ERA

POST-COVID CHALLENGES IN CRIMINAL JUSTICE

FOCUS ON INTERNET SEARCHES FOR EU LEGAL PRACTITIONERS

Cracow, 21-22 September 2023

FACE-TO-FACE

EXCELLENCE IN EUROPEAN LAW

Speakers and chairs

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

Olga Binert-Mielko, Senior Specialist, International Cooperation Department, Polish National School of Judiciary and Public Prosecution (KSSiP), Lublin

Steven David Brown, International Cybercrime Consultant, Vienna

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

Andrea Cruciani, Judge, Court Martial, Naples

Peter Dupont, Investigator and Researcher, Underground Child Foundation, Brussels

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

Christos Karagiannis, Prosecutor, Court of First Instance, Athens

Rafał Kierzynka, Judge, Seconded to the Ministry of Justice, Warsaw

Emmanuelle Legrand, Magistrate, AI Project Manager, Digital Economy Department, Ministry of the Economy, Finances and Recovery, Paris

Mirjam Hannah Steinfeld, Attorney at Law, Of Counsel, Rosinus Partner, Frankfurt am Main

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 and other computer-generated or stored documents
- Presenting internet searches in court

Language
English

Event number
323DT13

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

european.law

POST-COVID CHALLENGES IN CRIMINAL JUSTICE

Thursday, 21 September 2023

09:00 Arrival and registration of participants

09:30 **Welcome and introduction to the programme**
Olga Binert-Mielko & Laviero Buono

PART I: TECHNICAL ISSUES AND BASIC UNDERSTANDING OF THE INTERNET ACHITECTURE 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 current internet technologies.

Chair: Laviero Buono

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

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

Philip Anderson

10:30 Discussion

10:45 Break

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

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

Seanpaul Gilroy

12:15 Discussion

12:30 Lunch

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

Chair: Steven David Brown

13:30 **An overview of the defence rights related issues regarding the use of e-evidence collected on the internet**
Mirjam Hannah Steinfeld

14:15 Discussion

14:30 **Presenting evidence in court: e-files, videoconferences and remote trials**

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

Andrea Cruciani

15:15 Discussion

15:30 Break

16:00 **The problem with evidence obtained by non-LEA**

- Undercover investigations
- Pros and cons of using AI for collecting e-evidence

Peter Dupont

Objective

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

This series of events addresses various challenges that judges, prosecutors and lawyers in private practice working in the field of EU criminal justice will have to face for the years ahead. Some of these challenges will remain in the "new normal" well beyond the end of the pandemic.

This seminar will focus on internet searches for legal practitioners.

About the Project

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

Who should attend?

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

Venue

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

16:45 Discussion

17:00 End of first day

19:30 Dinner offered by the organisers

Friday, 22 September 2023

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

Chair: Philip Anderson

09:30 **Handling electronic evidence in courts**

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

Emmanuelle Legrand

10:00 Discussion

10:15 **Game of bits: putting the tech in detection**

- Playing attribution chess
- Tools and Tactics for unmasking cybercriminals
- Ethical considerations and challenges of judicial oversight
- Enforcement jurisdiction and considerations of sovereignty

Steven David Brown

10:45 Discussion

11:00 Break

11:30 **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

12:00 Discussion

12:15 **Collecting, authenticating and evaluating digital data in the framework of legal proceedings: best practices**

- Issuing order
- Presentation in court & admissibility of e-evidence
- Case studies

Rafał Kierzynka

12:45 Discussion

13:00 End of online seminar and light lunch

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

CPD

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

Your contact persons

Laviero Buono
Head of Section

Susanne Babion
Assistant
Tel.: +49(0)651 9 37 37 422
E-Mail: sbabion@era.int

This programme has been produced with the financial support of the Justice Programme of 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

Cracow, 21-22 September 2023 / Event number: 323DT13/SBa

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 first come first served and according to nationality. Spanish applicants who work for the prosecution service must apply for this event through CEJ.

2. Applications should be submitted before **05 June 2023.**
3. A response will be sent to every applicant after this deadline. **We advise you not to book any travel before you receive our confirmation**.

Registration Fee

4. €130 including documentation, coffee breaks, lunches and dinner.

Travel and Accommodation Expenses

5. Participants will receive a fixed contribution towards their travel expenses and are asked to book their own travel. The condition for payment of this contribution is to sign all attendance sheets at the event. No supporting documents are needed. The amount of the contribution will be determined by the EU unit cost calculation guidelines, which are based on the distance from the participant's place of work to the seminar location and will not take account of the participant's actual travel costs.
6. Travel costs from outside Poland: participants can calculate the contribution to which they will be entitled on the European Commission website (https://era-comm.eu/go/calculator). The distance should be calculated from their place of work to the seminar location *(in case of participants from Austria, Czech Republic, Germany, Hungary, Lithuania, Latvia, Romania and Slovakia the amounts for Inter-Member States return journeys between 50 and 400 km is fixed. Please consult p.11 on https://era-comm.eu/go/unit-cost-decision-travel).*
7. For those travelling within Poland, the contribution for travel is fixed at €20 (for a distance between 50km and 400km). Please note that no contribution will be paid for travel under 50km. For more information, please consult p.10 on https://era-comm.eu/go/unit-cost-decision-travel
8. Accommodation: Participants' accommodation has already been reserved at Dom Aplikanta, located at the National School. ERA has booked and will pay for two nights, single occupancy accommodation at Dom Aplikanta, no accommodation costs will be reimbursed. The booking is for 20-22 September 2023 (2 nights).
9. 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

10. Participation at the whole conference is required and your presence will be recorded.
11. 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.
12. The participant's address and other relevant information will 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 unless the participant indicates that he or she does not wish ERA to do so.
13. A certificate of attendance will be distributed by email within a week after the end of the conference.

Apply online for "Post-Covid Challenges in Criminal Justice" online: **www.era.int/?132162&en**

Venue

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

Language

English

Contact Person

Susanne Babion
Assistant
Tel.: +49(0)651 9 37 37 422
E-Mail: sbabion@era.int

323DT13
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.

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

A1-05	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	Consolidated Version of the Statute of the Court of Justice of the European Union (01 August 2016)
A2-02	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
A3-02	Case of Mihalache v. Romania [GC] (Application no. 54012/10), Strasbourg, 08 July 2019
A3-03	Case of Altay v. Turkey (no. 2) (Application no. 11236/09), Strasbourg, 09 April 2019
A3-04	Case Beuze v. Belgium (Application no. 71409/10), Strasbourg, 09 November 2018
A3-05	Case of Vizgirda v. Slovenia (Application no. 59868/08), Strasbourg, 28 August 2018
A3-06	Case of Şahin Alpay v. Turkey (Application no. 16538/17), Strasbourg, 20 March 2018
A3-07	Grand Chamber Hearing, Beuze v. Belgium [GC] (Application no. 71409/10), Strasbourg, 20 December 2017
A3-08	Case of Blokhin v. Russia (Application no. 47152/06), Judgment European Court of Human Rights, Strasbourg, 23 March 2016
A3-09	Case of A.T. v. Luxembourg (Application no. 30460/13), Judgment European Court of Human Rights, Strasbourg, 09 April 2015
A3-10	Case of Blaj v. Romania (Application no. 36259/04), Judgment European Court of Human Rights, Strasbourg, 08 April 2014
A3-11	Case of Boz v. Turkey (Application no. 7906/05), Judgment European Court of Human Rights, Strasbourg, 01 October 2013 (FR)
A3-12	Case of Pishchalnikov v. Russia (Application no. 7025/04), Judgment European Court of Human Rights, Strasbourg, 24 October 2009
A3-13	Case of Salduz v. Turkey (Application no. 36391/02), Judgment, European Court of Human Rights, Strasbourg, 27 November 2008

A4) Brexit

A4-01	Draft text of the Agreement on the New Partnership between the European Union and the United Kingdom (UKTF 2020-14), 18 March 2020
A4-02	Draft Working Text for an Agreement on Law enforcement and Judicial Cooperation in Criminal Matters
A4-03	The Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 (2019/742), 28th March 2019
A4-04	Brexit next steps: The European Arrest Warrant, House of Commons, 20 February 2020

A4-05	Brexit next steps: The Court of Justice of the EU and the UK, House of Commons, 7 February 2020
A4-06	The Law Society, “Brexit no deal: Criminal Justice Cooperation”, London, September 2019
A4-07	European Commission, Factsheet, „A „No-deal“-Brexit: Police and judicial cooperation”, April 2019
A4-08	CEPS: Criminal Justice and Police Cooperation between the EU and the UK after Brexit: Towards a principled and trust-based partnership, 29 August 2018
A4-09	Policy paper: The future relationship between the United Kingdom and the European Union, 12 July 2018
A4-10	House of Lords, Library Briefing, Proposed UK-EU Security Treaty, London, 23 May 2018
A4-11	HM Government, Technical Note: Security, Law Enforcement and Criminal Justice, May 2018
A4-12	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
A4-13	House of Commons, Home Affairs Committee, UK-EU Security Cooperation after Brexit, Fourth Report of Session 2017-19, London, 21 March 2018
A4-14	HM Government, Security, Law Enforcement and Criminal Justice, A future partnership paper
A4-15	European Criminal Law after Brexit, Queen Mary University London, Valsamis Mitsilegas, 2017
A4-16	House of Lords, European Union Committee, Brexit: Judicial oversight of the European Arrest Warrant, 6th Report of Session 2017-19, London, 27 July 2017
A4-17	House of Commons, Brexit: implications for policing and criminal justice cooperation (24 February 2017)
A4-18	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	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)*
B2-02	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)*
B2-03	Case law by the Court of Justice of the European Union on the European Arrest Warrant – Overview, Eurojust, 15 March 2020
B2-04	Case C-717/18, X (European arrest warrant – Double criminality) Judgement of the Court of 3 March 2020
B2-05	Case C-314/18, SF Judgement of the Court of 1 March 2020
B2-06	Joined Cases C-566/19 PPU (JR) and C-626/19 PPU (YC), Opinion of AG Campos Sánchez-Bordona, 26 November 2019
B2-07	Case C-489/19 PPU (NJ), Judgement of the Court (Second Chamber) of 09 October 2019
B2-08	Case 509/18 (PF), Judgement of the Court (Grand Chamber), 27 May 2019
B2-09	Joined Cases C-508/18 (OG) and C-82/19 PPU (PI), Judgement of the Court (Grand Chamber), 24 May 2019
B2-10	The Guardian Press Release: Dutch court blocks extradition of man to 'inhumane' UK prisons, 10 May 2019
B2-11	Case 551/18, IK, Judgement of the Court of 06 December 2018 (First Chamber)
B2-12	CJEU Press Release No 141/18, Judgement in Case C-207/16, Ministerio Fiscal, 2 October 2018
B2-13	CJEU Press Release No 135/18, Judgement in Case C-327/18 PPU RO, 19 September 2019
B2-14	Case C-268/17, AY, Judgement of the Court of 25 July 2018 (Fifth Chamber)
B2-15	Case C-220/18 PPU, ML, Judgement of the Court of 25 July 2018 (First Chamber)
B2-16	Case C-216/18 PPU, LM, Judgement of the Court of 25 July 2018 (Grand Chamber)
B2-17	InAbsentiEAW, Background Report on the European Arrest Warrant - The Republic of Poland, Magdalena Jacyna, 01 July 2018
B2-18	Case C-571/17 PPU, Samet Ardic, Judgment of the court of 22 December 2017
B2-19	C-270/17 PPU, Tupikas, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-20	Case C-271/17 PPU, Zdziaszek, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-21	Case C-579/15, Popławski, Judgement of the Court (Fifth Chamber), 29 June 2017

B2-22	Case C-640/15, Vilkas, Judgement of the Court (Third Chamber), 25 January 2017
B2-23	Case C-477/16 PPU, Kovalkovas, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-24	Case C-452/16 PPU, Poltorak, Judgement of the Court (Fourth chamber), 10 November 2016
B2-25	Case C-453/16 PPU, Özçelik, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-26	Case C-294/16 PPU, JZ v Śródmieście, Judgement of the Court (Fourth Chamber), 28 July 2016
B2-27	Case C241/15 Bob-Dogi, Judgment of the Court (Second Chamber) of 1 June 2016
B2-28	C-108/16 PPU Paweł Dworzecki, Judgment of the Court (Fourth Chamber) of 24 May 2016
B2-29	Cases C-404/15 Pál Aranyosi and C-659/15 PPU Robert Căldăraru, Judgment of 5 April 2016
B2-30	Case C-237/15 PPU Lanigan, Judgment of 16 July 2015 (Grand Chamber)
B2-31	Case C-168/13 PPU *Jeremy F / Premier ministre*, Judgement of the court (Second Chamber), 30 May 2013
B2-32	Case C-399/11 *Stefano Melloni v Ministerio Fiscal*, Judgment of of 26 February 2013
B2-33	Case C-396/11 Ciprian Vasile Radu, Judgment of 29 January 2013
B2-34	C-261/09 Mantello, Judgement of 16 November 2010
B2-35	C-123/08 Wolzenburg, Judgement of 6 October 2009
B2-36	C-388/08 Leymann and Pustovarov, Judgement of 1 December 2008
B2-37	C-296/08 Goicoechea, Judgement of 12 August 2008
B2-38	C-66/08 Szymon Kozlowski, Judgement of 17 July 2008

B3) Mutual recognition: freezing and confiscation and asset recovery

B3-01	FATF, COVID-19-related Money Laundering and Terrorist Financing Risk and Policy Responses, Paris, 4 May 2020
B3-02	Money-Laundering and COVID-19: Profit and Loss, Vienna, 14 April 2020
B3-03	FATF President Statement – COVID-19 and measures to combat illicit financing, Paris 1 April 2020
B3-04	Moneyval Plenary Meeting report, Strasbourg, 31 January 2020
B3-05	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
B3-06	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
B3-07	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
B3-08	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

B3-09	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
B3-10	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
B3-11	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)
B3-12	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)
B3-13	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)
B3-14	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
B3-15	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)
B3-16	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	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
B5-02	Joint Note of Eurojust and the European Judicial Network on the Practical Application of the European Investigation Order, June 2019
B5-03	European Commission, Press Release, „Security Union: Commission recommends negotiating international rules for obtaining electronic evidence", Brussels, 05 February 2019
B5-04	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
B5-05	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
B5-06	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
B5-07	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
B5-08	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)
B5-09	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
B5-10	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
B5-11	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)*
B5-12	Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace *(7 December 2016)*
B5-13	ENISA 2014 - Electronic evidence - a basic guide for First Responders (Good practice material for CERT first responders)
B5-14	Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130/1; 1.5.2014)
B5-15	Guidelines on Digital Forensic Procedures for OLAF Staff" (Ref. Ares(2013)3769761 - 19/12/2013, 1 January 2014
B5-16	ACPO Good Practice Guide for Digital Evidence *(March 2012)*
B5-17	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*)
B5-18	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*)
B5-19	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)*
B5-20	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	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)*
B6-06	Council Decision on the exchange of information extracted from criminal records – Manual of Procedure *(6397/5/06 REV 5; 15.1.2007)*
B6-07	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
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	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-02	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-03	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-04	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-05	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-06	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-07	Case C-659/18, Judgement of the Court of 2 March 2020
C-08	Case C-688/18, Judgement of the Court of 3 February 2020
C-09	Case C-467/18, Rayonna prokuratura Lom, Judgment of the Court of 19 September 2019
C-10	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-11	Case C-377/18, AH a. o., Judgment of the Court of 05 September 2019
C-12	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-13	Case C-8/19 PPU, criminal proceedings against RH (presumption of innocence), Decision of the Court (First Chamber), 12. February 2019
C-14	Case C-646/17, Gianluca Moro, Opinion of the AG Bobek, 05 February 2019
C-15	Case C-551/18 PPU, IK, Judgment of the Court (First Chamber), 6 December 2018
C-16	Case C-327/18 PPU, RO, Judgment of 19 September 2018 (First Chamber)
C-17	Case C-268/17, AY, Judgment of the Court (Fifth Chamber), 25 July 2018
C-18	Case C-216/18 PPU, LM, Judgment of 25 July 2018 (Grand Chamber)

C-19	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-20	Case C-439/16 PPU, Emil Milev (presumption of innocence), Judgment of the Court (Fourth Chamber), 27 October 2016
C-21	Case C-278/16 Frank Sleutjes ("essential document" under Article 3 of Directive 2010/64), Judgment of 12 October 2017 (Fifth Chamber)
C-22	C-25/15, István Balogh, Judgment of 9 June 2016 (Fifth Chamber)
C-23	Opinion of Advocate General Sharpston, delivered on 10 March 2016, Case C-543/14
C-24	C-216/14 Covaci, Judgment of 15 October 2015 (First Chamber)

D) Approximating criminal law and Victims´ Rights

D1) Terrorism

D1-01	Terrorism Situation and Trend Report (TE-SAT) 2019
D1-02	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
D1-03	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
D1-04	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
D1-05	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)
D1-06	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
D1-07	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
D1-08	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)
D1-09	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)
D1-10	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)

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

D2-01	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
D2-02	European Migrant Smuggling Centre – 4th Annual Activity Report, The Hague, 15 May 2020
D2-03	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
D2-04	UNODC – Global Study on Smuggling of Migrants 2018, Vienna/New York, June 2018
D2-05	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
D2-06	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 Assement (IOCTA) 2019
D3-02	Special Eurobarometer 480, Report, "Europeans´ Attitudes towards Internet Security", Brussels, March 2019
D3-03	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
D3-04	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*)
D3-05	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems *(OJ L 69/67; 16.3.2005*)
D3-06	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*)
D3-07	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)
D3-08	Convention on Cybercrime (Budapest, 23.XI.2001)

D4) Protecting Victims´ Rights

D4-01	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
D4-02	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
D4-03	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
D4-04	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
D4-05	Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order
D4-06	Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims
D4-07	Website of the European Union Agency for Fundamental Rights (FRA) – Victims' rights
D4-08	Victim Support Europe

E) Criminal justice bodies and networks

E1) European Judicial Network

E1-01	European Judicial Network, Report on Activities and Management 2017-2018
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	Eurojust Annual Report 2019
E2-04	Guidelines for deciding on competing requests for surrender and extradition, October 2019
E2-05	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 Report – Beyond the Pandemic – How COVID-19 will shape the serious and organised crime landscape in the EU, 30 April 2020
E3-02	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	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*)
E4-02	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
E4-03	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)
E4-04	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
E4-05	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
E4-06	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’)
E4-07	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)
E4-08	Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor’s Office (‘the EPPO’)

F) Data Protection

F-01	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	European Commission, Press Release, „Commission marks ten years of judicial and police cooperation between between Member States of the European Union", 01 December 2019
G1-02	Regulation of the European Parliament and of the Council on establishing a framework of interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726 and (EU) 2018/1862 and (EU) 2019/816 [the ECRIS-TCN Regulation], PE-CONS 31/19, Brussels, 2 May 2019
G1-03	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
G1-04	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)*
G1-05	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)*
G1-06	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)*
G1-07	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	Third JIT Evaluation Report, Eurojust, March 2020
G2-03	Joint Investigation Teams Practical Guide (Brussels, 14 February 2017; 6128/1/17)
G2-04	Council Resolution on a Model Agreement for Setting up a Joint Investigation Team (JIT) – 2017/C18/01, Strasbourg, 19 January 2017

G2-05	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 | KRAKOW, 21-22 SEPTEMBER 2023

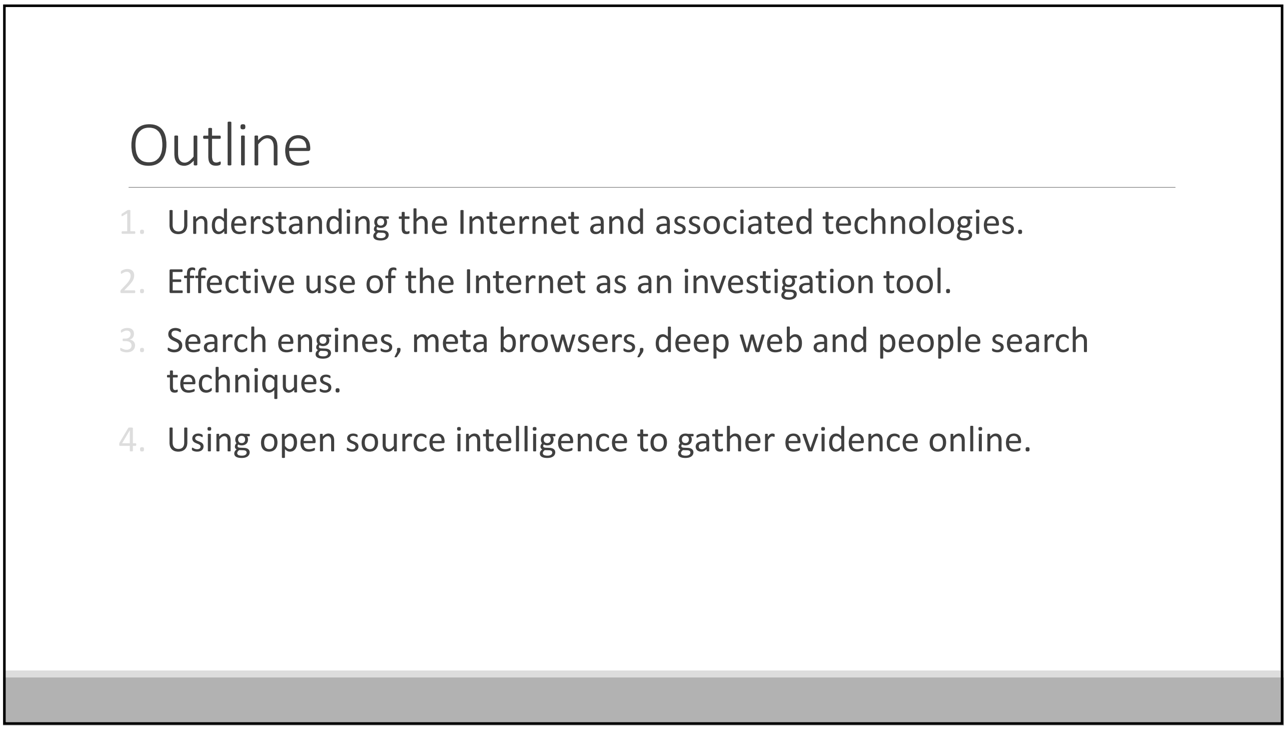
Co-funded by the Justice Programme of the European Union

1

Speaker Background

- Assistant Professor/Senior Lecturer @ Northumbria University.
- Over 16 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.

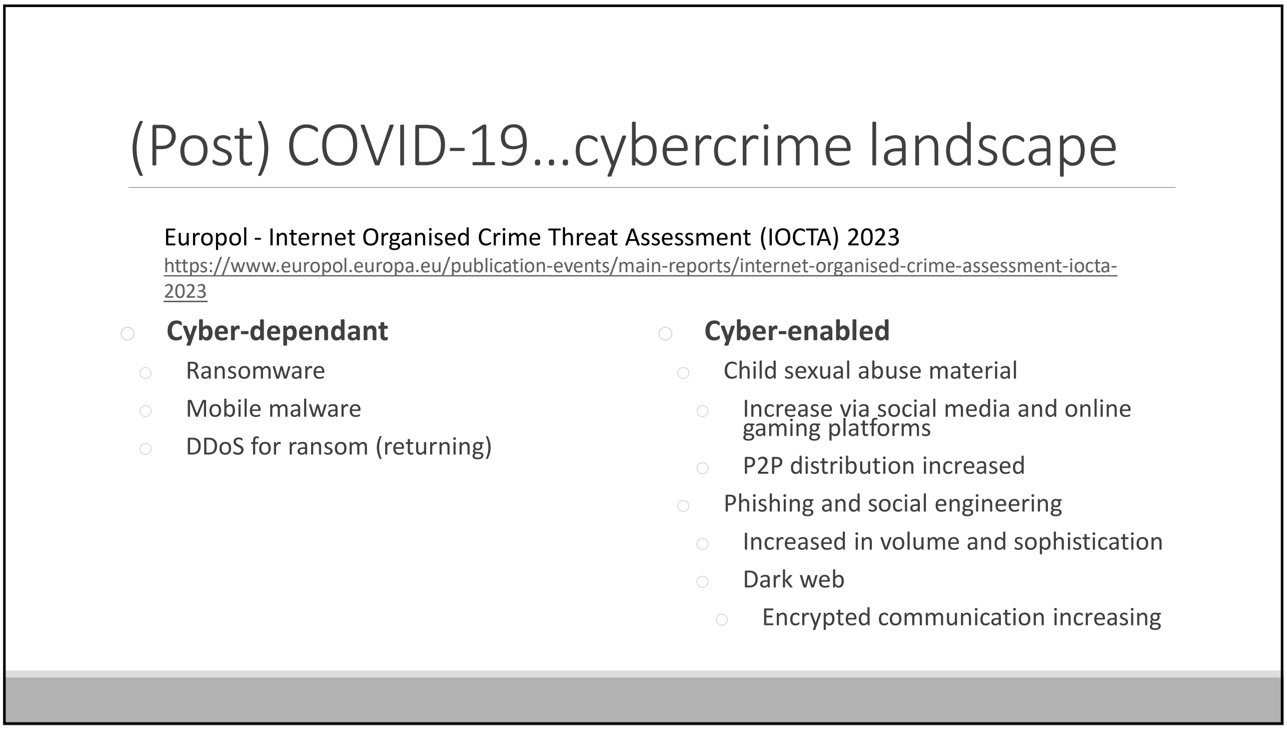
2



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.

3



(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

4

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.

5

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

6

#1

Understanding the Internet and associated technologies

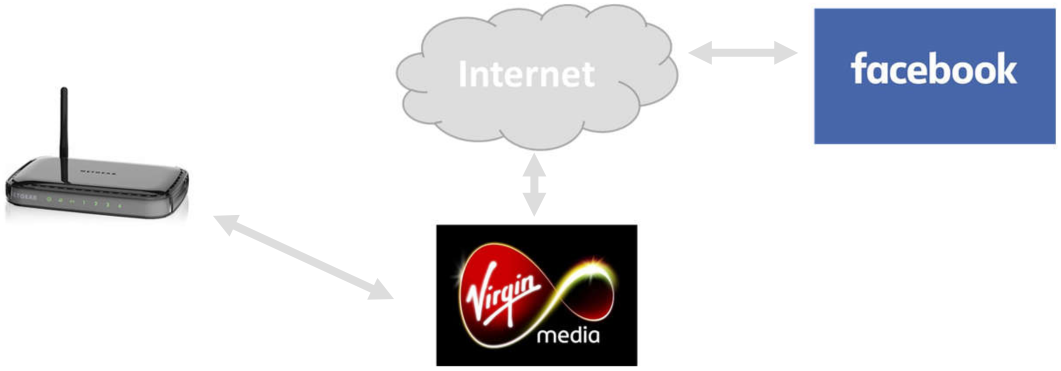
7

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

8

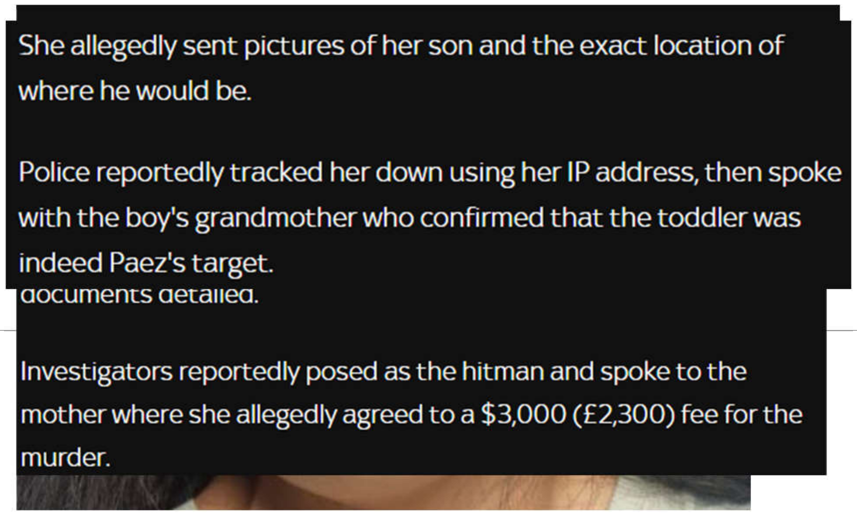
How does it work… Infrastructure



Internet Service Provider (ISP)

9

Example



She allegedly sent pictures of her son and the exact location of where he would be.

Police reportedly tracked her down using her IP address, then spoke with the boy's grandmother who confirmed that the toddler was indeed Paez's target.

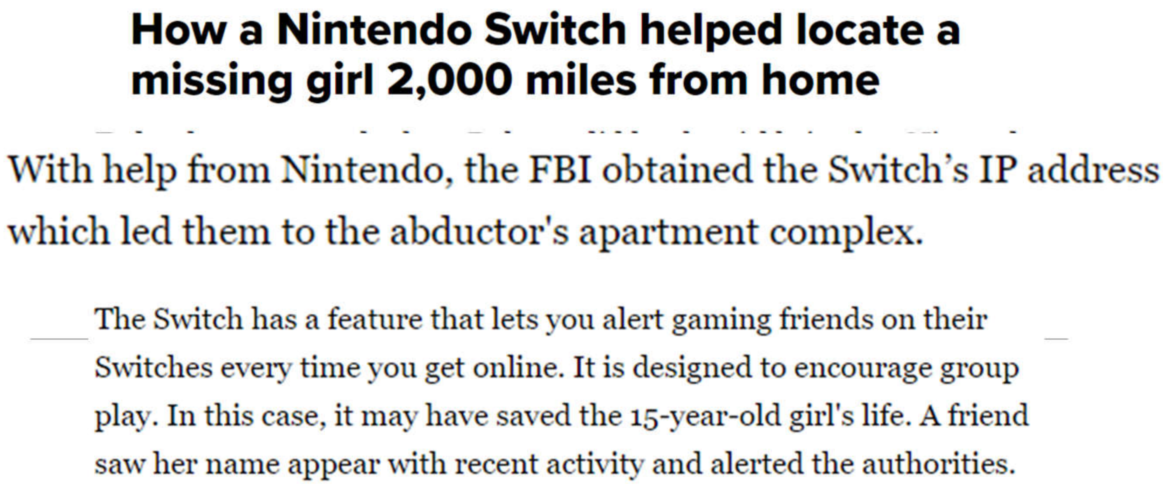
documents detailed.

Investigators reportedly posed as the hitman and spoke to the mother where she allegedly agreed to a $3,000 (£2,300) fee for the murder.

Source: https://news.sky.com/story/mother-18-allegedly-tried-to-hire-hitman-to-kill-toddler-son-and-agreed-to-pay-3000-for-murder-12924074

10

Example



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

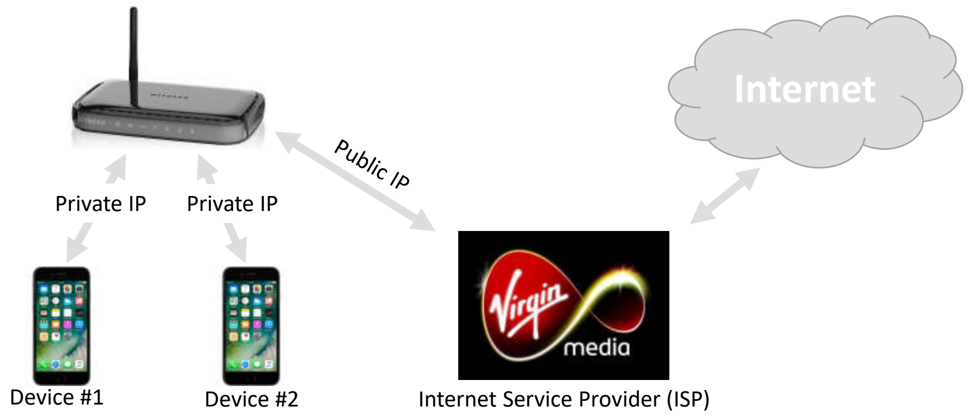
With help from Nintendo, the FBI obtained the Switch's IP address which led them to the abductor's apartment complex.

The Switch has a feature that lets you alert gaming friends on their Switches every time you get online. It is designed to encourage group play. In this case, it may have saved the 15-year-old girl's life. A friend saw her name appear with recent activity and alerted the authorities.

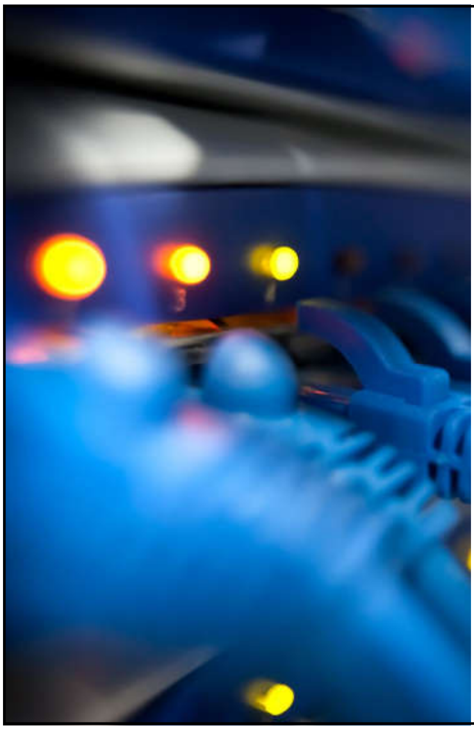
Source: https://www.abc15.com/news/local-news/investigations/how-a-nintendo-switch-helped-locate-a-missing-girl-2-000-miles-from-home

11

How does it work… Public and Private IP



12

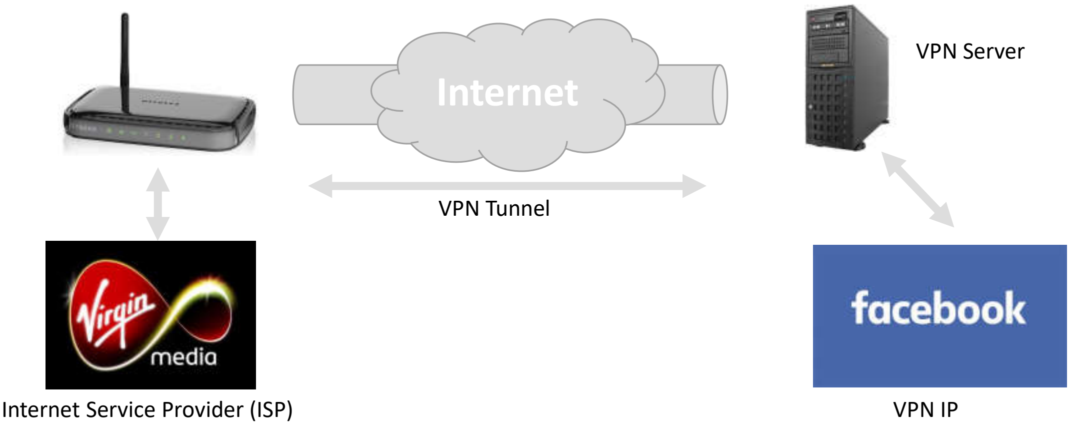


How does it work…Public and Private IP.

- 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

13

How does it work… Privacy | Anonymity



14

#2

Effective use of the Internet as an investigation tool

15

Investigations…

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

16

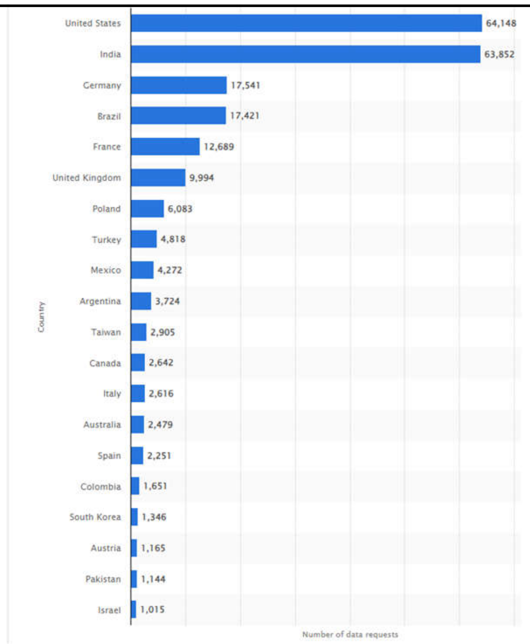
Investigations… social media

- As of April 2023, 4.8 billion social media users from 5.1 billion Internet users[1]
- Most popular social networks worldwide as of January 2023[2]
  - Facebook – 2.95 billion
  - YouTube – 2.51 billion
  - WhatsApp – 2 billion
  - Instagram – 1.4 billion
  - TikTok – 1 billion

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

[2] Statista - https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

17



Number of user data requests issued to Facebook from federal agencies and governments during 2nd half 2022, by country

Source: https://www.statista.com/statistics/287845/global-data-requests-from-facebook-by-federal-agencies-and-governments/

18

Investigations… social media

- ○ “FBI busts TikTok star after identifying his sneakers”
- ○ “The FBI arrested an aspiring social media influencer after it connected him to a series of robberies by identifying his sneakers in TikTok videos.”

Source: https://nypost.com/2022/03/02/fbi-busts-tiktok-star-c-for-series-of-armed-robberies/?utm_source=url_sitebuttons&utm_medium=site%20buttons&utm_campaign=site%20buttons

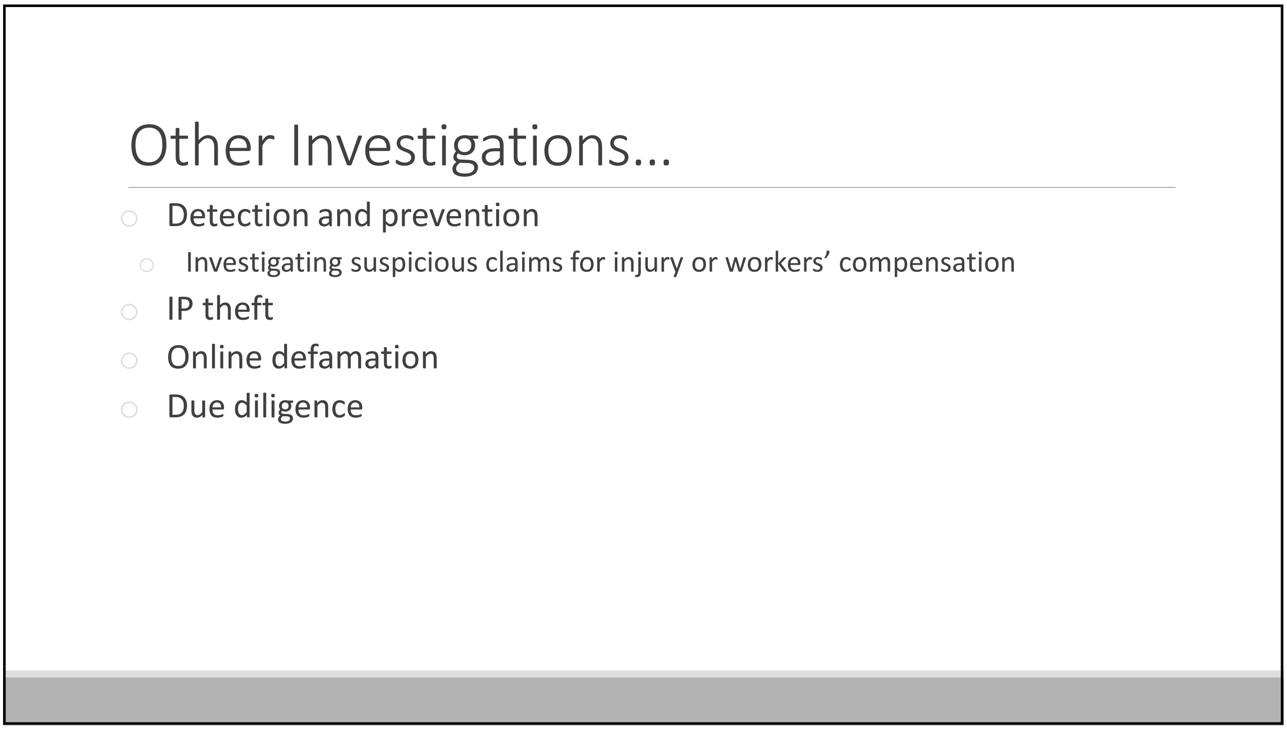
19

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

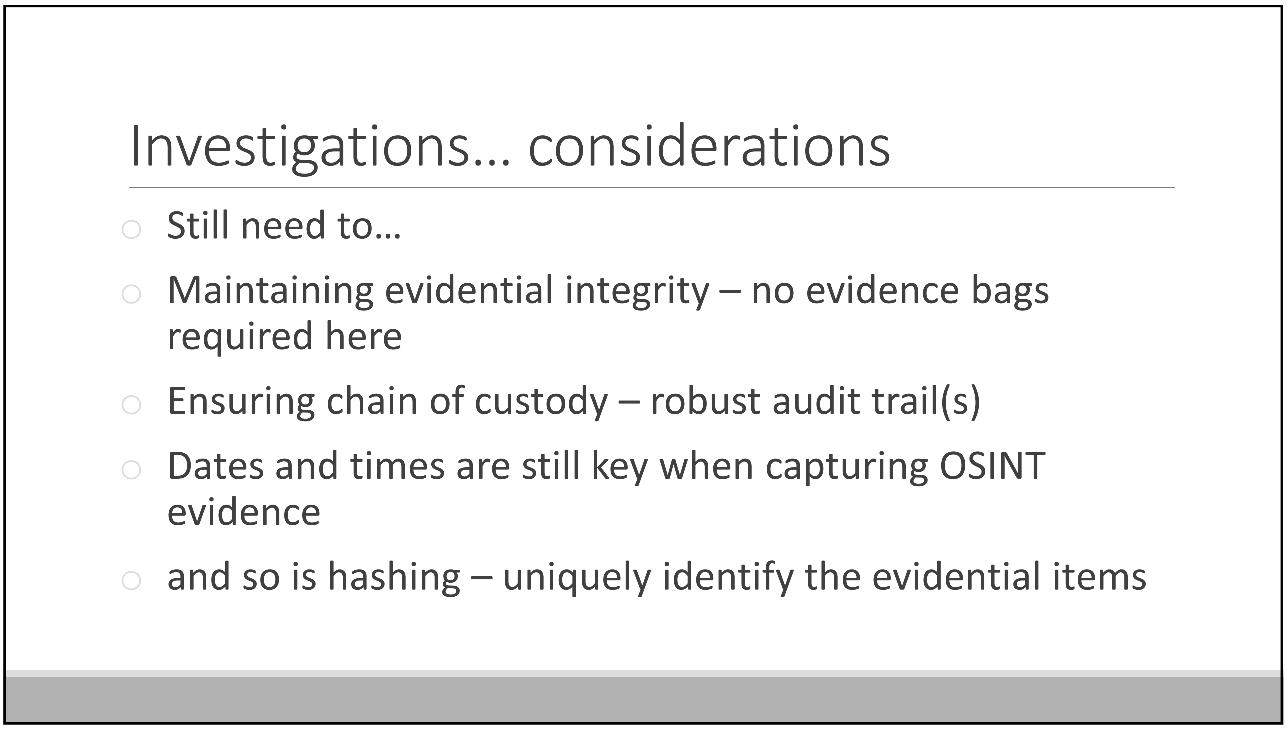
20



Other Investigations…

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

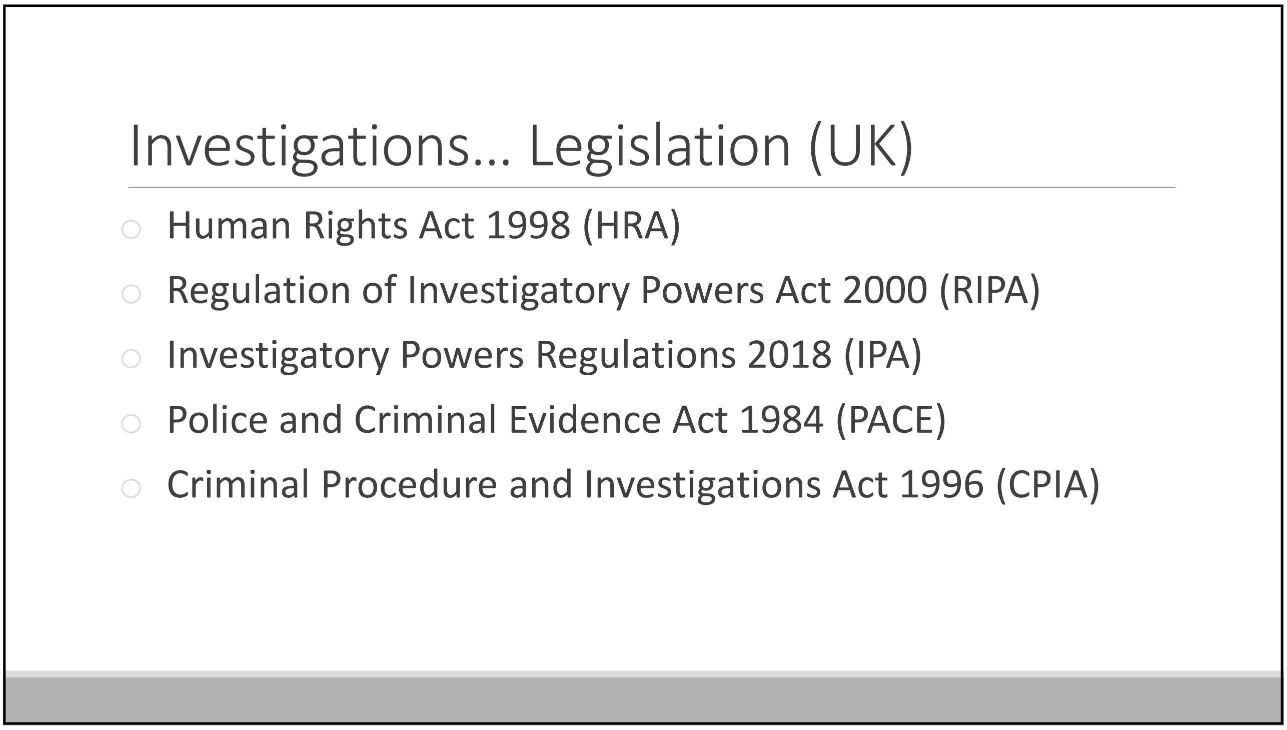
21



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

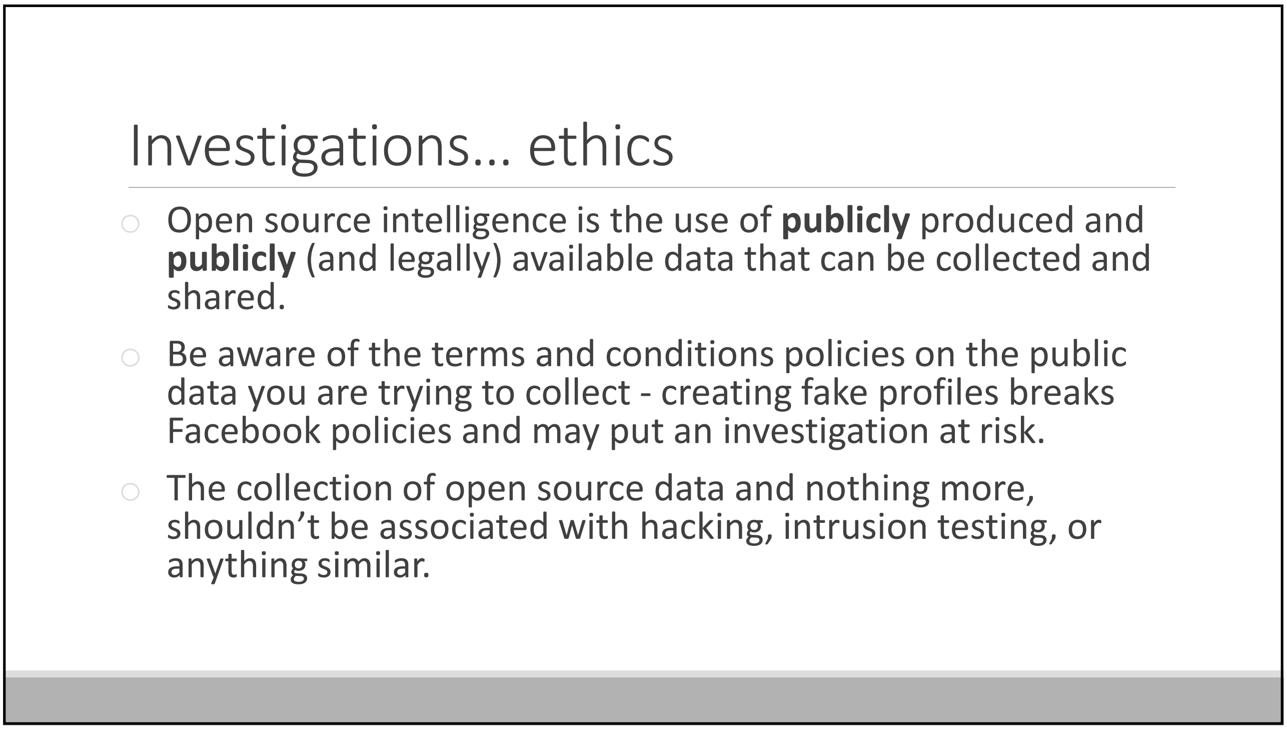
22



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)

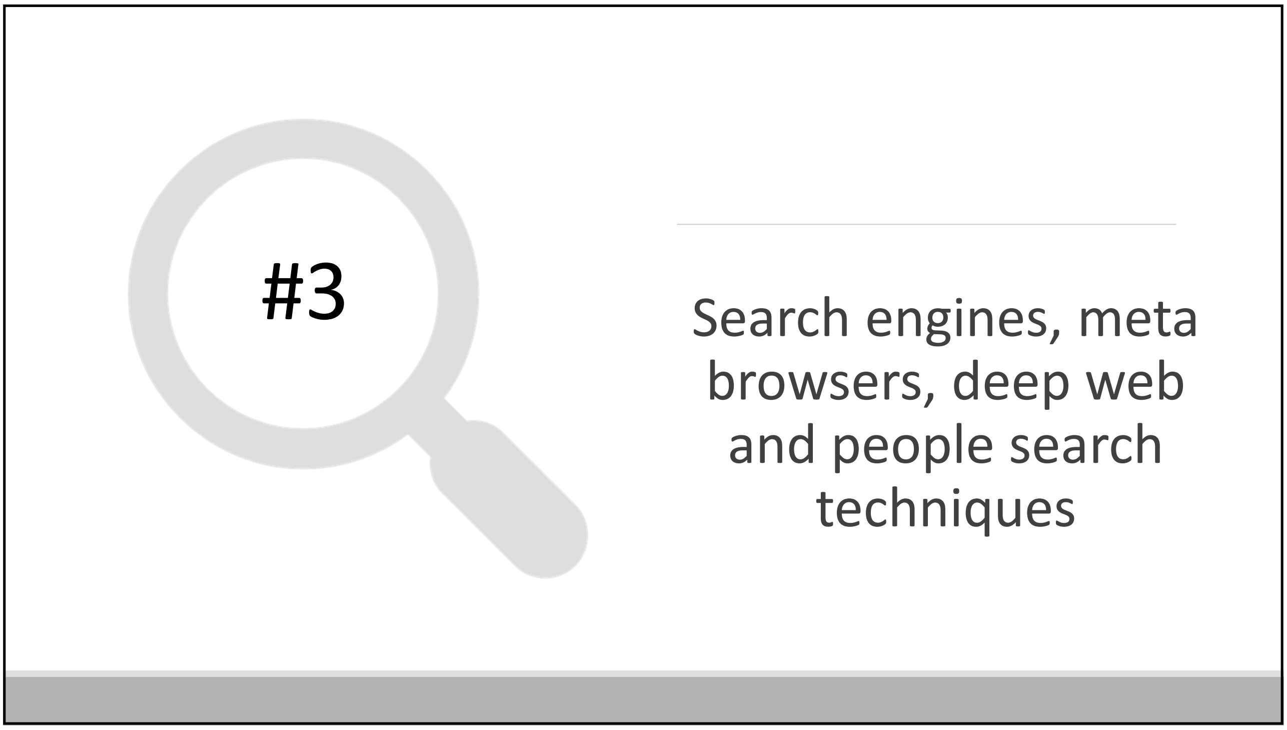
23



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 - creating fake profiles breaks Facebook policies and may put an investigation at risk.
- The collection of open source data and nothing more, shouldn’t be associated with hacking, intrusion testing, or anything similar.

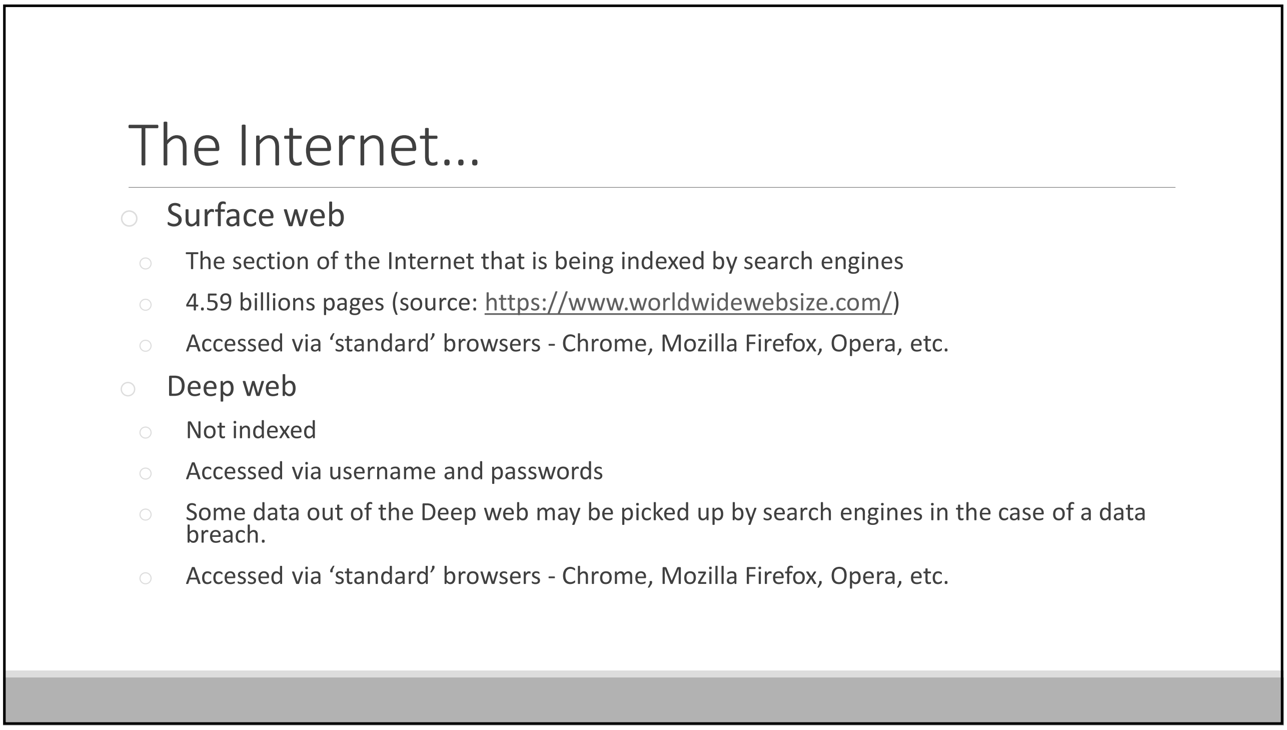
24



#3

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

25



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.

26

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.

27

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.

