



## (POST)COVID CHALLENGES IN CRIMINAL JUSTICE: INVESTIGATING WEB 2.0

- Criminals' new modi operandi
- Legal implications of e-evidence
- Cryptocurrencies and bitcoins
- Investigations in the darkweb

Bucharest, 19-20 September 2022

**UP  
GRADE**  
YOUR LEGAL  
EXPERTISE

Criminal Law

### Speakers and chairs

**Ioana Albani**, Chief Prosecutor, Directorate for Investigating Organised Crime and Terrorism (DIICOT), Bucharest

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

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

**Andrea Cruciani**, Judge, Court Martial, Naples

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

**Seanpaul Gilroy**, Digital Forensics Unit, Northumbria Police, Newcastle

**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

**Cristina Rotaru-Radu**, Director, National Institute of Magistracy (NIM), Bucharest

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

### Key topics

- Understanding the internet and associated technology
- Dark web investigations
- Open source tools (OST)
- Handling e-evidence in court
- (Mis)use of cryptocurrencies in criminal justice

Language  
English

Event number  
322DT58

Organisers  
ERA (Laviero Buono) in cooperation  
with the National Institute of  
Magistracy, Romania



# (POST)COVID CHALLENGES IN CRIMINAL JUSTICE

**Monday, 19 September 2022**

08:30 Arrival and registration of participants

09:00 **Welcome and introduction to the programme**  
*Cristina Rotaru-Radu & Laviero Buono*

---

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

---

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

*Chair: Laviero Buono*

09:15 **Using open source intelligence to gather evidence online**

- Understanding the Internet and associated technology
- Effective use of the Internet as an investigative fraud investigation tool
- Search engines, meta browsers, deep web & people search techniques
- Open Source Intelligence (OSINT) links

*Philip Anderson*

10:15 Discussion

10:30 Break

11:00 **Open source tools, computer forensics in the “Cloud”**

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

*Seanpaul Gilroy*

12:00 Discussion

12:15 Lunch

---

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

---

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

*Chair: Philip Anderson*

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

*Rainer Franosch*

14:15 Discussion

14:30 **Internet-related crimes, digital evidence and cloud forensics: contemporary legal challenges and the power of disposal**

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

*Christos Karagiannis*

## **Objective**

Covid-19 resulted in altering the *modi operandi* of criminals. Offences related to cybercrime and online criminal activities increased significantly. Trade of illicit goods and services has moved even more to the Darknet; the number of phishing attempts, cases of online fraud, investment fraud, cyberattacks in the health sector and trade in counterfeit medical products has increased. As children spend more time online, the number of child sexual exploitation cases has also risen sharply in Europe. Isolation has made people more vulnerable to internet-related crimes. This series of events addresses various challenges that judges, prosecutors and lawyers in private practice working in the field of EU criminal justice will have to face for the years ahead. Some of these challenges will remain in the “new normal” well beyond the end of the pandemic. This seminar will focus on online investigations.

## **About the Project**

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

## **Who should attend?**

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

## **Venue**

National Institute of Magistracy  
Regina Elisabeta Boulevard, nr.53,  
Bucharest, Sector 5

## **CPD**

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

- 15:00 Break
- 15:30 **Handling e-evidence from a technical point of view**
- First Responder's E-Learning
  - Value of Live Data Forensics
  - Value of Memory Forensics
  - Encryption as challenge
- Victor Voelzow*
- 16:15 Discussion
- 16:30 End of first day and dinner offered by the organisers (19:30)

## Tuesday, 20 September 2022

---

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

---

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

*Chair: Rainer Franosch*

- 09:30 **Cross-border access to data and admissibility of evidence**
- Obtaining e-evidence
  - Voluntary access to evidence
  - Legal process
  - Direct access
- Eneli Laurits*
- 10:00 Discussion
- 10:15 **Managing traditional physical evidence electronically: towards videoconference witness examinations, electronic criminal files and online remote trials**
- Andrea Cruciani*
- 10:45 Discussion
- 11:00 Break
- Chair: Eneli Laurits*
- 11:30 **The proposed European Production Order (EPO) and its effectiveness in collecting evidence (including evidence stored on mobile devices)**
- Jordy Mullers*
- 12:00 Discussion
- 12:15 **The key features of the Second Additional Protocol to the Council of Europe Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence**
- Ioana Albani*
- 12:45 Discussion, end of seminar and lunch (13:00)

---

For programme updates: [www.era.int](http://www.era.int) - Programme may be subject to amendment.

### Your contact persons



Laviero Buono  
Head of Section  
E-Mail: [LBuono@era.int](mailto:LBuono@era.int)



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

[www.era.int/elearning](http://www.era.int/elearning)



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

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

Apply online for "(Post)Covid Challenges in Criminal Justice":  
[www.era.int/?131102&en](http://www.era.int/?131102&en)

# Application

(Post-)Covid Challenges in Criminal Justice: Investigating Web 2.0  
Bucharest, 19-20 September 2022 / Event number: 322DT58/SBa



## Terms and conditions of participation

### Selection

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

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

2. Applications should be submitted before **4 August 2022**.
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 expenses

5. Travel costs up to €350 can be reimbursed by ERA upon receipt of the original receipts, tickets, boarding passes, invoices after the seminar. Participants are asked to book their own travel and accommodation. These rules do not apply to representatives of EU Institutions and Agencies who are supposed to cover their own travel and accommodation. Participants are advised of the obligation to use the most cost-efficient mode of transport available.

### Accommodation

6. Maximum 2 single occupancy hotel nights (up to 130 EUR/night) can be reimbursed by ERA, only upon receipt of the original hotel invoice.

### Other services

7. Two lunches, beverages consumed during the event and the seminar documents are offered by ERA. One joint conference dinner is also included.

### Participation

8. Participation at the whole conference is required and your presence will be recorded.
9. 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.
10. 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.
11. A certificate of attendance will be distributed at the end of the conference.

Apply online for  
“(Post)Covid Challenges in  
Criminal Justice”:  
[www.era.int/?131102&en](http://www.era.int/?131102&en)

### Venue

National Institute of Magistracy  
Regina Elisabeta Boulevard, nr.53,  
Bucharest, Sector 5

### Language

English

### Contact Person

Susanne Babion  
Assistant  
[sbabion@era.int](mailto:sbabion@era.int)  
+49 651 9 37 37 422



# 322DT58

## 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.

- I. GENERAL INFORMATION ABOUT THE SEMINAR
- II. SPEAKERS' CONTRIBUTIONS
- III. BACKGROUND DOCUMENTATION

### Work carried out by the European Union on e-evidence

1	Proposal for a Council Decision authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence ( <i>Brussels, 25.11.2021 COM(2021) 719 final</i> )	1
2	Proposal for a Regulation of the European Parliament and the Council on the European Production and Preservation Orders for electronic evidence in criminal matters ( <i>Strasbourg, 17.4.2018 COM(2018) 225 final</i> )	25
3	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 ( <i>Strasbourg, 17.4.2018 COM(2018) 226 final</i> )	81

### Other EU criminal justice documents

#### A) The institutional framework for criminal justice in the EU

##### A1) Main treaties and conventions

A1-01	Protocol (No 36) on Transitional Provisions
A1-02	Statewatch Analysis, "The Third Pillar acquis" after the Treaty of Lisbon enters into force, Professor Steve Peers, University of Essex, Second Version, 1 December 2009
A1-03	Consolidated version of the Treaty on the functioning of the European Union, art. 82-86 ( <i>OJ C 326/47; 26.10.2012</i> )
A1-04	Consolidated Version of the Treaty on the European Union, art. 9-20 ( <i>OJ C326/13; 26.10.2012</i> )

A1-05	Charter of fundamental rights of the European Union ( <i>OJ. C 364/1; 18.12.2000</i> )
A1-06	Explanations relating to the Charter of Fundamental Rights ( <i>2007/C 303/02</i> )
A1-07	Convention implementing the Schengen Agreement of 14 June 1985 ( <i>OJ L 239; 22.9.2000, P. 19</i> )

#### 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, 6 <sup>th</sup> 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.1959)

B1-07	Third Additional Protocol to the European Convention on Extradition ( <i>Strasbourg, 10.XI.2010</i> )
B1-08	Second Additional Protocol to the European Convention on Extradition ( <i>Strasbourg, 17.III.1978</i> )
B1-09	Additional Protocol to the European Convention on Extradition ( <i>Strasbourg, 15.X.1975</i> )
B1-10	European Convention on Extradition ( <i>Strasbourg, 13.XII.1957</i> )

## 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 ( <i>OJ L 81/24; 27.3.2009</i> )
B2-02	Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States ( <i>OJ L 190/1; 18.7.2002, P. 1</i> )
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	InAbsentiaEAW, 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 Śródmięście, 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 <i>Jeremy F / Premier ministre</i> , Judgement of the court (Second Chamber), 30 May 2013
B2-32	Case C-399/11 <i>Stefano Melloni v Ministerio Fiscal</i> , 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 Kozłowski, 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 ( <i>OJ L 294/20; 11.11.2009</i> )
B4-02	Council Framework Decision 2008/947/JHA on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions ( <i>OJ L 337/102; 16.12.2008</i> )
B4-03	Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union ( <i>OJ L 327/27; 5.12.2008</i> )
B4-04	Council Framework Decision 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings ( <i>OJ L 220/32; 15.08.2008</i> )
B4-05	Case C-234/18, Judgment of 20 March 2020
B4-06	Case C-390/16, Dániel Bertold Lada, Opinion of AG Bot, delivered on 06 February 2018
B4-07	Case C-171/16, Trayan Beshkov, Judgement of the Court (Fifth Chamber), 21 September 2017
B4-08	Case C-528/15, Policie ČR, Krajské ředitelství policie Ústeckého kraje, odbor cizinecké policie v Salah Al Chodor, Ajlin Al Chodor, Ajvar Al Chodor, Judgement of the Court (Second Chamber), 15 March 2017
B4-09	Case C-554/14, Ognyanov, Judgement of the Court (Grand Chamber), 8 November 2016
B4-10	Case C-439/16 PPU, Milev, Judgement of the Court (Fourth Chamber), 27 October 2016
B4-11	C-294/16 PPU, JZ v Śródmiście, 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 ( <i>OJ L, 350/72, 30.12.2008</i> )
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 ( <i>OJ L 196/45; 2.8.2003</i> )
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) ( <i>Official Journal L 178/1, 17.7.2000</i> )
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 ( <i>COM (97) 503</i> ), 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 ) ( <i>OJ L 135/85, 22.05.2019</i> )
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 ( <i>OJ L 135/85, 22.05.2019</i> )
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 ( <i>OJ L 135/27, 22.05.2019</i> )
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 ( <i>OJ L 93/23; 07.4.2009</i> )
B6-06	Council Decision on the exchange of information extracted from criminal records – Manual of Procedure ( <i>6397/5/06 REV 5; 15.1.2007</i> )
B6-07	Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record ( <i>OJ L 322/33; 9.12.2005</i> )

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 Assessment (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 ( <i>OJ L 348/130, 24.12.2008, P. 130</i> )

##### E2) Eurojust

E2-01	Eurojust quarterly newsletter
E2-02	Eurojust Guidelines on Jurisdiction
E2-03	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 ( <i>OJ L 274/1, 28.10.2019</i> )
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 ( <i>OJ L 210/12; 06.08.2008</i> )
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 ( <i>OJ L 210/1; 06.08.2008</i> )
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 ( <i>OJ L 386/89; 29.12.2006, P. 89</i> )
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 ( <i>10900/05; 27.5.2005</i> )

### G2) Joint Investigation Teams (JITs)

G2-01	Eurojust Information on JITs
G2-02	Third JIT Evaluation Report, Eurojust, March 2020
G2-03	Joint Investigation Teams Practical Guide (Brussels, 14 February 2017; 6128/1/17)
G2-04	Council Resolution on a Model Agreement for Setting up a Joint Investigation Team (JIT) – 2017/C18/01, Strasbourg, 19 January 2017



G2-05	Council Framework Decision of 13 June 2002 on joint investigation teams (OJ L 162/1; 20.6.2002)
-------	--

# Technical Issues and basic understanding of the Internet architecture and concepts

Using open source intelligence to gather evidence online

---

PHILIP ANDERSON

ERA | BUCHAREST, 19-20 SEPTEMBER 2022

Co-funded by the Justice Programme of the European Union



1

## Speaker Background

---

- Assistant Professor/Senior Lecturer @ Northumbria University.
- Over 15 years teaching digital forensics and incident response.
- 5 years teaching digital investigations and digital evidence to police on the Police Constable Degree Apprenticeship programme.
- Consulted with the European Union Agency for Cybersecurity (ENISA) from 2010 up until 2021 in identifying emerging and future ICT risks in the area of Information Security Risk Assessment and Management.
- My current research focuses on the application of artificial intelligence to digital forensic challenges.

2

## Outline

---

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

3

## (Post) COVID-19...cybercrime landscape

---

Europol - Internet Organised Crime Threat Assessment (IOCTA) 2021

<https://www.europol.europa.eu/publications-events/main-reports/iocta-report>

- **Cyber-dependant**
  - Ransomware
  - Mobile malware
  - DDoS for ransom (returning)
- **Cyber-enabled**
  - Child sexual abuse material
  - Increase via social media and online gaming platforms
  - P2P distribution increased
  - Phishing and social engineering
    - Increased in volume and sophistication
  - Dark web
    - Encrypted communication increasing

4



# #1

## Understanding the Internet and associated technologies

5

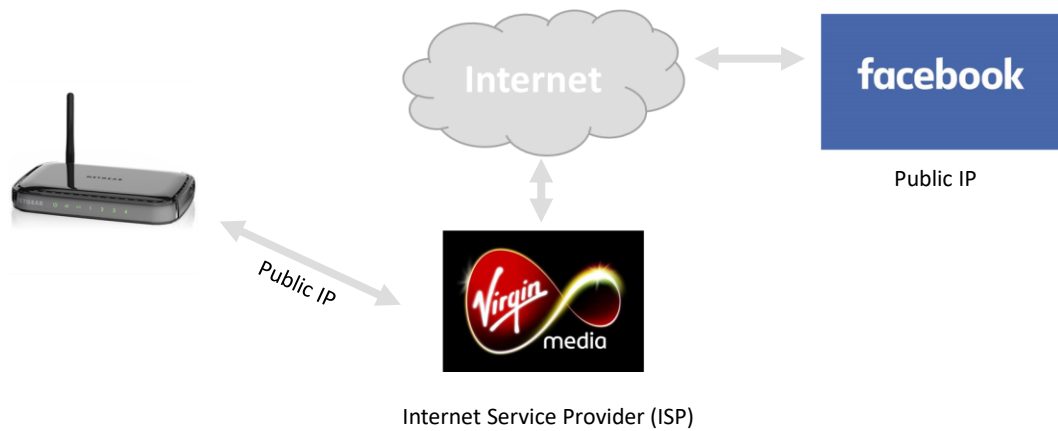


### How does it work.

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

6

## How does it work... Infrastructure



7

## How does it work... Internet Service Provider

- Gateways to the Internet
- Infrastructure
- IP Addresses

8

## How does it work...IP Address

---

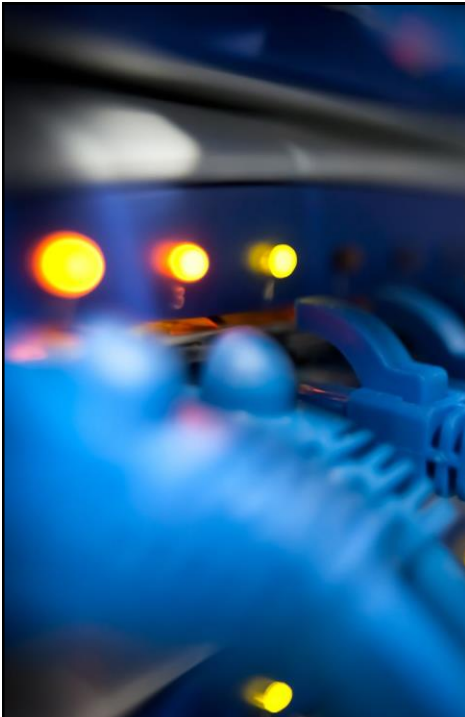
IP Address - 217.32.165.148

1. 217 – Class
2. 32 – Network No.
3. 165 – Sub-network No
4. 148 – Computer No.

