



POST-COVID CHALLENGES IN CRIMINAL JUSTICE: INVESTIGATING WEB 2.0

CRIMINALS' NEW MODI OPERANDI, E-EVIDENCE,
INVESTIGATIONS IN THE DARKWEB

Tallinn, 20-21 June 2024



EXCELLENCE IN
EUROPEAN LAW¹

Speakers and chairs

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

Muthupandi Ganesan, Barrister at Law & Partner, Aliant Law, London

Patricia Hamel, Judge, Higher Regional Court, Munich

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

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

Taavi Pern, Chief State Prosecutor, Tallinn

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

Bilal Sen, Senior Investigator, Coninsec, Cologne

Remco Sprooten, Senior Security Consultant, Team Leader, Security Operation Center, ENGIE NL, Amsterdam

Nina Sunde, Police Superintendent, PhD in Criminology, Department of Criminology and Sociology of Law, University of Oslo,

Victor Voelzow, Trainer for Digital Forensics, Hesse State Policy Academy

Key topics

- Understanding the internet and associated technology
- Open-source tools (OST)
- Handling e-evidence in court
- Investigating the dark web

Language
English

Event number
324DT08

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



POST-COVID CHALLENGES IN CRIMINAL JUSTICE

Thursday, 20 June 2024

08:30 Arrival and registration of participants

09:00 **Welcome and introduction to the programme**
Taavi Pern & Laviero Buono

PART I: TECHNICAL ISSUES AND BASIC UNDERSTANDING OF THE INTERNET, CRYPTO AND OSINT

Chair: Laviero Buono

09:15 **Fighting 2.0 crimes with Web 3.0 possibilities**

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

Lilija Mažeikiene

10:15 Discussion

10:30 Break

11:00 **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

Bilal Sen

12:00 Discussion

12:15 Lunch

PART II: DIGITAL FORENSICS AND EXAMINATION OF E-EVIDENCE

Chair: Bilal Sen

13:30 **Technical and human errors (and their sources) related to the collection and presentation of electronic evidence**

- Is digital evidence objective, value-neutral and reliable?
- Bias and noise in digital forensic examinations
- Evidence dynamics and evidence elasticity
- Transparency and auditability of digital forensic investigation practices

Nina Sunde

14:00 Discussion

14:15 **Examination of digital devices, such as computers, mobile phones, media storage (USB, memory cards, etc.)**

- File systems (NTFS, macOS, Linux)
- Windows and MacOS artefacts
- Chain on custody & digital evidence handling

Anna Illamaa

14:45 Discussion

15:00 Break

15:30 **Handling e-evidence from a technical point of view**

- First Responder's E-Learning
- Value of Live Data Forensics
- Value of Memory Forensics
- Encryption as a Challenge

Victor Voelzow

Objective

Covid-19 resulted in altering the *modi operandi* of criminals. Offences related to cybercrime and online criminal activities increased significantly. The trade of illicit goods and services has moved to the Darknet even more; the number of phishing attempts, cases of online fraud, investment fraud, cyberattacks in the health sector and trade in counterfeit medical products has increased. As children spend more time online, the number of child sexual exploitation cases has also risen sharply in Europe. Isolation has made people more vulnerable to internet-related crimes.

This series of events addresses various challenges 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 will remain in the “new normal” well beyond the end of the pandemic.

This seminar will focus on online investigations.

About the Project

This seminar is part of a large-scale project sponsored by the European Commission entitled “Preparing criminal justice professionals to address new (post-) pandemic challenges as a result of criminals’ new *modi operandi*”. It consists of seven seminars to take place in Bucharest, Dublin, Lisbon, Cracow, Barcelona, Thessaloniki and Tallinn over the period 2022-2024.

Who should attend?

Judges, prosecutors and lawyers in private practice from eligible EU Member States.

Venue

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

CPD

ERA’s programmes meet the standard requirements for recognition as Continuing Professional Development (CPD). Participation in the full programme of this event corresponds to **8 CPD hours**.

A certificate of participation for CPD purposes with indication of the number of training hours completed will be issued on request. CPD certificates must be requested at the latest 14 days after the event.

- 16:00 Discussion
16:15 End of first day
19:00 Dinner offered by the organisers

Friday, 21 June 2024

PART III: E-EVIDENCE AND CROSS-BORDER ACCESS TO DATA

Chair: Victor Voelzow

- 09:30 **New EU rules to improve cross-border access to electronic evidence: what has been done so far and where we currently stand**
Patricia Hamel

10:15 Discussion

- 10:30 **Case study: Collecting e-evidence in modern enterprise environments**
An employee of an enterprise organisation is the suspect in a fraud case. The company is willing to co-operate, but how to proceed?
Remco Sprooten

11:00 Discussion

11:15 Break

Chair: Patricia Hamel

- 11:45 **E-evidence, digital devices, pins & passwords – Mandatory disclosure: fair or unfair?**
Muthupandi Ganesan

12:15 Discussion

- 12:30 **Practical experiences with videoconferencing when hearing experts and witnesses**
Balázs Rozsnyai

13:00 End of seminar

13:10 Light lunch

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

Your contact persons



Laviero Buono
Head of Section
E-Mail: LBuono@era.int



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

Save the date

Social Network Investigations From “Likes” to Evidence
Online, 12-13 March 2024

Annual Conference on White-Collar Crime in the EU 2024
Trier & Online, 21-22 March 2024

Cracking Down on Digital Predators Investigating and Prosecuting Online Child Sexual Abuse and Sexual Violence
Online, 16-17 April 2024

Artificial Intelligence (AI) in Criminal Justice – From Predictive Policing to Sentencing: AI in the Courtroom
Dublin & Online, 13-14 June 2024

Apply online for “(Post)Covid Challenges in Criminal Justice”:
www.era.int/?132561&en



Co-funded 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

Post-Covid Challenges in Criminal Justice: Investigating Web 2.0

Tallinn, 20-21 June 2024 / Event number: 324DT08/JR



Terms and conditions of participation

Selection

1. Participation is only open to judges, prosecutors and lawyers in private practice from eligible EU Member States.

The number of places available is limited (30 places). Participation will be subject to a selection procedure. Selection will be according to professional eligibility, nationality and then "first come, first served". Spanish applicants who work for the prosecution service must apply for this event through CEJ.

2. Applications should be submitted before **28 February 2024**.
3. A response will be sent to every applicant after this deadline. **We advise you not to book any travel or hotel before you receive our confirmation.**

Registration Fee

4. €130 including documentation, lunches and dinner.

Travel and Accommodation Expenses

5. Participants will receive a fixed contribution towards their travel and accommodation expenses and are asked to book their own travel and accommodation. The condition for payment of this contribution is to sign all attendance sheets at the event. No supporting documents are needed. The amount of the contribution will be determined by the EU unit cost calculation guidelines, which are based on the distance from the participant's place of work to the seminar location and will not take account of the participant's actual travel and accommodation costs.
6. Travel costs from outside Estonia: participants can calculate the contribution to which they will be entitled on the European Commission website (<https://era-comm.eu/go/calculator>). The distance should be calculated from their place of work to the seminar location.
7. For those travelling within Estonia, the contribution for travel is fixed at €16 (for a distance between 50km and 400km). Please note that no contribution will be paid for travel under 50km. For more information, please consult p.10 on <https://era-comm.eu/go/unit-cost-decision-travel>
8. Accommodation costs: international participants and national participants travelling more than 50km one-way will receive a fixed contribution of €107 per night for up to two nights' accommodation. For more information, please consult p.13 on <https://era-comm.eu/go/unit-cost-decision-travel>
9. These rules do not apply to representatives of EU Institutions and Agencies who are required to cover their own travel and accommodation.
10. Successful applicants will be sent the relevant claim form and information on how to obtain payment of the contribution to their expenses. Please note that no payment is possible if the registered participant cancels their participation for any reason.

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, publications and/or other developments in the participant's area of interest.
14. A certificate of attendance will be distributed at the end of the conference.

Apply online for "Post-Covid Challenges in Criminal Justice":
www.era.int/?132561&en

Venue

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

Language

English

Contact Person

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

TABLE OF CONTENTS



With the support of the Justice Programme of
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 *****

Work carried out by the European Union on e-evidence

1	Council Decision (EU) 2023/436 of 14 February 2023 authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (ST/6438/2022/INIT, OJ L 63, 28.2.2023)	
2	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 (PE/4/2023/REV/1, OJ L 191, 28.7.2023, p. 118–180)	
3	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 (PE/3/2023/REV/1, OJ L 191, 28.7.2023, p. 181–190)	

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 (<i>OJ L 149</i> , 30.4.2021)
A4-02	Eurojust: Judicial cooperation in criminal matters between the European Union and the United Kingdom from 1 January 2021, 1 January 2021
A4-03	Draft text of the Agreement on the New Partnership between the European Union and the United Kingdom (UKTF 2020-14), 18 March 2020
A4-04	Draft Working Text for an Agreement on Law enforcement and Judicial Cooperation in Criminal Matters
A4-05	The Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 (2019/742), 28th March 2019
A4-06	Brexit next steps: The European Arrest Warrant, House of Commons, 20 February 2020
A4-07	Brexit next steps: The Court of Justice of the EU and the UK, House of Commons, 7 February 2020
A4-08	The Law Society, "Brexit no deal: Criminal Justice Cooperation", London, September 2019
A4-09	European Commission, Factsheet, „A „No-deal“-Brexit: Police and judicial cooperation”, April 2019
A4-10	CEPS: Criminal Justice and Police Cooperation between the EU and the UK after Brexit: Towards a principled and trust-based partnership, 29 August 2018
A4-11	Policy paper: The future relationship between the United Kingdom and the European Union, 12 July 2018
A4-12	House of Lords, Library Briefing, Proposed UK-EU Security Treaty, London, 23 May 2018
A4-13	HM Government, Technical Note: Security, Law Enforcement and Criminal Justice, May 2018
A4-14	LSE-Blog, Why Britain’s habit of cherry-picking criminal justice policy cannot survive Brexit, Auke Williams, London School of Economics and Political Science, 29 March 2018
A4-15	House of Commons, Home Affairs Committee, UK-EU Security Cooperation after Brexit, Fourth Report of Session 2017-19, London, 21 March 2018
A4-16	HM Government, Security, Law Enforcement and Criminal Justice, A future partnership paper
A4-17	European Criminal Law after Brexit, Queen Mary University London, Valsamis Mitsilegas, 2017
A4-18	House of Lords, European Union Committee, Brexit: Judicial oversight of the European Arrest Warrant, 6 th Report of Session 2017-19, London, 27 July 2017

A4-19	House of Commons, Brexit: implications for policing and criminal justice cooperation (24 February 2017)
A4-20	Scottish Parliament Information Centre, Briefing, Brexit: Impact on the Justice System in Scotland, Edinburgh, 27 October 2016

B) Mutual legal assistance

B1) Legal framework

B1-01	Council Act of 16 October 2001 establishing in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2001/C 326/01), (OJ C 326/01; 21.11.2001, P. 1)
B1-02	Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 197/1; 12.7.2000, P. 1)
B1-03	Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the surrender procedure between the Member States of the European Union and Iceland and Norway (OJ L 292, 21.10.2006, p. 2–19)
B1-04	Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 8.XI.2001)
B1-05	Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 17.III.1978)
B1-06	European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 20.IV.1959)
B1-07	Third Additional Protocol to the European Convention on Extradition (Strasbourg, 10.XI.2010)
B1-08	Second Additional Protocol to the European Convention on Extradition (Strasbourg, 17.III.1978)
B1-09	Additional Protocol to the European Convention on Extradition (Strasbourg, 15.X.1975)
B1-10	European Convention on Extradition (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	InAbsentiaEAW, Background Report on the European Arrest Warrant - The Republic of Poland, Magdalena Jacyna, 01 July 2018
B2-32	Case C-571/17 PPU, Samet Ardic, Judgment of the court of 22 December 2017

B2-33	C-270/17 PPU, Tupikas, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-34	Case C-271/17 PPU, Zdiaszek, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-35	Case C-579/15, Popławski, Judgement of the Court (Fifth Chamber), 29 June 2017
B2-36	Case C-640/15, Vilkas, Judgement of the Court (Third Chamber), 25 January 2017
B2-37	Case C-477/16 PPU, Kovalkovas, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-38	Case C-452/16 PPU, Poltorak, Judgement of the Court (Fourth chamber), 10 November 2016
B2-39	Case C-453/16 PPU, Özçelik, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-40	Case C-294/16 PPU, JZ v Śródmieście, Judgement of the Court (Fourth Chamber), 28 July 2016
B2-41	Case 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 <i>Jeremy F / Premier ministre</i> , Judgement of the court (Second Chamber), 30 May 2013
B2-46	Case C-399/11 <i>Stefano Melloni v Ministerio Fiscal</i> , Judgment of of 26 February 2013
B2-47	Case C-396/11 Ciprian Vasile Radu, Judgment of 29 January 2013
B2-48	C-261/09 Mantello, Judgement of 16 November 2010
B2-49	C-123/08 Wolzenburg, Judgement of 6 October 2009
B2-50	C-388/08 Leymann and Pustovarov, Judgement of 1 December 2008
B2-51	C-296/08 Goicoechea, Judgement of 12 August 2008
B2-52	C-66/08 Szymon Kozłowski, Judgement of 17 July 2008

B3) Mutual recognition: freezing and confiscation and asset recovery

B3-01	European Judicial Network (for information on mutual recognition of freezing and confiscation orders, including on competent authorities), 14 December 2020, last reviewed on 24 July 2023
B3-02	Moneyval 64th Plenary Meeting report, Strasbourg, 5 January 2023
B3-03	Proposal for a Directive of the European Parliament and of the Council on asset recovery and confiscation (<i>Brussels, 25.5.2022, COM (2022) 245 final</i>)
B3-04	Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010, (<i>Brussels, 20.7.2021 COM(2021) 421 final</i>)
B3-05	FATF, COVID-19-related Money Laundering and Terrorist Financing Risk and Policy Responses, Paris, 4 May 2020
B3-06	Money-Laundering and COVID-19: Profit and Loss, Vienna, 14 April 2020

B3-07	FATF President Statement – COVID-19 and measures to combat illicit financing, Paris 1 April 2020
B3-08	Moneyval Plenary Meeting report, Strasbourg, 31 January 2020
B3-09	Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019, laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA
B3-10	Commission Delegated Regulation (EU) .../... of 13.2.2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, C(2019) 1326 final
B3-11	Regulation 2018/1805 of the European Parliament and of the Council on the mutual recognition of freezing and confiscation orders, L 303/1, Brussels, 14 November 2018
B3-12	Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, L 284/22
B3-13	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), PE/72/2017/REV/1 OJ L 156, p. 43–74, 19 June 2018
B3-14	Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
B3-15	Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies (Text with EEA relevance)
B3-16	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance)
B3-17	Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Text with EEA relevance)
B3-18	Consolidated text: Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union
B3-19	Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community
B3-20	Council Framework Decision of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (2001/500/JHA)
B3-21	Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA)

B4) Mutual recognition: Convictions

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

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

B5-01	Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, (<i>OJ L 191, 28.7.2023</i>)
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, (<i>OJ L 191, 28.7.2023</i>)
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, (<i>Brussels, 20.7.2021, COM(2021) 409 final</i>)
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, <i>(COM (2020) 605 final)</i>
D1-11	Council Conclusions on EU External Action on Preventing and Countering Terrorism and Violent Extremism, Brussels, 16 June 2020
D1-12	Terrorism Situation and Trend Report (TE-SAT) 2019
D1-13	Communication from the Commission to the European Parliament, the European Council and the Council, Twentieth Progress Report towards an effective and genuine Security Union, COM(2019) 552 final, Brussels, 30 October 2019
D1-14	Communication from the Commission to the European Parliament, and the Council, Towards better Implementation of the EU's anti-money laundering and countering the financing of terrorism framework, COM(2019) 360 final, Brussels, 24 July 2019
D1-15	Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, L 123/18
D1-16	Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 amending Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries, L 125/4 (Text with EEA relevance)
D1-17	Council Decision (CFSP) 2019/25 of 08 January 2019 updating the list of persons, groups and entities subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism and repealing Decision (CFSP) 2016/1136, Brussels, 08 January 2019
D1-18	Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, 12.9.2018, <i>(COM(2018) 640 final)</i>
D1-19	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), <i>(OJ L 156, 19.6.2018)</i>
D1-20	Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327/20; 9.12.2017)
D1-21	Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88/6)
D1-22	Council Decision (CFSP) 2016/1693 of 20 September 2016 concerning restrictive measures against ISIL (Da'esh) and Al-Qaeda and persons, groups, undertakings and entities associated with them and repealing Common Position 2002/402/CFSP, <i>(OJ L 255, 21.9.2016)</i>

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

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

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

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

D3) Cybercrime

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

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

D4) Protecting Victims' Rights

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

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

E) Criminal justice bodies and networks

E1) European Judicial Network

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

E2) Eurojust

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

E3) Europol

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

E4) European Public Prosecutor's Office

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

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

F) Data Protection

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

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

G) Police Cooperation in the EU

G1) General

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

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

G2) Joint Investigation Teams (JITs)

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

Fighting 2.0 crimes with 3.0 possibilities

Lilija Mažeikienė
Investigations Team, EMEA
lilija@binance.com

What to expect?



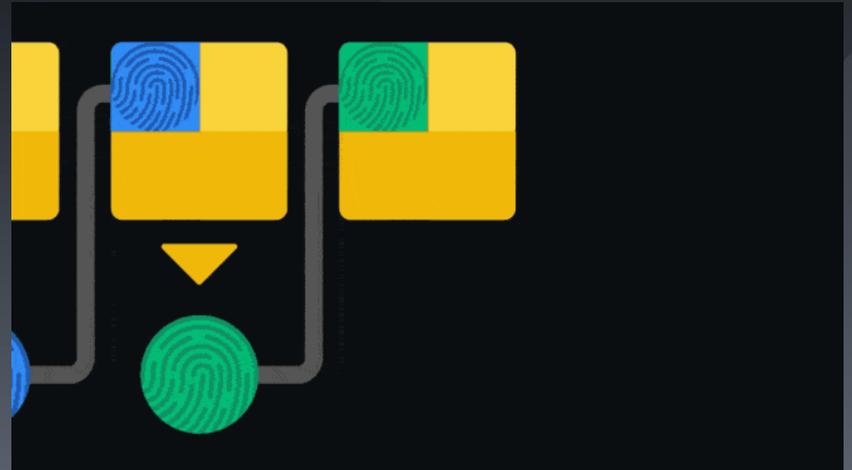
- 1 Crypto 101: technology, definitions, blockchain explorers**
- 2 (Ab)use of crypto**
- 3 Crypto services: internal controls, cooperation**

Crypto 101

Crypto 101: Blockchain Technology



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



Crypto 101: Blockchain Technology



Key elements:

- Cryptography
- Immutable Ledger
- Peer-to-Peer Network
- Consensus Protocol
- Block Validation (Mining)

Crypto 101: Blockchain vs. Cryptocurrency



Blockchain ≠ Cryptocurrency

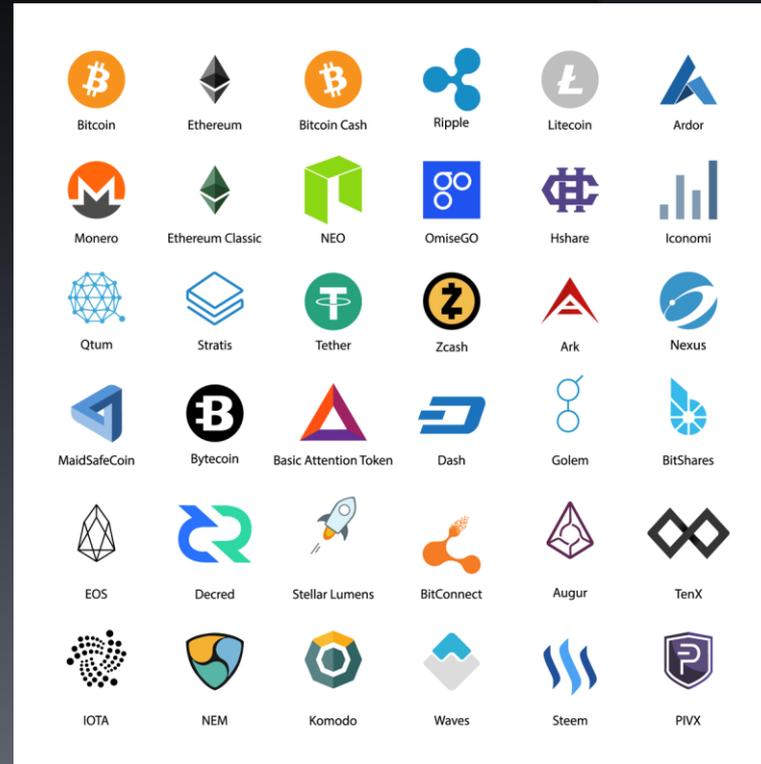
Transactions on a blockchain are usually economic, but any kind of information can be stored and verified in blocks.

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

Crypto 101: Cryptocurrency



Blockchain ≠ Cryptocurrency



Crypto 101: Definitions



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

Examples:

cca7507897abc89628f450e8b1e0c6fca4ec3f7b34cccf55f3f531c659ff4
d79

952a44587cfc5b4131570215bb85ce4af160863656c2fc6d1f71e8052d
053369

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

Examples:

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

public key

###

A public key is something like your bank account number, it is your wallet's address, to receive the crypto.



private key

###

The private key can be compared to your bank account **password** or the **PIN** to your debit card, it is **confidential**.

0X311729

61954613

Crypto 101: Definitions



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



Desktop wallets



Mobile wallets



Cold wallets/
Hot wallets



Online web wallets



Paper wallets

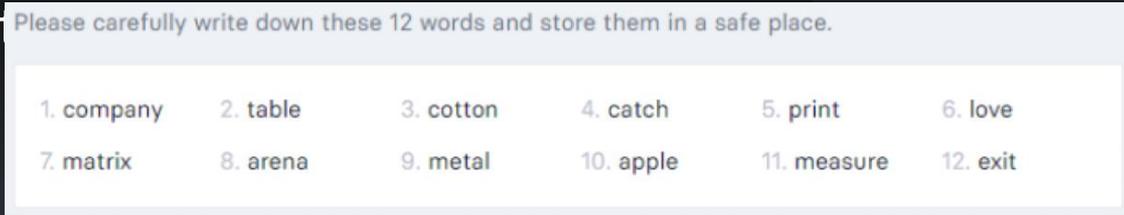


Hardware wallets

Crypto 101: Definitions



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



Blockchain Explorers

Blockchain Explorers: understanding the ledger



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

Blockchain Explorers: understanding the ledger



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

Blockchain Explorers: many possibilities



Google 🔍

Web Images Videos News Shopping More Search tools

About 4,810,000 results (0.35 seconds)

Blockchain.info: Bitcoin Block Explorer
<https://blockchain.info/>
Bitcoin Block Explorer & Currency Statistics. View detailed information on all bitcoin transactions and blocks.
[Wallet](#) - [Bitcoin Charts](#) - [Markets](#) - [Stats](#)
You've visited this page 4 times. Last visit: 5/17/15

Bitcoin Block Explorer: Home
<https://blockexplorer.com/>
Bitcoin Block Explorer is a web tool that provides detailed information about Bitcoin blocks, addresses, and transactions.
You've visited this page 2 times. Last visit: 3/27/15

Litecoin Explorer - Litecoin Cryptocurrency Blockchain ...
<https://block-explorer.com/>
Litecoin Block Explorer. ... GENERATED ON: 2015-06-07 07:58:47 UTC. Litecoin.
Search: You can search for block id, block hash, transaction hash, address.
You visited this page on 6/7/15.

Dash Explorer - Chainz
<https://chainz.cryptoid.info/dash/>
Dash Block Explorer and Statistics. Access detailed information on Dash (dash) transactions, blocks and addresses.

Biteasy.com: Bitcoin Block Explorer | Wallet | Merchant ...
<https://www.biteasy.com/>
Biteasy.com provides a powerful innovative bitcoin block explorer, a bitcoin wallet service and bitcoin merchant services for merchants.
You visited this page on 6/7/15.

BLOCKTRAIL | Bitcoin API and Block Explorer
<https://www.blocktrail.com/>
BlockTrail provides a secure bitcoin platform and API for developers and enterprises, enabling advanced transaction functionality and access to refined ...

Blockchain Explorers: many possibilities



WalletExplorer.com


ShapeShift

 **ARKHAM**

 **Blockchain.com**

 **Etherscan**

 **TRONSCAN**

 **BscScan**
A product of Etherscan

 **BLOCKCHAIR**

 **breadcrumbs**

Blockchain Explorers: what do they show?



ID: b8ba-c958 12/18/2017, 19:35:25	From 36rN-4KrA To 2 Outputs	-3.55972138 BTC • -\$229,199 Fee 102.5K Sats • \$66.02
From 1 36rNbEV2yvHwXZzb61sYJ6pPcdqsQY4KrA 3.55972138 BTC • \$229,199	To 1 3LUi3WA6sJgXxGooz1XdZUIJVkP2tZEvsL 3.54916313 BTC • \$228,519 2 1DSqeQSNhDWJCoo2CKsGhCMeauccS42x6 0.00953291 BTC • \$613.80	
ID: 1d58-70ce 12/18/2017, 18:25:35	From 32BW-LSHP To 2 Outputs	3.55972138 BTC • \$229,199 Fee 103.0K Sats • \$66.35
From 1 32BWCWKYCLhXsX3Fbs7bunkPwjVkybLSHP 3.63385883 BTC • \$233,973	To 1 17yJGb4oYv9MIUXEteqd1kNrHAWXuqqgTZ 0.07310700 BTC • \$4,707.14 2 36rNbEV2yvHwXZzb61sYJ6pPcdqsQY4KrA 3.55972138 BTC • \$229,199	



breadcrumbs BTC Enter any Bitcoin address or entity Our Tools

Untitled Report Bitcoin data updated a day ago

MiddleEarthMarketplace x Binance x

Filters

Date:
From: Not set
To: Not set
Set Filters

Product Tour



(Ab)use of Crypto

(Ab)use of Crypto



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

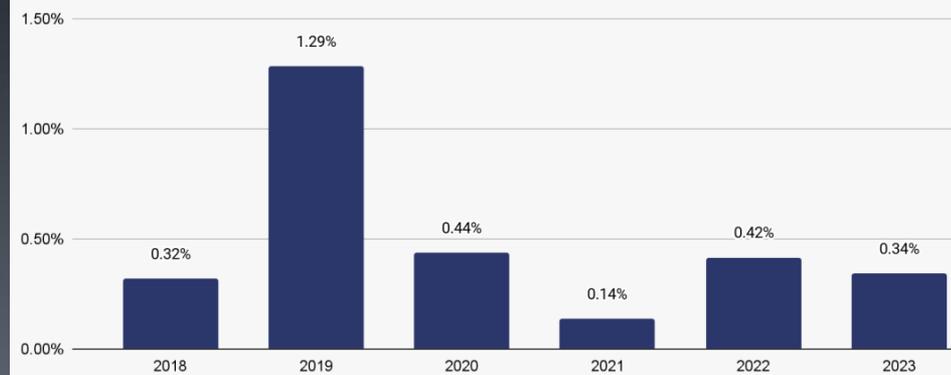
- Crypto market cap in 2023 - \$1.68T
- Value received by illicit addresses - \$24.2B
- Illicit share of all crypto volume - 0.34% (compared to estimated 2-5% of World's GDP)

Total cryptocurrency value received by illicit addresses
2018 - 2023



Chainalysis Crypto Crime Report 2023

Illicit share of all cryptocurrency transaction volume
2018 - 2023



(Ab)use of Crypto



1 Money Laundering

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

2 Scams

- Emerging variety of *modi operandi*
- Business-like criminal operation models, call centers

3 Hacks / Stolen Funds

- API hacks
- Crypto bridge hacks

4 Terror-Financing

- Three-way convergence: hawala networks, crypto, traditional finance
- Increasing use of TRX chain and USDT
- Early technology adopters

5 CSAM

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

6 Ransomware

- Attacking bigger targets to collect larger amounts
- Increase of \$1M payments

Scam Investigations

Investigating Scam

Modus Operandi - Investment Scam



Usual process:

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



jazynthea dangcil @jazynthea · Aug 13

Replying to @Rajjat52625177 and @cz_binance

Yes Best_recovery19 on Instagram will help you recover your account, he is the best and amazing



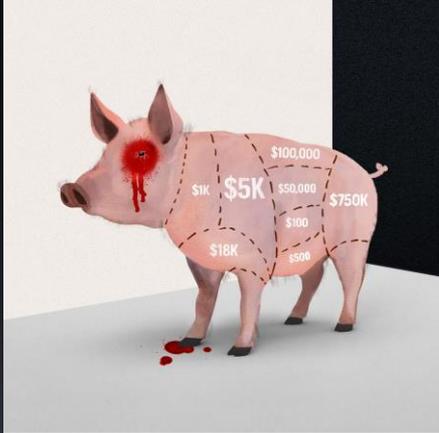
Tyler Madison @TylerMaddy · 21h

Replying to @Rajjat52625177

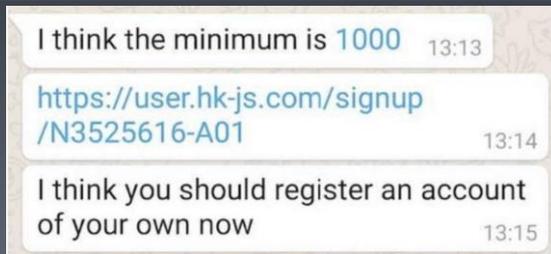
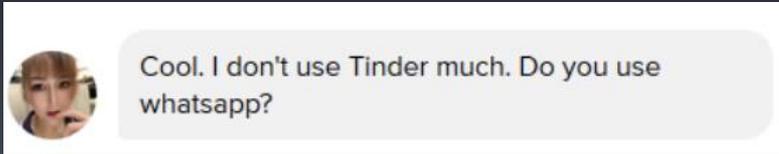
if you have proof,I'll suggest you quickly Reach out to the European_cyber on instagram,I'm pretty sure he must be of help to you,he helped me recover my funds when I had such issue [instagram.com/european_cyber](https://www.instagram.com/european_cyber)

Investigating Scam

Modus Operandi - Pig-Butchering

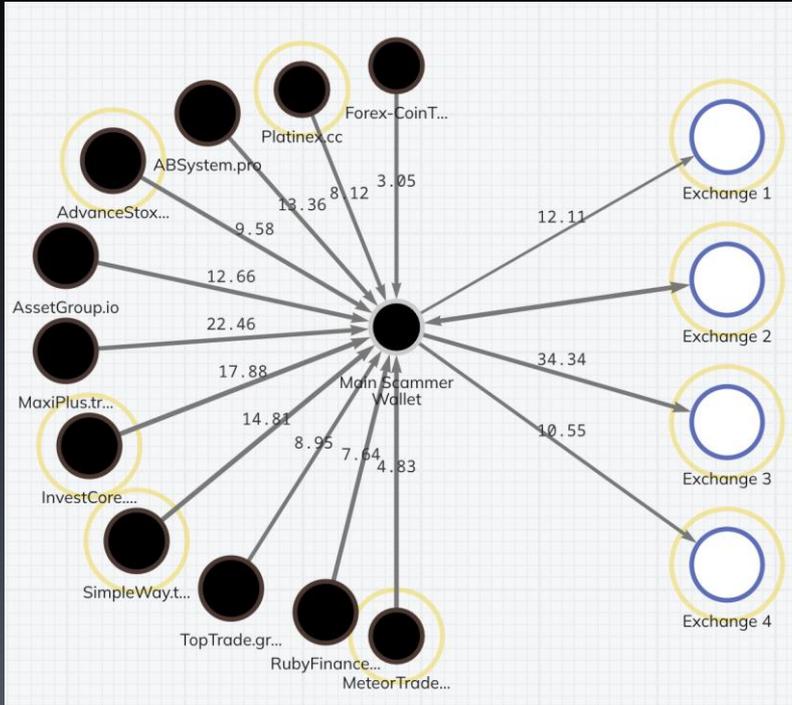


- Finding the victim (social media)
- Building trust
- Convincing to trade crypto
- Fattening "the pig"
- Failure to withdraw funds



Investigating Scam

One Criminal Group = Multiple Scam Sites?



The domain name
forex-cointrade.com
is for sale!

