POST-COVID CHALLENGES IN CRIMINAL JUSTICE

The web, the dark/deep web and other sources of evidence available online: what legal practitioners need to know

Lisbon, 16-17 May 2023

FACE-TO-FACE

EXCELLENCE IN EUROPEAN LAW

Speakers and chairs

Steven David Brown, International Cybercrime Consultant, Vienna

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

Savina Gruičić, Digital Forensic Consultant, INsig2, Zagreb

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

Christos Karagiannis, Prosecutor, Court of First Instance, Larissa

Eneli Laurits, District Prosecutor, Department for Drug Related, Grave and Organized Crimes, Tallinn

Jordy Mullers, Part-time Judge at Zeeland-West Brabant District Court, Legal Advisor at the Criminal Investigations Division of the Dutch National Police, Regional Unit Limburg

Vitor Neves, Criminal Defence Lawyer, IT Law, Data Protection and Fintech, Porto

John Van Krieken, Judge, Court of Appeal, Tilburg

Fernando Vaz Ventura, Judge of Appeal; Director, CEJ, Lisbon

Key topics

- Understanding the internet and associated technology
- Dark web investigations
- Open source tools (OST)
- How to conduct a forensics analysis
- Handling e-evidence in court

Language
English

Event number
323DT12

Organisers
ERA (Laviero Buono) in cooperation with the Portuguese Centre of Judicial Studies

CENTRO DE ESTUDOS JUDICIÁRIOS

With the support of the of the European Union

european.law

POST-COVID CHALLENGES IN CRIMINAL JUSTICE

Tuesday, 16 May 2023

09:00 Arrival and registration of participants

09:30 **Welcome and introduction to the programme**
Fernando Vaz Ventura & Laviero Buono

PART I: TECHNICAL ISSUES AND BASIC UNDERSTANDING OF THE INTERNET ACHITECTURE AND OPEN-SOURCE INTELLIGENCE TOOLS

Chair: Laviero Buono

09:35 **Cyber Post-Pandemic: The internet unmasked**
- The different dimensions and manifestations of the Internet (LAN, WAN, WWW, Cloud, Deep, Dark)
- Threats and opportunities in obtaining Internet evidence
- The challenges of live forensics
- How users mask their locations
- Logs, browser fingerprints and data breadcrumbs

Steven David Brown

10:45 Discussion

11:00 Break

11:30 **Using open-source intelligence to gather evidence online**
- OSINT and SOCMINT: is this a silver bullet for evidence search?
- Search engines: how does it work?
- Alternative search engines to explore the hidden Internet
- Main obstacles getting data from online sources or "How to think as a hacker"
- Visualization of forensics findings: must or nice to do

Rūta Jašinskienė

12:30 Discussion

12:45 Lunch break

PART II: CARRYING OUT REAL DIGITAL FORENSIC INVESTIGATIONS – DEMOS

Chair: Steven David Brown

13:45 **Conducting forensic analysis at the crime scene**
- Triage of the crime scene (search warrant, equipment considerations, protocols, interviewing the suspect)
- Gathering digital evidence from live memory
- Labs
- Scripts in digital forensic examinations
- Computer and mobile forensics

Savina Gruičić

14:45 Discussion

15:00 Break

PART III: COMPUTER FORENSICS AND LEGAL ASPECTS

15:30 **Cross-border access to data and admissibility of evidence**
- Obtaining e-evidence
- Voluntary access to evidence
- Direct access and legal process

Jordy Mullers

Objective

The main objective of this seminar is to train EU legal practitioners on the fundamentals of computer forensics enabling them to gain an understanding of the complex challenges related to criminal cases with tech/internet components. This event will focus on dark web investigations.

About the Project

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

Who should attend?

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

Venue

Centro de Estudos Judiciários,
Largo do Limoeiro
Lisbon (Portugal)

CPD

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

16:15 Discussion

16:30 End of first day

20:00 Dinner offered by the organisers

Wednesday, 17 May 2023

PART IV: HUNTING IN THE DARK…

Chair: John Van Krieken

09:30 **Hunting in the Dark: a prosecutor's experience to the darknet**
Eneli Laurits

10:00 Discussion

10:15 **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

10:45 Discussion

11:00 Break

Chair: Laviero Buono

11:30 **Special investigation techniques in the Darkweb: a new evidentiary frontier for the judge**
- Challenges posed by the darkweb
- Proving the authenticity of the data
- Presentation of evidence in court

John Van Krieken

12:00 Discussion

12:15 **Computer forensics, dark web investigations and electronic evidence in court: the experience in Portugal**
Vitor Neves

12:45 Discussion

13:00 End of seminar and light lunch

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

Your contact persons

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

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

Save the date

Legal Challenges of the #Metaverse
Trier & Online, 23-24 March 2023

Annual Conference on Artificial Intelligence Systems and Fundamental Rights 2023
Trier & Online, 27-28 April 2023

This programme has been produced with the financial support 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

Lisbon, 16-17 May 2023 / Event number: 323DT12/SBa

Apply online for "Post-Covid Challenges in Criminal Justice" online: **www.era.int/?131839&en**

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 **10 March 2023**.
3. A response will be sent to every applicant after this deadline. **We advise you not to book any travel or hotel before you receive our confirmation**.

Registration Fee

4. €130 including documentation, lunches and dinner.

Travel and Accommodation Expenses

5. Participants will receive a fixed contribution towards their travel and accommodation expenses and are asked to book their own travel and accommodation. The condition for payment of this contribution is to sign all attendance sheets at the event. No supporting documents are needed. The amount of the contribution will be determined by the EU unit cost calculation guidelines, which are based on the distance from the participant's place of work to the seminar location and will not take account of the participant's actual travel and accommodation costs.
6. Travel costs from outside Portugal: 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 Spanish participants the amounts for Inter-Member States return journeys between 50 and 400 km is fixed at €54, please consult p.11 on https://era-comm.eu/go/unit-cost-decision-travel).*
7. For those travelling within Portugal, the contribution for travel is fixed at €40 (for a distance between 50km and 400km). Please note that no contribution will be paid for travel under 50km. For more information, please consult p.10 on https://era-comm.eu/go/unit-cost-decision-travel
8. Accommodation costs: international participants and national participants travelling more than 50km one-way will receive a fixed contribution of €109 per night for up to two nights' accommodation. For more information, please consult p.13 on https://era-comm.eu/go/unit-cost-decision-travel
9. These rules do not apply to representatives of EU Institutions and Agencies who are required to cover their own travel and accommodation.
10. Successful applicants will be sent the relevant claim form and information on how to obtain payment of the contribution to their expenses. Please note that no payment is possible if the registered participant cancels their participation for any reason.

Participation

11. Participation at the whole conference is required and your presence will be recorded.
12. A list of participants including each participant's address will be made available to all participants unless the ERA receives written objection from the participant no later than one week prior to the beginning of the event.
13. 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.
14. A certificate of attendance will be distributed at the end of the conference.

Venue

Centro de Estudos Judiciários,
Largo do Limoeiro
Lisbon (Portugal)

Language

English

Contact Person

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

323DT12
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.

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*)

CENTRO DE ESTUDOS JUDICIÁRIOS

Cyber Pandemic: The Internet unmasked

ERA
Academy of European Law

Steven David Brown

Lisbon
16-17 May 2023

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

InZeit Excellence in Acuity

© All Rights Reserved

1

What is the Internet ?

Internet, a system architecture that has revolutionized communications and methods of commerce by allowing various computer networks around the world to interconnect. Sometimes referred to as a "network of networks"

https://www.britannica.com/technology/Internet

World Wide Web (WWW) […] the leading information retrieval service of the Internet (the worldwide computer network). The Web gives users access to a vast array of documents that are connected to each other by means of hypertext or hypermedia links—i.e., hyperlinks, electronic connections that link related pieces of information in order to allow a user easy access to them.

https://www.britannica.com/topic/World-Wide-Web

InZeit Excellence in Acuity

2

What is the Internet ?

Internet, a system architecture that has revolutionized communications and methods of commerce by allowing various computer networks around the world to interconnect. Sometimes referred to as a "network of networks"

https://www.britannica.com/technology/Internet

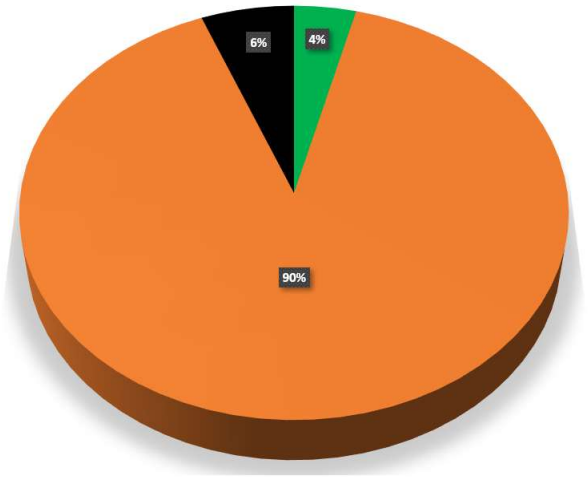
World Wide Web (WWW) […] the leading information retrieval service of the Internet (the worldwide computer network). The Web gives users access to a vast array of documents that are connected to each other by means of hypertext or hypermedia links—i.e., hyperlinks, electronic connections that link related pieces of information in order to allow a user easy access to them.

https://www.britannica.com/topic/World-Wide-Web

InZeit
Excellence in Acuity

3

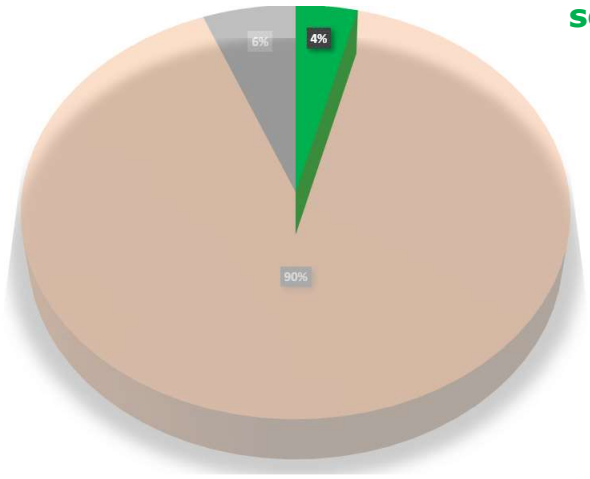
The Internet



InZeit
Excellence in Acuity

4

WWW 4%

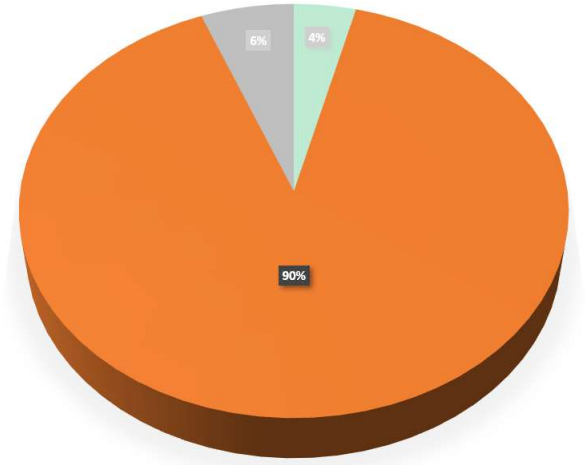


WWW
Indexed by search engines; publicly accessible

InZeit
Excellence in Acuity

5

Deep Web 90%



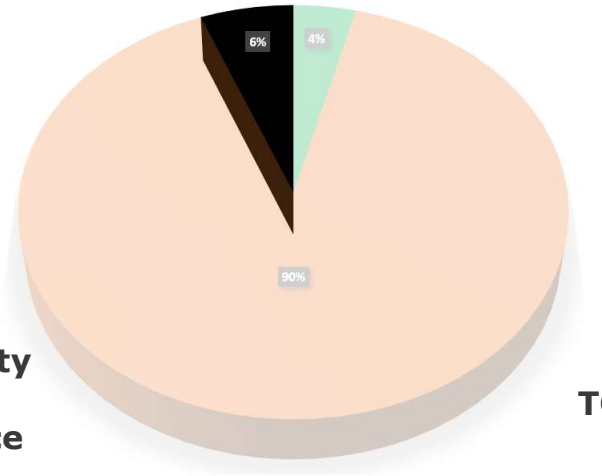
Not indexed by search engines:
Govt. communications;
banks; corporations; medical records;

InZeit
Excellence in Acuity

6

DarkNet 6%

Special software for access; spies, dissidents & criminals



Internet Anonymity and prevents online surveillance

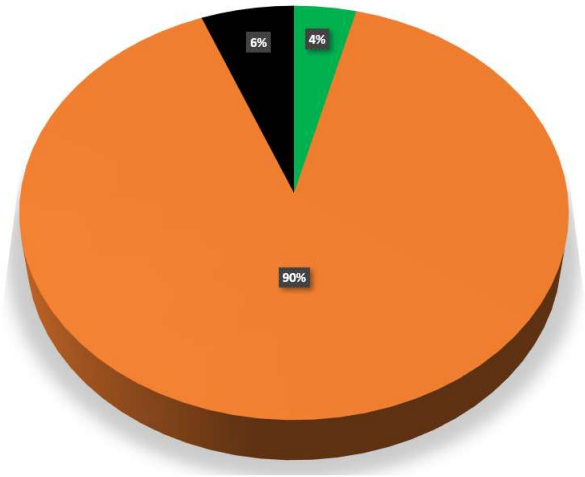
TOR ("The Onion Router") Started as US Navy-funded project 1995

InZeit Excellence in Acuity

7

DarkNet 6%

WWW 4%



US DARPA "ARPANET" 29 Oct 1969

Sir Tim Berners-Lee CERN* 1989

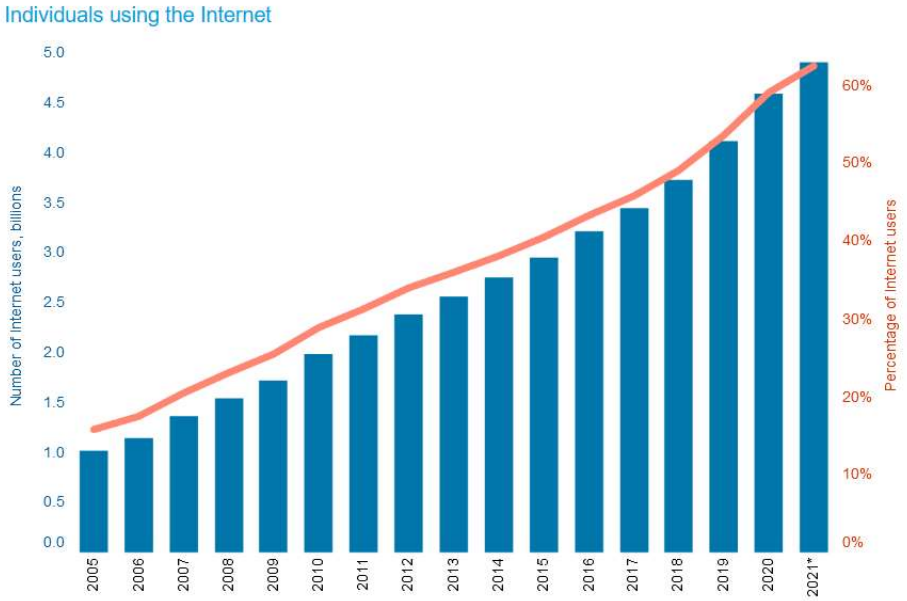
Deep Web 90%

InZeit Excellence in Acuity

*Conseil européen pour la recherche nucléaire

8

"Internet uptake has accelerated during the pandemic"

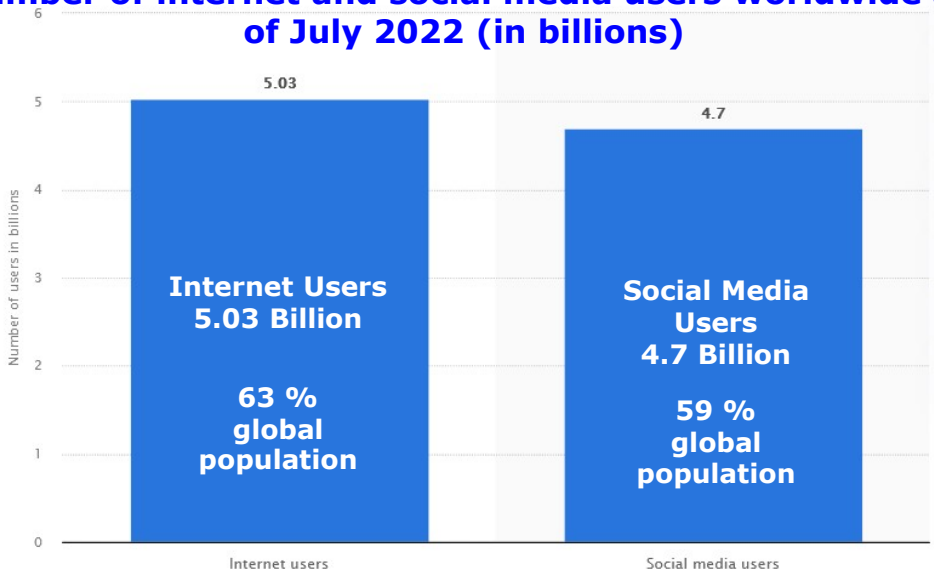


4.9 Billion (63%)

2019: 4.1 billion (54%)

https://www.itu.int/itu-d/reports/statistics/2021/11/15/internet-use/

Number of internet and social media users worldwide as of July 2022 (in billions)



Source: Statista September 20, 2022
https://www.statista.com/statistics/617136/digital-population-worldwide/

Pandemic Risks:

- Greater 'attack surface'
- Use of domestic devices & networks (less security)
- Bring Your Own Device
- Video Conferencing vulnerabilities
- Increased use for banking/shopping
- Loneliness (romance fraud)
- ??? Abrupt sacking of staff in IT companies???

Interesting presentation: https://rm.coe.int/presentation-fernando-miro-llinares-the-impact-of-covid-19-on-cybercri/1680a1e42f

11

The Internet?

Insecure by design

Image by Unknown Author is licensed under CC BY-NC

12

Must prove:

Which device used in the offence

AND

Who was using it at the relevant time. (traditional forensics may also help)

Please note:
Information has been simplified to make it easier to understand and remember

Identifiers have been redacted

InZeit
Excellence in Acuity

13

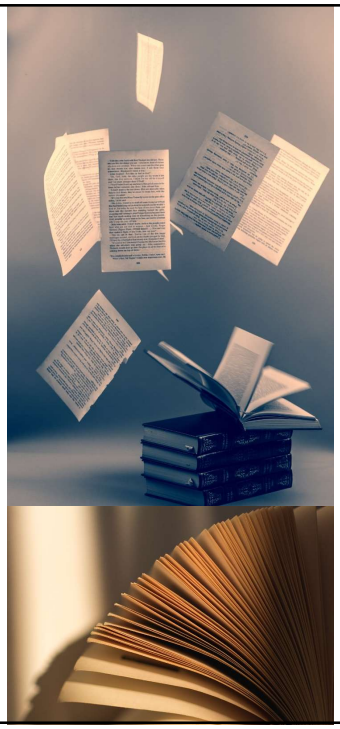
HTTP & HTTPS (Hyper Text Transfer Protocol (Secure))

Indexed 'pages'

Collection of pages = Website

Unique Resource Locators (URLs) = the website address in words (linked to IP Address)

Domain Name = the name you remember + the domain extension (e.g. era.int)



InZeit
Excellence in Acuity

Images by Unknown Author is licensed under CC BY-NC

14

http://www.era.int

InZeit Excellence in Acuity

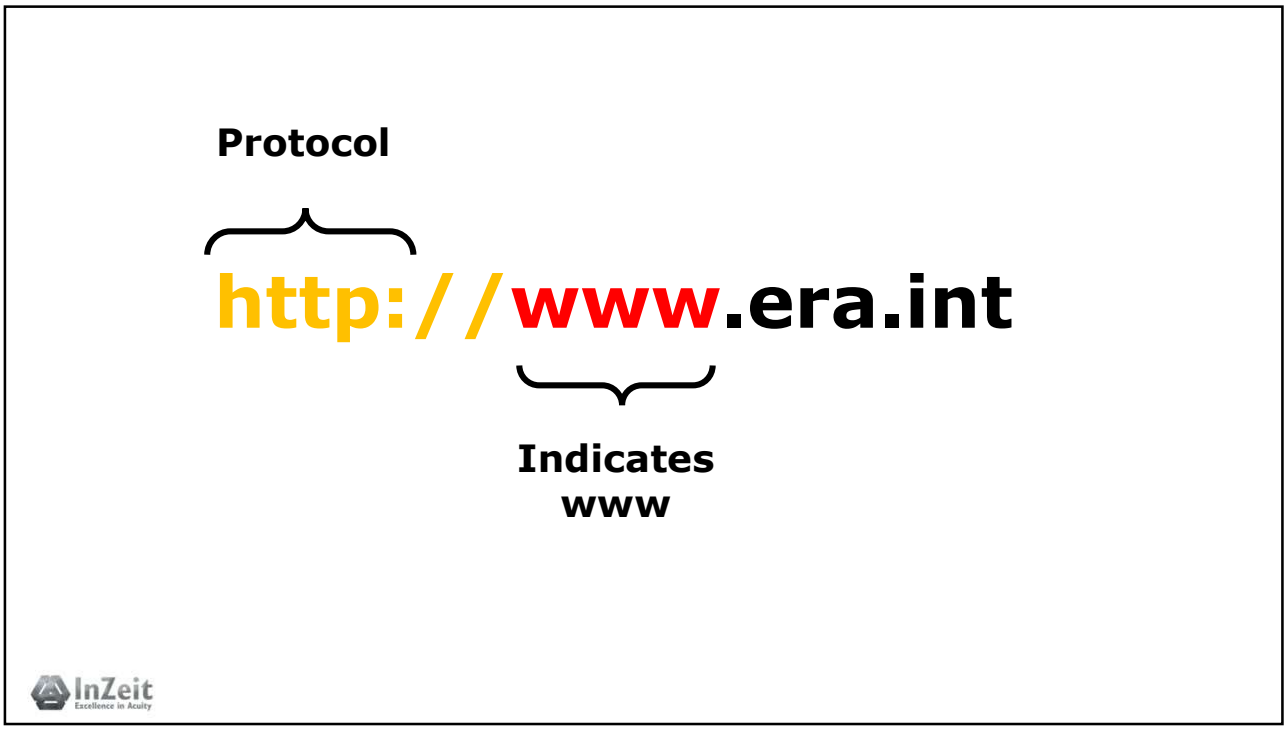
15

Protocol

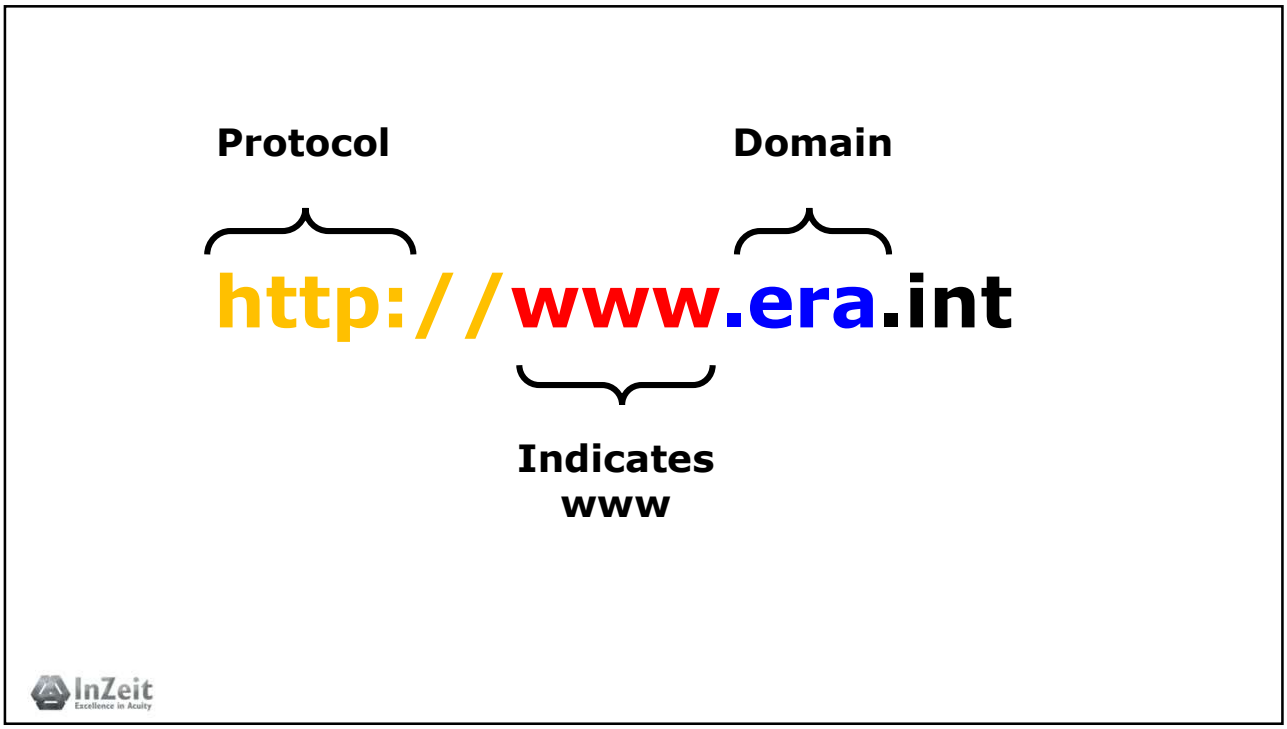
http://www.era.int

InZeit Excellence in Acuity

16


Protocol
http://www.era.int
Indicates
www
InZeit
Excellence in Acuity

17


Protocol
Domain
http://www.era.int
Indicates
www
InZeit
Excellence in Acuity

18

Protocol

Domain

http://www.era.int

Indicates www

Top level domain

.gov .com .edu .org .net .co.uk .de .fr

https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains

Whois

Register of Internet domain name 'owners'

