ERA

POST-COVID CHALLENGES IN CRIMINAL JUSTICE

INVESTIGATING WEB 2.0

Thessaloniki, 23-24 May 2024

FACE-TO-FACE

EXCELLENCE IN EUROPEAN LAW

Speakers

Philip Anderson, Senior Lecturer, Computer and Information Sciences Department, Northumbria University, Newcastle

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

Timothy De Groot, Belgian Federal Police, Brussels

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

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

Christos Karagiannis, Prosecutor, Court of First Instance, Larissa

Sapfo Katsanaki, Prosecutor, Seconded National Expert (SNE), EPPO, Luxembourg

Eleni Papadopoulou, Prosecutor, Economic Crime Prosecution Office, Athens

Alikakos Petros, Head of the Court of First Instance, Hellenic School of Judges, Thessaloniki

Dario Vrčković, Digital Forensic Consultant, INsig2, Zagreb

With the support of the European Union

Key topics

- Technical issues (internet caches, proxy servers, encryption, deep/dark web, etc.)
- Legal issues (evaluation of the search results, reliability and credibility of authentication, search across jurisdictions)
- Challenges posed by websites, social networks, emails, clouds, text messaging and other computer-generated or stored documents
- Presenting internet searches in court: prosecution and defence perspectives
- Internet search results in court: a new evidentiary frontier for the judge?

Language
English

Event number
324DT07

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

ΕΣΔΙ
NATIONAL SCHOOL OF THE JUDICIARY

european.law

POST-COVID CHALLENGES IN CRIMINAL JUSTICE

Thursday, 23 May 2024

09:00 Arrival and registration of participants

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

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

This Part aims to introduce participants to the concepts around the internet and its supporting tools for investigation/research. It will make participants aware of the sources of evidence available to them in online investigations. The objective is to improve their ability to work with the current internet technologies

Chair: Laviero Buono

09:45 **Internet anatomy and architecture**

- Understanding the internet and associated technology
- IPs, proxy servers, encryption issues
- Effective use of the internet as a fraud investigation tool
- Search engines, meta browsers, deep web & people search techniques

Philip Anderson

10:45 Discussion

11:00 Break

11:30 **Computer forensics in the "Cloud"**

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

Seanpaul Gilroy

12:30 Discussion

12:45 Lunch

PART II: CRIMINALS' NEW *MODI OPERANDI* AND (MIS)USE OF CRYPTOCURRENCIES

The COVID-19 pandemic has altered criminals' modi operandi, leading to a significant increase in offences involving cybercrime and online criminal activities. This session will show how internet-based criminals have had more opportunities to hit, and isolation has made people more vulnerable. Participants will gain an insight into these new forms of crimes. The experts will present real-life examples, case studies and tool demonstrations in order to illustrate the key concepts covered.

Chair: Philip Anderson

13:45 **Addressing new (post)-Covid pandemic challenges – criminals' *new modi* operandi: cybercrime, ransomware, child sexual abuse and non-cash payment fraud**
Rainer Franosch

14:30 Discussion

14:45 **The collection of evidence located abroad and the challenges of transborder access to data**

- Search across jurisdictions / devices seized
- Transborder access to data
- European enforcement challenges in the online context
- Shortcomings and remedies

Sapfo Katsanaki

Objective

The objective of this event is to help legal practitioners tackle the challenges and difficulties linked to online investigations. The seminar will provide participants with a thorough understanding of the internet's architecture and key concepts. It will then analyse the legal challenges related to digital investigations, enabling participants to grasp the complex issues related to admissibility of e-evidence in court, with a special focus on internet searches.

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 EU Member States.

Venue

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

CPD

ERA's programmes meet the standard requirements for recognition as Continuing Professional Development (CPD). Participation in the full programme of this event corresponds to **8 CPD hours**.
A certificate of participation for CPD purposes with indication of the number of training hours completed will be issued on request. CPD certificates must be requested at the latest 14 days after the event.

15:15 Discussion

15:30 Break

16:00 **Internet-related crimes, digital evidence and cloud forensics: contemporary legal challenges and the power of disposal**

- Cloud storage and cloud forensics
- Power of disposal
- Case studies

Christos Karagiannis

16:30 Discussion

16:45 End of first day

19:30 Dinner offered by the organisers

Friday, 24 May 2024

PART III: ONLINE INVESTIGATIONS AND HANDLING OF E-EVIDENCE – BEST PRACTICES

This Part will illustrate the sorts of legal disputes that can arise involving digital forensics investigations and electronic evidence, i.e. the legal, practical and technical problems that judges, prosecutors and lawyers in private practice are confronted with in criminal proceedings where e-evidence is collected, analysed and ultimately presented in court.

Chair: Rainer Franosch

09:30 **Digital evidence collection: Open Source Intelligence (OSINT)**

- Introduction and the role of OSINT
- Efficient dialogue with searching engines
- Use-case scenarios and OSINT tools
- Live case demonstration

Dario Vrčković

10:15 Discussion

10:30 **Technical insights for the preparation, identification and preservation phase**

- The importance of the chain of custody in handling the evidence
- Case studies

Timothy De Groot

11:15 Break

11:45 **e-Evidence in child sexual abuse cases**

Eleni Papadopoulou

12:15 Discussion

12:30 End of seminar and 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

12-13 March 2024 | Online
Social Network Investigations From "Likes" to Evidence

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

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

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

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

Thessaloniki, 23-24 May 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 **15 January 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 Greece: participants can calculate the contribution to which they will be entitled on the European Commission website, Table 2 (https://era-comm.eu/go/calculator). The distance should be calculated from their place of work to the seminar location, *(in case of Bulgarian participants the amounts for Inter-Member States return journeys between 50 and 400 km is fixed at € 37, please consult p.11 on https://era-comm.eu/go/unit-cost-decision-travel).*

7. For those travelling within Greece, the contribution for travel is fixed at €36 (for a distance between 50km and 400km). Please note that no contribution will be paid for travel under 50km. For more information, please consult p.10 on https://era-comm.eu/go/unit-cost-decision-travel

8. Accommodation costs: international participants 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" online: **www.era.int/?132560&en**

Venue

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

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

Other EU criminal justice documents

A) The institutional framework for criminal justice in the EU

A1) Main treaties and conventions

A1-03	Consolidated version of the Treaty on the functioning of the European Union, art. 82-86 *(OJ C 326/47; 26.10.2012)*
A1-04	Consolidated Version of the Treaty on the European Union, art. 9-20 *(OJ C326/13;, 26.10.2012)*
A1-05	Charter of fundamental rights of the European Union *(OJ. C 364/1; 18.12.2000)*
A1-06	Explanations relating to the Charter of Fundamental Rights *(2007/C 303/02)*
A1-07	Convention implementing the Schengen Agreement of 14 June 1985 *(OJ L 239; 22.9.2000, P. 19)*

A2) Court of Justice of the European Union

A2-01	Court of Justice of the European Union: Presentation of the Court
A2-02	European Parliament Fact Sheets on the European Union: Competences of the Court of Justice of the European Union, April 2023
A2-03	Regulation (EU, Euratom) 2019/629 of the European Parliament and of the Council of 17 April 2019 amending Protocol No 3 on the Statute of the Court of Justice of the European Union, OJ L 111, 17 April 2019
A2-04	Consolidated Version of the Statute of the Court of Justice of the European Union (01 August 2016)
A2-05	Consolidated version of the Rules of Procedure of the Court of Justice (25 September 2012)

A3) European Convention on Human Rights (ECHR)

A3-01	Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 together with additional protocols No. 4, 6, 7, 12 and 13, Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11, 14 and 15, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, Council of Europe
A3-02	Guide on the case-law of the European Convention on Human Rights: European Union law in the Court's case-law, Council of Europe, updated on 31 August 2022
A3-03	Case of Grzeda v. Poland (Application no. 43572/18), Strasbourg, 15 March 2022
A3-04	Case of Mihalache v. Romania [GC] (Application no. 54012/10), Strasbourg, 08 July 2019
A3-05	Case of Altay v. Turkey (no. 2) (Application no. 11236/09), Strasbourg, 09 April 2019
A3-06	Case Beuze v. Belgium (Application no. 71409/10), Strasbourg, 09 November 2018
A3-07	Case of Vizgirda v. Slovenia (Application no. 59868/08), Strasbourg, 28 August 2018
A3-08	Case of Şahin Alpay v. Turkey (Application no. 16538/17), Strasbourg, 20 March 2018
A3-09	Grand Chamber Hearing, Beuze v. Belgium [GC] (Application no. 71409/10), Strasbourg, 20 December 2017
A3-10	Case of Blokhin v. Russia (Application no. 47152/06), Judgment European Court of Human Rights, Strasbourg, 23 March 2016

A3-11	Case of A.T. v. Luxembourg (Application no. 30460/13), Judgment European Court of Human Rights, Strasbourg, 09 April 2015
A3-12	Case of Blaj v. Romania (Application no. 36259/04), Judgment European Court of Human Rights, Strasbourg, 08 April 2014
A3-13	Case of Boz v. Turkey (Application no. 7906/05), Judgment European Court of Human Rights, Strasbourg, 01 October 2013 (FR)
A3-14	Case of Pishchalnikov v. Russia (Application no. 7025/04), Judgment European Court of Human Rights, Strasbourg, 24 October 2009
A3-15	Case of Salduz v. Turkey (Application no. 36391/02), Judgment, European Court of Human Rights, Strasbourg, 27 November 2008

A4) Brexit

A4-01	Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part *(OJ L 149, 30.4.2021)*
A4-02	Eurojust: Judicial cooperation in criminal matters between the European Union and the United Kingdom from 1 January 2021, 1 January 2021
A4-03	Draft text of the Agreement on the New Partnership between the European Union and the United Kingdom (UKTF 2020-14), 18 March 2020
A4-04	Draft Working Text for an Agreement on Law enforcement and Judicial Cooperation in Criminal Matters
A4-05	The Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 (2019/742), 28th March 2019
A4-06	Brexit next steps: The European Arrest Warrant, House of Commons, 20 February 2020
A4-07	Brexit next steps: The Court of Justice of the EU and the UK, House of Commons, 7 February 2020
A4-08	The Law Society, “Brexit no deal: Criminal Justice Cooperation”, London, September 2019
A4-09	European Commission, Factsheet, „A „No-deal“-Brexit: Police and judicial cooperation”, April 2019
A4-10	CEPS: Criminal Justice and Police Cooperation between the EU and the UK after Brexit: Towards a principled and trust-based partnership, 29 August 2018
A4-11	Policy paper: The future relationship between the United Kingdom and the European Union, 12 July 2018
A4-12	House of Lords, Library Briefing, Proposed UK-EU Security Treaty, London, 23 May 2018
A4-13	HM Government, Technical Note: Security, Law Enforcement and Criminal Justice, May 2018
A4-14	LSE-Blog, Why Britain´s habit of cherry-picking criminal justice policy cannot survive Brexit, Auke Williams, London School of Economics and Political Science, 29 March 2018
A4-15	House of Commons, Home Affairs Committee, UK-EU Security Cooperation after Brexit, Fourth Report of Session 2017-19, London, 21 March 2018
A4-16	HM Government, Security, Law Enforcement and Criminal Justice, A future partnership paper
A4-17	European Criminal Law after Brexit, Queen Mary University London, Valsamis Mitsilegas, 2017
A4-18	House of Lords, European Union Committee, Brexit: Judicial oversight of the European Arrest Warrant, 6th Report of Session 2017-19, London, 27 July 2017

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

B) Mutual legal assistance

B1) Legal framework

B1-01	Council Act of 16 October 2001 establishing in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union *(2001/C 326/01), (OJ C 326/01; 21.11.2001,P. 1)*
B1-02	Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union *(OJ C 197/1; 12.7.2000, P. 1)*
B1-03	Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the surrender procedure between the Member States of the European Union and Iceland and Norway (OJ L 292, 21.10.2006, p. 2–19)
B1-04	Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters *(Strasbourg, 8.XI.2001*)
B1-05	Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters *(Strasbourg, 17.III.1978*)
B1-06	European Convention on Mutual Assistance in Criminal Matters *(Strasbourg, 20.IV.195*9)
B1-07	Third Additional Protocol to the European Convention on Extradition (*Strasbourg, 10.XI.2010*)
B1-08	Second Additional Protocol to the European Convention on Extradition *(Strasbourg, 17.III.1978)*
B1-09	Additional Protocol to the European Convention on Extradition (*Strasbourg, 15.X.1975*)
B1-10	European Convention on Extradition (*Strasbourg, 13.XII.1957*)

B2) Mutual recognition: the European Arrest Warrant

B2-01	Proposal for a Regulation of the European Parliament and of the Council on the transfer of proceedings in criminal matters, COM/2023/185 final, 5 April 2023
B2-02	European Parliament resolution of 20 January 2021 on the implementation of the European Arrest Warrant and the surrender procedures between Member States (2019/2207(INI)), *(OJ C 456, 10.11.2021)*
B2-03	Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial *(OJ L 81/24; 27.3.2009)*
B2-04	Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States *(OJ L 190/1; 18.7.2002, P. 1)*
B2-05	Case law by the Court of Justice of the European Union on the European Arrest Warrant – Overview, Eurojust, 15 March 2020

B2-06	Case C-142/22, OE, Judgment of the Court (Second Chamber), 6 July 2023
B2-07	Case C-699/21, E.D.L, Judgment of the Court (Grand Chamber), 18 April 2023
B2-08	Joined Cases C-514/21 and C-515/21, LU and PH, Judgment of the Court (Fourth Chamber), 23 March 2023
B2-09	Case C-158/21, Puig Gordi and Others, Judgment of the Court (Grand Chamber), 31 January 2023
B2-10	Case C-168/21, Procureur général près la cour d'appel d'Angers, Judgment of the Court (Third Chamber), 14 July 2022
B2-11	Joined Cases C-562/21 PPU and C-563/21 PPU, Openbaar Ministerie (Tribunal établi par la loi dans l'État membre d'émission), Judgment of the Court (Grand Chamber), 22 February 2022
B2-12	Case C-649/19, Spetsializirana prokuratura (Déclaration des droits), Judgement of the Court (Fifth Chamber), 28 January 2021
B2-13	Case C-414/20 PPU, MM, Judgment of the Court (Third Chamber), 13 January 2021
B2-14	Joined Cases C-354/20 PPU and C-412/20 PPU, Openbaar Ministerie (Indépendance de l'autorité judiciaire d'émission), Judgement of the Court (Grand Chamber), 17 December 2020
B2-15	Case C-416/20 PPU, Generalstaatsanwaltschaft Hamburg, Judgement of the Court (Fourth Chamber), 17 December 2020
B2-16	Case C-584/19, A and Others, Judgement of the Court (Grand Chamber), 8 December 2020
B2-17	Case C-510/19, AZ, Judgement of the Court (Grand Chamber), 24 November 2020
B2-18	Case C-717/18, X (European arrest warrant – Double criminality) Judgement of the Court of 3 March 2020
B2-19	Case C-314/18, SF Judgement of the Court of 1 March 2020
B2-20	Joined Cases C-566/19 PPU (JR) and C-626/19 PPU (YC), Opinion of AG Campos Sánchez-Bordona, 26 November 2019
B2-21	Case C-489/19 PPU (NJ), Judgement of the Court (Second Chamber) of 09 October 2019
B2-22	Case 509/18 (PF), Judgement of the Court (Grand Chamber), 27 May 2019
B2-23	Joined Cases C-508/18 (OG) and C-82/19 PPU (PI), Judgement of the Court (Grand Chamber), 24 May 2019
B2-24	The Guardian Press Release: Dutch court blocks extradition of man to 'inhumane' UK prisons, 10 May 2019
B2-25	Case 551/18, IK, Judgement of the Court of 06 December 2018 (First Chamber)
B2-26	CJEU Press Release No 141/18, Judgement in Case C-207/16, Ministerio Fiscal, 2 October 2018
B2-27	CJEU Press Release No 135/18, Judgement in Case C-327/18 PPU RO, 19 September 2019
B2-28	Case C-268/17, AY, Judgement of the Court of 25 July 2018 (Fifth Chamber)
B2-29	Case C-220/18 PPU, ML, Judgement of the Court of 25 July 2018 (First Chamber)
B2-30	Case C-216/18 PPU, LM, Judgement of the Court of 25 July 2018 (Grand Chamber)
B2-31	InAbsentiEAW, Background Report on the European Arrest Warrant - The Republic of Poland, Magdalena Jacyna, 01 July 2018
B2-32	Case C-571/17 PPU, Samet Ardic, Judgment of the court of 22 December 2017

B2-33	C-270/17 PPU, Tupikas, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-34	Case C-271/17 PPU, Zdziaszek, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-35	Case C-579/15, Popławski, Judgement of the Court (Fifth Chamber), 29 June 2017
B2-36	Case C-640/15, Vilkas, Judgement of the Court (Third Chamber), 25 January 2017
B2-37	Case C-477/16 PPU, Kovalkovas, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-38	Case C-452/16 PPU, Poltorak, Judgement of the Court (Fourth chamber), 10 November 2016
B2-39	Case C-453/16 PPU, Özçelik, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-40	Case C-294/16 PPU, JZ v Śródmieście, Judgement of the Court (Fourth Chamber), 28 July 2016
B2-41	Case C241/15 Bob-Dogi, Judgment of the Court (Second Chamber) of 1 June 2016
B2-42	C-108/16 PPU Paweł Dworzecki, Judgment of the Court (Fourth Chamber) of 24 May 2016
B2-43	Cases C-404/15 Pál Aranyosi and C-659/15 PPU Robert Căldăraru, Judgment of 5 April 2016
B2-44	Case C-237/15 PPU Lanigan, Judgment of 16 July 2015 (Grand Chamber)
B2-45	Case C-168/13 PPU *Jeremy F / Premier ministre*, Judgement of the court (Second Chamber), 30 May 2013
B2-46	Case C-399/11 *Stefano Melloni v Ministerio Fiscal*, Judgment of of 26 February 2013
B2-47	Case C-396/11 Ciprian Vasile Radu, Judgment of 29 January 2013
B2-48	C-261/09 Mantello, Judgement of 16 November 2010
B2-49	C-123/08 Wolzenburg, Judgement of 6 October 2009
B2-50	C-388/08 Leymann and Pustovarov, Judgement of 1 December 2008
B2-51	C-296/08 Goicoechea, Judgement of 12 August 2008
B2-52	C-66/08 Szymon Kozlowski, Judgement of 17 July 2008

B3) Mutual recognition: freezing and confiscation and asset recovery

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

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

B4) Mutual recognition: Convictions

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

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

B5-01	Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *(OJ L 191, 28.7.2023)*
B5-02	Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, *(OJ L 191, 28.7.2023)*
B5-03	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *(Brussels, 20.7.2021, COM(2021) 409 final)*
B5-04	The European Law Blog, „E-Evidence: The way forward. Summary of a Workshop held in Brussels on 25 September 2019, Theodore Christakis, 06 November 2019
B5-05	Joint Note of Eurojust and the European Judicial Network on the Practical Application of the European Investigation Order, June 2019
B5-06	European Commission, Press Release, „Security Union: Commission recommends negotiating international rules for obtaining electronic evidence", Brussels, 05 February 2019
B5-07	EURCRIM, "The European Commission‘s Proposal on Cross Border Access to e-Evidence – Overview and Critical Remarks" by Stanislaw Tosza, Issue 4/2018, pp. 212-219
B5-08	Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, Brussels, 05 February 2019
B5-09	Annex to the Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, Brussels, 05 February 2019
B5-10	Fair Trials, Policy Brief, „The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters", October 2018
B5-11	ECBA Opinion on European Commission Proposals for: (1) A Regulation on European Production and Preservation Orders for electronic evidence & (2) a Directive for harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, Rapporteurs: Stefanie Schott (Germany), Julian Hayes (United Kingdom)
B5-12	Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final, Strasbourg, 17 April 2018
B5-13	Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Strasbourg, 17 April 2018

B5-14	Non-paper from the Commission services: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward *(8 June 2017)*
B5-15	Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace *(7 December 2016)*
B5-16	ENISA 2014 - Electronic evidence - a basic guide for First Responders (Good practice material for CERT first responders)
B5-17	Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130/1; 1.5.2014)
B5-18	Guidelines on Digital Forensic Procedures for OLAF Staff" (Ref. Ares(2013)3769761 - 19/12/2013, 1 January 2014
B5-19	ACPO Good Practice Guide for Digital Evidence *(March 2012)*
B5-20	Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters *(OJ L, 350/72, 30.12.2008*)
B5-21	Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence *(OJ L 196/45; 2.8.2003*)
B5-22	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce*) (Official Journal L 178/1, 17.7.2000)*
B5-23	Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions ensuring security and trust in electronic communication - Towards a European Framework for Digital Signatures and Encryption *(COM (97) 503)*, October 1997

B6) Criminal records, Interoperability

B6-01	Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726) (*OJ L135/85, 22.05.2019*)
B6-02	Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (*OJ L 135/85, 22.05.2019*)
B6-03	Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (*OJ L 135/27, 22.05.2019*)
B6-04	Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records

	Information System (ECRIS), and replacing Council Decision 2009/316/JHA, PE-CONS 87/1/18, Strasbourg, 17 April 2019
B6-05	Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States. *(COM/2017/0341 final, 29.06.2017)*
B6-06	Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States *(OJ L 93/23; 07.4.2009)*
B6-07	Council Decision on the exchange of information extracted from criminal records – Manual of Procedure *(6397/5/06 REV 5; 15.1.2007)*
B6-08	Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record *(OJ L 322/33; 9.12.2005)*

B7) Conflicts of jurisdiction – *Ne bis in idem*

B7-01	Case law by the Court of Justice of the European Union on the principle of ne bis in idem in criminal matters, Eurojust, April 2020 Case-law by the Court of Justice of the European Union on the Principle of ne bis in idem in Criminal Matters, Eurojust, December 2021
B7-02	Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings *(OJ L 328/42; 15.12.2009, P.42*)
B7-03	European Convention on the Transfer of Proceedings in Criminal Matters (Strasbourg, 15.V.1972)

C) Procedural guarantees in the EU

C-01	Report from the Commission to the European Parliament and the Council on the implementation of Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, COM/2023/44 final, 1 February 2023
C-02	Commission Recommendation (EU) 2023/681 of 8 December 2022 on procedural rights of suspects and accused persons subject to pre-trial detention and on material detention conditions, *(OJ L 86, 24.3.2023)*
C-03	FRA Report, Presumption of innocence and related rights – Professional perspectives, Luxembourg, 31 March 2021
C-04	FRA Report, Rights in practice: Access to a lawyer and procedural rights in criminal and European Arrest Warrant proceedings, Luxembourg, 27 September 2019
C-05	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third person informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, COM/2019/560 final, 26 September 2019
C-06	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and

	translation in criminal proceedings, COM/2018/857 final, 18 December 2018
C-07	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, COM/2018/858 final, 18 December 2018
C-08	Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings (OJ L 297/1, 4.11.2016)
C-09	Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings (OJ L 132 1; 21.5.2016)
C-10	Directive 2016/343 of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings (11.3.2016; OJ L 65/1)
C-11	Directive 2013/48/EU of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ L 294/1; 6.11.2013)
C-12	Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (1.6.2012; OJ L 142/1)
C-13	Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings *(OJ L 280/1; 26.10.2010*)
C-14	C-209/22 - Rayonna prokuratura Lovech, TO Lukovit (Fouille corporelle), 7 September 2023
C-15	C-660/21 - K.B. and F.S. (Relevé d’office dans le domaine pénal), 22 June 2023
C-16	C-430/22, C-468/22 - VB (Information du condamné par défaut), 8 June 2023
C-17	C-608/21 - Politseyski organ pri 02 RU SDVR, 25 May 2023
C-18	C-694/20 - Orde van Vlaamse Balies i in., 8 December 2022
C-19	C-348/21 - HYA and Others (Impossibilité d’interroger les témoins à charge), 8 December 2022
C-20	C-347/21 - DD (Réitération de l’audition d’un témoin), 15 September 2022
C-21	C-242/22 PPU - TL () and de traduction), 1 August 2022
C-22	C-564/19 - IS (Illégalité de l’ordonnance de renvoi), 23 November 2021
C-23	C-282/20 - ZX (Régularisation de l'acte d'accusation), 21 October 2021
C-24	C-649/19 - Spetsializirana prokuratura (Déclaration des droits), 28 January 2021
C-25	Case C-659/18, Judgement of the Court of 2 March 2020
C-26	Case C-688/18, Judgement of the Court of 3 February 2020
C-27	Case C467/18, Rayonna prokuratura Lom, Judgment of the Court of 19 September 2019
C-28	Case C-467/18 on directive 2013/48/EU on the right of access to a lawyer in criminal proceedings, EP, Judgement of the court (Third Chamber), 19. September 2019
C-29	Case C377/18, AH a. o., Judgment of the Court of 05 September 2019

C-30	Case C-646/17 on directive 2012/13/EU on the right to information in criminal proceedings, Gianluca Moro, Judgement of the Court (First Chamber), 13 June 2019
C-31	Case C-8/19 PPU, criminal proceedings against RH (presumption of innocence), Decision of the Court (First Chamber), 12. February 2019
C-32	Case C646/17, Gianluca Moro, Opinion of the AG Bobek, 05 February 2019
C-33	Case C-551/18 PPU, IK, Judgment of the Court (First Chamber), 6 December 2018
C-34	Case C-327/18 PPU, RO, Judgment of 19 September 2018 (First Chamber)
C-35	Case C-268/17, AY, Judgment of the Court (Fifth Chamber), 25 July 2018
C-36	Case C-216/18 PPU, LM, Judgment of 25 July 2018 (Grand Chamber)
C-37	Joined Cases C-124/16, C-188/16 and C-213/16 on Directive 2012/13/EU on the right to information in criminal proceedings Ianos Tranca, Tanja Reiter and Ionel Opria, Judgment of 22 March 2017 (Fifth Chamber)
C-38	Case C-439/16 PPU, Emil Milev (presumption of innocence), Judgment of the Court (Fourth Chamber), 27 October 2016
C-39	Case C-278/16 Frank Sleutjes ("essential document" under Article 3 of Directive 2010/64), Judgment of 12 October 2017 (Fifth Chamber)
C-40	C-25/15, István Balogh, Judgment of 9 June 2016 (Fifth Chamber)
C-41	Opinion of Advocate General Sharpston, delivered on 10 March 2016, Case C543/14
C-42	C-216/14 Covaci, Judgment of 15 October 2015 (First Chamber)

D) Approximating criminal law and Victims´ Rights

D1) Terrorism

D1-01	EU Centre of Expertise for Victims of Terrorism
D1-02	EU's Counter-Terrorism Coordinator
D1-03	Eurojust Meeting on Counter-Terrorism, 16-17 November 2022, Summary of Discussions, 05 April 2023
D1-04	Eurojust Casework on Counter-Terrorism: Insights 2020 – 2021, December 2021
D1-05	Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance), *(OJ L 172, 17.5.2021)*
D1-06	European Commission, EU Handbook on Victims of Terrorism, January 2021
D1-07	2019 Eurojust Report on Counter- Terrorism, 09 December 2020
D1-08	Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, 9 December 2020, COM(2020) 795 final
D1-09	Report from the Commission to the European Parliament and the Council based on Article 29(1) of Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, COM(2020) 619 final, Brussels, 30 September 2020
D1-10	Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social

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

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

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

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

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

D3) Cybercrime

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

	and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance), *(OJ L 333, 27.12.2022)*
D3-08	Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance), *(OJ L 333, 27.12.2022)*
D3-09	Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, *(COM/2022/454 final, 15 September 2022)*
D3-10	Internet Organised Crime Threat Assessment (IOCTA) 2021
D3-11	Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (Text with EEA relevance), *(OJ L 274, 30.7.2021)*
D3-12	European Commission, Public consultation on Fighting child sexual abuse: detection, removal and reporting of illegal content online, 11 February 2021
D3-13	European Judicial Cybercrime Network 9th Plenary Meeting - 2nd Outcome report 2020, 27 January 2021
D3-14	European Commission, Study on the retention of electronic communications non-content data for law enforcement purposes, Final report, September 2020
D3-15	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: EU strategy for a more effective fight against child sexual abuse, *(COM (2020) 607 final, Brussels, 24 July 2020)*
D3-16	Internet Organised Crime Threat Assessment (IOCTA) 2020
D3-17	Internet Organised Crime Threat Assement (IOCTA) 2019
D3-18	Special Eurobarometer 480, Report, “Europeans´ Attitudes towards Internet Security”, Brussels, March 2019
D3-19	Directive 2013/40/EU of the European Parliament and of the Council of 12 august 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Official Journal L 218/8 of 14.08.2013)
D3-20	Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA *(OJ L 335/; 17.12.2011*)
D3-21	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems *(OJ L 69/67; 16.3.2005*)
D3-22	Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography (*OJ L 13/44; 20.1.2004*)
D3-23	Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Strasbourg, 28.I.2003)
D3-24	Convention on Cybercrime (Budapest, 23.XI.2001)

D4) Protecting Victims´ Rights

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

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

E) Criminal justice bodies and networks

E1) European Judicial Network

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

E2) Eurojust

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

E3) Europol

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

E4) European Public Prosecutor's Office

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

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

F) Data Protection

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

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

G) Police Cooperation in the EU

G1) General

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

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

G2) Joint Investigation Teams (JITs)

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

Technical Issues and basic understanding of the Internet architecture and concepts

Using open-source intelligence to gather evidence online

PHILIP ANDERSON

ERA | THESSALONIKI, 23-24 MAY 2024

Co-funded by the European Union

Speaker Background

- Assistant Professor/Senior Lecturer @ Northumbria University.
- Over 17 years teaching digital forensics and incident response.
- 6 years teaching digital investigations and digital evidence to police officers on the Police Constable Degree Apprenticeship programme.
- Consulted with the European Union Agency for Cybersecurity (ENISA) from 2010 up until 2021 in identifying emerging and future ICT risks in the area of Information Security Risk Assessment and Management.
- My current research focuses on the application of artificial intelligence to digital forensic challenges.

Outline

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

(Post) COVID-19…cybercrime landscape

Europol - Internet Organised Crime Threat Assessment (IOCTA) 2023
https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

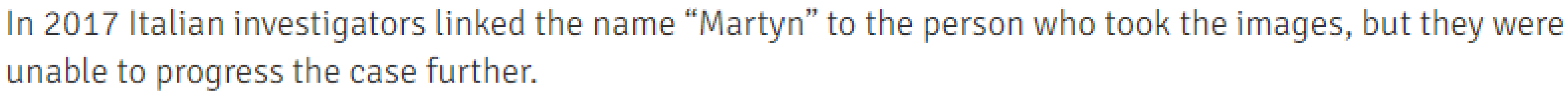
- **Cyber-dependant**
  - Ransomware
  - Mobile malware
  - DDoS for ransom (returning)

- **Cyber-enabled**
  - Child sexual abuse material
    - Increase via social media and online gaming platforms
    - P2P distribution increased
  - Phishing and social engineering
    - Increased in volume and sophistication
    - Dark web
      - Encrypted communication increasing

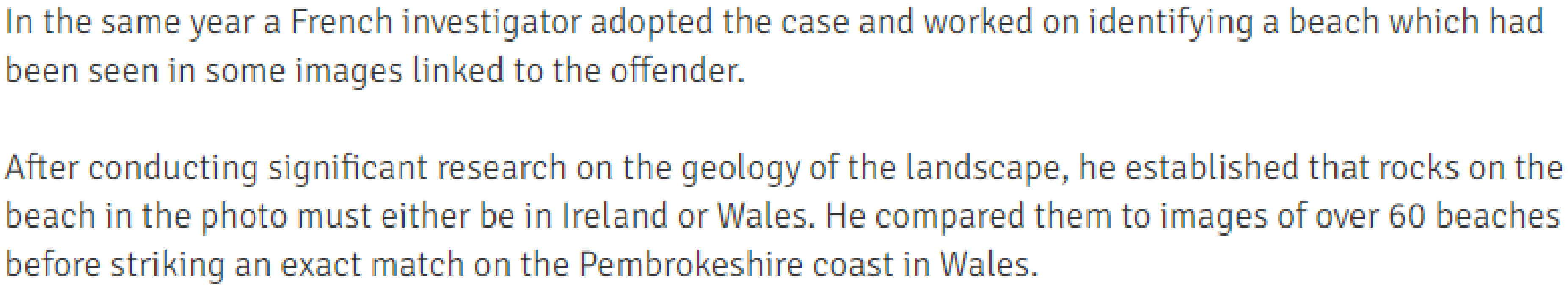
Example

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

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



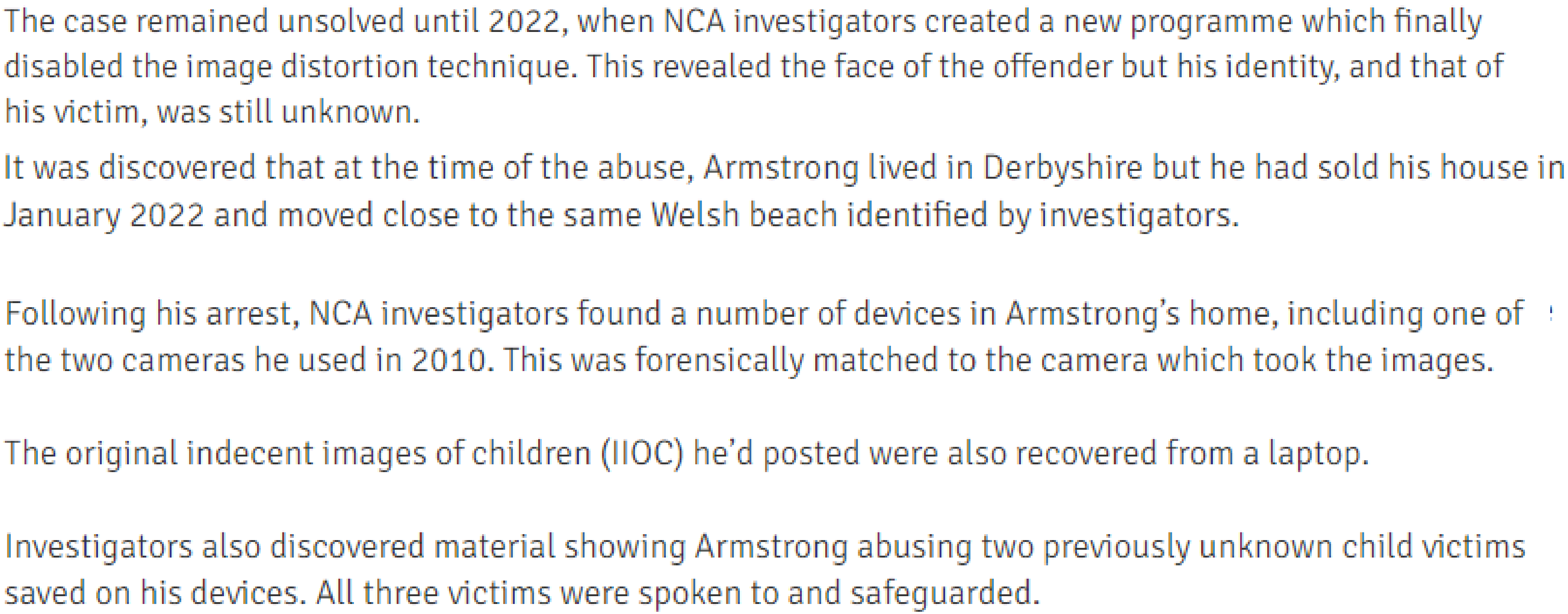
In 2017 Italian investigators linked the name “Martyn” to the person who took the images, but they were unable to progress the case further.



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

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

Example



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

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

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

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

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

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

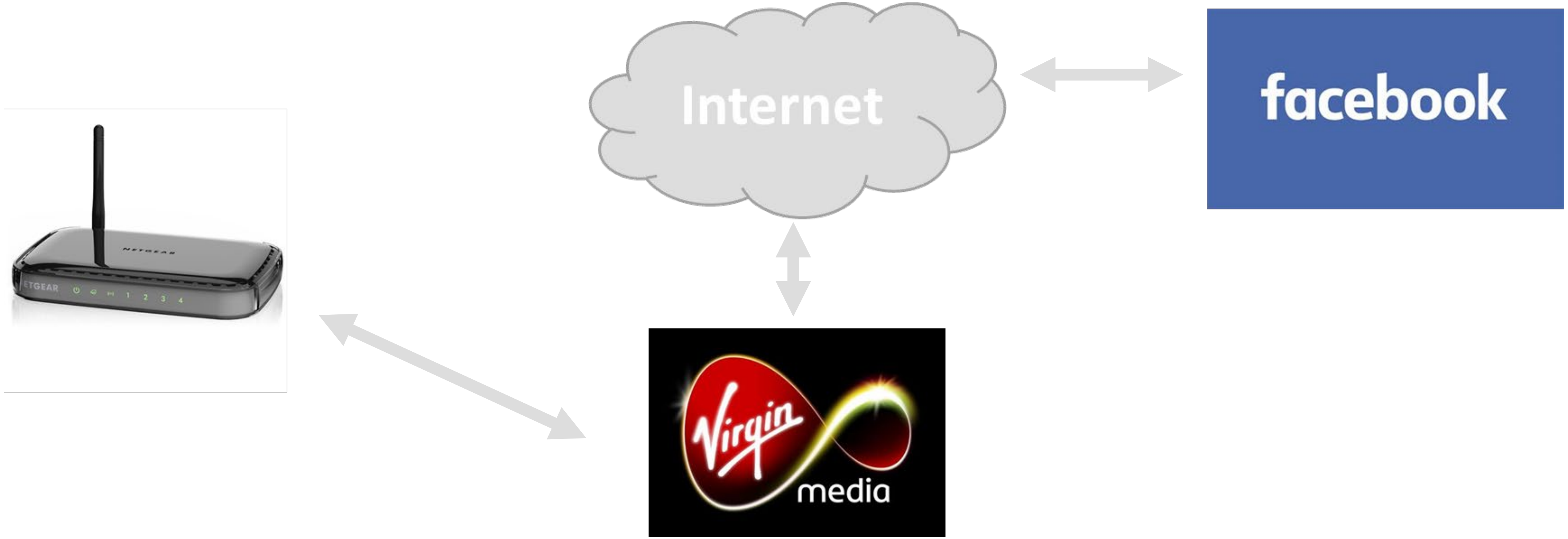
#1

Understanding the Internet and associated technologies

How does it work.

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

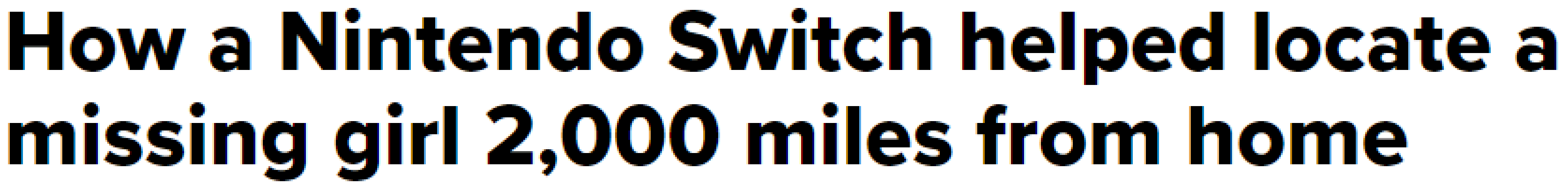
How does it work… Infrastructure



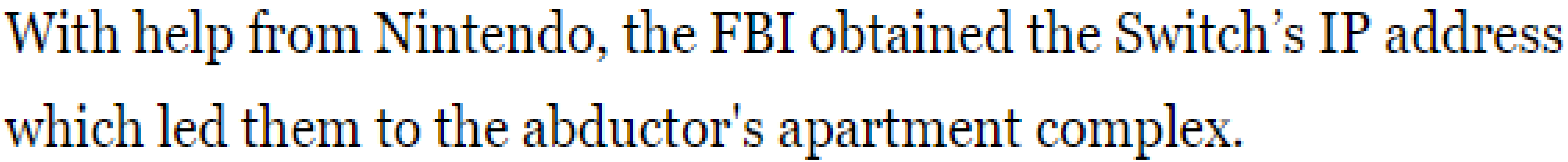
Internet Service Provider (ISP)

Example

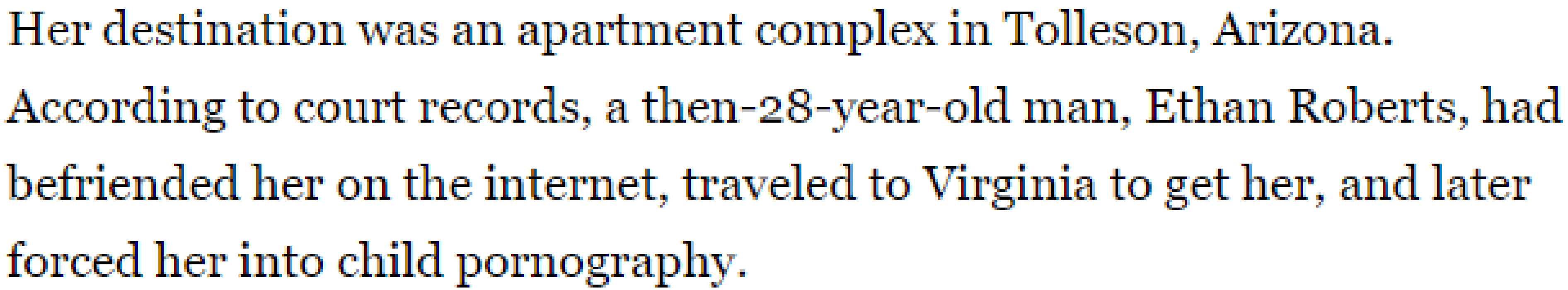
Example



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



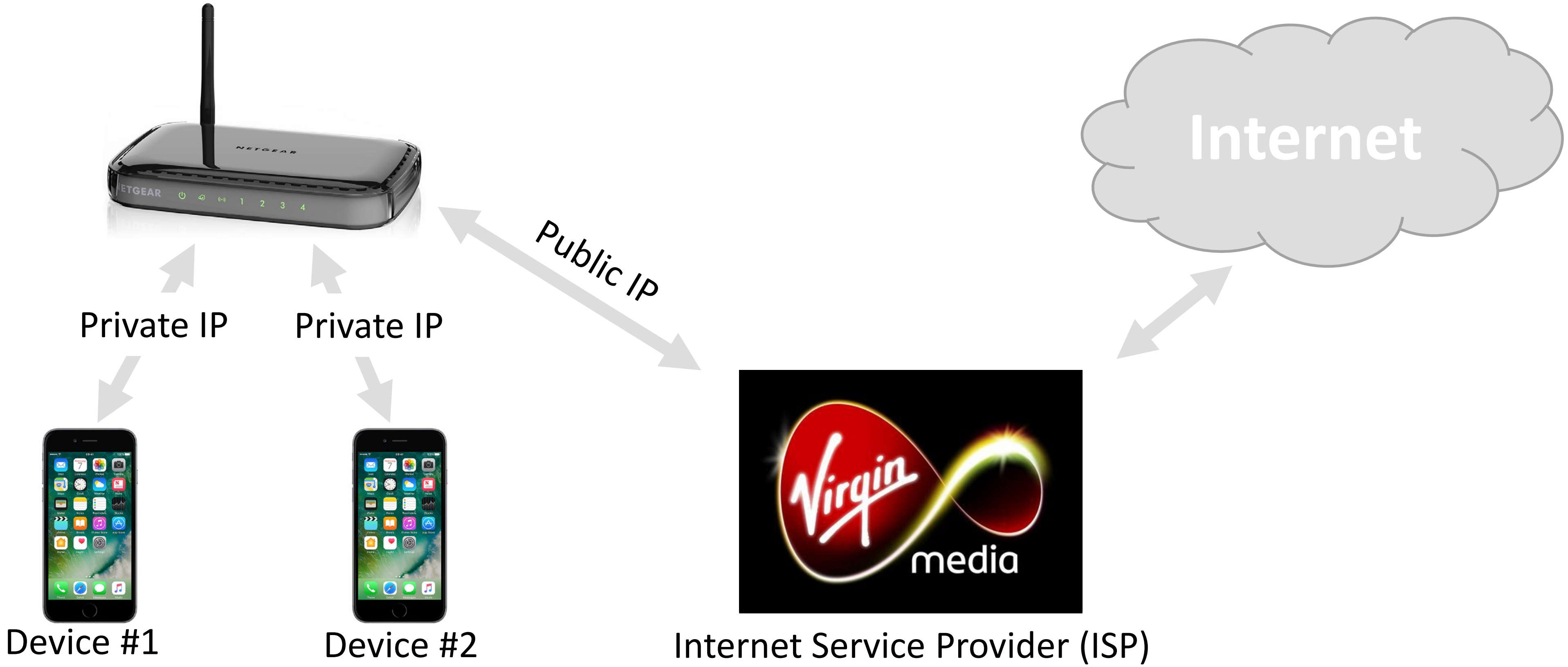
With help from Nintendo, the FBI obtained the Switch's IP address which led them to the abductor's apartment complex.

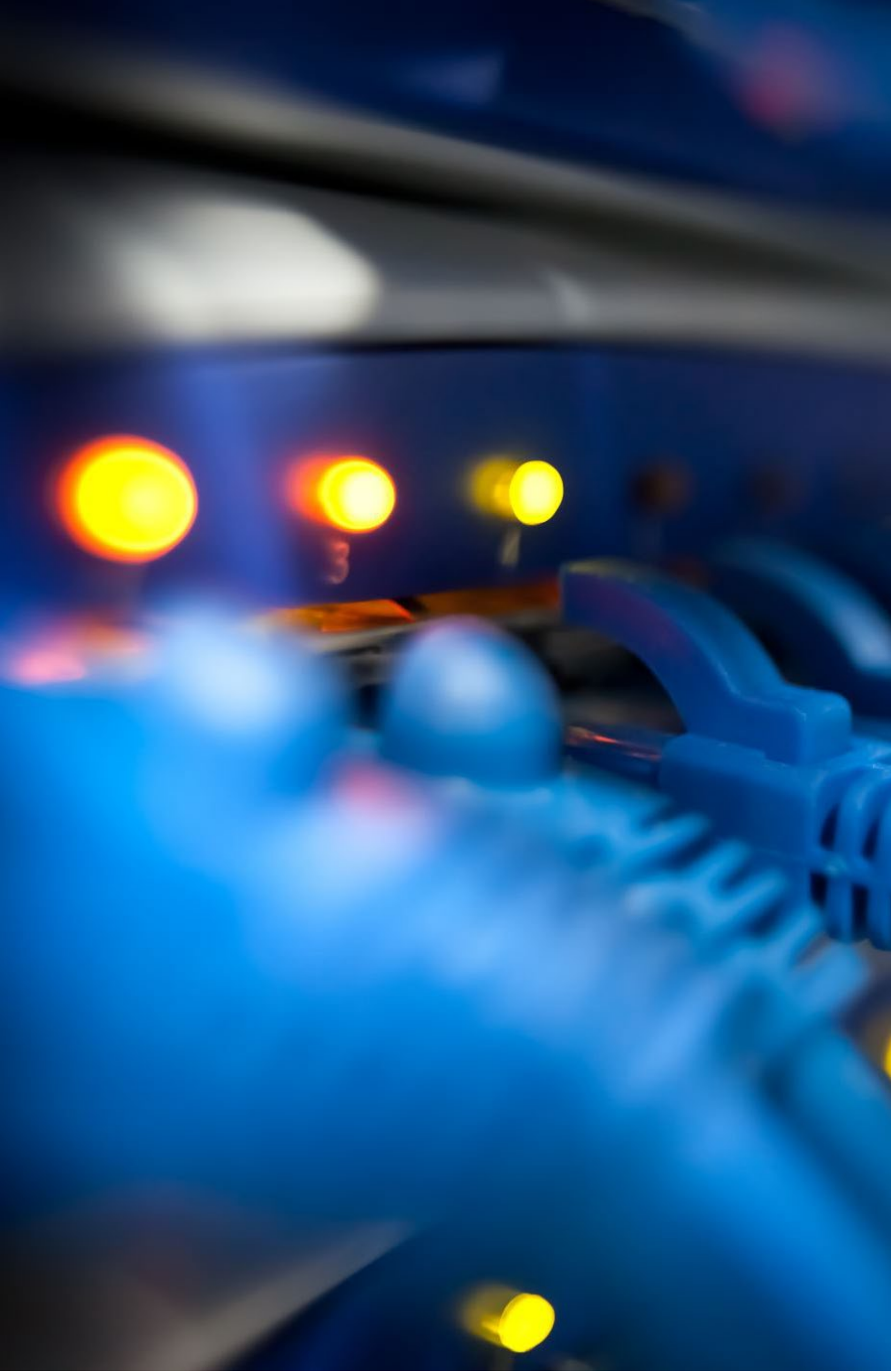


Her destination was an apartment complex in Tolleson, Arizona. According to court records, a then-28-year-old man, Ethan Roberts, had befriended her on the internet, traveled to Virginia to get her, and later forced her into child pornography.

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

How does it work… Public and Private IP

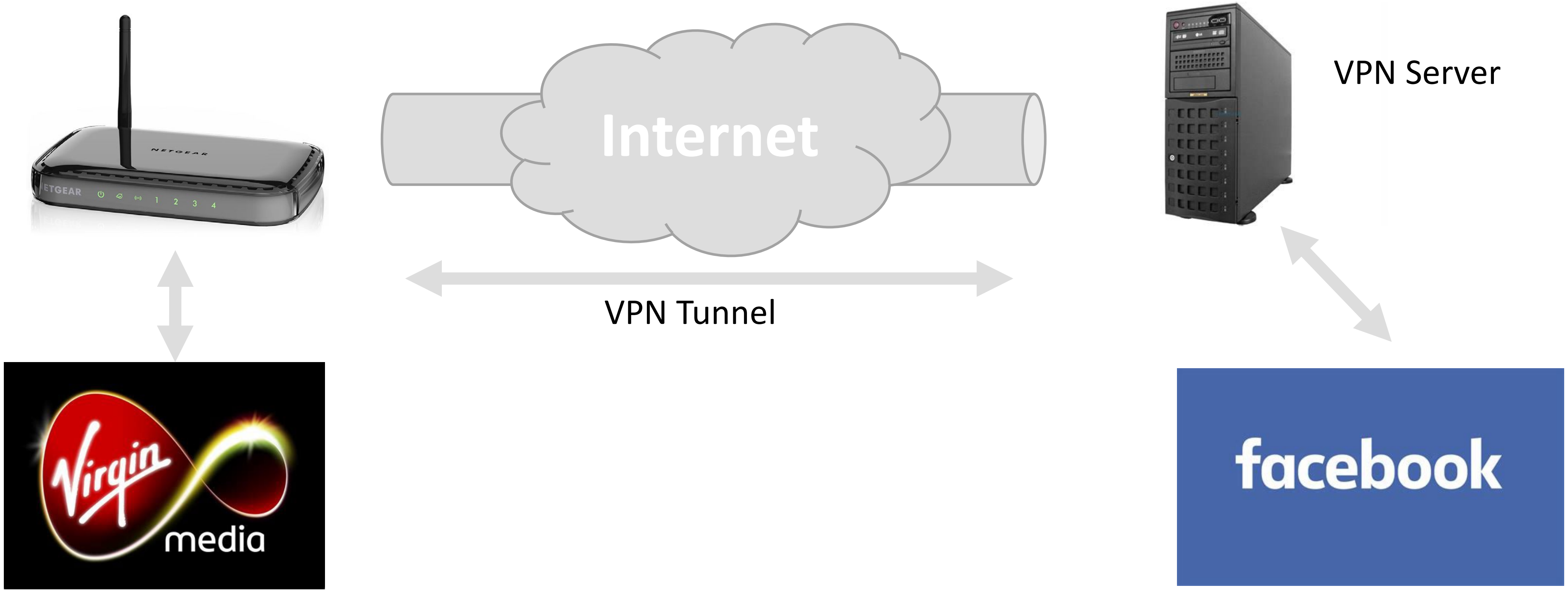




How does it work…Public and Private IP.

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

How does it work… Privacy | Anonymity



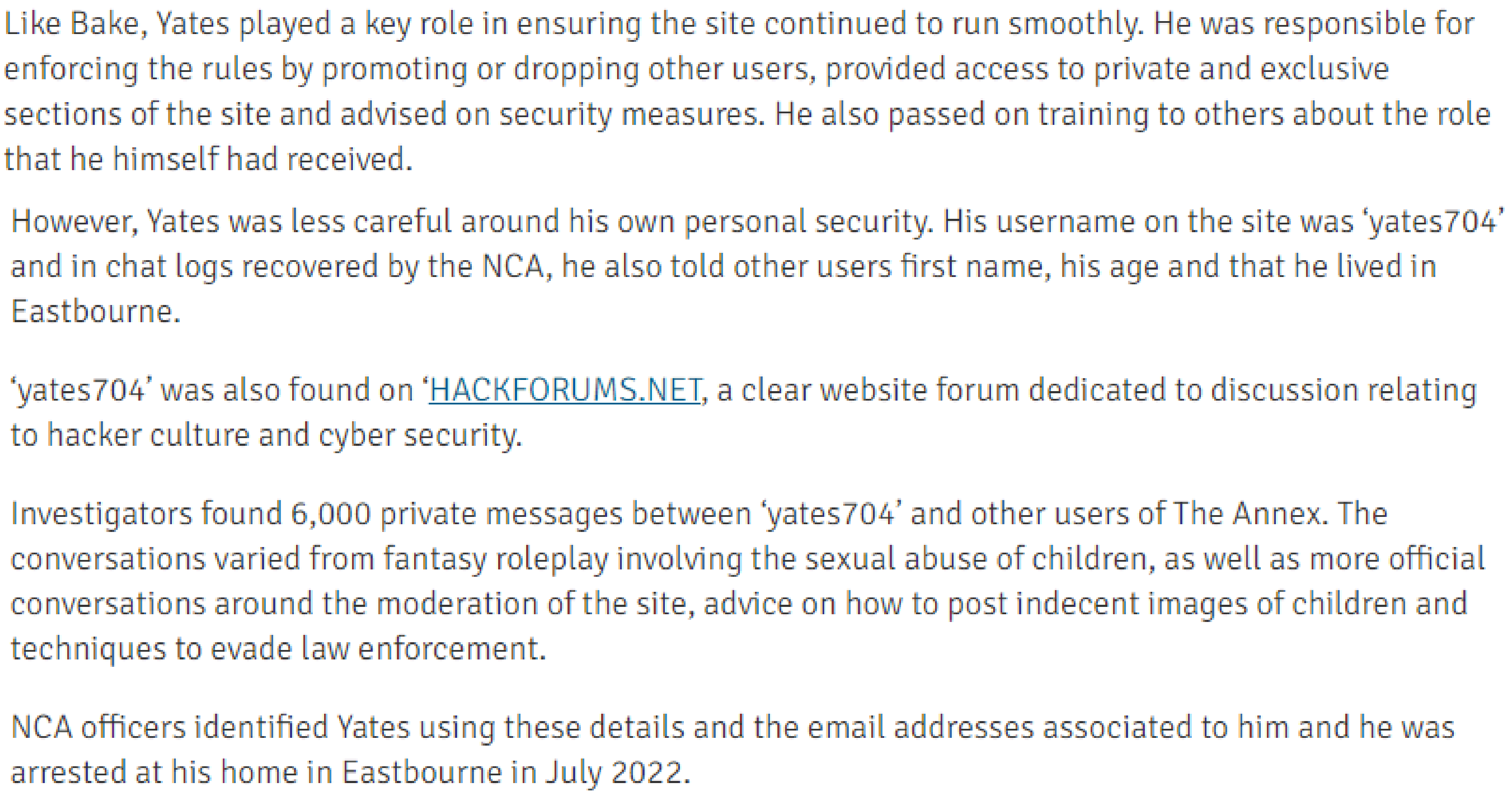
VPN Server

VPN Tunnel

Internet Service Provider (ISP)

VPN IP

Investigations… Dark Web | Email



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

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

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

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

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

impres

fore be

orcement detection,

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

#2

Effective use of the Internet as an investigation tool

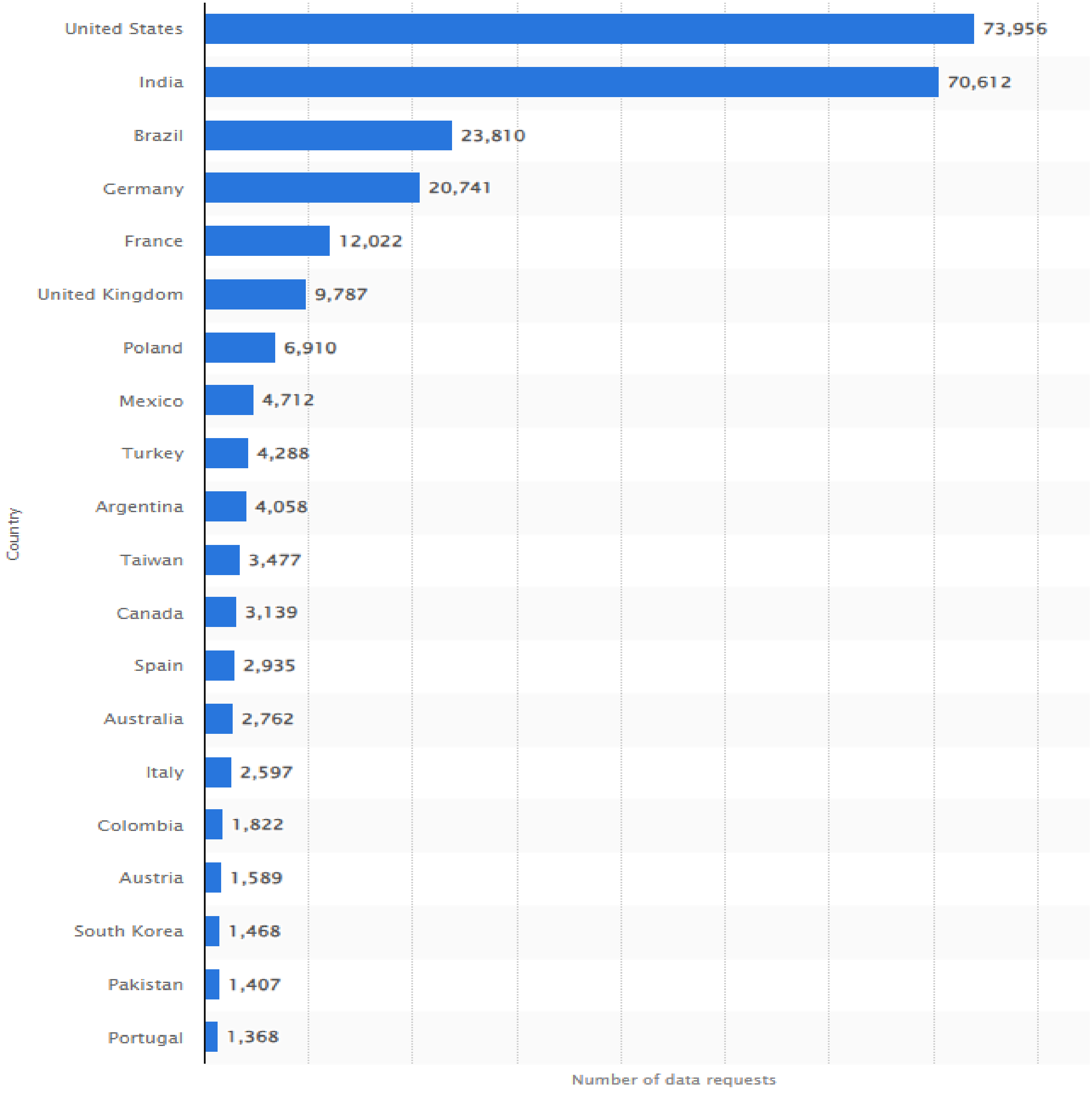
Investigations…

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

Investigations… Social media

- As of Jan 2024, 5.04 billion social media users from 5.35 billion Internet users[1]

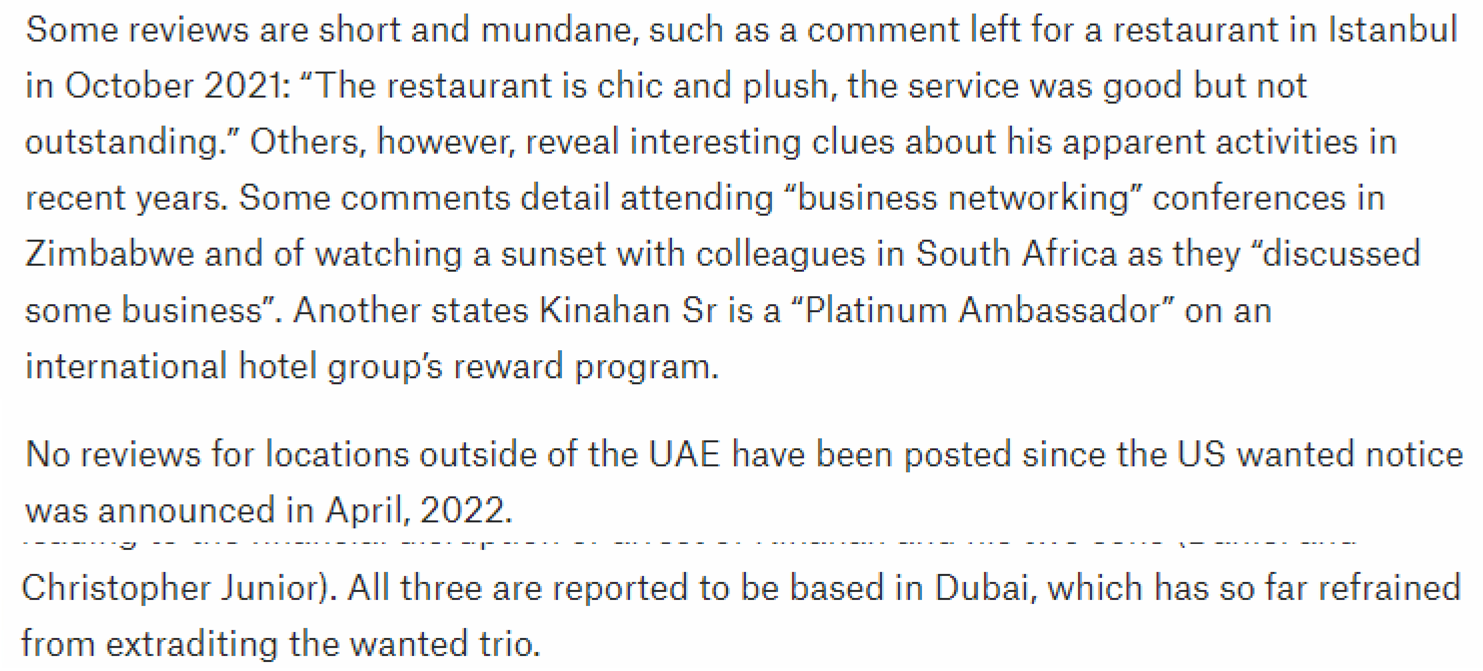
[1] Statista - https://www.statista.com/statistics/617136/digital-population-worldwide/



#1 Most popular social networks worldwide as of January 2024, ranked by number of monthly active users. Source: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

#2 Number of user data requests issued to Facebook by federal agencies and governments during 1st half 2023, by country (Dec 2023). Source: https://www.statista.com/statistics/287845/global-data-requests-from-facebook-by-federal-agencies-and-governments/

Investigations… Google Reviews



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

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

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

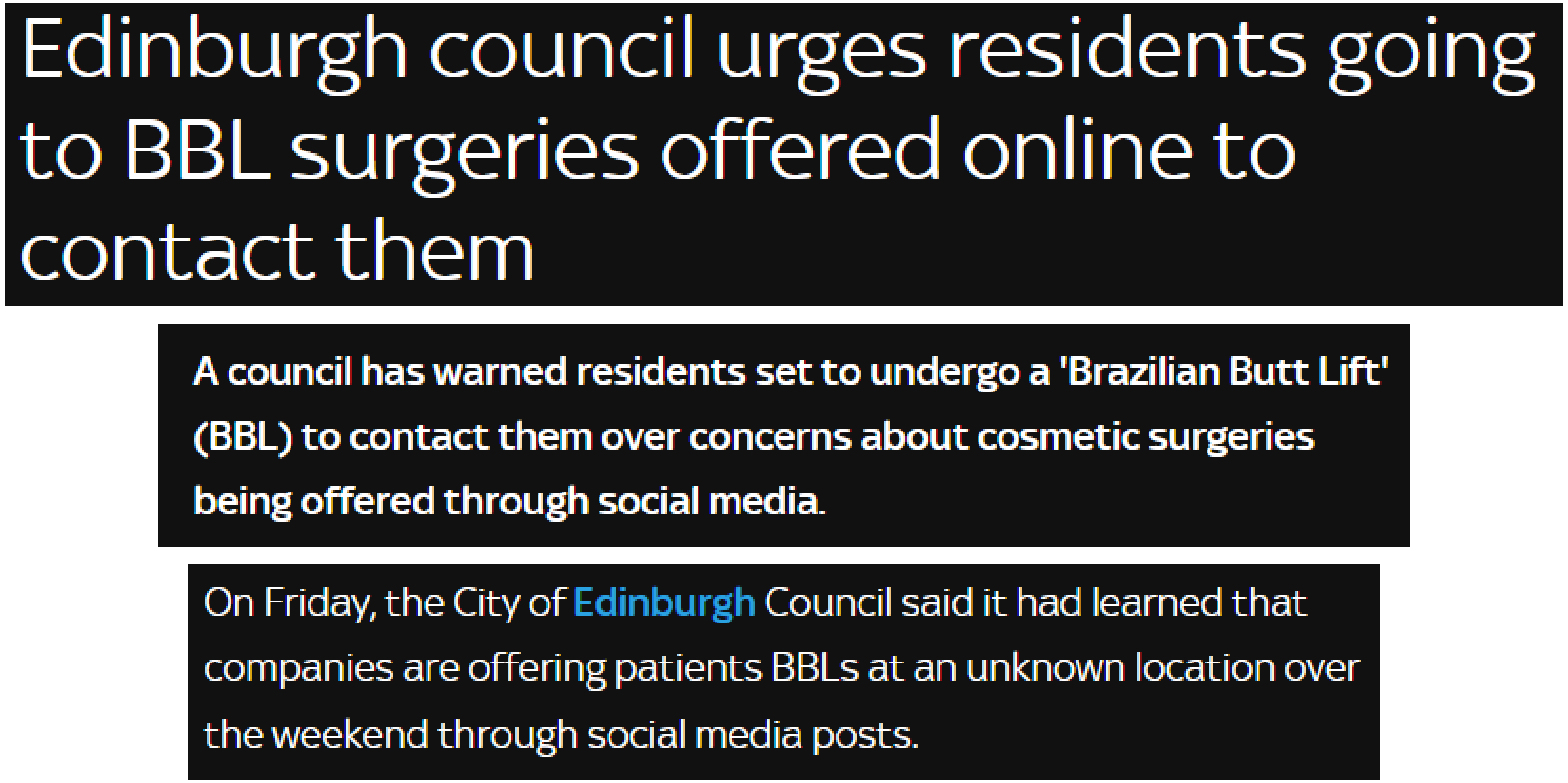
Source: https://www.bellingcat.com/news/2024/03/30/kinahan-cartel-wanted-narco-boss-exposes-whereabouts-by-posting-google-reviews/

Investigations… Social media

- “UK's gang scene glorified in flashy social media brags about criminal lifestyle”
- “Images of sports cars, flash clothing, wads of cash and expensive jewellery are often uploaded online to give a 'filtered illusion' of a high-end lifestyle...”
- “The social media posts portraying the life of a gangster are even said to be used as a way of recruiting new members…”

Source: https://www.mirror.co.uk/news/uk-news/uks-gang-scene-uncovered-social-16189451

Investigations… Social media



Edinburgh council urges residents going to BBL surgeries offered online to contact them

A council has warned residents set to undergo a 'Brazilian Butt Lift' (BBL) to contact them over concerns about cosmetic surgeries being offered through social media.

On Friday, the City of Edinburgh Council said it had learned that companies are offering patients BBLs at an unknown location over the weekend through social media posts.

Source: https://news.sky.com/story/edinburgh-council-urges-residents-going-to-bbl-surgeries-offered-online-to-contact-them-13123237

Other Investigations…

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

Investigations… considerations

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

Investigations… Legislation (UK)

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

Investigations… Ethics

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

#3

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

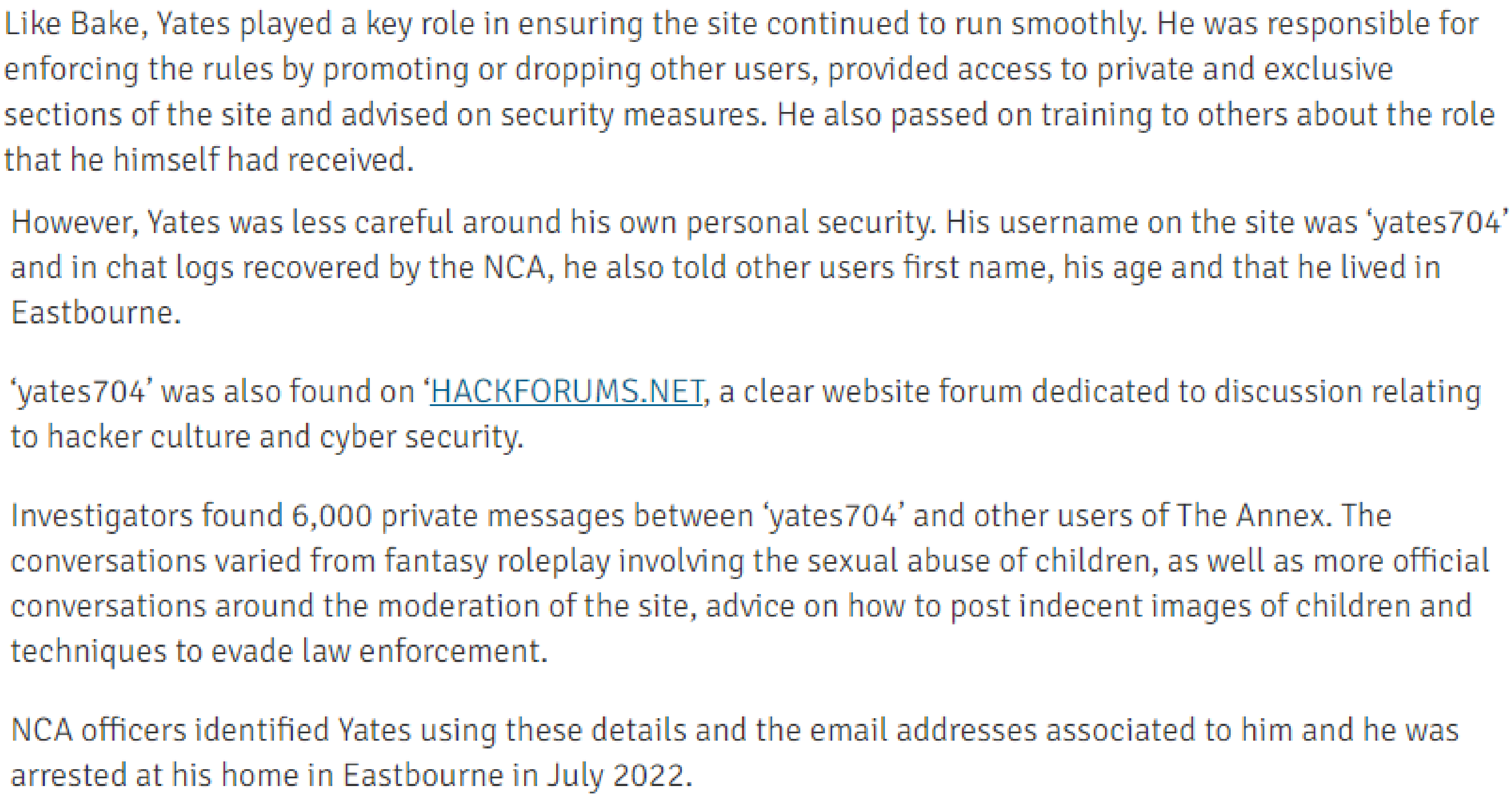
The Internet…

- Surface web
  - The section of the Internet that is being indexed by search engines
  - 4.59 billions pages (source: https://www.worldwidewebsize.com/)
  - Accessed via ‘standard’ browsers - Chrome, Mozilla Firefox, Opera, etc.
- Deep web
  - Not indexed
  - Accessed via username and passwords
  - Some data out of the Deep web may be picked up by search engines in the case of a data breach.
  - Accessed via ‘standard’ browsers - Chrome, Mozilla Firefox, Opera, etc.