DS
Listed by
Domain seller

Get this domain

Pay the full USD \$688 now, or select
Lease to Own

Buy now **USD \$688**

Lease to own **USD \$115**
/month

assetgroup.io
is available for sale!

assetgroup.io \$280.00
Privacy Protection Included

Order Total \$280.00

Buy Now

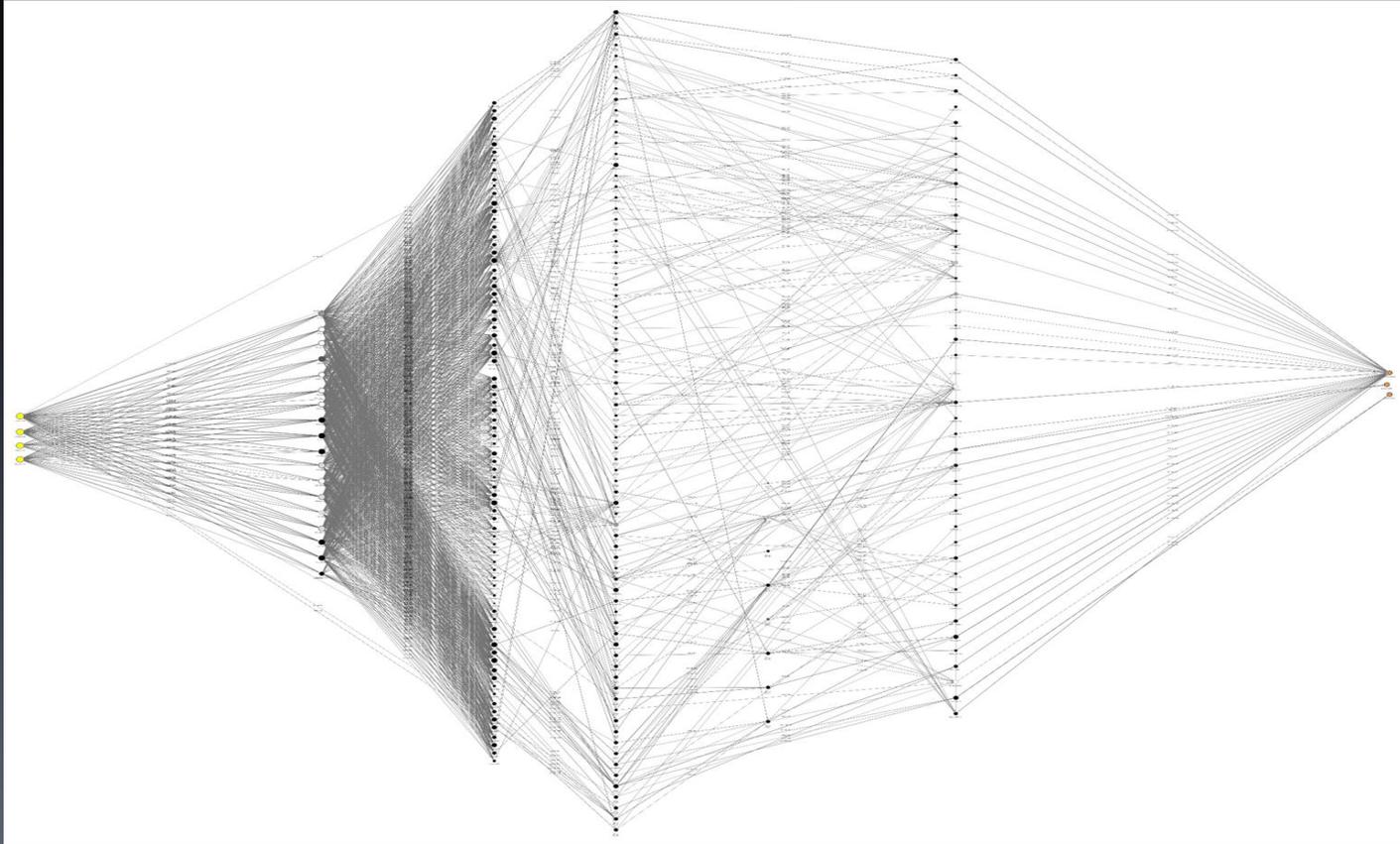
Investigating Scam

Tip of the Iceberg



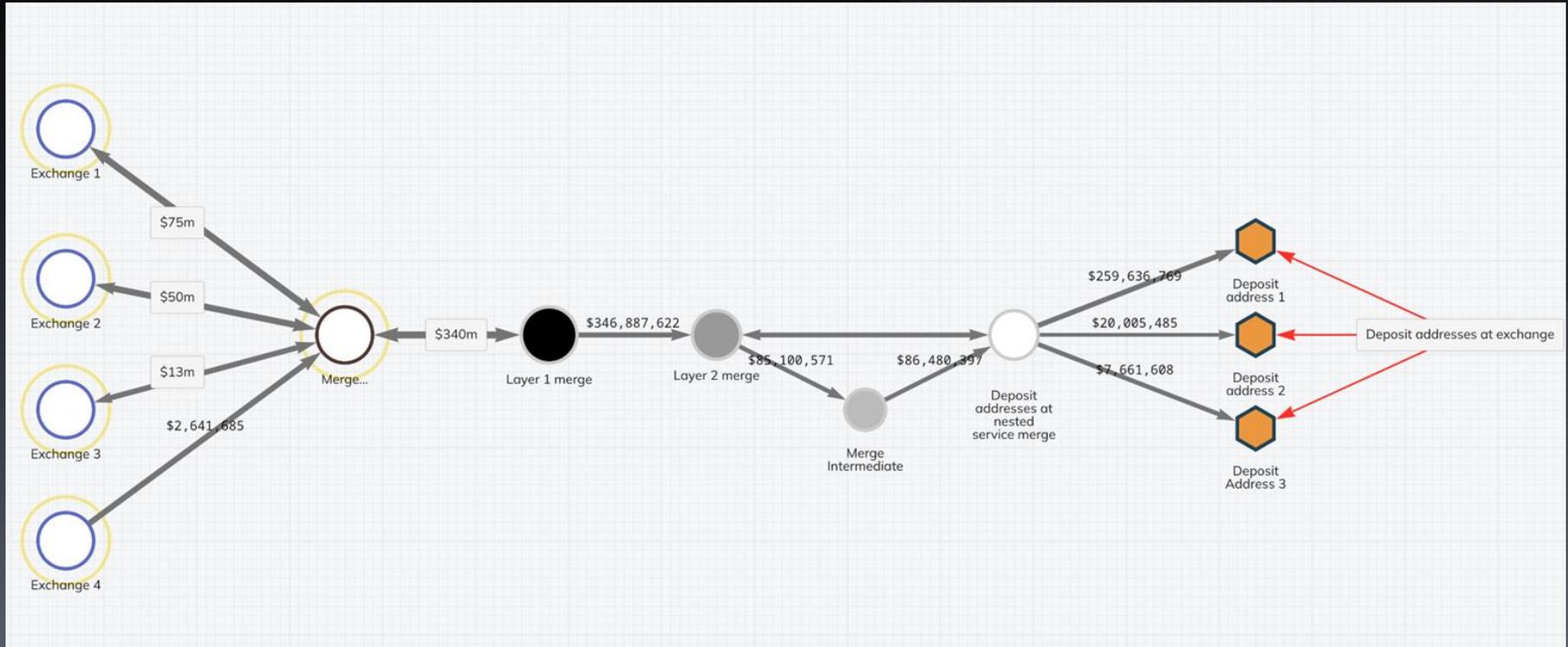
Investigating Scam

Flow of Funds



Investigating Scam

Flow of Funds (cleaned-up)



Investigating Scam

Identification



- **Behavioral Analysis**
 - How do scam networks operate?
 - Attack vectors, modi operandi.
 - Developing tactics and techniques to stop the criminals.
 - **Predictive Modelling**
 - Scams with similar MO's
 - What addresses will be generated next?
 - **Proactive Engagement with Public and Private Sector: Intelligence Sharing**
 - **Awareness and Education**
-
- **Tracing funds**
 - Follow the money (lifo), or trace the source of funds (via gas fees):
network analysis
 - **Investigations at account level**
 - Linked accounts
 - Investigating User's Behavior at exchange
 - **Prevention Measures**
 - Warning Questionnaires & Pop-ups
 - Cool-down periods
 - Withdrawal blacklists

Challenges

Third-party Tracing / Recovery Companies



crypto recovery companies



All



News

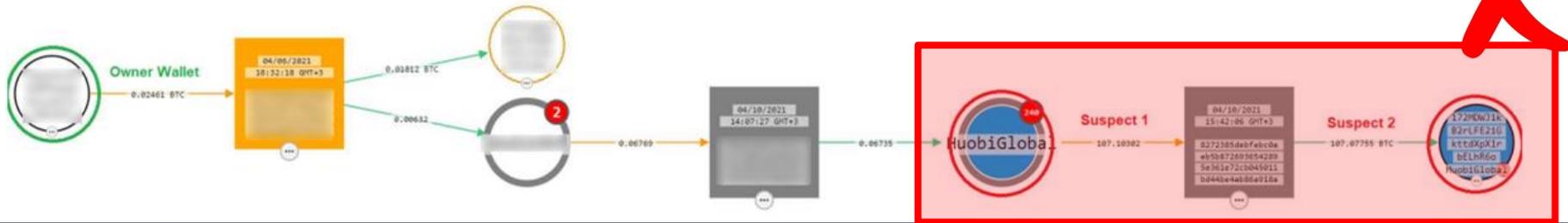


Images



Videos

About 24.700.000 results (0,52 seconds)



Investigating Scam

Private-Public Partnership



 EZRA REGUERRA OCT 03, 2023

Binance collaborates with Royal Thai Police to seize \$277M from scammers

Over 3,000 victims of the alleged crypto scammers have come forward to the authorities to file for compensation claims.

16840 Total views 19 Total shares [Listen to article](#)   2:15



COINTELEGRAPH 

[Collect article](#) Own this piece of history as an NFT

The Cyber Crime Investigation Bureau (CCIB) of the Royal Thai Police teamed up with Binance and U.S. Homeland Security Investigation (HSI) to dismantle a criminal ring behind a significant pig butchering scam that had impacted thousands of people in Thailand.

Armed with intelligence from Binance and HSI, the CCIB arrested five principal members of this group and confiscated assets valued at around THB 10 billion (\$277M), which included luxury cars, homes, land, and other upscale items. Since these events, over 3,200 victims have come forward seeking compensation.

Crypto Services: Internal Controls & Cooperation

Crypto Crime Risk Mitigation



- 1 Internal procedures: KYC/KYB, AML/CFT policies, Transaction Monitoring, Blacklisting**
- 2 Law Enforcement response, proactive investigations**
- 3 Public-private partnership**
- 4 Capacity building + awareness-raising**

Internal Controls

Onboarding



KYB & KYC

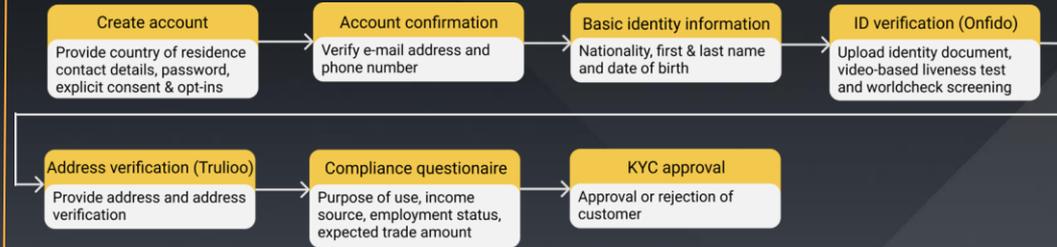
Name screening against multiple worldwide AML watchlist databases.

Proof of residency checks.

Other systems to review user's ID card and selfie / liveness check.

Mandatory ID verification.

Geoblocks.



Internal Controls

Transaction Monitoring



Transaction Monitoring

The live/post monitoring of all customer transactions (fiat & crypto)

Process

- Monitor transactions and assessing historical / current customer information

Purpose

- Identify suspicious transactions from an AML/CFT perspective for Binance to take appropriate actions

How Do We Do This

- Use a combination of internal and external tools that tracks fiat and crypto transactions
- Alerts will be identified for analyst review and investigation of the customer and account

Internal Controls

Suspicious Activity Reporting



Internal SAR

Every employee has an obligation to report suspicious activity on the platform.

Compliance Review / Investigation

Internal SARs are reviewed and further investigated by dedicated teams within Financial Crime Compliance department.

MLRO

Binance has regulatory obligation to report suspicious activity in certain jurisdictions.

MLROs assess SAR escalations to ensure compliance with regulatory requirements and company's risk appetite.

External SAR / STR

Reporting is done through the Money Laundering Reporting Officers (MLROs).

Suspicious activity may also be reported as a proactive referral to Law Enforcement.

Law Enforcement Response

Law Enforcement Response



Case Team

Most data requests are processed by a dedicated Case Team

Kodex Portal

<https://app.kodexglobal.com/binance/signup>



Investigations Team

Processes high-profile, complex, urgent cases

investigations@binance.com

Things to consider



Binance generally complies with cross-border law enforcement requests served directly to us **on a voluntary basis**, but...

- 1 Legal grounds/limitations to request data from a foreign entity**
- 2 Addressing proper legal entity**
- 3 Is the request necessary and proportionate?**
- 4 How confident are you in the tracing that led to Binance? Can you account for all hops in between?**
- 5 Can funds subject to seizure be linked to victim's lost funds? Are there any other victims?**

1 - For Account Records Requests:

Requests need to be addressed to appropriate data controller.

For global users - Nest Services Limited, House of Francis, Room 303, Ile Du Port, Mahe, Seychelles.

For EEA+CH users - Binance (Services) Holdings Ltd., 6th Floor, South Bank House, Barrow Street, Dublin 4, Ireland.

For users under local entities - local competent authorities through MLA, EIO or equivalent.

2 - For Account Freezes and Seizures:

Requests need to be addressed to appropriate operating entity that handles user assets.

For global users (including EEA+CH) - Nest Services Limited, House of Francis, Room 303, Ile Du Port, Mahe, Seychelles.

For users under local entities - local jurisdictions, through MLA, EIO or equivalent.

Licensed Jurisdictions

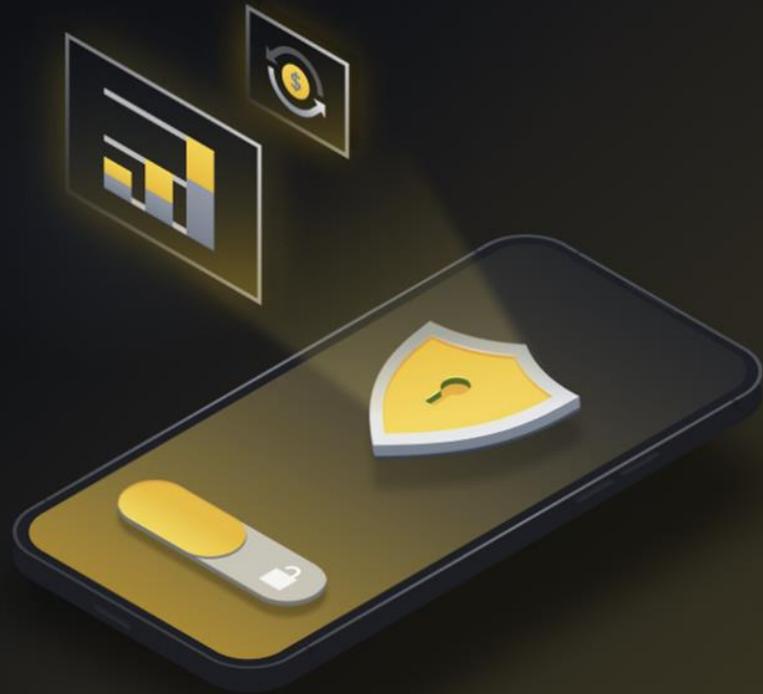
Different Data Disclosure and Legal Action Regime



- **Europe:** France, Italy, Lithuania, Poland, Spain, Sweden
- **CIS:** Kazakhstan
- **Middle East:** Abu Dhabi, Bahrain, Dubai
- **Asia-Pacific:** Australia, Indonesia, Japan, New Zealand, Thailand
- **Americas:** El Salvador, Mexico
- **Africa:** South Africa



What is Bifinity?



Requests: Do's and Don'ts



1 Submit requests via Kodex Portal

<https://app.kodexglobal.com/binance/signup>

- For prior consultation / coordination -
investigations@binance.com

2 Always include your full details to expedite the process

- Name, Position, Contact Information

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

4 Include description of suspicious activity / modus operandi

Requests: Do's and Don'ts



5 Provide the starting point

6 Avoid overly broad requests (fishing expeditions)

- Broad requests will get pushed back and additional justification will be requested

7 Provide unique identifiers

8 Add csv/excel or other copyable document

- No bullet-points / numbering

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

Unique Identifiers



- **Transaction hash/ID**
- **Binance deposit address**
- **For withdrawals - transaction hash and destination address**
- **Email address**
- **Phone number**
- **Internal identifiers (user ID, order number)**
- **For FIAT transactions: date, amount, credit card number (6 first, 4 last digits), full IBAN, sometimes ARNs**

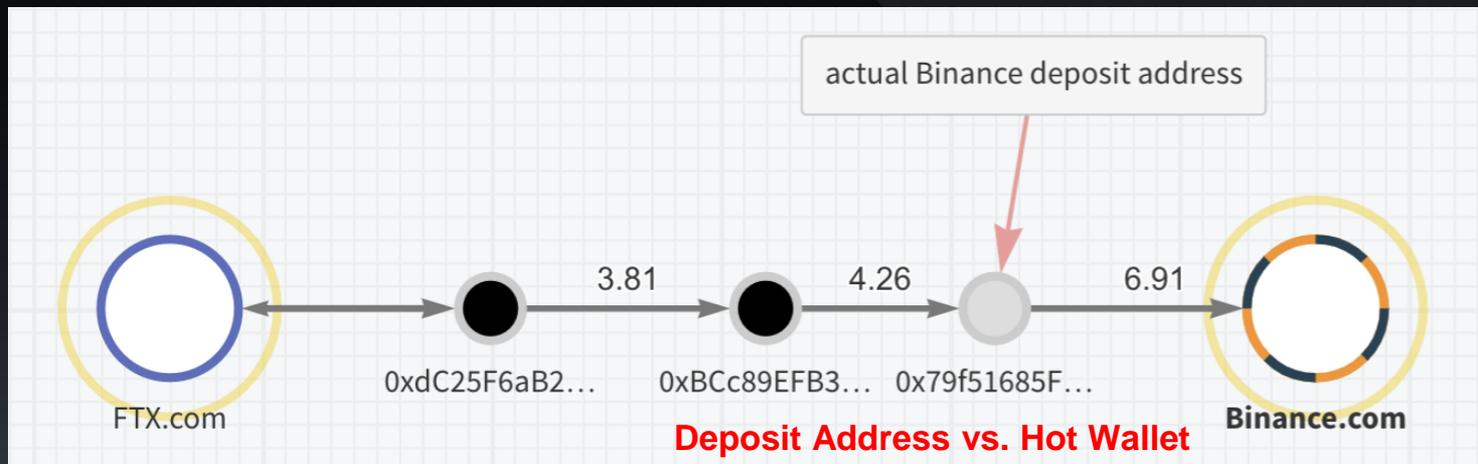
Not-that-unique Identifiers



- **Name and or last name**
 - **Include DOB**
 - **Consider different variants, alphabets**
 - **No fuzzy match, has to be exact**

- **IP addresses**
 - **Include time range, better yet - multiple time ranges for the same IP address**
 - **Manage expectations - dynamic / mobile / VPN / proxy**

Deposit Address



Deposit Address vs. Hot Wallet

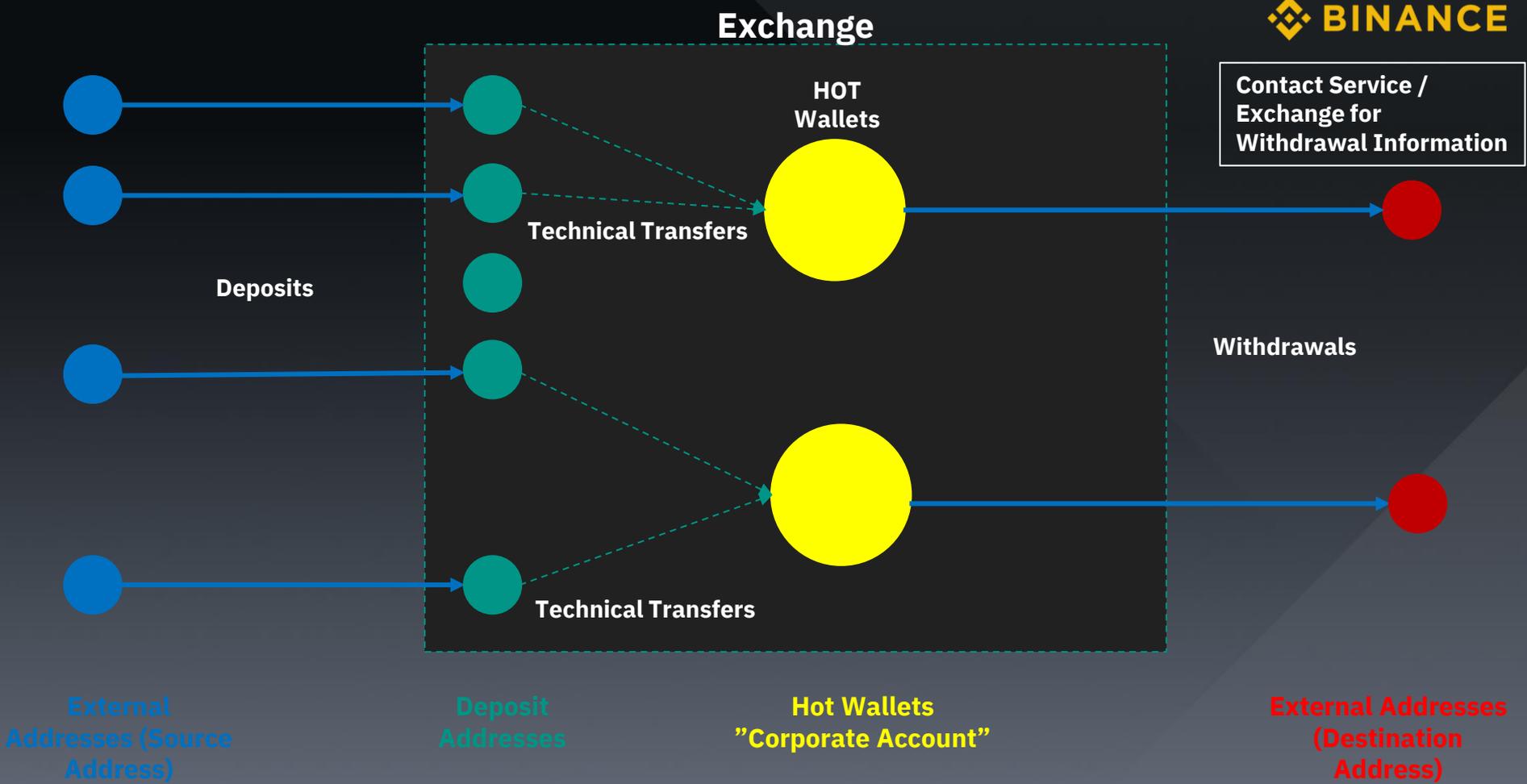
The screenshot shows a blockchain explorer interface. At the top, it displays the address 0x79f51685F69DAbEc806ca049f8FF8D9D968F1DC8. Below this, there is a featured section about DEX trading pairs. The main content is divided into two columns. The left column has an 'Overview' section with a table:

Balance:	0.062436866645711948 Ether
Ether Value:	\$161.10 (@ \$2,580.25/ETH)

The right column shows the profile for 'Binance' with the address 0x79f51...f1dc8 and a label 'Exchange'. Below that, it lists 'Related Entities' including 'Binance'.

Tracing Tools Are Not 100% Accurate!

Hot Wallet



Withdrawal address



Transaction 35 [redacted].5388

Blockchain Bitcoin

TxHash
350b69 [redacted]

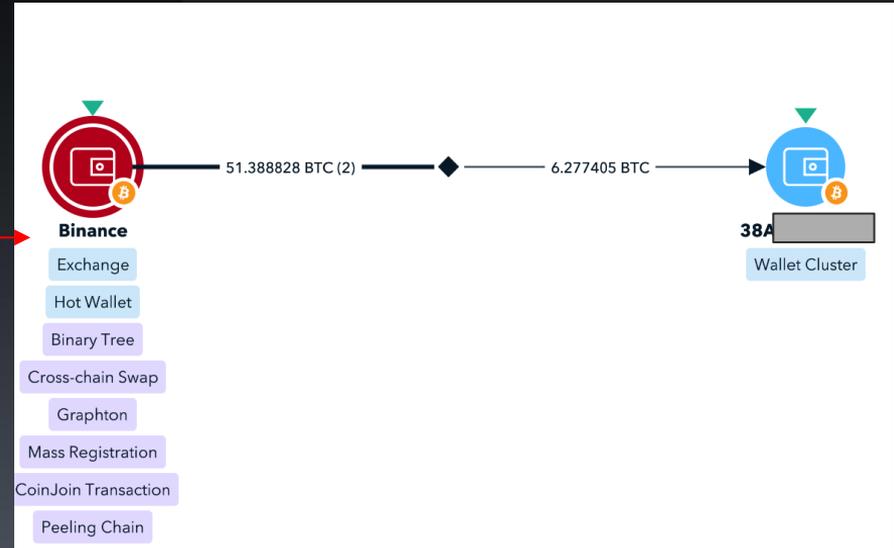
Timestamp:
Nov 25, 2020 2 [redacted]

Transfers Details

Total volume (USD) \$1,997,642

Inputs 3			Outputs 99		
	Address	Amount		Address	Amount
<input checked="" type="checkbox"/>	1N [redacted]	-49.641176	<input type="checkbox"/>	bc1 [redacted]	+10
<input type="checkbox"/>	bc [redacted]	-0.011045	<input type="checkbox"/>	bc1 [redacted]	+0.014
<input checked="" type="checkbox"/>	1N [redacted]	-1.747651	<input type="checkbox"/>	3Q3 [redacted]	+0.052637
			<input type="checkbox"/>	1Na [redacted]	+0.0995
			<input type="checkbox"/>	1Ng [redacted]	+0.001098
			<input type="checkbox"/>	1Bz [redacted]	+0.3195
			<input type="checkbox"/>	3EW [redacted]	+0.101066
			<input type="checkbox"/>	bc1 [redacted]	+0.001
			<input type="checkbox"/>	3Hz [redacted]	+0.499577
			<input type="checkbox"/>	3AB [redacted]	+0.0188

< 1 2 3 4 5 ... 10 >



Asset Freezes

Temporary Freezes



- **Separate Kodex ticket**
- **Courtesy Freeze**
 - Up to 7 days
 - LE contact details (unless NDO is issued, except: TF, CSAM, imminent threat to life)
- **Freeze upon Legal Order**
 - Court / Prosecutor
 - LE contact details
 - Should not be long-term even when legitimate

Asset Seizures



- **Separate Kodex ticket**
- **Legal enforcement document (court order)**
- **Seizure instruction template**
- **LE's contact details**
- **Specific assets and amounts to be seized, no conversion**
- **Recipient address: LE / victim**
 - **If FIAT (bank account), confirmation of ownership from the bank**

'Nested' services



Some services use the liquidity or the backend system of an exchange for their services.

- Service registration data not to be disclosed (unless they are the subject of investigation)
- No visibility into end-user data
- LE advised to send requests directly to the service
- Account freezes/seizures will also have to be addressed to the service

Examples: Swapping services, OTC-services, regional exchanges, hosted wallet services.

Welcome to Crypto

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

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

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



Education, Prevention, Awareness



BINANCE

Know Your Scam

How to Identify Fake Shopping Websites

BINANCE

Know Your Scam

How to Identify and Avoid Ponzi Schemes

BINANCE

Know Your Scam

How to Spot and Protect Yourself From Romance Scams

BINANCE

Know Your Scam

Fake Crypto Investments to Watch Out For

BINANCE

Know Your Scam

A definitive guide to crypto's most prevalent scams

BINANCE

Know Your Scam

Protect yourself from crypto giveaway scams

Phishing Scam Alert

There has been a recent, large-scale SMS phishing scam sending users a link to cancel fake crypto withdrawals. The SMS directs the recipient to a URL similar to www.cancelXXX.com. The website is, in fact, a phishing attempt to steal your account.

GOT IT

Risk Disclaimer

Read the risk disclaimer carefully, and check the following options to acknowledge confirmation.

Do you confirm the purpose of this withdrawal and guarantee that there is no risk of fraud?

I confirm that this withdrawal is risk-free.

This withdrawal may result in the loss of funds. Funds cannot be recovered once the withdrawal is successful. Do you want to continue?

I want to continue and will bear the risk associated with any possible loss of funds.

Next

Verification Questionnaire

In order to keep your assets secure, you will need to complete a verification questionnaire before making withdrawals.

01. If someone claiming to be "Binance Customer Service" asks you to log into your account or to transfer money, would you do as they request?

A. Yes

B. No

Next

Cooperation with HKPF

- ⚠️ "In 2021, more than 19,000 online or offline scam cases occurred in Hong Kong, averaging one case every half hour!"
- ⚠️ Beware of new scams. Under no circumstances will Binance call you directly. [Learn more](#)
- ✅ Participate in activities only on the official Binance website
- ✅ Verify sources via [Binance Verify](#) to check if it is official
- ❌ Ignore unrealistic high ROI investments
- ❌ Ignore requests from government impersonators
- ❌ Do not withdraw to unofficial addresses or platforms
- ❌ Do not disclose your verification code or account information to anyone
- ⚠️ If in doubt, call the "Anti-Scam Helpline (+852) 18222" (Hong Kong Police Force) for enquiries or verify the counterparty's URL, fund receiving accounts, phone number, etc. using [Scameter](#)
- ⚠️ For more anti-scam advices, please visit the websites of the [Anti-Deception Coordination Centre](#) and [Cyber Defender](#) from the Hong Kong Police Force.





Binance Launches Global Law Enforcement Training Program



Questions?



investigations@binance.com

lilija@binance.com



Open source tools, computer forensics in the “Cloud”

Bilal Şen

Corporate Investigations and Cybercrime Advisor



Consultancy Investigation Security
www.coninsec.com



Co-funded by
the European Union



OSINT

Open Source Intelligence (OSINT) refers to the collection, analysis, and dissemination of information from publicly available sources. These sources include media, the internet, public government data, professional publications, commercial data, and more. OSINT is used by various organizations, including governments, businesses, and non-governmental entities, to gain insights and make informed decision

COMMON OSINT USAGE

It is not hacking

It is not invented by law enforcement

It is not always 'free'

It is not just the internet

It is not something the subject/s cant do

It is not as easy as we think it is

It is not only for justice and security

Publicly available?

May require verification

Litigation Check

Evidence Collection

Investigation (Crime or Dispute)

Due Diligence (Company Accusation)

Competition (Commercial Intelligence)

Protection (Parents & Juveniles)

Reconnaissance (Hacking)

PenTest (Cyber Security)

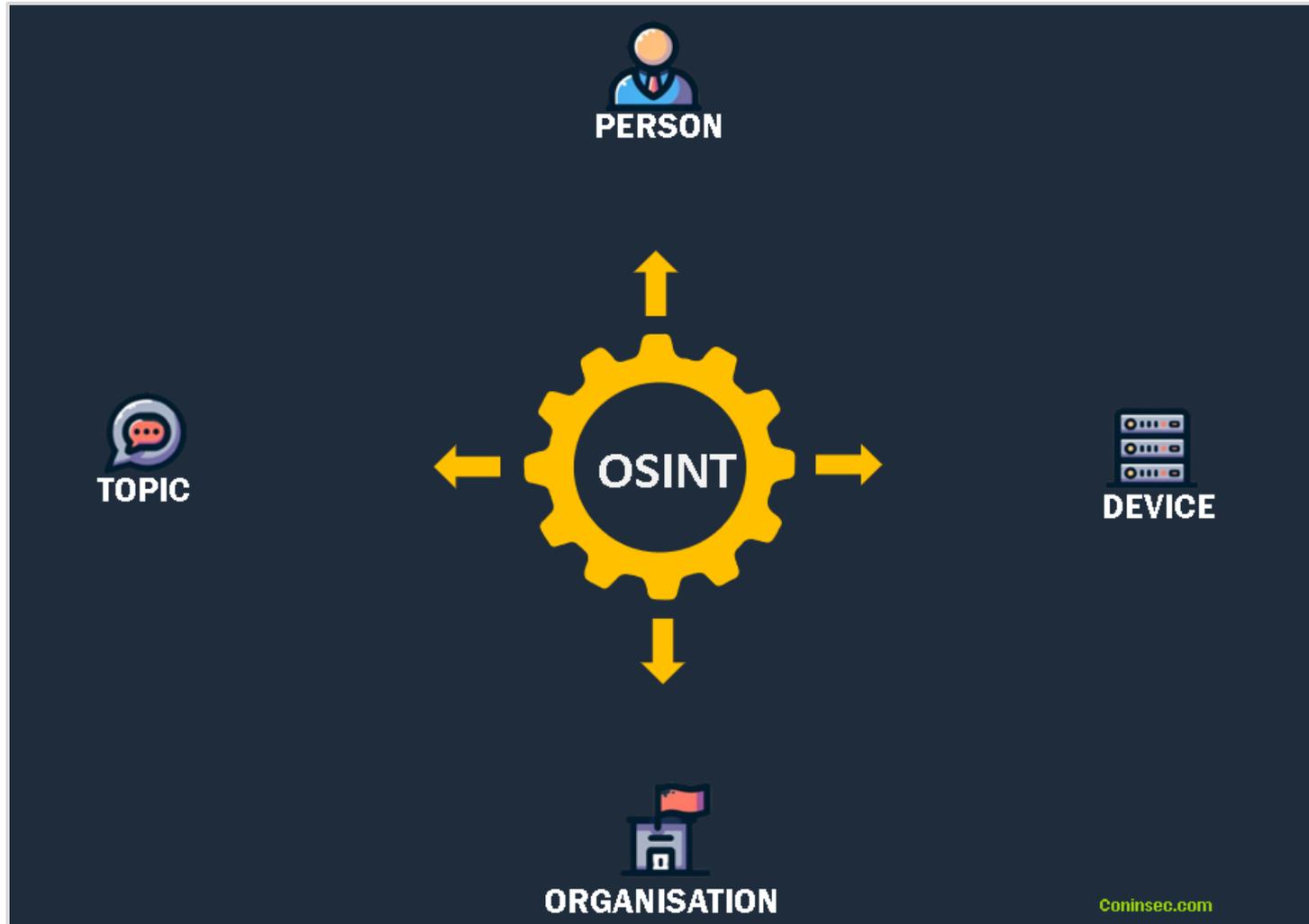
Research (Neighborhood Check)

Verification (CV Verification)

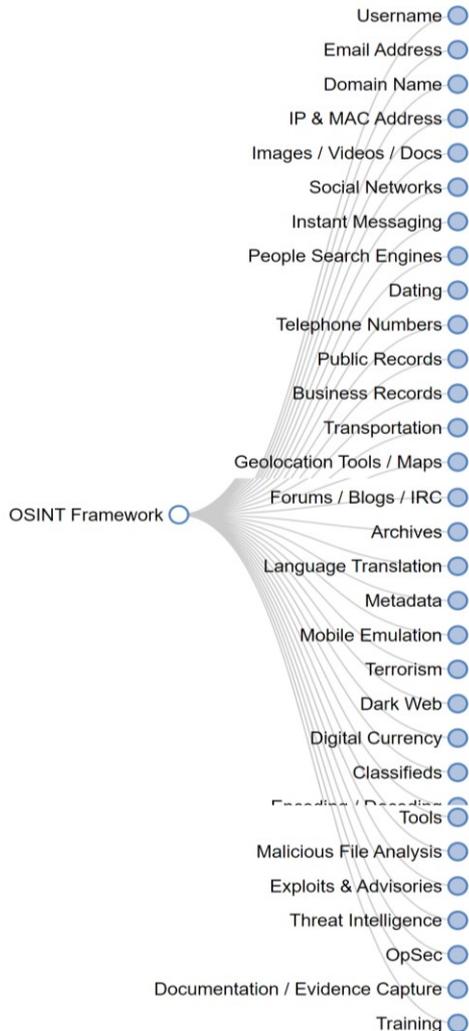
Defense (Military Monitor)

Academic (Research)

