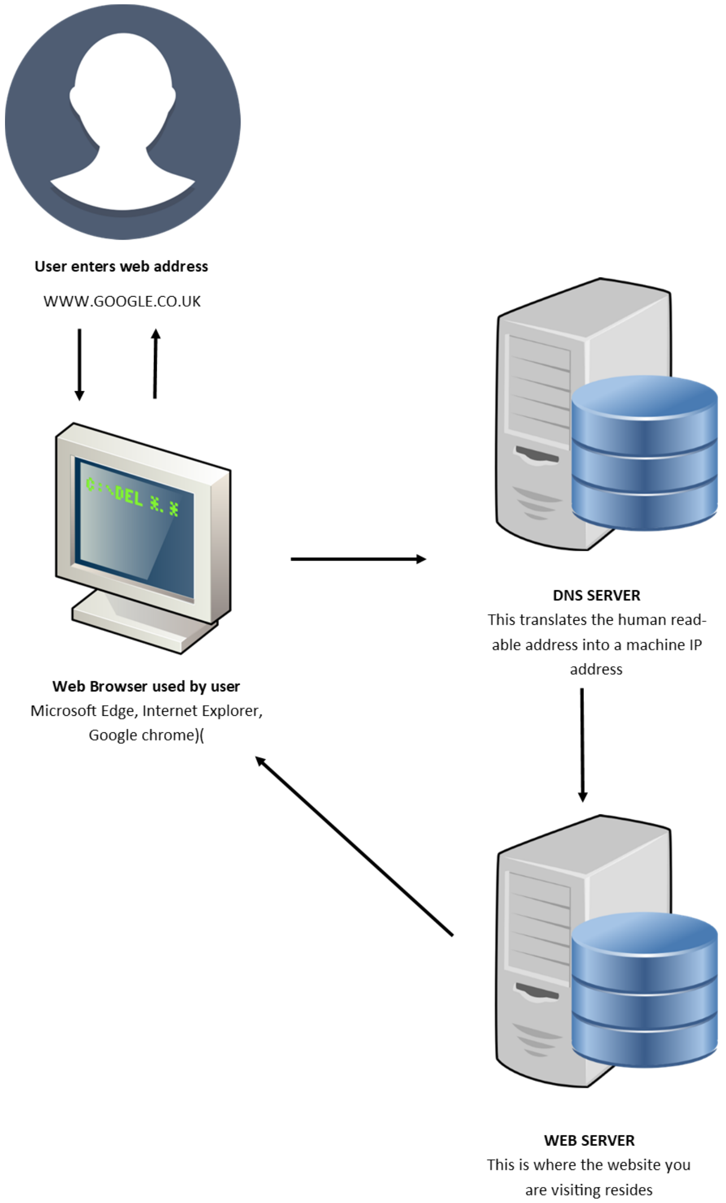
DOMAIN NAMES

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

Name

Address

Email


User enters web address

WWW.GOOGLE.CO.UK

Web Browser used by user

Microsoft Edge, Internet Explorer, Google chrome)(

DNS SERVER

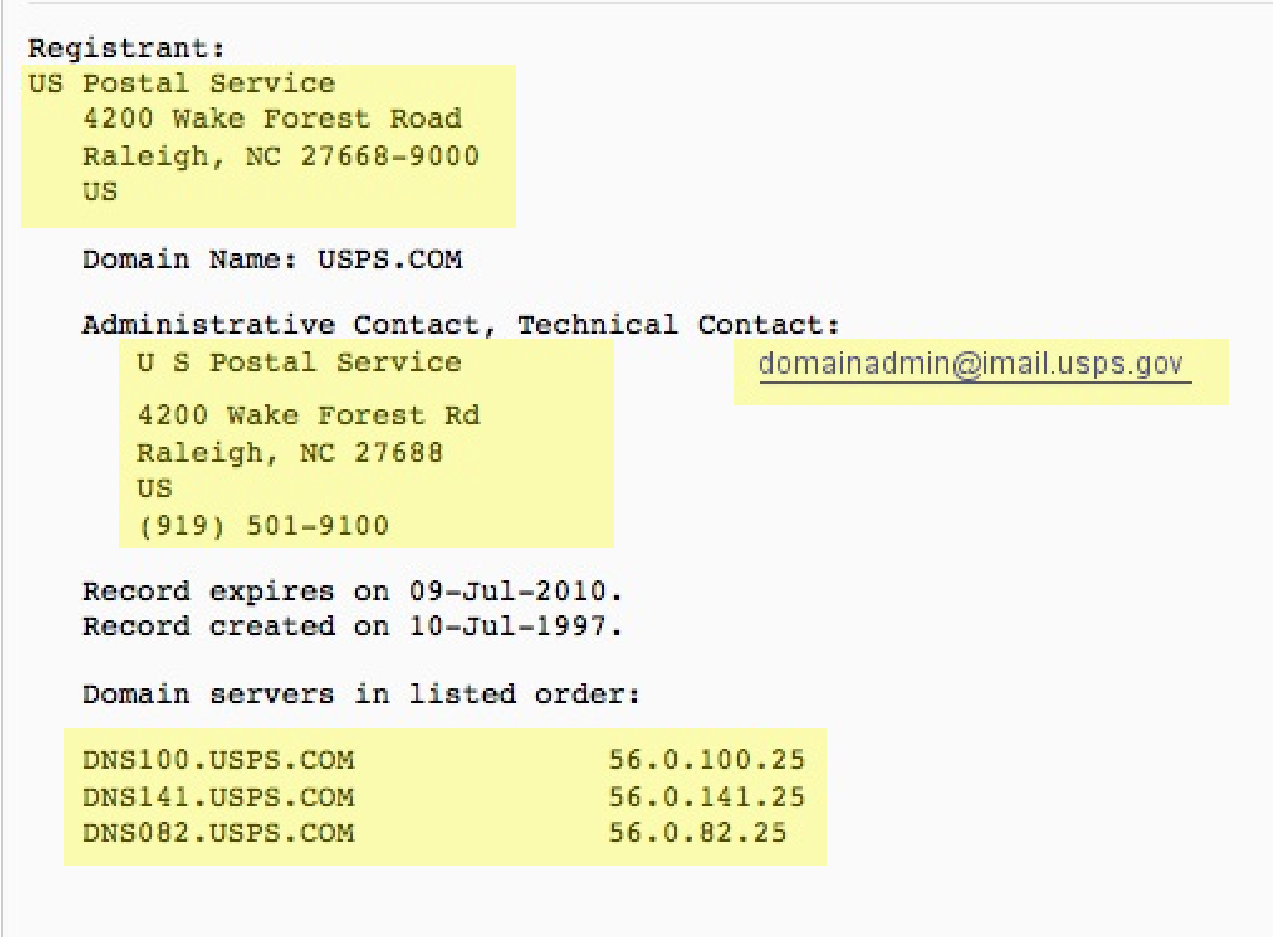
This translates the human read-able address into a machine IP address

WEB SERVER

This is where the website you are visiting resides

DOMAIN NAMES - WHOIS

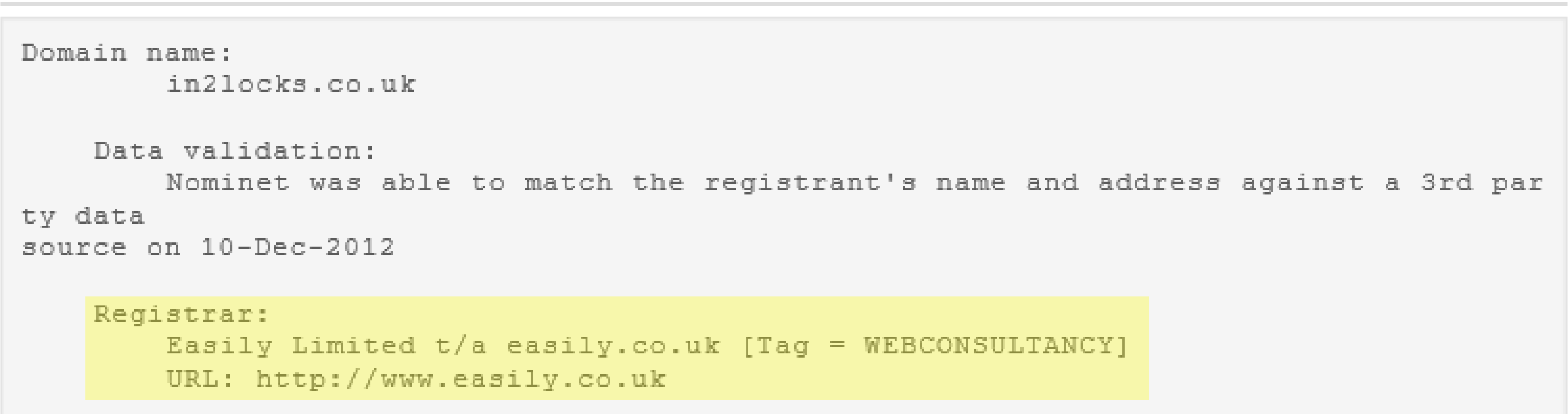
- As investigators, this information may help us identify the owner of a website:
  - http://whois.domaintools.com
- WHOIS search conducted for the US Postal Service domain name
  - www.usps.com
- This reveals a number of details
  - Postal address
  - Telephone number
  - Email address
  - IP addresses



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

   Domain Name: USPS.COM

   Administrative Contact, Technical Contact:
      U S Postal Service                              domainadmin@imail.usps.gov

      4200 Wake Forest Rd
      Raleigh, NC 27688
      US
      (919) 501-9100

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

   Domain servers in listed order:

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

DOMAIN NAMES – PROXY

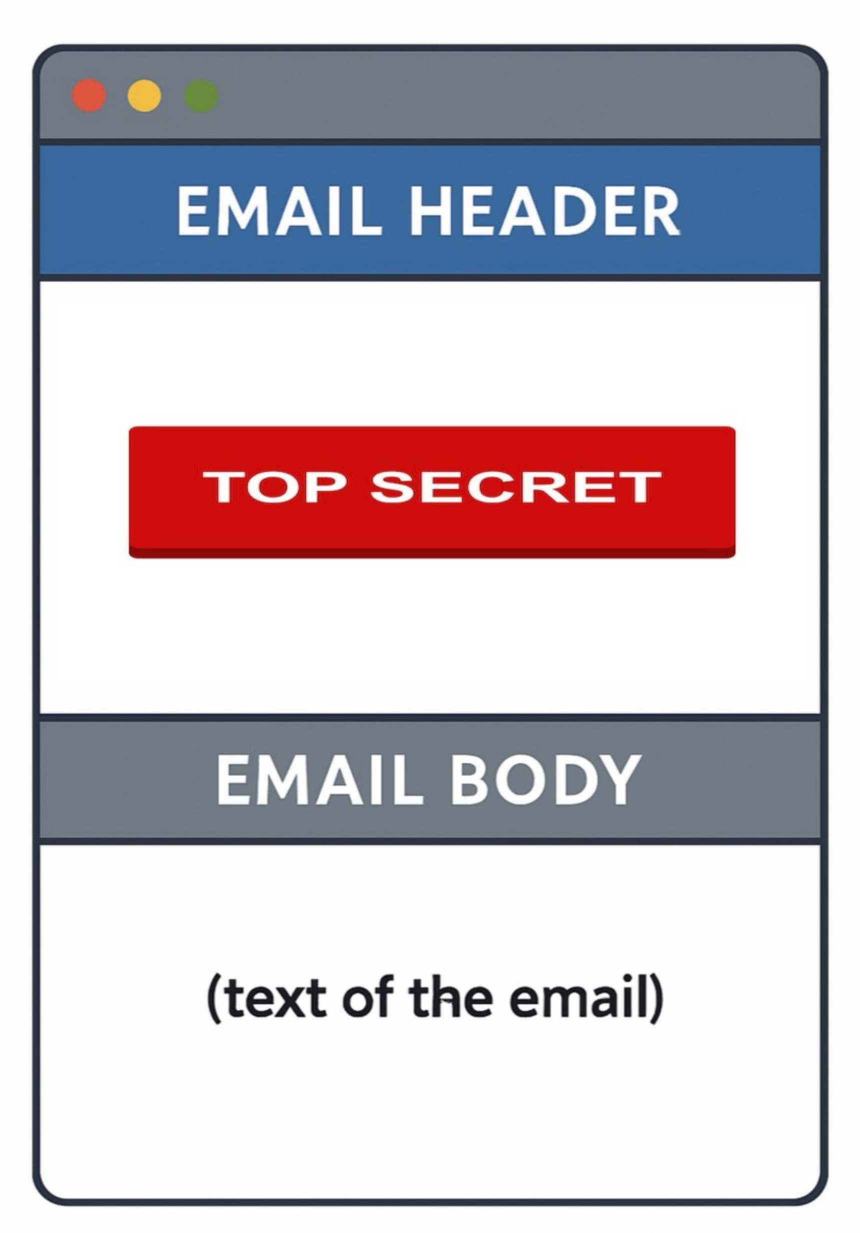
- Privacy is important part of many peoples lives
  - Think about the latest Apple adverts – all about privacy!
- To assist with privacy, domain name sellers offer a service called Domain Proxy
  - Domain proxy is a paid service which allows you to privately register a domain name
  - The service replaces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



```
Domain name:
        in2locks.co.uk

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

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

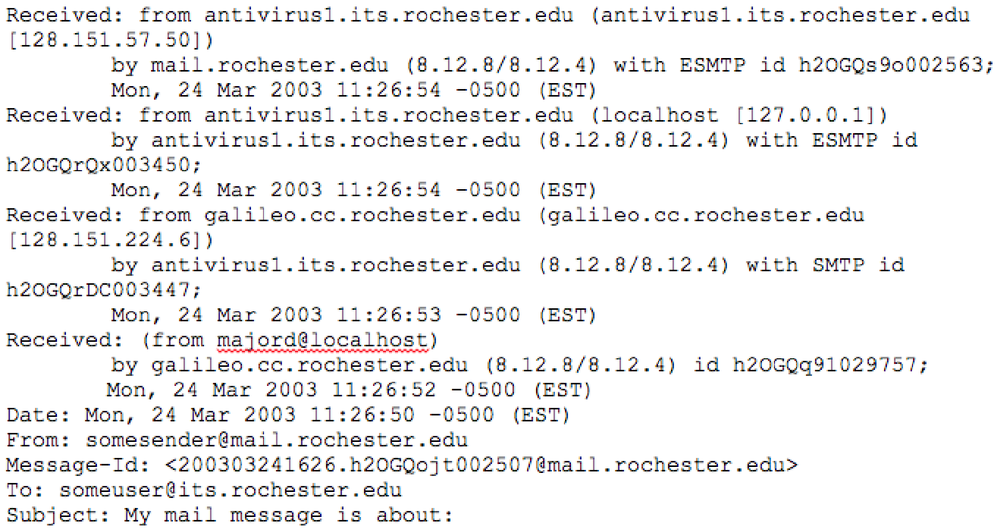
EMAILS

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



EMAIL HEADERS

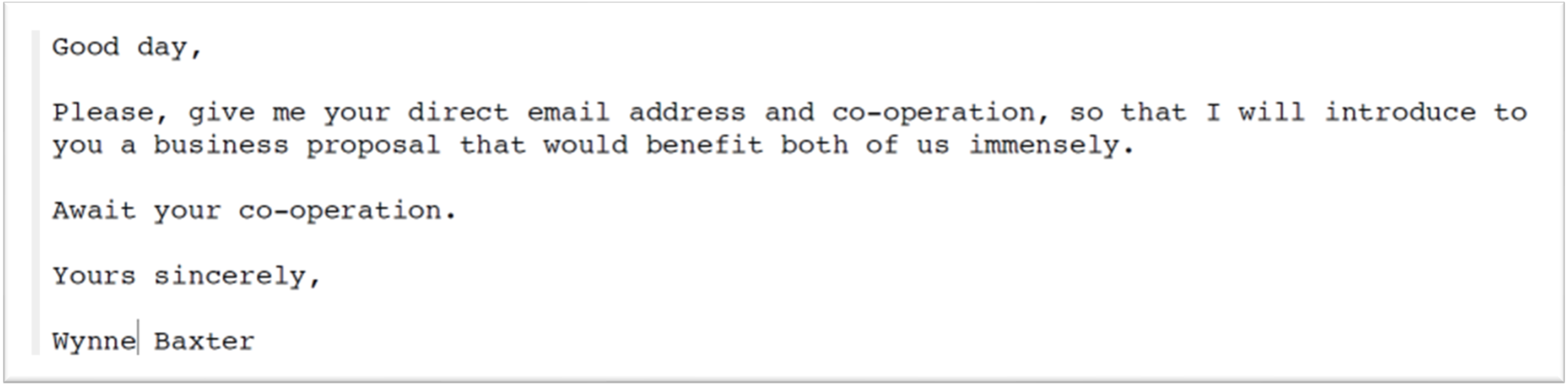
- Often difficult to interpret, until we understand the different areas of interest
  - **Content-Type:** Notes whether the email is HTML or plain text.
  - **Date:** When the email was written.
  - **Delivery Date:** When the email was received by your mail server.
  - **From:** Who sent the email.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



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

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

EMAIL HEADERS – EXERCISE 1



Good day,

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

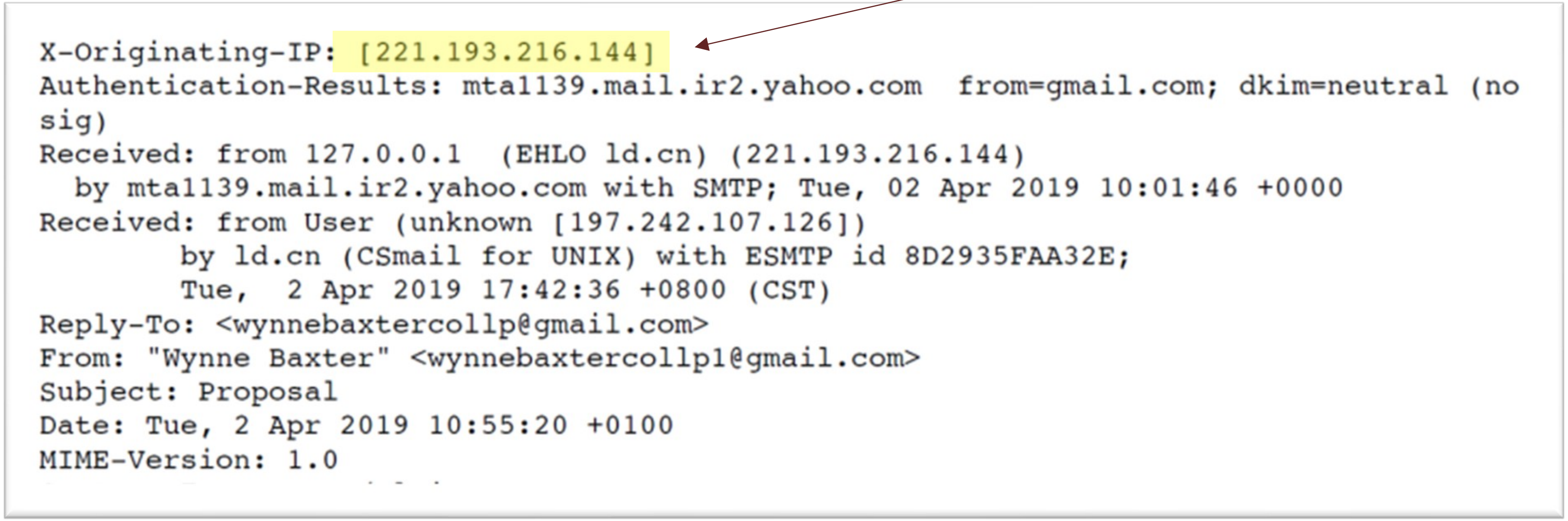
Await your co-operation.

Yours sincerely,

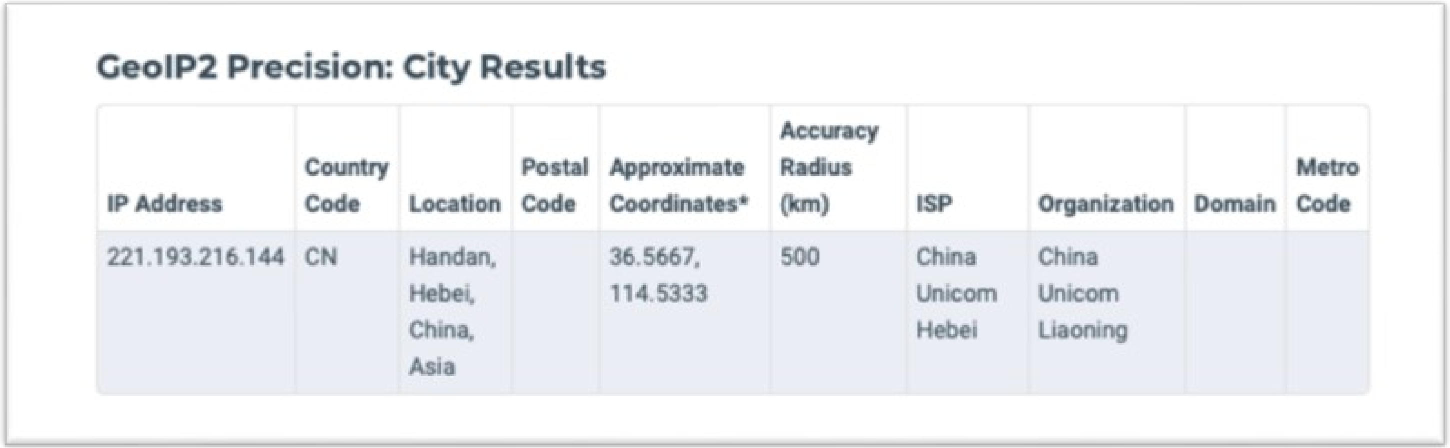
Wynne Baxter

EMAIL HEADERS – EXERCISE 1

Remember: this could be assigned by a VPN



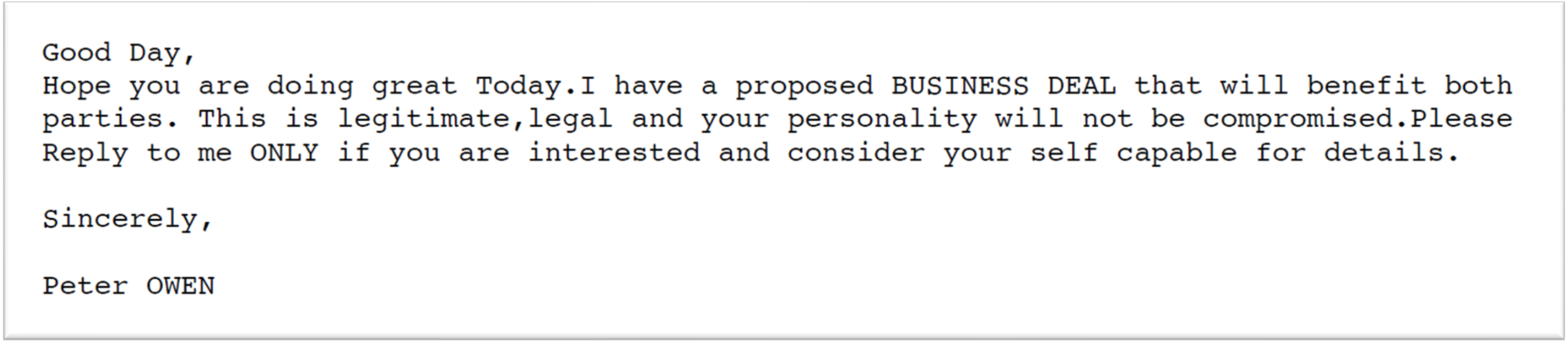
```
X-Originating-IP: [221.193.216.144]
Authentication-Results: mta1139.mail.ir2.yahoo.com  from=gmail.com; dkim=neutral (no
sig)
Received: from 127.0.0.1  (EHLO ld.cn) (221.193.216.144)
  by mta1139.mail.ir2.yahoo.com with SMTP; Tue, 02 Apr 2019 10:01:46 +0000
Received: from User (unknown [197.242.107.126])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



GeoIP2 Precision: City Results

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

EMAIL HEADERS – EXERCISE 2



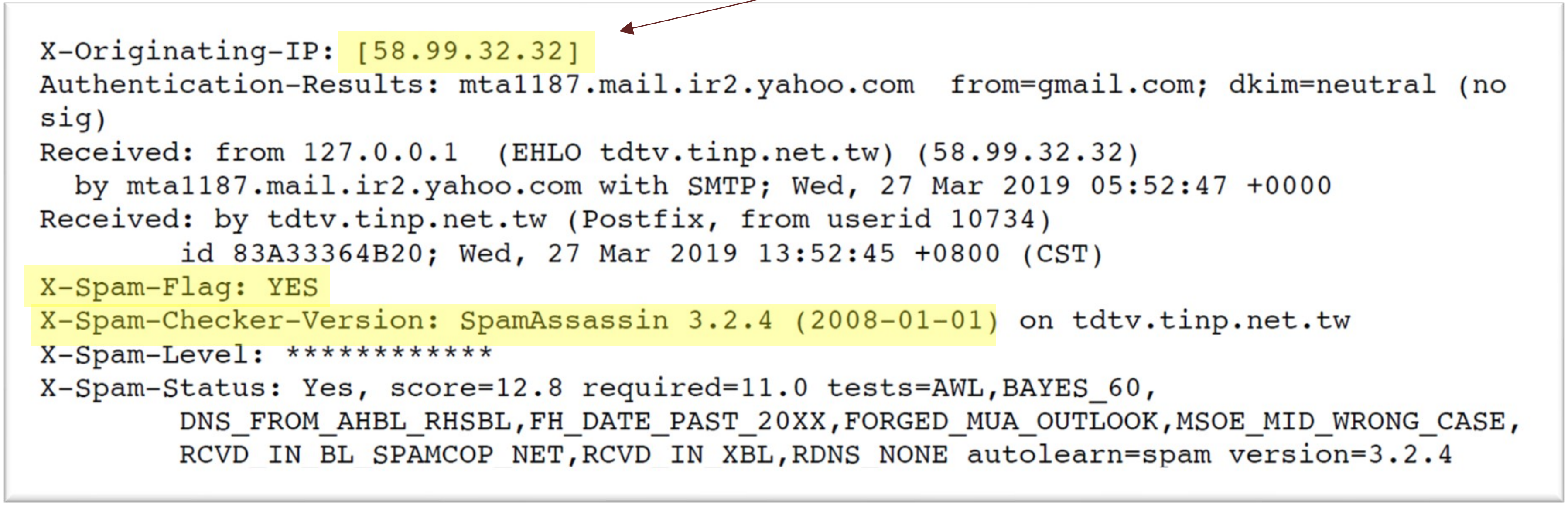
Good Day,
Hope you are doing great Today.I have a proposed BUSINESS DEAL that will benefit both parties. This is legitimate,legal and your personality will not be compromised.Please Reply to me ONLY if you are interested and consider your self capable for details.

Sincerely,

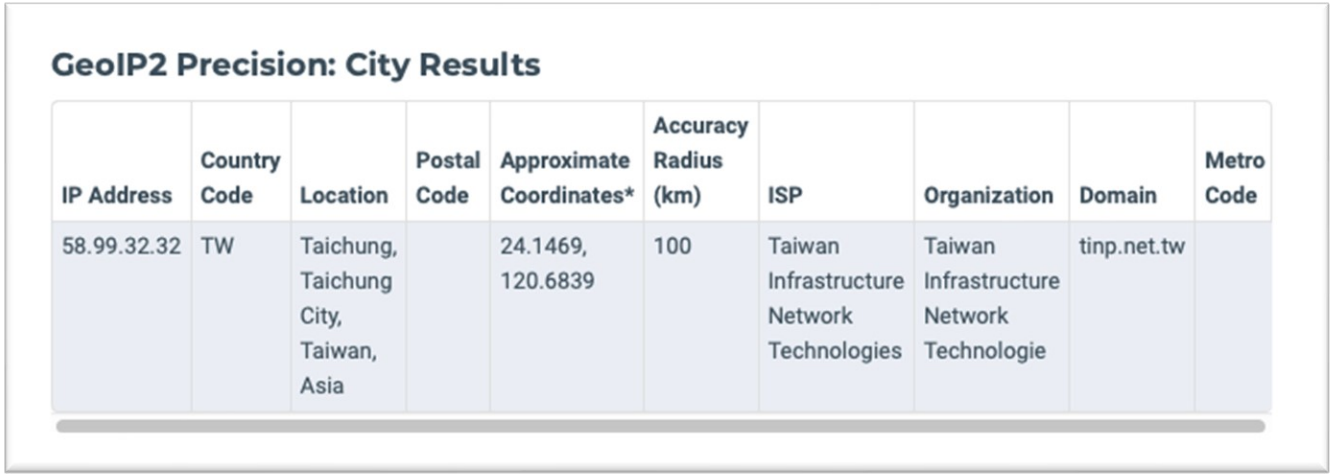
Peter OWEN

EMAIL HEADERS – EXERCISE 2

Remember: this could be assigned by a VPN



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



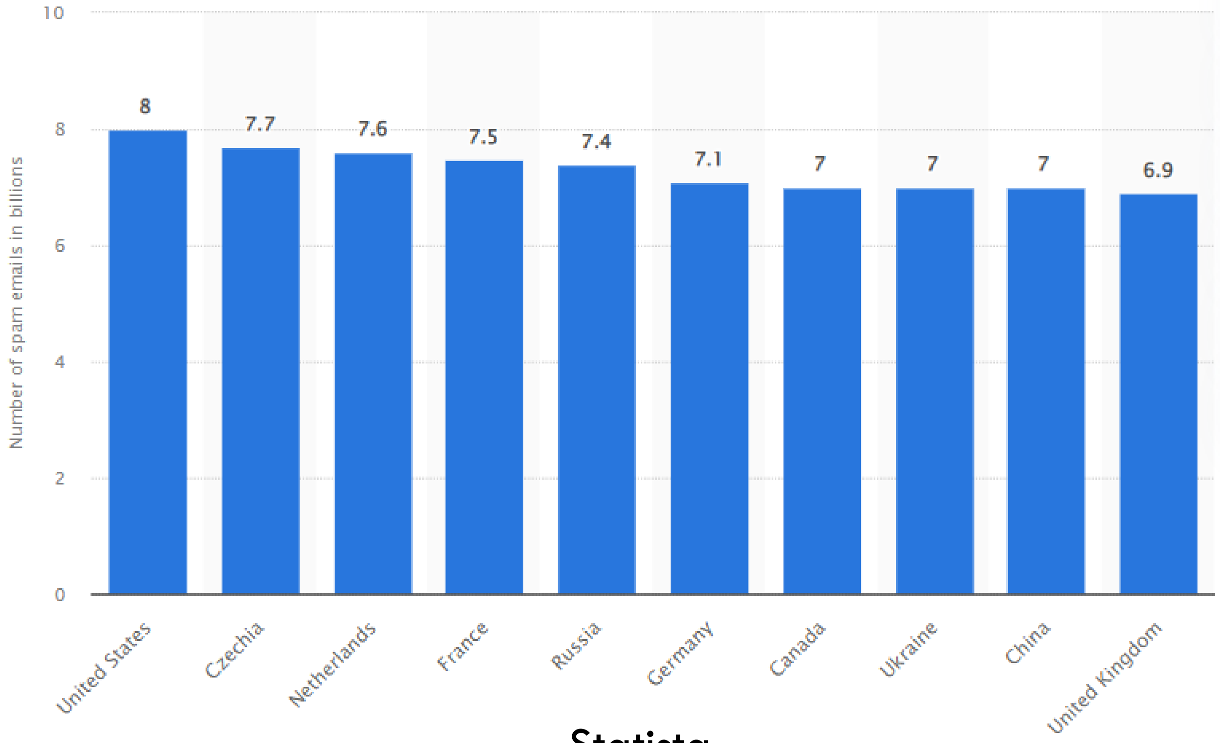
GeoIP2 Precision: City Results

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

EMAIL SPAM

- Spam (Junk mail) is sent for a number of reasons:
  - Advertising
  - Scam money
  - Phishing to obtain personal information such as credit card, bank details and passwords
  - Spread malicious code i.e. viruses

Daily number of spam emails sent worldwide as of January 2023, by country (in billions)