- Registrant data may be false
- Hidden behind a registration service
- Place to start search
- EU GDPR Rules – Whois blocked

(Authorised groups still have access)

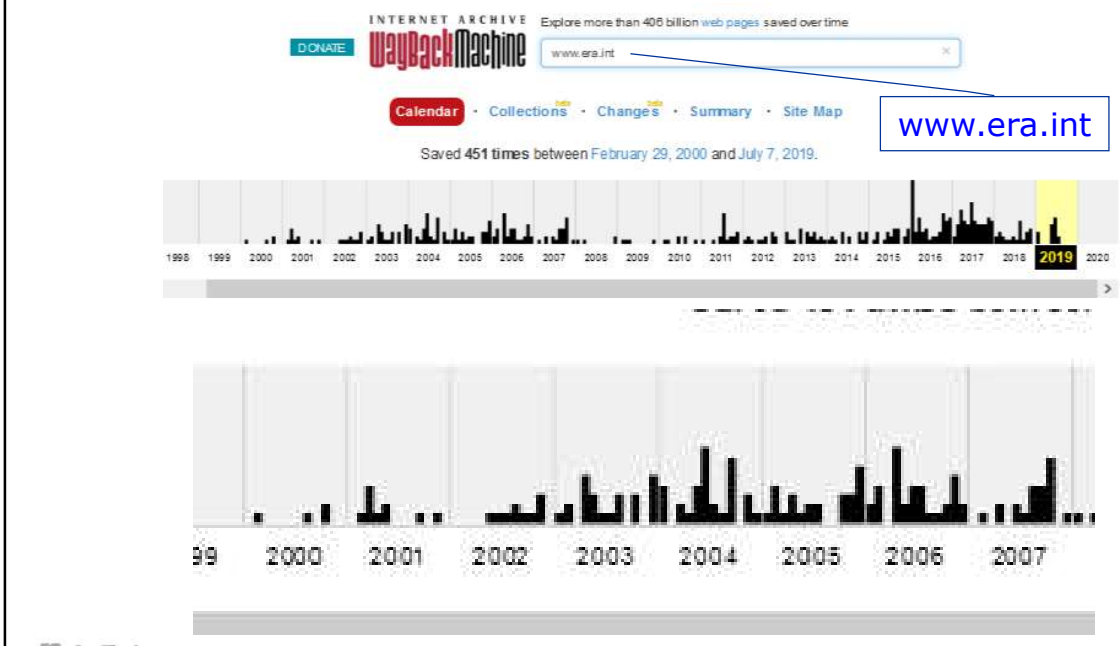
When websites change:

INTERNET ARCHIVE
WayBackMachine

(http://web.archive.org)

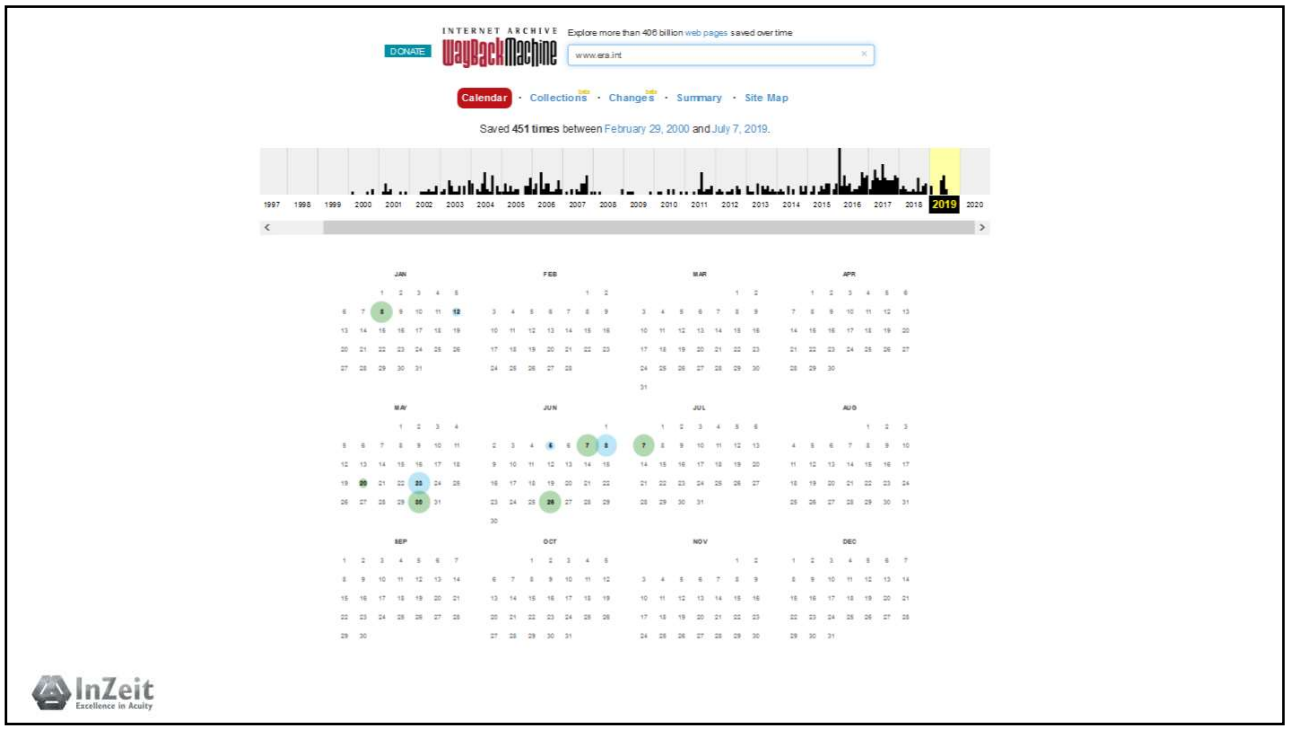
InZeit
Excellence in Acuity

21



InZeit
Excellence in Acuity

22



23

Website from 23 June 2000

24

Normally:
First step is to '
the IP A

Can be faked, hidden or 'borrowed'

An Internet ess is the unique number generated ervice Provider and assigned to a connec to identify the source & destination of messages across the Internet (like a postal address).

InZeit
Excellence in Acuity

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"

Images by Unknown Author are licensed under CC BY-SA

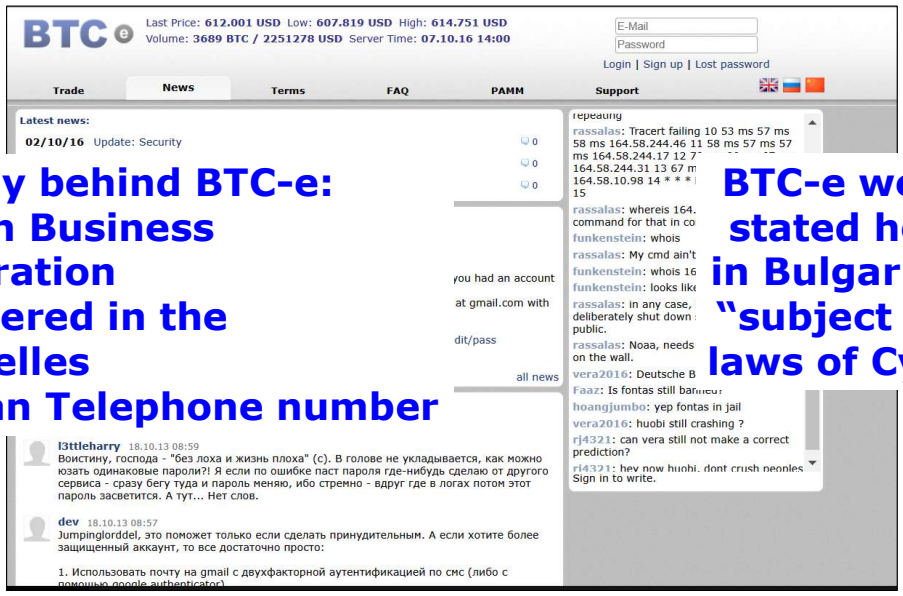
26

Stolen BTC tracked by Chainalysis

Eventually ended up at BTC-e Exchange

BTC-e ownership and location unknown

Images by Unknown Author are licensed under CC BY-SA



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"

InZeit Excellence in Acuity

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

BTC-e
Bitcoin Exchange

CLOUDFLARE.

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

InZeit
Excellence in Acuity

Images by Unknown Author are licensed under CC BY-SA

29

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"

InZeit
Excellence in Acuity

30

User WME = Alexander Vinnik

July 2017 Arrested in Thessaloniki

France, Russia, USA sought Extradition

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

2020 extradited to France

Sentenced to 5 years, deported to Greece 2022

5 August 2022 extradited to USA

InZeit Excellence in Acuity

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

Internet Protocol (IP) Addresses

Two types:

- **Static** (always the same)
- **Dynamic** (only lasts as long as connected)

Two versions:

IPv4

(4.3 billion - not enough numbers for everyone)

IPv6

What's yours? www.ipchicken.com

InZeit Excellence in Acuity

Every website (every connection to Internet) has an associated IP address:

www.era.int

IPv4:

195.243.153.54

IPv6:

0:0:0:0:0:ffff:c3f3:9936

InZeit Excellence in Acuity

33

IP Address:

- **Geo-specific**
- **Identifies:**
  - **The country**
  - **The ISP**

ISP holds records of usage

InZeit Excellence in Acuity

34

Be careful what you ask for …

IP Address:
Needs to be carefully recorded
Time stamped to the second

InZeit Excellence in Acuity

35

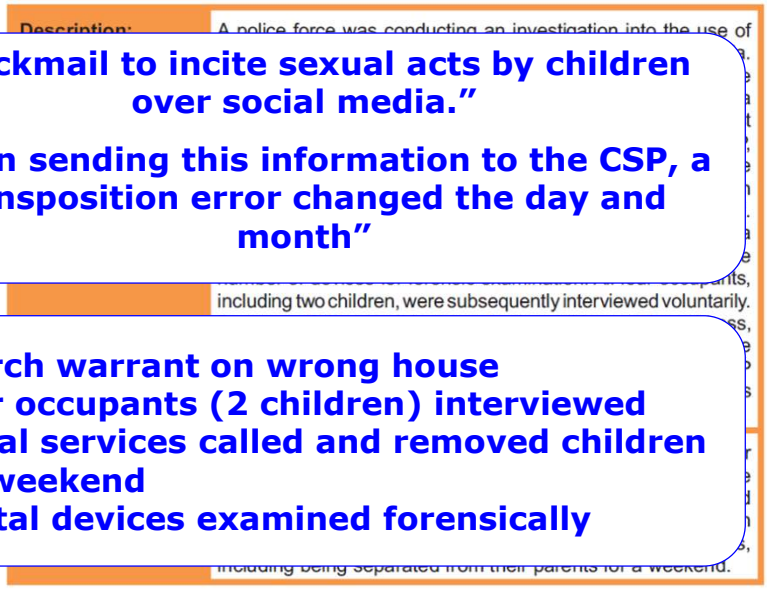
UK Information Commissioner's Report 2016

Description:	A police force was conducting an investigation into the use of blackmail to incite sexual acts by children over social media. The force made a series of accurate applications to identify the person using the offending account. In their final application, a request was made to find the broadband account used to first register the username. When sending this information to the CSP, a transposition error changed the day and month. The name and address received in response to this incorrect information became the base upon which an intelligence package was built. This intelligence was sent to another force who executed a search warrant at the incorrect address. Officers seized a large number of devices for forensic examination. All four occupants, including two children, were subsequently interviewed voluntarily. Because of the possible threat to the children at the address, social services were called in to assist, and briefly separated the children from their parents. The family's solicitor received the IP resolution results through the legal disclosure process. This was queried by the account holder, and the error was revealed.
Consequence:	The police searched an address unconnected with their investigation, carried out forensic examination of a large number of devices owned by innocent people and conducted voluntary interviews of four people. This included two children who were then subject to formal safeguarding processes, including being separated from their parents for a weekend.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/670219/IOCCO_annual_report_2016_2.PDF p74

InZeit Excellence in Acuity

36



"Blackmail to incite sexual acts by children over social media."

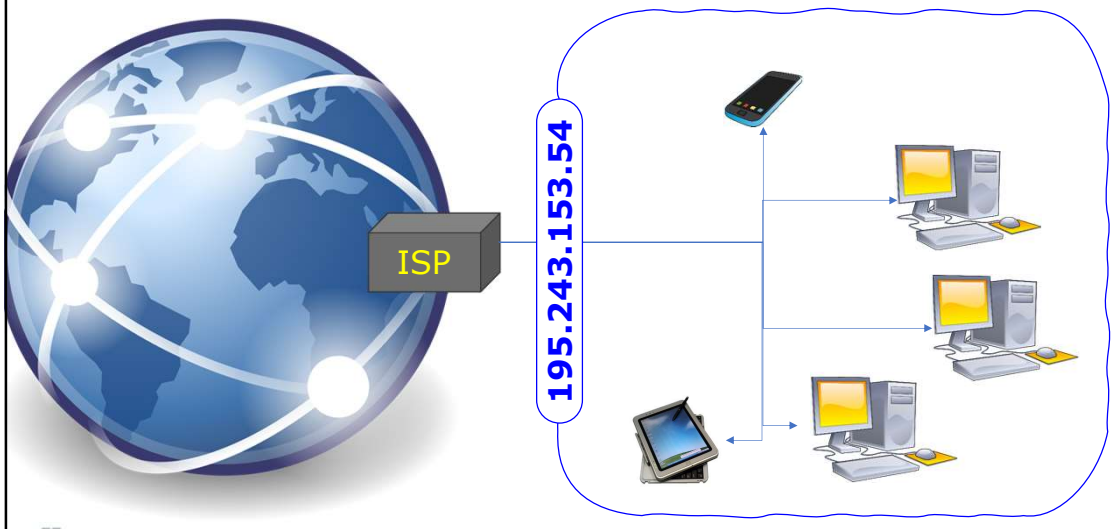
"When sending this information to the CSP, a transposition error changed the day and month"

- **Search warrant on wrong house**
- **Four occupants (2 children) interviewed**
- **Social services called and removed children for weekend**
- **Digital devices examined forensically**

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/670219/IOCCO_annual_report_2016_2.PDF p74

37

MAC Address:
(Media Access Control or Physical Address)

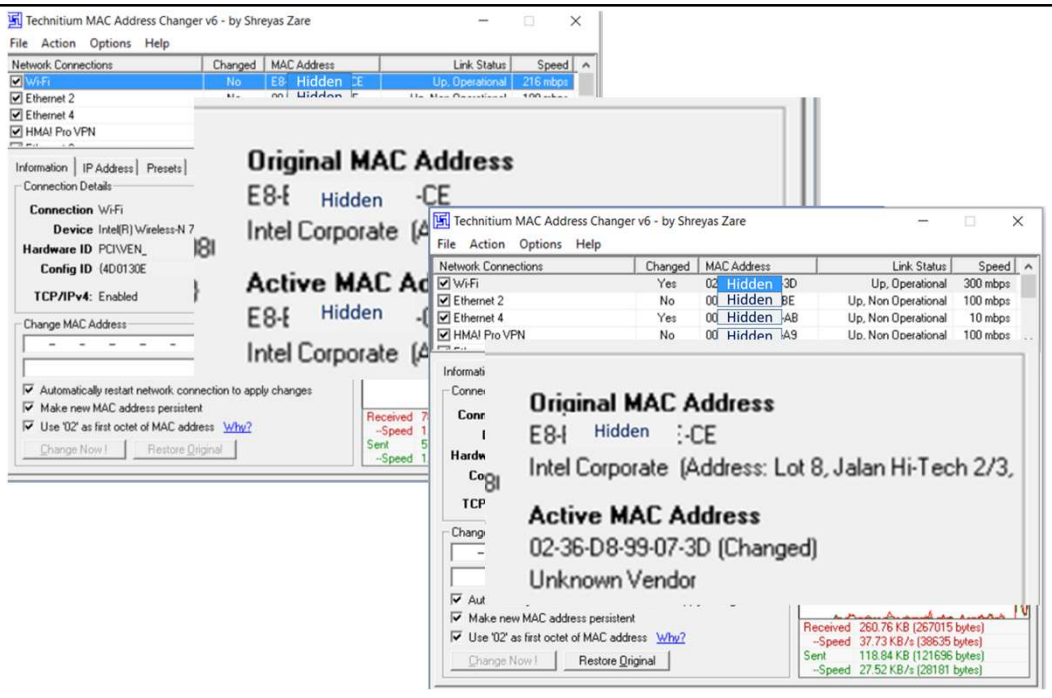


38

MAC Address: (Media Access Control or Physical Address)

- Identifies the device on the network
- Built into the device by manufacturer
- (normally) not broadcast beyond network
- But can 'leak' (e.g. some IPv6 versions)

InZeit Excellence in Acuity



InZeit Excellence in Acuity

Phones - IMEI

International Mobile Equipment Identity

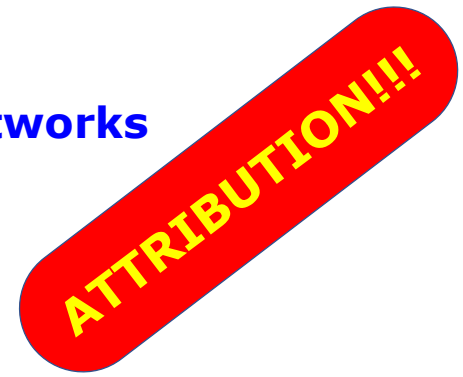
- Also MEID (Mobile Equipment Identifier)
- Hardcoded into mobile device by manufacturer (make and model can be traced)
- Identifies the device to the Cell Network
- Get IMEI Number key in: *#06#

InZeit Excellence in Acuity

41

Hiding an IP

- Public Access Points
- Piggybacking
- Compromised devices
- Proxy servers
- Virtual Private Networks
- Anonymisers
- Carriergrade NAT



InZeit Excellence in Acuity

42

4 March 2015, California

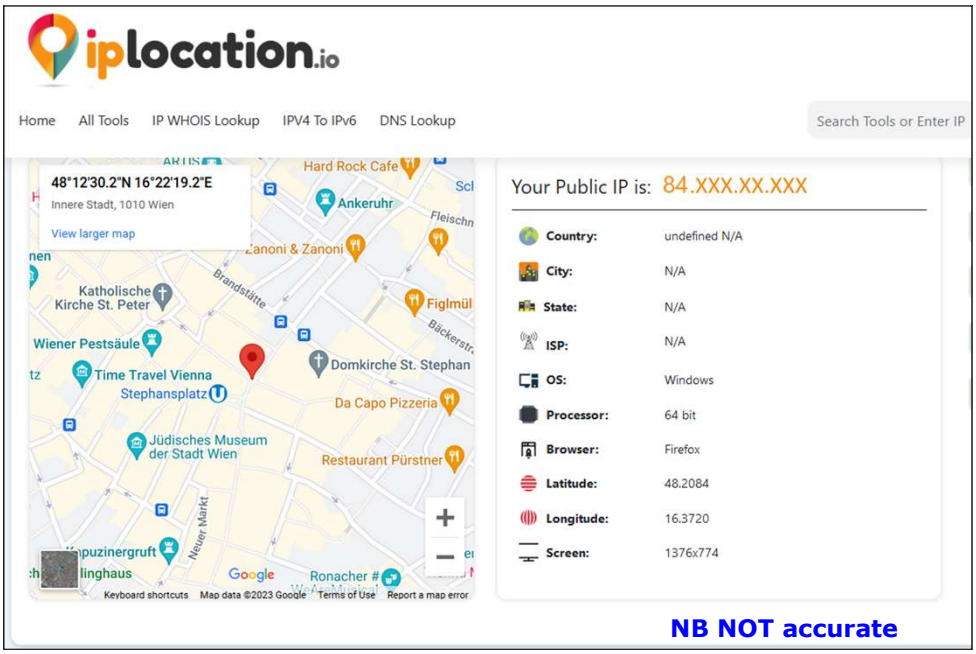
- Home burgled
- 65-inch Smart TV (with Netflix) stolen
- Victim realised someone using her Netflix account

InZeit Excellence in Acuity

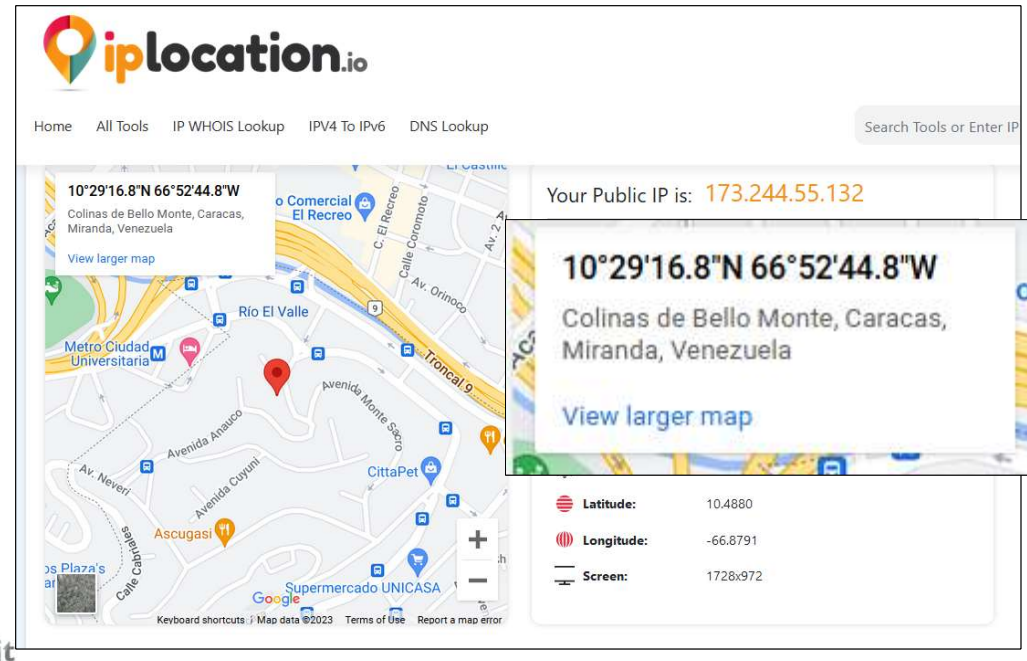
Bobby Alexander

- Police obtained IP address
- Raided the given address
- Came up with nothing
- Owners explained neighbour used their wifi account

InZeit Excellence in Acuity


iplocation.io
Home
All Tools
IP WHOIS Lookup
IPV4 To IPv6
DNS Lookup
Search Tools or Enter IP
48°12'30.2"N 16°22'19.2"E
Innere Stadt, 1010 Wien
View larger map
Hard Rock Cafe
Ankeruhr
Zanoni & Zanoni
Katholische Kirche St. Peter
Figlmül
Wiener Pestsäule
Time Travel Vienna
Stephansplatz
Domkirche St. Stephan
Da Capo Pizzeria
Jüdisches Museum der Stadt Wien
Restaurant Pürstner
Google
Keyboard shortcuts
Map data ©2023 Google
Terms of Use
Report a map error
Your Public IP is: 84.XXX.XX.XXX
Country: undefined N/A
City: N/A
State: N/A
ISP: N/A
OS: Windows
Processor: 64 bit
Browser: Firefox
Latitude: 48.2084
Longitude: 16.3720
Screen: 1376x774
NB NOT accurate

45


iplocation.io
Home
All Tools
IP WHOIS Lookup
IPV4 To IPv6
DNS Lookup
Search Tools or Enter IP
10°29'16.8"N 66°52'44.8"W
Colinas de Bello Monte, Caracas, Miranda, Venezuela
View larger map
Río El Valle
Metro Ciudad Universitaria
Troncal 9
Avenida Anauco
Avenida Cuyuni
Av. Neveri
CittaPet
Ascugasi
Supermercado UNICASA
Google
Keyboard shortcuts
Map data ©2023
Terms of Use
Report a map error
Your Public IP is: 173.244.55.132
10°29'16.8"N 66°52'44.8"W
Colinas de Bello Monte, Caracas, Miranda, Venezuela
View larger map
Latitude: 10.4880
Longitude: -66.8791
Screen: 1728x972

46

Virtual Private Networks (VPNs)

VPNs enable access to the Internet through a remote computer/server using encrypted communication channel/tunnel

VPNs can be used by criminals to hide their location

VPN Providers often cooperate with legal process … some don't!