The Internet…

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

Example



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

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

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

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

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

impres

fore be

orcement detection,

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

Methods… Information Sources

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

Methods… Information Gathering

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

Methods… Information sources

- General search engines
- National search engines
- Meta search engines
  - Results from multiple search engines
- Image, video and document search
- Reverse image search
- Geolocation

- Social Media networks
  - Facebook, Twitter, YouTube, Instagram, Snapchat
  - Weibo (China), VK (Russia)
- Blog search
- Newspaper searches
- Public records
- Business records
  - Government websites

- Transportation
- Doman names
- Internet archives
- People search engines
  - Name, Address, Phone, Email
  - IP Address

Methods… Tools

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

- Capturing the (online) evidence
  - Hunchly – web capture tool
    - Searching
    - Collecting and documenting
      - Timestamps and hashing
    - Audit trail
    - Secure cloud storage
    - Reporting

#4

Using open source intelligence to gather evidence online

Open Source… Methods

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

Open Source… Case Studies - Bellingcat

- Unravelling the Killing of Colombian Protester Lucas Villa - https://www.bellingcat.com/news/2021/12/06/unravelling-the-killing-of-colombian-protester-lucas-villa/
- Examined social media posts
- Analysed private CCTV footage

- Black Gold Burning: In Search Of South Sudan’s Oil Pollution - https://www.bellingcat.com/news/africa/2020/01/23/black-gold-burning-in-search-of-south-sudans-oil-pollution/
- Location of the spills was collected through social media research
- Data on the oil fields was gathered from various public sources

Open Source… Case Studies - Bellingcat

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

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

Open Source…

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

Open Source… Caution

- Avoid interaction with other people online
- Where required fictional accounts (https://www.osinttechniques.com/fictional-accounts.html)
- Only non-attributable computers
- Evidentially capture information

Additional Learning Resources

- Council of Europe ‘training and other materials on cybercrime and electronic evidence’ - https://www.coe.int/en/web/octopus/training

Thank you

Questions?

Philip Anderson

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

OPEN SOURCE TOOLS, COMPUTER FORENSICS IN THE "CLOUD"

Seanpaul Gilroy

Senior Digital Forensic Investigator

(POST)COVID CHALLENGES IN CRIMINAL JUSTICE:

Co-funded by the European Union

What will we discuss?

Overview of Open Source Investigations

Protecting your privacy during open source investigations

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

Geo-location tools for Open Source Investigations

Investigating Web 2.0 – social networking, blogs and online gaming

About Me

Senior Digital Forensic Investigator at Northumbria Police

- Manage a team of Digital Forensic Investigators
- Based in Newcastle Upon Tyne, England
- Worked in the field of Digital Forensics for 10 years

Deliver training inputs to both new and existing police officers on a regular basis:

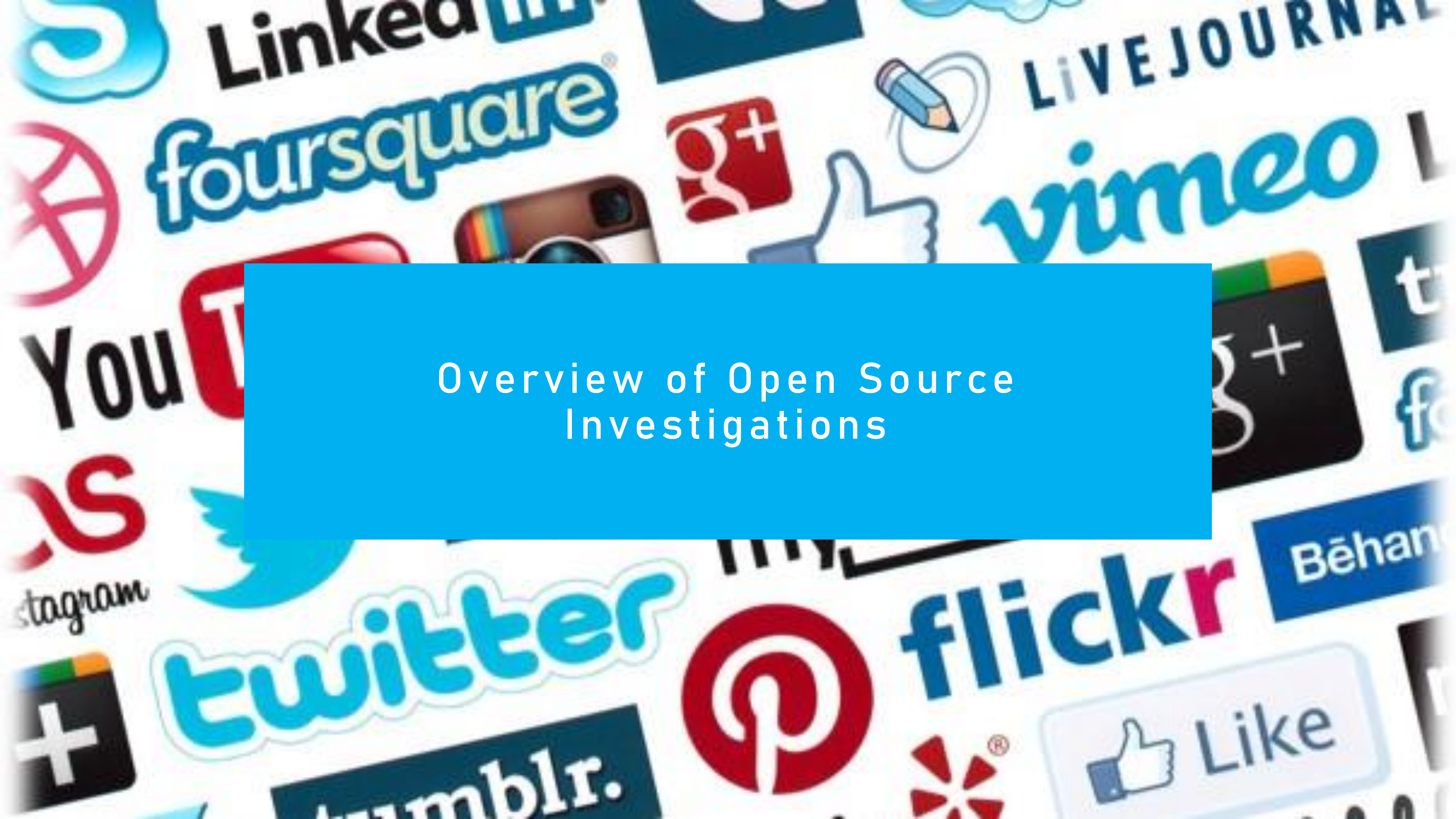
- Seizure of digital evidence and best practice
- Analysis of digital evidence & digital forensic opportunities

Hybrid Investigator

- Worked on a variety of device/data types including computer, mobiles phones and Cloud

REMINDER

- All of the techniques shown in the presentation are to provide you with an idea of what is possible during an OSINT investigation
- Be aware of local legislation when considering the use of any of these techniques
- I'm not an expert in law
  - As part of my role I work with specialists in legislation (RIPA, DSA, TEI) when considering investigative techniques



Overview of Open Source Investigations

WHAT IS OPEN SOURCE?

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

National Police Chiefs Council (NPCC)

DIGITAL FORENSICS

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

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

DIGITAL FORENSIC LIFECYCLE

Seizure

- Device seized
- Advice is to isolate device from the network and power off where possible (in most circumstances)

Device Pre-Acquired

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

Data Extraction

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

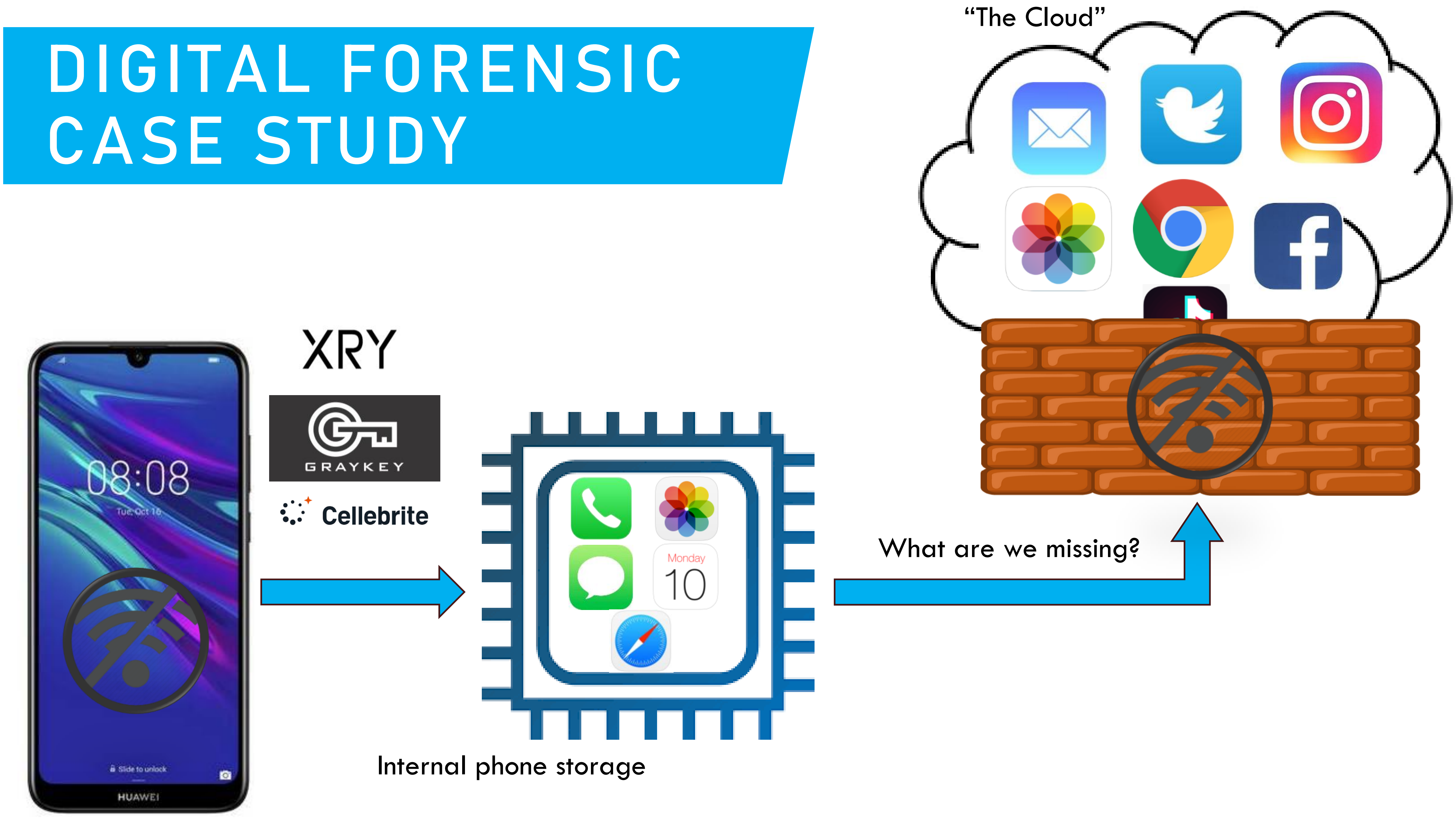
Data Analysis

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

Production of Reports

- Reports produced and submitted into the criminal justice system

DIGITAL FORENSIC CASE STUDY



"The Cloud"

XRY

GRAYKEY

Cellebrite

Internal phone storage

What are we missing?

Protecting your privacy during open source investigations

PROTECTING YOUR PRIVACY ONLINE

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

Device name

Usernames/passwords

Download history

IP Address

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

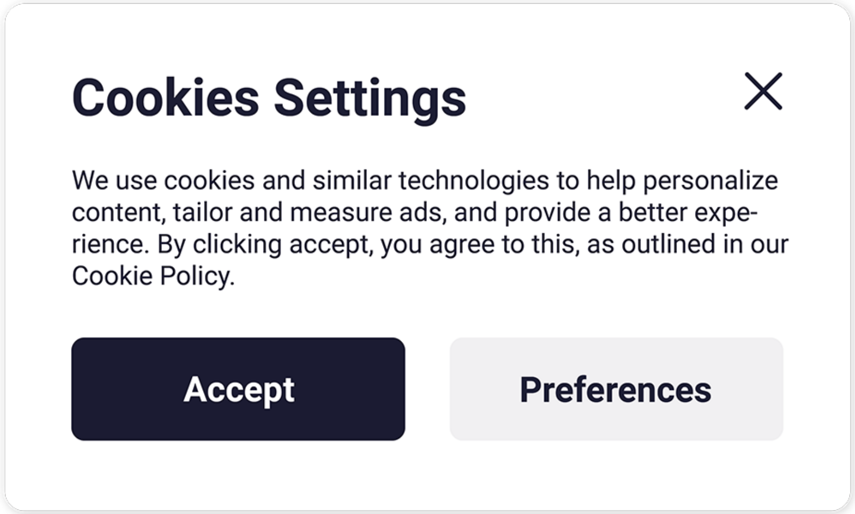
Location Data (longitude and latitude)

Internet History

Social media information

PROTECTING YOUR PRIVACY ONLINE

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



Cookies Settings

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

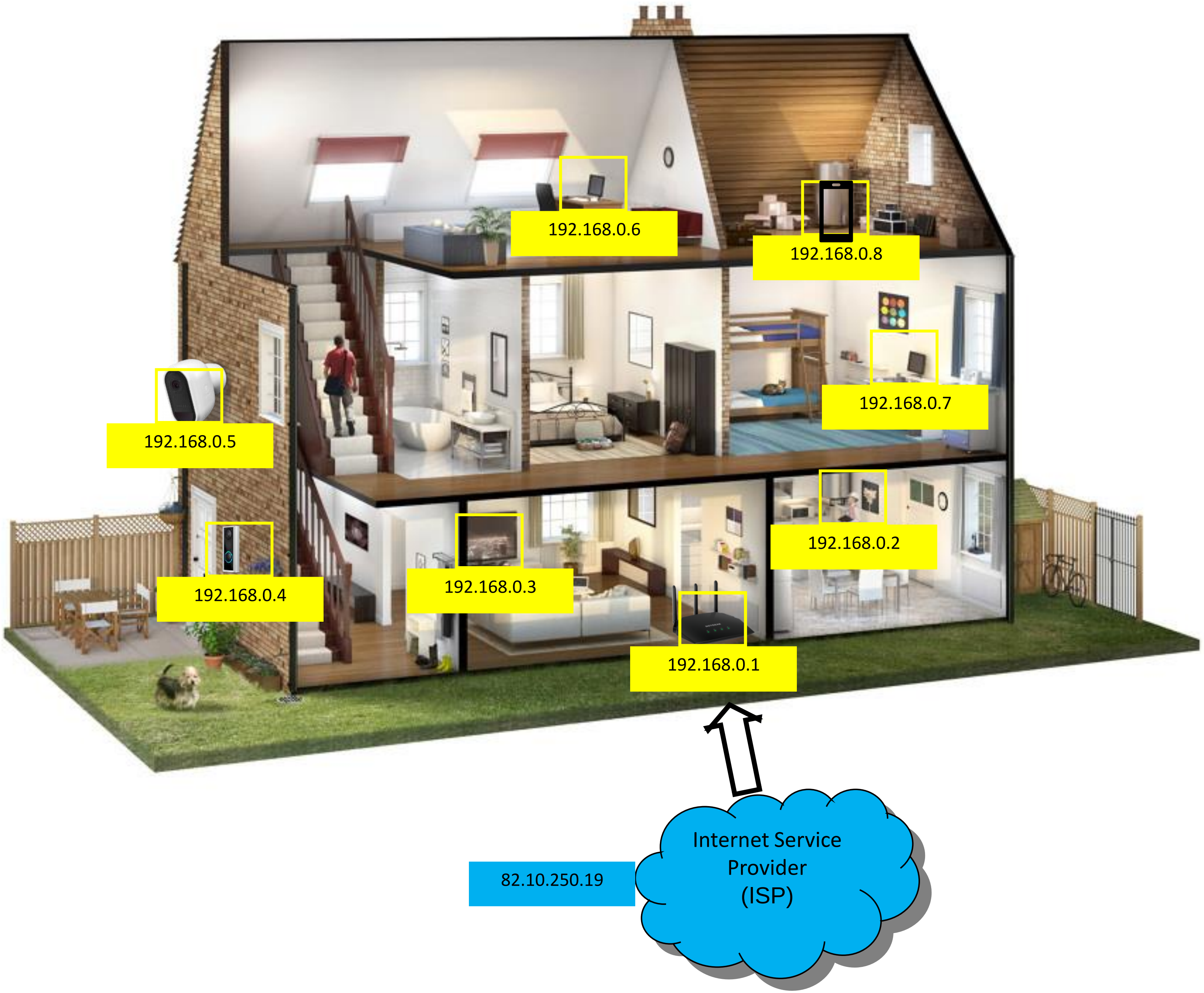
IP ADDRESSES

- IP Address is short for Internet Protocol Address.
  - In simple terms it is similar to your home address
  - May look something like 192.188.0.1
- IP Addresses are used to identify digital devices connected to the internet
- When connecting to the internet, the network you use will be allocated a public IP address by your Internet Service Provider (ISP).
  - Unique to your network
  - Lease periods
- When visiting BBC News, your computer will request information from the BBC News Server,
  - Your IP address is used so that BBC News knows who it needs to send the information to
  - In simple terms, your return address on a letter
- Can your IP address be used to identify you?

My IP Address
63.255.173.183

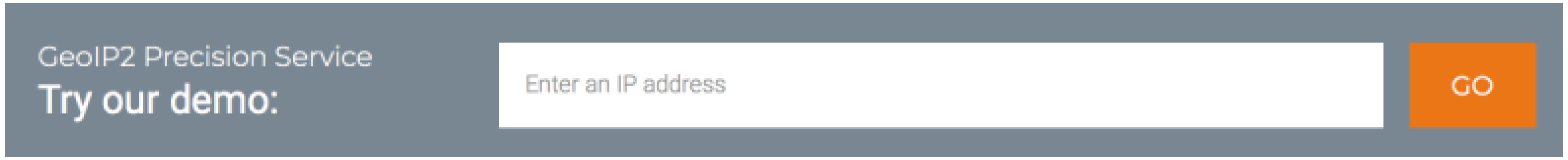
🟨 Private IP

🟦 Private IP



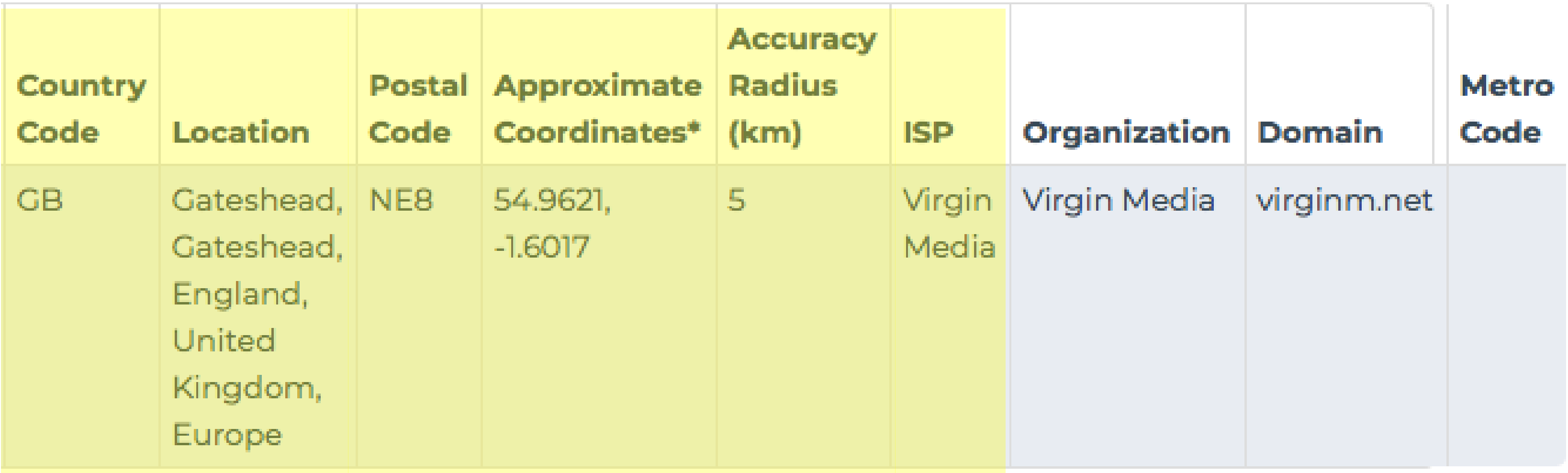
IP ADDRESS EXERCISE

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



IP ADDRESS – EXERCISE

- What information can be obtain from my IP address:

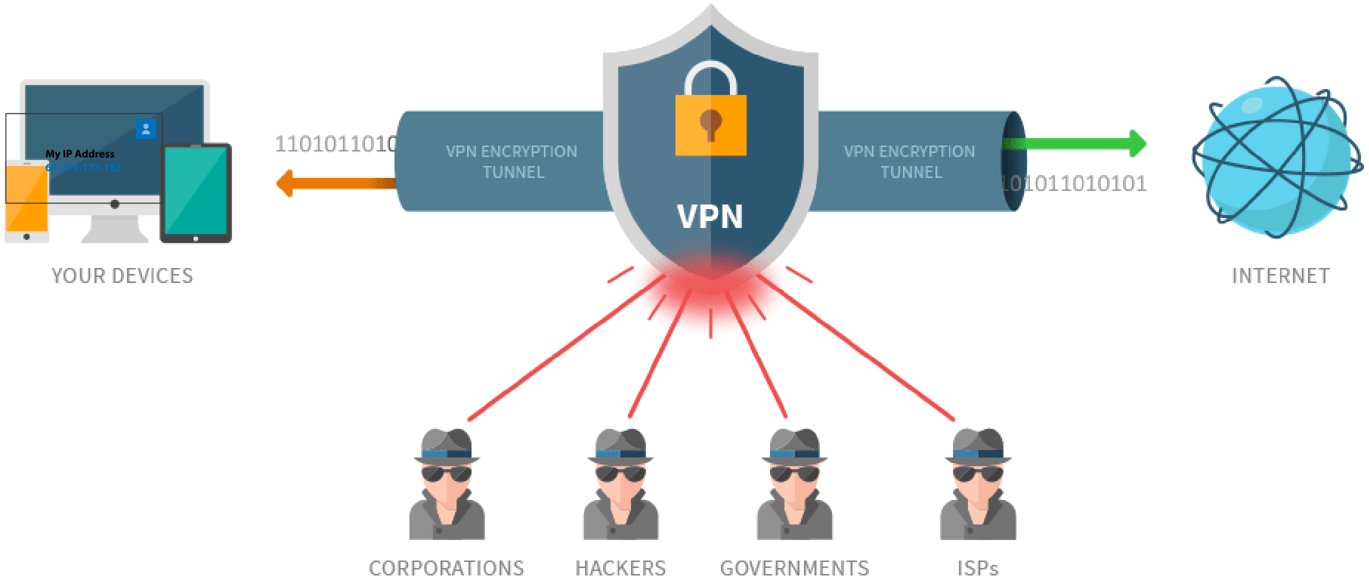


Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
GB	Gateshead, Gateshead, England, United Kingdom, Europe	NE8	54.9621, -1.6017	5	Virgin Media	Virgin Media	virginm.net	

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

VIRTUAL PRIVATE NETWORKS

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



VIRTUAL PRIVATE NETWORKS

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

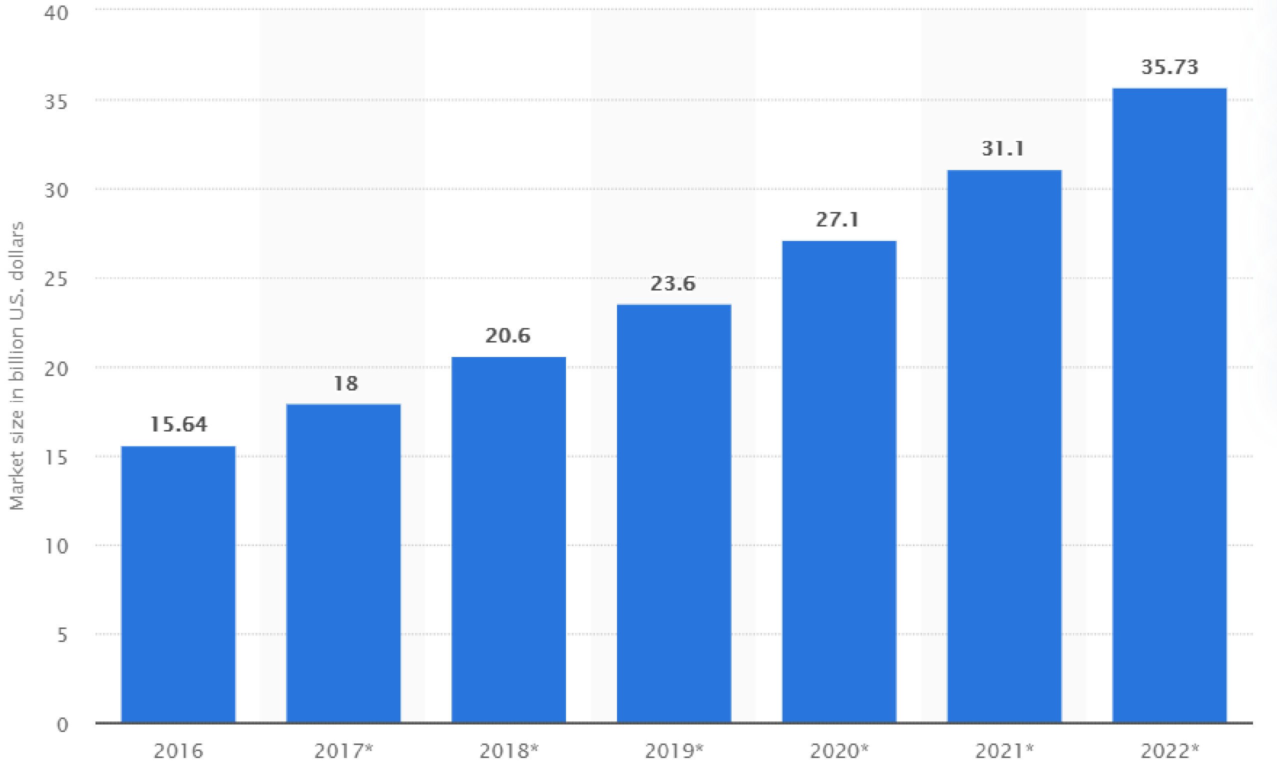
NordVPN®

ProtonVPN

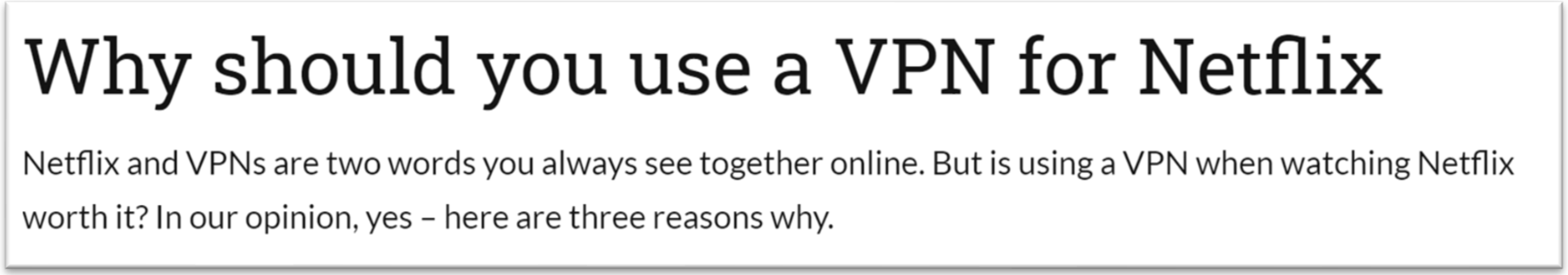
Mozilla VPN

VIRTUAL PRIVATE NETWORKS

Size of the virtual private network (VPN) market worldwide from 2016 to 2022 (Statista)

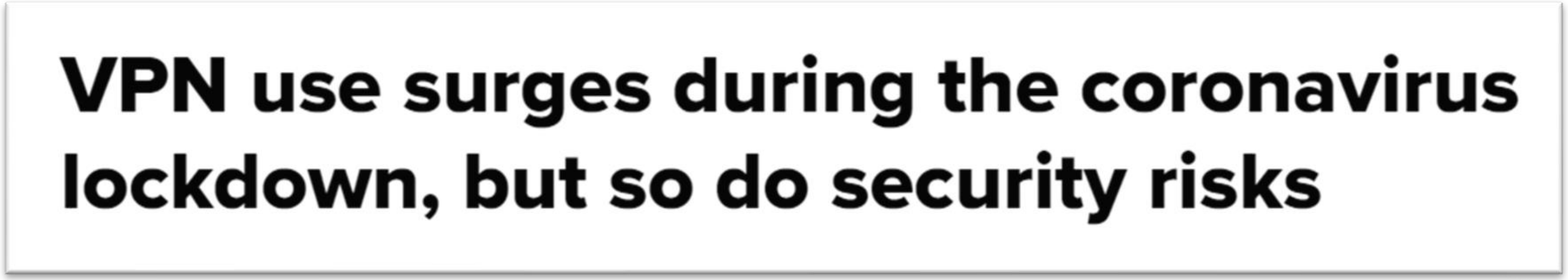


VIRTUAL PRIVATE NETWORKS

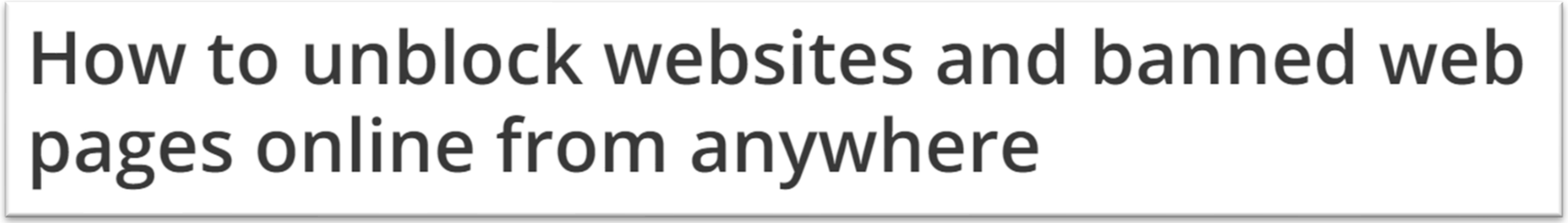


Why should you use a VPN for Netflix

Netflix and VPNs are two words you always see together online. But is using a VPN when watching Netflix worth it? In our opinion, yes – here are three reasons why.



VPN use surges during the coronavirus lockdown, but so do security risks



How to unblock websites and banned web pages online from anywhere

VIRTUAL PRIVATE NETWORKS – EXERCISE

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

Step 2) Enter your IP into Maxmind

Step 3) Register and Download Proton VPN

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

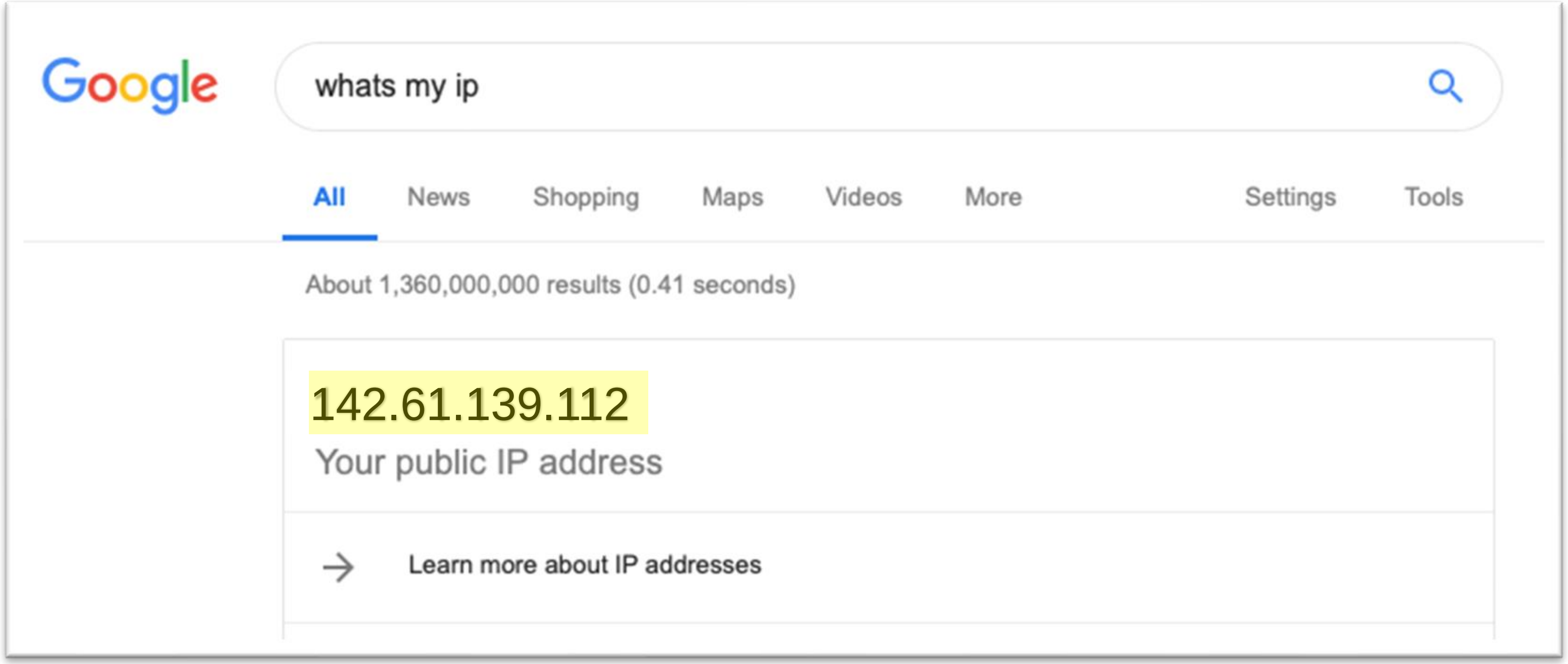
Step 5) Identify your IP address

Step 6) Enter your new IP into Maxmind

What do you notice?

VIRTUAL PRIVATE NETWORKS – EXERCISE

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



whats my ip

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

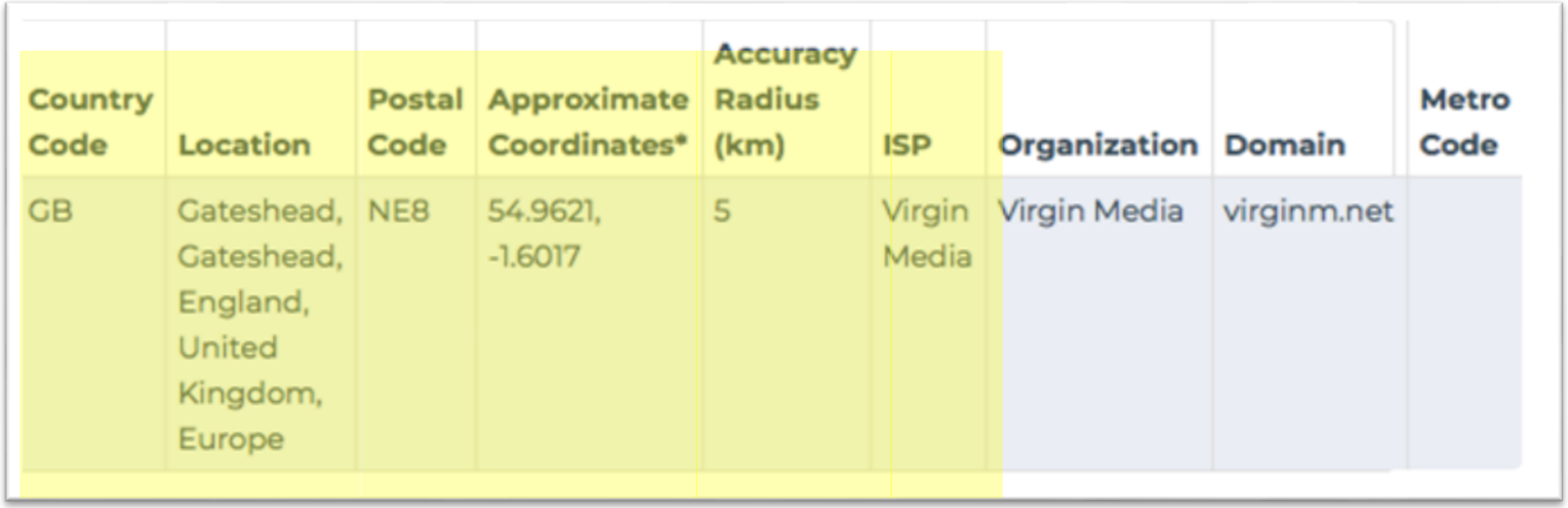
142.61.139.112

Your public IP address

→ Learn more about IP addresses

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 2) Enter your IP into Maxmind

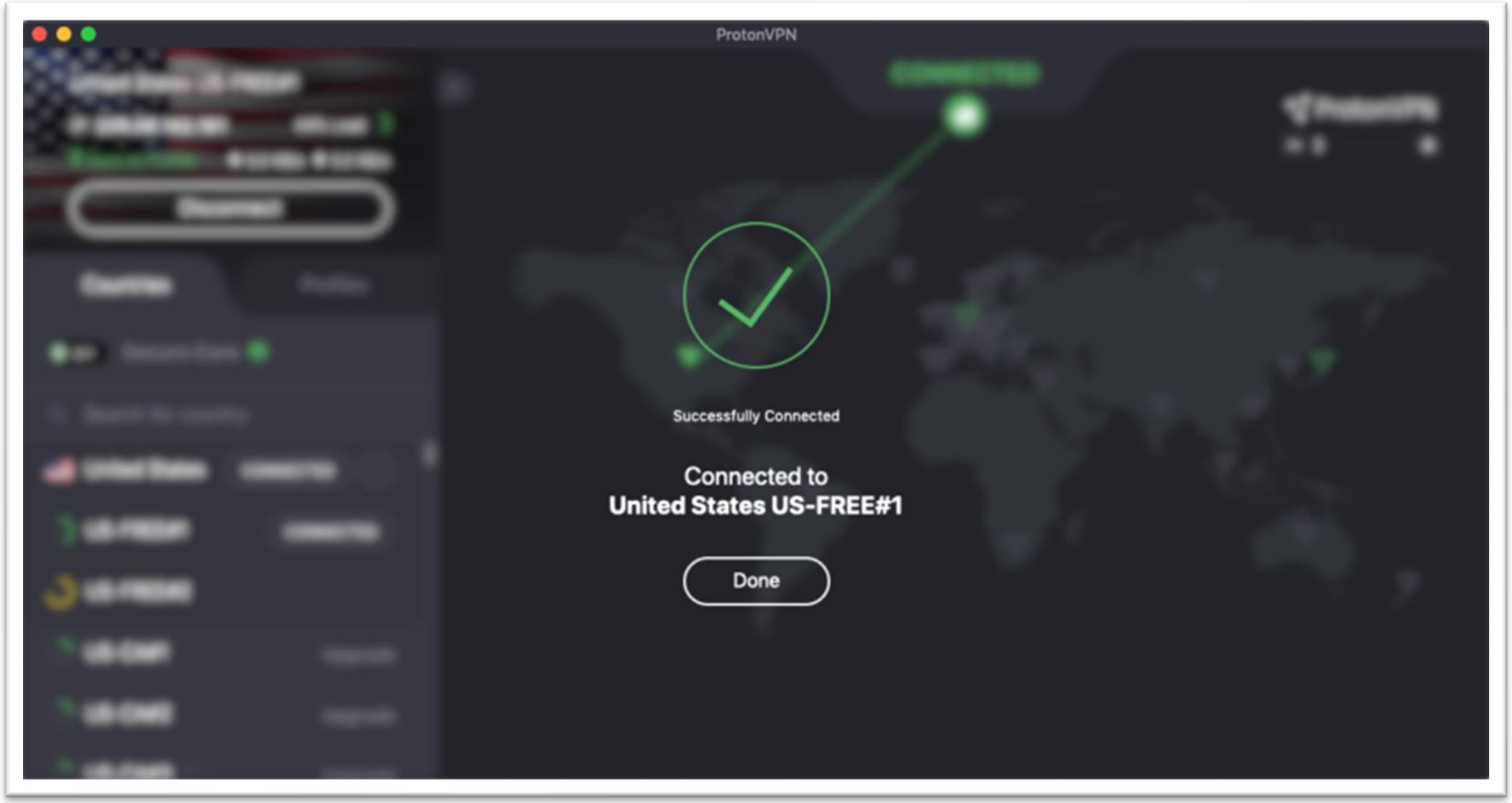


Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
GB	Gateshead, Gateshead, England, United Kingdom, Europe	NE8	54.9621, -1.6017	5	Virgin Media	Virgin Media	virginm.net	

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 3) Register and Download Proton VPN

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

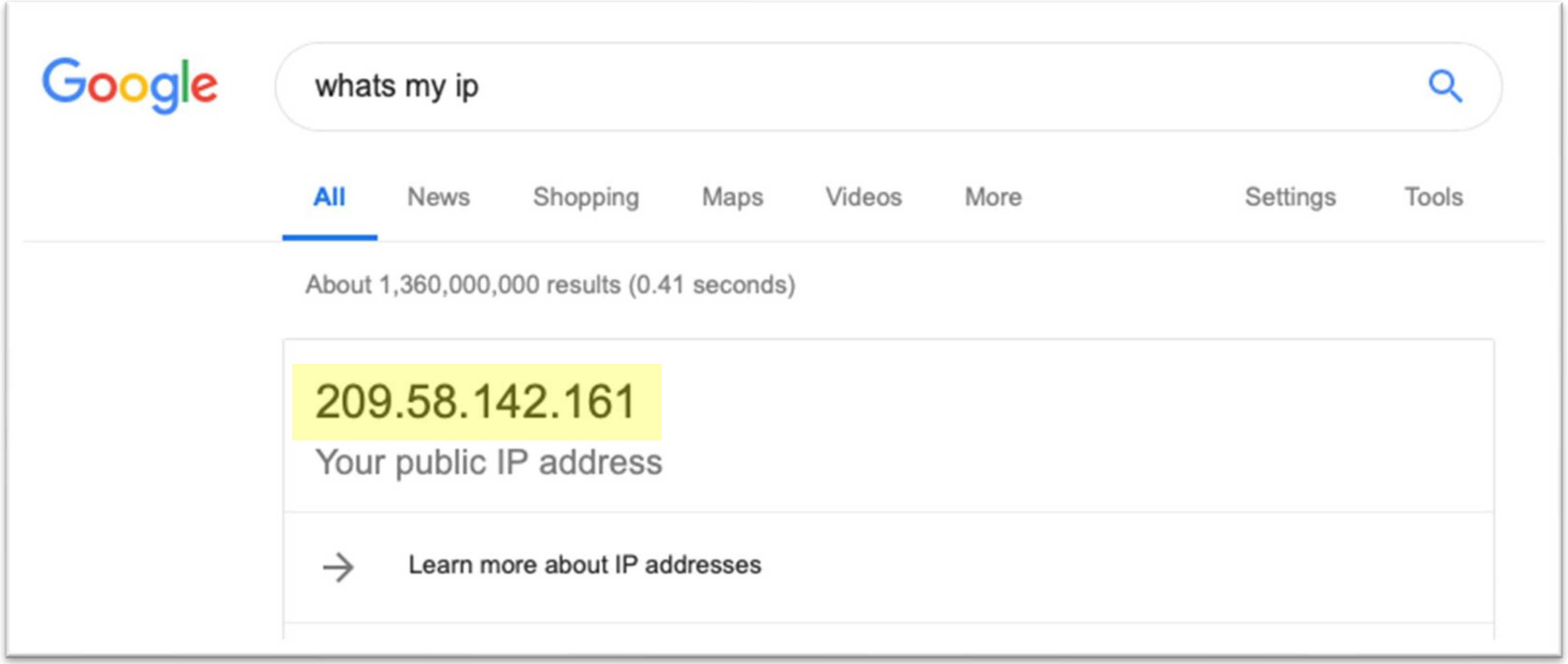


Successfully Connected

Connected to
United States US-FREE#1

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 5) Identify your IP address



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

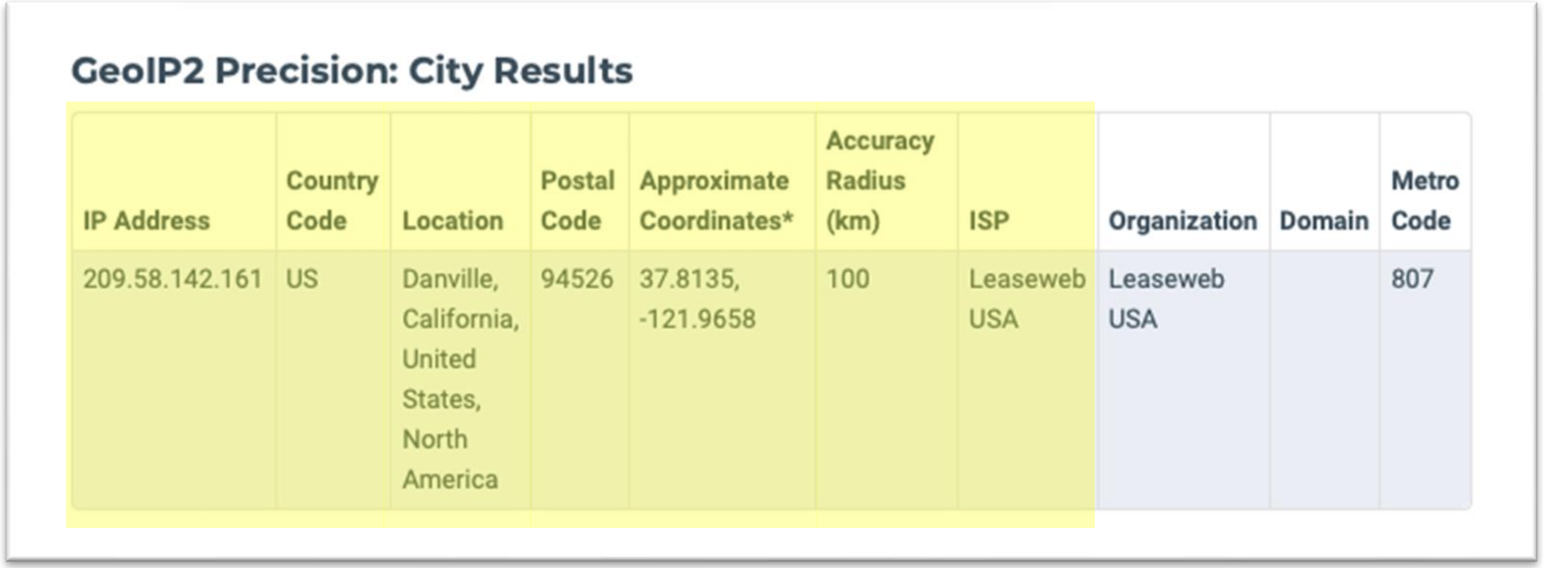
209.58.142.161

Your public IP address

→ Learn more about IP addresses

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 6) Enter your new IP into Maxmind



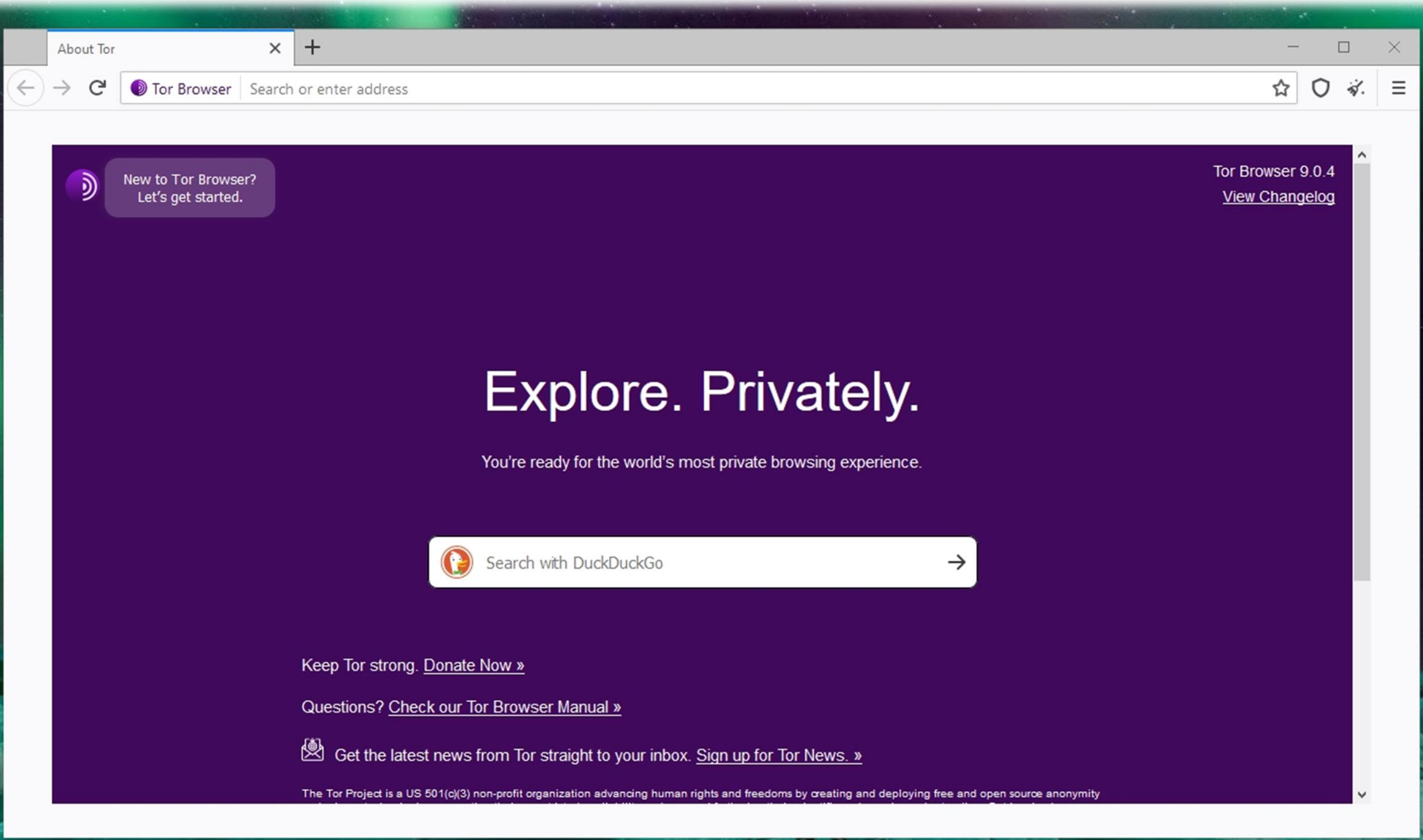
GeoIP2 Precision: City Results

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
209.58.142.161	US	Danville, California, United States, North America	94526	37.8135, -121.9658	100	Leaseweb USA	Leaseweb USA		807

What do you notice?

TOR BROWSER

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



New to Tor Browser? Let's get started.

Tor Browser 9.0.4
View Changelog

Explore. Privately.

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

Keep Tor strong. Donate Now »

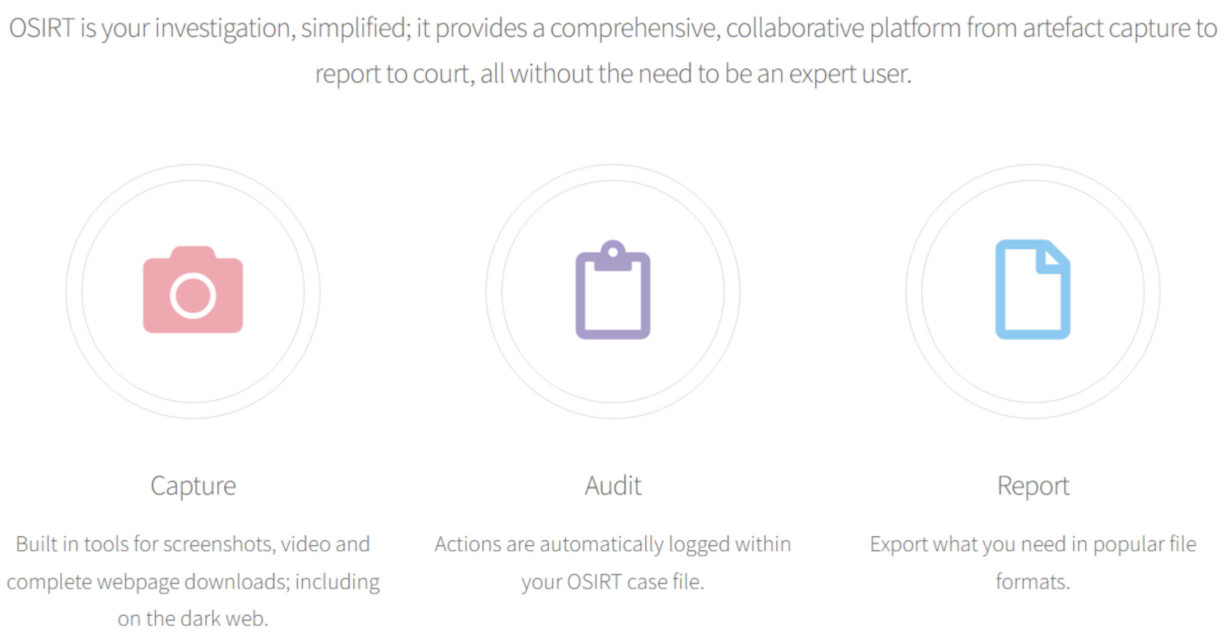
Questions? Check our Tor Browser Manual »

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

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

OSIRT BROWSER

- OSIRT is a web browser which was developed specifically for use in open source investigations
- OSIRT stands for
  - **O**pen
  - **S**ource
  - **I**nternet
  - **R**esearch
  - **T**ool
- OSIRT is a free and open source application:
  - Only works with Microsoft Windows
- New version due for next week



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

Capture

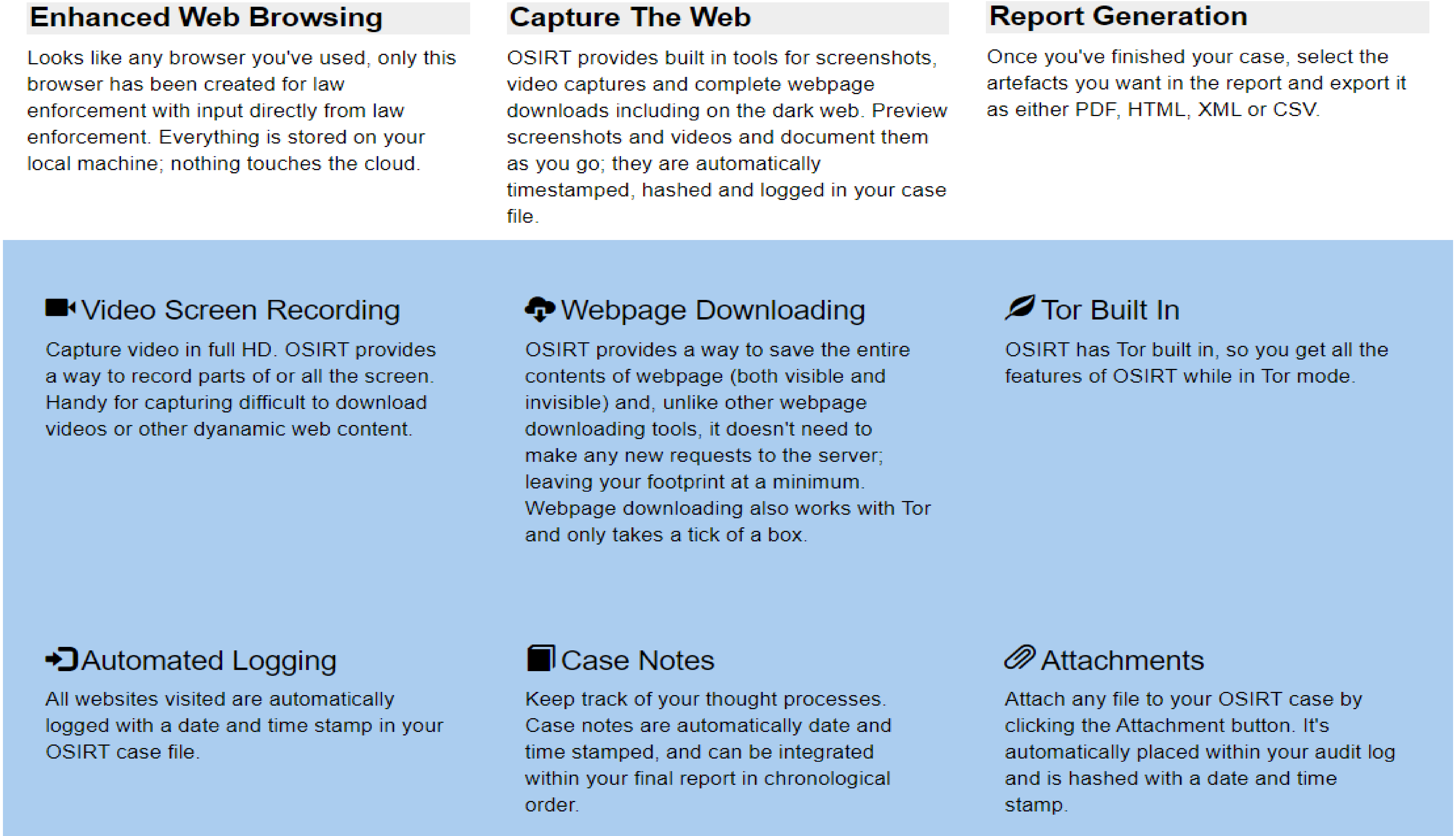
Built in tools for screenshots, video and complete webpage downloads; including on the dark web.

Audit

Actions are automatically logged within your OSIRT case file.

Report

Export what you need in popular file formats.



Enhanced Web Browsing

Looks like any browser you've used, only this browser has been created for law enforcement with input directly from law enforcement. Everything is stored on your local machine; nothing touches the cloud.

Capture The Web

OSIRT provides built in tools for screenshots, video captures and complete webpage downloads including on the dark web. Preview screenshots and videos and document them as you go; they are automatically timestamped, hashed and logged in your case file.

Report Generation

Once you've finished your case, select the artefacts you want in the report and export it as either PDF, HTML, XML or CSV.

Video Screen Recording

Capture video in full HD. OSIRT provides a way to record parts of or all the screen. Handy for capturing difficult to download videos or other dyanamic web content.

Webpage Downloading

OSIRT provides a way to save the entire contents of webpage (both visible and invisible) and, unlike other webpage downloading tools, it doesn't need to make any new requests to the server; leaving your footprint at a minimum. Webpage downloading also works with Tor and only takes a tick of a box.

Tor Built In

OSIRT has Tor built in, so you get all the features of OSIRT while in Tor mode.

Automated Logging

All websites visited are automatically logged with a date and time stamp in your OSIRT case file.

Case Notes

Keep track of your thought processes. Case notes are automatically date and time stamped, and can be integrated within your final report in chronological order.

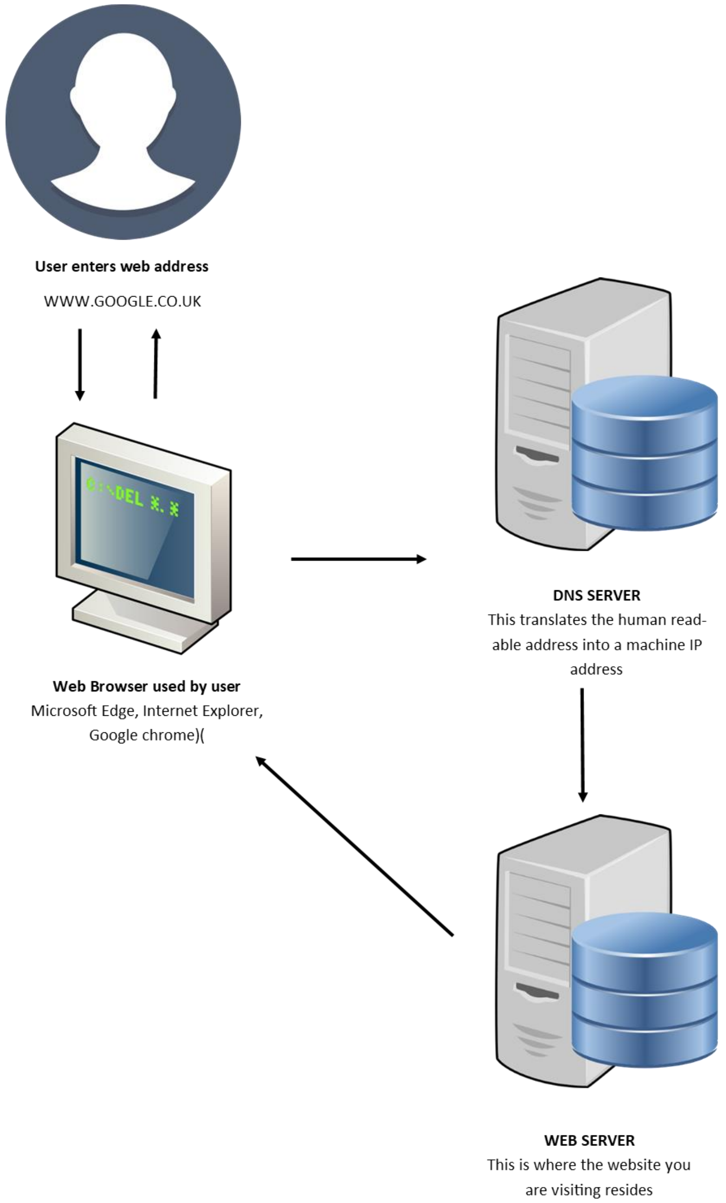
Attachments

Attach any file to your OSIRT case by clicking the Attachment button. It's automatically placed within your audit log and is hashed with a date and time stamp.