Statista

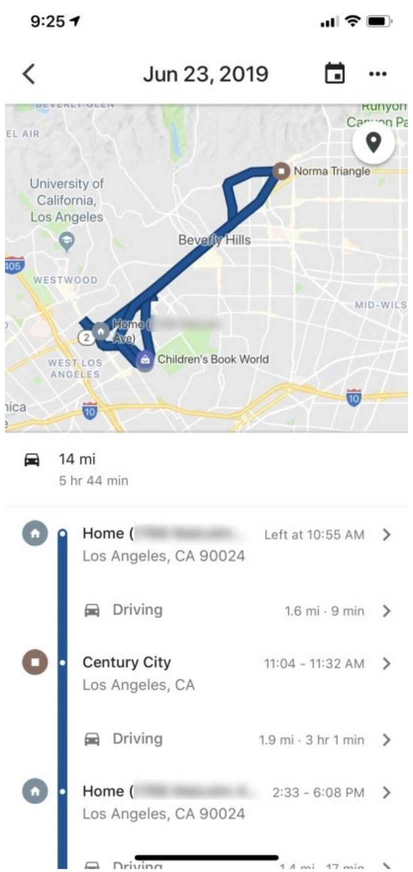
EMAIL BLACKLISTS

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

Geo-location tools for Open Source Investigations

GEO-LOCATION

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



14 mi
5 hr 44 min

Home ([redacted]) Los Angeles, CA 90024 — Left at 10:55 AM

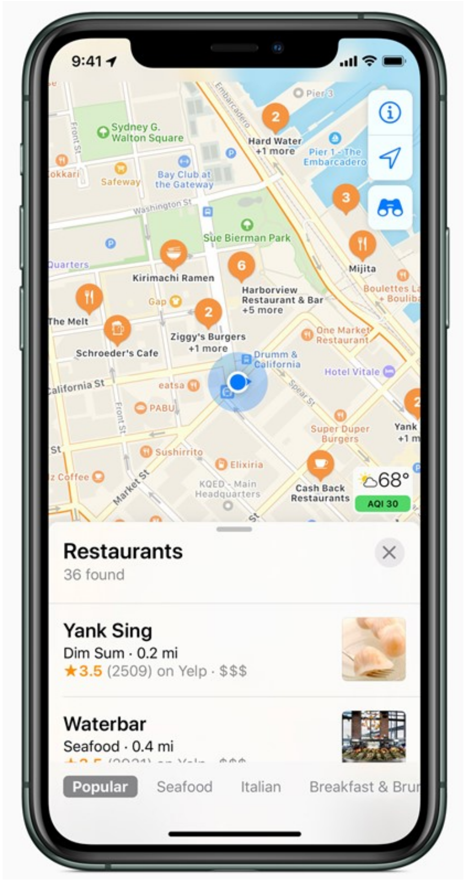
Driving — 1.6 mi · 9 min

Century City, Los Angeles, CA — 11:04 - 11:32 AM

Driving — 1.9 mi · 3 hr 1 min

Home ([redacted]) Los Angeles, CA 90024 — 2:33 - 6:08 PM

Driving — 1.4 mi · 17 min



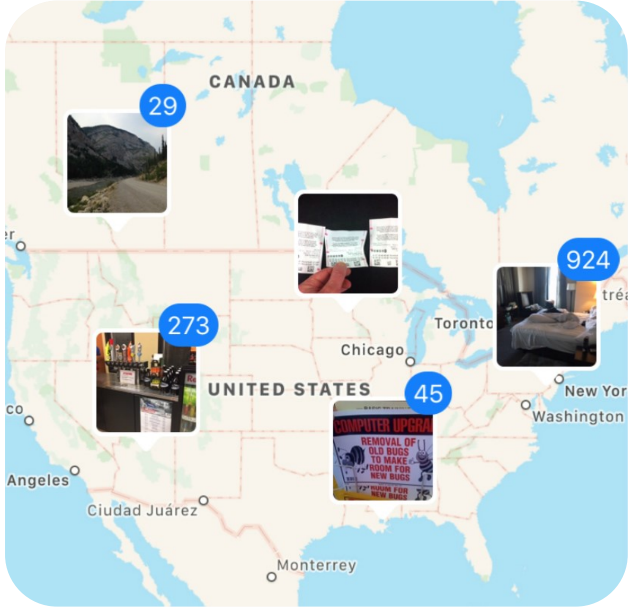
Restaurants
36 found

Yank Sing
Dim Sum · 0.2 mi
★3.5 (2509) on Yelp · $$$

Waterbar
Seafood · 0.4 mi

GEO-LOCATION

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

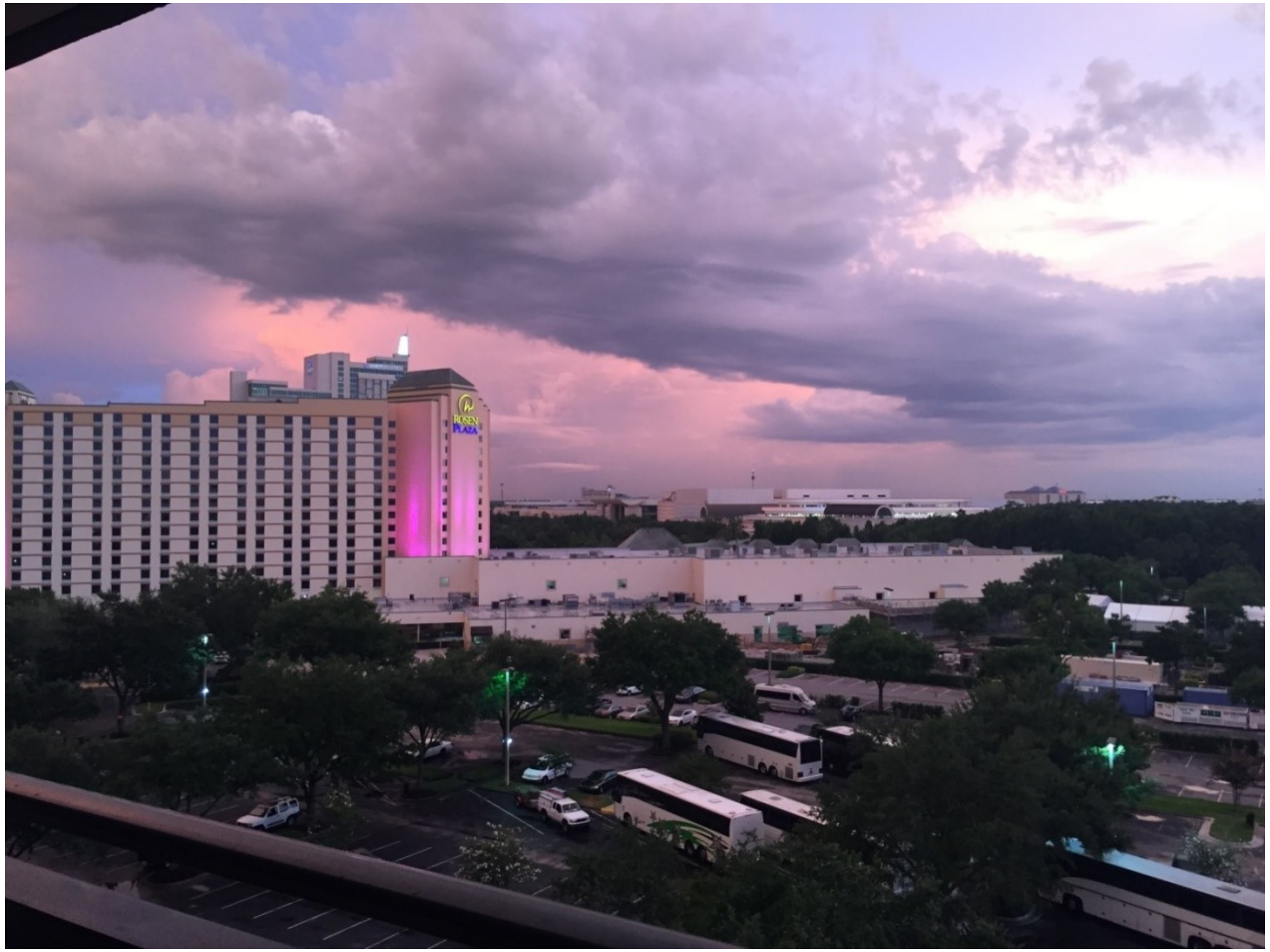


EXIF DATA EXERCISE

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

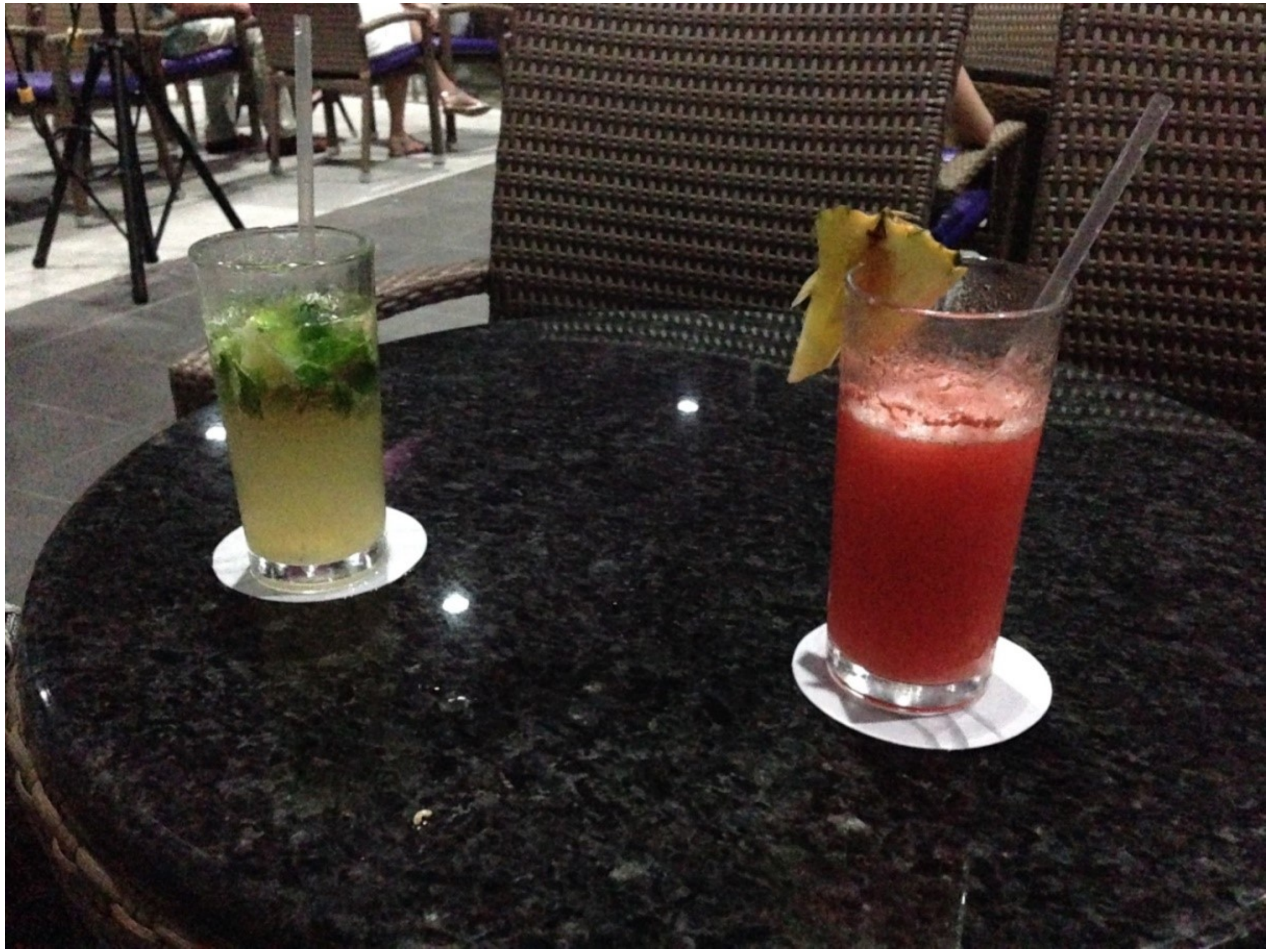
EXIF DATA EXERCISE

- Filename: IMG_7300.JPG



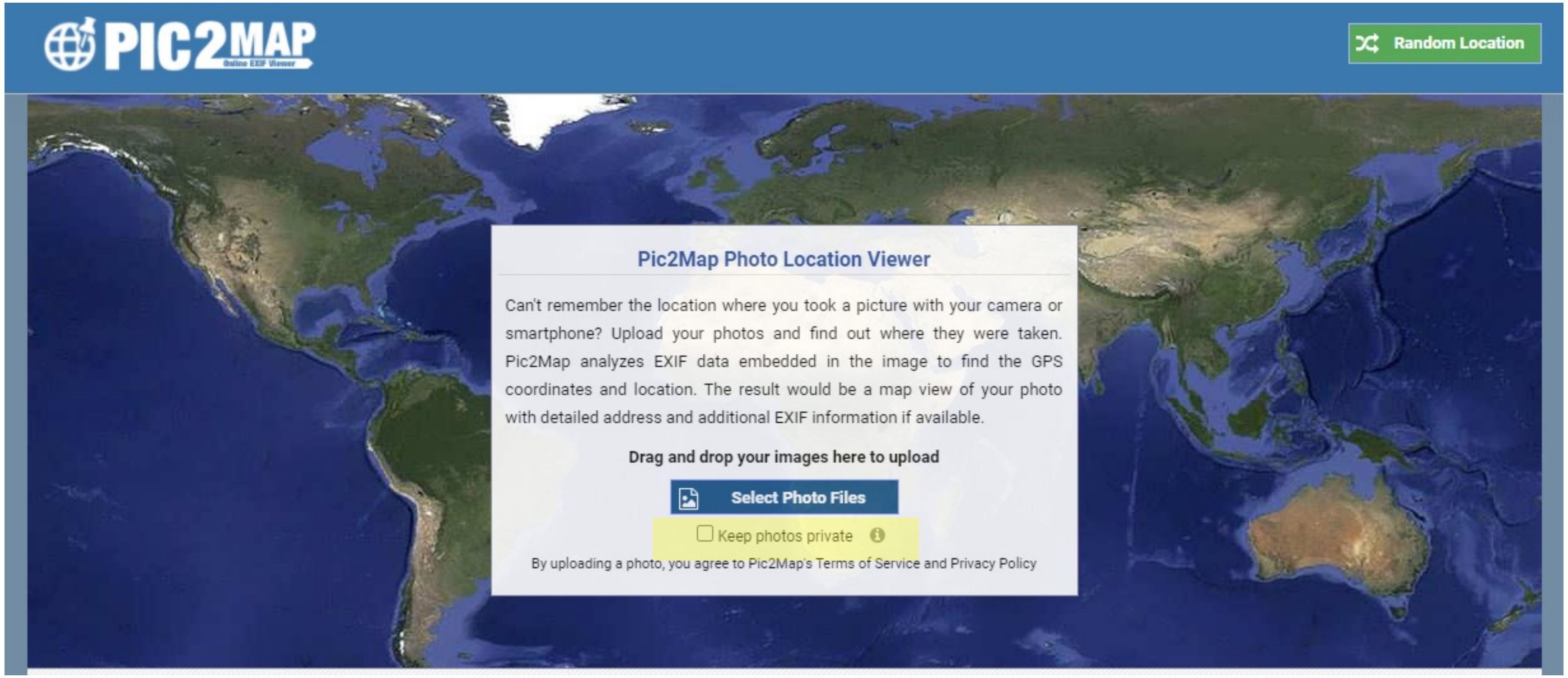
EXIF DATA EXERCISE

- Filename: IMG_3561.JPG



EXIF DATA EXERCISE

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



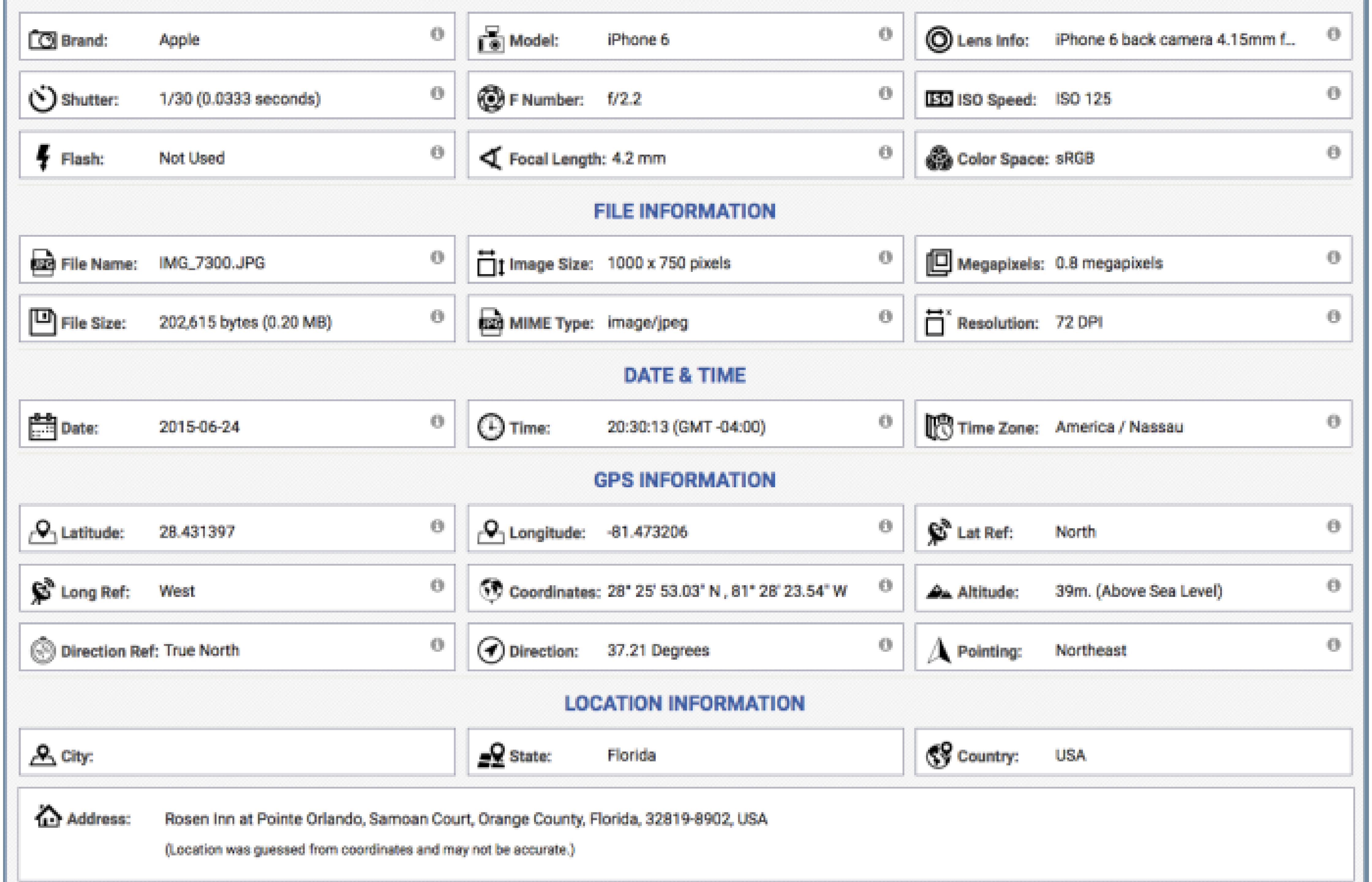
Pic2Map Photo Location Viewer

Can't remember the location where you took a picture with your camera or smartphone? Upload your photos and find out where they were taken. Pic2Map analyzes EXIF data embedded in the image to find the GPS coordinates and location. The result would be a map view of your photo with detailed address and additional EXIF information if available.

Drag and drop your images here to upload

□ Keep photos private

By uploading a photo, you agree to Pic2Map's Terms of Service and Privacy Policy



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

FILE INFORMATION

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

DATE & TIME

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

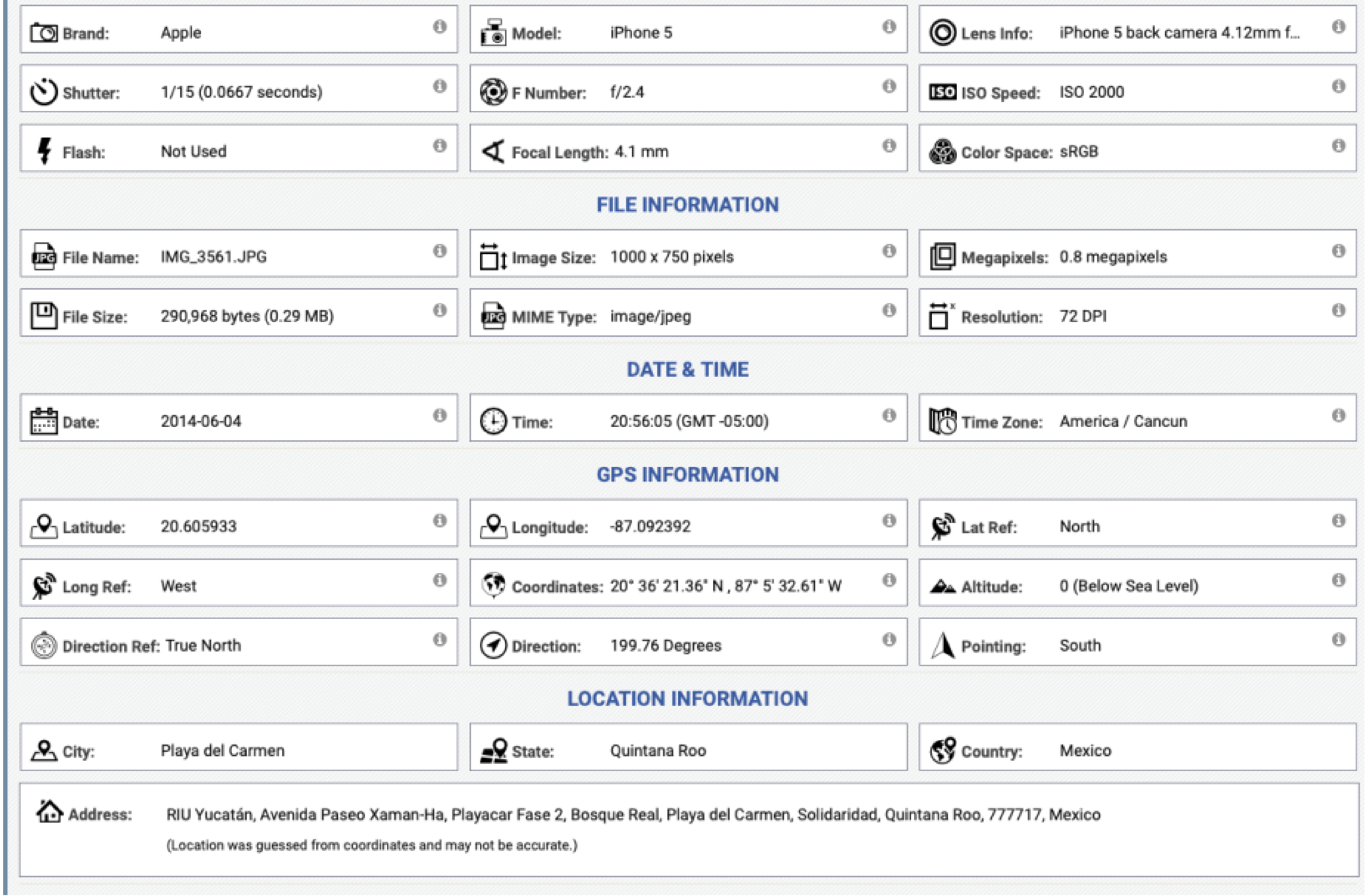
GPS INFORMATION

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

LOCATION INFORMATION

City:	State: Florida	Country: USA

Address: Rosen Inn at Pointe Orlando, Samoan Court, Orange County, Florida, 32819-8902, USA
(Location was guessed from coordinates and may not be accurate.)



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

FILE INFORMATION

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

DATE & TIME

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

GPS INFORMATION

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

LOCATION INFORMATION

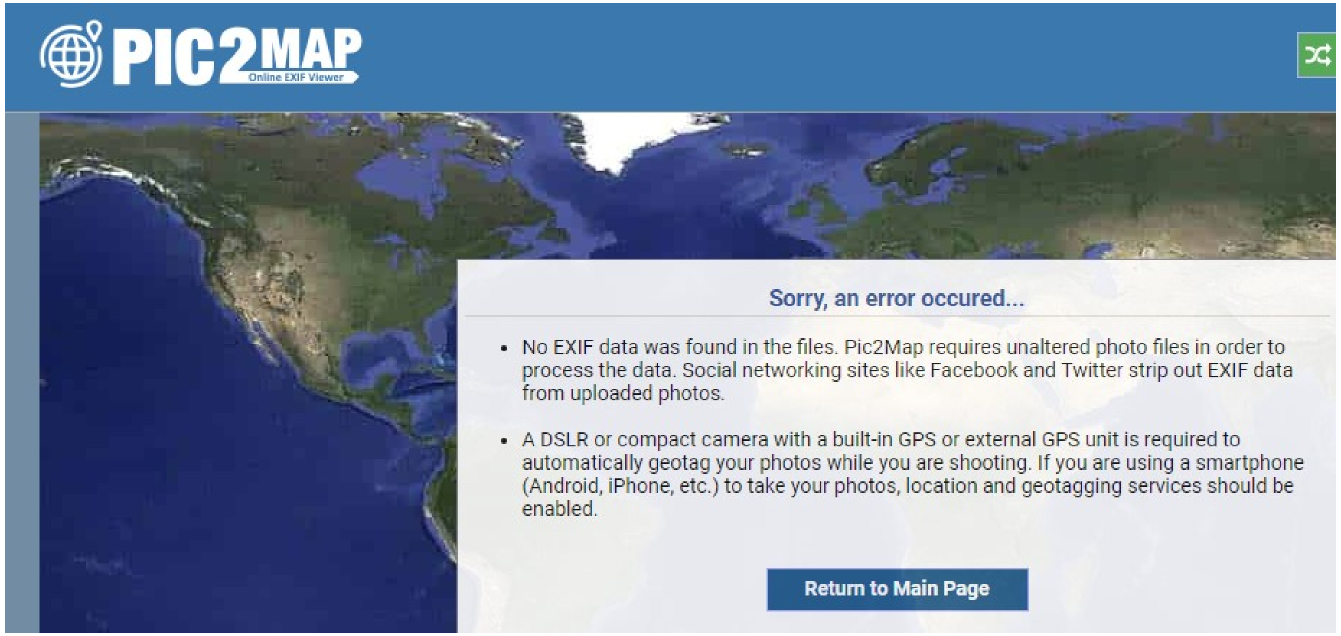
City: Playa del Carmen	State: Quintana Roo	Country: Mexico

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

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

EXIF DATA EXERCISE

- Not all photographs have EXIF Data

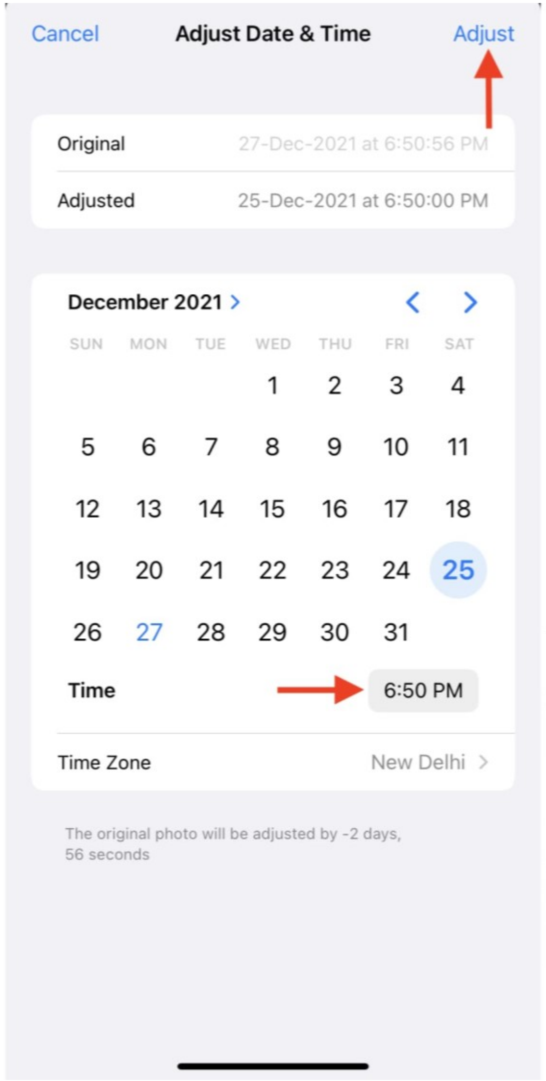


Sorry, an error occured...

- No EXIF data was found in the files. Pic2Map requires unaltered photo files in order to process the data. Social networking sites like Facebook and Twitter strip out EXIF data from uploaded photos.
- A DSLR or compact camera with a built-in GPS or external GPS unit is required to automatically geotag your photos while you are shooting. If you are using a smartphone (Android, iPhone, etc.) to take your photos, location and geotagging services should be enabled.

EXIF DATA REMINDER

- Although most users are not aware of this data, there are also free tools available online which will allow users to:
  - Edit the metadata embedded within a photograph
  - Remove the metadata embedded within a photograph
- As a result, keep in mind that the metadata, including the geo-location data could be altered!
- In iOS16, Apple implemented a feature which allows users to edit EXIF using the native Photos application:
- WhatsApp or Facebook Messenger often strip the metadata from files
  - To reduce file size for transfer



Cancel | Adjust Date & Time | Adjust

Original: 27-Dec-2021 at 6:50:56 PM

Adjusted: 25-Dec-2021 at 6:50:00 PM

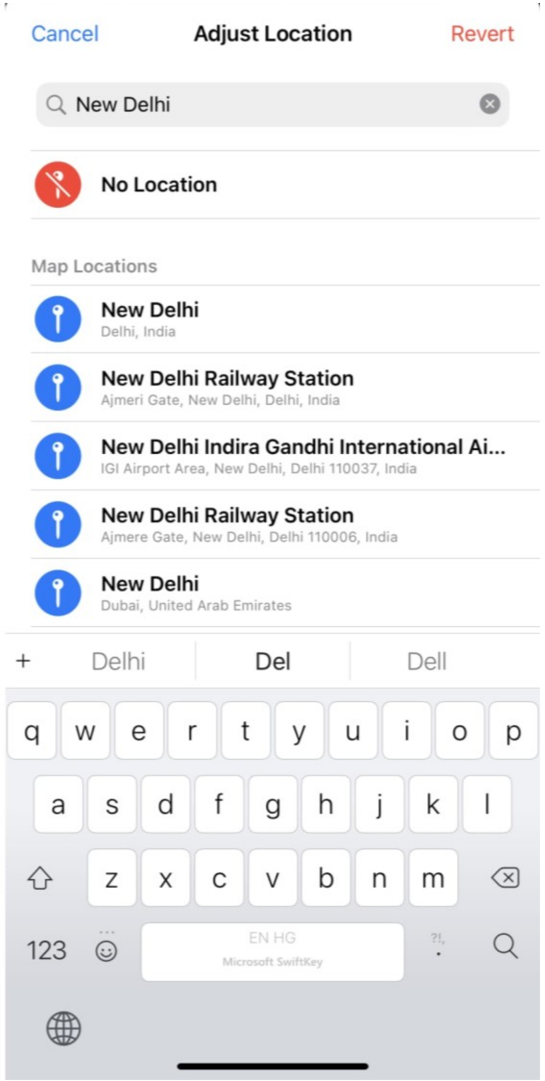
December 2021

SUN	MON	TUE	WED	THU	FRI	SAT
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Time: 6:50 PM

Time Zone: New Delhi

The original photo will be adjusted by -2 days, 56 seconds



Cancel | Adjust Location | Revert

New Delhi

No Location

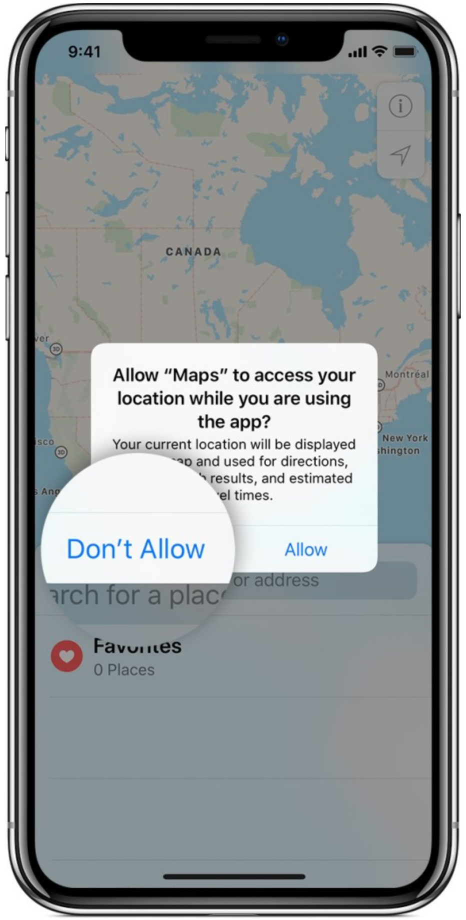
Map Locations

- New Delhi — Delhi, India
- New Delhi Railway Station — Ajmeri Gate, New Delhi, Delhi, India
- New Delhi Indira Gandhi International Ai... — IGI Airport Area, New Delhi, Delhi 110037, India
- New Delhi Railway Station — Ajmere Gate, New Delhi, Delhi 110006, India
- New Delhi — Dubai, United Arab Emirates

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

X - TWITTER

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

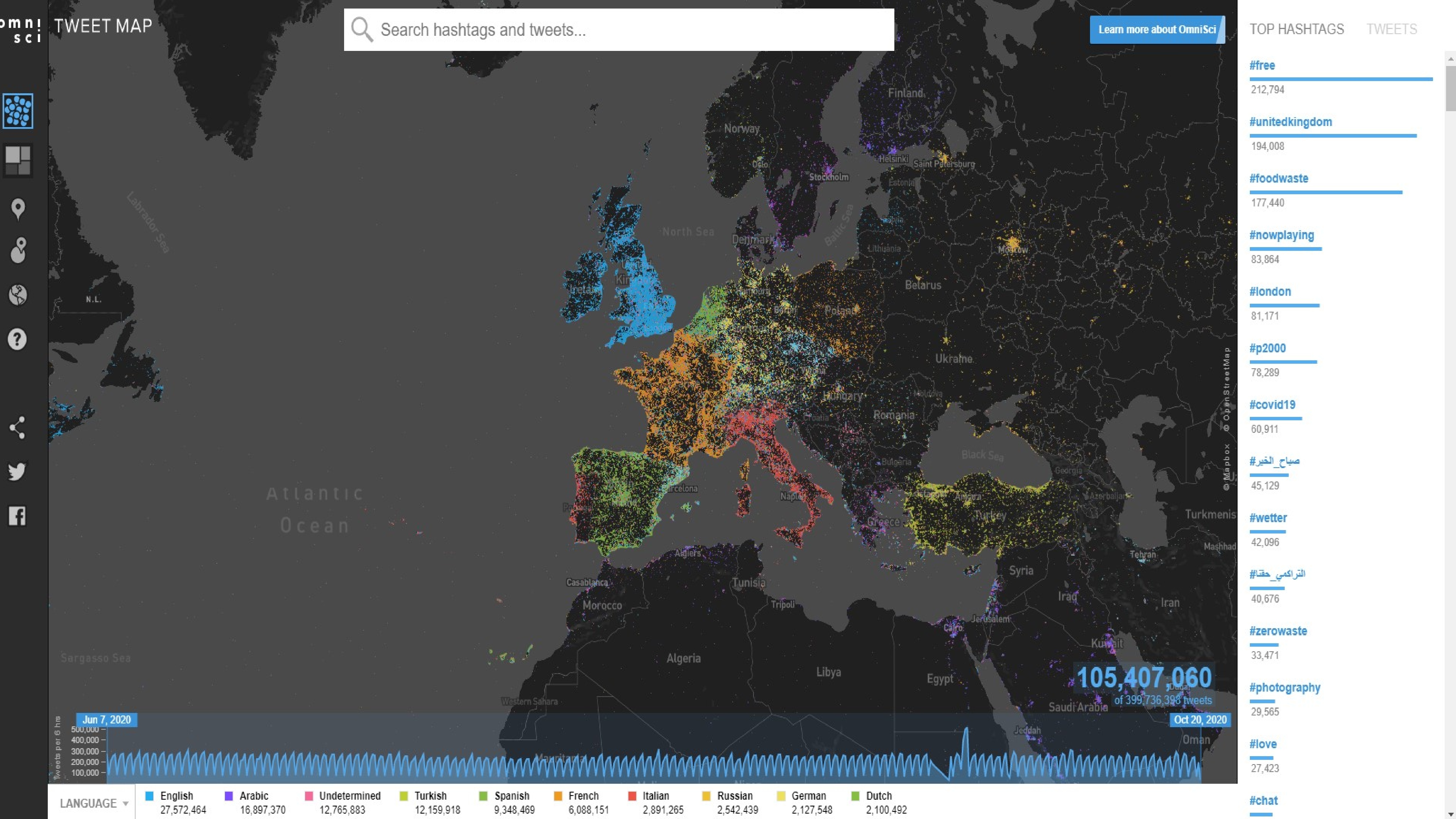


Allow “Maps” to access your location while you are using the app?

Your current location will be displayed ...ap and used for directions, ...h results, and estimated ...el times.

OMNISCI

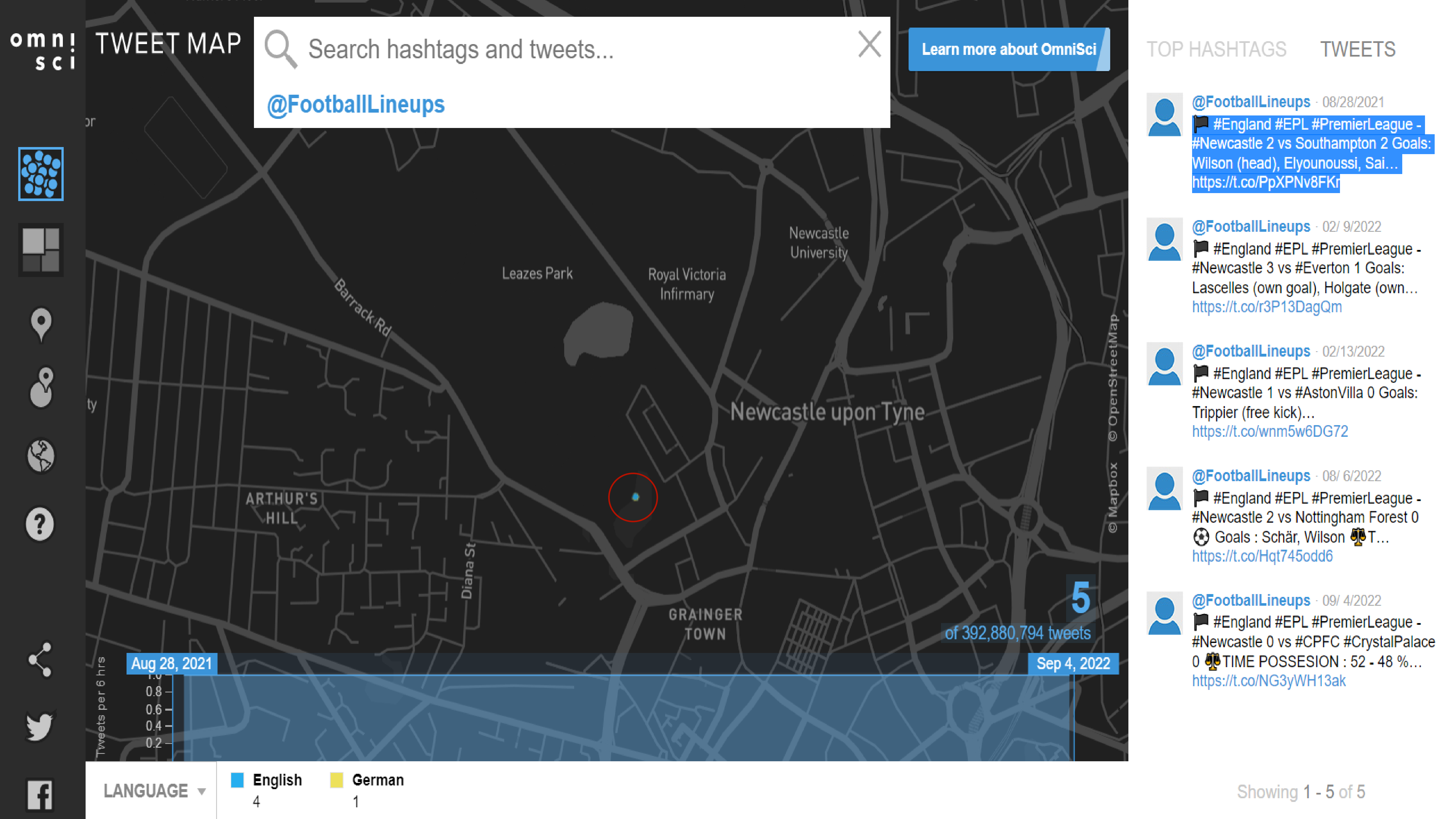
- OMNI SCI is an online tool which allows a user to visualise hundreds of millions of tweets in real time.
- This gives us an understanding of how much location data X tracks
- Provides numerous analytical tools which may be useful during an open source investigation
  - Search by username
  - Search by location
  - Search by content
  - Search by hashtag
- This is one of many tools like this, some have a subscription service, some are free.



#free	212,794
#unitedkingdom	194,008
#foodwaste	177,440
#nowplaying	83,864
#london	81,171
#p2000	78,289
#covid19	60,911
#صباح_الخير	45,129
#wetter	42,096
#التراكمي_حقنا	40,676
#zerowaste	33,471
#photography	29,565
#love	27,423
#chat	

105,407,060
of 399,736,398 tweets

English	Arabic	Undetermined	Turkish	Spanish	French	Italian	Russian	German	Dutch
27,572,464	16,897,370	12,765,883	12,159,918	9,348,469	6,088,151	2,891,265	2,542,439	2,127,548	2,100,492



@FootballLineups

5

of 392,880,794 tweets

🟦 English 4

🟨 German 1

@FootballLineups · 08/28/2021
🏴 #England #EPL #PremierLeague - #Newcastle 2 vs Southampton 2 Goals: Wilson (head), Elyounoussi, Sai… https://t.co/PpXPNv8FKr

@FootballLineups · 02/ 9/2022
🏴 #England #EPL #PremierLeague - #Newcastle 3 vs #Everton 1 Goals: Lascelles (own goal), Holgate (own… https://t.co/r3P13DagQm

@FootballLineups · 02/13/2022
🏴 #England #EPL #PremierLeague - #Newcastle 1 vs #AstonVilla 0 Goals: Trippier (free kick)… https://t.co/wnm5w6DG72

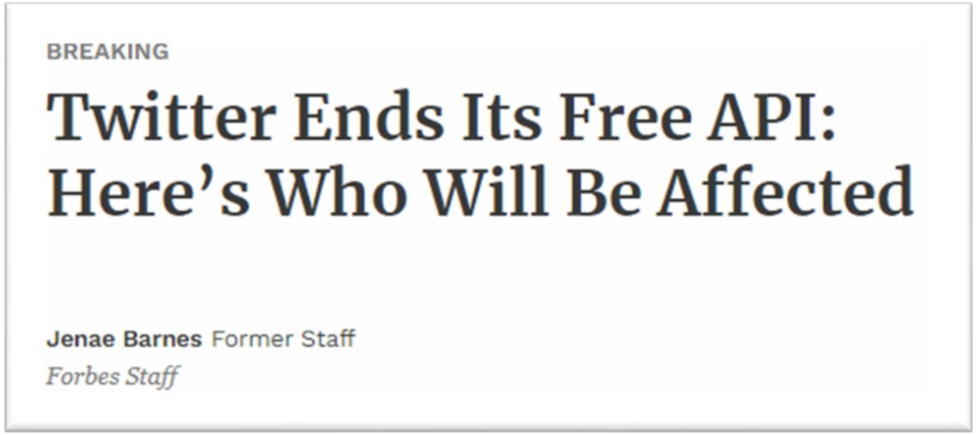
@FootballLineups · 08/ 6/2022
🏴 #England #EPL #PremierLeague - #Newcastle 2 vs Nottingham Forest 0 ⚽ Goals : Schär, Wilson ⚖T… https://t.co/Hqt745odd6

@FootballLineups · 09/ 4/2022
🏴 #England #EPL #PremierLeague - #Newcastle 0 vs #CPFC #CrystalPalace 0 ⚖TIME POSSESION : 52 - 48 %… https://t.co/NG3yWH13ak

Showing 1 - 5 of 5

X (TWITTER) API

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



BREAKING

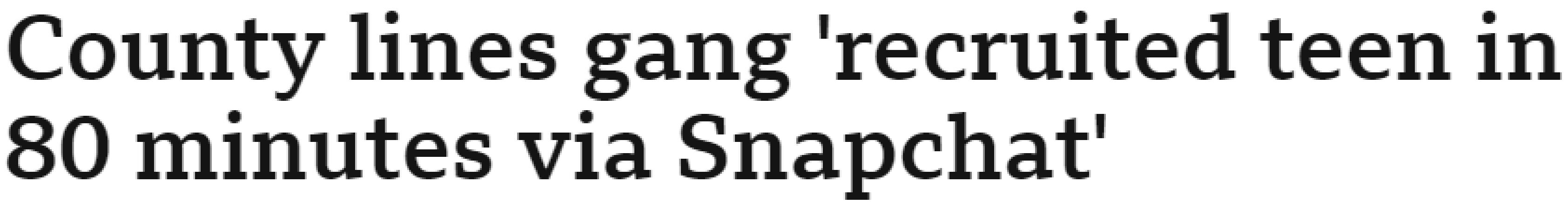
Twitter Ends Its Free API: Here's Who Will Be Affected

Jenae Barnes Former Staff

Forbes Staff

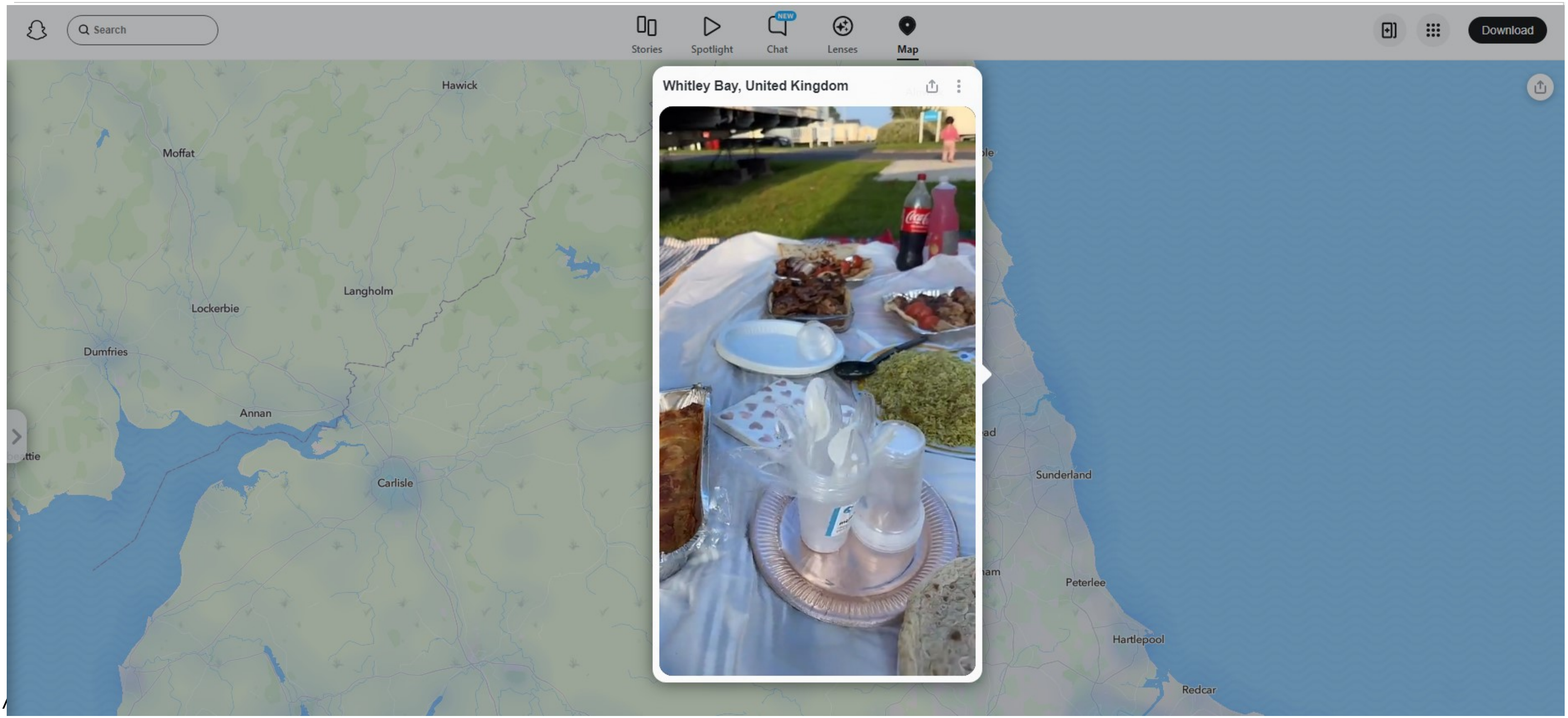
SNAPCHAT

- In 2025 Snapchat had around 900 million monthly active users worldwide
- The application was originally developed for person to person sharing,
  - Since evolved to the use of public stories and other sharing features
- Snapchat launched Snap Map in June 2017, it allows users to see the location of their friends
  - It also allows users to view a world map and view publicly available Snaps
- Snap Map can be accessed on the Snapchat Website
  - Snap Map (snapchat.com) **(Now need a Snapchat login to review Snapmap)**
- Users can use Ghost mode to hide their location and choose not to share their Stories to the public Snap Map.