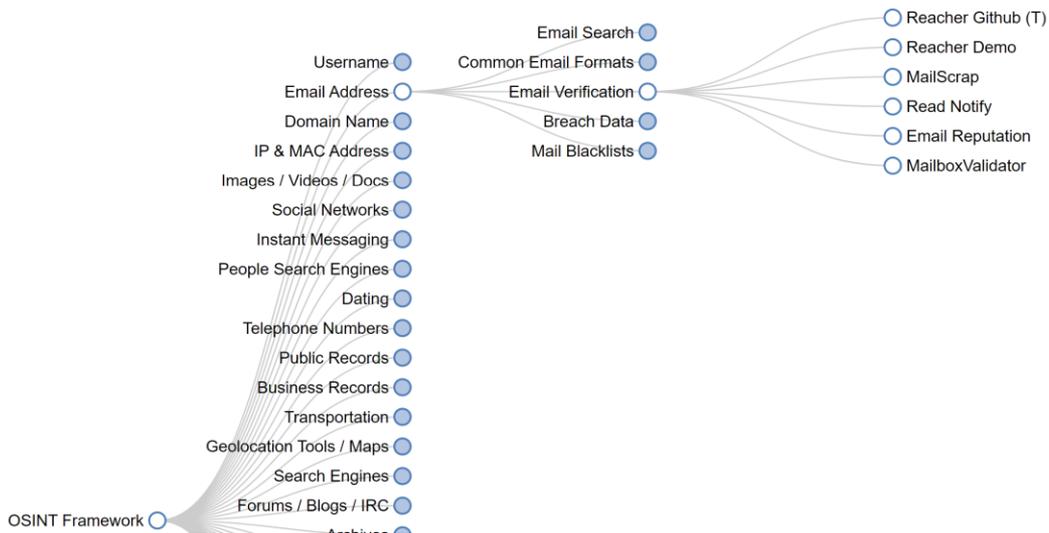
OSINT



OSINT FRAMEWORK



OSINT Framework

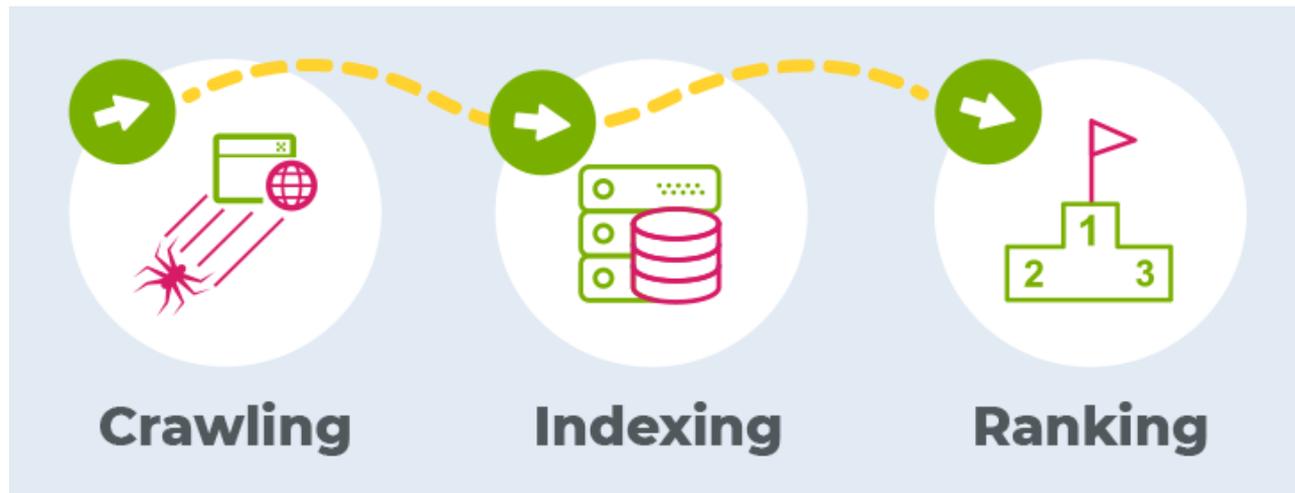




SEARCH POSSIBLE WITH

- TEXT
- IMAGE
- VOICE
- VIDEO
- FILE
- URL

GOOGLE SEARCH PROCESS



ROBOT.TXT

```
User-agent: *  
Disallow: /cgi-bin/  
Disallow: /wp-admin/  
Disallow: /wp-content/  
Disallow: /wp-includes/  
Disallow: /recommended/  
Disallow: /comments/feed/  
Disallow: /trackback/  
Disallow: /index.php  
Disallow: /xmlrpc.php  
Disallow: /wp-content/plugins/
```



**Will always be
ignored by the
Search Engine bots.**

```
User-agent: NinjaBot  
Allow: /
```

```
User-agent: Mediapartners-Google*  
Allow: /
```

```
User-agent: Googlebot-Image  
Allow: /wp-content/uploads/
```

```
User-agent: Adsbot-Google  
Allow: /
```

```
User-agent: Googlebot-Mobile  
Allow: /
```

GOOGLE LOCAL COPY SEARCH TEST

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

isearchfrom.com



I Search From

Google Search from a different location & device

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

Country: ⓘ

Language: ⓘ

Device: ⓘ

More options

City: ⓘ

Find only pages from the specified country: ⓘ

Find only pages in the specified language: ⓘ

Logged in: ⓘ

Personalized search: ⓘ

Location: Greece



MOST HELPFUL INFO TO START

PERSON

FULL NAME

EMAIL ADDRESS

MOBILE PHONE

NUMBER

FACE PHOTO

ENTITY

FULL NAME

WEBSITE

TAX NUMBER

EMAIL ADDRESSES

BUSINESS ADDRESSES

WHO CREATE/UPLOADS INFO ABOUT US

- WE
- OUR PRIVATE AND PROFESSIONAL CONTACTS/
COMPATITORS
- PROFESSIONALS
- INSTITUTIONS
- BREACH RECORDS
- MACHINES

Some of Breach Records



2016 : 117 Million

April 2021 : 700 Million

Feb 2023 : 500 Million



Sep 2019: 700 Million

April 2021: 530 Million



Jan 2021: Unknown

Jan 2023: 200 Million



**Power your passion for
sports**

DOWNLOAD THE FREE APP!



site:sports-tracker.com



sports-tracker.com

<https://sports-tracker.com> > view_profile > arivenem

Ari Venemies

Ari Venemies · 1150 h · 13536 km · 1134 h · 25044 km · 134 h · 1711 km. No public workouts ...



sports-tracker.com

<https://sports-tracker.com> > view_profile > albormax

Albonino Massimo

3rd fastest time on this route. Albonino Massimo Maniva. Send. Albonino Massimo Jul 1, 2021 at 8:56 AM · OpenStreetMap, Thunderforest.



sports-tracker.com

<https://sports-tracker.com> > rah_kis · [Translate this page](#)

Kimmo Rahkamaa

Kimmo Rahkamaa Kolmen huipun päivä: Tennkogel-2333, Frauenkogel-2424 ja Gamskarkogel-2467. Lähdettiin 1740 m:stä, johon myös palattiin. Kokonaisnousu 900m. HR ...



sports-tracker.com

<https://sports-tracker.com> > view_profile > eduardosamuco

Eduardo Samuco

Eduardo Samuco. Add friend. Request sent Request pending. Follow Requested Cancel Following Unfollow Follows you Um pouco da minha rotina desportiva.

site:sports-tracker.com Wiesbaden



All Images News Videos Books More Tools

Weather Hotel Sehenswürdigkeiten Football Zip code Time Exchange USAG

About 1 results (0,25 seconds)

Images :



Sascha

Sports Tracker



Lars Lampe

Sports Tracker



Lars Lampe

Sports Tracker

[Feedback](#)

6 more images

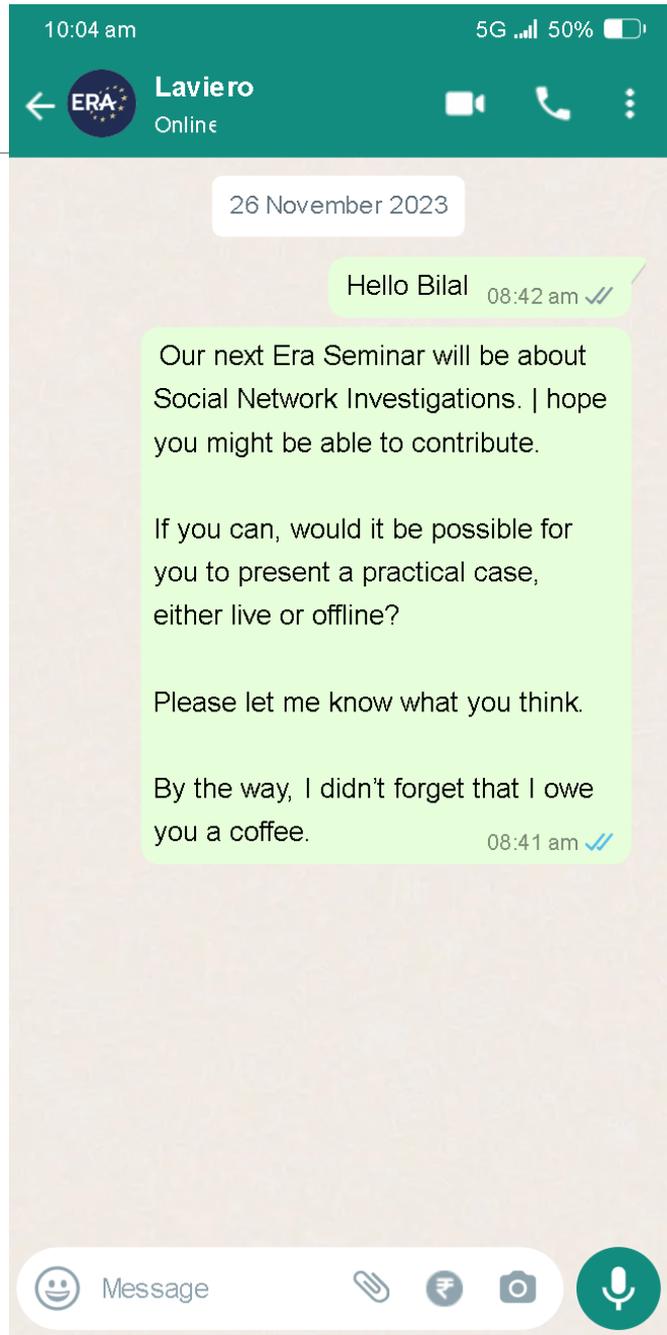


sports-tracker.com

<https://www.sports-tracker.com> > Ila · [Translate this page](#)

Lars Lampe

Sonntag-Skaten in **Wiesbaden** hat nicht statt gefunden :-D 2. Die Strecke war staubfrei und hatte geringeren Rollwiderstand 3. Es waren recht wenige Fußgänger ...



10:04 am 5G 50%

← ERA **Laviero** Online

📺 📞 ⋮

26 November 2023

Hello Bilal 08:42 am ✓✓

Our next Era Seminar will be about Social Network Investigations. I hope you might be able to contribute.

If you can, would it be possible for you to present a practical case, either live or offline?

Please let me know what you think.

By the way, I didn't forget that I owe you a coffee. 08:41 am ✓✓

😊 Message 📎 ₹ 📷 🎤

Fake Whatsapp Chat Generator

 Desktop View

 Mobile View

Hide Header

Hide Footer

Dark Theme

Layout :

Android

iPhone

Network

5G

10:04



12 Hour

Battery Options

Horizontal

50

% Battery

Show Percentage

Hide Payment

Dual Sim

Change Background 

Reset 

Live preview





-  Whatsapp »
-  Facebook »
-  Instagram »
-  X (formerly Twitter) »
-  Tiktok »
-  YouTube »
-  Hangouts »
-  Chats »

Fake Det

Generate Mail

The Fake Mail Generator is a site that enables you to circumvent email affirmations by giving you a one time email address to utilize. Next time a site requests your email address, give them a Fake Mail Generator address and stay away from the spam that is certain to follow.



Events | e-Learning | Resources and Projects | About ERA

ERA Annual Report 2023 available

Everything you always wanted to know about ERA's achievements in 2023, but were afraid to ask... is now available in our annual report!

Curious about our impact? Here are just a few of the questions our annual report answers:

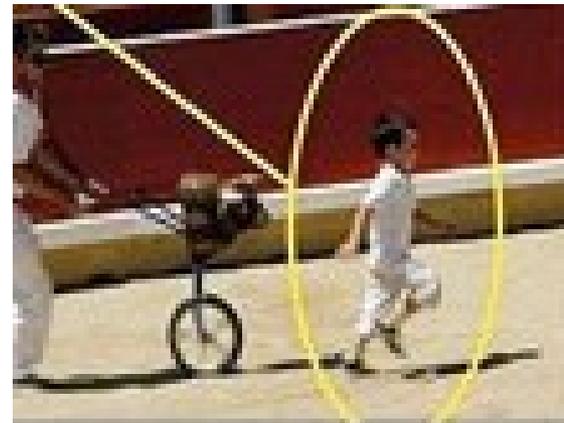
- How many legal professionals did ERA train in 2023?
- Where did they come from?
- What is our strategy for the young(er) generation?
- How does our team look like?
- What is the European Forum of the Legal Professions?
- Who were our partners last year?

You'll find the answers to all these existential questions in the report. Discover all the highlights and achievements from an incredible year.

Happy reading!
Link: <https://annualreport2023.era.int/>



ADMISSIBILITY & VERIFICATION



PROTECTING YOUR PRIVACY WHEN INVESTIGATING

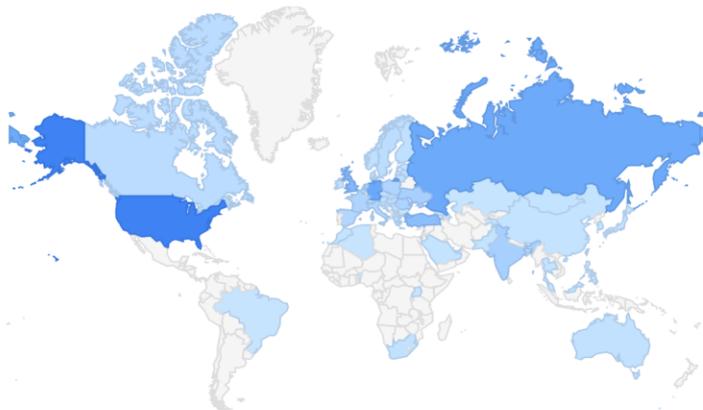


[See Full Report](#)



[See Full Report](#)

Sessions by country



Countries

United States >	68
Germany >	42
Russia >	41
United Kingdom >	30
Turkey >	27
Ukraine >	14

PROTECTING YOUR PRIVACY WHEN INVESTIGATING

Use a VPN (Virtual Private Network)

Encrypts your internet connection.

Masks your IP address and location.

Provides anonymity and prevents tracking.

Utilize VM (Virtual Machines)

Isolates your investigation environment from your primary system.

Protects your main system from malware and other online threats.

Allows you to use different operating systems and configurations securely

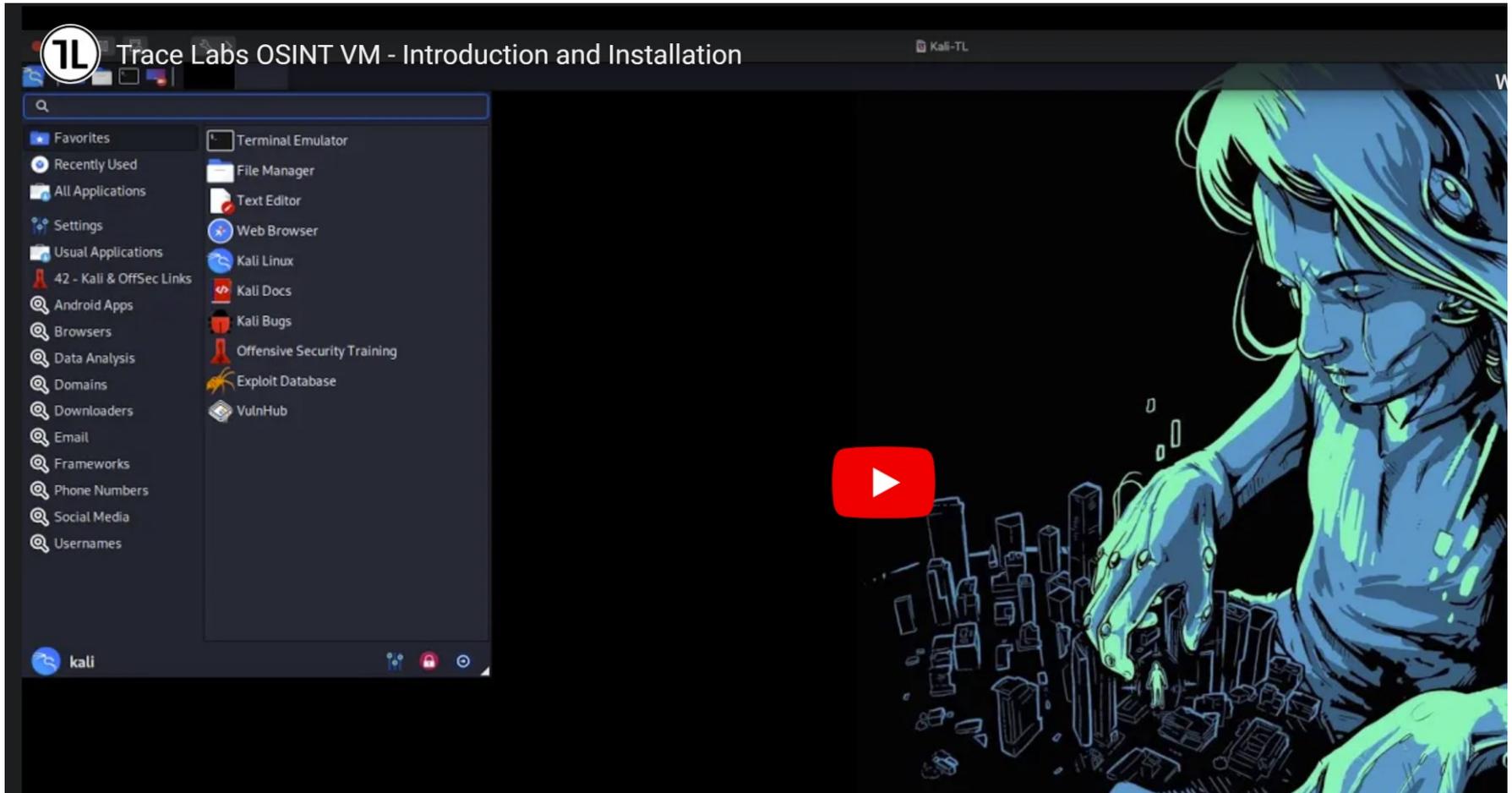
User Agent Changer

Modifies your browser's user agent string.

Helps in disguising the type of device and browser you are using.

Useful extensions include User-Agent Switcher and Manager for browser.

PROTECTING YOUR PRIVACY WHEN INVESTIGATING



ALERT MANAGEMENT



The creation and management of search alerts is an automated process that passively gathers information, aiding in the collection of timely and updated data.

www.talkwalker.com/alerts

www.google.com/alerts

LETS DO PRACTICAL

Your job should you choose to accept it



WHATSAPPMYNAME

Enter the username(s) in the search box, select any category filters & click the search icon or press CTRL+Enter

Category Filters ▾

🔍
👤

Active Filter: All (exclude NSFW)

Found: 45 **Processed:** 592 / 592

- Show Found
Show False Positives
Show Not Found
Show All
Open All Links
🖨️

<p>biolink</p> <p>Username: bilalsen Category: misc Account Found</p>	<p>Behance</p> <p>Username: bilalsen Category: business Account Found</p>
<p>Blogspot</p> <p>Username: bilalsen Category: blog Account Found</p>	<p>buymeacoffee</p> <p>Username: bilalsen Category: finance Account Found</p>
<p>Chess.com</p> <p>Username: bilalsen</p>	<p>Clubhouse</p> <p>Username: bilalsen</p>

Filter by Username:

bilalsen

Show 50 rows ▾
Copy
CSV
PDF
Search:

SITE	USERNAME	CATEGORY	LINK
Behance	bilalsen	business	https://www.behance.net/bilalsen
biolink	bilalsen	misc	https://bio.link/bilalsen
Blogspot	bilalsen	blog	http://bilalsen.blogspot.com
buymeacoffee	bilalsen	finance	https://www.buymeacoffee.com/bilalsen
Chess.com	bilalsen	gaming	https://www.chess.com/member/bilalsen
Clubhouse	bilalsen	social	https://www.clubhouse.com/@bilalsen



ONLINE DATA & OLD DATA & DELETED DATA

ARCHIVE

URL COLLECTION

FREEZING THE TIME

ALTERNATIVE COULD BE BETTER

GOOGLE MAP RESULTS

Thracomakedonon 101, Acharne

Hellenic Police Officers School
Σχολή Αξιωματικών Ελληνικής Αστυνομίας
4.4 ★★★★★ 107 reviews ⓘ
Police academy

Thracomakedonon 101, Acharnes 136 71, Greece

Θρακομακεδόνων 101, Αχαρνές 136 71

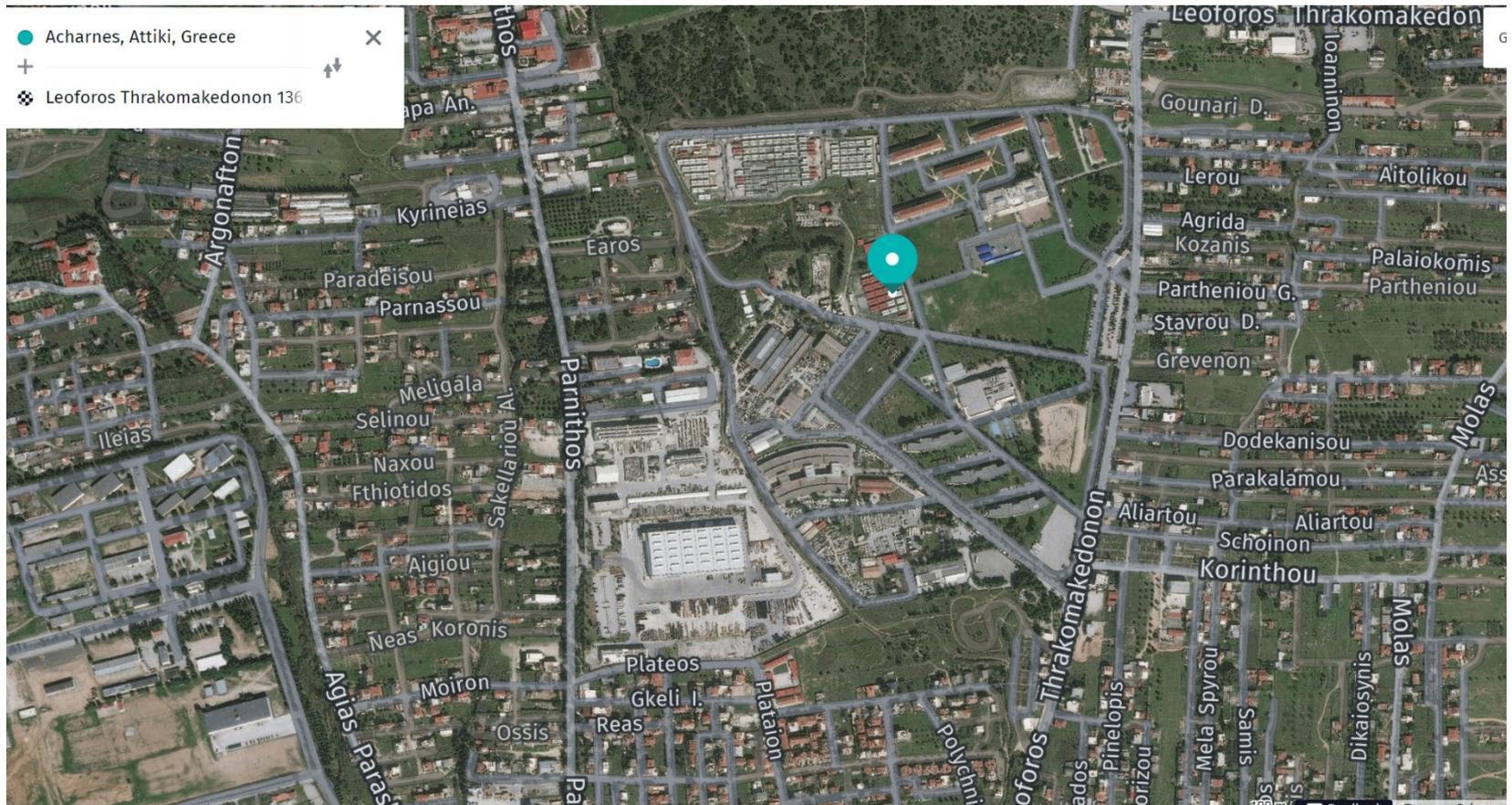
Open 24 hours

astynomia.gr

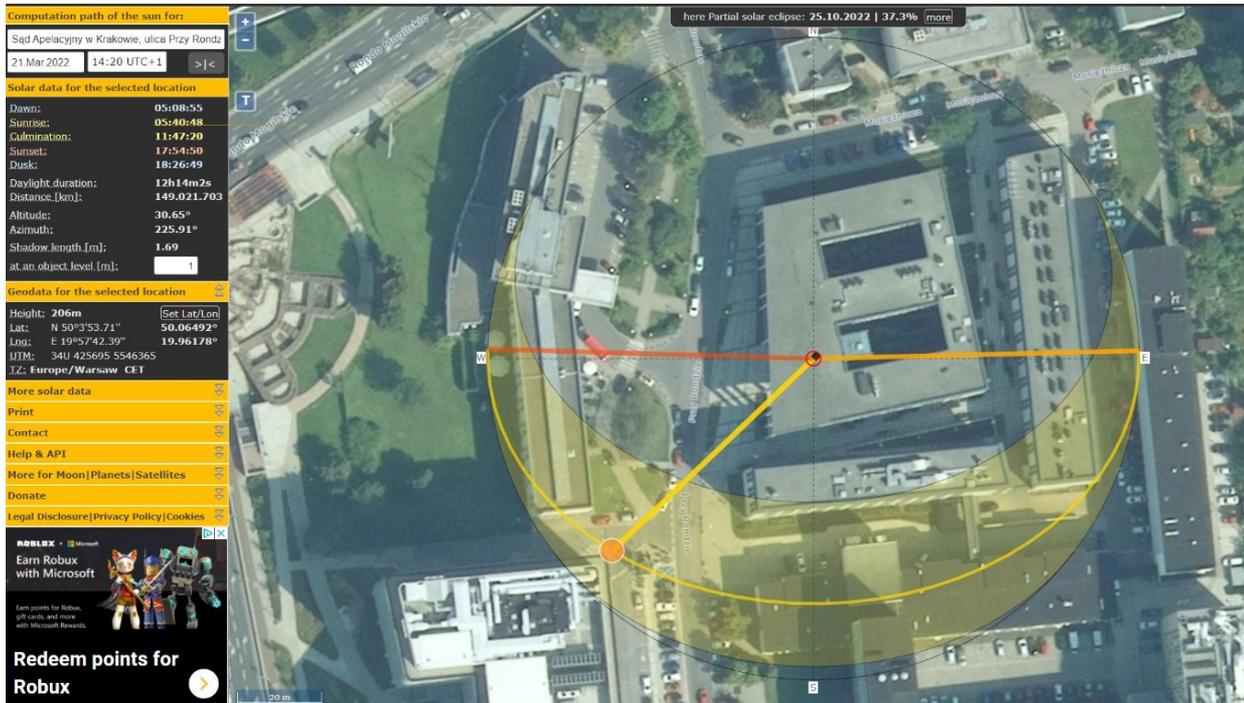
Map labels: Peloponnisos Event Venue - ΠΕΛΟΠΟΝΝΗΣΟΣ, Κτήμα Κοτρωνιάς, HOTEL CAVALLARI PALACE, Tavern Vlachos ΤΑΒΕΡΝΑ Θ ΒΛΑΧΟΣ, ΟΤΕ LOGISTICS CENTER, Κτίμαορίνο Κτήμα Ορεινό # gamos parnitha, Πιρουνάκια grill Gyrol restaurant, Μασούλης Μασούτης, ΧΑΤΖΗΓΕΩΡΓΙΟΥ ΕΜΜΑΝΟΥΗΛ, IL TOTO Θρακομακεδόνες, Γαλακτοπωλείο ΣΤΑΜΟΥ Γαλακτοπωλείο Στάμου, Arma Shoes S.A. ARMA SHOES A.E., MEGALA SCHINA ΜΕΓΑΛΑ ΣΧΙΝΑ, Esti Athens

ALTERNATIVE COULD BE BETTER

wego.here.com



suncalc.org



The SunCalc is a sunlight calculator. It helps determine time and date by sun movement and sunlight analysis during the given day at the given location.

COMPETITOR ANALYSIS FOR AUTOMATIVE

Uncover Everything About Your
Trade Partner and Make Informed
Decisions



HOW THE COMPATITOR IS THIS FAST





Search

Technology

Products

About

We are hiring

Reverse Image Search

Find where images appear online. [How to use TinEye.](#)

 Upload

Paste or enter image URL



Tineye Test



tineye.com



STOCK · SPONSORED www.shutterstock.com ENJOY 15% OFF. Use **TINEYE15** on Shutterstock.

[image-photo/paris-sept-17-2014-wester...](#) - First found on Jun 11, 2022



STOCK · SPONSORED stock.adobe.com

[images/Prospetto-di-Notre-Dame-a-Par...](#) - First found on Oct 25, 2021



STOCK · SPONSORED www.alamy.com

[paris-sept-17-2014-the-western-facade...](#) - First found on Sep 25, 2021



dinneratmidnight.wordpress.com

[2010/11/14/travels-part-2-paris/](#) - First found on May 14, 2017

[2010/11/14/travels-part-2-paris/](#) - First found on May 14, 2017

[view all 3 matches](#)

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



shutterstock | 

GET 10 FREE IMAGES

ARTIFICIAL INTELLIGENCE & OSINT



CHATGPT CONTRIBUTION

How you may contribute law practitioners at public and private domain?

1. Legal Research Assistance:
2. Drafting Legal Documents:
3. Case Analysis:
4. Legal Writing Support:
5. Compliance Guidance:
6. Language Translation:
7. Legal Education:
8. Stay Updated on Legal Trends:
9. Ethical Considerations:
10. Automation of Routine Tasks:
11. Client Communication:
12. Data Analysis:

It's important to note that while AI can be a valuable tool for legal professionals, it should **complement, not replace**, the expertise of human practitioners. Legal AI can **expedite processes, increase efficiency, and enhance the quality of work**, but **human judgment and interpretation are crucial** in many legal contexts.

GOOGLE AND CHATGPT TOGETHER



list all all new laws in Germany introduced in 2020



All News Books Images Shopping More Tools

About 1.730.000.000 results (0,51 seconds)

<https://www.gibsondunn.com> › 2020-year-end-german-... :

2020 Year-End German Law Update - Gibson Dunn

14 Jan 2021 — The draft bill provides for new rules designed to bolster both the ... On November 20, 2020, the German government released a draft tax bill ...

<https://www.iamexpat.de> › german-expat-news › 2020-... :

2020 in Germany: All of the changes expats need to know about

1 Jan 2020 — New year, new laws! 2020 is here, and it's brought a whole shedload of changes to Germany. Here is an overview of the most important changes ...

People also ask :

What is the new law in Germany 2020 about immigration? ▾

What is the new law in Germany? ▾

What are the new laws for refugees in Germany 2022? ▾

What is the new law for duldung in Germany 2022? ▾

Feedback

<https://www.bundestag.de> › legislation › passage-245704 :

Passage of legislation - German Bundestag

First comes the bill Laws determine how individuals live together. They are general rules that are binding on the whole community.

Missing: 2020 | Must include: 2020

<https://www.make-it-in-germany.com> › visa-residence :

The Skilled Immigration Act - Make it in Germany

The Skilled Immigration Act is a new law which expands the number of opportunities for qualified professionals to come to work in Germany.

ChatGPT



As an AI language model, I do not have access to real-time data and my training data only goes up until September 2021. However, I can tell you that there were many new laws introduced in Germany in 2020 covering a wide range of topics such as climate change, digitalization, health, and social policies, among others. Some examples include the following:

- The Act on the Establishment of a Federal Climate Change Act (Bundesklimaschutzgesetz) to regulate the country's greenhouse gas emissions and set targets for reducing them by 2030 and beyond.
- The Act on the Protection of Children and Youth in Online Media (Jugendschutzgesetz) to better safeguard minors from harmful content and improve online safety.
- The Act for the Improvement of Nursing Care (Pflegepersonal-Stärkungsgesetz) to increase the number of nursing staff in hospitals and nursing homes and improve their working conditions.
- The Act on the Expansion of the Renewable Energy Sources (Erneuerbare-Energien-Gesetz) to promote the use of renewable energy and reduce the reliance on fossil fuels.
- The Act on the Modernization of the Occupational Safety and Health Act (Arbeitsschutzmodernisierungsgesetz) to strengthen worker protection and improve working conditions.

It is important to note that this is not an exhaustive list and there may have been additional laws introduced in Germany in 2020 that are not mentioned here.

AI OSINT EVALUATION: YOU.COM



"bilal sen" cyber



All Chat Images Videos News Maps More

2 apps and 5,110,000 results

LinkedIn

Edit

linkedin.com > pulse > stopping-ransom...

Stopping Ransomware and Cyberattacks Part 1: Picture of Horror - LinkedIn

Bilal Sen Corporate investigations and Cybercrime Advisor Published Feb 10, 2022 + Follow Cybersecurity has...

de.linkedin.com > in > bilal-sen

Bilal Sen – Köln, Nordrhein-Westfalen, Deutschland | Berufsprofil...

Bilal Sen – Köln, Nordrhein-Westfalen, Deutschland | Berufsprofil | LinkedIn
Bilal Sen Corporate investigations an...

linkedin.com > pulse >

Stopping Ransomware and Cyberattacks Part 2 Blue...

Bilal Sen Investigation Advisor Published Feb... Follow In today's legal...

GERMANY/DENMARK/France/UNITED KINGDOM : Bilal Sen, Audere, EuroSatory ...

intelligenceonline.com/corporate-intelligence > 2022/06/08 > bilal-sen-audere...

Cologne: Turkish ex-cyber police official moves into German corporate intelligence **Bilal Sen**, a founder of the Turkish National Police (TNP) cybercrime department, is increasingly involved in his new Cologne-based firm...

Stopping Ransomware and Cyberattacks Part 1: Picture of Horror - LinkedIn

linkedin.com > pulse > stopping-ransomware-cyberattacks-part-1-picture-horror...

Bilal Sen Corporate investigations and Cybercrime Advisor Published Feb 10, 2022 + Follow Cybersecurity has become an increasingly important matter over the last 15 years, but it has never been...

February 2023

B

"bilal sen" cyber

Bilal Sen – Köln, Nordrhein-...

 de.linkedin.com

Stopping Ransomware and...

 bilalsen.medium.com

Bilal Sen Archives - Peninsula Press

 peninsulapress.com

FBI, Secret Service in New...

 fbi.gov

Bilal SEN's Email & Phone - ...

 contactout.com

GERMANY/DENMARK/France/UNIT...

 intelligenceonline.com

Bilal Sen and Cybersecurity

Bilal Sen is a name associated with cybersecurity and law enforcement. While there isn't a lot of information available about Bilal Sen specifically, here are some relevant details:

- Bilal Sen is mentioned in a LinkedIn profile based in Köln, Nordrhein-Westfalen, Deutschland (Germany).
- He has written an article on Medium about stopping ransomware and cyberattacks.
- Bilal Sen has been part of an international law enforcement panel at Stanford, representing the United Nations Office on Drugs and Crime ¹.
- He is also associated with the field of cybercrimes and emerging technologies in the security and investigations industry.
- Bilal Sen has been involved in the establishment of a Cologne-based firm called Coninsec (Consulting Investigation Security), which provides investigation consultancy on risks, cybercrime, and fraud using comprehensive open-source intelligence (OSINT) and human intelligence (HUMINT) techniques in Germany ².