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

DOMAIN NAMES

- What is a domain name?
  - A domain name is a unique name for identifying a website
  - Remember IP addresses?
    - 212.58.226.75 > www.bbc.co.uk/news
  - It is a user friendly version of an IP address
  - It would be virtually impossible to remember the IP addresses for all your favorite websites
- Website developers can purchase a domain name from a number of different companies:
  - 123-reg
  - GoDaddy
- Like many online purchases, a user is required to provide numerous pieces of information when purchasing a domain name:
  - Name
  - Address
  - Email



User enters web address

WWW.GOOGLE.CO.UK

Web Browser used by user

Microsoft Edge, Internet Explorer, Google chrome)(

DNS SERVER

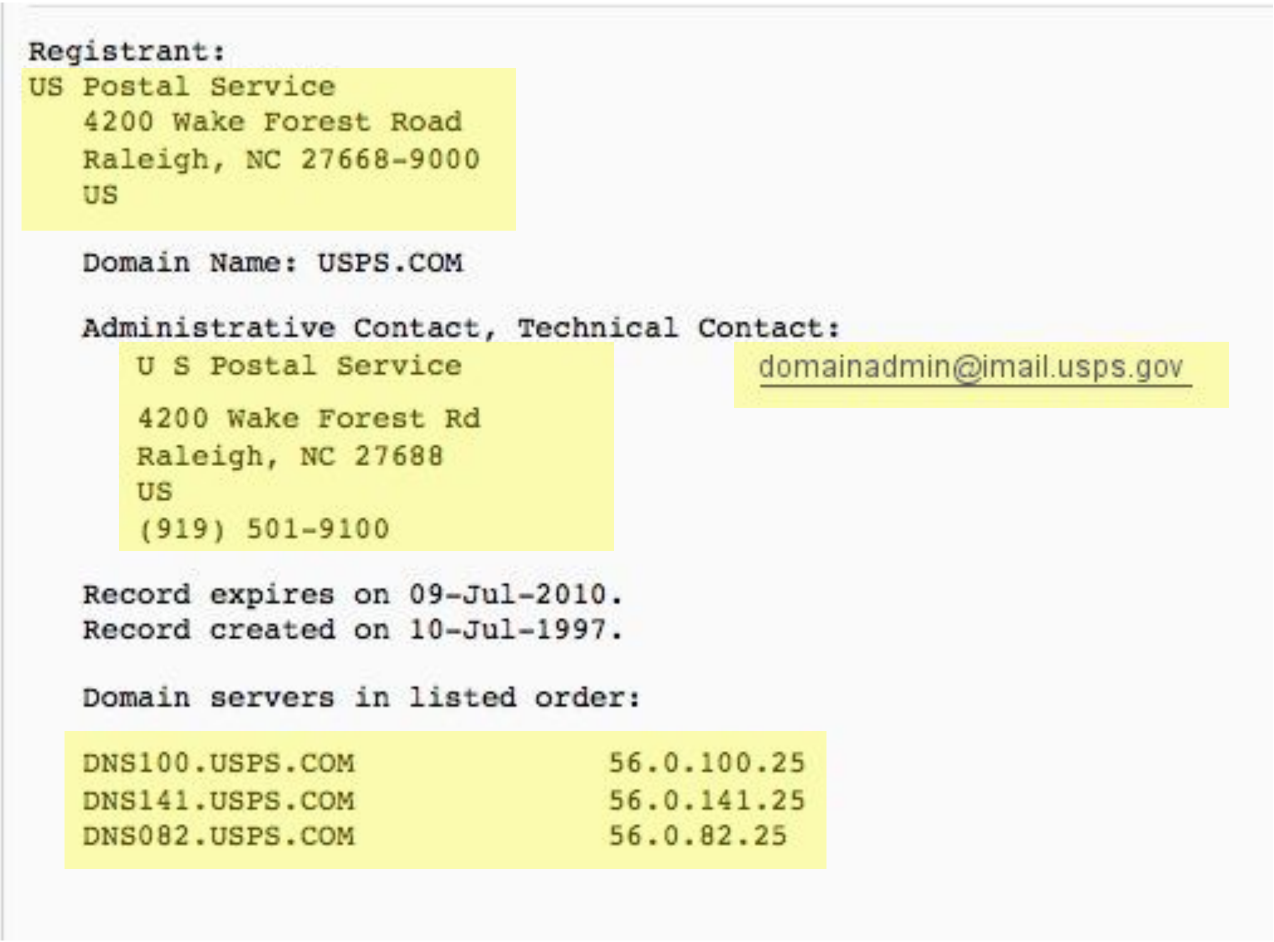
This translates the human read-able address into a machine IP address

WEB SERVER

This is where the website you are visiting resides

DOMAIN NAMES - WHOIS

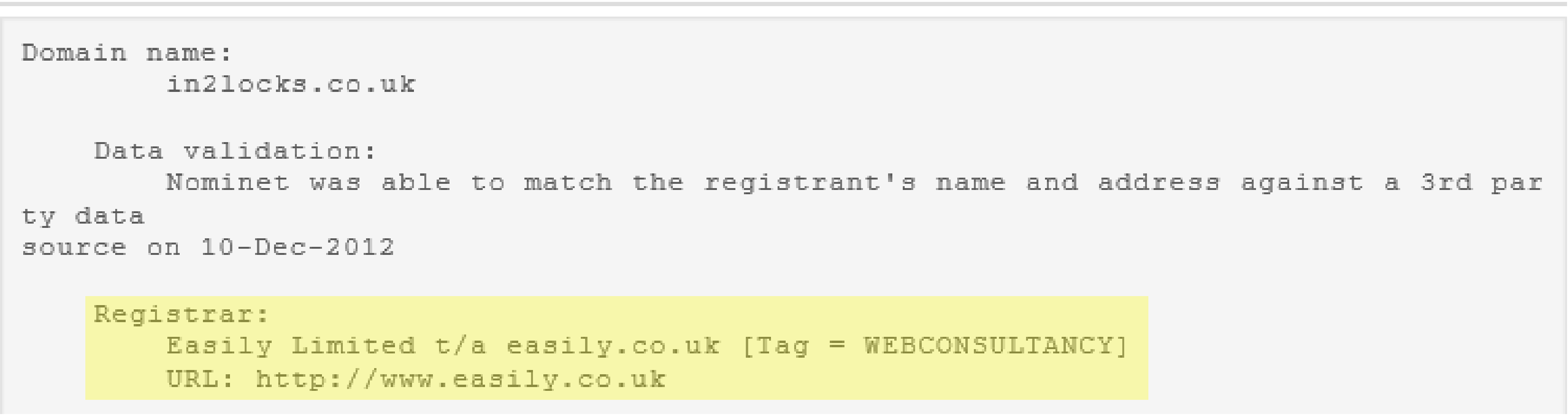
- As investigators, this information may help us identify the owner of a website:
  - http://whois.domaintools.com
- WHOIS search conducted for the US Postal Service domain name
  - www.usps.com
- This reveals a number of details
  - Postal address
  - Telephone number
  - Email address
  - IP addresses



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

   Domain Name: USPS.COM

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

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

   Domain servers in listed order:

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

DOMAIN NAMES – PROXY

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



```
Domain name:
        in2locks.co.uk

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

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

EMAILS

- A commonly used form of communication
- Emails can contain hidden information which is useful during an open source investigations
- An email contains two main parts

Body

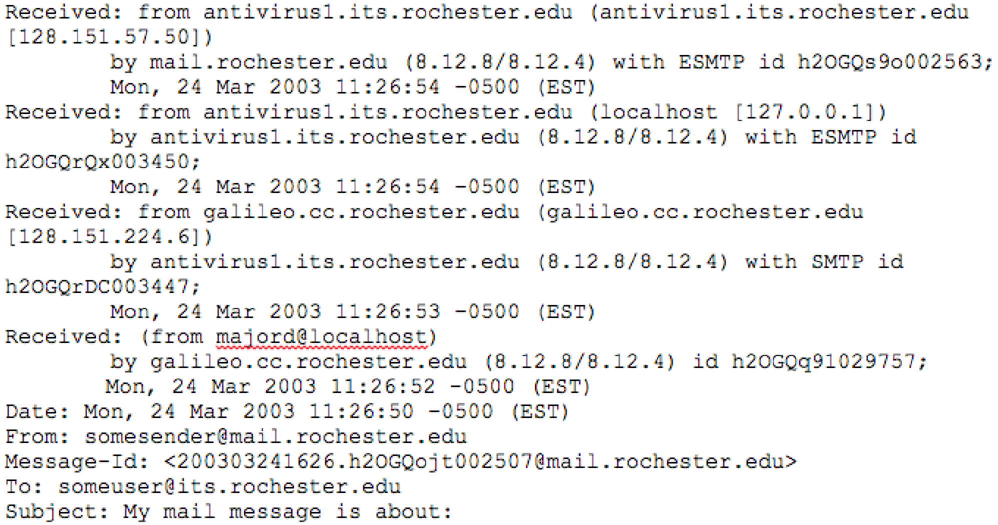
- The body of the message is the section the we see as a general user)
- The section most people associate with the word email

Header

- A header is responsible for ensuring the email is delivered to the correct person.
  - Comparable to a delivery tracking service when you order a parcel online
- This hidden header can often contain lots of information which can be useful during an investigation
  - To
  - From
  - Subject
  - Route
  - Origin information
- Not all email headers will contain the same information:
  - The information contained within the header depends upon the email provider of the sender.

EMAIL HEADERS

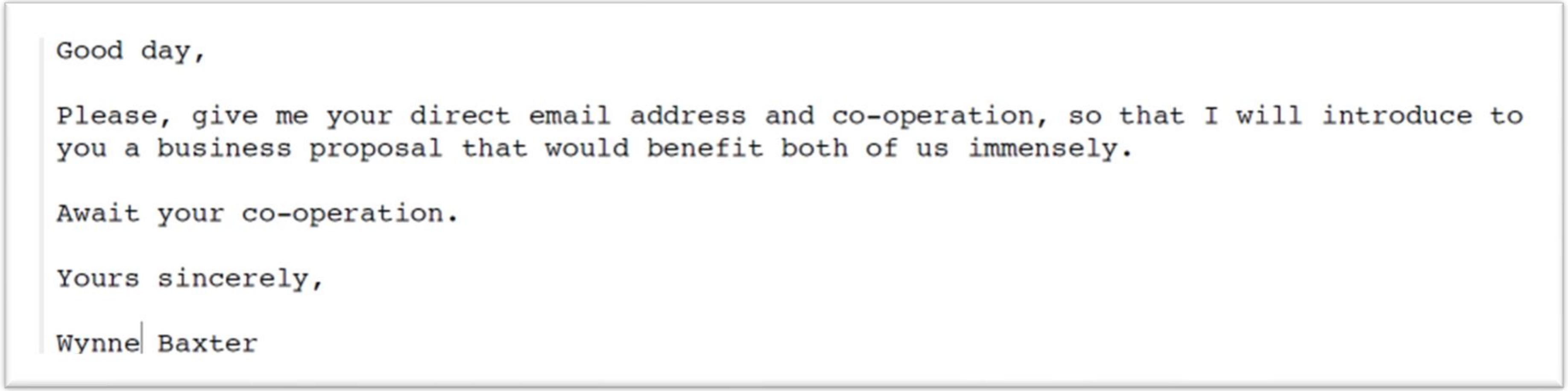
- Often difficult to interpret, until we understand the different areas of interest
    - **Content-Type:** Notes whether the email is HTML or plain text.
    - **Date:** When the email was written.
    - **Delivery Date:** When the email was received by your mail server.
    - **From:** Who sent the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



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

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

EMAIL HEADERS – EXERCISE 1



Good day,

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

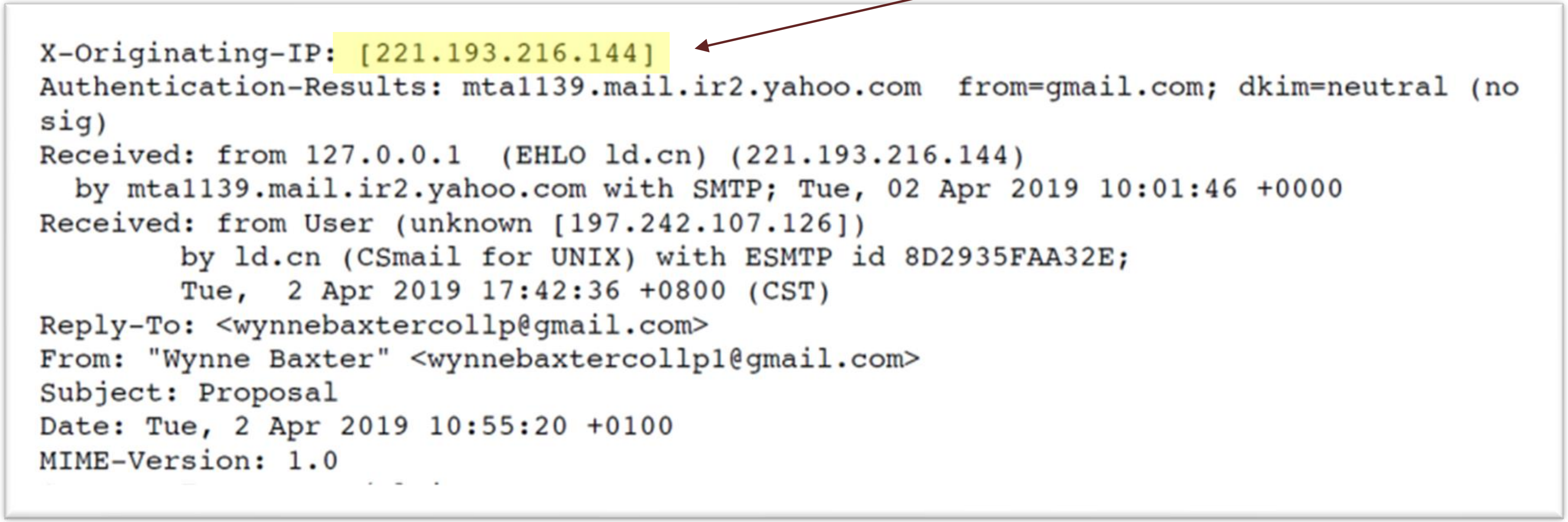
Await your co-operation.

Yours sincerely,

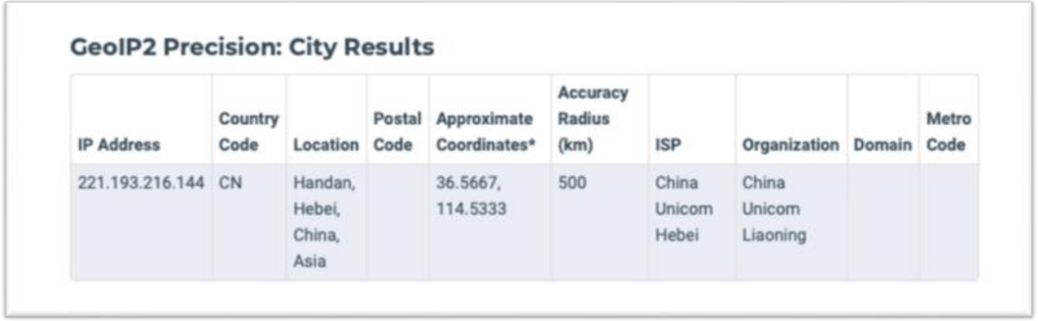
Wynne Baxter

EMAIL HEADERS – EXERCISE 1

Remember: this could be assigned by a VPN



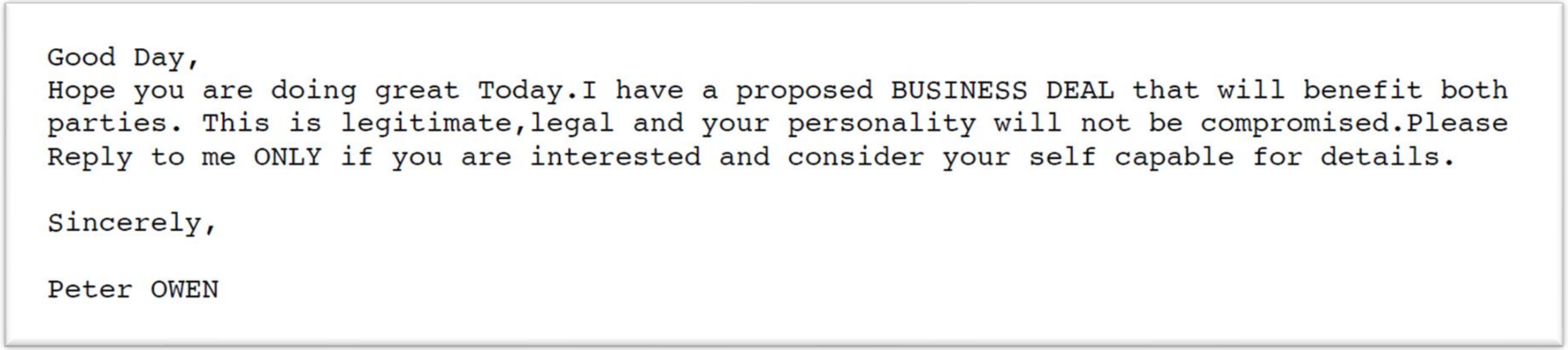
```
X-Originating-IP: [221.193.216.144]
Authentication-Results: mta1139.mail.ir2.yahoo.com  from=gmail.com; dkim=neutral (no
sig)
Received: from 127.0.0.1  (EHLO ld.cn) (221.193.216.144)
  by mta1139.mail.ir2.yahoo.com with SMTP; Tue, 02 Apr 2019 10:01:46 +0000
Received: from User (unknown [197.242.107.126])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



GeoIP2 Precision: City Results

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

EMAIL HEADERS – EXERCISE 2



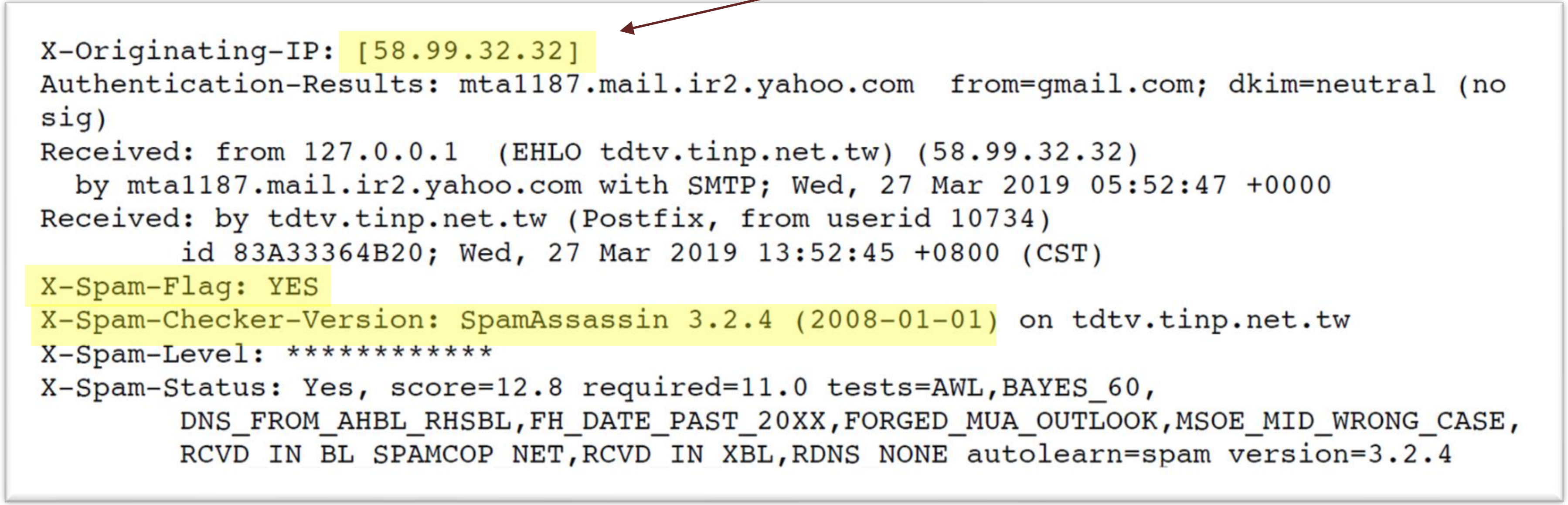
Good Day,
Hope you are doing great Today.I have a proposed BUSINESS DEAL that will benefit both parties. This is legitimate,legal and your personality will not be compromised.Please Reply to me ONLY if you are interested and consider your self capable for details.

Sincerely,

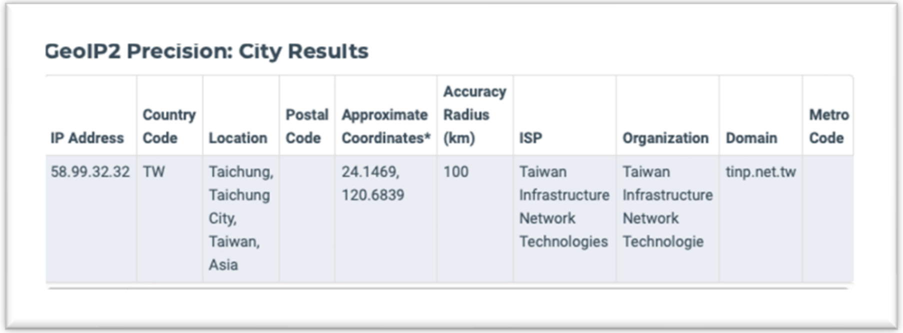
Peter OWEN

EMAIL HEADERS – EXERCISE 2

Remember: this could be assigned by a VPN



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



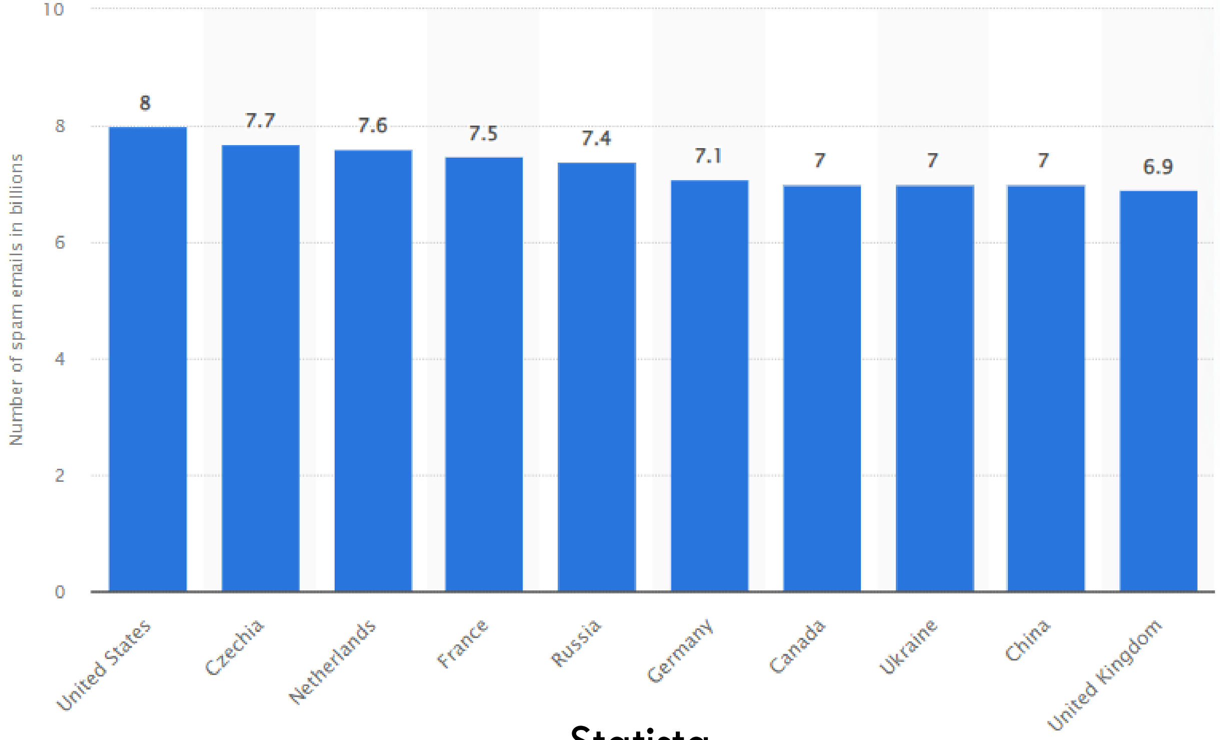
GeoIP2 Precision: City Results

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

EMAIL SPAM

- Spam is also often referred to as Junk mail and are sent for a number of reasons:
  - Make money
  - Phishing to obtain personal information such as credit card, bank details and passwords
  - Spread malicious code i.e. viruses

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



Statista

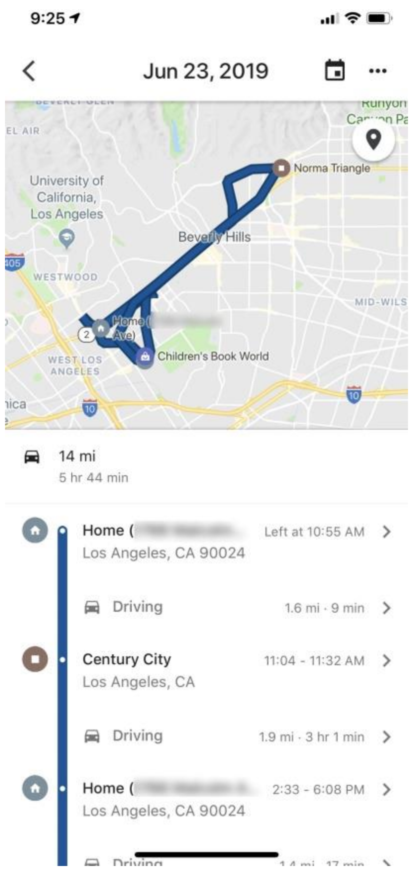
EMAIL BLACKLISTS

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

Geo-location tools for Open Source Investigations

GEO-LOCATION

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



14 mi
5 hr 44 min

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

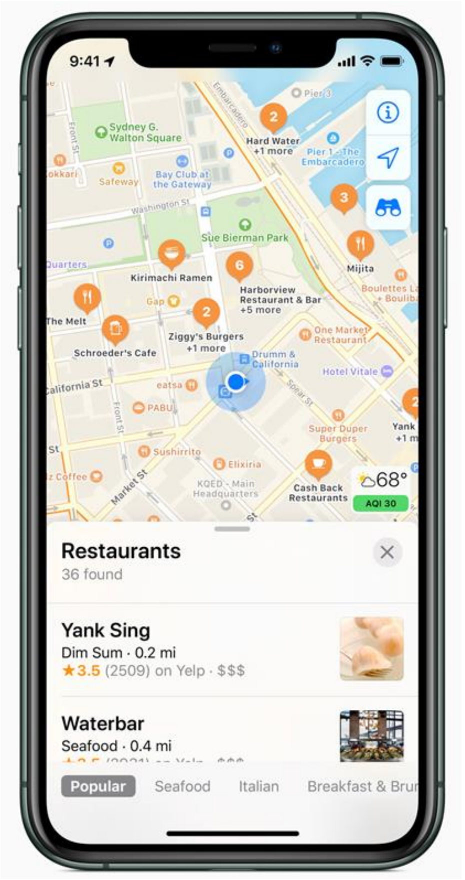
Driving 1.6 mi · 9 min

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

Driving 1.9 mi · 3 hr 1 min

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

Driving



Restaurants
36 found

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

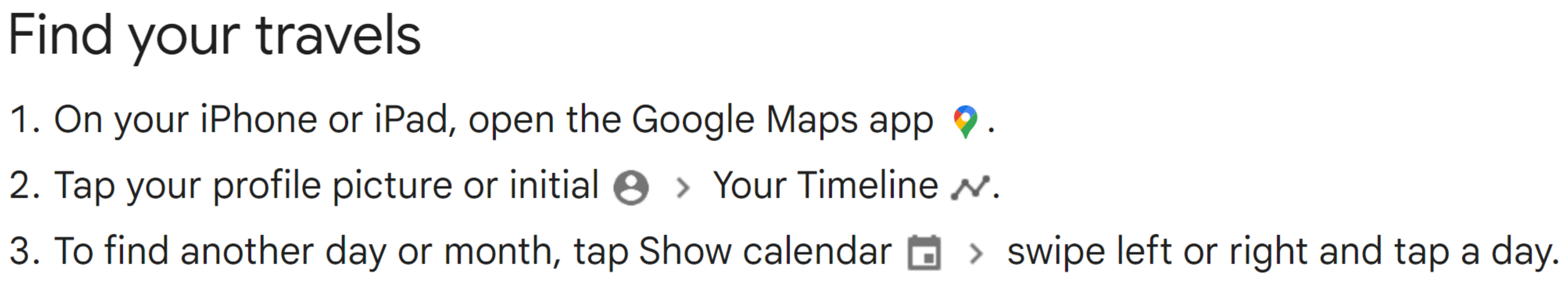
Waterbar
Seafood · 0.4 mi

Popular | Seafood | Italian | Breakfast & Bru

GOOGLE MAPS EXAMPLE

- Think of your own Google Maps account
  - How much data do they hold about you?

Who in this room uses Google Maps?

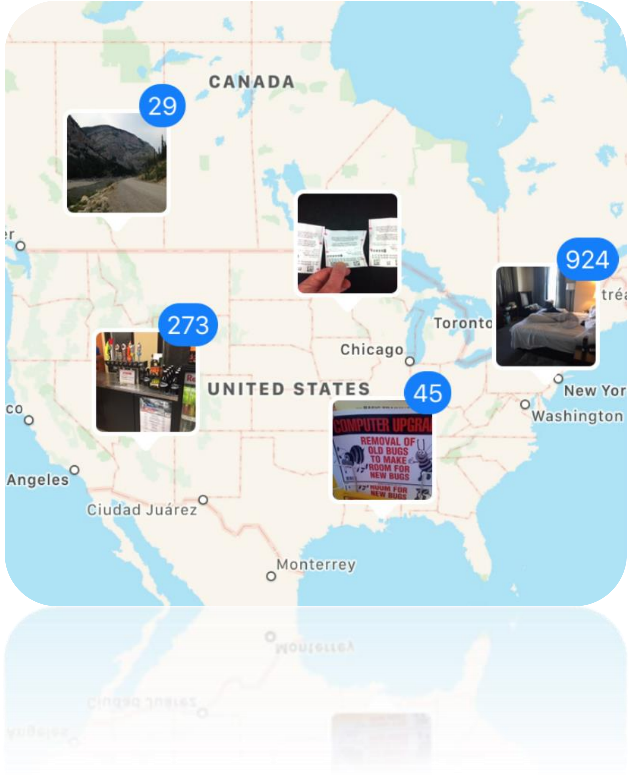


Find your travels

1. On your iPhone or iPad, open the Google Maps app .
2. Tap your profile picture or initial › Your Timeline .
3. To find another day or month, tap Show calendar › swipe left or right and tap a day.

GEO-LOCATION

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

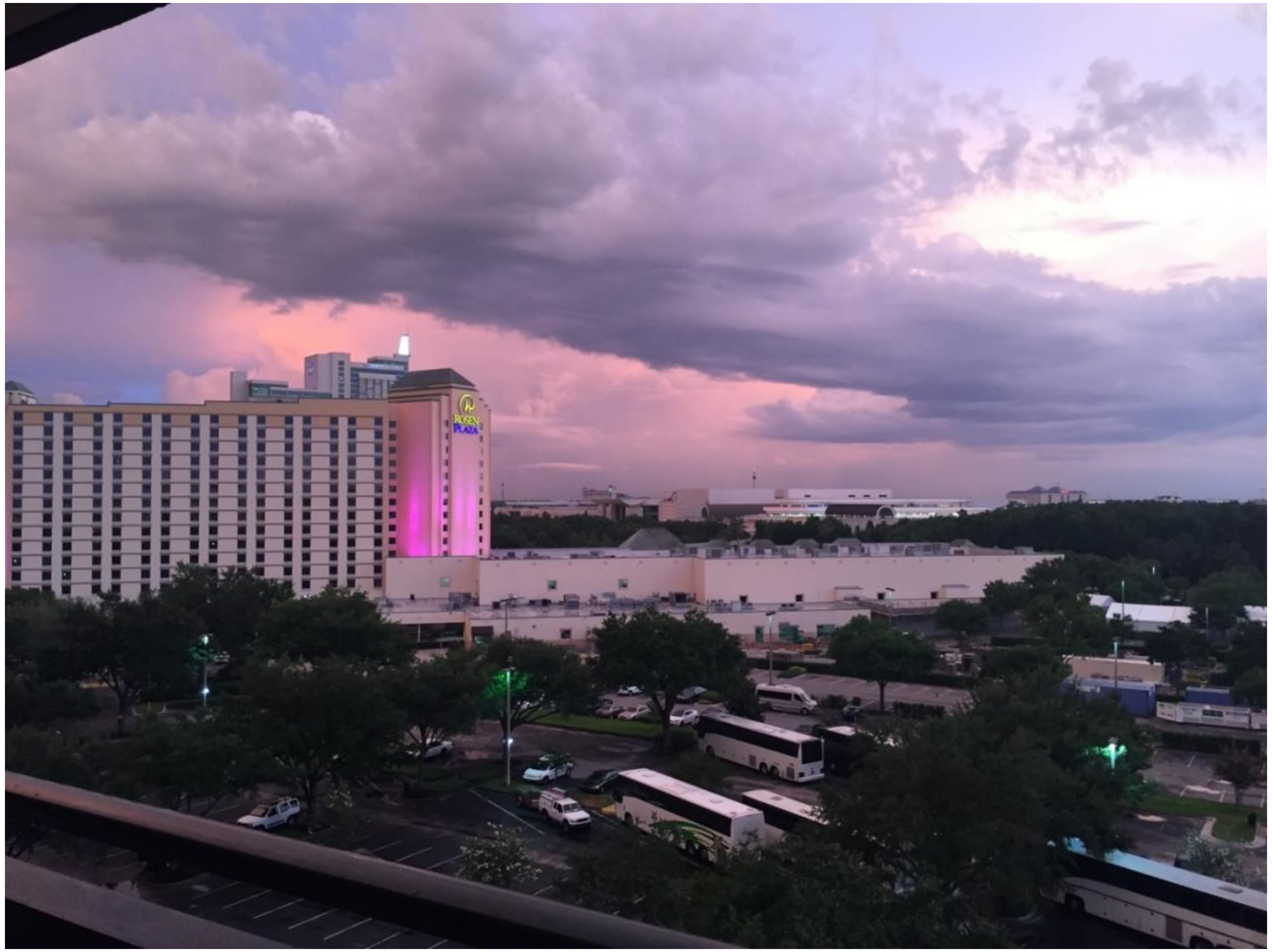


EXIF DATA EXERCISE

- During an investigation we have recovered two photographs which are relevant
- The investigation team need to understand more information about the images, such as:
  - What device was used to take the photographs
  - The location he photograph was taken
- This scenario contains two photographs:
    - IMG_7300.JPG
    - IMG_3561.JPG
- Using a free online tool, we will see what other information we can obtain from the photograph
  - For this exercise we will use www.pic2map.com

EXIF DATA EXERCISE

- Filename: IMG_7300.JPG

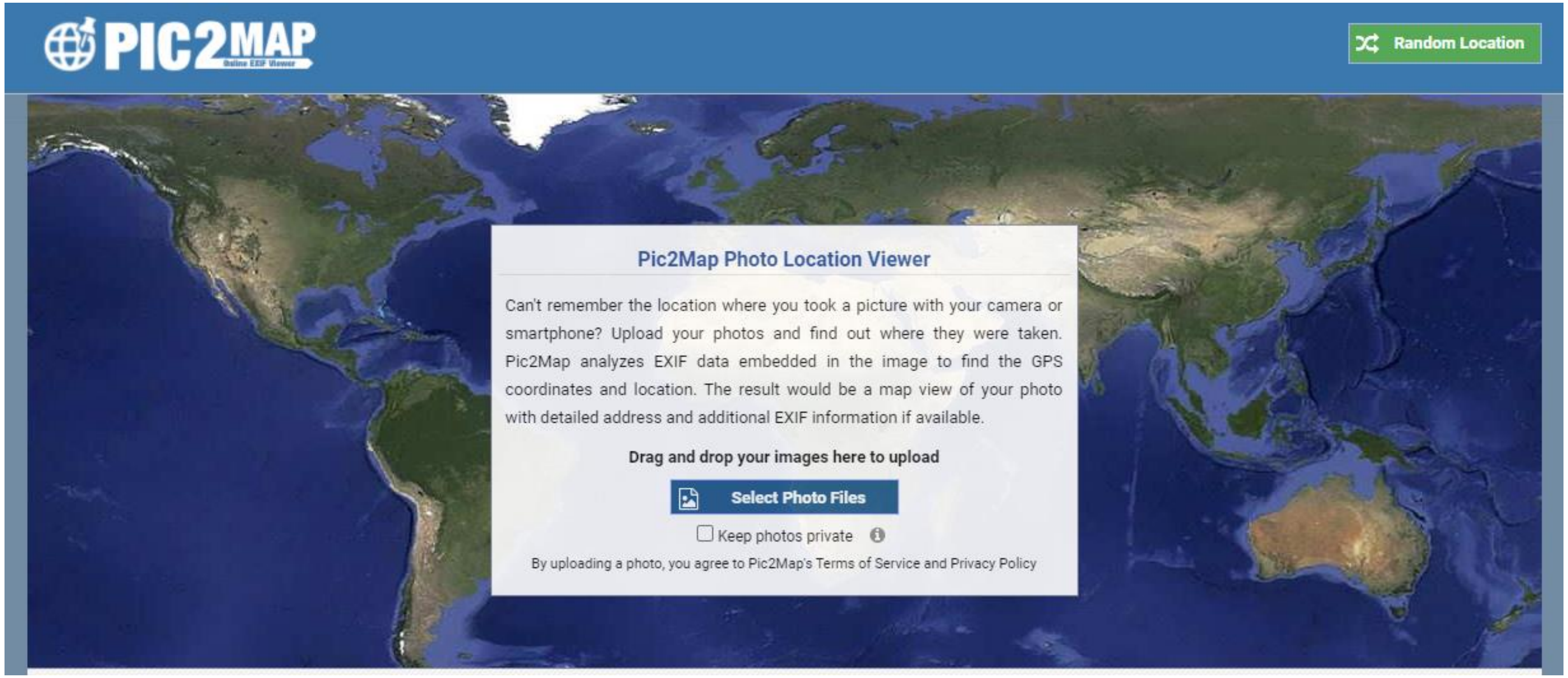


EXIF DATA EXERCISE

- Filename: IMG_3561.JPG

EXIF DATA EXERCISE

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



Pic2Map Photo Location Viewer

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

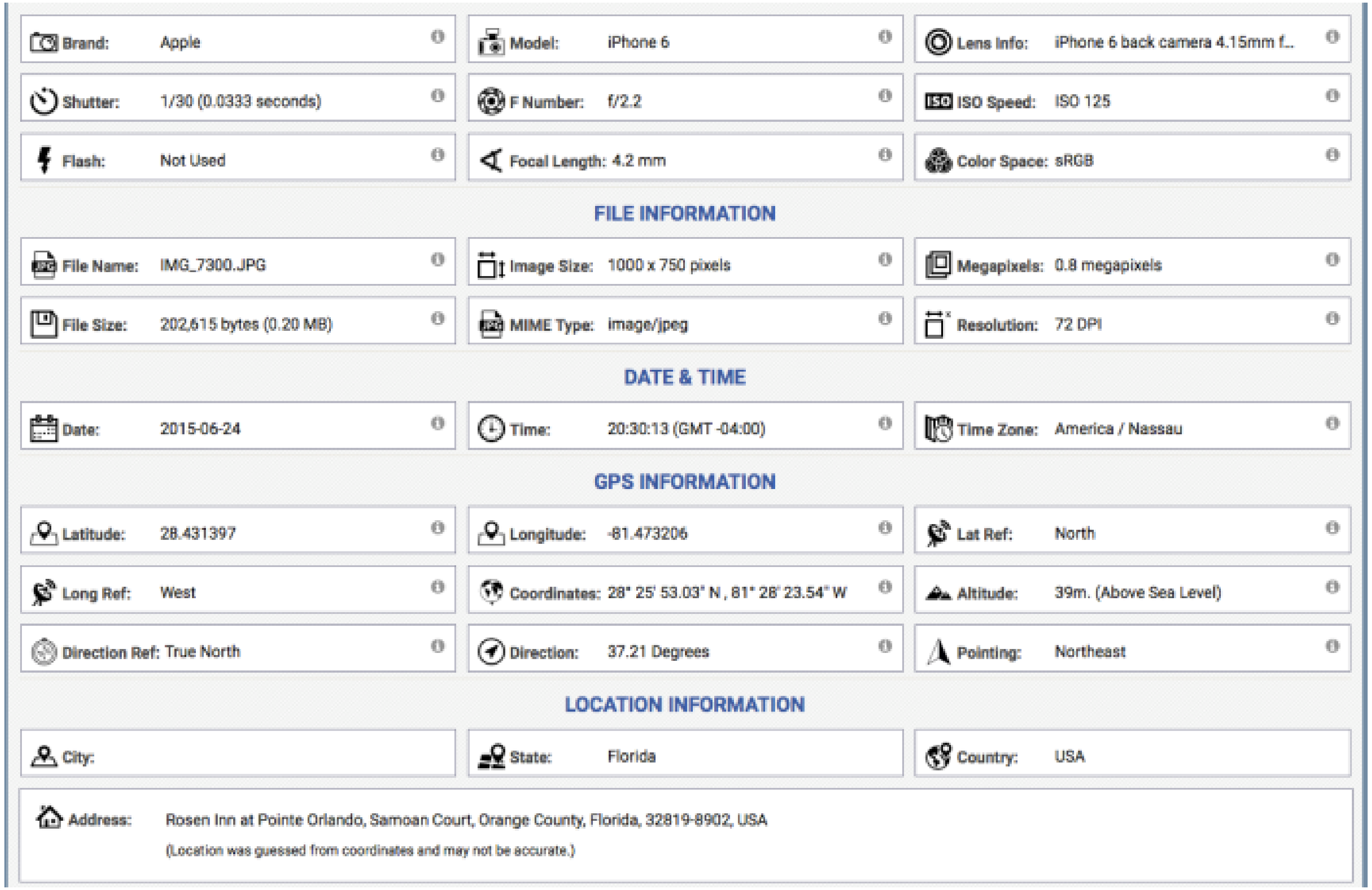
Drag and drop your images here to upload

□ Keep photos private

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

EXIF DATA EXERCISE

- IMG_7300.JPG



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

FILE INFORMATION

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

DATE & TIME

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

GPS INFORMATION

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

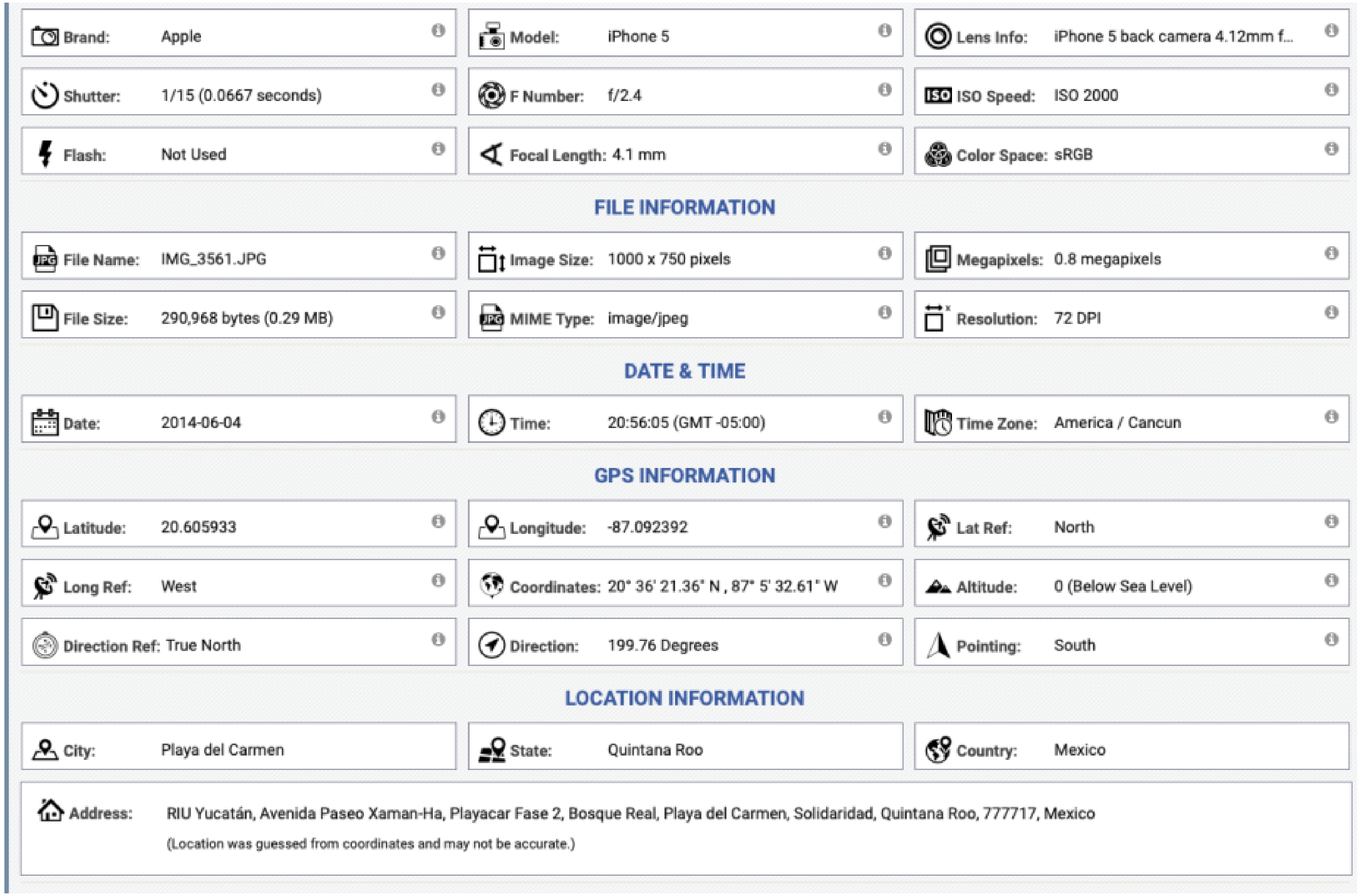
LOCATION INFORMATION

City:	State: Florida	Country: USA

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

EXIF DATA EXERCISE

- IMG_3561.JPG



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

FILE INFORMATION

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

DATE & TIME

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

GPS INFORMATION

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

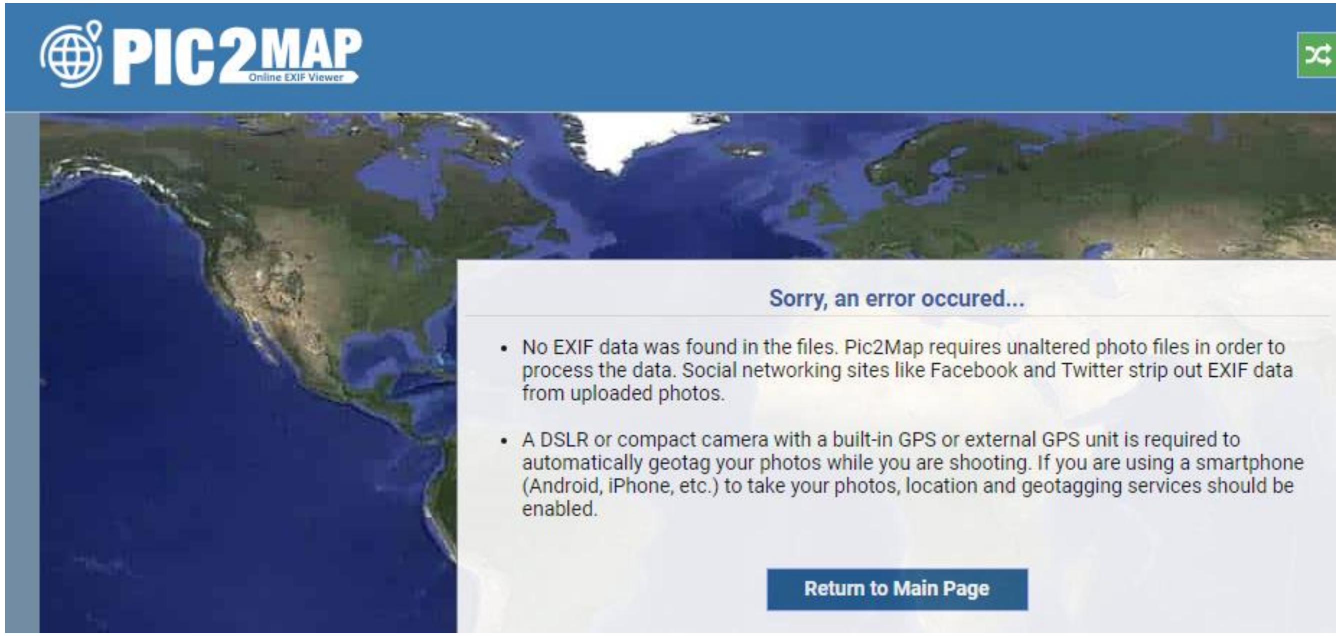
LOCATION INFORMATION

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

Address: RIU Yucatán, Avenida Paseo Xaman-Ha, Playacar Fase 2, Bosque Real, Playa del Carmen, Solidaridad, Quintana Roo, 777717, Mexico
(Location was guessed from coordinates and may not be accurate.)

EXIF DATA EXERCISE

- Not all photographs have EXIF Data

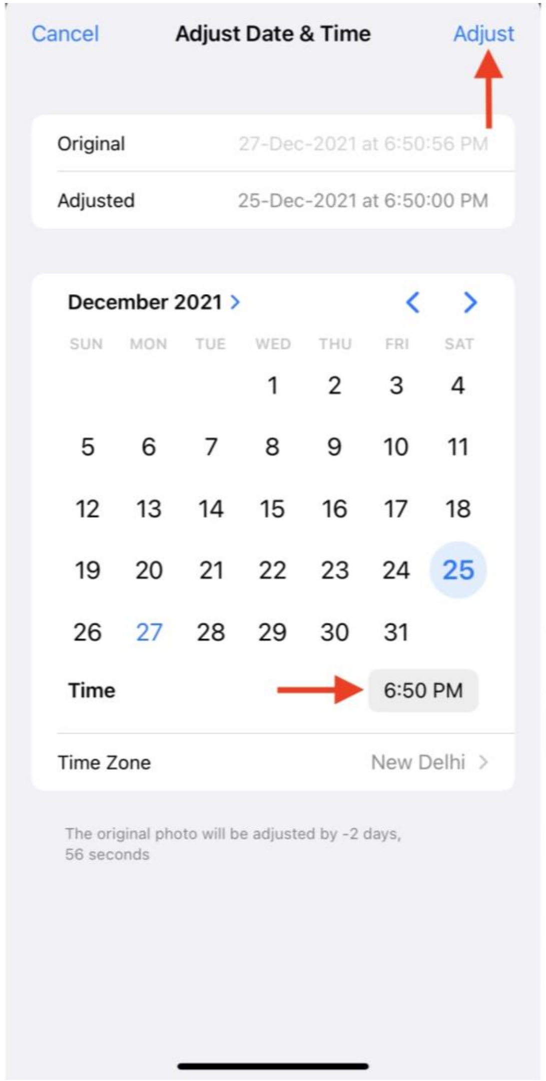


Sorry, an error occured...

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

EXIF DATA REMINDER

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



Cancel | Adjust Date & Time | Adjust

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

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

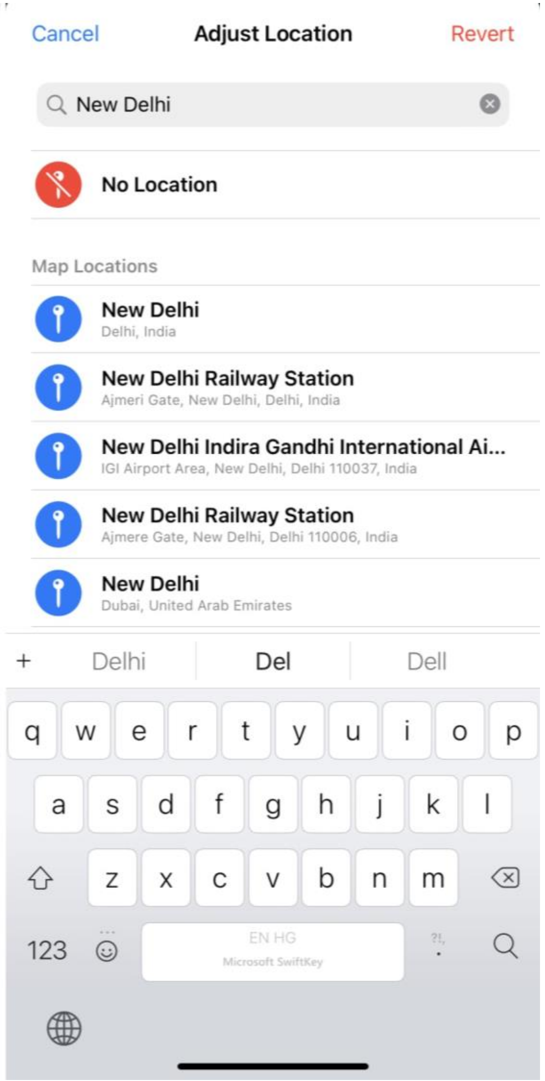
December 2021

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

Time 6:50 PM

Time Zone New Delhi

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



Cancel | Adjust Location | Revert

New Delhi

No Location

Map Locations

New Delhi
Delhi, India

New Delhi Railway Station
Ajmeri Gate, New Delhi, Delhi, India

New Delhi Indira Gandhi International Ai...
IGI Airport Area, New Delhi, Delhi 110037, India

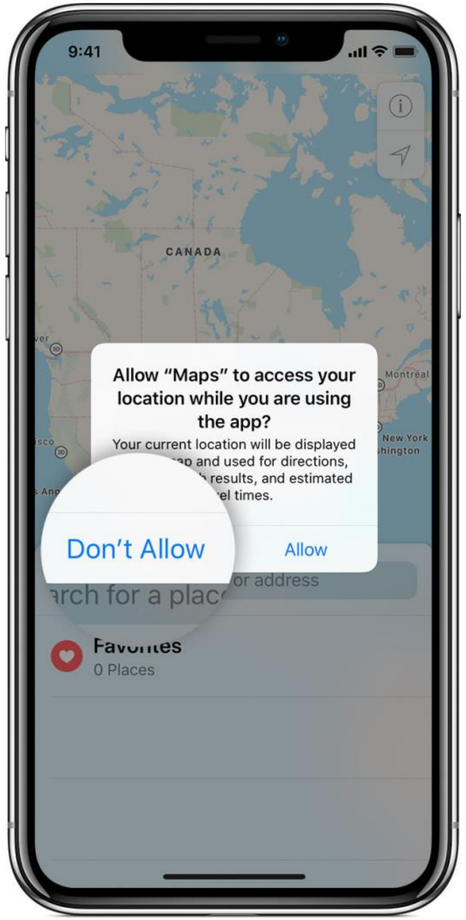
New Delhi Railway Station
Ajmere Gate, New Delhi, Delhi 110006, India

New Delhi
Dubai, United Arab Emirates

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

X - TWITTER

- In April 2024 X reported they have had 500 million monthly active users
  - UK Population in 2022 was 66 million people
- Social network commonly used and can be a rich source of information
- Users are often unaware that social media tracks lots of data useful to an investigator
  - A lot of people (myself included) just press “Allow” when installing a new application
- X is one of the social media sites which can track the location of tweets
- A number of free tools which are available online which can be used to search tweets containing geo-location data
  - One Million Tweet Map
  - Geo Social Footprint

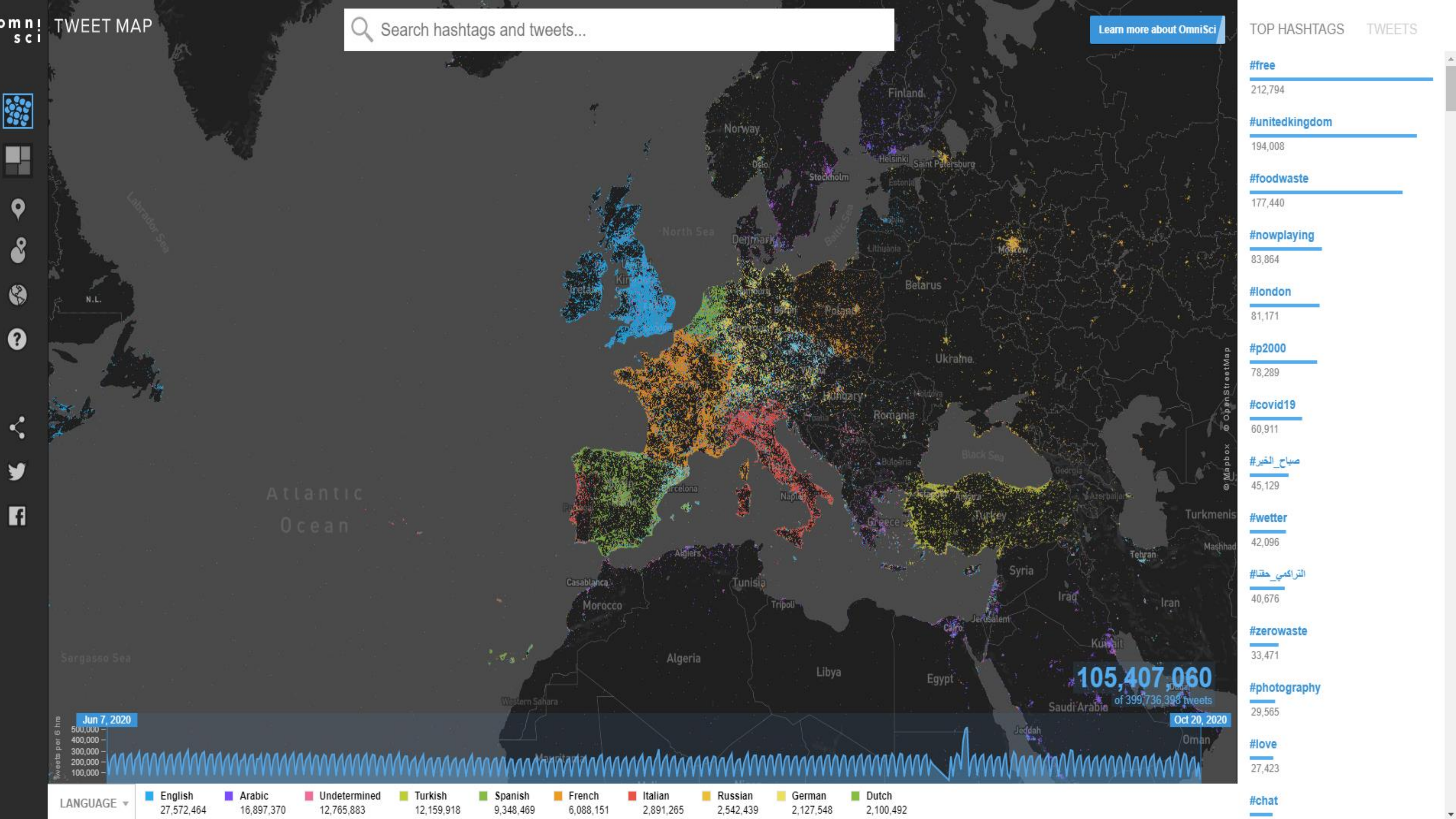


Allow “Maps” to access your location while you are using the app?

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

OMNISCI

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



omni sci TWEET MAP

Search hashtags and tweets...

Learn more about OmniSci

TOP HASHTAGS TWEETS

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

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

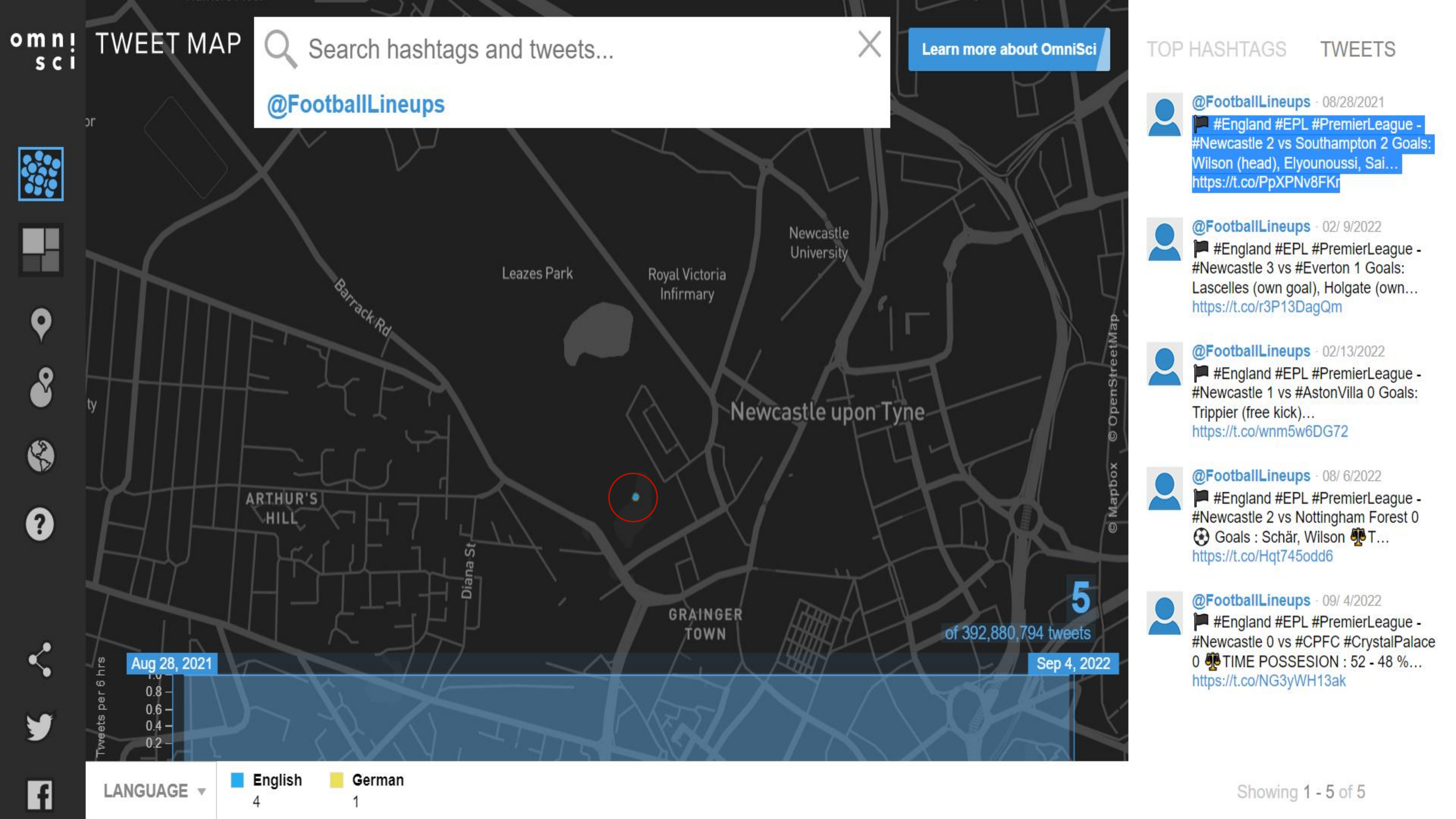
Jun 7, 2020
Oct 20, 2020

LANGUAGE ▾

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

GEO-LOCATION (X) EXERCISE

- Visit HEAVY.AI | OMNI SCI Tweetmap
- Account of interest is **@FootballLineups**
  - **@FootballLineups** is a random account I found online using OMNI SCI, the content of the account hasn't been reviewed
  - Is there any evidence to suggest the user has been to Newcastle upon Tyne



@FootballLineups

5
of 392,880,794 tweets

■ English	■ German
4	1

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

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

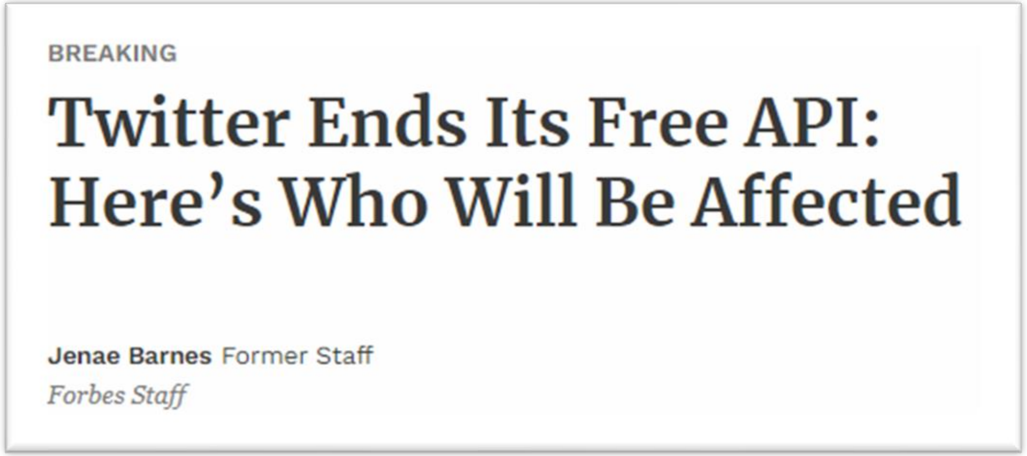
@FootballLineups · 02/13/2022
🏴 #England #EPL #PremierLeague - #Newcastle 1 vs #AstonVilla 0 Goals: Trippier (free kick)… https://t.co/wnm5w6DG72

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

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

X (TWITTER) API

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



BREAKING

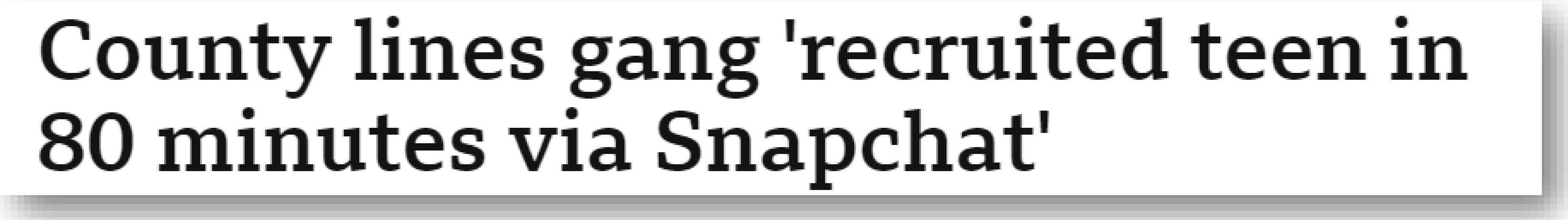
Twitter Ends Its Free API: Here's Who Will Be Affected

Jenae Barnes Former Staff

Forbes Staff

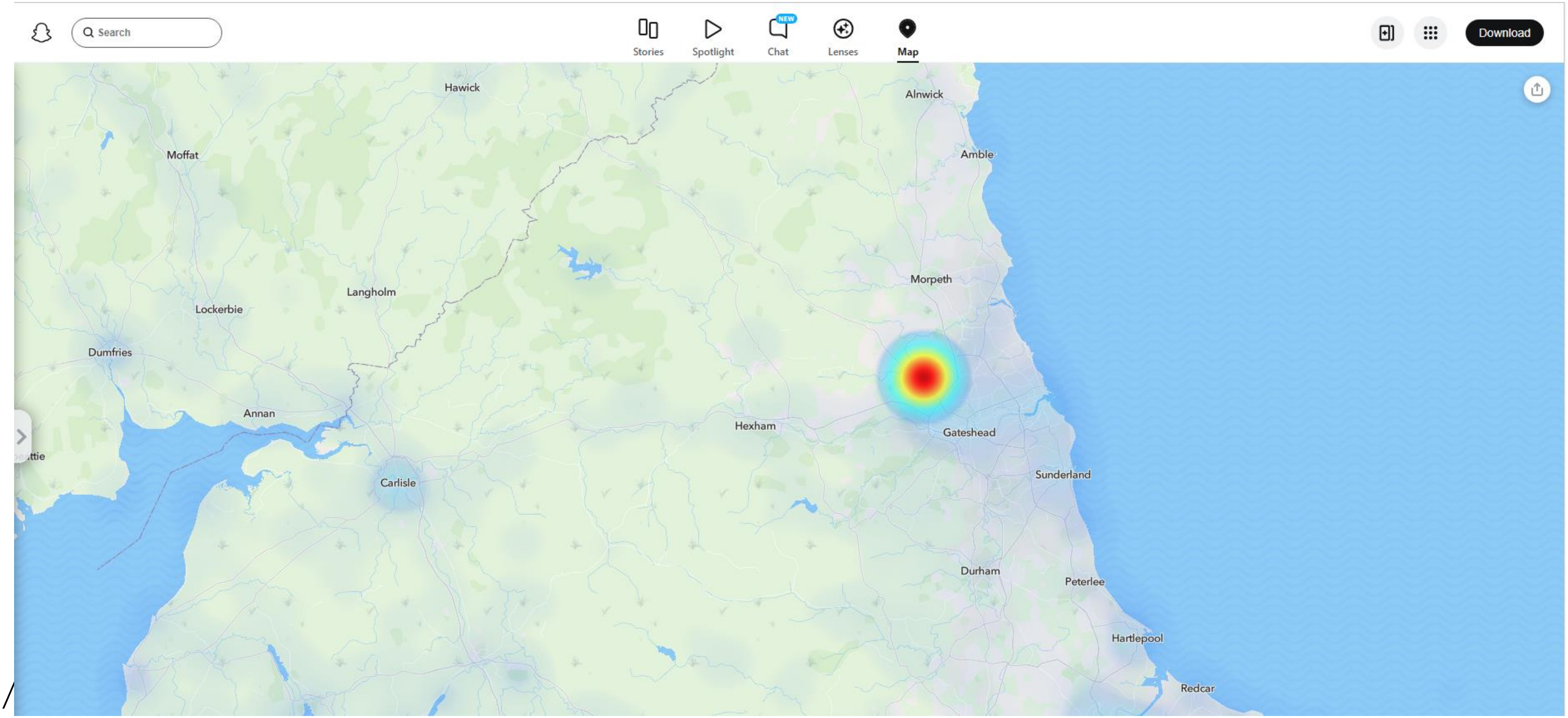
SNAPCHAT

- In 2023 Snapchat had around 397 million daily active users worldwide
- The application was originally developed for person to person sharing, it has since evolved to the use of public stories and other sharing features
- Snapchat launched Snap Map in June 2017, it allows users to see the location of their friends
  - It also allows users to view a world map and view publicly available Snaps
- Snap Map can be accessed on the Snapchat Website
  - Snap Map (snapchat.com)
  - **Recently changed – you now need a Snapchat login to review the Snapmap**
- Users can use Ghost mode to hide their location and choose no to share their Stories to the public Snap Map.