Telephone Number 4401934822862

1. +44 – UK
2. 01934 – Somerset
3. 822 – Sandford
4. 862 – Local Number

9



## How does it work...Public and Private IP.

---

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

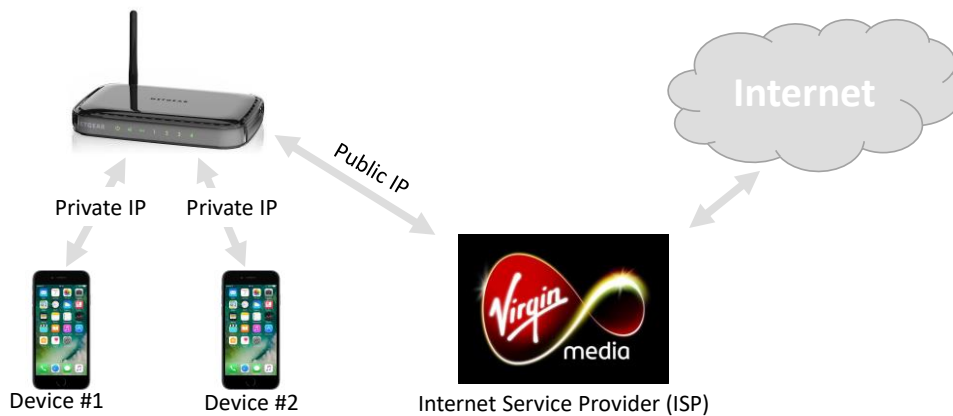
10

## How does it work...Dynamic and Static IP.

- Dynamic IP – could be different at the start of every internet session
- Static IP – remains the same for each session

11

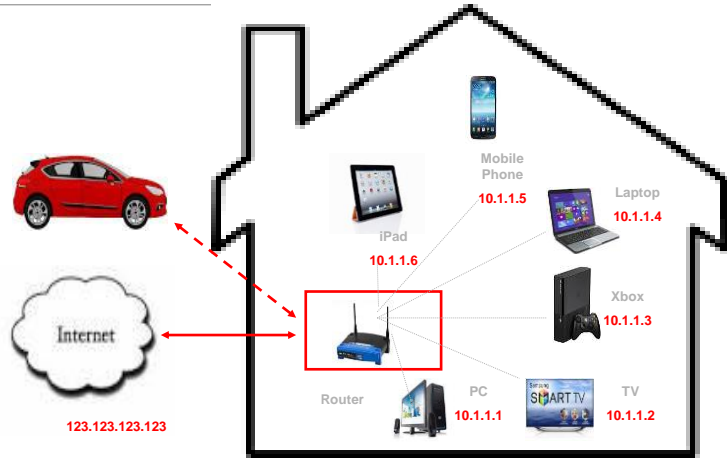
## How does it work... Public and Private IP



12

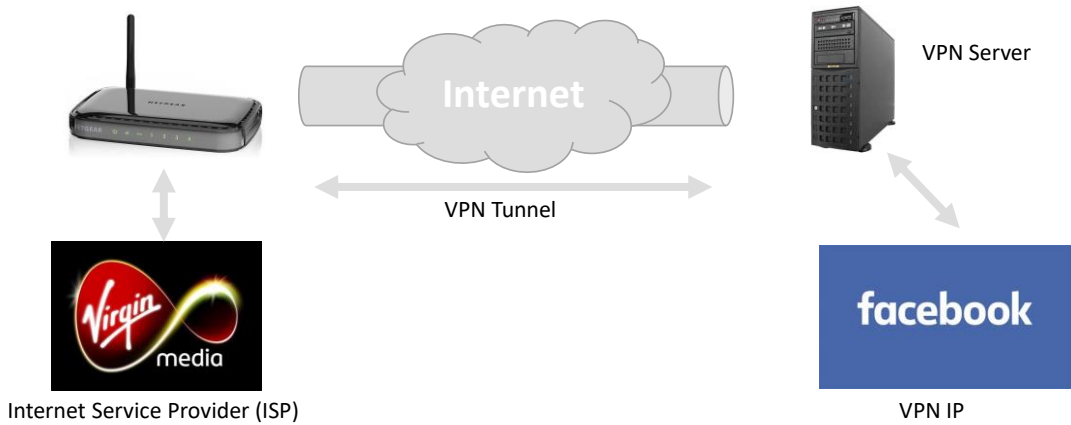


# How does it work...



13

# How does it work... Privacy | Anonymity



14

## How does it work...Email

```

https://mail.google.com/mail/u/0?ik=a622703d51...
header.b=vrReMQfY;
spf=pass (google.com: domain of bounce@charterforcompassion.org
designates 138.68.254.119 as permitted sender)
smtp.mailfrom=bounce@charterforcompassion.org
Return-Path: <bounce@charterforcompassion.org>
Received: from charter.nswd11c.com (charter.nswd11c.com. [138.68.254.119])
by mx.google.com with ESMTPS id
s27si5506922pfd.345.2020.04.03.01.24.14
for <...@gmail.com>
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Fri, 03 Apr 2020 01:24:15 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounce@charterforcompassion.org
designates 138.68.254.119 as permitted sender); client-ip=138.68.254.119;
Authentication-Results: mx.google.com;
dkim=pass header.i=@charterforcompassion.org header.s=acy
header.b=vrReMQfY;
spf=pass (google.com: domain of bounce@charterforcompassion.org
designates 138.68.254.119 as permitted sender)
smtp.mailfrom=bounce@charterforcompassion.org
Received: from compassionc by charter.nswd11c.com with local (Exim 4.93)
(envelope-from <bounce@charterforcompassion.org>) id 1jKHcb-00045w-JU for

```

Source: <https://www.maketecheasier.com/blacklist-whitelist-ip-addresses-gmail/>

15



Effective use of the  
Internet as an  
investigation tool

16

## Investigations...

---

- “The sheer volume is daunting, and separating wheat from chaff requires skill, knowledge, and a reliance on sophisticated information technology. It also takes a concerted effort to coordinate with partners to avoid duplication and make the best use of resources, but the payoff in both effectiveness and efficiency is high.”
- Source: <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html>

17

## Investigations...

---

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

18

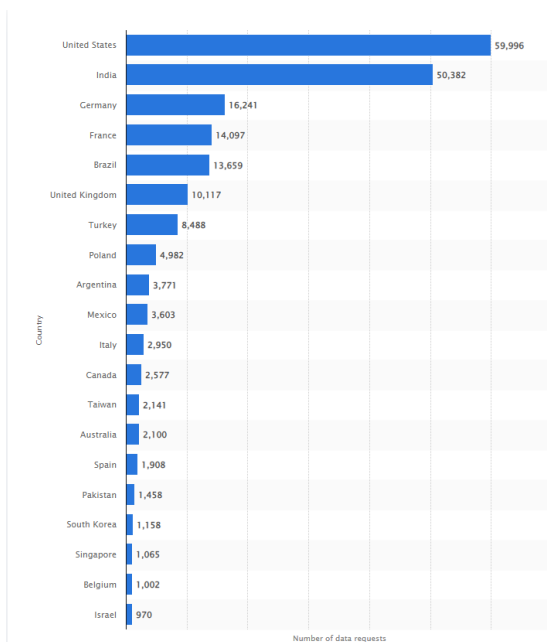
## Investigations... social media

- As of April 4.65 billion social media users from 5 billion Internet users<sup>1</sup>
- Most popular social networks worldwide as of January 2022<sup>2</sup>
  - Facebook – 2.9 billion
  - YouTube – 2.5 billion
  - Instagram – 1.4 billion
  - TikTok – 1 billion

1. Statista - <https://www.statista.com/statistics/617136/digital-population-worldwide/>

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

19



Number of user data requests issued to Facebook from federal agencies and governments during 2nd half 2021, by country

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

20

## Investigations... social media



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

Source: [https://nypost.com/2022/03/02/fbi-busts-tiktok-star-c-for-series-of-armed-robberies/?utm\\_source=url\\_sitebuttons&utm\\_medium=site%20buttons&utm\\_campaign=site%20buttons](https://nypost.com/2022/03/02/fbi-busts-tiktok-star-c-for-series-of-armed-robberies/?utm_source=url_sitebuttons&utm_medium=site%20buttons&utm_campaign=site%20buttons)

21

## Investigations... social media



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

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

22

## Investigations... fraud

---

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

23

## Investigations... considerations

---

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

24

## Investigations... Legislation (UK)

---

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

25

## Investigations... ethics

---

- Open source intelligence is the use of **publicly** produced and **publicly** available data that can be collected and shared.
- Be aware of the terms and conditions policies on the public data you are trying to collect - creating fake profiles breaks Facebook policies, and could therefore put an investigation at risk.
- The collection of open source data and nothing more, shouldn't be associated with hacking, intrusion testing, or anything similar.

26



---

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

27

## Internet...accessing

---

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

28



## Internet...accessing

---

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

29

## Methods... information sources

---

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

30

## Methods... Information gathering

---

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

31

## Methods... Information sources

---

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

32

## Methods... tools

---

- Remember
  - Evidential integrity
  - Evidential chain of custody
  - No digital devices have been seized or examined.
- Capturing the (online) evidence
  - Hunchly – web capture tool
  - Searching
  - Collecting and documenting
    - Timestamps and hashing
  - Audit trail
  - Secure cloud storage
  - Reporting

33

## Methods... capture

---



34



#4

---

Using open source intelligence to gather evidence online

35

## Open Source... methods

---

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

36

## Open Source... Case Studies - Bellingcat

- Unravelling the Killing of Colombian Protester Lucas Villa - <https://www.bellingcat.com/news/2021/12/06/unravelling-the-killing-of-colombian-protester-lucas-villa/>
- Examined social media posts
- Analysed private CCTV footage
- Black Gold Burning: In Search Of South Sudan's Oil Pollution - <https://www.bellingcat.com/news/africa/2020/01/23/black-gold-burning-in-search-of-south-sudans-oil-pollution/>
- Location of the spills was collected through social media research
- Data on the oil fields was gathered from various public sources

37

## Open Source... Case Studies - Bellingcat

- Two Europol StopChildAbuse Images Geolocated - <https://www.bellingcat.com/news/2019/12/05/two-europol-stopchildabuse-images-geolocated-part-i-madagascar/>
- Google maps photos
- Google Earth imagery
- Geographic and demographic data examined
- Timeline analysis – tropical storms
- Skripal Poisoning Suspect Dr. Alexander Mishkin, Hero of Russia - <https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia/>
- Passport photos
- Online biographical data
- Locations searches
- Telephone numbers

38

## Open Source... caution

---

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

39

## Open Source...

---

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

40

## Additional learning resources

---

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

41

## Thank you

---

# Questions?

Philip Anderson

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

42





# OPEN SOURCE TOOLS, COMPUTER FORENSICS IN THE "CLOUD"

Seanpaul Gilroy

Senior Digital Forensic Investigator

(POST)COVID CHALLENGES IN CRIMINAL JUSTICE: INVESTIGATING WEB 2.0







Co-funded by the Justice Programme of the European Union



1

## TOPICS

-  Overview of Open Source Investigations
-  Protecting your privacy during open source investigations
-  Tracing domain name owners, the origin of an email and email blacklists
-  Geo-location tools for Open Source Investigations
-  Investigating Web 2.0 – social networking, blogs and online gaming

9/7/2022

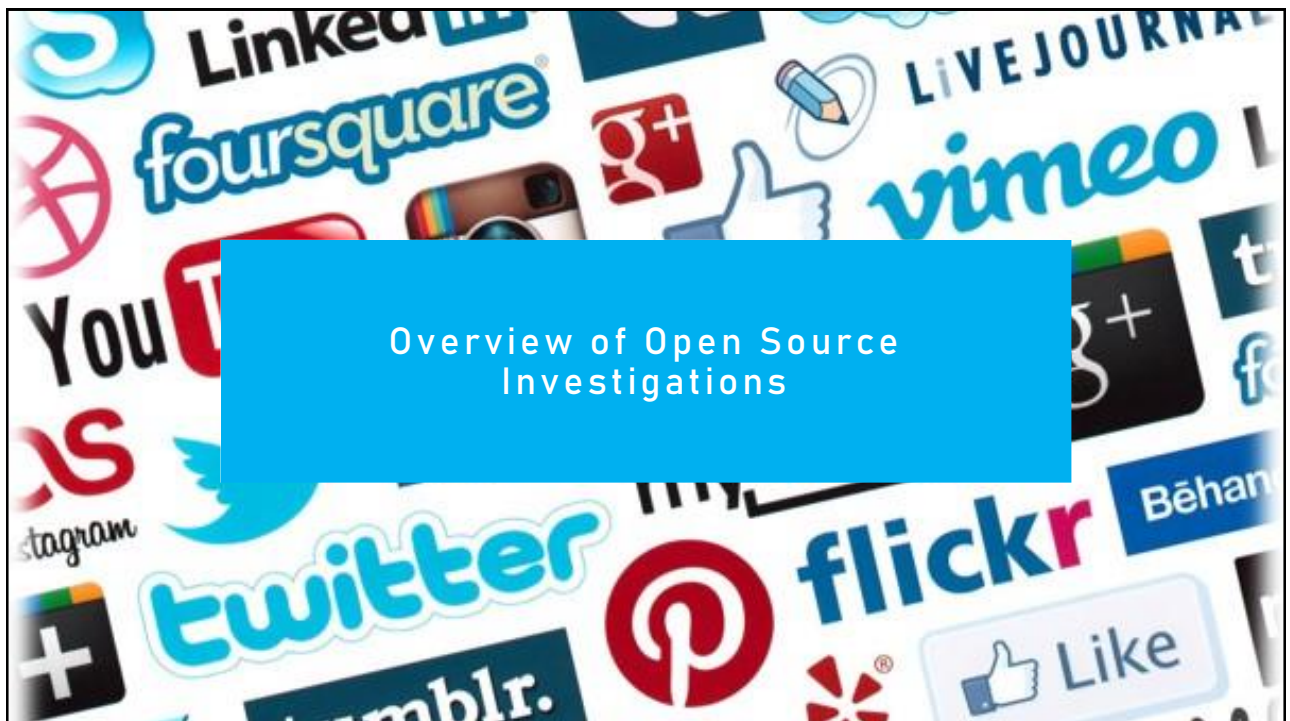
2

## ABOUT ME

- Senior Digital Forensic Investigator, Northumbria Police
  - Manage a team of 7 Digital Forensic Investigators
  - Based in Newcastle Upon Tyne, England
- BSc Hons in Computer Forensics
- Worked in the field of Digital Forensics for around 8 years
- Completed numerous courses relating to the field of Digital Forensics
  - Computer Forensics
  - Mobile Device Forensics
  - Cloud Forensics
- Deliver training inputs to both new and existing police officers on a regular basis:
  - Seizure of digital evidence
  - Analysis of digital evidence
  - Forensic quality standards (ISO 17025)

9/7/2022

3



4

## WHAT IS OPEN SOURCE?

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

National Police Chiefs Council (NPCC)

9/7/2022

5

## DIGITAL FORENSICS

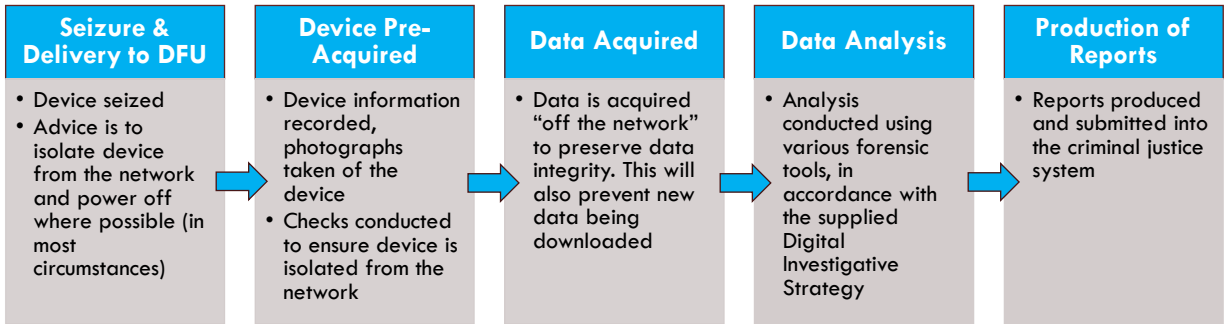
- Digital Forensics has developed rapidly over the past few years
- Traditionally, digital forensics has been referred to as “**dead box forensics**”
- A Digital Forensic Investigator will encounter an array of different devices on a case-by-case basis
  - Dynamic field, adapting to new technologies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



9/7/2022

6

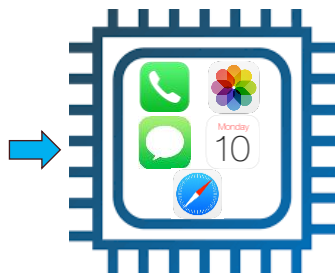
# DIGITAL FORENSIC LIFECYCLE



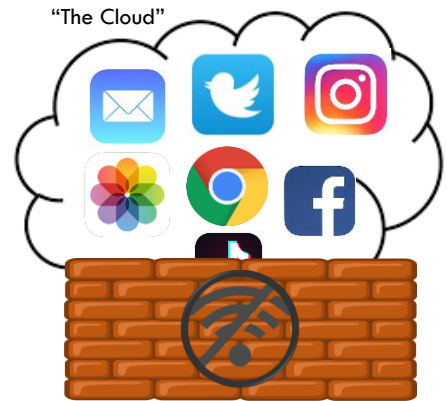
9/7/2022

7

# DIGITAL FORENSIC CASE STUDY



Internal phone storage



9/7/2022

8



## Protecting your privacy during open source investigations

9

## PROTECTING YOUR PRIVACY ONLINE

- The use of technology records a lot of information as part of its functionality,
  - often to improve the user's experience
- The end user is often unaware that such information is recorded:
  - Device details (Device make, model, serial number, IMEI)
  - Location Data (longitude and latitude)
  - Usernames/passwords
  - Internet History
  - Download history
  - Social media information
- As such, when conducting open source investigations, the investigators information may be recorded and preserved
- It is imperative that we protect our identity when conducting open source investigations, as you will see in upcoming slides
- **What steps can we take to protect our identity?**

9/7/2022

10

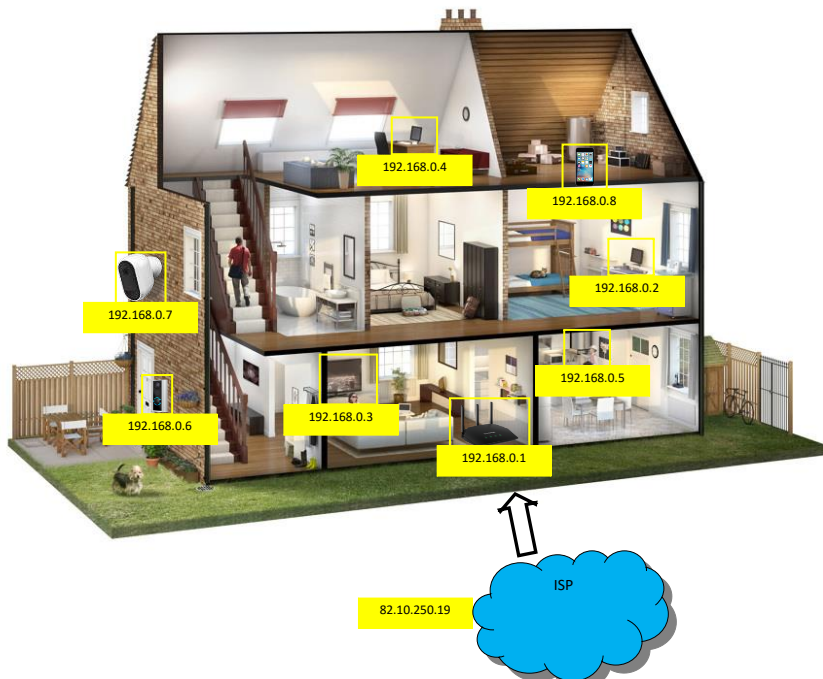
# IP ADDRESSES

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



9/7/2022

11



12



## IP ADDRESS EXERCISE

- **Step 1)** Visit Google
- **Step 2)** Search “What’s my IP”
  - Google will usually display your IP address, if not it will list a number of free tools which may help
  - <https://www.whatismyip.com> is one of many tools which are available
  - Make a note of your IP address
- **Step 3)** Visit <https://www.maxmind.com>
- **Step 4)** Enter your IP address in the GeolIP2 precision service search box and press go

GeolIP2 Precision Service  
Try our demo:



9/7/2022

13

## IP ADDRESS - EXERCISE

- What information can be obtained from my IP address:

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

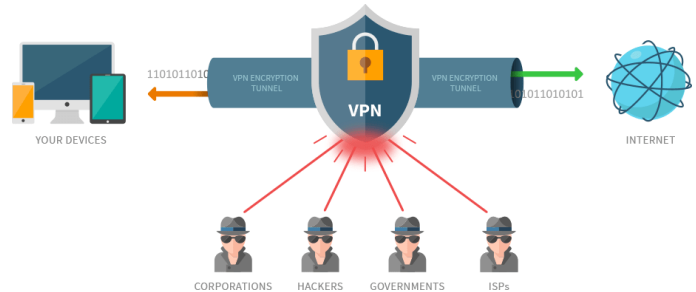
- This reveals some key information about my identity online which could be used to assist to identify me as an investigator
- What can we do as investigators to protect our identity online?