28

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/

29

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

30

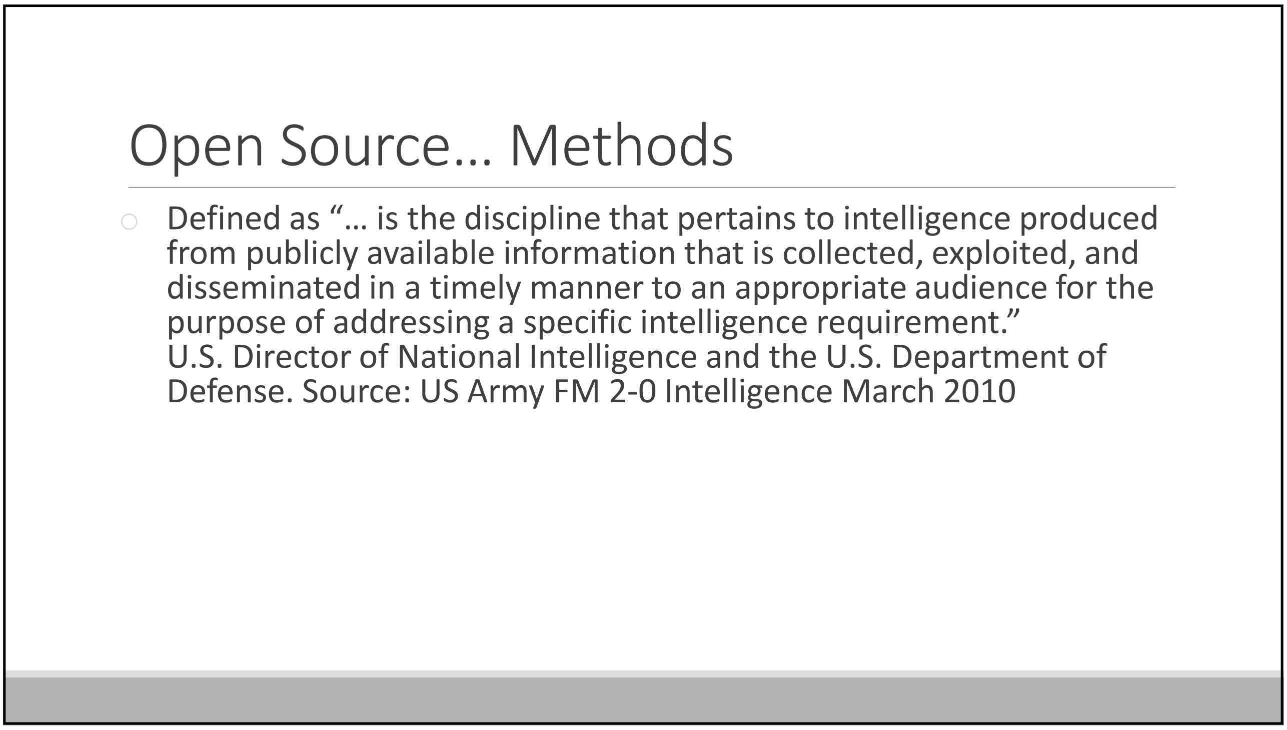
Methods… Tools

- 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

31

Using open source intelligence to gather evidence online

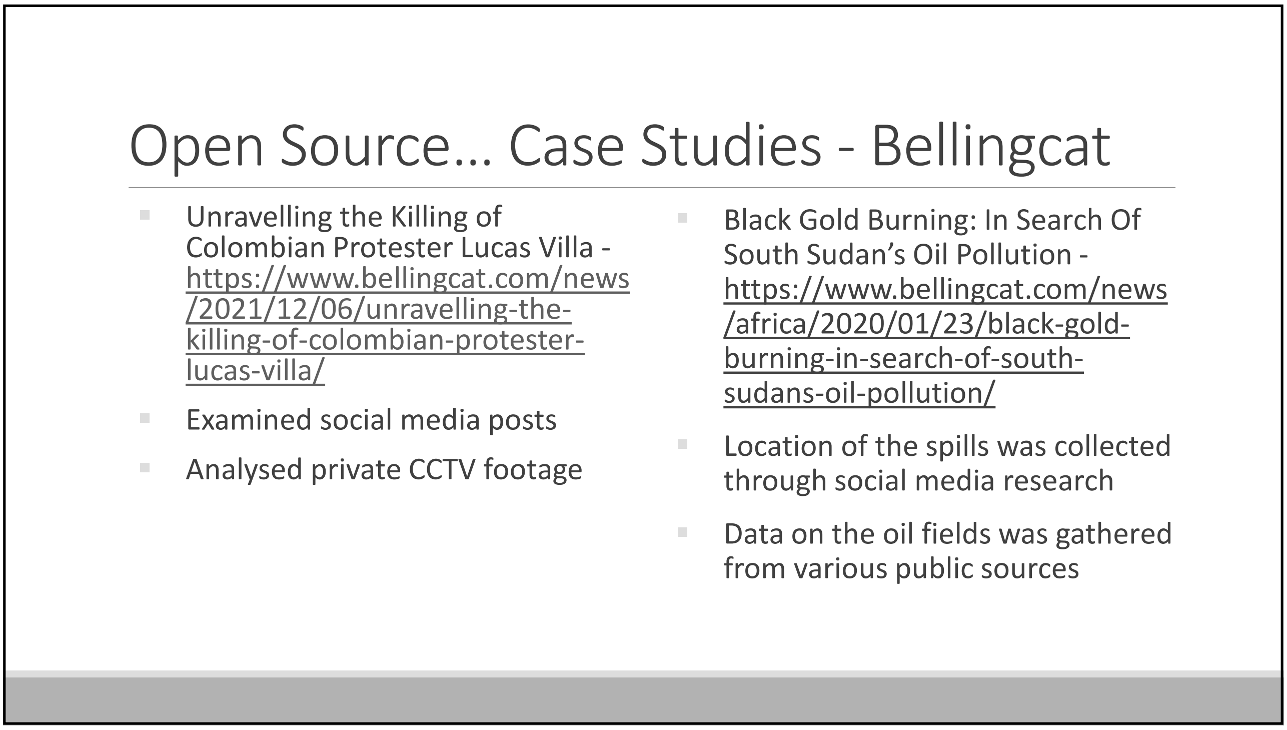
32



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

33



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

34

Open Source… Case Studies - Bellingcat

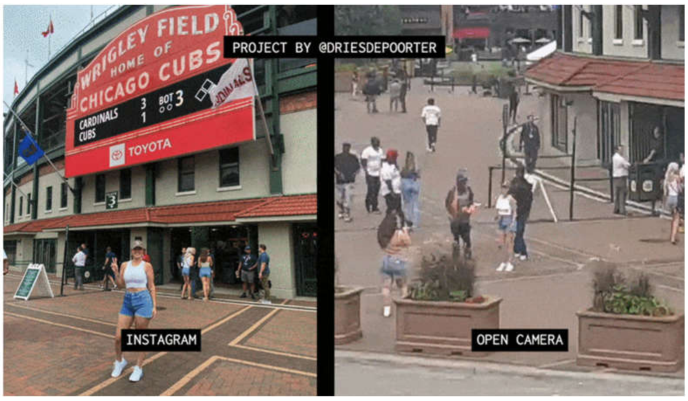
- Two Europol StopChildAbuse Images Geolocated - https://www.bellingcat.com/news/2019/12/05/two-europol-stopchildabuse-images-geolocated-part-i-madagascar/
- Google maps photos
- Google Earth imagery
- Geographic and demographic data examined
- Timeline analysis – tropical storms

- 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

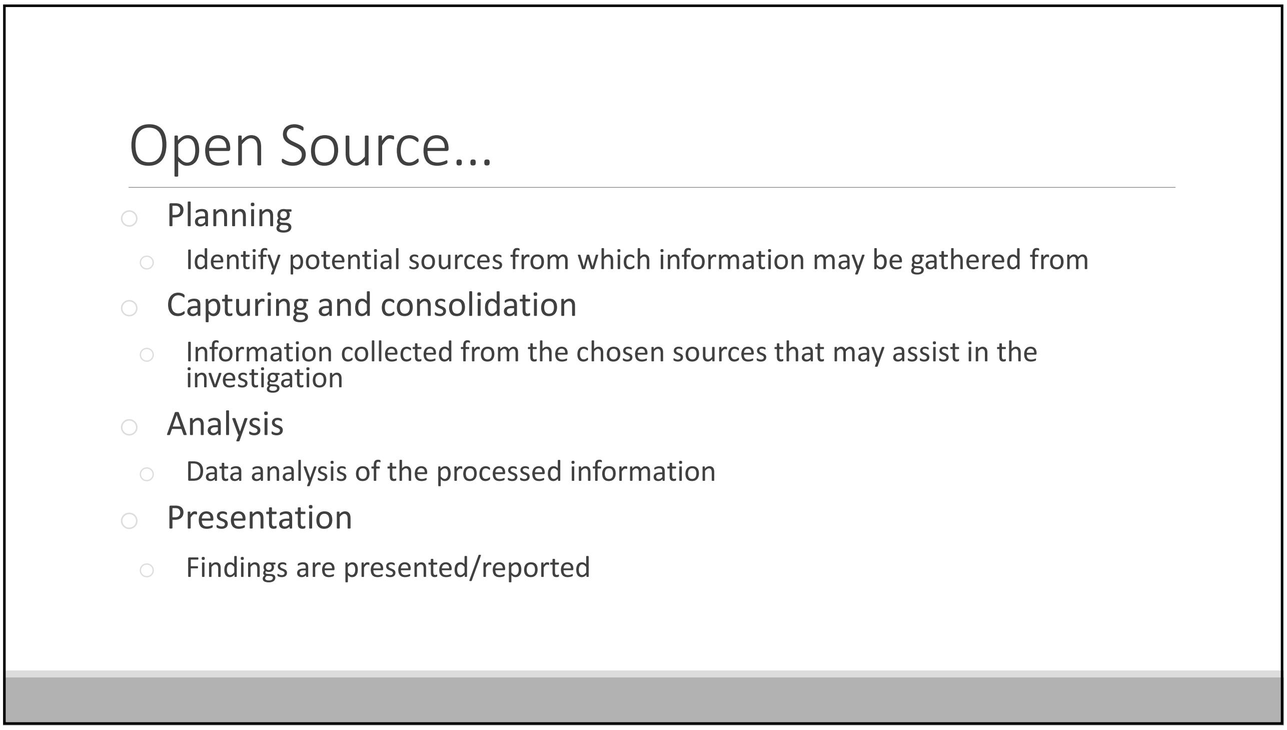
35

Open Source… methods

- Dries Depoorter |The Follower https://driesdepoorter.be/thefollower/
- How does this work?
  1. Recorded a selection of open cameras for weeks.
  2. Scraped all Instagram photos tagged with the locations of the open cameras.
  3. Software compares the Instagram with the recorded footage.



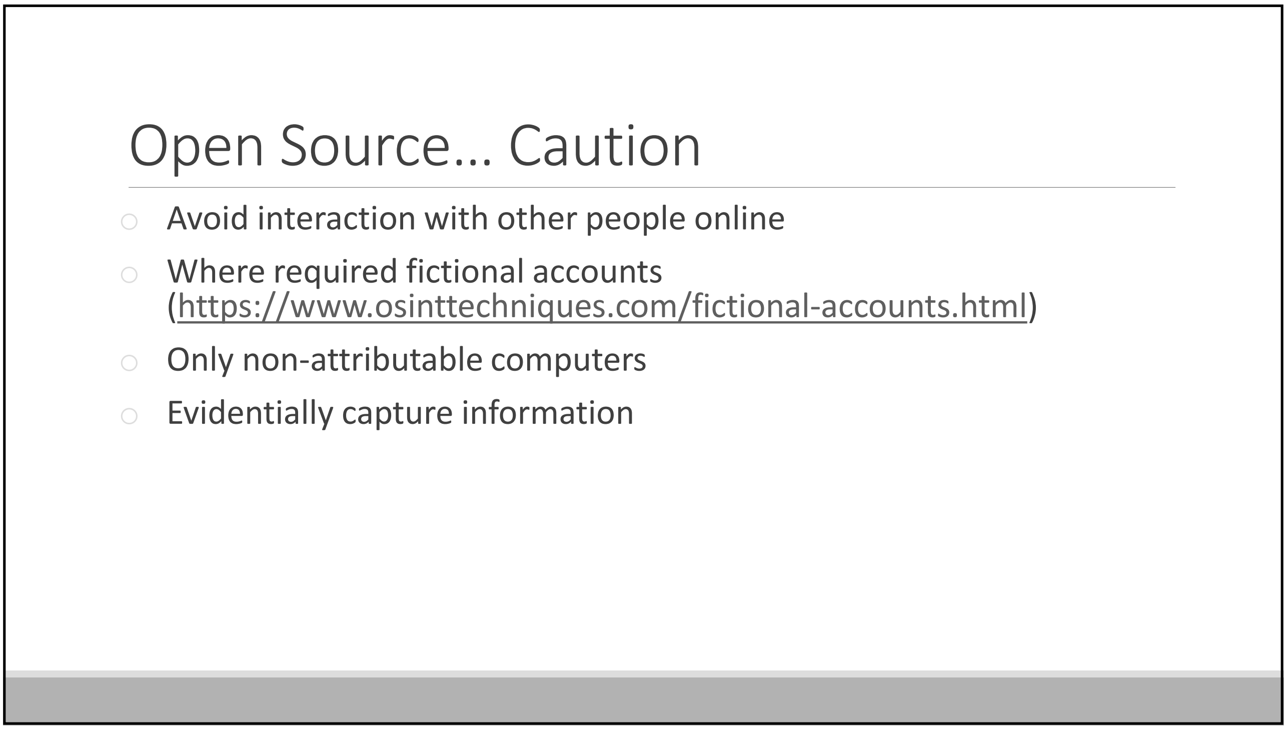
36



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

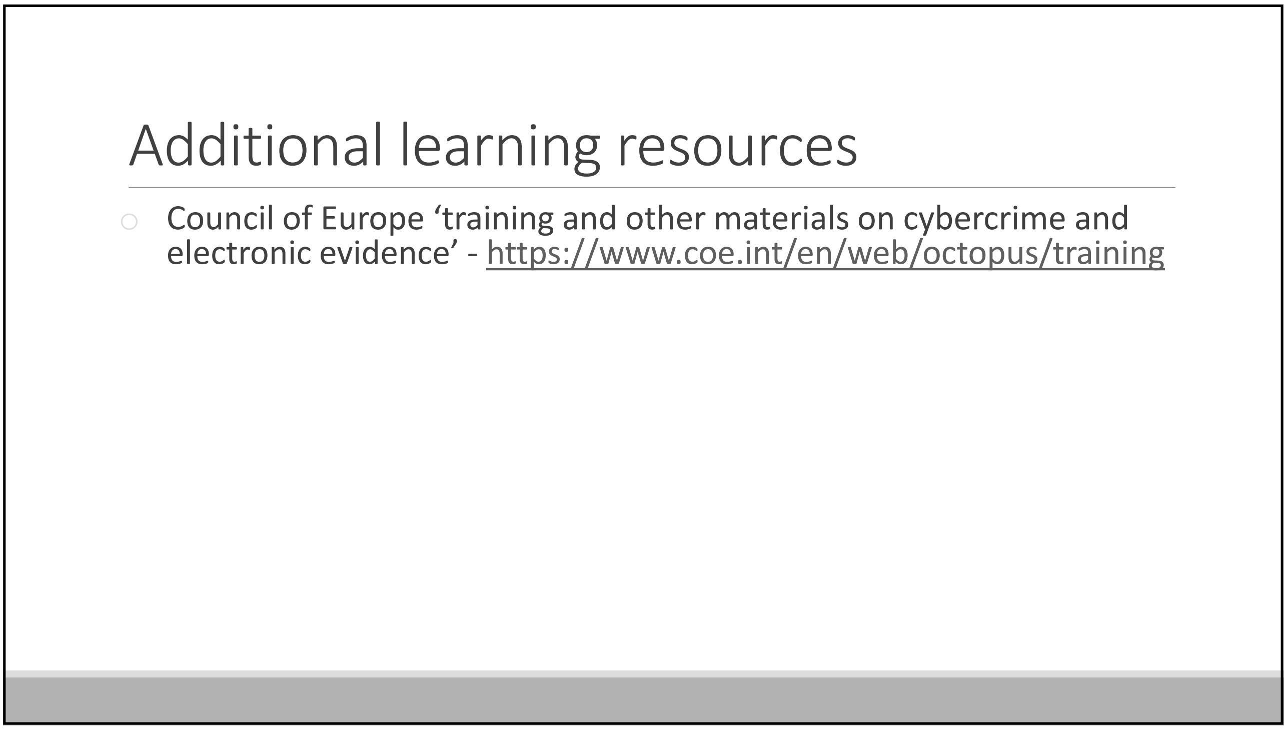
37



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

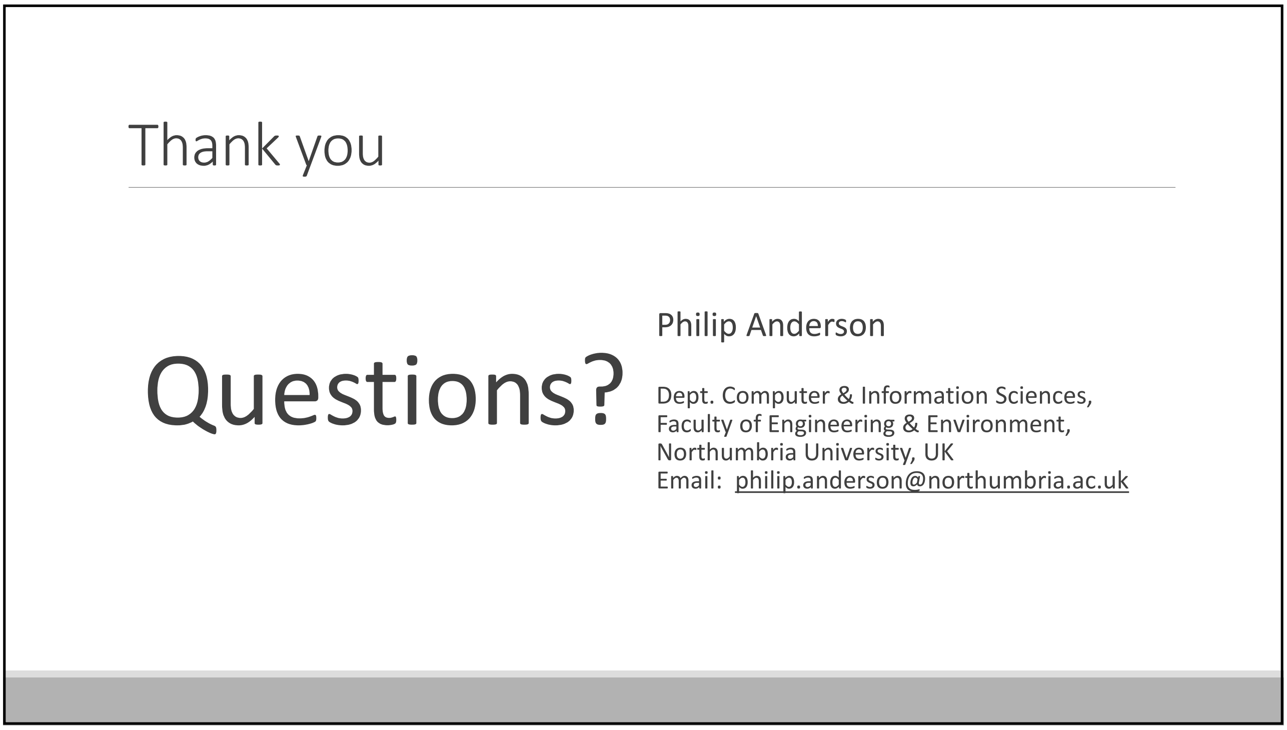
38



Additional learning resources

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

39



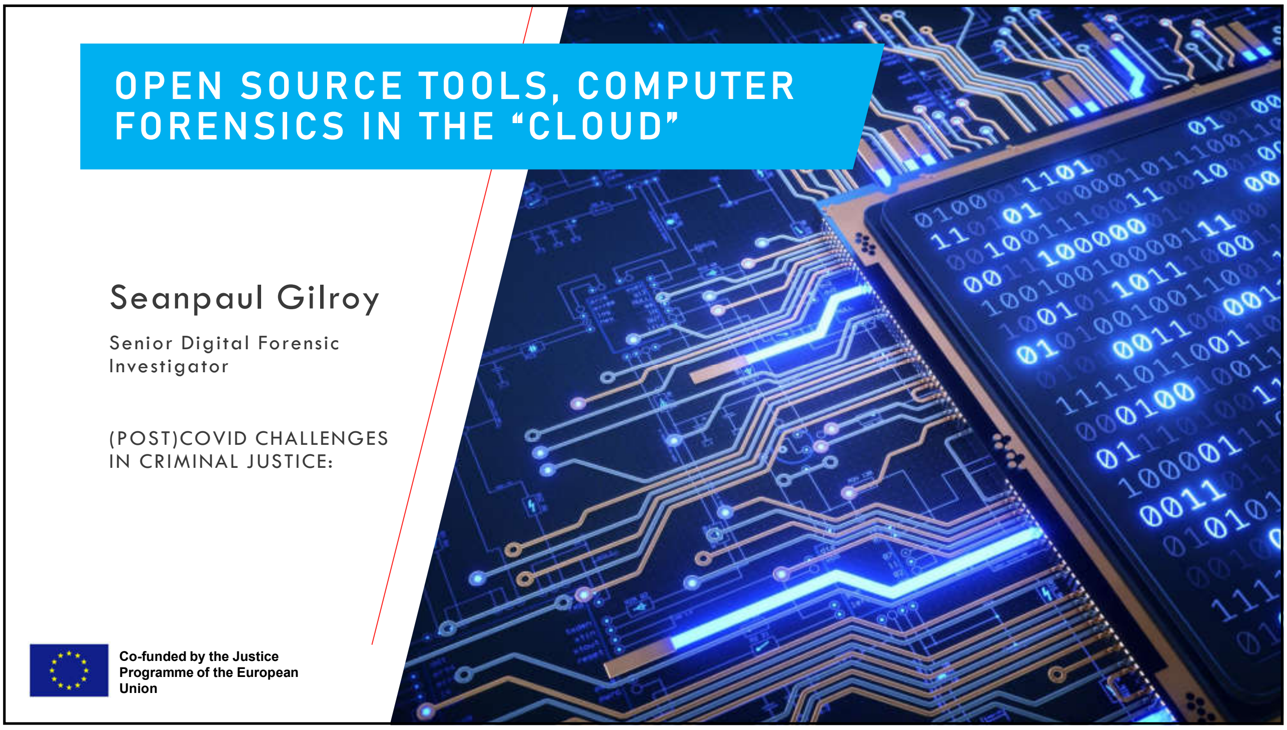
Thank you

Questions?

Philip Anderson

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

40



OPEN SOURCE TOOLS, COMPUTER FORENSICS IN THE “CLOUD”

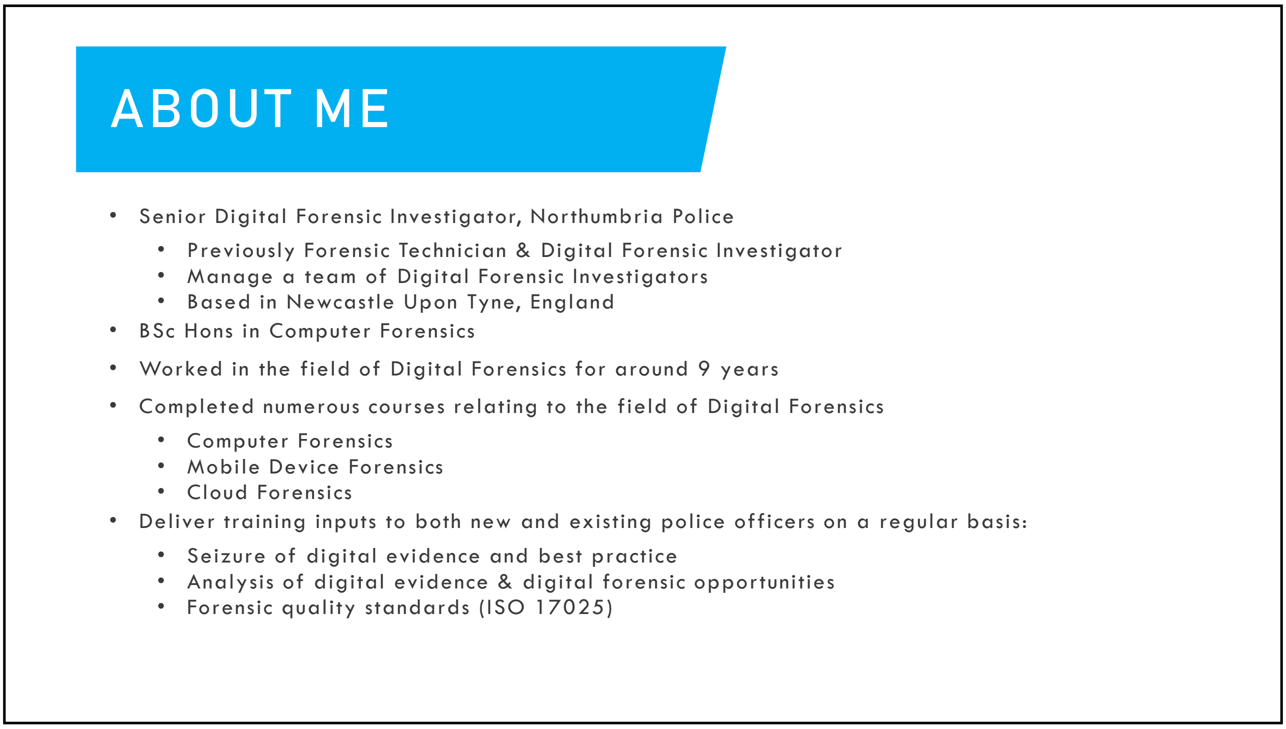
Seanpaul Gilroy

Senior Digital Forensic Investigator

(POST)COVID CHALLENGES IN CRIMINAL JUSTICE:

Co-funded by the Justice Programme of the European Union

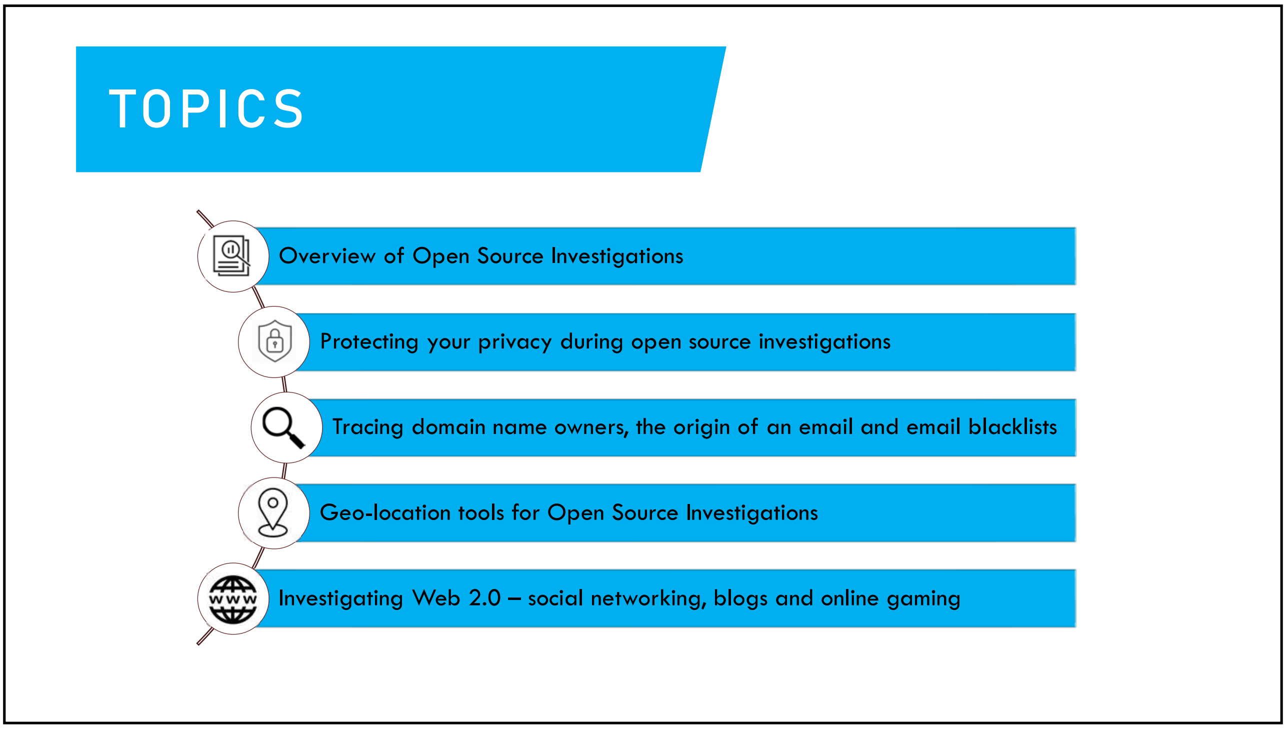
1



ABOUT ME

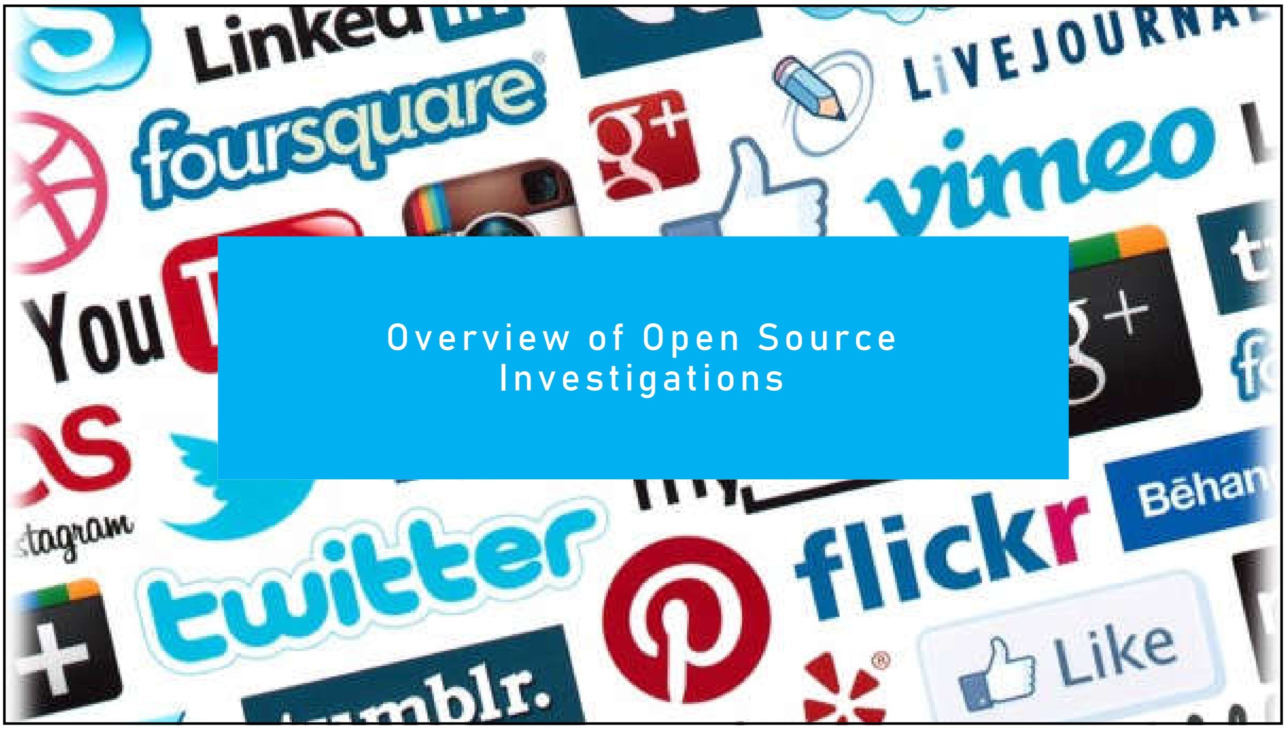
- Senior Digital Forensic Investigator, Northumbria Police
  - Previously Forensic Technician & Digital Forensic Investigator
  - Manage a team of Digital Forensic Investigators
  - Based in Newcastle Upon Tyne, England
- BSc Hons in Computer Forensics
- Worked in the field of Digital Forensics for around 9 years
- Completed numerous courses relating to the field of Digital Forensics
  - Computer Forensics
  - Mobile Device Forensics
  - Cloud Forensics
- 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
  - Forensic quality standards (ISO 17025)

2



TOPICS

- 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



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)

5

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

6

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/Acquisition

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

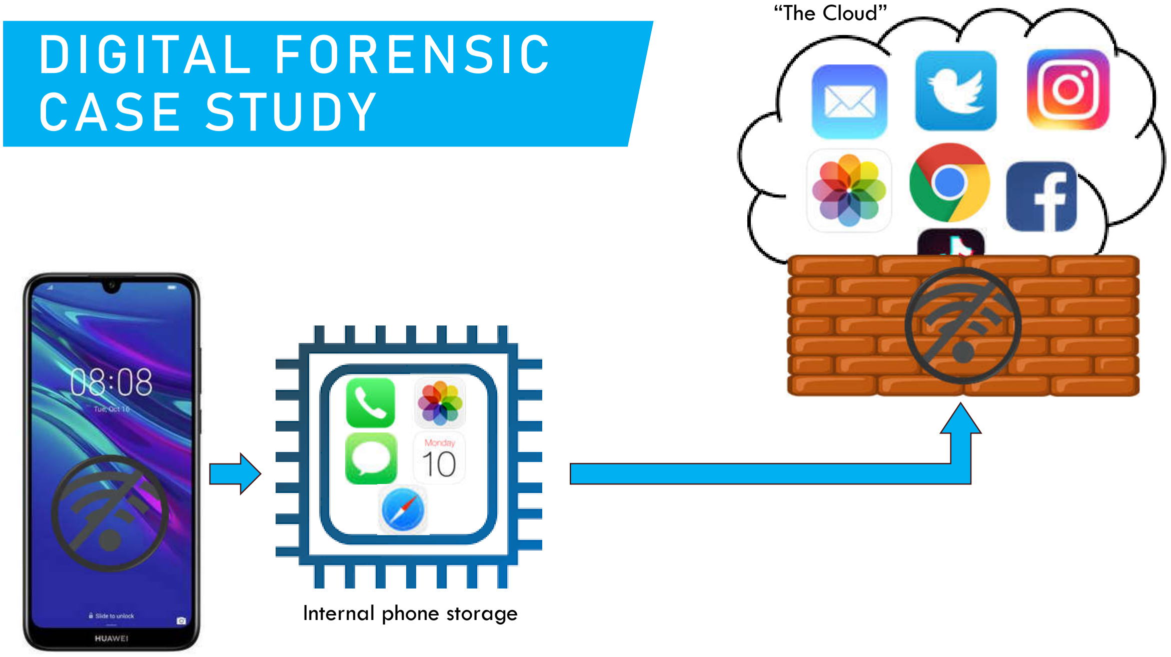
Data Analysis

- Analysis conducted using various 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



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 often to improve the user's experience
  - Can be used for other purposes
- The end user is often unaware that such information is recorded via cookies:

Device name

Usernames/passwords

Download history

IP Address

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

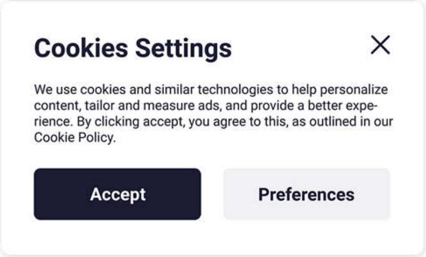
Location Data (longitude and latitude)

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 imperative 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.

11

SGS2

IP ADDRESSES

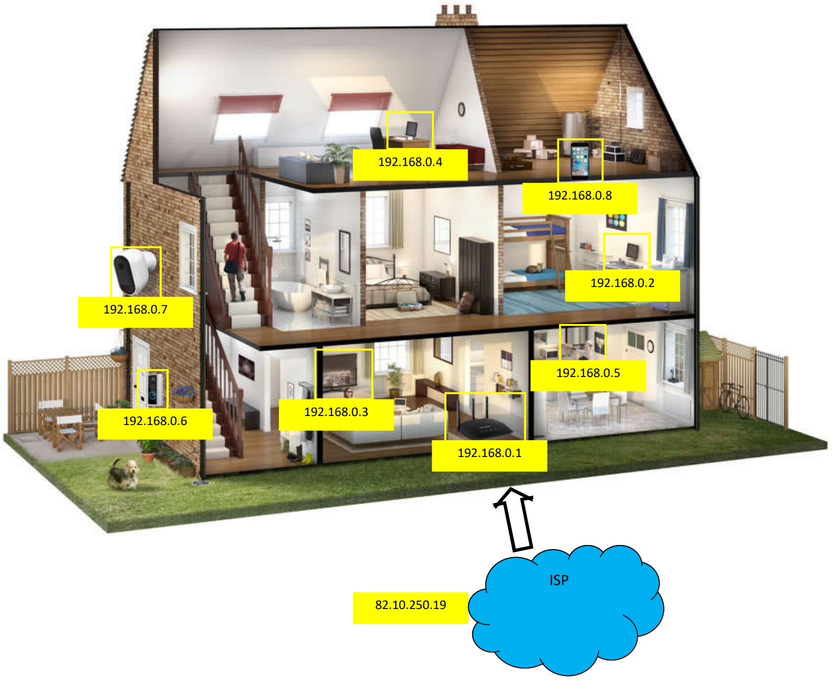
- IP Address is short for Internet Protocol Address.
  - In simple terms it is similar to your home address
  - May look something like 192.188.0.1
- IP Addresses are used to identify digital devices connected to the internet
- When connecting to the internet, the network you use will be allocated a 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

12

Slide 12

SG52 Seanpaul Gilroy 5890, 6 Sep 2022

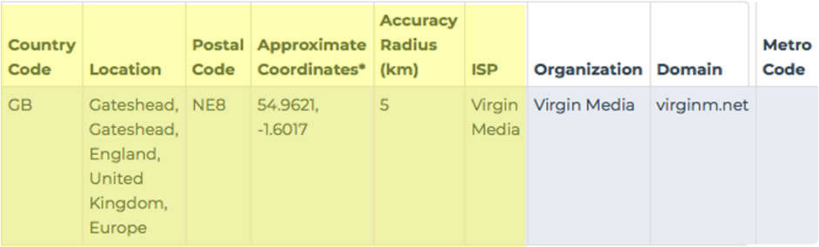


IP ADDRESS EXERCISE

- **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:

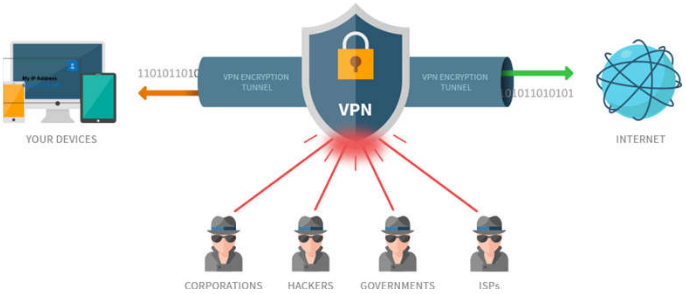


Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
GB	Gateshead, Gateshead, England, United Kingdom, Europe	NE8	54.9621, -1.6017	5	Virgin Media	Virgin Media	virginm.net	

- 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.



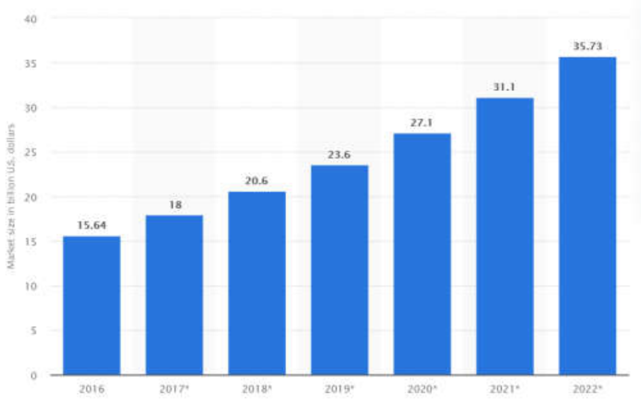
VIRTUAL PRIVATE NETWORKS

- 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)

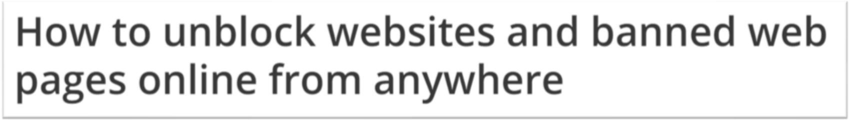


VIRTUAL PRIVATE NETWORKS

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

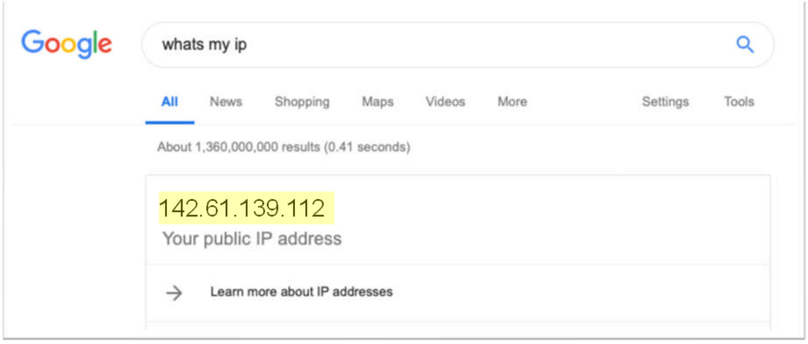
VIRTUAL PRIVATE NETWORKS – EXERCISE

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)



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

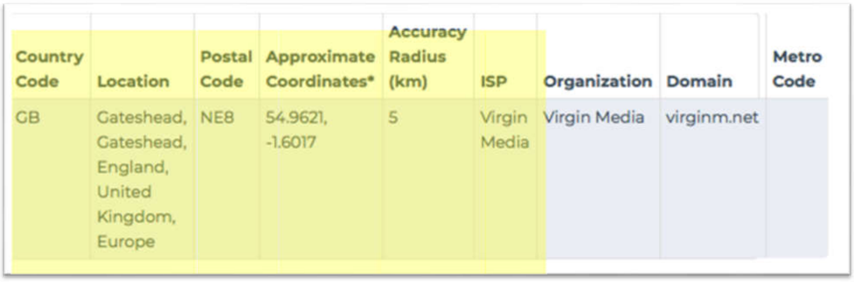
142.61.139.112

Your public IP address

Learn more about IP addresses

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 2) Enter your IP into Maxmind

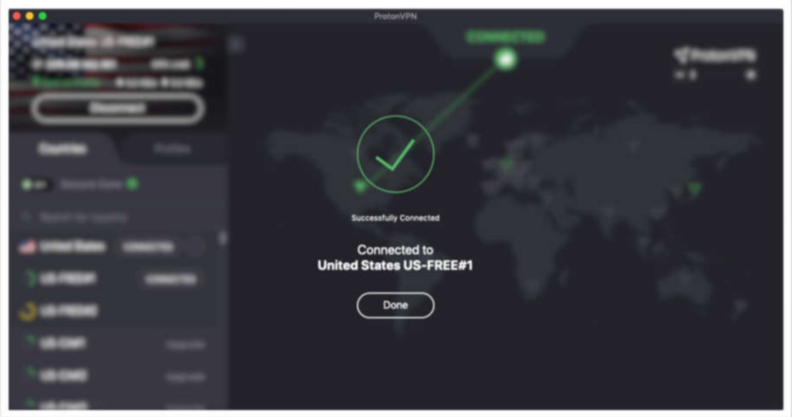


Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
GB	Gateshead, Gateshead, England, United Kingdom, Europe	NE8	54.9621, -1.6017	5	Virgin Media	Virgin Media	virginm.net	

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 3) Register and Download Proton VPN

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

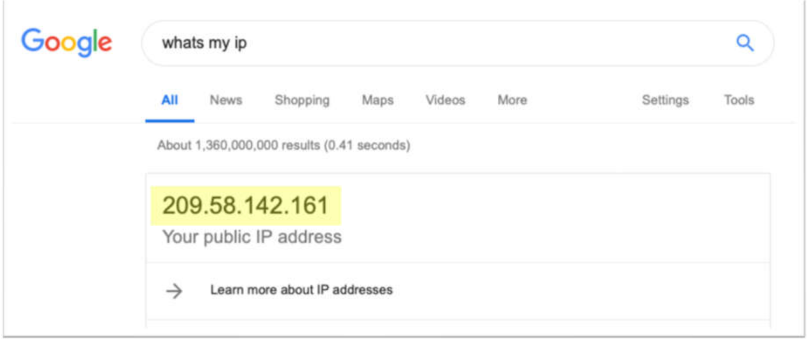


Successfully Connected

Connected to
United States US-FREE#1

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 5) Identify your IP address



whats my ip

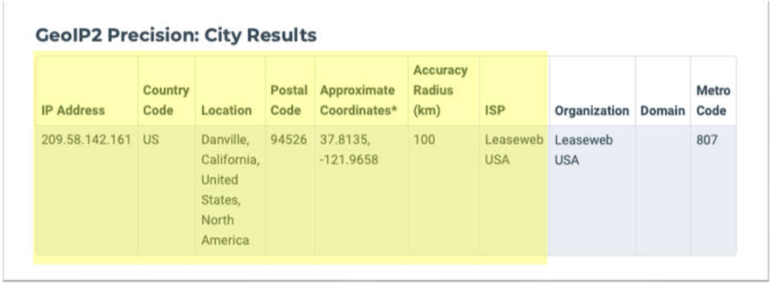
About 1,360,000,000 results (0.41 seconds)

209.58.142.161
Your public IP address

Learn more about IP addresses

VIRTUAL PRIVATE NETWORKS – EXERCISE

Step 6) Enter your new IP into Maxmind



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?

9/20/2023

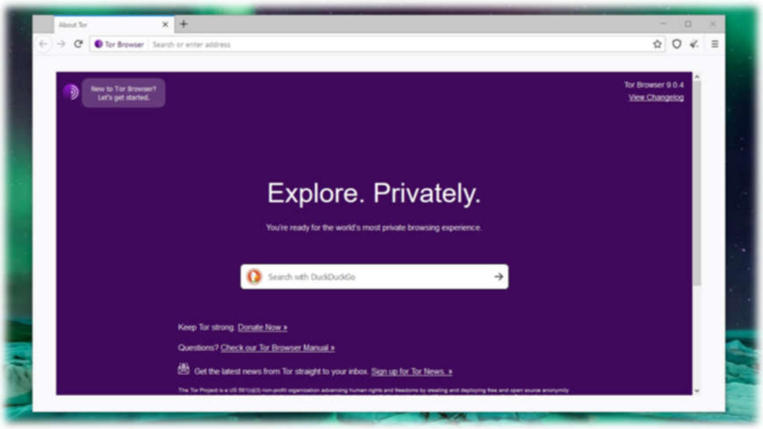
TOR BROWSER

- 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

9/20/2023

TOR BROWSER

- The browser looks very similar to other common web browsers



About Tor

Tor Browser | Search or enter address

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.

Search with DuckDuckGo

Keep Tor strong. Donate Now »

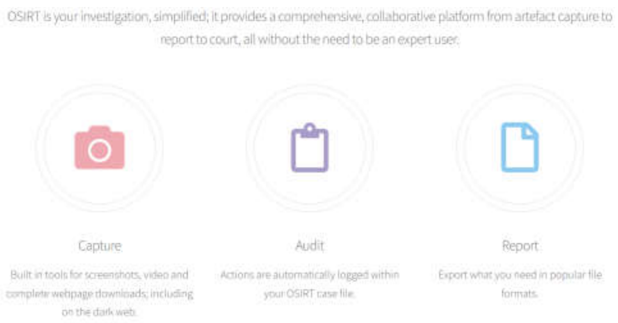
Questions? Check our Tor Browser Manual »

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 being launched 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.

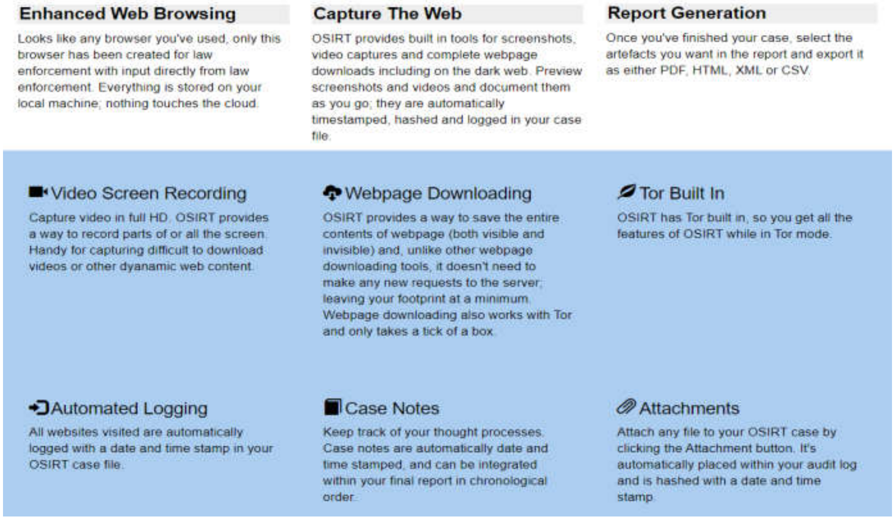
Audit

Actions are automatically logged within your OSIRT case file.

Report

Export what you need in popular file formats.

OSIRT BROWSER



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.

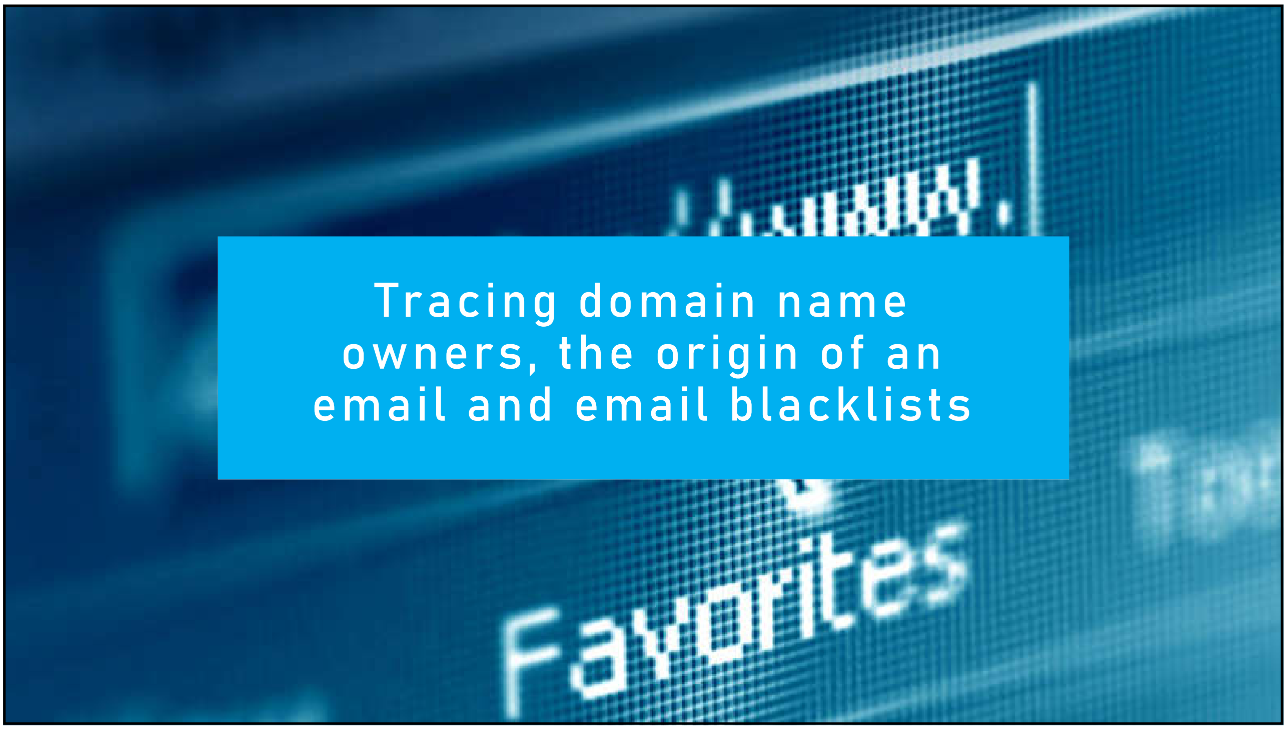
Case Notes

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.

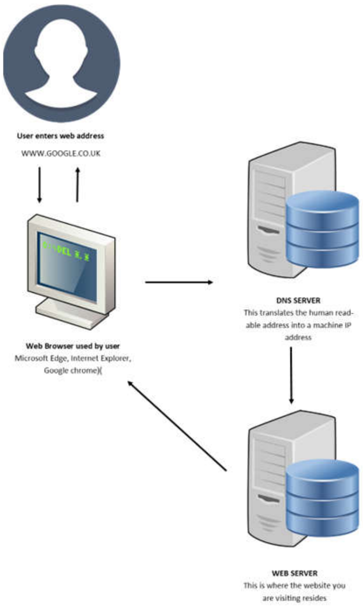
9/20/2023



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

DOMAIN NAMES

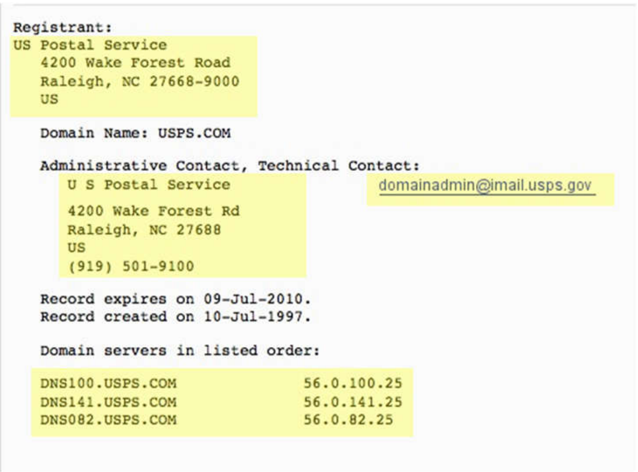
- What is a domain name?
  - A domain name is a unique name of identifying a website
  - Remember IP addresses?
    - 212.58.226.75 > www.bbc.co.uk/news
  - It is a user friendly version of an IP address
  - It would be virtually impossible to remember the IP addresses for all of your favorite websites
- 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

9/20/2023

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

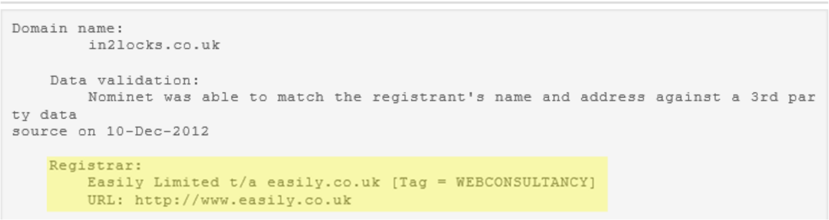


```
Registrant:
US Postal Service
   4200 Wake Forest Road
   Raleigh, NC 27668-9000
   US

   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
```

9/20/2023

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



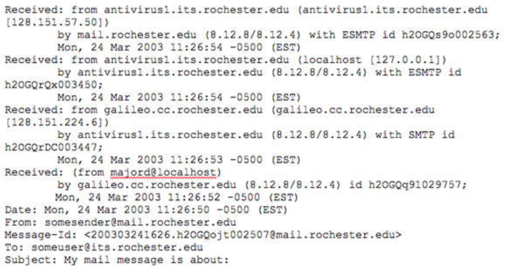
```
Domain name:
        in2locks.co.uk

    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, which can contain hidden information which is useful during an open source investigations
- An email contains two main parts
  - The body of the message (The section the we see as a general user)
  - The header (The hidden bit – of interest to investigators)
- A header is responsible for ensuring the email is delivered to the correct person.
  - Similar 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

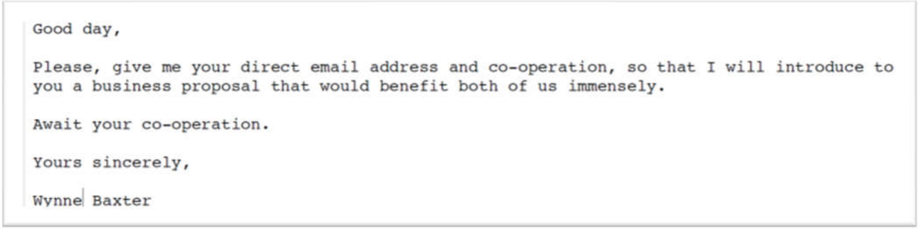
- Often difficult to interpret, until we understand the different areas of interest
  - **Content-Type:** Notes whether the email is HTML or plain text.
  - **Date:** When the email was written.
  - **Delivery Date:** When the email was received by your mail server.
  - **From:** Who sent the email.
  - **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.

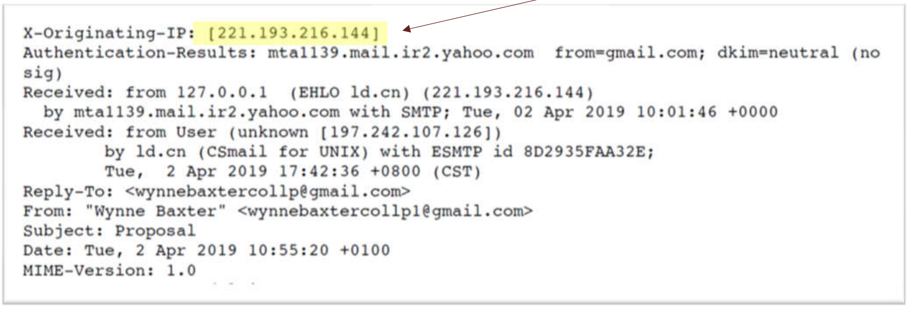
Await your co-operation.

Yours sincerely,

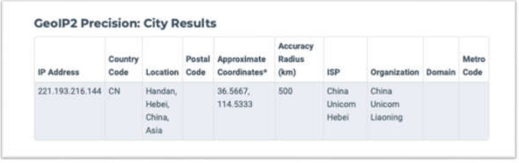
Wynne Baxter

EMAIL HEADERS – EXERCISE 1

Remember: this could be assigned by a VPN



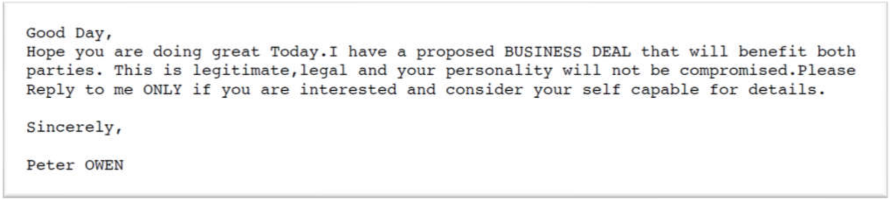
```
X-Originating-IP: [221.193.216.144]
Authentication-Results: mta1139.mail.ir2.yahoo.com  from=gmail.com; dkim=neutral (no
sig)
Received: from 127.0.0.1  (EHLO ld.cn) (221.193.216.144)
  by mta1139.mail.ir2.yahoo.com with SMTP; Tue, 02 Apr 2019 10:01:46 +0000
Received: from User (unknown [197.242.107.126])
        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		

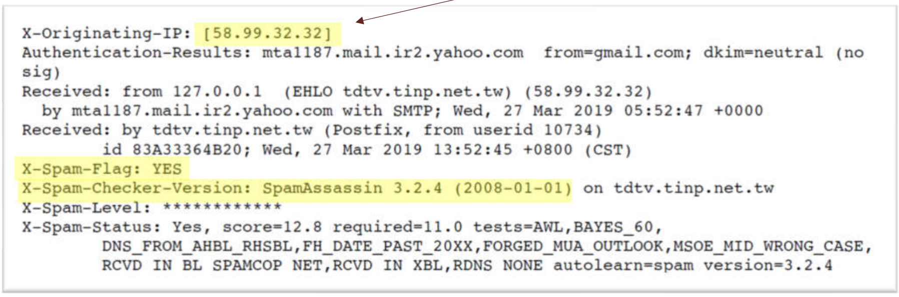
EMAIL HEADERS – EXERCISE 2



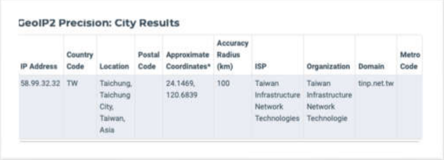
```
Good Day,
Hope you are doing great Today.I have a proposed BUSINESS DEAL that will benefit both
parties. This is legitimate,legal and your personality will not be compromised.Please
Reply to me ONLY if you are interested and consider your self capable for details.

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
```

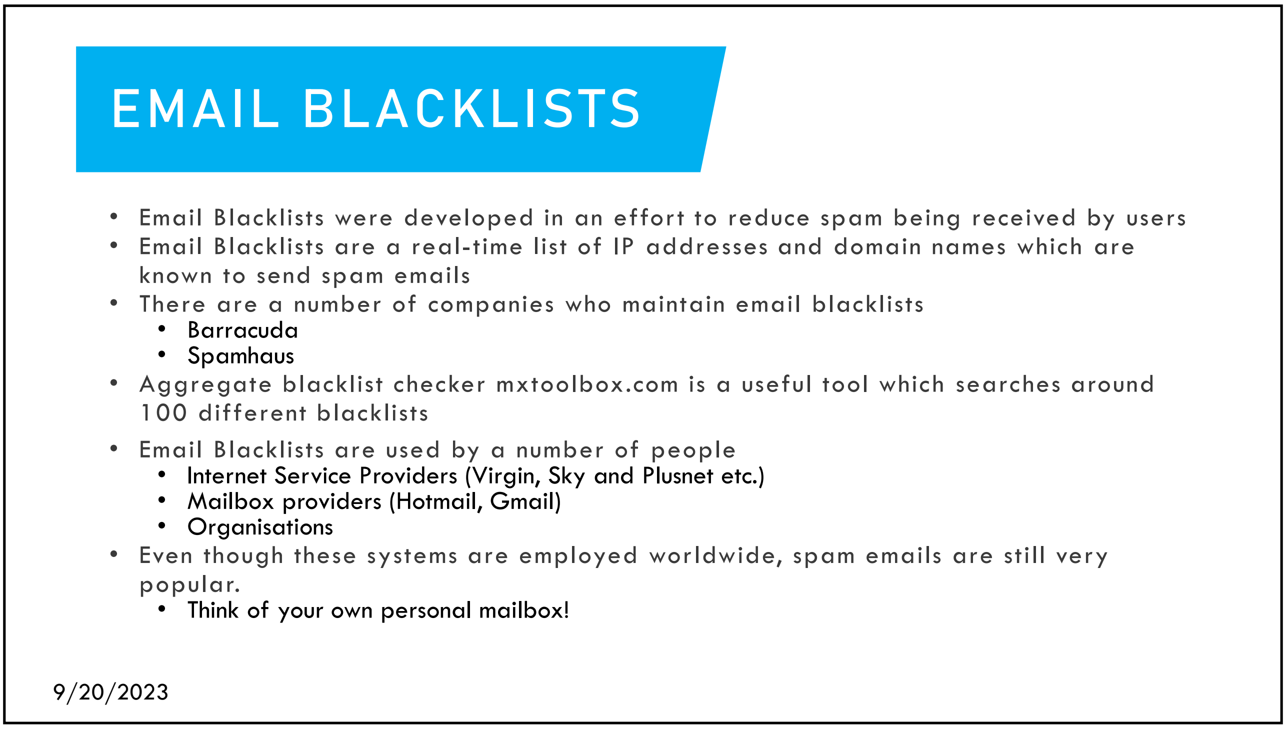


GeoIP2 Precision: City Results

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
  - Unsolicited messages sent in bulk by email.
- Spam emails 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
- Cisco reported in April 2019
  - Average Daily Legitimate Emails 72.56 Billion
  - Average Daily Spam Volume 416.78 Billion
- Statista reported:
  - Between October 2020 and September 2021, global daily spam volume reached its highest point in July 2021, with almost 283 billion spam emails from a total of 336.41 billion sent emails



EMAIL BLACKLISTS

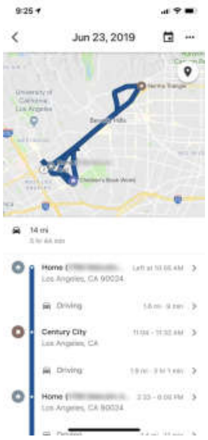
- Email Blacklists were developed in an effort to reduce spam being received by users
- Email Blacklists are a real-time list of IP addresses and domain names which are known to send spam emails
- There are a number of companies who maintain email blacklists
  - Barracuda
  - Spamhaus
- Aggregate blacklist 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.
  - Think of your own personal mailbox!