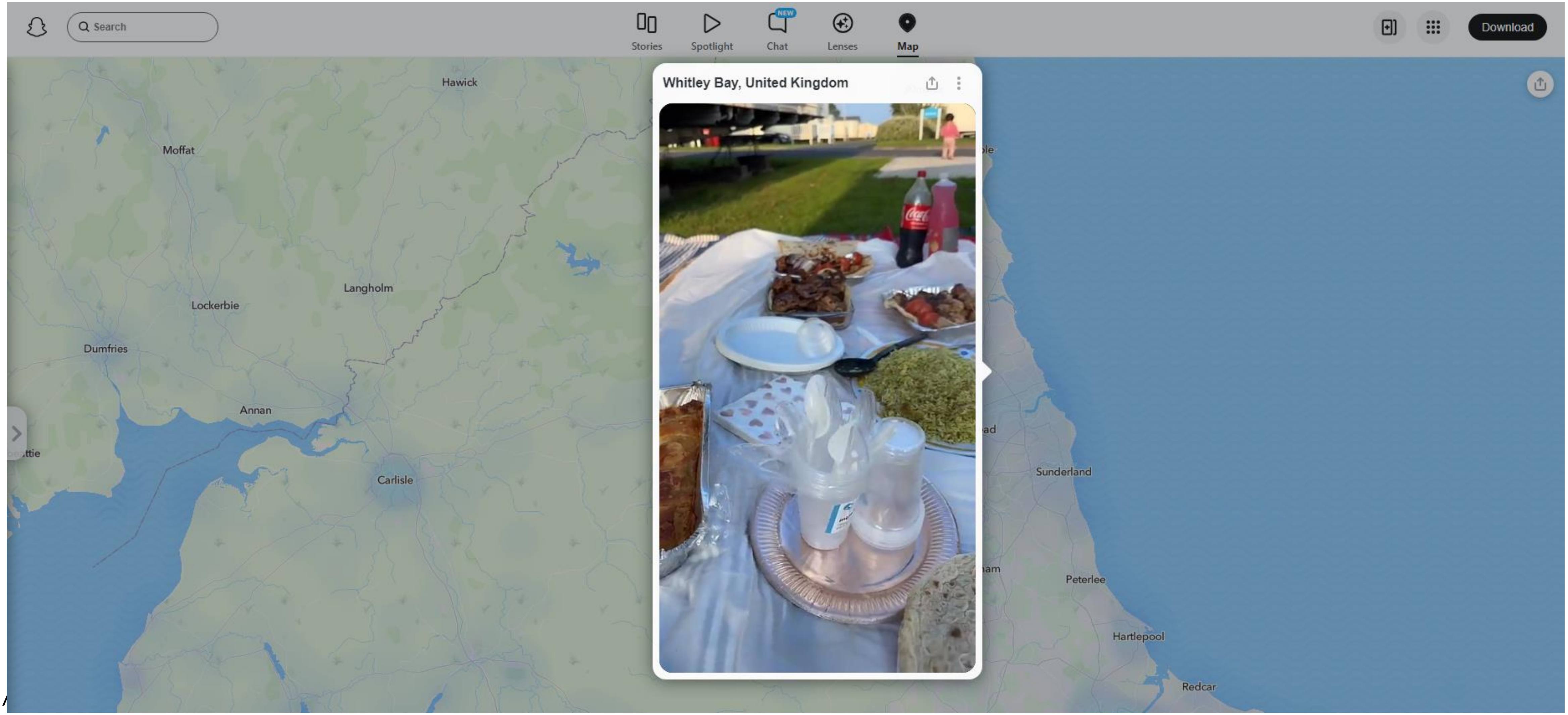
County lines gang 'recruited teen in 80 minutes via Snapchat'

SNAP MAP



Search
Stories
Spotlight
NEW
Chat
Lenses
Map
Download
Hawick
Alnwick
Moffat
Amble
Morpeth
Langholm
Lockerbie
Dumfries
Annan
Hexham
Gateshead
ttie
Carlisle
Sunderland
Durham
Peterlee
Hartlepool
Redcar

SNAP MAP

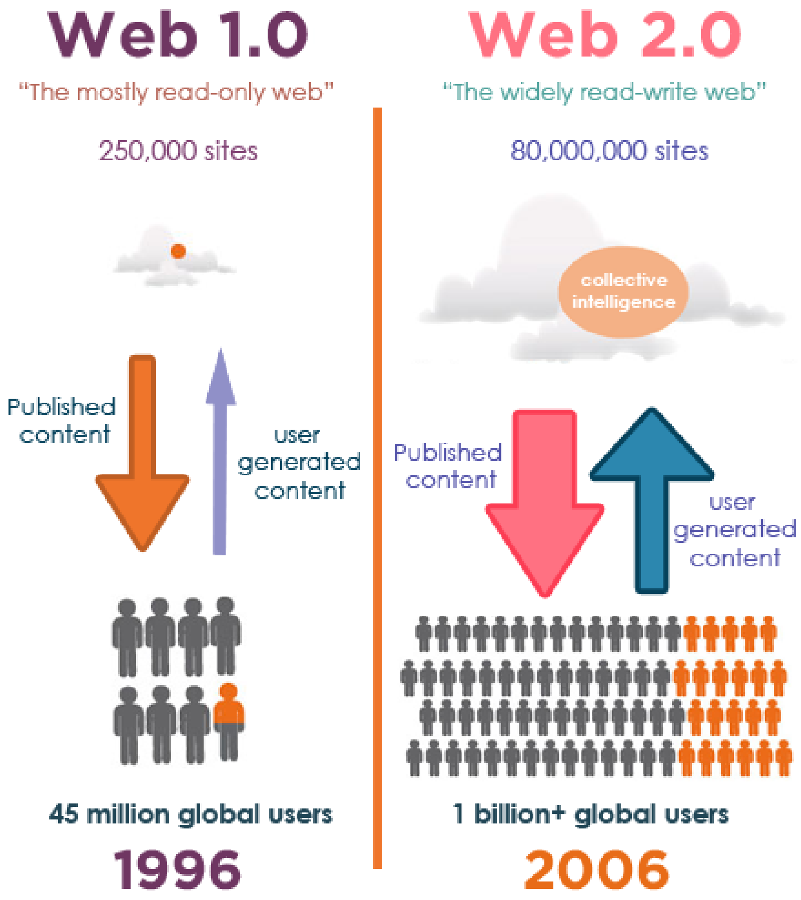


Whitley Bay, United Kingdom

Investigating Web 2.0 – social networking, blogs and online gaming

WHAT IS WEB 2.0

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



WEB 2.0 WEBSITES

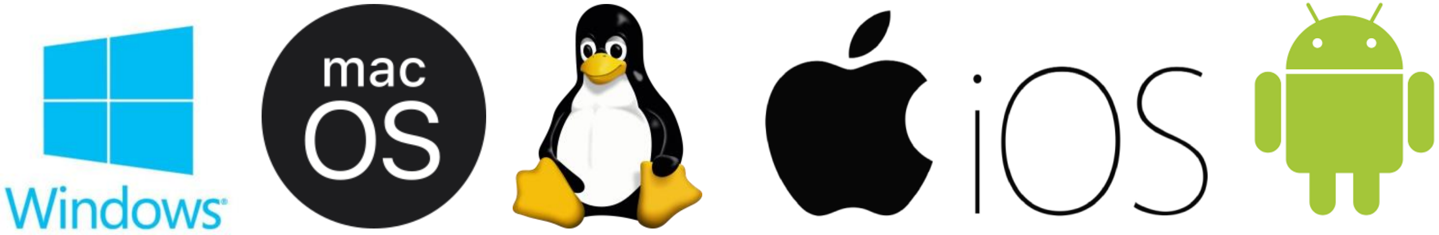
Examples of web 2.0 websites commonly used:

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

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

STEAM (ONLINE GAMING)

- Steam is digital platform owned by Valve Corporation
- Steam is a gaming platform which is used to purchase and play video games on a number of different platforms

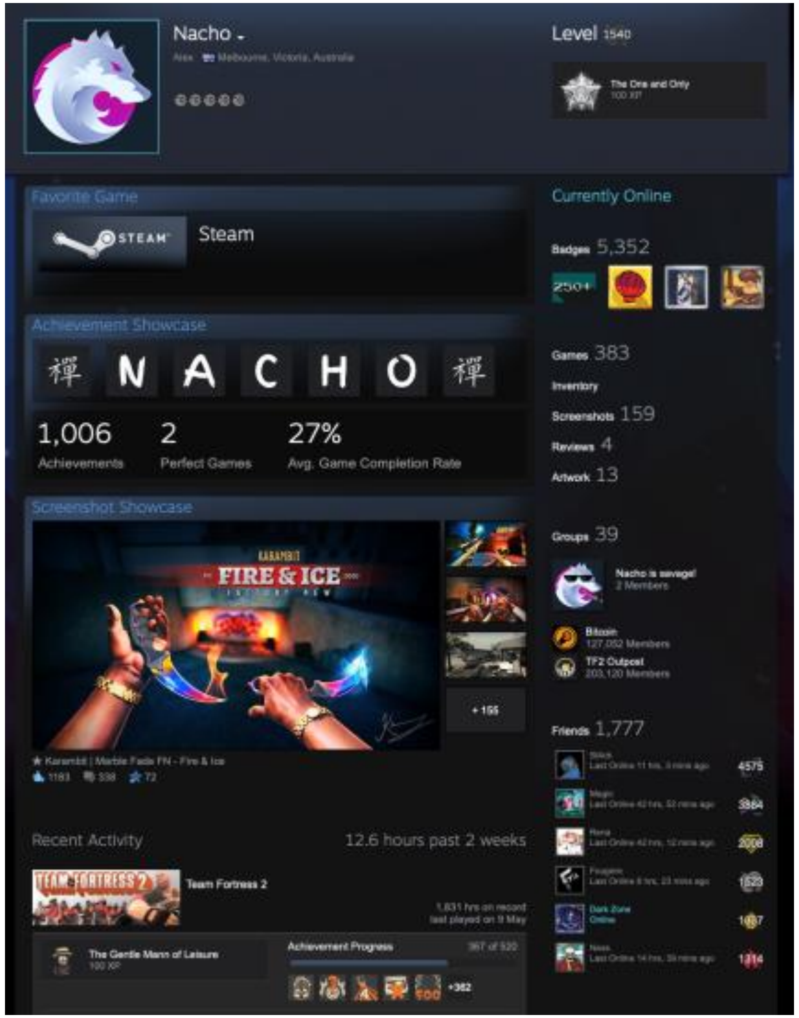


- Usage Statistics
  - Statista reported in In 2023, Steam had 33 million peak concurrent users worldwide
- Steam has the ability to stream videos and network with other users using chat (group, voice and private chat)
- Steam also has the ability to share video, pictures and tweets too
  - Sharing of tweets may allow us to explore more open source opportunities

STEAM (ONLINE GAMING)

- Steampowered.com allows you to search the Steam Community for free:
    - Search for a username
- You can then view a users profile
    - So what sort of information can we get from a users profile?
- The information we see will be dependant upon their privacy settings
    - Just like social media

STEAM USERNAME “NACHO”



Nacho
Alex Melbourne, Victoria, Australia

Level 1540

The One and Only
100 XP

Favorite Game

Steam

Achievement Showcase

禪 N A C H O 禪

1,006 Achievements

2 Perfect Games

27% Avg. Game Completion Rate

Screenshot Showcase

★ Karambit | Marble Fade FN - Fire & Ice
1183 338 72

Recent Activity 12.6 hours past 2 weeks

Team Fortress 2
1,831 hrs on record
last played on 9 May

The Gentle Mann of Leisure
100 XP

Achievement Progress 367 of 520

+362

Currently Online

Badges 5,352

Games 383

Inventory

Screenshots 159

Reviews 4

Artwork 13

Groups 39

Nacho is savage!
2 Members

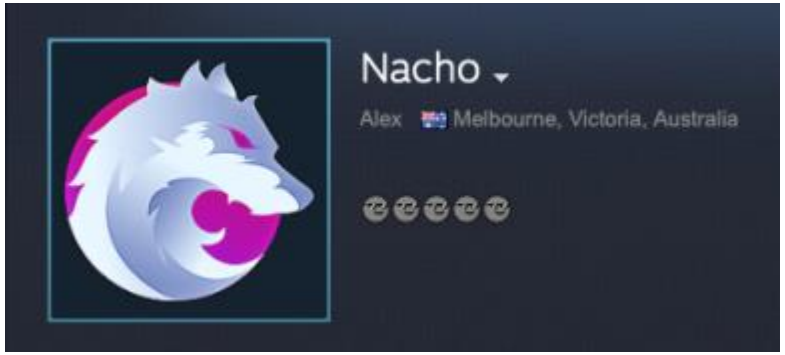
Bitcoin
127,052 Members

TF2 Outpost
203,120 Members

Friends 1,777

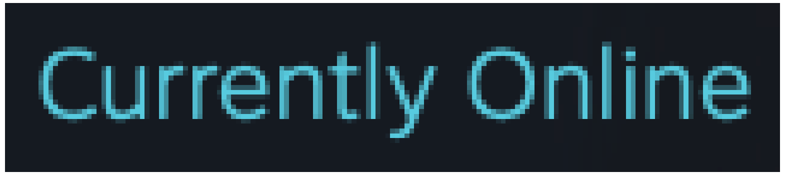
Stick	Last Online 11 hrs, 3 mins ago	4575
Magic	Last Online 42 hrs, 52 mins ago	3864
Rena	Last Online 42 hrs, 12 mins ago	2008
Fougere	Last Online 8 hrs, 23 mins ago	1523
Dark Zone	Online	1697
Nova	Last Online 14 hrs, 39 mins ago	1314

STEAM USERNAME "NACHO"

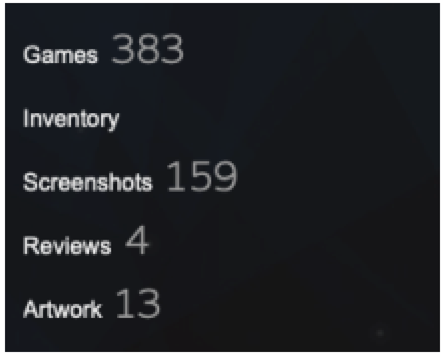


Nacho

Alex Melbourne, Victoria, Australia



Currently Online



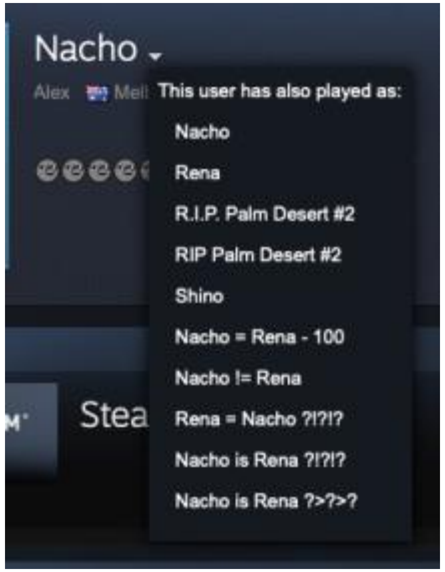
Games 383

Inventory

Screenshots 159

Reviews 4

Artwork 13



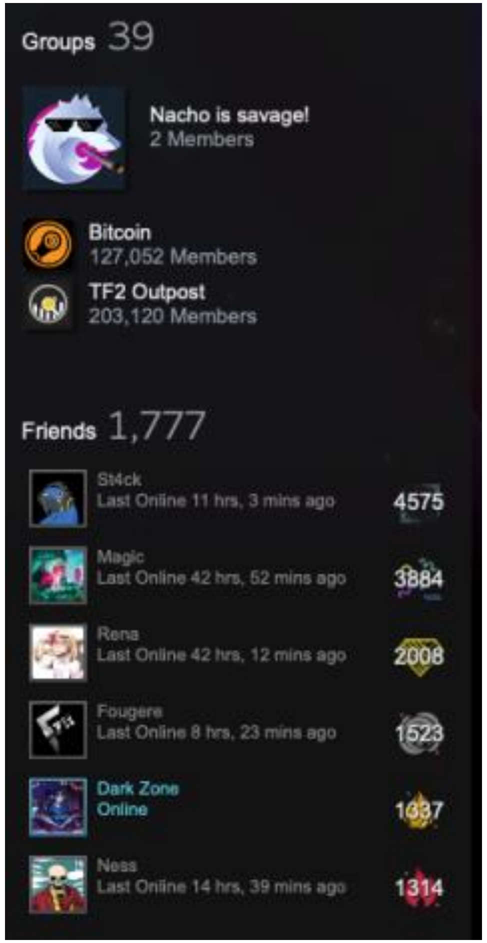
Nacho

Alex Mel

This user has also played as:

- Nacho
- Rena
- R.I.P. Palm Desert #2
- RIP Palm Desert #2
- Shino
- Nacho = Rena - 100
- Nacho != Rena
- Rena = Nacho ?!?!?
- Nacho is Rena ?!?!?
- Nacho is Rena ?>?>?

Stea



Groups 39

Nacho is savage!
2 Members

Bitcoin
127,052 Members

TF2 Outpost
203,120 Members

Friends 1,777

St4ck	Last Online 11 hrs, 3 mins ago	4575
Magic	Last Online 42 hrs, 52 mins ago	3884
Rena	Last Online 42 hrs, 12 mins ago	2008
Fougere	Last Online 8 hrs, 23 mins ago	1523
Dark Zone	Online	1637
Ness	Last Online 14 hrs, 39 mins ago	1314

INSTAGRAM

- Instagram is a social media platform designed to share images and movies
- Similar to other social networking sites, people are able to follow other users
- Instagram is now owned by Meta
- Users can lock down their profiles to allow access to only those who follow them
  - This has an impact on our open source investigation
- Statista reported
  - In 2019 Instagram had1 billion active users each month
  - In 2023, Instagram had 2 billion active users each month
- What sort of information can we obtain from a users profile?
  - Posts (Media with captions and tags)
  - Instagram Stories
  - Followers
  - Following
  - Personal bio
  - Tagged posts

INSTAGRAM EXERCISE

Instagram Exercise 1

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

Step 2) Enter “nufc” search for the profile

Can we see the profile?

Instagram Exercise 2

If you have an Instagram account (ensure it is private), try the following

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

Step 2) Enter your Instagram name and review your profile

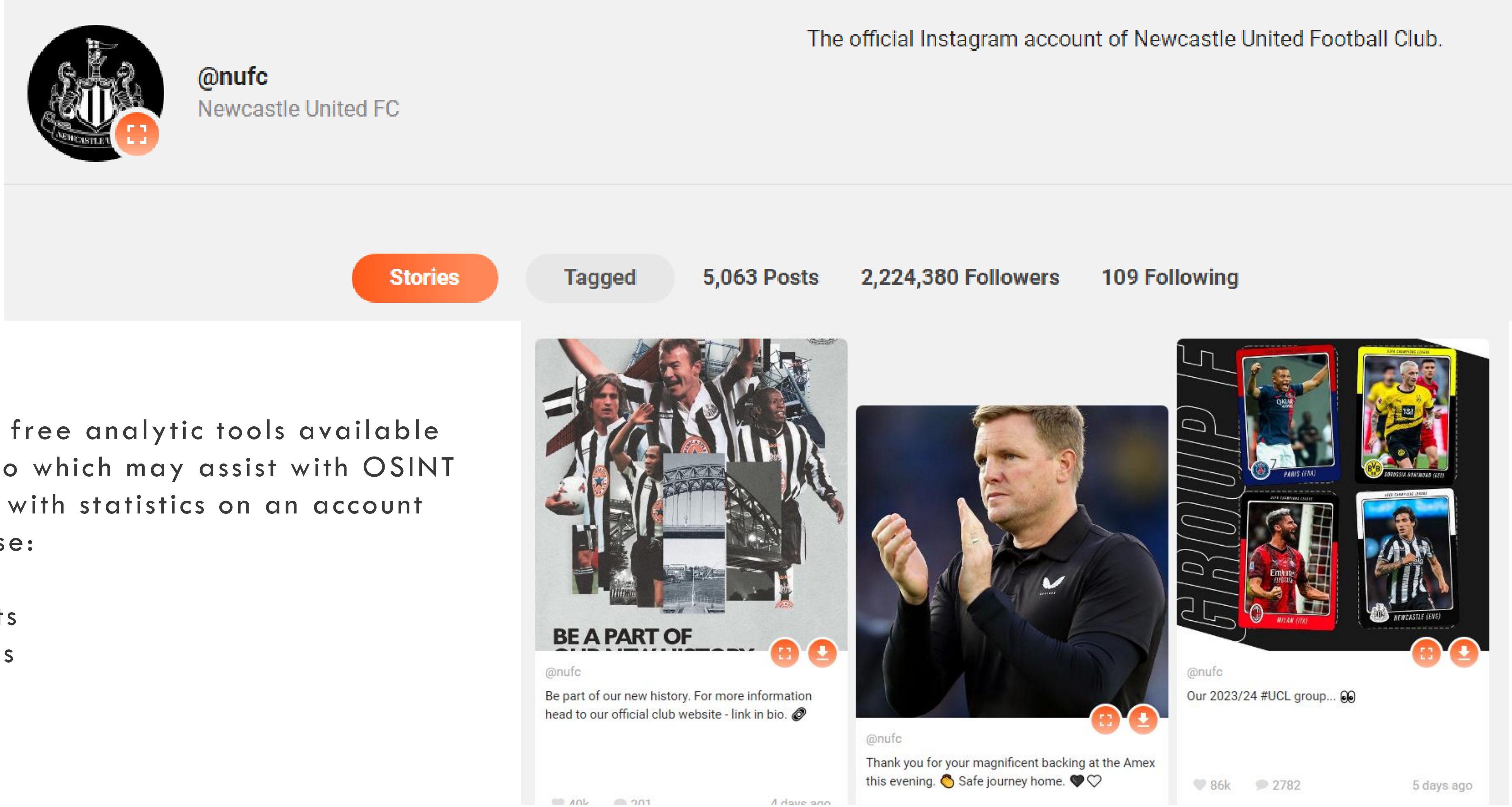
Can we see the profile?

Privacy settings on an account will impact what information we can obtain from an Instagram account.

The world is becoming more conscious about their online presence

INSTAGRAM EXERCISE

- There are a number of free analytic tools available for Instagram online too which may assist with OSINT
- These will provide you with statistics on an account should you require these:
  - Top Hashtags
  - Most popular posts
  - Common post times



@nufc

Newcastle United FC

The official Instagram account of Newcastle United Football Club.

Stories | Tagged | 5,063 Posts | 2,224,380 Followers | 109 Following

@nufc

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

40k 201 4 days ago

@nufc

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

@nufc

Our 2023/24 #UCL group... 👀

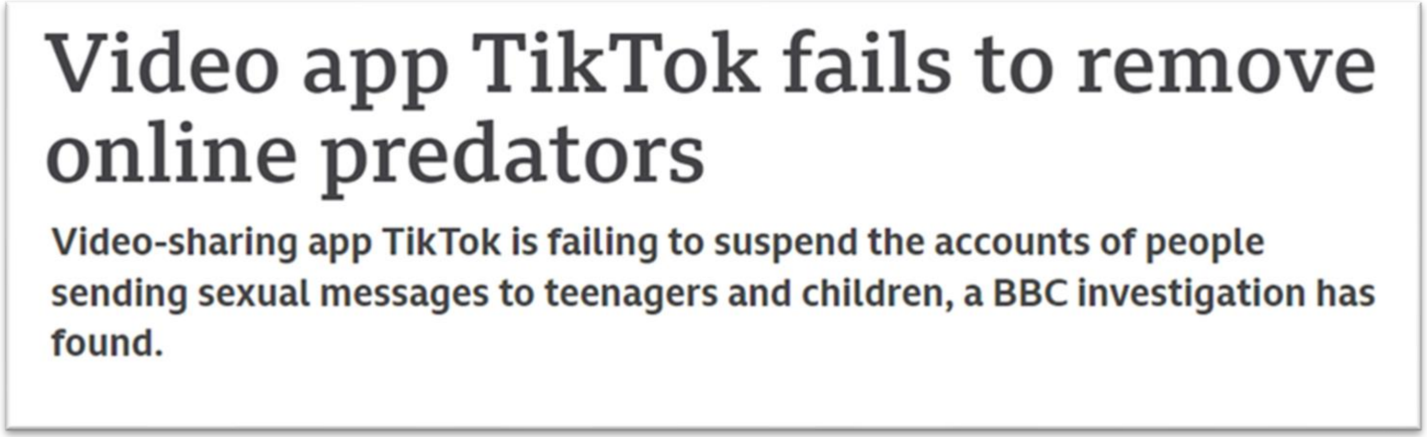
86k 2782 5 days ago

FACEBOOK

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

TIKTOK

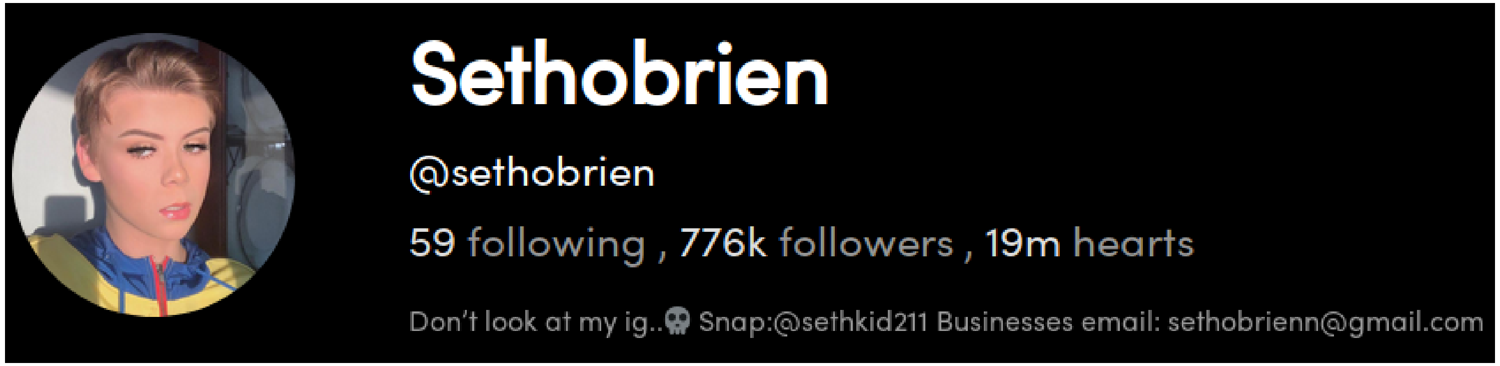
- TikTok is a social video app that allows users to share short videos.
  - Become very popular during COVID-19 lockdown
- Statista reported that TikTok have approximately 1.7 billion users worldwide
  - Up by over 66% when compared to 2020
- The application allows users to comment on videos and also offers private messaging.
- The application is incredibly popular in the UK, as a result as Digital Forensic Investigators we need to understand how the application works and any relevant forensic/open source techniques.
- As the platform is relatively new, techniques are constantly changing



Video app TikTok fails to remove online predators

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

TIKTOK EXERCISE



Sethobrien

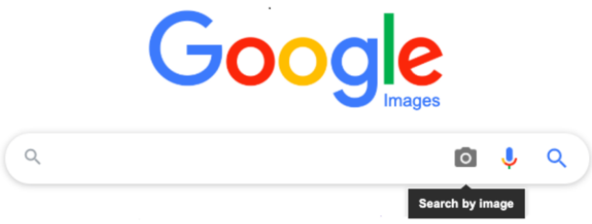
@sethobrien

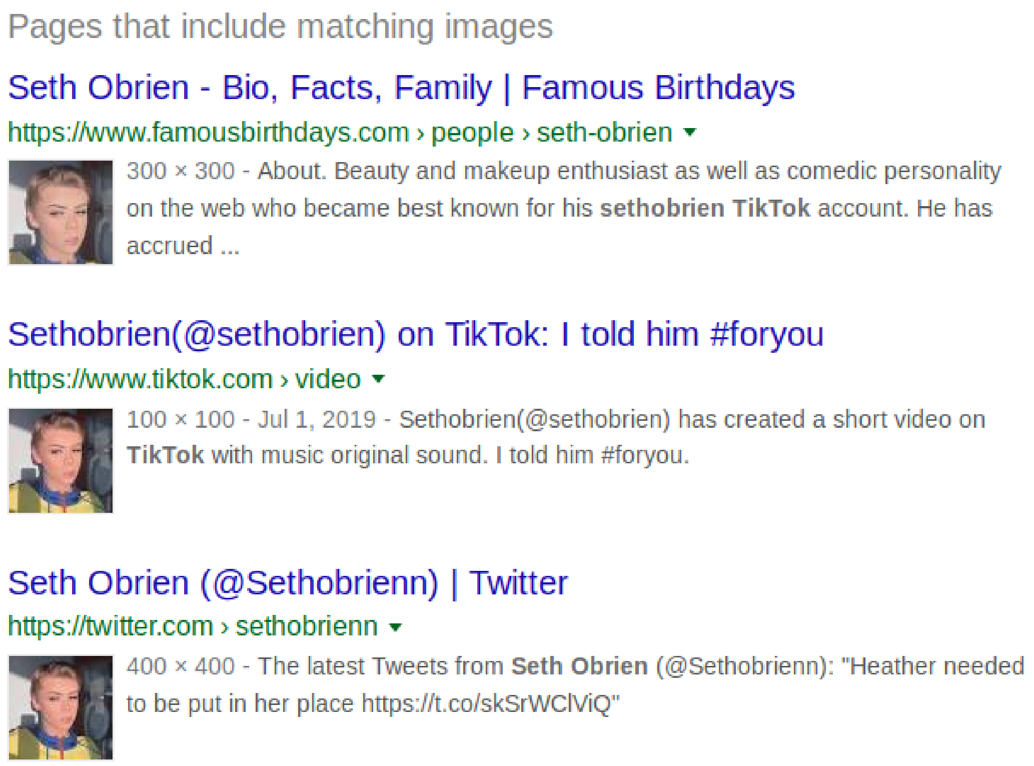
59 following , 776k followers , 19m hearts

Don’t look at my ig..💀 Snap:@sethkid211 Businesses email: sethobrienn@gmail.com

TIKTOK EXERCISE

- There aren’t always tools available to assist in open source investigations for a particular website
- Don’t forget about the power of search engines
  - Google
  - Bing
- Conducting a reverse image search of the TikTok profile picture may assist us




Pages that include matching images

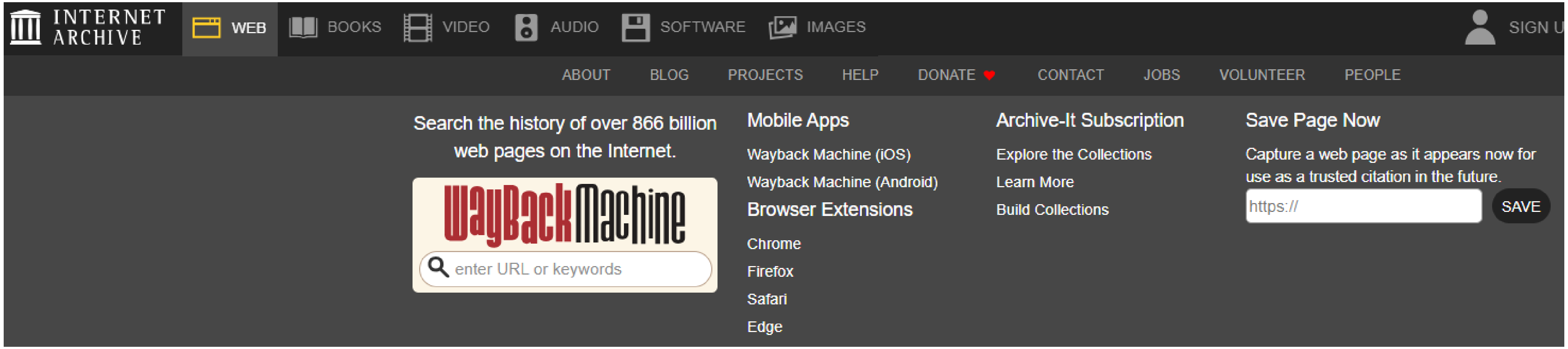
Seth Obrien - Bio, Facts, Family | Famous Birthdays
https://www.famousbirthdays.com › people › seth-obrien ▾
300 × 300 - About. Beauty and makeup enthusiast as well as comedic personality on the web who became best known for his **sethobrien TikTok** account. He has accrued ...

Sethobrien(@sethobrien) on TikTok: I told him #foryou
https://www.tiktok.com › video ▾
100 × 100 - Jul 1, 2019 - Sethobrien(@sethobrien) has created a short video on **TikTok** with music original sound. I told him #foryou.

Seth Obrien (@Sethobrienn) | Twitter
https://twitter.com › sethobrienn ▾
400 × 400 - The latest Tweets from **Seth Obrien** (@Sethobrienn): "Heather needed to be put in her place https://t.co/skSrWClViQ"

TIKTOK POST CAPTURE

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



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

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

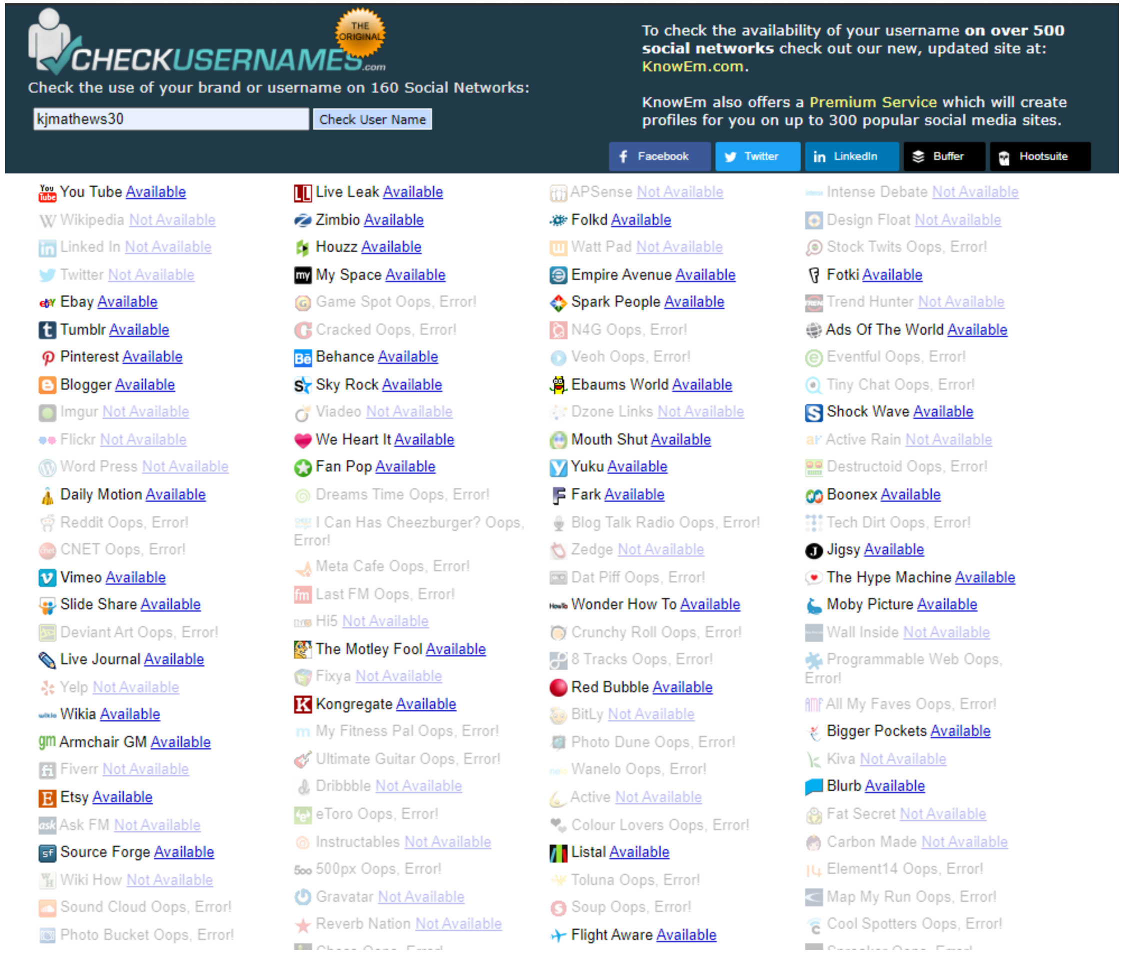
- Conducting an opensource investigation on TikTok Web Version has limitations
  - Web browser version wont show the comments
  - Full content is available the TikTok app

GOOGLE

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

ONLINE USERNAMES

- In my experience, users often use their usernames across various platforms
- This is often very useful when trying to identify any other platforms of interest
- There are a number of resources freely available online to identify whether a given username is available on a website
  - https://checkusernames.com is a useful resource to identify whether the username is used on another website
    - Checkusernames searches 160 social networks
  - Namechk (www.namechk.com)
  - Further verification will then be required on the website to identify further information about the account
  - Google OSINT YouTube and various resources will be returned



Check the use of your brand or username on 160 Social Networks:

kjmathews30 | Check User Name

To check the availability of your username **on over 500 social networks** check out our new, updated site at: KnowEm.com.

KnowEm also offers a Premium Service which will create profiles for you on up to 300 popular social media sites.

You Tube Available
Wikipedia Not Available
Linked In Not Available
Twitter Not Available
Ebay Available
Tumblr Available
Pinterest Available
Blogger Available
Imgur Not Available
Flickr Not Available
Word Press Not Available
Daily Motion Available
Reddit Oops, Error!
CNET Oops, Error!
Vimeo Available
Slide Share Available
Deviant Art Oops, Error!
Live Journal Available
Yelp Not Available
Wikia Available
Armchair GM Available
Fiverr Not Available
Etsy Available
Ask FM Not Available
Source Forge Available
Wiki How Not Available
Sound Cloud Oops, Error!
Photo Bucket Oops, Error!

Live Leak Available
Zimbio Available
Houzz Available
My Space Available
Game Spot Oops, Error!
Cracked Oops, Error!
Behance Available
Sky Rock Available
Viadeo Not Available
We Heart It Available
Fan Pop Available
Dreams Time Oops, Error!
I Can Has Cheezburger? Oops, Error!
Meta Cafe Oops, Error!
Last FM Oops, Error!
Hi5 Not Available
The Motley Fool Available
Fixya Not Available
Kongregate Available
My Fitness Pal Oops, Error!
Ultimate Guitar Oops, Error!
Dribbble Not Available
eToro Oops, Error!
Instructables Not Available
500px Oops, Error!
Gravatar Not Available
Reverb Nation Not Available

APSense Not Available
Folkd Available
Watt Pad Not Available
Empire Avenue Available
Spark People Available
N4G Oops, Error!
Veoh Oops, Error!
Ebaums World Available
Dzone Links Not Available
Mouth Shut Available
Yuku Available
Fark Available
Blog Talk Radio Oops, Error!
Zedge Not Available
Dat Piff Oops, Error!
Wonder How To Available
Crunchy Roll Oops, Error!
8 Tracks Oops, Error!
Red Bubble Available
BitLy Not Available
Photo Dune Oops, Error!
Wanelo Oops, Error!
Active Not Available
Colour Lovers Oops, Error!
Listal Available
Toluna Oops, Error!
Soup Oops, Error!
Flight Aware Available

Intense Debate Not Available
Design Float Not Available
Stock Twits Oops, Error!
Fotki Available
Trend Hunter Not Available
Ads Of The World Available
Eventful Oops, Error!
Tiny Chat Oops, Error!
Shock Wave Available
Active Rain Not Available
Destructoid Oops, Error!
Boonex Available
Tech Dirt Oops, Error!
Jigsy Available
The Hype Machine Available
Moby Picture Available
Wall Inside Not Available
Programmable Web Oops, Error!
All My Faves Oops, Error!
Bigger Pockets Available
Kiva Not Available
Blurb Available
Fat Secret Not Available
Carbon Made Not Available
Element14 Oops, Error!
Map My Run Oops, Error!
Cool Spotters Oops, Error!

OPEN SOURCE INVESTIGATION CHALLENGES

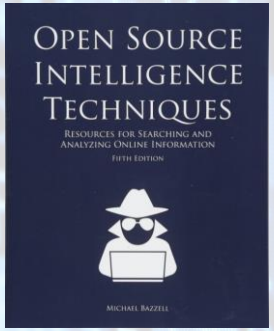
- There are a number challenges in relation to open source investigations
  - Legislation (cross-borders)
    - The techniques are available, but are they legal? (DSA, TEI, IPA etc)
  - Online platforms regularly change their functionality
    - It is not uncommon for applications to update (on a weekly basis)
    - As a result, a tool that worked yesterday, may not be able to interpret the data today
    - Support for tools is limited – may be taken offline with no notice
  - New social networks and applications
  - Privacy settings
    - Privacy is a fundamental part of peoples lives
  - Data is online and real-time
    - Data can easily be deleted or hidden by users, capturing the data at the earliest opportunity is important
    - Consider the Wayback Machine
  - Validation of tools
    - Accreditation standards - ISO/IEC 17025:2017
    - Bellingcat Article – Russia ECHR Article

THANK YOU
ANY QUESTIONS?

Seanpaul Gilroy

Useful Resources

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


OPEN SOURCE INTELLIGENCE TECHNIQUES
RESOURCES FOR SEARCHING AND ANALYZING ONLINE INFORMATION
FIFTH EDITION
MICHAEL BAZZELL

Hessisches Ministerium der Justiz

HESSEN

Ransomware, Online Child Sexual Abuse and Non-Cash Payment Fraud

POST-COVID CHALLENGES IN CRIMINAL JUSTICE
INVESTIGATING WEB 2.0

Thessaloniki, 23-24 May 2024

Co-funded by the European Union

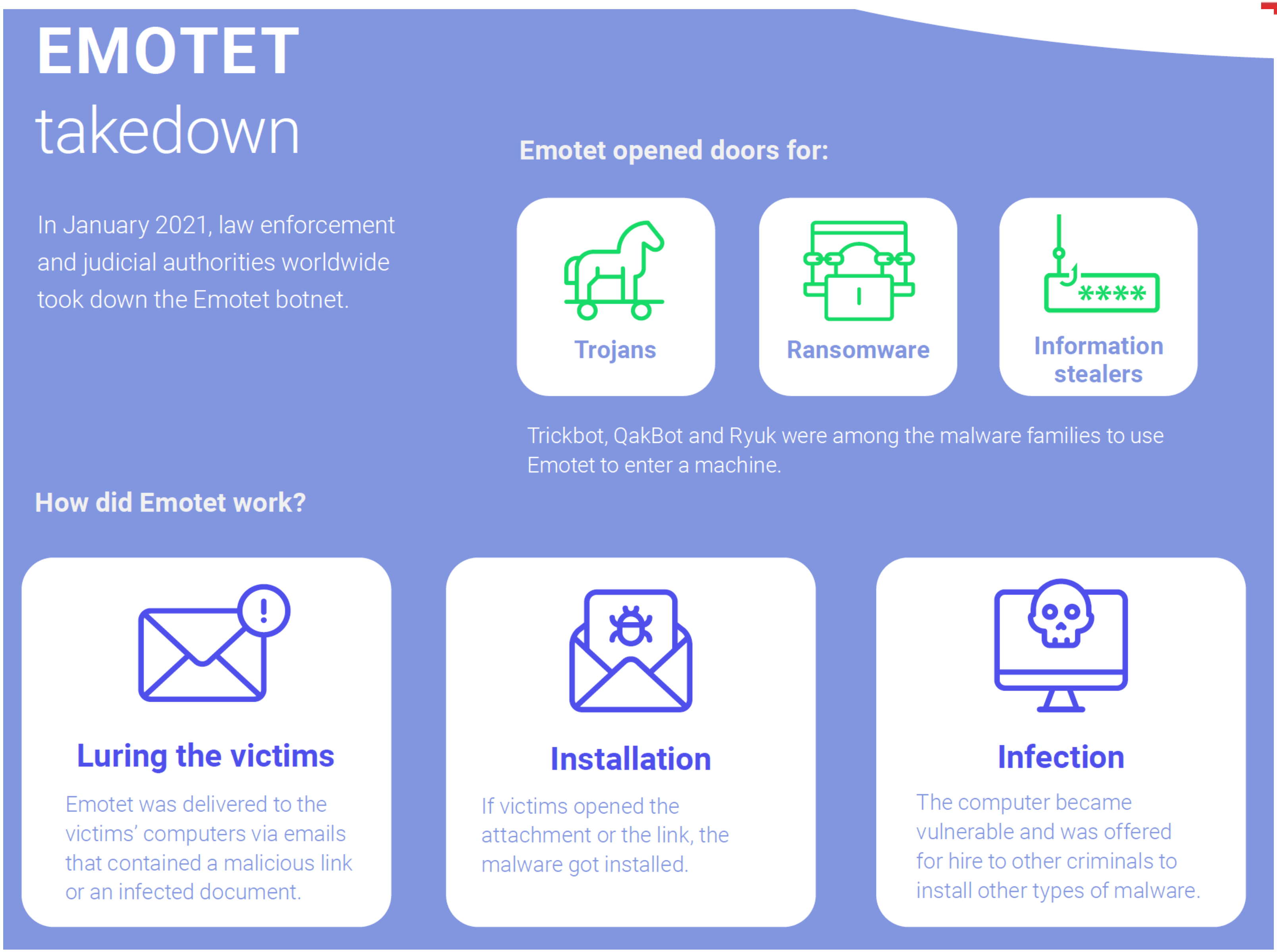
Rainer Franosch, Deputy Director-General for Criminal Law
Ministry of Justice of the German Federal State of Hesse

Ransomware

- Ransomware remains the primary threat – malware is becoming increasingly accessible and is constantly evolving.
- Leaks of source code enable even less skilled actors to deploy ransomware. The reuse of existing source codes, with some modifications possibly made, leads to new and readily available ransomware variants.
- Even after the dismantling or dissolution of ransomware groups, source code from ransomware continues to pose a threat.
- The damage potential of ransomware is increasing rapidly.
- According to Allianz Insurance, ransomware alone is expected to cost its victims about $265 billion annually by 2031, primarily referring to the costs of rebuilding.

The Emotet investigation

The Emotet investigation



EMOTET takedown

In January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet.

Emotet opened doors for:

- Trojans
- Ransomware
- Information stealers

Trickbot, QakBot and Ryuk were among the malware families to use Emotet to enter a machine.

How did Emotet work?

Luring the victims

Emotet was delivered to the victims' computers via emails that contained a malicious link or an infected document.

Installation

If victims opened the attachment or the link, the malware got installed.

Infection

The computer became vulnerable and was offered for hire to other criminals to install other types of malware.

What was Emotet?

- Emotet was a prolific spam-based malware and botnet.
- During its lifespan, Emotet sent billions of spam phishing emails and infected millions of victim computers.
- Emotet caused hundreds of millions of dollars in total loss. Some cybersecurity researchers estimate more than two billion in loss.

What was Emotet? (cont'd)

- As malware, Emotet was identified by cybersecurity researchers as early as 2014 as a banking Trojan.
- Over time, Emotet evolved into a loader or dropper of other malware, including ransomware: Trickbot (and Ryuk), Dridex, Qakbot, IcedID/Bokbot, and ZeuS Panda.
- Malware-as-a-Service

Who has been affected in Germany?

- Courts
- Federal agencies
- Municipalities
- Hospitals
- Medical practices
- Universities
- Schools
- Companies

Emotet disruption

- In January 2021, Emotet was dismantled through an international effort coordinated through Eurojust.

- It was important to understand the technical details of the malware and its distribution and control infrastructure.

- Equally essential was focusing on people, in particular the Emotet server administrator.

How was Emotet spread?

- Emotet malware spread primarily through spam phishing emails with malicous scripts or attachments.
- Spam was targeted against particular countries and industries with custom attachments.
- During initial infection, victim computers downloaded Emotet malware from a distribution server and then received instructions from control servers.

Characteristics of Emotet malware

- Emotet malware was polymorphic, meaning parts of the code changed periodically.
- Emotet could detect being run in a virtual machine.
- Emotet harvested credentials from the victim computer and then spread within the network by brute-force guessing credentials to other networked computers.

Lifecycle of an Emotet infection

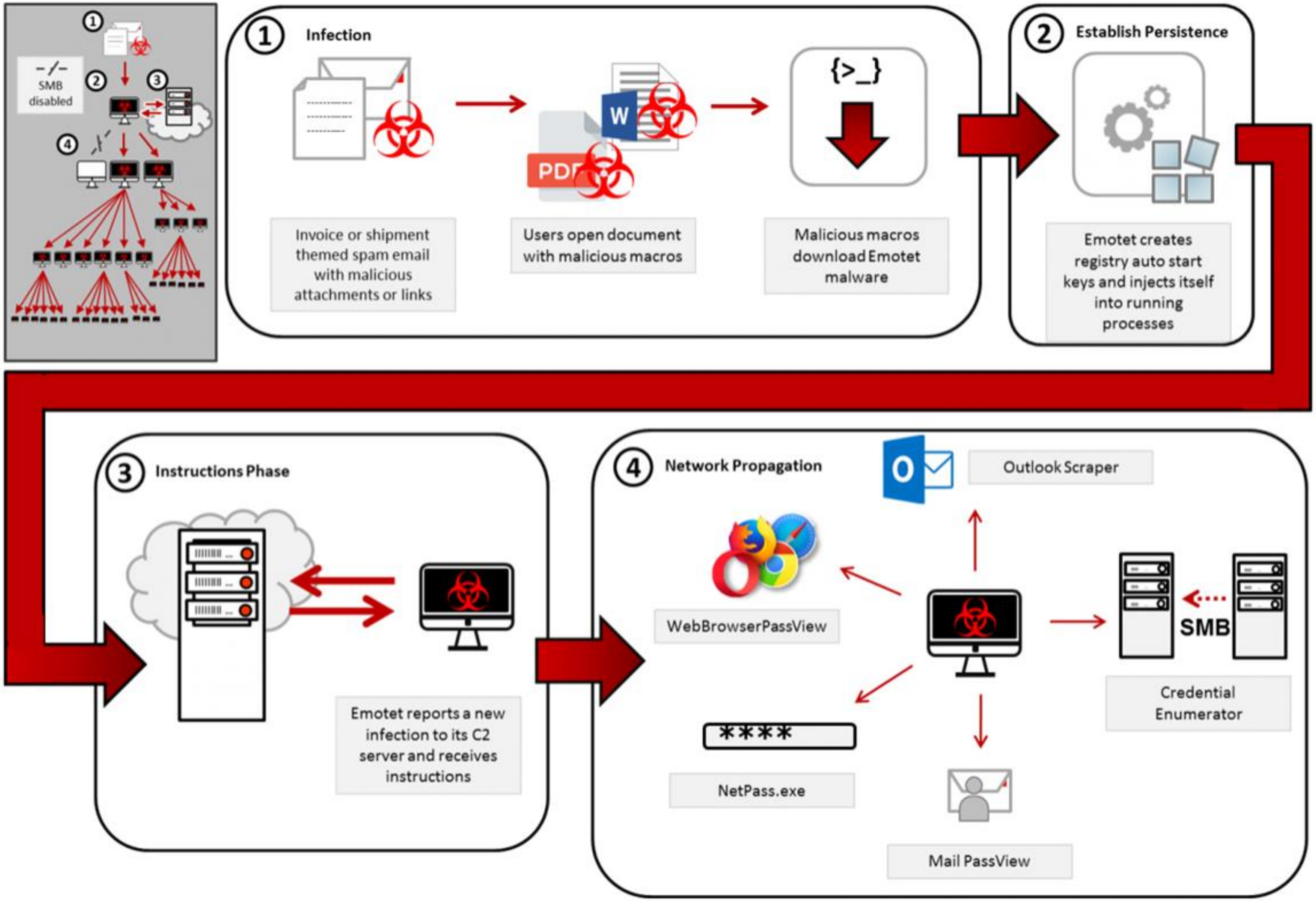

1
2
3
4
SMB disabled
1 Infection
Invoice or shipment themed spam email with malicious attachments or links
Users open document with malicious macros
W
PDF
{>_}
Malicious macros download Emotet malware
2 Establish Persistence
Emotet creates registry auto start keys and injects itself into running processes
3 Instructions Phase
Emotet reports a new infection to its C2 server and receives instructions
4 Network Propagation
O
Outlook Scraper
WebBrowserPassView
SMB
Credential Enumerator
****
NetPass.exe
Mail PassView

Figure 2: Emotet infection process

Emotet malware (cont’d)

- Emotet malware on victim computers was hard-coded with Internet Protocol (IP) addresses of control servers.

- The malware cycled through these IPs until making a successful connection. Then, every 15 minutes, the malware was updated, including new control server IPs.

- Other malware, including ransomare, was loaded through Emotet.

Emotet tiered infrastructure

- Emotet distribution and control networks were tiered.
- Tier 1 servers, which tended to be compromised servers, communicated with Tier 2 servers, which communicated with Tier 3 servers.
- All communications were encrypted.

Why was Emotet so prolific?

- The Malware: Relentless spam campaigns. Persistence within networks. Updated every 15 minutes.
- The Infrastructure: Tiered distribution and control servers. Multiple epochs. Different encryption keys.
- Scale: By January 2021, there were more than 1500 distribution and control servers located in more than 60 countries.

The beginning of the investigation

- **Phenomenological evaluation on Emotet by the BKA.**
- **Malware analysis by the BKA.**
- **In August 2018, the BSI shared the address of a server hosted in Brazil from which Emotet was being downloaded and whose log files were freely accessible.**

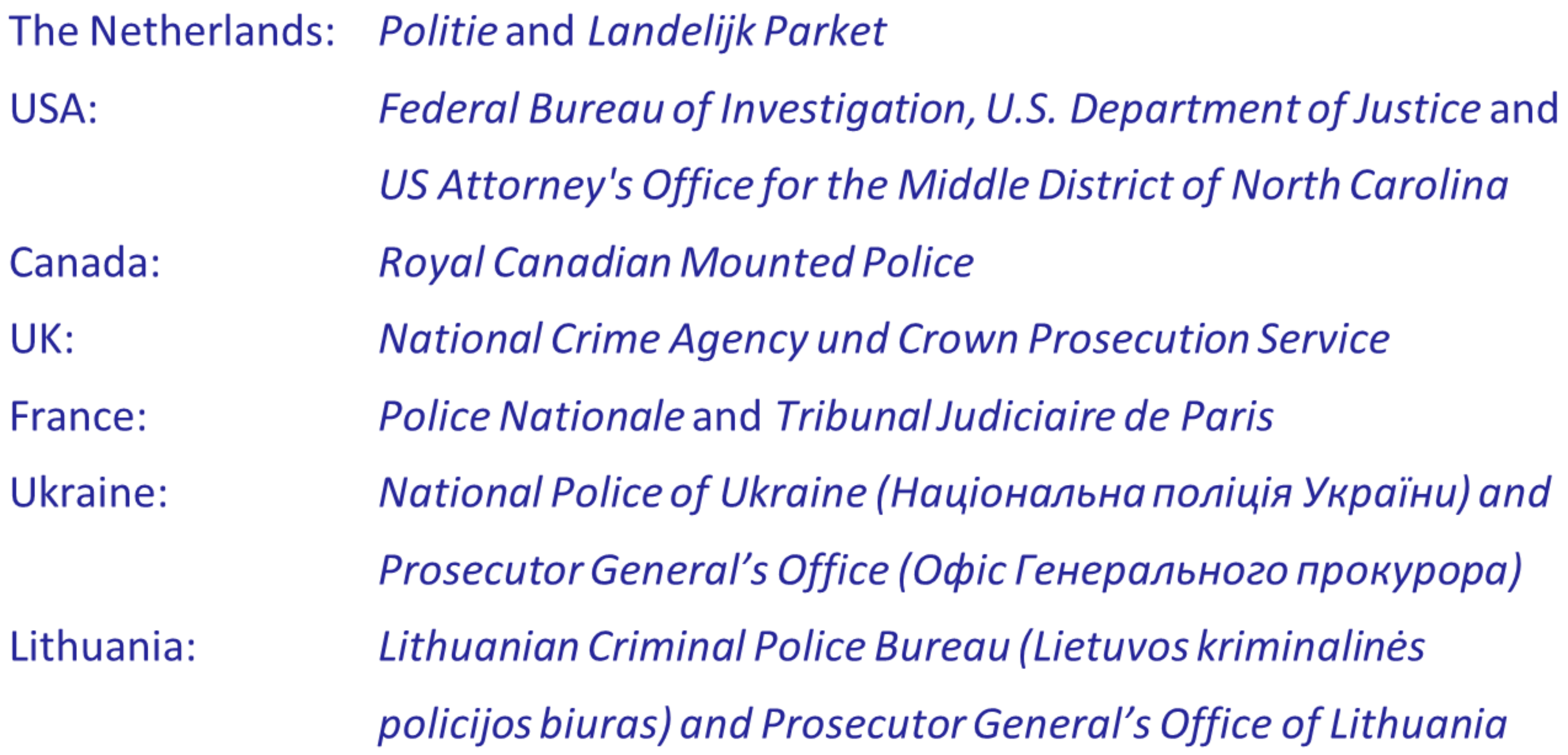
The beginning of the investigation

- **In these log files, a technical address of a server hosted at a provider in Germany relevant within the Emotet infrastructure could be detected.**
- **Cybercrime Center of the GPPO Frankfurt started a formal investigation, wire-tapping this server – many should follow.**

The Emotet investigation

HESSEN

International partners
Law enforcement agencies and judicial authorities from 7 countries:



The Netherlands:	*Politie* and *Landelijk Parket*
USA:	*Federal Bureau of Investigation, U.S. Department of Justice* and *US Attorney's Office for the Middle District of North Carolina*
Canada:	*Royal Canadian Mounted Police*
UK:	*National Crime Agency und Crown Prosecution Service*
France:	*Police Nationale* and *Tribunal Judiciaire de Paris*
Ukraine:	*National Police of Ukraine (Національна поліція України) and Prosecutor General’s Office (Офіс Генерального прокурора)*
Lithuania:	*Lithuanian Criminal Police Bureau (Lietuvos kriminalinės policijos biuras) and Prosecutor General’s Office of Lithuania*

Coordination of international cooperation

EUROJUST

Conferences coordinated by Eurojust for the development of common strategies and the exchange of information between representatives of law enforcement agencies and judicial authorities from the participating countries, with the involvement of representatives of Europol on a regular basis.

EUROPOL

Challenges and solutions

Planning of an international action day with joint actions in individual countries, including national measures as well as measures by way of mutual legal assistance under COVID-19 restrictions

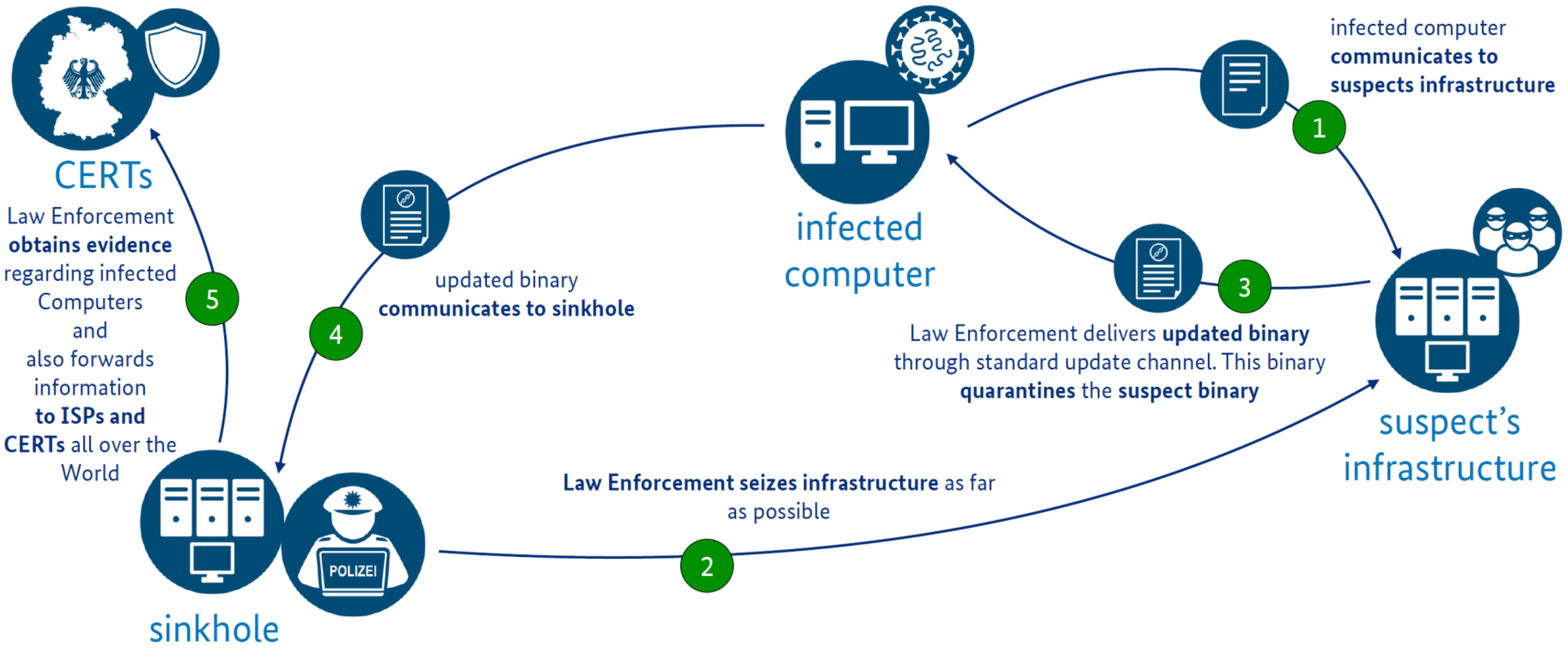
- **operational centers at Europol and Eurojust with colleagues on site as well as supporting video conferences**
- **national operational centers**

Challenges and solutions

Legal basis of rerouting the traffic of the purely IP-based, constantly changing Emotet infrastructure

- „ hybrid court order" with elements of seizure, as well as the usage of the so-called annex competence with extension to systems newly discovered through technical measures

Challenges and solutions



CERTs
Law Enforcement **obtains evidence** regarding infected Computers and also forwards information **to ISPs and CERTs** all over the World
5
4
updated binary **communicates to sinkhole**
infected computer
infected computer **communicates to suspects infrastructure**
1
3
Law Enforcement delivers **updated binary** through standard update channel. This binary **quarantines** the **suspect binary**
suspect's infrastructure
Law Enforcement seizes infrastructure as far as possible
2
POLIZEI
sinkhole

Challenges and solutions

Limits of the legal and factual implementation possibilities of the measures in the countries involved, in particular the legal transfer of the measures requested by way of mutual legal assistance

- ➢ **requests for legal assistance were prepared in close coordination with colleagues from the requested and requesting countries**

Online Child Sexual Abuse

What has the COVID-19 pandemic changed?

- The global impact of COVID-19 means people are spending more time online. This includes both children and adults.

- Adults working remotely are less able to spend time with their children, who are allowed greater unsupervised internet access. As a result, children are:

  - ➢ more exposed to offenders through online gaming, the use of chat groups in apps, unsolicited contact in social media and through less secure online educational applications;
  - ➢ more inclined towards making explicit material to exchange with peers, eventually reaching child sex offenders;
  - ➢ in some cases, becoming lonely and isolated, which offenders try to benefit from, connecting with them to produce explicit material or to arrange a meeting in real life.

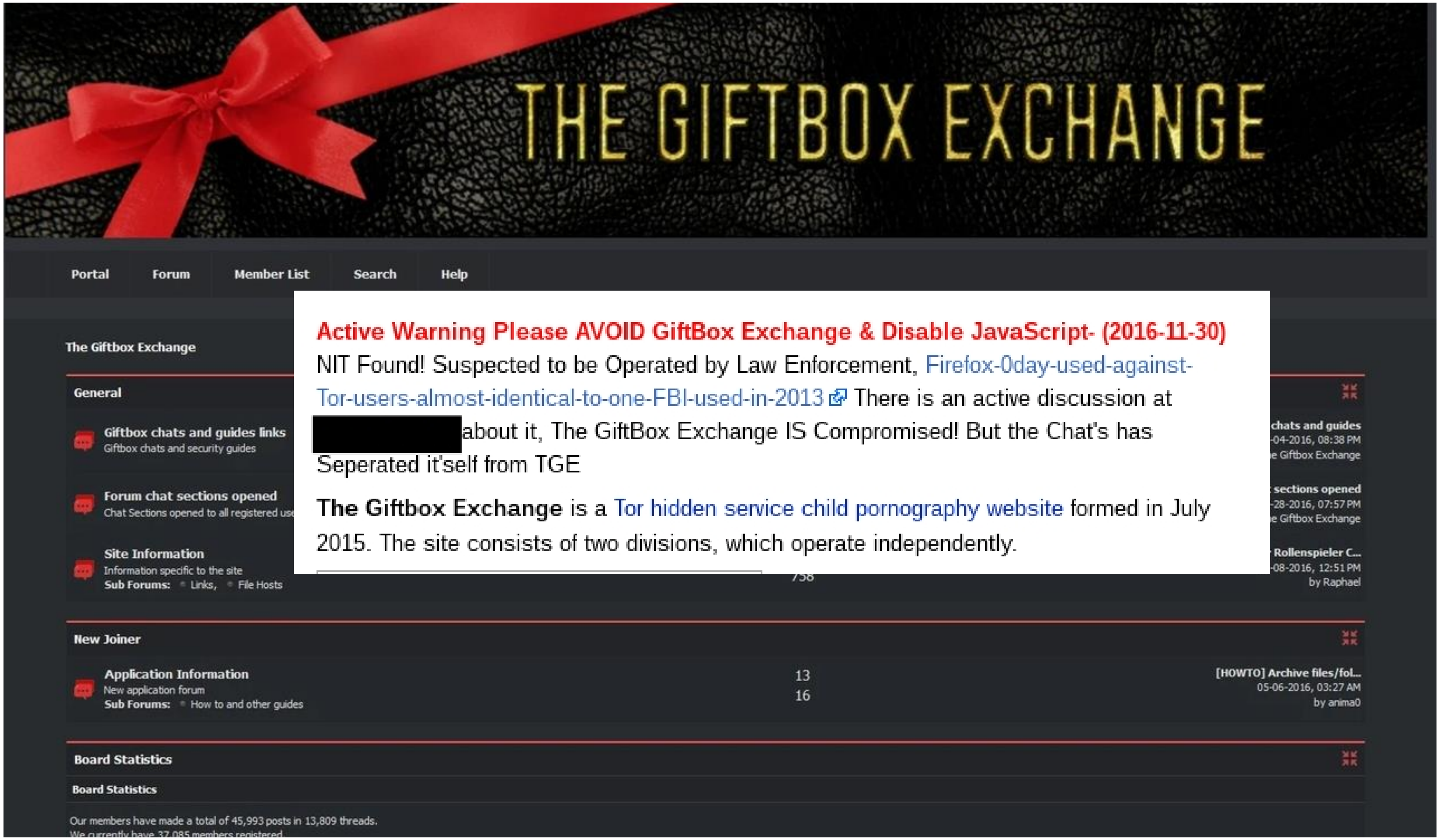
2023 trends

- There has been a steep increase in online grooming activities on social media and online gaming platforms.

- The production of self generated material is a key threat. This material is displaying increasingly younger children.

- The Dark Web remains an important platform for the exchange of child sexual abuse material (CSAM).

Operation ARTEMIS (The Giftbox Exchange / Elysium) – a combined approach



THE GIFTBOX EXCHANGE

Active Warning Please AVOID GiftBox Exchange & Disable JavaScript- (2016-11-30)
NIT Found! Suspected to be Operated by Law Enforcement, Firefox-0day-used-against-Tor-users-almost-identical-to-one-FBI-used-in-2013 There is an active discussion at [redacted] about it, The GiftBox Exchange IS Compromised! But the Chat's has Seperated it'self from TGE

The Giftbox Exchange is a Tor hidden service child pornography website formed in July 2015. The site consists of two divisions, which operate independently.

The Giftbox Exchange

General

Giftbox chats and guides links
Giftbox chats and security guides

Forum chat sections opened
Chat Sections opened to all registered use

Site Information
Information specific to the site
Sub Forums: Links, File Hosts

758

chats and guides
-04-2016, 08:38 PM
e Giftbox Exchange

sections opened
-28-2016, 07:57 PM
e Giftbox Exchange

Rollenspieler C...
-08-2016, 12:51 PM
by Raphael

New Joiner

Application Information
New application forum
Sub Forums: How to and other guides

13
16

[HOWTO] Archive files/fol...
05-06-2016, 03:27 AM
by anima0

Board Statistics

Board Statistics

Our members have made a total of 45,993 posts in 13,809 threads.
We currently have 37,085 members registered.

“Those Who Live by Anonymity, Die by Anonymity”

“Criminals are attracted to the dark net and Bitcoin due to the perceived anonymity that these technologies provide. TOR browsers and other programs limit law enforcement’s ability to track IP traffic back to the target. Dark net marketplaces by their very nature are unfriendly to law enforcement. (…) The use of these anonymizing technologies gives criminals a sense of invulnerability.

And that is how we get them.

As any experienced investigator will attest, de-anonymizing criminals on the internet is as much a matter of psychology as technology.”

Matthew J. Cronin, Hunting in the Dark: A Prosecutor’s Guide to the Dark Net and Cryptocurrencies, 66 U.S. ATT’Y BULL. (July 2018), p. 65 et seq.

“Those Who Live by Anonymity, Die by Anonymity”

“Dark net operators rely heavily on the powerful shield of anonymity that the dark net and cryptocurrencies provide them. Use their greatest asset against them. Just as agents cannot immediately identify a dark net target, the dark net target cannot identify an agent. Cloaked in the same anonymous technology, a well-trained federal agent can infiltrate any dark net criminal community. Operating undercover on the dark net, agents are able to generate tremendous amounts of information about their targets, potentially becoming a target’s valued customer or even a “friend.” That is especially true when an undercover agent gains access to an account with significant criminal transaction history (and thus digital street cred) or, even better, has longstanding ties to the target.”

Matthew J. Cronin, Hunting in the Dark: A Prosecutor’s Guide to the Dark Net and Cryptocurrencies, 66 U.S. ATT’Y BULL. (July 2018), p. 65 et seq.

Operation ARTEMIS

- In May 2016, Australian LEA (Taskforce ARGOS) were being offered access to the account details of a European moderator of the CSAM darknet site “The Giftbox Exchange” by a third-party LEA.

- This European agency sought out Taskforce ARGOS due to the stricter regulations placed on controlled operations in its own jurisdiction.

- At the same time, another CSAM forum, “Child’s Play”, was founded.

- Officers monitoring the Giftbox Exchange suspected a connection with Child’s Play due to a range of similarities in messages posted by Giftbox Exchange moderator CuriousVendetta and Child’s Play founder WarHead.

Operation ARTEMIS

- **Both usernames could be traced to a Canadian man, Benjamin Faulkner, who was subsequently arrested along with Giftbox Exchange founder Patrick Falte in Montpelier, Virginia, on 1 October 2016.**

- **U.S. LEA was able to extract the passwords for Child's Play from Faulkner, which were then passed on to Taskforce ARGOS and allowed them to take over control over the CSAM site.**

The „ELYSIUM“-investigation

- At the beginning of 2017, the Australian police took over the account of the moderator of the website The Giftbox Exchange on the Darknet and came across a German who was already planning another CSAM site called “Elysium”.

- The Cybercrime Prosecution Centre of the State of Hesse (ZIT), a specialized unit of the General Public Prosecutor's Office in Frankfurt am Main took over the investigation.

- In June 2017, the site Elysium was shut down by the authorities. So far, 14 suspects and 29 victims have been identified and images have been found that pointed to perpetrators in Germany.

The „ELYSIUM“-investigation

- After locating the server of the Elysium platform, German law enforcement commenced electronic surveillance of the server and defendant one as well as undercover operations.

- The surveillance measures included uploading avatar images to confirm the server location as well as surveillance of messages sent.

- This helped identify defendants one and two.

- Additionally, in 2016 the German Bundeskriminalamt was sent abuse images of defendant three from which the image of a fingertip and, hence, the fingerprint of the abuser could be deduced thereby identifying defendant three.

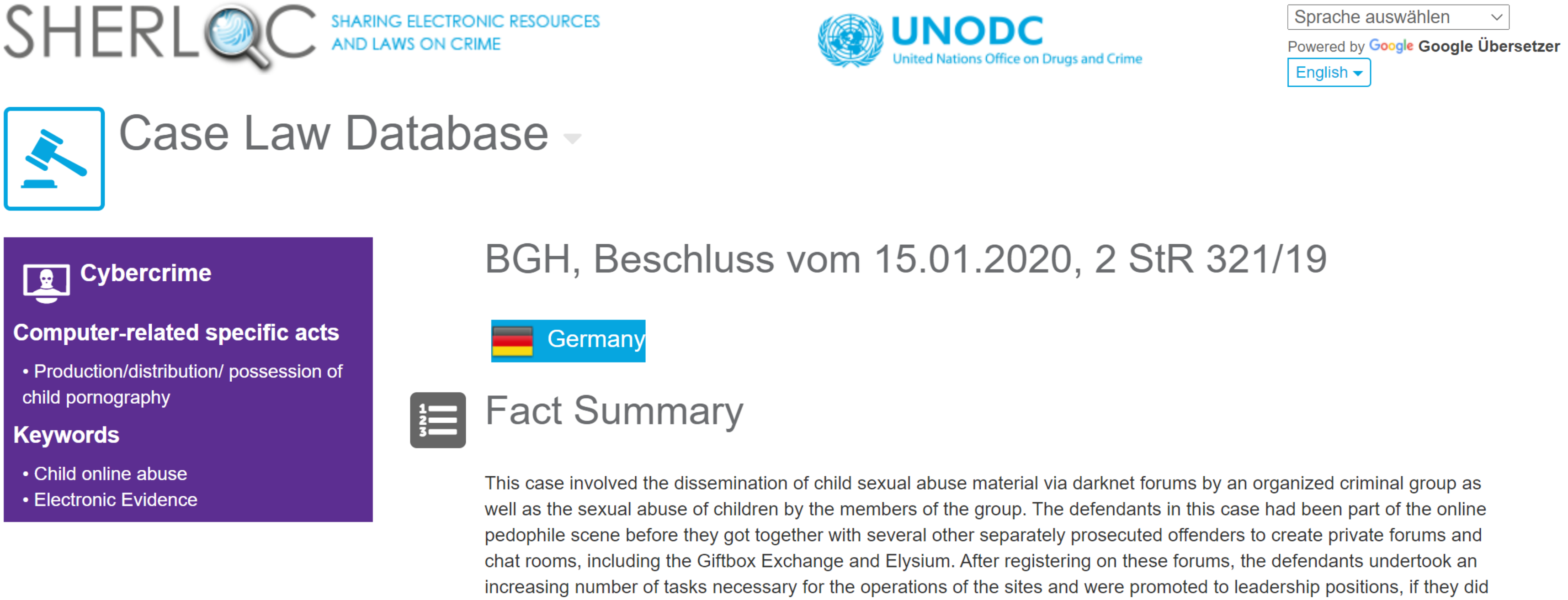
- By locating an in-memoriam site for the at-that-point-already-arrested defendant one, defendant four could be identified.

The „ELYSIUM“-investigation

- The well-documented case involved the dissemination of child sexual abuse material via darknet forums by an organized criminal group as well as the sexual abuse of children by the members of the group.

- The defendants in this case had been part of the online pedophile scene before they got together with several other separately prosecuted offenders to create private forums and chat rooms, including the Giftbox Exchange and Elysium.

The „ELYSIUM“-investigation



SHERLOC SHARING ELECTRONIC RESOURCES AND LAWS ON CRIME
UNODC United Nations Office on Drugs and Crime
Sprache auswählen
Powered by Google Google Übersetzer
English

Case Law Database

Cybercrime

Computer-related specific acts

- Production/distribution/ possession of child pornography

Keywords

- Child online abuse
- Electronic Evidence

BGH, Beschluss vom 15.01.2020, 2 StR 321/19

Germany

Fact Summary

This case involved the dissemination of child sexual abuse material via darknet forums by an organized criminal group as well as the sexual abuse of children by the members of the group. The defendants in this case had been part of the online pedophile scene before they got together with several other separately prosecuted offenders to create private forums and chat rooms, including the Giftbox Exchange and Elysium. After registering on these forums, the defendants undertook an increasing number of tasks necessary for the operations of the sites and were promoted to leadership positions, if they did

New German legislation: police is now allowed to distribute fictual (computer generated) CSAM for the purpose of arresting perpetrators

Section 184b (5) of the German Penal Code (StGB) was supplemented by p. 2:

„Paragraph 1, numbers 1 and 4, shall not apply to official acts within the scope of criminal investigation proceedings if the act relates to child pornographic content that does not reflect an actual event and was also not produced using a picture recording of a child or juvenile, and the clarification of the facts would otherwise be futile or substantially impeded“

New German legislation: police is now allowed to distribute fictual (computer generated) CSAM for the purpose of arresting perpetrators

The offence exception is flanked by Section 110d of the German Code of Criminal Procedure (StPO), which provides that operations require

- A court order (in case of imminent danger, the consent of the public prosecutor's office is sufficient, but that the measure must be terminated unless there is a court order is given within three working days);
- It must be stated in the application by the PPO that the acting police officers have been comprehensively prepared for the operation; and
- The court order must be given in writing and be limited in time.