InZeit Excellence in Acuity

47

China	Banned (unless licenced)
Turkey	Banned
Iraq	Banned
Russia	Banned
Belarus	Banned
North Korea	Banned
Turkmenistan	Banned
UAE	Only approved VPNs
Iran	Only approved VPNs
Oman	Not for personal use
India	Data reporting requirement
Myanmar	Only approved VPNs
Pakistan	Only if user registers

N.B. VPNs are controlled in some countries (check local law before use)

https://www.comparitech.com/vpn/where-are-vpns-legal-banned/

InZeit Excellence in Acuity

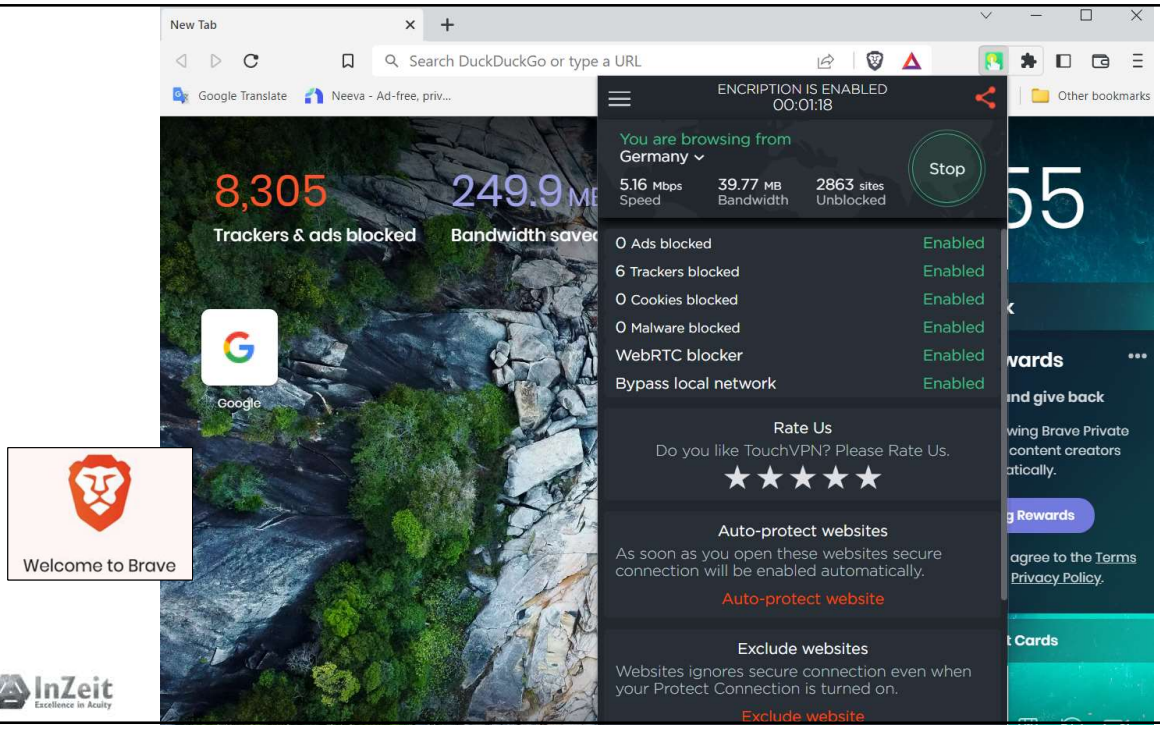
48

Well known VPN providers:

ExpressVPN
NordVPN
Hidemyass
CyberGhost VPN
Proton VPN

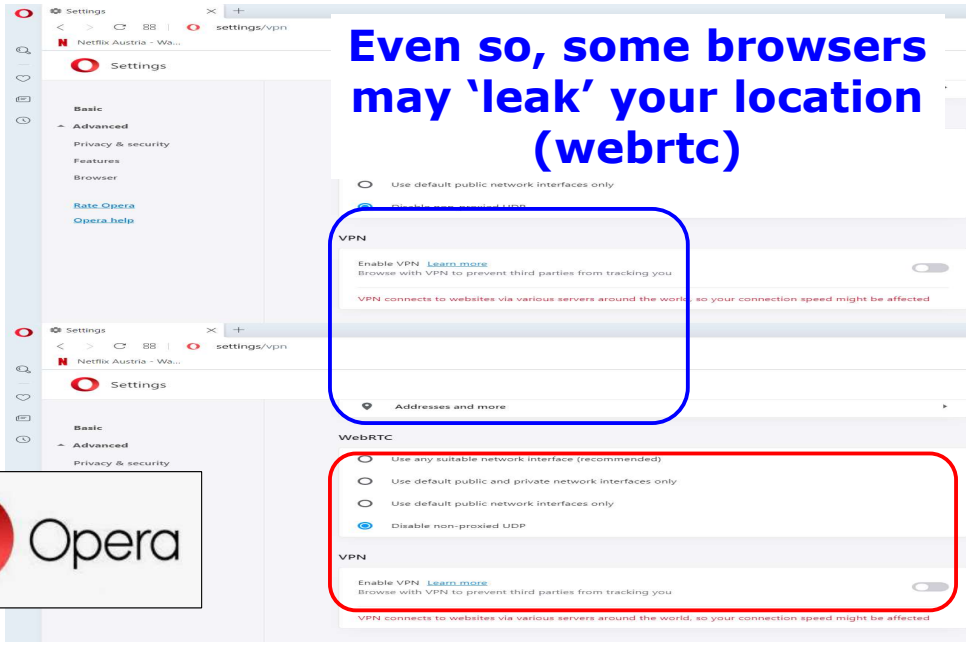
Also included in some anti-virus/internet security packages And browsers

InZeit Excellence in Acuity



InZeit Excellence in Acuity

Even so, some browsers may ‘leak’ your location (webrtc)



Opera

InZeit Excellence in Acuity

Settings/Advanced/Privacy & security/

All you need is logs

… the automatically produced and time-stamped documentation of events relevant to a particular system

(source:www.techtarget.com)

InZeit Excellence in Acuity

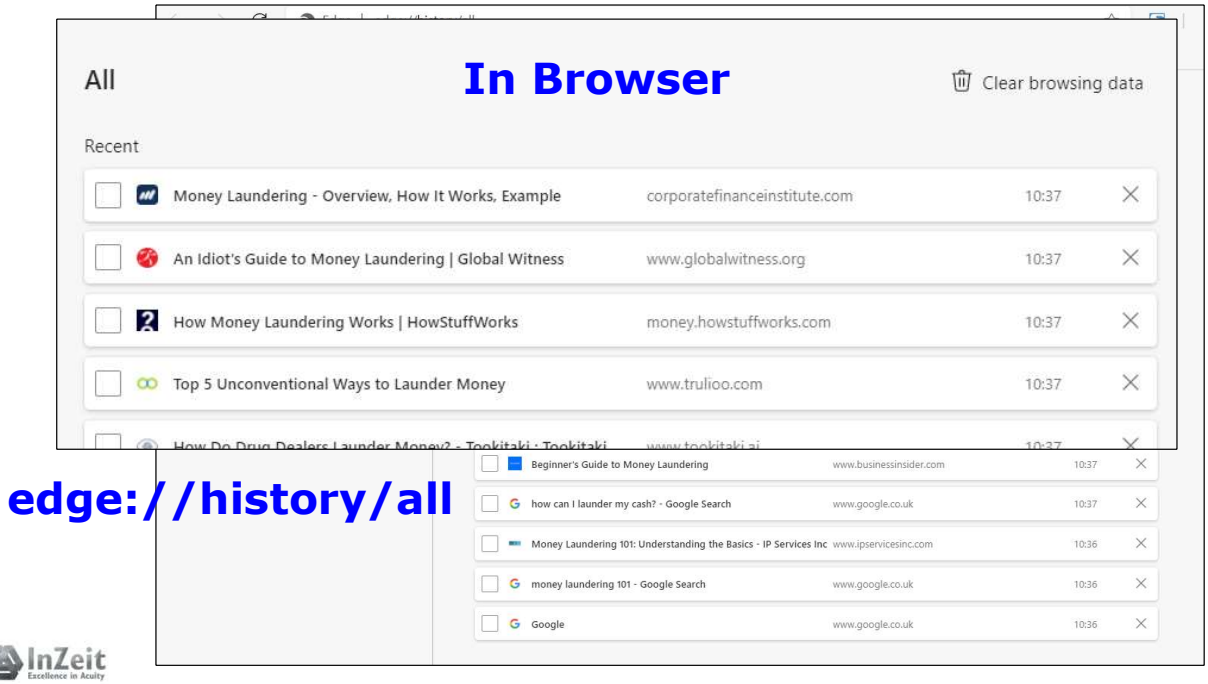
LOGS

- Originally created for tracing bugs & improving performance
- Billing/maintenance records
- Generated automatically
- On the device
- On servers in the network
- Service providers
- Record meta-, traffic-data

InZeit Excellence in Acuity

53

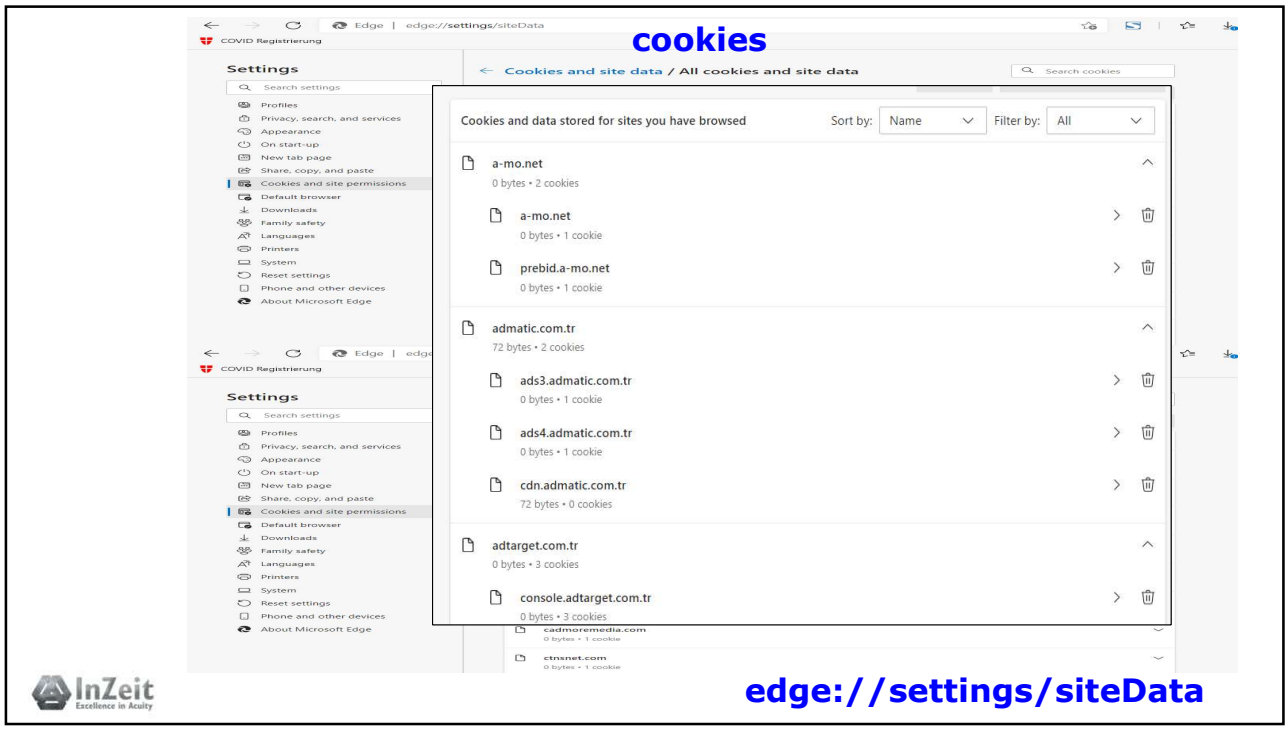
In Browser



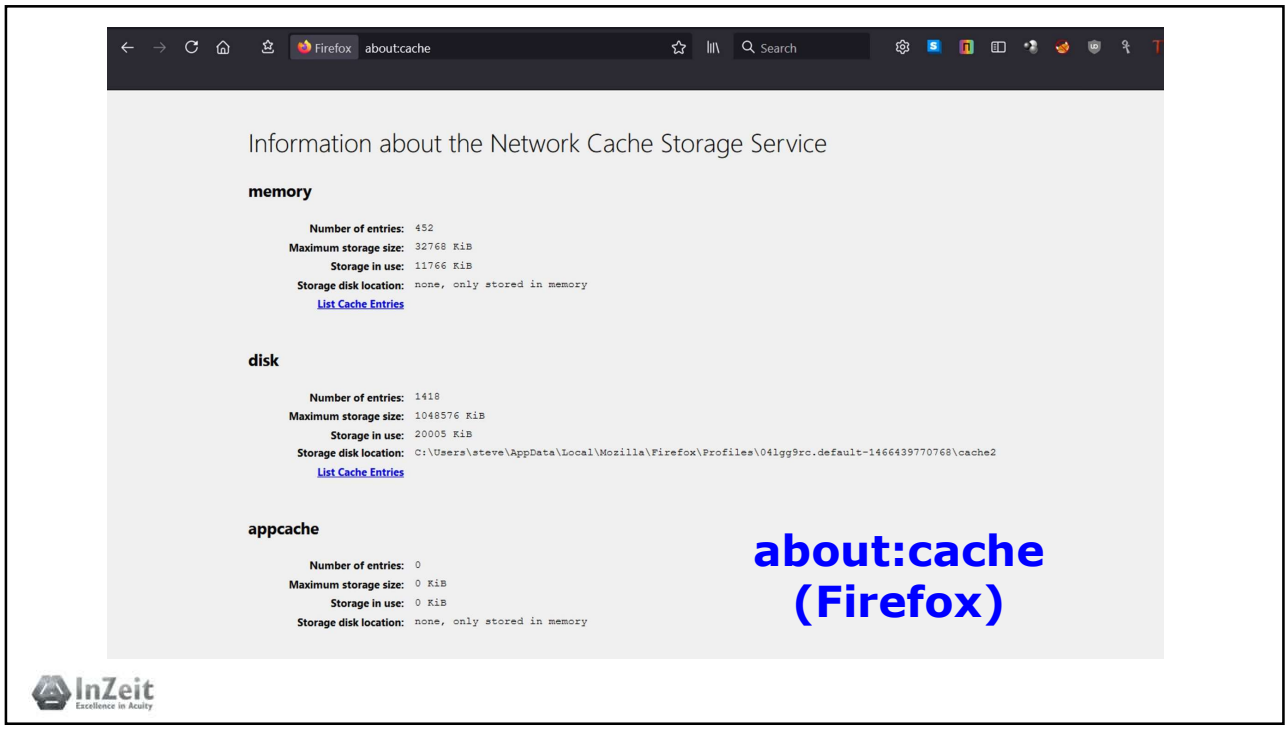
edge://history/all

InZeit Excellence in Acuity

54

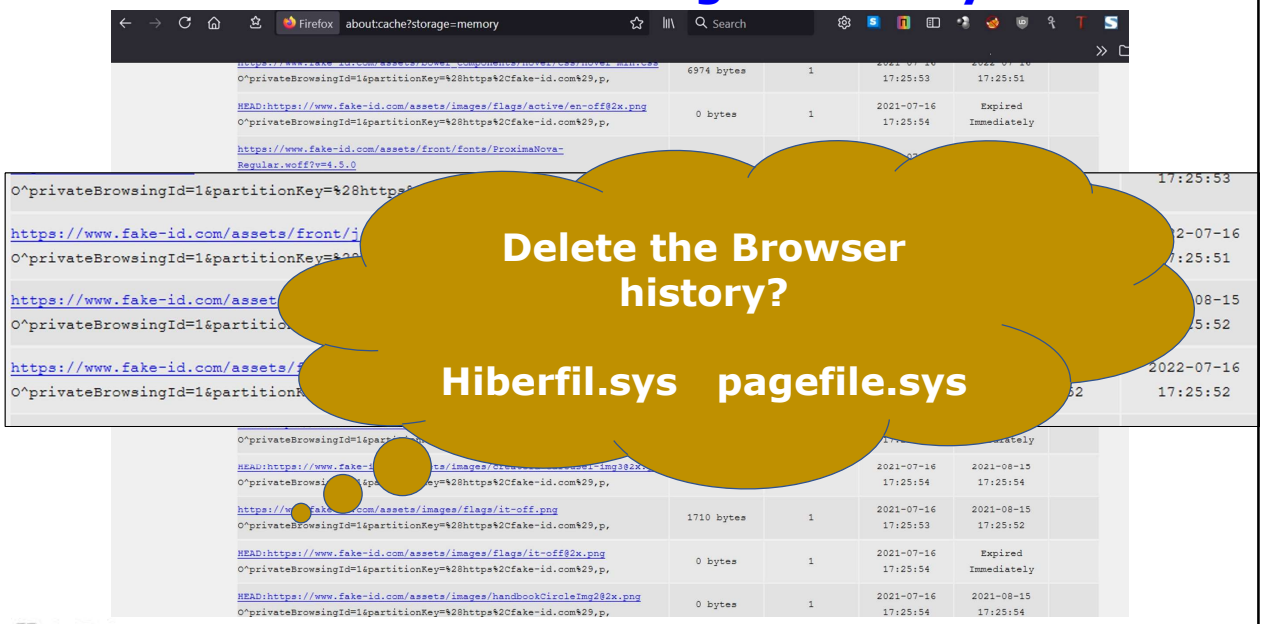

cookies
Edge | edge://settings/siteData
COVID Registrierung
Settings
Search settings
Profiles
Privacy, search, and services
Appearance
On start-up
New tab page
Share, copy, and paste
Cookies and site permissions
Default browser
Downloads
Family safety
Languages
Printers
System
Reset settings
Phone and other devices
About Microsoft Edge
Cookies and site data / All cookies and site data
Search cookies
Cookies and data stored for sites you have browsed
Sort by: Name
Filter by: All
a-mo.net
0 bytes • 2 cookies
a-mo.net
0 bytes • 1 cookie
prebid.a-mo.net
0 bytes • 1 cookie
admatic.com.tr
72 bytes • 2 cookies
ads3.admatic.com.tr
0 bytes • 1 cookie
ads4.admatic.com.tr
0 bytes • 1 cookie
cdn.admatic.com.tr
72 bytes • 0 cookies
adtarget.com.tr
0 bytes • 3 cookies
console.adtarget.com.tr
0 bytes • 3 cookies
edge://settings/siteData

55


Firefox about:cache
Search
Information about the Network Cache Storage Service
memory
Number of entries: 452
Maximum storage size: 32768 KiB
Storage in use: 11766 KiB
Storage disk location: none, only stored in memory
List Cache Entries
disk
Number of entries: 1418
Maximum storage size: 1048576 KiB
Storage in use: 20005 KiB
Storage disk location: C:\Users\steve\AppData\Local\Mozilla\Firefox\Profiles\04lgg9rc.default-1466439770768\cache2
List Cache Entries
appcache
Number of entries: 0
Maximum storage size: 0 KiB
Storage in use: 0 KiB
Storage disk location: none, only stored in memory
about:cache
(Firefox)

56

about:cache?storage=memory



InZeit Excellence in Acuity

57

Mohammed Ammer Ali –Computer Programmer
Father of two, Bolton, UK
2015 ordered enough ricin on Dark Web to kill 700 - 1,400 people

Username weirdos 0000

500 mg for 2.1849 BTC
(then = GBP320 those were the days!!!!!)

Encrypted chats discussed with seller:

- **the price of a lethal dose,**
- **discounts for bulk orders and repeat purchases**
- **ricin's shelf life**

Asked: "How do I test this ricin?"
Reply:"You must test it on a rodent."

InZeit Excellence in Acuity

58

Investigators found on Ali's Computer notepad:
To do "paid ricin guy" and "get pet to murder"

Searches for chinchillas, animal rescue centres, rabbits and "pocket-sized pets"

Google searches:

"abrin v ricin"
"home made cyanide and ricin"
"hydrogen peroxide"

On LG Nexus smartphone searched Yahoo for:

"what poison kills you quick, is foolproof, easily found/made, easily concealed and hard to detect post mortem"

InZeit Excellence in Acuity

https://www.theguardian.com/uk-news/2015/sep/18/breaking-bad-fan-jailed-over-ricin-plot
https://www.bbc.com/news/uk-england-merseyside-36483593

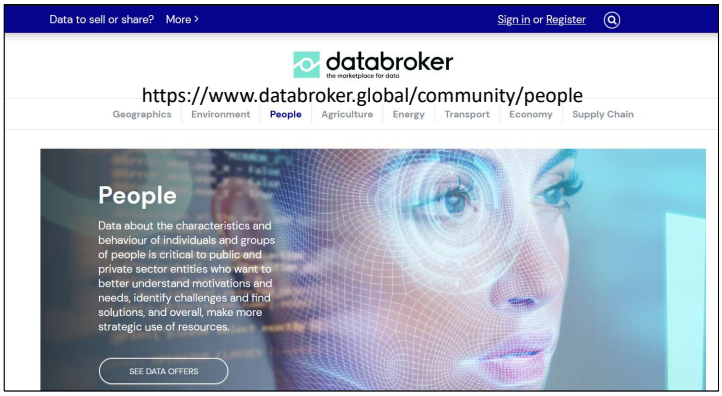
Cookies, search history and device configuration create a characteristic 'browser fingerprint'

Try this out:

https://webkay.robinlinus.com/

InZeit Excellence in Acuity

Commercial value – profile used by Data Brokers for targeted online advertising.