9/7/2022

14

# VIRTUAL PRIVATE NETWORKS

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



9/7/2022

15

# VIRTUAL PRIVATE NETWORKS

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



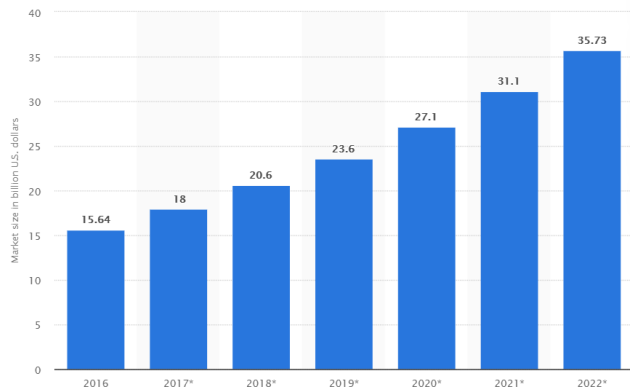
9/7/2022

16



# VIRTUAL PRIVATE NETWORKS

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



9/7/2022

17

# VIRTUAL PRIVATE NETWORKS

## Why should you use a VPN for Netflix

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

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

How to unblock websites and banned web pages online from anywhere

9/7/2022

18

## VIRTUAL PRIVATE NETWORKS - EXERCISE

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

**Step 2)** Enter your IP into Maxmind

**Step 3)** Register and Download Proton VPN

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

**Step 5)** Identify your IP address

**Step 6)** Enter your new IP into Maxmind

What do you notice?

9/7/2022

19

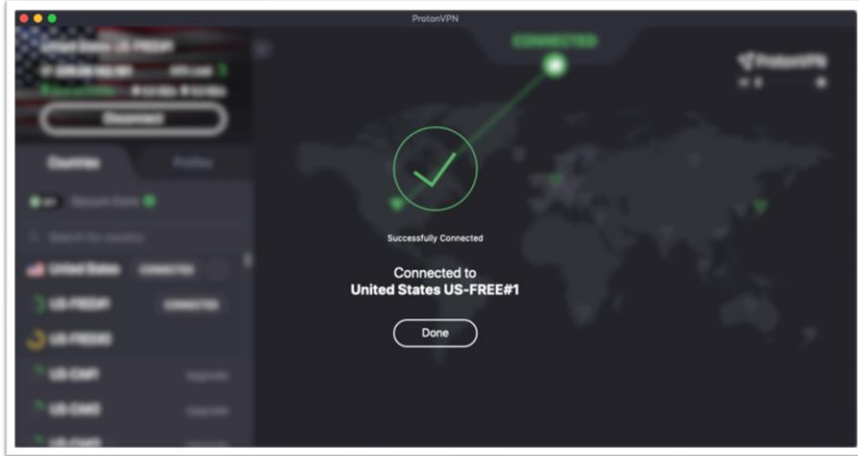
## VIRTUAL PRIVATE NETWORKS - EXERCISE

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

9/7/2022

20

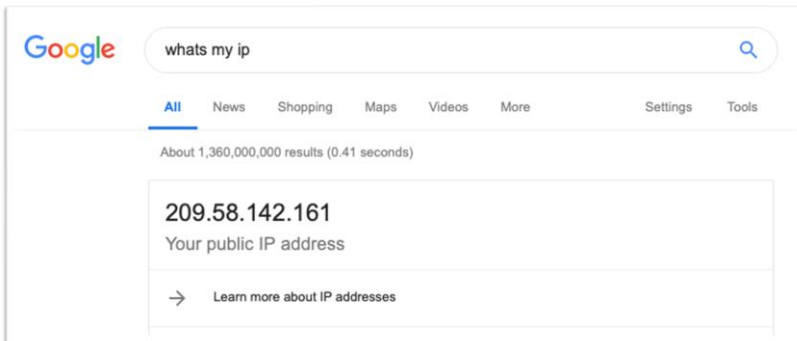
# VIRTUAL PRIVATE NETWORKS - EXERCISE



9/7/2022

21

# VIRTUAL PRIVATE NETWORKS - EXERCISE



9/7/2022

22

## VIRTUAL PRIVATE NETWORKS - EXERCISE

**GeoIP2 Precision: City Results**

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

9/7/2022

23

## TOR BROWSER

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

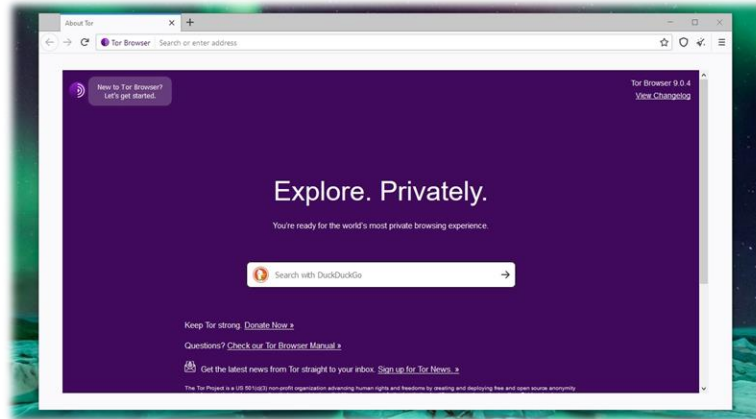


9/7/2022

24

# TOR BROWSER

- The browser looks very similar to other common web browsers



9/7/2022

25

# OSIRT BROWSER

- OSIRT is a web browser which was developed specifically for use in open source investigations
- OSIRT stands for **O**pen **S**ource **I**nternet **R**esearch **T**ool
- OSIRT is a free and open source application:
  - Only works with Microsoft Windows
- Currently being re-developed and due for release around Spring 2022
- Contains a number of useful features
  - Built in tools to capture video and screenshots
  - Webpage download
  - Tor built in to protect your identity
  - Ability to create reports
  - Automated logging
  - Case notes
- Download from [www.osirtbrowser.com](http://www.osirtbrowser.com)

9/7/2022

26

# OSIRT BROWSER

## Enhanced Web Browsing

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

## Capture The Web

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

## Report Generation

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

### Video Screen Recording

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

### Webpage Downloading

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

### Tor Built In

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

### Automated Logging

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

### Case Notes

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

### Attachments

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

9/7/2022

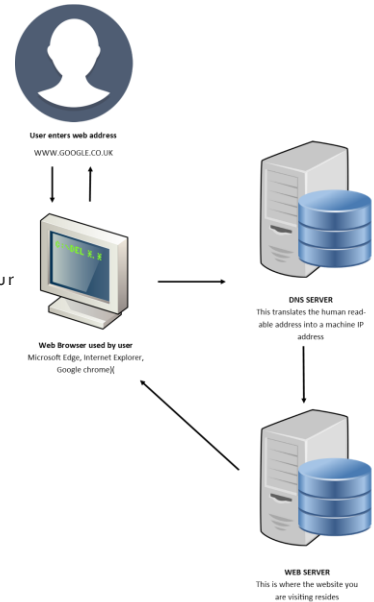
27

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

28

# DOMAIN NAMES

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



9/7/2022

29

# DOMAIN NAMES - WHOIS

- WHOIS search conducted for the US Postal Service domain name
  - [www.usps.com](http://www.usps.com)
- This reveals a number of details
  - Postal address
  - Telephone number
  - Email address
  - IP addresses

```

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

Domain Name: USPS.COM

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

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

Domain servers in listed order:
DNS100.USPS.COM      56.0.100.25
DNS141.USPS.COM      56.0.141.25
DNS082.USPS.COM      56.0.82.25
  
```

9/7/2022

30

## DOMAIN NAMES – PROXY

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

```

Domain name:
    in2locks.co.uk

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

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

9/7/2022

31

## EMAILS

- A commonly used form of communication, which can contain hidden information which is useful during an open source investigations
- An email contains two main parts
  - The body of the message (The section the we see as a general user)
  - The header (The hidden bit – of interest to investigators)
- A header is responsible for ensuring the email is delivered to the correct person.
  - Similar to a delivery tracking service when you order a parcel online
- This hidden header can often contain lots of information which can be useful during an investigation
  - To
  - From
  - Subject
  - Route
  - Origin information
- Not all email headers will contain the same information:
  - The information contained within the header depends upon the email provider of the sender.

9/7/2022

32



# EMAIL HEADERS

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

```
Received: from antivirus1.its.rochester.edu (antivirus1.its.rochester.edu
[128.151.57.50])
  by mail.rochester.edu (8.12.8/8.12.4) with ESMTTP id h2OGQe9e002563;
  Mon, 24 Mar 2003 11:26:54 -0500 (EST)
Received: from antivirus1.its.rochester.edu (localhost [127.0.0.1])
  by antivirus1.its.rochester.edu (8.12.8/8.12.4) with ESMTTP id
h2OGQrQx003450;
  Mon, 24 Mar 2003 11:26:54 -0500 (EST)
Received: from galileo.cc.rochester.edu (galileo.cc.rochester.edu
[128.151.224.6])
  by antivirus1.its.rochester.edu (8.12.8/8.12.4) with SMTP id
h2OGQrDC003447;
  Mon, 24 Mar 2003 11:26:53 -0500 (EST)
Received: (from majord@localhost)
  by galileo.cc.rochester.edu (8.12.8/8.12.4) id h2OGQq91029757;
  Mon, 24 Mar 2003 11:26:52 -0500 (EST)
Date: Mon, 24 Mar 2003 11:26:50 -0500 (EST)
From: someuser@mail.rochester.edu
Message-Id: <200303241626.h2OGQqJt002507@mail.rochester.edu>
To: someuser@its.rochester.edu
Subject: My mail message is about:
```

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

9/7/2022

33

# EMAIL HEADERS - EXERCISE 1

Good day,

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

Await your co-operation.

Yours sincerely,

Wynne Baxter

9/7/2022

34

# EMAIL HEADERS - EXERCISE 1

Remember: this could be assigned by a VPN

```
X-Originating-IP: [221.193.216.144]
Authentication-Results: mtall39.mail.ir2.yahoo.com from=gmail.com; dkim=neutral (no sig)
Received: from 127.0.0.1 (EHLO ld.cn) (221.193.216.144)
    by mtall39.mail.ir2.yahoo.com with SMTP; Tue, 02 Apr 2019 10:01:46 +0000
Received: from User (unknown [197.242.107.126])
    by ld.cn (CStmail for UNIX) with ESMTSP id 8D2935FAA32E;
    Tue, 2 Apr 2019 17:42:36 +0800 (CST)
Reply-To: <wynnebaxtercollp@gmail.com>
From: "Wynne Baxter" <wynnebaxtercollp1@gmail.com>
Subject: Proposal
Date: Tue, 2 Apr 2019 10:55:20 +0100
MIME-Version: 1.0
```

GeoIP2 Precision: City Results

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
221.193.216.144	CN	Handan, Hebei, China, Asia		36.5467, 114.5333	500	China Unicom Hebei	China Unicom Liaoning		

9/7/2022

35

# EMAIL HEADERS - EXERCISE 2

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

Sincerely,  
Peter OWEN

9/7/2022

36

# EMAIL HEADERS - EXERCISE 2

Remember: this could be assigned by a VPN