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

SNAP MAP

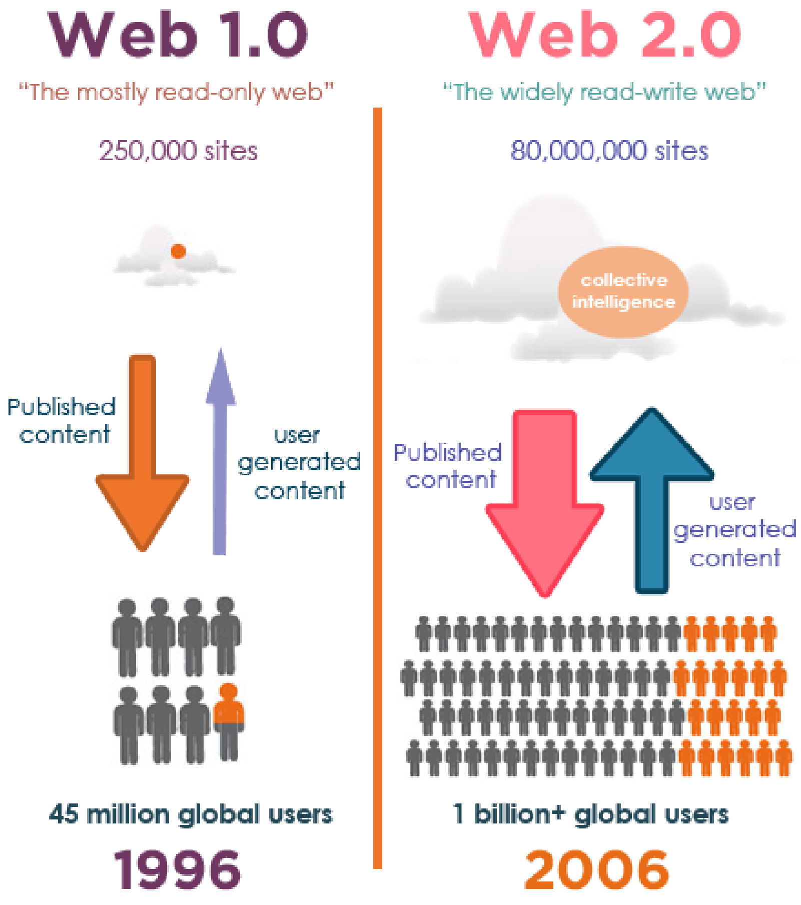


Search
Stories
Spotlight
NEW
Chat
Lenses
Map
Download
Whitley Bay, United Kingdom
Hawick
Moffat
Langholm
Lockerbie
Dumfries
Annan
Carlisle
Sunderland
Peterlee
Hartlepool
Redcar

Investigating Web 2.0 – social networking, blogs and online gaming

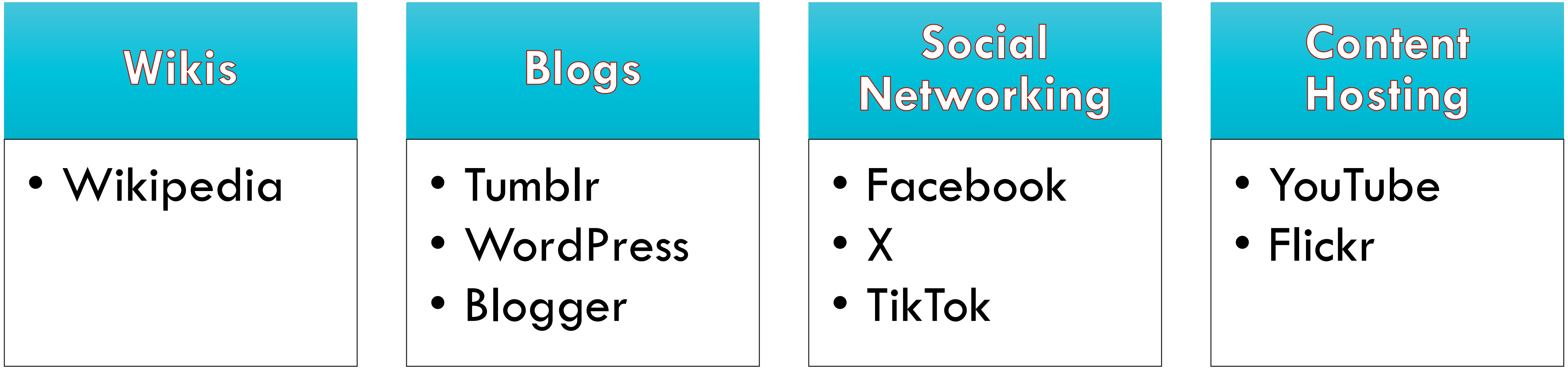
WHAT IS WEB 2.0

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



WEB 2.0 WEBSITES

Examples of web 2.0 websites commonly used:

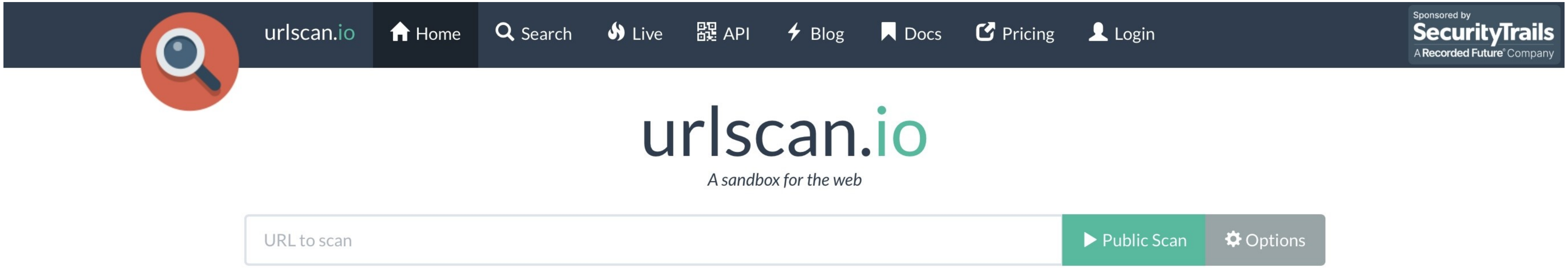


Wikis	Blogs	Social Networking	Content Hosting
• Wikipedia	• Tumblr • WordPress • Blogger	• Facebook • X • TikTok	• YouTube • Flickr

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

URLSCAN

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



www.bbc.co.uk

Back to summary

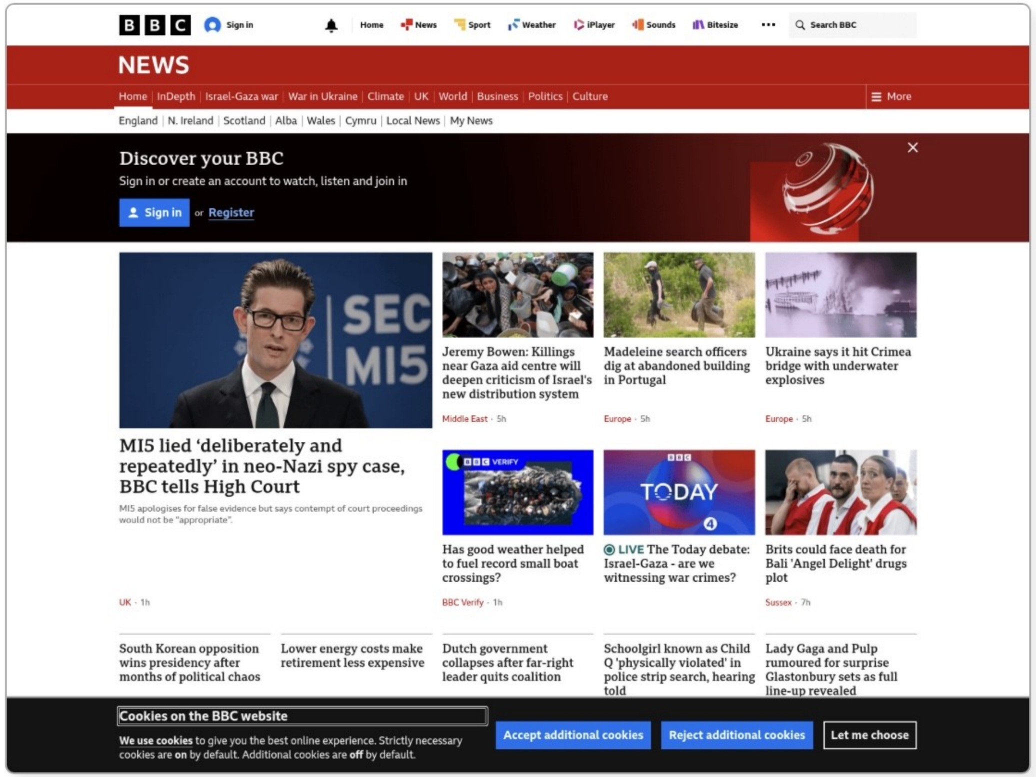
151.101.64.81 Public Scan

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

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

Screenshot during scan

Image



BBC Sign in Home News Sport Weather iPlayer Sounds Bitesize ••• Search BBC

NEWS

Home | InDepth | Israel-Gaza war | War in Ukraine | Climate | UK | World | Business | Politics | Culture | More

England | N. Ireland | Scotland | Alba | Wales | Cymru | Local News | My News

Discover your BBC

Sign in or create an account to watch, listen and join in

Sign in or Register

MI5 lied 'deliberately and repeatedly' in neo-Nazi spy case, BBC tells High Court

MI5 apologises for false evidence but says contempt of court proceedings would not be "appropriate".

UK · 1h

Jeremy Bowen: Killings near Gaza aid centre will deepen criticism of Israel's new distribution system

Middle East · 5h

Madeleine search officers dig at abandoned building in Portugal

Europe · 5h

Ukraine says it hit Crimea bridge with underwater explosives

Europe · 5h

Has good weather helped to fuel record small boat crossings?

BBC Verify · 1h

LIVE The Today debate: Israel-Gaza - are we witnessing war crimes?

Brits could face death for Bali 'Angel Delight' drugs plot

Sussex · 7h

South Korean opposition wins presidency after months of political chaos

Lower energy costs make retirement less expensive

Dutch government collapses after far-right leader quits coalition

Schoolgirl known as Child Q 'physically violated' in police strip search, hearing told

Lady Gaga and Pulp rumoured for surprise Glastonbury sets as full line-up revealed

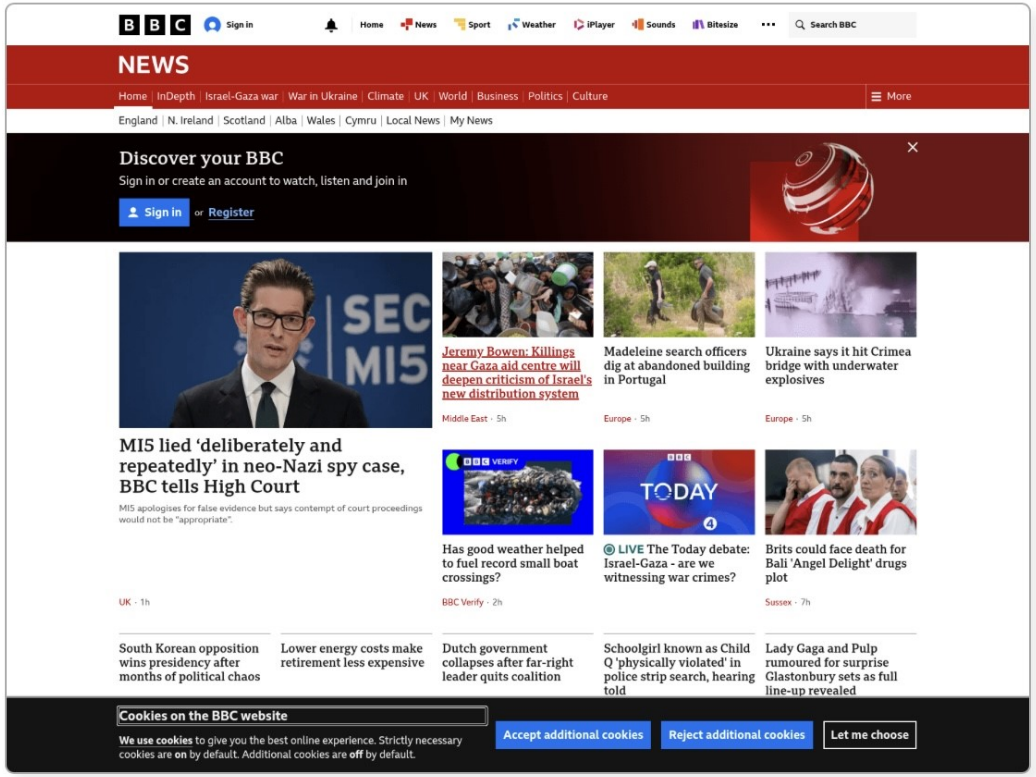
Cookies on the BBC website

We use cookies to give you the best online experience. Strictly necessary cookies are on by default. Additional cookies are off by default.

Accept additional cookies Reject additional cookies Let me choose

Screenshot now Submitted URL

Image



BBC Sign in Home News Sport Weather iPlayer Sounds Bitesize ••• Search BBC

NEWS

Home | InDepth | Israel-Gaza war | War in Ukraine | Climate | UK | World | Business | Politics | Culture | More

England | N. Ireland | Scotland | Alba | Wales | Cymru | Local News | My News

Discover your BBC

Sign in or create an account to watch, listen and join in

Sign in or Register

MI5 lied 'deliberately and repeatedly' in neo-Nazi spy case, BBC tells High Court

MI5 apologises for false evidence but says contempt of court proceedings would not be "appropriate".

UK · 1h

Jeremy Bowen: Killings near Gaza aid centre will deepen criticism of Israel's new distribution system

Middle East · 5h

Madeleine search officers dig at abandoned building in Portugal

Europe · 5h

Ukraine says it hit Crimea bridge with underwater explosives

Europe · 5h

Has good weather helped to fuel record small boat crossings?

BBC Verify · 2h

LIVE The Today debate: Israel-Gaza - are we witnessing war crimes?

Brits could face death for Bali 'Angel Delight' drugs plot

Sussex · 7h

South Korean opposition wins presidency after months of political chaos

Lower energy costs make retirement less expensive

Dutch government collapses after far-right leader quits coalition

Schoolgirl known as Child Q 'physically violated' in police strip search, hearing told

Lady Gaga and Pulp rumoured for surprise Glastonbury sets as full line-up revealed

Cookies on the BBC website

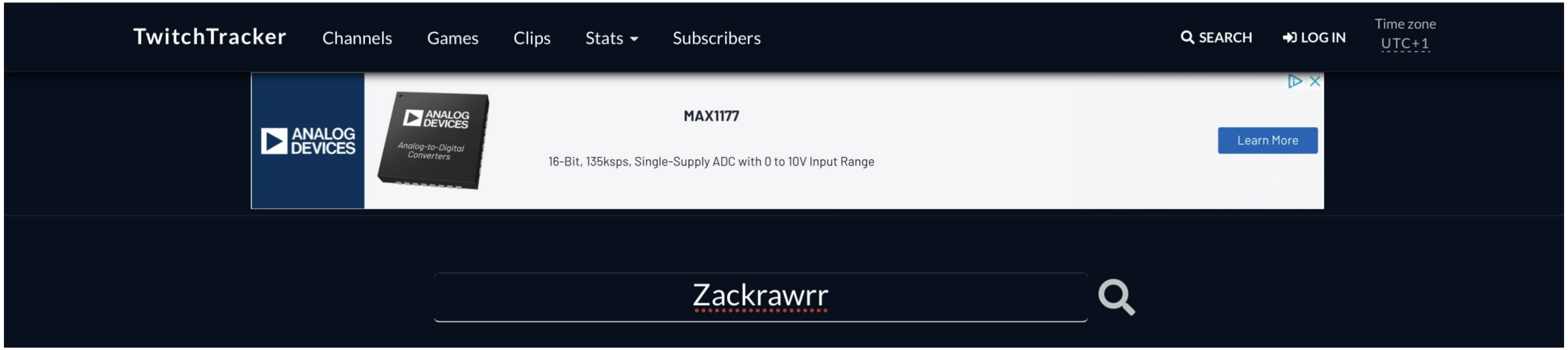
We use cookies to give you the best online experience. Strictly necessary cookies are on by default. Additional cookies are off by default.

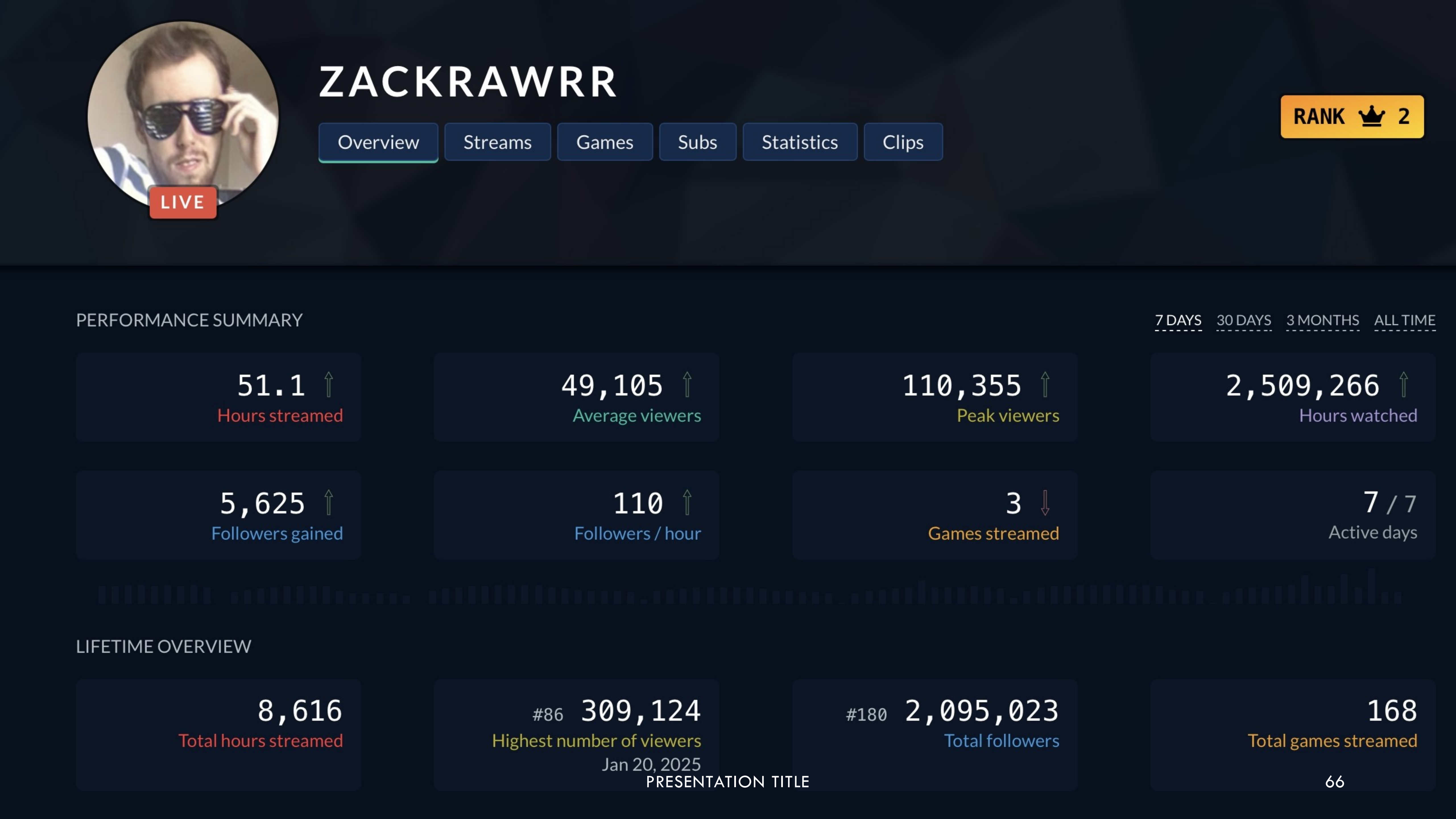
Accept additional cookies Reject additional cookies Let me choose

IPs Countries Transfer Size Cookies

TWITCH

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





ZACKRAWRR

PERFORMANCE SUMMARY

51.1 ↑
Hours streamed

49,105 ↑
Average viewers

110,355 ↑
Peak viewers

2,509,266 ↑
Hours watched

5,625 ↑
Followers gained

110 ↑
Followers / hour

3 ↓
Games streamed

7 / 7
Active days

LIFETIME OVERVIEW

8,616
Total hours streamed

#86 309,124
Highest number of viewers
Jan 20, 2025

#180 2,095,023
Total followers

168
Total games streamed

INSTAGRAM

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

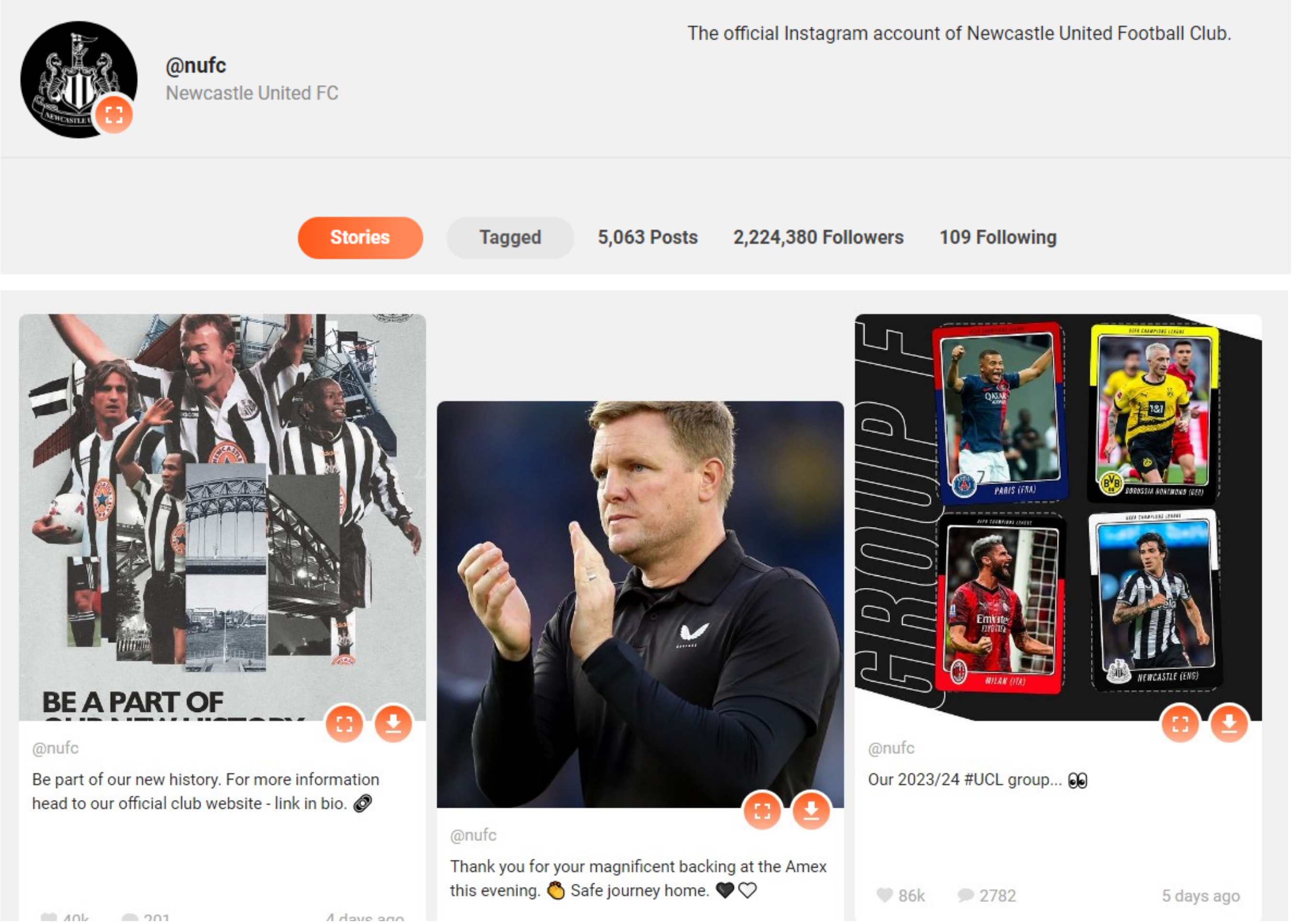
INSTAGRAM EXERCISE

Instagram Exercise 1

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

Step 2) Enter “nufc” search for the profile

Can we see the profile?



The official Instagram account of Newcastle United Football Club.

@nufc

Newcastle United FC

5,063 Posts 2,224,380 Followers 109 Following

@nufc

Be part of our new history. For more information head to our official club website - link in bio. 🔗

@nufc

Thank you for your magnificent backing at the Amex this evening. 👏 Safe journey home. 🖤🤍

@nufc

Our 2023/24 #UCL group... 👀

86k 2782 5 days ago

INSTAGRAM EXERCISE

Instagram Exercise 2

If you have an Instagram account, try the following

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

Step 2) Enter your Instagram name and review your profile

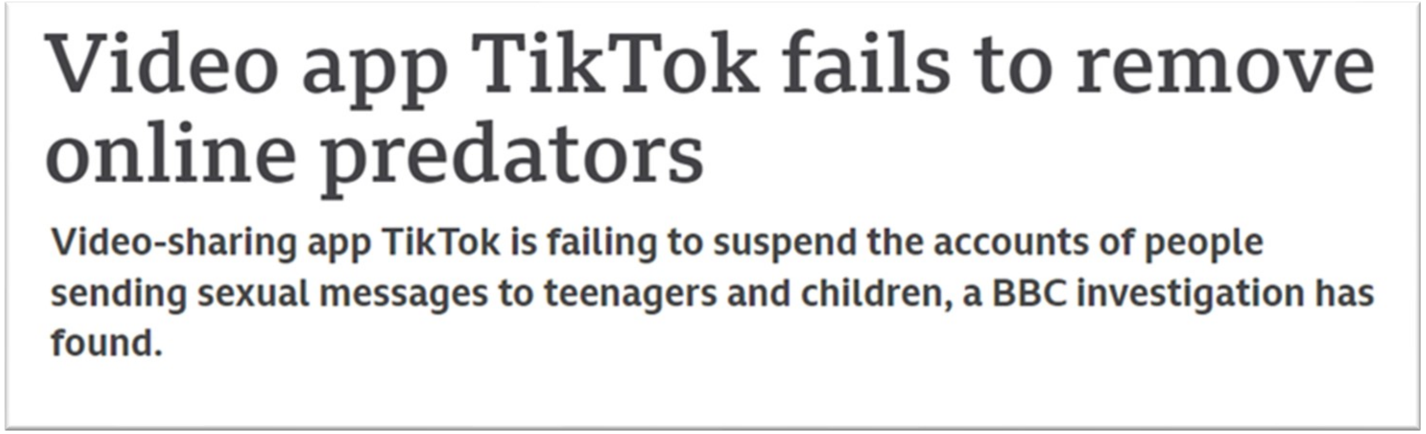
Can we see the profile?

FACEBOOK

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

TIKTOK

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

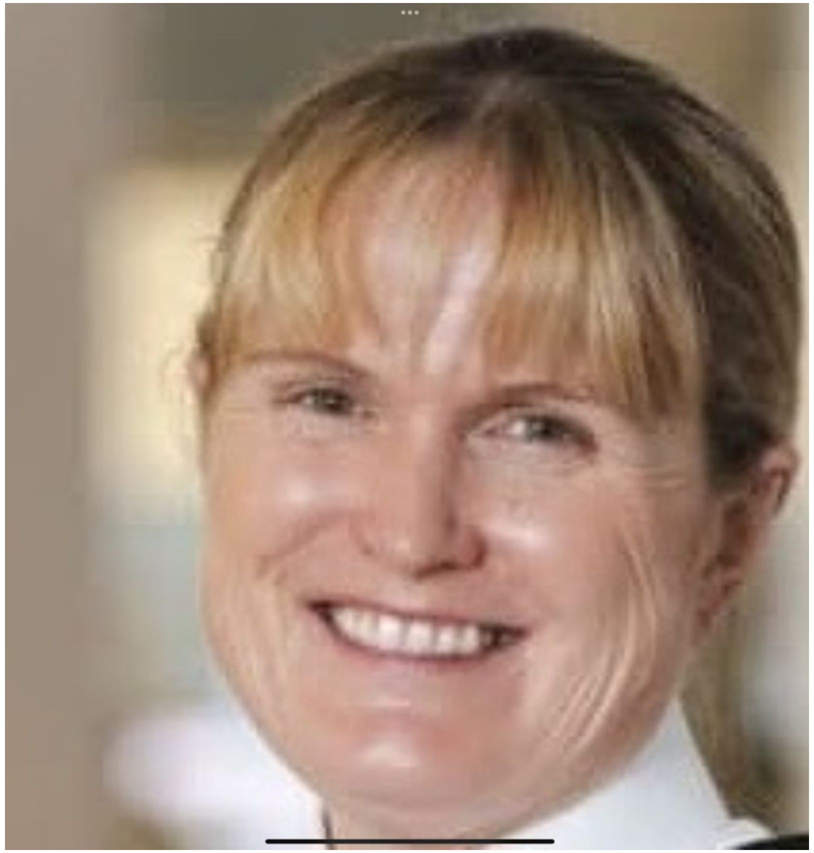


Video app TikTok fails to remove online predators

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

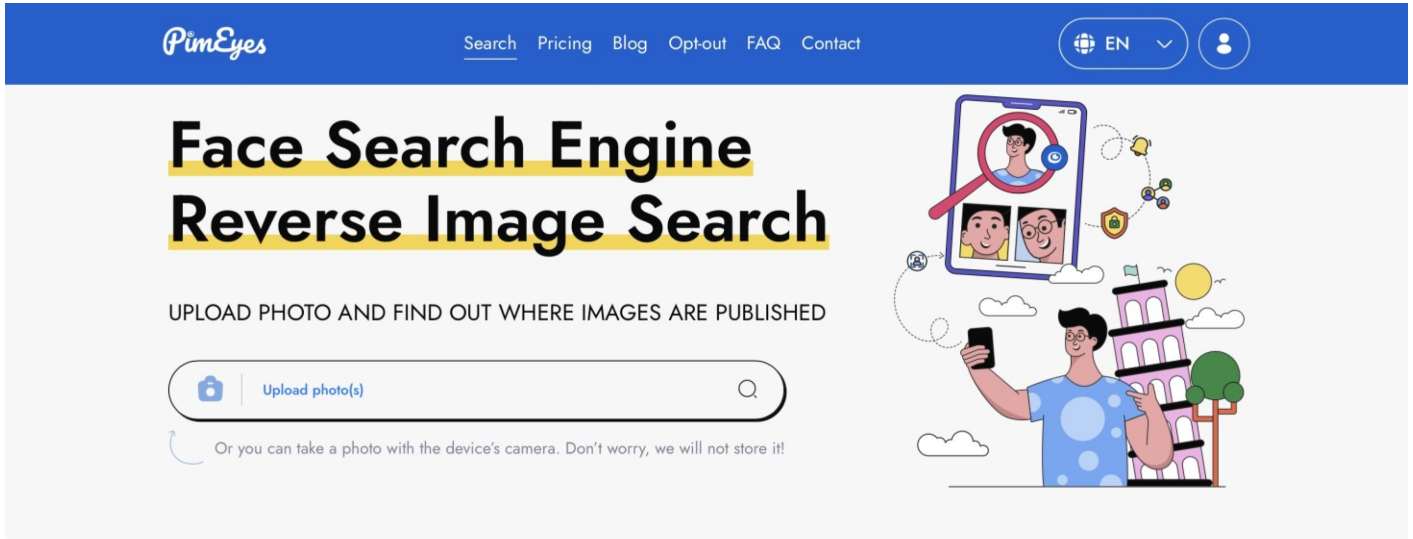
TIKTOK EXERCISE

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



TIKTOK EXERCISE

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

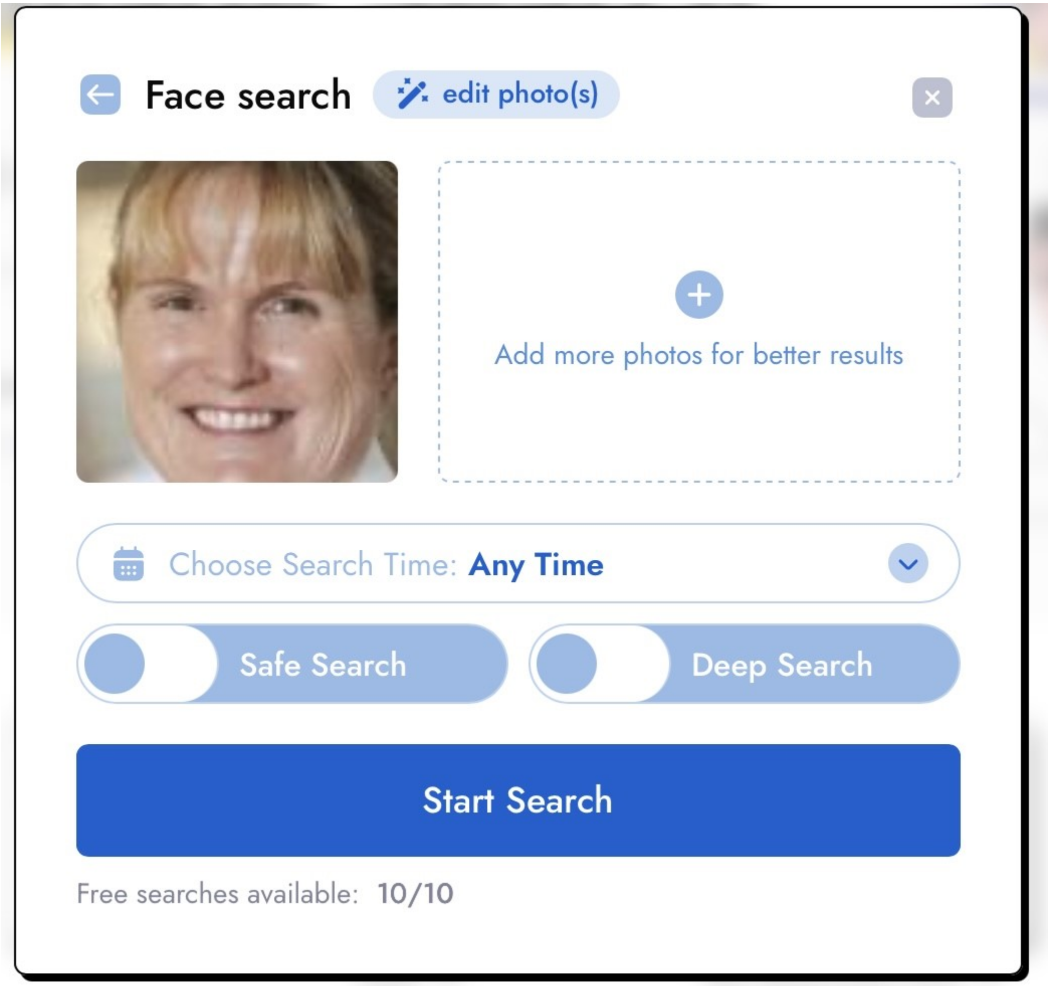


Face Search Engine
Reverse Image Search

UPLOAD PHOTO AND FIND OUT WHERE IMAGES ARE PUBLISHED

Or you can take a photo with the device's camera. Don't worry, we will not store it!

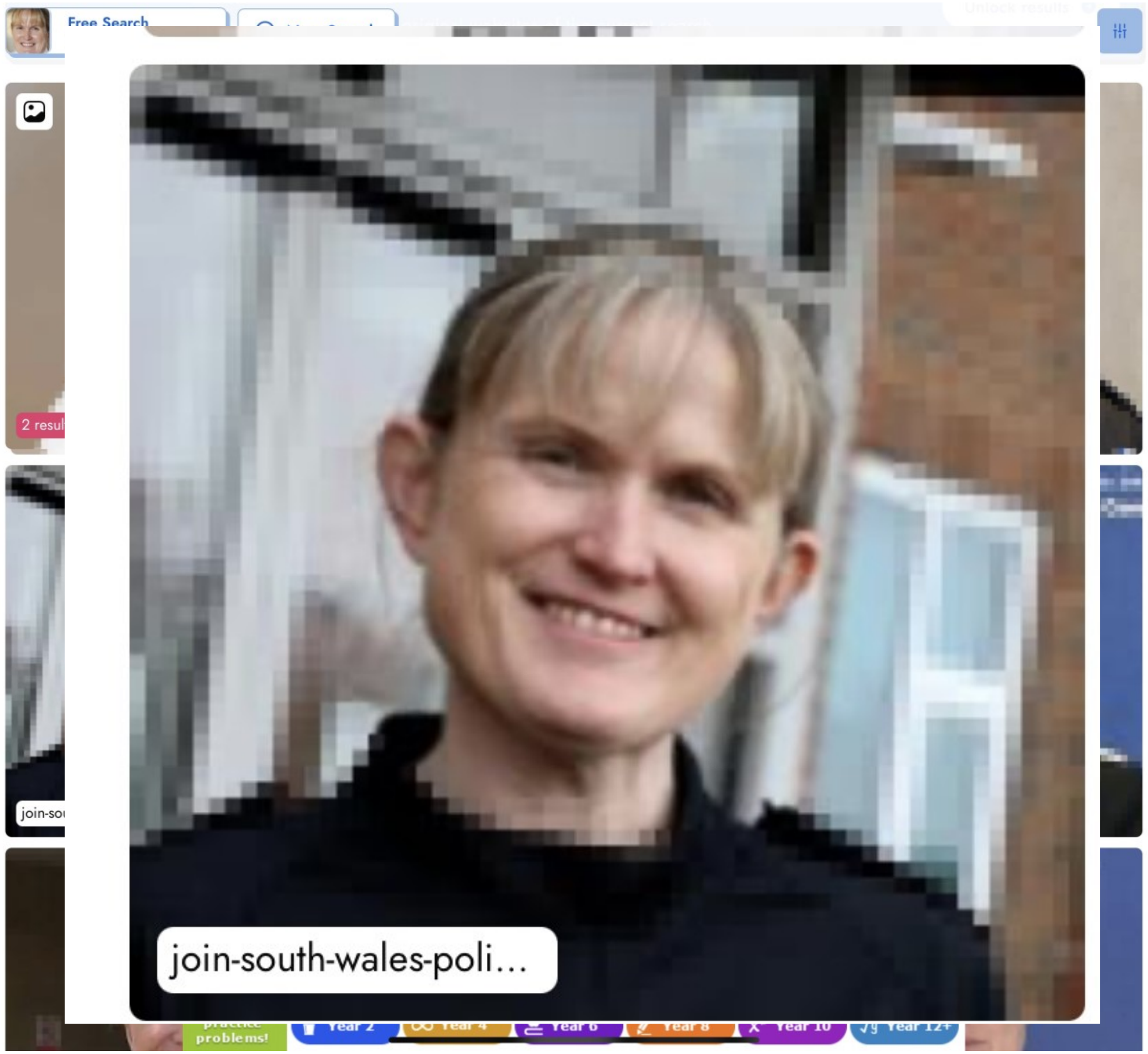
TIKTOK EXERCISE



Face search

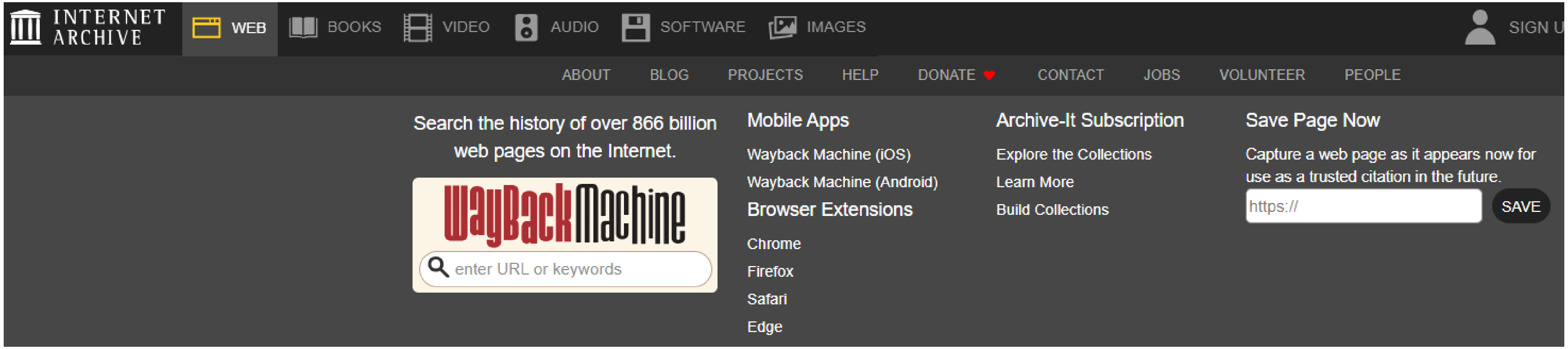
Choose Search Time: Any Time

Free searches available: 10/10



TIKTOK POST CAPTURE

- Wayback machine offers a useful tool for capturing web pages
- Can be used to capture TikTok posts on the web version



Search the history of over 866 billion web pages on the Internet.

Capture a web page as it appears now for use as a trusted citation in the future.