March 2024

OSINT Case Demonstration





QUESTIONS & DISCUSSION

Bilal Şen

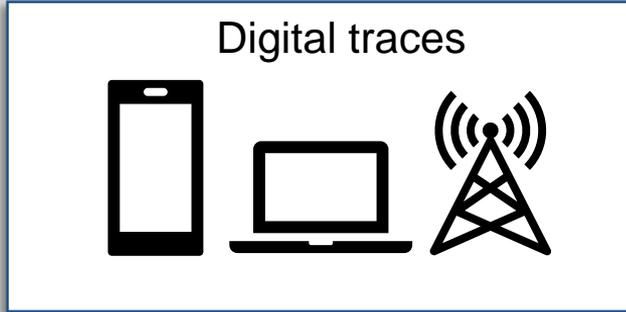
bs@coninsec.com

Technical and human errors (and their sources) related to the collection and presentation of electronic evidence

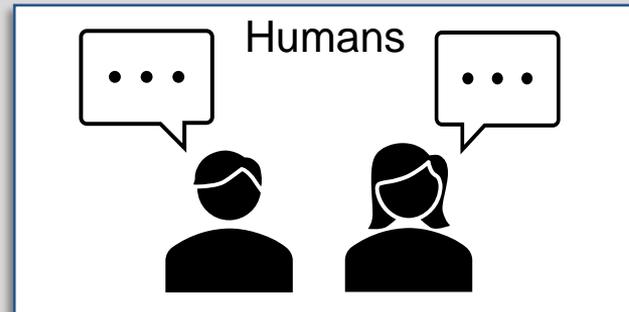
Nina Sunde, Police Superintendent /PhD
Norwegian Police University College

Agenda

- Is digital evidence objective, value-neutral and reliable?
- Bias and noise in digital forensic examinations
- Evidence dynamics and evidence elasticity
- Transparency and auditability of digital forensic investigation practices



Objective
Value-neutral
Independent
Detailed, reliable, and accurate
Silent digital witness - 'Does not lie'



Subjective
Influenced by moral and emotions
Biased
Vulnerable cognitive processes may result
in inaccurate or erroneous accounts
May lie

**UNIVERSITY
OF OSLO**

Faculty of Law

Nina Sunde

Constructing digital evidence

A study on how cognitive and human factors affect digital evidence

2022



Digital Investigation 29 (2009) 461–469

Contents lists available at ScienceDirect

Digital Investigation

ELSEVIER

journal homepage: www.elsevier.com/locate/diin

Cognitive and human factors in digital forensics: Problems, challenges, and the way forward

Nina Sunde ^{a,*}, Itiel E. Dror ^b

^a University of Oslo, Norwegian Police University College, Norway
^b University College London, UK

Forensic Science International: Digital Investigation 37 (2021) 301075

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

ELSEVIER

journal homepage: www.elsevier.com/locate/fsidi

A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making

Nina Sunde ^{a,*}, Itiel E. Dror ^b

^a University of Oslo, Norwegian Police University College, Norway
^b University College London, UK

Science & Justice 61 (2021) 100–106

Contents lists available at ScienceDirect

Science & Justice

ELSEVIER

journal homepage: www.elsevier.com/locate/scjus

Original Research Article

What does a digital forensics opinion look like? A comparative study of digital forensics and forensic science reporting practices

Nina Sunde

Norwegian Police University College, Postboks 2109 Viks, 0123 Oslo, Norway

Forensic Science International: Digital Investigation 40 (2022) 301107

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

ELSEVIER

journal homepage: www.elsevier.com/locate/fsidi

Strategies for safeguarding examiner objectivity and evidence reliability during digital forensic investigations

Nina Sunde

University of Oslo, The Norwegian Police University College, Pb. 2109 Viks, 0125, Oslo, Norway

cogent social sciences

Cogent Social Sciences

Taylor & Francis

ISSN: (Print) (Online) journal homepage: <https://www.tandfonline.com/loi/qsas20>

Unpacking the evidence elasticity of digital traces

Nina Sunde

Opportunities

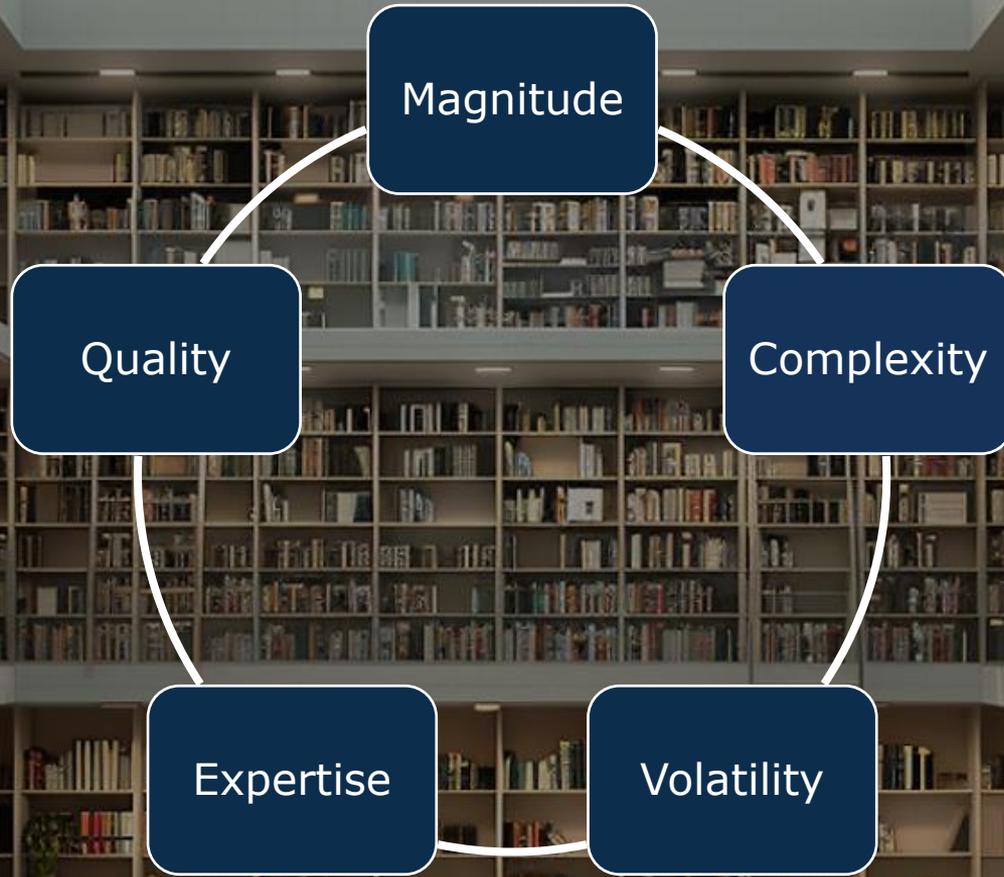
Everything we do leaves traces

- Large amounts of information are generated beyond the user's awareness and control

Digital traces can reveal:

- Activities, movements, and behavioural patterns
- Locations and timestamps
- Relationships, conversations, and communication patterns
- Thoughts, intentions, habits, and preferences





The New York Times

Flaws in Cellphone Evidence Prompt Review of 10,000 Verdicts in Denmark



Audience members holding up cellphones at a concert in Copenhagen. Errors in tracking data may have affected court cases in Denmark. Irfan Cemiloglu/Anadolu Agency, via Getty Images

By Martin Selsoe Sorensen
Aug. 20, 2019

NEWS

Confirmation bias led Post Office to prosecute subpostmasters without investigation, inquiry told

Former Post Office tech leader tells public inquiry that confirmation bias led to hundreds of subpostmasters being prosecuted for financial crimes without proper investigation



By Karl Flinders, Chief reporter and senior editor EMEA

Published: 03 Nov 2022 14:50

Post Office investigators were so convinced that subpostmasters were cooking the books that they failed to investigate alleged IT problems, a public inquiry has been told.

Speaking to the statutory public inquiry into the Post Office Horizon scandal, Jeremy Folkes, former senior tech lead at the Post Office, said there was an understanding in investigation teams that there were concerns over the accounting system integrity, but they ignored them.

ComputerWeekly.com

Which technologies will drive your roadmap in 2023



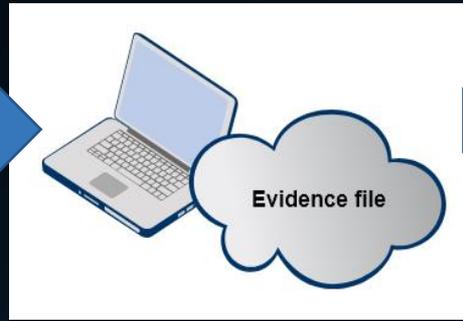
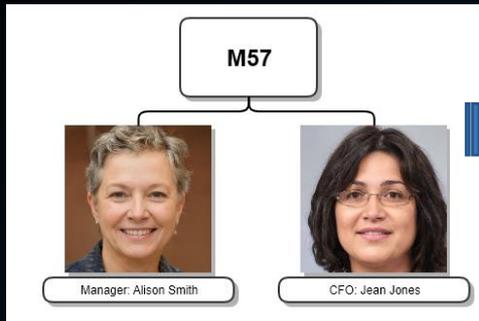
Take the survey

ComputerWeekly.com

IT PRIORITIES SURVEY

Which technologies will drive your

Latest News

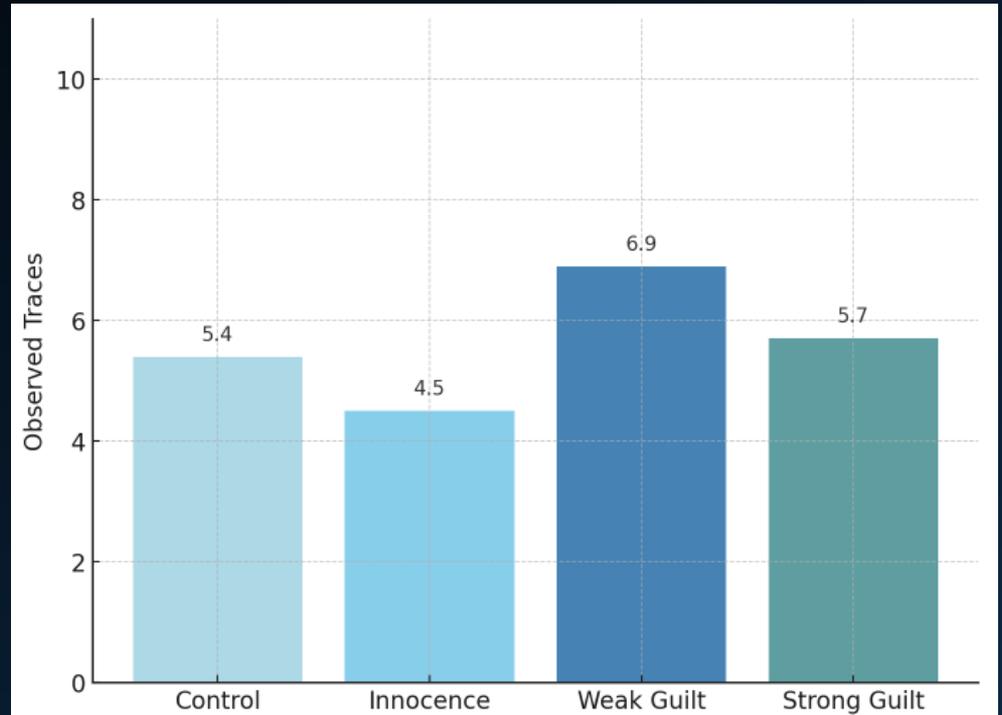


53 independent reports

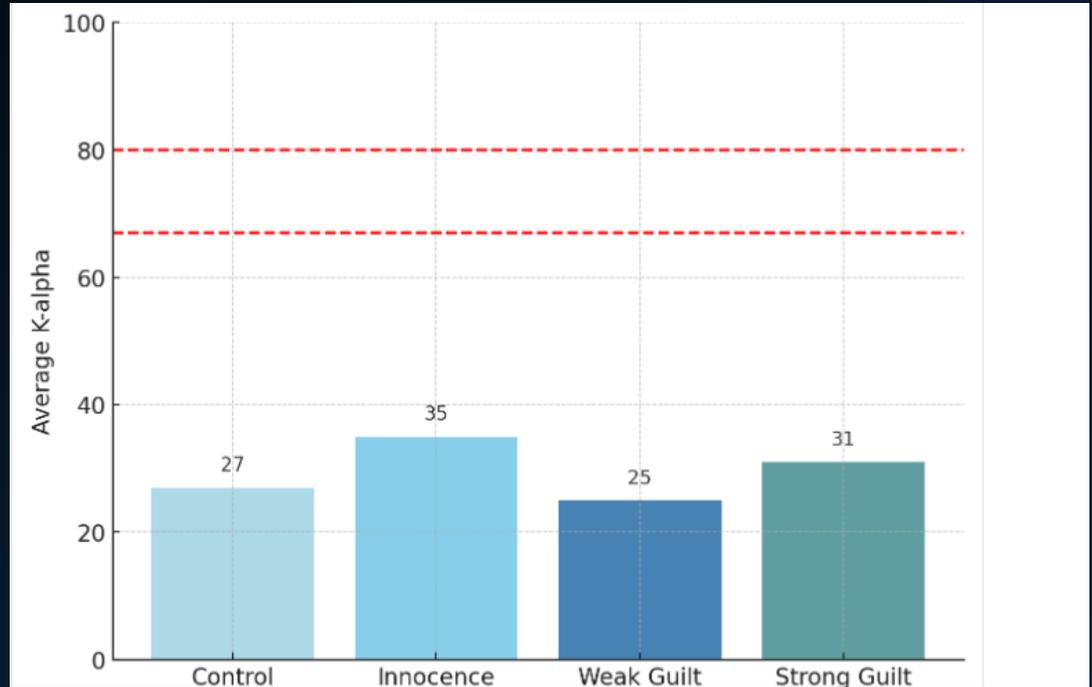
Bias and noise (reliability)



Biased observations due to task-irrelevant context



Between-examiner reliability (noise)



What happened?

- CFO fraud
- Phishing
- Spear phishing
- Hacking
- Leakage of confidential information
- No information was leaked

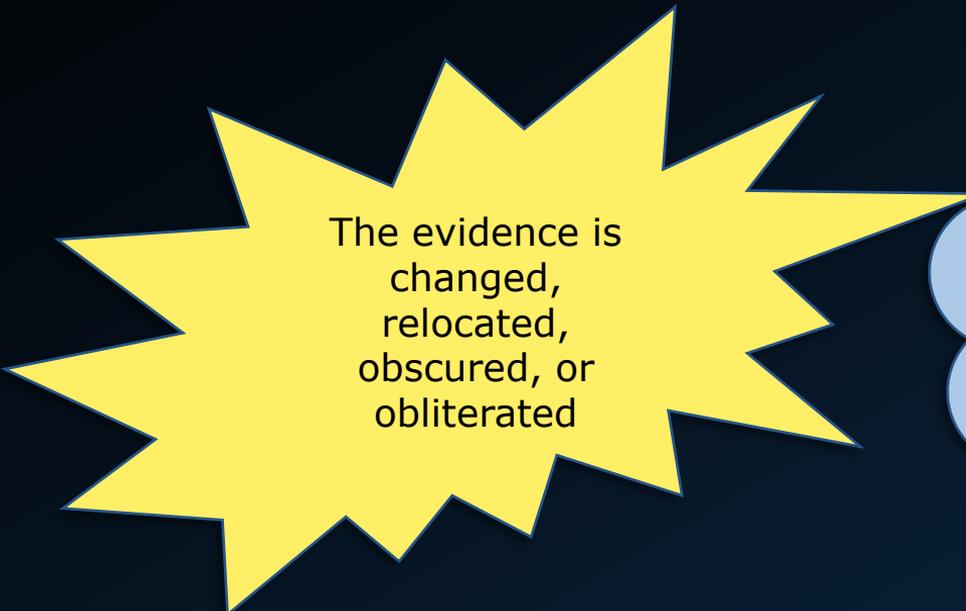
Who were involved?

- Jean (CFO)
- Alison (CEO)
- Carol (programmer)
- NN external
- NN internal

How did it happen?

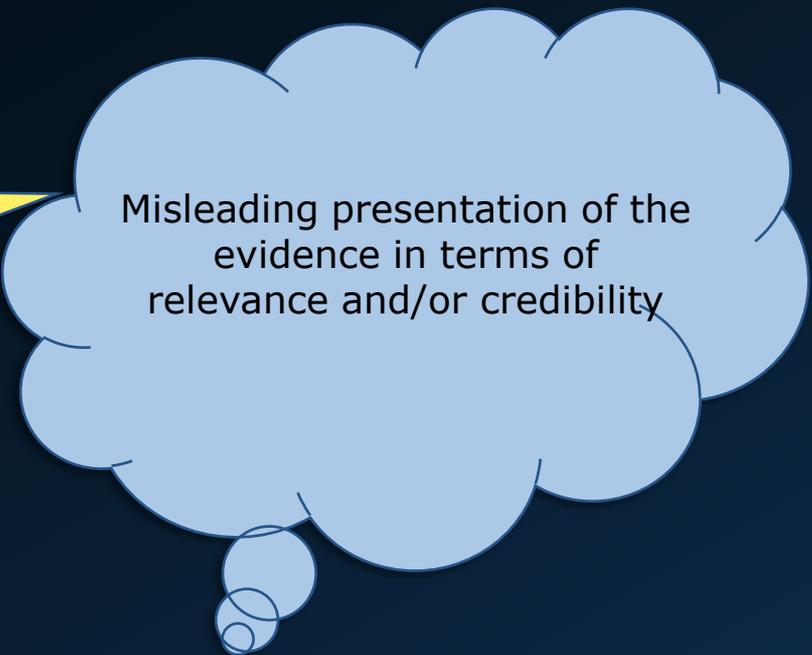
- Sent by email
- Copied to USB
- Stolen through hacking
- No information was leaked

Revis-dynamikk
Evidence dynamics

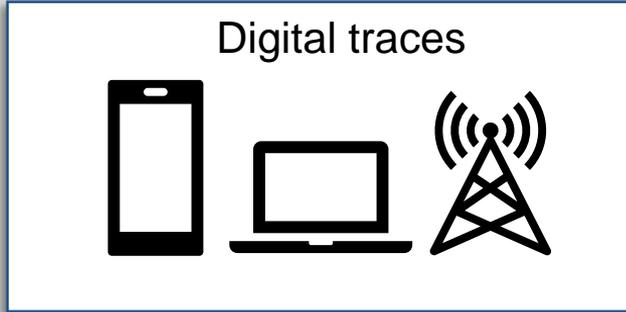


The evidence is
changed,
relocated,
obscured, or
obliterated

Evidence elasticity

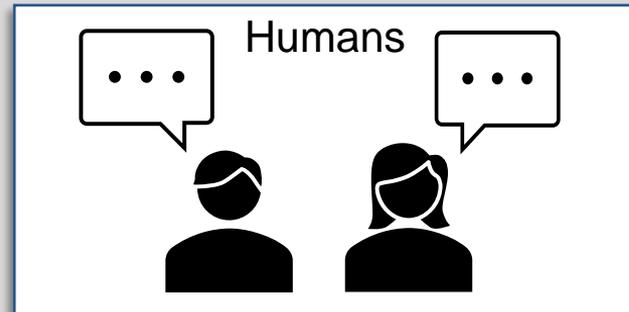


Misleading presentation of the
evidence in terms of
relevance and/or credibility



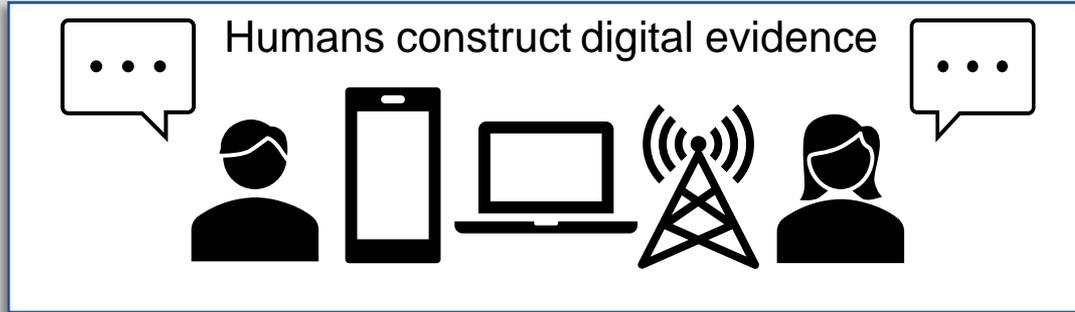
Objective
Value-neutral
Independent

Detailed, reliable, and accurate
Silent digital witness - 'Does not lie'



Subjective
Influenced by moral and emotions
Biased

Vulnerable cognitive processes may result
in inaccurate or erroneous accounts
May lie



Objective => Subjective

Value-neutral => Influenced by moral and emotions

Independent => Biased

Detailed, reliable, and accurate => Vulnerable cognitive processes may result in inaccurate or erroneous accounts

Silent digital witness - 'Does not lie' => May lie

**ELSEVIER**Contents lists available at [ScienceDirect](https://www.sciencedirect.com)**Science & Justice**journal homepage: www.elsevier.com/locate/scijus

Original Research Article

What does a digital forensics opinion look like? A comparative study of digital forensics and forensic science reporting practices



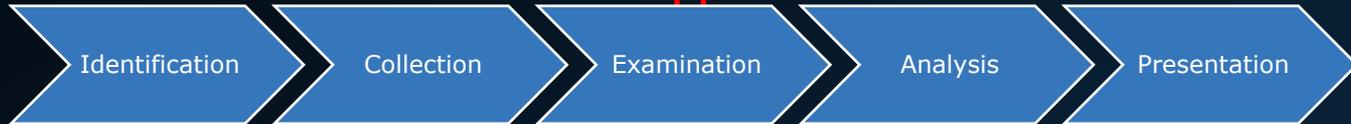
Nina Sunde

Norwegian Police University College, Postboks 2109 Vikta, 0125 Oslo, Norway

Accurate and complete description of the assignment:	52,5%
Accurate and complete description of context:	12,5%
Description of own competency/expertise:	5%
Accurate description of analysis tool/software:	57,5%
Description and explanation of time zone:	15%
Reliability of applied methods/tools:	0%
Accurate description of applied methodology:	17,5%
Explanation of applied technical terms:	15%

Quality assurance and quality control

Prevent

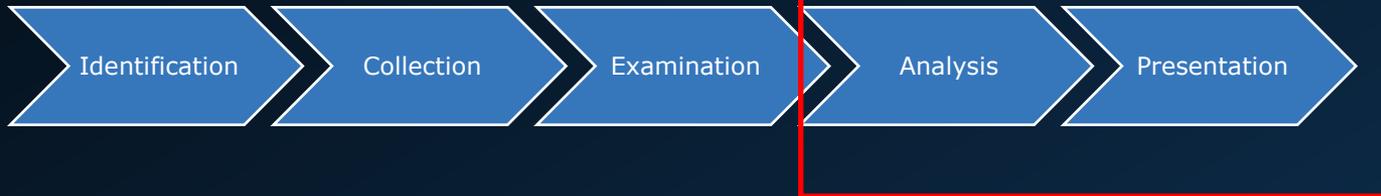
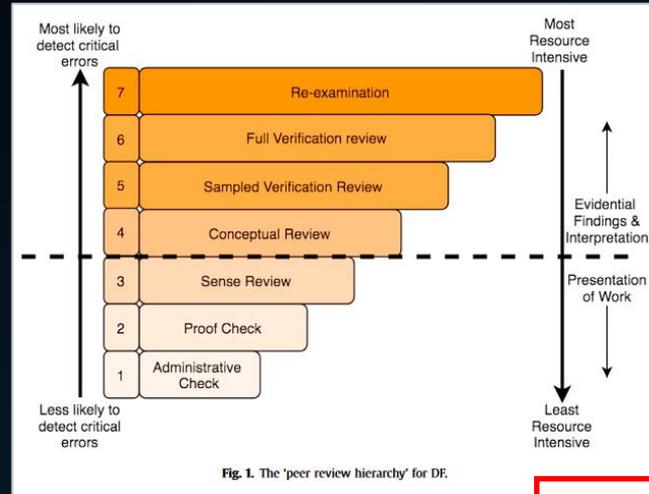


- Education and training
- Standardisation
- Validation of tools and methods
- Risk identification and management
- Bias mitigation measures

Detect and correct

- Peer review and verification
- External review

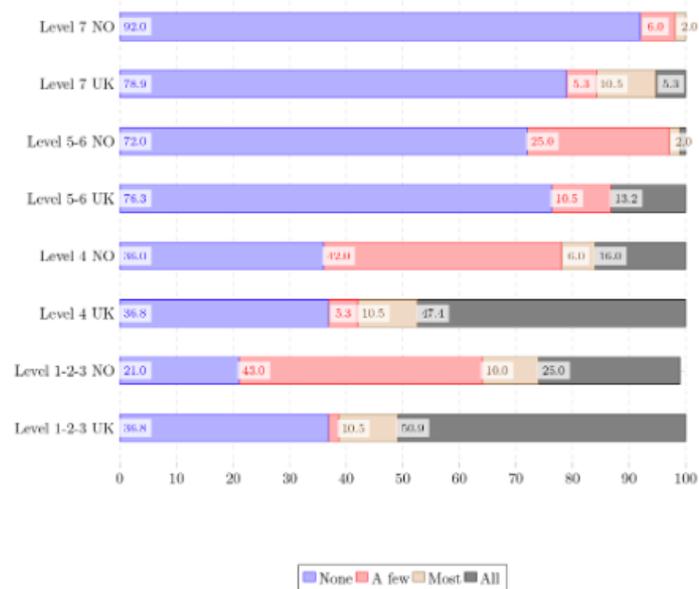
Quality control of reported findings



Evaluating the Scope of Peer Review in Digital Forensics: Insights from Norway and the U.K (under peer review)

- Comparative study by E. Ryser, R. K. Bauge, N. Sunde, and G. Horsman
- If any quality control is conducted, it is typically limited to a review of the report
- Only a small proportion of digital forensic findings are subject to verification

Figure 14: % Practitioners (NO (n=50)/UK (n=19)): Nb of quality control performed in the last 12 months



Summary

- Digital evidence should not be presumed to be objective, value-neutral or inherently reliable
- Bias and noise present challenges in digital forensic examinations
- Digital evidence may be flawed due to both the dynamics of evidence and its elasticity
- Transparency and auditability in digital forensic investigation practices are essential for error mitigation and continuous improvement





Thank you for your attention!
Nina.Sunde@phs.no

Literature

Sunde, N. & Dror, I. E. (2021). A Hierarchy of Expert Performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making. *Forensic Science International: Digital Investigation*, 37, 301175.

<https://doi.org/10.1016/j.fsidi.2021.301175>

Sunde, N. (2021). What does a digital forensics opinion look like? A comparative study of digital forensics and forensic science reporting practices. *Science & Justice*, 61(5) 586-596.

<https://doi.org/10.1016/j.scijus.2021.06.010>

News articles

- [Flaws in Cellphone Evidence Prompt Review of 10,000 Verdicts in Denmark - The New York Times \(nytimes.com\)](https://www.nytimes.com/2021/08/18/us/politics/cellphone-evidence-denmark-10000-convictions.html)
- [Confirmation bias led Post Office to prosecute subpostmasters without investigation, inquiry told | Computer Weekly](https://www.computerweekly.com/News/Confirmation-bias-led-Post-Office-to-prosecute-subpostmasters-without-investigation-inquiry-told)

Academy of European Law

Examination of digital devices

Tallinn, 2024

Anna ILLAMAA, anna.illamaa@gmail.com

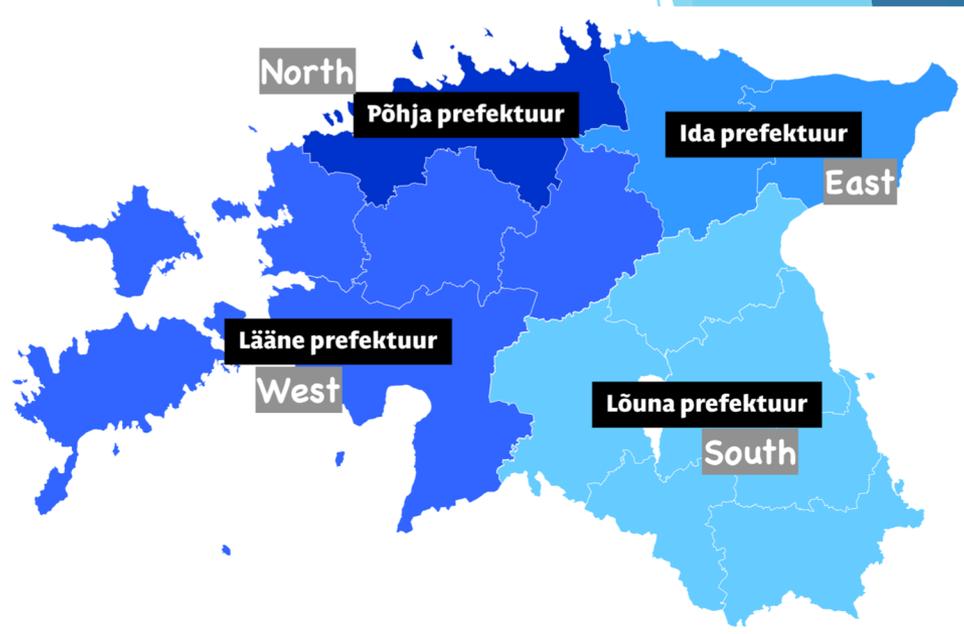


Co-funded by
the European Union

Anna ILLAMAA

National Criminal Police

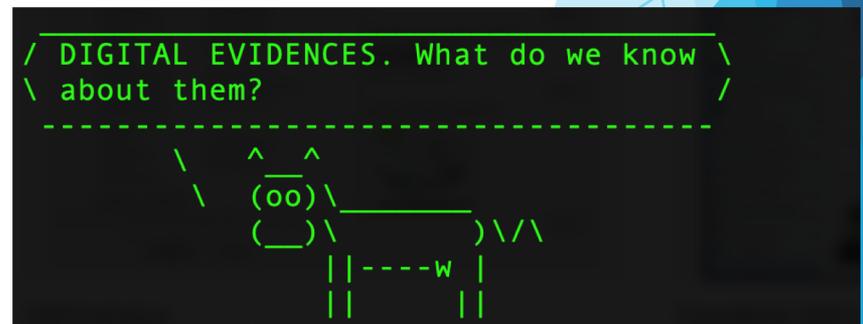
Forensics examiner



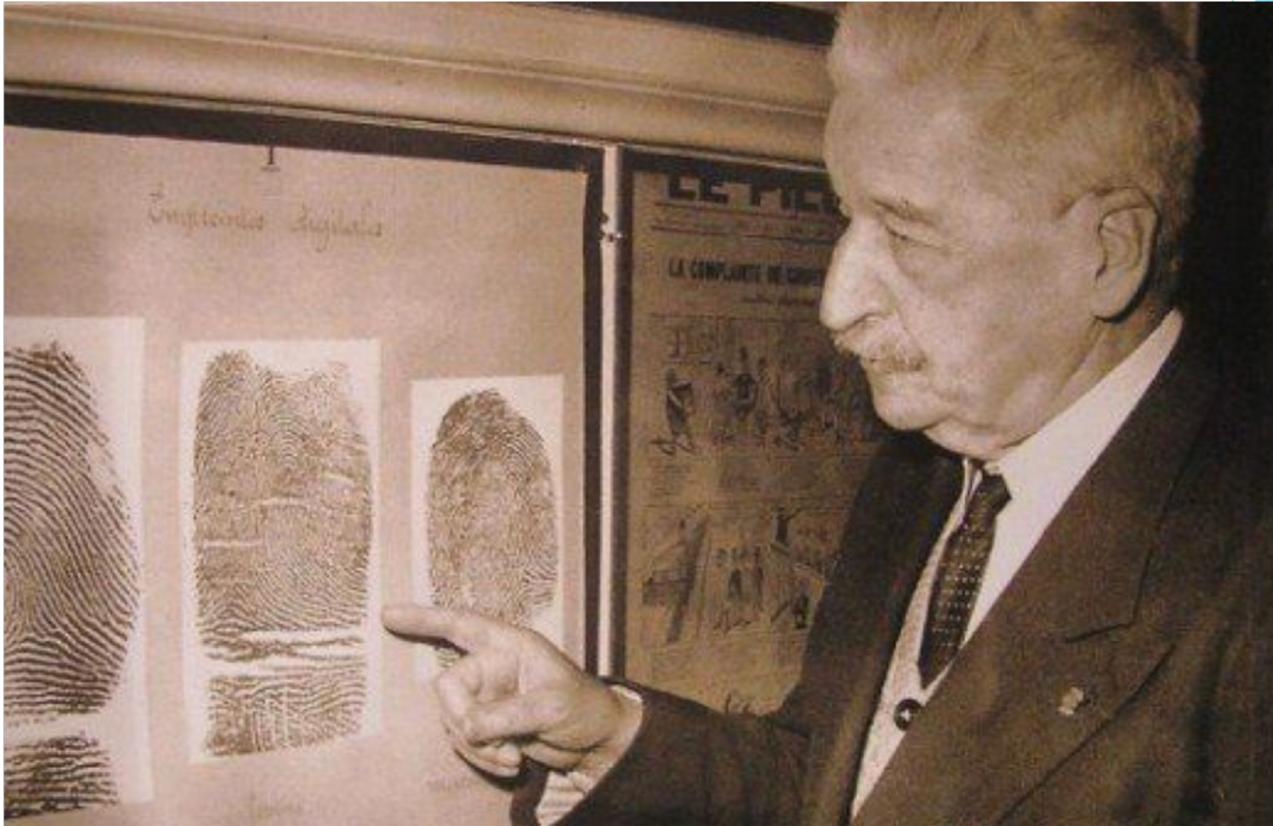
Estonian Police
and Border Guard Board

Objectives

- ▶ Digital evidences handling
 - ▶ Methodology
 - ▶ Chain of custody
- ▶ Windows, macOS, Linux artefacts
 - ▶ File systems



Edmond Locard, Sherlock Holmes of France



“Every contact leaves a trace”