```
X-Originating-IP: [58.99.32.32]
Authentication-Results: mtall187.mail.ir2.yahoo.com from=gmail.com; dkim=neutral (no sig)
Received: from 127.0.0.1 (EHLO tdtv.tinp.net.tw) (58.99.32.32)
  by mtall187.mail.ir2.yahoo.com with SMTP; Wed, 27 Mar 2019 05:52:47 +0000
Received: by tdtv.tinp.net.tw (Postfix, from userid 10734)
  id 83A33364B20; Wed, 27 Mar 2019 13:52:45 +0800 (CST)
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 3.2.4 (2008-01-01) on tdtv.tinp.net.tw
X-Spam-Level: *****
X-Spam-Status: Yes, score=12.8 required=11.0 tests=AWL,BAYES_60,
  DNS_FROM_AHBL_RHSBL,FH_DATE_PAST_20XX,FORGED_MUA_OUTLOOK,MSEO_MID_WRONG_CASE,
  RCVD_IN_BL_SPAMCOP_NET,RCVD_IN_XBL,RDNS_NONE autolearn=spam version=3.2.4
```

GeoIP2 Precision: City Results

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Radius (km)	ISP	Organization	Domain	Metro Code
58.99.32.32	TW	Taichung		24.1465, 120.6839	100	Taiwan Infrastructure Network Technologies	Taiwan Infrastructure Network Technologies	tinp.net.tw	

9/7/2022

37

# EMAIL SPAM

- Spam is also often referred to as Junk
  - unsolicited messages sent in bulk by email.
- Spam emails are sent for a number of reasons:
  - Make money
  - Phishing to obtain personal information such as credit card, bank details and passwords
  - Spread malicious code i.e. viruses
- Cisco reported in April 2019
  - Average Daily Legitimate Emails 72.56 Billion
  - Average Daily Spam Volume 416.78 Billion
- Statista reported:
  - Between October 2020 and September 2021, global daily spam volume reached its highest point in July 2021, with almost 283 billion spam emails from a total of 336.41 billion sent emails

9/7/2022

38

# EMAIL BLACKLISTS

- Email Blacklists were developed in an effort to reduce spam being received by users
- Email blacklists is a real-time list of IP addresses and domain names which are known to send spam emails
- There are a number of companies who maintain email blacklists
  - Barracuda
  - Spamhaus
  - Spamcop
- Email Blacklists are used by a number of people
  - Internet Service Providers (Virgin, Sky and Plusnet etc.)
  - Mailbox providers (Hotmail, Gmail)
  - Organisations
- Even though these systems are employed worldwide, spam emails are still very popular.
  - Think of your own personal mailbox!

9/7/2022

39

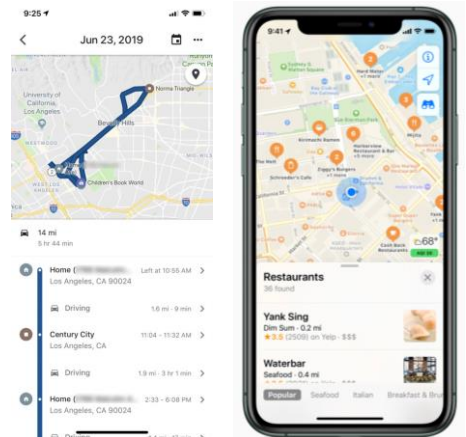


## Geo-location tools for Open Source Investigations

40

# GEO-LOCATION

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

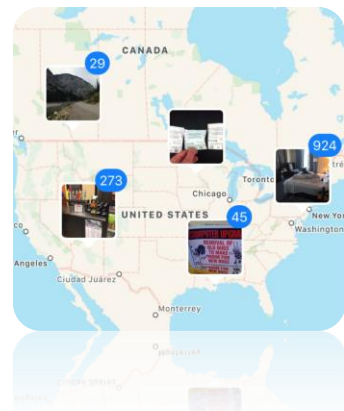


9/7/2022

41

# GEO-LOCATION

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



9/7/2022

42

## EXIF DATA EXERCISE

- During an investigation we have recovered two photographs which are relevant
- The investigation team need to understand more information about the images, such as:
  - What device was used to take the photographs
  - The location he photograph was taken
- This scenario contains two photographs:
  - IMG\_7300.JPG
  - IMG\_3561.JPG
- Using a free online tool, we will see what other information we can obtain from the photograph
  - For this exercise we will use [www.pic2map.com](http://www.pic2map.com)

9/7/2022

43

## EXIF DATA EXERCISE

- Filename: IMG\_7300.JPG



9/7/2022

44

## EXIF DATA EXERCISE

- Filename: IMG\_3561.JPG

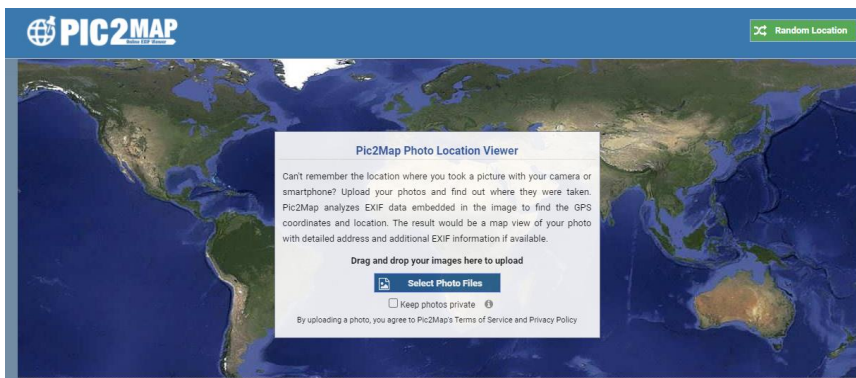


9/7/2022

45

## EXIF DATA EXERCISE

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



9/7/2022

46



# EXIF DATA EXERCISE

- IMG\_7300.JPG

Brand: Apple	Model: iPhone 6	Lens Info: iPhone 6 back camera 4.15mm f.
Shutter: 1/30 (0.0333 seconds)	F Number: f/2.2	ISO Speed: ISO 125
Flash: Not Used	Focal Length: 4.2 mm	Color Space: sRGB
<b>FILE INFORMATION</b>		
File Name: IMG_7300.JPG	Image Size: 1000 x 750 pixels	Megapixels: 0.8 megapixels
File Size: 202,615 bytes (0.20 MB)	MIME Type: image/jpeg	Resolution: 72 DPI
<b>DATE &amp; TIME</b>		
Date: 2015-06-24	Time: 20:30:13 (GMT -04:00)	Time Zone: America / Nassau
<b>GPS INFORMATION</b>		
Latitude: 28.431397	Longitude: -81.473206	Lat Ref: North
Long Ref: West	Coordinates: 28° 25' 53.03" N, 81° 28' 23.54" W	Altitude: 39m. (Above Sea Level)
Direction Ref: True North	Direction: 37.21 Degrees	Pointing: Northeast
<b>LOCATION INFORMATION</b>		
City:	State: Florida	Country: USA
Address: Rosen Inn at Pointe Orlando, Sarnoan Court, Orange County, Florida, 32819-8902, USA (Location was guessed from coordinates and may not be accurate.)		

9/7/2022

47

# EXIF DATA EXERCISE

- IMG\_3561.JPG

Brand: Apple	Model: iPhone 5	Lens Info: iPhone 5 back camera 4.12mm f.
Shutter: 1/15 (0.0667 seconds)	F Number: f/2.4	ISO Speed: ISO 2000
Flash: Not Used	Focal Length: 4.1 mm	Color Space: sRGB
<b>FILE INFORMATION</b>		
File Name: IMG_3561.JPG	Image Size: 1000 x 750 pixels	Megapixels: 0.8 megapixels
File Size: 290,968 bytes (0.29 MB)	MIME Type: image/jpeg	Resolution: 72 DPI
<b>DATE &amp; TIME</b>		
Date: 2014-06-04	Time: 20:56:05 (GMT -05:00)	Time Zone: America / Cancun
<b>GPS INFORMATION</b>		
Latitude: 20.605933	Longitude: -87.092392	Lat Ref: North
Long Ref: West	Coordinates: 20° 36' 21.36" N, 87° 5' 32.61" W	Altitude: 0 (Below Sea Level)
Direction Ref: True North	Direction: 199.76 Degrees	Pointing: South
<b>LOCATION INFORMATION</b>		
City: Playa del Carmen	State: Quintana Roo	Country: Mexico
Address: RIU Yucatán, Avenida Paseo Xaman-Ha, Playacar Fase 2, Bosque Real, Playa del Carmen, Solidaridad, Quintana Roo, 77717, Mexico (Location was guessed from coordinates and may not be accurate.)		

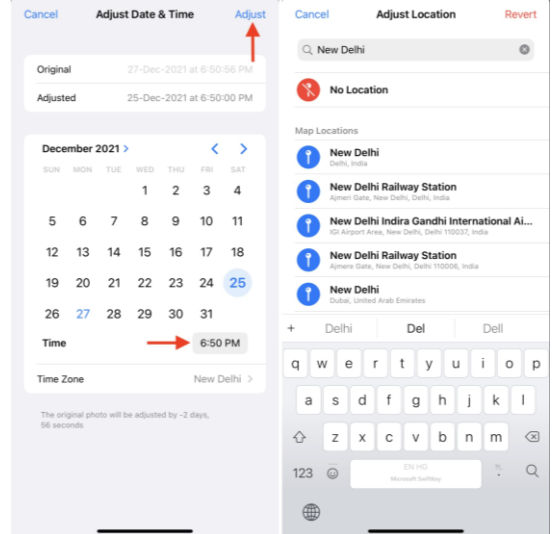
9/7/2022

48



## EXIF DATA REMINDER

- Although most users are not aware of this data, there are also free tools available online which will allow users to:
  - Edit the metadata embedded within a photograph
  - Remove the metadata embedded within a photograph
- As a result, keep in mind that the metadata, including the geo-location data could be altered!
- In iOS16, Apple implemented a feature which allows users to edit EXIF using the Photos application:
  - No specialist tool is required
  - [How to Edit the Metadata for Multiple Photos on iPhone on iOS 16 \(nerdschalk.com\)](https://nerdschalk.com)
- Where possible, may need to be corroborated with other evidence
  - Examine the original photographs
    - Not a copy of the photograph which has been sent through WhatsApp or Facebook Messenger etc.
    - In order to reduce file size, these applications often strip the metadata from files

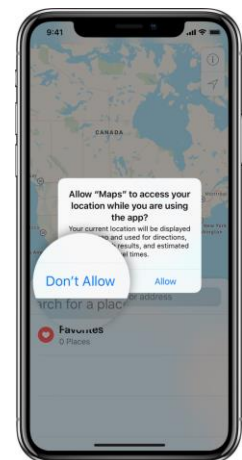


9/7/2022

49

## TWITTER

- Statista forecasts that in 2023, Twitter will have 465 million active users
  - UK Population in 2017 was 66 million people
- Social network commonly used and can be a rich source of information
- Users are often unaware that social media tracks lots of data useful to an investigator
  - A lot of people (myself included) just press "Allow" when installing a new application
- Twitter is one of the social media sites which can track the location of tweets
- A number of free tools which are available online which can be used to search tweets containing geo-location data
  - One Million Tweet Map
  - Geo Social Footprint



9/7/2022

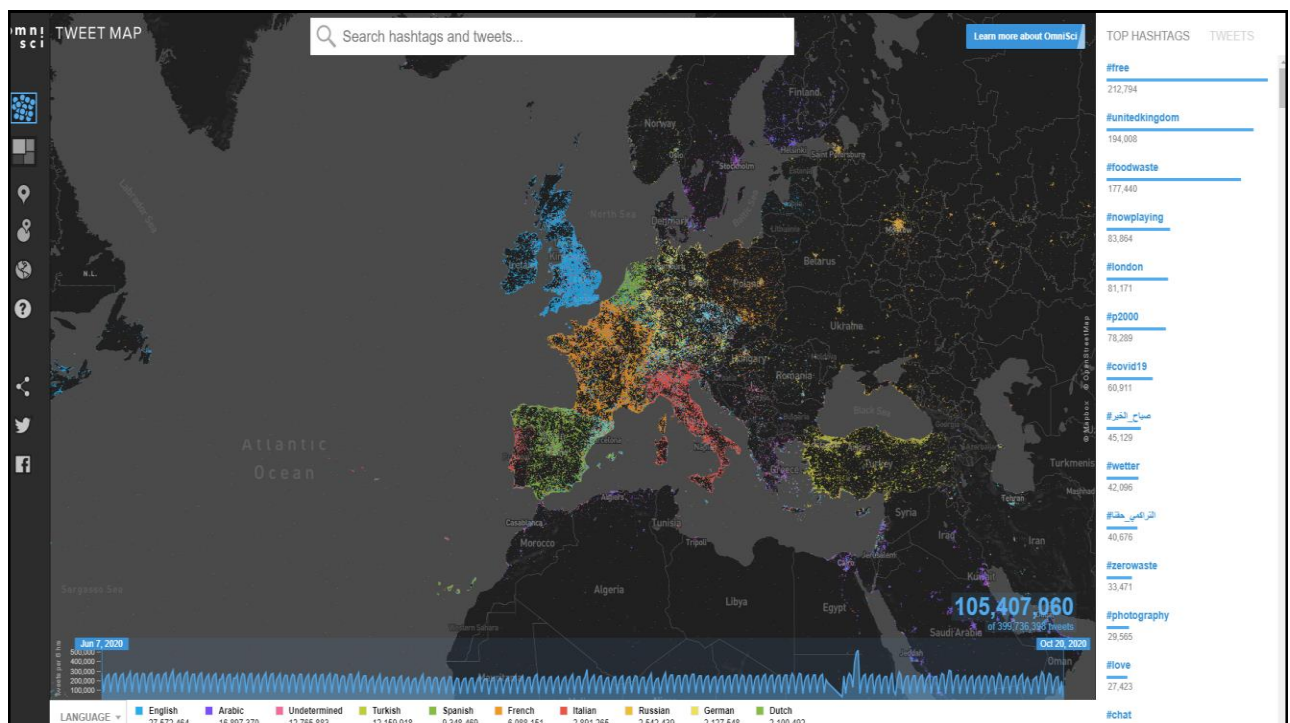
50

# OMNISI

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

9/7/2022

51



52

# GEO-LOCATION (TWITTER) EXERCISE

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

9/7/2022

53

The screenshot shows the TweetMap interface. The main map area displays a map of Newcastle upon Tyne with a search bar at the top containing "@FootballLineups". A red dot on the map indicates a location near Newcastle University. The right sidebar shows a list of tweets from @FootballLineups, including match reports and goals.

**TOP HASHTAGS**    **TWEETS**

- @FootballLineups** · 08/28/2021  
#England #EPL #PremierLeague - #Newcastle 2 vs Southampton 2 Goals: Wilson (head), Elyounoussi, Sai...  
<https://t.co/PpXPNv8FK>
- @FootballLineups** · 02/ 9/2022  
#England #EPL #PremierLeague - #Newcastle 3 vs #Everton 1 Goals: Lascelles (own goal), Holgate (own...  
<https://t.co/r3P13DagQm>
- @FootballLineups** · 02/13/2022  
#England #EPL #PremierLeague - #Newcastle 1 vs #AstonVilla 0 Goals: Trippier (free kick)...  
<https://t.co/wm5w6DG72>
- @FootballLineups** · 08/ 6/2022  
#England #EPL #PremierLeague - #Newcastle 2 vs Nottingham Forest 0 Goals : Schär, Wilson ⚽ T...  
<https://t.co/Hq745oddb>
- @FootballLineups** · 09/ 4/2022  
#England #EPL #PremierLeague - #Newcastle 0 vs #CPFC #CrystalPalace 0 ⚽ TIME POSSESSION : 52 - 48 %...  
<https://t.co/NG3yWH13ak>

Showing 1 - 5 of 5

54



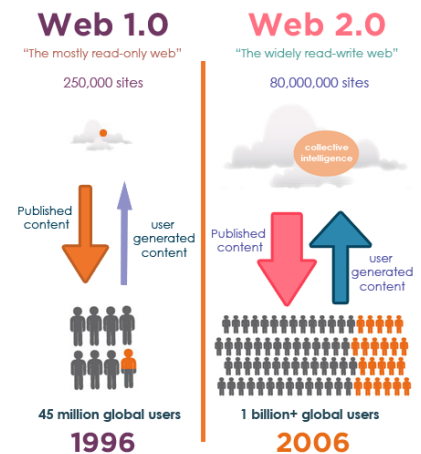
## Investigating Web 2.0 – social networking, blogs and online gaming

55

## WHAT IS WEB 2.0

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

9/7/2022



56

## WEB 2.0 WEBSITES

Examples of web 2.0 websites commonly used:

- Wikis
  - Wikipedia
- Blogs
  - Tumblr
  - WordPress
- Social Networking
  - Facebook
  - Twitter
  - TikTok
- Content Hosting
  - YouTube
  - Flickr
- If there are no tools available specifically for the above websites, consider using the OSIRT browser to record the webpage.

9/7/2022

57

## STEAM (ONLINE GAMING)

- Steam is digital platform owned by Valve Corporation
- Steam is a gaming platform which is used to purchase and play video games on a number of different platforms
  - Windows
  - Mac OS
  - Linux
  - iOS
  - Android
- Usage Statistics
  - PC Gamer reported in Jan 2019 that Steam had 90 million monthly users
  - InputMag reported in Jan 2021 that steam had 120 million monthly users
- Steam has the ability to stream videos and network with other users using chat (group, voice and private chat)
- Steam also has the ability to share video, pictures and tweets too
  - Sharing of tweets may allow us to explore more open source opportunities

9/7/2022

58

# STEAM (ONLINE GAMING)

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

9/7/2022

59

# STEAM USERNAME "NACHO"

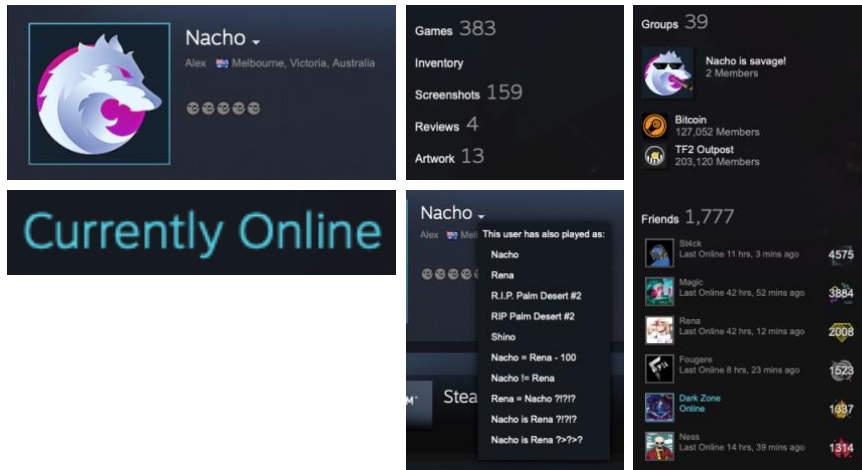
The screenshot shows the Steam profile for a user named 'Nacho'. The profile includes the following information:

- Profile Name:** Nacho
- Level:** 156
- Location:** The City and City
- Favorite Game:** STEAM
- Currently Online:** Badges: 5,352
- Achievement Showcase:**
  - 1,006 Achievements
  - 2 Perfect Games
  - 27% Avg. Game Completion Rate
- Gameplay Showcase:** FIRE & ICE
- Statistics:**
  - Games: 363
  - Inventory
  - Screenhots: 159
  - Reviews: 4
  - Annals: 13
- Groups:** 39
- Friends:** 1,777
- Recent Activity:** Team Fortress 2 (12.6 hours past 2 weeks)
- Recent Game:** The Darker Mass of Labour

9/7/2022

60

# STEAM USERNAME "NACHO"



9/7/2022

61

# INSTAGRAM

- Instagram is a social media platform designed to share images and movies
- Similar to other social networking sites, people are able to follow other users
- Instagram is now owned by Facebook
- Users can lock down their profiles to allow access to only those who follow them
  - **This has an impact on our open source investigation**
- Statista reported in 2019 that Instagram has 1 billion active users each month
- What sort of information can we obtain from a users profile?
  - Posts (Media with captions and tags)
  - Instagram Stories
  - Followers
  - Following
  - Personal bio
  - Tagged posts



9/7/2022

62

# INSTAGRAM EXERCISE

## Instagram Exercise 1

**Step 1)** Visit <https://searchusers.com/>

**Step 2)** Enter "nufc" search for the profile

**Can we see the profile?**

## Instagram Exercise 2

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

**Step 1)** Visit <https://searchusers.com/>

**Step 2)** Enter your Instagram name and review your profile

**Can we see the profile?**

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

The world is becoming more conscious about their online presence

9/7/2022

63

# INSTAGRAM EXERCISE

**1,657** Posts

**14,194** Likes Per Post

**166** Comments Per Post

**Top Hashtags**

- #NFC
- #WOLHEW
- #premierleague
- #OnThisDay
- #paraguay
- #PL
- #Peru

**Most Liked**

**Top User Mentions**

- @jacobmurphy95
- @premierleague
- @yohancabaye\_\_7
- @rodrigoilca10\_

**Most Commented**

9/7/2022

64



# FACEBOOK

- Facebook is another commonly used social network
- Statista reported in Q2 of 2022, Facebook had 2.9 billion monthly active users
- Facebook has the ability to record lots of data about a user
  - Friends
  - Employer
  - Photographs
  - Location data
- Over the years Facebook has been under increased scrutiny regarding how they protect a user privacy
  - This has resulted in user's privacy settings being altered numerous times
  - A large number of accounts are restricted with privacy settings
- Open source with Facebook has become challenging.
- Although challenging, there are a number of sites which provide tools
  - Inteltechniques.com
  - Osintframework.com
- Facebook built in search can be very useful
  - To use this you need an account
- Facebook are strict with accounts (Often close accounts)



9/7/2022

65

# TIKTOK

- TikTok is a social video app that allows users to share short videos.
  - Become very popular during COVID-19 lockdown
- Statista reported that had over 8.9 million active users in the month of January 2022
- The application allows users to comment on videos and also offers private messaging.
- The application is incredibly popular in the UK, as a result as Digital Forensic Investigators we need to understand how the application works and any relevant forensic/open source techniques.
- As the platform is relatively new, techniques are constantly changing

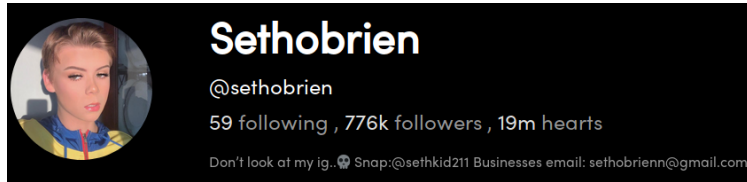
## Video app TikTok fails to remove online predators

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

9/7/2022

66

## TIKTOK EXERCISE



9/7/2022

67

## TIKTOK EXERCISE

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



9/7/2022

68

# TIKTOK EXERCISE

Pages that include matching images

## Seth Obrien - Bio, Facts, Family | Famous Birthdays

[https://www.famousbirthdays.com > people > seth-obrien](https://www.famousbirthdays.com/people/seth-obrien) ▼



300 × 300 - About. Beauty and makeup enthusiast as well as comedic personality on the web who became best known for his **sethobrien** TikTok account. He has accrued ...

## Sethobrien(@sethobrien) on TikTok: I told him #foryou

[https://www.tiktok.com > video](https://www.tiktok.com/video) ▼



100 × 100 - Jul 1, 2019 - Sethobrien(@sethobrien) has created a short video on TikTok with music original sound. I told him #foryou.

## Seth Obrien (@Sethobrienn) | Twitter

[https://twitter.com > sethobrienn](https://twitter.com/sethobrienn) ▼



400 × 400 - The latest Tweets from Seth Obrien (@Sethobrienn): "Heather needed to be put in her place <https://t.co/skSrWCiVlQ>"

9/7/2022

69

# GOOGLE

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

9/7/2022

70

# ONLINE USERNAMES

- In my experience, users often use their usernames across various platforms
- This is often very useful when trying to identify any other platforms of interest
- There are a number of resources freely available online to identify whether a given username is available on a website
  - <https://checkusernames.com> is a useful resource to identify whether the username is used on another website
    - Checkusernames searches 160 social networks
  - [KnowEm Username Search: Social Media, Domains and Trademarks](#)
    - Checks over 500 social networks, similar to checkusernames.com
  - Further verification will then be required on the website to identify further information about the account
  - Google OSINT YouTube and various resources will be returned

9/7/2022

71

**CHECKUSERNAMES.com**  
Check the use of your brand or username on 160 Social Networks:

Search:

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

Navigation: Facebook, Twitter, LinkedIn, Buffer, Hootsuite

YouTube <b>Available</b>	Live Leak <b>Available</b>	APSense <b>Not Available</b>	Intense Debate <b>Not Available</b>
Wikipedia <b>Not Available</b>	Zimbio <b>Available</b>	Folkd <b>Available</b>	Design Float <b>Not Available</b>
LinkedIn <b>Not Available</b>	Houzz <b>Available</b>	Watt Pad <b>Not Available</b>	Stock Twits Ooops, Error
Twitter <b>Not Available</b>	My Space <b>Available</b>	Empire Avenue <b>Available</b>	Fotki <b>Available</b>
Ebay <b>Available</b>	Game Spot Ooops, Error	Spark People <b>Available</b>	Trend Hunter <b>Not Available</b>
Tumblr <b>Available</b>	Cracked Ooops, Error	N4G Ooops, Error	Ads Of The World <b>Available</b>
Pinterest <b>Available</b>	Behance <b>Available</b>	Veoh Ooops, Error	Eventful Ooops, Error
Blogger <b>Available</b>	Sky Rock <b>Available</b>	Ebaums World <b>Available</b>	Tiny Chat Ooops, Error
Imgur <b>Not Available</b>	Vitideo <b>Not Available</b>	Dzone Links <b>Not Available</b>	Shock Wave <b>Available</b>
Flickr <b>Not Available</b>	We Heart It <b>Available</b>	Mouth Shut <b>Available</b>	Active Rain <b>Not Available</b>
Word Press <b>Not Available</b>	Fan Pop <b>Available</b>	Yuku <b>Available</b>	Destructoid Ooops, Error
Daily Motion <b>Available</b>	Dreams Time Ooops, Error	Fark <b>Available</b>	Boonex <b>Available</b>
Reddit Ooops, Error	I Can Has Cheezburger? Ooops, Error	Blog Talk Radio Ooops, Error	Tech Dirt Ooops, Error
CNET Ooops, Error	Meta Cafe Ooops, Error	Zedge <b>Not Available</b>	Jigsy <b>Available</b>
Vimeo <b>Available</b>	Last FM Ooops, Error	Dat Piff Ooops, Error	The Hype Machine <b>Available</b>
Slide Share <b>Available</b>	H5 <b>Not Available</b>	Wonder How To <b>Available</b>	Moby Picture <b>Available</b>
Deviant Art Ooops, Error	The Motley Fool <b>Available</b>	Crunchy Roll Ooops, Error	Wall Inside <b>Not Available</b>
Live Journal <b>Available</b>	Fkya <b>Not Available</b>	8 Tracks Ooops, Error	Programmable Web Ooops, Error