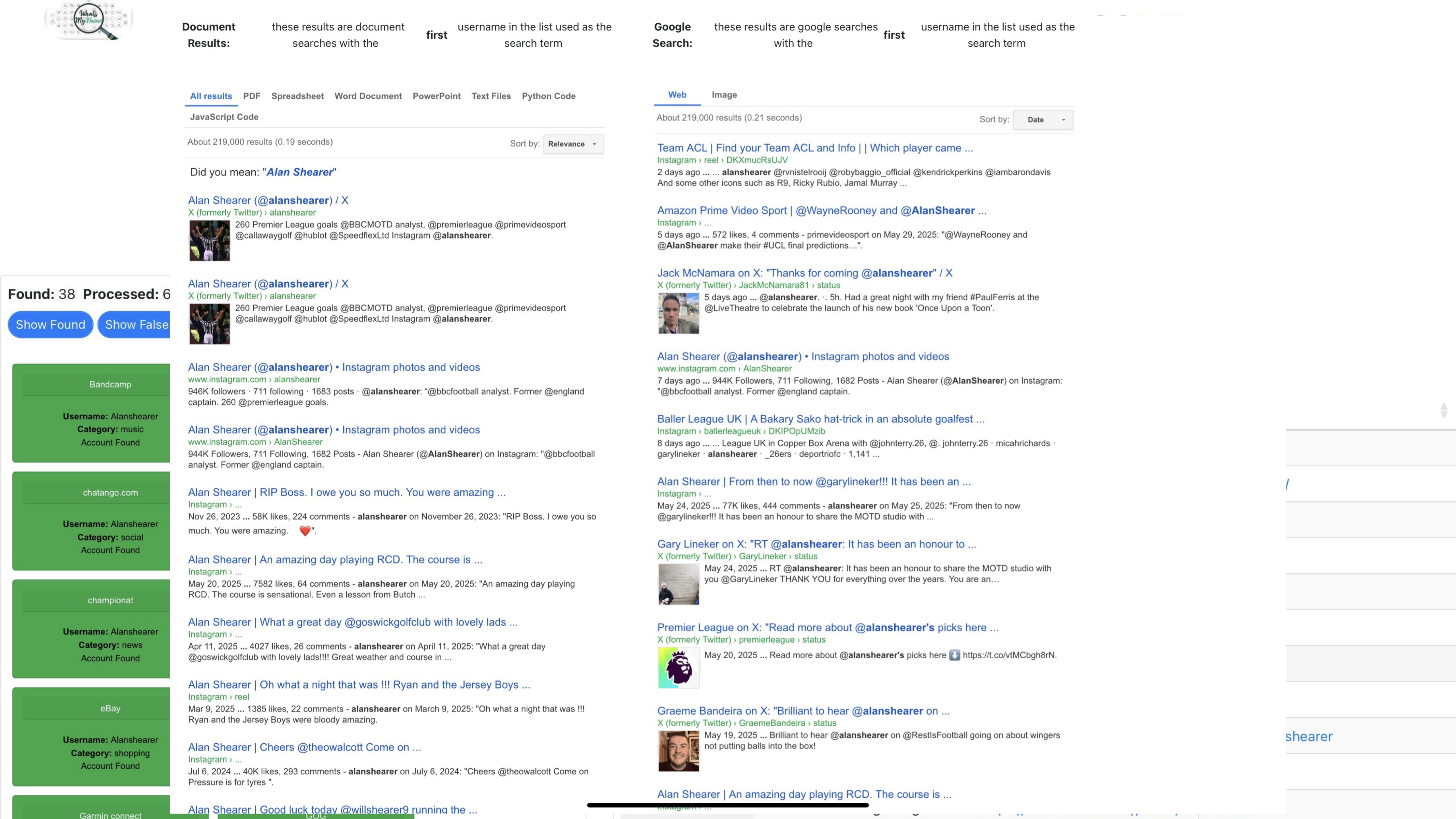
- Conducting an opensource investigation on TikTok Web Version has limitations
  - Web browser version wont show the comments
  - Full content is available the TikTok app

GOOGLE

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

ONLINE USERNAMES

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



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

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

Found: 38 **Processed:** 6

Bandcamp

Username: Alanshearer
Category: music
Account Found

chatango.com

Username: Alanshearer
Category: social
Account Found

championat

Username: Alanshearer
Category: news
Account Found

eBay

Username: Alanshearer
Category: shopping
Account Found

Garmin connect

About 219,000 results (0.19 seconds)

Sort by: Relevance

Did you mean: "*Alan Shearer*"

Alan Shearer (@**alanshearer**) / X
X (formerly Twitter) › alanshearer
260 Premier League goals @BBCMOTD analyst, @premierleague @primevideosport @callawaygolf @hublot @SpeedflexLtd Instagram @**alanshearer**.

Alan Shearer (@**alanshearer**) / X
X (formerly Twitter) › alanshearer
260 Premier League goals @BBCMOTD analyst, @premierleague @primevideosport @callawaygolf @hublot @SpeedflexLtd Instagram @**alanshearer**.

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

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

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

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

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

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

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

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

About 219,000 results (0.21 seconds)

Sort by: Date

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

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

Jack McNamara on X: "Thanks for coming @**alanshearer**" / X
X (formerly Twitter) › JackMcNamara81 › status
5 days ago ... @**alanshearer**. ·. 5h. Had a great night with my friend #PaulFerris at the @LiveTheatre to celebrate the launch of his new book 'Once Upon a Toon'.

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

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

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

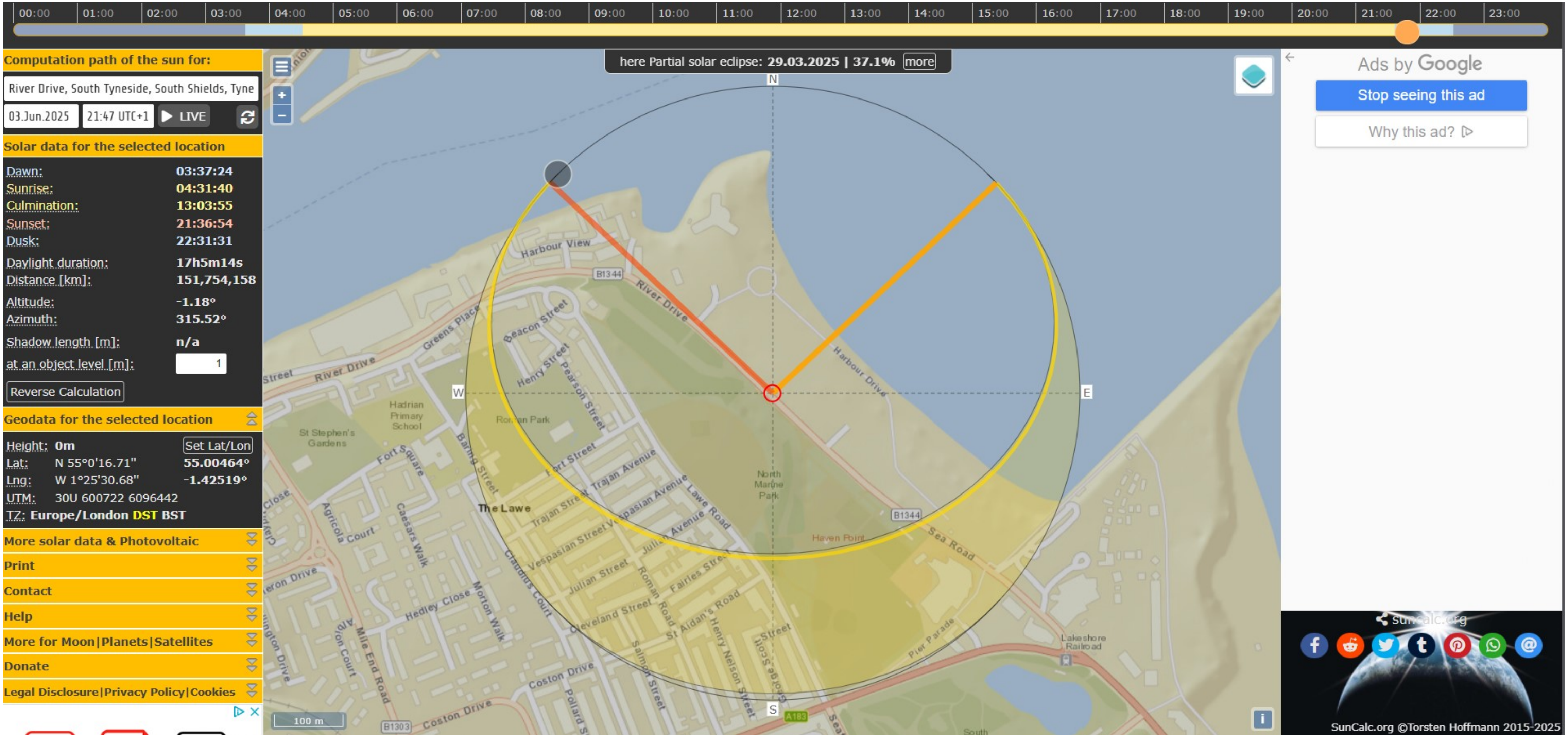
Gary Lineker on X: "RT @**alanshearer**: It has been an honour to ...
X (formerly Twitter) › GaryLineker › status
May 24, 2025 ... RT @**alanshearer**: It has been an honour to share the MOTD studio with you @GaryLineker THANK YOU for everything over the years. You are an…

Premier League on X: "Read more about @**alanshearer's** picks here ...
X (formerly Twitter) › premierleague › status
May 20, 2025 ... Read more about @**alanshearer's** picks here ⬇️ https://t.co/vtMCbgh8rN.

Graeme Bandeira on X: "Brilliant to hear @**alanshearer** on ...
X (formerly Twitter) › GraemeBandeira › status
May 19, 2025 ... Brilliant to hear @**alanshearer** on @RestIsFootball going on about wingers not putting balls into the box!

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

THE POWER OF OSINT



Computation path of the sun for:

River Drive, South Tyneside, South Shields, Tyne

03.Jun.2025 | 21:47 UTC+1 | ▶ LIVE

Solar data for the selected location

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

Reverse Calculation

Geodata for the selected location

Height:	0m	Set Lat/Lon
Lat:	N 55°0'16.71"	55.00464°
Lng:	W 1°25'30.68"	-1.42519°
UTM:	30U 600722 6096442	
TZ:	Europe/London DST BST	

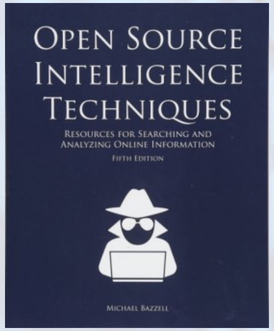
here Partial solar eclipse: 29.03.2025 | 37.1% more

THANK YOU
ANY QUESTIONS?

Seanpaul Gilroy

Useful Resources

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


Open Source Intelligence Techniques
Resources for Searching and Analyzing Online Information
Fifth Edition
Michael Bazzell

ChatGPT

FACULTY
OF LAW
Charles University

Co-funded by
the European Union

Charles University, Faculty of Law

nám. Curieových 901/7, 116 40 Prague 1

An overview of the defence rights-related issues regarding the use of e-evidence

prof. JUDr. Tomáš Gřivna, Ph.D.

JUDr. Martin Richter, Ph.D.

FACULTY
OF LAW
Charles University

RIGHT TO A FAIR TRIAL (ARTICLE 6 ECHR)

- The use of electronic evidence does not in itself violate the right to a fair trial, provided that the key principles are respected.
  - Legality of obtaining evidence.
  - The right to an adversarial procedure.
  - Equality of arms.
  - Justification of the credibility and relevance of the electronic evidence.

RIGHT TO A FAIR TRIAL (ARTICLE 6 ECHR)

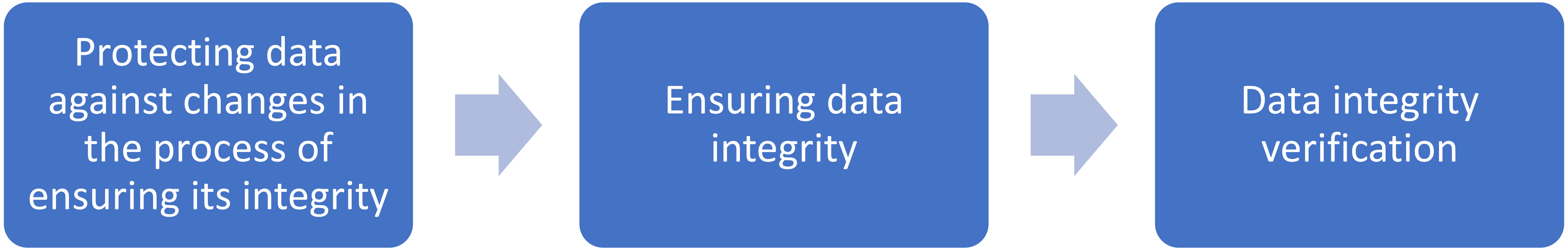
- Dragojević v Croatia.
- Bykov v. Russia.

RIGHT OF ACCESS TO EVIDENCE AND CHALLENGE EVIDENCE

- Full access to exculpatory e-evidence.
- Timely disclosure of digital materials gathered by prosecution.
- The right to a real opportunity to verify the reliability of data = chain of custody.

CHAIN OF CUSTODY

Defence must be able to scrutinize how the data was obtained and preserved.



Protecting data against changes in the process of ensuring its integrity

Ensuring data integrity

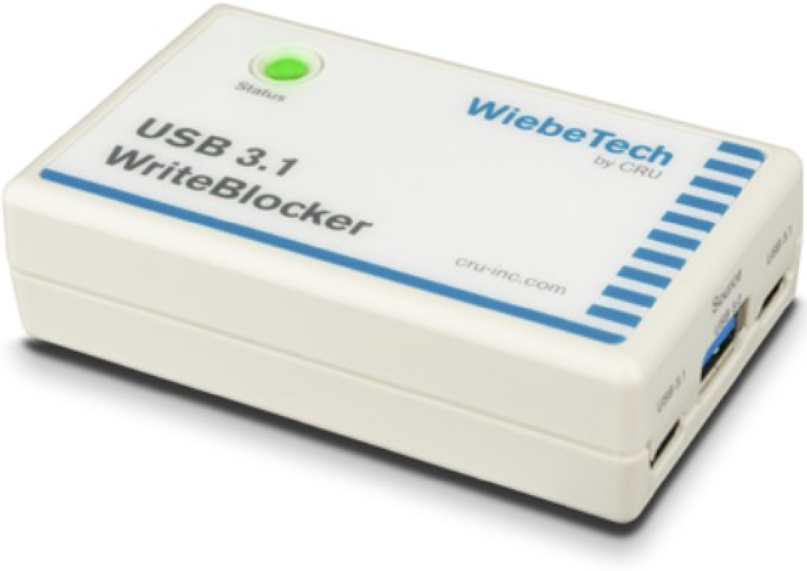
Data integrity verification

CHAIN OF CUSTODY – WHAT ARE WE AFRAID OF?

Prosecution of Mr. Hala

- The case of the criminally prosecuted former director of a state corporation.
- Originally investigated for economic crimes.
- Finally prosecuted for possession of child pornography based on falsified data.

WRITE BLOCKER



Source: https://forenzniprodukty.cz/produkt/cru-wiebetech-usb-3-1-writeblocker/

BITSTREAM IMAGE

HASH

LEGAL PROBLEM = FORENSIC EXPERT (EXPERT WITNESS) GATES RUBBER CO. V. BANDO CHEMICAL INDUSTRY, 1996

- Copyright infringement, embezzlement
- When the expert examined the PC, he copied a program (Norton's Unerase) onto it, which randomly erased 7-8% of the information from the hard drive.
- Question: Does failure to make a copy of the hard drive render the evidence unusable?
- Colorado District Court: Yes, there is an obligation to use the method that produces the most complete and accurate results. It is essential to ensure that the integrity of the electronic evidence is maintained and that it is verifiable.

BREACH OF CHAIN OF CUSTODY

- Is the electronic evidence inadmissible in a criminal proceeding?
- Is it a deal only when the evidence was seized by the police?

JURISDICTIONAL CONFLICTS

DATA JURISDICTION
IN CRIMINAL INVESTIGATIONS
WHERE ARE THE DATA LOCATED?
FROM WHERE ARE THE DATA ACCESSIBLE?
Country A
Country B

FACULTY
OF LAW
Charles University

INTERNATIONAL COOPERATION

- EncroChat encrypted communication network uncovered by police in 2017
  - Arrested more then 6.000 people worldwide.
  - Confiscation of 740 milion EUR.
  - Confiscation of 100 tons of cocaione.
  - Confiscation of 740 milion EUR.
  - Confiscation of 30 milion pils and drugs.

VIOLATION OF THE FUNDAMENTAL HUMAN RIGHT TO PRIVACY

- Případ Macharik proti České republice

ELECTRONIC EVIDENCE - SEIZURE IN THE CZECH REPUBLIC

- There are two distinct models for the use of procedural institutes (tools) that are applicable today for securing the same category of data. Each of these models provides a different level of procedural guarantees.
- The applicability of one or the other model of the use of procedural institutes depends on one circumstance, namely whether the police have succeeded in securing a tangible data carrier.
- In the Czech Republic, it is assumed that the material carrier has been properly seized in accordance with the Criminal Procedure Code (surrender of the item, removal of the item, search, etc.).

EXAMPLE – SEIZURE OF A LAPTOP

- The data stored on the laptop's hard drive can be retrieved by simply looking at it. This is not the case for message traffic data (e.g. emails), which is only stored on the laptop hard drive after it has been secured by an Internet connection, which can only be secured as an wiretapping.
- Data only apparently stored on the laptop but actually located on remote storage can only be retrieved with the judge's consent (e.g. emails, some files in OneDrive, iCloud Drive).
- Data captured without the user's involvement in the so-called "cache", i.e. located on the laptop's hard disk, can be retrieved by simply looking at it, as well as deleted data.

DE LEGE FERENDA

✓ **Operational data**

arise automatically when the device is used, against the user's will or independently

User data

data intentionally created by the user (free access VS. private data)

Thank you for your attention

richterm@prf.cuni.cz

Generalstaatsanwaltschaft Frankfurt am Main
- Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) -

HESSEN

ERA

#DIGITALISATION and #ARTIFICIAL INTELLIGENCE in Criminal Justice
Prague, 12-13 June 2025

Using electronic evidence and AI in criminal investigations and presenting it in court

Senior Public Prosecutor Linda Bertram

Co-funded by the European Union

HESSEN
GENERALSTAATSANWALTSCHAFT FRANKFURT AM MAIN
ZIT

TEAM ILA

WE DISCONNECT.
WORLDWIDE.

Artificial Intelligence in criminal proceedings

Source:www.vidhikarya.com

Artificial Intelligence in criminal proceedings
Legal framework

Numerous approaches are being developed around the world to make the use of artificial intelligence trustworthy.

Two regulatory initiatives stand out due to their binding legal character:

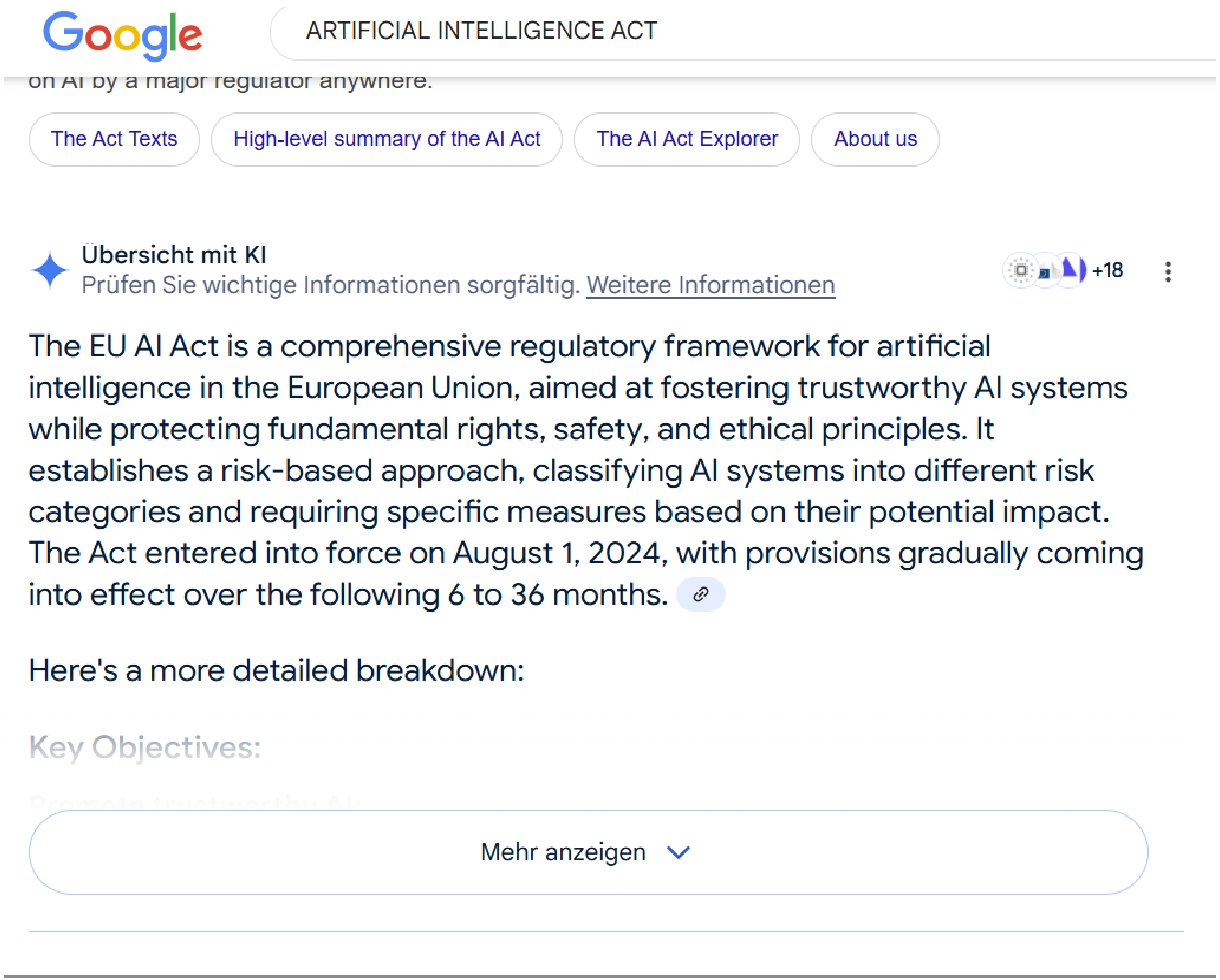
- the **Artificial Intelligence Act** and
- **AI Convention of the Council of Europe**

Artificial Intelligence in criminal proceedings
Legal framework

On the initiative of the European Commission, the legislative bodies of the European Union, the Council and the European Parliament, started working on an AI regulation:

ARTIFICIAL INTELLIGENCE ACT

(proposal by the European Commission, Brussels, 21.4.2021, COM (2021) 206 final; 2021/0106 (COD)))



on AI by a major regulator anywhere.

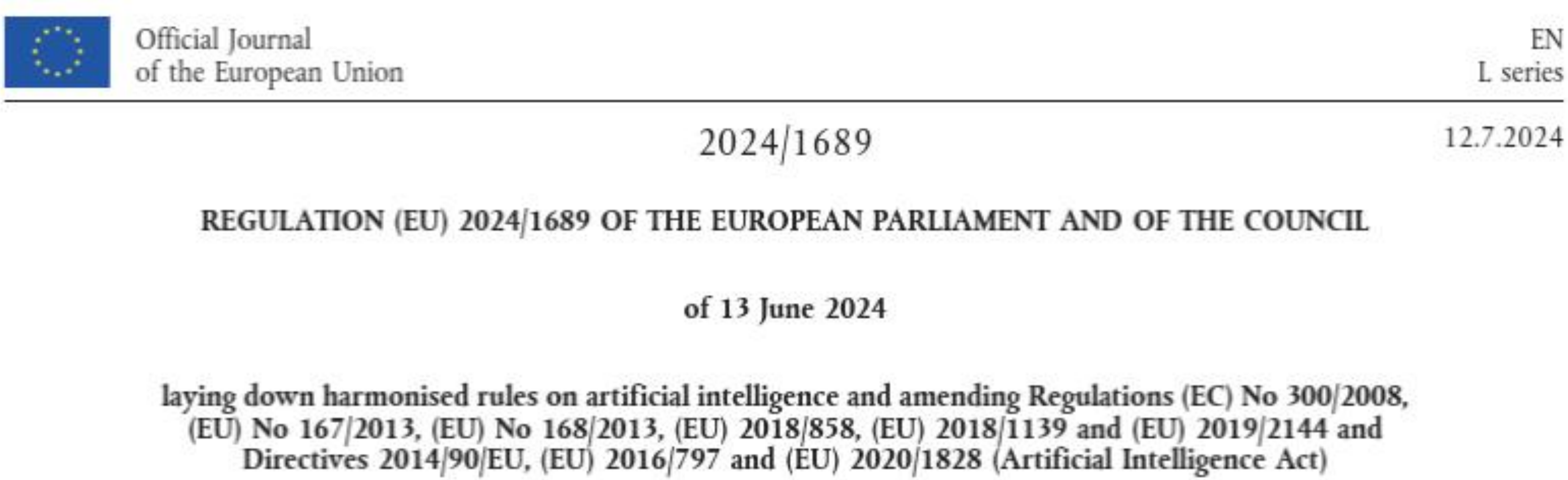
Übersicht mit KI
Prüfen Sie wichtige Informationen sorgfältig. Weitere Informationen

The EU AI Act is a comprehensive regulatory framework for artificial intelligence in the European Union, aimed at fostering trustworthy AI systems while protecting fundamental rights, safety, and ethical principles. It establishes a risk-based approach, classifying AI systems into different risk categories and requiring specific measures based on their potential impact. The Act entered into force on August 1, 2024, with provisions gradually coming into effect over the following 6 to 36 months.

Here's a more detailed breakdown:

Key Objectives:

Artificial Intelligence in criminal proceedings
Legal framework



Official Journal
of the European Union

EN
L series

2024/1689

12.7.2024

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

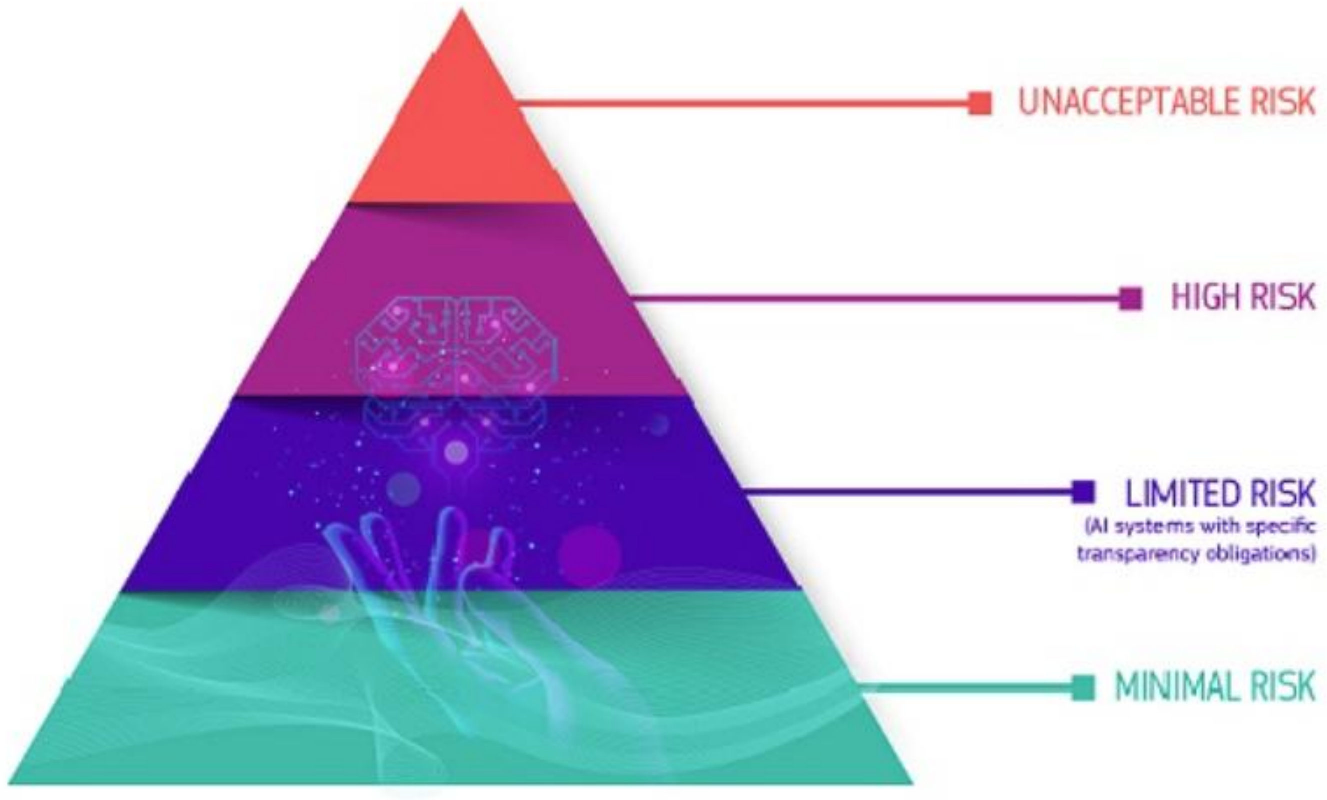
of 13 June 2024

laying down harmonised rules on artificial intelligence and amending Regulations (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)

Download:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689

A risk-based approach

The AI Act defines 4 levels of risk for AI systems:



[Source: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai]

Artificial Intelligence in criminal proceedings
Legal framework

The four risk levels are provided for:

- Prohibitions,
- quality requirements for high-risk AI systems,
- labeling requirements,
- voluntary self-commitment

Artificial Intelligence in criminal proceedings
Legal framework

Prohibited AI practices

As the rules follow a risk-based approach, they establish obligations for providers and those deploying AI systems depending on the level of risk the AI can generate.

AI systems with an unacceptable level of risk to people's safety would therefore be prohibited, such as those used for social scoring (classifying people based on their social behaviour or personal characteristics).

Artificial Intelligence in criminal proceedings
Legal framework

MEPs expanded the list to include bans on intrusive and discriminatory uses of AI, such as:

- "Real-time" remote biometric identification systems in publicly accessible spaces;

- "Post" remote biometric identification systems, with the only exception of law enforcement for the prosecution of serious crimes and only after judicial authorization;

- biometric categorisation systems using sensitive characteristics (e.g. gender, race, ethnicity, citizenship status, religion, political orientation);

Artificial Intelligence in criminal proceedings
Legal framework

- predictive policing systems (based on profiling, location or past criminal behaviour);

- emotion recognition systems in law enforcement, border management, the workplace, and educational institutions; and

- untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases (violating human rights and right to privacy).

Artificial Intelligence in criminal proceedings
Legal framework

The AI Act entered into force on 1 August 2024,
and will be fully applicable 2 years later on 2 August 2026,
with some exceptions:

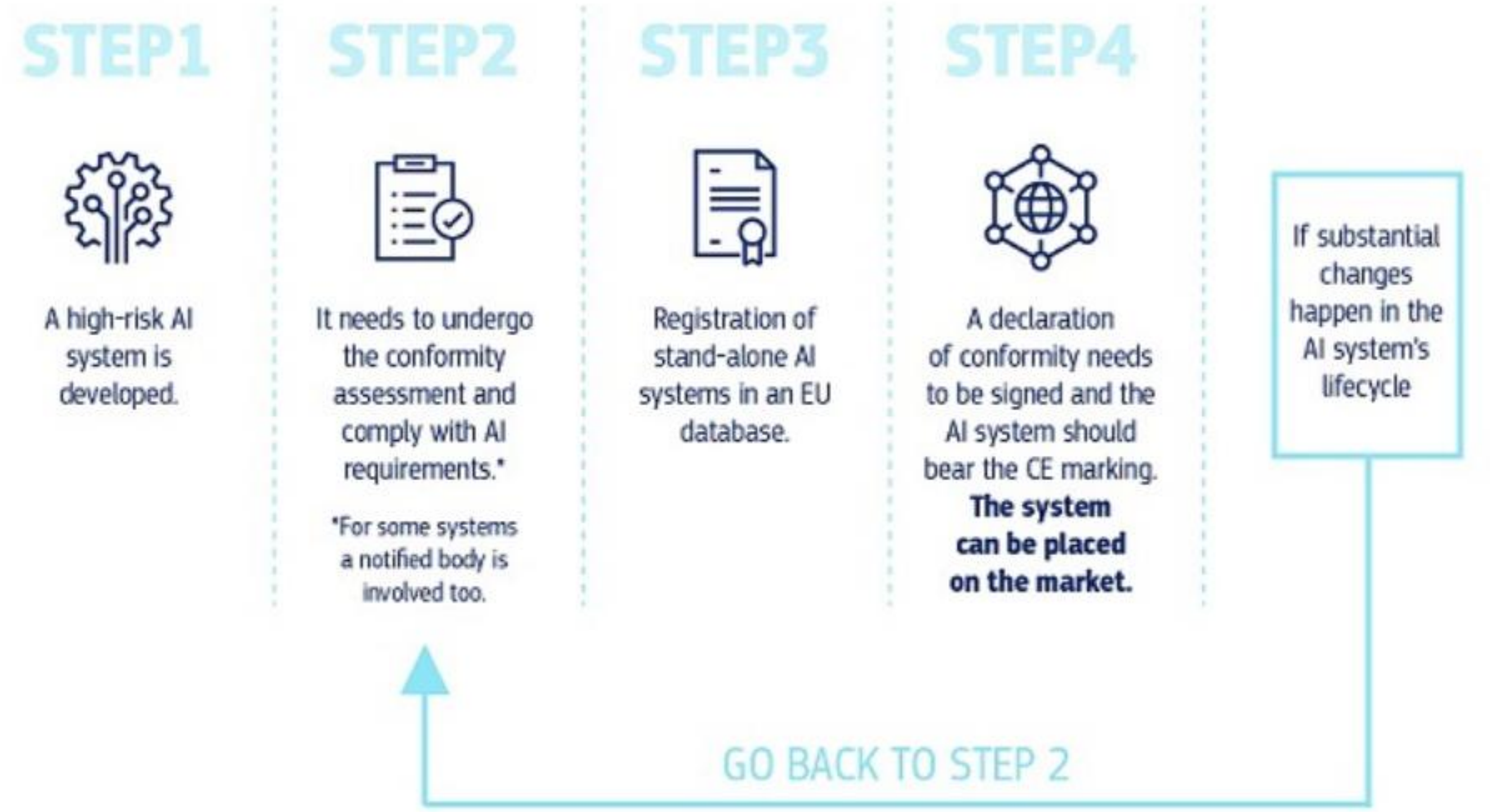
- prohibitions and AI literacy obligations entered into application from 2 February 2025
- the governance rules and the obligations for general-purpose AI models become applicable on 2 August 2025
- the rules for high-risk AI systems - embedded into regulated products - have an extended transition period until 2 August 2027

Artificial Intelligence in criminal proceedings
Legal framework – monitoring

Once an AI system is on the market,

- authorities are in charge of market surveillance
- deployers ensure human oversight and monitoring, and
- providers have a post-market monitoring systems in place
- Providers and deployers will also report serious incidents and malfunctioning.

Artificial Intelligence in criminal proceedings
Legal framework – monitoring



A high-risk AI system is developed.

It needs to undergo the conformity assessment and comply with AI requirements.*

*For some systems a notified body is involved too.

Registration of stand-alone AI systems in an EU database.

A declaration of conformity needs to be signed and the AI system should bear the CE marking. **The system can be placed on the market.**

If substantial changes happen in the AI system's lifecycle

GO BACK TO STEP 2

[Source:https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai]

Artificial Intelligence in criminal proceedings

Legal framework

The Framework Convention on Artificial Intelligence

COUNCIL OF EUROPE FRAMEWORK CONVENTION ON ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS, DEMOCRACY AND THE RULE OF LAW

Download:

https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

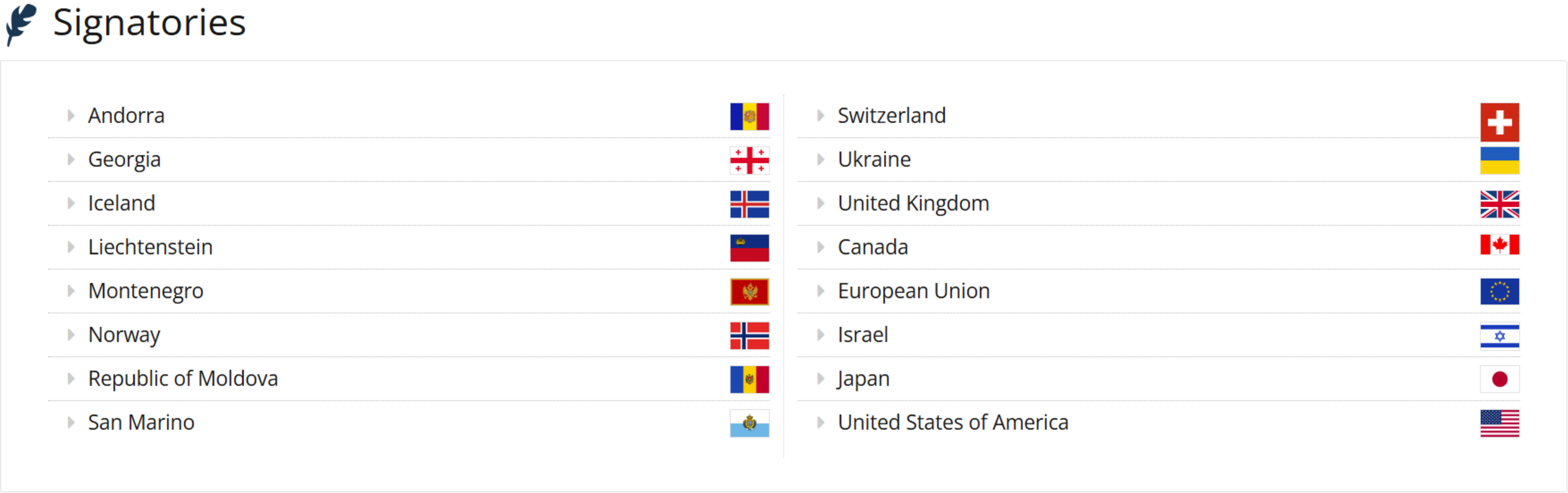
Artificial Intelligence in criminal proceedings
Legal framework

The Council of Europe Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law

is the first-ever international legally binding treaty in this field.

Opened for signature on 5 September 2024,
it aims to ensure that activities within the lifecycle of artificial Intelligence systems are fully consistent with human rights, democracy and the rule of law, while being conducive to Technological progress and innovation.

Artificial Intelligence in criminal proceedings
Legal framework



Signatories

- Andorra
- Georgia
- Iceland
- Liechtenstein
- Montenegro
- Norway
- Republic of Moldova
- San Marino
- Switzerland
- Ukraine
- United Kingdom
- Canada
- European Union
- Israel
- Japan
- United States of America

[as of June 12, 2025,
source: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence]

Artificial Intelligence in criminal proceedings
Legal framework

In terms of content, the AI Convention sets out general requirements for

- the design,
- development and
- use of AI systems

and is intended to define the basic principles for the use of AI.

Artificial Intelligence in criminal proceedings
Legal framework

Possible dangers in the use of this technology are identified, such as

- possible discrimination and bias,

- and means of avoiding the dangers are regulated, such as the creation of accountability obligations and the establishment of principles of responsibility.

Artificial Intelligence in criminal proceedings
Legal framework

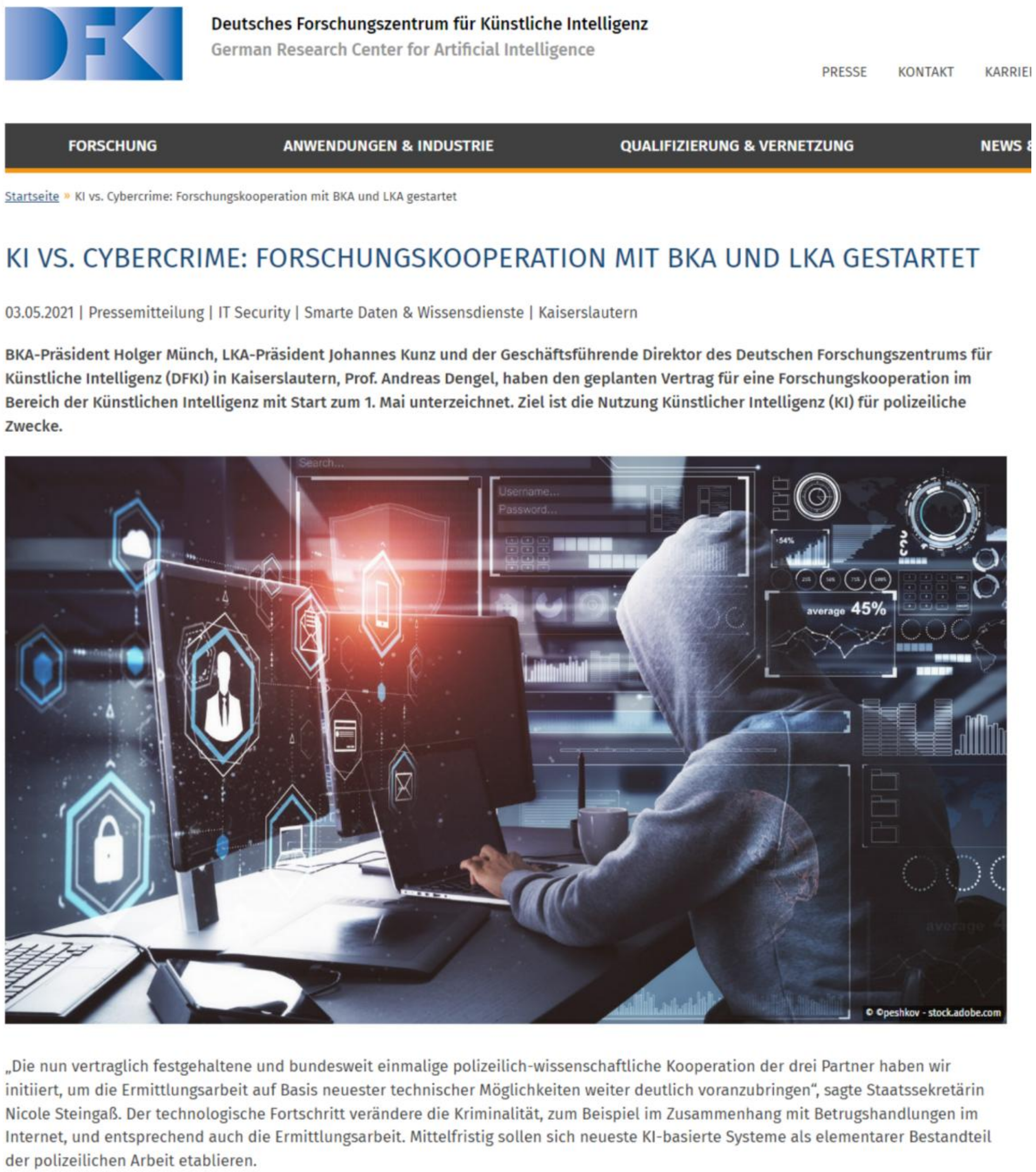
The implementation of a risk assessment is also envisaged.