Role of Expert

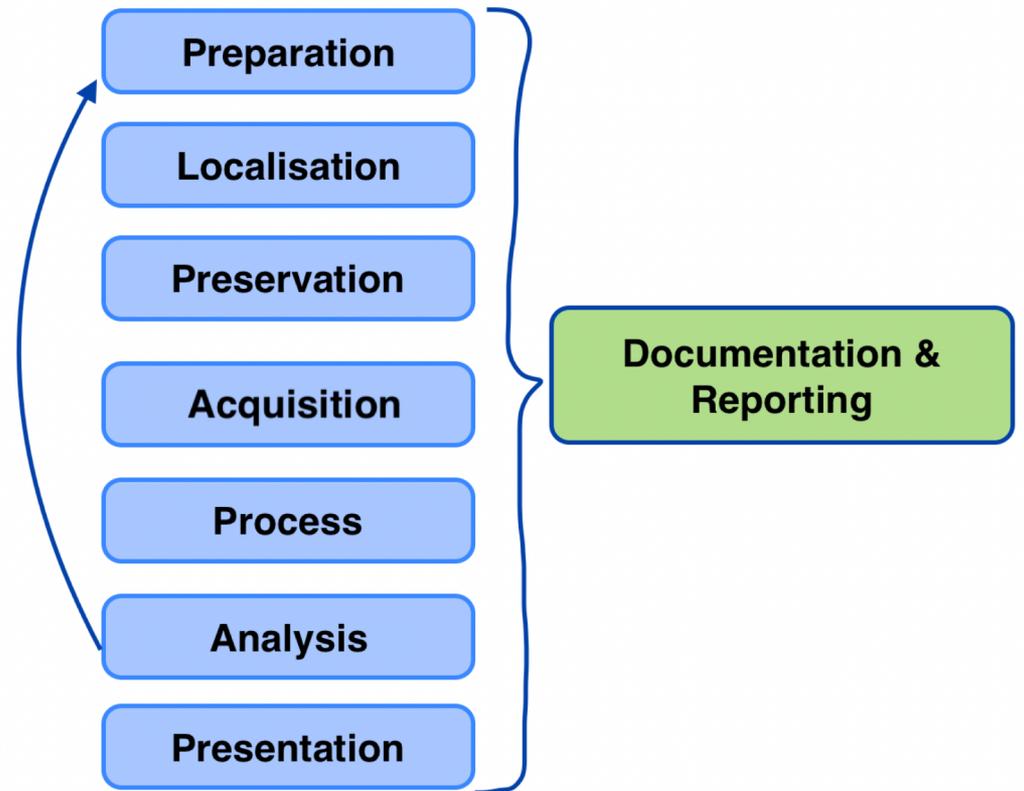
- To collect, to analyse, to preserve, to document the data in accurate and trustworthy way
- To Be objective (avoid confirmation bias)
- To update knowledge base

Forensics examiners are experts and not a court

Methodology

Overall Methodology:
one size fits all-
solutions

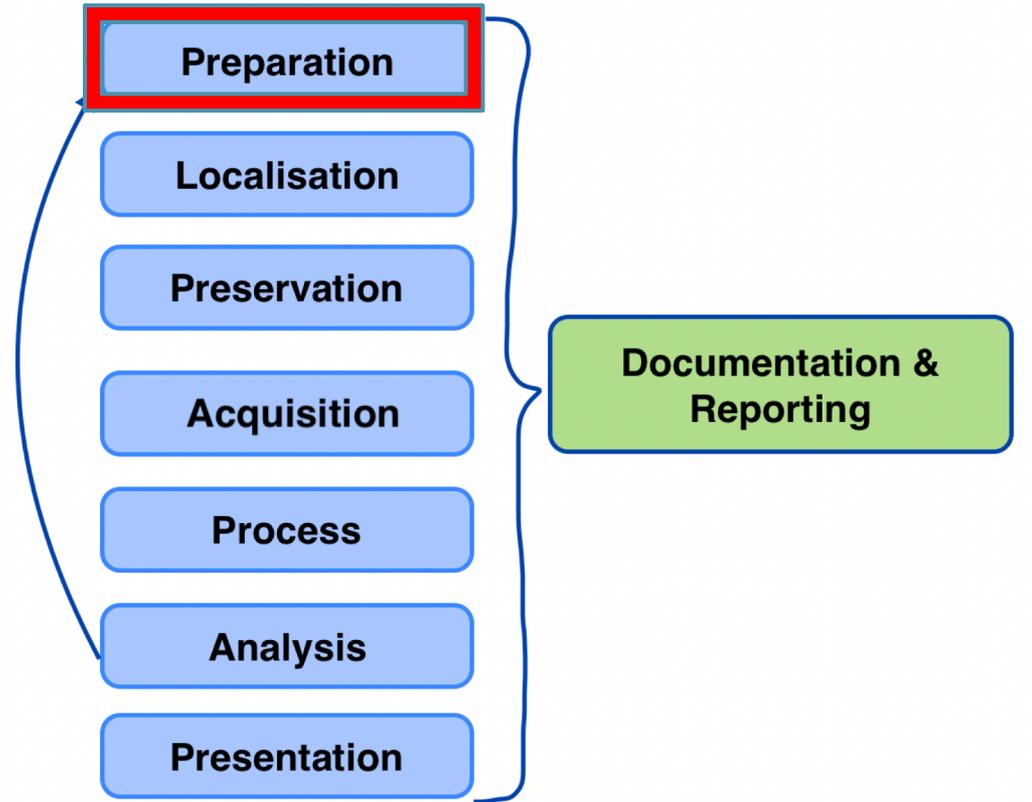
*What is the idea of the
methodology in the eye
of Law?*



Preparation

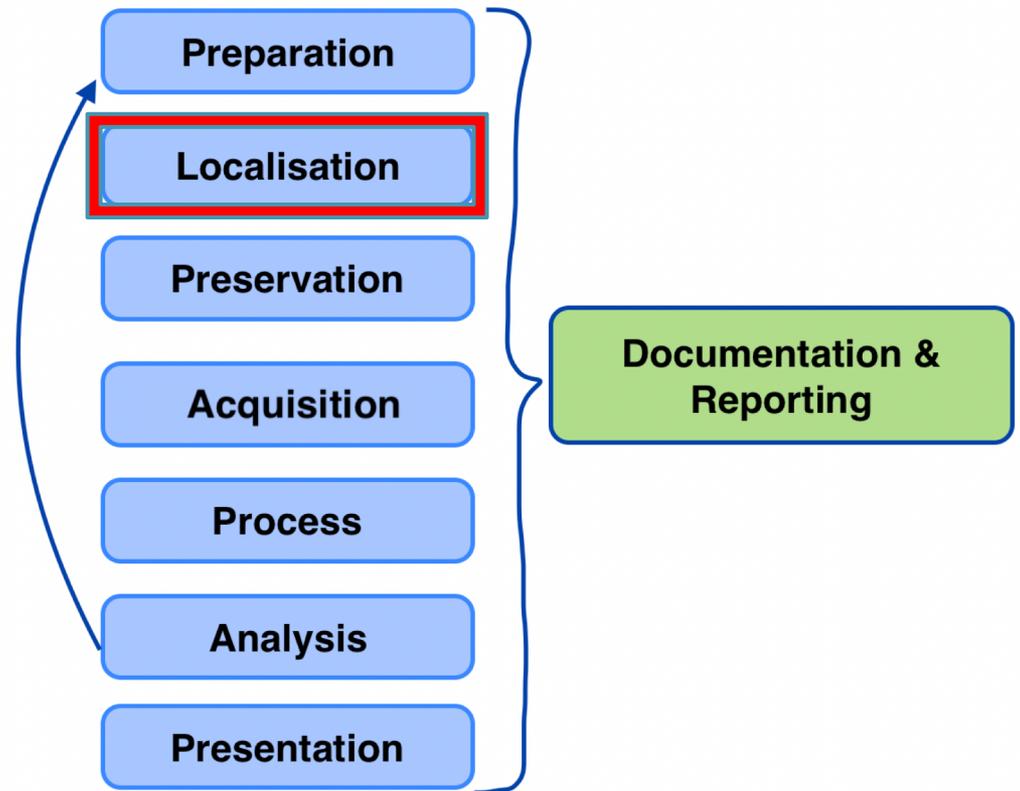
Case dependent

- *Tools*
- *Media*
- *Software*
- *Hardware*



Localisation

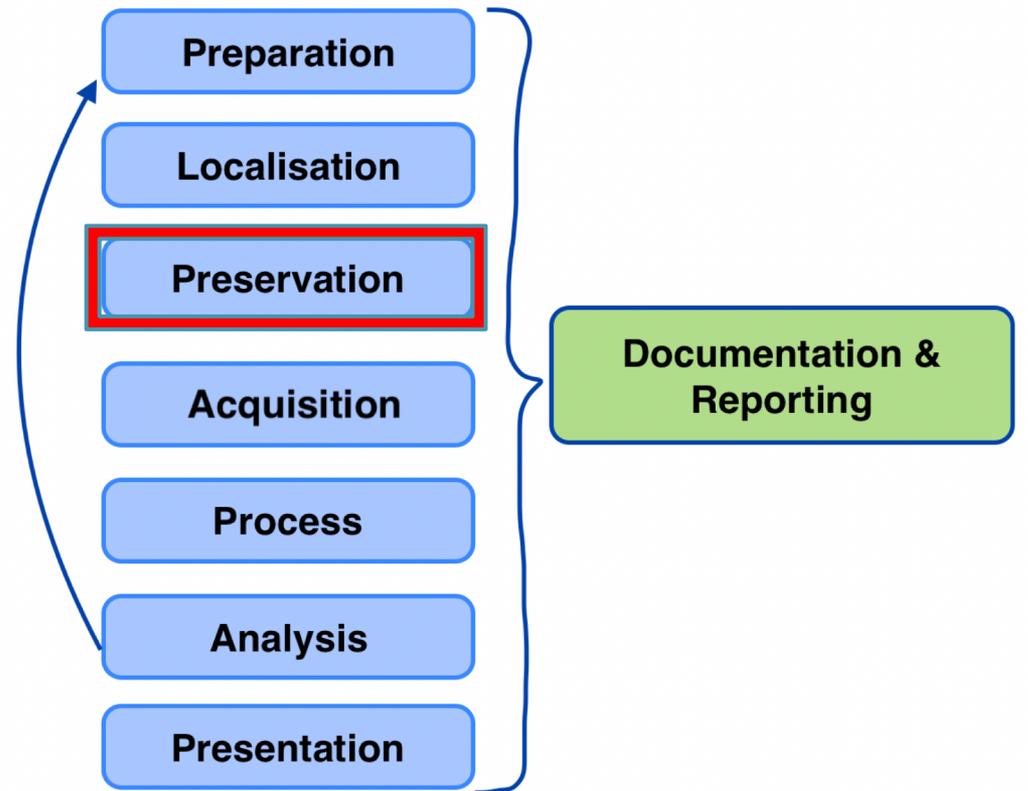
- *Where you have found the devices*
- *Circumstances*
- *Taking pictures or video*



Preservation

- *Packaging*
 - physical shock and electromagnetism
- *Tagging*

This is the starting point of the *Chain of Custody*!



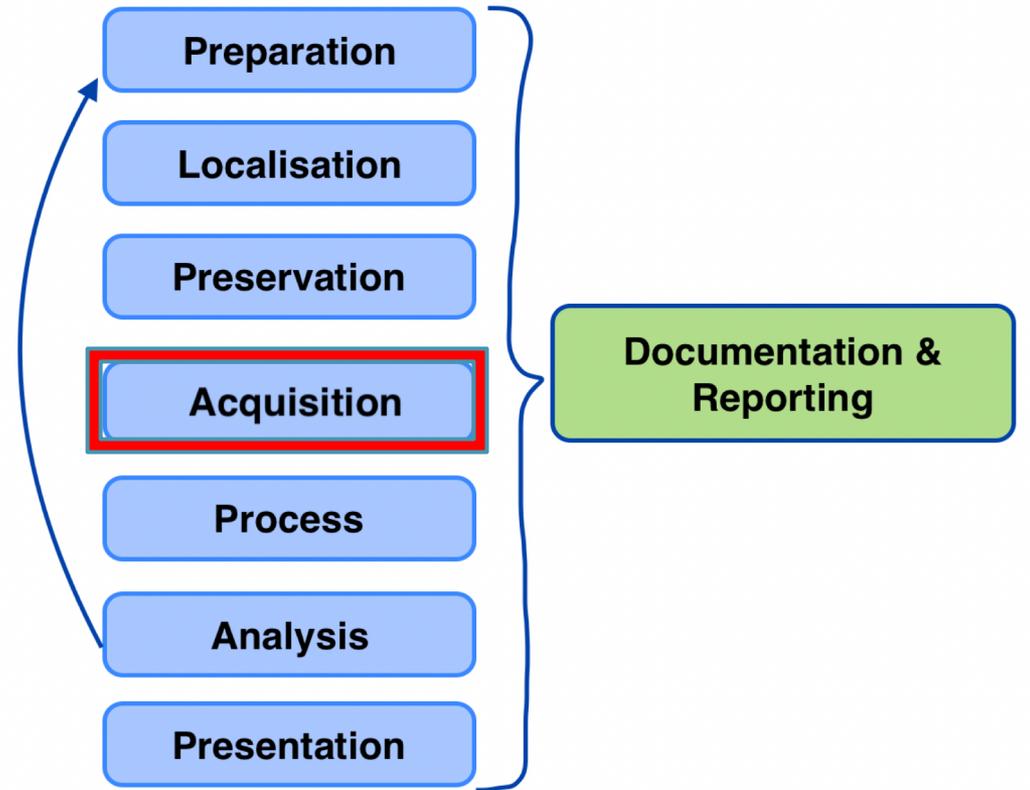
Acquisition

Aka <disk imaging>

- *at the crime scene*
- *in a forensic lab*

Needs:

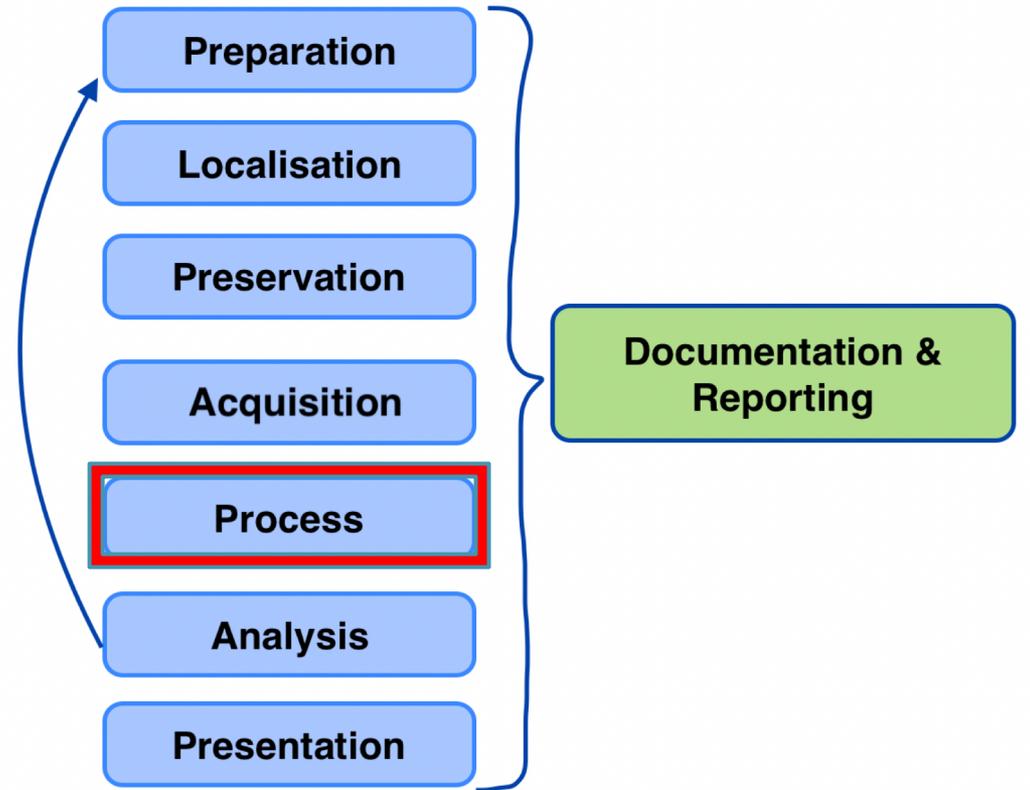
- *software*
- *hardware*



Process

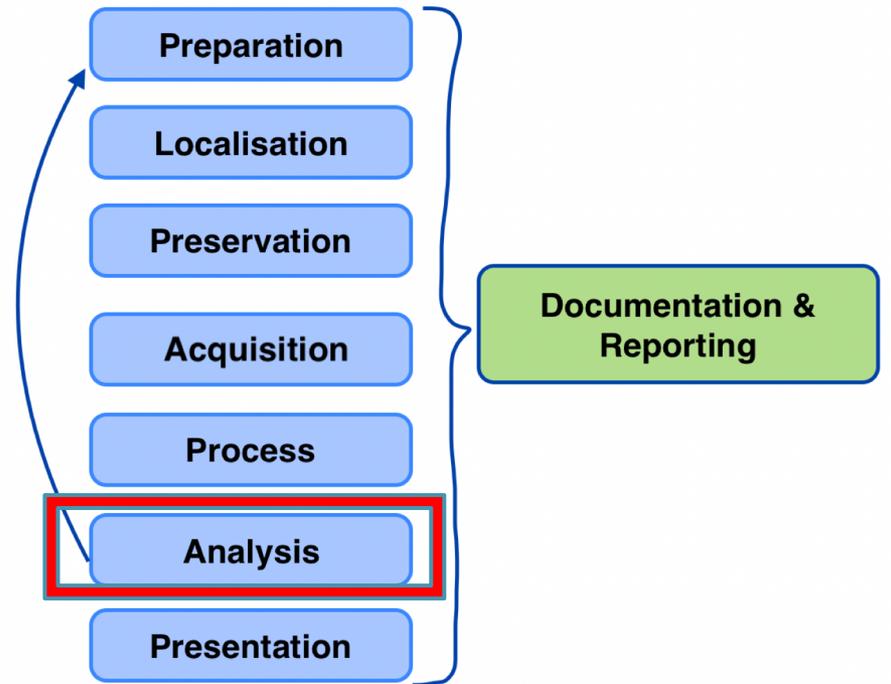
last preparations before analysis

- *Decrypting*
- *Recovering*
- *Extracting*



Analysis

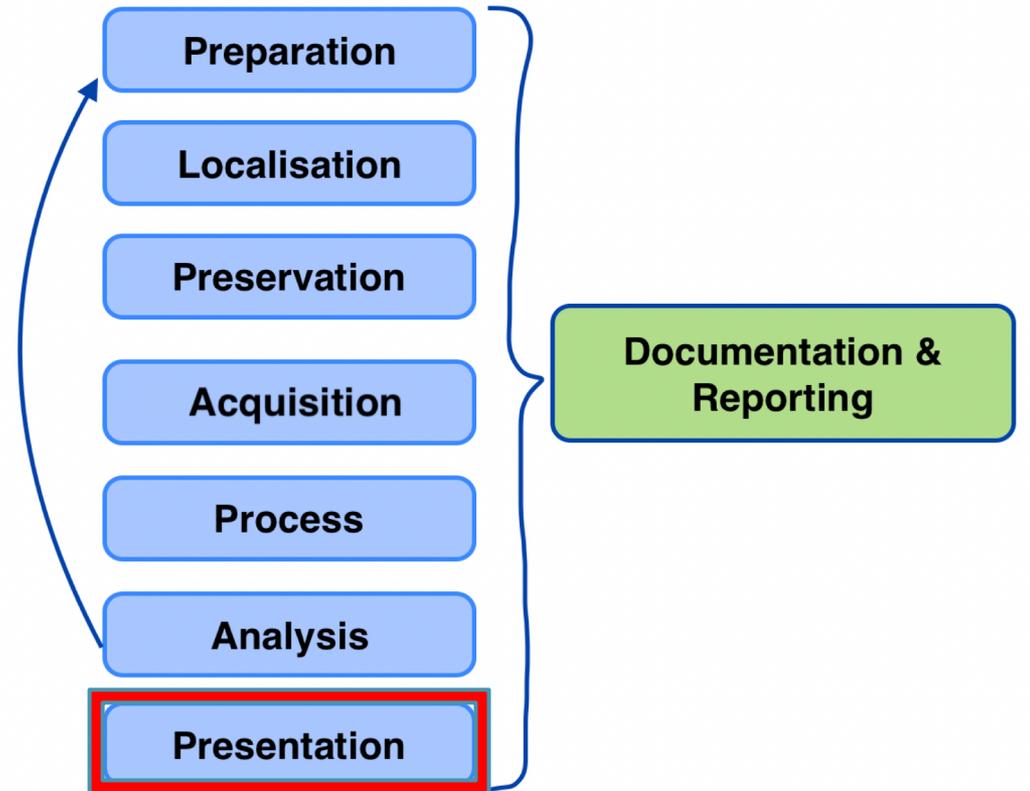
- *open mind*
- *Evidence(s) which not only proves guilt of a suspect, but also the evidence which proves innocence*
- *verification*



Presentation

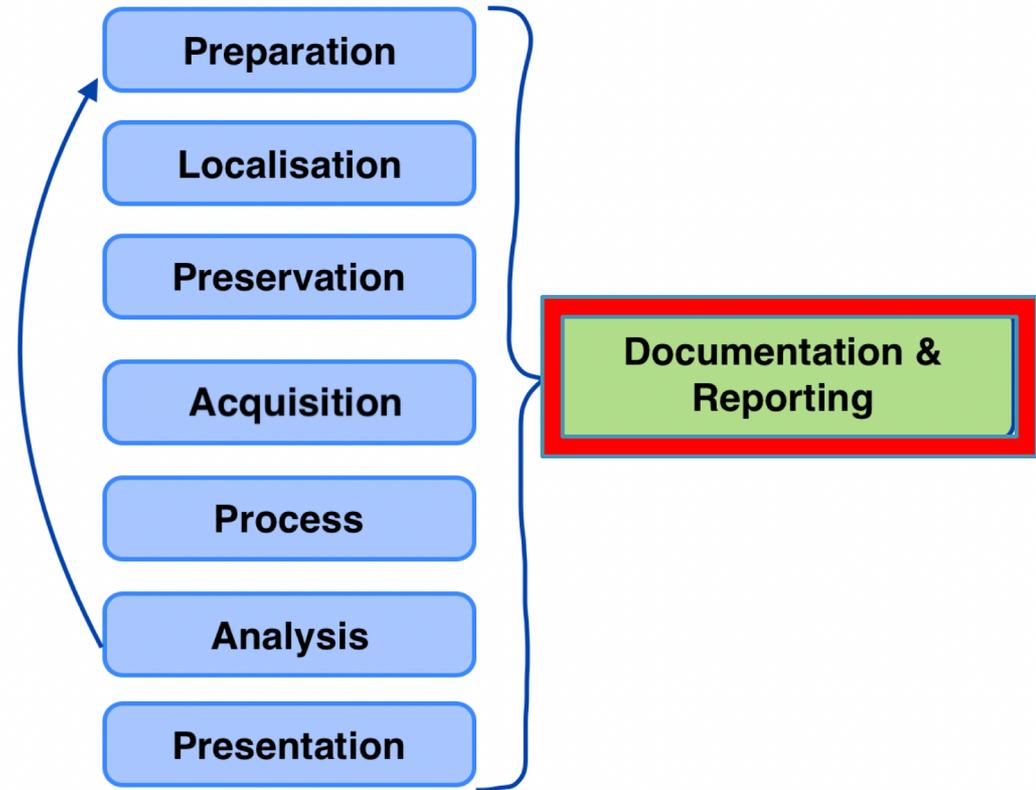
Report

- *layman language*
- *open and clear*

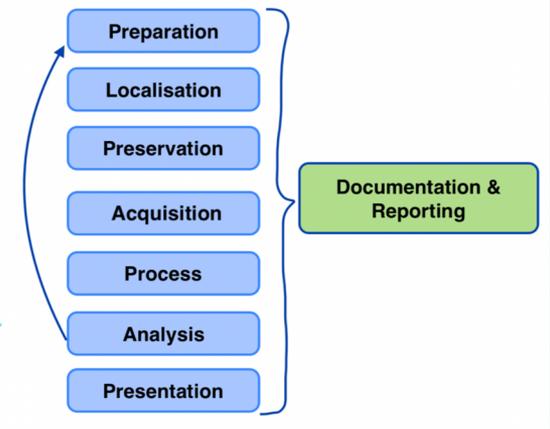
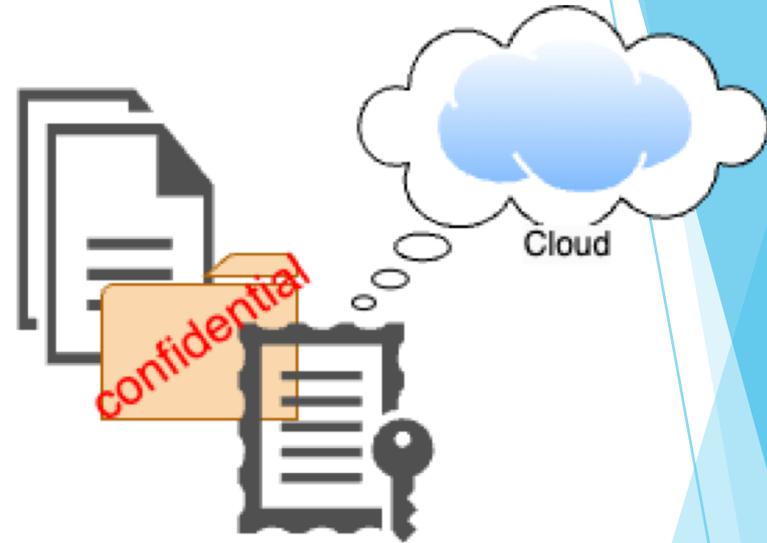


Documentation

- *Integration into the process*
- *During the all stages*
- *Recreation of process and findings*



CASE STUDY. Leaked Data



Hashing

- It can't be predicted
- no two files can have the same hash value
- if the file changes, the hash value changes



SHA1:
4e1243bd22c66e76c2ba9eddc1f91394e57f9f83



SHA1:
4a4d9ae5e92c369e257c529900ae3f7ff54a7cf4

CASE. Leaked Data

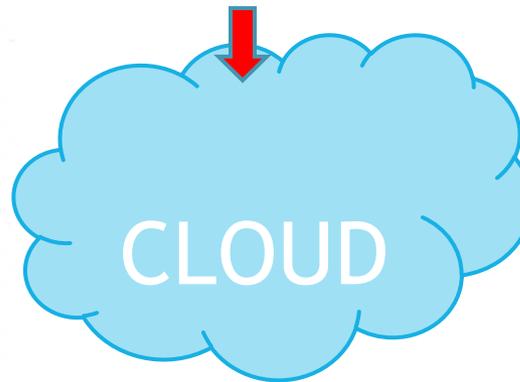
```
Desktop -- -sh -- 45x30
AnNa:Desktop anna$ cat hash-suspect.txt
0956b2989a3e88669555c592faa48ec6
1807fe5c8108aa592a70eecd8b8b5257
1807fe5c8108aa592a70eecd8b8b5257
31878974e481d77c57d7445b84c3bedb
3588126fc7d10f1ec9d01be5e39fc270
517e38aadd2b7474e4ffa65fcec04407
54f88e55d79cfc7c8b6bc02e5e877b9f
5bddc1a2b988d793f3faafba0ff7d070
6f268e6bf93fcdcb834b0c945af488ba
6f268e6bf93fcdcb834b0c945af488ba
80d975967f679ebd98e22eb6afdfa780
858560be6f41ab2fd3fd4e15b4e0a4c5
858560be6f41ab2fd3fd4e15b4e0a4c5
8ef72d742a0884b3f9dd07b3dbe7bdb5
942a5ab50592a2c9092d3e937826831b
956467dac1b079dd7db3e5e6e28c77f2
9dc21e3a8497ac3e229c991bace64e92
a5d5d09934d0a84c5e96634cb9d53f36
a6e4a88382159a53a4e12526fe0c73b6
a6e4a88382159a53a4e12526fe0c73b6
abd496f5aafba4bac60dfe53cc41f0bc
c382ad3b0d05ce31030c8612227c09f6
cf375cab8c7325dc136d2be579d63c0a
d4ebe4da7c348a99f2b880d2fb7db430
de35d7e32a10113c762fce6de478cead
f6a17058c00f08a5db6d10f1de7d31a4

Desktop -- -sh -- 48x24
AnNa:Desktop anna$ cat hash-leaked.txt
5dd581b448648ca8cba4398c00844588
6f268e6bf93fcdcb834b0c945af488ba
858560be6f41ab2fd3fd4e15b4e0a4c5
b636536fe08fccb67d040c4d4ab1f4f8
AnNa:Desktop anna$

Desktop -- -sh -- 61x13
AnNa:Desktop anna$ comm -12 hash-suspect.txt hash-leaked.txt
6f268e6bf93fcdcb834b0c945af488ba
858560be6f41ab2fd3fd4e15b4e0a4c5
AnNa:Desktop anna$
```

Sources of Digital Evidence

Physical Devices - Data related to a person - Other



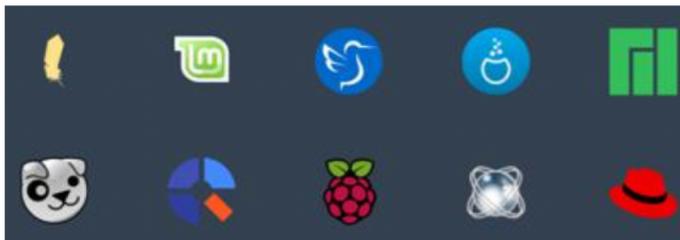
Operating system

- is the main controlling software between the computer hardware and the user

- Windows
- macOS
- Linux/Unix



source: www.edureka.co



source: www.uhacc.org



source: www.deepakkeswani.com

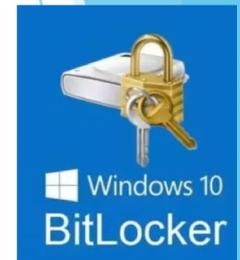
Operating System Forensics

- is a process of retrieving data from the Operating System (OS) of the computer or mobile device in question.
- *(source: www.infosecinstitute.com)*
- the aim of data collecting is to locate and acquire important information for the case.
- we have to remember, that acquired data may prove or disprove crime and the task of forensics examiner is to establish the facts and not assumptions.

Encryption as a challenge

- *Level of encryption:*
 - *Full disk*
 - *Partition(s)*
 - *File(s)*

No access to the data, but data exists!



LUKS
Linux Unified Key Setup

Encrypting Drives in Linux

CASE STUDY. BitLocker

BitLocker

Enter the PIN to unlock this drive

Use the number keys or function keys F1-F10 (use F10 for 0).

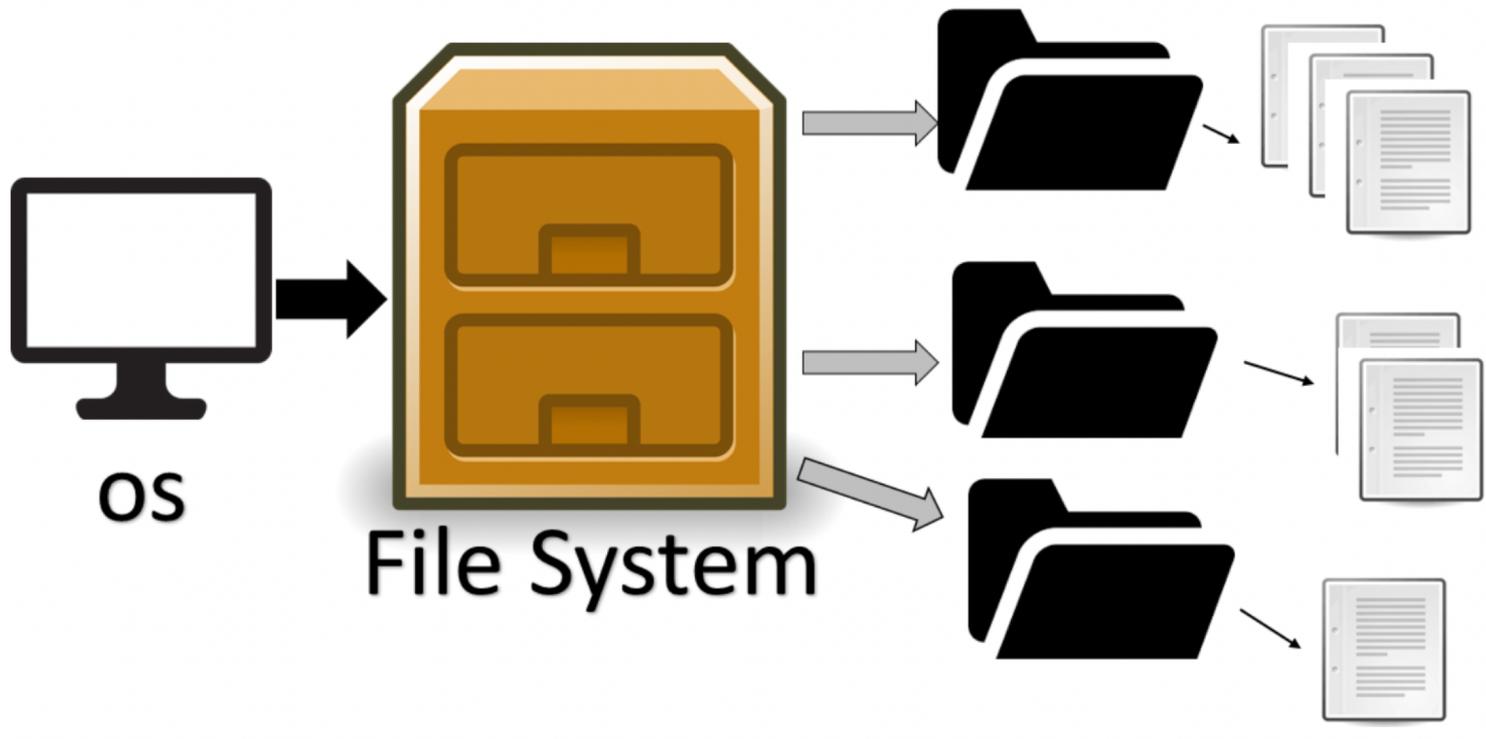
Press the Insert key to see the PIN as you type.