Online Fraud

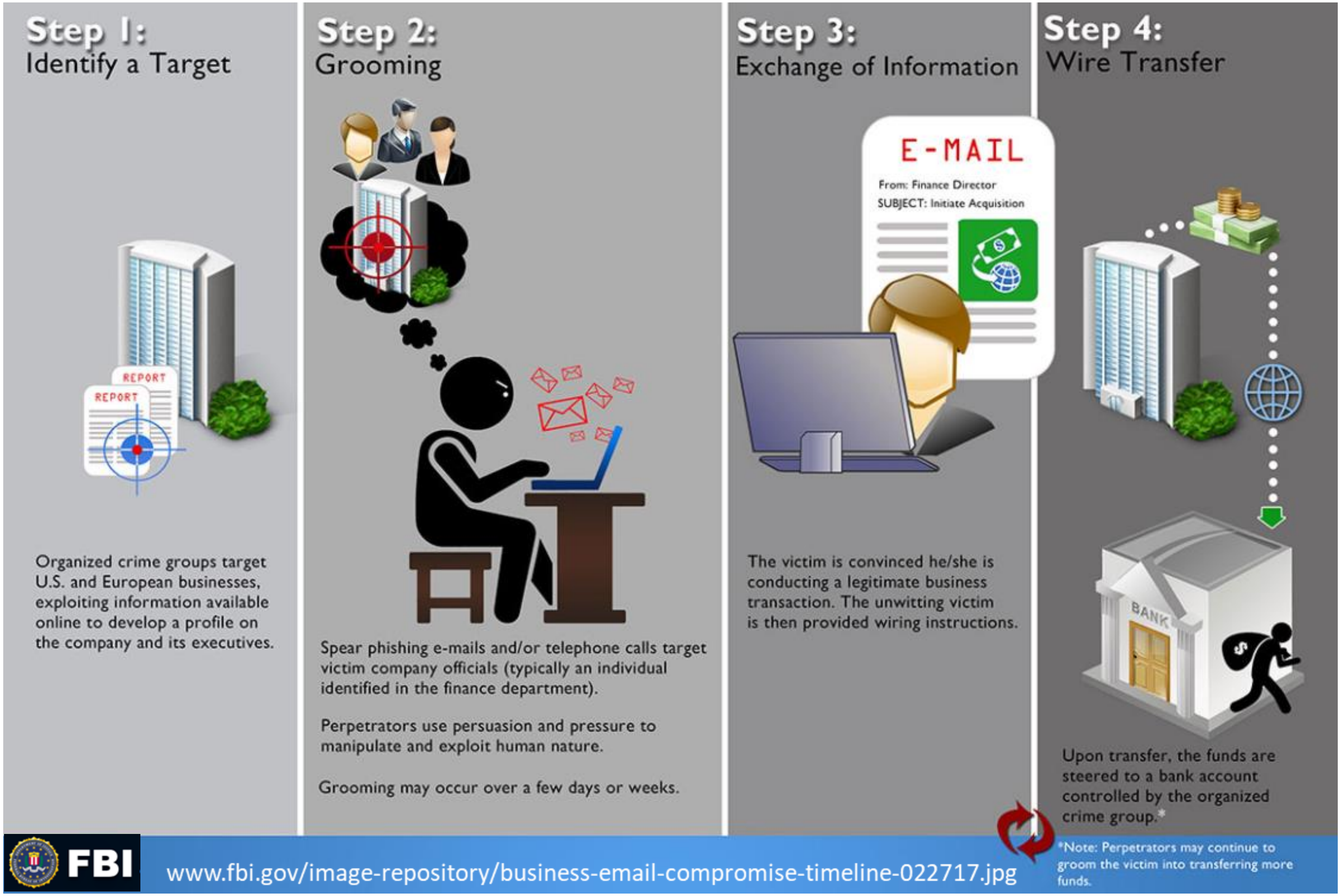
Online Fraud

- **COVID-19 has a significant impact on the European fraud landscape even after the pandemic.**
- **Phishing and social engineering remain the main vectors for payment fraud, increasing in both volume and sophistication.**
- **Investment fraud is thriving as citizens incur devastating losses, but business email compromise (BEC) and CEO fraud also remain key threats.**

Business Email Compromise (BEC)

- BEC is defined as a fraud targeting businesses that regularly perform wire transfer payments.

- The scam is carried out when perpetrators compromise e-mail accounts through social engineering or through computer intrusion techniques to fraudulently direct electronic fund transfers.



Step 1:
Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2:
Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3:
Exchange of Information

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4:
Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

www.fbi.gov/image-repository/business-email-compromise-timeline-022717.jpg

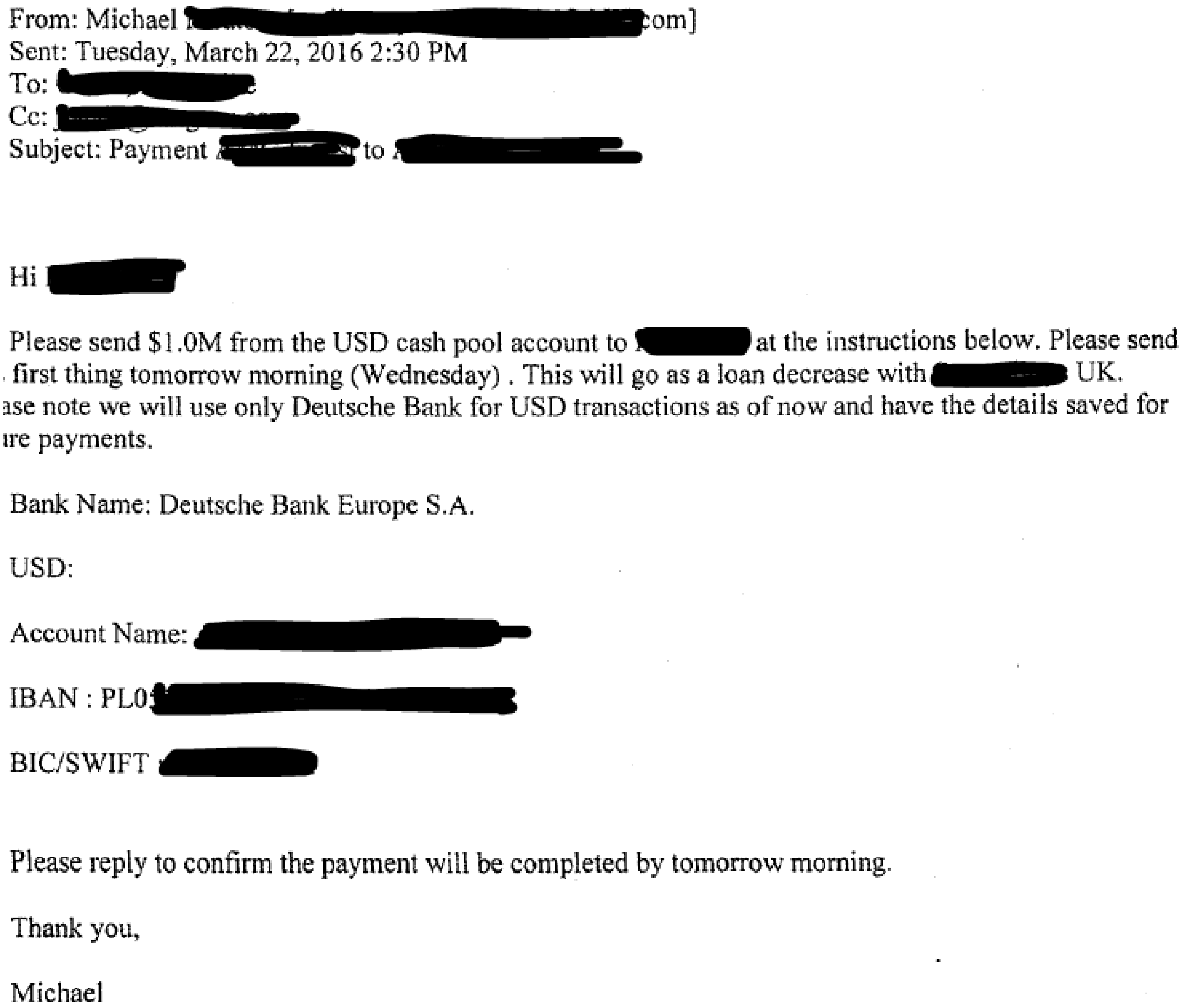
Social engineering attacks – CEO fraud

- A refined variant of spear phishing, CEO fraud, has evolved into a key threat as a growing number of businesses are targeted by organised groups of professional fraudsters.

- CEO fraud is a scam in which cybercriminals spoof company email accounts and impersonate executives to try and fool an employee in accounting or HR into executing unauthorized wire transfers, or sending out confidential tax information.

- Successful CEO frauds often result in significant losses for the targeted companies.

CEO-fraud: Example



From: Michael [redacted]com]
Sent: Tuesday, March 22, 2016 2:30 PM
To: [redacted]
Cc: [redacted]
Subject: Payment [redacted] to [redacted]

Hi [redacted]

Please send $1.0M from the USD cash pool account to [redacted] at the instructions below. Please send
first thing tomorrow morning (Wednesday) . This will go as a loan decrease with [redacted] UK.
ase note we will use only Deutsche Bank for USD transactions as of now and have the details saved for
ure payments.

Bank Name: Deutsche Bank Europe S.A.

USD:

Account Name: [redacted]

IBAN : PL0[redacted]

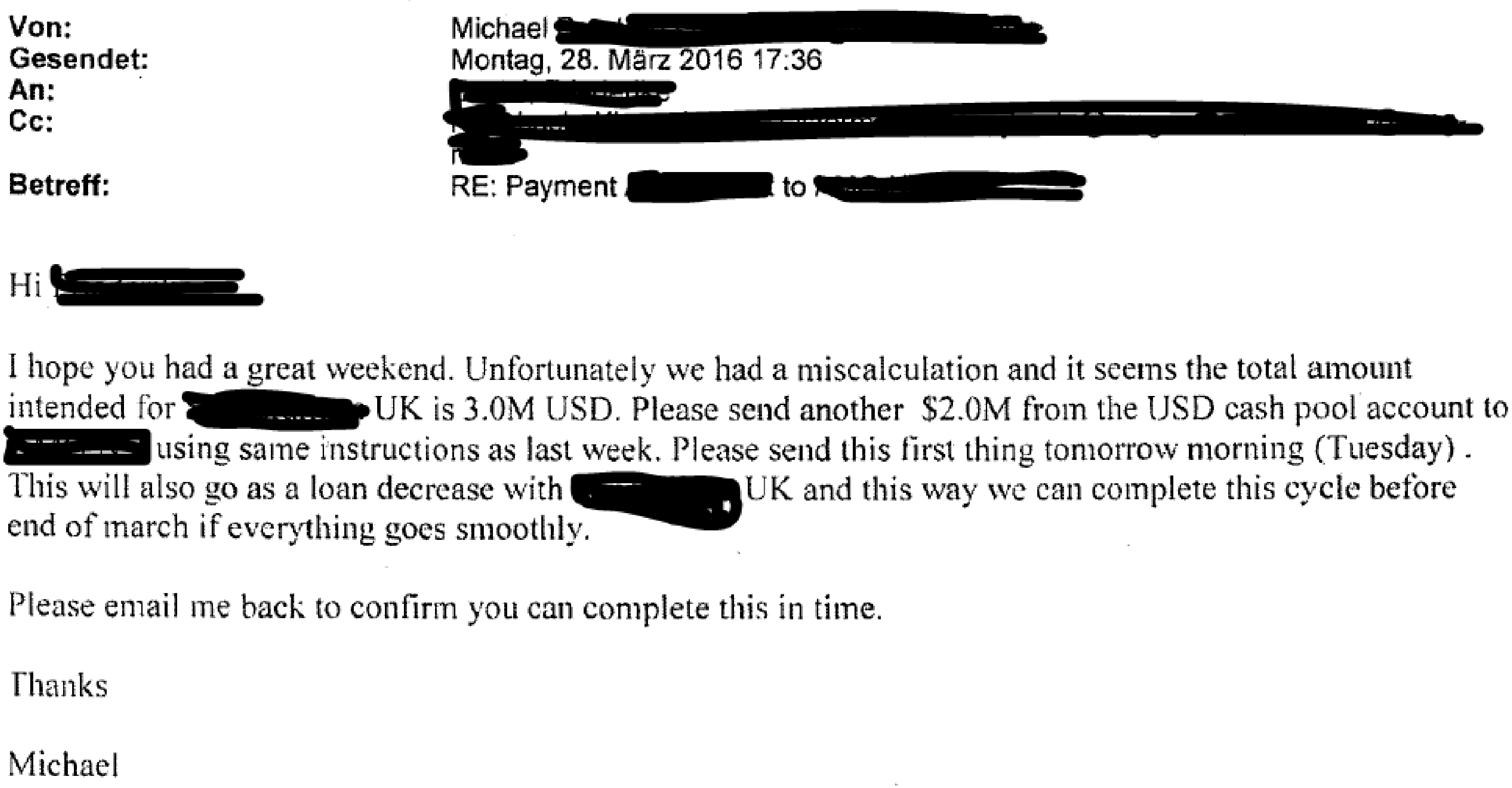
BIC/SWIFT [redacted]

Please reply to confirm the payment will be completed by tomorrow morning.

Thank you,

Michael

CEO-fraud: Example



Von: Michael [redacted]
Gesendet: Montag, 28. März 2016 17:36
An: [redacted]
Cc: [redacted]

Betreff: RE: Payment [redacted] to [redacted]

Hi [redacted]

I hope you had a great weekend. Unfortunately we had a miscalculation and it seems the total amount intended for [redacted] UK is 3.0M USD. Please send another $2.0M from the USD cash pool account to [redacted] using same instructions as last week. Please send this first thing tomorrow morning (Tuesday) . This will also go as a loan decrease with [redacted] UK and this way we can complete this cycle before end of march if everything goes smoothly.

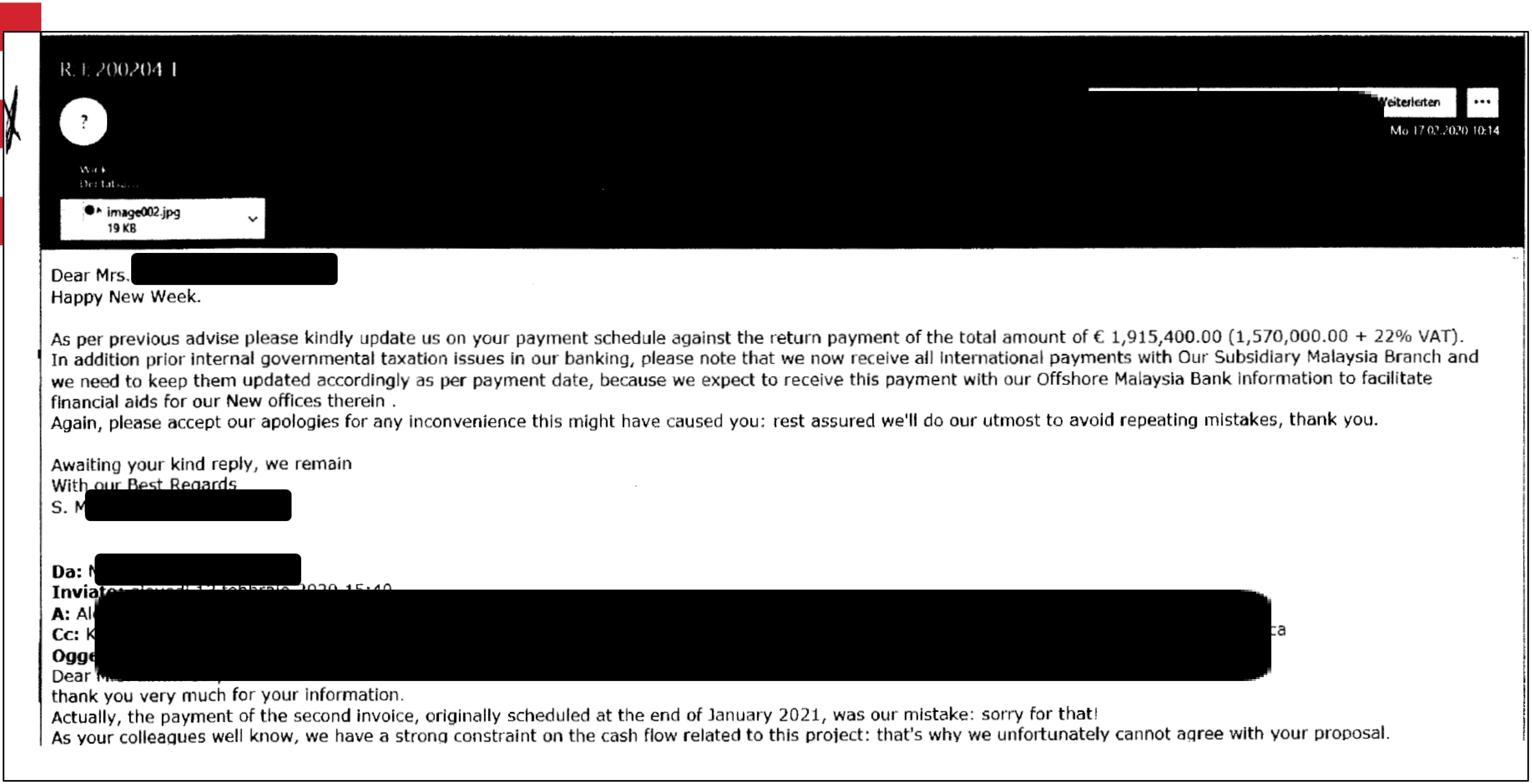
Please email me back to confirm you can complete this in time.

Thanks

Michael

HESSEN

CEO-fraud: Example



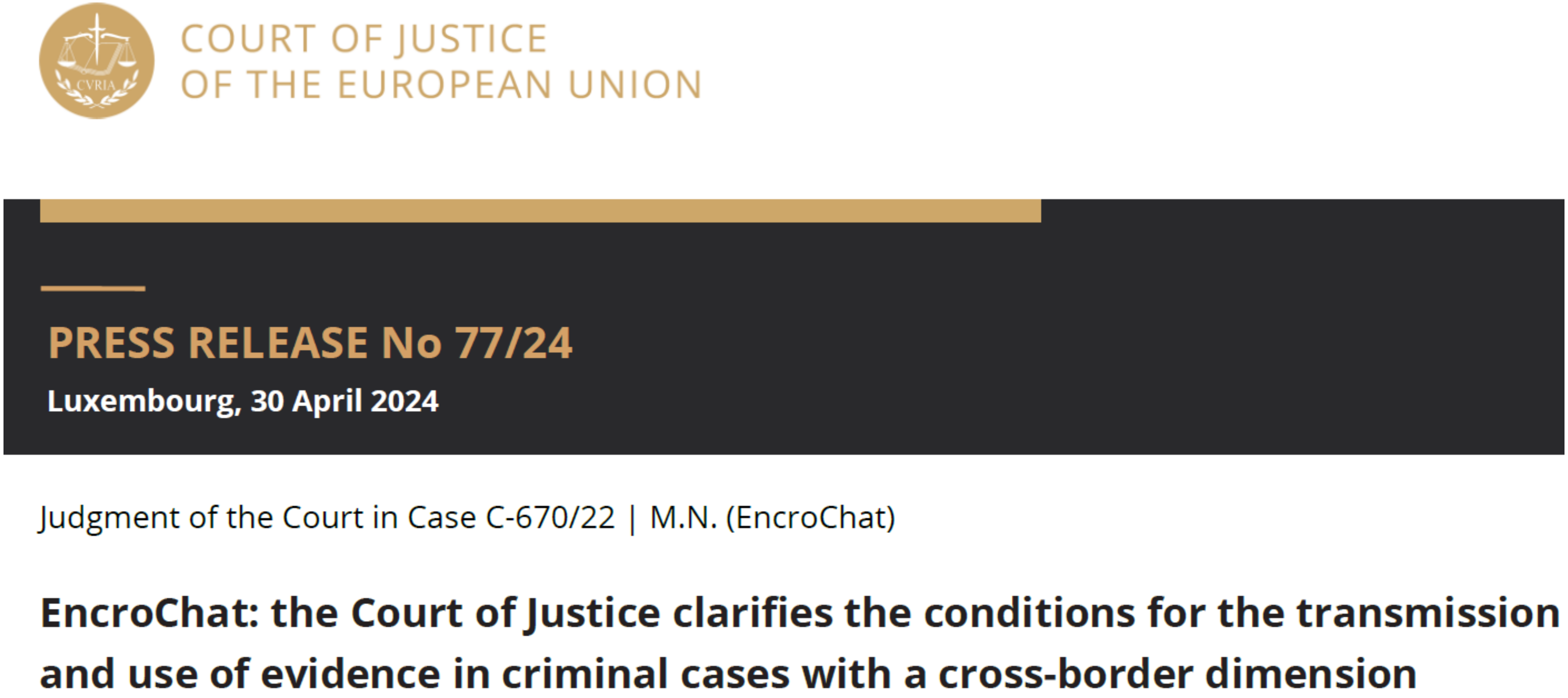
[redacted]

Dear Mrs. [redacted]
Happy New Week.

As per previous advise please kindly update us on your payment schedule against the return payment of the total amount of € 1,915,400.00 (1,570,000.00 + 22% VAT).
In addition prior internal governmental taxation issues in our banking, please note that we now receive all international payments with Our Subsidiary Malaysia Branch and we need to keep them updated accordingly as per payment date, because we expect to receive this payment with our Offshore Malaysia Bank information to facilitate financial aids for our New offices therein .
Again, please accept our apologies for any inconvenience this might have caused you: rest assured we'll do our utmost to avoid repeating mistakes, thank you.

Awaiting your kind reply, we remain
With our Best Regards
S. [redacted]

Da: [redacted]
Inviat [redacted]
A:
Cc:
Ogge
Dear
thank you very much for your information.
Actually, the payment of the second invoice, originally scheduled at the end of January 2021, was our mistake: sorry for that!
As your colleagues well know, we have a strong constraint on the cash flow related to this project: that's why we unfortunately cannot agree with your proposal.



COURT OF JUSTICE
OF THE EUROPEAN UNION

PRESS RELEASE No 77/24

Luxembourg, 30 April 2024

Judgment of the Court in Case C-670/22 | M.N. (EncroChat)

EncroChat: the Court of Justice clarifies the conditions for the transmission and use of evidence in criminal cases with a cross-border dimension

The Encrochat investigation

- "EncroChat" was a provider of cell phones on which an app was installed that allowed EncroChat users to send encrypted messages to each other.
- Due to the specifics of the system, the distribution channels, and the high cost of such a device, EncroChat phones were and are believed to be used almost exclusively for conducting criminal business.
- Encro devices could be purchased together with a user license for six months at a price of approximately EUR 1,600.
- There were no persons who presented themselves to the outside world as responsible for EncroChat, nor was there an official company headquarters.

How EncroChat worked

- Customers bought subscriptions and were given a handset.
- They were identified to the system by a nickname, not their real name
- All communications between handsets were routed/mediated through a server
- At each use the server authenticated the handset and allowed contacts with other authenticated handsets
- Server had the ability to update handsets with new apps and to switch off handsets
- Communications were end-to-end encrypted

The Encrochat investigation

How EncroChat worked

- The French police were able, with the assistance of Dutch experts and the authorisation of a French court, to infiltrate the encrypted telecommunications service EncroChat.
- The service was being used worldwide on encrypted mobile phones for the purpose of illegal drug trafficking.
- The German Federal Criminal Police Office was able, via a Europol server, to retrieve the intercepted data relating to EncroChat users in Germany.
- Acting on the EIOs issued by the German public prosecutor’s office, the French court authorised the transmission of those data and their use in criminal proceedings in Germany.

Arguments against admissibility of the Enco data

1. National courts cannot rely on lawful action by the French authorities in view of the unknown monitoring technology and the associated control deficit of the court.

2. The EIO issued subsequently violates Article 6 (1) (b) of the Directive because the transmission and use of the data could not have been ordered in a comparable domestic case because there was no qualified suspicion against the users of the Encro devices.

3. French authorities violated fundamental standards in the sense of ordre public because they had specifically searched for incidental findings, also abroad.

4. French authorities had not complied with their duty to notify under Article 31 of the EIO Directive.

Judgment of the Court in Case C-670/22 | M.N.

- **The German Federal Court (BGH) has already ruled that the Encrochat evidence is admissible (BGH, Beschluss vom 8.2.2022 – 6 StR 639/21)**

- **One chamber of the Regional Court (LG) of Berlin, before which criminal proceedings were brought, disagrees and still queries the lawfulness of those EIOs.**

- **It therefore submitted to the Court of Justice a series of questions for a preliminary ruling on the Directive regarding the European Investigation Order in criminal matters (EIO)**

- **The referred questions were answered in a manner that should not fundamentally change the jurisprudence**

Judgment of the Court in Case C-670/22 | M.N.

- An EIO for the transmission of evidence already in the possession of the competent authorities of the executing State (in this case, France) does not necessarily need to be issued by a judge. It may be issued by a public prosecutor if he or she is competent, in a purely domestic case, to order the transmission of evidence that has already been gathered.

- The issuing of such an EIO does not need to satisfy the same substantive conditions as those that apply to the gathering of evidence.

- In particular, it is not required that there be a suspicion of a serious criminal offense against each individual user at the time of issuance of the EIO

- However, a court before which an action against that EIO is brought must be able to review compliance with the fundamental rights of the persons concerned.

Judgment of the Court in Case C-670/22 | M.N.

- A measure entailing the infiltration of terminal devices for the purpose of gathering traffic, location and communication data of an internet-based communication service must be notified to the Member State in which the subject of that measure is located (in this case, Germany). The competent authority of that Member State then has the right to indicate that that interception of telecommunications may not be carried out or must be terminated.

- Those rights and obligations are intended not only to guarantee respect for the sovereignty of the notified Member State but also to protect the rights of the persons concerned.

- National criminal courts are required to disregard evidence, in the context of criminal proceedings against a person suspected of having committed criminal offences, when the person concerned is not in a position to comment on that evidence and the said evidence is likely to have a preponderant influence on the findings of fact.

•

Judgment of the Court in Case C-670/22 | M.N.

- This finding leaves room for interpretation, but it is more likely that this will not have effects on the EncroChat cases (CJEU paras. 126 ff.).

- Each court dealing with the matter independently reviews the admissibility of the obtained EncroChat data, also considering the Fair Trials principle (cf. Art. 47 f. of the EU Charter of Fundamental Rights).

- The accused/defendant can of course respond at any stage, etc.

- However, it is explicitly solely a matter of national law to determine prohibitions on the use of evidence (CJEU para. 128).

Judgment of the Court in Case C-670/22 | M.N.

- Whether this constitutes a contradiction or the BGH simply differentiated more precisely should likely have no practical consequences.

- Although a notification under Art. 31 EIO Directive this does not lead to inadmissibility.

- For the BGH has extensively stated that in the event that an individual protection character of the norm exists, the balancing doctrine would have to be applied, according to which the violation in the present case would not outweigh the state interest in the prosecution of serious criminal offenses.

- This consideration would then be transferable to other proceedings/cases in doubt.

Judgment of the Court in Case C-670/22 | M.N.

- The LG Berlin had also expressed concerns about the proportionality of the EIO, arguing that the integrity of the EncroChat data could not be verified, as the technical foundations of the surveillance measure and the data transfer to the Europol server were not disclosed by the French authorities, citing military secrecy.

- The LG therefore also wanted to know whether in the case of a European Investigation Order that is unlawful under Union law, a prohibition on the use of evidence directly follows from the Union law principles of effectiveness or equivalence.

- The CJEU explicitly stated that the issuance of a European Investigation Order is not precluded if the integrity of the data obtained through the surveillance measure cannot be verified due to the confidentiality of the technical foundations that enabled this measure, provided the right to a fair trial in the subsequent criminal proceedings is ensured. (CJEU para. 90, 100)

Judgment of the Court in Case C-670/22 | M.N.

- In reference to its consistent jurisprudence, the CJEU reaffirmed the general principle that a fair trial is no longer given when a party is unable to appropriately respond to evidence (CJEU paras. 105, 130).

- The term "appropriately" goes back to the CJEU's judgment in the case "Steffensen" and concerned the practical impossibility of obtaining a counter-expertise to a food law analysis result (CJEU EuZW 2003, 666 para. 76 ff.).

- According to CJEU jurisprudence, the requirements for a fair trial (Article 6 I ECHR) are met when the parties involved have a genuine opportunity to effectively respond to the evidence (CJEU EuZW 2003, 666 para. 77 f.).

- Clearly, the CJEU did not assume that the secrecy of the technical foundations of the surveillance measure and the data transfer to the Europol server alone already constitutes a violation of the principle of a fair trial.

Judgment of the Court in Case C-670/22 | M.N.

- **No indications of circumventing national provisions (no "Forum Shopping")**

- **It has been frequently claimed that the acquisition of the EncroChat data was carried out by circumventing national provisions in the form of so-called "forum shopping." The CJEU expressly contradicted this:**

“Admittedly, Article 6(1)(b) of Directive 2014/41 seeks to ensure that the rules and guarantees provided for by the national law of the issuing State are not circumvented. However, in the present case, it does not appear that that gathering of evidence and the transmission, by means of an EIO, of the evidence thus gathered would have had the aim or effect of such circumvention, which it is for the referring court to ascertain.”

Judgment of the Court in Case C-670/22 | M.N.

1. ~~Na[illegible]nal courts cannot rely on lawful action by the F[illegible]nch a[illegible]s in view of the unknown monitoring t[illegible]y and [illegible]ated control deficit of the c[illegible]~~

2. ~~The EIO issu[illegible]uently vi[illegible]cle 6 (1) (b) of the Directive beca[illegible] and use of the data could not have been [illegible] comparable domestic case because ther[illegible]uspicion against the users of the E[illegible]s.~~

3. ~~Fren[illegible]es violated fundamenta[illegible] in the s[illegible] ordre public because they had [illegible]lly se[illegible]ed for incidental findings, also abroad.~~

4. French authorities had not complied with their duty to notify under Article 31 of the EIO Directive.

Thank you for your attention!

Questions? Remarks?

The collection of evidence located abroad and the challenges of transborder access to data

Sapfo Katsanaki
Public Prosecutor
SNE to EPPO*
LLM IT Law (London)
LLM Penal Sciences (Athens)

Thessaloniki, 16-17 February 2023

*The views and opinions expressed in this presentation are those of the speaker and do not necessarily reflect the views or positions of the EPPO.

Co-funded by
the European Union

Transborder access to data

Cross- border search

- ❖ unilaterally access
- ❖ computer data stored in another jurisdiction
- ❖ without seeking MLA

(Para.293 Explanatory Report to the Budapest Convention)

Directly contacting a foreign provider

- ❖ Through a voluntary request
- ❖ Through an order with which the provides has to comply

Issues raised by transborder access

- Jurisdiction to enforce (including jurisdiction to investigate by LEAs) is territorial
- Lotus case: "…the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State."

❖ Would it constitute a breach of international law/breach of sovereignty?

❖ Would it make any difference if remote investigations were limited to accessing the data/ not copying or seizing ?

❖ What if the location of the data is unknown?

Examples of transborder access under national legislation

The Belgian provisions

- under conditions, a computer search may be extended to an informatics system or part thereof located in a place other than the place where the search takes place (Art. 88ter Code of Criminal Procedure)
- when it appears that the data found is not located on the territory of Belgium, the data is only copied (para.3 Art.88 CCP)

The Portuguese provisions

- when, during a of search, there are reasons to believe that the information sought is stored in another computer system or in a different part of the previous system, but that these data are lawfully accessible from the initial system, the search can be extended by authorisation of the competent authority(Art.15 para.5 Law Law no. 109/2009 on Cybercrime).
- No geographical or jurisdictional limits are established under this article
- Transposition of article 19.2 of the Budapest Convention, which however creates the obligation for Parties to extend the search to data stored ***in the territory*** of that Party

The provisions under the Greek Legislation

Art.265 para.1c Code of Criminal Procudure provides the seizure of a remote computer system or part of it and computer data stored therein or in a remote computer-data storage medium, interconnected to the computer system to which the person conducting the investigation has physical access.

BUT

Data stored in the cloud is not considered to be stored on a remote computer system or on a remote computer-data storage medium interconnected to the computer system to which the investigator has physical access (art. 265 par.1c).

Judicial Council of Athens 613/2016: The procedure of lawful interception, should be followed to lawfully seize data stored in the cloud, connected to the accused's mobile seized (not an unanimous one).

limitations are established with regard to cloud but only with regard to preconditions of accessing data in the Cloud.

HOWEVER

the provision, according to the Explanatory Memorandum transposes the relevant provision of article 19.2 of the Budapest Convention, which creates the obligation to extend the search to data stored ***in the territory*** of that Party

Collection of evidence located abroad through MLA
EU instruments

EIO Directive (2014/41 EU)

Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000

EIO Directive (2014/41 EU)
Provisions for access to data

identification of persons holding a subscription of a specified phone number or IP address.

(Art.10 para 2(e)

Interception of telecommunications with technical assistance - Filling in Annex A Section H7 (Art. 30)

Interception of telecommunications without technical assistance - Only **notification** of ANNEX C (Art. 31)

Investigative measures implying the gathering of evidence in real time, continuously and over a certain period of time (Art.28)

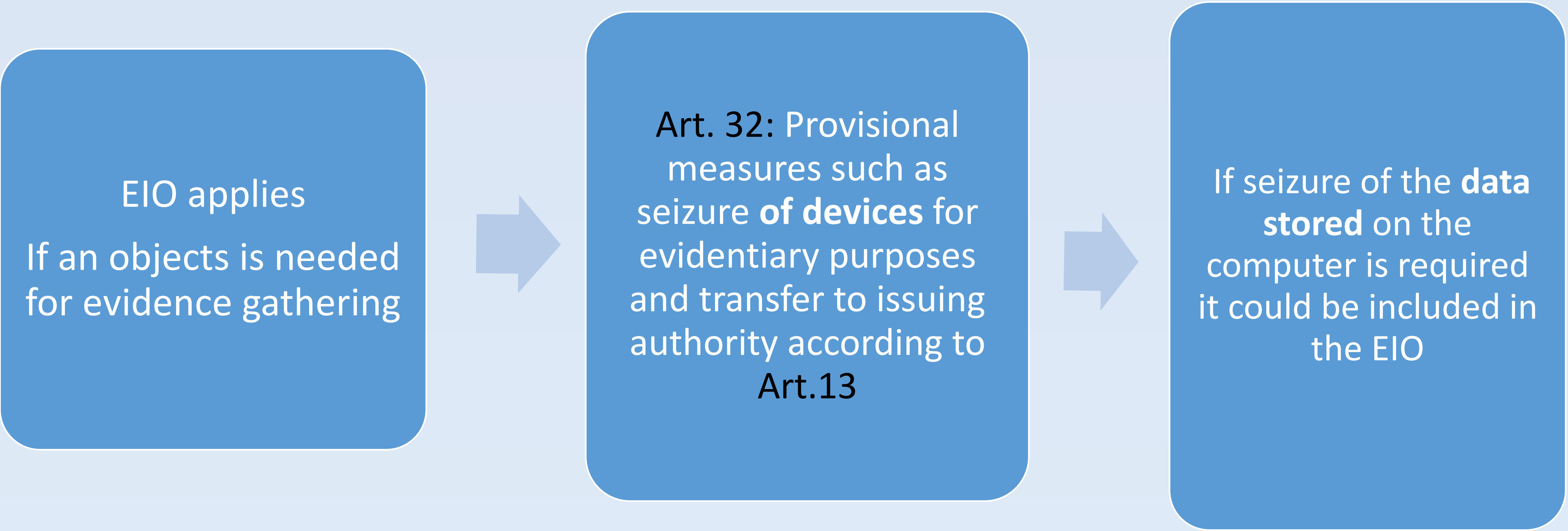
Video surveillance and tracking or tracing with the use of technical devices (GPS**) where only movement** is recorded could be ordered under this Article

Remote search of computer data under the EIO Directive

- Art. 30 and 31 could apply by analogy depending on whether the the technical assistance of the State where the computer is located, is needed
- principle of proportionality should be considered

- Art 29 applies to on-line covert investigations WHEN technical assistance is required from the other state
- If no technical assistance is required from the other state Art.31 applies and no special agreement between the issuing and the executing State is needed.

Seizure under the EIO



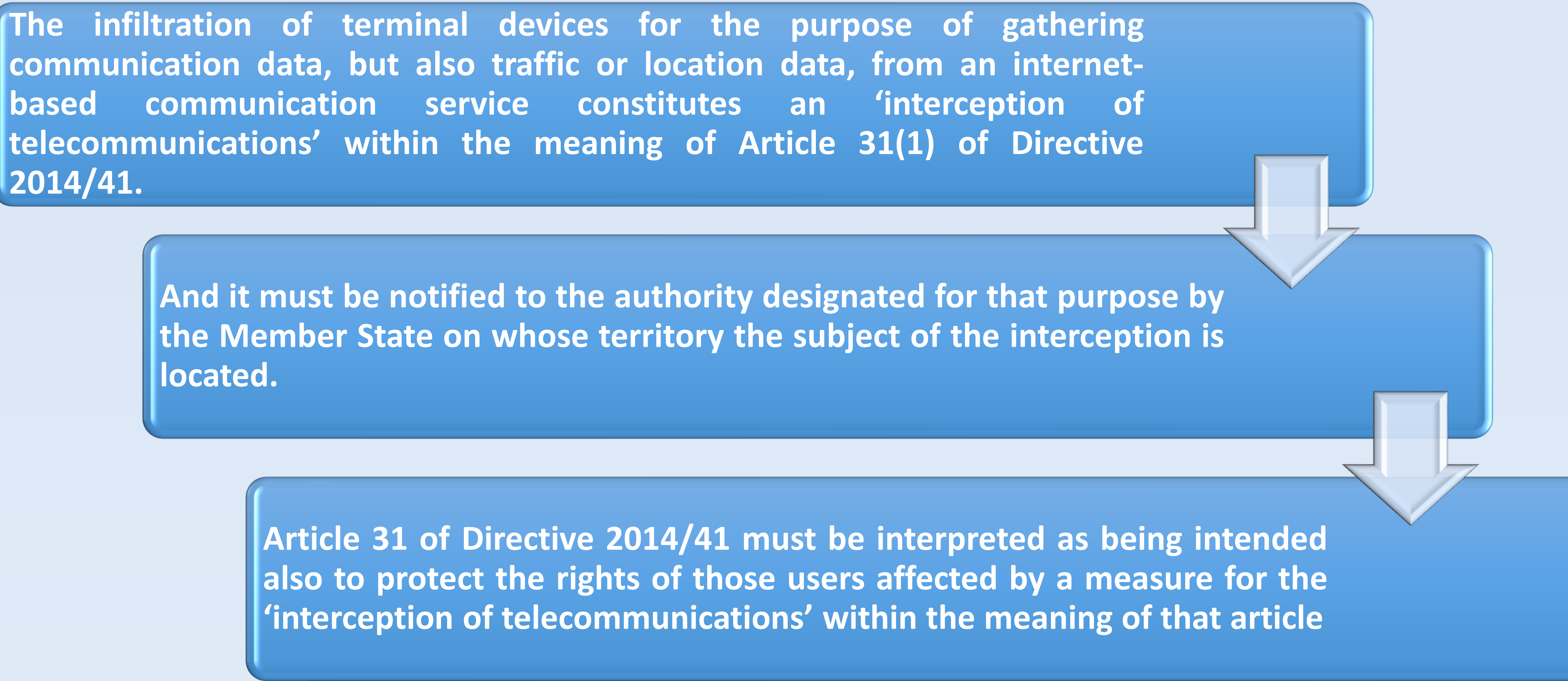
EIO applies

If an objects is needed for evidence gathering

Art. 32: Provisional measures such as seizure **of devices** for evidentiary purposes and transfer to issuing authority according to Art.13

If seizure of the **data stored** on the computer is required it could be included in the EIO

Judgment of the Court in Case C-670/22 (EncroChat)



The infiltration of terminal devices for the purpose of gathering communication data, but also traffic or location data, from an internet-based communication service constitutes an ‘interception of telecommunications’ within the meaning of Article 31(1) of Directive 2014/41.

And it must be notified to the authority designated for that purpose by the Member State on whose territory the subject of the interception is located.

Article 31 of Directive 2014/41 must be interpreted as being intended also to protect the rights of those users affected by a measure for the ‘interception of telecommunications’ within the meaning of that article

2. Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000

Replaced by EIO Directive
BUT
still applies to Ireland and Denmark

- Art.18: Request for interception of telecommunications (Covers situations in which a MS is requested by another member state to order an interception operation from its own territory)
- Art. 19 :Interceptions of telecommunications on national territory by the use of service providers (permits the installation of remote control equipment)
- Art.20: Interception of telecommunications without the technical assistance of another Member State (in a spill-over scenario- prior notification is required)

Collection of evidence located abroad through MLA
Council of Europe instruments

European Convention on mutual assistance in criminal matters 1959

Convention on Cybercrime

European Convention on mutual assistance in criminal matters 1959

- Art.3 on letters Rogatory for the purpose of procuring evidence or transmitting articles to be produced in evidence, records or documents and Art.15 on their communication.

- RECOMMENDATION No. R (85) 10 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES CONCERNING THE PRACTICAL APPLICATION OF THE EUROPEAN CONVENTION ON MUTUAL ASSISTANCE IN CRIMINAL MATTERS IN RESPECT OF LETTERS ROGATORY FOR THE INTERCEPTION OF TELECOMMUNICATION

➡ Grounds for refusal and content of request (under 1 and 2)

The Convention on Cybercrime

Mutual legal assistance provisions on collection of data

Art.25 para.2: Each Party shall a also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

- Art. 31 Access of Stored computer data (includes seizure/copying/removing as provided under Art.19)
- Art.33 Real Time Collection of traffic data- at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case
- Art.34 Interception of content data

Unilateral access to data under the Cybercrime Convention

Article 32

Trans-border access to stored computer data with consent or where publicly available

Limitations : refers to stored computer data located in another party and when the location is known

a) publicly available (open source) stored computer data

- Access includes download/secure/take screenshots

b) With the lawful and voluntary consent of the person who has the lawful authority to disclose the data

- The account holder / the cloud service provider?

Article 18 on the productions order
A provision for a national measure but….

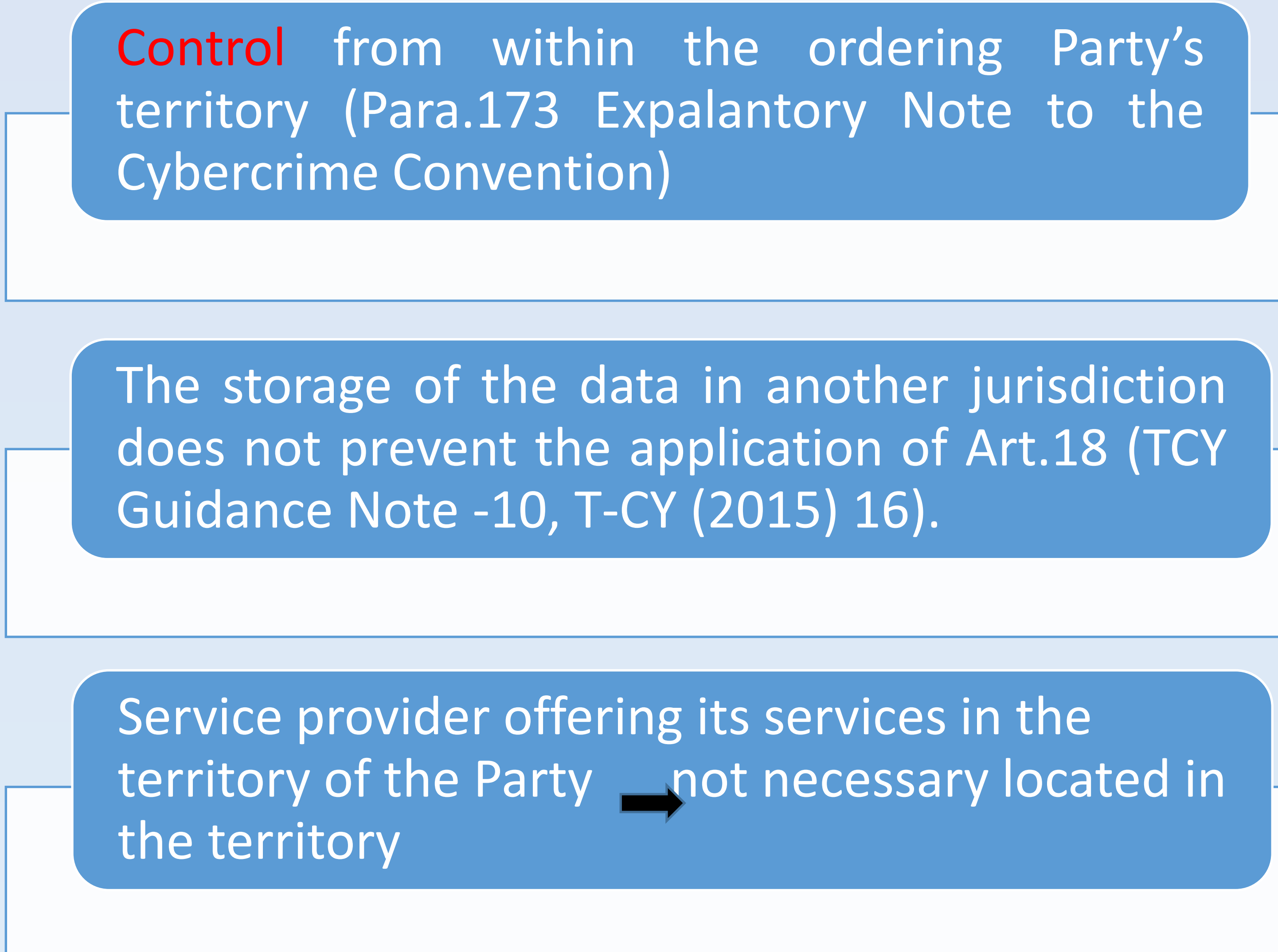
The relevant provision

Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a) A person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium

b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control

The interpretations



Control from within the ordering Party's territory (Para.173 Expalantory Note to the Cybercrime Convention)

The storage of the data in another jurisdiction does not prevent the application of Art.18 (TCY Guidance Note -10, T-CY (2015) 16).

Service provider offering its services in the territory of the Party → not necessary located in the territory

Direct Cooperation with Service Providers

The e-evidence package

Second Additional protocol to the Cybercrime Convention

Voluntary cooperation with SPs

Regulation 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings

Shall apply from 18 August 2026

EPOC and EPOC – PR

- ➢ issued or validated by a judicial authority in a Member State
- ➢ to a service provider offering services in the Union AND
- ➢ established in another MS or, if not established, represented by a legal representative in another MS

These instruments are used only for stored data in cross border situations and only when services are offered within the EU.

The new Instruments under the E- Evidence Regulation

European Production Order

For Subscriber data or data requested solely for identification

- issued by a judge, a court, an investigating judge or a public prosecutor or validated by them when issued by another competent authority
- FOR ALL OFFENCES and for the execution of custodial sentence or detention order of at least 4 months

For traffic or content data

- issued by a judge or Court or an investigating judge or validated by them when issued by another competent authority
- Only for the offences mentioned under Art.5 para.4 and under specific conditions for the execution of sentences (Point d of para.4)

European Preservation Order

For all data

issued by a judge, a court, an investigating judge or a public prosecutor or validated by them when issued by another competent authority

for any offence

for the execution of custodial sentence or detention order of at least 4 months

DIRECTIVE (EU) 2023/1544 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 proceeding

Applies only to SPs (as defined under art.2) offering services to the Union

SPs established in the Union shall designate designated establishments

SPs NOT establish in the Union shall appoint legal representatives

SPs established in MS not taking part in the instrument shall appoint legal representatives in MS taking part in the instruments

For the receipt of, compliance and enforcement of decisions and orders under

→ Regulation EU 2023/1546

→ Directive 2014/41EU

→ Convention on Mutual Assistance in Criminal Matters between Member States of the Union

Provisions of the Second Protocol Procedures on the direct co-operation with providers and entities in other Parties

Art.6 Request for domain name Registration Information

- Definition of competent authority under Art.3 para.2
- Issuance of **requests** → **non-binding** (para.77 of the Explanatory Report) → the entity is only asked to reason its refusal (para.5)

Article 7 – Disclosure of subscriber information

- Subscriber information (definition under Art.18 para.3 of the Budapest Convention) any information other than traffic data (Art. 1d of the Budapest Convention and para.30 of the Explanatory Report to the Budapest Convention). What about IP?
- Service provider in another Party's territory
- Issued by/under the supervision of Prosecutor/or under independent supervision only if so declared (Art.7 para.2b) and notification to the party only if so declared (Art.7 para.5a,e)
- Grounds for refusal (Art.7 para.5c)

Accessing data in the US

- Non- content data is provided by US Service Providers on a voluntary basis
- US is a party to the Budapest Convention
- Clarifying Lawful Overseas Use of Data Cloud Act (Cloud Act)
  - Creates a new mechanism for other countries to access the content of communications held by US service providers through executive agreements” with certain “qualified” foreign governments.
  - September 25, 2019 EC started negotiations with US aimed at concluding a transatlantic agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters.

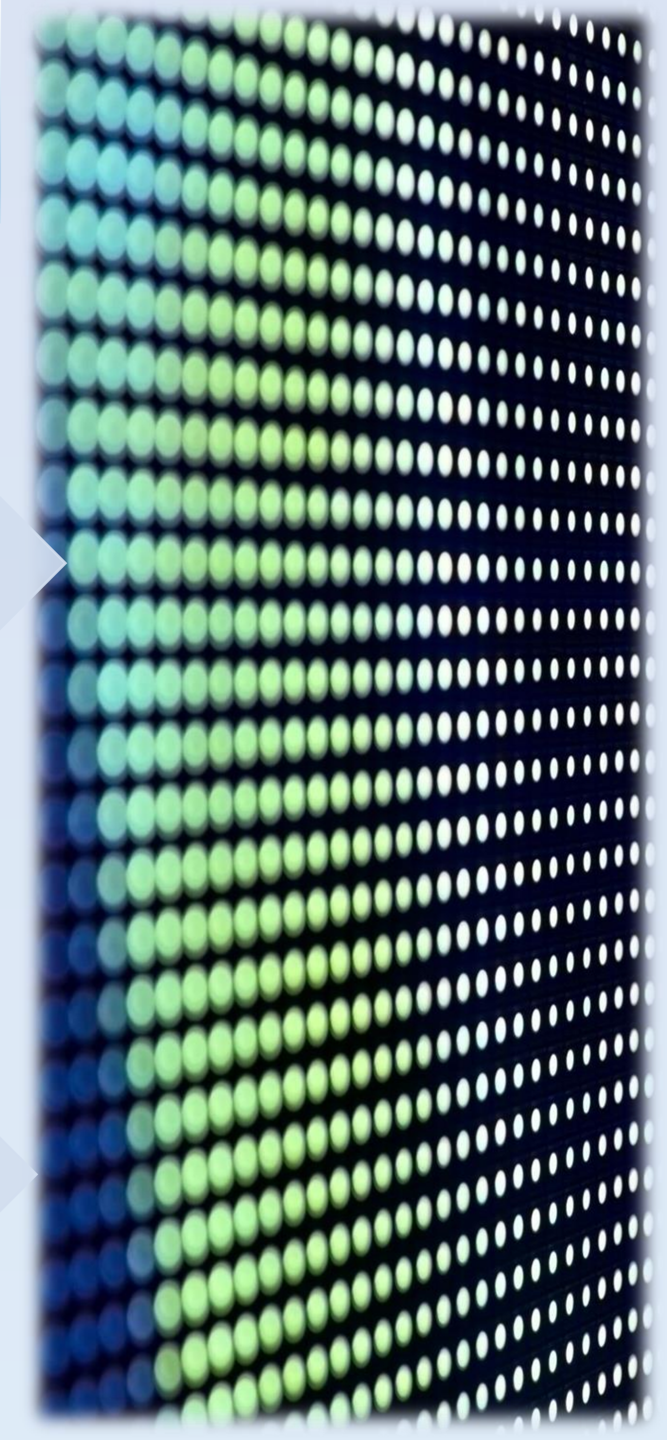
Challenges regarding access to data

Encryption

- Art.19 para.4 Budapest Convention Measures could include disclosing a password or other security measure
- In case of transborder access, assistace could be asked through MLA
- Mandatory key disclosure laws
- an obligation imposed to providers to decrypt communications weaken the encryption mechanism for all users and is accordingly not proportionate (PODCHASOV v. RUSSIA,13.02.2024)

Data authenticity/integrity

- Chain of custody
- No physical acquisition is possible/ special tools to conduct forensic acquisitions are needed.
- Challenges raised by Cloud computing technology /common forensic procedures cannot apply



What other options are there?

- Further regulation under the Budapest Convention- Suggestions by the TCY-Committee
  - Broaden the scope of Art.32b to allow for access to data located in non-Parties.
  - Transborder access without consent but with lawfully obtained credentials.
  - Transborder access without consent in good faith or in exigent or other circumstances.
  - Amending Art.19.2 to authorise an extension of a search to connected computer systems without the territorial limitation.
- The power of disposal as an alternative to the principle of territoriality*

* See the Discussion paper on Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? at [2079 Cloud Computing power disposal 31Aug10a (coe.int)]

Thank you for your attention

Questions ?

“Hunting in the Cloud” - Locating and extracting the evidence

Co-funded by
the European Union

I WAS HOPING FOR A SLIGHTLY MORE DETAILED EXPLANATION OF HOW CLOUD COMPUTING WORKS THAN – "IT'S MAGIC"!
IT
© D.Fletcher for CloudTweaks.com

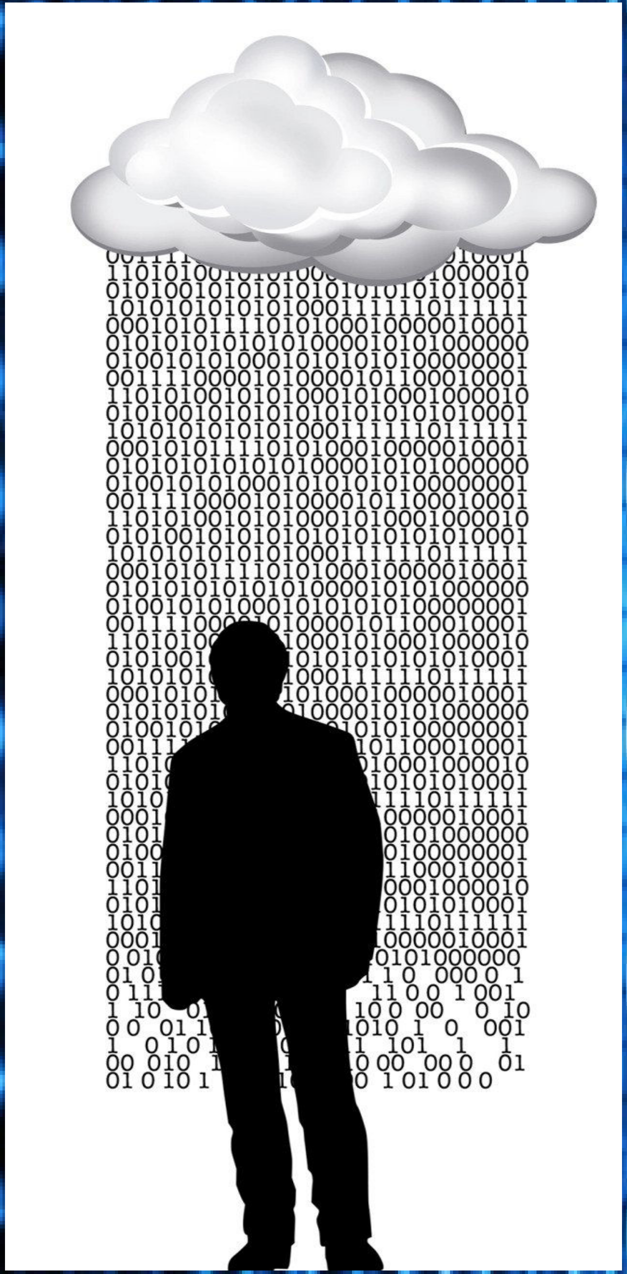
The Cloud as a "Fishnet of Hard Drives"

Interconnected Data Centers, scattered in different geographical places, from where the stored data is recalled on-demand, regardless of the end-user's whereabouts

Data Redundancy : Multiplication of data for safety and performance optimization reasons

[Safety: technical problem, catastrophic event]

[Performance Optimization: propagation delay]



The Main Characteristic of Cloud Storage Technology is the Loss Of Location :
No Geographically Fixed Reference Point

Main Legal Challenge : Data Territoriality and Applicable Law

A] “Possession” of Cloudly Stored Data

B] Extracting Digital Evidence In The Cloud

A] “Possession” of Cloudly Stored Data

- **Using somebody else’s device**
- **The Cloud Storage Provider cannot be liable for criminally interesting possession**
- **Simply Viewing ≠ Possessing ≠ Accessing (Art. 5 para. 2 Directive 2011/93/EU)**

B] Extracting Digital Evidence In The Cloud

- **U.S.A.**

  a) **Stored Communications Act (1986)**

  b) **Microsoft Ireland Case (2013-2016)**

  c) **CLOUD Act (2018)**

- **EU**

  a) **G8: Principles on Transborder Access to Stored Computer Data – Principles on Accessing Data Stored In A Foreign State (1997)**

  b) **(Budapest) Convention On Cybercrime (2001)**

  c) **European Investigation Order (2014)**

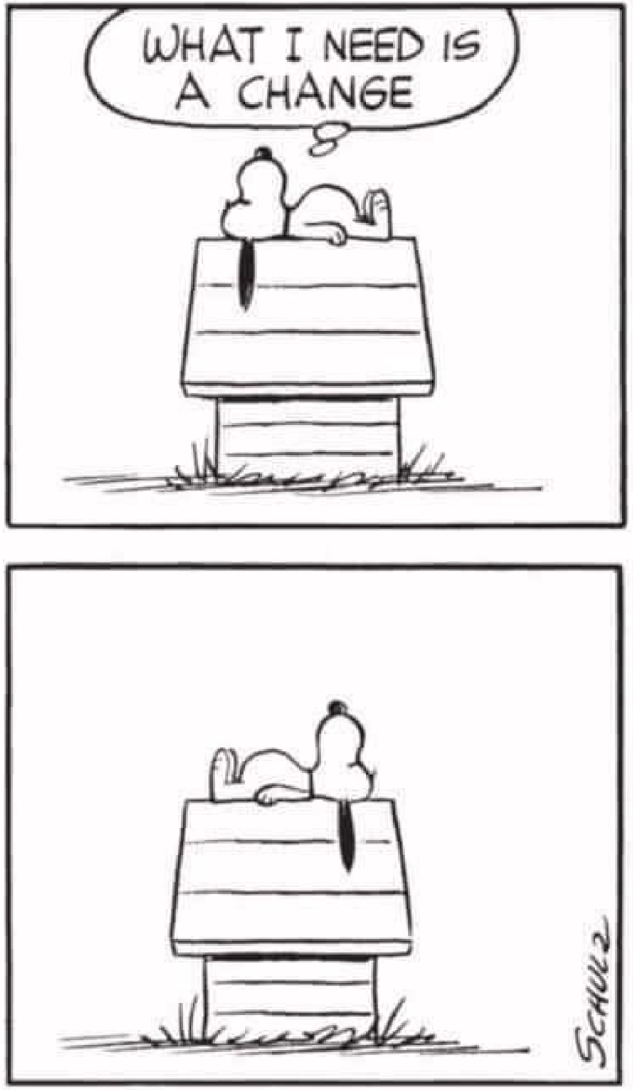
B] Extracting Digital Evidence In The Cloud (2)

- Cloud Storage Providers reveal only their own technical data and metadata to the LEA and are understandably reluctant to grant unconditional full access to the content of the files per se

- The not obligatory but simply goal-setting Directive 2014/41/EU/3-4-2014 is not enacted by national legislation in every State (Ireland)

- European Production and Preservation Orders for electronic evidence in criminal matters [Regulation (EU) 2023/1543] : Decentralized IT System for the secure digital communication and data exchange → in force from 18th August 2023 / it shall apply from 18th August 2026

Understanding of Technology Paves The Way to A Change Of The Legal Approach



Power of Disposal

The ability of a specific person to obtain sole or collaborative access and hold the right to alter, delete, suppress, render unusable or even exclude others from access and usage of certain electronic data

The exact physical location of digital evidence and the possible implications of legally defining the actual ownership of data become indifferent matters, while at the same time the specific technical features of “The Cloud” are taken into consideration.

Cyber =
Connected

Thank You For Your Attention !

Christos Karagiannis
Prosecutor, Court Of First Instance,
Greece
karagiannisxristos@yahoo.gr

INSIG2

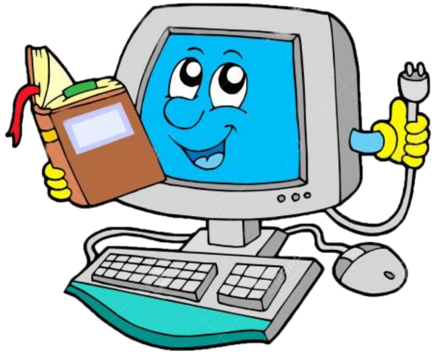
ERA Thessaloniki 2024

DIGITAL EVIDENCE COLLECTION: OPEN SOURCE INTELLIGENCE (OSINT)

Co-funded by
the European Union

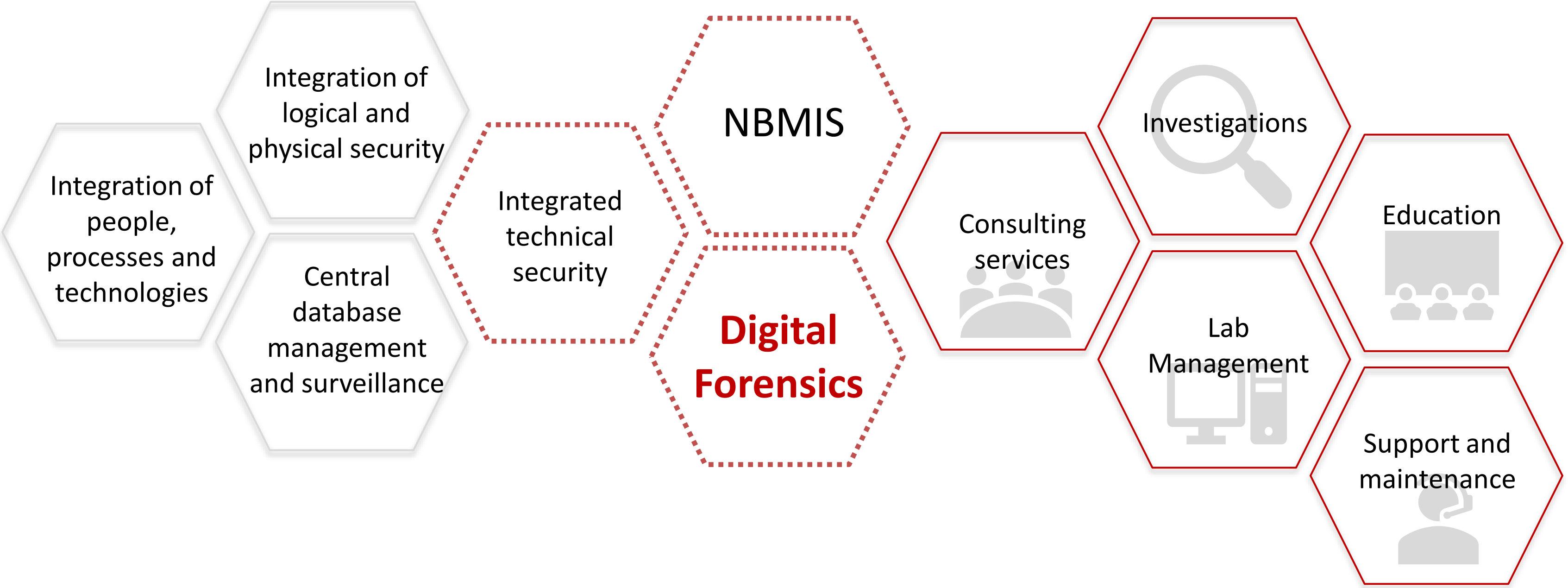
Dario Vrčković

- TVZ - Master of Engineering in Information Technology (M.Eng.IT)
- Digital Forensics Consultant in INsig2 Ltd.
- Windows Forensics, OSINT, Network Forensics…



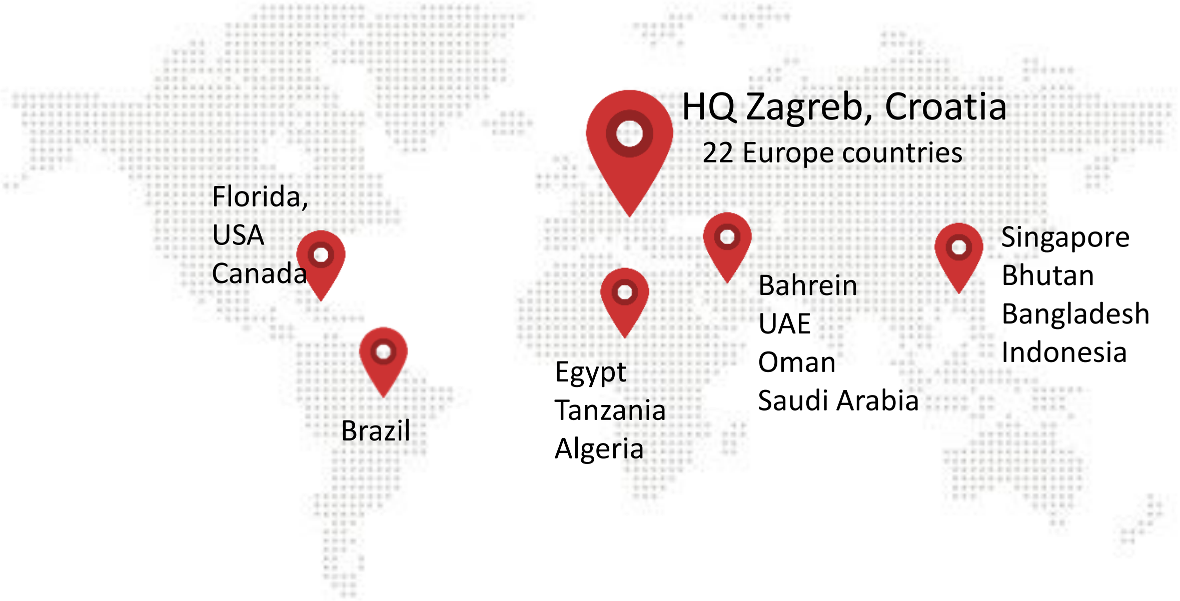
INsig2

- Three business units
- „One-stop-shop” in the field of Digital Forensics

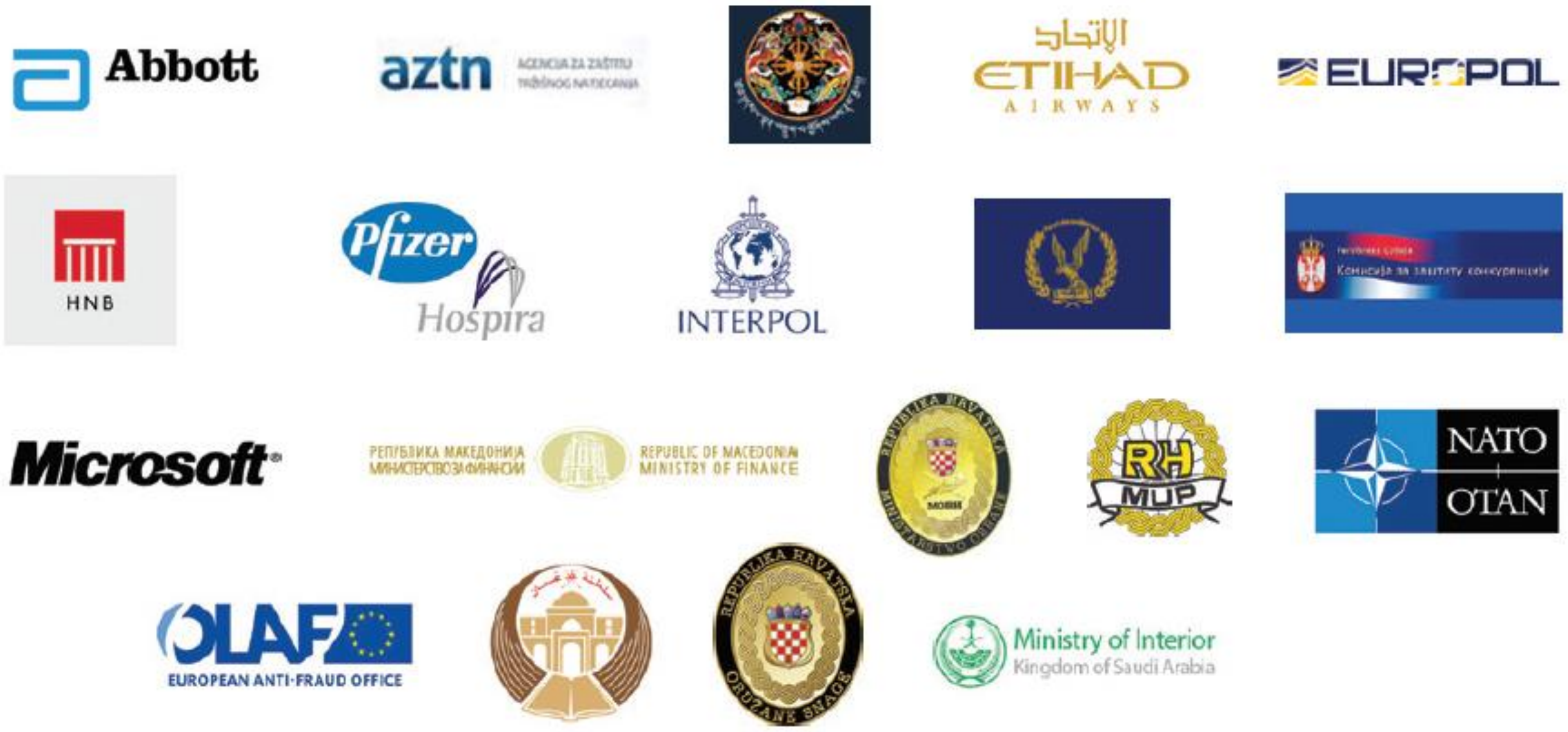

Integration of people, processes and technologies
Integration of logical and physical security
Central database management and surveillance
Integrated technical security
NBMIS
Digital Forensics
Consulting services
Investigations
Lab Management
Education
Support and maintenance

INsig2 Trainings

- Intensive training schedule has been in place since late 2011 and since then INsig2 has successfully completed over 500 trainings at 5 continents and trained over 3000 law enforcement professionals



Clients


Abbott
aztn AGENCIJA ZA ZAŠTITU TRŽIŠNOG NATJECANJA
الإتحاد
ETIHAD AIRWAYS
EUROPOL
HNB
Pfizer
Hospira
INTERPOL
Комисија за заштиту конкуренције
Microsoft
РЕПУБЛИКА МАКЕДОНИЈА МИНИСТЕРСТВО ЗА ФИНАНСИИ
REPUBLIC OF MACEDONIA MINISTRY OF FINANCE
REPUBLIKA HRVATSKA MINISTARSTVO OBRANE
RH MUP
NATO
OTAN
OLAF
EUROPEAN ANTI-FRAUD OFFICE
REPUBLIKA HRVATSKA ORUŽANE SNAGE
Ministry of Interior
Kingdom of Saudi Arabia

Ministry of Interior Macedonia, Montenegro, Republic of Bosnia and Hercegovina, Serbia, Slovenia

Partners

SUMURI
Forensics Simplified

AccessData

Belkasoft
forensics made easier

Digital Intelligence

mh
SERVICE GmbH

Guidance
SOFTWARE

nuix

Cellebrite

MAGNET
FORENSICS

TEELtechnologies
Canada

TEELtechnologies
Europe

IACIS
The International Association of Computer Investigative Specialists

OXYGEN
FORENSICS
Helping good people to make this world safer

AMPED
SOFTWARE

paraben
corporation

BlackBag
TECHNOLOGIES

TABLEAU

MSAB

ELCOMSOFT
PROACTIVE SOFTWARE

Introduction and the role of OSINT

OSINT Defined

Open-source intelligence is a multi-method methodology for collecting, analysing and making decisions about data accessible in publicly available sources to be used in an **intelligence** context. In the intelligence community, the term "open" refers to overt, publicly available sources.