This should help the relevant stakeholders to identify and assess the risks to human rights, democracy and the rule of law associated with the development or use of an AI system.

In addition, certain AI practices that pose an unacceptable risk to human rights, democracy and the rule of law are to be banned.

Artificial Intelligence in criminal proceedings
Legal framework

- The Framework Convention establishes a follow-up mechanism, the Conference of the Parties, composed of official representatives of the Parties to the Convention to determine the extent to which its provisions are being implemented.
- Their findings and recommendations help to ensure States' compliance with the Framework Convention and guarantee its long-term effectiveness.
- The Conference of the Parties shall also facilitate cooperation with relevant stakeholders, including through
  public hearings concerning pertinent aspects of the implementation of the Framework Convention.


DFKI
Deutsches Forschungszentrum für Künstliche Intelligenz
German Research Center for Artificial Intelligence
PRESSE
KONTAKT
KARRIEI
FORSCHUNG
ANWENDUNGEN & INDUSTRIE
QUALIFIZIERUNG & VERNETZUNG
NEWS &
Startseite » KI vs. Cybercrime: Forschungskooperation mit BKA und LKA gestartet

KI VS. CYBERCRIME: FORSCHUNGSKOOPERATION MIT BKA UND LKA GESTARTET

03.05.2021 | Pressemitteilung | IT Security | Smarte Daten & Wissensdienste | Kaiserslautern

BKA-Präsident Holger Münch, LKA-Präsident Johannes Kunz und der Geschäftsführende Direktor des Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI) in Kaiserslautern, Prof. Andreas Dengel, haben den geplanten Vertrag für eine Forschungskooperation im Bereich der Künstlichen Intelligenz mit Start zum 1. Mai unterzeichnet. Ziel ist die Nutzung Künstlicher Intelligenz (KI) für polizeiliche Zwecke.

© ©peshkov - stock.adobe.com

„Die nun vertraglich festgehaltene und bundesweit einmalige polizeilich-wissenschaftliche Kooperation der drei Partner haben wir initiiert, um die Ermittlungsarbeit auf Basis neuester technischer Möglichkeiten weiter deutlich voranzubringen", sagte Staatssekretärin Nicole Steingaß. Der technologische Fortschritt verändere die Kriminalität, zum Beispiel im Zusammenhang mit Betrugshandlungen im Internet, und entsprechend auch die Ermittlungsarbeit. Mittelfristig sollen sich neueste KI-basierte Systeme als elementarer Bestandteil der polizeilichen Arbeit etablieren.

Artificial Intelligence in criminal proceedings Current situation in Germany

The cooperation primarily focuses on the pre-selection and Relevance assessment of immense amounts of data and the analysis of unstructured raw data.

The latter is particularly important in cases where suspects expect search measures and delete data from digital devices, but raw data remains in fragmented form.

Reconstruction should enable conclusions to be drawn about the content.

Artificial Intelligence in criminal proceedings Examples

Kusel - the first use of VR glasses in a German court

What happened?

On the night of January 30/31, 2022, a patrol of two police officers is on the road in the West Palatinate region as part of the investigation into a series of burglaries; the 29-year-old chief inspector and a 24-year-old police trainee (both from the Saarland) are using a civilian vehicle for this purpose.

Shortly after 4 a.m. on the L22 between Ulmet and Kusel, they notice a suspicious van parked on the side of the road.

Artificial Intelligence in criminal proceedings Examples

They stop and check a 38-year-old man named Andreas S. and another 32-year-old man on the spot. The police officers make a radio call saying that they have come across dubious people and that the trunk is full of wild animals. Shortly afterwards, shots are fired.

The 24-year-old policewoman is unexpectedly shot in the head during the check. According to the investigation, she was then seriously injured and fell unconscious onto the street.

Artificial Intelligence in criminal proceedings
Examples

Her colleague then radioed for help and fired several shots before also being hit in the head.

The 29-year-old fired 15 shots from his service weapon, but only hit the van in the darkness.
The unconscious policewoman is then killed by another shot to the head.

Artificial Intelligence in criminal proceedings
Examples

The main defendant S. denied having shot the policewoman, saying that this was V.'s fault.

Although he admitted that he had shot the police officer in the subsequent incident, he claimed that this had happened in a kind of self-defense situation, as he had been shot at first.

He also claimed that it was only after the third shot from the hunting rifle that he realized that his "opponent" was a police officer.

Artificial Intelligence in criminal proceedings Examples

Police not only created a 360-degree image of the crime scene, but also used **a laser scanner** to map the location.

A laser scan ensures that the reflection of an emitted laser beam captures image points of the surroundings and combines them into a complex point cloud.

The result is then a virtual reconstructed model of the location in which you can move around freely.

Artificial Intelligence in criminal proceedings Examples

This is what the presiding judge did during the main hearing, when - equipped with VR glasses - he **went to the crime scene virtually and walked through various "beam points"**.

Such "beam points" are markings in the VR model to which the user can "beam" - the background to this is that many users suffer from nausea when making fluid movements in VR, such as controller-controlled walking in the virtual world (so-called visually induced motion sickness, or "vims" for short).

Artificial Intelligence in criminal proceedings Examples

The main perpetrator was sentenced to life imprisonment for murder.

Source:www.swr.de

The verdict is final, the Federal Court of Justice has dismissed the defendant's appeal.

Artificial Intelligence in criminal proceedings
Examples

Speeding case in Wiesbaden – Murder?

What happened?

In October 2022, a young man was speeding through the city in his car near Wiesbaden's main railway station, allegedly at speeds of up to 130 km/h.
This resulted in an accident with a vehicle turning left, the driver of which was fatally injured.

Artificial Intelligence in criminal proceedings
Examples

As part of the public prosecutor's investigation into the question of whether the perpetrator could possibly be accused of murder, the police cordoned off the scene of the accident and recreated the (alleged) course of the accident.

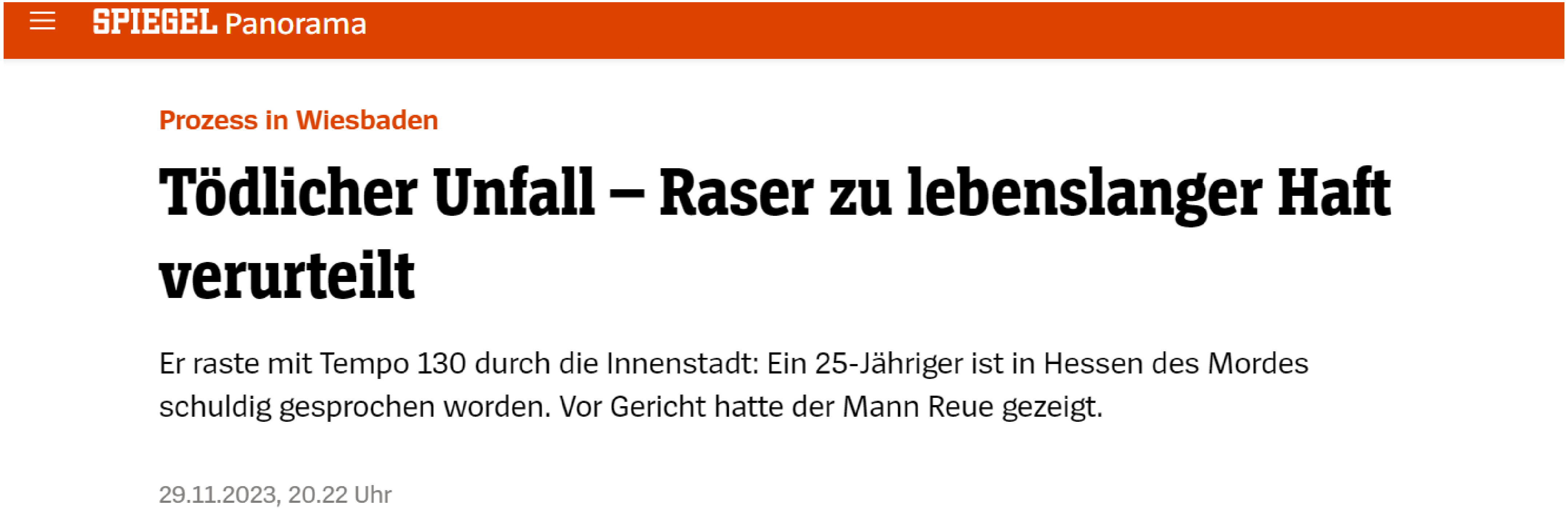
The police drove around the scene in identical vehicles - the special feature: **a 360-degree camera** was installed at the driver's eye level in both the perpetrator's and the victim's vehicle. Their recordings are now to show the investigators and possibly the court what view the parties involved had of the accident. The police also placed a corresponding camera at the location of a witness.

Artificial Intelligence in criminal proceedings
Examples

The court used AI-assisted VR to reconstruct the crime scene in 3D, providing:

- Immersive view of
  - Driving path and speed
  - Visibility and timing
  - Possibility to prevent the crash
- AI-assisted VR helped assess intent and foreseeability
- VR use was pioneering in German criminal court
- Enhanced evidentiary clarity and spatial understanding

Artificial Intelligence in criminal proceedings
Examples



SPIEGEL Panorama

Prozess in Wiesbaden

Tödlicher Unfall – Raser zu lebenslanger Haft verurteilt

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

29.11.2023, 20.22 Uhr

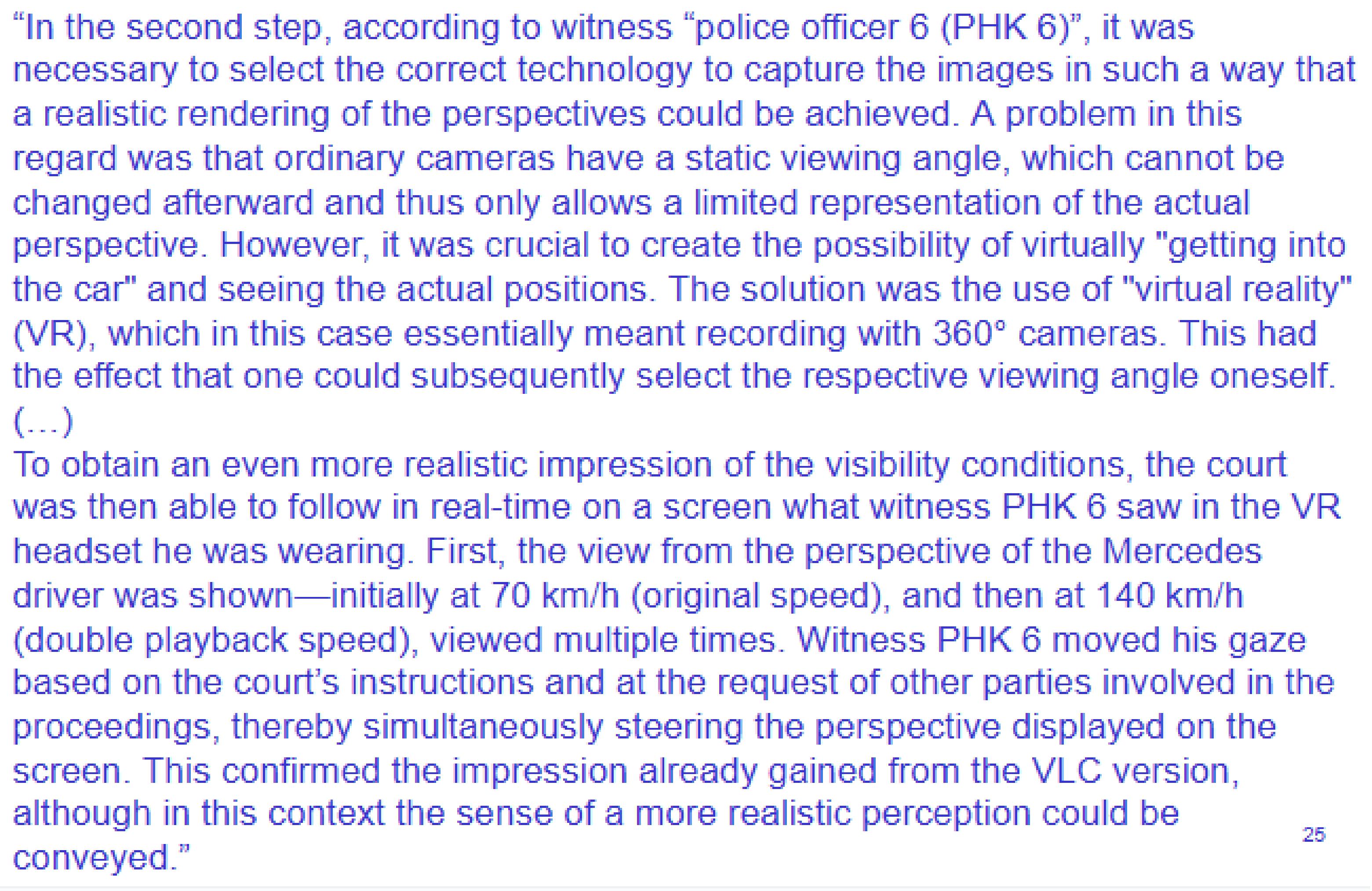
Artificial Intelligence in criminal proceedings Examples

The main perpetrator was sentenced to life imprisonment for murder.

Source:www.ffh.de

Artificial Intelligence in criminal proceedings

Examples – From the verdict:



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

25

Artificial Intelligence in criminal proceedings
Examples

Regional Court Darmstadt (Hesse/Germany):

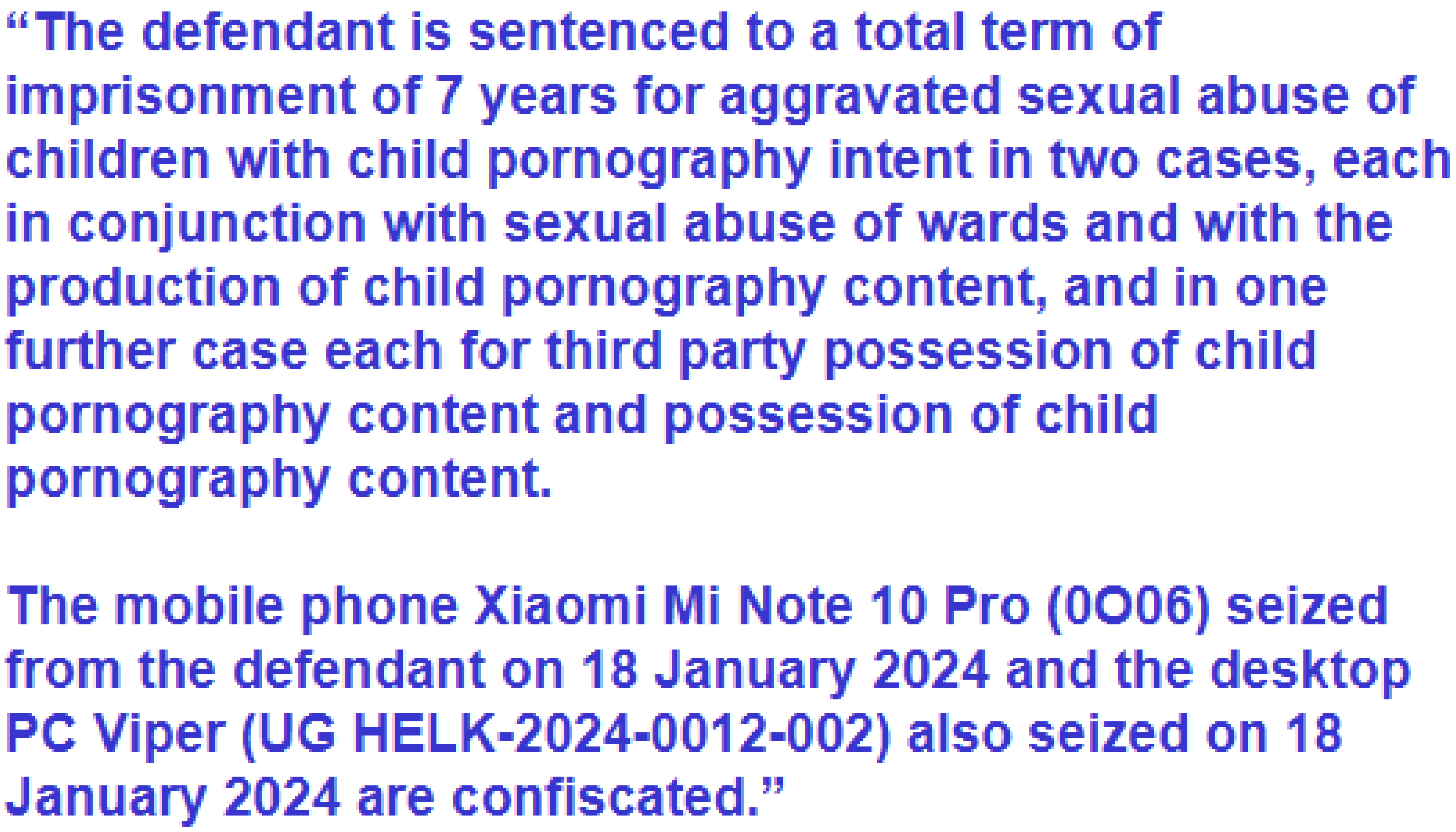
The defendant claimed that an incriminating video – found on his mobile phone and showing him engaging in sexual acts with his three-year-old biological daughter – had been artificially generated, using AI.

He asserted that the video did not depict a real event.

Artificial Intelligence in criminal proceedings
Examples

Expert witness from the German Federal Criminal Police Office (Bundeskriminalamt, BKA) stated that the metadata ruled out artificial generation

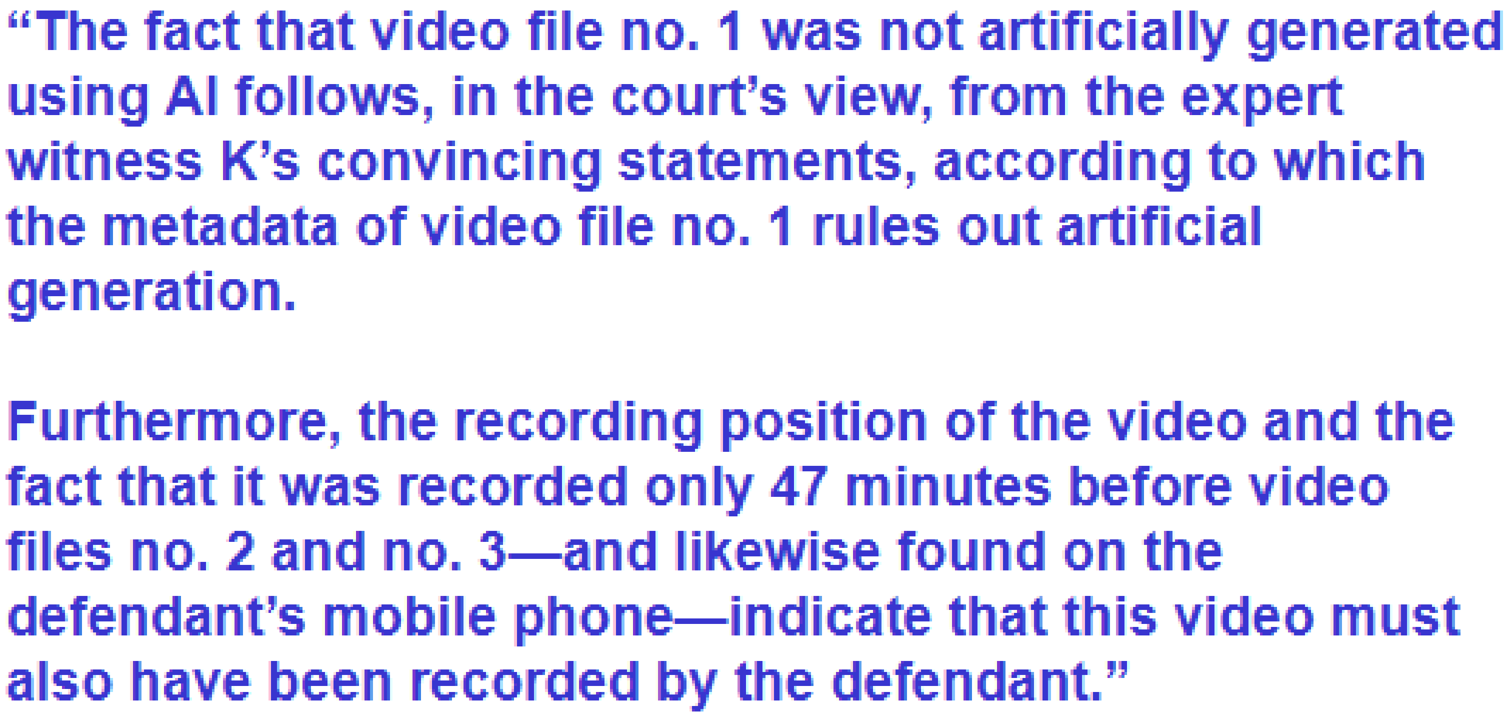
Artificial Intelligence in criminal proceedings
Examples – From the verdict:



“The defendant is sentenced to a total term of imprisonment of 7 years for aggravated sexual abuse of children with child pornography intent in two cases, each in conjunction with sexual abuse of wards and with the production of child pornography content, and in one further case each for third party possession of child pornography content and possession of child pornography content.

The mobile phone Xiaomi Mi Note 10 Pro (0O06) seized from the defendant on 18 January 2024 and the desktop PC Viper (UG HELK-2024-0012-002) also seized on 18 January 2024 are confiscated.”

Artificial Intelligence in criminal proceedings
Examples – From the verdict:



“The fact that video file no. 1 was not artificially generated using AI follows, in the court’s view, from the expert witness K’s convincing statements, according to which the metadata of video file no. 1 rules out artificial generation.

Furthermore, the recording position of the video and the fact that it was recorded only 47 minutes before video files no. 2 and no. 3—and likewise found on the defendant’s mobile phone—indicate that this video must also have been recorded by the defendant.”

NEW TEAM:

~~ARTIFICIAL INTELLIGENCE~~

INNOVATION

EUROPOL EMPACT OA 1.3

“CYBERCRIME IN THE AGE OF AI”

EMPACT

European Multidisciplinary Platform Against Criminal Threats

Operation Action 1.3

Action Leader: Bundeskriminalamt - Unit Cybercrime

Co-Action Leader: United States Secret Service

Title: Cybercime in the Age of AI

Subtitle: The alarming threat caused by the misuse of GPT and other AI-Systems

Project period 01.01.2024 to 31.12.2025

Targets

- Establish a sustainable network for operational purposes

- Generate new investigative approaches

✓ Network

→ Operation

♲ Knowledge hub

✓ Deconfliction

- Gather information, resources, and expertise to facilitate learning and collaboration

- Create synergies that promote investigations and analysis

International Partners

LEA:

Austria, Cyprus, Czech Republic, Denmark, European Commission, Europol, Finland, Germany, Greece, Hungary, Iceland, Japan, Malta, Netherlands, Poland, Portugal, Romania, Spain, South Africa, Sweden, Switzerland, Ukraine, United Kingdom, USA

Private sector:

Amazon, Google, Meta, Microsoft, OpenAI, Group IB, Fraunhofer ForenSwiss, O2 UK, Destesia

Focus

GenAI Fraud:

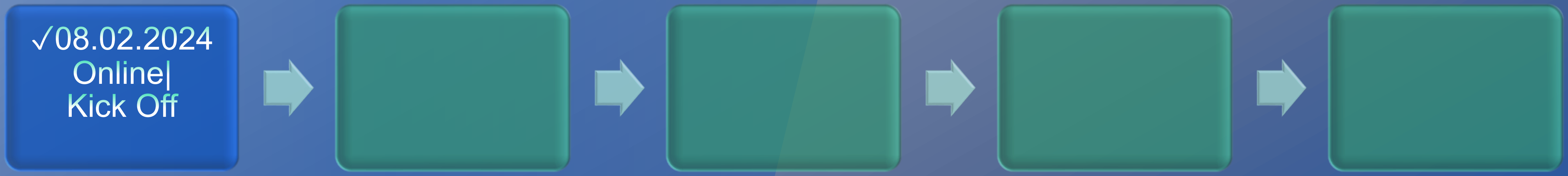
Text, Picture, Movies, Voice Cloning, Coding and Deepfakes

Cybercrime mit GenAI Fraud:

- Cybercrime (Phishing, Malware, CEO Fraud)
- High-risk criminal networks
- Cyber attacks

Other criminal areas:

Financial crime, CSAM, politically motivated crime, arms trafficking crime, drug-related crime and others



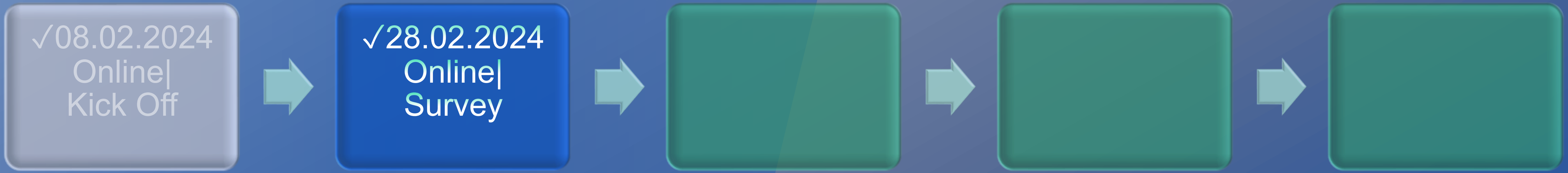
✓08.02.2024
Online|
Kick Off

Knowledge Hub

Empirical survey with participants on:

1) Identification of dark LLMs

2) Misuse of legitimate AI systems



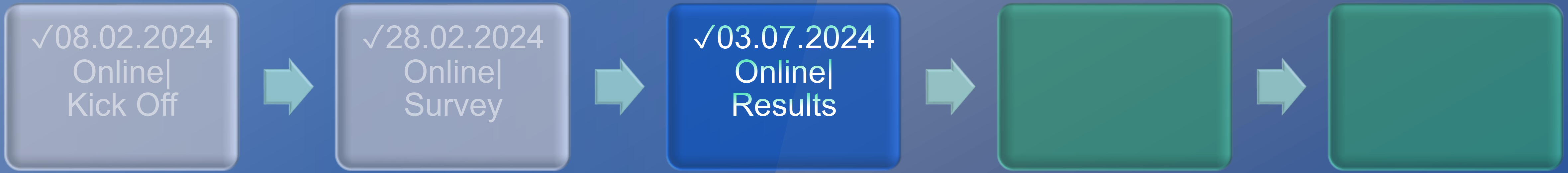
√08.02.2024 Online| Kick Off

√28.02.2024 Online| Survey

AI

Results

- Discovery of unknown incriminated AI systems (dark LLMs)
- Various possible applications discovered
- No specifically tailored criminal standards
- Generally large dark field



✓08.02.2024
Online|
Kick Off

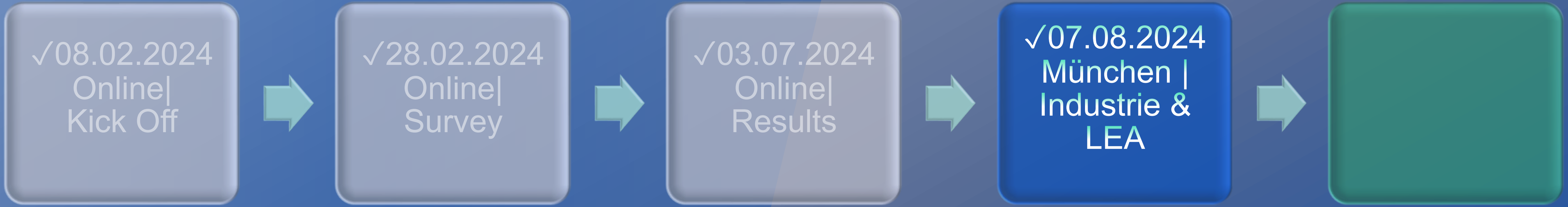
✓28.02.2024
Online|
Survey

✓03.07.2024
Online|
Results

Companies and LEA

Important collaborations:

- Every company is working on fraud detection
- Utilize synergy effects effectively and sustainably
- Manufacturers of AI systems improve their security restrictions



√08.02.2024
Online|
Kick Off

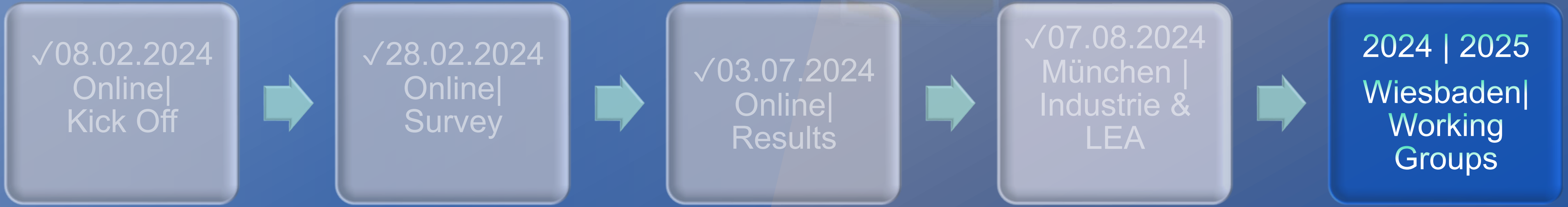
√28.02.2024
Online|
Survey

√03.07.2024
Online|
Results

√07.08.2024
München |
Industrie &
LEA

Cooperation

- Monthly case studies
- Working groups for operational evaluations
- Identify further preventive and operational cooperation opportunities and detectors



√08.02.2024 Online| Kick Off

√28.02.2024 Online| Survey

√03.07.2024 Online| Results

√07.08.2024 München | Industrie & LEA

2024 | 2025 Wiesbaden| Working Groups

TEAM ILA

WE DISCONNECT. WORLDWIDE.

Thank you – Any questions?

Linda Bertram

Oberstaatsanwältin/
Senior Public Prosecutor

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

International **L**egal **A**ssistance

Konrad-Adenauer-Straße 15
60313 Frankfurt am Main

Phone: + 49 69 1367 4222
Mob.: + 49 171 28 93 504 (SPOC for ILA 24/7)
Mail: linda.bertram@gsta.justiz.hessen.de

#DIGITALISATION and #ARTIFICIALINTELLIGENCE in Criminal Justice

Digital tech as a tool to commit crimes

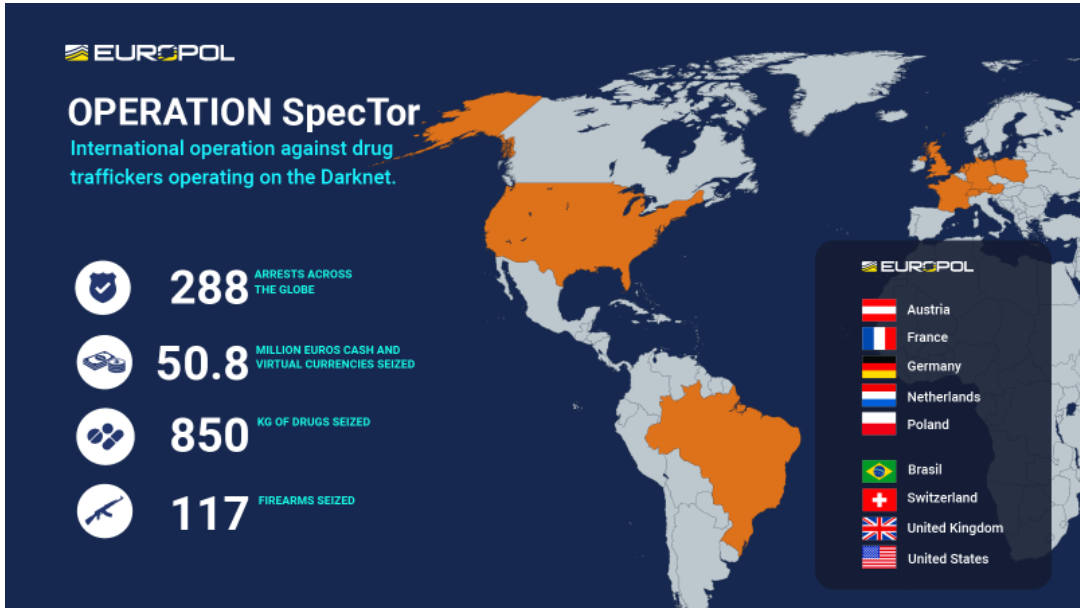
David Silva Ramalho
Lawyer | Assistant Teacher at the University of Lisbon's School of Law

Co-funded by the European Union

Illegal trade on the Dark Web

Dark Web

- Narcotics: cannabis to cocaine, synthetic drugs, prescription pills, etc.



EUROPOL

OPERATION SpecTor

International operation against drug traffickers operating on the Darknet.

288 ARRESTS ACROSS THE GLOBE

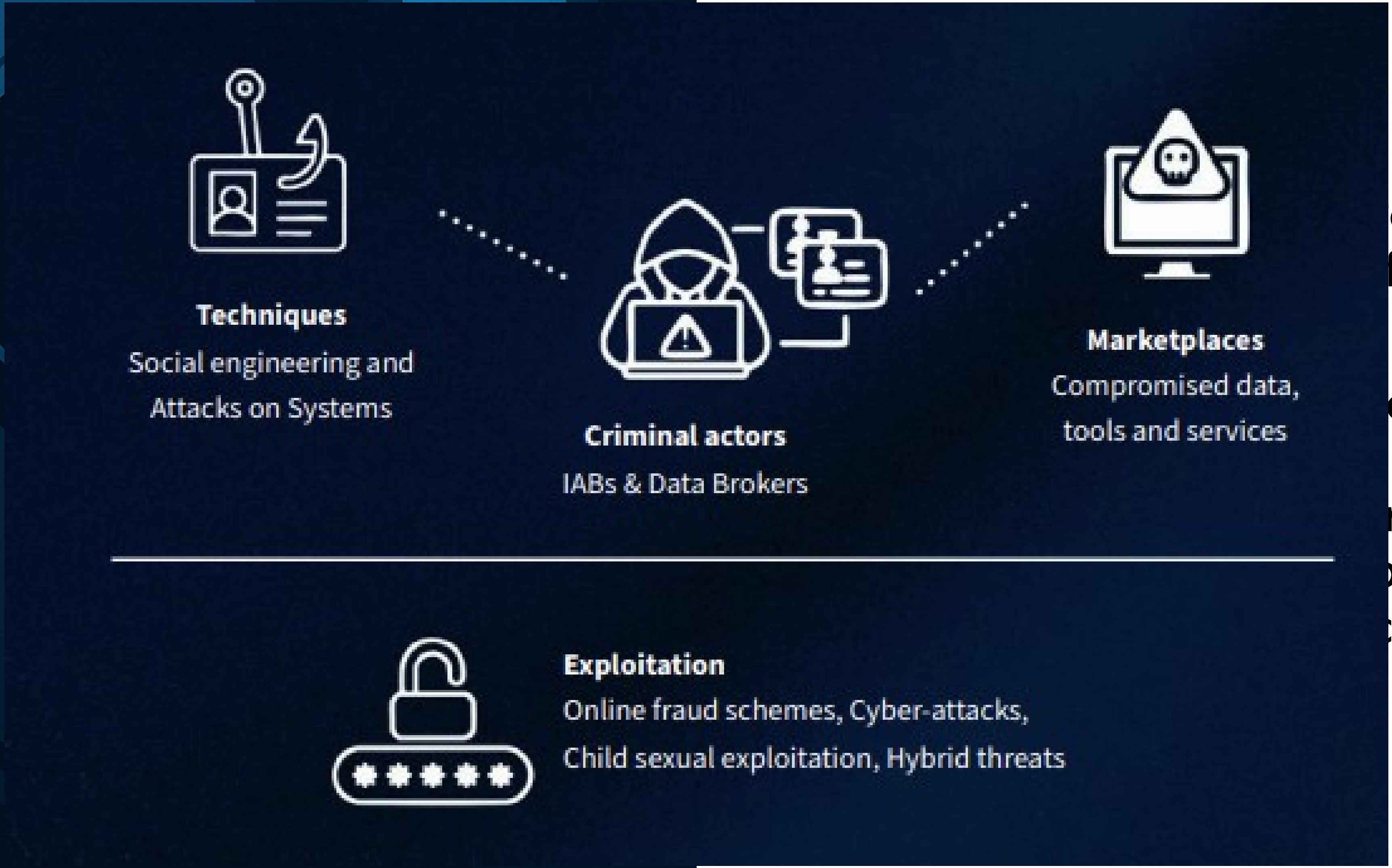
50.8 MILLION EUROS CASH AND VIRTUAL CURRENCIES SEIZED

850 KG OF DRUGS SEIZED

117 FIREARMS SEIZED

EUROPOL

- Austria
- France
- Germany
- Netherlands
- Poland
- Brasil
- Switzerland
- United Kingdom
- United States



Techniques
Social engineering and
Attacks on Systems

Criminal actors
IABs & Data Brokers

Marketplaces
Compromised data,
tools and services

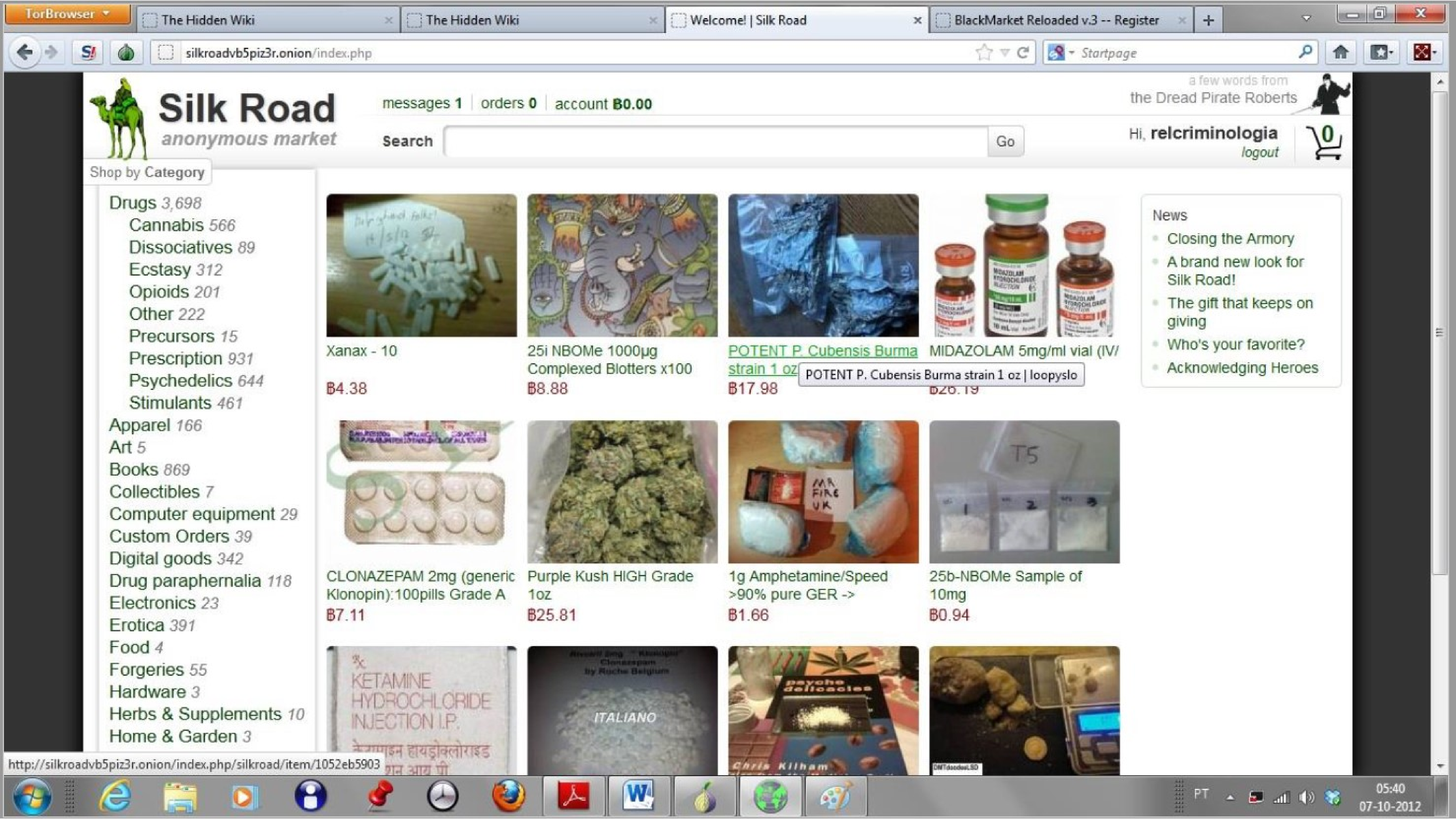
Exploitation
Online fraud schemes, Cyber-attacks,
Child sexual exploitation, Hybrid threats

eapons
for 3D

ercrime
and
ng of
otnets,
c.)