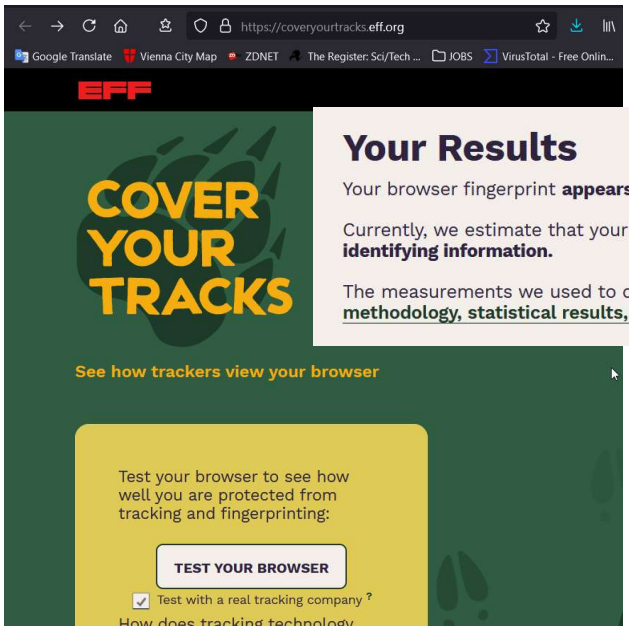


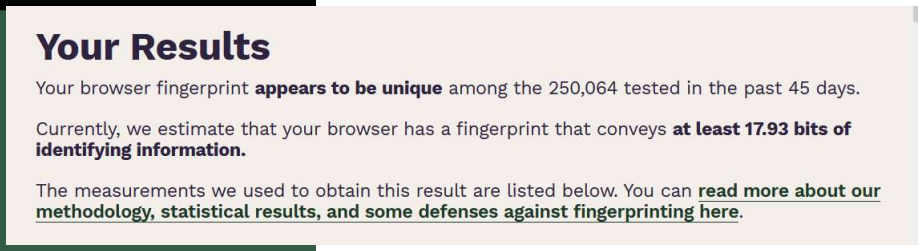
https://www.databroker.global/community/people

'In 2017, both Alphabet (Google's parent company) and Facebook made an overwhelming majority of their total profits through digital advertising—88% and 97%, respectively.'

https://us.norton.com/internetsecurity-privacy-how-data-brokers-find-and-sell-your-personal-info.html

61

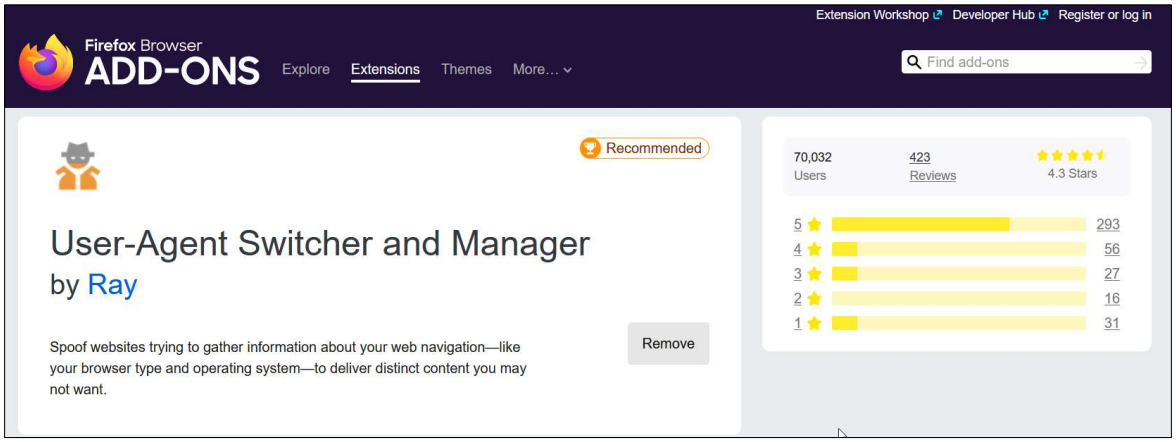




Browser Fingerprinting
https://coveryourtracks.eff.org/

62

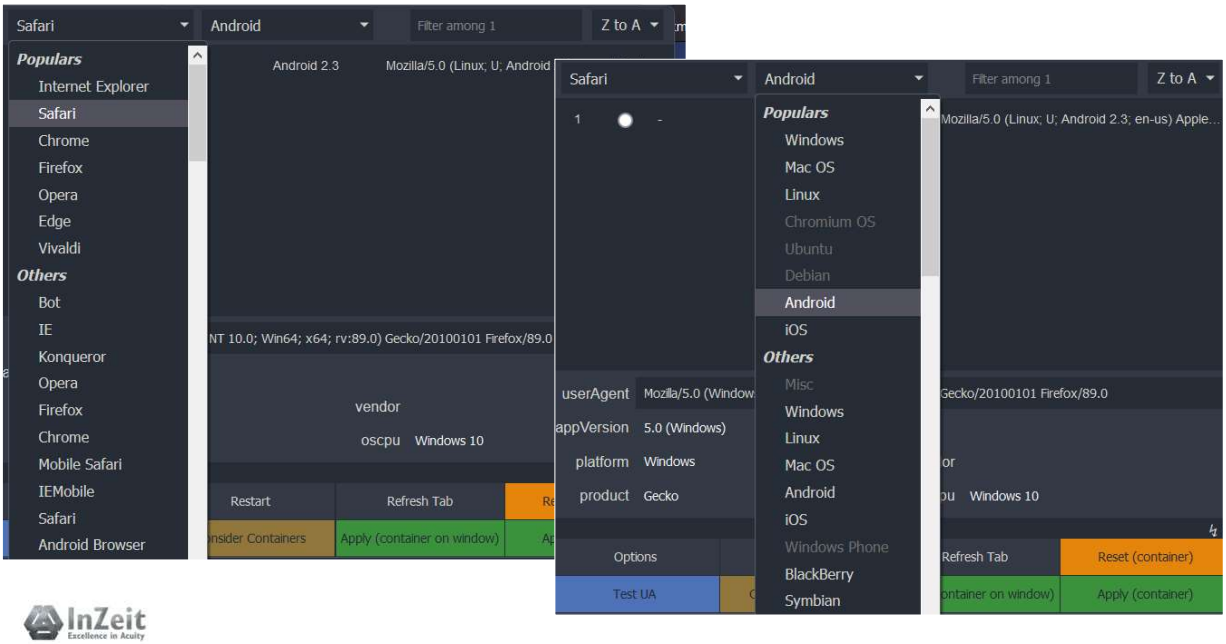
Browser fingerprint can also be faked:



InZeit Excellence in Acuity

63

Browser fingerprint can also be faked:



InZeit Excellence in Acuity

64

Your data may be spread across servers in multiple jurisdictions

Your data stored & processed somewhere else

gmail, outlook, yahoo mail, yandex mail , icloud, facebook

The Cloud

Outsourcing: Iaas, Paas, Saas

Relocated for business reasons (like load or electricity prices)

Even Cloud provider may not know where it is

Problems getting evidence:

- No control
- One of 1000s of requests
- Have to trust the provider's standards

InZeit Excellence in Acuity

65




IOT

Estimated 22 billion - 50 billion devices

All connected

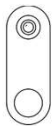


All generating & logging data

InZeit Excellence in Acuity

66






IOT

How secure are they?

Default passwords

Most lack built-in security

https://www.zdnet.com/article/your-insecure-internet-of-things-devices-are-putting-everyone-at-risk-of-attack/

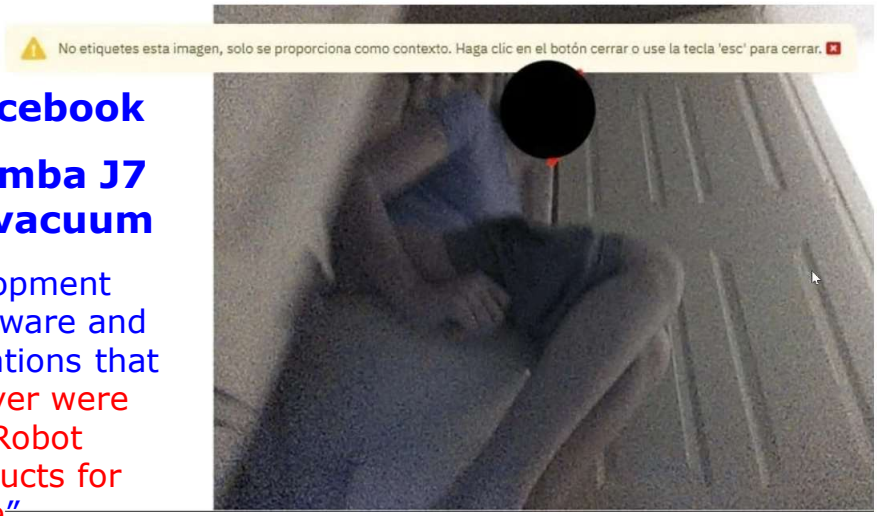
InZeit Excellence in Acuity

67

Posted to Facebook

iRobot's Roomba J7 series robot vacuum

"special development robots with hardware and software modifications that are not and never were present on iRobot consumer products for purchase"



https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/

InZeit Excellence in Acuity

68

Reuters 6 April 2023

Special Report: Tesla workers shared sensitive images recorded by customer cars

Naked man approaching car
Child knocked off bike
Doing laundry
'Really intimate things'
'certain sexual wellness items'
People walking by

(Banned in some places in China!)

https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/

Posted

iRobot
series

"specia
robots w
software
are not
prese
consum
p

https://www.techn intelligence-training-data-privacy/

InZeit Excellence in Acuity

69

InZeit Excellence in Acuity

70

No central control

All websites end with .onion

Can be used to access DarkNet

TOR
The Onion Router

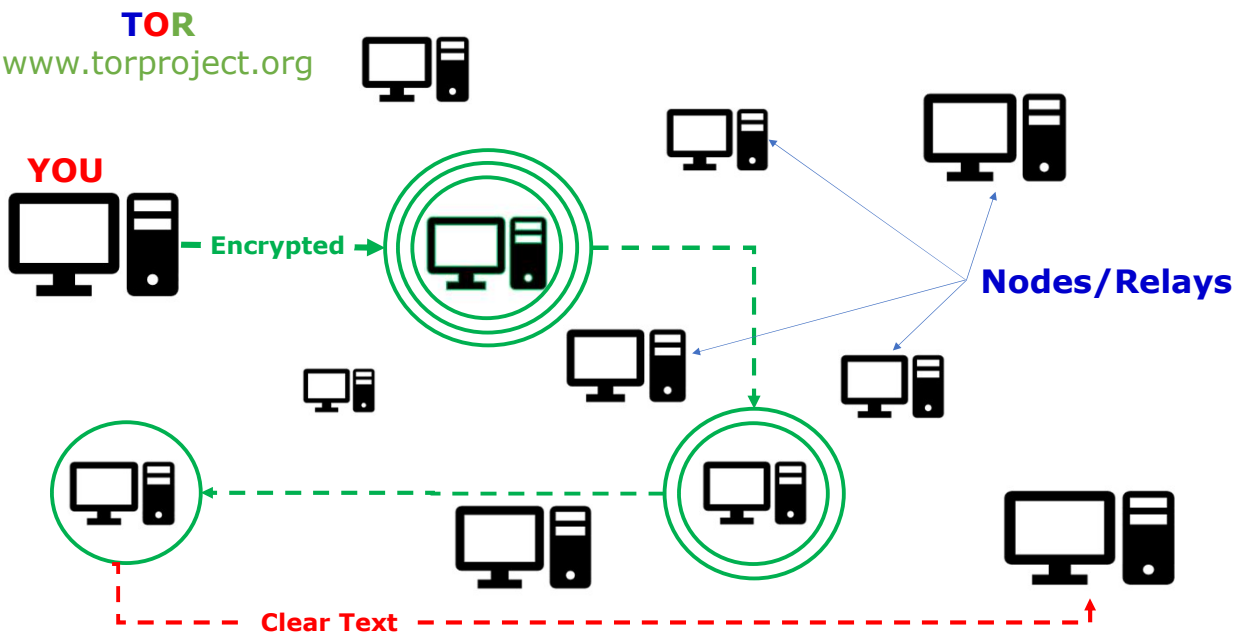
Peer to Peer Network (people volunteer part of their hard drive)

'Anonymising technology' (there are others)

InZeit Excellence in Acuity

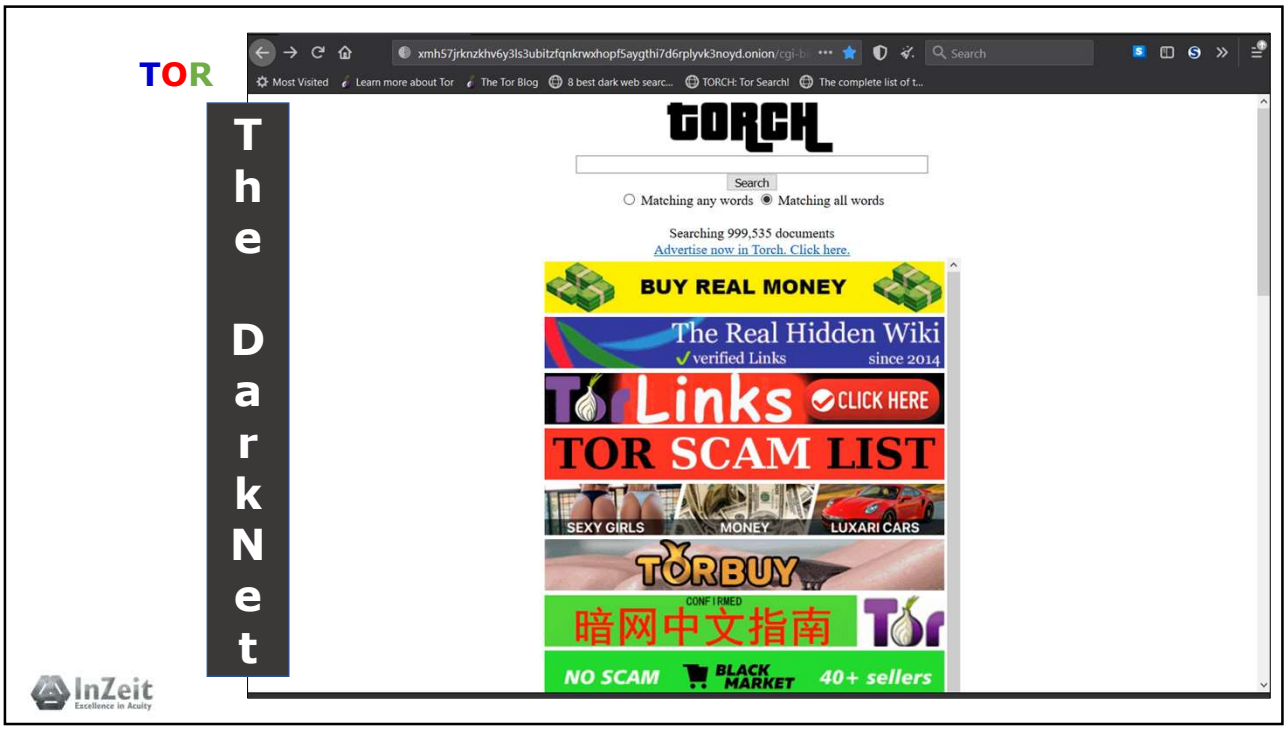
71

TOR
www.torproject.org



InZeit Excellence in Acuity

72


TOR
The DarkNet
xmh57jrknzkhv6y3ls3ubitzfqnkrwxhopf5aygthi7d6rplyvk3noyd.onion
TORCH
Search
Matching any words
Matching all words
Searching 999,535 documents
Advertise now in Torch. Click here.
BUY REAL MONEY
The Real Hidden Wiki
verified Links
since 2014
Links
CLICK HERE
TOR SCAM LIST
SEXY GIRLS
MONEY
LUXARI CARS
TORBUY
CONFIRMED
暗网中文指南
NO SCAM
BLACK MARKET
40+ sellers
InZeit
Excellence in Acuity

73


(Find your Darknet URL on ahmia.fi)
Onion.ws
Onion.ws is a darknet gateway or proxy. Simply replace .onion with .onion
url bar, press go and you will be redirected to that darknet site without the
configure any new software such as Tor and I2P.
Tor2web: Browse the Tor Onion Services
https://www.tor2web.org
WARNING: Tor2web only protects publishers, not readers. As a reader installing Tor Browser will give you much greater anonymity, confidentiality, and authentication than using Tor2web. Using Tor2web trades off security for convenience and usability.
available by volounteers Tor2web operators Example:
https://duskgytldkxiuqc6.onion.to/
This connects you with Tor2web, which then talks to the onion service via Tor and relays the response back to you.
WARNING: Tor2web only protects publishers, not readers. As a reader installing Tor Browser will give you much greater anonymity, confidentiality, and authentication than using Tor2web. Using Tor2web trades off security for convenience and usability.
Tor2web & Tor Onion Sites Resources
Below a set of useful resources, Tor Onion Services indexes, search engines and applications available on the internet trough Tor2web Proxies:
Ahmia Directory of Tor Onion sites
Ahmia Search Engine for Tor Onion site
Onion City: Google+Tor2web Powered search engine for Tor Onion Site
Accessing Dark Net
using normal browser
.onion.ws
.onion.to
InZeit
Excellence in Acuity

74

CENTRO DE ESTUDOS JUDICIÁRIOS

Cyber Pandemic: The Internet unmasked

ERA
Academy of European Law

Steven David Brown

Lisbon
16-17 May 2023

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

InZeit
Excellence in Acuity

© All Rights Reserved

75

Resources and further reading

(NB Links are active so you should be able to click on them)

Definition
https://www.britannica.com/technology/Internet
https://www.britannica.com/topic/World-Wide-Web

Data Estimation
https://www.statista.com/statistics/617136/digital-population-worldwide/
https://www.worldwidewebsize.com/
https://www.the-next-tech.com/blockchain-technology/how-much-data-is-produced-every-day-2019/

Protocols
Gross,M. (updated) 12 common network protocols and their functions explained
https://www.techtarget.com/searchnetworking/feature/12-common-network-protocols-and-their-functions-explained

Wayback Machine (for old website versions)
http://web.archive.org

Find your IP address
www.ipchicken.com
http://www.privateinternetaccess.com/pages/whats-my-ip

76

Bitcoin Transactions
Greenberg, A. (2022) *Tracers in the Dark*, Doubleday Publishing

Changes in cybercrime trends during Pandemic:
https://rm.coe.int/presentation-fernando-miro-llinares-the-impact-of-covid-19-on-cybercri/1680a1e42f
https://aag-it.com/the-latest-cyber-crime-statistics/
https://www.itu.int/itu-d/reports/statistics/2021/11/15/internet-use/

UK Information Commissioner's Report 2016
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/670219/IOCCO_annual_report_2016_2.PDF p74

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

VPN bans
O'Driscoll,A. (2022) *Where are VPNs legal and where are they banned?*
https://www.comparitech.com/vpn/where-are-vpns-legal-banned/

WebRTC leaks
Vigderman,A. Turner,G. (2021) *WebRTC Leaks: A Complete Guide* https://www.security.org/vpn/webrtc-leak/

77

Your Browser Logs
(Enter in address bar of browser)

Google Chrome:
chrome://history/
(try this software utility:
https://www.nirsoft.net/utils/chrome_cache_view.html)

Microsoft Edge:
edge://history/all
edge://settings/siteData

Mozilla Firefox:
about:cache
about:cache?storage=memory

Ricin Dark Net case
Press Association (2015) *Breaking Bad fan jailed for trying to buy ricin* https://www.theguardian.com/uk-news/2015/sep/18/breaking-bad-fan-jailed-over-ricin-plot
BBC (2016) *Mohammed Ali: Breaking Bad ricin plotter's appeal turned down* https://www.bbc.com/news/uk-england-merseyside-36483593

Browser Fingerprinting
https://webkay.robinlinus.com/
https://coveryourtracks.eff.org/

78

Data Brokers
https://www.databroker.global/community/people
Rafter,D. (2021) *How data brokers find and sell your personal info* https://us.norton.com/internetsecurity-privacy-how-data-brokers-find-and-sell-your-personal-info.html

Internet of Things
Palmer,D. (2021) *Your insecure Internet of Things devices are putting everyone at risk of attack*
https://www.zdnet.com/article/your-insecure-internet-of-things-devices-are-putting-everyone-at-risk-of-attack/
Guo,E. (2022*) A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook?*
https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/
Stecklow, S. Cunningham, W. Jin, H. (2023) *Special Report: Tesla workers shared sensitive images recorded by customer cars*
https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/

Meta-Search Engines
- Dogpile.com
- Metacrawler.com
- Wolframalpha.com
- Metager.com
- Startpage.com

At your own risk:
- Torproject.prg
- Tor2web.org
- Onion.ws

NRD Cyber Security

Internet searches and computer forensics in criminal cases: using open-source intelligence to gather evidence online

Rūta Jašinskienė
Information analysis expert, NRD Cyber Security

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

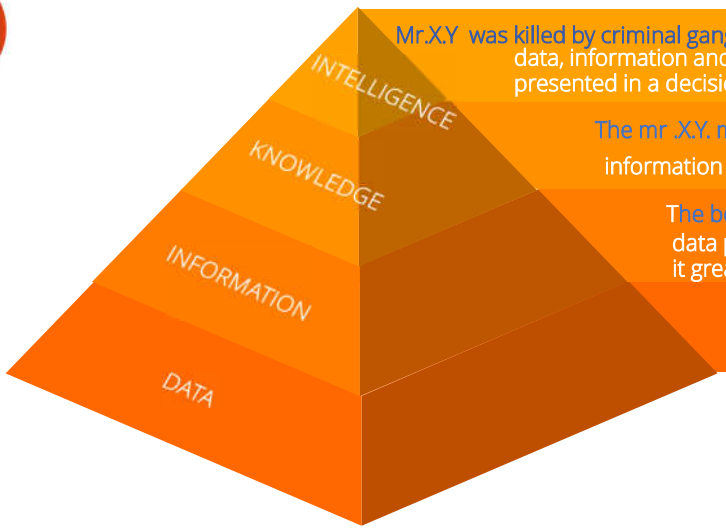
NRD Cyber Security

INTRODUCTION

- OSINT and SOCMINT: is this a silver bullet for evidence search?
- Search engines: how it works?
- Alternative search engines to explore the hidden Internet
- Main obstacles getting data from online sources or "How to think as a hacker?"
- Visualization of forensics findings - must or nice to do?