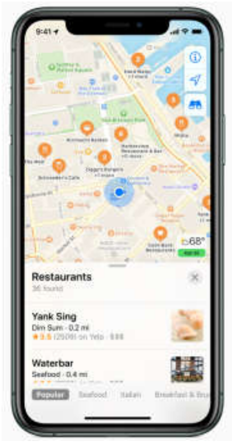
9/20/2023

Geo-location tools for Open Source Investigations

GEO-LOCATION

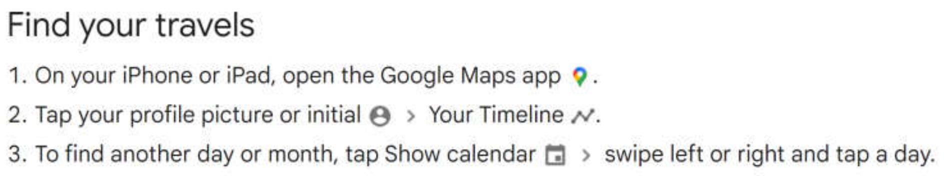
- Geo-location is defined as a technique of identifying the geographical location of a person/device using digital data.
    - Geolocation data can be found within various forms of digital data including:
        - Photographs
        - Social Media
        - Video
        - Posts
- Digital devices record 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
- Think of your own Google Maps account, how much data do they hold about you?





GOOGLE MAPS EXAMPLE

Who in this room uses Google Maps?

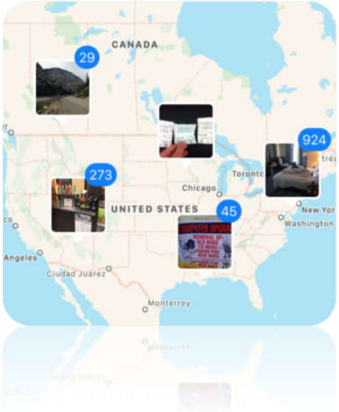


Find your travels

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.
  - However these tools are often expensive
- There are various 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

9/20/2023

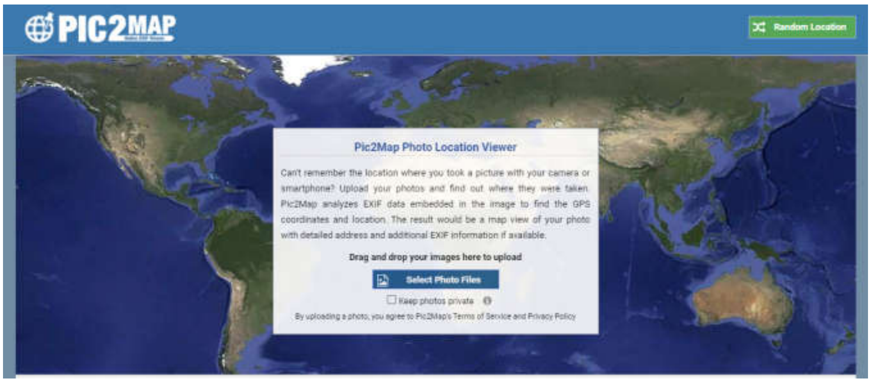
EXIF DATA EXERCISE

- Filename: IMG_3561.JPG

9/20/2023

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

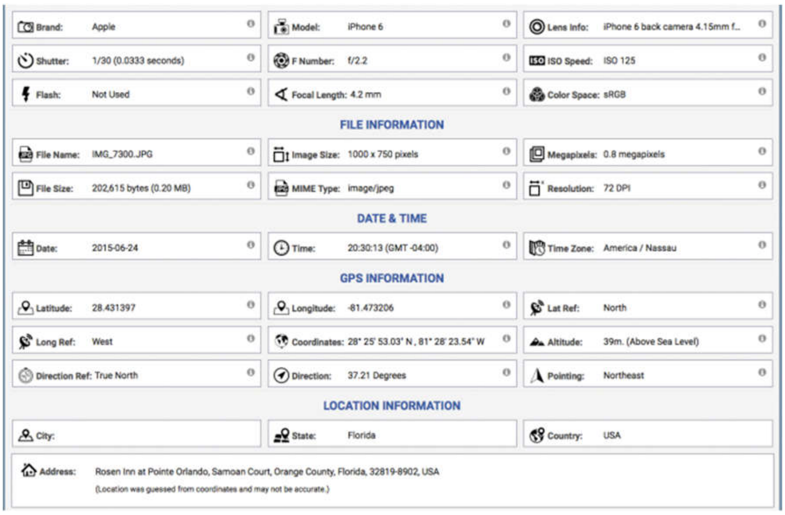
Select Photo Files

□ 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

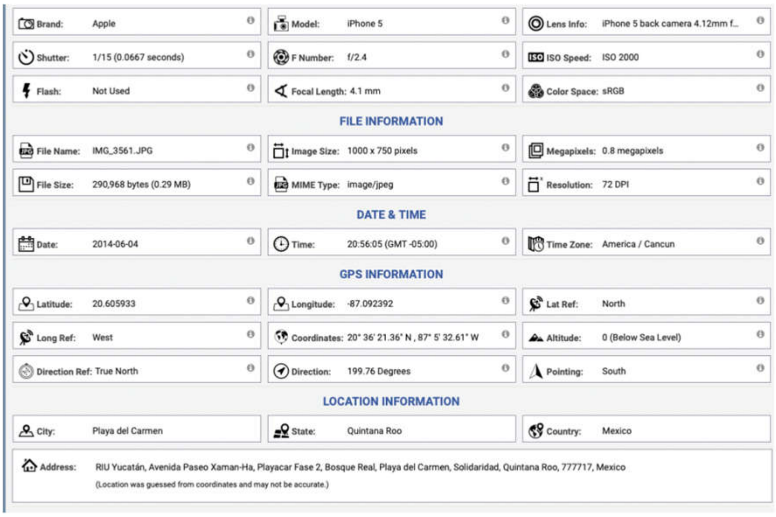
LOCATION INFORMATION

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

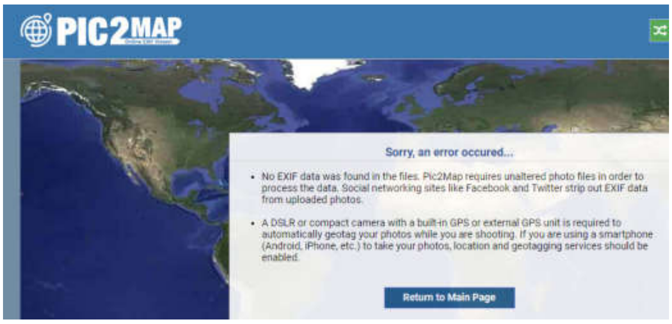
LOCATION INFORMATION

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

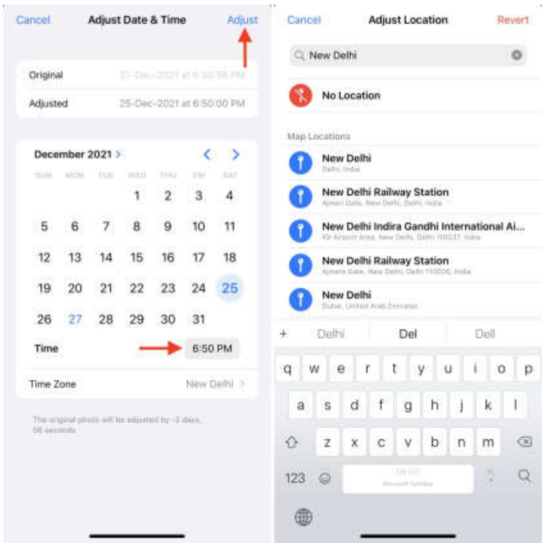


Sorry, an error occured...

- 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:
  - No specialist tool is required
- Where possible, may need to be corroborated with other evidence
  - Examine the original photographs
    - Not a copy of the photograph which has been sent through WhatsApp or Facebook Messenger etc.
    - In order to reduce file size, these applications often strip the metadata from files



Original 27-Dec-2021 at 6:30:56 PM

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

Time 6:50 PM

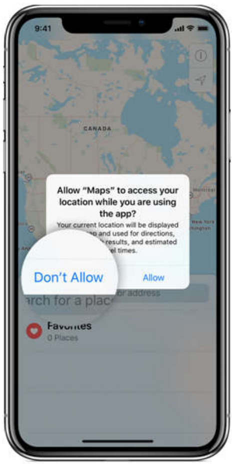
Time Zone New Delhi

New Delhi

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

TWITTER

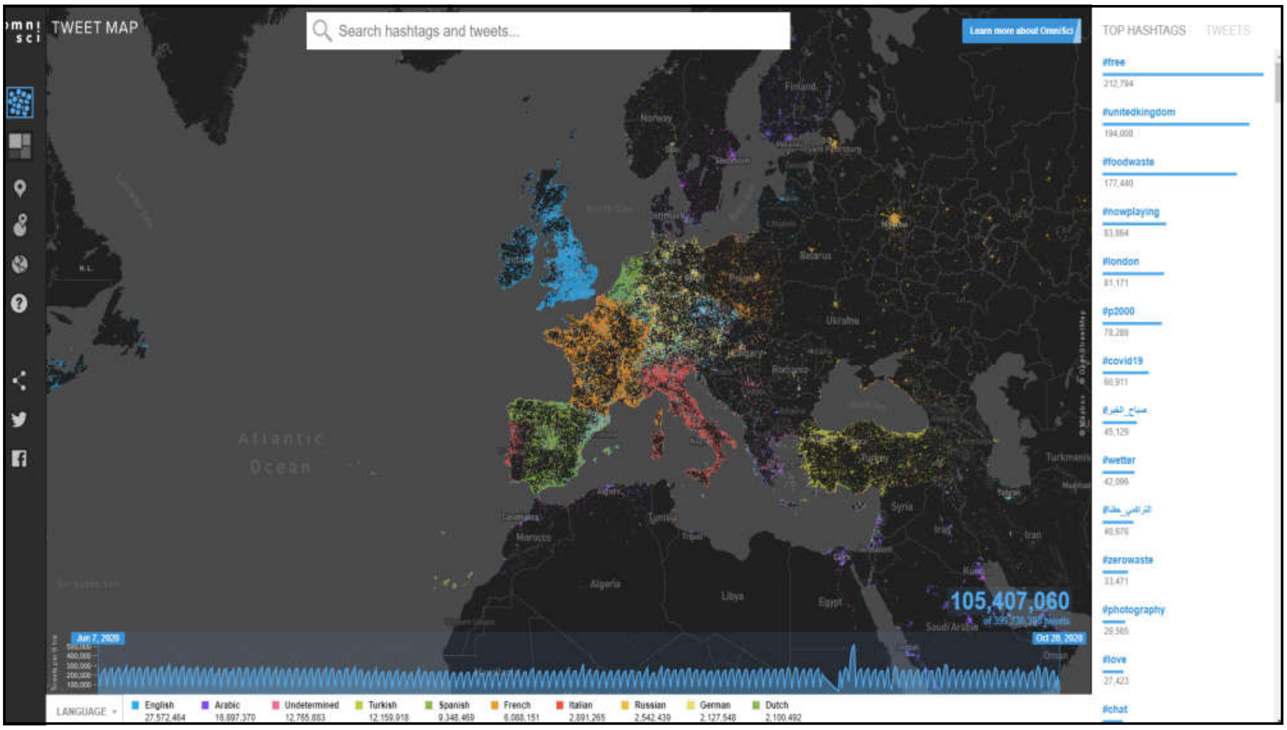
- Statista forecasts that in 2023, Twitter will have 465 million active users
  - UK Population in 2017 was 66 million people
- Social network commonly used and can be a rich source of information
- Users are often unaware that social media tracks lots of data useful to an investigator
  - A lot of people (myself included) just press “Allow” when installing a new application
- Twitter 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


9:41
CANADA
Allow “Maps” to access your location while you are using the app?
Don't Allow
Allow
Favorites

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 Twitter 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.

9/20/2023



TOP HASHTAGS TWEETS

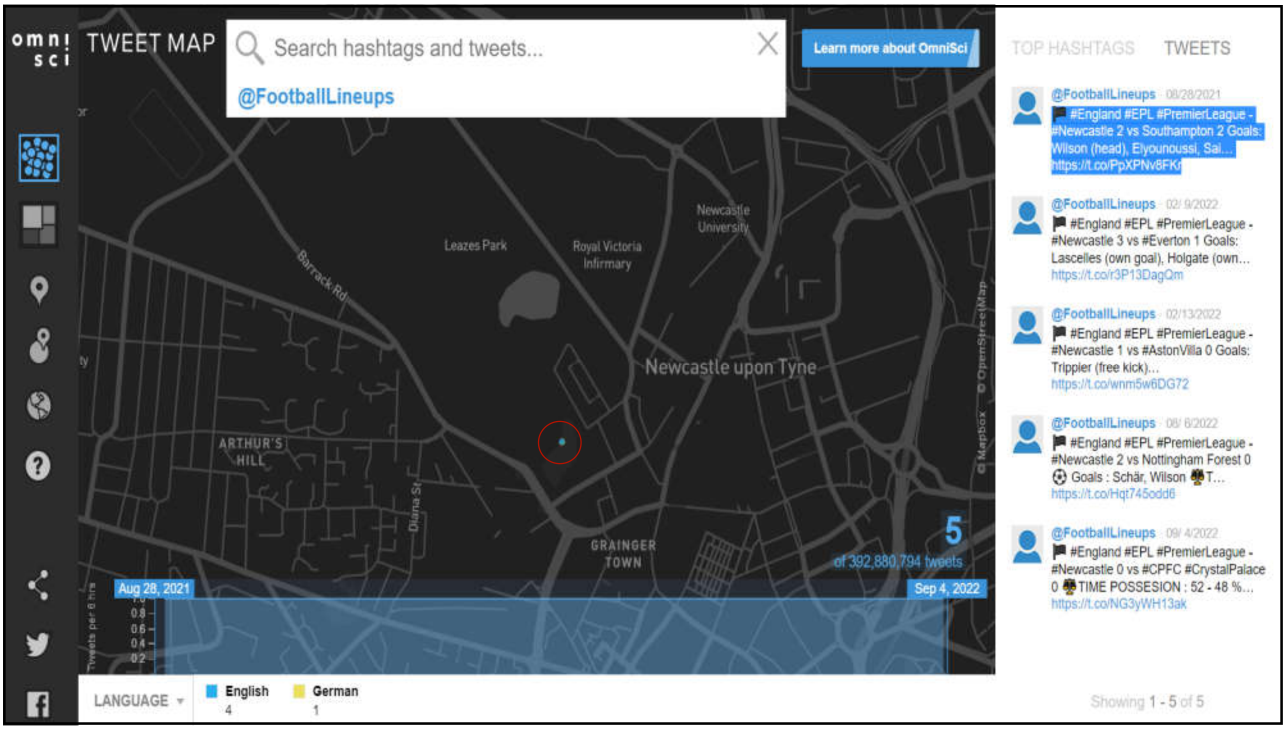
#free 212,794
#unitedkingdom 194,000
#foodwaste 177,440
#nowplaying 83,864
#london 81,171
#p2000 78,289
#covid19 60,911
#صباح_الخير 45,129
#wetter 42,096
#الراقي_بفكره 40,676
#zerowaste 33,471
#photography 29,565
#love 27,423
#chat

LANGUAGE

English	Arabic	Undetermined	Turkish	Spanish	French	Italian	Russian	German	Dutch
27,572,464	18,897,370	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 (TWITTER) 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 08/28/2021
🏴 #England #EPL #PremierLeague - #Newcastle 2 vs Southampton 2 Goals: Wilson (head), Elyounoussi, Sai... https://t.co/PpXPNv8FKr

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

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

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

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

Showing 1 - 5 of 5

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 tocommunicate 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

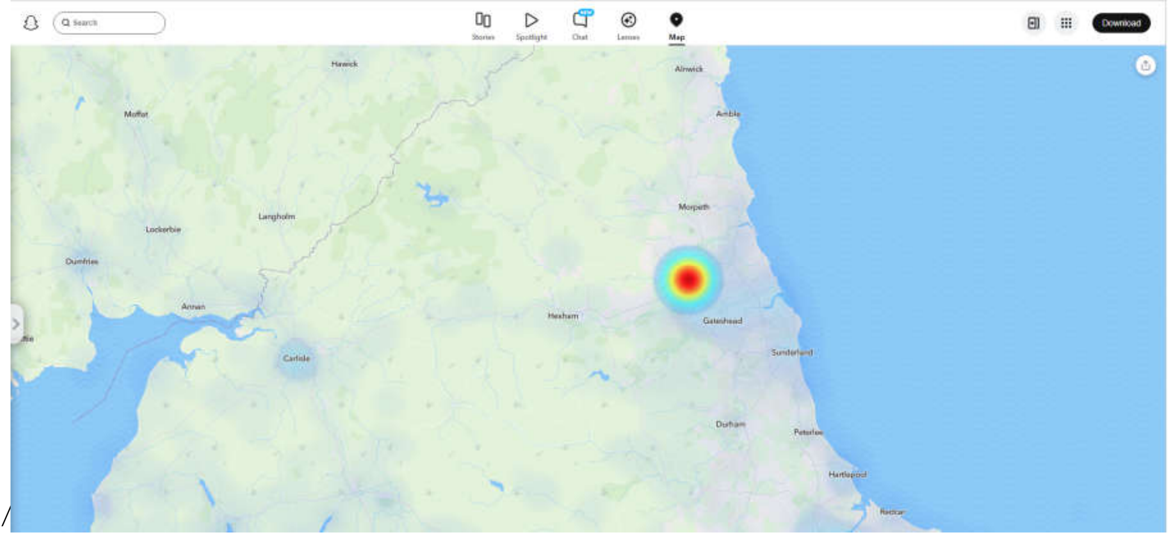
Jenae Barnes Former Staff

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)
- Users can use Ghost mode to hide their location and choose no to share their Stories to the public Snap Map.
- Press stories regarding the app being used to recruit drug dealers
    - County Lines Offences

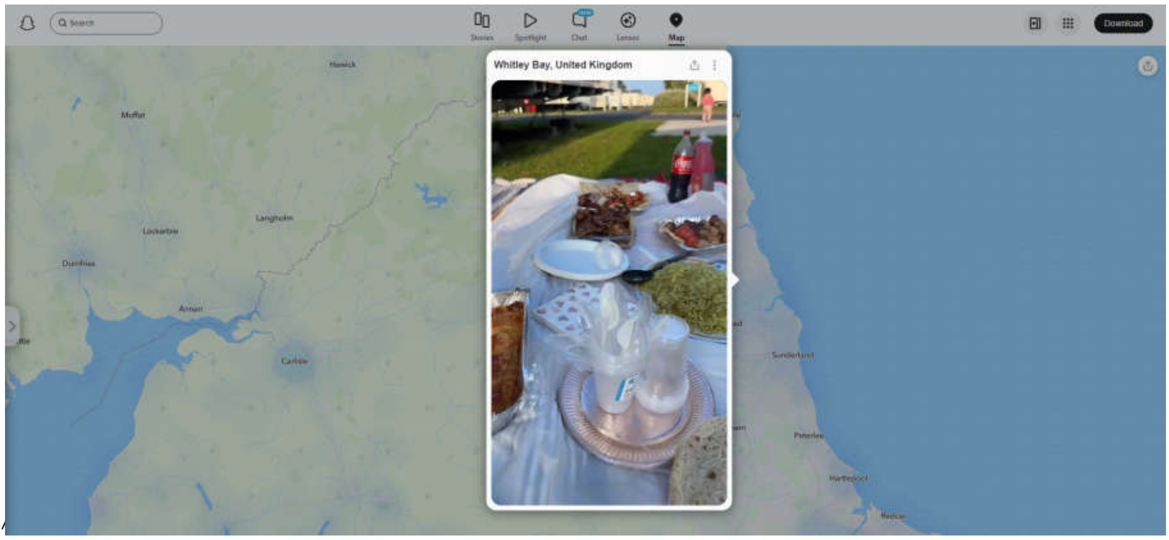
SNAP MAP



9/

61

SNAP MAP



Whitley Bay, United Kingdom

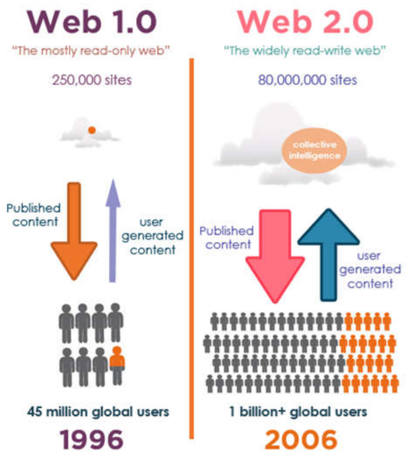
9/

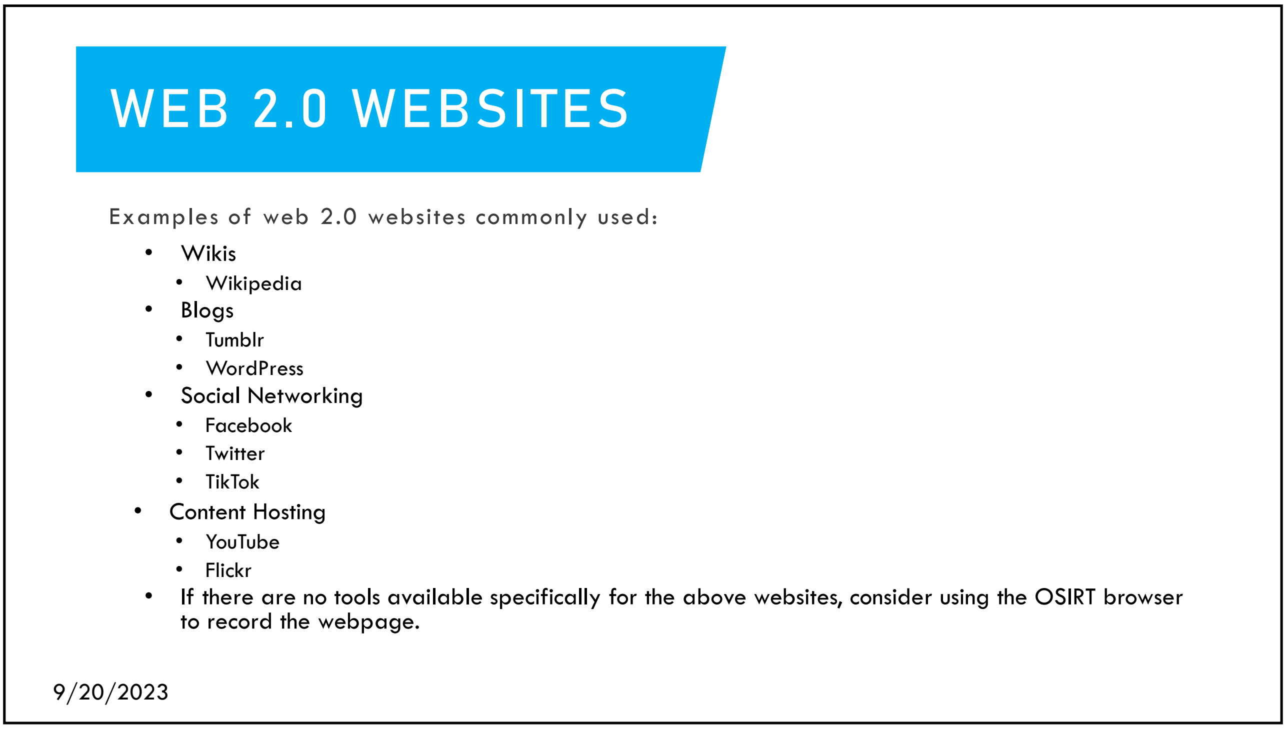
62

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.

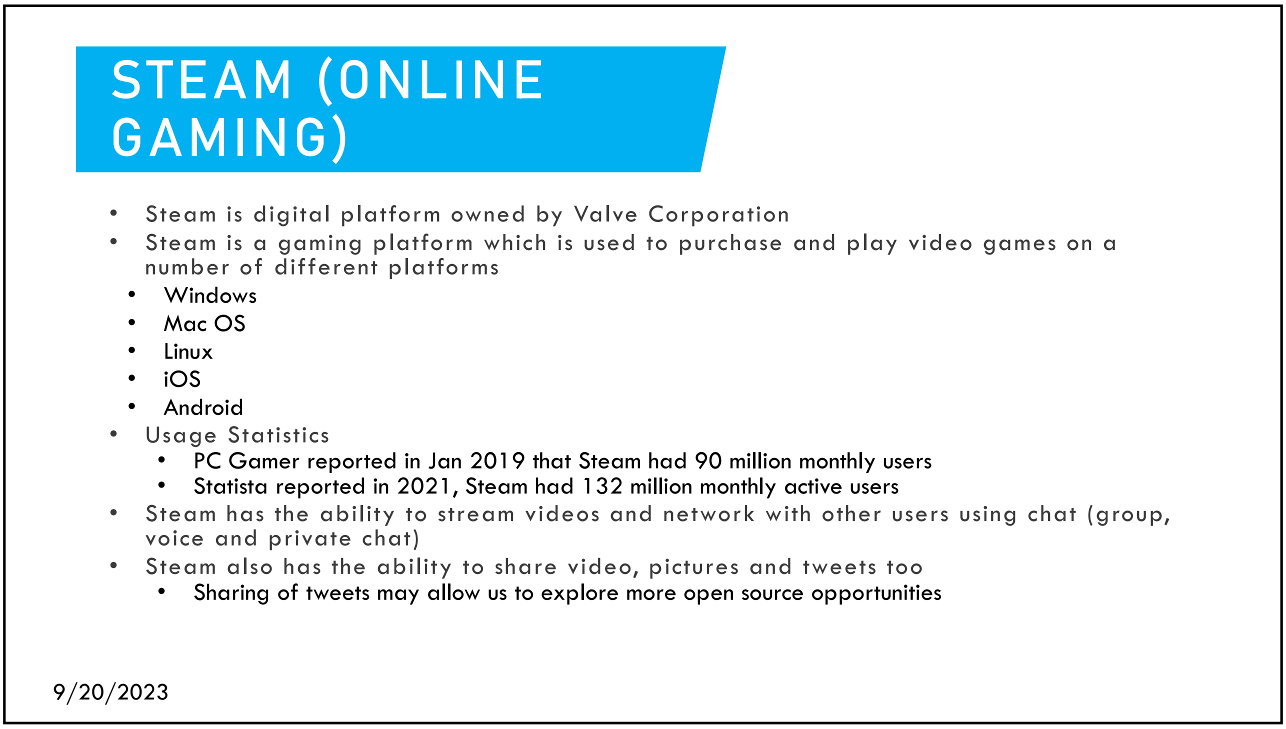




WEB 2.0 WEBSITES

Examples of web 2.0 websites commonly used:

- Wikis
  - Wikipedia
- Blogs
  - Tumblr
  - WordPress
- Social Networking
  - Facebook
  - Twitter
  - TikTok
- Content Hosting
  - 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)

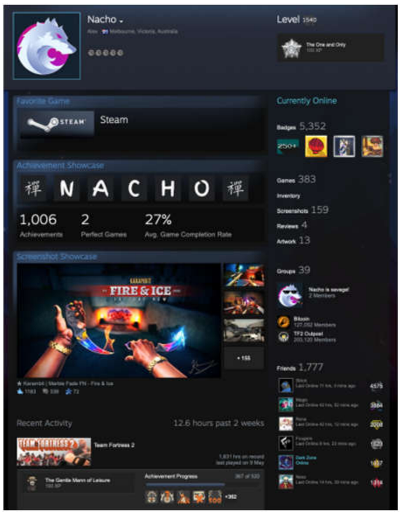
- Steam is digital platform owned by Valve Corporation
- Steam is a gaming platform which is used to purchase and play video games on a number of different platforms
  - Windows
  - Mac OS
  - Linux
  - iOS
  - Android
- Usage Statistics
  - PC Gamer reported in Jan 2019 that Steam had 90 million monthly users
  - Statista reported in 2021, Steam had 132 million monthly active users
- 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

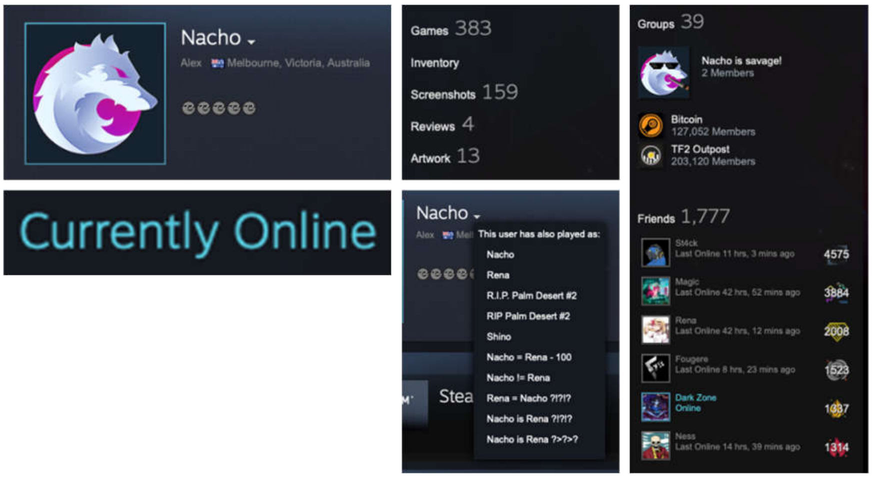
9/20/2023

STEAM USERNAME "NACHO"



9/20/2023

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	1337
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 Facebook
- 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

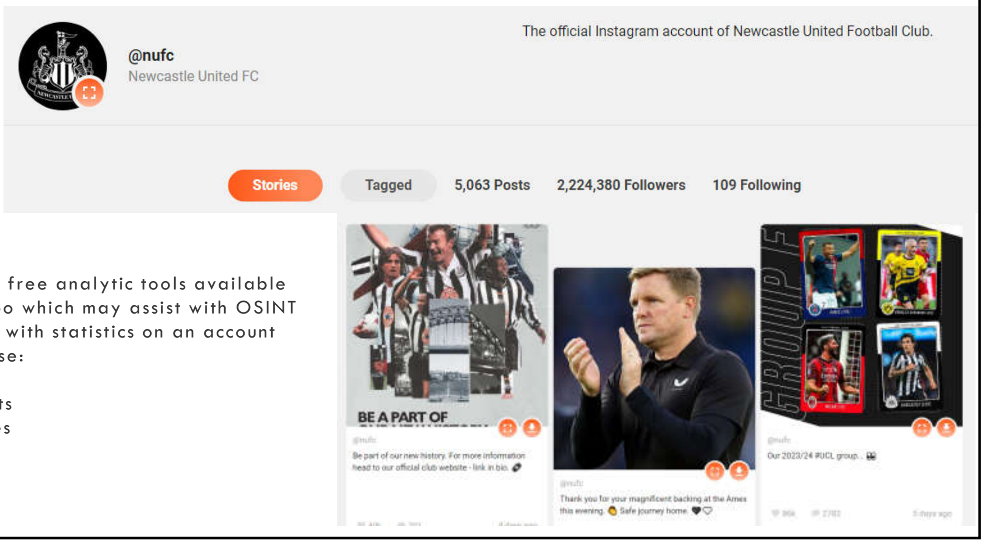
Can we see the profile?

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

9/20/2023

INSTAGRAM EXERCISE



@nufc

Newcastle United FC

The official Instagram account of Newcastle United Football Club.

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

@nufc

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

@nufc

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

@nufc

Our 2023/24 #UCL group...

5 days ago

- 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

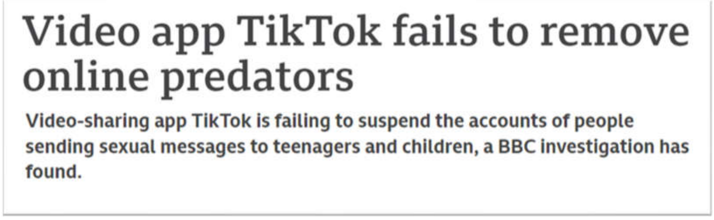
9/20/2023

FACEBOOK

- Facebook is another commonly used social network
- Statista reported in Q2 of 2022, Facebook had 2.9 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 user 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.
- 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
- Facebook are strict with accounts (Often close accounts)

TIKTOK

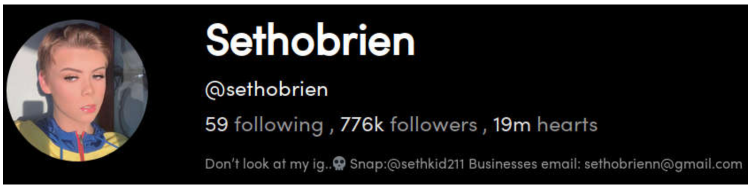
- TikTok is a social video app that allows users to share short videos.
  - Become very popular during COVID-19 lockdown
- Statista reported that TikTok have approximately 1.7 billion users worldwide
  - Up by over 66% when compared to 2020
- The application allows users to comment on videos and also 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

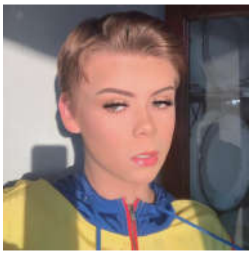


Sethobrien

@sethobrien

59 following , 776k followers , 19m hearts

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

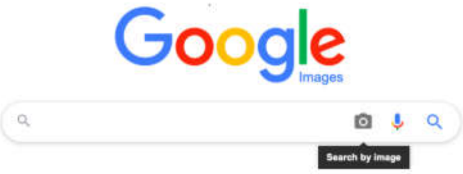


9/20/2023

75

TIKTOK EXERCISE

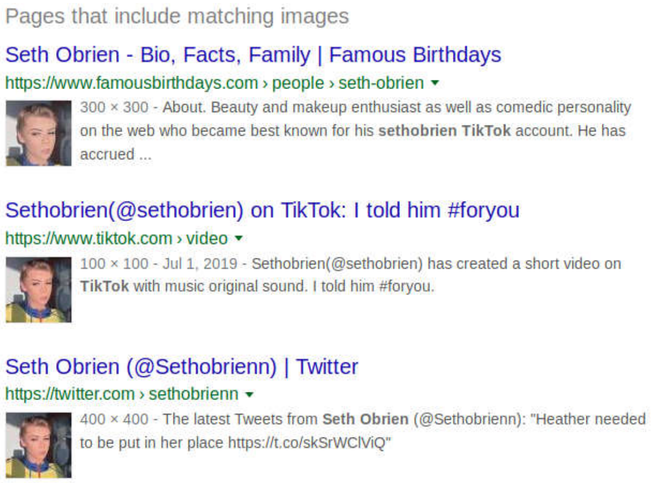
- There aren't always tools available to assist in open source investigations for a particular website
- Don't forget about the power of search engines
  - Google
  - Bing
- Conducting a reverse image search of the TikTok profile picture may assist us



9/20/2023

76

TIKTOK EXERCISE



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"

9/20/2023

77

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

9/20/2023

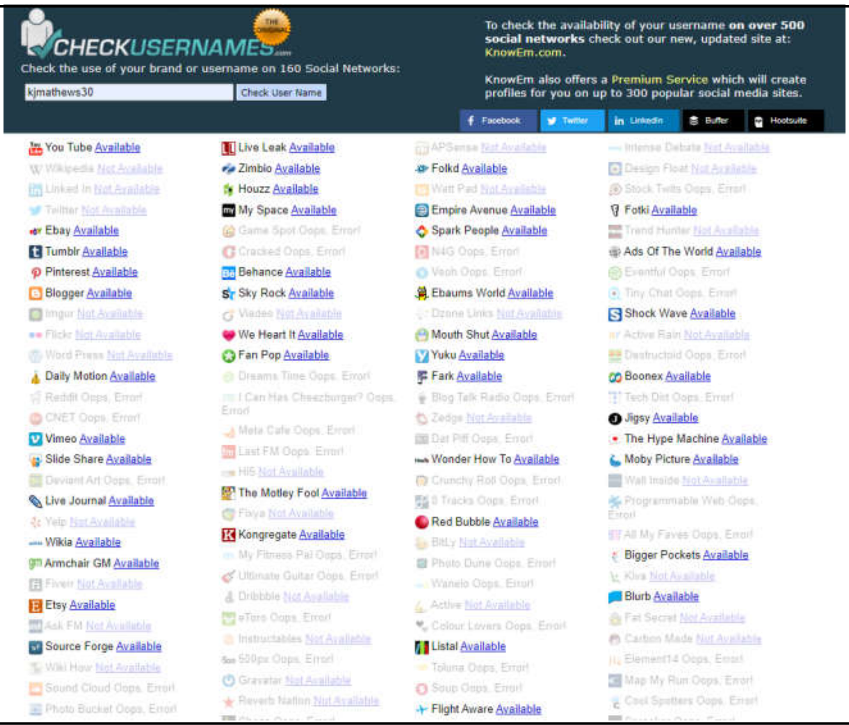
78

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
  - 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

9/20/2023

79



CHECKUSERNAMES.com

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!

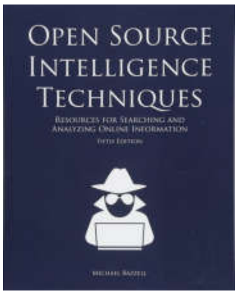
80

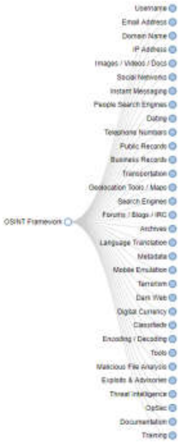
OPEN SOURCE INVESTIGATION CHALLENGES

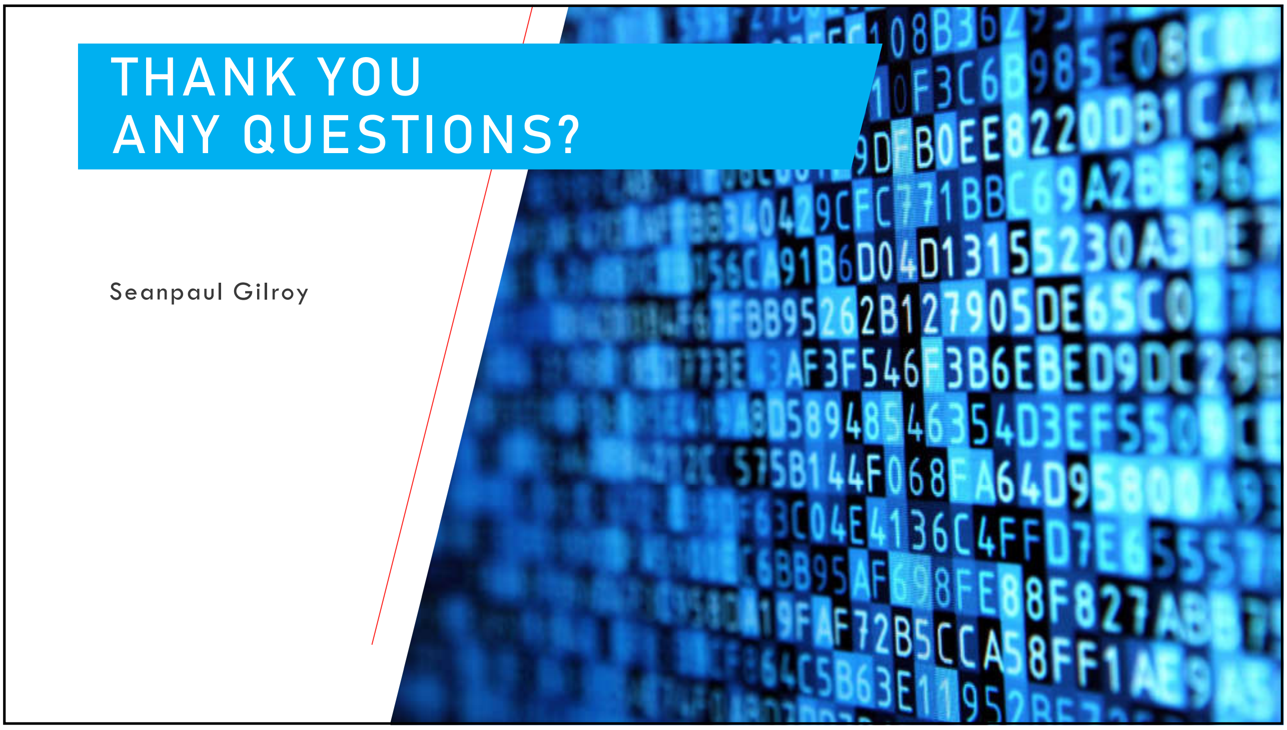
- There are a number challenges in relation to open source investigations
  - Legislation (cross-borders)
    - The techniques are available, but are they legal?
    - Do you need a DSA or equivalent?
  - Online platforms regularly change their functionality
    - It is not uncommon for applications 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

RESOURCES

- The Ultimate OSINT Collection - start.me
- OSINT Framework
- Open Source Intelligence Techniques – Book
- UK-OSINT
- Inteltechniques.com


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





THANK YOU ANY QUESTIONS?

Seanpaul Gilroy

Co-funded by the European Union

ROSINUS PARTNER

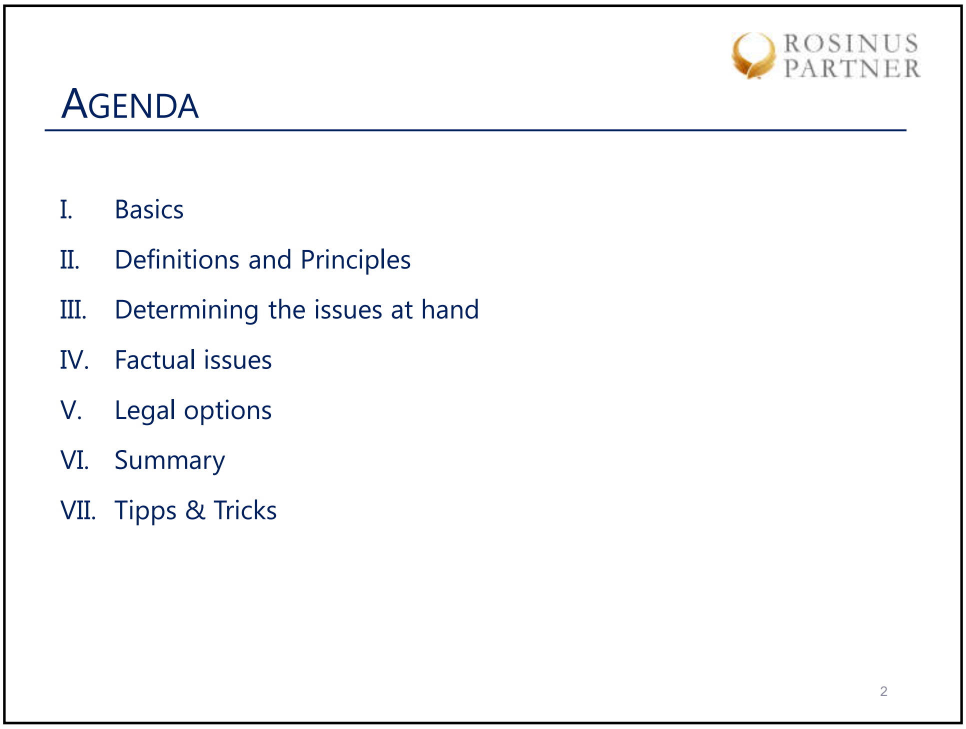
An overview of the defence rights related issues regarding the use of e- evidence collected on the internet

Presentation for the Seminar on
“Post-Covid Challenges in Criminal Justice
Focus on Internet Searches for EU Legal Practicioners“

Rechtsanwältin Mirjam Hannah Steinfeld, MBA, CFE
Fachanwältin für Strafrecht
Of Counsel

Cracow, 21-22 September 2023

1



ROSINUS PARTNER

AGENDA

I. Basics

II. Definitions and Principles

III. Determining the issues at hand

IV. Factual issues

V. Legal options

VI. Summary

VII. Tipps & Tricks

2

2

I. Basics

3

3

ROSINUS PARTNER

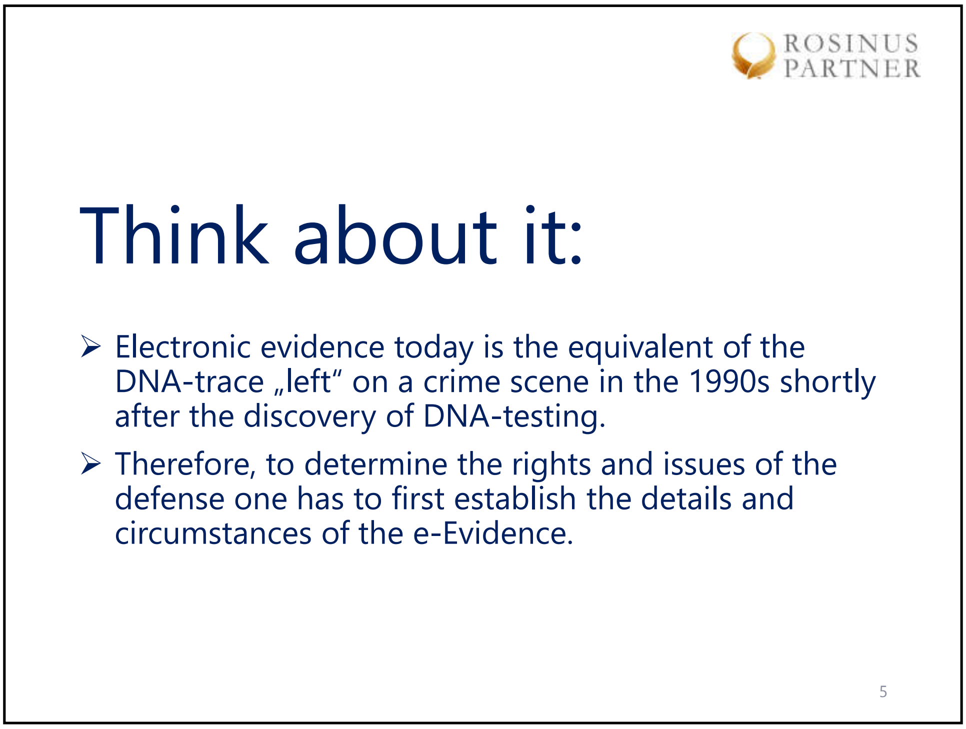
What is

E-Evidence

that can be collected on the internet?

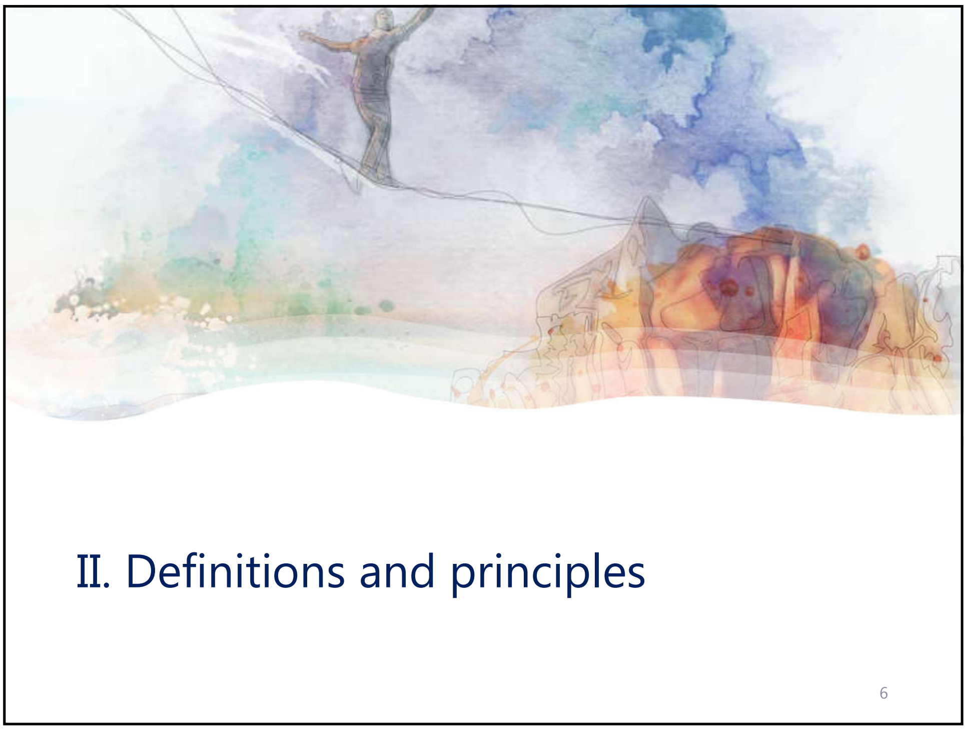
4

4

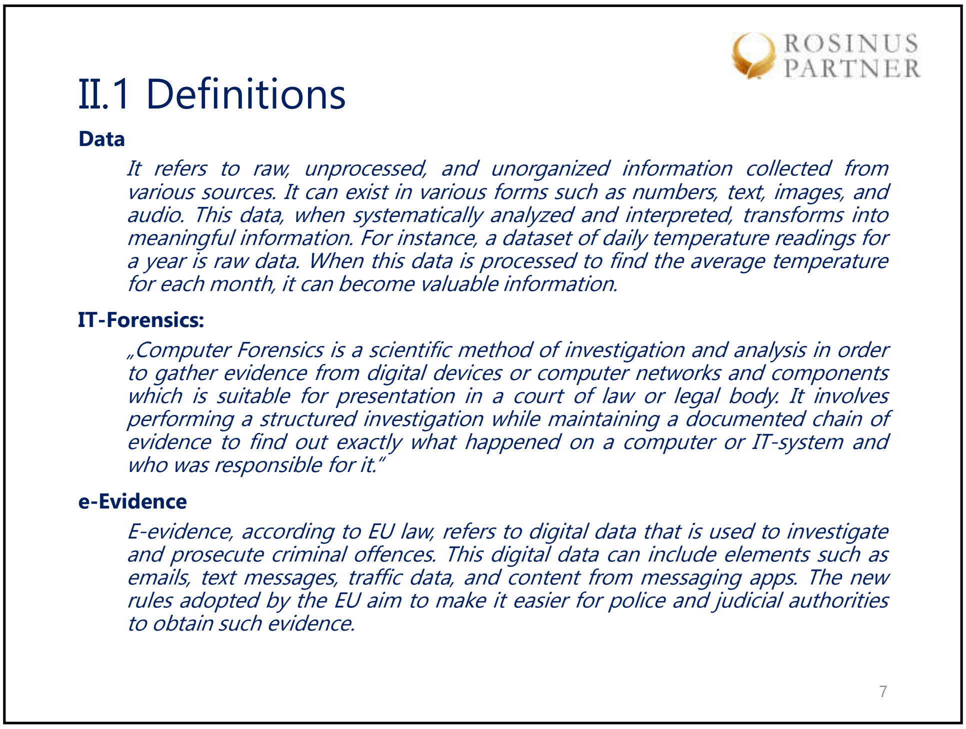


Think about it:

- ➢ Electronic evidence today is the equivalent of the DNA-trace „left“ on a crime scene in the 1990s shortly after the discovery of DNA-testing.
- ➢ Therefore, to determine the rights and issues of the defense one has to first establish the details and circumstances of the e-Evidence.



II. Definitions and principles



ROSINUS
PARTNER

II.1 Definitions

Data

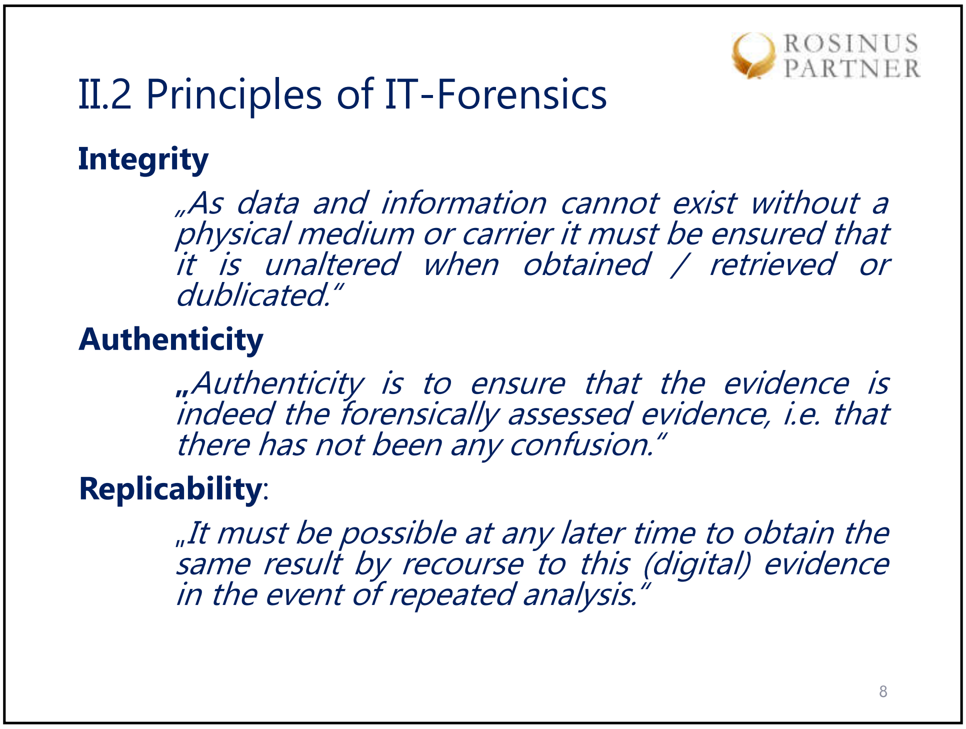
It refers to raw, unprocessed, and unorganized information collected from various sources. It can exist in various forms such as numbers, text, images, and audio. This data, when systematically analyzed and interpreted, transforms into meaningful information. For instance, a dataset of daily temperature readings for a year is raw data. When this data is processed to find the average temperature for each month, it can become valuable information.

IT-Forensics:

„Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer or IT-system and who was responsible for it."

e-Evidence

E-evidence, according to EU law, refers to digital data that is used to investigate and prosecute criminal offences. This digital data can include elements such as emails, text messages, traffic data, and content from messaging apps. The new rules adopted by the EU aim to make it easier for police and judicial authorities to obtain such evidence.



ROSINUS
PARTNER

II.2 Principles of IT-Forensics

Integrity

„As data and information cannot exist without a physical medium or carrier it must be ensured that it is unaltered when obtained / retrieved or dublicated."

Authenticity

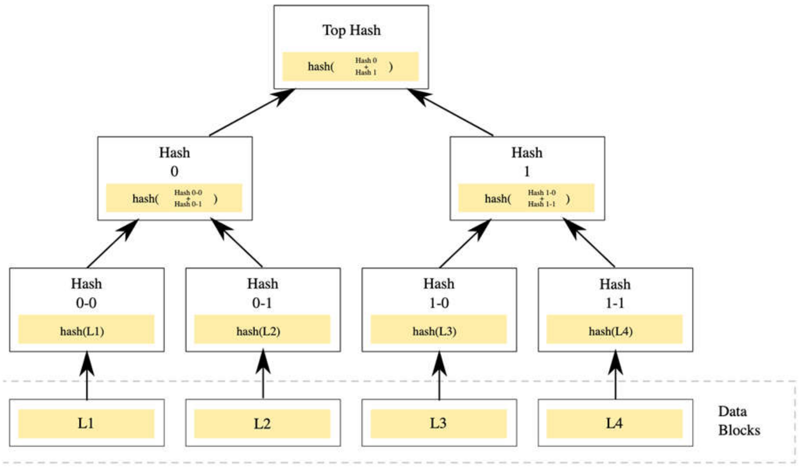
„Authenticity is to ensure that the evidence is indeed the forensically assessed evidence, i.e. that there has not been any confusion."

Replicability:

„It must be possible at any later time to obtain the same result by recourse to this (digital) evidence in the event of repeated analysis."

Excursus: Merkle Tree

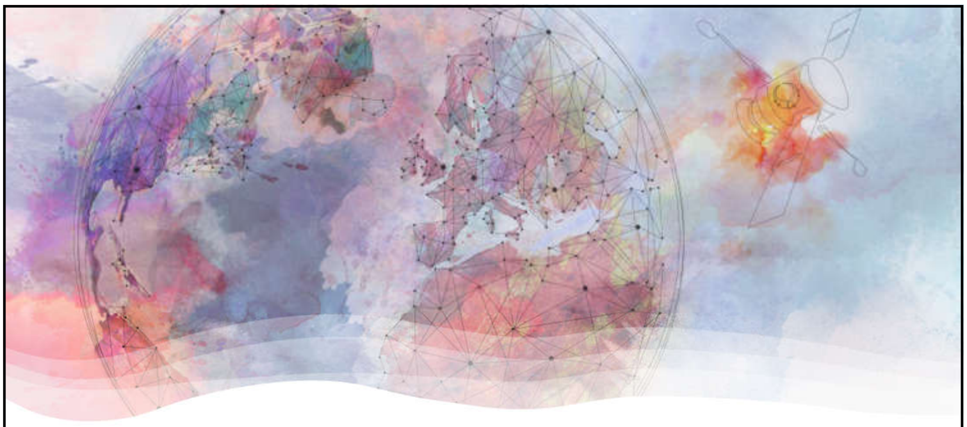
ROSINUS PARTNER



Source: Creative Commons (Wikipedia)

9

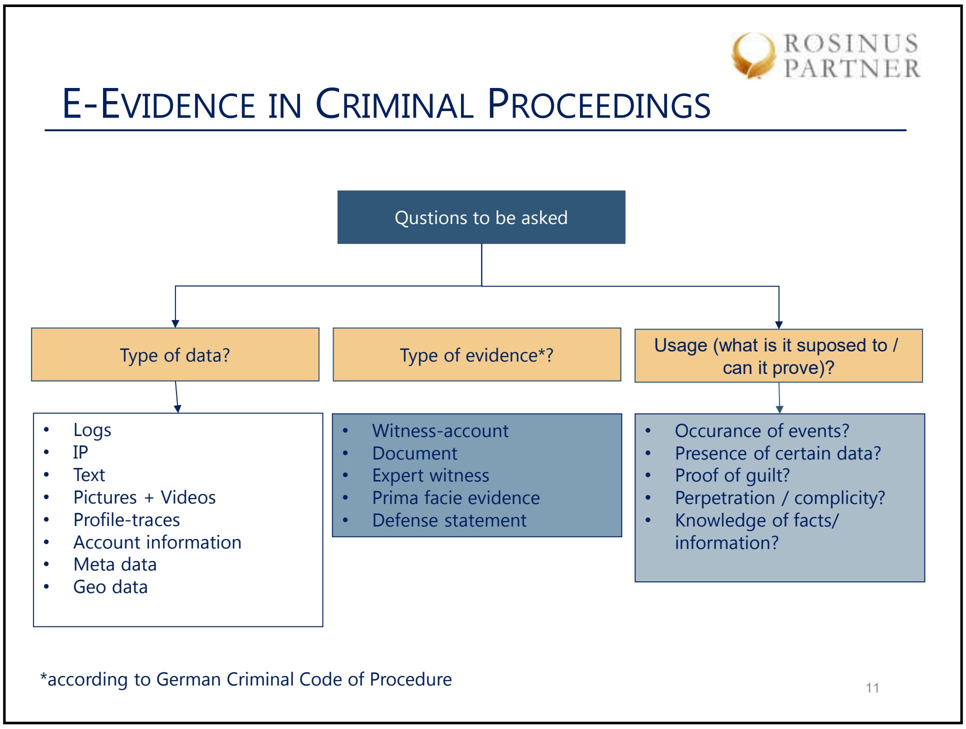
9



III. Determining the issues at hand

10

10



ROSINUS PARTNER

E-Evidence in Criminal Proceedings

Qustions to be asked

Type of data?

- Logs
- IP
- Text
- Pictures + Videos
- Profile-traces
- Account information
- Meta data
- Geo data

Type of evidence*?

- Witness-account
- Document
- Expert witness
- Prima facie evidence
- Defense statement

Usage (what is it suposed to / can it prove)?

- Occurance of events?
- Presence of certain data?
- Proof of guilt?
- Perpetration / complicity?
- Knowledge of facts/ information?