Dark Web

- Fraudulent goods and documents (counterfeit currency, forged passports and driver’s licenses)
- Explicit ilegal content (CSAM)
- Other services (illegal gambling, terrorist propaganda, match-fixing forums)



Silk Road

anonymous market

messages 1 | orders 0 | account Ƀ0.00

a few words from the Dread Pirate Roberts

Search [ ] Go

Hi, **relcriminologia**
logout

0

Shop by Category

- Drugs *3,698*
  - Cannabis *566*
  - Dissociatives *89*
  - Ecstasy *312*
  - Opioids *201*
  - Other *222*
  - Precursors *15*
  - Prescription *931*
  - Psychedelics *644*
  - Stimulants *461*
- Apparel *166*
- Art *5*
- Books *869*
- Collectibles *7*
- Computer equipment *29*
- Custom Orders *39*
- Digital goods *342*
- Drug paraphernalia *118*
- Electronics *23*
- Erotica *391*
- Food *4*
- Forgeries *55*
- Hardware *3*
- Herbs & Supplements *10*
- Home & Garden *3*

Xanax - 10
Ƀ4.38

25i NBOMe 1000µg Complexed Blotters x100
Ƀ8.88

POTENT P. Cubensis Burma strain 1 oz
Ƀ17.98

POTENT P. Cubensis Burma strain 1 oz | loopyslo

MIDAZOLAM 5mg/ml vial (IV/
Ƀ26.19

CLONAZEPAM 2mg (generic Klonopin):100pills Grade A
Ƀ7.11

Purple Kush HIGH Grade 1oz
Ƀ25.81

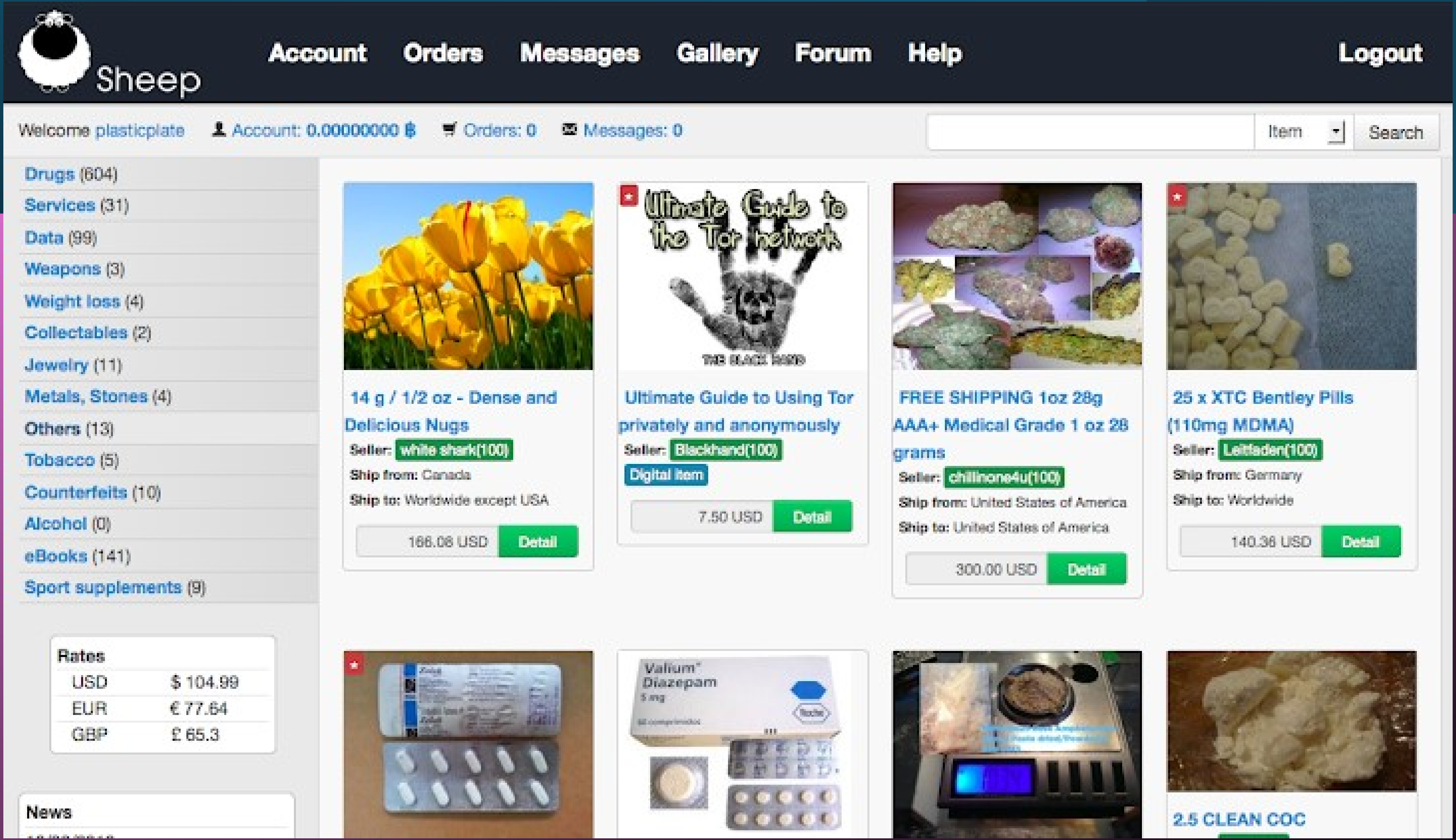
1g Amphetamine/Speed >90% pure GER ->
Ƀ1.66

25b-NBOMe Sample of 10mg
Ƀ0.94

News

- Closing the Armory
- A brand new look for Silk Road!
- The gift that keeps on giving
- Who's your favorite?
- Acknowledging Heroes

http://silkroadvb5piz3r.onion/index.php/silkroad/item/1052eb5903



Welcome plasticplate Account: 0.00000000 ฿ Orders: 0 Messages: 0

Drugs (604)
Services (31)
Data (99)
Weapons (3)
Weight loss (4)
Collectables (2)
Jewelry (11)
Metals, Stones (4)
Others (13)
Tobacco (5)
Counterfeits (10)
Alcohol (0)
eBooks (141)
Sport supplements (9)

Rates	
USD	$ 104.99
EUR	€ 77.64
GBP	£ 65.3

News

14 g / 1/2 oz - Dense and Delicious Nugs
Seller: white shark(100)
Ship from: Canada
Ship to: Worldwide except USA
166.08 USD

Ultimate Guide to Using Tor privately and anonymously
Seller: Blackhand(100)
7.50 USD

FREE SHIPPING 1oz 28g AAA+ Medical Grade 1 oz 28 grams
Seller: chillinone4u(100)
Ship from: United States of America
Ship to: United States of America
300.00 USD

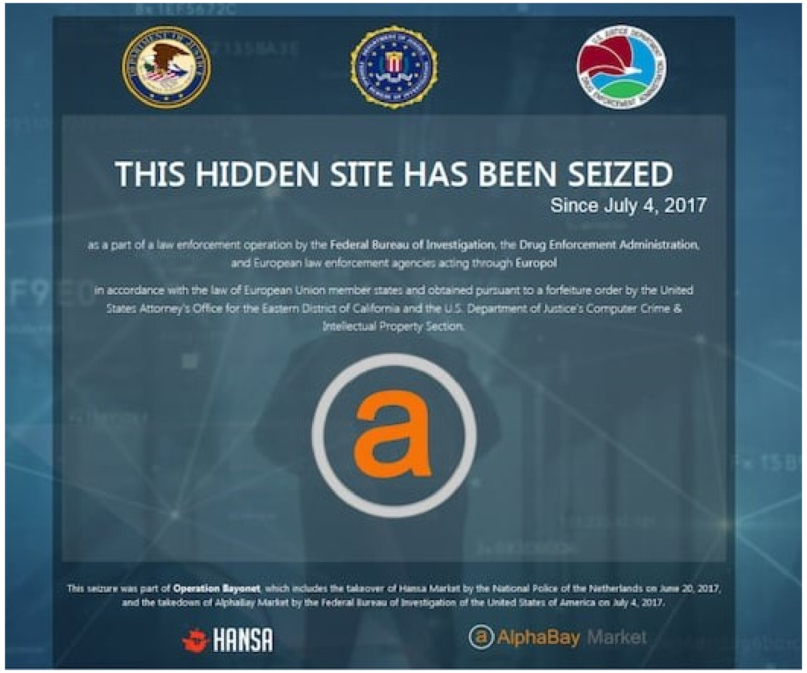
25 x XTC Bentley Pills (110mg MDMA)
Seller: Leitfaden(100)
Ship from: Germany
Ship to: Worldwide
140.36 USD

2.5 CLEAN COC

Tackling ilegal trade on the Dark Web

Marketplace takedowns

- Identifying server locations or administrators of dark web sites and seizing them.
- Sometimes even operating the markets covertly (e.g. Hansa Market).
- Technical exploitation (hacking, compromising accounts, finding technical flaws for deanonymization)



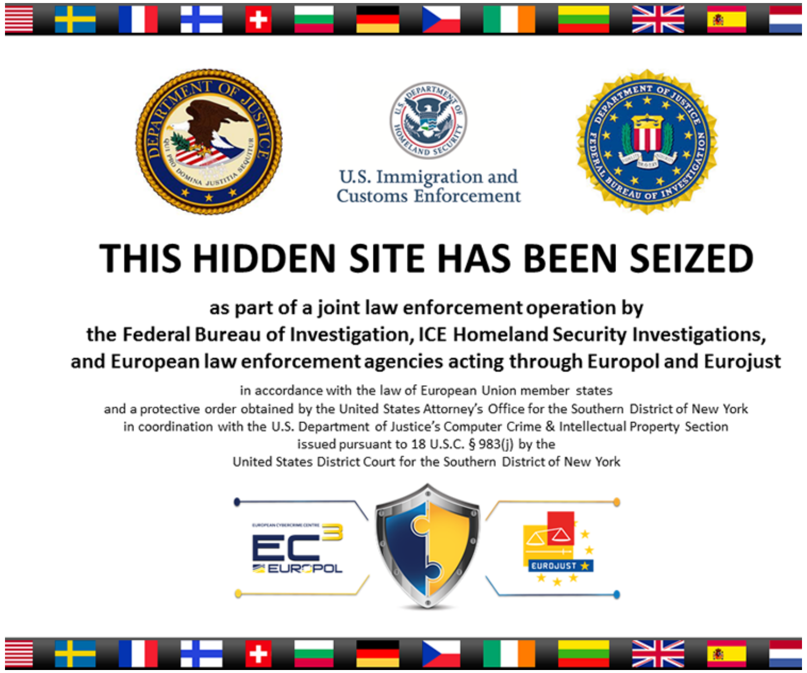
THIS HIDDEN SITE HAS BEEN SEIZED

Since July 4, 2017

as a part of a law enforcement operation by the Federal Bureau of Investigation, the Drug Enforcement Administration, and European law enforcement agencies acting through Europol

in accordance with the law of European Union member states and obtained pursuant to a forfeiture order by the United States Attorney's Office for the Eastern District of California and the U.S. Department of Justice's Computer Crime & Intellectual Property Section.

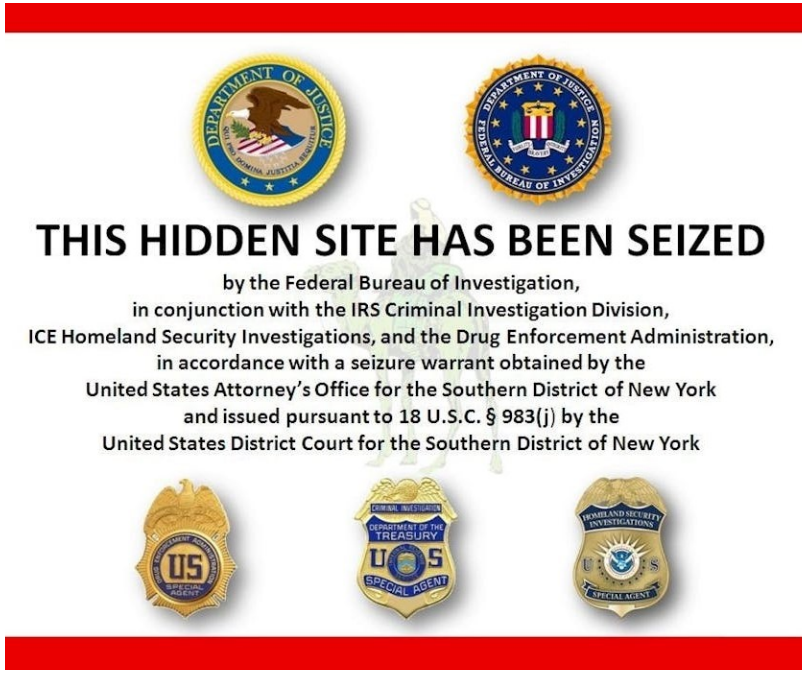
This seizure was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands on June 20, 2017, and the takedown of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.



THIS HIDDEN SITE HAS BEEN SEIZED

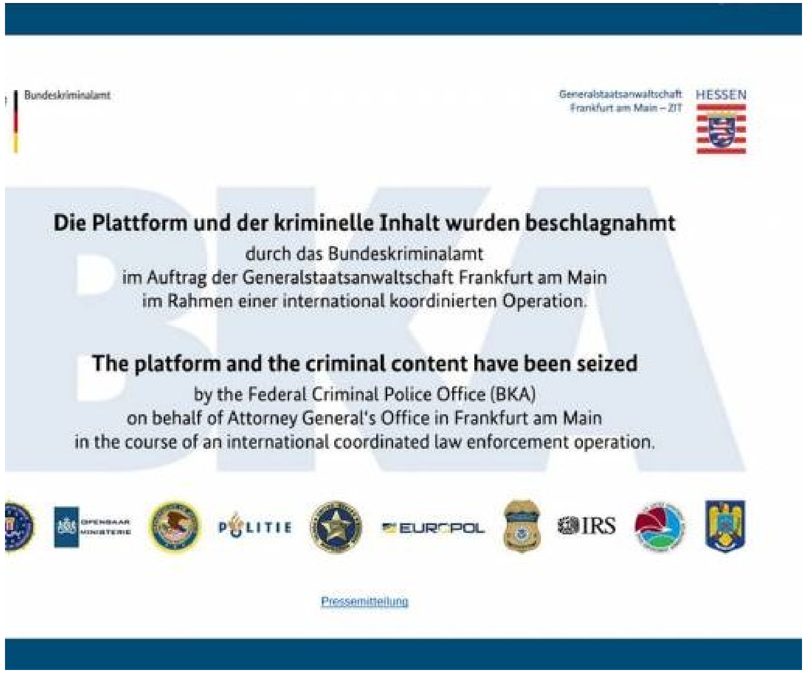
as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York



THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York



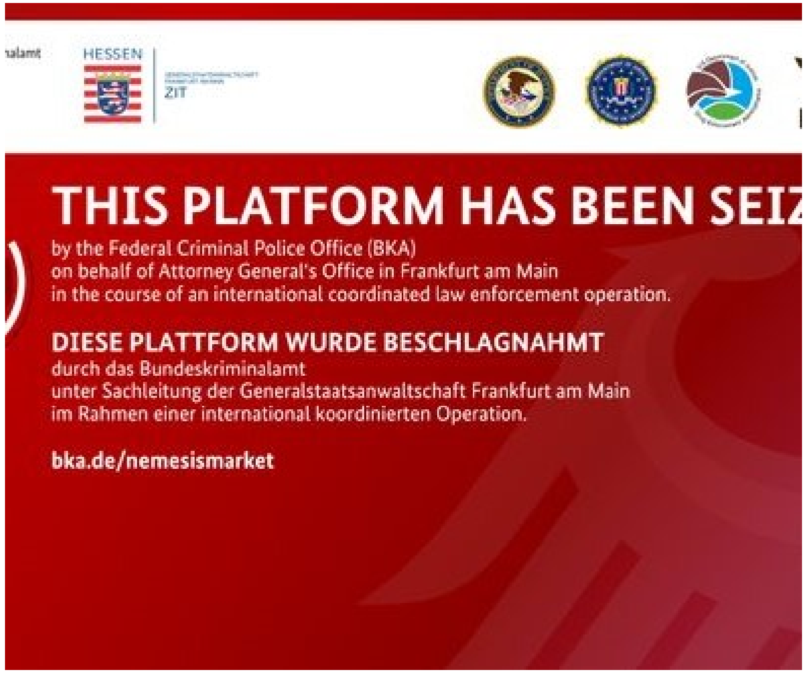
Die Plattform und der kriminelle Inhalt wurden beschlagnahmt

durch das Bundeskriminalamt
im Auftrag der Generalstaatsanwaltschaft Frankfurt am Main
im Rahmen einer international koordinierten Operation.

The platform and the criminal content have been seized

by the Federal Criminal Police Office (BKA)
on behalf of Attorney General's Office in Frankfurt am Main
in the course of an international coordinated law enforcement operation.

Pressemitteilung



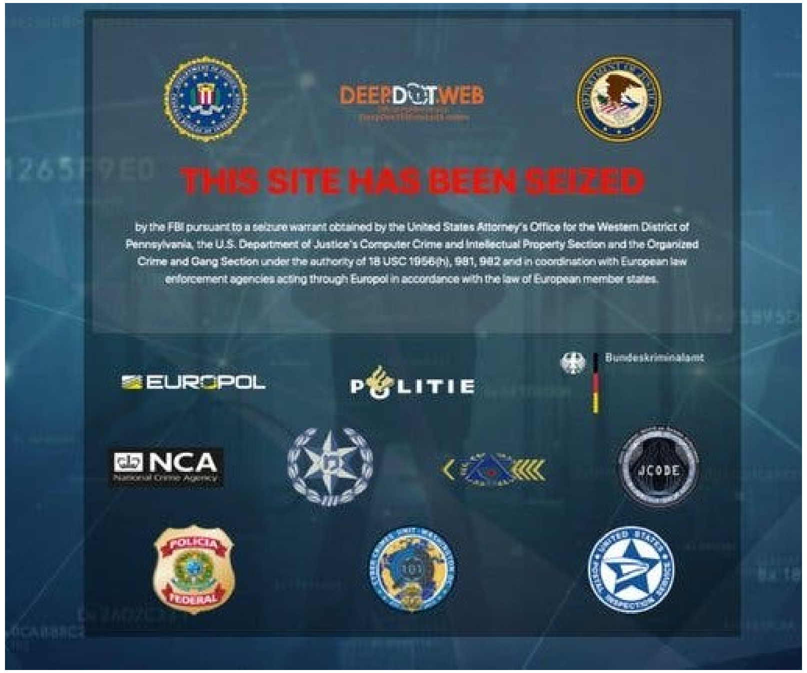
THIS PLATFORM HAS BEEN SEIZ

by the Federal Criminal Police Office (BKA)
on behalf of Attorney General's Office in Frankfurt am Main
in the course of an international coordinated law enforcement operation.

DIESE PLATTFORM WURDE BESCHLAGNAHMT

durch das Bundeskriminalamt
unter Sachleitung der Generalstaatsanwaltschaft Frankfurt am Main
im Rahmen einer international koordinierten Operation.

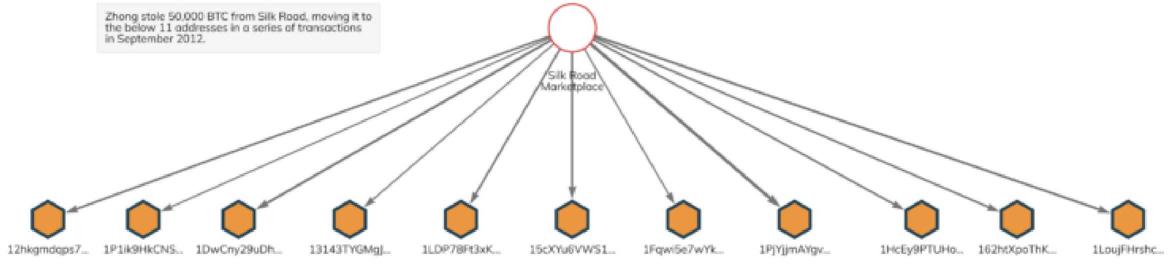
bka.de/nemesismarket



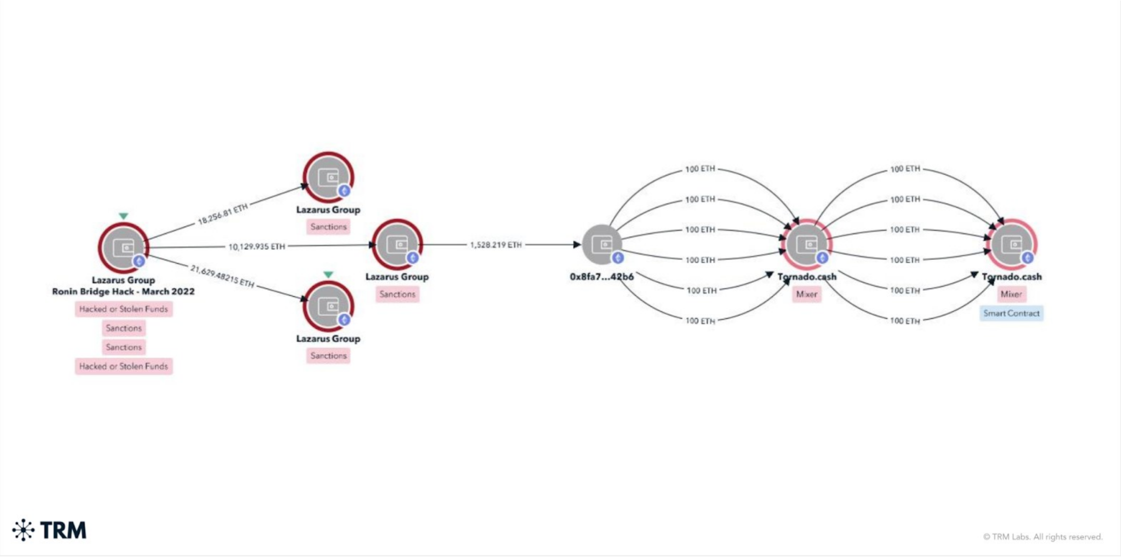
THIS SITE HAS BEEN SEIZED

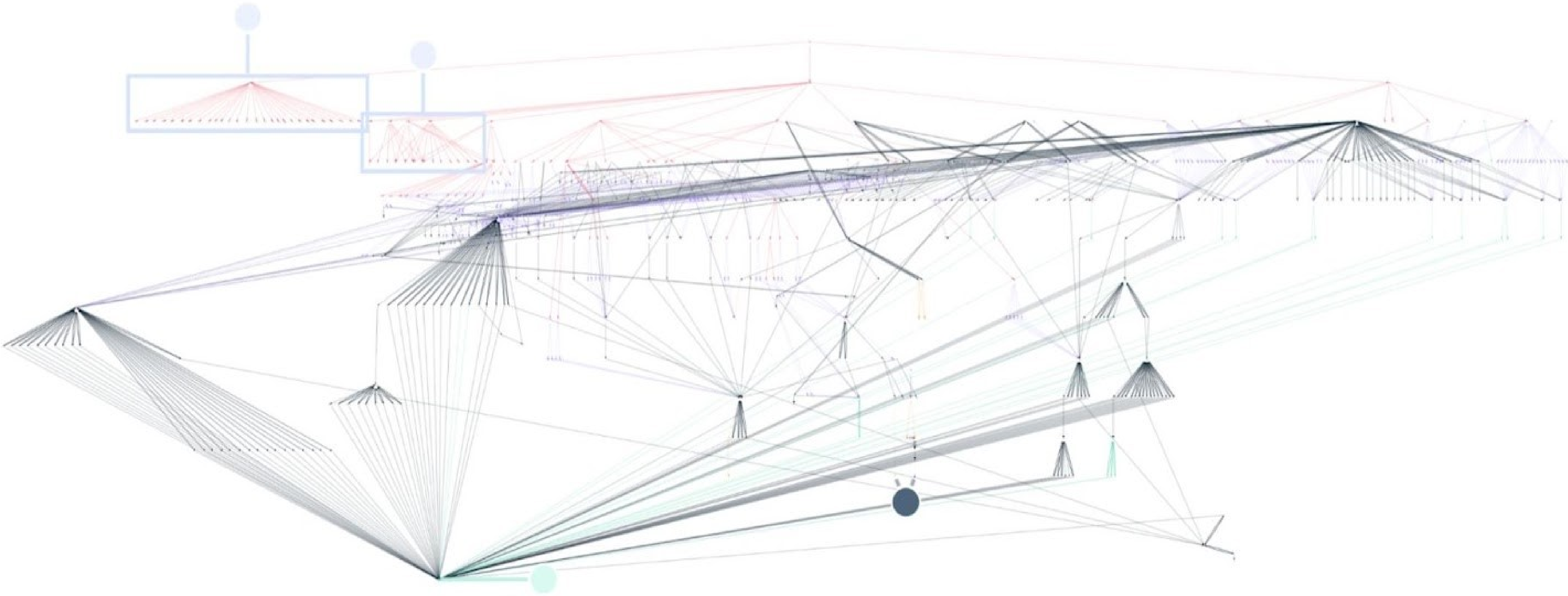
by the FBI pursuant to a seizure warrant obtained by the United States Attorney's Office for the Western District of Pennsylvania, the U.S. Department of Justice's Computer Crime and Intellectual Property Section and the Organized Crime and Gang Section under the authority of 18 USC 1956(h), 981, 982 and in coordination with European law enforcement agencies acting through Europol in accordance with the law of European member states.

Cryptocurrency tracing



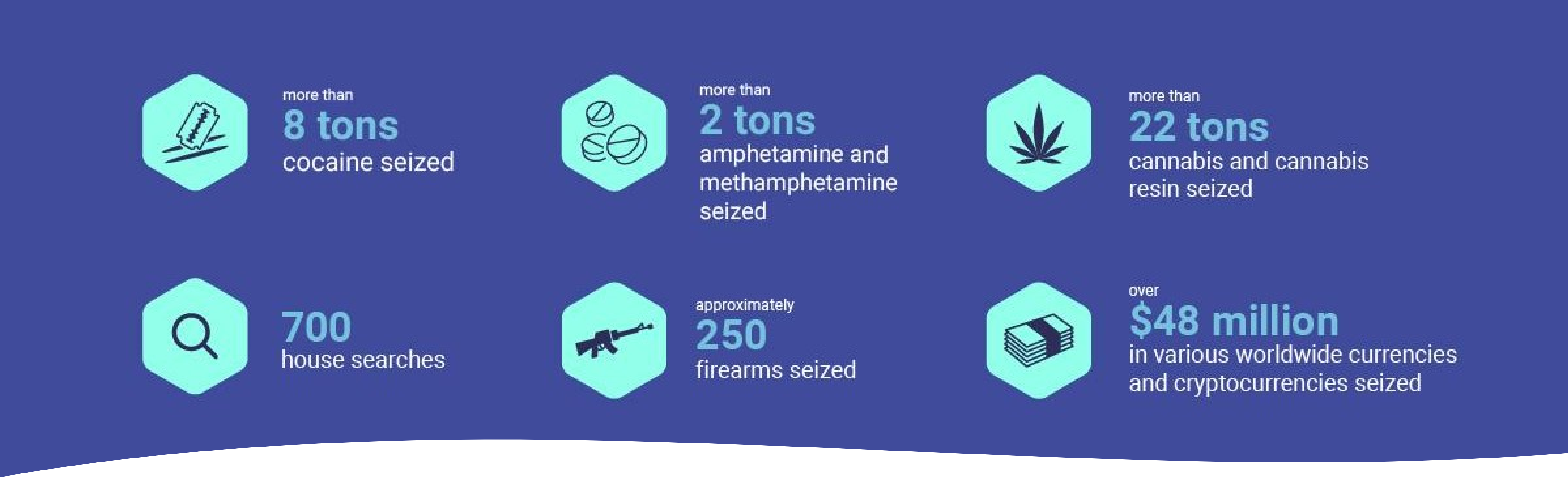
Zhong stole 50,000 BTC from Silk Road, moving it to the below 11 addresses in a series of transactions in September 2012.





Undercover operations and stings

- Creating fake vendor profiles to gather evidence on buyers (sometimes selling substances)
- Posing as buyers to build cases against sellers
- From cyber patrolling to sting operations (ANOM)



more than
8 tons
cocaine seized

more than
2 tons
amphetamine and methamphetamine seized

more than
22 tons
cannabis and cannabis resin seized

700
house searches

approximately
250
firearms seized

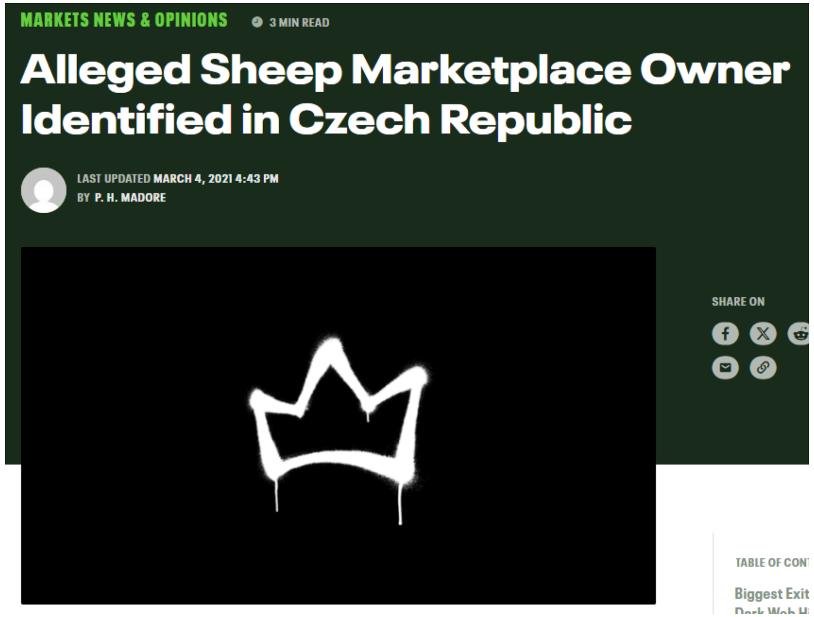
over
$48 million
in various worldwide currencies and cryptocurrencies seized

“The US Federal Bureau of Investigation (FBI), the Dutch National Police (Politie), and the Swedish Police Authority (Polisen), in cooperation with the US Drug Enforcement Administration (DEA) and 16 other countries have carried out with the support of Europol one of the largest and most sophisticated law enforcement operations to date in the fight against encrypted criminal activities.

Since 2019, the US Federal Bureau of Investigation, in close coordination with the Australian Federal Police, strategically developed and covertly operated an encrypted device company, called ANOM, which grew to service more than 12 000 encrypted devices to over 300 criminal syndicates operating in more than 100 countries, including Italian organised crime, outlaw motorcycle gangs, and international drug trafficking organisations.

The goal of the new platform was to target global organised crime, drug trafficking, and money laundering organisations, regardless of where they operated, and offer an encrypted device with features sought by the organised crime networks, such as remote wipe and duress passwords, to persuade criminal networks to pivot to the device.

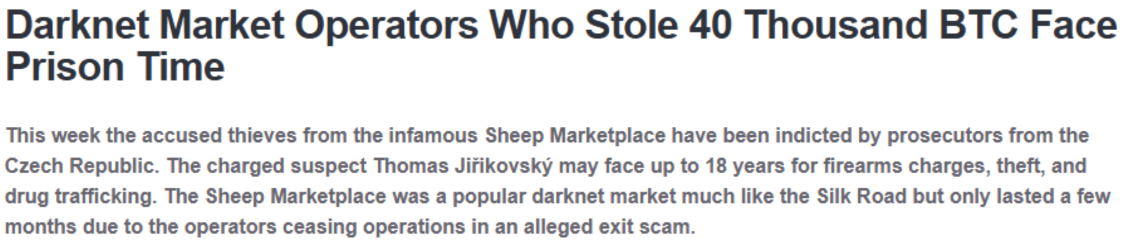
The FBI and the 16 other countries of the international coalition, supported by Europol and in coordination with the US Drug Enforcement Administration, then exploited the intelligence from the 27 million messages obtained and reviewed them over 18 months while ANOM’s criminal users discussed their criminal activities.”



MARKETS NEWS & OPINIONS 3 MIN READ

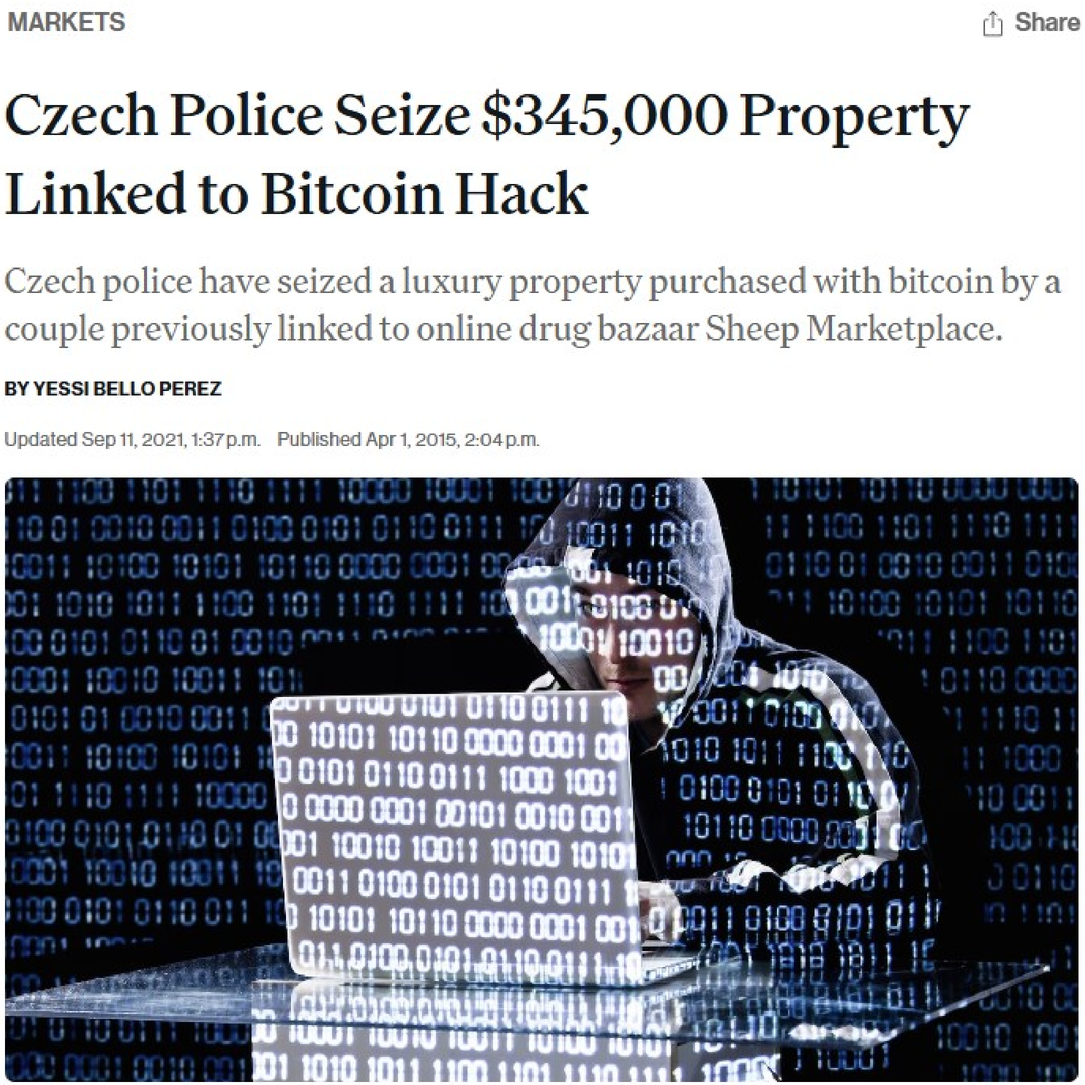
Alleged Sheep Marketplace Owner Identified in Czech Republic

LAST UPDATED MARCH 4, 2021 4:43 PM
BY P. H. MADORE



Darknet Market Operators Who Stole 40 Thousand BTC Face Prison Time

This week the accused thieves from the infamous Sheep Marketplace have been indicted by prosecutors from the Czech Republic. The charged suspect Thomas Jiřikovský may face up to 18 years for firearms charges, theft, and drug trafficking. The Sheep Marketplace was a popular darknet market much like the Silk Road but only lasted a few months due to the operators ceasing operations in an alleged exit scam.



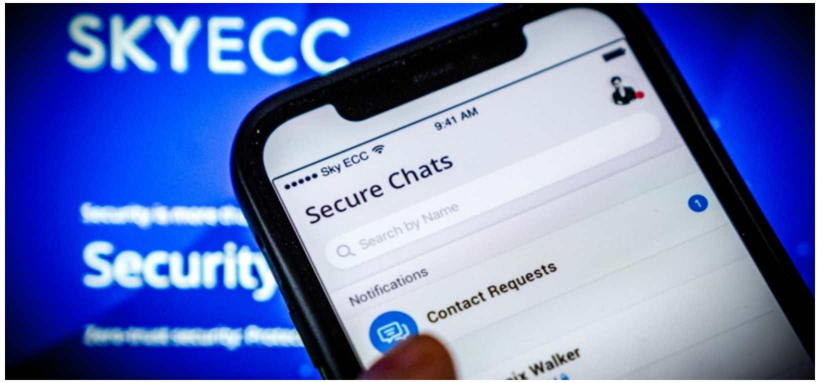
MARKETS

Czech Police Seize $345,000 Property Linked to Bitcoin Hack

Czech police have seized a luxury property purchased with bitcoin by a couple previously linked to online drug bazaar Sheep Marketplace.

BY YESSI BELLO PEREZ

Updated Sep 11, 2021, 1:37 p.m. Published Apr 1, 2015, 2:04 p.m.


SKYECC
Security
Sky ECC
9:41 AM
Secure Chats
Search by Name
Notifications
Contact Requests

ANØM

EncroChat

Feature	EncroChat	Sky ECC	ANOM (Trojan Shield)
Initiator	European police joint op	Belgian/French/Dutch police	FBI & Australian police
Infiltration type	Server-side malware	Phishing-style backdoor	Honeypot / owned platform
Users intercepted	~60,000	~170,000 registered	~11,800 devices
Messages captured	Millions	≈1 billion	27 million
Arrests	~6,500 across Europe	Dozens jailed per country	800+ worldwide
Seizures	€900M assets	17 t cocaine (Belgium alone)	250 guns, 40 t+ drugs
Legal challenges	Admissibility varied	Privacy/fair trial concerns	Entrapment & enticement debates

Mass criminal investigation

InfoCuria
Case-law

Can the evidence be used?

In April 2024, the **CJEU’s EncroChat judgment** delivered a ruling (Case C-670/22) that said:

- European Investigation Orders could be used to lawfully transfer EncroChat data from France to Germany
- Evidence is only admissible if the EIO was properly issued under the rules of the issuing state and the defense had a genuine opportunity to contest it.
- There is no automatic cross-border validation merely because the executing State complied with its own procedures.
- A prosecutor (not necessarily a judge) may issue an EIO for already-obtained evidence
- It isn’t required to show suspicion for each person a priori if national law doesn’t demand that.
- While the lawfulness of the collection itself isn't examined by the issuing authority, national courts must exclude the evidence if the defense cannot meaningfully challenge it under Article 14(7) of the EIO Directive.

Can the evidence be used?

Article 14(7) of Directive 2014/41

must be interpreted as meaning that, in criminal proceedings against a person suspected of having committed criminal offences, national criminal courts are required to disregard information and evidence if that person is not in a position to comment effectively on that information and on that evidence and the said information and evidence are likely to have a preponderant influence on the findings of fact.

Legal trends

Legal hacking

- Source interception
- Infiltration of computer systems
- Activating of hardware (France [?], Sweden, Belgium, Italy, Norway, Poland, Romania, etc.)
- Independent supervision (France, the Netherlands, Sweden)
- Different safeguards

Necessary safeguards

- A clear distinction between the so-called online searches and the use of equipment to monitor its surroundings;
- Restricted only to the most serious offences (accidental findings);
- Judicial warrant stating clearly:
  - — Target devices and the content sought;
  - — Scope of the measure (suspects, duration, data);
  - — The terms in which the data may be searched and accessed;
  - — Persons authorized to use it in a given investigation;
  - — Authorization to keep copies of the information.

Necessary safeguards

- Duty of notification;
- External oversight;
- The need for periodic review of the need for this measure;
- Implementation of a certification system for the malware;
- Right of the defence to access all of the relevant information, excluding that which is strictly operational;
- Creation of measures for uninstalling the malware.
- The right of the defence to confirm that the malware used is certified.

Cyber patrolling and undercover operations

- **Cyber patrolling**: proactive monitoring of online spaces by law enforcement to detect and investigate criminal activity (Internet scanning, OSINT, AI)
- **Undercover operations**: Covert infiltration. Includes interaction with third parties (in open or closed channels)

Cyber patrolling and undercover operations

- **Monitoring chatrooms?**

“The risk of being overheard by an eavesdropper … or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak” – Hoffa v. United States - 385 U.S. 293, 87 S. Ct. 408 (1966)

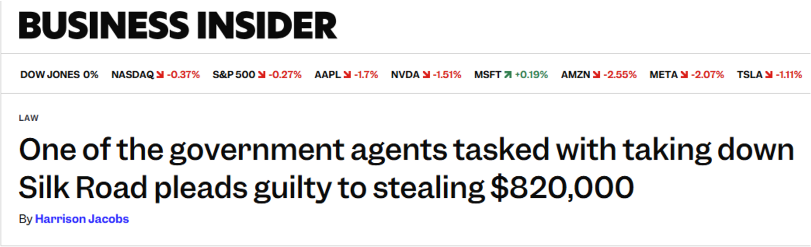
- **When does cyber-patrolling become an undercover operation?**

Undercover operations

Unified approach (e.g. Portugal and Spain)

vs

Differentiated approach (France)



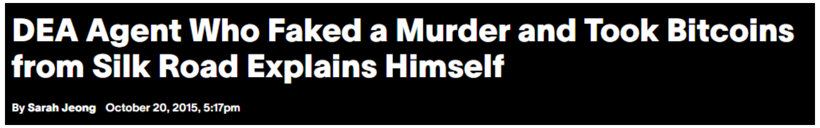
BUSINESS INSIDER

DOW JONES 0% NASDAQ ↘ -0.37% S&P 500 ↘ -0.27% AAPL ↘ -1.7% NVDA ↘ -1.51% MSFT ↗ +0.19% AMZN ↘ -2.55% META ↘ -2.07% TSLA ↘ -1.11%

LAW

One of the government agents tasked with taking down Silk Road pleads guilty to stealing $820,000

By Harrison Jacobs



DEA Agent Who Faked a Murder and Took Bitcoins from Silk Road Explains Himself

By Sarah Jeong October 20, 2015, 5:17pm

Risks

Undercover operations: what we need to have

- Judicial warrant specifying (law or good practices):
  - Need for the operation (proportionality assessment)
  - Duration and purposes of the operation;
  - List of usable nicknames;
  - List of computer systems or locations from which the operation may take place;
  - List of actions that are authorized (e.g. recording of communications)
  - In case the undercover agent is not from law enforcement, limitation of access to the credentials.