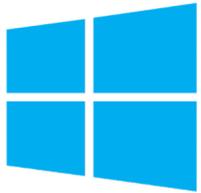
PASSWORDS

File System

- is a method of organizing files on physical media, such as hard disks, CD's, and flash drives



File System



Windows OS



NTFS

FAT32

exFAT



macOS



HFS+

APFS

FAT32

exFAT



Linux/Unix OS

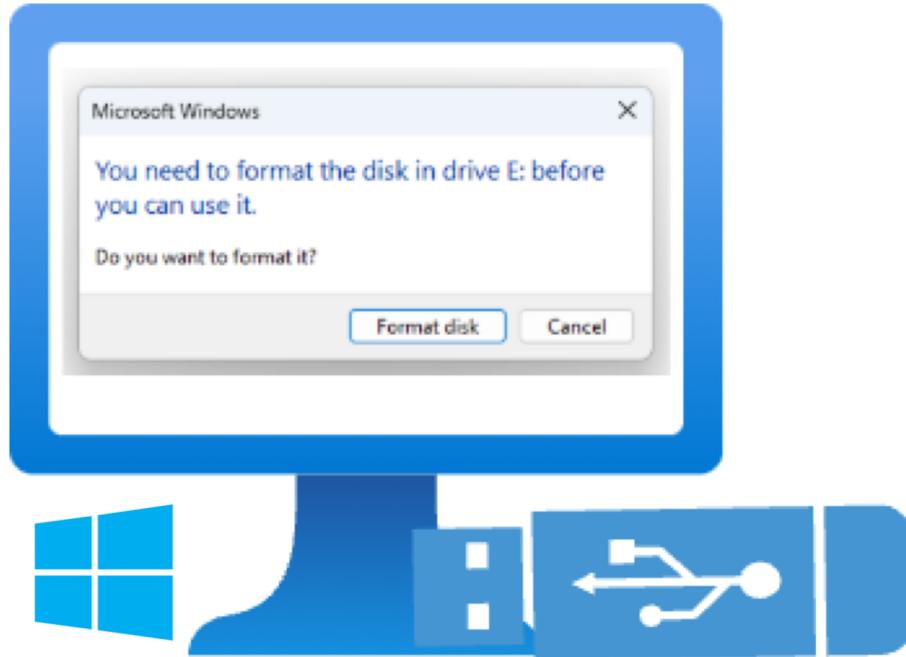


ext 2/3/4

FAT32

exFAT

CASE STUDY. File System/Operating System



Model General UDisk (5.00)
Serial Number 1608180115351100853102
Size 1.0 GB (1006632960 bytes)
Partitioning Master Boot Record

Volumes

no-name
Partition 1
1.0 GB Ext4

Size 1.0 GB — 972 MB free (3.5% full)
Contents **Ext4** (version 1.0) — Mounted at [/media/parallels/no-name](#)
Device /dev/sdb1
UUID F5dc6d4a-597e-4fef-87da-bf7df43e469b
Partition Type Linux (Bootable)



Forensics Artifacts

- are objects that have forensic value

- PerfLogs
- Program Files
- Program Files (Arm)
- Program Files (x86)
- ProgramData
- Recovery
- RM2 Template Helper
- tmp
- tmp_core
- tmp_directory
- Users
- Windows

- .file
- .vol
- .Volumelcon.icns
- Applications
- bin
- cores
- etc
- home
- Library
- opt
- private
- sbin
- System
- tmp
- Users
- usr
- var
- Volumes

- > bin
- > boot
- > dev
- > etc
- > home
- > lib
- > lost+found
- > media
- > mnt
- > opt
- > proc
- > root
- > run
- > sbin
- > snap
- > srv
- > sys
- > tmp
- > usr
- > var

Forensics Artifacts

- are objects that have forensic value

- PerfLogs
- Program Files
- Program Files (Arm)
- Program Files (x86)
- ProgramData
- Recovery
- RM2 Template Helper
- tmp
- tmp_core
- tmp_directory
- Users
- Windows



- .file
- .vol
- .Volumelcon.icns
- Applications
- bin
- cores
- etc
- home
- Library
- opt
- private
- sbin
- System
- tmp
- Users
- usr
- var
- Volumes



- > bin
- > boot
- > dev
- > etc
- > home
- > lib
- > lost+found
- > media
- > mnt
- > opt
- > proc
- > root
- > run
- > sbin
- > snap
- > srv
- > sys
- > tmp
- > usr
- > var



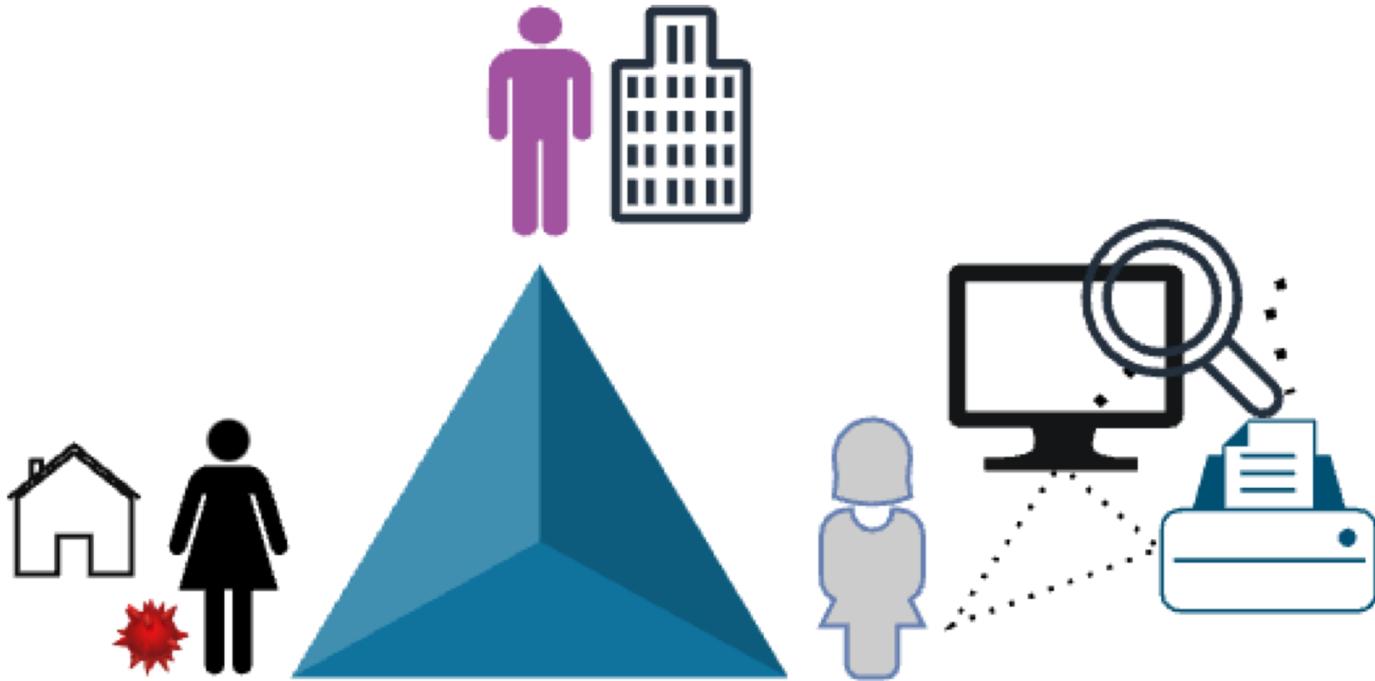
Forensics Artifacts

- are objects that have forensic value



Windows	macOS	Linux
Recycle Bin	Trash	Trash
Recent	plist	User account information
Registry	DS_Stores	App configuration
Thumbs.db	FSEvents	App and security logs
Print Spooling		

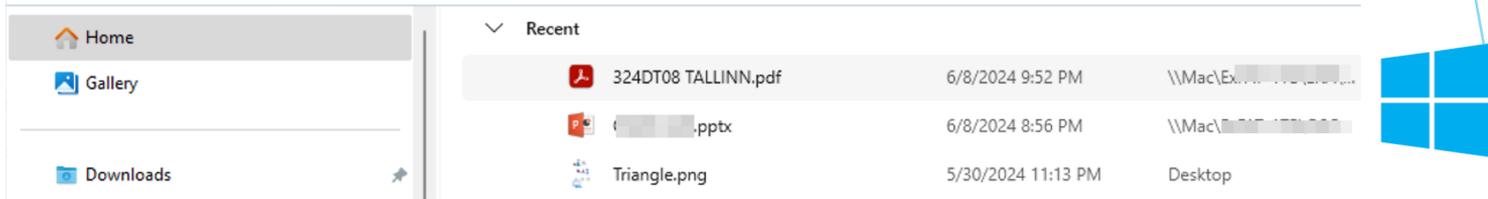
CASE STUDY. Artifacts



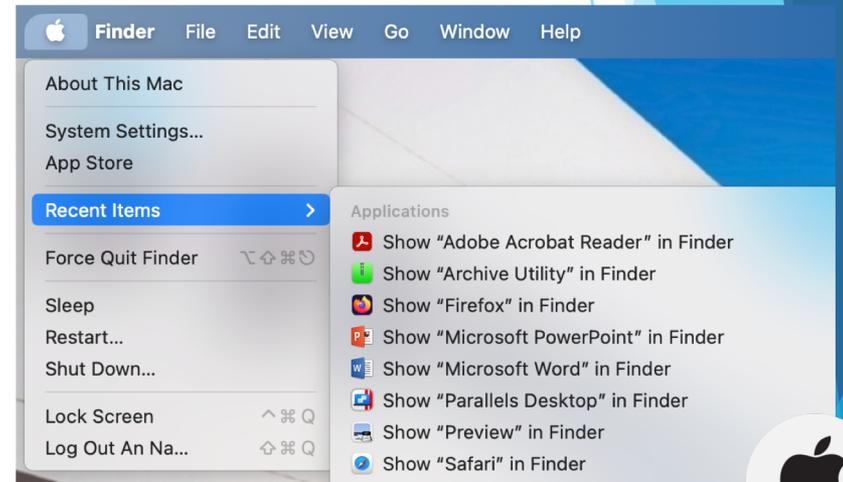
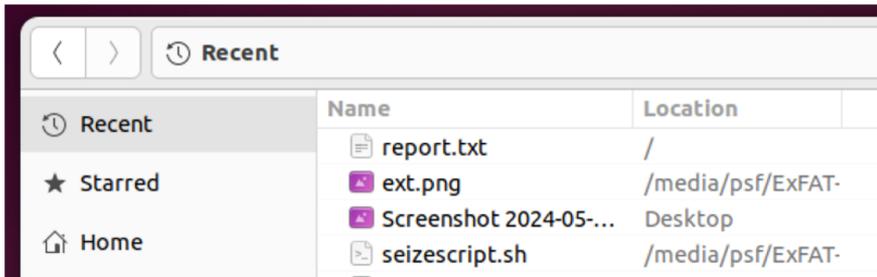
Forensics Artifacts

User Recent Documents:

`\Users\<<Username>\AppData\Roaming\Microsoft\Windows\Recent\`



`~/ .local/share/recently-used.xbel`



`~/Library/Preferences/com.apple.finder.plist`

Forensics Artifacts



The screenshot shows the Windows Event Viewer interface. The left pane shows the 'System' log selected under 'Windows Logs'. The main pane displays a list of events filtered by the criteria: 'Log: System; Source: ; Event ID: 6005,6006,4624,4634'. A 'Filter Current Log' dialog box is open, showing the 'Filter' tab with the 'Includes/Excludes Event IDs' field containing the text '6005,6006,4624,4634'. The 'Actions' pane on the right shows the 'Filter Current...' option highlighted.

Level	Date and Time	Source	Event ID	Task Category
Information	3/18/2024 10:14:57 PM	EventLog	6006	None
Information	3/18/2024			
Information	9/24/2024			
Information	9/20/2024			
Information	9/19/2024			
Information	9/19/2024			
Information	9/19/2024			

Event 6006, EventLog

General Details

The Event log service was stopped.

Log Name: System
Source: EventLog
Event ID: 6006

Filter Current Log

Filter XML

Logged: Any time

Event level: Critical Warning Verbose
 Error Information

By log: Event logs: System

By source: Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

6005,6006,4624,4634

Task category:

Keywords:

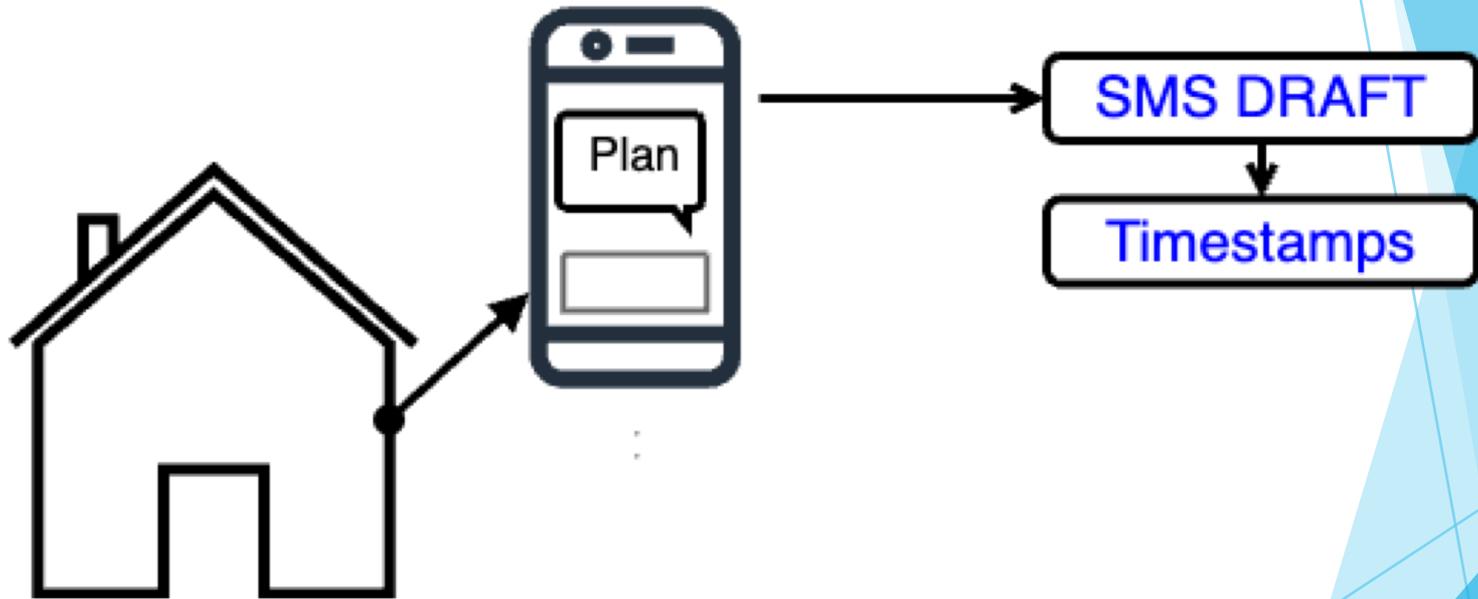
User: <All Users>

Computer(s): <All Computers>

Clear

- Event ID 6005: The event log service was started (system startup).
- Event ID 6006: The event log service was stopped (system shutdown).
- Event ID 4624: An account was successfully logged on.
- Event ID 4634: An account was logged off.

CASE STUDY. Artifacts



CASE STUDY. Continue

What could be done differently?

- Transport to the LAB asap
- Documentation on the place

We have discussed:

- Methodology
- Sources of digital evidences, handling, chain of custody
- OS, FS and artifacts
- Hashing
- Cases
- Questions?



**Thank you for your
attention!**

Anna ILLAMAA, anna.illamaa@gmail.com

The e-evidence package

New EU rules to improve cross-border access to electronic evidence

Post-covid challenges in criminal justice: investigating web 2.0,
Tallinn, 20-21 June 2024

The e-evidence package in a nutshell

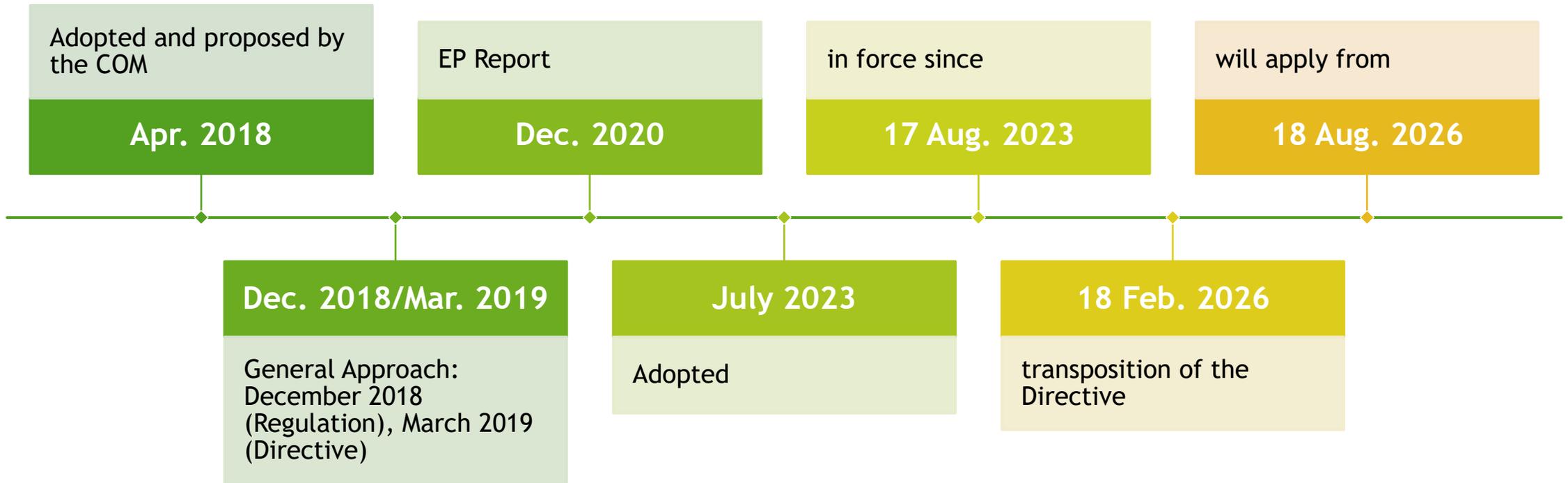
Regulation

procedural instrument; new form of judicial cooperation: directly sent to the addressee/service provider (SP) in another MS

Directive

to ensure a level playing field
all SPs offering services in the EU need to designate a “designated establishment” or “legal representative”

Timeline



Directive

- Obliges SPs (offering services in the EU):
 - if established (entity with economic activity and legal personality) in the EU: at least one „**designated establishment**“
 - if not established in the EU: at least one „**legal representative**“
- both must be **equipped with the legal and factual powers** needed to comply with (national and cross-border) decisions and orders sent to them as addressees for **gathering of electronic evidence**; not limited to the e-evidence
Regulation

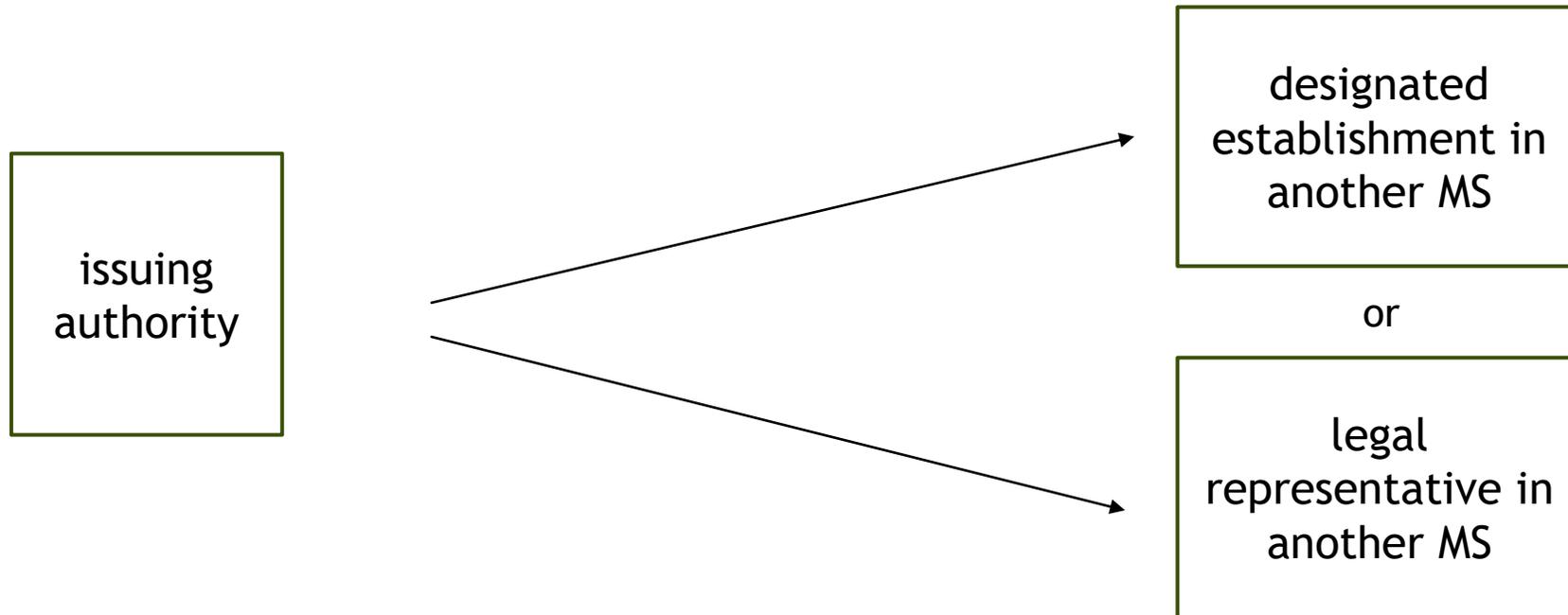
Regulation

in a nutshell

- ▶ **European Production Order and European Preservation Order;**
- ▶ **in the framework of criminal proceedings (not for prevention of crime) and for execution of custodial sentences;**
- ▶ **irrespective of the data location**
- ▶ **served directly via a Certificate (EPOC or EPOC-PR) to the “designated establishment” or “legal representative” (respective SP offering services in the EU; requested data are related to these services) in another MS (only cross-border!);**

Regulation

addressee of the Certificate



re **European Production Order**: additional condition, Art. 5(6) to identify the correct SP: “data controller first”-principle, but with exceptions (cannot be identified; detrimental to investigations)

Regulation

data covered

- ▶ **Only stored data;** no real-time interception, no data retention obligations
- ▶ **Data categories:**
 - ✓ subscriber data,
 - ✓ data requested for sole purpose of identifying the user (in the original COM proposal: “access data”)
 - ✓ traffic data
 - ✓ content data
- ▶ **Different sets of conditions/rules** depending on the request (EPOC or EPOC-PR) and the data categories (subscriber/other identification data vs. traffic/content data)

Regulation

issuing authority

European Preservation Order
irrespective of the data category

+

European Production Order
for subscriber and other identifying data



issued or validated by a **prosecutor, judge or court**; not police! (but see below)

exception in emergency cases, where possible in national law - then ex-post validation by a prosecutor, judge or court



European Production Order
for traffic and content data



issued or validated (only) by a **judge or court**;

Regulation

Conditions for issuing

- re all European Production Orders, irrespective of the data: data requested are part of an infrastructure provided to a public authority, Art. 5 (8): can only be issued when the issuing authority and the public authority are in the same MS
- for all European Production and Preservation Orders: necessity and proportionality; could have been issued under the same conditions in a similar domestic case;
- Orders to **preserve** (all data categories) and **produce** subscriber and other identifying data: for all criminal offences
- Orders to **produce** traffic and content data: only for criminal offences
 - with a maximum custodial sentence of at least 3 years in the issuing (!) MS or
 - one of the offences listed in the Directives listed in Art. 5(4) (b) and (c);
 - or re the execution of a custodial sentence or detention order of at least 4 months following criminal proceedings (if not rendered in absentia)

[re. Orders to produce traffic or content data: additional rules re immunities and privileges, Art. 5 (9) and Art 5(10)]

Regulation

Notification (1)

- **Notification** of the “enforcing MS”= MS where the addressee is located;
 - ❖ only for Production Orders
 - ❖ only re traffic and content data
 - ❖ exception: issuing MS has reasonable grounds to believe person whose data is sought resides in the issuing MS (recital (53)) and offense committed in issuing MS (“national link”);

Regulation

Notification (2)

➤ Consequence:

- ❖ **suspensive effect** of the notification in non-emergency cases;
- ❖ where other MS is notified **4 grounds for refusal**, Art. 12 (raised within 10 days or in emergency cases within 96 hours):
 - (1) immunities and privileges;
 - (2) in exceptional circumstances: indications for manifest breach of Art. 6 TEU;
 - (3) ne bis in idem;
 - (4) no double criminality / list of categories

Regulation

Obligations for addressee

in general:

- **Confidentiality:** no information to the person whose data is sought
upon receipt of an EPOC-PR:

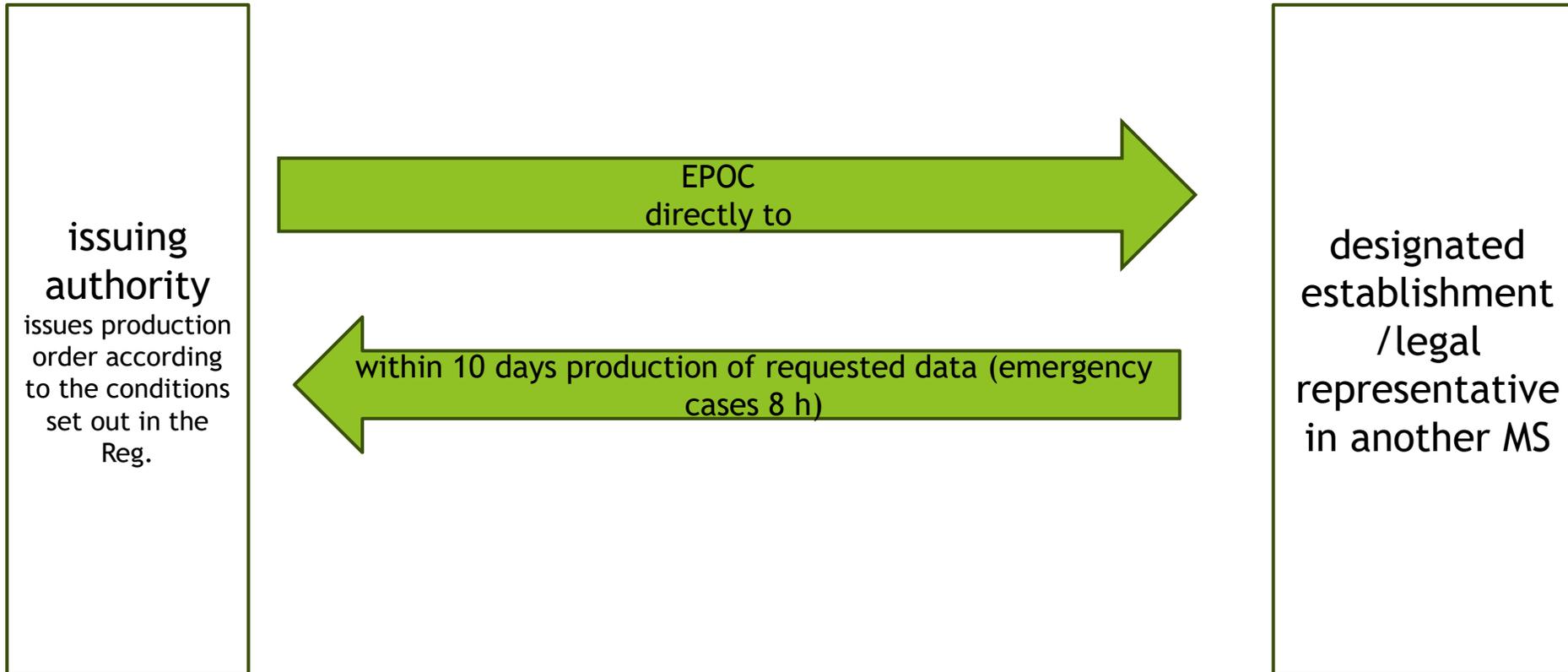
- Preservation for **60 days** - can be extended by an **additional 30 days**
- where issuing authority confirms that a subsequent request for production has been issued: preservation till produced

upon receipt of an EPOC:

- Production of the requested data **within 10 days**; where a notification took place: when the 10 days ceased (and the notified MS did not raise any grounds for refusal)
- and in **emergency cases** within 8 hours;

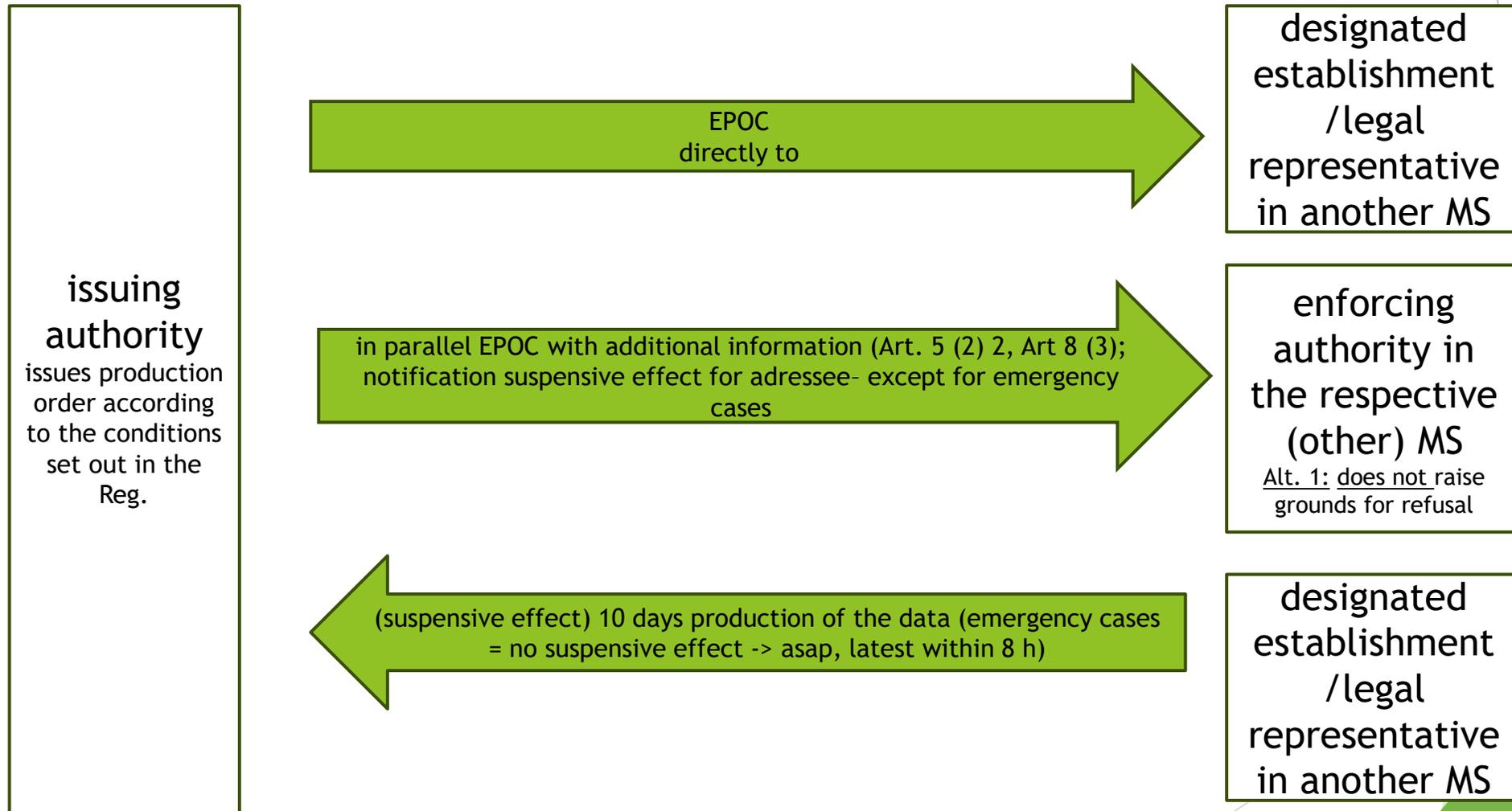
Regulation

EPOC (1) subscriber/other identifying data &
(2) traffic and content data without notification



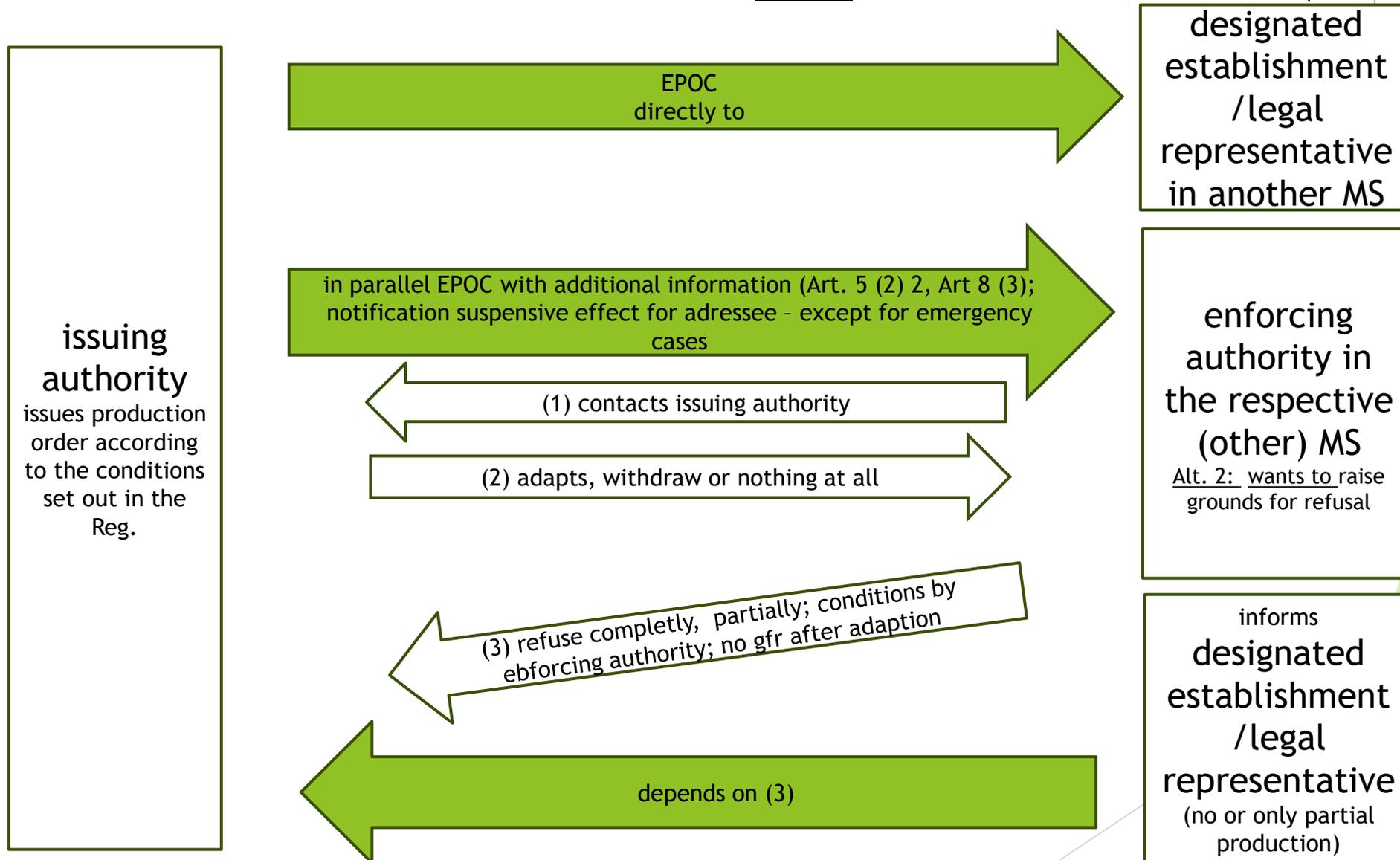
Regulation

EPOC traffic and content data with notification Art. 8 VO (Alt. 1)