Yelp <b>Not Available</b>	Kongregate <b>Available</b>	Red Bubble <b>Available</b>	All My Favos Ooops, Error
Wikia <b>Available</b>	My Fitness Pal Ooops, Error	Bitly <b>Not Available</b>	Bigger Pockets <b>Available</b>
Armchair GM <b>Available</b>	Ultimate Guitar Ooops, Error	Photo Dune Ooops, Error	Kiva <b>Not Available</b>
Fiverr <b>Not Available</b>	Dribbble <b>Not Available</b>	Wanelo Ooops, Error	Blurb <b>Available</b>
Etsy <b>Available</b>	Toro Ooops, Error	Active <b>Not Available</b>	Fat Secret <b>Not Available</b>
Ask FM <b>Not Available</b>	Instructables <b>Not Available</b>	Colour Lovers Ooops, Error	Carbon Made <b>Not Available</b>
Source Forge <b>Available</b>	500px Ooops, Error	Listal <b>Available</b>	Element14 Ooops, Error
Wiki How <b>Not Available</b>	Gravatar <b>Not Available</b>	Toluna Ooops, Error	Map My Run Ooops, Error
Sound Cloud Ooops, Error	Reverb Nation <b>Not Available</b>	Soup Ooops, Error	Cool Spotters Ooops, Error
Photo Bucket Ooops, Error		Flight Aware <b>Available</b>	

72

## OPEN SOURCE INVESTIGATION CHALLENGES

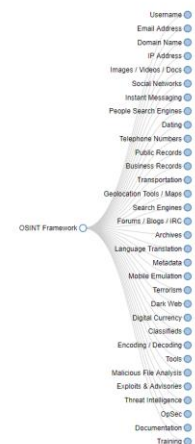
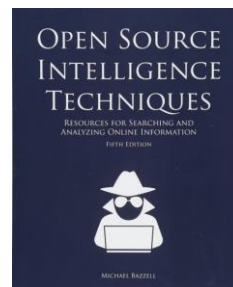
- There are a number challenges in relation to open source investigations
  - Legislation (cross-borders)
  - Online platforms regularly change their functionality
    - It is not uncommon for applications to update on a weekly basis
    - As a result, a tool that worked yesterday, may not be able to interpret the data today
    - Support for tools is limited – may be taken offline with no notice
  - New social networks and applications
  - Privacy settings
    - Privacy is a fundamental part of peoples lives
  - Data is online and real-time
    - Data can easily be deleted or hidden by users, capturing the data at the earliest opportunity is important
    - Consider the Wayback Machine

9/7/2022

73

## RESOURCES

- [The Ultimate OSINT Collection - start.me](#)
- OSINT Framework
- Open Source Intelligence Techniques – Book
- UK-OSINT
- Inteltechniques.com



9/7/2022

74

THANK YOU  
ANY QUESTIONS?

Seanpaul Gilroy





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

### (POST)COVID CHALLENGES INCRIMINAL JUSTICE: INVESTIGATING WEB 2.0

Bucharest  
19-20 September 2022

Co-funded by the Justice Programme of the European Union



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



## Ransomware

- Ransomware was once again the primary overall cybercrime threat. The threat and damage potential increased noticeably again in 2021.
- 2021 was characterized by attacks on critical infrastructures, public administration and international supply chains. In addition to monetary damage, such attacks also impair the ability of the community to function.
- The damage potential of ransomware is increasing rapidly.
- Annual damage caused by ransomware

2021: approx. € 24.3 billion

2019: approx. € 5.3 billion



# The Emotet investigation



# The Emotet investigation

## EMOTET takedown

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

Emotet opened doors for:

Trojans

Ransomware

Information stealers

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

How did Emotet work?

**Luring the victims**

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

**Installation**

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

**Infection**

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





## The beginning of the investigation

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



## The beginning of the investigation

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



## Who has been affected in Germany?

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



## The Emotet investigation





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

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



## Coordination of international cooperation



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



## Challenges and solutions

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

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



## Challenges and solutions

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

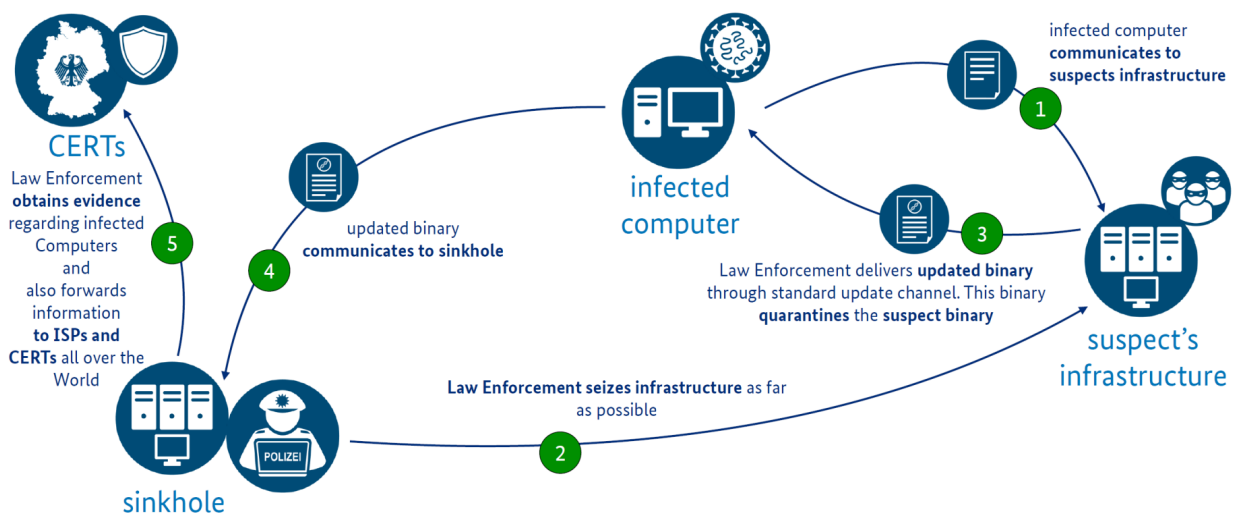
- **„ hybrid court order" with elements of seizure, as well as the usage of the so-called annex competence with extension to systems newly discovered through technical measures**

## Challenges and solutions

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

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

## Challenges and solutions



## State of play

- **Takeover of the bot net through joint action within the framework of the international action day on 01/26/2021**
- **Searches of the accused and two witnesses in Ukraine with subsequent interrogations**
- **Seizure of servers in Germany (victim control site, distribution site and unique bots) as well as in NL, USA, Canada, UK, France, Lithuania and Ukraine**
- **Evaluation of the data is ongoing – as well as the chase...**

## Online Child Sexual Abuse

## What has the COVID-19 pandemic changed?

- The global impact of COVID-19 means people are spending more time online. This includes both children and adults.
- Adults working remotely are less able to spend time with their children, who are allowed greater unsupervised internet access. As a result, children are:
  - more exposed to offenders through online gaming, the use of chat groups in apps, unsolicited contact in social media and through less secure online educational applications;
  - more inclined towards making explicit material to exchange with peers, eventually reaching child sex offenders;
  - in some cases, becoming lonely and isolated, which offenders try to benefit from, connecting with them to produce explicit material or to arrange a meeting in real life.

17

## 2021 trends

- There has been a steep increase in online grooming activities on social media and online gaming platforms.
- The production of selfgenerated material is a key threat. This material is displaying increasingly younger children.
- The Dark Web remains an important platform for the exchange of child sexual abuse material (CSAM).

18

## 2021 trends

- There has been a steep increase in online grooming activities on social media and online gaming platforms.
- The production of selfgenerated material is a key threat. This material is displaying increasingly younger children.
- **The Dark Web** remains an important platform for the exchange of child sexual abuse material (CSAM).

## Case study - the Dark Web as the major enabler for the dissemination of CSAM:

### The „ELYSIUM“-investigation

- At the beginning of 2017, the Australian police took over the account of the moderator of the website The Giftbox Exchange on the Darknet and came across a German who was already planning another CSAM site called “Elysium”.
- The Cybercrime Prosecution Centre of the State of Hesse (ZIT), a specialized unit of the General Public Prosecutor's Office in Frankfurt am Main took over the investigation.
- In June 2017, the site Elysium was shut down by the authorities. So far, 14 suspects and 29 victims have been identified and images have been found that pointed to perpetrators in Germany.





## The „ELYSIUM“-investigation

- After locating the server of the Elysium platform, German law enforcement commenced electronic surveillance of the server and defendant one as well as undercover operations.
- The surveillance measures included uploading avatar images to confirm the server location as well as surveillance of messages sent.
- This helped identify defendants one and two.
- Additionally, in 2016 the German Bundeskriminalamt was sent abuse images of defendant three from which the image of a fingertip and, hence, the fingerprint of the abuser could be deduced thereby identifying defendant three.
- 
- By locating an in-memoriam site for the at-that-point-already-arrested defendant one, defendant four could be identified.

21



## The „ELYSIUM“-investigation

- The well-documented case involved the dissemination of child sexual abuse material via darknet forums by an organized criminal group as well as the sexual abuse of children by the members of the group.
- The defendants in this case had been part of the online pedophile scene before they got together with several other separately prosecuted offenders to create private forums and chat rooms, including the Giftbox Exchange and Elysium.

22



# The „ELYSIUM“-investigation



**Cybercrime**

**Computer-related specific acts**

- Production/distribution/ possession of child pornography

**Keywords**

- Child online abuse
- Electronic Evidence

BGH, Beschluss vom 15.01.2020, 2 StR 321/19



## Fact Summary

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



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

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

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



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

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

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



## **Online Fraud**



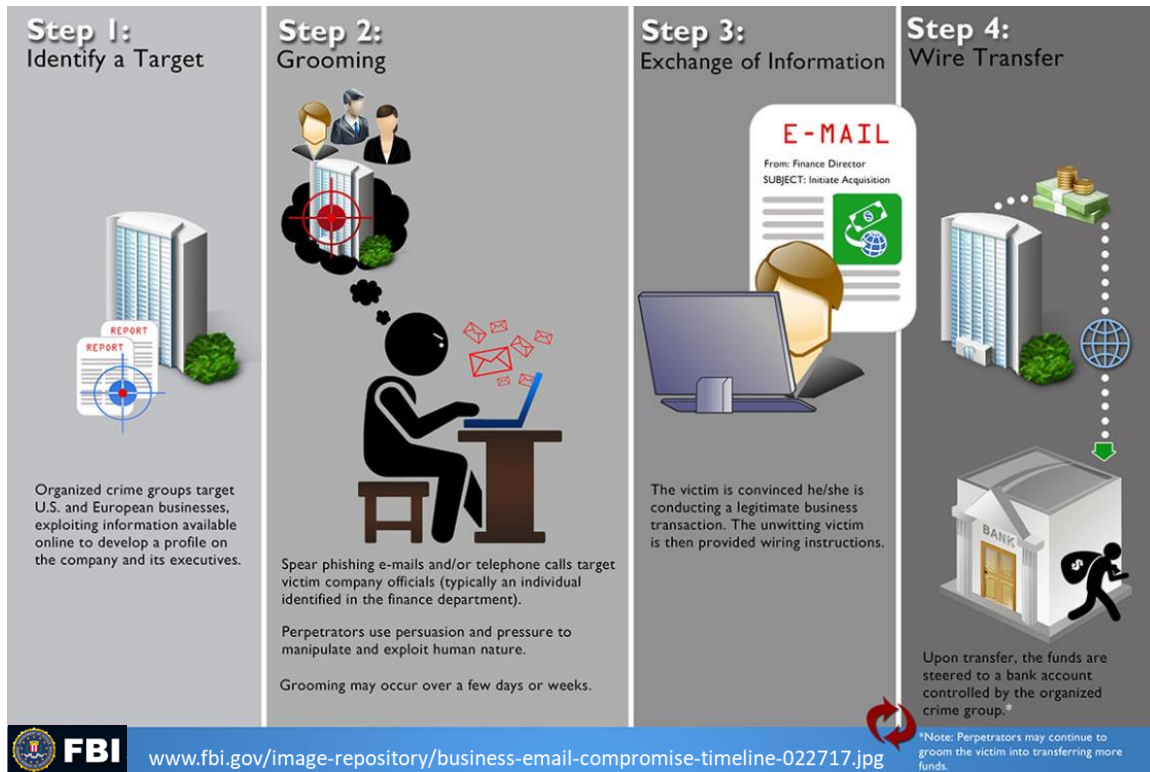
## Online Fraud

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



## Business Email Compromise (BEC)

- **BEC is defined as a fraud targeting businesses that regularly perform wire transfer payments.**
- **The scam is carried out when perpetrators compromise e-mail accounts through social engineering or through computer intrusion techniques to fraudulently direct electronic fund transfers.**



## Social engineering attacks – CEO fraud

- A refined variant of spear phishing, CEO fraud, has evolved into a key threat as a growing number of businesses are targeted by organised groups of professional fraudsters.
- CEO fraud is a scam in which cybercriminals spoof company email accounts and impersonate executives to try and fool an employee in accounting or HR into executing unauthorized wire transfers, or sending out confidential tax information.
- Successful CEO frauds often result in significant losses for the targeted companies.



## CEO-fraud: Example

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

Hi [REDACTED]

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

Bank Name: Deutsche Bank Europe S.A.

USD:

Account Name: [REDACTED]

IBAN : PLO [REDACTED]

BIC/SWIFT [REDACTED]

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

Thank you,

Michael



## CEO-fraud: Example

Von: Michael [REDACTED]  
Gesendet: Montag, 28. März 2016 17:36  
An: [REDACTED]  
Cc: [REDACTED]  
Betreff: RE: Payment [REDACTED] to [REDACTED]

Hi [REDACTED]

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

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

Thanks

Michael



*Thank you for your attention!*

*Questions? Remarks?*

**Cybercrime Division**



**Ministry of Justice, State of Hesse, Germany**









# Digital Evidence “hidden in the Cloud”

-

## Contemporary Legal Challenges

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



Co-funded by the Justice Programme  
of the European Union

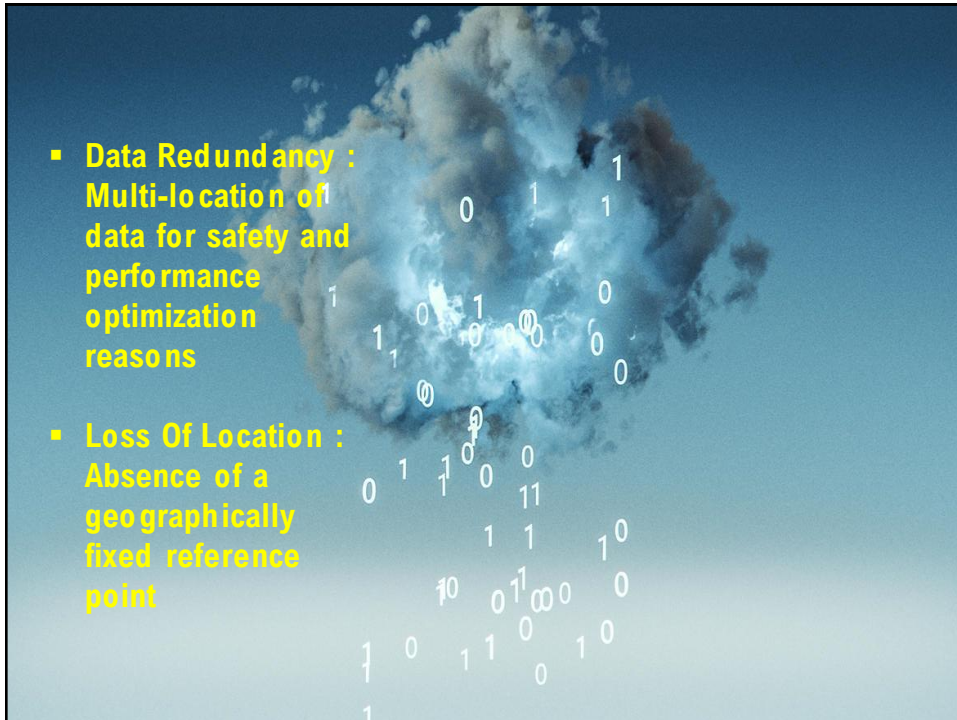
1



### «The Cloud»:

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



3



4



## A] Data Territoriality and Applicable Law

- Criminal Event Theory
- Criminal Instrument Theory
- Direct Consequence Theory
- Nationality Theory

5

## B] “Possessing” Cloudly Stored Data

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

6

## C] Obtaining 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

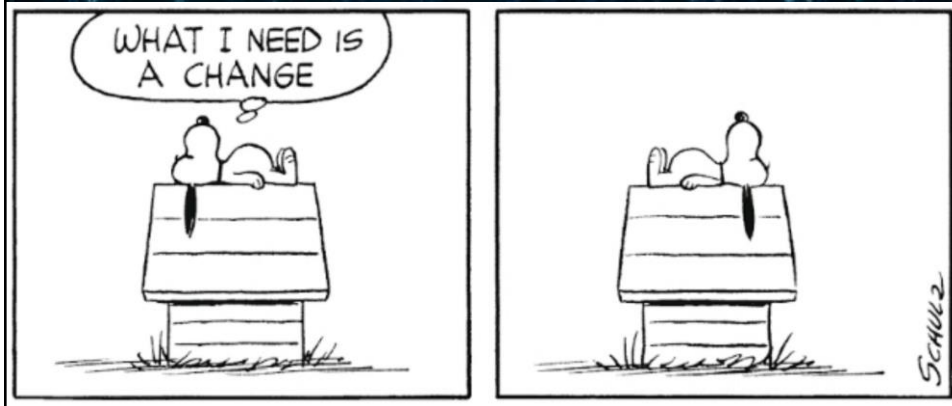
## C] Obtaining Digital Evidence In The Cloud (2)

- 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 : rapidly issued judicial requests that can be served directly on Cloud Storage Providers or on their legal representatives, where they exist

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

https://www.mdpi.com/2070-2409/12/5/101/htm

MDPI 25th Anniversary Journals Information Author Services Initiatives About Sign In / Sign Up Submit

Search for Articles:  Title / Keyword  Author / Affiliation  Information  All Article Types  Search Advanced

Journals / Information / Volume 12 / Issue 5 / 10.3390/info12050181

01010  
01010  
01010 **information**

Submit to this Journal  
Review for this Journal  
Edit a Special Issue

**Article Menu**

Article Overview

Article Versions

Related Info Links

K

Open Access Article

**Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal**

by Christos Karagiannis <sup>1,2</sup> and Kostas Vergidis <sup>1,\*</sup>

<sup>1</sup> Department of Applied Informatics, University of Macedonia, 54636 Thessaloniki, Greece  
<sup>2</sup> Prosecutor of the Court of First Instance, 11222 Larissa, Greece  
\* Author to whom correspondence should be addressed.

Academic Editor: Georgios Kambourakis

*Information* **2021**, *12*(5), 181; <https://doi.org/10.3390/info12050181>

Received: 31 March 2021 / Revised: 19 April 2021 / Accepted: 20 April 2021 / Published: 22 April 2021

11



12



# Handling e-evidence from a technical point of view

**(POST) Covid Challenges in Criminal Justice:**

**Investigating Web 2.0**

Bucharest

19-20 September 2022



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

1

## About the speaker

- Victor Voelzow
- Police Officer since 2001
- Working in Digital Forensics since 2007
- MSc Forensic Computing and Cybercrime Investigations (UCD, Ireland, 2011)
- Trainer at Hesse State University for Public Management and Security
- Vice-Chair of European Cybercrime Training and Education Group (ECTEG.eu)
- Projects, trainings, guides for different national and international organisations, e.g.:



2

## Agenda



1. First Responder's E-Learning
2. Value of Live Data Forensics
3. Value of Memory Forensics
4. Encryption as challenge

3

## 1. First Responder's e-learning

The “first responders e-learning” package is an **interactive online** training course which focuses on essential IT forensics and IT crime knowledge for **first responders**.

It is adapted to different EU languages (+ Arabic and Thai with collaboration of UNODC and the Council of Europe) and the different national legislations



4



# 1. First Responder's e-learning

Driver : **ECTEG & Portuguese Judicial Police**

Funded by the EU Commission

In cooperation with CEPOL, CoE, UNDODC and Europol



5

# 1. First Responder's e-learning

Who is a First Responder?

Each police officer:

- On the field (patrol, house search)
- At the office, when taking victim's complaint
- During the investigation

They might be the first ones to be in contact with possible **digital evidence**.

**BUT:**

e-First may also be interesting for prosecutors and judges



6

# 1. First Responder's e-learning

There are over 1,5 million Law Enforcement users only in EU:

- Not well skilled on new technologies
- Not all able to acquire knowledge in English
- Not available for usual course attendance



7

# 1. First Responder's e-learning

## Languages









<b>Algerian</b>	<b>Norwegian</b>
<b>Danish</b>	<b>Moroccan</b>
<b>English</b>	<b>Portugese</b>
<b>Finnish</b>	<b>Tunisian</b>
<b>French</b>	<b>Romanian</b>
<b>German/Austrian</b>	<b>Spanish</b>
<b>Greek</b>	<b>Swedish</b>
<b>Italian</b>	<b>Thai</b>
<b>Lebanese</b>	
<b>Polish</b>	



8

# 1. First Responder's e-learning

## Aims

	Understand the importance of electronic evidence
	Identify and seize items with potential electronic evidence
	Do urgent measures to preserve (electronic) traces
	Protect evidence integrity
	Live Data Forensics whenever needed
	Welcome & correctly support victims
	Case specific victim aid & advice
	Contribute to citizen awareness and crime prevention

9

# 1. First Responder's e-learning

## Contents

- Definitions, explanations of devices and phenomena.
- Guidelines for search and seizure of electronic evidence.
- Case-Games: Interactive criminal investigations, covering several topics and related to phenomena such as Darkweb and crypto currencies, fake identity on Social Networks, Phishing ...
- Quizzes and Tests Materials and resources ...

10

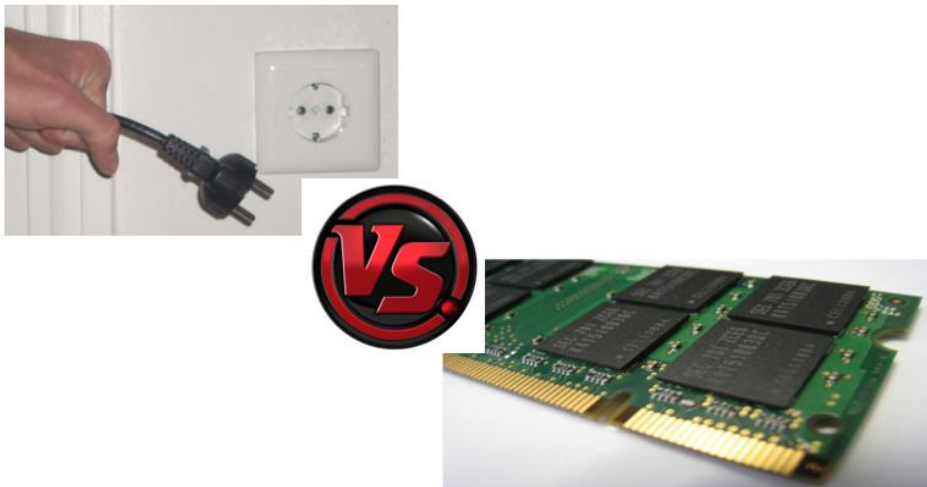
## Demo



Picture source: [http://clipart-library.com/clipart/demo-cliparts\\_2.htm](http://clipart-library.com/clipart/demo-cliparts_2.htm)

11

## 2. Value of Live Data Forensics



12

## 2. Value of Live Data Forensics

### What is Live Data Forensics?

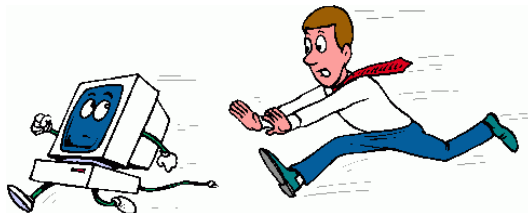
Live Data Forensics deals with situations where it is necessary to capture **volatile data** from devices before they are turned off or disconnected from networks or power supplies.

It requires a higher level of specialism than the procedure in the search and seizure of dead boxes because the possibility of altering or even overwriting evidence is very high.

13

## 2. Value of Live Data Forensics

### What are volatile data?



Volatile Data are data, digitally stored in such a way, that the probability is very high for the contents to be deleted, overwritten or altered in a short amount of time by human or automated interaction.

14

## 2. Value of Live Data Forensics

### Examples for volatile data

- Caches (e.g. arp- and dns-caches)
- Unsaved documents
- Running processes
- **Passwords and encryption keys**
- Open network connections
- Private Browsing History
- Logged in users
- Temporarily connected remote storage
- Malware binaries only stored in RAM



Picture source: <https://freesvg.org/hdd-crypt>

15

## 2. Value of Live Data Forensics

### Two types of volatile data

- **Volatile Data on the Physical Computer** like open network connections, running processes and services, arp- and dns caches.