NRD Cyber Security

KNOWLEDGE PYRAMID



Mr.X.Y was killed by criminal gangs due to his activity promoting the strict regulation on drugs...
data, information and knowledge that have been evaluated, analysed and presented in a decision-making format for action-oriented purposes

The mr .X.Y. member of Parliament was robbed and murdered
information that has been given an interpretation and understanding

The body was found on a street in Kaunas last Friday
data put in context and empowered with meaning, which gives it greater relevance and purpose

41 24.2028, 210.4418 25.03.2022
raw and uninterpreted observations and measurements

NRD Cyber Security

INTELLIGENCE

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

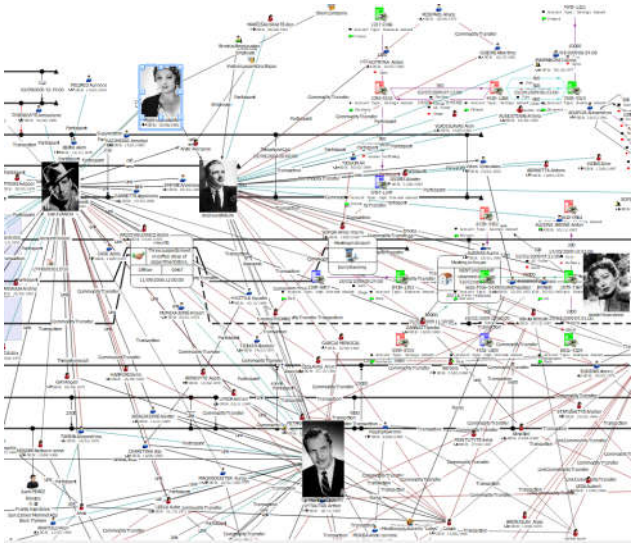
„The mind is a wonderful instrument for observing the world and formulating hypotheses, but it requires careful attention and training to function accurately.„
William James

NRD Cyber Security

OPEN-SOURCE INTELLIGENCE (OSINT)

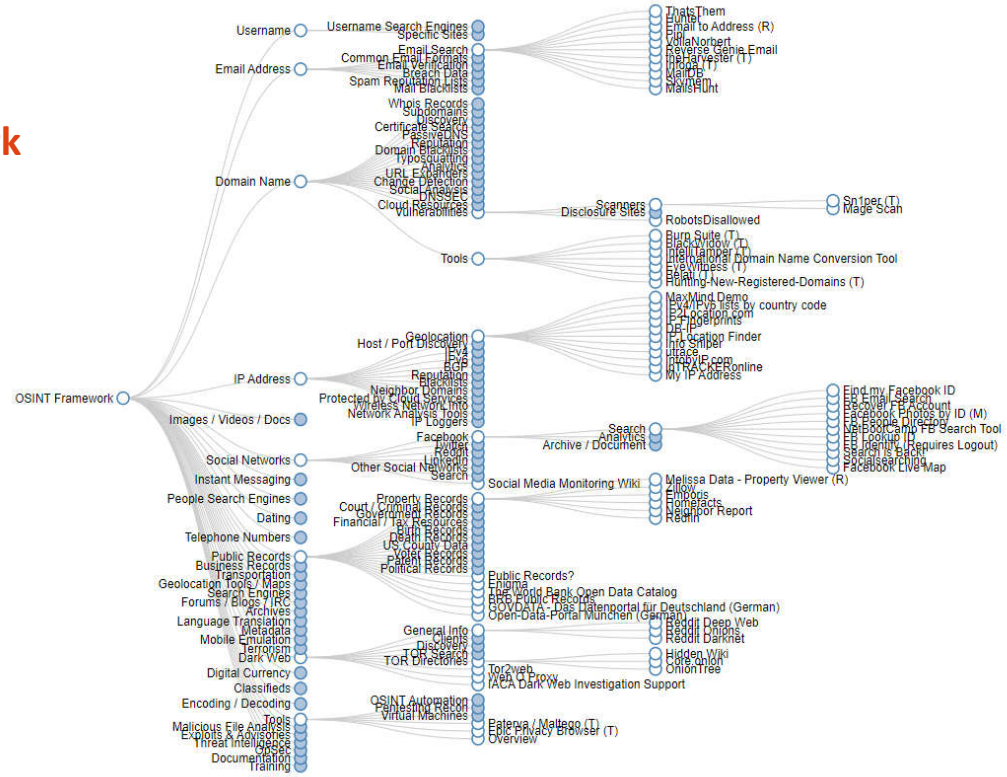
OSINT - intelligence derived from publicly available sources of information.

This information is collected, processed, analyzed and disseminated to address a specific intelligence requirement.



NRD Cyber Security

OSINT Framework

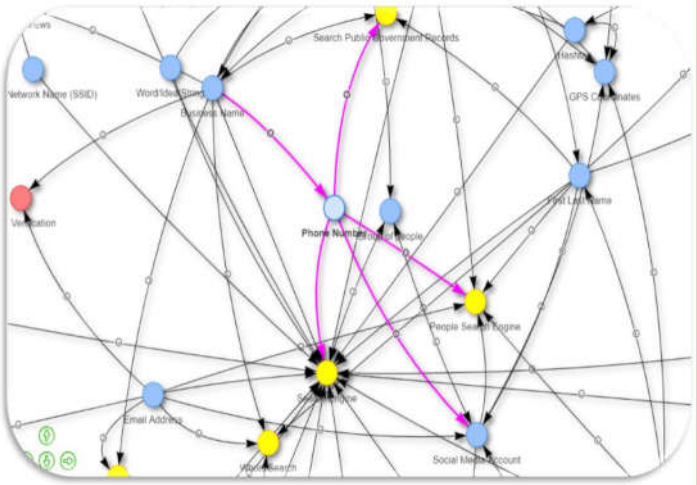


https://osintframework.co

NRD Cyber Security

YOGA

Your OSINT Graphical Analyzer - a project to help people understand different courses of action to take based upon the data they have.

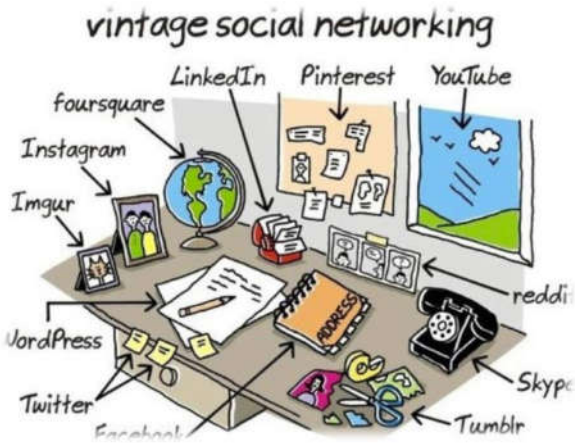


https://yoga.osint.ninja/

NRD Cyber Security

What OSINT is Not?

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



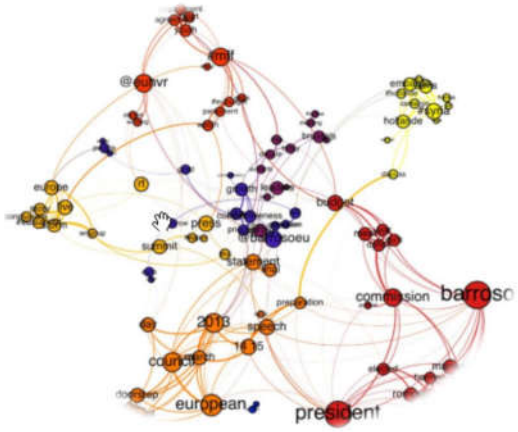
NRD Cyber Security

Social Media Intelligence (SOCMINT)

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

Such information can be public or private.

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



NRD Cyber Security

Types of social media platforms

- Social networking (e.g. Facebook)
- Professional (e.g. LinkedIn)
- Photo sharing (e.g. Instagram, Flickr)
- Video sharing (e.g. YouTube)
- Social bookmarking (e.g. Pinterest)
- Blogging (e.g. Blogger)
- Microblogging (e.g. Twitter, Tumblr)
- Forums (e.g. Reddit)
- Q&A sites (e.g. Quora)
- Review websites (e.g. Yelp)

NRD Cyber Security

OSINT benefits

- Global coverage, scope
- Provides context
- Realtime utility
- Strategic and operational
- Inexpensive
- Shareable
- Legally admissible

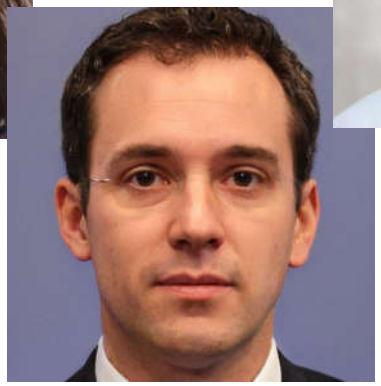
NRD Cyber Security

Why OSINT does NOT a silver bullet?

- Overwhelming
- Reliability
- Validity
- Inadequate training and investment

NRD Cyber Security

Which of these people do not exist?



NRD Cyber Security

Is it real?

NRD Cyber Security

Source reliability and information validity

anna holligan
@annaholligan

Incorrect assumptions and articles about Noa's dead ever reached the Vatican #NoaPothoven

> **Pope Francis** @Pontifex
> Euthanasia and assisted suicide are a defeat for all. We are called never abandon those who are suffering, never giving up but caring and lovin restore hope.

2:30 AM · Jun 6, 2019

3 10 Copy link to Tweet

Lisa Westerveld
@Lisawesterveld

There is a lot of misinformation in international press about the tragic death of Noa. Her friends and family want people to know that she did not die of euthanasia. I ask all media to respect the privacy of Noa's family and let them grieve in peace.

euronews.

Noa Pothoven: Raped girl, 17, dies by legal euthanasia in the Netherlands

By Lauren Chadwick 04/06/2019

INDEPENDENT

Teenager who was sexually assaulted multiple times ends her own life through legal euthanasia

Noa Pothoven had been repeatedly re-admitted to hospital to try and treat her post traumatic stress disorder, depression and anorexia

HEARTBREAKING

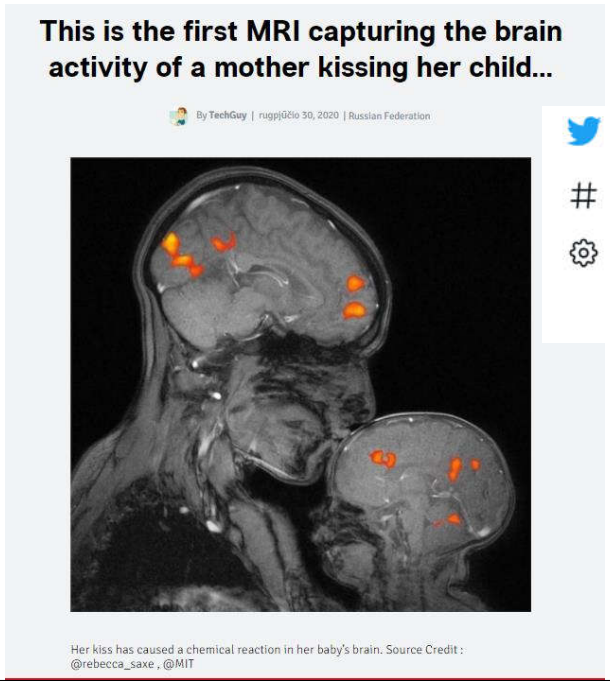
17-Year-Old Dutch Girl Who Was Raped as a Child Is Legally Euthanized

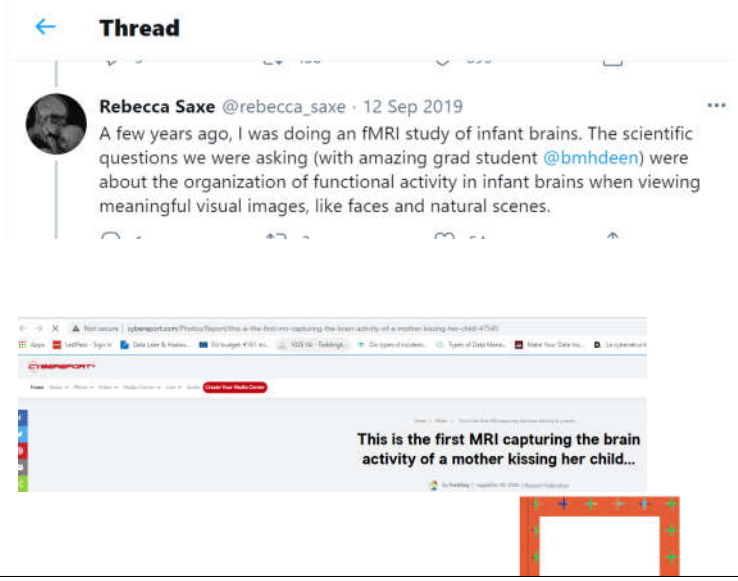
Daily Mail MORE STORIES

Dutch girl, 17, who was sexually abused at 11 and raped as a 14-year-old is legally euthanised at her home by 'end-of-life' clinic because she felt her life was unbearable due to depression

NRD Cyber Security

Source reliability and information validity

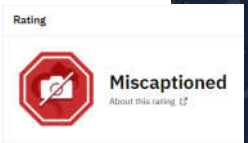




NRD Cyber Security

Fake or real

https://www.snopes.com/
https://www.factcheck.org/
https://www.politifact.com/



NRD Cyber Security

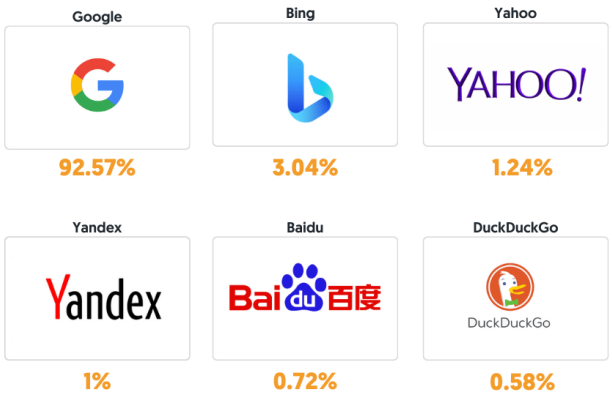
Search Engines

- How do search engines work?
  - Data and metadata
  - Robots
  - Indexing
  - Databases
  - Filtering and ranking
  - Search algorithms

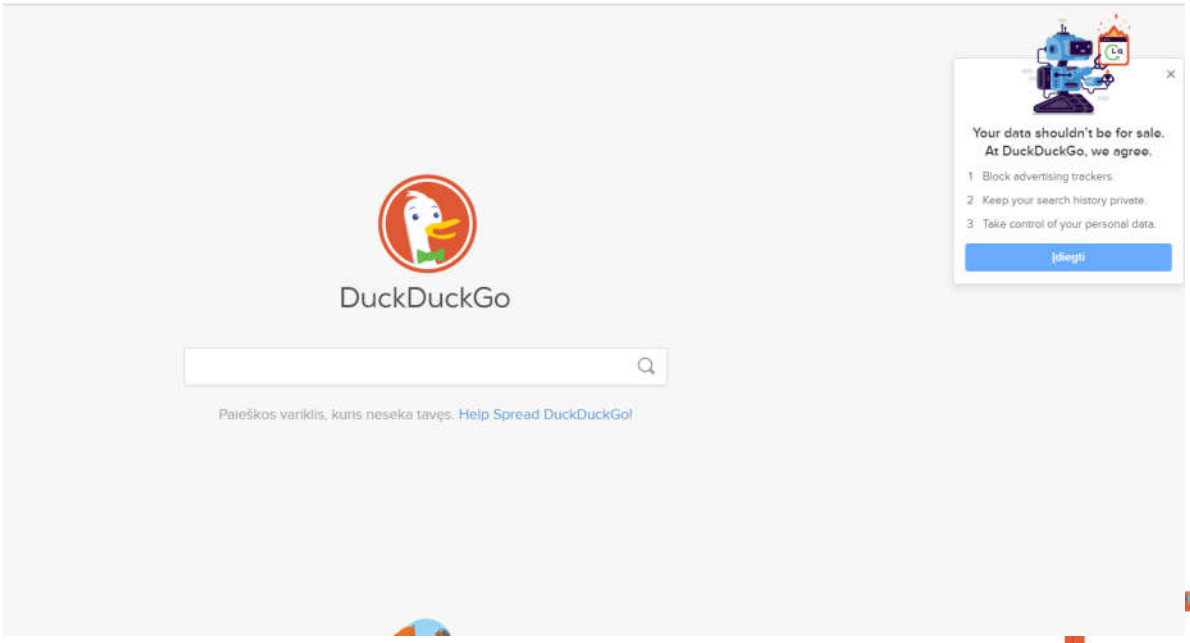
NRD Cyber Security

Popular General Search Engines

Market share 2023



NRD Cyber Security



NRD Cyber Security

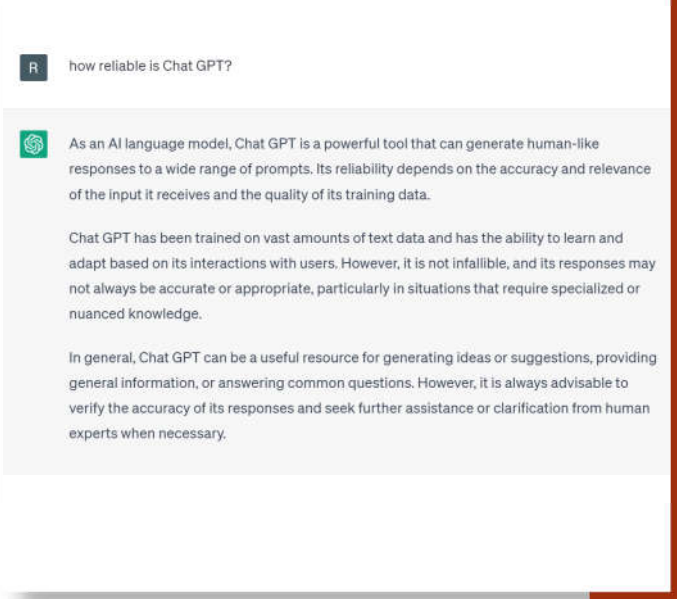
Specialized Search Engines and Websites

- carrot2.org
- archive.org
- archive.eu
- cachedview.com
- 2lingual.com
- gofindwho.com
- opencorporates.com
- findagrave.com
- platesmania.com
- millionshort.com
- ahmia.fi
- darksearch.io
- Baidu browser
- searchftps.com

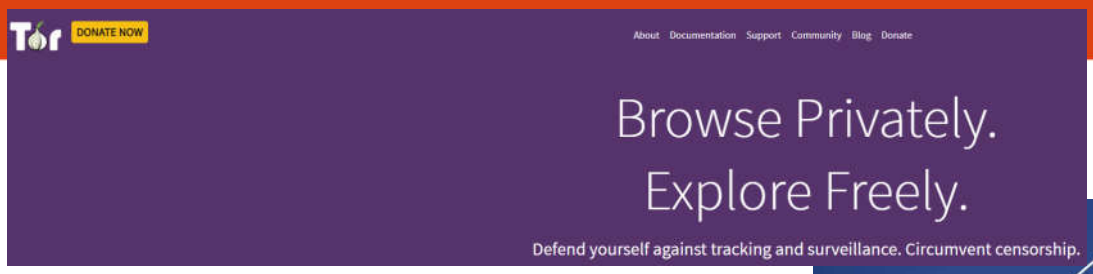
NRD Cyber Security

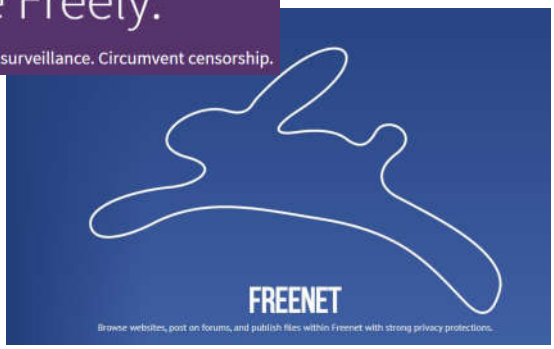
Chat GBT

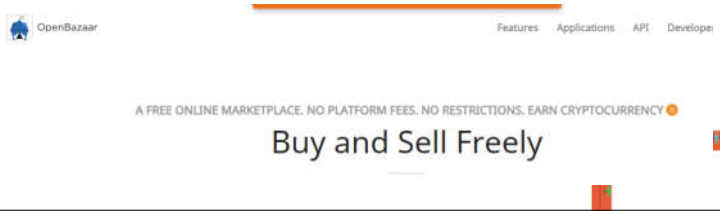
- How reliable is it?
- How easy it is to deceive?



NRD Cyber Security







NRD Cyber Security

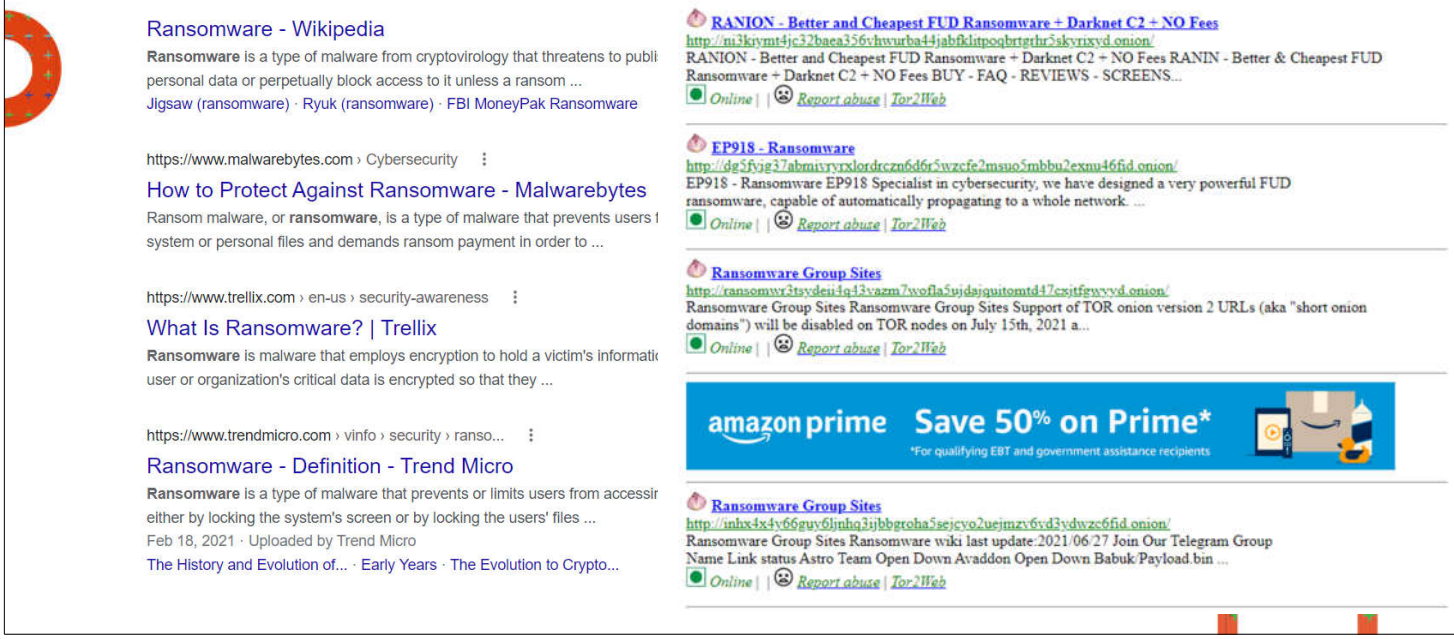
Tor Network

- Onion Services are the most anonymous web servers that exist today
- **IP addresses are not used** for Onion Services – no possibility to scan every IP address on the planet, like we can do for the WWW
- You need to know the URL of the website you are going to visit
  - e.g. http://**cannazon**ceujdye3.onion/
  - e.g. http://**garden**2b7zwrjskh2y3f4pkscgg2waogjp2ilax2mvikjlzmamylznad.onion

- Over 2 million users access the Tor platform daily.
- Only 45% of websites on the dark web host illicit activities.
- Russia has the biggest share of daily Tor users.
- Bitcoin transactions on the dark web were on track to reach $1 billion in 2019.