*according to German Criminal Code of Procedure

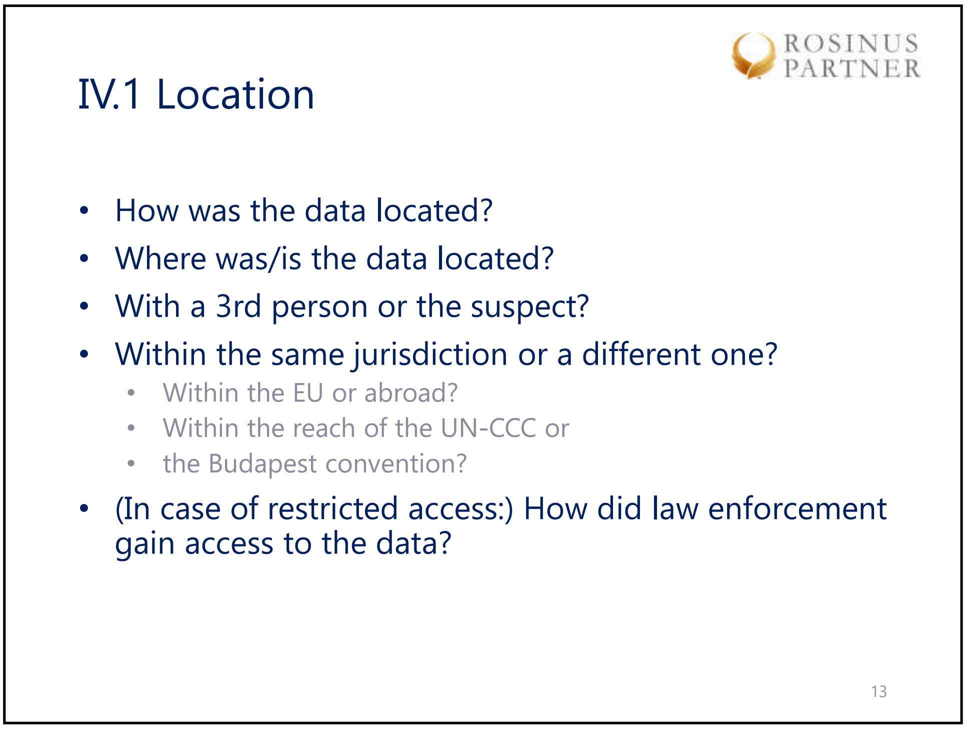
11

11

IV. Factual issues

12

12



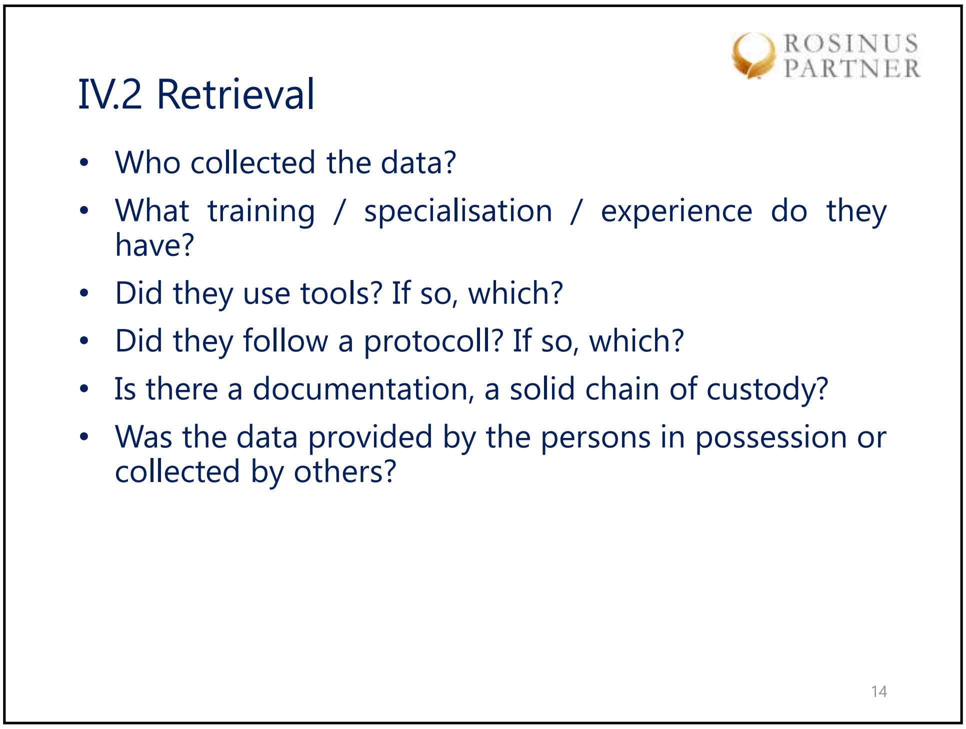
ROSINUS PARTNER

IV.1 Location

- How was the data located?
- Where was/is the data located?
- With a 3rd person or the suspect?
- Within the same jurisdiction or a different one?
  - Within the EU or abroad?
  - Within the reach of the UN-CCC or
  - the Budapest convention?
- (In case of restricted access:) How did law enforcement gain access to the data?

13

13



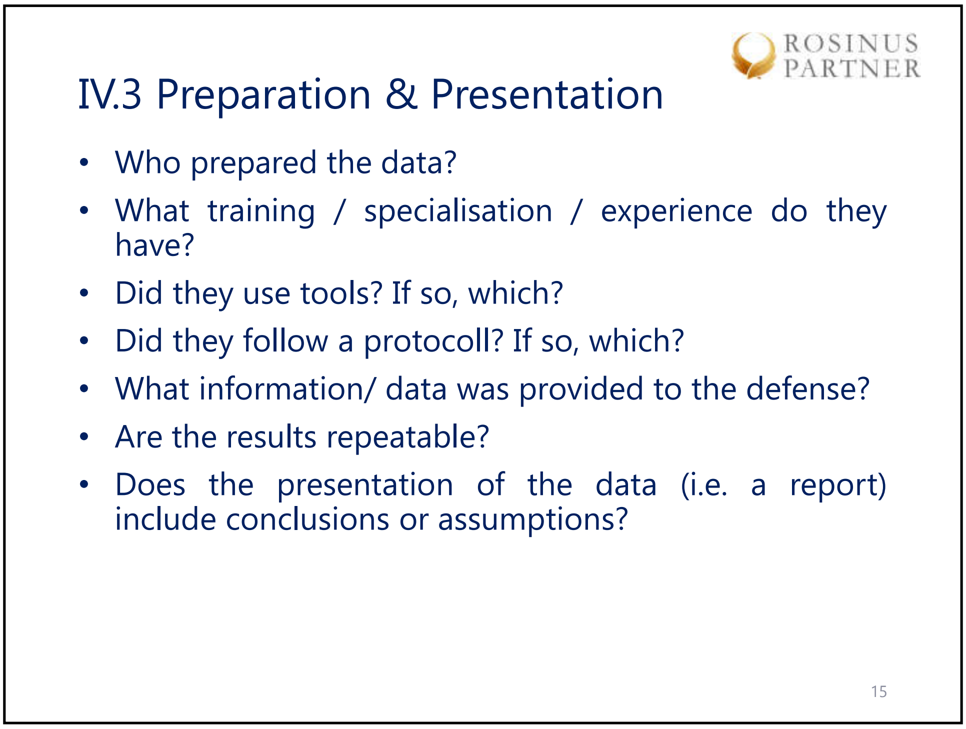
ROSINUS PARTNER

IV.2 Retrieval

- Who collected the data?
- What training / specialisation / experience do they have?
- Did they use tools? If so, which?
- Did they follow a protocoll? If so, which?
- Is there a documentation, a solid chain of custody?
- Was the data provided by the persons in possession or collected by others?

14

14



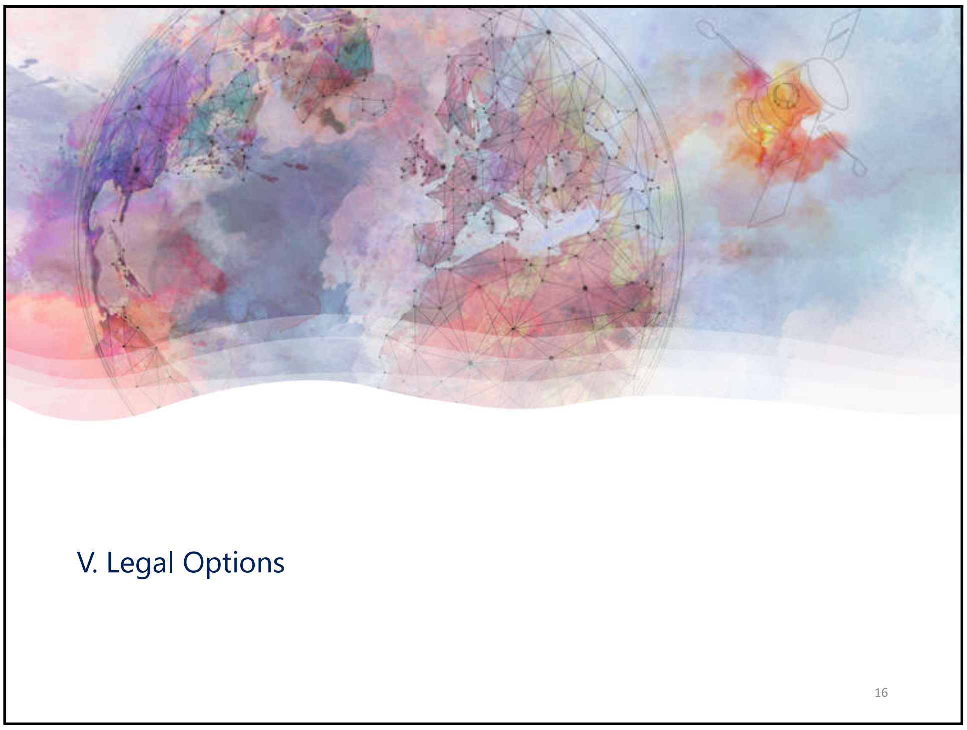
ROSINUS PARTNER

IV.3 Preparation & Presentation

- Who prepared the data?
- What training / specialisation / experience do they have?
- Did they use tools? If so, which?
- Did they follow a protocoll? If so, which?
- What information/ data was provided to the defense?
- Are the results repeatable?
- Does the presentation of the data (i.e. a report) include conclusions or assumptions?

15

15



V. Legal Options

16

16

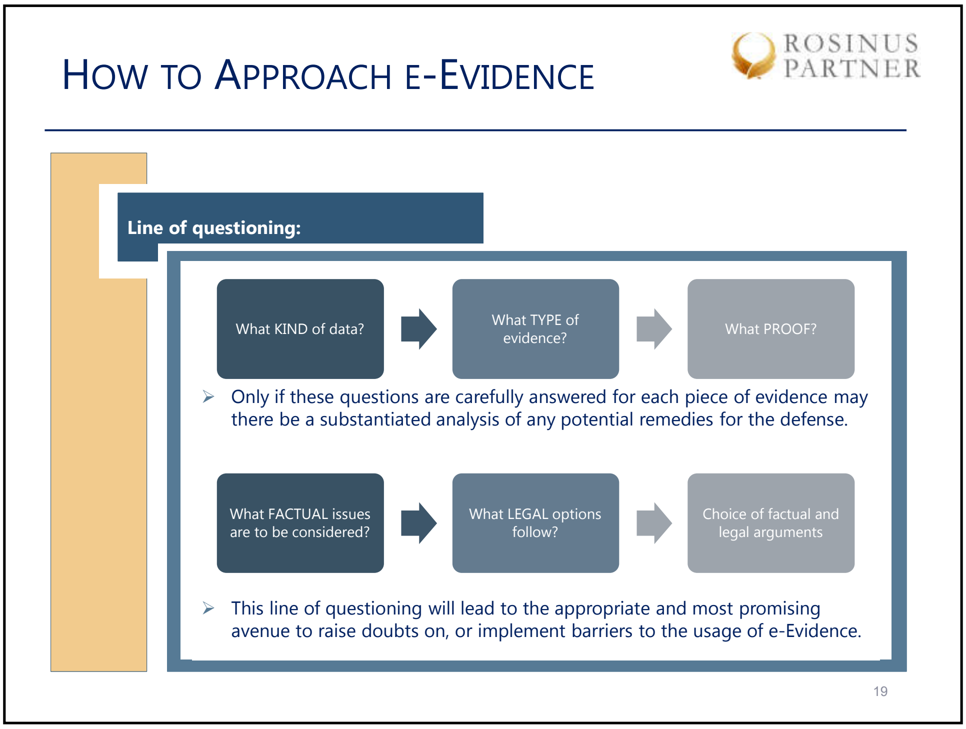
V. Legal Options

1. Administrative rights and duties
   - ➢ Electronic Evidence Guide
   - ➢ BSI-Leitfaden IT-Forensik
2. Procedural rights
   - ➢ Judiciary reservation
   - ➢ Selection of expert witnesses
   - ➢ Degree of suspicion
3. Consitutional rights
   - ➢ Right to a fair trial
   - ➢ Presumption of innocence
4. EU Charta / European Court of Justice
   - ➢ i.e. ECJ, C-339/20

17

VI. Summary

18



HOW TO APPROACH E-EVIDENCE

ROSINUS PARTNER

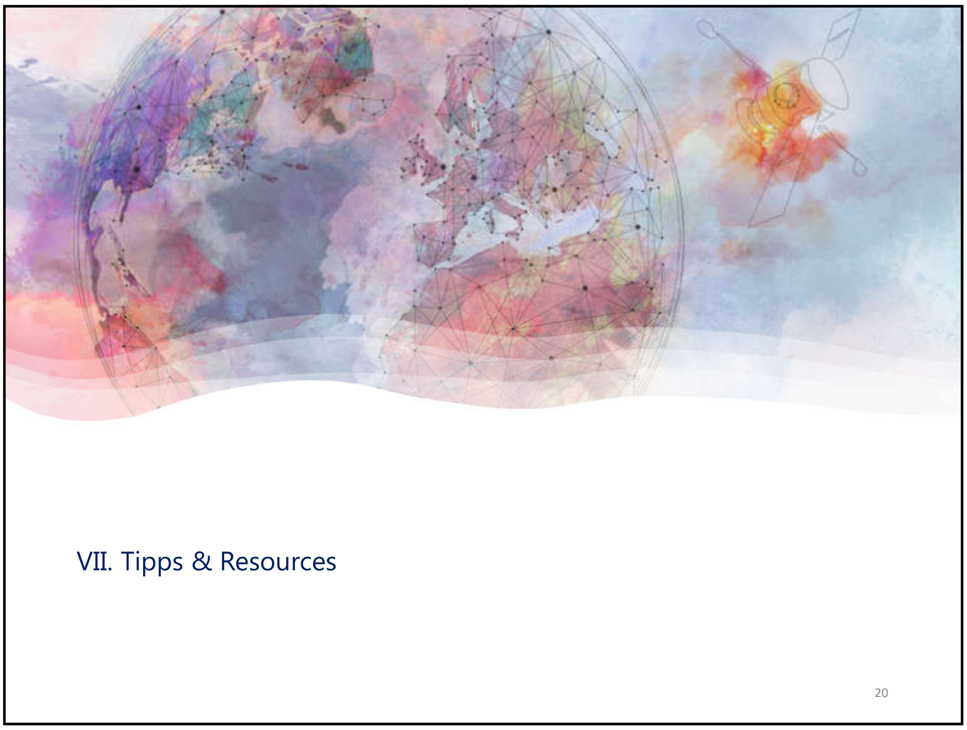
Line of questioning:

What KIND of data? → What TYPE of evidence? → What PROOF?

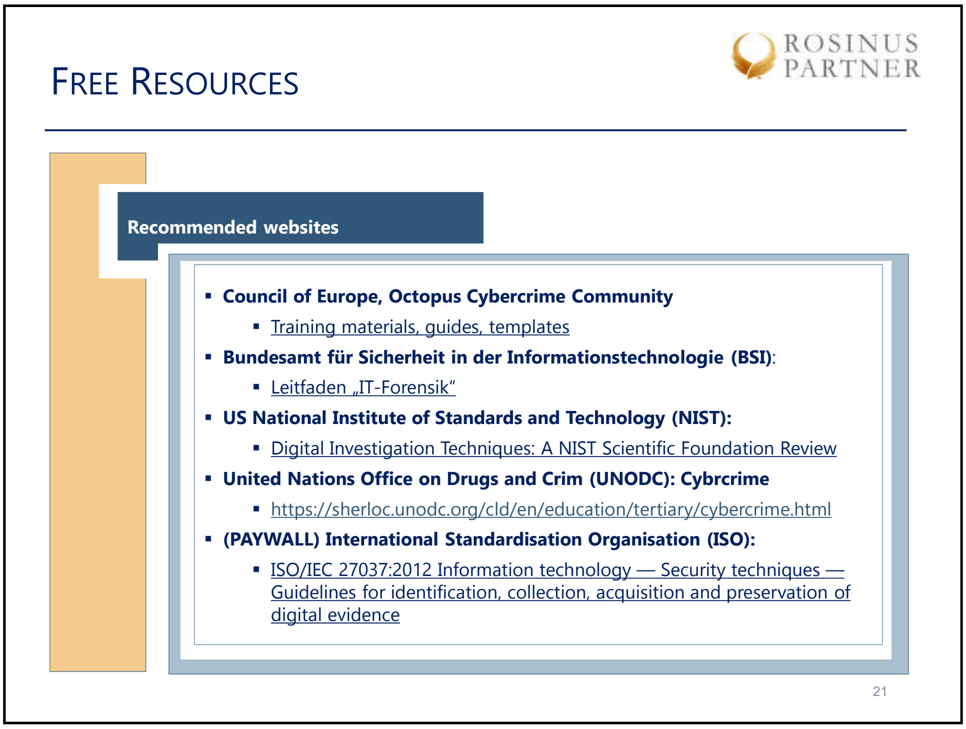
- ➢ Only if these questions are carefully answered for each piece of evidence may there be a substantiated analysis of any potential remedies for the defense.

What FACTUAL issues are to be considered? → What LEGAL options follow? → Choice of factual and legal arguments

- ➢ This line of questioning will lead to the appropriate and most promising avenue to raise doubts on, or implement barriers to the usage of e-Evidence.



VII. Tipps & Resources



ROSINUS PARTNER

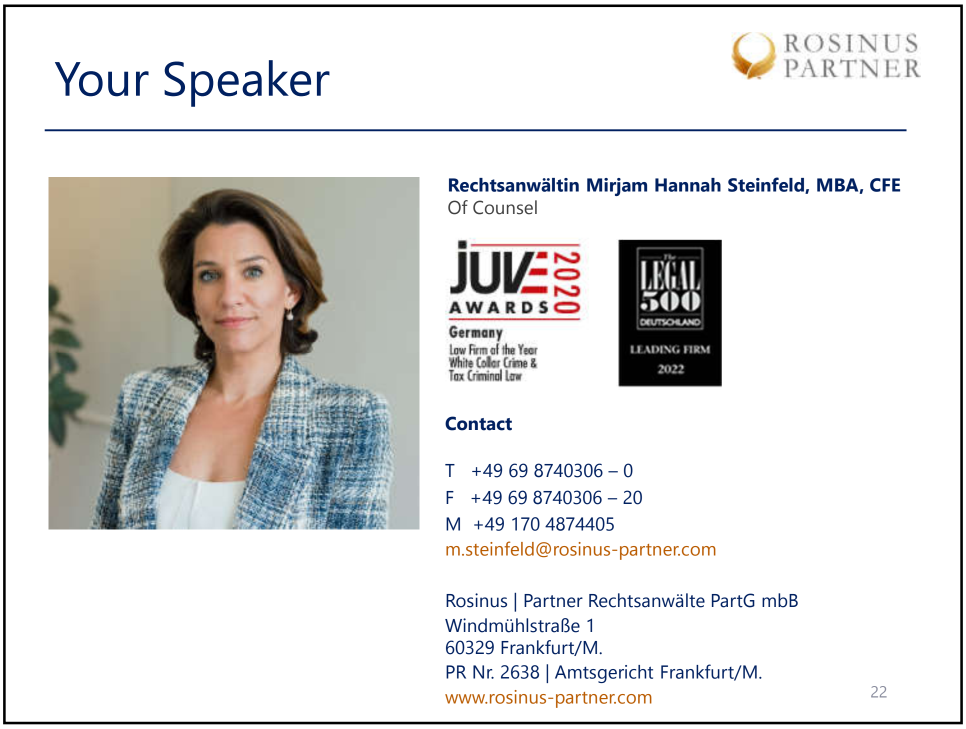
FREE RESOURCES

Recommended websites

- **Council of Europe, Octopus Cybercrime Community**
  - Training materials, guides, templates
- **Bundesamt für Sicherheit in der Informationstechnologie (BSI)**:
  - Leitfaden „IT-Forensik"
- **US National Institute of Standards and Technology (NIST):**
  - Digital Investigation Techniques: A NIST Scientific Foundation Review
- **United Nations Office on Drugs and Crim (UNODC): Cybrcrime**
  - https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime.html
- **(PAYWALL) International Standardisation Organisation (ISO):**
  - ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

21

21



ROSINUS PARTNER

Your Speaker

Rechtsanwältin Mirjam Hannah Steinfeld, MBA, CFE
Of Counsel

JUVE 2020 AWARDS
Germany
Law Firm of the Year
White Collar Crime &
Tax Criminal Law

The LEGAL 500
DEUTSCHLAND
LEADING FIRM
2022

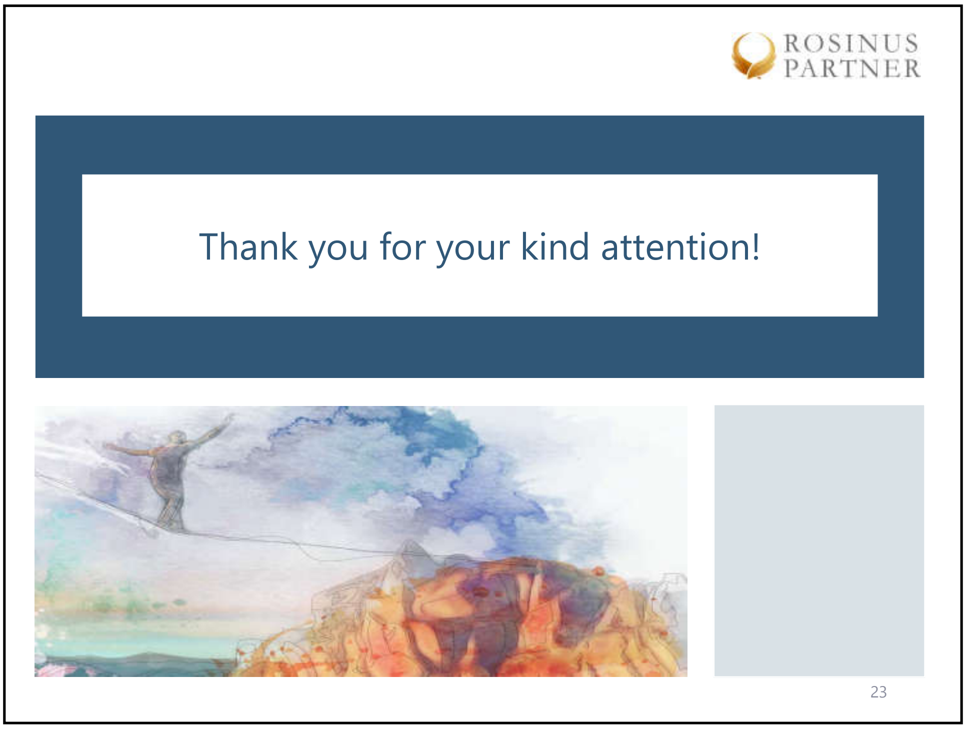
Contact

T +49 69 8740306 – 0
F +49 69 8740306 – 20
M +49 170 4874405
m.steinfeld@rosinus-partner.com

Rosinus | Partner Rechtsanwälte PartG mbB
Windmühlstraße 1
60329 Frankfurt/M.
PR Nr. 2638 | Amtsgericht Frankfurt/M.
www.rosinus-partner.com

22

22



ROSINUS
PARTNER

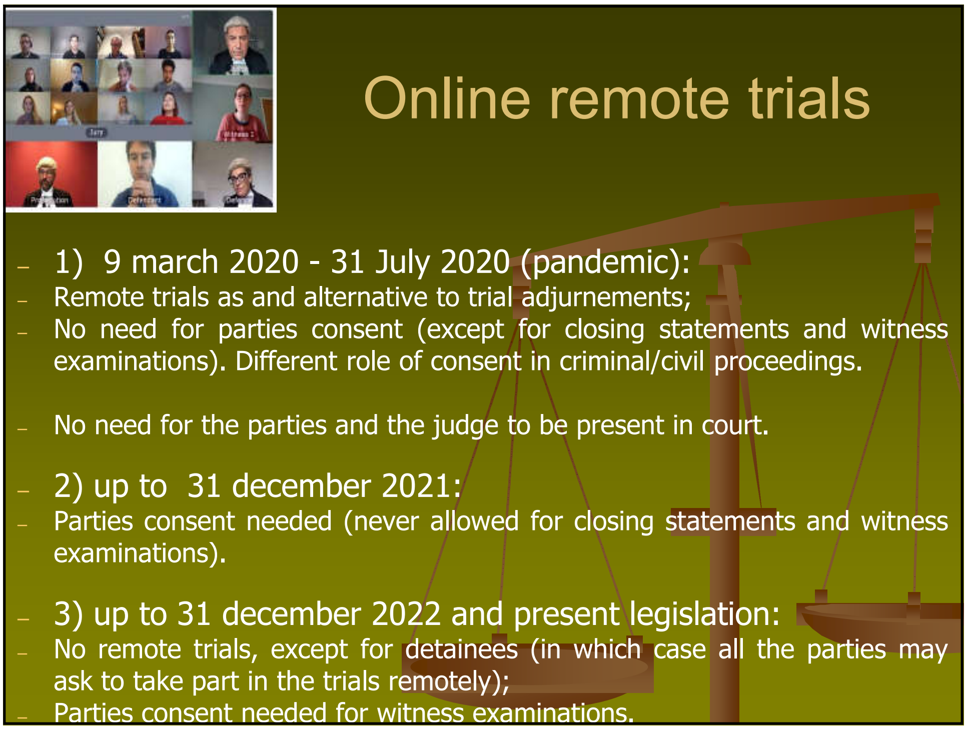
Thank you for your kind attention!

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

Andrea CRUCIANI
Judge at Military Tribunal of Naples

Co-funded by the European Union

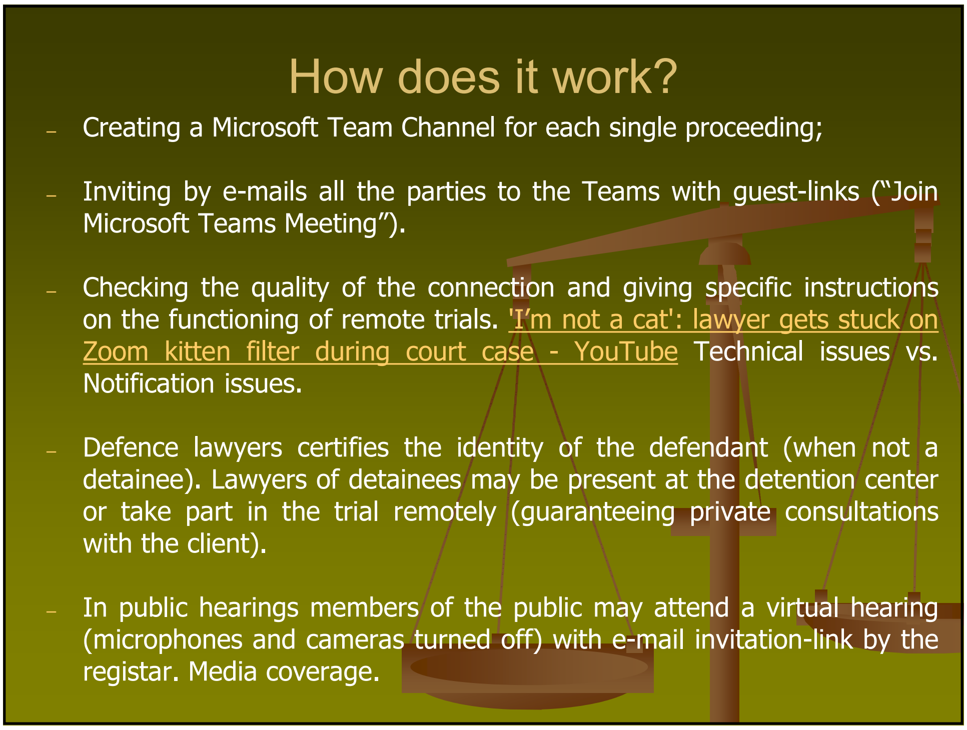
1



Online remote trials

- 1) 9 march 2020 - 31 July 2020 (pandemic):
- Remote trials as and alternative to trial adjurnements;
- No need for parties consent (except for closing statements and witness examinations). Different role of consent in criminal/civil proceedings.
- No need for the parties and the judge to be present in court.
- 2) up to 31 december 2021:
- Parties consent needed (never allowed for closing statements and witness examinations).
- 3) up to 31 december 2022 and present legislation:
- No remote trials, except for detainees (in which case all the parties may ask to take part in the trials remotely);
- Parties consent needed for witness examinations.

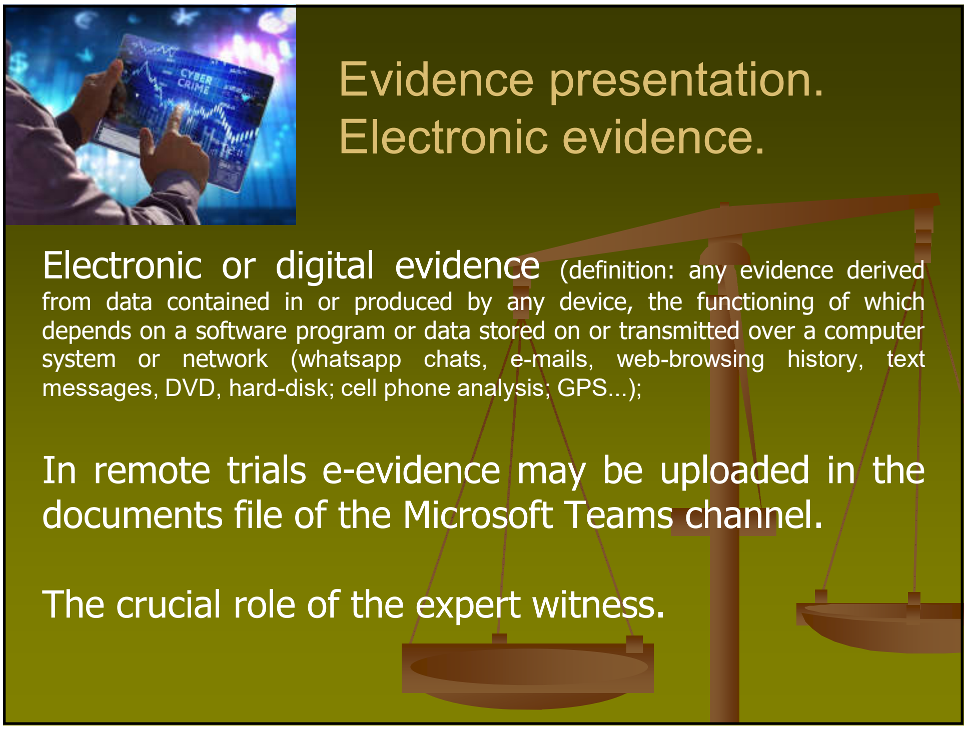
2



How does it work?

- Creating a Microsoft Team Channel for each single proceeding;
- Inviting by e-mails all the parties to the Teams with guest-links (“Join Microsoft Teams Meeting”).
- Checking the quality of the connection and giving specific instructions on the functioning of remote trials. 'I’m not a cat': lawyer gets stuck on Zoom kitten filter during court case - YouTube Technical issues vs. Notification issues.
- Defence lawyers certifies the identity of the defendant (when not a detainee). Lawyers of detainees may be present at the detention center or take part in the trial remotely (guaranteeing private consultations with the client).
- In public hearings members of the public may attend a virtual hearing (microphones and cameras turned off) with e-mail invitation-link by the registar. Media coverage.

3



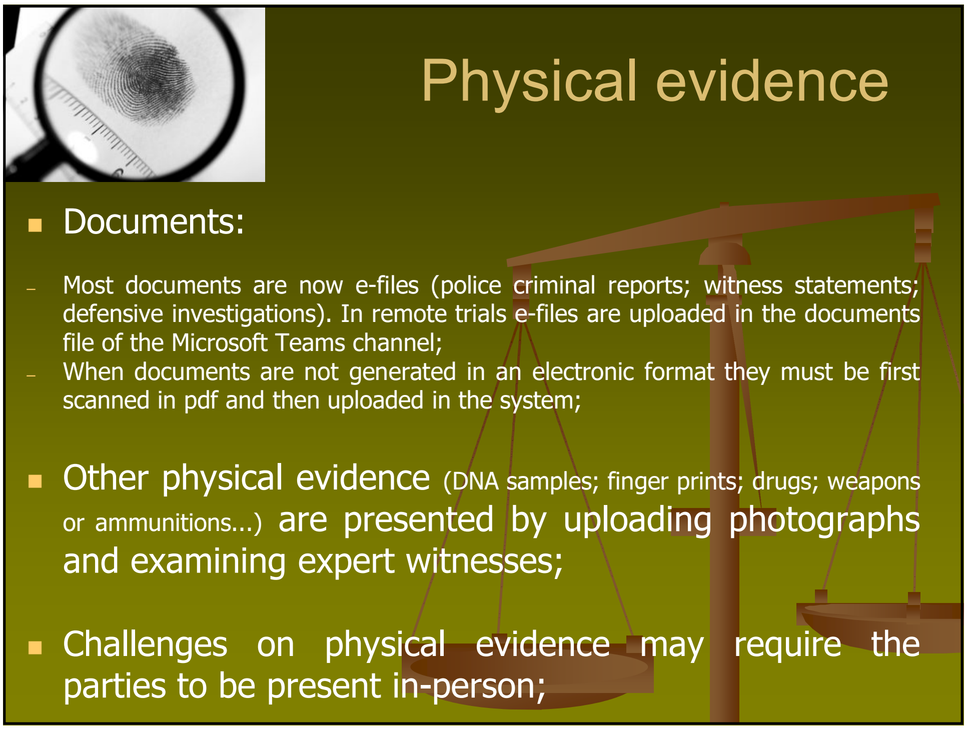
Evidence presentation. Electronic evidence.

Electronic or digital evidence (definition: any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network (whatsapp chats, e-mails, web-browsing history, text messages, DVD, hard-disk; cell phone analysis; GPS...);

In remote trials e-evidence may be uploaded in the documents file of the Microsoft Teams channel.

The crucial role of the expert witness.

4



Physical evidence

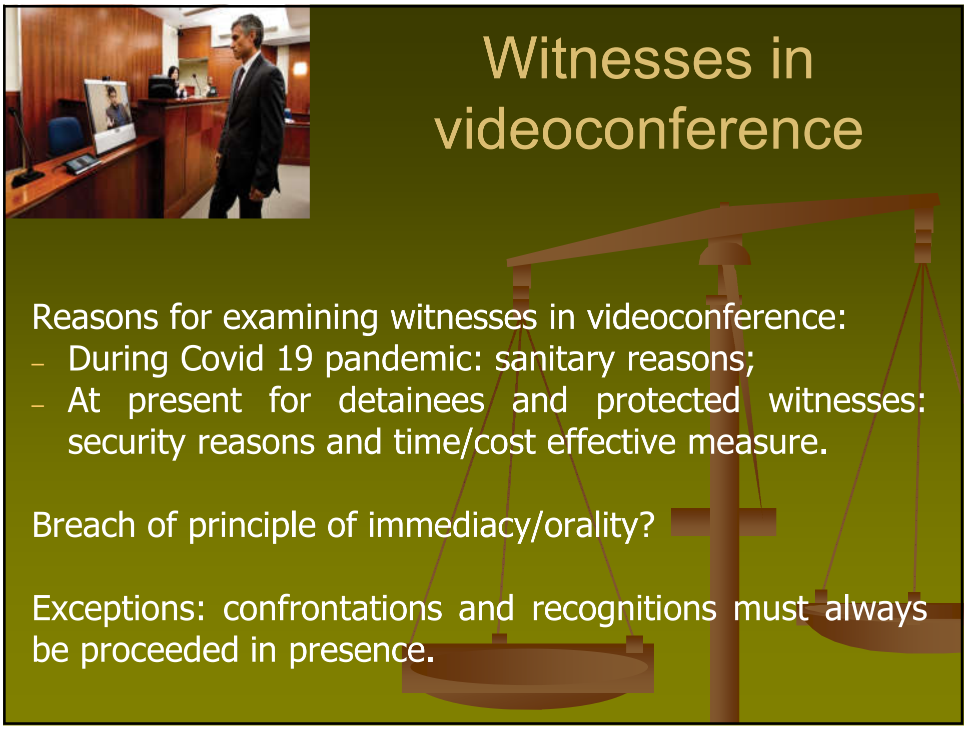
- Documents:

  - Most documents are now e-files (police criminal reports; witness statements; defensive investigations). In remote trials e-files are uploaded in the documents file of the Microsoft Teams channel;
  - When documents are not generated in an electronic format they must be first scanned in pdf and then uploaded in the system;

- Other physical evidence (DNA samples; finger prints; drugs; weapons or ammunitions…) are presented by uploading photographs and examining expert witnesses;

- Challenges on physical evidence may require the parties to be present in-person;

5



Witnesses in videoconference

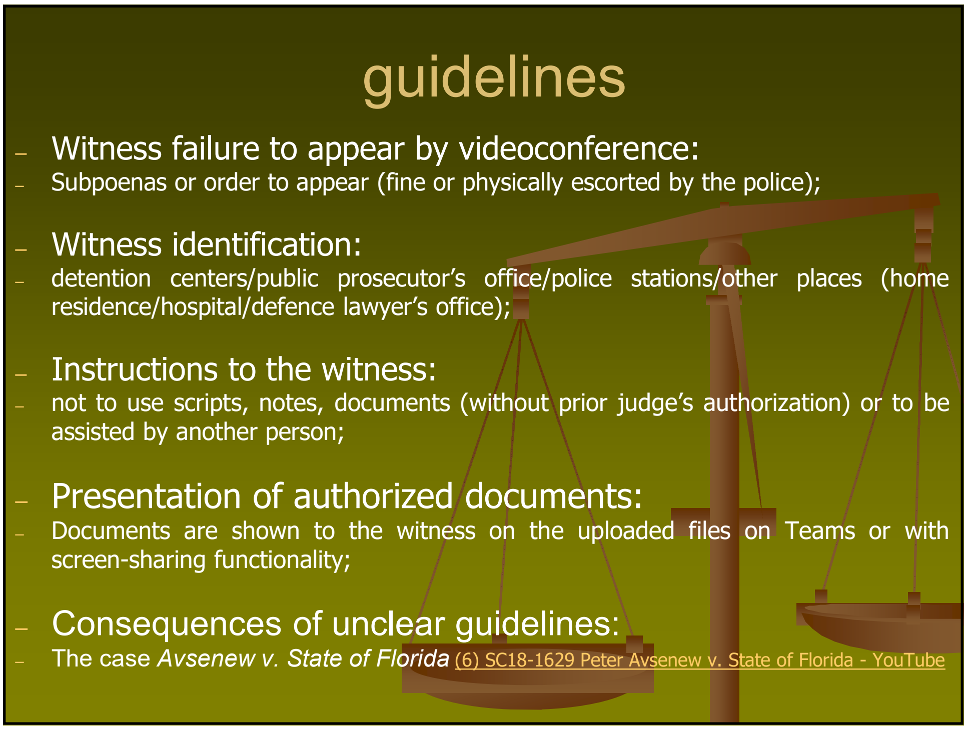
Reasons for examining witnesses in videoconference:

- During Covid 19 pandemic: sanitary reasons;
- At present for detainees and protected witnesses: security reasons and time/cost effective measure.

Breach of principle of immediacy/orality?

Exceptions: confrontations and recognitions must always be proceeded in presence.

6



guidelines

- Witness failure to appear by videoconference:
- Subpoenas or order to appear (fine or physically escorted by the police);

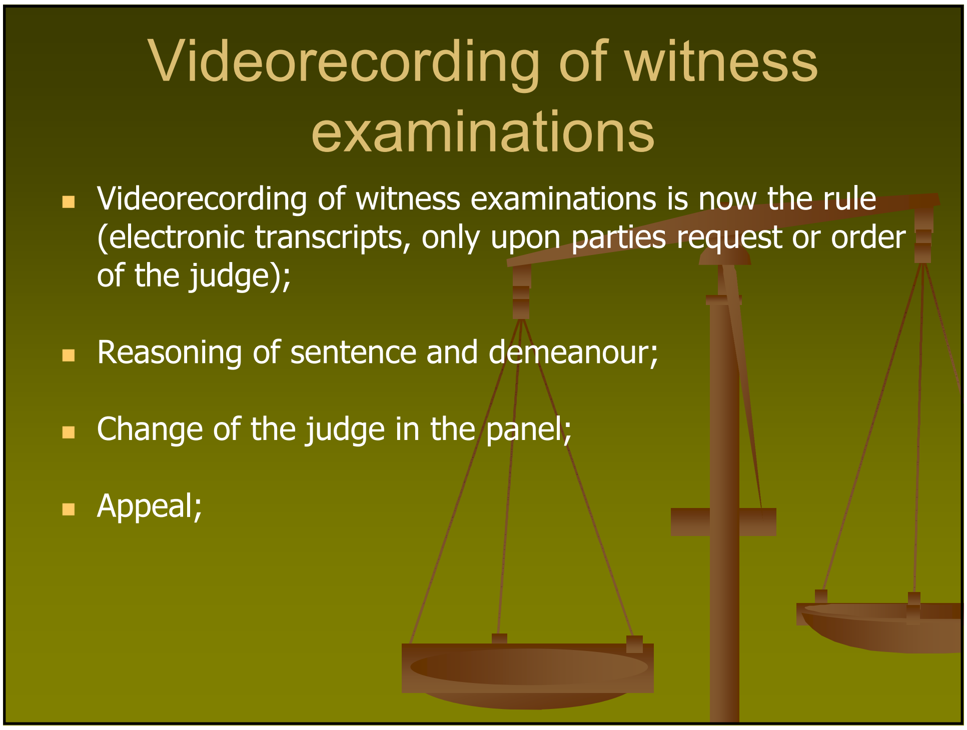
- Witness identification:
- detention centers/public prosecutor’s office/police stations/other places (home residence/hospital/defence lawyer’s office);

- Instructions to the witness:
- not to use scripts, notes, documents (without prior judge’s authorization) or to be assisted by another person;

- Presentation of authorized documents:
- Documents are shown to the witness on the uploaded files on Teams or with screen-sharing functionality;

- Consequences of unclear guidelines:
- The case *Avsenew v. State of Florida* (6) SC18-1629 Peter Avsenew v. State of Florida - YouTube

7



Videorecording of witness examinations

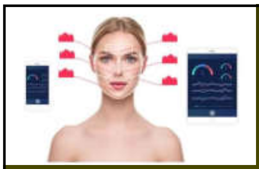
- Videorecording of witness examinations is now the rule (electronic transcripts, only upon parties request or order of the judge);

- Reasoning of sentence and demeanour;

- Change of the judge in the panel;

- Appeal;

8



Evaluating witnesses and AI

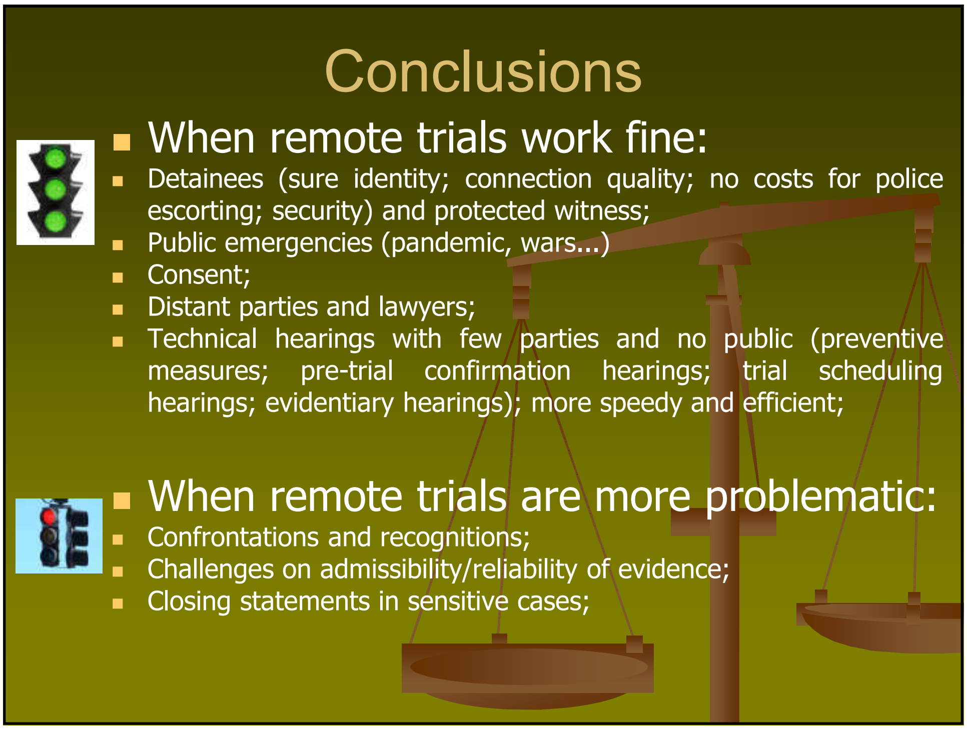
- Credibility (trustworthiness: truthful or untruthful?): from polygraphs to AI tools: eyes tracking, brain imaging; blood pressure measurement (transdermal optical imaging and the Pinocchio Effect).
- Reliability (or accuracy: right or wrong?); perception, memory, deposition; ADVOKATE;
- From demeanour to consistency: apps checking witness declarations for gaps/incoherences/contradictions (even in real time for cross examination purposes);
- Open issues: AI algorithms transparancy and intellectual property;

9

Closing statements in remote trials

- Technically feasible (members of the panel take the decision in a videoconference-chamber; screen-sharing functionality for judgement reading);
- In-presence and humanity in criminal trials (especially in sensitive cases. Capital punishment virdicts on Zoom in some countries have been heavily criticised).

10



Conclusions

- When remote trials work fine:
  - Detainees (sure identity; connection quality; no costs for police escorting; security) and protected witness;
  - Public emergencies (pandemic, wars…)
  - Consent;
  - Distant parties and lawyers;
  - Technical hearings with few parties and no public (preventive measures; pre-trial confirmation hearings; trial scheduling hearings; evidentiary hearings); more speedy and efficient;
- When remote trials are more problematic:
  - Confrontations and recognitions;
  - Challenges on admissibility/reliability of evidence;
  - Closing statements in sensitive cases;

11

1

Underground

Child

Foundation

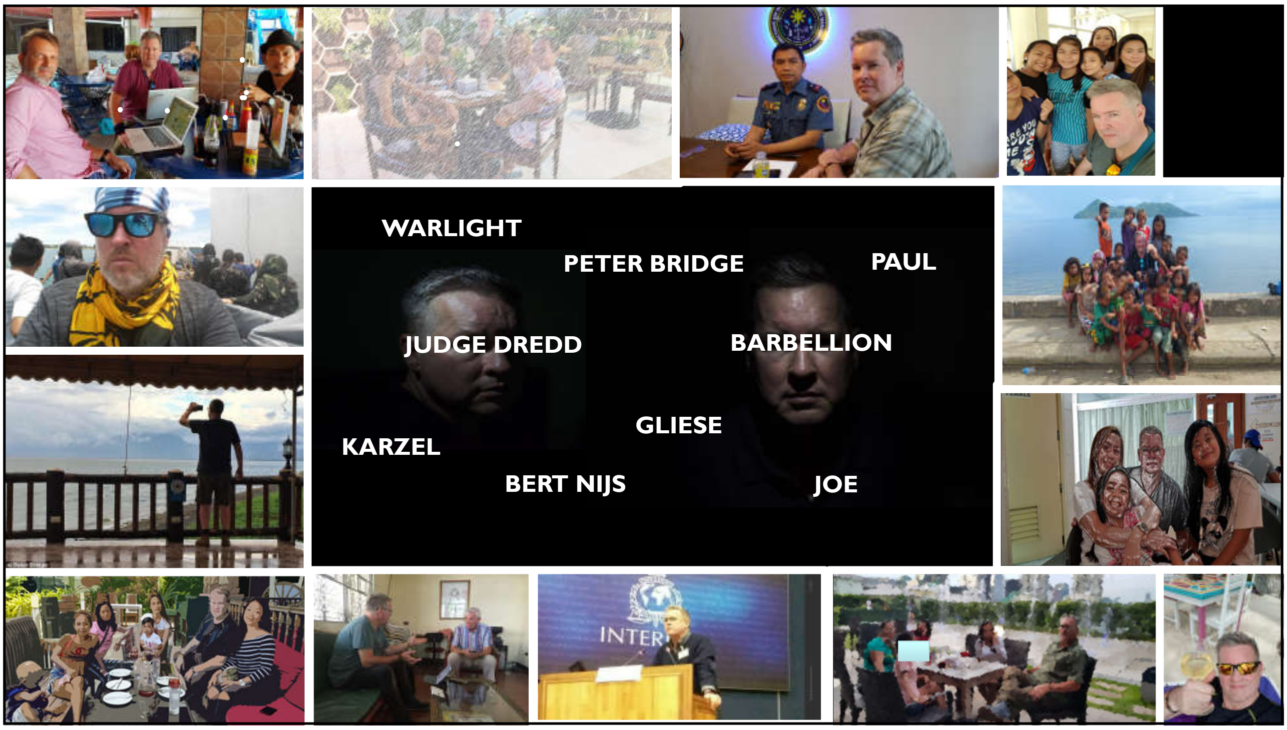
Get Up. Stand up. Speak Up.
Do Something.

Co-funded by the European Union

2

JOE

3



WARLIGHT

PETER BRIDGE

PAUL

JUDGE DREDD

BARBELLION

GLIESE

KARZEL

BERT NIJS

JOE

4

KVDSO_MANILLA V01 01032019

5

5

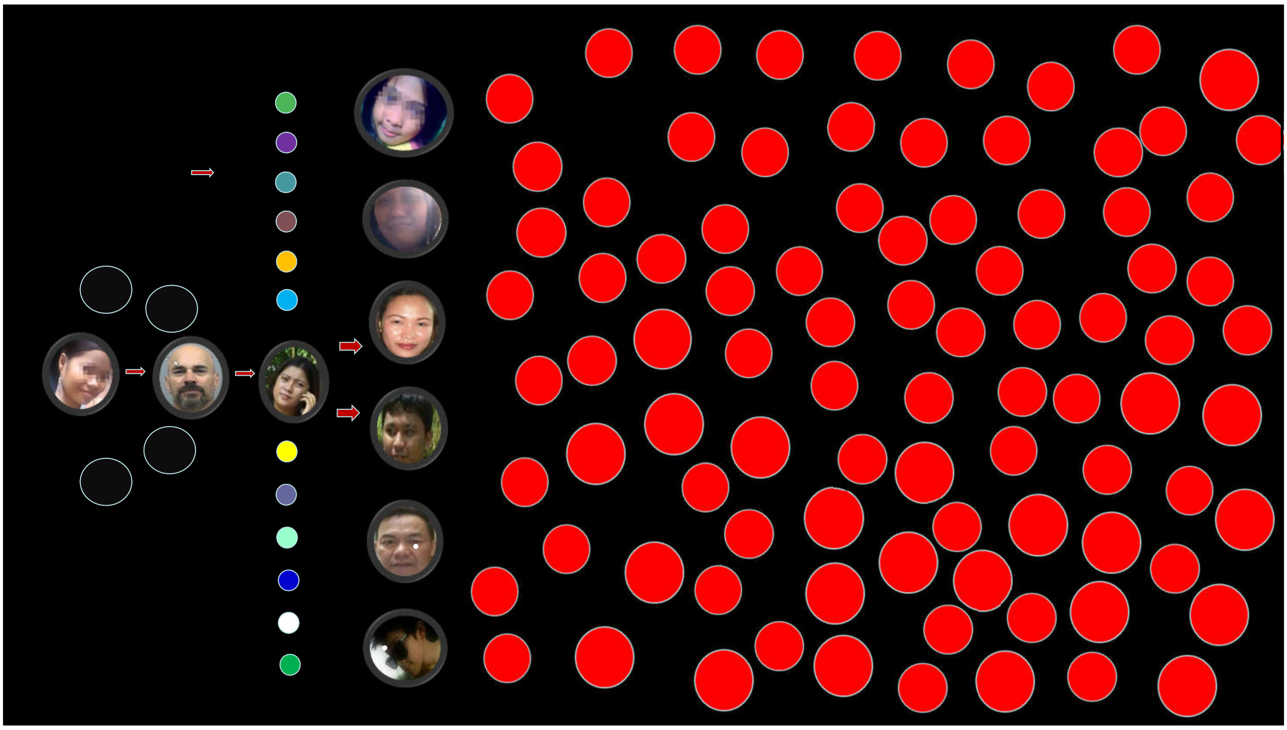
ONLINE SEXUAL ABUSE AND EXPLOITATION OF CHILDREN

OSAEC

6

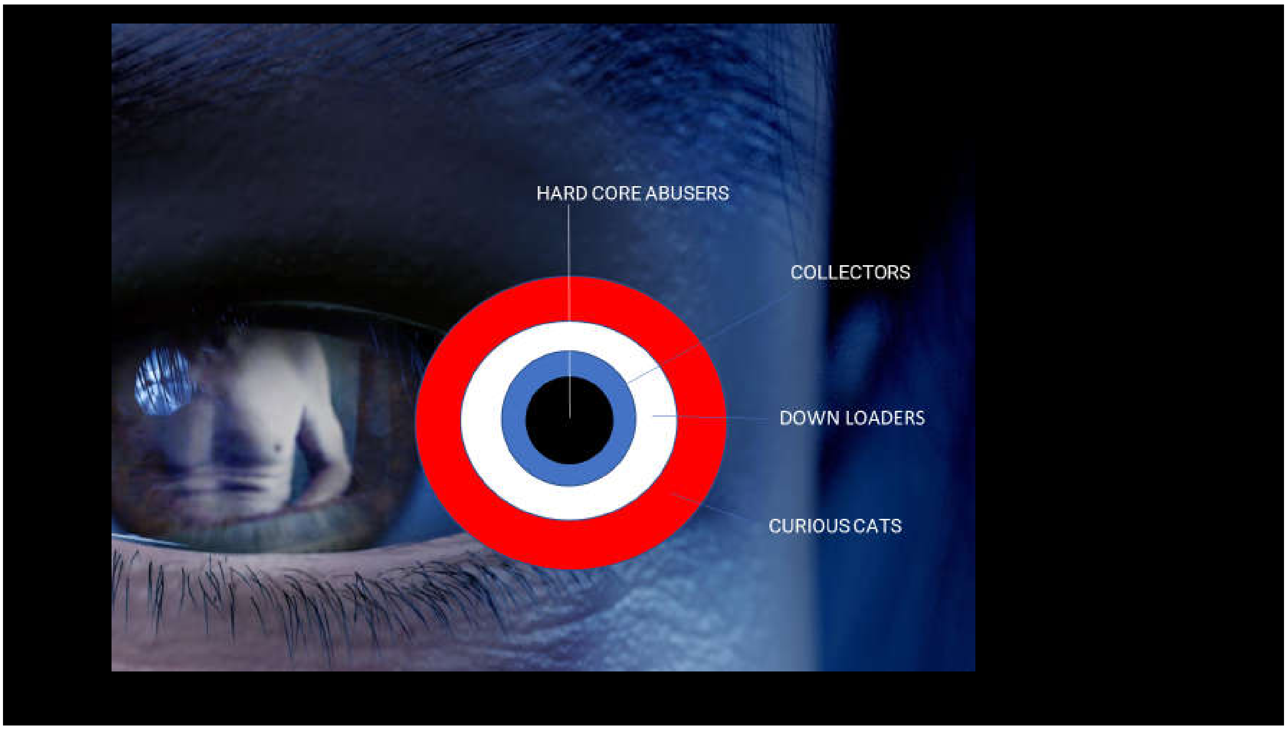
OSAEC is child sexual abuse is facilitated or occurs through the Internet and other related media.