Benefits vs Challenges

+

- Global scope
- Fast (near-real time)
- Multi-level (strategic/tactical)
- Inexpensive
- Shareable

-

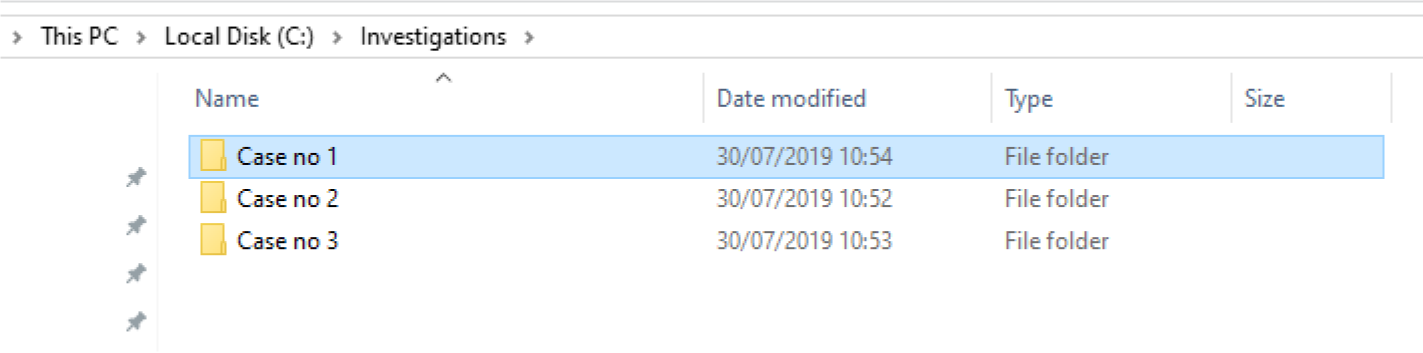
- Overwhelming
- Challenge of verification
- Language barriers
- Overreliance on web
- Lack of training
- Perception of "inferiority"

Basic Elements

- Mindset
- Methodology & Workflow
- Virtual machines
- Web browsers
- Computer Networks and infrastructure
- Staying anonymous
- Maps
- Geolocation
- Pictures
- Videos
- Social networks
- Online Communities
- Data Breaches & Leaks
- Searching the web
- Google dorking
- People and search engines
- Telephone numbers
- Usernames
- Documents
- Email
- Leveraging android emulation
- Virtual currencies
- Government & Business Records
- Tools
  - Maltego
  - Spiderfoot
  - Hunchly
  - FOCA
  - Scripts

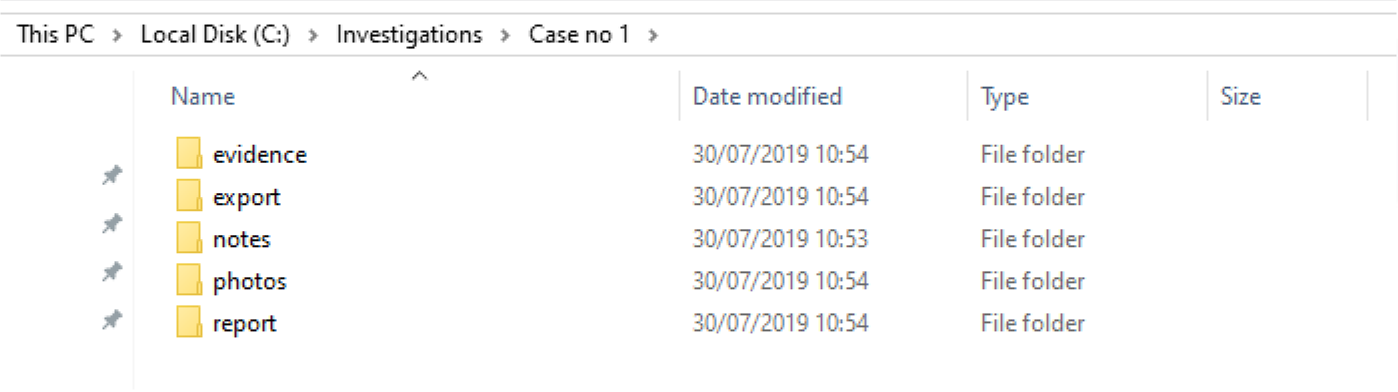
Be organized

- Organize your folders!
  - Start with the case name or number
  - Have subfolders for each case
    - Screenshots
    - Exports
    - Web dumps
    - Documents
    - …



This PC › Local Disk (C:) › Investigations ›

Name	Date modified	Type	Size
Case no 1	30/07/2019 10:54	File folder	
Case no 2	30/07/2019 10:52	File folder	
Case no 3	30/07/2019 10:53	File folder	

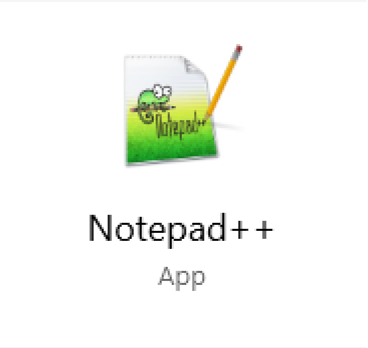


This PC › Local Disk (C:) › Investigations › Case no 1 ›

Name	Date modified	Type	Size
evidence	30/07/2019 10:54	File folder	
export	30/07/2019 10:54	File folder	
notes	30/07/2019 10:53	File folder	
photos	30/07/2019 10:54	File folder	
report	30/07/2019 10:54	File folder	

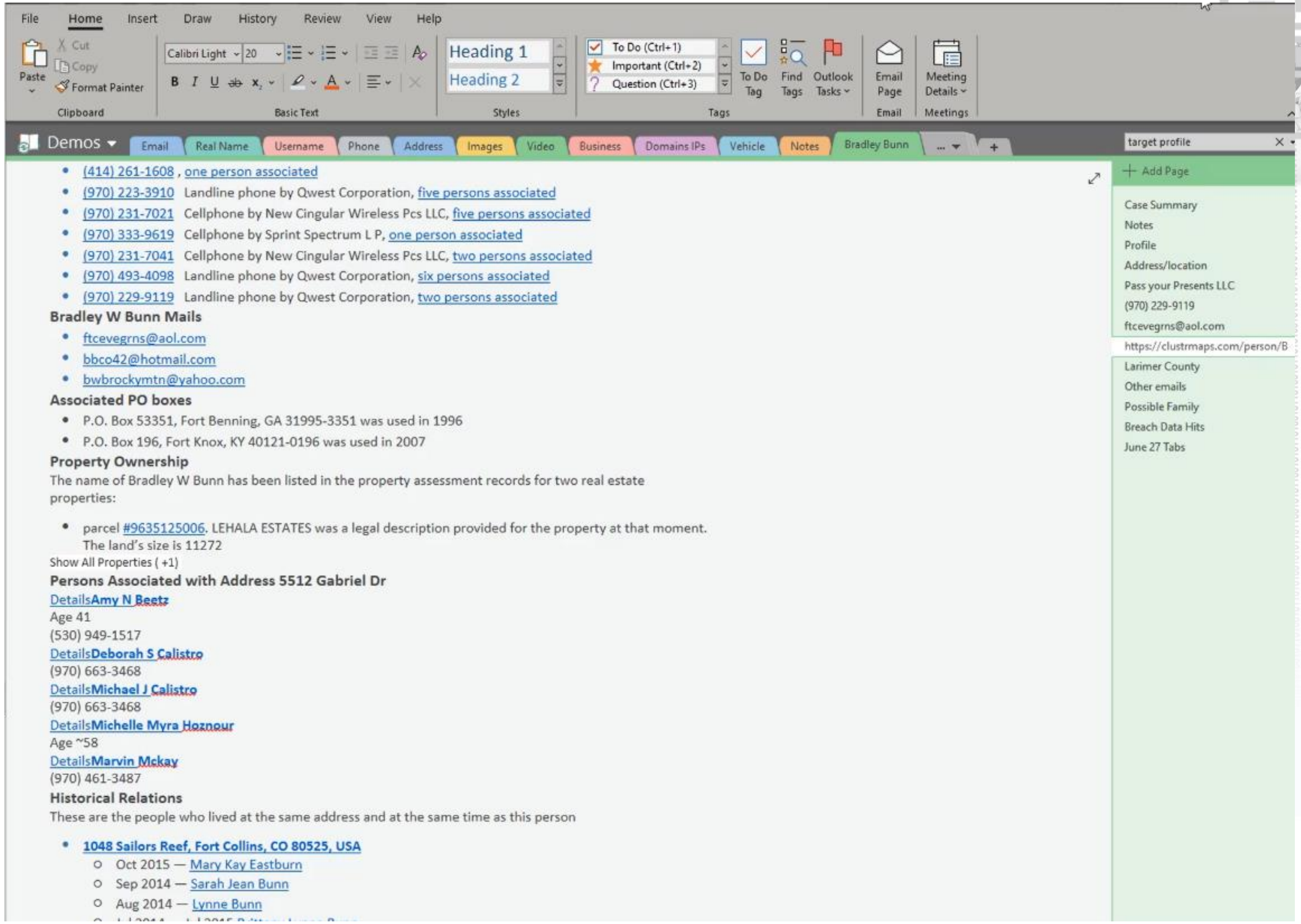
Be organized

- Keep notes
  - You should record everything that you do
  - Notepad is ok, but limited at some points
  - Notepad ++ is better solution
    - Can open bigger files
    - Can make changes even if a file is open with another program
    - With batch scripting automatically puts everything into programming mode
  - Use Microsoft word for some reports
  - Use note keeping apps such Evernote, Google Keep, Emeditor etc.



Typical setup of the workstation: Notetaking

- Paper notebook
- OneNote
- Standard Notes
  - Standardnotes.org
- Atom
  - Atom.io
- Cherrytree – for Linux



- (414) 261-1608 , one person associated
- (970) 223-3910 Landline phone by Qwest Corporation, five persons associated
- (970) 231-7021 Cellphone by New Cingular Wireless Pcs LLC, five persons associated
- (970) 333-9619 Cellphone by Sprint Spectrum L P, one person associated
- (970) 231-7041 Cellphone by New Cingular Wireless Pcs LLC, two persons associated
- (970) 493-4098 Landline phone by Qwest Corporation, six persons associated
- (970) 229-9119 Landline phone by Qwest Corporation, two persons associated

Bradley W Bunn Mails

- ftcevegrns@aol.com
- bbco42@hotmail.com
- bwbrockymtn@yahoo.com

Associated PO boxes

- P.O. Box 53351, Fort Benning, GA 31995-3351 was used in 1996
- P.O. Box 196, Fort Knox, KY 40121-0196 was used in 2007

Property Ownership

The name of Bradley W Bunn has been listed in the property assessment records for two real estate properties:

- parcel #9635125006. LEHALA ESTATES was a legal description provided for the property at that moment.
  The land’s size is 11272

Show All Properties (+1)

Persons Associated with Address 5512 Gabriel Dr

Details**Amy N Beetz**
Age 41
(530) 949-1517
Details**Deborah S Calistro**
(970) 663-3468
Details**Michael J Calistro**
(970) 663-3468
Details**Michelle Myra Hoznour**
Age ~58
Details**Marvin Mckay**
(970) 461-3487

Historical Relations

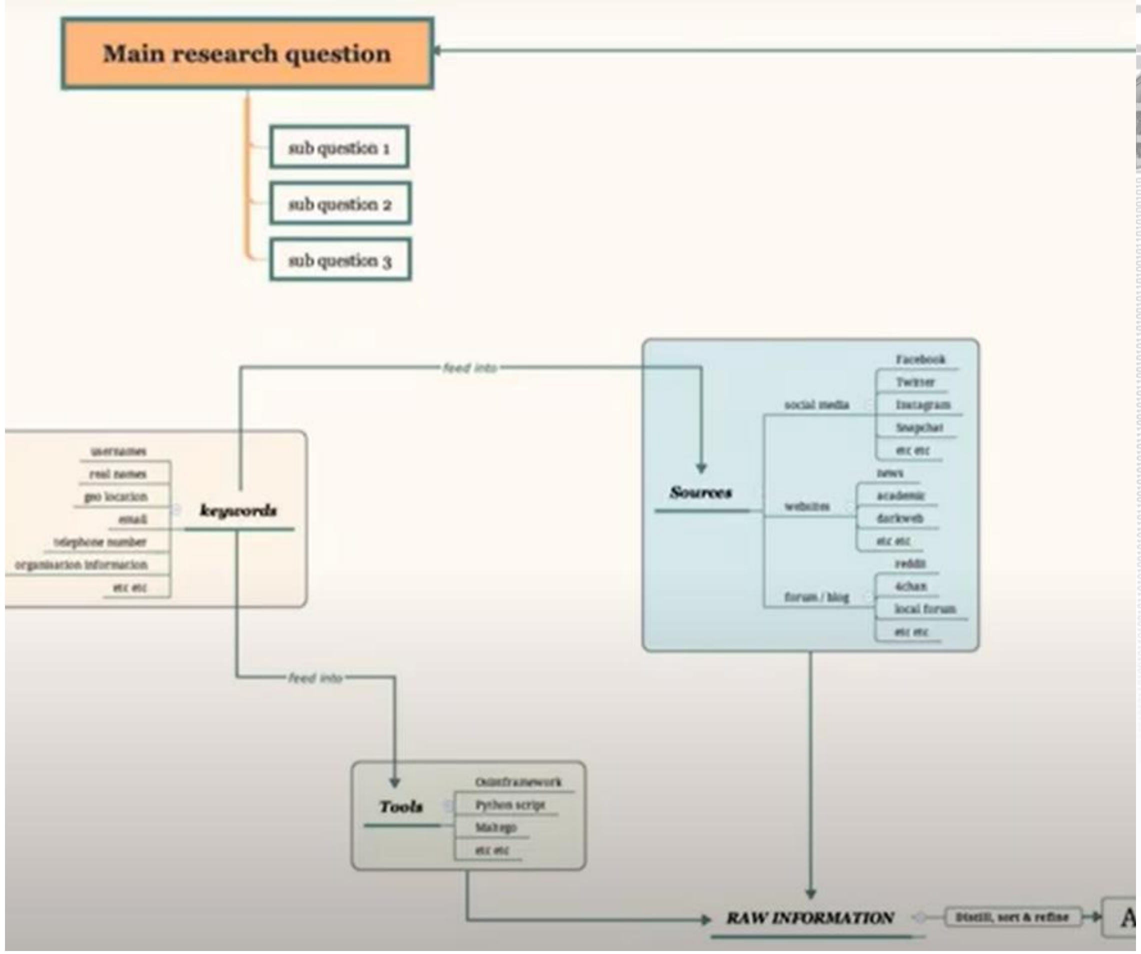
These are the people who lived at the same address and at the same time as this person

- **1048 Sailors Reef, Fort Collins, CO 80525, USA**
  - Oct 2015 — Mary Kay Eastburn
  - Sep 2014 — Sarah Jean Bunn
  - Aug 2014 — Lynne Bunn

Case Summary
Notes
Profile
Address/location
Pass your Presents LLC
(970) 229-9119
ftcevegrns@aol.com
https://clustrmaps.com/person/B
Larimer County
Other emails
Possible Family
Breach Data Hits
June 27 Tabs

Be organized

- Investigative crumb path
  - Keep track of every step you’ve taken
  - Keep track of your thought process
  - Exhaust all your resources
  - Never give up!
  - Use tools to support the process



Be organized

- Know what is important
- Internet is full of information - they may be true or false positive, you need to recognize the correct ones
- Per the latest estimates, 328.77 million terabytes of data are created each day

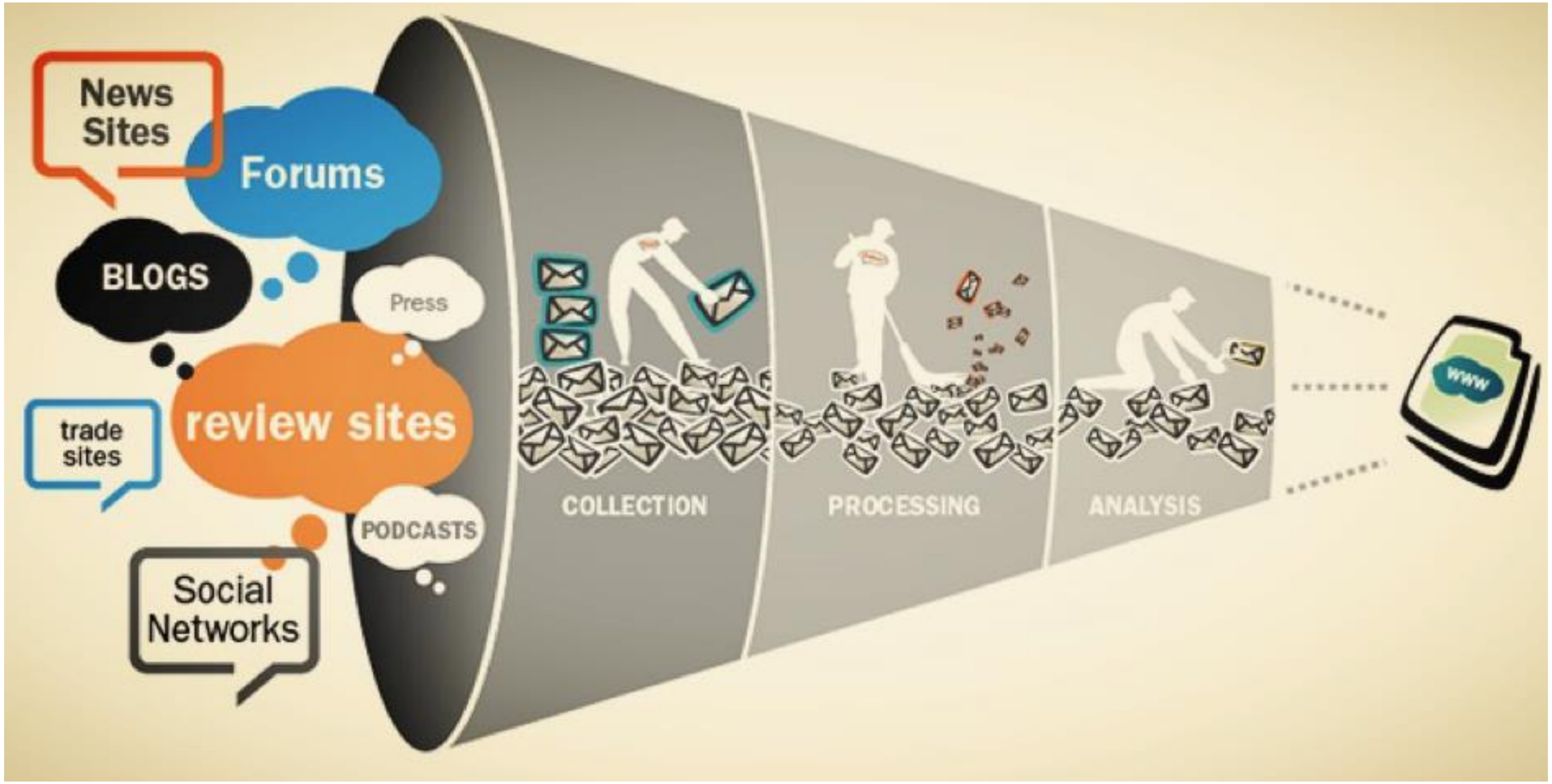
Correct mindset

- By definition, acquiring a lot of ‘intelligence’
- Reality, lots of rubbish with some key ‘hits’
- Key is learning what is relevant

Wrong: Get me EVERYTHING about John Doe

Right: Does John Doe possess X company

Correct mindset



Correct mindset

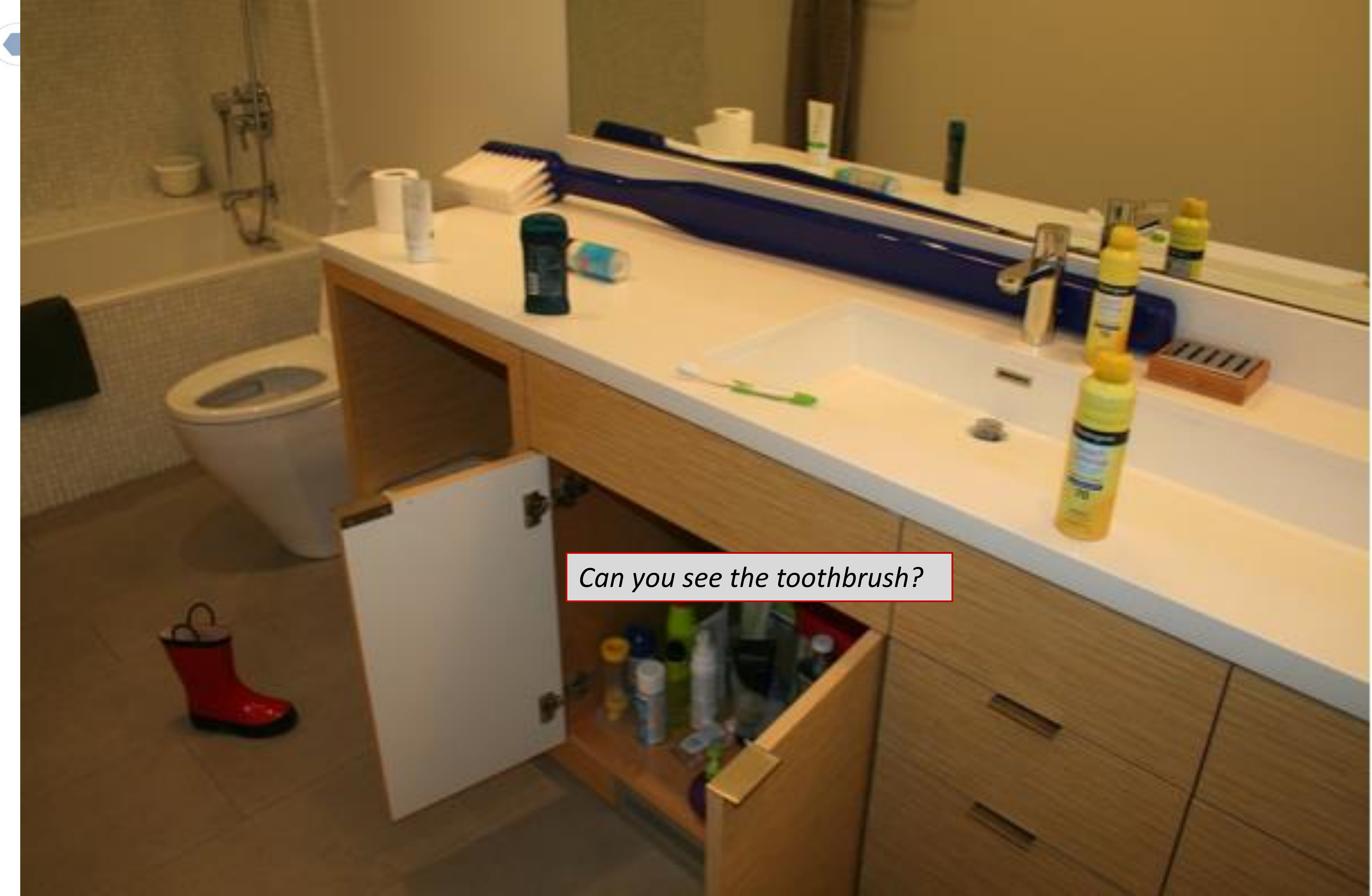
- OSINT is a state of mind
- Manage your research time in an orderly and efficient manner
  - 20+ tabs open in chrome following every social media rabbit hole without any real process

MINDSET IS WHAT SEPARATES THE BEST FROM THE REST.

Correct mindset

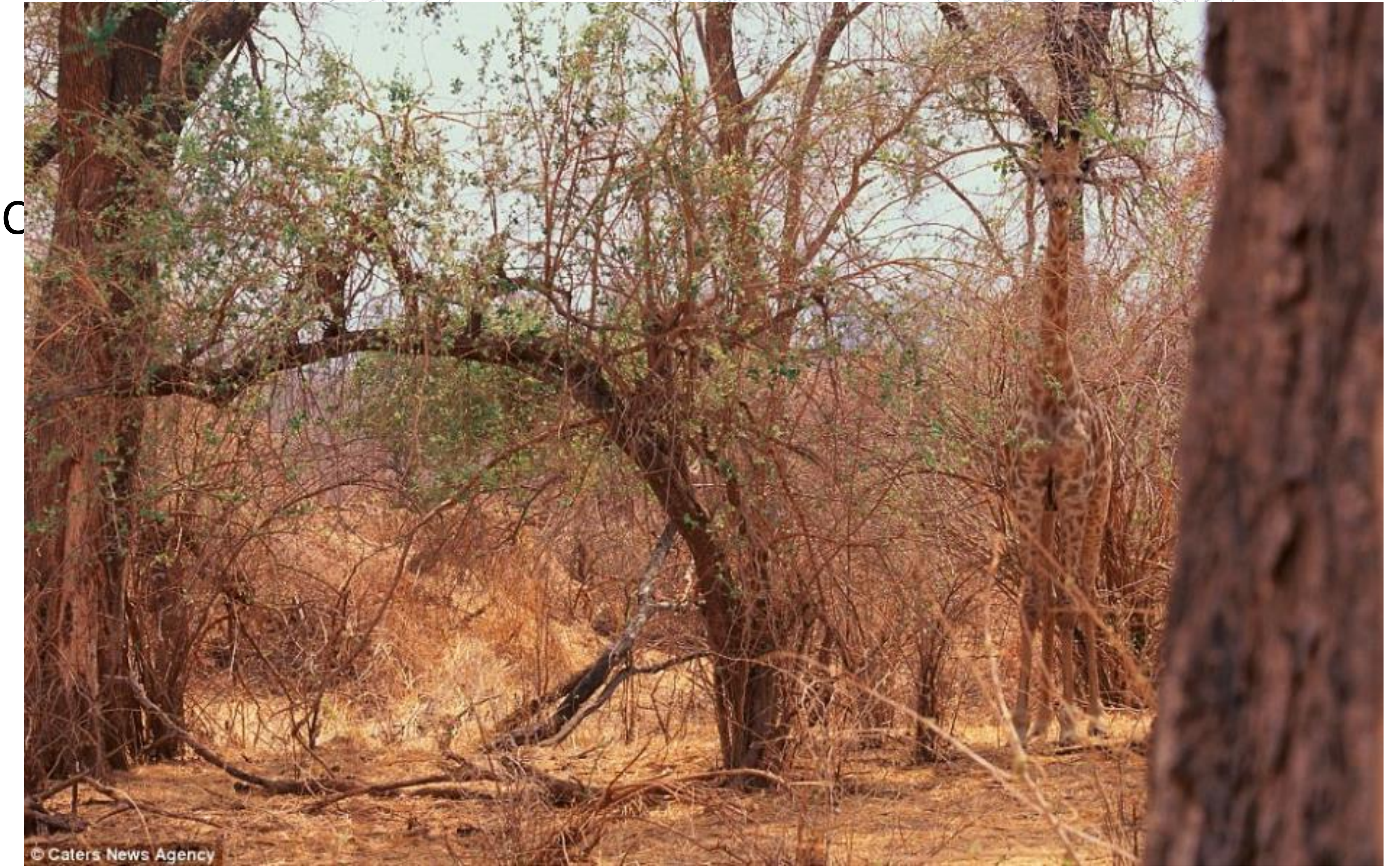
- Never reject data out of hand but think twice to decide what is relevant
- A lot of reading, many useless information, many falls positive results
- Take LOTS of breaks!
- Reject **bias**

MINDSET IS WHAT SEPARATES THE BEST FROM THE REST.



Can you see the toothbrush?

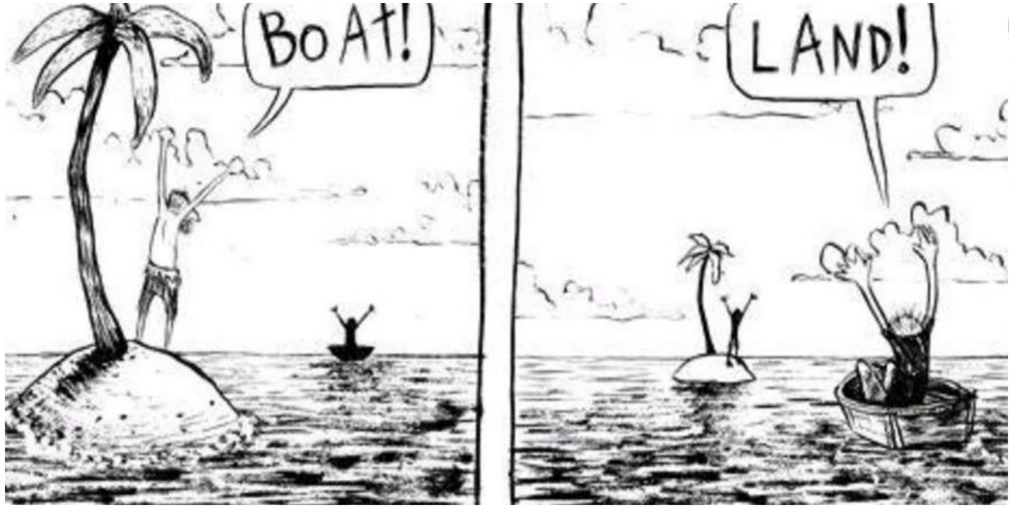
- C



© Caters News Agency

Visual Bias

- We all have bias – means we see what our brain wants us to see
  - Cultural
  - Emotional
  - Gender
  - Interests
  - **Bias caused by scope of the investigation**

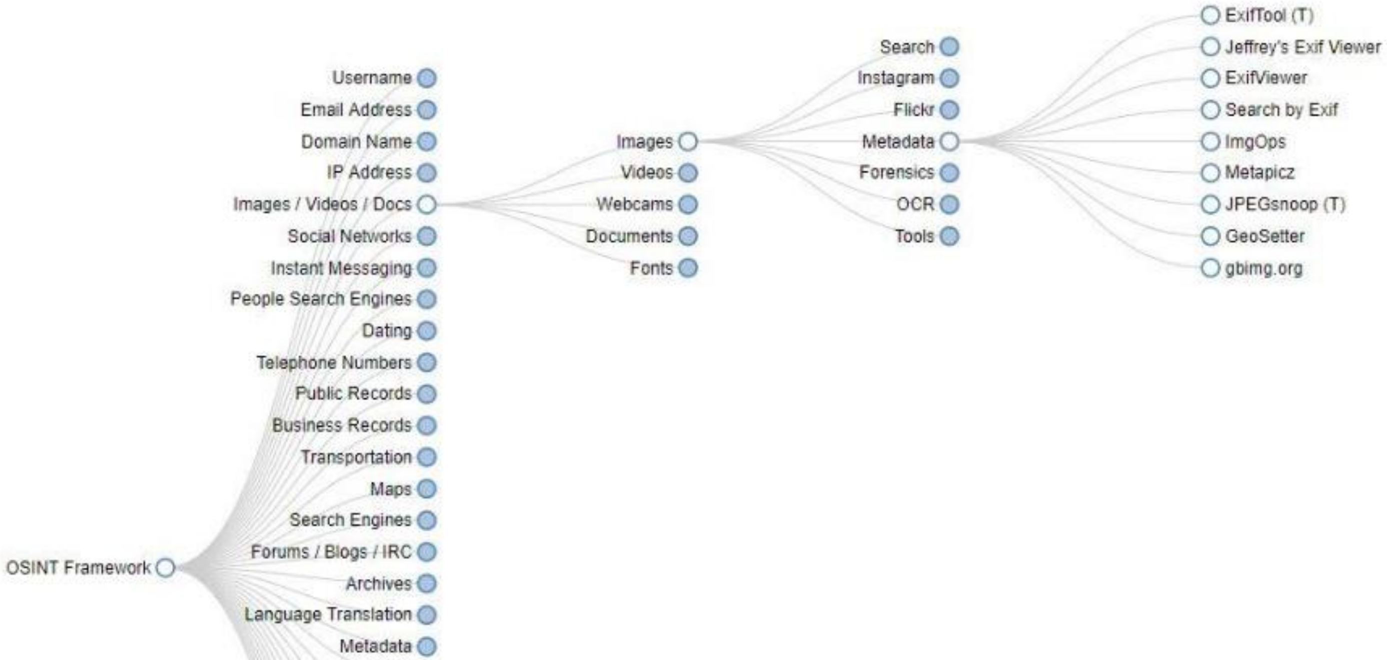


- Risk we see things that are not there
- Miss things that are there for us to see

OSINT Frameworks

Osintframework.com

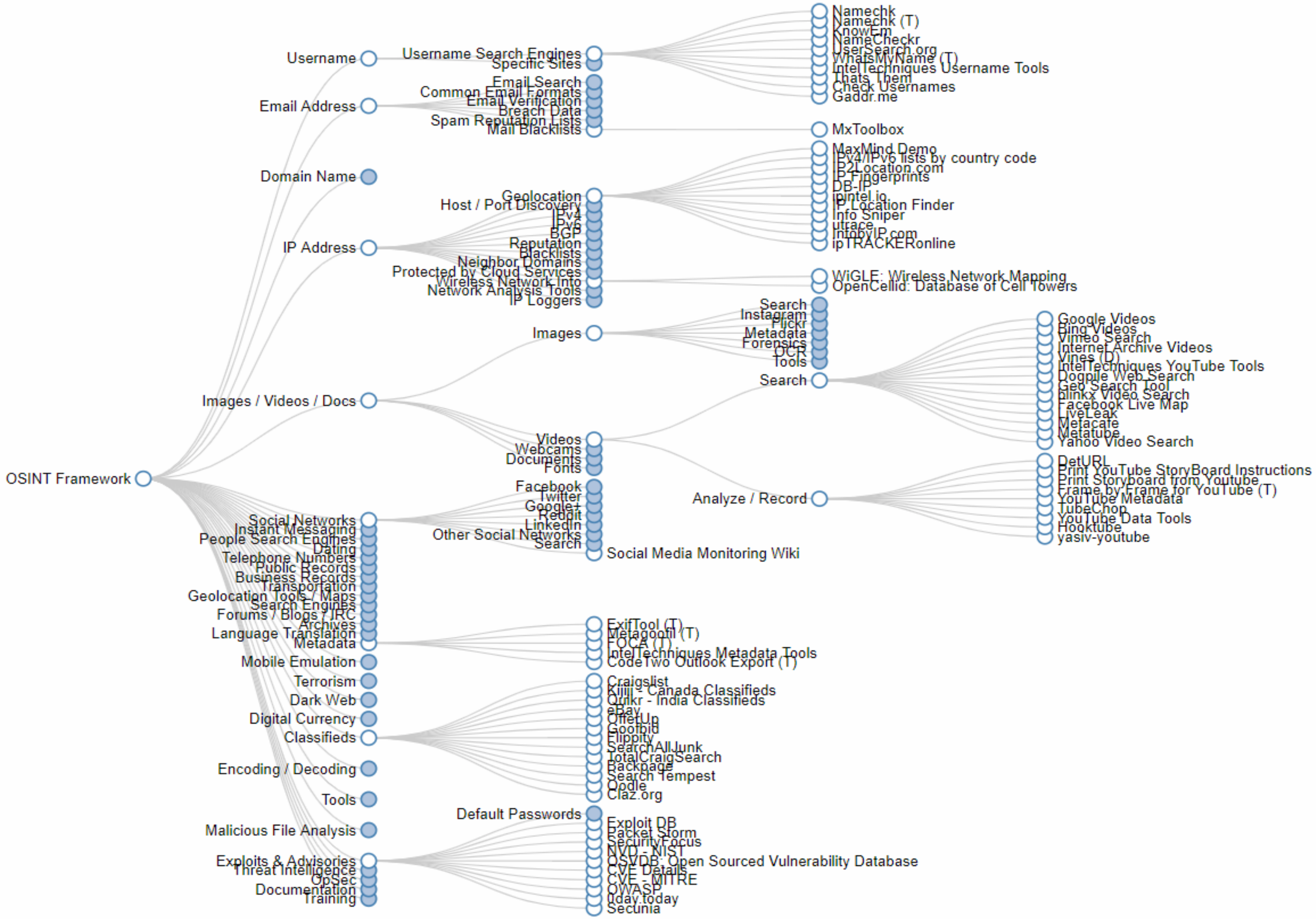
- Osintframework.com can help you to organize your search.
- OSINT framework is focused on gathering information from free tools or resources. Some sites might require registration or offer paid upgrades



OSINT Framework

- It can be overwhelming

- Script on GitHub which includes all the tools with clear instructions how to install/use them



Efficient dialogue with searching engines

Browser vs Search engine

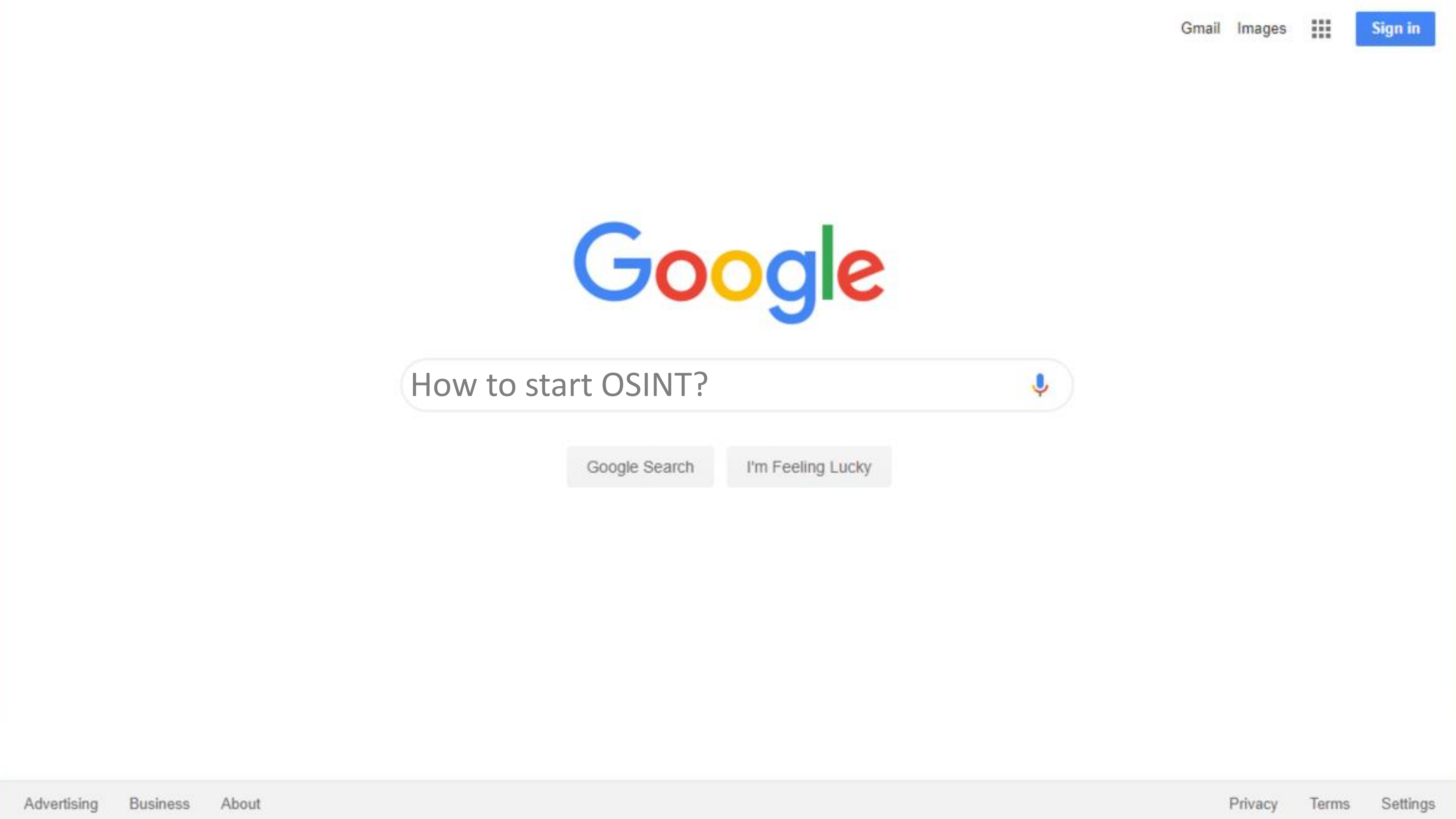
Browser

- Browse a webpage
- Can exist without search engine
- Installed on your PC

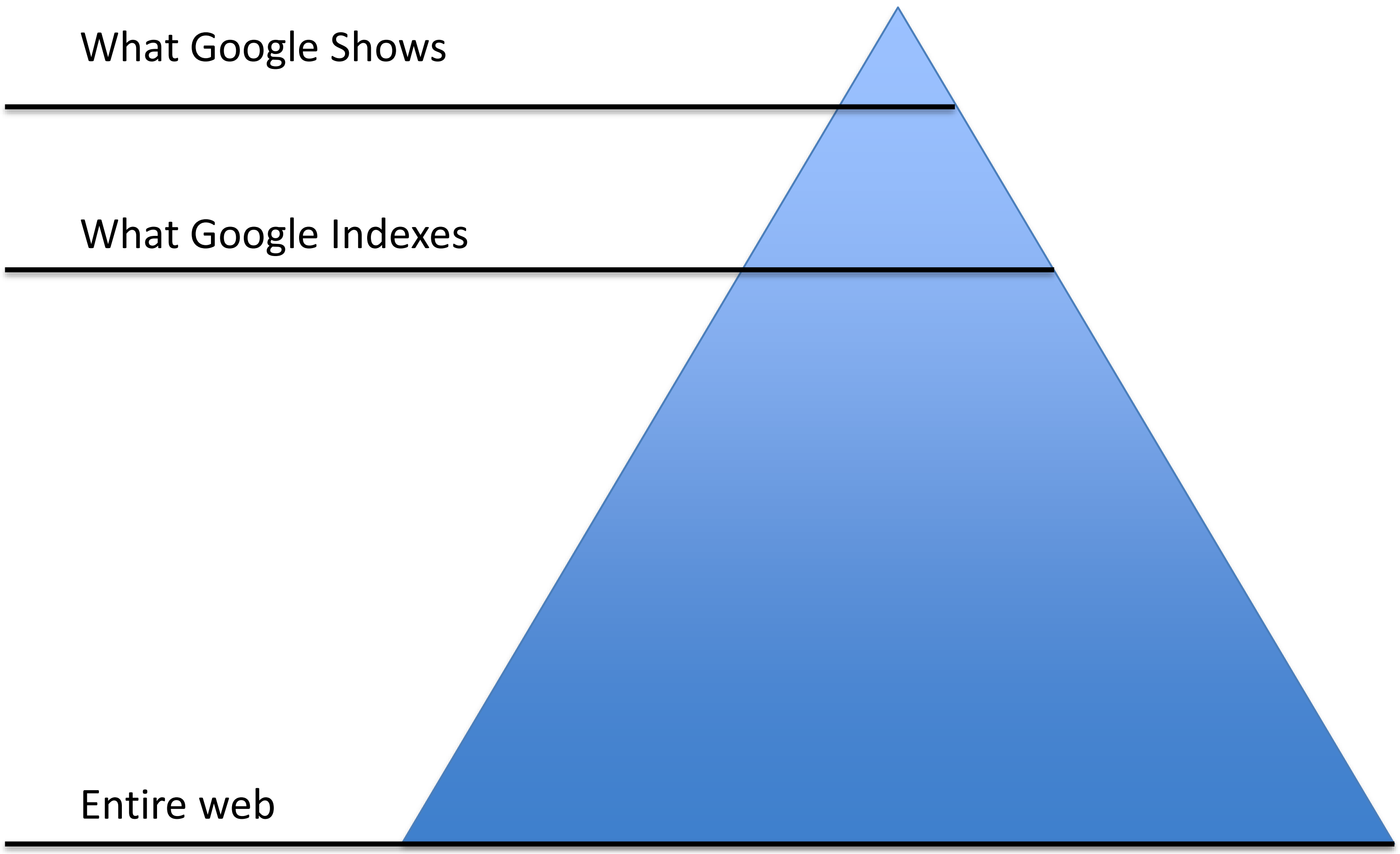
Search engine

- Search a webpage
- Needs a browser to display results
- Software running on the internet

INSIG7



How to start OSINT?



What Google Shows

What Google Indexes

Entire web

Selective Exposure Theory – Search Engine Bias

- What about the search engines we use?
- There are more out there than just Google.

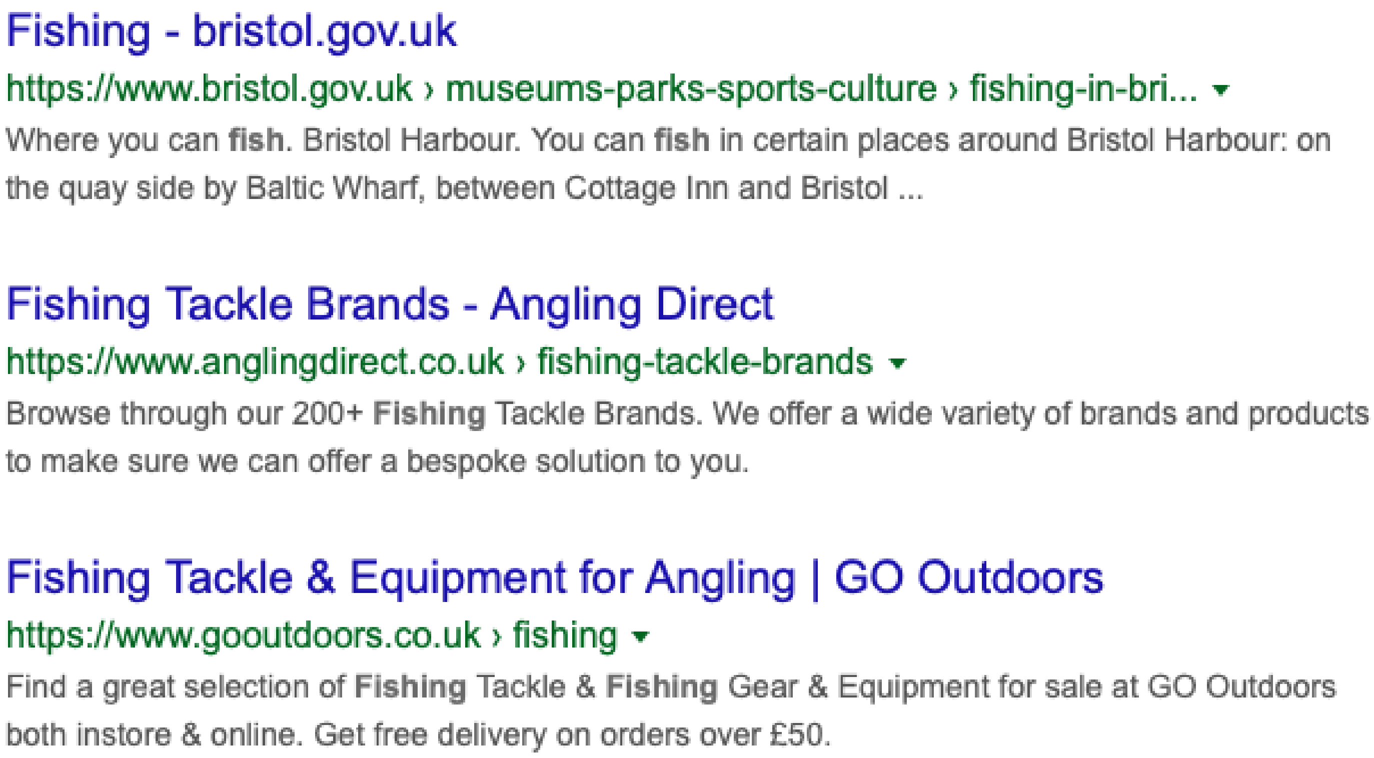
- Little OSI Secret……..

GOOGLE IS TERRIBLE AT SEARCHING THE INTERNET!!!!!

- Results will vary drastically
- Hence, we need to force Google to give us data we want!

Selective Exposure Theory – Search Engine Bias

- Google.co.uk



Fishing - bristol.gov.uk

https://www.bristol.gov.uk › museums-parks-sports-culture › fishing-in-bri... ▾

Where you can **fish**. Bristol Harbour. You can **fish** in certain places around Bristol Harbour: on the quay side by Baltic Wharf, between Cottage Inn and Bristol ...

Fishing Tackle Brands - Angling Direct

https://www.anglingdirect.co.uk › fishing-tackle-brands ▾

Browse through our 200+ **Fishing** Tackle Brands. We offer a wide variety of brands and products to make sure we can offer a bespoke solution to you.

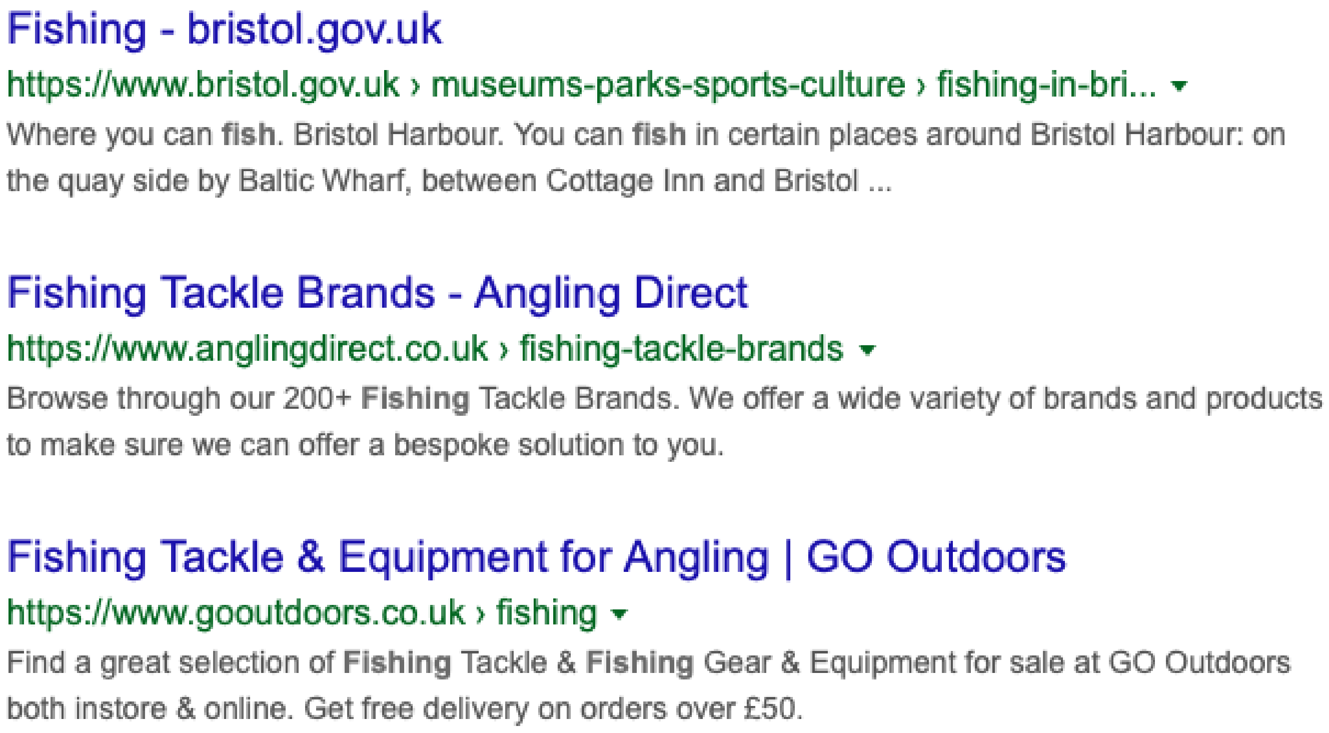
Fishing Tackle & Equipment for Angling | GO Outdoors

https://www.gooutdoors.co.uk › fishing ▾

Find a great selection of **Fishing** Tackle & **Fishing** Gear & Equipment for sale at GO Outdoors both instore & online. Get free delivery on orders over £50.

Selective Exposure Theory – Search Engine Bias

- Google.com.au



Fishing - bristol.gov.uk

https://www.bristol.gov.uk › museums-parks-sports-culture › fishing-in-bri... ▾

Where you can **fish**. Bristol Harbour. You can **fish** in certain places around Bristol Harbour: on the quay side by Baltic Wharf, between Cottage Inn and Bristol ...

Fishing Tackle Brands - Angling Direct

https://www.anglingdirect.co.uk › fishing-tackle-brands ▾

Browse through our 200+ **Fishing** Tackle Brands. We offer a wide variety of brands and products to make sure we can offer a bespoke solution to you.

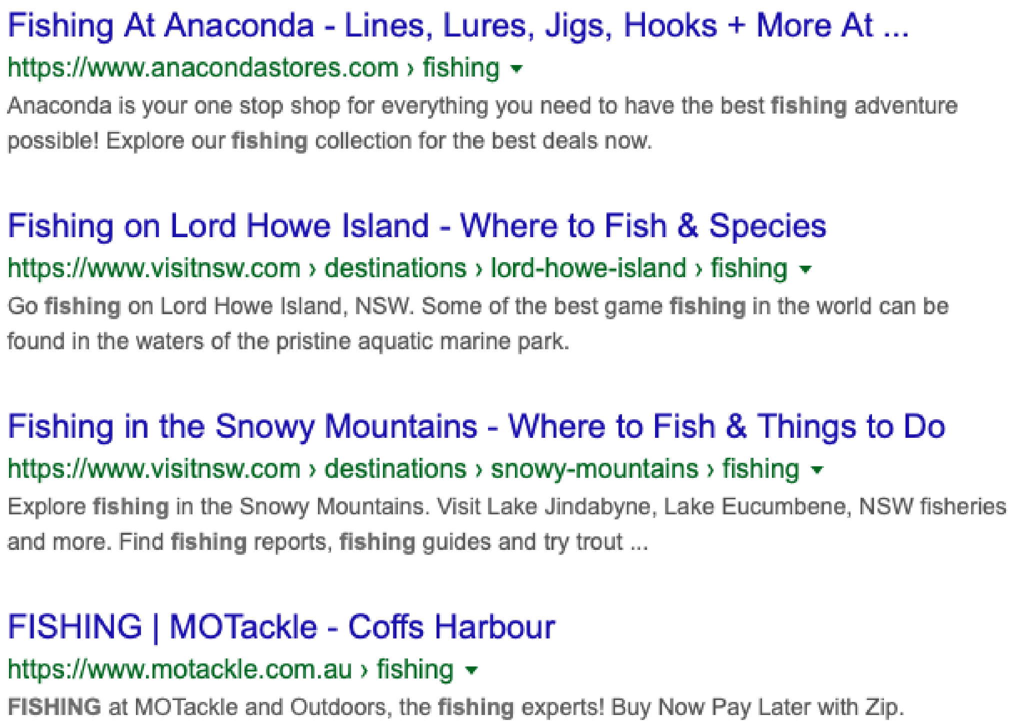
Fishing Tackle & Equipment for Angling | GO Outdoors

https://www.gooutdoors.co.uk › fishing ▾

Find a great selection of **Fishing** Tackle & **Fishing** Gear & Equipment for sale at GO Outdoors both instore & online. Get free delivery on orders over £50.

Selective Exposure Theory – Search Engine Bias

- Google.com.au whilst VPN’d into Australia



Fishing At Anaconda - Lines, Lures, Jigs, Hooks + More At ...
https://www.anacondastores.com › fishing ▾
Anaconda is your one stop shop for everything you need to have the best **fishing** adventure possible! Explore our **fishing** collection for the best deals now.

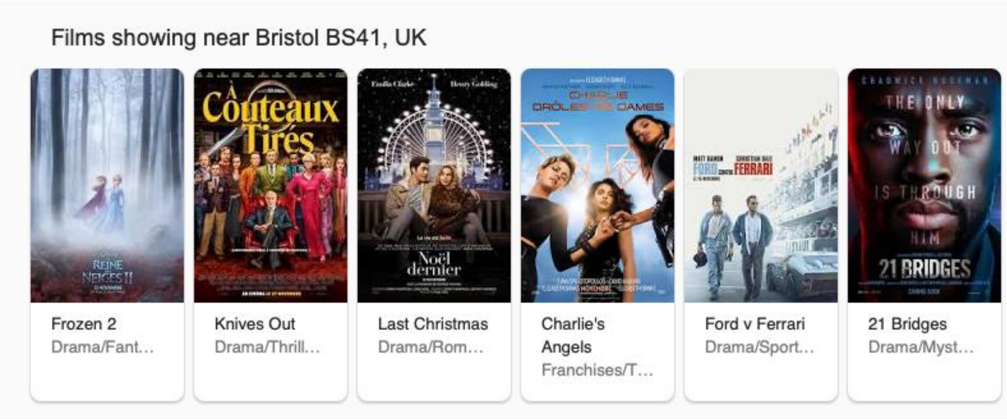
Fishing on Lord Howe Island - Where to Fish & Species
https://www.visitnsw.com › destinations › lord-howe-island › fishing ▾
Go **fishing** on Lord Howe Island, NSW. Some of the best game **fishing** in the world can be found in the waters of the pristine aquatic marine park.

Fishing in the Snowy Mountains - Where to Fish & Things to Do
https://www.visitnsw.com › destinations › snowy-mountains › fishing ▾
Explore **fishing** in the Snowy Mountains. Visit Lake Jindabyne, Lake Eucumbene, NSW fisheries and more. Find **fishing** reports, **fishing** guides and try trout ...

FISHING | MOTackle - Coffs Harbour
https://www.motackle.com.au › fishing ▾
FISHING at MOTackle and Outdoors, the **fishing** experts! Buy Now Pay Later with Zip.

Selective Exposure Theory – Search Engine Bias

- Actually, Google is incredibly good at giving you what **IT THINKS** you want
- Just search for Movies



Films showing near Bristol BS41, UK

Frozen 2 Drama/Fant…	Knives Out Drama/Thrill…	Last Christmas Drama/Rom…	Charlie's Angels Franchises/T…	Ford v Ferrari Drama/Sport…	21 Bridges Drama/Myst…

I Don't Have the Data You Asked For But I Do Have The Data You Need.

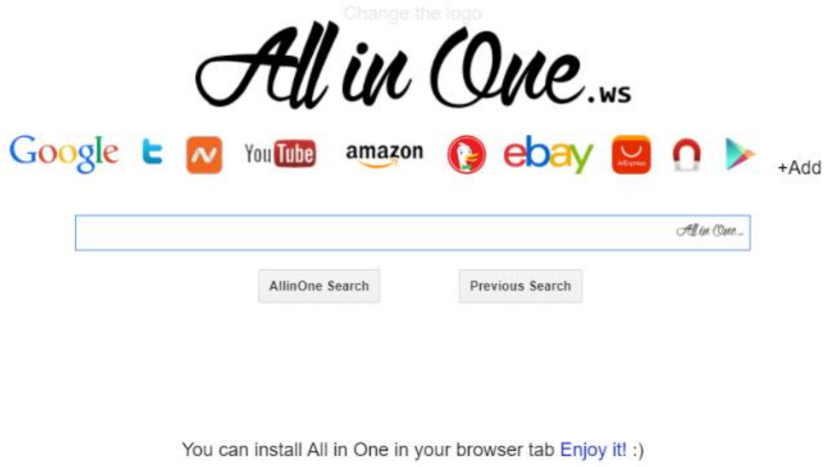
Search engines

Largest & with more websites indexed:

- Google (Largest)
- Yandex (Russian)
- DuckDuckGo (US)
- Baidu (Chinese)
- Bing (Microsoft)

...

https://all-io.net/



You can install All in One in your browser tab Enjoy it! :)

Google

Yandex

DuckDuckGo

Baidu 百度

Bing

Search engines

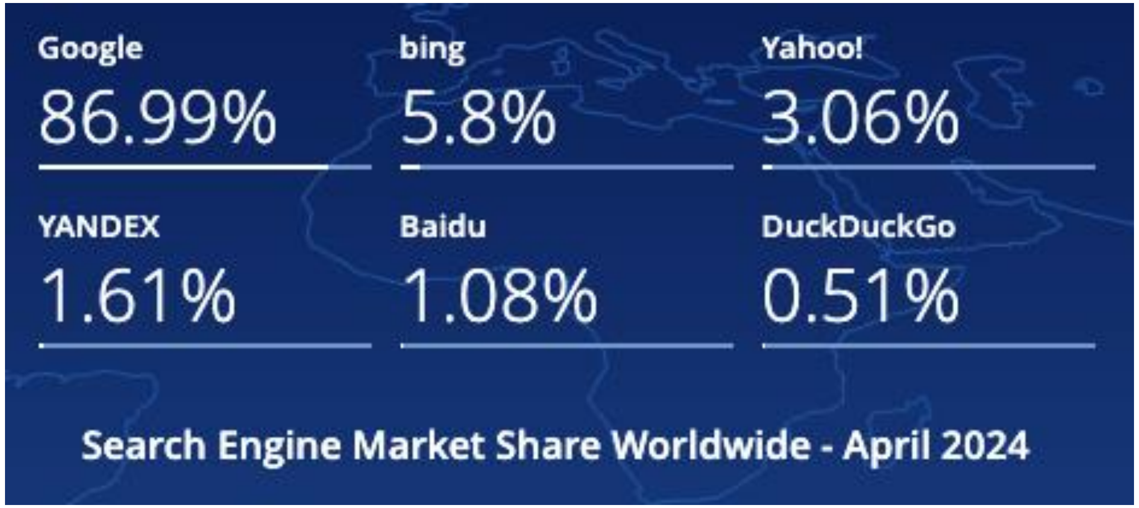
Each search engine runs on a different algorithm

Translators are different on other search engines.

All these factors have impact on search results.

For comprehensive research use more search engines and specific country search engines.

Google has largest market share, but it does not mean it will find you what you are searching for.



Google
86.99%

bing
5.8%

Yahoo!
3.06%

YANDEX
1.61%

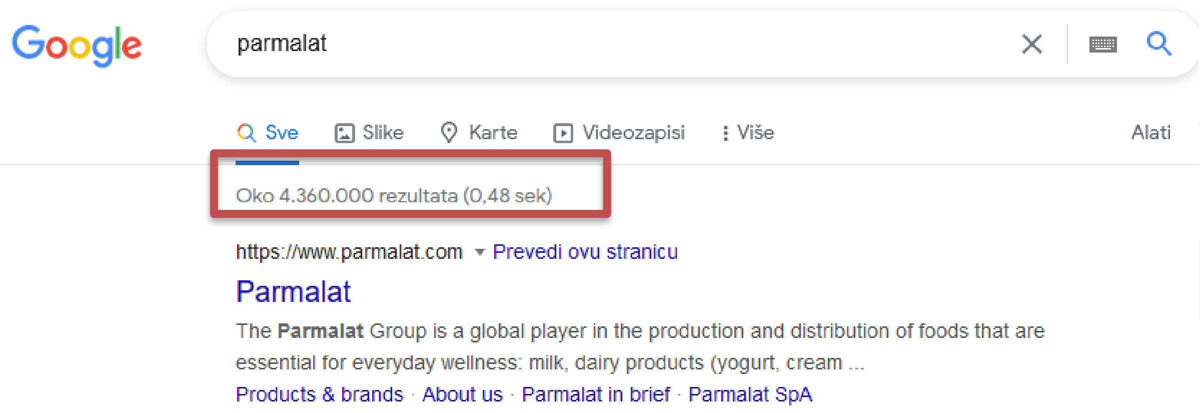
Baidu
1.08%

DuckDuckGo
0.51%

Search Engine Market Share Worldwide - April 2024

Search engines (results)

- Factors that will make search results different:
  - Algorithm
  - Language
  - Computer IP
  - Your Personal interest if you log in to Google
  - Number of indexed data (*as you can see Google have index 5 times more data than Bing*)



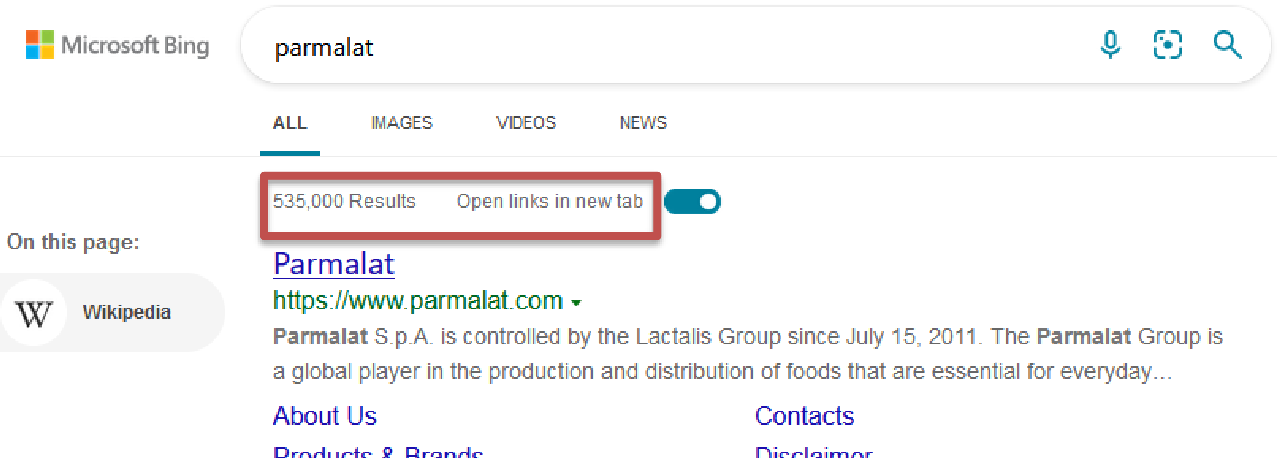
Oko 4.360.000 rezultata (0,48 sek)

https://www.parmalat.com ▾ Prevedi ovu stranicu

Parmalat

The **Parmalat** Group is a global player in the production and distribution of foods that are essential for everyday wellness: milk, dairy products (yogurt, cream ...

Products & brands · About us · Parmalat in brief · Parmalat SpA



535,000 Results Open links in new tab

Parmalat

https://www.parmalat.com ▾

Parmalat S.p.A. is controlled by the Lactalis Group since July 15, 2011. The **Parmalat** Group is a global player in the production and distribution of foods that are essential for everyday...

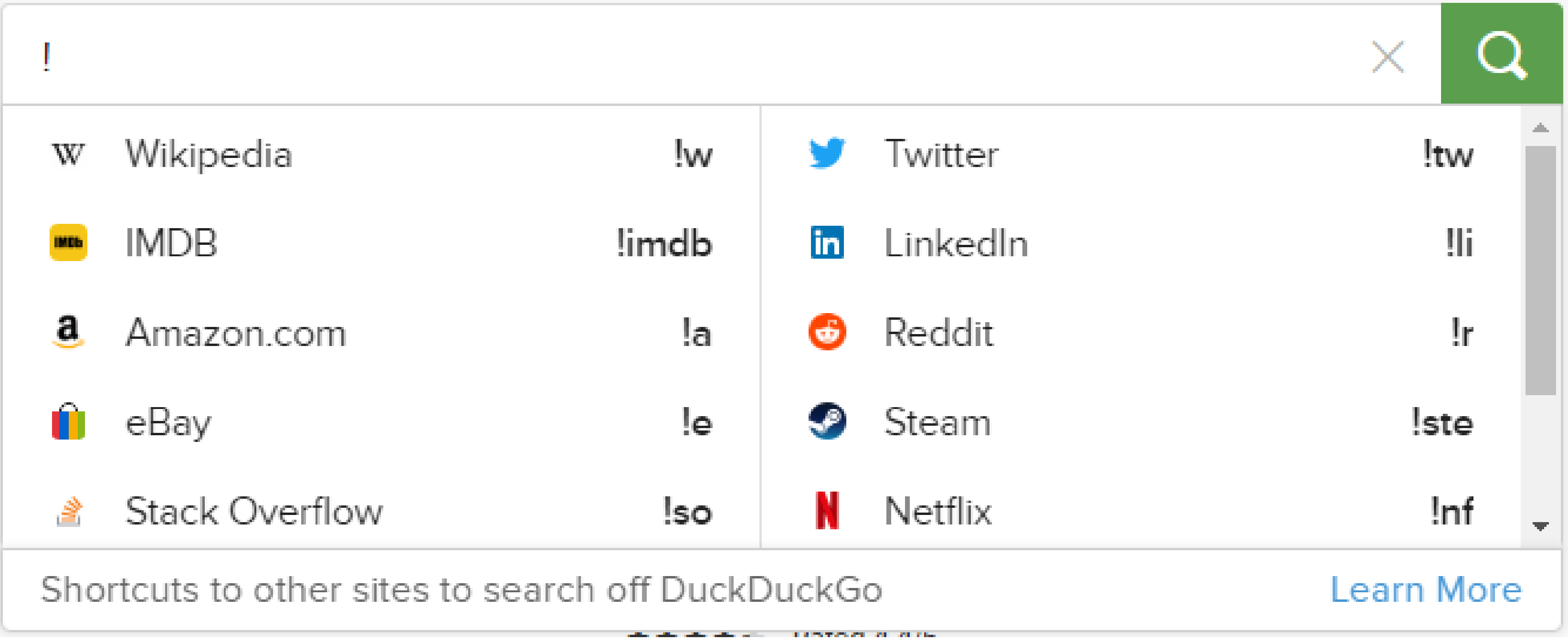
About Us Contacts

Products & Brands Disclaimer

DuckDuckGo.com

- No tracking (*same search for everyone*)
- Can direct search to other engines
- No Ads to interfere the search

DuckDuckGo



!

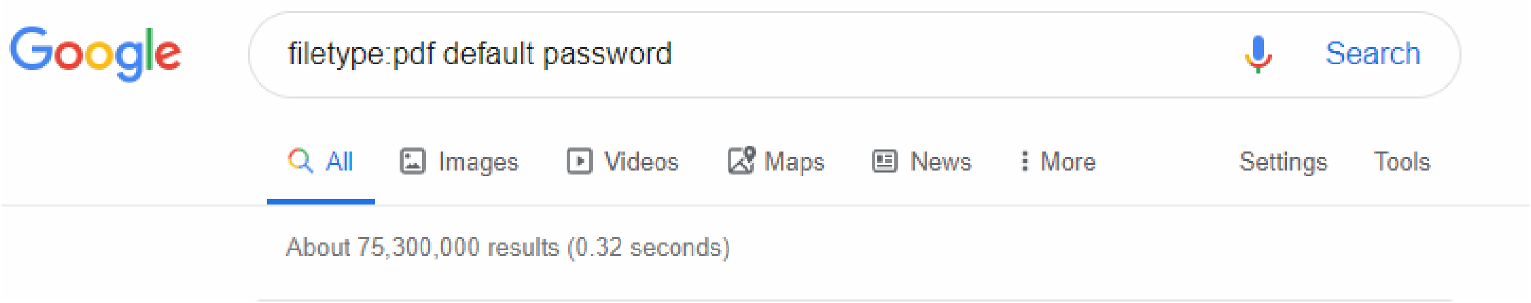
Wikipedia	!w	Twitter	!tw
IMDB	!imdb	LinkedIn	!li
Amazon.com	!a	Reddit	!r
eBay	!e	Steam	!ste
Stack Overflow	!so	Netflix	!nf

Shortcuts to other sites to search off DuckDuckGo

Documents

- Did you know that google allows us to look specifically for documents?