NRD Cyber Security

Ordinary browsers vs Tor browser



NRD Cyber Security

Boolean Operators

- The three operators common to most search engines are called Boolean operators in honour of the mathematician George Boole
- Boolean operators – AND, OR, NOT – are used as conjunctions to combine or exclude words in a search query. It can be used in almost every search engine, database, or online catalogue.
- Improve the quality and accuracy of your search results
- Reduce the time spent searching, thus allowing more time for reading

NRD Cyber Security

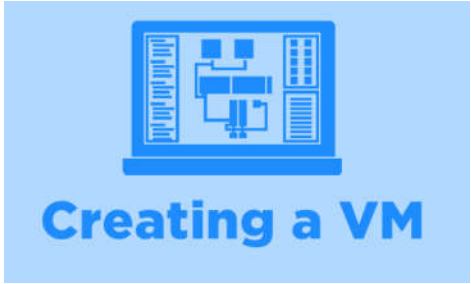
Google Operators

- inurl: limit your search to page URLs
- allinurl: search for multiple keywords and phrases in a URL
- intext: searches within the text of a page only
- allintext: searches for multiple keywords and phrases within the text of a page
- before: / after: narrow your results to a specific date range
- wild card (*) look for spelling variations, alternate word endings etc
- cache: operator returns the most recent, cached version of a web page
- related: returns websites Google considers similar to your target

NRD Cyber Security

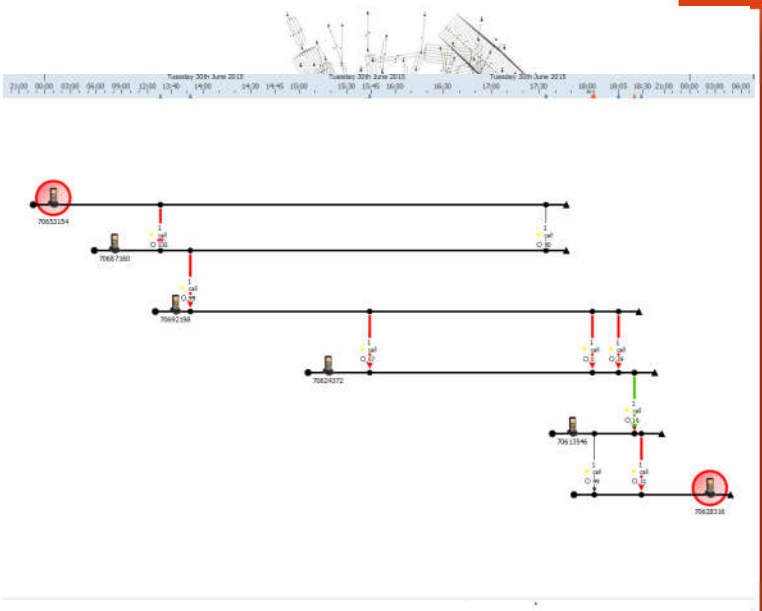
Do not leave a footprint behind….

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



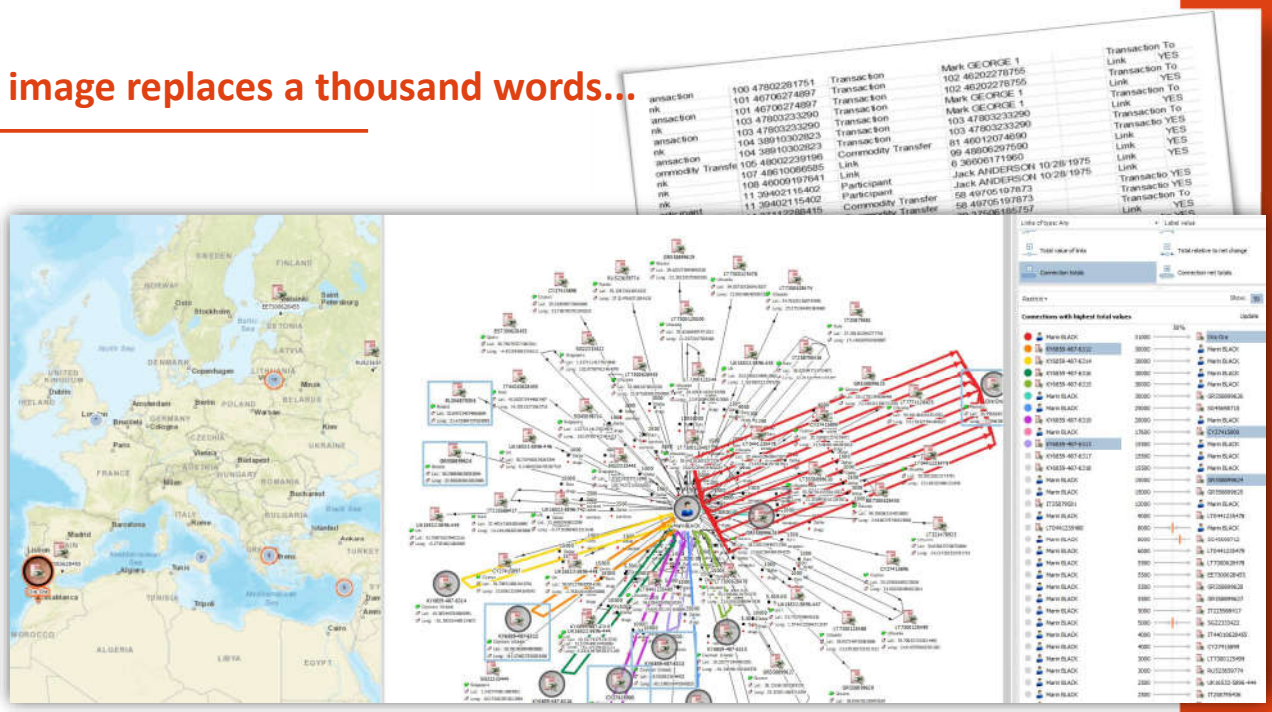
NRD Cyber Security

Perception and visual analysis



NRD Cyber Security

One image replaces a thousand words...



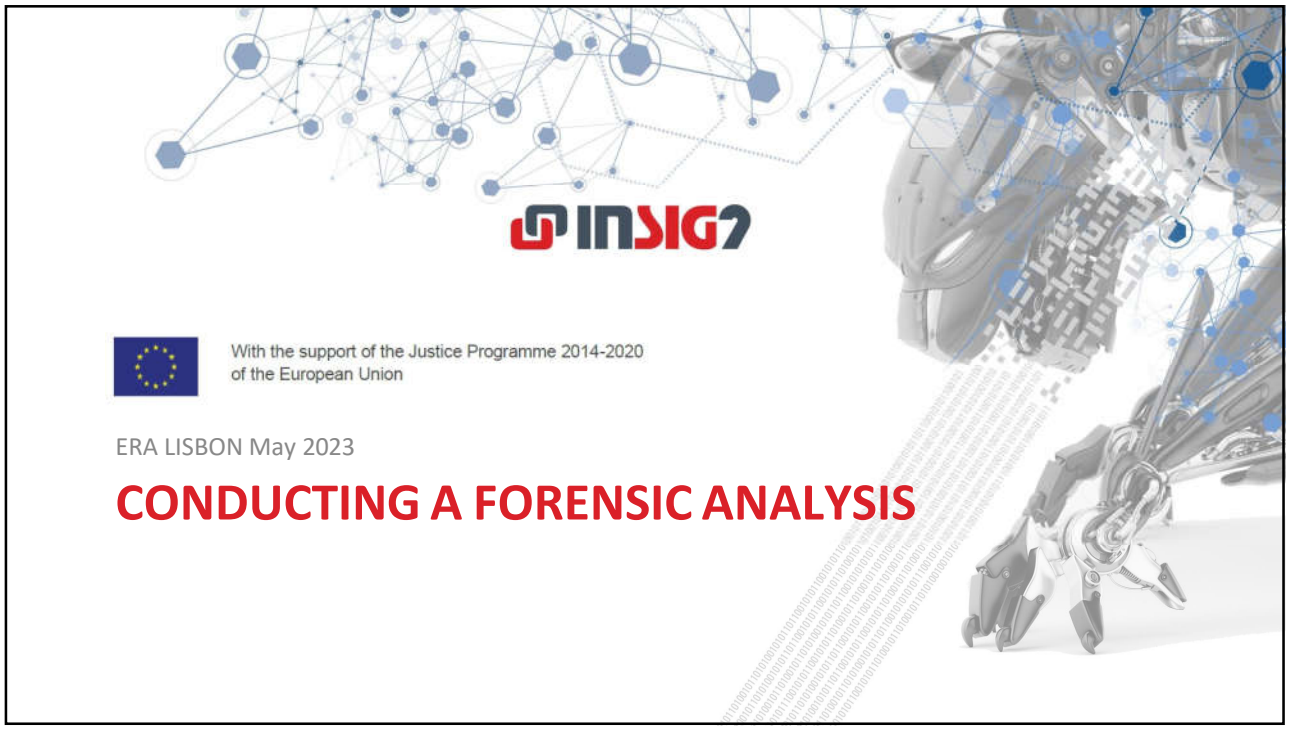
NRD Cyber Security

Thank you!!!!

Rūta JAŠINSKIENĖ

rj@nrdcs.lt

www.linkedin.com/in/ruta-jasinskiene


INSIG2
With the support of the Justice Programme 2014-2020
of the European Union
ERA LISBON May 2023
CONDUCTING A FORENSIC ANALYSIS

1


Savina Gruičić
OXYGEN FORENSIC EXPERT
CYBERCRIME FORENSICS TRAINING CENTER
FER
TVZ
EnCase Certified Examiner
EnCE
Guidance Software
EC-Council
C|HFI
CERTIFIED
cellebrite certified
CCME
mobile examiner
INSIG2

2

About INsig2

- Established in 2004, HQ in Zagreb
- 2018 INsig2 business expansion in Indonesia
- 70+ highly educated employees
- Educational & Training centre

Education & Training Centre in Zagreb, Croatia
- Accommodates up to 15 people per classroom
- Equipment, forensic tools & materials provided

3

INsig2

- Two business units
- „One-stop-shop" in the field of Digital Forensics

We teach what we do!

4

E-learning platform

- Customized courses
- For legal entities, law enforcement, and private sectors
- Courses on deeper aspects of digital forensics and forensic value of the evidence while collecting, processing, and presenting digital evidence in criminal and administrative proceedings
- Website: https://insig2-and-zyberglobal.learnworlds.com/

5

Triage of the crime scene

INSIG2

6

Uncovering evidence tracks

- It is important to follow the SOP and to ensure data and evidence integrity
- Evidence examination
  - Purpose of investigation, points to prove?
  - What digital evidence do you expect to find?
  - Home or office?
  - Administrator?
  - Is there a network?
  - Cloud storage utilized?
  - Encryption?

INSIG2

7

Uncovering evidence tracks

- Once you have the answers to the questions from the previous slide you have to look at the evidence collected
  - Data at rest
    - HDD, SSD, USB, CD…
  - Volatile data (from RAM)
    - Live acquisition
  - Mobile devices data
  - Network data
    - Network packet or logs
  - Data in the Cloud
    - Credentials, web site, cloud backup

INSIG2

8

Uncovering evidence tracks

- Next step is to choose you weapon aka Digital Forensic Tool
  - What is available?
  - What is the best tool for the case and evidence type?
    - Computer or mobile
    - Commercial or free/open source
  - With what tool are you most comfortable?
  - Special tool required?
    - Cloud acquisition, analytics, chip off, python
  - Knowledge required for the case?
    - Malware, networking, RAM analysis, linux, scripting

9

Why care about live data?

- Computers regularly left on
- Corporate needs
- Encryption
- Covert requirements
- Because we miss loads of data when we pull the plug

10

Digital forensics

11

Preparation

Intelligence assessment	Purpose of investigation, points to prove?
	What digital evidence do you expect to find?
	Home or office?
	Administrator?
	Is there a network?
	Cloud storage utilized?
	Encryption?

12

Preparation

Proper Planning Prevents Poor Performance

13

Identification

Has there been an incident at all?

Often what seems like an attack could just be a system malfunction or loose wire

What kind of incident?

Interview the suspect

Is this your computer / have access to it?
What is the user account name & password?
Who else uses the computer?
Do they have separate accounts?
Encryption
Cloud Storage

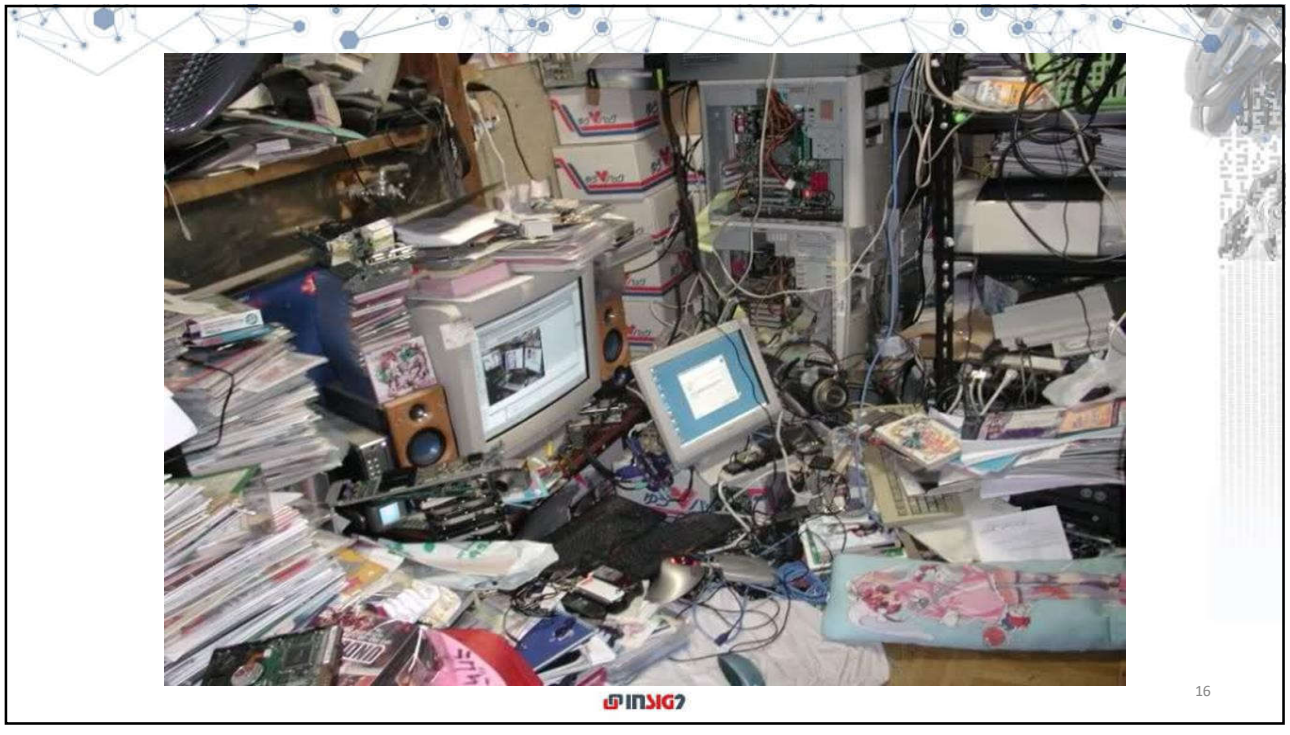
Confiscate or analyze on scene?

Identify items and locations of potential evidence

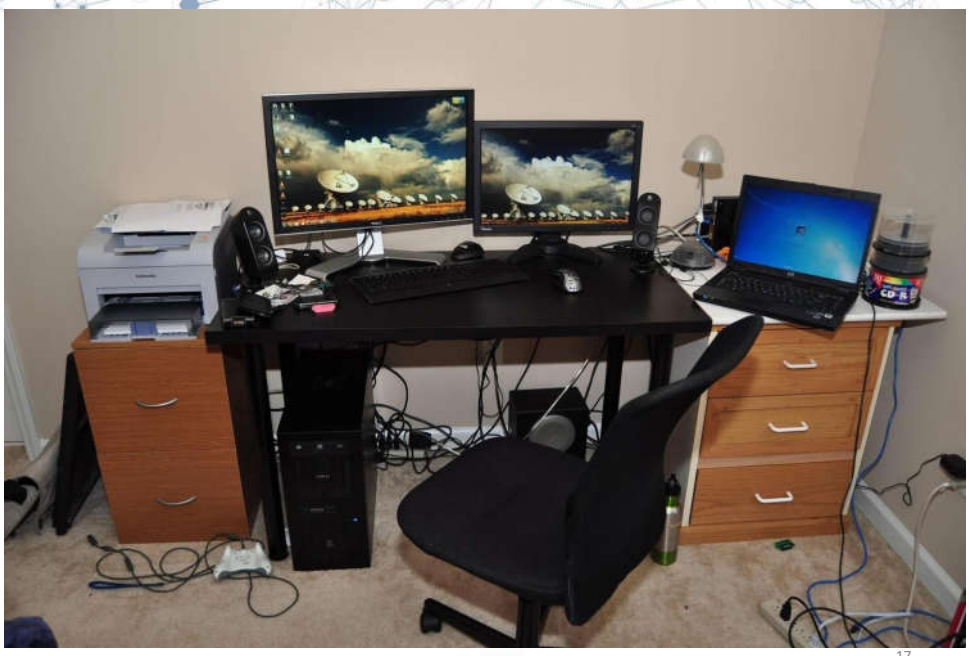
HDD, RAM, registry, browser, attached devices, mail accounts, servers, cloud…

14

15



16



17

Seizure

- On site processing techniques
  - Logical acquisition
  - Physical acquisition
  - Triage / Preview
- Seizure vs. Triage
  - Volume of evidence to be examined
  - Technical limitations
  - Potential for destructive data processes set up by suspect

18

When to triage?

- Live scene
- Corporate investigations
- Covert operations
- Lab

19

Live scene

- Dawn raids
  - Preparation!
    - Suspect is using computer at the moment
      - ON and UNLOCKED
- Triage:
  - Photograph!
  - Date and time!
  - Encryption?
  - Malicious processes?

20

Triage - general procedure

Rule #1

- **If the computer is off, leave it off**

Rule #2

- **If the computer is turned on, *it depends*…**

21

Triage - general procedure

- Photograph first!
  - *„A picture is worth a thousand words"*
- Document
  - What is it?
    - Make, Model, Serial
  - What state is it in?
    - Off / On / Disconnected / Damage

22

Triage - general procedure

- Client workstation
  - Destructive process running or system is locked:
    - Pull the plug – from the back of the computer (UPS)
    - Observe time from authoritative source
    - Document, document, document!
    - NOTE: If the client hosts network services, especially databases, shutdown normally
  - No destructive process observed:
    - Observe time from authoritative source
    - Document, document, document!
    - RAM dump
    - Perform a normal shutdown

Triage – general procedure

- If possible, save the encryption keys or create a logical image of the device in decrypted form
- DOCUMENT!

Triage - general procedure

- If computer is ON and unlocked, do a RAM dump!
  - A lot of information can be found inside RAM
    - Sometimes RAM is all you have
  - Passwords, encryption keys, pictures, recent files, network connections, processes, malware…

25

Gathering digital evidence from live memory

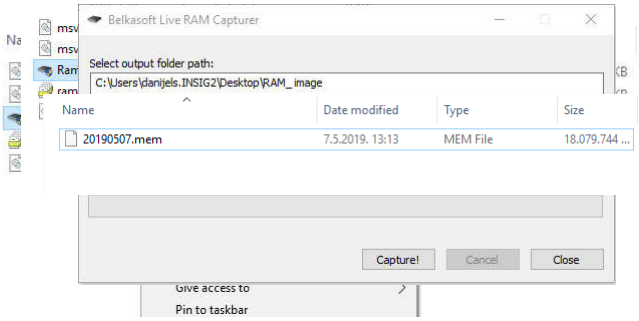
26

RAM imaging & analysis

- Which tool to use?
  - Most reliable
  - Least memory consumption
  - Smallest footprint
    - FTK Imager – 64MB
    - Dumpit – 615 KB
    - Belkasoft – 58 KB
- Any memory acquisition tool will always dump the entire memory of the system
- All generated files will be the same size

27

Creating RAM dump using Belkasoft



28

Live Scene

- Before you start always record the date and time:
  - On your device
  - From the target machine
- An unrecorded time offset could mess up your evidence

29

Scripts in digital forensic examinations

30

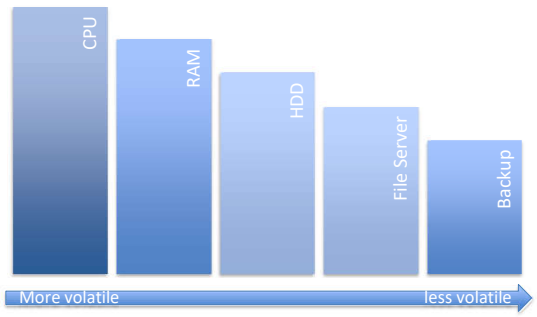
Date and time

```
Command Prompt

C:\Users>time /T
13:33

C:\Users>date /T
uto 07.05.2019.

C:\Users>echo %time%
13:33:35,41

C:\Users>
```

31

Volatile Data

- What is volatile data?
  - How often does the data change?
    - 1s, 1m, 1h, 1day, 1 week, 1 month, 1 year!?