7



8

9



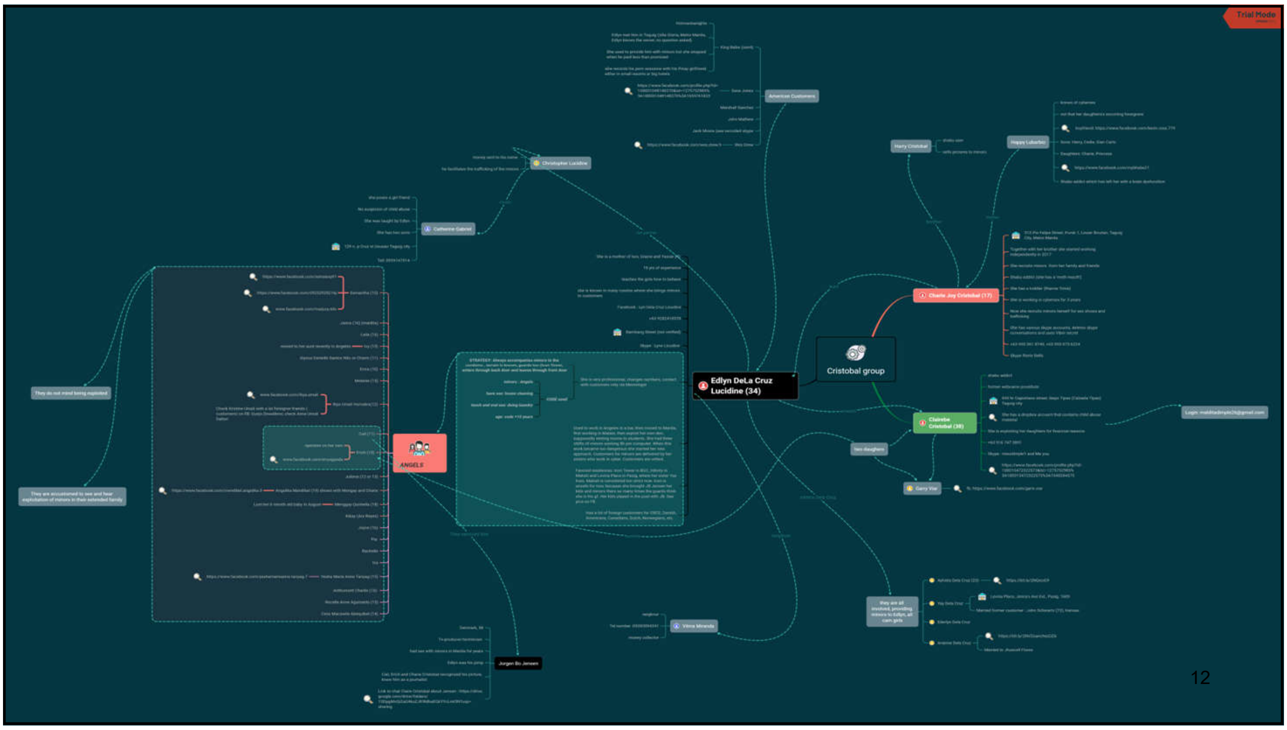
10

SWEETIE - TDH

1

2

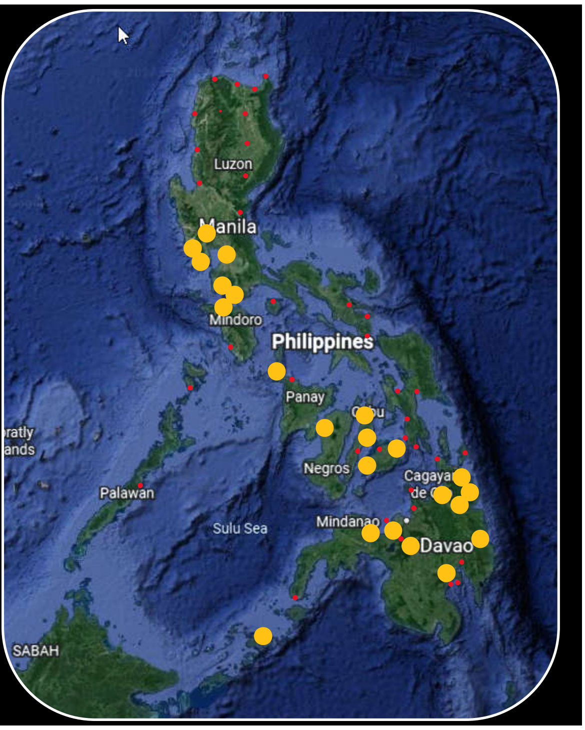
3



1. THE ARENA

13

PHILLIPINES



14

Metro Manila

The Province

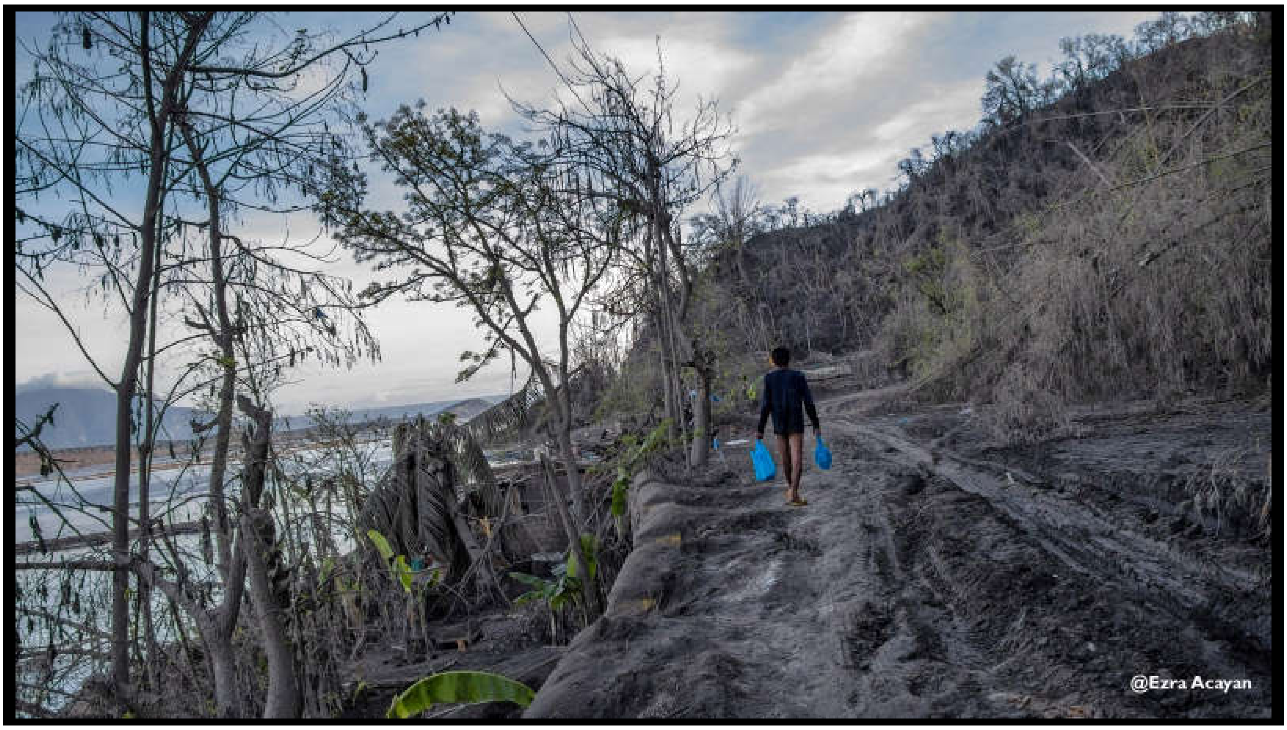
15

16

17

18

19



20

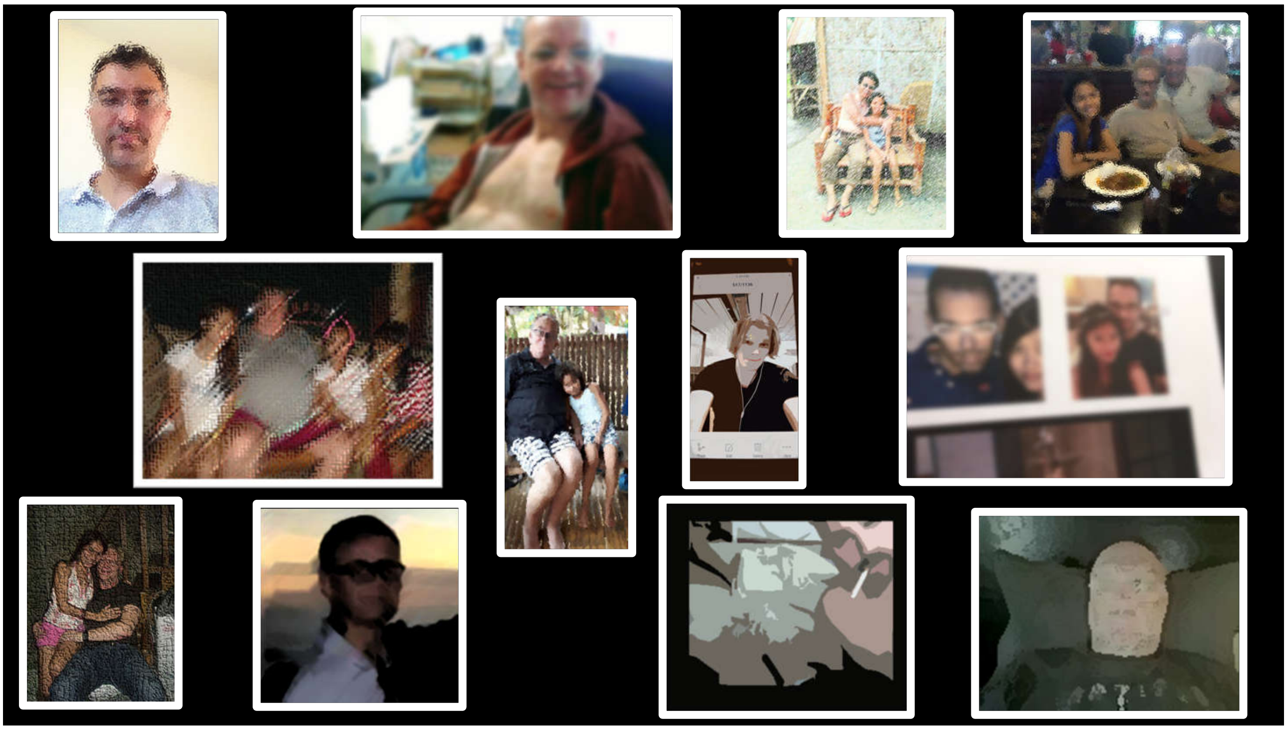
21

22

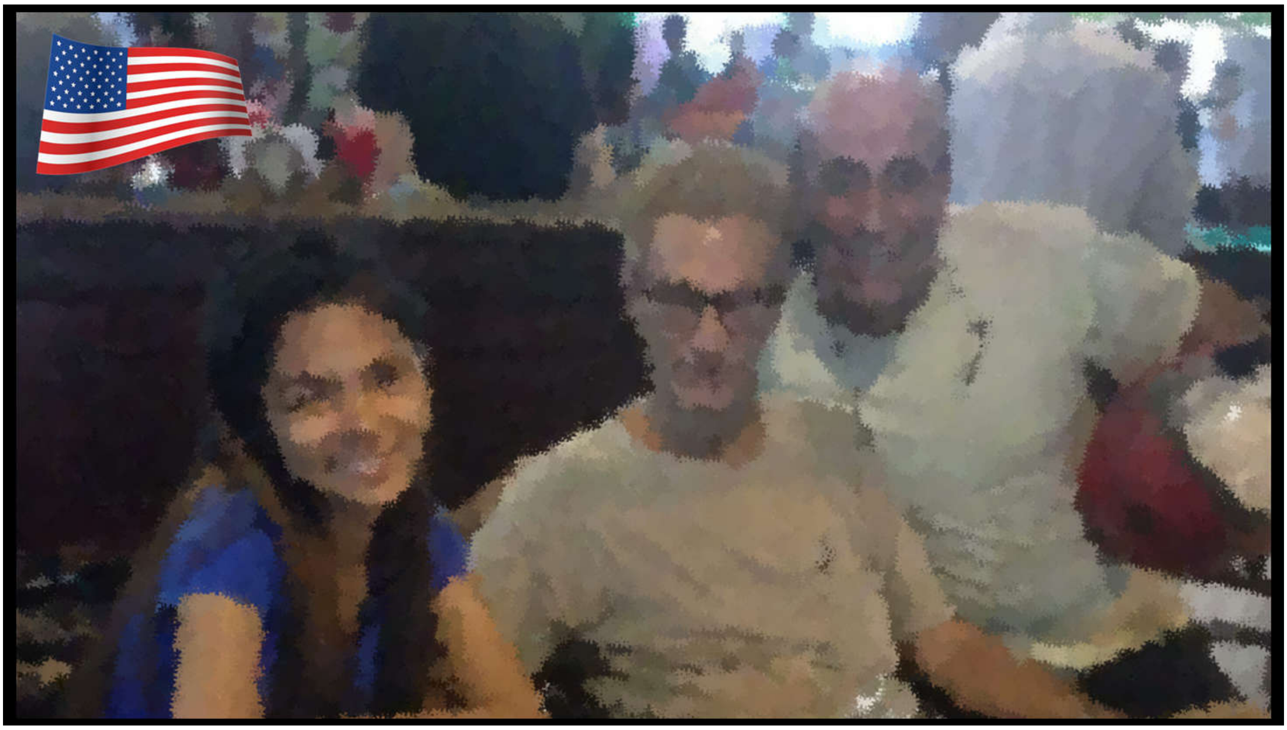
2. THE POREIGNER

23

24



25



26

27

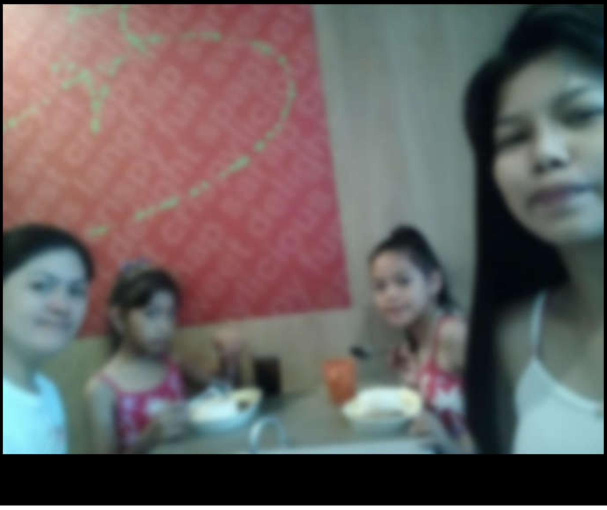
28

3. THE FACILITATOR

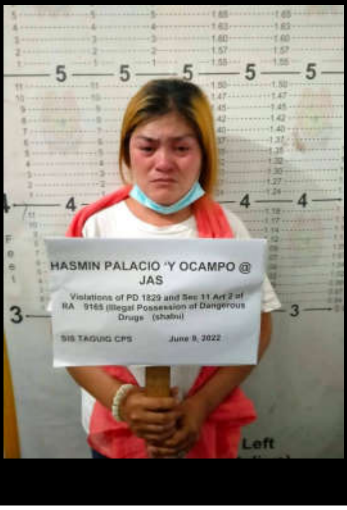
29

J.

2019



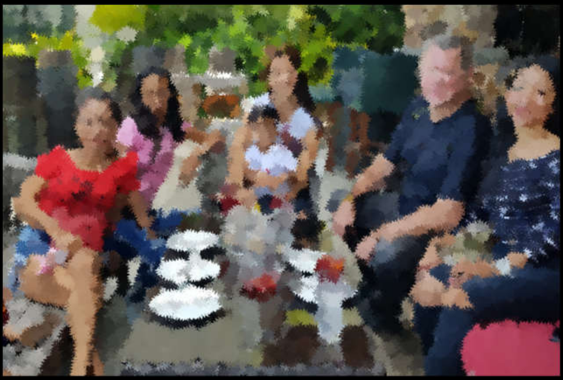
2022


HASMIN PALACIO 'Y OCAMPO @
JAS
Violations of PD 1829 and Sec 11 Art 2 of
RA 9165 (Illegal Possession of Dangerous
Drugs (shabu)
SIS TAGUIG CPS
June 9, 2022
Left

30

L.

2018



2022

31

A

2014

2018

32

4. THE YOUNG

33

34

35

36

37

5. POST-COVID

38

CHALLENGES 1

- Learning poverty 91%
- Food insecurity
- Job loss
- Higher cost of living
- Online games and betting
- Explosion of live streaming
- Discord/Steam/Twitch/
- Viber/Whatsapp/WeChat

39

Challenges 2

- Tech/language
- Too much data
- ISP remain deaf
- Laws ineffective
- Child users
- Sex work proliferation
- Asian customers

40

Challenges 3

- No worldwide registration
- Underreporting
- Unreliable definitions
- Jurisdictional differences
- Cultural lens
- Younger facilitators
- OSEC industry
- Studies - grey literature

41

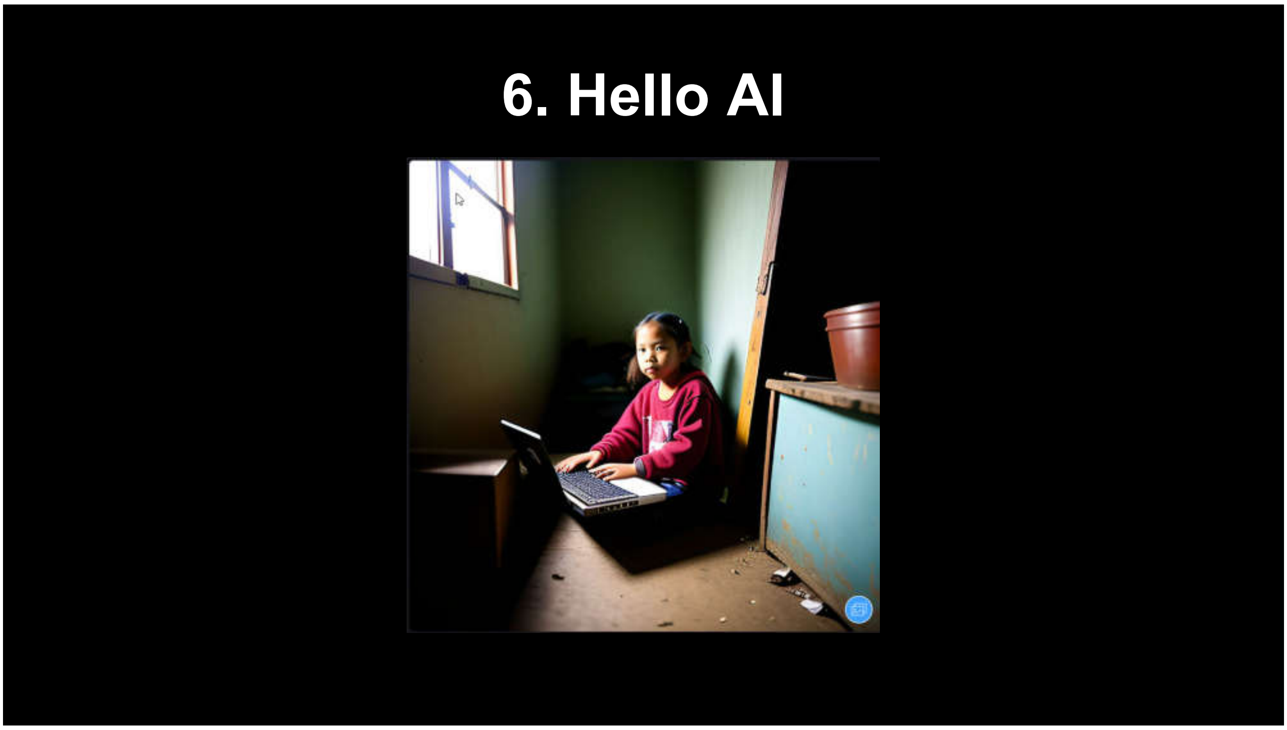
2022

500,000 children were trafficked to produce CSAM

3 in 1,000 adults was a facilitator

2% of the children was rescued

42

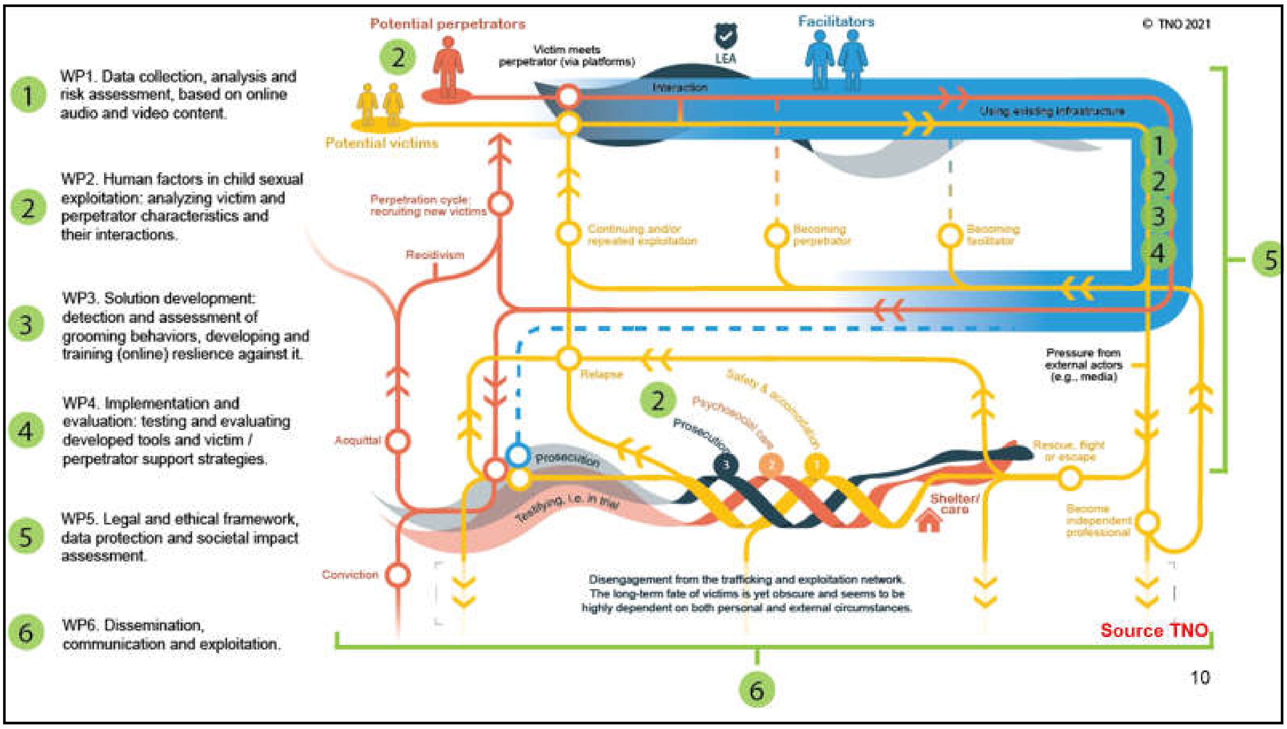


6. Hello AI

43

Pieter Ceulen

44



1 WP1. Data collection, analysis and risk assessment, based on online audio and video content.

2 WP2. Human factors in child sexual exploitation: analyzing victim and perpetrator characteristics and their interactions.

3 WP3. Solution development: detection and assessment of grooming behaviors, developing and training (online) reslience against it.

4 WP4. Implementation and evaluation: testing and evaluating developed tools and victim / perpetrator support strategies.

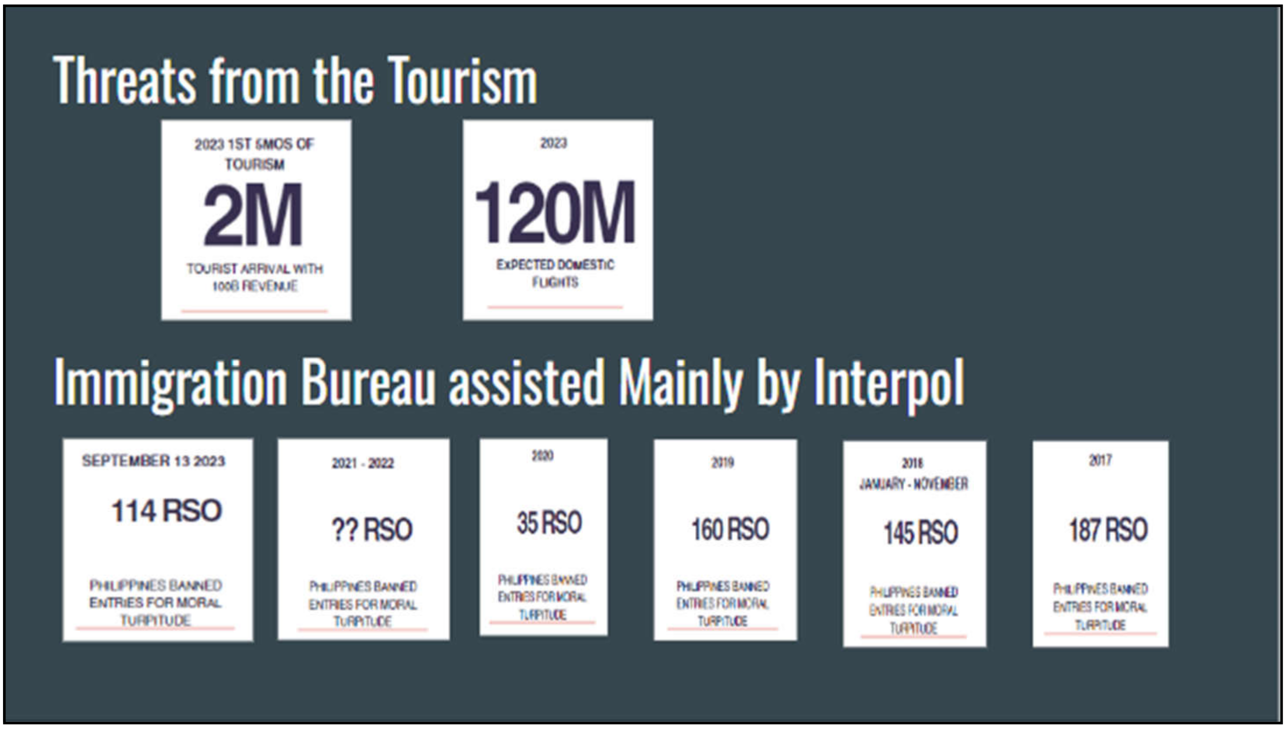
5 WP5. Legal and ethical framework, data protection and societal impact assessment.

6 WP6. Dissemination, communication and exploitation.

Potential perpetrators
2
Victim meets perpetrator (via platforms)
LEA
Facilitators
© TNO 2021
Interaction
Using existing infrastructure
Potential victims
1
2
3
4
5
Perpetration cycle: recruiting new victims
Recidivism
Continuing and/or repeated exploitation
Becoming perpetrator
Becoming facilitator
Pressure from external actors (e.g., media)
Relapse
2
Safety & accomodation
Psychosocial care
Prosecution
3
2
1
Prosecution
Acquittal
Testifying, i.e. in trial
Rescue, fight or escape
Shelter/ care
Become independent professional
Conviction
Disengagement from the trafficking and exploitation network. The long-term fate of victims is yet obscure and seems to be highly dependent on both personal and external circumstances.
6
10

Source TNO

45



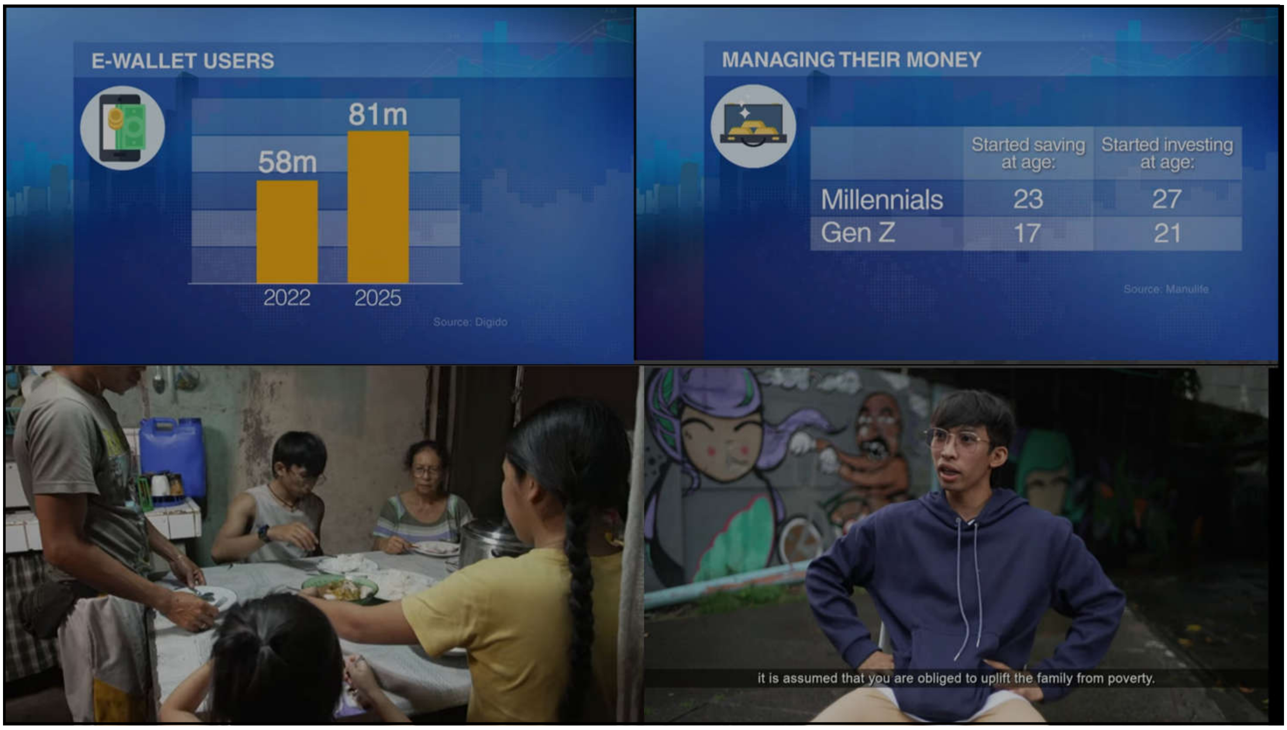
Threats from the Tourism

2023 1ST 6MOS OF TOURISM	2023
2M	120M
TOURIST ARRIVAL WITH 100B REVENUE	EXPECTED DOMESTIC FLIGHTS

Immigration Bureau assisted Mainly by Interpol

SEPTEMBER 13 2023	2021 - 2022	2020	2019	2018 JANUARY - NOVEMBER	2017
114 RSO	?? RSO	35 RSO	160 RSO	145 RSO	187 RSO
PHILIPPINES BANNED ENTRIES FOR MORAL TURPITUDE	PHILIPPINES BANNED ENTRIES FOR MORAL TURPITUDE	PHILIPPINES BANNED ENTRIES FOR MORAL TURPITUDE	PHILIPPINES BANNED ENTRIES FOR MORAL TURPITUDE	PHILIPPINES BANNED ENTRIES FOR MORAL TURPITUDE	PHILIPPINES BANNED ENTRIES FOR MORAL TURPITUDE

46



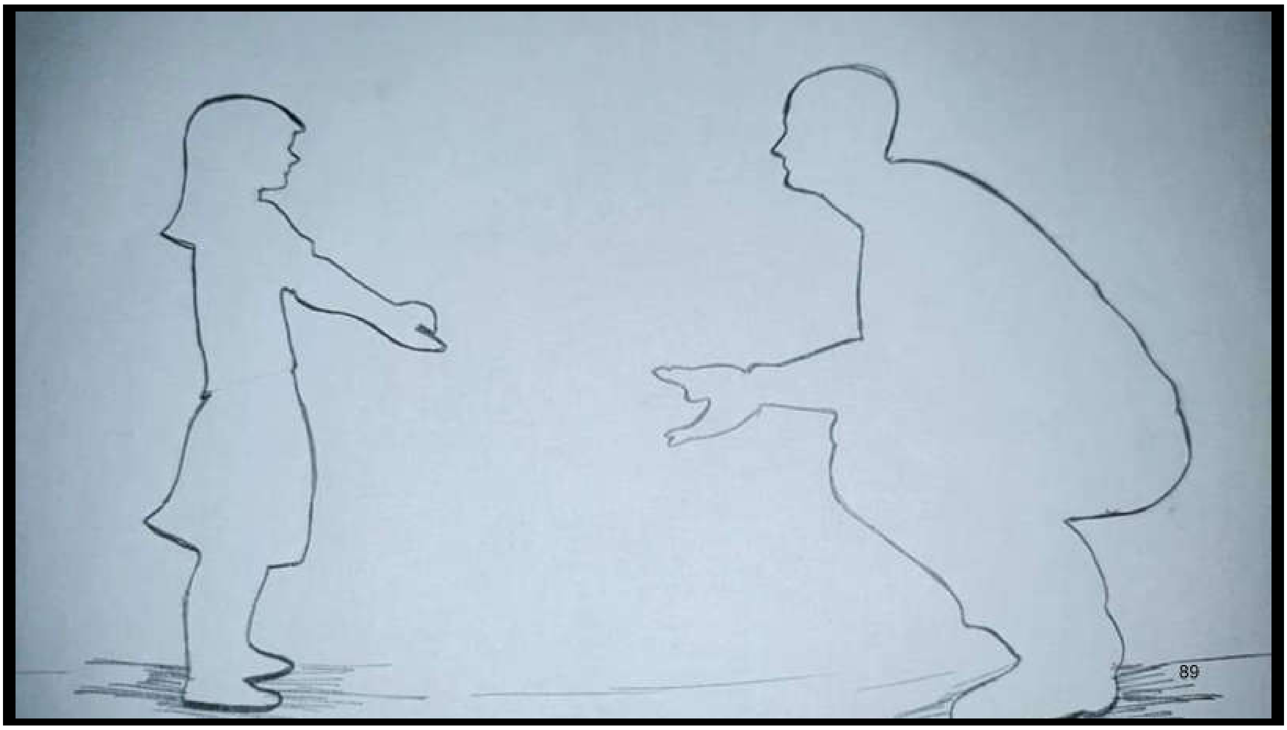
MANAGING THEIR MONEY

	Started saving at age:	Started investing at age:
Millennials	23	27
Gen Z	17	21

Source: Manulife

it is assumed that you are obliged to uplift the family from poverty.

47



48

HANDLING ELECTRONIC EVIDENCE IN COURTS

ERA Seminar in Cracow, 21-22 September 2023
Polish National School of the Judiciary and Public Prosecution

Emmanuelle Legrand
French Magistrate
emmanuelle.legrand@finances.gouv.fr

Senior Legal and Policy Officer (Artificial intelligence/Cloud & Data) - Digital Economy Department - French Ministry of Economy, Finance, and Industrial and Digital Sovereignty

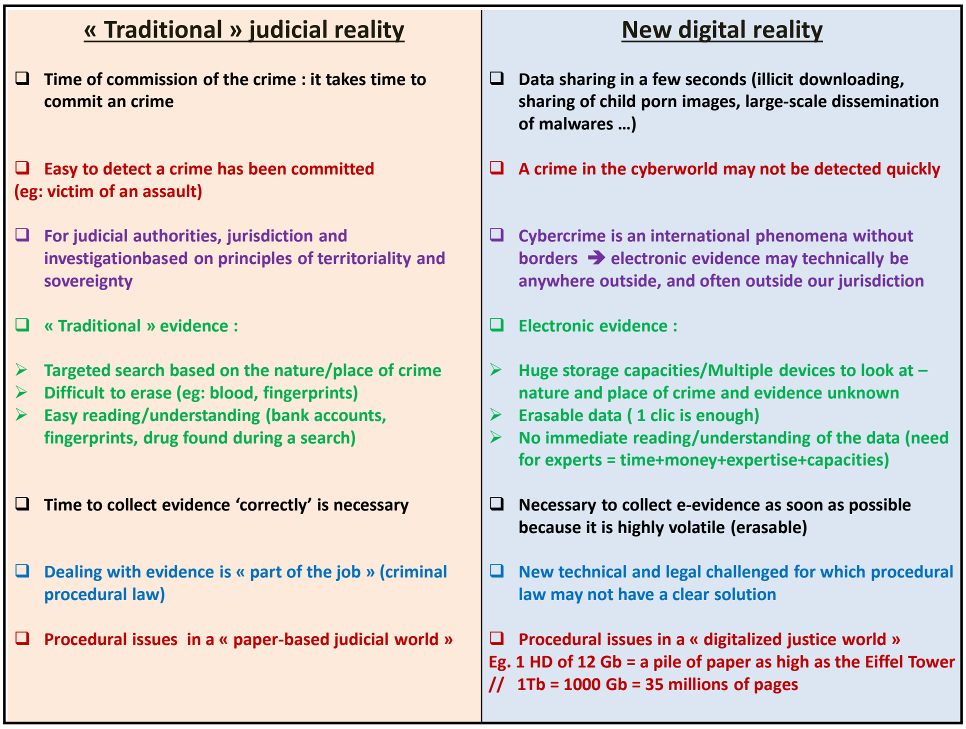
Former prosecutor, investigating judge, trial judge, Central authority prosecutor on mutual legal assistance, Seconded National Expert on electronic evidence and judicial cooperation in the EU Commission, French liaison prosecutor in Western Balkans

Engaged in the French cyber citizen's reserve in the National Gendarmerie (Lieutenant-Colonel (RC) - ad honores)

Co-funded by the European Union

Disclaimer: The views presented are personal and are not endorsed by any institution.

1



« Traditional » judicial reality	New digital reality
❑ Time of commission of the crime : it takes time to commit an crime	❑ Data sharing in a few seconds (illicit downloading, sharing of child porn images, large-scale dissemination of malwares …)
❑ Easy to detect a crime has been committed (eg: victim of an assault)	❑ A crime in the cyberworld may not be detected quickly
❑ For judicial authorities, jurisdiction and investigationbased on principles of territoriality and sovereignty	❑ Cybercrime is an international phenomena without borders ➔ electronic evidence may technically be anywhere outside, and often outside our jurisdiction
❑ « Traditional » evidence :	❑ Electronic evidence :
➢ Targeted search based on the nature/place of crime ➢ Difficult to erase (eg: blood, fingerprints) ➢ Easy reading/understanding (bank accounts, fingerprints, drug found during a search)	➢ Huge storage capacities/Multiple devices to look at – nature and place of crime and evidence unknown ➢ Erasable data (1 clic is enough) ➢ No immediate reading/understanding of the data (need for experts = time+money+expertise+capacities)
❑ Time to collect evidence 'correctly' is necessary	❑ Necessary to collect e-evidence as soon as possible because it is highly volatile (erasable)
❑ Dealing with evidence is « part of the job » (criminal procedural law)	❑ New technical and legal challenged for which procedural law may not have a clear solution
❑ Procedural issues in a « paper-based judicial world »	❑ Procedural issues in a « digitalized justice world » Eg. 1 HD of 12 Gb = a pile of paper as high as the Eiffel Tower // 1Tb = 1000 Gb = 35 millions of pages

2

Quick survey

How many of you think your national law expressly deals with all situations you may encounter with electronic evidence?

3

Handling electronic evidence in court:

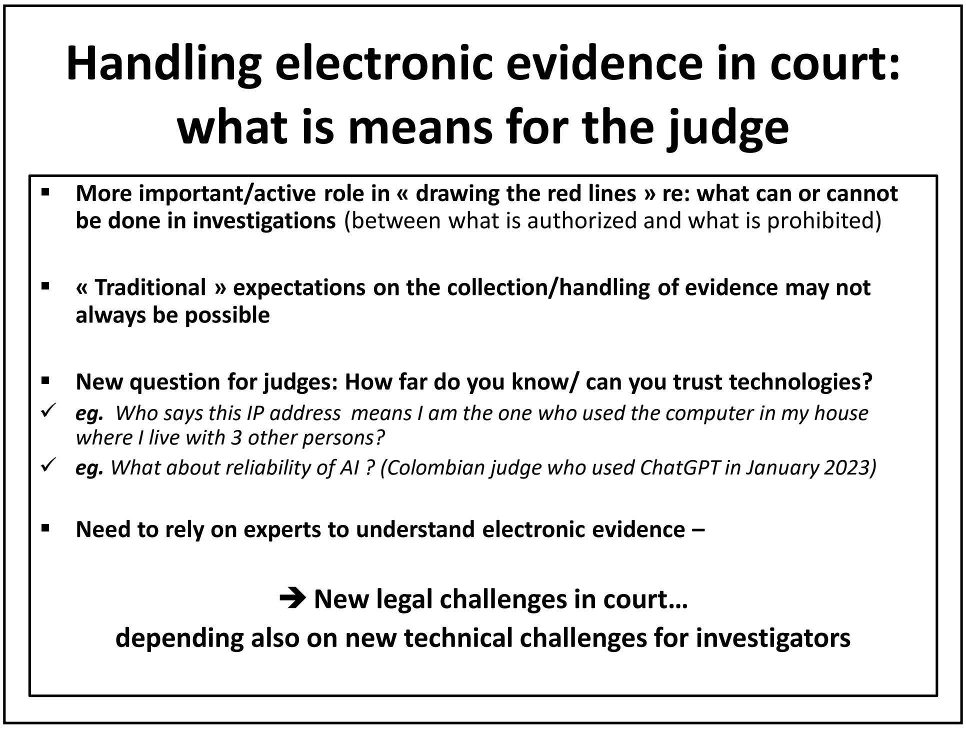
When a situation is NOT specifically dealt with in the criminal procedural law, does that mean:

ALLOWED BECAUSE NOT FORBIDDEN

OR

FORBIDDEN BECAUSE NOT EXPRESSLY ALLOWED

4



Handling electronic evidence in court: what is means for the judge

- **More important/active role in « drawing the red lines » re: what can or cannot be done in investigations** (between what is authorized and what is prohibited)
- **« Traditional » expectations on the collection/handling of evidence may not always be possible**
- **New question for judges: How far do you know/ can you trust technologies?**

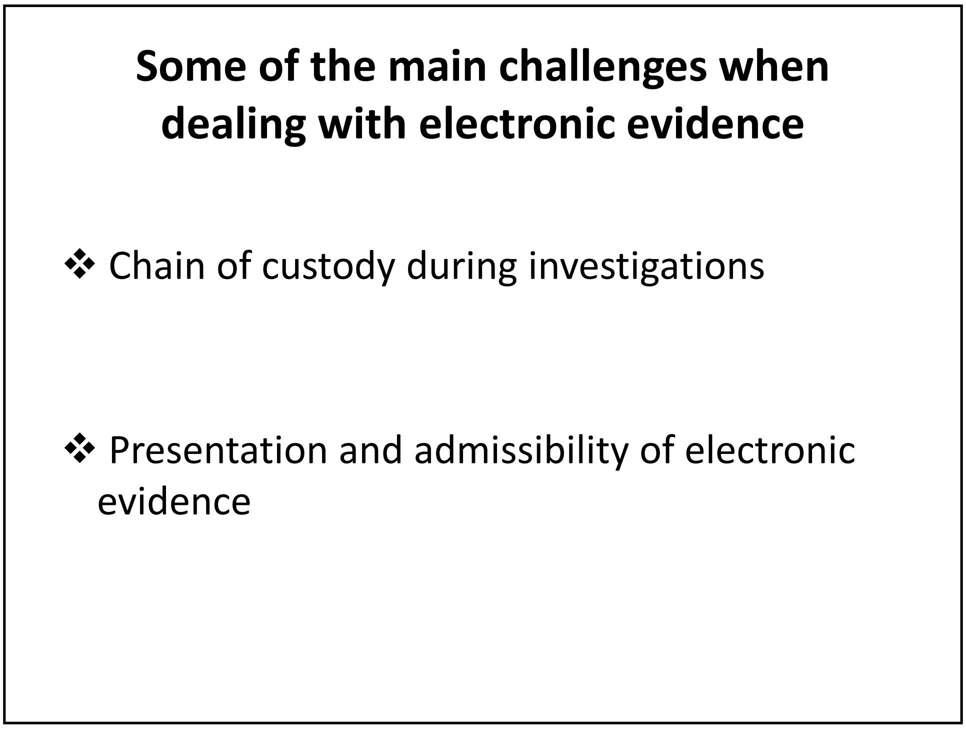
✓ ***eg.*** *Who says this IP address means I am the one who used the computer in my house where I live with 3 other persons?*

✓ ***eg.*** *What about reliability of AI ? (Colombian judge who used ChatGPT in January 2023)*

- **Need to rely on experts to understand electronic evidence –**

➔ New legal challenges in court…
depending also on new technical challenges for investigators

5

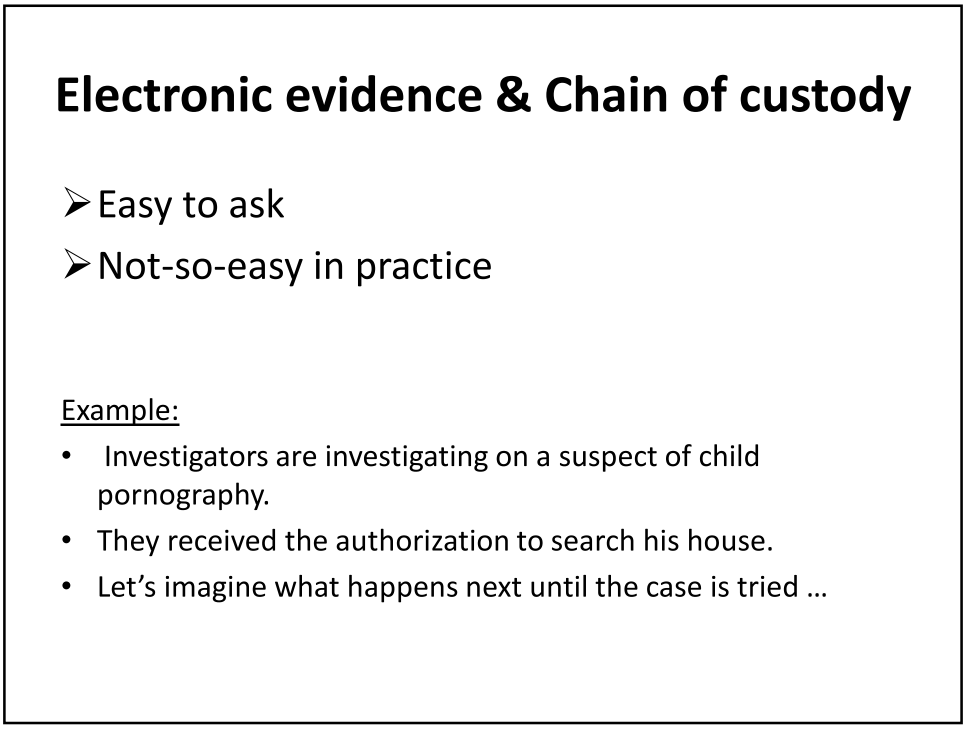


Some of the main challenges when dealing with electronic evidence

❖ Chain of custody during investigations

❖ Presentation and admissibility of electronic evidence

6



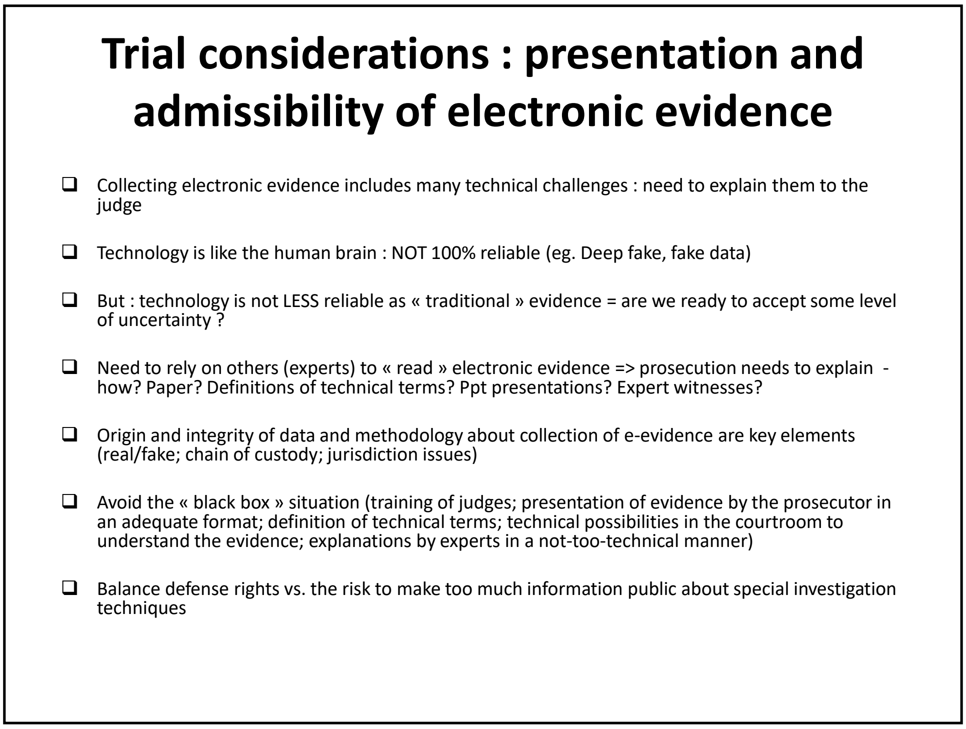
Electronic evidence & Chain of custody

- ➢ Easy to ask
- ➢ Not-so-easy in practice

Example:

- Investigators are investigating on a suspect of child pornography.
- They received the authorization to search his house.
- Let’s imagine what happens next until the case is tried …

7



Trial considerations : presentation and admissibility of electronic evidence

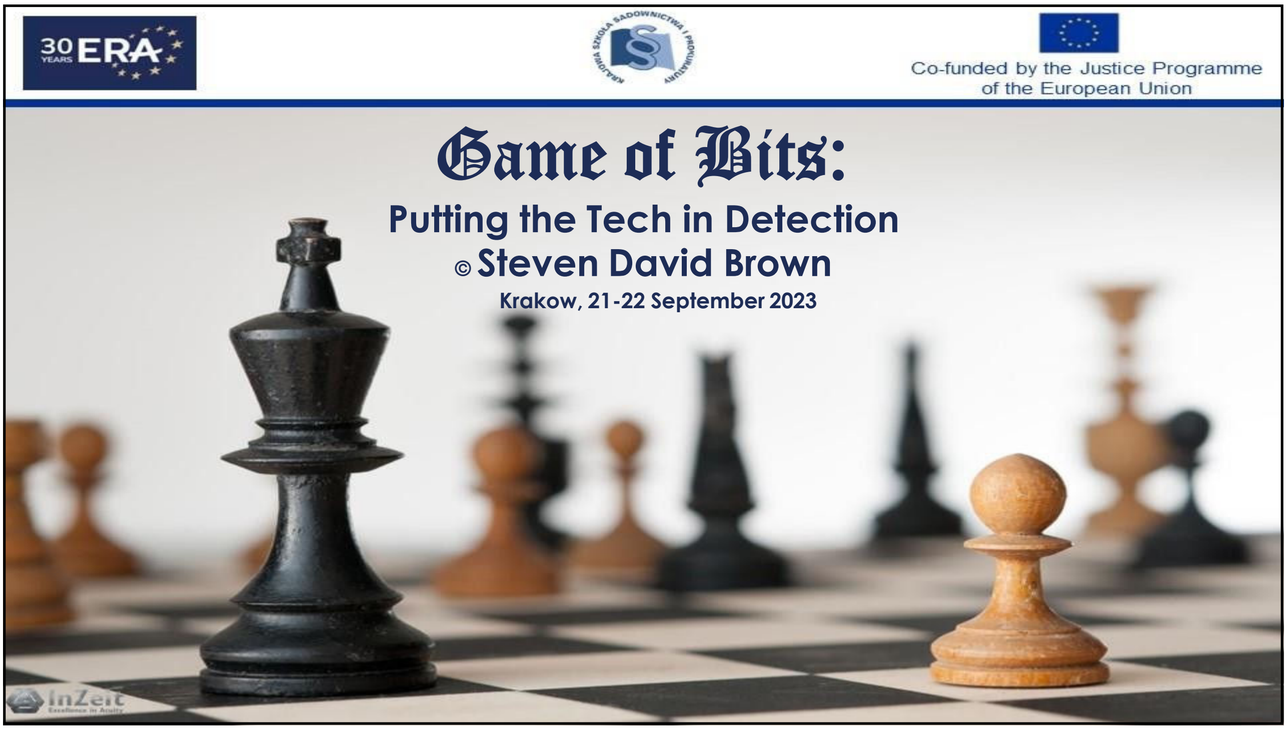
- ❑ Collecting electronic evidence includes many technical challenges : need to explain them to the judge
- ❑ Technology is like the human brain : NOT 100% reliable (eg. Deep fake, fake data)
- ❑ But : technology is not LESS reliable as « traditional » evidence = are we ready to accept some level of uncertainty ?
- ❑ Need to rely on others (experts) to « read » electronic evidence => prosecution needs to explain - how? Paper? Definitions of technical terms? Ppt presentations? Expert witnesses?
- ❑ Origin and integrity of data and methodology about collection of e-evidence are key elements (real/fake; chain of custody; jurisdiction issues)
- ❑ Avoid the « black box » situation (training of judges; presentation of evidence by the prosecutor in an adequate format; definition of technical terms; technical possibilities in the courtroom to understand the evidence; explanations by experts in a not-too-technical manner)
- ❑ Balance defense rights vs. the risk to make too much information public about special investigation techniques

8

Good practices to share?
Questions?

emmanuelle.legrand@finances.gouv.fr

9



Co-funded by the Justice Programme of the European Union

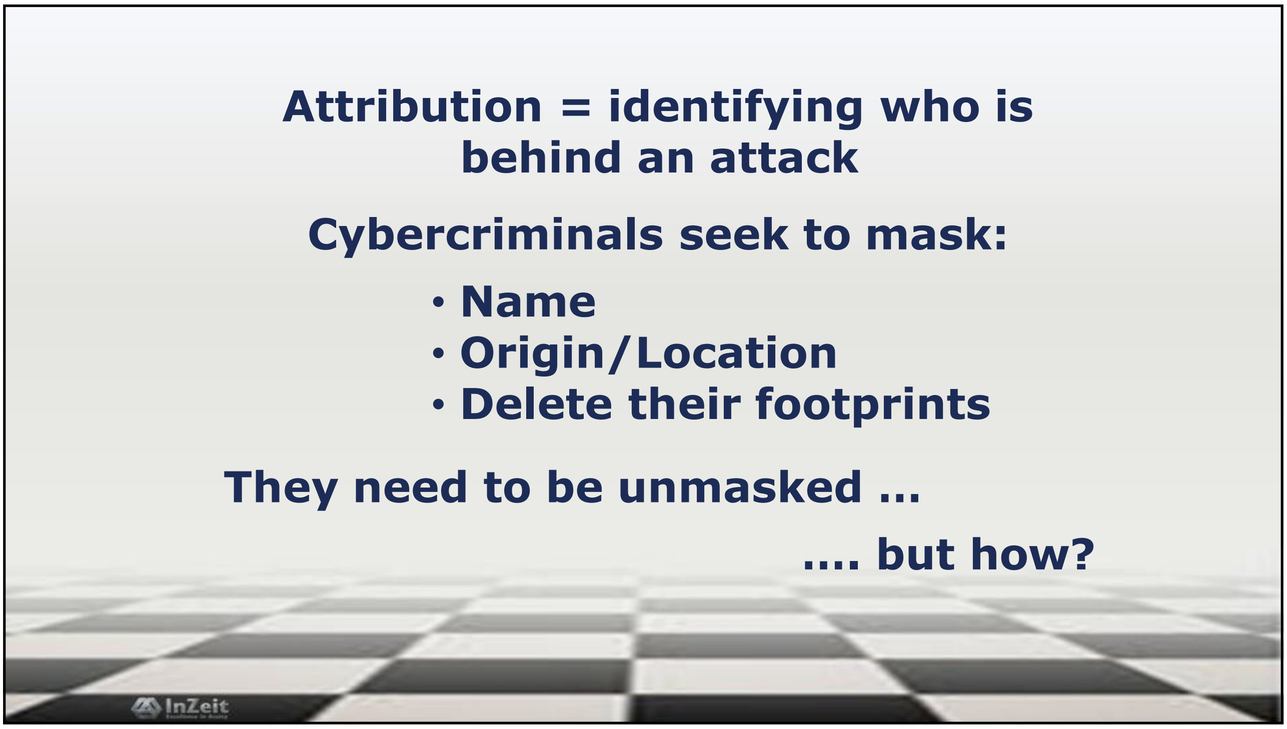
Game of Bits:

Putting the Tech in Detection

© Steven David Brown

Krakow, 21-22 September 2023

1



Attribution = identifying who is behind an attack

Cybercriminals seek to mask:

- **Name**
- **Origin/Location**
- **Delete their footprints**

They need to be unmasked …

…. but how?

2

The Challenge

Alias Accounts

Public wifi

Proxy ("Bullet proof") Servers

Ill-equipped counterparts

VPNs

Botnets

Hostile jurisdictions

Encryption

Lack of skills and equipment

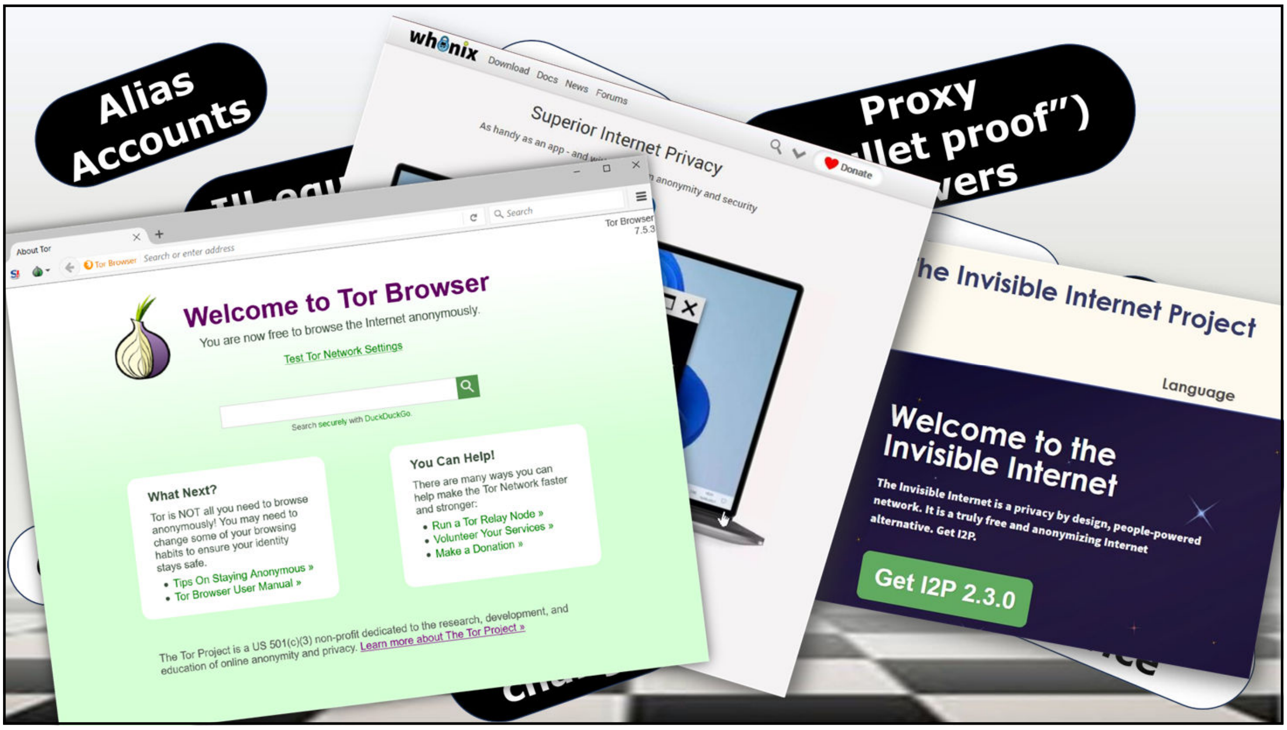
Carriergrade NAT

Crime-as-a-Service

Speed of change

InZeit

3



Alias Accounts

Proxy

llet proof")

vers

whonix

Download Docs News Forums

Superior Internet Privacy

As handy as an app - and wi

n anonymity and security

Donate

About Tor

Tor Browser Search or enter address

Search

Tor Browser 7.5.3

Welcome to Tor Browser

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with DuckDuckGo.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

- Tips On Staying Anonymous »
- Tor Browser User Manual »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

he Invisible Internet Project

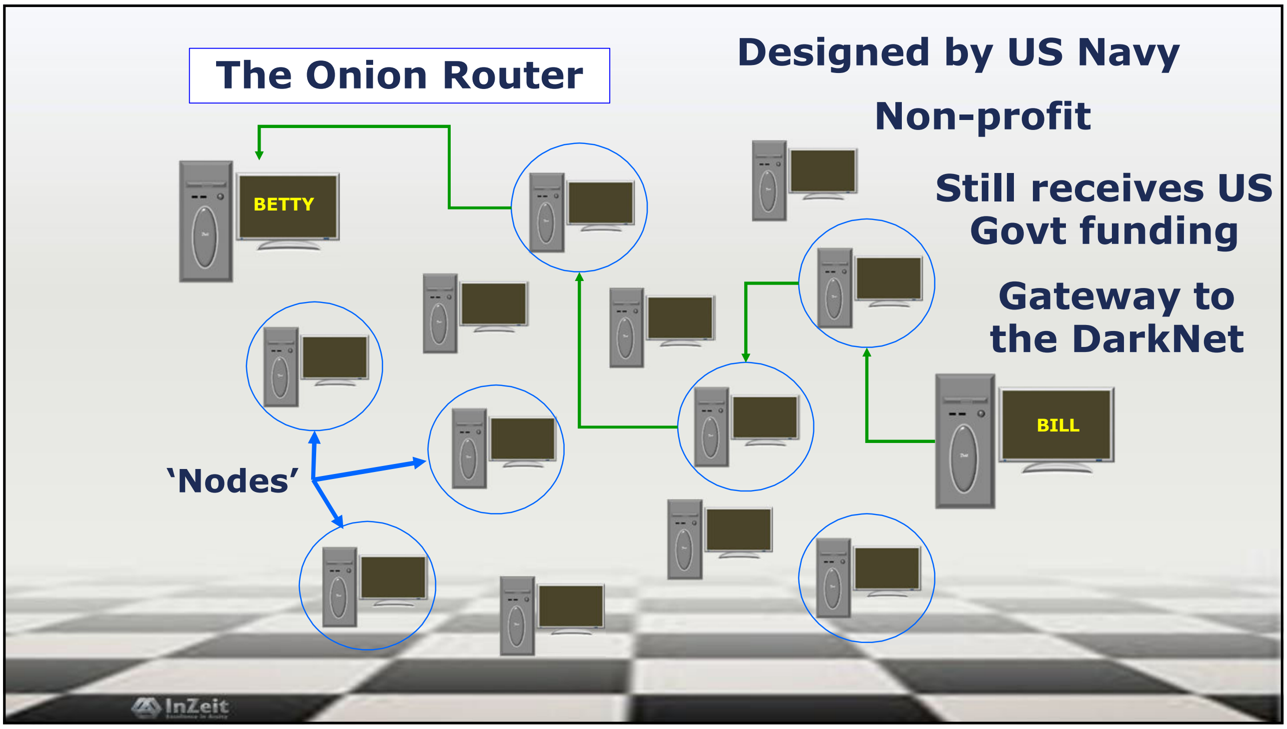
Language

Welcome to the Invisible Internet

The Invisible Internet is a privacy by design, people-powered network. It is a truly free and anonymizing Internet alternative. Get I2P.

Get I2P 2.3.0

4



The Onion Router

Designed by US Navy

Non-profit

Still receives US Govt funding

Gateway to the DarkNet

5

Has it been seen before?

Has it been linked to any actor(s)?

(i.e.) Has it been attributed?

Analysis of the malware code

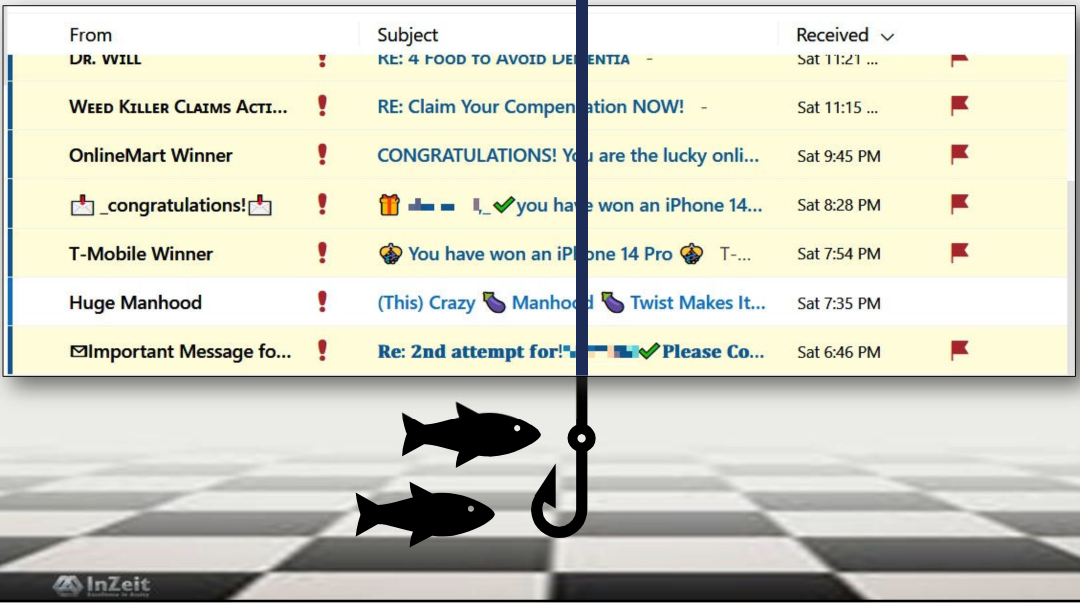
Any comments in code?