Undercover operations: what we need to have

- Clarification of the criteria for the existence of an online undercover operation;
- Obligation to disclose the existence of an undercover operation with adequate reporting of the undercover agent’s actions;
- Allowing the undercover agent to send illegal content when strictly necessary;
- Allowing for the monitorization of these files as they are resent;
- Restricting cases where infiltration is made with existing accounts;
- Adapting the crimes subject to this measure to cybercrime.

Undercover operations and entrapment

Entrapment criteria according to ECHR (Bannikova v Russia):

the Court would apply the substantive test of incitement, which entailed examining

- whether there were objective suspicions that the applicant had been involved in or was predisposed to criminal activity,
- whether the undercover agents had merely "joined" the criminal acts or had instigated them,
- and whether they had subjected the applicant to pressure to commit the offence

Concluding remarks

Thank you!

David Silva Ramalho

dsramalho@mlgts.pt

The nexus between Artificial Intelligence and Criminal Law

David Silva Ramalho – dsramalho@mlgts.pt

Lawyer – Morais Leitão

Assistant Teacher – University of Lisbon’s Faculty of Law

ERA

SKYNET
NEURAL NET-BASED ARTIFICIAL INTELLIGENCE
CYBERDYNE SYSTEMS CORPORATION

Co-funded by the European Union

Main components of AI

1. **The Algorithm:** instructions to perform a calculation or to solve a given problem, implementable by a computer.

2. **The Data:** units of information, usually about people or objects, either quantitative or qualitative.

3. **The Computer:** computer resources needed to process the AI model

4. **The Human:** they develop and control the models

Definition of AI

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

Article 3 (1) of the AI Act

Main functions of AI

1. **Automation**: AI systems can automate repetitive tasks with high efficiency and accuracy, reducing the need for human intervention. This is seen in manufacturing, customer service (chatbots), and administrative processes.

2. **Data Analysis and Pattern Recognition**: AI can process large amounts of data quickly to identify patterns, trends, and insights that are difficult for humans to detect. This is critical in fields like finance, marketing, and scientific research.

Main functions of AI

3. **Decision-Making**: AI systems are used to assist or even make autonomous decisions based on pre-defined criteria and data analysis. Examples include recommendation systems (e.g., Netflix or Amazon), credit scoring, and risk management systems.

4. **Learning and Adaptation (Machine Learning)**: AI systems can learn from data and improve their performance over time without being explicitly programmed. This function is at the heart of AI technologies like neural networks and deep learning.

Main functions of AI

5. **Vision and Perception:** AI is used in image recognition, object detection, and video analysis. Applications range from facial recognition and autonomous vehicles to medical imaging and quality control in manufacturing.

6. **Robotics and Control Systems:** AI enables robots to perform complex tasks, from industrial automation to healthcare assistance, by giving them the ability to sense, plan, and act in dynamic environments.

Main functions of AI

7. **Prediction and Forecasting:** AI models are used to make predictions about future events or behaviors, such as weather forecasting, stock market predictions, or anticipating customer behavior in retail.

AI in criminal investigation

ERA

SKYNET

NEURAL NET-BASED ARTIFICIAL INTELLIGENCE

CYBERDYNE SYSTEMS CORPORATION

Main uses for AI in criminal proceedings

Specific uses:

1. **Predictive vigilance:** including predictive policing and facial recognition. Allocating police resources.

2. **Predicting risks:** reoffending, flight risk, evidence destruction, asset dissipation

3. **Deciding (or assisting), namely on sentencing and parole:** dangerousness of the offender

Dutch police are using AI to pick out the most solvable cold cases

Dutch Police are using artificial intelligence to crack unsolved cases, according to The Next Web.

The national police force is working to digitize the more than 1,500 reports and 30 million pages of material in its cold case archive, only 15 percent of which is currently stored electronically. (The Dutch police defines a cold case as any case since 1988 that carries a jail sentence for over 12 years and has gone unsolved for at least three years.) Once the transfer is complete, a machine learning algorithm will begin combing through the records and deciding which cases have the most promising evidence, reducing case processing time from weeks to a single day.

AI and Criminal Law

ERA

OCP

OMNI CONSUMER PRODUCTS

Possible scenarios

Types of AI systems

- **Deterministic robots**: pre-programmed and aimed at performing specific tasks;

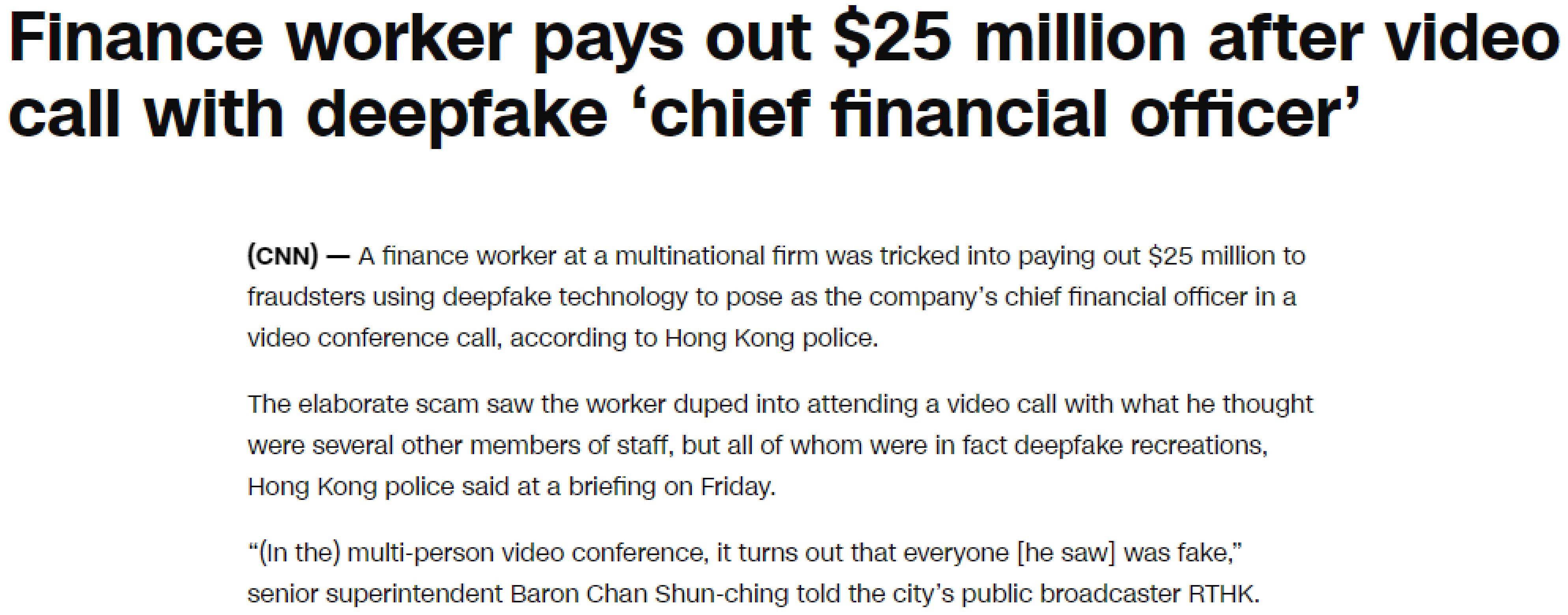
- **Cognitive robots**: systems that are capable of acting with autonomy in complex situations, making choices and performing tasks that have not been previously programmed and that were in fact unpredictable to the programmer (e.g. customer interaction).

Possible scenarios

AI and crime

- AI is programmed or created to commit a crime;
- AI commits a crime due to faulty programming;
- AI commits a crime accidentally;
- AI commits a crime due to its own “decision” (autonomous, unpredictable, unprogrammed decision)

The “easy” cases: AI for crimes



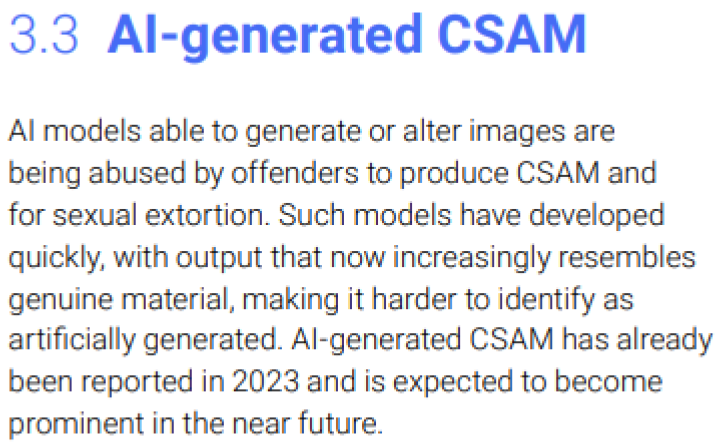
Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

(CNN) — A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company’s chief financial officer in a video conference call, according to Hong Kong police.

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

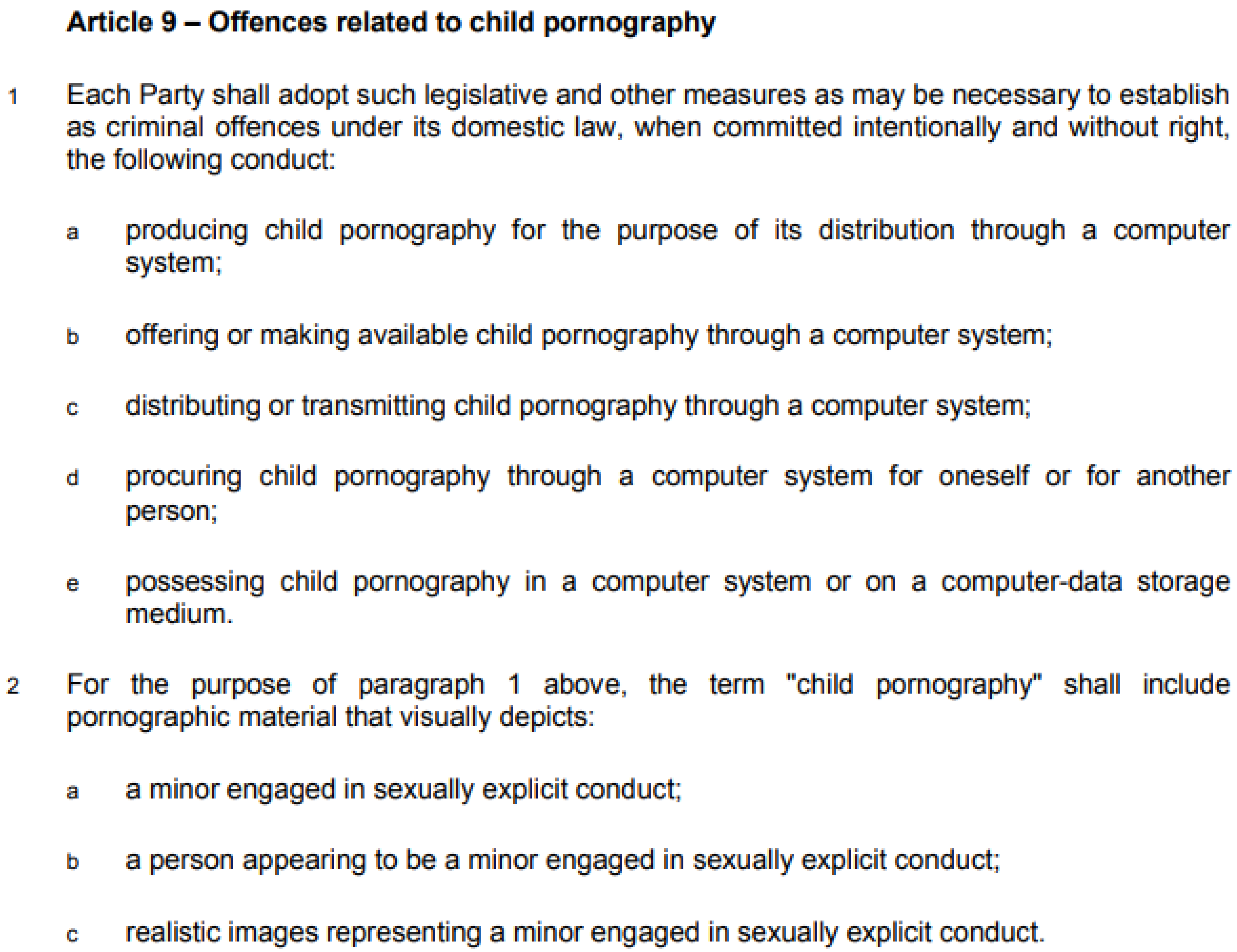
“(In the) multi-person video conference, it turns out that everyone [he saw] was fake,” senior superintendent Baron Chan Shun-ching told the city’s public broadcaster RTHK.

The “easy” cases: AI for crimes - CSAM



3.3 AI-generated CSAM

AI models able to generate or alter images are being abused by offenders to produce CSAM and for sexual extortion. Such models have developed quickly, with output that now increasingly resembles genuine material, making it harder to identify as artificially generated. AI-generated CSAM has already been reported in 2023 and is expected to become prominent in the near future.



Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

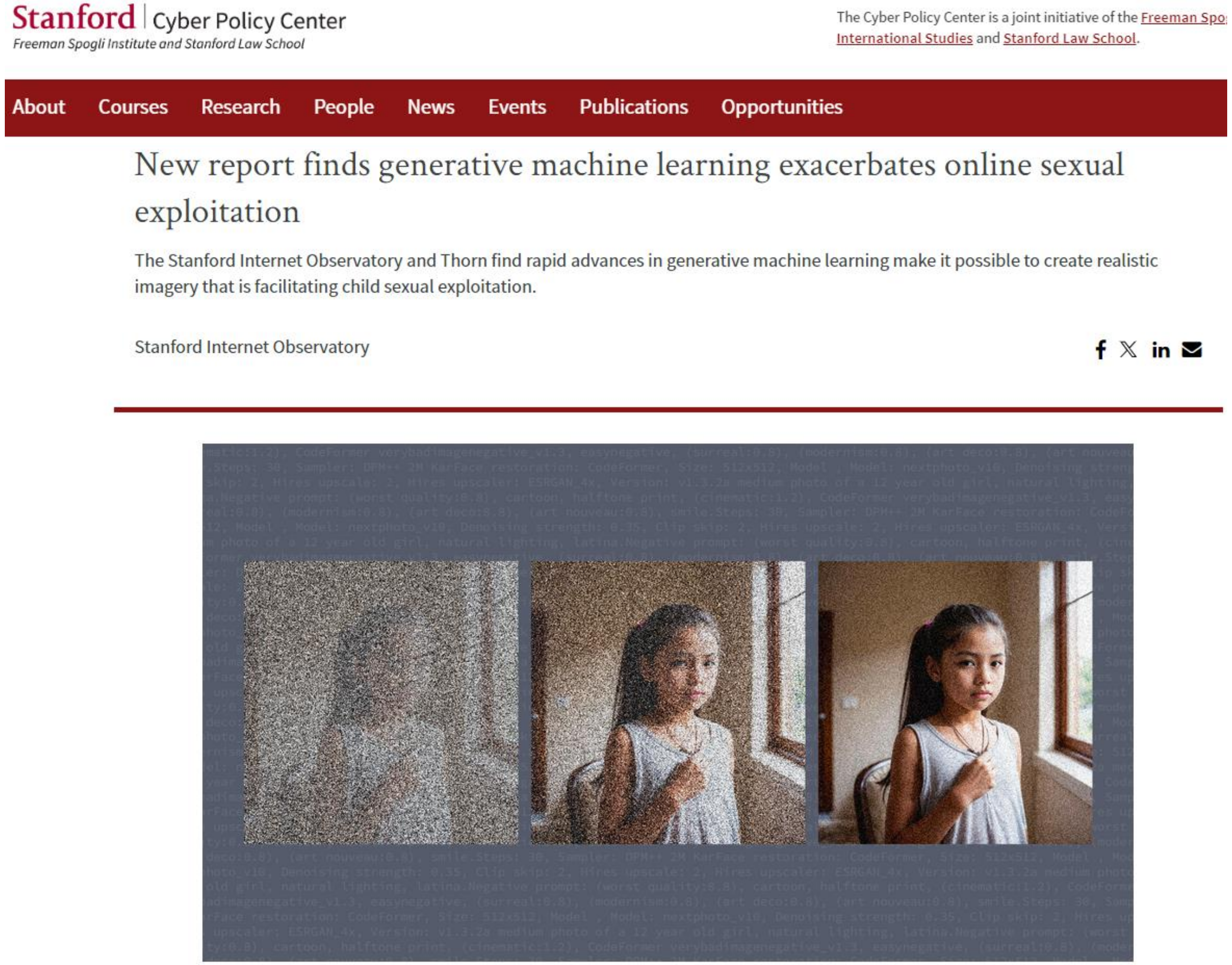
2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

The "easy" cases: child abuse



Stanford | Cyber Policy Center
Freeman Spogli Institute and Stanford Law School

The Cyber Policy Center is a joint initiative of the Freeman Spo
International Studies and Stanford Law School.

New report finds generative machine learning exacerbates online sexual exploitation

The Stanford Internet Observatory and Thorn find rapid advances in generative machine learning make it possible to create realistic imagery that is facilitating child sexual exploitation.

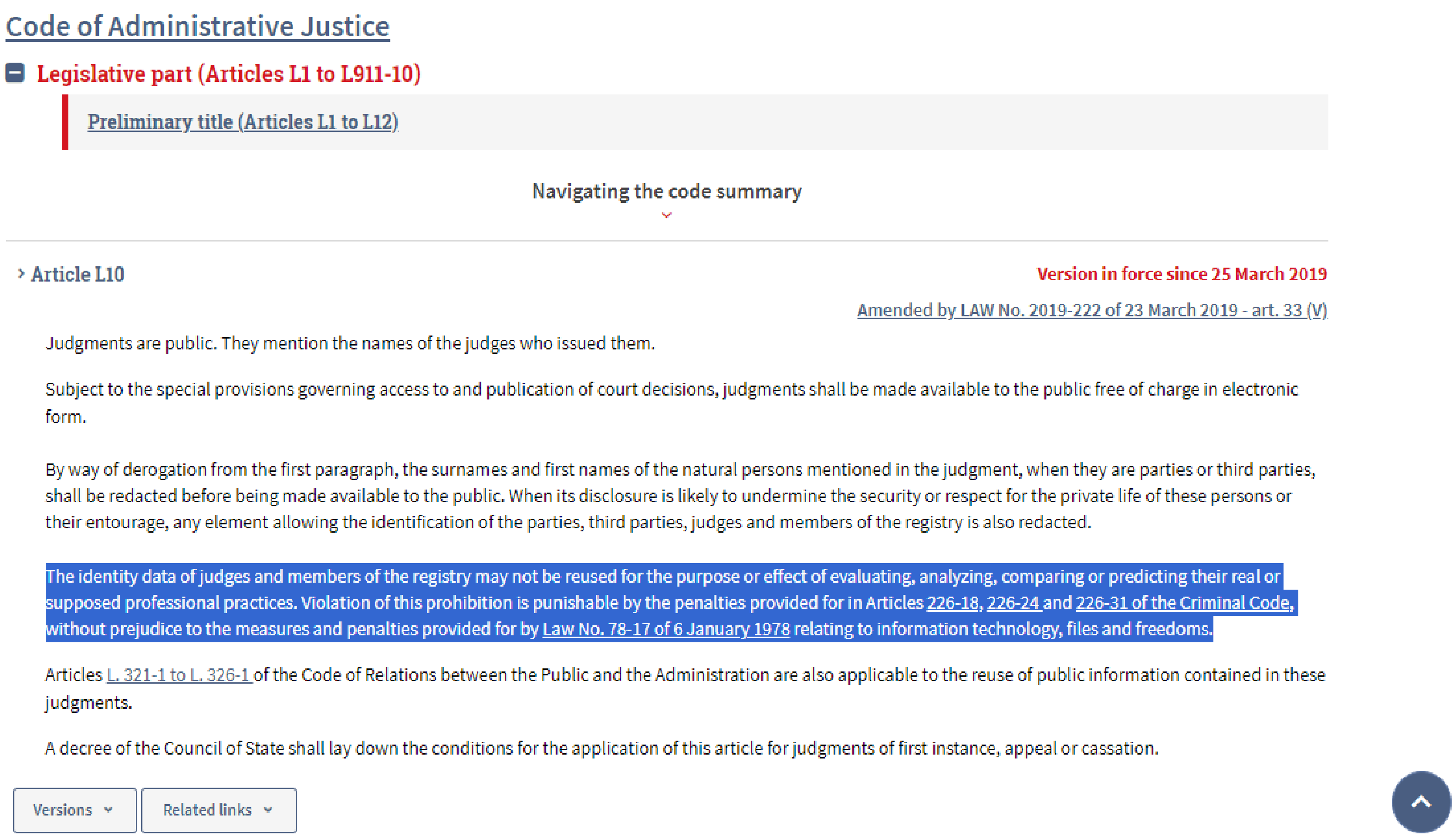
Stanford Internet Observatory

The “easy” cases

Conclusion:

- AI is just another tool to commit offenses.
- Criminal activity is covered by general provisions.
- Possibility to hold the programmer liable in certain conditions.
- Some new offences may need to be created.

The “easy” cases: new crimes



Code of Administrative Justice

Legislative part (Articles L1 to L911-10)

Preliminary title (Articles L1 to L12)

Article L10

Version in force since 25 March 2019

Amended by LAW No. 2019-222 of 23 March 2019 - art. 33 (V)

Judgments are public. They mention the names of the judges who issued them.

Subject to the special provisions governing access to and publication of court decisions, judgments shall be made available to the public free of charge in electronic form.

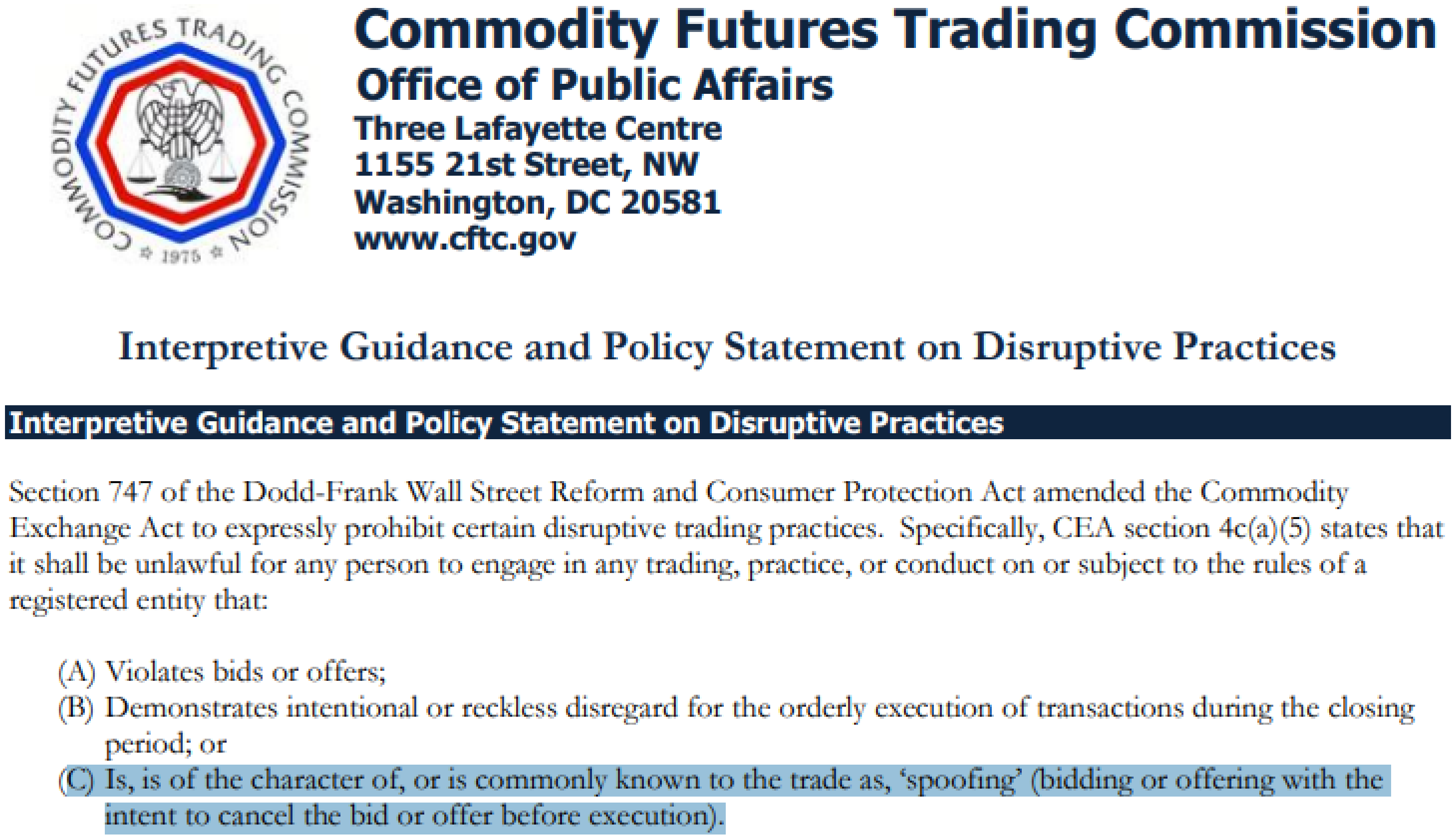
By way of derogation from the first paragraph, the surnames and first names of the natural persons mentioned in the judgment, when they are parties or third parties, shall be redacted before being made available to the public. When its disclosure is likely to undermine the security or respect for the private life of these persons or their entourage, any element allowing the identification of the parties, third parties, judges and members of the registry is also redacted.

The identity data of judges and members of the registry may not be reused for the purpose or effect of evaluating, analyzing, comparing or predicting their real or supposed professional practices. Violation of this prohibition is punishable by the penalties provided for in Articles 226-18, 226-24 and 226-31 of the Criminal Code, without prejudice to the measures and penalties provided for by Law No. 78-17 of 6 January 1978 relating to information technology, files and freedoms.

Articles L. 321-1 to L. 326-1 of the Code of Relations between the Public and the Administration are also applicable to the reuse of public information contained in these judgments.

A decree of the Council of State shall lay down the conditions for the application of this article for judgments of first instance, appeal or cassation.

The “easy” cases: new crimes



Commodity Futures Trading Commission
Office of Public Affairs
Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581
www.cftc.gov

Interpretive Guidance and Policy Statement on Disruptive Practices

Interpretive Guidance and Policy Statement on Disruptive Practices

Section 747 of the Dodd-Frank Wall Street Reform and Consumer Protection Act amended the Commodity Exchange Act to expressly prohibit certain disruptive trading practices. Specifically, CEA section 4c(a)(5) states that it shall be unlawful for any person to engage in any trading, practice, or conduct on or subject to the rules of a registered entity that:

(A) Violates bids or offers;
(B) Demonstrates intentional or reckless disregard for the orderly execution of transactions during the closing period; or
(C) Is, is of the character of, or is commonly known to the trade as, ‘spoofing’ (bidding or offering with the intent to cancel the bid or offer before execution).

The “hard” cases

What happens when the crime is:

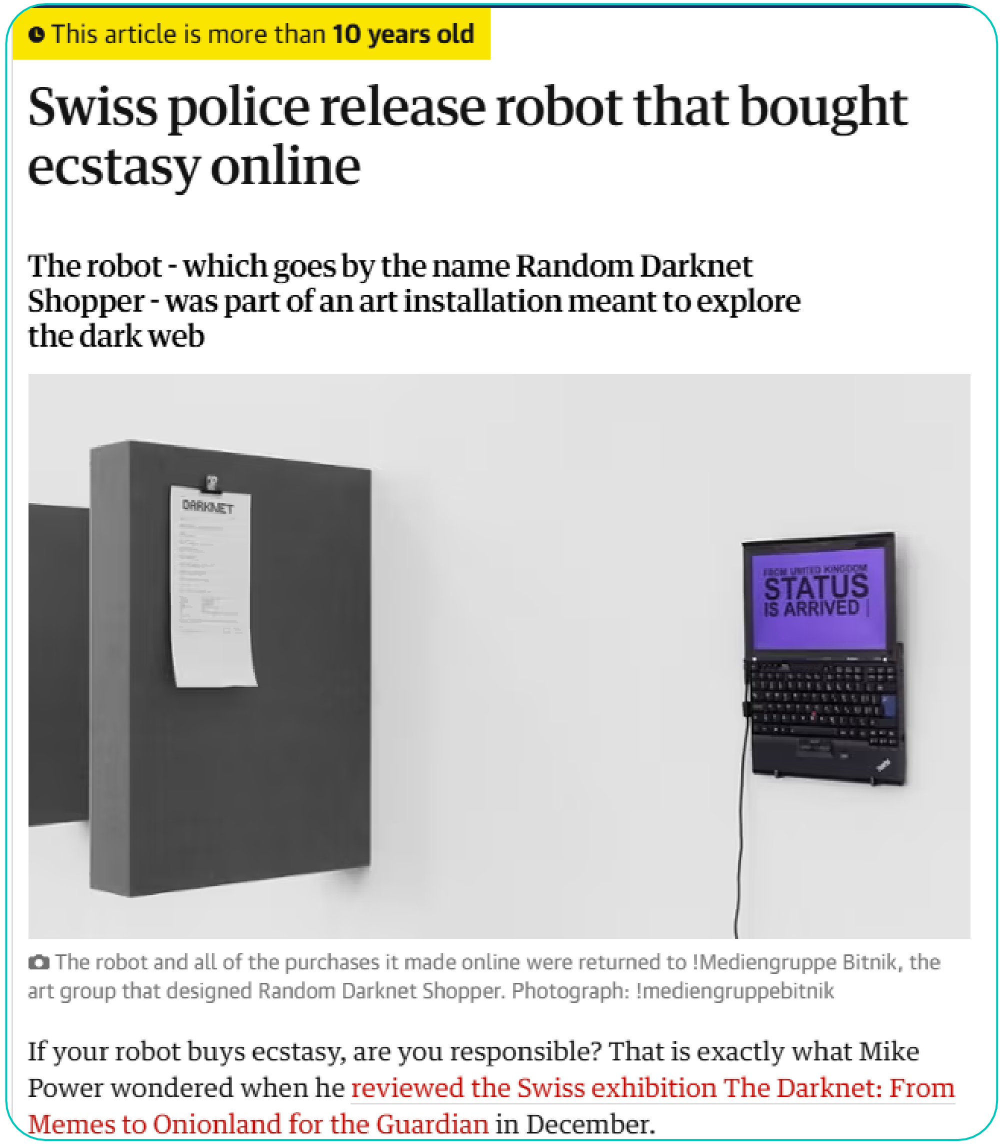
- Unpredictable
- Autonomous
- Unexplainable
- Robotic

The responsibility gap

Who do we blame?

Who do we blame?

- AI programmers (those who collect the data and train the algorithm)?
- Machine-makers?
- The owners?
- Those who market it?
- The AI system?



This article is more than **10 years old**

Swiss police release robot that bought ecstasy online

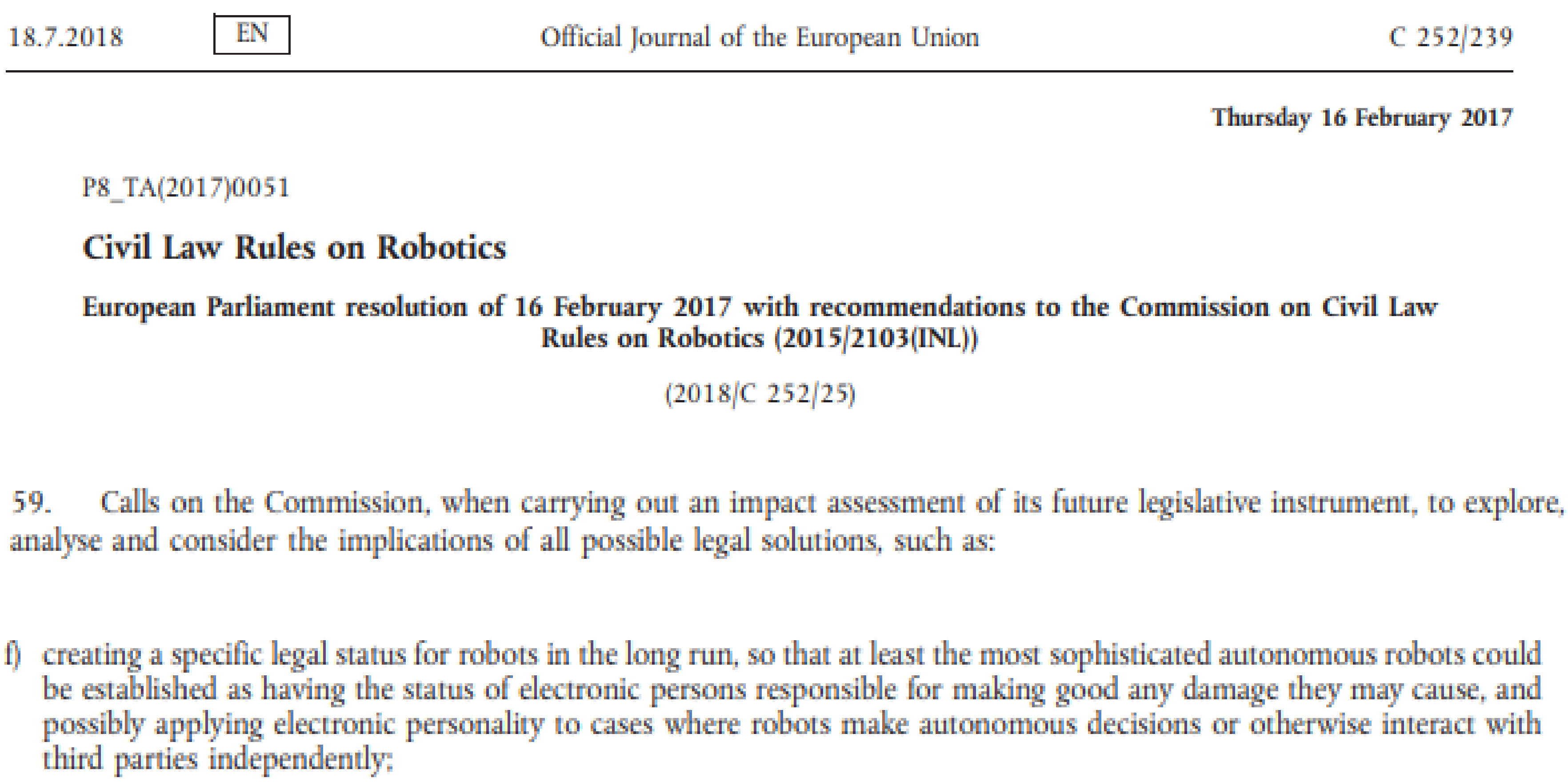
The robot - which goes by the name Random Darknet Shopper - was part of an art installation meant to explore the dark web

The robot and all of the purchases it made online were returned to !Mediengruppe Bitnik, the art group that designed Random Darknet Shopper. Photograph: !mediengruppebitnik

If your robot buys ecstasy, are you responsible? That is exactly what Mike Power wondered when he reviewed the Swiss exhibition The Darknet: From Memes to Onionland for the Guardian in December.

Who do we blame?

Who do we blame?



18.7.2018 EN Official Journal of the European Union C 252/239

Thursday 16 February 2017

P8_TA(2017)0051

Civil Law Rules on Robotics

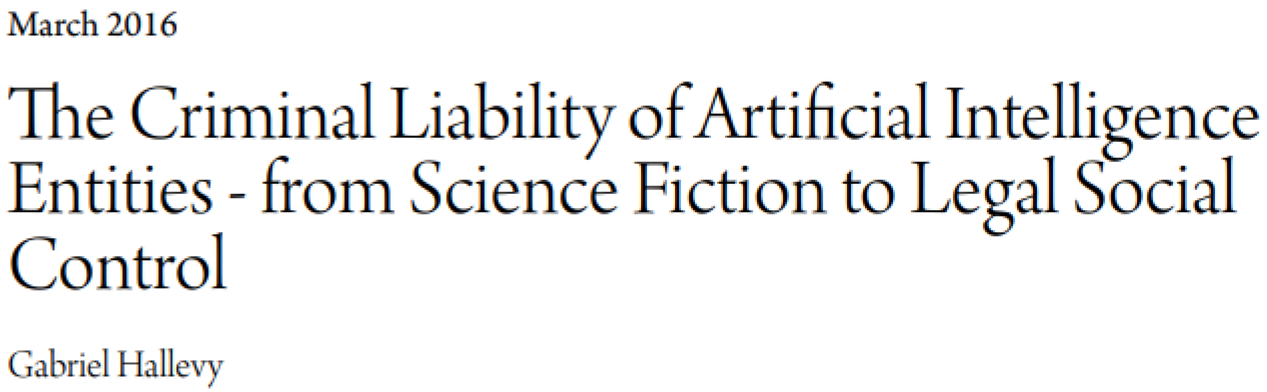
European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))

(2018/C 252/25)

59. Calls on the Commission, when carrying out an impact assessment of its future legislative instrument, to explore, analyse and consider the implications of all possible legal solutions, such as:

f) creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently;

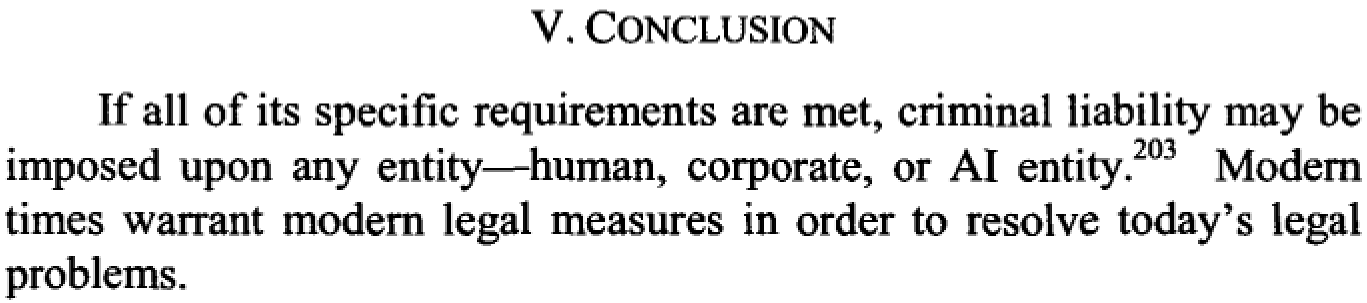
Who do we blame?



March 2016

The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control

Gabriel Hallevy

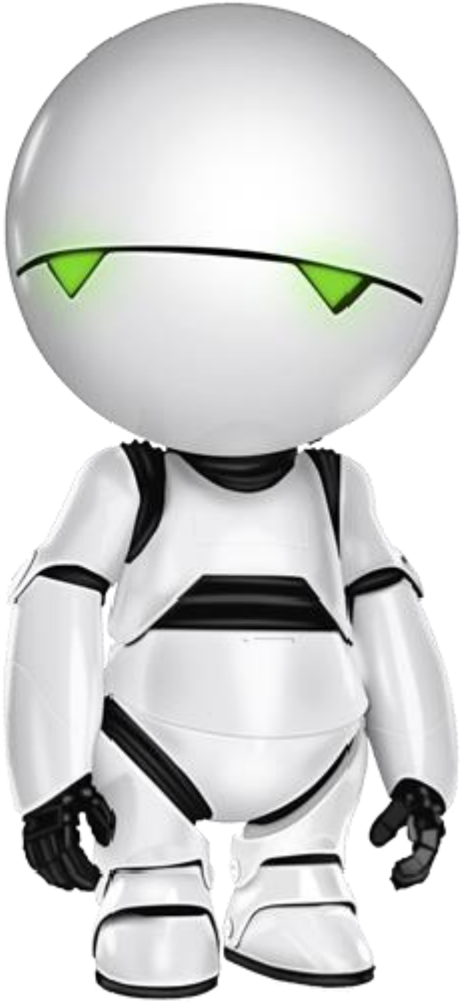


V. CONCLUSION

If all of its specific requirements are met, criminal liability may be imposed upon any entity—human, corporate, or AI entity.[203] Modern times warrant modern legal measures in order to resolve today's legal problems.

Problem with this solution

- It confuses crime with result
- The concept of blame is, at this stage, intrinsically human
- Criminal liability depends on the subject's ability to be conscious, act rightfully and understand the meaning of the norm.
- There is an ethical basis in criminal punishment
- It leaves the makers unpunished
- Not comparable with corporate liability (Susana Aires de Sousa)



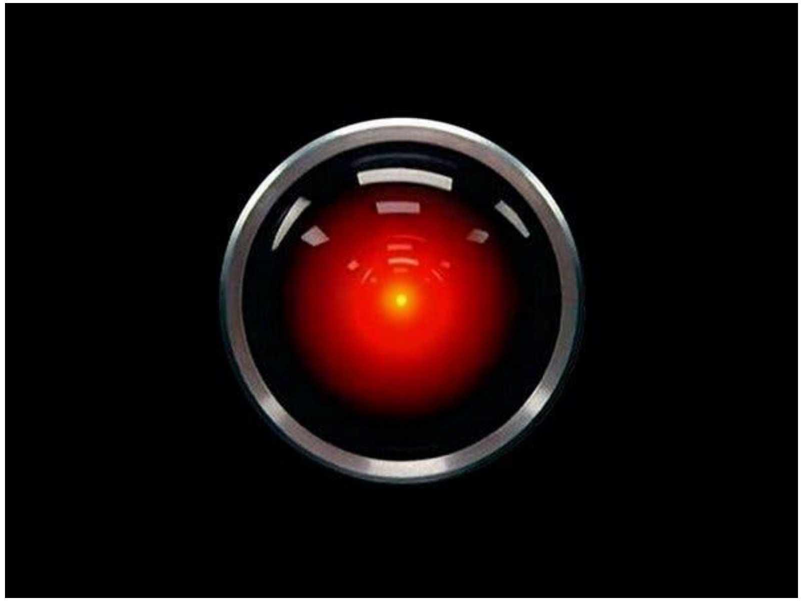
Causality

- The black box problem

- Lack of visibility to the decision-making process.