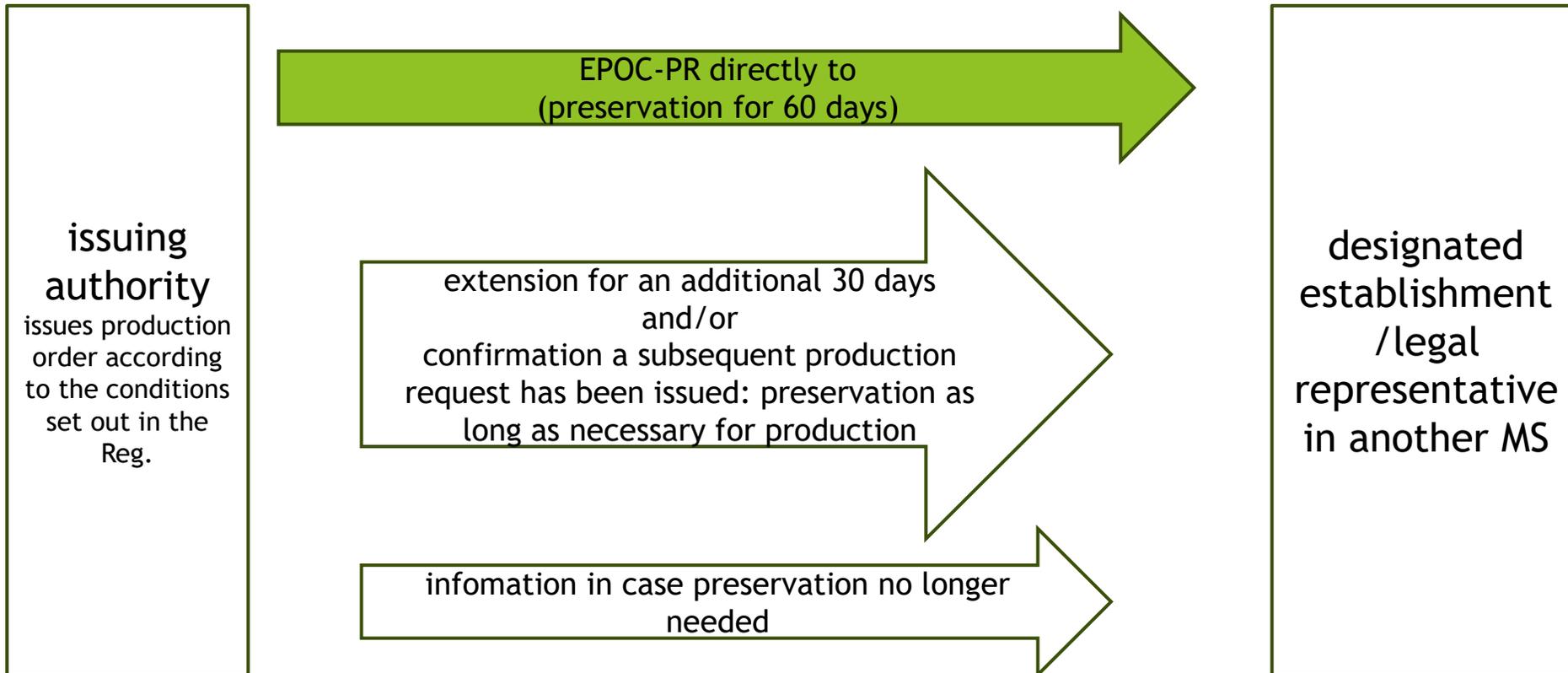
Regulation

EPOC traffic and content data with notification, Art. 8 (Alt. 2)



Regulation

EPOC- PR all data categories



Regulation

Additional safeguards, conditions, remedies

- A decentralised **IT System** will be developed for the safe transfer of the requests, notifications, related exchange and data; mandatory use with exceptions;
- All **criminal law safeguards** and **data protection** rules apply;
- **Information rights** and **effective remedies** in the issuing State;
- **Comity clause** to address conflicting obligations under the rules of other countries, including judicial review in the issuing MS

Regulation

The role of immunities and privileges in the Regulation (1)

■ (1) phase of issuing a European Production Order:

- law of the issuing MS (for all data categories)
- Art. 5 (10): where the issuing authority has reasons to believe the requested traffic and content data are **protected by immunities and privileges in the enforcing MS** the issuing authority may seek clarification **before issuing** by contacting competent authorities in the enforcing MS (directly, Eurojust or EJN); if it finds the requested traffic and content data are protected by immunities and privileges it shall not issue the Order (text does not include possibility to waive; no distinction whether “national link”= notification case +/-)
- traffic or content data requested are part of an infrastructure provided to **professionals covered by a professional privilege**, Art 5 (9): can only be issued (1) where the issuing authority and the professional reside in the same MS, (2) where addressing the privileged professional might be detrimental to the investigation or (3) the privileges were waived in accordance with the “applicable” law.

Regulation

The role of immunities and privileges in the Regulation (2)

- (2a) European Production Order for traffic and content data was issued, Art. 10 (5); addressee considers immunities and privileges under the law of the enforcing MS affected
 - no notification: issuing takes it into account and shall decide on its own initiative
 - notification took place: issuing takes it into account and shall decide on its own initiative; enforcing can raise grounds for refusal (Art. 12)
- (2b) European Production Order for traffic and content data; notification case, Art 12 (1) (a);
 - enforcing MS can raise grounds for refusal; possibility to waive included in text
- (3) enforcement phase, Art. 16 (4) (f):
 - irrespective of data category or notification case/”national link”; nothing included in text regarding the possibility to waive

Where do we stand re implementation?

Thank you for your attention!

Patricia Hamel
patricia.hamel@olg-m.bayern.de



Collecting e-evidence in enterprise environments

Remco Sprooten

Thu, 20th June 2024



**Co-funded by
the European Union**

Remco Sprouten

Senior Security Research Engineer

Elastic Security Labs



Objectives

- Insights into the different enterprise types
- Discover what kind of information is available
- How and when can we use that information
- Practical:
 - What are the questions to ask?
 - Who do we need to address the questions?

Enterprises

Micro Enterprises

1-9 Employees

Generally rely on outsourcing IT services

Small Enterprises

10-49 Employees

Often use a mix of outsourcing for specialized IT needs and cloud services for everyday operations

Medium Enterprises

50-249 Employees

Typically have a dedicated in-house IT department complemented by strategic outsourcing

Large Enterprises

250+ Employees

Maintain substantial in-house IT departments, utilizing a combination of insourcing, selective outsourcing, and hybrid cloud environments to handle diverse and sophisticated IT requirements at scale.

Micro Enterprises

1-9 Employees

- If any the IT will be outsourced to small / local IT providers
- Common cloud services:
 - Microsoft Office 365 / Google Workspace
 - Slack / Zoom
- Key point: No internal IT staff

Small Enterprises

10-49 Employees

- Small enterprises outsource IT services like
 - Basic support and maintenance
 - Cybersecurity
 - Network management
 - Software development
- Additional cloud services like:
 - CRM
 - Support desks

Medium Enterprises

50-249 Employees

- A hybrid mix of internal and outsourced IT partners.
- More complex network setup
- Might work with multiple IT service suppliers

Large Enterprises

250+ Employees

- Will have an internal dedicated staff for managing:
 - General IT
 - Support
 - Security
- You will find a mix of suppliers, managed service providers and external services.
- A complex mix of cloud and hybrid applications. Often managed by multiple teams

IT Providers

Level 1

Handle primarily workstations and small networks

Level 2

Will be able to manage (multi) server setups. Limited cloud application support

Level 3

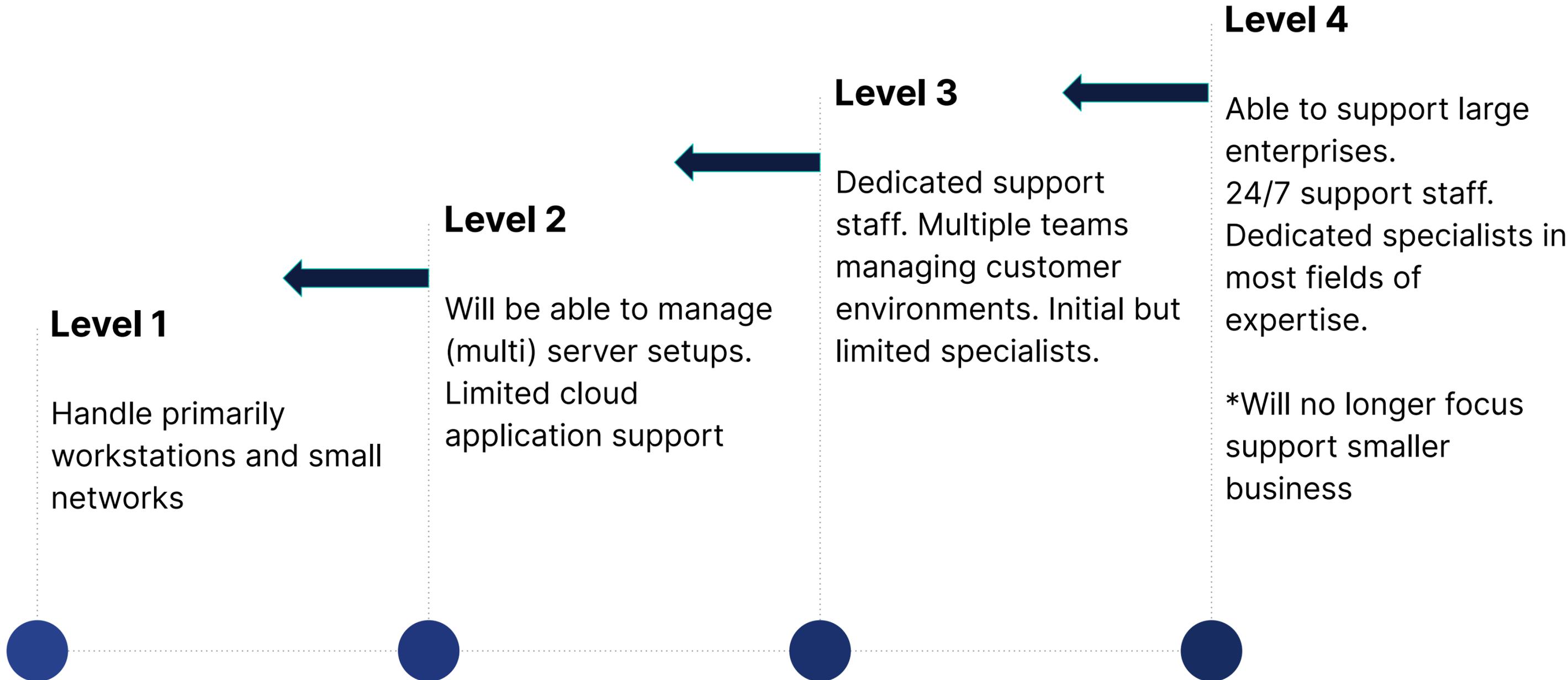
Dedicated support staff. Multiple teams managing customer environments. Initial but limited specialists.

Level 4

Able to support large enterprises. 24/7 support staff. Dedicated specialists in most fields of expertise.

*Will no longer focus support smaller business

IT Providers



66

The big question?

Security Operations Centers



Security Operations Center Information Sources (examples)

Endpoints

Information from devices like laptops and desktops which can help detect suspicious activity and malware.

Network Traffic Data

Monitored through firewalls, routers, and intrusion detection systems (IDS), this data helps in identifying unusual patterns and potential threats

Mobile Device Management

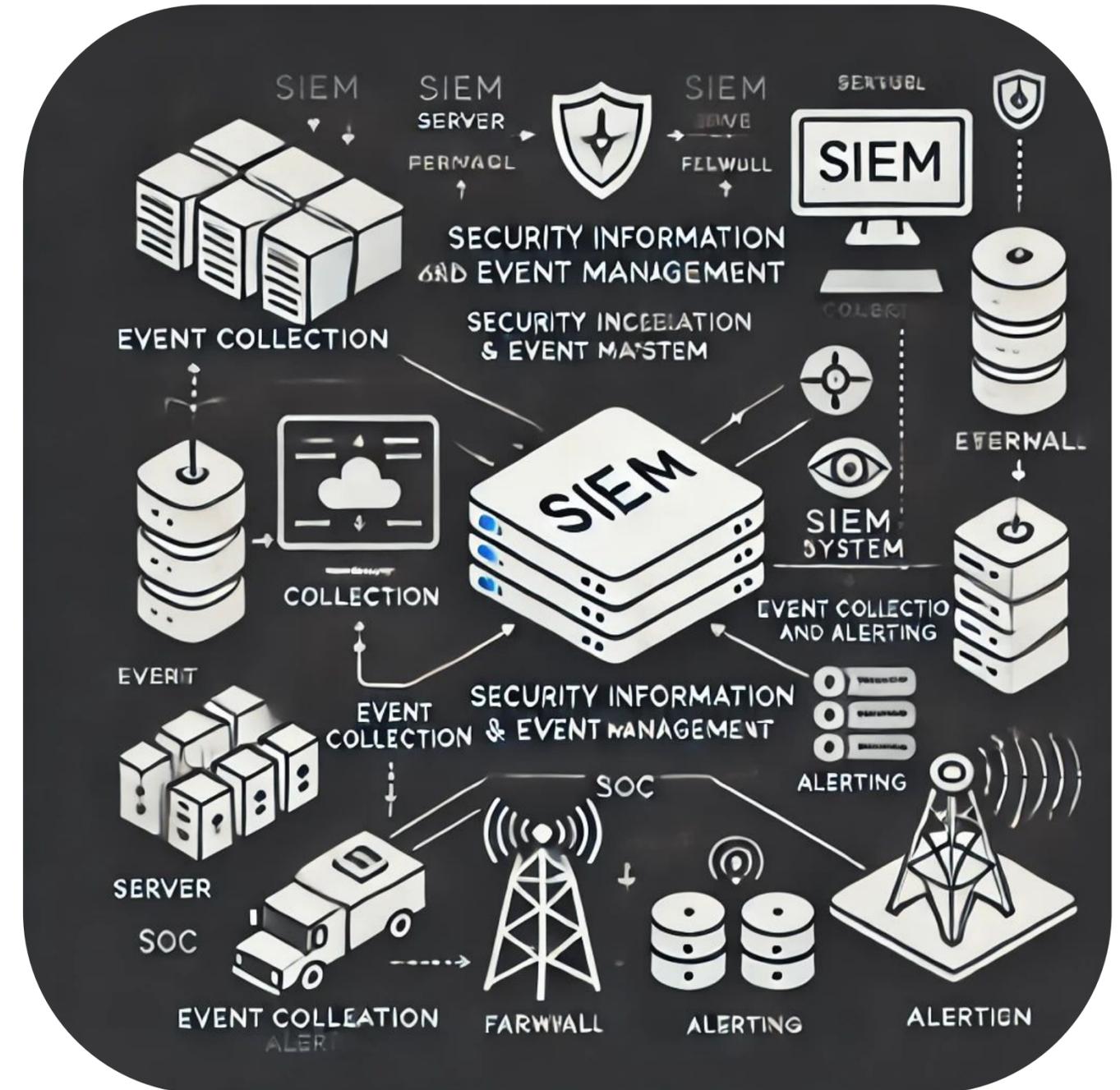
Data from MDM systems, which manage and secure mobile devices, ensuring they comply with security policies and detecting potential threats.

Logs from IT Systems and Applications

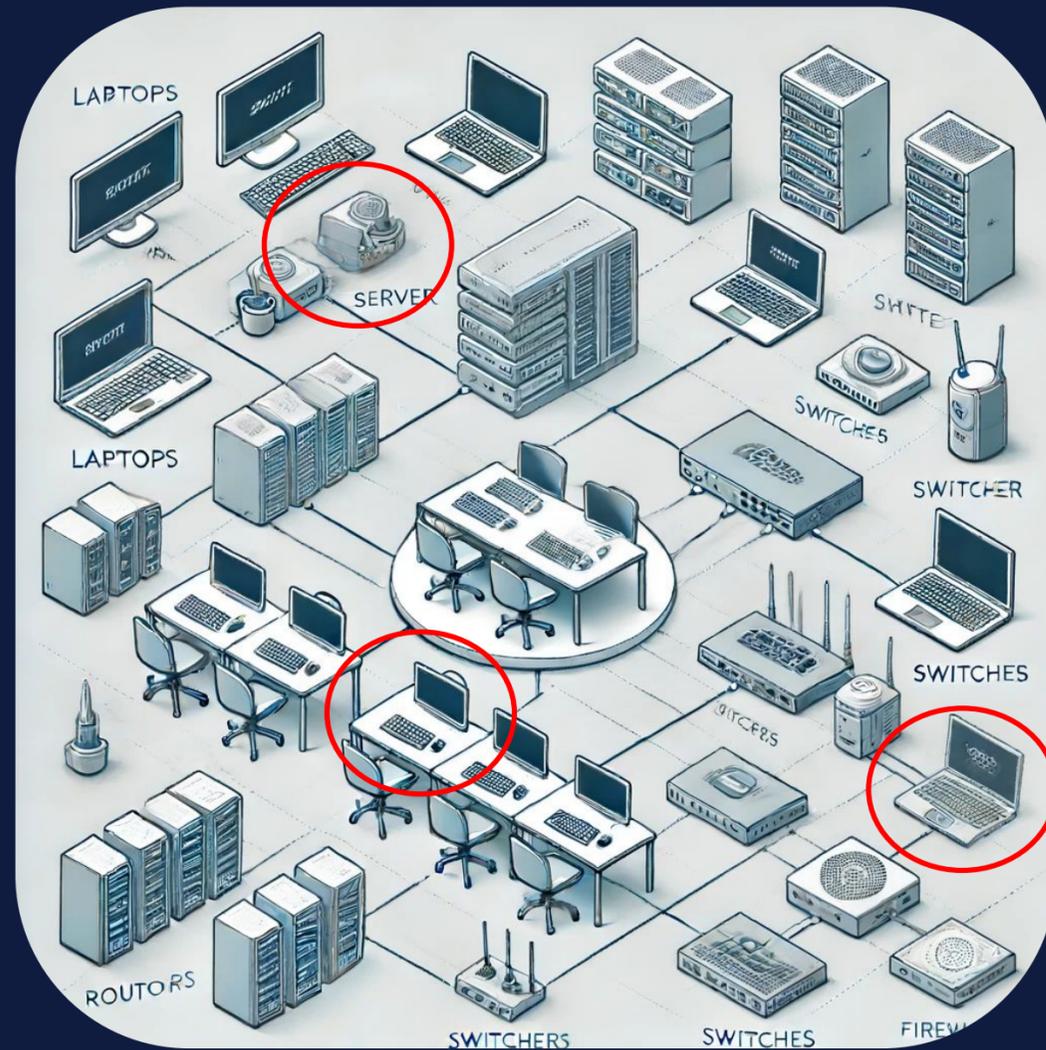
Detailed records of activities and events occurring within servers, databases, applications, and other IT systems. This includes cloud applications

SIEM: Security Information Event Management

- **Centralized Monitoring:** A SIEM system collects and monitors data from various sources like servers, networks, and devices to provide a unified view of an organization's security.
- **Threat Detection:** It analyzes the data in real-time to identify unusual activities or potential security threats.
- **Alerting and Reporting:** When a threat is detected, the SIEM system generates alerts and detailed reports to help the security team take quick and informed actions.



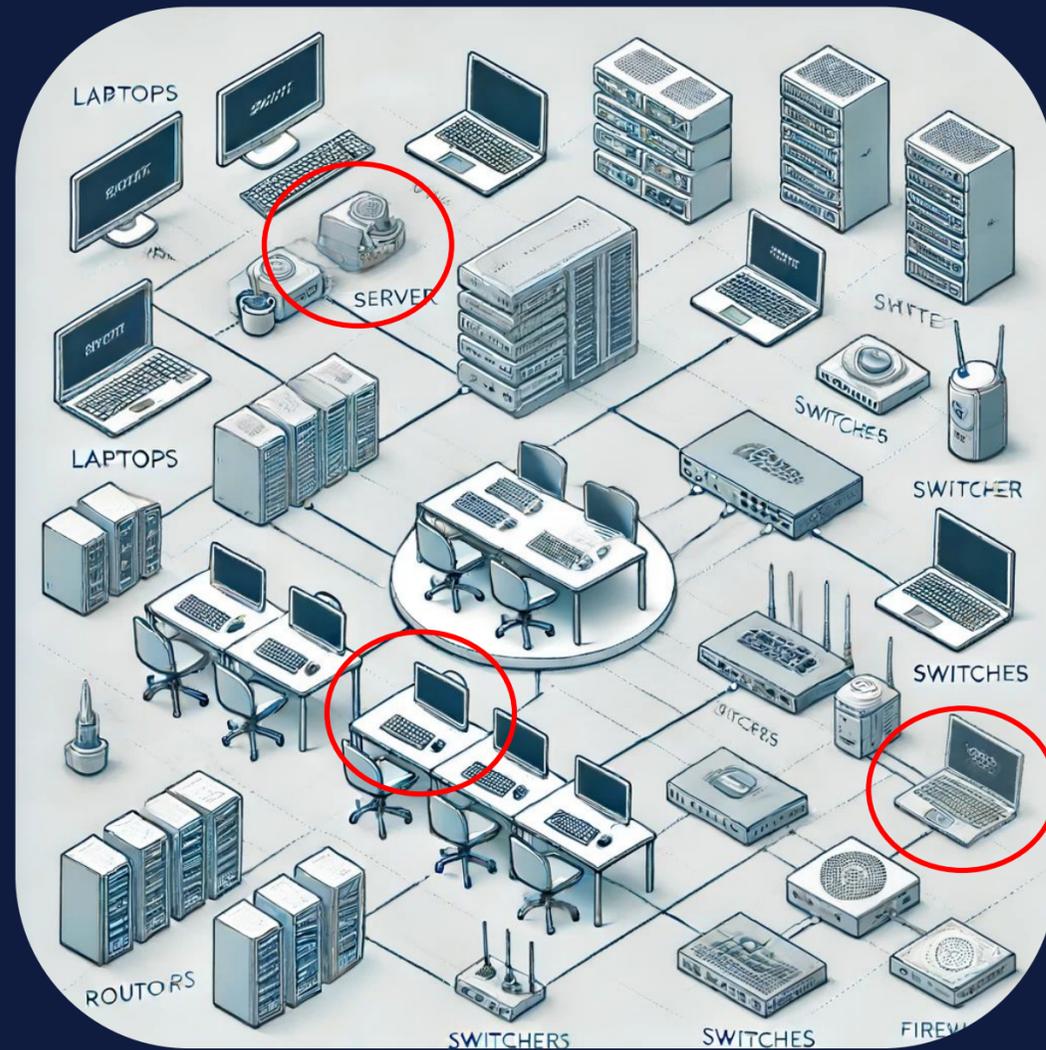
Traditional data collection



Suspected evidence

- Identify
- Collect
- Bring back to the lab for investigation

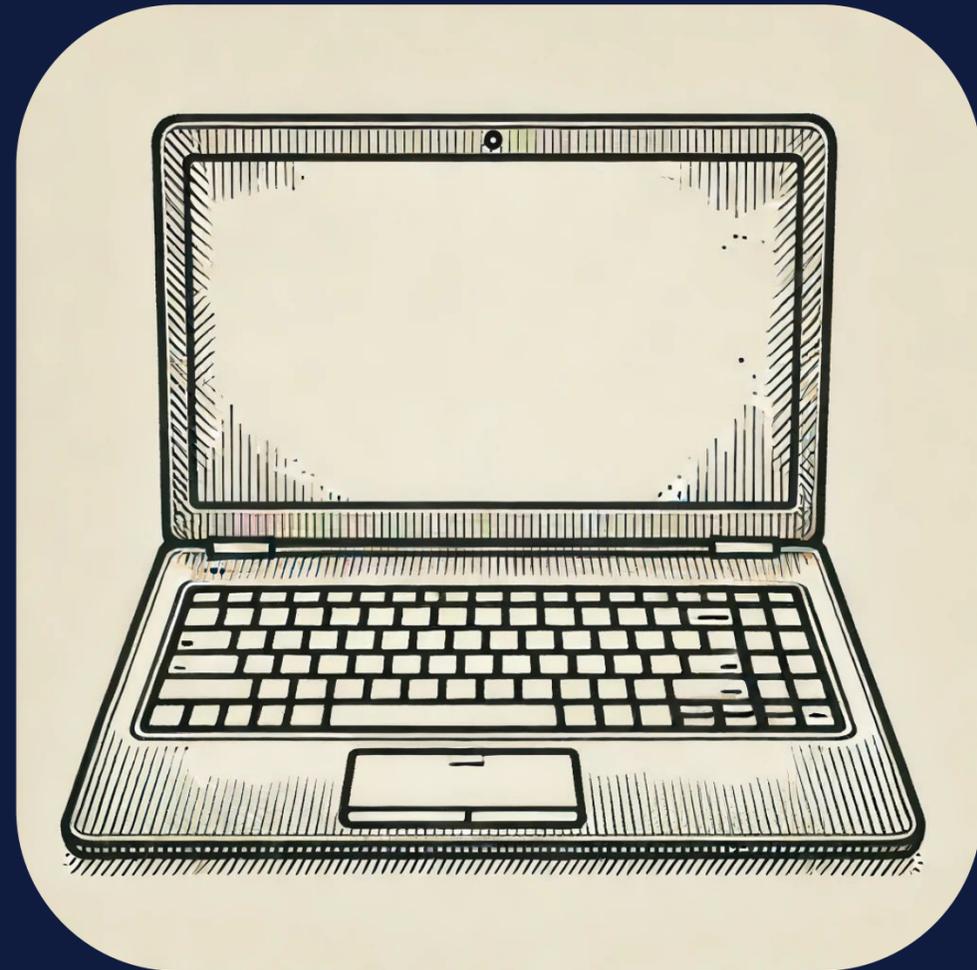
Traditional data collection



In the lab we find:

- Laptops (encrypted)
- Phones (encrypted)
- Drives (encrypted)
- Network Connection (no longer present)

Example: Laptops



Mobile Device Management

EDR (Anti Virus)

Log monitoring

Example: Laptops



Mobile Device Management

- Can hold the encryption key

EDR (Anti Virus)

- Every action the user takes, including accessing file, starting programs

Log monitoring

- Even if the logs are erased the SOC wil have a copy in the SIEM

Example: Laptops



- Connected WiFi network
- IP of locations visited
- Devices connected
- Any changes to the settings

Example: Smartphones

Mobile Device Management

- Device Location History
- Application Usage Logs
- Security Policy Compliance



Example: Application logs



- Authentications to applications
- Activity logs
 - User interactions
 - Passive activities

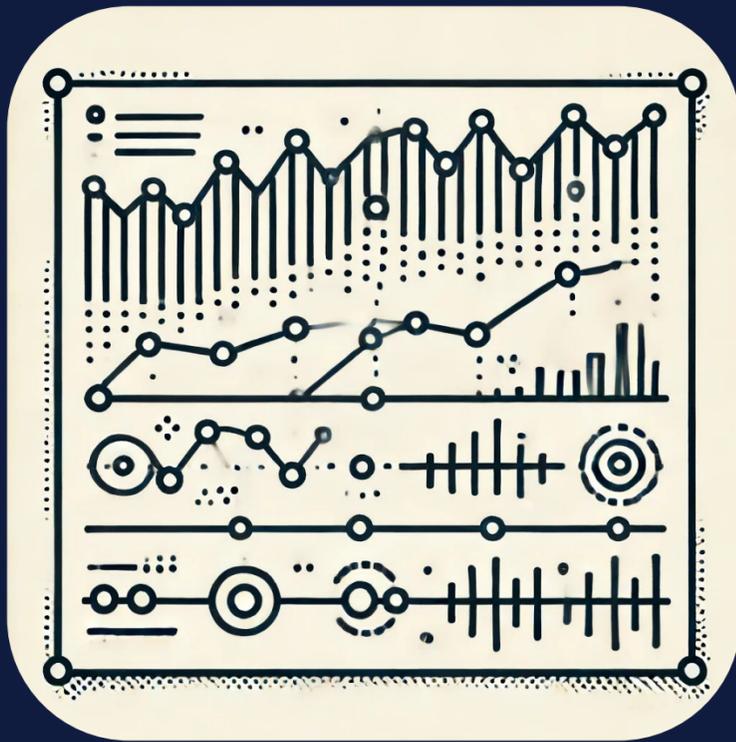
Telemetry Data

The public kept secret



Telemetry Data

The public kept secret

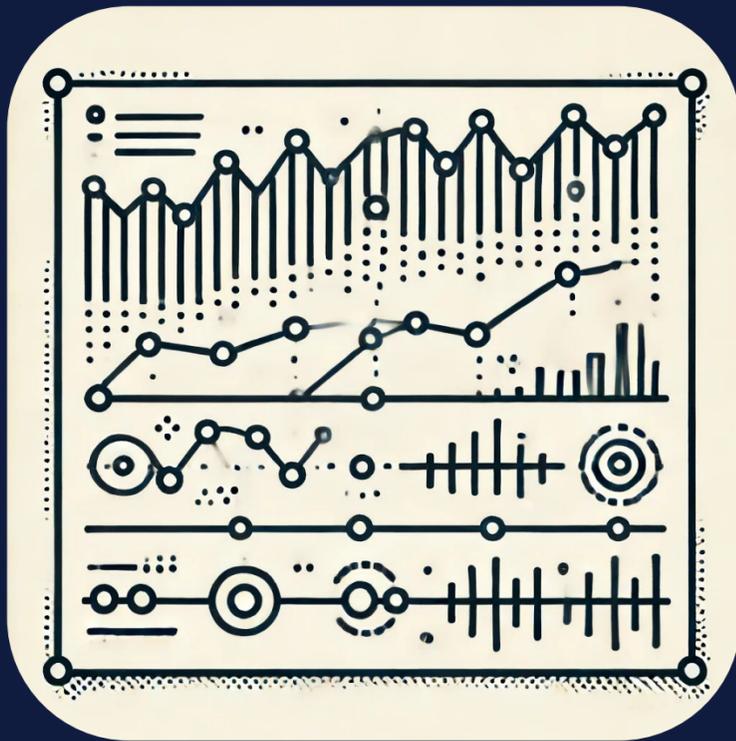


EDR/AV Vendors:

- Copy of alerts
- Downloads of updates
- Usage statistics

Telemetry Data

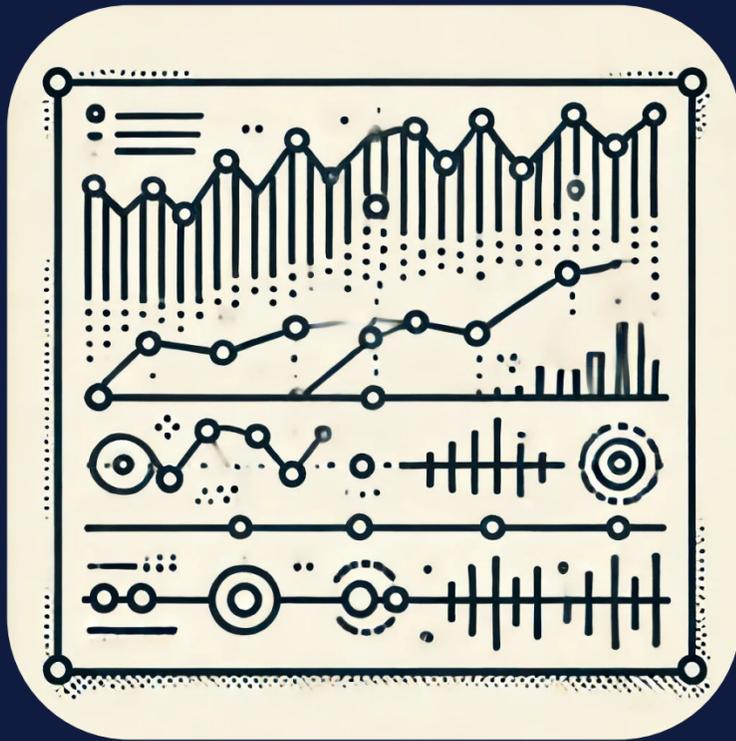
The public kept secret



- Common EDR vendors:
 - CrowdStrike
 - Microsoft
 - SentinelOne
 - VMware Carbon Black
 - Elastic
 - Palo Alto Networks
 - Trellix
 - Trend Micro
 - Cisco

Telemetry Data

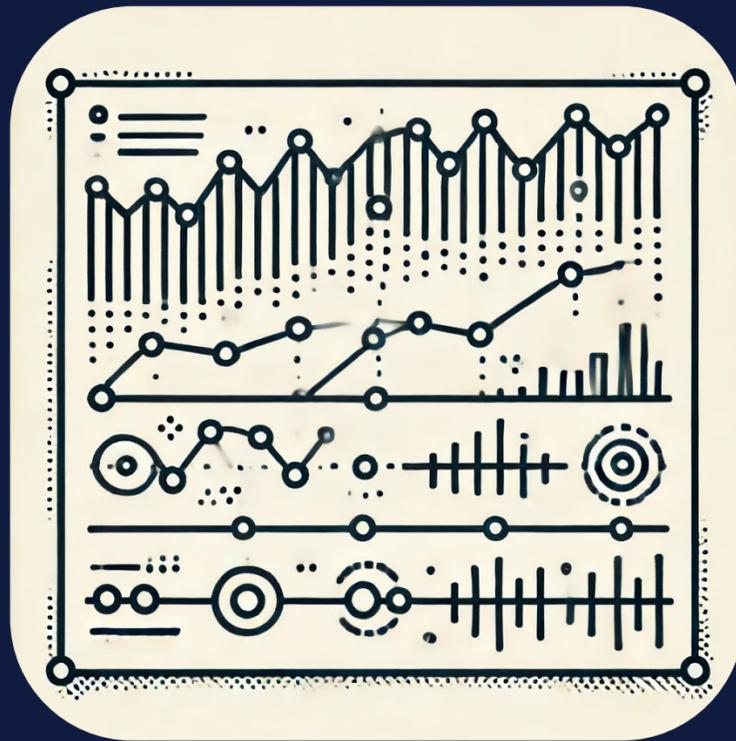
The public kept secret



- Common MDM vendors:
 - JumpCloud
 - Microsoft
 - AirDroid Business
 - Miradore
 - Hexnode
 - Jamf

Telemetry Data

The public kept secret



Upcoming markets:

- ChatGPT
- Microsoft CoPilot
- Google Gemini

66

DEMO

Closing remarks

- Enterprise information can be valuable to an investigation but you need to know who to ask and what to ask for.
- It is important to establish prior relationships with key partners

Thank you!