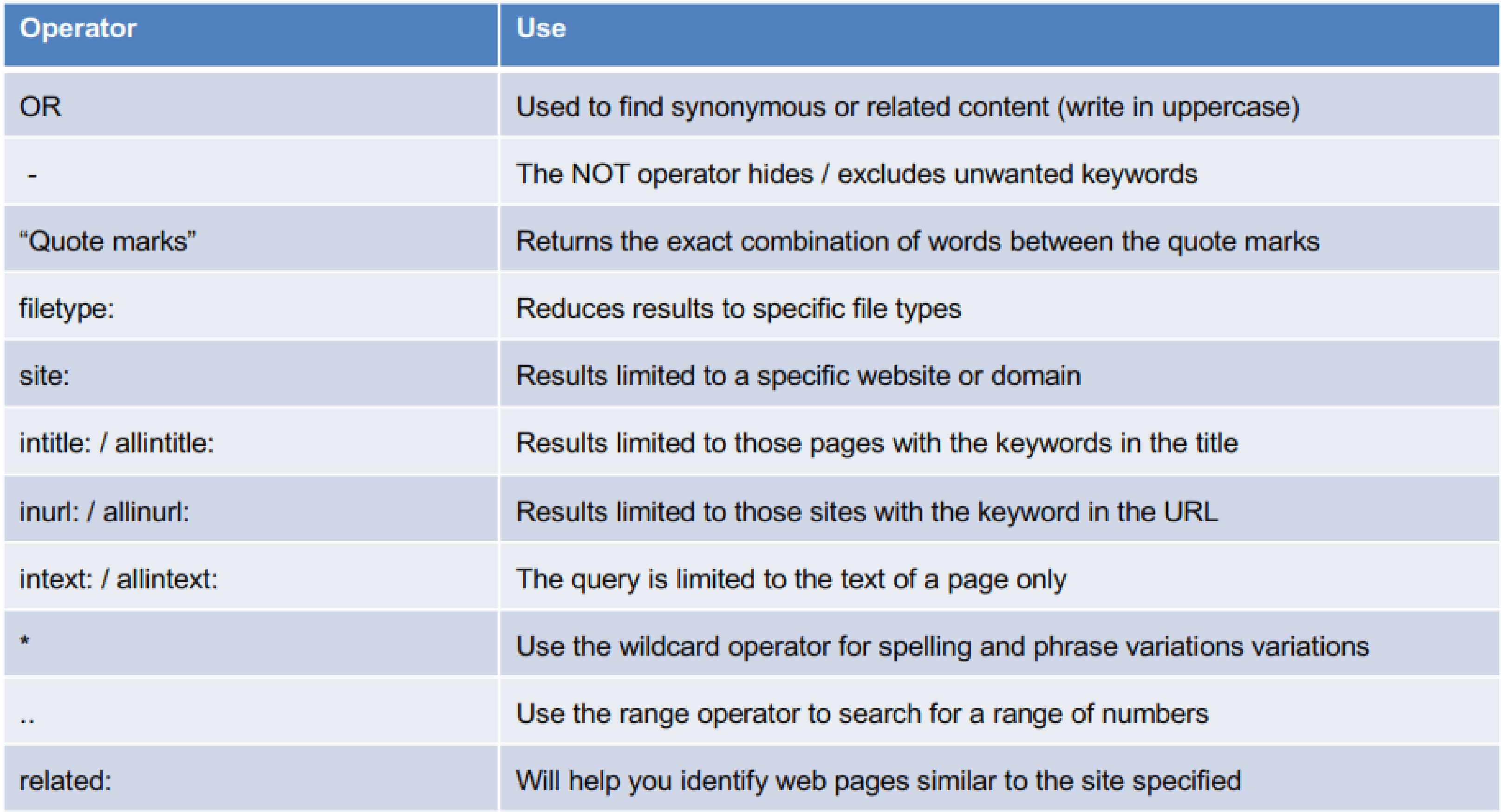
- We just have to supply the filetype
  - Filetype:pdf
  - Filetype:csv
  - Filetype:doc



filetype:pdf default password

About 75,300,000 results (0.32 seconds)

Google operators



Operator	Use
OR	Used to find synonymous or related content (write in uppercase)
-	The NOT operator hides / excludes unwanted keywords
“Quote marks”	Returns the exact combination of words between the quote marks
filetype:	Reduces results to specific file types
site:	Results limited to a specific website or domain
intitle: / allintitle:	Results limited to those pages with the keywords in the title
inurl: / allinurl:	Results limited to those sites with the keyword in the URL
intext: / allintext:	The query is limited to the text of a page only
*	Use the wildcard operator for spelling and phrase variations variations
..	Use the range operator to search for a range of numbers
related:	Will help you identify web pages similar to the site specified

Smart queries for People Search

- Master Search Engine operators

  Ex: “username” site:facebook.com inurl:photos; “username” inurl:profile

- Check online spaces (websites, blogs, wikis etc)

  Ex: site:wix.com “username”

- Check Q&A sites (quora, stackexchange, answers etc)

  Ex: “username” site:stackexchange.com

- Check user groups

  Ex: “username” site:groups.google.com

- Search document repositories (Docs, Aws, OneDrive, Slideshare etc)

Smart queries for People Search

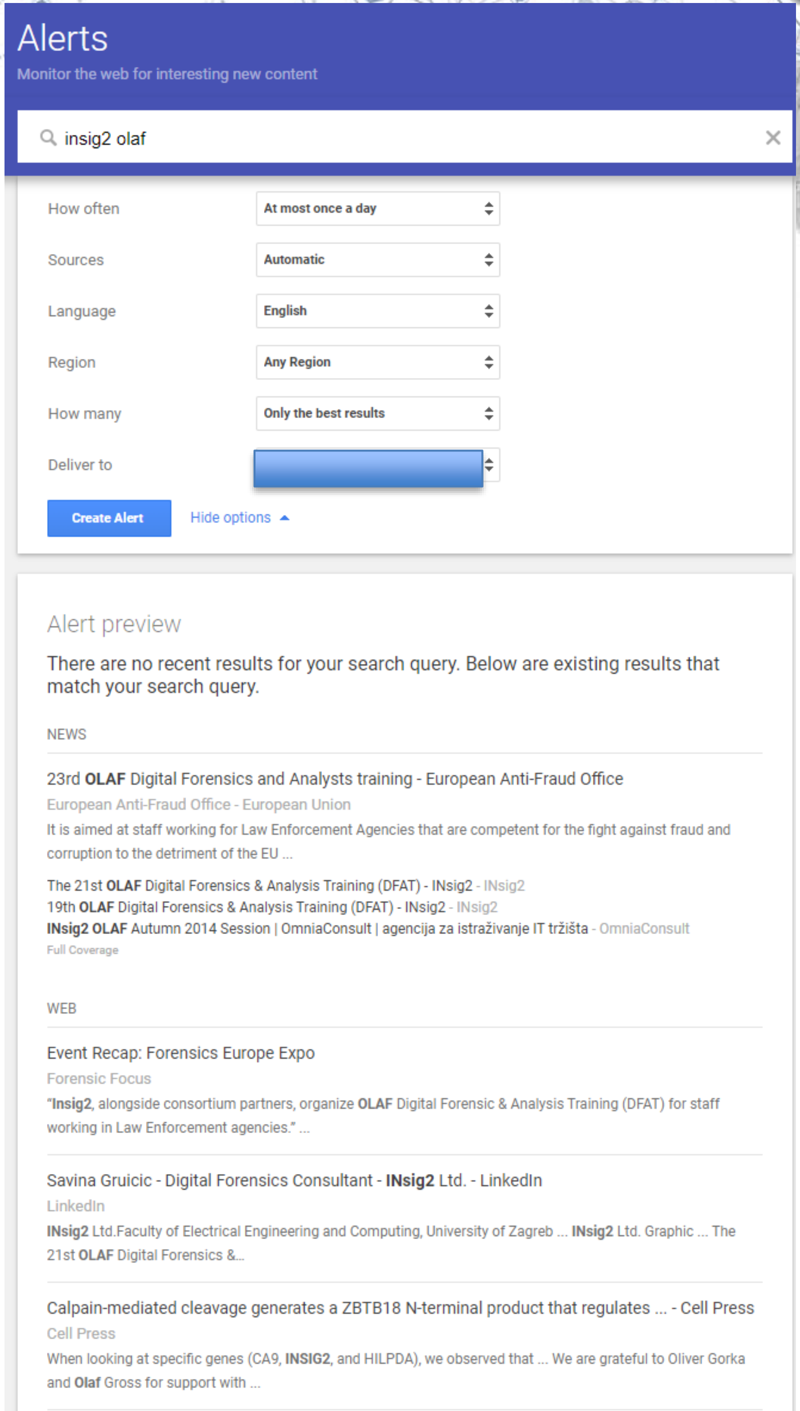
- Search for CVs (ex: “Name” “CV” inurl:resume OR intitle:resume
- Check dating sites (username + “site” operator)
- Check online marketplaces (username + site or inurl; ex: alibaba.com)
- Education history (site: + domain or education institution)
- Validate credentials through complex queries (ex: intitle:“TARGET NAME” inurl:speaker OR inurl:speakers OR inurl:author OR inurl:authors OR inurl:instructor OR inurl:instructors OR inurl:expert OR inurl:experts

Email search

- Usernames often associate with emails
- Run Google queries / setup Google Alerts
- Check breached data (https://haveibeenpwned.com etc)
- Check specialized email search tools (https://epieos.com etc)
- Find private email address (constructs and guesses, socmint)
- Find professional email address (www.hunter.io etc)
- Run email validator (www.email-validator.net etc)
- Reverse email checks (www.pipl.com etc)
- Check email provider for business emails (www.mxtoolbox.com etc)
- Check blacklists (www.mxtoolbox.com etc)

Google Alerts

- Monitor the web for interesting new content
  – Google.com/alerts



Alerts

Monitor the web for interesting new content

insig2 olaf

How often: At most once a day

Sources: Automatic

Language: English

Region: Any Region

How many: Only the best results

Deliver to

Alert preview

There are no recent results for your search query. Below are existing results that match your search query.

NEWS

23rd **OLAF** Digital Forensics and Analysts training - European Anti-Fraud Office
European Anti-Fraud Office - European Union
It is aimed at staff working for Law Enforcement Agencies that are competent for the fight against fraud and corruption to the detriment of the EU ...

The 21st **OLAF** Digital Forensics & Analysis Training (DFAT) - INsig2 - INsig2
19th **OLAF** Digital Forensics & Analysis Training (DFAT) - INsig2 - INsig2
INsig2 OLAF Autumn 2014 Session | OmniaConsult | agencija za istraživanje IT tržišta - OmniaConsult
Full Coverage

WEB

Event Recap: Forensics Europe Expo
Forensic Focus
"**Insig2**, alongside consortium partners, organize **OLAF** Digital Forensic & Analysis Training (DFAT) for staff working in Law Enforcement agencies." ...

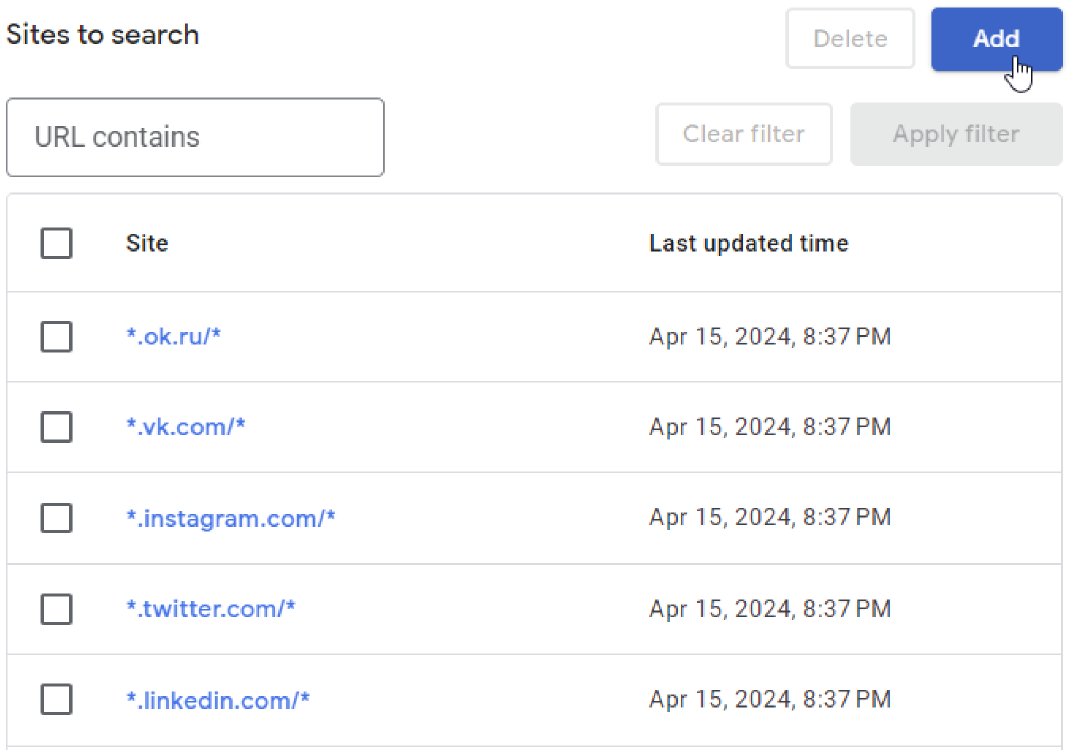
Savina Gruicic - Digital Forensics Consultant - **INsig2** Ltd. - LinkedIn
LinkedIn
INsig2 Ltd.Faculty of Electrical Engineering and Computing, University of Zagreb ... **INsig2** Ltd. Graphic ... The 21st **OLAF** Digital Forensics &...

Calpain-mediated cleavage generates a ZBTB18 N-terminal product that regulates ... - Cell Press
Cell Press
When looking at specific genes (CA9, **INSIG2**, and HILPDA), we observed that ... We are grateful to Oliver Gorka and **Olaf** Gross for support with ...

GOOGLE Programmable Search Engine (PSE)
a.k.a. Custom search engine (CSE)

Google Custom Search (CSE)

- It is alternative to Google Dorks
- Simple to use
- Sites relevant to search can be added
- Custom filters in a form of smart queries filter data further



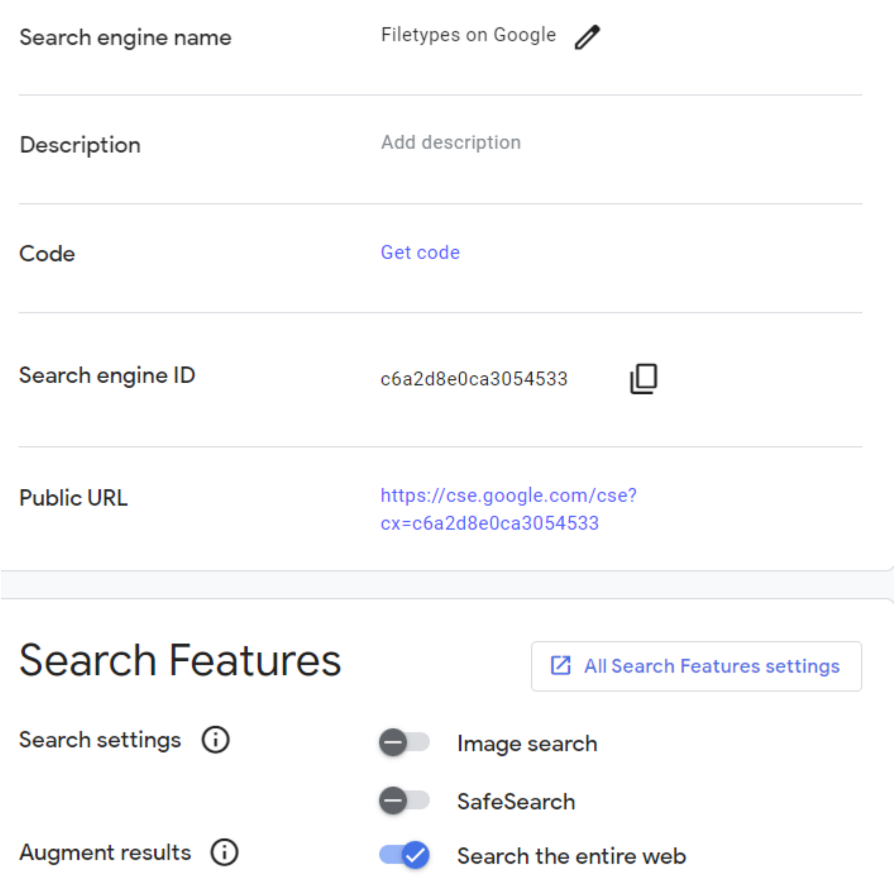
Sites to search

URL contains

□	Site	Last updated time
□	*.ok.ru/*	Apr 15, 2024, 8:37 PM
□	*.vk.com/*	Apr 15, 2024, 8:37 PM
□	*.instagram.com/*	Apr 15, 2024, 8:37 PM
□	*.twitter.com/*	Apr 15, 2024, 8:37 PM
□	*.linkedin.com/*	Apr 15, 2024, 8:37 PM

Google Custom Search

- CSEs can be shared / edited / refined

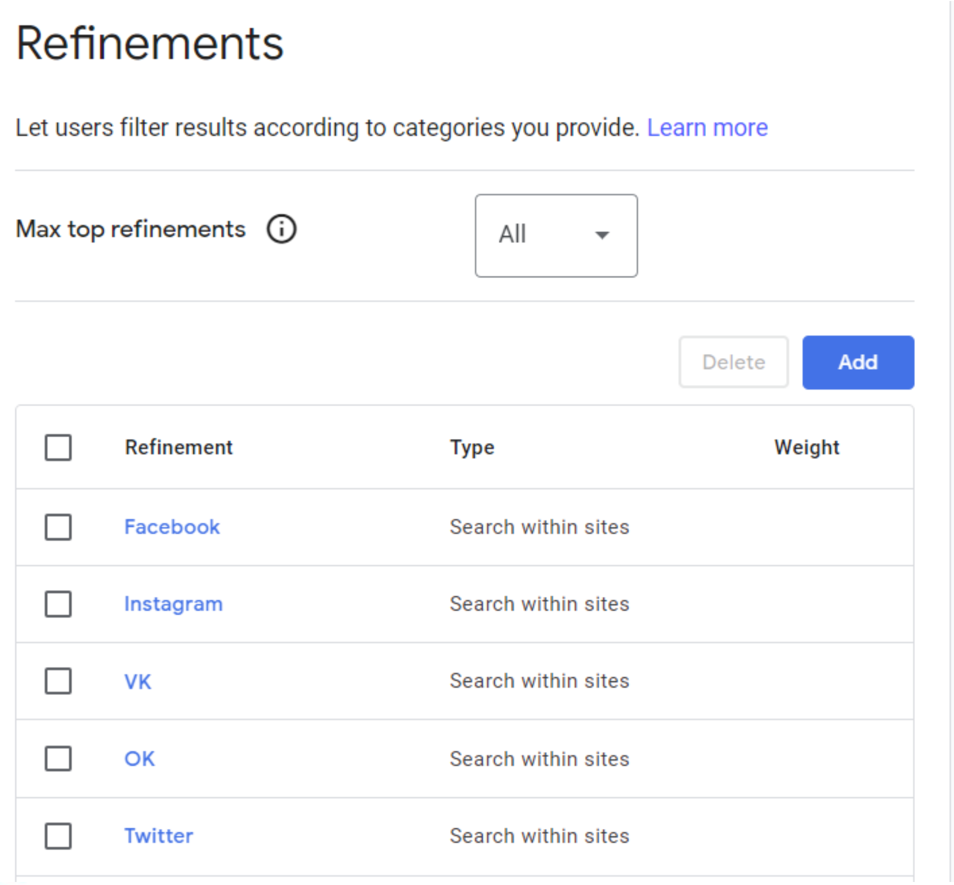


Search engine name	Filetypes on Google
Description	Add description
Code	Get code
Search engine ID	c6a2d8e0ca3054533
Public URL	https://cse.google.com/cse?cx=c6a2d8e0ca3054533

Search Features

Search settings
- ○ Image search
- ○ SafeSearch

Augment results
- ● Search the entire web



Refinements

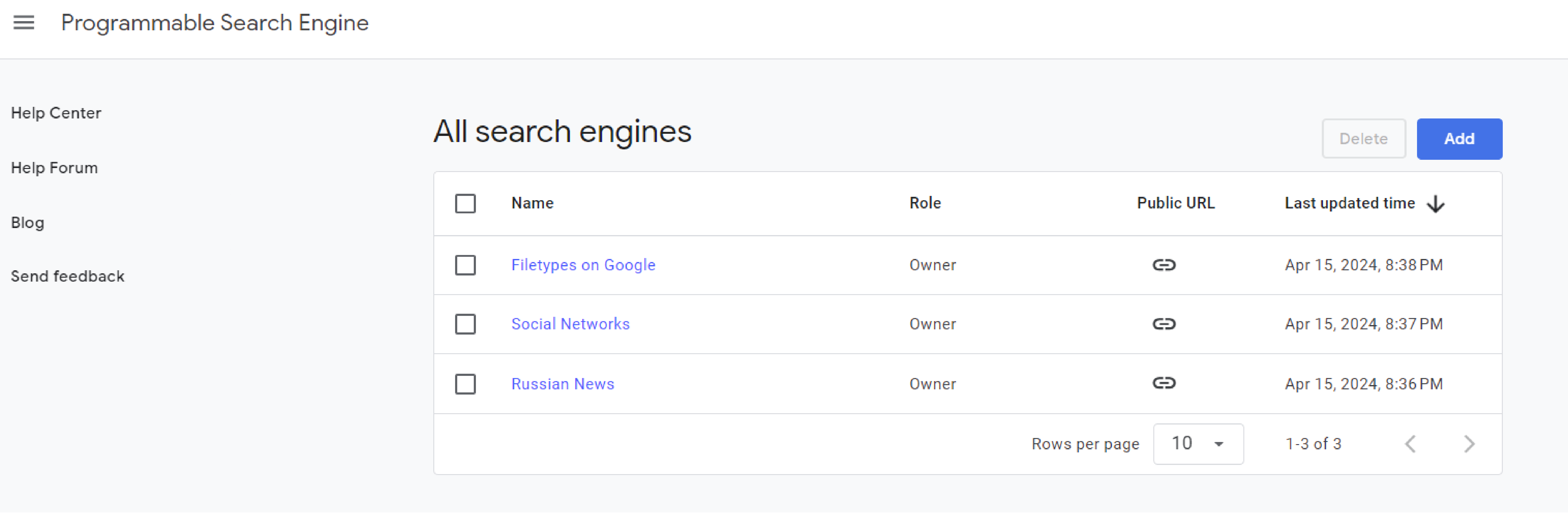
Let users filter results according to categories you provide. Learn more

Max top refinements: All

□	Refinement	Type	Weight
□	Facebook	Search within sites	
□	Instagram	Search within sites	
□	VK	Search within sites	
□	OK	Search within sites	
□	Twitter	Search within sites	

Google Custom Search

- CSE (PSE) makes repeated, targeted searches more efficient

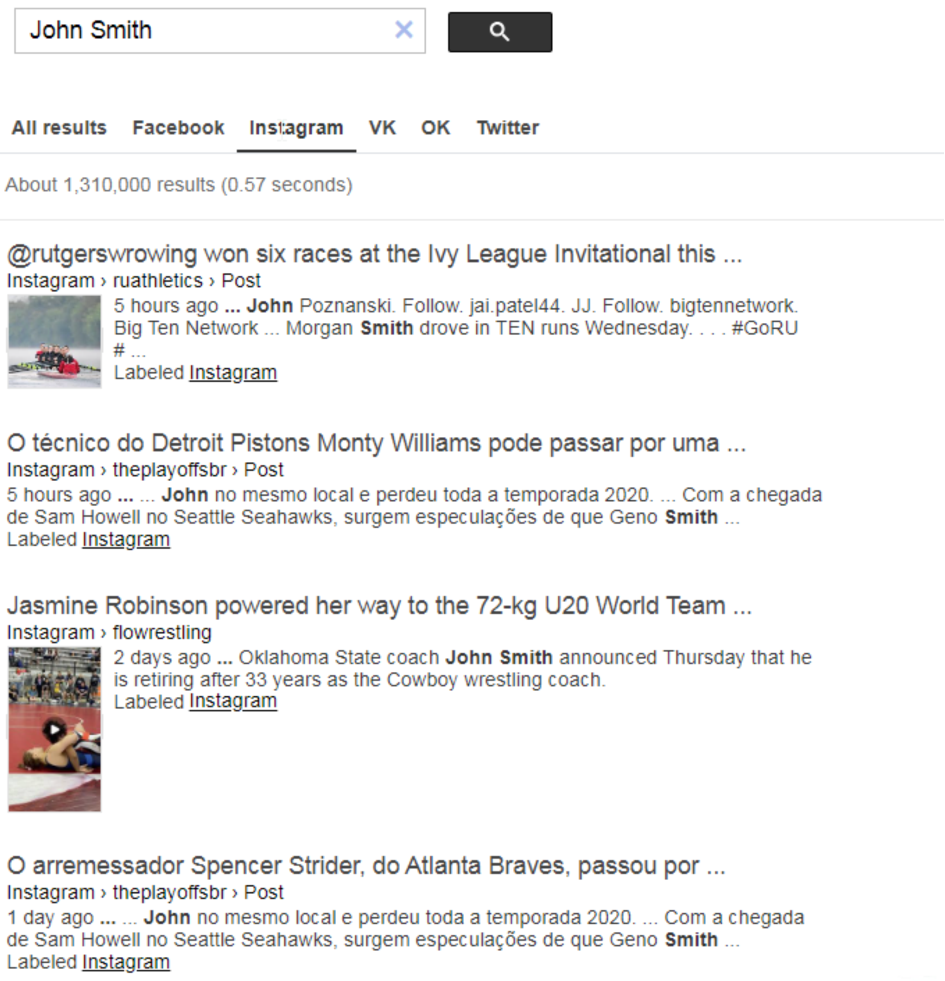


All search engines

□	Name	Role	Public URL	Last updated time ↓
□	Filetypes on Google	Owner	🔗	Apr 15, 2024, 8:38 PM
□	Social Networks	Owner	🔗	Apr 15, 2024, 8:37 PM
□	Russian News	Owner	🔗	Apr 15, 2024, 8:36 PM

Google Custom Search

- Final CSEs can be conveniently used



John Smith

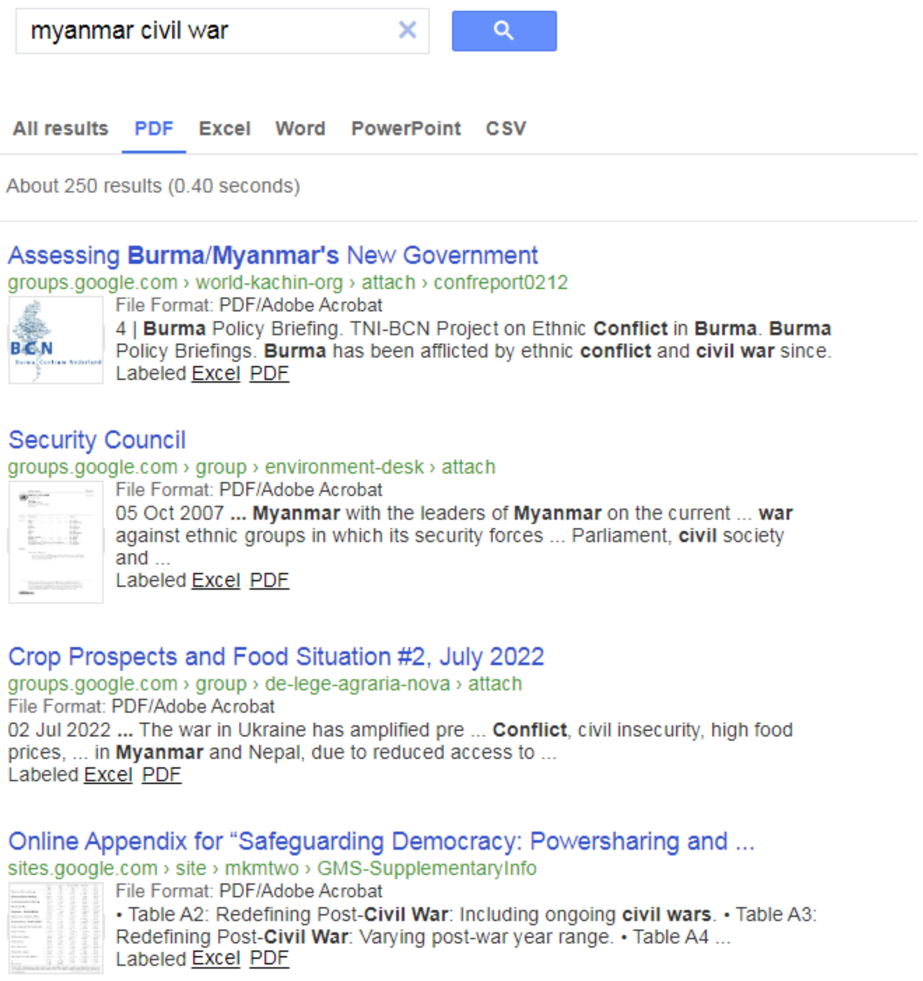
About 1,310,000 results (0.57 seconds)

@rutgerswrowing won six races at the Ivy League Invitational this ...
Instagram › ruathletics › Post
5 hours ago ... **John** Poznanski. Follow. jai.patel44. JJ. Follow. bigtennetwork. Big Ten Network ... Morgan **Smith** drove in TEN runs Wednesday. . . . #GoRU # ...
Labeled Instagram

O técnico do Detroit Pistons Monty Williams pode passar por uma ...
Instagram › theplayoffsbr › Post
5 hours ago ... ... **John** no mesmo local e perdeu toda a temporada 2020. ... Com a chegada de Sam Howell no Seattle Seahawks, surgem especulações de que Geno **Smith** ...
Labeled Instagram

Jasmine Robinson powered her way to the 72-kg U20 World Team ...
Instagram › flowrestling
2 days ago ... Oklahoma State coach **John Smith** announced Thursday that he is retiring after 33 years as the Cowboy wrestling coach.
Labeled Instagram

O arremessador Spencer Strider, do Atlanta Braves, passou por ...
Instagram › theplayoffsbr › Post
1 day ago ... ... **John** no mesmo local e perdeu toda a temporada 2020. ... Com a chegada de Sam Howell no Seattle Seahawks, surgem especulações de que Geno **Smith** ...
Labeled Instagram



myanmar civil war

About 250 results (0.40 seconds)

Assessing **Burma**/**Myanmar's** New Government
groups.google.com › world-kachin-org › attach › confreport0212
File Format: PDF/Adobe Acrobat
4 | **Burma** Policy Briefing. TNI-BCN Project on Ethnic **Conflict** in **Burma**. **Burma** Policy Briefings. **Burma** has been afflicted by ethnic **conflict** and **civil war** since.
Labeled Excel PDF

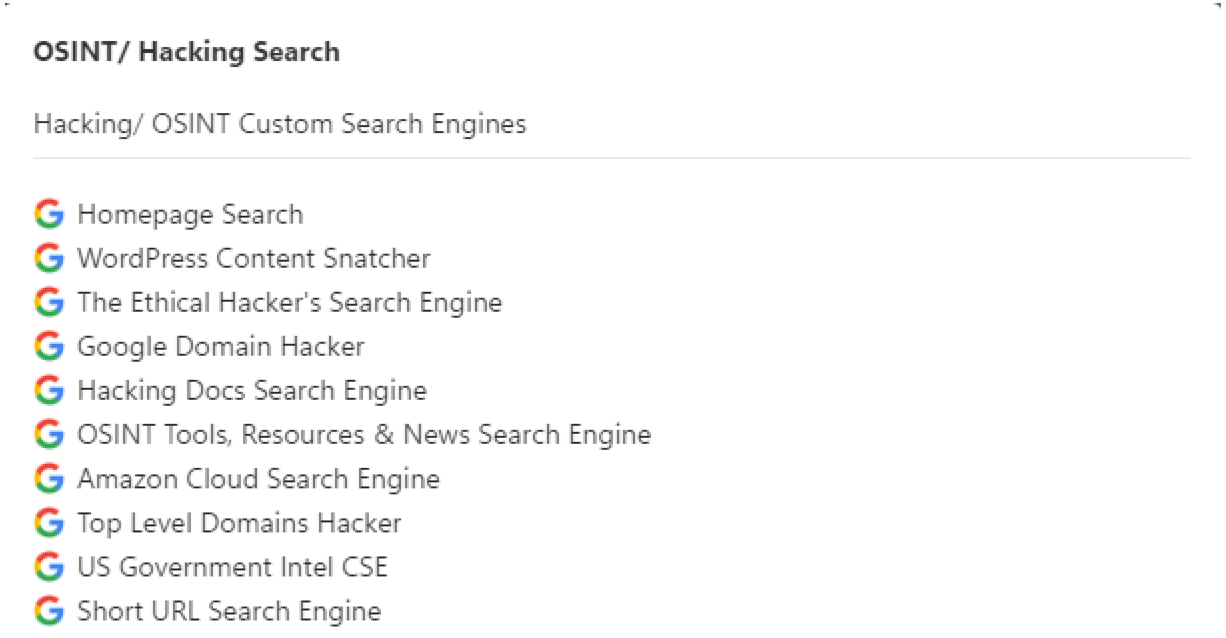
Security Council
groups.google.com › group › environment-desk › attach
File Format: PDF/Adobe Acrobat
05 Oct 2007 ... **Myanmar** with the leaders of **Myanmar** on the current ... **war** against ethnic groups in which its security forces ... Parliament, **civil** society and ...
Labeled Excel PDF

Crop Prospects and Food Situation #2, July 2022
groups.google.com › group › de-lege-agraria-nova › attach
File Format: PDF/Adobe Acrobat
02 Jul 2022 ... The war in Ukraine has amplified pre ... **Conflict**, civil insecurity, high food prices, ... in **Myanmar** and Nepal, due to reduced access to ...
Labeled Excel PDF

Online Appendix for “Safeguarding Democracy: Powersharing and ...
sites.google.com › site › mkmtwo › GMS-SupplementaryInfo
File Format: PDF/Adobe Acrobat
• Table A2: Redefining Post-**Civil War**: Including ongoing **civil wars**. • Table A3: Redefining Post-**Civil War**: Varying post-war year range. • Table A4 ...
Labeled Excel PDF

Google Custom Search

- Additional resources:
  - https://start.me/p/EL84Km/cse-utopia
  - https://www.osintme.com/index.php/2020/09/28/using-the-google-custom-search-engine-for-osint/



OSINT/ Hacking Search

Hacking/ OSINT Custom Search Engines

- Homepage Search
- WordPress Content Snatcher
- The Ethical Hacker's Search Engine
- Google Domain Hacker
- Hacking Docs Search Engine
- OSINT Tools, Resources & News Search Engine
- Amazon Cloud Search Engine
- Top Level Domains Hacker
- US Government Intel CSE
- Short URL Search Engine

Reverse image search

How is this useful?

- In general OSINT investigation, pictures and in general media are extremely powerful!
  - Picture tells the story of thousand words!
- Just by observing a picture, we can find out a lot of information
- In many cases we have to rely on our intuition and observe details
- Questions that can be answered
  - Who is in the media?
  - When was it taken?
  - Where was it taken?
  - Event pictures
  - Information on a location or environment/situation

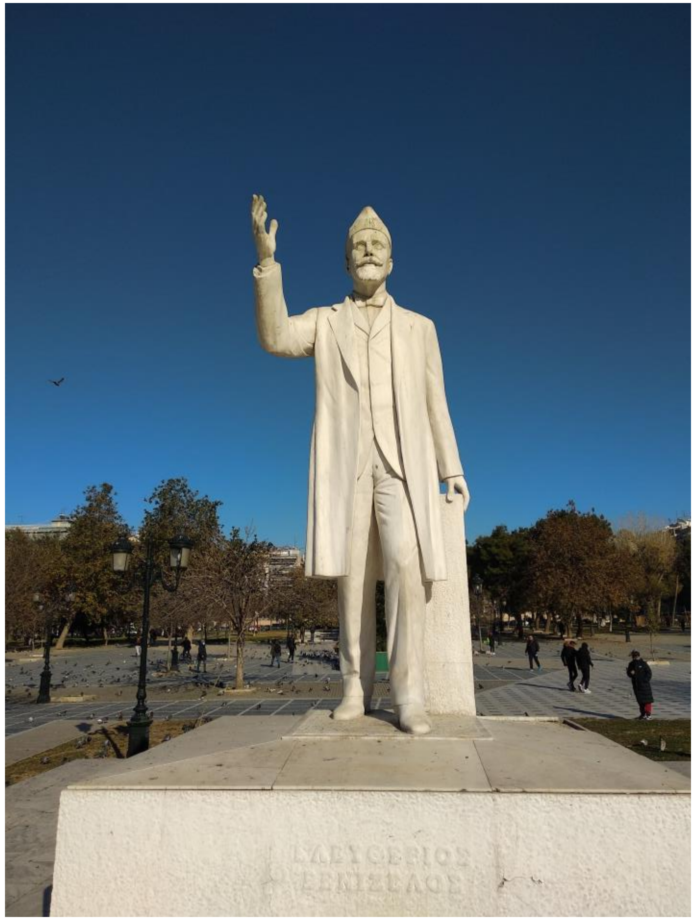
Reverse image search

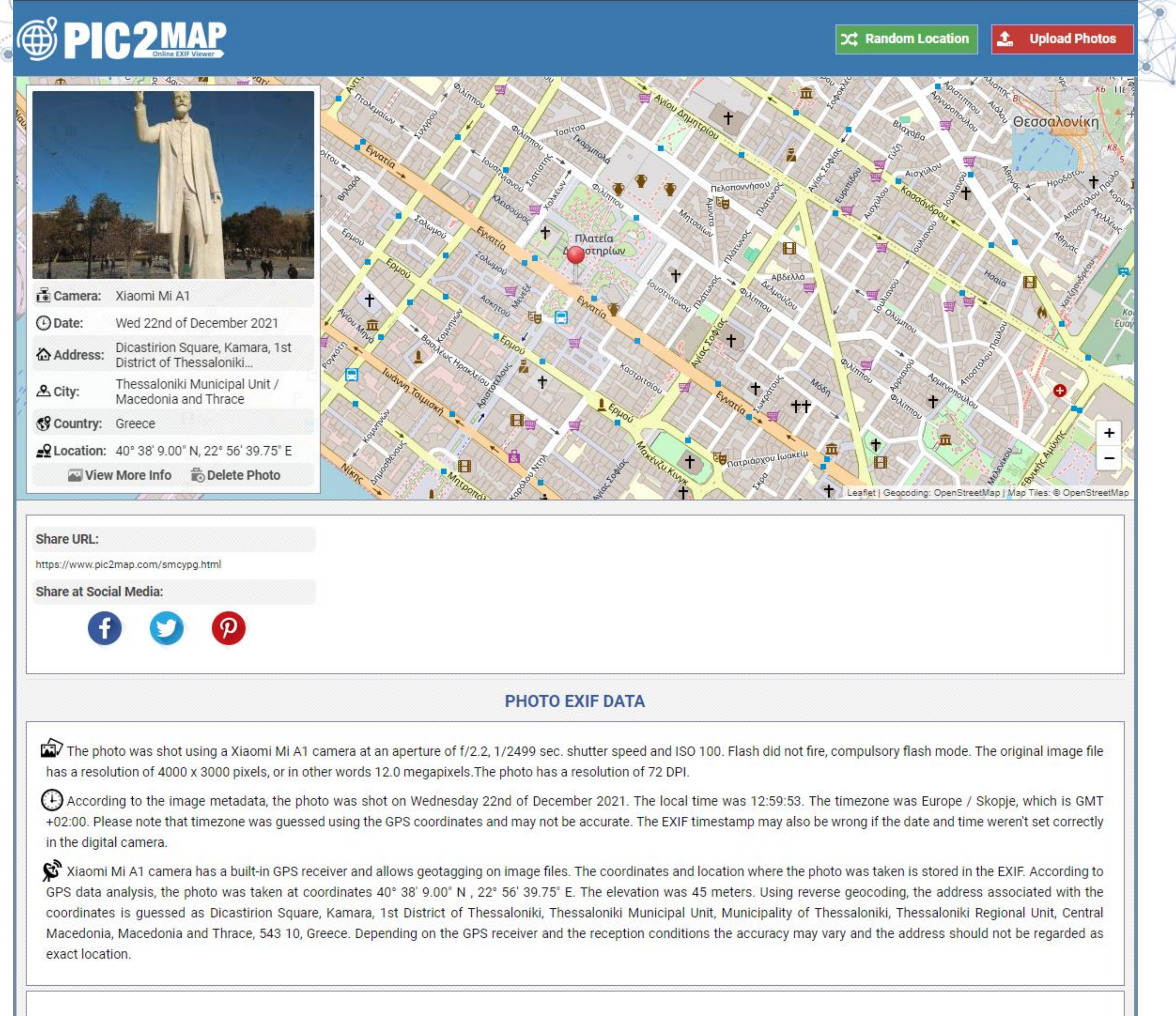
- **Exchangeable Image File** (EXIF) is a standard that specifies the format for storing interchange information of images that use JPEG compression by digital cameras, smartphones…

- EXIF stores information such as:
  - Shutter speed
  - Exposure
  - Compression
  - Metering system that was used
  - ISO number
  - Date and time when the image was taken
  - GPS information

Exercise (EXIF data analysis)

- Use Pic2map website to find information:
  - IMG_20211222_125953.jpg





Camera:	Xiaomi Mi A1
Date:	Wed 22nd of December 2021
Address:	Dicastirion Square, Kamara, 1st District of Thessaloniki...
City:	Thessaloniki Municipal Unit / Macedonia and Thrace
Country:	Greece
Location:	40° 38' 9.00" N, 22° 56' 39.75" E

Share URL:

https://www.pic2map.com/smcypg.html

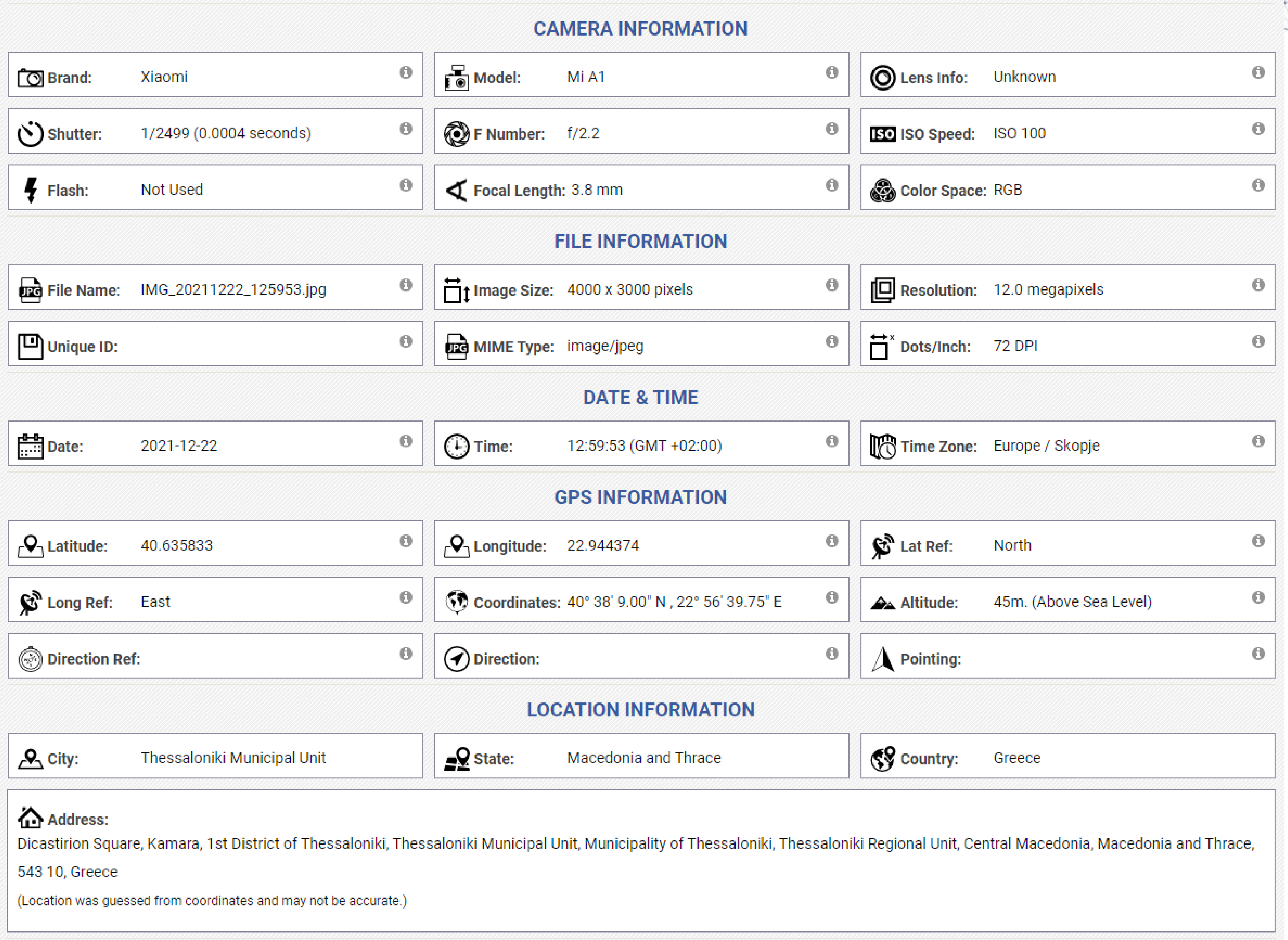
Share at Social Media:

PHOTO EXIF DATA

The photo was shot using a Xiaomi Mi A1 camera at an aperture of f/2.2, 1/2499 sec. shutter speed and ISO 100. Flash did not fire, compulsory flash mode. The original image file has a resolution of 4000 x 3000 pixels, or in other words 12.0 megapixels.The photo has a resolution of 72 DPI.

According to the image metadata, the photo was shot on Wednesday 22nd of December 2021. The local time was 12:59:53. The timezone was Europe / Skopje, which is GMT +02:00. Please note that timezone was guessed using the GPS coordinates and may not be accurate. The EXIF timestamp may also be wrong if the date and time weren't set correctly in the digital camera.

Xiaomi Mi A1 camera has a built-in GPS receiver and allows geotagging on image files. The coordinates and location where the photo was taken is stored in the EXIF. According to GPS data analysis, the photo was taken at coordinates 40° 38' 9.00" N , 22° 56' 39.75" E. The elevation was 45 meters. Using reverse geocoding, the address associated with the coordinates is guessed as Dicastirion Square, Kamara, 1st District of Thessaloniki, Thessaloniki Municipal Unit, Municipality of Thessaloniki, Thessaloniki Regional Unit, Central Macedonia, Macedonia and Thrace, 543 10, Greece. Depending on the GPS receiver and the reception conditions the accuracy may vary and the address should not be regarded as exact location.



CAMERA INFORMATION

Brand:	Xiaomi	Model:	Mi A1	Lens Info:	Unknown
Shutter:	1/2499 (0.0004 seconds)	F Number:	f/2.2	ISO Speed:	ISO 100
Flash:	Not Used	Focal Length:	3.8 mm	Color Space:	RGB

FILE INFORMATION

File Name:	IMG_20211222_125953.jpg	Image Size:	4000 x 3000 pixels	Resolution:	12.0 megapixels
Unique ID:		MIME Type:	image/jpeg	Dots/Inch:	72 DPI

DATE & TIME

Date:	2021-12-22	Time:	12:59:53 (GMT +02:00)	Time Zone:	Europe / Skopje

GPS INFORMATION

Latitude:	40.635833	Longitude:	22.944374	Lat Ref:	North
Long Ref:	East	Coordinates:	40° 38' 9.00" N , 22° 56' 39.75" E	Altitude:	45m. (Above Sea Level)
Direction Ref:		Direction:		Pointing:	

LOCATION INFORMATION

City:	Thessaloniki Municipal Unit	State:	Macedonia and Thrace	Country:	Greece

Address:
Dicastirion Square, Kamara, 1st District of Thessaloniki, Thessaloniki Municipal Unit, Municipality of Thessaloniki, Thessaloniki Regional Unit, Central Macedonia, Macedonia and Thrace, 543 10, Greece

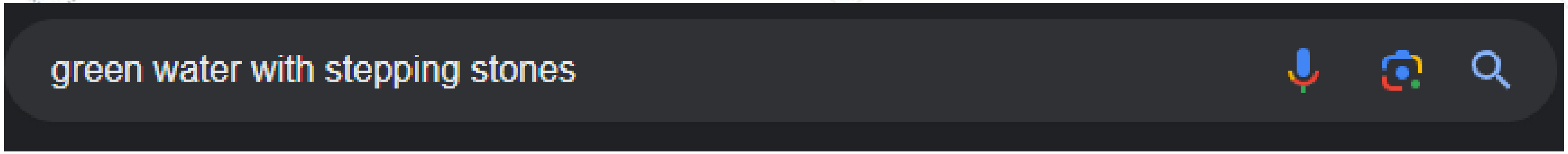
(Location was guessed from coordinates and may not be accurate.)

Reverse image search

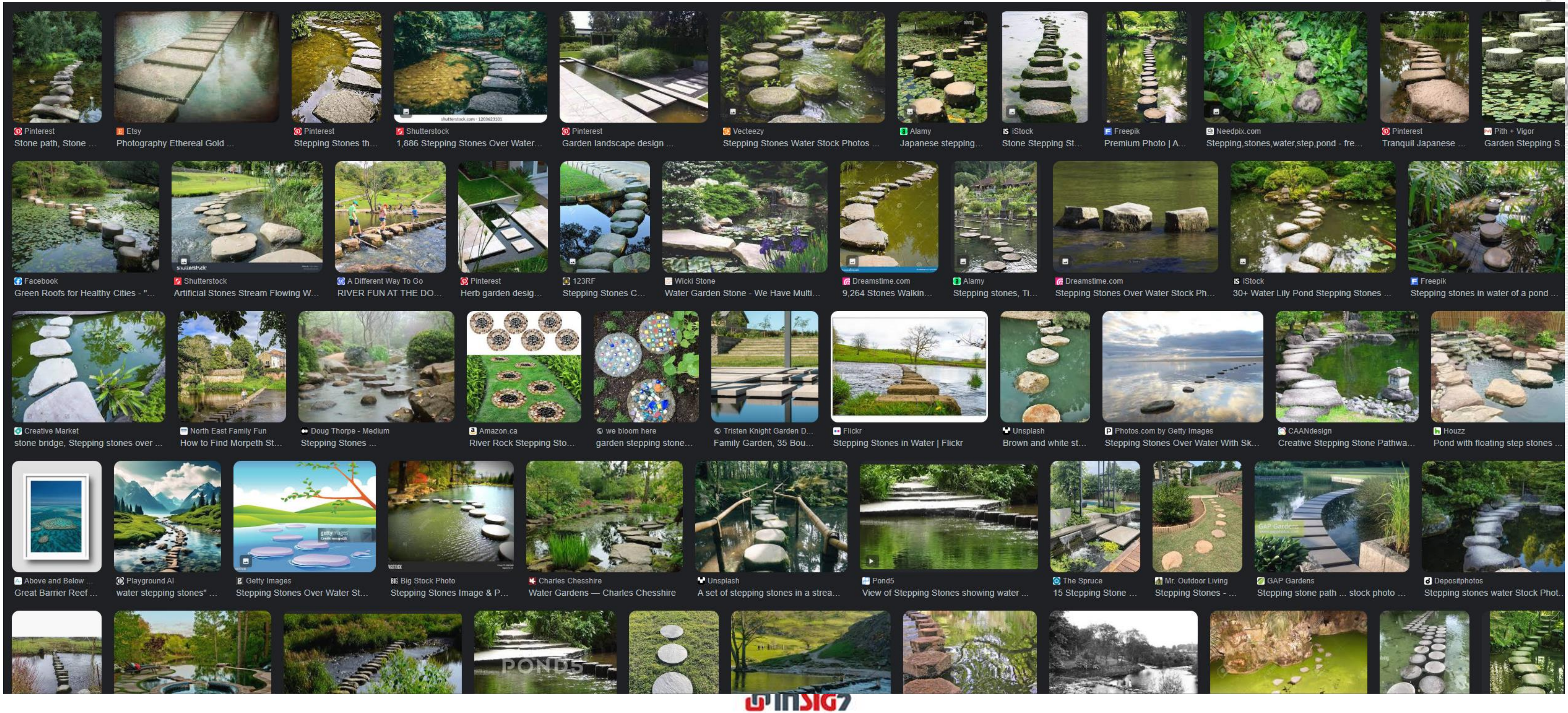
- Takes an image file as an input query and returns results related to the image

- Search by Image – browser extension
- Google Images – https://www.google.com/imghp?hl=en
- Yandex Images – https://yandex.com/images/
- Flickr Image Search – https://www.flickr.com/search/
- Shutterstock – https://www.shutterstock.com/
- Getty Images – https://www.gettyimages.co.uk/
- Tin Eye – https://tineye.com/

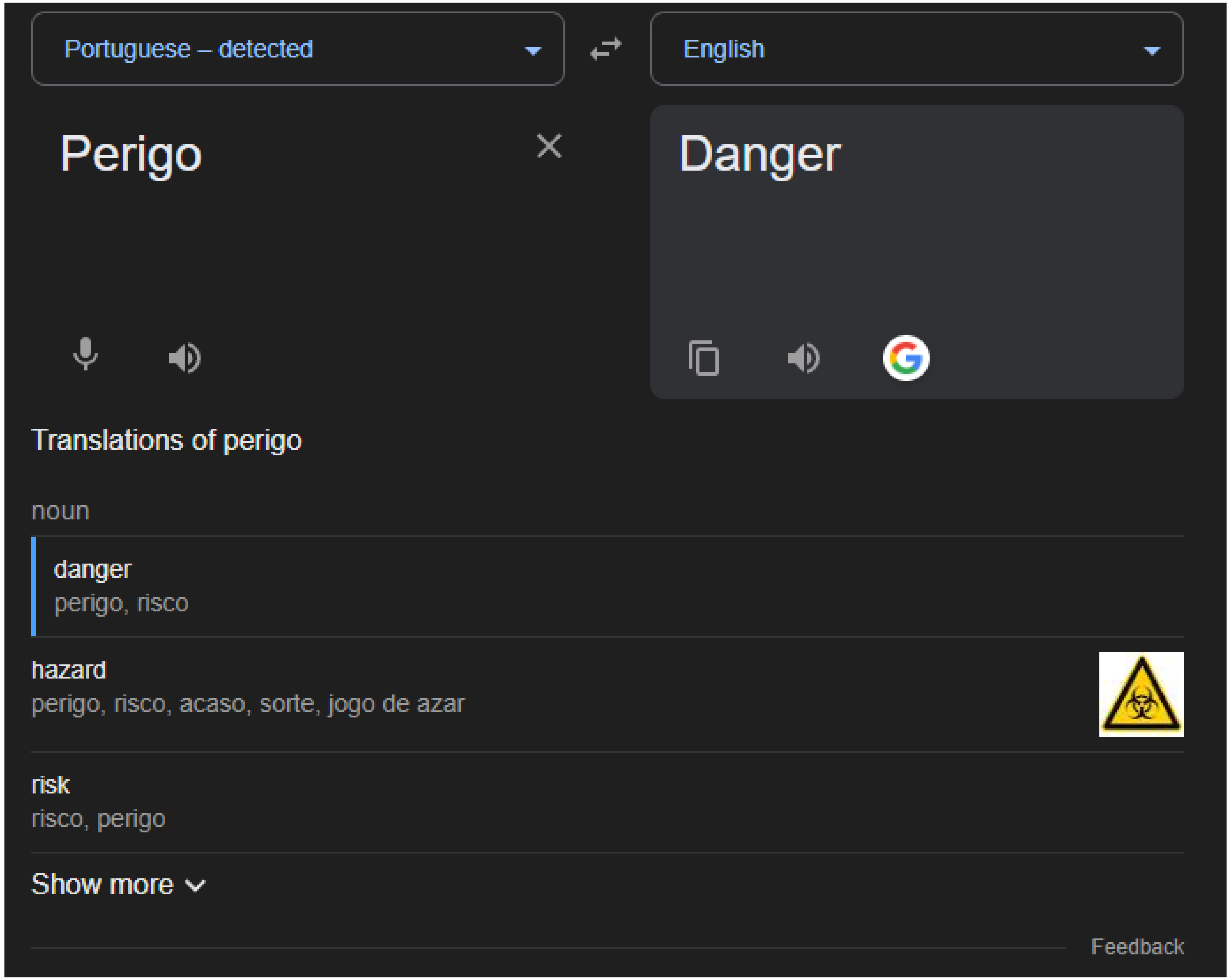
Regular location search



green water with stepping stones


Pinterest
Stone path, Stone ...
Etsy
Photography Ethereal Gold ...
Pinterest
Stepping Stones th...
Shutterstock
1,886 Stepping Stones Over Water...
Pinterest
Garden landscape design ...
Vecteezy
Stepping Stones Water Stock Photos ...
Alamy
Japanese stepping...
iStock
Stone Stepping St...
Freepik
Premium Photo | A...
Needpix.com
Stepping,stones,water,step,pond - fre...
Pinterest
Tranquil Japanese ...
Pith + Vigor
Garden Stepping S...
Facebook
Green Roofs for Healthy Cities - "...
Shutterstock
Artificial Stones Stream Flowing W...
A Different Way To Go
RIVER FUN AT THE DO...
Pinterest
Herb garden desig...
123RF
Stepping Stones C...
Wicki Stone
Water Garden Stone - We Have Multi...
Dreamstime.com
9,264 Stones Walkin...
Alamy
Stepping stones, Ti...
Dreamstime.com
Stepping Stones Over Water Stock Ph...
iStock
30+ Water Lily Pond Stepping Stones ...
Freepik
Stepping stones in water of a pond ...
Creative Market
stone bridge, Stepping stones over ...
North East Family Fun
How to Find Morpeth St...
Doug Thorpe - Medium
Stepping Stones ...
Amazon.ca
River Rock Stepping Sto...
we bloom here
garden stepping stone...
Tristen Knight Garden D...
Family Garden, 35 Bou...
Flickr
Stepping Stones in Water | Flickr
Unsplash
Brown and white st...
Photos.com by Getty Images
Stepping Stones Over Water With Sk...
CAANdesign
Creative Stepping Stone Pathwa...
Houzz
Pond with floating step stones ...
Above and Below ...
Great Barrier Reef ...
Playground AI
water stepping stones" ...
Getty Images
Stepping Stones Over Water St...
Big Stock Photo
Stepping Stones Image & P...
Charles Chesshire
Water Gardens — Charles Chesshire
Unsplash
A set of stepping stones in a strea...
Pond5
View of Stepping Stones showing water ...
The Spruce
15 Stepping Stone ...
Mr. Outdoor Living
Stepping Stones - ...
GAP Gardens
Stepping stone path ... stock photo ...
Depositphotos
Stepping stones water Stock Phot...

PERIGO
Cuidado ao
(profundida
Take care when



Portuguese – detected

English

Perigo

Danger

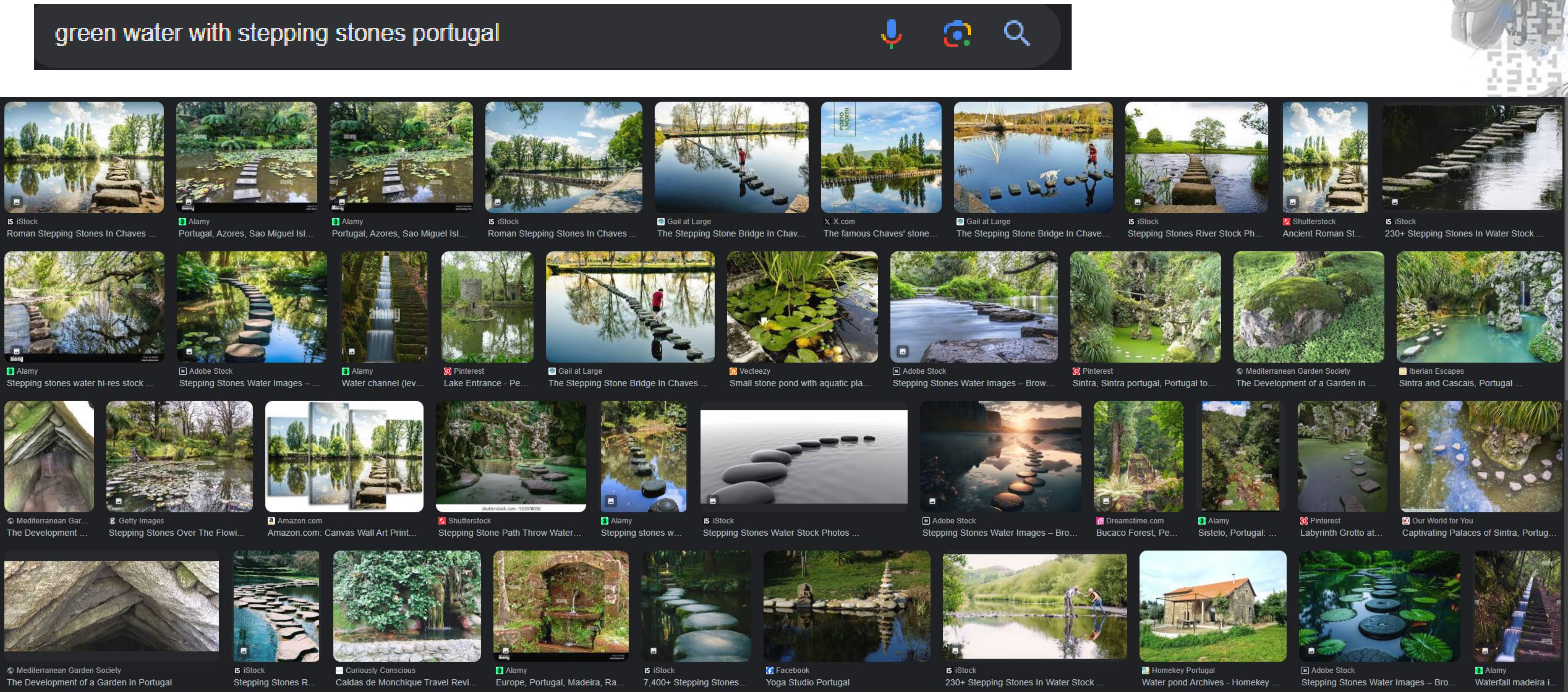
Translations of perigo

noun

danger	perigo, risco
hazard	perigo, risco, acaso, sorte, jogo de azar
risk	risco, perigo

Show more

Feedback



green water with stepping stones portugal

iStock
Roman Stepping Stones In Chaves ...

Alamy
Portugal, Azores, Sao Miguel Isl...

Alamy
Portugal, Azores, Sao Miguel Isl...

iStock
Roman Stepping Stones In Chaves ...

Gail at Large
The Stepping Stone Bridge In Chav...

X.com
The famous Chaves' stone...

Gail at Large
The Stepping Stone Bridge In Chave...

iStock
Stepping Stones River Stock Ph...

Shutterstock
Ancient Roman St...

iStock
230+ Stepping Stones In Water Stock ...

Alamy
Stepping stones water hi-res stock ...

Adobe Stock
Stepping Stones Water Images – ...

Alamy
Water channel (lev...

Pinterest
Lake Entrance - Pe...

Gail at Large
The Stepping Stone Bridge In Chaves ...

Vecteezy
Small stone pond with aquatic pla...

Adobe Stock
Stepping Stones Water Images – Brow...

Pinterest
Sintra, Sintra portugal, Portugal to...

Mediterranean Garden Society
The Development of a Garden in ...

Iberian Escapes
Sintra and Cascais, Portugal ...

Mediterranean Gar...
The Development ...

Getty Images
Stepping Stones Over The Flowi...

Amazon.com
Amazon.com: Canvas Wall Art Print...

Shutterstock
Stepping Stone Path Throw Water...

Alamy
Stepping stones w...

iStock
Stepping Stones Water Stock Photos ...

Adobe Stock
Stepping Stones Water Images – Bro...

Dreamstime.com
Bucaco Forest, Pe...

Alamy
Sistelo, Portugal: ...

Pinterest
Labyrinth Grotto at...

Our World for You
Captivating Palaces of Sintra, Portug...

Mediterranean Garden Society
The Development of a Garden in Portugal

iStock
Stepping Stones R...

Curiously Conscious
Caldas de Monchique Travel Revi...

Alamy
Europe, Portugal, Madeira, Ra...

iStock
7,400+ Stepping Stones...

Facebook
Yoga Studio Portugal

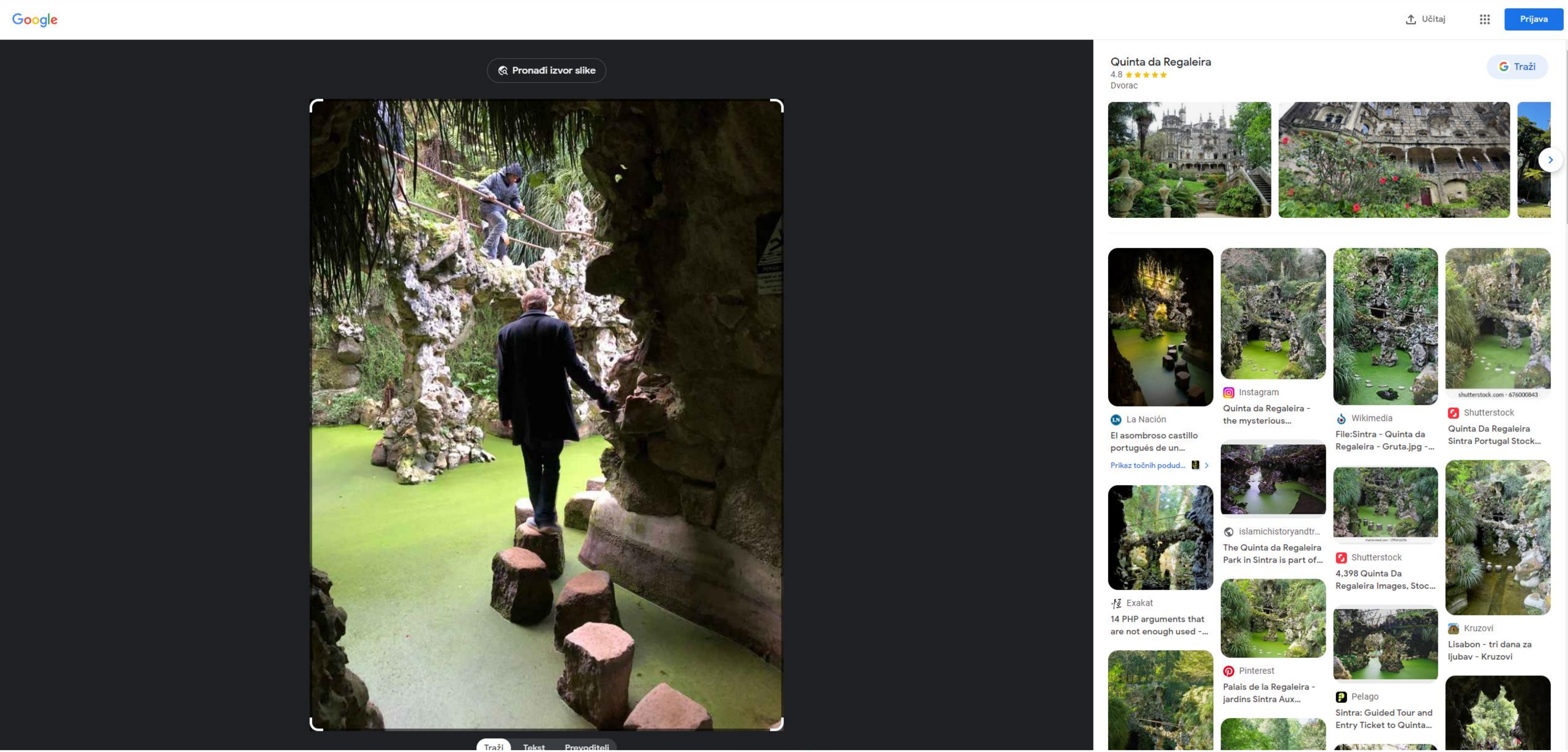
iStock
230+ Stepping Stones In Water Stock ...

Homekey Portugal
Water pond Archives - Homekey ...

Adobe Stock
Stepping Stones Water Images – Bro...

Alamy
Waterfall madeira i...

Reverse image search



Google

Učitaj

Prijava

Pronađi izvor slike

Traži Tekst Prevoditelj

Quinta da Regaleira
4.8 ★★★★★
Dvorac

Traži

La Nación
El asombroso castillo portugués de un...
Prikaz točnih podud...

Exakat
14 PHP arguments that are not enough used -...

Instagram
Quinta da Regaleira - the mysterious...

islamichistoryandtr...
The Quinta da Regaleira Park in Sintra is part of...

Pinterest
Palais de la Regaleira - jardins Sintra Aux...

Wikimedia
File:Sintra - Quinta da Regaleira - Gruta.jpg -...