What language used?

Timing of attacks

6

Phishing



From		Subject	Received	
Dr. Will	!	RE: 4 Food to Avoid De entia -	Sat 11:21 ...	🚩
Weed Killer Claims Acti...	!	RE: Claim Your Compen ation NOW! -	Sat 11:15 ...	🚩
OnlineMart Winner	!	CONGRATULATIONS! Y u are the lucky onli...	Sat 9:45 PM	🚩
_congratulations!	!	✓you ha e won an iPhone 14...	Sat 8:28 PM	🚩
T-Mobile Winner	!	You have won an iP one 14 Pro T-...	Sat 7:54 PM	🚩
Huge Manhood	!	(This) Crazy Manho d Twist Makes It...	Sat 7:35 PM	
Important Message fo...	!	Re: 2nd attempt for! ✓Please Co...	Sat 6:46 PM	🚩

Kaspersky: "The number of phishing attacks doubled to reach over 500 million in 2022"

https://www.kaspersky.com/about/press-releases/2023_the-number-of-phishing-attacks-doubled-to-reach-over-500-million-in-2022

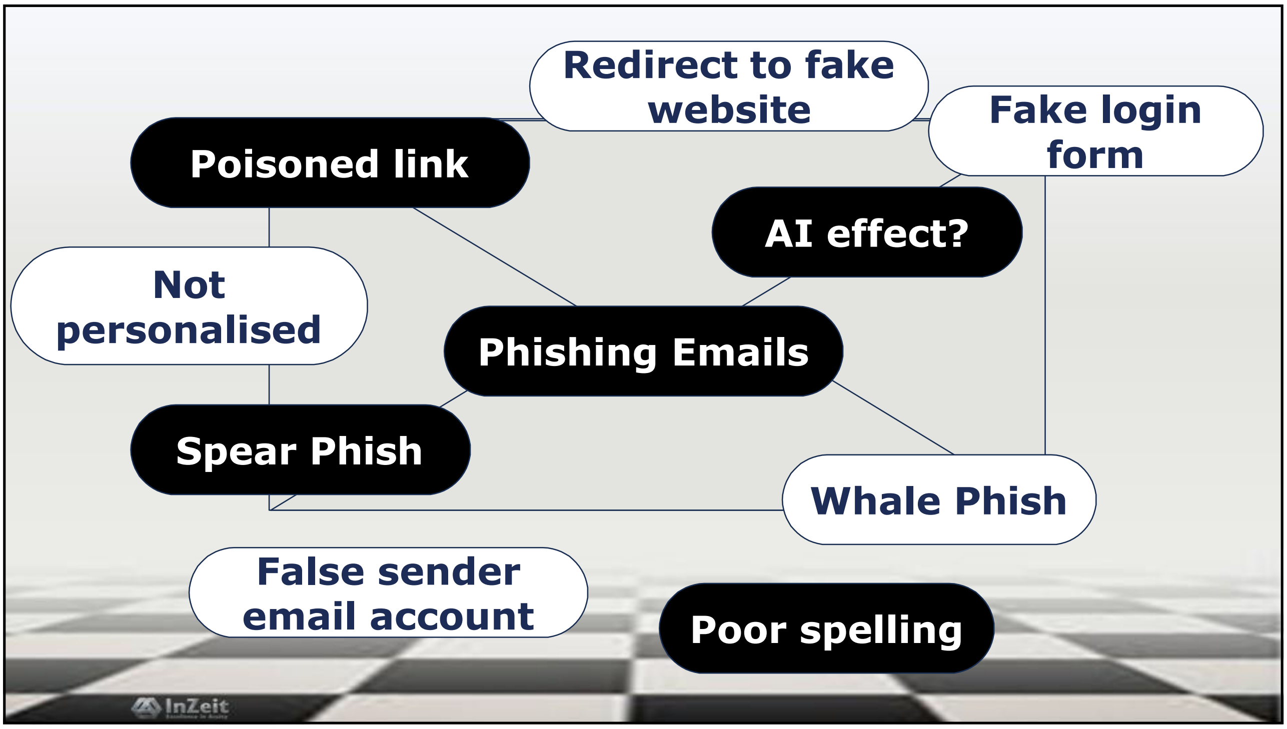
"Trend Micro™ Cloud App Security discovered nearly 40 million high-risk email threats in 2022"

https://www.trendmicro.com/en_us/ciso/23/e/worldwide-email-phishing-stats-examples-2023.html

"Phishing scams account for nearly 36% of all data breaches, according to Verizon's 2022 Data Breach Report. And according to a Proofpoint study, 83% of all companies experienced a phishing attack in 2021. "

https://www.techopedia.com/phishing-statistics#Phishing_Statistics_Highlights

Phishing



Redirect to fake website

Fake login form

Poisoned link

AI effect?

Not personalised

Phishing Emails

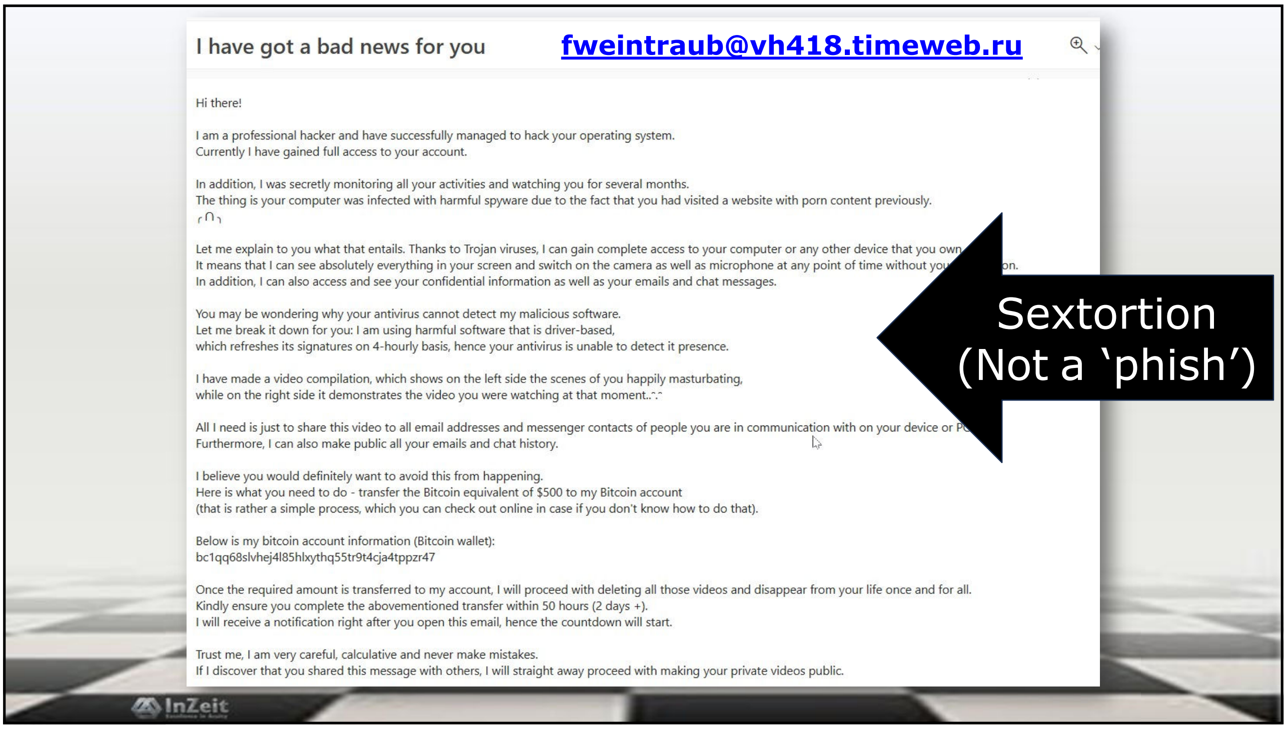
Spear Phish

Whale Phish

False sender email account

Poor spelling

9



I have got a bad news for you fweintraub@vh418.timeweb.ru

Hi there!

I am a professional hacker and have successfully managed to hack your operating system.
Currently I have gained full access to your account.

In addition, I was secretly monitoring all your activities and watching you for several months.
The thing is your computer was infected with harmful spyware due to the fact that you had visited a website with porn content previously.
╭∩╮

Let me explain to you what that entails. Thanks to Trojan viruses, I can gain complete access to your computer or any other device that you own
It means that I can see absolutely everything in your screen and switch on the camera as well as microphone at any point of time without you on.
In addition, I can also access and see your confidential information as well as your emails and chat messages.

You may be wondering why your antivirus cannot detect my malicious software.
Let me break it down for you: I am using harmful software that is driver-based,
which refreshes its signatures on 4-hourly basis, hence your antivirus is unable to detect it presence.

I have made a video compilation, which shows on the left side the scenes of you happily masturbating,
while on the right side it demonstrates the video you were watching at that moment..˜.˜

All I need is just to share this video to all email addresses and messenger contacts of people you are in communication with on your device or P
Furthermore, I can also make public all your emails and chat history.

I believe you would definitely want to avoid this from happening.
Here is what you need to do - transfer the Bitcoin equivalent of $500 to my Bitcoin account
(that is rather a simple process, which you can check out online in case if you don't know how to do that).

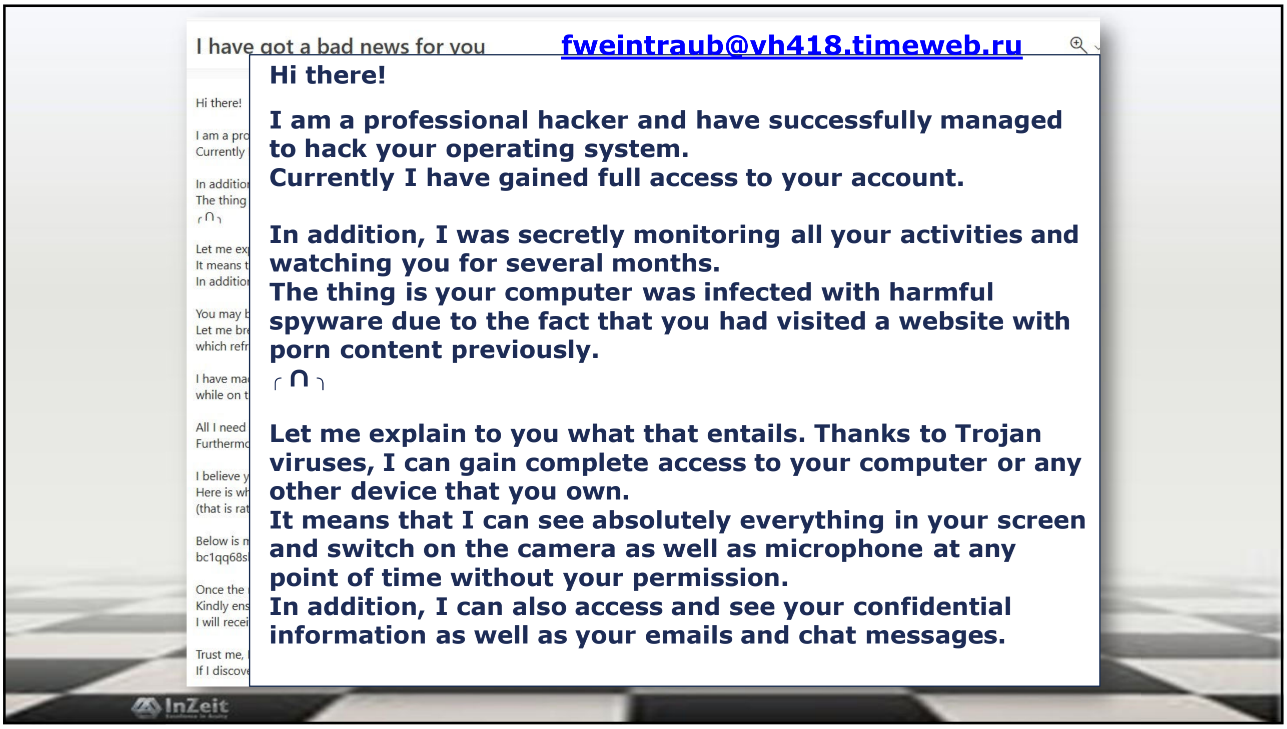
Below is my bitcoin account information (Bitcoin wallet):
bc1qq68slvhej4l85hlxythq55tr9t4cja4tppzr47

Once the required amount is transferred to my account, I will proceed with deleting all those videos and disappear from your life once and for all.
Kindly ensure you complete the abovementioned transfer within 50 hours (2 days +).
I will receive a notification right after you open this email, hence the countdown will start.

Trust me, I am very careful, calculative and never make mistakes.
If I discover that you shared this message with others, I will straight away proceed with making your private videos public.

Sextortion
(Not a 'phish')

10



fweintraub@vh418.timeweb.ru

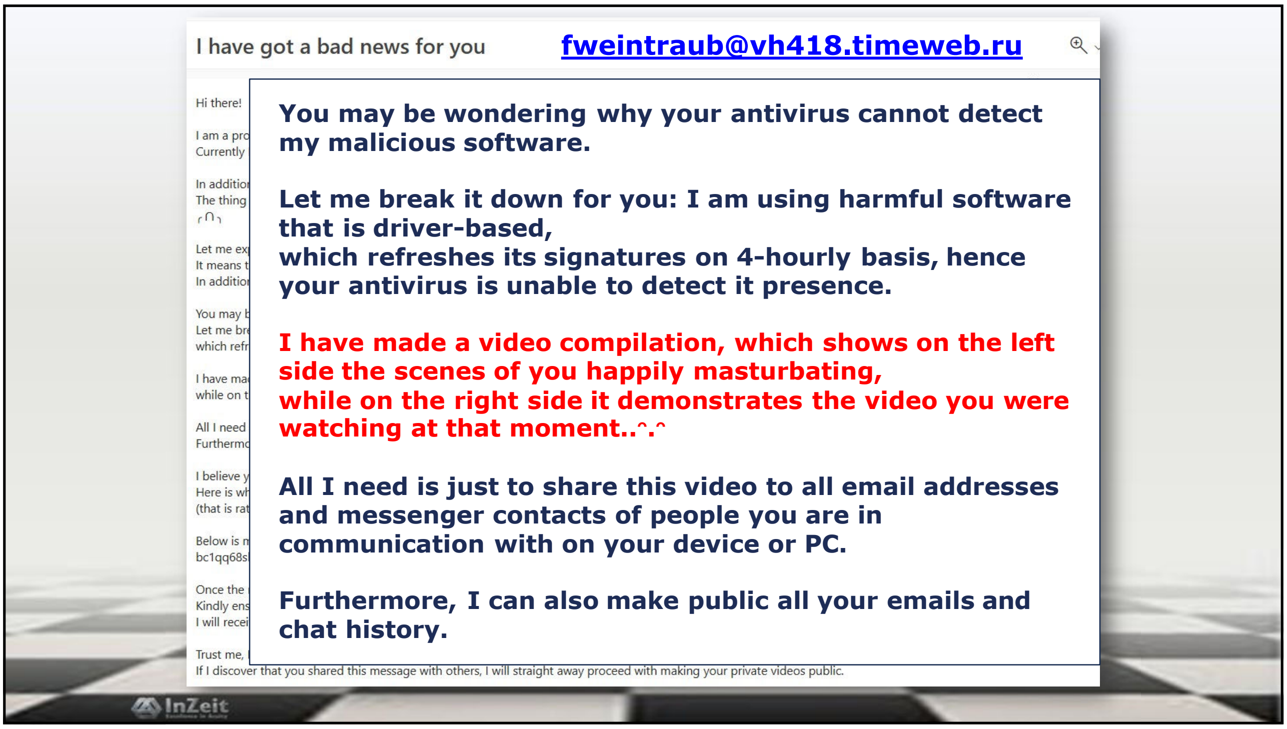
Hi there!

I am a professional hacker and have successfully managed to hack your operating system.
Currently I have gained full access to your account.

In addition, I was secretly monitoring all your activities and watching you for several months.
The thing is your computer was infected with harmful spyware due to the fact that you had visited a website with porn content previously.
╭∩╮

Let me explain to you what that entails. Thanks to Trojan viruses, I can gain complete access to your computer or any other device that you own.
It means that I can see absolutely everything in your screen and switch on the camera as well as microphone at any point of time without your permission.
In addition, I can also access and see your confidential information as well as your emails and chat messages.

11



fweintraub@vh418.timeweb.ru

You may be wondering why your antivirus cannot detect my malicious software.

Let me break it down for you: I am using harmful software that is driver-based,
which refreshes its signatures on 4-hourly basis, hence your antivirus is unable to detect it presence.

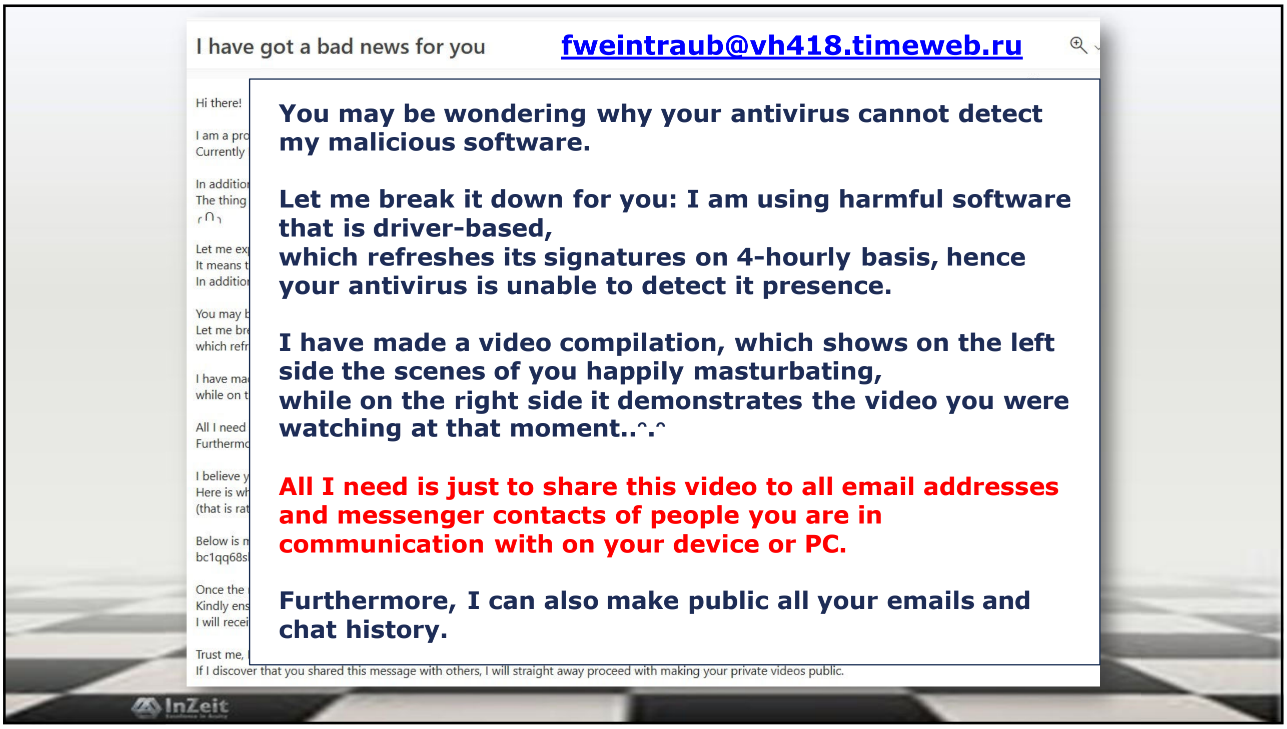
I have made a video compilation, which shows on the left side the scenes of you happily masturbating,
while on the right side it demonstrates the video you were watching at that moment..^.^

All I need is just to share this video to all email addresses and messenger contacts of people you are in communication with on your device or PC.

Furthermore, I can also make public all your emails and chat history.

If I discover that you shared this message with others, I will straight away proceed with making your private videos public.

12



I have got a bad news for you

fweintraub@vh418.timeweb.ru

Hi there!

I am a pro
Currently

In additio
The thing

Let me ex
It means t
In additio

You may b
Let me br
which refr

I have ma
while on t

All I need
Furtherm

I believe y
Here is wh
(that is rat

Below is m
bc1qq68s

Once the
Kindly ens
I will recei

Trust me,
If I discover that you shared this message with others, I will straight away proceed with making your private videos public.

You may be wondering why your antivirus cannot detect my malicious software.

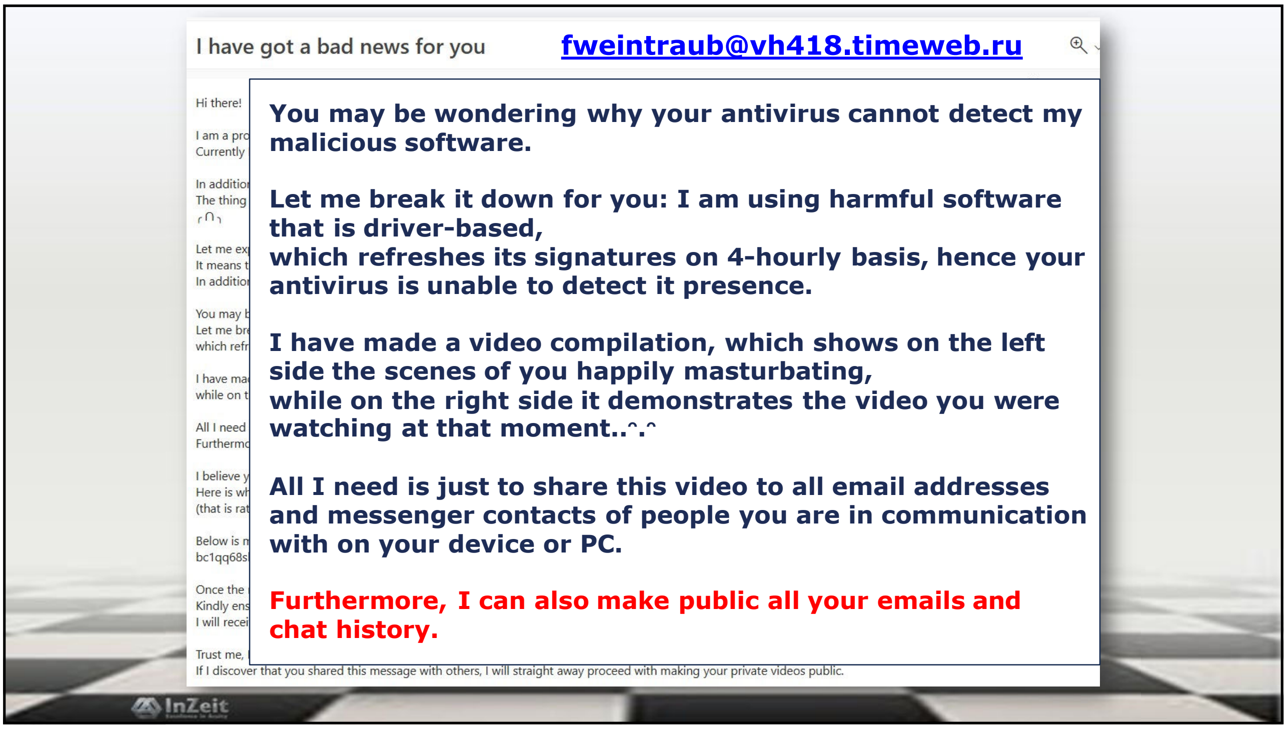
Let me break it down for you: I am using harmful software that is driver-based,
which refreshes its signatures on 4-hourly basis, hence your antivirus is unable to detect it presence.

I have made a video compilation, which shows on the left side the scenes of you happily masturbating,
while on the right side it demonstrates the video you were watching at that moment..^.^

All I need is just to share this video to all email addresses and messenger contacts of people you are in communication with on your device or PC.

Furthermore, I can also make public all your emails and chat history.

13



I have got a bad news for you

fweintraub@vh418.timeweb.ru

Hi there!

I am a pro
Currently

In additio
The thing

Let me ex
It means t
In additio

You may b
Let me br
which refr

I have ma
while on t

All I need
Furtherm

I believe y
Here is wh
(that is rat

Below is m
bc1qq68s

Once the
Kindly ens
I will recei

Trust me,
If I discover that you shared this message with others, I will straight away proceed with making your private videos public.

You may be wondering why your antivirus cannot detect my malicious software.

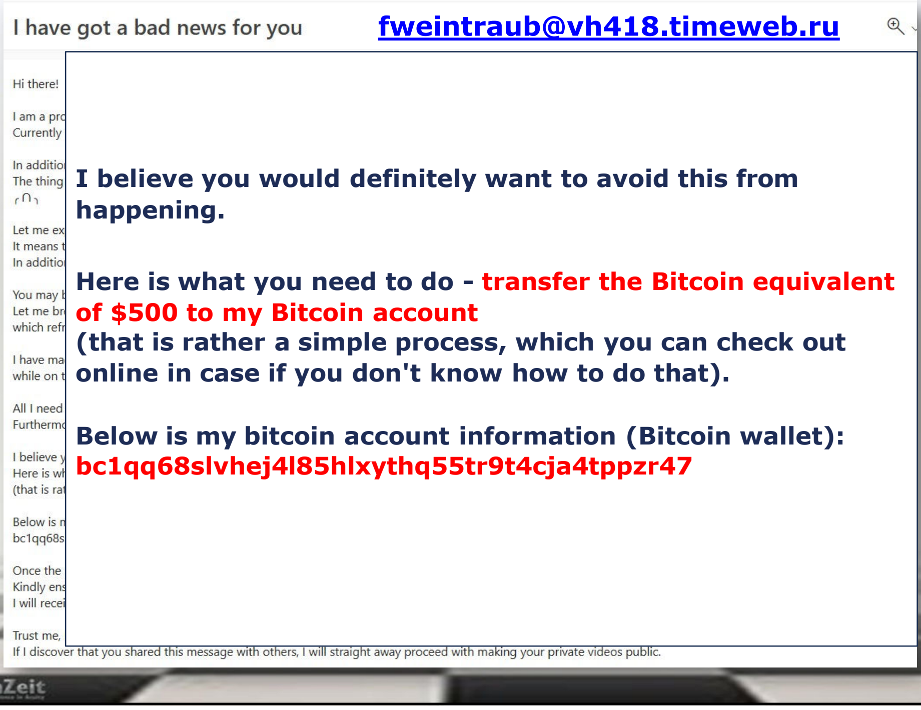
Let me break it down for you: I am using harmful software that is driver-based,
which refreshes its signatures on 4-hourly basis, hence your antivirus is unable to detect it presence.

I have made a video compilation, which shows on the left side the scenes of you happily masturbating,
while on the right side it demonstrates the video you were watching at that moment..^.^

All I need is just to share this video to all email addresses and messenger contacts of people you are in communication with on your device or PC.

Furthermore, I can also make public all your emails and chat history.

14



I have got a bad news for you

fweintraub@vh418.timeweb.ru

Hi there!

I am a pro
Currently

In additio
The thing

Let me ex
It means t
In additio

You may b
Let me br
which refe

I have ma
while on t

All I need
Furthermo

I believe y
Here is wh
(that is rat

Below is m
bc1qq68s

Once the
Kindly ens
I will recei

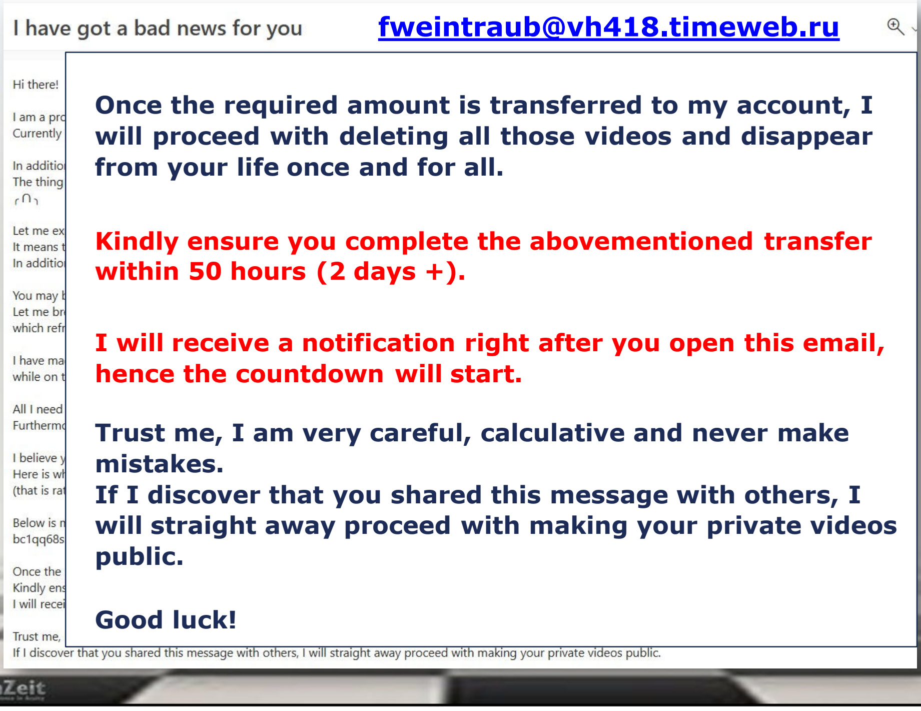
Trust me,
If I discover that you shared this message with others, I will straight away proceed with making your private videos public.

I believe you would definitely want to avoid this from happening.

Here is what you need to do - transfer the Bitcoin equivalent of $500 to my Bitcoin account
(that is rather a simple process, which you can check out online in case if you don't know how to do that).

Below is my bitcoin account information (Bitcoin wallet):
bc1qq68slvhej4l85hlxythq55tr9t4cja4tppzr47

15



I have got a bad news for you

fweintraub@vh418.timeweb.ru

Hi there!

I am a pro
Currently

In additio
The thing

Let me ex
It means t
In additio

You may b
Let me br
which refe

I have ma
while on t

All I need
Furthermo

I believe y
Here is wh
(that is rat

Below is m
bc1qq68s

Once the
Kindly ens
I will recei

Trust me,
If I discover that you shared this message with others, I will straight away proceed with making your private videos public.

Once the required amount is transferred to my account, I will proceed with deleting all those videos and disappear from your life once and for all.

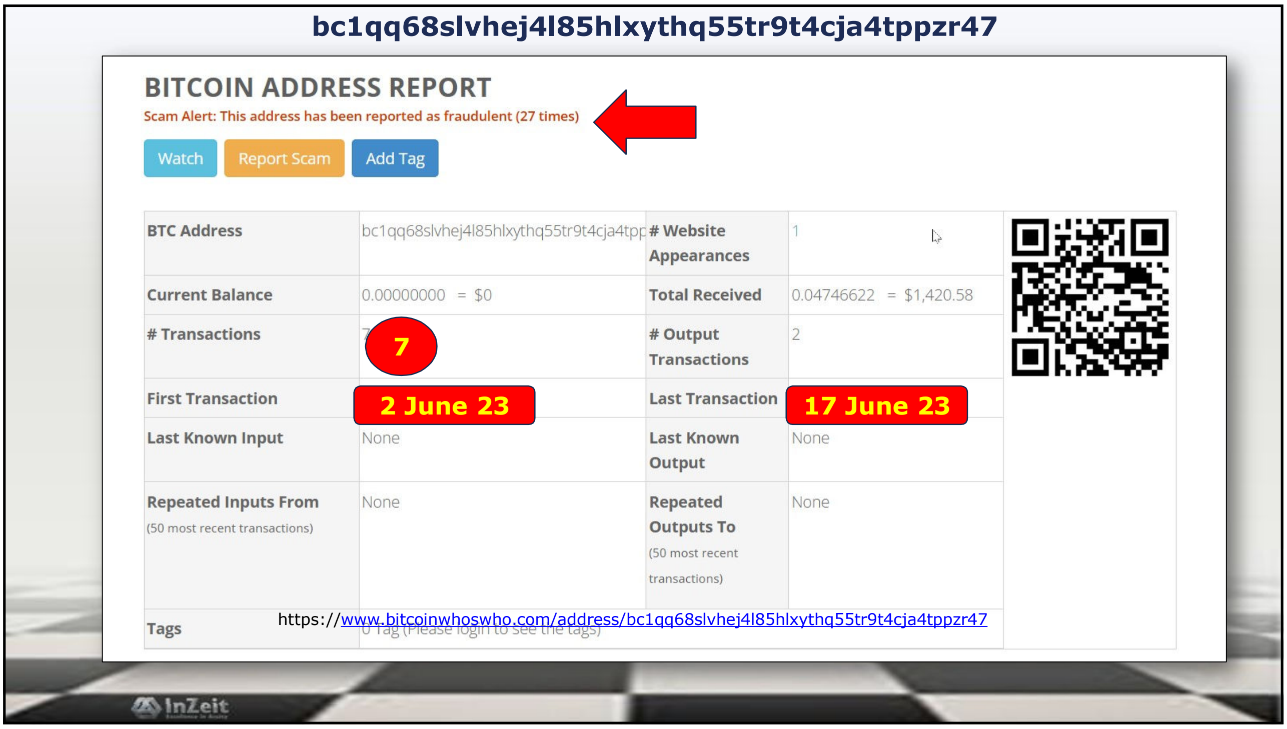
Kindly ensure you complete the abovementioned transfer within 50 hours (2 days +).

I will receive a notification right after you open this email, hence the countdown will start.

Trust me, I am very careful, calculative and never make mistakes.
If I discover that you shared this message with others, I will straight away proceed with making your private videos public.

Good luck!

16



bc1qq68slvhej4l85hlxythq55tr9t4cja4tppzr47

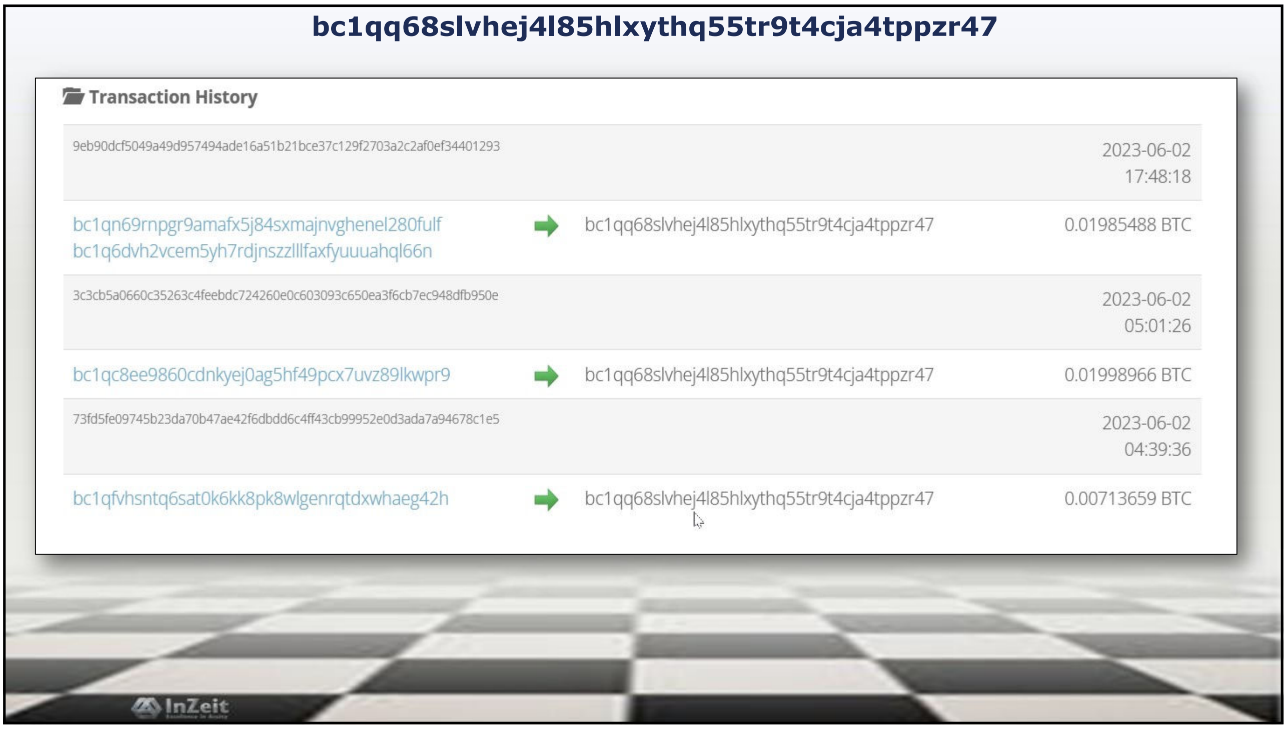
BITCOIN ADDRESS REPORT

Scam Alert: This address has been reported as fraudulent (27 times)

BTC Address	bc1qq68slvhej4l85hlxythq55tr9t4cja4tpp	# Website Appearances	1
Current Balance	0.00000000 = $0	Total Received	0.04746622 = $1,420.58
# Transactions	7	# Output Transactions	2
First Transaction	2 June 23	Last Transaction	17 June 23
Last Known Input	None	Last Known Output	None
Repeated Inputs From (50 most recent transactions)	None	Repeated Outputs To (50 most recent transactions)	None
Tags	0 Tag (Please login to see the tags)		

https://www.bitcoinwhoswho.com/address/bc1qq68slvhej4l85hlxythq55tr9t4cja4tppzr47

17

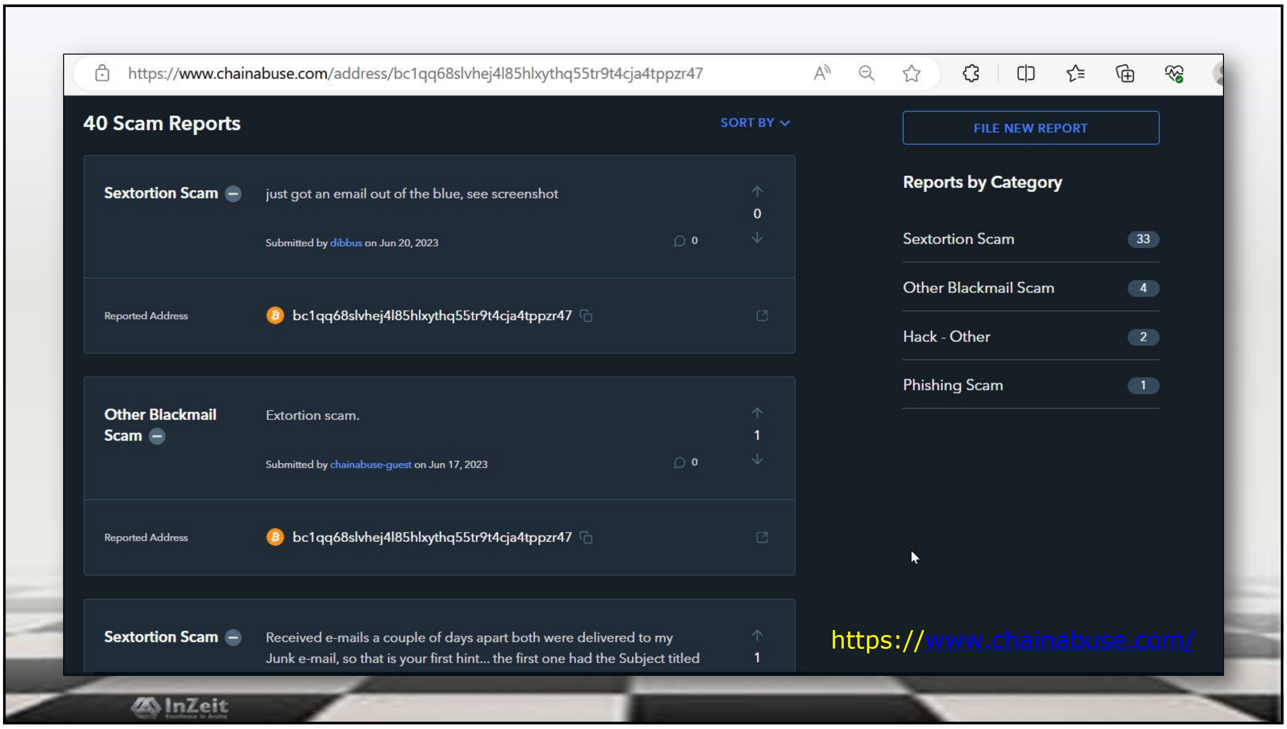


bc1qq68slvhej4l85hlxythq55tr9t4cja4tppzr47

Transaction History

9eb90dcf5049a49d957494ade16a51b21bce37c129f2703a2c2af0ef34401293			2023-06-02 17:48:18
bc1qn69rnpgr9amafx5j84sxmajnvghenel280fulf bc1q6dvh2vcem5yh7rdjnszzlllfaxfyuuuahql66n	➡	bc1qq68slvhej4l85hlxythq55tr9t4cja4tppzr47	0.01985488 BTC
3c3cb5a0660c35263c4feebdc724260e0c603093c650ea3f6cb7ec948dfb950e			2023-06-02 05:01:26
bc1qc8ee9860cdnkyej0ag5hf49pcx7uvz89lkwpr9	➡	bc1qq68slvhej4l85hlxythq55tr9t4cja4tppzr47	0.01998966 BTC
73fd5fe09745b23da70b47ae42f6dbdd6c4ff43cb99952e0d3ada7a94678c1e5			2023-06-02 04:39:36
bc1qfvhsntq6sat0k6kk8pk8wlgenrqtdxwhaeg42h	➡	bc1qq68slvhej4l85hlxythq55tr9t4cja4tppzr47	0.00713659 BTC

18



https://www.chainabuse.com/address/bc1qq68slvhej4l85hlxythq55tr9t4cja4tppzr47

40 Scam Reports

SORT BY

FILE NEW REPORT

Sextortion Scam — just got an email out of the blue, see screenshot

Submitted by dibbus on Jun 20, 2023 — 0

Reported Address: bc1qq68slvhej4l85hlxythq55tr9t4cja4tppzr47

Other Blackmail Scam — Extortion scam.

Submitted by chainabuse-guest on Jun 17, 2023 — 1

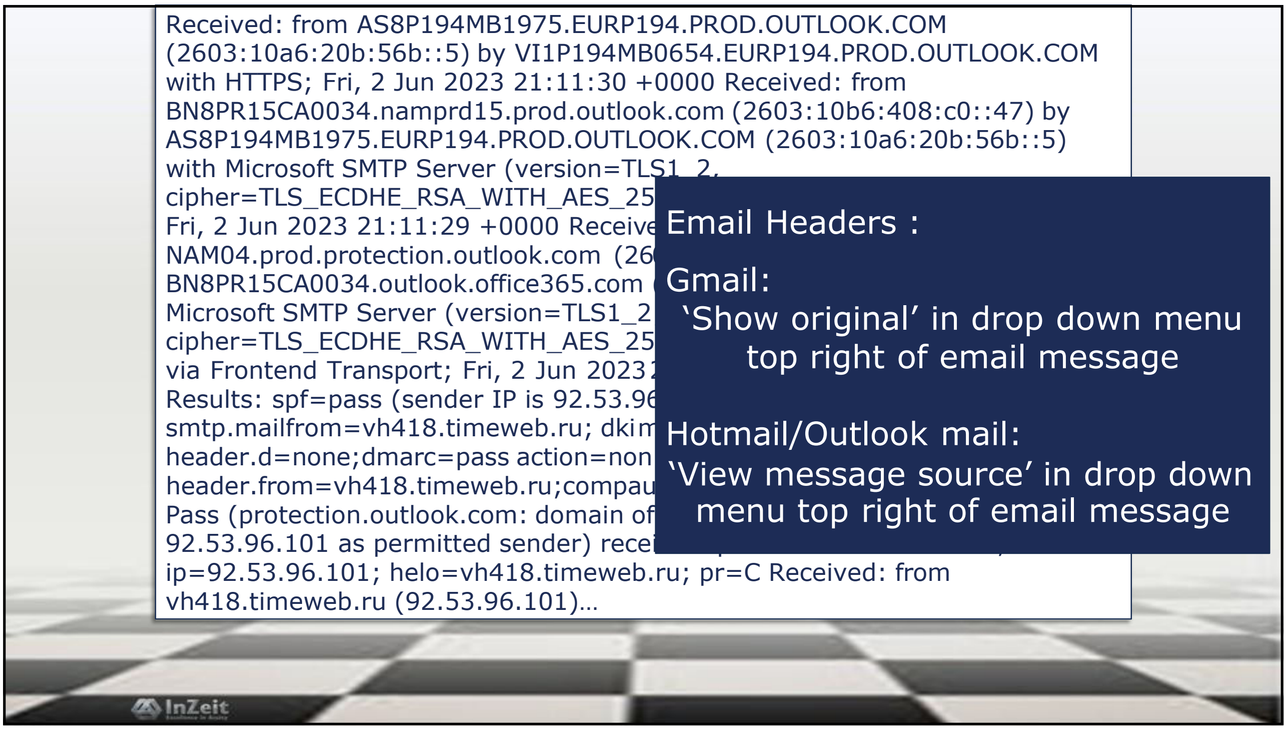
Reported Address: bc1qq68slvhej4l85hlxythq55tr9t4cja4tppzr47

Sextortion Scam — Received e-mails a couple of days apart both were delivered to my Junk e-mail, so that is your first hint... the first one had the Subject titled — 1

Reports by Category

Sextortion Scam	33
Other Blackmail Scam	4
Hack - Other	2
Phishing Scam	1

https://www.chainabuse.com/

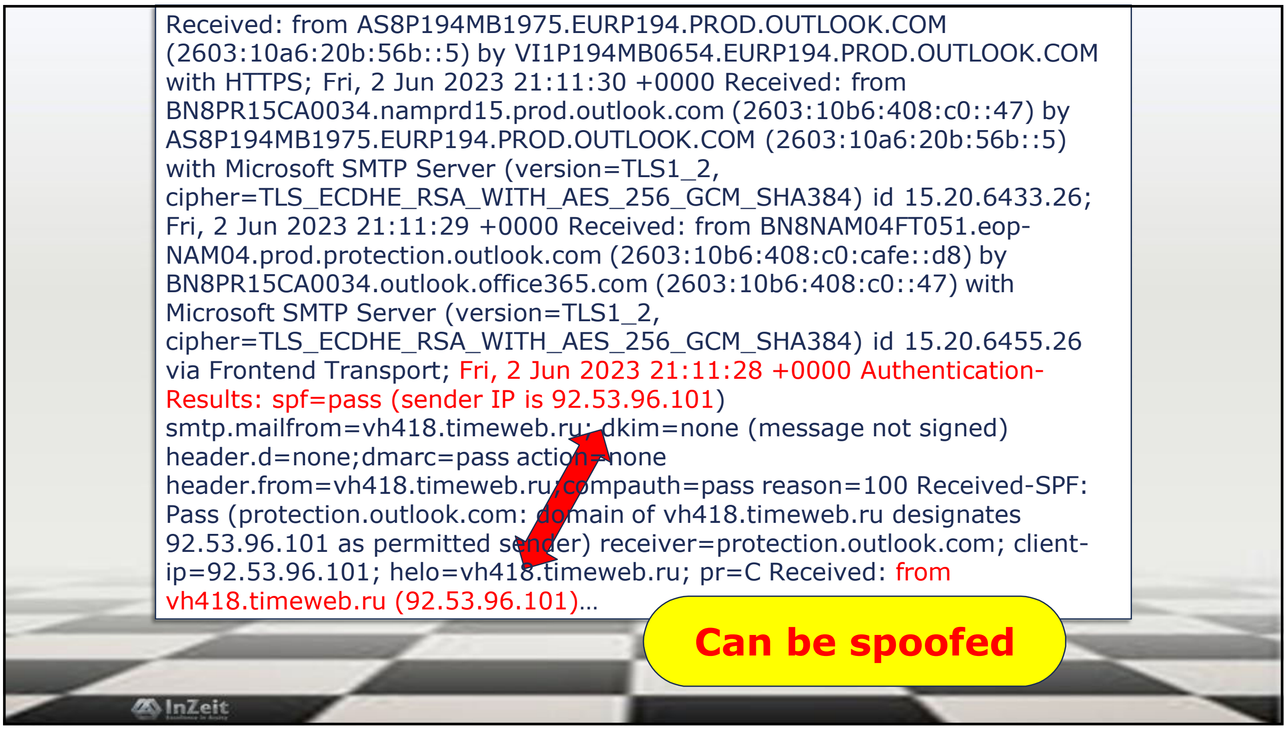


Received: from AS8P194MB1975.EURP194.PROD.OUTLOOK.COM (2603:10a6:20b:56b::5) by VI1P194MB0654.EURP194.PROD.OUTLOOK.COM with HTTPS; Fri, 2 Jun 2023 21:11:30 +0000 Received: from BN8PR15CA0034.namprd15.prod.outlook.com (2603:10b6:408:c0::47) by AS8P194MB1975.EURP194.PROD.OUTLOOK.COM (2603:10a6:20b:56b::5) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_25
Fri, 2 Jun 2023 21:11:29 +0000 Receive
NAM04.prod.protection.outlook.com (26
BN8PR15CA0034.outlook.office365.com (
Microsoft SMTP Server (version=TLS1_2
cipher=TLS_ECDHE_RSA_WITH_AES_25
via Frontend Transport; Fri, 2 Jun 2023
Results: spf=pass (sender IP is 92.53.96
smtp.mailfrom=vh418.timeweb.ru; dkim
header.d=none;dmarc=pass action=non
header.from=vh418.timeweb.ru;compau
Pass (protection.outlook.com: domain of
92.53.96.101 as permitted sender) recei
ip=92.53.96.101; helo=vh418.timeweb.ru; pr=C Received: from vh418.timeweb.ru (92.53.96.101)...

Email Headers :

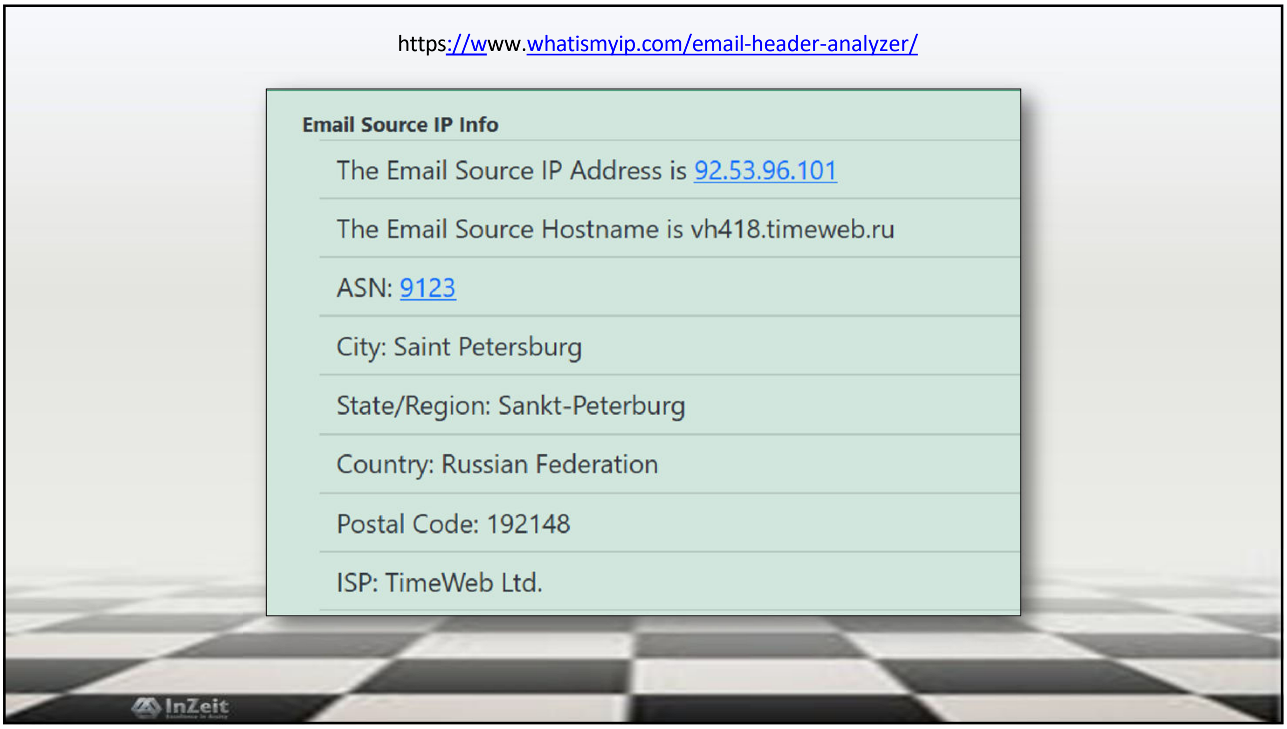
Gmail:
'Show original' in drop down menu top right of email message

Hotmail/Outlook mail:
'View message source' in drop down menu top right of email message



Received: from AS8P194MB1975.EURP194.PROD.OUTLOOK.COM (2603:10a6:20b:56b::5) by VI1P194MB0654.EURP194.PROD.OUTLOOK.COM with HTTPS; Fri, 2 Jun 2023 21:11:30 +0000 Received: from BN8PR15CA0034.namprd15.prod.outlook.com (2603:10b6:408:c0::47) by AS8P194MB1975.EURP194.PROD.OUTLOOK.COM (2603:10a6:20b:56b::5) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6433.26; Fri, 2 Jun 2023 21:11:29 +0000 Received: from BN8NAM04FT051.eop-NAM04.prod.protection.outlook.com (2603:10b6:408:c0:cafe::d8) by BN8PR15CA0034.outlook.office365.com (2603:10b6:408:c0::47) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6455.26 via Frontend Transport; Fri, 2 Jun 2023 21:11:28 +0000 Authentication-Results: spf=pass (sender IP is 92.53.96.101) smtp.mailfrom=vh418.timeweb.ru; dkim=none (message not signed) header.d=none;dmarc=pass action=none header.from=vh418.timeweb.ru;compauth=pass reason=100 Received-SPF: Pass (protection.outlook.com: domain of vh418.timeweb.ru designates 92.53.96.101 as permitted sender) receiver=protection.outlook.com; client-ip=92.53.96.101; helo=vh418.timeweb.ru; pr=C Received: from vh418.timeweb.ru (92.53.96.101)...

Can be spoofed



https://www.whatismyip.com/email-header-analyzer/

Email Source IP Info

The Email Source IP Address is 92.53.96.101

The Email Source Hostname is vh418.timeweb.ru

ASN: 9123

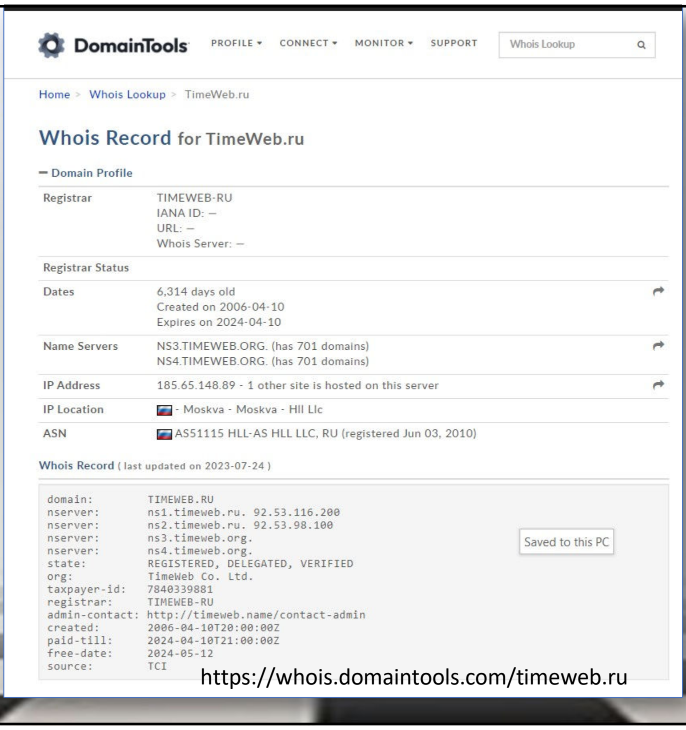
City: Saint Petersburg

State/Region: Sankt-Peterburg

Country: Russian Federation

Postal Code: 192148

ISP: TimeWeb Ltd.



Whois Record for TimeWeb.ru

— Domain Profile

Registrar	TIMEWEB-RU IANA ID: – URL: – Whois Server: –
Registrar Status	
Dates	6,314 days old Created on 2006-04-10 Expires on 2024-04-10
Name Servers	NS3.TIMEWEB.ORG. (has 701 domains) NS4.TIMEWEB.ORG. (has 701 domains)
IP Address	185.65.148.89 - 1 other site is hosted on this server
IP Location	- Moskva - Moskva - Hll Llc
ASN	AS51115 HLL-AS HLL LLC, RU (registered Jun 03, 2010)

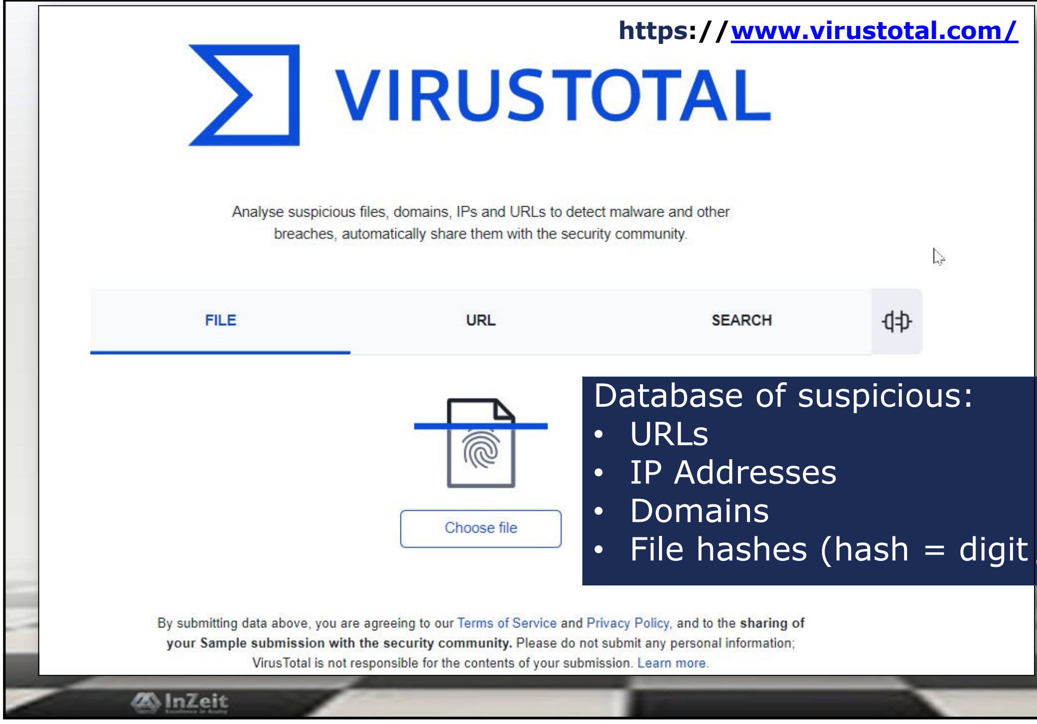
Whois Record (last updated on 2023-07-24)

```
domain:        TIMEWEB.RU
nserver:       ns1.timeweb.ru. 92.53.116.200
nserver:       ns2.timeweb.ru. 92.53.98.100
nserver:       ns3.timeweb.org.
nserver:       ns4.timeweb.org.
state:         REGISTERED, DELEGATED, VERIFIED
org:           TimeWeb Co. Ltd.
taxpayer-id:   7840339881
registrar:     TIMEWEB-RU
admin-contact: http://timeweb.name/contact-admin
created:       2006-04-10T20:00:00Z
paid-till:     2024-04-10T21:00:00Z
free-date:     2024-05-12
source:        TCI
```

https://whois.domaintools.com/timeweb.ru

23

https://www.virustotal.com/

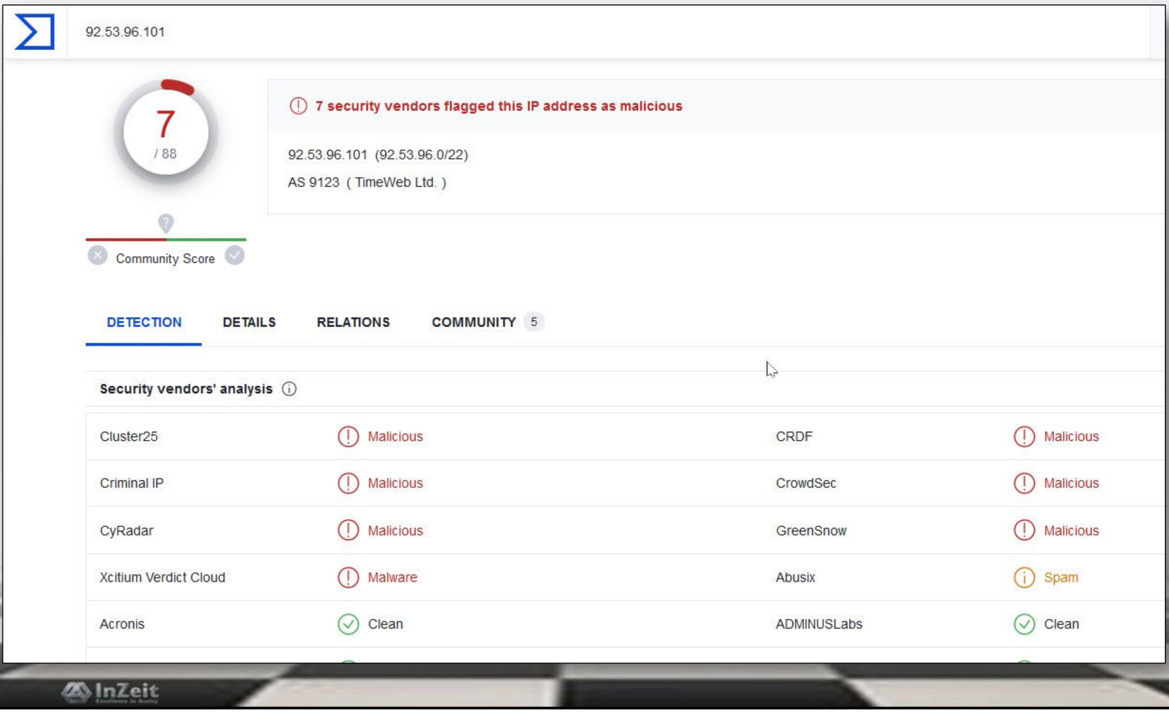


Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

Database of suspicious:
- URLs
- IP Addresses
- Domains
- File hashes (hash = digital fingerprint)

24



92.53.96.101

7
/ 88

7 security vendors flagged this IP address as malicious

92.53.96.101 (92.53.96.0/22)
AS 9123 (TimeWeb Ltd.)