Scenario 1: introduction

We have a case where a man was caught stealing IT equipment from his job site. His employer was missing expensive inventory, so he decided to check the CCTV footage. It was clear that the man was seen putting inventory that was supposed to be sold to customers in his backpack just before leaving the building. They found at least three other occasions where this happened.

The next day, the employee was called to the manager's office and confronted. He was told that they would file a police report and that he had been fired.

As per company policy, all his accounts had been deactivated, and his authentication was revoked.

Scenario 1: introduction

Unfortunately, this was not the end. As soon as the man came home, he put his frustration on his family. Without going into details, his wife and two kids did not survive this incident.

After realizing what he'd done, the man managed to flee.
It is our job to find him.

Scenario 1: Hints

During the search of his house the police found the SIM card of his telephone.

There were strong indications that the man has or is in the process of leaving the country.

There is no information to be found concerning where the man is going to or how he is going to travel.

Scenario 1: Results

Since the man has left his SIM card behind the police assumed that he would be changing network providers so they put out a search for his last known IMEI. this did not yield any results.

However a week later the police were contacted by the man's former employer. They (their IT provider) noticed that there had been failed attempts to logon to his account from and IP address in Egypt.

Scenario 2: introduction

There was a significant announcement. A company in the IT space announced that it had reached an agreement with a bigger competitor and that the company would be sold. Both companies were publicly traded. The smaller company was trading at \$100 per share before the announcement. The accepted buyout price, however, was \$140 per share.

Two days after the announcement, the public noticed that three days before, there had been a big buy order. Someone had managed to buy a considerable amount of options that would make this individual over 20 million dollars overnight.

Scenario 2: Initial investigation

The initial investigation concluded the following:

All information about the merger was strictly controlled.

- Everyone involved was issued an NDA
- All digital information was stored on prepared devices that were actively monitored.
- All documents were protected with
 - Watermarks
 - Data loss prevention software
 - Active tracking

Scenario 2: Hints

Investigating Dark Web Activity

Suspecting that this could involve more sophisticated channels like the dark web, we enlisted our cybercrime specialists:

- **Dark Web Monitoring:** Deployed tools to monitor dark web marketplaces and forums for any hints of company information being sold.
- **Cryptocurrency Analysis:** Tracing cryptocurrency transactions potentially linked to the case.

Scenario 2: Results

Our dark web monitoring eventually uncovered a post on a hidden forum offering "premium financial forecasts" related to several companies, including our company.

Thank you!





E-Evidence, digital devices, pins & passwords – Mandatory Disclosure – fair or unfair?

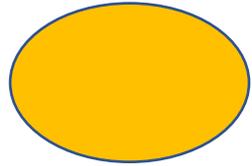


20 June 2024
Tallinn

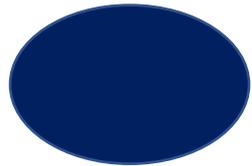
Muthupandi Ganesan
Barrister & Partner
Aliant Law



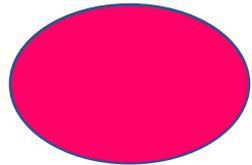
This Webinar will cover



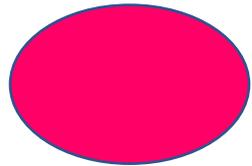
Mandatory Disclosure under UK regime



Notice under section 49 RIPA



Trial procedure & Expert Evidence



Unfairness



ALIAN^T
Powered by *Human Intelligence*

Mandatory Disclosure of Pins and Passwords

➤ **What type of material can be subject of mandatory disclosure?**

➤ **Protection Information**

➤ **Comes in to possession of the Police lawfully**

➤ **Appropriate Persons – on reasonable grounds believes that:**

(a) that a key to the protected information is in the possession of any person,

(b) that the imposition of a disclosure requirement in respect of the protected information is—

(i) necessary on grounds falling within subsection (3), or

(ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,

(c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and

(d) that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section, the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.



Criteria for disclosure?

- ❑ A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary—
 - (a) in the interests of national security;
 - (b) for the purpose of preventing or detecting crime; or
 - (c) in the interests of the economic well-being of the United Kingdom.(section 49 (3))

- ❑ Notice to be given under section 49(4)

Notice requirement

must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;

(b) **must describe the protected information** to which the notice relates;

(c) must specify the matters falling within subsection (2)(b)(i) or (ii) by reference to which the notice is given;

(d) must specify the office, rank or position held by the person giving it;

(e) must specify the office, rank or position of the person who **for the purposes** of Schedule 2 granted permission for the giving of the notice or (if the person giving the notice was entitled to give it without another person's permission) must set out the circumstances in which that entitlement arose;

(f) must specify the time by which the notice is to be complied with; and

(g) must set out the disclosure that is required by the notice and the form and manner in which it is to be made;

and the time specified for the purposes of paragraph (f) **must allow a period for compliance which is reasonable in all the circumstances.**

Rex v Jonathan Nuttall – Central Criminal Court – 2023

- 5 months trial
- 6 Defendant trial
- Allegations of bomb hoax, money laundering and failure to provide pins and passwords
- Chronology
 - March 2022: Arrest and seizure of electronic devices (30 items)
 - April 2022: Charged with bomb hoax and money laundering.
 - July 2022: Request for disclosure of pins and passwords
 - August 2022: Response by the Defendant – cannot recall the passwords and pins.
 - January 2023: Further charges of failure to give pins and passwords.

Notice under section 49

- The protected information to which the Section 49 Notice relates to are as follows:
 - 1.RJB/33 - iPhone 11 Pro A2160 – requires alphanumeric PIN
 - 2.RJB/81 - iPhone 12 Pro Max A2342 – requires alphanumeric PIN
 - 3.RJB/47 - Integral Courier USB Stick – encrypted USB
 - 4.RJB/75 - Integral Courier USB Stick – encrypted USB
 - 5.AAW/20 – IronKey USB in box – requires password
 - 6. AAW/3 – MacBook Pro in case – requires password



Defendant Response

1. The Devices have a long and complex password as advised to the public by the National Crime Agency.
2. The Defendant did not write it down or make a note of it and as such cannot recall.
3. The Defendant did not use the same password for different digital devices.
4. The passage of time of nearly 5 months by the time of the NOTICE meant that he cannot recall.

Expert Evidence

- Examined only after Defendant gave evidence.
- 2 x Devices - did not have passwords
- 1 x Device – on factory settings
- 1 x Device – cant be sure, if password was set up.

Sentence:

Count 5 and 6: Failure to provide pins and passwords to two telephones seized by the Police. The Defendant was sentenced to 6 months imprisonment concurrent for both Counts 5 and 6 but consecutive to other sentences for counts 1, 3 and 4.

Fairness?

- Case specific: Victim v Defendants Rights
- Nature of criminal investigation (child abuse/ child sex images v economic crime or other forms serious organised crime)
- Timing of criminal investigation
- Evidential basis
- Trustworthiness of decision making?
- Sentence: up to 2 years.
- Remedy?



ALIAN.T[®]
Powered by *Human Intelligence*

Any questions?

Muthupandi Ganesan
Barrister & Partner

E-mail: mganesan@aliantlaw.com

20 June 2024

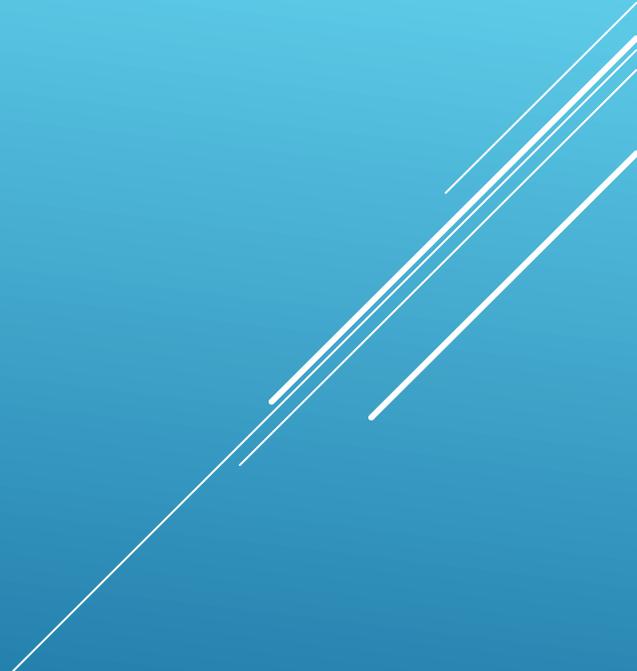


PRACTICAL EXPERIENCES WITH VIDEOCONFERENCING WHEN HEARING EXPERTS AND WITNESSES

21 JUNE 2024
ERA, TALLIN
BALÁZS ROZSNYAI



OVERVIEW

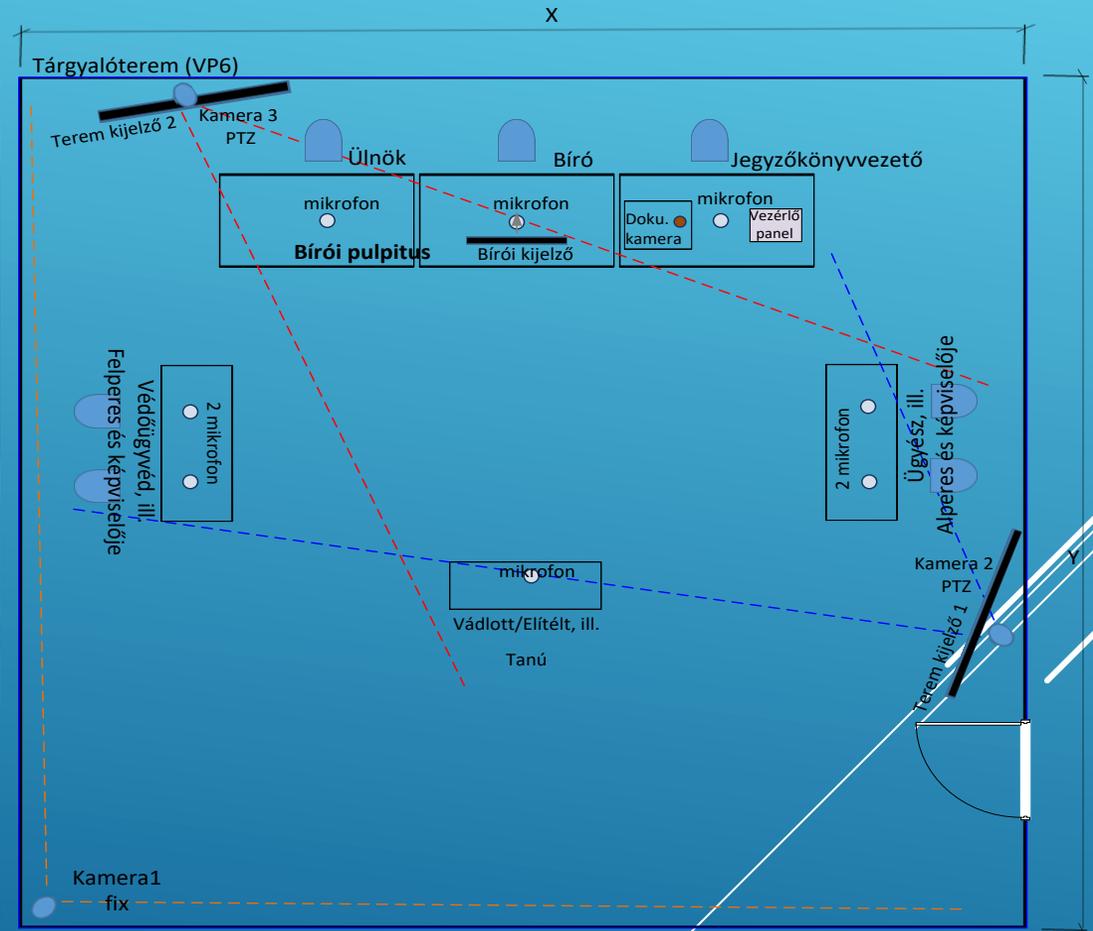
- I. Source of the experiences / Development and improvement
 - II. Legal basis
 - III. Requesting a videoconference
 - IV. Rules and Experiences
 - v. Conclusion
- 

/ad I. THE BEGINNINGS AND OBJECTIVES OF THE HUNGARIAN PROJECT

- To implement widespread and efficient **electronic court administration**
 - Joined project in **2018**
 - Remote hearing **endpoints** at courts, governmental offices, governmental customer service points, police stations, prisons
- 

/ad I.

COURTROOM WITH REMOTE HEARINGS TERMINAL



/ad I.

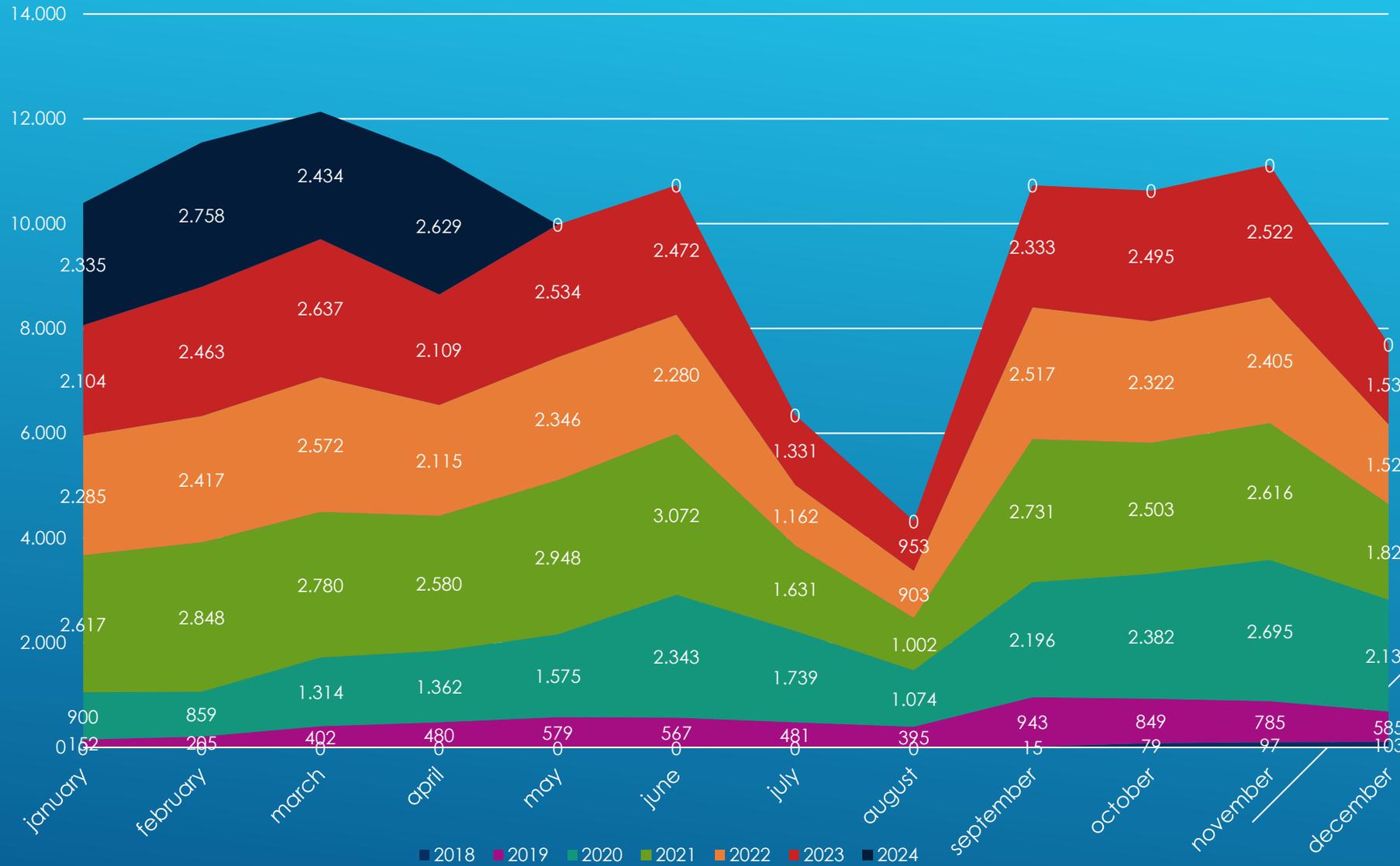


FREQUENCY OF USE

- 216 **courtrooms** have been equipped
- the judicial system **has not stopped** operating during the **pandemic**
- the number of remote hearings increased by almost **60%**

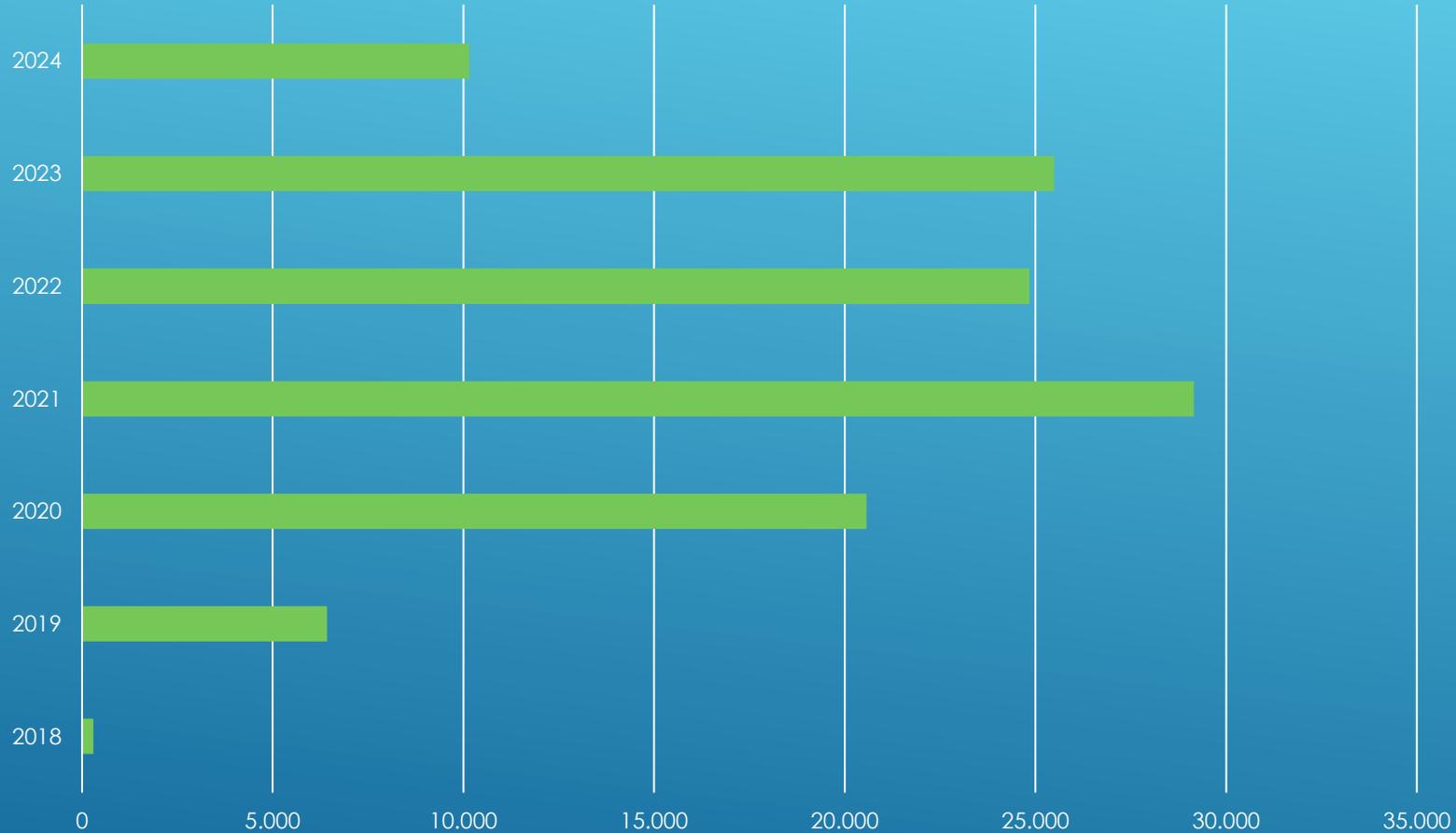
/ad l.

THE NUMBER OF REMOTE HEARINGS BY MONTH BETWEEN JANUARY 2018 – APRIL 2024



/ad I.

THE NUMBER OF REMOTE HEARINGS PER YEAR BETWEEN JANUARY 2018 - APRIL 2024

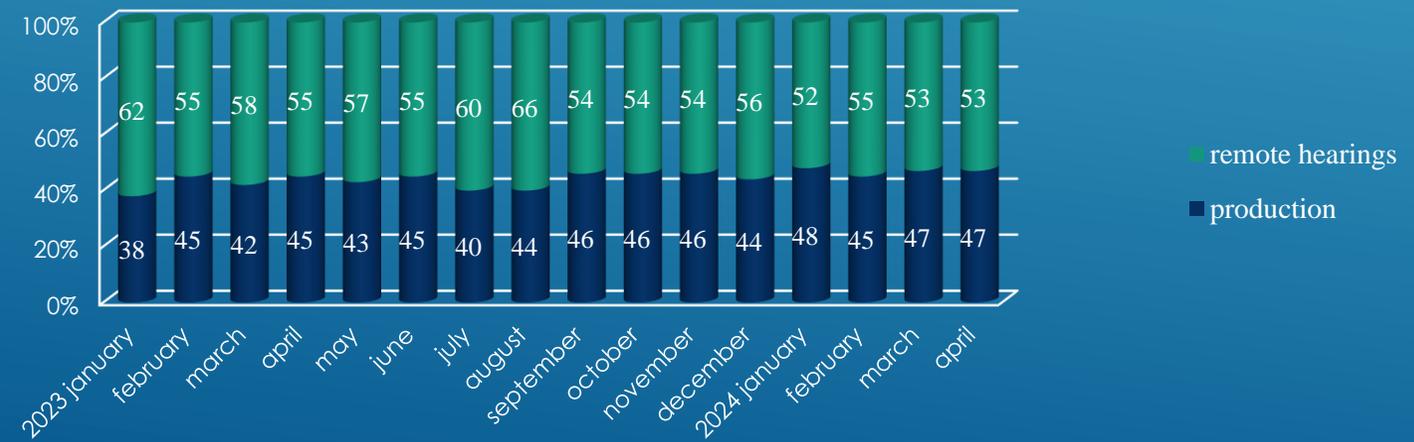
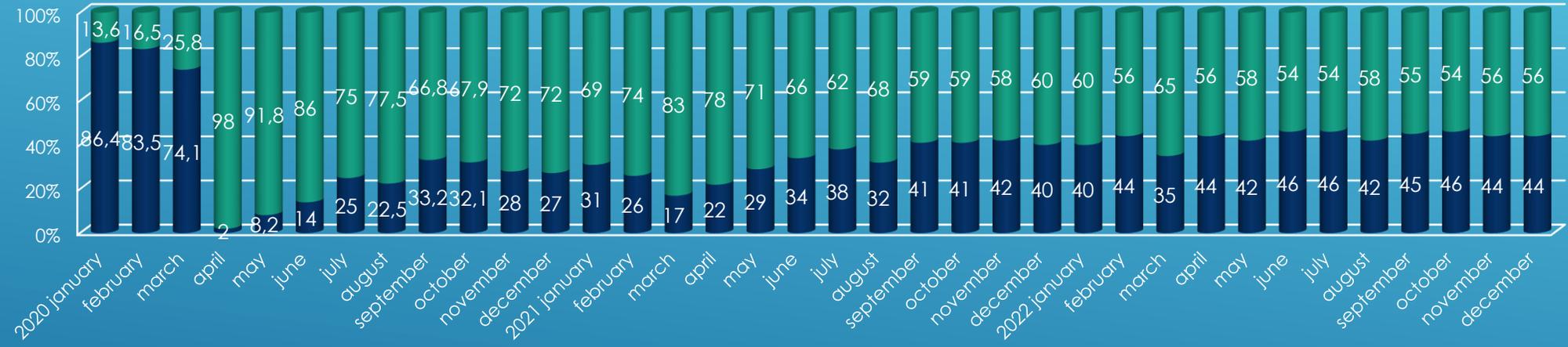


	2018	2019	2020	2021	2022	2023	2024
■ number of hearings	294	6.423	20.569	29.157	24.844	25.488	10.156

/ad I. HEARING OF PERSONS IN DETENTION

- ✓ The **largest proportion** of remote hearings in criminal cases is the hearing of **prison inmates**
- ✓ During the COVID period up to **80% of the personal presence** of the inmates was replaced by remote hearings

The evolution of the proportion of remote hearings and productions ordered by courts



■ remote hearings
■ production

/ad I.

DEVELOPMENT AND IMPROVEMENT



- a **new technology** is a time-consuming process
- after the adoption of the emergency law the entire society switched to teleworking in literally a **few days**
- working as a judge on the online space was initially a **challenge for everyone**
- both the call and its content are **encrypted by the software**
- most important benefits of using videoconference in court: clients and lawyers **save a lot of time and money**, work more convenient and **easier to plan, the length of the proceedings** can also be **reduced**
- today, any authorised party is **able to join** a hearing held via videoconference from anywhere securely with **their own device** with internet access

/ad I.



/ad II.

LEGAL BASIS AND ALTERNATIVES

- **DIRECTIVE** 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 regarding the **European Investigation Order** in criminal matters
- For EU Member States not implementing the EIO Directive (Ireland, Denmark): **Article 10 of the CONVENTION (MLA, 2000)** established by the Council on Mutual Assistance in Criminal Matters between the Member States of the European Union
- **With non-EU Member States: (Strasbourg Convention) Article 9** of the Second Additional Protocol (2001) to the European Convention on Mutual Assistance in Criminal Matters, signed in Strasbourg, 1959

~ ~ ~

Alternatives:

1. **Hearing by telephone conference** (Article 25)
2. **Hearing by a court of a requested Member State** (Article 10 (1)c)
(Full Guarantees but questions need to be very carefully prepared)

BUT - Videoconference (article 24) – (The most typical procedural act)

- Hearing via the NISZ VIKI WEB interface
- Skype for Business/Teams/Zoom

/ad III.

REQUESTING A VIDEOCONFERENCE I.

- ORGANIZING A VIDEOCONFERENCE -

- **court decision is required** (general EIO rule)
- **EIO form**
 - Section B, C, G and H2
- **Other**
 - Directly/informally (e-mail)
 - Technical details, test call and interview/hearing date
 - Who calls whom (usually the issuer calls the executor)
 - Who provides an interpreter
- **Problem**
 - technical incompatibility  web interviews or hearings by request

/ad III. REQUESTING A VIDEOCONFERENCE II. - WITH EIO -

SECTION B: Urgency • optional

Please indicate if there is any urgency due to

Evidence being concealed or destroyed

Imminent trial date

Any other reason → e.g. - defendant is under arrest
- statute of limitations

BUT! speeding up the case



Please specify below:

Time limits for execution of the EIO are laid down in Directive .../.../EU*. However, if a shorter or specific time limit is necessary, please provide the date and explain the reason for this:

• only if really justified!!!

REC - contact executing authority ASAP (before issuing)

→ (@; fax; phone - art. 7 / 2000 MLA Conv.)

- check urgent cases of MSs: <https://www.ejforum.eu/cp/registry-files/3339/Competent-authorities-languages-accepted-scope-30-September-2019.pdf>

/ad III. REQUESTING A VIDEOCONFERENCE III. - WITH EIO -

 FINLAND	
ACCEPTED LANGUAGES	Finnish, Swedish or English. The executing authority can always in urgent cases be asked if other languages besides Finnish, Swedish or English can be used.

SECTION C: Investigative measure(s) to be carried out. **always fill in!**

1. Describe the assistance/investigative measure(s) required AND indicate, if applicable, if it is one of the following investigative measures:

.....
• **Be precise! - short/simple sentences**
.....

.....
REC: - questions of interrogations here / in annex
.....
- use 1 form (if 1 case but more measures /
.....
more concerned persons) EXCEPTIONS: - complex cases / more executing MS
.....

.....
• **no tick box for measure → do not be scared!:)**
.....
.....

/ad III. REQUESTING A VIDEOCONFERENCE IV. - WITH EIO -

- Identification of persons holding a subscription of a specified phone number or IP address
- Temporary transfer of a person held in custody to the issuing State
- Temporary transfer of a person held in custody to the executing State
- Hearing by videoconference or other audiovisual transmission
 - witness = victim? REC: persons with different legal status (witness vs. accused) → both warnings!
 - expert
 - suspected or accused person
 - only with their consent (Eu.tv. 63/C § (4)a) = 'may refuse'
 - in trial phase - an alternative for temporary transfer
- Hearing by telephone conference
 - witness = victim? • not for suspected/accused persons!
 - expert

/ad III. REQUESTING A VIDEOCONFERENCE V. - WITH EIO -

SECTION G: Grounds for issuing the EIO

• always fill in!

1. Summary of the facts

Set out the reasons why the EIO is issued, including a summary of the underlying facts, a description of offences charged or under investigation, the stage the investigation has reached, the reasons for any risk factors and any other relevant information.

- lengthy vs. too short descriptions → interpretation issues (necessity/proportionality/double criminality)

.....
REC: - short and simple sentences

.....
- describe relevant facts + provide reason for the measure

.....
- indicate the name of defendant (reason: non bis in idem)

- if description is unsatisfactory → consultation (art. 11 (4) EIO DIR)

2. Nature and legal classification of the offence(s) for which the EIO is issued and the applicable statutory provision/code:

.....
(fill in for double criminality check)
.....

/ad III.

REQUESTING A VIDEOCONFERENCE V.

- WITH EIO -

3. Is the offence for which the EIO is issued punishable in the issuing State by a custodial sentence or detention order of a maximum of at least three years as defined by the law of the issuing State and included in the list of offences set out below? (please tick the relevant box)

- participation in a criminal organisation
- terrorism
- trafficking in human beings
- sexual exploitation of children and child pornography
- illicit trafficking in narcotic drugs and psychotropic substances
- illicit trafficking in weapons, munitions and explosives
- corruption
- fraud, including that affecting the financial interests of the European Union within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests
- laundering of the proceeds of crime
- counterfeiting currency, including of the euro
- computer-related crime
- environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties
- facilitation of unauthorised entry and residence
- murder, grievous bodily injury
- illicit trade in human organs and tissue
- kidnapping, illegal restraint and hostage-taking
- racism and xenophobia
- organised or armed robbery
- illicit trafficking in cultural goods, including antiques and works of art
- swindling
- racketeering and extortion
- counterfeiting and piracy of products
- forgery of administrative documents and trafficking therein
- forgery of means of payment
- illicit trafficking in hormonal substances and other growth promoters
- illicit trafficking in nuclear or radioactive materials
- trafficking in stolen vehicles
- rape
- arson
- crimes within the jurisdiction of the International Criminal Court
- unlawful seizure of aircraft/ships
- sabotage

• always mark, if applicable!

/ad III. REQUESTING A VIDEOCONFERENCE VI. - WITH EIO-

SECTION H2: Video or telephone conference or other audiovisual transmission

If hearing by videoconference or telephone conference or other audiovisual transmission is requested:

Please indicate the name of the authority that will conduct the hearing (contact details/language):

.....

Please indicate reasons for requesting this measure:

.....

- (a) hearing by videoconference or other audiovisual transmission:
 - the suspected or accused person has given his/her consent
- (b) hearing by telephone conference

/ad IV.

RULES AND EXPERIENCES I.

- SPECIFIC GROUNDS FOR REFUSAL -

- **No consent of the defendant**(article 24.2 (a))
 - to be obtained in writing or recorded in the minutes
- **No consent of the witness** (EJN Fisches Belges)
- **the execution of the particular requested measure would be contrary to the fundamental principles of the law of the executing State.**

/ad IV.

RULES AND EXPERIENCES II.

- PROCEDURAL RULES -

- The legislation of the issuing MS applies ("**forum regit actum**")
but !
- the person to be questioned may also exercise the right to refuse to testify, to cooperate or to express his or her views in accordance with local law ("**locus regit actum**")
- persons present are subject to the law of the place of execution + **BUT!** the official of the requested Member State who is present may (or may not) warn him/her in accordance with his/her own law
- a member of the executing court is present at the place where the procedural act is performed
 - ensures the enforcement of the rules of the national law and verifies identity of the person concerned
- **Minutes of the hearing:**
 - records the persons present and compliance with the procedural rules
 - the issuing court prepares the minutes of the proceedings
 - the recording must be sent to the national authority without delay

/ad IV.

RULES AND EXPERIENCES III.

- TRANSLATION-

- interpreter as liaison - criminal cost
- Contact language to be agreed (form)
- Appointment of an interpreter: issuing Member State (advisable, for reasons of criminal costs)
- in Executing MS - interpreter may be needed to follow the proceedings - own costs [Article 21(1)]
- too high costs → negotiation

Background rule: Directive on Interpretation [2010/64/EU]

/ad IV.

RULES AND EXPERIENCES IV.

- VIDEOCONFERENCE WITH NON-EU MEMBER STATES -

- **Article 9** of the Second Additional Protocol (2001) to the European Convention on Mutual Assistance in Criminal Matters (**Strasbourg Convention**)

Main difference

- As a general rule; only witness and expert
- Defendants only by special agreement, or not at all
 - see reservations <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=182>
- If addressed to Hungary: consent of witness and expert required

/ad IV.

RULES AND EXPERIENCES V.



- General rule: witnesses and experts must appear **personally**
- The use of videoconference ensures the oral and direct nature of the procedure
- The right to **ask questions**, to **initiate questions**, to **make comments**, to **make observations** or even **cross-examination** can be easily resolved
- The **expert institutes** requested that the experts should be heard remotely as well
- criminal procedural law applicable to experts also apply to **interpreters**
- Witnesses can join the hearing **from abroad/home/work**
- The system can also guarantee the **safety of protected victims and witnesses** who require special treatment
- In the last 6 years we have established remote hearing connections with more than **90 countries**

/ad IV.

RULES AND EXPERIENCES VI.

- PERSONAL EXPERIENCE -

- 1.) No more reluctance to use
- 2.) Clients are in favour of the system as well
- 3.) Less issues with keeping order during the trial
- 4.) No upper limit for endpoints
- 5.) „issues" might occur with weblinks
- 6.) hearing witnesses abroad via weblink - C-255/23 and C-285/23
- 7.) Recordings as trial minutes
- 8.) Ad hoc videoconferences by sending weblink/direct dialing
- 9.) Organizing training events
- 10.) Judges are good at using the system



SUVEREIGNTY ISSUES?!

/ad V.

CONCLUSION



THANK YOU FOR YOUR ATTENTION!