The closer the data is to the CPU it will be more volatile

32

Volatile Data

- Data lost when we turn computer off:
  - Passwords
  - Encryption keys
  - Active network connections
  - Opened programs and status windows
  - Notifications
  - Running processes
  - Malware – some will only live in memory
  - …

33

Volatile Data

- If we want to extract volatile data from the computer whilst it's running
- We can run commands from command shell
  - `netstat -na` – network connections
  - `ipconfig /all` – network adapters
  - `systeminfo` - system info
  - `tasklist` – list of running tasks
  - Etc…

34

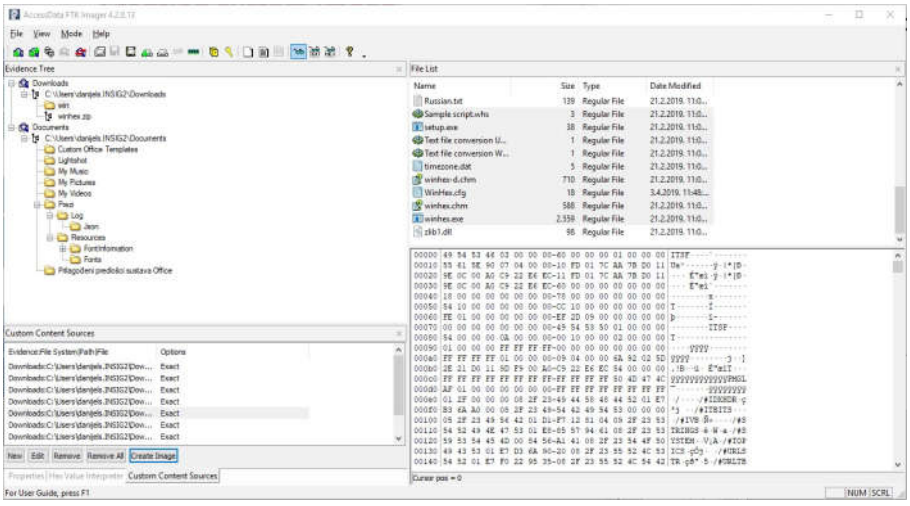
Using batch scripts in forensic purposes

- Automating the forensic process using self-made scripts

```
REM running from c:\temp folder
@echo off

set /p drive=What drive would you like to search?
REM c:\
set /p name=What file name do you want?
REM with .txt extension

date /T >> %name%
time /T >> %name%

REM position where tchunt.exe is saved
cd C:\Users\savinag\Desktop\incident response\Encryption detection
tchunt -d %drive%

REM position where Belkasoft RAM capturer is saved
cd "C:\Users\savinag\Desktop\incident response\Belkasoft RAM capturer\x64"
RamCapture64.exe

REM path to your memdump file
cd c:\temp\tools
Strings64.exe "C:\Users\savinag\Desktop\incident response\Belkasoft RAM capturer\x64\20190301.mem" | findstr /i http >> %name%

netstat -na >> %name%
ipconfig /all >> %name%
systeminfo >> %name%
hostname >> %name%
tasklist >> %name%

pause
```

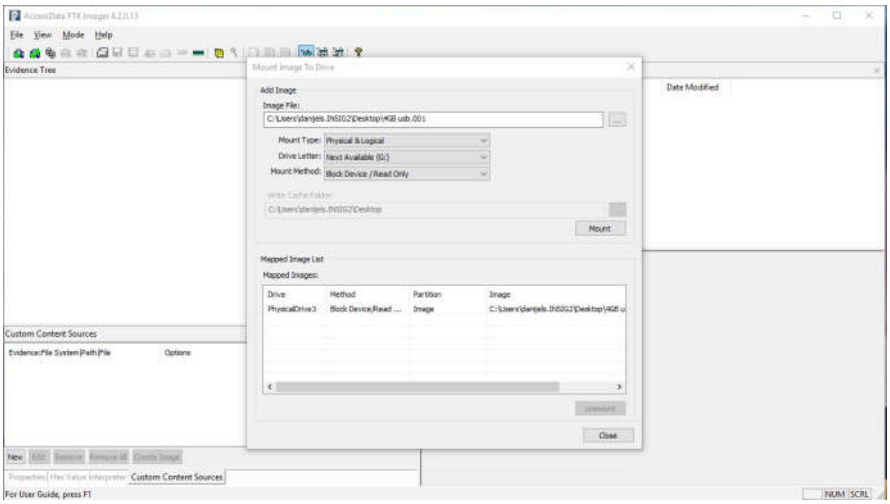
35

FTK Imager
Creating custom image



36

FTK Imager
Image mounting and previewing

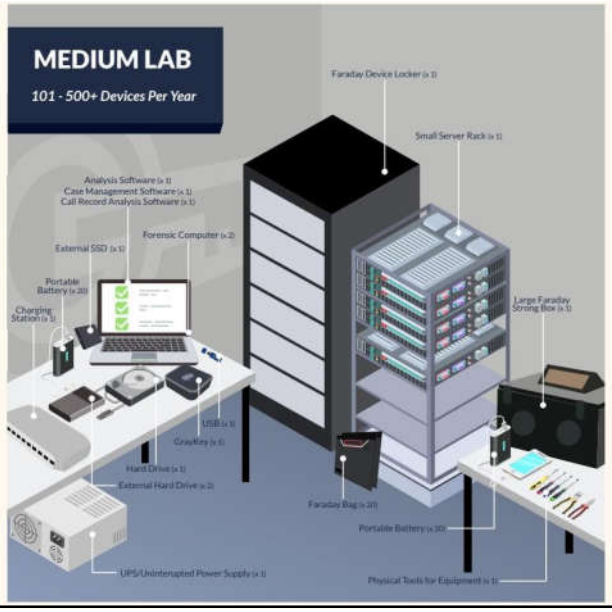


37

Labs

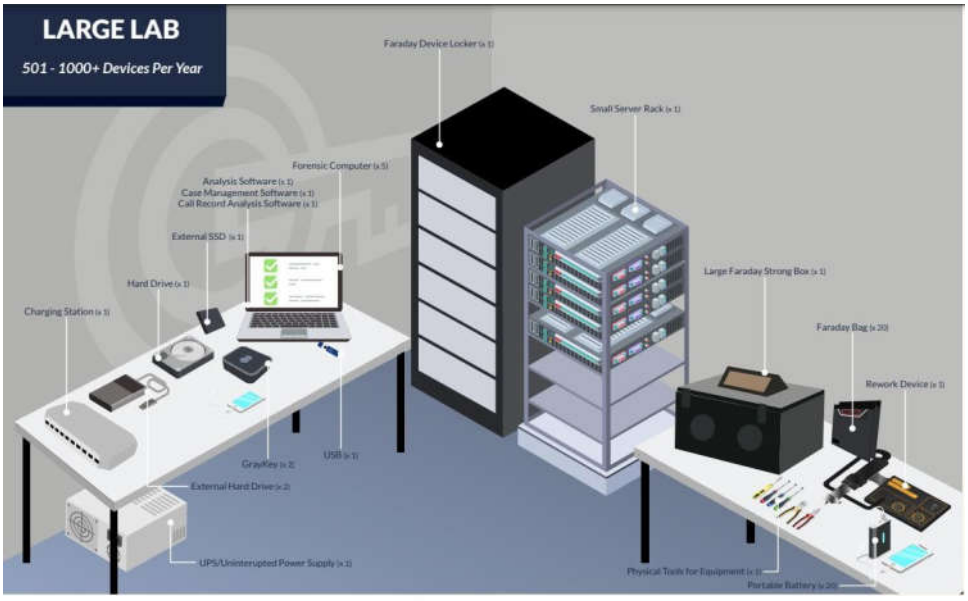
38

Building a (mobile) forensics lab



39

Building a (mobile) forensics lab



40

Computer and mobile forensics

41

Digital crime

42

Digital evidence

Information in digital form that confirms or excludes a crime has been committed

43

44

Collecting Devices and Storage Media at the Scene

- Every successful examination starts with a successful physical seizure of the devices that hold the data and/or the repository (such as cloud storage)
- So many things to think about

45

What can you find on computers?

- Installed software
- Emails
- Multimedia
- Documents
- Web history
- Databases
- Settings and configuration files
- …

46

What can you find on mobile devices?

- Password
- Caller Identification information
- Contacts
- Serial numbers (digital and non digital)
- SMS
- E-mail
- Voice mail
- Documents
- Web browser artifacts
- Calendar
- Hand writing information
- APPLICATIONS and their data

47

What is mobile device digital forensics and why is it important?

- Information sources
  - Participants and witnesses
  - Third party sources (CSP/CDR)
  - Physical evidence from scene
- Fundamental questions:
  - Who?
  - What?
  - When?
  - Where?
  - How?
  - Why?

48

Need for mobile forensics

- With the mass adoption of mobile devices, digital evidence is more prevalent in criminal cases than ever before
- By the year 2024, 4.5 billion people will be using smartphones
- Few cases that don't involve mobile devices
  - this presents challenges for law enforcement when it comes to investigating crimes
- Having a mobile device forensics lab that can properly process seized phones is critical (maintaining Chain of Custody)
  - because when you can access mobile devices, you can solve crimes more quickly

49

What is mobile device digital forensics and why is it important?

- Subcategory of digital forensics
  - process of recovering data from mobile devices
- This data can be used to track down a suspect, understand a crime, or gain insights into a person's life
- Here are a few reasons why mobile device digital forensics is essential to investigations today:
  - Mobile devices contain a wealth of evidence that can be used in any type of investigation
  - Often the only source of evidence
  - Can be used to track down a suspect who may be hiding their tracks on a traditional computer system
  - Can help investigators understand how a crime was committed and who was responsible

50

Terminology

- **Device** - target mobile phone, tablet, or other technology from which we are acquiring data
- **Collection and acquisition** - can imply the seizure of a device or the process of obtaining an image.
  - "seizure" for the process of physically obtaining a device from a scene
  - "collection" and "acquisition" for the process of obtaining a forensic image to include associated processes such as network isolation
- **Image** - forensic image
- **Imaging** - process of creating a forensic image
- **Exploit** -
  - Exploit (noun): vulnerability which we will use to gain access (or more access) to a device
  - Exploit (verb): action taken when we "exploit a device" – use a vulnerability to take action against the device such as gaining necessary access in order to image a device

51

What tools and techniques do you need for mobile device digital forensics?

- **Tools**:
  - **Network Isolation Hardware**: Isolate devices from radio frequency signals to maintain evidence integrity
  - **Portable Batteries and Device Cables**: Ensure on-scene officers have the equipment and accessories they need to properly secure seized devices
  - **Computer System**: Run digital forensics imaging and analysis software to process digital evidence
  - ***GrayKey/Cellebrite Premium/Cellebrite CAS:** Access and extract encrypted or inaccessible data from mobile devices
  - **Data Analysis Software**: Import extracted mobile device data into analysis software to begin examining digital evidence
  - **Device Storage:** Safely store mobile device extractions and simplify chain of custody and data integrity
  - **External Data/Evidence Storage**: Relieve storage space from computer systems and store evidence long term (Data approved cloud storage)

52

What tools and techniques do you need for mobile device digital forensics?

- **Techniques**:
  - **Preserve Digital Evidence**:
    - Dedicated evidence intake personnel should be educated on the proper way to preserve digital evidence
    - Properly seizing and storing digital evidence can be paramount to your investigations due to the security implemented on digital devices
    - Educating team members on proper device handling is worthwhile, even if that is the only time they will interact with the evidence
    - Chain of Custody

53

What tools and techniques do you need for mobile device digital forensics?

- **Techniques**:
  - **Copy, Copy, Copy**:
    - Once the evidence is back at your lab, you must create a forensic image, or copy, of the digital evidence
    - You will conduct your investigation on the forensic image as opposed to the evidence item itself
    - While manually searching the device itself is sometimes necessary, this is not typical in most investigations

54

What tools and techniques do you need for mobile device digital forensics?

- **Techniques**:
  - **Hashes**:
    - After you create your forensic image, a hash value will be reported for the newly created file
    - This hash value results from a calculation or hash algorithm performed on the forensic image obtained from the device
    - This hash value is important as it is used to verify the integrity of your forensic image throughout the life cycle of your investigation

55

What tools and techniques do you need for mobile device digital forensics?

- **Techniques**:
  - **Maintain Chain of Custody**:
    - Whatever methods are applied to search for data, examinations of the evidence must be thorough and proper note-taking is critical
    - The results from any examination need to be repeatable
    - Logging who has interacted with the evidence at any point during the investigation helps prove evidence authenticity and document chain of custody in court

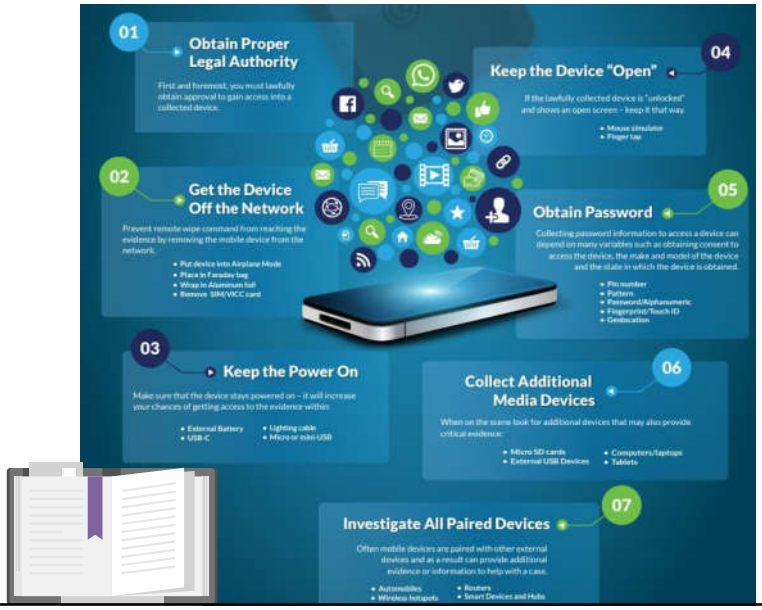
56

What tools and techniques do you need for mobile device digital forensics?

- **Techniques**:
  - **Ask the Investigator**:
    - It can be beneficial to ask the investigator many questions about the case before beginning your analysis
    - Anyone in this position has heard the line “Give me everything.
    - As you can imagine, that can be an overwhelming amount of data, and without applying techniques to filter through the data, evidence could be missed

57

7 things to do when collecting mobile devices



58

Thank you!

savina.gruicic@insig2.com

INSIG2

59

de Rechtspraak
Rechtbank Zeeland – West-Brabant

Cross-border access to data and admissibility of evidence

POST-COVID CHALLENGES IN CRIMINAL JUSTICE

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

1

de Rechtspraak
Rechtbank Zeeland – West-Brabant

Introduction

Studies:
- Computer Science
- Law School

Professional experience:
- Legal assistant, Lawyer at the Dutch Judiciary
- Legal advisor, Policy Officer cybercrime and digital investigations at the Dutch Police

Current Position, Additional Positions:
- CISO EQUANS Central Europe
- Judge at the criminal court of Zeeland West-Brabant
- Legal advisor, Policy Officer cybercrime and digital investigations at the Dutch Police

2

Safety mome

https://www.youtube.com/watch?v=MFfZWt3APS0

Guideline

- Safety moment
- Introduction and some figures
- Mutual Legal assistants
- Difficulties in investigating (Cyber)crime
- European Production Order and Preservation Order
- Innovation in Law in the Netherlands
- Case study

de Rechtspraak
Rechtbank Zeeland – West-Brabant

Cybercriminals are increasing efficiency with coordinated attacks

We are under attack

The lost productivity as a result of the WannaCry attack cost $ 4 billion

- Ransomware has been assessed as the prime threat for 2020-2022.
- Cybercriminals are increasingly motivated by monetization of their activities, e.g. ransomware.
- Malware decline that was observed in 2020 continues during 2021 and 2022.
- The volume of crypto jacking infections attained a record high in the first quarter of 2021, compared to recent years.
- There was a surge in healthcare sector related data breaches.
- Traditional DDoS (Distributed Denial of Service) campaigns in 2021 are more targeted, more persistent and increasingly multivector. In 2022 en 2023 Healthcare sectors and energy sectors were struck.
- In 2020 and 2021, we observe a spike in non-malicious incidents, as the COVID-19 pandemic became a multiplier for human errors and system misconfigurations, up to the point that most of the breaches in 2023 were caused by errors.

- January: Microsoft Exchange Server data breach
- April: Over 500 million Facebook users' personal info was discovered posted on a hackers' website
- April: The Ivanti Pulse Connect Secure data breach of unauthorized access to the networks
- May: Operation of the U.S. Colonial Pipeline is interrupted by a ransomware cyber operation.
- May: On 21 May 2021 Air India was subjected to a cyberattack wherein the personal details of about 4.5 million customers around the world were compromised
- July: On 22 July 2021 Saudi Aramco data were leaked by a third-party contractor and demanded $50 million ransom from Saudi Aramco.
- August: T-Mobile reported that data files with information from about 40 million former or prospective T-Mobile customers were compromised.
- September and October: 2021 Epik data breach. Anonymous obtained and released over 400 gigabytes of data from the domain registrar and web hosting company Epik.
- October: an anonymous 4chan reportedly hacked and leaked the source code of Twitch
- November and December: zero-day vulnerability (later dubbed Log4Shell) involving the use of arbitrary code execution in the ubiquitous Java logging framework software Log4j.

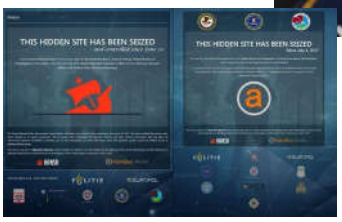
de Rechtspraak
Rechtbank Zeeland – West-Brabant

During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface.”

Developments

Achievements

Vera Jourová, EU Commissioner for Justice: "*While law enforcement authorities still work with cumbersome methods, criminals use fast and cutting-edge technology to operate. We need to equip law enforcement authorities with 21st century methods to tackle crime, just as criminals use 21st century methods to commit crime.*"



Mutual Legal Assistance

European Convention on Mutual Assistance in Criminal Matters (ETS No. 30)

- Under this Convention, Parties agree to afford each other the widest measure of mutual assistance with a view to gathering evidence, hearing witnesses, experts and prosecuted persons etc.
- National procedures on judicial co-operation in the criminal field.
- Practitioners are urged to consult the lists of signatures and ratifications as well as the declarations and reservations of any convention.
- Treaties create binding obligations on states parties, but actual execution of a request for international cooperation also requires analysis and consideration of the domestic laws of the requesting and requested states

General Principles International Cooperation in Criminal Matters

- Widest Cooperation Possible
- Dual Criminality
- Specialty Principle
- Proportionality

Difficulties traditional MLA in cybercrime cases

Traditional legal concepts

Territoriality

Jurisdiction

the need to have access to digital evidence which has been growing exponentially!

Exceptions

- Article 26 – Spontaneous information
  - within the limits of its domestic law and without prior request,
  - forward information obtained within the framework of its own investigations
  - when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning (cyber)criminal offences or might lead to a request for (cyber)co-operation.

- Article 32 – Trans-border access to stored computer data with consent or where publicly available
  - without the authorization of another Party:
    - a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
    - b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

11

European Production and Preservation Orders
Background

- Current framework is not sufficiently workable
- The information and communication technology in everyday life

First

Digital evidence is held on servers owned by service providers.

Second

the territorial approach to the jurisdiction to enforce – that is impractical and outdated

12

European Production and Preservation Orders
Summary of the proposed Regulation

- Issued or validated by a judicial authority of a Member State
- Preservation or production of data that is stored by a service provider located in another jurisdiction
- Necessary as evidence in criminal investigations or criminal proceedings
- Only be issued if a similar measure is available for the same criminal offence in a comparable domestic situation in the issuing State

13

13

European Production and Preservation Orders
Legal Basis, Subsidiarity and Proportionality

- **Legal basis**
- **Choice of the instrument**
- **Subsidiarity**
- **Proportionality**

14

14

Status

- 29 November 2022: Press release provisional political agreement European Parliament and Council;
- After published in Official Journal in January 2023
  - The regulation enter into force 20 days later en enter into application three years after that;
  - The directive enter into force 20 days later and Member states must adopt within two and half year

15

European Production and Preservation Orders
Legal Basis, Subsidiarity and Proportionality

Criminals don't stop at Europe's borders. Nowadays, the use fast and modern technologies to organise their illegal activities and erase their path afterwards. A lot of the data needed to track down these criminals is stored in the U.S. or by U.S. companies. An EU-US agreement to speed up the access of our law enforcement authorities to e-evidence is therefore of outmost importance. This will make Europe a safer place but, at the same time, it must do so while protecting our citizens' data, privacy and procedural rights.

Ana Birchall, Romanian Vice Prime Minister, Minister for Justice ad-interim

06-06-2019 The Council adopted today two mandates authorizing the Commission to negotiate on behalf of EU an agreement with the US facilitating access to e-evidence for the purpose of judicial cooperation in criminal matters and to participate in the negotiations in the Council of Europe on a second additional protocol to the Cybercrime Convention, respectively.

16

Innovation Law in the Netherlands

- Collecting, saving and take notice of data stored on a device after seizure, 556 Sv;
- Investigating data that is stored elsewhere at the time of or after the seizure of a device (network search), 557 Sv
- The forced biometric unlocking of a seized device, 558 Sv.

17

Collecting and investigation of data stored on a device after seizure, 556 Sv;

- In case of a red-handed felony or a felony that allows pre-trail custody;
- The public prosecutor can order;
- After authorization of the investigation Judge;
- That a police officer can investigate data that is received after seizure;
- If it is needed for the investigation.
- Period 3 days, 3 months of 6 months (severity of the crime and necessary for the investigation)

Synchronization? Existing connection?

18

Investigating data that is stored elsewhere at the time of or after the seizure of a device (network search), 557 Sv

- In case of a red-handed felony or a felony that allows pre-trail custody;
- The public prosecutor can order;
- After authorization of the investigation Judge;
- That a police officer can investigate data that is stores elsewhere during seizure;
- If it is needed for revealing the truth.
- Period 3 days, 3 months of 6 months (severity of the crime and necessary for the investigation)

Territoriality?
Existing connection?

Case Study: A sixteen-year-old girl is extorted with a sex video on Facebook and commits suicide. Who is the blackmailer?

- 16-year-old girls commits suicide;
- Suicide note;
  - Explicit video performing sexual acts;
  - BTC;
  - Video distributed;
  - Slickrick

OSINT on Facebook: 'SlickRick'

Investigation Facebook: 'SlickRick'

- OSINT on Facebook: 'SlickRick'
  → No visibility only for friends
- Request subscriber data Facebook
  → Telephone number by registration;
  → IP address by registration;

Next Step?

Phone number / IP-address

- Number:
  - → Bulgarian Mobile Telecom provider, Sim only;
  - → Whatsapp?
  - → True caller?

- IP address
  - → Italian telecom provider;
  - → Carrier grade NAT (Multiple users, same IP address)
  - → No logging
  - → Last used IP address → Tor node

Chat Function:

- Content data (request US)
- Login to account?
  - Victim;
  - Slickrick? Pay for leaked data set?
- Undercover?
- Hacking?

Next step?

Investigating the video and the victim's laptop:

- Video on a USB-stick form a friend
  → Metadata was removed;
  → Are the images real?

- Victims' laptop
  → No login credentials;
  → RAT found;
  → Send to NFI;

Investigating the video and the victim's laptop:

- Privacy of the Victim?
- Using credentials of the Victim?
- Checking the cloud?

- RAT → connecting?
- Password Vault?

Next step?

Investigation:

- Investigating the Police systems;
  → More Cases in other regions. Same MO (RAT / BTC)
- Another victim;
  → Balance account SlickRick
  → Chats
- Investigation Bitcoin account;
  → Chainalysis
- Cooperation at Europol
  → Polish investigation (undercover, IP tap)
  → Share information?
- Plot twist and final

27

Thanks!

Questions?

Contact:
https://www.linkedin.com/in/jordy-mullers-5583b829/
J.mullers@rechtspraak.nl

28

SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

Co-financed by the European Union

Electronic evidence and criminal procedure.

From open source to dark web.

ENELI LAURITS

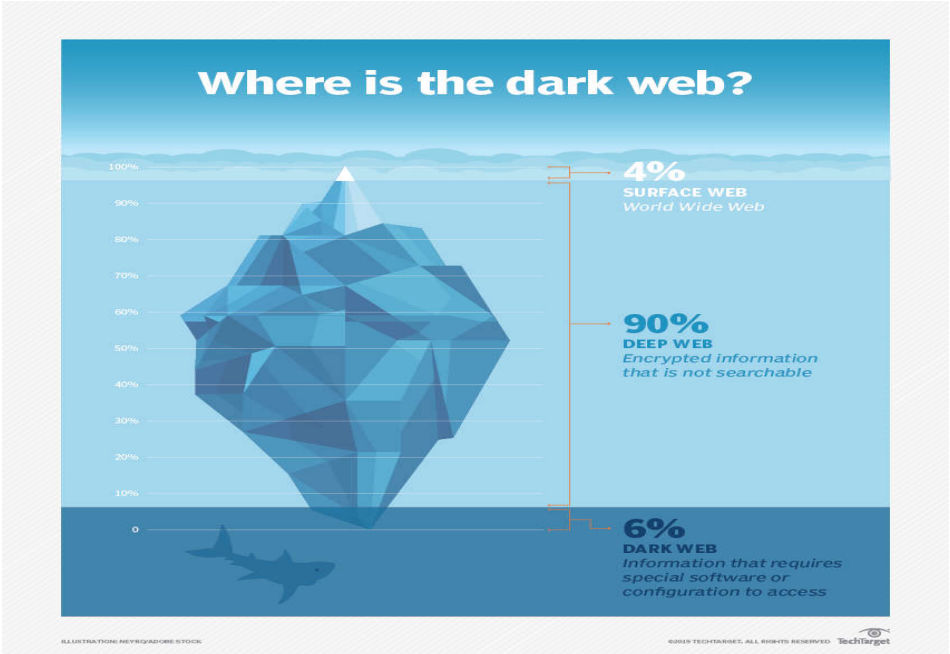
1

SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

Setting the stage

1. Dark web?
2. How to collect electronic evidence ***according to law***?
3. Publicly available data. Reasonable expectation of privacy and restrictions to collection of evidence.