- If causality needs to be adequate, then foreseeability is required.

- After the risk has materialized, failure to act may fulfill this requirement



Agency

- Should AI be treated like an employee, or more like a product (such that product liability and manufacturer duty concepts apply), or more like an animal (requiring the owner's responsibility)

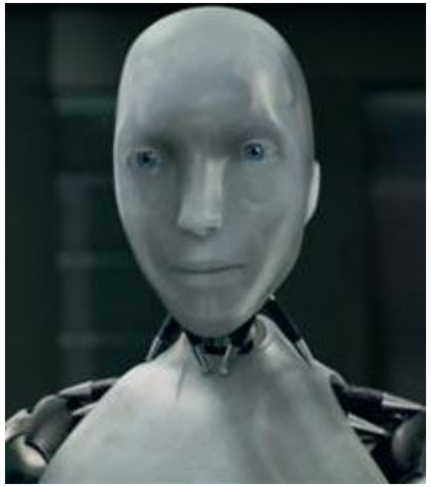
- The action of the AI system vs the omission of the producer (requisites).

- There may be action if someone uses the AI system for a crime, regardless of where the agent understands the causal chain and the mechanisms involved.

Intent, knowledge, recklessness or negligence (mens rea)?

- The creator of the AI system does not want the result.

- The system may aim at a result that is not desired but is the consequence of the mission it has received.



Corporate criminal liability?

- Not all countries have it.

- It still requires human behaviour.

- If the algorithm “decides” to act in an unforeseeable manner, there lacks a relevant human conduct.

- Liability for not anticipating what cannot be anticipated?

- Without human conduct, there is no criminal liability (corporate mind?).

Product liability?

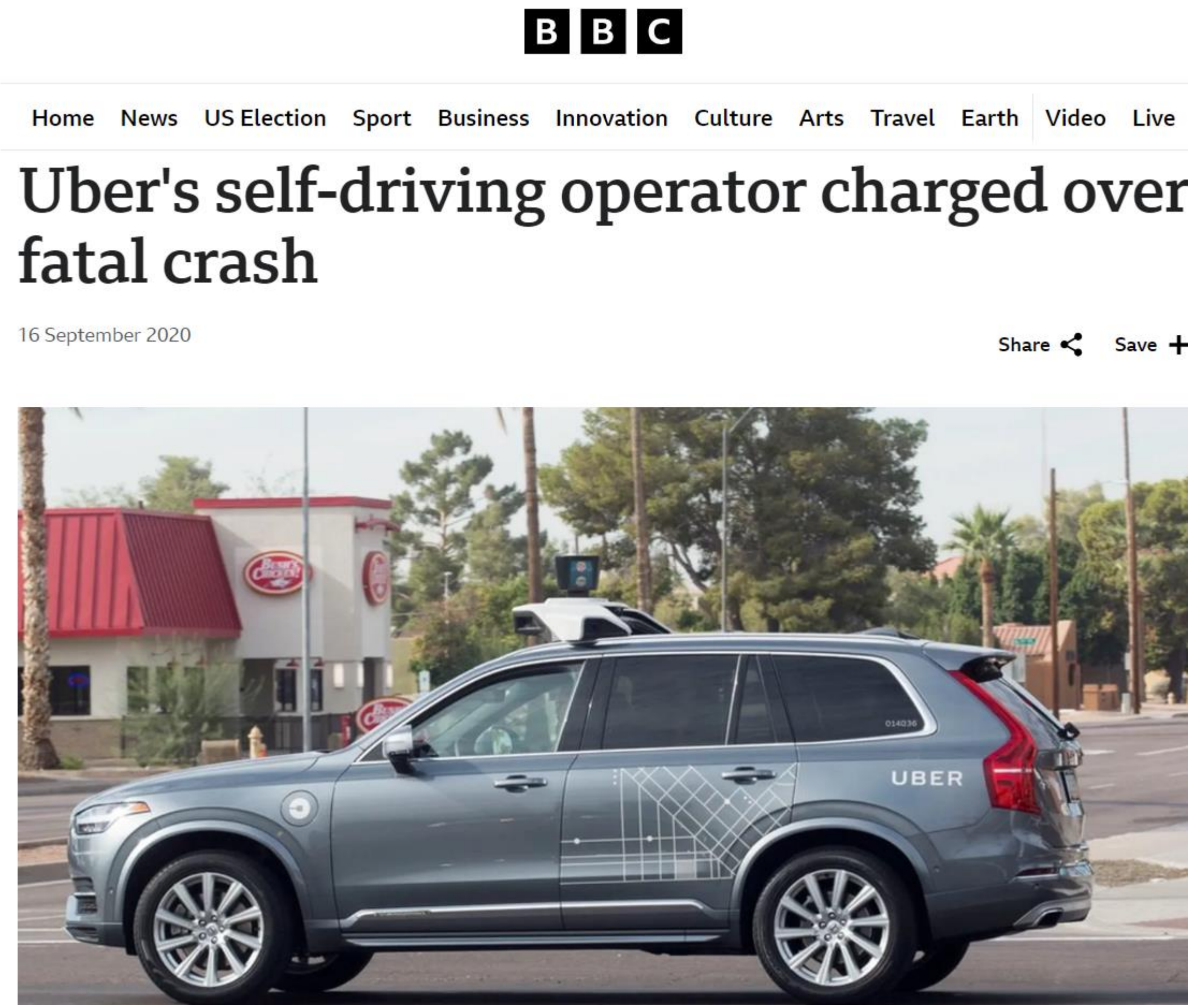
- Mostly for civil cases.
- Classic case: faulty programming leading to a car hitting someone.
- Easy if there is a safety violation that may be attributable to someone
- Implementation of safety procedures and regulation may give grounds for criminal liability (it suggests negligence)

Product liability?

- The design test: AI must be compatible with this and that principle.
- The principle of precaution: “dangerous until proven safe”
- The need for responsive regulation and the sandbag approach.
- Criminal principles and general theory are lost…

… like tears in the rain

The Elaine Herzberg case



BBC

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

Uber's self-driving operator charged over fatal crash

16 September 2020

Share Save

The Elaine Herzberg case

- Elaine Herzberg was crossing a road pushing a bicycle.
- The car did not detect that the obstacle was, in fact, a person, and did not activate the designated driver function.
- Only the driver was charged for manslaughter.
- Ended in plea bargain for endangerment.

Final remarks

Thank you!

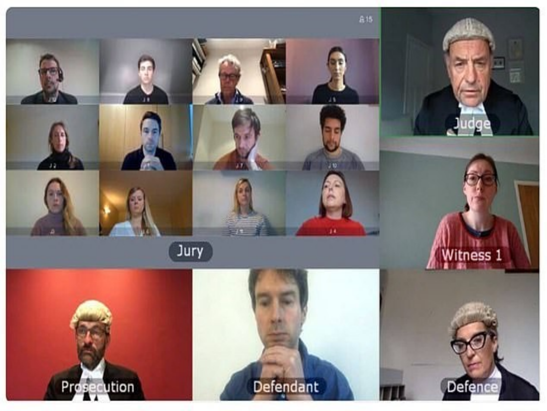
“What are you doing” Dav[e] Silva Ramalho

dsramalho@mlgts.pt

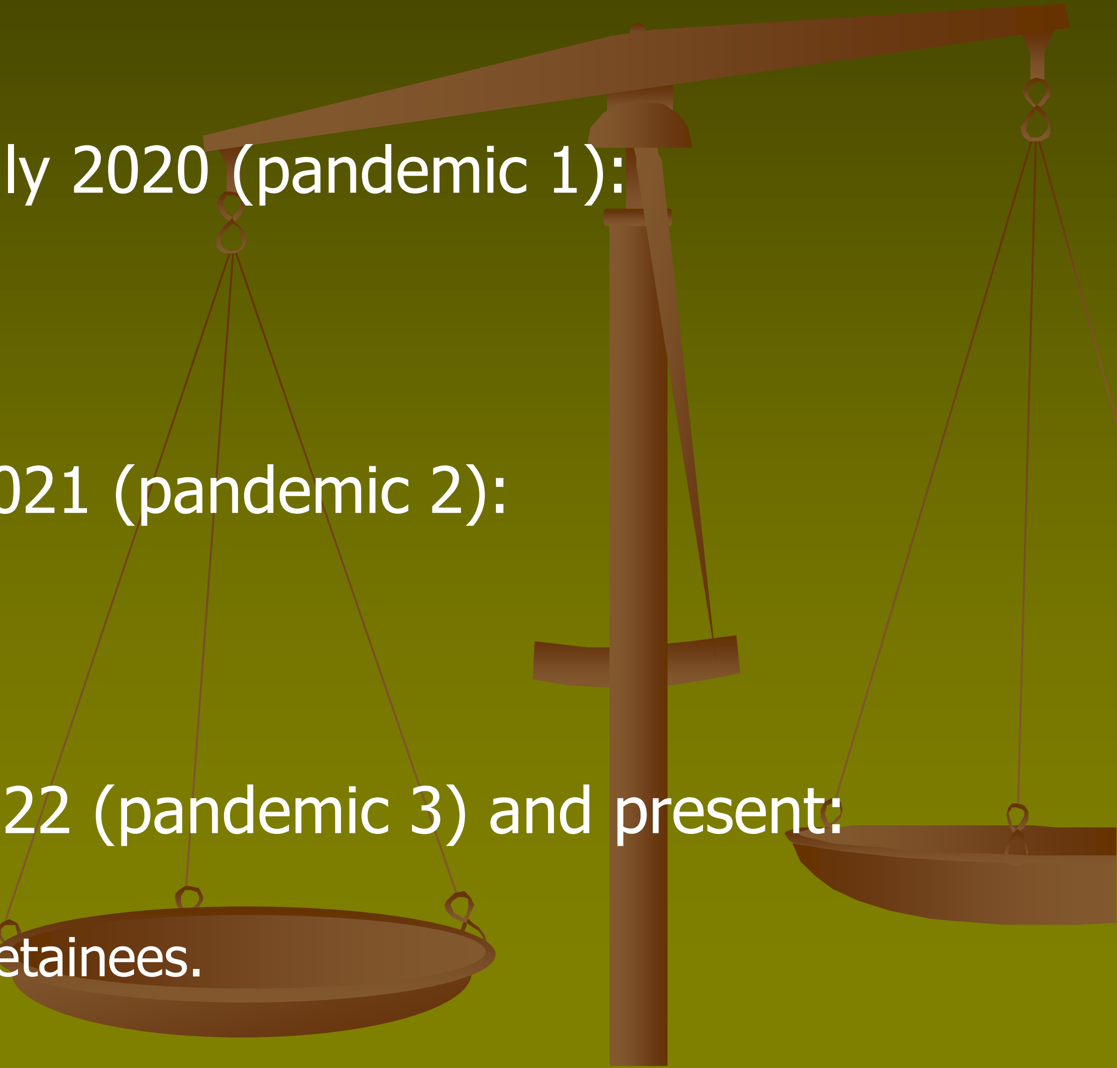
Presenting evidence in court: e-files, videoconferences and remote trials.

Andrea CRUCIANI
Judge at Military Tribunal of Naples

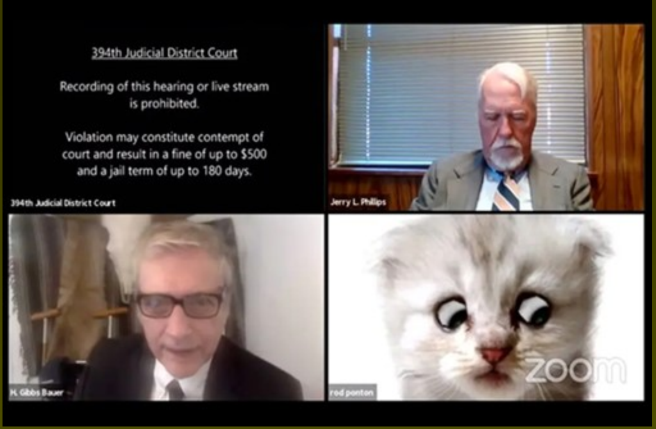
Co-funded by the European Union



Online remote trials



- 1) 9 march 2020 - 31 July 2020 (pandemic 1):
- Parties consent not needed.
- 2) up to 31 december 2021 (pandemic 2):
- Parties consent needed.
- 3) up to 31 december 2022 (pandemic 3) and present:
- No remote trials, except for detainees.



394th Judicial District Court

Recording of this hearing or live stream is prohibited.

Violation may constitute contempt of court and result in a fine of up to $500 and a jail term of up to 180 days.

Remote trials

- Creating a Microsoft Teams Channel for each single proceeding; Inviting by e-mails all the parties with guest-links ("Join Microsoft Teams Meeting").

- Checking the quality of the connection (https://www.youtube.com/watch?v=lGOofzZOyl8) and giving specific instructions on the functioning of remote trials.

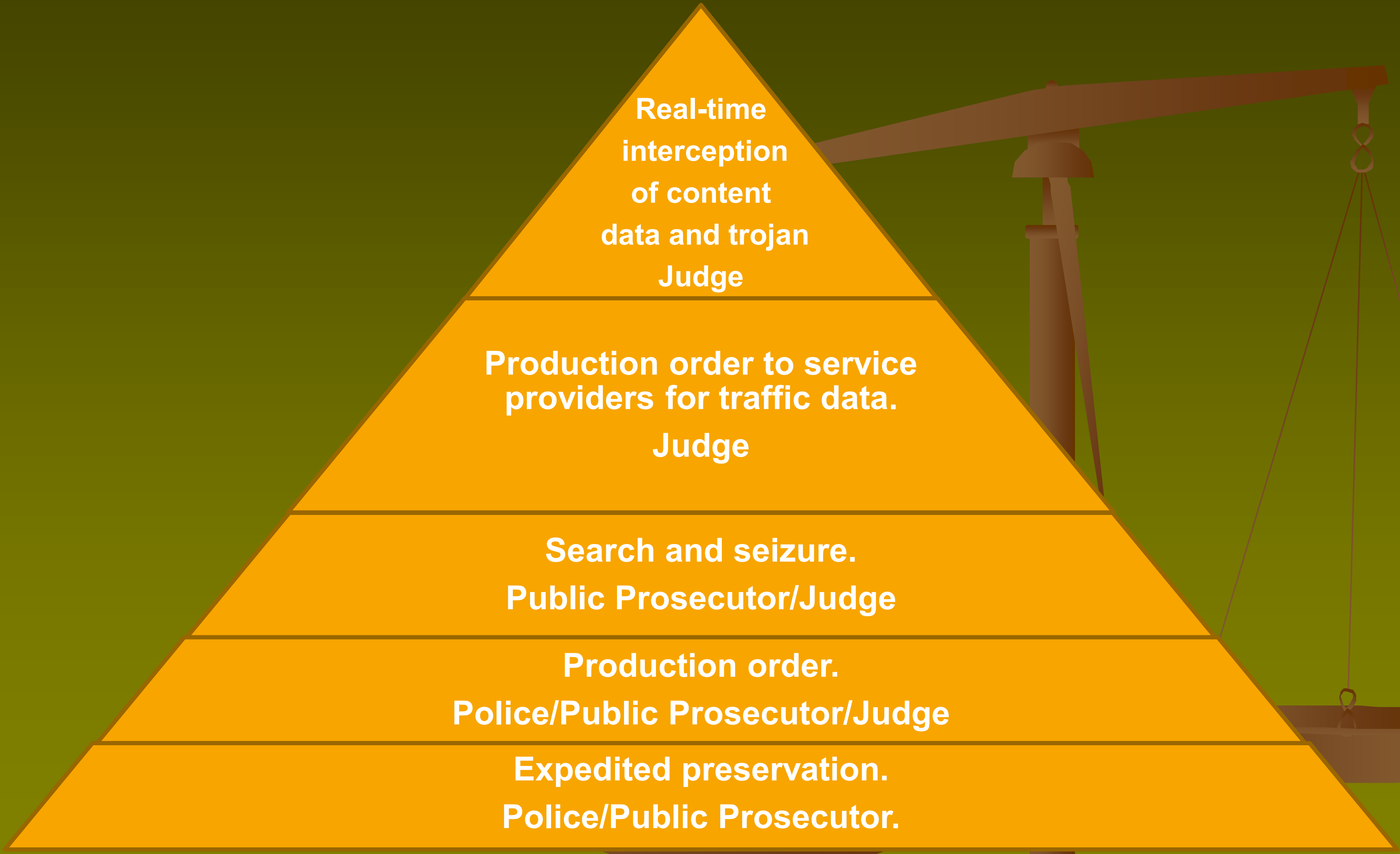
- Defence lawyer certifies the identity of the defendant (when not a detainee).

- Presentation of analogic/physical and electronic evidence.

- Closing statements and final judgment.

E-evidence.

- Before and after 2021 (CJEU, Grand Chamber, 2 March 2021, H. K. c. /Prokuratuur, C-746/18).
- Documents/computer data (pictures, office documents stored in the memory of pc or smarthone);
- Past communications (e-mails; whatsapp messages);
- Service providers traffic data (GPS positioning);
- Service providers real-time content data;



Real-time interception of content data and trojan

Judge

Production order to service providers for traffic data.

Judge

Search and seizure.

Public Prosecutor/Judge

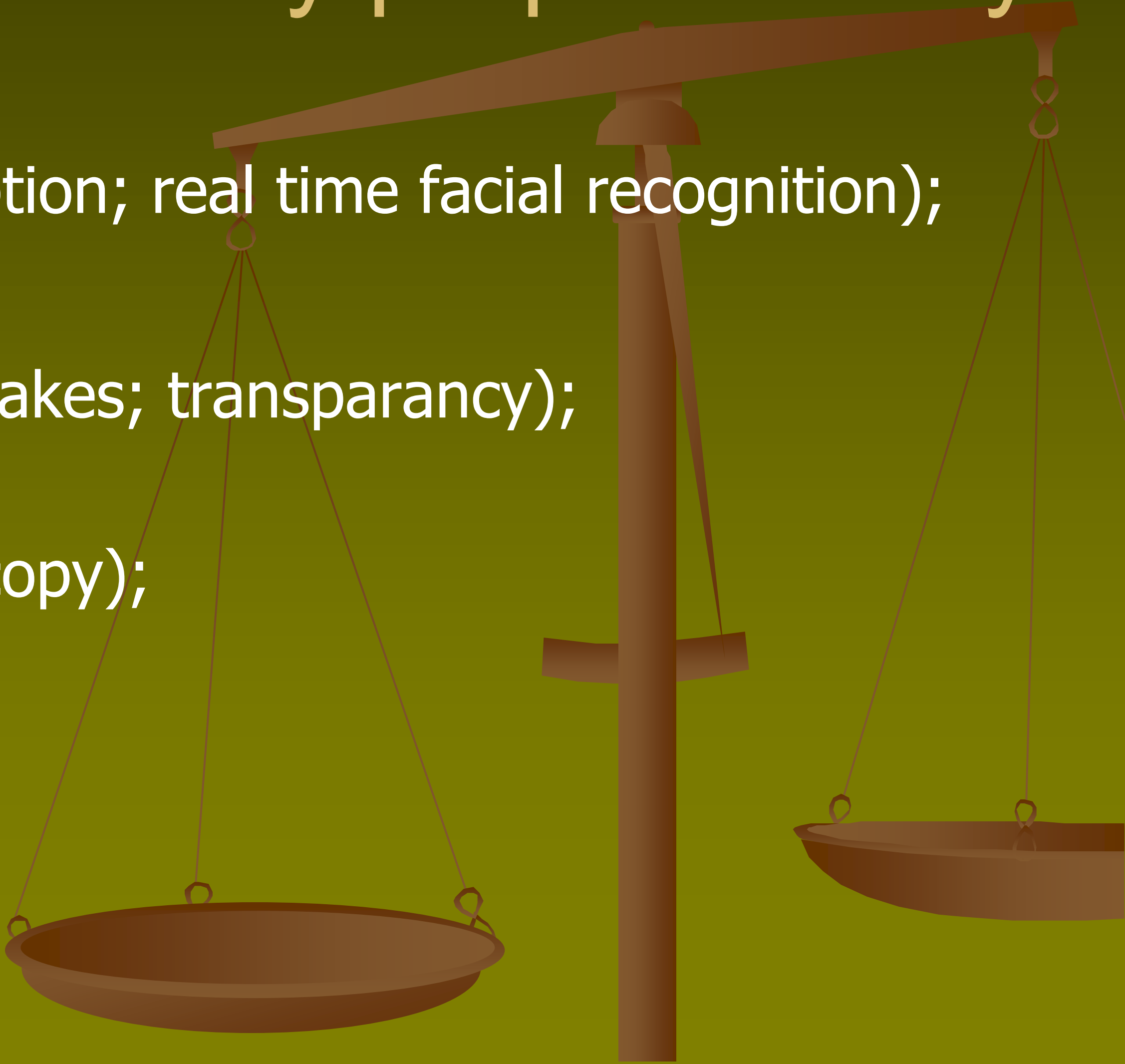
Production order.

Police/Public Prosecutor/Judge

Expedited preservation.

Police/Public Prosecutor.

E-evidence H.R. and necessity/proportionality



- Admissibility (encryption; real time facial recognition);
- Presentation (deep fakes; transparancy);
- Relevance (forensic copy);

Witness videoconferencing. Why?

Detainees and protected witnesses: security reasons; time/cost effective measure;

Sanitary reasons during Covid-19 pandemic;

More efficient (less costs; limits geographical or health impediments);

Transparent and repeatable evidence (for both lawyers and judges, appeal courts); reasoning and demeanour; change of panel judge;

Interaction with remote trials and AI tools.

Does it work?

- Setting up the courtroom with proper technical equipments.
- Witness failure to appear by videoconference.
- Witness identification.
- Instructions to the witness.
- Consequences of unclear guidelines:
- The case *Avsenew v. State of Florida* (6) SC18-1629 Peter Avsenew v. State of Florida - YouTube

Evaluating witnesses and AI

- Credibility (reliability; trustworthiness: truthful or untruthful?):

from polygraphs to AI tools: eyes and demeanour tracking; blood pressure measurement (transdermal optical imaging and the Pinocchio Effect); brain imaging; a-IAT (Autobiographical Implicit Association Test);

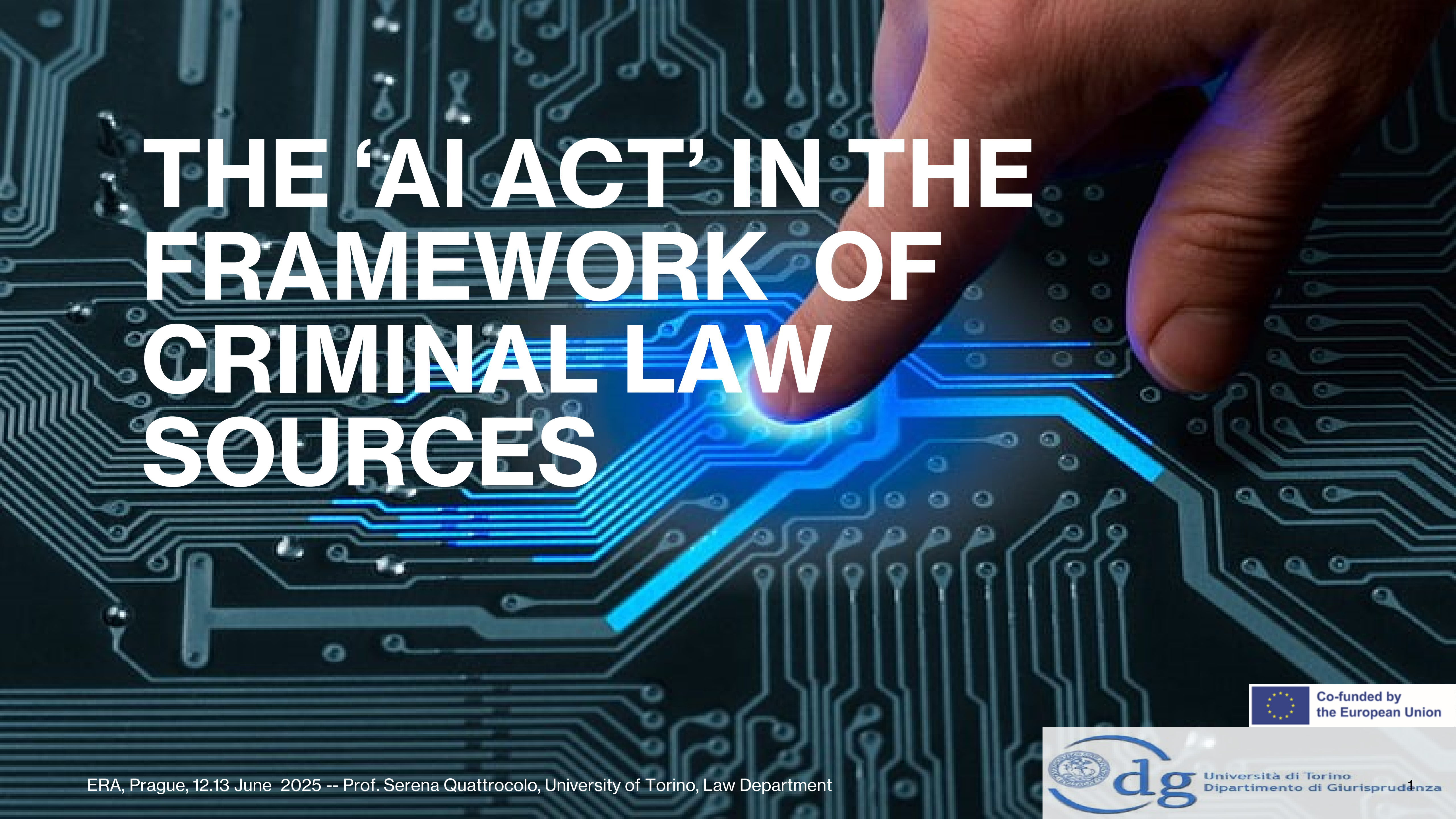
- Accuracy (right or wrong?); perception, memory, deposition;

Advokate; Immersive technology (virtual theater/simulation/reconstruction/metaverse and avatars); Text to image/video AI or image/video generator AI tools (ChatGPT, OPEN AI and Canva, Synthesia, Sora, Midjourney, Dall-e); from demeanour to consistency (algorithms checking witness declarations for gaps/incoherences/contradictions; Virtual practitioner);

Takeaways.

- **Pros:** Efficiency (time, costs, security, accuracy), neutrality, predictability and uniformity;
- **Cons:** AI algorithms transparancy and intellectual property; cyber attacks; data leaks; deep fakes; judicial overconfidence; standardization of the justice system;

A proactive role of judges (and lawyers) is needed to ensure balance between E-evidence/AI and HR/rule of law. . The irreplaceable role of judges in ensuring «under user control» and fairness of criminal proceedings (Cogito ergo sum, not digito ergo sum).



THE ‘AI ACT’ IN THE FRAMEWORK OF CRIMINAL LAW SOURCES

Co-funded by the European Union

Università di Torino
Dipartimento di Giurisprudenza

ERA, Prague, 12.13 June 2025 -- Prof. Serena Quattrocolo, University of Torino, Law Department

LEGAL BASIS

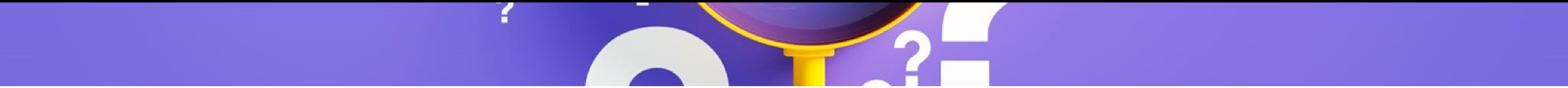
ART 114 TFEU: […] The European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.

Is the AI Act a binding source of criminal law?

…But recital no. 3

[…] To the extent that this Regulation contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for remote biometric identification for the purpose of law enforcement, of the use of AI systems for risk assessments of natural persons for the purpose of law enforcement and of the use of AI systems of biometric categorisation for the purpose of law enforcement, it is appropriate to base this Regulation, in so far as those specific rules are concerned, on Article 16 TFEU. In light of those specific rules and the recourse to Article 16 TFEU, it is appropriate to consult the European Data Protection Board.

Are there similar references also to art. 82 or 83 TFEU?



NOT AT ALL…
HAS THE EU A COMPETENCE TO SET HARMONISATION GOALS IN CRIMINAL MATTERS BEYOND ARTT. 82 AND 83 TFEU?

A NUMBER OF PROVISIONS ESTABLISH A PROHIBITION 'TO USE' SPECIFIC KINDS OF AI TOOLS (ART. 5)

The prohibition, *per se*, affects any possible use of it, encompassing also law enforcement applications. MSs are not free to regulate the use of such tools in different ways

Nevertheless, for each case of prohibition, there are several hypothesis of exception

PROHIBITIONS (?)

...AND EXCEPTIONS

Art. 5 h

The use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

7. (i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;
8. (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;
9. (iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years

The prohibition under art. 5 lett. h is not effective, as the exceptions outbalance the limitations

- SEARCH FOR SPECIFIC VICTIMS

- THREAT TO THE LIFE OR PHYSICAL SAFETY OF NATURAL PERSONS

- THREAT OF A TERRORIST ATTACK

- PERSON SUSPECTED OF HAVING COMMITTED A CRIMINAL – OFFENCE REFERRED TO IN ANNEX II AND PUNISHABLE IN THE MEMBER STATE CONCERNED BY A CUSTODIAL SENTENCE OR A DETENTION ORDER FOR A MAXIMUM PERIOD OF AT LEAST FOUR YEARS

Art. 5 d

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

Annex III § 6 (high risk but allowed AI)

(d) AI systems intended to be used by law enforcement authorities or on their behalf or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups

In annex III the term 'risk assessment' is not used explicitly!

Annex III § 6 (high risk but allowed AI)

(e) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of the detection, investigation or prosecution of criminal offences.

Comparing art. 5 and Annex III.6 d

THE FOLLOWING AI PRACTICES SHALL BE PROHIBITED:

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

HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)

AI systems intended to be used by law enforcement authorities or on their behalf or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups

⚠

Are there differences?

While in art. 5 ‘profiling’ and ‘assessment of personality traits’ appear to be ”methodologies” on which the risk assessment tool is based, in Annex III no. 6 lett. *d* (and *e*), they appear to be purposes of the action of ‘assessing the risk’ and ‘assessing personality’

DOES A RISK ASSESSMENT TOOL EXIST WHICH IS NOT BASED ON THE 'ASSESSMENT OF PERSONALITY TRAITS AND CHARACTERISTICS'?

Apparently, not in the common understanding of psycho-criminology experts…

Should we think that art. 5 lett. D has no real meaning?

Università di Torino
Dipartimento di Giurisprudenza

Any way-out?

1) PROHIBITION (ART. 5)/EXCEPTIONS (ANNEX III)

exceptions to general prohibitions must be subject to strict interpretation!

2) Recital 42 refers to the need for human judgment: could this mean that fully actuarial risk assessment tools should not be used for law enforcement purposes? The judge is, definitively, a human in the decision-making process, but s/he could be not able to provide what rec. 42 intends as ‘human assessment’, when recurring to actuarial tools. ‘Human’ may mean an expert in the risk assessment phase

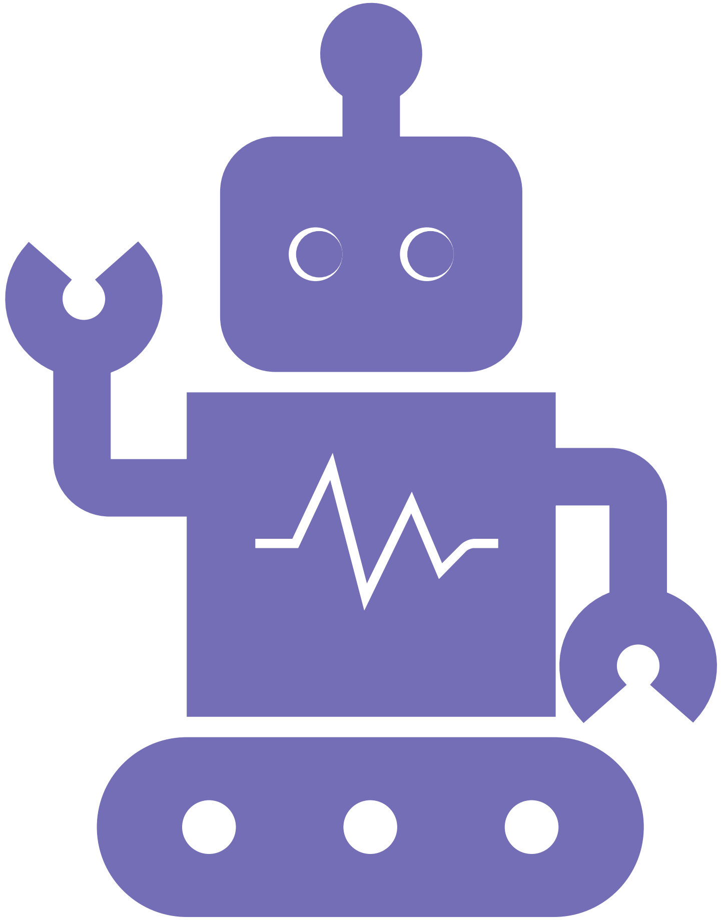
NON-PROHIBITED HIGH RISK AI

Annex III, section 6 and 8

Which binding level?

Art. 15

- 1. High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle.
- 2 [...]
- 3. The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.



High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

6. Law enforcement, in so far as their use is permitted under relevant Union or national law:

(a) AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf to assess the risk of a natural person becoming the victim of criminal offences;

(b) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities as polygraphs or similar tools;

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

(d) AI systems intended to be used by law enforcement authorities or on their behalf or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups;

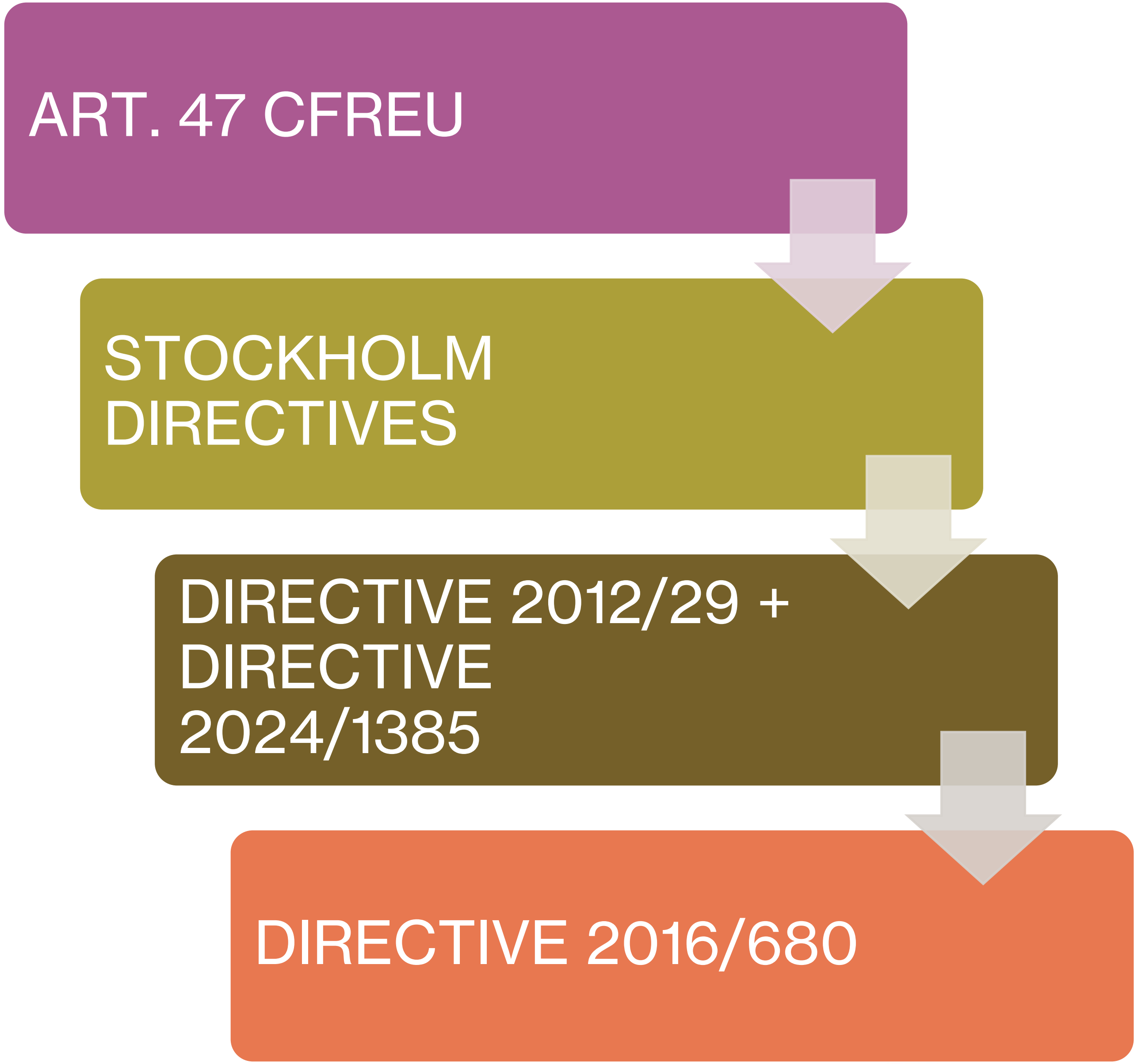
(e) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of the detection, investigation or prosecution of criminal offences.

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

6. Administration of justice and democratic processes:

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

We must consider this provisions against the general legal backdrop



ART. 47 CFREU

STOCKHOLM DIRECTIVES

DIRECTIVE 2012/29 + DIRECTIVE 2024/1385

DIRECTIVE 2016/680

IMPACT OF AI ACT

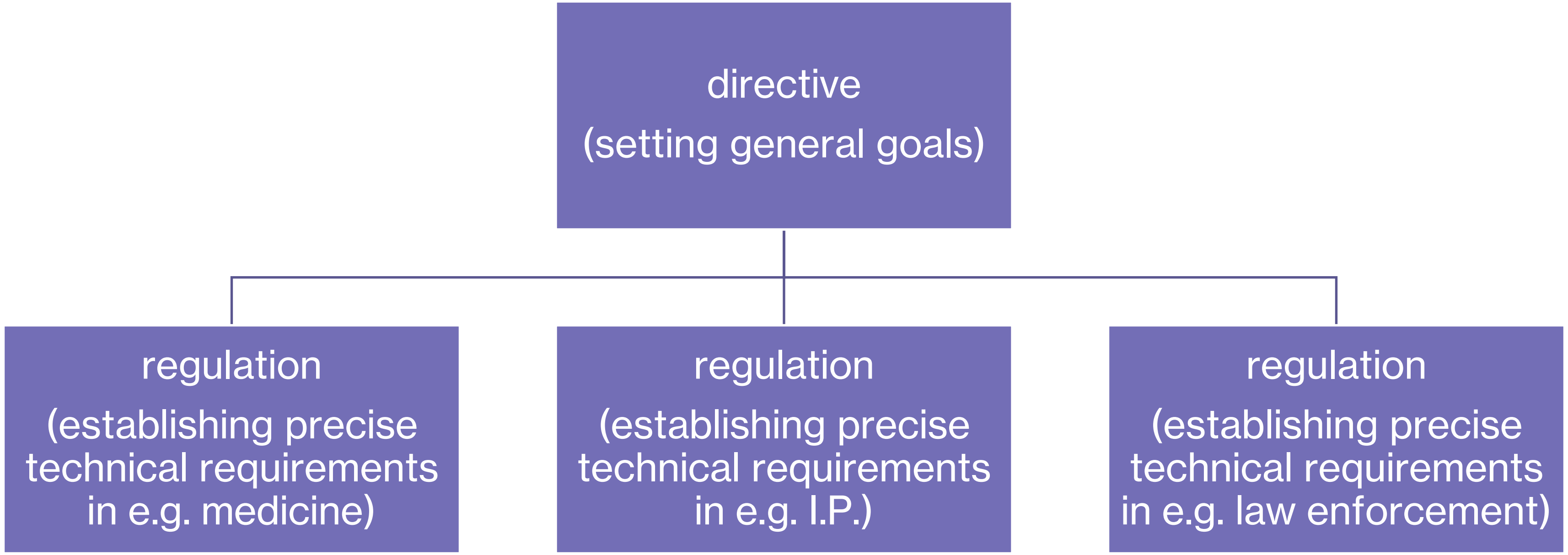
GOLDEN RULE?

LANDSCAPE PHOTOGRAPHY?

Does the AI act provide trustworthy AI for law enforcement purposes?

- For high risk AI, the regulation sets forth a compliance system which does not seem to be based on the specificity of each area of expertise

Because of this, in my opinion a better approach would have been:



directive

(setting general goals)

regulation

(establishing precise technical requirements in e.g. medicine)

regulation

(establishing precise technical requirements in e.g. I.P.)

regulation

(establishing precise technical requirements in e.g. law enforcement)

more

risks? or benefits?

risks?

- Developers are confused by the regulation
- The regulation is overlooked

benefits?

- Triggering sensitivity for new issues
- Pushing MSs to be proactive

THANK YOU FOR YOUR ATTENTION