- **Transient Data** that are not volatile in their nature but are only accessible on scene. Encrypted volumes as well as remote resources are examples for this kind of data. The characteristic of these data is that the contents of the data might get inaccessible, altered or deleted after the search, if the investigator is not be able to acquire them.



16

## 2. Value of Live Data Forensics



### 1.7.1 Principle 1 – Data Integrity

**No taken action should materially change any data, electronic device or media which may subsequently be used as evidence in court.**

- Electronic devices and data must not be changed, either in relation to hardware or software. The person in charge of a crime scene, or for collecting the evidence, is responsible for maintaining the integrity of the material recovered and for ensuring the forensic chain of custody. Subsequent custodians of the devices and/or data must assume that responsibility.
- In cases where data cannot be acquired without the risk of changing other data (i.e. on running devices or on flash storage), this must be done in the manner that causes the least impact on the data and by a person qualified to do so. Principles 2 to 5 apply if this course of action is found to be necessary.

Source: Council of Europe – Electronic Evidence Guide 3.0 (2022) - <https://www.coe.int/en/web/octopus/training>

17

## 2. Value of Live Data Forensics

**Handling live data brings the following added values:**

- Avoid loss of volatile data
- May save unsaved documents, private browsing history
- May help securing crypto assets
- May help with decrypting encrypted data or disks
- May reveal further investigative leads
- May provide fast answers in time-critical cases

18

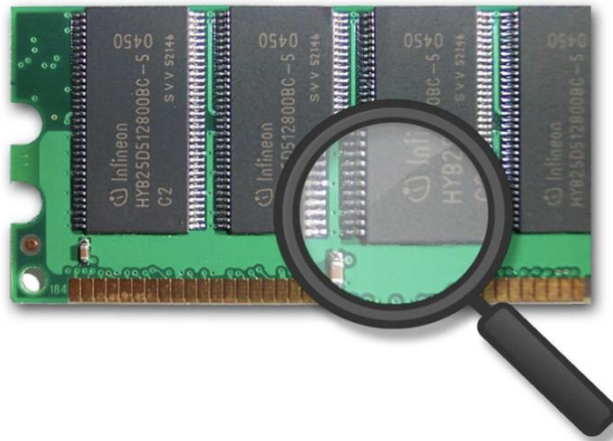
## Demo



Picture source: [http://clipart-library.com/clipart/demo-cliparts\\_2.htm](http://clipart-library.com/clipart/demo-cliparts_2.htm)

19

## 3. Value of Memory Forensics



20



### 3. Value of Memory Forensics

#### Information of potential interest

- File contents
  - Images / Video / Audio
  - Documents
  - Text
- Process / system information
  - Running Processes
  - Network Connections
  - (Malicious) Code
- Password Hashes
- Encryption Keys
- User Activity
- Timeline

21

#### Demo



Picture source: [http://clipart-library.com/clipart/demo-cliparts\\_2.htm](http://clipart-library.com/clipart/demo-cliparts_2.htm)

22

## 4. Encryption as a challenge



Picture source: <https://freesvg.org/hdd-crypt>

23

## 4. Encryption as a challenge

Encryption can be found always everywhere:

- Built-in Full Disk Encryption on client and server computers, using e.g. Windows Bitlocker, macOS FileVault&APFS, Linux dmCrypt&Luks
- Mobile devices, e.g. iPhones, Android devices, cryptophones
- Files, eg. ZIP, PDF, DOCX
- Encrypted containers/drives, using e.g. Veracrypt
- Encrypted network traffic

24

## 4. Encryption as a challenge



- Detecting encryption
- Success of attacks depends on many factors, e.g.
  - Device used
  - Encryption software & algorithm
  - Strength of password
  - Strength of Dictionaries
  - Power of decryption platform
  - Availability of attack vectors

Picture source: Flickr, Vorstius, <https://www.flickr.com/photos/48321643@N00/>

25

## Questions?



Please ask!

26





# Challenges in collecting e-evidence

---

ENELI LAURITS

Co-funded by the Justice Programme of the European Union



## Setting the stage

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



## 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.



## Digital evidence

- Is latent, like fingerprints or DNA evidence;
  - Crosses jurisdictional borders quickly and easily;
  - Is easily altered, damaged, or destroyed;
  - Can be time sensitive.
- 
- Which issues might this raise in courts?



# Convention on Cybercrime

## 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.**



# 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.



## Publicly available data

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, is regularly determined by areal considerations.



## Publicly available data

- In *US v Auernheimer*\* the defendant was convicted of unauthorised access for collecting information from a website of US telecommunication provider AT&T 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 analogous to a home where 'the front door is left open or unlocked' the data was still protected.
- Courts are increasingly starting to presume that publication of data 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/>>





## Social media evidence – publicly available?

- Social media evidence includes, among other things, photographs, status updates, a person's location at a certain time, and direct communications to or from a certain social media account.
- Facebook—and social media generally—present novel questions regarding their users' expectations of privacy. Facebook users may decide to keep their profiles completely private, share them only with “friends” or more expansively with “friends of friends,” or disseminate them to the public at large.



## Social media evidence – privacy concerns

- When a social media user disseminates his postings and information to the public, they are not protected for privacy. However, postings using more secure privacy settings reflect the user's intent to preserve information as private.
- When a person with a public privacy setting tweets, he or she intends that anyone that wants to read the tweet may do so, so there can be no reasonable expectation of privacy.



## United States v. Meregildo

Governments collected evidence by using a cooperating witness who was one of suspects' Facebook "friends" and gave the Government access to suspects' Facebook profile.

To which extent can one say that his social media account is private?  
Could it be at some circumstances be seen as publicly available information?

**Could LEA collect such data without any further authorisation?**



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

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.



- 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 is 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.**



## 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?**



# Social media evidence

Social media is subject to same rules of evidence as paper documents or other electronically stored information, but the unique nature of social media as well as the ease with which it can be manipulated or falsified creates hurdles to admissibility not faced with other evidence.

## Methods of authentication include:

1. presenting a witness with personal knowledge of the information (they wrote it, they received it, or they copied it),
2. searching the computer itself to see if it was used to post or create the information, or
3. attempting to obtain the information in question from the actual social media company that maintained the information in the ordinary course of their business.



# Social media evidence

There are two distinct types of authentication that must occur for evidence from social networking sites.

1. One is to authenticate the authorship of the evidence on the website.
2. The other is to authenticate that the exhibit used at trial, typically a printout of the webpage, is a fair and accurate representation of what was on the computer screen.

Testimony by a witness who viewed the information on the website is usually sufficient to meet the latter requirement.



- The fact that a witness held and managed an account does not provide enough of a foundation for authentication; the proponent must show that the communication in question came from the witness and “not simply from her Facebook account.”
- Courts have raised concerns because social networking accounts may be compromised by hackers and anyone may create a fictitious account under another’s name. In addition, users “frequently remain logged in to their accounts while leaving their computers and cell phones unattended,” raising the likelihood of third parties creating unauthorized posts.



## Collection of extraterritorial data

### Convention on Cybercrime

#### 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.**



# 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.**



## Example

Judge/prosecutor has authorised a house search and seizing all electronic devices in order to collect digital data from them, including correspondence between the suspect and A.

You arrive at the place where the search is authorised and you discover that the computer is working and e-mail account is open. This is a mail.ru account.

You see that there are multiple letters between your suspect and A.

There is reason to suspect that the suspect is using encryption.

**What will you do?**



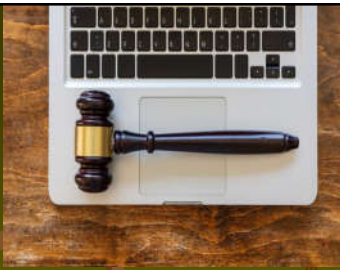
THANK YOU!

Co-funded by the Justice Programme of the European Union










With financial support of the Justice Programme 2014-2020 of the European Union

Managing traditional physical evidence electronically: towards videoconference witness examinations, electronic criminal files and online remote trials.

Andrea CRUCIANI  
Judge at Court Martial of Naples

1

## Online remote trials in response to Covid-19



- On line remote trials as an alternative to adjournments of trials during Covid-19 pandemic:
- 1) 9 march 2020 - 31 July 2020: remote trials even without parties consent (needed for closing statements and witnesses examination) or for detainees.
  - No need for the parties and the judge to be present in court.
  - Defence lawyers certifies the identity of the defendant (when not a detainee). For detainees, lawyers may be present at the detention center or take part in the trial remotely (guaranteeing private consultations with the client).

2

2) up to 31 december 2021: remote trials only with parties consent (never allowed for closing statements and witnesses examination) or for detainees.

3) up to 31 december 2022; no remote trials (except for detainees, in which case all the parties may ask to take part in the trials remotely).

3

## Getting started...

- Microsoft Teams application.
- Creating a Team-Channel for each single proceeding;
- Inviting by e-mails all the parties to the Teams dedicated channel communicating the guest-link ("Join Microsoft Teams Meeting").
- Checking the quality of the connection and giving specific instructions on the functioning of remote trials.
- ['I'm not a cat': lawyer gets stuck on Zoom kitten filter during court case - YouTube](#)
- Technical issues vs. Notifications issues. Adjournment of the trial (only in the absence of essential parties: not always injured party/offended party);
- The role of consent in criminal proceedings (except for detainees) vs. civil proceedings.
- Public hearings. Members of the public may attend a virtual hearing (microphones and cameras turned off) with e-mail invitation-link by the register.

4

## Evidence presentation. Electronic evidence.



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

Remote trials: e-evidence may be uploaded in the documents file of the M.Teams channel. Expert witness.

5

## Witnesses



Even before Covid 19 videoconference was allowed to examine detainees and protected witnesses: security reasons and time/cost effective measure.

During Covid 19 witnesses on videoconference was allowed only in the first phase and with parties consent.

Confrontations and recognitions must always be proceeded in presence.

6

## guidelines

- Witness failing to appear by videoconference? Subpoenas or order to appear (fine or physically escorted by the police);
- Recommendations to the witness not to use scripts, notes, documents (without authorization of the judge) or to be assisted by another person;
- Authorized documents are presented to the witness on the uploaded files on Teams or with screen-sharing functionality;
- In case of confidential information break-out rooms may be used to exclude virtual attendees who are not entitled to hear such information.
- Need for clear and shared rules and guidelines.

7

## *Avsenew v. State of Florida*

The defendant was found guilty of first-degree murder by the trial court and sentenced to death largely due to the testimony of his mother, Jeanne Avsenew. However, Ms. Avsenew was unable to attend the trial in-person due to a serious health condition, and so appeared remotely via virtual conferencing technology.

While she could view the courtroom, she was unable to see the defendant during her testimony, an arrangement found by the Supreme Court of Florida to violate Florida Rule of Criminal Procedure 3.190(i), and the inclusion of Ms. Avsenew's testimony was found not to be a harmless error.

As a result, the Supreme Court of Florida reversed the ruling by the trial court and remanded to the circuit court for a new trial.

8

## Physical evidence



- **Documents.** Criminal justice system is moving towards e-files (police criminal reports; witnesses statements; defensive investigations); e-files are directly uploaded in Teams. When documents are not in an electronic format they must be first scanned in pdf and then uploaded;
- DNA samples; finger prints; drugs; weapons or ammunitions are all presented by photographs and expert witness;
- Challenges on physical evidence may require the parties to be present in-person;

9

## Closing statements and judgement reading.



- **Technically possible** (members of a panel take the decision in a videoconference chamber; screen-sharing functionality for judgement reading) **but...human factor or rituality of the court room** (especially in sensitive cases. Capital punishment verdicts on Zoom in Singapore and Nigeria have been heavily criticised).

10

## Conclusions



- All in or all out approach;



### ■ Remote trials work fine:

- Detainees (sure identity; connection quality; no costs for police escorting; security) and protected witness;
- Public emergencies (pandemic, wars...)
- Consent;
- Distant parties and lawyers;
- Technical hearings with few parties and no public (preventive measures; pre-trial confirmation hearings; trial scheduling hearings; evidentiary hearings); more speedy and efficient;



### ■ Remote trials more problematic:

- Confrontations and recognitions;
- Challenges on admissibility/reliability of evidence;
- Closing statements;



## The proposed European Production Order (EPO) and its effectiveness in collecting evidence

(POST)COVID CHALLENGES IN CRIMINAL JUSTICE: INVESTIGATING WEB 2.0

1

20 September 2022

The proposed European Production Order (EPO) and its effectiveness in collecting evidence

### 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 Position, Volunteered:

- CISO EQUANS
- Judge at the criminal court of Zeeland West-Brabant
- Legal advisor, Policy Officer cybercrime and digital investigations at the Dutch Police



2

2

Titel  
Datum 9 mei 2021

1

## Guideline

- Introduction and some figures
- Mutual Legal assistants
- Difficulties in investigating (Cyber)crime
- European Production Order and Preservation Order
- Case study

Cybercriminals are increasing efficiency with coordinated attacks

## We are under attack

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

Figure 1: OMEA Threat Landscape 2021 - Overview



- Ransomware has been assessed as the prime threat for 2020-2021.
- Cybercriminals are increasingly motivated by monetization of their activities, e.g. ransomware.
- Malware decline that was observed in 2020 continues during 2021.
- The volume of crypto jacking infections attained a record high in the first quarter of 2021, compared to recent years.
- COVID-19 is still the dominant lure in campaigns for e-mail attacks.
- 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 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 2020 were caused by errors.

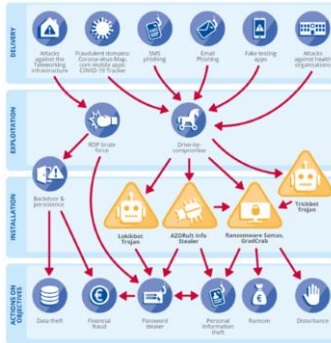
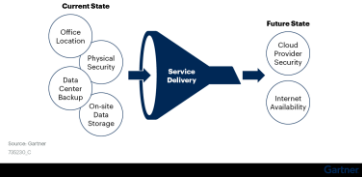
- January: Microsoft Exchange Server data breach
- April: Over 500 million Facebook users' personal info was discovered posted on a hackers' website
- April: The Ivanti Pulse Connect Secure data breach of unauthorized access to the networks
- May: Operation of the U.S. Colonial Pipeline is interrupted 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.



### Near future, post Covid 19

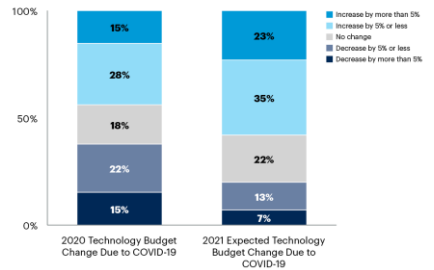
During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface."

#### Evolving Dependency Landscape



#### Expected Changes in Technology Budgets

Percentage of Respondents



### Developments

### Achievements

**Pollitie zoekt tientallen IT'ers, hackers en analisten**  
 Het nieuwe tijdperk van criminaliteitsbestrijding. Met die slogan zet de federale politie een reeks vacatures in de markt. De rekruken van de speciale eenheden worden geen zwakbrennende mannen in gepanzerde trucks, maar computerspecialisten.



#### 'Investeer in aanpak cybercrime'

**Nederland:** Cybercrime, maar ook opdigitaleisde normen van 'karakter' online vergrijpen nemen fors toe. In het eerste kwartaal van 2022 zag de politie een verduubing van het aantal geregistreerde digitale misdrijven ten opzichte van het jaar ervoor. Vooral oplichting via WhatsApp en fraude in de online handel springen eruit.



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

7

7

## General Principles International Cooperation in Criminal Matters

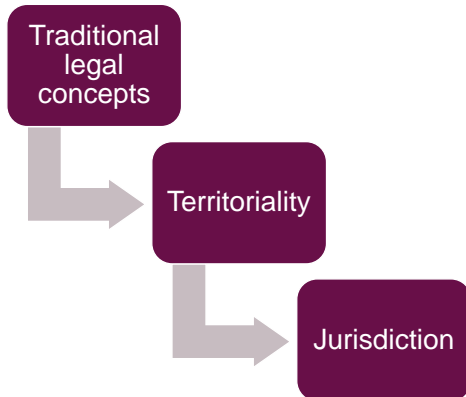
- Widest Cooperation Possible
- Dual Criminality
- Specialty Principle
- Proportionality



8

8

## Difficulties traditional MLA in cybercrime cases



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

## 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

## 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

11

11