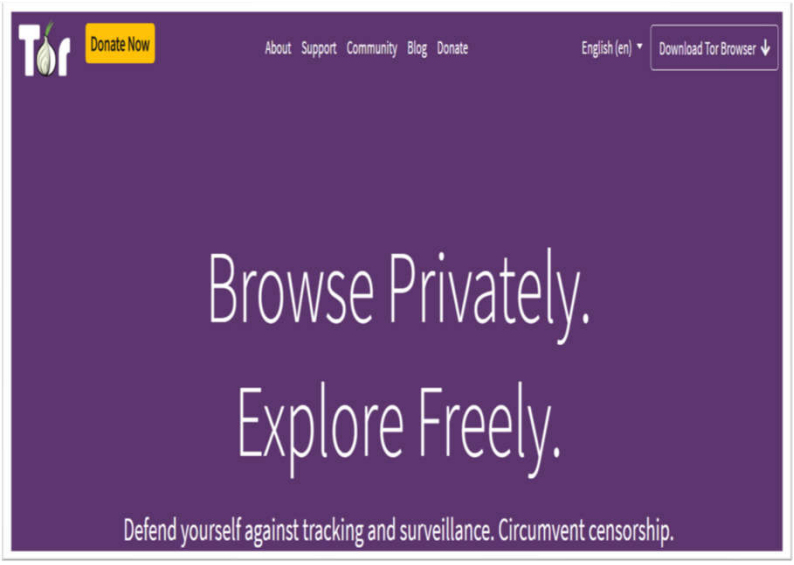
2



3

- The terms "dark web" and "deep web" are often used interchangeably, but they are not the same. Rather, the dark web is a small, less accessible part of the deep web.
- Both the dark and deep web share one thing in common: neither can be found in search engine results. The difference between them primarily lies in how their content is accessed. Deep web pages can be accessed by anyone with a standard web browser who knows the URL.
- Dark web pages, in contrast, require special software with the correct decryption key, as well as access rights and knowledge of where to find the content.

4



Darknet websites are accessible only through networks such as Tor.

Tor (originally, The Onion Router) is an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network's users, by routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption.

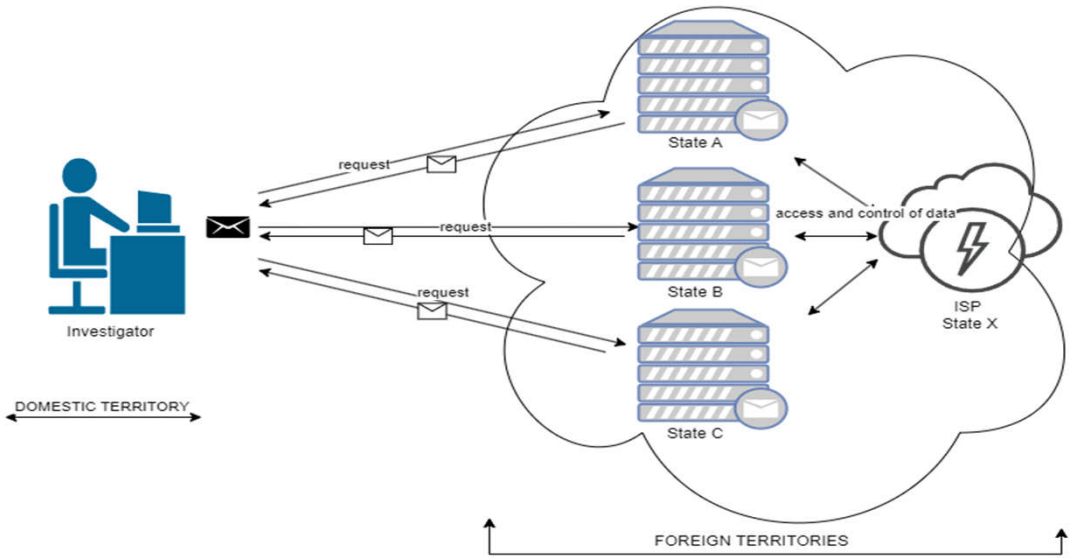
5

Requirements for admissibility - legitimacy

Digital evidence is considered legitimate and lawful when:

- It has been gathered without violating fundamental rights.
- It has been obtained and processed according to the procedure established by law.
- It must be obtained in compliance with best practices to be admissible in court.

6



7

Dark web investigations

- **Playpen** was a notorious darknet child pornography website that operated from August 2014 to March 2015. The website operated through a hidden service through the Tor network which allowed users to use the website anonymously. After running the website for 6 months, the website owner was captured. After his capture, the FBI continued to run the website for another 13 days as part of **Operation Pacifier**.
- When it was shut down in March 2015, the site had over 215,000 users and hosted 23,000 sexually explicit images and videos of children as young as toddlers.

8

Dark web investigations

- The term "network investigative technique" [NIT] is a euphemism for law enforcement hacking;
- It describes a law enforcement surveillance method that entails remotely accessing and installing malware on a computer without the permission of its owner or operator.
- Network investigative techniques are especially useful in the pursuit of criminal suspects who use anonymizing software to obscure their location.
- NITs have lead to many cases which have eventually ended up in international cooperation. As Kerr and Murphy* put it: „To date, not only has the most usual response [to discovering a foreign law enforcement agency engaged in the unauthorised access of data stored within its jurisdiction] been one of acquiescence, but, indeed, of providing even more cooperation."

*Orin S. Kerr & Sean D. Murphy. Essay. **Government Hacking to Light the Dark Web.** ***Risks to International Relations and International Law? - Stanford Law Review, vol 70, July 2017.***

9

SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

Publicly available data

Article 32 –Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorization of another Party:

a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

10

Capturing evidence from the internet

As a general rule, data recovered by the investigator will have to withstand some of the following questions being asked:

- Where does the data come from?
- Are you sure about the integrity of this data?
- Are you sure about the completeness of this data?
- Are you sure there aren't any details you might be unaware of, regarding the data which might render your conclusions drawn upon it invalid?

Or simply: Can you guarantee the integrity of you evidence?

11

Publicly available data

- Compliance with legal regulations is only possible if the subjects of the law understand what is required from them.
- To date there is no globally valid legal definition of public availability. Public availability is often falsely used synonymous with **'not protected in any way'.**
- The core of the understanding appears to be that data is publicly available if access to it is not limited to a specified group of persons.
- The key question under EU legislation is if data are related to natural persons and hence fall under the scope of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. The mere public availability of data is no feature that can completely disable the protection of a natural person through Articles 7 and 8 EU-CFR.

12

Publicly available data

The US perspective: in contrast to Article 7 EU-CFR the protection is not automatically granted if data is 'related to a natural person' but rather depends on the reasonable expectation of privacy of the affected person.

If that expectation exists, it is regularly determined by areal considerations.

13

Social media – publicly availabe?

A sub-section of the surface web is social media (eg Instagram, Snapchat, Facebook, Tinder). Social connections have always been an important investigative approach, with the shift from real-life to electronic communication these connections are often easily accessible and generate valuable insights for law enforcement.

Some of the currently existing networks allow users to limit the reach of their content to certain user groups (everyone, network participants, friends, friends of friends).

The public availability for such restricted data hence often depends on factual barriers that these settings eventually raise.*

Thilo Gottschalk. „The Data-Laundromat? Public-Private-Partnerships and Publicly Available Data in the Area of Law Enforcement."

14

- Data on social networks are easily relatable to natural persons and often give insights in particularly sensitive areas of a persons' life such as religious or political beliefs or sexual preferences.
- Accessing social media data hence bears severe risks to the fundamental rights of the data subject.
- **While data on social media may be manifestly made public, this cannot be re-interpreted as consent or abandoning fundamental rights protection.**

15

US example – case of Meregildo

- Where Facebook privacy settings allow viewership of postings by “friends,” could the Government access them through a cooperating witness who is a “friend” without violating the rights to privacy?
- While the user undoubtedly believes that his Facebook profile would not be shared with law enforcement, does he have a justifiable expectation that his “friends” would keep his profile private? And the wider his circle of “friends,” the more likely his posts would be viewed by someone he never expected to see them.

16

- In US vs Meregildo, the defendant Melvin Colon wanted to suppress evidence that the government obtained from his Facebook account. The government accessed this information from his Facebook "friend" who cooperated with law enforcement. Colon's Facebook "friend" gave the government access to view Colon's profile.
- The Judge in the case evaluated the evidence in the context of Colon's privacy settings and his circle of friends. The Judge denied Colon's motion to suppress and said that his Facebook information was lawfully obtained and useful in the case.
- The Judge emphasized the privacy settings used by Colon on his Facebook account. These privacy settings allowed the cooperating witness, Colon's Facebook "friend," to see the messages he posted to his account. As such, the Judge ruled that accessing this information was not a violation of the Fourth Amendment. Colon allowed "friends" to view his posts and he had a wide circle of friends. The Judge believed that because of this, Colon's expectation of privacy ended when he posted on Facebook.

17

The Deep web. US v Auernheimer*

- The defendant was convicted of unauthorised access for collecting information from a website of a US telecommunication provider, which was accessible on a hard-to-guess website that was not intended to be accessed.
- Although the data was publicly accessible, the court stated that the data was still protected, analogous to a home where 'the front door is left open or unlocked'.
- The defence argued that the information was made available to everyone and the general public was authorised to view the data.
- Courts increasingly assume that data publication does not necessarily preclude an expectation of privacy.

*Supreme Court of the United States, United States v Andrew Auernheimer (2014) <https://cite.case.law/f3d/748/525/

18

Concluding thoughts

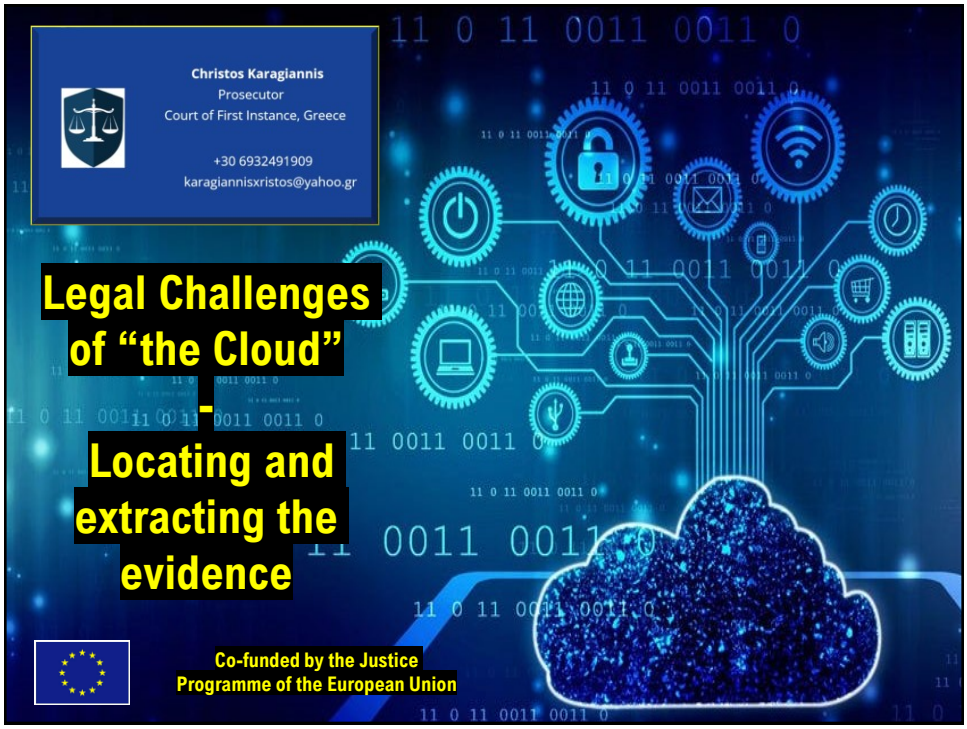
It doesn't much matter whether it is the surface web, deep web or dark web as evidence in criminal procedure is considered legitimate and lawful when:

- It has been gathered without violating fundamental rights
- It has been obtained and processed according to the procedure established by law
- It must be obtained in compliance with best practices to be admissible in court

19

THANK YOU!

20


Christos Karagiannis
Prosecutor
Court of First Instance, Greece
+30 6932491909
karagiannisxristos@yahoo.gr
Legal Challenges of "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

2

- **Data Redundancy : Multiplication of data for safety and performance optimization reasons**
- **Loss Of Location : No geographically fixed reference point**

3

Main Legal Challenges

A] Data Territoriality and Applicable Law

B] "Possession" of Cloudly Stored Data

C] Extracting Digital Evidence In The Cloud

4

A] Data Territoriality and Applicable Law

- Where is data stored ? (criminal event)
- Who provides the tools? (criminal instrument)
- Where is the crime realized? (direct consequence)
- Nationality of perpetrator or victim

5

B] "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)
- Ruling 1648/2016 of the Supreme Court of Greece (Criminal Department)

6

C] 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

C] 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
- Ruling 613/2016 of the Misdemeanor Council of Athens (GR)

8

Change Of The Legal Approach

9

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.

10

11

25 april 2023 Lisbon, May 18th and 19th 2023

de Rechtspraak
Gerechtshof 's-Hertogenbosch

ERA

European Commission

Two Sides of the Decryption Medal

Legal Challenges after Unwrapping the Gift Package

John van Krieken LLM MMO

Co-financed by the European Union

1

25 april 2023

de Rechtspraak
Gerechtshof 's-Hertogenbosch

Encryption, Blessing or Curse

- The official point of view:

- Encryption is is a human right and needed to guarantee privacy
- Manufacturers will not be forced to build 'backdoors'
- Not all jurisdictions guarantee human rights
- Problems for law enforcement are accepted as collateral damage.

2

Standard Encryption

- Communication apps use standard encryption, Skype, WhatsApp, Telecom
- They use peer to peer encryption, “impossible” to decode

- Software to encrypt hardware is not included in this presentation

Enter the commercial providers

- Individuals do not trust the standardstandard encryption
- Metadata of the communications are available to law enforcement
- Commercial services entered this market with dedicated networks and handsets
- Law enforcement officers found the handsets during arrest and searches

Ennetcom

5

Ennetcom

6

Ennetcom

- Criminals used special Blackberries
- Only messaging through Ennetcom infrastructure
- PGP encryption, so very robust
- Encryption keys generated by endusers
- But in fact generated by the Ennetcom servers.

7

Ennetcom

- Servers found in Canada
- Keymanagementsystem found and copied
- Messages only 24 hs saved?
- But several millions of items available?
- 1 mln nicknames
- Lawyer claims impossible in a legal way

8

Ennetcom

- Police claim 500 users/nicknames identified, used in 25 investigations
- In October 2016 recieved, in November already first use.
- Between 13/10/2016 and 12/7/2017 1,6 mln massages downloaded in “Hansken”
- Filtered: less than 3 words, non-Dutch or English

9

Ennetcom

- Results searched with topics, typical words used in organised crime
- 5503 positive adresses and 4282 contacts
- Of which 500 identified

10

Now it's getting Serious!

11

What's New with Enchrochat?

- Peer to peer encryption vs encryption in the server
- Europe based, servers in France, EU rules apply
- Data are of no useafter processing by the app

- Handsets cost over 1000 Euro's plus subscription, only use is sending and receiving tekst messages
- Over 50.000 users of whom 12.000 in NL

12

Joint Investigation Team, 26 Lemont

- French and Dutch police developed a tool
- Software introduced to the servers in Lille, France
- That tool infected all the connected handsets with a keylogger
- All the keystrokes/messages were sent to a Europol server
- An enormous collection of communication content was collected
- Explored with specially designed software called ‘Hansken’

A Gift for Law Enforcement, but a Challenge to the Judiciary

- 26Lemont is a criminal charge against Encrochat, but encryption is perfectly legal
- French police placed a bot in handsets wherever they were, mainly in other jurisdictions. Breach of sovereignty?
- If so: what should be the consequence?
- How far goes the principle of mutual trust?
- EU regulations on data protection involved?

What's the Charge against Encrochat?

- Complicity to serious crimes, like drug trafficking, money landering and related violent crimes
- Like driving a car to and from the scene of a robbery a legal activity may add up to complicity
- No or very scarce legal use due to high cost and limited possibilities of the system

Breach of National Sovereignty

- A state needs permission to investigate on the territory of another jurisdiction
- A breach of that obligatiom may vreate a diplomatic incident
- It is up to the state involved to decide to act, accept or ignore the breach
- A prosecuted individual cannot claim any rights or immunity in case the state doesn't act.

Mutual Trust

- Principle of mutual trust is not put aside by a JIT agreement
- There is no obligation to add a copy of the document to the casefile
- If a competent state official claims to act within the criteria set out by the law, an official of another state may rely upon his word.
- The cooperation of the Dutch police (in developing the tool) does not change that, the tool is applied onder French responsability.

17

Do the EU regulations on Data Protection Apply

- Yes, of course, but not the rules that bind telecom providers, including te ban on data retention, The General Data Protection Regulation EU 2016/679
- Its the Law Enforcement Data Protection Regulation EU 2016/680
- Data must be preserved if possible under scrutiny
- Must be destroyed if no longer needed for that cause
- Or tranferred if needed in another serious matter
- Which is exactly what happened here.

18

To be Continued

- There will be other networks, like SKY/ECC, Anom etc.
- There will be new lawyers, with new interventions. There is a cross-Europe network of law offices, in NL alone 47 members that specialise in these cases.
- If there is a lawyer that will argue this kind of evidence he or she will put all the arguments on the table.

19

Questions?

- John van Krieken LLM MMO
- Senior Judge
- Appeal Court ‘s-Hertogenbosch
- J.van.krieken@rechtspraak.nl
- +31 6 4813 5890

20

Computer Forensics

Dark Web Investigations

Electronic Evidence in Court

The Experience in Portugal

Lisboa 17.05.2023

Vítor Neves

1

PORTUGUESE LAW

Cybercrime Law — L 109/2009 15.09

Data Retention Law — L 32/2008 17.07

Code of Criminal Procedure — DL 78/87 17.02

Penal Code - DL 400/82 23.09

Constitution of the Portuguese Republic

2

COMPUTER CRIME, CYBERCRIMINALITY OR CYBERCRIME?

An act defined by law as a crime in which a computer system is the object or instrument of the crime or the commission of which is significantly linked to the use of a computer system.

In addition to crimes that offend goods directly linked to the computer environment, which aim to protect the very use of computers and its characteristic aspects such as software and surfing the Internet, also crimes that offend traditional legal goods, but which are committed through the use of computer systems

3

3

COMPUTER FORENSICS

Preservation, identification, extraction and documentation of electronic evidence stored as data or magnetically encoded information.

LATO SENSU

Any form of digital expertise and data analysis used in the course of an investigation

STRICTO SENSU

Set of methodological procedures and techniques for identifying, collecting, preserving, extracting, interpreting, documenting and presenting evidence from computer equipment in a manner that is acceptable during a legal or administrative proceeding in court.

4

4

SURFACE WEB, DEEP WEB AND DARK WEB

Surface Web - Regular Browsers and Search Engines (ex. *Google*)

Deep Web — Free, Safe and Anonymous Websurfing (ex. *Freenet / TOR)*

Dark Web — Deep Web Sites with Criminal Origins and Activities

5

5

COMPUTER FORENSICS AND E-EVIDENCE IN COURT

E-evidence shows up in 85% of criminal investigations

Fragmentary, Fragile, Volatile, Alterable, Unstable, Erasable and Manipulable, Invisible and Especially Dispersed.

«*Given the numerous ways information is stored on a computer, openly and surreptitiously, a search can be as much an art as a science*» — US Court of Appeals - US vs Brooks

6

6

COMPUTER FORENSICS AND E-EVIDENCE IN COURT

Where to find electronic evidence?

- networks and workstations
- removable disks
- temporary files
- swap files
- mirror disks
- program files
- websites
- cookies
- e-mails
- laptops and home computers
- smartphones

7

7

COMPUTER FORENSICS AND E-EVIDENCE IN COURT

Obtaining the information

The parties must access the information in a lawful manner, without violating the fundamental rights.

Incorporating data to the process

In order to incorporate the data into the process, it should meet some requirements: relevance, necessity, legality and procedural admissibility.

Value of the incorporated data

If the above requirements on obtaining and incorporating data are met, the electronic evidence will be subject to assessment by court.

8

8

COMPUTER FORENSICS AND E-EVIDENCE IN COURT

Two basic types of electronic evidence:

Data stored in computer systems or devices

Information transmitted electronically through communication networks

COMPUTER FORENSICS AND E-EVIDENCE IN COURT

Information transmitted electronically through communication networks is:

- Firstly regulated in articles 187 and 188 of the Code of Criminal Procedure, by reference from article 189.

Criminal procedural law confers the same conditions of admissibility and formalities on conversations or communications transmitted by electronic mail or other forms of data transmission by electronic means as it does on interceptions of telephone tapping.

- Also, Cybercrime Law - L 109/2009 15.09
Article 18 Interception of communications

COMPUTER FORENSICS AND E-EVIDENCE IN COURT

Data stored in computer systems and/or devices

CYBERCRIME LAW — L 109/2009 15.09
(Budapest Convention on Cybercrime)

Expedited preservation of stored computer data - article 12

Expedited preservation and partial disclosure of traffic data - article 13

Production Order - article 14

Search and seizure of stored computer data - articles 15 and 16

Online search - article 15,5

Seizure of e-mails and communication records of a similar nature - article 17

11

11

ANTI FORENSICS

Any attempts to compromise the availability or usefulness of evidence to the forensics process.

Compromising evidence availability includes any attempts to prevent evidence from existing, hiding existing evidence or otherwise manipulating evidence to ensure that it is no longer within reach of the investigator.

Usefulness maybe compromised by obliterating the evidence itself or by destroying its integrity

12

12

ANTI FORENSICS

Avoid detection
- Anonymizers
- Virtual currencies

Prevent examination and analysis of computer data
- Data erasure
- Data concealment
- Data tampering
- Attacks against forensics

13

13

ANTI FORENSICS

New technologies have made it easier to commit criminal offenses in the digital environment while making it more difficult to detect and, above all, to prove them.

Digital evidence, due to its special fragility, must be collected in compliance with the applicable forensic rules, under penalty of contamination, prohibiting its valorization.

The knowledge or mere suspicion, by the investigated party, of the pendency of a criminal process against him/her is often a sufficient condition for the digital evidence to be inevitably contaminated, concealed or eliminated - even after the seizure of the physical supports.

Criminal investigation in the digital environment, especially in the case of particularly serious crimes, has to move into the shadows or accept its inefficiency

14

14

DARK WEB INVESTIGATIONS

Digital Undercover Agents

Cybercrime Law - article 19

Covert Operations Law - L 101/2001 25.08
- Physical Ops - Analogical World

15

15

DARK WEB INVESTIGATIONS

Covert Operations Law - L 101/2001 25.08

Being a law created in 2001 it is completely outdated

It does not provide for any form of digital evidence collection, establishing exclusively the use of the undercover agent in the physical environment under the control of the portuguese criminal police - Polícia Judiciária

Cybercrime Law - L 109/2009 15.09

The rule on covert actions in digital media only extends the catalogue of crimes where it is possible to resort to this form of investigation.
Despite being amended in 2021 it does not introduce new means of obtaining evidence.
Using the rules foreseen for the interception of communications does not allow the action of the digital undercover agent.
Intercepting is not interacting.

16

16

DATA RETENTION

Portuguese Constitutional Court

Ac.268/2022 15APR2022

On those grounds, the Constitutional Court rules to:
a) Declare the unconstitutionality, with general mandatory force, of the rule contained in article 4 of Law no. 32/2008, of 17 July, in conjunction with article 6 of the same law, for violation of the provisions of paragraphs 1 and 4 of article 35 and paragraph 1 of article 26, in conjunction with paragraph 2 of article 18, all of the Constitution;
b) Declare the unconstitutionality, with general mandatory force, of the rule of article 9 of Law no. 32/2008, of 17 July, on the transmission of stored data to the competent authorities for the investigation, detection and prosecution of serious crimes, in so far as it does not provide for a notification to the person concerned that the retained data have been accessed by the criminal investigation authorities, provided that such communication is not likely to jeopardize the investigations or the life or physical integrity of third parties, for violation of the provisions of Article 35(1) and Article 20(1), in conjunction with Article 18(2), all of the Constituição.

17

17

DATA RETENTION

Remedies being studied as we speak:

Access to data retained for billing purposes for 3 months

Without geo localization

Notification to the person concerned that the retained data have been accessed by the criminal investigation authorities

18

18


THANK YOU
vitor.neves@me.com