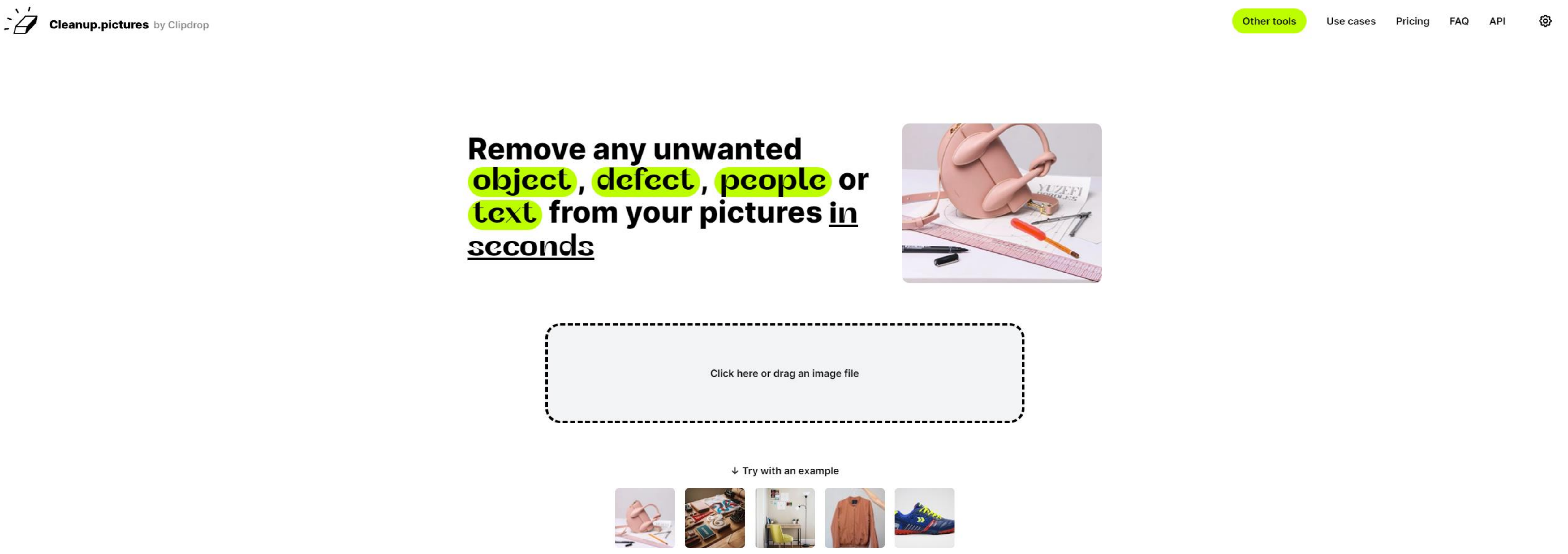
Shutterstock
4,398 Quinta Da Regaleira Images, Stoc...

Pelago
Sintra: Guided Tour and Entry Ticket to Quinta...

Shutterstock
Quinta Da Regaleira Sintra Portugal Stock...

Kruzovi
Lisabon - tri dana za ljubav - Kruzovi

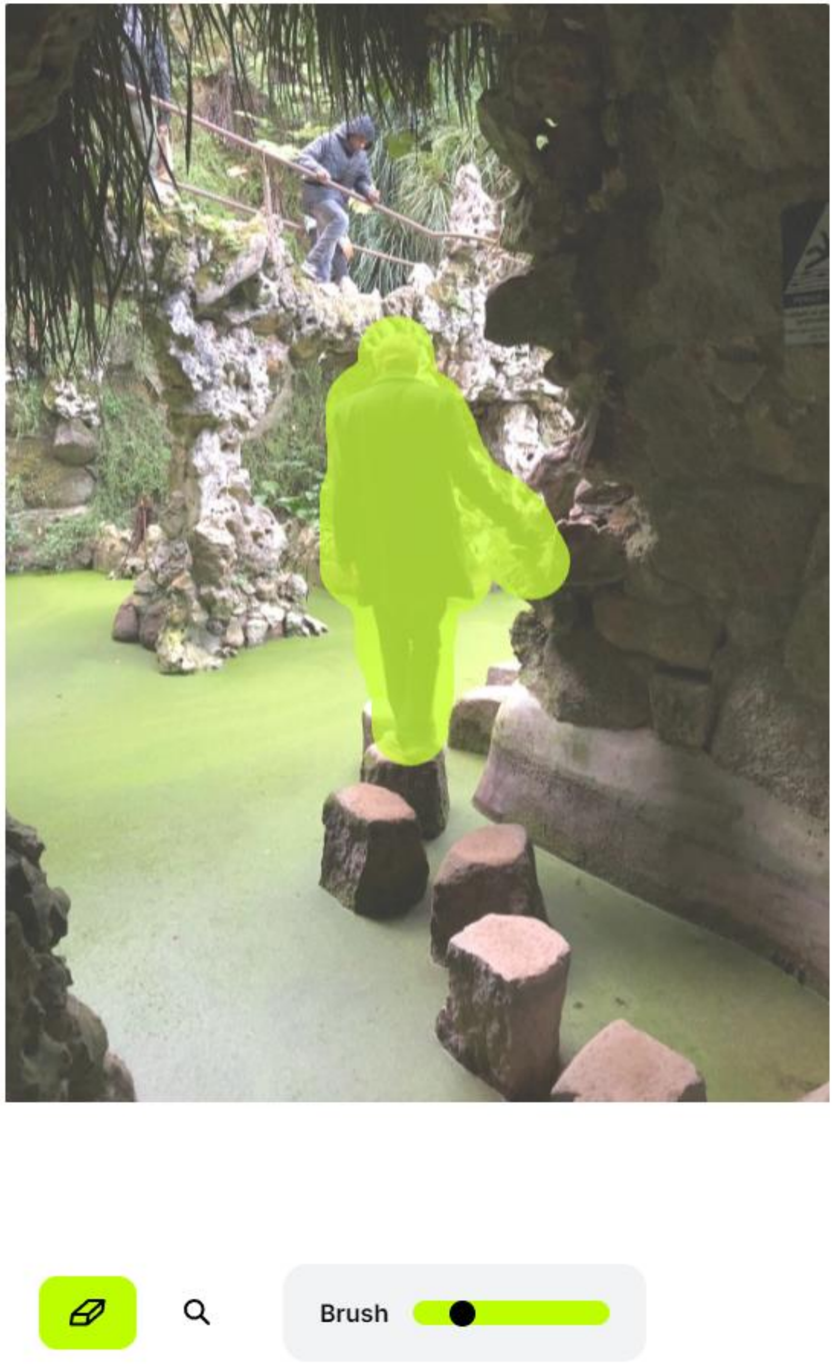
Reverse image search

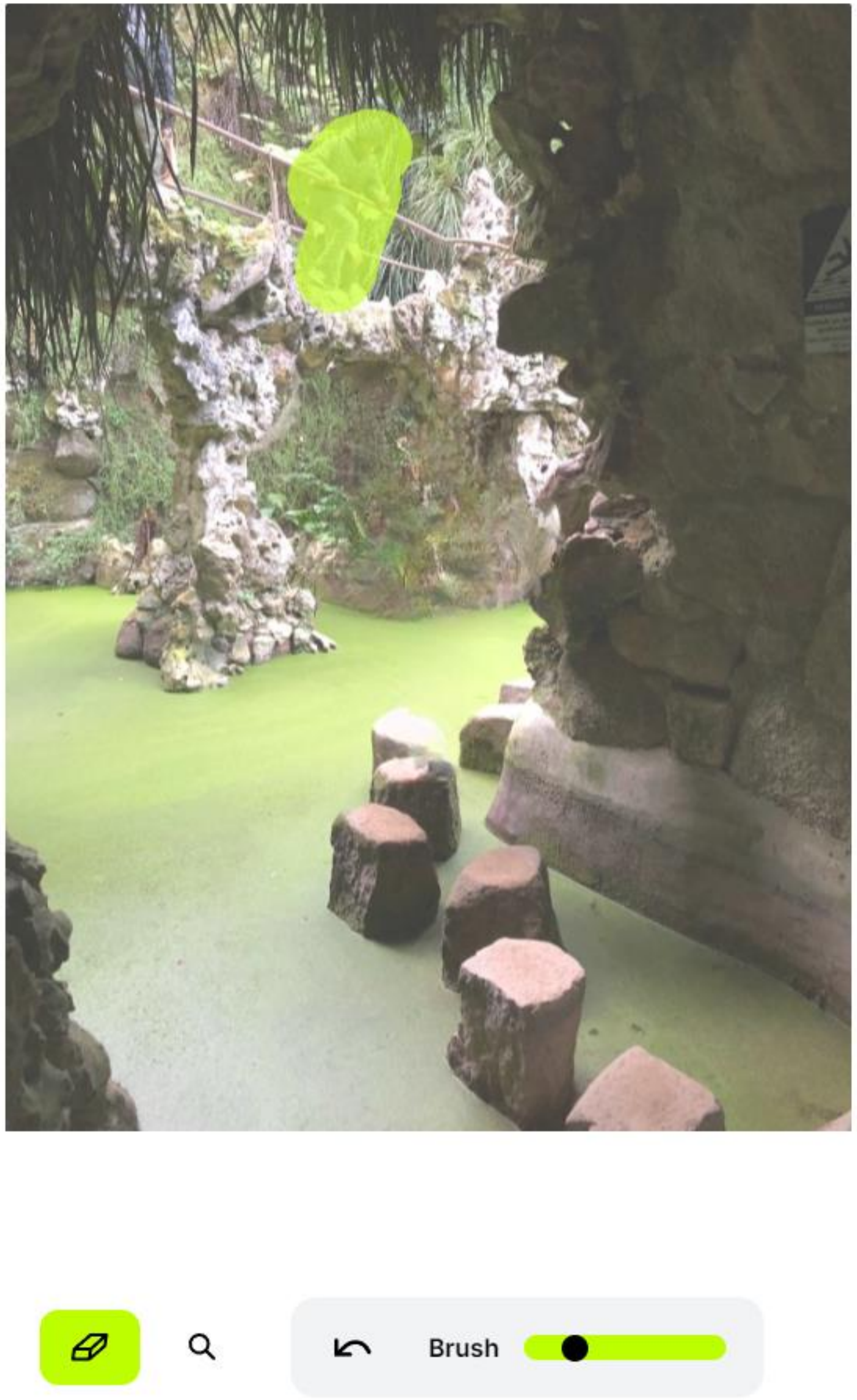


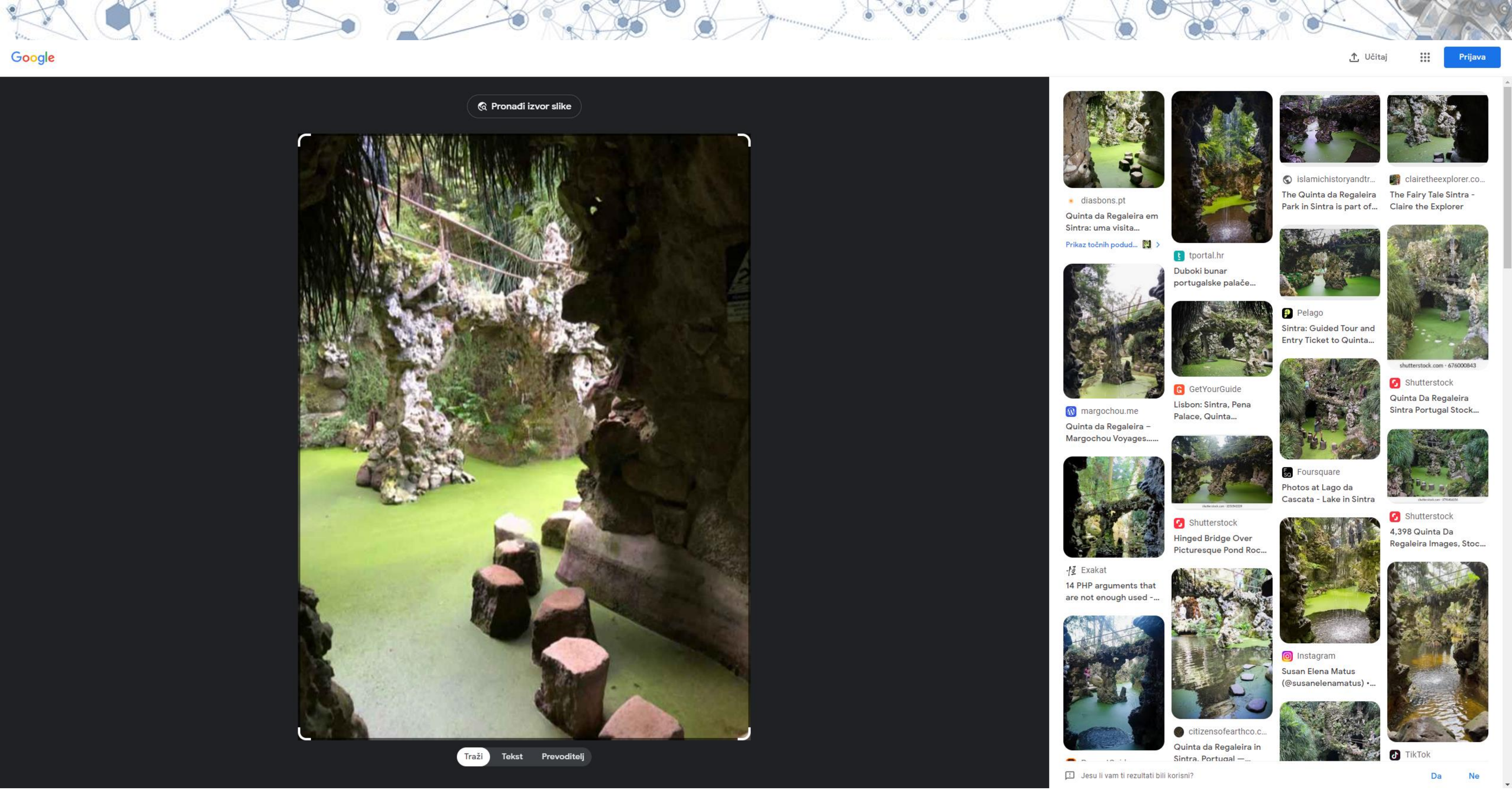
Cleanup.pictures by Clipdrop
Other tools
Use cases
Pricing
FAQ
API

Remove any unwanted object, defect, people or text from your pictures in seconds

Click here or drag an image file
↓ Try with an example


Brush


Brush



diasbons.pt
Quinta da Regaleira em Sintra: uma visita...
Prikaz točnih podud...

tportal.hr
Duboki bunar portugalske palače...

islamichistoryandtr...
The Quinta da Regaleira Park in Sintra is part of...

clairetheexplorer.co...
The Fairy Tale Sintra - Claire the Explorer

margochou.me
Quinta da Regaleira – Margochou Voyages...…

GetYourGuide
Lisbon: Sintra, Pena Palace, Quinta...

Pelago
Sintra: Guided Tour and Entry Ticket to Quinta...

Shutterstock
Quinta Da Regaleira Sintra Portugal Stock...

Foursquare
Photos at Lago da Cascata - Lake in Sintra

Exakat
14 PHP arguments that are not enough used -...

Shutterstock
Hinged Bridge Over Picturesque Pond Roc...

Shutterstock
4,398 Quinta Da Regaleira Images, Stoc...

Instagram
Susan Elena Matus (@susanelenamatus) •...

citizensofearthco.c...
Quinta da Regaleira in Sintra, Portugal —...

TikTok

Jesu li vam ti rezultati bili korisni?
Da
Ne

Thank you!

dario.vrckovic@insig2.com

INSIG2

Introduction to

Digital Evidence
ACPO
The Digital Forensic Process

M.Sc. Timothy De Groot, Belgian Federal Police

Co-funded by
the European Union

Possible Devices

- Computer, laptop
- Mobile devices (wearables, drones, etc.)
- External devices (USB, memory card, etc.)
- Network devices (routers, switches, etc.)
- Cloud
- Gaming consoles
- In-Vehicle systems (GPS devices, navigation systems)
- IoT devices (smart home, home appliances, etc.)
- Digital video recording systems
- …

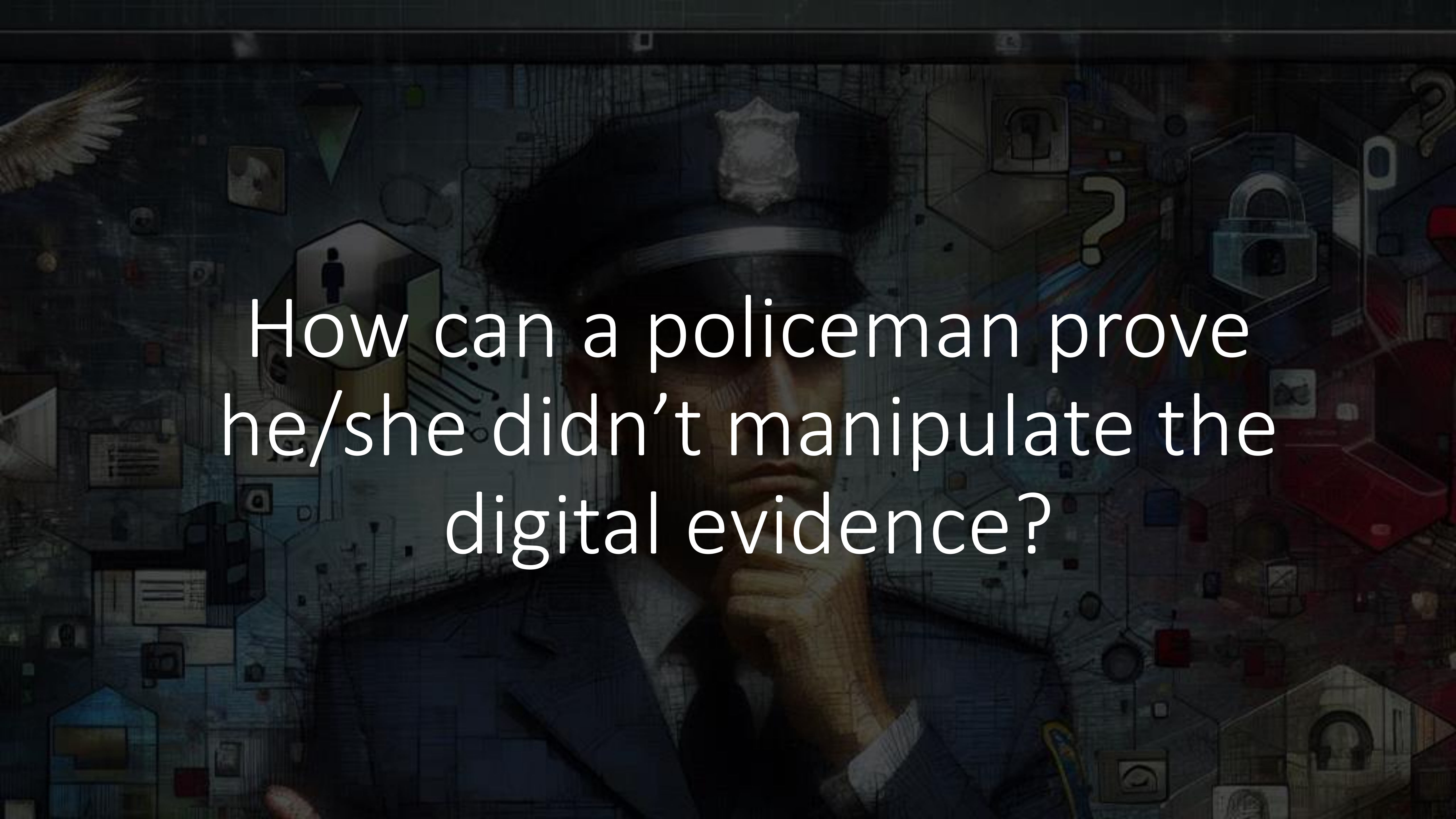
ACPO

- “**No action** taken by law enforcement agencies, or their **agents should change data** held on a computer or storage media which may subsequently be relied upon in court”

- “In circumstances where a person finds **it necessary to access original data** held on a computer or on storage media, that **person must be competent** to do so and be able to give evidence **explaining** the **relevance** and the **implications** of their actions”

- “An **audit trail** or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent **third party should be able to examine** those processes and achieve the same result”

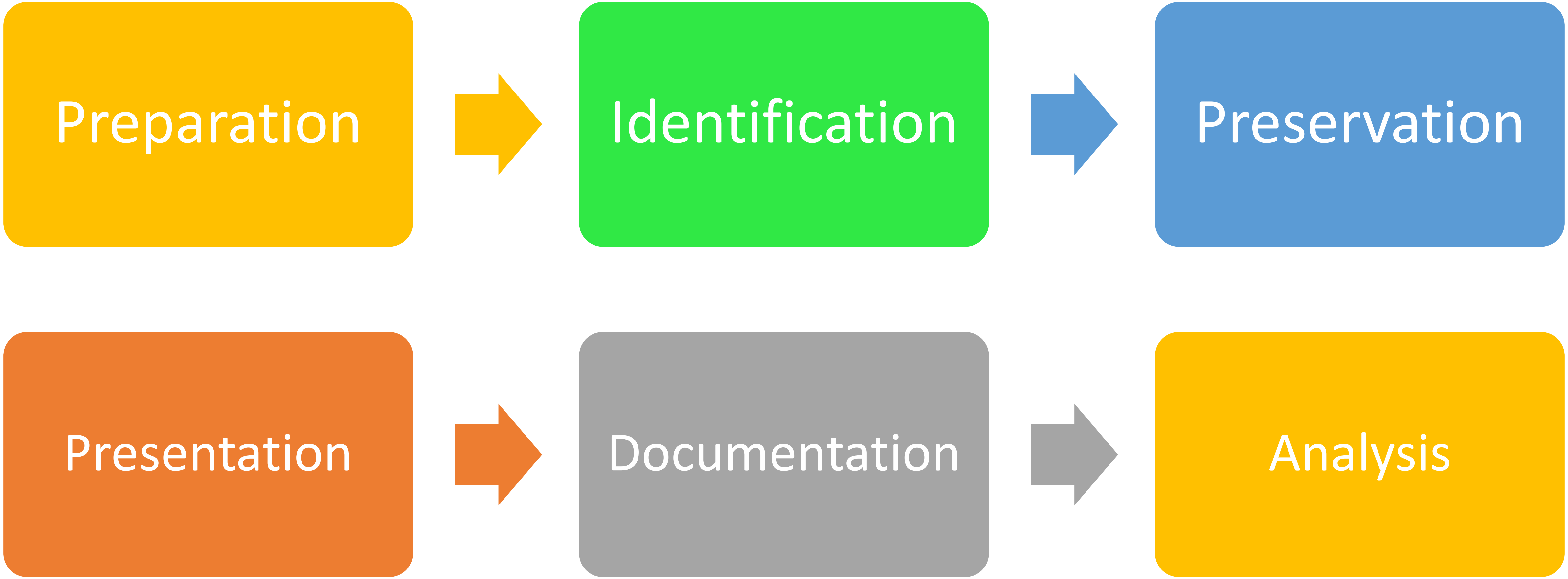
- “The **person in charge** of the investigation (the case officer) has **overall responsibility** for ensuring that the law and these principles are adhered to”



How can a policeman prove he/she didn’t manipulate the digital evidence?

PRINCIPLES

Principles



Preparation

Identification

Preservation

Presentation

Documentation

Analysis

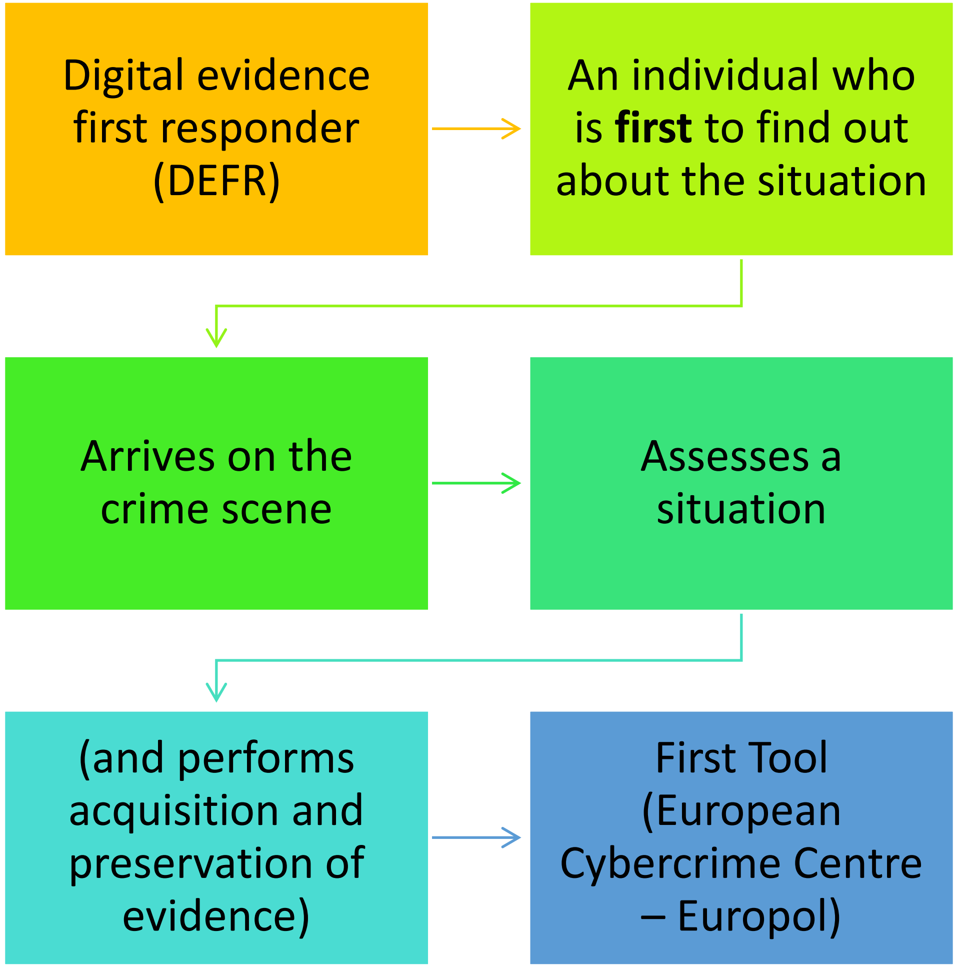
Preparation

- Purpose of investigation?
- What digital evidence do you expect to find?
- Home or office? – Administrator?
- Is there a network?
- Cloud storage utilized?
- Search Warrant?

Identification

- The act of searching
- **Detecting** & **documenting** (digital) evidence
- DEFR must examine all devices used in the action of crime

DEFR



Digital evidence first responder (DEFR)

An individual who is **first** to find out about the situation

Arrives on the crime scene

Assesses a situation

(and performs acquisition and preservation of evidence)

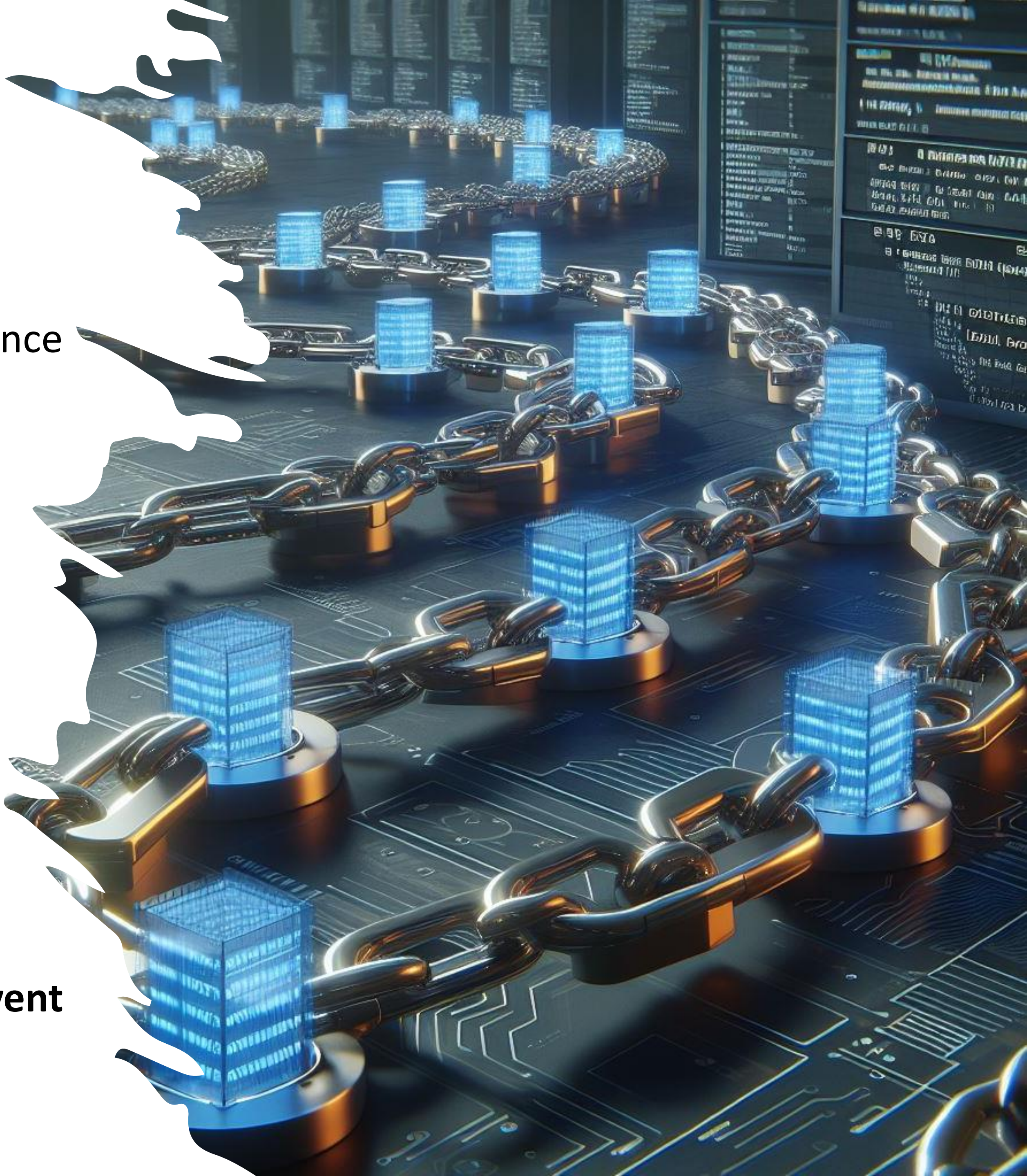
First Tool (European Cybercrime Centre – Europol)

Preservation

- Bag & Tag
- Transport
- Lab environment
- In-lab preservation

Chain Of Custody

- **Chronological** documentation of electronic evidence
- Indicates
  - the **collection**
  - **sequence** of control
  - **transfer**
  - **analysis**
- Includes documentation of:
  - Each **person** who **handled** the evidence
  - The **date/time** evidence was **collected** or **transferred**
  - The **purpose** of the transfer
- Preserving the **integrity** of the evidence and **prevent** it from **contamination**



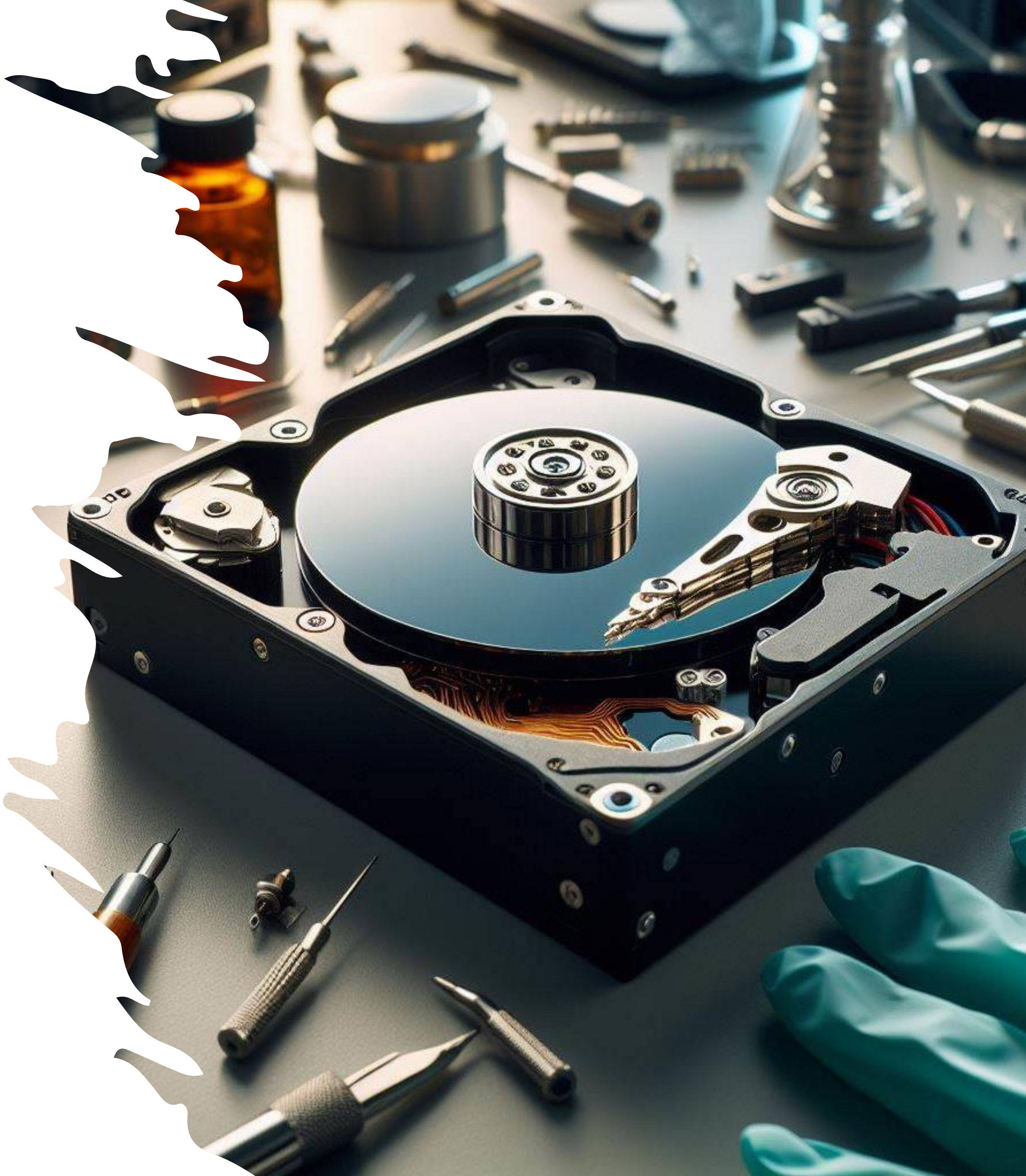
Analysis

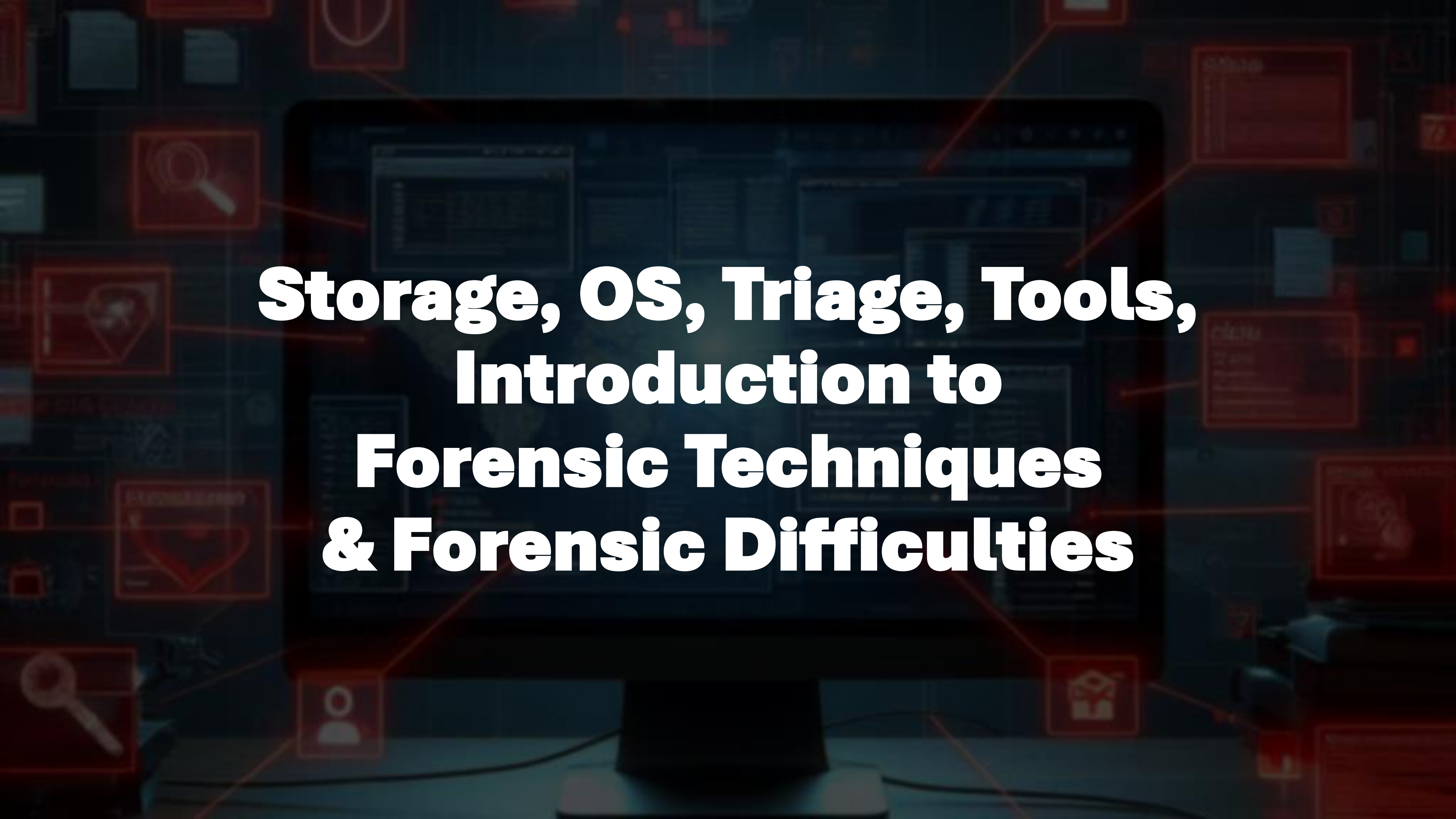
- **Analysis** and **examination** of electronically stored information
- **Purpose**: identify information that may support or contest matters in a civil or criminal investigation and/or court proceeding
- Evidence should first be **extracted** or **acquired**
- Analysis should be performed on a **copy** of the **media**
- Tools used must be previously validated

DOCUMENTATION

Presentation

- **Everything** from digital evidence seizure to the end of analysis phase must be **explained**
- An investigator must be able to **state** that the **results** provided are **correct** and **weren't changed** in any way

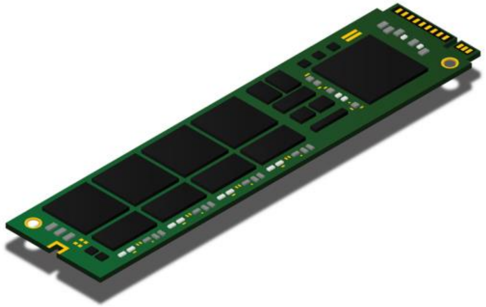




Storage, OS, Triage, Tools, Introduction to Forensic Techniques & Forensic Difficulties

Storage

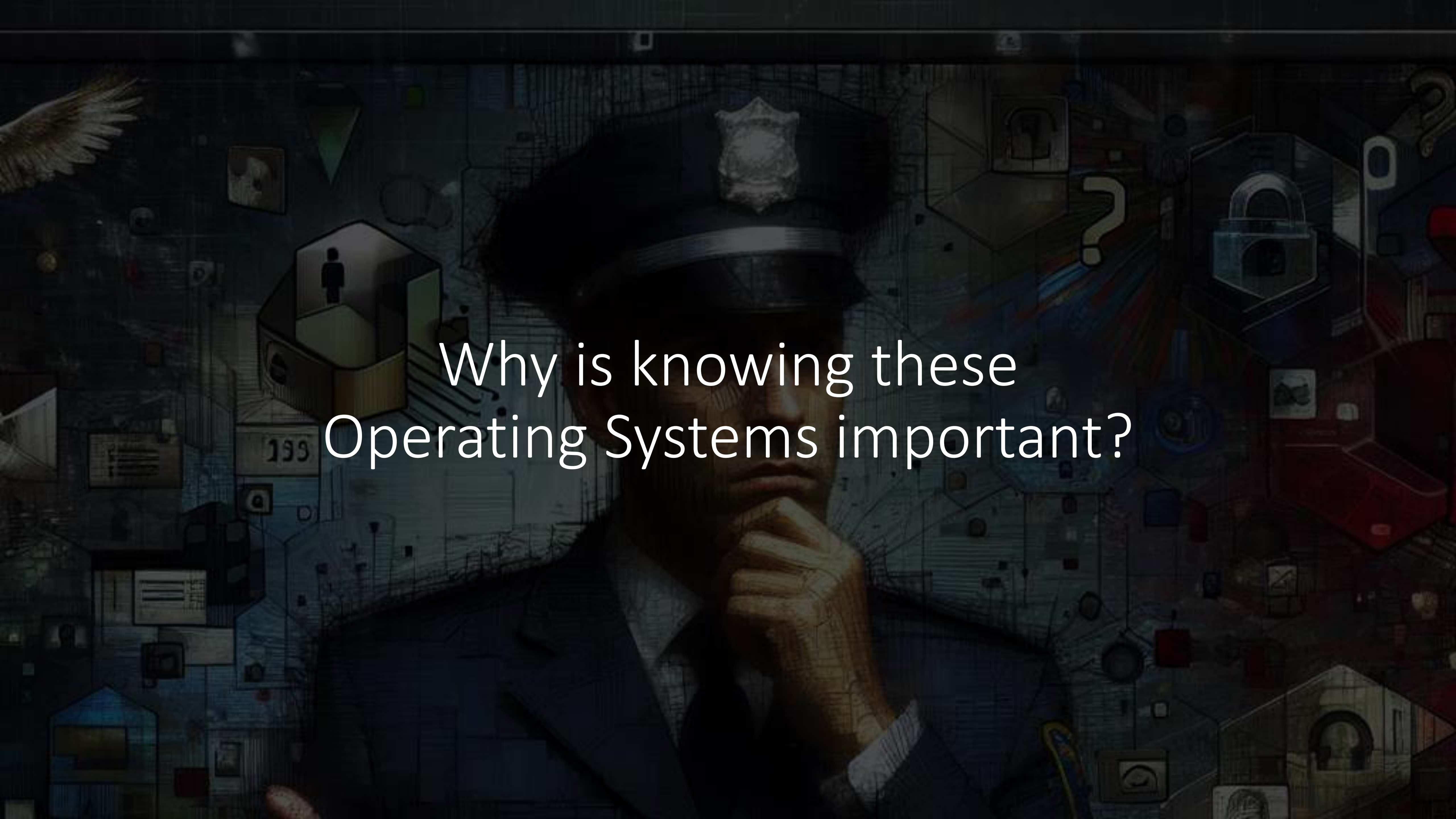
- Storage media
- HDD
- SSD
- CD
- DVD
- USB
- …



Operating System & File system

- Operating systems
  - Windows: vista, 7, 8, 10, 11 (and older)
  - macOS (changed names): Mojave, Catalina, Big Sur, Monterey (and older)
  - Linux & distro’s: Debian, Ubuntu, Linux Mint, …

- File systems
  - NTFS, FAT32, exFAT, ReFS, …
  - HFS, HFS+, APFS, …
  - Ext3, Ext4, …



Why is knowing these Operating Systems important?

Mobile device (example)

What can be found?

- Contacts Call **logs**
- Calendar
- Messages
- Emails
- Photographs
- videos
- Social networking **accounts**
- Notes
- documents
- **Financial** information
- Wi-Fi connections
- Internet browser **history**
- Applications
- Geolocations
- …

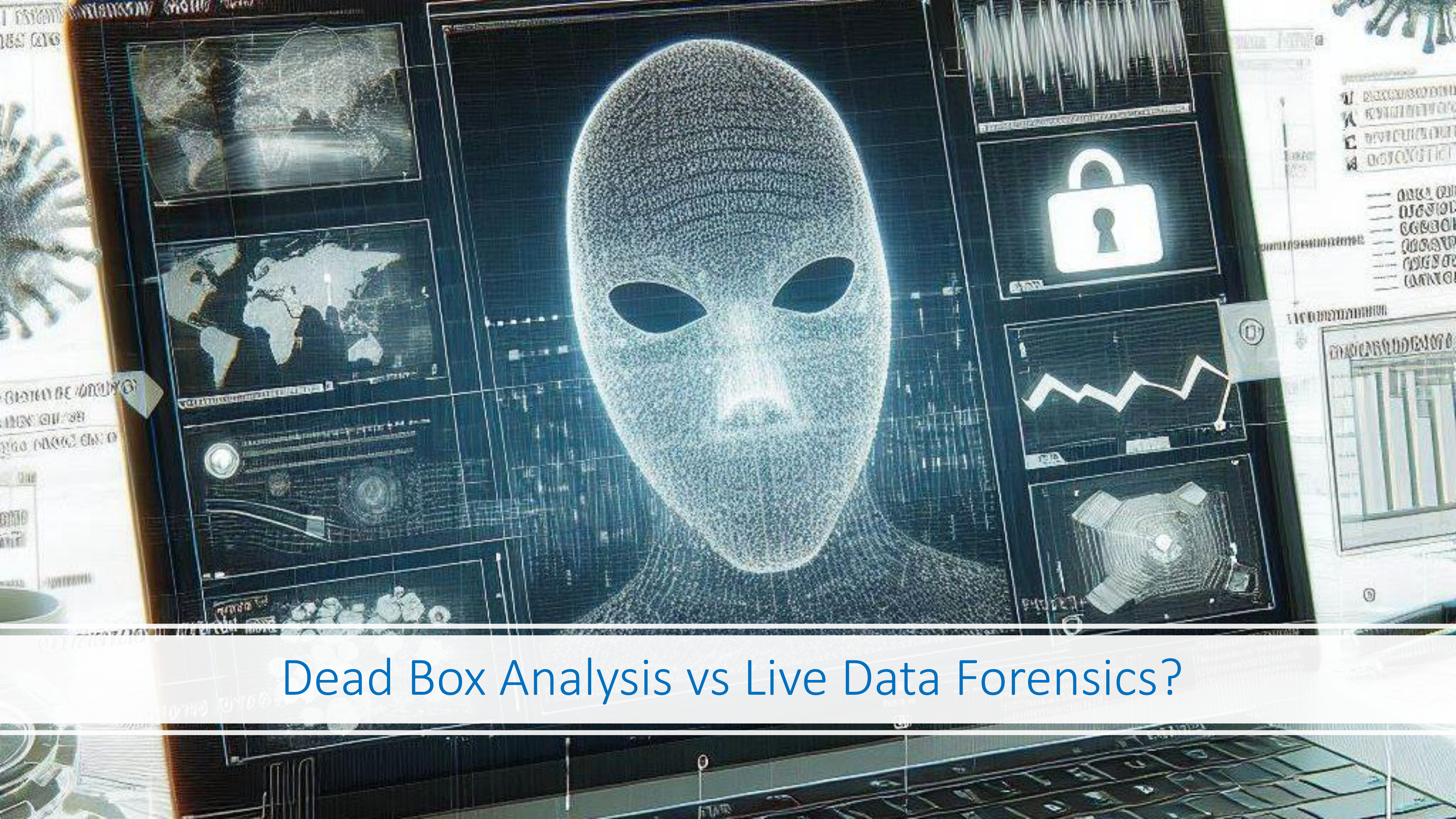
Triage

The process by which an investigator:

- Collects
- Assembles
- Analyzes
- and prioritizes digital evidence from a crime or investigation
- **Purpose**: to quickly identify data that could contain evidential value Capture what is necessary to prove or disprove investigation goals

Live scene

What to do when encountering a booted computer at the crime scene?



Dead Box Analysis vs Live Data Forensics?

Intro to Forensic Techniques

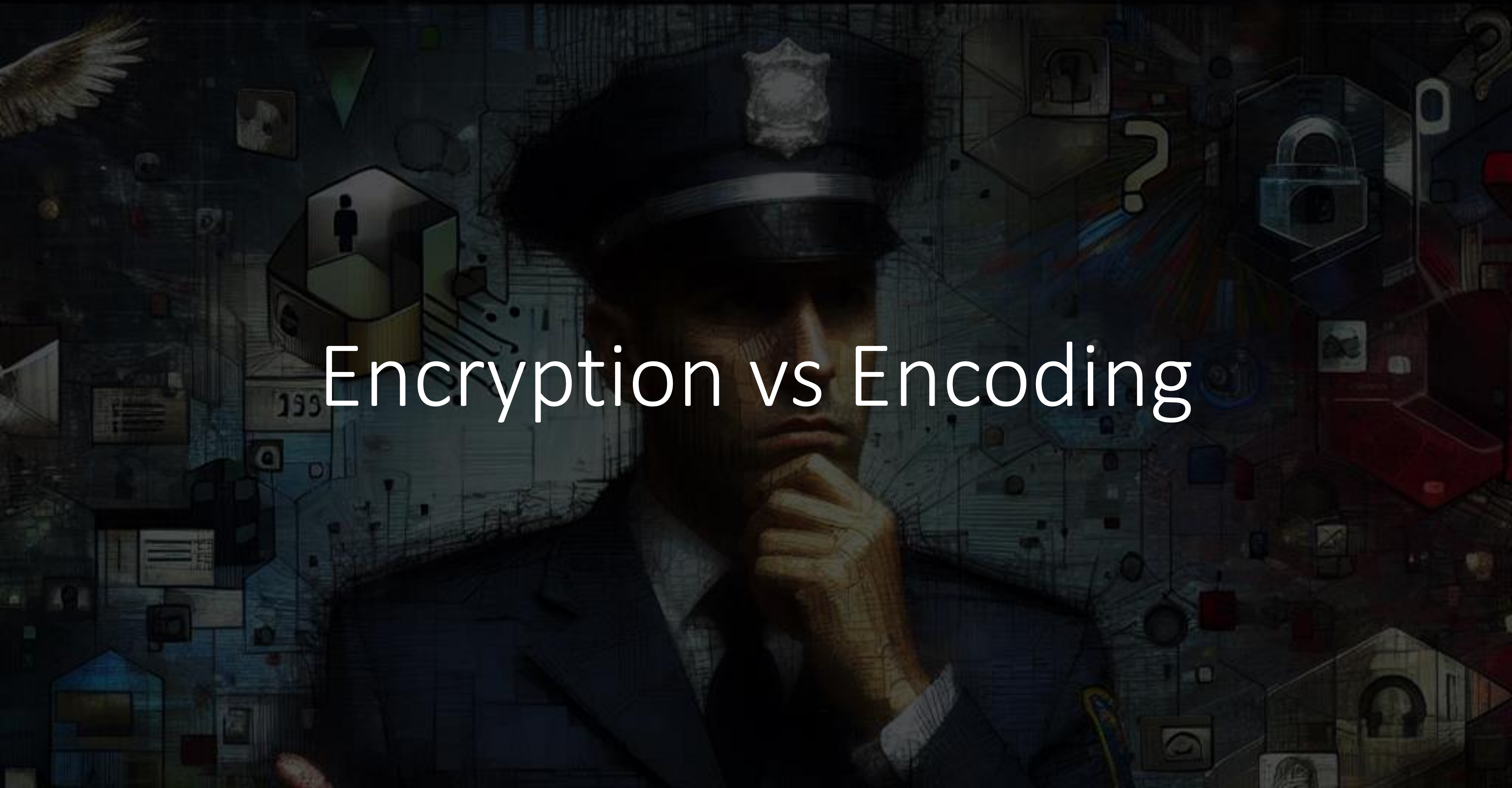
- Artefacts
  - Browser history
  - Event logs
  - Registry
  - … (much more)
- File recovery
- Carving
- E-mail investigation (headers, pst, …)
- Network investigation
- Specific searches (Regular Expressions = filters)
- LDF
- …

E-mail investigation

- Mail headers
- Log files
- Internet
    - Router & Servers
        - Hops (map)
    - IP-addresses
        - Public
        - Private
    - DNS
    - VPN (+proxy)

Forensic Difficulties

- Closed hardware
- Password & 2FA
- Encryption
- Big volumes
- Time
- Hashing countermeasures
- Anti-forensic software
- Steganography
- Hidden volumes
- …



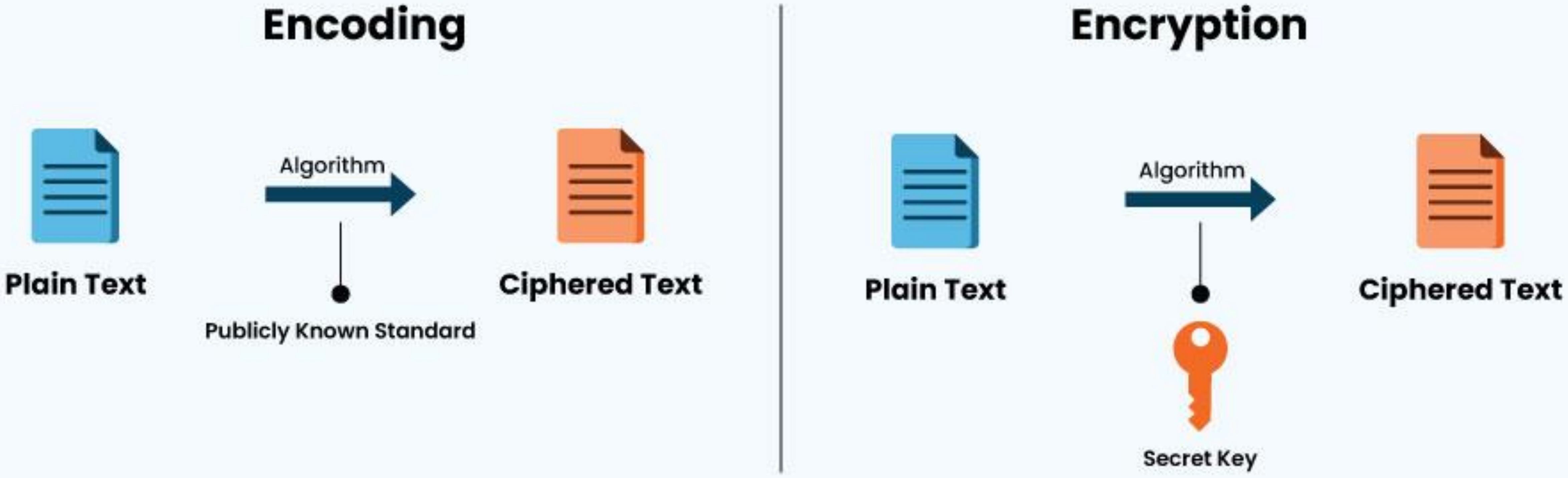
Encryption vs Encoding

ZW5jb2Rl

- the process of putting characters into a specialized format
- for efficient transmission or storage
- I.e; base64
- ZW5jb2Rl = ?

ZW5jb2Rl

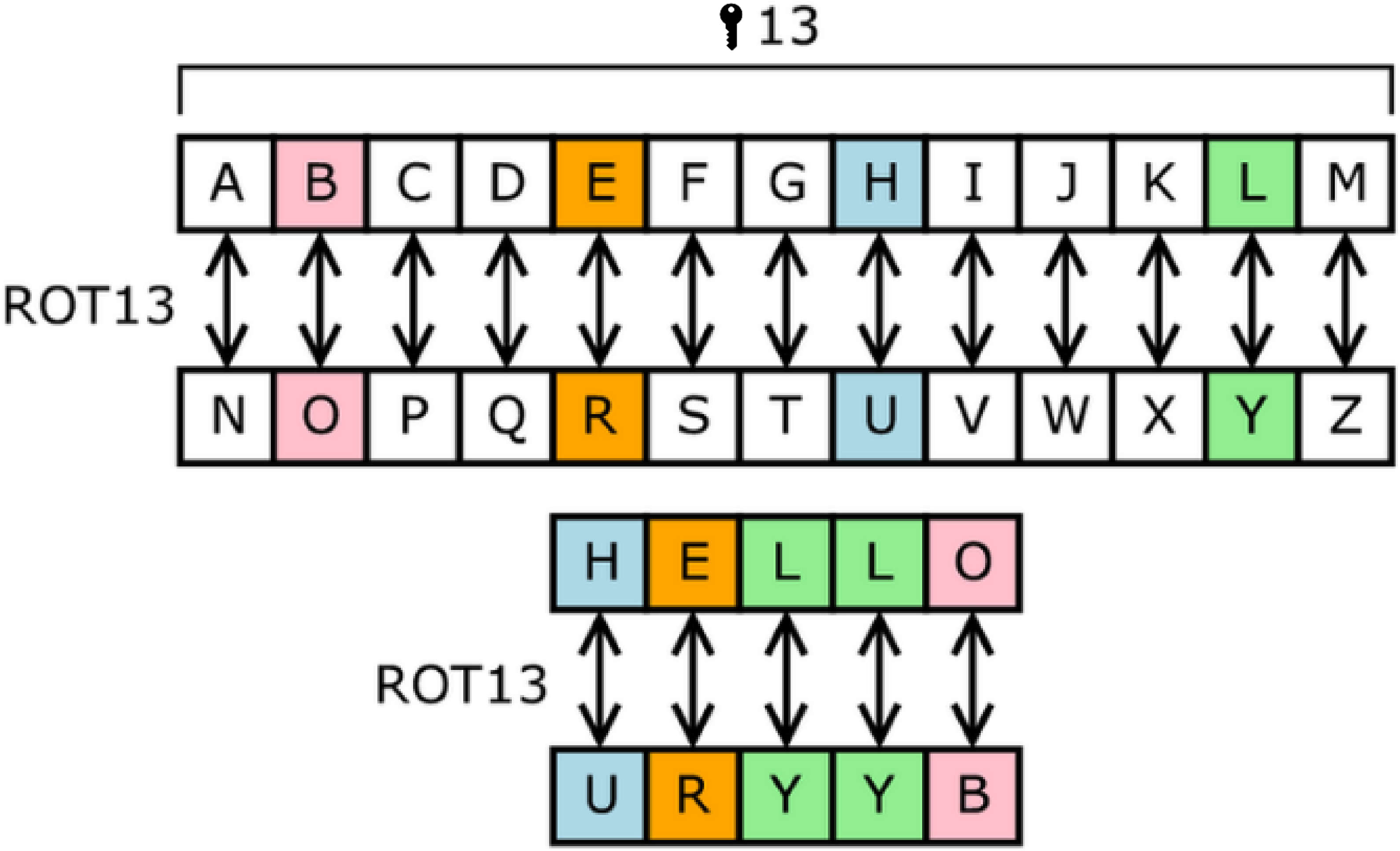
- the process of putting characters into a specialized format
- for efficient transmission or storage
- I.e; base64
- ZW5jb2Rl ⇔ ENCODE

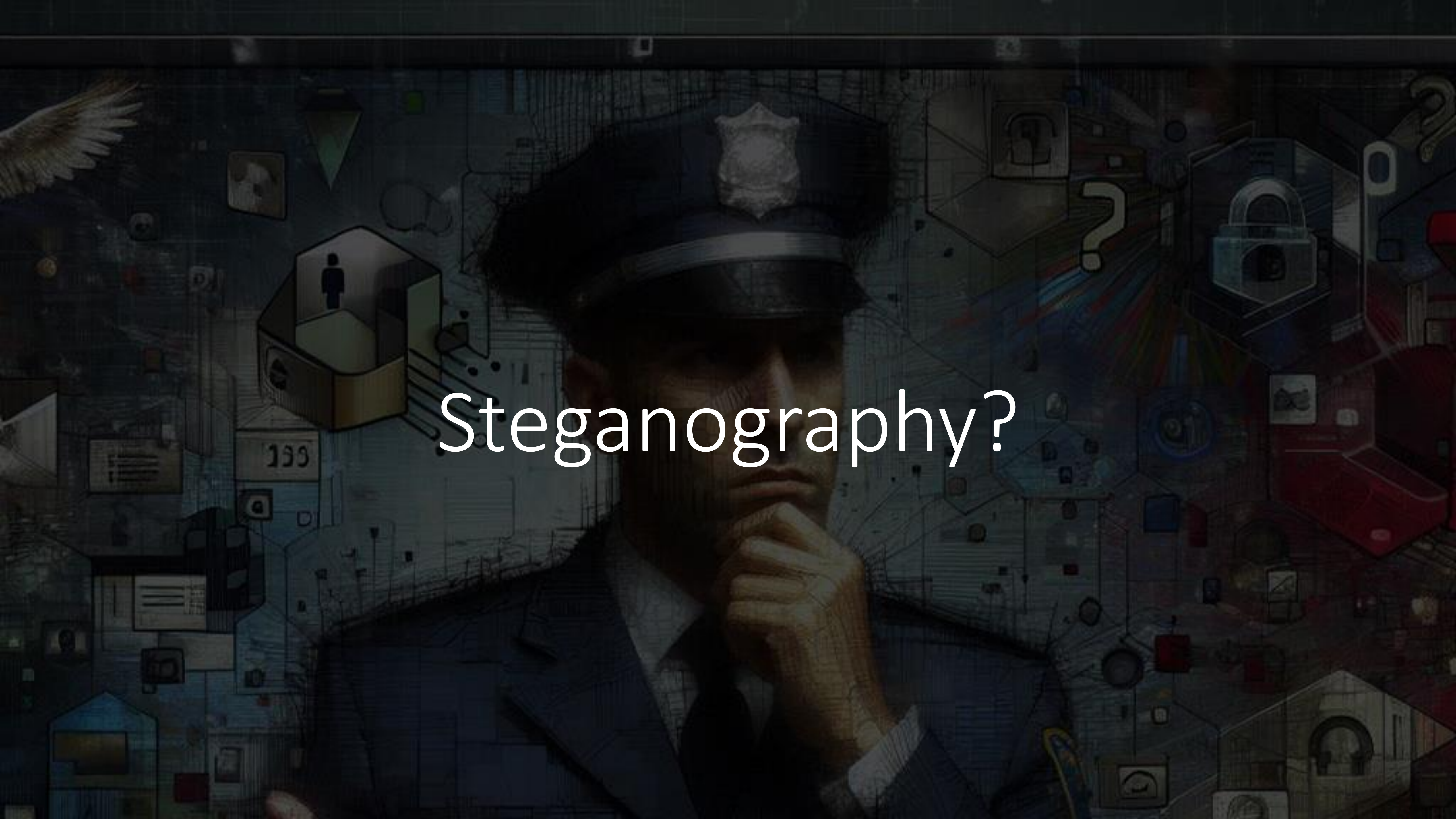


Encoding Vs. Encryption Difference

Source: https://cheapsslweb.com/resources/encoding-vs-encryption

REN


13
ROT13
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
ROT13
H E L L O
U R Y Y B



Steganography?

Questions & contact

Timothy De Groot

- **Mail:** timothy.degroot@police.belgium.eu
- **Tel:** +32 (0) 495 43 48 45
- **LinkedIn:** Timothy D.G.

POST COVID CHALLENGES IN CRIMINAL JUSTICE

Investigating Web 2.0

Thessaloniki, 23 – 24 May 2024

E – evidence in child sexual abuse cases

Speaker : Eleni Papadopoulou

Public Prosecutor at the Court of First Instance of Athens and the Economic Crime Prosecution Office

Co-funded by
the European Union

The Modern Definition of CSA crimes – New forms of CSA crimes - Legal TOOLS

- Eu Directive 2011/93
- **Child Pornography** (article 2 of the Directive)
- Other cyber related crimes include **Revenge Porn** (the act of distributing sexual containing material without the consent of the party) **+ On line Child grooming (**the proposal by means of information and communication technology by an adult to meet a child for the purpose of committing a sexual offence)
- **New challenges → Proposal of the Commission (6/2/2024)** on combatting child sexual abuse which covers also offences as **livestreaming of child sexual abuse** and **intentional access** and **dissemination of child sexual abuse deepfakes**
- Convention on Cybercrime of the Council of Europe
- **Resolution of the UN** for the establishment of an open-ended ad hoc committee (AHC)
- **Interim regulation** adopted on the 14 July 2021 → until 3/4/2026
- 11/5/2022 : **A proposal** on permanent rules from the Commission → obligation to the providers to detect, report and remove CSA material, number of new elements

Investigative tools
The use of e – evidence in the "more conventional" CSA crimes

- **Crime recordings**
- **Communication** between the offender and the victim
- Mobile phones : An ally when the perpetrator is someone close to home…
- **Areios Pagos 2081/2018: Text messaging revealed that the offender knew that the rape victim was a minor**
- **Testimonies versus text messaging** : Adolescents like to talk with friends; not with experts
- **Location data** → the scene of the crime
- **Areios Pagos 101/2021** : The disclosure of the encrypted code by the accused is not a mitigating factor at sentencing

Investigative tools
The use of e – evidence in the "new normal" CSA crimes

- House search = protection of the physical scene + identification of devices + protection from intervention + registration + additional evidence + digital data seizure + report = evidence + analysis of the data + report = expert opinion
- Body search (Judicial Council of Rhodes 39/2021) → leads to another suspect
- Undercover Investigation on the computer – volatile data - concealed identity → COURT ORDER OR NOT (case law: text messaging : Areios Pagos 954/2020, e – mails, Areios Pagos 1/2017, data on hard drives, Opinion of the Prosecutor at Areios Pagos 6/2008 → NO COURT ORDER, Cloud storage : Judicial Council of Athens 613/2016 → YES COURT ORDER)
- Profiling of the suspect
- Open Sources Intelligence – Mom takes action! Judicial Council of Athens 4533/2016
- Deposition by means of electronic devises = Evidence only if combined with other evidences

Report on digital data on child pornography – usual questions

IN A COMPREHENSIVE WAY – PROFILING OF THE SUSPECT

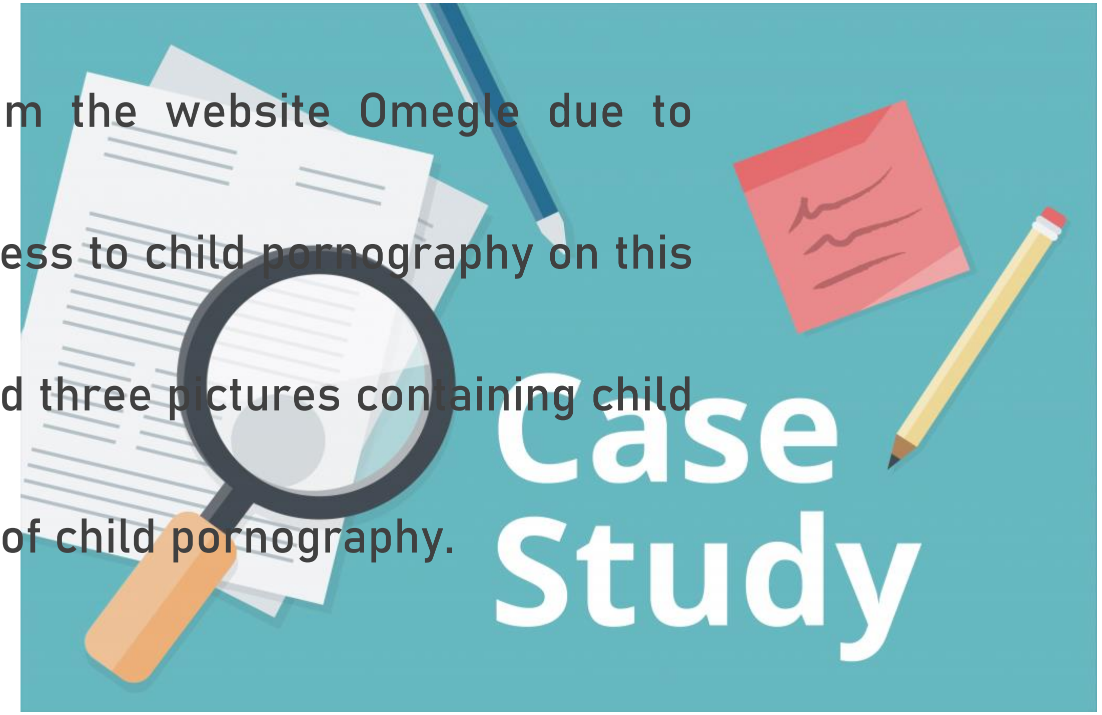
- Is there any child pornography material on the device?
- When was the material produced/downloaded?
- What is the percentage of child pornography compared with the one of adult pornography?
- How many times did the offender access the child pornography material?
- Where deleted files are retrieved, the date and time must be recorded
- Has the offender produced any child pornography material?
- Did the offender have access to websites containing such a material? Did the offender have accounts on these websites?
- Are there any p2p systems?
- Did the offender use any online applications such as Messenger, Chat and What's Up?
- Is there any child pornography material stored in the cloud?

Case law – importance of the investigation on e – evidence

- **The non bis in idem argument** : Prosecution for 150 pictures on 13/7/2016. Another Prosecution for 338 pictures The non bis in idem argument. **Judicial Council of the Court of Appeals of Thessaloniki 831/2019** = Different DATE, Different PICTURES, TWO devices = DIFFERECT ACT OF POSSESSION →
- **The case of the Military Academy :** LACK of proper report on the matter of confiscation + LACK of investigation on the hard drive = ACQUITAL
- **Court of Appeals of Dodecanisa 3/2019 :** Not a single file was found indicating there was a communication and/or file sharing between the accused and the victim. + The examination and analysis of the laptop revealed that the conversations didn't take place originally at the accused's laptop. The communication and multimedia files in question auto synced between the accused's laptop and another device + There was no digital evidence of sharing, obtaining and distributing child pornography = ACQUITAL

CASE STUDY

- A hard drive was confiscated.
- A visual check of the suspect's laptop showed that the program ManyCam was downloaded.
- IE history check: the suspect was banned from the website Omegle due to inappropriate behavior.
- However, on 16-3-2016 he was able to obtain access to child pornography on this website.
- On the file "Downloads", there were one video and three pictures containing child pornography material.
- The hard drive of the suspect contained 5 videos of child pornography.



Claims of the accused

- Chat on Omegle with unknown users who sent him hyperlinks
- Not many files
- The files were downloaded automatically without his knowledge.
- Poor IT knowledge (Most common argument : WATCH OUT for the downloading of elaborated applications, access to the darkweb, use of keywords and symbols associated with content depicting child pornography)

❖ Areios Pagos 643/2020 : 1) Visible Files, 2) The existence of other files essential to the accused' s profession in the same drive prove that he had knowledge of the child pornography material, 3) Encrypted Files

❖ Court of Appeals of Piraeus : No distribution + Deletion + no proof that he had opened the files + at the same time music files were downloaded → ACQUITAL

Prosecutor’s response

- Poor IT knowledge? It was a fact that he did install ManyCam and used it to watch a child pornography video.
- NOT many files? Still there are files containing CSA material
- Shift of burden of proof → It was he who had to prove that he lacked the knowledge to retrieve the pictures from the unallocated space
- He had access to DEEPWEB.
- He used signals and symbols associated with content depicting child pornography
- He visited OMEGLE many times until he was banned from the site.

Indictment of the accused before the Mixed Jury Court of First Instance of Corinth

- He was found guilty
- He was sentenced to 4 years of imprisonment
- The hard disc containing child pornography material was SEIZED

To summarise

Information → IP addresses → Police → Digital Traces → Prosecutor + Judicial Council → Court orders → Identification → House search → Seizure of Mobile devices + Visual check of the devices in real time → Forensic Analysis → Files containing pictures and videos + IE history + Downloading of programs useful to gain access to child pornography + Keywords with child pornography connotations = PROSECUTION and CONDEMNATION

Digital information used for the investigation consisted of IP addresses and digital traces, which was critical for the court orders and the subsequent identification of the suspect. The visual check of the devices (in real time) that were seized in the house search led to a forensic analysis which revealed a range of information including files with videos/pictures, IE history, keywords with child pornography as well as programmes download which was useful to gain access to child pornography =PROSECUTION & CONDEMNATION

Thank you for your attention!

Any questions or comments?