## European Production and Preservation Orders

### Legal Basis, Subsidiarity and Proportionality

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



12

12

Titel  
 Datum 9 mei 2021

6

## 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 organize 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 utmost 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.

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



### Investigation:

- OSINT on Facebook: 'SlickRick'
- Phone number / IP-address
- Chat function
- Investigating the video
- Investigation victims' computer
- Investigation in the Police systems
- Investigation Bitcoin account
- Cooperation at Europol
- Plot twist and final



Thanks!  
Questions?



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

## (POST)COVID CHALLENGES IN CRIMINAL JUSTICE: INVESTIGATING WEB 2.0

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

The key features of the 2<sup>nd</sup> Additional Protocol to the Council of Europe Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

Bucharest  
20 September 2022

Ioana Albani  
DIICOT, prosecutor



With financial support of the European Union

## The mechanism of the Budapest Convention

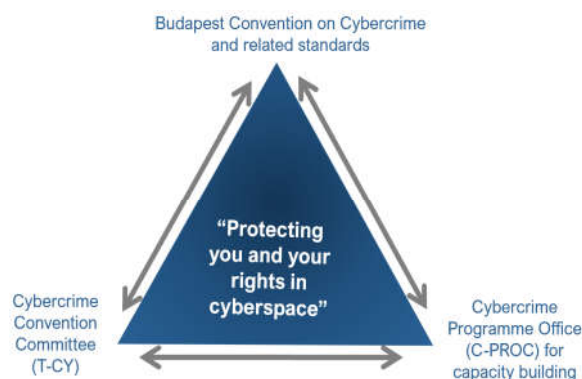
### Budapest Convention on Cybercrime (2001):

1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ 1<sup>st</sup> Protocol on Xenophobia and Racism via Computer Systems

+ Guidance Notes

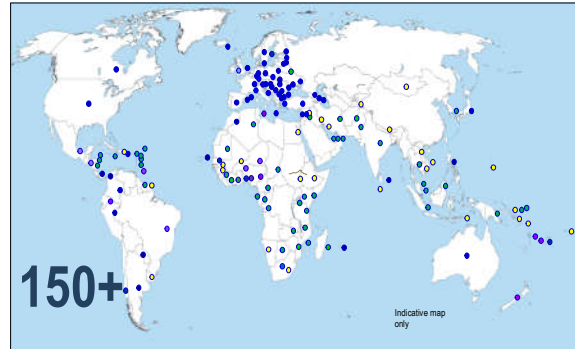
+ 2<sup>nd</sup> Protocol on enhanced cooperation on cybercrime and electronic evidence opened for signature 12 May 2022



## Reach of the Budapest Convention



- ✓ 20 years of Budapest Convention (2001-2021): global impact
- ✓ 66 Parties + 2 signatories + 13 States invited to accede
- ✓ 120+ States with substantive laws aligned with BC
- ✓ 150+ States have used it as a guideline or source
- ✓ 180+ States have been participating in COE activities on cybercrime
- ✓ Promoting rule of law and human rights in cyberspace



- ▶ **Multilateral instrument** – the same expected from 2<sup>nd</sup> Additional Protocol

## The mechanism of the Budapest Convention



TYPE OF EVIDENCE	LEGAL PROCESS
Computer system	<ul style="list-style-type: none"> <li>• search and seizure (Art.19)</li> </ul>
Computer data	<ul style="list-style-type: none"> <li>• expedited preservation (Art.16, Art.29)</li> <li>• production order (Art.18.1.a)</li> <li>• search and seizure (Art.19; Art.31)</li> <li>• interception of content data (Art.21; Art.34)</li> </ul>
Traffic data	<ul style="list-style-type: none"> <li>• expedited preservation of traffic data and partial disclosure (Art.16-17; Art.29-30)</li> <li>• production order (Art.18.1.a)</li> <li>• real-time collection of traffic data (Art.20; Art.33)</li> </ul>
Subscriber information	<ul style="list-style-type: none"> <li>• expedited preservation (Art.16; Art.29)</li> <li>• production order (Art.18.1.a and 18.1.b)</li> </ul>





### Protocol:

- Prepared by Protocol Drafting Plenary and Drafting Groups established by the Cybercrime Convention Committee September 2017 to May 2021
- 91 sessions of the PDP, PDG and PDG subgroups
- 75 States and several international organizations participated with over 620 experts
- Data protection experts participated in negotiations
- 6 rounds of stakeholder consultations



**Formally adopted on 17 November 2021**

**Carefully calibrated text designed to be consistent with the *acquis* of the Council of Europe but also to meet the requirements of all other Parties to the Budapest Convention**

**12 May 2022, Council of Europe, Strasbourg:  
Opening for signature of the 2<sup>nd</sup> Additional Protocol**

## 2<sup>nd</sup> Additional Protocol on enhanced co-operation and disclosure of electronic evidence



### CONTENT

#### Chapter I – Common provisions

Article 1 – Purpose

Article 2 – Scope of application

#### Article 3 – Definitions

- applicable definitions – Article 1; Article 18.3

+

- “central authority”

- “competent authority”

- “emergency”

- “personal data”

- “transferring Party”

Article 4 – Language

#### Chapter III – Conditions and safeguards

Article 13 – Conditions and safeguards

Article 14 – Protection of personal data

#### Chapter IV – Final provisions

Article 15-25

#### Chapter II - Measures for enhanced co-operation

Article 5 – General principles applicable to Chapter II

**Article 6** – Request for domain name registration information ► Gov2Private entity

**Article 7** – Disclosure of subscriber information ► Gov2Private entity

**Article 8** – Giving effect to orders from another party for expedited production of subscriber information and traffic data ► Gov2Gov (but not necessarily MLA)

**Article 9** – Expedited disclosure of stored computer data in an emergency ► Gov2Gov (but not necessarily MLA)

**Article 10** – Emergency mutual assistance ► Gov2Gov (MLA)

**Article 11** – Video conferencing ► Gov2Gov (MLA)

**Article 12** – Joint investigation teams and joint investigations ► Gov2Gov (MLA)

The 2<sup>nd</sup> Additional Protocol on  
enhanced co-operation and disclosure of electronic evidence



TYPE OF EVIDENCE	LEGAL PROCESS
Computer data	<ul style="list-style-type: none"> <li>• Art. 9 - Expedited disclosure of data in an emergency</li> <li>• Art. 10 – Emergency mutual assistance</li> </ul>
Traffic data	<ul style="list-style-type: none"> <li>• Art. 8 – Giving effects to orders from another party for expedited production of data (reservation possible)</li> <li>• Art. 9 – Expedited disclosure of data in an emergency</li> <li>• Art. 10 – Emergency mutual assistance</li> </ul>
Subscriber information	<ul style="list-style-type: none"> <li>• Art. 6 – Request for domain name registration (some information may be considered as a part of subscriber information)</li> <li>• Art. 7 – Disclosure of subscriber information</li> <li>• Art. 8 – Giving effects to orders from another party for expedited production of data (stand alone in certain conditions or as an enforcement mechanism)</li> </ul>

Article 12 – Joint investigation teams and joint investigation may serve as a procedure for obtain or exchange evidence in electronic form in a specific criminal investigation

The 2<sup>nd</sup> Additional Protocol on  
enhanced co-operation and disclosure of electronic evidence



### Article 1 – Purpose

The purpose of this Protocol is to supplement:

- the Convention as between the Parties to this Protocol; and
- the First Protocol as between the Parties to this Protocol that are also Parties to the First Protocol.

### Article 2 – Scope of application

Except as otherwise specified herein, the measures described in this Protocol shall be applied:

- as between Parties to the Convention that are Parties to this Protocol, **to specific criminal investigations or proceedings covered by Article 14 of the Budapest Convention:**
  - paragraph 2.a - offences provided by BCCC in Articles 2 to 11;
  - paragraph 2.b - other criminal offences committed by means of a computer system;
  - paragraph 2.c - the collection of evidence in electronic form of a criminal offence; and
- as between Parties to the First Protocol that are Parties to this Protocol, **to specific criminal investigations or proceedings concerning criminal offences established pursuant to the First Protocol.**

Each Party shall adopt such legislative and other measures as may be necessary to carry out the obligations set forth in this Protocol.



**Issue: no basis for direct cooperation**

**Current practices:**

- Limited information publicly offered/available due to data protection rules
- MLA

**Article 6 – Request for domain name registration information**

**OBJECTIVE** – to set legal basis and provide procedure for (voluntary) direct cooperation between the competent authorities of one Party and an entity providing domain name registration in the territory of another Party

**LIMITED SCOPE** – specific criminal investigation or proceeding (concerning criminal offences related to computer systems and data and to the collection of evidence in electronic form of a criminal offence) for information for identifying or contacting the registrant of a domain name



**Definitions used**

**2<sup>nd</sup>AP Art.3 - Competent authority means:**

- a judicial, administrative, or other law enforcement authority that is empowered by domestic law to order, authorize, or undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

**Legal construction**

based on the presumption that domestic law empowers the competent authorities in a Party to obtain the same data from entities located in its territory

**Parties to adopt any necessary measures:**

- to foresee for a **legal process** empowering their competent authorities to issue **a request to be submitted directly to an entity** in another Party providing domain name registration services (paragraph 1)
- to permit **an entity** in their territory to disclose such information in response to a request from a competent authority in another Party (paragraph 2)

**Standard format** (paragraph 3)

**Request** – may be an order, if provided in the domestic law

**No statement of facts is required, however additional information may be needed** (see ER para.85)

**Electronic transmission is permitted** (paragraph 4)



## EXECUTION

- **No enforcement** mechanism is provided. The execution is voluntarily for the requested entity
- **When no response**
  - ✓ the requesting Party may ask for the reason why the information is not disclosed
  - ✓ the requesting Party may seek consultations with the Party in which the entity is located (paragraph 5)

Paragraph 6 - Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, or at any other time, communicate to the Secretary General of the Council of Europe the authority designated for the purpose of consultation under paragraph 5.



## Safeguards Procedural safeguards

- the authority and its prerogatives for issuing the request – **“the competent authority”**
- **limited/standard information provided by the issuer including a statement** (paragraph 6.c) **that:**
  - the request is issued pursuant to this Protocol
  - the need for the information derives from its relevance to a specific criminal investigation or proceeding
  - the information will only be used for that specific criminal investigation or proceeding
- **limited information to be disclosed by the entity** (information for identifying or contacting the registrant of a domain name)
- **Art.13 – Conditions and safeguards** – reference to Article 15 of the Budapest Convention ► **each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Protocol are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties** ► principle of proportionality, other principles as appropriate in view of the nature of the procedure or power concerned, judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure
- **Art.14 of the Protocol related to the processing of personal data disclosed and transferred**



**Issue: Voluntary disclosure [of subscriber information] by service providers**

**Current practices:**

- More than 200,000 requests/year by BC Parties/Observers to major US providers
- Disclosure of subscriber information (ca. 64%)
- Providers decide whether to respond to lawful requests and to notify customers
- Provider policies/practices volatile
- Data protection concerns
- No admissibility of data received in some States

**OBJECTIVE** – to set legal basis and provide procedure for direct cooperation between the competent authorities of one Party and a service provider in the territory of another Party, which has possession or control of the data sought.

**Article 7 – Direct disclosure of subscriber information**

**LIMITED SCOPE** – specific criminal investigation or proceeding (concerning criminal offences related to computer systems and data and to the collection of evidence in electronic form of a criminal offence) and only for specified stored **subscriber information** that is **needed** for a specific investigation



**Definitions used**

**2<sup>nd</sup>AP Art.3 - Competent authority means:**

- a judicial, administrative, or other law enforcement authority that is empowered by domestic law to order, authorize, or undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

**BCCC Art.1 let. c – Service provider means:**

- any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
- any other entity that processes or stores computer data on behalf of such communication service or users of such service.

**BCCC Art.18 para.3 – Subscriber information means:**

- any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
  - the type of communication service used, the technical provisions taken thereto and the period of service;
  - the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
  - any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.



### Legal construction

based on the presumption that domestic law empowers the competent authorities in a Party to obtain the same data from a service provider located in its territory

### Parties to adopt any necessary measures:

- to foresee for a **legal process** to empower their competent authorities to issue **an order to be submitted directly** to a service provider in another Party (paragraph 1)
- to permit service providers in the territory of a Party **to respond** to an order issued by a competent authority in another Party and **to disclose** the subscriber information sought (paragraph 2.a)

### Standard format

(paragraphs 3 and 4)

### Electronic transmission permitted

(paragraph 6)



### Safeguards

**As a Requesting Party : Procedural safeguards**  
deriving from **the nature of the legal process according to the domestic law**  
(see Art.13 SAP – reference to Art.15 BCCC):

- **principle of proportionality** (the power or procedure should be proportional to the nature or circumstances of an offence); **principle of relevance** (the information sought must be relevant to the investigation); other principles as appropriate in view of the nature of the procedure or power concerned, **judicial or other independent supervision**, **grounds justifying application**, and **limitation of the scope** and the **duration** of such power or procedure

### As a requested Party: Specific safeguards

- **Declaration:** incoming orders made under Article 7 **must be issued by or under the supervision of a prosecutor or other judicial authority, or otherwise be issued under independent supervision** (paragraph 2.a)
- **Notification:**
  - **Simultaneous notification required** in every case or in identified circumstances when an order is sent to a service provider located in the Requested Party (paragraph 5.a)
    - ✓ the order; the supplemental information and a summary of the facts related to the investigation or proceeding
  - **Domestic consultation procedure -** in identified circumstances prior to disclosure when an order is sent to a service provider located in the Requested Party (paragraph 5.b)



**A single authority to receive notification** (paragraph 5.e)

**The authorities notified or consulted may, without undue delay, instruct the service provider not to disclose the subscriber information if** (paragraph 5.c):

- disclosure may prejudice criminal investigations or proceedings in that Party; or
- conditions or grounds for refusal would apply under Article 25 paragraph 4, and Article 27 paragraph 4 (political offence or related to; the execution is likely to prejudice its sovereignty, security, ordre public or other essential interests) of the Convention as if the subscriber information had been sought through mutual assistance

**The authorities notified or consulted with** (paragraph 5.d):

- may request additional information from the appropriate authority in the requesting Party for the purpose of determining whether the service provider should be instructed or not to disclose the subscriber information. **Additional information shall not be disclosed to the service provider without that authority's consent;** and
- shall promptly inform the appropriate authority in the Requesting Party if the service provider has been instructed not to disclose the subscriber information and give the reasons for doing so.



**Timeframe for execution** (paragraph 4.d and 7) **as in the order or 30 days of receipt of the order**

**Specific enforcement mechanism when** (paragraph 7):

- the time for the execution of the order has expired (the timeframe specified in the order or 30 days whichever period is longer)
- the service provider informed that it will not disclose the subscriber information sought (the issuing Party may request the reason)
- the service provider has been instructed not to disclose the subscriber information

**The issuing Party may seek to enforce the order only via Article 8 “Giving effect”** (a simplified procedure of conversion of the order into an enforceable order under a mechanism provided by the domestic law of the requested Party) **or other forms of mutual assistance.**

**Parties proceeding under this article may not seek unilateral enforcement.**



## Reservations/Declarations

A Party may, at the time of signature or when depositing its instrument of ratification, acceptance or approval:

- **declare** that an incoming order under Article 7 “**must be issued by or under the supervision of a prosecutor or other judicial authority, or otherwise be issued under independent supervision**” (a Party making use of this declaration must accept such an order) – paragraph 2.b
- **declare** that an issuing Party **shall seek disclosure of subscriber information from the service provider before seeking it under Article 8**, unless the issuing Party provides reasonable explanation for not having done so – paragraph 8