Security vendors' analysis

Cluster25	Malicious	CRDF	Malicious
Criminal IP	Malicious	CrowdSec	Malicious
CyRadar	Malicious	GreenSnow	Malicious
Xcitium Verdict Cloud	Malware	Abusix	Spam
Acronis	Clean	ADMINUSLabs	Clean

25

Example: tracking a Russian Money Launderer

MT.GOX

2014 Tokyo Bitcoin Exchange went bankrupt

Hacked:

750,000 BTC users
100,000 BTC own
(7% of all BTC in existence)

“Loss: $530million”

26

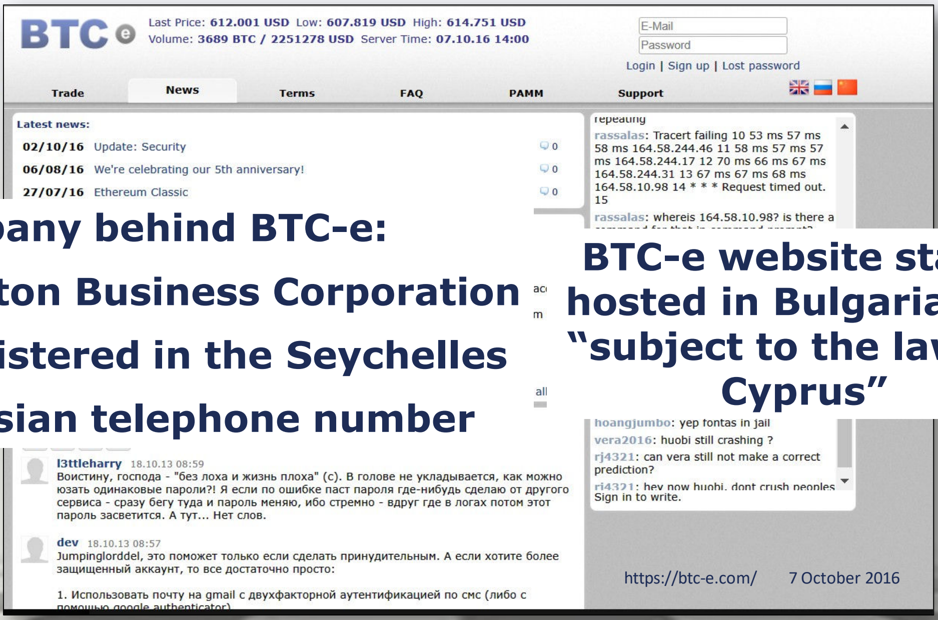
Stolen BTC tracked by Chainalysis

Eventually ended up at BTC-e Exchange

BTC-e

BTC-e ownership and location unknown

InZeit



BTC e

Last Price: **612.001 USD** Low: **607.819 USD** High: **614.751 USD**
Volume: **3689 BTC / 2251278 USD** Server Time: **07.10.16 14:00**

Latest news:

02/10/16	Update: Security	0
06/08/16	We're celebrating our 5th anniversary!	0
27/07/16	Ethereum Classic	0

repeating

rassalas: Tracert failing 10 53 ms 57 ms 58 ms 164.58.244.46 11 58 ms 57 ms 57 ms 164.58.244.17 12 70 ms 66 ms 67 ms 164.58.244.31 13 67 ms 67 ms 68 ms 164.58.10.98 14 * * * Request timed out. 15

rassalas: whereis 164.58.10.98? is there a command for that in command prompt?

hoangjumbo: yep fontas in jail

vera2016: huobi still crashing ?

rj4321: can vera still not make a correct prediction?

rj4321: hey now huobi, dont crush peoples

Sign in to write.

l3ttleharry 18.10.13 08:59
Воистину, господа - "без лоха и жизнь плоха" (с). В голове не укладывается, как можно юзать одинаковые пароли?! Я если по ошибке паст пароля где-нибудь сделаю от другого сервиса - сразу бегу туда и пароль меняю, ибо стремно - вдруг где в логах потом этот пароль засветится. А тут... Нет слов.

dev 18.10.13 08:57
Jumpinglorddel, это поможет только если сделать принудительным. А если хотите более защищенный аккаунт, то все достаточно просто:

1. Использовать почту на gmail с двухфакторной аутентификацией по смс (либо с помощью google authenticator)

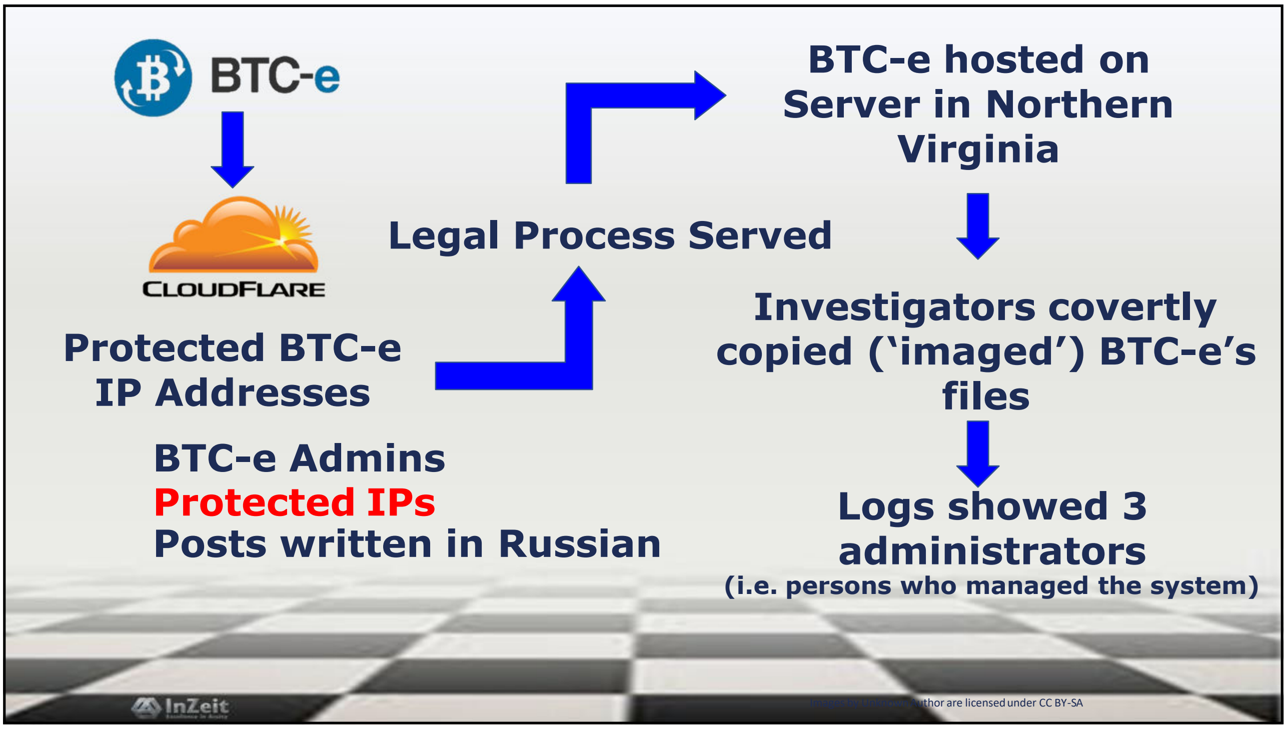
Company behind BTC-e:

- **Canton Business Corporation**
- **Registered in the Seychelles**
- **Russian telephone number**

BTC-e website stated hosted in Bulgaria, but "subject to the laws of Cyprus"

https://btc-e.com/ 7 October 2016

InZeit



Protected BTC-e IP Addresses

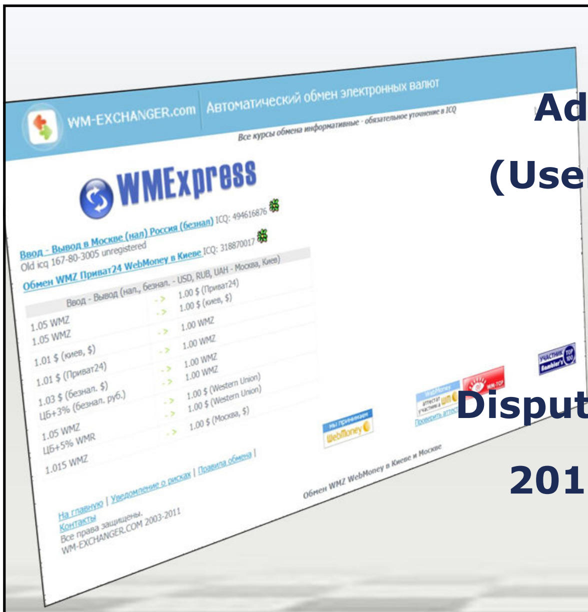
Legal Process Served

BTC-e hosted on Server in Northern Virginia

Investigators covertly copied (‘imaged’) BTC-e’s files

Logs showed 3 administrators
(i.e. persons who managed the system)

BTC-e Admins
Protected IPs
Posts written in Russian



WM-EXCHANGER.com | Автоматический обмен электронных валют

Все курсы обмена информативные - обязательное уточнение в ICQ

Ввод - Вывод в Москве (нал) Россия (безнал) ICQ: 494616876
Old icq 167-80-3005 unregistered
Обмен WMZ Приват24 WebMoney в Киеве ICQ: 318870017

Ввод - Вывод (нал., безнал. - USD, RUB, UAH - Москва, Киев)		
1.05 WMZ	->	1.00 $ (Приват24)
1.05 WMZ	->	1.00 $ (киев, $)
1.01 $ (киев, $)	->	1.00 WMZ
1.01 $ (Приват24)	->	1.00 WMZ
1.03 $ (безнал. $)	->	1.00 WMZ
ЦБ+3% (безнал. руб.)	->	1.00 WMZ
1.05 WMZ	->	1.00 $ (Western Union)
ЦБ+5% WMR	->	1.00 $ (Western Union)
1.015 WMZ	->	1.00 $ (Москва, $)

На главную | Уведомление о рисках | Правила обмена |
Контакты
Все права защищены.
WM-EXCHANGER.COM 2003-2011

Обмен WMZ WebMoney в Киеве и Москве

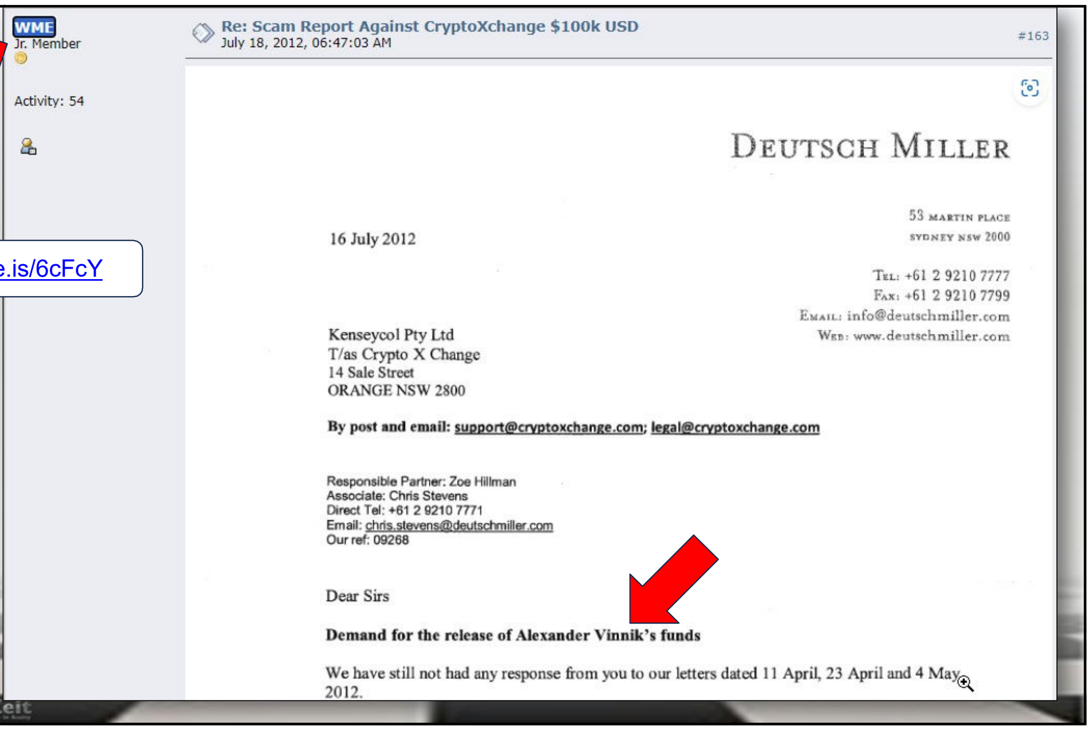
Bitcointalk Forum
Admin used Username: “WME”

(Username linked to known carder)

Email account on
wm-exchanger.com
Web Money Exchanger

Dispute with CryptXchange (Australia)

2012 Posted Lawyer’s letter headed
“Demand for the release of
Alexander Vinnik’s funds”



WME
Jr. Member

Activity: 54

Re: Scam Report Against CryptoXchange $100k USD
July 18, 2012, 06:47:03 AM

#163

DEUTSCH MILLER

16 July 2012

53 MARTIN PLACE
SYDNEY NSW 2000

TEL: +61 2 9210 7777
FAX: +61 2 9210 7799
EMAIL: info@deutschmiller.com
WEB: www.deutschmiller.com

Kenseycol Pty Ltd
T/as Crypto X Change
14 Sale Street
ORANGE NSW 2800

By post and email: support@cryptoxchange.com; legal@cryptoxchange.com

Responsible Partner: Zoe Hillman
Associate: Chris Stevens
Direct Tel: +61 2 9210 7771
Email: chris.stevens@deutschmiller.com
Our ref: 09268

Dear Sirs

Demand for the release of Alexander Vinnik's funds

We have still not had any response from you to our letters dated 11 April, 23 April and 4 May 2012.

http://archive.is/6cFcY

User WME = Alexander Vinnik

Monitored Vinnik's accounts

Mid-2016 he logged into one of accounts using unmasked IP

IP of luxury hotel outside Russia

Hotel Chain HQ in USA

Subpoena for Passport

July 2017 Arrested in Thessaloniki

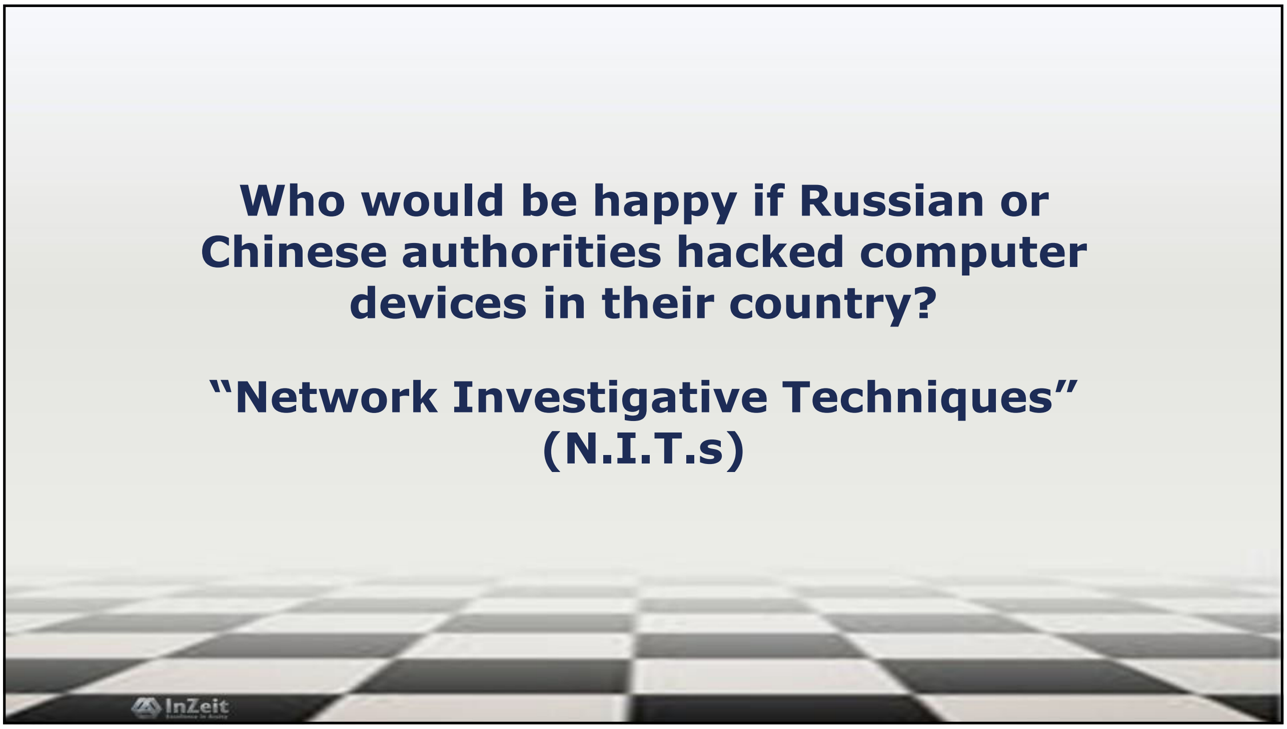
France, Russia, USA sought Extradition

2020 extradited to France

Sentenced to 5 years, deported to Greece 2022

5 August 2022 extradited to USA

Further Reading: "Tracers in the Dark" (2022) Andy Greenberg



Who would be happy if Russian or Chinese authorities hacked computer devices in their country?

“Network Investigative Techniques” (N.I.T.s)

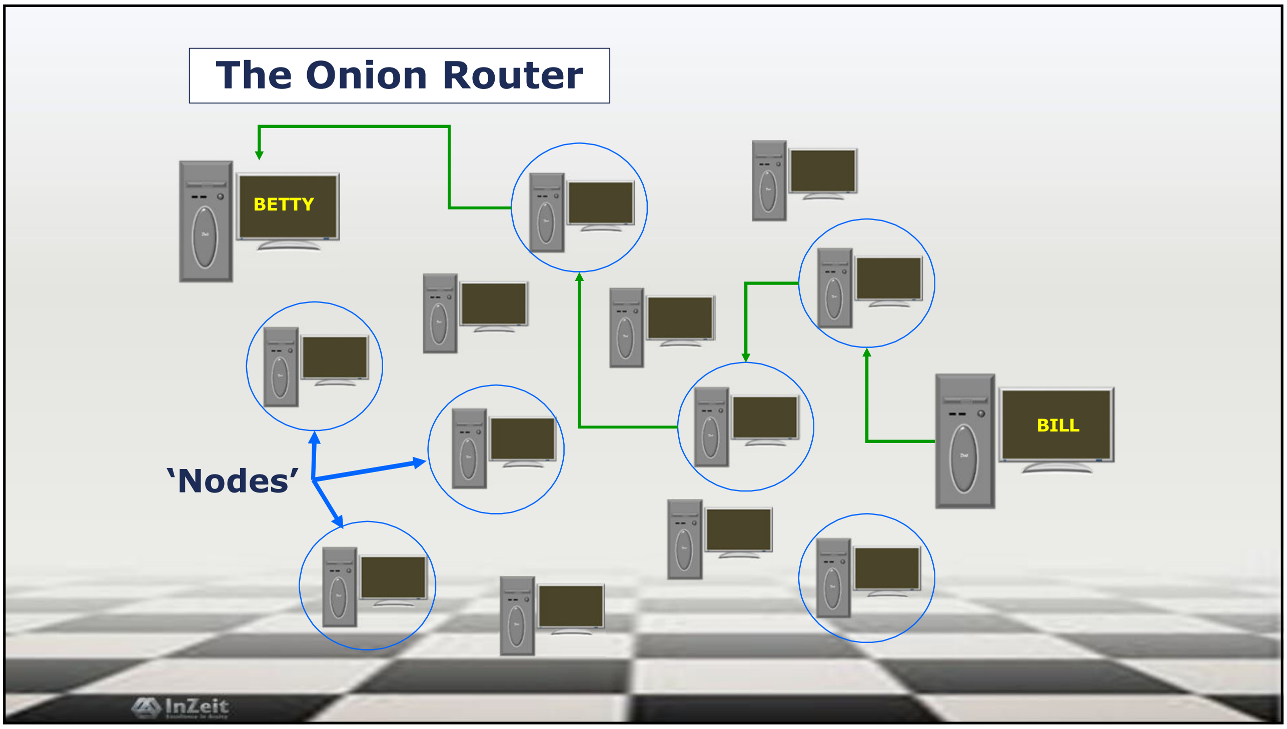
33

FBI Operation Onymous (2014):

- Darkweb market place (accessed through TOR)
- 6 month operation
- 17 countries
- 17 arrests
- 23-400+ websites dismantled
- $180K in cash
- $1Billion BTC & property

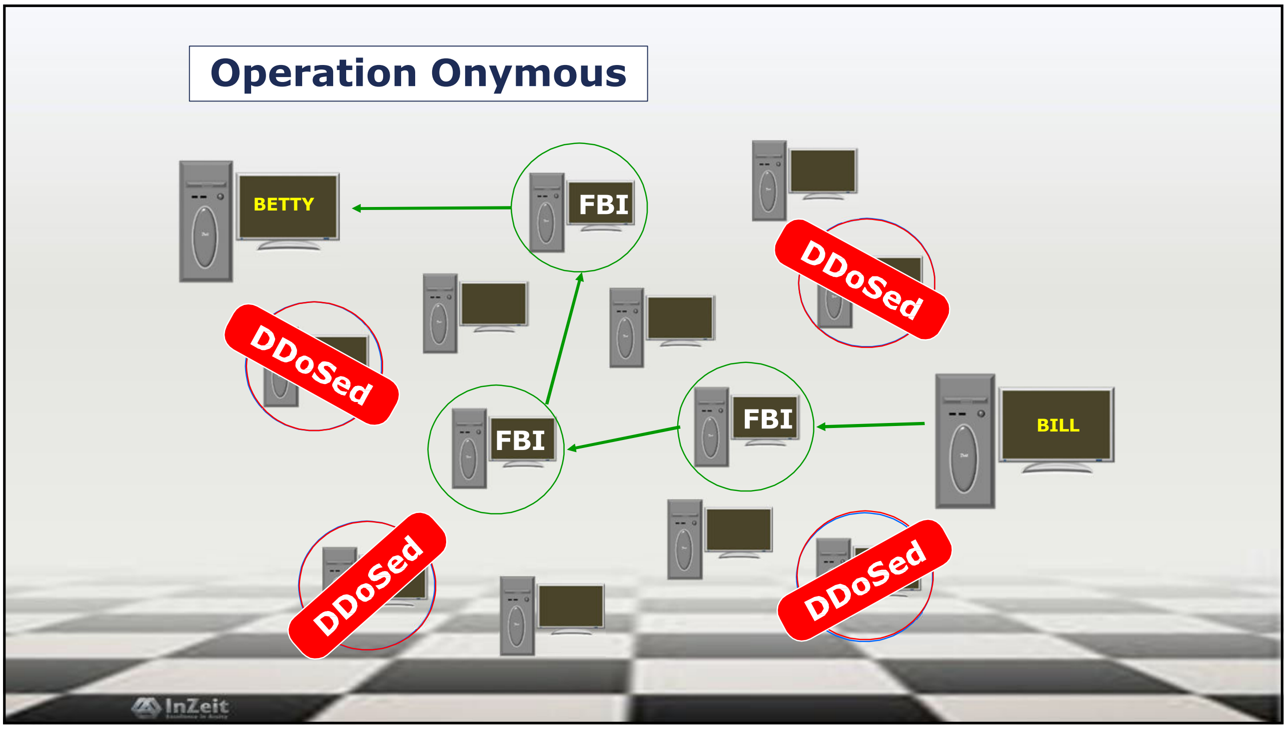
34

The Onion Router



35

Operation Onymous



36

Playpen (Operation Pacifier) 2014

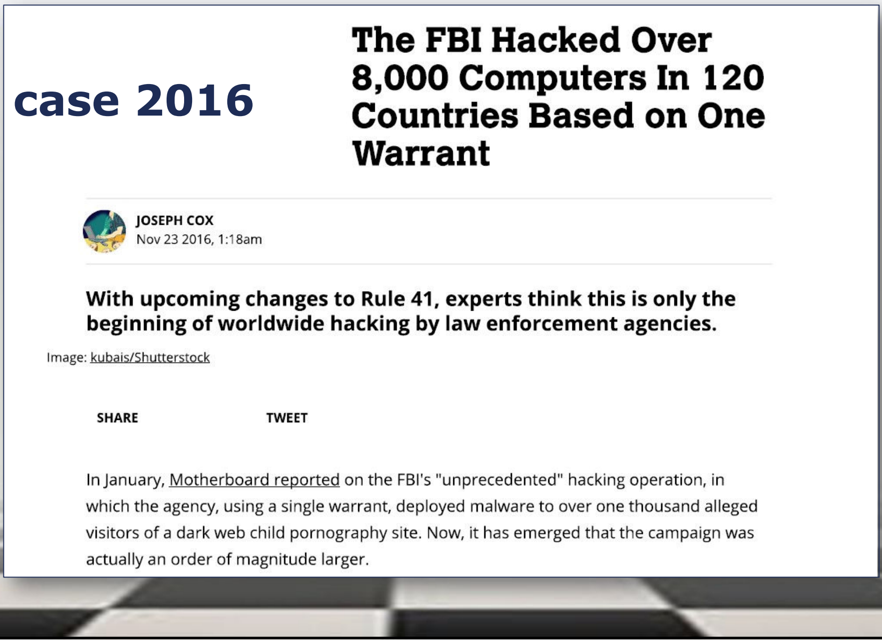
- Playpen paedophile site for 13 days hosted on a government server.
- Sent Tor exploit to visitors to certain threads on the site.
- Malware returned the real IP address.

https://motherboard.vice.com/en_us/article/53d4n8/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant

37

https://motherboard.vice.com/en_us/article/53d4n8/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant

Playpen case 2016



The FBI Hacked Over 8,000 Computers In 120 Countries Based on One Warrant

JOSEPH COX
Nov 23 2016, 1:18am

With upcoming changes to Rule 41, experts think this is only the beginning of worldwide hacking by law enforcement agencies.

Image: kubais/Shutterstock

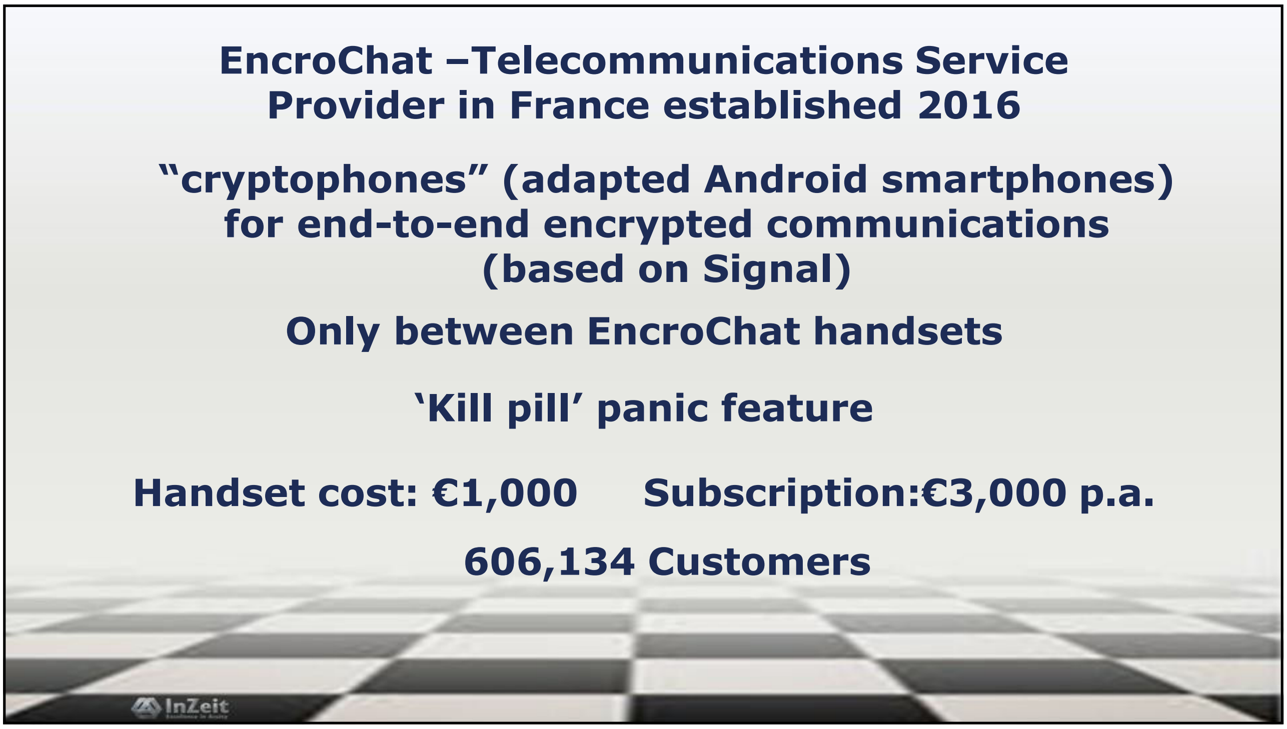
In January, Motherboard reported on the FBI's "unprecedented" hacking operation, in which the agency, using a single warrant, deployed malware to over one thousand alleged visitors of a dark web child pornography site. Now, it has emerged that the campaign was actually an order of magnitude larger.

38

EncroChat

Photo © Gendarmerie Nationale (FR)

39



EncroChat –Telecommunications Service Provider in France established 2016

“cryptophones” (adapted Android smartphones) for end-to-end encrypted communications (based on Signal)

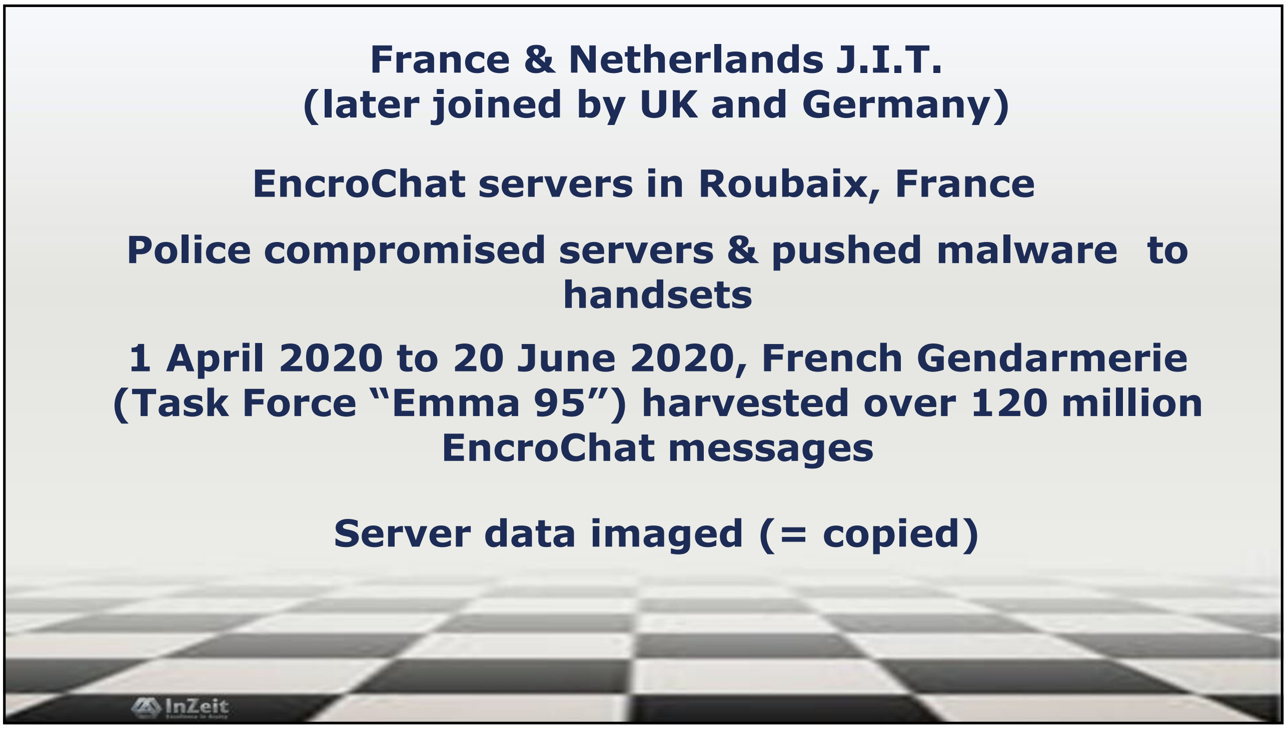
Only between EncroChat handsets

‘Kill pill’ panic feature

Handset cost: €1,000   Subscription:€3,000 p.a.

606,134 Customers

40



France & Netherlands J.I.T.
(later joined by UK and Germany)

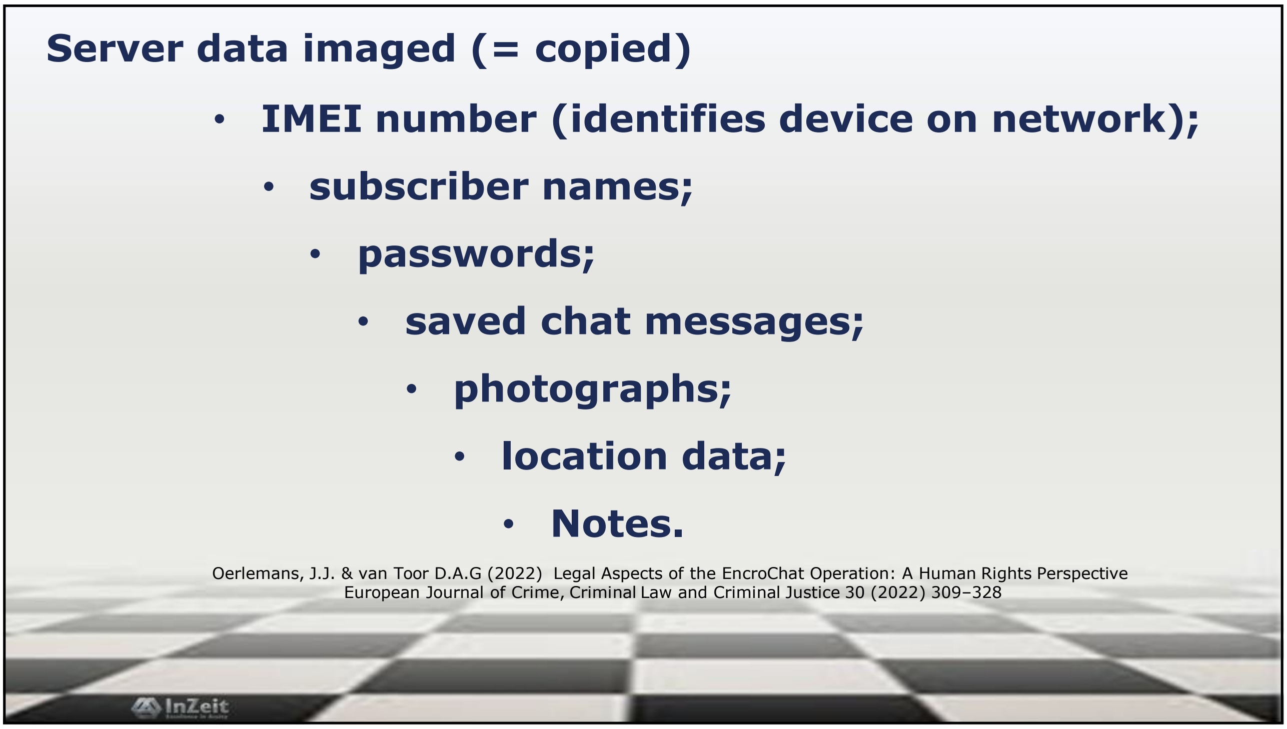
EncroChat servers in Roubaix, France

Police compromised servers & pushed malware to handsets

1 April 2020 to 20 June 2020, French Gendarmerie (Task Force "Emma 95") harvested over 120 million EncroChat messages

Server data imaged (= copied)

41

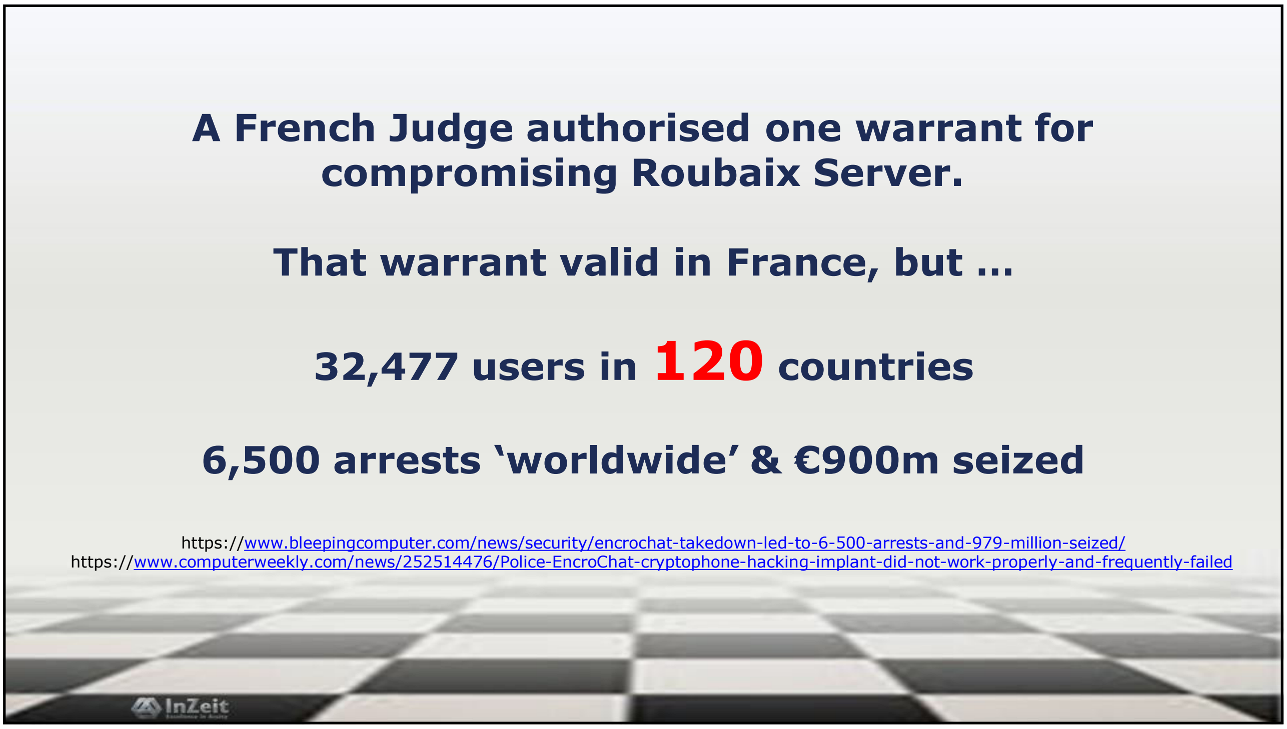


Server data imaged (= copied)

- IMEI number (identifies device on network);
- subscriber names;
- passwords;
- saved chat messages;
- photographs;
- location data;
- Notes.

Oerlemans, J.J. & van Toor D.A.G (2022) Legal Aspects of the EncroChat Operation: A Human Rights Perspective
European Journal of Crime, Criminal Law and Criminal Justice 30 (2022) 309–328

42



A French Judge authorised one warrant for compromising Roubaix Server.

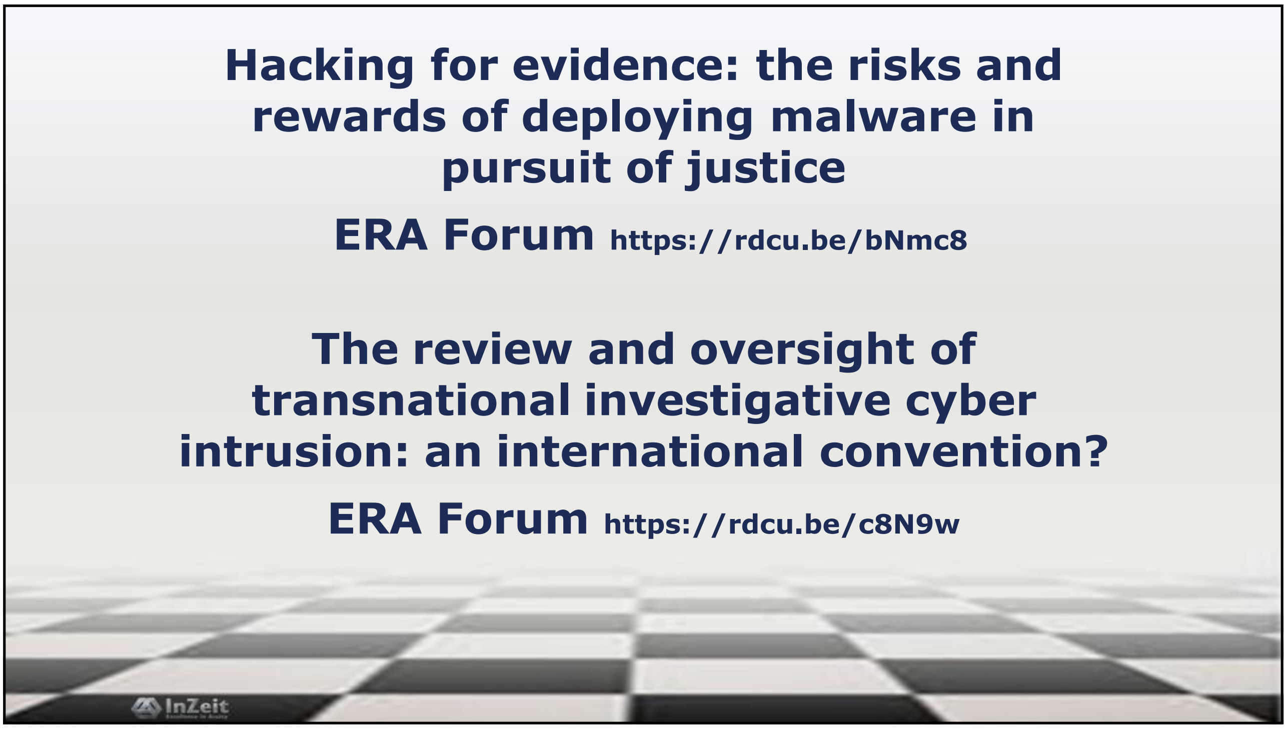
That warrant valid in France, but …

32,477 users in 120 countries

6,500 arrests 'worldwide' & €900m seized

https://www.bleepingcomputer.com/news/security/encrochat-takedown-led-to-6-500-arrests-and-979-million-seized/
https://www.computerweekly.com/news/252514476/Police-EncroChat-cryptophone-hacking-implant-did-not-work-properly-and-frequently-failed

43



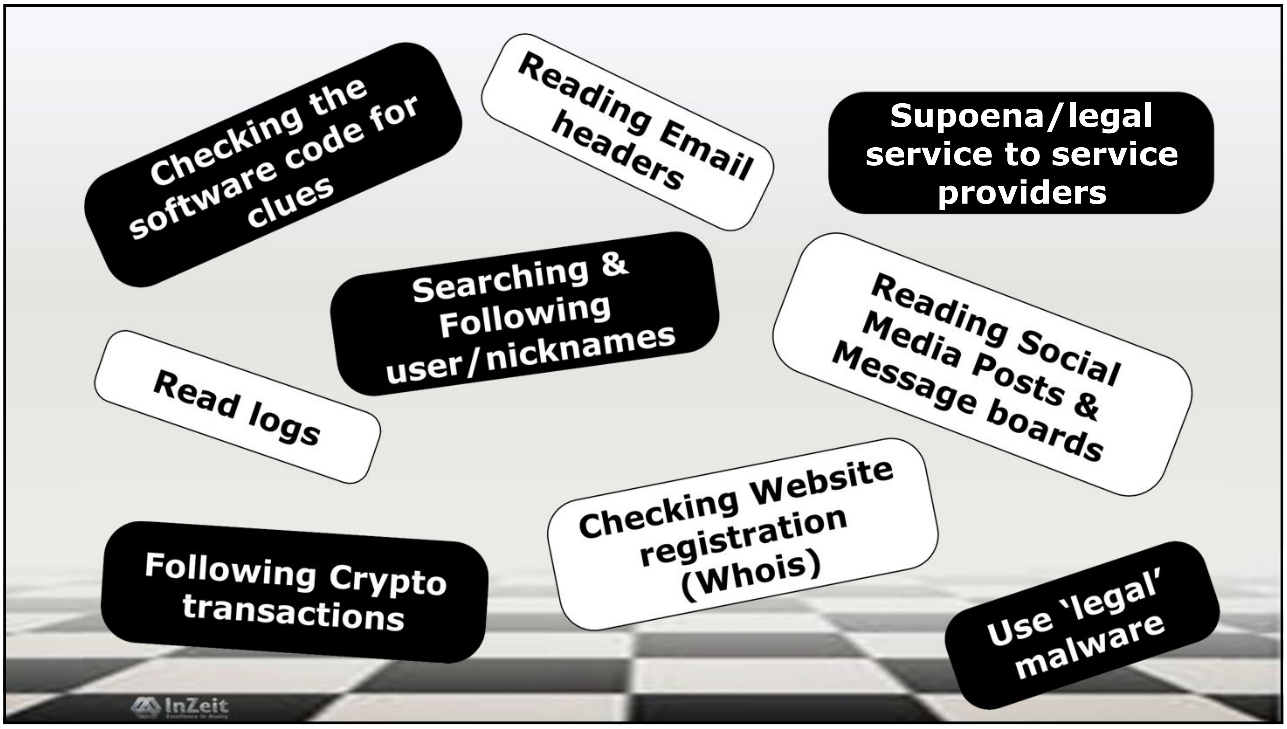
Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice

ERA Forum https://rdcu.be/bNmc8

The review and oversight of transnational investigative cyber intrusion: an international convention?

ERA Forum https://rdcu.be/c8N9w

44



Checking the software code for clues

Reading Email headers

Supoena/legal service to service providers

Searching & Following user/nicknames

Reading Social Media Posts & Message boards

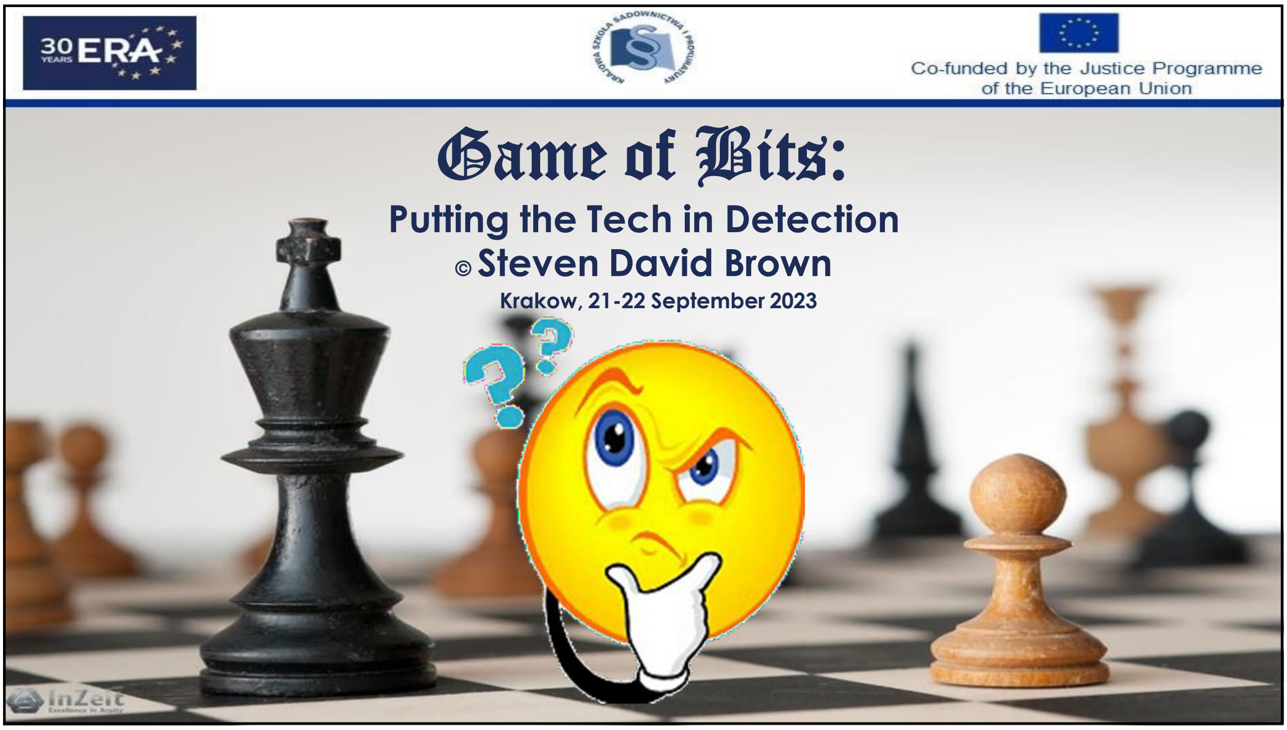
Read logs

Checking Website registration (Whois)

Following Crypto transactions

Use 'legal' malware

45



Co-funded by the Justice Programme of the European Union

Game of Bits:

Putting the Tech in Detection

© Steven David Brown

Krakow, 21-22 September 2023

46

References and Further Reading

Anonymisers

TOR Browser https://www.torproject.org/download/

Whonix https://www.whonix.org/

I2P Invisible Internet Project https://geti2p.net/en/

Phishing Statistics

Kaspersky

https://www.kaspersky.com/about/press-releases/2023_the-number-of-phishing-attacks-doubled-to-reach-over-500-million-in-2022

Trend Micro

https://www.trendmicro.com/en_us/ciso/23/e/worldwide-email-phishing-stats-examples-2023.html

Technopedia

https://www.techopedia.com/phishing-statistics#Phishing_Statistics_Highlights

Checking Bitcoin Transactions and Wallets

Bitcoin Whos Who https://www.bitcoinwhoswho.com

Chainabuse https://www.chainabuse.com/

Email Header Analysers (don’t upload sensitive data!)

https://www.whatismyip.com/email-header-analyzer/

https://mxtoolbox.com/EmailHeaders.aspx

https://mailheader.org/

https://wintelguy.com/mtrace.pl

Checking URLs, IP addresses and Files

Whois https://whois.domaintools.com/timeweb.ru

VirusTotal https://www.virustotal.com/

MtGox Investigation example

BTC-Exchange

https://btc-e.com

Web Money Exchanger

https://wm-exchanger.com

Example taken from here:

Greenberg, A. (2022) “Tracers in the Dark” pub. Random House

49

Logs

Definition

https://www.techtarget.com/whatis/definition/log-log-file

Network Investigative Techniques

Brown, S.D. (2020) *Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice*. ERA Forum **20**, 423–438 (2020). https://doi.org/10.1007/s12027-019-00571-z Available at https://rdcu.be/bNmc8

Brown, S.D. (2023) *The review and oversight of transnational investigative cyber intrusion: an international convention? ERA Forum* Available at https://rdcu.be/c8N9w

Cox, J. (2016) *The FBI Hacked Over 8,000 Computers in 120 CXountries Based on One Warrant* https://motherboard.vice.com/en_us/article/53d4n8/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant

Gallagher, S. (2014) *Silk Road, other Tor "darknet" sites may have been "decloaked" through DDoS [Updated]* https://arstechnica.com/information-technology/2014/11/silk-road-other-tor-darknet-sites-may-have-been-decloaked-through-ddos/

50

EncroChat

Oerlemans, J.J. & van Toor D.A.G (2022) *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*
European Journal of Crime, Criminal Law and Criminal Justice 30 (2022) 309–328

Toulas, B. (2023) *EncroChat takedown led to 6,500 arrests and $979 million seized* https://www.bleepingcomputer.com/news/security/encrochat-takedown-led-to-6-500-arrests-and-979-million-seized/

Goodwin, B. (2022) *Police EncroChat cryptophone hacking implant did not work properly and frequently failed* https://www.computerweekly.com/news/252514476/Police-EncroChat-cryptophone-hacking-implant-did-not-work-properly-and-frequently-failed

51

Open Sourcery: Online magic for investigators

Co-funded by the Justice Programme of the European Union 2014-2020

© Steven David Brown

22nd September 2023

Krakow, Poland

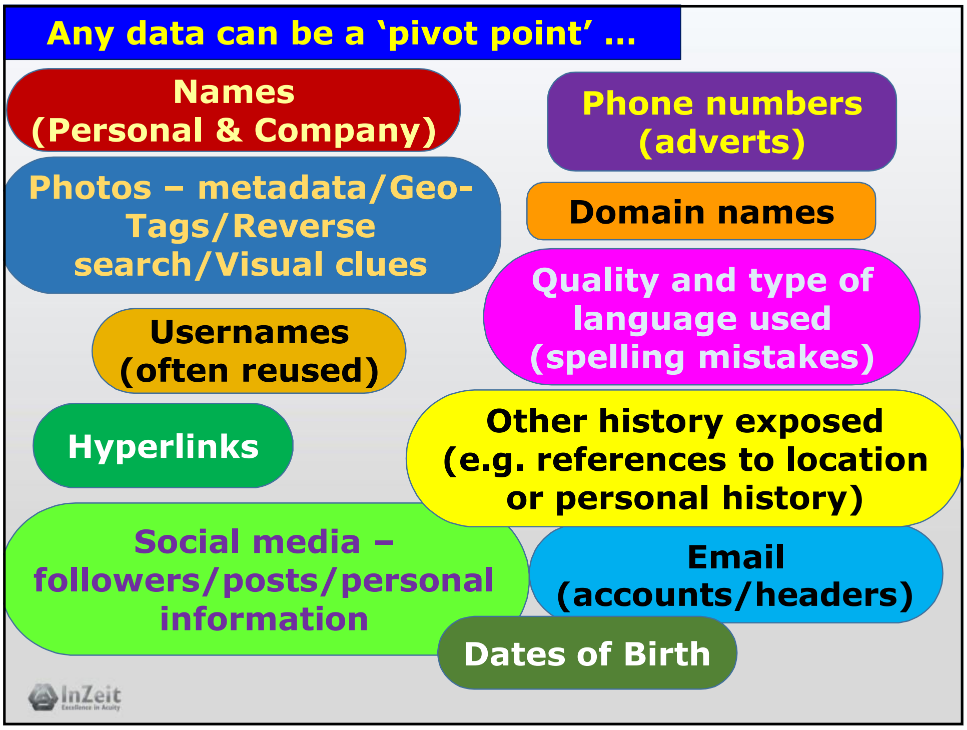
1

Opportunities

- Persistence & longevity
- General indiscriminate use of technology
- Chronicling of mundane experience
- Complacency and convenience
- Mass ‘surveillance capitalism’

N.B. These are just highlights of an editied OSINT presentation

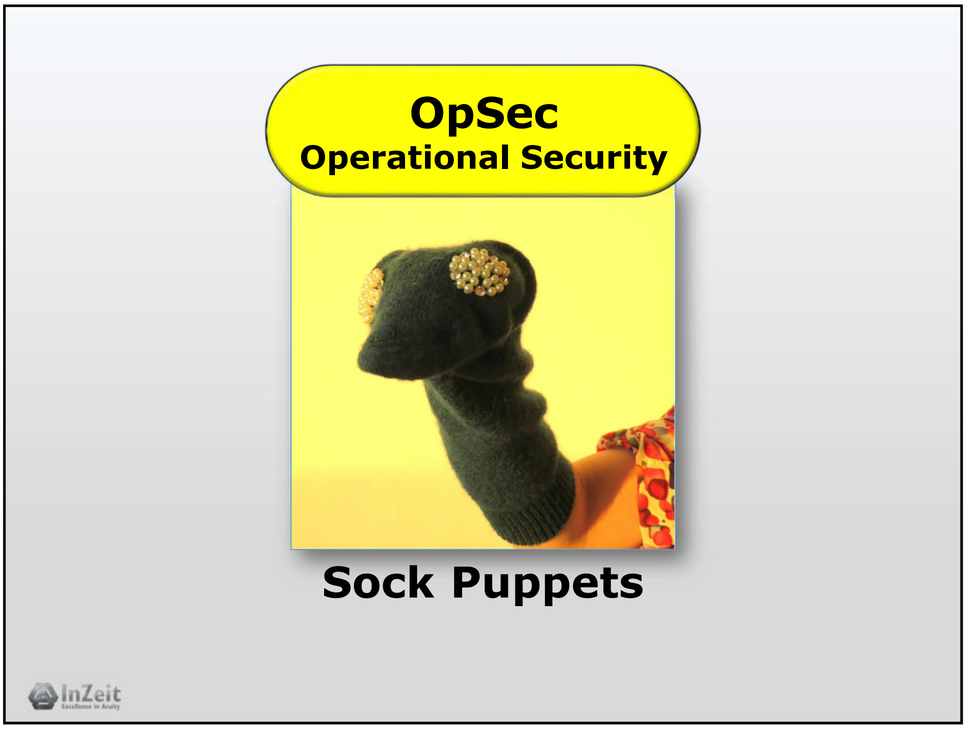
2



Any data can be a 'pivot point' …

- Names (Personal & Company)
- Phone numbers (adverts)
- Photos – metadata/Geo-Tags/Reverse search/Visual clues
- Domain names
- Quality and type of language used (spelling mistakes)
- Usernames (often reused)
- Hyperlinks
- Other history exposed (e.g. references to location or personal history)
- Social media – followers/posts/personal information
- Email (accounts/headers)
- Dates of Birth

3

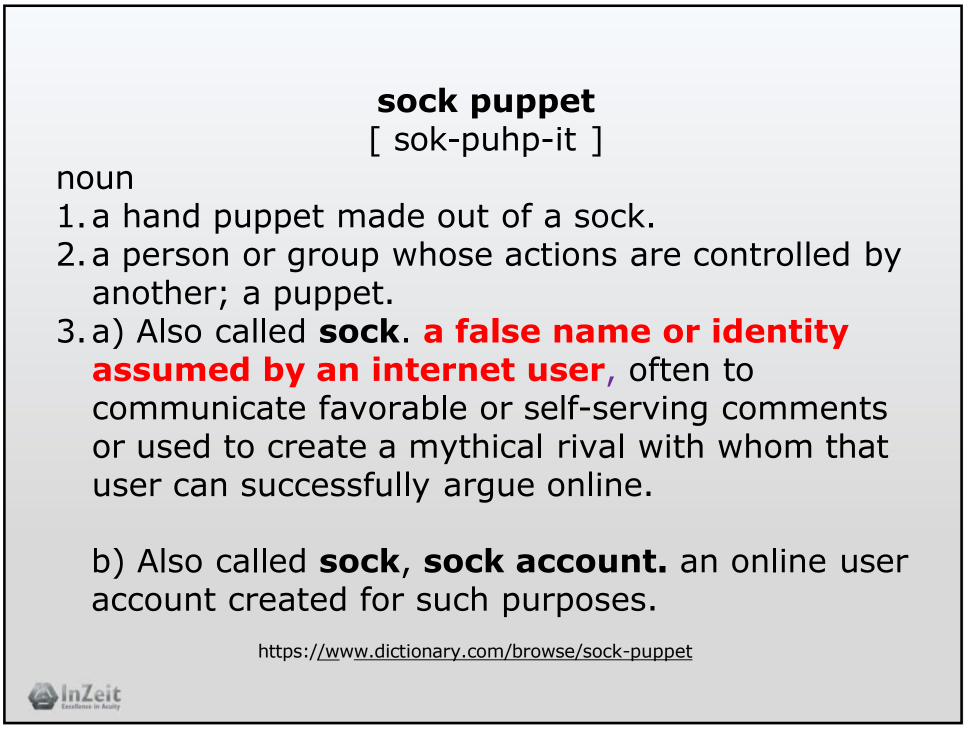


OpSec

Operational Security

Sock Puppets

4



sock puppet
[sok-puhp-it]

noun

1. a hand puppet made out of a sock.
2. a person or group whose actions are controlled by another; a puppet.
3. a) Also called **sock**. **a false name or identity assumed by an internet user**, often to communicate favorable or self-serving comments or used to create a mythical rival with whom that user can successfully argue online.

   b) Also called **sock**, **sock account.** an online user account created for such purposes.

https://www.dictionary.com/browse/sock-puppet

Who? Why?

Create Social Media accounts

Mask ID

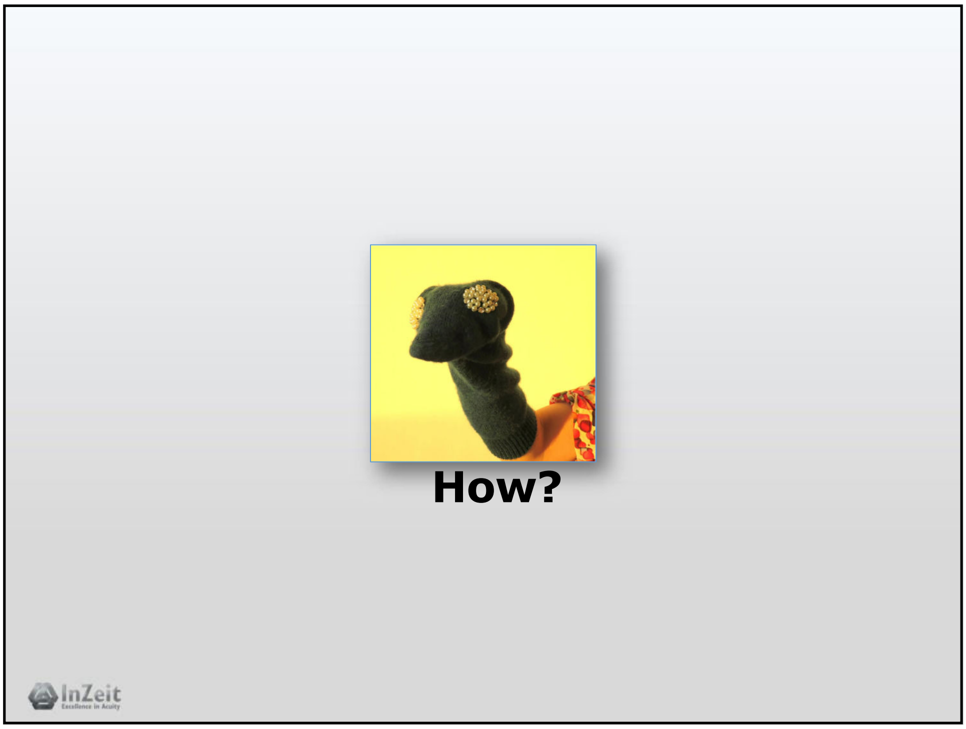
Criminal

Law Enforcement

Other Investigators (e.g. journalists)

Protect ID from revenge attack

Not to flag investigation underway

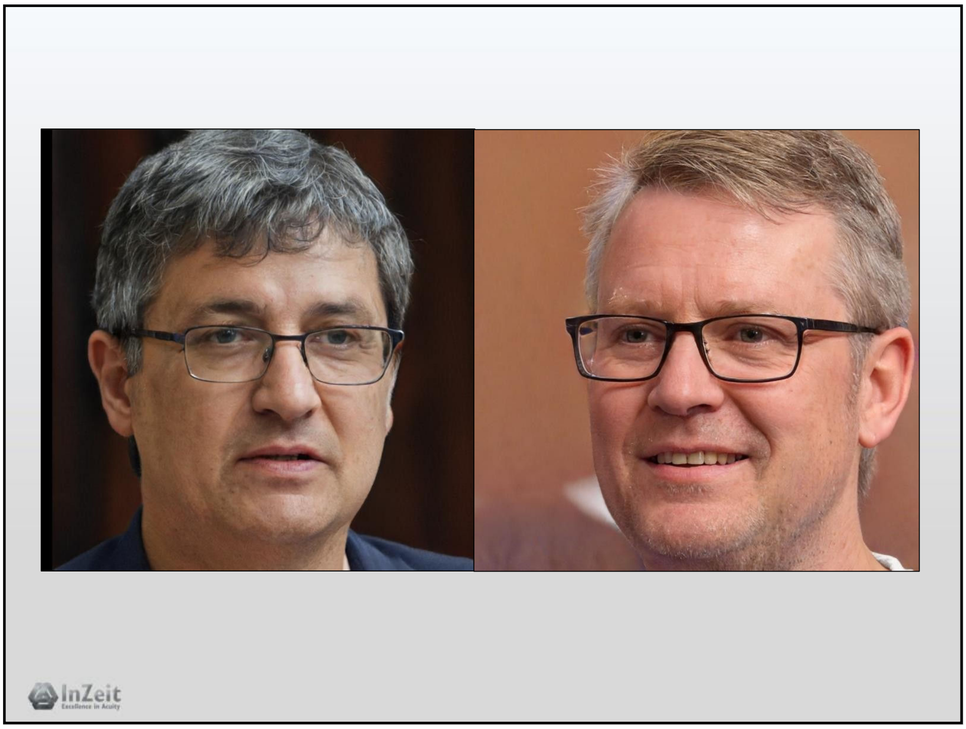


How?

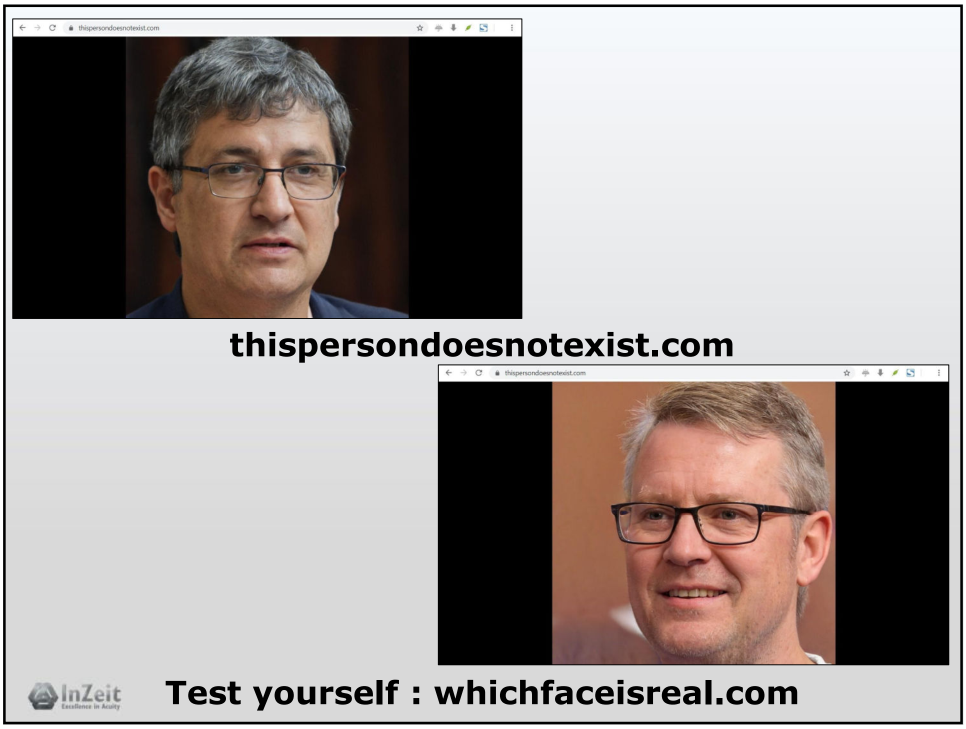
7

First, find a face …

8



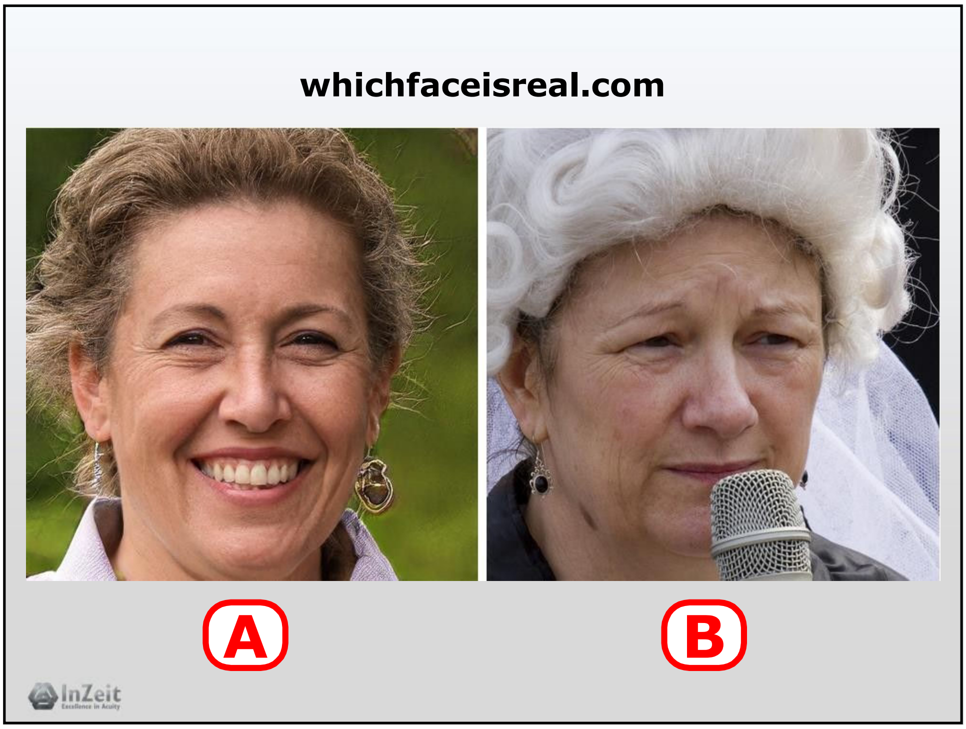
9



thispersondoesnotexist.com

Test yourself : whichfaceisreal.com

10



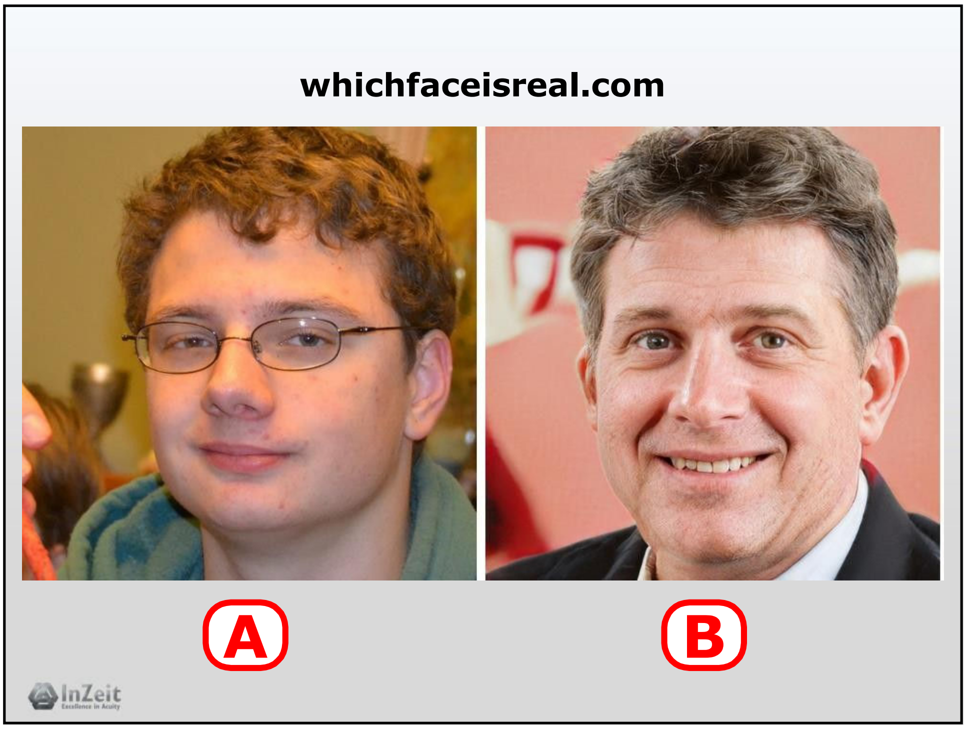
whichfaceisreal.com

A

B

InZeit

11



whichfaceisreal.com

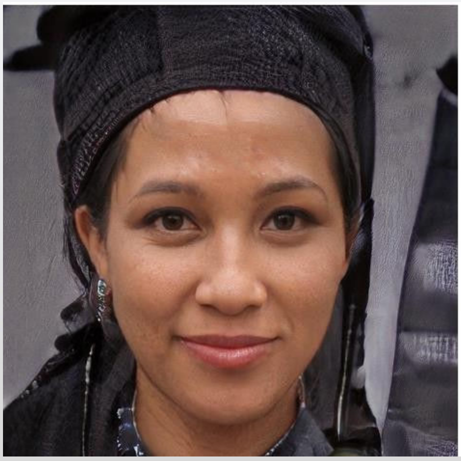
A

B

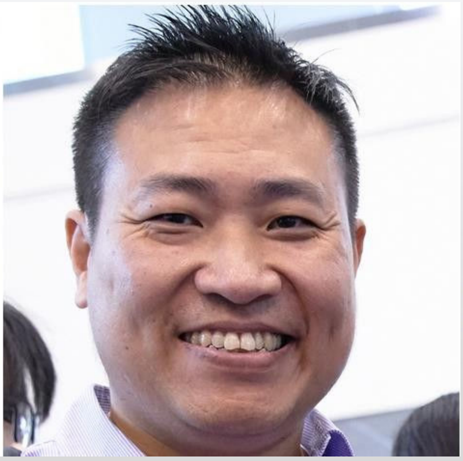
InZeit

12

whichfaceisreal.com



A



B

13

Creating Online Presence (online accounts):

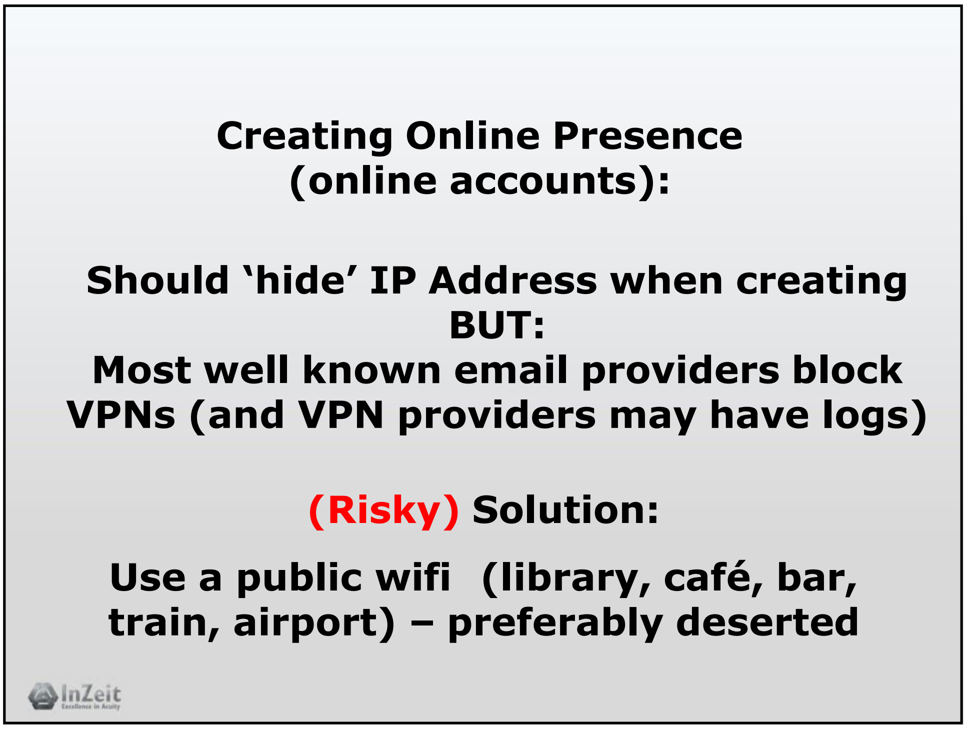
Email/Facebook/Twitter(X) /Instagram/TikTok help to validate a sock puppet

May require backup email for validation

May require mobile phone number

May require SMS validation

14

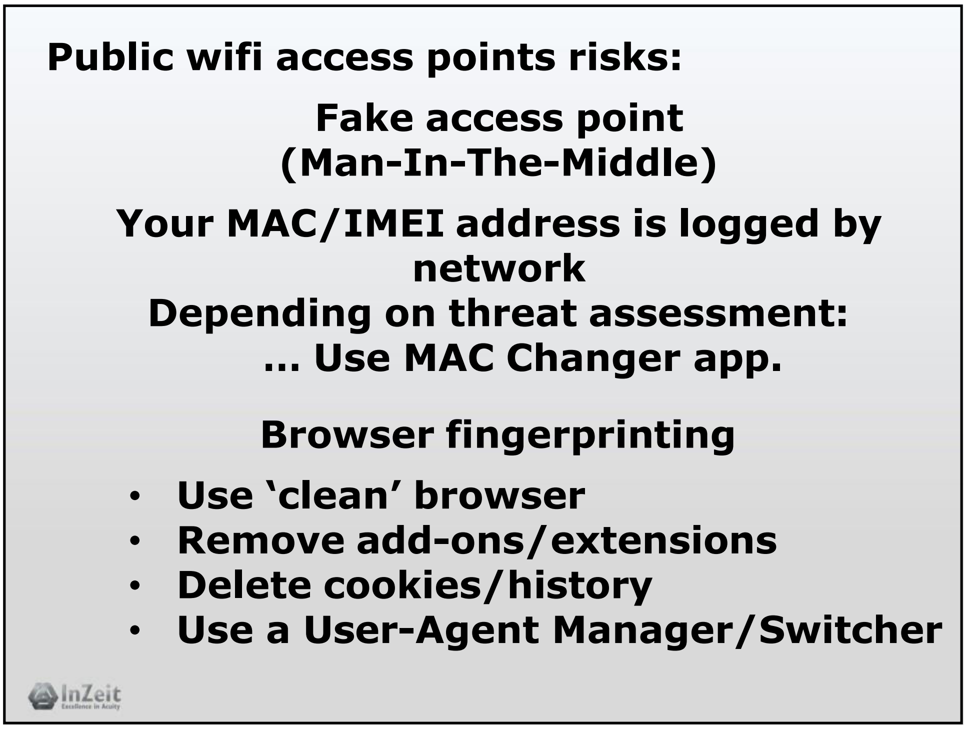


Creating Online Presence (online accounts):

Should ‘hide’ IP Address when creating
BUT:
Most well known email providers block VPNs (and VPN providers may have logs)

(Risky) Solution:

Use a public wifi (library, café, bar, train, airport) – preferably deserted



Public wifi access points risks:

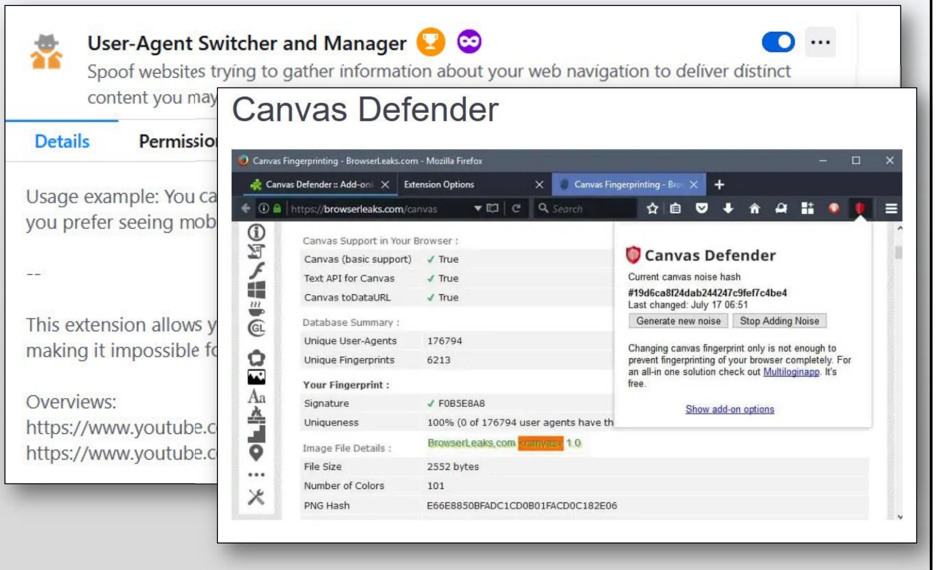
Fake access point
(Man-In-The-Middle)

Your MAC/IMEI address is logged by network
Depending on threat assessment:
… Use MAC Changer app.

Browser fingerprinting

- Use ‘clean’ browser
- Remove add-ons/extensions
- Delete cookies/history
- Use a User-Agent Manager/Switcher

User-Agent Manager/Switcher
(Browser add-on)



User-Agent Switcher and Manager

Spoof websites trying to gather information about your web navigation to deliver distinct content you may

Details | Permissio

Usage example: You ca
you prefer seeing mob

--

This extension allows y
making it impossible fo

Overviews:
https://www.youtube.c
https://www.youtube.c

Canvas Defender

Canvas Fingerprinting - BrowserLeaks.com - Mozilla Firefox

Canvas Defender :: Add-ons | Extension Options | Canvas Fingerprinting - Bro

https://browserleaks.com/canvas

Canvas Support in Your Browser :

Canvas (basic support)	✓ True
Text API for Canvas	✓ True
Canvas toDataURL	✓ True

Database Summary :

Unique User-Agents	176794
Unique Fingerprints	6213

Your Fingerprint :

Signature	✓ F0B5E8A8
Uniqueness	100% (0 of 176794 user agents have th

Image File Details : BrowserLeaks.com <canvas> 1.0

File Size	2552 bytes
Number of Colors	101
PNG Hash	E66E8850BFADC1CD0B01FACD0C182E06

Canvas Defender

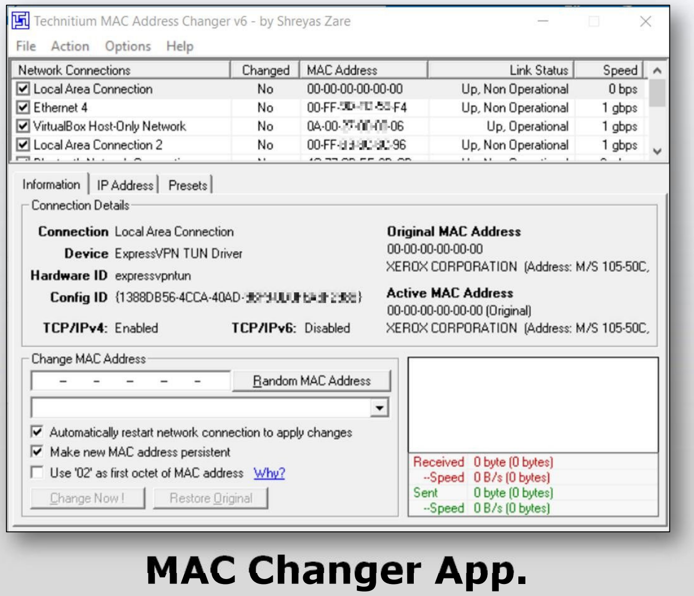
Current canvas noise hash
#19d6ca8f24dab244247c9fef7c4be4
Last changed: July 17 06:51

Generate new noise | Stop Adding Noise

Changing canvas fingerprint only is not enough to prevent fingerprinting of your browser completely. For an all-in one solution check out Multiloginapp. It's free.

Show add-on options

InZeit



Technitium MAC Address Changer v6 - by Shreyas Zare

File | Action | Options | Help

Network Connections	Changed	MAC Address	Link Status	Speed
☑ Local Area Connection	No	00-00-00-00-00-00	Up, Non Operational	0 bps
☑ Ethernet 4	No	00-FF-[redacted]-F4	Up, Non Operational	1 gbps
☑ VirtualBox Host-Only Network	No	0A-00-[redacted]-06	Up, Operational	1 gbps
☑ Local Area Connection 2	No	00-FF-[redacted]-96	Up, Non Operational	1 gbps

Information | IP Address | Presets

Connection Details

Connection Local Area Connection
Device ExpressVPN TUN Driver
Hardware ID expressvpntun
Config ID {1388DB56-4CCA-40AD-[redacted]}
TCP/IPv4: Enabled **TCP/IPv6:** Disabled

Original MAC Address
00-00-00-00-00-00
XEROX CORPORATION (Address: M/S 105-50C,

Active MAC Address
00-00-00-00-00-00 (Original)
XEROX CORPORATION (Address: M/S 105-50C,

Change MAC Address

- - - - - | Random MAC Address

☑ Automatically restart network connection to apply changes
☑ Make new MAC address persistent
□ Use '02' as first octet of MAC address Why?

Change Now ! | Restore Original

Received	0 byte (0 bytes)
--Speed	0 B/s (0 bytes)
Sent	0 byte (0 bytes)
--Speed	0 B/s (0 bytes)

MAC Changer App.

InZeit

Creating Online Presence (online accounts):

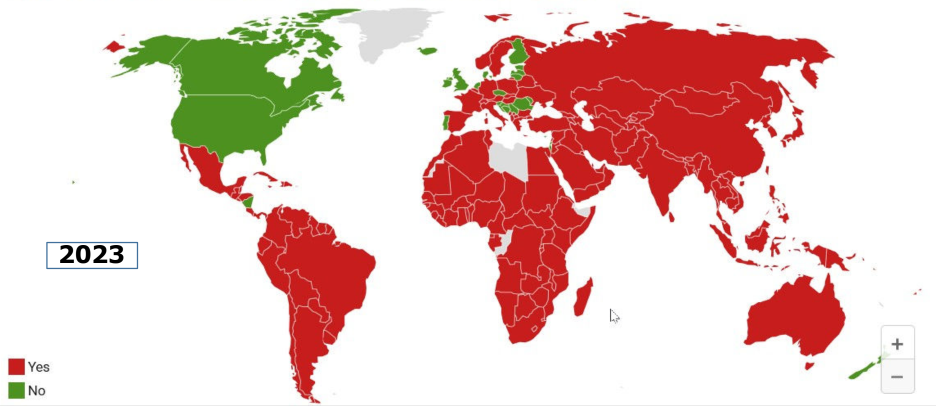
Many companies require mobile phone number for validation

Solution:

Get a burner phone (not as easy as it used to be)

19

Map of Countries with Mandatory SIM-Card Registration



https://www.comparitech.com/blog/vpn-privacy/sim-card-registration-laws/

20

Creating Online Presence (online accounts):

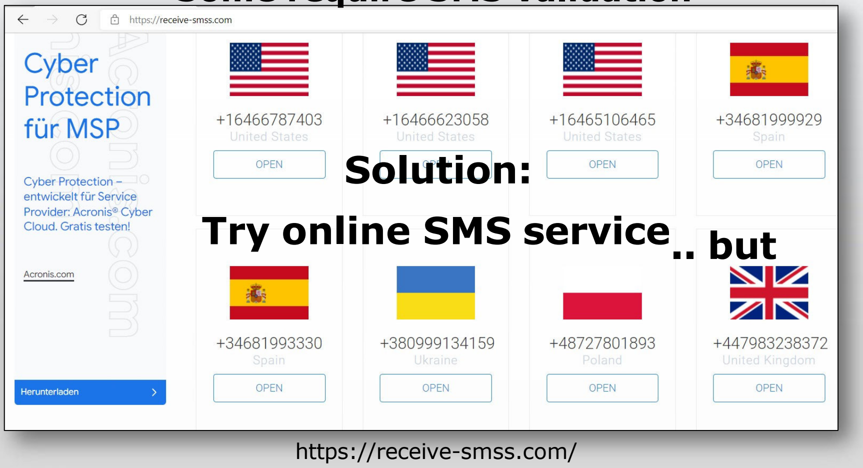
Some providers require backup email for validation

Solution:

Use an alternative email account (such as protonmail or tutanota) Or an email alias service like simplelogin.io

Creating Online Presence (online accounts):

Some require SMS validation



https://receive-smss.com

Cyber Protection für MSP

Cyber Protection – entwickelt für Service Provider: Acronis® Cyber Cloud. Gratis testen!

Acronis.com

Herunterladen

+16466787403 United States OPEN

+16466623058 United States OPEN

+16465106465 United States OPEN

+34681999929 Spain OPEN

+34681993330 Spain OPEN

+380999134159 Ukraine OPEN

+48727801893 Poland OPEN

+447983238372 United Kingdom OPEN

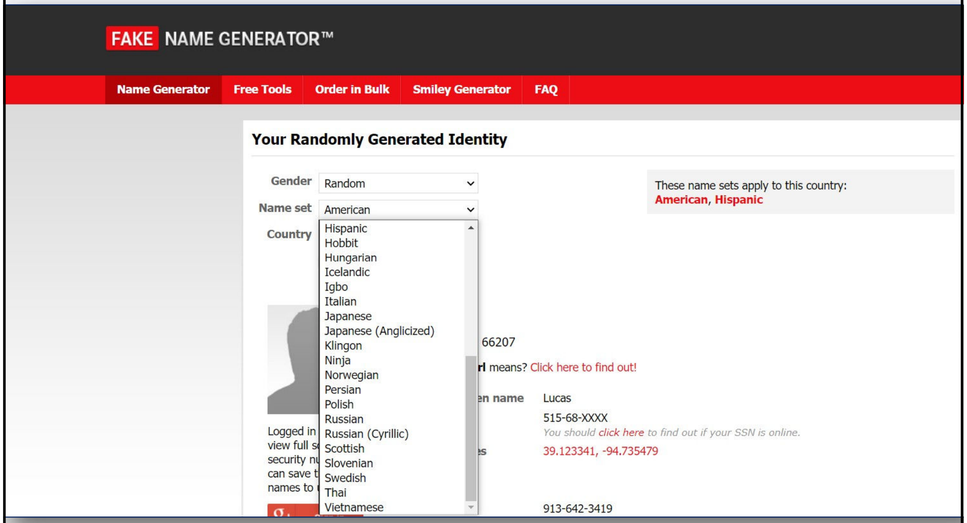
Solution:

Try online SMS service .. but

https://receive-smss.com/

Build character profile

Use your imagination or …



Your Randomly Generated Identity

Gender: Random

Name set: American

Country

These name sets apply to this country: **American, Hispanic**

66207

rl means? Click here to find out!

en name: Lucas

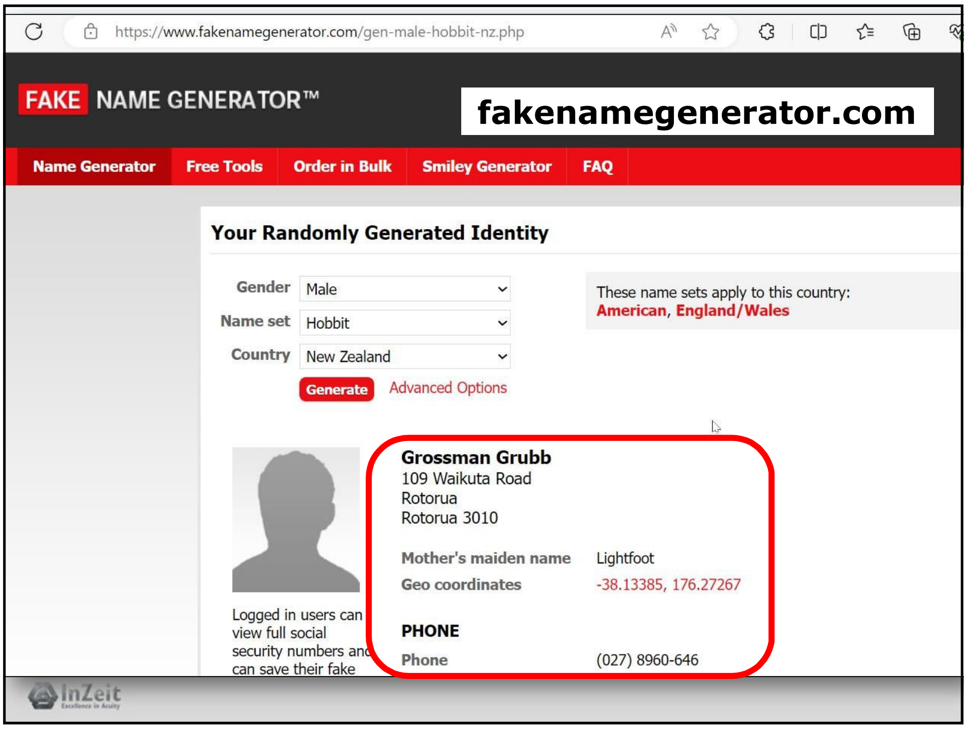
515-68-XXXX

You should click here to find out if your SSN is online.

39.123341, -94.735479

913-642-3419

Logged in
view full s
security nu
can save t
names to



fakenamegenerator.com

Your Randomly Generated Identity

Gender: Male

Name set: Hobbit

Country: New Zealand

Generate Advanced Options

These name sets apply to this country: American, England/Wales

Grossman Grubb
109 Waikuta Road
Rotorua
Rotorua 3010

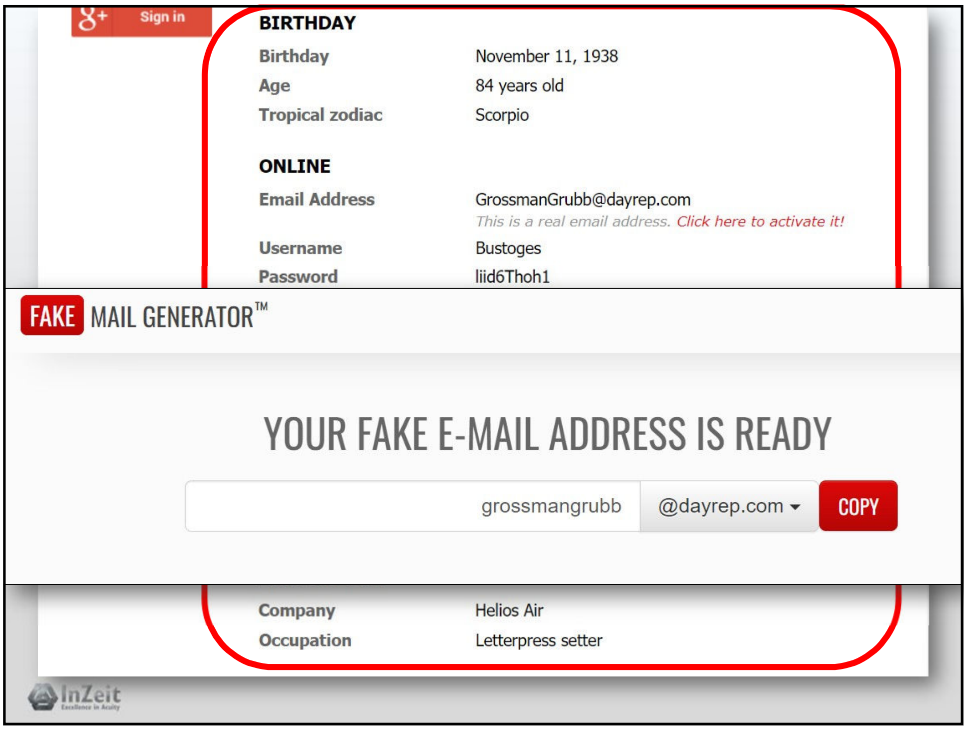
Mother's maiden name	Lightfoot
Geo coordinates	-38.13385, 176.27267

PHONE

Phone	(027) 8960-646

Logged in users can view full social security numbers and can save their fake

25



BIRTHDAY

Birthday	November 11, 1938
Age	84 years old
Tropical zodiac	Scorpio

ONLINE

Email Address	GrossmanGrubb@dayrep.com *This is a real email address. Click here to activate it!*
Username	Bustoges
Password	liid6Thoh1

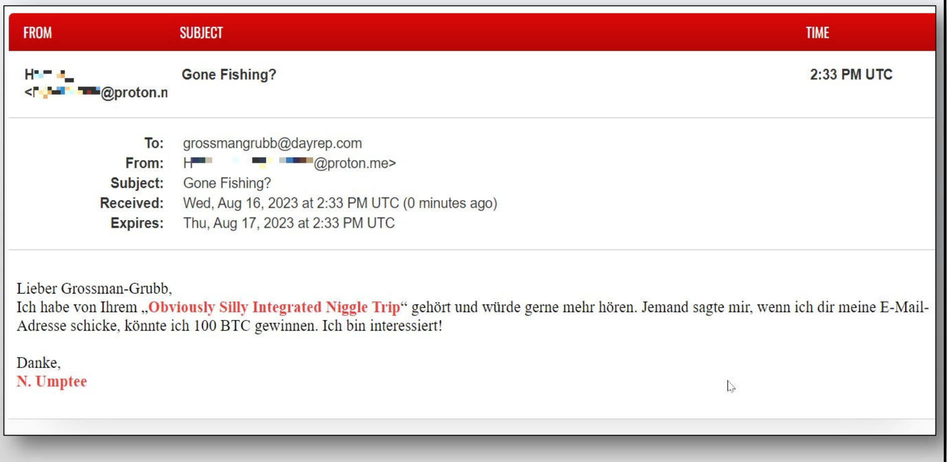
FAKE MAIL GENERATOR™

YOUR FAKE E-MAIL ADDRESS IS READY

grossmangrubb @dayrep.com ▾ COPY

Company	Helios Air
Occupation	Letterpress setter

26



FROM	SUBJECT	TIME
[redacted]@proton.n	Gone Fishing?	2:33 PM UTC

To: grossmangrubb@dayrep.com
From: [redacted]@proton.me>
Subject: Gone Fishing?
Received: Wed, Aug 16, 2023 at 2:33 PM UTC (0 minutes ago)
Expires: Thu, Aug 17, 2023 at 2:33 PM UTC

Lieber Grossman-Grubb,
Ich habe von Ihrem „**Obviously Silly Integrated Niggle Trip**" gehört und würde gerne mehr hören. Jemand sagte mir, wenn ich dir meine E-Mail-Adresse schicke, könnte ich 100 BTC gewinnen. Ich bin interessiert!

Danke,
N. Umptee

A quick case study …

(Due to the sensitive nature of the study, these slides will not be included in the handout)

Open Sourcery:

Online m tigators

NT

Co-funded by the Justice Programm of the European Union 2014-2020

© Stev

22n

The component images by Unknown Authors are licensed under CC BY-SA

29

Links and References

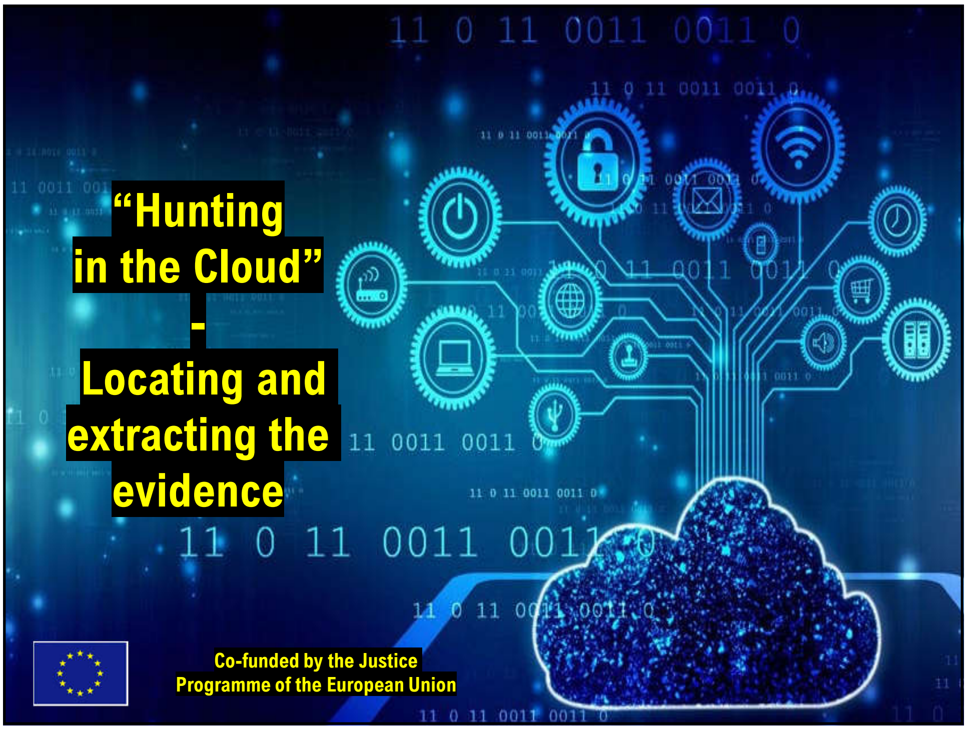
Technitium MAC Address Changer
https://technitium.com/tmac/

https://download.cnet.com/Smart-DNS-Changer/3001-2381_4-76158452.html

Online Alias
thispersondoesnotexist.com
whichfaceisreal.com
fakenamegenerator.com
www.behindthename.com

Other
opencorporates.com
https://csilinux.com/using-sock-puppet-accounts-for-osint/

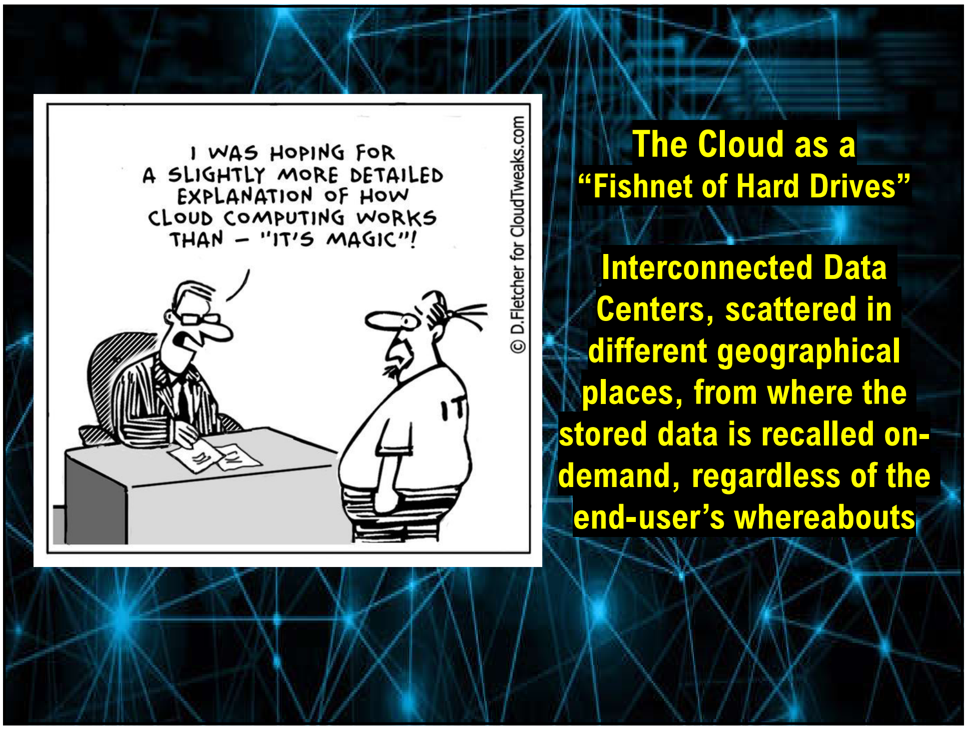
30



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

Co-funded by the Justice Programme of the European Union

1



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

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

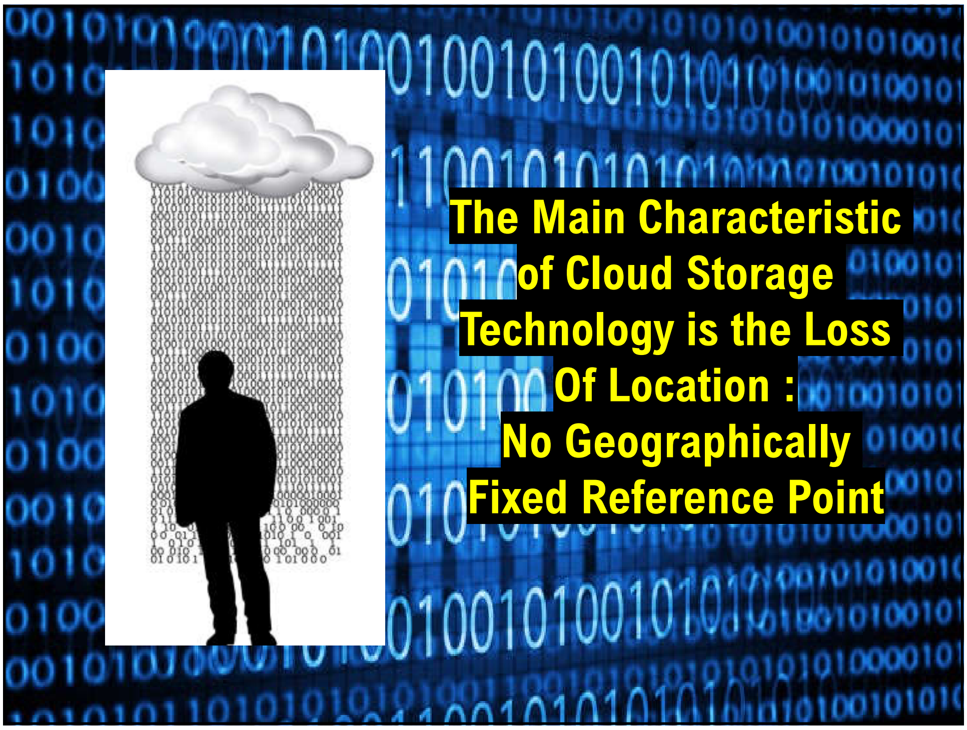
2

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

[Safety: technical problem, catastrophic event]

[Performance Optimization: propagation delay (d/s)]

3



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

4

Main Legal Challenge : Data Territoriality and Applicable Law

A] “Possession” of Cloudly Stored Data

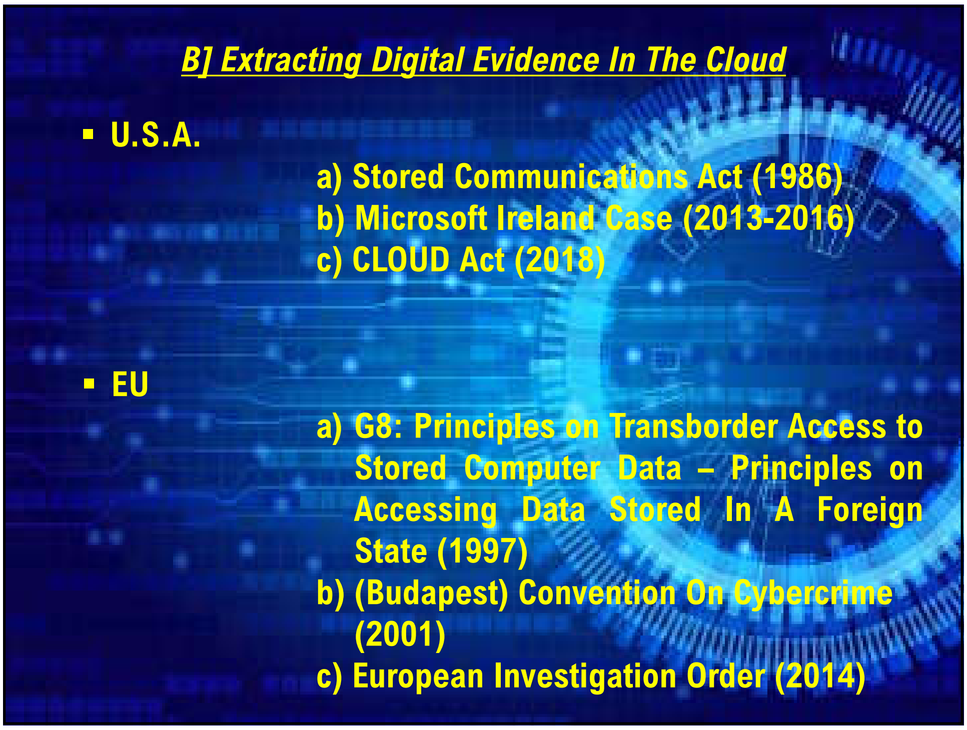
B] Extracting Digital Evidence In The Cloud

5

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)

6



B] Extracting Digital Evidence In The Cloud

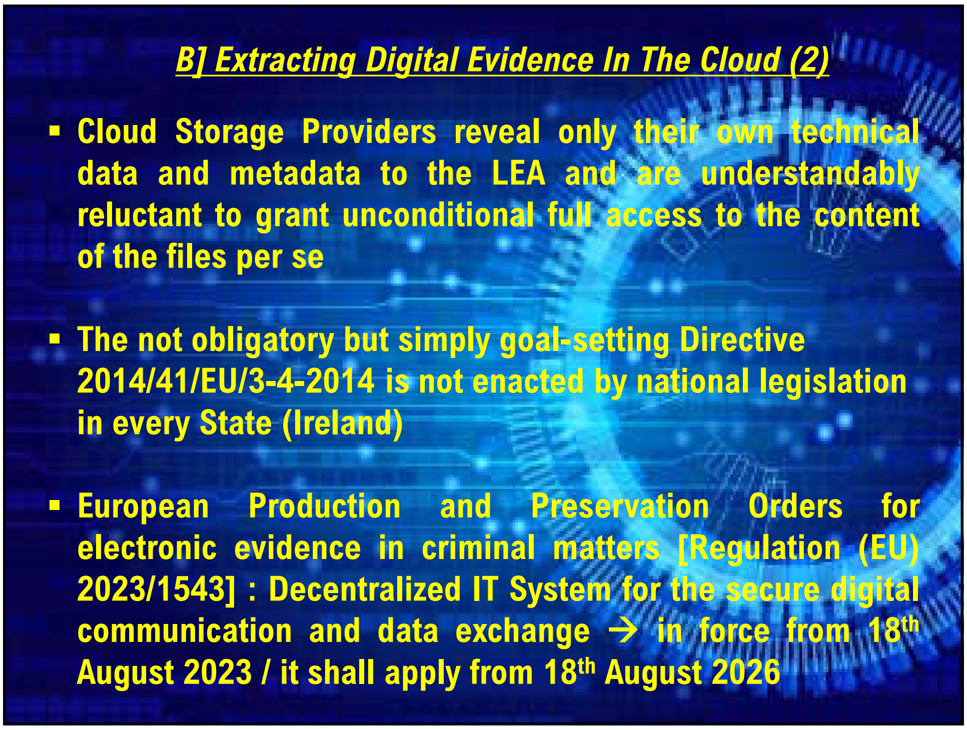
- U.S.A.

  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)

7



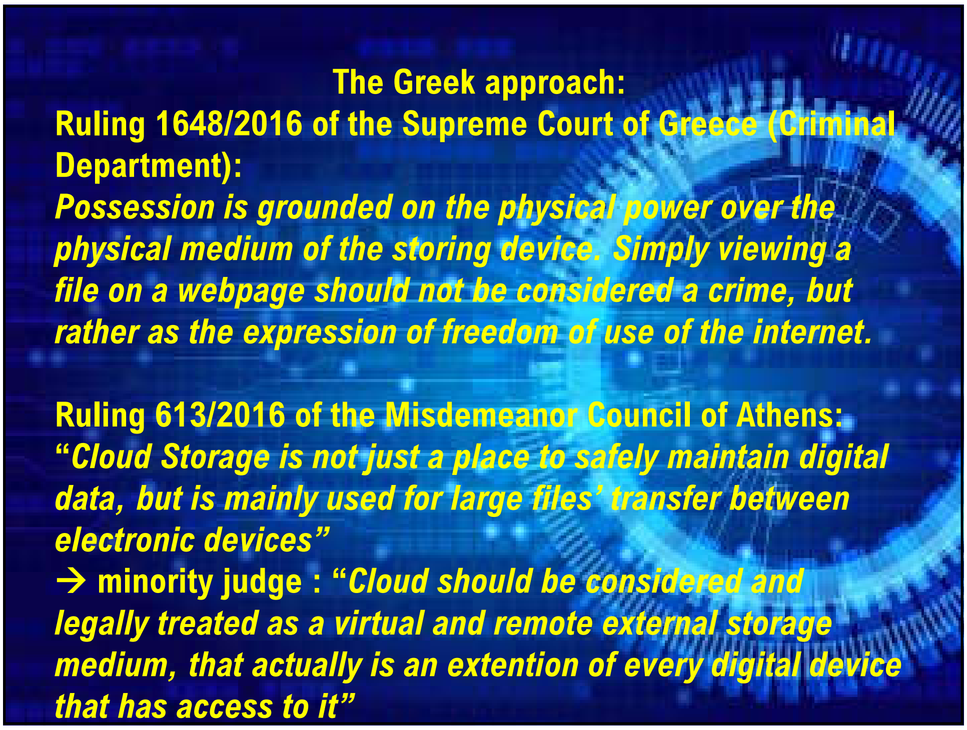
B] Extracting Digital Evidence In The Cloud (2)

- 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

8

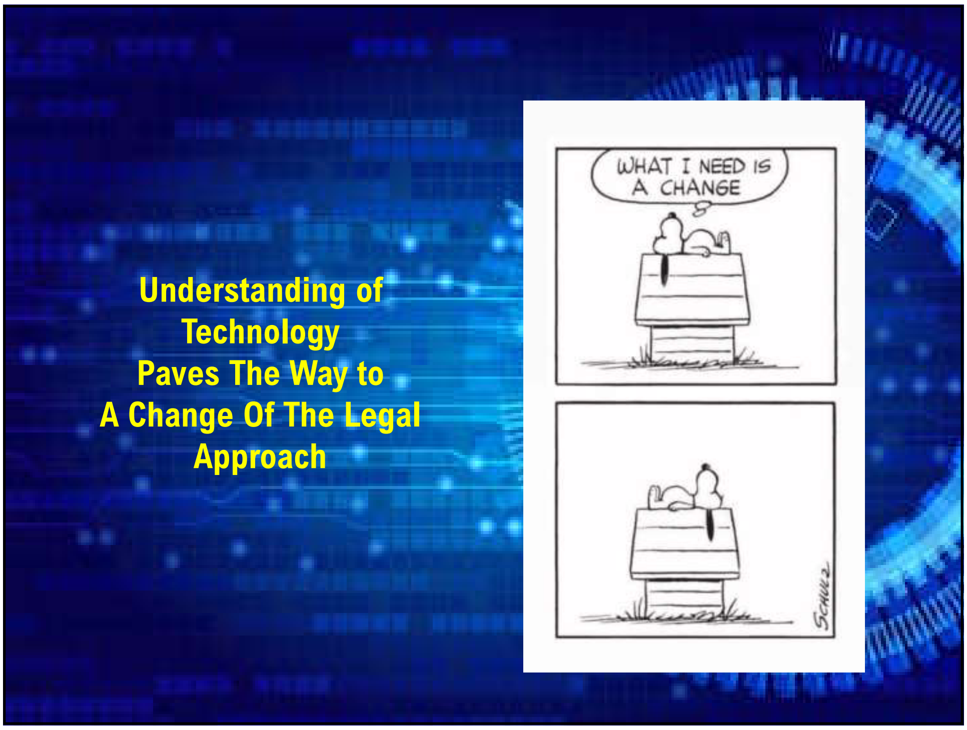


The Greek approach:

Ruling 1648/2016 of the Supreme Court of Greece (Criminal Department):
Possession is grounded on the physical power over the physical medium of the storing device. Simply viewing a file on a webpage should not be considered a crime, but rather as the expression of freedom of use of the internet.

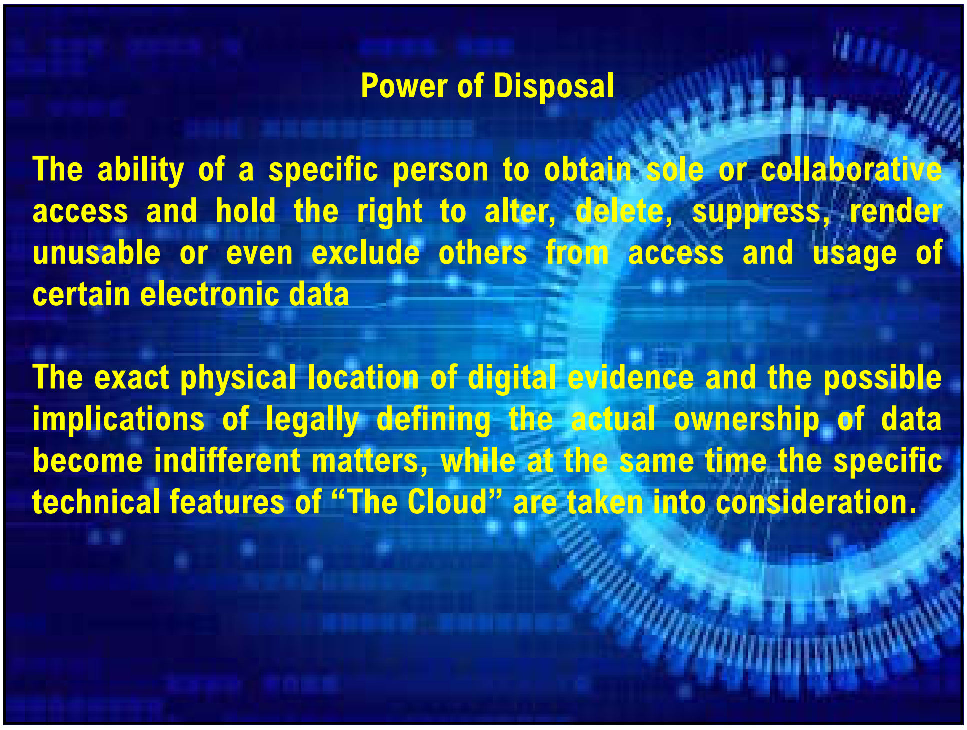
Ruling 613/2016 of the Misdemeanor Council of Athens:
"Cloud Storage is not just a place to safely maintain digital data, but is mainly used for large files' transfer between electronic devices"
→ minority judge : *"Cloud should be considered and legally treated as a virtual and remote external storage medium, that actually is an extention of every digital device that has access to it"*

9



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

10



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