- **reserve the right not to apply this Article** – paragraph 9.a
- **Partial reservation** - if disclosure of certain types of **access numbers** would be inconsistent with the fundamental principles of its domestic legal system, **reserve the right not to apply this Article to such numbers** – paragraph 9.b

**A Party that made one or both reservations  
is not permitted to issue orders under this Article with respect to the object of the reservation**



**Issue: the sensitive nature of the traffic data/ different interpretation re dynamic/static IP, log in IP)**

### Current practices:

- Providers decide whether to respond to lawful requests and to notify customers
- Provider policies/practices volatile
- Data protection concerns
- No admissibility of data received in some States

**Article 8 – “Giving effect”**

**OBJECTIVE – compelling mechanism to produce data** upon an order issued by authorities in another Party, as a part of a request (a **simplified procedure of conversion of an order issued in another Party into an enforceable order under a mechanism provided by the domestic law of the requested Party**)

### LIMITED SCOPE

- a. production of stored **subscriber information or traffic data that is needed** in a specific criminal investigation or proceeding
- b. **specific enforcement mechanism for orders issued under Article 7**





## Definitions used

### 2<sup>nd</sup>AP Art.3 - Competent authority means:

- a judicial, administrative, or other law enforcement authority that is empowered by domestic law to order, authorize, or undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

### BCCC Art.1 let. c – Service provider means:

- any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
- any other entity that processes or stores computer data on behalf of such communication service or users of such service.

### BCCC Art.1 let. d – Traffic data means:

- any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of the underlying service

### BCCC Art.18 para.3 – Subscriber information means:

- any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
  - the type of communication service used, the technical provisions taken thereto and the period of service;
  - the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
  - any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.



## Legal construction

### Parties to adopt any necessary measures:

- to foresee for a **legal process** to empower their competent authorities (as Requesting Party) to issue **an order** as a part of a request to another Party (paragraph 1)
- to empower their authorities (as Requested Party) **to give effect** to an order issued under this article with a view of compelling a service provider in their territory to produce stored computer data (subscriber information or traffic data) – paragraph 2
  - ✓ **to give effect** – a legal mechanism in the Requested Party, at its choice, that makes the order enforceable under the domestic law (the order is accepted as an equivalent to domestic orders, or it is endorsed, thus giving it the same effect as a domestic one or is doubled by an order issued by the authorities in the Requested Party)



### Authorities involved (paragraph 10)

Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe and keep up to date the contact information of the authorities designated:

- to submit an order under this article; and
- to receive an order under this article.

A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, **declare that it requires that requests by other Parties under this article be submitted to it by the central authority of the Requesting Party**, or by such other authority as mutually determined between the Parties concerned (paragraph 11)

### Standard format

(paragraph 3)

### Electronic transmission permitted

(paragraph 5)



### Safeguards

#### As a Requesting Party: Procedural safeguards deriving from the nature of the legal process according to the domestic law

(see Art.13 SAP – reference to Art.15 BCCC):

- **principle of proportionality** (the power or procedure should be proportional to the nature or circumstances of an offence); **principle of relevance** (the information sought must be relevant to the investigation); other principles as appropriate in view of the nature of the procedure or power concerned, **judicial or other independent supervision, grounds justifying application, and limitation of the scope** and the **duration** of such power or procedure

#### As a Requested Party: Specific safeguards

- **Declaration** – a Party may declare at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, that **additional supporting information is required** to give effect to orders under this Article (paragraph 4)
- **Reservation** - a Party may reserve the right **not to apply this article to traffic data** (paragraph 13)
- **Grounds for refusal** (paragraph 8)
  - **BCCC** - Article 25, paragraph 4 – MLA is subject to conditions provided for by the law of the Requested Party or by applicable MLA. MLA shall not be refused in relation to the offences referred in Articles 2 to 11, solely on the ground that the request concern an offences which is considered a fiscal offence
  - **BCCC** - Article 27, paragraph 4 - the request concerns an offence which the requested Party considers a political offence, or an offence connected with a political offence, or it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.



**Issue: no common understanding on “emergency”, thus lack of predictability in providing responsive approaches in such cases**

### Article 3 – Definitions

...

2.c. For the purposes of this Protocol, the following additional definitions apply: an “emergency” means a situation in which there is a significant and imminent risk to the life or safety of any natural person;

#### Examples:

Hostage situations, kidnappings, ongoing sexual abuse of a child, anticipated terrorist attack, cyber attacks on critical infrastructure resulting in imminent death or injury.

**OBJECTIVE** – legal basis for obtaining immediate assistance in **emergency situations as defined**, for expedited disclosure of **specified, stored computer data** in a **service provider’s** possession or control in the territory of another Party, **without a request for mutual assistance.**

### Article 9 – Expedited disclosure of data in an emergency

- to enable Party’s 24/7 PoC to transmit a request to and receive a request from a 24/7 PoC in another Party, seeking immediate assistance
- to foresee for a legal process to empower a competent authority to seek data from a service provider in the Party’s territory following a request under Article 9 and to provide the requested data to the Requesting Party
- to adopt measures to enable a service provider to disclose the requested data to its authorities in response to a request formulated by its authorities pursuing a request under Article 9



## Definitions used

### 2<sup>nd</sup>AP Art.3 b. - Competent authority means:

- a judicial, administrative, or other law enforcement authority that is empowered by domestic law to order, authorize, or undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

### BCCC Art.1 let. c – Service provider means:

- any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
- any other entity that processes or stores computer data on behalf of such communication service or users of such service.

## Article 35 – 24/7 Network

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
  - a. the provision of technical advice;
  - b. the preservation of data pursuant to Articles 29 and 30;
  - c. the collection of evidence, the provision of legal information, and locating of suspects.
2. a. A Party’s point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
  - b. If the point of contact designated by a Party is not part of that Party’s authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. (...)



### Standard format (paragraph 3)

#### The request shall specify:

- the competent authority seeking the data and date on which the request was issued;
- a statement that the request is issued pursuant to this Protocol;
- the name and address of the service provider(s) in possession or control of the data sought;
- the offence(s) that is/are the subject of the criminal investigation or proceeding and a reference to its legal provisions and applicable penalties;
- **sufficient facts to demonstrate that there is an emergency and how the data sought relates to it;**
- a detailed description of the data sought;
- any special procedural instructions; and
- any other information that may assist in obtaining disclosure of the requested data.

**Electronic transmission permitted, orally transmission permitted, however, may require confirmation in electronic form** (paragraph 4)



### Procedural issues and/or limitations

- A Requested Party, when applicable, **may specify conditions under which it would provide the data or any other forms of co-operation that may be available** (paragraph 6)
  - when the requesting Party cannot comply with, it shall immediately inform, and the requested Party shall determine whether the information or material should nevertheless be provided
  - when the requesting Party accept them, it shall be bound to respect them
- **Declaration**  
As a Requested Party, that:
  - will not execute requests under Article 9 seeking only the disclosure of subscriber information (paragraph 1.b)
  - requires following the execution of the request, that the Requesting Party to submit the request and any supplemental information transmitted in support thereof, in a format and through such channel, which may include mutual assistance, as specified (paragraph 5)



Issue: no common understanding on “emergency”, thus lack of predictability in providing responsive approaches in such cases

#### Article 3 – Definitions

...

2.c. For the purposes of this Protocol, the following additional definitions apply: an “emergency” means a situation in which there is a significant and imminent risk to the life or safety of any natural person;

#### Examples:

Hostage situations, kidnappings, ongoing sexual abuse of a child, anticipated terrorist attack, cyber attacks on critical infrastructure resulting in imminent death or injury.

**OBJECTIVE** - to provide a maximally expedited procedure for mutual assistance requests made in emergency situations as defined

#### Article 10 Emergency mutual assistance

- **mandatory content** besides the content required in a mutual assistance request ▶ **a description of the facts that demonstrate that there is an emergency and how the assistance sought relates to it**
- **obligation to ensure** with the central authorities or other authorities responsible **a system available 24/7 with the purpose of reviewing a request in an emergency situation outside business hours** – this doesn't mean a central authority may become operative
- **declaration to nominate 24/7 PoC as a channel of transmission**



#### Definitions used

2ndAP Art.3 a. – “central authority” means:

- the authority or authorities designated under a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned, or, in the absence thereof, the authority or authorities designated by a Party under Article 27, paragraph 2.a, of the Convention ▶ Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution (see paragraph 38-39 of the ER)

**Electronic transmission permitted** (paragraph 2)

**Declaration** (paragraph 9)

As a Requested Party – that accepts requests sent directly to its judicial authorities or through INTERPOL, 24/7 POC with a simultaneous copy sent to its CA

#### EXECUTION

- **Article 25, paragraph 4** of the Convention applies to the execution of a request made under Article 10
- Such execution is subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation.**



## EXECUTION

- Where **NO mutual assistance treaty or arrangement based on uniform or reciprocal legislation is in force** between the Requesting and Requested Parties, **a request made under Article 10** (paragraph 7)
  - ✓ shall be executed in accordance with the procedures specified by the Requesting Party, except where incompatible with the law of the Requested Party (paragraph 7 reference to article 27.3 of BCCC)
  - ✓ the Requesting Party may request that the Requested Party keep confidential the request made under this Article, except to the extent necessary for its execution. If the Requested Party cannot comply with the request for confidentiality, it shall promptly inform the Requesting Party, which shall then determine whether the request should nevertheless be executed (paragraph 7 reference to article 27.8 BCCC complemented with the provisions of Article 28.2 and 28.4 BCCC on confidentiality and limitation of use)
- Where between the Requesting Party and the Requested Party **IS** in force **a mutual assistance treaty or arrangement based on uniform or reciprocal legislation** (paragraph 8)
  - ✓ the application of Article 10 shall be supplemented by the provisions of such a treaty or arrangement **except** for the situation in which the parties involved decide to apply any or all the provisions of the BC, specifically any or all the provisions mentioned in paragraph 7 (Article 27.2b; 27.3; 27.8; 28.2 and 28.4 BCCC) – paragraph 8

## “Emergency situation” vs “Urgent circumstances” (Article 25 BCCC)



### ➤ “emergency situation” – defined

- ✓ limited application to the situations falling under the definition of “emergency situation”
- ✓ obligation to put in place with the central authorities or other authorities responsible a system available 24/7 with the purpose of reviewing outside business hours, a request made in an emergency situation
- ✓ legal basis for a mutually determined channel for transmission of the response/evidence
- ✓ possibility for a declaration that makes available other channels than the Central Authority for transmitting a request in an emergency situation
- ✓ obligation for accepting an electronic transmission of the request under appropriate level of security

### ➤ “urgent circumstances” – not defined

- ✓ broader application
- ✓ it is likely that the urgency may derive from a high risk of losing the data/evidence in electronic form
- ✓ the objective of paragraph 3 is to facilitate acceleration of the process of obtaining mutual assistance
- ✓ empower the Parties **to make urgent requests** for co-operation **through expedited means of communications**
- ✓ require the **Requested Party to use expedited means to respond to requests in such circumstances**
- ✓ **each Party is required to have the ability to apply this measure if its mutual assistance treaties, laws or arrangement do not already so provide**



### Article 10

**OBJECTIVE** - to provide legal basis for a maximally expedited procedure for **mutual assistance requests** made in emergency situations

#### LIMITED to emergency situations as defined

**NOT LIMITED to stored evidence in a service provider's possession or control in the territory of another Party**

**Mandatory content** - a description of the facts that demonstrate that there is an emergency and how the assistance sought relates to it

**Option for a Party to declare the 24/7 Point of Contact as a channel of transmission**

### Article 9

**OBJECTIVE** – legal basis for obtaining immediate assistance for expedited disclosure of **specified, stored computer data** without a request for mutual assistance.

**LIMITED to specified stored computer data in a service provider's possession or control** in the territory of another Party

**Standard content**

**Legal process** to enable the 24/7 Point of Contact to transmit a request to and receive a request from a 24/7 Point of Contact in another Party seeking immediate assistance



### Article 13 – Conditions and safeguards

- reference to **Article 15 of the Budapest Convention**
- ✓ each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties
- ✓ principle of proportionality, other principles as appropriate (as principle of relevance) in view of the nature of the procedure or power concerned, judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure

#### Application in Article 6 to 9

accompanied with a set of more specific/dedicated conditions and safeguards provided for in each article, such as:

- **Article 6** – limited information to be disclosed, standard format para.3
- **Article 7** – limited scope (information sought) declaration under para.2a, para.8, para.9a and 9b; mechanism for simultaneous notification and/or consultation procedure under para.5a, 5b, 5e, grounds for refusal under para.5c, standard format para.3 and 4
- **Article 8** – para.4, partial reservation para.13, standard format para.3
- **Article 9** – limited scope (emergency situation), declaration para.1b, post disclosure procedure para.5



### Operational value:

- Legal basis for disclosure of WHOIS information
- Basis for direct cooperation with service providers for subscriber information (“direct disclosure”)
- Effective means to obtain subscriber information and traffic data (“giving effect”)
- Cooperation in emergencies (“expedited disclosure” + “emergency MLA”)
- Mutual assistance tools (“video-conferencing”, “JITs”)
- Data protection safeguards to permit the flow of personal data under the Protocol

### Policy value:

- Convention on Cybercrime will remain relevant and effective
- Efficient cooperation with rule of law and data protection safeguards is feasible
- Respect for free Internet with limited restrictions in case of criminal misuse (specific criminal investigations, specified data)

**THANK YOU!**

Ioana Albani  
Prosecutor  
albani\_ioana@mpublic.ro